ESET PROTECT

Guia de Instalação Atualização e Migração

Clique aqui para exibir a versão da Ajuda deste documento

Digital Security
Progress. Protected.

ESET PROTECT foi desenvolvido por ESET, spol. s r.o.

Para obter mais informações, visite https://www.eset.com.

Suporte técnico: https://support.eset.com

REV. 17-04-2024

Sobre a ajuda

Este guia de instalação foi escrito para ajudá-lo com a instalação e atualização do ESET PROTECT e oferece instruções para o processo.

Para fins de uniformidade e para ajudar a impedir confusão, a terminologia usada neste guia é baseada nos nomes de parâmetros ESET PROTECT. Também usamos um conjunto de símbolos para destacar tópicos de interesse ou significado em particular.

As notas podem oferecer informações valiosas, como recursos específicos ou um link para algum tópico relacionado.

Isso requer sua atenção e não deve ser ignorado. Normalmente, oferece informações não críticas, mas significativas.

Informações críticas que devem ser tratadas com grande cuidado. Os alertas são colocados especificamente para impedi-lo de cometer erros potencialmente nocivos. Leia e compreenda o texto colocado nos parênteses de alerta, pois eles fazem referência a configurações do sistema altamente sensíveis ou a algo arriscado.

Cenário de exemplo que descreve um caso de usuário relevante para o tópico onde está incluído. Exemplos são usados para explicar tópicos mais complicados.

Convenção	Significado
Negrito	Nomes de itens de interface como caixas e botões de opção.
Itálico	Espaço reservado para informações fornecidas por você. Por exemplo, nome de arquivo ou caminho significa o caminho ou nome do arquivo real.
`Courier New`	Amostras ou comandos de código.
Hyperlink	Fornece um acesso rápido e fácil a tópicos de referência cruzada ou a um local da web externo. Hyperlinks são destacados em azul e podem estar sublinhados.
%ProgramFiles%	O diretório do sistema Windows que armazena programas instalados do Windows e outros.

- A Ajuda on-line é a fonte primária de conteúdo de ajuda. A versão mais recente da Ajuda on-line será exibida automaticamente quando você tiver uma conexão com a internet que funcione. As páginas de ajuda on-line ESET PROTECT incluem quatro guias ativas no topo do cabeçalho de navegação: Instalação/Atualização, Administração, Instalação VA e Guia SMB.
- Os tópicos neste guia são divididos em vários capítulos e subcapítulos. Você pode encontrar informações relevantes usando o campo Pesquisar no topo.

Depois de abrir o Guia do Usuário da barra de navegação no topo da página, a pesquisa será limitada aos conteúdos daquele guia. Por exemplo, se você abrir o guia do Administrador, tópicos dos guias de Instalação/Atualização e Implantação VA não serão incluídos nos resultados de pesquisa.

- A Base de conhecimento ESET contém respostas para as perguntas mais frequentes, assim como soluções recomendadas para vários problemas. Atualizada regularmente por especialistas técnicos, a Base de conhecimento é a ferramenta mais poderosa para solucionar vários tipos de problemas.
- O Fórum ESET oferece aos usuários ESET uma forma fácil de obter ajuda e de ajudar os outros. Você pode postar qualquer problema ou pergunta relacionada aos seus produtos ESET.

Instalação/atualização/migração

ESET PROTECT é um aplicativo que permite que você gerencie produtos ESET em estações de trabalho de cliente, servidores e dispositivos móveis em um ambiente em rede a partir de um local central. Com o sistema de gerenciamento de tarefas integrado do ESET PROTECT, você pode instalar soluções de segurança ESET em computadores remotos e responder rapidamente a novos problemas e detecções.

o ESET PROTECT não fornece proteção contra código malicioso por si próprio. A proteção de seu ambiente conta com a presença de uma solução de segurança ESET como ESET Endpoint Security em estações de trabalho e dispositivos móveis ou ESET Server Security para Windows nas máquinas do servidor.

o ESET PROTECT foi desenvolvido com base em dois princípios essenciais:

- **Gerenciamento centralizado** - a rede inteira pode ser configurada, gerenciada e monitorada de um só lugar.

- **Escalabilidade** - o sistema pode ser implantado em uma pequena rede, assim como em ambientes de grandes empresas. O ESET PROTECT é projetado para acomodar o crescimento da sua infraestrutura.

O ESET PROTECT é compatível com a nova geração de produtos de segurança ESET e também com a geração anterior de produtos.

As páginas de ajuda ESET PROTECT incluem um guia completo de instalação e atualização:

- Arquitetura do ESET PROTECT
- Processo de instalação
- Procedimentos de atualização
- Procedimentos de migração
- Procedimentos de desinstalação
- Gerenciamento de licenças
- Processos de implantação e Implementação do agente usando GPO ou SCCM
- Primeiras etapas após a instalação do ESET PROTECT
- Guia de Administração

Novos recursos no ESET PROTECT 10.1

Visualização da empresa para clientes MSP

Os administradores do MSP podem filtrar dados na seção Painel por cliente. Além disso, há uma nova seção dedicada do menu, Clientes gerenciados, onde os administradores podem obter uma visão geral de todos os clientes gerenciados. Agora, os administradores do MSP também podem filtrar modelos de relatório por cliente ao criar relatórios agendados por meio da tarefa Agendar relatórios ou de uma tarefa do servidor. Saiba mais

Agrupamento de detecções

Agora você pode agrupar detecções por atributos comuns como categoria de detecção, computador, gravidade e assim por diante. Assim, fica mais fácil navegar pelas detecções e encontrar uma específica. Saiba mais

Pesquisa aprimorada

Agora você pode pesquisar dentro do ESET PROTECT mais facilmente, sem precisar escolher a categoria primeiro. Basta começar a escrever a palavra-chave, e ela será pesquisada em todas as categorias. Saiba mais

Outras melhorias e correções de bugs

Descubra o que mais foi melhorado no registro de mudanças.

Arquitetura

O ESET PROTECT é uma nova geração de um sistema de gerenciamento remoto.

Para realizar uma implantação completa dos produtos de segurança ESET, instale os componentes a seguir (plataformas Windows e Linux):

- Servidor ESET PROTECT
- Console da Web ESET PROTECT
- Agente ESET Management

Os seguintes componentes compatíveis são opcionais, recomendamos que você os instale para garantir o melhor desempenho do aplicativo na rede:

- Sensor RD
- ESET Bridge Proxy HTTP
- Mobile Device Connector

Componentes do ESET PROTECT usam certificados para fazerem a comunicação com o Servidor ESET PROTECT. Leia mais sobre certificados no ESET PROTECT no nosso artigo da Base de conhecimento.

Visão geral dos elementos de infraestrutura

A tabela abaixo contém uma visão geral dos elementos de infraestrutura do ESET PROTECT e suas funções principais:

Funcionalidade	ESET PROTECTServidor	Agente ESET Management	Produto de Segurança ESET	ESET Bridge Proxy HTTP	Servidor ESET	Conector de dispositivo móvel
Gerenciamento remoto de produtos de segurança ESET (criação de políticas, tarefas, relatórios, etc.)	✔	X	X	X	X	X
Comunicação com o Servidor ESET PROTECT e gerenciamento do produto de segurança ESET no dispositivo do cliente	X	✔	X	X	X	✔

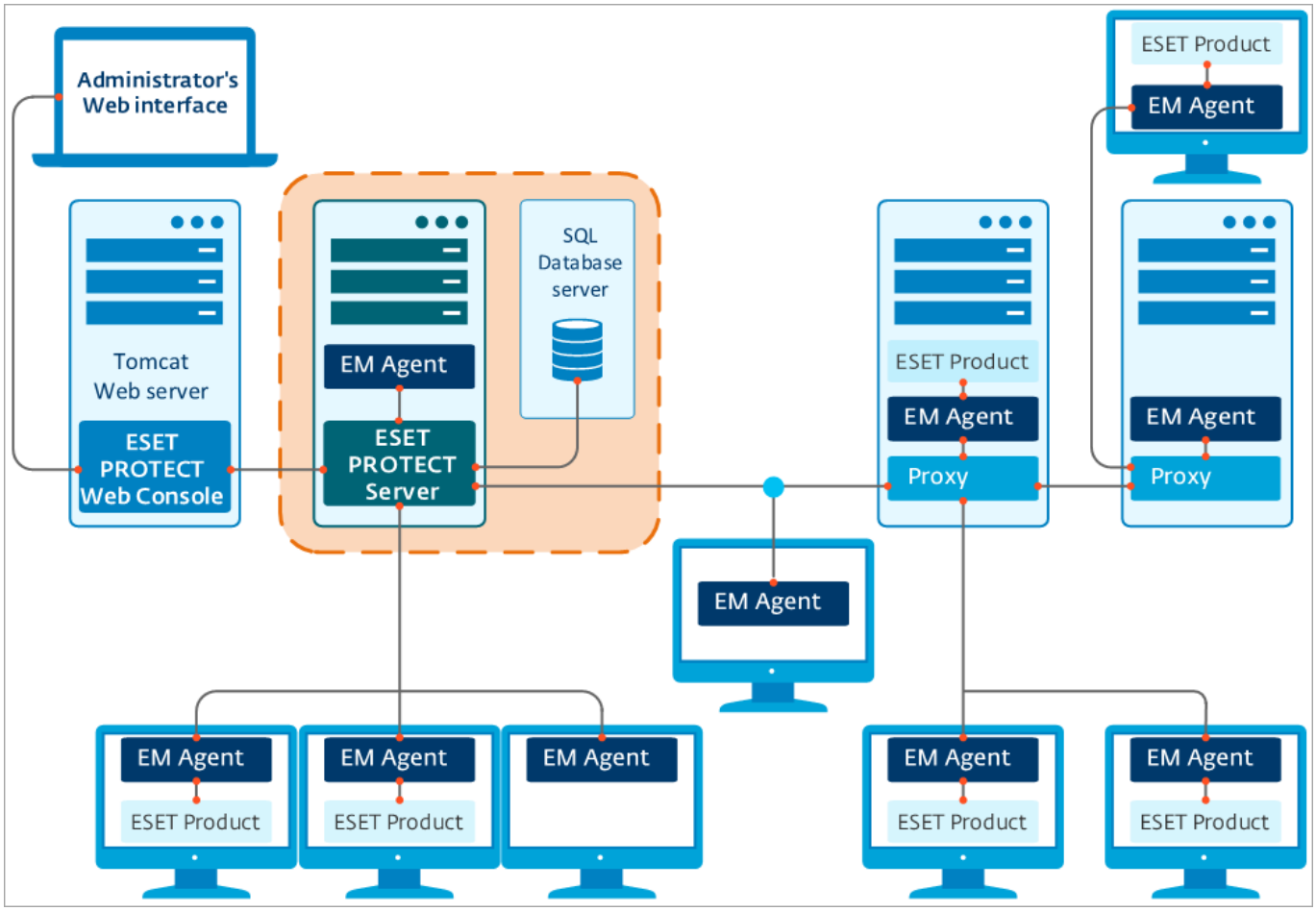
Funcionalidade	ESET PROTECTServidor	Agente ESET Management	Produto de Segurança ESET	ESET Bridge Proxy HTTP	Servidor ESET	Conector de dispositivo móvel
Fornecimento de atualizações, validação de licença	X	X	X	*	✔	X
Armazenamento em cache e encaminhamento de atualizações (mecanismo de detecção, instaladores, módulos)	X	X	**	✔	X	X
Encaminhamento de tráfego da rede entre o Agente ESET Management e o Servidor ESET PROTECT	X	X	X	✔	X	X
Proteção do dispositivo do cliente	X	X	✔	X	X	X
Gerenciamento remoto de dispositivos móveis	X	X	X	X	X	✔

* Apenas com um repositório off-line.

** Os produtos de segurança ESET não armazenam instaladores em cache.

Servidor

O Servidor ESET PROTECT é o aplicativo executivo que processa todos os dados recebidos de clientes que se conectam ao Servidor (por meio do Agente ESET Management ou HTTP Proxy). Para processar dados corretamente, o Servidor exige uma conexão estável com um servidor de banco de dados no qual os dados de rede são armazenados. Recomendamos que você instale o servidor de banco de dados em outro computador para obter melhor desempenho.

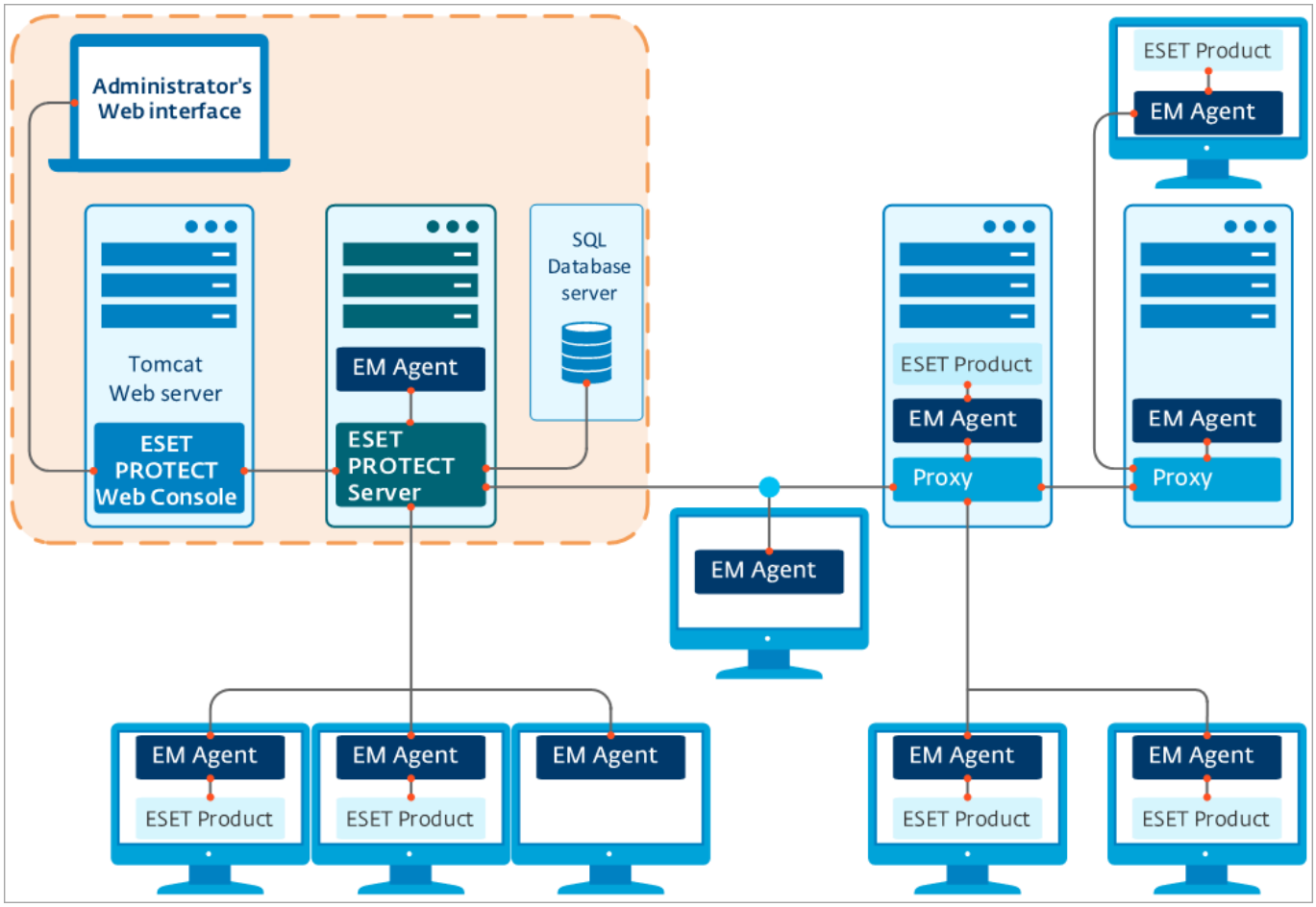


Web Console

O Console web ESET PROTECT é uma interface do usuário baseada na web que permite que você gerencie soluções de segurança da ESET em seu ambiente. Ele exibe uma visão geral do status de clientes em sua rede e pode ser usado para implantar remotamente soluções da ESET em computadores não gerenciados. O Web Console é acessado por meio do navegador (consulte Navegadores da Web compatíveis). Se você escolher tornar o servidor Web acessível pela internet, poderá usar o ESET PROTECT de praticamente qualquer lugar e dispositivo.

O console web usa o Apache Tomcat como o servidor web HTTP. Ao usar o Tomcat em conjunto no instalador ESET ou na Máquina virtual, ele permite apenas conexões TLS 1.2 e 1.3 ao console web.

Você pode escolher instalar o Web Console ESET PROTECT em um computador diferente do computador executando o Servidor ESET PROTECT.



ESET Bridge Proxy HTTP

Você pode usar o ESET Bridge com o ESET PROTECT como um serviço de Proxy para:

- Download e cache: Atualizações de módulos ESET, pacotes de instalação e atualização pressionados pelo ESET PROTECT (por exemplo, instalador MSI ESET Endpoint Security), atualizações de produto de segurança ESET (atualizações de componente e produto), resultados ESET LiveGuard.

- Encaminhar comunicação dos Agentes ESET Management com o Servidor ESET PROTECT.

Leia a Ajuda on-line ESET Bridge para mais detalhes sobre a instalação e configuração do ESET Bridge.

Apache HTTP Proxy usuários

Começando com o ESET PROTECT 10.0, o ESET Bridge substitui o Apache HTTP Proxy. O Apache HTTP Proxy agora está com Suporte limitado. Se você usar o Apache HTTP Proxy, recomendamos migrar para o ESET Bridge.

Agente

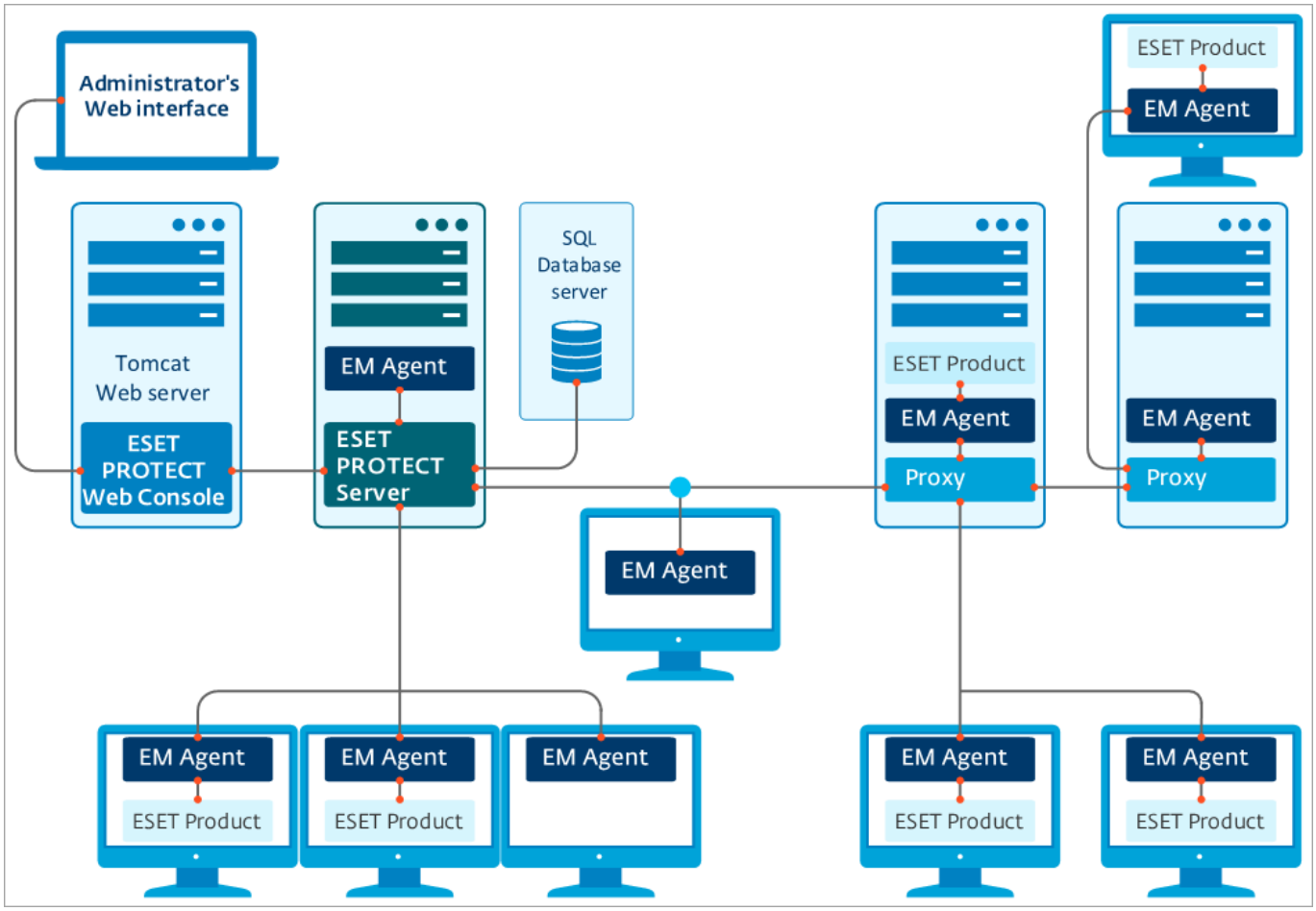
O Agente ESET Management é uma parte essencial do ESET PROTECT. Os clientes não se comunicam diretamente com o Servidor ESET PROTECT, em vez disso o Agente facilita essa comunicação. O Agente coleta informações do cliente e as envia para o Servidor ESET PROTECT. Se o Servidor ESET PROTECT enviar uma tarefa para o cliente, ela é enviada para o Agente e o Agente enviará essa tarefa para o cliente. O Agente ESET Management está usando um novo protocolo de comunicação melhorado.

Para simplificar a implementação da proteção de endpoint, o Agente ESET Management autônomo é incluído no pacote ESET PROTECT. Ele é um serviço simples, extremamente modular e ágil que cobre toda a comunicação entre o servidor ESET PROTECT e qualquer sistema operacional ou produto ESET. Em vez de se comunicar diretamente com o Servidor ESET PROTECT, os produtos ESET se comunicam por meio do Agente. Computadores cliente que tenham o Agente ESET Management instalado e podem se comunicar com o servidor ESET PROTECT são chamados de "gerenciados". Você pode instalar o Agente em qualquer computador, independentemente de outro software ESET ter sido instalado ou não.

Os benefícios são:

- Fácil de configurar – você pode implantar o Agente como parte da instalação corporativa padrão.
- Gerenciamento de segurança vigente – como o Agente pode ser configurado para armazenar vários cenários de segurança, o tempo de reação a uma detecção é significativamente reduzido.
- Gerenciamento de segurança off-line - o Agente pode responder a um evento se não estiver conectado ao servidor ESET PROTECT.

O protocolo de comunicação entre o Agente e o Servidor ESET PROTECT não é compatível com a autenticação. Qualquer solução de proxy usada para encaminhar a comunicação do Agente para o Servidor ESET PROTECT e que precise de autenticação não funcionará.
Se você escolher usar uma porta não padrão para o console web ou Agente, poderá ser necessário fazer um ajuste de firewall. Caso contrário, a instalação poderá falhar.



Sensor Rogue Detection

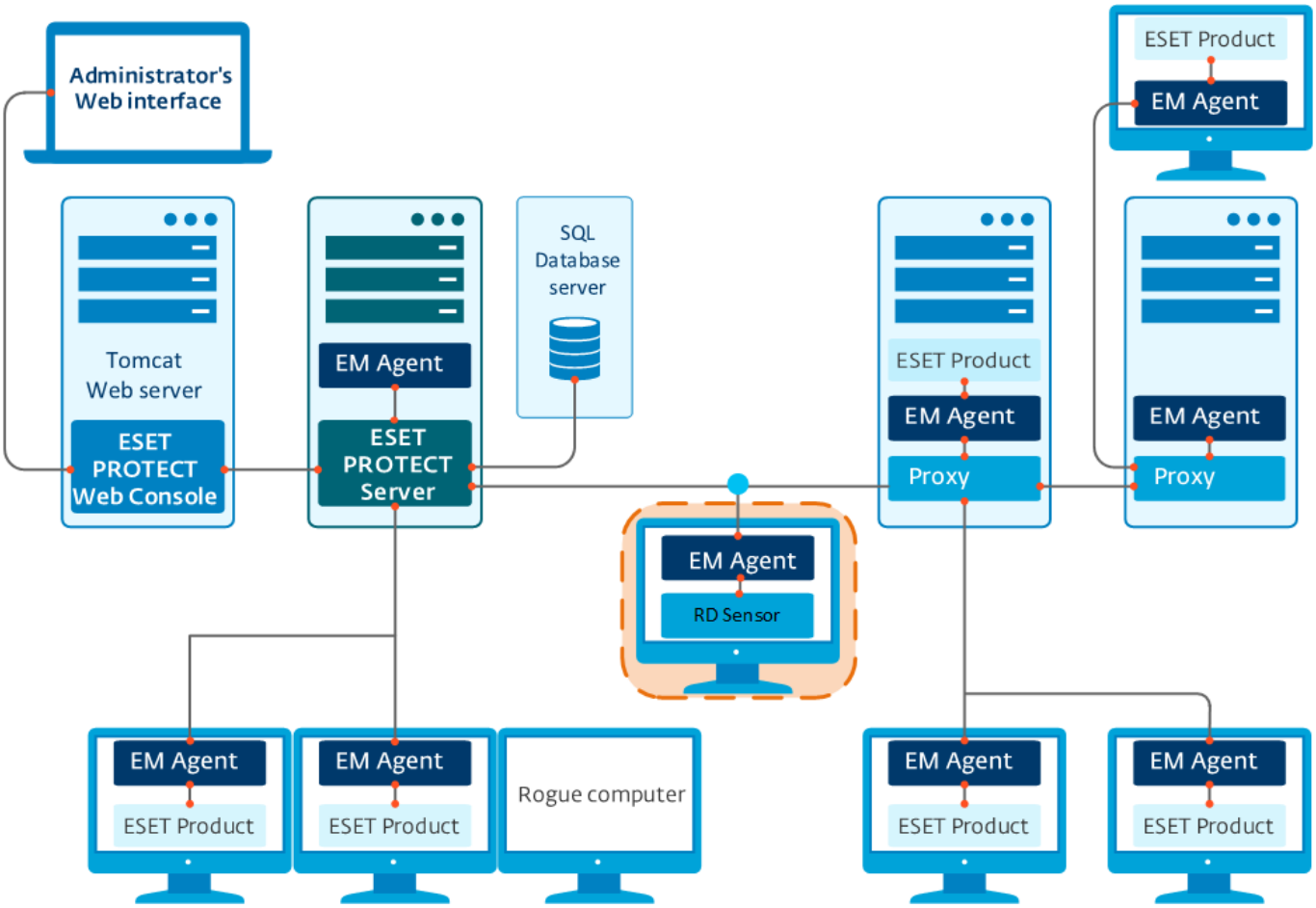
O **Rogue Detection Sensor (Sensor RD)** é uma ferramenta de detecção de sistema invasor que pesquisa sua rede de computadores. O Sensor é conveniente, pois pode localizar novos computadores do ESET PROTECT, sem a necessidade de pesquisar e adicioná-los manualmente. Máquinas descobertas são imediatamente localizadas e reportadas em um relatório pré-definido, permitindo que você mova-as para grupos estáticos específicos e continue com as tarefas de gerenciamento.

O RD Sensor escuta ativamente as transmissões ARP. Quando o RD Sensor detecta um novo componente de rede ativo, o RD Sensor envia os unicasts ARP, realiza a impressão digital do host (usando várias portas) e envia informações sobre os computadores detectados para o Servidor ESET PROTECT. O Servidor ESET PROTECT então avalia se os PCs detectados na rede são desconhecidos para o servidor ESET PROTECT ou se já são gerenciados.

Não é possível desativar a impressão digital do host porque ela é a principal funcionalidade do RD Sensor.

Se houver vários segmentos de rede, o Rogue Detection Sensor deve ser instalado separadamente em cada segmento de rede para produzir uma lista abrangente de todos os dispositivos em toda a rede.

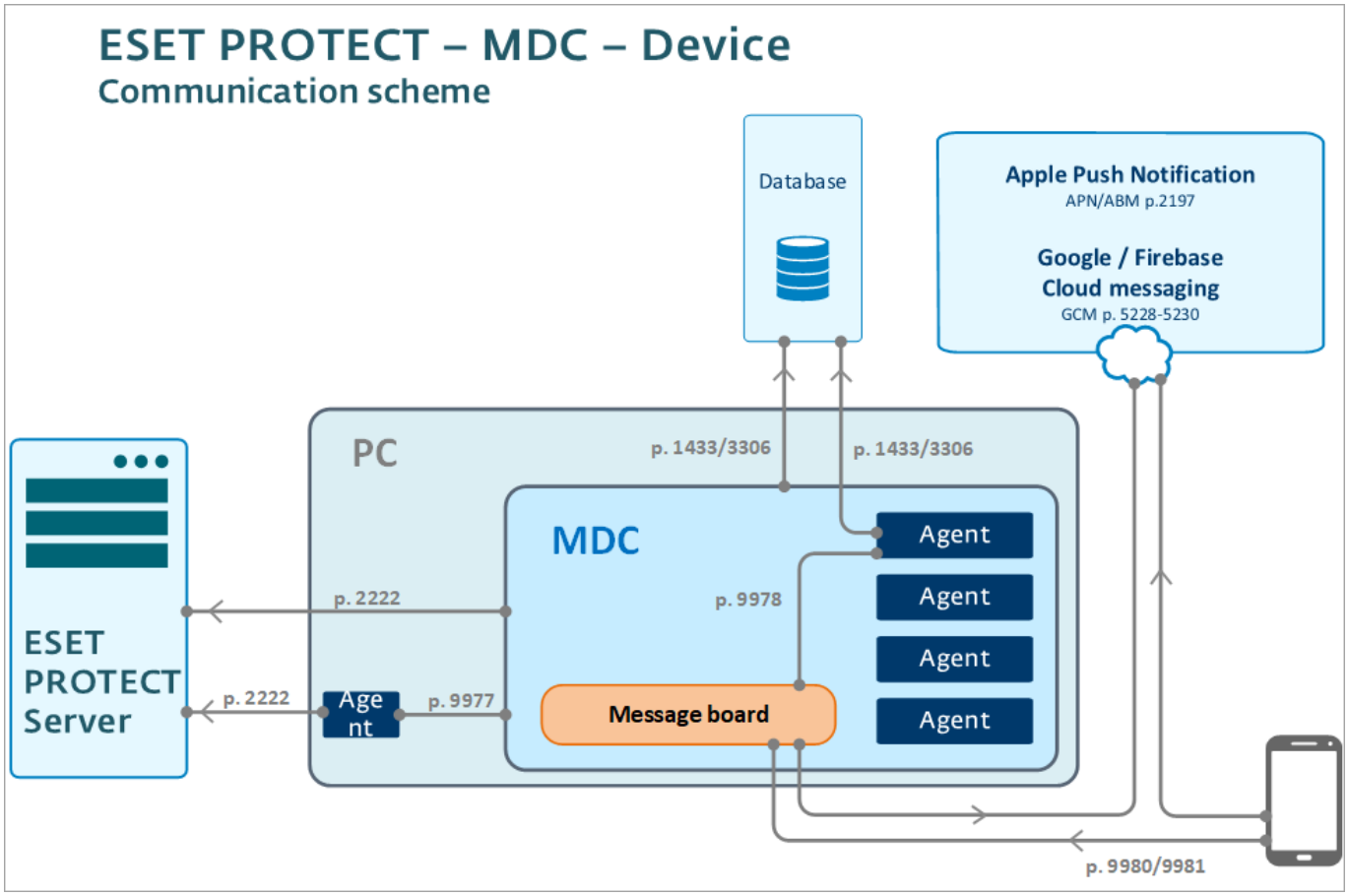
Cada computador na estrutura da rede (domínio, LDAP, rede Windows) é adicionado automaticamente à lista de computadores do Servidor ESET PROTECT por meio de uma tarefa de sincronização de servidor. O uso do RD Sensor é uma forma conveniente de localizar computadores que não estão no domínio ou outra estrutura de rede e adicioná-los ao servidor ESET PROTECT. O RD Sensor lembrará dos computadores que já estão detectados e não enviará as mesmas informações duas vezes.



Conector de dispositivo móvel

O Conector de dispositivo móvel ESET PROTECT é um componente que permite o gerenciamento de dispositivo móvel com o ESET PROTECT, permitindo a você gerenciar dispositivos móveis (Android e iOS) e administrar o ESET Endpoint Security para Android.

O componente do Gerenciamento de dispositivo móvel/Conector ESET PROTECT (MDM/MDC) (apenas no local) teve seu fim da vida útil agendado. Ler mais. Recomendamos que você migre para o gerenciamento de dispositivo móvel em nuvem.



Ver a imagem maior

Recomendamos que você instale seu componente MDM em um dispositivo host separado daquele que é o host do Servidor ESET PROTECT.

As pré-condições de hardware recomendadas para aproximadamente 80 dispositivos móveis gerenciados são:

Hardware	Configuração recomendada
Processador	4 núcleos, 2.5 GHz
RAM:	4 GB (recomendado)
HDD	100 GB

Para mais de 80 dispositivos móveis gerenciados, os requisitos de hardware não são muito maiores. A latência entre o envio da tarefa do ESET PROTECT e a execução da tarefa no dispositivo móvel vai aumentar proporcionalmente dependendo do número de dispositivos no seu ambiente.

Siga as instruções de instalação MDM para Windows (Instalador tudo-em-um ou instalação de componente) ou Linux.

Diferenças entre o ESET Bridge Proxy HTTP, Ferramenta de imagem e conectividade direta

A comunicação do produto ESET envolve o mecanismo de detecção e atualizações do módulo de programa, assim como a troca de dados ESET LiveGrid® (veja a tabela abaixo) e informações de licença.

O ESET PROTECT faz o download dos produtos mais recentes para distribuição aos computadores clientes a partir do repositório. Depois de distribuído, o produto está pronto para ser implantado na máquina de destino.

Assim que um produto de segurança ESET estiver instalado, ele deve ser ativado, ou seja, o produto precisa verificar suas informações de licença no servidor de licença. Depois da ativação, o mecanismo de detecção e os módulos do programa são atualizados regularmente.

O ESET LiveGrid® Early Warning System ajuda a garantir que a ESET seja informada imediata e continuamente sobre novas infiltrações para proteger rapidamente nossos clientes. O sistema permite que novas detecções sejam enviadas ao Laboratório de Ameaças ESET, onde elas são analisadas e processadas.

A maioria do tráfego de rede é gerado por atualizações dos módulos do produto. Em geral, um produto de segurança ESET faz download de aproximadamente 23,9MB de atualizações de módulo em um mês.

Dados do ESET LiveGrid® (aproximadamente 22,3 MB) e o arquivo da versão de atualização (até 11 Kb) são os únicos arquivos distribuídos que não podem ser armazenados em cache.

Há dois tipos de lista de atualizações – atualizações de nível e nano. Visite nosso artigo da Base de conhecimento para mais informações sobre tipos de atualização.

Existem duas formas de diminuir a carga da rede ao distribuir atualizações para uma rede de computadores, ESET BridgeProxy HTTP ou Ferramenta de imagem (disponível para Windows e Linux).

> Leia este artigo da Base de conhecimento para configurar o encadeamento da Ferramenta de imagem (configurar a Ferramenta de imagem para fazer download de atualizações de outra Ferramenta de imagem).

Tipos de comunicação ESET

Tipo de comunicação	Frequência de comunicação	Impacto de tráfego de rede	Comunicação encaminhada por proxy	Opção de armazenamento em cache de Proxy1	Opção de Imagem2	Opção de ambiente off-line
Implantação do agente (Push / Instaladores em tempo real do repositório)	Uma vez	Aproximadamente 50 MB por cliente	SIM	SIM3	NÃO	SIM (GPO / SCCM, instaladores em tempo real editados)4
Instalação Endpoint (Instalação de software do repositório)	Uma vez	Aproximadamente 100 MB por cliente	SIM	SIM3	NÃO	SIM (GPO / SCCM, instalação por pacote de URL)4
Módulo do mecanismo de detecção / Atualização de módulo do programa	6+ vezes por dia	23.9 MB por mês5	SIM	SIM	SIM	SIM (Off-line Mirror Tool e Servidor HTTP personalizado)6
Atualização do arquivo de versão update.ver	~ 8 vezes por dia	2.6 MB por mês7	SIM	NÃO	-	-
Verificação de Ativação / Licenciamento	4 vezes por dia	desprezível	SIM	NÃO	NÃO	SIM (Arquivos off-line gerados em ESET Business Account)8
ESET LiveGrid® Reputação baseada em nuvem	Instantaneamente	11 MB por mês	SIM	NÃO	NÃO	NÃO

1.Para o impacto / benefícios de cache em proxy veja Quando começar a usar o ESET Bridge Proxy HTTP?

2.Para o impacto da imagem veja Quando começar a usar a Ferramenta de imagem?

3.Uma vez por instalação / atualização, recomendamos que você implante um agente (um por versão específica) / endpoint inicialmente para que o instalador seja armazenado em cache.

4.Para implantar o Agente ESET Management em uma rede grande, veja Implantação do agente usando GPO e SCCM.

5.Sua atualização inicial do mecanismo de detecção pode ser maior do que o normal, dependendo da idade do pacote de instalação, pois todas as atualizações do mecanismo de detecção e atualizações de módulo serão baixados. Recomendamos instalar um cliente inicialmente e deixá-lo atualizar, para que as atualizações necessárias do mecanismo de detecção e de módulos do programa sejam armazenadas em cache.

6.Sem uma conexão com a internet, o Mirror Tool não consegue fazer download de atualizações do mecanismo de detecção. Você pode usar o Apache Tomcat como um servidor HTTP para fazer download da atualização para um diretório disponível na Ferramenta de imagem (disponível para Windows e Linux).

7.Ao buscar atualizações do mecanismo de detecção, o arquivo *update.ver* é sempre baixado e analisado. Por padrão, a Agenda do produto endpoint ESET está consultando para uma nova atualização a cada hora. Assumimos que uma estação de trabalho do cliente está ligada 8 horas por dia. O arquivo *update.ver* contém aproximadamente 11 kB.

8.Fez download do arquivo de licença off-line ESET Business Account.

Você não pode armazenar em cache atualizações para a versão 4 e 5 dos produtos usando o ESET Bridge Proxy HTTP. Para distribuir atualizações para esses produtos, use a Ferramenta de imagem.

Quando começar a usar ESET Bridge (HTTP Proxy)

Com base em nossos testes práticos, recomendamos que você implante o ESET Bridge Proxy HTTP se tiver uma rede de 37 computadores ou mais.

É crucial para o armazenamento em cache efetivo que a data e a hora no servidor proxy HTTP estejam configurados corretamente. Diferenças de vários minutos fazem com que o mecanismo de cache não funcione de maneira eficiente e seria feito o download de mais arquivos do que o necessário.

A análise de largura de banda de rede usada unicamente por atualizações em uma rede de teste com 1.000 computadores onde várias instalações e desinstalações ocorreram mostrou o seguinte:

- um único computador faz download de 23,9 MB/mês em atualizações na média, se estiver diretamente conectado à internet (o Proxy HTTP não é usado)
- usando o Proxy HTTP, os downloads para toda a rede totalizaram 900 MB/mês

Uma simples comparação dos dados de atualização baixados em um mês usando a conexão com a internet direta ou o Proxy HTTP em uma rede de computadores:

Número de PCs na sua rede corporativa	25	36	50	100	500	1.000
Conexão direta à internet (MB/mês)	375	900	1.250	2.500	12.500	25.000
ESET Bridge Proxy Apache HTTP (MB/mês)	30	50	60	150	600	900

Quando começar a usar Mirror Tool

Se você tem um ambiente off-line, ou seja, os computadores em sua rede não se conectam à internet por um período prolongado de tempo (meses, um ano) a Ferramenta de imagem (disponível para Windows e Linux) é a única maneira de distribuir atualizações de módulos do produto, pois ele faz download de todas as atualizações de Nível e Nano disponíveis a cada nova solicitação de atualização, se houver uma nova atualização disponível.

Leia este artigo da Base de conhecimento para configurar o encadeamento da Ferramenta de imagem (configurar a Ferramenta de imagem para fazer download de atualizações de outra Ferramenta de imagem).

A maior diferença entre o ESET Bridge Proxy HTTP e a Ferramenta de imagem é que o ESET Bridge Proxy HTTP faz

download apenas das atualizações faltando (por exemplo, atualização Nano 3), enquanto o Mirror Tool faz download de todas as atualizações Nível e Nano (ou apenas atualizações de Nível, se for especificado) disponíveis, independentemente de qual atualização falta ao módulo do produto em particular.

> As atualizações enviadas não estão disponíveis com a Ferramenta de imagem. Recomendamos que você prefira a atualização via ESET Bridge Proxy HTTP para atualizar de um espelho sempre que possível. Mesmo se um computador estiver off-line mas tiver acesso a outra máquina que esteja conectada à Internet e possa executar o ESET Bridge Proxy HTTP para armazenar em cache os arquivos de atualização, selecione esta opção.

Na mesma rede de 1.000 computadores, testamos a Ferramenta de imagem em vez do ESET Bridge Proxy HTTP. A análise mostrou que foram 5.500 MB de atualizações baixados para o mês. O tamanho das atualizações baixadas não aumenta ao adicionar mais computadores na rede. Isto ainda é uma grande diminuição de carga em comparação com uma configuração onde os clientes se conectam diretamente à Internet, mas a melhora no desempenho não é tão substancial como quando o Proxy HTTP é usado.

Número de PCs na sua rede corporativa	25	36	50	100	500	1.000
Conexão direta à internet (MB/mês)	375	900	1.250	2.500	12.500	25.000
Ferramenta de imagem (MB/mês)	5.500	5.500	5.500	5.500	5.500	5.500

> Mesmo que houvesse mais de 1.000 computadores em uma rede, o uso da banda relacionado às atualizações não aumentaria significativamente usando o ESET Bridge Proxy HTTP ou a Ferramenta de imagem.

Requisitos do sistema e dimensionamento

Seu sistema deve cumprir com um conjunto de pré-requisitos de hardware, banco de dados, rede e software para instalar e operar o ESET PROTECT.

Sistemas operacionais compatíveis

As seções a seguir descrevem o suporte do componente ESET PROTECT para versões do sistema operacional Windows, Linux, macOS e móvel.

Windows

A tabela a seguir mostra os sistemas operacionais Windows compatíveis para cada componente do ESET PROTECT:

> ## Controle de versão e suporte do Agente ESET Management
> O Agente ESET Management segue o número da versão local ESET PROTECT e a Política de fim da vida útil:
> - As versões compatíveis com o Agente ESET Management são 9.x–10.x.
> - Cada versão do Agente ESET Management recebe seis meses de Suporte completo e dois anos de Suporte limitado. Em seguida, a versão transita para o Fim da vida útil.
>
> A versão mais recente do Agente ESET Management compatível é a 10.1. Recomendamos usar a versão mais recente do Agente ESET Management para gerenciar totalmente a versão mais recente dos produtos de segurança ESET e seus recursos. Se você usar uma versão anterior do Agente ESET Management que a versão do Servidor ESET PROTECT, alguns dos recursos de gerenciamento mais recentes podem não estar disponíveis.

Sistema operacional	Servidor	Agente	Sensor RD	MDM***
Windows Server 2008 R2 x64 SP1 com KB4474419 e KB4490628 instalados		8.x, 9.x—10.x**	✔	
Windows Server 2008 R2 CORE x64 com KB4474419 e KB4490628 instalados		8.x, 9.x—10.x**	✔	
Windows Storage Server 2008 R2 x64 com KB4474419 e KB4490628 instalados		8.x, 9.x—10.x**	✔	
Microsoft SBS 2011 Standard x64		8.x, 9.x—10.x**	✔	
Microsoft SBS 2011 Essentials x64		8.x, 9.x—10.x**	✔	
Windows Server 2012 x64	✔	8.x, 9.x—10.x	✔	✔
Windows Server 2012 CORE x64	✔	8.x, 9.x—10.x	✔	✔
Windows Server 2012 R2 x64	✔	8.x, 9.x—10.x	✔	✔
Windows Server 2012 R2 CORE x64	✔	8.x, 9.x—10.x	✔	✔
Windows Storage Server 2012 R2 x64	✔	8.x, 9.x—10.x	✔	✔
Windows Server 2016 x64	✔	8.x, 9.x—10.x	✔	✔
Windows Storage Server 2016 x64	✔	8.x, 9.x—10.x	✔	✔
Windows Server 2019 x64	✔	8.x, 9.x—10.x	✔	✔
Windows Server 2022 x64	✔	9.x—10.x	✔	✔

Sistema operacional	Servidor	Agente	Sensor RD	MDM***
Windows 7 x86 SP1 com as atualizações mais recentes do Windows (pelo menos KB4474419 e KB4490628)		8.x, 9.x—10.x**	✔	
Windows 7 x64 SP1 com as atualizações mais recentes do Windows (pelo menos KB4474419 e KB4490628)		8.x, 9.x—10.x**	✔	
Windows 8 x86		8.x, 9.x—10.x**	✔	
Windows 8 x64		8.x, 9.x—10.x**	✔	□*
Windows 8.1 x86		8.x, 9.x—10.x**	✔	
Windows 8.1 x64		8.x, 9.x—10.x**	✔	□*
Windows 10 x86		8.x, 9.x—10.x	✔	
Windows 10 x64 (todos os lançamentos oficiais)	□*	8.x, 9.x—10.x	✔	□*
Windows 10 no ARM		8.x, 9.x—10.x		
Windows 11 x64	□*	8.x, 9.x (21H2) 10.x (21H2 e 22H2) 10.1 (23H2)	✔	□*
Windows 11 no ARM		10.x		

* Instalar componentes ESET PROTECT em um sistema operacional do cliente pode não estar alinhado com a política de licenciamento Microsoft. Verifique a política de licenciamento Microsoft ou consulte seu fornecedor de software para detalhes. Em ambientes SMB / de redes pequenas, encorajamos você a considerar uma instalação ESET PROTECT Linux ou um equipamento virtual onde aplicável.

** O Agente ESET Management 10.x é a versão mais recente compatível com o Windows 7/8.x e Windows Server 2008 R2/Microsoft SBS 2011.

*** O componente do Gerenciamento de dispositivo móvel/Conector ESET PROTECT (MDM/MDC) (apenas no local) teve seu fim da vida útil agendado. Ler mais. Recomendamos que você migre para o gerenciamento de dispositivo móvel em nuvem.

Sistemas Microsoft Windows anteriores:
• Sempre tenha o pacote de serviço mais recente instalado, especialmente em sistemas mais velhos como o Server 2008 e Windows 7.
• O ESET PROTECT não é compatível com o gerenciamento de computadores executando o Windows 7 (sem SP), Widows Vista e Windows XP.
• A partir de 24 de março de 2020, a ESET não vai mais oficialmente fornecer suporte técnico ao ESET PROTECT (Servidor e MDM) instalado nos seguintes sistemas operacionais Microsoft Windows: Windows 7, Windows Server 2008 (todas as versões).
Não temos compatibilidade com sistemas operacionais ilegais ou pirateados.
Você pode executar o ESET PROTECT em um sistema operacional sem servidor sem a necessidade de ESXi. Instalar o VMware Player em um sistema operacional de desktop e implantar o equipamento virtual do ESET PROTECT.

Linux

A tabela a seguir mostra os sistemas operacionais Linux compatíveis para cada componente do ESET PROTECT:

Controle de versão e suporte do Agente ESET Management

O Agente ESET Management segue o número da versão local ESET PROTECT e a Política de fim da vida útil:
• As versões compatíveis com o Agente ESET Management são 9.x–10.x.
• Cada versão do Agente ESET Management recebe seis meses de Suporte completo e dois anos de Suporte limitado. Em seguida, a versão transita para o Fim da vida útil.
A versão mais recente do Agente ESET Management compatível é a 10.1. Recomendamos usar a versão mais recente do Agente ESET Management para gerenciar totalmente a versão mais recente dos produtos de segurança ESET e seus recursos. Se você usar uma versão anterior do Agente ESET Management que a versão do Servidor ESET PROTECT, alguns dos recursos de gerenciamento mais recentes podem não estar disponíveis.

Sistema operacional	Servidor	Agente	Sensor RD	MDM
Ubuntu 16.04.1 LTS x64 Desktop	✔	8.x, 9.x—10.x	✔	***
Ubuntu 16.04.1 LTS x64 Server	✔	8.x, 9.x—10.x	✔	***
Ubuntu 18.04.1 LTS x64 Desktop	✔	8.x, 9.x—10.x	✔	***
Ubuntu 18.04.1 LTS x64 Server	✔	8.x, 9.x—10.x	✔	***
Ubuntu 20.04 LTS x64	✔	8.x, 9.x—10.x	✔	***
Ubuntu 22.04 LTS x64		10.x	✔	
Linux Mint 20		10.x	✔	
Linux Mint 21		10.1	✔	
RHEL Server 7 x64	✔	8.x, 9.x—10.x	✔	***
RHEL Server 8 x64	****	8.x, 9.x—10.x		****
RHEL Server 9 x64		8.x, 9.x—10.x	✔	
CentOS 7 x64	✔	8.x, 9.x—10.x	✔	***

Sistema operacional	Servidor	Agente	Sensor RD	MDM
SLED 15 x64		8.x, 9.x—10.x	✔	
SLES 12 x64		8.x, 9.x—10.x	✔	
SLES 15 x64		8.x, 9.x—10.x	✔	
Debian 9 x64		8.x, 9.x—10.x	✔	
Debian 10 x64	✔	8.x, 9.x—10.x	✔	*
Debian 11 x64		8.x, 9.x—10.x	✔	
Debian 12 x64		10.1	✔	
Oracle Linux 8		9.x—10.x	✔	
Amazon Linux 2		9.x—10.x	✔	
Alma Linux 9		10.1	✔	
Rocky Linux 8		10.1		
Rocky Linux 9		10.1		

* O componente do Gerenciamento de dispositivo móvel/Conector ESET PROTECT (MDM/MDC) (apenas no local) teve seu fim da vida útil agendado. Ler mais. Recomendamos que você migre para o gerenciamento de dispositivo móvel em nuvem.

** O Red Hat Entreprise Linux Server 8.x não é compatível com a geração de relatórios *.pdf* – veja mais detalhes em problemas conhecidos do ESET PROTECT.

macOS

Controle de versão e suporte do Agente ESET Management

O Agente ESET Management segue o número da versão local ESET PROTECT e a Política de fim da vida útil:

- As versões compatíveis com o Agente ESET Management são 9.x–10.x.
- Cada versão do Agente ESET Management recebe seis meses de Suporte completo e dois anos de Suporte limitado. Em seguida, a versão transita para o Fim da vida útil.

A versão mais recente do Agente ESET Management compatível é a 10.1. Recomendamos usar a versão mais recente do Agente ESET Management para gerenciar totalmente a versão mais recente dos produtos de segurança ESET e seus recursos. Se você usar uma versão anterior do Agente ESET Management que a versão do Servidor ESET PROTECT, alguns dos recursos de gerenciamento mais recentes podem não estar disponíveis.

Sistema operacional	Agente
macOS Sierra (10.12)	8.x, 9.x—10.x
macOS High Sierra (10.13)	8.x, 9.x—10.x
macOS Mojave (10.14)	8.x, 9.x—10.x
macOS Catalina (10.15)	8.x, 9.x—10.x
macOS Big Sur (11.0)	8.x, 9.x—10.x
macOS Monterey (12.0)	9.x—10.x
macOS Ventura (13.0)	9.x—10.x
macOS Sonoma (14.0)	10.1

O macOS é compatível somente como cliente. O Agente ESET Management e os produtos ESET para macOS podem ser instalados no macOS. Porém, o Servidor ESET PROTECT não pode ser instalado no macOS.

Móvel

O componente do Gerenciamento de dispositivo móvel/Conector ESET PROTECT (MDM/MDC) (apenas no local) teve seu fim da vida útil agendado. Ler mais. Recomendamos que você migre para o gerenciamento de dispositivo móvel em nuvem.

Sistema operacional	EESA	Proprietário de dispositivo EESA	MDM iOS	MDM iOS ABM
Android 6.x+	✔			
Android 7.x+	✔	✔		
Android 8.x+	✔	✔		
Android 9.0	✔	✔		
Android 10.0	✔	✔		
Android 11	✔	✔		
Android 12	✔	✔		
Android 13	✔	✔		
Android 14	✔	✔		
iOS 9.x+			✔	*
iOS 10.x+			✔	*
iOS 11.x+			✔	*
iOS 12.0.x			✔	*
iOS 13.x+			✔	✔
iOS 14.x+			✔	✔
iOS 15			✔	✔
iOS 16			✔	✔
iOS 17			✔	✔
iPadOS 13.x+			✔	✔
iPadOS 14.x+			✔	✔
iPadOS 15			✔	✔
iPadOS 16			✔	✔
iPadOS 17			✔	✔

* iOS ABM está disponível apenas em países selecionados.

Recomendamos que você atualize o sistema operacional do seu dispositivo móvel na versão mais recente para continuar a receber patches de segurança importantes.

Requisitos para o iOS 10.3 e versões posteriores:

Desde o lançamento do iOS 10.3, uma CA que está instalada como parte do perfil de inscrição pode não ser confiada automaticamente. Para resolver esse problema, siga as etapas abaixo:
a)Use um certificado emitido por um emissor de certificados de confiança da Apple.
b)Instale o certificado de confiança manualmente antes da inscrição. Isso significa que você precisará instalar o CA raiz manualmente no dispositivo móvel antes da inscrição e ativar a confiança total para o certificado instalado.

Requisitos para iOS 12:

Consulte os requisitos para iOS 10.3 e versões posteriores.

- A conexão deve usar **TLS 1.2 ou maior**.
- A conexão deve usar uma **cifra simétrica AES-128** ou **AES-256**. O conjunto da cifra de conexão TLS negociada deve ser compatível com **perfect forward secrecy (PFS)** através de uma **troca de chave de Elliptic Curve Diffie-Hellman Ephemeral (ECDHE)**, e deve ser um dos seguintes:

```
TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384
TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA
TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256
TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA
```

- Assinada com uma **chave RSA** com comprimento de **pelo menos 2048 bits**. O algoritmo de hash do certificado deve ser um **SHA-2 com comprimento de digestão** (por vezes chamado de "impressão digital") de no mínimo 256 (ou seja, **SHA-256 ou maior**). Você pode gerar um certificado que cumpra esses requisitos no ESET PROTECT com a Segurança avançada ativada.
- Os certificados precisam ter **toda a cadeia do certificado inclusive a raiz CA**. A Raiz CA incluída no certificado é usada para estabelecer confiança com os dispositivos e é instalada como parte do perfil de inscrição MDM.

Requisitos para iOS 13:

- Gerenciamento de dispositivos móveis iOS 13 necessário para atender aos novos requisitos do Certificado de comunicação Apple (MDM HTTPS). Certificados emitidos antes de 1º de julho de 2019 também devem cumprir com esses critérios.
- O certificado HTTPS assinado pelo ESMC CA não cumpre com esses requisitos.

> É altamente recomendado não atualizar seus dispositivos para o iOS 13 antes de atender aos requisitos do Certificado de comunicação Apple. Essa ação fará com que seus dispositivos parem de conectar ao ESET PROTECT MDM.

- Se você já atualizou sem o certificado adequado e seus dispositivos pararam de conectar ao ESET PROTECT MDM, é preciso primeiro trocar seu certificado HTTPS atual usado para comunicação com dispositivos iOS para o certificado que atende aos requisitos do Certificado de comunicação Apple (MDM HTTPS) e, depois disso, inscrever seus dispositivos iOS novamente.
- Se você não atualizou para o iOS 13, certifique-se de que seu certificado MDM HTTPS atual usado para comunicação com dispositivos iOS cumpre com os requisitos do Certificado de comunicação Apple (MDM HTTPS). Se sim, você pode continuar a atualizar seus dispositivos iOS para o iOS 13. Se ele não cumprir com os requisitos, altere o certificado MDM HTTPS atual para o certificado HTTPS que cumpre com os requisitos do Certificado de comunicação Apple (MDM HTTPS) e depois atualize seus dispositivos iOS para o iOS 13.

Ambientes de provisionamento de área de trabalho compatíveis

O provisionamento de área de trabalho torna o gerenciamento de dispositivo mais fácil e fornece uma entrega mais rápida de computadores da área de trabalho para os usuários finais.

As áreas de trabalho fornecidas normalmente são físicas ou virtuais. Para ambientes virtualizados que usam um Streamed OS (serviços de provisionamento Citrix), veja a lista de hypervisors compatíveis.

ESET PROTECT é compatível com:

- sistemas com discos não persistentes
- Ambientes VDI
- identificação de computadores clonados

Hypervisors e extensões de hypervisors compatíveis

Hypervisor	ESET PROTECT	ESET Full Disk Encryption
Citrix XenServer	✔	X
Microsoft Hyper-V	✔	✔ (inicialização segura não compatível)
VMware vSphere	✔	✔ (7.0.3.00300)
VMware ESXi	✔	✔ (7.0)
VMware Workstation	✔	✔ (16.2.3)
VMware View	✔	X
Oracle VirtualBox	✔	X
VMwareMware	X	✔ (12.2.3)
Paralelos	X	✔

Extensão do hypervisor	ESET PROTECT	ESET Full Disk Encryption
Citrix VDI-in-a-box	✔	X
Citrix XenDesktop	✔	X

Ferramentas

(aplicável a máquinas virtuais e físicas)

- Microsoft SCCM
- Windows Server 2012/2016/2019/2022 Server Manager
- Windows Admin Center

Dimensionamento de hardware e infraestrutura

A máquina do Servidor ESET PROTECT deve cumprir com as recomendações de hardware definidas a seguir na tabela abaixo.

Número de clientes	ESET PROTECTServidor + servidor de banco de dados SQL				
	Núcleos de CPU	Velocidade do relógio de CPU (GHz)	RAM (GB)	Unidade de disco 1	IOPS2 de disco
Até 1.000	4	2.1	4	Único	500
5.000	8	2.1	8		1.000
10,000 3	4	2.1	16	Separado	2.000
20.000	4	2.1	16		4.000
50.000	8	2.1	32		10.000
100.000	16	2.1	64+		20.000

1 Unidade de disco única/separada – recomendamos instalar o banco de dados em uma unidade separada para sistemas com mais de 10.000 clientes.

2 IOPS (total de operações de E/S por segundo) – valor mínimo necessário.

- Recomendamos ter aproximadamente 0,2 IOPS por cliente conectado, mas no mínimo 500.
- Você pode conferir o IOPS da sua unidade usando a ferramenta diskspd, use o comando a seguir:

Número de clientes	Comando
Até 5.000 clientes	`diskspd.exe -c1000M -b4K -d120 -Sh -r -z -w50 C:\testfile.dat`
Mais de 5.000 clientes	`diskspd.exe -c10000M -b4K -d600 -Sh -r -z -w50 C:\testfile.dat`

3 Veja o exemplo de cenário para o ambiente de 10.000 clientes.

Recomendações de unidade de disco

A unidade de disco é o fator crítico que influencia o desempenho do ESET PROTECT.

- A instância do servidor SQL pode compartilhar recursos com o Servidor ESET PROTECT para aumentar ao máximo o uso e minimizar a latência. Execute o servidor ESET PROTECT e o servidor de banco de dados para aumentar o desempenho do ESET PROTECT.
- O desempenho de um servidor SQL é aprimorado se você colocar o banco de dados e os arquivos de relatório de transação em unidades separadas, de preferência separadas por unidades SSD físicas.
- Se você tiver uma única unidade de disco, recomendamos usar uma unidade SSD.
- Recomendamos que você use a arquitetura all-flash. Unidades de estado sólido (SSD) são muito mais rápidas do que o HDD padrão.
- Se você tem uma configuração RAM alta, a configuração SAS com R5 é suficiente. Configuração testada:

Discos 10x 1,2 TB SAS em R5 - dois grupo de paridade em 4+1 sem armazenamento em cache extra.

• O desempenho não melhora ao usar um nível empresarial SSD com alto IOPS.

• A capacidade de 100 GB é suficiente para qualquer número de clientes. Você pode precisar de uma capacidade maior se fizer backup do banco de dados com frequência.

• Não use uma unidade de rede, pois seu desempenho iria diminuir a velocidade do ESET PROTECT.

• Se você tem uma infraestrutura de armazenamento multicamadas em funcionamento que permite a migração de armazenamento on-line, recomendamos começar com camadas mais lentas compartilhadas e monitorar seu desempenho ESET PROTECT. Se você perceber que a latência de leitura/gravação ultrapassa 20ms, você pode realizar um movimento não perturbador na sua camada de armazenamento para um nível mais rápido para usar o backend mais econômico. Você pode fazer o mesmo em um hypervisor (se você usar o ESET PROTECT como máquina virtual).

Recomendações de dimensionamento para contagens de clientes diferentes

Abaixo você pode encontrar os resultados de desempenho para um ambiente virtual com um número determinado de clientes sendo executados por um ano.

i O banco de dados e o ESET PROTECT estão sendo executados em máquinas virtuais separadas com configurações de hardware idênticas.

Núcleos de CPU	Velocidade do relógio de CPU (GHz)	RAM (GB)	Desempenho		
			10.000 clientes	20.000 clientes	40.000 clientes
8	2.1	64	Alto	Alto	Normal
8	2.1	32	Normal	Normal	Normal
4	2.1	32	Normal	Normal	Baixo
2	2.1	16	Baixo	Baixo	Insuficiente
2	2.1	8	Muito baixa (não recomendado)	Muito baixa (não recomendado)	Insuficiente

Recomendações de implantação

Melhores práticas para a implantação do ESET PROTECT

Número de clientes	Até 1.000	1,000–5,000	5,000–10,000	10,000–50,000	50,000–100,000	100.000+
ESET PROTECT E Servidor do banco de dados na mesma máquina	✔	✔	✔	X	X	X
Uso do Microsoft SQL Express	✔	✔*	X	X	X	X
Uso do Microsoft SQL	✔	✔	✔	✔	✔	✔
Uso do MySQL	✔	✔	✔	X	X	X
Uso do Equipamento virtual ESET PROTECT	✔	✔	Não recomendado	X	X	X
Uso do servidor VM	✔	✔	✔	Opcional	X	X

Número de clientes	Até 1.000	1,000–5,000	5,000–10,000	10,000–50,000	50,000–100,000	100.000+
Intervalo de conexão recomendado (durante a fase de implantação)	60 segundos	5 minutos	10 minutos	15 minutos	20 minutos	25 minutos
Intervalo de conexão recomendado (após a implantação, durante uso normal)	10 minutos	10 minutos	20 minutos	30 minutos	40 minutos	60 minutos

* Para evitar o preenchimento do banco de dados ESET PROTECT, não recomendamos este cenário se você também usa o ESET Inspect.

Intervalo de conexão

O Servidor ESET PROTECT está conectado aos Agentes ESET Management usando conexões permanentes. Apesar da conexão permanente, a transmissão de dados ocorre apenas uma vez durante o intervalo de conexão. Por exemplo, se o intervalo de replicação em 5.000 clientes estiver configurado para oito minutos, haverá 5.000 transmissões em 480 segundos, 10,4 transmissões por segundo. Certifique-se de configurar o intervalo de conexão do cliente adequado. Certifique-se de manter o número total de conexões Agente – Servidor abaixo de 1.000 por segundo mesmo para configurações de hardware de alto desempenho.

Se um servidor estiver sobrecarregado ou se houver uma crise de malware (por exemplo, conectamos 20.000 clientes em um servidor que é capaz de atender apenas a 10.000 clientes em um intervalo de cada 10 minutos), ele ignorará alguns dos clientes conectados. Nenhum cliente conectado vai tentar se conectar ao Servidor ESET PROTECT mais tarde.

Servidor individual (pequenas empresas)

Para gerenciar redes pequenas (1.000 clientes ou menos), uma única máquina com Servidor ESET PROTECT e todos os componentes ESET PROTECT instalados nela. Em ambientes SMB / de redes pequenas, encorajamos você a considerar uma instalação ESET PROTECT Linux ou um equipamento virtual onde aplicável.

Ramificações remotas com proxies

Se as máquinas dos clientes não estiverem vendo diretamente o Servidor ESET PROTECT, use um proxy para encaminhar a comunicação dos produtos ESET. O Proxy HTTP não está agregando a comunicação nem diminuindo o tráfego da replicação.

Alta disponibilidade (empresas)

Para ambientes corporativos (mais de 10.000 clientes), considere o seguinte:

- O RD Sensor ajuda a pesquisar sua rede e descobrir novos computadores.
- Você pode instalar Servidor ESET PROTECT em um Cluster de failover.
- Configure seu Proxy HTTP para um alto número de clientes ou use mais proxies.

Configuração do Web Console para soluções empresariais ou sistemas de baixo desempenho

Por padrão, o Web Console ESET PROTECT instalado por meio do Instalador tudo-em-um para Windows reserva um limite de memória de 1024 MB para o Apache Tomcat.

Você pode alterar a configuração padrão do Web Console com base em sua infraestrutura:

- Em um ambiente empresarial, a configuração padrão do Web Console pode sofrer instabilidade ao trabalhar com um número alto de objetos. Altere as configurações Tomcat para impedi falta de memória. Certifique-se de que o sistema tem RAM suficiente (16 GB ou mais) antes de fazer essas alterações.

- Se você tiver um sistema de desempenho baixo com recursos de hardware limitados, você pode diminuir o uso de memória do Tomcat.

> Os valores de memória fornecidos abaixo são recomendações. Você pode ajustar as configurações de memória do Tomcat com base nos recursos de hardware.

Windows

1. Abra o *tomcat9w.exe* ou execute o aplicativo `Configure Tomcat`.
2. Alternar para a guia **Java**.
3. Alterar o uso de memória:
   a. Aumentar (empresarial): Altere os valores do **Pool de memória inicial** para 2048 MB e o **Pool de memória máximo** para 16384 MB.
   b. Diminuir (sistemas de baixo desempenho): Altere os valores do **Pool de memória inicial** para 256 MB e o **Pool de memória máximo** para 2048 MB.
4. Reinicie o serviço Tomcat.

LINUX e Equipamento Virtual ESET PROTECT

1. Abra o Terminal como root ou use `sudo`.
2. Abra o arquivo
   a. Máquina virtual ESET PROTECT / CentOS: `/etc/sysconfig/tomcat`
   b. Debian: `/etc/default/tomcat9`
3. Adicione a linha a seguir ao arquivo:
   a. Aumentar o uso de memória (empresarial): `JAVA_OPTS="-Xms2048m -Xmx16384m"`
   b. Diminuir o uso de memória (sistemas de baixo desempenho): `JAVA_OPTS="-Xms256m -Xmx2048m"`
4. Salve o arquivo e reinicie o serviço Tomcat.

```
service tomcat restart
```

Implantação para 10.000 clientes

Abaixo você pode encontrar os resultados de desempenho para um ambiente virtual com 10.000 clientes sendo executados por um ano.

Configuração do servidor hypervisor

Componente	Valor
VMware	Atualização do ESXi 6.7 2 e versões posteriores (VM versão 15)
Hypervisor	VMware ESXi, 6.7.0
Processadores lógicos	112
Tipo de processador	Intel(R) Xeon(R) Platinum 8176 CPU @ 2.10GHz

O teste foi executado em máquinas dedicadas
O banco de dados e o ESET PROTECT estão sendo executados em máquinas virtuais separadas com configurações de hardware idênticas.

Software usado em máquinas virtuais

ESET PROTECT:

- Sistema operacional: Microsoft Windows Server 2016 Standard (64-bit)

Banco de dados:

- Servidor do banco de dados: Microsoft SQL Server 2017 (RTM) Standard Edition (64-bit)
- Sistema operacional: Microsoft Windows Server 2016 Standard (64-bit)

Descrição do ambiente ESET PROTECT

- 10.000 clientes conectando
- Aproximadamente 2.000 grupos dinâmicos e 2.000 modelos para grupos dinâmicos
- Aproximadamente 255 grupos estáticos
- 20 usuários
- Intervalo de conexão de 15 minutos para Agentes ESET Management
- Depois que o ambiente estiver sendo executado por um ano, o tamanho do banco de dados é de 15 GB

Contagem de CPU	RAM (GB)	Desempenho
8	64	Alto
4	32	Normal
2	16	Baixo
2	8	Muito baixa (não recomendado)

Banco de dados

Especifique o servidor de banco de dados e o conector que você quer usar ao instalar o Servidor ESET PROTECT. Você pode usar um servidor de banco de dados existente em execução em seu ambiente, mas ele deve atender aos requisitos abaixo.

O instalador único ESET PROTECT 10.1 instala o Microsoft SQL Server Express 2019 por padrão.

- Se você estiver usando uma versão mais antiga do Windows (Server 2012 ou SBS 2011), o Microsoft SQL Server Express 2014 será instalado por padrão.

- O instalador gera automaticamente uma senha aleatória para autenticação de banco de dados (armazenada em *%PROGRAMDATA%\ESET\RemoteAdministrator\Server\EraServerApplicationData\Configuration\startupconfiguration.ini*).

O Microsoft SQL Server Express tem um limite de tamanho de 10 GB de cada banco de dados relacional. Não recomendamos usar o Microsoft SQL Server Express:
- Em ambientes empresariais ou grandes redes.
- Se quiser usar o ESET PROTECT com o ESET Inspect.

Servidores de banco de dados e conector de banco de dados compatíveis

O ESET PROTECT é compatível com dois tipos de servidores de banco de dados: Microsoft SQL Server e MySQL.

O MariaDB não é compatível com o MariaDB. O ESET PROTECT é um banco de dados padrão nos ambientes Linux mais atuais e é instalado quando você escolhe instalar o MySQL.

Servidor de banco de dados compatíveis	Versões de banco de dados compatíveis	Conectores de banco de dados compatíveis
Microsoft SQL Server	• Edições Express e non-Express • 2014, 2016, 2017, 2019, 2022	• Servidor SQL • Servidor SQL Cliente nativo 10.0 • Unidade ODBC para SQL Servidor 11, 13, 17, 18
MySQL	• 5.6* • 5.7 • 8.0 • 8.1	Versões da unidade MySQLODBC: • 5.1, 5.2 • 5.3.0-5.3.10 • 8.0.16, 8.0.17 • 8.0.27, 8.0.31, 8.0.33 Apenas Windows

* O MySQL 5.6 chegou ao fim de vida em fevereiro de 2021. Recomendamos que você atualize seu servidor do banco de dados MySQL para a versão 5.7 e versões posteriores.

As versões da unidade MySQL ODBC a seguir não são compatíveis:
- 5.3.11 e versões posteriores do 5.3. x
- 8.0.0-8.0.15
- 8.0.18 e versões posteriores

Requisitos de hardware de servidor de banco de dados

Veja as instruções de hardware e dimensionamento.

Recomendações de desempenho

Recomendamos usar a versão mais recente compatível do Microsoft SQL Server como seu banco de dados ESET PROTECT para obter o melhor desempenho. Embora o ESET PROTECT seja compatível com MySQL, o uso do MySQL pode afetar negativamente o desempenho do sistema ao trabalhar com grandes quantidades de dados, incluindo painéis, detecções e clientes. O mesmo hardware com Microsoft SQL Server pode lidar com significativamente mais clientes que com o MySQL.

Você pode decidir se vai instalar um servidor de banco de dados SQL:

- Na mesma máquina que o Servidor ESET PROTECT.
- A mesma máquina, mas em um disco separado.
- Em um servidor dedicado para instalação de um servidor de banco de dados SQL.

Recomendamos usar uma máquina dedicada com recursos reservados se quiser gerenciar mais de 10.000 clientes.

Banco de dados	Cliente SMB	Cliente Empresarial	Limite de clientes	Windows	Linux
Microsoft SQL Express	✔	(opcional)	5.000	✔	
Microsoft SQL Server	✔	✔	Nenhuma	✔	
MySQL	✔	✔	10.000	✔	✔

Informações adicionais

ESET PROTECTO Servidor não usa um backup integrado. Recomendamos muito que você faça backup do seu servidor de banco de dados para evitar a perda de dados.

- Não instale o SQL Server em um controlador de domínio (por exemplo, Windows SBS/Essentials). Recomendamos que instale o ESET PROTECT em outro servidor ou não selecione o componente SQL Server Express durante a instalação (isso requer que você use seu Servidor SQL ou MySQL existente para executar o banco de dados ESET PROTECT).
- Se você pretende usar a conta de usuário de banco de dados dedicada que terá acesso apenas ao banco de dados ESET PROTECT, é necessário criar uma conta de usuário com privilégios específicos antes da instalação. Para mais informações, veja Conta do usuário de banco de dados dedicado. Além disso, você vai precisar criar um banco de dados vazio que será usado pelo ESET PROTECT.
- Veja as instruções sobre como instalar e configurar o MySQL para Windows e MySQL para Linux para que funcionem corretamente com o ESET PROTECT.
- O Microsoft SQL Server para Linux não é compatível. Mas você pode conectar o Servidor ESET PROTECT no Linux ao Microsoft SQL Server no Windows.

- Se você instalar o Servidor ESET PROTECT e Servidor Microsoft SQL em computadores separados, você pode ativar uma conexão criptografada ao banco de dados.

- A configuração de cluster do banco de dados em ambientes Windows é compatível apenas com o Microsoft SQL Server, não com o MySQL.

Versões compatíveis do Apache Tomcat e Java

Apache Tomcat

O Apache Tomcat é um componente obrigatório necessário para executar o console web ESET PROTECT.

O ESET PROTECT é compatível apenas com o Apache Tomcat 9.x (64 bits). Recomendamos que você use a versão mais recente do Apache Tomcat 9.x.

O ESET PROTECT não é compatível com versões alpha/beta/RC do Apache Tomcat.

Java

O Apache Tomcat requer 64 bits Java/OpenJDK.

Se você tiver várias versões do Java instaladas em seu sistema, recomendamos desinstalar as versões mais antigas do Java e manter apenas a versão mais recente do Java compatível.

⚠ A partir de janeiro de 2019, atualizações públicas do Oracle JAVA SE 8 para uso de negócios, comercial ou de produção precisarão de uma licença comercial. Se você não comprar uma assinatura JAVA SE, você pode usar este guia para mudar para uma alternativa sem custos. Consulte as versões compatíveis do JDK.

Navegadores da Web, produtos de segurança ESET e idiomas compatíveis

Os sistemas operacionais a seguir são compatíveis com o ESET PROTECT:

- Windows, Linux e macOS

O Console da Web ESET PROTECT pode ser acessado usando os navegadores da web a seguir:

Navegador da Web
Mozilla Firefox
Microsoft Edge
Google Chrome
Safari
Opera

Para uma melhor experiência com o console web ESET PROTECT, recomendamos manter seus navegadores web

atualizados.

Versões mais recentes dos produtos ESET podem ser gerenciadas através do ESET PROTECT 10.1

> As versões do produto de segurança ESET listadas abaixo são gerenciáveis com o Agente ESET Management da versão 10.1 e versões posteriores.
> Recomendamos usar a versão mais recente do Agente ESET Management para gerenciar totalmente a versão mais recente dos produtos de segurança ESET e seus recursos. Se você usar uma versão anterior do Agente ESET Management que a versão do Servidor ESET PROTECT, alguns dos recursos de gerenciamento mais recentes podem não estar disponíveis.

Produto	Versão do produto
ESET Endpoint Security para Windows	7.3, 8.x, 9.x, 10.x
ESET Endpoint Antivirus para Windows	7.3, 8.x, 9.x, 10.x
ESET Endpoint Security para macOS	6.10+
ESET Endpoint Antivirus para macOS	6.10+
ESET Endpoint Security para Android	2.x, 3.x, 4.x
ESET Server Security para Microsoft Windows Server (anteriormente ESET File Security para Microsoft Windows Server)	7.3, 8.x, 9.x, 10.x
ESET Mail Security para Microsoft Exchange Server	7.3, 8.x, 9.x, 10.x
ESET Security para Microsoft SharePoint Server	7.3, 8.x, 9.x, 10.x
ESET Mail Security para IBM Domino	7.3, 8.x, 9.x, 10.x
ESET Server Security para Linux (anteriormente ESET File Security para Linux)	7.2, 8.x, 9.x, 10.x
ESET Endpoint Antivirus para Linux	7.1, 8.x, 9.x, 10.x
ESET LiveGuard Advanced	
ESET Inspect Connector	1.6+
ESET Full Disk Encryption para Windows	
ESET Full Disk Encryption para macOS	

Versões mais recentes dos produtos ESET podem ser gerenciadas através do ESET PROTECT 10.1

Produto	Versão do produto
ESET Endpoint Security para Windows	6.5
ESET Endpoint Antivirus para Windows	6.5
ESET File Security para Microsoft Windows Server	6.5
ESET Mail Security para Microsoft Exchange Server	6.5
ESET Mail Security para IBM Domino	6.5
ESET Security para Microsoft SharePoint Server	6.5

Versões dos produtos de segurança ESET anteriores àquelas exibidas na tabela acima não podem ser gerenciadas usando o ESET PROTECT10.1.
Para mais informações sobre a compatibilidade, visite a política de fim de vida para os produtos empresariais ESET.

Produtos compatíveis com a ativação através da licença de Assinatura

Produto ESET	Disponível desde a versão
ESET Endpoint Antivírus/Security para Windows	7.0
ESET Endpoint Antivírus/Security para macOS	6.8.x
ESET Endpoint Security para Android	2.0.158
ESET Mobile Device Management para Apple iOS	7.0
ESET File Security para Microsoft Windows Server	7.0
ESET Mail Security para Microsoft Exchange	7.0
ESET File Security para Windows Server	7.0
ESET Mail Security para IBM Domino	7.0
ESET Security para Microsoft SharePoint Server	7.0
ESET File Security para Linux	7.0
ESET Endpoint Antivirus para Linux	7.0
ESET Server Security para Windows	8.0
ESET Server Security para Linux	8.1
ESET LiveGuard Advanced	
ESET Inspect (com ESET Endpoint para Windows 7.3 e versões posteriores)	1.5

Idiomas compatíveis

Idioma	Código
Inglês (Estados Unidos)	en-US
Árabe (Egito)	ar-EG
Chinês simplificado	zh-CN
Chinês tradicional	zh-TW
Croata (Croácia)	hr-HR
Tcheco (República Tcheca)	cs-CZ
Francês (França)	fr-FR
Francês (Canadá)	fr-CA
Alemão (Alemanha)	de-DE
Grego (Grécia)	el-GR
Húngaro (Hungria)*	hu-HU
Indonésio (Indonésia)*	id-ID
Italiano (Itália)	it-IT
Japonês (Japão)	ja-JP

Idioma	Código
Coreano (Coréia)	ko-KR
Polonês (Polônia)	pl-PL
Português (Brasil)	pt-BR
Russo (Rússia)	ru-RU
Espanhol (Chile)	es-CL
Espanhol (Espanha)	es-ES
Eslovaco (Eslováquia)	sk-SK
Turco (Turquia)	tr-TR
Ucraniano (Ucrânia)	uk-UA

* Apenas o produto está disponível neste idioma, a Ajuda on-line não está disponível.

Rede

É essencial que tanto o Servidor ESET PROTECT quanto os computadores do cliente gerenciados pelo ESET PROTECT tenham uma conexão à Internet que funcione, para que possam acessar os servidores de repositório e de ativação da ESET. Se você prefere que os clientes não se conectem diretamente à Internet, você pode usar um servidor proxy (não o mesmo que o ESET Bridge Proxy HTTP) para facilitar a comunicação com a rede e a Internet.

O Servidor ESET PROTECT deve ser visível para computadores do cliente – computadores do cliente devem ser capazes de comunicar com seu Servidor ESET PROTECT para usar a implantação remota e o recurso de Chamada de despertar.

O ESET PROTECT para Windows/Linux é compatível com os protocolos de Internet IPv4 e IPv6. A Máquina virtual ESET PROTECT é compatível apenas com IPv4.

Portas usadas

Se sua rede usar um firewall, veja nossa lista de portas de comunicação de rede possíveis usadas quando o ESET PROTECT e seus componentes estiverem instalados na sua infraestrutura.

Impacto do tráfego de rede pelo Servidor ESET PROTECT e comunicação do Agente ESET Management

Aplicativos em máquinas do cliente não se comunicam diretamente com o Servidor ESET PROTECT, o Agente ESET Management facilita essa comunicação. Essa solução é mais fácil de gerenciar e cria menos demandas sobre os dados transferidos pela rede. O tráfego de rede depende do intervalo de conexão do cliente e dos tipos de tarefas realizadas pelos clientes. Mesmo se nenhuma tarefa for executada ou agendada em um cliente, o Agente ESET Management comunica-se com o Servidor ESET PROTECT uma vez a cada intervalo de conexão. Cada conexão gera tráfego. Consulte a tabela abaixo para exemplos de tráfego:

Tipo de ação	Tráfego em um único intervalo de conexão
Tarefa do cliente: Rastrear sem limpar	4 kB
Tarefa do cliente: Atualização de módulos	4 kB

Tipo de ação	Tráfego em um único intervalo de conexão
Tarefa do cliente: Solicitação de relatório do SysInspector	300 kB
Política Antivírus - Segurança máxima	26 kB

ESET ManagementIntervalo de replicação do Agente	Tráfego diário gerado pelo Agente ESET Management ocioso
1 minuto	16 MB
15 minutos	1 MB
30 minutos	0,5 MB
1 hora	144 kB
1 dia	12 kB

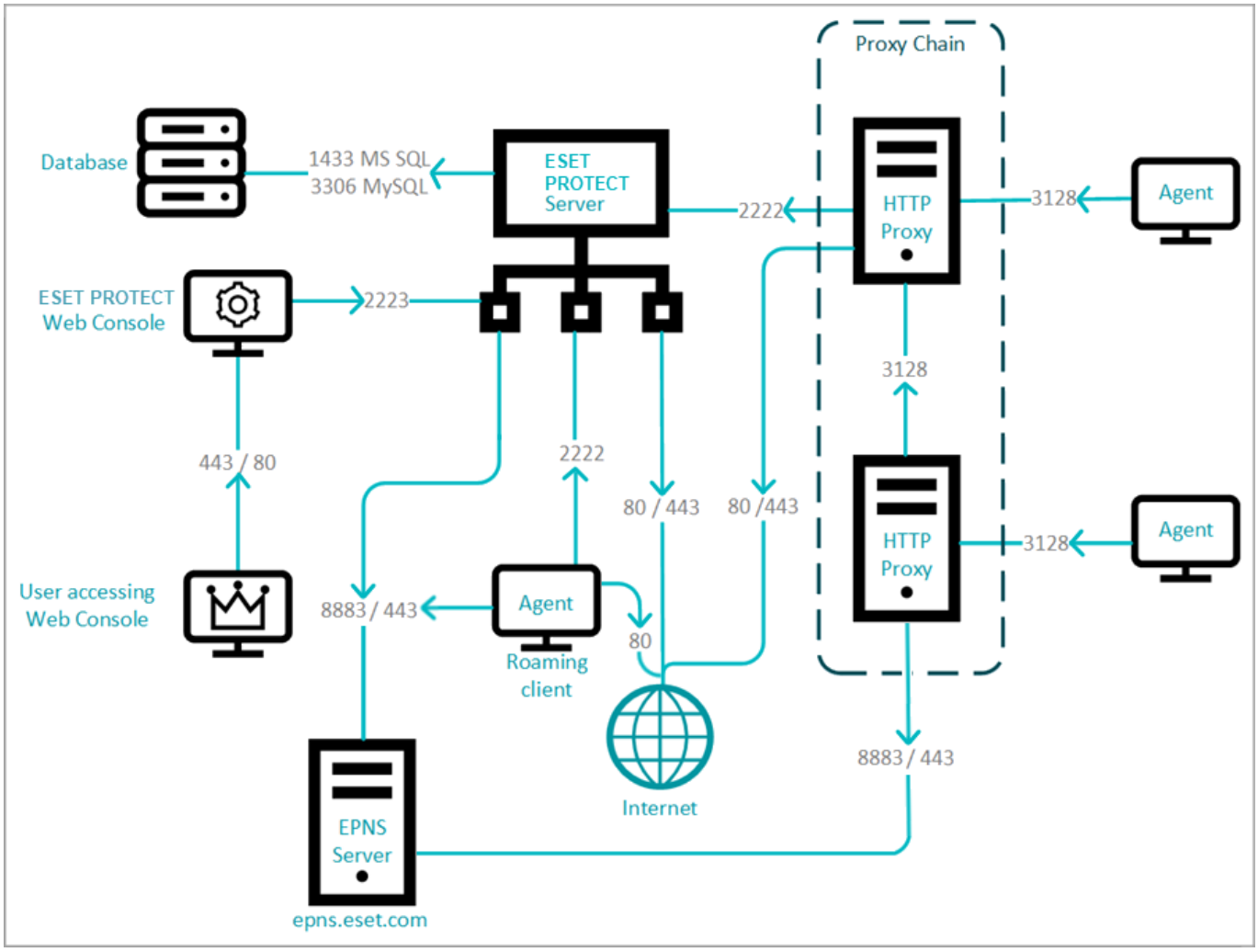
Para estimar o tráfego geral gerado por Agentes ESET Management, use a fórmula a seguir:

*Número de clientes * (Tráfego diário do agente ocioso + (Tráfego para uma determinada tarefa * ocorrência diária da tarefa))*

Se você usar o ESET Inspect, o Connector ESET Inspect gera tráfego diário de 2 a 5 MB (varia de acordo com o número de eventos).

Portas usadas

O Servidor ESET PROTECT pode ser instalado no mesmo computador que o banco de dados, o Console web ESET PROTECT e o Proxy HTTP. O diagrama abaixo mostra a instalação separada e as portas usadas (as setas indicam o tráfego da rede):



As tabelas a seguir relacionam todas as portas de comunicação de rede possíveis usadas quando o ESET PROTECT e seus componentes estiverem instalados na sua infraestrutura. Outros tipos de comunicação ocorrem por meio dos processos nativos de sistema operacional (por exemplo, NetBIOS por meio de TCP/IP).

Para o funcionamento adequado do ESET PROTECT, outros aplicativos não devem usar nenhuma das portas abaixo.
Certifique-se de configurar qualquer firewall dentro de sua rede para permitir a comunicação através das portas listadas acima.

Cliente (Agente ESET Management) ou máquina do ESET Bridge Proxy HTTP

Protocolo	Porta	Descrições
TCP	2222	Comunicação entre os Agentes ESET Management e o Servidor ESET PROTECT
TCP	80	Conexão ao repositório da ESET
MQTT	8883, 443	Serviço de notificação por push da ESET - Chamadas para despertar entre o Servidor ESET PROTECT e o Agente ESET Management, a porta de failover é a 443.
TCP	3128	Comunicação com o ESET Bridge (Proxy HTTP)
TCP	443	Comunicação com o ESET LiveGuard Advanced (somente proxy)

Agente ESET Management - portas usadas para instalação remota em um computador de destino com sistema operacional Windows

Protocolo	Porta	Descrições
TCP	139	Usando o compartilhamento ADMIN$
TCP	445	Acesso direto a recursos compartilhados usando TCP/IP durante a instalação remota (uma alternativa para TCP 139)
UDP	137	Resolução de nome durante a instalação remota
UDP	138	Procurar durante a instalação remota

Máquina do console web ESET PROTECT (se não for a mesma que a máquina do Servidor ESET PROTECT)

Protocolo	Porta	Descrições
TCP	2223	Comunicação entre o Console da Web ESET PROTECT e o Servidor ESET PROTECT, usada para instalação Assistida
TCP	443/80	Tomcat transmitindo o console Web.
TCP	443	Feed RSS para Notícias de Suporte: • https://era.welivesecurity.com:443 • https://support.eset.com:443/rss/news.xml

Máquina do servidor ESET PROTECT

Protocolo	Porta	Descrições
TCP	2222	Comunicação entre o Agente ESET Management e o Servidor ESET PROTECT
TCP	80	Conexão ao repositório da ESET
MQTT	8883	Serviço de notificação por push da ESET - Chamadas para despertar entre o Servidor ESET PROTECT e o Agente ESET Management
TCP	2223	Resolução de DNS e fallback MQTT
TCP	3128	Comunicação com o ESET Bridge (Proxy HTTP)
TCP	1433 (Microsoft SQL) 3306 (MySQL)	Conexão para um banco de dados externo (apenas se o banco de dados estiver em outra máquina).
TCP	389	Sincronização LDAP. Abra essa porta também no seu controlador AD.
UDP	88	Tíquetes Kerberos (aplicável apenas à Máquina virtual ESET PROTECT)

Sensor Rogue Detection (RD)

Protocolo	Porta	Descrições
TCP	22, 139	Detecção do sistema operacional via protocolos SMB (TCP 139) e SSH (TCP 22).
UDP	137	Resolução do nome de host do computador via NetBIOS.

Máquina MDC ESET PROTECT

Protocolo	Porta	Descrições
TCP	9977 9978	Comunicação **interna** entre o Conector de dispositivo móvel e Agente ESET Management
TCP	9980	Inscrição de dispositivo móvel
TCP	9981	Comunicação de dispositivos móveis
TCP	2195	Enviar notificações para o serviço de notificação por push da Apple. (*gateway.push.apple.com*) até o ESMC versão 7.2.11.1
TCP	2196	Serviço de feedback da Apple (*feedback.push.apple.com*) até o ESMC versão 7.2.11.1
HTTPS	2197	• Notificação por push da Apple e feedback (*api.push.apple.com*) ESMC versão 7.2.11.3 e versões posteriores.
TCP	2222	Comunicação (replicação) entre o Agente ESET Management, MDC e o Servidor ESET PROTECT
TCP	1433 (Microsoft SQL) 3306 (MySQL)	Conexão para um banco de dados externo (apenas se o banco de dados estiver em outra máquina)

Dispositivo gerenciado por MDM

Protocolo	Porta	Descrições
TCP	9980	Inscrição de dispositivo móvel
TCP	9981	Comunicação de dispositivos móveis
TCP	5223	Comunicação externa com o serviço de notificação por push da Apple (iOS)
TCP	443	• Fallback apenas no Wi-Fi, quando dispositivos não conseguem acessar APNS na porta 5223. (iOS) • Conexão de dispositivo Android ao servidor GCM. • Conexão com o portal de licenciamento ESET. • ESET LiveGrid® (Android) (Entrada: *https://l1.c.eset.com*; Saída: *https://l3.c.eset.com*) • Informações estatísticas anônimas para o Laboratório de pesquisas ESET (Android) (*https://ts.eset.com*) • Categorização de aplicativos instalada no dispositivo. Usado para o Controle de aplicações quando o bloqueio de algumas características do aplicativo foi definido. (Android) (*https://play.eset.com*) • Para enviar uma solicitação de suporte usando a função de Solicitação de suporte (Android) (*https://suppreq.eset.eu*)
TCP	5228 5229 5230	Enviando notificações ao Google Cloud Messaging (Android)* Enviando notificações ao Firebase Cloud Messaging (Android)*
TCP	80	• Atualização de módulos (Android) (*http://update.eset.com*) • Usado apenas na versão Web. Informações sobre a versão mais recente do aplicativo, atualização e download de uma nova versão. (Android) (*http://go.eset.eu*)

* O serviço GCM (Google Cloud Messaging) foi descontinuado e removido em 11 de abril de 2019. Ele foi substituído pelo FCM (Firebase Cloud Messaging). O MDM v7 substituiu o serviço GCM pelo serviço FCM até essa data, e então você precisará permitir apenas a comunicação para o serviço FCM.

As portas predefinidas 2222 e 2223 podem ser alteradas se necessário.

Processo de instalação

O guia de instalação contém muitas maneiras de instalar o ESET PROTECT e foi feito principalmente para clientes empresariais. Consulte o guia para pequenas e médias empresas se quiser instalar o ESET PROTECT em uma plataforma Windows para gerenciar até 250 produtos de endpoint ESET no Windows.
Para obter instruções para atualizar sua instalação ESET PROTECT existente, vá para Procedimentos de atualização.

Instaladores ESET PROTECT estão disponíveis na seção Download ESET PROTECT do site da ESET. Diferentes formatos estão disponíveis compatíveis com métodos de instalação diferentes. Por padrão, a guia **Instalador Tudo-em-um** é selecionada. Clique na guia adequada para fazer download de um VA ou instalador autônomo. Os seguintes downloads estão disponíveis:

- O pacote do ESET PROTECTInstalador Tudo-em-um para Windows em formato zip.
- Uma imagem ISO que contém todos os instaladores do ESET PROTECT (exceto o Equipamento Virtual ESET PROTECT)
- Equipamentos virtuais (arquivos OVA). A implantação de um Aplicativo Virtual ESET PROTECT é recomendada para usuários que queiram executar o ESET PROTECT em um ambiente virtualizado ou que preferem uma instalação sem problemas. Veja nosso ESET PROTECTguia de implantação de Aplicativo Virtual completo para obter instruções passo-a-passo.
- Instaladores separados para cada componente para plataformas Windows e Linux.

Métodos de instalação adicionais:

- Instruções de instalação passo a passo para Linux

A partir de novembro de 2022, não fornecemos o Appliance ESET PROTECT no Azure Marketplace. Alternativamente, você pode usar o ESET PROTECT Cloud e permitir que a ESET gerencie todos os componentes de infraestrutura necessários.

Não altere o nome do Computador da sua máquina do Servidor ESET PROTECT depois da instalação. Veja Alteração do endereço IP ou nome de host no Servidor ESET PROTECT para mais informações.

Se você quiser decidir qual tipo de instalação ESET PROTECT é adequada para seu ambiente, consulte a tabela de decisão a seguir, ela irá guiá-lo para a melhor escolha: Por exemplo:

- Não use uma conexão à Internet lenta para o ESET PROTECT na nuvem.
- Escolha o instalador tudo-em-um se você for um cliente SMB.

Confira também Dimensionamento de hardware e infraestrutura. Você pode instalar o ESET PROTECT em máquinas virtuais ou físicas.

Método de instalação	Tipo de cliente		Migração		Ambiente para instalação ESET PROTECT					Conexão com a Internet		
	SMB	Empresa	Sim	Não	Nenhum servidor	Servidor dedicado	Servidor compartilhado	Plataforma de virtualização	Servidor de nuvem	Nenhuma	Bom	Ruim
Tudo-em-um em Windows Server	✓	✓	✓			✓	✓		✓	✓	✓	✓
Tudo-em-um em Windows Desktop	✓		✓		✓					✓	✓	✓
Equipamento virtual	✓		✓					✓		✓	✓	✓
Componente Linux		✓	✓			✓	✓		✓	✓	✓	✓
Componente Windows		✓	✓			✓	✓		✓	✓	✓	✓

Instalação tudo-em-um no Windows

Você pode instalar o ESET PROTECT de algumas formas diferentes. Selecione o tipo de instalação que mais bem se adapta às suas necessidades e ambiente. O método mais simples é usar o instalador Tudo-em-um do ESET PROTECT. Este método permite que você instale o ESET PROTECT e seus componentes em uma máquina individual.

A instalação de componente permite que você personalize a instalação e instale cada componente ESET PROTECT em um computador separado, desde que atenda aos requisitos do sistema.

Você pode instalar o ESET PROTECT usando:

- Instalação do pacote Tudo-em-um do Servidor ESET PROTECT, ESET Bridge Proxy HTTP ou Conector de dispositivo móvel
- Instaladores autônomos para componentes ESET PROTECT (instalação do componente)

Cenários de instalação personalizada incluem:

- Instalação com os Certificados personalizados
- Instalação em um agrupamento de failover

A maioria dos cenários de instalação requer que você instale vários componentes do ESET PROTECT em diferentes máquinas para acomodar diversas arquiteturas de rede, atender aos requisitos de desempenho ou por outros motivos. Os pacotes de instalação a seguir estão disponíveis para componentes individuais ESET PROTECT:

Instalação de principais componentes:

- Servidor ESET PROTECT
- Console da Web ESET PROTECT – Você pode escolher instalar o Web Console ESET PROTECT em um computador diferente do computador executando o Servidor ESET PROTECT.
- Agente ESET Management (precisa estar instalado nos computadores do cliente, opcional no Servidor ESET PROTECT)

Instalação de componentes opcionais:

- Sensor RD
- Conector de dispositivo móvel

- ESET Bridge Proxy HTTP
- Ferramenta de imagem

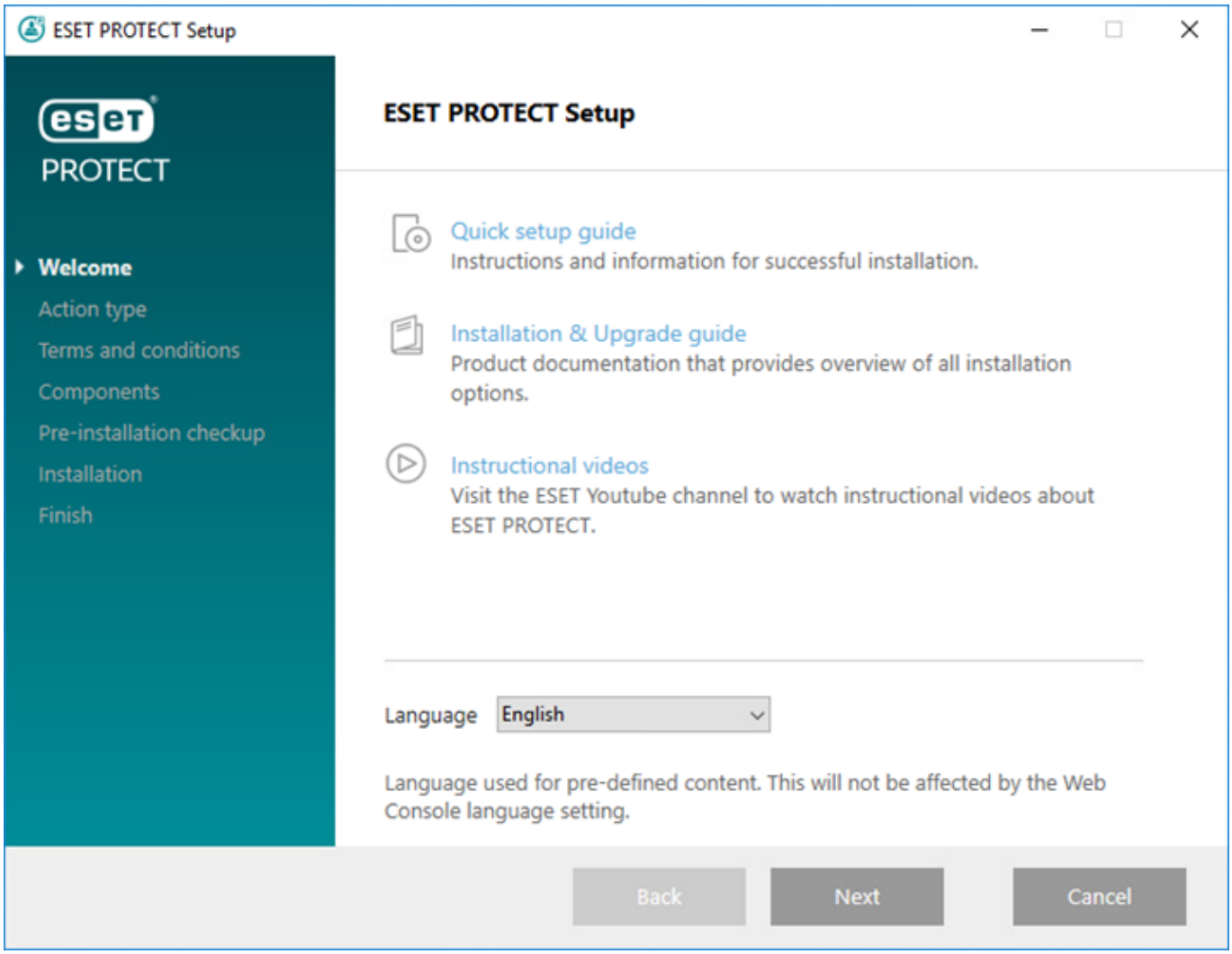
Veja também instalação Tudo-em-um ESET PROTECT.

Para instruções sobre como atualizar o ESMC para o ESET PROTECT 10.1 mais recente, consulte nossos procedimentos de atualização.

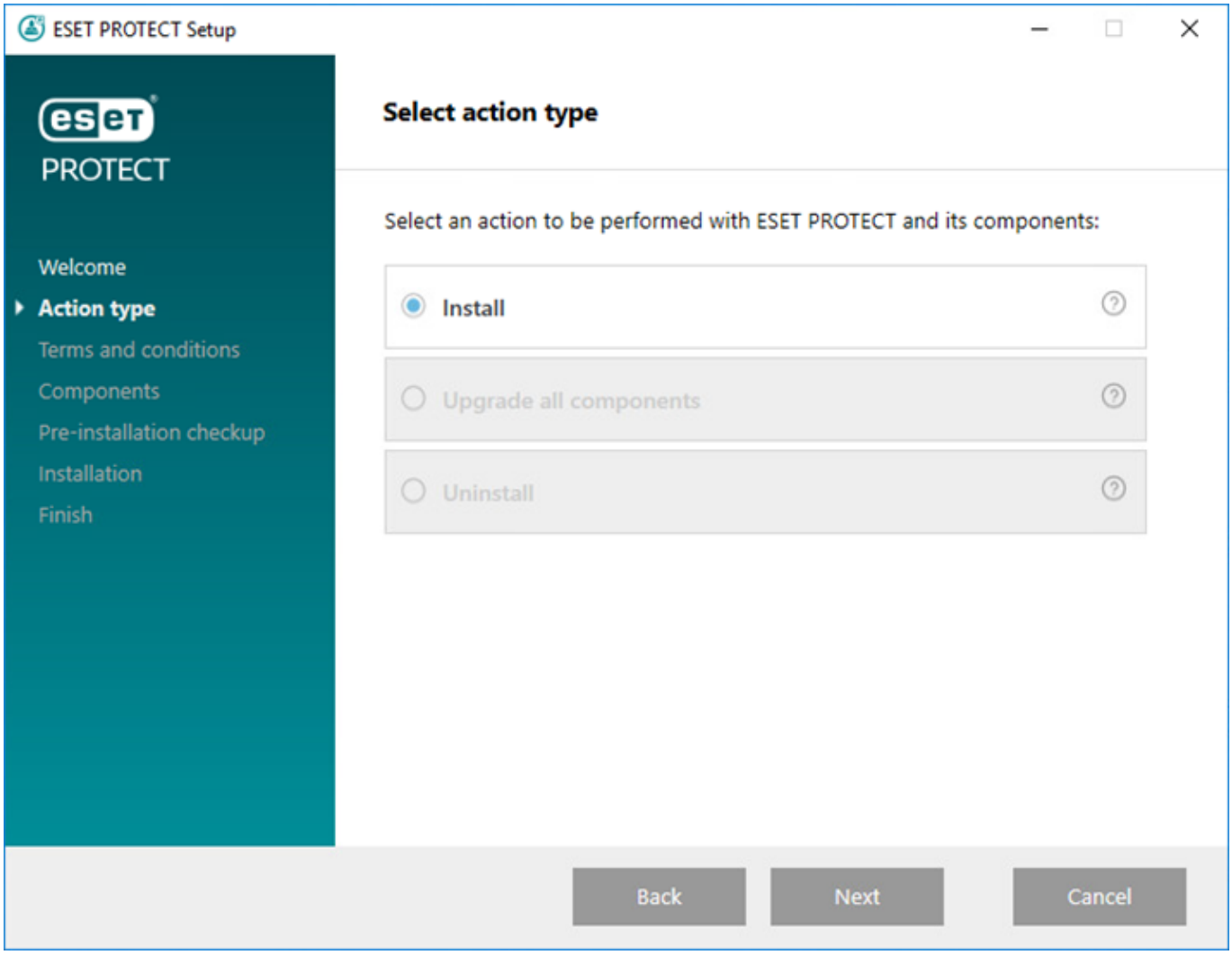
Instalar o Servidor ESET PROTECT

O instalador Tudo-em-um ESET PROTECT está disponível somente para sistemas operacionais Windows. O Instalador tudo-em-um permite que você instale todos os componentes do ESET PROTECT usando o Assistente de instalação ESET PROTECT.

1. Abra o pacote de instalação. Na tela Bem-vindo, use o menu suspenso **Idioma** para ajustar as configurações de idioma. Clique em **Avançar** para continuar.



2. Selecione **Instalar** e clique em **Avançar**.



3. Marque a caixa de seleção ao lado de **Participar do programa de melhoria do produto** para enviar relatórios de travamento e dados de telemetria anônimos para a ESET (versão e tipo do sistema operacional, versão do produto ESET e outras informações específicas do produto). Depois de aceitar o EULA, clique em **Avançar**.

4. Selecione os componentes a instalar e clique em **Avançar**.

Microsoft SQL Server Express

- O instalador único ESET PROTECT 10.1 instala o Microsoft SQL Server Express 2019 por padrão.

oSe você estiver usando uma versão mais antiga do Windows (Server 2012 ou SBS 2011), o Microsoft SQL Server Express 2014 será instalado por padrão.

oO instalador gera automaticamente uma senha aleatória para autenticação de banco de dados (armazenada em *%PROGRAMDATA%\ESET\RemoteAdministrator\Server\EraServerApplicationData\Configuration\startupconfiguration.ini*).

> O Microsoft SQL Server Express tem um limite de tamanho de 10 GB de cada banco de dados relacional. Não recomendamos usar o Microsoft SQL Server Express:
> - Em ambientes empresariais ou grandes redes.
> - Se quiser usar o ESET PROTECT com o ESET Inspect.

- Se você já tem outra versão compatível do Microsoft SQL Server ou MySQL instalada, ou se planeja conectar a um SQL Server diferente, desmarque a caixa de seleção ao lado de **Microsoft SQL Server Express**.
- Não instale o SQL Server em um controlador de domínio (por exemplo, Windows SBS/Essentials). Recomendamos que instale o ESET PROTECT em outro servidor ou não selecione o componente SQL Server Express durante a instalação (isso requer que você use seu Servidor SQL ou MySQL existente para executar o banco de dados ESET PROTECT).

Adicionar certificado HTTPS personalizado para o console web

- Selecione esta opção se quiser usar um certificado HTTPS personalizado para o console web ESET PROTECT.
- Se você não selecionar essa opção, o instalador gera automaticamente um novo keystore para o Tomcat (um certificado auto-assinado HTTPS).

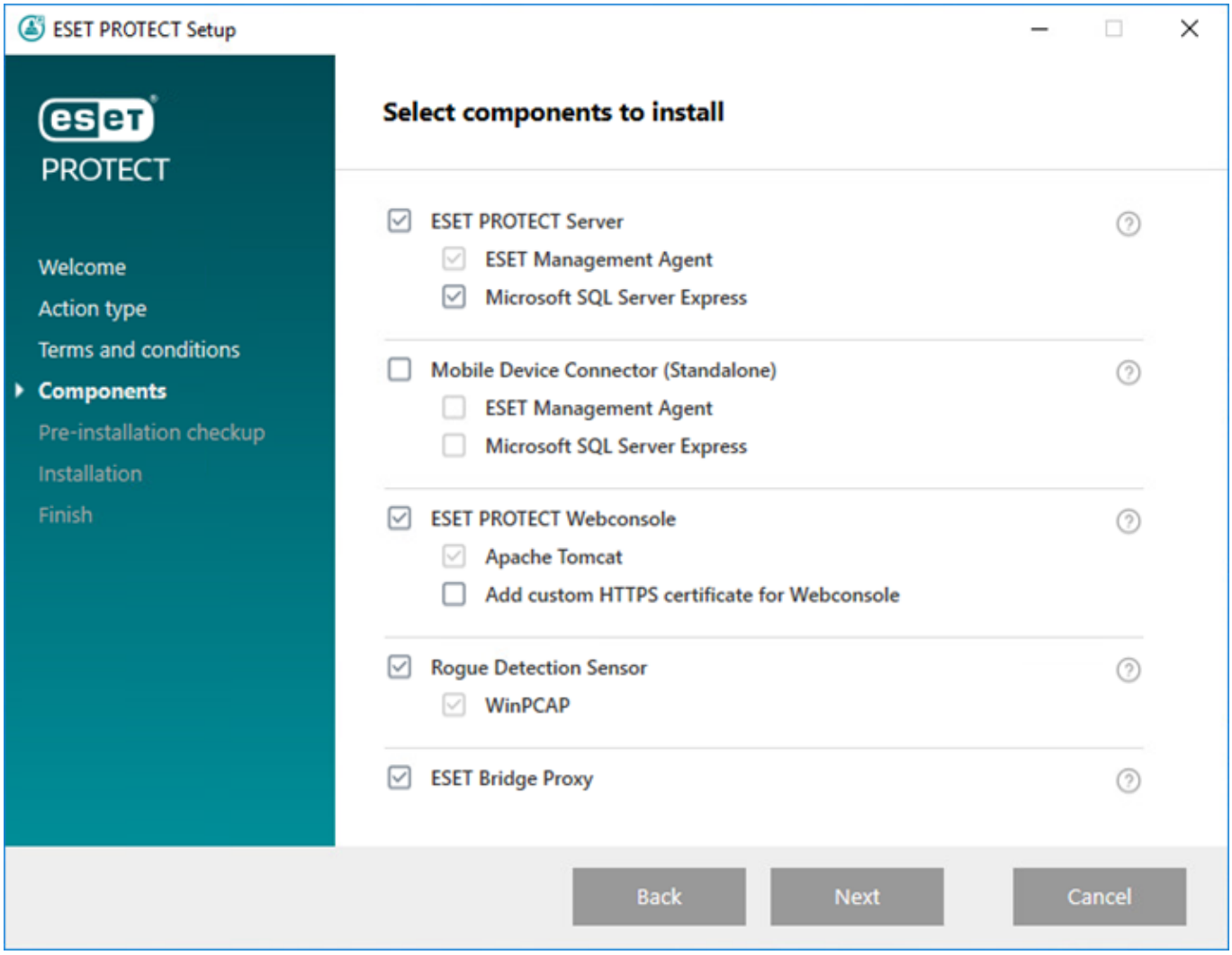
ESET Bridge Proxy

> A opção **ESET Bridge Proxy** é projetada apenas para redes pequenas ou centralizadas, sem clientes em roaming. Se você selecionar essa opção, o instalador configura os clientes para a comunicação por túnel com a ESET através de um proxy instalado na mesma máquina que o Servidor ESET PROTECT. Essa conexão não vai funcionar se não houver visibilidade de rede direta entre os clientes e o Servidor ESET PROTECT.

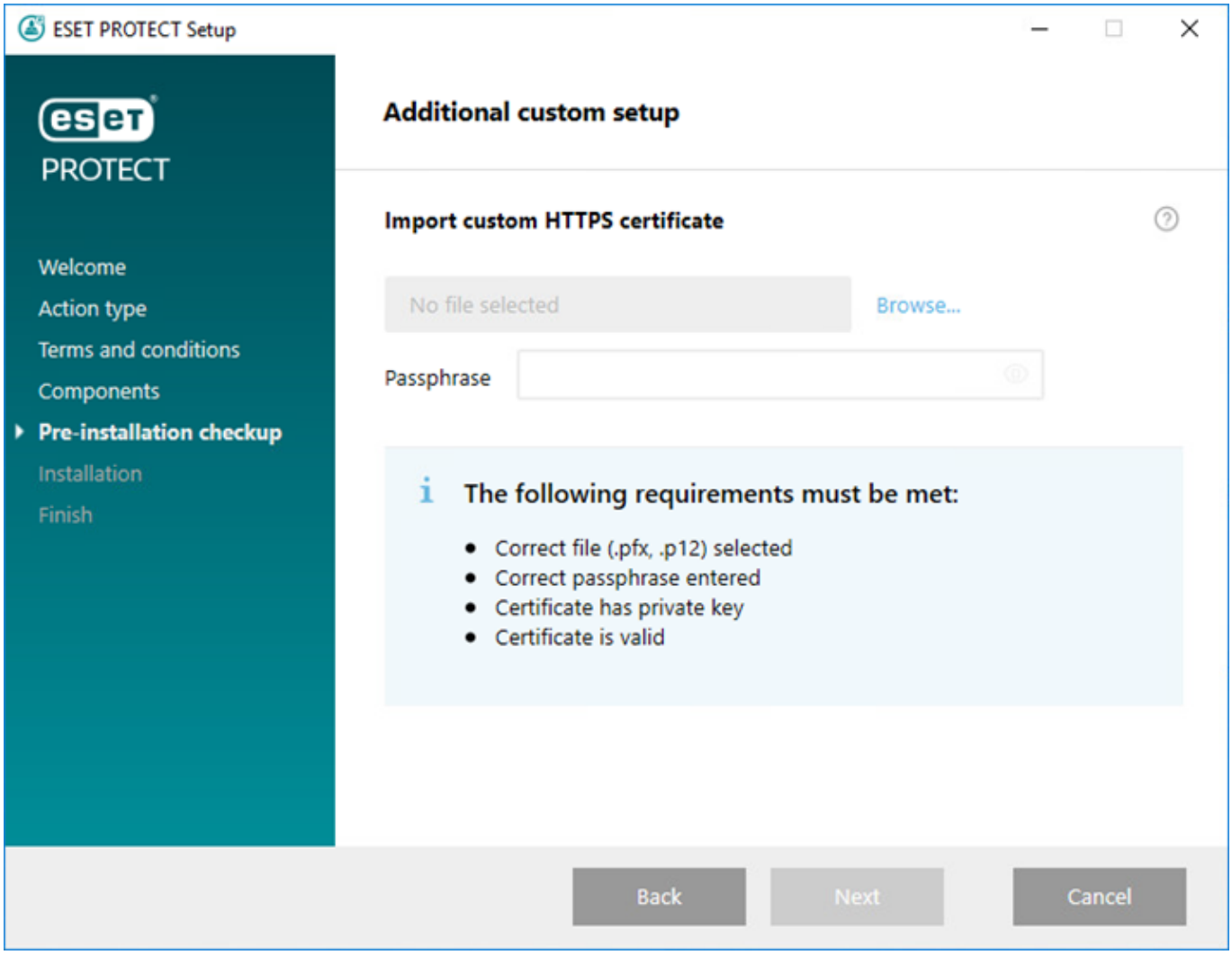
- Usar o Proxy HTTP pode economizar bastante largura de banda em dados baixados da Internet e melhorar as velocidades de download para atualizações de produto. Recomendamos marcar a caixa de seleção ao lado do **ESET BridgeProxy** se for gerenciar mais de 37 computadores do ESET PROTECT. Você também pode escolher instalar o ESET Bridge mais tarde.
- Para mais informações, veja ESET Bridge (Proxy HTTP) e Diferenças entre o ESET Bridge (Proxy HTTP), Ferramenta de imagem e conectividade direta.

> O instalador tudo-em-um cria políticas de **HTTP Proxy Uso** padrão para o Agente ESET Management e para produtos de segurança ESET aplicados ao grupo estático **Todos**. As políticas configuram Agentes ESET Management e produtos de segurança ESET automaticamente em computadores gerenciados para usar o ESET Bridge como Proxy para armazenamento em cache de pacotes de atualização. O cache de tráfego HTTPS está habilitado por padrão:
> - A política ESET Bridge contém o certificado HTTPS e a alternância **Tráfego de cache HTTPS** está habilitada.
> - A política de uso **HTTP Proxy** do ESET Endpoint para Windows contém a Autoridade de Certificação para o cache de tráfego HTTPS.

O host de proxy HTTP é o endereço IP local do Servidor ESET PROTECT e a porta 3128. A autenticação está desativada. Você pode copiar essas configurações para outras políticas, se precisar configurar outros produtos.



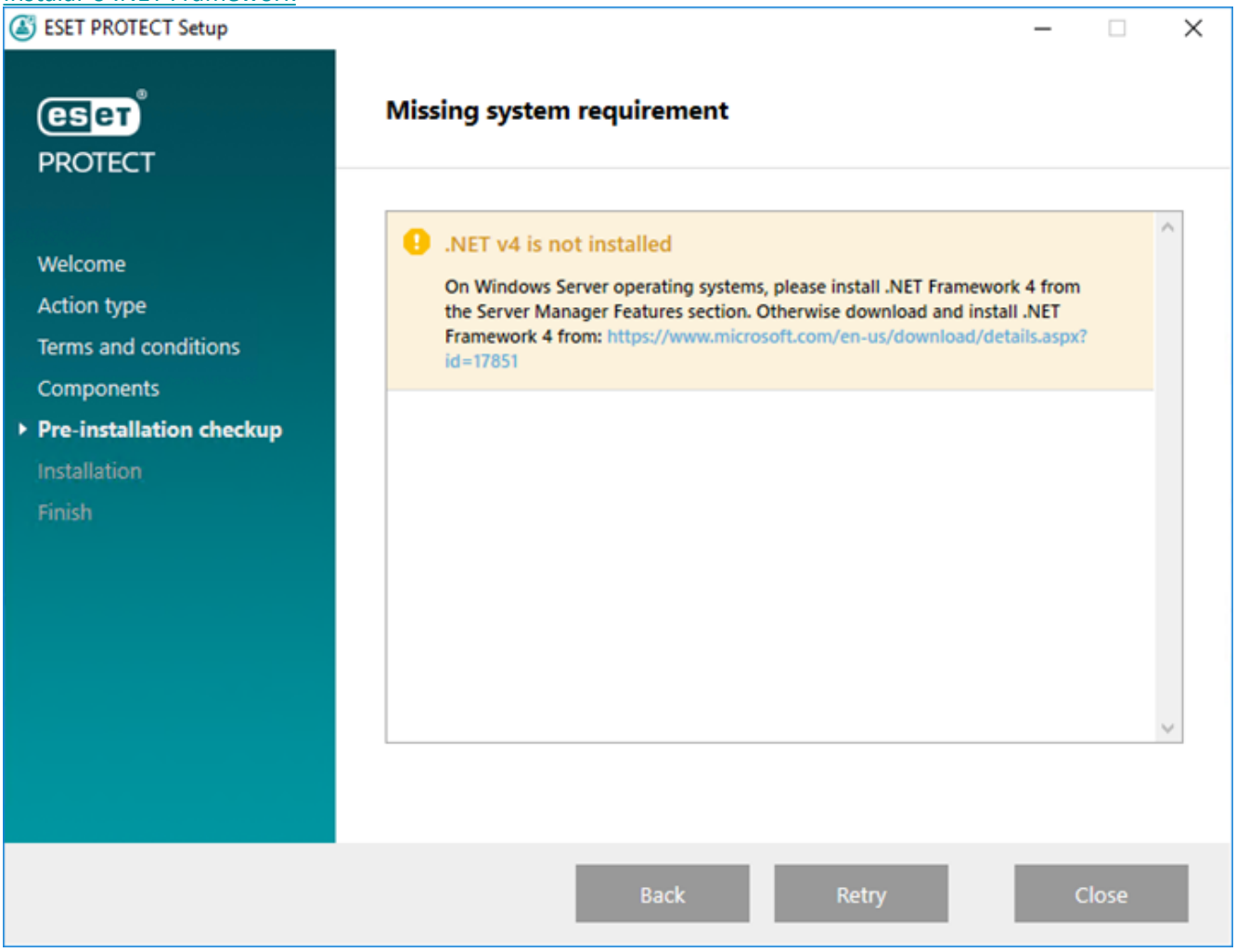
5. Se você selecionou **Adicionar certificado HTTPS personalizado para o console web**, clique em **Procurar** e selecione um Certificado válido (*.pfx* ou arquivo .p12) e digite sua **Senha** (ou deixe o campo em branco, se não houver senha). O instalador vai instalar o certificado de acesso ao Web Console no seu servidor Tomcat. Clique em **Avançar** para continuar.



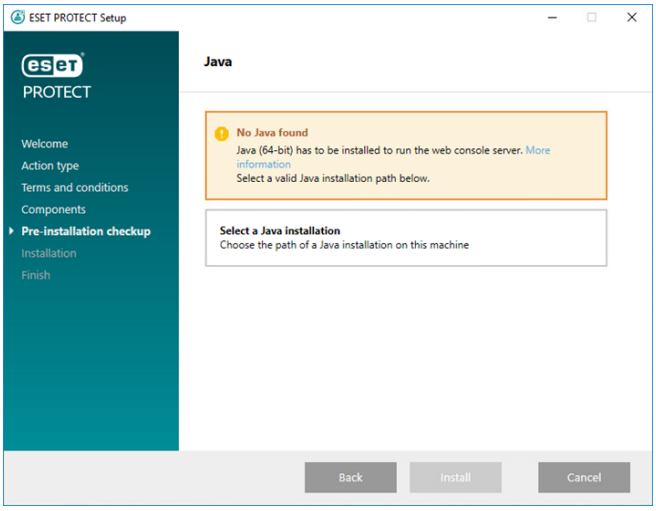
6. Se forem encontrados erros durante a verificação de pré-requisitos, resolva-os devidamente. Certifique-se de que seu sistema atenda a todos os pré-requisitos.

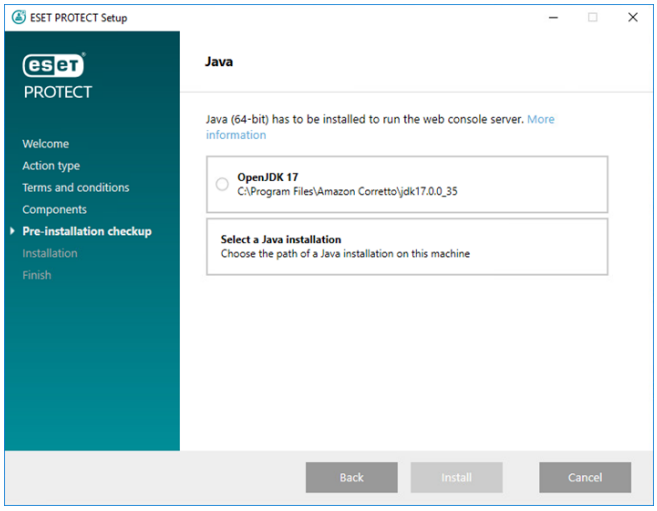
.NET v4 não está instalado

Instalar o .NET Framework



O Java não foi encontrado/Java (64 bits) detectado





Se você tiver várias versões do Java instaladas em seu sistema, recomendamos desinstalar as versões mais antigas do Java e manter apenas a versão mais recente do Java compatível.

> ⚠ A partir de janeiro de 2019, atualizações públicas do Oracle JAVA SE 8 para uso de negócios, comercial ou de produção precisarão de uma licença comercial. Se você não comprar uma assinatura JAVA SE, você pode usar este guia para mudar para uma alternativa sem custos. Consulte as versões compatíveis do JDK.

a)Para selecionar o Java já instalado, clique em **Selecionar uma instalação Java**, selecione a pasta onde o Java está instalado (com uma subpasta *bin*, por exemplo *C:\Program Files\Amazon Corretto\jdk1.8.0_212*) e clique em **OK**. O instalador informará se você tiver selecionado um caminho inválido.
b)Clique em **Instalar** para continuar ou **alterar** para alterar o caminho de instalação do Java.

A instalação não está no estado válido/Microsoft SQL Server Express

O instalador pode exibir essa notificação por vários motivos:
- O instalador está corrompido. Por exemplo, alguns arquivos do instalador estão faltando. Faça o download e execute o instalador tudo-em-um novamente.
- O caminho para o instalador tudo-em-um contém caracteres especiais, por exemplo: letras com diacríticos. Execute o instalador tudo-em-um do ESET PROTECT de um caminho sem caracteres especiais.

O disco do sistema tem apenas 32 MB livres

O instalador pode exibir esta notificação se seu sistema não tiver espaço em disco suficiente para instalar o ESET PROTECT.
Você precisa ter pelo menos 4.400 MB de espaço livre em disco para instalar o ESET PROTECT e todos os seus componentes.

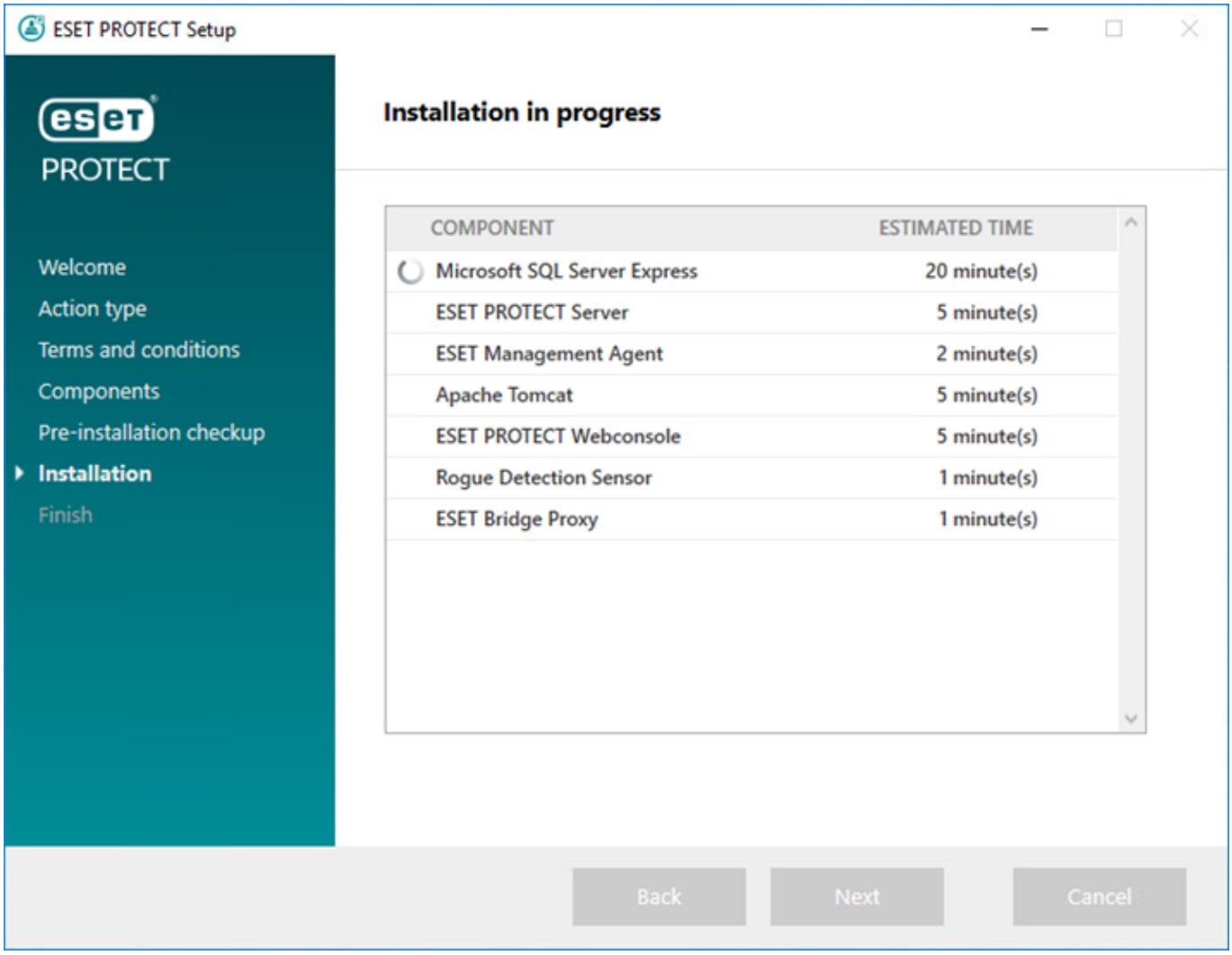
O ESET Remote Administrator 5.x ou anterior está instalado na máquina.

Se você tiver o ERA 5.x/6.x ou o ESMC 7.0/7.1:
- A atualização direta para ESET PROTECT 10.1 o não é compatível.
- Realize uma instalação limpa do ESET PROTECT 10.1.

Você pode atualizar diretamente para o ESET PROTECT 10.1 do ESMC 7.2 e de versões posteriores.

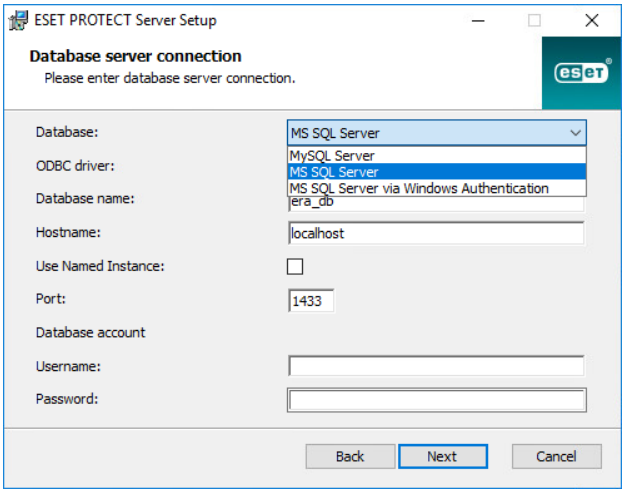
7. Quando a verificação de pré-requisitos for concluída e seu ambiente atender a todos os requisitos, a instalação será iniciada. Esteja ciente de que a instalação pode levar mais de uma hora, dependendo do seu sistema e configuração de rede.

> ℹ Quando a instalação está em andamento, o Assistente de instalação ESET PROTECT não responde.



8. Se você escolheu instalar o **Microsoft SQL Server Express** na etapa 4, o instalador vai realizar uma verificação de conexão de banco de dados. Se você tiver um servidor de banco de dados existente, o instalador irá solicitar que você insira seus detalhes de conexão de banco de dados:

Configure a conexão ao SQL/MySQL Server

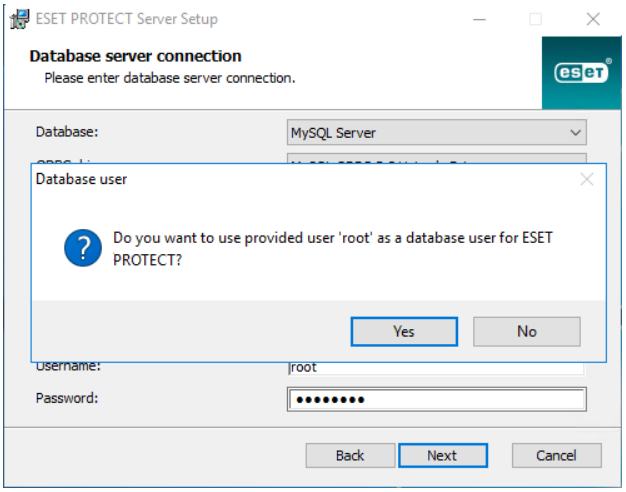


Digite seu **Nome do banco de dados**, **Nome de host**, número da **Porta** (você pode encontrar essas informações no Gerente de Configuração do Microsoft SQL Server) e detalhes da **conta de banco de dados** (**usuário** e **senha**) nos campos apropriados, e clique em **Avançar**. O instalador verificará a conexão do banco de dados. Se você tem um banco de dados existente (de uma instalação ESMC/ESET PROTECT) em seu servidor de banco de dados, isso será detectado. Você pode escolher **Usar banco de dados existente e aplicar atualização** ou **Remover banco de dados existente e instalar nova versão**.

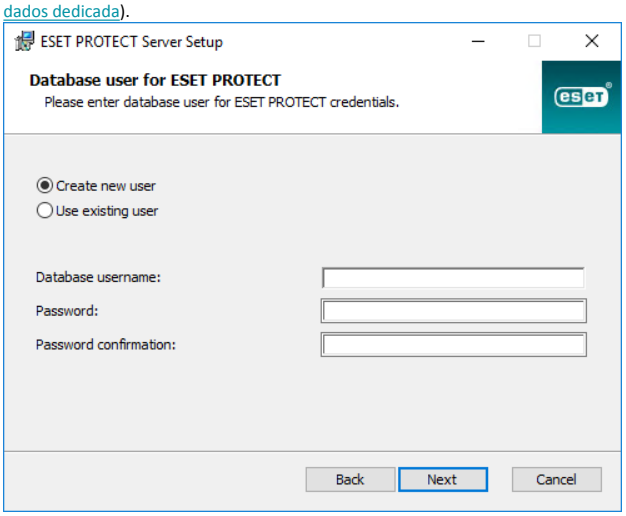
Usar instância nomeada – se você estiver usando um banco de dados Microsoft SQL, também será possível selecionar a caixa de marcação **Usar instância nomeada** para usar uma instância de banco de dados personalizada. Isso pode ser definido no campo **Nome de host** no formato *HOSTNAME\DB_INSTANCE* (por exemplo, *192.168.0.10\ESMC7SQL*). Para o banco de dados em agrupamento use apenas o nome do agrupamento. Se essa opção estiver selecionada, você não poderá alterar a porta de conexão do banco de dados: o sistema usará as portas padrão determinadas pela Microsoft. Para conectar o Servidor ESET PROTECT ao banco de dados Microsoft SQL instalado em um Cluster de failover, digite o nome do agrupamento no campo **Nome de host**.

Há duas opções ao inserir informações da **Conta do banco de dados**. Você pode usar uma **conta de usuário de banco de dados dedicada** que terá acesso apenas ao banco de dados ESET PROTECT, ou usar uma **conta SA** (Microsoft SQL) ou **conta de raiz** (MySQL). Se você decidir usar uma conta de usuário dedicada, você precisa que criar a conta com privilégios específicos. Para detalhes, consulte as Contas do usuário de banco de dados dedicado. Se você não pretende usar uma conta de usuário dedicada, digite a conta do administrador (SA ou raiz).

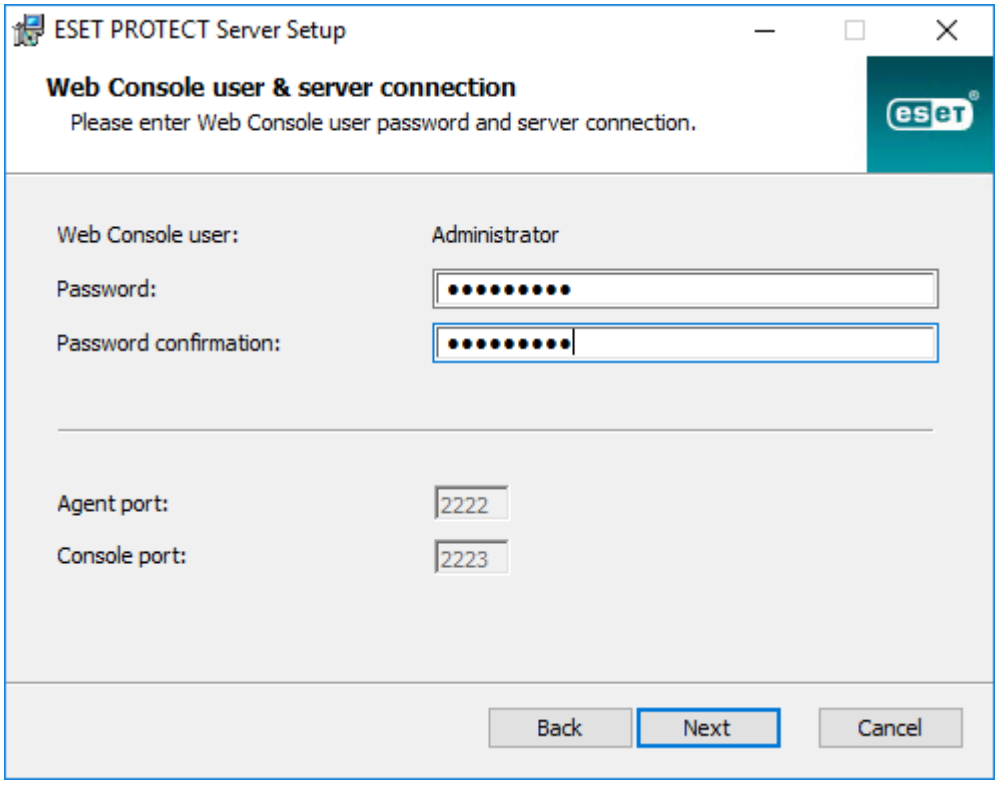
Se você inseriu uma **conta SA** ou **conta de raiz** na janela anterior, clique em **Sim** para continuar usando a conta SA/conta de raiz como o usuário de banco de dados para o ESET PROTECT.



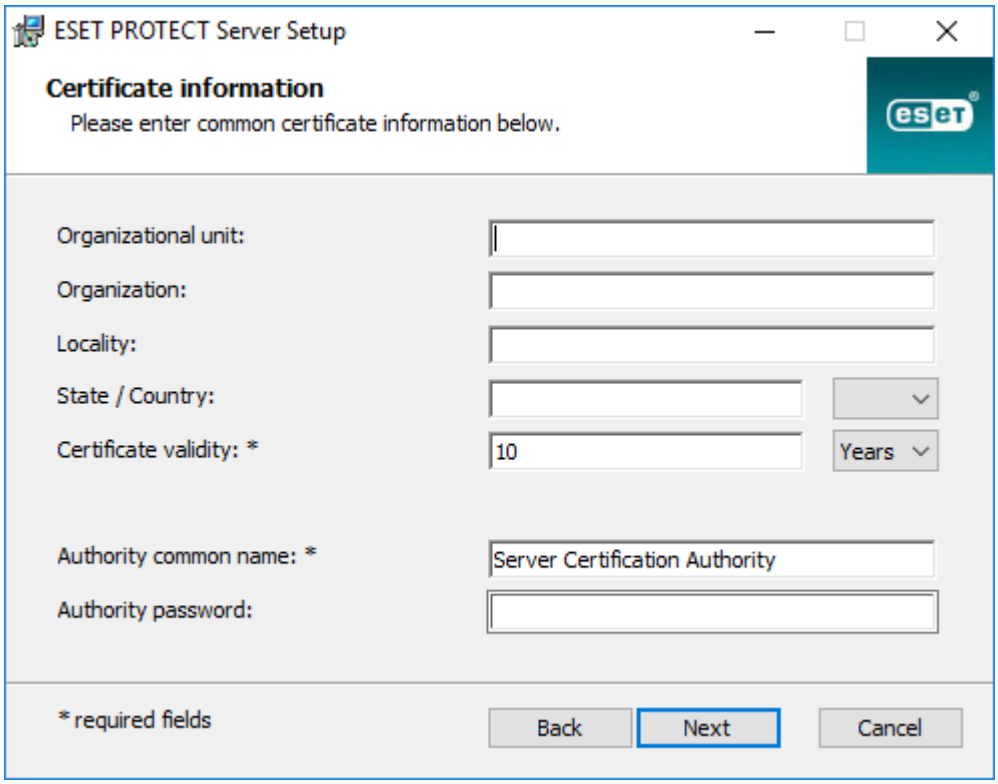
Se você clicar em **Não**, você precisará selecionar **Criar novo usuário** (se você ainda não criou um) ou **Usar usuário existente** (se você tiver uma conta de usuário de banco de dados dedicada).



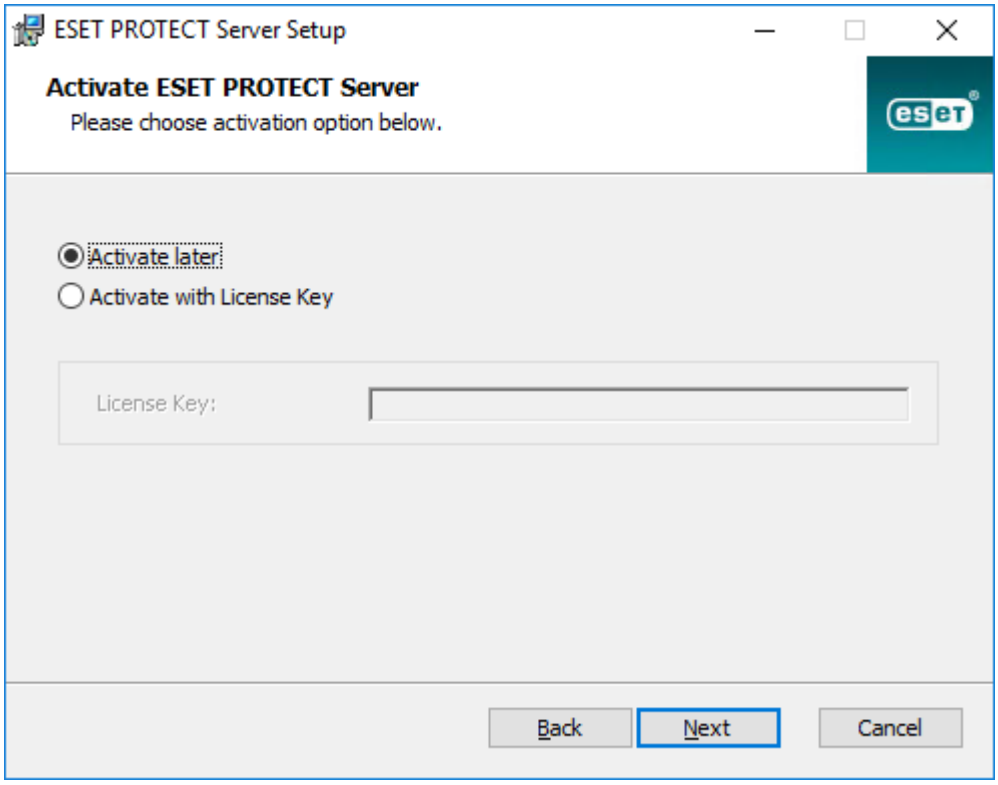
9. O instalador irá solicitar que você insira uma senha para a conta do Administrador do Web Console. Essa senha é importante, pois você a usará para fazer login no Console da Web ESET PROTECT. Clique em **Avançar**.



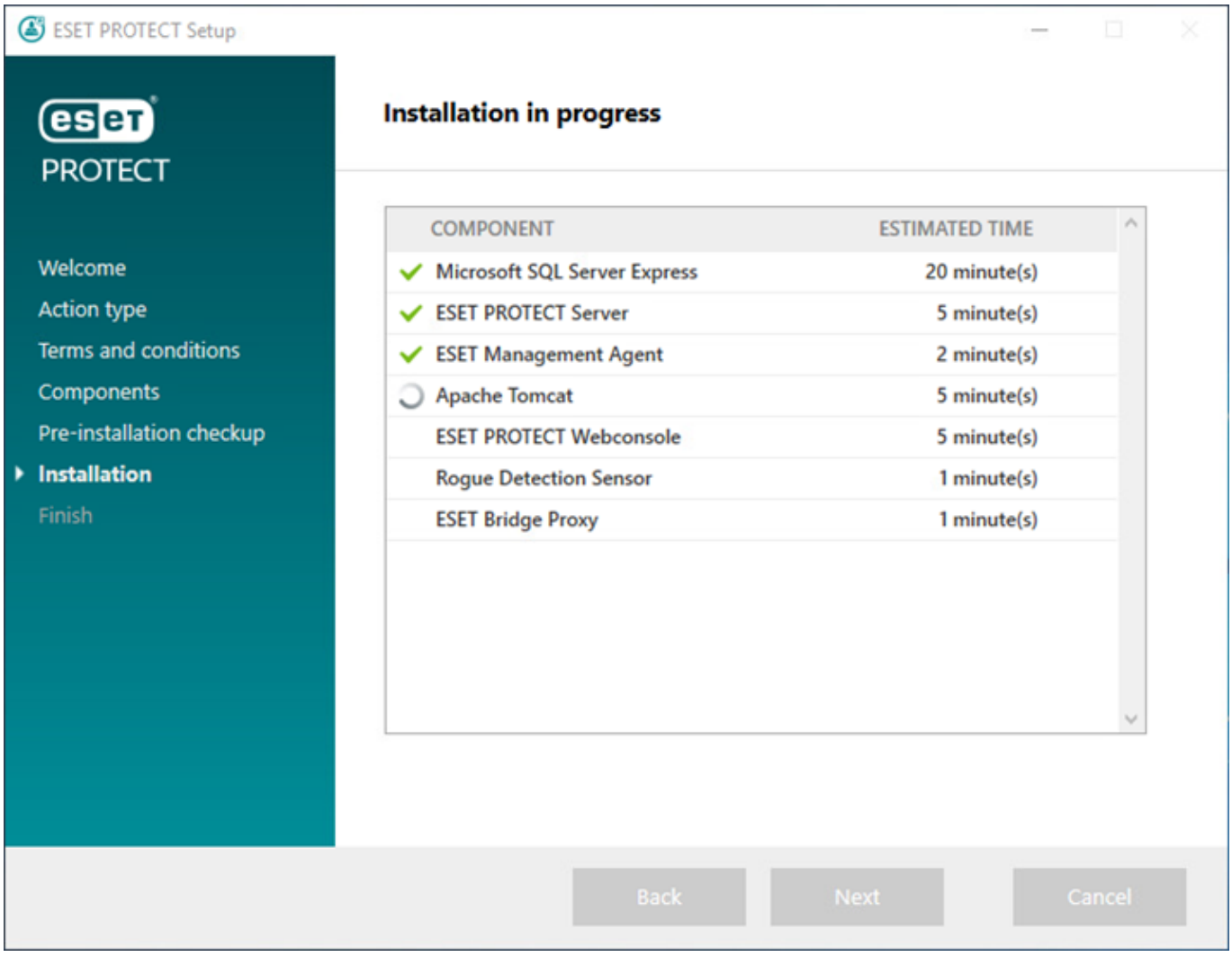
10. Você pode deixar os campos como estão, ou digitar suas informações corporativas para que apareçam nos detalhes dos certificados do Agente ESET Management e Servidor ESET PROTECT. Se você escolher inserir uma senha no campo **Senha de autoridade**, certifique-se de lembrá-la. Clique em **Avançar**.



11. Insira uma **Chave de licença** válida (incluída no novo email de compra que você recebeu da ESET) e clique em **Avançar**. Alternativamente, você pode escolher **Ativar mais tarde** (consulte o capítulo Ativação para instruções adicionais).



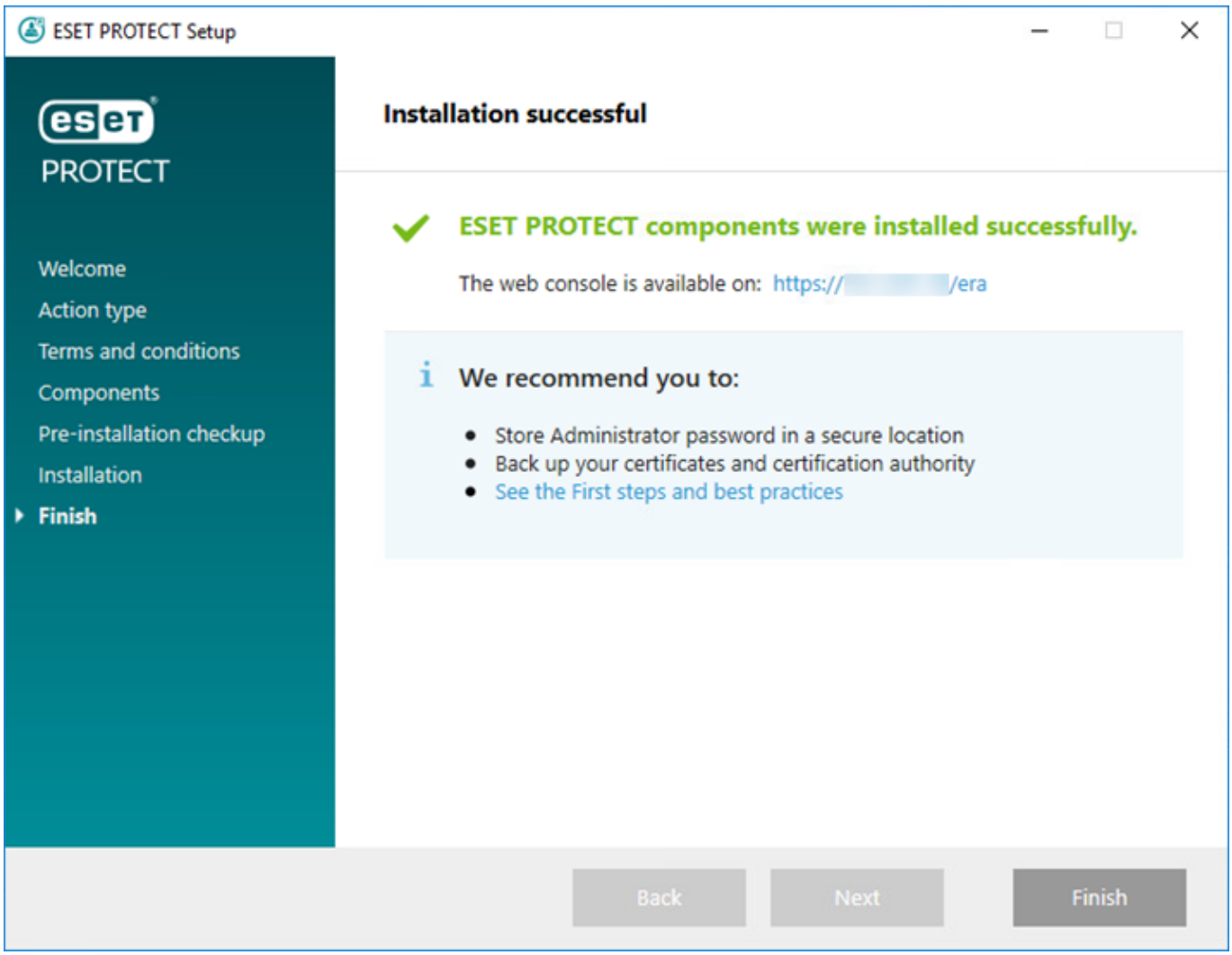
12. Você verá o progresso da instalação.



13. Se você escolheu instalar o **Rogue Detection Sensor**, você verá a janela de instalação para a unidade

WinPcap. Certifique-se de selecionar a caixa de seleção **Iniciar automaticamente a unidade WinPcap na inicialização**.

14. Quando a instalação estiver concluída, "A instalação do Servidor ESET PROTECT foi concluída com êxito" será exibido além do seu endereço URL do console web ESET PROTECT. Clique no URL para abrir o Console da Web ou clique em **Concluir**.



Se a instalação não for concluída com êxito:

- Revise os arquivos de relatório de instalação do pacote de Instalação tudo-em-um. O diretório de relatórios é o mesmo que o diretório do Instalador tudo-em-um, por exemplo: `C:\Users\Administrator\Downloads\x64\logs\`

- Consulte Solução de problemas para etapas adicionais para resolver seu problema.

Instale o Conector de dispositivo móvel ESET PROTECT (Autônomo)

O componente do Gerenciamento de dispositivo móvel/Conector ESET PROTECT (MDM/MDC) (apenas no local) teve seu fim da vida útil agendado. Ler mais. Recomendamos que você migre para o gerenciamento de dispositivo móvel em nuvem.

Para instalar o conector de dispositivo móvel como uma ferramenta autônoma, em um computador diferente daquele do Servidor ESET PROTECT, execute as etapas a seguir.

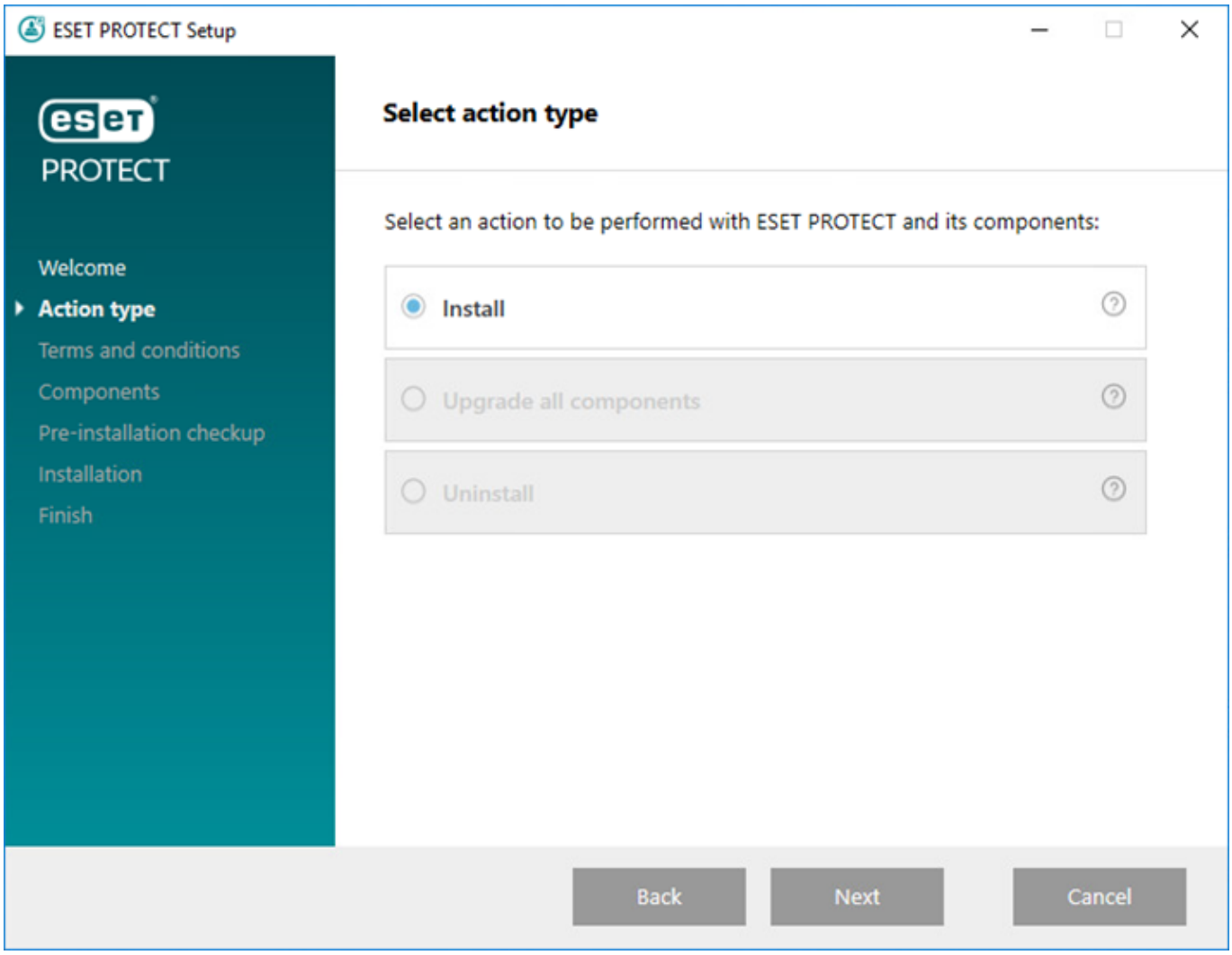
O Conector de dispositivo móvel deve ser acessível da internet de forma que os dispositivos móveis possam ser gerenciados em todos os momentos independentemente da sua localização.

Leve em conta que um dispositivo móvel se comunica com o Conector de dispositivo móvel, que inevitavelmente afeta o uso de dados móveis. Isso se aplica especialmente para o roaming.

Siga as etapas abaixo para instalar o Conector de dispositivo móvel no Windows:

1. Primeiro leia os pré-requisitos e certifique-se de que eles todos são cumpridos.

2. Clique duas vezes no pacote de instalação para abri-lo, selecione **Instalar** e clique em **Avançar**.

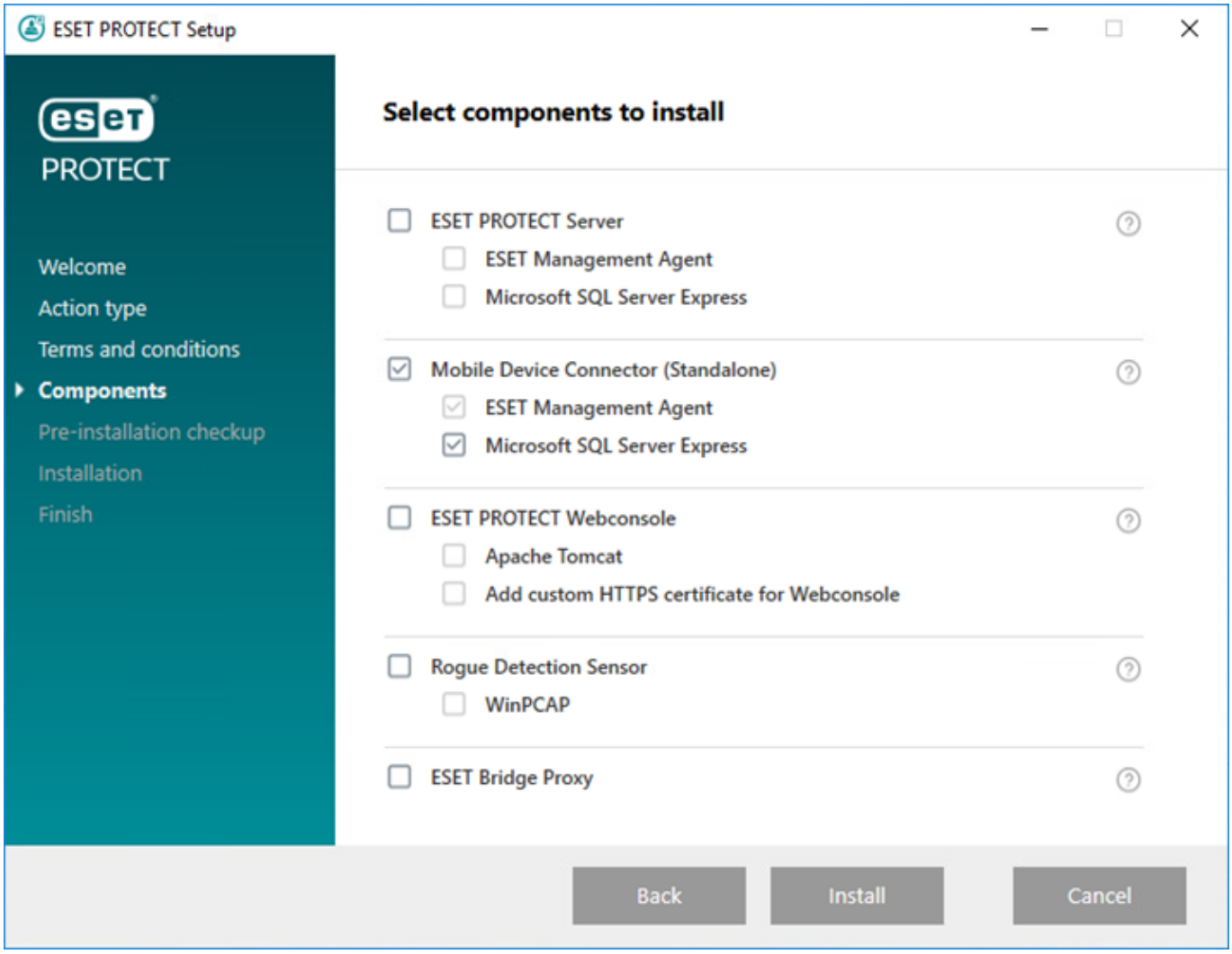


3. Marque a caixa de seleção ao lado de **Participar do programa de melhoria do produto** para enviar relatórios de travamento e dados de telemetria anônimos para a ESET (versão e tipo do sistema operacional, versão do produto ESET e outras informações específicas do produto).

4. Depois de aceitar o EULA, clique em **Avançar**.

5. Selecione apenas a caixa de marcação ao lado de **Mobile Device Connector (Autônomo)**. O Conector de dispositivo móvel ESET PROTECT requer um **banco de dados** para operação. Selecione o **Microsoft SQL Server Express** se quiser instalar o banco de dados, ou deixe a caixa de seleção desmarcada. Se quiser conectar a um

banco de dados existente, essa opção estará disponível durante a instalação. Clique em **Instalar** para continuar com a instalação.



6. Se você instalou um banco de dados como parte da instalação na etapa 5, o banco de dados agora será instalado automaticamente e você pode pular para a etapa 8. Se você escolheu não instalar um banco de dados na etapa 5, agora será solicitado que você conecte o componente MDM ao seu banco de dados existente.

> Você pode usar o mesmo servidor de banco de dados que você está usando para o banco de dados ESET PROTECT, mas recomendamos que use um servidor DB diferente se estiver planejando inscrever mais de 80 dispositivos móveis.

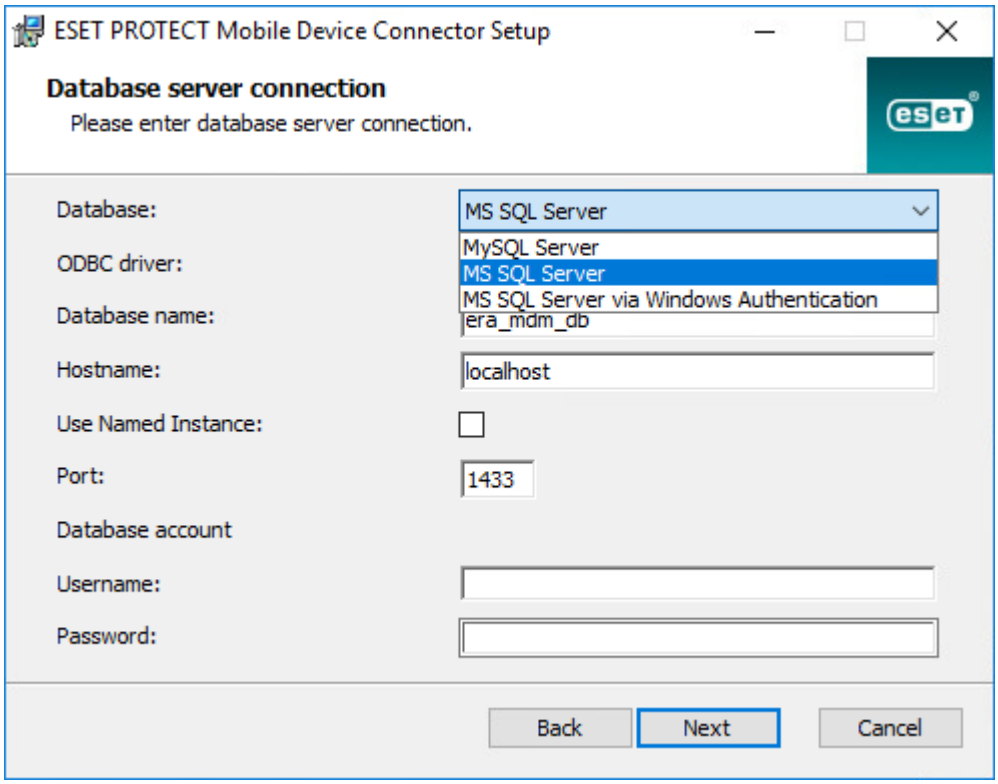
7. O instalador deve se conectar a um banco de dados existente que será usado pelo Conector de dispositivo móvel. Especifique os seguintes detalhes de conexão:

- **Banco de dados**: MySQL Server/MS SQL Server/MS SQL Server via autenticação do Windows
- **Driver ODBC**: MySQL ODBC 5.1 Driver/MySQL ODBC 5.2 Unicode Driver/MySQL ODBC 5.3 Unicode Driver/MySQL ODBC 8.0 Unicode Driver/SQL Server/SQL Server Native Client 10.0/ODBC Driver 11 for SQL Server/ODBC Driver 13 for SQL Server/ODBC Driver 17 for SQL Server/ODBC Driver 18 for SQL Server
- **Nome do banco de dados**: Recomendamos usar o nome pré-definido ou altera-lo, se necessário.
- **Nome de host**: nome de host ou endereço IP do seu servidor de banco de dados

- **Porta**: usado para conexão com o servidor do banco de dados

- **Nome de usuário/senha** de conta do administrador do banco de dados

- **Usar instância nomeada** – se você estiver usando um banco de dados Microsoft SQL, também será possível selecionar a caixa de marcação **Usar instância nomeada** para usar uma instância de banco de dados personalizada. Isso pode ser definido no campo **Nome de host** no formato *HOSTNAME\DB_INSTANCE* (por exemplo, *192.168.0.10\ESMC7SQL*). Para o banco de dados em agrupamento use apenas o nome do agrupamento. Se essa opção estiver selecionada, você não poderá alterar a porta de conexão do banco de dados: o sistema usará as portas padrão determinadas pela Microsoft. Para conectar o Servidor ESET PROTECT ao banco de dados Microsoft SQL instalado em um Cluster de failover, digite o nome do agrupamento no campo **Nome de host**.

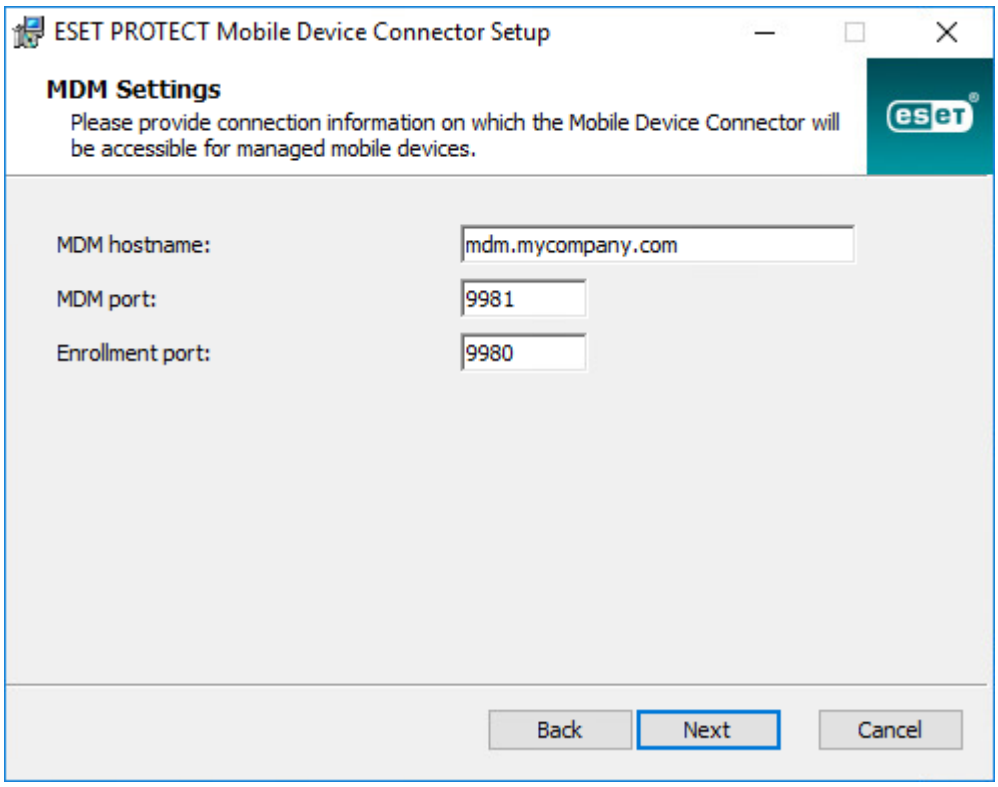


8. Se a conexão for bem sucedida, você será solicitado a verificar que quer usar o usuário fornecido como um usuário de banco de dados para o ESET PROTECT MDM.

9. Depois do novo banco de dados ser instalado com sucesso, ou do instalador ser conectado com sucesso a um banco de dados existente, você pode continuar com a Instalação MDM. Especifique seu **nome do host MDM**: é o domínio público ou endereço IP público do seu servidor MDM na forma como ele é acessível por dispositivos móveis da Internet.

O nome de host MDM deve ser digitado da mesma forma que está especificado no seu **certificado de Servidor HTTPS**, caso contrário o dispositivo móvel iOS vai se recusar a instalar o perfil MDM. Por exemplo, se houver um endereço IP especificado no certificado HTTPS, digite este endereço IP no campo de **nome de host MDM**. Se um FQDN estiver especificado (por exemplo, `mdm.mycompany.com`) no certificado HTTPS, insira este FQDN no campo **nome de host MDM**. Além disso, se um coringa * for usado (por exemplo, `*.mycompany.com`) no certificado HTTPS, você poderá usar `mdm.mycompany.com` no campo de **nome de host MDM**.

Tenha cuidado com o que é preenchido no campo **Nome de host MDM** nessa etapa da instalação. Se as informações estiverem incorretas, ou em um formato errado, o Conector MDM não funcionará adequadamente e a única forma de solucionar este problema será através da reinstalação do componente.



10. Na próxima etapa verifique a conexão ao banco de dados clicando em **Avançar**.

11. Conecte o Conector MDM ao Servidor ESET PROTECT. Preencha o **host de Servidor** e a **porta de Servidor** necessários para a conexão com o Servidor ESET PROTECT e selecione a **Instalação auxiliada por servidor** ou **Instalação off-line** para continuar:

- **Instalação auxiliada por servidor** - Fornece ao ESET PROTECT as credenciais do administrador do Console da Web e o instalador vai fazer download dos certificados necessários automaticamente. Verifique também as permissões necessárias para a instalação auxiliada por servidor.

    1.Insira seu **host de Servidor** - nome ou endereço IP do seu Servidor ESET PROTECT e **porta do console da Web** (deixe a porta padrão 2223 se você não estiver usando uma porta personalizada). Forneça também as credenciais de conta do administrador do console da Web - **Nome de usuário/Senha**.

    2.Quando pedirem para Aceitar o certificado, clique em **Sim**. Continue para a etapa 11.

- **Instalação off-line** - Fornece um certificado de Proxy e uma Autoridade de certificação que pode ser exportada do ESET PROTECT. Alternativamente, é possível usar seu certificado personalizado e a Autoridade de certificação adequada.

    1.Clique em **Navegar** ao lado de Certificado de mesmo nível e navegue até o local do seu **Certificado de mesmo nível** (este é o certificado de Proxy que você exportou do ESET PROTECT). Deixe o campo de texto de **Senha certificada** em branco, pois este certificado não requer senha.

    2.Repita o procedimento para a Autoridade de Certificação e continue para a etapa 11.

Se estiver usando certificados personalizados com o ESET PROTECT (em vez dos padrão gerados automaticamente durante a instalação do ESET PROTECT), eles devem ser usados quando você é solicitado a fornecer um certificado Proxy.

12. Especifique a pasta de destino para o conector de dispositivo móvel (recomendamos usar o padrão), clique em **Avançar** > **Instalar**.

Depois de concluir a instalação MDM, será solicitado que você realize a instalação do Agente. Clique em **Avançar** para começar a instalação e aceite o EULA se você concordar com ele, depois siga essas etapas:

1. Digite o **Host do servidor** (nome de host ou endereço IP do seu Servidor ESET PROTECT) e a **porta de servidor** (a porta padrão é 2222, se você estiver usando uma porta diferente, substitua a porta padrão pelo seu número de porta personalizado).

Certifique-se de que o **Host do servidor** corresponde a pelo menos um dos valores (de preferência o FQDN) definido no campo **Host** do **Certificado do servidor**. Caso contrário, você receberá um erro dizendo "O certificado de servidor recebido não é válido". A única exceção é caso exista um caractere curinga (*) no campo de Host do certificado do servidor, o que significa que ele vai funcionar com qualquer **Host de servidor**.

2. Se você estiver usando um proxy, selecione a caixa de seleção **Usar Proxy**. Quando selecionada, o instalador continuará com a **instalação off-line**.

Essa configuração de proxy é usada apenas para (replicação) entre o Agente ESET Management e o Servidor ESET PROTECT, não para o armazenamento em cache de atualizações.
- **Nome de host do Proxy**: nome de host ou endereço IP da máquina do Proxy HTTP.
- **Porta Proxy**: o valor padrão é 3128.
- **Nome de usuário**, **Senha**: insira as credenciais usadas pelo seu proxy se ele usar autenticação.

Você pode alterar as configurações de proxy mais tarde na sua política. O Proxy deve ser instalado antes de ser possível configurar uma conexão Agente - Servidor via Proxy.

3. Selecione uma das opções de instalação a seguir e siga os passos da seção apropriada abaixo:

Instalação auxiliada por servidor - será necessário fornecer credenciais de administrador do Console da Web ESET PROTECT (o instalador vai fazer download dos certificados necessários automaticamente).

Instalação off-line - você precisará fornecer um Certificado de Agente e Autoridade de certificação que pode ser exportado do ESET PROTECT. Alternativamente, é possível usar seu certificado personalizado.

- Para continuar com a instalação **do Agente auxiliada por servidor** siga as etapas a seguir:

1. Insira o nome de host ou endereço IP do seu console da Web ESET PROTECT (igual ao do Servidor ESET PROTECT) no campo **Host do servidor**. Deixe a **porta do console da Web** definida na porta padrão 2223 se não estiver usando uma porta personalizada. Além disso, insira as credenciais da sua conta do console da Web nos campos **Nome de usuário e Senha**. Para entrar como um usuário do domínio, selecione a caixa de seleção ao lado de **Entrar no domínio**.

- Certifique-se de que o **Host do servidor** corresponde a pelo menos um dos valores (de preferência o FQDN) definido no campo Host do **Certificado do servidor**. Caso contrário, você receberá um erro dizendo “O certificado de servidor recebido não é válido”. A única exceção é caso exista um caractere curinga (*) no campo de Host do certificado do servidor, o que significa que ele vai funcionar com qualquer **Host de servidor**.
- Não é possível usar um usuário com autenticação em dois fatores para instalações auxiliadas por servidor.

2. Clique em **Sim** quando perguntado se deseja aceitar o certificado.

3. Selecione **Não criar computador (o computador será criado automaticamente durante a primeira conexão)** ou **Escolher grupo estático personalizado**. Se clicar em **Escolher grupo personalizado estático** você será capaz de selecionar a partir de uma lista de grupos estáticos no ESET PROTECT. O computador será adicionado ao grupo selecionado.

4. Especifique uma pasta de destino para o Agente ESET Management (recomendamos usar o local padrão), clique em **Avançar** e depois em **Instalar**.

- Para continuar com a **instalação do Agente off-line** siga essas etapas:

1. Se você selecionou **Usar Proxy** na etapa anterior, forneça o **nome de host do Proxy**, **porta do Proxy** (a porta padrão é 3128),**Nome de usuário** e **Senha** e clique em **Avançar**.

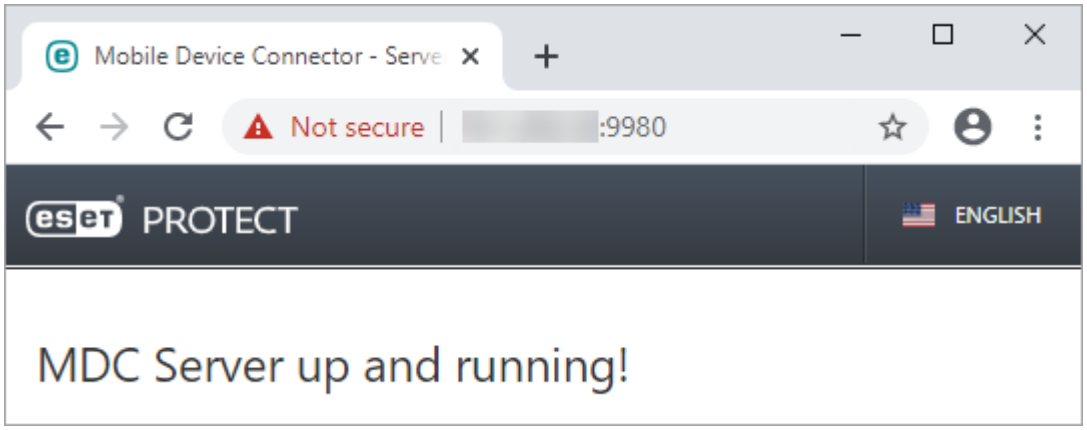
2. Clique em **Procurar** e vá até a localização do seu certificado de mesmo nível (este é o Certificado de Agente exportado do ESET PROTECT). Deixe o campo de texto de **Senha certificada** em branco, pois este certificado não requer senha. Você não precisa procurar uma **Autoridade de certificação** - deixe esse campo em branco.

Se estiver usando um certificado personalizado com ESET PROTECT (em vez dos modelos padrão gerados automaticamente durante a instalação do ESET PROTECT), use seus certificados personalizados de acordo.

A senha do certificado não deve ter os seguintes caracteres: " \ Esses caracteres causam um erro crítico durante a inicialização do Agente.

3. Clique em **Avançar** para instalar a pasta padrão ou clique em **Alterar** para escolher outra pasta (recomendamos usar a localização padrão).

Depois de concluída a instalação, verifique se o Conector de dispositivo móvel está sendo executado corretamente abrindo *https://your-mdm-hostname:enrollment-port* (por exemplo, *https://mdm.company.com:9980*) no seu navegador da web ou de um dispositivo móvel. Se a instalação for realizada com êxito, você verá a mensagem a seguir:



Agora você pode ativar MDM do ESET PROTECT.

Instalação de componente no Windows

A maioria dos cenários de instalação requer que você instale vários componentes do ESET PROTECT em diferentes máquinas para acomodar diversas arquiteturas de rede, atender aos requisitos de desempenho ou por outros motivos. Os pacotes de instalação a seguir estão disponíveis para componentes individuais ESET PROTECT:

Instalação de principais componentes:

- Servidor ESET PROTECT
- Console da Web ESET PROTECT – Você pode escolher instalar o Web Console ESET PROTECT em um computador diferente do computador executando o Servidor ESET PROTECT.
- Agente ESET Management (precisa estar instalado nos computadores do cliente, opcional no Servidor ESET PROTECT)

Instalação de componentes opcionais:

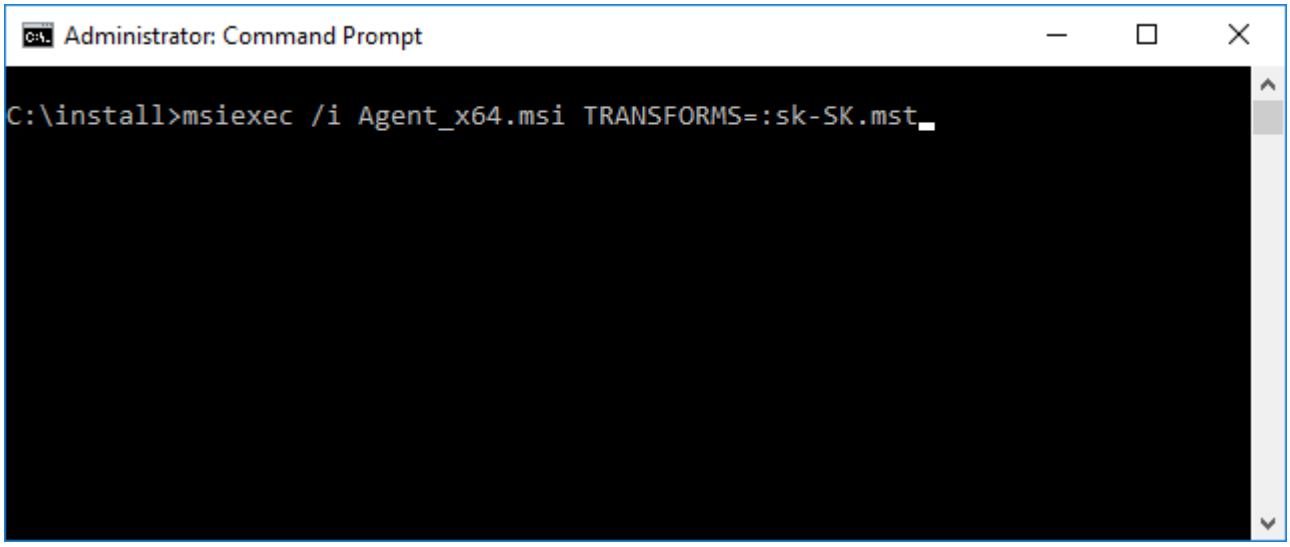
- Sensor RD
- Conector de dispositivo móvel
- ESET Bridge Proxy HTTP
- Ferramenta de imagem

Veja também instalação Tudo-em-um ESET PROTECT.

Para instruções sobre como atualizar o ESMC para o ESET PROTECT 10.1 mais recente, consulte nossos procedimentos de atualização.

Se quiser executar a instalação em seu idioma local, será preciso iniciar o instalador MSI de um componente ESET PROTECT em particular da linha de comando.

Abaixo temos um exemplo de como executar a instalação no idioma eslovaco:



Para selecionar o idioma no qual você quer executar o instalador, especifique o parâmetro `TRANSFORMS` correspondente de acordo com esta tabela:

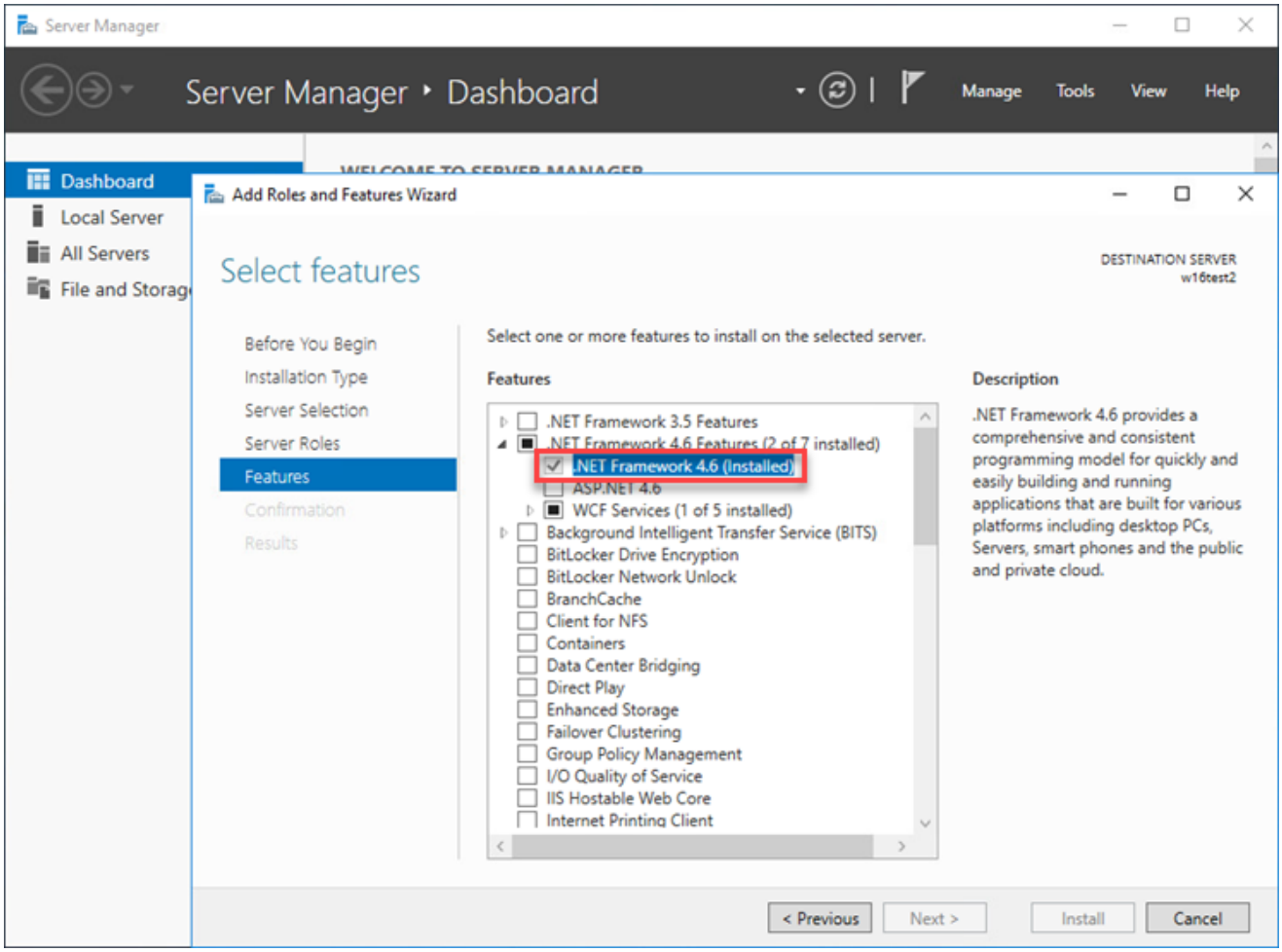
Idioma	Código
Inglês (Estados Unidos)	en-US
Árabe (Egito)	ar-EG
Chinês simplificado	zh-CN
Chinês tradicional	zh-TW
Croata (Croácia)	hr-HR
Tcheco (República Tcheca)	cs-CZ
Francês (França)	fr-FR
Francês (Canadá)	fr-CA
Alemão (Alemanha)	de-DE
Grego (Grécia)	el-GR
Húngaro (Hungria)*	hu-HU
Indonésio (Indonésia)*	id-ID
Italiano (Itália)	it-IT
Japonês (Japão)	ja-JP
Coreano (Coréia)	ko-KR
Polonês (Polônia)	pl-PL
Português (Brasil)	pt-BR
Russo (Rússia)	ru-RU
Espanhol (Chile)	es-CL
Espanhol (Espanha)	es-ES
Eslovaco (Eslováquia)	sk-SK
Turco (Turquia)	tr-TR
Ucraniano (Ucrânia)	uk-UA

* Apenas o produto está disponível neste idioma, a Ajuda on-line não está disponível.

Instalação do servidor – Windows

Pré-requisitos

- Você deve ter uma chave de licença válida.
- Você deve ter um sistema operacional Windows compatível.
- As portas necessárias devem estar abertas e disponíveis – consulte a lista completa de portas aqui.
- O servidor e conector de banco de dados compatíveis (Microsoft SQL Server ou MySQL) estão instalados e em execução. Recomendamos que você revise os detalhes de configuração do servidor do banco de dados (Microsoft SQL Server ou MySQL) para ter o banco de dados configurado adequadamente para uso com o ESET PROTECT. Leia nosso artigo da Base de conhecimento para configurar seu banco de dados e o usuário do banco de dados para Microsoft SQL ou MySQL.
- Console web ESET PROTECT instalado para gerenciar o Servidor ESET PROTECT.
- A instalação do Microsoft SQL Server Express requer o Microsoft .NET Framework 4. Você pode instalar usando o **Assistente para adicionar de funções e recursos**:



Instalação

Siga as etapas abaixo para instalar o componente do Servidor ESET PROTECT no Windows:

Certifique-se de atender a todos os pré-requisitos de instalação listados acima.

1. Visite a seção de download ESET PROTECT para fazer download de um instalador autônomo para este componente ESET PROTECT (*server_x64.msi*).

2. Execute o instalador do Servidor ESET PROTECT e aceite o EULA se você concordar com ele.

3. Marque a caixa de seleção ao lado de **Participar do programa de melhoria do produto** para enviar relatórios de travamento e dados de telemetria anônimos para a ESET (versão e tipo do sistema operacional, versão do produto ESET e outras informações específicas do produto).

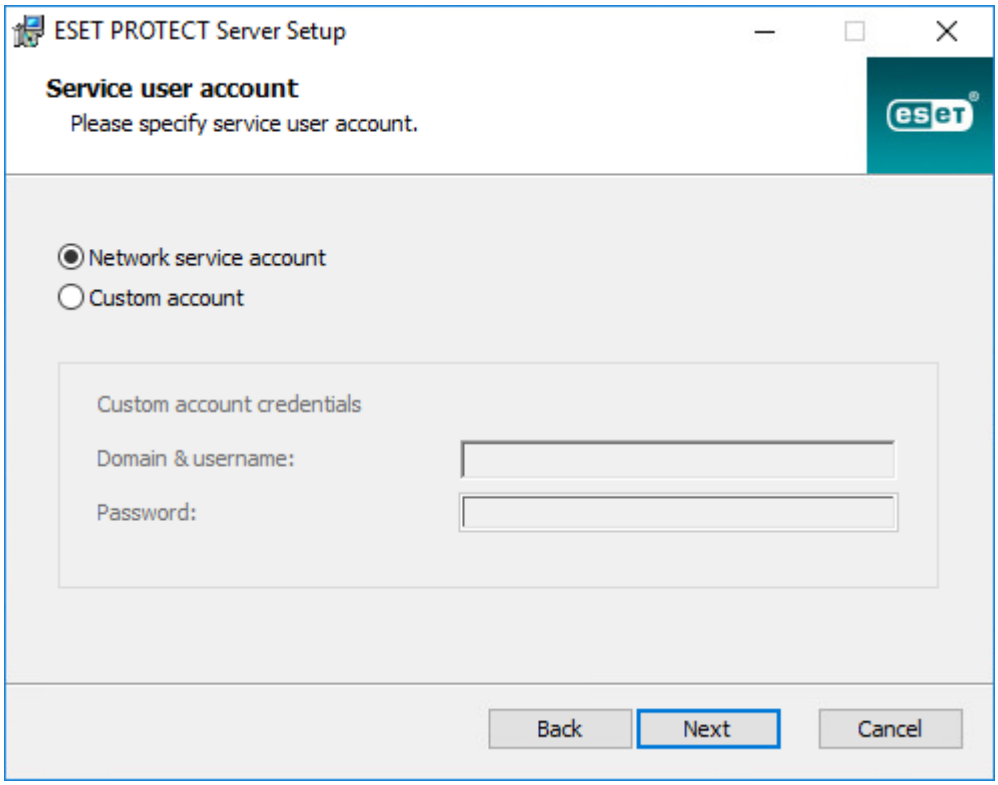
4. Deixe vazia a caixa de seleção ao lado de **Esta é uma instalação de agrupamento** e clique em **Avançar**.

Esta é uma instalação de agrupamento?

Se você estiver instalando um Servidor ESET PROTECT em um agrupamento de failover, marque a caixa de seleção ao lado de **Esta é uma instalação de agrupamento**. Especifique o **Caminho de dados de aplicativo personalizado** para apontar para um armazenamento compartilhado do agrupamento. Os dados devem ser armazenados em um local que possa ser acessado por todos os nós dentro do agrupamento.

5. Selecione uma **Conta de serviço de usuário**. Essa conta será usada para executar o Serviço de servidor ESET PROTECT. As opções disponíveis são:

- **Conta de serviço de rede** – selecione essa opção se você não usar um domínio.
- **Conta personalizada**: forneça credencias do usuário do domínio: `DOMÍNIO\NOMEDEUSUARIO` e senha.



6. Conecte-se a um banco de dados. Todos os dados são armazenados aqui (senha do console da Web ESET PROTECT, relatórios do computador cliente, etc.):

- **Banco de dados**: MySQL Server/MS SQL Server/MS SQL Server via autenticação do Windows

• **Driver ODBC**: MySQL ODBC 5.1 Driver/MySQL ODBC 5.2 Unicode Driver/MySQL ODBC 5.3 Unicode Driver/MySQL ODBC 8.0 Unicode Driver/SQL Server/SQL Server Native Client 10.0/ODBC Driver 11 for SQL Server/ODBC Driver 13 for SQL Server/ODBC Driver 17 for SQL Server/ODBC Driver 18 for SQL Server

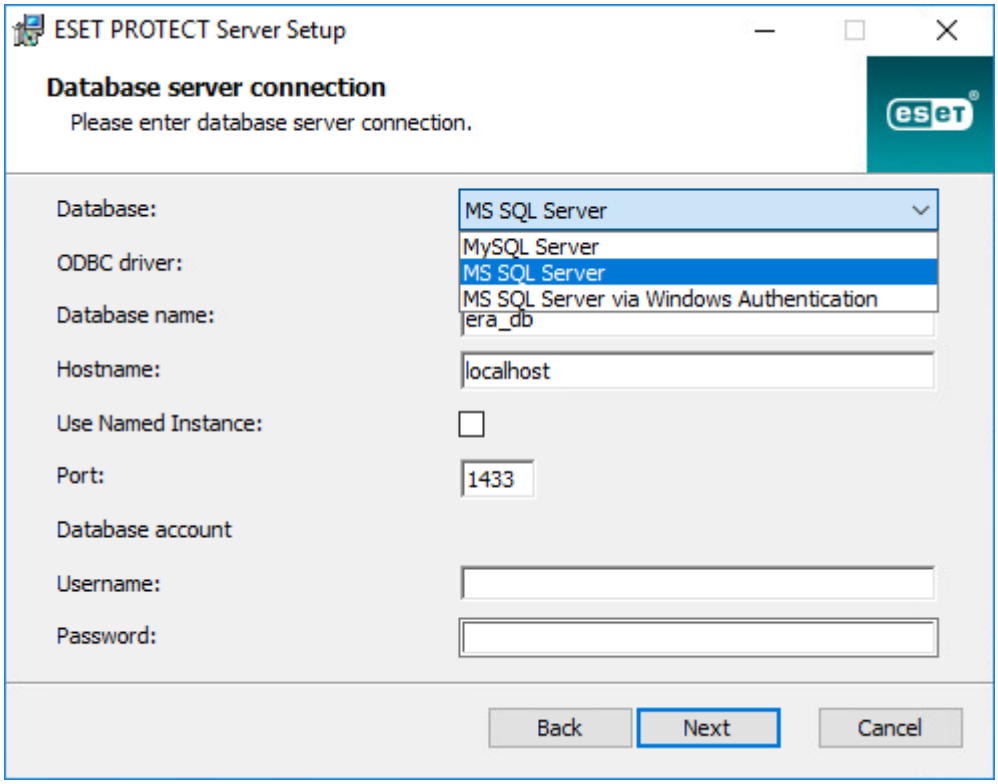
• **Nome do banco de dados**: Recomendamos usar o nome pré-definido ou altera-lo, se necessário.

• **Nome de host**: nome de host ou endereço IP do seu servidor de banco de dados

• **Porta**: usado para conexão com o servidor do banco de dados

• **Nome de usuário/senha** de conta do administrador do banco de dados

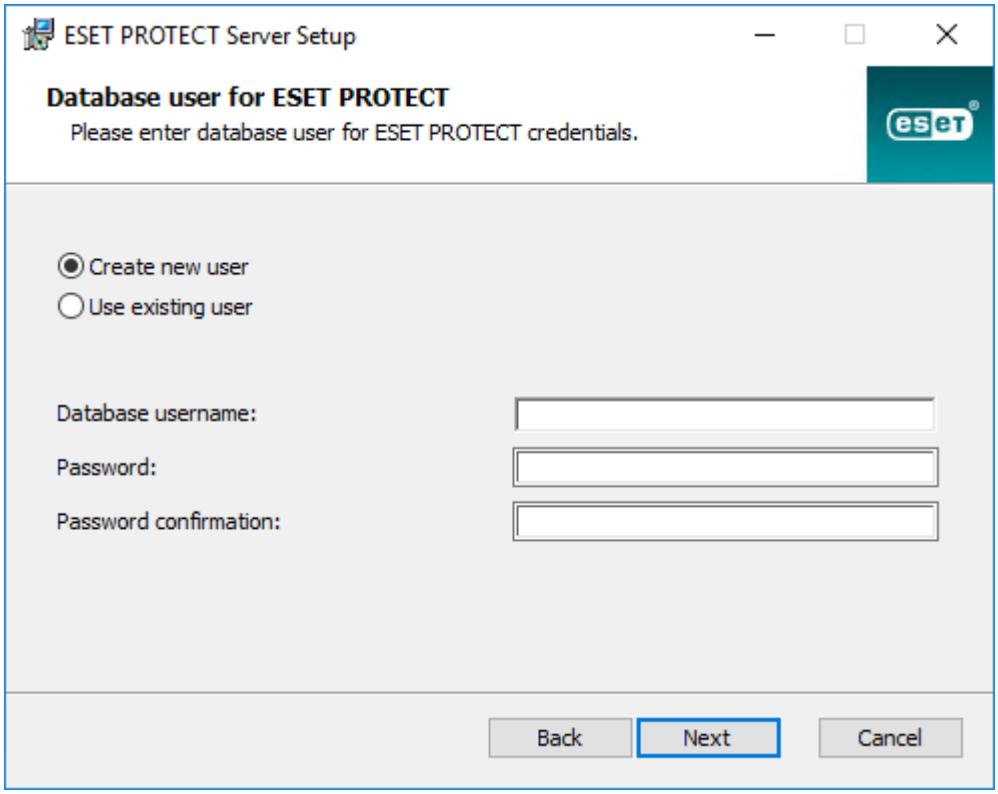
• **Usar instância nomeada** – se você estiver usando um banco de dados Microsoft SQL, também será possível selecionar a caixa de marcação **Usar instância nomeada** para usar uma instância de banco de dados personalizada. Isso pode ser definido no campo **Nome de host** no formato *HOSTNAME\DB_INSTANCE* (por exemplo, *192.168.0.10\ESMC7SQL*). Para o banco de dados em agrupamento use apenas o nome do agrupamento. Se essa opção estiver selecionada, você não poderá alterar a porta de conexão do banco de dados: o sistema usará as portas padrão determinadas pela Microsoft. Para conectar o Servidor ESET PROTECT ao banco de dados Microsoft SQL instalado em um Cluster de failover, digite o nome do agrupamento no campo **Nome de host**.



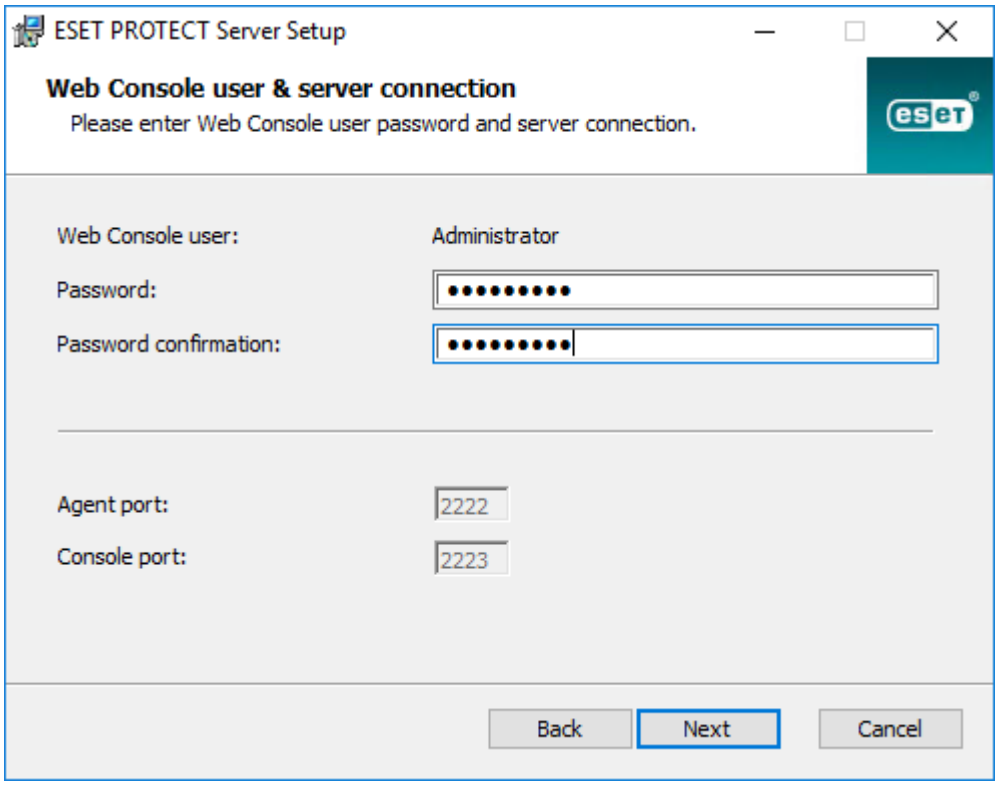
O Servidor ESET PROTECT armazena grandes blocos de dados no banco de dados. Portanto, é necessário configurar o MySQL para aceitar pacotes grandes para que o ESET PROTECT seja executado corretamente.

Essa etapa verificará sua conexão com o banco de dados. Se a conexão for boa, vá para a próxima etapa.

7. Selecione um usuário do ESET PROTECT que tenha acesso ao banco de dados. Você pode utilizar um usuário existente ou a configuração pode criar um usuário para você.



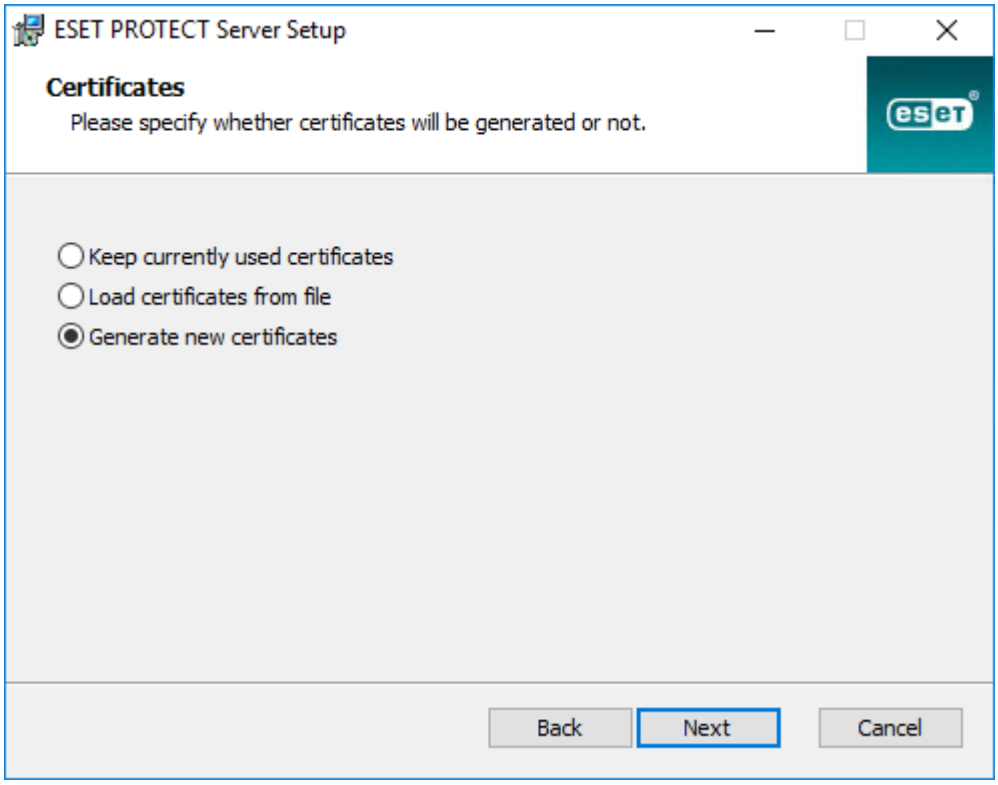
8. Insira uma senha para o acesso ao **console da Web**.



9. O ESET PROTECT utiliza certificados para a comunicação cliente-servidor. Selecione uma das seguintes opções:

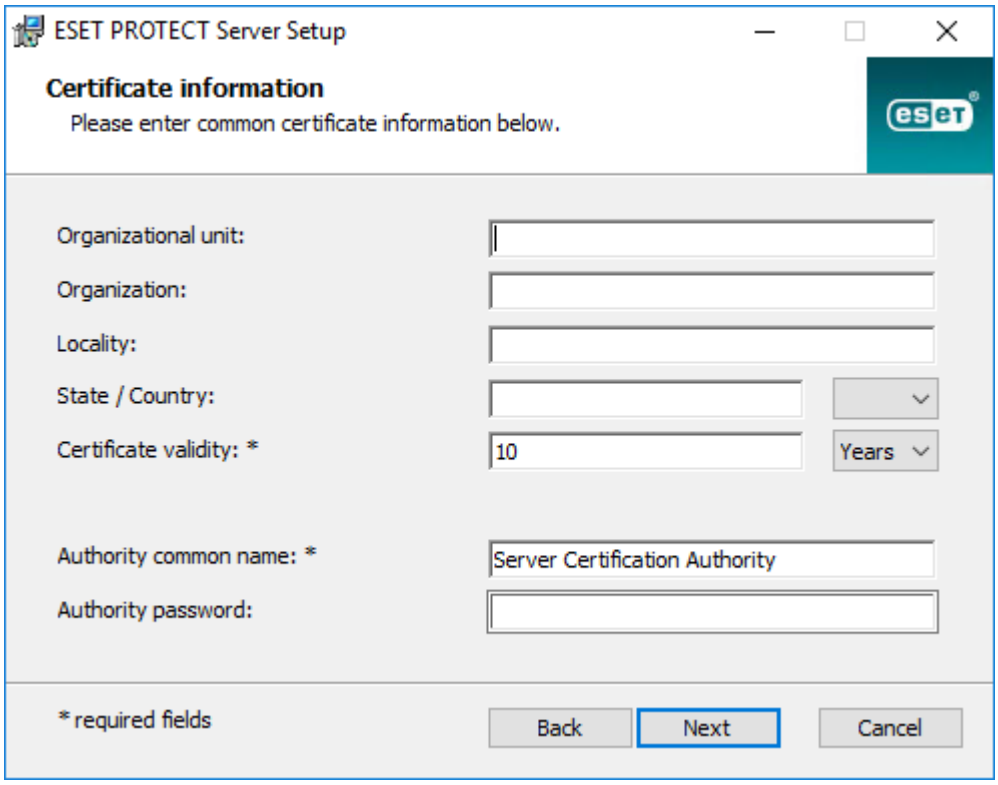
- **Manter certificados atualmente usados** – esta opção só está disponível se o banco de dados já foi usado com outro Servidor ESET PROTECT.
- **Carregar certificados do arquivo** – selecione seu certificado de Servidor e Autoridade de certificação existentes.

- **Gerar novos certificados** – o instalador gera novos certificados.



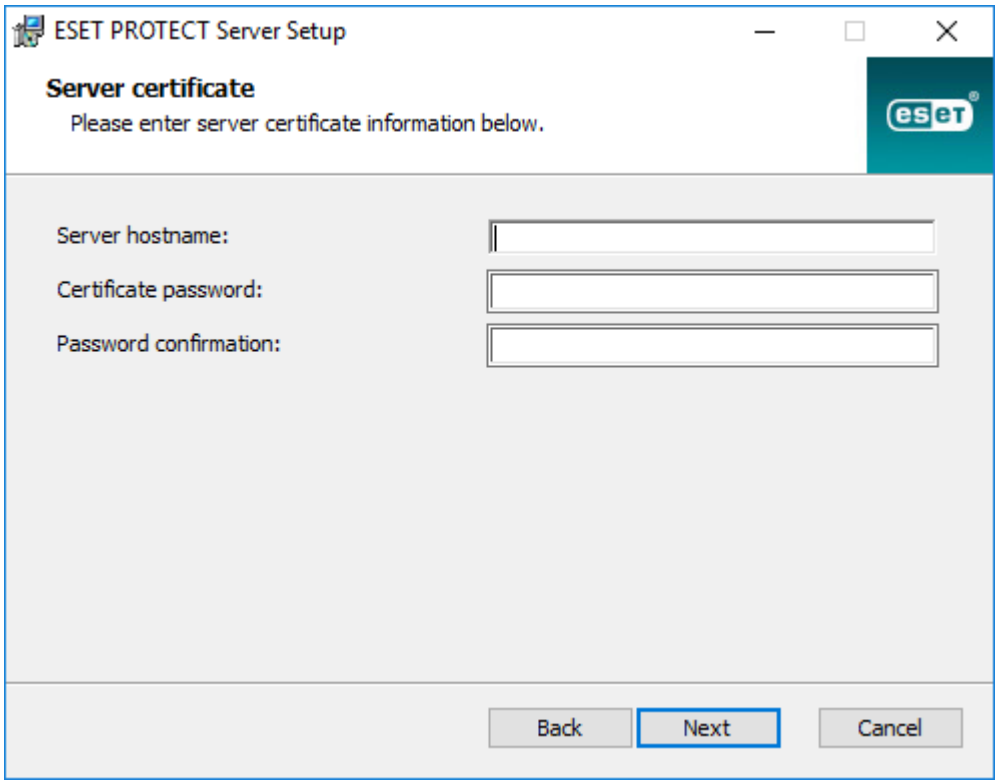
10. Siga esta etapa se você selecionou a opção **Gerar novos certificados** na etapa anterior.

    a)Especifique informações adicionais sobre os certificados (opcional). Se você digitar a **Senha da autoridade**, certifique-se de lembrá-la.

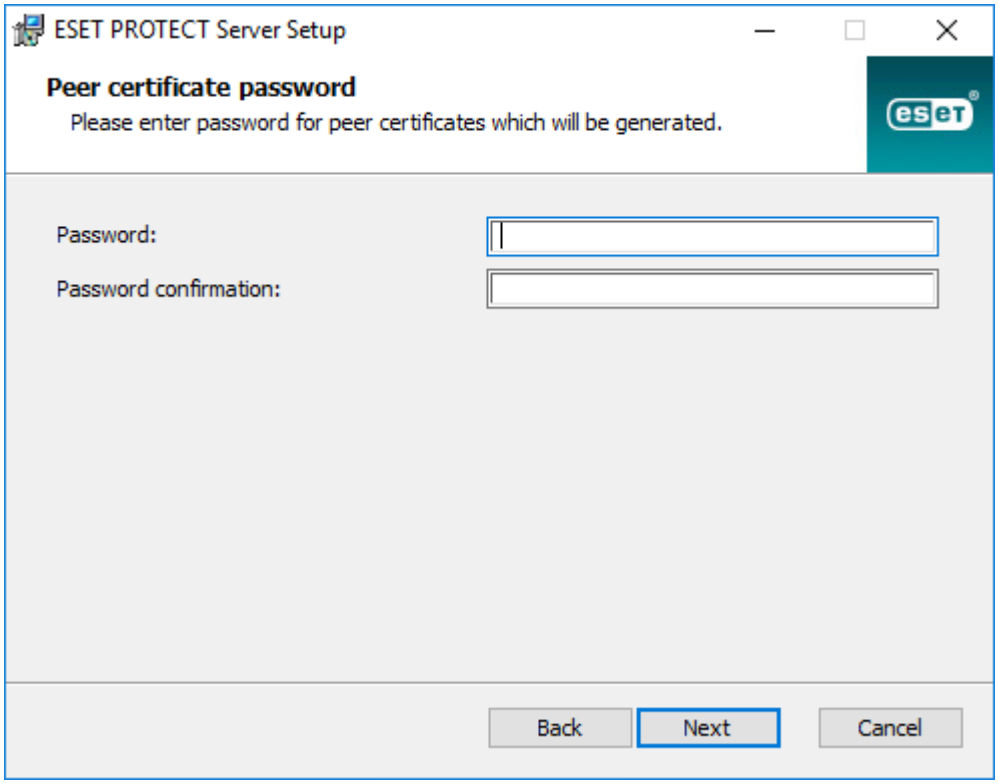


    b)No campo **Certificado do servidor**, digite o **Nome de host do servidor** e a **Senha do certificado** (opcional).

O **Nome de host do servidor** no Certificado so servidor não deve ter qualquer uma das seguintes palavras-chave: `server`, `proxy`, `agent`.

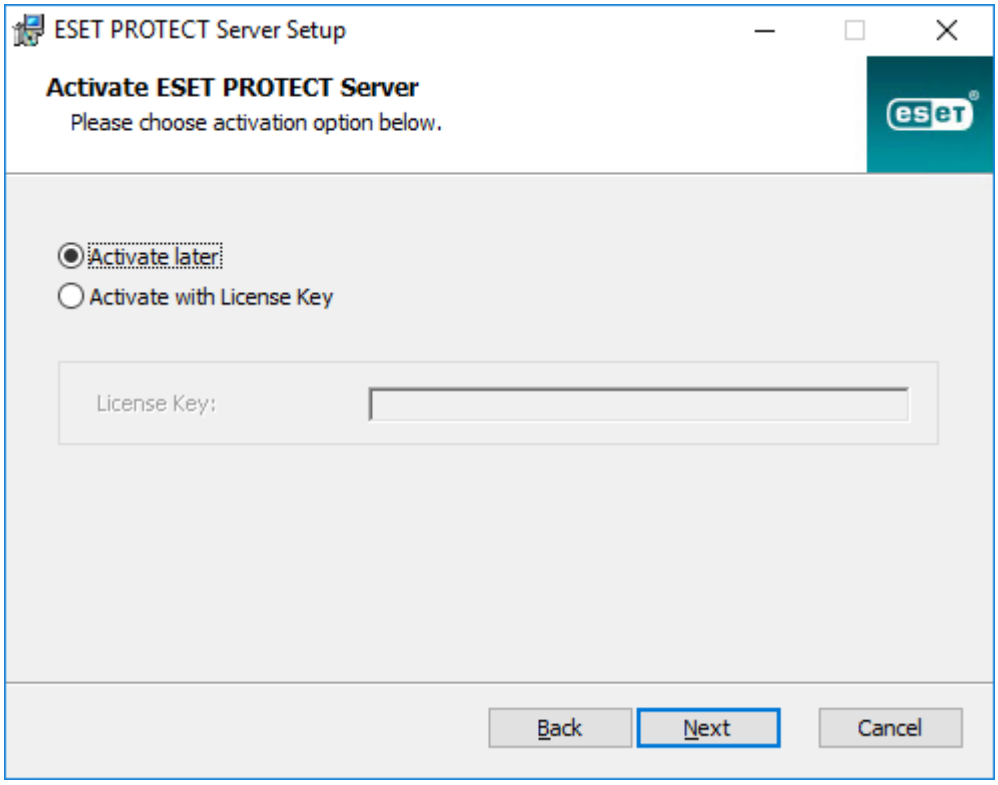


c)No campo **Senha do certificado de mesmo nível**, digite a senha para os Certificados de mesmo nível do Agente e do Proxy.



11. A configuração poderá realizar uma tarefa inicial Sincronização de grupo estático. Selecione o método (**Não sincronizar**, **Sincronizar com rede Windows**, **Sincronizar com Active Directory**) e clique em **Avançar**.

12. Insira uma Chave de licença válida ou escolha **Ativar mais tarde**.



13. Confirme ou altere a pasta de instalação do servidor e clique em **Avançar**.

14. Clique em **Instalar** para instalar o servidor ESET PROTECT.

Quando tiver concluído a instalação do Servidor ESET PROTECT, é possível instalar o Agente ESET Management na mesma máquina (opcional) para permitir o gerenciamento do Servidor da mesma forma que gerencia um computador cliente.

Requisitos do Microsoft SQL Server

Os seguintes requisitos para o Microsoft SQL Server devem ser atendidos:

- Instale uma versão compatível do Microsoft SQL Server. Escolha a autenticação em **Modo misturado** durante a instalação.

- Se você já tiver o Microsoft SQL Server instalado, defina a autenticação para o **Modo misturado (autenticação do SQL Server e autenticação Windows)**. Para fazer isso, siga as Instruções neste artigo da Base de conhecimento. Se quiser usar a **Autenticação do Windows** para entrar no Microsoft SQL Server, siga as etapas neste artigo da Base de conhecimento.

- Permitir conexões TCP/IP ao SQL Server. Para isso, siga as instruções neste artigo da Base de conhecimento da parte **II. Permitir conexões TCP/IP ao banco de dados SQL**.

- Para configurar, gerenciar e administrar o Microsoft SQL Server (banco de dados e usuários), faça o download do SQL Server Management Studio (SSMS).
- Não instale o SQL Server em um controlador de domínio (por exemplo, Windows SBS/Essentials). Recomendamos que instale o ESET PROTECT em outro servidor ou não selecione o componente SQL Server Express durante a instalação (isso requer que você use seu Servidor SQL ou MySQL existente para executar o banco de dados ESET PROTECT).

Instalação e configuração MySQL Server

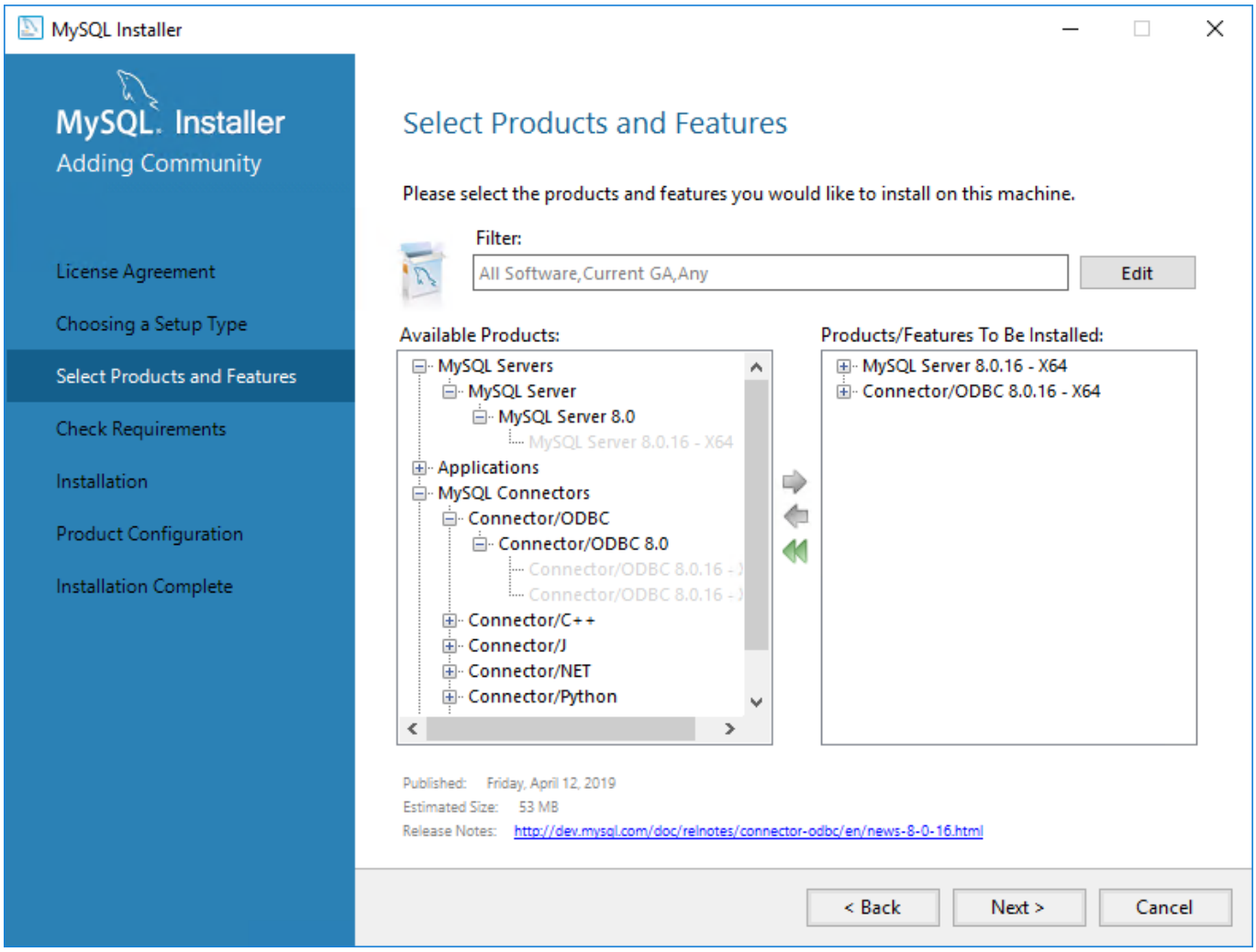
Instalação

Certifique-se de instalar uma versão compatível do MySQL Server e do Conector ODBC.

1. Faça o download do instalador do MySQL 8 Windows de https://dev.mysql.com/downloads/installer/ e execute-o.

2. Selecione a caixa de seleção **Aceito os termos de licença** e clique em **Avançar**.

3. Durante a configuração da instalação selecione **Personalizado** e selecione **MySQL Server** e **Conector/ODBC** para instalar. Certifique-se de que o Conector ODBC tem a mesma taxa de bits do MySQL Server instalado (x86 ou x64).



4. Clique em **Avançar** e **Executar** para instalar o MySQL Server e o Conector ODBC.

5. Clique em **Avançar**. Em **Alta disponibilidade**, selecione **MySQL Server autônomo/Replicação MySQL Clássica** e clique em **Avançar**.

6. Em **Tipo e rede**, selecione **Computador do servidor** no menu suspenso **Tipo de configuração** e clique em **Avançar**.

7. Em **Método de autenticação**, selecione a opção recomendada **Usar criptografia de senha forte para autenticação** e clique em **Avançar**.

8. Em **Contas e funções**, digite sua **Senha raiz MySQL** duas vezes. Recomendamos também criar uma conta de usuário de banco de dados dedicada.

9. No **Serviço do Windows**, mantenha os valores pré-selecionados e clique em **Avançar**.

10. Clique em **Executar** e aguarde até a instalação do Servidor MySQL ser concluída. Clique em **Concluir**, **Avançar** e **Concluir** para fechar a janela de instalação.

Configuração

1. Abra o arquivo a seguir em um editor de texto:

C:\ProgramData\MySQL\MySQL Server 8.0\my.ini

2. Encontre e edite ou anexe a configuração a seguir na seção `[mysqld]` do arquivo *my.ini*:

- Cria a seção `[mysqld]` se ela não estiver presente no arquivo.
- Se os parâmetros não estiverem presentes no arquivo, adicione-os à seção `[mysqld]`.
- Para determinar sua versão do MySQL, execute o comando: `mysql --version`

Parâmetro	Comentários e valores recomendados	MySQL versão
`max_allowed_packet=33M`		Todas as versões compatíveis.
`log_bin_trust_function_creators=1`	Alternativamente, é possível desativar o registro em relatório binário: `log_bin=0`	Versões 8.x compatíveis
`innodb_log_file_size=100M` `innodb_log_files_in_group=2`	A multiplicação de valores desses dois parâmetros deve ser no mínimo **200**. O valor mínimo para `innodb_log_files_in_group` é **2** e o valor máximo é **100**;, o valor também precisa ser um número inteiro.	Versões 8x compatíveis 5.7 5.6.22 (e versões posteriores 5.6.x)
`innodb_log_file_size=200M`	Defina o valor como no mínimo **200M**, mas no máximo **3000M**.	5.6.20 e 5.6.21

3. Salve e feche o arquivo *my.ini*.

4. Abra o Prompt de comando e digite o comando a seguir para reiniciar o MySQL Server e aplicar a configuração (o nome do processo depende da versão do MySQL: 8.0 = mysql80, etc.):

```
net stop mysql80
net start mysql80
```

5. Insira o seguinte comando no prompt de comando para verificar se o servidor MySQL está em execução:

```
sc query mysql80
```

Contas do usuário de banco de dados dedicado

Se você não quiser usar uma **conta SA** (Microsoft SQL) ou **conta raiz** (MySQL), você pode criar uma **conta de usuário de banco de dados dedicado**. Esta conta de usuário dedicada será usada para acessar somente o banco de dados ESET PROTECT. Recomendamos que você crie uma conta de usuário de banco de dados dedicada dentro de seu servidor de banco de dados antes de iniciar a instalação do ESET PROTECT. Além disso, você precisará criar um banco de dados vazio que será acessado pelo ESET PROTECT usando esta conta de usuário dedicada.

Há um conjunto mínimo de privilégios que devem ser concedidos a uma conta de usuário de banco de dados dedicada:

- Privilégios de usuário MySQL: `ALTER`, `ALTER ROUTINE`, `CREATE`, `CREATE ROUTINE`, `CREATE TEMPORARY TABLES`, `CREATE VIEW`, `DELETE`, `DROP`, `EXECUTE`, `INDEX`, `INSERT`, `LOCK TABLES`, `SELECT`, `UPDATE`, `TRIGGER`. – para mais informações sobre os privilégios MySQL, consulte http://dev.mysql.com/doc/refman/8.0/en/grant.html.

- Funções no nível do banco de dados Microsoft SQL Server: Um usuário do banco de dados ESET PROTECT deve ser um membro da função de banco de dados db_owner. Para obter mais informações sobre as funções no nível do banco de dados do Microsoft SQL Server, consulte https://msdn.microsoft.com/en-us/library/ms189121%28v=sql.100%29.aspx

Você pode encontrar um guia detalhado sobre como configurar seu banco de dados e conta de usuário para o Microsoft SQL e o MySQL em nosso artigo da base de conhecimento.

Instalação do Agente - Windows

Métodos disponíveis

Vários métodos de instalação estão disponíveis para instalação do Agente ESET Management em estações de trabalho Windows:

Método	Documentação	Descrição
Instalação baseada em GUI do instalador *.msi*	• Este capítulo • KB	• O método de instalação **padrão**. • Esse método pode ser executado como uma instalação auxiliada pelo servidor ou off-line. • Use esse método ao instalar o Agente na máquina do Servidor ESET PROTECT.
ESET Remote Deployment Tool	• Ajuda on-line	• Recomendado para implantação em massa em uma rede local. • Pode ser usado para o Instalador tudo-em-um (Agente + produto de segurança ESET)
Instalador tudo-em-um do Agente	• Criar um Instalador Tudo-em-um do Agente • KB	• O instalador também pode incluir um produto de segurança e uma política incorporada. • O tamanho do instalador é de várias centenas de MBs.
Script do agente instalador	• Criar instalador de script do Agente • KB	• O instalador é um script executável. Ele tem um tamanho pequeno, mas precisa acessar o local do instalador *.msi*. • O script pode ser editado para usar o instalador local e Proxy HTTP.
Instalação SCCM e GPO	• SCCM • GPO • KB	• Método avançado de instalação remota em massa. • Usando um arquivo *.ini* pequeno.
Tarefa do servidor - Instalação do Agente	• Ajuda on-line • KB	• Uma alternativa ao SCCM e GPO. • Não é viável por Proxy HTTP. • Executado pelo Servidor ESET PROTECT do console web ESET PROTECT. • Use esse método para implantar o Agente ESET Management nos computadores sincronizados do Active Directory.

O protocolo de comunicação entre o Agente e o Servidor ESET PROTECT não é compatível com a autenticação. Qualquer solução de proxy usada para encaminhar a comunicação do Agente para o Servidor ESET PROTECT e que precise de autenticação não funcionará.
Se você escolher usar uma porta não padrão para o console web ou Agente, poderá ser necessário fazer um ajuste de firewall. Caso contrário, a instalação poderá falhar.

Instalação baseada em GUI

Siga as etapas abaixo para instalar o componente do Agente ESET Management localmente no Windows:

1. Visite a seção de download ESET PROTECT para fazer download de um instalador autônomo para este componente ESET PROTECT (*agent_x86.msi* ou *agent_x64.msi* ou *agent_arm64.msi*).

2. Execute o instalador do Agente ESET Management e aceite o EULA se você concordar com ele.

3. Marque a caixa de seleção ao lado de **Participar do programa de melhoria do produto** para enviar relatórios de travamento e dados de telemetria anônimos para a ESET (versão e tipo do sistema operacional, versão do produto ESET e outras informações específicas do produto).

4. Digite o **Host do servidor** (nome de host ou endereço IP do seu Servidor ESET PROTECT) e a **porta de servidor** (a porta padrão é 2222, se você estiver usando uma porta diferente, substitua a porta padrão pelo seu número de porta personalizado).

Certifique-se de que o **Host do servidor** corresponde a pelo menos um dos valores (de preferência o FQDN) definido no campo **Host** do **Certificado do servidor**. Caso contrário, você receberá um erro dizendo "O certificado de servidor recebido não é válido". Usar o caractere coringa (*) no campo de Host do certificado do servidor vai permitir que o certificado funcione com qualquer **Host de servidor**.

5. Se você usar proxy para a conexão Agente - Servidor, selecione a caixa de seleção ao lado de **Usar Proxy**. Quando selecionada, o instalador continuará com a instalação off-line.

Essa configuração de proxy é usada apenas para (replicação) entre o Agente ESET Management e o Servidor ESET PROTECT, não para o armazenamento em cache de atualizações.
- **Nome de host do Proxy**: nome de host ou endereço IP da máquina do Proxy HTTP.
- **Porta Proxy**: o valor padrão é 3128.
- **Nome de usuário**, **Senha**: insira as credenciais usadas pelo seu proxy se ele usar autenticação.

Você pode alterar as configurações de proxy mais tarde na sua política. O Proxy deve ser instalado antes de ser possível configurar uma conexão Agente - Servidor via Proxy.

6. Selecione uma das opções de instalação a seguir e siga os passos da seção apropriada abaixo:

- Instalação auxiliada por servidor - será necessário fornecer credenciais de administrador do Console da Web ESET PROTECT. O instalador vai fazer download dos certificados necessários automaticamente.

Não é possível usar um usuário com autenticação em dois fatores para instalações auxiliadas por servidor.

- Instalação off-line - você precisará fornecer um Certificado de Agente e Autoridade de certificação. Ambos podem ser exportados do ESET PROTECT. Alternativamente, é possível usar seu certificado personalizado.

Instalação de linha de comando

O instalador *MSI* pode ser executado de maneira local ou remota. Faça download do Agente ESET Management do site da ESET.

Parâmetro	Descrição e valores permitidos
P_HOSTNAME=	Nome de host ou endereço IP do Servidor ESET PROTECT.
P_PORT=	Porta do servidor para conexão do Agente (opcional. Se não estiver especificado, a porta padrão 2222 será usada).
P_CERT_PATH=	Caminho para o Certificado do Agente em formato Base64 no arquivo *.txt* (exportado do console web ESET PROTECT).
P_CERT_AUTH_PATH=	Caminho para a Autoridade de Certificação em formato Base64 no arquivo *.txt* (exportado do console web ESET PROTECT).

Parâmetro	Descrição e valores permitidos
P_LOAD_CERTS_FROM_FILE_AS_BASE64=	**YES**; Use esse parâmetro ao fazer referência ao certificado do Agente e Autoridade de Certificação armazenados nos arquivos *.txt*.
P_CERT_PASSWORD=	Use este parâmetro para fornecer uma senha para o certificado do Agente.
P_CERT_CONTENT=	String do certificado do Agente em formato Base64 (exportada do console web ESET PROTECT).
P_CERT_AUTH_CONTENT=	String da Autoridade de Certificação em formato Base64 (exportada do console web ESET PROTECT).
PASSWORD=	Senha para desinstalação de um Agente protegido por senha.
P_ENABLE_TELEMETRY=	**0** – desativado (opção padrão); **1** – ativado. Envio de relatórios de travamento e dados de telemetria para a ESET (parâmetro opcional).
P_INSTALL_MODE_EULA_ONLY=	**1**; Use este parâmetro para a instalação semissilenciosa do Agente ESET Management. Você verá a janela de instalação do Agente e será solicitado a aceitar o Acordo de Licença para o Usuário Final e ativar/desativar a telemetria (P_ENABLE_TELEMETRY é ignorada quando especificado). Outras configurações de instalação do Agente são retiradas dos parâmetros da linha de comando. Você verá a conclusão do processo de instalação do Agente.
P_USE_PROXY=	**1**; Use este parâmetro para ativar o uso do Proxy HTTP (que já está instalado em sua rede) para replicação entre o Agente ESET Management e o Servidor ESET PROTECT (não para atualizações de cache).
P_PROXY_HTTP_HOSTNAME=	Nome de host ou endereço IP do Proxy HTTP.
P_PROXY_HTTP_PORT=	Porta do Proxy HTTP para conexão do Agente.

Exemplos de instalação da linha de comando

Substitua o código laranja abaixo conforme necessário.

- Instalação silenciosa (parâmetro `/q`) com conexão de porta padrão, telemetria ativada e certificado de Agente e Autoridade de Certificação armazenados em arquivos:

```
Agent_x64.msi /q P_HOSTNAME=10.20.30.40 P_ENABLE_TELEMETRY=1 P_CERT_PATH=C:\Users\Administrator\Desktop\certificate.txt P_CERT_AUTH_PATH=C:\Users\Administrator\Desktop\ca.txt P_LOAD_CERTS_FROM_FILE_AS_BASE64=YES
```

- Instalação silenciosa com strings fornecidas para o certificado do Agente e para a Autoridade de Certificação e senha do certificado do Agente e parâmetros do Proxy HTTP:

```
Agent_x64.msi /q P_HOSTNAME=protect_server_name P_ENABLE_TELEMETRY=1 P_CERT_CONTENT=CJfXtf1kZqlZKAl9P48HymBHa3CkW P_CERT_PASSWORD=abcd1234EFGH P_CERT_AUTH_CONTENT=45hvkpqayzjJZhSY8qswDQYJKoZIhvc P_USE_PROXY=1 P_PROXY_HTTP_HOSTNAME=proxy_server P_PROXY_HTTP_PORT=3128
```

- Instalação semissilenciosa:

```
Agent_x64.msi P_INSTALL_MODE_EULA_ONLY=1 P_HOSTNAME=10.20.30.40 P_CERT_PATH=C:\Users\Administrator\Desktop\certificate.txt P_CERT_AUTH_PATH=C:\Users\Administrator\Desktop\ca.txt P_LOAD_CERTS_FROM_FILE_AS_BASE64=YES
```

Instalação do Agente assistida pelo servidor

Para continuar com a instalação **do Agente auxiliada por servidor** siga as etapas a seguir:

1. Insira o nome de host ou endereço IP do seu console da Web ESET PROTECT (igual ao do Servidor ESET PROTECT) no campo **Host do servidor**. Deixe a **porta do console da Web** definida na porta padrão 2223 se não estiver usando uma porta personalizada. Além disso, insira as credenciais da sua conta do console da Web nos campos **Nome de usuário e Senha**. Para entrar como um usuário do domínio, selecione a caixa de seleção ao lado de **Entrar no domínio**.

- Certifique-se de que o **Host do servidor** corresponde a pelo menos um dos valores (de preferência o FQDN) definido no campo Host do **Certificado do servidor**. Caso contrário, você receberá um erro dizendo “O certificado de servidor recebido não é válido”. A única exceção é caso exista um caractere curinga (*) no campo de Host do certificado do servidor, o que significa que ele vai funcionar com qualquer **Host de servidor**.
- Não é possível usar um usuário com autenticação em dois fatores para instalações auxiliadas por servidor.

2. Clique em **Sim** quando perguntado se deseja aceitar o certificado.

3. Selecione **Não criar computador (o computador será criado automaticamente durante a primeira conexão)** ou **Escolher grupo estático personalizado**. Se clicar em **Escolher grupo personalizado estático** você será capaz de selecionar a partir de uma lista de grupos estáticos no ESET PROTECT. O computador será adicionado ao grupo selecionado.

4. Especifique uma pasta de destino para o Agente ESET Management (recomendamos usar o local padrão), clique em **Avançar** e depois em **Instalar**.

Instalação do Agente off-line

Para continuar com a **instalação do Agente off-line** siga essas etapas:

1. Se você selecionou **Usar Proxy** na etapa anterior, forneça o **nome de host do Proxy**, **porta do Proxy** (a porta padrão é 3128),**Nome de usuário** e **Senha** e clique em **Avançar**.

2. Clique em **Procurar** e vá até a localização do seu certificado de mesmo nível (este é o Certificado de Agente exportado do ESET PROTECT). Deixe o campo de texto de **Senha certificada** em branco, pois este certificado não requer senha. Você não precisa procurar uma **Autoridade de certificação** - deixe esse campo em branco.

Se estiver usando um certificado personalizado com ESET PROTECT (em vez dos modelos padrão gerados automaticamente durante a instalação do ESET PROTECT), use seus certificados personalizados de acordo.

A senha do certificado não deve ter os seguintes caracteres: " \ Esses caracteres causam um erro crítico durante a inicialização do Agente.

3. Clique em **Avançar** para instalar a pasta padrão ou clique em **Alterar** para escolher outra pasta (recomendamos usar a localização padrão).

ESET Remote Deployment Tool

O ESET Remote Deployment Tool é uma maneira conveniente de distribuir o pacote do instalador criado pelo ESET PROTECT para implantar o Agente ESET Management e os produtos de segurança ESET nos computadores de uma rede.

O ESET Remote Deployment Tool está disponível gratuitamente no site da ESET como um Componente ESET

PROTECT autônomo. A ferramenta de implantação é feita principalmente para a implantação em redes pequenas a médias e é executada com privilégios de administrador.

> A ESET Remote Deployment Tool é dedicada a implantar o Agente ESET Management apenas em computadores clientes com sistemas operacionais Microsoft Windows compatíveis.

Para obter mais detalhes sobre os pré-requisitos e o uso da ferramenta, consulte o capítulo ESET Remote Deployment Tool.

Instalação do Web Console – Windows

Você pode instalar o Web Console ESET PROTECT no Windows de duas formas:

- É recomendado usar o Instalador tudo-em-um
- Usuários avançados podem realizar uma instalação manual

> Você pode escolher instalar o Web Console ESET PROTECT em um computador diferente do computador executando o Servidor ESET PROTECT.

Instalar o Web Console usando o Instalador tudo-em-um

Pré-requisitos

- Servidor ESET PROTECT instalado.

> Você pode escolher instalar o Web Console ESET PROTECT em um computador diferente do computador executando o Servidor ESET PROTECT. Este procedimento requer etapas adicionais.

- O Apache Tomcat é um componente obrigatório necessário para executar o console web ESET PROTECT.
- O Apache Tomcat requer 64 bits Java/OpenJDK. Se você tiver várias versões do Java instaladas em seu sistema, recomendamos desinstalar as versões mais antigas do Java e manter apenas a versão mais recente do Java compatível.

> A partir de janeiro de 2019, atualizações públicas do Oracle JAVA SE 8 para uso de negócios, comercial ou de produção precisarão de uma licença comercial. Se você não comprar uma assinatura JAVA SE, você pode usar este guia para mudar para uma alternativa sem custos. Consulte as versões compatíveis do JDK.

Instalação

Para instalar o componente Web Console ESET PROTECT no Windows usando o Instalador tudo-em-um:

> Certifique-se de atender a todos os pré-requisitos de instalação listados acima.

1. Faça o download do Instalador tudo-em-um ESET PROTECT do site da ESET e descompacte o arquivo

baixado.

2. Se quiser instalar a versão mais recente do Apache Tomcat e o Instalador tudo-em-um contém uma versão mais antiga do Apache Tomcat (esta etapa é opcional, pule para a etapa 4 se você não precisar da versão mais recente do Apache Tomcat):

a.Abra a pasta *x64* e navegue até a pasta *installers*.

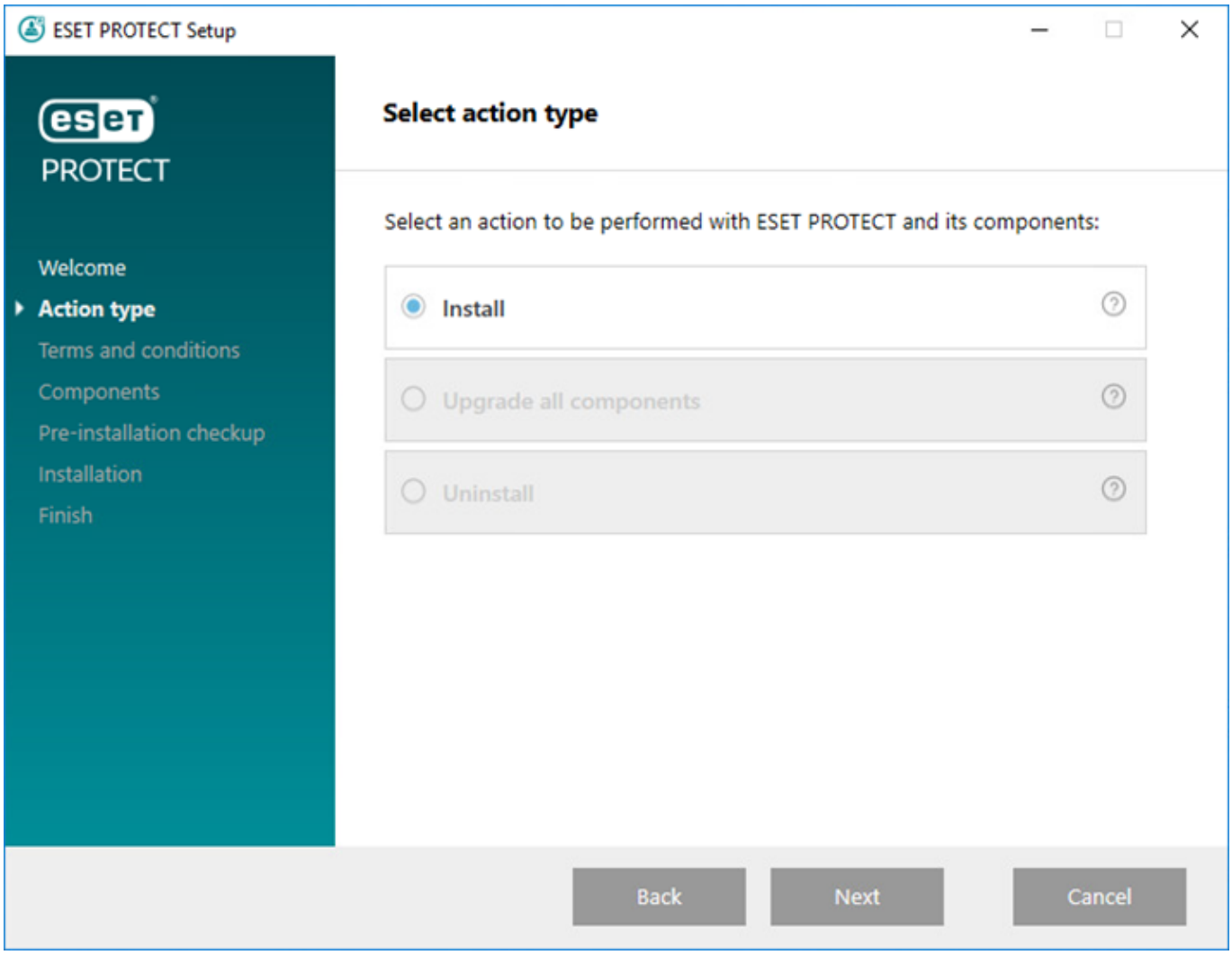
b.Remova o arquivo *apache-tomcat-9.0.x-windows-x64.zip* localizado na pasta *installers*.

c.Faça o download do Apache Tomcat 9 pacote zip para Windows 64 bits.

d.Mova o pacote zip do download para a pasta *installers*.

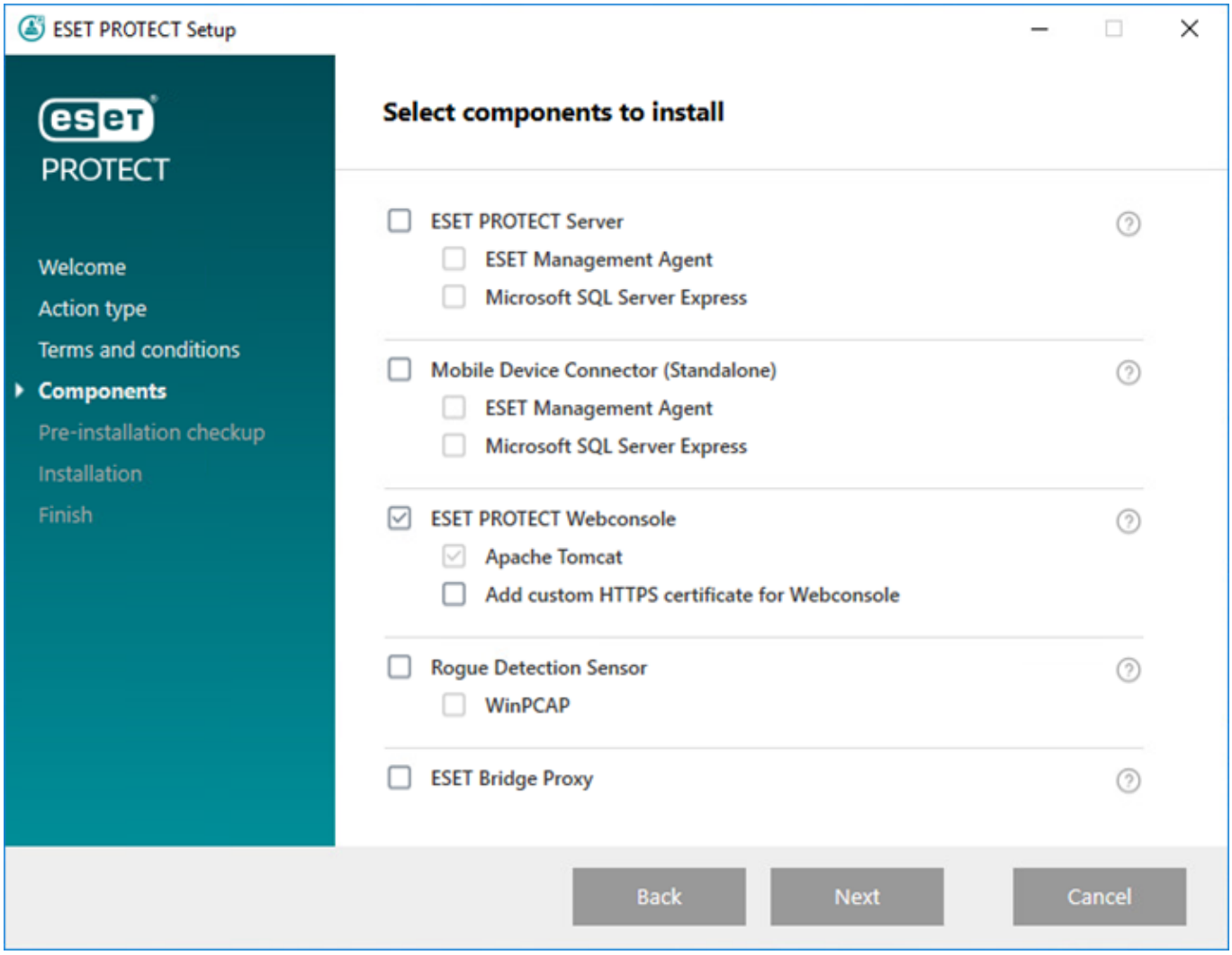
3. Para iniciar o Instalador tudo-em-um, clique duas vezes no arquivo *Setup.exe*, clique em **Avançar** na tela **Bem-vindo**.

4. Selecione **Instalar** e clique em **Avançar**.



5. Depois de aceitar o EULA, clique em **Avançar**.

6. Em **Selecione os componentes a serem instalados**, selecione a caixa de seleção **Web Console ESET PROTECT** e clique em **Avançar**.

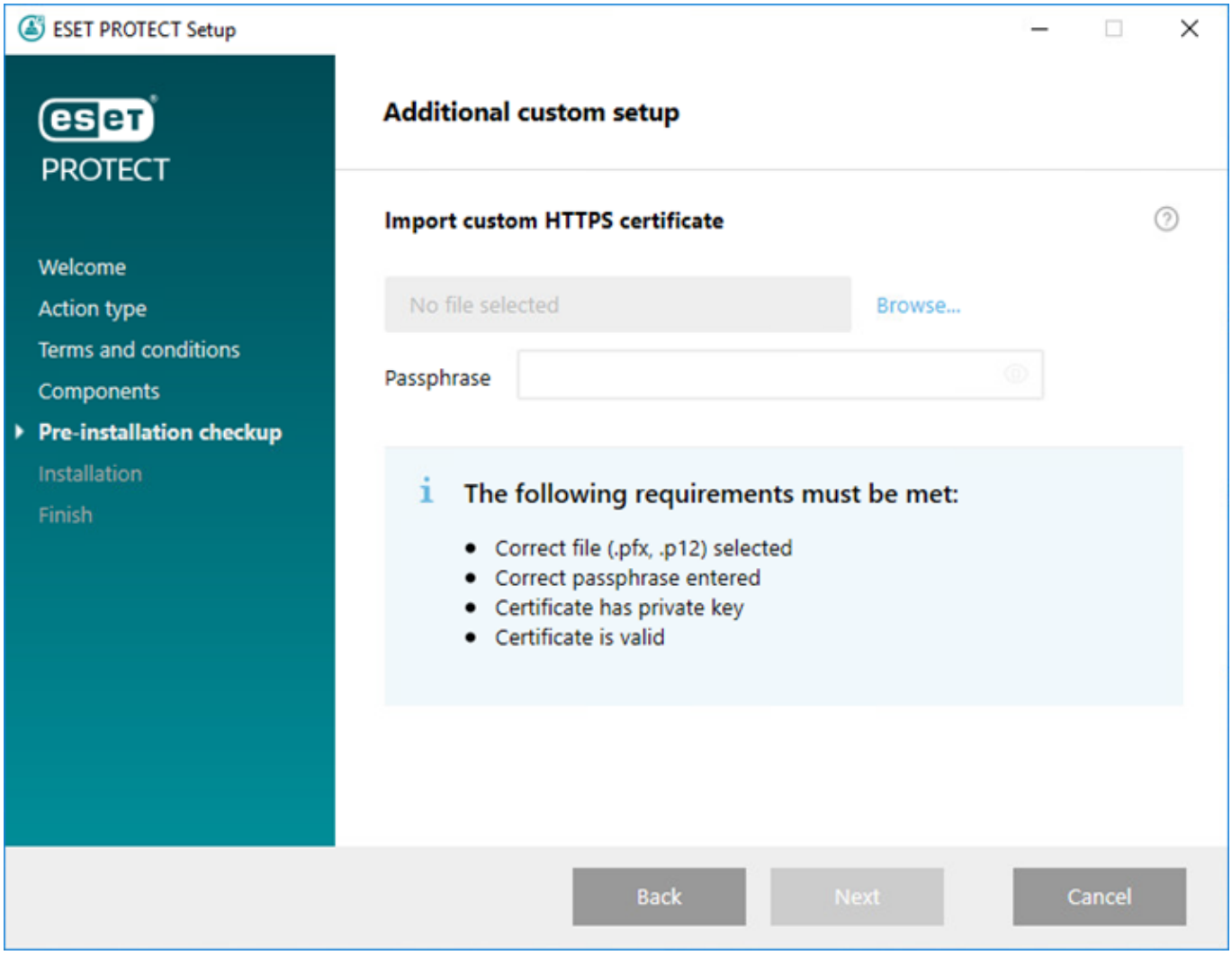


Opcionalmente, selecione a caixa de seleção **Adicionar certificado HTTPS personalizado para o Web Console**.

- Selecione esta opção se quiser usar um certificado HTTPS personalizado para o console web ESET PROTECT.

- Se você não selecionar essa opção, o instalador gera automaticamente um novo keystore para o Tomcat (um certificado auto-assinado HTTPS).

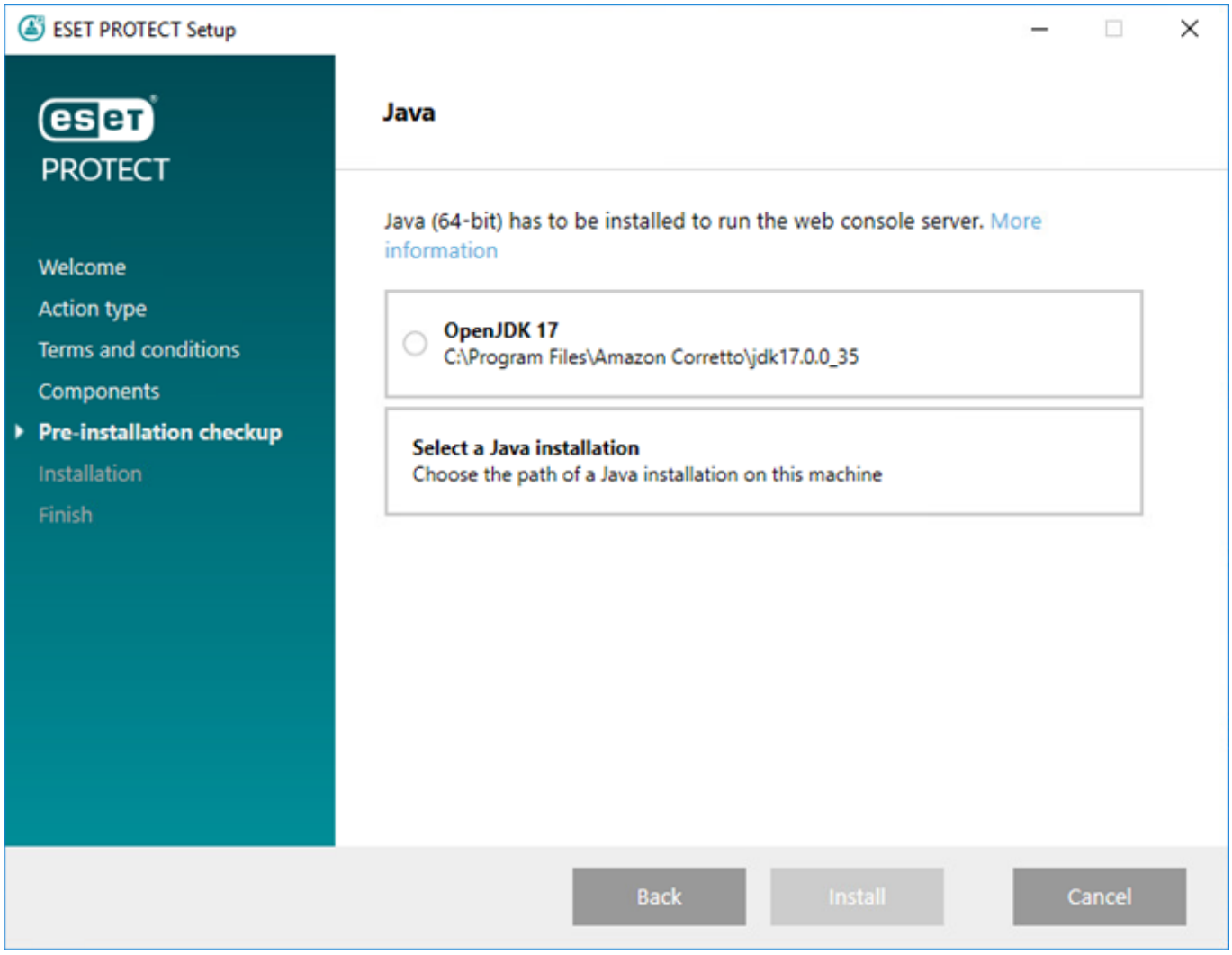
- Se você selecionou **Adicionar certificado HTTPS personalizado para o console web**, clique em **Procurar** e selecione um Certificado válido (*.pfx* ou arquivo .p12) e digite sua **Senha** (ou deixe o campo em branco, se não houver senha). O instalador vai instalar o certificado de acesso ao Web Console no seu servidor Tomcat. Clique em **Avançar** para continuar.



7. Selecione uma instalação Java no computador. Certifique-se de estar usando a versão mais recente do Java/OpenJDK.

a)Para selecionar o Java já instalado, clique em **Selecionar uma instalação Java**, selecione a pasta onde o Java está instalado (com uma subpasta *bin*, por exemplo *C:\Program Files\Amazon Corretto\jdk1.8.0_212*) e clique em **OK**. O instalador informará se você tiver selecionado um caminho inválido.

b)Clique em **Instalar** para continuar ou **alterar** para alterar o caminho de instalação do Java.



8. Quando a instalação estiver concluída, clique em **Concluir**.

Se você instalou o console web ESET PROTECT em um computador diferente do Servidor ESET PROTECT, realize essas etapas adicionais para permitir a comunicação entre o console web ESET PROTECT e o Servidor ESET PROTECT:
a)Interrompa o serviço Apache Tomcat: Vá para **Início** > **Serviços** > clique com o botão direito no serviço Apache Tomcat e selecione **Parar**.
b)Execute o Bloco de notas como Administrador e edite o *C:\Program Files\Apache Software Foundation\[Tomcat pasta]\webapps\era\WEB-INF\classes\sk\eset\era\g2webconsole\server\modules\config\EraWebServerConfig.properties*.
c)Encontre o `server_address=localhost`.
d)Substitua `localhost` com o endereço IP do seu Servidor ESET PROTECT e salve o arquivo.
e) Reinicie o serviço Apache Tomcat: Vá para **Início** > **Serviços** > clique com o botão direito no serviço Apache Tomcat e selecione **Iniciar**.

9. Abra o Web Console ESET PROTECT em um navegador da web compatível, uma tela de login será exibida.

- Do computador hospedando o Web Console ESET PROTECT: *https://localhost/era*

- De qualquer computador com acesso à Internet ao Web Console ESET PROTECT (substitua *IP_ADDRESS_OR_HOSTNAME* pelo endereço IP ou nome de host do seu Web Console ESET PROTECT): *https://IP_ADDRESS_OR_HOSTNAME/era*

Veja também a configuração adicional do Web Console para soluções empresariais ou para sistemas de baixo desempenho.

Instalar o Web Console manualmente

A instalação manual do Web Console ESET PROTECT é um procedimento avançado. Recomendamos que você instale o Web Console ESET PROTECT usando o Instalador tudo-em-um.

Pré-requisitos

- Servidor ESET PROTECT instalado.

Você pode escolher instalar o Web Console ESET PROTECT em um computador diferente do computador executando o Servidor ESET PROTECT. Este procedimento requer etapas adicionais.

- O Apache Tomcat é um componente obrigatório necessário para executar o console web ESET PROTECT. Instalar o Apache Tomcat:

  a)Faça o download da versão compatível mais recente do arquivo instalador Apache Tomcat (Instalador de serviço Windows 32 bits/64 bits) *apache-tomcat-[versão].exe* de https://tomcat.apache.org.

  b)Execute o instalador.

  c)Durante a instalação, selecione o caminho para Java (pasta pai das pastas Java *bin* e *lib*) e selecione a caixa de marcação **Run Apache Tomcat**.

  d)Depois da instalação, certifique-se de que o serviço Apache Tomcat está em execução e que o tipo de inicialização está configurado como **Automático** (em **services.msc**).

- O Apache Tomcat requer 64 bits Java/OpenJDK. Se você tiver várias versões do Java instaladas em seu sistema, recomendamos desinstalar as versões mais antigas do Java e manter apenas a versão mais recente do Java compatível.

A partir de janeiro de 2019, atualizações públicas do Oracle JAVA SE 8 para uso de negócios, comercial ou de produção precisarão de uma licença comercial. Se você não comprar uma assinatura JAVA SE, você pode usar este guia para mudar para uma alternativa sem custos. Consulte as versões compatíveis do JDK.

Instalação

Para instalar o componente Console da web ESET PROTECT no Windows, siga as etapas abaixo:

Certifique-se de atender a todos os pré-requisitos de instalação listados acima.

1. Visite a seção de download ESET PROTECT para fazer download de um instalador autônomo para este componente ESET PROTECT (Web Console*era.war*).

2. Copie *era.war* para a pasta de aplicativos da web do Apache Tomcat:

C:\Program Files\Apache Software Foundation\[Tomcat pasta]\webapps

3. O Apache Tomcat extrai automaticamente o arquivo *era.war* na pasta *era* e instala o Web Console ESET PROTECT. Aguarde alguns minutos até a extração ser concluída. Se a extração não acontecer, siga as etapas da solução de problemas.

4. Se você instalou o Web Console ESET PROTECT no mesmo computador que o Servidor ESET PROTECT, reinicie o serviço Apache Tomcat. Vá para **Início** > **Serviços** > clique com o botão direito no serviço Apache Tomcat e selecione **Parar**. Clique em Parar, espere 30 segundos e depois clique em **Iniciar**.

Se você instalou o console web ESET PROTECT em um computador diferente do Servidor ESET PROTECT, realize essas etapas adicionais para permitir a comunicação entre o console web ESET PROTECT e o Servidor ESET PROTECT:
a)Interrompa o serviço Apache Tomcat: Vá para **Início** > **Serviços** > clique com o botão direito no serviço Apache Tomcat e selecione **Parar**.
b)Execute o Bloco de notas como Administrador e edite o *C:\Program Files\Apache Software Foundation\[Tomcat pasta]\webapps\era\WEB-INF\classes\sk\eset\era\g2webconsole\server\modules\config\EraWebServerConfig.properties*.
c)Encontre o `server_address=localhost`.
d)Substitua `localhost` com o endereço IP do seu Servidor ESET PROTECT e salve o arquivo.
e) Reinicie o serviço Apache Tomcat: Vá para **Início** > **Serviços** > clique com o botão direito no serviço Apache Tomcat e selecione **Iniciar**.

5. Abra o Web Console ESET PROTECT em um navegador da web compatível para ver uma tela de login:

- Do computador hospedando o Web Console ESET PROTECT: *http://localhost:8080/era*

- De qualquer computador com acesso à Internet ao Web Console ESET PROTECT (substitua *IP_ADDRESS_OR_HOSTNAME* pelo endereço IP ou nome de host do seu Web Console ESET PROTECT): *http://IP_ADDRESS_OR_HOSTNAME:8080/era*

6. Configurar o Web Console depois da instalação:

- A porta HTTP padrão é configurada no 8080 durante a instalação manual do Apache Tomcat. Recomendamos configurar uma conexão HTTPS para Apache Tomcat.

- Veja também a configuração adicional do Web Console para soluções empresariais ou para sistemas de baixo desempenho.

Instalação do Sensor RD – Windows

Pré-requisitos

- WinPcap – use a versão mais recente do WinPcap (4.1.0 e versões posteriores)

- A rede deve ser configurada adequadamente (portas adequadas abertas, comunicação de entrada não sendo bloqueada por um firewall, etc.)

- O servidor ESET PROTECT está acessível

- O Agente ESET Management deve estar instalado no computador local para oferecer suporte total a todos os recursos do programa.

Se houver vários segmentos de rede, o Rogue Detection Sensor deve ser instalado separadamente em cada segmento de rede para produzir uma lista abrangente de todos os dispositivos em toda a rede.

Instalação

Siga as etapas abaixo para instalar o componente do Sensor RD no Windows:

Certifique-se de atender a todos os pré-requisitos de instalação listados acima.

1. Visite a seção de download ESET PROTECT para fazer download de um instalador autônomo para este componente ESET PROTECT (*rdsensor_x86.msi* ou *rdsensor_x64.msi*).

2. Clique duas vezes no arquivo do instalador do Sensor RD para iniciar a instalação.

3. Aceite o EULA e clique em **Avançar**.

4. Marque a caixa de seleção ao lado de **Participar do programa de melhoria do produto** para enviar relatórios de travamento e dados de telemetria anônimos para a ESET (versão e tipo do sistema operacional, versão do produto ESET e outras informações específicas do produto).

5. Selecione o local de instalação do RD Sensor e clique em **Avançar** > **Instalar**.

6. O ESET Rogue Detection Sensor será iniciado depois da instalação ser concluída.

Você pode encontrar o arquivo de relatório do Rogue Detection Sensor nos Arquivos de relatório:
C:\ProgramData\ESET\Rogue Detection Sensor\Logs

Ferramenta de imagem – Windows

Você é um usuário do Linux?

A ferramenta de imagem é necessária para atualizações off-line do mecanismo de detecção. Se os computadores do cliente não tiverem uma conexão à Internet e precisarem de atualizações do mecanismo de detecção, você pode usar a ferramenta de imagem para fazer download de arquivos de atualização dos servidores de atualização ESET e armazená-los localmente.

A Ferramenta de imagem tem as funções a seguir:
• Atualizações de módulo – faz o download de atualizações do mecanismo de detecção e outros módulos de programa, mas não das atualizações automáticas (uPCU).
• Criação do repositório – pode criar um repositório off-line completo, incluindo atualizações automáticas (uPCU).
A Ferramenta de imagem não faz download de dados do ESET LiveGrid®.

Pré-requisitos

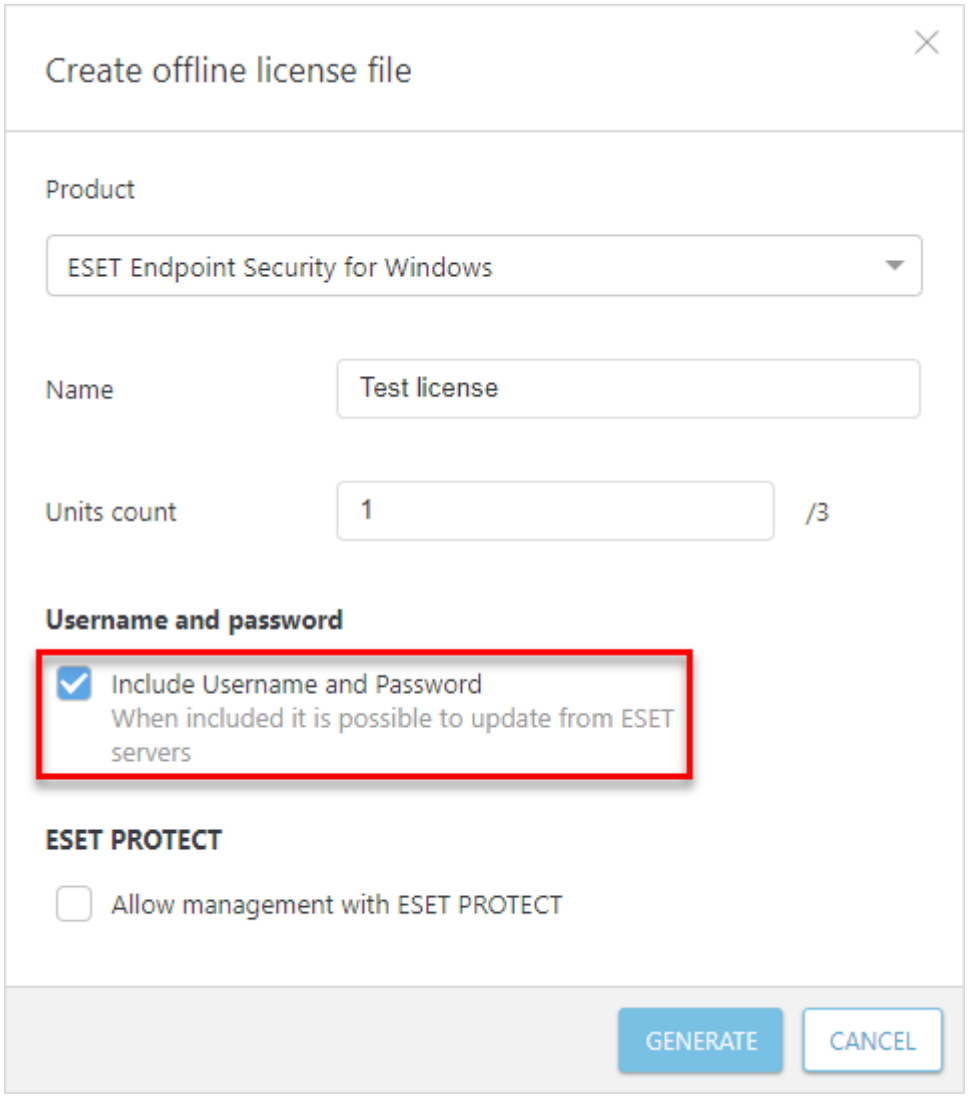
A ferramenta de imagem não é compatível com o Windows XP e Windows Server 2003.

• A pasta de destino deve estar disponível para compartilhamento, serviço Samba/Windows ou HTTP/FTP, dependendo de como você quer que as atualizações sejam acessíveis.

oProdutos de Segurança ESET para Windows – podem ser atualizados remotamente usando HTTP ou uma pasta compartilhada.

- Produtos de Segurança ESET para Linux/macOS – podem ser atualizados remotamente apenas usando o HTTP. Se você usar uma pasta compartilhada, ela deve estar no mesmo computador que o produto de segurança ESET.

- Você deve ter um arquivo de Licença off-line válido incluindo o Nome de usuário e Senha. Ao gerar um arquivo de licença, certifique-se de selecionar a caixa de seleção ao lado de **Incluir Nome de Usuário e Senha**. Além disso, você deve digitar um **Nome** de licença. Um arquivo de licença off-line é necessário para a ativação da ferramenta de imagem e para gerar a imagem de atualização.



- Antes de executar a Ferramenta de imagem, será preciso ter os pacotes a seguir instalados:
- Visual C++ Redistributable for Visual Studio 2010
- Visual C++ 2015 Redistributable x86

Como usar a Ferramenta de imagem

1.Faça o download da Ferramenta de imagem da página de download ESET (seção de **Instaladores autônomos**).

2.Descompacte o arquivo do download.

3.Abra o Prompt de comando e vá até a pasta com o arquivo *MirrorTool.exe*.

4.Execute o comando abaixo para ver todos os parâmetros disponíveis para a Ferramenta de imagem e sua versão:

```
MirrorTool.exe --help
```

```
C:\Users\                    >MirrorTool.exe --help
Mirror Tool v1.0.1294.0, Copyright (c) ESET, spol. s r.o. 1992-2021. All rights
reserved.
Allowed options:
  --mirrorType arg                      [required for module update]
                                        Type of mirror. Possible values (case
                                        insensitive): regular, pre-release,
                                        delayed.
  --intermediateUpdateDirectory arg     [required for module update]
                                        Files will be downloaded to this
                                        directory to create mirror in output
                                        directory.
  --offlineLicenseFilename arg          [required for module update]
                                        Offline license file.
  --updateServer arg                    [optional]
                                        Update server. (e.g.:
                                        http://update.eset.com/eset_upd/ep6/)
                                        Mirror will be created in output
                                        directory, only specified path in
                                        server will be mirrored.
  --outputDirectory arg                 [required for module update]
                                        Directory where mirror will be created.
  --proxyHost arg                       [optional]
                                        Http proxy address (fqdn or IP).
  --proxyPort arg                       [optional]
                                        Http proxy port.
  --proxyUsername arg                   [optional]
                                        Http proxy username.
  --proxyPassword arg                   [optional]
                                        Http proxy password.
  --networkDriveUsername arg            [optional]
                                        Username used, when output directory is
                                        accessed using smb(e.g:\\hostname).
  --networkDrivePassword arg            [optional]
                                        Password used, when output directory is
                                        accessed using smb(e.g:\\hostname).
  --excludedProducts arg                [optional]
                                        Disable creating mirror for specified
                                        products. Use --listUpdatableProducts
                                        to see possible values.
  --listUpdatableProducts               Show list of all products which modules
                                        are downloaded by default.
  --repositoryServer arg                [required for repository update]
                                        Repository server for repository
                                        creation.
  --intermediateRepositoryDirectory arg [required for repository update]
                                        Files will be downloaded to this
                                        directory to create offline mirror in
                                        output directory.
  --outputRepositoryDirectory arg       [required for repository update]
                                        Directory where offline repository will
                                        be created.
  --trustDownloadedFilesInRepositoryTemp
                                        [optional]
                                        If set, hashes on already downloaded
                                        files are not checked.
  --mirrorOnlyLevelUpdates              [optional]
                                        If set, only level upgrades will be
                                        downloaded (nano/continuous updates
                                        will not be downloaded)
  --mirrorFileFormat arg                [optional]
                                        Specifies which type of update files
                                        will be downloaded. Possible values
                                        (case insensitive): dll, dat.
  --compatibilityVersion arg            [optional]
                                        Version of compatible products.
  --filterFilePath arg                  [optional]
                                        Path to filter file in json format.
                                        Parameter compatibilityVersion has to
                                        be higher than 7.1.0.0 to run program.
  --dryRun arg                          [optional]
                                        Specifies dry run of program with path
                                        to csv file where will be saved list of
                                        products to be downloaded with current
                                        filter configuration.
  --help                                [optional]
                                        Display this help and exit
```

Todos os filtros diferenciam maiúsculas e minúsculas.

Você pode usar os parâmetros para criar a imagem do repositório ou a imagem dos módulos:

Parâmetros para as imagens do repositório e dos módulos

--proxyHost
--proxyPort
--proxyUsername
--proxyPassword
--help

Parâmetros específicos do repositório

--repositoryServer
--intermediateRepositoryDirectory
--outputRepositoryDirectory
--compatibilityVersion
--dryRun
--filterFilePath
--trustDownloadedFilesInRepositoryTemp

Parâmetros específicos dos módulos

--mirrorType
--intermediateUpdateDirectory
--offlineLicenseFilename
--updateServer
--outputDirectory
--networkDriveUsername
--networkDrivePassword
--excludedProducts
--listUpdatableProducts
--mirrorOnlyLevelUpdates
--mirrorFileFormat

Parâmetro	Descrição
--updateServer	A Mirror Tool cria uma estrutura de pastas diferente da que é criada pela imagem do Endpoint. Cada pasta guarda arquivos de atualização para um grupo de produtos. Você precisa especificar o link completo do servidor de atualização (caminho completo para a pasta correta) nas configurações de atualização do produto usando a imagem.

Parâmetro	Descrição
`--offlineLicenseFilename`	Você deve especificar um caminho para o arquivo de licença off-line (como mencionado acima).
`--mirrorOnlyLevelUpdates`	Nenhum argumento é necessário. Se estiver definido, será feito o download apenas das atualizações de nível (o download de atualizações nano não será feito). Leia mais sobre os tipos de atualização em nosso artigo da Base de conhecimento.
`--mirrorFileFormat`	Antes de usar o parâmetro `--mirrorFileFormat`, certifique-se de que o ambiente não contém as versões mais antigas (6.5 e versões anteriores) e mais recentes (6.6 e versões mais recentes) do produto de segurança ESET. O uso incorreto deste parâmetro pode resultar em atualizações incorretas de seus produtos de segurança ESET. Você pode especificar de qual tipo de arquivos de atualização será feito o download. Valores possíveis (diferencia maiúsculas de minúsculas): • `dat` – Use este valor se você tiver um ambiente apenas com versões de produto de segurança ESET da versão 6.5 e versões anteriores. • `dll` – Use este valor se você tiver um ambiente apenas com versões de produto de segurança ESET da versão 6.6 e versões posteriores. O parâmetro é ignorado ao criar uma imagem para produtos legados (`ep4`, `ep5`).
`--compatibilityVersion`	Este parâmetro opcional se aplica à Ferramenta de imagem distribuída com o ESET PROTECT 8.1 e versões posteriores. A Ferramenta de imagem vai fazer download de arquivos de atualização compatíveis com a versão do repositório ESET PROTECT que você especificar no argumento de parâmetro no formato `x.x` ou `x.x.x.x`, por exemplo: `--compatibilityVersion 10.1` ou `--compatibilityVersion 8.1.13.0`. O parâmetro `-compatibilidadeVersion` exclui as atualizações automáticas (uPCU) da imagem. Se você precisar das atualizações automáticas (uPCU) em seu ambiente e quiser diminuir o tamanho da imagem, use o parâmetro `--filterFilePath`.

Para reduzir a quantidade de dados com dowload feito do repositório ESET, recomendamos usar os novos parâmetros na Ferramenta de imagem distribuídos com o ESET PROTECT 9: `--filterFilePath` e `--dryRun`:
1.Crie um filtro em um formato *JSON* (veja `--filterFilePath` abaixo).
2.Realize um teste da Ferramenta de imagem com o parâmetro `--dryRun` (veja abaixo) e ajuste o filtro conforme necessário.
3.Execute a Ferramenta de imagem com o parâmetro `--filterFilePath` e o filtro de download definido, junto com os parâmetros `--intermediateRepositoryDirectory` e `--outputRepositoryDirectory`.
4.Execute a Ferramenta de imagem regularmente para sempre usar os instaladores mais recentes.

Parâmetro	Descrição

`--filterFilePath`	Use este parâmetro opcional para filtrar os produtos de segurança ESET com base em um arquivo de texto no formato *JSON* colocado na mesma pasta que a Ferramenta de imagem, por exemplo: `--filterFilePath filter.txt`)
	Descrição de configuração do filtro:
	O formato de arquivo de configuração para filtragem de produto é *JSON* com a estrutura a seguir:
	• objeto de raiz *JSON*:
	o`use_legacy` (booleano, opcional) – se for verdadeiro, os produtos legado serão incluídos.
	o`defaults` (objeto *JSON*, opcional) – define as propriedades de filtro que serão aplicadas a todos os produtos.
	■`languages` (lista) – especifica os códigos de idioma ISO dos idiomas a incluir, por exemplo, `"fr_FR"` para o tipo francês. Outros códigos de linguagem estão na tabela abaixo. Para selecionar mais linguagens, separe-as com uma vírgula e um espaço, por exemplo: (`["en_US", "zh_TW", "de_DE"]`)
	■`platforms` (lista) - plataformas a incluir (`["x64", "x86", "arm64"]`).
	⚠ Use o filtro `platforms` com cuidado. Por exemplo, se a Ferramenta de imagem fazer download de apenas instaladores de 64 bits e houver computadores de 32 bits na sua infraestrutura, os produtos de segurança ESET de 64 bits não serão instalados em computadores de 32 bits.
	■`os_types` (lista) – tipos de sistema operacional a incluir (`["windows"]`, `["linux"]`, `["mac"]`).
	o`products` (lista de objetos JSON, opcional) – filtros a aplicar em produtos específicos – anulam o `defaults` para produtos especificados. Os objetos têm as propriedades a seguir:
	■`app_id` (string) - necessário se `name` não estiver especificado.
	■`name` (string), necessário se `app_id` não estiver especificado.
	■`version` (string) - especifica a versão ou intervalo de versões a incluir.
	■`languages` (lista) - códigos de idioma ISO dos idiomas a incluir (consulte a tabela abaixo).
	■`platforms` (lista) - plataformas a incluir (`["x64", "x86", "arm64"]`).
	■`os_types` (lista) – tipos de sistema operacional a incluir (`["windows"]`, `["linux"]`, `["mac"]`).
	ℹ Para determinar os valores apropriados para os campos, execute a Ferramenta de imagem no modo de operação seca e encontre o produto relevante no arquivo CSV criado.
	Descrição do formato da string da versão
	Todos os números de versão são compostos por quatro números separados por pontos (por exemplo, `7.1.0.0`). Você pode especificar menos números ao escrever filtros de versão (por exemplo `7.1`) e o resto dos números será zero (`7.1` é igual a `7.1.0.0`).
	A string de versão pode ter um dos dois formatos a seguir:
	• [>|<|>=|<=|=]<n>.(<n>.(<n>.(<n>)))
	oSeleciona versões maiores/menores ou iguais/menores ou iguais/iguais do que a versão especificada.
	• <n>.(<n>.(<n>.(<n>))) - <n>.(<n>.(<n>.(<n>)))
	oSeleciona versões que são maiores que ou iguais ao limite inferior e menores que ou iguais ao limite superior.
	As comparações são feitas numericamente em cada parte do número da versão, da esquerda para a direita.
	Exemplo JSON
	✓
	`{`
	`"use_legacy": true,`
	`"defaults": {`
	`"languages": [ "en_US" ],`
	`"platforms": [ "x64", "x86" ]`
	`},`
	`"products": [`
	`{`
	`"app_id": "com.eset.apps.business.ees.windows",`
	`"version": "7.1.0.0–8.0.0.0"`
	`},`
	`{`
	`"app_id": "com.eset.apps.business.eea.windows",`
	`"version": ">7.1.0.0"`
	`}`
	`]`
	`}`
	O parâmetro `--filterFilePath` substitui os parâmetros `--languageFilterForRepository`, `--productFilterForRepository` e `--downloadLegacyForRepository` usados nas versões mais antigas da Ferramenta de imagem (lançadas com ESET PROTECT 8.x).

Parâmetro	Descrição
`--dryRun`	Quando você usa esse parâmetro opcional, a Ferramenta de imagem não vai fazer download de nenhum arquivo, mas vai gerar um arquivo *.csv* listando todos os pacotes que serão baixados. Você pode usar esse parâmetro sem os parâmetros obrigatórios `--intermediateRepositoryDirectory` e `--outputRepositoryDirectory`, por exemplo: • Windows: `MirrorTool.exe --repositoryServer AUTOSELECT --dryRun test.csv` • Linux: `sudo ./MirrorTool --repositoryServer AUTOSELECT --dryRun test.csv` ℹ Alguns instaladores da ESET são genéricos para o idioma (com o código de idioma `multilang`) e a Ferramenta de imagem vai listar esses instaladores no arquivo *.csv* mesmo se você especificar `idiomas` no `--filterFilePath`. Se você usar o parâmetro `--dryRun` e também os parâmetros `--intermediateRepositoryDirectory` e `--outputRepositoryDirectory`, a Ferramenta de imagem não limpa o *outputRepositoryDirectory*.
`--listUpdatableProducts`	Liste todos os produtos ESET para os quais o Mirror Tool pode fazer download de atualizações de módulo (a menos que o `--excludedProducts` que seja usado). O parâmetro está disponível a partir das versões Mirror Tool: 1.0.1294.0 (Windows), 1.0.2226.0 (Linux).

Estrutura da pasta da Mirror Tool

Por padrão, se você não especificar o parâmetro `--updateServer`, a Mirror Tool criará essa estrutura de pasta no seu servidor HTTP:

Não usar um servidor de imagem apenas HTTP

Certifique-se de que o servidor de imagem local usa os protocolos HTTP e HTTPS ou apenas HTTPS. Se o servidor de imagem usar apenas o HTTP, você não poderá usar a tarefa de cliente de Instalação de software porque o Acordo de Licença para o Usuário Final do produto de segurança ESET não pode ser recuperado de um servidor HTTP.

Pastas padrão da Mirror Tool	Produto de Segurança ESET	Servidor de atualização (de acordo com a localização raiz do seu servidor HTTP)
mirror/eset_upd/era6	A pasta de imagem *era6* é comum para as soluções de gerenciamento remoto da ESET: ERA 6, ESMC 7 e ESET PROTECT.	Para atualizar o ESET PROTECT 10.1 da imagem, defina o servidor de atualização como *http://your_server_address/mirror/eset_upd/era6*
mirror/eset_upd/ep[versão]	ESET Endpoint Antivirus/Security versão 6.x (e versões posteriores) para Windows. Cada versão principal tem sua pasta, por exemplo, *ep10* para a versão 10.x.	*http://your_server_address/mirror/eset_upd/ep10* (um exemplo para a versão 10.x)
mirror/eset_upd/v5	ESET Endpoint Antivirus/Security versão 5.x para Windows	*http://your_server_address/mirror/eset_upd/v5*

Produtos de Segurança ESET Linux/macOS

Você deve especificar o parâmetro `--updateServer` e criar pastas adicionais para atualizar os produtos de segurança ESET para Linux/macOS da imagem HTTP (veja abaixo).

--updateServer	Pasta adicional da Mirror Tool	Produto de Segurança ESET	Servidor de atualização (de acordo com a localização raiz do seu servidor HTTP)
http://update.eset.com/eset_upd/businesslinux	*mirror/eset_upd/*BusinessLinux	ESET Endpoint Antivirus para Linux	*http://your_server_address/mirror/eset_upd/BusinessLinux*
http://update.eset.com/eset_upd/serverlinux	*mirror/eset_upd/*LinuxServer	ESET Server Security para Linux	*http://your_server_address/mirror/eset_upd/LinuxServer*
http://update.eset.com/eset_upd/businessmac	*mirror/eset_upd/*BusinessMac	ESET Endpoint Security; versão 7.x+ para macOS	*http://your_server_address/mirror/eset_upd/BusinessMac*

Tabela de códigos de idioma

Para criar uma imagem, execute a Ferramenta de imagem com pelo menos os parâmetros mínimos necessários. Veja um exemplo:

```
MirrorTool.exe --mirrorType regular ^
--intermediateUpdateDirectory c:\temp\mirrorTemp ^
--offlineLicenseFilename c:\temp\offline.lf ^
--outputDirectory c:\temp\mirror
```

Aqui está um exemplo de configuração mais avançada para um repositório off-line com os produtos selecionados, idiomas e download de arquivos legado ativado definidos no arquivo *filter.txt* (veja o exemplo de conteúdo do arquivo nos detalhes do `--filterFilePath` acima):

```
MirrorTool.exe --repositoryServer AUTOSELECT ^
--intermediateRepositoryDirectory c:\temp\repoTemp ^
--outputRepositoryDirectory c:\temp\repository ^
--filterFilePath filter.txt
```

Ferramenta de imagem e Configurações de atualização

- Para automatizar o download das atualizações de módulo, você pode criar um cronograma para executar a Ferramenta de imagem. Para fazer isso, abra seu console da Web e vá para **Tarefas de clientes** > **Sistema Operacional** > **Executar comando. Selecione** a **Linha de comando para execução** (incluindo um caminho para o *MirrorTool.exe*) e um acionador razoável (como o Cron para cada hora 0 0 * * * ? *). Alternativamente, você

pode usar o Agendador de Tarefas do Windows ou `Cron` no Linux.

- Para configurar atualizações em um computador do cliente, crie uma nova política e configure **Servidor de Atualização** para apontar para o endereço da imagem ou pasta compartilhada.

Se você estiver usando um servidor de imagem HTTPS, será preciso importar seu certificado para o armazenamento de raiz confiável na máquina do cliente. Consulte Instalação do certificado raiz confiável no Windows.

Leia este artigo da Base de conhecimento para configurar o encadeamento da Ferramenta de imagem (configurar a Ferramenta de imagem para fazer download de atualizações de outra Ferramenta de imagem).

Instalação do conector de dispositivo móvel – Windows

O componente do Gerenciamento de dispositivo móvel/Conector ESET PROTECT (MDM/MDC) (apenas no local) teve seu fim da vida útil agendado. Ler mais. Recomendamos que você migre para o gerenciamento de dispositivo móvel em nuvem.

O Conector de dispositivo móvel deve ser acessível da internet de forma que os dispositivos móveis possam ser gerenciados em todos os momentos independentemente da sua localização.

Recomendamos que você instale seu componente MDM em um dispositivo host separado daquele que é o host do Servidor ESET PROTECT.

Siga as etapas abaixo para instalar o componente do Mobile Device Connector para ESET PROTECT Server no Windows:

Certifique-se de atender a todos os pré-requisitos de instalação.

1. Visite a seção de download ESET PROTECT para fazer download de um instalador autônomo para este componente ESET PROTECT (*mdmcore_x64.msi*).

2. Execute o instalador do Conector de dispositivo móvel e aceite o EULA se você concordar com ele.

3. Clique em **Procurar**, navegue até a localização do seu certificado SSL para comunicação via HTTPS, digite a senha para este certificado.

4. Especificar **Nome do host de MDM**: é o domínio público ou endereço IP público do seu servidor MDM na forma como ele é acessível por dispositivos móveis da Internet.

O nome de host MDM deve ser digitado da mesma forma que está especificado no seu **certificado de Servidor HTTPS**, caso contrário o dispositivo móvel iOS vai se recusar a instalar o perfil MDM. Por exemplo, se houver um endereço IP especificado no certificado HTTPS, digite este endereço IP no campo de **nome de host MDM**. Caso o FQDN seja especificado (por exemplo `mdm.mycompany.com`) no certificado HTTPS, insira este FQDN no campo **nome de host MDM**. Além disso, se um coringa * for usado (por exemplo, `*.mycompany.com`) no certificado HTTPS, você pode usar `mdm.mycompany.com` no campo de **nome de host MDM**.

5. O instalador agora precisa se conectar a um banco de dados existente que será usado pelo Conector de dispositivo móvel. Especifique os seguintes detalhes de conexão:

- **Banco de dados**: MySQL Server/MS SQL Server/MS SQL Server via autenticação do Windows

- **Driver ODBC**: MySQL ODBC 5.1 Driver/MySQL ODBC 5.2 Unicode Driver/MySQL ODBC 5.3 Unicode Driver/MySQL ODBC 8.0 Unicode Driver/SQL Server/SQL Server Native Client 10.0/ODBC Driver 11 for SQL Server/ODBC Driver 13 for SQL Server/ODBC Driver 17 for SQL Server/ODBC Driver 18 for SQL Server

- **Nome do banco de dados**: Recomendamos usar o nome pré-definido ou altera-lo, se necessário.

- **Nome de host**: nome de host ou endereço IP do seu servidor de banco de dados

- **Porta**: usado para conexão com o servidor do banco de dados

- **Nome de usuário/senha** de conta do administrador do banco de dados

- **Usar instância nomeada** – se você estiver usando um banco de dados Microsoft SQL, também será possível selecionar a caixa de marcação **Usar instância nomeada** para usar uma instância de banco de dados personalizada. Isso pode ser definido no campo **Nome de host** no formato *HOSTNAME\DB_INSTANCE* (por exemplo, *192.168.0.10\ESMC7SQL*). Para o banco de dados em agrupamento use apenas o nome do agrupamento. Se essa opção estiver selecionada, você não poderá alterar a porta de conexão do banco de dados: o sistema usará as portas padrão determinadas pela Microsoft. Para conectar o Servidor ESET PROTECT ao banco de dados Microsoft SQL instalado em um Cluster de failover, digite o nome do agrupamento no campo **Nome de host**.

> Você pode usar o mesmo servidor de banco de dados que você está usando para o banco de dados ESET PROTECT, mas é recomendado que use um servidor DB diferente se estiver planejando inscrever mais de 80 dispositivos móveis.

6. Especifique o usuário para o banco de dados do Conector de dispositivo móvel recém-criado. Você pode **Criar um novo usuário** ou **Usar usuário do banco de dados existente**. Insira a senha do usuário do banco de dados.

7. Insira **Host do servidor** (nome ou endereço IP do seu Servidor ESET PROTECT) e a **porta de servidor** (padrão é 2222, se você estiver usando uma porta diferente, substitua a porta padrão pelo seu número de porta personalizado).

8. Conecte o Conector MDM ao Servidor ESET PROTECT. Preencha o **host de Servidor** e a **porta de Servidor** necessários para a conexão com o Servidor ESET PROTECT e selecione a **Instalação auxiliada por servidor** ou **Instalação off-line** para continuar:

- **Instalação auxiliada por servidor** - Fornece ao ESET PROTECT as credenciais do administrador do Console da Web e o instalador vai fazer download dos certificados necessários automaticamente. Verifique também as permissões necessárias para a instalação auxiliada por servidor.

    1.Insira seu **host de Servidor** - nome ou endereço IP do seu Servidor ESET PROTECT e **porta do console da Web** (deixe a porta padrão 2223 se você não estiver usando uma porta personalizada). Forneça também as credenciais de conta do administrador do console da Web - **Nome de usuário/Senha**.

    2.Quando pedirem para Aceitar o certificado, clique em **Sim**. Continue para a etapa 10.

- **Instalação off-line** - Fornece um **certificado de Proxy** e uma **Autoridade de certificação** que pode ser exportada do ESET PROTECT. Alternativamente, é possível usar seu certificado personalizado e a Autoridade

de certificação adequada.

1.Clique em **Navegar** ao lado de Certificado de mesmo nível e navegue até o local do seu **Certificado de mesmo nível** (este é o certificado de Proxy que você exportou do ESET PROTECT). Deixe o campo de texto de **Senha certificada** em branco, pois este certificado não requer senha.

2.Repita o procedimento para a Autoridade de Certificação e continue para a etapa 10.

Se estiver usando certificados personalizados com o ESET PROTECT (em vez dos padrão gerados automaticamente durante a instalação do ESET PROTECT), eles devem ser usados quando você é solicitado a fornecer um certificado Proxy.

9. Especifique a pasta de destino para o conector de dispositivo móvel (recomendamos usar o padrão), clique em **Avançar** e depois em **Instalar**.

10. Depois de concluída a instalação, verifique se o Mobile Device Connector está sendo executado corretamente abrindo o *https://your-mdm-hostname:enrollment-port* (por exemplo, *https://mdm.company.com:9980*) no seu navegador da web ou de um dispositivo móvel. Se a instalação for realizada com êxito, você verá a mensagem a seguir: Servidor MDM funcionando!

11. Agora você pode ativar MDM do ESET PROTECT.

Pré-requisitos do Conector de dispositivo móvel

Se a porta ou o nome de host para o servidor MDM for alterado, será preciso reinscrever todos os dispositivos móveis.
Por isso, recomendamos que você configure um nome de host dedicado para o servidor MDM para que, se você algum dia precisar mudar o dispositivo host no servidor MDM, isso possa ser feito com uma nova atribuição do endereço IP ao nome de host MDM nas suas configurações DNS.

Os pré-requisitos a seguir devem ser atendidos para instalar o Mobile Device Connector no Windows:

- Endereço IP/nome de host público ou domínio público acessível da Internet.

Se precisar mudar o nome de host do seu Servidor MDM, será preciso executar uma instalação de reparo do seu componente MDC. Se você alterar o nome do host do seu servidor MDM, você precisará importar um novo **certificado do Servidor HTTPS** incluindo este novo nome do host, para que o MDM continue a funcionar corretamente.

- Portas abertas e disponíveis, consulte a lista completa de portas aqui. Recomendamos usar números de porta padrão 9981 e 9980, mas eles também podem ser alterados no arquivo de configuração do seu Servidor MDM, se necessário. Certifique-se de que os dispositivos móveis são capazes de se conectar através das portas especificadas. Altere suas configurações de firewall e/ou rede (se aplicável) para tornar isso possível. Leia mais sobre a arquitetura MDM.

- Configurações de firewall - ao instalar o Conector de dispositivo móvel em um sistema operacional que não de servidor como o Windows 7 (apenas para fins de avaliação), certifique-se de permitir portas de comunicação criando regras de firewall para:

C:\Program Files\ESET\RemoteAdministrator\MDMCore\ERAMDMCore.exe, TCP porta 9980

C:\Program Files\ESET\RemoteAdministrator\MDMCore\ERAMDMCore.exe, TCP porta 9981

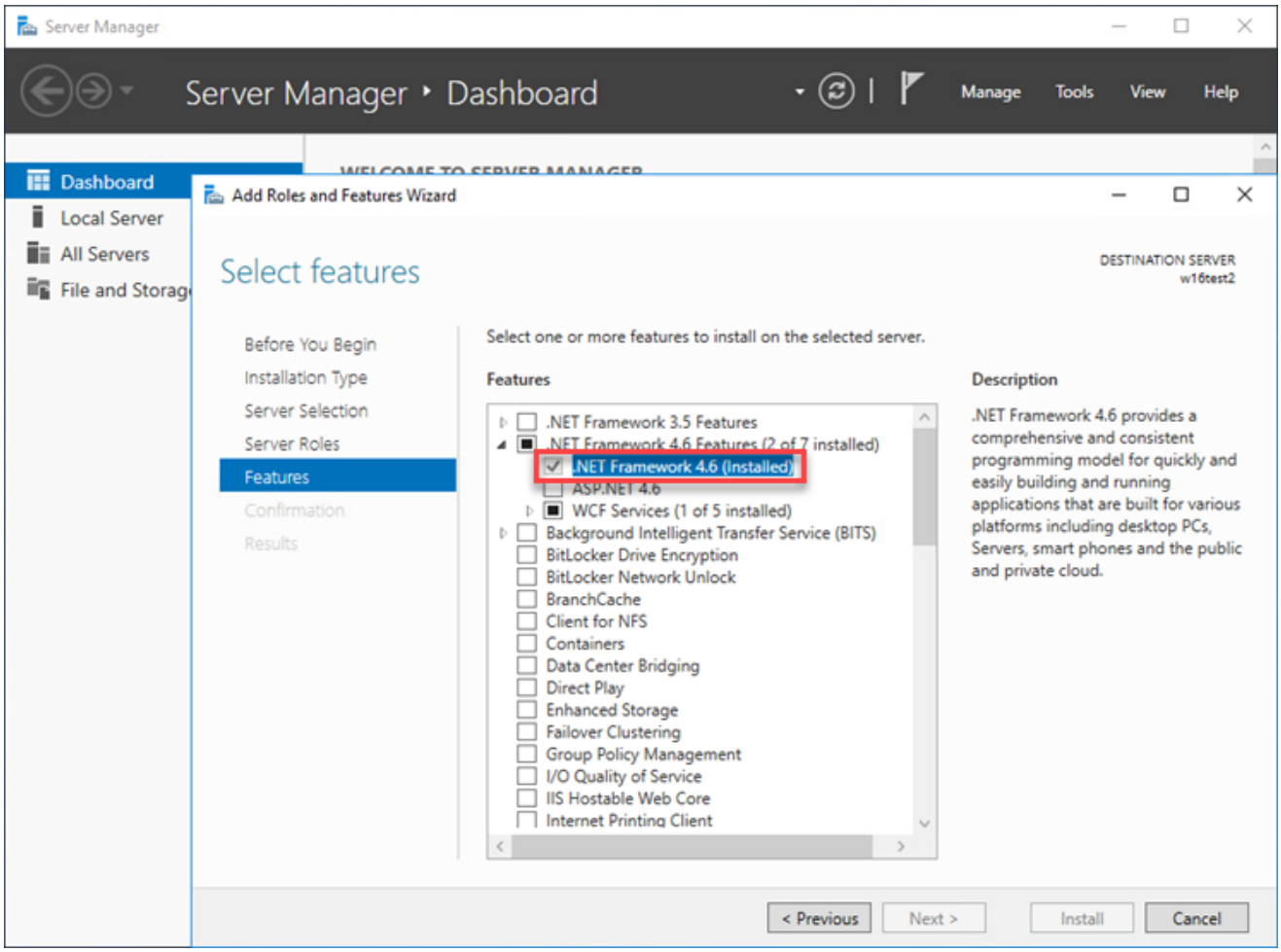
C:\Program Files\ESET\RemoteAdministrator\Server\ERAServer.exe, TCP porta 2222

> Caminhos reais para arquivos *.exe*podem variar dependendo de onde cada um dos componentes ESET PROTECT está instalado no sistema operacional do seu cliente.

- Um servidor do banco de dados já está instalado e configurado. Certifique-se de cumprir com os requisitos do Microsoft SQL ou MySQL.

- O uso de RAM de conector MDM é otimizado, portanto só podem existir no máximo 48 processos "ESET PROTECT MDMCore Module" executados simultaneamente e se o usuário se conectar a mais dispositivos, os processos vão mudar periodicamente para cada dispositivo que atualmente precisa usar os recursos.

- A instalação do Microsoft SQL Server Express requer o Microsoft .NET Framework 4. Você pode instalar usando o **Assistente para adicionar de funções e recursos**:



Requisitos do certificado

- Você precisará de um **Certificado SSL** em formato *.pfx*para comunicação segura por HTTPS. Recomendamos que você use um certificado fornecido por uma Autoridade de certificação terceira. Certificados com assinatura própria (inclusive certificados assinados pela CA ESET PROTECT) não são recomendados porque nem todos os dispositivos móveis permitem que os usuários aceitem certificados com assinatura própria.

- Você precisa ter um certificado assinado por CA e a chave privada correspondente, e usar procedimentos padrão (tradicionalmente usando OpenSSL) para fazer a mesclagem deles em um arquivo *.pfx*:
```
openssl pkcs12 -export -in certificate.cer -inkey privateKey.key -out
httpsCredentials.pfx
```
Este é o procedimento padrão para a maioria dos servidores que usam certificados SSL.

- Para Instalação off-line, você também precisará de um certificado de mesmo nível (o **Certificado de Agente** exportado do ESET PROTECT). Alternativamente, é possível usar seu certificado personalizado com o ESET PROTECT.

Ativação do Conector de dispositivo móvel

Depois de ter instalado o Conector de dispositivo móvel, é preciso ativá-lo com a licença do ESET endpoint, business ou office:

1. Adicione a licença do ESET Endpoint, Business ou Office ao Gerenciamento de licenças ESET PROTECT.

2. Ativar o Mobile Device Connector usando uma tarefa de cliente Ativação do produto. Este procedimento é o mesmo que ao ativar qualquer produto ESET em um computador do cliente, neste caso o Conector de dispositivo móvel é um computador cliente.

Funcionalidade de licenciamento MDM iOS

Como a ESET não oferece aplicativos na Apple App Store, o Conector de dispositivo móvel ESET armazena todos os detalhes de licenciamento para dispositivos iOS.

As licenças são por dispositivo e podem ser ativadas usando uma Tarefa de ativação do produto (assim como no Android).

As licenças iOS podem ser desativadas das seguintes formas:

- Remoção do dispositivo do gerenciamento através de uma tarefa de gerenciamento Parar
- Desinstalação do MDC através da opção **Remover banco de dados**
- Desativação por outros meios (ESET PROTECT ou desativação EBA)

Como o MDC se comunica com os servidores de licenciamento da ESET em nome dos dispositivos iOS, o portal EBA reflete o estado do MDC e não o estado de dispositivos individuais. Informações do dispositivo atuais estão sempre disponíveis no Console da Web ESET PROTECT.

Dispositivos que não estão ativados ou dispositivos com licenças expiradas vão exibir um status da proteção vermelho e a mensagem "Produto não ativado". Estes dispositivos vão se recusar a lidar com tarefas, definir políticas e entregar relatórios não-críticos.

Durante a desinstalação do MDM, se **Não remova o banco de dados** for selecionado as licenças usadas não serão desativadas. Essas licenças podem ser reutilizadas se MDM for reinstalado nesse banco de dados, removido via ESET PROTECT ou desativado com o EBA. Ao mover para outro servidor MDM, você vai precisar realizar a Tarefa de ativação do produto novamente.

Requisitos do certificado HTTPS

Para inscrever um dispositivo no Conector de dispositivo móvel ESET, certifique-se de que o servidor HTTPS envia a corrente de certificado completa.

Para que o certificado funcione corretamente, esses requisitos devem ser cumpridos:

- O certificado HTTPS (contêiner pkcs#12/pfx) deve ter toda a cadeia do certificado, inclusive o CA raiz.
- O certificado deve ser válido durante o período requerido (válido de / válido até)
- O **CommonName** ou **subjectAltNames** devem combinar com o nome de host MDM.

Se o **nome de host MDM** for,hostname.mdm.domain.com por exemplo , seu certificado pode ter nomes como:
- hostname.mdm.domain.com
- *.mdm.domain.com

Mas não nomes como:
- *
- *.com
- *.domain.com

Basicamente, o " * " não pode substituir o "ponto". Este comportamento é confirmado pela forma como o iOS aceita os certificados para MDM.

Observe que alguns dispositivos levam em conta seu fuso horário atual ao verificar a validade do certificado, outros dispositivos não. Para evitar problemas em potencial, defina a validade do certificado um ou dois dias antes da data atual.

Repositório off-line – Windows

Você pode usar a Ferramenta de imagem para criar um repositório off-line (no Windows). Normalmente isso é necessário para redes fechadas de computador ou redes com acesso a internet limitado. A Ferramenta de imagem pode ser usada para criar um clone do repositório ESET em uma pasta local. Este repositório clonado pode ser posteriormente movido (por exemplo, para um disco externo) para um local na rede fechada. Você pode copiar o repositório para um local seguro na rede local e torná-lo disponível através de um Servidor HTTP (por exemplo, ESET Bridge).

Para atualizar o repositório off-line, execute o mesmo comando com os mesmos parâmetros usados para a criação do repositório off-line. Os dados anteriores na pasta intermediária serão utilizados e o download será feito apenas para os arquivos desatualizados.

Esteja ciente de que o tamanho do repositório está crescendo e o diretório intermediário será do mesmo tamanho. Certifique-se de ter pelo menos **1.2 TB** de espaço livre antes de iniciar esse procedimento.

Melhores práticas

Consulte também o artigo da Base de conhecimento ESET Melhores práticas para usar em um ambiente ESET PROTECT off-line.

Exemplo de cenário para Windows

I. Criar clone do repositório

1. Faça o download da Ferramenta de imagem.

2. Extraia a Ferramenta de imagem do arquivo *.zip* baixado.

3. Preparar (criar) pastas para:

   - arquivos intermediários
   - repositório final

4. Abra o prompt de comando e mude o diretório para onde a pasta de Imagem está extraída (comando `cd`).

5. Execute o comando a seguir (altere os diretórios de repositório intermediário e de saída para as pastas da etapa 3):

```
MirrorTool.exe --repositoryServer AUTOSELECT ^
--intermediateRepositoryDirectory C:\Intermediary ^
--outputRepositoryDirectory C:\Repository
```

6. Depois que o repositório é copiado para a pasta `outputRepositoryDirectory`, mova a pasta e seu conteúdo para outra máquina de onde é possível acessar sua rede fechada.

II. Configure o servidor HTTP

1. Você precisa de um servidor HTTP sendo executado na máquina na rede fechada. Você pode usar:

   - Proxy ESET Bridge do site de download da ESET (este cenário)
   - um servidor HTTP diferente

2. Instale o proxy ESET Bridge.

III. Execute o repositório off-line

1. Navegue até *C:\Program Files\ESET\Bridge* e abra o arquivo *pkgid* usando um editor de texto simples. Mude as configuração do `http_proxy_settings_static_content_enabled` para `true` para ativar o servidor de repositório off-line. Salve as alterações e feche o arquivo *pkgid*.

2. Copie o repositório baixado da etapa 6 (seção I. acima) para o diretório do servidor do repositório off-line:

   • O diretório padrão do servidor de repositório off-line é o *C:\ProgramData\ESET\Bridge\OfflineRepository* com direitos de acesso adequados.

   • Para usar um diretório personalizado, crie uma nova pasta para o repositório off-line (por exemplo, *C:\Repository*). No arquivo*pkgid*, substitua a linha `"http_proxy_settings_offline_repository_dirPath": "%DATADIR%\\OfflineRepository"` por `"http_proxy_settings_offline_repository_dirPath": "C:\\Repository"`. O usuário

NETWORK SERVICE precisa de direitos de acesso total ao diretório.

3. Reinicie o serviço ESET Bridge usando os comandos de linha de comando: `net stop "EsetBridge"` e `net start "EsetBridge"`. Você deve reiniciar o serviço somente depois de alterar o arquivo *pkgid*. Não é preciso reiniciar o serviço quando os dados do repositório são alterados, removidos ou adicionados.

4. O repositório off-line é executado no endereço *http://YourIPaddress:4449* (por exemplo, *http://10.1.1.10:4449*).

5. Defina o novo endereço do repositório usando o Web Console ESET PROTECT:

a.Servidor ESET PROTECT – clique em **Mais** > **Configurações** > **Configurações avançadas** > **Repositório** e insira o endereço do repositório off-line no campo **Servidor**.

b.Agentes ESET Management – clique em **Políticas** clique na política do Agente > **Editar** > **Configurações** > **Configurações avançadas** > **Repositório** > insira o endereço do repositório off-line no campo **Servidor**.

c.Produtos endpoint ESET (para Windows) – clique em **Políticas**, clique na política **ESET Endpoint para Windows** > **Editar** > **Configurações** > **Atualizar** > **Perfis** > **Atualizações** > **Atualizações de módulos** > insira o endereço do repositório off-line no campo **Servidor personalizado**.

Cluster de failover – Windows

Abaixo estão as etapas de alto nível necessárias para instalar o ESET PROTECT em um ambiente de Agrupamento de failover.

> Consulte também esse artigo da Base de conhecimento sobre a instalação de agrupamento do Servidor ESET PROTECT.

1. Criar um agrupamento de failover com um disco compartilhado:

- Instruções para criar um agrupamento de failover no Windows Server 2016 e 2019
- Instruções para criar um agrupamento de failover no Windows Server 2012 e 2012 R2

2. No **Assistente para criação de agrupamento** digite o nome de host desejado (crie um) e endereço IP.

3. Coloque o disco compartilhado do agrupamento on-line no nó1 e instale o Servidor ESET PROTECT usando o instalador autônomo nele. Certifique-se de que **Esta é uma instalação de agrupamento** está selecionado durante a instalação e selecione o disco compartilhado como armazenamento de dados do aplicativo. Faça um nome de host e digite-o para o certificado do Servidor do ESET PROTECT Server ao lado dos nomes de host pré-preenchidos. Lembre-se deste nome de host e use-o na etapa nº. 6, ao criar a função do Servidor ESET PROTECT no Gerenciador de agrupamento.

4. Pare o ESET PROTECT Server no nó1, coloque o disco compartilhado do agrupamento on-line no nó2 e instale o Servidor ESET PROTECT usando o instalador autônomo nele. Certifique-se de que **Esta é uma instalação de agrupamento** está selecionado durante a instalação. Escolha o disco compartilhado como o armazenamento de dados do aplicativo. Mantenha a conexão de banco de dados e informações do certificado intactas, elas foram configuradas durante a instalação do ESET PROTECT Server no nó 1.

5. Configure seu firewall para permitir conexões de entrada em todas as portas usadas pelo ESET PROTECT

Server.

6. No gerenciador de configuração de agrupamento crie e inicie uma Função (**Configurar função** > **Selecionar função** > **Serviço genérico**) para o serviço do Servidor ESET PROTECT. Selecione o serviço do Servidor **ESET PROTECT** na lista de serviços disponíveis. É muito importante usar o mesmo nome de host que foi usado na etapa 3 para a Função, em relação ao certificado de Servidor.

7. Instale o Agente ESET Management em todos os nós do agrupamento usando o instalador autônomo. Nas telas **Configuração do agente** e **Conexão ao ESET PROTECT** use o nome de host usado na etapa nº. 6. Armazene os dados do Agente no nó local (não no disco de cluster).

8. O servidor da web (Apache Tomcat) não é compatível em um cluster, portanto ele precisa ser instalado em um disco sem cluster ou em uma máquina diferente:

a. Instale o Web Console em um computador separado e configure-o adequadamente para conectar-se à ESET PROTECT função de cluster do Servidor.

b. Depois que o console da Web é instalado, localize seu arquivo de configuração em: *C:\Program Files\Apache Software Foundation\[Tomcat pasta]\webapps\era\WEB-INF\classes\sk\eset\era\g2webconsole\server\modules\config\EraWebServerConfig.properties*

c. Abra o arquivo no bloco de notas ou qualquer outro editor de texto simples. Na linha `server_address=localhost` substitua localhost pelo endereço IP ou nome de host da Função de cluster do Servidor ESET PROTECT.

Instalação de componente no Linux

Na maioria dos cenários de instalação, você precisa instalar vários componentes do ESET PROTECT em diferentes máquinas para acomodar diversas arquiteturas de rede, atender aos requisitos de desempenho ou por outros motivos.

Siga as instruções de instalação passo a passo do ESET PROTECT.

Instalação de principais componentes:

- Servidor ESET PROTECT
- Console da Web ESET PROTECT – Você pode escolher instalar o Web Console ESET PROTECT em um computador diferente do computador executando o Servidor ESET PROTECT.
- Agente ESET Management
- um servidor de banco de dados

Instalação de componentes opcionais:

- Sensor RD
- Conector de dispositivo móvel
- ESET Bridge Proxy HTTP

- Ferramenta de imagem

Para atualizar o ESET PROTECT para Linux para a versão mais recente veja o capítulo da Tarefa de atualização de componentes no nosso artigo da Base de conhecimento.

Instalação passo-a-passo do ESET PROTECT no Linux

Neste cenário de instalação, vamos simular a instalação passo-a-passo do Servidor ESET PROTECT e console da Web ESET PROTECT. Vamos simular a instalação usando MySQL.

> **Instruções de instalação para distribuições Linux selecionadas**
> Você pode seguir nossos artigos da Base de conhecimento com instruções específicas para a distribuição:
> - CentOS 7
> - Debian 10
> - SUSE Linux Enterprise Server (SLES)

Antes da instalação

1. Verifique a presença do servidor de banco de dados na sua rede e certifique-se de ter acesso a ele no seu servidor local/remoto. Se um servidor de banco de dados não estiver instalado, instale e configure um novo.

2. Download dos Componentes autônomos do Linux ESET PROTECT (Agente, Servidor, Web Console). Esses arquivos de instalação podem ser encontrados na categoria Instaladores autônomos ESET PROTECT disponível no site da ESET.

Processo de instalação

Você deve ser capaz de usar o comando `sudo` ou instalar sob privilégios `root` para concluir a instalação.

1. Instale os pacotes necessários para o Servidor ESET PROTECT.

2. Configure a conexão ao servidor MySQL, como mostrado no tópico configuração MySQL.

3. Verifique a configuração da unidade ODBC do MySQL. Consulte Instalação e configuração ODBC para mais informações.

4. Personalize os parâmetro de instalação e execute a instalação de servidor ESET PROTECT. Consulte Instalação de servidor - Linux para mais informações.

5. Instale os pacotes Java e Tomcat necessários e instale o Web Console ESET PROTECT. Se você tiver problemas com a conexão HTTPS para o Web Console ESET PROTECT, veja a configuração de conexão HTTPS/SSL.

6. Instale o Agente ESET Management na máquina do servidor.

> Recomendamos remover comandos contendo dados sensíveis (por exemplo, uma senha) do histórico da linha de comando:
> 1.Execute `history` para ver a lista de todos os comandos no histórico.
> 2.Execute `history -d line_number` (especifique o número da linha do comando). Alternativamente, execute `history -c` para remover todo o histórico da linha de comando.

Instalação e configuração MySQL

Instalação

> ⚠ Certifique-se de instalar uma versão compatível do MySQL Server e do Conector ODBC.

Se você já instalou e configurou o MySQL, continue para a Configuração.

1. Adicionar o repositório MySQL:

Debian, Ubuntu	Execute os comandos a seguir no Terminal:
	`a)wget https://dev.mysql.com/get/mysql-apt-config_0.8.15-1_all.deb`
	`b)sudo dpkg -i mysql-apt-config_0.8.15-1_all.deb`
	Você pode selecionar as versões dos componentes que deseja instalar durante a instalação do pacote. Recomendamos selecionar as opções padrão. Veja também Adicionar o repositório MySQL APT

CentOS, Red Hat	Adicionar o repositório MySQL Yum
SUSE Linux Enterprise Server	Adicionar o repositório MySQL SLES

2. Atualize seu cache de repositório local:

Debian, Ubuntu	`sudo apt-get update`
CentOS, Red Hat	`sudo yum update`
SUSE Linux Enterprise Server	`sudo zypper update`

3. A instalação do MySQL será diferente dependendo da distribuição Linux e da versão usada:

Linux distribuição:	MySQL Comando de instalação de servidor:	MySQL Instalação avançada do servidor:
Debian, Ubuntu	`sudo apt-get install mysql-server`	Installing MySQL from Source with the MySQL APT Repository
CentOS, Red Hat	`sudo yum install mysql-community-server`	Installing MySQL on Linux Using the MySQL Yum Repository
SUSE Linux Enterprise Server	`sudo zypper install mysql-community-server`	Steps for a Fresh Installation of MySQL

Faça o download do MySQL Community Server para uma instalação manual.

Configuração

1. Abra o arquivo de configuração *my.cnf* em um editor de texto:

```
sudo nano /etc/my.cnf
```

Se o arquivo não estiver presente, tente `/etc/mysql/my.cnf` ou `/etc/my.cnf.d/community-mysql-server.cnf` ou `/etc/mysql/mysql.conf.d/mysqld.cnf`.

2. Descubra a configuração a seguir na seção `[mysqld]` do arquivo configuração *my.cnf* e modifique os valores.

> - Cria a seção `[mysqld]` se ela não estiver presente no arquivo.
> - Se os parâmetros não estiverem presentes no arquivo, adicione-os à seção `[mysqld]`.
> - Para determinar sua versão do MySQL, execute o comando: `mysql --version`

Parâmetro	Comentários e valores recomendados	MySQL versão
`max_allowed_packet=33M`		Todas as versões compatíveis.
`log_bin_trust_function_creators=1`	Alternativamente, é possível desativar o registro em relatório binário: `log_bin=0`	Versões 8.x compatíveis
`innodb_log_file_size=100M` `innodb_log_files_in_group=2`	A multiplicação de valores desses dois parâmetros deve ser no mínimo **200**. O valor mínimo para `innodb_log_files_in_group` é **2** e o valor máximo é **100**;, o valor também precisa ser um número inteiro.	Versões 8x compatíveis 5.7 5.6.22 (e versões posteriores 5.6.x)
`innodb_log_file_size=200M`	Defina o valor como no mínimo **200M**, mas no máximo **3000M**.	5.6.20 e 5.6.21

3. Pressione **CTRL + X** e digite **Y** para salvar as alterações e fechar o arquivo.

4. Reinicie o servidor MySQL e aplique a configuração (em alguns casos, o nome do serviço é `mysqld`):

```
sudo systemctl restart mysql
```

5. Configure privilégios e senha MySQL (isso é opcional e pode não funcionar para algumas distribuições Linux):

a)Revelar a senha temporária MySQL: `sudo grep 'temporary password' /var/log/mysql/mysqld.log`

b)Copie e salve a senha.

c)Defina uma nova senha seguindo uma dessas opções:

- Execute `/usr/bin/mysql_secure_installation` e digite a senha temporária. Então você será solicitado a criar uma nova senha.

- Execute `mysql -u root -p` e digite a senha temporária. Execute `ALTER USER 'root'@'localhost' IDENTIFIED BY 'strong_new_password';` para alterar a senha raiz (substitua `strong_new_password` pela sua senha) e digite `Quit`.

Veja também melhorar a segurança de instalação MySQL no manual de referência MySQL.

6. Verifique se o serviço do servidor MySQL está em execução:

```
sudo systemctl status mysql
```

Instalação e configuração ODBC

⚠ Certifique-se de instalar uma versão compatível do MySQL Server e do Conector ODBC.

ℹ Você pode instalar a unidade Microsoft ODBC (versão 13 e versões posteriores) para conectar o Servidor ESET PROTECT no Linux para o Microsoft SQL Server no Windows. Para obter mais informações, visite este artigo da Base de conhecimento.

Instale a unidade MySQL ODBC usando o Terminal. Siga as etapas para sua distribuição Linux:

- Debian, Ubuntu
- CentOS 7
- Outras distribuições Linux compatíveis

Debian, Ubuntu

1. Instalando drivers unixODBC:

```
sudo apt-get install unixodbc
```

2. Download do conector ODBC:

Ubuntu 16	`wget https://downloads.mysql.com/archives/get/p/10/file/mysql-connector-odbc-8.0.17-linux-ubuntu16.04-x86-64bit.tar.gz`
Ubuntu 18	`wget https://downloads.mysql.com/archives/get/p/10/file/mysql-connector-odbc-8.0.17-linux-ubuntu18.04-x86-64bit.tar.gz`
Ubuntu 20	`wget https://downloads.mysql.com/archives/get/p/10/file/mysql-connector-odbc-8.0.17-linux-ubuntu19.04-x86-64bit.tar.gz`
Debian 10	`wget https://downloads.mysql.com/archives/get/p/10/file/mysql-connector-odbc-8.0.17-linux-debian10-x86-64bit.tar.gz`

⚠
- Selecionar e fazer o download da versão compatível com sua distribuição e versão Linux.
- Você pode fazer o download do conector ODBC para MySQL do site oficial MySQL.

3. Descompacte o arquivo ODBC da unidade (o nome do pacote muda de acordo com o link usado):

```
gunzip mysql-connector-odbc-8.0.17-linux-ubuntu19.04-x86-64bit.tar.gz
```

4. Extraia a unidade ODBC (o nome do pacote muda de acordo com o link usado):

```
tar xvf mysql-connector-odbc-8.0.17-linux-ubuntu19.04-x86-64bit.tar
```

5. Navegue até a pasta da unidade ODBC (o nome do pacote muda de acordo com o link usado):

```
cd mysql-connector-odbc-8.0.17-linux-ubuntu19.04-x86-64bit
```

6. Copiar arquivos da unidade ODBC:

```
sudo cp bin/* /usr/local/bin
sudo cp lib/* /usr/local/lib
```

7. Registre o driver para ODBC.

- Para novas versões Linux como Ubuntu 20.x recomendamos usar a unidade Unicode:

```
sudo myodbc-installer -a -d -n "MySQL ODBC 8.0 Driver" -t
"Driver=/usr/local/lib/libmyodbc8w.so"
```

- Para outros sistemas, ou quando a unidade Unicode não estiver funcionando:

```
sudo myodbc-installer -a -d -n "MySQL ODBC 8.0" -t
"Driver=/usr/local/lib/libmyodbc8a.so"
```

8. Liste as unidades instaladas:

```
sudo myodbc-installer -d -l
```

Para obter mais informações, consulte:
https://dev.mysql.com/doc/connector-odbc/en/connector-odbc-installation-binary-unix-tarball.html.

CentOS 7

1. Instalando drivers unixODBC:

```
sudo yum install unixODBC -y
```

2. Download do conector ODBC:

```
wget
https://downloads.mysql.com/archives/get/p/10/file/mysql-connector-odbc-8.0.17-1.e
l7.x86_64.rpm
```

- Não instale o conector ODBC usando o YUM, ele instalaria a versão mais recente, não a versão compatível.
- Selecionar e fazer o download da versão compatível com sua distribuição e versão Linux.
- Você pode fazer o download do conector ODBC para MySQL do site oficial MySQL.

3. Instalar o Driver ODBC:

```
sudo rpm -ivh mysql-connector-odbc-8.0.17-1.e17.x86_64.rpm --nodeps
```

4. Configure a unidade ODBC:

```
sudo myodbc-installer -a -d -n "MySQL ODBC 8.0.17" -t
"Driver=/usr/lib64/libmyodbc8w.so"
```

5. Liste as unidades instaladas:

```
sudo myodbc-installer -d -l
```

Outras distribuições Linux compatíveis

- Selecionar e fazer o download da versão compatível com sua distribuição e versão Linux.
- Você pode fazer o download do conector ODBC para MySQL do site oficial MySQL.

1. Siga estas instruções para instalar o driver ODBC:

- **SUSE Linux Enterprise Server**: `sudo zypper install unixODBC`. Veja também https://dev.mysql.com/doc/connector-odbc/en/connector-odbc-installation-binary-unix-rpm.html

- Instalando o Conector/ODBC de uma distribuição de tarball binário

2. Execute o comando a seguir para abrir o arquivo *odbcinst.ini* em um editor de texto:

```
sudo nano /etc/odbcinst.ini
```

ou `sudo nano/etc/unixODBC/odbcinst.ini`

3. Copie a configuração a seguir para o arquivo *odbcinst.ini* (certifique-se de que os caminhos para o **Driver** e **Setup** estão corretos), em seguida salve e feche o arquivo:

```
[MySQL]
Description = ODBC for MySQL
Driver = /usr/lib/x86_64-linux-gnu/odbc/libmyodbc.so
Setup = /usr/lib/x86_64-linux-gnu/odbc/libodbcmyS.so
FileUsage = 1
```

O driver pode estar em um local diferente para algumas distribuições. Você pode encontrar o arquivo usando o comando a seguir:

```
sudo find /usr -iname "*libmyodbc*"
```

4. Atualize os arquivos de configuração que controlam o acesso ODBC para os servidores de banco de dados no host atual executando o comando a seguir:

```
sudo odbcinst -i -d -f /etc/odbcinst.ini
```

ou `sudo odbcinst -i -d -f /etc/unixODBC/odbcinst.ini`

Instalação de servidor - Linux

> **Instruções de instalação para distribuições Linux selecionadas**
> Você pode seguir nossos artigos da Base de conhecimento com instruções específicas para a distribuição:
> - CentOS 7
> - Debian 10
> - SUSE Linux Enterprise Server (SLES)

Instalação

Siga as etapas abaixo para instalar o componente do Servidor ESET PROTECT no Linux usando o comando Terminal:

> Certifique-se de atender a todos os pré-requisitos de instalação.

1. Faça o download do componente do Servidor ESET PROTECT:

```
wget https://download.eset.com/com/eset/apps/business/era/server/linux/latest/server
```

```
-linux-x86_64.sh
```

2. Tornar o arquivo do download executável:

```
chmod +x server-linux-x86_64.sh
```

3. Você pode preparar um script de instalação e executá-lo usando `sudo`.

Execute o script de instalação com base no exemplo abaixo (novas linhas serão divididas por "\" para copiar o comando inteiro no Terminal):

```
sudo ./server-linux-x86_64.sh \
--skip-license \
--db-type="MySQL Server" \
--db-driver="MySQL ODBC 8.0 Driver" \
--db-hostname=localhost \
--db-port=3306 \
--db-admin-username=root \
--db-admin-password=password \
--server-root-password=password \
--db-user-username=root \
--db-user-password=password \
--cert-hostname="hostname, IP, FQDN"
```

Você pode modificar os seguintes atributos:

Atributo	Descrição	Requerido
`--uninstall`	Desinstala o produto.	-
`--keep-database`	O banco de dados não será removido durante a desinstalação.	-
`--locale`	O identificador de localidade (LCID) do servidor instalado (o valor padrão é `en_US`). Consulte os idiomas compatíveis para as opções disponíveis. Se você não especificar o `--locale`, o servidor ESET PROTECT será instalado em inglês. Depois da instalação do ESET PROTECT, você pode definir um idioma para cada sessão do Web Console ESET PROTECT. Nem todos os elementos do Web Console serão alterados depois da alteração do idioma. Alguns dos elementos (painéis, políticas, tarefas, etc.) padrão são criados durante a instalação do ESET PROTECT e seu idioma não pode ser alterado.	Sim
`--skip-license`	A instalação não solicitará que o usuário confirme o acordo de licença.	-
`--skip-cert`	Ignorar a geração de certificados (use com o parâmetro `--server-cert-path`).	-
`--license-key`	Chave de licença da ESET. Você pode fornecer a chave de licença mais tarde.	-
`--server-port`	ESET PROTECT porta do servidor (o valor padrão é `2222`).	-

Atributo	Descrição	Requerido
`--console-port`	ESET PROTECT porta do console (o valor padrão é `2223`)	-
`--server-root-password`	A senha do login do Console da Web do usuário "Administrador" deve ter, pelo menos, 8 caracteres.	Sim
`--db-type`	O tipo de banco de dados que será usado (possíveis valores: `"MySQL Server"`, `"MS SQL Server"`) O Microsoft SQL Server para Linux não é compatível. Mas você pode conectar o Servidor ESET PROTECT no Linux ao Microsoft SQL Server no Windows.	-
`--db-driver`	Unidade ODBC usada para conexão com o banco de dados especificado no arquivo *odbcinst.ini* (o comando `odbcinst -q -d` dá uma lista de unidades disponíveis, use uma dessas unidades por exemplo: `--db-driver="MySQL ODBC 8.0 Driver"`, `--db-driver="MySQL ODBC 8.0 Unicode Driver"` ou `--db-driver="MySQL ODBC 8.0.17"`).	Sim
`--db-hostname`	Nome do computador ou endereço IP do servidor de banco de dados. A instância de banco de dados nomeada não é compatível.	Sim
`--db-port`	Porta do servidor de banco de dados (o valor padrão é `3306`).	Sim
`--db-name`	Nome do banco de dados do servidor ESET PROTECT (o valor padrão é `era_db`)	-
`--db-admin-username`	Nome de usuário do administrador do banco de dados (usado pela instalação para criação e modificação do banco de dados). Esse parâmetro pode ser omitido se houver um usuário de banco de dados criado anteriormente definido no `--db-user-username` e `--db-user-password`	Sim
`--db-admin-password`	Senha do administrador do banco de dados. Esse parâmetro pode ser omitido se houver um usuário de banco de dados criado anteriormente definido por `--db-user-username` e `--db-user-password`	Sim
`--db-user-username`	Nome de usuário do usuário do servidor ESET PROTECT do banco de dados (usado pelo servidor ESET PROTECT para conexão com o banco de dados); não deve ter mais de 16 caracteres.	Sim
`--db-user-password`	Senha de usuário do servidor ESET PROTECT do banco de dados	Sim
`--cert-hostname`	Contém todos os nomes e/ou IP possíveis do computador do Servidor ESET PROTECT. O valor deve corresponder com o nome de servidor especificado no certificado do Agente que tenta se conectar ao servidor.	Sim
`--server-cert-path`	Caminho para certificado de mesmo nível de servidor (use essa opção se você tiver especificado `--skip-cert` também)	-
`--server-cert-password`	Senha do certificado de mesmo nível do servidor	-
`--agent-cert-password`	Senha do certificado de mesmo nível do agente	-
`--cert-auth-password`	Senha da autoridade de certificação	-

Atributo	Descrição	Requerido
`--cert-auth-path`	Caminho para o arquivo da Autoridade de certificação do Servidor	-
`--cert-auth-common-name`	Nome comum da autoridade de certificação (use `""`)	-
`--cert-organizational-unit`	-	-
`--cert-organization`	-	-
`--cert-locality`	-	-
`--cert-state`	-	-
`--cert-country`	-	-
`--cert-validity`	Validade do certificado em dias ou anos (especifique no argumento `--cert-validity-unit`)	-
`--cert-validity-unit`	Unidade para validade de certificado; os valores possíveis são "Anos" ou "Dias" (o valor padrão é `Years`)	-
`--ad-server`	Servidor Active Directory	-
`--ad-user-name`	Nome do usuário que tem direitos para pesquisar na rede do AD	-
`--ad-user-password`	Senha de usuário do Active Directory	-
`--ad-cdn-include`	Caminho de árvore do Active Directory que será sincronizado; use aspas vazias "" para sincronizar uma árvore inteira	-
`--enable-imp-program`	Ativar o Programa de melhoria do produto.	-
`--disable-imp-program`	Desativar o Programa de melhoria do produto.	-

Recomendamos remover comandos contendo dados sensíveis (por exemplo, uma senha) do histórico da linha de comando:
1.Execute `history` para ver a lista de todos os comandos no histórico.
2.Execute `history -d line_number` (especifique o número da linha do comando). Alternativamente, execute `history -c` para remover todo o histórico da linha de comando.

4. A instalação convida você a participar do programa de melhoria do Produto. Pressione **Y** se concordar em enviar relatórios de travamento e dados de telemetria para a ESET ou pressione **N** para não enviar nenhum dado.

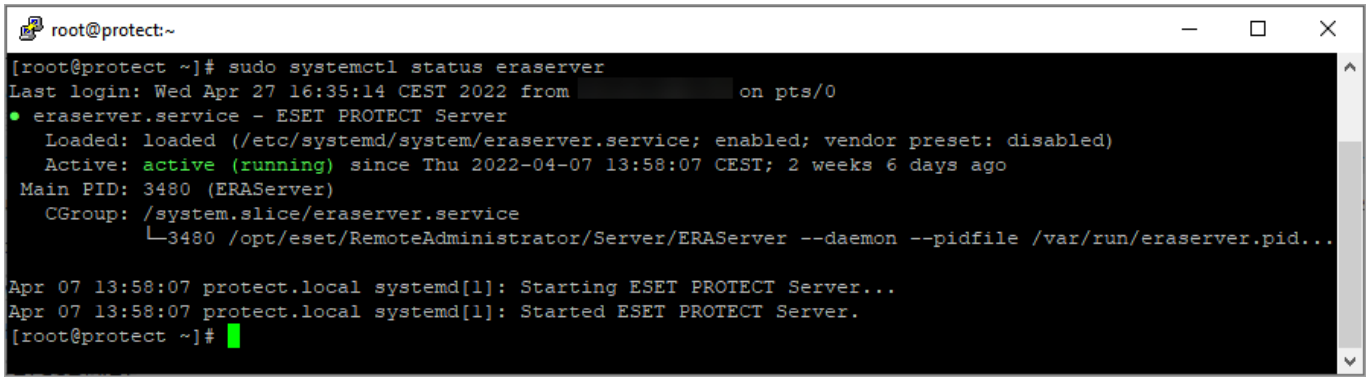
5. O servidor ESET PROTECT e o serviço `eraserver` serão instalados no seguinte local:

/opt/eset/RemoteAdministrator/Server

A instalação pode terminar com **SELinux policy... failure**. Você pode ignorar se não usar SELinux.

6. Depois da instalação, verifique se o serviço do Servidor ESET PROTECT está em execução usando o comando exibido abaixo:

```
sudo systemctl status eraserver
```



Relatório do instalador

O relatório do instalador pode ser útil para solução de problemas e você pode encontrá-lo nos Arquivos de relatório.

Pré-requisitos de servidor - Linux

Certifique-se de atender aos seguintes pré-requisitos para instalar o Servidor ESET PROTECT no Linux:

- Você deve ter uma licença válida.
- Você deve ter um sistema operacional Linux compatível.
- As portas necessárias devem estar abertas e disponíveis – consulte a lista completa de portas aqui.
- Um servidor do banco de dados deve ser instalado e configurado com uma conta de raiz. Uma conta de usuário não precisa ser criada antes da instalação. O instalador pode criar a conta. O Microsoft SQL Server para Linux não é compatível. Mas você pode conectar o Servidor ESET PROTECT no Linux ao Microsoft SQL Server no Windows.

> O Servidor ESET PROTECT armazena grandes blocos de dados no banco de dados. Configure o MySQL para aceitar pacotes grandes para que o ESET PROTECT seja executado corretamente.

- **Unidade ODBC** – A Unidade ODBC é usada para estabelecer conexão com o servidor de banco de dados (MySQL).
- Defina o arquivo de instalação do servidor como um executável usando o comando Terminal:

```
chmod +x server-linux-x86_64.sh
```

- Recomendamos que você **use a versão mais recente do OpenSSL1.1.1**. O Agente ESET Management é compatível com o OpenSSL 3.x. A versão mínima compatível do OpenSSL para Linux é openssl-1.0.1e-30. Podem existir mais versões do OpenSSL instaladas em um sistema simultaneamente. Pelo menos uma versão compatível deve estar presente no seu sistema.
    - Use o comando `openssl version` para exibir sua versão padrão atual.
    - Você pode listar todas as versões do OpenSSL presentes no seu sistema. Veja as terminações de nome de arquivo listadas usando o comando `sudo find / -iname *libcrypto.so*`
    - Você pode verificar se seu cliente Linux é compatível usando o comando a seguir: `openssl s_client`

```
-connect google.com:443 -tls1_2
```

ESET PROTECTO Servidor/gerenciamento de dispositivo móvel não são compatíveis com o OpenSSL 3.x. O Agente ESET Management é compatível com o OpenSSL 3.x.

- **Xvfb** - Necessário para a impressão correta de relatórios (Gerar relatório) em sistemas de servidor Linux sem uma interface gráfica.

- **Xauth** – o pacote é instalado junto com o **xvfb**. Você precisa instalar o **xauth** se não instalar o **xvfb**.

- **cifs-utils** – Necessário para implantação apropriada do Agente para um sistema operacional Windows.

- **Bibliotecas Qt4 WebKit** - Usado para impressão de relatórios no formato PDF e PS (deve ser a versão 4.8, e não 5). Todas as outras dependências Qt4 serão instaladas automaticamente. Se o pacote não estiver disponível em você no repositório do sistema operacional, você poderá compilar você mesmo em uma máquina de destino ou instalar de um repositório de terceiros (por exemplo, repositórios EPEL): Instruções do CentOS 7, instruções do Ubuntu 20.04.

- **kinit + klist** – o Kerberos é usado para autenticar um usuário do domínio durante a tarefa de login e sincronização do Active Directory. Certifique-se de configurar o Kerberos adequadamente (*/etc/krb5.conf*). ESET PROTECT é compatível com a sincronização com vários domínios.

- **ldapsearch** – Usado na tarefa de sincronização AD e para autorização.

- **snmptrap** – opcional, usado para enviar intercepções SNMP. O SNMP também requer configuração.

- **Pacote SELinux devel** - Usado durante a instalação do produto para construir módulos de política SELinux. Isso só é necessário em sistemas com SELinux ativado (CentOS, RHEL). SELinux pode causar problemas com outros aplicativos. Para um Servidor ESET PROTECT isso não é necessário.

- **lshw** - Instale o pacote `lshw` na máquina Linux do cliente/servidor para que o Agente ESET Management relate o inventário de hardware corretamente.

A tabela abaixo contém os comandos de terminais adequados para cada pacote descrito acima para várias distribuições Linux (execute os comandos como `sudo` ou `root`):

Pacote	Distribuições Debian e Ubuntu	Distribuições CentOS e Red Hat
Unidade ODBC	Consulte a Instalação e configuração ODBC.	Consulte a Instalação e configuração ODBC.
OpenSSL	`apt-get install openssl`	`yum install openssl -y`
xvfb	`apt-get install xvfb`	`yum install xorg-x11-server-Xvfb -y`
cifs-utils	`apt-get install cifs-utils`	`yum install cifs-utils`

Bibliotecas Qt4 WebKit	`apt-get install libqtwebkit4`
	Veja as instruções para o Ubuntu 20.04.
		O Qt4 WebKit não está no repositório CentOS padrão. Instale esses pacotes:
		`yum install -y epel-release`
		`yum install qtwebkit-devel`
		Alternativamente, você pode instalar o pacote de repositórios Fedora.

kinit+klist – opcional (necessário para o serviço do Active Directory)	`apt-get install krb5-user`	`yum install krb5-workstation`
ldapsearch	`apt-get install ldap-utils libsasl2-modules-gssapi-mit`	`yum install openldap-clients cyrus-sasl-gssapi cyrus-sasl-ldap -y`
snmptrap	`apt-get install snmp`	`yum install net-snmp-utils net-snmp`
Pacote SELinux devel (opcional – não é necessário para o Servidor ESET PROTECT; SELinux pode causar problemas com outros aplicativos.)	`apt-get install selinux-policy-dev`	`yum install policycoreutils-devel`
samba (opcional, necessário apenas para a implantação remota)	`apt-get install samba`	`yum install samba samba-winbind-clients`

Pacote	Distribuições Debian e Ubuntu	Distribuições CentOS e Red Hat
lshw	`apt-get install -y lshw`	`yum install -y lshw`

Instalação de agente - Linux

Pré-requisitos

- Recomendamos que você **use a versão mais recente do OpenSSL1.1.1**. O Agente ESET Management é compatível com o OpenSSL 3.x. A versão mínima compatível do OpenSSL para Linux é openssl-1.0.1e-30. Podem existir mais versões do OpenSSL instaladas em um sistema simultaneamente. Pelo menos uma versão compatível deve estar presente no seu sistema.
  - Use o comando `openssl version` para exibir sua versão padrão atual.
  - Você pode listar todas as versões do OpenSSL presentes no seu sistema. Veja as terminações de nome de arquivo listadas usando o comando `sudo find / -iname *libcrypto.so*`
  - Você pode verificar se seu cliente Linux é compatível usando o comando a seguir: `openssl s_client -connect google.com:443 -tls1_2`

> ESET PROTECTO Servidor/gerenciamento de dispositivo móvel não são compatíveis com o OpenSSL 3.x. O Agente ESET Management é compatível com o OpenSSL 3.x.

- Instale o pacote `lshw` na máquina Linux do cliente/servidor para que o Agente ESET Management relate o inventário de hardware corretamente.

Distribuição Linux	Comando de terminal
Debian, Ubuntu	`sudo apt-get install -y lshw`
Red Hat, CentOS, RHEL	`sudo yum install -y lshw`
OpenSUSE	`sudo zypper install lshw`

- Para o Linux CentOS recomendamos instalar o pacote `policycoreutils-devel`. Execute o comando para instalar o pacote:

```
yum install policycoreutils-devel
```

- Instalação do Agente assistida pelo servidor:
  - O computador servidor deve poder ser alcançado da rede e ter o Servidor ESET PROTECT e o Console da Web ESET PROTECT instalados.
- Instalação do Agente off-line:
  - O computador servidor deve poder ser alcançado da rede e ter o Servidor ESET PROTECT instalado.
  - Um Certificado para o agente deve estar presente.

- Um arquivo de chave pública da Autoridade de certificação do servidor deve estar presente.

Instalação

Siga as etapas abaixo para instalar o componente do Agente ESET Management no Linux usando um comando de Terminal:

Certifique-se de atender a todos os pré-requisitos de instalação listados acima.

1. Faça o download do script de instalação do Agente:

```
wget https://download.eset.com/com/eset/apps/business/era/agent/latest/agent-linux-x86_64.sh
```

2. Torne o arquivo executável:

```
chmod +x agent-linux-x86_64.sh
```

3. Execute o script de instalação com base no exemplo abaixo (novas linhas serão divididas por "\" para copiar o comando inteiro no Terminal):

Para mais detalhes, consulte Parâmetros abaixo.

Instalação assistida pelo servidor:

```
sudo ./agent-linux-x86_64.sh \
--skip-license \
--hostname=10.1.0.1 \
--port=2222 \
--webconsole-user=Administrator \
--webconsole-password=aB45$45c \
--webconsole-port=2223
```

Instalação off-line:

```
sudo ./agent-linux-x86_64.sh \
--skip-license \
--cert-path=/home/admin/Desktop/agent.pfx \
--cert-auth-path=/home/admin/Desktop/CA.der \
--cert-password=N3lluI4#2aCC \
--hostname=10.1.179.36 \
--port=2222
```

Recomendamos remover comandos contendo dados sensíveis (por exemplo, uma senha) do histórico da linha de comando:
1.Execute `history` para ver a lista de todos os comandos no histórico.
2.Execute `history -d line_number` (especifique o número da linha do comando). Alternativamente, execute `history -c` para remover todo o histórico da linha de comando.

4. Quando solicitado, pressione **y** para aceitar o certificado. Você pode ignorar quaisquer erros sobre o SELinux devolvidos pelo instalador.

5. Depois da instalação, verifique se o serviço do Agente ESET Management está em execução:

```
sudo systemctl status eraagent
```

6. Configure o serviço **eraagent** para iniciar na inicialização: `sudo systemctl enable eraagent`

> **Relatório do instalador**
> O relatório do instalador pode ser útil para solução de problemas. Isso pode ser encontrado nos Arquivos de relatório.

Parâmetros

A conexão com o Servidor ESET PROTECT é resolvida usando os parâmetros --hostname e --port (a porta não é usada quando um registro SRV é fornecido). Possíveis formatos de conexão.

- **Nome de host** e **porta**
- **Endereço IPv4** e **porta**
- **Endereço IPv6** e **porta**
- Registro de serviço (registro SRV) - para configurar o registro de recurso DNS no Linux, o computador deve estar em um domínio com um servidor DNS funcionando. Consulte Registro de recurso DNS. O registro SRV deve começar com o prefixo "_NAME._tcp" onde 'NAME' representa o nome personalizado (por exemplo, 'era').

Atributo	Descrição	Requerido
`--hostname`	Nome de host ou endereço IP do Servidor ESET PROTECT onde conectar.	Sim
`--port`	ESET PROTECT Porta do servidor () (o valor padrão é `2222`).	Sim
`--cert-path`	Caminho local para o arquivo de certificado do Agente (mais sobre o certificado).	Sim (Off-line)
`--cert-auth-path`	Caminho para o arquivo da Autoridade de certificação do Servidor (mais sobre a autoridade).	Sim (Off-line)
`--cert-password`	Senha do certificado do Agente.	Sim (Off-line)
`--cert-auth-password`	Senha da autoridade de certificação.	Sim (se usado)
`--skip-license`	A instalação não solicitará que o usuário confirme o acordo de licença.	Não
`--cert-content`	Base64 codificou o conteúdo do certificado de chave pública codificado PKCS12 mais a chave privada usada para configurar canais de comunicação segura com o Servidor e os Agentes. Use apenas uma das opções `--cert-path` ou `--cert-content`.	Não
`--cert-auth-content`	Base64 codificou o conteúdo do certificado de chave privada da autoridade de certificação codificada DER usado para verificar os pares remotos (Proxy ou Servidor). Use apenas uma das opções `--cert-auth-path` ou `--cert-auth-content`.	Não
`--webconsole-hostname`	Nome de host ou endereço IP usado pelo Web Console para conectar ao servidor (se for deixado em brando, o instalador vai copiar o valor de 'nome de host').	Não
`--webconsole-port`	Porta usada pelo console da web para conectar ao servidor (o valor padrão é `2223`).	Não
`--webconsole-user`	Nome de usuário usado pelo console da web para conectar ao servidor (o valor padrão é `Administrator`). Não é possível usar um usuário com autenticação em dois fatores para instalações auxiliadas por servidor.	Não
`--webconsole-password`	Senha usada pelo Console da web para conectar ao servidor.	Sim (auxiliado por Servidor)
`--proxy-hostname`	Nome de host do proxy HTTP. Use este parâmetro para ativar o uso do Proxy HTTP (que já está instalado em sua rede) para replicação entre o Agente ESET Management e o Servidor ESET PROTECT (não para atualizações de cache).	Se o proxy for usado
`--proxy-port`	Porta do Proxy HTTP para conexão ao servidor.	Se o proxy for usado
`--enable-imp-program`	Ativar o Programa de melhoria do produto.	Não
`--disable-imp-program`	Desativar o Programa de melhoria do produto.	Não

Conexão e certificados

- **A conexão ao Servidor ESET PROTECT** deve ser fornecida: `--hostname`, `--port` (a porta não é necessária se o registro do serviço foi fornecido, o valor de porta padrão é `2222`)

- Forneça as informações de conexão para **Instalação auxiliada por servidor**: `--webconsole-port, --webconsole-user, --webconsole-password`

- Forneça informações de certificado para a **Instalação off-line**: `--cert-path`, `--cert-password`. Os parâmetros de instalação `--cert-path` e `--cert-auth-path` requerem arquivos de certificação (*.pfx* e *.der*) que podem ser exportados do console web ESET PROTECT. (Leia como exportar o arquivo .pfx e o arquivo .der.)

Parâmetros do tipo de senha

Parâmetros do tipo de senha podem ser fornecidos como variáveis do ambiente, arquivos, leitura do `stdin` ou fornecidos como texto simples. Ou seja:

`--password=env:SECRET_PASSWORD` onde `SECRET_PASSWORD` é uma variável de ambiente com senha

`--password=file:/opt/secret` onde a primeira linha do arquivo regular `/opt/secret` contém sua senha

`--password=stdin` instrui o instalador a ler a senha da entrada padrão

`--password="pass:PASSWORD"` é igual a `--password="PASSWORD"` e é obrigatório se a senha atual seja `"stdin"` (entrada padrão) ou uma string começando com `"env:"`, `"file:"` ou `"pass:"`

A senha do certificado não deve ter os seguintes caracteres: `"` `\` Esses caracteres causam um erro crítico durante a inicialização do Agente.

Conexão de Proxy HTTP

Se você estiver usando o Proxy HTTP para replicação entre o Agente ESET Management e o Servidor ESET PROTECT (não para armazenamento em cache de atualizações), é possível especificar os parâmetros de conexão no `--proxy-hostname` e `--proxy-port`.

EXEMPLO - instalação do Agente off-line com Conexão Proxy HTTP:

```
./agent-linux-x86_64.sh \
--skip-license \
--cert-path=/home/admin/Desktop/agent.pfx \
--cert-auth-path=/home/admin/Desktop/CA.der \
--cert-password=N3lluI4#2aCC \
--hostname=10.1.179.36 \
--port=2222 \
--proxy-hostname=10.1.180.3 \
--proxy-port=3333 \
```

O protocolo de comunicação entre o Agente e o Servidor ESET PROTECT não é compatível com a autenticação. Qualquer solução de proxy usada para encaminhar a comunicação do Agente para o Servidor ESET PROTECT e que precise de autenticação não funcionará.
Se você escolher usar uma porta não padrão para o console web ou Agente, poderá ser necessário fazer um ajuste de firewall. Caso contrário, a instalação poderá falhar.

Atualização e reparo da instalação do Agente no Linux

Se você executa a instalação do Agente manualmente em um sistema onde o Agente já está instalado, o cenário a seguir pode acontecer:

- **Atualização** – execute uma versão posterior do instalador.
  - Instalação auxiliada por servidor - o aplicativo é atualizado, mas vai continuar usando os certificados anteriores.
  - Instalação off-line - o aplicativo é atualizado, novos certificados são usados.
- **Reparo** – execute a mesma versão do instalador. Você pode usar esta opção para migrar o Agente para um Servidor ESET PROTECT diferente.
  - Instalação auxiliada por servidor - o aplicativo é reinstalado e vai obter os certificados atuais do Servidor ESET PROTECT (definido pelo parâmetro `hostname`).
  - Instalação off-line – o aplicativo é reinstalado e novos certificados são usados.

Se você estiver migrando o agente do Servidor antigo para um Servidor ESET PROTECT diferente mais novo manualmente, e está usando a instalação auxiliada por servidor, execute o comando de instalação duas vezes. O primeiro vai atualizar o Agente e o segundo vai obter os novos certificados, para que o Agente possa conectar ao Servidor ESET PROTECT.

Instalação do console da Web - Linux

Siga essas etapas para instalar o Web Console ESET PROTECT:

Você pode escolher instalar o Web Console ESET PROTECT em um computador diferente do computador executando o Servidor ESET PROTECT. Este procedimento requer etapas adicionais.

1. Instale os pacotes Apache Tomcat e Java.

Exemplos de nomes de pacote abaixo podem ser diferentes dos pacotes do repositório de distribuição Linux. O repositório padrão de sua distribuição Linux pode não conter a versão mais recente compatível do Apache Tomcat e do Java.

Distribuição Linux	Comandos de terminal
distribuições Debian e Ubuntu	`sudo apt-get update` `sudo apt-get install openjdk-17-jdk tomcat9`
distribuições CentOS e Red Hat	`yum update` `yum install java-17-openjdk tomcat`
SUSE Linux	`zypper refresh` `sudo zypper install java-17-openjdk tomcat9`

2. Faça o download do arquivo do Web Console (*era.war*):

```
wget https://download.eset.com/com/eset/apps/business/era/webconsole/latest/era.war
```

3. Copie o arquivo *era.war* para a pasta Tomcat:

Debian, **Ubuntu**	`sudo cp era.war /var/lib/tomcat9/webapps/`
CentOS, **Red Hat**	`sudo cp era.war /var/lib/tomcat/webapps/`
SUSE Linux Enterprise Server	`sudo cp era.war /usr/share/tomcat/webapps/`

4. Reinicie o serviço Tomcat para implantar o arquivo *era.war*:

Debian, **Ubuntu**	`sudo systemctl restart tomcat9`
CentOS, **Red Hat**	`sudo systemctl restart tomcat`
SUSE Linux Enterprise Server	`sudo systemctl restart tomcat`

5. Verifique se a pasta *era* está presente na pasta Tomcat:

Debian, **Ubuntu**	`ls /var/lib/tomcat9/webapps`
CentOS, **Red Hat**	`ls /var/lib/tomcat/webapps`
SUSE Linux Enterprise Server	`ls /usr/share/tomcat/webapps`

O resultado deve ser parecido com: `era era.war`

6. Configure o serviço Tomcat para iniciar na inicialização: `sudo systemctl enable tomcat` (ou `tomcat9` com base no nome do serviço)

7. Se você instalou o console web ESET PROTECT em um computador diferente do Servidor ESET PROTECT, realize essas etapas adicionais para permitir a comunicação entre o console web ESET PROTECT e o Servidor ESET PROTECT:

a)Pare o serviço Tomcat: `sudo systemctl stop tomcat`

b)Edite o arquivo *EraWebServerConfig.properties*:

```
sudo nano /var/lib/tomcat/webapps/era/WEB-
INF/classes/sk/eset/era/g2webconsole/server/modules/config/EraWebServerConfig.prop
erties
```

Se o arquivo *EraWebServerConfig.properties* não for localizado no caminho acima, você pode usar o comando a seguir para encontrar o arquivo no seu sistema:

```
find / -iname "EraWebServerConfig.properties"
```

c)Encontre o `server_address=localhost`

d)Substitua `localhost` com o endereço IP do seu Servidor ESET PROTECT e salve o arquivo.

e)Reinicie o serviço Tomcat: `sudo systemctl restart tomcat` (ou `tomcat9` com base no nome do

serviço)

f)Configure o serviço Tomcat para iniciar na inicialização: `sudo systemctl enable tomcat` (ou `tomcat9` com base no nome do serviço)

8. Abra o Web Console ESET PROTECT em um navegador da web compatível para ver uma tela de login:

• Do computador hospedando o Web Console ESET PROTECT: *http://localhost:8080/era*

• De qualquer computador com acesso à Internet ao Web Console ESET PROTECT (substitua *IP_ADDRESS_OR_HOSTNAME* pelo endereço IP ou nome de host do seu Web Console ESET PROTECT): *http://IP_ADDRESS_OR_HOSTNAME:8080/era*

9. Configurar o Web Console depois da instalação:

• A porta HTTP padrão é configurada no 8080 durante a instalação manual do Apache Tomcat. Recomendamos configurar uma conexão HTTPS para Apache Tomcat.

• Veja também a configuração adicional do Web Console para soluções empresariais ou para sistemas de baixo desempenho.

Instalação do rogue detection sensor – Linux

Pré-requisitos

• A rede deve poder ser pesquisável (portas abertas, firewall não bloqueando comunicação de entrada, etc.).

• Pode ser possível alcançar o computador ESET PROTECT Servidor.

• O Agente ESET Management deve estar instalado no computador local para oferecer suporte total a todos os recursos do programa.

Se houver vários segmentos de rede, o Rogue Detection Sensor deve ser instalado separadamente em cada segmento de rede para produzir uma lista abrangente de todos os dispositivos em toda a rede.

Instalação

Siga as etapas abaixo para instalar o componente do Sensor RD no Linux usando o comando Terminal:

Certifique-se de atender a todos os pré-requisitos de instalação listados acima.

1. Visite a seção de download ESET PROTECT para fazer download de um instalador autônomo para este componente ESET PROTECT (*rdsensor-linux-i386.sh* ou *rdsensor-linux-x86_64.sh*).

2. Defina o arquivo de instalação do Sensor RD como um executável: `chmod +x rdsensor-linux-x86_64.sh`

3. Use o seguinte comando para executar o arquivo de instalação como sudo:

```
sudo ./rdsensor-linux-x86_64.sh
```

4. Leia o Acordo de licença de usuário final. Use a **barra de espaço** para ir para a próxima página do EULA. O instalador irá solicitar que você especifique se aceita o acordo. Pressione **Y** no seu teclado se concordar. Caso contrário, pressione **N**.

5. Pressione **Y** se você concordar em participar do Programa de melhoria do produto. Caso contrário, pressione **N**.

6. O ESET Rogue Detection Sensor será iniciado depois da instalação ser concluída.

7. Para verificar se a instalação foi bem-sucedida, verifique se o serviço está em execução ao executar o comando a seguir:

```
sudo systemctl status rdsensor
```

Você pode encontrar o arquivo de relatório do Rogue Detection Sensor nos Arquivos de relatório: */var/log/eset/RogueDetectionSensor/trace.log*

Instalação do conector de dispositivo móvel - Linux

O componente do Gerenciamento de dispositivo móvel/Conector ESET PROTECT (MDM/MDC) (apenas no local) teve seu fim da vida útil agendado. Ler mais. Recomendamos que você migre para o gerenciamento de dispositivo móvel em nuvem.

Você pode instalar o conector de dispositivo móvel em um servidor diferente daquele no qual seu servidor ESET PROTECT está sendo executado. Por exemplo, você pode usar esse cenário de instalação para que o Mobile Device Connector possa ser acessado da internet para gerenciar os dispositivos móveis do usuário em todos os momentos.

Siga as etapas abaixo para instalar o componente Mobile Device Connector no Linux usando o comando Terminal:

Certifique-se de atender a todos os pré-requisitos de instalação.

1. Faça o download do script de instalação do Mobile Device Connector:

```
wget https://download.eset.com/com/eset/apps/business/era/mdm/latest/mdmcore-linux-x86_64.sh
```

2. Execute o script de instalação com base no exemplo abaixo (novas linhas serão divididas por "\" para copiar o comando inteiro no Terminal):

```
sudo ./mdmcore-linux-x86_64.sh \
--https-cert-path="full_path/proxycert.pfx" \
--https-cert-password="123456789" \
--port=2222 \
--db-type="MySQL Server" \
--db-driver="MySQL ODBC 8.0 Driver" \
--db-admin-username="root" \
--db-admin-password=123456789 \
--db-user-password=123456789 \
--db-hostname="127.0.0.1" \
```

```
--webconsole-password=123456789 \
--hostname=username.LOCAL \
--mdm-hostname=username.LOCAL
```

Para obter uma lista completa dos parâmetros disponíveis (imprimir mensagens de ajuda), use:

```
--help
```

> Recomendamos remover comandos contendo dados sensíveis (por exemplo, uma senha) do histórico da linha de comando:
> 1.Execute `history` para ver a lista de todos os comandos no histórico.
> 2.Execute `history -d line_number` (especifique o número da linha do comando). Alternativamente, execute `history -c` para remover todo o histórico da linha de comando.

Parâmetros necessários do comando de instalação

Existem muitos parâmetros opcionais de instalação, mas alguns deles são obrigatórios:

- Certificado de mesmo nível – existem dois métodos de obter o certificado de mesmo nível ESET PROTECT:

  - **Instalação auxiliada por servidor** – será necessário fornecer credenciais de administrador do Web Console ESET PROTECT (o instalador vai fazer download dos certificados necessários automaticamente).

  - **Instalação off-line** - você precisará fornecer um Certificado de mesmo nível (o Certificado de Proxy exportado do ESET PROTECT). Alternativamente, é possível usar seu certificado personalizado.

    oPara uma **Instalação auxiliada por servidor** inclua pelo menos:

    ```
    --webconsole-password=
    ```

    oPara uma **Instalação off-line** inclua:

    ```
    --cert-path=
    --cert-password=
    ```

(O Certificado de Agente padrão criado durante a instalação do Servidor ESET PROTECT não precisa de uma senha.)

- Certificado de Proxy do HTTPS:

  oSe você já tem um certificado HTTPS:

  ```
  --https-cert-path=
  --https-cert-password=
  ```

- Para gerar um novo certificado HTTPS:

```
--https-cert-generate
--mdm-hostname=
```

- Conexão com o Servidor ESET PROTECT (nome ou endereço IP):

```
--hostname=
```

- Conexão de banco de dados:
  - Para um banco de dados MySQL inclua:

```
--db-type="MySQL Server"
--db-driver=
--db-admin-username=
--db-admin-password=
--db-user-password=
```

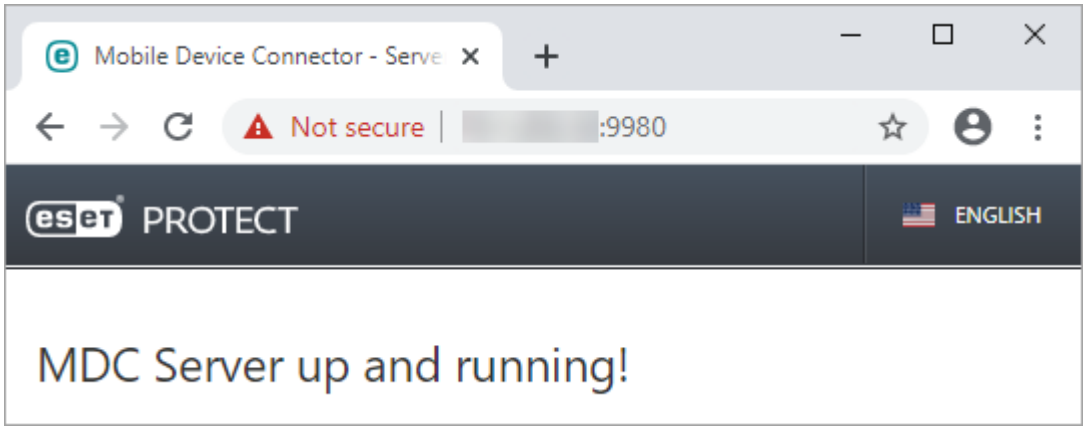
  - Para um banco de dados MICROSOFT SQL inclua:

```
--db-type="Microsoft SQL Server"
--db-driver=
--db-admin-username=
--db-admin-password=
--db-user-password=
```

Relatório do instalador

O relatório do instalador pode ser útil para solução de problemas e você pode encontrá-lo nos Arquivos de relatório.

Depois de concluída a instalação, verifique se o Conector de dispositivo móvel está sendo executado corretamente abrindo *https://seu-nome-de-host-mdm:porta-de-inscrição* (por exemplo, *https://eramdm:9980*) no seu navegador da web. Se a instalação for realizada com êxito, você verá a mensagem a seguir:



Você também pode usar este URL para verificar a disponibilidade do servidor do Conector de dispositivo móvel da internet (se estiver configurado de tal maneira), visitando-o a partir de um dispositivo móvel. Se você não conseguir acessar a página, verifique seu firewall e a configuração de sua infraestrutura de rede.

Pré-requisitos do conector de dispositivo móvel - Linux

Os pré-requisitos a seguir devem ser atendidos para instalar o Mobile Device Connector no Linux:

- Um servidor do banco de dados já está instalado e configurado com uma conta raiz (uma conta de usuário não precisa ser criada antes da instalação, o instalador pode criar a conta).
- Um driver ODBC para a conexão com o servidor do banco de dados (MySQL/Microsoft SQL) instalado no computador. Consulte o capítulo Instalação e configuração ODBC.

> Você deve usar o pacote `unixODBC_23` (não o `unixODBC` padrão) para que o MDC conecte ao banco de dados MySQL sem problemas. Isso é especialmente no caso de SUSE Linux.

> Recomendamos que você instale seu componente MDM em um dispositivo host separado daquele que é o host do Servidor ESET PROTECT.

- Arquivo de instalação MDMCore definido como um executável.

```
chmod +x mdmcore-linux-x86_64.sh
```

- Após a instalação, verifique se o serviço MDMCore está em execução.

```
sudo systemctl status eramdmcore
```

- Recomendamos que você **use a versão mais recente do OpenSSL1.1.1**. O Agente ESET Management é compatível com o OpenSSL 3.x. A versão mínima compatível do OpenSSL para Linux é openssl-1.0.1e-30. Podem existir mais versões do OpenSSL instaladas em um sistema simultaneamente. Pelo menos uma versão compatível deve estar presente no seu sistema.
  - Use o comando `openssl version` para exibir sua versão padrão atual.
  - Você pode listar todas as versões do OpenSSL presentes no seu sistema. Veja as terminações de nome de arquivo listadas usando o comando `sudo find / -iname *libcrypto.so*`
  - Você pode verificar se seu cliente Linux é compatível usando o comando a seguir: `openssl s_client -connect google.com:443 -tls1_2`

ESET PROTECTO Servidor/gerenciamento de dispositivo móvel não são compatíveis com o OpenSSL 3.x. O Agente ESET Management é compatível com o OpenSSL 3.x.

Se o seu banco de dados MDM no MySQL for muito grande (milhares de dispositivos) o valor padrão `innodb_buffer_pool_size` será muito pequeno. Para obter mais informações sobre a otimização de banco de dados, veja: https://dev.mysql.com/doc/refman/5.6/en/optimizing-innodb-diskio.html

Requisitos do certificado

• Você precisará de um **Certificado SSL** em formato *.pfx*para comunicação segura por HTTPS. Recomendamos que você use um certificado fornecido por uma Autoridade de certificação terceira. Certificados com assinatura própria (inclusive certificados assinados pela CA ESET PROTECT) não são recomendados porque nem todos os dispositivos móveis permitem que os usuários aceitem certificados com assinatura própria.

• Você precisa ter um certificado assinado por CA e a chave privada correspondente, e usar procedimentos padrão (tradicionalmente usando OpenSSL) para fazer a mesclagem deles em um arquivo *.pfx*:
`openssl pkcs12 -export -in certificate.cer -inkey privateKey.key -out httpsCredentials.pfx`
Este é o procedimento padrão para a maioria dos servidores que usam certificados SSL.

• Para Instalação off-line, você também precisará de um certificado de mesmo nível (o **Certificado de Agente** exportado do ESET PROTECT). Alternativamente, é possível usar seu certificado personalizado com o ESET PROTECT.

Ferramenta de imagem – Linux

Você é um usuário do Windows?

A ferramenta de imagem é necessária para atualizações off-line do mecanismo de detecção. Se os computadores do cliente não tiverem uma conexão à Internet e precisarem de atualizações do mecanismo de detecção, você pode usar a ferramenta de imagem para fazer download de arquivos de atualização dos servidores de atualização ESET e armazená-los localmente.

A Ferramenta de imagem tem as funções a seguir:
• Atualizações de módulo – faz o download de atualizações do mecanismo de detecção e outros módulos de programa, mas não das atualizações automáticas (uPCU).
• Criação do repositório – pode criar um repositório off-line completo, incluindo atualizações automáticas (uPCU).
A Ferramenta de imagem não faz download de dados do ESET LiveGrid®.

Pré-requisitos

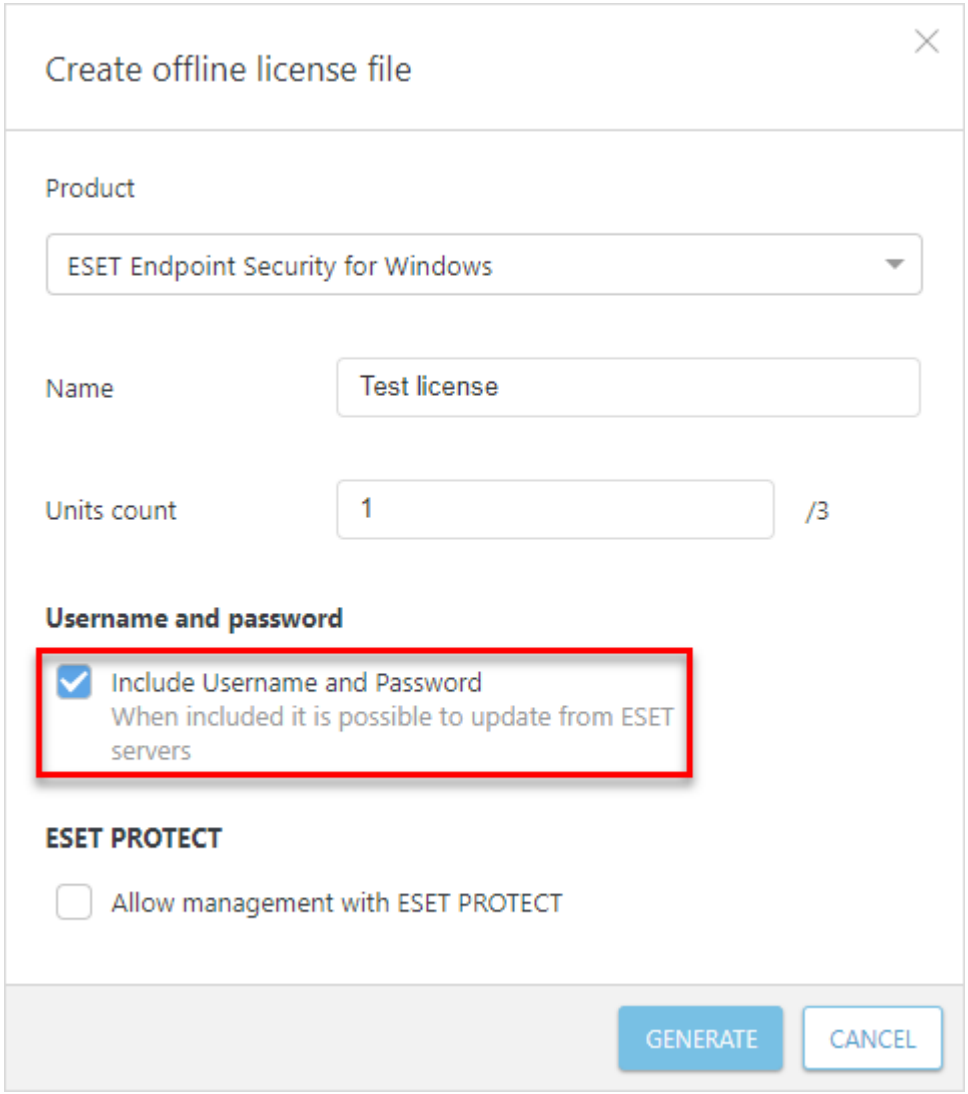
• O repositório onde a imagem é criada deve ter permissões de leitura e execução para todos os usuários. Execute este comando como um usuário privilegiado para conceder a permissão: `chmod 755 mirror/folder/path` (substitua o `mirror/folder/path` pelo caminho da pasta de imagem).

• A pasta de destino deve estar disponível para compartilhamento, serviço Samba/Windows ou HTTP/FTP, dependendo de como você quer que as atualizações sejam acessíveis.

- Produtos de Segurança ESET para Windows – podem ser atualizados remotamente usando HTTP ou uma pasta compartilhada.

- Produtos de Segurança ESET para Linux/macOS – podem ser atualizados remotamente apenas usando o HTTP. Se você usar uma pasta compartilhada, ela deve estar no mesmo computador que o produto de segurança ESET.

• Você deve ter um arquivo de Licença off-line válido incluindo o Nome de usuário e Senha. Ao gerar um arquivo de licença, certifique-se de selecionar a caixa de seleção ao lado de **Incluir Nome de Usuário e Senha**. Além disso, você deve digitar um **Nome** de licença. Um arquivo de licença off-line é necessário para a ativação da ferramenta de imagem e para gerar a imagem de atualização.



Como usar a Ferramenta de imagem

1.Faça o download da Ferramenta de imagem da página de download ESET (seção de **Instaladores autônomos**).

2.Descompacte o arquivo do download.

3.Abra o Terminal na pasta com o arquivo *MirrorTool* e faça com que o arquivo seja executável:

```
chmod +x MirrorTool
```

4.Execute o comando abaixo para ver todos os parâmetros disponíveis para a Ferramenta de imagem e sua versão:

```
./MirrorTool --help
```

```
root@ubuntu:/home/user/Desktop/x86_64/x86_64# ./MirrorTool --help
Mirror Tool v1.0.2226.0, Copyright (c) ESET, spol. s r.o. 1992-2021. All rights reserved.
Allowed options:
  --mirrorType arg                      [required for module update]
                                        Type of mirror. Possible values (case
                                        insensitive): regular, pre-release,
                                        delayed.
  --intermediateUpdateDirectory arg     [required for module update]
                                        Files will be downloaded to this
                                        directory to create mirror in output
                                        directory.
  --offlineLicenseFilename arg          [required for module update]
                                        Offline license file.
  --updateServer arg                    [optional]
                                        Update server. (e.g.:
                                        http://update.eset.com/eset_upd/ep6/)
                                        Mirror will be created in output
                                        directory, only specified path in
                                        server will be mirrored.
  --outputDirectory arg                 [required for module update]
                                        Directory where mirror will be created.
  --proxyHost arg                       [optional]
                                        Http proxy address (fqdn or IP).
  --proxyPort arg                       [optional]
                                        Http proxy port.
  --proxyUsername arg                   [optional]
                                        Http proxy username.
  --proxyPassword arg                   [optional]
                                        Http proxy password.
  --networkDriveUsername arg            [optional]
                                        Username used, when output directory is
                                        accessed using smb(e.g:\\hostname).
  --networkDrivePassword arg            [optional]
                                        Password used, when output directory is
                                        accessed using smb(e.g:\\hostname).
  --excludedProducts arg                [optional]
                                        Disable creating mirror for specified
                                        products. Use --listUpdatableProducts
                                        to see possible values.
  --listUpdatableProducts               Show list of all products which modules
                                        are downloaded by default.
  --repositoryServer arg                [required for repository update]
                                        Repository server for repository
                                        creation.
  --intermediateRepositoryDirectory arg [required for repository update]
                                        Files will be downloaded to this
                                        directory to create offline mirror in
                                        output directory.
  --outputRepositoryDirectory arg       [required for repository update]
                                        Directory where offline repository will
                                        be created.
  --trustDownloadedFilesInRepositoryTemp
                                        [optional]
                                        If set, hashes on already downloaded
                                        files are not checked.
  --mirrorOnlyLevelUpdates              [optional]
                                        If set, only level upgrades will be
                                        downloaded (nano/continuous updates
                                        will not be downloaded)
  --mirrorFileFormat arg                [optional]
                                        Specifies which type of update files
                                        will be downloaded. Possible values
                                        (case insensitive): dll, dat.
  --compatibilityVersion arg            [optional]
                                        Version of compatible products.
  --filterFilePath arg                  [optional]
                                        Path to filter file in json format.
                                        Parameter compatibilityVersion has to
                                        be higher than 7.1.0.0 to run program.
  --dryRun arg                          [optional]
                                        Specifies dry run of program with path
                                        to csv file where will be saved list of
                                        products to be downloaded with current
                                        filter configuration.
  --help                                [optional]
                                        Display this help and exit
```

Todos os filtros diferenciam maiúsculas e minúsculas.

Você pode usar os parâmetros para criar a imagem do repositório ou a imagem dos módulos:

Parâmetros para as imagens do repositório e dos módulos

--proxyHost
--proxyPort
--proxyUsername
--proxyPassword
--help

Parâmetros específicos do repositório

--repositoryServer
--intermediateRepositoryDirectory
--outputRepositoryDirectory
--compatibilityVersion
--dryRun
--filterFilePath
--trustDownloadedFilesInRepositoryTemp

Parâmetros específicos dos módulos

--mirrorType
--intermediateUpdateDirectory
--offlineLicenseFilename
--updateServer
--outputDirectory
--networkDriveUsername
--networkDrivePassword
--excludedProducts
--listUpdatableProducts
--mirrorOnlyLevelUpdates
--mirrorFileFormat

Parâmetro	Descrição
--updateServer	A Mirror Tool cria uma estrutura de pastas diferente da que é criada pela imagem do Endpoint. Cada pasta guarda arquivos de atualização para um grupo de produtos. ⚠ Você precisa especificar o link completo do servidor de atualização (caminho completo para a pasta correta) nas configurações de atualização do produto usando a imagem.
--offlineLicenseFilename	Você deve especificar um caminho para o arquivo de licença off-line (como mencionado acima).

Parâmetro	Descrição
`--mirrorOnlyLevelUpdates`	Nenhum argumento é necessário. Se estiver definido, será feito o download apenas das atualizações de nível (o download de atualizações nano não será feito). Leia mais sobre os tipos de atualização em nosso artigo da Base de conhecimento.
`--mirrorFileFormat`	⚠ Antes de usar o parâmetro `--mirrorFileFormat`, certifique-se de que o ambiente não contém as versões mais antigas (6.5 e versões anteriores) e mais recentes (6.6 e versões mais recentes) do produto de segurança ESET. O uso incorreto deste parâmetro pode resultar em atualizações incorretas de seus produtos de segurança ESET. Você pode especificar de qual tipo de arquivos de atualização será feito o download. Valores possíveis (diferencia maiúsculas de minúsculas): • `dat` – Use este valor se você tiver um ambiente apenas com versões de produto de segurança ESET da versão 6.5 e versões anteriores. • `dll` – Use este valor se você tiver um ambiente apenas com versões de produto de segurança ESET da versão 6.6 e versões posteriores. O parâmetro é ignorado ao criar uma imagem para produtos legados (`ep4`, `ep5`).
`--compatibilityVersion`	Este parâmetro opcional se aplica à Ferramenta de imagem distribuída com o ESET PROTECT 8.1 e versões posteriores. A Ferramenta de imagem vai fazer download de arquivos de atualização compatíveis com a versão do repositório ESET PROTECT que você especificar no argumento de parâmetro no formato `x.x` ou `x.x.x.x`, por exemplo: `--compatibilityVersion 10.1` ou `--compatibilityVersion 8.1.13.0`. O parâmetro `-compatibilidadeVersion` exclui as atualizações automáticas (uPCU) da imagem. Se você precisar das atualizações automáticas (uPCU) em seu ambiente e quiser diminuir o tamanho da imagem, use o parâmetro `--filterFilePath`.

ℹ Para reduzir a quantidade de dados com dowload feito do repositório ESET, recomendamos usar os novos parâmetros na Ferramenta de imagem distribuídos com o ESET PROTECT 9: `--filterFilePath` e `--dryRun`:
1.Crie um filtro em um formato *JSON* (veja `--filterFilePath` abaixo).
2.Realize um teste da Ferramenta de imagem com o parâmetro `--dryRun` (veja abaixo) e ajuste o filtro conforme necessário.
3.Execute a Ferramenta de imagem com o parâmetro `--filterFilePath` e o filtro de download definido, junto com os parâmetros `--intermediateRepositoryDirectory` e `--outputRepositoryDirectory`.
4.Execute a Ferramenta de imagem regularmente para sempre usar os instaladores mais recentes.

Parâmetro	Descrição

`--filterFilePath`	Use este parâmetro opcional para filtrar os produtos de segurança ESET com base em um arquivo de texto no formato *JSON* colocado na mesma pasta que a Ferramenta de imagem, por exemplo: `--filterFilePath filter.txt`)
	Descrição de configuração do filtro:
	O formato de arquivo de configuração para filtragem de produto é *JSON* com a estrutura a seguir:
	• objeto de raiz *JSON*:
	o`use_legacy` (booleano, opcional) – se for verdadeiro, os produtos legado serão incluídos.
	o`defaults` (objeto *JSON*, opcional) – define as propriedades de filtro que serão aplicadas a todos os produtos.
	■`languages` (lista) – especifica os códigos de idioma ISO dos idiomas a incluir, por exemplo, `"fr_FR"` para o tipo francês. Outros códigos de linguagem estão na tabela abaixo. Para selecionar mais linguagens, separe-as com uma vírgula e um espaço, por exemplo: (`["en_US", "zh_TW", "de_DE"]`)
	■`platforms` (lista) - plataformas a incluir (`["x64", "x86", "arm64"]`).
	⚠ Use o filtro `platforms` com cuidado. Por exemplo, se a Ferramenta de imagem fazer download de apenas instaladores de 64 bits e houver computadores de 32 bits na sua infraestrutura, os produtos de segurança ESET de 64 bits não serão instalados em computadores de 32 bits.
	■`os_types` (lista) – tipos de sistema operacional a incluir (`["windows"]`, `["linux"]`, `["mac"]`).
	o`products` (lista de objetos JSON, opcional) – filtros a aplicar em produtos específicos – anulam o `defaults` para produtos especificados. Os objetos têm as propriedades a seguir:
	■`app_id` (string) - necessário se `name` não estiver especificado.
	■`name` (string), necessário se `app_id` não estiver especificado.
	■`version` (string) - especifica a versão ou intervalo de versões a incluir.
	■`languages` (lista) - códigos de idioma ISO dos idiomas a incluir (consulte a tabela abaixo).
	■`platforms` (lista) - plataformas a incluir (`["x64", "x86", "arm64"]`).
	■`os_types` (lista) – tipos de sistema operacional a incluir (`["windows"]`, `["linux"]`, `["mac"]`).
	ℹ Para determinar os valores apropriados para os campos, execute a Ferramenta de imagem no modo de operação seca e encontre o produto relevante no arquivo CSV criado.
	Descrição do formato da string da versão
	Todos os números de versão são compostos por quatro números separados por pontos (por exemplo, `7.1.0.0`). Você pode especificar menos números ao escrever filtros de versão (por exemplo `7.1`) e o resto dos números será zero (`7.1` é igual a `7.1.0.0`).
	A string de versão pode ter um dos dois formatos a seguir:
	• [>|<|>=|<=|=]<n>.(<n>.(<n>.(<n>)))
	oSeleciona versões maiores/menores ou iguais/menores ou iguais/iguais do que a versão especificada.
	• <n>.(<n>.(<n>.(<n>))) - <n>.(<n>.(<n>.(<n>)))
	oSeleciona versões que são maiores que ou iguais ao limite inferior e menores que ou iguais ao limite superior.
	As comparações são feitas numericamente em cada parte do número da versão, da esquerda para a direita.
	Exemplo JSON
	✓
	`{`
	`"use_legacy": true,`
	`"defaults": {`
	`"languages": [ "en_US" ],`
	`"platforms": [ "x64", "x86" ]`
	`},`
	`"products": [`
	`{`
	`"app_id": "com.eset.apps.business.ees.windows",`
	`"version": "7.1.0.0–8.0.0.0"`
	`},`
	`{`
	`"app_id": "com.eset.apps.business.eea.windows",`
	`"version": ">7.1.0.0"`
	`}`
	`]`
	`}`
	O parâmetro `--filterFilePath` substitui os parâmetros `--languageFilterForRepository`, `--productFilterForRepository` e `--downloadLegacyForRepository` usados nas versões mais antigas da Ferramenta de imagem (lançadas com ESET PROTECT 8.x).

Parâmetro	Descrição
`--dryRun`	Quando você usa esse parâmetro opcional, a Ferramenta de imagem não vai fazer download de nenhum arquivo, mas vai gerar um arquivo *.csv* listando todos os pacotes que serão baixados. Você pode usar esse parâmetro sem os parâmetros obrigatórios `--intermediateRepositoryDirectory` e `--outputRepositoryDirectory`, por exemplo: • Windows: `MirrorTool.exe --repositoryServer AUTOSELECT --dryRun test.csv` • Linux: `sudo ./MirrorTool --repositoryServer AUTOSELECT --dryRun test.csv` ℹ Alguns instaladores da ESET são genéricos para o idioma (com o código de idioma `multilang`) e a Ferramenta de imagem vai listar esses instaladores no arquivo *.csv* mesmo se você especificar `idiomas` no `--filterFilePath`. Se você usar o parâmetro `--dryRun` e também os parâmetros `--intermediateRepositoryDirectory` e `--outputRepositoryDirectory`, a Ferramenta de imagem não limpa o *outputRepositoryDirectory*.
`--listUpdatableProducts`	Liste todos os produtos ESET para os quais o Mirror Tool pode fazer download de atualizações de módulo (a menos que o `--excludedProducts` que seja usado). O parâmetro está disponível a partir das versões Mirror Tool: 1.0.1294.0 (Windows), 1.0.2226.0 (Linux).

Estrutura da pasta da Mirror Tool

Por padrão, se você não especificar o parâmetro `--updateServer`, a Mirror Tool criará essa estrutura de pasta no seu servidor HTTP:

Não usar um servidor de imagem apenas HTTP

Certifique-se de que o servidor de imagem local usa os protocolos HTTP e HTTPS ou apenas HTTPS. Se o servidor de imagem usar apenas o HTTP, você não poderá usar a tarefa de cliente de Instalação de software porque o Acordo de Licença para o Usuário Final do produto de segurança ESET não pode ser recuperado de um servidor HTTP.

Pastas padrão da Mirror Tool	Produto de Segurança ESET	Servidor de atualização (de acordo com a localização raiz do seu servidor HTTP)
mirror/eset_upd/era6	A pasta de imagem *era6* é comum para as soluções de gerenciamento remoto da ESET: ERA 6, ESMC 7 e ESET PROTECT.	Para atualizar o ESET PROTECT 10.1 da imagem, defina o servidor de atualização como *http://your_server_address/mirror/eset_upd/era6*
mirror/eset_upd/ep[versão]	ESET Endpoint Antivirus/Security versão 6.x (e versões posteriores) para Windows. Cada versão principal tem sua pasta, por exemplo, *ep10* para a versão 10.x.	*http://your_server_address/mirror/eset_upd/ep10* (um exemplo para a versão 10.x)
mirror/eset_upd/v5	ESET Endpoint Antivirus/Security versão 5.x para Windows	*http://your_server_address/mirror/eset_upd/v5*

Produtos de Segurança ESET Linux/macOS

Você deve especificar o parâmetro `--updateServer` e criar pastas adicionais para atualizar os produtos de segurança ESET para Linux/macOS da imagem HTTP (veja abaixo).

--updateServer	Pasta adicional da Mirror Tool	Produto de Segurança ESET	Servidor de atualização (de acordo com a localização raiz do seu servidor HTTP)
http://update.eset.com/eset_upd/businesslinux	*mirror/eset_upd/*BusinessLinux	ESET Endpoint Antivirus para Linux	*http://your_server_address/mirror/eset_upd/BusinessLinux*
http://update.eset.com/eset_upd/serverlinux	*mirror/eset_upd/*LinuxServer	ESET Server Security para Linux	*http://your_server_address/mirror/eset_upd/LinuxServer*
http://update.eset.com/eset_upd/businessmac	*mirror/eset_upd/*BusinessMac	ESET Endpoint Security; versão 7.x+ para macOS	*http://your_server_address/mirror/eset_upd/BusinessMac*

Tabela de códigos de idioma

Para criar uma imagem, execute a Ferramenta de imagem com pelo menos os parâmetros mínimos necessários. Veja um exemplo:

```
sudo ./MirrorTool --mirrorType regular \
--intermediateUpdateDirectory /tmp/mirrorTool/mirrorTemp \
--offlineLicenseFilename /tmp/mirrorTool/offline.lf \
--outputDirectory /tmp/mirrorTool/mirror
```

Aqui está um exemplo de configuração mais avançada para um repositório off-line com os produtos selecionados, idiomas e download de arquivos legado ativado definidos no arquivo *filter.txt* (veja o exemplo de conteúdo do arquivo nos detalhes do `--filterFilePath` acima):

```
sudo ./MirrorTool --repositoryServer AUTOSELECT \
--intermediateRepositoryDirectory /tmp/repoTemp \
--outputRepositoryDirectory /var/lib/tomcat9/webapps/mirrorRepo \
--filterFilePath filter.txt
```

Recomendamos remover comandos contendo dados sensíveis (por exemplo, uma senha) do histórico da linha de comando:
1.Execute `history` para ver a lista de todos os comandos no histórico.
2.Execute `history -d line_number` (especifique o número da linha do comando). Alternativamente, execute `history -c` para remover todo o histórico da linha de comando.

Ferramenta de imagem e Configurações de atualização

- Para automatizar o download das atualizações de módulo, você pode criar um cronograma para executar a Ferramenta de imagem. Para fazer isso, abra seu console da Web e vá para **Tarefas de clientes** > **Sistema Operacional** > **Executar comando. Selecione** a **Linha de comando para execução** (incluindo um caminho para o *MirrorTool.exe*) e um acionador razoável (como o Cron para cada hora 0 0 * * * ? *). Alternativamente, você pode usar o Agendador de Tarefas do Windows ou `Cron` no Linux.

- Para configurar atualizações em um computador do cliente, crie uma nova política e configure **Servidor de Atualização** para apontar para o endereço da imagem ou pasta compartilhada.

Instalação de componente no macOS

Na maioria dos cenários de instalação, você precisa instalar vários componentes do ESET PROTECT em diferentes máquinas para acomodar diversas arquiteturas de rede, atender aos requisitos de desempenho ou por outros motivos.

O macOS é compatível somente como cliente. O Agente ESET Management e os produtos ESET para macOS podem ser instalados no macOS. Porém, o Servidor ESET PROTECT não pode ser instalado no macOS.

Instalação do Agente - macOS

Você pode instalar o Agente ESET Management no macOS de duas formas:

- Remotamente – usando a tarefa do servidor **implantação do Agente**. Caso você tenha problemas com a implementação do Agente ESET Management remotamente (a tarefa do servidor **implementação do agente** termina com um status com falha), consulte Solução de problemas para Implantação do agente.

- Localmente – veja as instruções abaixo.

Pré-requisitos

- ESET PROTECTServidor e o ESET PROTECTconsole da Web estão instalados (em um computador Servidor).

- Um certificado de Agente é criado e preparado no seu drive local.

- Uma Autoridade de certificação é preparada em sua unidade local (necessária apenas para certificados não assinados).

Instalação

Siga as etapas abaixo para instalar o componente do Agente ESET Management localmente no macOS:

Certifique-se de atender a todos os pré-requisitos de instalação listados acima.

1. Obtenha o arquivo de instalação (instalador de agente autônomo *.dmg*) do site de download da ESET ou do seu administrador do sistema.

2. Clique duas vezes no arquivo *Agent-MacOSX-x86_64.dmg* e clique duas vezes no arquivo *.pkg* para iniciar a instalação.

3. Continue com a instalação. Quando solicitado, digite os dados de **conexão do Servidor**:

- **Nome de host do servidor**: nome de host ou endereço IP do Servidor ESET PROTECT
- **Porta do servidor**: porta para comunicação Agente - Servidor, o padrão é 2222.
- **Usar Proxy**: clique se quiser usar o Proxy HTTP para a conexão Agente - Servidor.

Essa configuração de proxy é usada apenas para (replicação) entre o Agente ESET Management e o Servidor ESET PROTECT, não para o armazenamento em cache de atualizações.
- **Nome de host do Proxy**: nome de host ou endereço IP da máquina do Proxy HTTP.
- **Porta Proxy**: o valor padrão é 3128.
- **Nome de usuário**, **Senha**: insira as credenciais usadas pelo seu proxy se ele usar autenticação.

Você pode alterar as configurações de proxy mais tarde na sua política. O Proxy deve ser instalado antes de ser possível configurar uma conexão Agente - Servidor via Proxy.

4. Selecione um certificado de mesmo nível e uma senha para esse certificado. Como opção, você pode adicionar uma autoridade de certificação.

A senha do certificado não deve ter os seguintes caracteres: " \ Esses caracteres causam um erro crítico durante a inicialização do Agente.

5. Verifique o local de instalação e clique em **Instalar**. O Agente será instalado em seu computador.

6. Permitir acesso total ao disco para o Agente ESET Management:

Localmente:

a)Abra as **Preferências do sistema** > **Privacidade e segurança** > **Privacidade**.

b)Desbloqueie as configurações no canto inferior esquerdo.

c)Clique em **Acesso total ao disco**.

d)Clique em **+** > **Aplicativo** > **ESET** > **Abrir** e adicione o Agente ESET Management à lista de aplicativos na pasta de **Acesso total ao disco**.

e)Bloqueie as configurações no canto inferior esquerdo.

Remotamente:

a)Faça o download do arquivo de configuração da lista .plist.

b)Gere dois UUIDs com um gerador UUID de sua escolha e use um editor de texto para substituir cadeias de caracteres pelo texto. Insira seu UUID 1 e UUID 2 no perfil de configuração baixado.

c)Implante o arquivo do perfil de configuração .plist usando o servidor de gerenciamento de dispositivo móvel. Seu computador precisa estar inscrito no servidor de gerenciamento de dispositivo móvel para implantar perfis de configuração em computadores.

7. O computador com o Agente instalado vai aparecer no seu Web Console ESET PROTECT, e pode ser

gerenciado usando o ESET PROTECT.

Instalação e solução de problemas do Agente

Verifique se o Agente está em execução: Clique em **Ir** > **Utilitários** e clique duas vezes no **Monitor de atividade**. Clique na guia **Energia** ou na guia **CPU** e localize o processo chamado **ERAAgent**.

O relatório do Agente ESET Management pode ser encontrado aqui:

/Library/Application Support/com.eset.remoteadministrator.agent/Logs/
/Users/%user%/Library/Logs/EraAgentInstaller.log

O protocolo de comunicação entre o Agente e o Servidor ESET PROTECT não é compatível com a autenticação. Qualquer solução de proxy usada para encaminhar a comunicação do Agente para o Servidor ESET PROTECT e que precise de autenticação não funcionará.
Se você escolher usar uma porta não padrão para o console web ou Agente, poderá ser necessário fazer um ajuste de firewall. Caso contrário, a instalação poderá falhar.

Imagem ISO

Um arquivo de imagem ISO é um dos formatos nos quais você pode fazer download dos instaladores do ESET PROTECT (categoria de Instaladores Tudo-em-um). A imagem ISO contém o seguinte:

- ESET PROTECT Pacote de instalador
- Instaladores separados para cada componente

A imagem ISO é útil quando você quer manter todos os instaladores do ESET PROTECT em um só local. Ela também elimina a necessidade de download dos instaladores do site da ESET sempre que você precisar executar a instalação. A imagem ISO também é útil de se ter quando você precisa instalar o ESET PROTECT em uma máquina virtual.

Registro de serviço DNS

Para configurar um Registro de recurso DNS:

1.Em seu Servidor DNS (servidor DNS em seu controlador de domínio), acesse **Painel de controle** > **Ferramentas administrativas**.

2.Selecione o valor DNS.

3.No Gerenciador DNS, selecione _tcp da árvore e crie um novo registro **Localização do serviço (SRV)**.

4.Insira o nome do serviço no campo **Serviço** de acordo com as regras padrão de DNS, digite um símbolo de sublinhado (_) na frente do nome de serviço (use seu próprio nome de serviço, por exemplo, **_era**).

5.Digite o protocolo tcp no campo **Protocolo** no seguinte formato: _tcp.

6.Insira a porta 2222 no campo **Número da porta**.

7.Insira o FQDN (fully qualified domain name, nome de domínio totalmente qualificado) do Servidor ESET PROTECT no campo **Host oferecendo este serviço**.

8.Clique em **OK** > **Concluído** para salvar o registro. O registro será exibido na lista.

Para verificar o registro DNS:

1.Faça login em qualquer computador em seu domínio e abra um prompt de comando (cmd.exe).

2.Digite `nslookup` no prompt de comando e pressione **Enter**.

3.Digite `set querytype=srv` e pressione **Enter**.

4.Digite `_era._tcp.domain.name` e pressione **Enter**. A localização do serviço é exibida corretamente.

> Não se esqueça de alterar o valor "Host oferecendo este serviço:" para o FQDN de seu novo servidor quando instalar o Servidor ESET PROTECT em outra máquina.

Cenário de instalação off-line para ESET PROTECT

Para instalar o ESET PROTECT e seus componentes em ambientes sem acesso à internet, siga as instruções de instalação de alto nível (com o ESET PROTECT instalado no Windows).

Em um computador com conexão com a internet

1. Crie uma pasta de rede compartilhada.

2. Faça o download dos instaladores a seguir para a pasta compartilhada:

- Instalador tudo-em-um ESET PROTECT
- Um pacote JDK compatível (necessário para o Web Console).
- Instalador do agente ESET Management
- Instaladores do produto de segurança ESET (por exemplo: ESET Endpoint Security)

Em um computador Windows off-line na mesma rede local

1. Copie os instaladores da pasta compartilhada de rede para um computador Windows off-line onde você deseja instalar o ESET PROTECT.

2. Instale o pacote JDK.

3. Instale o ESET PROTECT no Windows usando o Instalador tudo-em-um. Escolha **Ativar mais tarde** durante a instalação.

4. Ative o ESET PROTECT com uma licença off-line.

5. Implante o Agente ESET Management em computadores em seu ambiente off-line através do Script do agente instalador. Modifique o script de instalação para usar o novo URL para acessar o pacote de instalação

do agente da pasta de rede compartilhada.

6. Implante os produto de segurança ESET em estações de trabalho usando uma Tarefa de instalação de software. Selecione **<Choose package>** e forneça um URL personalizado para o pacote de instalação do repositório local.

7. Ativar endpoints gerenciados com uma licença off-line.

8. Desativar o ESET LiveGrid®.

Recomendamos fortemente manter a infraestrutura off-line ESET atualizada usando um repositório de atualização local. Atualize os módulos do produto de segurança ESET regularmente. Se os módulos não estiverem atualizados, o Web Console ESET PROTECT sinaliza os computadores como **Não atualizados**. Para silenciar este aviso do Web Console, clique no computador na lista e selecione **Mudo** no menu de contexto.

Para instruções para atualizar o ESET PROTECT, veja Atualizar componentes ESET PROTECT em ambiente off-line.

Procedimentos de atualização

Existem formas diferentes de atualizar seu Servidor ESET PROTECT e outros componentes ESET PROTECT. Veja também os procedimentos de migração e reinstalação.

Certifique-se de que você tem um sistema operacional compatível antes de atualizar para o ESET PROTECT 10.1.
Recomendamos que você faça backup do banco de dados ESET PROTECT antes de atualizar.
Se você tiver um banco de dados incompatível mais antigo instalado (MySQL 5.5 ou Microsoft SQL 2008/2012), atualize seu banco de dados para uma versão de banco de dados compatível antes de atualizar o Servidor ESET PROTECT.

Atualizar do ERA 5.x/6.5 ou ESMC 7.0/7.1

Se você tiver o ERA 5.x/6.x ou o ESMC 7.0/7.1:

- A atualização direta para ESET PROTECT 10.1 o não é compatível.
- Realize uma instalação limpa do ESET PROTECT 10.1.

Você pode atualizar diretamente para o ESET PROTECT 10.1 do ESMC 7.2 e de versões posteriores.

Atualize do ESMC 7.2 ou uma versão anterior do ESET PROTECT para ESET PROTECT 10.1

Selecione um dos procedimentos de atualização:

Procedimentos de atualização	Sistema operacional	Comentário
Tarefa de Atualização de componentes no Web Console	Windows/Linux	Você pode atualizar para o ESET PROTECT 10.1 usando a tarefa de Atualização de componentes do ESET PROTECT 8.0 e versões posteriores. Se você tiver o ESMC 7.2, você deve atualizar usando a tarefa de Atualização de componentes em duas etapas: primeiro para o ESET PROTECT 10.0, e depois do 10.0 para o 10.1.
Instalador tudo-em-um ESET PROTECT 10.1	Windows	O Instalador tudo-em-um é a opção de atualização recomendada se a instalação existente foi realizada por meio do Instalador tudo-em-um (você tem instalações padrão do banco de dados Microsoft SQL e do Apache Tomcat).
Atualização manual baseada em componente	Linux	Instruções do Linux para usuários avançados.
Atualizar a Máquina virtual ESET PROTECT	(Equipamento virtual) Linux	

Para pesquisar qual versão de cada componente ESET PROTECT você está executando, verifique qual é sua versão do Servidor ESET PROTECT. Vá para a página Sobre no Web Console ESET PROTECT e veja a lista de todas as versões componentes do ESET PROTECT.

Tarefa de Atualização de componentes ESET PROTECT

Recomendações antes da atualização

Recomendamos usar a tarefa ESET PROTECT Atualização de componentes disponível no console web ESET PROTECT para atualizar sua infraestrutura ESET PROTECT. Revise cuidadosamente as instruções aqui antes de atualizar.

Se a atualização de componentes falhar em uma máquina executando o Servidor ESET PROTECT ou o console web, pode não ser possível fazer login no console web remotamente. Recomendamos que você configure o acesso físico para a máquina do servidor antes de realizar esta atualização. Se não for possível obter acesso físico à máquina, certifique-se de que você pode fazer login nela com privilégios administrativos usando a área de trabalho remota. Recomendamos que você faça backup dos seus banco de dados do Servidor ESET PROTECT e Conector de dispositivo móvel antes de realizar esta operação. Para fazer backup do seu Equipamento Virtual, crie um instantâneo ou clone sua máquina virtual.

Você está fazendo a atualização do ESMC Máquina virtual ?

A instância do Servidor ESET PROTECT está instalada em um cluster de failover?

Se a sua instância do servidor ESET PROTECT estiver instalada em um agrupamento de failover, é preciso atualizar o componente do servidor ESET PROTECT de cada nó de agrupamento manualmente. Depois de atualizar o Servidor ESET PROTECT, execute a tarefa de Atualização de componentes para atualizar o resto da sua infraestrutura (por exemplo, Agente ESET Management em computadores do cliente).

Você pode atualizar para o ESET PROTECT 10.1 usando a tarefa de Atualização de componentes do ESET PROTECT 8.0 e versões posteriores. Se você tiver o ESMC 7.2, você deve atualizar usando a tarefa de Atualização de componentes em duas etapas: primeiro para o ESET PROTECT 10.0, e depois do 10.0 para o 10.1.

O ESET PROTECT notifica automaticamente quando uma nova versão do Servidor ESET PROTECT está disponível.

Faça o back-up dos dados a seguir antes de executar a atualização:

- Todos os certificados (Autoridade de certificação, Certificado de servidor, Certificado de proxy e agente)
- Exporte seus Certificados da Autoridade de Certificação de um Servidor ESET PROTECT antigo para um arquivo *.der* e salve em um armazenamento externo.
- Exporte seus Certificados de mesmo nível (para o Agente ESET Management, Servidor ESET PROTECT) e arquivo de chave privada *.pfx* de um antigo Servidor ESET PROTECT e salve em um armazenamento externo.
- Seu banco de dados ESMC/ESET PROTECT. Se você tiver um banco de dados incompatível mais antigo instalado (MySQL 5.5 ou Microsoft SQL 2008/2012), atualize seu banco de dados para uma versão de banco de dados compatível antes de atualizar o Servidor ESET PROTECT.

Certifique-se de que você tem um sistema operacional compatível antes de atualizar para o ESET PROTECT 10.1.

Para atualizar os produtos de segurança ESET, execute a tarefa de Instalação de software usando o pacote do instalador mais recente para instalar a versão mais recente sobre seu produto existente.

Procedimento de atualização recomendado

1. Atualizar o Servidor ESET PROTECT – selecione apenas a máquina com o Servidor ESET PROTECT como destino para a tarefa de **Atualização de componentes do ESET PROTECT**.

2. Selecione alguns computadores cliente (como uma amostra de teste: pelo menos um cliente de cada sistema operacional e capacidade de bits) e execute neles a tarefa de **Atualização de componentes do ESET PROTECT**.

Recomendamos usar o ESET Bridge Proxy HTTP (ou qualquer outro proxy da web transparente com armazenamento em cache ativado) para limitar a carga de rede. As máquinas de teste do cliente vão acionar o download/armazenamento em cache dos instaladores. Quando a tarefa for executada novamente, os instaladores serão distribuídos aos computadores clientes diretamente do cache.

3. Depois que os computadores com o Agente ESET Management atualizado estiverem se conectando com sucesso ao Servidor ESET PROTECT, continue com a atualização do resto dos clientes.

Para atualizar os Agentes ESET Management em todos os computadores gerenciados na rede, selecione o Grupo estático **Todos** como destino para a tarefa de **Atualização de componentes do ESET PROTECT**. A tarefa vai ignorar computadores que já executaram o Agente ESET Management mais recente.
O ESET PROTECT é compatível com a atualização automática de Agentes ESET Management em computadores gerenciados.

Componentes atualizados automaticamente:

- ESET PROTECTServidor
- Agente ESET Management
- Console web ESET PROTECT – aplicável apenas quando o Apache Tomcat foi instalado em sua pasta de instalação padrão nas distribuições do Windows e Linux, inclusive a Máquina virtual ESET PROTECT (por exemplo: */var/lib/tomcat8/webapps/*, */var/lib/tomcat7/webapps/*, */var/lib/tomcat/webapps/*).

Limitações de atualização do Web Console

- O Apache Tomcat não é atualizado durante a atualização do console web ESET PROTECT por meio da tarefa de Atualização de componentes.
- A atualização do console web ESET PROTECT não funcionará se o Apache Tomcat foi instalado em um local personalizado.
- Se uma versão personalizada do Apache Tomcat estiver instalada (instalação manual do serviço Tomcat), a atualização subsequente do Web Console ESET PROTECT por meio do Instalador tudo-em-um ou da Tarefa de atualização de componentes não será compatível.

- ESET PROTECT Mobile Device Connector

Componentes que exigem uma atualização manual:

Componentes ESET

- ESET Rogue Detection Sensor – use a tarefa de Instalação de software para a atualização. Alternativamente, instale a versão mais recente em uma versão anterior (siga as instruções de instalação para Windows ou Linux). Se você instalou o RD Sensor com um ESMC 7.2 e versões posteriores ele não precisará ser atualizado, já que não há novos lançamentos do RD Sensor.

Componentes de terceiros

Além dos componentes ESET, o ESET PROTECT usa componentes de terceiros que precisam de uma atualização manual.

No Web Console ESET PROTECT, clique em **Links rápidos** > **Componentes do servidor** para ver componentes de terceiros com uma versão posterior disponível.

- Recomendamos instalar a versão mais recente de componentes de terceiros assim que possível. A versão mais recente disponível pode variar com base no sistema operacional usado para executar o Servidor ESET PROTECT.
- A Máquina virtual ESET PROTECT não reporta atualizações disponíveis para componentes de terceiros.

O Web Console ESET PROTECT recomenda uma atualização para versões anteriores às listadas abaixo:

Componente de terceiros:	Versão:	Observações:	Instruções de atualização
Microsoft SQL Server	2019 (compilação 15.0.4312.0)	Determine sua versão e edição do Mecanismo de banco de dados do SQL Server e instale a atualização cumulativa mais recente.	Servidor do banco de dados
MySQL	8.0.0.0	Clique em **Ajuda** > **Sobre** no Web Console ESET PROTECT para ver a versão do banco de dados instalado.	Servidor do banco de dados
Sistema operacional	Windows Server 2016	O ESET PROTECT não reporta as atualizações disponíveis para o Linux.	Sistema operacional
Apache Tomcat	9.0.73	Determine a versão instalada do Apache Tomcat: • Windows – navegue até *C:\Program Files\Apache Software Foundation\[Tomcat pasta]* e abra o arquivo *RELEASE-NOTES* em um editor de texto para verificar o número da versão. • Linux – execute o comando Terminal: `tomcat version`	Apache Tomcat
Java	17.0	Determine a versão instalada do Java: • Windows – abra o prompt de comando e execute: `java -version` • Linux – execute o comando Terminal: `java -version`	Java Runtime Environment
Apache HTTP Proxy	-	**Apache HTTP Proxy usuários** Começando com o ESET PROTECT 10.0, o ESET Bridge substitui o Apache HTTP Proxy. O Apache HTTP Proxy agora está com Suporte limitado. Se você usar o Apache HTTP Proxy, recomendamos migrar para o ESET Bridge.	Migrar para o ESET Bridge

O componente do Gerenciamento de dispositivo móvel/Conector ESET PROTECT (MDM/MDC) (apenas no local) teve seu fim da vida útil agendado. Ler mais. Recomendamos que você migre para o gerenciamento de dispositivo móvel em nuvem.

Solução de problemas

• Verifique se você pode acessar o repositório ESET PROTECT de um computador atualizado.

• Executar novamente a tarefa de Atualização de componentes ESET PROTECT não vai funcionar se houver no mínimo um componente já atualizado para uma versão mais nova.

• Se o Web Console ESET PROTECT não carregar ou se você ver um erro durante o login, consulte a solução de problemas do Web Console.

• Se não houver um motivo claro para a falha, você pode atualizar os componentes manualmente. Veja nossas instruções para o Windows ou Linux.

• Veja informações gerais para solução de problemas para obter mais sugestões para resolver os problemas de atualização.

Use o instalador Tudo-em-um ESET PROTECT 10.1 para atualizar

Use o Instalador tudo-em-um ESET PROTECT 10.1 para atualizar o ESMC 7.2 ou uma versão mais antiga do ESET PROTECT para a versão ESET PROTECT 10.1 mais recente.

O Instalador tudo-em-um é a opção de atualização recomendada se a instalação existente foi realizada por meio do Instalador tudo-em-um (você tem instalações padrão do banco de dados Microsoft SQL e do Apache Tomcat).

O instalador único ESET PROTECT 10.1 instala o Microsoft SQL Server Express 2019 por padrão.

- Se você estiver usando uma versão mais antiga do Windows (Server 2012 ou SBS 2011), o Microsoft SQL Server Express 2014 será instalado por padrão.

- O instalador gera automaticamente uma senha aleatória para autenticação de banco de dados (armazenada em *%PROGRAMDATA%\ESET\RemoteAdministrator\Server\EraServerApplicationData\Configuration\startupconfiguration.ini*).

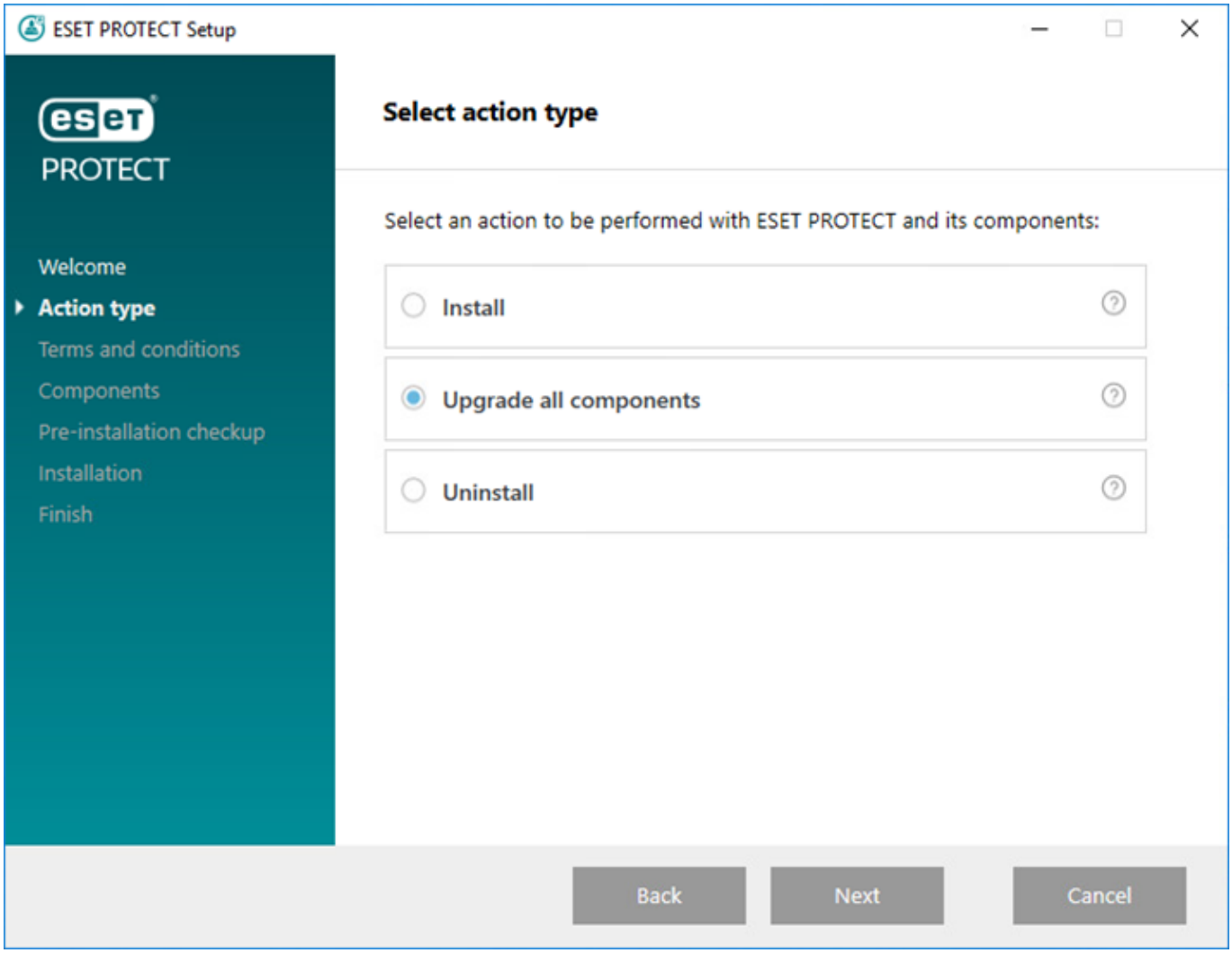
O Microsoft SQL Server Express tem um limite de tamanho de 10 GB de cada banco de dados relacional. Não recomendamos usar o Microsoft SQL Server Express:
- Em ambientes empresariais ou grandes redes.
- Se quiser usar o ESET PROTECT com o ESET Inspect.

Você pode atualizar diretamente para o ESET PROTECT 10.1 do ESMC 7.2 e versões posteriores.
Faça o back-up dos dados a seguir antes de executar a atualização:
• Todos os certificados (Autoridade de certificação, Certificado de servidor, Certificado de proxy e agente)
• Exporte seus Certificados da Autoridade de Certificação de um Servidor ESET PROTECT antigo para um arquivo *.der* e salve em um armazenamento externo.
• Exporte seus Certificados de mesmo nível (para o Agente ESET Management, Servidor ESET PROTECT) e arquivo de chave privada *.pfx* de um antigo Servidor ESET PROTECT e salve em um armazenamento externo.
• Seu banco de dados ESMC/ESET PROTECT. Se você tiver um banco de dados incompatível mais antigo instalado (MySQL 5.5 ou Microsoft SQL 2008/2012), atualize seu banco de dados para uma versão de banco de dados compatível antes de atualizar o Servidor ESET PROTECT.
Certifique-se de que você tem um sistema operacional compatível antes de atualizar para o ESET PROTECT 10.1.

1.Execute o *Setup.exe*.

2.Selecione o idioma e clique em **Avançar**.

3.Selecione **Atualizar todos os componentes** e clique em **Avançar**.



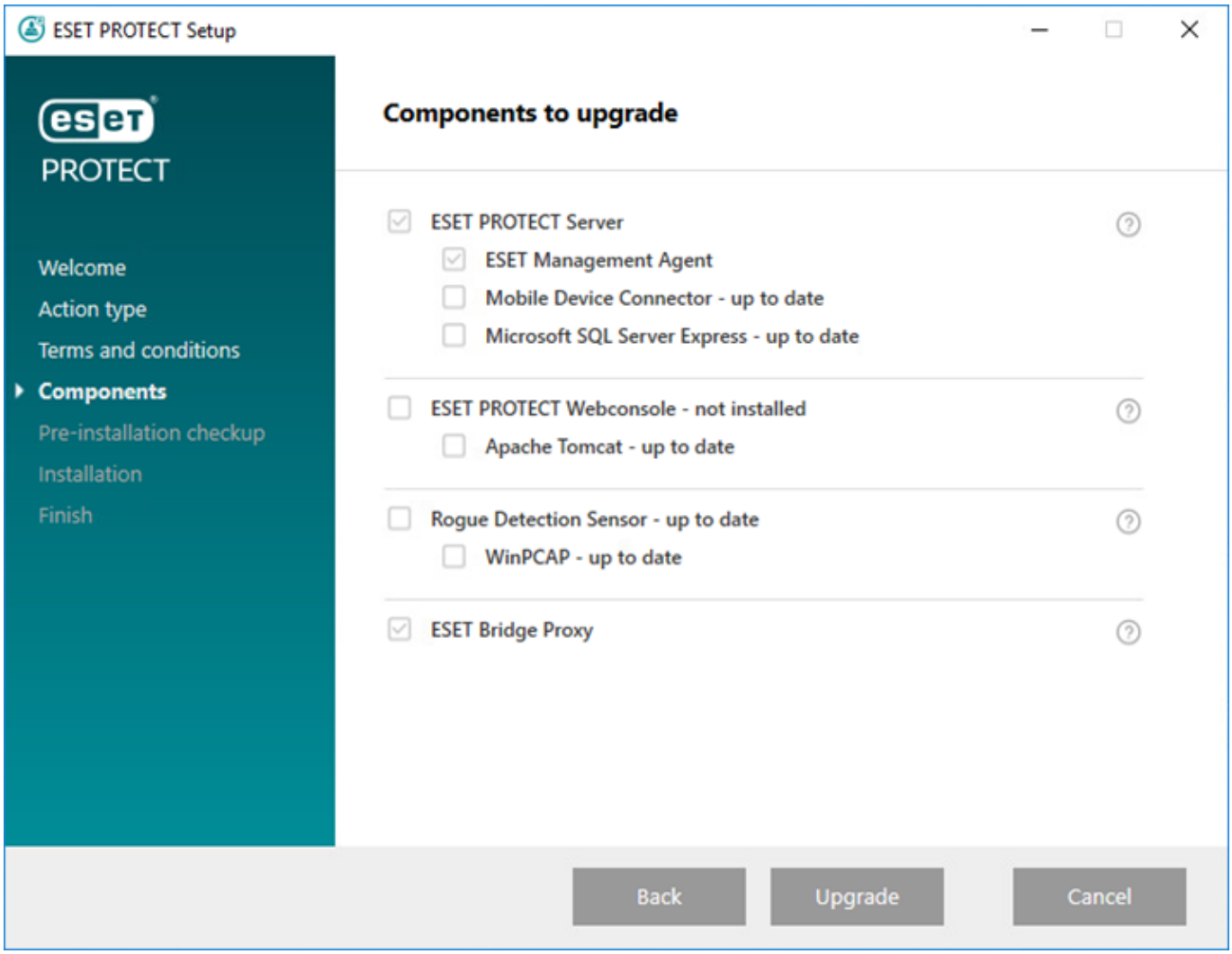
4.Leia o **Acordo de Licença para o Usuário Final**, aceite-o e clique em **Avançar**.

5.Em **Componentes**, revise os componentes do ESET PROTECT que podem ser atualizados e clique em **Avançar**.

Limitações de atualização do Apache Tomcat e Web Console

- Se uma versão personalizada do Apache Tomcat estiver instalada (instalação manual do serviço Tomcat), a atualização subsequente do Web Console ESET PROTECT por meio do Instalador tudo-em-um ou da Tarefa de atualização de componentes não será compatível.
- Atualizar o Apache Tomcat removerá a pasta *era* localizada em *C:\Program Files\Apache Software Foundation\[Tomcat pasta]\webapps*. Se você estiver usando a pasta *era* para armazenar dados adicionais, certifique-se de fazer um backup dos dados antes de atualizar.
- Se *C:\Program Files\Apache Software Foundation\[Tomcat pasta]*O *webapps* contém dados adicionais (além das pastas *era* e *ROOT*), a atualização do Apache Tomcat não acontecerá e apenas o console web será atualizado.
- A atualização do Web Console e Apache Tomcat limpa os arquivos da Ajuda off-line. Se você usou a ajuda off-line com o ESMC ou com uma versão mais antiga do ESET PROTECT, crie novamente a ajuda para o ESET PROTECT 10.1 depois da atualização para garantir que você tenha a ajuda off-line mais recente conforme sua versão do ESET PROTECT.

Se você executar o instalador tudo-em-um em uma máquina Windows com o Apache HTTP Proxy instalado, o instalador irá desinstalar o Apache HTTP Proxy e instalar o ESET Bridge automaticamente.



6.Siga a **Verificação pré-instalação** para certificar-se de que seu sistema atenda a todos os pré-requisitos.

7.Clique em **Atualizar** para iniciar a atualização ESET PROTECT. A atualização pode levar algum tempo, dependendo do seu sistema e configuração de rede.

8.Quando a atualização for concluída, clique em **Concluir**.

9.Depois de atualizar o ESET PROTECT, atualize o Agente ESET Management em computadores gerenciados usando a tarefa Atualização de componentes. O ESET PROTECT é compatível com a atualização automática de Agentes ESET Management em computadores gerenciados.

Backup/atualização do servidor do banco de dados

ESET PROTECT usa um banco de dados para armazenar dados do cliente. As seções a seguir detalham o backup e a atualização do banco de dados do Servidor ESET PROTECT (ou Servidor ESMC) ou banco de dados MDM:

- Se você não tiver um banco de dados configurado para usar com o Servidor ESET PROTECT, o **Microsoft SQL Server Express** está incluído com o instalador. O instalador único ESET PROTECT 10.1 instala o Microsoft SQL Server Express 2019 por padrão.

  - Se você estiver usando uma versão mais antiga do Windows (Server 2012 ou SBS 2011), o Microsoft SQL Server Express 2014 será instalado por padrão.

  - O instalador gera automaticamente uma senha aleatória para autenticação de banco de dados (armazenada em *%PROGRAMDATA%\ESET\RemoteAdministrator\Server\EraServerApplicationData\Configuration\startupconfiguration.ini*).

> ⚠ O Microsoft SQL Server Express tem um limite de tamanho de 10 GB de cada banco de dados relacional. Não recomendamos usar o Microsoft SQL Server Express:
> - Em ambientes empresariais ou grandes redes.
> - Se quiser usar o ESET PROTECT com o ESET Inspect.

- Se você tiver um banco de dados incompatível mais antigo instalado (MySQL 5.5 ou Microsoft SQL 2008/2012), atualize seu banco de dados para uma versão de banco de dados compatível antes de atualizar o Servidor ESET PROTECT.

Veja também migração de banco de dados ESET PROTECT.

Os seguintes requisitos para o Microsoft SQL Server devem ser atendidos:

- Instale uma versão compatível do Microsoft SQL Server. Escolha a autenticação em **Modo misturado** durante a instalação.

- Se você já tiver o Microsoft SQL Server instalado, defina a autenticação para o **Modo misturado (autenticação do SQL Server e autenticação Windows)**. Para fazer isso, siga as Instruções neste artigo da Base de conhecimento. Se quiser usar a **Autenticação do Windows** para entrar no Microsoft SQL Server, siga as etapas neste artigo da Base de conhecimento.

- Permitir conexões TCP/IP ao SQL Server. Para isso, siga as instruções neste artigo da Base de conhecimento da parte **II. Permitir conexões TCP/IP ao banco de dados SQL**.

- Para configurar, gerenciar e administrar o Microsoft SQL Server (banco de dados e usuários), faça o download do SQL Server Management Studio (SSMS).
- Não instale o SQL Server em um controlador de domínio (por exemplo, Windows SBS/Essentials). Recomendamos que instale o ESET PROTECT em outro servidor ou não selecione o componente SQL Server Express durante a instalação (isso requer que você use seu Servidor SQL ou MySQL existente para executar o banco de dados ESET PROTECT).

Backup e restauração do servidor de banco de dados

Todas as informações e configurações do ESET PROTECT estão armazenadas no banco de dados. Recomendamos que você faça backup de seu banco de dados regularmente para evitar a perda de dados. Você pode usar o backup mais tarde, ao migrar o ESET PROTECT para um novo servidor. Consulte a seção apropriada a seguir de seu banco de dados:

- Os nomes dos bancos de dados e relatórios continuam iguais mesmo depois da mudança do nome do produto de ESET Security Management Center para ESET PROTECT.
- Se você usar a Máquina virtual ESET PROTECT, siga as instruções de backup do banco de dados VA.

Exemplos de backup Microsoft SQL

Para fazer o backup um banco de dados Microsoft SQL para um arquivo, siga o exemplo mostrado abaixo:

Estes exemplos são destinados ao uso com as configurações padrão (por exemplo, nome do banco de dados e configurações de conexão de banco de dados padrões). Seu script de backup precisará ser personalizado para acomodar todas as alterações feitas nas configurações padrão.
Você precisará de direitos suficientes para executar os comandos abaixo. Se você não usar uma conta de usuário administrador local, será preciso alterar o caminho de backup, por exemplo, para *'C:\USERS\PUBLIC\BACKUPFILE'*.

Backup do banco de dados único

Execute este comando em um prompt de comando do Windows para criar um backup no arquivo chamado de **BACKUPFILE**:

```
SQLCMD -S HOST\ERASQL -
Q "BACKUP DATABASE ERA_DB TO DISK = N'C:\USERS\ADMINISTRATOR\DESKTOP\BACKUPFILE'"
```

Neste exemplo **HOST** significa o endereço IP ou nome de host e **ERASQL** significa o nome da instância do servidor Microsoft SQL. Você pode instalar o Servidor ESET PROTECT em uma instância SQL com nome personalizado (ao usar o banco de dados Microsoft SQL). Modificar scripts de backup de acordo nesse cenário.

Backup regular de banco de dados com o script SQL

Escolha um dos scripts SQL a seguir:

a)Criar backups regulares e armazená-los com base na data de criação:

```
@ECHO OFF
```

```
SQLCMD.EXE -S HOST\ERASQL -d ERA_DB -E -
Q "BACKUP DATABASE ERA_DB TO DISK = N'C:\USERS\ADMINISTRATOR\DESKTOP\BACKUPFILE'

  WITH NOFORMAT,INIT, NAME = N'ERA_DB', SKIP, NOREWIND, NOUNLOAD, STOP_ON_ERROR, CHE
CKSUM, STATS=10"


REN BACKUPFILE BACKUPFILE-
[%DATE:~10,4%%DATE:~4,2%%DATE:~7,2%_T%TIME:~0,2%%TIME:~3,2%].bac
```

b)Anexar seu backup a um arquivo:

```
@ECHO OFF


SQLCMD.EXE -S HOST\ERASQL -d ERA_DB -E -
Q "BACKUP DATABASE ERA_DB TO DISK = N'C:\USERS\ADMINISTRATOR\DESKTOP\BACKUPFILE'

   WITH NOFORMAT, NOINIT, NAME = N'ERA_DB', SKIP, NOREWIND, NOUNLOAD, STOP_ON_ERROR,
 CHECKSUM, STATS=10"
```

Restaurar Microsoft SQL

Para restaurar um banco de dados Microsoft SQL de um arquivo, siga o exemplo mostrado abaixo:

```
SQLCMD.EXE -S HOST\ERASQL -d ERA_DB -E -
Q "RESTORE DATABASE ERA_DB FROM DISK = N'C:\USERS\ADMINISTRATOR\DESKTOP\BACKUPFILE'"
```

Backup MySQL

Para fazer o backup um banco de dados MySQL para um arquivo, siga o exemplo mostrado abaixo:

```
mysqldump --host HOST --disable-keys --extended-insert --routines -u ROOTLOGIN -
p DBNAME -r BACKUPFILE
```

Neste exemplo **HOST** significa o endereço IP ou nome de host do servidor MySQL, **ROOTLOGIN** significa a conta raiz do Servidor MySQL e **DBNAME** significa o nome do banco de dados ESET PROTECT.

Restaurar MySQL

Para restaurar um banco de dados MySQL de um arquivo, siga o exemplo mostrado abaixo:

```
mysql --host HOST -u ROOTLOGIN -p DBNAME < BACKUPFILE
```

Para mais informações sobre o backup do Microsoft SQL Server, visite o site techNet da Microsoft. Para mais informações sobre o backup do servidor MySQL, visite o site da documentação MySQL.

Atualização do servidor do banco de dados

Siga as instruções abaixo para atualizar uma instância existente do servidor de banco de dados para uma versão mais recente para uso com o banco de dados do servidor ESET PROTECT:

1. Pare todos os serviços do servidor ESMC/ESET PROTECT ou Proxy em execução conectados ao servidor do banco de dados que você vai atualizar. Além disso, interrompa qualquer outro aplicativo que possa estar se conectando à sua instância do servidor do banco de dados.

2. Faça backup de todos os banco de dados relevantes com segurança antes de continuar.

3. Realize a atualização do servidor de banco de dados:

SQL Server (Windows):

- Siga o artigo da Base de conhecimento para atualizar o banco de dados Microsoft SQL Express para a versão mais recente.
- Alternativamente, siga as instruções do fabricante do banco de dados: https://msdn.microsoft.com/en-us/library/bb677622.aspx.
- O Microsoft SQL Server para Linux não é compatível. Mas você pode conectar o Servidor ESET PROTECT no Linux ao Microsoft SQL Server no Windows.

MySQL Server (Windows e Linux):

- Atualizar do MySQL 5.6 para a versão 5.7
- Atualizar do MySQL 5.7 para a versão 8

4. Inicie o serviço do servidor ESET PROTECT e verifique seus relatórios de traço para verificar se a conexão do banco de dados está funcionando corretamente.

Atualizar ESMC/ESET PROTECT instalado no Cluster de Failover no Windows

Se você tem um Servidor ESMC/ESET PROTECT instalado em um ambiente de Cluster de Failover no Windows, siga as etapas abaixo para atualizar para o ESET PROTECT mais recente:

Certifique-se de ter um sistema operacional compatível.

1. Pare a função de agrupamento do Servidor ESMC/ESET PROTECT no Gerenciador de agrupamento. Certifique-se de que o serviço (**ESET Security Management Center Server** ou **ESET PROTECT Server**) é interrompido em todos os nós do cluster.

2. Coloque o disco compartilhado de cluster on-line no nó 1 e atualize o componente do Servidor manualmente executando o instalador *.msi* mais recente, como no caso de uma instalação de componente.

3. Depois do fim da instalação (atualização), certifique-se de que o serviço **ESET PROTECT Server** é interrompido.

4. Coloque o disco compartilhado do cluster on-line no nó 2 e atualize o componente do Servidor da mesma

forma que é feita na etapa 2.

5. Assim que um Servidor ESET PROTECT for atualizado em todos os nós de agrupamento, inicie a **Função do Servidor ESET PROTECT** no Gerenciador de agrupamento.

6. Atualize o Agente ESET Management manualmente executando o instalador *.msi* mais recente em todos os nós do agrupamento.

7. No Console da Web ESET PROTECT verifique se as versões do Agente e do Servidor de todos os nós reportam para a versão mais recente para a qual você atualizou.

Atualizar o Apache Tomcat

O Apache Tomcat é um componente obrigatório necessário para executar o console web ESET PROTECT.

Se você estiver atualizando para a versão mais recente do ESET PROTECT, ou se você não atualizou o Apache Tomcat por um longo período de tempo, você deve considerar atualizar o Apache Tomcat para a versão mais recente. Manter atualizados serviços voltados ao público, incluindo o Apache Tomcat e suas dependências, vai diminuir os riscos de segurança para seu ambiente.

Para atualizar o Apache Tomcat, siga as instruções:

- Instruções do Windows (o Instalador tudo-em-um ESET PROTECT mais recente) – Essa é a opção de atualização recomendada se a instalação do Apache Tomcat existente foi realizada usando o Instalador tudo-em-um.
- Instruções do Windows (instalação manual) – Atualize o Apache Tomcat manualmente se você realizou a instalação existente Apache Tomcat manualmente ou se você não tem o Instalador Tudo-em-um ESET PROTECT mais recente.
- Instruções do Linux

Atualizar o Apache Tomcat usando o Instalador tudo-em-um (Windows)

O Apache Tomcat é um componente obrigatório necessário para executar o console web ESET PROTECT. Use este método para atualizar o Apache Tomcat usando o Instalador tudo-em-um ESET PROTECT 10.1 mais recente. Essa é a opção de atualização recomendada se a instalação do Apache Tomcat existente foi realizada usando o Instalador tudo-em-um. Alternativamente, você pode atualizar o Apache Tomcat manualmente.

Antes de atualizar

Faça o backup dos arquivos a seguir:

C:\Program Files\Apache Software Foundation\[Tomcat pasta]\.keystore
C:\Program Files\Apache Software Foundation\[Tomcat pasta]\conf\server.xml
C:\Program Files\Apache Software Foundation\[Tomcat pasta]\webapps\era\WEB-INF\classes\sk\eset\era\g2webconsole\server\modules\config\EraWebServerConfig.properties

Se estiver usando um depósito de certificado SSL personalizado na pasta *Tomcat*, faça também o backup do certificado.

Limitações de atualização do Apache Tomcat e Web Console

- Se uma versão personalizada do Apache Tomcat estiver instalada (instalação manual do serviço Tomcat), a atualização subsequente do Web Console ESET PROTECT por meio do Instalador tudo-em-um ou da Tarefa de atualização de componentes não será compatível.
- Atualizar o Apache Tomcat removerá a pasta *era* localizada em *C:\Program Files\Apache Software Foundation\[Tomcat pasta]\webapps*. Se você estiver usando a pasta *era* para armazenar dados adicionais, certifique-se de fazer um backup dos dados antes de atualizar.
- Se *C:\Program Files\Apache Software Foundation\[Tomcat pasta]*O *webapps* contém dados adicionais (além das pastas *era* e *ROOT*), a atualização do Apache Tomcat não acontecerá e apenas o console web será atualizado.
- A atualização do Web Console e Apache Tomcat limpa os arquivos da Ajuda off-line. Se você usou a ajuda off-line com o ESMC ou com uma versão mais antiga do ESET PROTECT, crie novamente a ajuda para o ESET PROTECT 10.1 depois da atualização para garantir que você tenha a ajuda off-line mais recente conforme sua versão do ESET PROTECT.

Procedimentos de atualização

1. Faça o download do Instalador tudo-em-um ESET PROTECT do site da ESET e descompacte o arquivo baixado.

2. Se quiser instalar a versão mais recente do Apache Tomcat e o Instalador tudo-em-um contém uma versão mais antiga do Apache Tomcat (esta etapa é opcional, pule para a etapa 4 se você não precisar da versão mais recente do Apache Tomcat):

   a. Abra a pasta *x64* e navegue até a pasta *installers*.

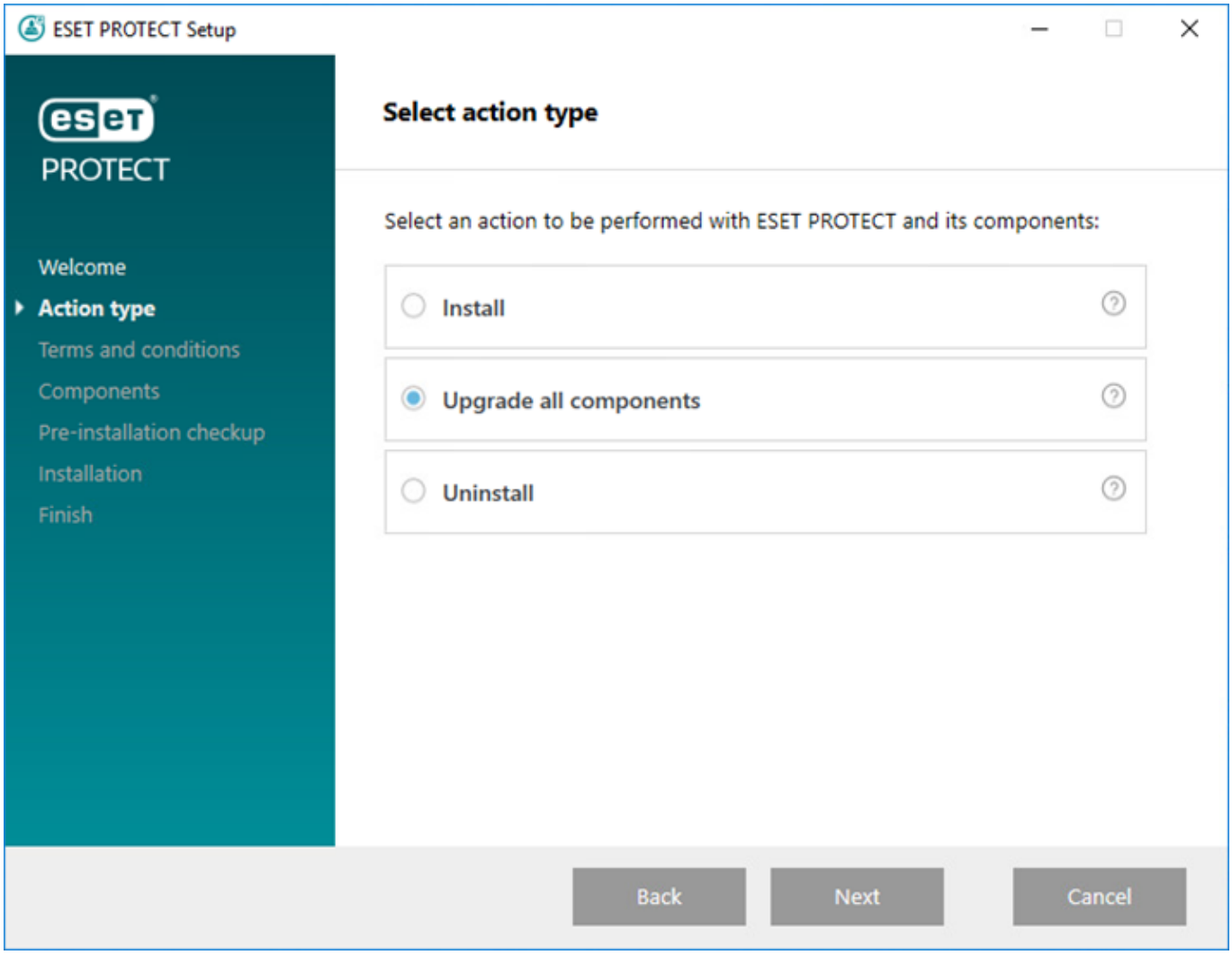
   b. Remova o arquivo *apache-tomcat-9.0.x-windows-x64.zip* localizado na pasta *installers*.

   c. Faça o download do Apache Tomcat 9 pacote zip para Windows 64 bits.

   d. Mova o pacote zip do download para a pasta *installers*.

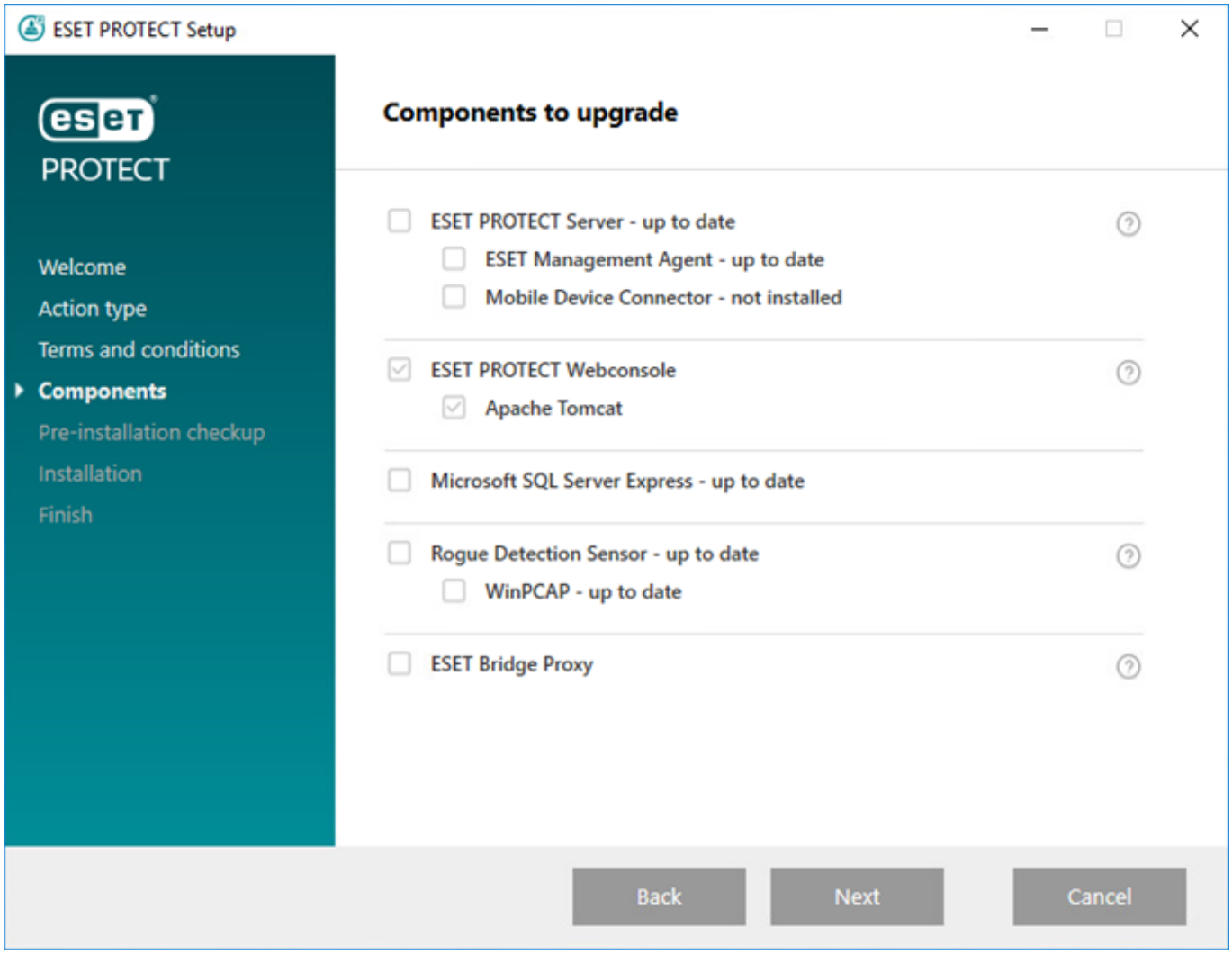
3. Para iniciar o Instalador tudo-em-um, clique duas vezes no arquivo *Setup.exe*, clique em **Avançar** na tela **Bem-vindo**.

4. Selecione **Atualizar todos os componentes** e clique em **Avançar**.



5. Depois de aceitar o EULA, clique em **Avançar**.

6. O Instalador tudo-em-um detecta automaticamente se a atualização está disponível: há caixas de marcação ao lado dos componentes do ESET PROTECT que podem ser atualizados. Clique em **Avançar**.



7. Selecione uma instalação Java no computador. O Apache Tomcat requer 64 bits Java/OpenJDK. Se você tiver várias versões do Java instaladas em seu sistema, recomendamos desinstalar as versões mais antigas do Java e manter apenas a versão mais recente do Java compatível.

⚠ A partir de janeiro de 2019, atualizações públicas do Oracle JAVA SE 8 para uso de negócios, comercial ou de produção precisarão de uma licença comercial. Se você não comprar uma assinatura JAVA SE, você pode usar este guia para mudar para uma alternativa sem custos. Consulte as versões compatíveis do JDK.

8. Clique em **Atualizar** para concluir a atualização e depois em **Concluir**.

9. Se você instalou o console web em um computador diferente do computador onde o Servidor ESET PROTECT está:

a. Interrompa o serviço Apache Tomcat: Vá para **Início** > **Serviços** > clique com o botão direito no serviço Apache Tomcat e selecione **Parar**.

b.Restaure o arquivo *EraWebServerConfig.properties* (da etapa 1) para sua localização original.

c. Reinicie o serviço Apache Tomcat: Vá para **Início** > **Serviços** > clique com o botão direito no serviço Apache Tomcat e selecione **Iniciar**.

10. Conecte ao Web Console ESET PROTECT e certifique-se de que o Web Console é carregado corretamente.

Veja também a configuração adicional do Web Console para soluções empresariais ou para sistemas de baixo desempenho.

Solução de problemas

Se a atualização do Apache Tomcat falhar, desinstale o Apache Tomcat e instale-o novamente e aplique a configuração a partir da etapa 1.

Atualizar o Apache Tomcat manualmente (Windows)

O Apache Tomcat é um componente obrigatório necessário para executar o console web ESET PROTECT. Atualize o Apache Tomcat manualmente se você realizou a instalação existente Apache Tomcat manualmente ou se você não tem o Instalador Tudo-em-um ESET PROTECT mais recente.

Se uma versão personalizada do Apache Tomcat estiver instalada (instalação manual do serviço Tomcat), a atualização subsequente do Web Console ESET PROTECT por meio do Instalador tudo-em-um ou da Tarefa de atualização de componentes não será compatível.

Antes de atualizar

- O Apache Tomcat requer 64 bits Java/OpenJDK. Se você tiver várias versões do Java instaladas em seu sistema, recomendamos desinstalar as versões mais antigas do Java e manter apenas a versão mais recente do Java compatível.

A partir de janeiro de 2019, atualizações públicas do Oracle JAVA SE 8 para uso de negócios, comercial ou de produção precisarão de uma licença comercial. Se você não comprar uma assinatura JAVA SE, você pode usar este guia para mudar para uma alternativa sem custos. Consulte as versões compatíveis do JDK.

- Marque para ver qual versão do Apache Tomcat está sendo usada no momento.

  a.Navegue para a pasta de instalação do Apache Tomcat:
  C:\Program Files\Apache Software Foundation\[Tomcat pasta]

  b.Abra o arquivo RELEASE-NOTES em um em um editor de texto e verifique o número da versão (por exemplo 9.0.34).

  c.Se uma versão compatível mais recente estiver disponível, realize uma atualização.

Procedimentos de atualização

1. Interrompa o serviço Apache Tomcat: Vá para **Início** > **Serviços** > clique com o botão direito no serviço Apache Tomcat e selecione **Parar**.

Feche o *Tomcat7w.exe* se ele estiver sendo executado na sua área de notificações do Windows.

2. Faça o backup dos arquivos a seguir:

   C:\Program Files\Apache Software Foundation\[Tomcat pasta]\.keystore
   C:\Program Files\Apache Software Foundation\[Tomcat pasta]\conf\server.xml
   C:\Program Files\Apache Software Foundation\[Tomcat pasta]\webapps\era\WEB-

INF\classes\sk\eset\era\g2webconsole\server\modules\config\EraWebServerConfig.properties

Se estiver usando um depósito de certificado SSL personalizado na pasta *Tomcat*, faça também o backup do certificado.

3. Desinstale a versão atual do Apache Tomcat.

4. Exclua a pasta a seguir se ela ainda estiver presente no seu sistema:

C:\Program Files\Apache Software Foundation\[Tomcat pasta]

5. Faça o download da versão compatível mais recente do arquivo instalador Apache Tomcat (Instalador de serviço Windows 32 bits/64 bits) `apache-tomcat-[versão].exe` de https://tomcat.apache.org.

6. Instale a versão mais nova do Apache Tomcat que você baixou:

- Se você tiver mais versões Java instaladas, selecione o caminho para o Java mais recente durante a instalação.

- Quando a instalação for concluída, desmarque a caixa de seleção ao lado de **Executar o Apache Tomcat**.

7. Restaure *.keystore*, *server.xml* e certificados personalizados para seus locais originais.

8. Abra o arquivo *server.xml* e certifique-se de que o caminho *keystoreFile* está correto (atualize o caminho se você atualizou para uma versão principal posterior do Apache Tomcat):

keystoreFile="C:\Program Files\Apache Software Foundation\[Tomcat pasta]\.keystore"

9. Certifique-se de que a conexão HTTPS para Apache Tomcat para o Web Console ESET PROTECT foi configurada adequadamente.

10. Instale o console web ESET PROTECT (Instalação do console web – Windows).

11. Restaurar *EraWebServerConfig.properties* ao seu local original.

12. Execute o Apache Tomcat e defina um Java VM correto:

a.Navegue para a pasta *C:\Program Files\Apache Software Foundation\[Tomcat pasta]\bin* e execute *Tomcat9w.exe*.

b.Na guia **Geral**, defina **Tipo de inicialização** para **Automático** e clique em **Iniciar**.

c.Clique na guia **Java**, desmarque **Usar padrão** e certifique-se de que a **Máquina virtual Java** inclui o caminho para o arquivo *jvm.dll* (consulte as instruções ilustradas na Base de conhecimento), e clique em **OK**.

13. Conecte ao Web Console ESET PROTECT e certifique-se de que o Web Console é carregado corretamente.

> Veja também a configuração adicional do Web Console para soluções empresariais ou para sistemas de baixo desempenho.

Solução de problemas

- Se você não conseguir configurar uma conexão HTTPS para o Apache Tomcat, você pode ignorar esta etapa e usar uma conexão HTTP temporariamente.

- Se você não conseguir atualizar o Apache Tomcat, instale sua versão original e aplique a configuração da etapa 2.

- A atualização do Web Console e Apache Tomcat limpa os arquivos da Ajuda off-line. Se você usou a ajuda off-line com o ESMC ou com uma versão mais antiga do ESET PROTECT, crie novamente a ajuda para o ESET PROTECT 10.1 depois da atualização para garantir que você tenha a ajuda off-line mais recente conforme sua versão do ESET PROTECT.

Atualize o Apache Tomcat e Java (Linux)

O Apache Tomcat é um componente obrigatório necessário para executar o console web ESET PROTECT.

Antes de atualizar

1. Execute o comando a seguir para ver a versão instalada do Apache Tomcat (em alguns casos, o nome da pasta é `tomcat7` ou `tomcat8`):

```
cd /usr/share/tomcat/bin && ./version.sh
```

2. Se uma versão posterior estiver disponível:

   a.Certifique-se de que a versão posterior seja compatível.

   b.Faça back-up do arquivo de configuração Tomcat */etc/tomcat7/server.xml*.

Procedimentos de atualização

1. Execute o comando a seguir para parar o serviço Apache Tomcat (em alguns casos o nome do serviço é `tomcat7`):

```
sudo systemctl stop tomcat
```

2. Atualize o Apache Tomcat e Java.

Exemplos de nomes de pacote abaixo podem ser diferentes dos pacotes do repositório de distribuição Linux. O repositório padrão de sua distribuição Linux pode não conter a versão mais recente compatível do Apache Tomcat e do Java.

Distribuição Linux	Comandos de terminal
distribuições Debian e Ubuntu	`sudo apt-get update` `sudo apt-get install openjdk-17-jdk tomcat9`
distribuições CentOS e Red Hat	`yum update` `yum install java-17-openjdk tomcat`
SUSE Linux	`zypper refresh` `sudo zypper install java-17-openjdk tomcat9`

3. Substitua o arquivo */etc/tomcat9/server.xml* pelo arquivo *server.xml* do seu backup.

4. Abra o arquivo *server.xml* e certifique-se de que o caminho *keystoreFile* está correto.

5. Certifique-se de que a conexão HTTPS para o Apache Tomcat está configurada corretamente.

Veja também a configuração adicional do Web Console para soluções empresariais ou para sistemas de baixo desempenho.

6. Se você tiver atualizado o Java, siga as etapas abaixo para configurar o Apache Tomcat para usar o pacote mais recente do Java instalado em seu sistema:

a.Navegue até a pasta de configuração Apache Tomcat:

```
cd /usr/share/tomcat/conf/
```

b.Abra o arquivo *tomcat.conf* em um editor de texto:

```
nano tomcat.conf
```

c.Atualize o caminho para o pacote Java instalado mais recentemente na variável `JAVA_HOME` (o caminho difere com base no pacote Java instalado em seu sistema):

```
JAVA_HOME="/usr/lib/jvm/jre-11-openjdk"
```

d.Salve e feche o arquivo: Pressione **CTRL+X** e depois pressione **Y** e **ENTER**.

e.Reinicie o serviço **tomcat**:

```
sudo systemctl restart tomcat
```

f.Execute o comando abaixo para verificar o pacote Java usado pelo Apache Tomcat:

```
sudo systemctl status tomcat
```

Depois de atualizar o Apache Tomcat para uma versão posterior avançada (por exemplo Apache Tomcat versão 7.x para 9.x):
1.Instale o console web ESET PROTECT novamente (veja Instalação do console web ESET PROTECT - Linux)
2.Reutilize o *%TOMCAT_HOME%/webapps/era/WEB-INF/classes/sk/eset/era/g2webconsole/server/modules/config/EraWebServerConfig.properties* para preservar quaisquer configurações personalizadas no console web ESET PROTECT.
A atualização do Web Console e Apache Tomcat limpa os arquivos da Ajuda off-line. Se você usou a ajuda off-line com o ESMC ou com uma versão mais antiga do ESET PROTECT, crie novamente a ajuda para o ESET PROTECT 10.1 depois da atualização para garantir que você tenha a ajuda off-line mais recente conforme sua versão do ESET PROTECT.

Procedimentos de migração e reinstalação

Existem formas diferentes de migrar e reinstalar o Servidor ESET PROTECT e outros componentes ESET PROTECT:

- Migre ou reinstale o ESET PROTECT 10.1 de um servidor para outro.

Para migrar de um Servidor ESET PROTECT para uma nova máquina de servidor, exporte/faça backup de todas as Autoridades de certificação e do Certificado do Servidor ESET PROTECT. Caso contrário, nenhum dos componentes do ESET PROTECT será capaz de comunicar com seu novo Servidor ESET PROTECT.

- migração do banco de dados ESET PROTECT
- Migração de MDM
- Como alterar um endereço IP ou nome de host em um Servidor ESET PROTECT.

Consulte procedimentos de atualização.

Migração de um servidor para outro

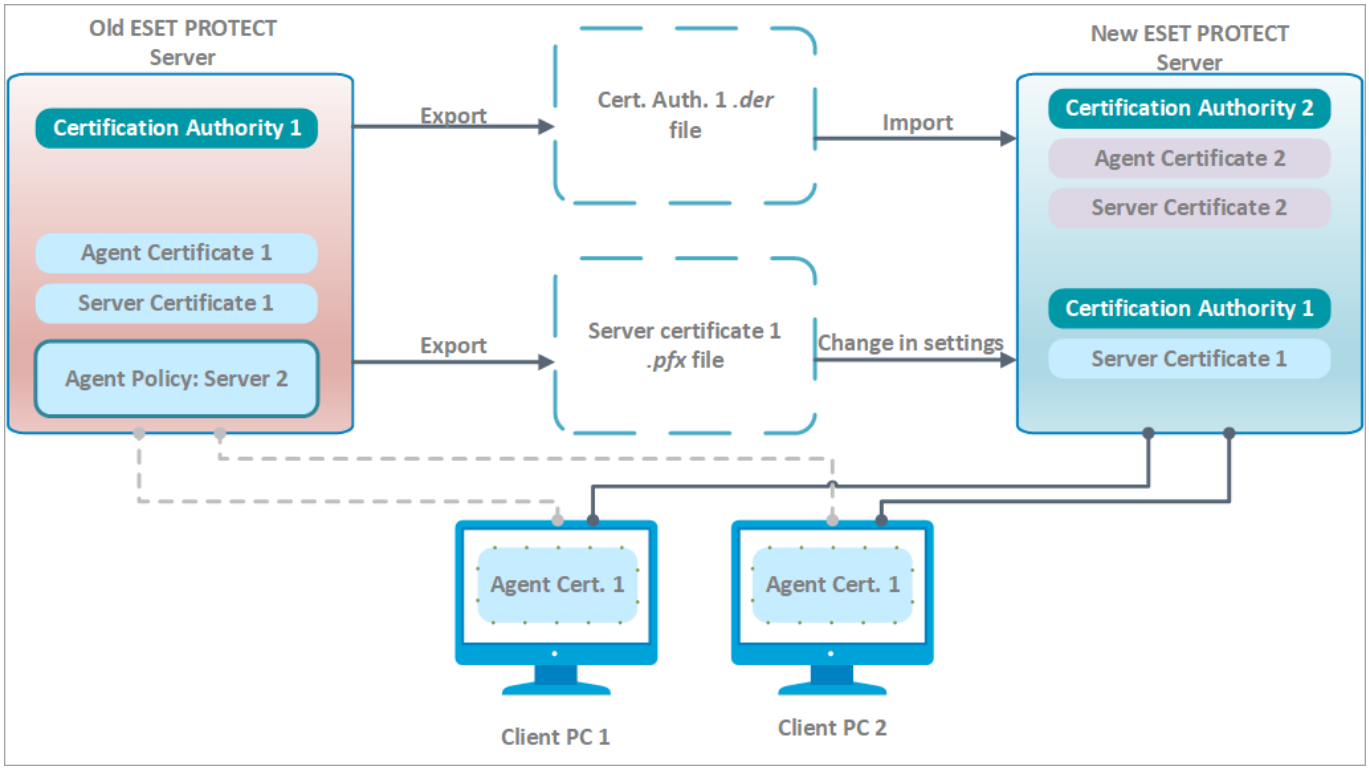
Existem várias formas para migrar o ESET PROTECT de um servidor para outro (estes cenários podem ser usados ao reinstalar o Servidor ESET PROTECT):

- Instalação limpa - mesmo endereço IP - A nova instalação não usa o banco de dados anterior do Servidor ESET PROTECT antigo e mantém o endereço IP.
- Instalação limpa – endereços IP diferente (artigo da Base de conhecimento) – A nova instalação não usa o banco de dados anterior do Servidor ESET PROTECT antigo e tem um endereço IP diferente.
- Banco de dados migrado – endereço IP igual/diferente – a migração de banco de dados só pode ser realizada entre dois banco de dados similares (de MySQL para MySQL ou de Microsoft SQL para Microsoft SQL) e duas versões similares do ESET PROTECT.

Instalação limpa - mesmo endereço IP

O objetivo deste procedimento é instalar uma instância completamente nova do Servidor ESET PROTECT que não usa o banco de dados anterior. Este novo Servidor ESET PROTECT terá **o mesmo endereço IP** do seu servidor anterior, mas não usará o banco de dados do Servidor ESET PROTECT antigo.

As instruções abaixo requerem que seu Servidor ESET PROTECT antigo esteja sendo executado com um Web Console acessível. Se seu Servidor ESET PROTECT antigo estiver inacessível:
1. Instale o Servidor ESET PROTECT/MDM usando o pacote do instalador Tudo-em-um (Windows) ou escolha outro método de instalação (instalação manual pelo Windows, Linux ou Equipamento Virtual).
2. Conecte ao console da Web ESET PROTECT.
3. Adicione computadores cliente à infraestrutura ESET PROTECT e implante o Agente ESET Management de forma local ou remota.



Ver a imagem maior

I. No seu Servidor ESET PROTECT atual (antigo):

Se você gerenciar dispositivos criptografados com o ESET Full Disk Encryption, siga essas etapas para evitar a perda de dados de recuperação.
1.Antes da migração – navegue para **Visão geral do status** > **Criptografia**. Aqui você pode **Exportar** seus **Dados de recuperaçãoESET Full Disk Encryption** atuais.
2.Depois da migração – **Importar** os **Dados de recuperação ESET Full Disk Encryption** no seu novo console de gerenciamento.
Se você não conseguir realizar essas etapas, será preciso remover a criptografia dos dispositivos gerenciados antes da migração. Depois da migração, você pode criptografar os dispositivos gerenciados do Web Console ESET PROTECT.

1. Exporte um certificado do servidor do seu Servidor ESET PROTECT atual e salve no seu armazenamento externo.

   • Exporte todos os Certificados da Autoridade de Certificação do seu Servidor ESET PROTECT e salve cada certificado CA como um arquivo *.der*.

   • Exporte o Certificado do servidor do seu Servidor ESET PROTECT para um arquivo *.pfx*. O *.pfx* exportado vai incluir também uma chave privada.

2. Pare o serviço do Servidor ESET PROTECT.

3. Desativar sua máquina do Servidor ESET PROTECT.

Não desinstale/desconfigure seu Servidor ESET PROTECT antigo ainda.

II. No seu novo Servidor ESET PROTECT:

Para usar um novo Servidor ESET PROTECT com o mesmo endereço IP, certifique-se de a configuração de rede no seu novo Servidor ESET PROTECT (**endereço IP, FQDN, nome do computador, registro SRV DNS**) combina com a do seu Servidor ESET PROTECT antigo.

1. Instale o Servidor ESET PROTECT/MDM usando o pacote do instalador Tudo-em-um (Windows) ou escolha outro método de instalação (instalação manual pelo Windows, Linux ou Equipamento Virtual).

2. Conecte ao console da Web ESET PROTECT.

3. Importar todos os CAs exportados do seu Servidor ESET PROTECT antigo. Para isso, siga as instruções para importar uma chave pública.

4. Altere o certificado de Servidor ESET PROTECT nas suas **Mais** > Configurações do servidor para usar o certificado de Servidor do seu Servidor ESET PROTECT antigo.

5. Importar todas as licenças ESET necessárias para ESET PROTECT.

6. Reinicie o serviço do Servidor ESET PROTECT, consulte nosso artigo da Base de Conhecimento para detalhes.

Depois de um ou dois Intervalos de conexão do agente, os computadores do cliente devem conectar ao seu novo Servidor ESET PROTECT usando seu certificado original de Agente ESET Management, que está sendo autenticado pelo CA importado do Servidor ESET PROTECT anterior. Se os clientes não estiverem conectando, veja Problemas depois da atualização/migração do Servidor ESET PROTECT.

Ao adicionar novos computadores do cliente, use uma nova Autoridade de certificação para assinar os certificados de Agente. Isso é feito porque um CA importado não pode ser usado para assinar novos certificados de mesmo nível, ele só pode autenticar Agentes ESET Management dos computadores do cliente que foram migrados.

III. Desinstalação do Servidor ESET PROTECT/MDM antigo:

Depois de ter tudo sendo executado corretamente em seu novo Servidor ESET PROTECT, desmonte cuidadosamente seu Servidor ESET PROTECT/MDM antigo usando nossas instruções passo-a-passo.

Banco de dados migrado – endereço IP igual/diferente

O objetivo deste procedimento é instalar uma instância completamente nova do Servidor ESET PROTECT e **manter seu banco de dados ESET PROTECT existente**, incluindo o existente em computadores do cliente. O novo Servidor ESET PROTECT terá **o endereço IP igual ou diferente**, e o banco de dados do Servidor ESET PROTECT antigo será importado para a nova máquina do servidor antes da instalação.

- A Migração de bancos de dados só é compatível entre tipos de bancos de dados idênticos (de MySQL para MySQL ou de Microsoft SQL para Microsoft SQL).
- Ao migrar um banco de dados, você deve migrar entre instâncias da mesma versão do ESET PROTECT. Consulte nosso artigo da Base de Conhecimento para instruções para determinar as versões de seus componentes ESET PROTECT. Depois de concluir a migração de banco de dados, você pode realizar uma atualização, se necessário, para obter a versão mais recente do ESET PROTECT.

I. No seu Servidor ESET PROTECT atual (antigo):

Recomendamos migrar para um endereço IP diferente apenas para usuários avançados. Se seu novo Servidor ESET PROTECT tiver um **endereço IP diferente**, execute estas etapas adicionais no seu Servidor ESET PROTECT atual (antigo):
a)Gerar um novo certificado de Servidor ESET PROTECT (com informações de conexão para o novo Servidor ESET PROTECT). Deixe o valor padrão (um asterisco) no campo **Host** para permitir a distribuição deste certificado sem nenhuma associação a um nome de DNS específico ou endereço IP.
b)Criar uma política para definir o novo endereço IP do Servidor ESET PROTECT e atribuir a política a todos os computadores. Espere a política ser distribuída para todos os computadores do cliente (os computadores vão parar de reportar conforme eles recebem as novas informações do servidor).

1. Pare o serviço do Servidor ESET PROTECT.

2. Exportar/Fazer backup do banco de dados ESET PROTECT.

3. Desativar a máquina do Servidor ESET PROTECT atual (opcional se o novo servidor tiver um endereço IP diferente).

Não desinstale/desconfigure seu Servidor ESET PROTECT antigo ainda.

II. No seu novo Servidor ESET PROTECT:

Para usar um novo Servidor ESET PROTECT com o mesmo endereço IP, certifique-se de a configuração de rede no seu novo Servidor ESET PROTECT (**endereço IP, FQDN, nome do computador, registro SRV DNS**) combina com a do seu Servidor ESET PROTECT antigo.

1. Instalar/iniciar um banco de dados ESET PROTECT compatível.

2. Importar/Restaurar o ESET PROTECTbanco de dados do seu Servidor ESET PROTECT antigo.

3. Instale o Servidor ESET PROTECT/MDM usando o pacote do instalador Tudo-em-um (Windows) ou escolha outro método de instalação (instalação manual pelo Windows, Linux ou Equipamento Virtual). Especifique suas configurações de conexão do banco de dados durante a instalação do Servidor ESET PROTECT.

4. Conecte ao console da Web ESET PROTECT.

5. Navegue para **Mais** > **Configurações** > **Conexão**. Clique em **Alterar certificado** > **Abrir lista de certificados** e selecione **Certificado do servidor** do Servidor ESET PROTECT antigo e clique em **OK** duas vezes.

6. Reinicie o serviço do Servidor ESET PROTECT.

7. Entre no Web Console ESET PROTECT e clique em **Computadores**.

Depois de um ou dois intervalos de conexão do Agente, os computadores do cliente devem se conectar ao seu novo Servidor ESET PROTECT usando seu certificado de Agente ESET Management original. Se os clientes não estiverem conectando, veja Problemas depois da atualização/migração do Servidor ESET PROTECT.

III. Desinstalação do Servidor ESET PROTECT/MDM antigo:

Depois de ter tudo sendo executado corretamente em seu novo Servidor ESET PROTECT, desmonte cuidadosamente seu Servidor ESET PROTECT/MDM antigo usando nossas instruções passo-a-passo.

migração do banco de dados ESET PROTECT

Essas instruções se aplicam à migração de banco de dados ESET PROTECT entre instâncias diferentes do SQL Server (também são aplicáveis ao migrar para uma versão diferente do SQL Server ou ao migrar para um SQL Server com host em uma máquina diferente):

- Processo de migração para o Microsoft SQL Server
- Processo de migração para MySQL Server

Processo de migração para o Microsoft SQL Server

Este processo de migração é o mesmo para o **Microsoft SQL Server** e o **Microsoft SQL Server Express**.

Para mais informações, consulte o seguinte artigo da Base de conhecimento Microsoft: https://msdn.microsoft.com/en-us/library/ms189624.aspx.

Pré-requisitos

- As instâncias de origem e destino do SQL Server devem estar instaladas. Elas podem ter host em máquinas diferentes.
- A instância do SQL Server de destino deve ser no mínimo da mesma versão que a instância de origem. Desatualizar não é suportado!
- O **SQL Server Management Studio** deve estar instalado. Se as instâncias do SQL Server estiverem em máquinas diferentes, ele deve estar presente em ambas.

Migração usando o SQL Server Management Studio

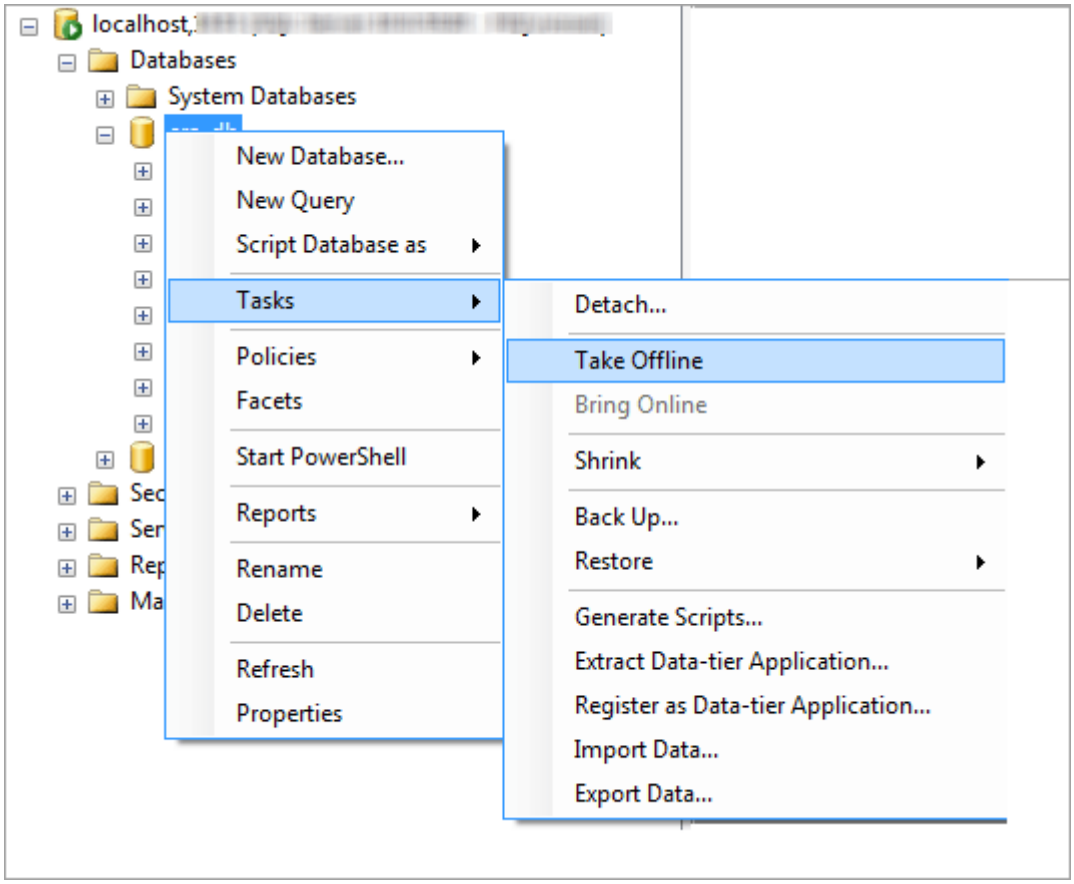
1. Pare o Serviço do servidor ESET PROTECT (ou Serviço do servidor ESMC) ou Serviço ESET PROTECT MDM.

⚠ Não inicie o Servidor ESET PROTECT ou o ESET PROTECT MDM antes de completar todas as etapas abaixo.

2. Faça login na instância do SQL Server através do SQL Server Management Studio.

3. Crie um backup completo de banco de dados do banco de dados a ser migrado. Recomendamos especificar um novo nome de definição de backup. Caso contrário, se a definição de backup já tiver sido usada, o novo backup será anexado ao antigo, o que vai causar um arquivo de backup desnecessariamente grande.

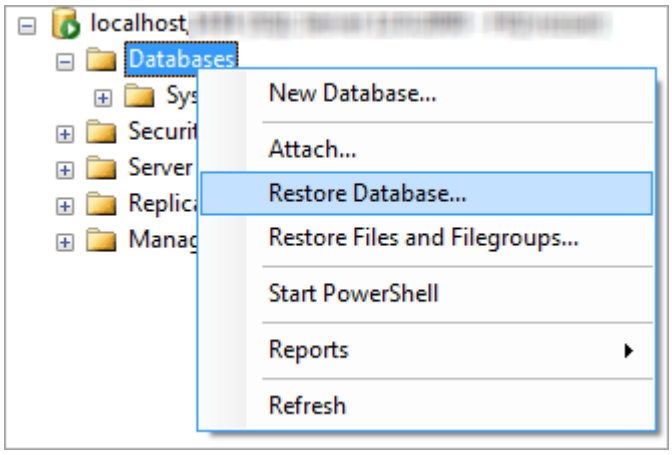
4. Coloque o banco de dados de origem off-line, selecione **Tarefas** > **Colocar off-line**.



5. Copie o arquivo de backup (*.bak*) criado na etapa 3 para um local que pode ser acessado pela instância do SQL Server de destino. Pode ser necessário editar os direitos de acesso para o arquivo de backup do banco de dados.

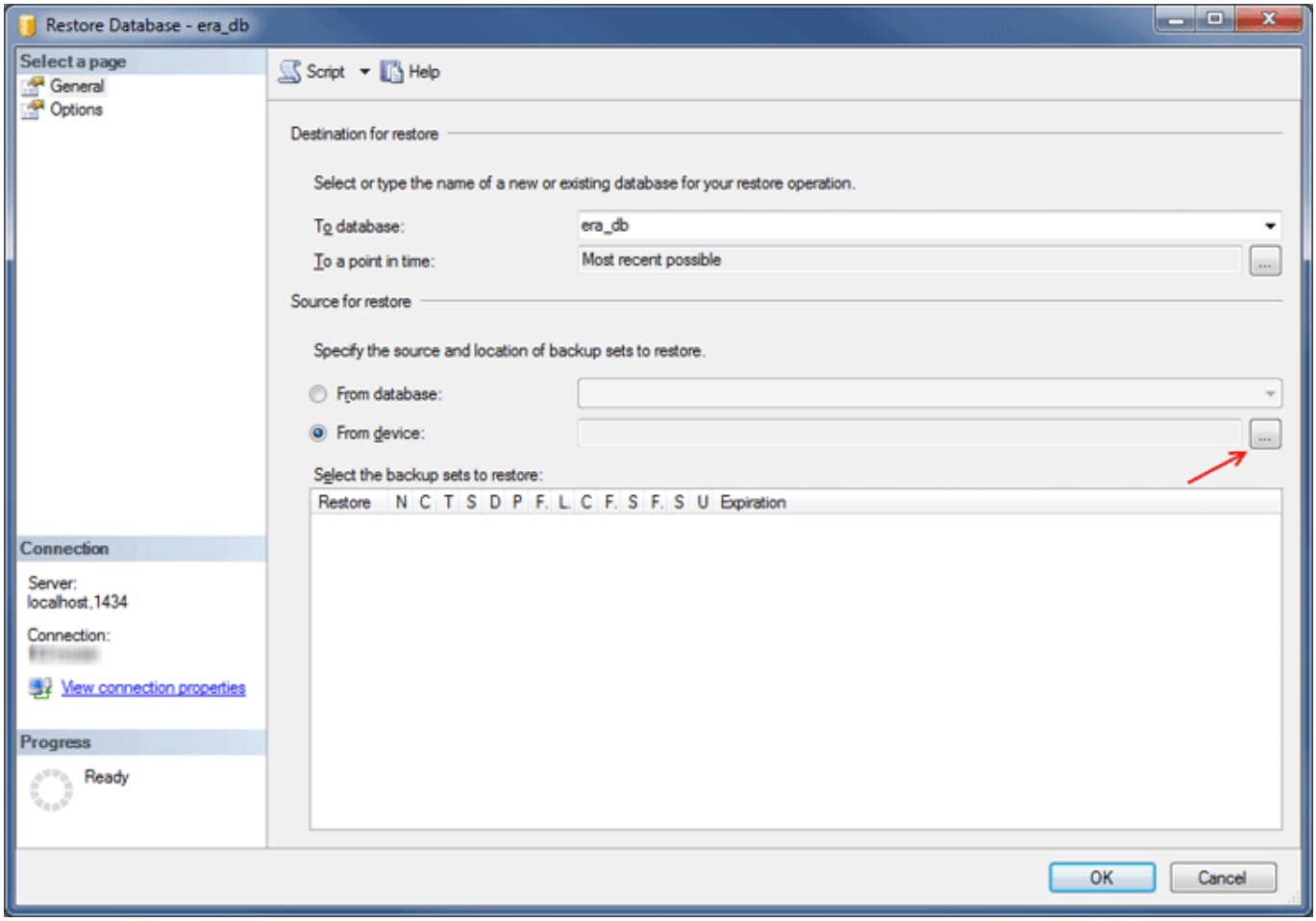
6. Faça login na instância do SQL Server de destino com o SQL Server Management Studio.

7. Restaure seu banco de dados na instância do SQL Server de destino.



8. Digite um nome para seu novo banco de dados no campo **Para banco de dados**. Se preferir, é possível usar o mesmo nome do seu banco de dados anterior.

9. Selecione Do dispositivo em **Especificar a origem e localização do conjunto de backup a restaurar** e em seguida clique em … .

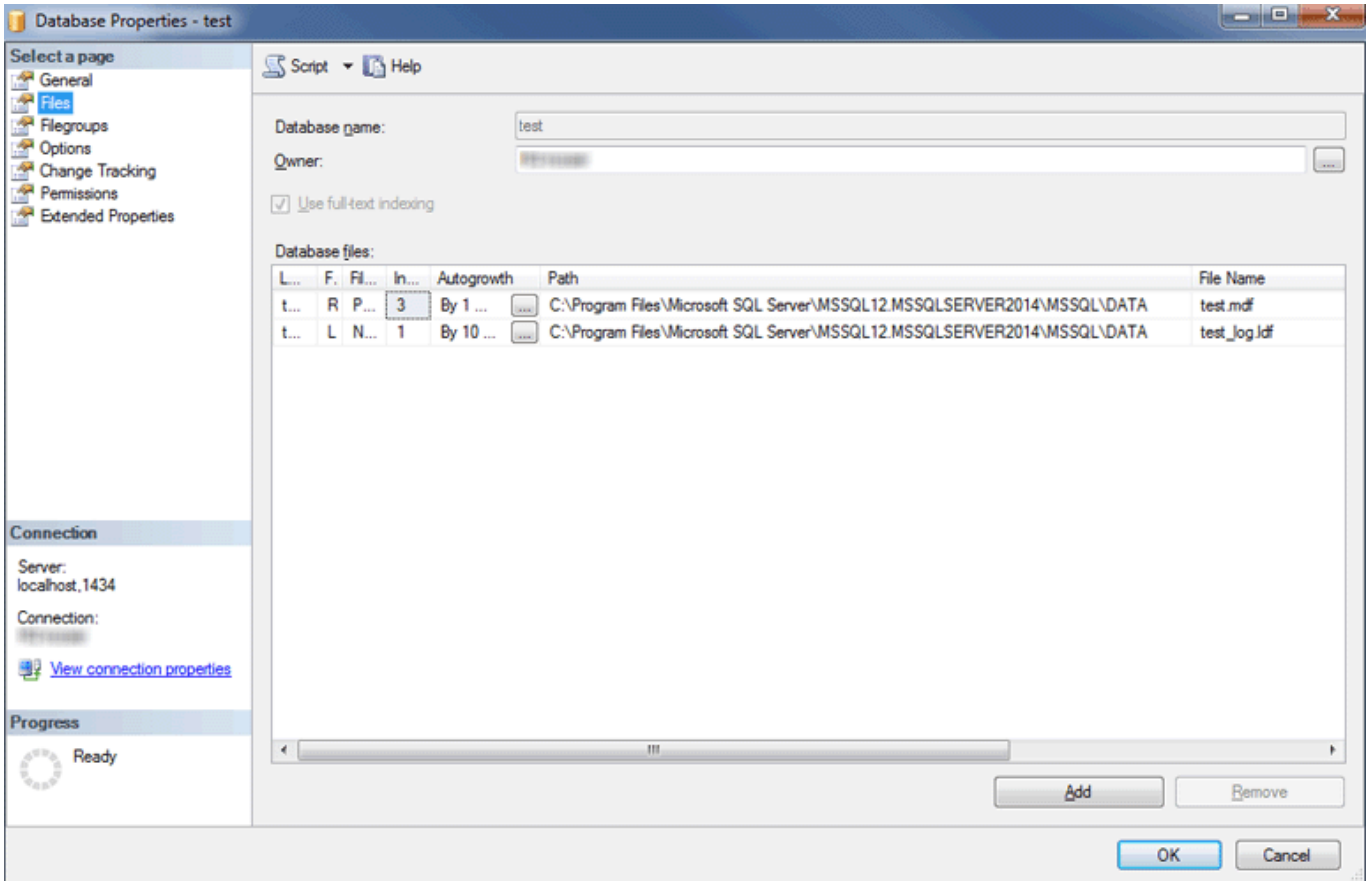


10. Clique em **Adicionar, vá até seu arquivo de backup e abra-o**.

11. Selecione o backup mais recente possível para restaurar (o conjunto de backup pode ter vários backups).

12. Clique na página **Opções** do assistente de restauração. Opcionalmente, selecione **Sobrescrever banco de dados existente** e certifique-se de que os locais de restauração para o banco de dados (*.mdf*) e para o relatório (*.ldf*) estão corretos. Deixar os valores padrão inalterados vai usar os caminhos do seu SQL Server de origem, então verifique esses valores.

- Se não tiver certeza de onde os arquivos DB estão armazenados na instância do SQL Server de destino, clique com o botão direito em um banco de dados existente, selecione **propriedades** e clique na guia **Arquivos**. O diretório onde o banco de dados está armazenado é exibido na coluna **Caminho** da tabela exibida abaixo.

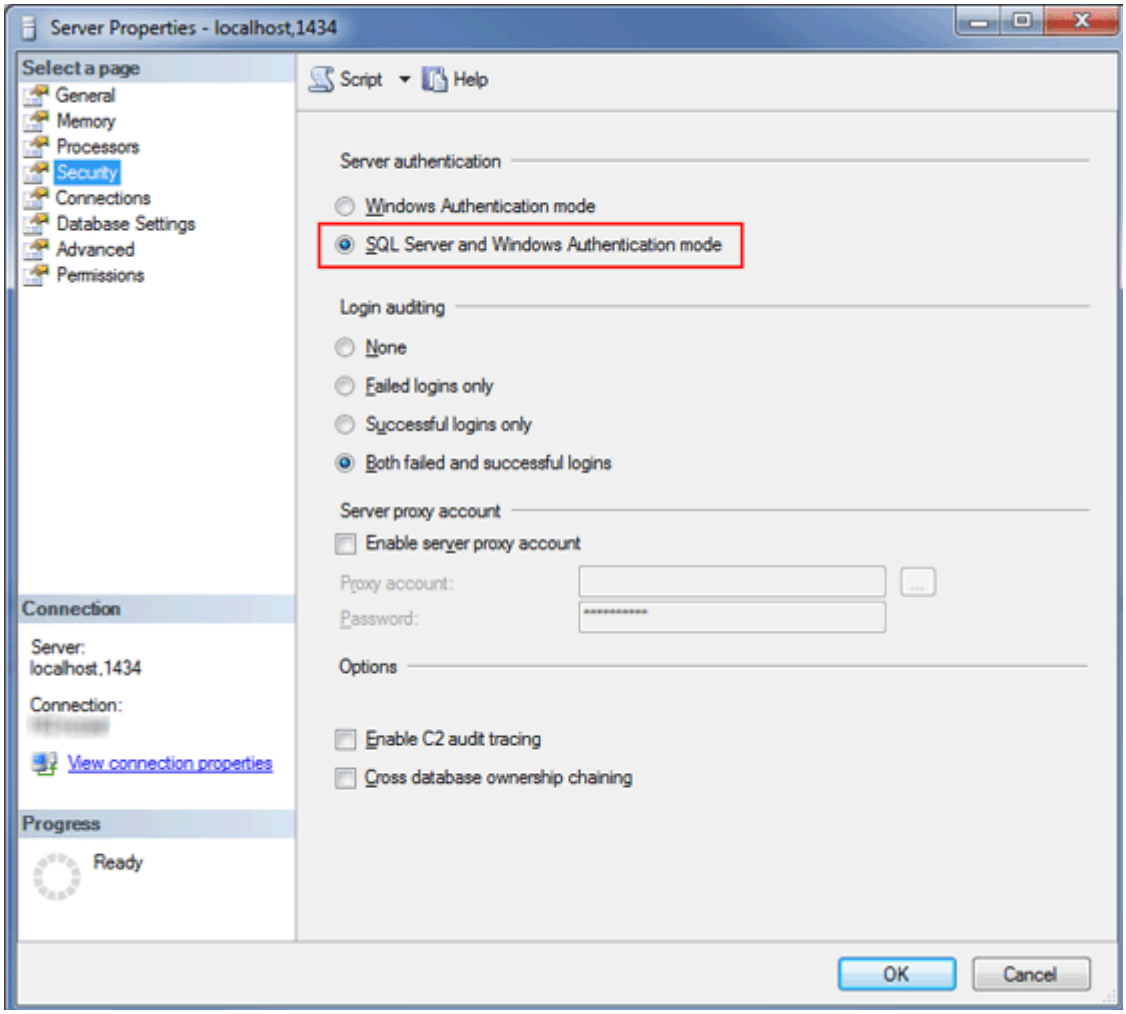


13. Clique em **OK** na janela do assistente de restauração.

14. Clique com o botão direito no banco de dados **era_db**, selecione **Nova consulta** e execute a consulta abaixo para remover o conteúdo da tabela **tbl_authentication_certificate** (caso contrário, os Agentes podem não conseguir realizar a conexão ao novo Servidor):

```
delete from era_db.dbo.tbl_authentication_certificate where certificate_id = 1;
```

15. Certifique-se de que o novo servidor de banco de dados tem a **autenticação de SQL Server ativada**. Clique com o botão direito no servidor e clique em **Propriedades**. Vá para **Segurança** e verifique se o **Modo de autenticação de SQL Server e Windows** está selecionado.



16. Crie um novo login do SQL Server (para servidor ESET PROTECT/ESET PROTECT MDM) no SQL Server de destino com a **autenticação SQL Server** e mapeie o login para um usuário no banco de dados restaurado.

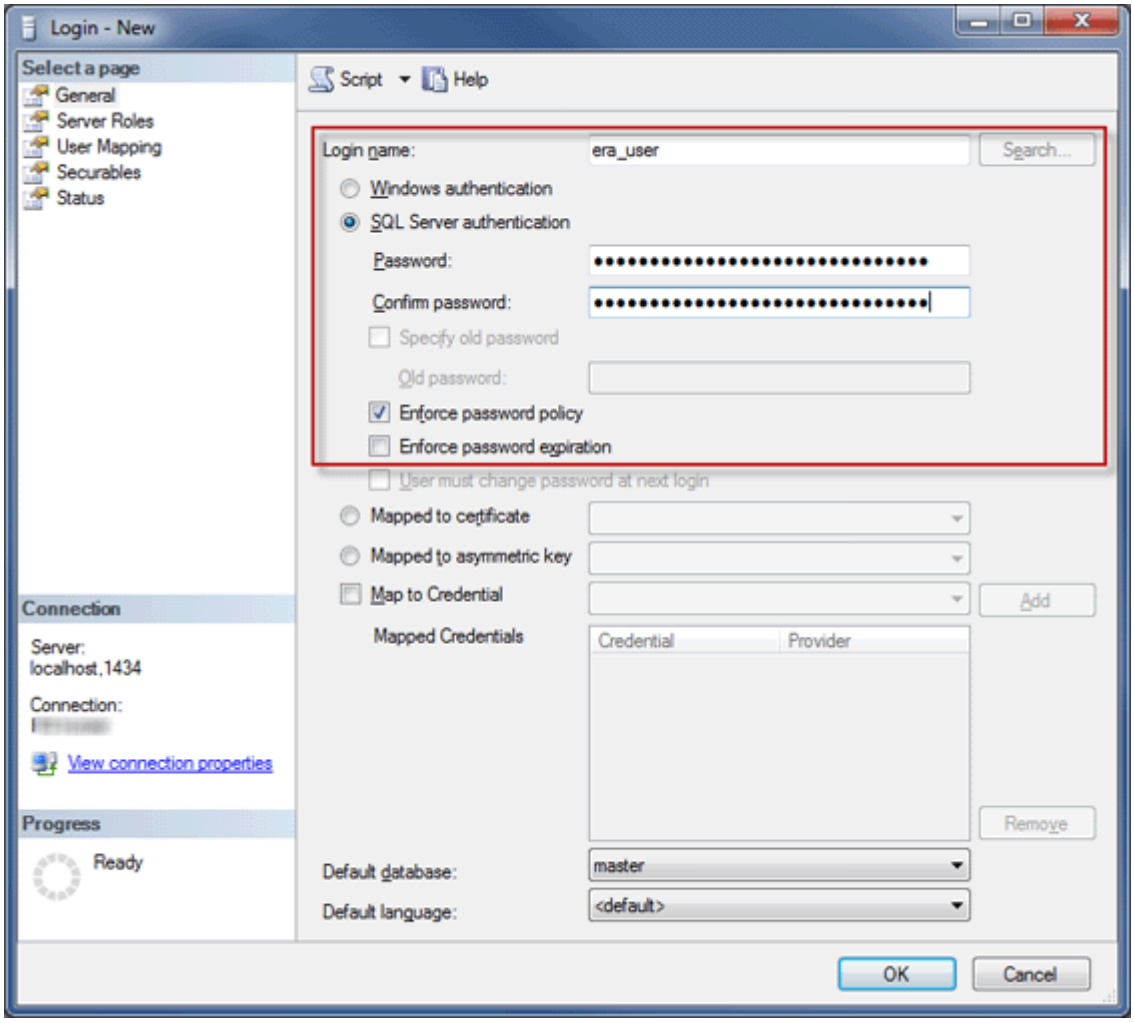
- Não execute a expiração de senha!

- Caracteres recomendados para nomes de usuário: Letras ASCII minúsculas, números e caractere sublinhado "_"

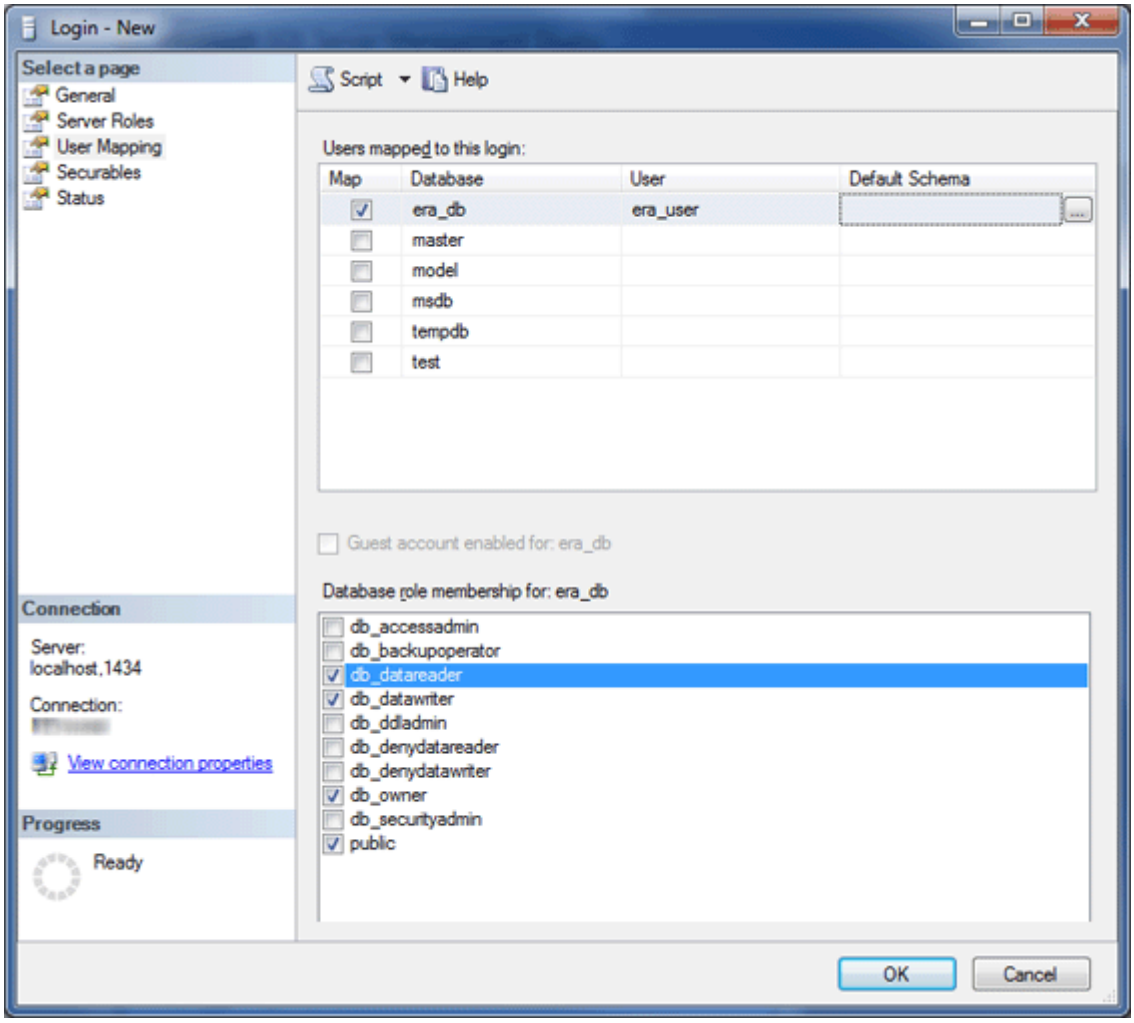
- Caracteres recomendados para senhas: SOMENTE caracteres ASCII, incluindo letras ASCII maiúsculas e minúsculas, números, espaços, caracteres especiais

- Não use caracteres que não ASCII, colchetes {} ou @

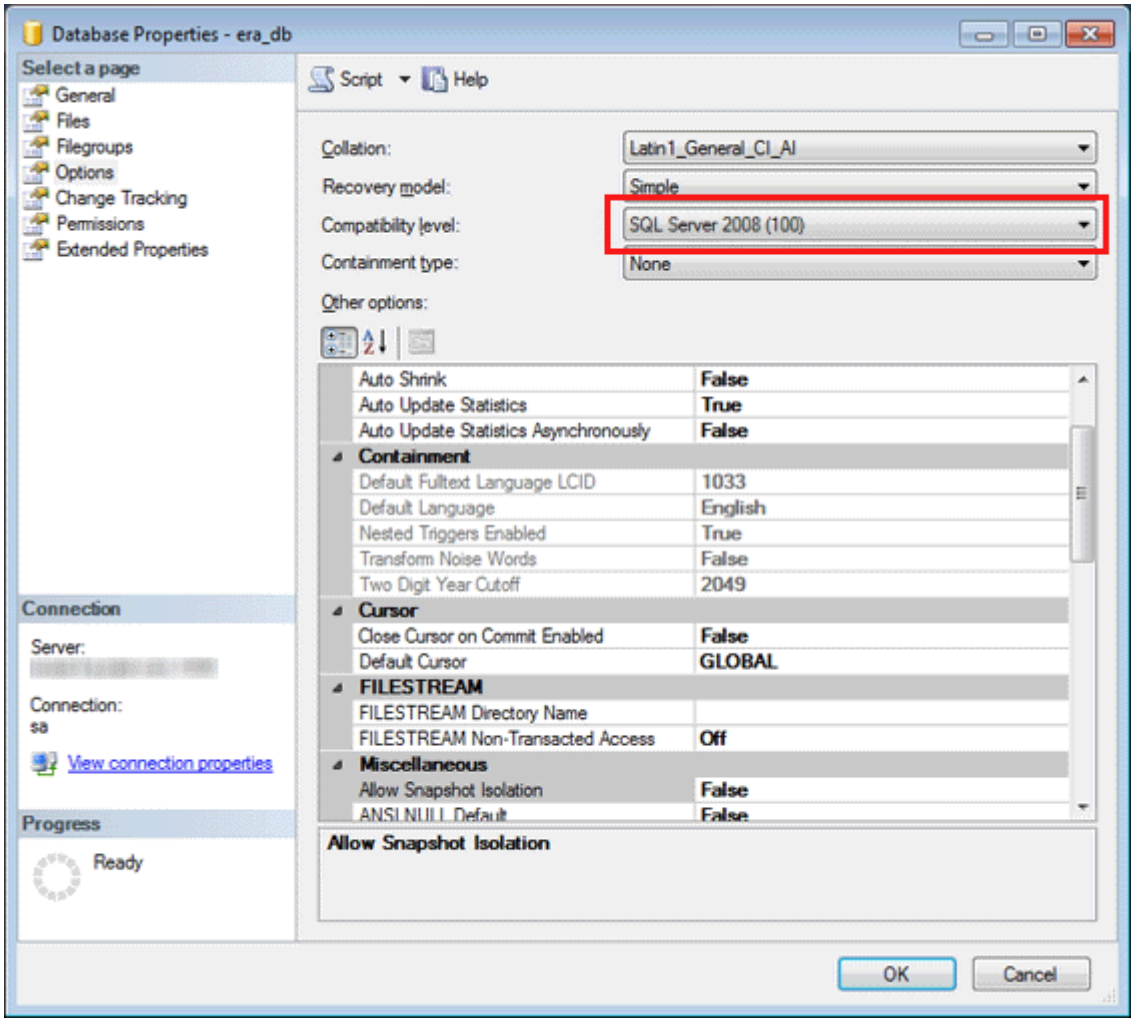
- Note que se você não seguir as recomendações de caracteres acima, você pode ter problemas de conectividade de banco de dados ou vai precisar pular os caracteres especiais em etapas posteriores durante a modificação de string de conexão de banco de dados. Regras de caracteres ignorados não estão incluídas neste documento.



17. Mapeie o login para um usuário no banco de dados de destino. Na guia de **mapeamento de usuário**, certifique-se de que o usuário do banco de dados tem os papéis: **db_datareader**, **db_datawriter**, **db_owner**.

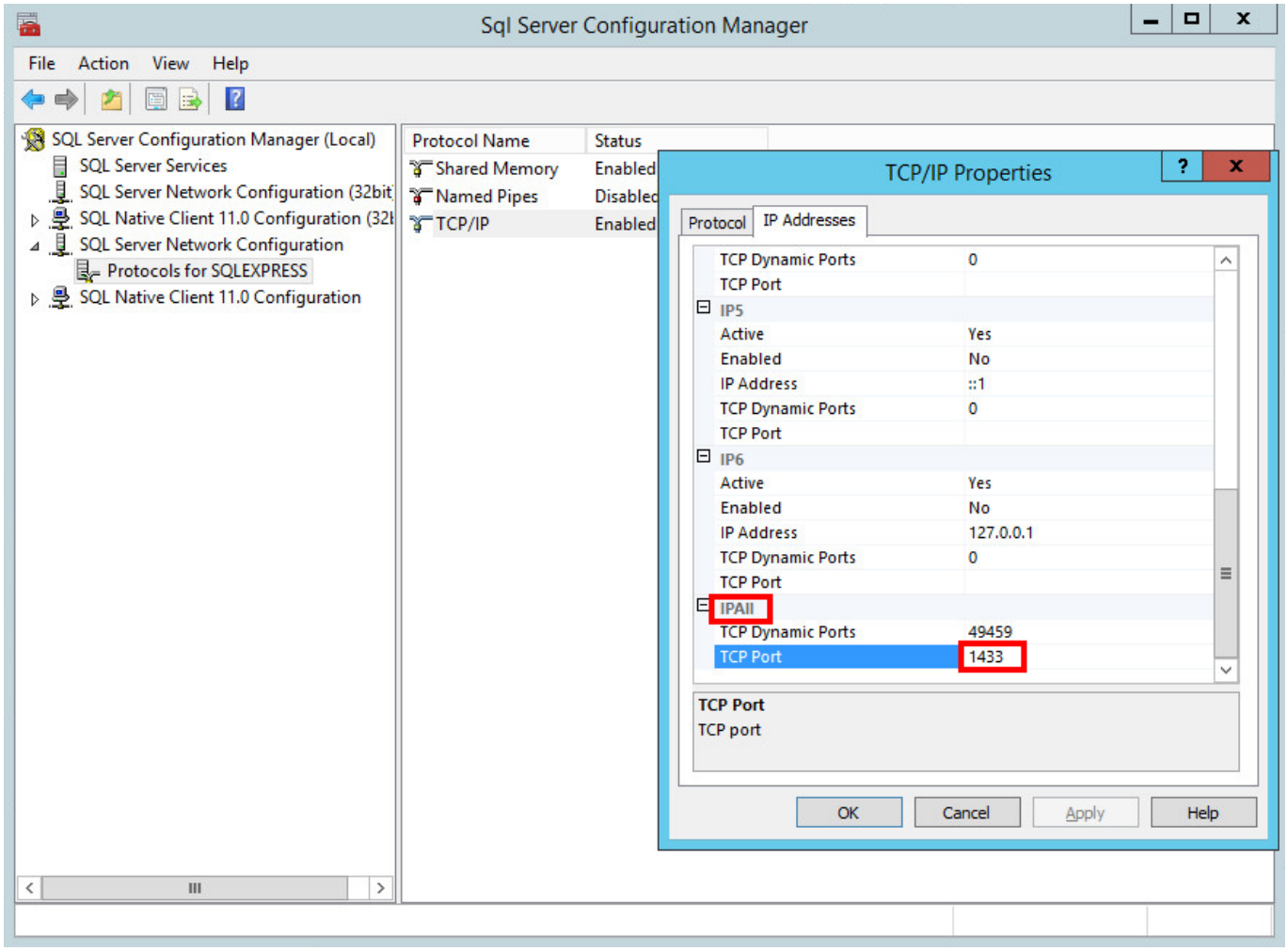


18. Para ativar os recursos do servidor de banco de dados mais recentes, altere o **Nível de compatibilidade** do banco de dados restaurado para o mais recente. Clique com o botão direito no novo banco de dados e abra as **Propriedades** do banco de dados.



> O SQL Server Management Studio não é capaz de definir níveis de compatibilidade posteriores do que os da versão sendo usada. Por exemplo, o SQL Server Management Studio 2014 não consegue definir o nível de compatibilidade para o SQL Server 2019.

19. Certifique-se de que o protocolo de conexão **TCP/IP** está **ativado** para o "db_instance_name" (por exemplo SQLEXPRESS ou MSSQLSERVER) e que a **porta** TCP/IP está configurada para **1433**. Para fazer isso abra o **Gerente de configuração do SQL Server**, vá para **Configuração de rede do SQL Server** > **Protocolos para db_instance_name**, clique com o botão direito em **TCP/IP** e selecione **Ativado**. Clique duas vezes em **TCP/IP**, vá para a guia **Protocolos**, role a tela até **IPAll** e no campo **Porta TCP** digite 1433. Clique em **OK** e reinicie o serviço do **SQL Server**.



20. Conecte o Servidor ESET PROTECT ou MDM ao banco de dados.

Processo de migração para MySQL Server

Pré-requisitos

• As instâncias de origem e destino do SQL Server devem estar instaladas. Elas podem ter host em máquinas diferentes.

• Ferramentas MySQL devem estar disponíveis em no mínimo um dos computadores (`mysqldump` e cliente mysql).

Links úteis

- https://dev.mysql.com/doc/refman/5.6/en/copying-databases.html
- https://dev.mysql.com/doc/refman/5.6/en/mysqldump.html
- https://dev.mysql.com/doc/refman/5.6/en/mysql.html

Processo de migração

Nos comandos, arquivos de configuração ou declarações SQL abaixo, substitua sempre:
- **SRCHOST** com o endereço do servidor do banco de dados de origem
- **SRCROOTLOGIN** com o login de usuário raiz do MySQL server de origem
- **SRCDBNAME** com o nome do banco de dados ESET PROTECT de origem do qual fazer backup
- **BACKUPFILE** com o caminho para o arquivo onde o backup será armazenado
- **TARGETROOTLOGIN** com o login de usuário raiz do MySQL server de destino
- **TARGETHOST** com o endereço do servidor de banco de dados de destino
- **TARGETDBNAME** com o nome do banco de dados ESET PROTECT de destino (depois da migração)
- **TARGETLOGIN** com o nome de login para o usuário do novo banco de dados ESET PROTECT no servidor de banco de dados de destino
- **TARGETPASSWD** com a senha para o novo usuário do banco de dados ESET PROTECT no servidor do banco de dados de destino

Não é necessário executar as declarações SQL abaixo através da linha de comando. Se houver uma ferramenta de interface gráfica do usuário disponível, é possível usar o aplicativo que você já conhece.

1. Pare os serviços do servidor ESET PROTECT/MDM.

2. Crie um backup completo do banco de dados do banco de dados ESET PROTECT de origem (o banco de dados que você planeja migrar):

```
mysqldump --host SRCHOST --disable-keys --extended-insert --routines -
u SRCROOTLOGIN -p SRCDBNAME > BACKUPFILE
```

3. Prepare um banco de dados vazio no MySQL server de destino:

```
mysql --host TARGETHOST -u TARGETROOTLOGIN -p "--
execute=CREATE DATABASE TARGETDBNAME /*!40100 DEFAULT CHARACTER SET utf8 */;"
```

Use o caractere de apóstrofe ' em vez da marca de citação " em sistemas Linux.

4. Restaure o banco de dados no MySQL server de destino para o banco de dados vazio preparado previamente:

```
mysql --host TARGETHOST -u TARGETROOTLOGIN -p TARGETDBNAME < BACKUPFILE
```

5. Crie um usuário de banco de dados ESET PROTECT no MySQL server de destino:

```
mysql --host TARGETHOST -u TARGETROOTLOGIN -p "--
execute=CREATE USER TARGETLOGIN@'%' IDENTIFIED BY 'TARGETPASSWD';"
```

Caracteres recomendados para **TARGETLOGIN**:

- Letras ASCII minúsculas, números e sublinhado "_"

Caracteres recomendados para **TARGETPASSWD**:

- Somente caracteres ASCII, incluindo letras ASCII maiúsculas e minúsculas, números, espaços e caracteres especiais
- Não use caracteres que não ASCII, colchetes {} ou @

Note que se você não seguir as recomendações de caracteres acima, você pode ter problemas de conectividade de banco de dados ou vai precisar pular os caracteres especiais em etapas posteriores durante a modificação de string de conexão de banco de dados. Regras de caracteres ignorados não estão incluídas neste documento.

6. Conceda os direitos de acesso adequados para o usuário do banco de dados ESET PROTECT no MySQL server de destino:

```
mysql --host TARGETHOST -u TARGETROOTLOGIN -p "--
execute=GRANT ALL ON TARGETDBNAME.* TO TARGETLOGIN;"
```

Use o caractere de apóstrofe ' em vez da marca de citação " em sistemas Linux.

7. Remova o conteúdo da tabela **tbl_authentication_certificate** (caso contrário, o Agente pode não conseguir se conectar ao novo Servidor):

```
 mysql --host TARGETHOST -u root -p "--
execute=DELETE FROM era_db.tbl_authentication_certificate where certificate_id = 1;"
```

8. Conecte o Servidor ESET PROTECT ou MDM ao banco de dados.

Conecte o Servidor ESET PROTECT ou MDM a um banco de dados

Siga as etapas abaixo na máquina onde o Servidor ESET PROTECT ou o MDM ESET PROTECT está instalado para conectá-lo a um banco de dados.

1. Pare o serviço do Servidor ESET PROTECT/MDM.
2. Localize *startupconfiguration.ini*
   - Windows:

Servidor:

```
%PROGRAMDATA%\ESET\RemoteAdministrator\Server\EraServerApplicationData\Configurati
on\startupconfiguration.ini
```

MDMCore:

```
%PROGRAMDATA%\ESET\RemoteAdministrator\MDMCore\EraServerApplicationData\Configurat
ion\startupconfiguration.ini
```

- Linux:

Servidor:

```
/etc/opt/eset/RemoteAdministrator/Server/StartupConfiguration.ini
```

MDMCore:

```
/etc/opt/eset/RemoteAdministrator/MDMCore/startupconfiguration.ini
```

3. Altere a string de conexão de banco de dados no servidor ESET PROTECT/MDM *startupconfiguration.ini*

   - Defina o endereço e porta do novo servidor de banco de dados.
   - Defina o novo nome de usuário e senha do ESET PROTECT na string de conexão.

O resultado final deve ser parecido com:

- Microsoft SQL:

```
DatabaseType=MSSQLOdbc

DatabaseConnectionString=Driver=SQL Server;Server=TARGETHOST,1433;Uid=TARGETLOGIN;Pw
d={TARGETPASSWD};CharSet=utf8;Database=TARGETDBNAME;
```

- MySQL:

```
DatabaseType=MySqlOdbc
DatabaseConnectionString=Driver=MySQL ODBC 5.3 Unicode Driver;Server=TARGETHOST;Port
=3306;User=TARGETLOGIN;
Password={TARGETPASSWD};CharSet=utf8;Database=TARGETDBNAME;
```

> Na configuração acima, substitua sempre:
> • **TARGETHOST** com o endereço do servidor de banco de dados de destino
> • **TARGETDBNAME** com o nome do banco de dados ESET PROTECT de destino (depois da migração)
> • **TARGETLOGIN** com o nome de login para o usuário do novo banco de dados ESET PROTECT no servidor de banco de dados de destino
> • **TARGETPASSWD** com a senha para o novo usuário do banco de dados ESET PROTECT no servidor do banco de dados de destino

4. Inicie o servidor ESET PROTECT ou ESET PROTECT MDM e verifique se este serviço está sendo executado de forma adequada.

Migração de MDM

O componente do Gerenciamento de dispositivo móvel/Conector ESET PROTECT (MDM/MDC) (apenas no local) teve seu fim da vida útil agendado. Ler mais. Recomendamos que você migre para o gerenciamento de dispositivo móvel em nuvem.

Para migrar o gerenciamento de dispositivo móvel (local) de um servidor para outro servidor, siga as instruções abaixo.

Migração de gerenciamento de dispositivo móvel de um servidor para outro servidor (local)

Deste procedimento é migrar sua instância existente do ESET PROTECT MDM e **manter seu banco de dados ESET PROTECT MDM existente**, incluindo o inscrito em dispositivos móveis. O ESET PROTECT MDM migrado terá **o mesmo endereço IP/nome de host** do ESET PROTECT MDM antigo, e o banco de dados do ESET PROTECT MDM antigo será importado para o novo host MDM antes da instalação.

- A Migração de bancos de dados só é compatível entre tipos de bancos de dados idênticos (de MySQL para MySQL ou de Microsoft SQL para Microsoft SQL).
- Ao migrar um banco de dados, você deve migrar entre instâncias da mesma versão do ESET PROTECT. Consulte nosso artigo da Base de Conhecimento para instruções para determinar as versões de seus componentes ESET PROTECT. Depois de concluir a migração de banco de dados, você pode realizar uma atualização, se necessário, para obter a versão mais recente do ESET PROTECT.

I. No seu Servidor ESET PROTECT MDM atual (antigo):

1. Criar um backup da configuração MDM.

   a)Em **Computadores**, clique no Servidor MDM e selecione **Detalhes**.

   b)Clique em **Configuração** > **Solicitar configuração**. Pode ser preciso aguardar algum tempo (dependendo do intervalo de conexão do seu Agente) até que a configuração solicitada seja criada.

   c)Clique em **ESET PROTECT Mobile Device Connector** e selecione **Abrir Configuração**.

   d)Exporte os itens a seguir da configuração para o armazenamento externo:

   - O Nome de host exato do seu Servidor MDM.
   - Certificados de mesmo nível – o arquivo *.pfx* exportado também terá a chave privada incluída.

Se você estiver executando o servidor ESET PROTECT MDM no Linux, será preciso exportar o certificado HTTPS da política de configuração MDM:
I.Clique em **Exibir** ao lado do **Certificado HTTPS**.
II.Clique em **Download** e faça o download do certificado HTTPS no formato PFX.

   e)Exporte também os certificados e tokens a seguir, se eles existirem:

- O certificado de assinatura de perfil de inscrição.
- Um Certificado APNS (exporte tanto o Certificado APNS quanto a Chave privada APNS).
- Token de autorização do Programa de Inscrição de Dispositivo Apple (DEP)

2. Pare o serviço do ESET PROTECT MDM.
3. Exportar/fazer backup do banco de dados ESET PROTECT MDM.
4. Desativar a máquina do ESET PROTECT MDM atual.

Não desinstale/desconfigure seu ESET PROTECT MDM antigo ainda.

II. No seu novo Servidor ESET PROTECT MDM:

Certifique-se de a configuração de rede no seu novo Servidor ESET PROTECT MDM (o nome de host que você exportou da configuração do seu servidor MDM "antigo") combina com a do seu ESET PROTECT MDM antigo.

1. Instalar/iniciar um banco de dados ESET PROTECT MDM compatível.
2. Importar/Restaurar o banco de dados ESET PROTECT MDM do seu ESET PROTECT MDM antigo.
3. Instale o Servidor ESET PROTECT/MDM usando o pacote do instalador Tudo-em-um (Windows) ou escolha outro método de instalação (instalação manual pelo Windows, Linux ou Equipamento Virtual). Especifique suas configurações de conexão do banco de dados durante a instalação do ESET PROTECT MDM.

Ao instalar o ESET PROTECT MDM no Linux, use o certificado HTTPS do seu backup.

4. Conecte ao console da Web ESET PROTECT.
5. Reinicie o serviço MDM ESET PROTECT.

Dispositivos móveis gerenciados agora devem se conectar ao seu novo servidor ESET PROTECT MDM usando seu certificado original.

III. Desinstalação do Servidor ESET PROTECT/MDM antigo:

Depois de ter tudo sendo executado corretamente em seu novo Servidor ESET PROTECT, desmonte cuidadosamente seu Servidor ESET PROTECT/MDM antigo usando nossas instruções passo-a-passo.

Alteração do endereço IP ou nome de host do Servidor ESET PROTECT depois da migração

Para alterar um endereço IP ou nome de host no seu Servidor ESET PROTECT, siga essas etapas:

1. Se seu certificado do Servidor ESET PROTECT tiver um endereço IP e/ou nome do host específico, crie um novo certificado de servidor e inclua o novo endereço IP ou nome de host para o qual você está mudando.

Porém, se você tiver um caractere coringa * no campo de host do certificado do Servidor, **pule para a etapa 2**. Se não, crie o novo certificado do Servidor adicionando o novo endereço IP e nome de host separados por vírgula e inclua também o endereço IP e nome de host anteriores.

2. Assinar o novo certificado de servidor usando a autoridade de certificação do servidor ESET PROTECT.

3. Crie uma política alterando as conexões do cliente para o novo endereço IP ou nome de host (de preferência o endereço IP), mas inclua uma segunda conexão (alternativa) para o endereço IP ou nome de host antigo para que o Agente ESET Management tenha a chance de conectar a ambos os servidores. Para mais detalhes, veja Criar política para Agentes ESET Management conectarem com o novo Servidor ESET PROTECT.

4. Aplique esta política nos seus computadores do cliente e permita a replicação dos Agentes ESET Management. Mesmo que essa política vá redirecionar clientes ao seu novo servidor (que não está sendo executado), os Agentes ESET Management usarão as informações alternativas do Servidor para conectar com o endereço IP original.

5. Defina seu novo certificado de servidor em Mais > Configurações.

6. Reinicia o serviço do servidor ESET PROTECT e altera o endereço IP ou nome de host.

Consulte nosso artigo da Base de Conhecimento para instruções ilustradas para alterar o endereço do Servidor ESET PROTECT.

Desinstale o Servidor ESET PROTECT e seus componentes

Selecione um dos capítulos abaixo para desinstalar o Servidor ESET PROTECT e seus componentes:

- Desinstalar Agente ESET Management
- Windows – desinstale o Servidor ESET PROTECT e seus componentes
- Linux – atualize, reinstale ou desinstale os componentes ESET PROTECT
- macOS – desinstale o Agente ESET Management e o produto ESET Endpoint
- Desmontar o servidor ESMC/ESET PROTECT/MDM antigo depois da migração para outro servidor

Desinstalar Agente ESET Management

O Agente ESET Management pode ser desinstalado de várias maneiras.

Remover desinstalação usando o console da Web ESET PROTECT

1. Entre ao console da Web ESET PROTECT.

2. Do painel **Computadores**, selecione um computador do qual você deseja remover o Agente ESET Management e clique em **Nova tarefa**.

Alternativamente, selecione vários computadores ao selecionar as caixas de seleção correspondentes e clicando em **Computador** > **Tarefas** > **Nova tarefa**.

3. Digite um **Nome** para a tarefa.

4. Do menu suspenso **Categoria de tarefa** selecione **ESET PROTECT**.

5. Do menu suspenso **Tarefa** selecione Interromper gerenciamento (desinstalar agente ESET Management).

Depois de desinstalar o Agente ESET Management do computador do cliente, o dispositivo não será mais gerenciado pelo ESET PROTECT:
• O produto de segurança ESET pode reter algumas configurações depois do Agente ESET Management ter sido desinstalado.
• Se o Agente ESET Management estiver protegido por senha, você deverá fornecer a senha para desinstalar, reparar ou atualizar (com alterações). Recomendamos redefinir algumas configurações que você não quer manter (por exemplo, proteção por senha) para as configurações padrão usando uma política antes do dispositivo ser removido do gerenciamento.
• Todas as tarefas sendo executadas no agente serão abandonadas. O status de execução **Em execução**, **Concluído** ou **Com falha** dessa tarefa poderá não ser exibido com precisão no console da Web ESET PROTECT, dependendo da replicação de dados.
• Depois do Agente ser desinstalado é possível gerenciar seu produto de segurança através da EGUI integrada ou do eShell.

6. Analise o **Resumo** da tarefa e clique em **Concluir**.

7. Clicar em Criar acionador para especificar quando essa tarefa de cliente deve ser executada e em quais **destinos**.

Desinstalação local – Windows

Veja também as instruções para a desinstalação local do Agente ESET Management no Linux ou macOS. Para a solução de problemas de desinstalação do Agente, consulte solução de problemas de desinstalação do Agente ESET Management.

1. Conecte ao computador endpoint onde você deseja remover o Agente ESET Management (por exemplo, via RDP).

2. Navegue para **Painel de Controle** > **Programas e Recursos** e clique duas vezes em **Agente ESET Management**.

3. Clique em **Avançar** > **Remover** e siga as instruções de desinstalação.

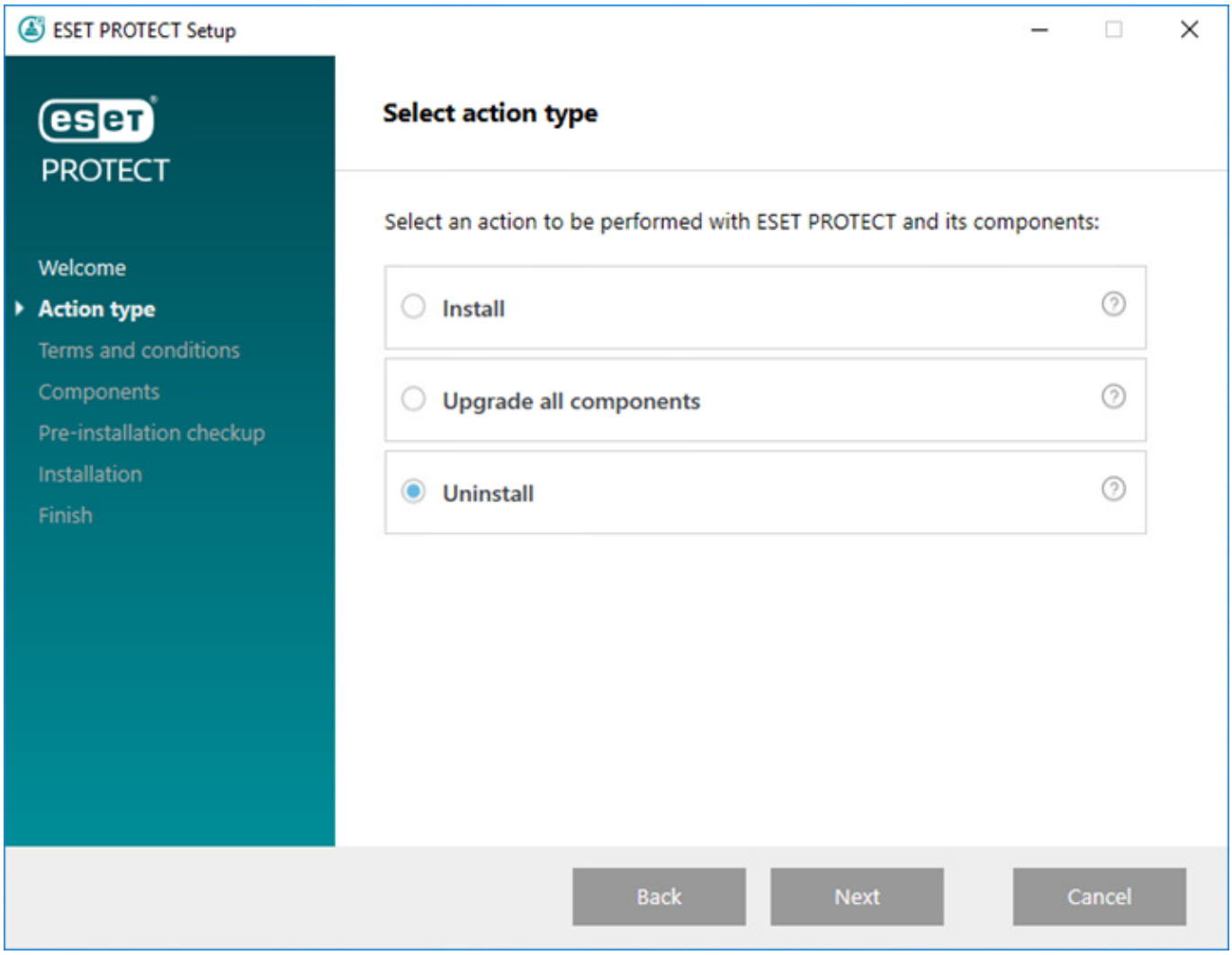
Se você configurou uma senha usando uma política para seus Agentes ESET Management, você terá as seguintes opções:
• Você precisará digitar a senha durante a desinstalação.
• Cancele a atribuição da política primeiro, antes de desinstalar o Agente ESET Management.
• Fazer uma nova implantação do Agente ESET Management sobre um Agente protegido por senha existente (um artigo da Base de conhecimento).

Windows – desinstale o Servidor ESET PROTECT e seus componentes

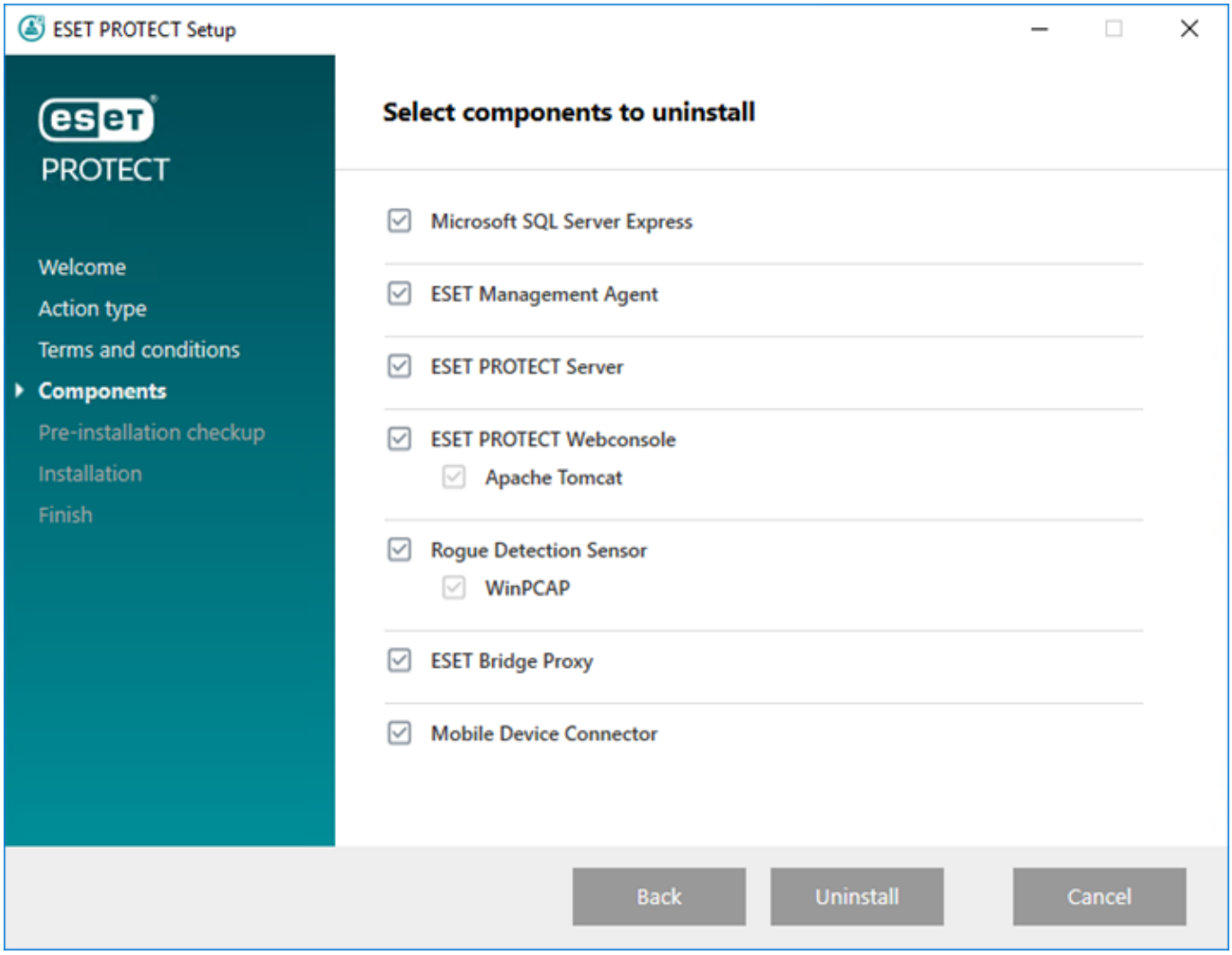
Antes de desinstalar o ESET PROTECT, desinstale os Agentes em computadores gerenciados.
Antes de desinstalar o Conector de dispositivo móvel, leia a Funcionalidade de licenciamento MDM iOS.

Siga essas etapas para desinstalar o Servidor ESET PROTECT e seus componentes no Windows:

1. Faça o download do Instalador tudo-em-um ESET PROTECT e descompacte o pacote.
2. Execute o *Setup.exe*. Você pode selecionar o **idioma** no menu suspenso. Clique em **Avançar**.
3. Selecione **Desinstalar** e clique em **Avançar**.



4. Aceite o EULA e clique em **Avançar**.
5. Selecione os componentes que deseja desinstalar e clique em **Desinstalar**.



6. Pode ser preciso reiniciar o computador para concluir a remoção de componentes em particular.

Consulte também Desmontar o servidor ESMC/ESET PROTECT/MDM antigo depois da migração para outro servidor.

Linux – atualize, reinstale ou desinstale os componentes ESET PROTECT

Se você quiser reinstalar ou atualizar para uma versão mais recente, execute o script de instalação novamente.

Para desinstalar um componente (neste caso o Servidor ESET PROTECT), execute o instalador com o parâmetro `--uninstall` como mostrado abaixo:

```
sudo ./server-linux-x86_64.sh --uninstall --keep-database
```

Se você deseja desinstalar o outro componente, use o nome de pacote adequado no comando. Por exemplo Agente ESET Management:

```
sudo ./agent-linux-x86_64.sh --uninstall
```

Os arquivos de configuração e banco de dados serão removidos durante a desinstalação. Para preservar arquivos do banco de dados, crie um despejo SQL do banco de dados ou use o parâmetro `--keep-database`.

Depois de desinstalar, verifique se

- este serviço `eraserver` é excluído.
- a pasta `/etc/opt/eset/RemoteAdministrator/Server/` é excluída.

Recomendamos que você crie um backup de despejo do banco de dados antes de realizar a desinstalação caso precise restaurar seus dados.
Para mais informações sobre reinstalar o Agente, consulte o capítulo relacionado.
Para a solução de problemas de desinstalação do Agente, consulte solução de problemas de desinstalação do Agente ESET Management.

macOS – desinstale o Agente ESET Management e o produto ESET Endpoint

Desinstale o Agente ESET Management e o produto ESET Endpoint de forma local ou remota via ESET PROTECT.

Você pode encontrar instruções mais detalhadas para a desinstalação local do Agente ESET Management e produto ESET Endpoint em nosso artigo da Base de conhecimento.

Se quiser desinstalar remotamente o produto ESET Endpoint, certifique-se de fazer isso antes de desinstalar o Agente ESET Management.

Desinstalar o Agente ESET Management localmente

1. Clique em **Localizador** para abrir uma nova janela do **Localizador**.
2. Clique em **Aplicativos** > mantenha pressionado o **CTRL** > clique em **Agente ESET Management** > selecione **Mostrar conteúdo do pacote** no menu de contexto.
3. Navegue até **Conteúdo** > **Scripts** e clique duas vezes em **Uninstaller.command** para executar o desinstalador.
4. Digite sua senha de administrador e pressione **Enter** se for solicitado que você insira uma senha.
5. Você verá a mensagem **Processo concluído** quando o Agente ESET Management for desinstalado.

Desinstalar o Agente ESET Management localmente via Terminal

1. Abra o **Localizador** > **Aplicativos** > **Utilitários** > **Terminal**.
2. Digite o código a seguir e pressione **Enter**:

```
sudo /Applications/ESET\ Management\ Agent.app/Contents/Scripts/Uninstall.command ;
 exit;
```

3. Digite sua senha de administrador e pressione **Enter** se for solicitado que você insira uma senha.

4. Você verá a mensagem **Processo concluído** quando o Agente ESET Management for desinstalado.

Desinstalar o ESET Management agente remotamente através do ESET PROTECT

Em **Computadores**, clique no computador do cliente MacOS e selecione **Remover** para desinstalar o Agente ESET Management e remover o computador do gerenciamento.

Para a solução de problemas de desinstalação do Agente, consulte solução de problemas de desinstalação do Agente ESET Management.

Desinstalar o produto ESET Endpoint localmente

1. Clique em **Localizador** para abrir uma nova janela do **Localizador**.

2. Clique em **Aplicativos** > mantenha pressionado **CTRL** > clique em **ESET Endpoint Security** ou **ESET Endpoint Antivirus** > selecione **Mostrar conteúdo do pacote** no menu de contexto.

3. Navegue até **Conteúdo** > **Auxiliares** e clique duas vezes em **Uninstaller.app** para executar o desinstalador.

4. Clique em **Desinstalar**.

5. Digite sua senha de administrador e clique em **OK** se for solicitado que você insira uma senha.

6. Você verá a mensagem de **Desinstalação bem-sucedida** quando o ESET Endpoint Security ou ESET Endpoint Antivirus tiver sido desinstalado com sucesso. Clique em **Fechar**.

Desinstalar o produto ESET Endpoint localmente via Terminal

1. Abra o **Localizador** > **Aplicativos** > **Utilitários** > **Terminal**.

2. Digite o código a seguir e pressione **Enter**:

- Desinstalar ESET Endpoint Antivirus:

```
sudo /Applications/ESET\ Endpoint\ Antivirus.app/Contents/Helpers/Uninstaller.app
/Contents/Scripts/uninstall.sh
```

- Desinstalar ESET Endpoint Security:

```
sudo /Applications/ESET\ Endpoint\ Security.app/Contents/Helpers/Uninstaller.app/
Contents/Scripts/uninstall.sh
```

3. Digite sua senha de administrador e pressione **Enter** se for solicitado que você insira uma senha.

4. Você verá a mensagem **Processo concluído** quando o produto ESET Endpoint for desinstalado.

Desinstalar o produto ESET Endpoint remotamente via ESET PROTECT

Para desinstalar o Agente ESET Management remotamente dia ESET PROTECT, você pode usar uma das seguintes opções:

- Em **Computadores**, clique no computador cliente MacOS, selecione **Detalhes** > **Aplicativos instalados** > Selecione **ESET Endpoint Security** ou **ESET Endpoint Antivirus** e clique no botão **Desinstalar**.
- Use a tarefa Desinstalação de software***.

Desmontar o servidor ESMC/ESET PROTECT/MDM antigo depois da migração para outro servidor

⚠ Certifique-se de que seu Servidor ESET PROTECT/MDM novo está sendo executado e que os computadores do cliente e dispositivos móveis estão se conectando ao seu novo ESET PROTECT corretamente.

Há algumas opções ao desmontar seu Servidor ESMC/ESET PROTECT/MDM antigo depois da migração para outro servidor:

I.**Manter o sistema operacional da máquina do servidor e reutilizá-lo**

1. Pare o serviço do Servidor ESMC/ESET PROTECT antigo.
2. Remova (`DROP DATABASE`) a instância antiga do banco de dados do Servidor ESMC/ESET PROTECT (Microsoft SQL ou MySQL).

⚠ Se você migrou o banco de dados para o novo Servidor ESET PROTECT, certifique-se de que excluiu o banco de dados no Servidor ESMC/ESET PROTECT antigo antes da desinstalação para impedir que as licenças sejam dissociadas (removidas) do banco de dados do novo Servidor ESET PROTECT.

3. Desinstale o Servidor /ESET PROTECT/MDM antigo e todos os seus componentes (incluindo o Agente ESET Management, Rogue Detection Sensor, MDM, etc.):
   - Desinstalação ESET PROTECT—Windows
   - Desinstale o ESET PROTECT – Linux

⚠ Não desinstale seu banco de dados se houver outro software dependente do seu banco de dados.

4. Planeje uma reinicialização do sistema operacional do seu servidor depois da desinstalação

II.**Manter a máquina do servidor**

A forma mais fácil de remover o ESMC/ESET PROTECT/MDM é formatar o disco onde ele está instalado.

⚠ Isto vai apagar tudo no disco, incluindo o sistema operacional.

Solução de problemas

Como o ESET PROTECT é um produto complexo que usa várias ferramentas de terceiros e é compatível com várias plataformas de sistemas operacionais, o potencial de você encontrar problemas que exigem solução de problemas existe.

A documentação da ESET inclui diversos métodos de solução de problemas do ESET PROTECT. Consulte Respostas para problemas comuns na instalação para resolver alguns problemas comuns com o ESET PROTECT. Veja também os problemas conhecidos para os produtos empresariais ESET.

Não foi possível resolver o problema?

- Cada componente do ESET PROTECT tem um relatório que você pode configurar para ser mais ou menos detalhado. Revisar relatórios para identificar erros que possam explicar o problema que você está tendo.

- O detalhamento de registro em relatório de cada componente é configurado em sua política > **Escanear detalhamento do relatório** - Defina o detalhamento de registro em relatório para determinar o nível de informações que serão coletadas e registradas em relatório, de **Rastrear** (com informações) a **Fatal** (informações essenciais mais importantes). A política deve ser aplicada ao dispositivo para ter efeito.

  - Política do Agente ESET Management - Para permitir o registro em relatório completo do Agente ESET Management no arquivo *trace.log*, crie um arquivo nomeado *traceAll* sem extensão na mesma pasta que o *trace.log* e reinicie o computador (para reiniciar o serviço do Agente ESET Management).

  - ESET Bridgepolítica

  - Política do ESET Mobile Device Connector – a política deve ser aplicada ao dispositivo para ter efeito. Veja também a solução de problemas MDM.

  - O detalhamento do relatório para o Servidor ESET PROTECT está em Configurações.

- Se você não conseguir resolver seu problema, você pode visitar o Fórum de Segurança ESET e consultar a comunidade ESET para informações sobre problemas que você pode encontrar.

- Ao entrar em contato com o Suporte Técnico ESET, você pode ser solicitado a coletar arquivos de relatório usando o ESET Log Collector ou a Ferramenta de diagnóstico. É altamente recomendável que você inclua os relatórios ao entrar em contato com o suporte para acelerar sua solicitação de serviço de atendimento ao cliente.

Atualizar componentes ESET PROTECT em ambiente off-line

Siga essas etapas para atualizar seus componentes ESET PROTECT e produtos ESET endpoint sem acesso à Internet:

Usar a Tarefa de atualização de componente para um ambiente off-line é possível quando:
- Há um repositório off-line disponível.
- A localização do repositório para o Agente ESET Management é configurada usando uma política para um local acessível.

Realize a atualização do Servidor ESET PROTECT e Console da Web

1. Verifique qual versão do console de gerenciamento está sendo executada no servidor.

2. Faça o download do Instalador tudo-em-um para Windows mais recente ou do instalador autônomo de componente do ESET PROTECT para Linux mais recente do site de download da ESET.

3. Realize a atualização do Servidor ESET PROTECT e Console da Web ESET PROTECT:

   - Windows – Atualizar usando o Instalador tudo-em-um
   - Linux – Atualização manual baseada em componente

> A atualização do Web Console e Apache Tomcat limpa os arquivos da Ajuda off-line. Se você usou a ajuda off-line com o ESMC ou com uma versão mais antiga do ESET PROTECT, crie novamente a ajuda para o ESET PROTECT 10.1 depois da atualização para garantir que você tenha a ajuda off-line mais recente conforme sua versão do ESET PROTECT.

Continue com a atualização off-line dos produtos ESET endpoint

1. Veja quais produtos ESET estão instalados nos clientes: Abra o Console da Web ESET PROTECT e navegue para **Painel** > **Aplicativos ESET**.

2. Certifique-se de ter as versões mais recentes dos produtos ESET endpoint.

3. Faça download dos instaladores do site de download ESET para o repositório local configurado durante a instalação off-line.

4. Execute uma tarefa de Instalação de software do Console da Web ESET PROTECT.

Respostas para problemas comuns na instalação

Abra a seção da mensagem de erro que você deseja resolver:

ESET PROTECTServidor

O serviço do Servidor ESET PROTECT não é iniciado:

Instalação quebrada

- Isso pode ser o resultado da falta de chaves de registro, falta de arquivos ou permissões de arquivos inválidas.
- O instalador Tudo-em-um ESET tem seu próprio relatório. Ao instalar um componente manualmente, use o método de Registro em relatório MSI.

Porta de escuta já utilizada (principalmente 2222 e 2223)

Use o Comando apropriado para seu sistema operacional:

- Windows:

```
netstat -an | find "2222"
netstat -an | find "2223"
```

- Linux:

```
netstat | grep 2222
netstat | grep 2223
```

Banco de dados não está em execução / inacessível

- Microsoft SQL Server: Verificar se a porta 1433 está disponível no/para o servidor de banco de dados ou tente fazer logon no SQL Server Management Studio
- MySQL: Verifique se a porta 3306 está disponível no/para o servidor de banco de dados ou tente fazer logon na sua interface de banco de dados (por exemplo, usando a interface de linha de comando MySQL ou `phpmyadmin`)

Banco de dados corrompido

Vários erros de SQL serão mostrados no relatório do Servidor ESET PROTECT. É recomendável que você restaure seu banco de dados a partir de um backup. Se não houver um backup presente, reinstale o ESET PROTECT.

Recursos do sistema insuficientes (RAM, espaço em disco)

Revisão dos processos em execução e desempenho do sistema:

- Usuários do Windows: Executar e revisar informações no Gerenciador de tarefas ou Visualizador de eventos
- Usuários do Linux: Execute um dos comandos a seguir:

`df -h` (pare revisar informações de espaço em disco)
`cat /proc/meminfo` (para revisar informações de espaço em memória)
`dmesg` (para revisar a saúde do sistema Linux)

Erro com o conector ODBC durante a instalação do Servidor ESET PROTECT

```
Error: (Error 65533) ODBC connector compatibility check failed.
Please install ODBC driver with support for multi-threading.
```

Reinstalar uma versão do driver ODBC que é compatível com multe encadeamento ou reconfigurar o *odbcinst.ini* como mostrado na seção de configuração ODBC.

Erro com a conexão do banco de dados durante a instalação do Servidor ESET PROTECT

A instalação do Servidor ESET PROTECT é concluída com a mensagem de erro genérica:

```
The database server is not configured correctly.
Please check the documentation and reconfigure the database server as needed.
```

Mensagem de erro do relatório de instalação:

```
Error: Execution test of long statement failed with exception:
CMysqlCodeTokenExecutor: CheckVariableInnodbLogFileSize:
Server variables innodb_log_file_size*innodb_log_files_in_group
value 100663296 is too low.
```

Verifique se a configuração do seu driver de banco de dados corresponde ao que é exibido na seção de configuração ODBC.

Agente ESET Management

Desinstalação e solução de problemas do Agente ESET Management

• Consulte relatórios do Agente ESET Management.
• Você pode desinstalar o Agente ESET Management usando um Desinstalador ESET ou usando uma forma não-padrão (como remoção de arquivos, remoção do serviço do Agente ESET Management e entradas de registro). Se houver um produto ESET endpoint na mesma máquina, não será possível devido a uma Autodefesa ativada.
• A mensagem "O banco de dados não pode ser atualizado. Primeiro remova o produto." é exibido durante a desinstalação do Agente – Reparar o Agente ESET Management:
1.Clique em **Painel de Controle** > **Programas e Recursos** e clique duas vezes em **Agente ESET Management**.
2.Clique em **Avançar** > **Reparar** e siga as instruções.
Todas as formas possíveis de desinstalar o Agente ESET Management são descritas na seção de Desinstalação.

Código de erro 1603 ocorreu durante a instalação do Agente

Este erro pode ocorrer quando os arquivos do instalador não estão localizados no disco local. Para corrigir isto, copie os arquivos de instalação para o diretório local e execute a instalação novamente. Se os arquivos já estiverem presentes, ou se o erro persistir, siga nossas instruções da Base de Conhecimento.

A mensagem de erro aparece durante a instalação do Agente no Linux

Mensagem de erro:

```
Checking certificate ... failed
Error checking peer certificate: NOT_REGULAR_FILE
```

A causa possível para este erro é um nome de arquivo incorreto no comando de instalação. O console é sensível a maiúsculas e minúsculas. Por exemplo `Agent.pfx` não é igual a `agent.pfx`.

A implantação remota do Linux para o Windows 8.1 (32-bit) falhou

Este é um problema de autenticação causado pelo KB3161949 da Microsoft. Isso pode ser resolvido apenas ao remover essa atualização dos hosts onde a implantação falhou.

O Agente ESET Management não conseguiu se conectar ao Servidor ESET PROTECT

Consulte Solução de problemas de conexão do Agente e nosso artigo da Base de conhecimento.

O script do instalador do Agente saiu com o código 30

Você usou o script do instalador do Agente com um local personalizado para o instalador e não editou o script corretamente. Revise a página de ajuda e tente novamente.

Web Console

ESET Bridge Proxy HTTP

ESET Rogue Detection Sensor

Por que a mensagem de erro a seguir é registrada continuamente no trace.log do ESET Rogue Detector?

```
Information: CPCAPDeviceSniffer [Thread 764]:
CPCAPDeviceSniffer on rpcap://\Device\NPF_
{2BDB8A61-FFDA-42FC-A883-CDAF6D129C6B} throwed error:
Device open failed with error:Error opening adapter:
The system cannot find the device specified. (20)
```

Este é um problema com o WinPcap. Pare o serviço do ESET Rogue Detector Sensor, reinstale a versão mais recente do WinPcap (no mínimo 4.1.0) e reinicie o serviço do ESET Rogue Detector Sensor .

Linux

Dependência libQtWebKit faltando no CentOS Linux

Se o seguinte erro for exibido:

```
Error: CReportPrinterModule [Thread 7f5f4c7b8700]:
ReportPrinter: ReportPrinterTool exited with:
/opt/eset/RemoteAdministrator/Server//ReportPrinterTool:
error while loading shared libraries: libQtWebKit.so.4:
cannot open shared object file: No such file or directory [code:127]
```

Siga as instruções em nosso artigo da Base de conhecimento.

A instalação de Servidor ESET PROTECT no CentOS 7 falhou

Se o seguinte erro for exibido:

```
Error: DbCheckConnection: locale::facet::_S_create_c_locale name not valid
```

O problema provavelmente está sendo causado por configurações de ambiente/local. Execute o comando a seguir antes do script de instalação do servidor deve ajudar:

```
export LC_ALL="en_US.UTF-8"
```

Microsoft SQL Server

Código de erro -2068052081 durante instalação do Microsoft SQL Server.

Reinicie seu computador e execute a configuração de novo. Se o problema continuar, desinstale o SQL Server Native Client e execute a instalação novamente. Se isso não solucionar o problema, desinstale todos os produtos do Microsoft SQL Server, reinicie seu computador e execute a instalação novamente.

Código de erro -2067922943 durante instalação do Microsoft SQL Server.

Verifique se seu sistema atende a todos os requisitos de banco de dados para ESET PROTECT.

Código de erro -2067922934 durante instalação do Microsoft SQL Server.

Certifique-se de que você tem os privilégios de conta de usuário corretos.

O console da web exibe “Falha ao carregar dados”.

O Servidor Microsoft SQL tenta usar o máximo de espaço em disco possível para relatórios de transação. Se você quiser limpar isso, visite o site oficial da Microsoft.

Código de erro -2067919934 durante instalação do Microsoft SQL Server.

Certifique-se de que todas as etapas anteriores foras concluídas com sucesso. Este erro é causado por arquivos de sistema com configuração errada. Reinicie seu computador e execute a instalação novamente.

Relatórios

Cada componente ESET PROTECT realiza o registro em relatório. Componentes ESET PROTECT gravam informações sobre certos eventos em relatórios. O local dos relatórios varia de acordo com o componente. O seguinte é uma lista de locais de relatórios:

Windows

ESET PROTECT componente	Localização dos arquivos de relatório
ESET PROTECTServidor	*C:\ProgramData\ESET\RemoteAdministrator\Server\EraServerApplicationData\Logs*
Agente ESET Management	*C:\ProgramData\ESET\RemoteAdministrator\Agent\EraAgentApplicationData\Logs* Veja também solução de problemas de conexão do Agente.
ESET PROTECTConsole da Web e Apache Tomcat	*C:\ProgramData\ESET\RemoteAdministrator\Tomcat\Logs* Veja também https://tomcat.apache.org/tomcat-9.0-doc/logging.html
Conector de dispositivo móvel	*C:\ProgramData\ESET\RemoteAdministrator\MDMCore\Logs* Veja também a solução de problemas MDM.
Sensor Rogue Detection	*C:\ProgramData\ESET\Rogue Detection Sensor\Logs*

ESET PROTECT componente	Localização dos arquivos de relatório
ESET Bridge (Proxy HTTP)	Consulte a Ajuda on-line ESET Bridge.

C:\ProgramData é oculto por padrão. Para exibir a pasta:
1.Navegue para **Iniciar** > **Painel de Controle** > **Opções de pasta** > **Exibir**.
2.Selecione **Mostrar arquivos, pastas e drives ocultos** e clique em **OK**.

Linux

ESET PROTECT componente	Localização dos arquivos de relatório
ESET PROTECTServidor	*/var/log/eset/RemoteAdministrator/Server/* */var/log/eset/RemoteAdministrator/EraServerInstaller.log*
Agente ESET Management	*/var/log/eset/RemoteAdministrator/Agent/* */var/log/eset/RemoteAdministrator/EraAgentInstaller.log*
Conector de dispositivo móvel	*/var/log/eset/RemoteAdministrator/MDMCore/* */var/log/eset/RemoteAdministrator/MDMCore/Proxy/* Veja também a solução de problemas MDM.
ESET Bridge (Proxy HTTP)	Consulte a Ajuda on-line ESET Bridge.
ESET PROTECTConsole da Web e Apache Tomcat	*/var/log/tomcat/* Veja também https://tomcat.apache.org/tomcat-9.0-doc/logging.html
ESET RD Sensor	*/var/log/eset/RogueDetectionSensor/*

Equipamento virtual ESET PROTECT

ESET PROTECT componente	Localização dos arquivos de relatório
Configuração VA ESET PROTECT	*/root/appliance-configuration-log.txt*
ESET PROTECTServidor	*/var/log/eset/RemoteAdministrator/EraServerInstaller.log*
ESET Bridge (Proxy HTTP)	Consulte a Ajuda on-line ESET Bridge.

macOS

/Library/Application Support/com.eset.remoteadministrator.agent/Logs/

/Users/%user%/Library/Logs/EraAgentInstaller.log

Ferramenta de diagnóstico

A ferramenta de diagnóstico é uma parte de todos os componentes ESET PROTECT. Ela é usada para coletar e compactar relatórios que podem ser usados por agentes e desenvolvedores de suporte para resolver problemas com componentes de produtos.

Localização da Ferramenta de diagnóstico

Windows

Pasta *C:\Program Files\ESET\RemoteAdministrator\[produto]* **Diagnostic.exe**.

Linux

No diretório a seguir do servidor: */opt/eset/RemoteAdministrator/[produto]/* , existe um **Diagnostic[produto]** executável (uma palavra, por exemplo, **DiagnosticServer**, **DiagnosticAgent**)

Uso (Linux)

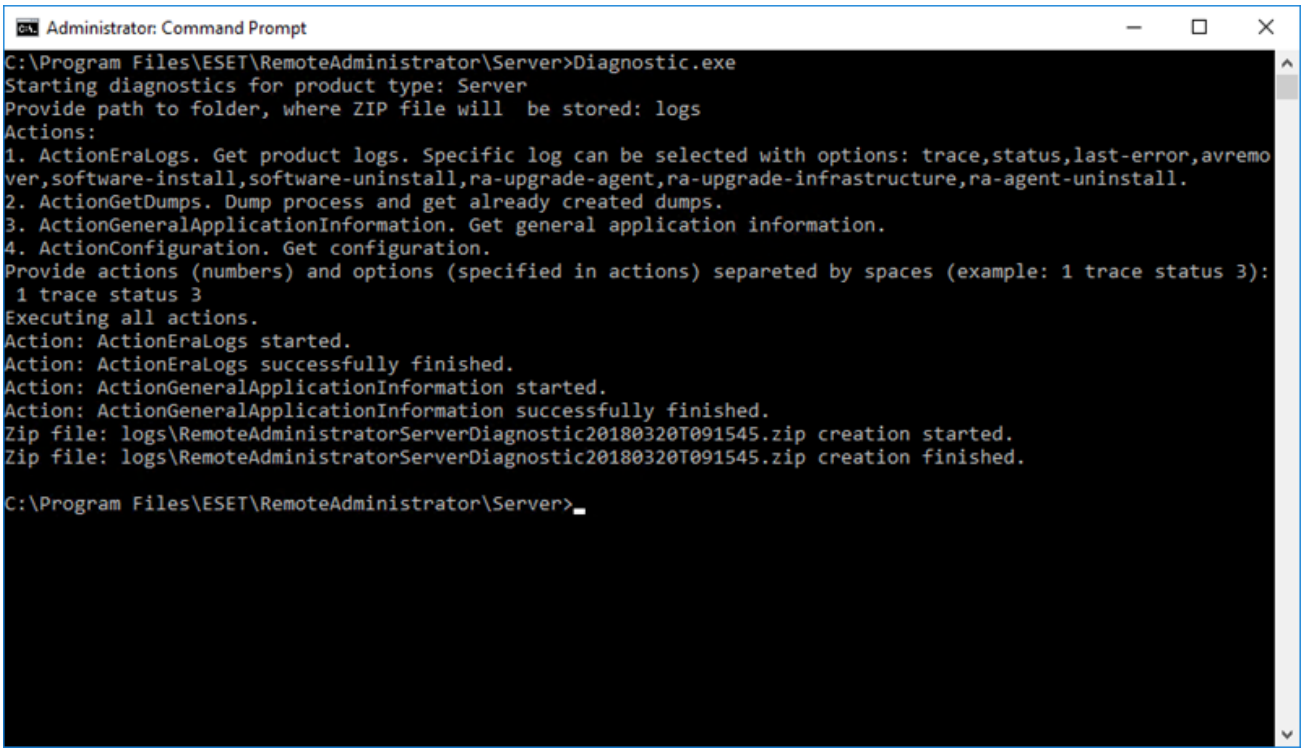
Execute o executável de diagnóstico no terminal como root e siga as instruções exibidas na sua tela.

Uso (Windows)

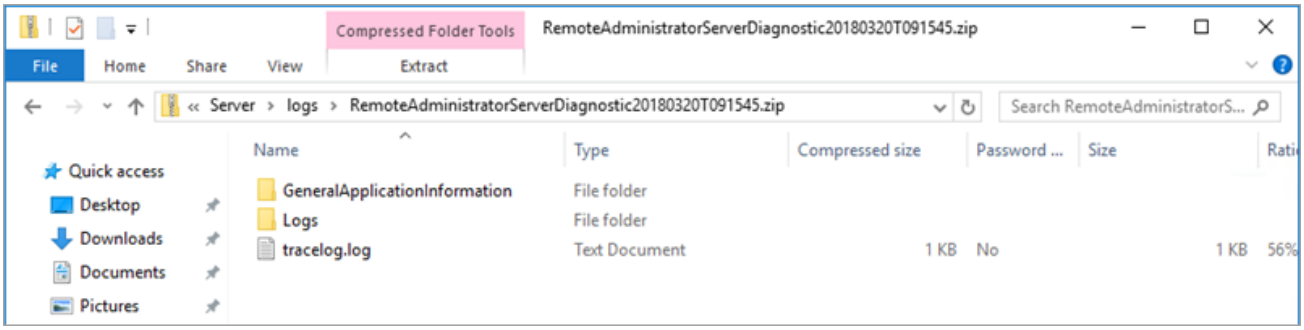
1. Execute a ferramenta usando um prompt de comando.

2. Digite a localização dos relatórios a serem armazenados (em nosso exemplo "logs") e pressione **Enter**.

3. Digite as informações que você quer coletar (em nosso exemplo, `1 trace status 3`). Veja **Ações** abaixo para obter mais informações.



4. Quando terminar, você pode encontrar os relatórios compactados em um arquivo *.zip* no diretório "**logs**" no local da Ferramenta de diagnóstico.



Ações

- **ActionEraLogs** - uma pasta de relatórios é criada onde todos os relatórios são salvos. Para especificar apenas certos relatórios, use um espaço para separar cada relatório.

- **ActionGetDumps** - é criada uma nova pasta. Um arquivo de despejo do processo geralmente é criado se um problema foi detectado. Quando um problema grave for detectado, um arquivo de despejo será criado pelo sistema. Para verificá-lo manualmente, acesse a pasta %temp% (no Windows) ou a pasta /tmp/ (no Linux) e insira um arquivo dmp.

> O serviço de componente (Agent, Server, RD Sensor,) deve estar em execução.

- **ActionGeneralApplicationInformation** - A pasta GeneralApplicationInformation é criada e, dentro dela, o arquivo *GeneralApplicationInformation.txt*. Este arquivo contém informações de texto, incluindo o nome do produto e a versão do produto do produto atualmente instalado.

- **ActionConfiguration** - Uma pasta de configuração será criada onde o arquivo storage.lua for salvo.

Problemas depois da atualização/migração do Servidor ESET PROTECT

Se você não conseguir iniciar o serviço do Servidor ESET PROTECT devido a uma instalação danificada e mensagens de erro de relatório desconhecidas, realize uma operação de reparo usando as etapas mostradas abaixo:

> Recomendamos que você faça um Backup de banco de dados do servidor antes de iniciar a operação de reparo.

1. Navegue para **Iniciar** > **Painel de Controle** > **Programa e Recursos** e clique duas vezes em **Servidor ESET PROTECT**.

2. Selecione **Reparar** e clique em **Avançar**.

3. Reutilize suas configurações de conexão de banco de dados existentes e clique em **Avançar**. Clique em **Sim se for solicitada uma confirmação**. Você pode encontrar aqui as informações de conexão do banco de dados: *%PROGRAMDATA%\ESET\RemoteAdministrator\Server\EraServerApplicationData\Configuration\startupconfiguration.ini*

4. Selecione **Usar senha do administrador já armazenada no banco de dados** e clique em **Avançar**.

5. Selecione **Manter certificados existentes atualmente** e clique em **Avançar**.

6. Ative o Servidor ESET PROTECT com uma chave de licença válida ou selecione **Ativar mais tarde** (consulte o Gerenciamento de licença para instruções adicionais) e clique em **Avançar**.

7. Clique em **Reparar**.

8. Conecte ao console da Web novamente e veja se está tudo OK.

Outros cenários de solução de problemas:

O Servidor ESET PROTECT não está em execução mas há um backup do banco de dados:

1. Restaure seu backup do banco de dados.

2. Verifique se a nova máquina usa o mesmo endereço IP ou nome de host da sua instalação anterior para ter certeza de que os Agentes vão conectar.

3. Repare o ESET PROTECT Server e use o banco de dados que você restaurou.

O Servidor ESET PROTECT não está em execução mas você tem o certificado de servidor exportado e a Autoridade de certificação dele:

1. Verifique se a nova máquina usa o mesmo endereço IP ou nome de host da sua instalação anterior para ter certeza de que os Agentes vão conectar.

2. Repare o ESET PROTECT Server usando certificados de backup (ao reparar, selecione **Carregar certificados do arquivo** e siga as instruções).

O Servidor ESET PROTECT não está em execução e você não tem um backup de banco de dados ou certificado de Servidor ESET PROTECT e Autoridade de certificação:

1. Reparar o Servidor ESET PROTECT.

2. Repare os Agentes ESET Management usando um dos métodos a seguir:

- Script do agente instalador
- Implementação remota (isto irá exigir que você desative o firewall nas máquinas de destino)
- Instalador de componente do Agente manual

Registro em relatório MSI

Isso é útil se você não for capaz de instalar um componente ESET PROTECT no Windows adequadamente, por exemplo Agente ESET Management:

```
msiexec /i C:\Users\Administrator\Downloads\Agent_x64.msi /L*v log.txt
```

ESET PROTECT API

O ESET PROTECT ServerApi (*ServerApi.dll*) é uma interface de programação do aplicativo; um conjunto de funções e ferramentas para a construção de aplicativos personalizados de software para atender às suas necessidades e especificidades. Ao usar o ServerApi, seu aplicativo pode fornecer uma interface, funcionalidade e operações personalizadas que você normalmente realizaria através do console da Web ESET PROTECT, como gerenciamento do ESET PROTECT, gerar e receber relatórios, etc.

Para obter mais informações e exemplos na linguagem C e uma lista de mensagens JSON disponíveis, consulte a ajuda online a seguir:

ESET PROTECT 10.1 API

FAQ

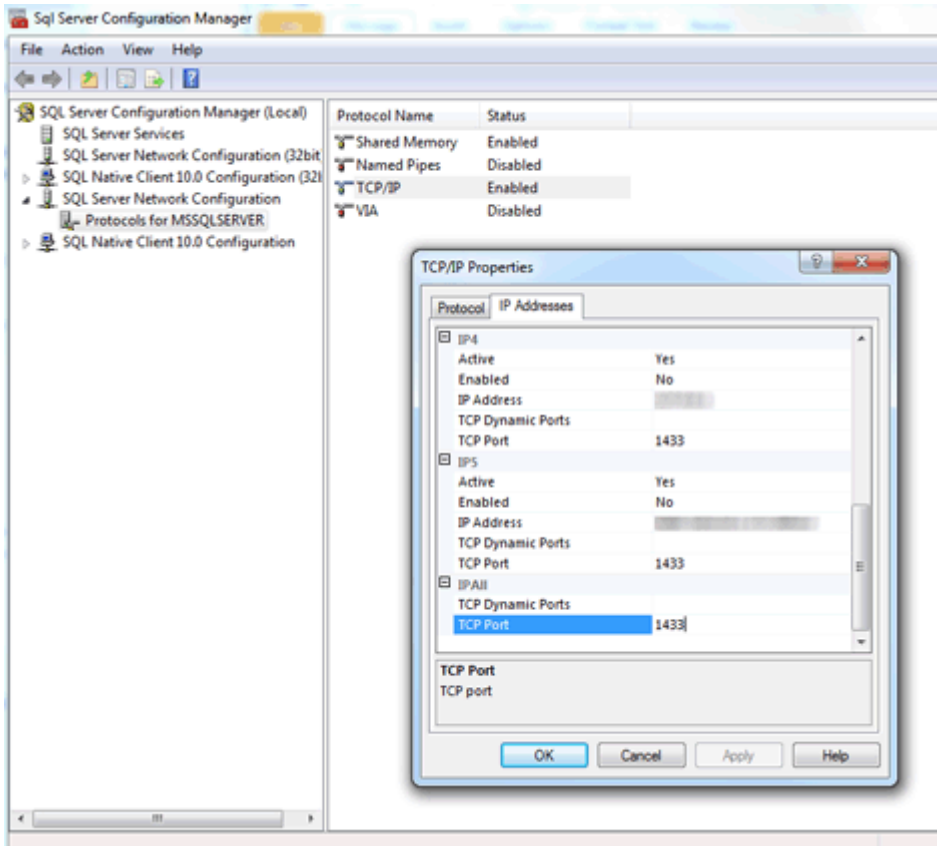
Por que estamos instalando Java em um servidor? Isso não cria um risco de segurança? A maioria das empresas de segurança e estruturas de segurança recomendam que você desinstale o Java dos computadores, especialmente dos servidores.

O console web ESET PROTECT requer que o Java/OpenJDK funcione. Java é um padrão da indústria para consoles baseados na web, e todos os principais consoles web estão usando Java e Servidor web (Apache Tomcat) para sua operação. O Java é necessário para apoiar um servidor da web multi-plataforma. É possível instalar um Servidor da Web em uma máquina dedicada por motivos de segurança.

A partir de janeiro de 2019, atualizações públicas do Oracle JAVA SE 8 para uso de negócios, comercial ou de produção precisarão de uma licença comercial. Se você não comprar uma assinatura JAVA SE, você pode usar este guia para mudar para uma alternativa sem custos. Consulte as versões compatíveis do JDK.

Como determinar qual porta o SQL Server está usando?

Há várias maneiras de determinar a porta usada pelo SQL Server. Você pode obter o resultado mais preciso com o SQL Server Configuration Manager. Veja a figura a seguir para obter um exemplo de onde localizar essas informações no SQL Configuration Manager:



Depois de instalar o SQL Server Express (incluído no pacote ESET PROTECT) no meu Windows Server 2012, ele não parece realizar a escuta em uma porta SQL padrão. É mais provável que a escuta esteja em outra porta, que não a padrão 1433.

Como faço para configurar o MySQL para aceitar grandes pacotes?

Veja Instalação e configuração MySQL para Windows ou Linux.

Se eu instalar o SQL, como devo criar um banco de dados para o ESET PROTECT?

Você não precisa. Um banco de dados é criado pelo instalador *Server.msi*, não pelo Instalador ESET PROTECT. O Instalador ESET PROTECT está incluído para simplificar etapas para você. Ele instala o SQL Server e o banco de dados é criado pelo instalador *Server.msi*.

Instalador ESET PROTECT pode criar um novo banco de dados para mim em uma instalação existente do Microsoft SQL Server se eu fornecer as credenciais e detalhes apropriados da conexão do MS SQL Server? Seria conveniente se o instalador fosse compatível com diferentes versões do SQL Server (2014, 2019, etc.).

O banco de dados é criado pelo *Server.msi*. Sim, é possível criar um banco de dados ESET PROTECT para você nas instâncias do SQL Server instaladas individualmente. As versões compatíveis do Microsoft SQL Server são 2014 e versões posteriores.

O instalador único ESET PROTECT 10.1 instala o Microsoft SQL Server Express 2019 por padrão.

- Se você estiver usando uma versão mais antiga do Windows (Server 2012 ou SBS 2011), o Microsoft SQL Server Express 2014 será instalado por padrão.

- O instalador gera automaticamente uma senha aleatória para autenticação de banco de dados (armazenada em *%PROGRAMDATA%\ESET\RemoteAdministrator\Server\EraServerApplicationData\Configuration\startupconfiguration.ini*).

> O Microsoft SQL Server Express tem um limite de tamanho de 10 GB de cada banco de dados relacional. Não recomendamos usar o Microsoft SQL Server Express:
> - Em ambientes empresariais ou grandes redes.
> - Se quiser usar o ESET PROTECT com o ESET Inspect.

Se a instalação estiver sendo realizada em um SQL Server existente, o SQL Server deve usar o modo de autenticação Windows integrado por padrão?

Não, pois o modo de autenticação Windows pode ser desativado no SQL Server e a única forma de fazer login é usar a autenticação SQL Server (inserir um nome de usuário e senha). Durante a instalação do Servidor ESET PROTECT, a autenticação de modo Misto (Autenticação do Servidor SQL e Autenticação Windows) é obrigatória. Ao instalar manualmente o SQL Server, recomendamos que você crie uma senha raiz (o usuário raiz é intitulado "sa", que significa "security admin" (administrador de segurança)) e a armazene para uso posterior em um local seguro. A senha raiz pode ser necessária ao atualizar o Servidor ESET PROTECT. Você pode configurar a Autenticação Windows depois de instalar o Servidor ESET PROTECT.

Posso usar o MariaDB em vez do MySQL?

Não, o MariaDB não é compatível. Certifique-se de instalar uma versão compatível do MySQL Server e do Conector ODBC. Veja Instalação e configuração MySQL.

Eu tive que instalar o Microsoft .NET Framework 4 como o Instalador ESET PROTECT indicou(http://www.microsoft.com/en-us/download/details.aspx?id=17851),mas isso não funcionou em uma instalação nova do Windows Server 2012 R2 com SP1.

Esse instalador não pode ser usado no Windows Server 2012 devido à política de segurança no Windows Server 2012. O Microsoft .NET Framework deve ser instalado via o **Assistente para adicionar de funções e recursos**.

É muito difícil saber se a instalação do SQL Server está em execução. Como posso saber o que está acontecendo se a instalação levar mais de 10 minutos?

A instalação do SQL Server pode, em casos raros, levar até uma hora. O tempo de instalação depende do desempenho do sistema.

Como faço para redefinir a senha do administrador para meu console da Web (inserida durante a instalação)?

É possível redefinir a senha executando o instalador do servidor e escolhendo **Reparar**. Esteja ciente que a senha pode ser necessária para ter acesso ao banco de dados ESET PROTECT se você não usou a autenticação do Windows durante a criação do banco de dados.

- Tenha cuidado, algumas das opções de reparo potencialmente causam a remoção de dados armazenados.
- A redefinição de senha desativa a 2FA.

Ao importar um arquivo contendo uma lista de computadores a adicionar

ao ESET PROTECT, qual é o formato requerido para o arquivo?

O formato é das linhas a seguir:

Tudo\Grupo1\GrupoN\Computador1
Tudo\Grupo1\GrupoM\ComputadorX

Tudo é o nome obrigatório do grupo de raiz.

É possível usar o IIS em vez de Apache Tomcat? E quanto a outro servidor HTTP?

IIS é um servidor HTTP. O console web precisa de um contêiner de servlet Java (como o Apache Tomcat) para ser executado, o servidor HTTP não é suficiente. Existem soluções sobre como alterar o IIS para um contêiner de servlet Java, mas, em geral, isso não é compatível.

Não usamos o Servidor Apache HTTP, usamos o Apache Tomcat, que é um produto diferente.

O ESET PROTECT tem uma interface de linha de comando?

Sim, temos o ESET PROTECT ServerApi.

É possível instalar o ESET PROTECT em um controlador de domínio?

Não instale o SQL Server em um controlador de domínio (por exemplo, Windows SBS/Essentials). Recomendamos que instale o ESET PROTECT em outro servidor ou não selecione o componente SQL Server Express durante a instalação (isso requer que você use seu Servidor SQL ou MySQL existente para executar o banco de dados ESET PROTECT).

A instalação do Servidor ESET PROTECT vai detectar se SQL já está

instalado no sistema? O que acontece se estiver? E o MySQL?

O ESET PROTECT irá verificar o SQL sendo executado em um sistema caso você esteja usando o assistente de instalação e tenha selecionado o SQL Express para instalar. No caso de já haver SQL em execução em um sistema, o assistente exibirá uma notificação para desinstalar o SQL existente e em seguida vai executar a instalação novamente, ou instalar o ESET PROTECT sem o SQL Express. Veja requisitos de banco de dados para ESET PROTECT.

Onde posso encontrar um componente ESET PROTECT mapeado pela sua versão de lançamento?

Visite nosso artigo da Base de conhecimento.

Como executar uma atualização do ESET PROTECT para a versão mais recente?

Consulte procedimentos de atualização.

Como posso atualizar um sistema sem uma conexão de internet?

Usar um ESET Bridge proxy HTTP instalado em uma máquina que pode se conectar aos servidores de atualização ESET (onde os arquivos de atualização são armazenados em cache) e apontar Endpoints para aquele proxy HTTP em uma rede local. Se seu servidor não tiver uma conexão com a Internet, você pode ativar o recurso de imagem do produto Endpoint em uma máquina, usar uma unidade USB para fornecer arquivos de atualização para este computador e configurar todos os outros computadores off-line para usá-lo como um servidor de atualização.

Para obter detalhes sobre como realizar uma instalação off-line, siga essas instruções.

Como reinstalar meu Servidor ESET PROTECT e conectá-lo a um servidor SQL existente se o servidor SQL foi criado automaticamente pela

instalação inicial do ESET PROTECT?

Se você estiver instalando a nova instância do Servidor ESET PROTECT usando a mesma conta do usuário (por exemplo, uma conta de domínio do administrador) na qual instalou o servidor ESET PROTECT original, você pode usar o **MS SQL Server via autenticação do Windows**.

Como faço para corrigir problemas com sincronização do Active Directory no Linux?

Verifique se seu nome de domínio é digitado em letras maiúsculas (`administrator@TEST.LOCAL` em vez de `administrator@test.local`).

Existe uma maneira de usar meu próprio recurso de rede (como o compartilhamento SMB) em vez do repositório?

Você pode optar por fornecer o URL direto de onde um pacote está localizado. Se estiver usando um compartilhamento de arquivos, especifique-o no formato a seguir: file:// seguido pelo caminho de rede completo para o arquivo, por exemplo:

file://\\eraserver\install\ees_nt64_ENU.msi

Como posso redefinir ou alterar minha senha?

Idealmente, a conta de administrador deve ser usada somente para criar contas para administradores individuais. Assim que as contas de administradores forem criadas, a senha de administrador deverá ser salva e a conta de administrador não deverá ser usada. Essa prática permite que a conta de administrador seja usada apenas para redefinir senhas/detalhes de conta.

Como redefinir senha de uma conta de Administrador ESET PROTECT incorporada:

1. Abra **Programas e recursos** (execute appwiz.cpl), localize o Servidor ESET PROTECT e clique nele com o botão direito.
2. Selecione **Alterar** no menu de contexto.
3. Escolha **Reparar**.
4. Especifique os detalhes de conexão do banco de dados.

5.Selecione **Usar banco de dados existente e aplicar atualização**.

6.Desmarque **Usar senha já armazenada no banco de dados** e insira uma nova senha.

7.Entre no Console da Web ESET PROTECT com sua nova senha.

Recomendamos muito criar contas adicionais com direitos de acesso específicos com base em competências desejadas de conta.

Como posso alterar as portas do Servidor ESET PROTECT e console da Web ESET PROTECT?

É necessário alterar a porta na configuração do seu servidor da web para permitir conexões do servidor para a nova porta. Para fazer isso, siga as etapas a seguir:

1. Desligue seu servidor da Web.
2. Modifique a porta na sua configuração do servidor web.

   a)Abra o arquivo *webapps/era/WEB-INF/classes/sk/eset/era/g2webconsole/server/modules/config/EraWebServerConfig.properties*

   b)Defina o novo número da porta (por exemplo, `server_port=44591`)
3. Iniciar o servidor web novamente.

Posso atualizar do ERA 5.x/6.x ou ESMC 7.x diretamente para o ESET PROTECT 10.1 usando o Instalador Tudo-em-um?

Se você tiver o ERA 5.x/6.x ou o ESMC 7.0/7.1:

- A atualização direta para ESET PROTECT 10.1 o não é compatível.
- Realize uma instalação limpa do ESET PROTECT 10.1.

Você pode atualizar diretamente para o ESET PROTECT 10.1 do ESMC 7.2 e de versões posteriores.

Estou recebendo mensagens de erro ou tenho problemas com o ESET PROTECT, o que devo fazer?

Veja os FAQs de Solução de problemas.

Acordo de Licença para o Usuário final

Em vigor a partir de 19 de outubro de 2021.

IMPORTANTE: leia atentamente os termos e as condições relativos ao produto estabelecidos a seguir antes do download, da instalação, da cópia ou do uso. **POR MEIO DO DOWNLOAD, DA INSTALAÇÃO, DA CÓPIA OU DO USO DO SOFTWARE, VOCÊ EXPRESSA SEU CONSENTIMENTO COM ESTES TERMOS E CONDIÇÕES E RECONHECE A POLÍTICA DE PRIVACIDADE.**

Acordo de Licença do Usuário Final

Sob os termos deste Contrato de licença para o usuário final (“Contrato”) executado por e entre a ESET, spol. s r. o., tendo sua sede em Einsteinova 24, 85101 Bratislava, Slovak Republic, registrada no Registro Comercial do Tribunal Regional de Bratislava I, Seção Sro, Nº de entrada 3586/B, Número de registro da empresa: 31333532 ("ESET" ou “Provedor”) e Você, uma pessoa física ou jurídica (“Você” ou “Usuário final”), recebe o direito de uso do Software definido no Artigo 1 deste Contrato. O Software definido no Artigo 1 deste Contrato pode ser armazenado em um carregador de dados, enviado por e-mail, obtido por download da Internet, obtido por download de servidores do Provedor ou obtido de outras fontes, sujeito aos termos e às condições especificados a seguir.

ESTE É UM CONTRATO SOBRE DIREITOS DO USUÁRIO FINAL E NÃO UM CONTRATO DE VENDA. O Provedor permanece o proprietário da cópia de Software e da mídia física fornecida na embalagem comercial e de todas as outras cópias a que o Usuário final tiver direito nos termos deste Contrato.

Ao clicar na opção “Eu aceito” ou “Eu aceito...” durante a instalação, download, cópia ou uso do Software, Você concorda com os termos e condições deste Contrato e reconhece a Política de Privacidade. Se Você não concordar com os termos e as condições deste Contrato e/ou com a Política de Privacidade, clique imediatamente na opção para cancelar, cancele a instalação ou o download, ou destrua ou devolva o Software, a mídia de instalação, a documentação que vem com o produto e o recibo de vendas para o Provedor ou a loja onde Você adquiriu o Software.

VOCÊ CONCORDA QUE SEU USO DO SOFTWARE CONFIRMA QUE VOCÊ LEU ESTE CONTRATO, QUE O COMPREENDEU E CONCORDA EM ESTAR VINCULADO A ELE POR MEIO DE SEUS TERMOS E CONDIÇÕES.

1. **Software.** Conforme usado neste Contrato, o termo "Software" significa: (i) o programa de computador acompanhado por este Contrato e todos os seus componentes; (ii) todos os conteúdos de discos, CD-ROMs, DVDs, e-mails e anexos, ou outras mídias nas quais este Contrato é fornecido, inclusive o formulário de código de objeto do Software fornecido no transportador de dados, através de correio eletrônico ou baixado na Internet; (iii) qualquer material explicativo por escrito relacionado e qualquer outra documentação possível em relação ao Software, sobretudo qualquer descrição do Software, suas especificações, qualquer descrição das propriedades ou operação do Software, qualquer descrição do ambiente operacional no qual o Software é usado, instruções para o uso ou instalação do Software ou qualquer descrição sobre como usar o Software ("Documentação"); (iv) cópias do Software, patches para possíveis erros no Software, adições ao Software, extensões ao Software, versões modificadas do Software e atualizações de componentes do Software se houverem, são licenciadas a Você pelo Provedor de acordo com o Artigo 3 deste Contrato. O Software será fornecido exclusivamente na forma

de código de objeto executável.

2. **Instalação, Computador e uma Chave de Licença**. O Software fornecido em um carregador de dados, enviado por email eletrônico, obtido por download da Internet, obtido por download de servidores do Provedor ou obtido de outras fontes requer instalação. Você deve instalar o Software em um Computador configurado corretamente que, pelo menos, esteja de acordo com os requisitos definidos na Documentação. A metodologia de instalação é descrita na Documentação. Nenhum computador ou hardware que possa ter um efeito adverso no Software pode ser instalado no Computador no qual Você instalar o Software. Computer significa hardware, incluindo sem limitação computadores pessoais, notebooks, estações de trabalho, computadores tipo palmtop, smartphones, dispositivos eletrônicos manuais ou outros dispositivos eletrônicos para os quais o Software foi projetado, no qual ele será instalado e/ou usado. Chave de licença significa a sequência exclusiva de símbolos, letras, números ou sinais especiais fornecidos ao Usuário Final para permitir o uso legal do Software, sua versão específica ou extensão do termo da Licença em conformidade com esse Contrato.

3. **Licença**. Desde que Você tenha concordado com os termos deste Contrato e cumprido com todos os termos e condições estabelecidos neste documento, o Provedor deverá conceder a Você os seguintes direitos ("a Licença"):

a) **Instalação e uso.** Você deverá ter o direito não exclusivo e não transferível para instalar o Software no disco rígido de um computador ou outra mídia permanente para armazenamento dos dados, instalação e armazenamento do Software na memória de um sistema computacional e para implementar, armazenar e exibir o Software.

b) **Estipulação do número de licenças.** O direito de utilizar o Software deverá estar vinculado ao número de Usuários finais. Um Usuário final deverá ser selecionado para referir-se ao seguinte: (i) instalação do Software em um sistema computacional; ou (ii) se a extensão de uma licença estiver vinculada ao número de caixas de email, então um Usuário final deverá ser selecionado para referir-se a um usuário de computador que aceita e-mail através de um Agente de usuário de email (“MUA”). Se um MUA aceitar e-mail e, subsequentemente, distribuí-lo de forma automática a vários usuários, então o número de Usuários finais deverá ser determinado de acordo com o número real de usuários para os quais o e-mail será distribuído. Se um servidor de email executar a função de um portal de email, o número de Usuários finais deverá ser igual ao número de servidores de email para o qual esse portal oferece serviços. Se um número não especificado de endereços de emails eletrônicos for direcionado para um usuário e aceito por ele (por exemplo, por meio de alias) e as mensagens não forem automaticamente distribuídas pelo cliente para um número maior de usuários, uma licença para um computador será exigida. Você não deve usar a mesma Licença ao mesmo tempo em mais de um computador. O Usuário Final tem o direito de inserir a Chave de Licença para o Software apenas até a extensão em que o Usuário Final tem o direito de usar o Software de acordo com a limitação criada pelo número de Licenças oferecido pelo Provedor. A Chave de licença é considerada confidencial, Você não deve compartilhar a Licença com terceiros ou permitir que terceiros usem a Chave de licença a menos que isso seja permitido por esse Contrato ou pelo Provedor. Se sua Chave de licença for comprometida, notifique o Provedor imediatamente.

c) **Home/Business Edition.** Uma versão Home Edition do Software será usada exclusivamente em ambientes particulares e/ou não comerciais apenas para uso familiar e doméstico. Uma versão Business Edition do Software deve ser obtida para uso em ambiente comercial, assim como para usar o Software em servidores de e-mail, relés de e-mail, gateways de e-mail ou gateways de Internet.

d) **Vigência da licença.** O direito de utilizar o Software deverá estar limitado a um período.

e) **Software OEM.** O Software classificado como "OEM" deve estar limitado ao Computador com o qual Você obteve o software. Ele não pode ser transferido para um computador diferente.

f) **Software NFR, AVALIAÇÃO.** Software classificado como "Não para revenda", NFR ou AVALIAÇÃO não pode ser atribuído para pagamento e deve ser usado apenas para demonstração ou teste dos recursos do Software.

g) **Término da licença.** A Licença deverá terminar automaticamente no final do período para o qual ela foi concedida. Se Você deixar de cumprir qualquer das cláusulas deste Contrato, o Provedor terá o direito de retirar-se do Contrato, sem prejuízo de qualquer direito ou solução jurídica abertos ao Provedor em tais eventualidades. No caso de cancelamento da Licença, Você deve excluir, destruir ou devolver imediatamente, às suas custas, o Software e todas as cópias de backup para a ESET ou loja em que Você obteve o Software. Mediante a rescisão da Licença o Provedor também estará autorizado a cancelar o direito do Usuário Final de usar as funções do Software que exigem conexão aos servidores do Provedor ou servidores de terceiros.

4. **Funções com coleta de dados e requisitos de conexão com a internet.** Para operar corretamente, o Software exige conexão com a Internet e deve conectar-se em intervalos regulares aos servidores do Provedor ou a servidores de terceiros e a coleta de dados aplicáveis de acordo com a Política de Privacidade. A conexão com a Internet e coleta de dados aplicáveis é necessária para o funcionamento do Software e para a atualização e upgrade do Software. O Provedor deverá emitir atualizações ou upgrades para o Software ("Atualizações"), mas não deverá ser obrigado a fornecer Atualizações. Esta função está ativada nas configurações padrão do Software, e as Atualizações são, portanto, instaladas automaticamente, a menos que o Usuário Final tenha desativado a instalação automática das Atualizações. Para o fornecimento de Atualizações é necessário fazer a verificação de autenticidade da Licença, incluindo informações sobre o Computador e/ou a plataforma na qual o Software está instalado de acordo com a Política de Privacidade.

O fornecimento de qualquer Atualização pode estar sujeito a uma Política de Fim de Vida ("Política EOL"), que está disponível em https://go.eset.com/eol_business. Nenhuma Atualização será fornecida depois do Software ou de qualquer um de seus recursos chegar à data de Fim da vida, conforme definido na Política EOL.

Para os fins desse Contrato é necessário coletar, processar e armazenar dados permitindo ao Provedor identificar Você de acordo com a Política de Privacidade. Você doravante reconhece que o Provedor verifica usando seus próprios meios se Você está usando o Software de acordo com as cláusulas deste Contrato. Você doravante reconhece que, para os fins deste Contrato, é necessário que seus dados sejam transferidos durante a comunicação entre o Software e os sistemas computacionais do Provedor ou de seus parceiros comerciais como parte da rede de distribuição e suporte do Provedor para garantir a funcionalidade do Software e a autorização para usar o Software e para a proteção dos direitos do Provedor.

Seguindo a conclusão deste Contrato, o Provedor ou qualquer de seus parceiros comerciais como parte da rede de distribuição e suporte do Provedor terão o direito de transferir, processar e armazenar dados essenciais que identifiquem Você, para fins de faturamento, execução deste Contrato e transmissão de notificações no seu Computador.

Detalhes sobre privacidade, proteção de dados pessoais e seus direitos como um assunto de dados podem ser encontrados na Política de Privacidade, que está disponível no site do Provedor e pode ser acessada diretamente a partir do processo de instalação. Você também pode visitar a seção de ajuda do Software.

5. **Exercício dos direitos do Usuário final**. Você deve exercer os direitos do Usuário final em pessoa ou por meio de seus funcionários. Você somente pode usar o Software para garantir suas operações e proteger esses Computadores ou sistemas computacionais para os quais Você tiver obtido uma Licença.

6. **Restrições aos direitos.** Você não pode copiar, distribuir, extrair componentes ou produzir trabalhos derivativos do Software. Ao usar o Software, Você é obrigado a cumprir as seguintes restrições:

a) Você pode fazer uma cópia do Software em uma mídia para armazenamento permanente como uma cópia de backup de arquivos, desde que a sua cópia de backup de arquivos não seja instalada ou usada em qualquer computador. Quaisquer outras cópias que Você fizer do Software constituirá uma violação deste Contrato.

b) Você não pode usar, modificar, traduzir ou reproduzir o Software ou transferir direitos para uso do Software nem cópias do Software de qualquer forma que não conforme expressamente fornecido neste Contrato.

c) Você não pode vender, sublicenciar, arrendar ou alugar ou emprestar o Software ou usar o Software para a prestação de serviços comerciais.

d) Você não pode fazer engenharia reversa, reverter a compilação ou desmontar o Software ou tentar descobrir de outra maneira o código fonte do Software, exceto na medida em que essa restrição for expressamente proibida por lei.

e) Você concorda que Você usará o Software somente de uma maneira que esteja de acordo com todas as leis aplicáveis na jurisdição em que Você usa o Software, incluindo sem limitação, restrições aplicáveis relacionadas a direitos autorais e a outros direitos de propriedade intelectual.

f) Você concorda que Você somente usará o Software e suas funções de uma forma que não limite as possibilidades de outros Usuários Finais acessarem esses serviços. O Provedor reserva o direito de limitar o escopo de serviços oferecidos para os usuários finais individuais, para habilitar o uso de serviços pelo número mais alto possível de Usuários Finais. A limitação do escopo de serviços também deve significar a eliminação total da possibilidade de usar qualquer uma das funções do Software e exclusão dos Dados e informação sobre os servidores do Provedor ou servidores de terceiro relacionados a uma função específica do Software.

g) Você concorda em não exercer nenhuma atividade que envolva o uso da Chave de licença que seja contrária aos termos desse Contrato ou que cause o fornecimento da Chave de licença para qualquer pessoa que não tenha o direito de usar o Software, como a transferência de Chaves de licença usadas ou não usadas de qualquer forma, assim como a reprodução ou distribuição não autorizada de Chaves de licença duplicadas ou geradas ou o uso do Software como resultado do uso de uma Chave de licença obtida de uma origem que não sejam o Provedor.

7. **Direitos autorais**. O Software e todos os direitos, incluindo, sem limitação, direitos de propriedade e direitos de propriedade intelectual, mencionados neste documento são de propriedade da ESET e/ou seus licenciadores. Eles estão protegidos pelas cláusulas de tratados internacionais e por todas as outras leis aplicáveis do país no qual o Software está sendo utilizado. A estrutura, a organização e o código do Software são segredos comerciais valiosos e informações confidenciais da ESET e/ou de seus licenciadores. Você não deve copiar o Software, exceto conforme especificado no Artigo 6(a). Quaisquer cópias que Você tiver permissão para fazer de acordo com este Contrato devem conter os mesmos avisos de direitos autorais e de propriedade que aparecerem no Software. Se Você fizer engenharia reversa, reverter a compilação, desmontar ou tentar descobrir de outra maneira o código fonte do Software, em violação das cláusulas deste Contrato, Você concorda que quaisquer informações relacionadas obtidas deverão automática e irrevogavelmente ser consideradas transferidas ao Provedor e de propriedade do Provedor em sua totalidade a partir do momento em que essas informações existirem, não obstante os direitos do Provedor em relação à violação deste Contrato.

8. **Reserva de direitos**. O Provedor reserva todos os direitos ao Software, com exceção dos direitos expressamente concedidos, nos termos deste Contrato, a Você como o Usuário final do Software.

9. **Versões em diversos idiomas, software de mídia dupla, várias cópias**. No caso de o Software suportar diversas plataformas ou idiomas ou se Você receber diversas cópias do Software, Você poderá usar o Software apenas para o número de sistemas computacionais e para as versões para as quais Você obteve uma Licença. Você não pode vender, alugar, arrendar, sublicenciar, emprestar ou transferir versões ou cópias do Software que Você não usar.

10. **Início e término do Contrato.** Este Contrato é vigente a partir da data em que Você concordar com os termos deste Contrato. Você pode terminar este Contrato a qualquer momento ao desinstalar, destruir e devolver definitivamente, às suas custas, o Software, todas as cópias de backup e todos os materiais relacionados fornecidos pelo Provedor ou pelos seus parceiros comerciais. Seu direito de usar o Software e qualquer um de seus recursos pode estar sujeito à Política EOL. Depois que o Software ou qualquer um de seus recursos chegar à data de fim de vida definida na Política EOL, o direito de utilizar o Software será encerrado. Independentemente do modo de término deste Contrato, as cláusulas dos Artigos 7, 8, 11, 13, 19 e 21 deverão continuar a ser

aplicadas por um tempo ilimitado.

11. **DECLARAÇÕES DO USUÁRIO FINAL**. COMO O USUÁRIO FINAL, VOCÊ RECONHECE QUE O SOFTWARE É FORNECIDO "NA CONDIÇÃO EM QUE ENCONTRA", SEM UMA GARANTIA DE QUALQUER TIPO, EXPRESSA OU IMPLÍCITA, E NA EXTENSÃO MÁXIMA PERMITIDA PELA LEGISLAÇÃO APLICÁVEL. O PROVEDOR, NEM OS LICENCIADORES NEM OS AFILIADOS NEM OS DETENTORES DOS DIREITOS AUTORAIS FAZEM QUALQUER TIPO DE REPRESENTAÇÕES OU GARANTIAS, EXPRESSAS OU IMPLÍCITAS, INCLUINDO, MAS NÃO SE LIMITANDO ÀS GARANTIAS DE COMERCIALIZAÇÃO OU ADEQUAÇÃO PARA UMA DETERMINADA FINALIDADE OU QUE O SOFTWARE NÃO INFRINGIRÁ QUAISQUER PATENTES DE TERCEIROS, DIREITOS AUTORAIS, MARCAS COMERCIAIS OU OUTROS DIREITOS. NÃO HÁ GARANTIA DO PROVEDOR OU QUALQUER OUTRA PARTE DE QUE AS FUNÇÕES CONTIDAS NO SOFTWARE ATENDERÃO SEUS REQUISITOS OU QUE A OPERAÇÃO DO SOFTWARE NÃO SERÁ INTERROMPIDA E NÃO TERÁ ERROS. VOCÊ ASSUME TOTAL RESPONSABILIDADE E RISCO PELA SELEÇÃO DO SOFTWARE PARA ATINGIR OS RESULTADOS PRETENDIDOS E PARA A INSTALAÇÃO, USO E RESULTADOS OBTIDOS A PARTIR DELE.

12. **Não há outras obrigações**. Este Contrato não cria obrigações por parte do Provedor e de seus licenciadores diferentes daquelas especificamente definidas neste documento.

13. **LIMITAÇÃO DE RESPONSABILIDADE**. ATÉ A EXTENSÃO MÁXIMA PERMITIDA PELA LEGISLAÇÃO APLICÁVEL, EM NENHUMA HIPÓTESE, O PROVEDOR, SEUS FUNCIONÁRIOS OU LICENCIADORES DEVERÃO SER CONSIDERADOS RESPONSÁVEIS POR QUALQUER PERDA DE LUCROS, RECEITA, VENDAS, DADOS OU CUSTOS DE AQUISIÇÃO DE BENS OU SERVIÇOS, DANOS MATERIAIS, DANOS PESSOAIS, INTERRUPÇÃO NOS NEGÓCIOS, PERDA DE INFORMAÇÕES COMERCIAIS OU POR QUAISQUER DANOS DIRETOS, INDIRETOS, ACIDENTAIS, ECONÔMICOS, DE COBERTURA, PUNITIVOS, ESPECIAIS OU SUBSEQUENTES, MAS CAUSADOS POR E DECORRENTES DO CONTRATO, DANOS, NEGLIGÊNCIA OU OUTRA TEORIA DE RESPONSABILIDADE, DECORRENTE DA INSTALAÇÃO, DO USO OU DA INCAPACIDADE DE USAR O SOFTWARE, MESMO QUE O PROVEDOR OU SEUS LICENCIADORES OU AFILIADOS SEJAM AVISADOS DA POSSIBILIDADE DE TAIS DANOS. COMO ALGUNS PAÍSES E JURISDIÇÕES NÃO PERMITEM A EXCLUSÃO DA RESPONSABILIDADE, MAS PODEM PERMITIR A SUA LIMITAÇÃO, A RESPONSABILIDADE DO PROVEDOR, SEUS FUNCIONÁRIOS OU LICENCIADORES OU AFILIADOS, NESSES CASOS, DEVERÁ ESTAR LIMITADA À SOMA QUE VOCÊ PAGOU PELA LICENÇA.

14. Nada contido neste Contrato deverá prejudicar os direitos legais de qualquer parte que atua como um consumidor se estiver executando o contrariem.

15. **Suporte técnico**. A ESET ou terceiros comissionados pela ESET deverão fornecer suporte técnico a seu critério, sem quaisquer garantias ou declarações. Nenhum suporte técnico será fornecido depois do Software ou de qualquer um de seus recursos chegar à data de Fim da vida, conforme definido na Política EOL. O Usuário final deverá ser solicitado a fazer backup de todos os dados, software e recursos de programa existentes antes do fornecimento de suporte técnico. A ESET e/ou terceiros comissionados pela ESET não pode aceitar responsabilidade por danos ou perda de dados, de propriedade, de software ou hardware ou perda de lucros devido ao fornecimento de suporte técnico. A ESET e/ou terceiros comissionados pela ESET reserva-se o direito de decidir que a solução do problema está além do escopo de suporte técnico. A ESET reserva-se o direito de recusar, suspender ou terminar o fornecimento de suporte técnico a seu critério. Informações de licença, Informações e outros dados em conformidade com a Política de Privacidade podem ser necessários para o fornecimento de suporte técnico.

16. **Transferência da licença**. O Software pode ser transferido de um sistema computacional para outro, a não ser que seja contrário aos termos do Contrato. Se não for contrário aos termos do Contrato, o Usuário Final somente será autorizado a transferir permanentemente a Licença e todos os direitos decorrentes deste Contrato para outro Usuário final com o consentimento do Provedor, desde que (i) o Usuário final original não retenha nenhuma cópia do Software, (ii) a transferência de direitos seja direta, ou seja, do Usuário final original para o novo Usuário final; (iii) o novo Usuário final tenha assumido todos os direitos e obrigações incumbidos ao Usuário final original,

nos termos deste Contrato; (iv) o Usuário final original tenha fornecido ao novo Usuário final a documentação que permite a verificação da autenticidade do Software, como especificado no Artigo 17.

17. **Verificação da autenticidade do Software.** O Usuário final pode demonstrar direito de usar o Software em uma das seguintes formas: (i) por meio de um certificado de licença emitido pelo Provedor ou por um terceiro indicado pelo Provedor, (ii) por meio de um acordo de licença por escrito, se tal acordo foi concluído, (iii) por meio do envio de um email enviado para o Provedor contendo detalhes do licenciamento (nome de usuário e senha). Informações de licença e dados de identificação do Usuário Final em conformidade com a Política de Privacidade podem ser necessários para a verificação de legitimidade do Software.

18. **Licenciamento para as autoridades públicas e para o governo dos EUA**. O Software deve ser fornecido às autoridades públicas, incluindo o governo dos Estados Unidos com os direitos de licença e as restrições descritas neste Contrato.

19. **Conformidade com o controle comercial**.

a) Você não vai, direta ou indiretamente, exportar, reexportar, transferir ou disponibilizar o Software a qualquer pessoa, nem utilizá-lo de qualquer maneira ou estar envolvido em qualquer ação que possa resultar na ESET ou em suas empresas proprietárias, subsidiárias e as subsidiárias de qualquer uma de suas proprietárias, bem como entidades controladas por suas proprietárias ("Filiais"), violando ou sujeitas a consequências negativas sob as Leis de Controle Comercial, que incluem:

i. quaisquer leis que controlem, restrinjam ou imponham requisitos de licenciamento para a exportação, reexportação ou transferência de bens, software, tecnologia ou serviços, emitidos ou adotados por qualquer governo, estado ou autoridade reguladora dos Estados Unidos da América, Cingapura, Reino Unido, União Europeia ou qualquer um de seus Estados-Membros ou qualquer país no qual as obrigações sob o Contrato sejam executadas, ou no qual a ESET ou qualquer uma de suas Filiais seja incorporada ou onde opere e

ii. quaisquer sanções, restrições, embargos econômicos, financeiros, comerciais ou outros, proibição de importação ou exportação, proibição da transferência de fundos ou ativos ou da realização de serviços, ou medidas equivalentes impostas por qualquer governo, estado ou autoridade reguladora dos Estados Unidos da América, Cingapura, Reino Unido, União Europeia ou qualquer um de seus Estados Membros, ou qualquer país no qual as obrigações sob o Contrato sejam executadas, ou no qual a ESET ou qualquer uma de suas Filiais seja incorporada ou onde opere.

(os atos legais mencionados nos pontos i e ii. acima, juntos, como "Leis de Controle Comercial").

b) A ESET terá o direito de suspender suas obrigações sob, ou rescindir, esses Termos com efeito imediato no caso de:

i. A ESET determinar que, em sua opinião razoável, o Usuário infringiu ou provavelmente vai infringir a disposição do Artigo 19 a) do Contrato; ou

ii. o Usuário Final e/ou o Software se tornar sujeito às Leis de Controle Comercial e, como resultado, a ESET determinar que, em sua opinião razoável, o desempenho contínuo de suas obrigações sob o Contrato poderia resultar na ESET ou suas Filiais violarem, ou estarem sujeitas a consequências negativas sob, as Leis de Controle Comercial.

c) Nada no Contrato tem a intenção de, e nada deve ser interpretado ou construído, para induzir ou requerer que qualquer uma das partes aja ou não aja (ou concorde em agir ou não agir) de qualquer maneira que não seja consistente com, que seja penalizada por ou proibida sob qualquer Lei de Controle Comercial aplicável.

20. **Avisos**. Todos os avisos e a devolução do Software e a Documentação devem ser entregues a: ESET, spol. s r.

o., Einsteinova 24, 85101 Bratislava, Slovak Republic, sem prejuízo do direito da ESET de comunicar a Você qualquer alteração a este Contrato, Políticas de Privacidade, Política EOL e Documentação de acordo com o art. 22 do Contrato. A ESET pode enviar a Você e-mails, notificações no aplicativo por meio do seu Software ou Conta ou publicar a comunicação em nosso site. Você concorda em receber comunicações legais da ESET em formato eletrônico, incluindo quaisquer comunicações sobre alteração nos Termos, Termos Especiais ou Políticas de Privacidade, qualquer tipo de proposta/aceitação de contrato ou convites para tratar, avisos ou outras comunicações legais. Tal comunicação eletrônica será considerada recebida por escrito, a menos que as leis aplicáveis especificamente solicitem uma forma de comunicação diferente.

21. **Legislação aplicável**. Este Contrato deverá ser interpretado e regido segundo as leis da República Eslovaca. O Usuário final e o Provedor concordam que os princípios do conflito da legislação e a Convenção das Nações Unidas sobre Contratos de Venda Internacional de Bens não se aplicam a este Contrato. Você concorda expressamente que quaisquer disputas ou reclamações decorrentes deste Contrato com relação ao Provedor ou quaisquer disputas ou reivindicações relativas ao uso do Software serão resolvidos pelo Tribunal Regional de Bratislava I e Você concorda expressamente com o referido tribunal que exerce a jurisdição.

22. **Disposições gerais**. Se uma ou mais cláusulas deste Contrato forem inválidas ou não aplicáveis, isso não deverá afetar a validade das outras cláusulas restantes do Contrato, que deverão permanecer válidas e vigentes de acordo com as condições estipuladas neste documento. Este Contrato foi assinado em inglês. Caso qualquer tradução do Contrato seja preparada para a conveniência ou qualquer outra finalidade ou em qualquer caso de discrepância entre as versões de idiomas deste Contrato, a versão em inglês prevalecerá.

A ESET reserva o direito de fazer alterações no Software, assim como revisar os termos deste Contrato, seus Anexos, Adendos, Política de Privacidade, Política EOL e Documentação ou qualquer parte deles, a qualquer momento, atualizando o documento relevante (i) para refletir alterações no Software ou na forma como a ESET faz negócios, (ii) por motivos de responsabilidade legal, regulação ou de segurança, ou (iii) para impedir abusos ou danos. Você será notificado sobre qualquer revisão do Contrato por e-mail, notificação no aplicativo ou por outros meios eletrônicos. Se Você não concordar com as alterações propostas no Contrato, Você pode rescindir o Contrato de acordo com o Art. 10 dentro de 30 dias após receber um aviso da alteração. A menos que Você rescinda o Contrato dentro deste limite de tempo, as alterações propostas serão consideradas aceitas e estarão em vigor em relação a Você a partir da data em que Você recebeu um aviso da alteração.

Este é todo o acordo entre o Provedor e Você em relação ao Software e anula qualquer declaração, discussão, acordo, comunicação ou propaganda anterior em relação ao Software.

ADENDO AO CONTRATO

Encaminhamento de informações ao Provedor. Provisões adicionais são aplicáveis ao Encaminhamento de informações ao Provedor da seguinte forma:

O Software contém funções que coletam dados sobre o processo de instalação, o Computador e/ou a plataforma na qual o Software está instalado, informações sobre as operações e funcionalidades do Software e informações sobre os dispositivos gerenciados (doravante as “Informações”) e envia-as ao Provedor. As Informações podem conter dados (inclusive dados pessoais obtidos de forma aleatória ou acidental) a respeito de dispositivos gerenciados. Ao ativar esta função do Software, Informações podem ser coletadas e processadas pelo Provedor como especificado na Política de privacidade e de acordo com os regulamentos legais relevantes.

O Software requer um componente instalado em um computador gerenciado, que permite a transferência de informações entre o computador gerenciado e o software de gerenciamento remoto. Informações que estão sujeitas a transferência contém dados de gerenciamento como informações de hardware e software do computador gerenciado e instruções de gerenciamento do software de gerenciamento remoto. Outros conteúdos dos dados transferidos do computador gerenciado serão determinados pelas configurações do software instalado no computador gerenciado. O conteúdo das instruções do software de gerenciamento será determinado pelas

configurações do software de gerenciamento remoto.

EULAID: EULA-PRODUCT-PROTECT; 3537.0

Política de Privacidade

ESET, spol. s r. o., com sede em Einsteinova 24, 851 01 Bratislava, República Eslovaca, registrada no Registro Comercial administrado pela Corte Distrital Bratislava I, Seção Sro, Registro Nº. 3586/B, Número de Registro Comercial: 31333532 como o Controlador de Dados (“ESET” ou “Nós”) deseja ser transparente quando ao processamento de dados pessoais e privacidade de nossos clientes. Para isso, estamos publicando essa Política de Privacidade com o objetivo exclusivo de informar nosso cliente ("Usuário Final" ou "Você") sobre os tópicos a seguir:

- Processamento de dados pessoais,
- Confidencialidade de Dados,
- Direitos do sujeito dos dados.

Processamento de dados pessoais

Serviços prestados pela ESET e implementados em nosso produto são fornecidos sob os termos do Acordo de Licença para o Usuário Final (“EULA”), mas alguns deles podem precisam de atenção específica. Gostaríamos de fornecer a Você mais detalhes sobre a coleta de dados em relação à prestação de nossos serviços. Nós prestamos vários serviços descritos no EULA e na documentação de produtos como o serviço de atualização, ESET LiveGrid®, proteção contra o uso errôneo de dados, suporte, etc. Para que tudo funcione, precisamos coletar as informações a seguir:

- O gerenciamento de produtos ESET Security requer e armazena localmente informações somo ID e nome da licença, nome do produto, informações de licença, informações de ativação e expiração, informações de hardware e software relacionadas ao computador gerenciado com o produto ESET Security instalado. Relatórios sobre atividades de produtos e dispositivos gerenciados pelo ESET Security são coletados e disponibilizados para facilitar os recursos e serviços de gerenciamento e supervisão sem serem enviados automaticamente para a ESET.
- Informações sobre o processo de instalação, inclusive sobre a plataforma na qual nosso produto é instalado, e informações sobre as operações e funcionalidades de nossos produtos, como impressão digital de hardware, IDs de instalação, despejos de memória, IDs de licença, endereços IP, endereços MAC, definições de configuração do produto que também podem incluir dispositivos gerenciados.
- Informações de licenciamento como ID da licença e dados pessoais como nome, sobrenome, endereço de email são necessários para fins de cobrança, verificação da legitimidade da licença e fornecimento de nossos serviços.
- Informações de contato e dados contidos em suas solicitações de suporte podem ser necessários para o serviço de suporte. Com base no canal escolhido por Você para entrar em contato conosco, podemos coletar seu endereço de e-mail, número de telefone, informações de licença, detalhes do produto e a descrição do seu caso de suporte. Podemos solicitar que você forneça outras informações para facilitar o serviço de suporte, como arquivos de relatório ou de despejo criados.
- Dados sobre o uso de nosso serviço estão completamente anônimos até o final da sessão. Nenhuma informação de identificação pessoal é armazenada depois do término da sessão.

Confidencialidade de dados

A ESET é uma empresa que opera no mundo todo através de entidades afiliadas ou parceiros como parte de nossa rede de distribuição, serviço e suporte. Informações processadas pela ESET podem ser transferidas de e para entidades afiliadas ou parceiros para o desempenho do Acordo de Licença para o usuário final, como o fornecimento de serviços ou suporte ou cobrança. Com base em sua localização e no serviço que Você escolhe usar, Nós podemos precisar transferir seus dados para um país que não tenha uma decisão de adequação pela Comissão Europeia. Mesmo nesse caso, toda transferência de informação está sujeita a uma regulação de legislação de proteção de dados e acontece apenas se for necessária. Cláusulas Contratuais Padrão, Regras Corporativas Vinculantes ou outra proteção adequada deve ser estabelecida sem exceção.

Estamos fazendo nosso melhor para impedir que os dados sejam armazenados por mais tempo do que o necessário enquanto fornecemos produtos e serviços sob o Acordo de Licença para o usuário final. Nosso período de retenção pode ser mais longo do que a validade de sua licença, apenas para dar a você um tempo para fazer a renovação de forma fácil e confortável. Estatísticas minimizadas e com pseudônimos e outros dados do ESET LiveGrid® podem ser processados ainda mais para fins estatísticos.

A ESET implementa medidas técnicas e organizacionais adequadas para garantir um nível de segurança que seja apropriado para os riscos potenciais. Estamos fazendo nosso melhor para garantir a confidencialidade, integridade, disponibilidade e resiliência constante de sistemas de processamento e serviços. Porém, em caso de violação de dados resultando em um risco aos seus direitos e liberdades, estamos prontos para notificar uma autoridade supervisora assim como os sujeitos dos dados. Como um sujeito de dados, Você tem o direito de enviar uma queixa à autoridade supervisora.

Direitos do sujeito dos dados

A ESET é sujeita ao regulamento das leis eslovacas e estamos vinculados pela legislação de proteção de dados como parte da União Europeia. Sujeito às condições estabelecidas pelas leis aplicáveis de proteção de dados, Você tem o direito ao seguinte como um titular dos dados:

- o direito de solicitar acesso aos seus dados pessoais da ESET,
- direito a uma retificação dos seus dados pessoais se estiverem incorretos (Você também tem o direito de completar dados pessoais incompletos),
- direito de solicitar que seus dados pessoais sejam apagados,
- direito de solicitar a restrição do processamento de seus dados pessoais
- direito a uma objeção ao processamento
- direito a fazer uma queixa assim como o
- direito à portabilidade de dados.

Se Você quiser exercer seus direitos como sujeito de dados ou se tiver uma pergunta ou dúvida, envie uma mensagem para:

ESET, spol. s r.o.
Data Protection Officer
Einsteinova 24
85101 Bratislava
Slovak Republic
dpo@eset.sk