ESET PROTECT

Guia de Administração

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

Introdução ao ESET PROTECT

Bem-vindo ao ESET PROTECT versão 10.0. O ESET PROTECT permite que você gerencie produtos ESET em estações de trabalho, servidores e dispositivos móveis em um ambiente em rede a partir de um local central. Usando o Console web ESET PROTECT é possível implementar soluções ESET, gerenciar tarefas, implementar políticas de segurança, monitorar o status do sistema e responder rapidamente a problemas ou detecções em computadores remotos.

Consulte o Glossário ESET para mais detalhes sobre as tecnologias ESET e os tipos de detecções/ataques contra os quais elas protegem.

ESET PROTECT componentes

- ESET PROTECT Servidor – você pode instalar o Servidor ESET PROTECT em servidores Windows e Linux ou implantá-lo como uma Máquina virtual pré-configurada. Ele lida com a comunicação com Agentes e coleta e armazena dados de aplicativo no banco de dados.

- Web Console ESET PROTECT – O Web Console ESET PROTECT é a interface primária que permite a você gerenciar computadores cliente no seu ambiente. Ele exibe uma visão geral do status de clientes em sua rede e permite que você use soluções da ESET em computadores não gerenciados remotamente. Depois de instalar o Servidor ESET PROTECT, é possível acessar o console da Web usando seu navegador da web. Se você escolher tornar o servidor da Web disponível pela internet, poderá usar o ESET PROTECT de qualquer lugar ou dispositivo com conexão à Internet. Você pode escolher instalar o Web Console ESET PROTECT em um computador diferente do computador executando o Servidor ESET PROTECT. Veja também Introdução ao Console Web ESET PROTECT.

- ESET ManagementAgente - O Agente ESET Management facilita a comunicação entre o Servidor ESET PROTECT e os computadores cliente. O Agente deve ser instalado em qualquer computador do cliente para estabelecer comunicação entre o computador e o Servidor ESET PROTECT. O uso do Agente ESET Management diminui de forma significativa o tempo de reação a novas detecções, pois ele está localizado no computador cliente e pode armazenar vários cenários de segurança. Usando o Console da Web ESET PROTECT é possível implementar o Agente ESET Management para computadores não gerenciados identificados através do seu Active Directory ou usando o ESET RD Sensor. Também é possível instalar manualmente o Agente ESET Management em computadores cliente.

- Rogue Detection Sensor – o ESET PROTECT Rogue Detection (RS) Sensor detecta computadores não gerenciados presentes na sua rede e envia as informações ao Servidor ESET PROTECT. É fácil adicionar novos computadores do cliente na sua rede segura. O Sensor RD lembrará dos computadores que já foram detectados e não enviará as mesmas informações duas vezes.

- 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.

- Conector de dispositivo móvel - 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.

Veja também a visão geral da arquitetura e dos elementos de infraestrutura do ESET PROTECT.

ESET PROTECT ferramentas autônomas

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

- ESET Remote Deployment Tool - esta ferramenta permite que você implante Pacotes Tudo-em-um criados pelo Console da Web ESET PROTECT. Você pode distribuir de forma conveniente o Agente ESET Management com um produto ESET nos computadores de uma rede.

Soluções adicionais da ESET

Para melhorar a proteção de dispositivos gerenciados em sua rede, você pode usar soluções adicionais da ESET:

- ESET Full Disk Encryption – o ESET Full Disk Encryption é um recurso complementar nativo do Web Console ESET PROTECT e fornece o gerenciamento da criptografia completa de disco de estações de trabalho gerenciadas do Windows e macOS com uma camada de segurança adicional no login pré-inicialização.

- O ESET LiveGuard Advanced – ESET LiveGuard Advanced (sandbox de nuvem) é um serviço pago oferecido pela ESET. Seu objetivo é adicionar uma camada de proteção especificamente projetada para mitigar ameaças novas.

- ESET Inspect - Um sistema abrangente de Detecção e Resposta Endpoint que inclui recursos como: detecção de incidentes, gerenciamento e resposta a incidentes, coleta de dados, indicadores de detecção de compromisso, detecção de anomalias, detecção de comportamento e violações de política.

O ESET Enterprise Inspector e o ESET Dynamic Threat Defense foram renomeados para ESET Inspect e ESET LiveGuard Advanced.
Você pode precisar resolver os problemas causados pela renomeação se você atualizou do ESET PROTECT 9.0 e versões anteriores e tem relatórios, grupos dinâmicos, notificações ou outros tipos de regras que filtram por ESET Dynamic Threat Defense ou ESET Enterprise Inspector.

Sincronizar licenças

Sincronizar licenças do ESET Business Account ou ESET MSP Administrator 2 com ESET PROTECT e usá-las para a ativação de produtos de segurança ESET nos dispositivos da sua rede.

- ESET Business Account – o portal de licenciamento para produtos comerciais ESET permite a você gerenciar licenças. Consulte a Ajuda on-line ESET Business Account para mais informações. Se você já tem um Usuário e Senha emitidos pela ESET que deseja converter para uma chave de licença, consulte a seção Converter credenciais de licença de legado.

- ESET MSP Administrator 2 – um sistema de gerenciamento de licenças para parceiros MSP ESET. Consulte a Ajuda on-line ESET MSP Administrator 2 para mais informações.

Sobre a ajuda

Este Guia de Administração foi criado para ajudá-lo a se familiarizar com o ESET PROTECT e fornece instruções de como usar o produto.

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.

Legenda de ícones

Esta é uma coleção de ícones usados no Console da Web ESET PROTECT e suas descrições. Alguns dos ícones descrevem ações, tipos de item ou status atual. A maioria dos ícones são exibidos em uma de três cores para indicar a acessibilidade de um elemento:

Ícone padrão - ação disponível

Ícone azul - elemento realçado quando você passa com o cursor do mouse

Ícone cinza - ação não disponível

Ícone de status	Descrições
	Detalhes sobre o dispositivo do cliente.
	Adicionar dispositivo – adicionar novos dispositivos. **Nova tarefa** - adiciona uma nova tarefa **Nova Notificação** - adiciona nova notificação. **Novo grupo Estático/Dinâmico** - adicionar novos grupos
	Editar - você pode editar as suas tarefas criadas, notificações, modelo de relatórios, grupos, políticas, etc.
	Duplicar - Permite criar uma nova política com base na política existente selecionada, um novo nome é necessário para a duplicada.
	Mover - Computadores, políticas, grupos estáticos ou dinâmicos. **Grupo de Acesso** - Mova o objeto para outro grupo estático onde ele está disponível para usuários com direitos suficientes para o grupo de destino. Alterar o Grupo de acesso é útil ao resolver problemas de acesso com outros usuários. O Grupo de acesso define o grupo estático do objeto e o acesso ao objeto com base nos direitos de acesso do usuário.
	Excluir - remove o cliente, grupo, etc. selecionado completamente.
	Renomear vários itens - se você selecionar vários itens, eles poderão ser renomeados um por um em uma lista ou você poderá usar a pesquisa Regex e substituir vários itens de uma vez.
	Escanear – usar dessa opção executará a tarefa Escaneamento sob demanda no cliente que relatou a detecção.
	Atualização > **Atualizar Módulos** - usar esta opção vai acionar a tarefa Atualizar Módulos (aciona uma atualização manualmente). **Atualizar** > **Atualizar produtos ESET –** atualize os produtos ESET instalados no dispositivo selecionado. **Atualizar** > **Atualizar sistema operacional** – atualize o sistema operacional no dispositivo selecionado.
	Relatório de auditoria - Exibe o Relatório de auditoria para o item selecionado.
	Executar a tarefa para dispositivos móveis.
	Inscrever novamente – Inscrever novamente em um dispositivo móvel.
	Desbloquear - O dispositivo será desbloqueado.
	Bloqueio - o dispositivo será bloqueado automaticamente quando uma atividade suspeita for detectada ou quando o dispositivo for marcado como perdido.
	Localizar - se você quiser solicitar as coordenadas de GPS de seu dispositivo móvel.
	Alarme/módulo perda - aciona um alarme sonoro remotamente, o alarme vai começar a tocar mesmo se o dispositivo estiver configurado como silencioso.
	Redefinição de fábrica - todos os dados armazenados no dispositivo serão apagados definitivamente.
	Energia – clique em um computador e selecione **Energia** > **Reiniciar** para reiniciar o dispositivo. Você pode configurar o comportamento de reinicialização/desligamento dos computadores gerenciados. O computador deve executar um Agente ESET Management 9.1 e um produto de segurança ESET compatível com esta configuração. **Restaurar** - restaurar arquivo colocado em quarentena para sua localização original.
	Desligar – clique em um computador e selecione **Energia** > **Desligar** para desligar o dispositivo. Você pode configurar o comportamento de reinicialização/desligamento dos computadores gerenciados. O computador deve executar um Agente ESET Management 9.1 e um produto de segurança ESET compatível com esta configuração. Desativar produto
	Sair **–** clique em um computador e selecione **Energia** > **Sair** para sair de todos os usuários do computador.
	Executar tarefa - selecione uma tarefa e configure o acionador e a alternância (opcional) para esta tarefa. A tarefa será colocada em fila de acordo com as configurações da tarefa. Essa opção acionará imediatamente uma tarefa existente, que você selecionará de uma lista de tarefas disponíveis.
	Tarefas recentes – exibe as tarefas recentes. Clique em uma tarefa para que ela seja executada novamente.
	Atribuir usuário - atribuir um usuário a um dispositivo. Você pode gerenciar usuários em Usuários do computador.
	Gerenciar políticas - uma Política também pode ser atribuída diretamente a um cliente (vários clientes), não apenas a um grupo. Selecione essa opção para atribuir a política a clientes selecionados.
	Enviar alerta – ESET PROTECT Servidor executa uma replicação instantânea do Agente ESET Management em uma máquina do cliente via EPNS. Isso é útil quando você não quer aguardar o intervalo regular quando o Agente ESET Management se conecta ao ESET PROTECT. Servidor. Por exemplo, quando quiser que uma Tarefa de cliente seja executada imediatamente em clientes ou se quiser que uma Política seja aplicada já.
	Implantar Agente – criar um ESET Management Instalador do Agente para implantar o Agente no dispositivo selecionado.
	Isolar da rede
	Parar com o isolamento da red **Conectar via RDP** - gere e faça download de um arquivo *.rdp* que vai deixar você conectar a um dispositivo de destino através do Remote Desktop Protocol.
	Sem áudio - Se você selecionar um computador e pressionar **Sem áudio**, o Agente desse cliente irá parar de se reportar ao ESET PROTECT e apenas agregará as informações. Um ícone sem áudio será exibido ao lado de um nome de computador na coluna Sem áudio. Assim que a opção sem áudio for desativada clicando em **Cancelar mudo**, o computador sem áudio começará a se reportar novamente e a comunicação entre o ESET PROTECT e o cliente será restaurada.
	Desativar - desativa ou remove a definição ou seleção.
	Atribuir - Para atribuir uma política a um cliente ou grupos.
	Importar – selecione os Relatórios/Políticas/Chave pública que deseja importar.
	Exportar – selecione os Relatórios/Políticas/Certificado de mesmo nível que deseja exportar.
	Marcações - Editar marcações (atribuir, remover atribuição, criar, remover).
	Grupo estático
	Grupo dinâmico
	Não aplicar sinalizador de política
	Aplicar sinalizador de política
	Forçar sinalizador de política
	Acionadores – veja a lista de Acionadores para a Tarefa do cliente selecionada.
	Área de trabalho
	Móvel
	Servidor
	Servidor de arquivo
	Servidor de email

Ícone de status	Descrições
	Servidor de gateway
	Servidor de colaboração
	Agente ESET Management
	Conector de dispositivo móvel
	Sensor Rogue Detection
	Servidor ESET PROTECT
	ESET InspectServidor
	Tipo de detecção de **antivírus**. Veja todos os tipos de detecção em Detecções. Clique em um computador e selecione **Soluções** > **Implantação de produto de segurança** para implantar um produto de segurança ESET no computador.
	Clique em um computador ou ícone de engrenagem ao lado de um grupo estático e selecione **Soluções** > **Ativar ESET LiveGuard** para ativar e habilitar o ESET LiveGuard Advanced.
	ESET Inspect Connector Clique em **Computadores** > clique em um computador ou selecione mais computadores e clique em **Computador** > **Soluções** > **Ativar o ESET Inspect** para implantar o Conector ESET Inspect nos computadores Windows/Linux/macOS gerenciados. Om ESET Inspect está disponível apenas quando você tem a licença ESET Inspect e o ESET Inspect conectado ao ESET PROTECT. Um usuário do Web Console precisa de permissão de **Leitura** ou acima para **Acessar o ESET Inspect** ou permissão de **Leitura** ou acima para o **Usuário ESET Inspect**.
	Clique em um computador e selecione **Soluções** > **Ativar criptografia** para ativar ESET Full Disk Encryption no computador.
	O computador tem o ESET Full Disk Encryption habilitado.

Ajuda off-line

A Ajuda off-line para o ESET PROTECT não está instalada por padrão. Se precisar de ajuda ESET PROTECT que você pode usar enquanto está off-line (caso você não tenha acesso à Internet às vezes, ou o tempo todo), execute os passos abaixo para adicionar a Ajuda off-line.

> 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 10.0 depois da atualização. Isso garante que você tenha a ajuda off-line mais recente compatível com a versão do seu ESET PROTECT.

Clique no código de linguagem para fazer download da Ajuda off-line para o ESET PROTECT no idioma desejado. Você até pode ter a Ajuda off-line instalada em vários idiomas.

Instruções de configuração da Ajuda off-line para Windows

1. Faça o download de um arquivo *.zip* clicando em código de idioma para fazer download da Ajuda off-line para o ESET PROTECT no seu idioma desejado.
2. Salve o arquivo *.zip* (por exemplo, em uma unidade USB).
3. Crie uma nova pasta chamada *help* no seu computador que executa o Web Console ESET PROTECT dentro do seguinte local: *%ProgramFiles%\Apache Software Foundation\[pasta Tomcat]\webapps\era\webconsole*
4. Copie o arquivo *.zip* para a pasta *help*.
5. Extraia o conteúdo do arquivo *.zip*, por exemplo *en-US.zip*, para uma pasta com o mesmo nome, neste caso **en-US**, para que a estrutura da pasta tenha a seguinte aparência: *%ProgramFiles%\Apache Software Foundation\[Tomcat folder]\webapps\era\webconsole\help\en-US*
Agora você pode abrir seu Console da Web ESET PROTECT, selecionar o idioma e fazer login. A Ajuda off-line do ESET PROTECT será aberta sempre que você clicar em **Ajuda** no canto superior direito e clicar em **Tópico atual – Ajuda**.

> Você pode adicionar a Ajuda off-line em vários idiomas, se necessário, seguindo os mesmos passos acima.

> Se seu computador ou um dispositivo móvel de onde você acessa o Console da Web ESET PROTECT não tiver uma conexão com a internet, você terá de alterar a configuração do Console da Web ESET PROTECT para **forçar a Ajuda off-line ESET PROTECT** a abrir por padrão (em vez da Ajuda on-line). Para fazer isso, siga as instruções abaixo da tabela.

Instruções de configuração da Ajuda off-line para Linux

1. Faça o download de um arquivo *.tar* clicando em código de idioma para fazer download da Ajuda off-line para o ESET PROTECT no idioma desejado.
2. Salve o arquivo *.tar* (por exemplo, em uma unidade USB).
3. Abra o terminal e navegue até */usr/share/tomcat/webapps/era/webconsole*
4. Crie uma nova pasta chamada *ajuda* executando o comando `mkdir help`.
5. Dentro da pasta *help*, crie uma nova pasta de idioma com o mesmo nome do arquivo *.tar*, por exemplo: execute o comando `mkdir en-US` para inglês.
6. Copie o arquivo *.tar* para a pasta de linguagem (por exemplo, */usr/share/tomcat/webapps/era/webconsole/help/en-US*) e extraia-o, por exemplo, executando o comando `tar -xvf en-US.tar`.

Agora você pode abrir seu Console da Web ESET PROTECT, selecionar o idioma e fazer login. A Ajuda off-line do ESET PROTECT será aberta sempre que você clicar em **Ajuda** no canto superior direito e clicar em **Tópico atual** – **Ajuda**.

Para atualizar a Ajuda off-line depois de migrar de uma versão anterior (por exemplo, do ESMC) remova a pasta de ajuda existente (*...webapps\era\webconsole\help*) e crie uma nova no mesmo lugar durante a etapa 3 do procedimento exibido acima. Continue normalmente depois de substituir a pasta.

Você pode adicionar a Ajuda off-line em vários idiomas, se necessário, seguindo os mesmos passos acima.

Se seu computador ou um dispositivo móvel de onde você acessa o Console da Web ESET PROTECT não tiver uma conexão com a internet, você terá de alterar a configuração do Console da Web ESET PROTECT para **forçar a Ajuda off-line ESET PROTECT** a abrir por padrão (em vez da Ajuda on-line). Para fazer isso, siga as instruções abaixo da tabela.

Idiomas compatíveis	Ajuda off-line HTML .zip	Ajuda off-line HTML .tar
English	en-US.zip	en-US.tar
Árabe	ar-EG.zip	ar-EG.tar
Chinês simplificado	zh-CN.zip	zh-CN.tar
Chinês tradicional	zh-TW.zip	zh-TW.tar
Croata	hr-HR.zip	hr-HR.tar
Tcheco	cs-CZ.zip	cs-CZ.tar
Francês	fr-FR.zip	fr-FR.tar
Francês canadense	fr-CA.zip	fr-CA.tar
Alemão	de-DE.zip	de-DE.tar
Grego	el-GR.zip	el-GR.tar
Italiano	it-IT.zip	it-IT.tar
Japonês	ja-JP.zip	ja-JP.tar
Coreano	ko-KR.zip	ko-KR.tar
Polonês	pl-PL.zip	pl-PL.tar
Português do Brasil	pt-BR.zip	pt-BR.tar
Russo	ru-RU.zip	ru-RU.tar
Espanhol	es-ES.zip	es-ES.tar
Espanhol latino	es-CL.zip	es-CL.tar
Eslovaco	sk-SK.zip	sk-SK.tar
Turco	tr-TR.zip	tr-TR.tar
Ucraniano	uk-UA.zip	uk-UA.tar

Forçar Ajuda off-line no Windows

1. **Abra** `C:\Program Files\Apache Software Foundation\[ Tomcat folder ]\webapps\era\WEB-INF\classes\sk\eset\era\g2webconsole\server\modules\config\EraWebServerConfig.properties` em um editor de texto.
2. **Localize** a linha `help_show_online=true`, altere o valor desta configuração para `false` e salve as alterações.
3. **Reinicie** o serviço Tomcat nos serviços ou através da linha de comando.

A Ajuda off-line do ESET PROTECT será aberta sempre que você clicar em **Ajuda** no canto superior direito e clicar em **Tópico atual – Ajuda**. A respectiva janela de ajuda da página atual será exibida.

Forçar Ajuda off-line no Linux

1. **Abra o arquivo de configuração** `/usr/share/tomcat/webapps/era/WEB-INF/classes/sk/eset/era/g2webconsole/server/modules/config/EraWebServerConfig.properties` em um editor de texto (por exemplo, `nano`).
2. **Localize** a linha `help_show_online=true`, altere o valor desta configuração para `false` e salve as alterações.
3. Pare o serviço `tomcat`, execute o comando `tomcat stop`.
4. Inicie o serviço `tomcat`, execute o comando `tomcat start`.

A Ajuda off-line do ESET PROTECT será aberta sempre que você clicar em **Ajuda** no canto superior direito e clicar em **Tópico atual – Ajuda**. A respectiva janela de ajuda da página atual será exibida.

Novos recursos no ESET PROTECT

Suporte VDI aprimorado

Ao configurar um ambiente VDI, agora você pode lidar com as identidades dos computadores (criando identidades novas e renovando as existentes) não só por meio da impressão digital de hardware do computador, mas também através do FQDN de um computador. Saiba mais

Tema escuro

Agora você pode experimentar o novo tema escuro que adicionamos ao ESET PROTECT. Os usuários do console agora podem ativá-lo nas configurações de Usuário. Saiba mais

Formato CEF para Syslog

Agora você pode enviar relatórios para o Syslog no Formato de evento comum. Saiba mais

Outros aprimoramentos e alterações de uso

Você pode encontrar mais detalhes no registro de alterações.

Registro de alterações

Veja também:

- A lista de todas as versões de componentes do ESET PROTECT
- ESET PROTECT problemas conhecidos
- política de Fim da vida útil ESET para produtos empresariais.

Ferramentas autônomas

Mirror Tool

Build version 1.0.1421.0 (Windows), 1.0.2346.0 (Linux)
Released: November 8, 2022

Build version 1.0.1383 (Windows), 1.0.2310 (Linux)
Released: April 28, 2022

- FIXED: MirrorTool downloads ESET Endpoint 6 modules from the ESET Endpoint 6.6 folder, allowing updates of newer ESET Endpoint 6 versions and using DLL modules
- FIXED: MirrorTool fails with "--mirrorFileFormat dll" on ESET Endpoint 6
- FIXED: Mirror chain linking fails with: Error: GetFile: Host 'update.eset.com' not found [error code: 20002]
- FIXED: MirrorTool v1.0.2226.0 ignores proxy setting for downloading product list

ESET Bridge (replaces Apache HTTP Proxy in ESET PROTECT 10 and later)

Consulte a Ajuda on-line ESET Bridge.

Apache HTTP Proxy (applies to ESET PROTECT 9.1 and earlier)

Build version: 2.4.56.64
Released: March 30, 2023

- FIXED: Apache HTTP Proxy (v 2.4.55.58) replaced with the latest version (v 2.4.56.64) due to discovered vulnerabilities in the earlier version. This release fixes vulnerability CVE-2023-25690

Build version: 2.4.55.58
Released: March 2, 2023

- FIXED: Apache HTTP Proxy (v 2.4.54.25) was replaced with the latest version (v 2.4.55.58) due to discovered vulnerabilities in the earlier version. This release updates OpenSSL from version 1.1.1q to version 1.1.1t to fix security vulnerabilities

Build version: 2.4.54.25
Released: September 26, 2022

- FIXED: Apache HTTP Proxy (v 2.4.54.0) replaced with the latest version (v 2.4.54.25) due to discovered vulnerabilities in the earlier version

Build version: 2.4.54.0
Released: August 3, 2022

- FIXED: Apache HTTP Proxy (v 2.4.53.1) replaced with the latest version (v 2.4.54.0) due to discovered vulnerabilities in the earlier version

Build version: 2.4.53.1
Released: July 7, 2022

- FIXED: Apache HTTP Proxy replaced with the latest version due to discovered vulnerabilities in the earlier version

Build version: 2.4.53.0
Released: March 31, 2022

- FIXED: Apache HTTP Proxy replaced with the latest version due to discovered vulnerabilities in the earlier version

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 10.0

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
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
ESET Server Security para Linux (anteriormente ESET File Security para Linux)	7.2, 8.x, 9.x
ESET Endpoint Antivirus para Linux	7.1, 8.x, 9.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 10.0

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 PROTECT10.0.
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

Idioma	Código
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.

Introdução ao ESET PROTECT

O ESET PROTECT pode ser configurado e gerenciado pelo console web ESET PROTECT. Depois de ter instalado o ESET PROTECT com sucesso ou implantado o ESET PROTECT VA, você pode conectar ao seu Servidor ESET PROTECT usando o Console da Web ESET PROTECT.

Depois de ter instalado com êxito o ESET PROTECT, você poderá começar a definir suas configurações.

Primeiras etapas após a implantação do Servidor ESET PROTECT

1. Abra o Console web ESET PROTECT em seu navegador da web e entre nele.

2. Adicione sua(s) licença(s) ao ESET PROTECT.

3. Adicione computadores clientes, servidores e dispositivos móveis à sua rede na estrutura ESET PROTECT.

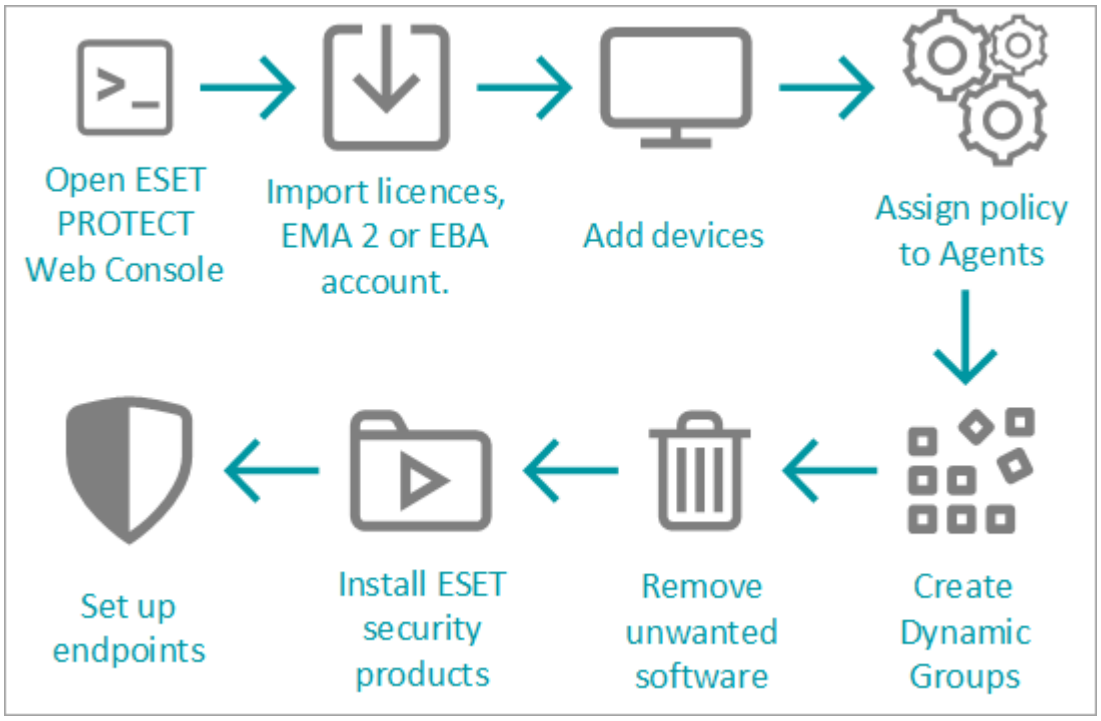
4. Atribuir a política interna de **Relatório de aplicativos – Relatar todos os aplicativos instalados** a todos os computadores.

5. Criar um grupo dinâmico para computadores com produtos domésticos da ESET.

6.Remova aplicativos antivírus de terceiros usando a tarefa Desinstalação de software.

7.Instale os produtos de segurança ESET usando a tarefa Instalação de software (a menos que você tenha instalado o Agente usando o Instalador tudo-em-um).

8.Atribua uma política com as configurações recomendadas a cada máquina com produtos de segurança ESET instalados. Por exemplo, para máquinas Windows com o ESET Endpoint, atribua a política interna **Antivírus – Segurança máxima – Recomendado**. Consulte também Como gerenciar produtos Endpoint do ESET PROTECT.



Etapas adicionais recomendadas

• Conheça o console web ESET PROTECT, já que ele é a interface que você usará para gerenciar os produtos de segurança ESET.

• Durante a instalação você cria uma conta de Administrador padrão. Recomendamos que você salve as credenciais da conta do Administrador em um local seguro e crie uma nova conta para gerenciar clientes e configurar suas permissões.

Não recomendamos usar a conta de **Administrador** ESET PROTECT padrão como uma conta de usuário normal. Ele serve como um backup caso algo aconteça com contas de usuários normais ou se você ficar trancado para fora. Você pode fazer login com a conta de Administrador para corrigir tais problemas.

• Use as notificações e relatórios para monitorar o status dos computadores clientes em seu ambiente. Por exemplo, se quiser ser notificado de que um determinado evento ocorreu ou quer ver ou fazer download de um relatório.

• Faça backup do seu banco de dados regularmente para evitar a perda de dados.

• Recomendamos que você exporte a Autoridade de certificação do servidor e os Certificados de mesmo nível. Caso seja preciso reinstalar o Servidor ESET PROTECT, você poderá usar o CA e os Certificados de mesmo nível do Servidor ESET PROTECT original e não precisará reinstalar os Agentes ESET Management nos computadores clientes.

Abrir o console da Web ESET PROTECT

O console da Web ESET PROTECT é a principal interface que se conecta ao Servidor ESET PROTECT. Você pode pensar nele como um painel de controle, um local central do qual é possível gerenciar suas soluções de segurança ESET. Ela é uma interface na web que pode ser acessada usando um navegador de qualquer local e qualquer dispositivo com acesso à Internet. Você pode escolher instalar o Web Console ESET PROTECT em um computador diferente do computador executando o Servidor ESET PROTECT.

Há várias maneiras de abrir o console da Web ESET PROTECT:

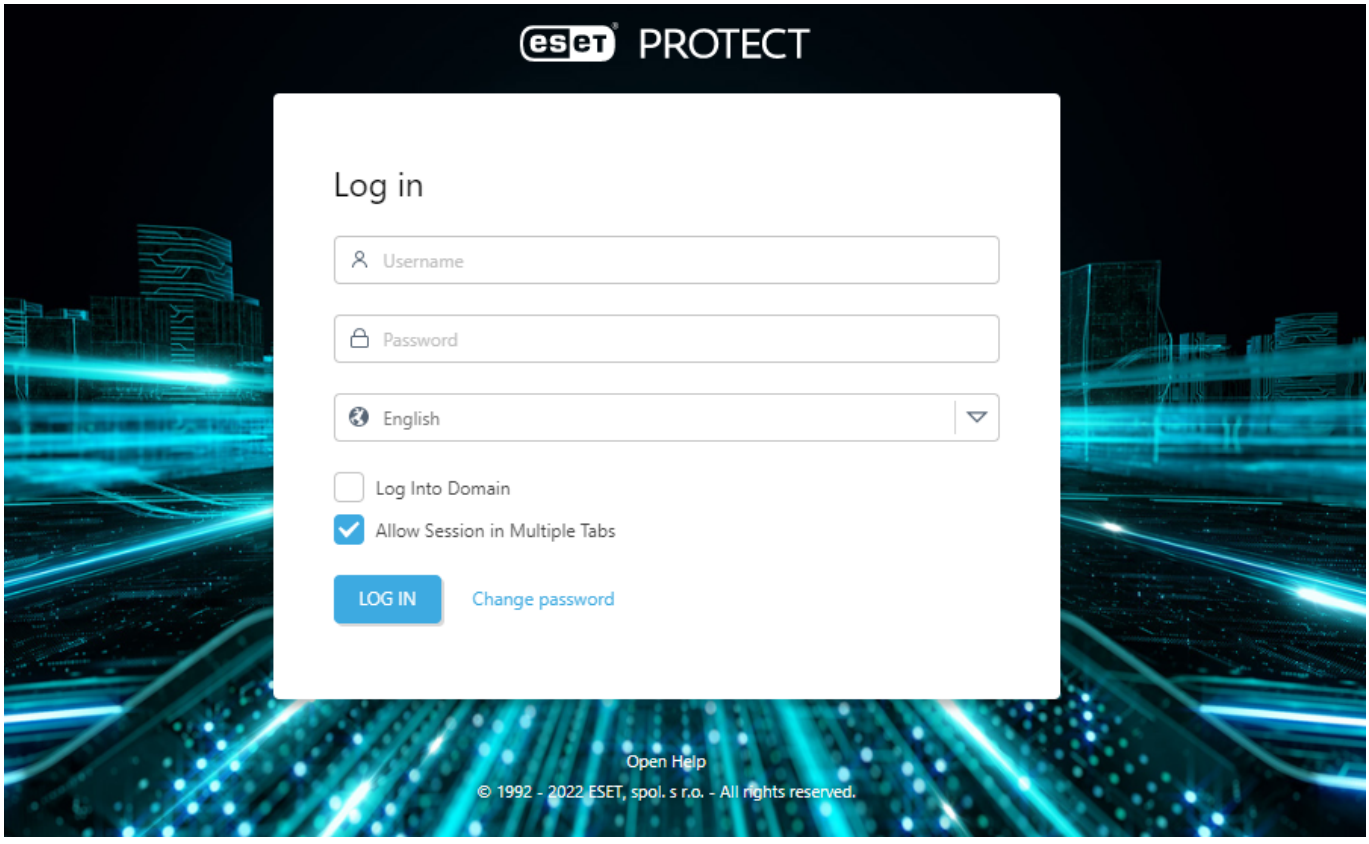
- Em seu **servidor local** (a máquina hospedando seu Console da Web), digite este URL no navegador da Web:
https://localhost/era/

- De **qualquer local com acesso à internet** para seu servidor Web, digite a URL no seguinte formato:
https://yourservername/era/
Substitua "nomedoseuservidor" pelo nome real ou endereço IP de seu servidor Web.

■Para fazer login no **equipamento virtual ESET PROTECT**, use o seguinte URL:
https://[endereço IP]/
Substitua "[endereço IP]" pelo endereço IP de sua ESET PROTECT VM.

■Em seu servidor local (a máquina hospedando seu console da Web), clique em **Iniciar** > **Todos os Programas** > **ESET** > **ESET PROTECT** > **ESET PROTECTConsole da web** - uma tela de login será aberta em seu navegador da Web padrão. Isso não se aplica ao equipamento virtual ESET PROTECT.

Quando o servidor Web (que executa o Console da Web ESET PROTECT) estiver ativo, a seguinte tela de login será exibida.



Se esse for seu primeiro login, forneça as credenciais que inseriu durante o processo de instalação. O usuário padrão do Web Console é o **Administrador**. Para obter mais detalhes sobre essa tela, consulte Tela de login do console da Web.

> Se você tiver problemas para fazer login e receber mensagens de erro ao tentar fazer login, veja Solução de Problemas do Console da Web.

Console da Web ESET PROTECT

O console da Web ESET PROTECT é a principal interface que se conecta ao ESET PROTECT. Servidor. Você pode pensar nele como um painel de controle, um local central de onde é possível gerenciar todas as suas soluções de segurança ESET. Ela é baseada na web que pode ser acessada usando um navegador (consulte Navegadores da Web compatíveis) de qualquer local e dispositivo com acesso à Internet. Quando você entrar no Web Console pela primeira vez, o Tour ESET PROTECT aparecerá.

No layout padrão do console da Web ESET PROTECT:

- O usuário atual é sempre mostrado no canto direito superior, onde aparece a contagem regressiva do limite de tempo de sua sessão. Você pode clicar em **Sair** para sair a qualquer momento. Você deve entrar novamente quando a sessão atingir seu limite de tempo (devido a uma inatividade). Para alterar as Configurações de usuário, clique em seu nome de usuário no canto superior direito do Web Console ESET PROTECT.

- O Menu principalestá sempre acessível à esquerda, exceto ao usar um Assistente. Clique em para abrir o menu no lado esquerdo da tela, ele pode ser fechado clicando em **Fechar**.

- Se você precisar de ajuda ao trabalhar com o ESET PROTECT, clique no ícone **Ajuda** na parte superior na direita e clique em **Tópico atual – Ajuda**. A janela de ajuda da página atual será exibida. Clique em **Ajuda** > Sobre para ver a versão do ESET PROTECT e outros detalhes.

- Na parte superior do Console da Web ESET PROTECT você pode usar a ferramenta **Pesquisa rápida**. Clique no ícone para selecionar um destino de pesquisa:

  - **Nome do computador**, **Descrição** e **Endereço IP** – Digite um **Nome do computador**, **Descrição do computador**, **Endereço IPv4/IPv6** ou **Nome do grupo** e pressione **Enter**. Você será redirecionado para a seção Computadores onde os resultados serão exibidos.

  - **Nome da detecção** – Você será redirecionado para a seção Detecções, onde os resultados serão exibidos.

  - **Nome de usuário** - Você pode procurar usuários AD importados, os resultados serão exibidos na seção Usuários do computador.

- Clique no botão **Links rápidos** para ver o menu:

Links rápidos
Configurar computadores
• Adicionar computador
• Adicionar dispositivo móvel

Links rápidos
• Implantar Agente
• Adicionar usuário de computador
Gerenciar Computadores
• Criar tarefa de cliente
• Criar nova política
• Atribuir política
Status de revisão
• Gerar relatório
• Componentes do servidor

• Na parte superior esquerda da tela, ao lado do nome do ESET PROTECT, você pode encontrar o ícone de navegação do produto  que ajudará você a navegar entre o ESET PROTECT e seus produtos: ESET Inspect, ESET Business Account e ESET MSP Administrator.

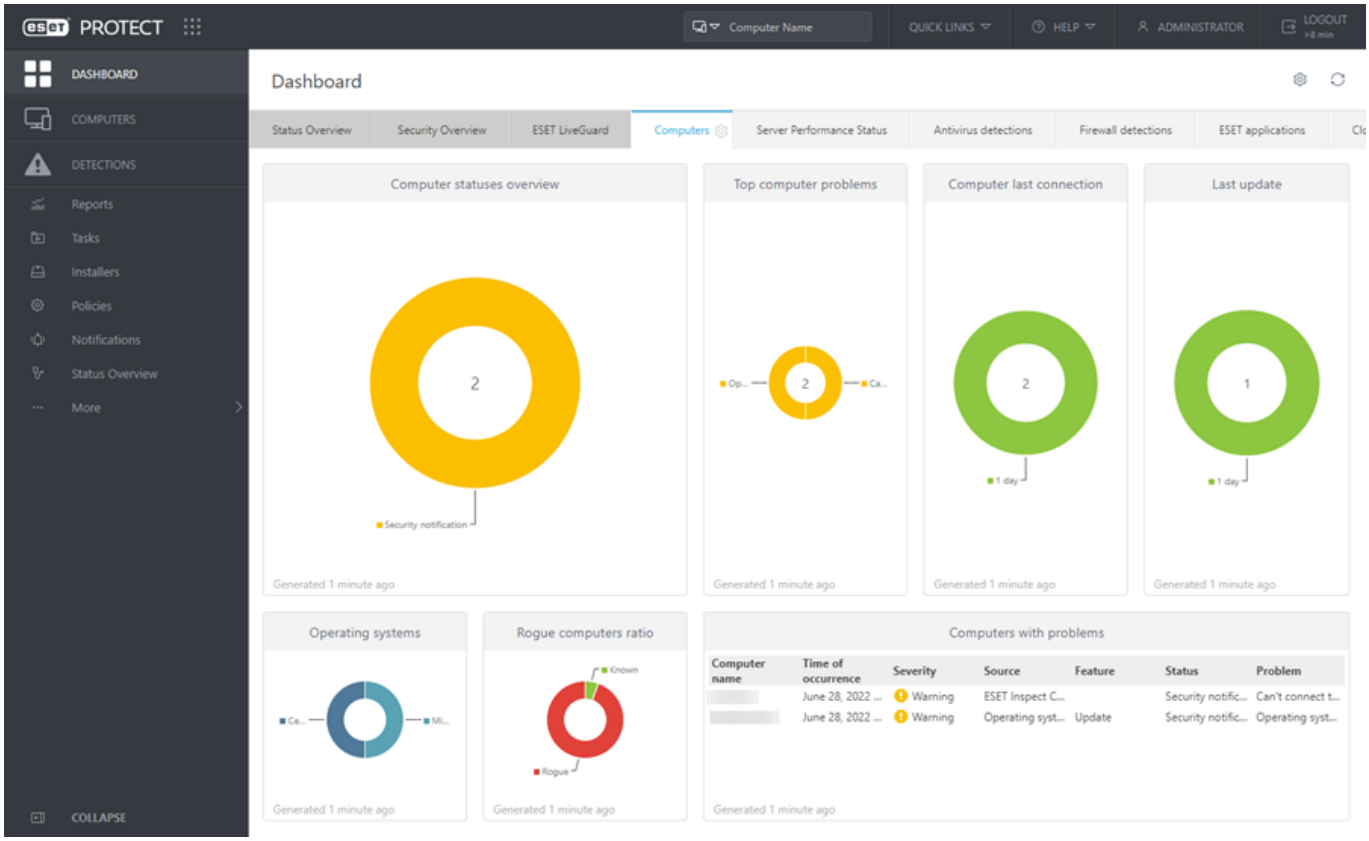
• O ícone de **Engrenagem** sempre denota um menu de contexto.

• Clique em **Atualizar** para recarregar/atualizar as informações exibidas.

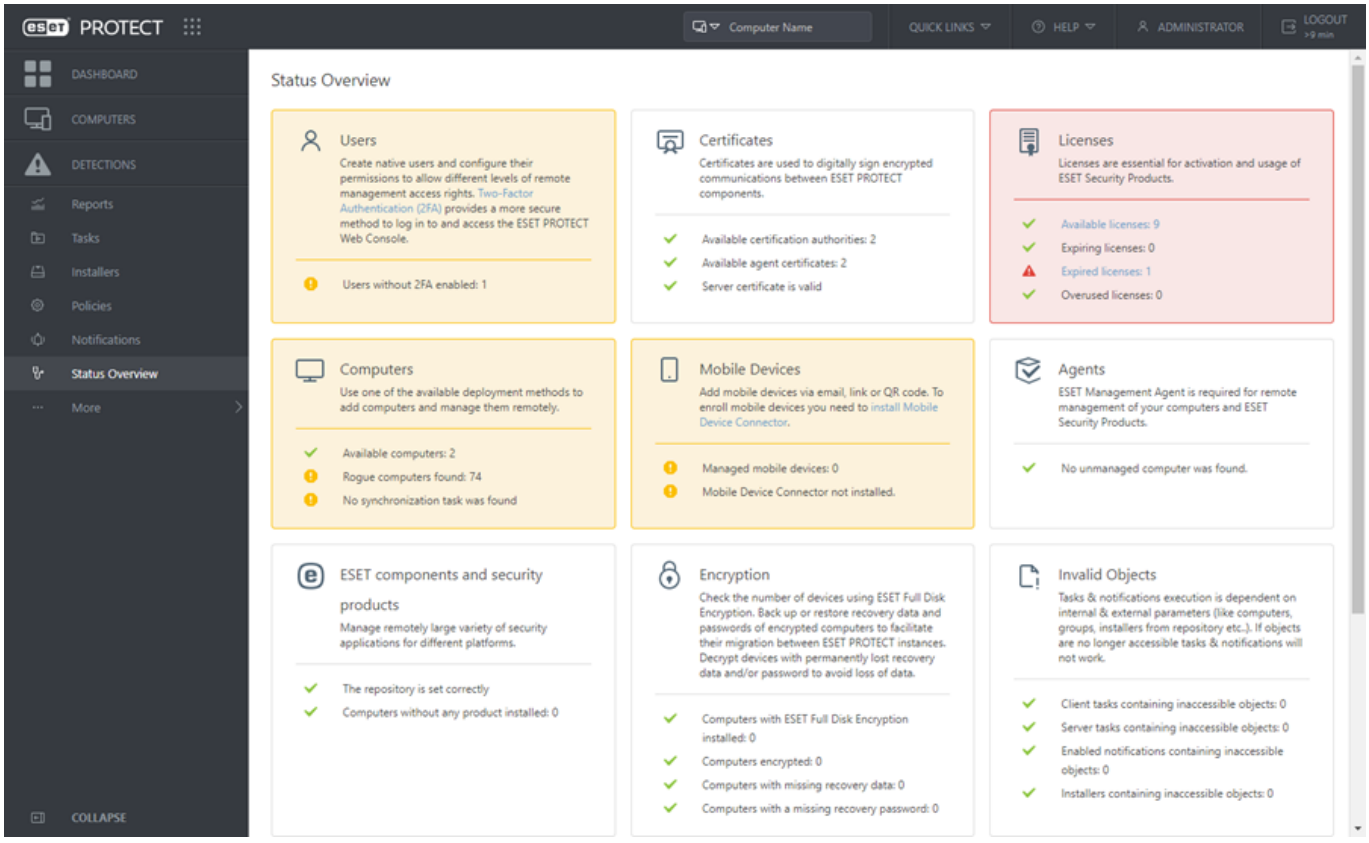
• Os botões na parte inferior da página são exclusivos para cada seção e função, e são descritos em detalhes em seus respectivos capítulos.

• O Web Console ESET PROTECT notifica o administrador sobre os Acordos de licença de usuário final atualizados dos produtos de segurança ESET gerenciados.

• Clique no logo ESET PROTECT para abrir a tela de Painel.



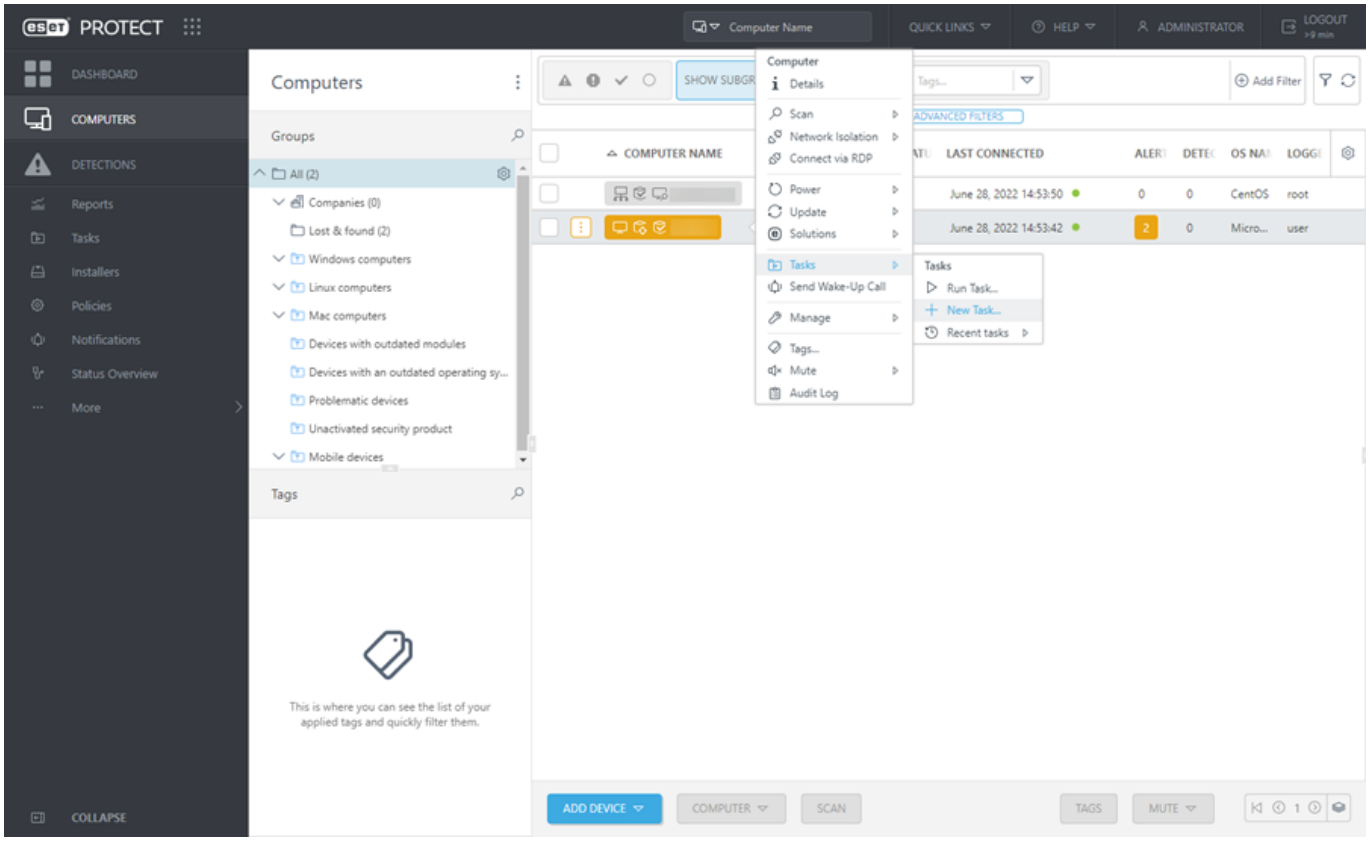
[Visão geral do status](#) mostra como obter o máximo do ESET PROTECT. Isso vai orientá-lo pelas etapas recomendadas.



As telas com árvores têm controles específicos. A árvore em si fica à esquerda com ações abaixo. Clique em um item na árvore para exibir as opções.

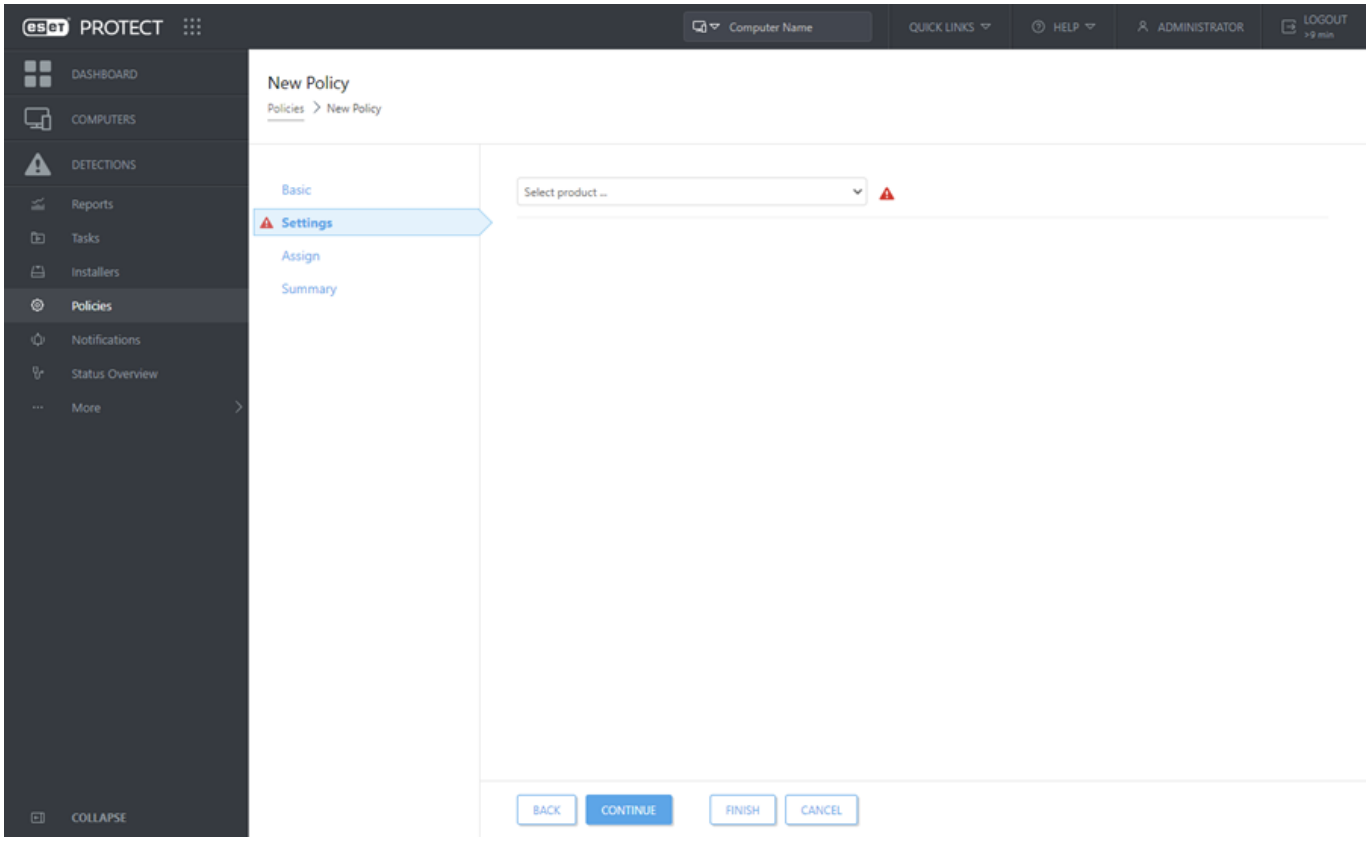
As tabelas permitem que você gerencie unidades a partir de linhas individualmente ou em um grupo (quando

mais linhas são selecionadas). Clique em uma linha para exibir opções para unidades nessa linha. Os dados nas tabelas podem ser filtrados e classificados.



Você pode editar objetos no ESET PROTECT usando assistentes. Todos os Assistentes compartilham os comportamentos a seguir:

- As etapas são orientadas verticalmente do início para o fim.
- Você pode retornar a qualquer etapa, a qualquer momento.
- As configurações obrigatórias (exigidas) são sempre marcadas com um ponto de exclamação vermelho ao lado da seção e das respectivas configurações.
- Dados de entrada inválidos são marcados quando você move o cursor para um novo campo. A etapa do Assistente contendo dados de entrada inválidos também é marcada.
- A opção **Concluir** não está disponível até que todos os dados de entrada estejam corretos.



Tela de login

Um usuário precisa de credenciais de login (nome de usuário e senha) para efetuar login no Web Console.

Para entrar como um usuário do domínio (um membro do grupo de segurança do domínio mapeado), selecione a caixa de seleção ao lado de **Entrar no domínio**. O formato de login depende do seu tipo de domínio:

- Windows Active Directory: `DOMAIN\username`
- Linux e máquina virtual ESET PROTECT LDAP: `username@FULL.DOMAIN.NAME`

> Se você tiver problemas para fazer login e receber mensagens de erro ao tentar fazer login, veja Solução de Problemas do Console da Web para sugestões de como resolver seu problema.

Você pode **selecionar seu idioma** clicando na seta suspensa ao lado do idioma selecionado no momento, para mais detalhes veja nosso artigo da Base de Conhecimento.

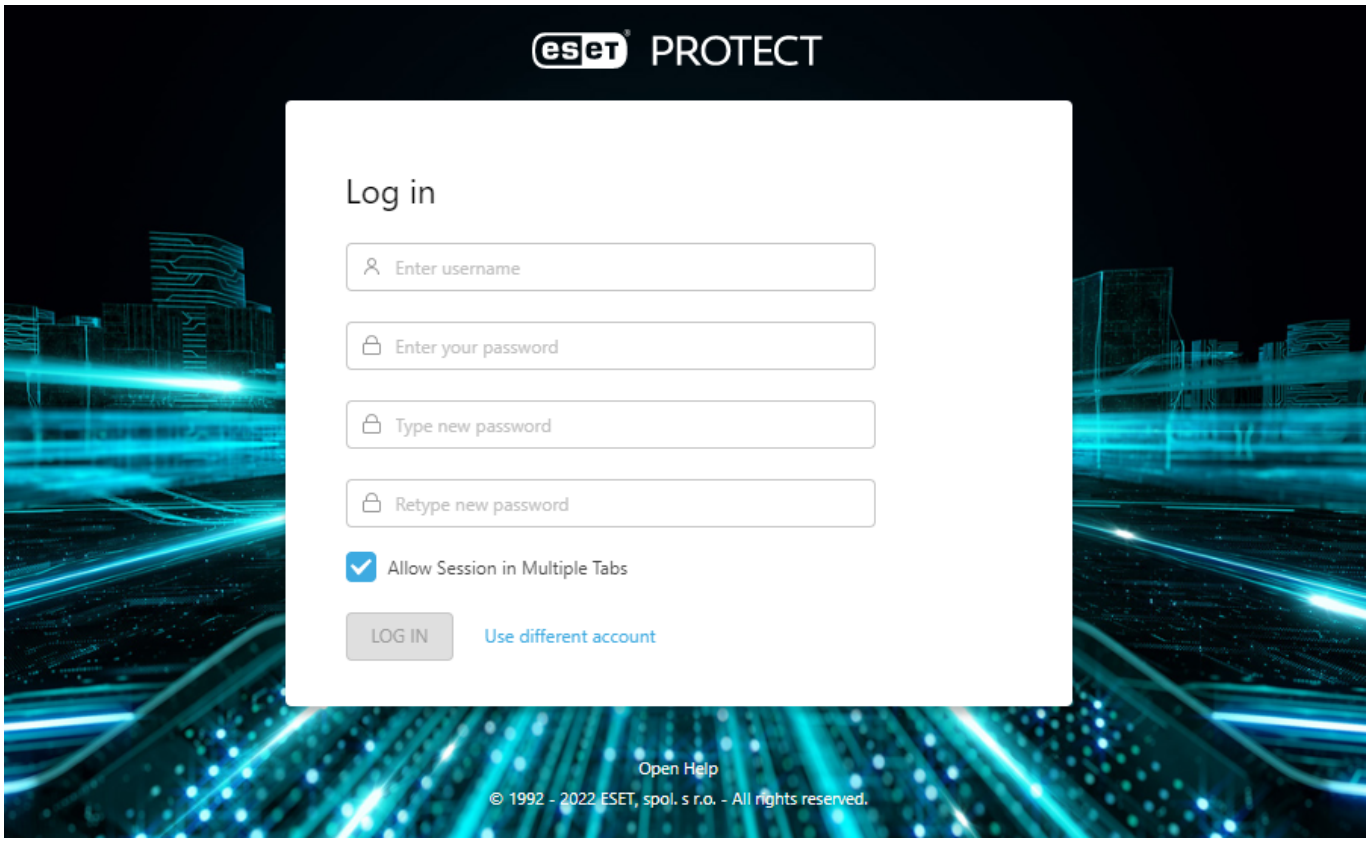
> Nem todos os elementos do Web Console serão alterados depois da alteração do idioma. Alguns dos elementos (painéis, políticas, tarefas, etc.) padrão são criados durante a instalação do ESET PROTECT e seu idioma não pode ser alterado.

Permitir sessão em várias guias- O console da Web pode ser aberto em várias guias de um único navegador.

- Se a caixa de marcação estiver selecionada cada guia com uma sessão do console da Web aberta em um navegador será conectada na mesma sessão. Se uma nova guia for aberta, todas as outras guias conectadas na mesma configuração vão se conectar a essa nova sessão. Se você sair da sessão em uma das guias, vai sair da sessão em todas as outras guias também.

• Se a caixa de marcação não estiver selecionada, cada nova guia vai abrir uma sessão independente do console da Web ESET PROTECT.

Alterar senha/Usar outra conta - permite que você altere a senha ou volte para a tela de login.



Gerenciamento de sessão e medidas de segurança:

Bloqueio de login do endereço IP

Depois de 10 tentativas mal sucedidas de entrar do mesmo endereço IP (por exemplo, usando credenciais de login incorretas), outras tentativas de entrar feitas por esse endereço IP serão bloqueadas temporariamente. Isso é indicado pela mensagem de erro: **Falha no login: O usuário estava bloqueado. Tente novamente mais tarde.** Depois de 10 minutos, entre usando as credenciais corretas. O bloqueio de endereço IP em tentativas de login não afeta sessões existentes.

Bloqueio de endereço de ID de sessão errado

Depois de usar um ID de sessão inválido 15 vezes do mesmo endereço IP, todas as outras tentativas de conexão desse endereço IP serão bloqueadas por cerca de 15 minutos. IDs de sessões expiradas não são contados. Se houver um ID de sessão expirada no navegador, ele não é considerado um ataque. O bloqueio de IP de 15 minutos é para todas as ações (inclusive solicitações válidas). O bloqueio pode ser liberado ao reiniciar o console web (serviço `tomcat`).

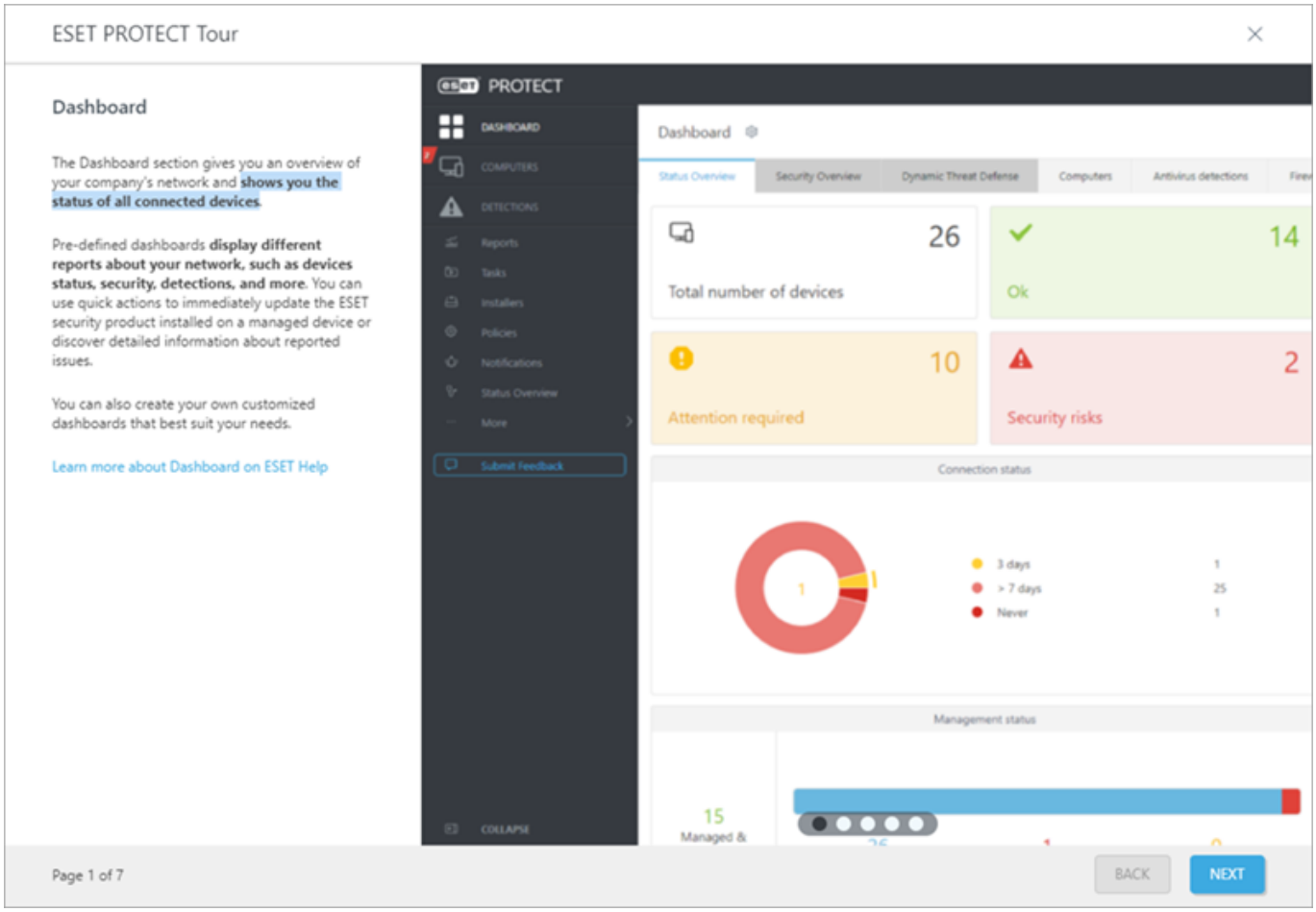
ESET PROTECT Tour

Quando você entrar no Web Console pela primeira vez, o **Tour ESET PROTECT** aparecerá.

Este assistente dará uma explicação básica das seções importantes do console web ESET PROTECT, Agente ESET

Management e produtos de segurança ESET. Você vai ler sobre Painéis, Computadores, Detecções, Tarefas, Políticas, Notificações e atualizações de produto automáticas.

Clique em **Proteger dispositivos** na última etapa do **ESET PROTECT Tour** para implantar Agentes ESET Management nos seus computadores de rede. Você também pode criar o instalador do Agente sem usar o assistente clicando em **Instaladores** > Criar instalador.



Clique em **X** se você não quiser usar o **ESET PROTECT Tour**. O console web ESET PROTECT será aberto. O **ESET PROTECT Tour** não vai aparecer na próxima vez que você entrar no Web Console ESET PROTECT.

Você pode ver o **ESET PROTECT Tour** novamente clicando em **Ajuda** > **ESET PROTECT Tour**.

Depois do primeiro login no console web ESET PROTECT, recomendamos que você execute a tarefa de cliente Atualizações do sistema operacional no computador onde o ESET PROTECT está instalado para garantir que o sistema operacional está atualizado (por motivos de segurança e desempenho).

Configurações do usuário

Nesta seção, você pode personalizar suas configurações do usuário. Clique em **Conta do usuário** no canto superior direito do Console Web ESET PROTECT (na esquerda do botão **Fazer logout**) para exibir todos os usuários ativos. Você pode estar conectado no Console da Web ESET PROTECT de navegadores da web, computadores ou dispositivos móveis diferentes ao mesmo tempo. Você verá todas as suas sessões aqui.

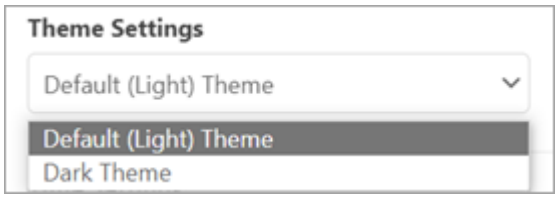
A configuração de usuário aplica-se apenas ao usuário que está conectado no momento.

Configurações de tema

Você pode selecionar a configuração de tema para exibição do ESET PROTECT:

- **Tema padrão (claro)**
- **Tema escuro**

Selecione o tema no menu suspenso:



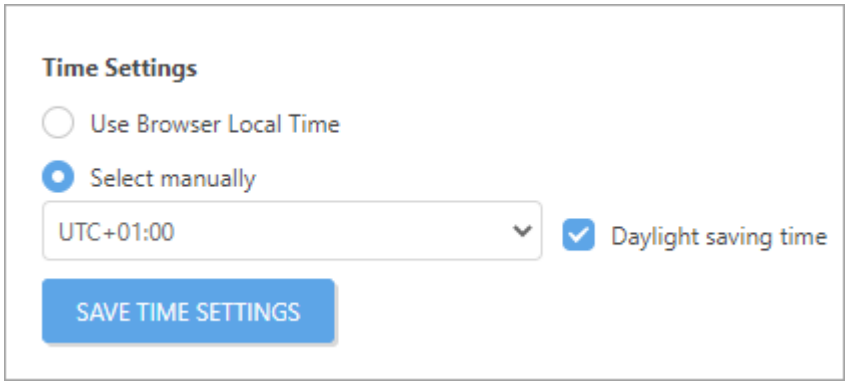
A exibição permanece na versão selecionada depois de sair do Web Console e entrar outra vez.

Configurações de hora

Cada usuário pode ter suas próprias configurações de tempo preferidas para o console da Web ESET PROTECT. Definições de tempo específicas do usuário são aplicadas a cada usuário, independentemente de onde eles acessam o console da Web ESET PROTECT.

Todas as informações são armazenadas internamente no ESET PROTECT usando o padrão UTC (Tempo Universal Coordenado). A hora UTC é automaticamente convertida para o fuso horário usado pelo console da Web ESET PROTECT (levando em conta o horário de verão). O console da Web ESET PROTECT exibe a hora local do sistema onde o console da Web ESET PROTECT está sendo executado (não o horário UTC interno). Você pode substituir essa configuração para definir o tempo mostrado no console da Web ESET PROTECT manualmente.

Se quiser substituir a configuração padrão **Usar horário local do navegador**, você pode escolher a opção **Selecionar manualmente**, em seguida especifique manualmente o fuso horário do console e decida se quer usar o horário de verão ou não.

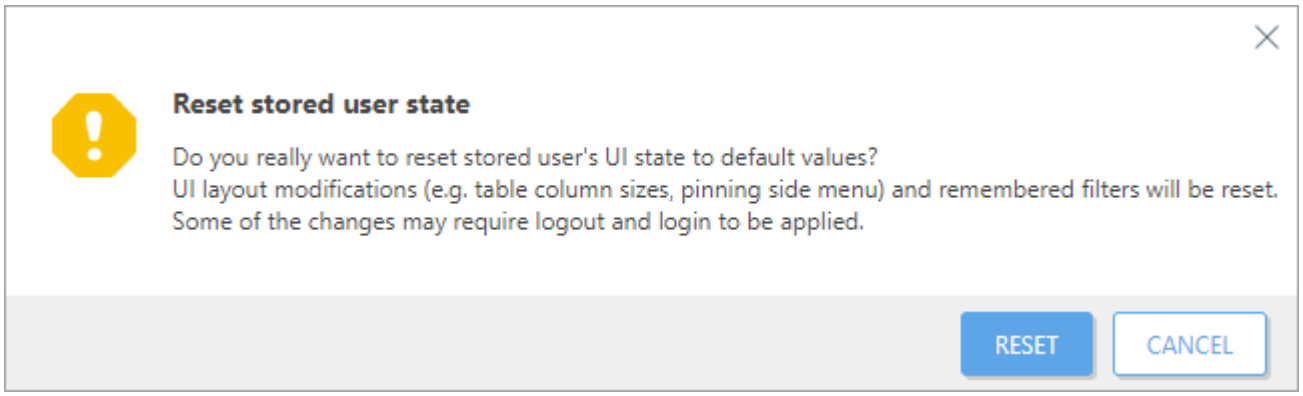


Em alguns casos, a opção de usar um fuso horário diferente será disponibilizada. Ao configurar um acionador, o fuso horário do Web Console ESET PROTECT é usado por padrão. Alternativamente, você pode selecionar a caixa de seleção **Usar horário local do destino** para usar o fuso horário local do dispositivo de destino em vez do fuso horário do Console ESET PROTECT para o acionador.

Clique em **Salvar configurações de tempo** para confirmar as alterações.

Estado do usuário armazenado

Você pode redefinir o estado da interface do usuário armazenada do usuário para o padrão clicando em **Redefinir estado do usuário armazenado**. Isso inclui o ESET PROTECT Tour, tamanhos das colunas da tabela, filtros lembradas, menu lateral fixado, etc.



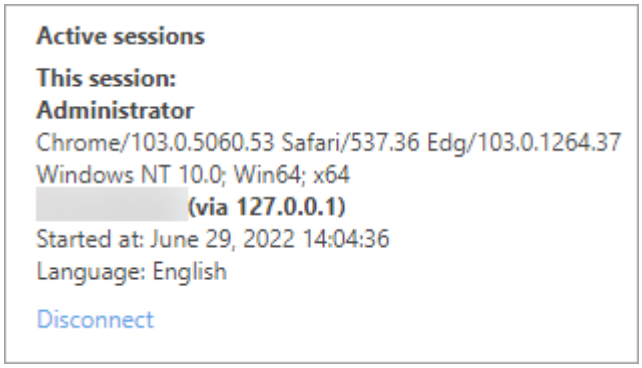
Dispositivos lembrados

Esquecer os dispositivos lembrados – requer a Autenticação em dois fatores em dispositivos lembrados para o usuário atual.

Sessões ativas

Informações sobre todas as sessões ativas do usuário atual contém:

- Nome de usuário atual.
- Detalhes do computador acessando o Web Console – navegador da web e sistema operacional.
- Endereço IP de um computador cliente ou um dispositivo do qual um usuário está conectado ao Web Console ESET PROTECT. O endereço IP de um servidor da web que executa o Web Console ESET PROTECT é exibido entre parênteses. Caso o Console da Web ESET PROTECT esteja sendo executado na mesma máquina que o Servidor ESET PROTECT, **via 127.0.0.1** é exibido.
- Data e hora em que um usuário fez login.
- Idioma selecionado para o Console da Web ESET PROTECT.



A sessão atual é chamada de **Esta sessão**. Se você quiser desconectar uma sessão ativa, clique em **Desconectar**.

Filtros e personalização de layout

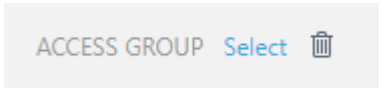
O console web ESET PROTECT permite a você personalizar o layout dos itens exibidos nas seções principais (por exemplo, **Computadores**, **Tarefas** etc.) de várias formas:

Adicionar filtro e predefinições de filtro

Para adicionar critérios de filtragem, clique em **Adicionar filtro** e selecione um item da lista. Digite as strings de pesquisa ou selecione os itens no menu suspenso no(s) campo(s) de filtro(s) e pressione **Enter**. Filtros ativos são destacados em azul.

Filtros podem ser salvos ao seu perfil de usuário para que você possa usá-los novamente no futuro. Clique no ícone **Predefinições** para gerenciar os conjuntos de filtro:

Conjuntos de filtro	Seus filtros salvos, clique em um para aplicá-lo. O filtro aplicado é marcado com uma marcação ✔. Selecione **Incluir colunas visíveis, classificação e páginas** para salvar esses parâmetros na predefinição.
Salvar conjunto de filtros	Salve sua configuração de filtro atual como uma nova predefinição. Depois que a predefinição estiver salva, não é possível editar a configuração de filtro na predefinição.
Gerenciar conjuntos de filtros	Remova ou renomeie as predefinições existentes. Clique em **Salvar** para aplicar mudanças nas predefinições.
Limpar valores do filtro	Clique para remover apenas os valores atuais dos filtros selecionados. As predefinições salvas vão continuar sem ser modificadas.
Remover filtros	Clique para remover os filtros selecionados. As predefinições salvas vão continuar sem ser modificadas.
Remover filtros não utilizados	Remova os campos de filtro sem valor.
Redefinir filtros padrão	Redefinir o painel de filtro e mostrar os filtros padrão.



O botão de filtro do **Grupo de acesso** permite aos usuários selecionarem um grupo estático e filtrar os objetos visualizados de acordo com o grupo onde estão contidos.

Você pode usar marcações para filtrar os itens exibidos.

Layout do painel lateral

Clique no ícone ao lado do nome da seção e ajuste o layout do painel lateral usando o menu de contexto (as opções disponíveis podem variar com base no layout atual):

- **Ocultar painel lateral**
- **Exibir painel lateral**
- **Grupos**
- **Grupos e marcações**
- **Marcações**

Se os Grupos estiverem visíveis, você também pode selecionar uma destas opções:

- **Ampliar tudo**
- **Recolher tudo**

Gerenciar a tabela principal

Para reordenar uma coluna, passe o mouse sobre o ícone ao lado do nome da coluna e arraste e solte a coluna. Veja também **Editar colunas** abaixo.

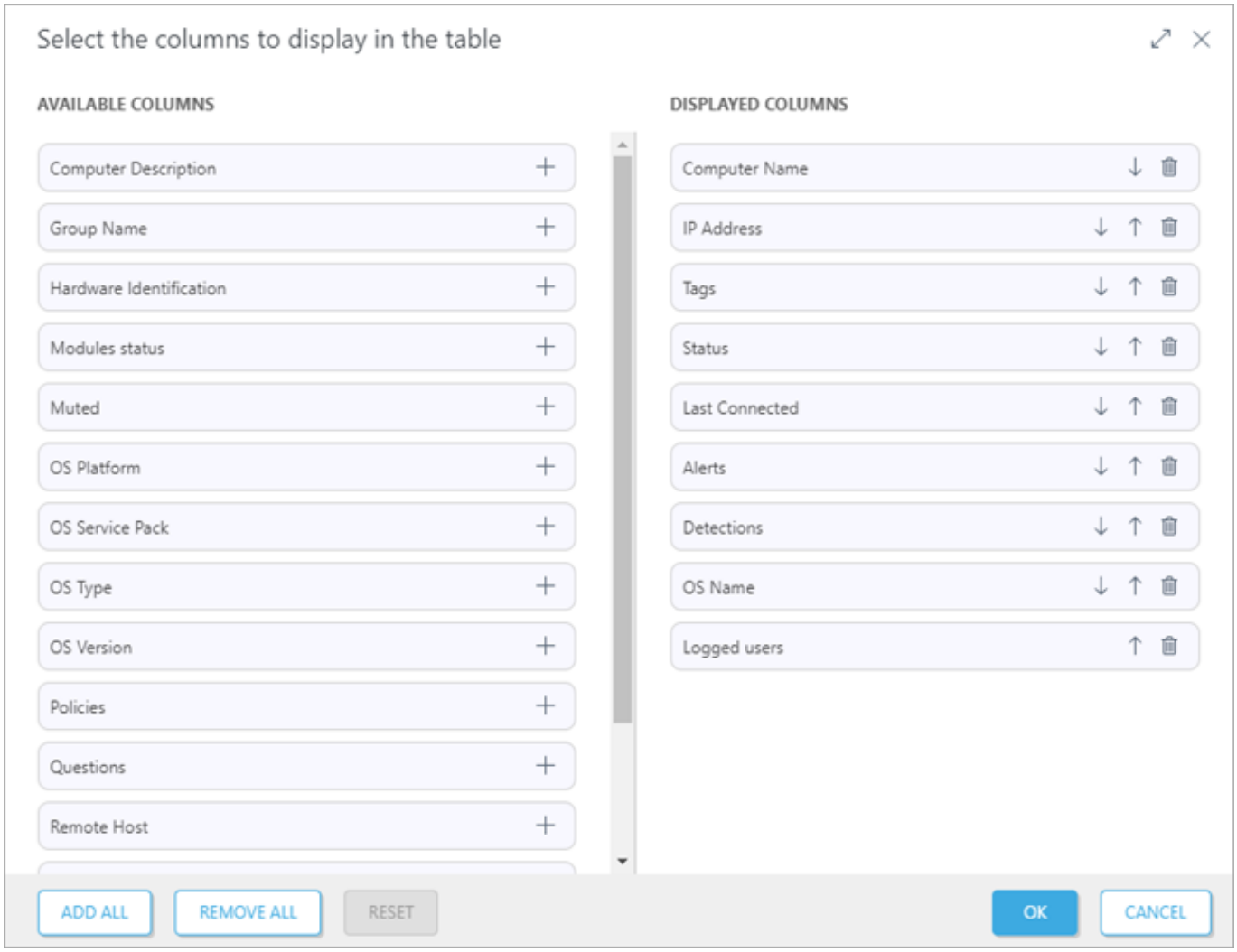
Para classificar por uma única coluna, clique no cabeçalho da coluna para classificar as linhas da tabela com base nos dados na coluna selecionada.

- Um clique resulta em classificação crescente (A–Z, 0–9) e ou dois cliques resulta em classificação decrescente (Z–A, 9–0).
- Depois de aplicar a classificação, uma pequena seta antes do cabeçalho da coluna indica o comportamento da classificação.
- Veja também a classificação múltipla abaixo.

Clique no ícone de engrenagem para gerenciar a tabela principal:

Ações

- **Editar colunas** –Usa o assistente para ajustar (adicionar, remover, reordenar) as colunas exibidas. Você também pode usar o recurso de arrastar e soltar para ajustar as colunas. Clique em **Redefinir** para redefinir as colunas da tabela para seu estado padrão (colunas disponíveis padrão em uma ordem padrão).



• **Ajustar automaticamente as colunas** – Ajusta automaticamente a largura das colunas.

• **Exibir tempo relativo/Exibir tempo absoluto**– altere o formato de exibição dos dados de tempo na tabela principal (por exemplo, **Última conexão** em **Computadores** ou **Ocorreu** em **Detecções**). Quando você ativar **Exibir tempo relativo**, passe o mouse sobre o tempo relativo na tabela para ver o tempo absoluto.

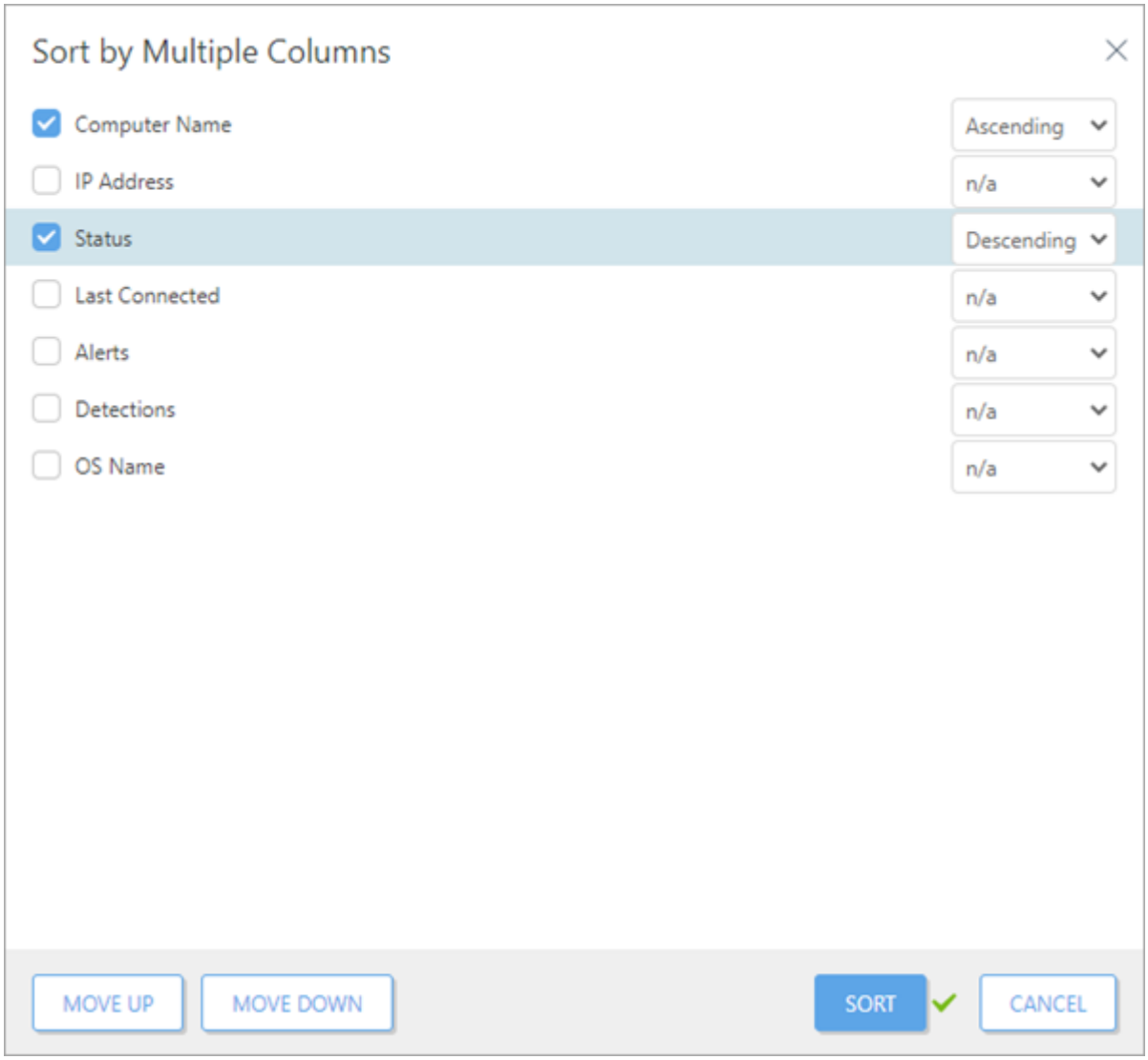
Classificação de tabela

• **Redefinir classificação** – redefine a classificação da coluna.

• **Classificação múltipla** – você pode classificar os dados da tabela ao selecionar várias colunas (até 4). Para cada uma das colunas, você pode ajustar:

oprioridade de classificação – altere a ordem das colunas clicando no botão **Mover para cima** ou **Mover para baixo** (primeira coluna: classificação primária, segunda coluna: classificação secundária, etc.). Depois de aplicar várias classificações, os números de índice aparecem antes dos cabeçalhos de coluna para indicar a prioridade de classificação.

ocomportamento de classificação – selecione **crescente** ou **decrescente** do menu suspenso.



1 classificação primária – coluna **Nome do computador**: classificação crescente aplicada.
2 classificação secundária – coluna **Status**: classificação decrescente aplicada como classificação secundária.

Relatórios

- **Exportar tabela como** – Exportar a tabela como um relatório no seu formato desejado. Você pode escolher de *.pdf* ou *.csv*. CSV é adequado apenas para dados da tabela e usa ; (ponto e vírgula) como delimitador. Se você fizer download de um relatório CSV e ver os números em uma coluna onde você espera um texto, recomendamos fazer download de um relatório PDF para ver os valores em texto.

- **Salvar um modelo de relatório** – Crie um novo modelo de relatório da tabela.

Marcações

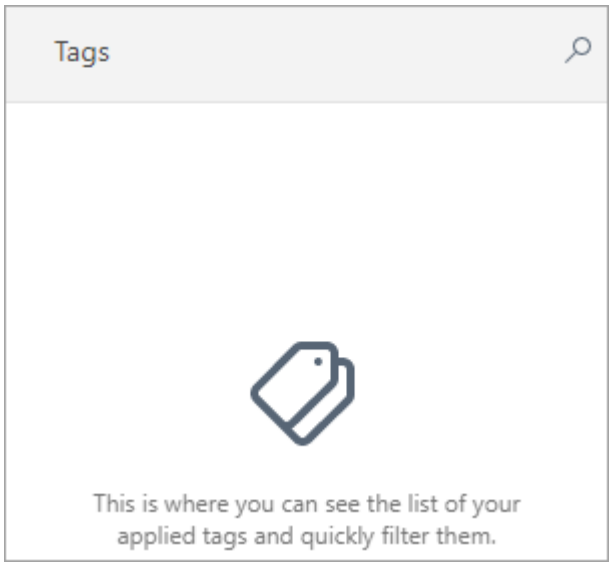
O ESET PROTECT permite marcar todos os objetos relevantes (computadores, detecções, tarefas, instaladores, políticas, notificações, licenças, etc.) com marcações definidas pelo usuário, que podem ser usadas para aprimorar ainda mais a filtragem e pesquisa. A marcação é integrada nativamente em todas as telas principais do console web ESET PROTECT.

As marcações são palavras-chave (rótulos) definidas pelo usuário que você pode adicionar a diferentes objetos para facilitar o agrupamento, filtragem e localização. Por exemplo, você pode atribuir uma marcação 'VIP' aos seus ativos relevantes e identificar rapidamente todos os objetos associados a eles.

Você pode criar e atribuir marcações manualmente. Os objetos MSP são marcados automaticamente com o nome do cliente.

Painel de marcações

Você pode ver as marcações existentes na seção **Marcações**, visível no canto inferior esquerdo da tela do menu console web ESET PROTECT:



Permissões para gerenciamento de marcações

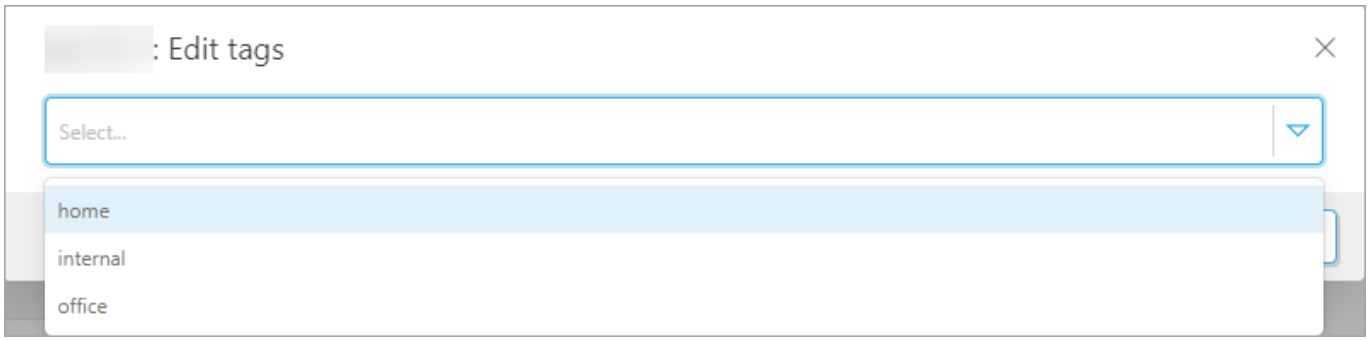
Para gerenciar marcações para um objeto, um usuário precisa ter direitos de acesso de **Uso** (conjunto de permissões atribuído) ao objeto. Usuários adicionais podem gerenciar marcações, ou seja, outro usuário pode remover uma marcação que você criou.

Atribuir marcações

Você pode atribuir marcações a um ou mais objetos.

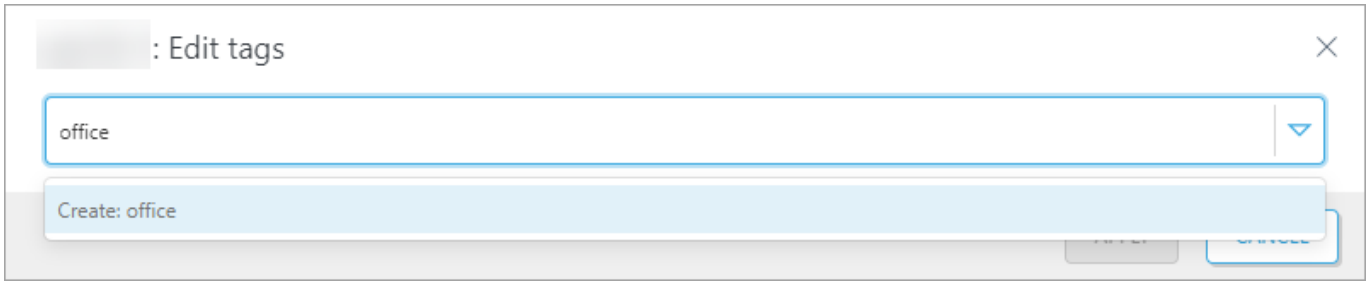
Para atribuir marcações, marque as caixas de seleção próximas ao(s) objeto(s) e clique em **Computador** > **Marcações**:

Para atribuir marcações já existentes, clique no campo de digitação em uma marcação da lista e clique em **Aplicar**.



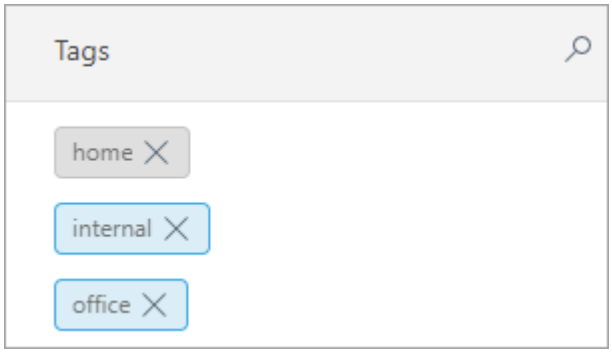
Criar uma nova marcação

Para criar uma nova marcação, digite o nome da marcação, selecione **Criar "tag_name"** e clique em **Aplicar**.



Filtrar objetos por marcações

Clique em uma marcação para aplicar um filtro aos objetos listados. As marcações selecionadas são azuis.

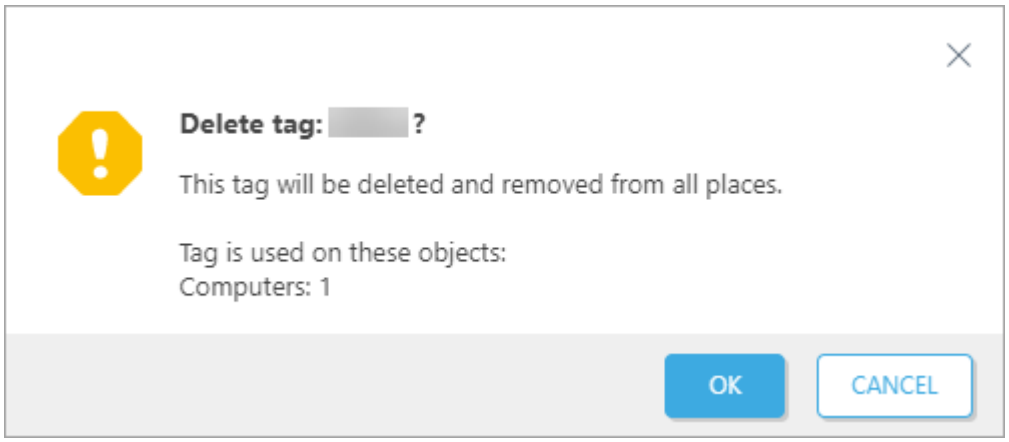


Cancelar atribuição de marcações

Para atribuir marcações, marque as caixas de seleção próximas ao(s) objeto(s) e clique em **Computador** > **Marcações**: Remova a marcação clicando no X e em **Aplicar**.

Remover uma marcação

Para remover uma marcação, passe o mouse sobre a marcação no painel **Marcações**, clique no ícone ✕ e clique em **OK** para confirmar que você deseja remover a marcação de todos os objetos no Web Console ESET PROTECT.



Importar CSV

A importação de uma lista pode ser realizada usando o arquivo *.csv* personalizado com uma estrutura adequada. Essa função é usada em vários menus na interface de usuário do ESET PROTECT. Dependendo do que vai ser importado, as colunas são alteradas.

1.Clique em **Importar CSV**.

2.**Carregar** - clique em **Escolher arquivo** e procure o arquivo *.csv* que você gostaria de **Carregar**.

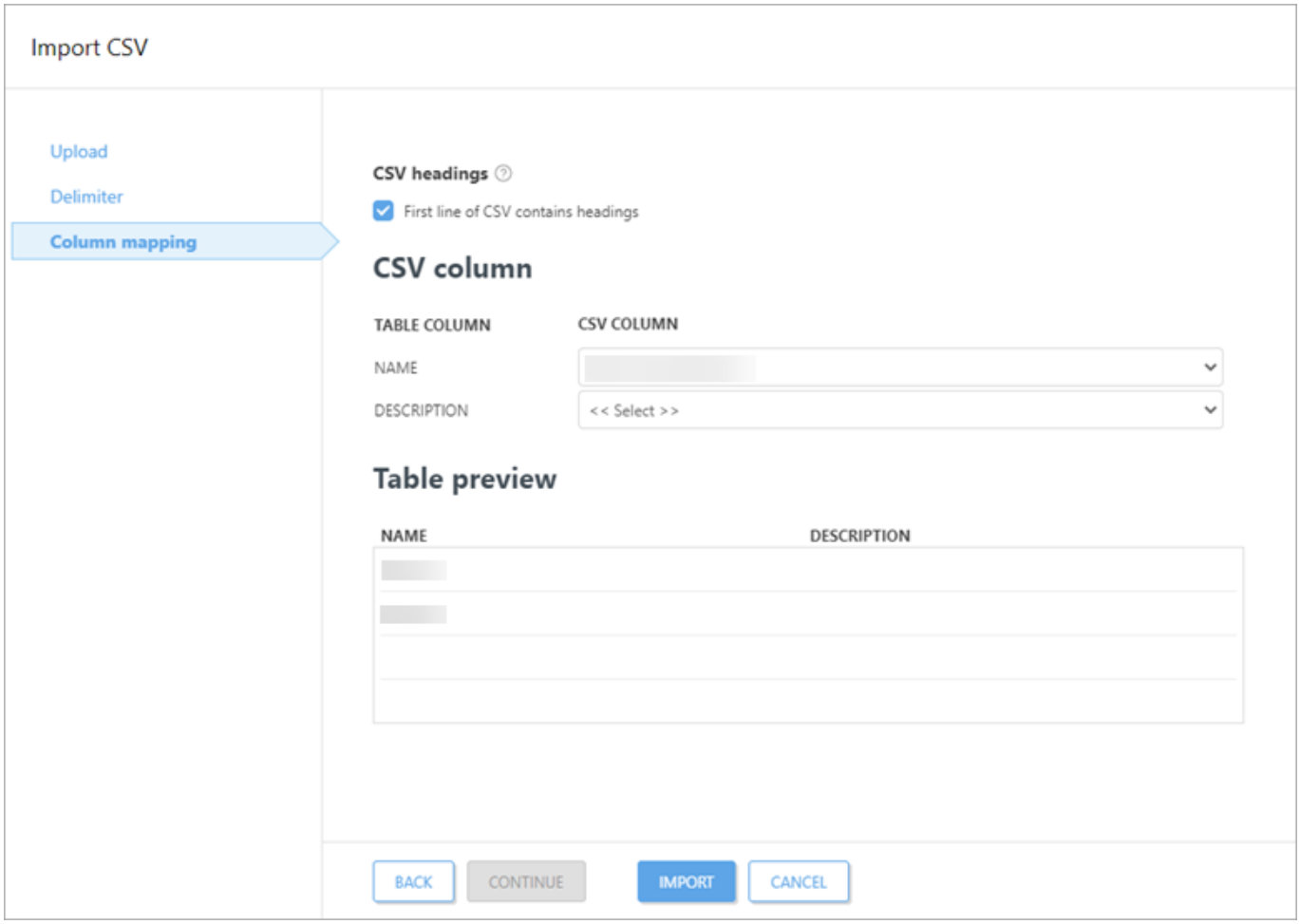
3.**Delimitador** - um delimitador é um caractere usado para separar strings de texto. Selecione o delimitador apropriado (**Ponto e vírgula**, **Vírgula**, **Espaço**, **Tabulação**, **Ponto**, **Barra vertical**) para combinar com o que o seu arquivo *.csv* usa. Se o seu arquivo *.csv* usa caracteres diferentes como delimitadores, selecione a caixa de seleção **Outros** e digite o caractere. **Visualização de dados** mostra o conteúdo de seu arquivo *.csv*, que pode ajudá-lo a identificar o tipo de delimitador que é usado para separar strings.

4.**Mapeamento de coluna** - assim que o arquivo *.csv* foi carregado e analisado, você pode mapear cada desejada no arquivo *.csv* importado para uma coluna ESET PROTECT **exibida na tabela. Use as listas suspensas para selecionar qual coluna CSV deve ser associada a uma coluna ESET PROTECT específica. Se seu arquivo** *.csv* **não tiver a linha de cabeçalho**, desmarque **Primeira linha de CSV contém cabeçalhos**.

5.Veja a **Pré-visualização da tabela** para garantir que o mapeamento de coluna está definido corretamente e a operação de importação vai funcionar da maneira que você quer.

6.Depois de ter mapeado com sucesso cada uma das colunas e a pré-visualização da Tabela parecer

correta, clique em **Importar** para iniciar a operação.



Solução de problemas - Console da Web

A tabela abaixo fornece algumas informações sobre as massagens e status de erros de login do console Web mais comuns, o que elas significam e algumas etapas adicionais de solução de problemas:

Mensagem de erro	Causa possível
⚠ Falha no login: Nome de usuário ou senha inválidos	Certifique-se de ter inserido seu Usuário e a Senha corretamente. Você pode redefinir a senha do Web Console ESET PROTECT.
⚠ Falha no login: Falha na conexão com estado 'Não conectado'	Verifique para ver se o serviço do Servidor ESET PROTECT e seu serviço de banco de dados estão em execução, consulte nosso artigo da Base de conhecimento para instruções passo a passo.
⚠ Falha no login: O usuário estava bloqueado. Tente novamente mais tarde.	Depois de 10 tentativas mal sucedidas de entrar do mesmo endereço IP (por exemplo, usando credenciais de login incorretas), outras tentativas de entrar feitas por esse endereço IP serão bloqueadas temporariamente. Depois de 10 minutos, entre usando as credenciais corretas.

Mensagem de erro	Causa possível
Falha no login: Erro de comunicação	Verifique se o serviço do Servidor ESET PROTECT está em execução e se o serviço do Apache Tomcat está em execução e funcionando corretamente. Revisão dos relatórios para o Apache Tomcat. Visite nosso artigo da Base de conhecimento para mais informações sobre este problema.
Falha no login: Tempo limite de conexão	Verifique a conexão de rede e as configurações de firewall para se certificar de que o Console da Web ESET PROTECT pode chegar ao Servidor ESET PROTECT. Além disso, o Servidor ESET PROTECT pode estar sobrecarregado, tente reiniciar. Este problema também pode acontecer se você está usando versões diferentes do Console da Web ESET PROTECT e do Servidor ESET PROTECT.
Falha no login: O usuário não tem direitos de acesso atribuídos	O usuário não tem nenhum direito de acesso atribuído. Faça login como administrador e edite a conta de usuário para que ele tenha pelo menos um Conjunto de permissões atribuído.
Falha no login: Erro de pareamento de resposta	Sua versão do console da Web e Servidor ESET PROTECT não são compatíveis. Isso pode acontecer durante ou depois da atualização dos componentes. Se o problema continuar, implemente a versão correta do console da Web manualmente.
Usando conexão não criptografada! Configure o servidor Web para usar HTTPS	Por razões de segurança, recomendamos configurar o console da Web ESET PROTECT para usar HTTPS.
O JavaScript está desativado. Ative o JavaScript no seu navegador.	Ative o JavaScript ou atualize seu navegador da web.
SEC_ERROR_INADEQUATE_KEY_USAGE (apenas Mozilla Firefox).	O Mozilla Firefox tem um depósito de certificado corrompido.

Erro	Causa possível
Você não visualiza a tela de login ou quando a tela de login aparecer ela parece estar constantemente sendo carregada.	• Reinicie o serviço ESET PROTECT Server. Assim que o serviço ESET PROTECT Server estiver em funcionamento novamente, reinicie o serviço Apache Tomcat. Depois disso, a tela de login do console da Web ESET PROTECT será carregada com êxito. Leia também nosso artigo da Base de conhecimento. • Se o Apache Tomcat não conseguir extrair o conteúdo do arquivo *era.war* e o Web Console não estiver acessível, siga as etapas em nosso artigo da Base de conhecimento.
O texto está faltando no menu de contexto e no menu de **Links rápidos** no console da Web ESET PROTECT.	Este problema pode ser causado por uma extensão de bloqueio de publicidade no navegador. Para resolver o problema, desative a extensão de bloqueio de publicidade do navegador para a página do console da Web ESET PROTECT.
Depois de entrar, o console web não é exibido corretamente (elementos faltando, etc.).	Verifique se você está usando um navegador da web compatível.

Depois de entrar, algumas telas do Web Console não carregam.	Se algumas telas do Web Console ESET PROTECT (por exemplo, computadores) não carregarem, abra o arquivo *Tomcat9w.exe* localizado em *C:\Program Files\Apache Software Foundation\[Tomcat pasta]*
	• Na guia **geral**, clique em **Parar** para parar o serviço Apache Tomcat.
	• Selecione a guia **Java** e adicione o código a seguir em **Java Options**:
	`-Duser.country=US`
	`-Duser.language=en`
	• Na guia **Geral**, clique em **Iniciar** para iniciar o serviço Apache Tomcat.

Erro	Causa possível
O Web Console leva muito tempo para ser carregado. Ao carregar um grande número de objetos, o console falha.	O Web Console precisa de memória adicional ao lidar com grandes conjuntos de objetos. Consulte o Web Console para as configurações corporativas.
Algumas telas no Web Console não são carregadas corretamente e você vê um erro. Por exemplo, ao editar uma política, você vê o erro: "ERROR WHILE INITIALIZING CONFIGURATION EDITOR.: (TYPEERROR) : ((INTERMEDIATE VALUE)(INTERMEDIATE VALUE) , K).INITCONFIGEDITOR IS NOT A FUNCTION"	Esse problema ocorre se você estiver usando um proxy inverso que evita que alguns módulos do Web Console sejam carregados. As strings de URL para módulos individuais do Web Console (carregados no Apache Tomcat) podem mudar dinamicamente (por exemplo, a string depois de `era/webconsole/configEngine/` em `era/webconsole/configEngine/02645EFC6ABCDE2B449042FB8S63FD3/v0.0/css/001_ce.ltr.css`). Para resolver o problema, certifique-se de que você configurou o proxy inverso corretamente.
Ao importar um arquivo grande (mais de 20 MB) (por exemplo, uma política) o processo falha.	O limite de tamanho de arquivo para o Web Console é de 20 MB. Você pode alterar isso editando o arquivo *EraWebServerConfig.properties*, localizado na pasta *[Tomcat folder]\webapps\era\WEB-INF\classes\sk\eset\era\g2webconsole\server\modules\config*. Altere `file_size_limit=20` para um valor superior, o valor máximo é de 250.

- Depois da atualização do ESET PROTECT, recomendamos que você remova o cache e os cookies do navegador da web antes de entrar no console web atualizado.
- Como o console da Web usa protocolo seguro (HTTPS), você poderá receber uma mensagem no navegador da Web em relação a um certificado de segurança ou conexão não confiável (o texto exato da mensagem dependerá do navegador que você está usando). Isso se deve ao fato de que o navegador deseja verificar a identidade do site que você está tentando acessar. Clique em **Avançado** > **Continuar para [endereço] (inseguro)** (Chrome/Edge) ou **Avançado** > **Aceitar o risco e continuar** (Firefox) para permitir o acesso ao Web Console ESET PROTECT. Isso se aplica somente quando você está tentando acessar o URL do Console da Web ESET PROTECT. Visite nosso artigo da Base de conhecimento para obter mais informações sobre como configurar a conexão HTTPS/SSL.

Como gerenciar produtos Endpoint a partir do ESET PROTECT

Antes que você possa começar a gerenciar as Soluções de Negócios ESET você precisa realizar a configuração inicial. Recomendamos que você use a Visão geral de status, especialmente se você tiver ignorado o ESET PROTECT Assistente de inicialização. O administrador pode realizar várias tarefas a partir do console da Web ESET PROTECT para instalar produtos e controlar computadores cliente.

Instalação do Agente ESET Management e produtos de segurança Endpoint

O ESET PROTECT requer que o Agente ESET Management seja instalado em cada computador cliente gerenciado. O Agente ESET Management pode ser instalado em combinação com seu produto de segurança Endpoint. Antes da instalação, recomendamos que você importe sua licença no ESET PROTECT para que ela possa ser usada para suas instalações consequentes. Existem vários métodos para instalar seu produto Endpoint:

- Use o instalador do Agente e do produto de segurança ESET ou o ESET Remote Deployment Tool para instalar seu produto Endpoint e Agente ESET Management ao mesmo tempo.

- Clique em um computador e selecione **Soluções** > **Implantação de produto de segurança** para implantar um produto de segurança ESET no computador.

- Instale seu produto ESET Endpoint em clientes onde você já instalou um Agente ESET Management usando uma tarefa de cliente.

Gerenciamento de produto de segurança ESET a partir de ESET PROTECT

Todos os produtos de segurança Endpoint podem ser gerenciados do console da Web ESET PROTECT. As políticas são usadas para aplicar configurações a computadores únicos ou grupos. Por exemplo, você pode criar uma política para bloquear o acesso a determinadas localidades da web, alterar as configurações de sensibilidade de detecção do escaneador (disponível no Endpoint 7.2 e versões posteriores) ou alterar todas as outras configurações de segurança ESET. Políticas podem ser mescladas, como mostrado em nosso exemplo. Políticas definidas usando o ESET PROTECT não podem ser substituídas por um usuário em uma máquina do cliente. Porém o administrador pode usar o recurso substituição para permitir que um usuário faça alterações em um cliente temporariamente. Quando tiver terminado de fazer as alterações, você pode solicitar a configuração final do cliente e salvar como uma nova política.

Tarefas também pode ser usadas para gerenciar clientes. As tarefas são implantadas a partir do Console da Web e executadas no cliente pelo Agente ESET Management. As tarefas de cliente mais comuns para o Windows Endpoints são:

- Atualizar módulos (também atualiza o banco de dados de vírus)

- Execução do Rastreamento sob demanda

- Executar comando personalizado

- Solicite a configuração do computador e produto

Atualizar produtos de segurança ESET

1. Clique no **Painel** > **Visão geral do status** > Status da versão do componente.

2. Clique no gráfico amarelo/vermelho representando componentes ou aplicativos desatualizados e selecione **Atualizar componentes ESET instalados** para iniciar uma atualização.

Relatórios do status do computador e obtenção de informações de clientes para ESET PROTECT

Cada computador cliente está conectado ao ESET PROTECT através do Agente ESET Management. O Agente reporta todas as informações solicitadas sobre a máquina do cliente e seu software para o ESET PROTECT. Servidor. A conexão entre o agente e o servidor é definida por padrão para 1 minuto, mas pode ser alterada em sua política do Agente ESET Management. Todos os relatórios dos Endpoints ou outros produto de segurança ESET são enviados ao ESET PROTECT. Servidor.

Informações sobre produtos ESET instalados e outras informações básicas sobre o sistema operacional e status de um cliente podem ser encontradas em **Computadores**. Selecione um cliente e clique em **Detalhes**. Na seção

Configuração desta janela, um usuário pode procurar as configurações mais antigas ou solicitar a configuração atual. Na seção **Sysinspector**, um usuário pode solicitar relatórios (apenas de computadores Windows).

O Console web também permite a você acessar uma lista de todas as detecções dos dispositivos do cliente. Detecções de dispositivos únicos podem ser vistas em **Computadores**. Selecione um cliente e clique em **Detalhes** > **Detecções e quarentenas**. Se o computador cliente executar o ESET Inspect, você poderá visualizar e gerenciar detecções do ESET Inspect.

Você pode gerar relatórios personalizados sob demanda ou usar uma tarefa agendada para ver os dados sobre clientes na sua rede. Modelos de relatório predefinidos oferecem uma forma rápida de coletar dados importantes, ou você pode criar seus próprios novos modelos. Exemplos de relatórios incluem informações agregadas sobre computadores, detecções, quarentena e atualizações necessárias.

Um usuário só pode usar modelos de relatório para os quais ele tenha permissões suficientes. Por padrão, todos os modelos são armazenados no grupo **Todos**. Um relatório só pode incluir informações sobre computadores e eventos dentro do escopo de permissões daquele usuário. Mesmo se o modelo de relatório for compartilhado entre mais usuários, o relatório de cada usuário só vai ter informações sobre os dispositivos para os quais aquele usuário têm permissão. Veja a lista de permissões para obter mais informações sobre os direitos de acesso.

Serviço de notificação por push da ESET

ESET Push Notification Service (EPNS) serve para receber mensagens do Servidor ESET PROTECT, se o servidor tiver uma notificação para o cliente. A conexão está sendo executada para que o ESET PROTECT possa enviar uma notificação (push) para um cliente imediatamente. Quando a conexão for quebrada, o cliente tentará se reconectar. A principal razão para a conexão permanente é disponibilizar os clientes para eles receberem mensagens.

Um usuário do Web Console pode enviar Chamadas para despertar via EPNS entre o ESET PROTECT Servidor e Agentes ESET Management. O Servidor ESET PROTECT envia chamadas **Wake on LAN**. Você pode definir endereços multicast para o **Wake on LAN** nas **Mais** > Configurações.

Detalhes da conexão

Para configurar sua rede local para permitir a comunicação com o EPNS, o Agente ESET Management e o Servidor ESET PROTECT precisam conseguir conectar ao servidor EPNS. Se você não conseguir estabelecer uma conexão com o EPNS para seus Agentes, apenas as Chamadas para despertar serão afetadas.

Protocolo de segurança criptográfico	TLS
Protocolo	MQTT (protocolo de comunicação de máquina para máquina)
Porta	• primário: 8883 • fallback: 443 e a porta do proxy definida pela política do Agente ESET Management A porta 8883 é a preferida, pois é uma porta MQTT. A porta 443 é apenas uma porta de fallback e é compartilhada com outros serviços. Além disso, um firewall pode anular a conexão na porta 443 devido a uma inatividade ou limite máximo de conexões abertas para o servidor Proxy HTTP.
Endereço de Host	*epns.eset.com*

Compatibilidade de proxy	Se você usar o Proxy HTTP para encaminhar a comunicação, as Chamadas para despertar também serão enviadas pelo Proxy HTTP. A autenticação não é compatível. Certifique-se de configurar a política do Agente Proxy HTTP nos computadores para os quais deseja enviar as Chamadas de despertar. Caso o Proxy HTTP não esteja funcionando, as Chamadas para despertar são enviadas diretamente.

Solução de problemas

- Certifique-se de que seu firewall está configurado para permitir a conexão com EPNS (veja os detalhes acima ou o artigo da Base de conhecimento).
- Certifique-se de que tanto o Agente quanto o Servidor podem se conectar diretamente ao servidor EPNS nas portas 443 e 8883 (para verificar a conexão, use o comando `telnet`).
- Se você executar a Máquina virtual e receber o alerta **não foi possível acessar os servidores do serviço EPNS**, consulte as etapas de solução de problemas.

VDI, clonagem e detecção de hardware

O ESET PROTECT é compatível com ambientes VDI, clonagem de máquinas e sistemas de armazenamento não persistentes. Esse recurso é necessário para criar uma marca para o computador mestre ou para resolver uma pergunta que aparece depois de uma clonagem ou mudança de hardware.

- Até que a pergunta seja respondida, a máquina do cliente não é capaz de replicar ao ESET PROTECT. Servidor. O cliente verifica apenas se a questão está resolvida.
- Desativar a detecção de hardware é irreversível, tenha muito cuidado e faça isso apenas em máquinas físicas!
- Ao resolver várias perguntas, use o bloco Visão geral do status - **Perguntas**.

Quais sistemas operacionais e hypervisors são compatíveis?

Antes de começar a usar o VDI com o ESET PROTECT, leia mais sobre os recursos compatíveis e incompatíveis de vários ambientes VDI em nosso artigo da Base de conhecimento.

- Apenas sistemas operacionais Windows são compatíveis.
- ESET Full Disk Encryption não é compatível.
- Dispositivos móveis gerenciados via MDM não são compatíveis.
- Clones vinculados na Virtual Box não podem ser separados entre si.
- Em casos muito raros, a detecção pode ser desligada automaticamente pelo ESET PROTECT. Isso acontece quando o ESET PROTECT não consegue analisar o hardware com confiança.
- Ver a lista de configurações compatíveis:
  - Citrix PVS 7.0+ com máquinas físicas

- Citrix PVS 7.0+ com máquinas virtuais em um Citrix XenServer 7+
- Citrix PVS 7.0+ e Citrix XenDesktop com Citrix XenServer 7+
- Serviços de criação de máquina Citrix
- (sem PVS) Citrix XenDesktop com Citrix XenServer 7+
- VMware Horizon 7.x e 8.0 com VMware ESXi
- Microsoft SCCM (para novas imagens)

- O ESET PROTECT é compatível com padrões de nomeação VDI para todos os hypervisors compatíveis.

Ambientes VDI

Você pode usar a máquina Mestre com o Agente ESET Management para uma pool VDI. Não há conector VDI necessário; toda a comunicação é tratada através do Agente ESET Management. O Agente ESET Management deve ser instalado na máquina mestre antes do pool VDI (catálogo da máquina) ser definido.

- Se quiser criar um pool VDI, marque o computador Mestre em Detalhes do computador > **Virtualização** antes de criar o pool. Selecione **Marcar como Mestre para clonagem (Correspondente com o computador existente)**.

- Se o computador Mestre for removido do ESET PROTECT, é proibido recuperar sua identidade (clonar). Novas máquinas do pool iriam obter uma nova identidade a cada vez (uma nova entrada de máquina é criada no console da Web).

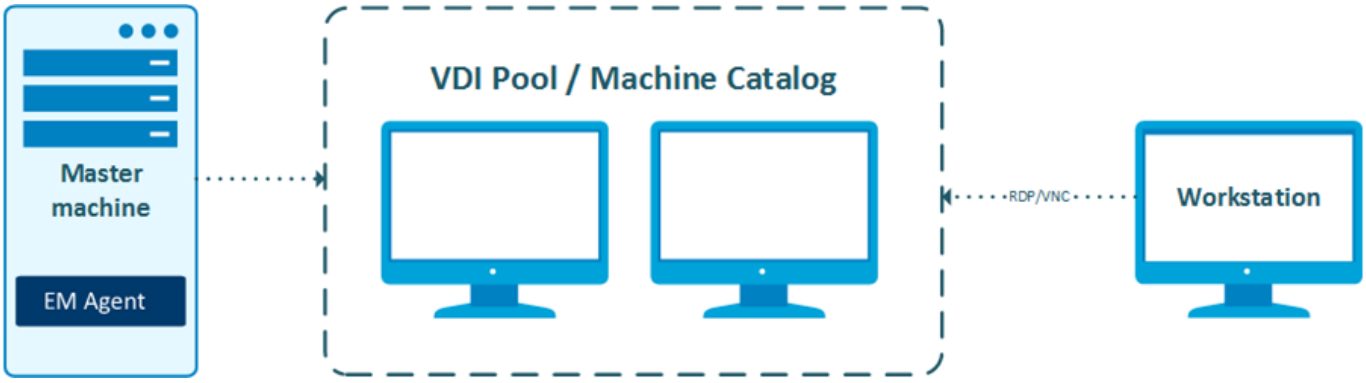
- Quando uma máquina do pool VDI conecta pela primeira vez, é obrigatório ter um intervalo de conexão de 1 minuto. Depois das primeiras replicações o intervalo de conexão é herdado do mestre.

- Nunca desative a detecção de hardware ao usar o pool VDI.

- Você pode ter a máquina mestre sendo executada junto com os computadores clonados, para que ela possa ser mantida atualizada.

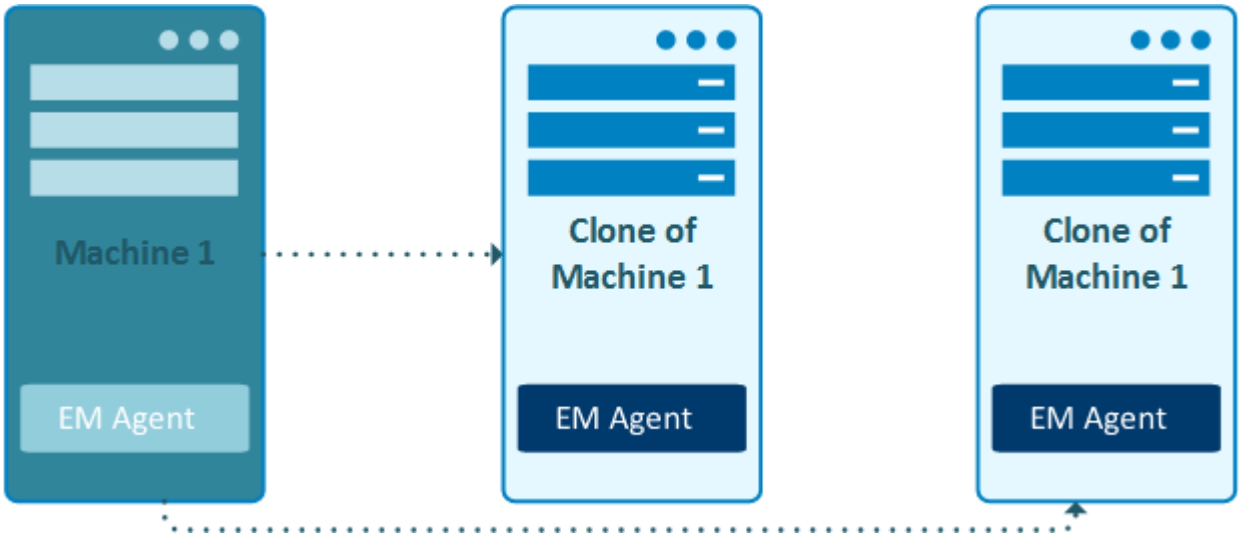
Grupo padrão para máquinas VDI

Novas máquinas clonadas do Mestre aparecem no grupo estático **Perdido e encontrado**. Isso não pode ser alterado.



Clonagem de máquinas no hypervisor

Você pode criar um clone de uma máquina regular. Aguarde o aparecimento da Pergunta e resolva-a selecionando **Criar novo computador apenas dessa vez**.



Criação de imagem de sistemas para máquinas físicas

Você pode usar a imagem Mestre com o Agente ESET Management instalado e implementá-la em computadores físicos. Há duas maneiras de realizar isso:

1. O sistema cria uma nova máquina no ESET PROTECT depois de cada instalação de imagem.

   • Resolva cada novo computador manualmente nasPerguntas e selecione **Criar um novo computador todas as vezes**.

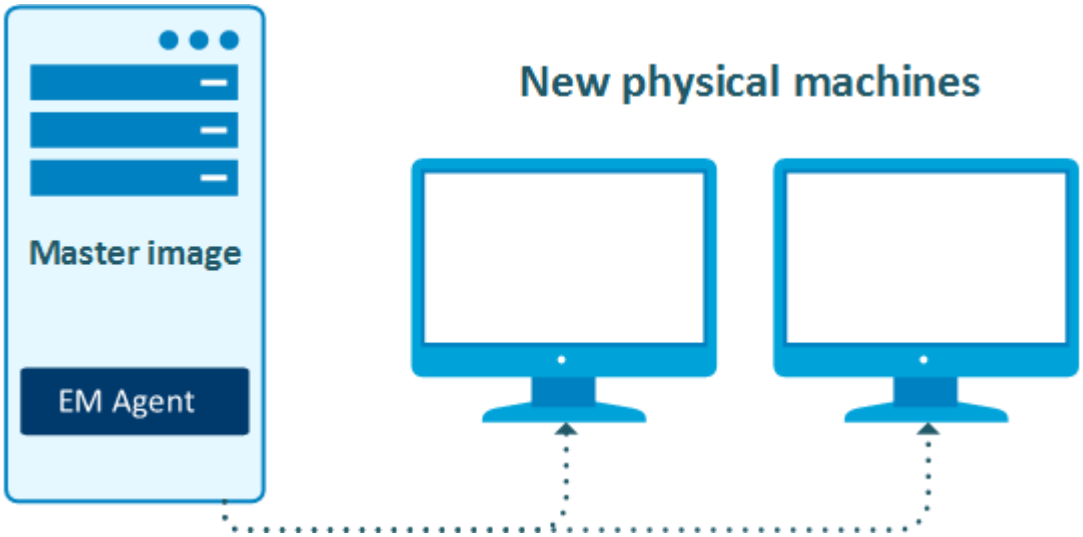
   • Marque a máquina Mestre antes de clonar. Selecione **Marca como Mestre para clonagem (Criar um novo computador)**.

2. O sistema cria uma nova máquina no ESET PROTECT depois da imagem ser instalada em uma nova máquina. Se a imagem for instalada novamente em uma máquina com histórico anterior no ESET PROTECT (que já tinha o Agente ESET Management instalado), essa máquina é conectada à sua identidade anterior no ESET PROTECT.

   • Resolva cada novo computador manualmente em Perguntas e selecione **Corresponder com um computador existente todas as vezes**.

• Marque a máquina mestre antes de clonar. Selecione **Marcar como Mestre para clonagem (Correspondente com o computador existente)**.

Se você tiver uma imagem (ou modelo) do seu computador mestre, mantenha-a atualizada. Sempre atualize a imagem depois da atualização ou reinstalação de qualquer componente ESET na máquina principal.



Replicação paralela

ESET PROTECT Servidor pode reconhecer e resolver a replicação paralela de várias máquinas para uma única identidade no ESET PROTECT. Tal evento é reportado para os Detalhes do computador – **Alertas** ("**Várias conexões com ID de agente idêntico**"). Há duas maneiras de resolver o problema:

• Use a ação em um clique disponível no alerta. Os computadores são divididos e sua detecção de hardware é desligada permanentemente.

• Em casos raros, mesmo os computadores com detecção de hardware desligada podem gerar conflitos. Nesses casos a tarefa Redefinir agente clonado é a única opção.

• Executar a Tarefa de redefinir agende clonado na máquina. Isso o impede de ter a detecção de hardware desativado.

Solução de problemas

Se você tiver problemas com um clone VDI, execute as etapas de solução de problemas VDI.

Resolver questões de clonagem

Toda vez que uma máquina conectar ao ESET PROTECT, uma entrada será criada com base em duas impressões digitais:

• um UUID de Agente ESET Management (identificador universalmente exclusivo) – ele muda depois do

Agente ESET Management ser reinstalado em uma máquina (consulte a Situação de Agente duplo).

- uma impressão digital de hardware da máquina – ela muda se a máquina for clonada ou reimplementada.

Uma pergunta é exibida se o ESET PROTECT Servidor detectar um dos seguintes:

- um dispositivo clonado conectando
- uma mudança de hardware em um dispositivo existente com o Agente ESET Management instalado

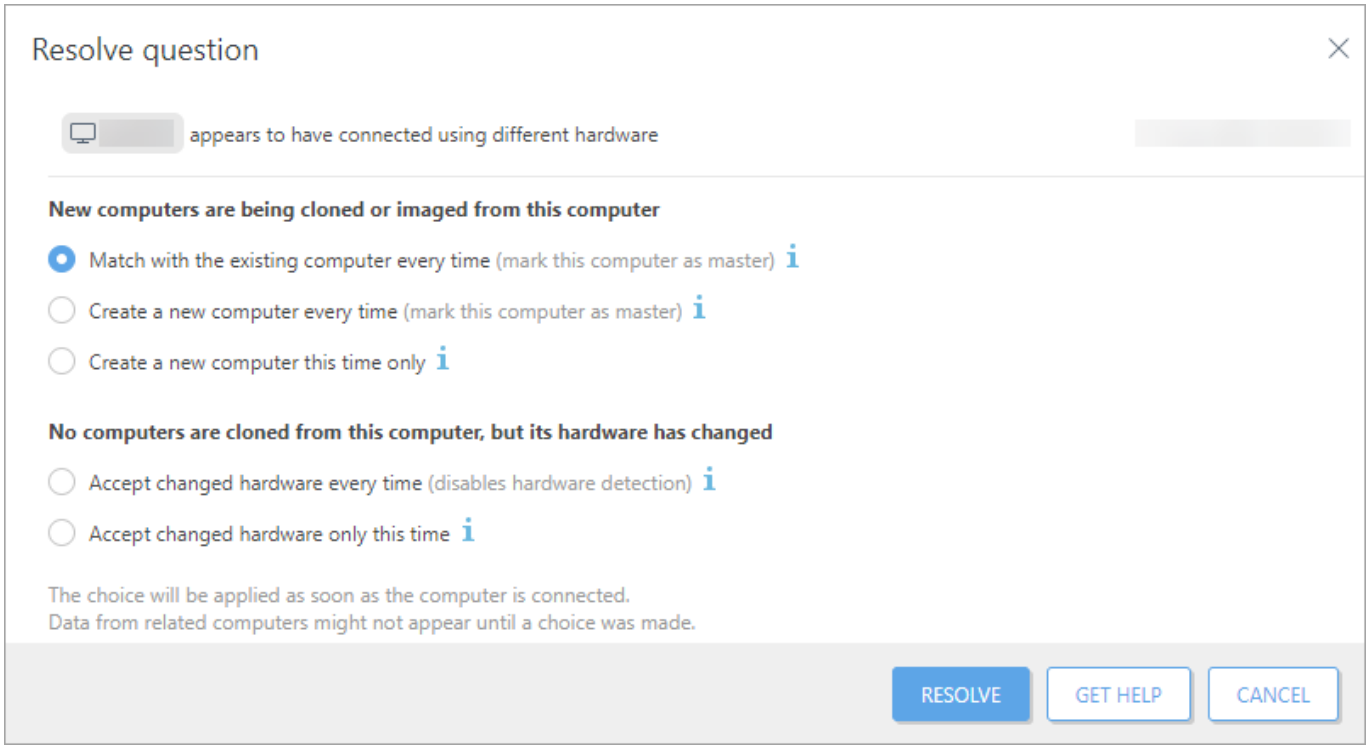
A detecção de Impressão digital de hardware não é compatível com:
- Linux, macOS, Android, iOS
- máquinas sem o Agente ESET Management

Clique na pergunta e selecione **Resolver pergunta** para abrir um menu com as opções a seguir:

Novos computadores estão sendo clonados ou tendo imagens criadas a partir deste computador	Ação	Mais detalhes
Corresponder com o computador existente todas as vezes	Selecione esta opção quando: • Você usa o computador como mestre e todas as duas imagens devem se conectar a uma entrada de computador existente no ESET PROTECT. • Você usa o computador como mestre para configurar um ambiente VDI e o computador está no pool VDI e espera-se que ele recupere sua identidade com base no ID de impressão digital de hardware.	Artigo KB
Criar um novo computador todas as vezes	Selecione esta opção quando usar esse computador como imagem mestre e se quiser que o ESET PROTECT reconheça automaticamente todos os clones desse computador como novos computadores. Não use com ambientes VDI.	Artigo KB
Criar um novo computador apenas dessa vez	O computador é clonado apenas uma vez. Selecione para criar uma nova instância para o dispositivo clonado.	Artigo KB

Nenhum computador é clonado a partir deste computador, mas seu hardware é alterado	Ação
Aceitar a alteração de hardware todas as vezes	Desative a detecção de hardware permanentemente para este dispositivo. Use apenas se mudanças de hardware não existentes forem reportadas. **Essa ação não pode ser revertida!** Se você desativar a detecção de hardware, tanto o Agente quanto o Servidor armazenam essa configuração. A nova implantação do Agente não restaura a detecção de HW desativada. Máquinas com detecção de hardware desativada não são adequadas para os cenários VDI no ESET PROTECT.
Aceitar o hardware alterado apenas dessa vez	Selecione para renovar a impressão digital de hardware do dispositivo. Use essa opção depois do hardware no computador cliente ser alterado. Futuras modificações de hardware serão reportadas novamente.

Clique em **Resolver** para enviar a opção selecionada.



Situação de Agente duplo

Se um Agente ESET Management for desinstalado (mas o computador não for removido do console da Web) na máquina do cliente e instalado novamente, existem dois computadores iguais no console da Web. Um está conectando ao ESET PROTECT e o outro não. Essa situação não é tratada pela janela de diálogo **Perguntas**. Tal situação é resultado de um procedimento de remoção de agente incorreto. A única solução é remover manualmente o computador que não está conectando do console da Web. O histórico e os relatórios criados antes da reinstalação serão perdidos depois dela.

Usando a tarefa Remover computadores não conectando

Se você tiver um pool de VDI de computadores e não resolver a questão (veja acima) corretamente, o console web criará uma nova instância do computador depois de recarregar o computador do pool. Instâncias de computador vão acumulando no console web e podem causar excesso de uso das licenças. Não recomendamos que isso seja resolvido com a configuração de uma tarefa para remover computadores não conectando. Tal procedimento remove o histórico (relatórios) dos computadores removidos e também pode causar excesso de uso das licenças.

Excesso de uso das licenças

Quando um computador de cliente com o ESET Management Agent instalado e produtos de segurança ESET ativados é clonado, cada máquina clonada pode reivindicar outra licença. Este processo pode causar excesso de uso das suas licenças. Em ambientes VDI, use um arquivo de licença off-line para a ativação de produtos ESET e entre em contato com a ESET para modificar sua licença.

Notificações para computadores clonados

Existem três notificações preparadas que o usuário pode usar para ações relacionadas a clonagem e alteração de

hardware, ou o usuário pode criar uma nova notificação personalizada usando eventos relacionados à clonagem. Para configurar uma notificação vá para o menu **Notificações** no console da Web.

- **Novo computador inscrito** – Notifica se um computador é conectado pela primeira vez para o grupo estático selecionado (o grupo **Todos** é selecionado por padrão).
- **Identidade do computador recuperada** – Notifica se um computador foi identificado com base no seu hardware. O computador foi clonado de uma máquina Mestre ou de outra fonte conhecida.
- **Clonagem de computador em potencial detectada** – Notifica sobre uma modificação de hardware significativa ou clonagem se a máquina de origem não foi marcada como Mestre anteriormente.

Solução de problemas

Se você tiver problemas com um clone VDI, execute as etapas de solução de problemas VDI.

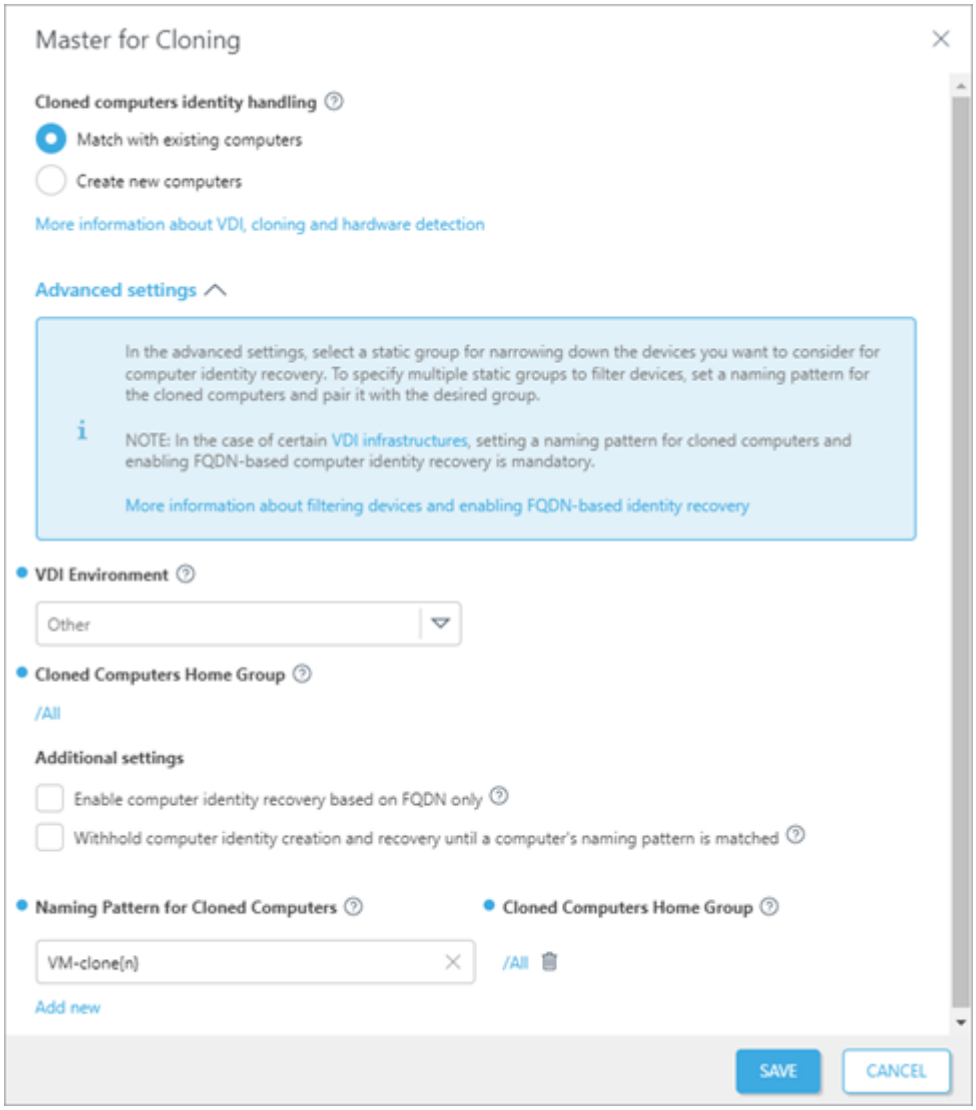
Identificação de hardware

O ESET PROTECT está coletando detalhes de hardware sobre cada dispositivo gerenciado e tenta identificá-los. Todos os dispositivos conectados ao ESET PROTECT pertencem a uma das categorias a seguir, exibidas na coluna **Identificação de hardware**, na janela **Computadores**.

- **Detecção de hardware ativada** – a detecção está ativada e funciona bem.
- **Detecção de hardware desativada** – a detecção foi desativada pelo usuário ou automaticamente pelo ESET PROTECT.
- **Sem informações de hardware** – sem informações de hardware disponíveis, ou o dispositivo do cliente está executando um sistema operacional incompatível ou uma versão antiga do Agente ESET Management.
- **Detecção de hardware não confiável** – a detecção é reportada pelo usuário como não sendo confiável, e será desativada. Esse status pode acontecer apenas durante o intervalo de replicação único antes da detecção ser desativada.

Mestre para clonagem

Clicar em **Virtualização** > **Marcar como Mestre para clonagem** em detalhes do computador exibe a notificação a seguir:



Selecione uma das opções de **Tratamento de identidade de computadores clonados** antes de criar o pool VDI:

- **Correspondente com o computadores existente** - Consulte a opção Sempre correspondente com um computador existente.
- **Criar novos computadores** – consulte a opção Sempre criar um novo computador.

> Para encontrar os computadores marcados como Mestre para clonagem, vá para **Computadores** > clique em **Adicionar filtro** > selecione **Mestre para clonagem** > selecione a caixa de seleção ao lado do filtro **Mestre para clonagem**.
> Você pode alterar as configurações do **Mestre para clonagem** posteriormente nos detalhes do computador:
> - Ajuste as configurações clicando no ícone de engrenagem no bloco **Virtualização**.
> - Remova as configurações clicando em **Virtualização** > **Desmarcar como Mestre para clonagem**.

Configurações avançadas

1. **Ambiente VDI** – Selecione o tipo de ambiente VDI para pré-preenchimento das configurações necessárias para o ambiente.

   - Citrix MCS/PVS Gen1 VMs

- Citrix PVS Gen2 VMs
- Clones vinculados do VMware Horizon
- Clones instantâneos do VMware Horizon
- SCCM
- Outras

2. **Grupo doméstico de computadores clonados** – selecione um grupo estático para limitar os dispositivos que você quer considerar para a recuperação de identidade do computador. O grupo estático selecionado também serve como o destino para máquinas virtuais recém-criadas.

3. **Configurações adicionais**:

- **Ativar a recuperação de identidade do computador baseada apenas em FQDN** – selecione a caixa de marcação para ativar a recuperação de identidade do computador baseada em FQDN (nome de domínio totalmente qualificado) se os atributos de hardware das máquinas clonadas geradas pela sua infraestrutura VDI não forem confiáveis para o processo de recuperação.

- **Reter a criação e recuperação de identidade do computador até que o padrão de nomeação do computador seja igualado** – selecione a caixa de seleção para garantir que o nome do computador clonado combina com um dos padrões de nomeação fornecidos. A criação e recuperação de identidade do computador não será concluída se um padrão correspondente não for encontrado.

Com base no ambiente VDI selecionado, as configurações recomendadas são pré-selecionadas (elas podem ser obrigatórias ou indisponíveis).

4. **Padrão de nomeação para computadores clonados** – clique em **Adicionar novo** e digite o padrão de nomeação para filtrar dispositivos.

Padrão de nomeação VDI

O ESET PROTECT reconhece apenas clones com nomes que combinam com o padrão de nomeação definido no ambiente VDI:

- **VMware** – o padrão de nomeação VDI é obrigatório para Clones instantâneos do VMware. O padrão de nomeação VDI deve ter um espaço reservado especificado para um número único `{n}` gerado pela infraestrutura VDI, por exemplo `VM-instant-clone-{n}`. Consulte a documentação VMware para mais detalhes sobre padrões de nomeação.
- **Citrix XenCenter/XenServer** – use o hash `#` no esquema de nomeação de catálogo da máquina, por exemplo `VM-office-##`. Consulte a documentação Citrix para mais detalhes sobre o esquema de nomeação.

5. Clique em **Selecionar** e selecione o **grupo doméstico de computadores clonados** – selecione o grupo estático associado como o grupo doméstico para dispositivos que correspondentes ao padrão de nomeação VDI.

6. Clique em **Adicionar novo** para adicionar mais padrões de nomeação VDI.

7. Clique em **Salvar**.

Para encontrar os computadores marcados como Mestre para clonagem, vá para **Computadores** > clique em **Adicionar filtro** > selecione **Mestre para clonagem** > selecione a caixa de seleção ao lado do filtro **Mestre para clonagem**.

Você pode alterar as configurações do **Mestre para clonagem** posteriormente nos detalhes do computador:

- Ajuste as configurações clicando no ícone de engrenagem no bloco **Virtualização**.
- Remova as configurações clicando em **Virtualização** > **Desmarcar como Mestre para clonagem**.

Solução de problemas

Se você tiver problemas com um clone VDI, execute as etapas de solução de problemas VDI.

ESET Management Implantação do agente

Esta seção descreve todos os métodos disponíveis que você pode usar para implantar o Agente ESET Management nos computadores cliente na sua rede. É muito importante, pois soluções de segurança ESET em execução em computadores cliente comunicam-se com o ESET PROTECT Servidor exclusivamente por meio do Agente.

Adicionar computadores cliente à estrutura do ESET PROTECT

Antes de começar a gerenciar os computadores do cliente na sua rede, você precisa adicioná-los ao ESET PROTECT. Use um dos métodos abaixo para adicionar:

- Sincronização do Active Directory
- Sensor RD
- Adicionar novos dispositivos manualmente

ESET Management Implantação do agente

A implantação do Agente ESET Management pode ser realizada de diferentes maneiras. Você pode implantar o Agente de forma local ou remota:

- Implantação local – instala o Agente ESET Management e o produto de segurança ESET localmente em um computador cliente.

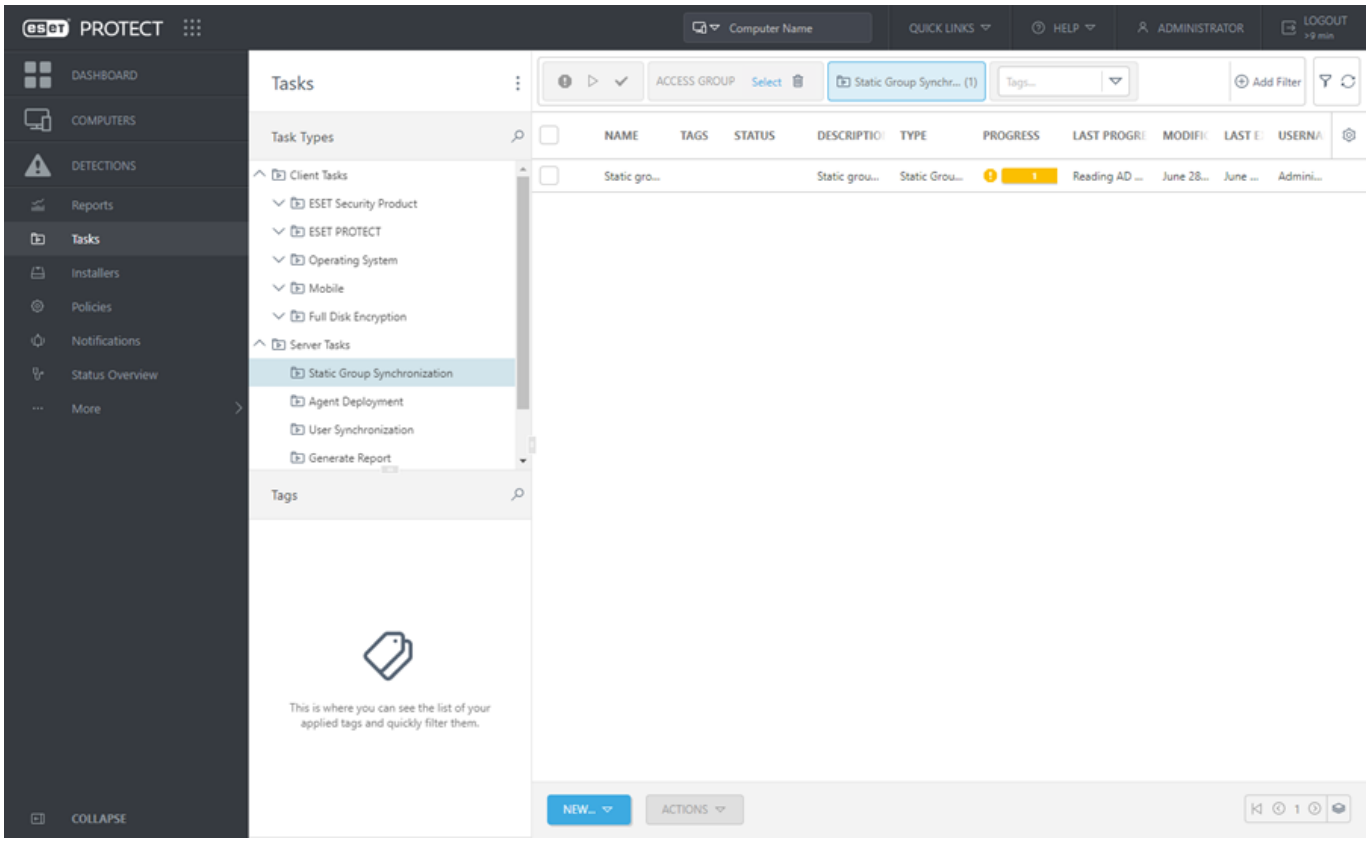
Recomendamos que você use a implantação local apenas se você tiver uma rede pequena (até 50 computadores). Para redes maiores, é possível Implantar o Agente ESET Management usando GPO ou SCCM.

- Implantação remota - recomendamos que você use este método para a implantação do Agente ESET Management em um grande número de computadores do cliente.

Adicionar computadores usando a sincronização do

Active Directory

A sincronização do AD é realizada por meio da execução da tarefa do servidor **Sincronização de grupo estático**. É uma tarefa padrão predefinida que você pode escolher executar automaticamente durante a instalação do ESET PROTECT. Se o computador estiver em um domínio, a sincronização será realizada e computadores do AD serão relacionados em um grupo padrão **Todos**.



Para iniciar o processo de sincronização, clique na tarefa e escolha **Executar agora**.

- Se você precisar criar uma nova tarefa de sincronização do AD, selecione um grupo ao qual deseja adicionar novos computadores a partir do AD.
- Selecione objetos no AD dos quais deseja sincronizar e o que fazer com as duplicatas.
- Insira as configurações de conexão do servidor do AD e defina o Modo de sincronização como **Active Directory/Open Directory/LDAP**. Siga as instruções passo a passo nesse artigo da Base de conhecimento ESET.

> Você pode executar a tarefa do servidor de Implantação do Agente para implantar o Agente ESET Management nos computadores sincronizados do Active Directory.

Adicionar novos dispositivos manualmente

Este recurso permite que você adicione manualmente **Computadores** ou Dispositivos móveis que não são encontrados ou adicionados automaticamente. A guia **Computadores** ou **Grupo** permite a você adicionar novos

computadores ou dispositivos móveis.

1. Para adicionar um novo computador, clique em **Computadores** > **Adicionar dispositivo** e selecione **Computadores** (alternativamente clique no ícone de engrenagem ao lado do **Grupo estático** existente e clique em **Adicionar novo**).

2. **Adicionar computadores** – você pode usar várias opções:

   - Digite o **endereço IP** ou **nome do host** de uma máquina que deseja adicionar e o ESET PROTECT pesquisará por ela na rede. Opcionalmente, insira uma **descrição** dos computadores.

   - **+ Adicionar dispositivo** para adicionar outros dispositivos. Se você quiser excluir o computador da lista de dispositivos, clique no ícone **Lixeira** ou clique em **Remover tudo**.

   - **Importar CSV** para carregar um arquivo *.csv* contendo uma lista de computadores para adicionar. Para mais informações, consulte carregar Importar CSV.

   - **Copiar e colar** uma lista personalizada de computadores separados por delimitadores personalizados. O recurso funciona de forma similar à importação de *.csv*.

3. Clique em **Selecionar marcações** para atribuir marcações.

4. **Grupo principal** - selecione um Grupo principal existente e clique em **OK**.

5. **Utilize a Resolução FQDN**:

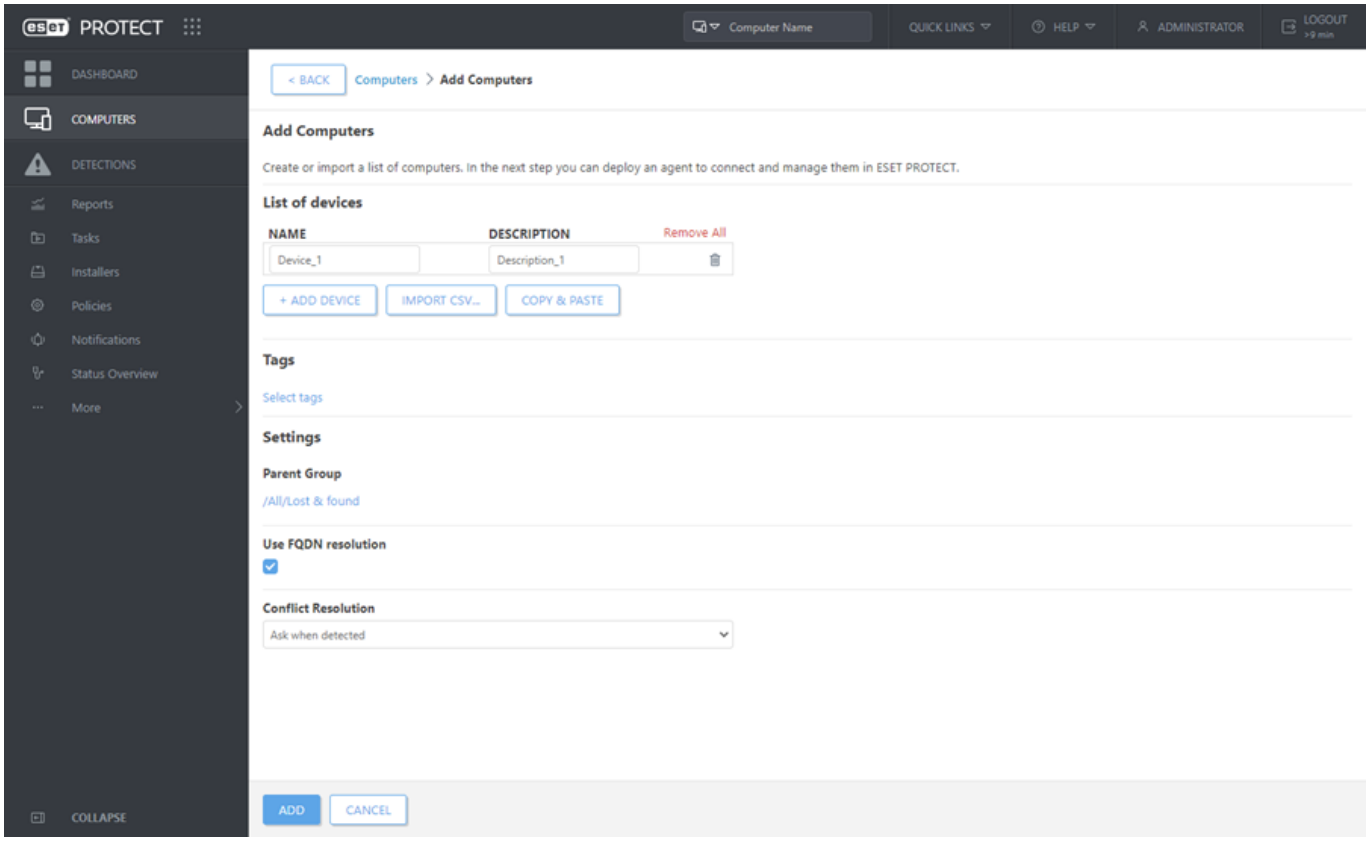
   - Marque a caixa de seleção e o Servidor ESET PROTECT converterá o endereço IP ou nome do host do computador fornecido em um nome de domínio totalmente qualificado.

   - Desmarque a caixa de seleção para importar os nomes de computador fornecidos. Essa opção faz com que a importação em lote de computadores com nomes no formato FQDN (por exemplo, importar de um *.csv*) seja mais rápida.

6. Use o menu suspenso de **Resolução de conflito** para selecionar a ação a ser realizada se um computador sendo adicionado já existir no ESET PROTECT:

   - **Perguntar quando detectado**: Quando um conflito for detectado, o programa pedirá que você selecione uma ação (veja as opções a seguir).
   - **Ignorar dispositivos duplicados:** Computadores duplicados não serão adicionados.
   - **Criar dispositivos duplicados:** Novos computadores serão adicionados, mas com nomes diferentes.
   - **Mover dispositivos duplicados no grupo... :** Computadores em conflito serão movidos para o **Grupo principal**.

7. Clique em **Adicionar** quando tiver concluído as alterações.



Adicionar vários computadores pode ser demorado (pode ser realizada uma busca DNS reversa, confira **Utilize a Resolução FQDN** acima).

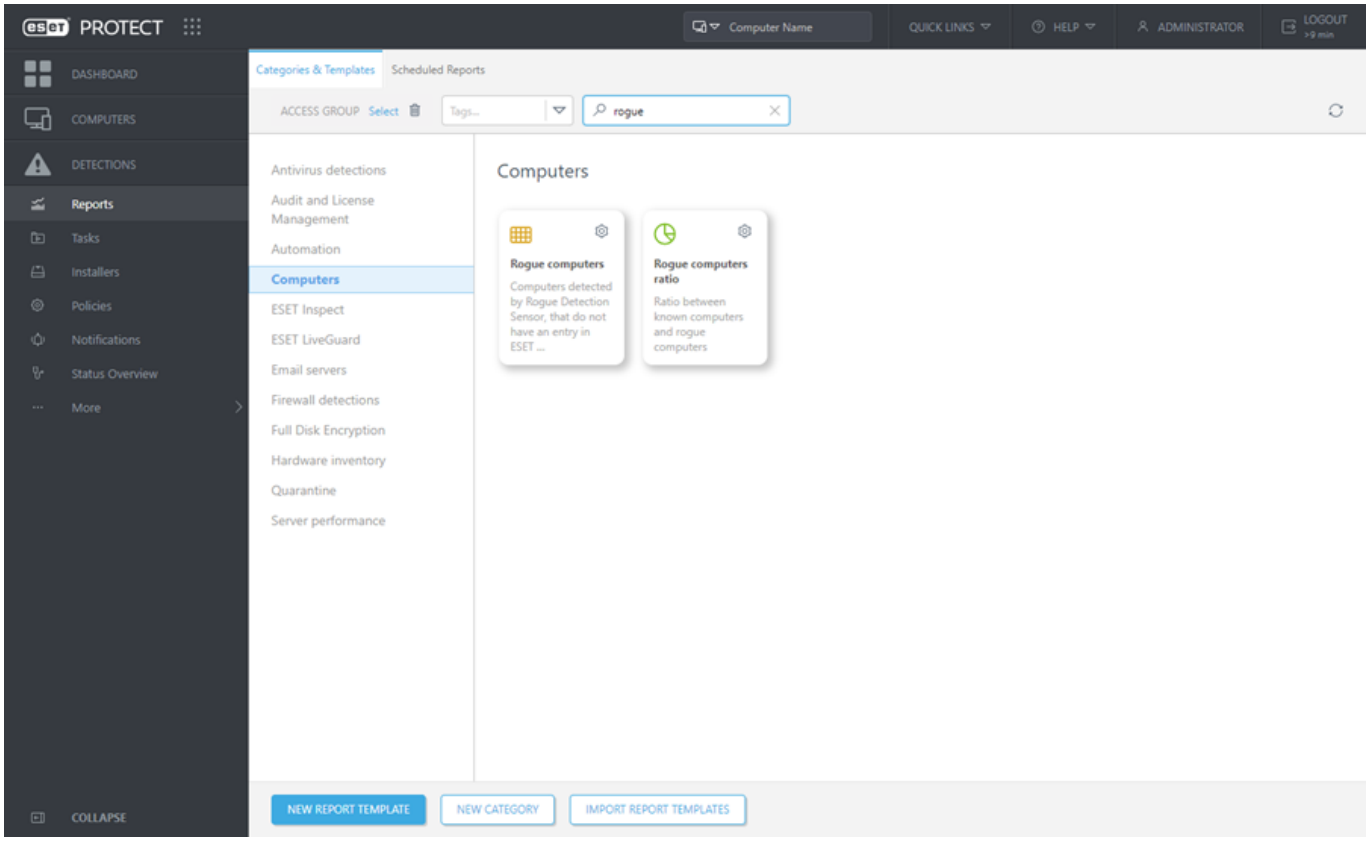
8. Uma janela abrirá com uma lista de dispositivos a serem adicionados. Clique em **OK** ou Implantar agente.

9. Se você clicou em **Implantar Agente**, selecione o sistema operacional e o tipo de implantação do Agente.

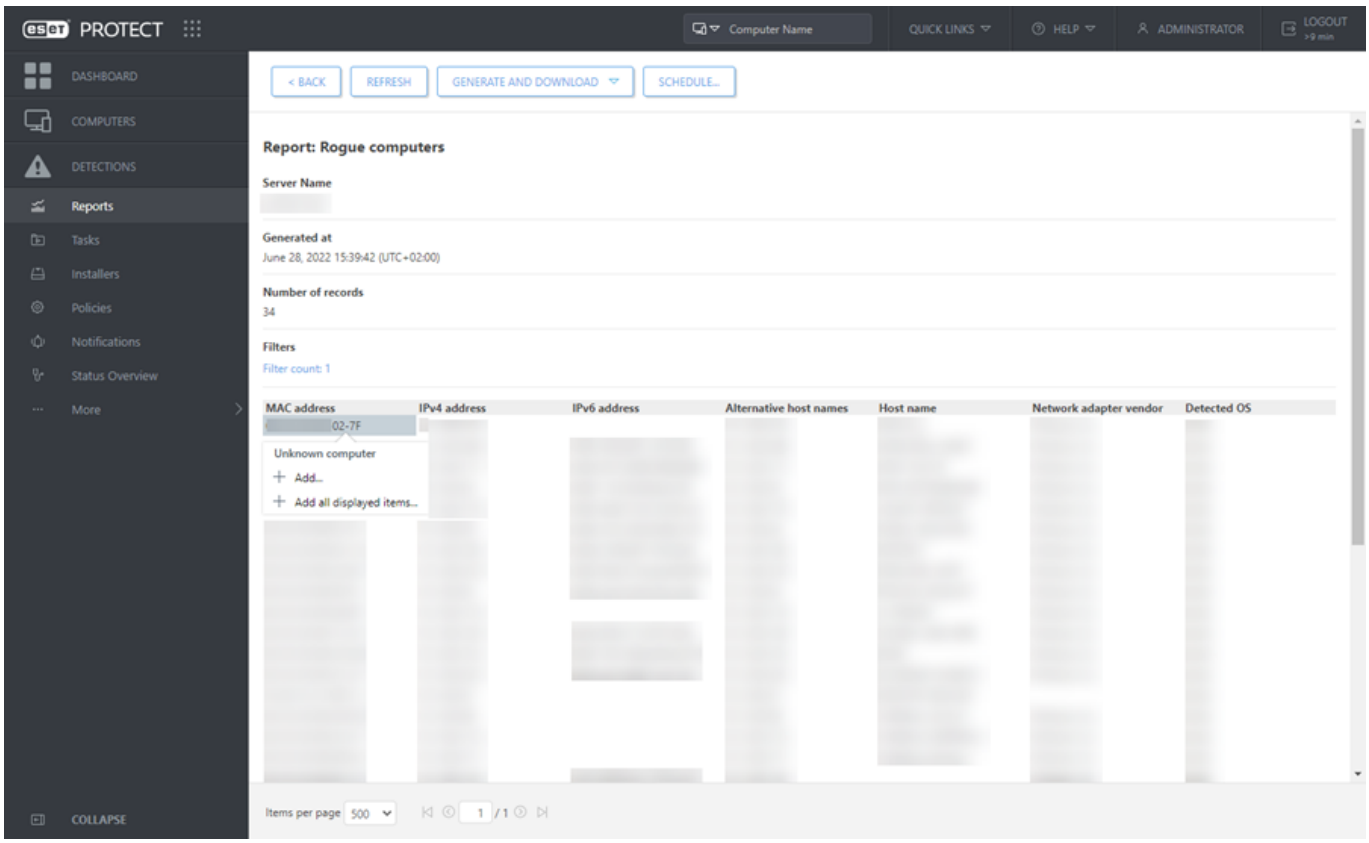
Adicionar computadores usando o RD sensor

Se você não estiver usando a sincronização AD, a forma mais fácil de encontrar um computador não gerenciado em sua estrutura de rede é usar o RD Sensor. O RD Sensor monitora a rede na qual ele está implantado e, quando um novo dispositivo sem um Agente se conecta à rede, ele reporta essas informações para o ESET PROTECT.

Em **Relatórios**, vá para a seção **Computadores** e clique no relatório **Computadores invasores**.



O relatório Computadores invasores lista computadores encontrados pelo RD Sensor. Você pode ajustar as informações reportadas pelo RD Sensor com a política do RD Sensor. Você pode adicionar computadores clicando no computador que deseja Adicionar, ou você pode Adicionar todos os itens exibidos.



Se você estiver adicionando um único computador, você pode usar um nome predefinido ou especificar seu próprio (esse é um nome de exibição que será usado somente no Console da Web ESET PROTECT, não um nome de host real).

- Também é possível adicionar uma descrição se quiser. Caso esse computador já exista em seu diretório do ESET PROTECT, você será notificado e poderá decidir o que fazer com a duplicata. As opções disponíveis são: **Implantar Agente**, **Ignorar**, **Repetir**, **Mover**, **Duplicar** ou **Cancelar**.

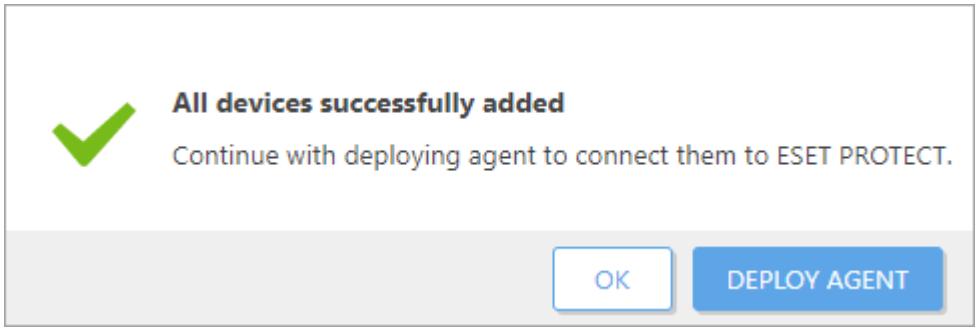
- Assim que o computador for adicionado, uma janela será aberta com uma opção para **Implantar Agente**.

Se você clicar em **Adicionar todos os itens exibidos** uma lista de computadores a serem adicionados à lista será exibida.

1.Clique em ao lado do nome de um computador específico se você não quiser incluí-lo em seu diretório ESET PROTECT nesse momento. Quando tiver concluído a remoção de computadores da lista, clique em **Adicionar**.

2.Selecione a ação a ser realizada quando uma duplicata for encontrada (poderá ocorrer um pequeno atraso dependendo do número de computadores em sua lista): **Ignorar, Tentar novamente, Mover**, **Duplicado** ou **Cancelar**.

3.Uma janela abre com uma opção para **Implantar Agentes** nesses computadores.



Os resultados desse rastreamento do Sensor RD são gravados em um relatório chamado `detectedMachines.log`. Ele contém uma lista de computadores detectados em sua rede. Você pode encontrar o arquivo do `detectedMachines.log` aqui:

- Windows
C:\ProgramData\ESET\Rogue Detection Sensor\Logs\detectedMachines.log

- Linux
/var/log/eset/RogueDetectionSensor/detectedMachines.log

Configurações de política do ESET Rogue Detection Sensor

É possível alterar o comportamento do ESET RD Sensor usando uma política. Isso é usado principalmente para alterar a filtragem de endereços. Você pode, por exemplo, incluir certos endereços na lista de proibições para que eles não sejam detectados.

Clique em **Políticas** e expanda as **Políticas personalizadas para** editar uma política existente para criar uma nova.

Filtros

IPv4 Filtro

Permitir filtragem de endereço IPv4 - Ao permitir a filtragem, somente computadores cujos endereços IP fazem parte da lista de permissões na lista de filtragem IPv4 serão detectados ou somente aqueles que não fazem parte da lista de proibições.

Filtros - Especifique se a lista será uma **Lista de permissões** ou **Lista de proibições**.

Lista de endereços **IPv4** - Clique em Editar lista **IPv4** para adicionar ou remover endereços da lista.

MAC filtro de prefixo de endereço

Permitir a filtragem de prefixo de endereço MAC - Ao permitir a filtragem, somente computadores cujos endereços MAC têm o prefixo (xx:xx:xx) fazem parte da lista de endereços MAC que serão detectados, ou somente aqueles que não fazem parte da lista de proibições.

Modo de filtragem - Especifique se a lista será uma **Lista de permissões** ou **Lista de proibições**.

MAC lista de prefixo do endereço - Clique em **Editar lista de prefixo do MAC** para adicionar ou remover um prefixo da lista.

Detecção

Detecção ativa - Ativar esta opção permitirá que o RD Sensor rastreie a rede local ativamente em busca de computadores. Isso pode melhorar os resultados de busca, mas também pode acionar alertas de firewall em algumas máquinas.

Portas de detecção de SO - O Sensor RD usa uma lista de portas pré-configuradas para rastrear a rede local em busca de computadores. Você pode editar a lista de portas.

Configurações avançadas

Participar do programa de melhoria do produto – ative ou desative o envio de relatórios de travamento se você não concordar em 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).

Atribuir

Especifique os clientes que receberão essa política. Clique em **Atribuir** para exibir todos os grupos estáticos e dinâmicos e seus membros. Selecione o computador no qual você deseja aplicar uma política e clique em **OK**.

Resumo

Verifique as configurações para esta política e clique em **Concluir**.

Implantação local

Este método de implantação é destinado a instalações no local. Criar ou fazer download de um pacote de instalação e permitir o acesso a ele através de uma pasta compartilhada, unidade USB ou email.

O pacote do instalador deve ser instalado por um Administrador ou Usuário com privilégios de Administrador.

Recomendamos que você use a implantação local apenas se você tiver uma rede pequena (até 50 computadores). Para redes maiores, é possível Implantar o Agente ESET Management usando GPO ou SCCM.

A implantação local pode ser realizada de três maneiras:

- Criar instalador do Agente (e produto de segurança ESET) (Apenas Windows)
- Criar instalador de script do Agente (Windows, Linux, macOS)
- Download do Agente do site da ESET (Windows, Linux, macOS)

Implantação local e permissão

Para obter mais informações sobre como permitir que um usuário implemente o Agente ESET Management localmente, siga as instruções neste exemplo.

Tenha em mente que o usuário será capaz de trabalhar com os Certificados ao criar instaladores. Um usuário precisa ter a permissão de **Uso** para **Certificados** com o acesso ao grupo estático onde os certificados estão contidos. Se um usuário quiser implantar um Agente ESET Management, será necessário receber a atribuição de uma permissão de **Uso** para a Autoridade de certificação onde o certificado de servidor real está assinado. Para informações sobre como dividir o acesso a Certificados e Autoridade de certificação, leia este exemplo. Veja a lista de permissões para obter mais informações sobre os direitos de acesso.

Criar instalador do Agente e produto de segurança ESET – Windows

Você pode criar o instalador para o Agente e o produto de segurança ESET para o Windows de várias formas:

- **Links rápidos** > **Implantar agente** > **Windows**
- **Instaladores** > **Criar instalador**
- ESET PROTECT Tour

Clique em **Windows** > **Fazer download do instalador ou usar a ESET Remote Deployment Tool**

O pacote do instalador é um arquivo *.exe* e é válido apenas para o sistema operacional Microsoft Windows.

1.**Distribuição** – Selecionar **Fazer download do instalador ou usar a ESET Remote Deployment Tool**

Se você selecionou outro tipo de instalador, siga as respectivas instruções:
- Implantar primeiro o Agente (instalador de script do Agente)
- Use GPO ou SCCM para implantação

2.**Componentes** – Marque as caixas de seleção entre as seguintes opções:

- **Management Agent** – se você não selecionar outros itens no conteúdo do **Componentes**, o instalador incluirá apenas o Agente ESET Management. Selecione essa opção se quiser instalar o produto de segurança ESET no computador cliente mais tarde, ou se o computador cliente já tem um produto de segurança ESET instalado.

- **Produto de segurança** – Inclua o produto de segurança ESET com o Agente ESET Management. Selecione esta opção se o computador cliente não tiver nenhum produto de segurança ESET instalado e se você quiser instalá-lo com o Agente ESET Management.

- **Criptografia completa de disco** – inclui o ESET Full Disk Encryption no instalador. Essa opção é visível apenas com uma licença ESET Full Disk Encryption ativa.

- **ESET Inspect Conector** – Incluir o Conector ESET Inspect no instalador. Essa opção é visível apenas com uma licença ESET Inspect ativa.

Uma caixa de seleção de produto ESET faltando

Se a caixa de verificação de produto ESET (**Full Disk Encryption** ou **ESET Inspect Conector**) estiver faltando ou for não selecionada automaticamente depois de selecionar o Grupo principal, você não terá a licença do produto ou a licença do produto não será alocada ao site ESET Business Account ou empresa ESET MSP Administrator para a qual você selecionou o Grupo principal, mesmo se você tiver direitos de acesso à licença. Alocar a licença do produto ESET ao site (no ESET Business Account) ou empresa (no ESET MSP Administrator). Em seguida, a caixa de verificação de produto ESET torna-se disponível e você pode incluir o produto ESET no instalador.

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.**Grupo principal** – selecione o Grupo principal onde o Web Console ESET PROTECT vai colocar o computador depois de uma instalação do Agente.

- Você pode selecionar um grupo estático existente ou criar um novo grupo estático ao qual o dispositivo será atribuído depois de usar o instalador.

- Selecionar um Grupo principal vai adicionar todas as políticas aplicadas ao grupo ao instalador.

- Selecionar o Grupo principal não afeta a localização do instalador. Depois de criar o instalador, ele é colocado no Grupo de acesso do usuário atual. O Grupo de acesso define o grupo estático do objeto e o acesso ao objeto com base nos direitos de acesso do usuário.

- O grupo principal é obrigatório se você usar o ESET Business Account com sites ou o ESET MSP Administrator opcional se você usar o ESET Business Account sem sites.

5.**Nome de host do servidor (opcional)** – digite o nome de host do Servidor ESET PROTECT ou endereço IP. Se necessário, especifique o número da **Porta** (o padrão é 2222).

6. **Certificado de mesmo nível**:

- **ESET PROTECT certificado** – um Certificado de mesmo nível para instalação do Agente e a Autoridade de Certificação ESET PROTECT é selecionada automaticamente. Para usar um certificado diferente, clique na **Descrição do certificado ESET PROTECT** para selecionar de um menu suspenso de certificados disponíveis.

- **Certificado personalizado** – se você usar um certificado personalizado para autenticação, clique em **Certificado personalizado** > **Selecionar** e envie o certificado .pfx, e selecione-o ao instalar o Agente. Para obter mais informações, consulte Certificados.

Senha do certificado – digite a senha do certificado se necessário – se você especificou o senha durante a instalação do servidor ESET PROTECT (na etapa na qual criou a Autoridade de certificação) ou se usa um certificado personalizado com uma senha. Caso contrário, deixe o campo **Código de certificado** em branco.

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

Esteja ciente de que é possível extrair o **Código do certificado** pois ele está incorporado no instalador.

7. Personalizar mais configurações

- Digite o **Nome** e a **Descrição do instalador** (opcional).
- **Instalação de componentes** – selecione a caixa de seleção **Sempre instalar a versão mais recente disponível de produtos e componentes** e o instalador sempre vai instalar a versão mais recente dos produtos e componentes selecionados em dispositivos conectados à Internet. Se um dispositivo não tiver acesso à internet, a versão selecionada na próxima etapa deste assistente será instalada. Recomendamos selecionar esta caixa de seleção se quiser usar o instalador por um tempo maior para garantir que você sempre instale a versão mais recente dos produtos e componentes.
- Clique em **Selecionar marcações** para atribuir marcações.
- **Configuração inicial (opcional)** – Use esta opção para aplicar uma política de configuração ao Agente ESET Management. Clique em **Selecionar** em **Configuração do agente** e escolha da lista de políticas disponíveis. Se nenhuma das políticas pré-definidas for adequada, você pode criar uma nova política ou personalizar as existentes.
- Se você usa um Proxy HTTP (recomendamos usar o ESET Bridge), marque a caixa de seleção **Ativar configurações de proxy HTTP** e especifique as configurações de Proxy (**Host**, **Porta**, **Nome de usuário** e **Senha**) para fazer o download do instalador via Proxy e configurar uma conexão do Agente ESET Management com o Proxy, para permitir o encaminhamento de comunicação entre o Agente ESET Management e o ESET PROTECT. Servidor. O campo **Host** é o endereço da máquina executando o Proxy HTTP. O ESET Bridge usa a porta 3128 por padrão. Você pode definir uma porta diferente, se necessário. Certifique-se de definir a mesma porta também na configuração do Proxy HTTP (veja Política ESET Bridge).

  O protocolo de comunicação entre o Agente e o ESET PROTECT Servidor não é compatível com autenticação. Qualquer solução de proxy usada para encaminhar a comunicação do Agente para o ESET PROTECT Servidor que precise de autenticação não funcionará.

A caixa de verificação **Usar conexão direta se o proxy HTTP não estiver disponível** está pré-selecionada. O assistente aplica a configuração como um fallback para o instalador – não é possível desmarcar a caixa de seleção. Você pode desativar a configuração usando uma Política do Agente ESET Management:
- Durante a criação do instalador – inclua a política na **Configuração inicial**.
- Depois da instalação do Agente ESET Management – atribua a política ao computador.

8. Clique em **Concluir** ou **Configuração do produto**.

9. Produto de segurança

a.Clique no produto de segurança ESET pré-selecionado e altere seus detalhes:
oSelecione outro produto de segurança ESET compatível.
o Selecione o idioma no menu suspenso **Idioma**.
oSelecione a caixa de seleção **Avançado**. Por padrão, a versão mais recente está selecionada (recomendado). Você pode selecionar uma versão anterior.

> Se você não ver nenhum arquivo de instalação do produto, certifique-se de definir o repositório como **AUTOSELECT**. Para obter mais informações consulte a seção **Configurações avançadas** das Configurações.

b. Selecione a caixa de seleção ao lado da configuração para ativá-la para o instalador:
oAtivar o sistema de feedback ESET LiveGrid® (recomendado)
oAtivar a detecção de aplicativos potencialmente indesejados – leia mais em nosso artigo da Base de conhecimento.
o**Permitir alterar as configurações de proteção durante a instalação** – recomendamos que você não selecione esta caixa de seleção.

c.Selecione a caixa de seleção **Aceito os termos do Contrato de licença para o usuário final do aplicativo e reconheço a Política de Privacidade**. Consulte o Acordo de Licença para o Usuário Final (EULA), Termos de Uso e Política de Privacidade dos produtos ESET.
d.**Personalizar mais configurações**:
o**Licença**: Selecione a licença de produto adequada na lista de licenças disponíveis. A licença ativará o produto de segurança ESET durante a instalação. A lista de licenças disponíveis não mostra licenças expiradas e usadas em excesso (aquelas no estado **Erro** ou **Obsoleto**). Se você não escolher uma licença, você pode instalar o produto de segurança ESET sem a licença e ativar o produto mais tarde. Você pode adicionar uma licença usando um dos métodos descritos em Gerenciamento de licenças. A adição/remoção da licença é restrita ao Administrador cujo grupo doméstico é **Todos** e que tem a permissão de **Gravação** nas licenças.
o**Configuração** Opcionalmente, você pode selecionar uma **Política** que será aplicada ao produto de segurança ESET durante sua instalação.
o **Executar o ESET AV Remover** – selecione a caixa de seleção para desinstalar ou remover completamente outros programas antivírus no dispositivo de destino.
o**Instalação de módulos** – a opção pode não estar disponível, dependendo do produto de segurança ESET selecionado. Por padrão, o instalador do produto contém apenas os módulos ESET essenciais. Os módulos restantes são baixados durante a primeira inicialização do produto. Selecione a caixa de seleção **Usar o instalador do produto de segurança com um conjunto completo de módulos ESET** para criar o instalador com todos os módulos (para implantações off-line).

Se você selecionou Full Disk Encryption ou Conector ESET Inspect na etapa 2, também é possível alterar as configurações.

Criptografia completa de disco

a.Clique no **ESET Full Disk Encryption** pré-selecionado e altere seus detalhes:
o Selecione o idioma no menu suspenso **Idioma**.
oSelecione a caixa de seleção **Avançado**. Por padrão, a versão mais recente está selecionada (recomendado). Você pode selecionar uma versão anterior.
b.Selecione a caixa de seleção **Aceito os termos do Contrato de licença para o usuário final do aplicativo e reconheço a Política de Privacidade**. Consulte o Acordo de Licença para o Usuário Final (EULA), Termos de Uso e Política de Privacidade dos produtos ESET.
c.**Configuração** – selecione uma política que será aplicada no ESET Full Disk Encryption durante sua instalação.
d.**Personalizar mais configurações**:
o**Licença**: Selecione a licença de produto adequada na lista de licenças disponíveis. A licença ativará o produto de segurança ESET durante a instalação. A lista de licenças disponíveis não mostra licenças expiradas e usadas em excesso (aquelas no estado **Erro** ou **Obsoleto**). Se você não escolher uma licença, você pode instalar o produto de segurança ESET sem a licença e ativar o produto mais tarde. Você pode adicionar uma licença usando um dos métodos descritos em Gerenciamento de licenças. A adição/remoção da licença é restrita ao Administrador cujo grupo doméstico é **Todos** e que tem a permissão de **Gravação** nas licenças.

ESET Inspect Connector

> Requisitos do Conector ESET Inspect:
> • Você deve ter uma licença ESET Inspect para ativar o Conector ESET Inspect.
> • Um produto de segurança ESET compatível instalado no computador gerenciado.

a.Clique no Conector **ESET Inspect pré-selecionado para** alterar seus detalhes:
o Selecione o idioma no menu suspenso **Idioma**.
oSelecione a caixa de seleção **Avançado**. Por padrão, a versão mais recente está selecionada (recomendado). Você pode selecionar uma versão anterior.

b.Selecione a caixa de seleção **Aceito os termos do Contrato de licença para o usuário final do aplicativo e reconheço a Política de Privacidade**. Consulte o Acordo de Licença para o Usuário Final (EULA), Termos de Uso e Política de Privacidade dos produtos ESET.
c.**Personalizar mais configurações**:
o**Licença**: Selecione a licença de produto adequada na lista de licenças disponíveis. A licença ativará o produto de segurança ESET durante a instalação. A lista de licenças disponíveis não mostra licenças expiradas e usadas em excesso (aquelas no estado **Erro** ou **Obsoleto**). Se você não escolher uma licença, você pode instalar o produto de segurança ESET sem a licença e ativar o produto mais tarde. Você pode adicionar uma licença usando um dos métodos descritos em Gerenciamento de licenças. A adição/remoção da licença é restrita ao Administrador cujo grupo doméstico é **Todos** e que tem a permissão de **Gravação** nas licenças.
o**Configuração** – clique em **Selecionar** para selecionar uma política de Conector ESET Inspect existente ou em **Criar** para criar uma nova política de Conector ESET Inspect. O instalador vai aplicar as configurações de política durante a instalação do Conector ESET Inspect.
oDigite o **nome de host do servidor** ESET Inspect e a **porta** de conexão especificada durante a instalação do servidor ESET Inspect (a porta padrão é 8093).
oSelecione a **Autoridade de Certificação** para conexão com o servidor ESET Inspect.

10. Clique em **Concluir**.

11. Faça o download do pacote de instalação Tudo-em-um gerado. Selecione a versão que deseja implantar:

o**32 bits** (por exemplo, *PROTECT_Installer_x86_en_US.exe*)

o**64 bits** (por exemplo, *PROTECT_Installer_x64_en_US.exe*)

o**ARM64** (por exemplo, *PROTECT_Installer_arm64.exe*) – você não pode instalar a versão x86 ou x64 do Agente ESET Management ou do produto de segurança ESET no Windows ARM64.

Todos os dados baixados do repositório (repositório ESET ou uma imagem de repositório personalizada) são assinados digitalmente pela ESET e o Servidor ESET PROTECT verifica os hashes de arquivo e assinaturas PGP. O Servidor ESET PROTECT gera o Instalador tudo-em-um localmente. Portanto, o Instalador tudo-em-um não está assinado digitalmente, o que pode gerar um aviso de navegador da web durante o download do instalador ou gerar um alerta do sistema operacional e impedir a instalação em sistemas onde instaladores não assinados estão bloqueados.

12. Depois de criar e fazer download do pacote do instalador Tudo-em-um, existem duas opções para implantar o Agente ESET Management:

- Localmente em um computador cliente Execute o arquivo do pacote de instalação em um computador cliente. Ele vai instalar o Agente ESET Management e o produto de segurança ESET no dispositivo e conectar o dispositivo ao ESET PROTECT. O instalador ESET Endpoint Antivirus/Security criado no ESET PROTECT 8.1 e versões posteriores é compatível com o Windows 10 Enterprise para áreas de trabalho virtuais e o modo multi-sessão do Windows 10. Para instruções passo a passo, veja o assistente de configuração. Você pode executar o pacote de instalação em um modo silencioso para ocultar a janela do assistente de configuração.

- Uso da Ferramenta de instalação remota ESET para implantar Agentes ESET Management em vários computadores cliente ao mesmo tempo.

Criar instalador de script do Agente – Windows/Linux/macOS

Esse tipo de implantação do Agente é útil quando as opções de implantação remota e local não são adequadas para você. Você pode distribuir o instalador de script do Agente por e-mail e permitir que o usuário o implante. Você também pode executar o Instalador de script do agente de uma mídia removível (uma unidade USB, por exemplo).

A máquina cliente precisa ter conexão com a Internet para efetuar o download do pacote de instalação do Agente e conectar com o ESET PROTECT.

Você pode criar o instalador de script do Agente para Windows/macOS/Linux de várias formas:

- **Links rápidos** > **Implantar agente**

- **Instaladores** > **Criar instalador** > **Windows/macOS/ Linux** > **Implantar primeiro o Agente (instalador de script do Agente)**

- ESET PROTECT Tour

1. 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).

2. **Grupo principal** – selecione o Grupo principal onde o Web Console ESET PROTECT vai colocar o computador depois de uma instalação do Agente.

- Você pode selecionar um grupo estático existente ou criar um novo grupo estático ao qual o dispositivo será atribuído depois de usar o instalador.
- Selecionar um Grupo principal vai adicionar todas as políticas aplicadas ao grupo ao instalador.
- Selecionar o Grupo principal não afeta a localização do instalador. Depois de criar o instalador, ele é colocado no Grupo de acesso do usuário atual. O Grupo de acesso define o grupo estático do objeto e o acesso ao objeto com base nos direitos de acesso do usuário.
- O grupo principal é obrigatório se você usar o ESET Business Account com sites ou o ESET MSP Administrator opcional se você usar o ESET Business Account sem sites.

3. **Nome de host do servidor (opcional)** – digite o nome de host do Servidor ESET PROTECT ou endereço IP. Se necessário, especifique o número da **Porta** (o padrão é 2222).

4. **Certificado de mesmo nível**:

- **ESET PROTECT certificado** – um Certificado de mesmo nível para instalação do Agente e a Autoridade de Certificação ESET PROTECT é selecionada automaticamente. Para usar um certificado diferente, clique na **Descrição do certificado ESET PROTECT** para selecionar de um menu suspenso de certificados disponíveis.
- **Certificado personalizado** – se você usar um certificado personalizado para autenticação, clique em **Certificado personalizado** > **Selecionar** e envie o certificado .pfx, e selecione-o ao instalar o Agente. Para obter mais informações, consulte Certificados.

Senha do certificado – digite a senha do certificado se necessário – se você especificou o senha durante a instalação do servidor ESET PROTECT (na etapa na qual criou a Autoridade de certificação) ou se usa um certificado personalizado com uma senha. Caso contrário, deixe o campo **Código de certificado** em branco.

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

5. Personalizar mais configurações

- Digite o **Nome** e a **Descrição do instalador** (opcional).
- Clique em **Selecionar marcações** para atribuir marcações.
- **Configuração inicial (opcional)** – Use esta opção para aplicar uma política de configuração ao Agente ESET Management. Clique em **Selecionar** em **Configuração do agente** e escolha da lista de políticas disponíveis. Se nenhuma das políticas pré-definidas for adequada, você pode criar uma nova política ou personalizar as existentes.
- Se você usa um Proxy HTTP (recomendamos usar o ESET Bridge), marque a caixa de seleção **Ativar configurações de proxy HTTP** e especifique as configurações de Proxy (**Host**, **Porta**, **Nome de usuário** e **Senha**) para fazer o download do instalador via Proxy e configurar uma conexão do Agente ESET Management com o Proxy, para permitir o encaminhamento de comunicação entre o Agente ESET Management e o ESET PROTECT. Servidor. O campo **Host** é o endereço da máquina executando o Proxy HTTP. O ESET Bridge usa a porta 3128 por padrão. Você pode definir uma porta diferente, se necessário. Certifique-se de definir a mesma porta também na configuração do Proxy HTTP (veja Política ESET Bridge).

> O protocolo de comunicação entre o Agente e o ESET PROTECT Servidor não é compatível com autenticação. Qualquer solução de proxy usada para encaminhar a comunicação do Agente para o ESET PROTECT Servidor que precise de autenticação não funcionará.

A caixa de verificação **Usar conexão direta se o proxy HTTP não estiver disponível** está pré-selecionada. O assistente aplica a configuração como um fallback para o instalador – não é possível desmarcar a caixa de seleção. Você pode desativar a configuração usando uma Política do Agente ESET Management:
- Durante a criação do instalador – inclua a política na **Configuração inicial**.
- Depois da instalação do Agente ESET Management – atribua a política ao computador.

6. Clique em **Salvar e Fazer download**.

7. Extraia o arquivo do arquivo do download no computador do cliente onde você quer implantar o Agente ESET Management.

8. Execute o script *PROTECTAgentInstaller.bat* (Windows) ou *PROTECTAgentInstaller.sh* (Linux ou macOS) para instalar o Agente. Siga as instruções detalhadas de instalação do Agente:

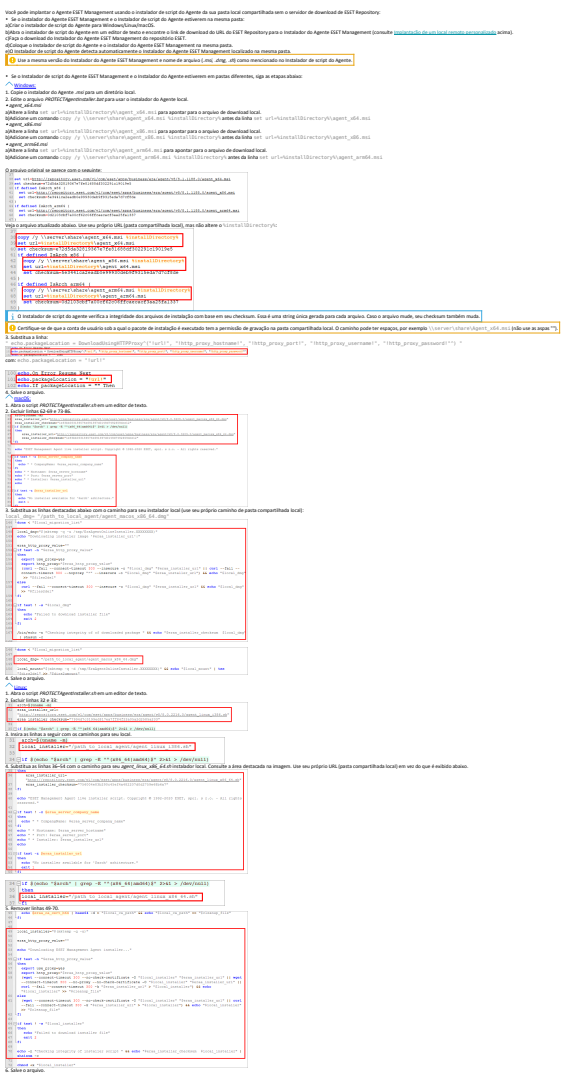
- Implantação do agente – Windows
- Implantação do Agente – Linux
- Implantação do agente – macOS

> O ESET PROTECT é compatível com a atualização automática do Agente ESET Management em computadores gerenciados.

Implantação de um local remoto personalizado

Para implantar o Agente de um local que não seja o repositório ESET, modifique o script de instalação para especificar a nova URL onde o pacote do Agente está localizado. Você também pode usar o endereço IP do novo pacote.
Localize e modifique as linhas a seguir:
Windows:
```
set url=http://repository.eset.com/v1/com/eset/apps/business/era/agent/v9.../agent_x64.msi
set url=http://repository.eset.com/v1/com/eset/apps/business/era/agent/v9.../agent_x86.msi
set url=http://repository.eset.com/v1/com/eset/apps/business/era/agent/v9.../agent_arm64.msi
```
Linux:
```
eraa_installer_url=http://repository.eset.com/v1/com/eset/apps/business/era/agent/v9.../agent-linux-i386.sh
eraa_installer_url=http://repository.eset.com/v1/com/eset/apps/business/era/agent/v9.../agent-linux-x86_64.sh
```
macOS:
```
eraa_installer_url=http://repository.eset.com/v1/com/eset/apps/business/era/agent/v9.../agent_macosx_x86_64.dmg
eraa_installer_url=http://repository.eset.com/v1/com/eset/apps/business/era/agent/v9.../agent-macosx-x86_64_arm64.dmg
```

Implantação de uma pasta local compartilhada



Implantação do agente – Windows

1. Faça o download do Script de instalação do agente para o computador do cliente.

2. Extraia o arquivo *PROTECTAgentinstaller.bat* do arquivo *PROTECTAgentinstaller.zip*.

3. Clique duas vezes no arquivo em lote extraído para instalar o Agente ESET Management.

4. Verifique o arquivo de relatório *status.html* na máquina do cliente localizada no *C:\ProgramData\ESET\RemoteAdministrator\Agent\Logs\status.html* para ter certeza de que o Agente ESET Management está funcionando corretamente.

5. O computador com o Agente instalado vai aparecer no seu Web Console ESET PROTECT, e pode ser gerenciado usando o ESET PROTECT.

- Se houver problemas com o Agente (por exemplo, se ele não estiver conectando ao Servidor ESET PROTECT), consulte a solução de problemas.
- O ESET PROTECT é compatível com a atualização automática do Agente ESET Management em computadores gerenciados.

Implantação do Agente – Linux

Pré-requisitos

- Deve ser possível alcançar o computador da rede.

- Recomendamos que você **use a versão mais recente do OpenSSL1.1.1**. O Servidor/gerenciamento de dispositivo móvel ESET PROTECT não são compatíveis com o OpenSSL 3.x. 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`

- Instale o pacote `lshw` na máquina Linux do cliente/servidor para que o Agente ESET Management reporte 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

Realize a instalação do componente Agente ESET Management no Linux usando um comando no Terminal.

O protocolo de comunicação entre o Agente e o ESET PROTECT Servidor não é compatível com autenticação. Qualquer solução de proxy usada para encaminhar a comunicação do Agente para o ESET PROTECT Servidor que precise de autenticação não funcionará.

Siga as etapas abaixo para instalar o Agente na estação de trabalho Linux.

1. Faça o download do Script de instalação do agente para o computador do cliente.

2. Extraia o arquivo *.sh* do arquivo *.gz*: `tar -xvzf PROTECTAgentInstaller.tar.gz`

3. Defina o arquivo de instalação do Agente ESET Management *.sh* como um executável: `chmod +x PROTECTAgentInstaller.sh`

4. Execute o arquivo *.sh* ou execute o comando Terminal: `sudo ./PROTECTAgentInstaller.sh`

5. Quando solicitado, digite a senha do administrador local e pressione **Enter**.

6. Depois de concluir a instalação do Agente, execute o comando a seguir na janela Terminal para verificar se o Agente está em execução: `sudo systemctl status eraagent`

7. O computador com o Agente instalado vai aparecer no seu Web Console ESET PROTECT, e pode ser gerenciado usando o ESET PROTECT.

Se o computador com o Agente instalado não aparecer no seu ESET PROTECT, execute a solução de problemas.

O ESET PROTECT é compatível com a atualização automática do Agente ESET Management em computadores gerenciados.

Implantação do agente – macOS

1. Faça o download do Script de instalação do agente para o computador do cliente.

2. Clique duas vezes em *PROTECTAgentInstaller.tar.gz* para extrair o arquivo *PROTECTAgentInstaller.sh* para sua área de trabalho.

3. Clique em **Ir** > **Utilitários** e clique duas vezes no Terminal para abrir uma nova janela de Terminal.

4. Na nova janela Terminal, digite os comandos a seguir:

```
cd Desktop

sudo bash PROTECTAgentInstaller.sh
```

5. Quando solicitado, digite a senha da conta de usuário e pressione **Voltar** para continuar a instalação.

6. 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**.

7. Permitir extensões do sistema para seu produto ESET para macOS.

8. Permitir acesso total ao disco:

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.

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 e o produto de segurança ESET à lista de aplicativos na pasta de **Acesso total ao disco**.

e)Bloqueie as configurações no canto inferior esquerdo.

9. O computador com o Agente instalado vai aparecer no seu Web Console ESET PROTECT, e pode ser gerenciado usando o ESET PROTECT.

Um Agente ARM64 ESET Management nativo (versão 9.1 e versões posteriores) será instalado nos sistemas ARM64 macOS.
O ESET PROTECT é compatível com a atualização automática do Agente ESET Management em computadores gerenciados.

Download do Agente do site da ESET

Faça download do pacote de instalação do Agente ESET Management do site da ESET. Selecione o pacote apropriado dependendo do sistema operacional no computador cliente:

- Linux instalação assistida por servidor e off-line
- macOS
- Windows

  - Instalação auxiliada por servidor - usando o pacote de instalação do Agente, este método efetua download de certificados do Servidor ESET PROTECT automaticamente (recomendado para implementação local).

  - Não é possível usar um usuário com autenticação em dois fatores para instalações auxiliadas por servidor.
  - Se você decidir permitir a instalação auxiliada por servidor por outro usuário, certifique-se de que as permissões a seguir estão definidas:
    - O usuário precisa ter permissão de Uso para a Autoridade de certificação que assinou o certificado de mesmo nível daquele servidor e permissão de Uso para pelo menos um certificado de mesmo nível. Se tal certificado não existir, o usuário precisará de permissão de Gravação para criar um novo.
    - **Permissão de Gravação** para o grupo estático onde o usuário quer adicionar o computador.

  - Instalação off-line - usando o pacote de instalação do Agente. Você deve exportar manualmente

certificados e usá-los nesse método de implementação.

Verifique o relatório de status na máquina cliente (localizado em *C:\ProgramData\ESET\RemoteAdministrator\Agent\EraAgentApplicationData\Logs\status.html*) para se certificar de que o Agente ESET Management esteja funcionando corretamente.

> Caso haja problemas com o Agente (por exemplo, não está se conectando com o Servidor ESET PROTECT), consulte a seção Solução de problemas - Implantação do agente.

Implantação remota

> Para implantações remotas, verifique todos os computadores do cliente com uma conexão com a internet.

A instalação remota pode ser realizada das seguintes maneiras:

- ESET Remote Deployment Tool – essa ferramenta permite que você implante pacotes do instalador do Agente ESET Management (e produto de segurança ESET) criados no Web Console ESET PROTECT.
- Objeto de Política de Grupo (GPO) e Gerenciador de Configuração Central de Sistema (SCCM) – Use esta opção para implantação em massa do Agente ESET Management em computadores do cliente.
- Tarefa do servidor Implantação Agente – uma alternativa ao GPO e SCCM.

Caso você tenha problemas com a implementação do Agente ESET Management remotamente (a tarefa do Servidor **Implementação do agente** falhar) consulte a seguir:

- Solução de problemas - Implantação do agente
- Solução de problemas - conexão de Agente
- Exemplo de cenários da implantação do Agente ESET Management

Implantação remota e permissão

Se quiser permitir que o usuário crie instaladores GPO ou scripts SCCM, defina suas permissões para combinarem com nosso exemplo.

As permissões a seguir são necessárias para Implantação de tarefa do servidor do Agente:

- **Permissão de Gravação** para **Grupos e Computadores** onde a implantação é executada
- Permissão de **Uso** para **Certificados** com o acesso ao grupo estático onde os certificados estão contidos
- Permissão de **Uso** para **Implantação do agente** na seção **Acionadores e tarefas do servidor**

Implantação do agente usando GPO ou SCCM

Além da implantação local, também é possível usar ferramentas de gerenciamento como Objeto de política de grupo (GPO), Gerenciador de configuração central de sistema (SCCM), Symantec Altiris ou Puppet para a implantação remota do Agente.

Para implantações remotas, verifique todos os computadores do cliente com uma conexão com a internet.

Use esta opção para implantação em massa do Agente ESET Management em computadores do cliente.

Você pode criar um script GPO/SCCM para implantação do Agente Windows em **Links Rápidos** > **Agente de Implantação** ou **Instaladores** > **Criar Instalador**.

1. Clique em **Windows** > **Use GPO ou SCCM para implantação**

2. 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).

3. **Grupo principal** – selecione o Grupo principal onde o Web Console ESET PROTECT vai colocar o computador depois de uma instalação do Agente.

   - Você pode selecionar um grupo estático existente ou criar um novo grupo estático ao qual o dispositivo será atribuído depois de usar o instalador.

   - Selecionar um Grupo principal vai adicionar todas as políticas aplicadas ao grupo ao instalador.

   - Selecionar o Grupo principal não afeta a localização do instalador. Depois de criar o instalador, ele é colocado no Grupo de acesso do usuário atual. O Grupo de acesso define o grupo estático do objeto e o acesso ao objeto com base nos direitos de acesso do usuário.

   - O grupo principal é obrigatório se você usar o ESET Business Account com sites ou o ESET MSP Administrator opcional se você usar o ESET Business Account sem sites.

4. **Nome de host do servidor (opcional)** – digite o nome de host do Servidor ESET PROTECT ou endereço IP. Se necessário, especifique o número da **Porta** (o padrão é 2222).

5. **Certificado de mesmo nível**:

   - **ESET PROTECT certificado** – um Certificado de mesmo nível para instalação do Agente e a Autoridade de Certificação ESET PROTECT é selecionada automaticamente. Para usar um certificado diferente, clique na **Descrição do certificado ESET PROTECT** para selecionar de um menu suspenso de certificados disponíveis.

   - **Certificado personalizado** – se você usar um certificado personalizado para autenticação, clique em **Certificado personalizado** > **Selecionar** e envie o certificado .pfx, e selecione-o ao instalar o Agente. Para obter mais informações, consulte Certificados.

Senha do certificado – digite a senha do certificado se necessário – se você especificou o senha durante a instalação do servidor ESET PROTECT (na etapa na qual criou a Autoridade de certificação) ou se usa um certificado personalizado com uma senha. Caso contrário, deixe o campo **Código de certificado** em branco.

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

6. Personalizar mais configurações

- Digite o **Nome** e a **Descrição do instalador** (opcional)
- Clique em **Selecionar marcações** para atribuir marcações.
- **Configuração inicial (opcional)** – Use esta opção para aplicar uma política de configuração ao Agente ESET Management. Clique em **Selecionar** em **Configuração do agente** e escolha da lista de políticas disponíveis. Se nenhuma das políticas pré-definidas for adequada, você pode criar uma nova política ou personalizar as existentes.
- Se você usa um Proxy HTTP (recomendamos usar o ESET Bridge), marque a caixa de seleção **Ativar configurações de proxy HTTP** e especifique as configurações de Proxy (**Host**, **Porta**, **Nome de usuário** e **Senha**) para fazer o download do instalador via Proxy e configurar uma conexão do Agente ESET Management com o Proxy, para permitir o encaminhamento de comunicação entre o Agente ESET Management e o ESET PROTECT. Servidor. O campo **Host** é o endereço da máquina executando o Proxy HTTP. O ESET Bridge usa a porta 3128 por padrão. Você pode definir uma porta diferente, se necessário. Certifique-se de definir a mesma porta também na configuração do Proxy HTTP (veja Política ESET Bridge).

  O protocolo de comunicação entre o Agente e o ESET PROTECT Servidor não é compatível com autenticação. Qualquer solução de proxy usada para encaminhar a comunicação do Agente para o ESET PROTECT Servidor que precise de autenticação não funcionará.

  A caixa de verificação **Usar conexão direta se o proxy HTTP não estiver disponível** está pré-selecionada. O assistente aplica a configuração como um fallback para o instalador – não é possível desmarcar a caixa de seleção. Você pode desativar a configuração usando uma Política do Agente ESET Management:
  - Durante a criação do instalador – inclua a política na **Configuração inicial**.
  - Depois da instalação do Agente ESET Management – atribua a política ao computador.

7. Clique em **Concluir**.

8. Faça o download do script GPO/SCCM e dos instaladores do Agente (32-bit, 64-bit, ARM64). Alternativamente, você pode fazer o download dos arquivos do instalador do **Agente** *.msi* na página de download da ESET – seção Instaladores autônomos.

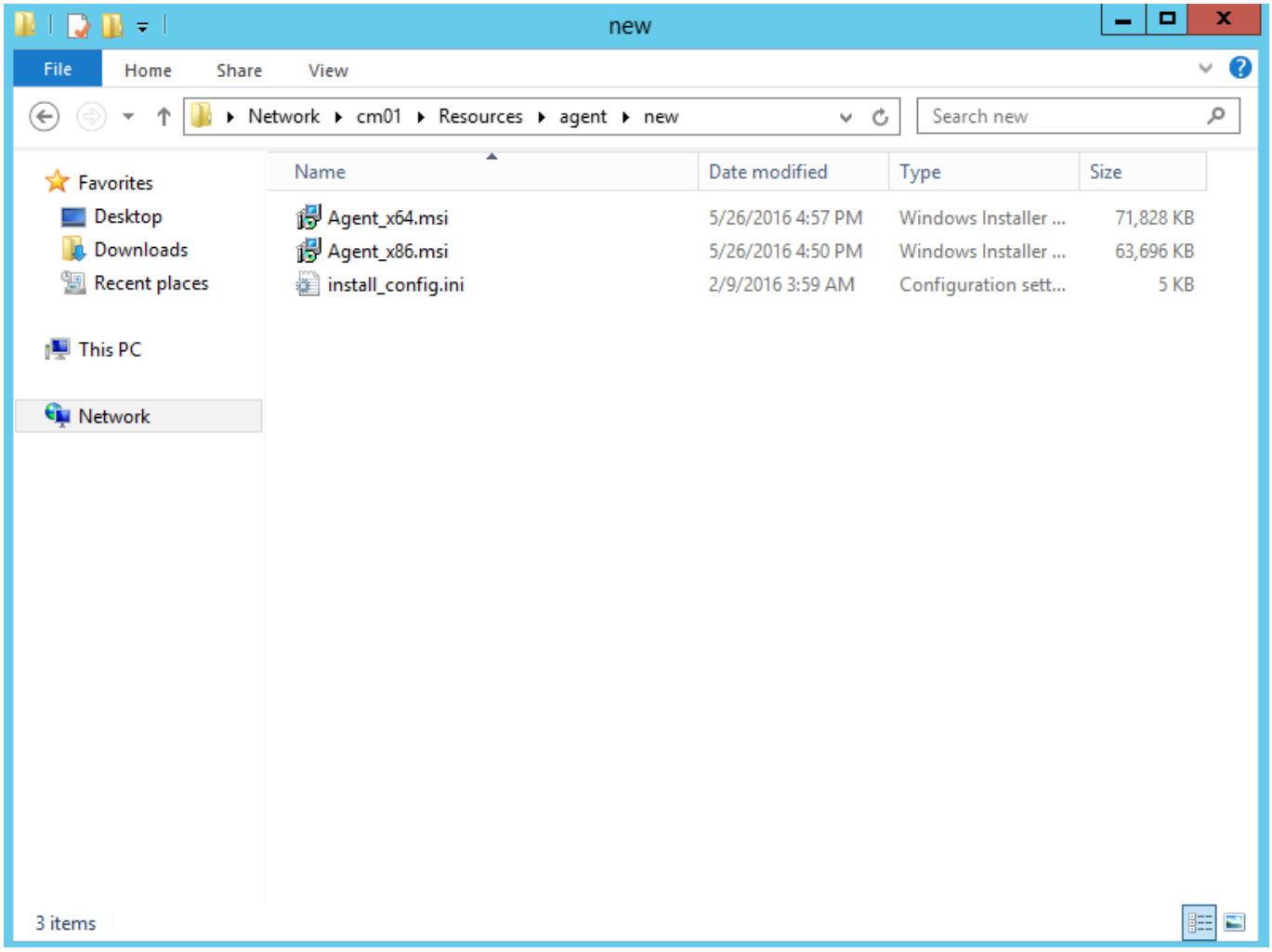
Clique no link adequado abaixo para ver instruções passo-a-passo para dois métodos populares de implantação remota do Agente ESET Management:

- Implantação do Agente ESET Management usando um Objeto de política do grupo (Group Policy Object, GPO) – Esse artigo da Base de conhecimento pode não estar disponível no seu idioma.
- Implantação do Agente ESET Management usando o Gerente de Configuração Central do Sistema (SCCM)

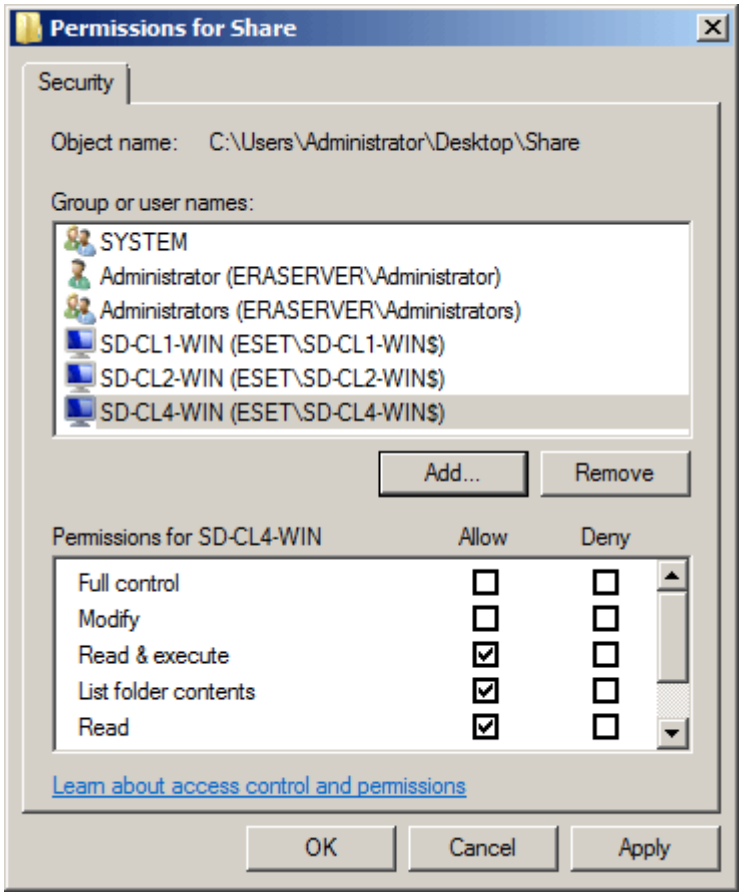
Etapas de implementação - SCCM

Para a implantação do Agente ESET Management usando o SCCM, continue com as etapas a seguir:

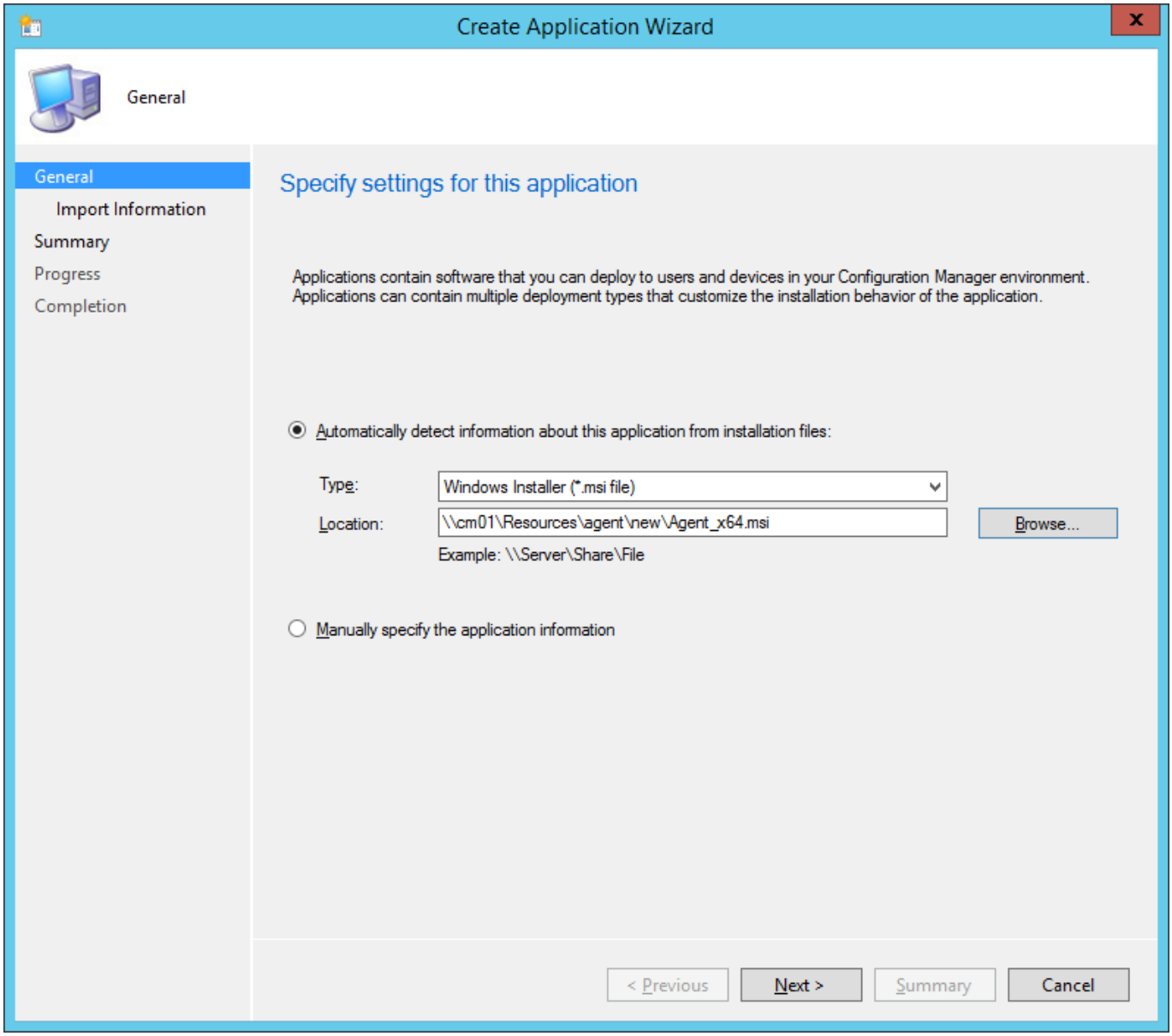
1. Coloque os arquivos *.msi* do instalador do Agente ESET Management e arquivo *install_config.ini* em uma pasta compartilhada.



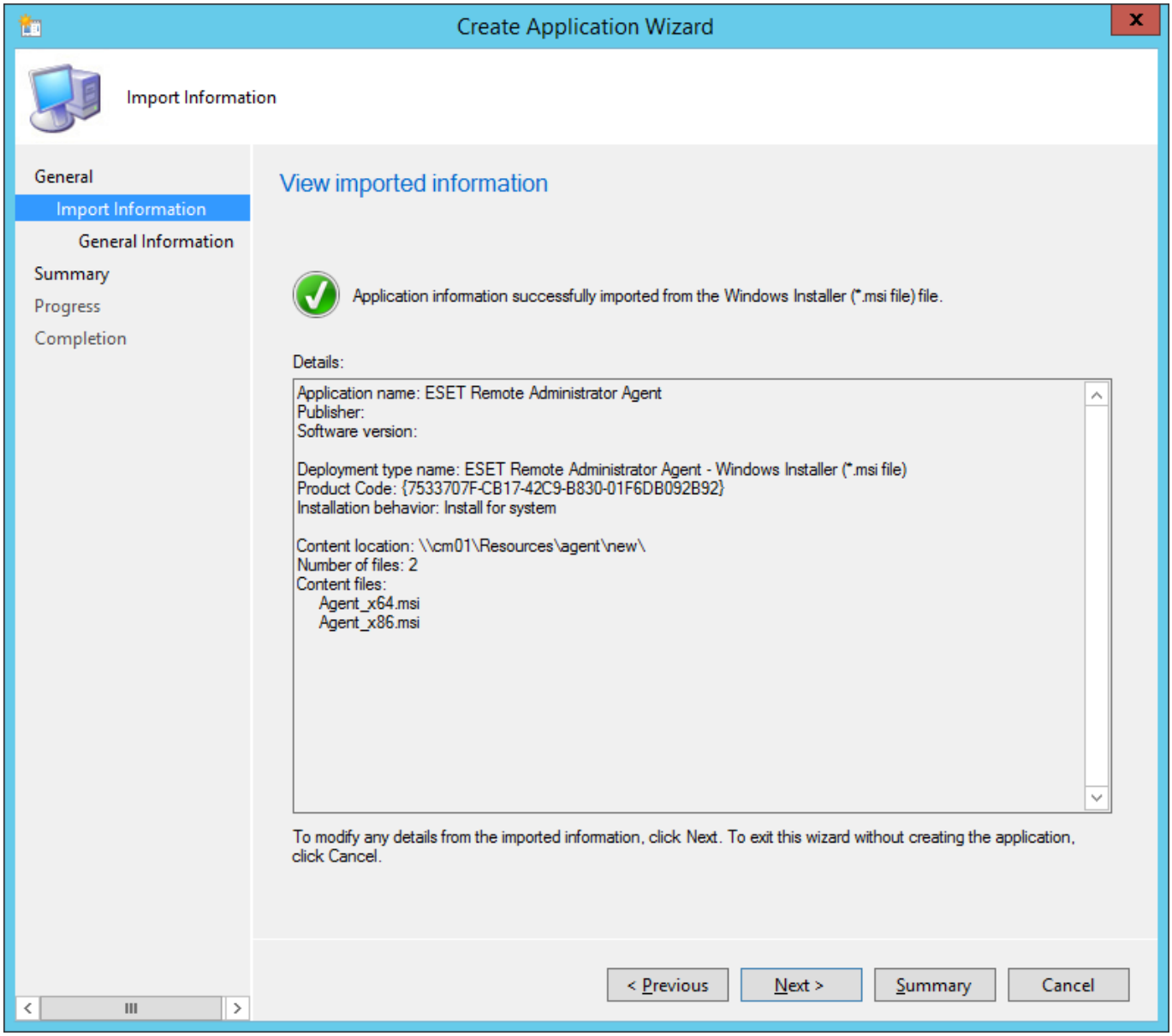
Computadores do cliente vão precisar de acesso de leitura/execução para esta pasta compartilhada.



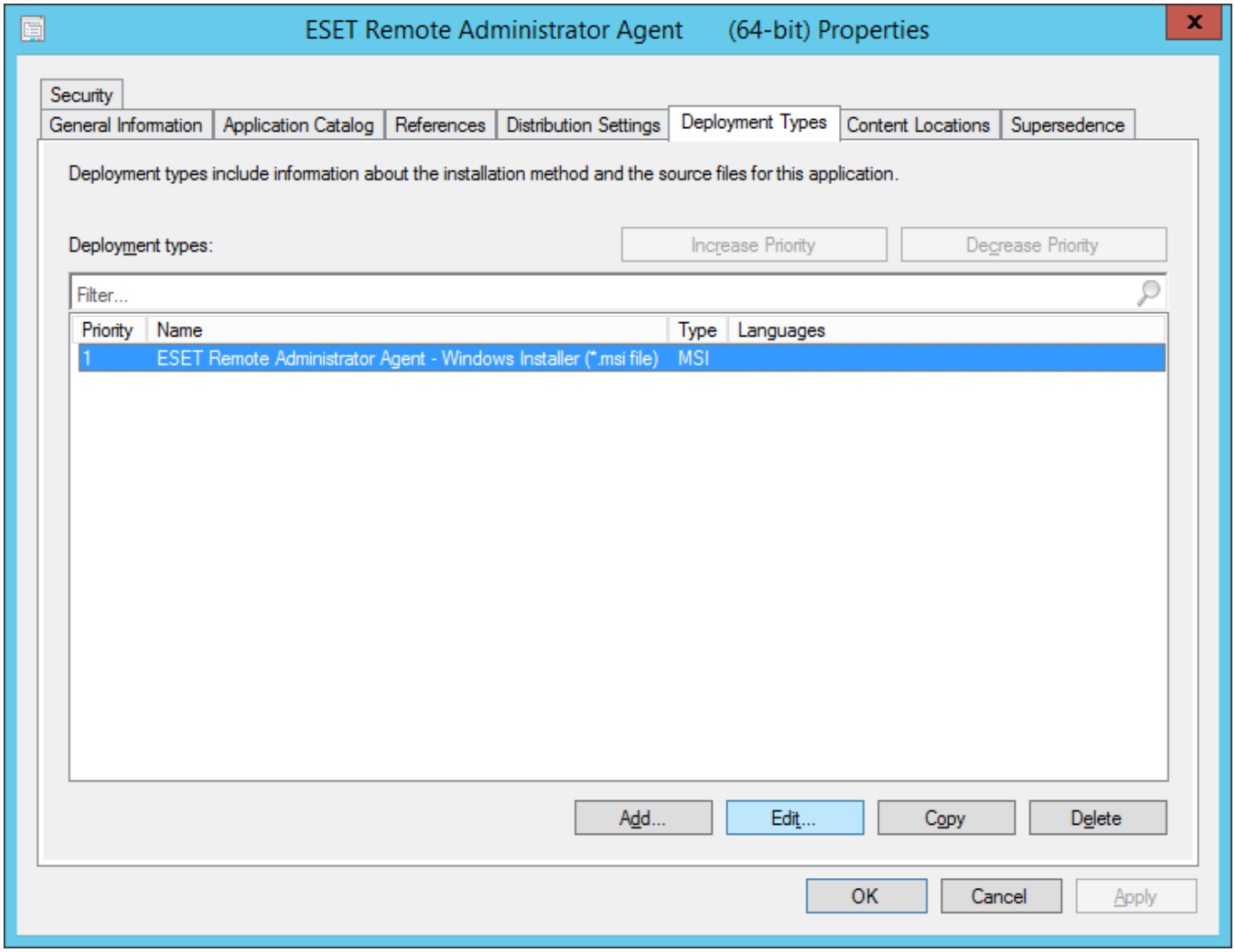
2. Abra o console SCCM e clique em **Biblioteca de software**. Em **Gestão de aplicativo** clique com o botão direito em **Aplicativos** e selecione **Criar aplicativo**. Escolha **Windows Installer (arquivo *.msi)**.



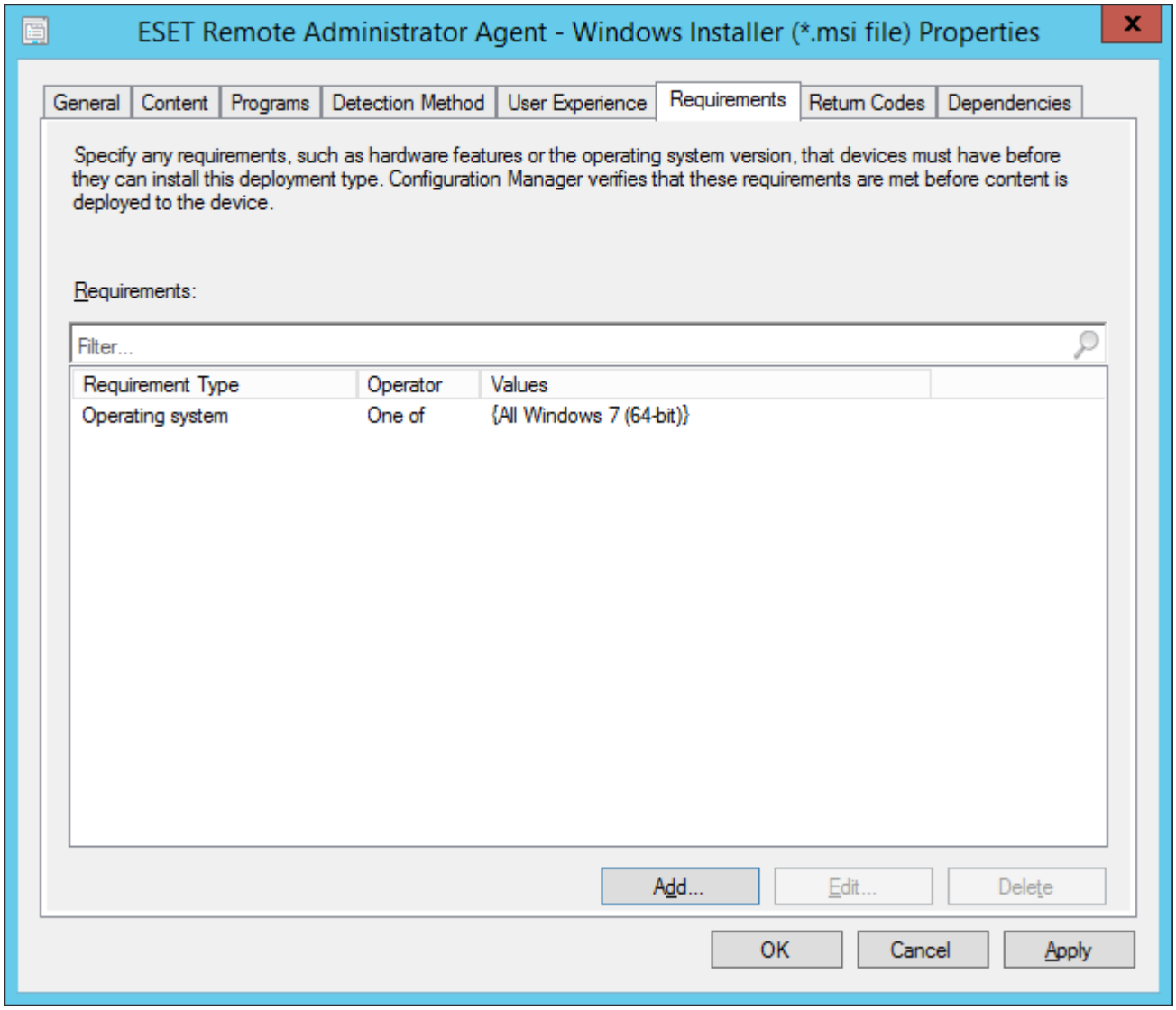
3. Especifique todas as informações necessárias sobre o aplicativo e clique em **Avançar**.

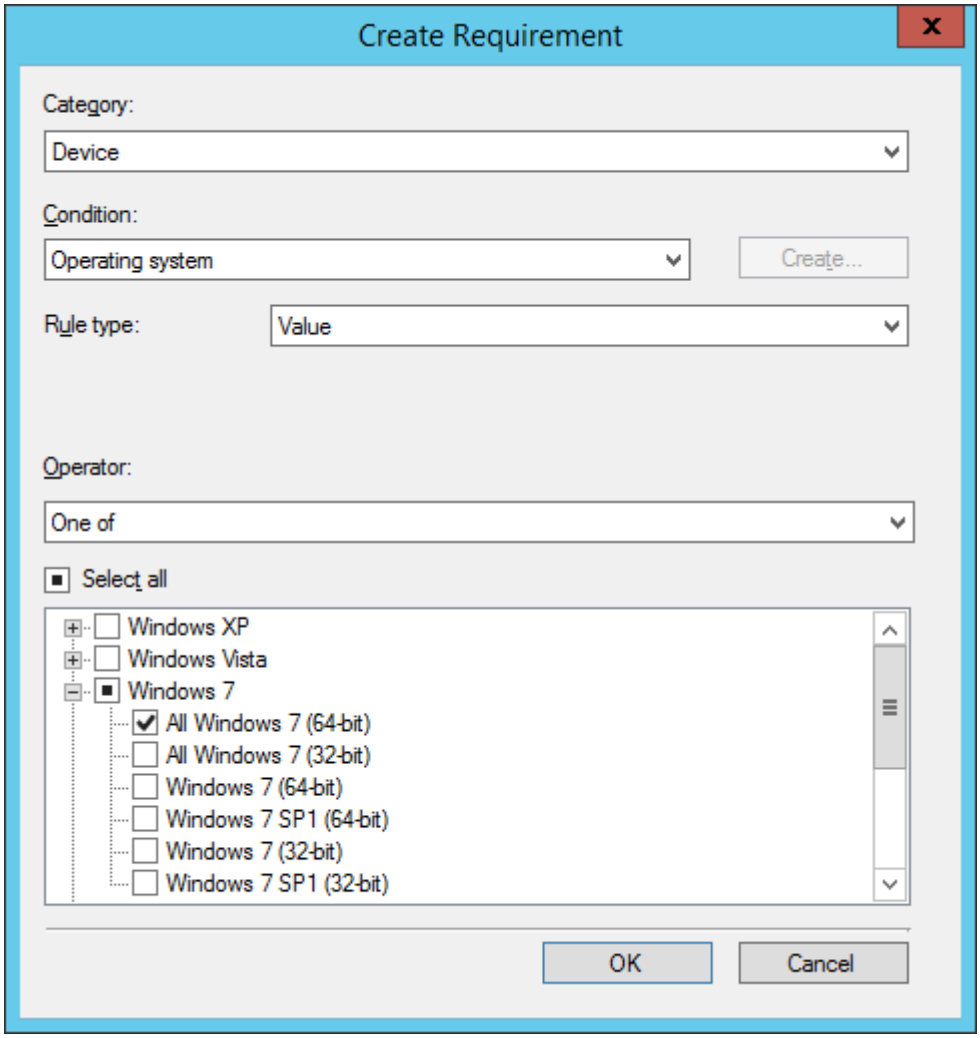


4. Clique com o botão direito no Aplicativo do Agente ESET Management, clique na guia **Tipos de implementação**, selecione a única implementação existente e clique em **Editar**.

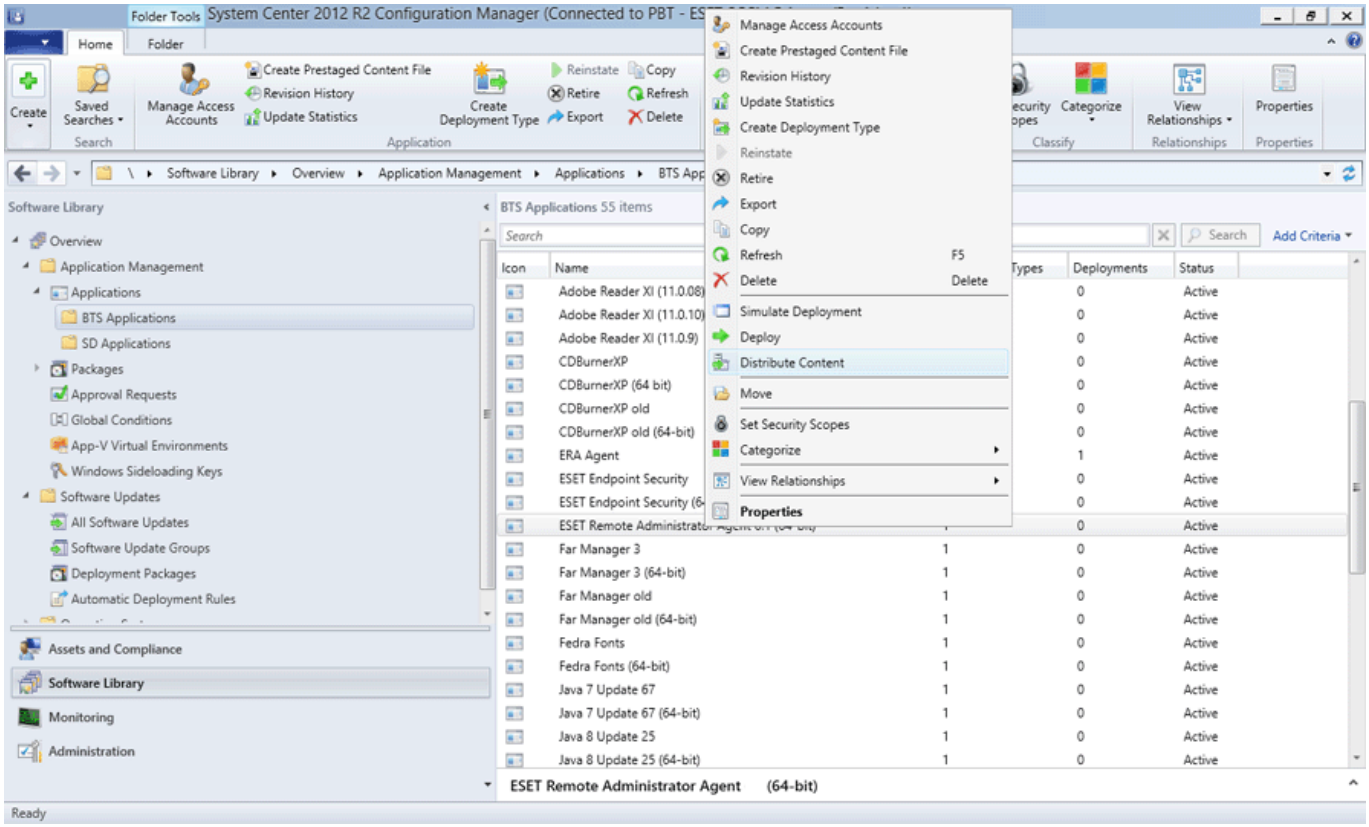


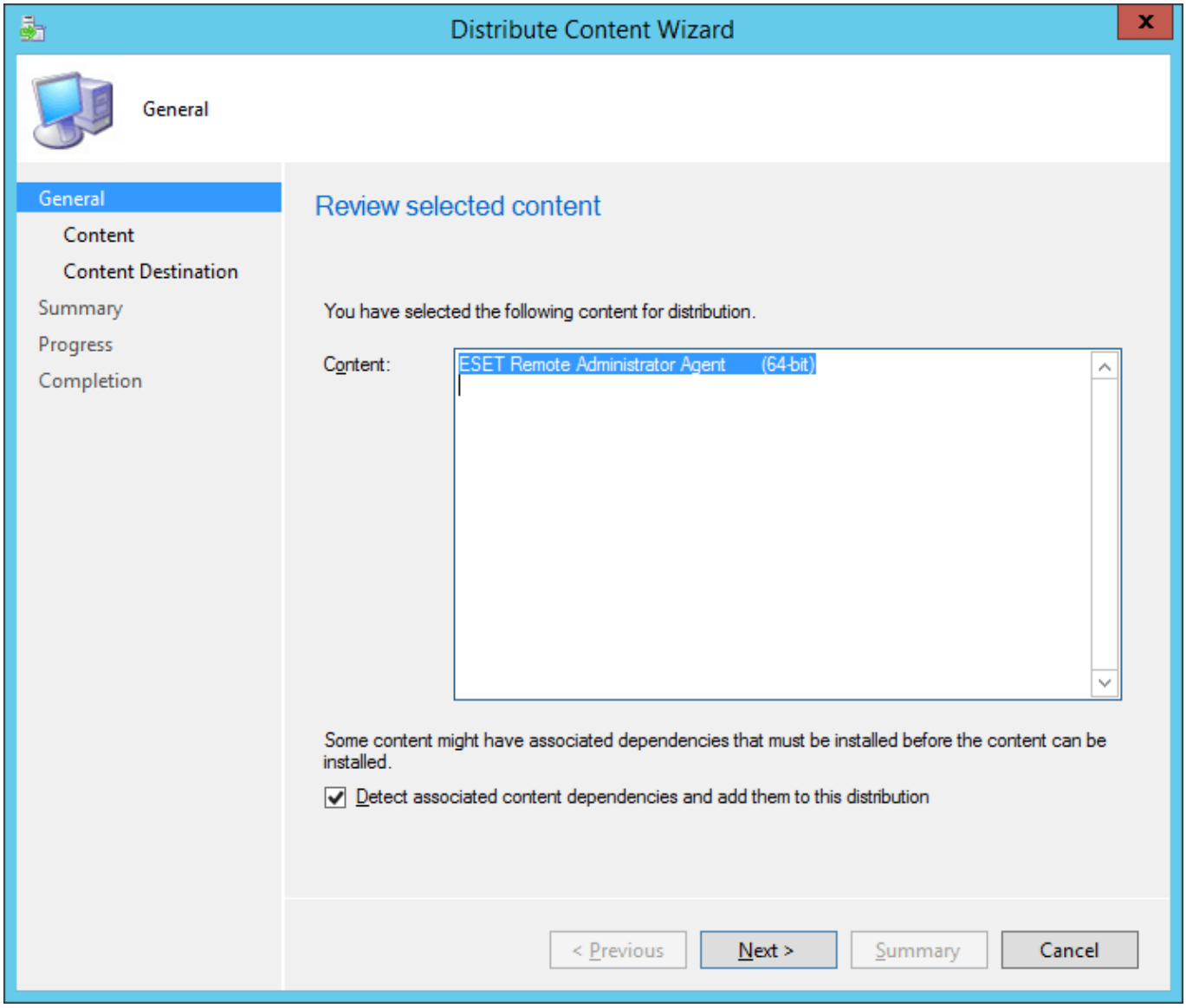
5. Clique na guia **Requisitos** e clique em **Adicionar**. Selecione o **sistema operacional** do menu suspenso **Condição**, selecione **Um** no menu suspenso **Operador** e depois especifique os sistemas operacionais que serão instalados ao marcar as caixas de seleção adequadas. Clique em **OK** quando tiver terminado e em seguida clique em **OK** para fechar qualquer janela restante e salvar suas alterações.

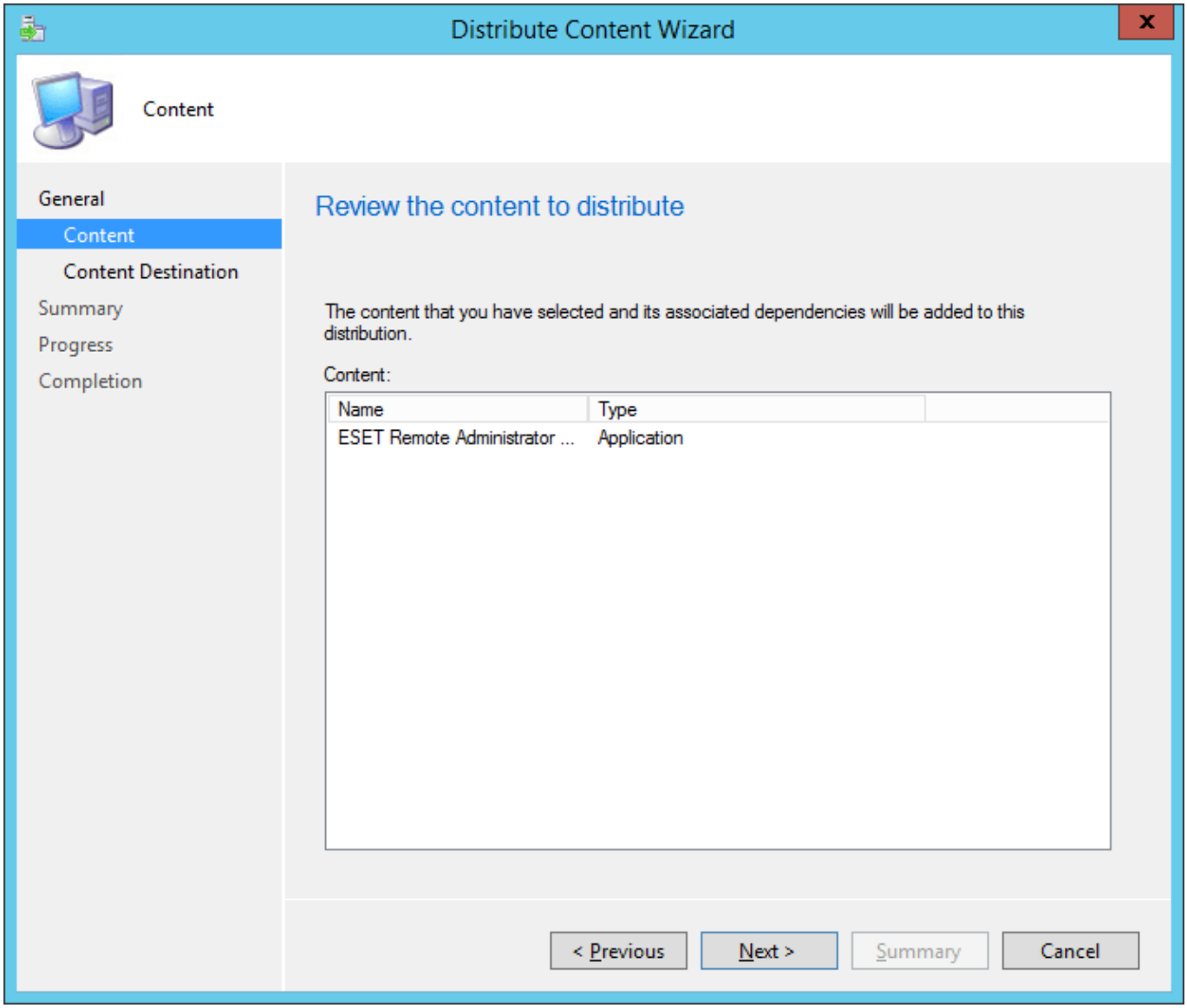

ESET Remote Administrator Agent - Windows Installer (*.msi file) Properties
General
Content
Programs
Detection Method
User Experience
Requirements
Return Codes
Dependencies
Specify any requirements, such as hardware features or the operating system version, that devices must have before they can install this deployment type. Configuration Manager verifies that these requirements are met before content is deployed to the device.
Requirements:
Filter...
Requirement Type
Operator
Values
Operating system
One of
{All Windows 7 (64-bit)}
Add...
Edit...
Delete
OK
Cancel
Apply



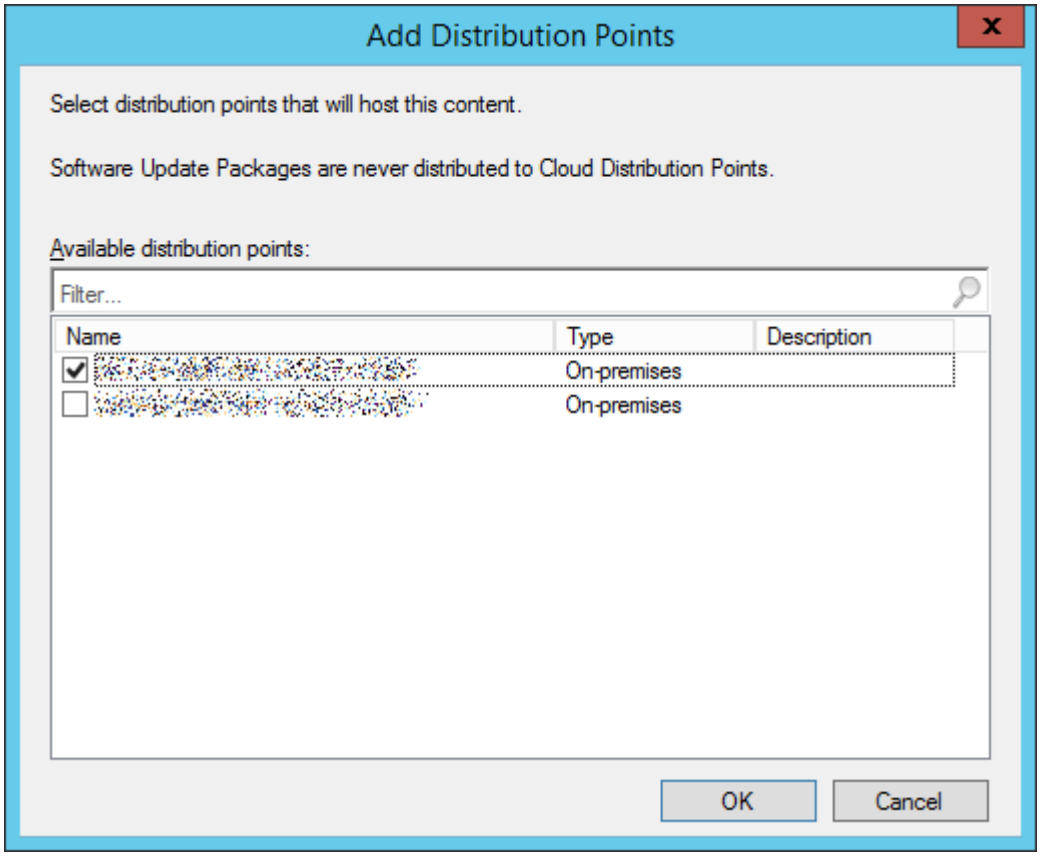
6. Na biblioteca central de software do sistema, clique com o botão direito em seu novo aplicativo e selecione **Distribuir conteúdo** no menu de contexto. Siga as instruções do Assistente de Implementação de Software para concluir a implementação do aplicativo.

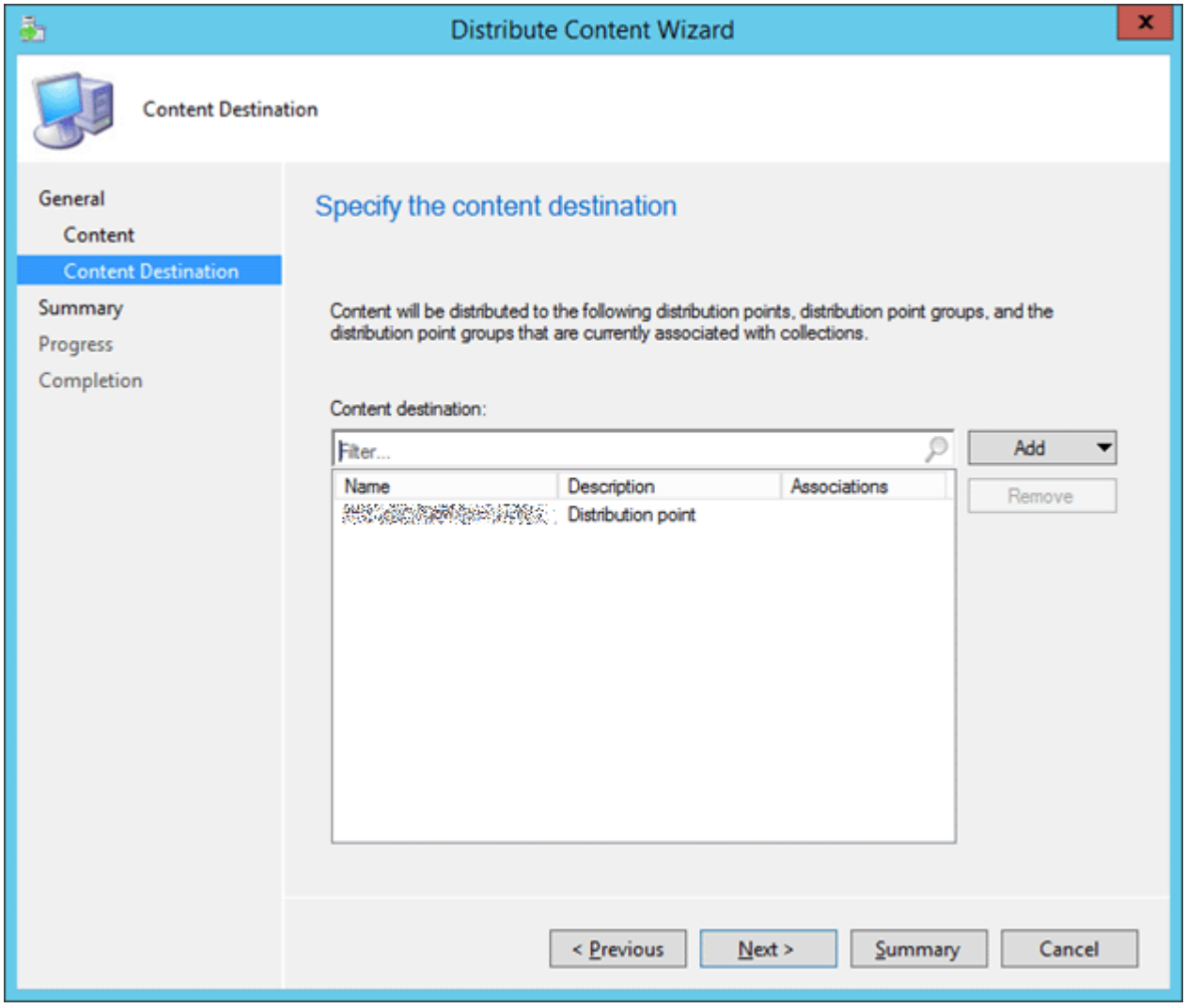

Folder Tools
System Center 2012 R2 Configuration Manager (Connected to PBT - ES
Home
Folder
Create
Saved Searches
Manage Access Accounts
Create Prestaged Content File
Revision History
Update Statistics
Create Deployment Type
Reinstate
Retire
Export
Copy
Refresh
Delete
Search
Application
Classify
Categorize
View Relationships
Properties
Relationships
Properties
Software Library ▸ Overview ▸ Application Management ▸ Applications ▸ BTS App
Software Library
Overview
Application Management
Applications
BTS Applications
SD Applications
Packages
Approval Requests
Global Conditions
App-V Virtual Environments
Windows Sideloading Keys
Software Updates
All Software Updates
Software Update Groups
Deployment Packages
Automatic Deployment Rules
Assets and Compliance
Software Library
Monitoring
Administration
BTS Applications 55 items
Search
Add Criteria
Icon
Name
Types
Deployments
Status
Adobe Reader XI (11.0.08)
Adobe Reader XI (11.0.10)
Adobe Reader XI (11.0.9)
CDBurnerXP
CDBurnerXP (64 bit)
CDBurnerXP old
CDBurnerXP old (64-bit)
ERA Agent
ESET Endpoint Security
ESET Endpoint Security (6
ESET Remote Administrator
Far Manager 3
Far Manager 3 (64-bit)
Far Manager old
Far Manager old (64-bit)
Fedra Fonts
Fedra Fonts (64-bit)
Java 7 Update 67
Java 7 Update 67 (64-bit)
Java 8 Update 25
Java 8 Update 25 (64-bit)
Active
ESET Remote Administrator Agent (64-bit)
Ready
Manage Access Accounts
Create Prestaged Content File
Revision History
Update Statistics
Create Deployment Type
Reinstate
Retire
Export
Copy
Refresh F5
Delete Delete
Simulate Deployment
Deploy
Distribute Content
Move
Set Security Scopes
Categorize
View Relationships
Properties

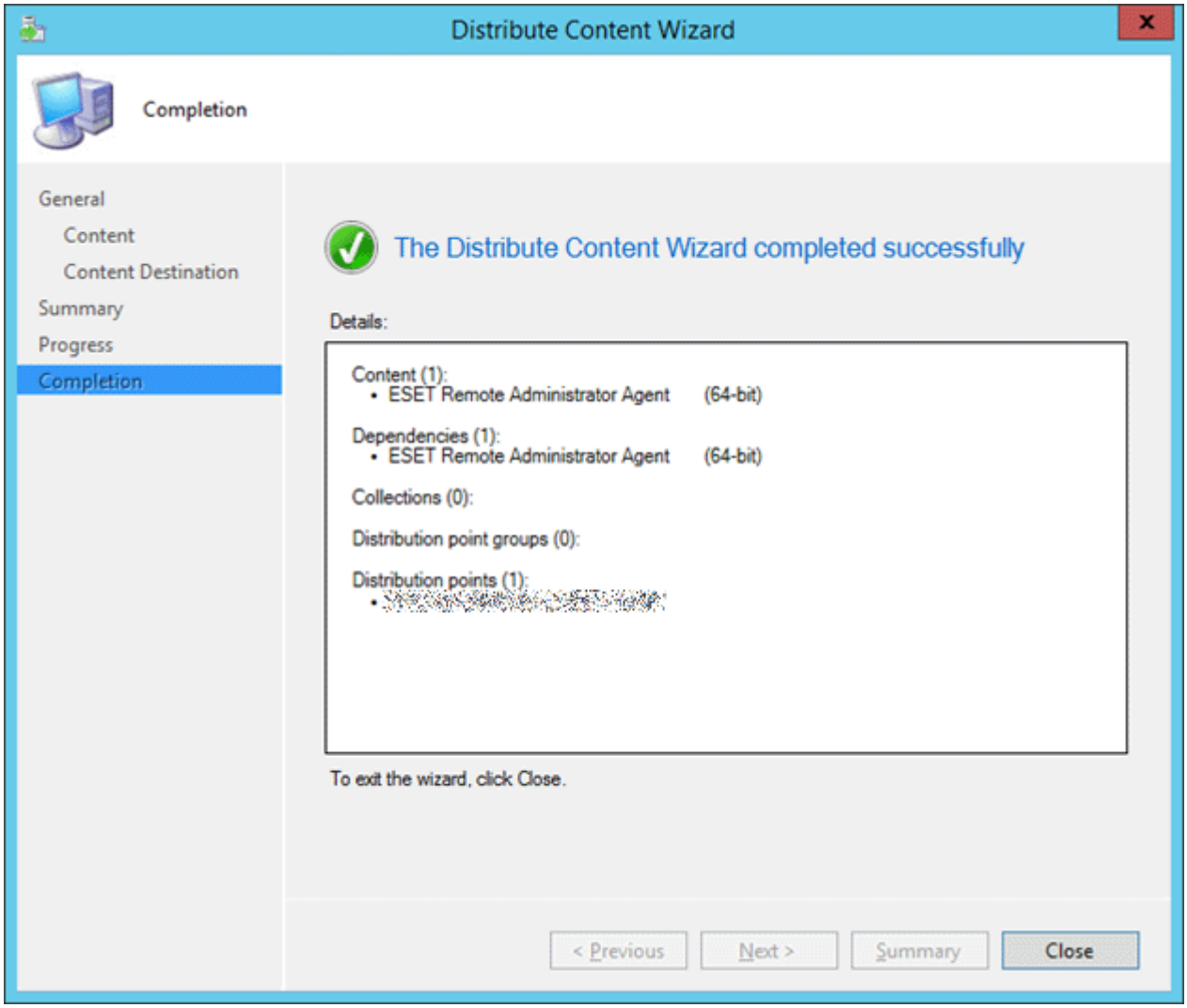

Distribute Content Wizard
General
General
Content
Content Destination
Summary
Progress
Completion
Review selected content
You have selected the following content for distribution.
Content:
ESET Remote Administrator Agent (64-bit)
Some content might have associated dependencies that must be installed before the content can be installed.
Detect associated content dependencies and add them to this distribution
< Previous
Next >
Summary
Cancel

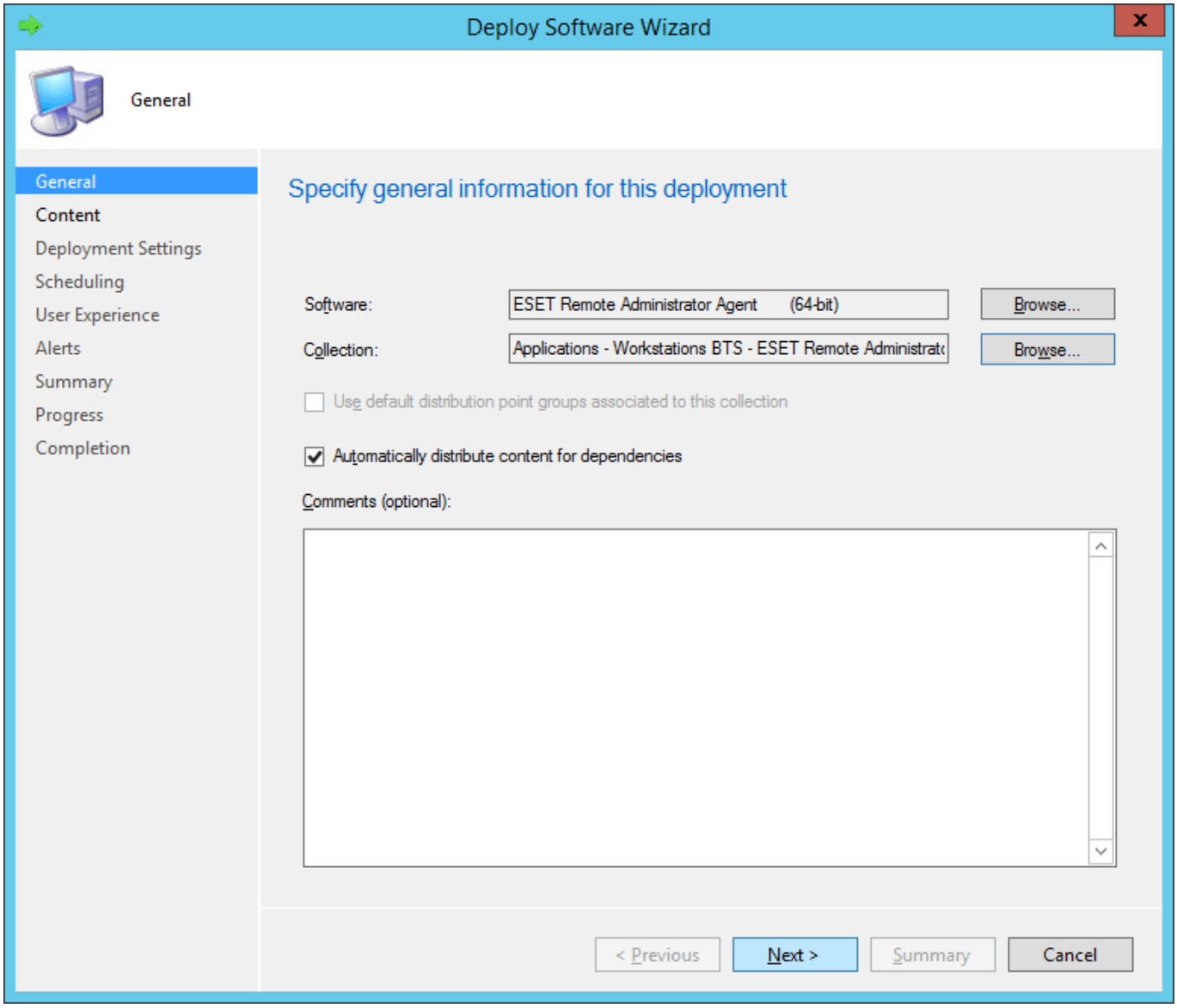


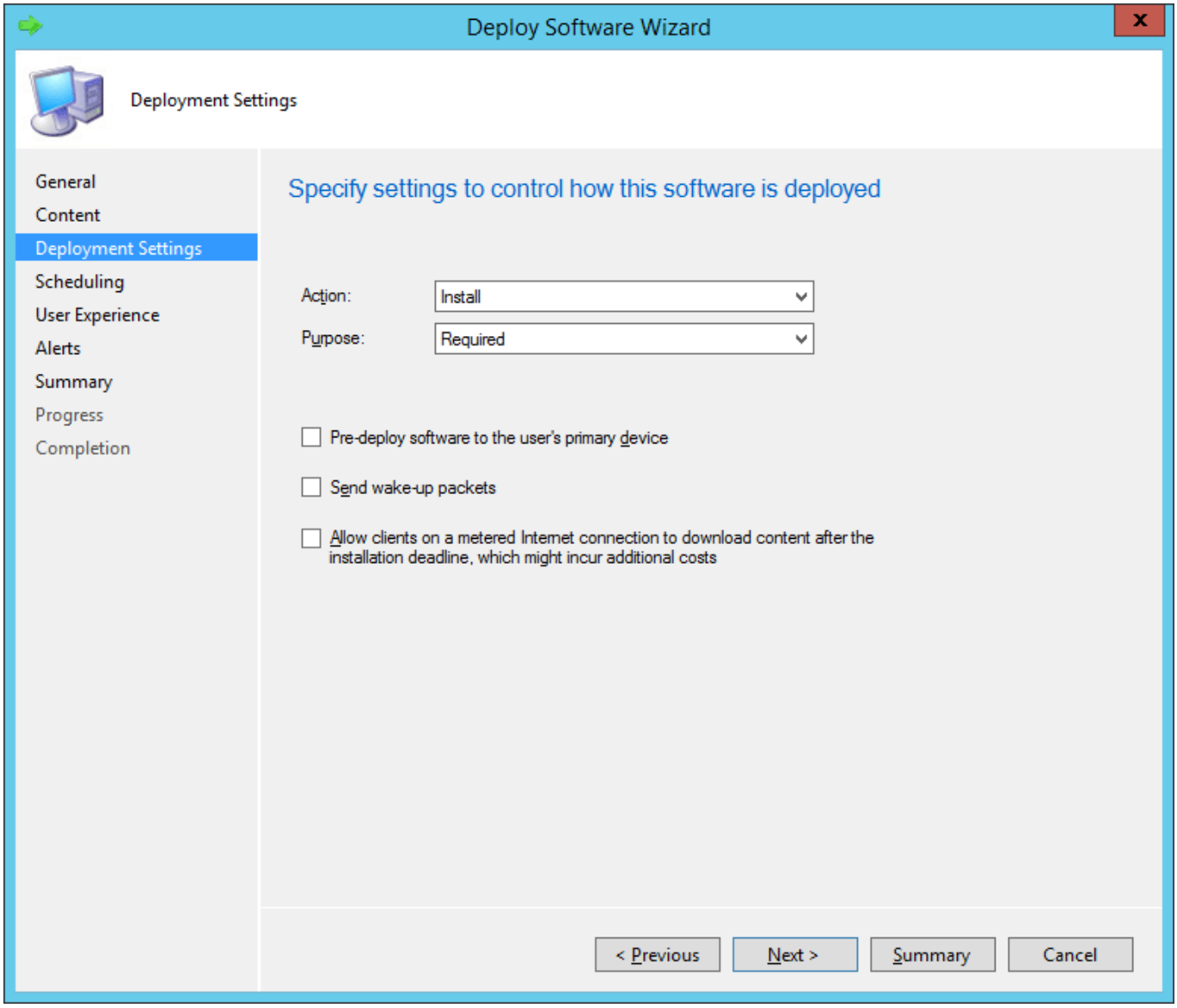
7. Clique com o botão direito no aplicativo e selecione **Implantar**. Siga o assistente e selecione a coleção e o destino para onde deseja implantar o agente.

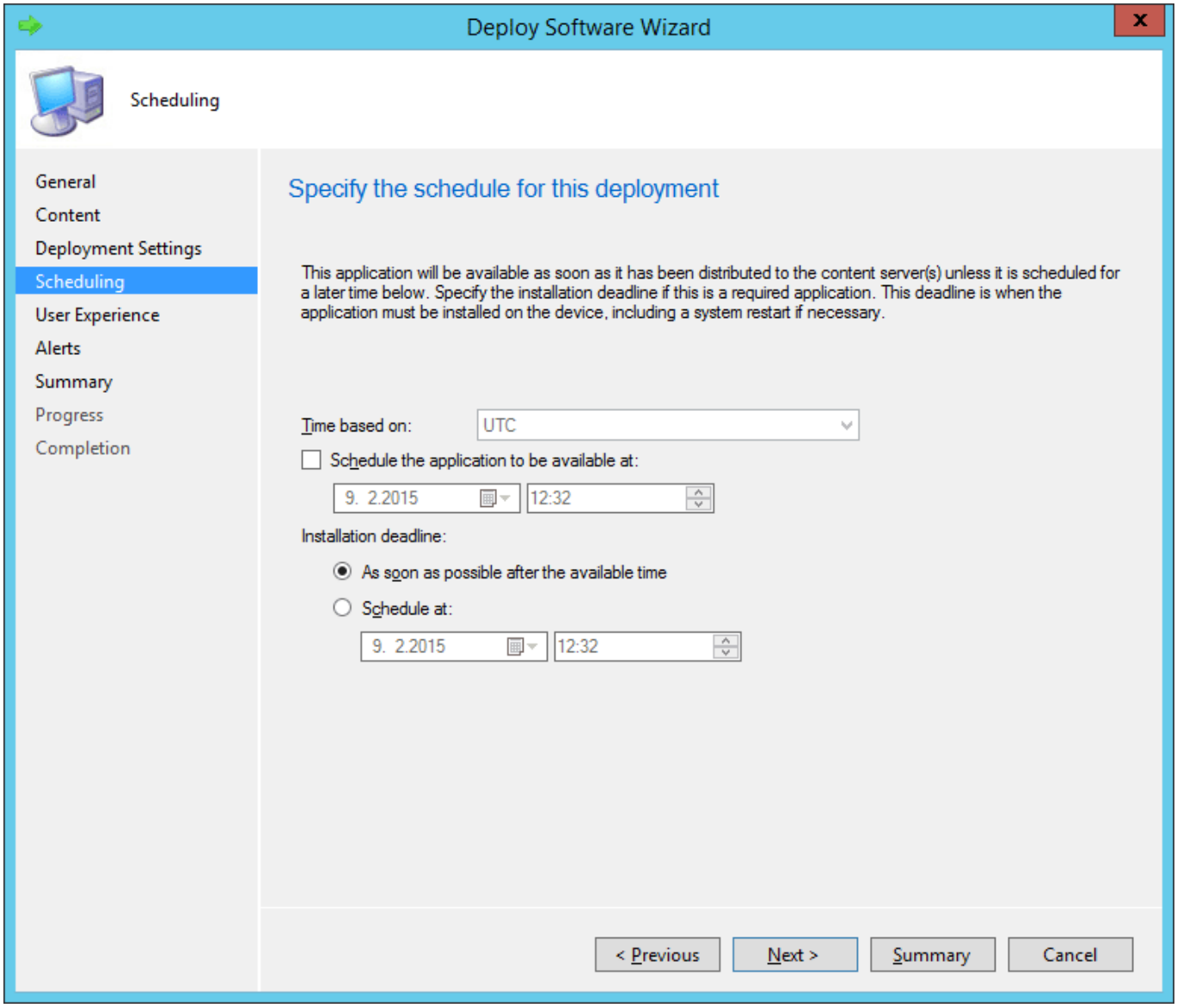

Add Distribution Points
Select distribution points that will host this content.
Software Update Packages are never distributed to Cloud Distribution Points.
Available distribution points:
Filter...
Name
Type
Description
On-premises
On-premises
OK
Cancel

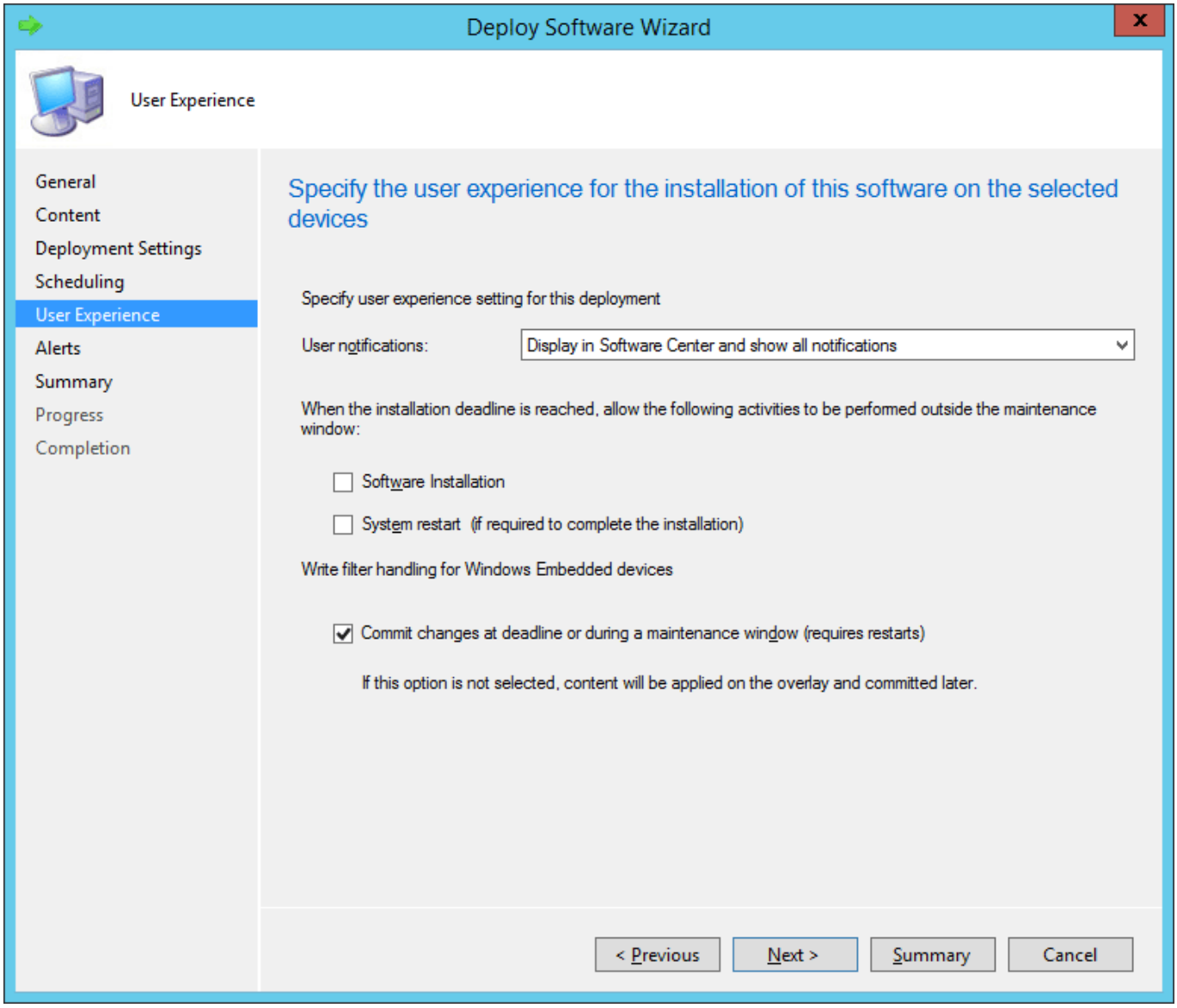

Distribute Content Wizard
Content Destination
General
Content
Content Destination
Summary
Progress
Completion
Specify the content destination
Content will be distributed to the following distribution points, distribution point groups, and the distribution point groups that are currently associated with collections.
Content destination:
Filter...
Add
Remove
Name
Description
Associations
Distribution point
< Previous
Next >
Summary
Cancel

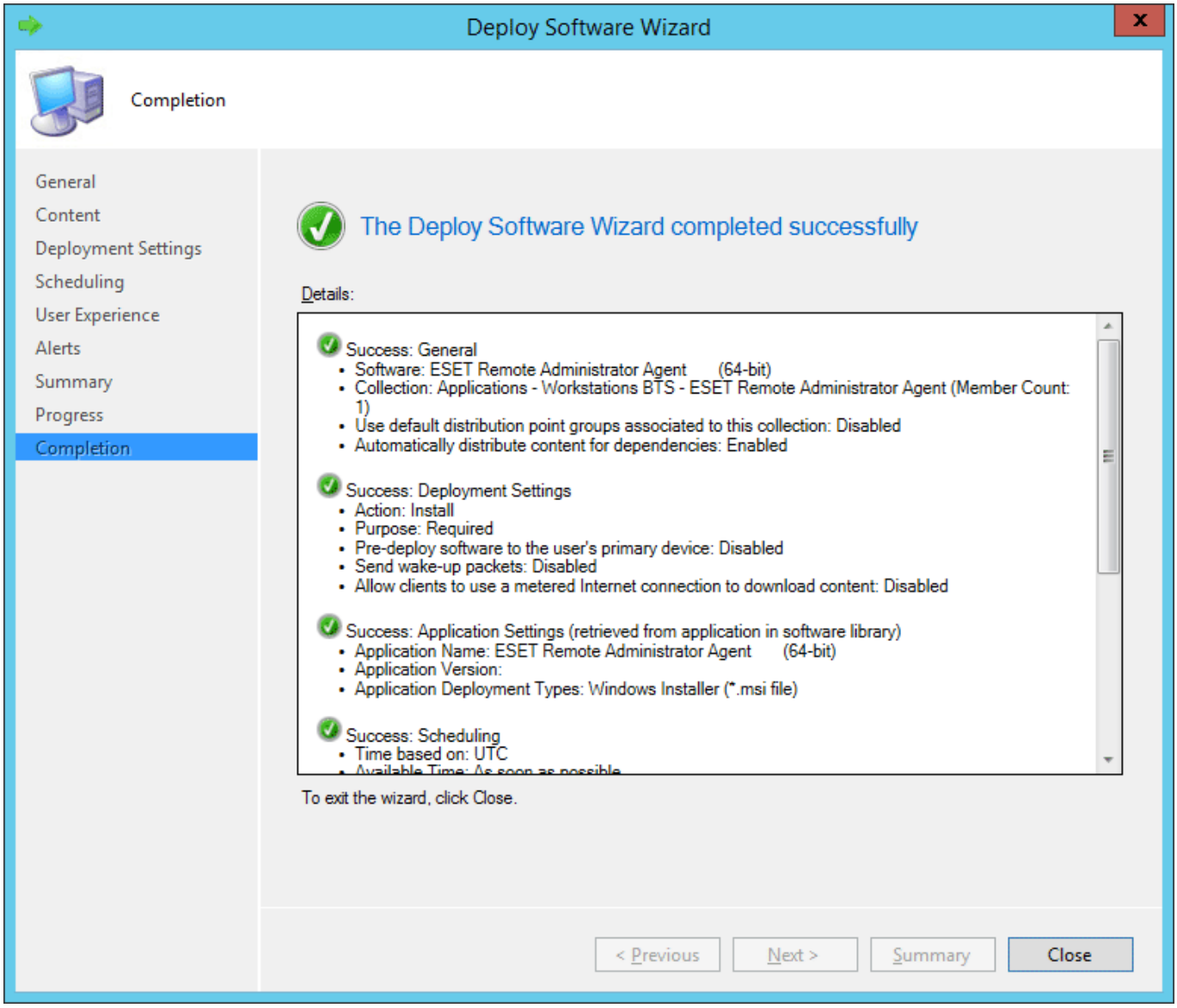

Distribute Content Wizard
Completion
General
Content
Content Destination
Summary
Progress
Completion
The Distribute Content Wizard completed successfully
Details:
Content (1):
• ESET Remote Administrator Agent (64-bit)
Dependencies (1):
• ESET Remote Administrator Agent (64-bit)
Collections (0):
Distribution point groups (0):
Distribution points (1):
To exit the wizard, click Close.
< Previous
Next >
Summary
Close


Deploy Software Wizard
General
General
Content
Deployment Settings
Scheduling
User Experience
Alerts
Summary
Progress
Completion
Specify general information for this deployment
Software:
ESET Remote Administrator Agent (64-bit)
Browse...
Collection:
Applications - Workstations BTS - ESET Remote Administrat
Browse...
Use default distribution point groups associated to this collection
Automatically distribute content for dependencies
Comments (optional):
< Previous
Next >
Summary
Cancel


Deploy Software Wizard
Deployment Settings
General
Content
Deployment Settings
Scheduling
User Experience
Alerts
Summary
Progress
Completion
Specify settings to control how this software is deployed
Action:
Install
Purpose:
Required
Pre-deploy software to the user's primary device
Send wake-up packets
Allow clients on a metered Internet connection to download content after the installation deadline, which might incur additional costs
< Previous
Next >
Summary
Cancel


Deploy Software Wizard
Scheduling
General
Content
Deployment Settings
Scheduling
User Experience
Alerts
Summary
Progress
Completion
Specify the schedule for this deployment
This application will be available as soon as it has been distributed to the content server(s) unless it is scheduled for a later time below. Specify the installation deadline if this is a required application. This deadline is when the application must be installed on the device, including a system restart if necessary.
Time based on:
UTC
Schedule the application to be available at:
9. 2.2015
12:32
Installation deadline:
As soon as possible after the available time
Schedule at:
9. 2.2015
12:32
< Previous
Next >
Summary
Cancel


Deploy Software Wizard
User Experience
General
Content
Deployment Settings
Scheduling
User Experience
Alerts
Summary
Progress
Completion
Specify the user experience for the installation of this software on the selected devices
Specify user experience setting for this deployment
User notifications:
Display in Software Center and show all notifications
When the installation deadline is reached, allow the following activities to be performed outside the maintenance window:
Software Installation
System restart (if required to complete the installation)
Write filter handling for Windows Embedded devices
Commit changes at deadline or during a maintenance window (requires restarts)
If this option is not selected, content will be applied on the overlay and committed later.
< Previous
Next >
Summary
Cancel



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.

> O ESET Remote Deployment Tool é dedicado para implantar o Agente ESET Management em computadores do cliente com os sistemas operacionais Microsoft Windows compatíveis.

Para implantar o Agente ESET Management e o produto de segurança ESET usando esses métodos, siga as etapas abaixo:

1. Faça o download da ESET Remote Deployment Tool do site da ESET.

2. Certifique-se de que todos os pré-requisitos sejam atendidos.

3. Execute a Ferramenta de implantação remota ESET no computador do cliente.

4. Selecione uma das seguintes opções de implantação:

    • Active Directory - Você precisará fornecer as credenciais do Active Directory. Essa opção inclui a exportação da estrutura do Active Directory para importação subsequente no ESET PROTECT.

    • Rastrear rede - Você precisará fornecer os intervalos de IP para rastrear computadores na rede.

    • Importar lista - Você precisará fornecer uma lista de nomes de host ou endereços IP.

    • Adicionar computadores manualmente - Você precisará fornecer uma lista de nomes de host ou endereços IP manualmente.

A implantação pode falhar devido a vários motivos. No caso de qualquer problema com a implantação, leia o capítulo de Solução de problemas ou cenários de exemplo verificados de implantação do Agente ESET Management.

Pré-requisitos da ferramenta de instalação remota ESET

Para implantações remotas, verifique todos os computadores do cliente com uma conexão com a internet.

Os seguintes pré-requisitos devem ser atendidos para usar a ferramenta de Implantação remota ESET no Windows:

• Servidor ESET PROTECT e o console da Web ESET PROTECT devem ser instalados (em um computador Servidor).

• A porta adequada deve ser aberta. Veja as portas usadas para implantação remota do Agente ESET Management para um computador de destino no sistema operacional Windows.

• Os nomes dos pacotes de instalação devem incluir a string "x86" ou "x64". Caso contrário a implantação não vai funcionar.

• Um pacote do instalador (tudo-em-um) deve ser criado e baixado para sua unidade local.

• É necessário ter permissões para criar o Instalador Tudo-em-um.

A implantação pode falhar devido a vários motivos. No caso de qualquer problema com a implantação, leia o capítulo de Solução de problemas ou cenários de exemplo verificados de implantação do Agente ESET Management.

Selecione computadores a partir do Active Directory

Para continuar com a implantação do Agente ESET Management e do produto de segurança ESET do capítulo anterior:

1. Leia e aceite o **Acordo de Licença para o Usuário final** e clique em **Avançar**.

2. Digite o **Servidor Active Directory** com endereço IP ou nome de host e a **Porta** onde você deseja conectar.

3. Digite o **Nome de usuário** e **Senha** para fazer login no servidor do Active Directory. Se você selecionar a caixa de verificação ao lado de **Usar credenciais de usuário atuais** as credenciais de login serão preenchidas automaticamente.

4. Opcionalmente, selecione a caixa de seleção ao lado de **Exportar lista de computadores para oESET PROTECT** se quiser exportar a estrutura do Active Directory para subsequente importação no ESET PROTECT.

Se um computador está no Active Directory, clique em **Avançar** e um login automático no Controlador de Domínio padrão acontecerá.

5. Selecione a caixa de seleção ao lado dos computadores que deseja adicionar e clique em **Avançar**. Selecione a caixa de marcação **Incluir subgrupos** para listar todos os computadores dentro de um grupo selecionado.

6. Os computadores selecionados para implantação remota serão exibidos. Certifique-se de que todos os computadores são adicionados e clique em **Avançar**.

Certifique-se de que todos os computadores selecionados têm a mesma plataforma (sistemas operacionais 64-bit ou 32-bit).

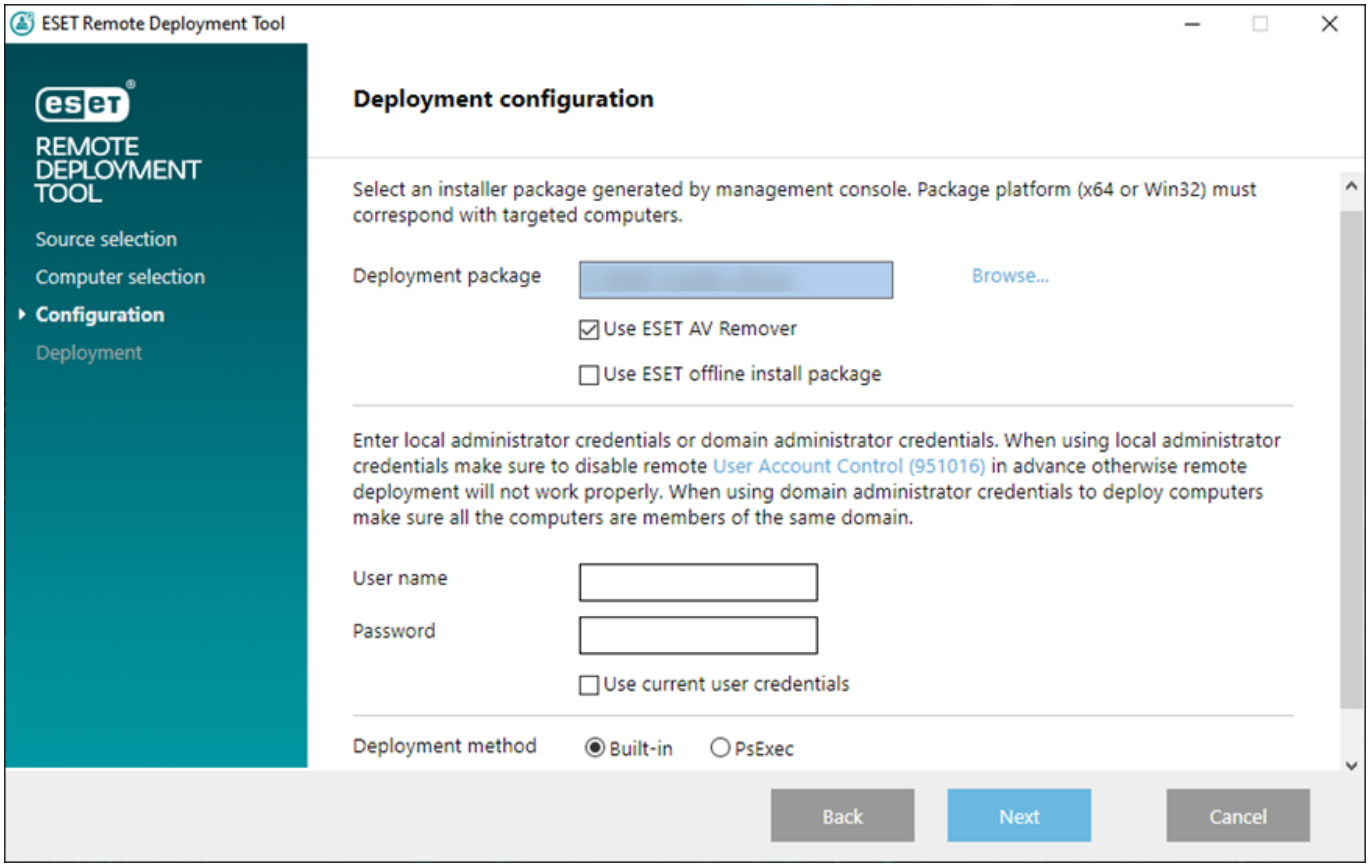
7. Clique em **Procurar** e selecione o pacote do instalador criado no Web Console ESET PROTECT ou ESET PROTECT Cloud.

- Você também pode selecionar **Usar o pacote de instalação off-line da ESET** (arquivo *.dat*) criado do Live Installer (apenas ESET PROTECT Cloud).

- Se você não tiver nenhum outro aplicativo de segurança instalado no seu computador local, desmarque a caixa de marcação ao lado de **Usar o ESET AV Remover**. O ESET AV Remover pode remover certos aplicativos.

8. Digite as credenciais de login para os computadores de destino. Se os computadores forem membros de um domínio, digite as **credenciais do administrador de domínio**. Se você fizer login com as **credenciais de administração local**, é necessário desativar o UAC remoto nos computadores de destino. Opcionalmente, você pode selecionar a caixa de verificação ao lado de **Usar credenciais de usuário atuais** e as credenciais de login serão preenchidas automaticamente.

9. O **método de implantação** é usado para executar programas em máquinas remotas. O método **Incorporado** é uma configuração padrão compatível com as mensagens de erro do Windows. **PsExec** é uma ferramenta de terceiros e é uma alternativa ao método incorporado. Selecione uma dessas opções e clique em **Avançar**.



Se você selecionou **PsExec** a implantação vai falhar, pois a ferramenta não conseguirá aceitar o Acordo de licença para o usuário final **PsExec**. Para uma implantação bem-sucedida, abra a linha de comando e execute o comando **PsExec** manualmente.

10. Quando a instalação for iniciada, "Sucesso" será exibido. Clique em **Concluir** para concluir a implantação. Se a implantação falhar, clique em **Mais informações** na coluna **Status** para ver mais detalhes. Você pode exportar uma lista de computadores com falha. Clique em **Procurar** ao lado do campo **Exportar computadores com falha**, selecione um arquivo *.txt* no qual você quer salvar a lista e clique em **Exportar computadores com falha**.

Você pode verificar o relatório de status (*C:\ProgramData\ESET\RemoteAdministrator\Agent\Logs\status.html*) na máquina do cliente para se certificar de que o Agente ESET Management esteja funcionando corretamente.

A implantação pode falhar devido a vários motivos. No caso de qualquer problema com a implantação, leia o capítulo de Solução de problemas ou cenários de exemplo verificados de implantação do Agente ESET Management.

Rastrear a rede local para computadores

Para continuar com a implantação do Agente ESET Management e do produto de segurança ESET do capítulo anterior:

1. Leia e aceite o **Acordo de Licença para o Usuário final** e clique em **Avançar**.

2. Insira os **Intervalos de IP** da rede na forma *10.100.100.10-10.100.100.250*

3. Selecione um dos seguintes **Métodos de escaneamento**:

- **Escanear ping** - Procura computadores do cliente com o comando `ping`.

> Alguns computadores do cliente nessa rede não precisam mandar uma resposta ao comando `ping` devido ao firewall bloqueando a conexão.

- **Escaneamento de porta** - Usa números de porta para rastrear a rede. Veja as portas compatíveis usadas para implantação remota dos Agentes ESET Management. O número da porta padrão é 445.

4. Para encontrar computadores na rede, clique em **Iniciar escaneamento**.

5. Selecione a caixa de seleção ao lado dos computadores que deseja adicionar e clique em **Avançar**.

6. Os computadores selecionados para implantação remota serão exibidos. Certifique-se de que todos os computadores são adicionados e clique em **Avançar**.

> Certifique-se de que todos os computadores selecionados têm a mesma plataforma (sistemas operacionais 64-bit ou 32-bit).

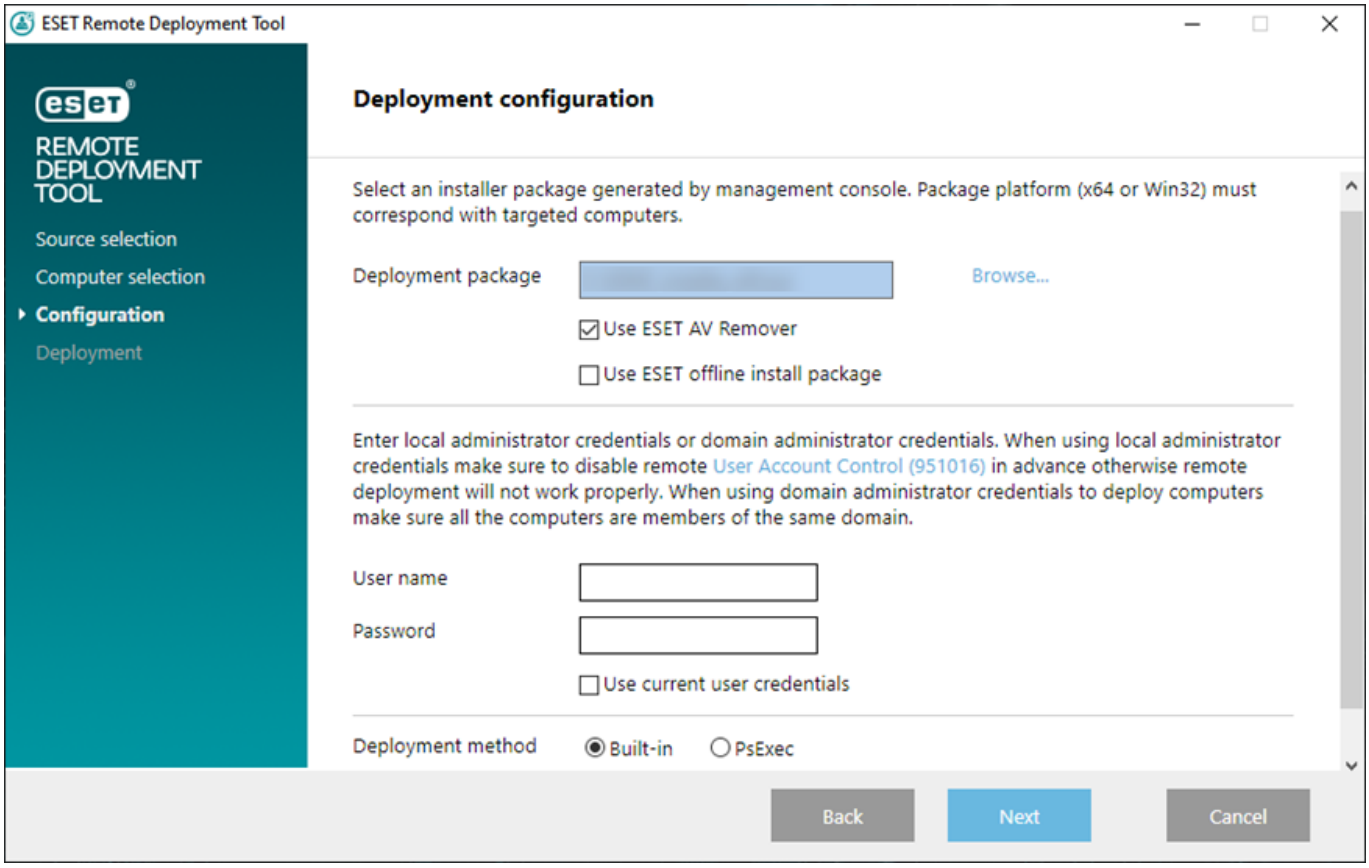
7. Clique em **Procurar** e selecione o pacote do instalador criado no Web Console ESET PROTECT ou ESET PROTECT Cloud.

- Você também pode selecionar **Usar o pacote de instalação off-line da ESET** (arquivo *.dat*) criado do Live Installer (apenas ESET PROTECT Cloud).

- Se você não tiver nenhum outro aplicativo de segurança instalado no seu computador local, desmarque a caixa de marcação ao lado de **Usar o ESET AV Remover**. O ESET AV Remover pode remover certos aplicativos.

8. Digite as credenciais de login para os computadores de destino. Se os computadores forem membros de um domínio, digite as **credenciais do administrador de domínio**. Se você fizer login com as **credenciais de administração local**, é necessário desativar o UAC remoto nos computadores de destino. Opcionalmente, você pode selecionar a caixa de verificação ao lado de **Usar credenciais de usuário atuais** e as credenciais de login serão preenchidas automaticamente.

9. O **método de implantação** é usado para executar programas em máquinas remotas. O método **Incorporado** é uma configuração padrão compatível com as mensagens de erro do Windows. **PsExec** é uma ferramenta de terceiros e é uma alternativa ao método incorporado. Selecione uma dessas opções e clique em **Avançar**.



Se você selecionou **PsExec** a implantação vai falhar, pois a ferramenta não conseguirá aceitar o Acordo de licença para o usuário final **PsExec**. Para uma implantação bem-sucedida, abra a linha de comando e execute o comando **PsExec** manualmente.

10. Quando a instalação for iniciada, "Sucesso" será exibido. Clique em **Concluir** para concluir a implantação. Se a implantação falhar, clique em **Mais informações** na coluna **Status** para ver mais detalhes. Você pode exportar uma lista de computadores com falha. Clique em **Procurar** ao lado do campo **Exportar computadores com falha**, selecione um arquivo *.txt* no qual você quer salvar a lista e clique em **Exportar computadores com falha**.

Você pode verificar o relatório de status (*C:\ProgramData\ESET\RemoteAdministrator\Agent\Logs\status.html*) na máquina do cliente para se certificar de que o Agente ESET Management esteja funcionando corretamente.

A implantação pode falhar devido a vários motivos. No caso de qualquer problema com a implantação, leia o capítulo de Solução de problemas ou cenários de exemplo verificados de implantação do Agente ESET Management.

Importar uma lista de computadores

Para continuar com a implantação do Agente ESET Management e do produto de segurança ESET do capítulo anterior:

1. Leia e aceite o **Acordo de Licença para o Usuário final** e clique em **Avançar**.

2. Selecione uma das seguintes opções:

   • **Arquivo de texto (um computador por linha)**: Um arquivo com nomes de host ou endereços IP. Cada endereço IP ou nome de host deve estar em uma nova linha.

   • **Exportar do console de gerenciamento**: Um arquivo com nomes de host ou endereços IP exportados do Console da Web ESET PROTECT.

3. Clique em **Procurar** e selecione o arquivo que você gostaria de carregar e clique em **Avançar**.

4. Os computadores selecionados para implantação remota serão exibidos. Certifique-se de que todos os computadores são adicionados e clique em **Avançar**.

Certifique-se de que todos os computadores selecionados têm a mesma plataforma (sistemas operacionais 64-bit ou 32-bit).

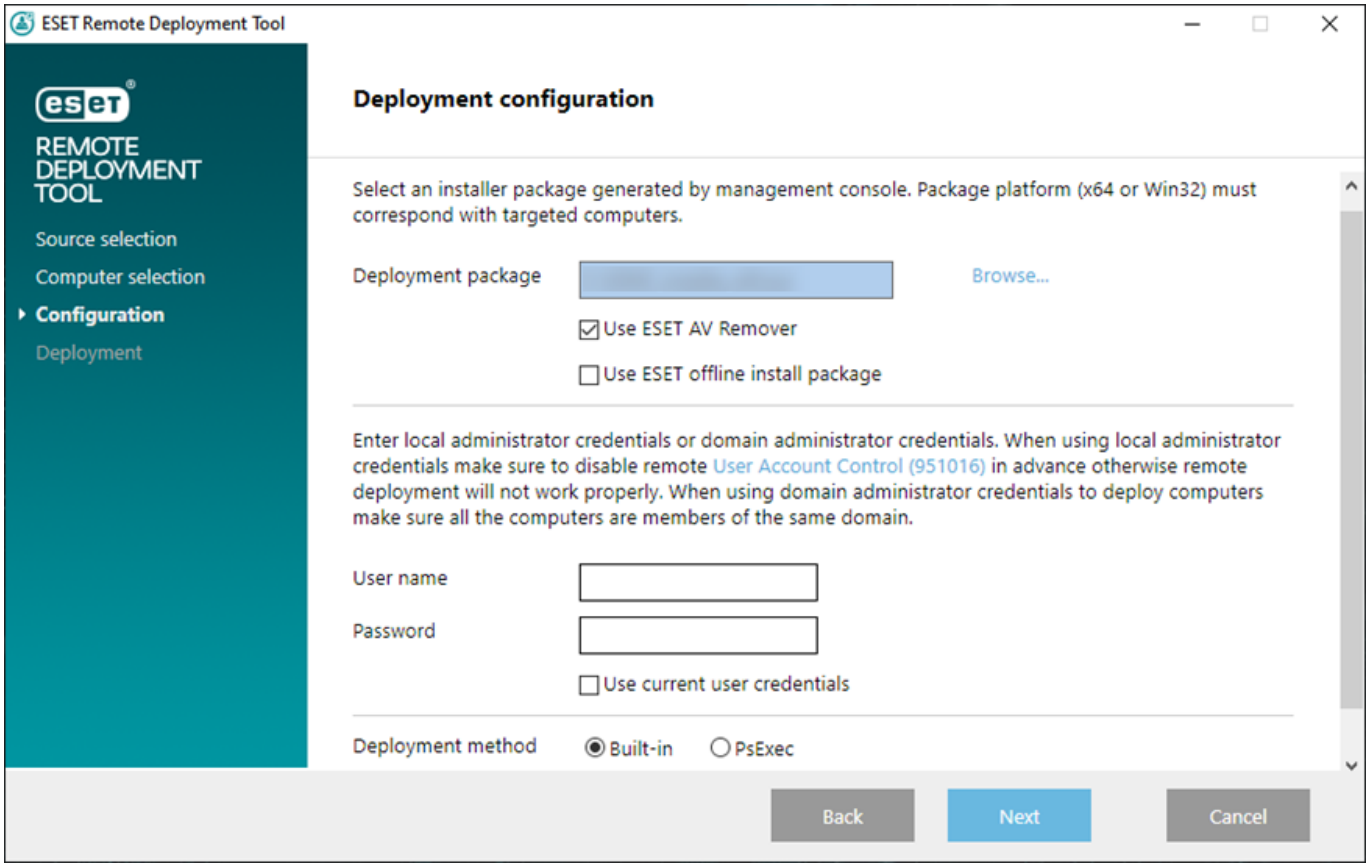
5. Clique em **Procurar** e selecione o pacote do instalador criado no Web Console ESET PROTECT ou ESET PROTECT Cloud.

   • Você também pode selecionar **Usar o pacote de instalação off-line da ESET** (arquivo *.dat*) criado do Live Installer (apenas ESET PROTECT Cloud).

   • Se você não tiver nenhum outro aplicativo de segurança instalado no seu computador local, desmarque a caixa de marcação ao lado de **Usar o ESET AV Remover**. O ESET AV Remover pode remover certos aplicativos.

6. Digite as credenciais de login para os computadores de destino. Se os computadores forem membros de um domínio, digite as **credenciais do administrador de domínio**. Se você fizer login com as **credenciais de administração local**, é necessário desativar o UAC remoto nos computadores de destino. Opcionalmente, você pode selecionar a caixa de verificação ao lado de **Usar credenciais de usuário atuais** e as credenciais de login serão preenchidas automaticamente.

7. O **método de implantação** é usado para executar programas em máquinas remotas. O método **Incorporado** é uma configuração padrão compatível com as mensagens de erro do Windows. **PsExec** é uma ferramenta de terceiros e é uma alternativa ao método incorporado. Selecione uma dessas opções e clique em **Avançar**.



Se você selecionou **PsExec** a implantação vai falhar, pois a ferramenta não conseguirá aceitar o Acordo de licença para o usuário final **PsExec**. Para uma implantação bem-sucedida, abra a linha de comando e execute o comando **PsExec** manualmente.

8. Quando a instalação for iniciada, "Sucesso" será exibido. Clique em **Concluir** para concluir a implantação. Se a implantação falhar, clique em **Mais informações** na coluna **Status** para ver mais detalhes. Você pode exportar uma lista de computadores com falha. Clique em **Procurar** ao lado do campo **Exportar computadores com falha**, selecione um arquivo *.txt* no qual você quer salvar a lista e clique em **Exportar computadores com falha**.

Você pode verificar o relatório de status (*C:\ProgramData\ESET\RemoteAdministrator\Agent\Logs\status.html*) na máquina do cliente para se certificar de que o Agente ESET Management esteja funcionando corretamente.

A implantação pode falhar devido a vários motivos. No caso de qualquer problema com a implantação, leia o capítulo de Solução de problemas ou cenários de exemplo verificados de implantação do Agente ESET Management.

Adicionar computadores manualmente

Para continuar com a implantação do Agente ESET Management e do produto de segurança ESET do capítulo anterior:

1. Leia e aceite o **Acordo de Licença para o Usuário final** e clique em **Avançar**.

2. Insira os nomes do host ou Endereços IP manualmente e clique em **Avançar**. Cada endereço IP ou nome de host deve estar em uma nova linha.

Certifique-se de que todos os computadores selecionados têm a mesma plataforma (sistemas operacionais 64-bit ou 32-bit).

3. Os computadores selecionados para implantação remota serão exibidos. Certifique-se de que todos os computadores são adicionados e clique em **Avançar**.

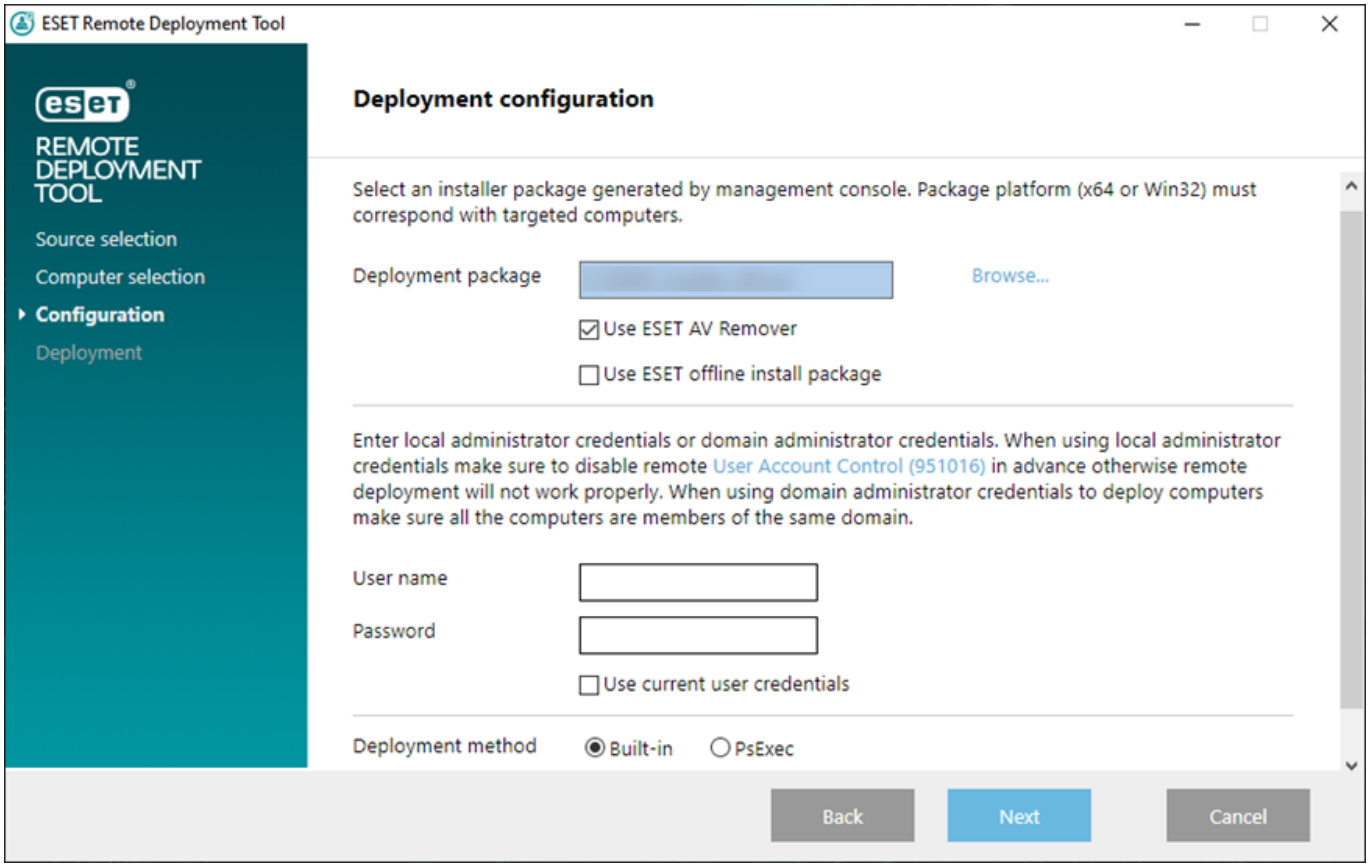
4. Clique em **Procurar** e selecione o pacote do instalador criado no Web Console ESET PROTECT ou ESET PROTECT Cloud.

- Você também pode selecionar **Usar o pacote de instalação off-line da ESET** (arquivo *.dat*) criado do Live Installer (apenas ESET PROTECT Cloud).

- Se você não tiver nenhum outro aplicativo de segurança instalado no seu computador local, desmarque a caixa de marcação ao lado de **Usar o ESET AV Remover**. O ESET AV Remover pode remover certos aplicativos.

5. Digite as credenciais de login para os computadores de destino. Se os computadores forem membros de um domínio, digite as **credenciais do administrador de domínio**. Se você fizer login com as **credenciais de administração local**, é necessário desativar o UAC remoto nos computadores de destino. Opcionalmente, você pode selecionar a caixa de verificação ao lado de **Usar credenciais de usuário atuais** e as credenciais de login serão preenchidas automaticamente.

6. O **método de implantação** é usado para executar programas em máquinas remotas. O método **Incorporado** é uma configuração padrão compatível com as mensagens de erro do Windows. **PsExec** é uma ferramenta de terceiros e é uma alternativa ao método incorporado. Selecione uma dessas opções e clique em **Avançar**.



Se você selecionou **PsExec** a implantação vai falhar, pois a ferramenta não conseguirá aceitar o Acordo de licença para o usuário final **PsExec**. Para uma implantação bem-sucedida, abra a linha de comando e execute o comando **PsExec** manualmente.

7. Quando a instalação for iniciada, "Sucesso" será exibido. Clique em **Concluir** para concluir a implantação. Se a implantação falhar, clique em **Mais informações** na coluna **Status** para ver mais detalhes. Você pode exportar uma lista de computadores com falha. Clique em **Procurar** ao lado do campo **Exportar computadores com falha**, selecione um arquivo *.txt* no qual você quer salvar a lista e clique em **Exportar computadores com falha**.

Você pode verificar o relatório de status (*C:\ProgramData\ESET\RemoteAdministrator\Agent\Logs\status.html*) na máquina do cliente para se certificar de que o Agente ESET Management esteja funcionando corretamente.

A implantação pode falhar devido a vários motivos. No caso de qualquer problema com a implantação, leia o capítulo de Solução de problemas ou cenários de exemplo verificados de implantação do Agente ESET Management.

ESET Remote Deployment Tool – solução de problemas

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.

> O ESET Remote Deployment Tool é dedicado para implantar o Agente ESET Management em computadores do cliente com os sistemas operacionais Microsoft Windows compatíveis.

A implantação pode falhar com várias mensagens de erro e devido a alguns dos motivos listados na tabela abaixo:

Mensagem de erro	Causas possíveis
O caminho da rede não foi encontrado (código de erro 0x35)	• O cliente não pode ser acessado na rede, o firewall bloqueia a comunicação • Portas de entrada 135, 137, 138, 139 e 445 não estão abertas no firewall no cliente ou Firewall do Windows: Permitir arquivo de entrada e exceção de compartilhamento de impressoras não é usado • Não foi possível resolver o nome do host do cliente, use nomes de computador FQDN válidos
Acesso negado (código de erro 0x5) **O nome de usuário ou senha está incorreto** (código de erro 0x52e)	• Ao implantar de um servidor unido a um domínio para um cliente unido ao domínio, use credenciais de um usuário que é membro do grupo de Administrador do domínio no formato **Domain\DomainAdmin** • Ao implantar de um servidor para um cliente que não está em um mesmo domínio, desative a filtragem UAC remota no computador de destino. • Ao implantar de um servidor para um cliente que não está no mesmo domínio, use credenciais de um usuário local membro do grupo de Administradores no formato Administrador. O nome do computador de destino será adicionado automaticamente ao login. • Não há uma senha definida para a conta do administrador • Direitos de acesso insuficientes • O compartilhamento administrativo ADMIN$ não está disponível • O compartilhamento administrativo IPC$ não está disponível • O uso de compartilhamento de arquivo simples está ativado
O pacote de instalação não é compatível com este tipo de processador (código de erro 1633)	O pacote de instalação não é compatível com esta plataforma. Crie e faça o download do pacote de instalação com a plataforma correta (sistema operacional de 64- bit ou 32- bit) no Console da Web ESET PROTECT.
O período de tempo limite do semáforo expirou	O cliente não conseguirá acessar o compartilhamento de rede com o pacote de instalação porque o SMB 1.0 está desativado no compartilhamento.

Siga as etapas da solução de problemas adequadas de acordo com a causa possível:

Causa possível	Etapas para a solução de problemas
O cliente não pode ser acessado na rede	Ping do cliente do ESET PROTECT Servidorse você obtiver uma resposta, tente fazer login na máquina cliente remotamente (por exemplo, via área de trabalho remota).
O firewall bloqueia a comunicação	Verifique as configurações de firewall no servidor e no cliente, bem como se há qualquer outro firewall entre essas duas máquinas (se aplicável). Depois da implantação realizada com êxito, as portas 2222 e 2223 não estão abertas no firewall. Certifique-se de que essas portas estejam abertas em todos os firewalls entre as duas máquinas (cliente e servidor).
Não foi possível resolver o nome do host do cliente	Possíveis soluções para problemas de DNS podem incluir, mas não estão limitadas a: • Usando o comando `nslookup` do endereço IP e nome de host do servidor e/ou os clientes tendo problemas de implantação do Agente. Os resultados devem corresponder às informações na máquina. Por exemplo, um `nslookup` de um nome de host deve ser resolvido para o endereço IP que um comando `ipconfig` mostra no host em questão. O comando `nslookup` precisará ser executado nos clientes e no servidor. • Como analisar manualmente registros DNS quanto a duplicatas.
Não há uma senha definida para a conta do administrador	Defina a senha apropriada para a conta do administrador (não use uma senha em branco)
Direitos de acesso insuficientes	Tente usar as credenciais do Administrador do domínio ao criar a tarefa de implantação do Agente. Se a máquina cliente estiver em um grupo de trabalho, use a conta do administrador local nessa máquina específica. Para o Windows 7 e versões posteriores, é necessário ativar a conta de usuário Administrador para executar a tarefa de implementação do Agente. Você pode criar um usuário local que é membro do grupo Administradores ou ativar a conta de Administrador local incorporada. Para ativar a conta de usuário Administrador: 1.Abra um prompt de comando administrativo 2.Tipo o seguinte comando: `net user administrator /active:yes`
O compartilhamento administrativo ADMIN$ não está disponível	A máquina cliente deve ter o recurso compartilhado **ADMIN$** ativado. Certifique-se de que ele esteja presente entre outros compartilhamentos (**Iniciar** > **Painel de controle** > **Ferramentas administrativas** > **Gerenciamento de computador** > **Pastas compartilhadas** > **Compartilhamentos**).
O compartilhamento administrativo IPC$ não está disponível	Verifique se o servidor pode acessar IPC$ ao emitir o seguinte prompt de comando no servidor: `net use \\clientname\IPC$` onde `clientname` é o nome do computador de destino.
O uso de compartilhamento de arquivo simples está ativado	Se você estiver recebendo a mensagem de erro **Acesso negado** e tiver um ambiente misto (com domínio e grupo de trabalho), desative **Usar compartilhamento de arquivo simples** ou **Usar assistente de compartilhamento** em todas as máquinas nas quais está tendo problema com a implementação do Agente. Por exemplo, no Windows 7 faça o seguinte: • Clique em **Iniciar**, digite `pasta` na caixa de **Pesquisa** e clique em **Opções de pasta**. Clique na guia **Visualizar** e, na caixa **Configurações avançadas**, role até a lista e desmarque a caixa de seleção **Usar assistente de compartilhamento**.

Proteção do agente

O Agente ESET Management é protegido por um mecanismo integrado de autodefesa. Este recurso fornece o seguinte:

- Proteção contra a modificação de registro do Agente ESET Management (HIPS)
- Arquivos pertencentes ao Agente ESET Management não podem ser modificados, substituídos, excluídos ou alterados (HIPS)
- Não é possível interromper o Processo do Agente ESET Management

- O serviço do Agente ESET Management não pode ser interrompido, pausado, desativado, desinstalado ou comprometido de qualquer outra forma

Parte da proteção é coberta pelo recurso HIPS, incluído no seu produto ESET.

> Para garantir a proteção integral do Agente ESET Management, HIPS deve ser ativado no computador do cliente.

Configuração protegida por senha

Além da autodefesa, você pode proteger por senha o acesso ao Agente ESET Management (disponível apenas para Windows). Quando a proteção por senha está configurada, o Agente ESET Management não pode ser desinstalado ou reparado a menos que a senha correta seja fornecida. Para definir uma senha do Agente ESET Management é preciso criar uma política para o Agente ESET Management adequada.

Configurações do Agente ESET Management

Você pode definir configurações específicas do Agente ESET Management usando uma política do Agente ESET Management. Essas são políticas predefinidas para o Agente ESET Management. Por exemplo **Conexão** - Conectar a cada (intervalo de conexão do Agente) ou **Relatórios de aplicativo** - Reportar todos os aplicativos instalados (não só aplicativos ESET). Para obter mais informações sobre como forçar a política baseada em localização, leia o exemplo.

Clique em **Políticas** e expanda **Políticas incorporadas** > **Agente ESET Management** para editar uma política existente ou para criar uma nova.

Conexão

- **Servidores onde se conectar** - Para adicionar detalhes de conexão do Servidor ESET PROTECT (nome de host/IP e um número de porta) clique em Editar lista de servidores. Vários Servidores ESET PROTECT podem ser especificados. Isso pode ser útil se, por exemplo, você alterou o endereço IP do seu Servidor ESET PROTECT ou se estiver fazendo uma migração.

- **Limite de dados** - Escolha o número máximo de bytes para o envio de dados.

- **Intervalo de conexão** - Escolha o Intervalo regular e especifique o valor de tempo para o intervalo de conexão (ou você pode usar a expressão CRON).

- **Certificado** - Você pode gerenciar Certificados de mesmo nível para o Agente ESET Management. Clique em **Alterar certificado** e selecione qual certificado do Agente ESET Management deve ser usado pelo Agente ESET Management. Para obter mais informações consulte Certificados de mesmo nível.

Atualizações

- **Intervalo de atualização** - intervalo no qual as atualizações serão recebidas. Selecione um Intervalo regular e definir as configurações (ou usar uma expressão CRON).

- **Servidor de atualização** – Servidor de atualização do qual o Agente ESET Management recebe atualizações de módulo.

• **Tipo de atualização** - selecione o tipo de atualizações que deseja receber. Escolha uma atualização regular ou de pré-lançamento. Não recomendamos que você selecione as atualizações de Teste para sistemas de produção, pois isso apresenta um risco.

• **Ativar atualização automática** – essa opção se aplica ao Agente ESET Management 8.1 e versões posteriores. Por padrão, o Agente ESET Management é atualizado automaticamente para a versão compatível mais recente. Você pode desativar esta opção para desativar a atualização automática do Agente ESET Management.

Configurações avançadas

• **Proxy HTTP** - Use um servidor proxy para facilitar o tráfego na internet de clientes da sua rede e a replicação do Agente para o Servidor ESET PROTECT.

o**Tipo de configuração de proxy**

■**Proxy Global** - Usar um servidor proxy para replicação do Agente e para armazenamento em cache de serviços ESET (por exemplo, atualizações).

■**Proxy diferente por serviço** - Usar um proxy para replicação de Agente e outro para o armazenamento em cache de serviços ESET (por exemplo, atualizações).

o**Proxy Global** - Essa opção só está disponível se for selecionada no **Tipo de configuração do proxy**. Clique em **Editar** e defina suas configurações de proxy.

As duas opções abaixo estão disponíveis apenas se você selecionar **Proxy diferente por serviço**. Você também pode usar uma das configurações de proxy, por exemplo, definir apenas **Serviços ESET** e deixar a **Replicação** desligada. Selecione ou desmarque a caixa de seleção **Usar conexão direta se o proxy HTTP não estiver disponível** para ativar ou desativar esta opção de fallback.

o**Replicação (para o Servidor de gerenciamento ESET)** – configure as configurações de conexão para um proxy que conecta o Agente ao Servidor.

o**Serviços ESET** - Configure configurações de conexão para um proxy que vai armazenar em cache os serviços ESET.

• **Chamada para acordar** - ESET PROTECT o Servidor pode executar uma replicação instantânea do Agente ESET Management em uma máquina via EPNS. Isso é útil quando você não quer aguardar o intervalo regular quando o Agente ESET Management se conecta ao Servidor ESET PROTECT. Por exemplo, quando quiser que uma Tarefa seja executada imediatamente em clientes ou se quiser que uma Política seja aplicada já.

• **Compatibilidade** - Para permitir o gerenciamento de produtos ESET versão 5 ou versões anteriores pelo Agente ESET Management, uma porta de escuta específica deve ser definida. Além disso, os produtos ESET precisam ser configurados para se reportar a esta porta e o endereço de servidor ESET PROTECT precisa ser definido como **localhost**.

• **Sistema operacional** – use as alternâncias para reportar certas informações ou problemas no computador do cliente. Por exemplo, ative o **Relatório de aplicativos não instalados pela ESET** para permitir o relatório de aplicativos de terceiros instalados.

• **Repositório** - local do repositório no qual todos os arquivos de instalação são armazenados.

O repositório padrão é **AUTOSELECT**.

• **Programa de melhoria do produto** - Ativa ou desativa a transmissão de relatórios de parada e dados de telemetria anônimos para a ESET.

• **Registro em 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). O arquivo do relatório do Agente ESET Management mais recente pode ser encontrado aqui em um computador do cliente:

• **Configuração** - Configuração protegida por senha é um recurso de proteção do Agente ESET Management (somente para Windows). Definir senha para ativar a proteção de senha do Agente ESET Management. Quando a política é aplicada, o Agente ESET Management não pode ser desinstalado ou reparado a menos que uma senha seja fornecida.

Se você esquecer esta senha, você não conseguirá desinstalar o Agente ESET Management da máquina de destino.

Atribuir

Especifique os clientes que receberão essa política. Clique em **Atribuir** para exibir todos os grupos estáticos e dinâmicos e seus membros. Selecione o computador no qual você deseja aplicar uma política e clique em **OK**.

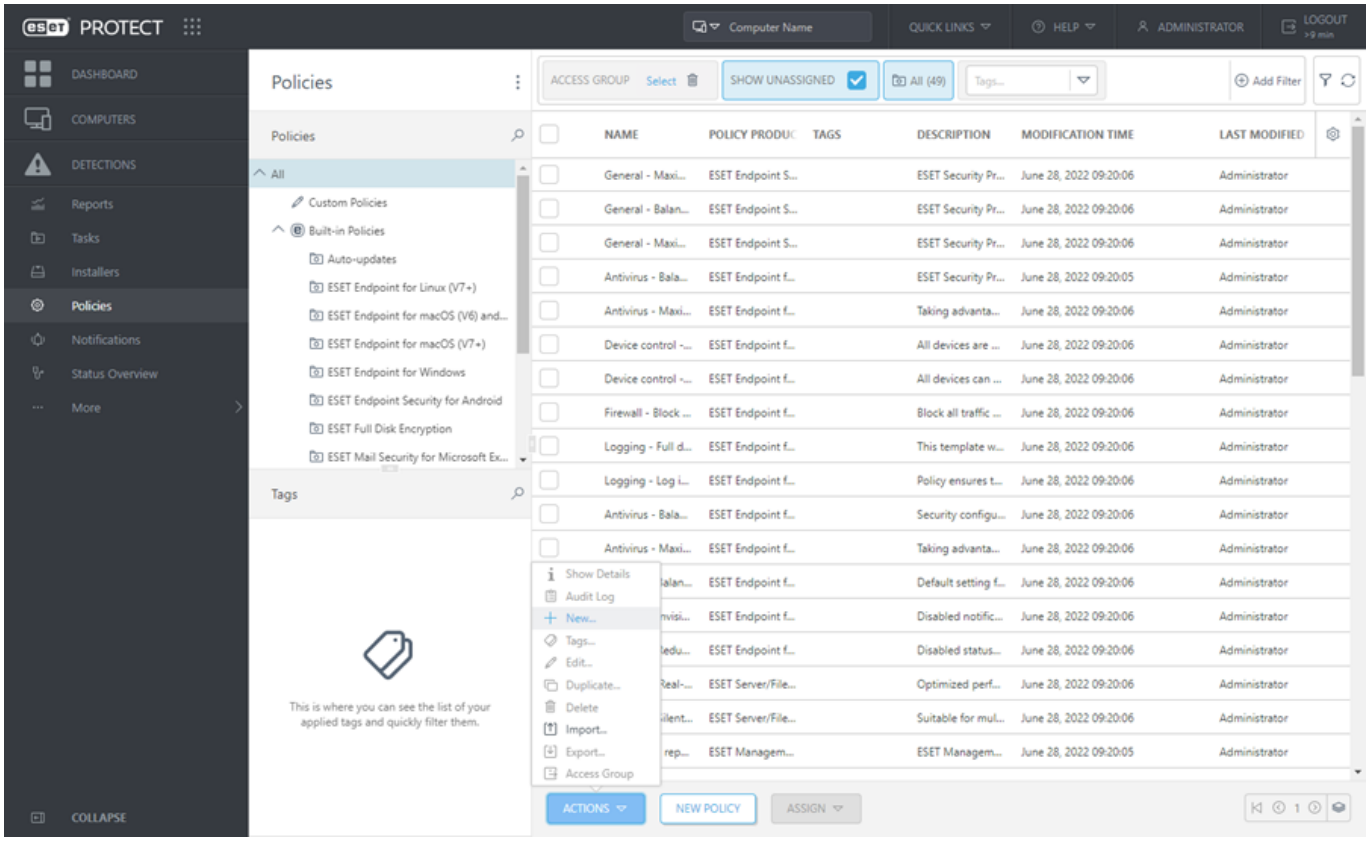
Resumo

Verifique as configurações para esta política e clique em **Concluir**.

Criar uma política para o intervalo de conexão do Agente ESET Management

Neste exemplo, criaremos uma nova política para o intervalo de conexão do Agente ESET Management. Este valor deve ser ajustado com base no tamanho da sua infraestrutura usando políticas depois de instalar o ESET PROTECT e implantar Agentes ESET Management e produtos ESET endpoint em máquinas do cliente.

Crie um Novo grupo estático. Adicione uma nova política clicando em **Políticas**. Clique em **Ações**, na parte inferior, e selecione **Novo**.

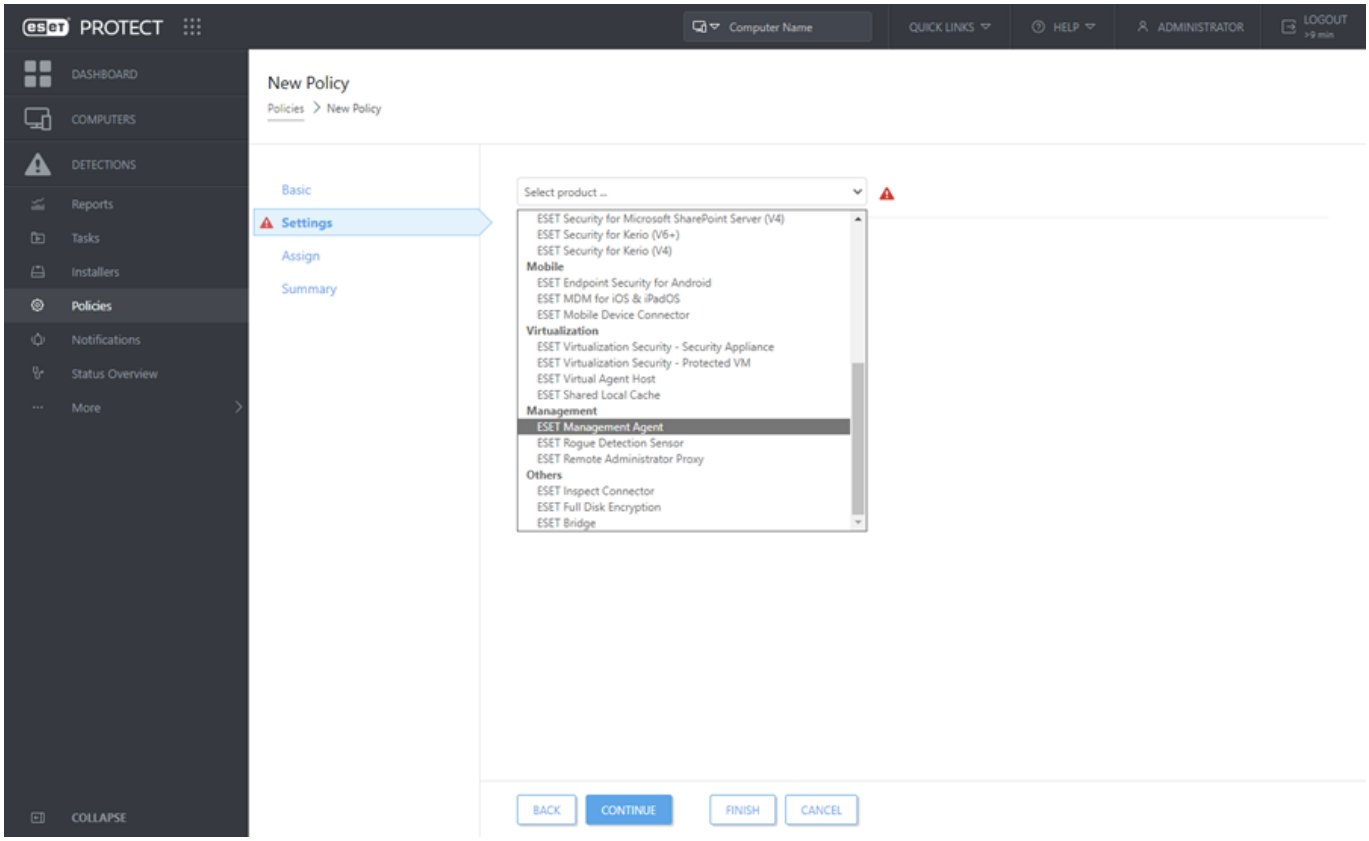


Básico

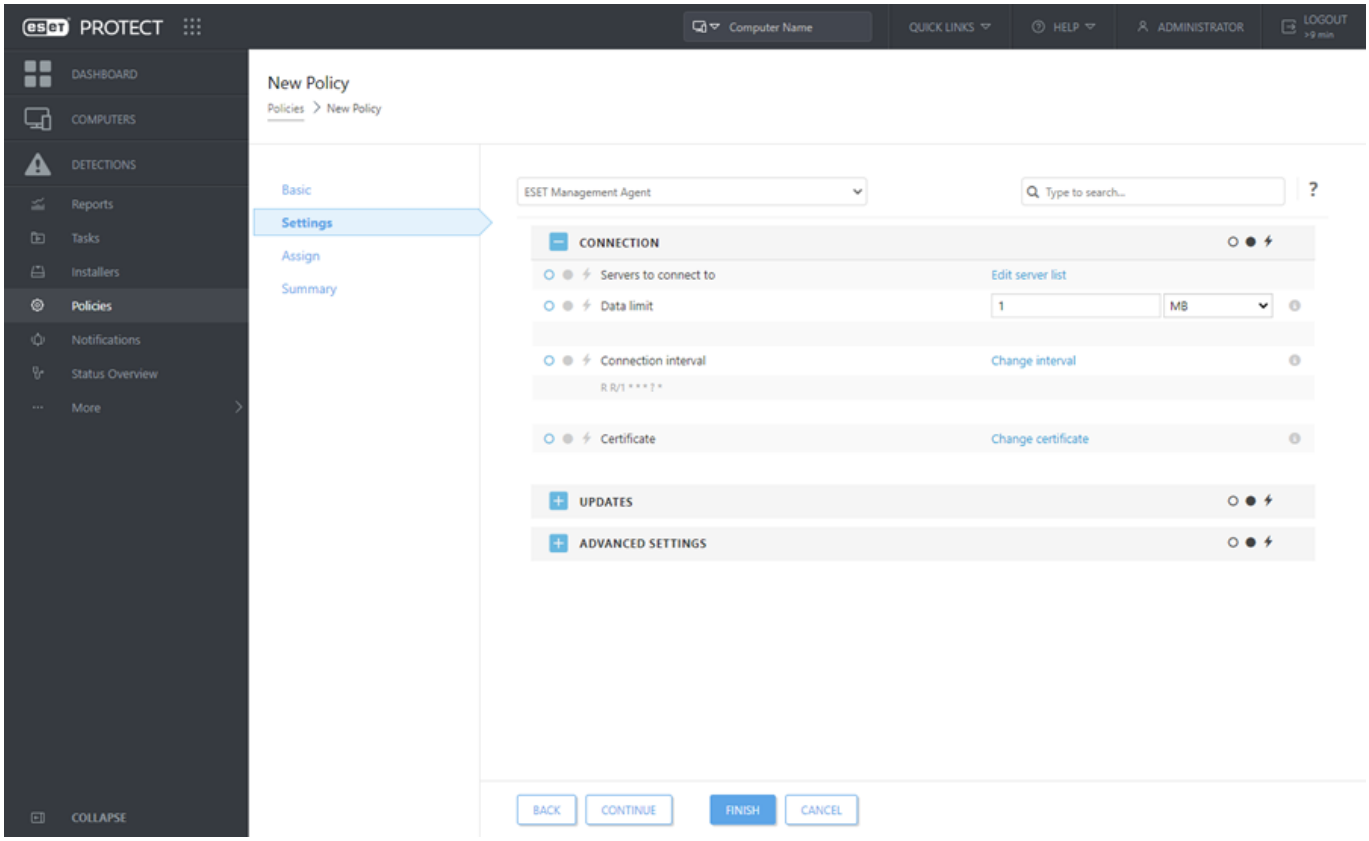
Insira um **Nome** para a nova política (por exemplo, “Intervalo de conexão do Agente”). O campo **Descrição** é opcional.

Configurações

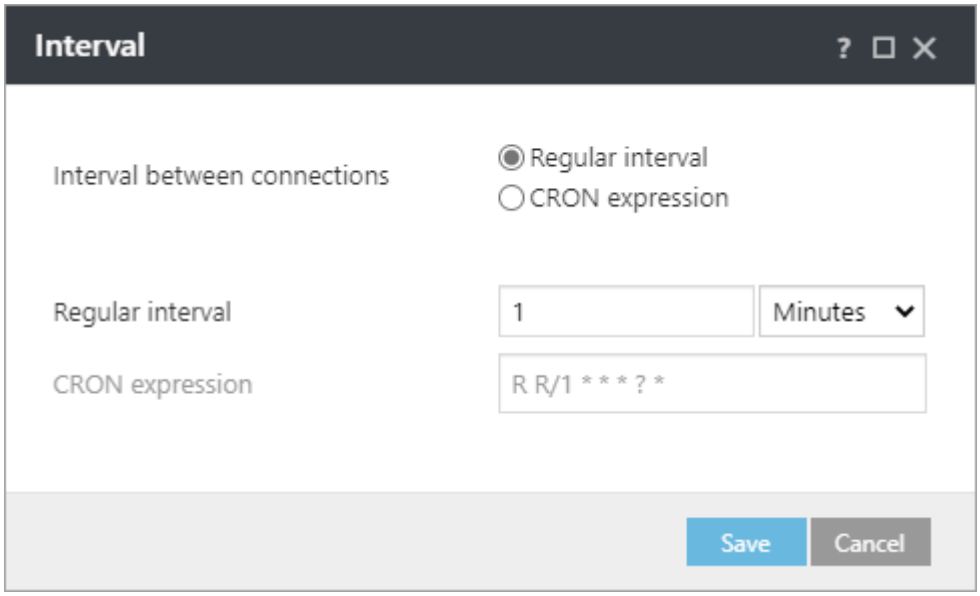
Selecione **ESET ManagementAgente** do menu suspenso **Produto** .



Clique em **Intervalo de conexão** > **Alterar intervalo**.

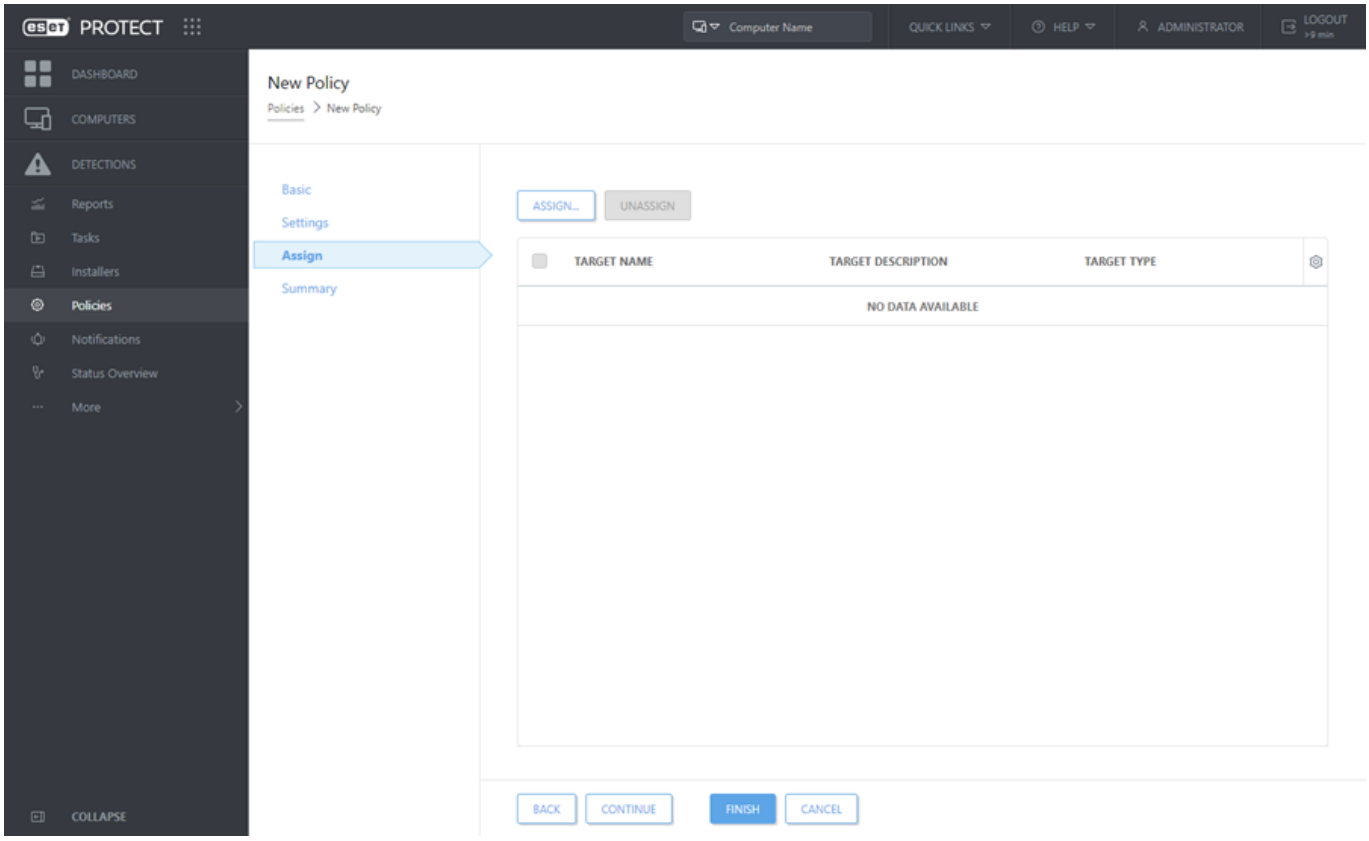


No campo **Intervalo regular**, altere o valor para seu tempo de intervalo preferido (60 segundos é o intervalo de replicação padrão do Agente ESET Management) e clique em **Salvar**.



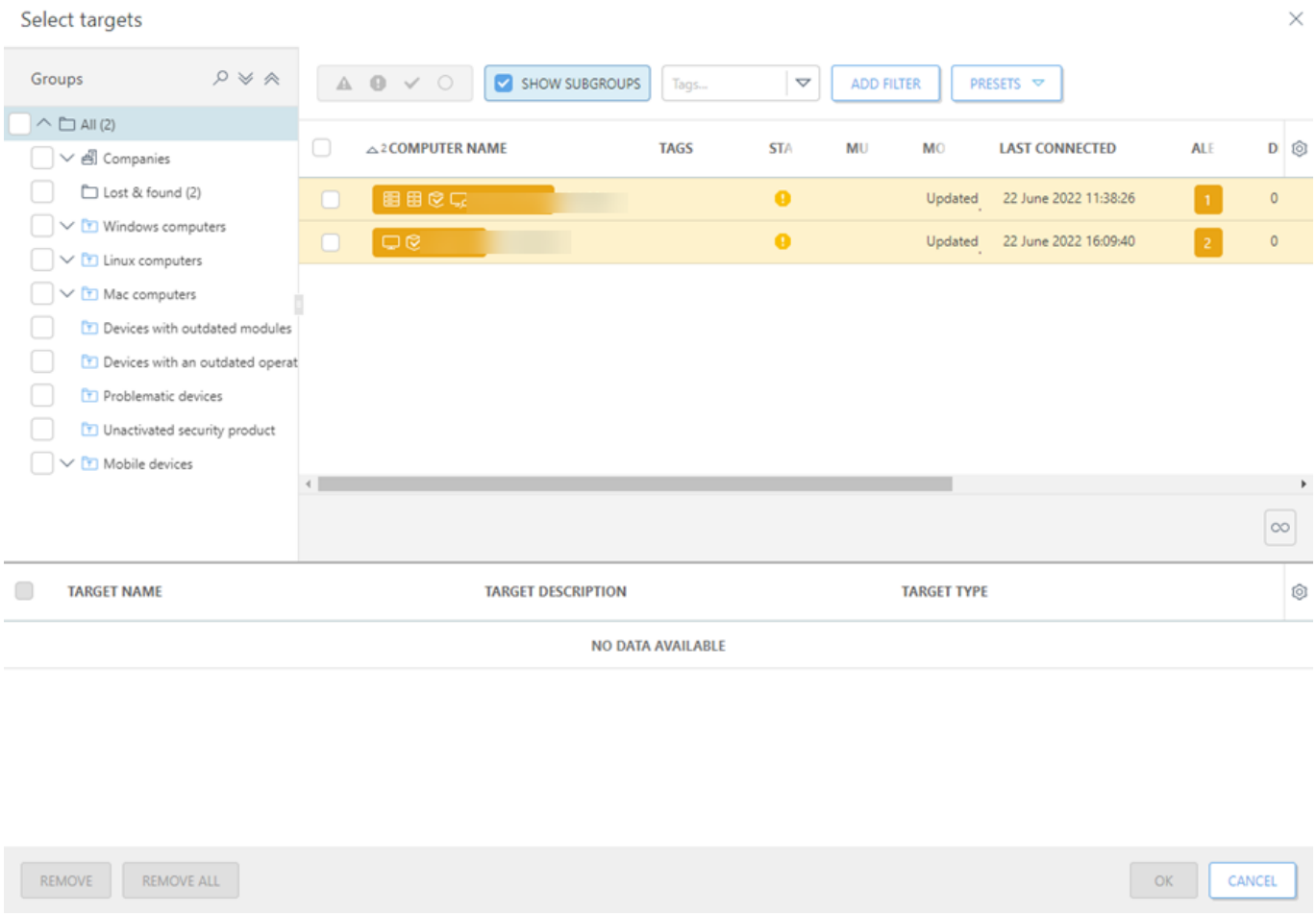
Atribuir

Especifique os clientes (computadores individuais/dispositivos móveis ou grupos inteiros) que serão os destinatários dessa política.



Clique em **Atribuir** para exibir todos os grupos estáticos e dinâmicos e seus membros. Selecione seus computadores ou grupos desejados e clique em **OK**.

Para atribuir todos os computadores em um grupo, atribua o grupo em vez de computadores individuais para impedir que a velocidade do Web Console diminua.
O Web Console exibirá um aviso se você selecionar um grande número de computadores.



Resumo

Verifique as configurações para esta política e clique em **Concluir**. A política é aplicada aos destinos depois da próxima conexão com o Servidor ESET PROTECT (dependendo do intervalo de conexão do agente).

Para aplicar a política imediatamente, você pode executar a ação **Enviar chamada para despertar** aos destinos nos **Computadores**.

Criar uma política para o Agente ESET Management conectar-se com o novo Servidor ESET PROTECT

Esta política permite que você altere o comportamento do Agente ESET Management ao modificar suas configurações. O seguinte é especialmente útil ao migrar máquinas clientes para um novo Servidor ESET PROTECT.

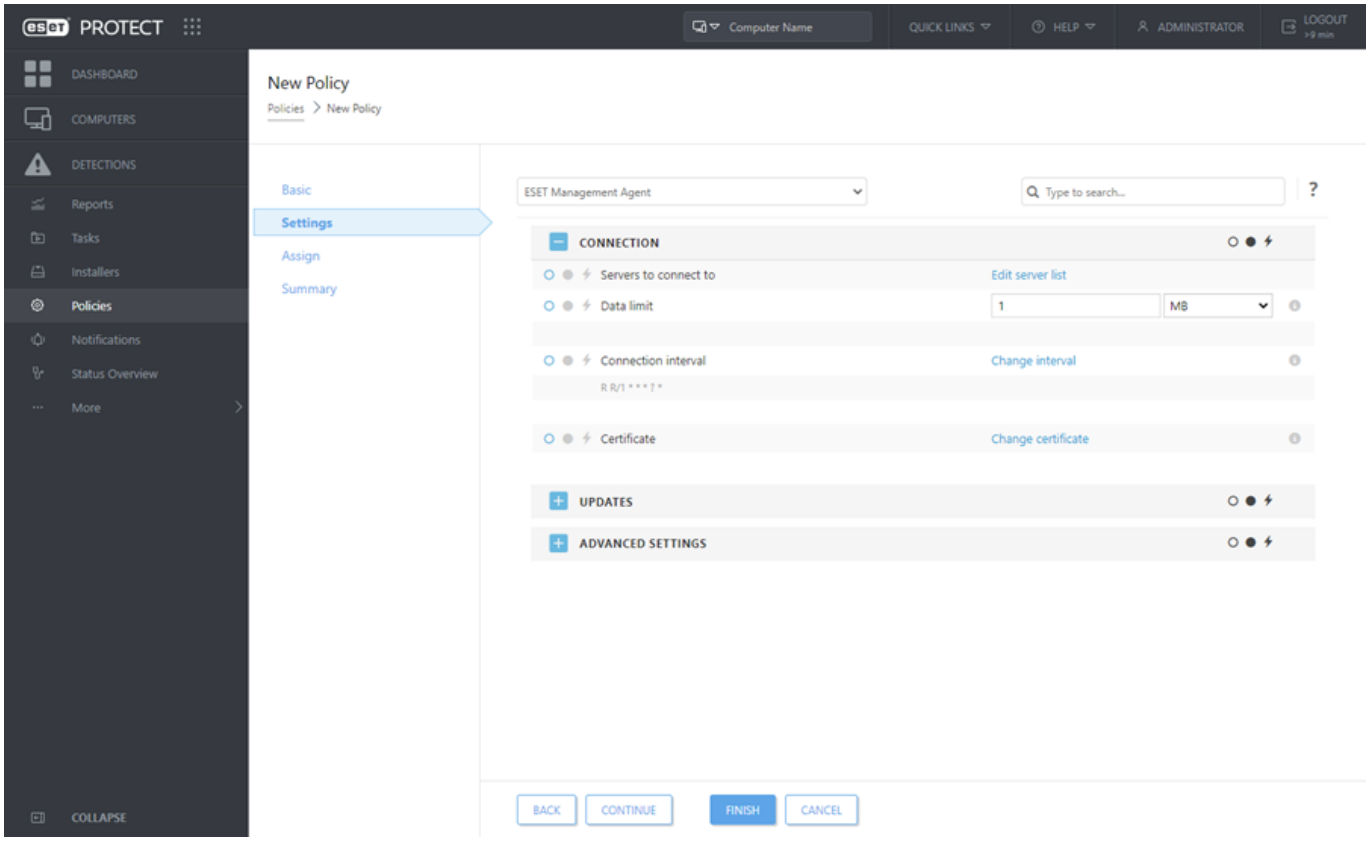
Criar uma nova política para definir o novo endereço IP do Servidor ESET PROTECT e atribuir a política a todos os computadores clientes. Selecione **Políticas** > criar **Novo**.

Básico

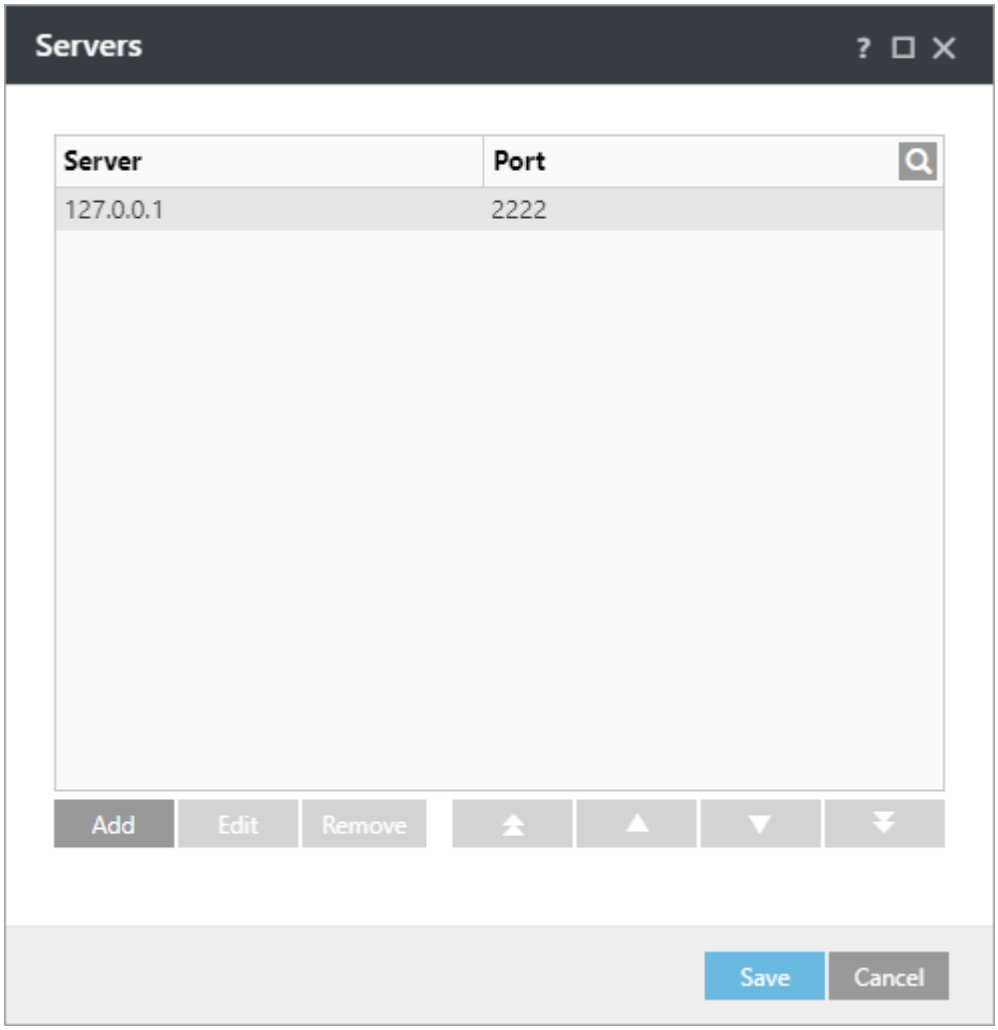
Digite um **Nome** para a política. O campo **Descrição** é opcional.

Configurações

Selecione **ESET ManagementAgente** do menu suspenso, abra **Conexão** e clique em **Editar lista de servidor** ao lado de **Servidores onde se conectar**.



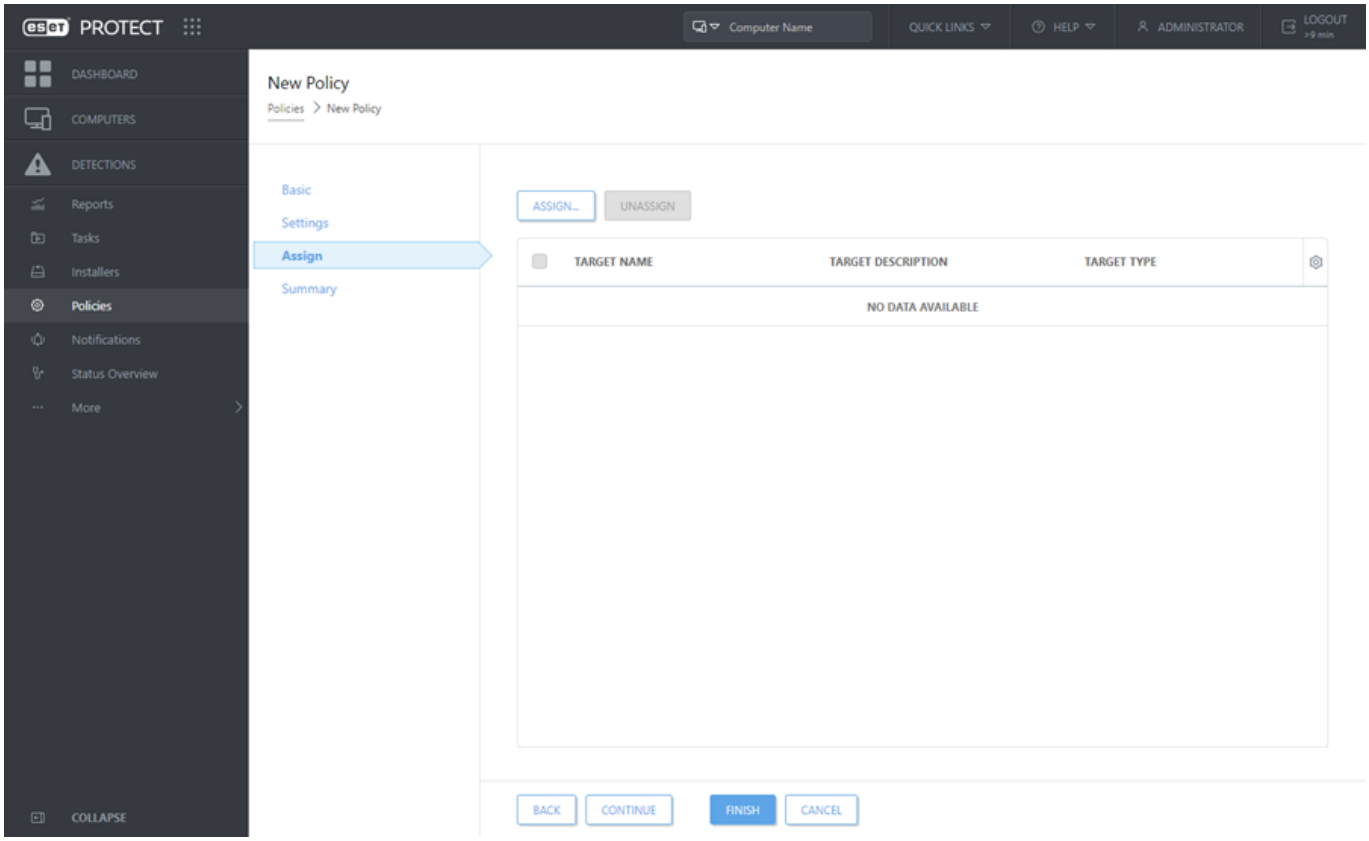
Uma janela será aberta com uma lista de endereços do Servidor ESET PROTECT aos quais o Agente ESET Management pode se conectar. Clique em **Adicionar** e digite o endereço IP do seu novo Servidor ESET PROTECT no campo **Host**. Se você estiver usando uma porta diferente da porta padrão do Servidor ESET PROTECT 2222, especifique seu número de porta personalizado.



Use botões de seta para alterar a prioridade de Servidores ESET PROTECT caso você tenha várias entradas na lista. Certifique-se de que seu novo Servidor ESET PROTECT está no topo, clicando no botão de **seta dupla** e clicando em **Salvar**.

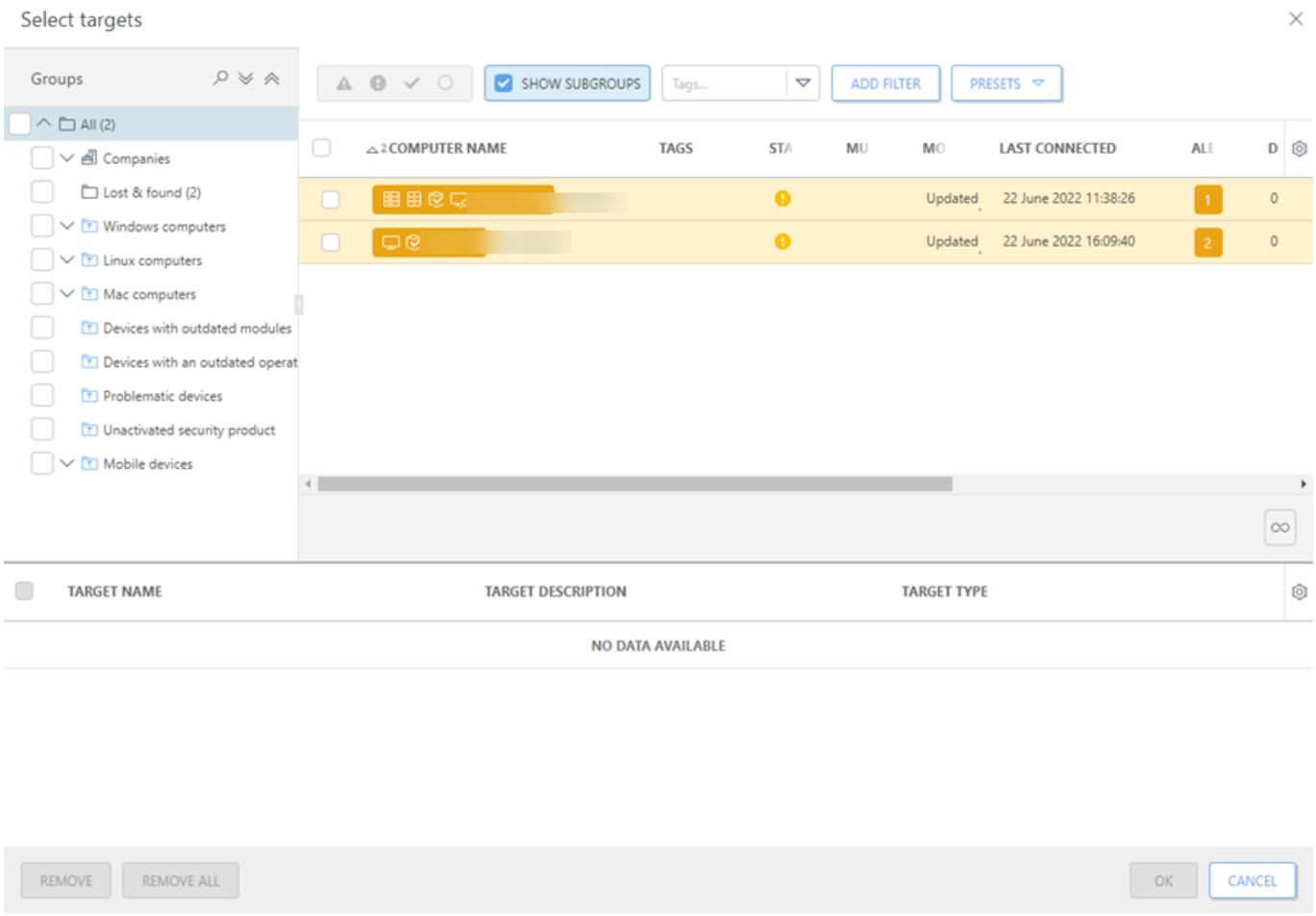
Atribuir

Especifique os clientes (computadores individuais/dispositivos móveis ou grupos inteiros) que serão os destinatários dessa política.



Clique em **Atribuir** para exibir todos os grupos estáticos e dinâmicos e seus membros. Selecione seus computadores ou grupos desejados e clique em **OK**.

Para atribuir todos os computadores em um grupo, atribua o grupo em vez de computadores individuais para impedir que a velocidade do Web Console diminua.
O Web Console exibirá um aviso se você selecionar um grande número de computadores.



Resumo

Verifique as configurações para esta política e clique em **Concluir**. A política é aplicada aos destinos depois da próxima conexão com o Servidor ESET PROTECT (dependendo do intervalo de conexão do agente).

Para aplicar a política imediatamente, você pode executar a ação **Enviar chamada para despertar** aos destinos nos **Computadores**.

Criar uma política para ativar a proteção de senha do Agente ESET Management

Siga as etapas abaixo para criar uma nova política que aplicará uma senha para proteger o Agente ESET Management. Quando **Configuração protegida por senha** é usada, o Agente ESET Management não pode ser desinstalado ou reparado a menos que uma senha seja fornecida. Consulte Proteção do agente para mais detalhes.

Básico

Digite um **Nome** para a política. O campo **Descrição** é opcional.

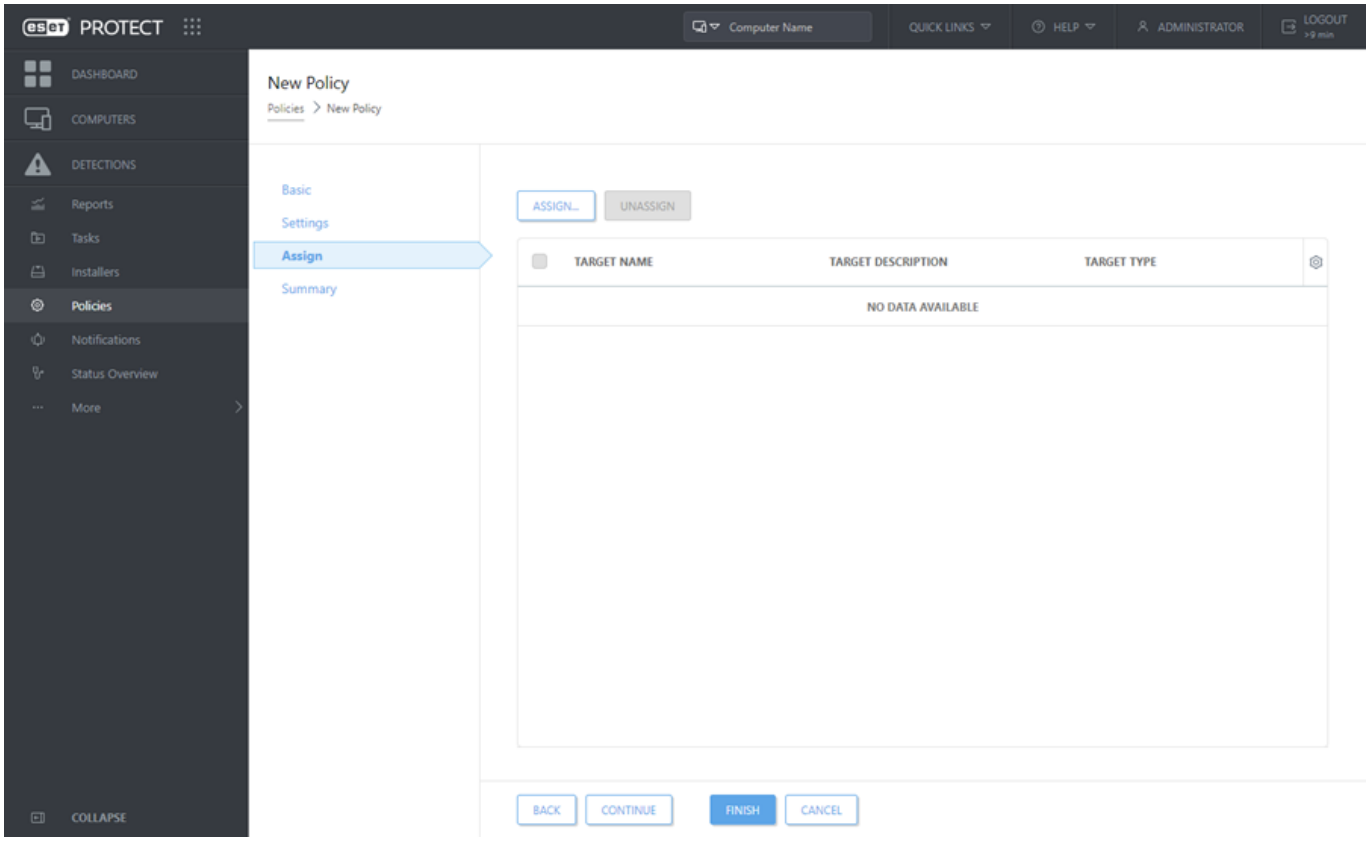
Configurações

Selecione **ESET ManagementAgente** na lista suspensa, abra **Configurações avançadas**, vá para **Configurações** e digite a senha no campo **Configuração protegida por senha**. Esta senha será necessária se alguém estiver tentando desinstalar ou reparar o Agente ESET Management em um computador cliente.

Certifique-se de registrar essa senha em um local seguro, é essencial inserir a senha para permitir a desinstalação do Agente ESET Management do computador do cliente. Não há outra maneira regular de desinstalar o Agente ESET Management sem uma senha correta a partir do momento que a política Configuração protegida por senha está em vigor.

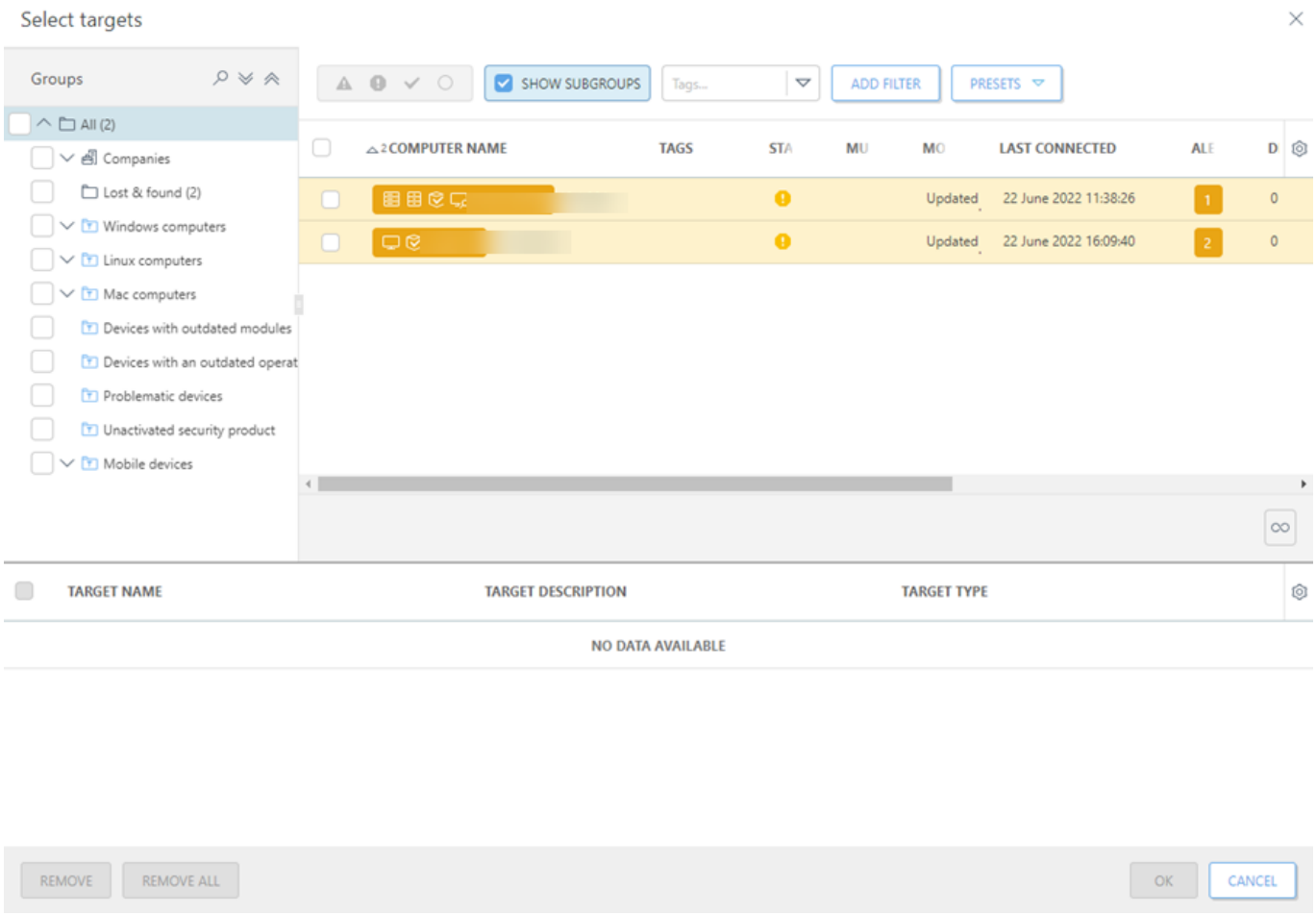
Atribuir

Especifique os clientes (computadores individuais/dispositivos móveis ou grupos inteiros) que serão os destinatários dessa política.



Clique em **Atribuir** para exibir todos os grupos estáticos e dinâmicos e seus membros. Selecione seus computadores ou grupos desejados e clique em **OK**.

Para atribuir todos os computadores em um grupo, atribua o grupo em vez de computadores individuais para impedir que a velocidade do Web Console diminua.
O Web Console exibirá um aviso se você selecionar um grande número de computadores.



Resumo

Verifique as configurações para esta política e clique em **Concluir**. A política é aplicada aos destinos depois da próxima conexão com o Servidor ESET PROTECT (dependendo do intervalo de conexão do agente).

> Para aplicar a política imediatamente, você pode executar a ação **Enviar chamada para despertar** aos destinos nos **Computadores**.

Solução de problemas - conexão de Agente

Quando um computador cliente não parece estar se conectando ao ESET PROTECT Servidor, recomendamos que você execute a solução de problemas do Agente ESET Management localmente na máquina do cliente.

Por padrão, o Agente ESET Management sincroniza com o Servidor ESET PROTECT a cada minuto. Você pode alterar essa configuração criando uma nova política para o Intervalo de conexão de agente ESET Management.

Verifique o relatório do Agente ESET Management mais recente. Isso pode ser encontrado aqui:

Windows	*C:\ProgramData\ESET\RemoteAdministrator\Agent\EraAgentApplicationData\Logs*
Linux	*/var/log/eset/RemoteAdministrator/Agent/* */var/log/eset/RemoteAdministrator/EraAgentInstaller.log*
macOS	*/Library/Application Support/com.eset.remoteadministrator.agent/Logs/* */Users/%user%/Library/Logs/EraAgentInstaller.log*

• **last-error.html** - protocolo (tabela) que exibe o último erro registrado enquanto o Agente ESET Management está em execução.

• **software-install.log** - protocolo de texto da última tarefa de instalação remota realizada pelo Agente ESET Management.

• **trace.log** - um relatório detalhado de toda a atividade do Agente ESET Management incluindo quaisquer erros que tenham sido registrados.

> 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).

• **status.html** - uma tabela que mostra o estado atual das comunicações (sincronização) do Agente ESET Management com o ESET PROTECT. Servidor. O relatório também contém a configuração do Proxy HTTP, uma lista de políticas aplicadas (inclusive as exclusões aplicadas) e uma lista de Grupos dinâmicos aos quais o dispositivo pertence.

> Recomendamos que você leia nosso artigo da Base de conhecimento sobre o uso do arquivo para a solução de problemas de conexão do Agente status.html.

Os problemas mais comuns que podem impedir o Agente ESET Management de se conectar ao Servidor ESET PROTECT são:

• Sua rede interna não está configurada adequadamente. Certifique-se de que o computador onde o Servidor ESET PROTECT está instalado pode se comunicar com os computadores clientes onde o Agente ESET Management está instalado.

• Seu servidor ESET PROTECT não está configurado para escutar na porta 2222.

• DNS não está funcionando corretamente, ou portas estão bloqueadas por um firewall - verifique nossa lista de portas usadas pelo ESET PROTECT, ou consulte o nosso artigo da base de conhecimento Quais endereços e portas em meu firewall de terceiros devo abrir para permitir a funcionalidade total para meu produto ESET?

• Um certificado gerado erroneamente contendo recursos falsos ou limitados que não combinam com a chave pública da Autoridade de Certificação do Servidor ESET PROTECT está implementado - crie um novo Certificado do Agente ESET Management para que isto seja solucionado.

Solução de problemas - Implantação do agente

Você pode se deparar com problemas durante a implantação do Agente ESET Management. Se a implementação falhar, há vários elementos que podem ser a causa. Esta seção ajudará você a:

- Descobrir a causa da falha de implantação do Agente ESET Management
- Verifique quanto a possíveis causas, de acordo com a tabela a seguir
- Solucionar o problema e realizar uma implantação com sucesso

Windows

1. Para descobrir o motivo de falha na implantação do Agente, vá para **Relatórios** > **Automação** e selecione **Informações de tarefas de implantação do agente nos últimos 30 dias**.
Uma tabela será exibida com informações de implementação. A coluna **Progresso** exibe mensagens de erro sobre o motivo de falha de implantação do agente.

Se você precisar de ainda mais detalhes, poderá alterar o detalhamento do relatório de rastreamento do Servidor ESET PROTECT. Navegue até **Mais** > Configurações > **Configurações avançadas** > **Registro em relatório** e selecione **Erro** no menu suspenso. Execute a implantação do Agente novamente e, quando falhar, verifique o relatório de rastreamento do Servidor ESET PROTECT em relação às entradas mais recentes do relatório, na parte inferior do arquivo. O relatório incluirá sugestões sobre como resolver o problema.

O arquivo mais recente pode ser encontrado aqui:

Relatório do Servidor ESET PROTECT	*C:\ProgramData\ESET\RemoteAdministrator\Server\EraServerApplicationData\Logs\trace.log*
Relatório do Agente ESET Management	*C:\ProgramData\ESET\RemoteAdministrator\Agent\EraAgentApplicationData\Logs*

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).
Em caso de problemas de conexão com o Agente ESET Management, consulte Solução de problemas - Conexão do Agente para obter mais informações.

2. A tabela abaixo contém vários motivos para falha de implementação do agente:

Mensagem de erro	Causa(s) possível(is)
Não foi possível se conectar	• O cliente não pode ser acessado na rede, o firewall bloqueia a comunicação • Portas de entrada 135, 137, 138, 139 e 445 não estão abertas no firewall no cliente ou Firewall do Windows: Permitir arquivo de entrada e exceção de compartilhamento de impressoras não é usado • Não foi possível resolver o nome do host do cliente, use nomes de computador FQDN válidos
Acesso negado	• Ao implantar de um servidor unido para um domínio, para um cliente unido para o domínio, use as credenciais de um usuário que seja membro do grupo Administrador do Domínio no formato: **Domínio\AdminDomínio** • Ao implantar a partir de um servidor unido a um domínio para um cliente unido ao domínio, você pode elevar temporariamente o serviço do Servidor ESET PROTECT do serviço de rede para ser executado sob a conta de administrador do domínio. • Ao implantar de um servidor para um cliente que não está em um mesmo domínio, desative a filtragem UAC remota no computador de destino. • Ao implantar de um servidor para um cliente em um domínio diferente, use as credenciais de um usuário local que seja membro do grupo Administradores no formato: **Admin**. O nome do computador de destino será adicionado automaticamente ao login. • Não há uma senha definida para a conta do administrador • Direitos de acesso insuficientes • O compartilhamento administrativo *ADMIN$* não está disponível • O compartilhamento administrativo *IPC$* não está disponível • Compartilhamento de arquivo simples está ativado
Pacote não encontrado no repositório	• O link para o repositório está incorreto • O repositório está indisponível • O repositório não contém o pacote necessário
Erro 1603	• Verifique o arquivo *ra-agent-install.log*. Pode ser encontrado aqui: *C:\Users\%user%\AppData\Local\Temp\ra-agent-install.log* no computador de destino. • Se o erro persistir, siga nosso artigo da Base de conhecimento.

3. Siga as etapas da solução de problemas adequadas de acordo com a causa possível:

- **O cliente não pode ser acessado na rede** - acesse o cliente a partir do Servidor ESET PROTECT; se você obtiver uma resposta, tente fazer logon na máquina cliente remotamente (por exemplo, via área de trabalho remota).

- **O firewall bloqueia a comunicação** - verifique as configurações de firewall no servidor e no cliente, bem como se há qualquer outro firewall entre essas duas máquinas (se aplicável).

- **Não foi possível resolver o nome do host do cliente** – possíveis soluções para problemas de DNS podem

incluir, mas não estão limitadas a:

- Usando o comando `nslookup` do endereço IP e nome de host do servidor e/ou os clientes tendo problemas de implantação do Agente. Os resultados devem corresponder às informações na máquina. Por exemplo, um `nslookup` de um nome de host deve ser resolvido para o endereço IP, um comando `ipconfig` é exibido no host em questão. O comando `nslookup` precisará ser executado nos clientes e no servidor.
- Como analisar manualmente registros DNS quanto a duplicatas.

• **As portas 2222 e 2223 não estão abertas no firewall** - mesmo que acima; certifique-se de que essas portas não estejam abertas em todos os firewalls entre as duas máquinas (cliente e servidor).

• **Não há uma senha definida para a conta do administrador** - defina a senha apropriada para a conta do administrador (não use uma senha em branco)

• **Direitos de acesso insuficientes** - tente usar as credenciais do Administrador do domínio ao criar a tarefa de implantação do Agente. Se a máquina cliente estiver em um grupo de trabalho, use a conta do administrador local nessa máquina específica.

> Depois da implantação realizada com êxito, as portas 2222 e 2223 não estão abertas no firewall. Certifique-se de que essas portas estejam abertas em todos os firewalls entre as duas máquinas (cliente e servidor).

• **Para ativar** a conta de usuário Administrador:

1. Abra um prompt de comando administrativo
2. Tipo o seguinte comando:

```
net user administrator /active:yes
```

• **O compartilhamento administrativo ADMIN$ não está disponível** - A máquina cliente deve ter o recurso *ADMIN$* ativado, certifique-se de que ele esteja presente entre outros compartilhamentos (**Iniciar** > **Painel de controle** > **Ferramentas administrativas** > **Gerenciamento de computador** > **Pastas compartilhadas** > **Compartilhamentos**).

• **O compartilhamento administrativo IPC$ não está disponível** - verifique se o servidor pode acessar *IPC$* ao emitir o seguinte prompt de comando no servidor:

`net use \\clientname\IPC$` onde `clientname` é o nome do computador de destino.

• **O uso de compartilhamento de arquivo simples está ativado** - se você estiver recebendo a mensagem de erro **Acesso negado** e tiver um ambiente misto (com domínio e grupo de trabalho), desative **Usar compartilhamento de arquivo simples** ou **Usar assistente de compartilhamento** em todas as máquinas nas quais está tendo problema com a implementação do Agente. Por exemplo, no Windows 7 faça o seguinte:

- Clique em **Iniciar**, digite `pasta` na caixa de **Pesquisa** e clique em **Opções de pasta**. Clique na guia **Visualizar** e, na caixa **Configurações avançadas**, role até a lista e desmarque a caixa de seleção **Usar assistente de compartilhamento**.

• **O link para o repositório está incorreto** - No Console da web ESET PROTECT, vá para **Mais** > Configurações, clique em **Configurações avançadas** > **Repositório** e certifique-se de que o URL do repositório esteja correto.

• **Pacote não encontrado no repositório** - essa mensagem de erro geralmente aparece quando não há conexão com o repositório ESET PROTECT. Verifique a sua conexão com a internet.

Linux e Mac OS

Se a implantação do Agente não funcionar em Linux ou macOS, isso geralmente é um problema relacionado a SSH. Verifique o computador cliente e certifique-se de que o daemon SSH esteja em execução. Assim que for corrigido, execute a implantação do Agente novamente.

Exemplo de cenários da implantação do Agente ESET Management

Esta seção contém quatro cenários verificados para implantação ESET PROTECT.

1.Implantação do Equipamento do servidor ESET PROTECT ou Servidor ESET PROTECT Linux nos destinos Windows não unidos a um domínio.

2.Implantação do Servidor ESET PROTECT Windows da origem do Windows não unido a um domínio para destinos do Windows não unidos ao domínio.

3.Implantação do Equipamento do servidor ESET PROTECT ou Servidor ESET PROTECT Linux nos destinos Windows unidos a um domínio.

4.Implantação do Servidor ESET PROTECT Windows da origem do Windows unido a um domínio para destinos do Windows unidos ao domínio.

Exemplo de cenários da implantação do Agente ESET Managementpara destinos não unidos ao domínio

As instruções abaixo cobrem esses cenários:

• Implantação do Equipamento do servidor ESET PROTECT ou Servidor ESET PROTECT Linux nos destinos Windows **não unidos a um domínio**.

• Implantação do Servidor ESET PROTECT Windows da origem do Windows não unido a um domínio para destinos do Windows **não unidos ao domínio**.

Pré-condições:

• Mesma rede local.

• Nomes funcionando do FQDN, por exemplo: desktop-win7.test.local mapeia para 192.168.1.20 e vice versa.

• Sistema operacional limpo instalado do MSDN com padrões.

Destinos:

Windows 10 Enterprise

Windows 8.1 Enterprise

Windows 7 Enterprise

1. Criar um usuário com senha que seja membro do grupo de Administradores, por exemplo: **Admin**.

   a.Abra o **Console de gerenciamento Microsoft** abrindo o console **Executar** e digitando "`mmc`" no campo e clicando em **OK**.

   b.Adicione o Snap-in **Usuários e grupos locais** de **Arquivo** > **Adicionar/remover Snap-in**. Adicione um novo usuário na pasta **Usuários** e preencha as informações solicitadas nos campos (não se esqueça de preencher a senha). Na seção **Grupos** abra as **Propriedades** do grupo **Administradores** e adicione o usuário criado recentemente no grupo clicando no botão **Adicionar**. Preencha o nome de login do novo usuário criado em **Inserir nomes de usuário a selecionar** e verifique clicando no botão **Verificar nomes**.

2. Na **Central de rede e compartilhamento** altere a configuração de rede de **Rede pública** para **Rede particular** clicando em **Rede pública** no canto esquerdo da **seção Visualizar suas redes ativas**.

3. Desative o **Firewall do Windows** para a **Rede particular** clicando em **Ligar ou desligar Firewall do Windows** e selecionando **Desligar Firewall do Windows** nas Configurações de localização de rede doméstica **ou de trabalho**.

4. Verifique se **Compartilhamento de arquivo e impressora** está ativado para a **Rede particular** clicando em **Alterar configurações avançadas de compartilhamento** no **Centro de rede e compartilhamento**.

5. Desativar as restrições remotas de User Account Control (UAC):

   a.Abra o **Editor de registro** digitando `regedit` no console **Executar** e localize `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System`

   b.No arquivo **Sistema**, crie um novo **Valor DWORD** com o nome `LocalAccountTokenFilterPolicy`.

   c.Abra o arquivo criado e defina os **Dados de valor** como **1**.

Console da Web ESET PROTECT:

No Web Console ESET PROTECT, crie uma nova tarefa do servidor de Implantação do agente:

1. **Destinos** – selecione computadores Windows de destino.

2. **Nome de host do servidor (opcional)** – digite o nome FQDN ou endereço IP do Servidor ESET PROTECT. (Você pode encontrar o nome FQDN da máquina clicando com o botão direito do mouse em **Computador** e selecionando **Propriedades**. O nome FQDN aparece ao lado do **Nome completo do computador**).

3. **Nome de usuário** – digite **Admin** (nenhum nome de domínio ou prefixo de nome do computador) e digite a **Senha** para este usuário.

4. **Certificado ESET PROTECT** – clique em **Nenhum certificado selecionado** e selecione o **Certificado do Agente.**

5. Clique em **Concluir** para executar a tarefa.

Exemplo de cenários da implantação do Agente ESET Managementpara destinos unidos ao domínio

As instruções abaixo cobrem esses cenários:

- Implantação do Equipamento do servidor ESET PROTECT ou Servidor ESET PROTECT Linux nos destinos Windows **unidos a um domínio**.

- Implantação do Servidor ESET PROTECT Windows da origem do Windows unido a um domínio para destinos do Windows **unidos ao domínio**.

Pré-condições:

- Mesma rede local.

- Nomes do FQDN que funcionem, por exemplo: desktop-win10.protect.local mapeia para 10.0.0.2 e vice versa.

- Sistema operacional limpo instalado do MSDN com padrões.

- Domínio criado `protect.local` com nome netbios `PROTECT`.

- Usuário criado `DomainAdmin` que é membro do grupo de segurança `Domain Admins` no controlador de domínio.

- Cada máquina entrou em um domínio `protect.local` com um usuário `DomainAdmin` e este usuário é o Administrador.

- `DomainAdmin` consegue fazer login em cada máquina e realizar tarefas da administração local.

- O serviço do Servidor ESET PROTECT do Windows está sendo executado temporariamente sob as credenciais `PROTECT\DomainAdmin`. Depois da implantação, a conta de **Serviço de rede** é suficiente (nenhuma alteração é necessária na Máquina virtual ou no Linux).

Destinos:

Windows 10 Enterprise

Windows 8.1 Enterprise

Windows 7 Enterprise

1. Abra a **Central de rede e compartilhamento**.

2. Verifique se a rede é uma **Rede de domínio** na seção **Ver suas redes ativas**.

3. Desative o **Firewall do Windows** para a **Rede de domínio** clicando em **Ligar ou desligar Firewall do Windows** e selecionando **Desligar Firewall do Windows** nas **Configurações de localização de rede de domínio**.

4. Verifique se **Compartilhamento de arquivo e impressora** está ativado para a **Domínio de rede** clicando em **Alterar configurações avançadas de compartilhamento** no **Centro de rede e compartilhamento**.

Console da Web ESET PROTECT:

No Web Console ESET PROTECT, crie uma nova tarefa do servidor de Implantação do agente:

1. **Destinos** – selecione computadores Windows de destino.

2. **Nome de host do servidor (opcional)** – digite o nome FQDN ou endereço IP do Servidor ESET PROTECT. (Você pode encontrar o nome FQDN da máquina clicando com o botão direito do mouse em **Computador** e selecionando **Propriedades**. O nome FQDN aparece ao lado do **Nome completo do computador**).

3. **Nome de usuário** – digite **PROTECT\DomainAdmin** (é importante incluir todo o domínio) e digite a **Senha** para este usuário.

4. **Certificado ESET PROTECT** – clique em **Nenhum certificado selecionado** e selecione o **Certificado do Agente.**

5. Clique em **Concluir** para executar a tarefa.

ESET PROTECT Menu principal

Todos os clientes são gerenciados por meio do ESET PROTECTConsole da Web. Você pode acessar o Console da Web ESET PROTECT de qualquer dispositivo usando um navegador compatível. O **Menu principal**está sempre acessível à esquerda, exceto ao usar um Assistente. Clique em para abrir o menu no lado esquerdo da tela, ele pode ser fechado clicando em **Fechar**.

O menu principal à esquerda contém as principais seções do ESET PROTECT e os seguintes itens:

Painel
Computadores
Detecções
Relatórios
Tarefas
Instaladores
Políticas
Notificações
Visão geral do status
Mais

Painel

O painel é a página padrão que é exibida depois que você entra no console da Web ESET PROTECT pela primeira vez. Ele exibe relatórios pré-definidos sobre sua rede. Você pode alternar entre os painéis usando as guias na barra de menus superior. Cada painel consiste em vários relatórios.

Manipulação do painel

- **Adicionar** – Clique no símbolo + na parte superior do cabeçalho do painel para adicionar um novo painel. Insira um nome para o novo Painel e clique em **Adicionar painel** para confirmar. Um novo painel em branco é criado.

- **Mover** - Clique e arraste o nome de um painel para alterar sua localização em relação a outros painéis.

- Você pode personalizar seus painéis adicionando, modificando, redimensionando, movendo e reorganizando relatórios.

- Selecione o painel, clique no ícone de engrenagem ao lado do e selecione **Definir como padrão** para usar seu painel como um painel padrão para todos os novos usuários do Web Console com acesso aos Painéis.

Clique no ícone de engrenagem ao lado do título do painel selecionado para obter as seguintes opções no menu suspenso:

Atualizar página	Atualiza os modelos de relatório neste painel.
Remover	Remover um painel.
Renomear	Renomear um painel.
Duplicar	Criar uma cópia do painel com os mesmos parâmetros no grupo inicial do usuário.
Alterar layout	Escolha um novo layout para esse painel. A alteração vai remover os modelos atuais do painel.

Não é possível personalizar esses painéis padrão: **Visão geral do status**, **Visão geral de segurança** e **ESET LiveGuard**.

O ESET Enterprise Inspector e o ESET Dynamic Threat Defense foram renomeados para ESET Inspect e ESET LiveGuard Advanced.
Você pode precisar resolver os problemas causados pela renomeação se você atualizou do ESET PROTECT 9.0 e versões anteriores e tem relatórios, grupos dinâmicos, notificações ou outros tipos de regras que filtram por ESET Dynamic Threat Defense ou ESET Enterprise Inspector.

Os painéis a seguir vêm pré-configurados no ESET PROTECT:

Visão geral do status

O painel **Visão geral do status** é a tela padrão que você vê ao entrar no ESET PROTECT (a menos que você defina outro painel como o padrão). Ele exibe informações gerais sobre sua rede.

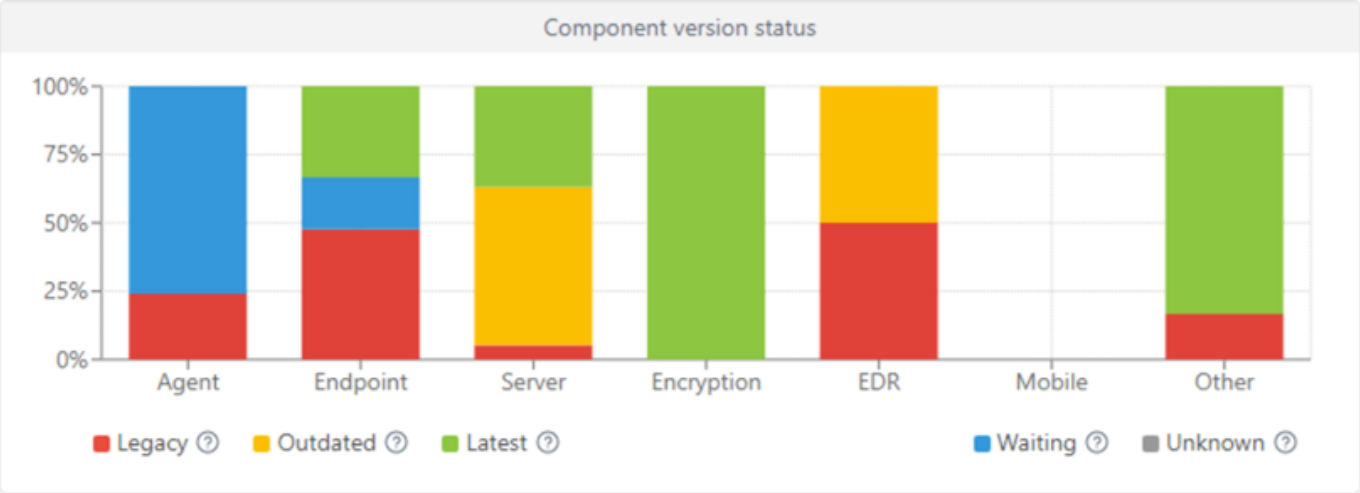
Filtros de dispositivo - Exibe o número de dispositivos gerenciados com base nos status reportados mais recentes. Você pode clicar em cada um dos 4 blocos para abrir uma lista filtrada de dispositivos.

Status do dispositivo - Exibe o número de dispositivos gerenciados com base no tipo de produto de segurança instalado nas respectivas guias. Se nenhum produto de segurança daquele grupo está implantado, a guia vai exibir uma opção para implantar o respectivo pacote do instalador.

Status de conexão - Exibe a lista de conexões recentes de dispositivos gerenciados.

Status da versão do componente

O gráfico exibe a taxa de versões de componentes ESET atualizados e desatualizados ou versões dos produtos de segurança ESET.



Clique no gráfico amarelo/vermelho representando componentes ou aplicativos desatualizados e selecione **Atualizar componentes ESET instalados** para iniciar uma atualização. Veja também a [política de Fim da vida útil ESET para produtos empresariais].

- **Vermelho** (**Legado**) – uma versão legado do componente/produto ESET ou uma versão anterior com uma vulnerabilidade de segurança descoberta que não é mais compatível e que não está mais no repositório ESET.

- **Amarelo** (**Desatualizado**) – a versão instalada do componente/produto ESET está desatualizada, mas ainda é compatível. Normalmente, duas versões mais antigas do que a versão mais recente estão no estado amarelo a menos que contenham uma vulnerabilidade de segurança descoberta recentemente.

- **Verde** (**OK**) – a versão mais recente do componente/produto ESET está instalada ou a versão instalada é a versão mais recente do componente/produto ESET compatível com o Web Console ESET PROTECT usado.

> Versões anteriores do componente/produto ESET reportam **OK** (**verde**) no gráfico se não houver uma versão mais nova compatível de componente/produto no repositório ESET para a versão ou plataforma do sistema operacional específico (x86, x64, ARM64).

- **Azul** (**Aguardando**) – as atualizações automáticas estão ativadas e a versão mais recente será instalada automaticamente. Leia mais detalhes sobre as atualizações automáticas de:

  - ESET Management Agentes

oProdutos de Segurança ESET

> Se os componentes ESET não estão sendo atualizados por um período de tempo longo, você pode atualizá-los manualmente clicando no gráfico azul e selecionando **Atualizar componentes ESET instalados**.
> Alternativamente, você pode usar a Tarefa do cliente ESET PROTECT Atualização de Componentes para atualizar Agentes e a Tarefa do cliente Instalação de Software para atualizar os produtos de segurança ESET.

• **Cinza** (**Desconhecido**) – a versão do componente/produto ESET não é reconhecida (por exemplo, logo depois de uma nova instalação do produto ESET).

Status de gerenciamento - Exibe o número de dispositivos **Gerenciados e protegidos** (dispositivos de clientes com o Agente ESET e com um produto de segurança instalado), **Gerenciado** (dispositivos de cliente apenas com o Agente), **Não gerenciados**(dispositivos de cliente na sua rede que o ESET PROTECT conhece mas que não tem o Agente) e **Invasores** (dispositivos de cliente desconhecidos para o ESET PROTECT mas detectados pelo Rogue Detection Sensor).

Feed RSS - Exibe um feed RSS do WeLiveSecurity e do Portal da Base de Conhecimento ESET. Quando você clica no ícone de engrenagem no **feed RSS**, pode escolher **Desligar reprodução automática do feed**, ou desligar a origem individual do feed ou **Desligar feed RSS**.

Visão geral de incidentes

Esse painel oferece uma visão geral de detecções não resolvidas descobertas nos últimos 7 dias, incluindo sua gravidade, método de detecção, status de resolução e 10 principais computadores/usuários com detecções.

ESET LiveGuard

Se estiver usando o ESET LiveGuard Advanced, você encontrará aqui uma visão geral de relatórios úteis do ESET LiveGuard Advanced. Clique no ícone de engrenagem em cima (ao lado de) e selecione **Ocultar/Exibir ESET LiveGuard** para ocultar/exibir o painel.

Computadores

Esse painel oferece a você uma visão geral de máquinas cliente, inclusive seu status de proteção, sistemas operacionais e status de atualização.

Status de desempenho do servidor

Nesse painel, você pode visualizar informações sobre o próprio servidor ESET PROTECT, incluindo carga do servidor, clientes com problemas, carga de CPU e conexões de banco de dados.

Detecções de antivírus

Aqui você pode ver relatórios do módulo antivírus dos produtos de segurança de cliente, inclusive detecções ativas, detecções nos últimos 7/30 dias e assim por diante.

Detecções de firewall

Eventos de firewall dos clientes conectados organizados de acordo com sua gravidade, tempo de relatório, etc.

Aplicativos ESET

Este painel permite que você visualize informações sobre os aplicativos instalados da ESET.

Proteção baseada em nuvem

Esse painel oferece a você uma visão geral dos relatórios de proteção baseada em nuvem (ESET LiveGrid® e, se você tiver uma licença elegível, também ESET LiveGuard Advanced).

Ações em um relatório do painel

Redimensionar	Clique para visualizar um relatório no modo de tela inteira.
Atualizar	Atualize o modelo de relatório.
Fazer download	Clique em **Download** para gerar e fazer download do relatório. Você pode escolher de *.pdf* ou *.csv*. CSV é adequado apenas para dados da tabela e usa `;` (ponto e vírgula) como delimitador. Se você fizer download de um relatório CSV e ver os números em uma coluna onde você espera um texto, recomendamos fazer download de um relatório PDF para ver os valores em texto.
Alterar	Altera o modelo de relatório para outro da lista de modelos.
Editar modelo de relatório	Edite um modelo de relatório existente. As mesmas configurações e opções usadas para criar um novo modelo de relatório são aplicáveis.
Definir intervalo de atualização	Define intervalos de atualização personalizados para o modelo.
Agendar	Agendar um relatório – Você pode modificar o acionador do agendamento, o throttling e a entrega de relatórios. Você pode encontrar todos os relatórios agendados na guia **Relatórios agendados** .
Remover	Remover o modelo de relatório do painel.
Renomear	Renomeie o modelo de relatório.
Essa célula	Escolha um novo layout para esse painel. A alteração vai remover os modelos atuais do painel.

Permissões para o Painel

Um usuário deve ter permissão apropriada para trabalhar com Painéis. Apenas modelos de relatório contidos em um grupo onde o usuário tem direitos de acesso podem ser usados em um Painel. Se o usuário não tiver direitos atribuídos para **Relatórios e Painel**, o usuário não verá nenhum dado na seção Painel. O administrador pode ver todos os dados por padrão.

- **Leitura** - o usuário pode listar modelos de relatório e suas categorias. O usuário também pode gerar relatórios com base nos modelos de relatório. O usuário é capaz de ler seu painel.
- **Uso** - o usuário pode modificar seu painel com modelos de relatório disponíveis
- **Gravação** - Cria / modifica / remove modelos de relatório e suas categorias.

Todos os modelos padrão estão localizados no grupo *Todos*.

Detalhamento

Você pode usar a funcionalidade de detalhamento do painel para examinar os dados em mais detalhes. Ela deixa que você selecione de forma interativa itens específicos para um resumo e veja dados detalhados sobre eles. Foca no item de interesse para obter um "detalhamento" das informações de resumo, a fim de ter mais informações sobre esse item específico. Geralmente há vários níveis de detalhamento.

Existem várias opções de detalhamento:

- Exibir **informações detalhadas** - Nome e descrição do computador, nome do Grupo estático, etc. Exibe os dados originais (não agregados) para a fileira clicada.

- Exibir **apenas o '***valor***'** - Mostra apenas os dados com o nível de gravidade selecionado: Informações, Crítico, Risco de segurança, Notificação de segurança, etc.

- **Expanda a coluna '***valor***'** - Isso vai mostrar as informações agregadas (normalmente para contagem ou soma). Por exemplo, se houver apenas um número na coluna e você clicar em Expandir coluna do computador, ele irá listar todos os detalhes sobre os computadores.

- Exibir **Na página Computadores (todos)** - Redireciona você para a página **Computadores** (exibe um resultado de apenas 100 itens).

Ações com um clique

Relatórios com informações sobre os problemas descobertos contém opções de detalhamento adicionais quando você clica no item na tabela/gráfico:

- '*tarefa para resolver o alerta selecionado*' – Você pode resolver o alerta selecionando a tarefa sugerida, que será executada o mais rápido possível.

  Se o alerta não puder ser resolvido por meio de uma tarefa, mas puder ser resolvido por uma configuração de política, as seguintes opções serão exibidas:

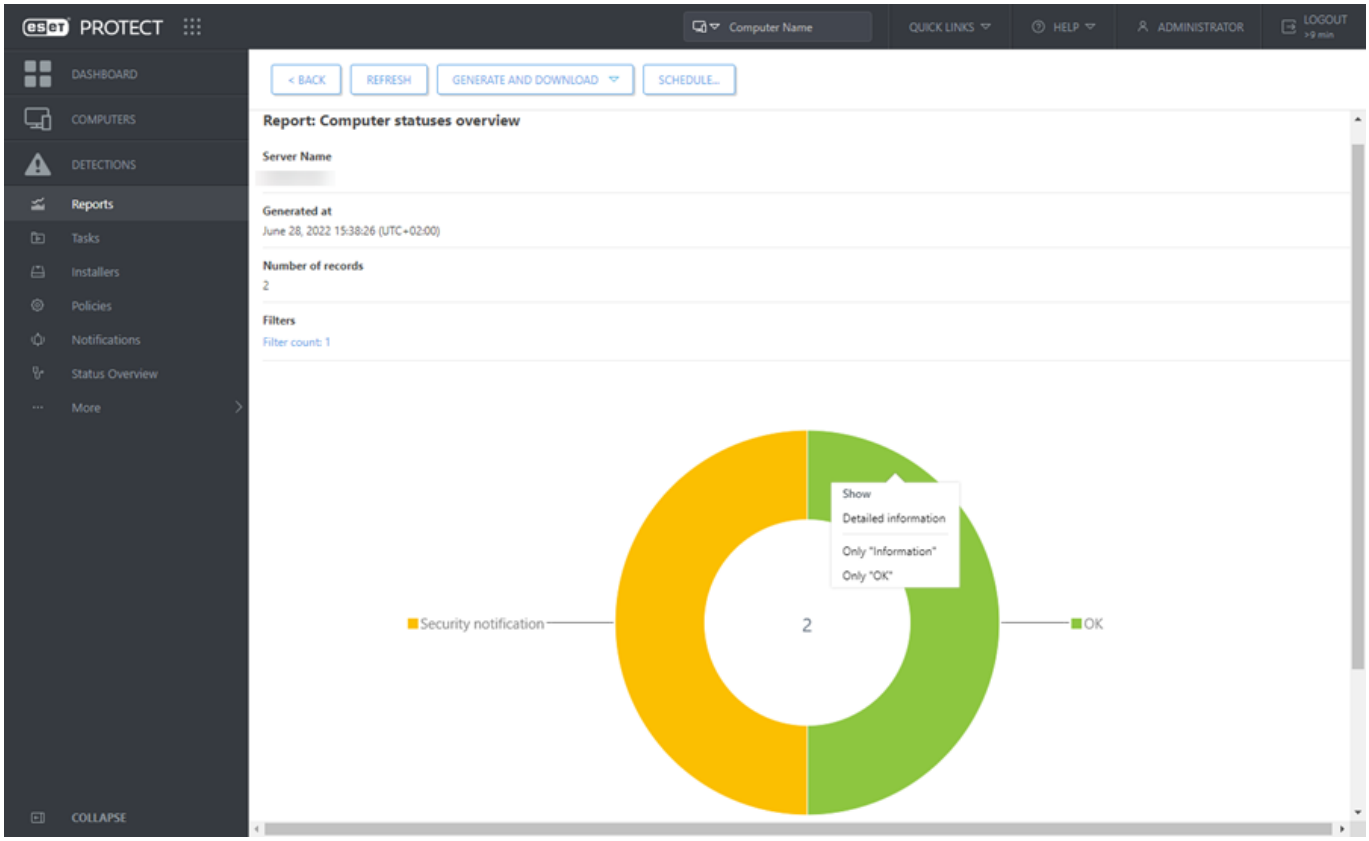
  - **Gerenciar políticas**

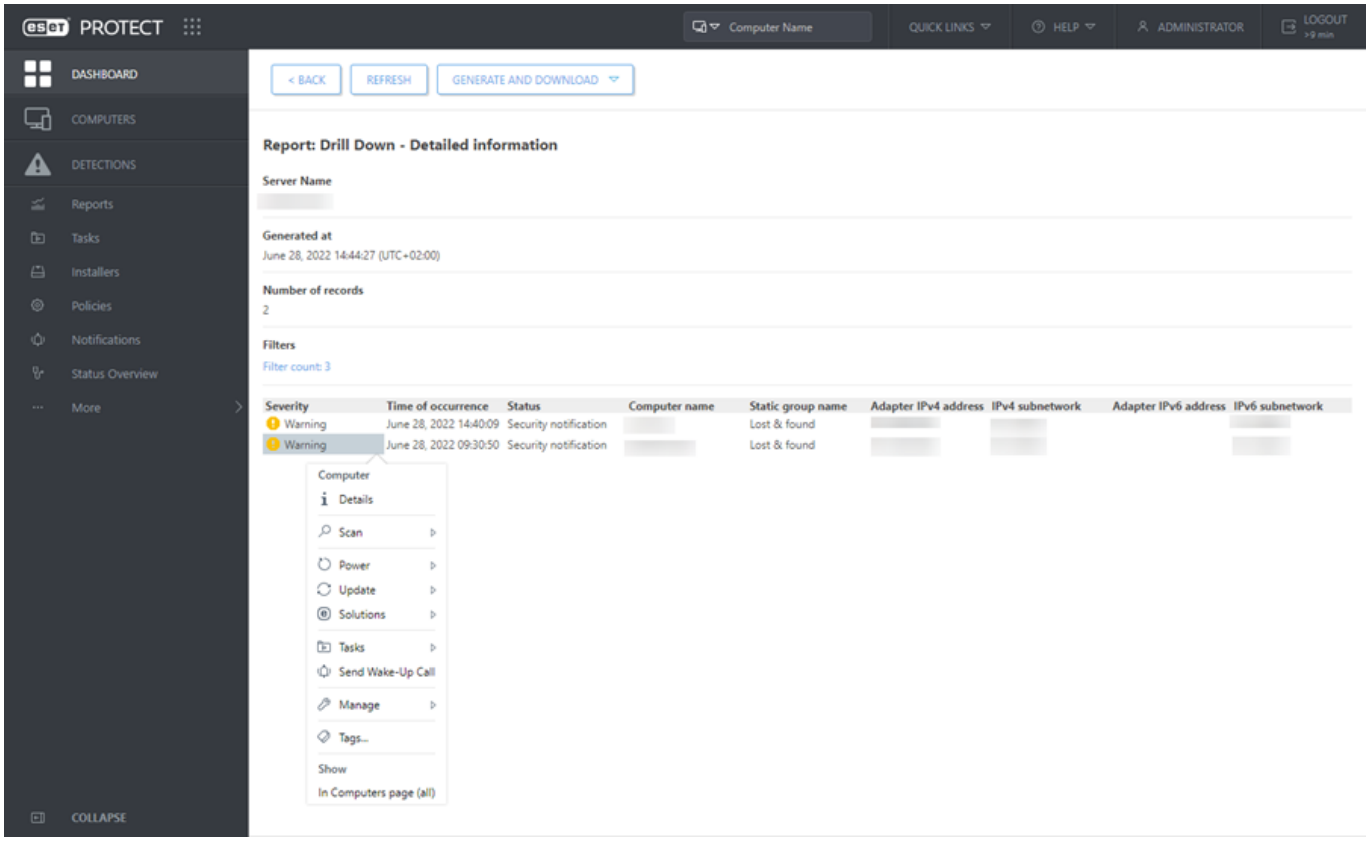
  - **Nova política**

- **Pesquisar na Web** - Aciona a pesquisa Google para o alerta selecionado. Você pode usar esta opção se não houver resposta sugerida (configuração de tarefa ou política) para resolver o alerta selecionado.

> Os resultados obtidos usando o detalhamento de outros relatórios mostram somente os primeiros 1.000 itens.

Clique no botão **Gerar e fazer download** se quiser gerar e fazer download do relatório. Você pode escolher de *.pdf* ou *.csv*. CSV é adequado apenas para dados da tabela e usa `;` (ponto e vírgula) como delimitador. Se você fizer download de um relatório CSV e ver os números em uma coluna onde você espera um texto, recomendamos fazer download de um relatório PDF para ver os valores em texto.





Computadores

Todos os dispositivos cliente que foram adicionados ao ESET PROTECT são mostrados aqui e são divididos em Grupos. Cada dispositivo é atribuído a um único grupo estático. Clicar em um grupo na lista (à esquerda) exibirá os membros (clientes) desse grupo no painel direito.

Computadores **não gerenciados** (clientes na rede que não têm o Agente ESET Management instalado) geralmente aparecem no grupo **Perdido e encontrado**. O status de um cliente que é exibido no console da Web ESET PROTECT é independente das configurações do produto de segurança ESET no cliente. É por isso que, mesmo se um determinado status não for exibido no cliente, ele ainda é reportado no console da Web ESET PROTECT. Você pode arrastar e soltar clientes para movê-los entre os grupos.

Clique no botão **Adicionar dispositivo** e selecione:

- **Computadores** - Você pode adicionar computadores ao grupo estático selecionado.
- **Dispositivos móveis** - Você pode adicionar dispositivos móveis ao grupo estático selecionado.
- **Sincronizar via servidor do diretório** - Você pode executar a tarefa de Sincronização do grupo estático.

Clique em um dispositivo para abrir um novo menu com ações disponível para aquele dispositivo. Você também pode selecionar a caixa de marcação ao lado de um dispositivo e clicar no botão **Computador** na barra inferior. O menu **Computador** vai exibir opções diferentes dependendo do tipo de dispositivo. Consulte a legenda de Ícones para detalhes sobre tipos de ícones e status diferentes. Clique no número de alertas na coluna **Alertas** para ver a lista de alertas na seção detalhes do computador.

Última conexão exibe a data e hora da última conexão do dispositivo gerenciado. Um ponto verde indica que o computador se conectou há menos de 10 minutos. As informações da **Última conexão** são destacadas para indicar que o computador não está se conectando:

- Amarelo (erro) – O computador não conecta há 2-14 dias.
- Vermelho (aviso) – O computador não conecta há mais de 14 dias.

O ícone **Inspect** abre a seção Computadores do ESET Inspect Web Console. Om ESET Inspect está disponível apenas quando você tem a licença ESET Inspect e o ESET Inspect conectado ao ESET PROTECT. Um usuário do Web Console precisa de permissão de **Leitura** ou acima para **Acessar o ESET Inspect** ou permissão de **Leitura** ou acima para o **Usuário ESET Inspect**.

Filtragem de visualização

Existem formas diferentes de filtrar sua visualização:

- Filtro padrão: Para adicionar critérios de filtragem, clique em **Adicionar filtro** e selecione um item da lista. Digite as strings de pesquisa ou selecione os itens no menu suspenso no(s) campo(s) de filtro(s) e pressione **Enter**. Filtros ativos são destacados em azul.

- Você pode filtrar por gravidade usando os ícones de status: vermelho – **Erros**, amarelo – **Avisos**, verde – **OK** e cinza – computadores **não gerenciados**. O ícone de gravidade representa o status atual do seu produto ESET em um determinado computador cliente. Você pode usar uma combinação desses ícones ativando-os ou desativando-os. Por exemplo, para ver somente os computadores com advertências, deixe somente o ícone amarelo selecionado ativado (o restante se os ícones deverem estar desmarcados). Para ver ambos, advertências e erros, deixe somente esses dois ícones ativados.

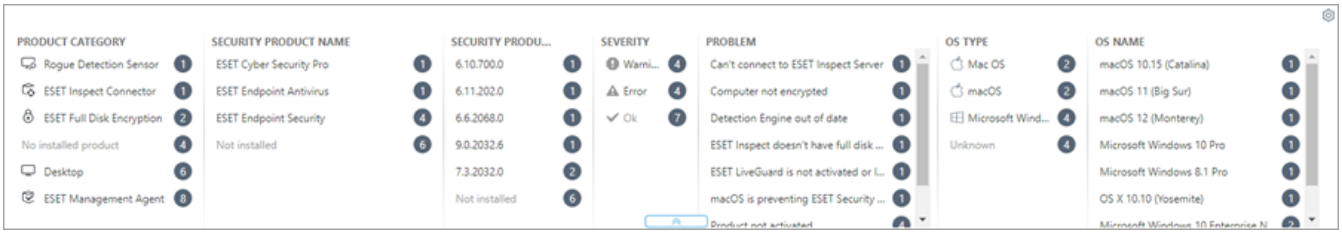
- Clique em **Adicionar filtro > Categoria de produto** e, usando o menu suspenso abaixo dos filtros, você pode selecionar os tipos de dispositivos a serem exibidos.

  - **Todos os dispositivos** -selecione esta opção do menu suspenso para ver todos os computadores cliente

novamente, sem limitar (filtrar) os clientes exibidos. Você pode usar uma combinação de todas as opções de filtro ao refinar a visualização.

- **Protegido pela ESET** - protegido por um Produto ESET.
- **ESET PROTECT** - componentes ESET PROTECT individuais como Agente, RD Sensor, Servidor, etc.
- **Outros** – Shared Local Cache, Equipamento de segurança virtual, Conector ESET Inspect, ESET Full Disk Encryption.

- Caixa de seleção **Exibir Subgrupos** - mostra subgrupos do grupo atualmente selecionado.
- Você pode ver os **Filtros avançados** como um painel de filtro expandível na tela **Computadores**.



Filtros avançados mostram uma visualização em tempo real de valores para vários filtros e o número exato de resultados para sua seleção.

Ao filtrar grandes conjuntos de computadores, os filtros avançados mostram quais valores de filtro vão obter um número gerenciável de resultados, permitindo que você encontre os dispositivos certos muito mais rapidamente.

Clique nos itens nas colunas para aplicar o filtro. Os filtros aplicados aparecem na parte superior dos filtros avançados como uma lista azul. Clique no filtro aplicado para alternar entre o valor **igual** ou **não igual**.

Clique no ícone de engrenagem em uma coluna para classificar os valores na coluna ou clique no ícone de engrenagem na parte superior dos filtros avançados. Usa o assistente para ajustar (adicionar, remover, reordenar) as colunas exibidas. Você também pode usar o recurso de arrastar e soltar para ajustar as colunas. Clique em **Redefinir** para redefinir as colunas da tabela para seu estado padrão (colunas disponíveis padrão em uma ordem padrão).

> Você pode usar filtros avançados apenas com Grupos estáticos. Grupos dinâmicos não são compatíveis com filtros avançados.

- Use Grupos dinâmicos ou Relatórios para uma filtragem mais avançada.
- Para encontrar os computadores marcados como Mestre para clonagem, clique em **Adicionar filtro** > selecione **Mestre para clonagem** > selecione a caixa de seleção ao lado do filtro **Mestre para clonagem**.

Filtros e personalização de layout

Você pode personalizar a exibição da tela atual do console web:

- Gerenciar o painel lateral e a tabela principal.
- Adicionar filtro e predefinições de filtro. Você pode usar marcações para filtrar os itens exibidos.

> Caso você não consiga localizar um determinado computador na lista e souber que ele está na infraestrutura ESET PROTECT, certifique-se de que todos os filtros estejam desativados.

Detalhes do computador

Para descobrir detalhes sobre um computador, selecione um computador cliente no grupo Estático ou Dinâmico e clique em **Detalhes** ou clique no nome do computador para exibir o painel lateral Visualização do computador no lado direito.

O ícone **Inspect** abre a seção Computadores do ESET Inspect Web Console. Om ESET Inspect está disponível apenas quando você tem a licença ESET Inspect e o ESET Inspect conectado ao ESET PROTECT. Um usuário do Web Console precisa de permissão de **Leitura** ou acima para **Acessar o ESET Inspect** ou permissão de **Leitura** ou acima para o **Usuário ESET Inspect**.

A janela de informações é composta pelas partes a seguir:

Visão geral:

Computador

- Clique no ícone editar para alterar o nome ou descrição do computador. Você pode selecionar **Permitir nome duplicado** se já houver outro computador gerenciado com o mesmo nome.
- Clique em **Selecionar marcações** para atribuir marcações.
- **FQDN** - Nome do domínio totalmente qualificado do computador

> Se você tiver os computadores cliente e o Servidor ESET PROTECT sendo executados no Active Directory, é possível automatizar o preenchimento dos campos **Nome** e **Descrição** usando a tarefa de Sincronização de grupo estático.

- **Grupo principal** - muda o Grupo estático principal do computador.
- **IP** - o endereço IP da máquina.
- **Contagem de políticas aplicadas** - Clique no número para ver uma lista de políticas aplicadas.
- **Membro de grupos dinâmicos** - A lista de grupos dinâmicos na qual o computador cliente está presente durante a última replicação.

Hardware

Esse bloco contém uma lista de parâmetros chave de hardware, informações sobre o sistema operacional e identificadores exclusivos. Clique no bloco para ver a guia **Detalhes - Hardware**. Veja também o inventário de

hardware.

Alertas

- **Alertas** - Link para a lista de problemas com o computador atual.

- **Contagem de detecções não resolvidas** – contagem de detecções não resolvidas. Clique na contagem para ver a lista de detecções não resolvidas.

- **Tempo conectado na última vez** -**Última conexão** exibe a data e hora da última conexão do dispositivo gerenciado. Um ponto verde indica que o computador se conectou há menos de 10 minutos. As informações da **Última conexão** são destacadas para indicar que o computador não está se conectando:

  - Amarelo (erro) – O computador não conecta há 2-14 dias.

  - Vermelho (aviso) – O computador não conecta há mais de 14 dias.

- **Hora da última inicialização** – a data e hora da última inicialização do dispositivo gerenciado. O computador gerenciado deve executar o Agente ESET Management 10.0 e versões posteriores, veja o **Último horário de inicialização**. Um Agente anterior reporta o **n/a**.

- **Hora do último escaneamento** – informações de horário do último escaneamento.

- **Mecanismo de detecção** - Versão do mecanismo de detecção no dispositivo de destino.

- **Atualizado** - O status de atualização.

Produtos e licenças

Lista de componentes ESET instalados no computador. Clique no bloco para ver a guia **Detalhes - Produto e licenças**.

Criptografia

O bloco de criptografia pode ser visto apenas em estações de trabalho compatíveis com o ESET Full Disk Encryption.

- Clique em **Criptografar computador** para iniciar o assistente para ativar criptografia.

- Quando a criptografia estiver ativa, clique em **Gerenciar** para gerenciar as opções de criptografia.

- Se o usuário não conseguir entrar com sua senha ou se não for possível acessar os dados criptografados na estação de trabalho devido a um problema técnico, o administrador pode iniciar o processo de recuperação de criptografia.

ESET LiveGuard Advanced

O bloco fornece informações básicas sobre o serviço. Ele pode ter dois blocos de status:

- Branco – o estado padrão. Depois que o ESET LiveGuard Advanced é ativado e está funcionando, o bloco ainda está no estado branco.

- Amarelo – se houver um problema com o serviço ESET LiveGuard Advanced, o bloco ficará amarelo e

exibirá as informações sobre o problema.

Ações disponíveis:

- **Ativar** – esta opção estará disponível depois que você importar a licença do produto. Clique para configurar a tarefa de ativação e política para o produto ESET LiveGuard Advanced na máquina atual.

> Cada dispositivo com ESET LiveGuard Advanced precisa ter um Sistema de Reputação ESET LiveGrid® e Sistema de Feedback ESET LiveGrid® ativados. Verifique as políticas do seu dispositivo.

- **Arquivos enviados** – atalho para o menu Arquivos enviados.

- **Saiba mais** – atalho para a página do produto.

Usuários

- **Usuários conectados** (apenas computadores) - Domínio e nome de usuário dos usuários que fizeram login no dispositivo.

- **Usuários atribuídos**

  - Clique em **Adicionar usuário** para atribuir um usuário de Usuários do computador para este dispositivo.

    > Um computador só pode ser atribuído a no máximo 200 usuários em uma operação.

  - Clique no ícone de lixo para remover a atribuição do usuário atual.

  - Clique no nome de usuário atribuído para exibir seus detalhes de conta.

Localização

O bloco está disponível apenas para dispositivos móveis. Você pode localizar dispositivos no iOS Apple Business Manager (ABM) apenas quando o Módulo perda estiver ativado.

Virtualização

O bloco aparece depois que você marca o computador como mestre para clonagem e exibe as configurações VDI. Clique no ícone de engrenagem para alterar as configurações VDI.

Os botões a seguir estão disponíveis na parte inferior:

- Clique no botão de **Isolamento de rede** para executar as tarefas do cliente de isolamento de rede no computador:

  - Isolar da rede

  - Parar com o isolamento da red

- O botão **Virtualização** é usado para configurar o computador para clonagem. Ele é necessário quando os

computadores são clonados ou quando o hardware do computador é alterado.

- Marcar como Mestre para clonagem

- **Desativar detecção de hardware** - Desativar a detecção de alterações de hardware permanentemente. Essa ação não pode ser revertida!

- **Desmarcar como mestre para clonagem** - Remove a marca de mestre. Depois disso ser aplicado, cada nova clonagem da máquina vai resultar em uma pergunta.

A detecção de Impressão digital de hardware não é compatível com:
- Linux, macOS, Android, iOS
- máquinas sem o Agente ESET Management

Configuração:

Guia **Configuração** - Contém uma lista de configurações de produtos ESET instalados (Agente ESET Management, ESET endpoint, etc.). As ações disponíveis são:

- Clique em **Solicitar configuração** para criar uma tarefa para o Agente ESET Management coletar todas as configurações de produtos gerenciados. Depois que a tarefa é entregue ao Agente ESET Management, ela é executada imediatamente e os resultados são entregues ao ESET PROTECT. Servidor na próxima conexão. Isso vai permitir que você veja uma lista de todas as configurações de produto gerenciado.

- Abra uma configuração através do menu de contexto e converta-a para a política. Clique em uma configuração para vê-la na visualização.

- Depois de abrir a configuração, ela pode ser convertida para uma política. Clique em **Converter para Política**, a configuração atual será transferida para o assistente de política e você pode modificar e salvar a configuração como uma nova política.

- Fazer download da configuração para fins de diagnóstico e suporte. Clique em uma configuração selecionada e clique em **Download para diagnóstico** no menu suspenso.

Guia **Políticas aplicadas** - lista de políticas aplicadas ao dispositivo. Se você tiver aplicado uma política para o produto ESET ou recurso de produto ESET que não está instalado no computador, a política listada estará indisponível.

Você pode ver as políticas atribuídas ao dispositivo selecionado, assim como as políticas aplicadas a grupos contendo o dispositivo.
Há um ícone de cadeado ao lado de políticas bloqueadas (não editáveis) – políticas internas específicas (por exemplo, a política de Atualizações automáticas ou as políticas ESET LiveGuard) ou políticas onde o usuário tem a permissão de **Leitura**, mas não de **Gravação**.

Clique em **Gerenciar políticas** para gerenciar, editar, atribuir ou excluir uma política. As políticas são aplicadas com base em sua ordem (coluna **Ordem da política**). Para alterar a prioridade de aplicação da política, selecione a caixa de seleção ao lado de uma política e clique no botão **Aplicar logo** ou **Aplicar depois**.

Guia **Exclusões aplicadas** – Lista de exclusões aplicadas ao dispositivo.

Relatórios (apenas computadores)

- **SysInspector** - Clique em **Solicitar relatório (apenas Windows)** para executar a tarefa Solicitação de relatório do SysInspector nos clientes selecionados. Depois da tarefa ser concluída, uma nova entrada será exibida na lista de relatórios ESET SysInspector. Clique em um relatório listado para explorar.

- **Log Collector** - Clique em **Executar o Log Collector** para executar a tarefa do Log collector. Depois da tarefa ser concluída, uma nova entrada é adicionada na lista de relatórios. Clique em um relatório na lista para fazer o download dele.
- **Relatórios de diagnóstico** - Clique em **Diagnósticos** > **Ativar** para iniciar o modo de Diagnóstico na máquina atual. O modo de Diagnóstico fará o cliente enviar todos os relatórios para o ESET PROTECT. Servidor. Você pode procurar por todos os relatórios dentro de 24 horas. Os relatórios são organizados em cinco categorias: **Relatório de spam**, **Relatório de firewall**, **Relatório de HIPS**, **Relatório de controle de dispositivo** e **Relatório de controle da web**. Clique em **Diagnóstico** > **Reenviar todos os relatórios** para reenviar todos os relatórios do Agente na próxima replicação. Clique em **Diagnóstico** > **Desligar** para parar o modo de Diagnóstico.

O limite de tamanho de arquivo para a entrega de relatório por dispositivo é de 200MB. Você pode acessar relatórios do Web Console na seção **Detalhes** > **Relatórios**. Se os relatórios coletados pela tarefa forem maiores do que 200 MB, a tarefa vai falhar. Se a tarefa falhar, você pode:
- Coletar os relatórios localmente no dispositivo.
- Alterar o detalhamento dos relatórios e tentar novamente a tarefa:
  - Para destinos o Windows, use o parâmetro `/Targets:EraAgLogs` para coletar apenas relatórios do Agente ESET Management.
  - Para destinos Linux/macOS, use o parâmetro `--no-productlogs` para excluir relatórios do produto de segurança ESET instalado.

Execução de tarefas

Uma lista de tarefas excluídas. Você pode filtrar a exibição para limitar os resultados, mostrar os detalhes da tarefa, editar, duplicar, remover ou executar em/reexecutar a tarefa.

Aplicativos instalados:

Exibe uma lista de programas instalados em um cliente com detalhes como versão, tamanho, status de segurança, etc. Você pode ativar relatórios de aplicativos de terceiros (que não são da ESET) usando a configuração de Política do Agente.

Selecione um aplicativo e clique em **Desinstalar** para removê-lo.

- Você precisará digitar seus **Parâmetros de desinstalação**. Esses são parâmetros opcionais da linha de comando para o instalador (pacote de instalação). Os parâmetros de desinstalação são exclusivos para cada instalador de software. Você pode encontrar mais informações na documentação do produto em particular.

- Selecione a caixa de seleção ao lado de **Reinicialização automática quando necessário** para fazer uma

reinicialização automática do computador do cliente depois da instalação. Alternativamente, você pode deixar esta opção desmarcada e reiniciar manualmente os computadores do cliente. Você pode configurar o comportamento de reinicialização/desligamento dos computadores gerenciados. O computador deve executar um Agente ESET Management 9.1 e um produto de segurança ESET compatível com esta configuração.

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 estiver protegido por senha, não será possível desinstalá-lo. 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.

Se houver uma atualização de produto ESET disponível, você pode atualizar o produto ESET clicando no botão **Atualizar produtos ESET**.

- O ESET PROTECT é compatível com a atualização automática do Agente ESET Management em computadores gerenciados.
- Dispositivos iOS reportam a lista de software instalado para o ESET PROTECT uma vez por dia. O usuário não consegue forçar a atualização da lista.

Alertas

Mostra uma lista de alertas e seus detalhes: Problema, Status, Produto, Ocorreu, Gravidade, etc. Esta lista pode ser acessada diretamente da seção **Computadores** clicando na contagem de alertas na coluna **Alertas**. É possível gerenciar os alertas através de ações de um clique.

Perguntas (apenas computadores)

A lista de perguntas relacionadas a clonagem está na guia **Perguntas**. Leia mais sobre a resolução de problemas para computadores alterados ou clonados.

Detecções e quarentenas

- **Detecções** – todos os tipos de detecção são exibidos, mas podem ser filtrados por **Categoria de detecção** – **Antivírus**, Arquivos bloqueados, ESET Inspect, **Firewall**, **HIPS** e **Proteção web**.

- **Quarentena** – uma lista de detecções em quarentena com detalhes como Nome da detecção, Tipo de detecção, Nome do objeto, Tamanho, Ocorreu pela primeira vez, Contagem, Motivo do usuário, etc.

Detalhes

- **Básico** - Informações sobre o dispositivo: Nome do sistema operacional, tipo, versão, número de série, nome FQDN, etc. Esta seção também inclui informações sobre se o dispositivo foi colocado em mudo, como ele é gerenciado, quando foi atualizado pela última vez e o número de políticas aplicadas.

- **Hardware** - informações sobre o hardware do computador, fabricante e modelo, CPU, RAM, armazenamento (inclusive a capacidade e o espaço livre), periféricos e informações sobre as redes (IPv4, IPV6, subrede, adaptador de rede...). Veja também o inventário de hardware.

- **Produtos e licenças** - Versão do mecanismo de detecção atual, versões de produtos de segurança ESET instalados, licenças usadas.

- **Criptografia** – se você usar o ESET Full Disk Encryption, consulte a visão geral do status da criptografia de disco.

Visualização do computador

Em **Computadores** clique em um nome de computador para exibir o painel lateral de Visualização do computador no lado direito. A painel lateral de Visualização do computador contém as informações mais importantes sobre o computador selecionado.

Manipulação de visualização do computador:

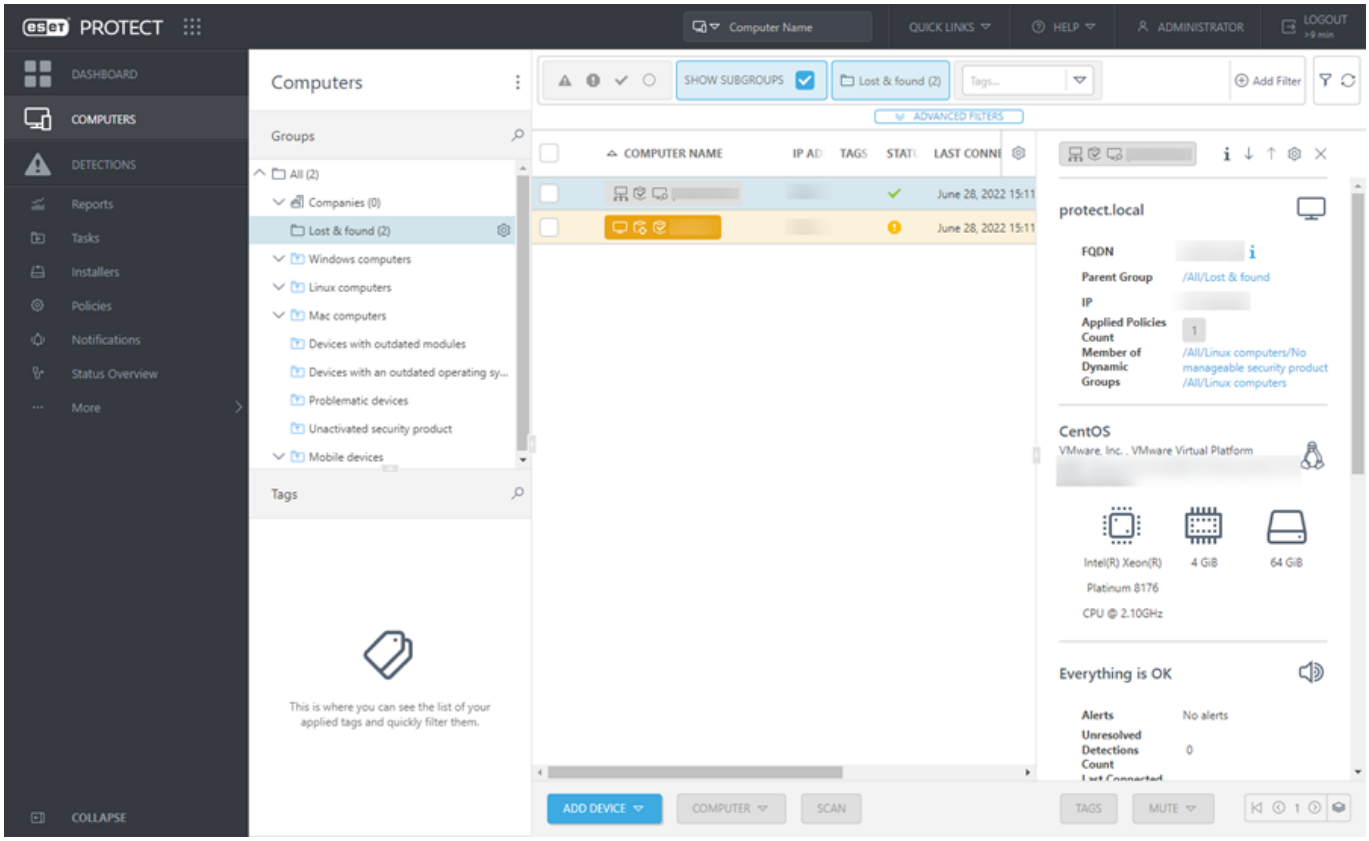
- **Mostrar detalhes** – abre o menu Detalhes do computador

- **Próximo** – mostrar o próximo dispositivo no painel lateral de visualização do computador.

- **Anterior** – exibe o dispositivo anterior no painel lateral de Visualização do computador.

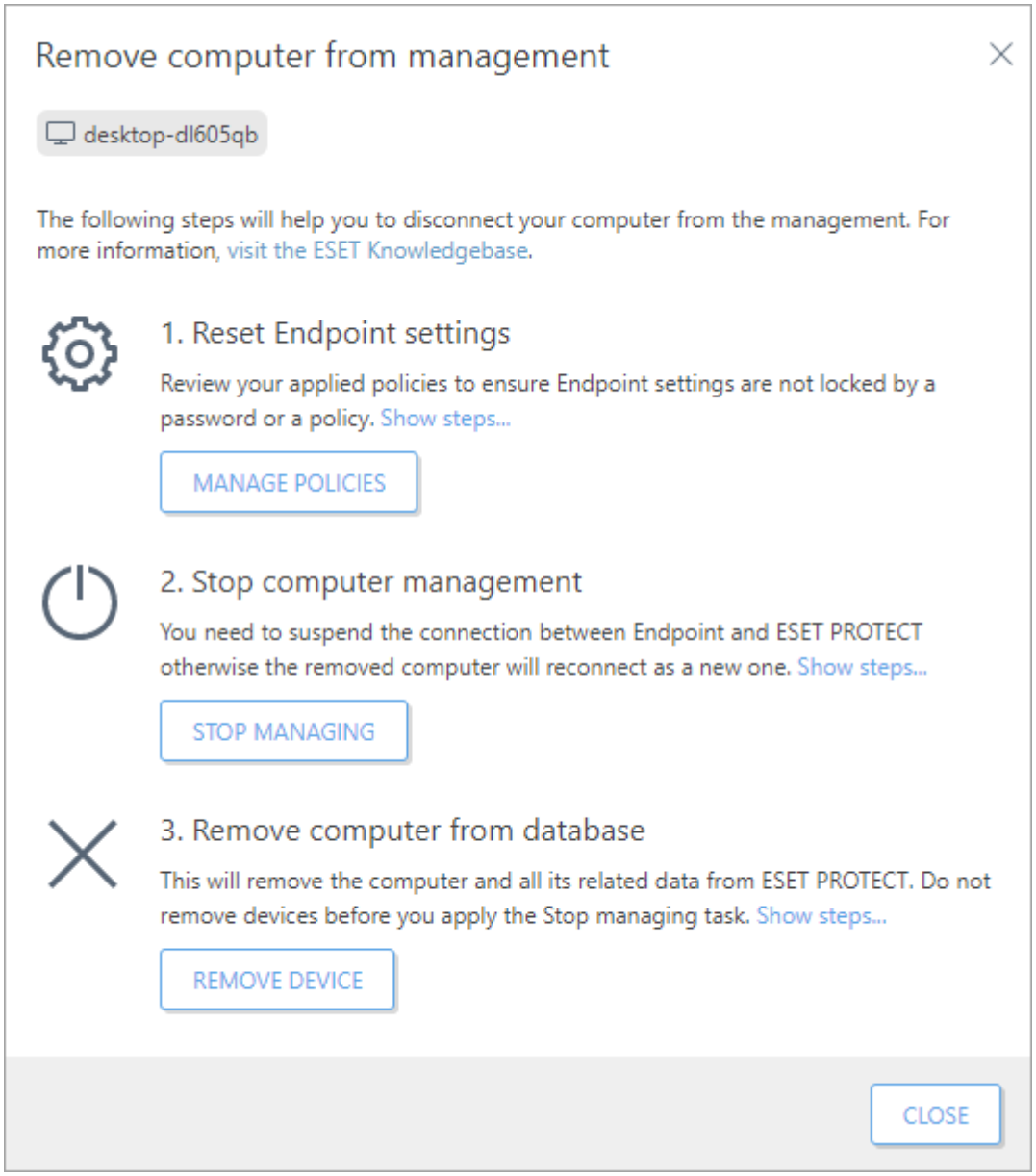
- **Gerenciar conteúdo para Detalhes do computador** – você pode gerenciar quais seções do painel lateral de visualização do computador serão exibidas e em qual ordem.

- **Fechar** – fecha o painel lateral de Visualização do computador.



Remover computador do gerenciamento

Para remover um dispositivo do gerenciamento, clique em **Computadores**, selecione um dispositivo > clique em **Gerenciar** > **Remover**. Uma caixa de diálogo vai exibir as etapas necessárias para remover o computador selecionado do gerenciamento.



Quando continuar para a próxima etapa, certifique-se de que você concluiu a etapa anterior. Isso é essencial para a remoção correta do dispositivo.

1. **Redefinir configurações Endpoint** - Clique em **Gerenciar políticas** e remova todas as políticas aplicadas para permitir o gerenciamento local de dispositivo. Consulte **Regras de remoção de política** na seção **Políticas** . Se houver uma senha definida para acessar a configuração do produto Endpoint, crie uma nova política para remover a senha (selecione para definir uma nova senha, mas não insira nenhuma senha). Para computadores criptografados com ESET Full Disk Encryption, siga as etapas de remoção da criptografia.

2. **Interromper gerenciamento do computador** - Execute uma tarefa Interromper gerenciamento ou desinstale o Agente ESET Management ou produto de segurança ESET localmente em um computador. Isso suspende a conexão entre o computador e o ESET PROTECT.

3. **Remover computador do banco de dados** - Depois de certificar-se que o computador não está mais conectando ao ESET PROTECT, ele pode ser removido da lista de dispositivos gerenciados.

- Marque a caixa de seleção **Desejo desativar os produtos ESET instalados** para remover a licença de todos os produtos ESET instalados no computador selecionado. Veja também desativação dos produtos comerciais ESET.

Grupos

Os grupos podem ser compreendidos como pastas onde os computadores e outros objetos são categorizados.

Para computadores e dispositivos, você pode usar grupos predefinidos e modelos de grupos ou criar novos grupos. Computadores cliente podem ser adicionados a grupos. Isso ajuda você a manter os computadores estruturados e organizados de acordo com suas preferências. Você pode adicionar computadores ao grupo estático.

Grupos estáticos são gerenciados manualmente enquanto grupos dinâmicos são organizados automaticamente com base em critérios específicos em um modelo. Assim que os computadores estiverem em grupos, você poderá atribuir políticas, tarefas ou configurações a esses grupos. A política, a tarefa ou configuração é então aplicada a todos os membros do grupo. Há dois tipos de grupos clientes:

Grupos estáticos

Grupos estáticos são grupos de computadores cliente selecionados e outros objetos. Os membros do grupo são estáticos e podem ser adicionados/removidos somente manualmente, não com base em critérios dinâmicos. Um objeto pode ser membro de apenas um grupo estático. Um grupo estático pode ser excluído apenas se não houverem objetos nele.

Grupos dinâmicos

Grupos dinâmicos são grupos de dispositivos (não de outros objetos como tarefas ou políticas) que se tornaram membros do grupo porque cumprem com critérios específicos. Se um dispositivo do cliente não atender aos critérios, ele será removido do grupo. Computadores que satisfazem os critérios serão adicionados automaticamente ao grupo (por isso o nome “dinâmico”).

Clique no ícone de engrenagem ao lado do nome do grupo para ver as ações do grupo disponíveis e os detalhes do grupo.

Computadores que são membros do grupo estão listados no painel à direita.

Ações do grupo

Navegue para **Computadores** e selecione o grupo que deseja gerenciar. Clique no ícone de engrenagem ao lado do nome do grupo e selecione Mover. Um menu com as opções a seguir será exibido:

Ação do grupo	Descrição de Ações do grupo	Grupos estáticos	Grupos dinâmicos
Mostrar detalhes	Fornece uma visão geral do grupo selecionado.	✔	✔
Relatório de auditoria	Exibe o Relatório de auditoria para o item selecionado.	✔	✔
Novo grupo estático	O grupo selecionado se torna o grupo principal padrão, mas você poderá alterar o grupo principal posteriormente quando criar um novo grupo estático.	✔	X
Novo grupo dinâmico	O grupo selecionado se torna o grupo principal padrão, mas você poderá alterar o grupo principal posteriormente quando criar um novo grupo dinâmico.	✔	✔
Nova notificação	Criar uma nova notificação.	X	✔
Adicionar novo	Adicionar um novo dispositivo.	✔	X

Ação do grupo	Descrição de Ações do grupo	Grupos estáticos	Grupos dinâmicos
Tarefas	Selecione tarefas de cliente a serem executadas nos dispositivos deste grupo: **Escaneamento** – Execute a tarefa Escaneamento sob demanda em todos os clientes no grupo selecionado. **Atualizar**: • **Módulos de atualização** – Execute a tarefa Atualização de módulos (aciona uma atualização manualmente). • **Atualizar produtos ESET** – execute a tarefa de Instalação de software em computadores com produtos de segurança ESET desatualizados. • **Atualizar sistema operacional** – execute a tarefa Atualizações do sistema operacional nos computadores no grupo selecionado. **Móvel** – Veja as Ações Anti-Theft para mais detalhes. • **Inscrever novamente** – Inscrever novamente em um dispositivo móvel. • **Localizar** - Solicitar as coordenadas de GPS de seu dispositivo móvel. • **Bloqueio** - o dispositivo será bloqueado automaticamente quando uma atividade suspeita for detectada ou quando o dispositivo for marcado como perdido. • **Desbloquear** - O dispositivo será desbloqueado. • **Limpar a senha** – remove a senha de um dispositivo iOS/iPadOS. • **Alarme/módulo perda** - aciona um alarme sonoro remotamente, o alarme vai começar a tocar mesmo se o dispositivo estiver configurado como silencioso. • **Redefinição de fábrica** - todos os dados armazenados no dispositivo serão apagados definitivamente. **Executar tarefa** – Selecione uma ou mais Tarefas do cliente e execute-as no dispositivo selecionado. **Nova tarefa** – Crie uma nova Tarefa do cliente. Selecione uma tarefa e configure a alternância (opcional) para essa tarefa. A tarefa será colocada em fila de acordo com as configurações da tarefa. Essa opção acionará imediatamente uma tarefa existente, que você selecionará de uma lista de tarefas disponíveis. O acionador não está disponível para esta tarefa, pois ele será executado imediatamente. **Tarefas recentes** - Lista de Tarefas de cliente recentes para todos os grupos e computadores.	✔	✔
Soluções	**Ativar o ESET Inspect** – clique em ao lado de um grupo estático e selecione **Soluções** > **Ativar o ESET Inspect** para ativar e habilitar o ESET Inspect no computador. **Ativar o ESET LiveGuard** –Clique em um computador ou ícone de engrenagem ao lado de um grupo estático e selecione **Soluções** > **Ativar ESET LiveGuard** para ativar e habilitar o ESET LiveGuard Advanced.	✔	X
Relatórios	Selecione e execute um relatório do grupo selecionado.	✔	X
Gerenciar políticas	Gerenciar políticas atribuídas ao grupo selecionado.	✔	✔
Editar	Editar o grupo selecionado. As mesmas configurações são aplicadas quando você cria um novo grupo (estático ou dinâmico).	✔	✔
Mover	Selecione um grupo e mova-o como um subgrupo de outro grupo.	✔	✔
Excluir	Remove o grupo selecionado.	✔	✔
Aplicar antes **Aplicar depois**	Alterar o nível de prioridade de um Grupo dinâmico.	X	✔
Importar	Importar uma lista (geralmente um arquivo de texto) de computadores, como membros do grupo selecionado. Se os computadores já existirem como membros desse grupo, o conflito será resolvido com base na ação selecionada.	✔	X
Exportar	Exporte os membros do grupo (e subgrupos, se selecionados) em uma lista (arquivo *.txt*). Essa lista pode ser usada para revisão ou importada posteriormente.	✔	X

Detalhes do grupo

Quando você seleciona uma ação de grupo **Mostrar detalhes**, você pode ver uma visão geral do grupo selecionado:

Visão geral:

Em **Visão geral**, você pode editar as configurações do grupo clicando em ou **Adicionar descrição**. Você pode visualizar informações sobre o posicionamento do grupo e seu **Grupo principal** e **Grupos secundários**. Se o grupo selecionado for um Grupo dinâmico, você também pode ver a operação e as regras baseadas nas quais os computadores foram avaliados e atribuídos ao grupo.

Tarefas

Você pode ver e editar as tarefas de cliente atribuídas ao grupo.

Políticas

Você pode atribuir uma política existente ao grupo ou criar uma nova política. Você pode ver e editar as políticas atribuídas ao grupo.

> Você pode ver apenas as políticas atribuídas ao grupo selecionado. Você não pode ver as políticas aplicadas a computadores individuais no grupo.

As políticas são aplicadas com base em sua ordem (coluna **Ordem da política**). Para alterar a prioridade de aplicação da política, selecione a caixa de seleção ao lado de uma política e clique no botão **Aplicar logo** ou **Aplicar depois**.

Alertas

A lista de alertas de computadores no grupo. É possível gerenciar os alertas através de ações de um clique.

Exclusões

A lista de exclusões aplicadas ao grupo.

Grupos estáticos

Grupos estáticos são usados para:

- Organize dispositivos e crie hierarquia de grupos e subgrupos
- Organizar objetos
- Serve como Grupo Inicial para usuários

Grupo doméstico – O grupo doméstico é detectado automaticamente com base no conjunto de permissões atribuído do usuário atualmente ativo.

> Exemplo de cenário:
> A conta de usuário atualmente ativa tem o direito de acesso de **Gravação** para a **Tarefa de cliente de Instalação de software** e a conta do **Grupo doméstico** é "Department_1". Quando o usuário criar uma nova **Tarefa de cliente de instalação de software**, "Department_1" será selecionado automaticamente como o **Grupo doméstico** da tarefa de cliente.

Se o Grupo doméstico pré-selecionado não atender às suas expectativas, você pode selecionar o Grupo doméstico manualmente.

Grupos estáticos só podem ser criados manualmente. Dispositivos podem ser movidos manualmente para os grupos. Cada computador ou dispositivo móvel pode pertencer a apenas um grupo estático. O gerenciamento de Grupos estáticos está disponível através das ações do grupo.

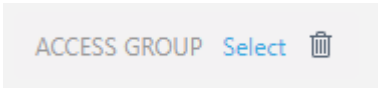
Há dois grupos estáticos padrão:

- **Todos** - Este é um grupo principal de todos os computadores na ESET PROTECT. Servidor rede Todos os objetos criados pelo administrador estão contidos neste grupo (por padrão). É sempre exibido e não pode ser renomeado. O acesso a este grupo dá aos usuários acesso a todos os subgrupos, portanto ele deve ser distribuído com cuidado.
- **Perdido e encontrado** - um grupo secundário do grupo **Todos**. Cada novo computador que se conecta ao ESET PROTECT Servidor pela primeira vez é automaticamente exibido neste grupo. O grupo pode ser renomeado ou copiado mas não pode ser excluído ou movido.

Para mover um computador para outro grupo estático, clique no computador > selecione **Gerenciar** > **Mover para grupo** > selecione o grupo estático de destino e clique em **OK**.

Um grupo estático pode ser excluído apenas se:
- O usuário tem permissão de gravação neste grupo
- O grupo está vazio

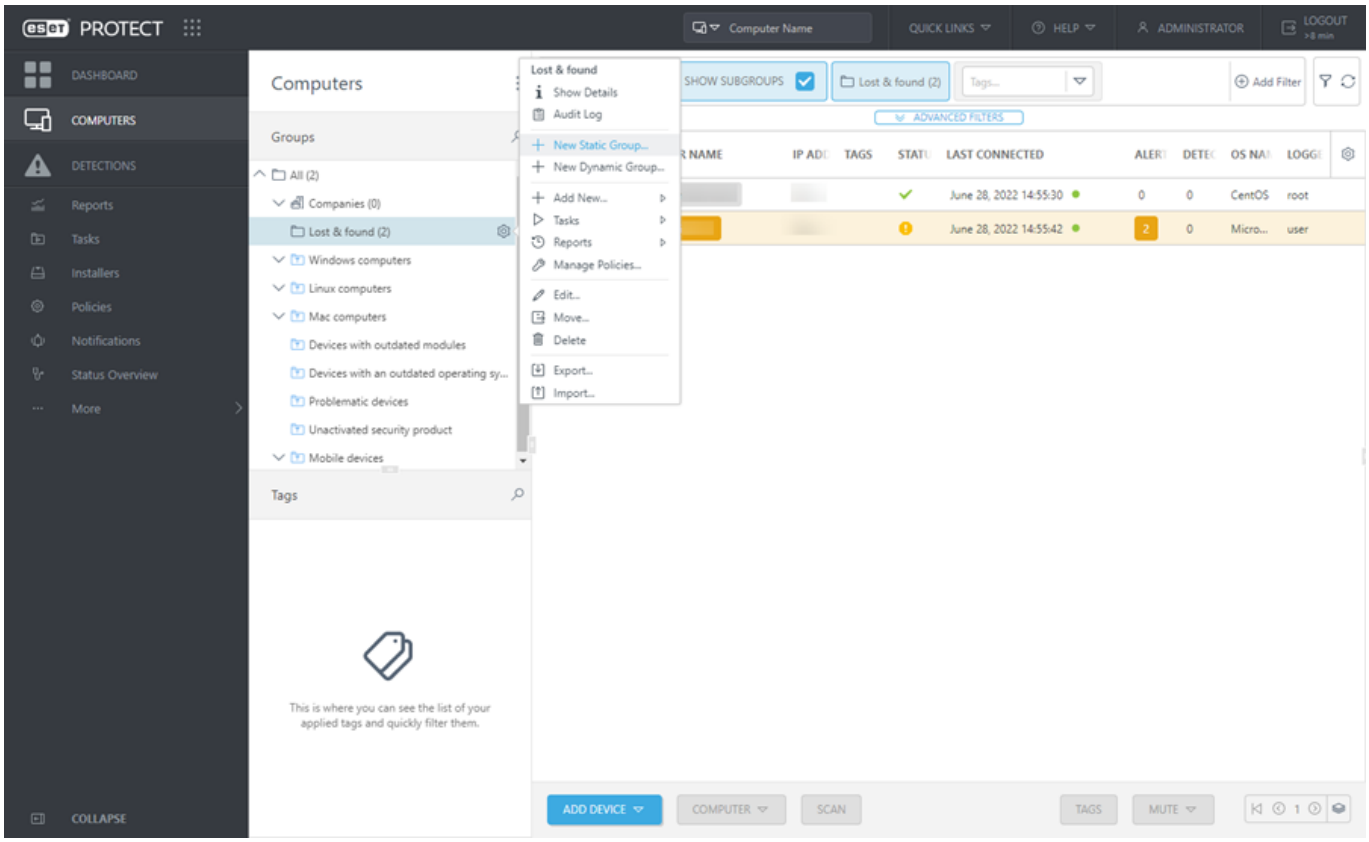
Se ainda existirem alguns objetos no grupo estático, a operação vai falhar. Há um botão de filtro do **Grupo de acesso** localizado em cada menu (por exemplo, **Instaladores**) com objetos.



Clique em **Selecionar** para escolher um grupo estático - apenas objetos contidos neste grupo serão listados na visualização. Com essa visualização filtrada, o usuário pode manipular facilmente os objetos de um grupo.

Crie um Novo grupo estático

Para criar um novo Grupo estático, clique em **Computadores**, selecione o ícone de engrenagem ao lado de um grupo estático e selecione **Novo grupo estático**.



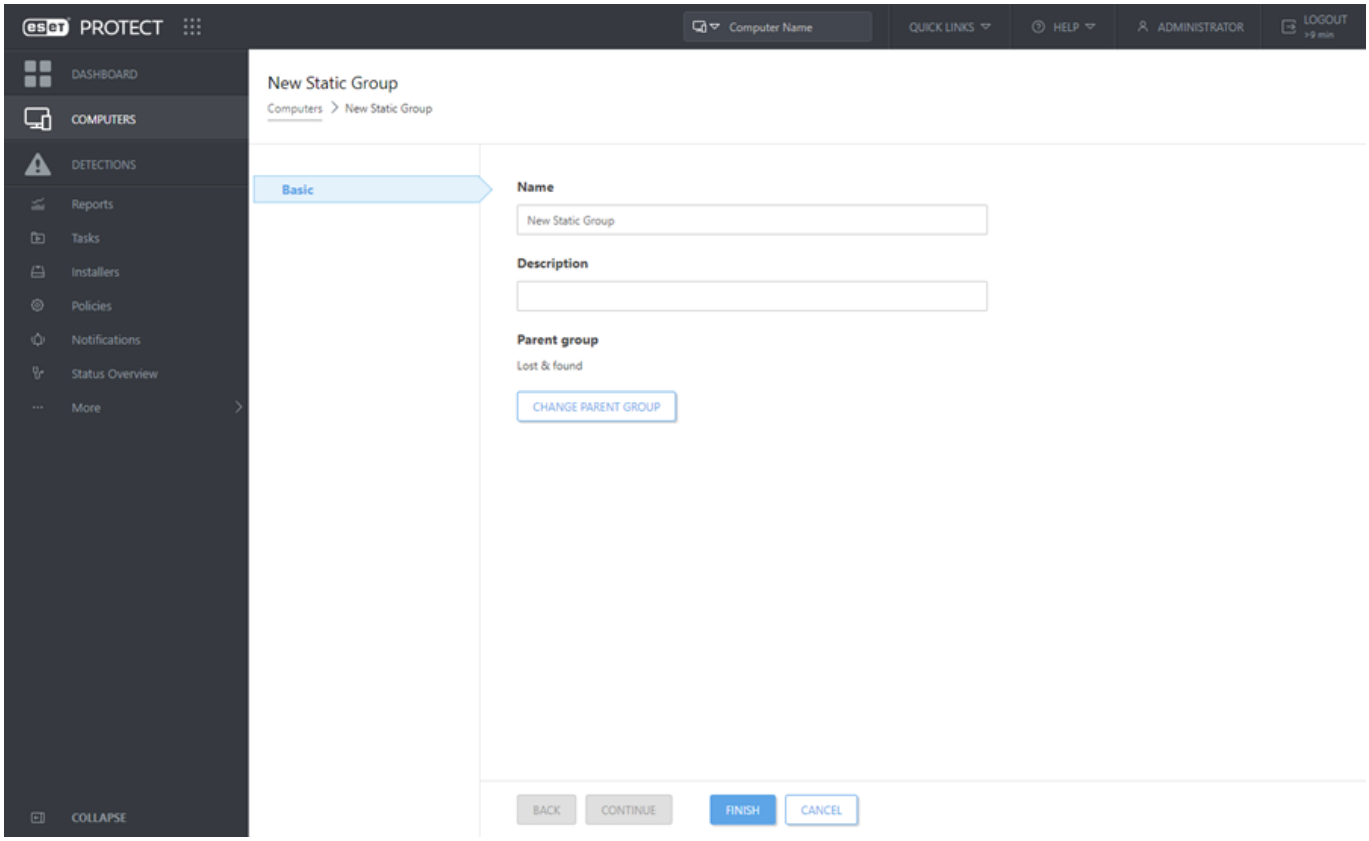
Básico

Insira um **Nome** e uma **Descrição** para o novo grupo.

- Opcionalmente, você pode alterar o **Grupo principal**. Por padrão, o grupo principal é o grupo que você selecionou quando começou a criar o novo grupo estático. Se quiser trocar seu grupo pai, clique em **Alterar grupo pai** e selecione o grupo pai da árvore.

- O pai do novo grupo estático deve ser um Grupo estático. Não é possível que um grupo estático seja incluído em um grupo dinâmico.

Clique em **Concluir** para criar o Novo grupo estático.



Importar clientes do Active Directory

Para importar clientes do AD, crie uma nova tarefa do servidor: Sincronização de grupo estático.

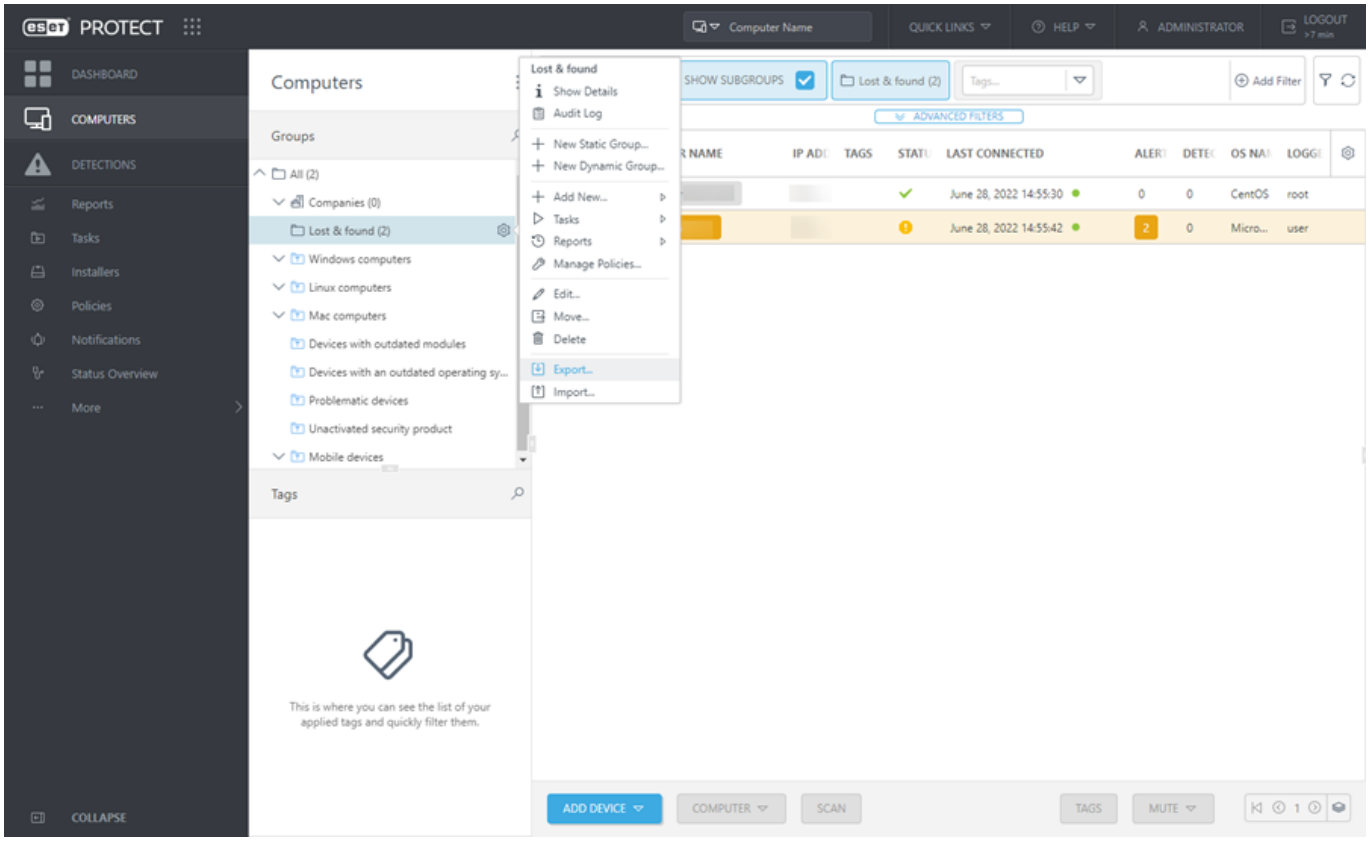
Selecione um grupo ao qual deseja adicionar novos computadores a partir do AD. Além disso, selecione objetos no AD dos quais deseja sincronizar e o que fazer com as duplicatas. Insira as configurações de conexão do servidor do AD e defina o Modo de sincronização como **Active Directory/Open Directory/LDAP**.

Exportar grupos estáticos

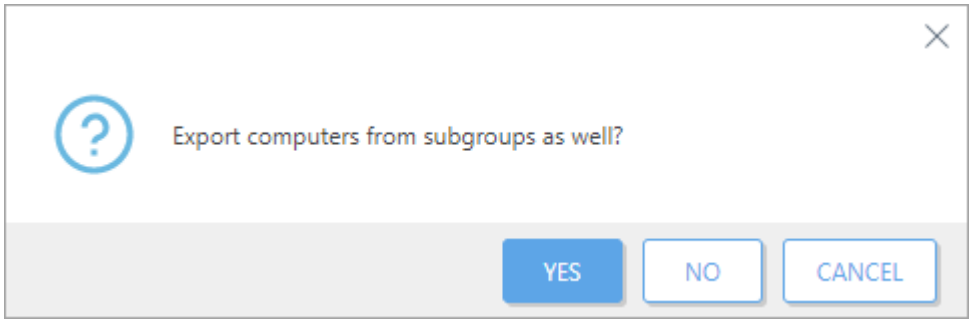
A exportação de uma lista de computadores que estejam na estrutura ESET PROTECT é simples. Você pode exportar a lista e armazená-la como um backup, a fim de que possa importar a lista de volta no futuro, por exemplo, se quiser restaurar a estrutura de grupo.

Grupos estáticos precisam conter pelo menos um computador. A exportação de grupos vazios não é possível.

1. Vá para **Computadores** e selecione um Grupo estático que deseja exportar.
2. Clique no ícone de engrenagem e selecione **Exportar**.



3. Se o Grupo estático selecionado tiver subgrupos com computadores, você pode optar por também exportar computadores de subgrupos.

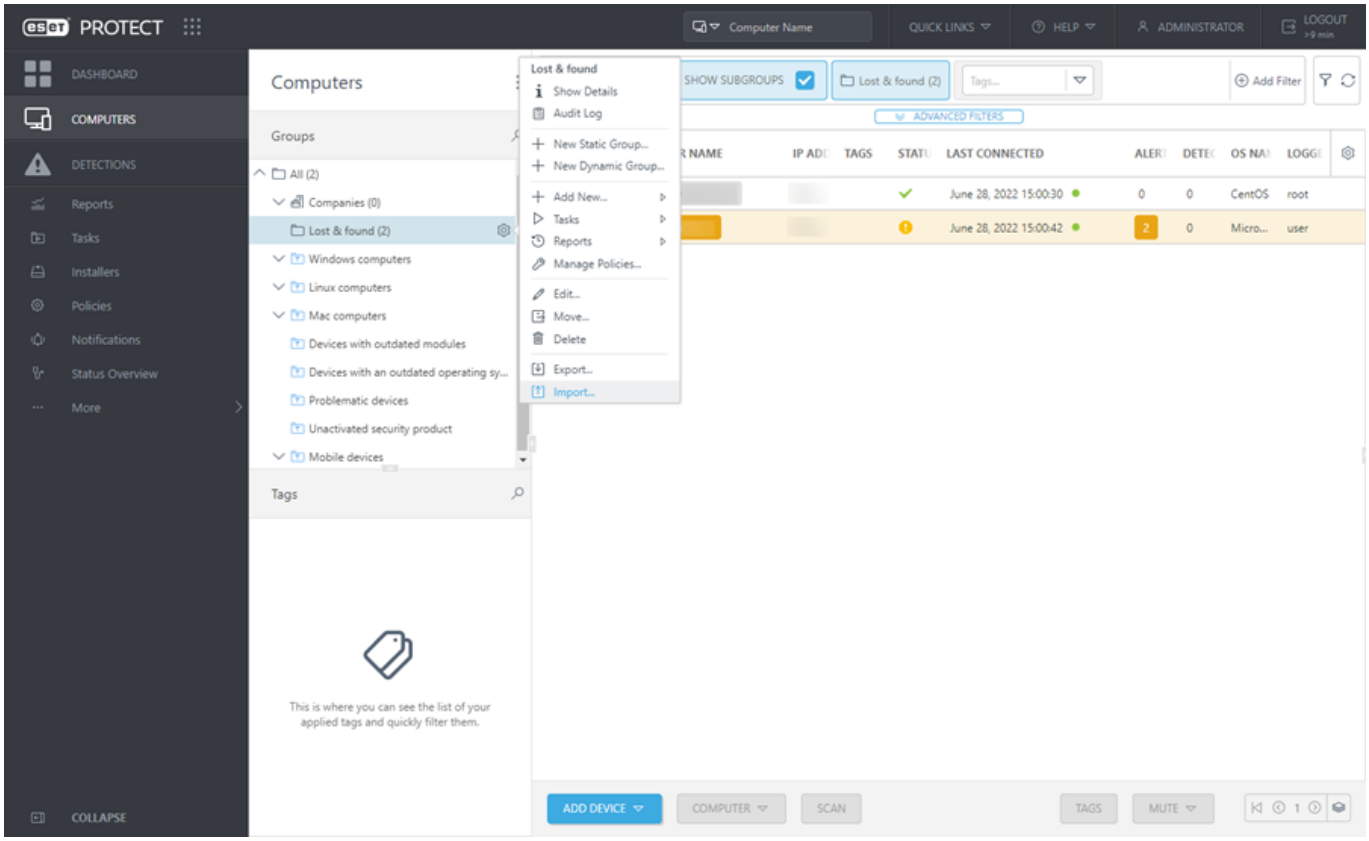


4. O arquivo será salvo em formato *.txt*.

Grupos dinâmicos não podem ser exportados, pois eles são apenas links para computadores, de acordo com os critérios definidos em modelos de grupos dinâmicos.

Importar grupos estáticos

Arquivos exportados de grupos estáticos podem ser importados de volta para o console da Web ESET PROTECT e incluídos em sua estrutura de grupo existente.



1.Clique em **Computadores** e selecione qualquer grupo estático.

2.Clique no ícone de engrenagem e selecione **Importar**.

3.Clique em **Procurar** e vá até o arquivo *.txt*.

4.Selecione o arquivo do grupo e clique em **Abrir**. O nome do arquivo é exibido na caixa de texto.

5.Selecione uma das seguintes opções para resolver conflitos:

- **Não criar nem mover nenhum dispositivo se as mesmas entradas foram encontradas em outros lugares**.

Se grupos estáticos e computadores do arquivo *.txt* já existirem nesse grupo, esses computadores serão ignorados e não serão importados. As informações sobre isso serão exibidas.

- **Mover os dispositivos existentes se eles ainda não existirem em caminhos importados. Mantém apenas os dispositivos gerenciados no mesmo caminho quando possível**.

Se existirem grupos estáticos e computadores do arquivo *.txt* já existirem nesse grupo, será necessário mover computadores para outros grupos estáticos antes da importação. Após a importação, esses computadores serão movidos de volta para grupos originais de onde ele foram movidos.

- **Duplicar os dispositivos existentes se eles ainda não existirem em caminhos importados**.

Se o grupo estático existir e computadores do arquivo *.txt* já existirem nesse grupo, serão criadas duplicatas desses computadores no mesmo grupo estático. O computador original será exibido com informações completas e a duplicata será exibida somente com esse nome de computador.

6.Clique em **Importar** para importar o grupo estático e computadores.

Árvore do grupo estático para ESET Business Account / ESET MSP Administrator

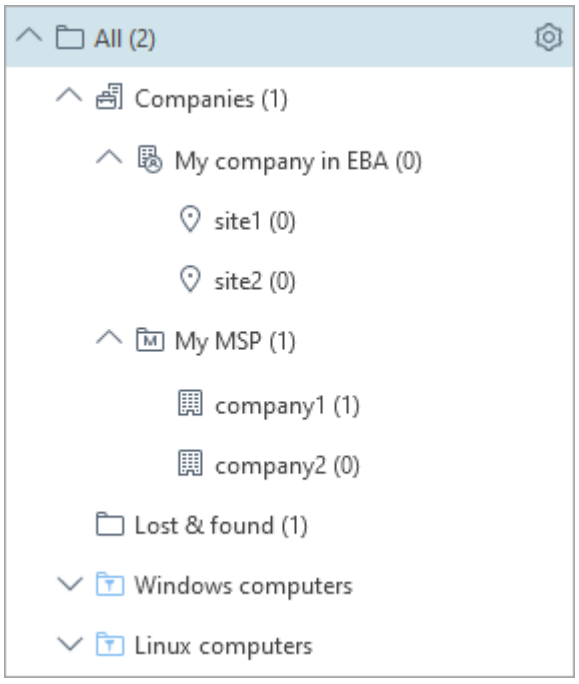
Se você importar licenças do ESET Business Account, a estrutura ESET Business Account da sua empresa (incluindo locais) será exibida na árvore do Grupo estático (um novo recurso no ESET PROTECT versão 9.1).

Se você importar licenças do ESET MSP Administrator, a estrutura ESET MSP Administrator será exibida na árvore do grupo estático. Leia mais sobre ESET PROTECT para Provedores de serviço gerenciados.

Estrutura de árvore de grupo estático para ESET Business Account/ESET MSP Administrator

Você pode ver a estrutura da árvore do Grupo estático para ESET Business Account/ESET MSP Administrator em **Computadores** na árvore do Grupo estático em **Todos** > **Empresas**.

Recomendamos que você use uma conta on-line (ESET Business Account ou ESET MSP Administrator – consulte também Introdução ao ESET Business Account) e sincronize a conta com o ESET PROTECT para usar o ESET PROTECT no seu potencial máximo.
Se você ativou o ESET PROTECT com uma chave de licença ou licença off-line e não sincronizou licenças do ESET Business Account ou ESET MSP Administrator, você não verá ESET Business Account ou ESET MSP Administrator na estrutura em árvore do Grupo estático.



Em **Empresas**, você pode ver uma ou mais árvores ESET Business Account ou ESET MSP Administrator, dependendo das contas sincronizadas no Gerenciamento de licenças.

Se você tiver uma conta ESET MSP Administrator, veja os detalhes sobre a estrutura das entidades no MSP.

Sincronização de site ESET Business Account

Se você tiver sites ESET Business Account, o ESET PROTECT sincroniza-os automaticamente para a árvore do Grupo estático e atribui licenças de cada site ao respectivo grupo estático (marcado com o ícone) sob a empresa ESET Business Account.

- Recomendamos que você use o site de Grupos estáticos criados automaticamente para gerenciar seus sites (em vez de criar grupos estáticos manualmente).
- Você precisa criar administradores do site e atribuir suas permissões manualmente. Selecione o respectivo grupo estático de site como grupo doméstico para cada administrador do site e atribua ao administrador um conjunto de permissões com o mesmo grupo doméstico.

Por exemplo, você tem dois sites (**site1** e **site2**):
1.Crie um usuário para cada site (**site1_admin** e **site2_admin**).
2.Opcional: Atribua o respectivo grupo doméstico (site) a cada usuário (**site1** para **site1_admin** e **site2** para **site2_admin**).
3.Crie um conjunto de permissões para cada usuário (**site1_permissions** para e **site1_admin** **site2_permissions** para **site2_admin**).
4.Atribua o respectivo Grupo estático a cada conjunto de permissões (**site1** para **site1_permissions** e **site2** para **site2_permissions**).
5.Atribua as funcionalidades necessárias de cada conjunto de permissões e o nível de acesso (**leitura**, **uso**, **gravação**).
6.Atribua cada conjunto de permissões ao respectivo usuário (**site1_permissions** para **site1_admin** e **site2_permissions** para **site2_admin**).
7.Agora cada administrador do site só pode ver seu site e seus objetos (por exemplo, licenças).

Se você tiver um site sincronizado na estrutura da árvore do Grupo estático e renomear o site no ESET Business Account, ele também será renomeado no ESET PROTECT.

Se você tiver um site sincronizado na estrutura da árvore do Grupo estático e remover o site no ESET Business Account, seu ícone no ESET PROTECT vai mudar para .

Objetos compartilhados

A estrutura de árvore do grupo estático ESET Business Account ou ESET MSP Administrator contém grupos estáticos dedicados adicionais, chamados de **Objetos compartilhados**.

Você pode usar os **Objetos compartilhados** para compartilhar objetos do Web Console (políticas, modelos de grupo dinâmico, etc.) para mais usuários com acesso limitado (acesso a grupos estáticos no mesmo nível que **Objetos compartilhados** ou sob eles na estrutura em árvore):

1. Selecione os **Objetos compartilhados** como o grupo de acesso para o objeto do Web Console. O Grupo de acesso define o grupo estático do objeto e o acesso ao objeto com base nos direitos de acesso do usuário.

2. Atribua a permissão de **Uso** a **Objetos compartilhados**.

- Certifique-se de que usuários limitados não estão atribuídos com a permissão de **Gravação** nos **Objetos compartilhados** para impedir que eles editem os objetos. A permissão de **Uso** é suficiente.
- Você não pode armazenar computadores nos **Objetos compartilhados**. **Objetos compartilhados** não são visíveis sob **Grupos** nos **computadores**.

Grupos dinâmicos

Grupos dinâmicos podem ser vistos como filtros com base em status do computador. Um computador pode ser aplicável para mais de um filtro e, portanto, pode ser atribuído a mais de um grupo dinâmico. Isso torna os grupos dinâmicos diferentes dos grupos estáticos, pois um único cliente não pode pertencer a mais de um grupo estático.

Grupos dinâmicos são grupos de clientes selecionados com base em condições específicas. Para que um computador se torne membro de um Grupo dinâmico em específico, ele precisa cumprir com as condições definidas em um Modelo de grupo dinâmico. Cada modelo é composto por uma ou várias Regras. Você pode especificar essas regras ao criar um novo Modelo. Se um computador de cliente não atender aos critérios, ele será removido do grupo. Se ele atender às condições definidas, ele será adicionado ao grupo.

Os dispositivos são avaliados para inclusão em Grupos dinâmicos cada vez que fazem check-in no ESET PROTECT. Quando um dispositivo cumpre com os valores especificados em um modelo de grupo dinâmico, ele é automaticamente atribuído a este grupo. Os computadores são filtrados no lado do Agente, assim nenhuma outra informação precisa ser transferida ao servidor. O Agente decide por si só a quais Grupos dinâmicos um cliente pertence, e só notifica o servidor sobre sua decisão.

> Se o dispositivo do cliente não estiver conectado (por exemplo, se estiver desligado), sua participação nos grupos dinâmicos não é atualizada. Depois do dispositivo ser conectado novamente, sua participação nos grupos dinâmicos será atualizada.

Existem alguns Grupos dinâmicos pré-definidos disponíveis depois de ter instalado o ESET PROTECT. Você também pode criar Grupos dinâmicos personalizados. Existem 2 formas de fazer isso:

- Crie um modelo primeiro e depois crie um Grupo dinâmico.
- Criar um novo modelo ao criar um novo Grupo dinâmico.

Você pode usar Grupos dinâmicos em outras partes do ESET PROTECT. É possível atribuir políticas a eles (veja como as políticas são aplicadas) ou preparar uma tarefa para todos os computadores no grupo.

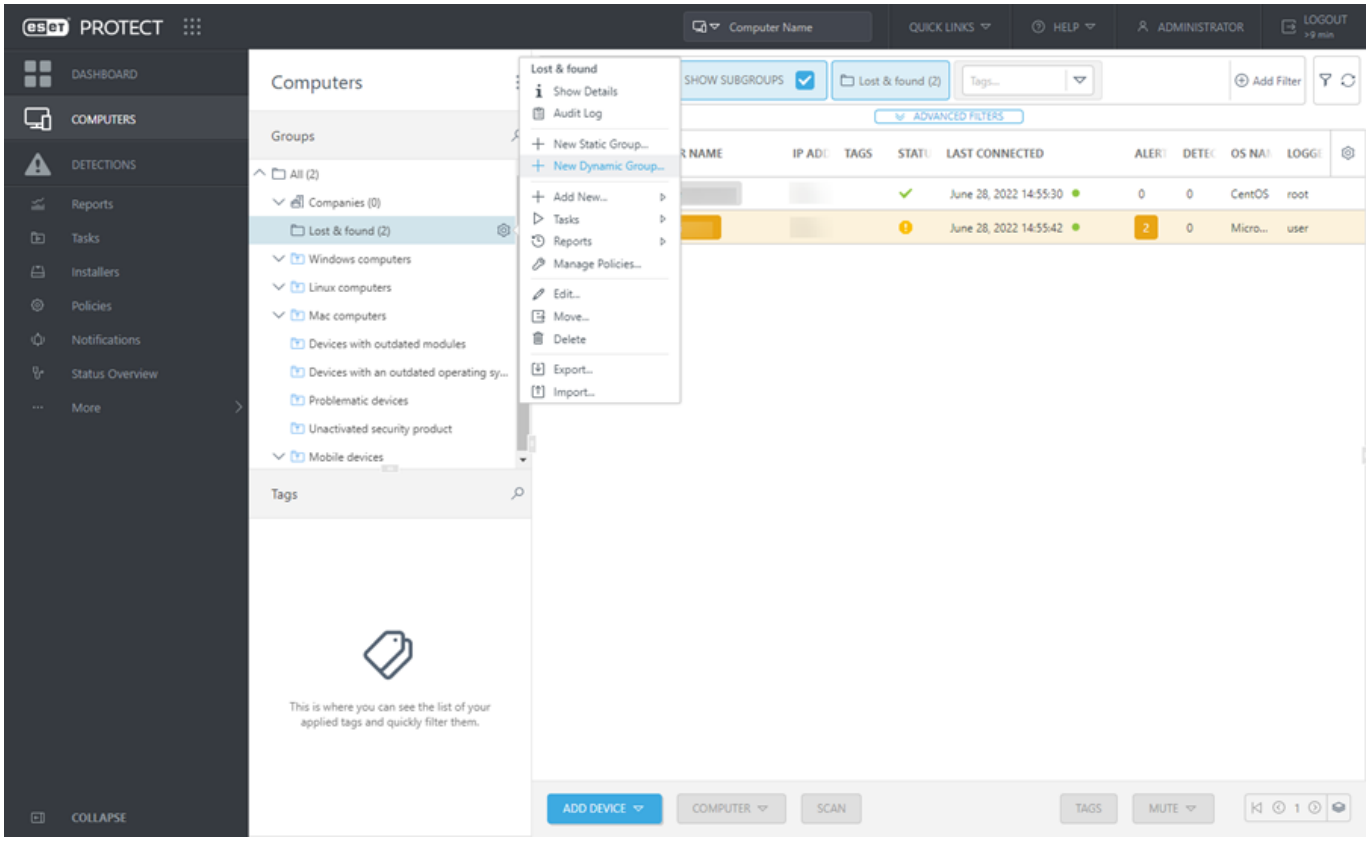
Um grupo dinâmico pode estar dentro de (sob) um grupo estático ou grupos dinâmicos. Porém o grupo estático não pode estar dentro de um grupo dinâmico. Todos os Grupos dinâmicos sob um certo Grupo estático filtram apenas os dispositivos daquele Grupo estático. Se um Grupo dinâmico estiver dentro de outro Grupo dinâmico, ele filtra os resultados do grupo dinâmico superior. Depois do grupo ser criado, ele pode ser movido livremente por toda a árvore.

O gerenciamento de Grupos dinâmicos está disponível através das ações do grupo.

Criar novo Grupo dinâmico

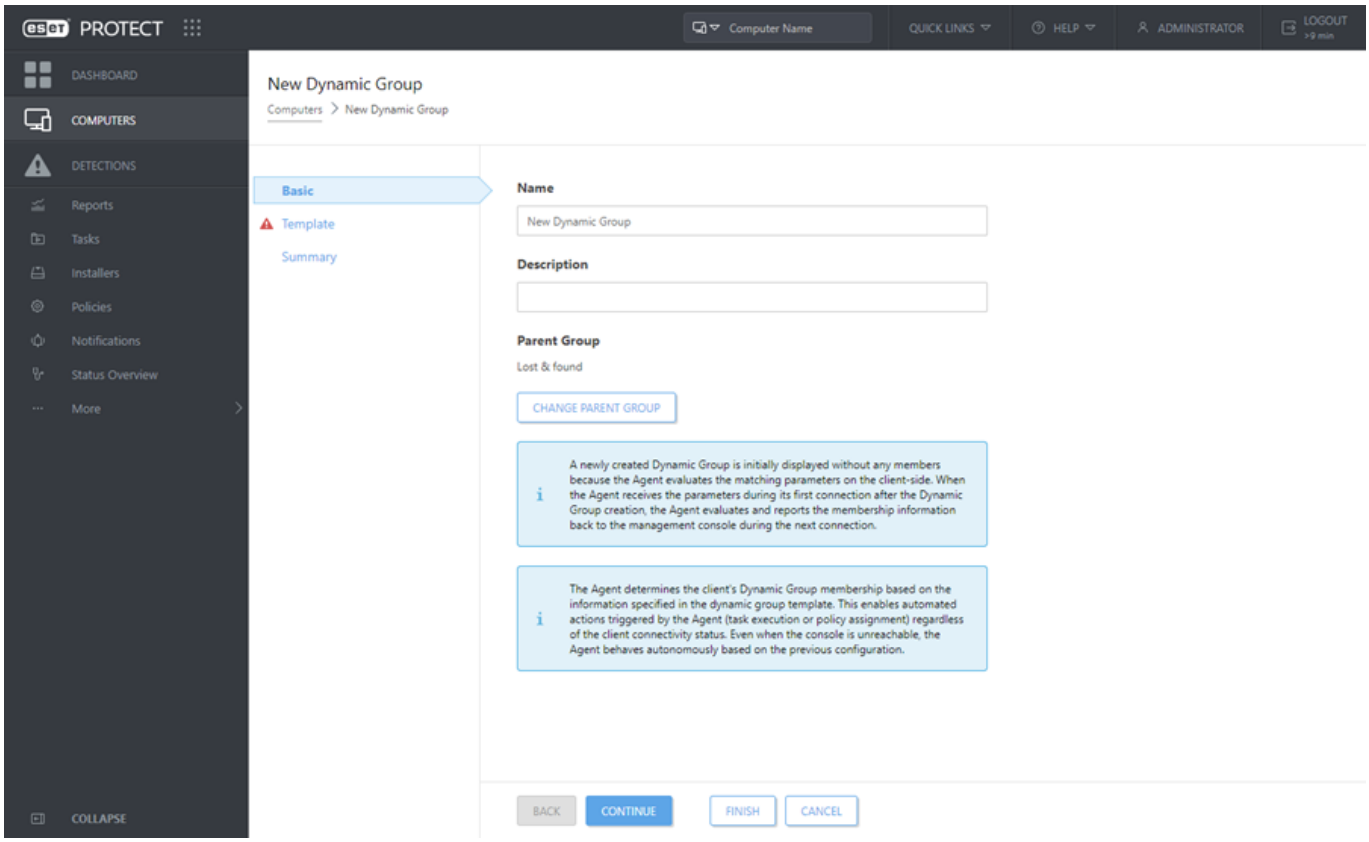
Para criar um Novo grupo dinâmico, siga as etapas abaixo.

1. Clique em **Computadores**, selecione o ícone de engrenagem ao lado de qualquer grupo e selecione **Novo grupo dinâmico**. Um Assistente de novo grupo dinâmico vai aparecer.



2.Insira um nome e uma descrição para o novo modelo.

3.Você pode alterar o grupo principal clicando em **Alterar grupo principal**.



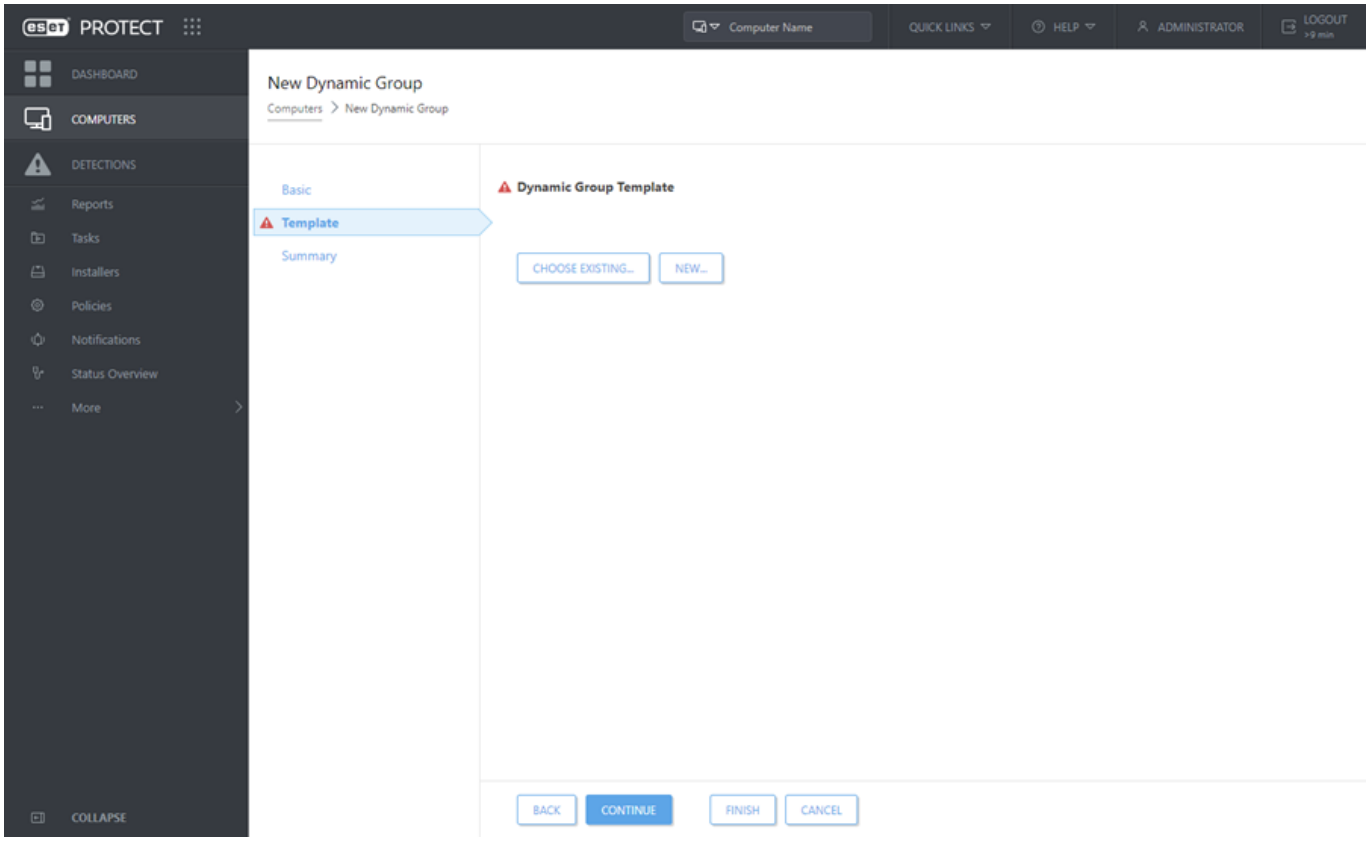
4.Clique em **Modelo**. Todo Grupo dinâmico é criado de um Modelo que define como o grupo filtra os computadores do cliente. Um número ilimitado de Grupos dinâmicos pode ser criado a partir de um modelo.

Um modelo é um objeto estático armazenado em um grupo estático. Usuários devem ter as permissões apropriadas para acessar os modelos. Um usuário precisa de permissões de acesso para ser capaz de trabalhar com modelos de Grupo dinâmico. Todos os modelos predefinidos estão localizados no grupo estático **Todos** e por padrão estão disponíveis apenas ao Administrador. Outros usuários precisam receber permissões adicionais. Como resultado, os usuários podem não conseguir ver ou usar os modelos padrão. Os modelos podem ser movidos para um grupo onde os usuários têm permissões.
Para duplicar um modelo o usuário precisa receber a atribuição de permissões de **Uso** (para modelos do Grupo dinâmico) para o grupo onde o modelo original está localizado, e permissões de **Gravação** para o grupo inicial do usuário (onde a duplicata será armazenada). Veja o exemplo de duplicação de objeto.

- Se você quiser criar o grupo a partir de um modelo predefinido ou a partir de um modelo que você já criou, clique em **Escolher existente** e selecione o modelo adequado a partir da lista.

- Se você ainda não tiver criado nenhum modelo, e se nenhum dos modelos predefinidos da lista for adequado para você, clique em **Novo** e siga as etapas para criar um novo modelo.

Para mais casos de uso sobre como criar um novo grupo dinâmico com base em um modelo de grupo dinâmico com regras, consulte os exemplos.



5.Clique em **Resumo**. O novo grupo vai aparecer sob o Grupo principal.

Mover grupo estático ou dinâmico

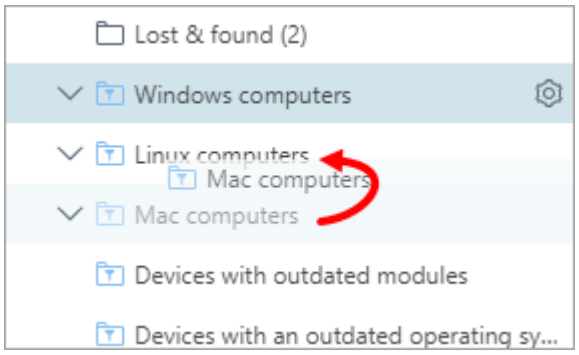
Um Grupo dinâmico pode ser membro de qualquer outro grupo, inclusive de Grupos estáticos. Um Grupo estático não pode ser movido para dentro de um Grupo dinâmico. Também não é permitido mover Grupos estáticos pré-definidos (por exemplo, o grupo estático **Perdido e encontrado**) para qualquer outro grupo. Outros grupos podem ser movidos livremente.

Clique no ícone de engrenagem ao lado do nome do grupo e selecione **Mover**. Uma janela será exibida mostrando a estrutura da árvore do grupo. Selecione o grupo de destino (estático ou dinâmico) para o qual você deseja mover o grupo selecionado. O grupo de destino vai se tornar o grupo principal. Também é possível mover grupos ao arrastar e soltar um grupo no grupo de destino de sua escolha.

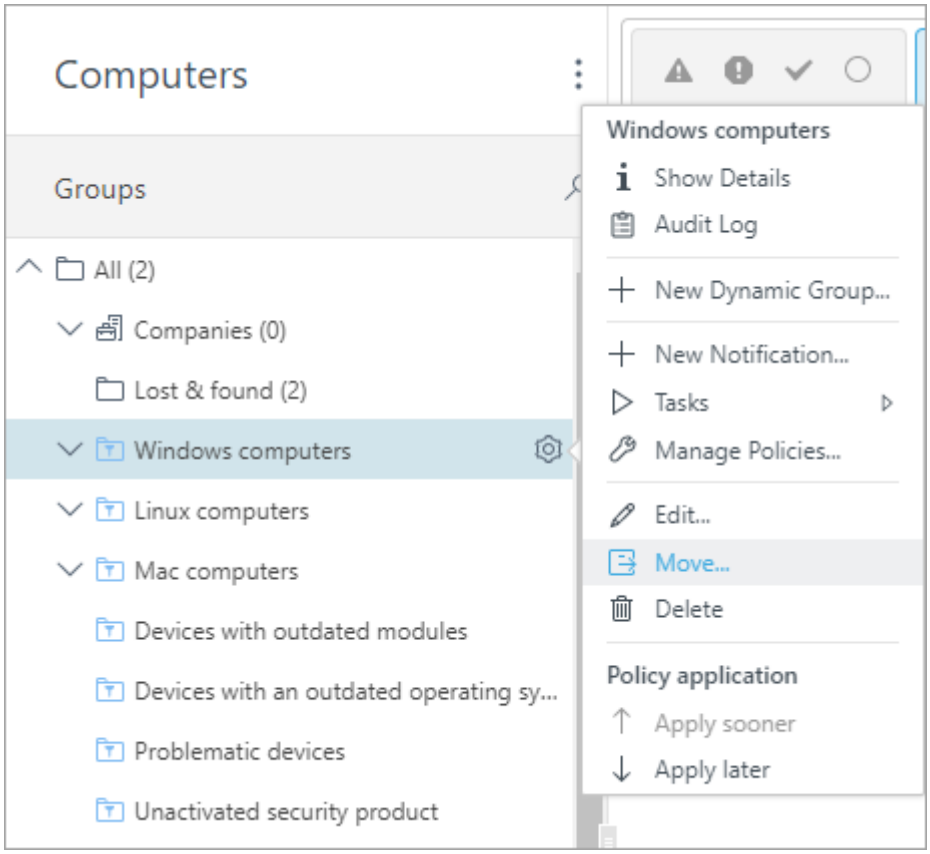
> O Grupo dinâmico em uma nova posição começa a filtrar os computadores (com base no modelo) sem qualquer relação com sua localização anterior.

Existem 3 métodos para mover um grupo:

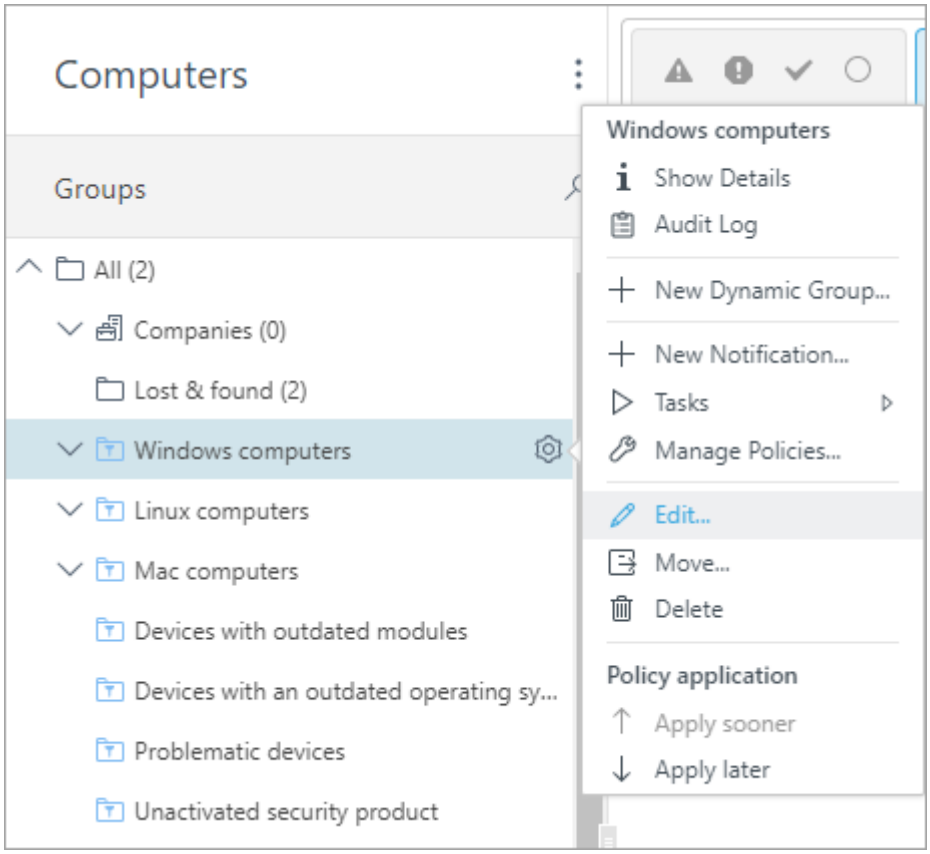
- **Arrastar e soltar** - clique e segure o grupo que deseja mover e solte-o sobre o novo grupo principal.



- Clique no ícone de engrenagem > **Mover** > selecione um novo grupo principal da lista e clique em **OK**.

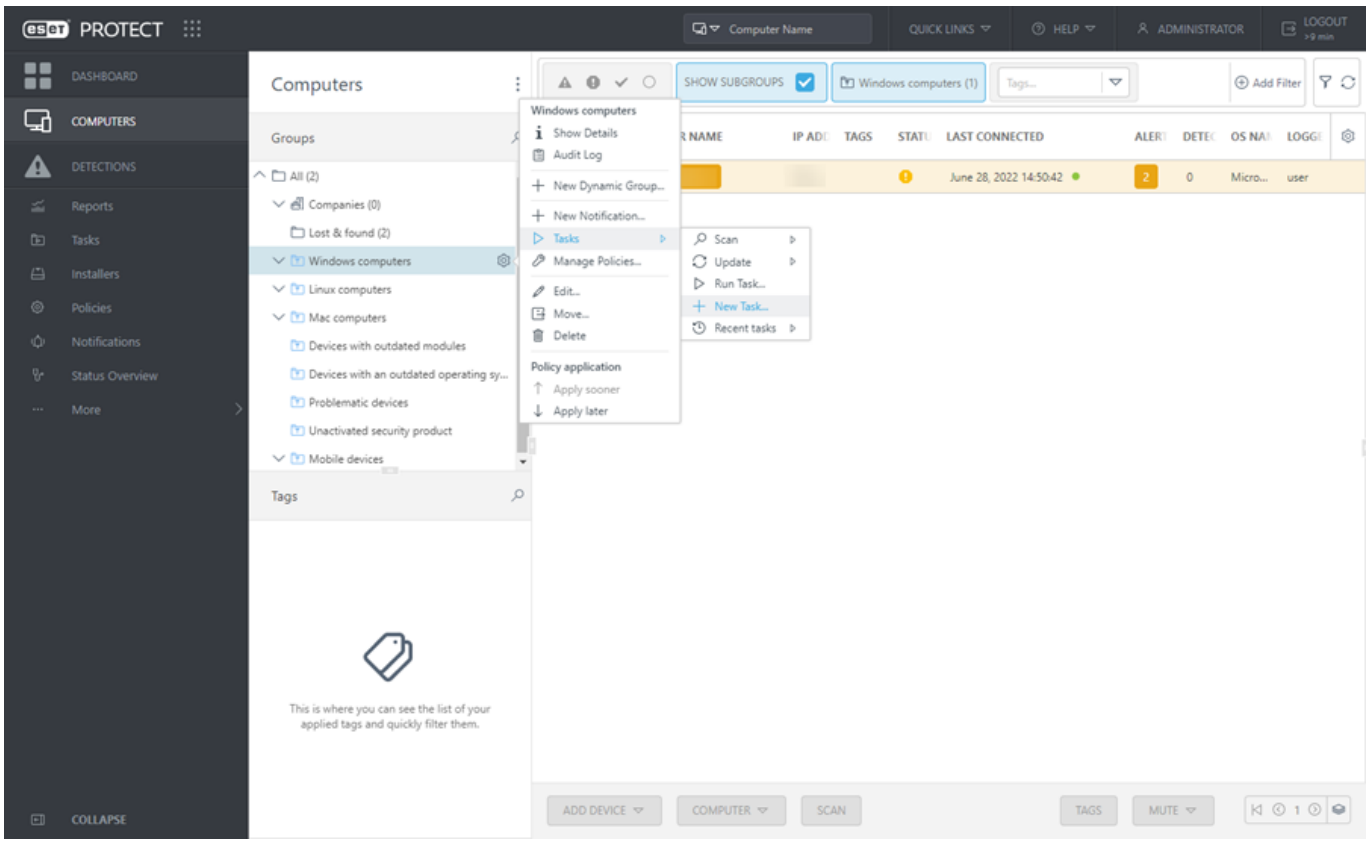


- Clique no ícone de engrenagem > **Editar >** selecione **Alterar grupo principal**. Selecione um novo grupo principal da lista e clique em **OK**.



Atribuir Tarefa do cliente a um Grupo

Clique em **Computadores**, selecione **Grupo estático** ou **Grupo dinâmico** e clique no ícone de engrenagem > **Tarefas** > **Nova tarefa**. Uma janela de Assistente de nova tarefa de cliente será aberta.

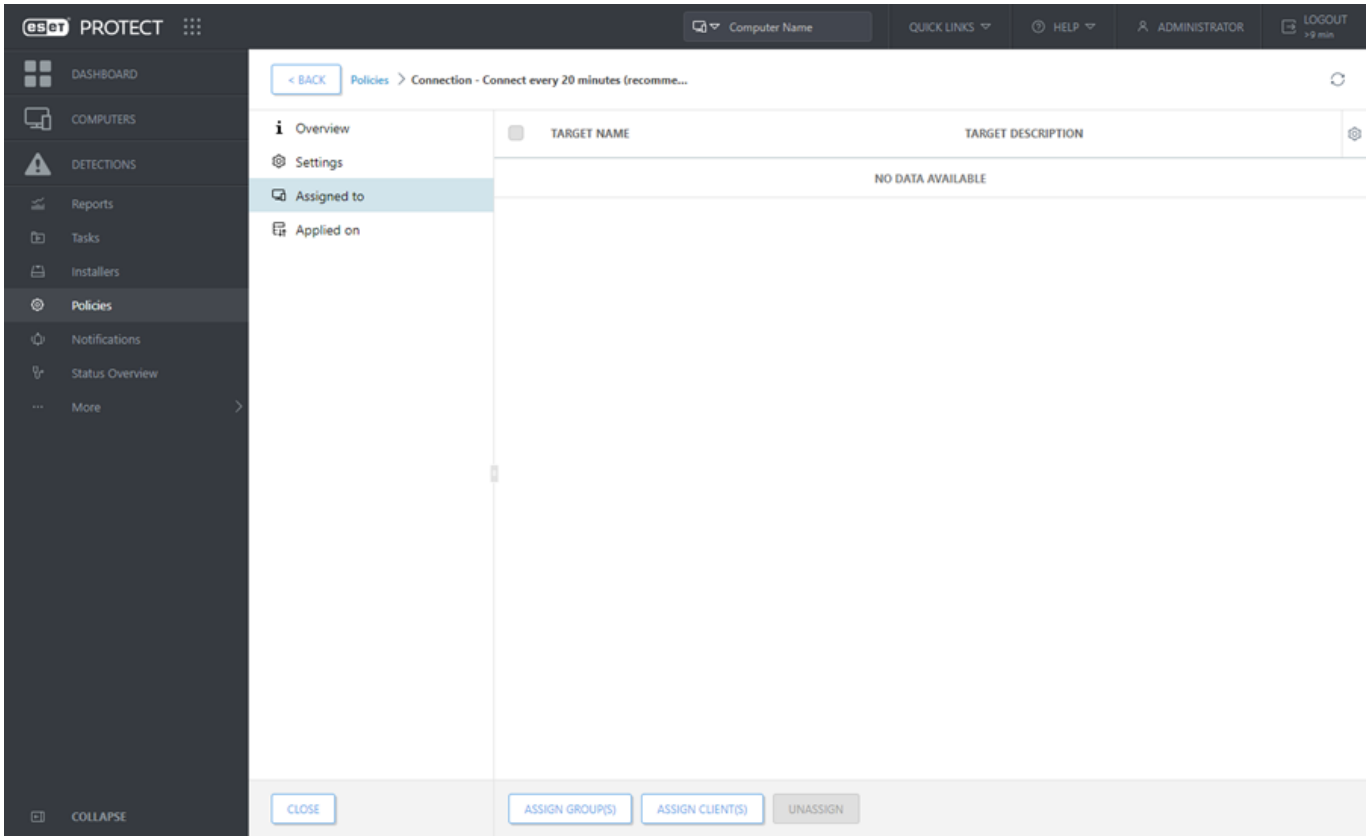


Atribuir política a um grupo

Depois que uma política é criada, você pode atribuí-la a um **grupo estático** ou **grupo dinâmico**. Existem duas maneiras de atribuir uma política:

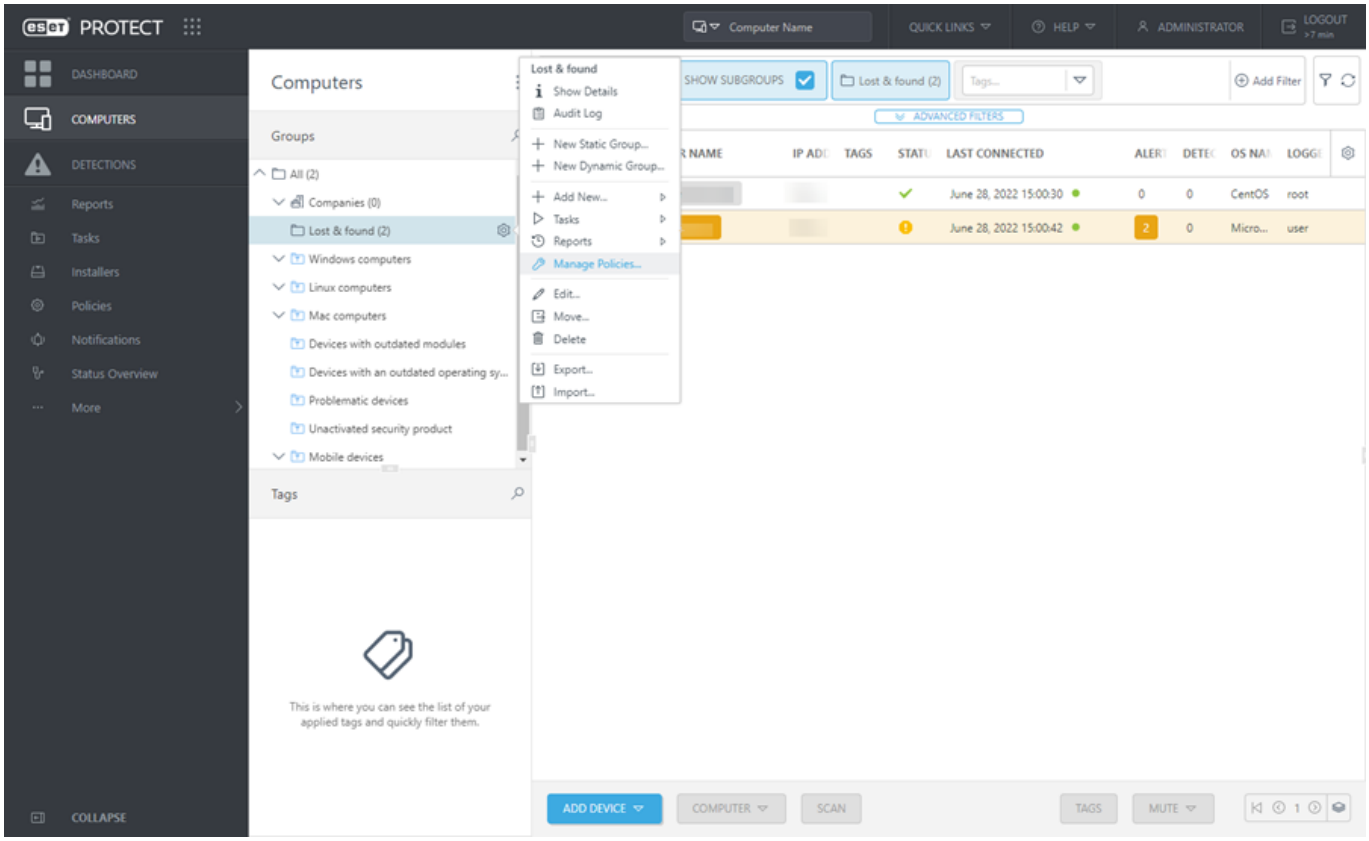
Método I.

Em **Políticas**, selecione uma política e clique em **Ações** > **Mostrar detalhes** > **Atribuído a** > **Atribuir grupo(s)**. Selecione um grupo estático ou dinâmico da lista (é possível selecionar mais grupos) e clique em **OK**.



Método II.

1. Clique em **Computadores**, clique no ícone de engrenagem ao lado do nome do grupo e selecione **Gerenciar políticas**.



2. Na janela **Ordem de aplicação de política** clique em **Adicionar política**.

3. Marque a caixa de seleção ao lado das políticas que deseja atribuir a esse grupo e clique em **OK**.

4. Clique em **Fechar**.

Para ver quais políticas estão atribuídas a um grupo em particular, selecione aquele grupo e clique na guia **Políticas** para ver uma lista de políticas atribuídas ao grupo.

Para ver quais grupos estão atribuídos a uma política específica, selecione a política e clique em **Mostrar Detalhes** > **Aplicado em**.

Para obter mais informações sobre políticas, consulte o capítulo Políticas.

Detecções

A seção **Detecções** dá a você uma visão geral de detecções encontradas em dispositivos gerenciados.

A estrutura de Grupo é exibida na esquerda. Você pode procurar grupos e visualizar detecções encontradas em membros de determinado grupo. Para visualizar todas as detecções encontradas nos clientes atribuídos a grupos para sua conta, selecione o **grupo Todos** e remova os filtros aplicados.

Consulte o Glossário ESET para mais detalhes sobre as tecnologias ESET e os tipos de detecções/ataques contra os quais elas protegem.

Status da detecção

Existem dois tipos de detecções com base em seu status:

- **Detecções ativas** – detecções ativas são detecções que ainda não foram limpas. Para limpar a detecção, execute um **Escaneamento detalhado** com a limpeza ativada na pasta que contém a detecção. A tarefa de escaneamento deve ser concluída com êxito para limpar a detecção e não fazer mais detecções. Se um usuário não resolver uma detecção ativa dentro de 24 horas de sua descoberta, ela perderá o status de **Ativa**, mas continuará não estando resolvida.

- **Detecções resolvidas** – são detecções que foram marcadas por um usuário como resolvidas, mas ainda não foram escaneadas usando o **Escaneamento detalhado**. Dispositivos com detecções marcadas como resolvidas ainda serão exibidos como filtrados até que o escaneamento seja realizado.

Um status de **Detecção tratada** indica se um produto de segurança ESET tomou medidas contra uma detecção (dependendo do tipo de detecção e da configurações do nível de limpeza):

- **Sim** – o produto de segurança ESET fez uma ação contra a detecção (remover, limpar ou colocar em quarentena).

- **Não** – o produto de segurança ESET não fez uma ação contra a detecção.

Você pode usar **Detecção tratada** como um filtro em Relatórios, Notificações e Modelos de grupo dinâmico.

Nem todas as detecções encontradas em dispositivos clientes são movidas para a quarentena. Detecções que não são colocadas em quarentena incluem:
- Detecções que não se pode remover
- Detecções que são suspeitas com base em seu comportamento, mas que não são detectadas como malware, por exemplo, PUAs.

Durante a limpeza do banco de dados, os itens em Detecções correspondentes aos relatórios de Incidentes limpos também são removidos (independentemente do status da detecção). Por padrão, o período de limpeza para relatórios de Incidente (e Detecções) está definido para 6 meses. Você pode alterar o intervalo em **Mais** > Configurações.

Agregação de detecções

Detecções são agrupadas por tempo e outros critérios para simplificar sua resolução. Se a mesma detecção ocorrer repetidamente, o console web vai exibi-la em uma única linha para facilitar sua resolução. As detecções com mais de 24 horas são agregadas automaticamente a cada meia noite. Você pode identificar detecções agrupadas pelo valor X/Y (itens resolvidos/total de itens) na coluna **Resolvido**. Você poderá ver a lista de detecções agregadas na guia **Ocorrências** nos detalhes da detecção.

Detecções em arquivos compactados

Se uma ou mais detecções forem encontradas em um arquivo compactado, o arquivo compactado e cada detecção dentro dele são reportados em **Detecções**.

Excluir um arquivo compactado que contém uma detecção não exclui a detecção. Será preciso excluir as detecções individuais dentro do arquivo. O tamanho máximo dos arquivos contidos em arquivos é 3 GB.

As detecções excluídas não serão mais detectadas, mesmo se elas ocorrerem em outro arquivo, compactado ou não.

Filtrando detecções

Por padrão, todos os tipos de detecções dos últimos sete dias são exibidos, inclusive detecções que foram limpas com sucesso. Você pode filtrar as detecções por vários critérios: **Computador colocado em mudo e Ocorreu** estão ativados por padrão.

Alguns filtros são ativados por padrão. Se as detecções estiverem indicadas no botão **Detecções** do menu principal mas você não conseguir vê-las na lista de detecções, verifique para ver quais filtros estão ativados.

Para uma visualização mais específica, você pode adicionar outros filtros, como:

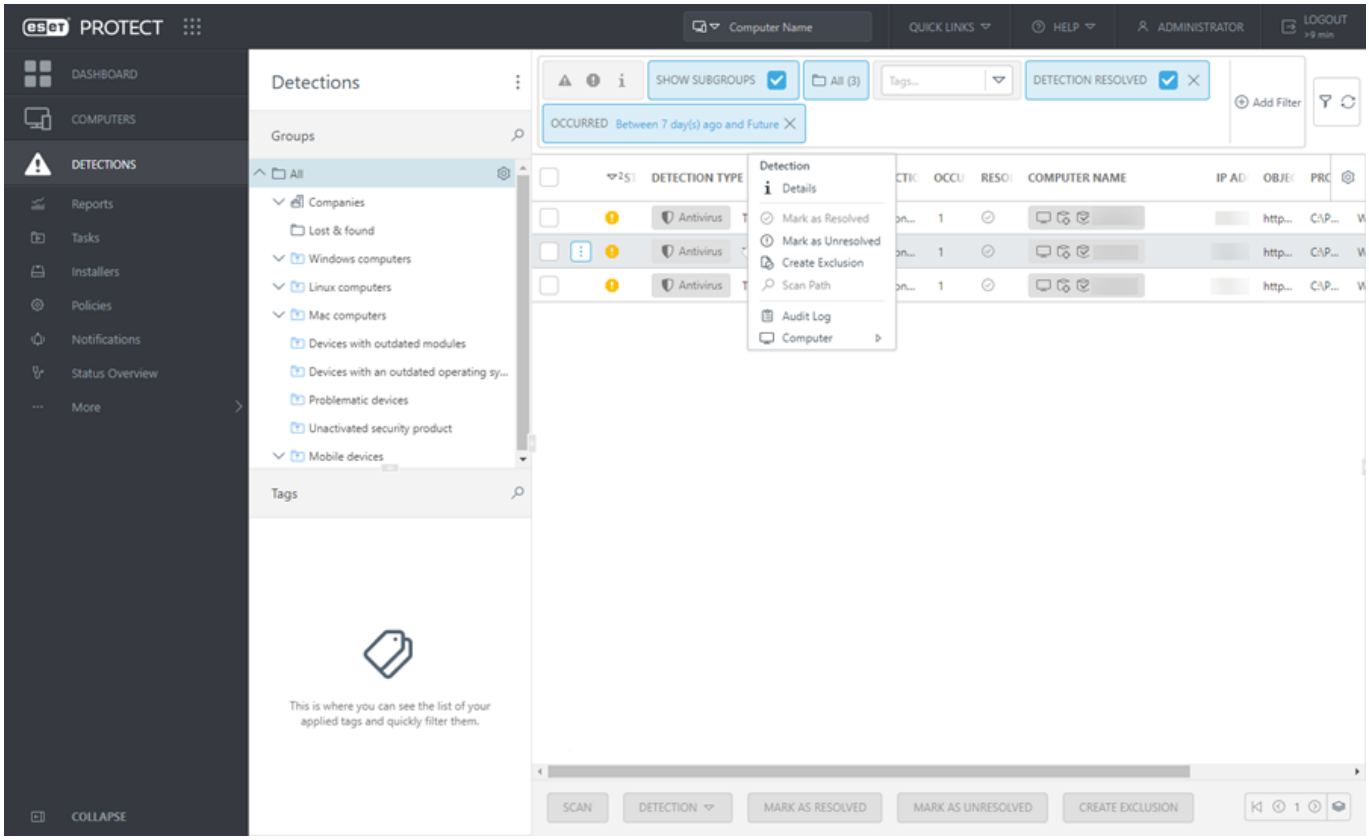
- **Categoria de detecção** – **Antivírus**, Arquivos bloqueados, ESET Inspect, **Firewall**, **HIPS** e **Proteção web**.
- **Tipo de detecção**
- **Endereço IP** do cliente que relatou a detecção
- **Escaneador** – selecione o tipo de escaneador que relatou a detecção. Por exemplo, o **Escaneador anti-ransomware** mostra as detecções reportadas pelo Escudo Anti-ransomware.
- **Ação** – selecione a ação realizada na detecção. Os produtos de segurança ESET reportam as ações a seguir para o ESET PROTECT:
  - **limpo** – a detecção foi limpa.
  - **removido / limpo por remoção** – a detecção foi removida.
  - **era parte do objeto excluído** – um arquivo compactado que incluía a detecção foi excluído.
  - **bloqueado / conexão encerrada** – o acesso ao objeto detectado foi bloqueado.
  - **retido** – nenhuma ação foi realizada devido a vários motivos, por exemplo:
    - ➢ No alerta interativo, o usuário selecionou manualmente não realizar nenhuma ação.
    - ➢ Nas configurações do mecanismo de detecção do produto de segurança ESET, o nível de **Proteção** para a categoria de detecção é definido abaixo do nível de **Relatório**.

Filtros e personalização de layout

Você pode personalizar a exibição da tela atual do console web:

- Gerenciar o painel lateral e a tabela principal.
- Adicionar filtro e predefinições de filtro. Você pode usar marcações para filtrar os itens exibidos.

Gerenciar detecções



Clique em um nome de detecção para exibir o painel lateral de Visualização de detecção no lado direito.

Para gerenciar detecções, clique no item e selecione uma das ações disponíveis ou marque a caixa de seleção ao lado de um ou mais itens e use os botões na parte inferior da tela Detecções:

- **Escaneamento** – executa a Tarefa de escaneamento sob demanda no dispositivo que relatou a detecção selecionada.
- **Detalhes** – exibe os Detalhes da detecção.
- **Computador** – uma lista de ações que você pode executar no computador onde a detecção foi encontrada. Essa lista é a mesma que a lista na seção Computadores.
- **Relatório de auditoria** - Exibe o Relatório de auditoria para o item selecionado.
- **Marcar como resolvido/** **Marcar como não resolvido** – você pode marcar as Detecções como resolvidas/não resolvidas aqui ou em Detalhes do computador.
- **Caminho de escaneamento** (disponível apenas para detecções **Antivírus** – arquivos com caminhos conhecidos) – cria a Tarefa de verificação sob demanda com caminhos e destinos predefinidos.
- **Criar exclusão** (disponível apenas para detecções de **Antivírus** e regras IDs de **Firewall**) – criar exclusões de detecção.
- **Investigar (Inspect)** permite abrir os detalhes do item diretamente no Web Console ESET Inspect. O ícone **Inspect** no canto superior direito abre a seção Detecções no Web Console ESET Inspect. Om ESET

Inspect está disponível apenas quando você tem a licença ESET Inspect e o ESET Inspect conectado ao ESET PROTECT. Um usuário do Web Console precisa de permissão de **Leitura** ou acima para **Acessar o ESET Inspect** ou permissão de **Leitura** ou acima para o **Usuário ESET Inspect**.

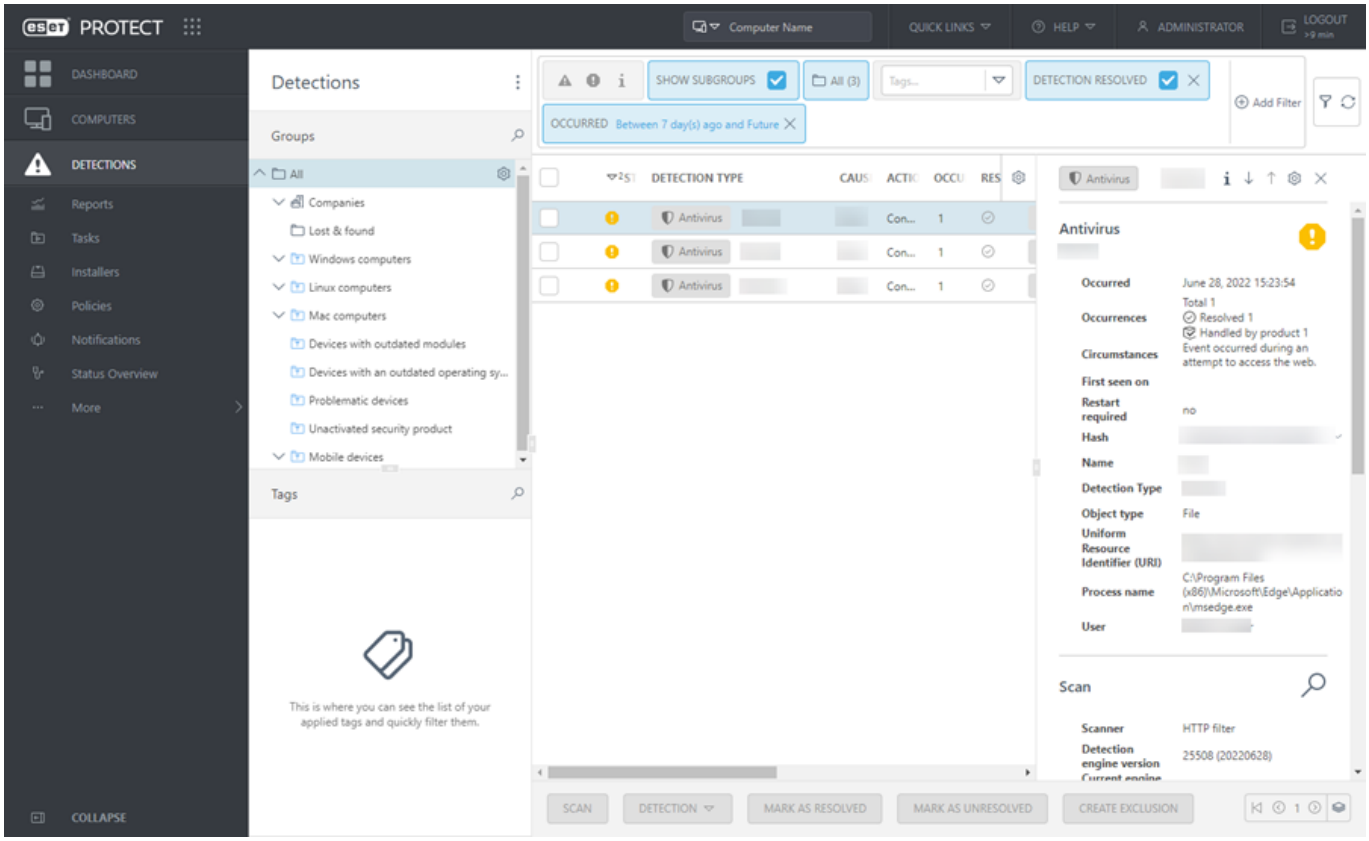
- **Enviar arquivo para ESET LiveGuard** está disponível apenas para **Arquivos bloqueados**. Você pode enviar um arquivo para análise de malware (ESET LiveGuard Advanced) do console web ESET PROTECT. Você pode ver os detalhes da análise do arquivo em Arquivos enviados. Você pode enviar manualmente arquivos executáveis para análise do ESET LiveGuard Advanced partindo do produto ESET endpoint (você precisa ter a licença ESET LiveGuard Advanced).

Visualização de detecção

Em **Detecções**, clique em um nome de detecção para exibir o painel lateral de Visualização de detecção no lado direito. O painel lateral de Visualização de detecção contém as informações mais importantes sobre a detecção selecionada.

Manipulação de visualização de detecção:

- **Mostrar detalhes** – abre os Detalhes da detecção.
- **Próximo** – exibe o próximo dispositivo no painel lateral de Visualização de detecção.
- **Anterior** – exibe o dispositivo anterior no painel lateral de Visualização de detecção.
- **Gerenciar conteúdo para Detalhes de detecção** – Você pode gerenciar quais seções do painel lateral de visualização de detecção serão exibidas e em qual ordem.
- **Fechar** – fecha o painel lateral de Visualização de detecção.



Detalhes da detecção

Há duas seções nos Detalhes da detecção:

- **Visão geral** – a seção **Visão geral** contém as informações básicas sobre a detecção. Nesta seção, você pode gerenciar a detecção com várias ações (as ações disponíveis dependem da categoria de detecção) ou ir para Detalhes do computador para ver detalhes sobre o computador onde a detecção ocorreu.

- **Ocorrências** – a seção **Ocorrências** está ativa apenas quando a detecção é agregada e fornece a lista de ocorrências individuais da detecção. Você pode marcar todas as ocorrências da mesma detecção como resolvidas/não resolvidas.

Criar exclusão

Você pode excluir os itens selecionados de futuras **detecções**. Clique em uma detecção e selecione **Criar exclusão**. Você pode excluir apenas detecções de **Antivírus** e detecções de **Firewall** – regras IDS. Você pode criar uma exclusão e aplicá-la a mais computadores/grupos. A seção **Mais** > **Exclusões** contém todas as exclusões criadas, aumenta sua visibilidade e simplifica seu gerenciamento.

⚠ Use as exclusões com cuidado - elas podem resultar em um computador infectado.

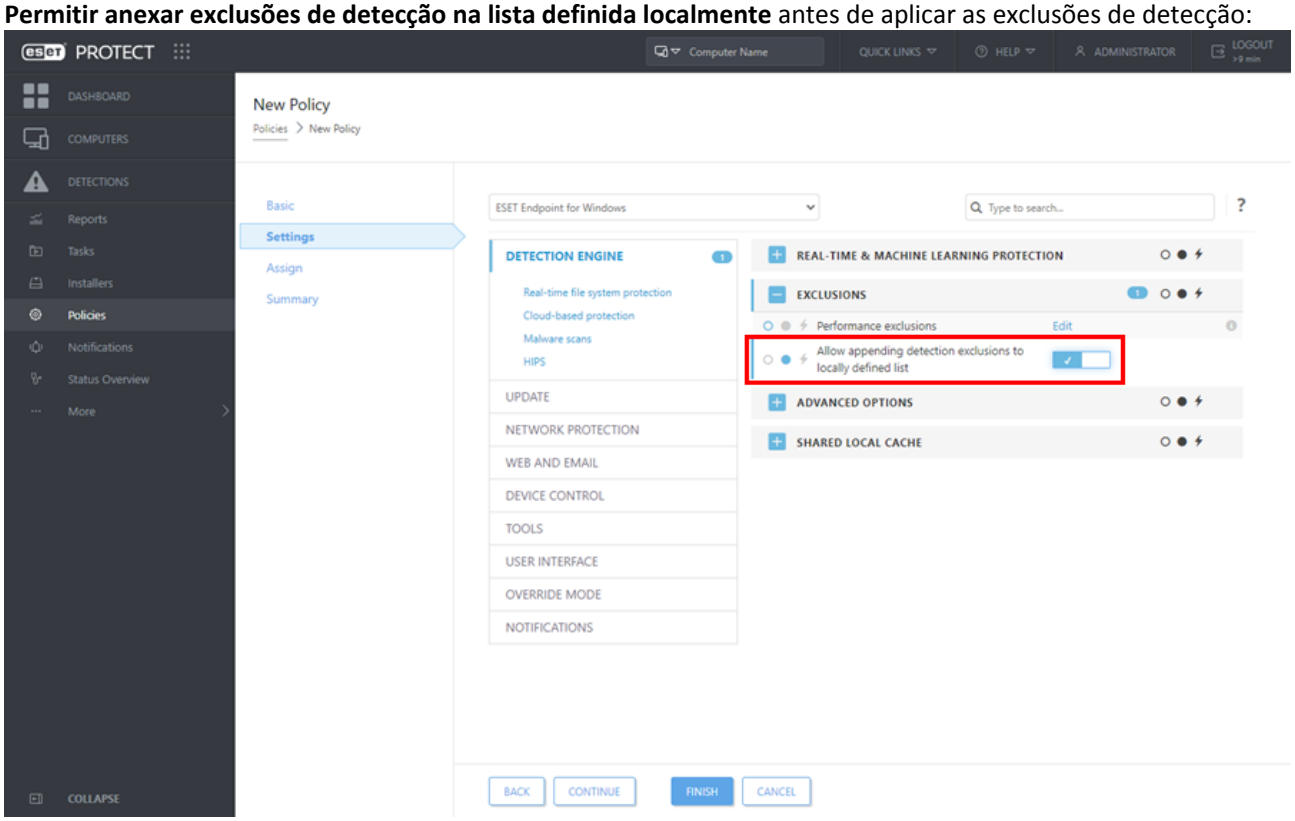
No ESET PROTECT, existem duas categorias de exclusão de **Antivírus**:

- **Exclusões de desempenho** – exclusões de arquivos e pastas definidas por um caminho. Elas podem ser criadas por meio de uma Política. Veja também o formato e os exemplos de exclusões de desempenho.

- **Exclusões de detecção** – exclusões de arquivos definidos por nome de detecção, nome de detecção e seu caminho, ou por hash do objeto. Veja também os exemplos de exclusões de detecção por nome de detecção.

Limitações das exclusões de detecção

- No ESET PROTECT não é possível criar exclusões de detecção por meio de uma Política.
- Se suas políticas anteriormente tinham exclusões de detecção, você poderá migrar exclusões de uma Política para a lista Exclusões.
- Por padrão, as exclusões de detecção substituem a lista de exclusões locais existentes nos computadores gerenciados. Para manter a lista de exclusões locais existente, é necessário aplicar a configuração de Política **Permitir anexar exclusões de detecção na lista definida localmente** antes de aplicar as exclusões de detecção:



Configurações

Você pode excluir uma ou mais detecções com base nos seguintes **Critérios de exclusão**:

Detecções de antivírus

- **Caminho e detecção** – exclui cada arquivo por seu nome e caminho de detecção, inclusive o nome do arquivo (por exemplo *file:///C:/Users/user/AppData/Local/Temp/34e1824e/ggdsfdgfd.pdf.exe*).
- **Arquivos exatos** – Exclui cada arquivo por seu hash.
- **Detecção** – Exclui cada arquivo por seu nome de detecção.

Detecções em arquivos compactados

Se uma ou mais detecções forem encontradas em um arquivo compactado, o arquivo compactado e cada detecção dentro dele são reportados em **Detecções**.

Excluir um arquivo compactado que contém uma detecção não exclui a detecção. Será preciso excluir as detecções individuais dentro do arquivo. O tamanho máximo dos arquivos contidos em arquivos é 3 GB.

As detecções excluídas não serão mais detectadas, mesmo se elas ocorrerem em outro arquivo, compactado ou não.

Detecções de firewall – regras IDS

- **Detecção e contexto** (recomendado) – exclui a detecção de firewall usando uma combinação dos critérios a seguir: por detecção, aplicativo e endereço IP.
- **Endereço IP** – exclui detecções de firewall por um endereço IP remoto. Use esta opção se a comunicação de rede com um computador em particular causar falsos positivos.
- **Detecção** – exclui a detecção e ignora o falso positivo acionado de vários computadores remotos.
- **Aplicativo** – exclui o aplicativo das detecções de rede. Permite a comunicação de rede para um aplicativo que causa um falso positivo de IDS.

A opção recomendada é pré-selecionada com base no tipo de detecção.

Marque a caixa de seleção **Resolver alertas correspondentes** para resolver automaticamente os alertas cobertos pela exclusão.

Opcionalmente, você pode adicionar um **Comentário**.

Destino

> Você pode atribuir exclusões (para ameaças de **Antivírus** e regras IDs de **Firewall**) somente a computadores com um produto de segurança ESET compatível instalado. Exclusões não serão aplicadas a produtos de segurança ESET incompatíveis e serão ignoradas neles.

Por padrão, uma exclusão é aplicada ao grupo doméstico do usuário.

Para mudar as atribuições, clique em **Adicionar destinos** e selecione o(s) destino(s) onde a exclusão será aplicada, ou selecione as atribuições existentes e clique em **Remover destinos**.

Visualizar

Permite que você veja a visão geral das exclusões criadas. Certifique-se de que todas as configurações de exclusão estão corretas com base em suas preferências.

> Depois de criar a exclusão, não é possível editá-la. Será possível apenas alterar a atribuição ou excluir a exclusão.

Clique em **Concluir** para criar a exclusão.

Você pode ver todas as exclusões criadas em **Mais** > **Exclusões**. Para verificar se um computador ou grupo tem qualquer exclusão aplicada, navegue até Detalhes do computador > **Configuração** > **Exclusões aplicadas** ou Detalhes do grupo > **Exclusões**.

Produtos de segurança ESET compatíveis com exclusões

⚠ Exclusões não serão aplicadas a produtos de segurança ESET incompatíveis e serão ignoradas neles.

Exclusões de detecção do antivírus

Todos os produtos de segurança gerenciados da ESET são compatíveis com exclusões de detecção de **Antivírus**, exceto o seguinte:

- ESET Endpoint Security para Android
- ESET LiveGuard Advanced
- ESET Inspect

Exclusões IDS de Firewall

Os produtos de segurança ESET a seguir são compatíveis com exclusões IDs de **Firewall**:

- ESET Endpoint Antivirus para Windows versão 8.0 e versões posteriores
- ESET Endpoint Security para Windows versão 8.0 e versões posteriores

Escudo contra ransomware

Produtos comerciais ESET (versão 7 e versões posteriores) incluem a **Proteção contra ransomware**. Esse novo recurso de segurança faz parte do HIPS e protege o computador contra ransomware. Quando o ransomware é detectado em um computador cliente, você pode visualizar os detalhes da detecção no console web ESET PROTECT em **Detecções**. Para filtrar apenas detecções de ransomware, clique em **Adicionar filtro** > **Escaneador** > **Escaneador anti-ransomware**. Para obter mais informações sobre o Escudo Anti-ransomware, consulte o Glossário ESET.

Você pode configurar remotamente a **Proteção contra ransomware** do console Web ESET PROTECT usando a configuração de **Política** para seu produto empresarial ESET.

- **Ativar Escudo Anti-ransomware** - O produto empresarial ESET bloqueia automaticamente todos os aplicativos suspeitos que se comportam como ransomware.
- **Ativar modo de auditoria** – quando você ativa o Modo de auditoria, as detecções identificadas pelo Escudo Anti-ransomware são reportadas no Web Console ESET PROTECT, mas não são bloqueadas pelo produto de segurança ESET. O administrador pode decidir bloquear a detecção detectada ou excluí-la, selecionando **Criar exclusão**. Esta configuração de política está disponível apenas via o console web ESET PROTECT.

Por padrão, a Proteção contra ransomware bloqueia todos os aplicativos com comportamento potencial de ransomware, inclusive aplicativos legítimos. Recomendamos que você **Ative o Modo de Auditoria** por um curto período em um novo computador gerenciado, para que você possa excluir aplicativos legítimos que são detectados como ransomware com base em seu comportamento (falsos positivos). Não recomendamos que você use o Modo de auditoria permanentemente, pois o ransomware nos computadores gerenciados não é bloqueado automaticamente quando o modo de auditoria está ativado.

ESET Inspect

ESET Inspect um sistema abrangente de Detecção e Resposta Endpoint que inclui recursos como: detecção de incidentes, gerenciamento e resposta a incidentes, coleta de dados, indicadores de detecção de compromisso, detecção de anomalias, detecção de comportamento e violações de política. Para obter mais informações sobre o ESET Inspect, sua instalação e funções, consulte a Ajuda ESET Inspect.

O ESET Enterprise Inspector e o ESET Dynamic Threat Defense foram renomeados para ESET Inspect e ESET LiveGuard Advanced.
Você pode precisar resolver os problemas causados pela renomeação se você atualizou do ESET PROTECT 9.0 e versões anteriores e tem relatórios, grupos dinâmicos, notificações ou outros tipos de regras que filtram por ESET Dynamic Threat Defense ou ESET Enterprise Inspector.

Configuração do ESET Inspect

O ESET Inspect requer que o ESET PROTECT:

- Crie um usuário ESET Inspect com permissões adequadas. O ESET PROTECT contém os conjuntos de permissões pré-definidos para os usuários ESET Inspect. Um usuário do Web Console precisa de permissão de **Leitura** ou acima para **Acessar o ESET Inspect** ou permissão de **Leitura** ou acima para o **Usuário ESET Inspect**.

- Criar certificados usados durante a Instalação do Servidor ESET Inspect.

- Ativar o ESET Inspect em um dispositivo conectado ao ESET PROTECT. Você precisa de uma licença ESET Inspect para ativar o ESET Inspect.

Se você atualizou o Servidor ESET PROTECT, reinicie o serviço de Servidor ESET Inspect para garantir que todas as alterações futuras no ESET PROTECT (por exemplo, atualizações de permissões) sejam refletidas no ESET Inspect.

Implantar o Conector ESET Inspect em computadores gerenciados

Clique em **Computadores** > clique em um computador ou selecione mais computadores e clique em **Computador** > **Soluções** > **Ativar o ESET Inspect** para implantar o Conector ESET Inspect nos computadores Windows/Linux/macOS gerenciados.

Relatório de detecções do ESET Inspect no ESET PROTECT

Se você adicionar um dispositivo que executa o Connector ESET Inspect (configurado corretamente e conectado ao Servidor ESET Inspect) no ESET PROTECT, o ESET Inspect reporta as detecções descobertas na seção Detecções

do ESET PROTECT. Você pode filtrar essas detecções selecionando a categoria de detecção **ESET Inspect**.

Outro tipo de detecção reportado pelo ESET Inspect são **Arquivos bloqueados** – as tentativas bloqueadas de iniciar executáveis bloqueados no ESET Inspect (hashes bloqueados).

Gerenciamento de detecções do ESET Inspect no ESET PROTECT

Clique na detecção e selecione **Investigar (Inspect)** para ver os detalhes da detecção no Web Console ESET Inspect.

> Certifique-se de usar os navegadores da web e produtos ESET compatíveis para permitir o gerenciamento de detecções ESET Inspect no Web Console ESET PROTECT.

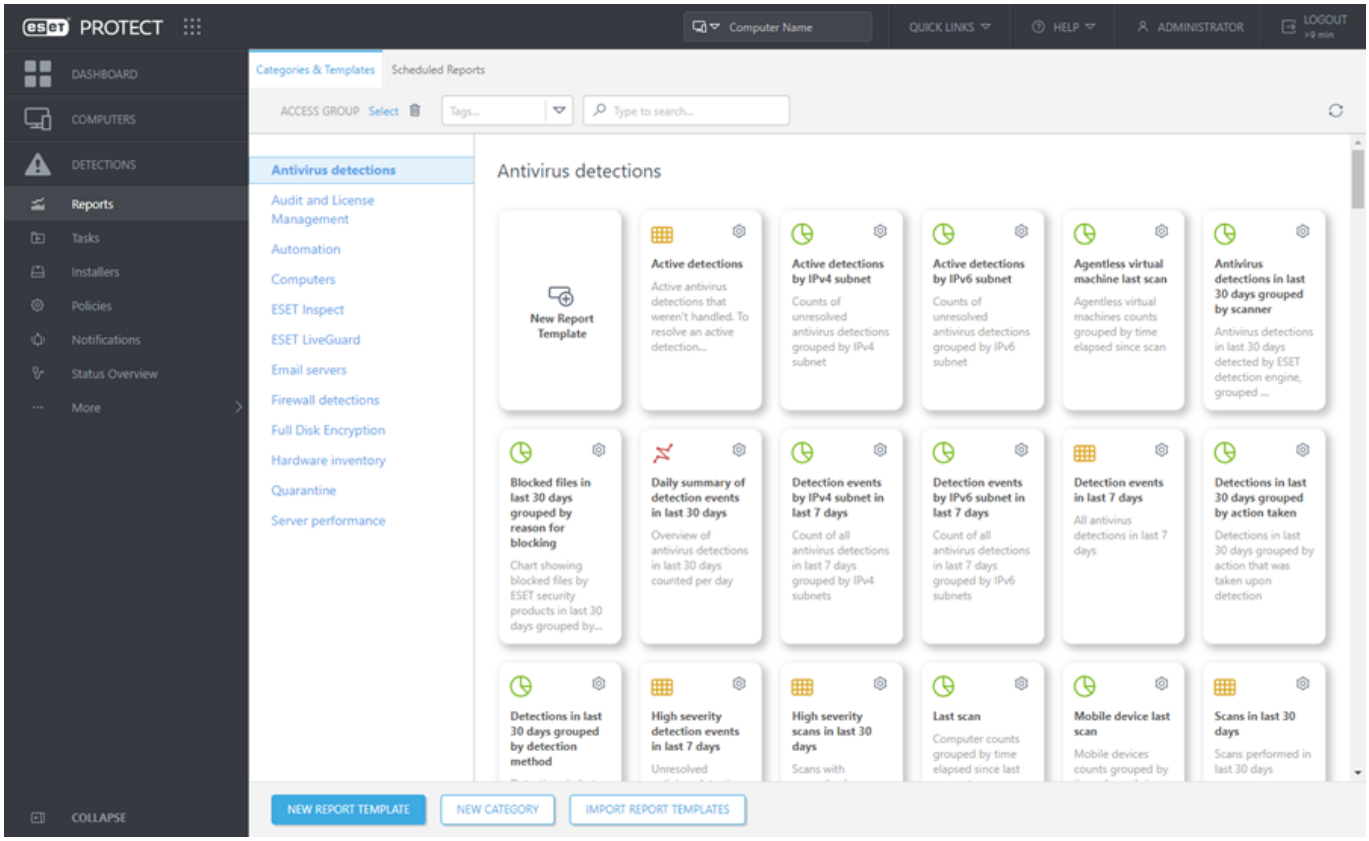
A integração de detecções ESET Inspect no Web Console ESET PROTECT permite a você gerenciar detecções do ESET Inspect diretamente do Web Console ESET PROTECT, sem precisar abrir o Web Console ESET Inspect. Por exemplo, se você marcar a detecção como resolvida no Console web ESET PROTECT, ela também será marcada como resolvida no Console web ESET Inspect e vice-versa.

Relatórios

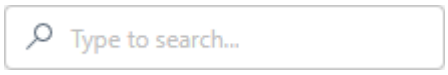
A opção Relatórios permite que você acesse e filtre dados do banco de dados de modo conveniente. A janela de relatórios é composta de duas guias:

- **Categorias e modelos** - essa é a guia padrão para a seção **Relatórios**. Ela inclui uma visão geral das categorias e modelos de relatório. Você pode criar novos relatórios e categorias ou realizar outras ações relacionadas ao relatório aqui.

- **Relatórios agendados** - essa guia oferece uma visão geral dos relatórios agendados, também é possível agendar um novo relatório aqui.

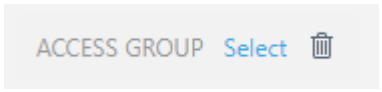


Os relatórios são gerados a partir de modelos que são categorizados por tipo de relatório. Um relatório pode ser gerado imediatamente ou pode ser agendado para ser gerado mais tarde. Para gerar e exibir um relatório imediatamente, clique em **Gerar agora** ao lado do modelo de relatório desejado. Você pode usar modelos de relatório predefinidos da lista de Categorias e modelos ou pode criar um novo modelo de relatório com configurações personalizadas. Clique em Novo modelo de relatório para abrir o assistente de modelo de relatório e especificar configurações personalizadas para um novo relatório. Também é possível criar uma nova categoria de relatório (**Nova categoria**) ou importar modelos de relatório exportados anteriormente (**Importar modelos de relatório**).



Existe uma barra de Pesquisa no topo da página. É possível pesquisar por categoria e nome de modelo, não por descrição.

Você pode usar marcações para filtrar os itens exibidos.



O botão de filtro do **Grupo de acesso** permite aos usuários selecionarem um grupo estático e filtrar os objetos visualizados de acordo com o grupo onde estão contidos.

Usando os modelos de relatório

Escolha um modelo de relatório e clique no ícone de engrenagem no bloco de modelos de relatório. As opções disponíveis são:

Gerar agora	O relatório será gerado e você poderá visualizar os dados de saída.

Fazer download	Clique em **Download** para gerar e fazer download do relatório. Você pode escolher de *.pdf* ou *.csv*. CSV é adequado apenas para dados da tabela e usa ; (ponto e vírgula) como delimitador. Se você fizer download de um relatório CSV e ver os números em uma coluna onde você espera um texto, recomendamos fazer download de um relatório PDF para ver os valores em texto.
Agendar	Agendar um relatório – Você pode modificar o acionador do agendamento, o throttling e a entrega de relatórios. Você pode encontrar todos os relatórios agendados na guia **Relatórios agendados** .
Editar	Edite um modelo de relatório existente. As mesmas configurações e opções usadas para criar um novo modelo de relatório são aplicáveis.
Relatório de auditoria	Exibe o Relatório de auditoria para o item selecionado.
Duplicar	Criar um novo relatório com base no relatório selecionado (um novo nome é necessário para o duplicado).
Excluir	Remove completamente o modelo de relatório selecionado.
Exportar	O modelo de relatório será exportado para um arquivo .dat.

O ESET Enterprise Inspector e o ESET Dynamic Threat Defense foram renomeados para ESET Inspect e ESET LiveGuard Advanced.
Você pode precisar resolver os problemas causados pela renomeação se você atualizou do ESET PROTECT 9.0 e versões anteriores e tem relatórios, grupos dinâmicos, notificações ou outros tipos de regras que filtram por ESET Dynamic Threat Defense ou ESET Enterprise Inspector.

Usando as categorias de relatório

Selecione a categoria de relatório e clique no ícone de engrenagem no canto direito da categoria. As opções disponíveis são:

Nova categoria	Insira um **Nome** para criar uma nova categoria de Modelos de relatório.
Novo modelo de relatório	Crie um novo modelo de relatório personalizado.
Excluir	Remove completamente a categoria de modelo de relatório selecionada.
Editar	Renomeie uma categoria de modelo de relatório existente.
Relatório de auditoria	Exibe o Relatório de auditoria para o item selecionado.
Exportar	A categoria de modelos de relatório e todos os modelos inclusos serão exportados para um arquivo *.dat*. Mais tarde é possível importar a categoria com todos os modelos ao clicar em **Importar modelos de relatório**. Isso é útil, por exemplo, quando você deseja migrar seus modelos de relatórios personalizados para outro ESET PROTECT. Servidor.
Grupo de acesso > **Mover**	Mova o objeto para outro grupo estático onde ele está disponível para usuários com direitos suficientes para o grupo de destino. Alterar o Grupo de acesso é útil ao resolver problemas de acesso com outros usuários. O Grupo de acesso define o grupo estático do objeto e o acesso ao objeto com base nos direitos de acesso do usuário.

O recurso **Importar modelos de relatório** / **Exportar** é projetado para importar e exportar apenas modelos de relatório, não um relatório real gerado com dados.

Permissões para Relatórios

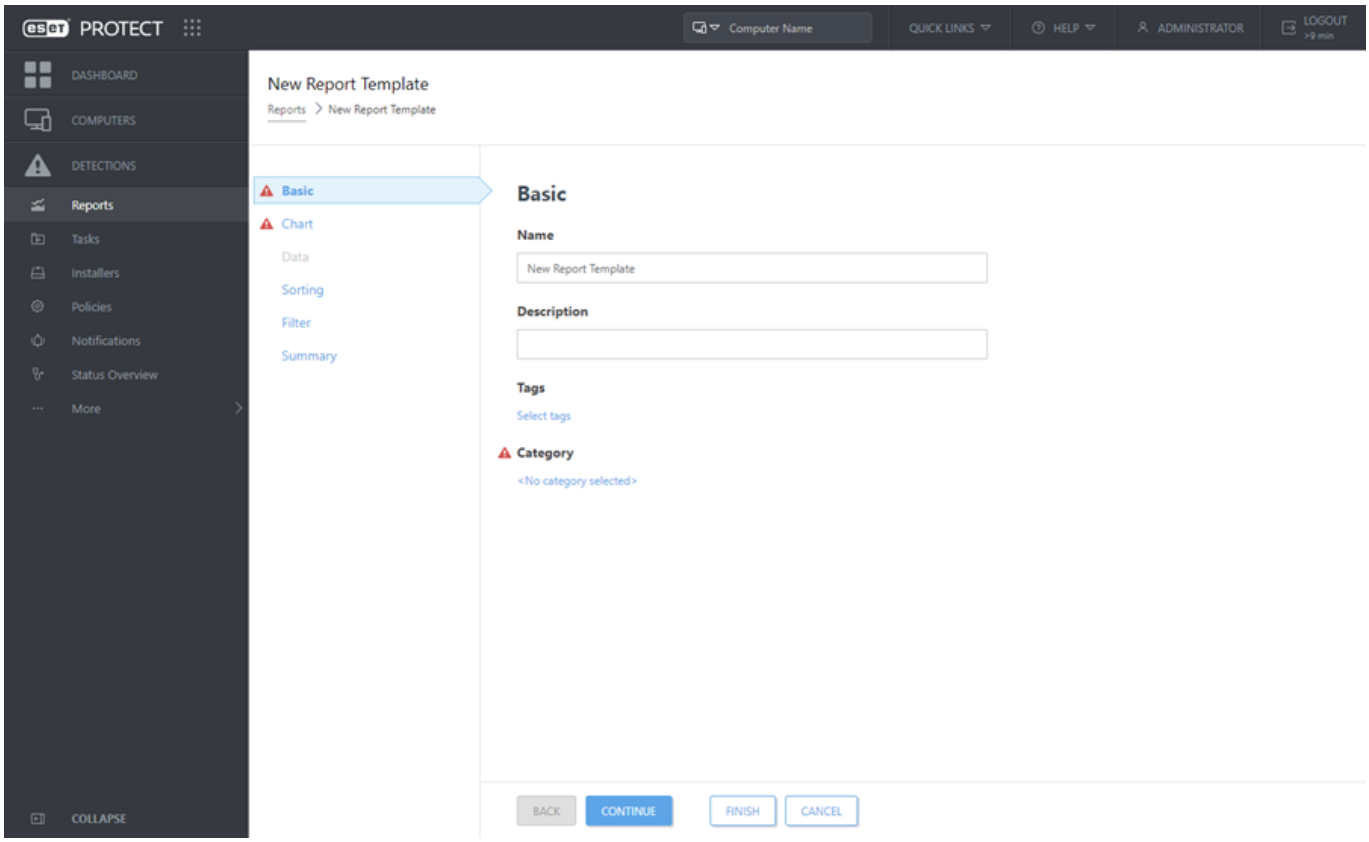
Relatórios são objetos estáticos que residem em uma estrutura de objetos no banco de dados ESET PROTECT. Cada novo modelo de relatório é armazenado no grupo inicial do usuário que o criou. Para acessar um relatório você precisa de permissões com a funcionalidade **Relatórios e Painel**. Você também precisa de permissões para objetos que são inspecionados pelo relatório. Por exemplo, se você gerar o relatório de **Visão geral de status do computador**, ele vai ter dados apenas de computadores onde você tem a permissão de **Leitura**.

- **Leitura** - o usuário pode listar modelos de relatório e suas categorias. O usuário também pode gerar relatórios com base nos modelos de relatório. O usuário é capaz de ler seu painel.
- **Uso** - o usuário pode modificar seu painel com modelos de relatório disponíveis
- **Gravação** - Cria / modifica / remove modelos de relatório e suas categorias.

Todos os modelos padrão estão localizados no grupo *Todos*.

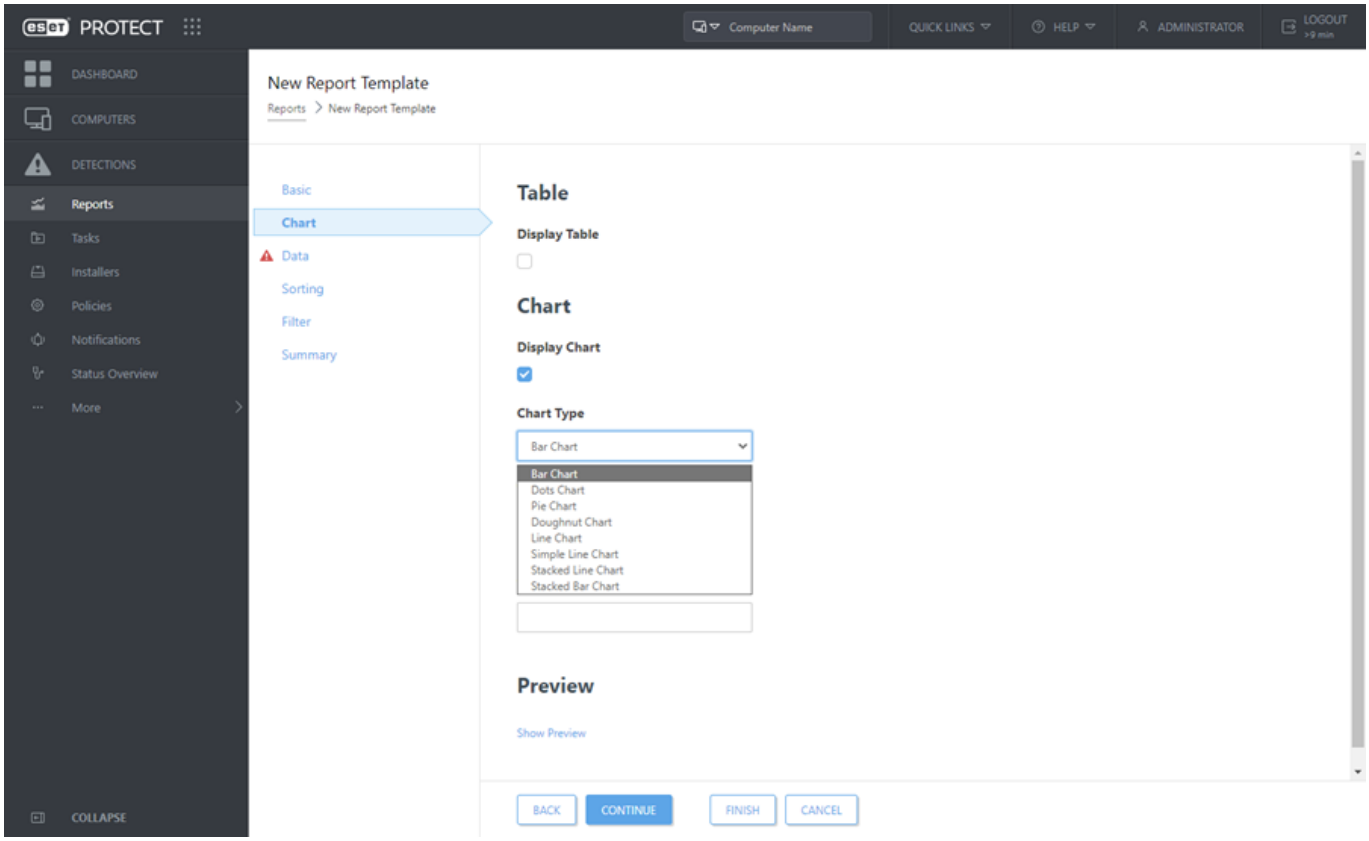
Criar um novo modelo de relatório

Navegue até **Relatórios** e clique em **Novo modelo de relatório**.



Básico

Edite as Informações básicas sobre o Modelo. Insira um **Nome**, **Descrição** e **Categoria**. Você só pode escolher das Categorias predefinidas. Se quiser criar uma nova categoria, use a opção **Nova categoria** (descrita no capítulo anterior). Clique em **Selecionar marcações** para atribuir marcações.



Gráfico

Na seção **Gráfico**, selecione o tipo **Relatório**. Uma **Tabela**, onde as informações são classificadas em linhas e colunas, ou um **Gráfico**, que representa dados usando um eixo X e Y.

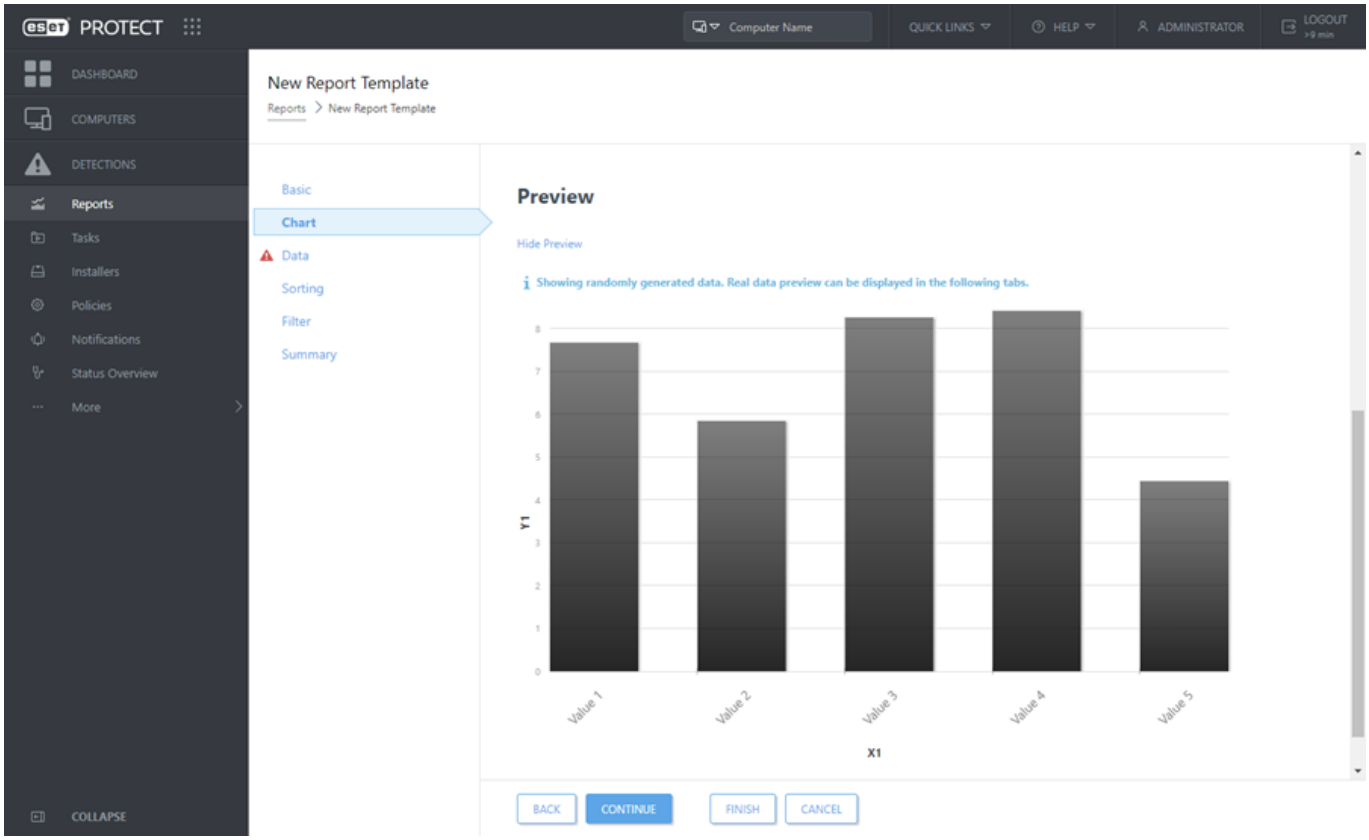
> O tipo de gráfico selecionado será exibido na seção **Visualizar**. Dessa forma, você pode ver como será o relatório em tempo real.

Selecionar um **Gráfico** oferece a você várias opções:

- **Gráfico de barras** - um gráfico com barras retangulares proporcionais aos valores que representam.
- **Gráfico de pontos** - Nesse gráfico, são usados pontos para exibir valores quantitativas (semelhante a um gráfico de barras).
- **Gráfico de pizza** - um gráfico de pizza é um gráfico circular dividido em setores proporcionais, representando valores.
- **Gráfico de rosca** - semelhante a um gráfico de pizza, mas o gráfico de rosca pode conter vários tipos de dados.
- **Gráfico de linha** - exibe informações como uma série de pontos de dados conectados por segmentos de linha reta.
- **Gráfico de linha simples** - exibe informações como uma linha com base em valores, sem pontos de dados visíveis.
- **Gráfico de linha empilhada** - esse tipo de gráfico é usado quando você quer analisar dados com diferentes unidades de medida.

• **Gráfico de barras empilhadas** - semelhante a um gráfico de barra simples, há vários tipos de dados com diferentes unidades de medidas empilhadas nas barras.

Como opção, você pode inserir um título para o eixo **X** e **Y** do gráfico para facilitar a leitura do gráfico e reconhecer tendências.



Dados

Na seção **Dados**, selecione as informações que deseja exibir:

a.**Colunas da tabela**: As informações da tabela são adicionadas automaticamente com base no tipo de relatório selecionado. Você pode personalizar os campos **Nome**, **Classificação** e **Formato** (veja a seguir).

b.**Gráfico Axes**: Selecione os dados para o eixo **X** e **Y**. Clicar em **Adicionar eixo** abrirá uma janela com opções. As opções disponíveis para o **Y** sempre dependerão das informações selecionadas para o eixo **X** e vice-versa, pois o gráfico exibirá sua relação e os dados devem ser compatíveis. Selecione as informações desejadas e clique em **OK**.

Formato

Clique no símbolo ⤢ na seção **Dados** para ver opções estendidas de formatação. Você pode alterar o **Formato** no qual os dados serão exibidos. Você pode ajustar a formatação para **Colunas da tabela** e **Eixos do Gráfico**. Nem todas as opções estão disponíveis para cada tipo de dados.

Coluna de formato	Escolha uma coluna de acordo com qual coluna atual vai ser formatada. Por exemplo, ao formatar a coluna **Nome**, escolha a coluna **Gravidade** para adicionar os ícones de gravidade ao lado dos nomes.
Valor mínimo	Define o limite mínimo para os valores exibidos.
Valor máximo	Define o limite máximo para os valores exibidos.

Cor	Escolhe um esquema de cores para a coluna. A cor é ajustada de acordo com o valor da coluna selecionado na **Coluna de formato**.
Ícones	Adicione ícones na coluna formatada de acordo com o valor da coluna selecionado na **Coluna de formato**.

Clique em uma das setas para mudar a ordem das colunas.

Classificando

Se os dados selecionados na seção **Dados** tiverem um símbolo classificável, a classificação está disponível. Clique em **Adicionar classificação** para definir a relação entre os dados selecionados. Selecione as informações iniciais (valor de classificação) e o método de classificação, seja **Ascendente** ou **Descendente**. Isso definirá o resultado exibido no gráfico. Clique em **Para cima** ou **Para baixo** para mudar a ordem dos elementos de classificação. Clique no ícone de lixo para remover o elemento da seleção.

Filtro

Defina o método de filtragem. Clique em **Adicionar filtro** e selecione o método de filtragem na lista, bem como seu valor. Isso define quais informações serão exibidas no gráfico. Clique no ícone de lixo para remover o elemento da seleção.

Resumo

No **Resumo**, verifique as opções selecionadas e informações. Clique em **Concluir** para criar um novo **modelo de relatório**.

Gerar relatório

Existem várias maneiras de gerar um relatório instantaneamente partindo de um modelo de relatório:

- Vá para **Links Rápidos** na barra superior e clique em **Gerar Relatório**. Selecione um modelo de relatório existente e clique em **Gerar agora**.

- Clique em **Relatórios** e selecione a guia **Categorias e Modelos**. Selecione um modelo de relatório do qual deseja gerar um relatório. Clique no ícone de engrenagem e depois clique em **editar** se quiser fazer alterações no modelo.

  - Você pode clicar no bloco de relatório para gerar e exibir o relatório no console web ESET PROTECT. Quando o relatório for gerado você pode clicar em **Gerar e fazer download** para salvar o relatório no seu formato desejado. Você pode escolher de *.pdf* ou *.csv*. CSV é adequado apenas para dados da tabela e usa ; (ponto e vírgula) como delimitador. Se você fizer download de um relatório CSV e ver os números em uma coluna onde você espera um texto, recomendamos fazer download de um relatório PDF para ver os valores em texto.

- Navegue até **Tarefas** > **Nova** > **Tarefa do Servidor** para criar uma nova tarefa Gerar relatório***.

  - A tarefa agora será criada e exibida na lista **Tipos de tarefa**. Selecione essa tarefa e clique em **Executar**

agora na parte inferior da página. A tarefa será executada imediatamente.

oDefina as configurações (como descrito na tarefa Gerar relatório) e clique em **Concluir**.

Quando você clica em um item exibido em um relatório mostrado no console da Web ESET PROTECT, um menu de detalhamento aparece com mais opções.

Agendar um relatório

Existem várias maneiras de agendar uma geração de relatório:

- Navegue até **Tarefas** > **Nova** > **Tarefa do Servidor** para criar uma nova tarefa Gerar relatório***.
- Vá para **Relatórios**, selecione um modelo de relatório do qual deseja gerar um relatório, clique no ícone de engrenagem no título do modelo e selecione **Agendar**. Você pode usar e editar um modelo de relatório predefinido ou criar um novo modelo de relatório.
- Clique em **Agendar** no menu de contexto de um modelo de relatório em um painel.
- Vá para a guia **Relatórios** > **Relatórios agendados** > clique em **Agendar relatório**.

Ao agendar um relatório você terá várias opções, como descrito na tarefa Gerar relatório:
- Escolha vários modelos de relatório para um relatório.
- Defina a entrega do relatório em um email e/ou salve em um arquivo.
- Opcionalmente define os parâmetros de acionador e alternância.

Depois de agendar o relatório, clique em **Concluir**. A tarefa é criada e será executada no intervalo definido no acionador (seja uma vez ou repetidamente) e com base nas configurações de throttling (opcional).

Guia Agendar relatórios

Você pode revisar seus relatórios agendados em **Relatórios > Relatórios agendados**. Outras ações disponíveis nessa guia são exibidas abaixo:

Agendar	Criar um novo agendamento para um relatório já existente.
Mostrar detalhes	Exibe informações detalhadas sobre a agenda selecionada.
Relatório de auditoria	Exibe o Relatório de auditoria para o item selecionado.
Marcações	Editar marcações (atribuir, remover atribuição, criar, remover).
Executar agora	Executar o relatório agendado agora.
Editar	Editar a agenda do relatório. Você pode adicionar ou desmarcar modelos de relatório, modificar configurações de agendamento ou editar as configurações de alternância e entrega do relatório.
Duplicar	Criar uma agenda duplicada em seu grupo inicial.
Excluir	Excluir a agenda. O modelo de relatório permanecerá.

Grupo de acesso > **Mover**	Mova o objeto para outro grupo estático onde ele está disponível para usuários com direitos suficientes para o grupo de destino. Alterar o Grupo de acesso é útil ao resolver problemas de acesso com outros usuários. O Grupo de acesso define o grupo estático do objeto e o acesso ao objeto com base nos direitos de acesso do usuário.

Filtros e personalização de layout

Você pode personalizar a exibição da tela atual do console web:

- Gerenciar o painel lateral e a tabela principal.
- Adicionar filtro e predefinições de filtro. Você pode usar marcações para filtrar os itens exibidos.

Aplicativos desatualizados

Use o relatório de **Aplicativos desatualizados** (localizado na categoria **Relatórios** > **Computadores**) para ver quais componentes ESET PROTECT não estão atualizados.

Existem dois métodos de executar este relatório:

- Adicionar um Novo painel ou modificar um dos blocos de painel existentes.
- Vá para **Relatórios** > categoria **Computadores** > bloco **Aplicativos desatualizados** > e clique em **Gerar agora**.

Se você tiver algum aplicativo desatualizado, será possível:

- Use a Tarefa de cliente ESET PROTECT Atualização de componentes para atualizar o Agente ESET Management, Servidor e MDM.
- Usar a tarefa de cliente Instalação de software para atualizar seu produto de segurança.

Exibidor de Relatório SysInspector

Usando o visualizador de relatórios SysInspector, você pode ver os relatórios de SysInspector depois deles serem executados em um computador cliente. Você também pode abrir os relatórios SysInspector diretamente de uma tarefa de solicitação de relatório do SysInspector depois que ele foi executado com sucesso. É possível fazer download e exibir arquivos de relatório no SysInspector na sua máquina local.

> O ESET SysInspector é executado apenas em computadores Windows.

Como ver o relatório SysInspector

De um painel

1. Adicionar um Novo painel ou editar um relatório de painel existente.
2. Selecione o modelo de relatório **Automação** > **Histórico de instantâneos do SysInspector nos últimos 30**

dias.

3.Abra o relatório, selecione um computador e selecione **Abrir visualização de relatório SysInspector** no menu suspenso.

De um relatório

1.Navegue para a categoria Relatórios > **Automação**.

2.Selecione o modelo **Histórico de instantâneos do SysInspector nos últimos 30 dias** da lista e clique em **Gerar agora**.

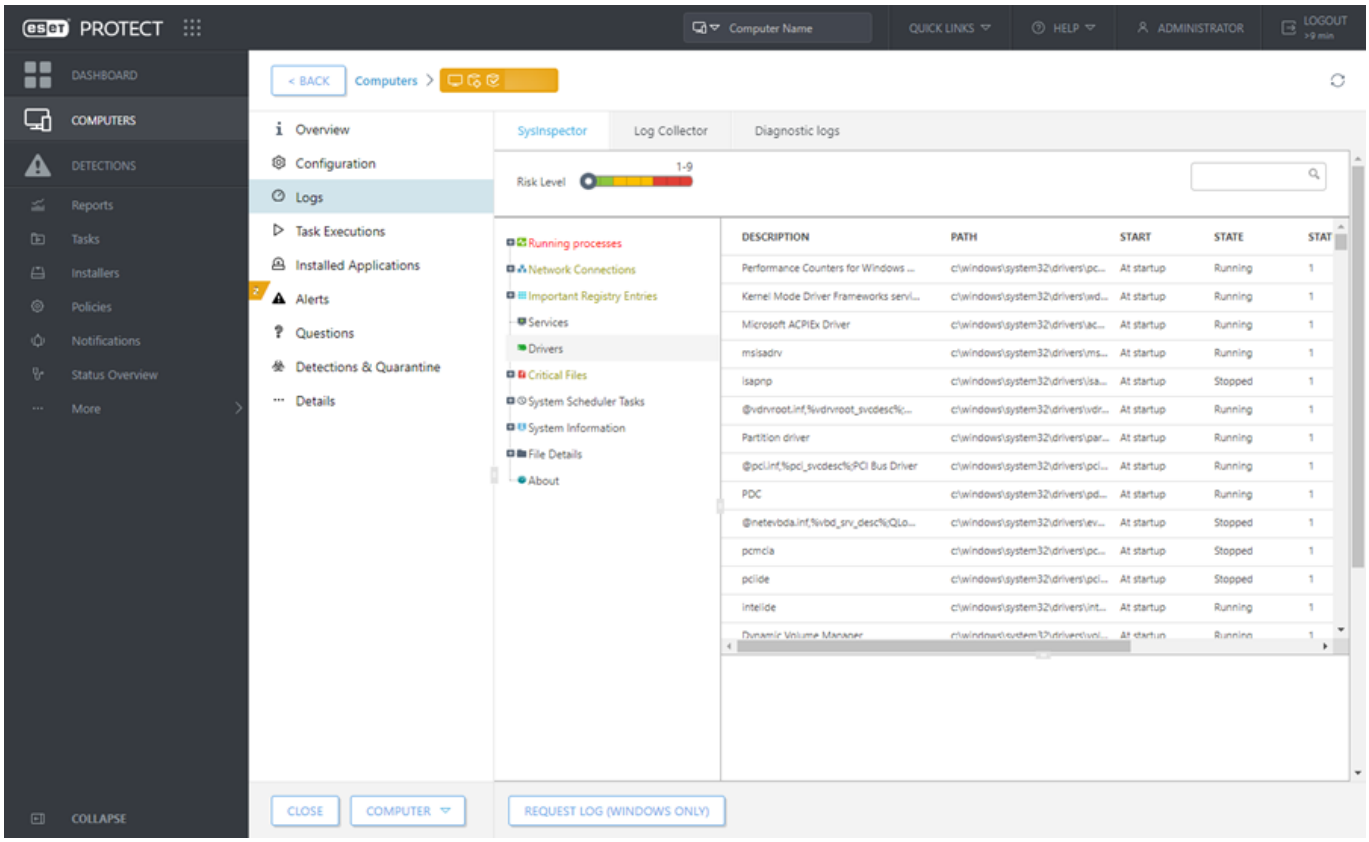
3.Abra o relatório, selecione um computador e selecione **Abrir visualização de relatório SysInspector** no menu suspenso.

Do menu Computadores

1.Navegar para Computadores.

2.Selecione um computador no Grupo Estático ou Dinâmico e clique em **Mostrar Detalhes**.

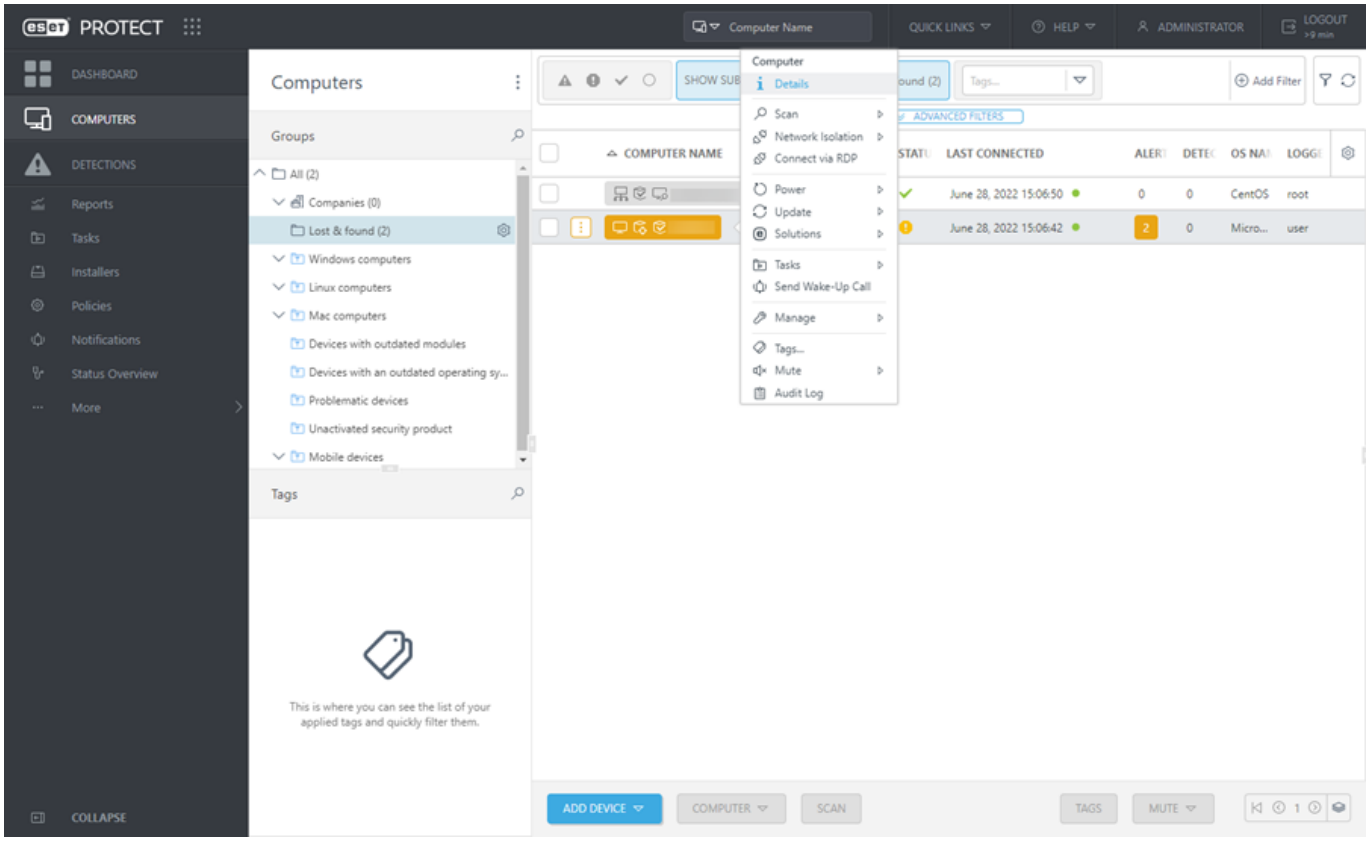
3.Navegue para a seção **Relatórios** > guia **SysInspector**, clique em uma entrada de lista e selecione **Abra o exibidor de Visualizador do Relatório do Sysinspector**.



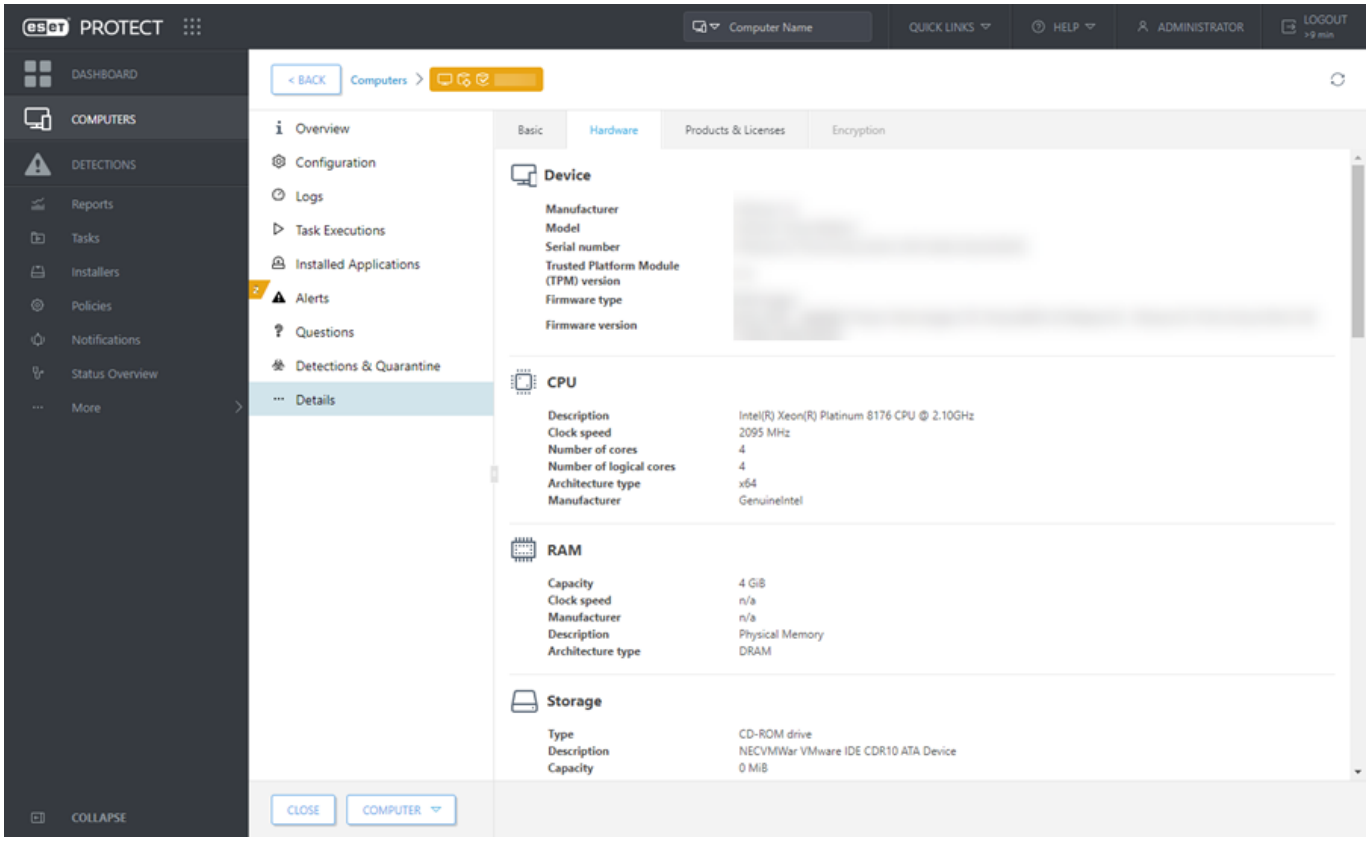
Inventário de hardware

O ESET PROTECT possui a capacidade de recuperar detalhes de inventário de hardware de dispositivos conectados, como detalhes sobre a RAM, armazenamento e processador de um dispositivo.

Clique em **Computadores** > clique em um dispositivo conectado e selecione **Detalhes**.



Clique em **Detalhes** e selecione a guia **Hardware**.



Relatórios de inventário de hardware

Você pode encontrar relatórios de inventário de hardware pré-definidos em **Relatórios** > **Inventário de hardware**. Você pode criar relatórios de Inventário de hardware personalizados. Ao criar um Novo modelo de relatório, em **Dados** selecione uma subcategoria de um dos filtros **Inventário HW**. Quando adicionar a primeira coluna ou eixo X da tabela, apenas dados compatíveis poderão ser selecionados.

Grupos dinâmicos baseados em inventário de hardware

Você pode criar Grupos dinâmicos personalizados com base nos detalhes de Inventário de hardware dos dispositivos conectados. Ao criar um Novo modelo de grupo dinâmico, selecione regra(s) das categorias de **Inventário de hardware** para filtrar dispositivos conectados com base em seus parâmetros de hardware.

Você pode selecionar a partir das categorias de Inventário de hardware a seguir: Chassi, informações do dispositivo, tela, adaptador de tela, dispositivo de entrada, armazenamento em massa, adaptador de rede, impressora, processador, RAM e dispositivo de som. Por exemplo, você pode criar um grupo dinâmico com dispositivos filtrados por sua capacidade RAM para ter uma visão geral dos dispositivos com uma certa quantidade de RAM.

Sistemas operacionais compatíveis com inventário de hardware

O recurso de inventário de hardware está disponível em todos os computadores Windows, Linux* e macOS compatíveis.

* Instale o pacote `lshw` na máquina Linux do cliente/servidor para que o Agente ESET Management reporte 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`

Relatório de auditoria.

O **Relatório de auditoria** contém todas as ações e alterações realizadas pelos usuários no ESET PROTECT. Servidor.

Para executar esse relatório, clique em **Relatórios** > categoria **Auditoria e gerenciamento de licenças** > **Relatório de auditoria**.

Você pode visualizar e filtrar um relatório de auditoria diretamente no Web Console em **Mais** > **Relatório de auditoria**.

Para ver o Relatório de auditoria, o usuário do Web Console deve ter um conjunto de permissões com a funcionalidade ***Relatório de auditoria.

Tarefas

Você pode usar **Tarefas** para gerenciar o ESET PROTECT Servidor, computadores do cliente e seus produtos ESET. Tarefas podem automatizar trabalhos de rotina. Há um conjunto de tarefas predefinidas que cobre os cenários mais comuns, ou você pode criar tarefas personalizadas com configurações específicas. Usar as tarefas solicitar uma ação dos computadores cliente. Para executar uma tarefa com sucesso, é preciso ter direitos de acesso suficientes para a tarefa e para os objetos (dispositivos) usados pela tarefa. Veja a lista de permissões para obter mais informações sobre os direitos de acesso.

Há duas categorias de tarefa principais: Tarefas do cliente e Tarefas do servidor.

- Você pode atribuir Tarefas do cliente a grupos ou computadores individuais. Quando criada, uma tarefa é executada usando um Acionador. Uma Tarefa do cliente pode ter mais acionadores configurados. Tarefas de cliente são distribuídas a clientes quando o Agente ESET Management de um cliente conecta ao ESET PROTECT. Servidor. Por isso, pode levar algum tempo para os resultados de uma execução de tarefa serem comunicados ao ESET PROTECT. Servidor. Você pode gerenciar seu intervalo de conexão do Agente ESET Management para reduzir os tempos de execução.

- As tarefas do servidor são executadas pelo ESET PROTECT Servidor em si mesmo ou em outros dispositivos. Tarefas do servidor não podem ser atribuídas a um cliente ou grupo de cliente específicos. Cada tarefa do servidor tem um acionador configurado. Se a tarefa precisar ser executada com vários eventos, é preciso que existam tarefas do servidor separadas para cada acionador.

Você pode criar uma nova tarefa de duas maneiras:

- Clique em **Novo** > **Tarefa do cliente** ou **Tarefa do servidor**.

- Selecione o tipo de tarefa desejado à esquerda e clique em **Novo** > Tarefa do cliente ou Tarefa do servidor.

As seguintes tarefas predefinidas estão disponíveis para sua conveniência (cada Categoria de tarefa contém Tipos de tarefas):

Todas as tarefas

Tarefas de cliente

Produto de Segurança ESET

Diagnóstico
Parar com o isolamento do computador
Exportar configuração de produtos gerenciados
Isolar computador da rede
Atualização de módulos
Reversão de atualização dos módulos
Rastreamento sob demanda
Ativação do produto
Gerenciamento de quarentena
Executar script do SysInspector
Enviar arquivo para ESET LiveGuard
Escaneamento de servidor
Instalação de software
Solicitação de relatório do SysInspector (apenas Windows)
Carregar arquivo em quarentena

ESET PROTECT

Diagnóstico
Redefinir agente clonado
Redefinição de banco de dados do Rogue Detection Sensor
Atualização de componentes do ESET PROTECT
Interromper gerenciamento (desinstalar agente ESET Management)

Sistema operacional

Exibir mensagem
Sair
Atualização de sistema operacional
Executar comando
Desligar computador
Instalação de software
Desinstalação de software
Interromper gerenciamento (desinstalar agente ESET Management)

Móvel

Ações Antifurto
Exibir mensagem
Exportar configuração de produtos gerenciados
Atualização de módulos
Rastreamento sob demanda
Ativação do produto
Instalação de software
Interromper gerenciamento (desinstalar agente ESET Management)

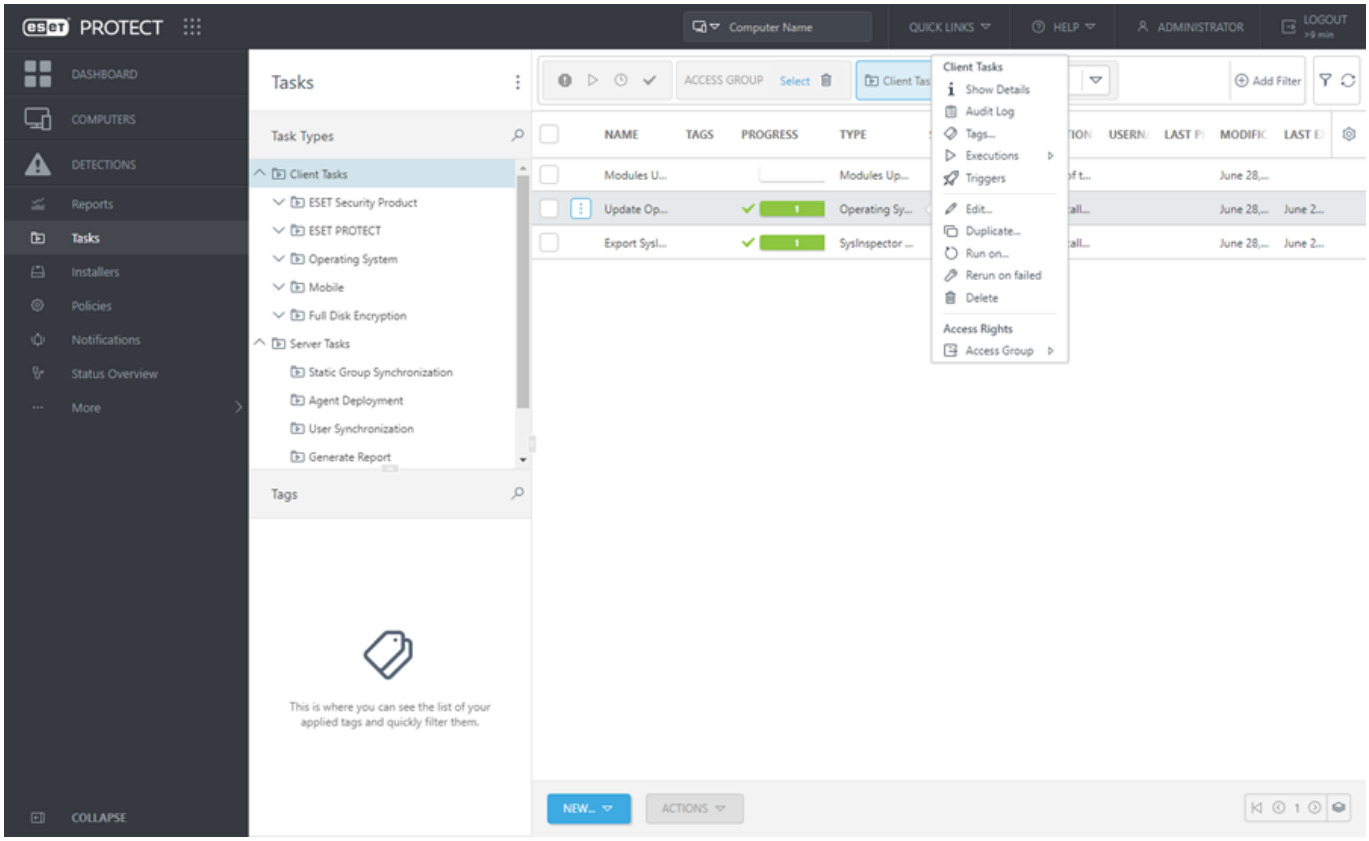
Tarefas do servidor

Implantação do Agente - distribui o Agente aos computadores cliente.
Excluir computadores não conectando - exclui os clientes que não se conectam mais ao ESET PROTECT a partir do console da Web.
Gerar relatório - usado para gerar relatórios conforme eles são necessários.
Renomear computadores - esta tarefa vai renomear computadores periodicamente em grupos usando o formato FQDN.
Sincronização de grupo estático - atualiza informações do grupo para exibir os dados atuais.
Sincronização de usuário - atualizações de usuário ou grupo de usuários.

Visão geral de tarefas

Em **Tarefas** você pode ver a barra de indicadores de progresso, o ícone de status e os detalhes para cada tarefa criada.

Você deve criar um Acionador para executar uma Tarefa do cliente.



Clique em uma tarefa para realizar mais ações de tarefa:

Mostrar detalhes	Exibir Detalhes da tarefa: resumo, execuções, acionadores (os detalhes do acionador estão disponíveis apenas para Tarefas do cliente).
Relatório de auditoria	Exibe o Relatório de auditoria para o item selecionado.
Marcações	Editar marcações (atribuir, remover atribuição, criar, remover).
Execuções	Apenas Tarefas do cliente: Você pode selecionar de resultados de execução de tarefas e tomar novas ações se necessário, vá para Detalhes da tarefa para mais detalhes.
Acionadores	Apenas Tarefas do cliente: Veja a lista de Acionadores para a Tarefa do cliente selecionada.
Editar	Editar a Tarefa selecionada. Editar tarefas existentes é útil quando você precisa fazer apenas pequenos ajustes. Para tarefas mais únicas, você pode preferir criar uma nova tarefa.
Duplicar	Criar uma nova tarefa com base na tarefa selecionada, um novo nome é necessário para a tarefa duplicada.
Executar agora	Apenas Tarefas do servidor: Execute a Tarefa do servidor selecionada.
Executar em	Apenas Tarefas do cliente: Adicione um Novo acionador e selecione os computadores ou grupos de destino para a Tarefa do cliente.

A nova execução falhou	Apenas Tarefas do cliente: Cria um novo Acionador com todos computadores que falharam durante uma execução anterior da Tarefa definidos como destinos. Você pode editar as configurações de tarefa se preferir, ou clicar em Concluir para executar novamente a tarefa inalterada.
Excluir	Remove completamente a tarefa selecionada. • Se a tarefa for excluída depois de ser criada mas antes de ser programada para começar, ela será excluída e não será executada nem vai começar. • Se a tarefa for excluída depois de estar com a execução agendada, a tarefa será concluída mas as informações não serão exibidas no console da Web.
Grupo de acesso > **Mover**	Mova o objeto para outro grupo estático onde ele está disponível para usuários com direitos suficientes para o grupo de destino. Alterar o Grupo de acesso é útil ao resolver problemas de acesso com outros usuários. O Grupo de acesso define o grupo estático do objeto e o acesso ao objeto com base nos direitos de acesso do usuário.

Filtros e personalização de layout

Você pode personalizar a exibição da tela atual do console web:

- Gerenciar o painel lateral e a tabela principal.
- Adicionar filtro e predefinições de filtro. Você pode usar marcações para filtrar os itens exibidos.

Indicador de progresso

O indicador de progresso é uma barra de cores que mostra o status de execução de uma Tarefa. Cada Tarefa tem seu próprio indicador (mostrado na linha **Progresso**). O status de execução de uma Tarefa é exibido em três cores diferentes, e inclui o número de computadores naquele estado para uma determinada tarefa:

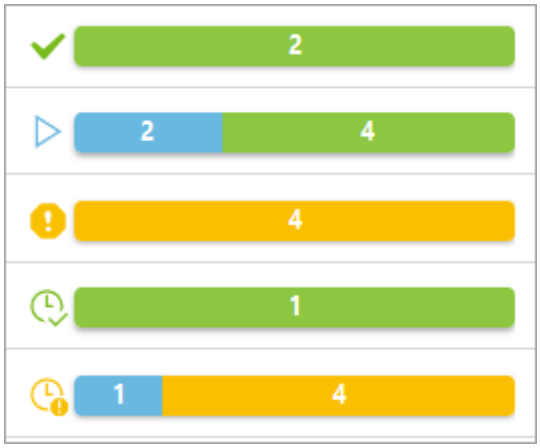
Em execução (azul)

Concluído com sucesso (verde)

Falha (laranja)

Tarefa criada recentemente (branco) – pode levar algum tempo até que o indicador mude de cor, o ESET PROTECT Servidor deve receber uma resposta do Agente ESET Management para exibir o status de execução. O indicador de progresso será branco se não houver acionador atribuído.

Uma combinação do acima:



Consulte o Ícone de status para detalhes sobre tipos de ícones e status diferentes.

O indicador de progresso mostra o status de uma tarefa quando ela foi executada pela última vez. Esta informação vem do Agente ESET Management. O indicador de progresso mostra exatamente o que o Agente ESET Management está relatando dos computadores cliente.

Ícone de status

O ícone ao lado do Indicador de progresso fornece informações adicionais. Ele mostra se existe alguma execução planejada para uma determinada Tarefa, assim como o resultado das execuções que foram concluídas. Esta informação é listada pelo ESET PROTECT. Servidor. Os seguintes estados podem ser indicados:

Em execução	A tarefa está sendo executada em pelo menos um destino, não há nada planejado e nenhuma falha de execução. Isso se aplica mesmo se a tarefa já terminou em alguns destinos.
Êxito	A tarefa foi concluída com êxito em todos os destinos, não há execução programada ou em andamento.
Erro	A Tarefa foi executada em todos os destinos, mas falhou em pelo menos um. Nenhuma outra execução está planejada (programada).
Planejado	A tarefa está planejada para execução, mas ainda não existem execuções em andamento.
Planejado / Em execução	A tarefa tem execuções planejadas (do passado ou no futuro). Nenhuma execução falhou e pelo menos uma execução está sendo executada atualmente.
Planejado / Bem sucedido	A tarefa ainda tem algumas execuções agendadas (do passado ou no futuro), nenhuma execução com falha ou em execução e pelo menos uma execução foi concluída com êxito.
Planejado / Erro	A tarefa ainda tem algumas execuções agendadas (do passado ou no futuro), nenhuma execução em andamento e pelo menos uma execução falhou. Isso é aplicado mesmo se algumas execuções foram concluídas com êxito.

Detalhes da tarefa

Clique em uma tarefa e selecione **Mostrar detalhes** para visualizar os detalhes da tarefa nas seguintes guias:

Resumo

Essa guia contém uma visão geral das configurações da tarefa.

Execuções

A guia **Execuções** exibe uma lista de computadores com resultados de execução de Tarefas do cliente. A guia **Execuções** não está disponível para Tarefas do servidor.

Se existirem muitas execuções, você pode filtrar a exibição para limitar os resultados.

Clique em **Adicionar filtro** para filtrar as execuções selecionadas por status:

- **Planejado** – **sim** (tarefa de cliente planejada para execução), **não** (execução da tarefa do cliente concluída).
- **Último status** – **Sem status**, **Em execução**, **Concluído**, **Falhou**

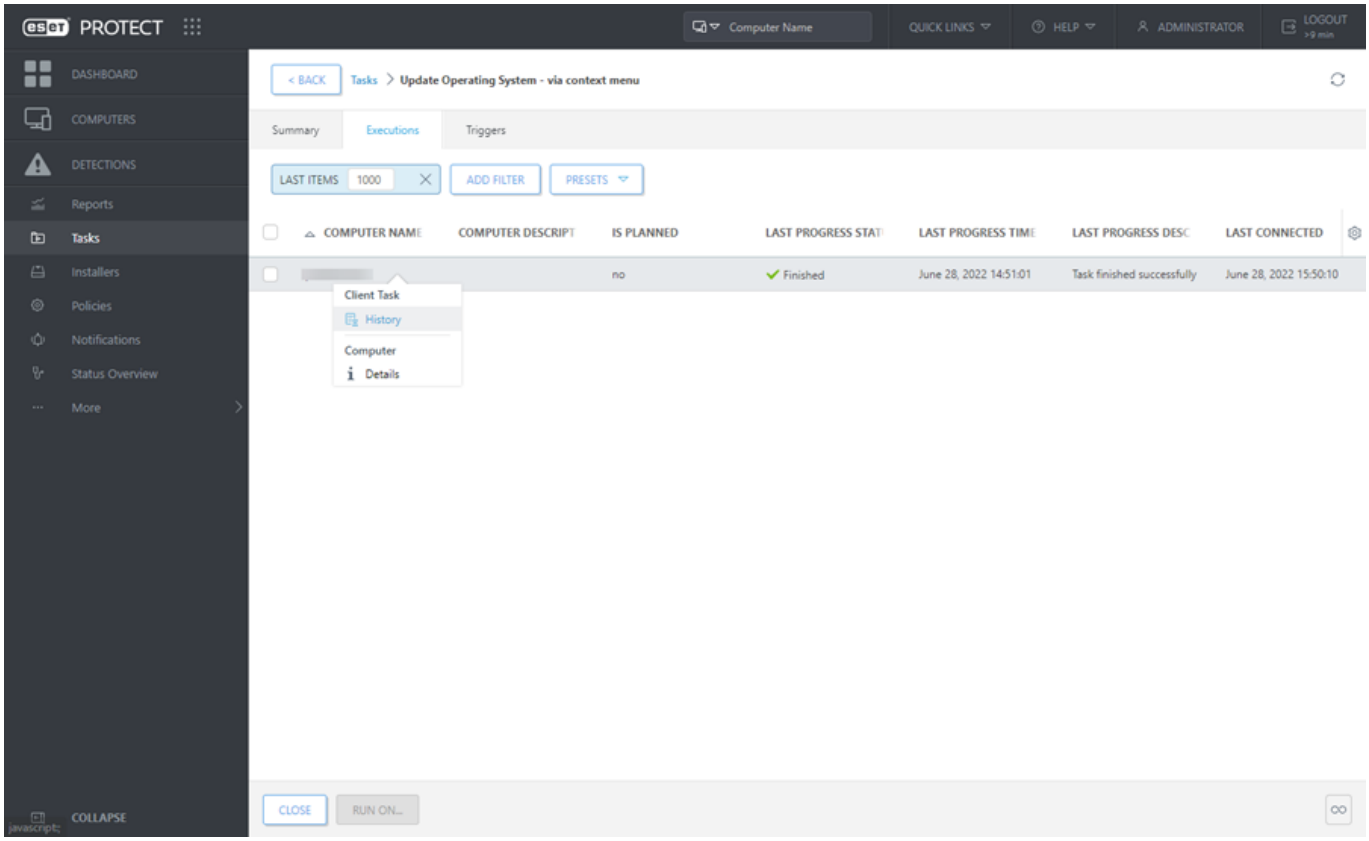
Você pode modificar o filtro ou desligá-lo para ver todos os computadores, independentemente do seu último status.

Clique em uma linha sob **Nome do computador** ou**Descrição do computador** para tomar novas ações:

- **Histórico** – veja os detalhes de execução da tarefa de cliente, inclusive quando a execução **Ocorreu**, o **Produto**, o **Status do progresso**, a **Descrição do progresso** e **Rastrear mensagem** (se estiver disponível). Você pode usar **Rastrear mensagem** para examinar o resultado da Tarefa de cliente que falhou.

> - Se você não estiver vendo nenhuma entrada na tabela **Histórico**, tente definir o filtro **Ocorreu** para uma duração maior.
> - Ao instalar produtos ESET anteriores, o Rastrear mensagem vai reportar: **Tarefa entregue para o produto gerenciado**.

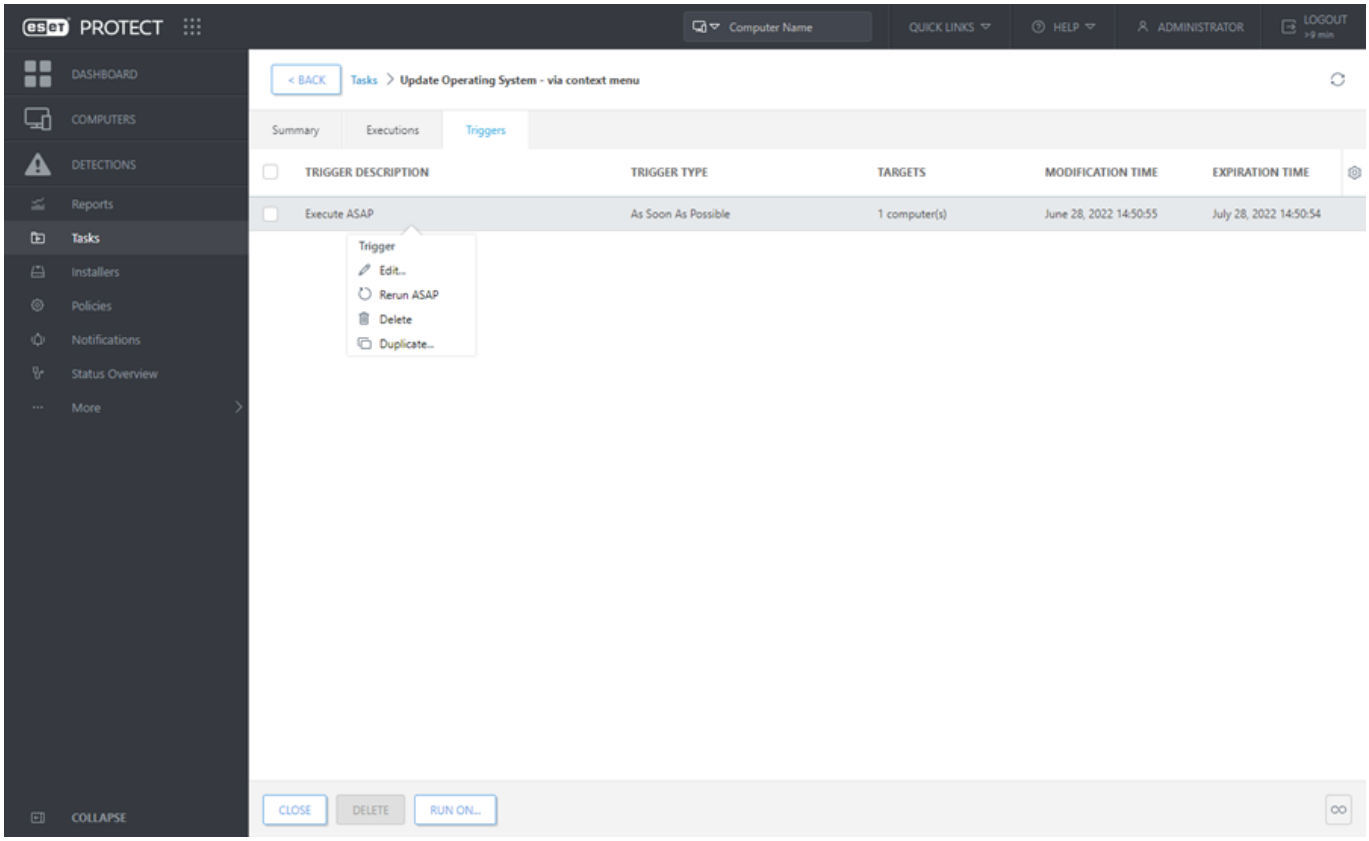
- **Detalhes** – exibir detalhes para o computador selecionado.



Acionadores

A guia **Acionadores** está disponível apenas para Tarefas do cliente e mostra a lista de Acionadores para a Tarefa do cliente selecionada. Para gerenciar o acionador, clique nele e selecione um dos itens a seguir:

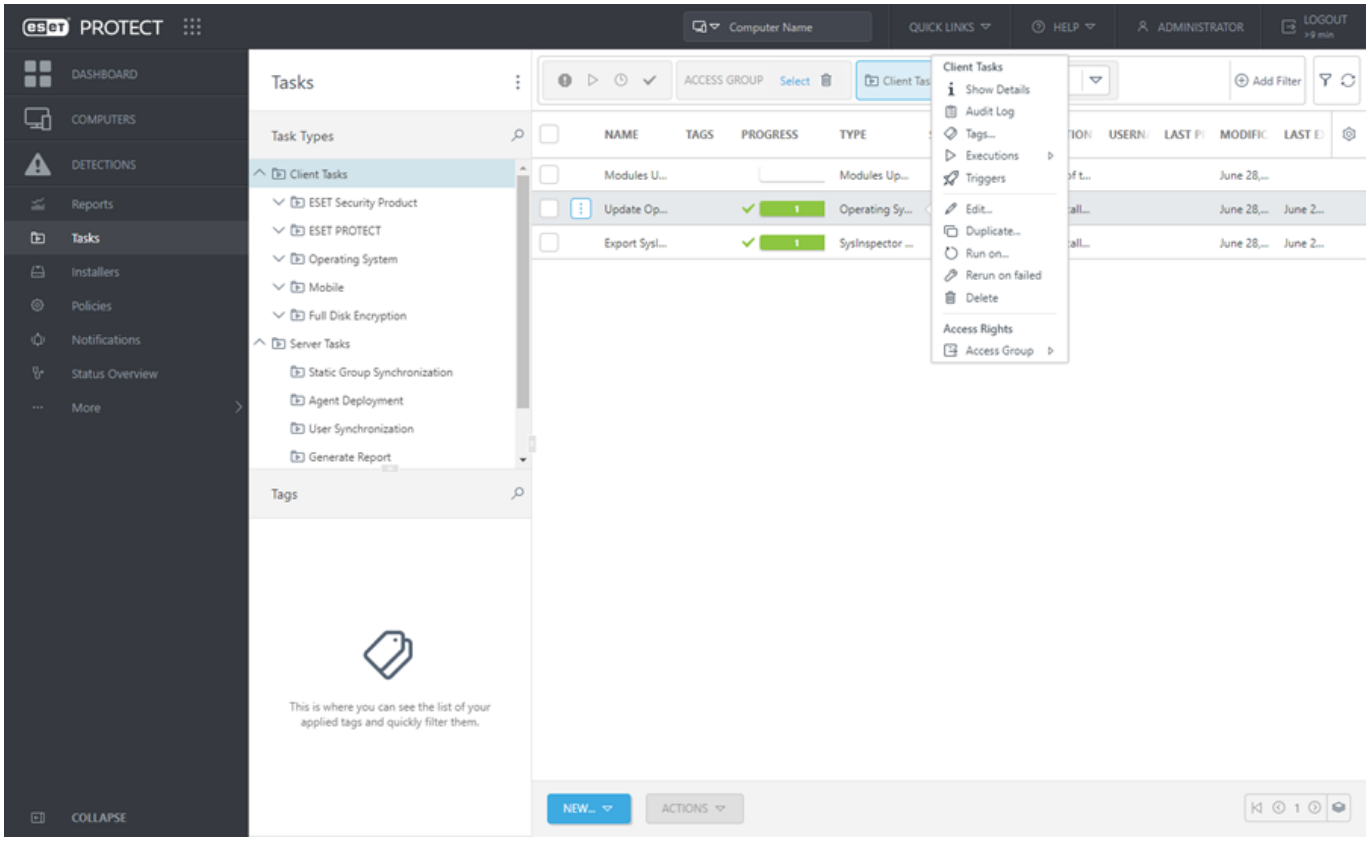
Editar	Editar o Acionador selecionado.
Nova execução ASAP	Executar novamente a tarefa do cliente (assim que possível) usando um Acionador existente logo em seguida sem nenhuma modificação.
Excluir	Remove completamente o acionador selecionado. Para remover vários acionadores, marque as caixas de seleção à esquerda e clique no botão **Remover**.
Duplicar	Criar um novo Acionador com base no acionador selecionado, um novo nome é necessário para o acionador duplicado.



Tarefas de cliente

Você pode atribuir Tarefas do cliente a grupos ou computadores individuais. Quando criada, uma tarefa é executada usando um Acionador. Uma Tarefa do cliente pode ter mais acionadores configurados. Tarefas de cliente são distribuídas a clientes quando o Agente ESET Management de um cliente conecta ao ESET PROTECT. Servidor. Por isso, pode levar algum tempo para os resultados de uma execução de tarefa serem comunicados ao ESET PROTECT. Servidor. Você pode gerenciar seu intervalo de conexão do Agente ESET Management para reduzir os tempos de execução.

Em **Tarefas** você pode ver a barra de indicadores de progresso, o ícone de status e os detalhes para cada tarefa criada.



Criar uma nova tarefa de cliente

1. Selecione uma das seguintes opções para criar uma nova tarefa de cliente:

   - Clique em **Tarefas** > **Nova** > **Tarefa do cliente**.
   - Clique em **Tarefas** > selecione o tipo de tarefa desejado e clique em **Nova** > **Tarefa do cliente**.
   - Clique no dispositivo de destino em **Computadores** e selecione **Tarefas** > **Nova tarefa**.

2. Na seção **Básico**, insira informações básicas sobre a tarefa, como **Nome e Descrição (opcional)**. Clique em **Selecionar marcações** para atribuir marcações.
No menu suspenso **Tarefa**, selecione o tipo de tarefa que deseja criar e configurar. Se você selecionou um tipo de tarefa específico antes de criar uma nova tarefa, a **Tarefa** é pré-selecionada com base na sua escolha anterior. **Tarefa** (consulte a lista de todas as Tarefas) define as configurações e o comportamento da tarefa.

3. Configure as configurações de tarefa na seção **Configurações**.

4. Verifique todas as configurações de tarefa na seção **Resumo** e clique em **Concluir**.

5. Clique em **Criar acionador** para criar um acionador para a **Tarefa do cliente** ou clique em fechar e crie o acionador mais tarde.

Acionadores de tarefa do cliente

É preciso atribuir um acionador a uma Tarefa de cliente para que ela seja executada. Para criar um Acionador, clique em **Tarefas** > clique na instância da Tarefa de cliente na tabela principal e selecione **Executar** no menu suspenso. Alternativamente, você pode atribuir a Tarefa do cliente a um Grupo ou Computador(es).

Para definir um Acionador, selecione computadores ou grupos de **Destino** nos quais uma tarefa de cliente deve ser executada. Com seu destino selecionado, defina as condições de **acionador** para executar a tarefa em um momento ou evento particular. Além disso, você pode usar Configurações avançadas - Alternância para ajustar ainda mais o acionador, se necessário.

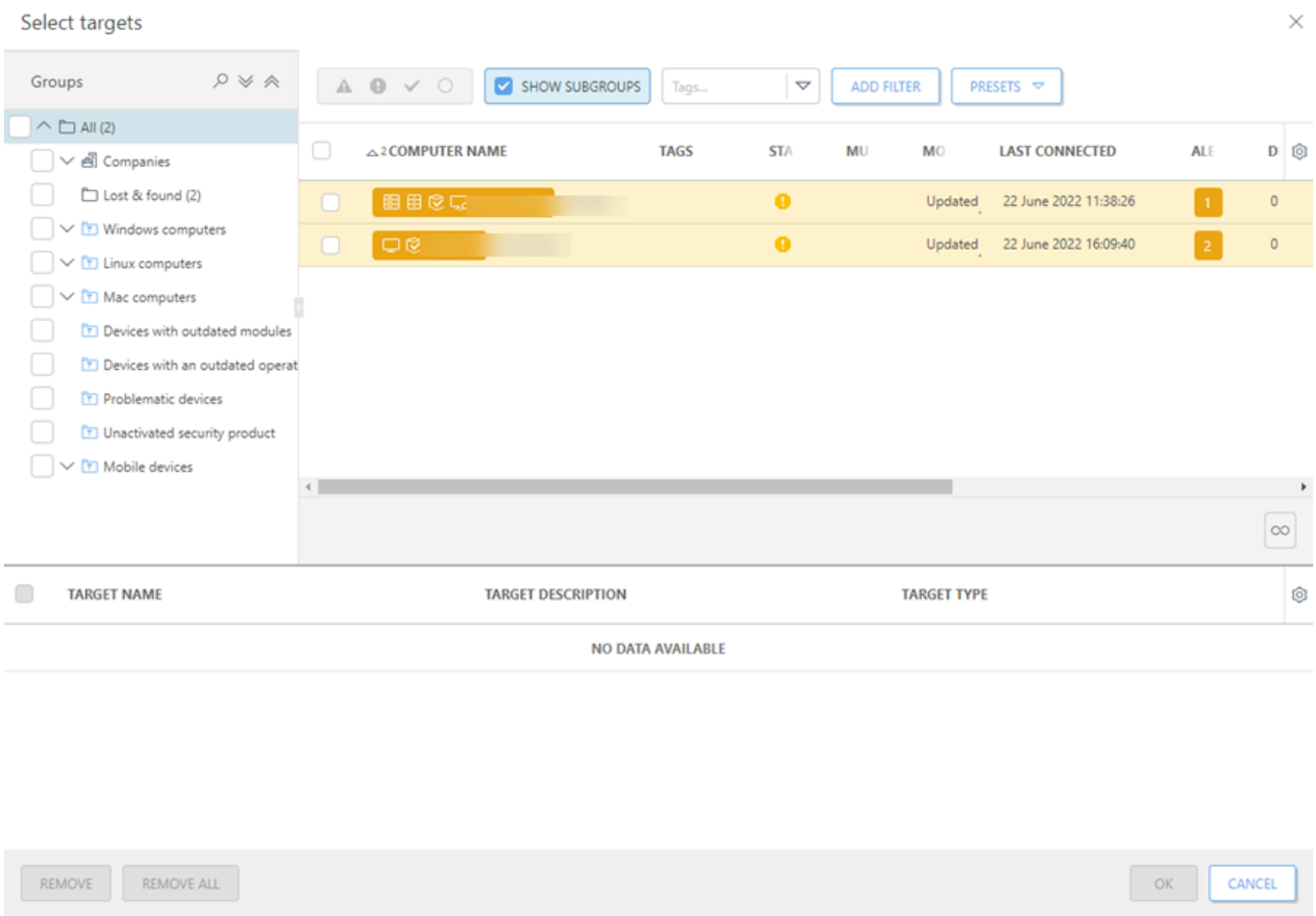
Básico

Insira informações básicas sobre o **Acionador no campo Descrição** e clique em **Destino**.

Destino

Na janela **Destino** você pode especificar os clientes (computadores individuais ou grupos) que serão os destinos dessa tarefa. Clique em **Adicionar destinos** para exibir todos os grupos estáticos e dinâmicos e seus membros e selecionar os grupos ou dispositivos.

> Para atribuir todos os computadores em um grupo, atribua o grupo em vez de computadores individuais para impedir que a velocidade do Web Console diminua.
> O Web Console exibirá um aviso se você selecionar um grande número de computadores.



Depois da seleção, clique em **OK** e prossiga para a seção **Acionador**.

Acionador

O acionador determina qual evento acionará a tarefa.

- **Assim que possível** - executa a tarefa assim que o cliente se conectar ao ESET PROTECT e receber a tarefa. Se a tarefa não puder ser entregue até a **Data de expiração**, a tarefa será removida da fila; a tarefa não será excluída, mas não será executada.
- **Agendado** - executa a tarefa em um momento selecionado.
- **Acionador de registro de evento** - executa a tarefa com base em eventos especificados aqui. Esse acionador é acionado quando um determinado evento ocorre em relatórios. Defina o **tipo de relatório**, **operador lógico** e critérios de **filtragem** que vão acionar a tarefa.
- **Acionador de grupo dinâmico ingressado** - esse acionador executa a tarefa quando um cliente ingressar no grupo dinâmico selecionado na opção Destino. Se um grupo estático ou clientes individuais forem selecionados, essa opção não estará disponível.
- Expressão CRON - Você também pode configurar seu intervalo de acionador usando uma Expressão CRON.

Para obter mais informações sobre acionadores, vá para o capítulo Tipos de acionadores de tarefas.

Configurações avançadas - Alternância

A alternância é usada para restringir uma tarefa de ser executada se uma tarefa for acionada por um evento com frequência recorrente, por exemplo, o **Acionador de registro de evento** ou o **Acionador de grupo dinâmico ingressado** (veja acima). Para obter mais informações, consulte o capítulo Configurações avançadas – Throttling.

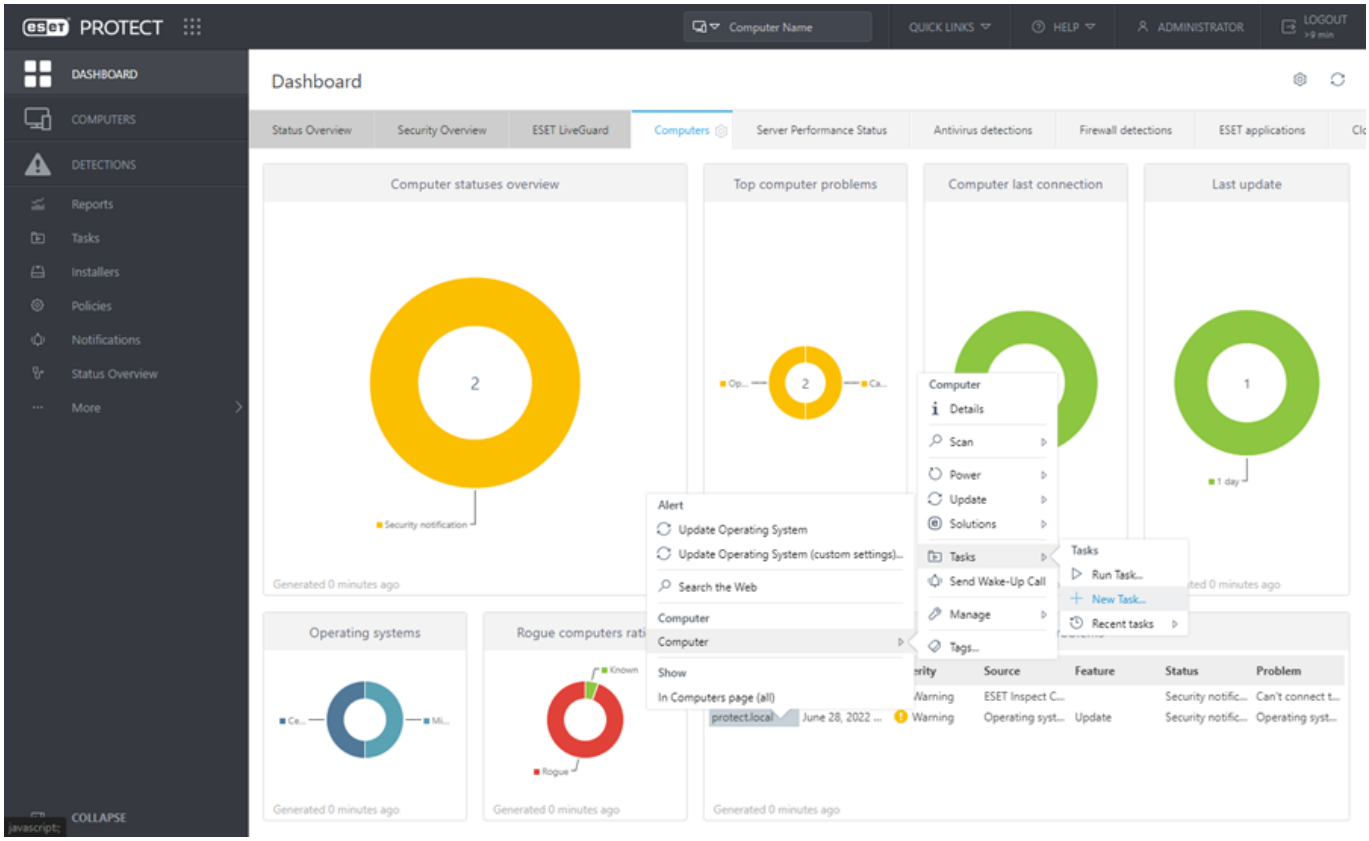
Clique em **Concluir** quando tiver definido os destinatários dessa tarefa e os acionadores que executam a tarefa.

Atribuir Tarefa do cliente a um Grupo ou Computador(es)

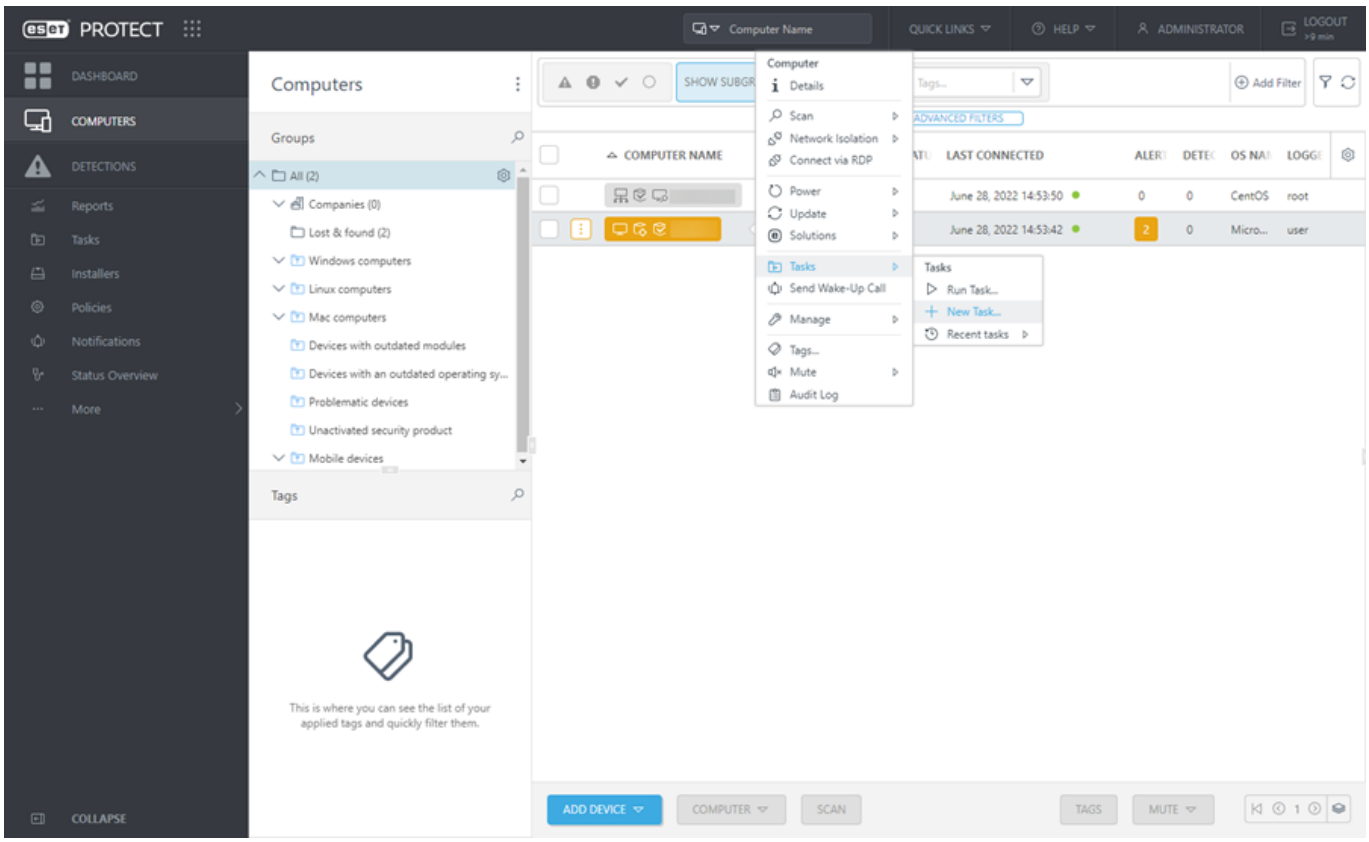
Leia aqui como Atribuir uma tarefa do cliente a um grupo.

Há duas formas de atribuir uma tarefa a um computador.

1. **Painel** > **Computadores** > **Computadores com problemas** > selecione um computador e clique em **Computador** > **Tarefas** > **Nova tarefa**



2.Computador > selecione o(s) computador(es) usando as caixas de seleção > **Tarefas** > **Nova tarefa**.



Uma janela de Assistente de nova tarefa de cliente será aberta.

Ações Antifurto

A funcionalidade **Antifurto** protege um dispositivo móvel contra o acesso não autorizado.

Se um dispositivo móvel (inscrito e gerenciado por ESET PROTECT) for perdido ou roubado, algumas ações são acionadas automaticamente e outras ações que podem ser realizadas usando uma tarefa de cliente.

Se uma pessoa não autorizada substituir um cartão SIM confiável por um SIM não confiável, o dispositivo será **bloqueado** automaticamente pelo ESET Endpoint Security for Android e um SMS de alerta será enviado para o(s) número(s) de telefone definido(s) pelo usuário. Essa mensagem vai incluir as informações a seguir:

- o número de dispositivo móvel do cartão SIM sendo usado no momento
- o número **IMSI** (Identidade internacional de assinante móvel)
- o número **IMEI** (Identidade internacional de equipamento móvel) do dispositivo móvel

O usuário não autorizado não terá conhecimento do envio desta mensagem porque ela será automaticamente excluída das sequências de mensagens do aparelho. Você também pode solicitar coordenadas de **GPS** do aparelho perdido ou apagar remotamente todos os dados armazenados no dispositivo usando uma tarefa de cliente.

Selecione uma das seguintes opções para criar uma nova tarefa de cliente:

- Clique em **Tarefas** > **Nova** > **Tarefa do cliente**.
- Clique em **Tarefas** > selecione o tipo de tarefa desejado e clique em **Nova** > **Tarefa do cliente**.
- Clique no dispositivo de destino em **Computadores** e selecione **Tarefas** > **Nova tarefa**.

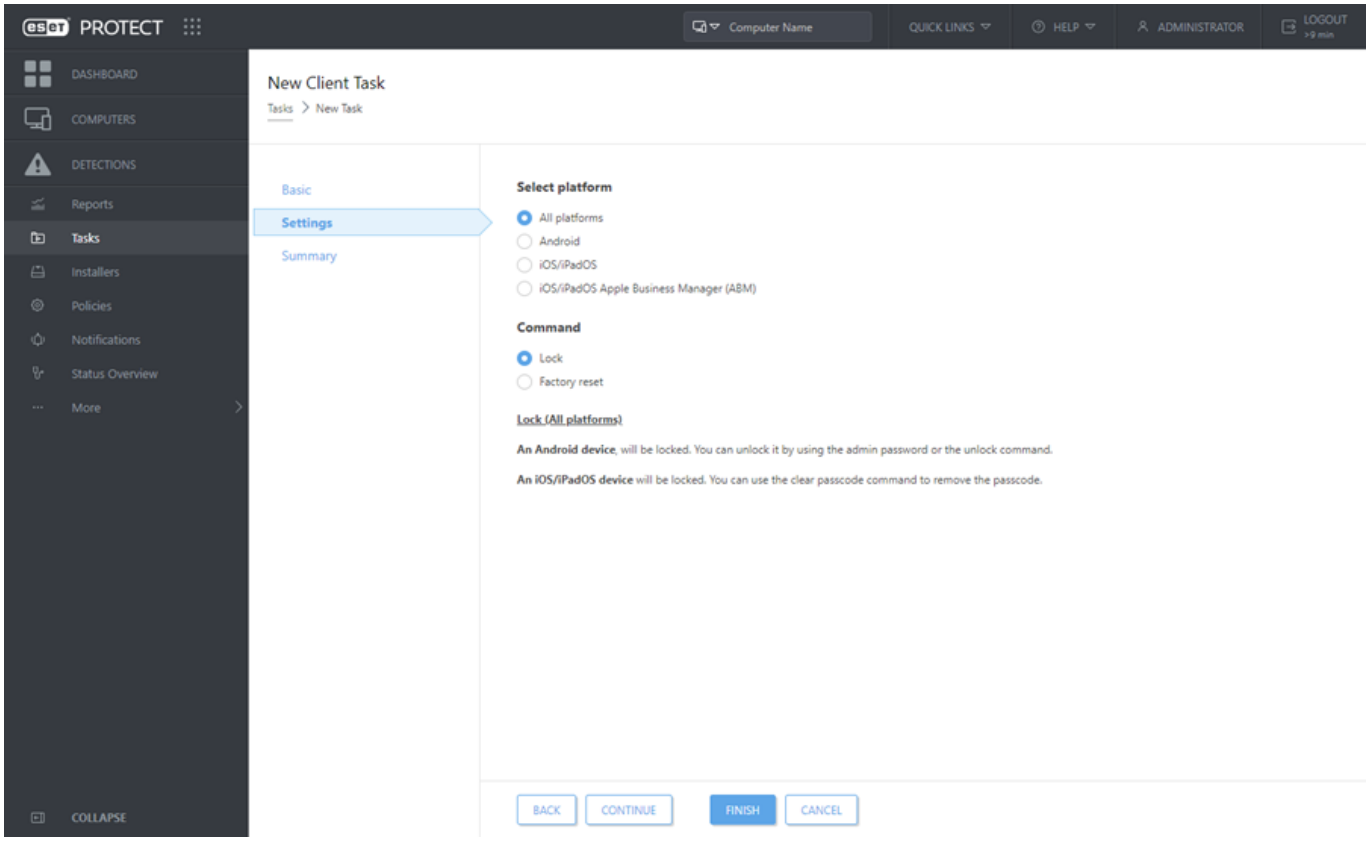
Básico

Na seção **Básico**, insira informações básicas sobre a tarefa, como **Nome e Descrição (opcional)**. Clique em **Selecionar marcações** para atribuir marcações.
No menu suspenso **Tarefa**, selecione o tipo de tarefa que deseja criar e configurar. Se você selecionou um tipo de tarefa específico antes de criar uma nova tarefa, a **Tarefa** é pré-selecionada com base na sua escolha anterior. **Tarefa** (consulte a lista de todas as Tarefas) define as configurações e o comportamento da tarefa.

Configurações

Ação	Comportamento em sistemas operacionais móveis	Descrição
Localizar		O dispositivo responderá com uma mensagem de texto contendo suas coordenadas GPS. Se um local mais preciso estiver disponível depois de 10 minutos, o dispositivo enviará uma mensagem novamente. As informações recebidas são exibidas nos detalhes do dispositivo. **Encontrar** funciona apenas se GPS no dispositivo estiver ativado.
		Não compatível.
Bloquear		O dispositivo será bloqueado. O dispositivo pode ser desbloqueado usando a senha de administrador ou o comando de **desbloqueio**.
		O dispositivo será bloqueado. A senha pode ser removida com o comando **limpar senha**.
Desbloquear		O dispositivo será desbloqueado para ele que possa ser usado novamente. O cartão SIM atualmente no dispositivo será salvo como SIM Confiável.
		Não compatível.
Som de alarme/módulo perda		O dispositivo será bloqueado e reproduzirá um som muito alto por cinco minutos (ou até ser desbloqueado).
		Não compatível.
Limpar a senha		Não compatível.
		Remove a senha do dispositivo. Será solicitado que o usuário configure uma nova senha assim que o dispositivo for ligado.

Ação	Comportamento em sistemas operacionais móveis	Descrição
Redefinição de fábrica		Todos os dados acessíveis no dispositivo serão apagados (cabeçalhos de arquivos serão destruídos) e o dispositivo será redefinido para suas configurações padrão de fábrica. Isso pode demorar vários minutos.
		Todas as configurações e informações serão removidas e o dispositivo será definido para suas configurações padrão de fábrica. Isso pode demorar vários minutos.
Ativar o Módulo perda e Encontrar		Compatível apenas no iOS ABM. O dispositivo vai passar para o "modo perdido", será bloqueado e só poderá ser desbloqueado ao executar a tarefa **Desligar modo perdido** do ESET PROTECT . Você pode personalizar o número de telefone, a mensagem e a nota de rodapé que será exibida na tela de dispositivo perdido. O status de proteção do dispositivo será alterado para **Perdido**.
Desativar o modo perdido		Compatível apenas no iOS ABM. O status de proteção do dispositivo vai mudar e o dispositivo vai voltar ao seu estado de serviço regular.

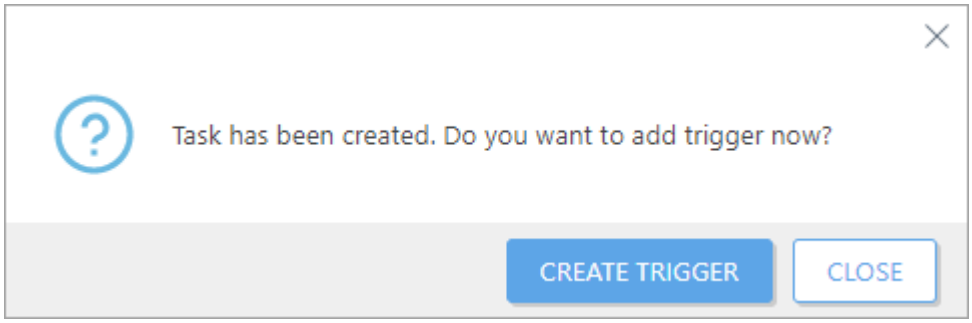


Resumo

Revise o resumo da ajustes configurados e clique em **Concluir**. A tarefa agora será criada e uma janela pequeno será aberta:

- Clique em Criar acionador (recomendado) para especificar destinos de tarefa do cliente (computadores ou grupos) e o Acionador.

- Se clicar em **Fechar**, você pode criar um Acionador mais tarde: clique na instância da Tarefa do cliente e selecione **Executar em** no menu suspenso.



Em **Tarefas** você pode ver a barra de indicadores de progresso, o ícone de status e os detalhes para cada tarefa

criada.

Diagnóstico

Use a tarefa **Diagnóstico** para solicitar uma ação de diagnóstico do produto de segurança ESET no computador cliente.

Selecione uma das seguintes opções para criar uma nova tarefa de cliente:

- Clique em **Tarefas** > **Nova** > **Tarefa do cliente**.
- Clique em **Tarefas** > selecione o tipo de tarefa desejado e clique em **Nova** > **Tarefa do cliente**.
- Clique no dispositivo de destino em **Computadores** e selecione **Tarefas** > **Nova tarefa**.

Básico

Na seção **Básico**, insira informações básicas sobre a tarefa, como **Nome e Descrição (opcional)**. Clique em **Selecionar marcações** para atribuir marcações.
No menu suspenso **Tarefa**, selecione o tipo de tarefa que deseja criar e configurar. Se você selecionou um tipo de tarefa específico antes de criar uma nova tarefa, a **Tarefa** é pré-selecionada com base na sua escolha anterior. **Tarefa** (consulte a lista de todas as Tarefas) define as configurações e o comportamento da tarefa.

Configurações

Ação de diagnóstico

- **Executar o Log Collector** - Coleta dados específicos (como configuração e relatórios) de uma máquina selecionada para facilitar a coleta de informações da máquina do cliente durante a resolução de um caso de suporte.
  - **Parâmetros do Log Collector** – você pode especificar os parâmetros do Log Collector no Windows, macOS ou Linux. Para coletar todos os dados disponíveis, deixe o campo **Parâmetros do Log Collector** em branco. Se você especificar parâmetros do Log Collector, selecione apenas computadores executando o sistema operacional aplicável como Destinos para a tarefa.

O limite de tamanho de arquivo para a entrega de relatório por dispositivo é de 200MB. Você pode acessar relatórios do Web Console na seção **Detalhes** > **Relatórios**. Se os relatórios coletados pela tarefa forem maiores do que 200 MB, a tarefa vai falhar. Se a tarefa falhar, você pode:
- Coletar os relatórios localmente no dispositivo.
- Alterar o detalhamento dos relatórios e tentar novamente a tarefa:
  - Para destinos o Windows, use o parâmetro `/Targets:EraAgLogs` para coletar apenas relatórios do Agente ESET Management.
  - Para destinos Linux/macOS, use o parâmetro `--no-productlogs` para excluir relatórios do produto de segurança ESET instalado.

- **Definir o modo de Diagnóstico** - O modo de diagnóstico é composto das seguintes categorias: **Relatório de spam**, **Relatório de firewall**, **Relatório de HIPS**, **Relatório de controle de dispositivo** e **Relatório de controle da web**. O objetivo principal do modo de Diagnóstico é coletar relatórios com todos os níveis de gravidade quando a solução de problemas for necessária.

- **Ativar** - Ativar o registro em relatório para todos os aplicativos ESET.
- **Desligar** - Você pode desligar o registro em relatório manualmente, ou o registro em relatório será desligado automaticamente depois do computador ser reiniciado.

Os pré-requisitos a seguir são necessários para a criação bem-sucedida de relatórios de diagnóstico:

- Relatórios de modo de diagnóstico podem ser coletados de computadores cliente executando os sistemas operacionais Windows e macOS.
- O computador cliente deve ter um produto de segurança ESET instalado e ativado.

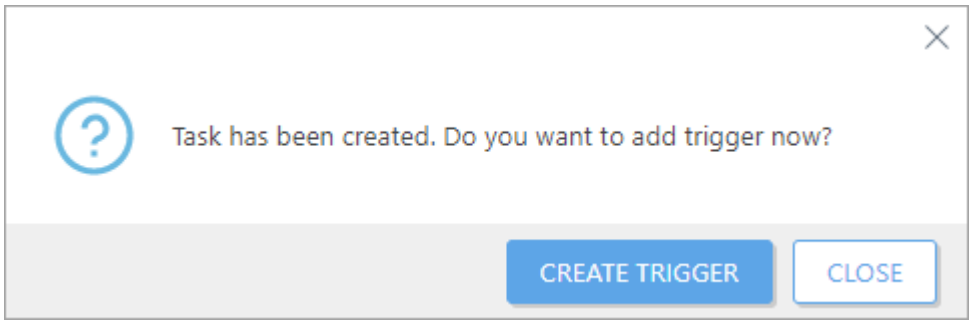
> O Agente ESET Management envia apenas relatórios coletados por um produto ESET instalado em um computador cliente. A categoria e detalhamento de relatório dependem do tipo e configuração do produto. Configure cada produto (através de Políticas) para coletar relatórios específicos.

Relatórios de diagnóstico com mais de 24 horas são removidos todos os dias durante a limpeza da meia noite. Isso protege o banco de dados ESET PROTECT de uma sobrecarga.

Resumo

Revise o resumo da ajustes configurados e clique em **Concluir**. A tarefa agora será criada e uma janela pequeno será aberta:

- Clique em Criar acionador (recomendado) para especificar destinos de tarefa do cliente (computadores ou grupos) e o Acionador.
- Se clicar em **Fechar**, você pode criar um Acionador mais tarde: clique na instância da Tarefa do cliente e selecione **Executar em** no menu suspenso.



Em **Tarefas** você pode ver a barra de indicadores de progresso, o ícone de status e os detalhes para cada tarefa criada.

Você pode ver os relatórios criados em Detalhes do computador: **Relatórios** > **Relatório de diagnóstico**.

Exibição de mensagem

A tarefa **Exibir mensagem** permite que você envie uma mensagem para qualquer dispositivo gerenciado (computador do cliente, tablet, celular, etc.). A mensagem será exibida na tela para informar o usuário.

- Windows - A mensagem é exibida como uma notificação.

No Windows, a Tarefa de cliente Exibir mensagem usa o comando msg.exe que está presente apenas em edições do Windows Professional/Enterprise. Como resultado, você não pode usar essa tarefa para exibir uma mensagem em um computador cliente executando o Windows Home edition.

- macOS e Linux - A mensagem é exibida apenas em um terminal.

Para ver a mensagem no macOS ou Linux, primeiro é preciso abrir o terminal.

Selecione uma das seguintes opções para criar uma nova tarefa de cliente:

- Clique em **Tarefas** > **Nova** > **Tarefa do cliente**.
- Clique em **Tarefas** > selecione o tipo de tarefa desejado e clique em **Nova** > **Tarefa do cliente**.
- Clique no dispositivo de destino em **Computadores** e selecione **Tarefas** > **Nova tarefa**.

Básico

Na seção **Básico**, insira informações básicas sobre a tarefa, como **Nome e Descrição (opcional)**. Clique em **Selecionar marcações** para atribuir marcações.
No menu suspenso **Tarefa**, selecione o tipo de tarefa que deseja criar e configurar. Se você selecionou um tipo de tarefa específico antes de criar uma nova tarefa, a **Tarefa** é pré-selecionada com base na sua escolha anterior. **Tarefa** (consulte a lista de todas as Tarefas) define as configurações e o comportamento da tarefa.

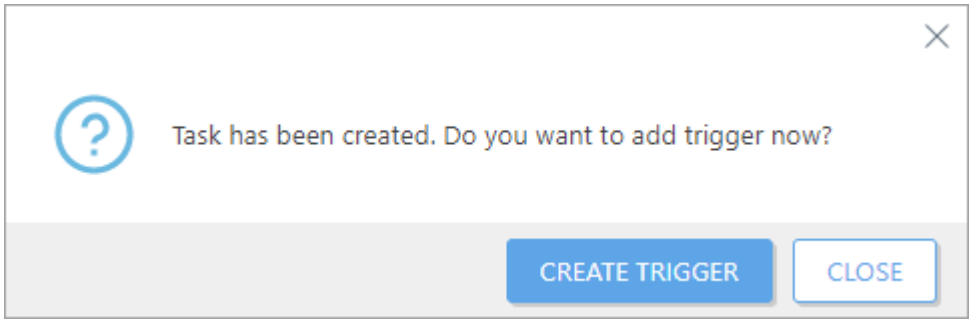
Configurações

Você pode inserir um **Título** e digitar sua **Mensagem**.

Resumo

Revise o resumo da ajustes configurados e clique em **Concluir**. A tarefa agora será criada e uma janela pequeno será aberta:

- Clique em Criar acionador (recomendado) para especificar destinos de tarefa do cliente (computadores ou grupos) e o Acionador.
- Se clicar em **Fechar**, você pode criar um Acionador mais tarde: clique na instância da Tarefa do cliente e selecione **Executar em** no menu suspenso.



Em **Tarefas** você pode ver a barra de indicadores de progresso, o ícone de status e os detalhes para cada tarefa criada.

Parar com o isolamento do computador

A tarefa **Parar com o isolamento do computador da rede** encerra o isolamento do computador da rede e permite novamente conexões do computador isolado. Use esta Tarefa apenas quando o problema de segurança tiver sido resolvido.

Selecione uma das seguintes opções para criar uma nova tarefa de cliente:

- Clique em **Tarefas** > **Nova** > **Tarefa do cliente**.
- Clique em **Tarefas** > selecione o tipo de tarefa desejado e clique em **Nova** > **Tarefa do cliente**.
- Clique no dispositivo de destino em **Computadores** e selecione **Tarefas** > **Nova tarefa**.

Básico

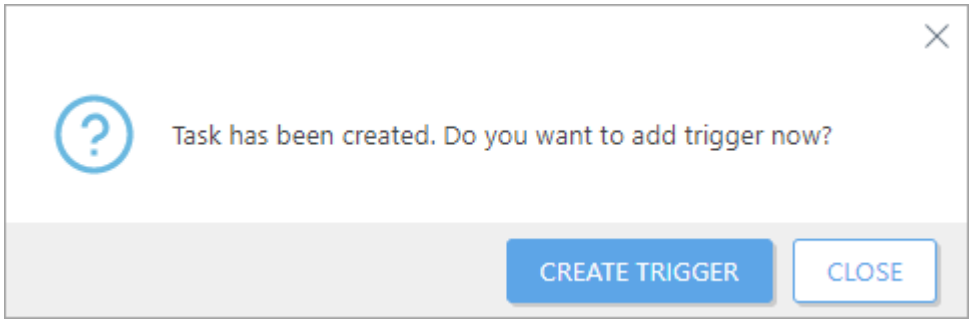
Na seção **Básico**, insira informações básicas sobre a tarefa, como **Nome e Descrição (opcional)**. Clique em **Selecionar marcações** para atribuir marcações.
No menu suspenso **Tarefa**, selecione o tipo de tarefa que deseja criar e configurar. Se você selecionou um tipo de tarefa específico antes de criar uma nova tarefa, a **Tarefa** é pré-selecionada com base na sua escolha anterior. **Tarefa** (consulte a lista de todas as Tarefas) define as configurações e o comportamento da tarefa.

> As **configurações** não estão disponíveis para essa tarefa.

Resumo

Revise o resumo da ajustes configurados e clique em **Concluir**. A tarefa agora será criada e uma janela pequeno será aberta:

- Clique em Criar acionador (recomendado) para especificar destinos de tarefa do cliente (computadores ou grupos) e o Acionador.
- Se clicar em **Fechar**, você pode criar um Acionador mais tarde: clique na instância da Tarefa do cliente e selecione **Executar em** no menu suspenso.



Em **Tarefas** você pode ver a barra de indicadores de progresso, o ícone de status e os detalhes para cada tarefa criada.

Exportar configuração de produtos gerenciados

A tarefa **Exportar configuração de produtos gerenciados** é usada para exportar as configurações de componentes ESET PROTECT individuais ou produtos de segurança ESET instalados nos clientes.

Selecione uma das seguintes opções para criar uma nova tarefa de cliente:

- Clique em **Tarefas** > **Nova** > **Tarefa do cliente**.
- Clique em **Tarefas** > selecione o tipo de tarefa desejado e clique em **Nova** > **Tarefa do cliente**.
- Clique no dispositivo de destino em **Computadores** e selecione **Tarefas** > **Nova tarefa**.

Básico

Na seção **Básico**, insira informações básicas sobre a tarefa, como **Nome e Descrição (opcional)**. Clique em **Selecionar marcações** para atribuir marcações.
No menu suspenso **Tarefa**, selecione o tipo de tarefa que deseja criar e configurar. Se você selecionou um tipo de tarefa específico antes de criar uma nova tarefa, a **Tarefa** é pré-selecionada com base na sua escolha anterior. **Tarefa** (consulte a lista de todas as Tarefas) define as configurações e o comportamento da tarefa.

Configurações

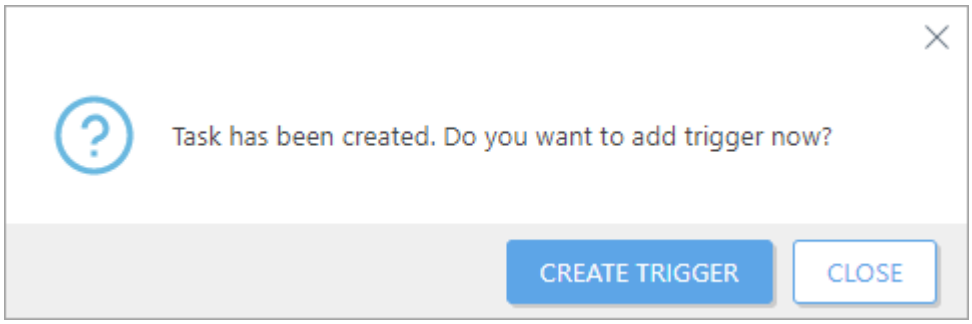
Exportar definições de configuração de produtos gerenciados.

- **Produto** - selecione um componente ESET PROTECT ou produto de ESET segurança cliente par ao qual deseja exportar a configuração.

Resumo

Revise o resumo da ajustes configurados e clique em **Concluir**. A tarefa agora será criada e uma janela pequeno será aberta:

- Clique em Criar acionador (recomendado) para especificar destinos de tarefa do cliente (computadores ou grupos) e o Acionador.
- Se clicar em **Fechar**, você pode criar um Acionador mais tarde: clique na instância da Tarefa do cliente e selecione **Executar em** no menu suspenso.



Em **Tarefas** você pode ver a barra de indicadores de progresso, o ícone de status e os detalhes para cada tarefa criada.

Quando a tarefa for concluída, você poderá encontrar a configuração exportada na guia **Configuração** em detalhes do computador dos computadores de destino.

Isolar computador da rede

A tarefa **Isolar computador da rede** isola os computadores selecionados da rede e todas as conexões, exceto aquelas necessárias para a operação correta dos produtos ESET, serão bloqueadas. As conexões permitidas incluem o seguinte:

- computador obtém um endereço IP
- comunicação do *ekrn.exe*, Agente ESET Management, Conector ESET Inspect
- entrar em um domínio

> O isolamento de rede é compatível apenas com os produtos de segurança ESET (Endpoint Antivirus/Security e produtos de segurança do servidor) da versão 7.2 e posterior.
> O isolamento da rede provavelmente interromperá a operação normal dos computadores e você deve usá-lo apenas em casos de emergência (por exemplo, se um problema grave de segurança for identificado em um computador gerenciado). Você pode terminar o isolamento com uma tarefa do cliente.

Selecione uma das seguintes opções para criar uma nova tarefa de cliente:

- Clique em **Tarefas** > **Nova** > **Tarefa do cliente**.
- Clique em **Tarefas** > selecione o tipo de tarefa desejado e clique em **Nova** > **Tarefa do cliente**.
- Clique no dispositivo de destino em **Computadores** e selecione **Tarefas** > **Nova tarefa**.

Básico

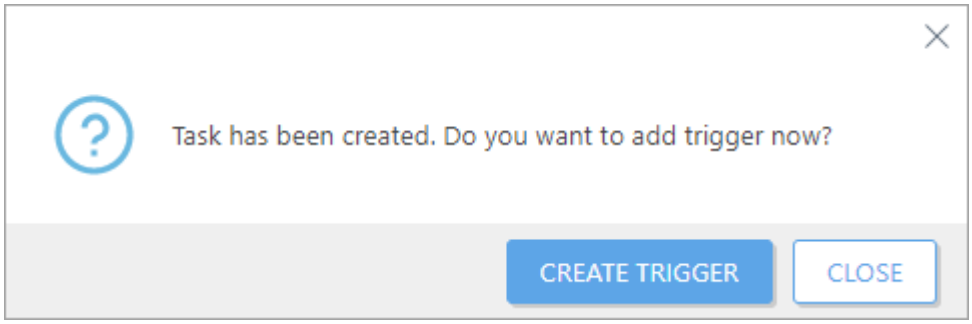
Na seção **Básico**, insira informações básicas sobre a tarefa, como **Nome e Descrição (opcional)**. Clique em **Selecionar marcações** para atribuir marcações.
No menu suspenso **Tarefa**, selecione o tipo de tarefa que deseja criar e configurar. Se você selecionou um tipo de tarefa específico antes de criar uma nova tarefa, a **Tarefa** é pré-selecionada com base na sua escolha anterior. **Tarefa** (consulte a lista de todas as Tarefas) define as configurações e o comportamento da tarefa.

> As **configurações** não estão disponíveis para essa tarefa.

Resumo

Revise o resumo da ajustes configurados e clique em **Concluir**. A tarefa agora será criada e uma janela pequeno será aberta:

- Clique em Criar acionador (recomendado) para especificar destinos de tarefa do cliente (computadores ou grupos) e o Acionador.
- Se clicar em **Fechar**, você pode criar um Acionador mais tarde: clique na instância da Tarefa do cliente e selecione **Executar em** no menu suspenso.



Em **Tarefas** você pode ver a barra de indicadores de progresso, o ícone de status e os detalhes para cada tarefa criada.

Sair

A tarefa **Sair** remove todos os usuários do computador de destino. Alternativamente, clique em um computador e selecione **Energia** > **Sair**.

O computador deve executar o Agente ESET Management ou 10.0 posteriormente. A tarefa do cliente **Sair** vai falhar em um computador que esteja executando uma versão anterior do Agente.

Selecione uma das seguintes opções para criar uma nova tarefa de cliente:

- Clique em **Tarefas** > **Nova** > **Tarefa do cliente**.
- Clique em **Tarefas** > selecione o tipo de tarefa desejado e clique em **Nova** > **Tarefa do cliente**.
- Clique no dispositivo de destino em **Computadores** e selecione **Tarefas** > **Nova tarefa**.

Básico

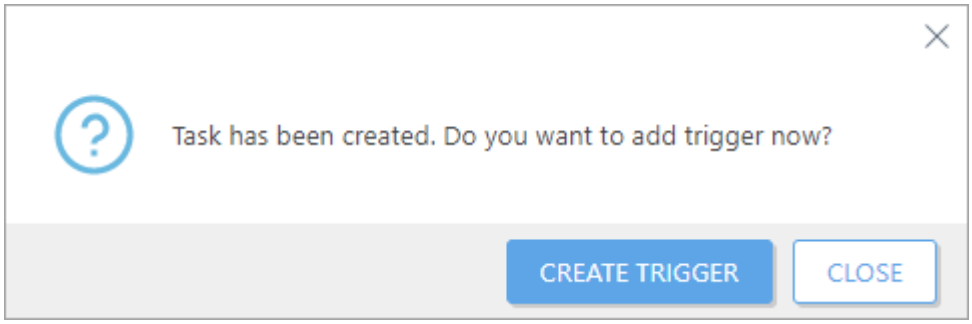
Na seção **Básico**, insira informações básicas sobre a tarefa, como **Nome e Descrição (opcional)**. Clique em **Selecionar marcações** para atribuir marcações.
No menu suspenso **Tarefa**, selecione o tipo de tarefa que deseja criar e configurar. Se você selecionou um tipo de tarefa específico antes de criar uma nova tarefa, a **Tarefa** é pré-selecionada com base na sua escolha anterior. **Tarefa** (consulte a lista de todas as Tarefas) define as configurações e o comportamento da tarefa.

As **configurações** não estão disponíveis para essa tarefa.

Resumo

Revise o resumo da ajustes configurados e clique em **Concluir**. A tarefa agora será criada e uma janela pequeno será aberta:

- Clique em Criar acionador (recomendado) para especificar destinos de tarefa do cliente (computadores ou grupos) e o Acionador.
- Se clicar em **Fechar**, você pode criar um Acionador mais tarde: clique na instância da Tarefa do cliente e selecione **Executar em** no menu suspenso.



Em **Tarefas** você pode ver a barra de indicadores de progresso, o ícone de status e os detalhes para cada tarefa criada.

Atualização de módulos

A tarefa **Atualização de módulos** força a atualização de todos os módulos do produto de segurança instalados em um dispositivo de destino. Essa é uma tarefa geral para todos os produtos de segurança em todos os sistemas. Você pode encontrar uma lista de todos os módulos do produto de segurança de destino na seção **Sobre** do produto de segurança.

Selecione uma das seguintes opções para criar uma nova tarefa de cliente:

- Clique em **Tarefas** > **Nova** > **Tarefa do cliente**.
- Clique em **Tarefas** > selecione o tipo de tarefa desejado e clique em **Nova** > **Tarefa do cliente**.
- Clique no dispositivo de destino em **Computadores** e selecione **Tarefas** > **Nova tarefa**.

Básico

Na seção **Básico**, insira informações básicas sobre a tarefa, como **Nome e Descrição (opcional)**. Clique em **Selecionar marcações** para atribuir marcações.
No menu suspenso **Tarefa**, selecione o tipo de tarefa que deseja criar e configurar. Se você selecionou um tipo de tarefa específico antes de criar uma nova tarefa, a **Tarefa** é pré-selecionada com base na sua escolha anterior. **Tarefa** (consulte a lista de todas as Tarefas) define as configurações e o comportamento da tarefa.

Configurações

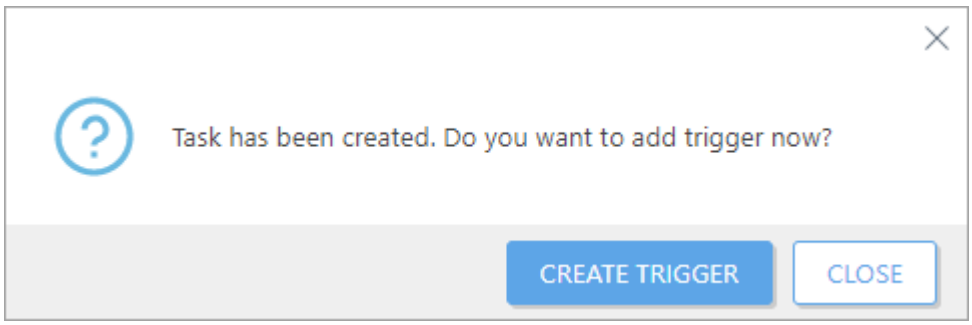
- **Limpar cache de atualização** - Essa opção exclui os arquivos de atualização temporários no cache no cliente e, com frequência, pode ser usada para reparar erros de atualização do módulo.

Resumo

Revise o resumo da ajustes configurados e clique em **Concluir**. A tarefa agora será criada e uma janela pequeno será aberta:

- Clique em Criar acionador (recomendado) para especificar destinos de tarefa do cliente (computadores ou grupos) e o Acionador.
- Se clicar em **Fechar**, você pode criar um Acionador mais tarde: clique na instância da Tarefa do cliente e

selecione **Executar em** no menu suspenso.



Em **Tarefas** você pode ver a barra de indicadores de progresso, o ícone de status e os detalhes para cada tarefa criada.

> **Definir um servidor personalizado para atualizações de módulos**
> Se a atualização de módulos no produto de segurança ESET falhar devido a um bloqueio geográfico, use uma política para definir um servidor personalizado para atualizações de módulos:
> 1. Nas configurações de política do produto de segurança ESET, selecione **Atualizações** > **Perfis** > **Atualizações**.
> 2. Em **Atualizações de módulos**, desligue **Escolher automaticamente** e digite o endereço do **Servidor personalizado**. Por exemplo, para usar os servidores de atualização dos EUA para ESET Endpoint Antivirus/Security 9 para Windows, digite *http://us-update.eset.com/eset_upd/ep9/* (versão 8: *http://us-update.eset.com/eset_upd/ep8/*).
> 3. Digite seu **Nome de usuário** (EAV-XXXXXXXX) e a **Senha** da licença. Essas informações podem ser obtidas dos detalhes da licença de legado.

Reversão de atualização dos módulos

Em casos quando uma atualização de módulo causar problemas, ou se você não quiser aplicar a atualização a todos os clientes (por exemplo para testes ou ao usar atualizações pré-lançamento), você pode usar a tarefa **Reversão de atualização dos módulos**. Quando você aplicar essa tarefa, os módulos serão redefinidos para a versão anterior.

Selecione uma das seguintes opções para criar uma nova tarefa de cliente:

- Clique em **Tarefas** > **Nova** > **Tarefa do cliente**.
- Clique em **Tarefas** > selecione o tipo de tarefa desejado e clique em **Nova** > **Tarefa do cliente**.
- Clique no dispositivo de destino em **Computadores** e selecione **Tarefas** > **Nova tarefa**.

Básico

Na seção **Básico**, insira informações básicas sobre a tarefa, como **Nome e Descrição (opcional)**. Clique em **Selecionar marcações** para atribuir marcações.
No menu suspenso **Tarefa**, selecione o tipo de tarefa que deseja criar e configurar. Se você selecionou um tipo de tarefa específico antes de criar uma nova tarefa, a **Tarefa** é pré-selecionada com base na sua escolha anterior. **Tarefa** (consulte a lista de todas as Tarefas) define as configurações e o comportamento da tarefa.

Configurações

Abra esta seção para personalizar as configurações de reversão de atualização do módulo.

Ação

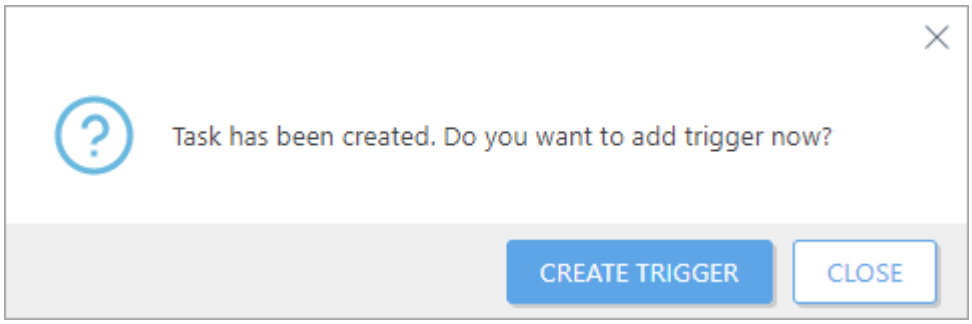
- **Ativar atualizações** - As atualizações estão ativadas e o cliente receberá a próxima atualização do módulo.
- **Reverter e desativar atualizações da próxima vez** - As atualizações são desativadas pelo período de tempo especificado no menu suspenso **Desativar intervalo** (12, 24, 36, 48 horas ou até revogação).

Tenha cuidado ao usar a opção **Até a revogação**, pois isso apresenta um risco de segurança.

Resumo

Revise o resumo da ajustes configurados e clique em **Concluir**. A tarefa agora será criada e uma janela pequeno será aberta:

- Clique em Criar acionador (recomendado) para especificar destinos de tarefa do cliente (computadores ou grupos) e o Acionador.
- Se clicar em **Fechar**, você pode criar um Acionador mais tarde: clique na instância da Tarefa do cliente e selecione **Executar em** no menu suspenso.



Em **Tarefas** você pode ver a barra de indicadores de progresso, o ícone de status e os detalhes para cada tarefa criada.

Rastreamento sob demanda

A tarefa **Rastreamento sob demanda** permite que você execute manualmente um rastreamento do computador cliente (separado de um rastreamento agendado regular).

Selecione uma das seguintes opções para criar uma nova tarefa de cliente:

- Clique em **Tarefas** > **Nova** > **Tarefa do cliente**.
- Clique em **Tarefas** > selecione o tipo de tarefa desejado e clique em **Nova** > **Tarefa do cliente**.
- Clique no dispositivo de destino em **Computadores** e selecione **Tarefas** > **Nova tarefa**.

Básico

Na seção **Básico**, insira informações básicas sobre a tarefa, como **Nome e Descrição (opcional)**. Clique em **Selecionar marcações** para atribuir marcações.
No menu suspenso **Tarefa**, selecione o tipo de tarefa que deseja criar e configurar. Se você selecionou um tipo de tarefa específico antes de criar uma nova tarefa, a **Tarefa** é pré-selecionada com base na sua escolha anterior. **Tarefa** (consulte a lista de todas as Tarefas) define as configurações e o comportamento da tarefa.

Configurações

Desligar computador após o escaneamento - se esta caixa de seleção for marcada, o computador vai desligar depois de concluir o escaneamento.

Você pode configurar o comportamento de reinicialização/desligamento dos computadores gerenciados. O computador deve executar um Agente ESET Management 9.1 e um produto de segurança ESET compatível com esta configuração.

Perfil de rastreamento

É possível selecionar o perfil que quiser a partir do menu suspenso:

- **Rastreamento detalhado** - este é um perfil predefinido no cliente, é configurado para ser o perfil de rastreamento mais completo e verifica o sistema inteiro, mas também exige mais tempo e recursos.

- **Escaneamento inteligente** - Om escaneamento inteligente permite que você inicie rapidamente om escaneamento do computador e limpe arquivos infectados, sem a necessidade de intervenção do usuário. A vantagem do Escaneamento inteligente é que ele é fácil de operar e não requer configuração de escaneamento detalhada. O Rastreamento inteligente verifica todos os arquivos nas unidades locais e limpa ou exclui automaticamente as infiltrações detectadas. O nível de limpeza é automaticamente ajustado ao valor padrão.

- **Rastrear do menu de contexto** - Rastreia um cliente usando um perfil de rastreamento pré-definido; você pode personalizar os destinos de rastreamento.

- **Perfil personalizado** - o rastreamento personalizado permite especificar parâmetros de rastreamento, como rastreamento de alvos e métodos de rastreamento. A vantagem do Rastreamento personalizado é a capacidade de configurar os parâmetros detalhadamente. As configurações podem ser salvas nos perfis de rastreamento definidos pelo usuário, o que facilita repetir o rastreamento com os mesmos parâmetros. Um perfil deve ser criado antes da execução da tarefa com a opção de perfil personalizado. Quando você seleciona um perfil personalizado do menu suspenso, digite o nome exato do perfil no campo **Personalizar perfil**.

Limpeza

Por padrão, a opção **Rastrear com limpeza** está selecionada. Essa configuração permite a limpeza automática de objetos encontrados infectados. Se isso não for possível, eles serão colocados em quarentena.

Destinos para rastreamento

A opção **Escanear todos os destinos** também está selecionada por padrão. Usando essa configuração, todos os alvos especificados no perfil de rastreamento serão rastreados. Se você desmarcar essa opção, precisará especificar manualmente alvos de rastreamento no campo **Adicionar alvo** a seguir. Digite o destino de rastreamento aqui e clique em **Adicionar**. O alvo será exibido no campo **Destinos de rastreamento** a seguir. Um destino de rastreamento pode ser um arquivo, localização ou você pode executar um rastreamento pré-definido usando qualquer uma das strings a seguir como um **Destino de rastreamento**:

Destino para rastreamento	Locais escaneados
`${DriveRemovable}`	Todas as unidades removíveis e dispositivos.
`${DriveRemovableBoot}`	Setores de inicialização de todas as unidades removíveis.
`${DriveFixed}`	Disco rígido (HDD, SSD).
`${DriveFixedBoot}`	Setores de inicialização de discos rígidos.
`${DriveRemote}`	Unidades de rede.
`${DriveAll}`	Todas as unidades disponíveis.
`${DriveAllBoot}`	Setores de inicialização e UEFI de todas as unidades. Leia mais sobre o Escaneador UEFI no glossário.
`${DriveSystem}`	Unidade do sistema.
`${Share}`	Unidades compartilhadas (apenas para produtos do servidor).
`${Boot}`	Setor de inicialização principal.
`${Memory}`	Memória operacional.
`${Registry}`	Registro do sistema (apenas para ESET Endpoint 8 e versões posteriores).
`${Wmi}`	Banco de dados WMI (apenas para o ESET Endpoint 8 e versões posteriores).

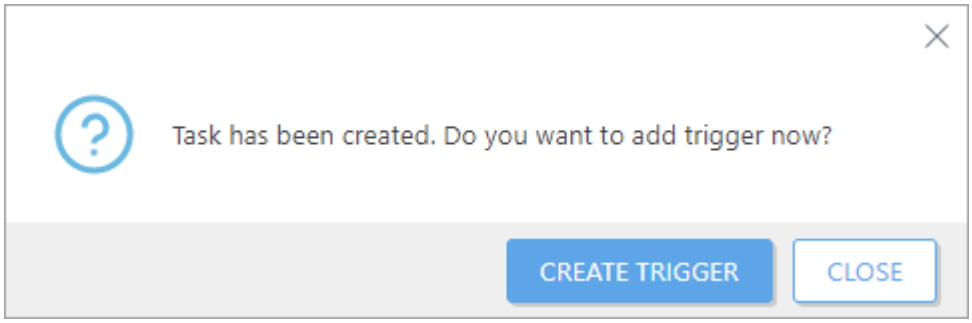
Abaixo mostramos alguns exemplos de como usar os parâmetros de destino de **Rastreamento sob demanda**:
■Arquivo: *C:\Users\Data.dat*
■Pasta *C:\MyFolder*
■Caminho Unix ou arquivo */usr/data*
■Local Windows UNC *\\server1\scan_folder*
■String predefinida `${Memory}`

Resumo

Revise o resumo da ajustes configurados e clique em **Concluir**. A tarefa agora será criada e uma janela pequeno será aberta:

- Clique em Criar acionador (recomendado) para especificar destinos de tarefa do cliente (computadores ou grupos) e o Acionador.

- Se clicar em **Fechar**, você pode criar um Acionador mais tarde: clique na instância da Tarefa do cliente e selecione **Executar em** no menu suspenso.



Em **Tarefas** você pode ver a barra de indicadores de progresso, o ícone de status e os detalhes para cada tarefa criada.

Atualização de sistema operacional

A tarefa Atualização de sistema operacional é usada para atualizar o sistema operacional do computador cliente. Essa tarefa pode acionar a atualização do sistema operacional em sistemas operacionais Windows, macOS e Linux.

- **macOS** – a tarefa instala todas as atualizações (a atualização de todos os pacotes) usando o comando:

```
/usr/sbin/softwareupdate --install --all
```

- **Linux** – a tarefa instala todas as atualizações (a atualização de todos os pacotes). Ele está verificando vários gerenciadores de pacote, portanto cobre a maioria das distribuições. Ela executa os comandos a seguir:

  Debian/Ubuntu:

  ```
  apt-get update --assume-no && apt-get dist-upgrade --assume-yes
  ```

  CentOS/Red Hat:

  ```
  yum update -y
  ```

  SLES/SLED:

  ```
  zypper --non-interactive update -t patch
  ```

- **Windows** – a tarefa instala atualizações do sistema operacional chamando um Windows API interno. Ela não instala as atualizações do recurso, que atualizam seu Windows para uma versão mais recente.

Selecione uma das seguintes opções para criar uma nova tarefa de cliente:

- Clique em **Tarefas** > **Nova** > **Tarefa do cliente**.
- Clique em **Tarefas** > selecione o tipo de tarefa desejado e clique em **Nova** > **Tarefa do cliente**.
- Clique no dispositivo de destino em **Computadores** e selecione **Tarefas** > **Nova tarefa**.

Básico

Na seção **Básico**, insira informações básicas sobre a tarefa, como **Nome e Descrição (opcional)**. Clique em **Selecionar marcações** para atribuir marcações.
No menu suspenso **Tarefa**, selecione o tipo de tarefa que deseja criar e configurar. Se você selecionou um tipo de tarefa específico antes de criar uma nova tarefa, a **Tarefa** é pré-selecionada com base na sua escolha anterior. **Tarefa** (consulte a lista de todas as Tarefas) define as configurações e o comportamento da tarefa.

Configurações

- **Aceitar EULA automaticamente** (apenas Windows) - selecione essa caixa de seleção se quiser aceitar o EULA automaticamente. Nenhum texto será exibido ao usuário. Se você não ativar a aceitação do EULA, a tarefa ignora as atualizações que precisam da aceitação do EULA.

- **Instalar atualizações opcionais** (apenas Windows) – as atualizações que estão marcadas como opcionais e não necessitam de ação do usuário também serão instaladas.

- **Permitir reinicialização** (Windows e macOS) – force o computador cliente a reiniciar depois de instalar atualizações que requerem uma reinicialização.

Você pode configurar o comportamento de reinicialização/desligamento dos computadores gerenciados. O computador deve executar um Agente ESET Management 9.1 e um produto de segurança ESET compatível com esta configuração. Se o computador gerenciado não for compatível com a configuração do comportamento de reinicialização:

- O Windows vai notificar o usuário do computador sobre a reinicialização forçada planejada 4 horas antes da reinicialização e 10 minutos antes da reinicialização.

- O macOS será reiniciado imediatamente depois da atualização.

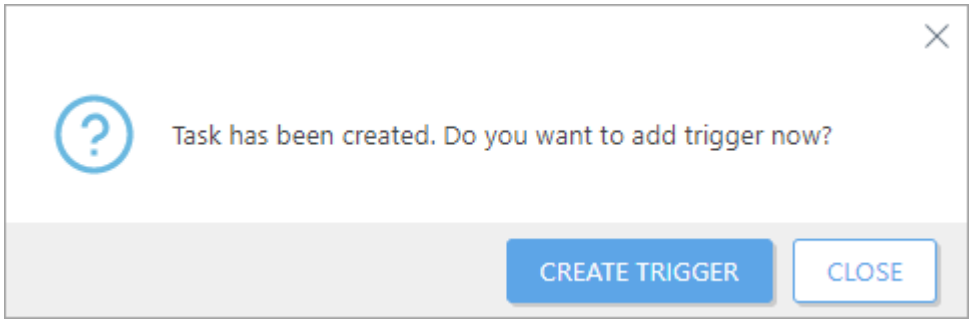
- Atualizações que requerem uma reinicialização serão instaladas mesmo se você não selecionar a caixa de seleção **Permitir reinicialização**.
- As **Configurações** não influenciam a tarefa se o dispositivo de destino estiver executando um tipo de sistema operacional incompatível.

Resumo

Revise o resumo da ajustes configurados e clique em **Concluir**. A tarefa agora será criada e uma janela pequeno será aberta:

- Clique em Criar acionador (recomendado) para especificar destinos de tarefa do cliente (computadores ou grupos) e o Acionador.

- Se clicar em **Fechar**, você pode criar um Acionador mais tarde: clique na instância da Tarefa do cliente e selecione **Executar em** no menu suspenso.



Em **Tarefas** você pode ver a barra de indicadores de progresso, o ícone de status e os detalhes para cada tarefa criada.

Gerenciamento de quarentena

A tarefa **Gerenciamento de quarentena** é usada para gerenciar objetos na quarentena do ESET PROTECT - objetos infectados ou suspeitos detectados durante o rastreamento.

Selecione uma das seguintes opções para criar uma nova tarefa de cliente:

- Clique em **Tarefas** > **Nova** > **Tarefa do cliente**.
- Clique em **Tarefas** > selecione o tipo de tarefa desejado e clique em **Nova** > **Tarefa do cliente**.
- Clique no dispositivo de destino em **Computadores** e selecione **Tarefas** > **Nova tarefa**.

Básico

Na seção **Básico**, insira informações básicas sobre a tarefa, como **Nome e Descrição (opcional)**. Clique em **Selecionar marcações** para atribuir marcações.
No menu suspenso **Tarefa**, selecione o tipo de tarefa que deseja criar e configurar. Se você selecionou um tipo de tarefa específico antes de criar uma nova tarefa, a **Tarefa** é pré-selecionada com base na sua escolha anterior. **Tarefa** (consulte a lista de todas as Tarefas) define as configurações e o comportamento da tarefa.

Configurações

Configurações de gerenciamento de quarentena

Ação - selecione a ação a ser realizada com o objeto em quarentena.

- **Restaurar objeto(s)** - restaura o objeto para seu local original, mas será rastreado e, se os motivos para a quarentena persistirem, o objeto será colocado em quarentena novamente.
- **Restaurar objeto(s) e excluir no futuro** - restaura o objeto para seu local original e não será colocado em quarentena novamente.
- **Excluir objeto(s)** - Exclui permanentemente o objeto.

Tipo de filtro - filtre os objetos na quarentena com base nos critérios definidos a seguir.

Configurações de filtro:

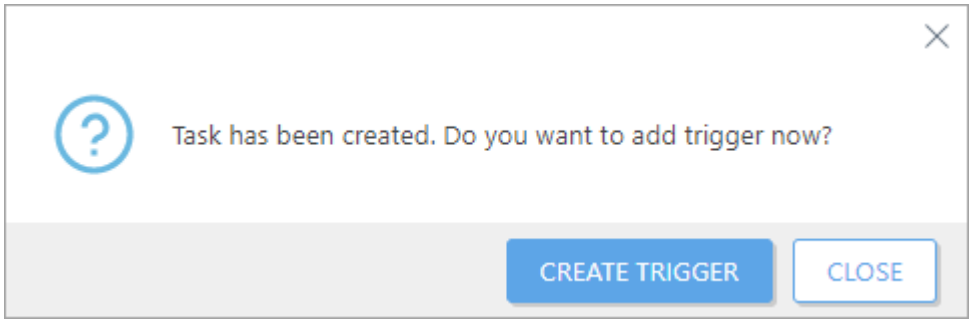
- **Itens de hash** – adiciona itens de hash ao campo. Somente objetos conhecidos podem ser inseridos, por exemplo, um objeto que já foi colocado em quarentena.
- **Ocorreu** > **Ocorreu de**, **Ocorreu até** – define o intervalo de tempo quando o objeto foi colocado em quarentena.
- **Tamanho** > **Tamanho mínimo/máximo (bytes)** - define a faixa de tamanho do objeto em quarentena (em bytes).
- **Nome da detecção** – selecione primeiro uma detecção dos itens em quarentena.

- **Nome do objeto** - selecione primeiro um objeto dos itens em quarentena.

Resumo

Revise o resumo da ajustes configurados e clique em **Concluir**. A tarefa agora será criada e uma janela pequeno será aberta:

- Clique em Criar acionador (recomendado) para especificar destinos de tarefa do cliente (computadores ou grupos) e o Acionador.
- Se clicar em **Fechar**, você pode criar um Acionador mais tarde: clique na instância da Tarefa do cliente e selecione **Executar em** no menu suspenso.



Em **Tarefas** você pode ver a barra de indicadores de progresso, o ícone de status e os detalhes para cada tarefa criada.

Ativação do produto

Use a tarefa **Ativação do produto** para ativar um produto de segurança ESET em um computador cliente ou dispositivo móvel.

Selecione uma das seguintes opções para criar uma nova tarefa de cliente:

- Clique em **Tarefas** > **Nova** > **Tarefa do cliente**.
- Clique em **Tarefas** > selecione o tipo de tarefa desejado e clique em **Nova** > **Tarefa do cliente**.
- Clique no dispositivo de destino em **Computadores** e selecione **Tarefas** > **Nova tarefa**.

Básico

Na seção **Básico**, insira informações básicas sobre a tarefa, como **Nome e Descrição (opcional)**. Clique em **Selecionar marcações** para atribuir marcações.
No menu suspenso **Tarefa**, selecione o tipo de tarefa que deseja criar e configurar. Se você selecionou um tipo de tarefa específico antes de criar uma nova tarefa, a **Tarefa** é pré-selecionada com base na sua escolha anterior. **Tarefa** (consulte a lista de todas as Tarefas) define as configurações e o comportamento da tarefa.

Configurações

Configurações de ativação do produto - Selecione a licença de produto adequada na lista de licenças disponíveis.

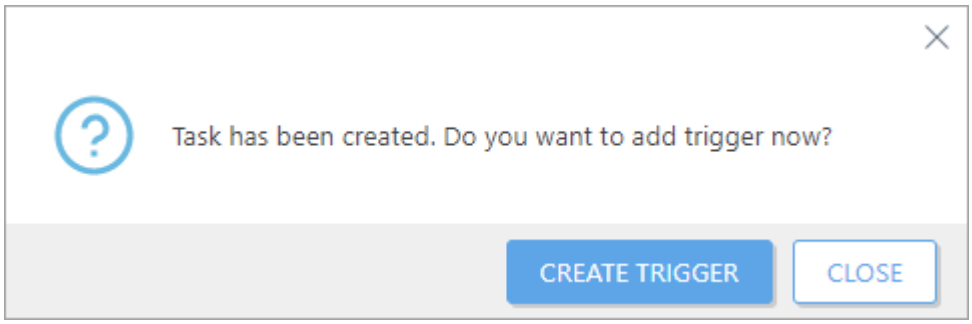
Esta licença será aplicada aos produtos já instalados no cliente. A lista de licenças disponíveis não mostra licenças expiradas e usadas em excesso (aquelas no estado **Erro** ou **Obsoleto**). Você pode adicionar uma licença usando um dos métodos descritos em Gerenciamento de licenças. A adição/remoção da licença é restrita ao Administrador cujo grupo doméstico é **Todos** e que tem a permissão de **Gravação** nas licenças.

A tarefa de **Ativação do produto** pode ativar um produto móvel, ESET Endpoint para Android, usando também uma licença off-line.
A tarefa de ativação não pode ativar os produtos ESET do versão 4 e 5 com a licença off-line. É preciso ativar o produto manualmente ou usar uma versão compatível do produto (Recomendamos usar a versão mais recente).

Resumo

Revise o resumo da ajustes configurados e clique em **Concluir**. A tarefa agora será criada e uma janela pequeno será aberta:

- Clique em Criar acionador (recomendado) para especificar destinos de tarefa do cliente (computadores ou grupos) e o Acionador.
- Se clicar em **Fechar**, você pode criar um Acionador mais tarde: clique na instância da Tarefa do cliente e selecione **Executar em** no menu suspenso.



Em **Tarefas** você pode ver a barra de indicadores de progresso, o ícone de status e os detalhes para cada tarefa criada.

Redefinir agente clonado

Você pode distribuir o Agente ESET Management na sua rede por meio de uma imagem predefinida, como descrito nesse artigo da Base de conhecimento. Agentes clonados têm a mesma SID, o que pode causar problemas (vários agentes com a mesma SID). Para resolver isso, use a tarefa **Redefinir agente clonado** para redefinir a SID e atribuir a Agentes uma identidade única.

O Agente ESET Management identifica máquinas clonadas de cliente sendo executadas no Windows automaticamente, sem a tarefa de Redefinir agente clonado. Somente máquinas clientes com Linux e MacOS (e clientes Windows onde a detecção de hardware foi desativada) precisam que a tarefa divida máquinas clonadas.

Selecione uma das seguintes opções para criar uma nova tarefa de cliente:

- Clique em **Tarefas** > **Nova** > **Tarefa do cliente**.
- Clique em **Tarefas** > selecione o tipo de tarefa desejado e clique em **Nova** > **Tarefa do cliente**.

- Clique no dispositivo de destino em **Computadores** e selecione **Tarefas** > **Nova tarefa**.

Básico

Na seção **Básico**, insira informações básicas sobre a tarefa, como **Nome e Descrição (opcional)**. Clique em **Selecionar marcações** para atribuir marcações.
No menu suspenso **Tarefa**, selecione o tipo de tarefa que deseja criar e configurar. Se você selecionou um tipo de tarefa específico antes de criar uma nova tarefa, a **Tarefa** é pré-selecionada com base na sua escolha anterior. **Tarefa** (consulte a lista de todas as Tarefas) define as configurações e o comportamento da tarefa.

Execute a tarefa com cuidado. Depois do Agente ESET Management atual ser redefinido, todas as tarefas sendo executadas nele serão abandonadas. O status de execução **Em execução**, **Concluído** ou **Falha** desta tarefa pode não ser observado, dependendo da replicação de dados.

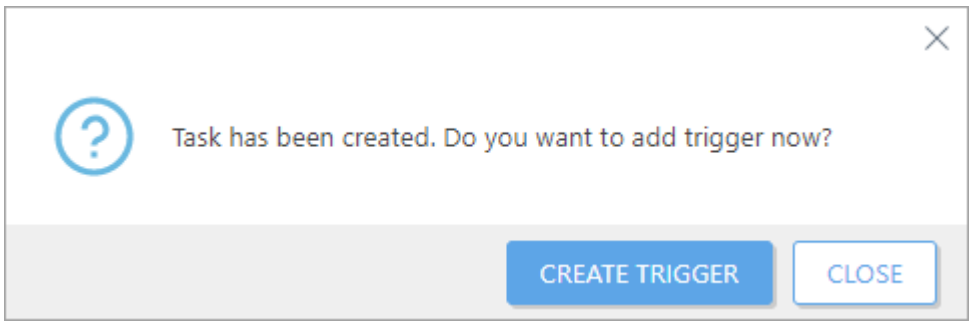
As **configurações** não estão disponíveis para essa tarefa.

Resumo

Revise o resumo da ajustes configurados e clique em **Concluir**. A tarefa agora será criada e uma janela pequeno será aberta:

- Clique em Criar acionador (recomendado) para especificar destinos de tarefa do cliente (computadores ou grupos) e o Acionador.

- Se clicar em **Fechar**, você pode criar um Acionador mais tarde: clique na instância da Tarefa do cliente e selecione **Executar em** no menu suspenso.



Em **Tarefas** você pode ver a barra de indicadores de progresso, o ícone de status e os detalhes para cada tarefa criada.

Redefinição de banco de dados do Rogue Detection Sensor

A tarefa **Redefinição de banco de dados do Sensor RD** é usada para redefinir o cache de pesquisa do Sensor RD. A tarefa exclui o cache e os resultados de pesquisa serão armazenados novamente. Essa tarefa não remove computadores detectados. Essa tarefa é útil quando computadores detectados ainda estiverem no cache e não forem relatados para o servidor.

Selecione uma das seguintes opções para criar uma nova tarefa de cliente:

- Clique em **Tarefas** > **Nova** > **Tarefa do cliente**.
- Clique em **Tarefas** > selecione o tipo de tarefa desejado e clique em **Nova** > **Tarefa do cliente**.
- Clique no dispositivo de destino em **Computadores** e selecione **Tarefas** > **Nova tarefa**.

Básico

Na seção **Básico**, insira informações básicas sobre a tarefa, como **Nome e Descrição (opcional)**. Clique em **Selecionar marcações** para atribuir marcações.
No menu suspenso **Tarefa**, selecione o tipo de tarefa que deseja criar e configurar. Se você selecionou um tipo de tarefa específico antes de criar uma nova tarefa, a **Tarefa** é pré-selecionada com base na sua escolha anterior. **Tarefa** (consulte a lista de todas as Tarefas) define as configurações e o comportamento da tarefa.

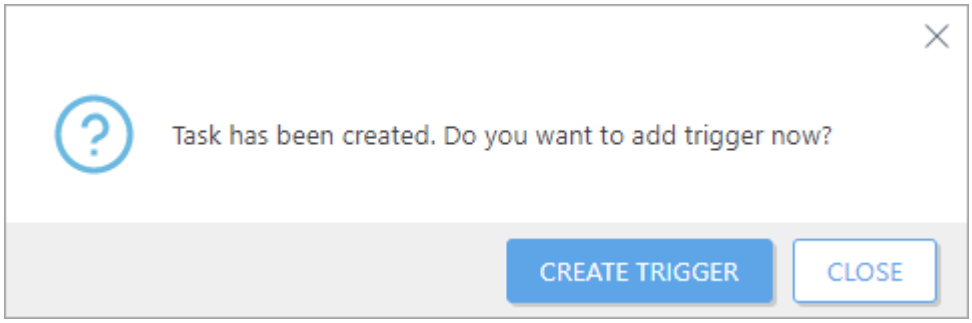
> As **configurações** não estão disponíveis para essa tarefa.

Ao criar um acionador para esta tarefa, tenha como destino um computador no qual o Sensor RD está instalado.

Resumo

Revise o resumo da ajustes configurados e clique em **Concluir**. A tarefa agora será criada e uma janela pequeno será aberta:

- Clique em Criar acionador (recomendado) para especificar destinos de tarefa do cliente (computadores ou grupos) e o Acionador.
- Se clicar em **Fechar**, você pode criar um Acionador mais tarde: clique na instância da Tarefa do cliente e selecione **Executar em** no menu suspenso.



Em **Tarefas** você pode ver a barra de indicadores de progresso, o ícone de status e os detalhes para cada tarefa criada.

Executar comando

A tarefa **Executar comando** pode ser usada para executar instruções específicas da linha de comando no cliente. O administrador pode especificar a entrada da linha de comando para execução.

Selecione uma das seguintes opções para criar uma nova tarefa de cliente:

- Clique em **Tarefas** > **Nova** > **Tarefa do cliente**.

- Clique em **Tarefas** > selecione o tipo de tarefa desejado e clique em **Nova** > **Tarefa do cliente**.
- Clique no dispositivo de destino em **Computadores** e selecione **Tarefas** > **Nova tarefa**.

Os comandos são executados sem acesso a um ambiente de área de trabalho. Como resultado, a execução de comandos com requisitos para a interface gráfica do usuário do aplicativo pode falhar.

Você pode usar comandos `ecmd` com a tarefa Executar comando. Para mais informações, visite o seguinte artigo da Base de conhecimento.

Sistema operacional	O comando será executado como usuário	Diretório de trabalho padrão	Locais de rede acessíveis	O comando será executado em
Windows	*Local System*	*C:\Windows\Temp*	Apenas localizações no domínio atual e disponível para o usuário do Sistema Local	Prompt de comando (`cmd.exe`)
Linux ou macOS	*root*	*/tmp*	Apenas a localização está montada e disponível para o usuário raiz	Console

Básico

Na seção **Básico**, insira informações básicas sobre a tarefa, como **Nome e Descrição (opcional)**. Clique em **Selecionar marcações** para atribuir marcações.
No menu suspenso **Tarefa**, selecione o tipo de tarefa que deseja criar e configurar. Se você selecionou um tipo de tarefa específico antes de criar uma nova tarefa, a **Tarefa** é pré-selecionada com base na sua escolha anterior. **Tarefa** (consulte a lista de todas as Tarefas) define as configurações e o comportamento da tarefa.

Configurações

- **Linha de comando para execução** - insira uma linha de comando que você deseja executar nos clientes.
- **Diretório de trabalho** - insira um diretório no qual a linha de comando acima será executada.

Você pode digitar um comando de várias linhas. Restrições de comprimento máximo do comando:
• O console web pode processar até 32.768 caracteres. Se você copiar e colar um comando mais longo, o console vai cortar silenciosamente o final.
• O Linux e o macOS podem processar todo o comprimento do comando. O Windows tem uma restrição para no máximo 8.191 caracteres.

• Para executar um script local localizado em um cliente no *C:\Users\user\script.bat* siga essas etapas:
1.Crie uma Nova tarefa de cliente e selecione **Executar comando**.
2.Na seção **Configurações**, insira:
Linha de comando para execução: `call script.bat`
Diretório de trabalho: *C:\Users\user*
3.Clique em **Concluir**, crie um acionador e escolha os clientes de destino.
• Para executar um comando de várias linhas para reiniciar um serviço do Windows remotamente (substitua `service_name` pelo nome do serviço, por exemplo `wuauserv` para o serviço Windows Update):

```
net stop service_name
net start service_name
```

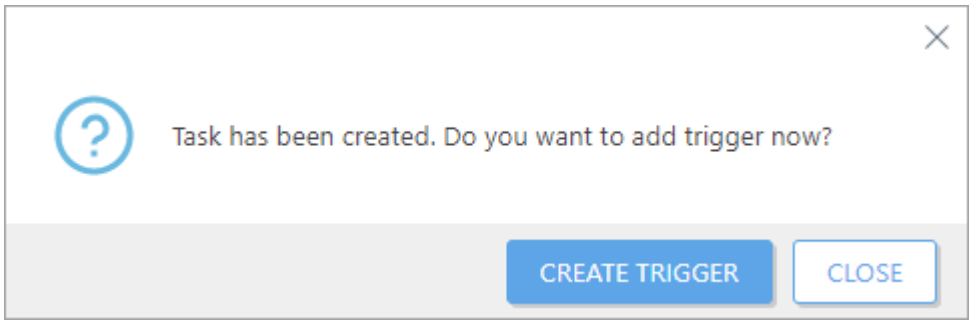
Resumo

Revise o resumo da ajustes configurados e clique em **Concluir**. A tarefa agora será criada e uma janela pequeno será aberta:

- Clique em Criar acionador (recomendado) para especificar destinos de tarefa do cliente (computadores ou

grupos) e o Acionador.

• Se clicar em **Fechar**, você pode criar um Acionador mais tarde: clique na instância da Tarefa do cliente e selecione **Executar em** no menu suspenso.



Em **Tarefas** você pode ver a barra de indicadores de progresso, o ícone de status e os detalhes para cada tarefa criada.

Examinar o resultado da tarefa Executar comando

1. Clique em **Tarefas** > clique na guia **Mostrar detalhes** > guia **Execução**, clique em uma linha na tabela > **Histórico**.

2. A coluna **Rastrear mensagem** contém os primeiros caracteres 255 de resultado da tarefa Executar comando. Você pode criar relatórios e processar esses dados a partir de vários computadores. Você pode fazer download de um resultado maior como um Relatório do Log Collector em **Detalhes** do computador > **Relatórios** > Log Collector.

Executar script do SysInspector

A tarefa **Executar script do SysInspector** é usada para remover objetos indesejados do sistema. Um Script do SysInspector precisa ser exportado do ESET SysInspector antes de usar essa tarefa. Depois de exportar o script, você poderá marcar objetos que deseja remover e executar o script com os dados modificados; os objetos marcados serão excluídos.

Selecione uma das seguintes opções para criar uma nova tarefa de cliente:

- Clique em **Tarefas** > **Nova** > **Tarefa do cliente**.
- Clique em **Tarefas** > selecione o tipo de tarefa desejado e clique em **Nova** > **Tarefa do cliente**.
- Clique no dispositivo de destino em **Computadores** e selecione **Tarefas** > **Nova tarefa**.

Básico

Na seção **Básico**, insira informações básicas sobre a tarefa, como **Nome e Descrição (opcional)**. Clique em **Selecionar marcações** para atribuir marcações.
No menu suspenso **Tarefa**, selecione o tipo de tarefa que deseja criar e configurar. Se você selecionou um tipo de tarefa específico antes de criar uma nova tarefa, a **Tarefa** é pré-selecionada com base na sua escolha anterior. **Tarefa** (consulte a lista de todas as Tarefas) define as configurações e o comportamento da tarefa.

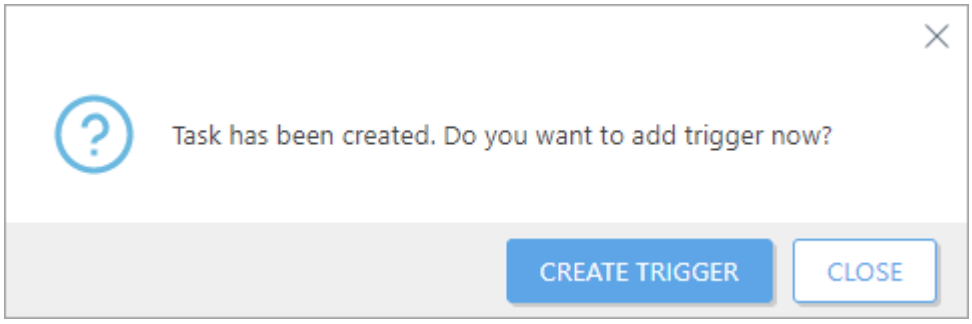
Configurações

- **Script do SysInspector** - clique em **Procurar** para acessar o script de serviço. O script de serviço precisa ser criado antes da execução dessa tarefa.
- **Ação** - você pode **Carregar** para ou **Fazer download** de um script do Console ESET PROTECT.

Resumo

Revise o resumo da ajustes configurados e clique em **Concluir**. A tarefa agora será criada e uma janela pequeno será aberta:

- Clique em Criar acionador (recomendado) para especificar destinos de tarefa do cliente (computadores ou grupos) e o Acionador.
- Se clicar em **Fechar**, você pode criar um Acionador mais tarde: clique na instância da Tarefa do cliente e selecione **Executar em** no menu suspenso.



Em **Tarefas** você pode ver a barra de indicadores de progresso, o ícone de status e os detalhes para cada tarefa criada.

Quando a tarefa for concluída, você pode verificar os resultados em um relatório.

Atualização de componentes do ESET PROTECT

A tarefa **ESET PROTECT Atualização de componentes** é usada para atualizar os componentes do ESET PROTECT (Agente ESET Management, Servidor ESET PROTECT, Web Console, ESET Bridge e MDM, mas não o Apache Tomcat ou o Proxy HTTP Apache). A tarefa de atualização pode ser executada apenas em uma máquina com o Agente ESET Management instalado. O Agente também é necessário em um Servidor ESET PROTECT.

O ESET PROTECT notifica automaticamente quando uma nova versão do Servidor ESET PROTECT está disponível.
Você pode atualizar para o ESET PROTECT 10.0 apenas do ESMC versão 7.2 e versões posteriores. Consulte o Guia de instalação para instruções detalhadas.
Veja também outras formas de atualizar o ESET PROTECT para a versão mais recente.

Para impedir uma falha na instalação, o ESET Management agente realiza as verificações a seguir antes de instalar ou atualizar produtos ESET:

- se o repositório puder ser acessado

- se há espaço livre suficiente (1 GB) na máquina do cliente (não disponível para Linux)

Selecione uma das seguintes opções para criar uma nova tarefa de cliente:

- Clique em **Tarefas** > **Nova** > **Tarefa do cliente**.
- Clique em **Tarefas** > selecione o tipo de tarefa desejado e clique em **Nova** > **Tarefa do cliente**.
- Clique no dispositivo de destino em **Computadores** e selecione **Tarefas** > **Nova tarefa**.

Básico

Na seção **Básico**, insira informações básicas sobre a tarefa, como **Nome e Descrição (opcional)**. Clique em **Selecionar marcações** para atribuir marcações.
No menu suspenso **Tarefa**, selecione o tipo de tarefa que deseja criar e configurar. Se você selecionou um tipo de tarefa específico antes de criar uma nova tarefa, a **Tarefa** é pré-selecionada com base na sua escolha anterior. **Tarefa** (consulte a lista de todas as Tarefas) define as configurações e o comportamento da tarefa.

Configurações

Selecione a caixa de seleção **Aceito os termos do Contrato de licença para o usuário final do aplicativo e reconheço a Política de Privacidade**. Consulte o Acordo de Licença para o Usuário Final (EULA), Termos de Uso e Política de Privacidade dos produtos ESET.

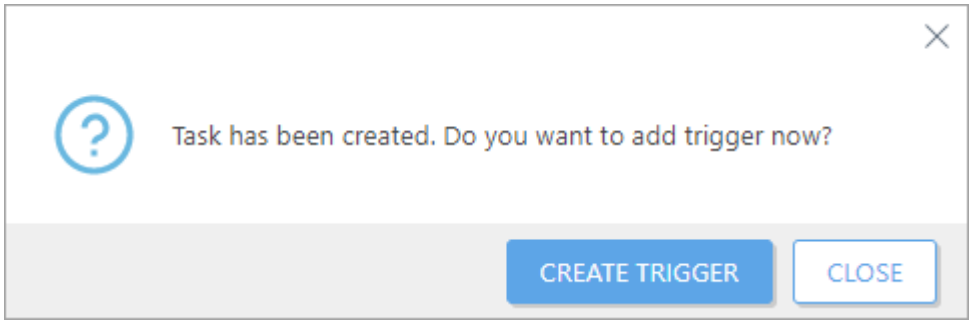
- **Servidor de referência do ESET PROTECT** – selecione a versão do Servidor ESET PROTECT da lista. Todos os componentes ESET PROTECT serão atualizados para versões compatíveis com o servidor selecionado.

Selecione a caixa de seleção ao lado de **Reinicialização automática quando necessário** para fazer uma reinicialização automática do computador do cliente depois da instalação. Alternativamente, você pode deixar esta opção desmarcada e reiniciar manualmente os computadores do cliente. Você pode configurar o comportamento de reinicialização/desligamento dos computadores gerenciados. O computador deve executar um Agente ESET Management 9.1 e um produto de segurança ESET compatível com esta configuração.

Resumo

Revise o resumo da ajustes configurados e clique em **Concluir**. A tarefa agora será criada e uma janela pequeno será aberta:

- Clique em Criar acionador (recomendado) para especificar destinos de tarefa do cliente (computadores ou grupos) e o Acionador.
- Se clicar em **Fechar**, você pode criar um Acionador mais tarde: clique na instância da Tarefa do cliente e selecione **Executar em** no menu suspenso.



Em **Tarefas** você pode ver a barra de indicadores de progresso, o ícone de status e os detalhes para cada tarefa criada.

A atualização pode levar um certo tempo, dependendo do seu sistema e configuração de rede. Não é possível acessar o Web Console durante a atualização do Servidor ESET PROTECT ou do Web Console. Depois da atualização, entre no Web Console e verifique se você tem a versão mais recente do ESET PROTECT em **Ajuda** > Sobre.

Enviar arquivo para ESET LiveGuard

Para executar esta Tarefa, navegue até **Detecções**.

Enviar arquivo para ESET LiveGuard está disponível apenas para **Arquivos bloqueados**. Você pode enviar um arquivo para análise de malware (ESET LiveGuard Advanced) do console web ESET PROTECT. Você pode ver os detalhes da análise do arquivo em Arquivos enviados. Você pode enviar manualmente arquivos executáveis para análise do ESET LiveGuard Advanced partindo do produto ESET endpoint (você precisa ter a licença ESET LiveGuard Advanced).

Escaneamento de servidor

Você pode usar a tarefa **Rastrear servidor** para rastrear clientes com soluções do Servidor ESET instaladas. Esse tipo de rastreamento depende da solução ESET instalada:

Produto	Rastrear	Descrição
ESET Server Security para Windows (anteriormente ESET File Security para Microsoft Windows Server)	**Hyper-V rastrear**	Esse tipo de escaneamento permite o escaneamento de discos de um Servidor Microsoft Hyper-V, que é uma máquina virtual (VM), sem instalar o Agente ESET Management na VM.
ESET Security para Microsoft SharePoint Server	**SharePoint rastreamento de banco de dados, Hyper-V rastreamento**	Essa funcionalidade deixa o ESET PROTECT usar o destino de escaneamento adequado ao executar a tarefa do Cliente **Escanear servidor** em um servidor com o ESET Security para Microsoft SharePoint.
ESET Mail Security para Microsoft Exchange Server	**Rastreamento de banco de dados de caixa de entrada sob demanda, rastreamento Hyper-V**	Essa funcionalidade deixa o ESET PROTECT usar o destino de rastreamento adequado. Quando o ESET PROTECT executa uma tarefa de cliente **Escanear servidor**, ele irá coletar a lista de destinos e você será solicitado a selecionar os destinos de escaneamento para o Rastreamento de banco de dados de caixa de entrada sob demanda naquele servidor em particular.

Produto	Rastrear	Descrição
ESET Mail Security para IBM Domino	**Escaneamento de banco de dados sob demanda, escaneamento Hyper-V**	Essa funcionalidade deixa o ESET PROTECT usar o destino de escaneamento adequado ao executar a tarefa do Cliente **Escanear servidor** em um servidor com o ESET Mail Security para IBM Domino.

Selecione uma das seguintes opções para criar uma nova tarefa de cliente:

- Clique em **Tarefas** > **Nova** > **Tarefa do cliente**.
- Clique em **Tarefas** > selecione o tipo de tarefa desejado e clique em **Nova** > **Tarefa do cliente**.
- Clique no dispositivo de destino em **Computadores** e selecione **Tarefas** > **Nova tarefa**.

Básico

Na seção **Básico**, insira informações básicas sobre a tarefa, como **Nome e Descrição (opcional)**. Clique em **Selecionar marcações** para atribuir marcações.
No menu suspenso **Tarefa**, selecione o tipo de tarefa que deseja criar e configurar. Se você selecionou um tipo de tarefa específico antes de criar uma nova tarefa, a **Tarefa** é pré-selecionada com base na sua escolha anterior. **Tarefa** (consulte a lista de todas as Tarefas) define as configurações e o comportamento da tarefa.

- Clique em **Selecionar** em **Servidor rastreado** e selecione um computador com a versão 6 ou versões posteriores dos produtos de segurança de servidor instalada. Você será solicitado a selecionar unidades, pastas ou arquivos específicos a serem rastreados naquele computador.
- Selecione um **Acionador** para essa tarefa, ou, se preferir, configure a alternância. Por padrão, a tarefa é realizada assim que possível.

Destinos para rastreamento

O ESET PROTECT oferece a você uma lista de destinos disponíveis no servidor selecionado. Para usar essa lista, **Gerar lista de destinos** deve estar ativado na política para seu produto de servidor sob **Ferramentas** > **Destinos de rastreamento ERA/ESMC**:

- **Gerar lista de destinos** - Ative essa configuração para permitir que o ESET PROTECT gere listas de destinos.
- **Período de atualização [minutos]** - Gerar a lista de destino pela primeira vez vai levar cerca de metade desse período.

Selecione destinos de rastreamento da lista. Para obter mais informações, consulte destinos de escaneamento ESET PROTECT.

Resumo

Todas as opções configuradas são exibidas aqui. Revise as configurações e clique em **Finalizar**.

Em **Tarefas** você pode ver a barra de indicadores de progresso, o ícone de status e os detalhes para cada tarefa criada.

Desligar computador

Você pode usar a tarefa **Desligar computador** para desligar ou reiniciar os computadores do cliente.

Selecione uma das seguintes opções para criar uma nova tarefa de cliente:

- Clique em **Tarefas** > **Nova** > **Tarefa do cliente**.
- Clique em **Tarefas** > selecione o tipo de tarefa desejado e clique em **Nova** > **Tarefa do cliente**.
- Clique no dispositivo de destino em **Computadores** e selecione **Tarefas** > **Nova tarefa**.

Básico

Na seção **Básico**, insira informações básicas sobre a tarefa, como **Nome e Descrição (opcional)**. Clique em **Selecionar marcações** para atribuir marcações.
No menu suspenso **Tarefa**, selecione o tipo de tarefa que deseja criar e configurar. Se você selecionou um tipo de tarefa específico antes de criar uma nova tarefa, a **Tarefa** é pré-selecionada com base na sua escolha anterior. **Tarefa** (consulte a lista de todas as Tarefas) define as configurações e o comportamento da tarefa.

Configurações

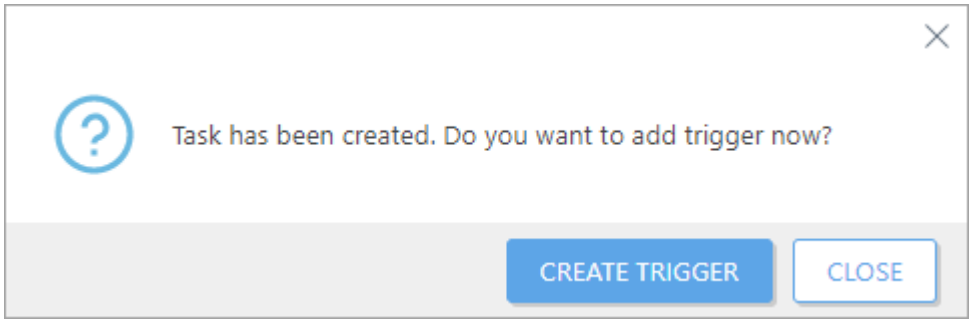
- **Reiniciar computador(es)** - selecione essa caixa de seleção se quiser reiniciar o computador cliente depois da conclusão da tarefa. Se deseja desligar o computador, deixe a opção desmarcada.

Você pode configurar o comportamento de reinicialização/desligamento dos computadores gerenciados. O computador deve executar um Agente ESET Management 9.1 e um produto de segurança ESET compatível com esta configuração.

Resumo

Revise o resumo da ajustes configurados e clique em **Concluir**. A tarefa agora será criada e uma janela pequeno será aberta:

- Clique em Criar acionador (recomendado) para especificar destinos de tarefa do cliente (computadores ou grupos) e o Acionador.
- Se clicar em **Fechar**, você pode criar um Acionador mais tarde: clique na instância da Tarefa do cliente e selecione **Executar em** no menu suspenso.



Em **Tarefas** você pode ver a barra de indicadores de progresso, o ícone de status e os detalhes para cada tarefa

criada.

Instalação de software

Use a tarefa **Instalação de software** para instalar software em seus computadores cliente:

- Instalar os produtos de segurança ESET. Alternativamente, você pode usar o menu de contexto em **Computadores**. Clique em um computador e selecione **Soluções** > **Implantação de produto de segurança** para implantar um produto de segurança ESET no computador.

- Atualizar produtos de segurança ESET Execute a tarefa usando o pacote do instalador mais recente para instalar a versão mais recente sobre sua solução existente. Você pode executar uma atualização de produto de segurança ESET imediata do **Painel** usando ações de um clique. Veja as instruções de atualização do ESET Security para Microsoft SharePoint para concluir essa atualização.

- Instalar software de terceiros.

Ambos ESET PROTECT Servidor o Agente ESET Management precisam ter acesso à internet para acessar o repositório e realizar instalações. Se você não tiver acesso à internet, é preciso instalar o software do cliente de forma local pois a instalação remota vai falhar, ou criar um repositório off-line. Para impedir uma falha na instalação, o ESET Management agente realiza as verificações a seguir antes de instalar ou atualizar produtos ESET:
- se o repositório puder ser acessado
- se há espaço livre suficiente (1 GB) na máquina do cliente (não disponível para Linux)

Ao realizar uma Tarefa de Instalação de software em computadores em um domínio com o Agente ESET Management em execução, o usuário deve ter permissão de *leitura* para a pasta onde os instaladores estão armazenados. Siga as etapas abaixo para conceder essas permissões se necessário.
1.Adicione uma conta de computador do Active Directory executando a tarefa (por exemplo *NewComputer$*).
2.Conceda permissões de **Leitura** para o *NewComputer$* clicando com o botão direito na pasta onde os instaladores estão localizados e selecionando **Propriedades** > **Compartilhamento** > **Compartilhar do menu de contexto**. Observe que o símbolo "$" precisa estar presente no final da string de nome do computador.
A instalação de um local compartilhado só é possível se a máquina do cliente estiver em um domínio.
Não use uma tarefa de Instalação de software para atualizar os componentes ESET PROTECT (Agente, Servidor, MDM). Use a Tarefa de atualização de componente em vez disso. Você pode usar uma tarefa de Instalação de software para atualizar apenas o componente do Rogue Detection Sensor.

Selecione uma das seguintes opções para criar uma nova tarefa de cliente:

- Clique em **Tarefas** > **Nova** > **Tarefa do cliente**.

- Clique em **Tarefas** > selecione o tipo de tarefa desejado e clique em **Nova** > **Tarefa do cliente**.

- Clique no dispositivo de destino em **Computadores** e selecione **Tarefas** > **Nova tarefa**.

Básico

Na seção **Básico**, insira informações básicas sobre a tarefa, como **Nome e Descrição (opcional)**. Clique em **Selecionar marcações** para atribuir marcações.
No menu suspenso **Tarefa**, selecione o tipo de tarefa que deseja criar e configurar. Se você selecionou um tipo de

tarefa específico antes de criar uma nova tarefa, a **Tarefa** é pré-selecionada com base na sua escolha anterior. **Tarefa** (consulte a lista de todas as Tarefas) define as configurações e o comportamento da tarefa.

Configurações

Pacote a instalar – existem duas opções:

- **Instalar pacote de repositório**

  o**Escolher sistema operacional** – selecione o sistema operacional para a instalação do produto.

  o**Escolher pacote do repositório –**clique em **Selecionar** e selecione um pacote instalador do produto de segurança ESET do repositório (por exemplo, ESET Endpoint Security). Selecione o idioma no menu suspenso **Idioma**. Por padrão, a versão mais recente está selecionada (recomendado). Você pode selecionar uma versão anterior. Para atualizar um produto ESET, selecione a versão mais recente disponível. Opcionalmente, clique em **Personalizar mais configurações** e selecione a versão do produto ESET. Clique em **Exibir o relatório de alterações** para ver o relatório de alterações da versão do produto selecionado. Clique em **OK**.

  o**Instalar a versão mais recente** – selecione a caixa de seleção para instalar a versão do produto ESET mais recente se o Acordo de Licença para o Usuário Final do produto já estiver aceito.

- **Instalar por URL de pacote direto** – para especificar um URL com o pacote de instalação, digite ou copie e cole o URL no campo de texto (não use um URL que exija autenticação):

  o*http://server_address/ees_nt64_ENU.msi* – Se você estiver instalando de um servidor da web público ou do seu próprio servidor HTTP.

  o*file://\\pc22\install\ees_nt64_ENU.msi* – se você estiver instalando do caminho da rede.

  o*file://C:\installs\ees_nt64_ENU.msi* – se você estiver instalando do caminho local.

Licença ESET –Selecione a licença de produto adequada na lista de licenças disponíveis. A licença ativará o produto de segurança ESET durante a instalação. A lista de licenças disponíveis não mostra licenças expiradas e usadas em excesso (aquelas no estado **Erro** ou **Obsoleto**). Se você não escolher uma licença, você pode instalar o produto de segurança ESET sem a licença e ativar o produto mais tarde. Você pode adicionar uma licença usando um dos métodos descritos em Gerenciamento de licenças. A adição/remoção da licença é restrita ao Administrador cujo grupo doméstico é **Todos** e que tem a permissão de **Gravação** nas licenças.

- Selecione uma licença apenas quando estiver instalando ou atualizando produtos que não estão ativos, ou se quiser alterar a licença atual para uma licença diferente.

- Não selecione uma licença ao atualizar um produto já ativado.

Ativar ESET LiveGuard – a caixa de seleção estará disponível se você tiver uma licença ESET LiveGuard Advanced e tiver selecionado um produto de segurança ESET compatível com o ESET LiveGuard Advanced e a licença do produto. Selecione a caixa de seleção para ativar o ESET LiveGuard Advanced nos computadores de destino da tarefa de Instalação de software. Depois da ativação, você pode gerenciar as configurações do ESET LiveGuard Advanced usando uma política.

Selecione a caixa de seleção **Aceito os termos do Contrato de licença para o usuário final do aplicativo e reconheço a Política de Privacidade**. Consulte o Acordo de Licença para o Usuário Final (EULA), Termos de Uso e Política de Privacidade dos produtos ESET.

Se você selecionou um produto de segurança ESET para Windows:Selecione a caixa de seleção ao lado da configuração para ativá-la para o instalador:

oAtivar o sistema de feedback ESET LiveGrid® (recomendado)

oAtivar a detecção de aplicativos potencialmente indesejados – leia mais em nosso artigo da Base de conhecimento.

Parâmetros de instalação (opcional):

- Use os parâmetros de instalação da linha de comando apenas com as configurações de interface do usuário **reduzidas**, **básicas** e **nenhuma**.
- Consulte a documentação da versão **msiexec** usada para as alternâncias da linha de comando apropriadas.
- Leia a respectiva Ajuda on-line para instalação por linha de comando dos produtos ESET Endpoint e produtos do Servidor ESET.

Selecione a caixa de seleção ao lado de **Reinicialização automática quando necessário** para fazer uma reinicialização automática do computador do cliente depois da instalação. Alternativamente, você pode deixar esta opção desmarcada e reiniciar manualmente os computadores do cliente. Você pode configurar o comportamento de reinicialização/desligamento dos computadores gerenciados. O computador deve executar um Agente ESET Management 9.1 e um produto de segurança ESET compatível com esta configuração.

Instalação de software de terceiro

Você pode usar a tarefa **Instalação de software** para instalar um software que não seja da ESET (de terceiros).

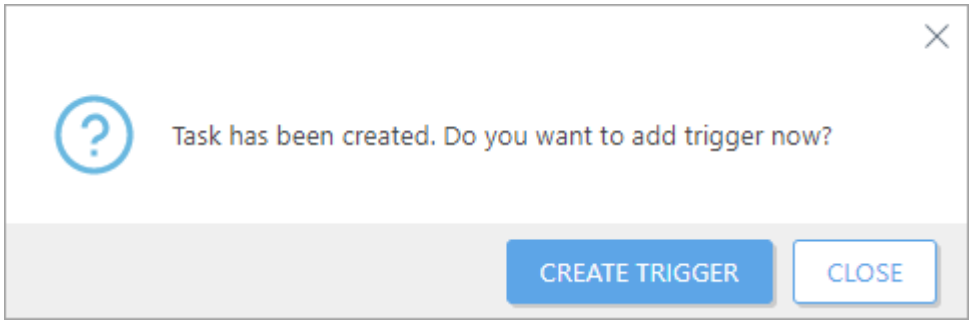
Sistema operacional	Tipos de arquivo de instalação compatíveis	Suporte para parâmetros de instalação
Windows	*.msi*	A tarefa de Instalação de software sempre realiza a instalação silenciosa dos pacotes *.msi*. Não é possível especificar parâmetros msiexec. Você pode especificar apenas parâmetros usados pelo próprio pacote de instalação (exclusivo para cada pacote de instalação de software).
Linux	*.deb*, *.rpm*, *.sh*	Você pode usar parâmetro apenas com arquivos *.sh* (*.deb* e *.rpm* não são compatíveis com parâmetros).
macOS	*.pkg*, *.dmg* (contendo o arquivo *.pkg*	Os parâmetros de instalação não são compatíveis.
Android	*.apk*	Os parâmetros de instalação não são compatíveis.
iOS	*.ipa*	Os parâmetros de instalação não são compatíveis.

Você quer instalar o software no Linux usando o arquivo *install_script.sh* que tem dois parâmetros: `-a` é o primeiro parâmetro, `-b` é o segundo parâmetro.
Instalação no terminal (como usuário root na pasta onde o *install_script.sh está localizado*):
`./install_script.sh -a parameter_1 -b parameter_2`
Instalação usando a tarefa de Instalação de software:
- Digite o caminho do arquivo em **Instalar por URL de pacote direto**, por exemplo: *file:///home/user/Desktop/install_script.sh*
- Digite os **parâmetros de instalação**: `-a parameter_1 -b parameter_2`.

Resumo

Revise o resumo da ajustes configurados e clique em **Concluir**. A tarefa agora será criada e uma janela pequeno será aberta:

- Clique em Criar acionador (recomendado) para especificar destinos de tarefa do cliente (computadores ou grupos) e o Acionador.
- Se clicar em **Fechar**, você pode criar um Acionador mais tarde: clique na instância da Tarefa do cliente e selecione **Executar em** no menu suspenso.



Em **Tarefas** você pode ver a barra de indicadores de progresso, o ícone de status e os detalhes para cada tarefa criada.

Lista de problemas quando a instalação falha

- Pacote de instalação não encontrado.
- É preciso ter uma versão mais recente necessária do Windows Installer Service.
- Outra versão ou produto em conflito já está instalado.
- Outra instalação já está em andamento. Conclua essa instalação antes de prosseguir com essa instalação.
- Instalação ou desinstalação concluída com êxito mas é necessário reiniciar o computador.
- A tarefa falhou – um erro aconteceu. É preciso ver o relatório de rastro do Agente e verificar o código de retorno do instalador.

Software Safetica

O que é o Safetica

Safetica é uma empresa de software de terceiros que faz parte da ESET Technology Alliance. A Safetica oferece uma solução de segurança de TI para Prevenção de perda de dados e é complementar às soluções de segurança ESET. Recursos primários do software Safetica incluem:

- Prevenção de perda de dados - monitoramento de todos os discos rígidos, unidades USB, transferências de arquivos de rede, emails e impressoras, assim como acesso a arquivos do aplicativo
- Relatórios e bloqueio de atividades - para operações de arquivo, sites, emails, mensagens instantâneas, uso de aplicativos e palavras-chave pesquisadas

Como o Safetica funciona

O Safetica usa um Agente (Cliente Safetica Endpoint) para seus endpoints desejados e mantém uma conexão regular com eles através do servidor (Serviço de Gerenciamento Safetica). Esse servidor constrói um banco de dados de atividades da estação de trabalho e distribui novas políticas de proteção de dados e regulamentos para cada estação de trabalho.

Integração do Safetica no ESET PROTECT

O Agente ESET Management detecta e reporta o software Safetica como um software ESET em **Detalhes do computador** > Aplicativos instalados. O Web Console ESET PROTECT vai atualizar o Agente Safetica se houver uma nova versão disponível.

Implantar Agente Safetica

Você pode implantar o Agente Safetica diretamente do Web Console ESET PROTECT do repositório de software ESET usando a tarefa de Instalação de software e digitando `STSERVER=Server_name` nos **Parâmetros de instalação** (`Server_name` é o nome de host/endereço IP do servidor onde o **Serviço de Gerenciamento Safetica** está instalado).

Alternativamente, é possível instalar o Agente Safetica com a Tarefa do cliente – Executar comando.

^ Use a tarefa Executar comando

```
msiexec /i safetica_agent.msi STSERVER=Server_name
```

Você pode usar o parâmetro `/silent` no final do comando para executar a instalação remotamente e no modo "silencioso": `msiexec /i safetica_agent.msi STSERVER=Server_name /silent`
Para a instalação mencionada acima, o pacote .msi já deve estar presente no dispositivo. Para executar a instalação quando o pacote *.msi* está em um local compartilhado, especifique o local no comando da seguinte maneira: `msiexec /i Z:\sharedLocation\safetica_agent.msi STSERVER=Server_name`

Atualizar Safetica Agente

Para atualizar o Agente Safetica em um computador gerenciado, vá para **Detalhes do computador** > Aplicativos instalados > selecione **Safetica Agente** e clique em **Atualizar produtos ESET**.

Desinstalar Agente Safetica

Para desinstalar o Agente Safetica de um computador gerenciado, vá para **Detalhes do computador** > Aplicativos instalados > selecione o **Safetica Agente** e clique em **Desinstalar**.

Desinstalação de software

A tarefa **Desinstalação de software** é usada para desinstalar um produto ESET de computadores do cliente quando eles não são mais desejados/necessários.

Selecione uma das seguintes opções para criar uma nova tarefa de cliente:

- Clique em **Tarefas** > **Nova** > **Tarefa do cliente**.
- Clique em **Tarefas** > selecione o tipo de tarefa desejado e clique em **Nova** > **Tarefa do cliente**.
- Clique no dispositivo de destino em **Computadores** e selecione **Tarefas** > **Nova tarefa**.

Básico

Na seção **Básico**, insira informações básicas sobre a tarefa, como **Nome e Descrição (opcional)**. Clique em **Selecionar marcações** para atribuir marcações.
No menu suspenso **Tarefa**, selecione o tipo de tarefa que deseja criar e configurar. Se você selecionou um tipo de tarefa específico antes de criar uma nova tarefa, a **Tarefa** é pré-selecionada com base na sua escolha anterior. **Tarefa** (consulte a lista de todas as Tarefas) define as configurações e o comportamento da tarefa.

Configurações

Configurações de desinstalação de software

Desinstalar - Aplicativo da lista

- **Nome do pacote** - Selecione um componente ESET PROTECT, um produto de segurança do cliente ou um aplicativo de terceiros. Você pode ativar relatórios de aplicativos de terceiros (que não são da ESET) usando a configuração de Política do Agente. Todos os pacotes que podem ser desinstalados dos clientes selecionados serão exibidos nessa lista.

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 estiver protegido por senha, não será possível desinstalá-lo. 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.

- **Versão do pacote** - Você pode remover uma versão específica (às vezes, uma versão específica pode causar problemas) do pacote ou **desinstalar todas as versões do pacote**.

- **Parâmetros de desinstalação** - Você pode especificar parâmetros para a desinstalação.

- Selecione a caixa de seleção ao lado de **Reinicialização automática quando necessário** para fazer uma reinicialização automática do computador do cliente depois da instalação. Alternativamente, você pode deixar esta opção desmarcada e reiniciar manualmente os computadores do cliente. Você pode configurar o comportamento de reinicialização/desligamento dos computadores gerenciados. O computador deve executar um Agente ESET Management 9.1 e um produto de segurança ESET compatível com esta configuração.

Desinstalar - Software antivírus de terceiros (com OPSWAT)

Você pode ativar relatórios de aplicativos de terceiros (que não são da ESET) usando a configuração de Política do Agente.

Para uma lista de Software AV compatíveis, consulte nosso artigo da Base de conhecimento. Esta remoção é diferente da desinstalação **Adicionar ou remover programas**. Ela usa métodos alternativos para remover

completamente software antivírus de terceiros, inclusive quaisquer entradas de registro residuais ou outros traços.

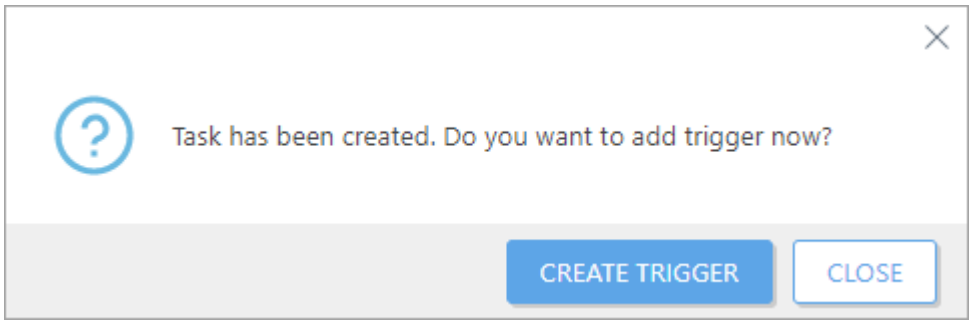
Siga as instruções passo a passo neste artigo Remover software antivírus de terceiros de computadores cliente usando o ESET PROTECT para enviar uma tarefa para remover software antivírus de terceiros de computadores do cliente.

Se quiser permitir a desinstalação de aplicativos protegidos por senha veja nosso artigo da Base de Conhecimento.

Resumo

Revise o resumo da ajustes configurados e clique em **Concluir**. A tarefa agora será criada e uma janela pequeno será aberta:

- Clique em Criar acionador (recomendado) para especificar destinos de tarefa do cliente (computadores ou grupos) e o Acionador.
- Se clicar em **Fechar**, você pode criar um Acionador mais tarde: clique na instância da Tarefa do cliente e selecione **Executar em** no menu suspenso.



Em **Tarefas** você pode ver a barra de indicadores de progresso, o ícone de status e os detalhes para cada tarefa criada.

> A tarefa de desinstalação do produto de segurança ESET pode falhar com um erro relacionado a senha, por exemplo: **Produto: ESET Endpoint Security -- Erro 5004. Digite uma senha válida para continuar a desinstalação**. Isso acontece devido a uma configuração de proteção de senha ativada no produto de segurança ESET. Aplique uma política ao(s) computador(es) do cliente para remover a proteção por senha. Então você pode desinstalar o produto de segurança ESET através da tarefa de Desinstalação de Software.

Interromper gerenciamento (desinstalar agente ESET Management)

Essa tarefa vai desinstalar o Agente ESET Management dos dispositivo de destino selecionados. Se uma área de trabalho for selecionada, a tarefa vai remover o Agente ESET Management. Se dispositivo móvel estiver selecionado a tarefa vai cancelar a inscrição MDM do dispositivo.

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 estiver protegido por senha, não será possível desinstalá-lo. 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.

Selecione uma das seguintes opções para criar uma nova tarefa de cliente:

- Clique em **Tarefas** > **Nova** > **Tarefa do cliente**.
- Clique em **Tarefas** > selecione o tipo de tarefa desejado e clique em **Nova** > **Tarefa do cliente**.
- Clique no dispositivo de destino em **Computadores** e selecione **Tarefas** > **Nova tarefa**.

Básico

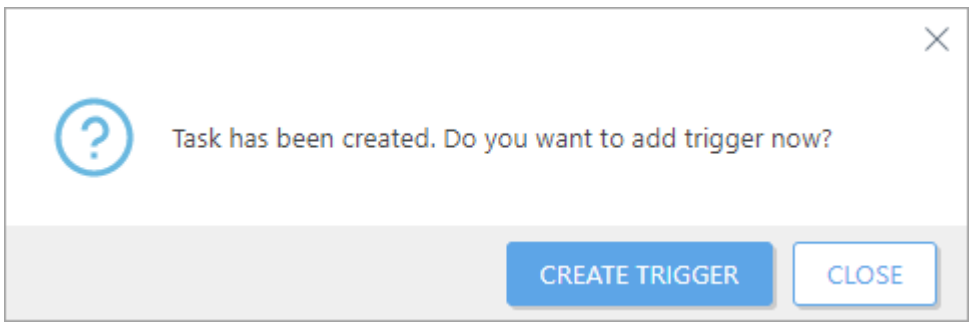
Na seção **Básico**, insira informações básicas sobre a tarefa, como **Nome e Descrição (opcional)**. Clique em **Selecionar marcações** para atribuir marcações.
No menu suspenso **Tarefa**, selecione o tipo de tarefa que deseja criar e configurar. Se você selecionou um tipo de tarefa específico antes de criar uma nova tarefa, a **Tarefa** é pré-selecionada com base na sua escolha anterior. **Tarefa** (consulte a lista de todas as Tarefas) define as configurações e o comportamento da tarefa.

As **configurações** não estão disponíveis para essa tarefa.

Resumo

Revise o resumo da ajustes configurados e clique em **Concluir**. A tarefa agora será criada e uma janela pequeno será aberta:

- Clique em Criar acionador (recomendado) para especificar destinos de tarefa do cliente (computadores ou grupos) e o Acionador.
- Se clicar em **Fechar**, você pode criar um Acionador mais tarde: clique na instância da Tarefa do cliente e selecione **Executar em** no menu suspenso.



Em **Tarefas** você pode ver a barra de indicadores de progresso, o ícone de status e os detalhes para cada tarefa criada.

Solicitação de relatório do SysInspector (apenas Windows)

A tarefa **Solicitação de log do SysInspector** é usada para solicitar o log do SysInspector de um produto de segurança cliente.

O ESET SysInspector é executado apenas em computadores Windows.

Selecione uma das seguintes opções para criar uma nova tarefa de cliente:

- Clique em **Tarefas** > **Nova** > **Tarefa do cliente**.
- Clique em **Tarefas** > selecione o tipo de tarefa desejado e clique em **Nova** > **Tarefa do cliente**.
- Clique no dispositivo de destino em **Computadores** e selecione **Tarefas** > **Nova tarefa**. Você também pode executar essa tarefa de **Computadores,** > clique em um computador > **Detalhes** > **Relatórios** > **Solicitar relatório (apenas Windows)**.

Básico

Na seção **Básico**, insira informações básicas sobre a tarefa, como **Nome e Descrição (opcional)**. Clique em **Selecionar marcações** para atribuir marcações.
No menu suspenso **Tarefa**, selecione o tipo de tarefa que deseja criar e configurar. Se você selecionou um tipo de tarefa específico antes de criar uma nova tarefa, a **Tarefa** é pré-selecionada com base na sua escolha anterior. **Tarefa** (consulte a lista de todas as Tarefas) define as configurações e o comportamento da tarefa.

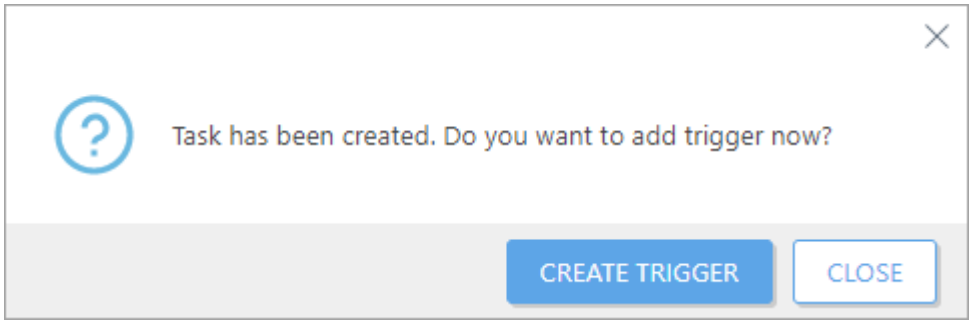
Configurações

- **Armazenar registro em cliente** - selecione isso se quiser armazenar o log do SysInspector no cliente, bem como no ESET PROTECT. Servidor. Por exemplo, quando um cliente tiver o ESET Endpoint Security instalado, o relatório geralmente será armazenado em *C:\Program Data\ESET\ESET Security\SysInspector*.

Resumo

Revise o resumo da ajustes configurados e clique em **Concluir**. A tarefa agora será criada e uma janela pequeno será aberta:

- Clique em Criar acionador (recomendado) para especificar destinos de tarefa do cliente (computadores ou grupos) e o Acionador.
- Se clicar em **Fechar**, você pode criar um Acionador mais tarde: clique na instância da Tarefa do cliente e selecione **Executar em** no menu suspenso.



Em **Tarefas** você pode ver a barra de indicadores de progresso, o ícone de status e os detalhes para cada tarefa criada.

Depois da tarefa ser concluída, uma nova entrada será exibida na lista de relatórios ESET SysInspector. Clique em um relatório listado para explorar.

Carregar arquivo em quarentena

A tarefa **Carregar arquivo em quarentena** é usada para gerenciar arquivos em quarentena em clientes. Você pode carregar arquivo em quarentena da quarentena para um local específico para uma investigação avançada.

Selecione uma das seguintes opções para criar uma nova tarefa de cliente:

- Clique em **Tarefas** > **Nova** > **Tarefa do cliente**.
- Clique em **Tarefas** > selecione o tipo de tarefa desejado e clique em **Nova** > **Tarefa do cliente**.
- Clique no dispositivo de destino em **Computadores** e selecione **Tarefas** > **Nova tarefa**.

Básico

Na seção **Básico**, insira informações básicas sobre a tarefa, como **Nome e Descrição (opcional)**. Clique em **Selecionar marcações** para atribuir marcações.
No menu suspenso **Tarefa**, selecione o tipo de tarefa que deseja criar e configurar. Se você selecionou um tipo de tarefa específico antes de criar uma nova tarefa, a **Tarefa** é pré-selecionada com base na sua escolha anterior.
Tarefa (consulte a lista de todas as Tarefas) define as configurações e o comportamento da tarefa.

Configurações

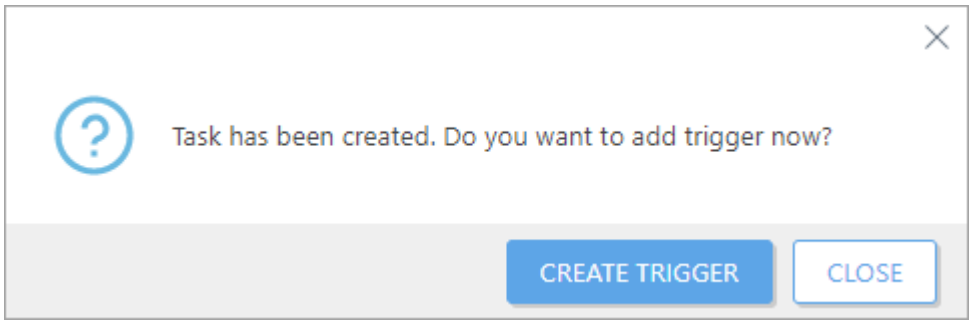
- **Objeto em quarentena** - selecione um objeto específico da quarentena.
- **Senha do objeto** - insira uma senha para criptografar o objeto por motivos de segurança. Note que a senha será exibida no relatório correspondente.
- **Carregar caminho** - insira um caminho para um local no qual deseja carregar o objeto. Use a sintaxe a seguir: *smb://server/share*
- **Carregar nome de usuário/senha** - no caso de o local exigir autenticação (compartilhamento de rede, etc.), insira as credenciais para acessar esse caminho. Se o usuário estiver em um domínio, use o formato `DOMAIN\username`.

No Acionador, certifique-se de selecionar o destino onde o arquivo foi colocado em quarentena.

Resumo

Revise o resumo da ajustes configurados e clique em **Concluir**. A tarefa agora será criada e uma janela pequeno será aberta:

- Clique em Criar acionador (recomendado) para especificar destinos de tarefa do cliente (computadores ou grupos) e o Acionador.
- Se clicar em **Fechar**, você pode criar um Acionador mais tarde: clique na instância da Tarefa do cliente e selecione **Executar em** no menu suspenso.



Em **Tarefas** você pode ver a barra de indicadores de progresso, o ícone de status e os detalhes para cada tarefa criada.

Depois que o arquivo colocado em quarentena foi enviado para o local do **Caminho de envio** selecionado:

- O arquivo é armazenado em um arquivo *.zip* protegido por senha. A senha é o nome do arquivo *.zip* (hash do arquivo em quarentena).
- O arquivo colocado em quarentena não tem extensão de arquivo. Para restaurar o arquivo, adicione a extensão do arquivo original a ele.

Tarefas do servidor

As tarefas do servidor são executadas pelo ESET PROTECT Servidor em si mesmo ou em outros dispositivos. Tarefas do servidor não podem ser atribuídas a um cliente ou grupo de cliente específicos. Cada tarefa do servidor tem um acionador configurado. Se a tarefa precisar ser executada com vários eventos, é preciso que existam tarefas do servidor separadas para cada acionador.

Permissões e tarefas do servidor

A tarefa e o acionador precisam, ambos, de um usuário que as executem. Este é o usuário que modificou a tarefa (e o acionador). O usuário deve ter permissões suficientes para a ação selecionada. Durante a execução a tarefa sempre toma o usuário que está executando a partir do acionador. Se a tarefa for executada usando a configuração **Executar tarefa imediatamente depois de concluir**, o usuário executando é o usuário que fez login no Console da Web ESET PROTECT. Um usuário com permissões (**Leitura**, **Uso**, **Gravação**) para a instância da **tarefa do servidor** selecionada se ele tiver essas permissões selecionadas em seu conjunto de permissões (**Mais** > **Conjuntos de permissões**) e se tiver essas permissões definidas para o Grupo estático onde a tarefa do servidor

está localizada. Veja a lista de permissões para obter mais informações sobre os direitos de acesso.

John, cujo grupo inicial é o *Grupo do John*, quer remover a *Tarefa do servidor 1:* **Gerar relatório**. A tarefa foi originalmente criada por *Larry*, portanto a tarefa está automaticamente contida no grupo inicial de Larry, o *Grupo do Larry*. As seguintes condições devem ser atendidas para que *John* remova a tarefa:
- *John* deve receber a atribuição de um conjunto de permissões com as permissões **gravação** para **Acionadores e tarefas do servidor** - **Gerar relatórios**.
- O conjunto de permissões deve ter o *Grupo do Larry* sob os **Grupos estáticos**.

Permissões necessárias para certas ações de tarefa do servidor

- Para criar uma nova tarefa do servidor, o usuário precisa de permissão de **gravação** para o tipo de tarefa selecionado e direitos de acesso adequados para os objetos referenciados (computadores, licenças, grupos).

- Para modificar uma tarefa do servidor, o usuário precisa de permissão de **gravação** para a instância de tarefa do servidor selecionada e direitos de acesso adequados para os objetos referenciados (computadores, licenças, grupos).

- Para remover uma tarefa do servidor, o usuário precisa de permissão de **gravação** para a instância de tarefa do servidor selecionada.

- Para executar uma tarefa do servidor, o usuário precisa de permissão de **uso** para a instância de tarefa do servidor selecionada.

Criar uma nova tarefa do servidor

1. Para criar uma nova Tarefa do servidor, clique em **Tarefas** > **Nova** > **Tarefa do servidor** ou selecione o tipo de tarefa desejado na esquerda e clique em **Novo** > **Tarefa do servidor**.

2. Na seção **Básico**, insira informações básicas sobre a tarefa, como **Nome e Descrição (opcional)**. Clique em **Selecionar marcações** para atribuir marcações.
No menu suspenso **Tarefa**, selecione o tipo de tarefa que deseja criar e configurar. Se você selecionou um tipo de tarefa específico antes de criar uma nova tarefa, a **Tarefa** é pré-selecionada com base na sua escolha anterior. **Tarefa** (consulte a lista de todas as Tarefas) define as configurações e o comportamento da tarefa.

Você também pode selecionar a partir das configurações de acionador de tarefa a seguir:

- **Executar tarefa imediatamente depois de concluir** - Selecione isto para que a tarefa seja executada automaticamente depois de clicar em Concluir.

- **Configurar acionador** - Selecione esta opção para ativar a seção Acionador, onde você pode configurar as configurações do acionador.

Para definir o acionador mais tarde, deixe as caixas de seleção desmarcadas.

3.Configure as configurações de tarefa na seção **Configurações**.

4.Defina o acionador na seção **Acionador**, se ele estiver disponível.

5.Verifique todas as configurações para esta tarefa na seção **Resumo** e clique em **Concluir**.

É recomendado que os usuários que estejam usando regularmente as Tarefas do servidor criem suas próprias tarefas em vez de compartilhá-las com outros usuários. Cada vez que a tarefa é executada ela usa as permissões do usuário executando-a. Isso pode confundir alguns usuários.

Implantação do agente

A tarefa do servidor de implantação do Agente executa a implantação remota do Agente ESET Management.

A tarefa de instalação do agente executa a instalação do Agente ESET Management nos computadores de destino um por um (sequencialmente). Como resultado, quando você executa a tarefa de Implantação do Agente em muitos computadores clientes, ela pode levar muito tempo para ser concluída. Portanto, recomendamos que você use a opção ESET Remote Deployment Tool. Ela executa a instalação do Agente ESET Management em todos os computadores de destino ao mesmo tempo (paralelamente) e também economiza largura de banda usando arquivos do instalador armazenados localmente, sem precisar acessar o repositório on-line.

Para criar uma nova Tarefa do servidor, clique em **Tarefas** > **Nova** > **Tarefa do servidor** ou selecione o tipo de tarefa desejado na esquerda e clique em **Novo** > **Tarefa do servidor**.

Básico

Na seção **Básico**, insira informações básicas sobre a tarefa, como **Nome e Descrição (opcional)**. Clique em **Selecionar marcações** para atribuir marcações.
No menu suspenso **Tarefa**, selecione o tipo de tarefa que deseja criar e configurar. Se você selecionou um tipo de tarefa específico antes de criar uma nova tarefa, a **Tarefa** é pré-selecionada com base na sua escolha anterior. **Tarefa** (consulte a lista de todas as Tarefas) define as configurações e o comportamento da tarefa.

Você também pode selecionar a partir das configurações de acionador de tarefa a seguir:

- **Executar tarefa imediatamente depois de concluir** - Selecione isto para que a tarefa seja executada automaticamente depois de clicar em Concluir.
- **Configurar acionador** - Selecione esta opção para ativar a seção Acionador, onde você pode configurar as configurações do acionador.

Para definir o acionador mais tarde, deixe as caixas de seleção desmarcadas.

Configurações de implantação do agente

Destinos - Clique nessa opção para selecionar os clientes que vão receber essa tarefa.

Se computadores de destino foram adicionados ao ESET PROTECT usando a tarefa de Sincronização de grupo estático, certifique-se de que os nomes dos computadores são os nomes de domínio completos. Esses nomes são usados como os endereços dos clientes durante a implantação e, se não estiverem corretos, a implantação vai falhar. Use o atributo `dNSHostName` como o **Atributo de nome de host do computador** durante a sincronização para fins de instalação do Agente.

Nome do host do servidor (opcional) - você pode inserir um nome do host do servidor se for diferente daquele por parte do cliente e do servidor.

Credenciais dos computadores de destino

Nome de usuário/Senha - o nome de usuário e a senha do usuário com direitos suficientes para realizar uma instalação remota do Agente.

Configurações de certificado

Certificado de mesmo nível:

- **ESET PROTECT certificado** – um Certificado de mesmo nível para instalação do Agente e a Autoridade de Certificação ESET PROTECT é selecionada automaticamente. Para usar um certificado diferente, clique na **Descrição do certificado ESET PROTECT** para selecionar de um menu suspenso de certificados disponíveis.

- **Certificado personalizado** – se você usar um certificado personalizado para autenticação, clique em **Certificado personalizado** > **Selecionar** e envie o certificado .pfx, e selecione-o ao instalar o Agente. Para obter mais informações, consulte Certificados.

Senha do certificado – digite a senha do certificado se necessário – se você especificou o senha durante a instalação do servidor ESET PROTECT (na etapa na qual criou a Autoridade de certificação) ou se usa um certificado personalizado com uma senha. Caso contrário, deixe o campo **Código de certificado** em branco.

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

O Servidor ESET PROTECT pode selecionar automaticamente o pacote de instalação do Agente apropriado para sistemas operacionais :

- Linux – selecione um usuário com permissão para usar o comando `sudo` ou um usuário `root`. Se o `root` for usado, o serviço `ssh` deve permitir a você fazer login como `root`.

- Linux ou macOS – certifique-se de que a máquina de destino tem o daemon SSH ativado e em execução na porta 22 e que o firewall não está bloqueando essa conexão. Use o comando a seguir (substitua o endereço IP com o IP do seu Servidor ESET PROTECT) para adicionar uma exceção no firewall do Linux:
```
iptables -A INPUT -s 10.0.0.1 -p tcp --dport 22 -m state --state NEW -j ACCEPT
```

- Para impedir a falha da tarefa de instalação do Agente, consulte a solução de problemas de instalação do Agente.

Outras configurações

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).

Acionador

A seção **Acionador** contém informações sobre os acionadores que devem executar uma tarefa. Cada **Tarefa do servidor** pode ter até um acionador. Cada acionador só pode executar uma **Tarefa do servidor**. Se **Configurar acionador** não estiver selecionado na seção **Básico**, um acionador não é criado. Uma tarefa pode ser criada sem um acionador. Tal tarefa pode ser executada depois manualmente ou um acionador pode ser adicionado mais

tarde.

Configurações avançadas - Alternância

Ao configurar a Alternância, você pode definir regras avançadas para o acionador criado. A configuração da alternância é opcional.

Resumo

Todas as opções configuradas são exibidas aqui. Revise as configurações e clique em **Finalizar**.

Em **Tarefas** você pode ver a barra de indicadores de progresso, o ícone de status e os detalhes para cada tarefa criada.

Solução de problemas

Se a tarefa de instalação do Agente falhar, consulte a solução de problemas de instalação do Agente.

> ⚠ Para instalar novamente o Agente ESET Management nunca remova o Agente instalado no momento. Execute a tarefa de instalação do Agente sobre o Agente instalado no momento. Quando você remove o Agente, o novo Agente pode começar a executar tarefas antigas depois da nova implantação.

Excluir computadores não conectando

A tarefa Excluir computadores não conectando permite que você remova os computadores de acordo com critérios especificados. Por exemplo, se o Agente ESET Management em um computador cliente não tiver se conectado durante 30 dias, ele pode ser removido a partir do console da Web ESET PROTECT.

Navegar para Computadores. **Última conexão** exibe a data e hora da última conexão do dispositivo gerenciado. Um ponto verde indica que o computador se conectou há menos de 10 minutos. As informações da **Última conexão** são destacadas para indicar que o computador não está se conectando:

- Amarelo (erro) – O computador não conecta há 2-14 dias.
- Vermelho (aviso) – O computador não conecta há mais de 14 dias.

Para criar uma nova Tarefa do servidor, clique em **Tarefas** > **Nova** > **Tarefa do servidor** ou selecione o tipo de tarefa desejado na esquerda e clique em **Novo** > **Tarefa do servidor**.

Básico

Na seção **Básico**, insira informações básicas sobre a tarefa, como **Nome e Descrição (opcional)**. Clique em **Selecionar marcações** para atribuir marcações.
No menu suspenso **Tarefa**, selecione o tipo de tarefa que deseja criar e configurar. Se você selecionou um tipo de tarefa específico antes de criar uma nova tarefa, a **Tarefa** é pré-selecionada com base na sua escolha anterior. **Tarefa** (consulte a lista de todas as Tarefas) define as configurações e o comportamento da tarefa.

Você também pode selecionar a partir das configurações de acionador de tarefa a seguir:

- **Executar tarefa imediatamente depois de concluir** - Selecione isto para que a tarefa seja executada automaticamente depois de clicar em Concluir.

- **Configurar acionador** - Selecione esta opção para ativar a seção Acionador, onde você pode configurar as configurações do acionador.

Para definir o acionador mais tarde, deixe as caixas de seleção desmarcadas.

Configurações

Nome do grupo - selecione um grupo estático ou crie um novo um grupo estático para computadores renomeados.

Número de dias que o computador não esteve conectado - digite o número de dias depois do qual os computadores serão removidos.

Desativar licença – selecione essa caixa de seleção para desativar as licenças nos computadores removidos.

Remover computadores não gerenciados – selecione essa caixa de seleção para remover também computadores não gerenciados.

Acionador

A seção **Acionador** contém informações sobre os acionadores que devem executar uma tarefa. Cada **Tarefa do servidor** pode ter até um acionador. Cada acionador só pode executar uma **Tarefa do servidor**. Se **Configurar acionador** não estiver selecionado na seção **Básico**, um acionador não é criado. Uma tarefa pode ser criada sem um acionador. Tal tarefa pode ser executada depois manualmente ou um acionador pode ser adicionado mais tarde.

Configurações avançadas - Alternância

Ao configurar a Alternância, você pode definir regras avançadas para o acionador criado. A configuração da alternância é opcional.

Resumo

Todas as opções configuradas são exibidas aqui. Revise as configurações e clique em **Finalizar**.

Em **Tarefas** você pode ver a barra de indicadores de progresso, o ícone de status e os detalhes para cada tarefa criada.

Gerar relatório

A tarefa **Gerar relatório** é usada para gerar relatórios a partir de modelos de relatório criados ou pré-definidos anteriormente.

Para criar uma nova Tarefa do servidor, clique em **Tarefas** > **Nova** > **Tarefa do servidor** ou selecione o tipo de tarefa desejado na esquerda e clique em **Novo** > **Tarefa do servidor**.

Básico

Na seção **Básico**, insira informações básicas sobre a tarefa, como **Nome e Descrição (opcional)**. Clique em **Selecionar marcações** para atribuir marcações.
No menu suspenso **Tarefa**, selecione o tipo de tarefa que deseja criar e configurar. Se você selecionou um tipo de tarefa específico antes de criar uma nova tarefa, a **Tarefa** é pré-selecionada com base na sua escolha anterior. **Tarefa** (consulte a lista de todas as Tarefas) define as configurações e o comportamento da tarefa.

Você também pode selecionar a partir das configurações de acionador de tarefa a seguir:

- **Executar tarefa imediatamente depois de concluir** - Selecione isto para que a tarefa seja executada automaticamente depois de clicar em Concluir.
- **Configurar acionador** - Selecione esta opção para ativar a seção Acionador, onde você pode configurar as configurações do acionador.

Para definir o acionador mais tarde, deixe as caixas de seleção desmarcadas.

Configurações

Modelos de relatório - Clique em Adicionar modelo de relatório para escolher um modelo de relatório da lista. O usuário criando a tarefa conseguirá ver e escolher apenas a partir dos Modelos de relatório que estiverem disponíveis para seu grupo. Você pode escolher vários modelos de relatório para um relatório.

Selecione Enviar email ou Salvar em arquivo para obter o relatório gerado.

Relatório de entrega

Enviar email

Para enviar/receber mensagens de email, é preciso configurar as configurações SMTP em **Mais** > Configurações > **Configurações avançadas**.

- **Enviar para** - Digite o(s) endereço(s) de email de destinatários dos emails de relatório. Separe endereços múltiplos com uma vírgula (,). Também é possível adicionar campos CC e BCC, eles funcionam da mesma forma que para clientes de email.
- O ESET PROTECT pré-preenche o assunto e o corpo do relatório com base no modelo de relatório selecionado. Você pode marcar a caixa de seleção em **Personalizar mensagem** para personalizar o **Assunto** e a **Mensagem**:
  - **Assunto** - Assunto da mensagem de relatório. Insira um assunto distinto, para que as mensagens chegando possam ser separadas. Esta é uma configuração opcional, mas recomendamos que ela não fique em branco.
  - **Mensagem** - Define o corpo da mensagem do relatório.
- **Enviar email se o relatório estiver vazio** - use esta opção se quiser que o relatório seja enviado mesmo se não houver dados nele.

Clique em **Mostrar opções de impressão** para exibir as seguintes configurações:

- **Formato de saída** - selecione o formato de arquivo apropriado. Você pode escolher de *.pdf* ou *.csv*. CSV é adequado apenas para dados da tabela e usa ; (ponto e vírgula) como delimitador. Se você fizer download de um relatório CSV e ver os números em uma coluna onde você espera um texto, recomendamos fazer download de um relatório PDF para ver os valores em texto.

> Selecionar CSV faz com que os valores de data e hora no seu relatório sejam armazenados no formato UTC. Quando você seleciona PDF, o relatório vai usar o horário local do servidor.

- **Idioma de saída** - selecione o idioma da mensagem. O idioma padrão tem como base o idioma selecionado do console da Web ESET PROTECT.

- **Tamanho da página/Resolução/Orientação do papel/Formato de cor/Unidades de margem/Margens** – selecione as opções apropriadas com base em suas preferências de impressão. Essas opções são relevantes se você quiser imprimir o relatório e aplicar apenas ao formato PDF, não ao formato CSV.

Salvar em arquivo

- **Caminho de arquivo relativo** - O relatório será gerado em um diretório específico, por exemplo:

  - Para Windows, o relatório normalmente é colocado em *C:\ProgramData\ESET\RemoteAdministrator\Server\EraServerApplicationData\Data\GeneratedReports*

  - Para Linux, o relatório normalmente é colocado em /var/opt/eset/RemoteAdministrator/Server/GeneratedReports/

> No Windows, alguns caracteres especiais (: ? \) não serão interpretados corretamente no nome de arquivo armazenado.

- **Salvar arquivo se o relatório estiver vazio** - use esta opção se quiser que o relatório seja salvo mesmo se não houver dados nele.

Clique em **Mostrar opções de impressão** para exibir as seguintes configurações:

- **Formato de saída** - selecione o formato de arquivo apropriado. Você pode escolher de *.pdf* ou *.csv*. CSV é adequado apenas para dados da tabela e usa ; (ponto e vírgula) como delimitador. Se você fizer download de um relatório CSV e ver os números em uma coluna onde você espera um texto, recomendamos fazer download de um relatório PDF para ver os valores em texto.

> Selecionar CSV faz com que os valores de data e hora no seu relatório sejam armazenados no formato UTC. Quando você seleciona PDF, o relatório vai usar o horário local do servidor.

- **Idioma de saída** - selecione o idioma da mensagem. O idioma padrão tem como base o idioma selecionado do console da Web ESET PROTECT.

- **Tamanho da página/Resolução/Orientação do papel/Formato de cor/Unidades de margem/Margens** – selecione as opções apropriadas com base em suas preferências de impressão. Essas opções são relevantes se você quiser imprimir o relatório e aplicar apenas ao formato PDF, não ao formato CSV.

Acionador

A seção **Acionador** contém informações sobre os acionadores que devem executar uma tarefa. Cada **Tarefa do servidor** pode ter até um acionador. Cada acionador só pode executar uma **Tarefa do servidor**. Se **Configurar acionador** não estiver selecionado na seção **Básico**, um acionador não é criado. Uma tarefa pode ser criada sem um acionador. Tal tarefa pode ser executada depois manualmente ou um acionador pode ser adicionado mais tarde.

Configurações avançadas - Alternância

Ao configurar a Alternância, você pode definir regras avançadas para o acionador criado. A configuração da alternância é opcional.

Resumo

Todas as opções configuradas são exibidas aqui. Revise as configurações e clique em **Finalizar**.

Em **Tarefas** você pode ver a barra de indicadores de progresso, o ícone de status e os detalhes para cada tarefa criada.

Renomear computadores

Você pode usar a tarefa **Renomear Computadores** para renomear computadores para o formato FQDN no ESET PROTECT. Você pode usar a tarefa do servidor existente que veio como padrão com sua instalação ESET PROTECT. Se um nome de dispositivo do cliente for diferente daquele reportado nos detalhes do dispositivo, executar essa tarefa pode restaurar o nome adequado.

Esta tarefa renomeia automaticamente os computadores sincronizados localizados no grupo **Perdido e encontrado** a cada hora.

Para criar uma nova Tarefa do servidor, clique em **Tarefas** > **Nova** > **Tarefa do servidor** ou selecione o tipo de tarefa desejado na esquerda e clique em **Novo** > **Tarefa do servidor**.

Básico

Na seção **Básico**, insira informações básicas sobre a tarefa, como **Nome e Descrição (opcional)**. Clique em **Selecionar marcações** para atribuir marcações.
No menu suspenso **Tarefa**, selecione o tipo de tarefa que deseja criar e configurar. Se você selecionou um tipo de tarefa específico antes de criar uma nova tarefa, a **Tarefa** é pré-selecionada com base na sua escolha anterior. **Tarefa** (consulte a lista de todas as Tarefas) define as configurações e o comportamento da tarefa.

Você também pode selecionar a partir das configurações de acionador de tarefa a seguir:

- **Executar tarefa imediatamente depois de concluir** - Selecione isto para que a tarefa seja executada automaticamente depois de clicar em Concluir.

- **Configurar acionador** - Selecione esta opção para ativar a seção Acionador, onde você pode configurar as configurações do acionador.

Para definir o acionador mais tarde, deixe as caixas de seleção desmarcadas.

Configurações

Nome do grupo - selecione um grupo estático ou dinâmico ou crie um novo grupo estático ou grupo dinâmico para computadores renomeados.

Renomear baseado em:

- **Nome do computador** - Cada computador é identificado na rede local por seu nome de computador único
- **FQDN (Nome do domínio totalmente qualificado) do computador** - Isso começa com o nome de host e continua com os nomes de domínio, até o nome de domínio de maior nível.

A resolução de conflitos de nome será realizada para computadores já presentes no ESET PROTECT (o nome do computador deve ser exclusivo) e aqueles adicionados via sincronização. As verificações aplicam-se somente aos nomes de computadores fora da sub-árvore sendo sincronizada.

Acionador

A seção **Acionador** contém informações sobre os acionadores que devem executar uma tarefa. Cada **Tarefa do servidor** pode ter até um acionador. Cada acionador só pode executar uma **Tarefa do servidor**. Se **Configurar acionador** não estiver selecionado na seção **Básico**, um acionador não é criado. Uma tarefa pode ser criada sem um acionador. Tal tarefa pode ser executada depois manualmente ou um acionador pode ser adicionado mais tarde.

Configurações avançadas - Alternância

Ao configurar a Alternância, você pode definir regras avançadas para o acionador criado. A configuração da alternância é opcional.

Resumo

Todas as opções configuradas são exibidas aqui. Revise as configurações e clique em **Finalizar**.

Em **Tarefas** você pode ver a barra de indicadores de progresso, o ícone de status e os detalhes para cada tarefa criada.

Sincronização de grupo estático

A tarefa **Sincronização de grupo estático** vai pesquisar sua rede (Active Directory, Open Directory, LDAP, rede local ou VMware) em busca de computadores e colocá-los em um Grupo estático. Se você selecionar **Sincronizar com o Active Directory** durante a Instalação do servidor, os computadores encontrados são adicionados ao grupo **Todos**. Para sincronizar os computadores Linux que ingressaram no domínio Windows, siga essas instruções detalhadas.

> O ESET PROTECT é compatível com a assinatura LDAP segura.

Existem três **Modos de sincronização**:

- Active Directory/Open Directory/LDAP - Digite as informações de conexão do servidor básicas.

> Você pode executar a tarefa do servidor de Implantação do Agente para implantar o Agente ESET Management nos computadores sincronizados do Active Directory.

- Rede MS Windows - Insira um **Grupo de trabalho** a ser usado, junto com as credenciais de usuário adequadas.

> O modo de sincronização de **rede do MS Windows** pode não funcionar devido a requisitos faltando (SMBv1) que são necessários para sua operação bem-sucedida. A ESET vai remover esse modo de sincronização no futuro.

- VMware- Digite as informações de conexão do servidor VMware vCenter.

Modo de sincronização - Active Directory/Open Directory/LDAP

Para criar uma nova Tarefa do servidor, clique em **Tarefas** > **Nova** > **Tarefa do servidor** ou selecione o tipo de tarefa desejado na esquerda e clique em **Novo** > **Tarefa do servidor**.

Básico

Na seção **Básico**, insira informações básicas sobre a tarefa, como **Nome e Descrição (opcional)**. Clique em **Selecionar marcações** para atribuir marcações.
No menu suspenso **Tarefa**, selecione o tipo de tarefa que deseja criar e configurar. Se você selecionou um tipo de tarefa específico antes de criar uma nova tarefa, a **Tarefa** é pré-selecionada com base na sua escolha anterior. **Tarefa** (consulte a lista de todas as Tarefas) define as configurações e o comportamento da tarefa.

Você também pode selecionar a partir das configurações de acionador de tarefa a seguir:

- **Executar tarefa imediatamente depois de concluir** - Selecione isto para que a tarefa seja executada automaticamente depois de clicar em Concluir.

- **Configurar acionador** - Selecione esta opção para ativar a seção Acionador, onde você pode configurar as configurações do acionador.

Para definir o acionador mais tarde, deixe as caixas de seleção desmarcadas.

Configurações

Configurações comuns

Clique em **Selecionar** sob **Nome do grupo estático** - por padrão, o grupo inicial do usuário executando a ação será usado para os computadores sincronizados. Alternativamente, você pode criar um **Novo grupo estático**.

- **Objeto a sincronizar** - Ou **Computadores e grupos** ou **Apenas Computadores**.
- **Processamento de colisão na criação de computador** - Se a sincronização adicionar computadores que já são membros do grupo estático, é possível selecionar um método de solução de conflito:
  - **Ignorar** (computadores sincronizados não serão adicionados)
  - **Mover** (novos computadores serão movidos a um subgrupo)
  - **Duplicar** (um novo computador é criado com o nome modificado)
- **Processamento de extinção de computador** - Se um computador não existir mais, você pode **Remover** este computador ou **Ignorar**.
- **Processamento de extinção de grupo** - Se um grupo não existir mais, você pode **Remover** este grupo ou **Ignorar**.

Se você definir o **Tratamento de extinção de grupo** como **Ignorar** e remover um grupo (Unidade Organizacional) do Active Directory, os computadores que pertenciam ao grupo no ESET PROTECT não serão removidos, mesmo quando você definir o **Tratamento de extinção do computador** deles para **Remover**.

- **Modo de sincronização** - **Active Directory/Open Directory/LDAP**

Leia nosso artigo da Base de conhecimento sobre o gerenciamento de computadores usando a sincronização do Active Directory no ESET PROTECT.

Configurações de conexão do servidor

- **Servidor** - Digite o nome do servidor ou endereço IP do seu controlador de domínio.
- **Efetuar login** - Digite o nome de usuário para seu controlador de domínio no formato a seguir:
  - `DOMAIN\username` (Servidor ESET PROTECT em execução no Windows)
  - `username@FULL.DOMAIN.NAME` ou `username` (Servidor ESET PROTECT em execução no Linux).

Não se esqueça de digitar o domínio em letras maiúsculas. Esta formatação é necessária para fazer a autenticação adequada de consultas no servidor do Active Directory.

- **Senha** - Digite a senha usada para fazer login no seu controlador de domínio.

O Servidor ESET PROTECT no Windows usa o protocolo LDAPS criptografado (LDAP sobre SSL) por padrão para todas as conexões com o Active Directory (AD). Você também pode Configurar LDAPS na máquina virtual ESET PROTECT.
Para uma conexão AD bem-sucedida no LDAPS, configure o seguinte:
1. O controlador de domínio deve ter um certificado de máquina instalado. Para emitir um certificado para seu controlador de domínio, siga as etapas abaixo:
a)Abra o **Gerenciador de servidor**, clique em **Gerenciar** > **Adicionar funções e recursos** e instale os **Serviços de certificados do Active Directory** > **Autoridade de certificação**. Uma nova Autoridade de certificação será criada em **Autoridades de certificação raiz confiáveis**.
b)Navegue até **Início** > digite `certmgr.msc` e pressione **Enter** para executar o snap-in do Console de Gerenciamento da Microsoft **Certificados** > **Certificados – computador local** > **Pessoal** > clique com o botão direito na janela vazia > **Todas as tarefas** > **Solicitar novo certificado** > função **Inscrever controlador de domínio**.
c)Verifique se o certificado emitido contém o FQDN do controlador de domínio.
d)No seu servidor ESMC, importe a CA gerada para o depósito de certificados (usando a ferramenta `certmgr.msc`) para a pasta de CAs confiáveis.

2. Ao fornecer as configurações de conexão ao servidor AD, digite o FQDN do controlador de domínio (conforme fornecido no certificado do controlador de domínio) no campo **Servidor** ou **Host**. O endereço IP não é mais suficiente para o LDAPS.

Para ativar o fallback para o protocolo LDAP, selecione a caixa de seleção **Usar LDAP em vez do Active Directory** e insira os atributos específicos para combinar com o seu servidor. Alternativamente, selecione **Pré-seleção** clicando em **Selecionar** e os atributos serão preenchidos automaticamente:

- **Active Directory**
- **Mac OS X Server Open Directory (nomes de host de computador)**
- **Mac OS X Server Open Directory (endereços IP de computador)**
- **OpenLDAP com registros de computador Samba** - Para configurar os parâmetros do nome DNS no Active Directory.

Ao selecionar **Usar LDAP em vez do Active Directory** e a predefinição do **Active Directory,** você pode preencher os detalhes do computador com atributos da sua estrutura do Active Directory. Apenas atributos do tipo `DirectoryString` podem ser usados. Você pode usar uma ferramenta (por exemplo *ADExplorer*) para inspecionar os atributos no seu Controlador de domínio. Veja os campos correspondentes na tabela abaixo:

Campos de detalhes do computador	Campos das tarefas de sincronização
Nome	**Atributo de nome de host do computador**
Descrição	**Atributo de descrição do computador**

Configurações de sincronização

- **Nome diferenciado** - Caminho (Nome diferenciado) para o nó na árvore do Active Directory. Deixar essa opção vazia vai sincronizar toda a árvore AD. Clique em **Procurar** ao lado de **Nome diferenciado**. Sua árvore do Active Directory será exibida. Selecione a entrada de cima para sincronizar todos os grupos com o ESET PROTECT, ou selecione somente os grupos específicos que você deseja adicionar. Apenas computadores e Unidades organizacionais são sincronizados. Clique em **OK** quando tiver terminado.

Determinar o Nome diferenciado

1.Abra o aplicativo **Usuários e computadores do Active Directory**.
2.Clique em **Exibir** e selecione **Recursos avançados**.
3.Clique com o botão direito do mouse no domínio > clique em **Propriedades** > selecione a guia **Editor de atributo**.
4.Localize **distinguishedName** a linha. Ele deve se parecer com este exemplo: `DC=ncop,DC=local`.

- **Nome(s) diferenciado(s) excluído(s)** - Você pode escolher excluir (ignorar) nós específicos na árvore do Active Directory.

- **Ignorar computadores desativados (somente no Active Directory)** - É possível selecionar para ignorar os computadores desativados no active directory (a tarefa vai pular esses computadores).

Se você receber o erro: `Server not found in Kerberos database` depois de clicar em **Procurar**, use o AD FQDN do servidor em vez do endereço IP.

Sincronização do servidor Linux

O Servidor ESET PROTECT sendo executado no Linux faz a sincronização de maneira diferente das máquinas Windows. O processo acontece da seguinte forma:
1. O nome de host e as credencias do controlador de domínio devem ser preenchidos.
2. O Servidor verifica as credencias e elas são convertidas para um bilhete Kerberos.
3. O Servidor detecta o nome diferenciado do Domínio, se ele não estiver presente.
4. A) Se a opção **Usar LDAP em vez de Active Directory** não estiver selecionada:
Várias chamadas para o `ldapsearch` enumeram a árvore. Um exemplo simplificado do processo de obter registros do computador:

```
kinit <username>
```

(Este é um comando dividido em duas linhas:)

```
ldapsearch -LLL -Y GSSAPI -h ad.domain.com -b 'DC=domain,DC=com' \
'(&(objectCategory=computer))' 'distinguishedName' 'dNSHostName'
```

B) Se a opção **Usar LDAP em vez de Active Directory** estiver selecionada:
O mesmo processo é chamado como na opção 4A, mas o usuário pode configurar os parâmetros.
5. O Kerberos usa um mecanismo de aperto de mão para autenticar o usuário e gerar um bilhete que pode ser usado posteriormente com outros serviços, para fazer a autorização sem enviar uma senha em texto simples (ao contrário da opção **Usar autenticação simples**).
6. O utilitário `ldapsearch` vai então usar o GSSAPI para fazer a autenticação contra o Active Directory com o bilhete Kerberos obtido.
7. Os resultados de pesquisa são enviados de volta por meio de um canal não criptografado.

Acionador

A seção **Acionador** contém informações sobre os acionadores que devem executar uma tarefa. Cada **Tarefa do servidor** pode ter até um acionador. Cada acionador só pode executar uma **Tarefa do servidor**. Se **Configurar acionador** não estiver selecionado na seção **Básico**, um acionador não é criado. Uma tarefa pode ser criada sem um acionador. Tal tarefa pode ser executada depois manualmente ou um acionador pode ser adicionado mais tarde.

Configurações avançadas - Alternância

Ao configurar a Alternância, você pode definir regras avançadas para o acionador criado. A configuração da alternância é opcional.

Resumo

Todas as opções configuradas são exibidas aqui. Revise as configurações e clique em **Finalizar**.

Em **Tarefas** você pode ver a barra de indicadores de progresso, o ícone de status e os detalhes para cada tarefa criada.

> Você pode executar a tarefa do servidor de Implantação do Agente para implantar o Agente ESET Management nos computadores sincronizados do Active Directory.

Modo de sincronização - Rede MS Windows

> O modo de sincronização de **rede do MS Windows** pode não funcionar devido a requisitos faltando (SMBv1) que são necessários para sua operação bem-sucedida. A ESET vai remover esse modo de sincronização no futuro.

Para criar uma nova Tarefa do servidor, clique em **Tarefas** > **Nova** > **Tarefa do servidor** ou selecione o tipo de tarefa desejado na esquerda e clique em **Novo** > **Tarefa do servidor**.

Básico

Na seção **Básico**, insira informações básicas sobre a tarefa, como **Nome e Descrição (opcional)**. Clique em **Selecionar marcações** para atribuir marcações.
No menu suspenso **Tarefa**, selecione o tipo de tarefa que deseja criar e configurar. Se você selecionou um tipo de tarefa específico antes de criar uma nova tarefa, a **Tarefa** é pré-selecionada com base na sua escolha anterior. **Tarefa** (consulte a lista de todas as Tarefas) define as configurações e o comportamento da tarefa.

Você também pode selecionar a partir das configurações de acionador de tarefa a seguir:

- **Executar tarefa imediatamente depois de concluir** - Selecione isto para que a tarefa seja executada automaticamente depois de clicar em Concluir.
- **Configurar acionador** - Selecione esta opção para ativar a seção Acionador, onde você pode configurar as configurações do acionador.

Para definir o acionador mais tarde, deixe as caixas de seleção desmarcadas.

Configurações

Configurações comuns

Clique em **Selecionar** sob **Nome do grupo estático** - por padrão, o grupo inicial do usuário executando a ação será usado para os computadores sincronizados. Alternativamente, você pode criar um **Novo grupo estático**.

- **Objeto a sincronizar** - Ou **Computadores e grupos** ou **Apenas Computadores**.
- **Processamento de colisão na criação de computador** - Se a sincronização adicionar computadores que já são membros do grupo estático, é possível selecionar um método de solução de conflito:

- **Ignorar** (computadores sincronizados não serão adicionados)
- **Mover** (novos computadores serão movidos a um subgrupo)
- **Duplicar** (um novo computador é criado com o nome modificado)

• **Processamento de extinção de computador** - Se um computador não existir mais, você pode **Remover** este computador ou **Ignorar**.

• **Processamento de extinção de grupo** - Se um grupo não existir mais, você pode **Remover** este grupo ou **Ignorar**.

• **Modo de sincronização** - **Rede MS Windows**

Na seção configurações de sincronização de rede do Microsoft Windows digite as informações a seguir:

• **Grupo de trabalho** - Digite o domínio ou grupo de trabalho que contém os computadores que serão sincronizados. Se não especificar um grupo de trabalho, todos os computadores visíveis serão sincronizados.

• **Login** - Insira as credenciais de login usadas para sincronização na sua rede do Windows.

• **Senha** - Digite a senha usada para fazer login na sua rede Windows.

O Servidor ESET PROTECT é executado sob privilégios de **Serviço de rede** que podem não ser suficientes para ler todos os computadores próximos. Se nenhuma credencial de usuário estiver presente, o servidor lerá todos os computadores próximos das pastas de Rede disponíveis no Windows que foram preenchidos automaticamente pelo sistema operacional. Se as credencias estiverem presentes, elas serão usadas pelo servidor para uma sincronização direta.

O modo de sincronização de **rede do MS Windows** pode não funcionar devido a requisitos faltando (SMBv1) que são necessários para sua operação bem-sucedida. A ESET vai remover esse modo de sincronização no futuro.

Acionador

A seção **Acionador** contém informações sobre os acionadores que devem executar uma tarefa. Cada **Tarefa do servidor** pode ter até um acionador. Cada acionador só pode executar uma **Tarefa do servidor**. Se **Configurar acionador** não estiver selecionado na seção **Básico**, um acionador não é criado. Uma tarefa pode ser criada sem um acionador. Tal tarefa pode ser executada depois manualmente ou um acionador pode ser adicionado mais tarde.

Configurações avançadas - Alternância

Ao configurar a Alternância, você pode definir regras avançadas para o acionador criado. A configuração da alternância é opcional.

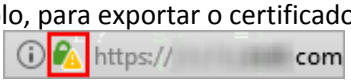
Resumo

Todas as opções configuradas são exibidas aqui. Revise as configurações e clique em **Finalizar**.

Em **Tarefas** você pode ver a barra de indicadores de progresso, o ícone de status e os detalhes para cada tarefa criada.

Modo de sincronização - VMware

É possível sincronizar máquinas virtuais sendo executadas no Servidor VMware vCenter.

> Para executar essa tarefa com sucesso é preciso importar o vCenter CA nos eu Servidor ESET PROTECT. Ele pode ser exportado através do seu navegador da web.
> Por exemplo, para exportar o certificado usando o Firefox clique no ícone de conexão segura na barra de endereços 
>
> e clique em **Exibir detalhes de conexão** > **Mais informações** > **Exibir certificado** > **Detalhes** > **Exportar** > **Salvar**.

Para criar uma nova Tarefa do servidor, clique em **Tarefas** > **Nova** > **Tarefa do servidor** ou selecione o tipo de tarefa desejado na esquerda e clique em **Novo** > **Tarefa do servidor**.

Básico

Na seção **Básico**, insira informações básicas sobre a tarefa, como **Nome e Descrição (opcional)**. Clique em **Selecionar marcações** para atribuir marcações.
No menu suspenso **Tarefa**, selecione o tipo de tarefa que deseja criar e configurar. Se você selecionou um tipo de tarefa específico antes de criar uma nova tarefa, a **Tarefa** é pré-selecionada com base na sua escolha anterior. **Tarefa** (consulte a lista de todas as Tarefas) define as configurações e o comportamento da tarefa.

Você também pode selecionar a partir das configurações de acionador de tarefa a seguir:

- **Executar tarefa imediatamente depois de concluir** - Selecione isto para que a tarefa seja executada automaticamente depois de clicar em Concluir.
- **Configurar acionador** - Selecione esta opção para ativar a seção Acionador, onde você pode configurar as configurações do acionador.

Para definir o acionador mais tarde, deixe as caixas de seleção desmarcadas.

Configurações

Configurações comuns

Clique em **Selecionar** sob **Nome do grupo estático** - por padrão, o grupo inicial do usuário executando a ação será usado para os computadores sincronizados. Alternativamente, você pode criar um **Novo grupo estático**.

- **Objeto a sincronizar** - Ou **Computadores e grupos** ou **Apenas Computadores**.
- **Processamento de colisão na criação de computador** - Se a sincronização adicionar computadores que já são membros do grupo estático, é possível selecionar um método de solução de conflito:
  - **Ignorar** (computadores sincronizados não serão adicionados)
  - **Mover** (novos computadores serão movidos a um subgrupo)

- **Duplicar** (um novo computador é criado com o nome modificado)

- **Processamento de extinção de computador** - Se um computador não existir mais, você pode **Remover** este computador ou **Ignorar**.

- **Processamento de extinção de grupo** - Se um grupo não existir mais, você pode **Remover** este grupo ou **Ignorar**.

- **Modo de sincronização** - **VMware**

Configurações de conexão do servidor

- **Servidor** - Digite o nome DNS ou endereço IP do servidor VMWare vCenter. O endereço deve ser exatamente o mesmo que o valor **CN** do vCenter CA importado. Esse valor pode ser encontrado na coluna **Assunto** da janela **Mais** > **Autoridades de certificação**.

- **Login** - Digite as credenciais de login para o servidor VMware vCenter.

- **Senha** - Digite a senha usada para fazer login no seu Servidor VMware vCenter.

Configurações de sincronização

- **Visualização de estrutura** - Selecione o tipo de visualização de estrutura, ou **Pastas** ou **Pool de recursos**.

- **Caminho de estrutura** - Clique em **Procurare navegue até a** pasta que deseja sincronizar. Se o campo for deixado vazio, toda a estrutura será sincronizada.

- **Visualização de computador** - Selecione se deseja exibir computadores por **Nome**, **Nome de host** ou **Endereço IP depois da sincronização**.

Se você receber o erro: `Server not found in Kerberos database` depois de clicar em **Procurar**, use o AD FQDN do servidor em vez do endereço IP.

Acionador

A seção **Acionador** contém informações sobre os acionadores que devem executar uma tarefa. Cada **Tarefa do servidor** pode ter até um acionador. Cada acionador só pode executar uma **Tarefa do servidor**. Se **Configurar acionador** não estiver selecionado na seção **Básico**, um acionador não é criado. Uma tarefa pode ser criada sem um acionador. Tal tarefa pode ser executada depois manualmente ou um acionador pode ser adicionado mais tarde.

Configurações avançadas - Alternância

Ao configurar a Alternância, você pode definir regras avançadas para o acionador criado. A configuração da alternância é opcional.

Resumo

Todas as opções configuradas são exibidas aqui. Revise as configurações e clique em **Finalizar**.

Em **Tarefas** você pode ver a barra de indicadores de progresso, o ícone de status e os detalhes para cada tarefa criada.

Sincronização de grupo estático - Computadores Linux

Um computador Linux colocado em um domínio Windows não exibe nenhum texto no Active Directory de Usuários e Computadores (ADUC) em Propriedades do computador, portanto é preciso inserir o texto manualmente.

Verifique os Pré-requisitos de servidor e os pré-requisitos a seguir:

- Os computadores Linux estão no Active Directory.
- O controlador de domínio tem um servidor DNS instalado.
- Editar ADSI está desinstalado.

1. Abra um prompt de comando e execute `adsiedit.msc`
2. Vá para **Ação** > **Conectar a**. A janela de configurações de conexão será exibida.
3. Clique em **Selecionar um contexto de nomeação bem conhecido**.
4. Abra a caixa de combo abaixo e selecione o contexto de nomeação **Padrão**.
5. Clique em **OK** - o valor ADSI na esquerda deve ser o nome do seu controlador de domínio - Contexto de nomeação padrão (seu controlador de domínio).
6. Clique no valor **ADSI** e expanda seu subgrupo.
7. Clique no **subgrupo** e vá para o CN (Nome comum) ou OU (Unidade organizacional) onde os computadores Linux são exibidos.
8. Clique no **nome de host** do computador Linux e selecione **Propriedades** do menu de contexto. Vá para o parâmetro **dNSHostName** e clique em **Editar**.
9. Altere o valor **not set** para um texto válido (por exemplo, `ubuntu.TEST`).
10. Clique em **OK** > **OK**. Abra **ADUC** e selecione as **propriedades** do computador Linux - o novo texto deve ser exibido aqui.

Sincronização de usuário

Esta Tarefa do servidor sincroniza as informações de Usuários e Grupos de Usuários de uma fonte, como o Active Directory, parâmetros LDAP, etc.

Para criar uma nova Tarefa do servidor, clique em **Tarefas** > **Nova** > **Tarefa do servidor** ou selecione o tipo de tarefa desejado na esquerda e clique em **Novo** > **Tarefa do servidor**.

Básico

Na seção **Básico**, insira informações básicas sobre a tarefa, como **Nome e Descrição (opcional)**. Clique em **Selecionar marcações** para atribuir marcações.
No menu suspenso **Tarefa**, selecione o tipo de tarefa que deseja criar e configurar. Se você selecionou um tipo de tarefa específico antes de criar uma nova tarefa, a **Tarefa** é pré-selecionada com base na sua escolha anterior. **Tarefa** (consulte a lista de todas as Tarefas) define as configurações e o comportamento da tarefa.

Você também pode selecionar a partir das configurações de acionador de tarefa a seguir:

- **Executar tarefa imediatamente depois de concluir** - Selecione isto para que a tarefa seja executada automaticamente depois de clicar em Concluir.
- **Configurar acionador** - Selecione esta opção para ativar a seção Acionador, onde você pode configurar as configurações do acionador.

Para definir o acionador mais tarde, deixe as caixas de seleção desmarcadas.

Configurações

Configurações comuns

Nome de grupo de usuário – por padrão a raiz dos usuários sincronizados será usada (por padrão, ela é o grupo **Todos**). Alternativamente, você pode criar um novo grupo de usuário.

Lidando com colisão de criação de usuário - dois tipos de conflitos que podem ocorrer:

- Há dois usuários com o mesmo nome no mesmo grupo.
- Há um usuário existente com o mesmo SID (em qualquer lugar no sistema).

Você pode configurar o lidar com colisão para:

- **Ignorar** - o usuário não é adicionado ao ESET PROTECT durante a sincronização com o Active Directory.
- **Substituir** - usuário existente no ESET PROTECT é substituído pelo usuário do Active Directory, em um caso de conflito SID o usuário existente no ESET PROTECT é removido da sua localização anterior (mesmo se o usuário estava em um grupo diferente).

Processamento de extinção de usuário - Se um usuário não existir mais, você pode **Remover** este usuário ou **Ignorar**.

Processamento de extinção de grupo de usuário - Se um grupo de usuário não existir mais, você pode **Remover** este grupo de usuário ou **Ignorar**.

> Se você usa atributos personalizados para um usuário defina **Processamento de colisão na criação de usuário** como **Ignorar**. Caso contrário o usuário (e todos os detalhes) serão substituídos por dados do Active Directory, perdendo atributos personalizados. Se quiser substituir o usuário, altere o **Processamento de extinção de usuário** para **Ignorar**.

Configurações de conexão do servidor

- **Servidor** - Digite o nome do servidor ou endereço IP do seu controlador de domínio.
- **Efetuar login** - Digite o nome de usuário para seu controlador de domínio no formato a seguir:
  - `DOMAIN\username` (Servidor ESET PROTECT em execução no Windows)
  - `username@FULL.DOMAIN.NAME` ou `username` (Servidor ESET PROTECT em execução no Linux).

> Não se esqueça de digitar o domínio em letras maiúsculas. Esta formatação é necessária para fazer a autenticação adequada de consultas no servidor do Active Directory.

- **Senha** - Digite a senha usada para fazer login no seu controlador de domínio.

> O Servidor ESET PROTECT no Windows usa o protocolo LDAPS criptografado (LDAP sobre SSL) por padrão para todas as conexões com o Active Directory (AD). Você também pode Configurar LDAPS na máquina virtual ESET PROTECT.
> Para uma conexão AD bem-sucedida no LDAPS, configure o seguinte:
> 1. O controlador de domínio deve ter um certificado de máquina instalado. Para emitir um certificado para seu controlador de domínio, siga as etapas abaixo:
> a)Abra o **Gerenciador de servidor**, clique em **Gerenciar** > **Adicionar funções e recursos** e instale os **Serviços de certificados do Active Directory** > **Autoridade de certificação**. Uma nova Autoridade de certificação será criada em **Autoridades de certificação raiz confiáveis**.
> b)Navegue até **Início** > digite `certmgr.msc` e pressione **Enter** para executar o snap-in do Console de Gerenciamento da Microsoft **Certificados** > **Certificados – computador local** > **Pessoal** > clique com o botão direito na janela vazia > **Todas as tarefas** > **Solicitar novo certificado** > função **Inscrever controlador de domínio**.
> c)Verifique se o certificado emitido contém o FQDN do controlador de domínio.
> d)No seu servidor ESMC, importe a CA gerada para o depósito de certificados (usando a ferramenta `certmgr.msc`) para a pasta de CAs confiáveis.
>
> 2. Ao fornecer as configurações de conexão ao servidor AD, digite o FQDN do controlador de domínio (conforme fornecido no certificado do controlador de domínio) no campo **Servidor** ou **Host**. O endereço IP não é mais suficiente para o LDAPS.

Para ativar o fallback para o protocolo LDAP, selecione a caixa de seleção **Usar LDAP em vez do Active Directory** e insira os atributos específicos para combinar com o seu servidor. Alternativamente, selecione **Pré-seleção** clicando em **Selecionar** e os atributos serão preenchidos automaticamente:

- **Active Directory**
- **Mac OS X Server Open Directory (nomes de host de computador)**
- **OpenLDAP com registros de computador Samba** - configurando os parâmetros do nome DNS no Active Directory.

Configurações de sincronização

- **Nome diferenciado** - Caminho (Nome diferenciado) para o nó na árvore do Active Directory. Deixar essa

opção vazia vai sincronizar toda a árvore AD. Clique em **Procurar** ao lado de **Nome diferenciado**. Sua árvore do Active Directory será exibida. Selecione a entrada de cima para sincronizar todos os grupos com o ESET PROTECT, ou selecione somente os grupos específicos que você deseja adicionar. Apenas computadores e Unidades organizacionais são sincronizados. Clique em **OK** quando tiver terminado.

> **Determinar o Nome diferenciado**
> 1.Abra o aplicativo **Usuários e computadores do Active Directory**.
> 2.Clique em **Exibir** e selecione **Recursos avançados**.
> 3.Clique com o botão direito do mouse no domínio > clique em **Propriedades** > selecione a guia **Editor de atributo**.
> 4.Localize **distinguishedName** a linha. Ele deve se parecer com este exemplo: `DC=ncop,DC=local`.

- **Grupo de usuário e atributos de usuário** - Os atributos padrão de um usuário são específicos ao diretório ao qual o usuário pertence. Se você quiser sincronizar os atributos do Active Directory, selecione o parâmetro AD do menu suspenso nos campos adequados ou digite um nome personalizado para o atributo. Ao lado de cada campo sincronizado está um espaço reservado ESET PROTECT (por exemplo: `${display_name}`) que vai representar este atributo em certas configurações de política ESET PROTECT.

- **Atributos avançados de usuário** - Se quiser usar atributos personalizados avançados selecione **Adicionar novo**. Estes campos vão herdar as informações do usuário, que podem ser tratadas no editor de política para iOS MDM como um espaço reservado.

> Se você receber o erro: `Server not found in Kerberos database` depois de clicar em **Procurar**, use o AD FQDN do servidor em vez do endereço IP.

Acionador

A seção **Acionador** contém informações sobre os acionadores que devem executar uma tarefa. Cada **Tarefa do servidor** pode ter até um acionador. Cada acionador só pode executar uma **Tarefa do servidor**. Se **Configurar acionador** não estiver selecionado na seção **Básico**, um acionador não é criado. Uma tarefa pode ser criada sem um acionador. Tal tarefa pode ser executada depois manualmente ou um acionador pode ser adicionado mais tarde.

Configurações avançadas - Alternância

Ao configurar a Alternância, você pode definir regras avançadas para o acionador criado. A configuração da alternância é opcional.

Resumo

Todas as opções configuradas são exibidas aqui. Revise as configurações e clique em **Finalizar**.

Em **Tarefas** você pode ver a barra de indicadores de progresso, o ícone de status e os detalhes para cada tarefa criada.

Tipos de acionadores de tarefas

Os acionadores são essencialmente sensores que reagem a certos eventos de maneira predefinida. Eles são usados para executar a tarefa para a qual são atribuídos. Eles podem ser ativados pela Agenda (eventos com

tempo) ou quando ocorrer um determinado evento do sistema.

> Não é possível reutilizar um acionador. Cada tarefa deve ser acionada com um acionador separado. Cada acionador só pode executar uma tarefa.

O acionador não executa tarefas recém-atribuídas imediatamente (exceto com o acionador “assim que for possível”) - a tarefa é executada assim que o acionador é disparado. A sensibilidade do acionador em relação a eventos pode ser reduzida ainda mais usando a alternância.

Tipos de acionadores:

- **Assim que possível** – Disponível apenas para Tarefas do cliente. A tarefa será executada assim que você clicar em **Concluir**. O valor da **Data de expiração** especifica a data depois da qual a tarefa não será mais executada.

Agendado

O acionador agendado vai executar a tarefa com base nas configurações de data e hora. As tarefas podem ser agendadas para serem **executadas uma vez**, de forma repetitiva ou na expressão CRON.

- **Agendar uma vez** - Este acionador é acionado uma vez na hora agendada. Ele pode ser atrasado por um intervalo aleatório.

- **Diariamente** - Esse acionador é acionado todos os dias selecionados. Você pode definir o início e o final do intervalo. Por exemplo, você pode executar uma tarefa por dez fins de semana consecutivos.

- **Semanalmente** - Esse acionador é acionado em um dia da semana selecionado. Por exemplo, executar uma tarefa toda a segunda-feira e sexta-feira entre 1 de julho e 31 de agosto.

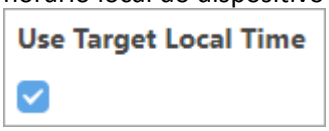
- **Mensalmente** - Este acionador é invocado em dias selecionados na semana selecionada de um mês, pelo período de tempo selecionado. O valor **Repetir em** define o dia da semana selecionado do mês (por exemplo, a segunda segunda-feira) a tarefa deve ser executada.

- **Anualmente** - Esse acionador é iniciado a cada ano (ou mais anos, se for configurado dessa forma) na data de **início** especificada.

> A configuração de **Intervalo de atraso aleatório** está disponível para acionadores do tipo Agendado. Ele define o intervalo de atraso máximo para a execução da tarefa. A aleatorização pode impedir a sobrecarga do servidor.

> Se *John* definir a **Tarefa** para ser acionada **Semanalmente** na *Segunda-feira* e **Iniciar** em *10 fev 2017 8:00:00*, com o **Intervalo de adiamento aleatório** definido como *1 hora* e **final até definido para** *6 abr 2017 00:00:00,* a tarefa seria executada com um adiamento aleatório de uma hora entre as 8:00 e 9:00 todas as segundas-feiras até a data de término especificada.

- Selecione a caixa de seleção **Invocar imediatamente se evento perdido** para executar a tarefa imediatamente se não for executada na hora definida.
- Ao configurar um acionador, o fuso horário do Web Console ESET PROTECT é usado por padrão. Alternativamente, você pode selecionar a caixa de seleção **Usar horário local do destino** para usar o fuso horário local do dispositivo de destino em vez do fuso horário do Console ESET PROTECT para o acionador.



Grupo dinâmico

Os acionadores de Grupo dinâmico estão disponíveis apenas para Tarefas do servidor:

- **Membros do grupo dinâmico alterados** - Este acionador é invocado quando o conteúdo do Grupo dinâmico for alterado. Por exemplo, se os clientes entrarem ou saírem de um Grupo dinâmico específico.

- **Tamanho do grupo dinâmico alterado de acordo com o limite** - Este acionador é invocado quando o número de clientes em um grupo dinâmico se torna superior ou inferior ao limite especificado. Por exemplo, se mais de 100 computadores estiverem em um determinado grupo.

- **Tamanho do grupo dinâmico alterado ao longo do período** - Este acionador é invocado quando o número de clientes em um grupo dinâmico é alterado em um período de tempo determinado. Por exemplo, se o número de computadores em um grupo determinado aumentar 10% em uma hora.

- **Tamanho do grupo dinâmico alterado de acordo com o grupo comparado** - Este acionador é invocado quando o número de clientes em um Grupo Dinâmico observado for alterado de acordo com um grupo de comparação (estático ou dinâmico). Por exemplo, se mais de 10% de todos os computadores estiverem infectadas (o grupo **Todos** em comparação com o grupo **Infectado**).

Outras

- **Servidor iniciado** – Disponível apenas para Tarefas do servidor. É chamado quando o servidor é iniciado. Por exemplo, este acionador é usado para a tarefa de Sincronização de Grupo estático.

- **Acionador de grupo dinâmico ingressado** – Disponível apenas para Tarefas do cliente. Esse acionador é chamado toda vez que um dispositivo entra no grupo dinâmico.

O **Acionador de grupo dinâmico ingressado** está disponível somente se um grupo dinâmico estiver selecionado na seção de Destino. O acionador vai executar a tarefa apenas em dispositivos que ingressam no grupo dinâmico depois do acionador ser criado. Para todos os dispositivos que já estão no grupo dinâmico, você terá que executar a tarefa manualmente.

- **Acionador de registro de evento** - Esse acionador é acionado quando um determinado evento ocorre em relatórios. Por exemplo, se há uma detecção no **relatório do** Escaneamento. Esse tipo de alternância fornece um conjunto de configurações especiais nas Configurações de alternância.

- **Expressão CRON** - Esse acionados é chamado em uma determinada data e hora.

Intervalo de Expressão CRON

Uma expressão CRON é usada para configurar instâncias específicas de um acionador. Principalmente para o acionamento repetitivo agendado. É uma string composta de 6 ou 7 campos que representam valores individuais da agenda. Esses campos são separados por um espaço e contém qualquer um dos valores permitidos com várias combinações.

A expressão CRON pode ser tão simples quanto: `* * * * ? *` ou mais complexa, como: `0/5 14,18,3-39,52 * ? JAN,MAR,SEP MON-FRI 2012-2020`

Lista de valores que você pode usar na expressão CRON:

Nome	Requerido	Valor	Caracteres especiais permitidos
Segundos	Sim	0-59	, - * / R
Minutos	Sim	0-59	, - * / R
Horas	Sim	0-23	, - * / R
Dia do mês	Sim	1-31	, - * / ? L W
Mês	Sim	1-12 ou JAN-DEC	, - */
Dia da semana	Sim	0-6 ou SUN-SAT	, - / ? L #
Ano	Sim	1970-2099	, - * /

A sintaxe da expressão CRON é a seguinte:

```
┌──────────── segundos (0-59)
│ ┌────────── minutos (0-59)
│ │ ┌──────── horas (0-23)
│ │ │ ┌────── Dia do mês (1 - 31)
│ │ │ │ ┌──── mês (1 a 12 ou JAN-DEC)
│ │ │ │ │ ┌── Dia da semana (0 - 6 ou SUNSAT)(por exemplo, 0 é o mesmo que SUN)
│ │ │ │ │ │ ┌ Ano
│ │ │ │ │ │ │
* * * * * ? *
```

- O 0 0 0 significa meia-noite (segundos, minutos, horas).
- Use ? quando um valor não pode ser definido porque foi definido em outro campo (dia do mês ou dia da semana).
- O * significa todos (segundos, minutos, horas, dia do mês, mês, dia da semana, ano).
- O SUN significa no domingo.

> Os nomes dos meses e dias da semana não diferenciam maiúsculas e minúsculas. Por exemplo, MON é igual a mon, ou JAN é igual a jan.

Caracteres especiais:

Vírgula (,)

Vírgulas são usadas para separar os itens de uma lista. Por exemplo, usar "MON,WED,FRI" no 6º campo (dia da semana) dignifica segundas, quartas e sextas-feiras.

Hífen (-)

Define intervalos. Por exemplo, 2012-2020 indica cada ano entre 2012 e 2020, inclusive.

Coringa (*)

Usado para selecionar todos os valores possíveis dentro de um campo. Por exemplo, * no campo minuto significa a cada minuto. O curinga não pode ser usado no campo dia da semana.

Ponto de interrogação (?)

Ao escolher um dia específico, você pode especificar um dia do mês ou dia da semana. Não é possível especificar ambos. Se você especificar dia do mês, você deve usar ? para dia da semana e vice versa. Por exemplo, se quiser que o acionador seja acionado em um determinado dia do mês (digamos que no dia 10), mas se não faz diferença qual dia da semana vai ser, coloque 10 no campo dia do mês e ? no campo dia da semana.

Hash (#)

Usado para especificar "o º" dia do mês. Por exemplo, o valor de 4#3 no campo dia da semana significa a terceira quinta-feira do mês (dia 4 = quinta-feira e #3 = a 3ª quinta-feira do mês). Se você especificar #5 e não houver um 5º do dia da semana determinado no mês, o acionador não será acionado naquele mês.

Barra (/)

Descreve aumentos de um intervalo. Por exemplo 3-59/15 no 2º campo (minutos) indica o terceiro minuto da hora e a cada 15 minutos depois disso.

Último (L)

Quando usado no campo dia da semana, ele permite que você especifique construções como a última sexta-feira (5L) de um determinado mês. No campo dia do mês, ele especifica o último dia do mês. Por exemplo, dia 31 para janeiro, dia 28 para fevereiro em anos que não são bissextos.

Dia da semana (W)

O caractere W é permitido para o campo dia do mês. Este caractere é usado para especificar o dia da semana (segunda a sexta-feira) mais próximo de um determinado dia. Por exemplo, se você especificar 15W como o valor para o campo dia do mês, o significado é o dia de semana mais próximo do dia 15 do mês. Então, se o dia 15 for um sábado, o acionador é acionado na sexta-feira, dia 14. Se o dia 15 for um domingo, o acionador é acionado na segunda-feira, dia 16. Porém, se você especificar 1W como o valor para o dia do mês, e o dia 1º for um sábado, o acionador é acionado na segunda-feira, dia 3, pois ele não ignora o limite dos dias de um mês.

Os caracteres L e W também podem ser combinados no campo dia do mês para resultar em LW, que é traduzido como último dia da semana do mês.

Aleatório (R)

O R é um caractere especial de expressão ESET PROTECT CRON que permite a você especificar momentos aleatórios no tempo. Por exemplo, o acionador R 0 0 * * ? * é acionado todo dia as 00:00 mas em um segundo aleatório (0-59).

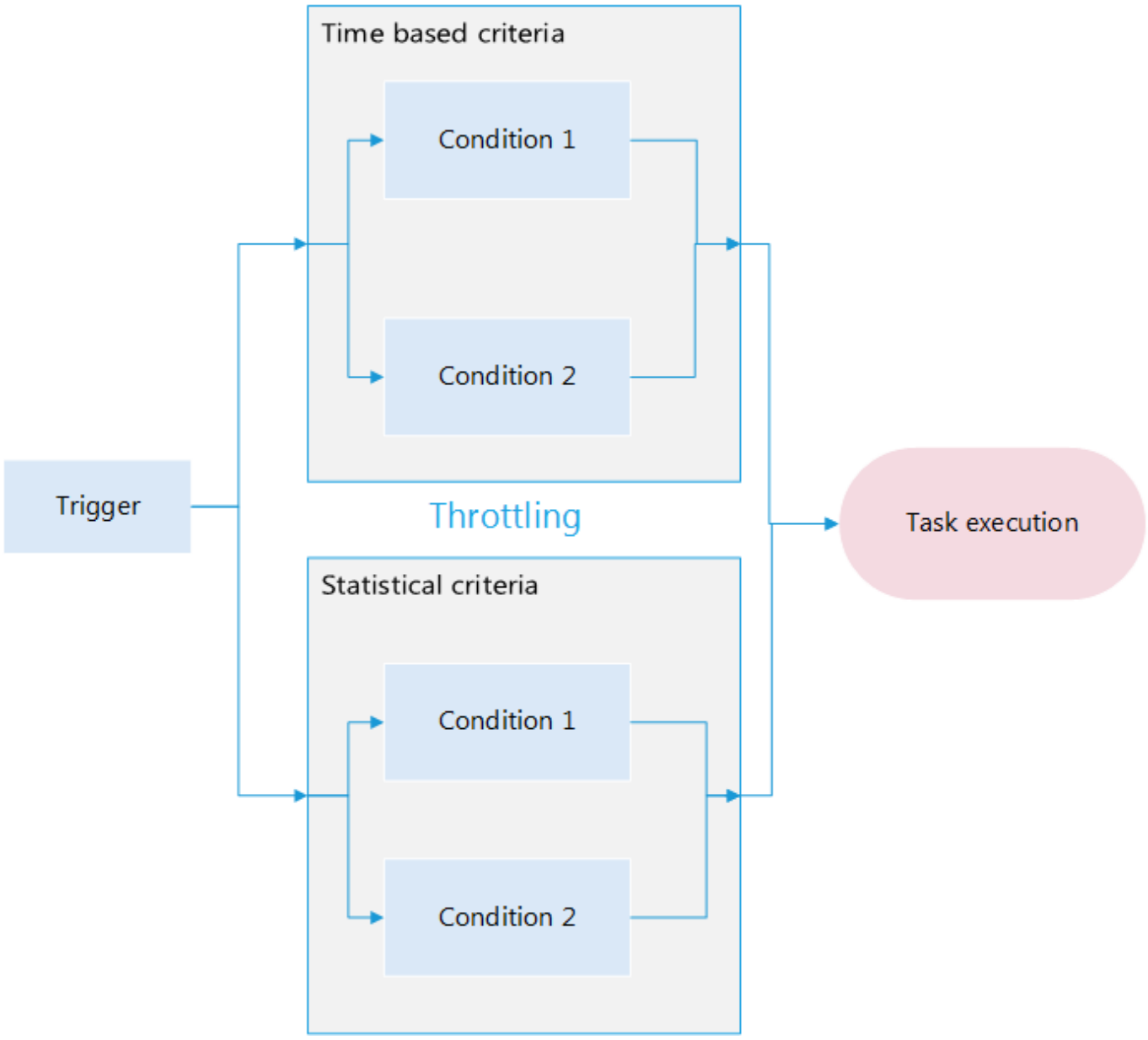
Recomendamos usar momentos no tempo aleatórios para impedir que todos os Agentes ESET Management se conectem ao mesmo tempo ao seu ESET PROTECT. Servidor.

Exemplos reais que ilustram algumas variações da Expressão CRON:

Expressão CRON	Significado
`0 0 12 * * ? *`	Acionar as 12:00 PM (meio dia) todos os dias.
`R 0 0 * * ? *`	Aciona as 00:00 mas em um segundo aleatório (0-59) todos os dias.
`R R R 15W * ? *`	Aciona no dia 15 de cada mês em uma hora aleatória (segundos, minutos, horas). Se o dia 15 for um sábado, o acionador é acionado na sexta-feira, dia 14. Se o dia 15 for um domingo, o acionador é acionado na segunda-feira, dia 16.
`0 15 10 * * ? 2016`	Acionar as 10:15 AM todos os dias durante o ano de 2016.
`0 * 14 * * ? *`	Iniciar a cada minuto a partir das 2:00 PM e terminando às 2:59 PM, todos os dias.
`0 0/5 14 * * ? *`	Acionar a cada 5 minutos a partir das 2:00 PM e terminando às 2:55 PM, todos os dias.
`0 0/5 14,18 * * ? *`	Acionar a cada 5 minutos a partir das 2:00 PM e terminando às 2:55 PM, e iniciar a cada 5 minutos a partir das 6:00 PM e terminando às 6:55 PM, todos os dias.
`0 0-5 14 * * ? *`	Iniciar a cada minuto a partir das 2:00 PM e terminando às 2:05 PM, todos os dias.
`0 10,44 14 ? 3 WED *`	Iniciar às 2:10 PM e às 2:44 PM a cada quarta-feira em março.
`0 15 10 ? * MON-FRI *`	Acionar às 10:15 AM todos os dias da semana (segunda-feira, terça-feira, quarta-feira, quinta-feira e sexta-feira).
`0 15 10 15 * ? *`	Acionar às 10:15 AM no dia 15 de cada mês.
`0 15 10 ? * 5L *`	Acionar às 10:15 AM na última sexta-feira de cada mês.
`0 15 10 ? * 5L 2016-2020`	Acionar às 10:15 AM em cada última sexta-feira de cada mês durante os anos de 2016 a 2020, inclusive.
`0 15 10 ? * 5#3 *`	Acionar às 10:15 AM na terceira sexta-feira de cada mês.
`0 0 * * * ? *`	Acionar a cada hora, todos os dias.

Configurações avançadas - Alternância

A alternância é usada para restringir uma tarefa de ser executada. A alternância normalmente é usada quando uma tarefa é acionada por um evento recorrente com frequência. Sob certas circunstâncias, a Alternância pode impedir que um acionador seja ativado. Cada vez que o acionador é acionado, ele é avaliado de acordo com o esquema abaixo. Apenas os acionadores que estão de acordo com condições especificadas podem então fazer a tarefa ser executada. Se nenhuma condição de alternância for definida, todos os eventos do acionador vão ser executados na tarefa.



Há três tipos de condições para Alternância:

- **Critérios com base em tempo**
- **Critérios estatísticos**
- **Critérios de registro de evento**

Para uma tarefa a ser executada:

- Ele tem que ser aprovado em todos os tipos de condições
- As condições devem ser definidas, se uma condição estiver vazia ela será omitida
- Todas as condições baseadas em tempo devem ser aprovadas, já que são avaliadas com o operador AND
- Todas as condições estatísticas avaliadas com o operador AND devem ser aprovadas, pelo menos uma condição estatística com o operador OR deve ser aprovada
- Condições estatísticas e baseadas em tempo devem ser aprovadas juntas, já que são avaliadas com o

operador AND - apenas depois disso a tarefa é executada

Se qualquer uma das condições definidas for realizada, as informações empilhadas de todos os observadores são redefinidas (a contagem começa de 0). Isso vale para condições baseadas em tempo e também para condições estatísticas. Essas informações também são reiniciadas se o Agente ou ESET PROTECT Servidor é reiniciado. Todas as modificações feitas em um acionador redefinem seu status. Recomendamos usar apenas uma condição estatística e várias condições baseadas em tempo. Várias condições estatísticas podem causar uma complicação desnecessária e podem alterar os resultados de acionador.

Pré-configurar

Existem três pré-configurações disponíveis. Quando você seleciona uma pré-configuração, suas configurações atuais de alternância são apagadas e substituídas pelos valores pré-definidos. Esses valores podem ser ainda mais modificador e usados, mas não é possível criar uma nova pré-configuração.

Critérios baseados em tempo

Período de tempo (T2) - Permite o acionamento uma vez durante o período de tempo especificado. Se, por exemplo, isso for configurado para dez segundos e durante esse tempo dez invocações acontecerem, apenas a primeira iria acionar o evento.

> É preciso configurar o throttling com critérios baseados em tempo para restringir a execução da tarefa a no máximo uma vez a cada 1 minutos (um ícone de cadeado indica a restrição):
> • Tarefas do servidor (incluindo a geração de relatório) – todos os tipos de acionador.
> • Tarefas do cliente – tipos de acionador **agendado** e **expressão CRON***.
> Se você atualizou do ESET PROTECT 8.x ou 9.x, 1 minutos serão aplicados automaticamente a todas as tarefas existentes com o período de tempo definido para menos de 1 minutos.
> O período de tempo mínimo de 15 minutos não se aplica às notificações.

Agendar (T1) - Permite o acionamento apenas dentro do intervalo de tempo definido. Clique em **Adicionar período** e uma janela pop-up é exibida. Defina uma **Duração de intervalo** em unidades de tempo selecionadas. Selecione uma opção da lista de **Recorrência** e preencha os campos, que mudam de acordo com a recorrência selecionada. Também é possível definir a recorrência na forma de uma Expressão CRON. Clique em **OK** para salvar o intervalo. É possível adicionar vários intervalos de tempo na lista, eles serão organizados de forma cronológica.

Todas as condições configuradas devem ser cumpridas para acionar a tarefa.

Critérios estatísticos

Condição - Condições estatísticas podem ser combinadas usando:

- **Enviar notificação quando todos os critérios estatísticos forem cumpridos** - **E** o operador lógico é usado para avaliação
- **Enviar notificação quando pelo menos um critério estatístico for cumprido** - **OU** o operador lógico é usado para avaliação

Número de ocorrências (S1) - Permite apenas um acionamento a cada x ocorrências. Por exemplo, se o valor for dez, apenas o décimo acionamento vai contar.

Número de ocorrências em um período de tempo

Número de ocorrências (S2) – permite o acionamento apenas dentro de um período de tempo definido. Isso vai definir a frequência mínima de eventos para acionar a tarefa. Por exemplo, você pode usar essa configuração para permitir a execução da tarefa se o evento for detectado 10x em uma hora. Acionar o acionador provoca uma redefinição do contador.

Período de tempo - Define o período de tempo para a opção descrita acima.

Uma terceira condição estatística está disponível apenas para certos tipos de acionador. Veja o **Acionador** > **Tipo de acionador** > **Acionador de registro de evento**.

Critérios de registro de evento

Esses critérios são avaliados pelo ESET PROTECT como critérios estatísticos de terceiros (S3). O operador de **Aplicação de critérios estatísticos** (AND / OR) é aplicado para avaliar todas as três condições estatísticas juntas. Recomendamos usar os critérios do relatório de eventos em combinação com a tarefa **Gerar relatório**. Todos os três campos são necessários para os critérios funcionarem. O buffer de símbolos é redefinido se o acionador for disparado e se já houver um símbolo no buffer.

Condição - Isso define quais eventos ou conjuntos de eventos são acionar a condição. As opções disponíveis são:

- **Recebido em sequência** - O número especificado de eventos que devem acontecer em sequência. Esses eventos devem ser distintivos.
- **Recebido desde última execução de acionador** - A condição é acionada quando o número selecionado de eventos distintivos for alcançado desde a última execução da tarefa.

Número de ocorrências - Digite o número de eventos distintos com o símbolo selecionado para executar a tarefa.

Símbolo - De acordo com o **Tipo de relatório**, que é definido no menu **Acionador**, você pode escolher um símbolo no relatório que você poderá buscar. Clique em **Selecionar** para exibir o menu. Você pode remover o símbolo selecionado clicando em **Remover**.

> Quando estiverem em uso com uma Tarefa do servidor, todos os computadores cliente são considerados. É improvável que você vá receber mais símbolos distintos seguidos. Use a configuração **Recebido em sequência** apenas para casos razoáveis. Um valor faltando (N/A) é considerado como “não único” e, portanto, o buffer é redefinido neste ponto.

Propriedades adicionais

Como afirmado acima, nem todos os eventos ativarão um acionador. Ações realizadas para eventos que não ativam podem ser:

- Se houver mais de um evento ignorado, agrupar os últimos **N** eventos em um (armazenar dados de marcações suprimidas) [**N** <= 100]
- Para **N** == 0, apenas o último evento é processado (**N** significa comprimento do histórico, o último evento sempre é processado)

• Todos os eventos sem ativação são mesclados (mesclando a última marcação com **N** marcações de histórico)

Se o acionador for acionado com muita frequência ou se quiser ser notificado com menos frequência, considere as sugestões a seguir:

• Se o usuário quiser reagir apenas se houver mais eventos, e não um único, consulte a condição estatística S1

• Se o acionador tiver que ser iniciado apenas quando um agrupamento de eventos ocorrer, siga a condição estatística S2

• Quando eventos com valores indesejados devem ser ignorados, consulte a condição estatística S3

• Quando eventos fora dos horários relevantes (por exemplo, do horário comercial) tiverem que ser ignorados, consulte a condição baseada em tempo T1

• Para definir um tempo mínimo entre disparos de acionador, use a condição baseada em tempo T2

> As condições também podem ser combinadas para formar cenários de alternância mais complexos. Consulte os exemplos de alternância para mais detalhes.

Exemplos de alternância

Exemplos de alternância explicam como as condições de alternância (T1, T2, S1, S2, S3) são combinadas e avaliadas.

> “Marcação” significa um impulso para o acionador. "T" significa os critérios baseados em tempo, "S" significa os critérios estatísticos. "S3" significa critérios de registro de evento.

S1: Critério para ocorrências (permitir a cada terceira marcação)

Hora	00	01	02	03	04	05	06	Acionador é modificado	07	08	09	10	11	12	13	14	15
Marcações	x	x	x	x	x	x	x		x	x		x	x		x		x
S1			1			1						1					1

S2: Critério de ocorrências dentro do tempo (permitir se três marcações ocorrerem dentro de quatro segundos)

Hora	00	01	02	03	04	05	06	Acionador é modificado	07	08	09	10	11	12	13
Marcações	x		x	x	x	x			x		x		x	x	x
S2				1										1	

S3: Critério para valores de símbolos únicos (permitir se três valores únicos estiverem em uma fileira)

Hora	00	01	02	03	04	05	06	Acionador é modificado	07	08	09	10	11	12	13
Valor	A	B	B	C	D	G	H		J	K	n/d	L	M	N	N
S3					1									1	

S3: Critério para valores de símbolos únicos (permitir se três valores únicos existirem desde a última marcação)

Hora	00	01	02	03	04	05	06	07	Acionador é modificado	08	09	10	11	12	13	14
Valor	A	B	B	C	D	G	H	Eu		J	K	n/d	L	M	N	N
S3				1			1						1			

T1: Permitir uma marcação em determinados intervalos de tempo (permitir todos os dias a partir das 08:10, duração de 60 segundos)

Hora	8:09:50	8:09:59	8:10:00	8:10:01	Acionador é modificado	8:10:59	8:11:00	8:11:01
Marcações	x	x	x	x		x	x	x
T1			1	1		1		

Este critério não tem estado, portanto as alterações de acionador não têm efeito sobre os resultados.

T2: Permitir uma única marcação em um intervalo de tempo (permitir no máximo uma vez a cada cinco segundos)

Hora	00	01	02	03	04	05	06	Acionador é modificado	07	08	09	10	11	12	13
Marcações	x		x	x	x	x			x		x		x	x	x
T2	1					1			1					1	

Combinação S1 + S2

- S1: a cada quinta marcação
- S2: três marcações dentro de quatro segundos

Hora	00	01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16
Marcações	x	x	x	x	x		x	x	x			x		x	x		
S1															1		
S2			1				1								1		
Resultado			1				1								1		

O resultado é listado como: S1 (lógico or) S2

Combinação S1 + T1

- S1: Permitir a cada terceira marcação
- T1: Permitir todos os dias a partir das 8:08, duração de 60 segundos

Hora	8:07:50	8:07:51	8:07:52	8:07:53	8:08:10	8:08:11	8:08:19	8:08:54	8:08:55	8:09:01
Marcações	x	x	x	x	x	x	x	x	x	x
S1			1			1			1	
T1					1	1	1	1	1	
Resultado						1			1	

O resultado é listado como: S1 (lógico and) T1

Combinação S2 + T1

- S2: três marcações dentro de dez segundos
- T1: Permitir todos os dias a partir das 8:08, por uma duração de 60 segundos

Hora	8:07:50	8:07:51	8:07:52	8:07:53	8:08:10	8:08:11	8:08:19	8:08:54	8:08:55	8:09:01
Marcações	x	x	x	x	x	x	x	x	x	x
S2			1	1			1			1
T1					1	1	1	1	1	
Resultado							1			

O resultado é listado como: S2 (lógico and) T1.

Observe que o estado do S2 é redefinido apenas quando o resultado global é 1.

Combinação S2 + T2

- S2: três marcações dentro de dez segundos
- T2: Permitir no máximo uma vez a cada 20 segundos

Hora	00	01	02	03	04	05	06	07	...	16	17	18	19	20	21	22	23	24
Marcações	x	x	x	x	x	x	x	x		x	x	x	x	x	x	x	x	x
S2			1			1	1	1				1	1	1	1	1		
T2	1	1	1													1		
Resultado			1													1		

O resultado é listado como: S2 (lógico and) T2.

Observe que o estado do S2 é redefinido apenas quando o resultado global é 1.

Instaladores

Esta seção mostra como criar pacotes do instalador do Agente para implantar o Agente ESET Management em computadores cliente. Os pacotes do instalador são salvos no Console da Web ESET PROTECT e você pode editar e fazer download deles novamente quando necessário.

Clique em **Instaladores** > **Criar Instalador** e selecione o sistema operacional.

Windows

- O pacote do Fazer download do instalador ou usar a ESET Remote Deployment Tool instalador do Agente e do produto de segurança ESET permite opções de configuração avançadas, inclusive configurações de Política para o Agente ESET Management e produtos ESET, Nome do host e Porta do Servidor ESET PROTECT, além da capacidade de selecionar um Grupo principal. Você pode implantar o instalador de forma local ou remota (usando o ESET Remote Deployment Tool).

- Implantar primeiro o Agente (instalador de script do Agente) –Esse tipo de implantação do Agente é útil quando as opções de implantação remota e local não são adequadas para você. Você pode distribuir o instalador de script do Agente por e-mail e permitir que o usuário o implante. Você também pode executar o Instalador de script do agente de uma mídia removível (uma unidade USB, por exemplo).

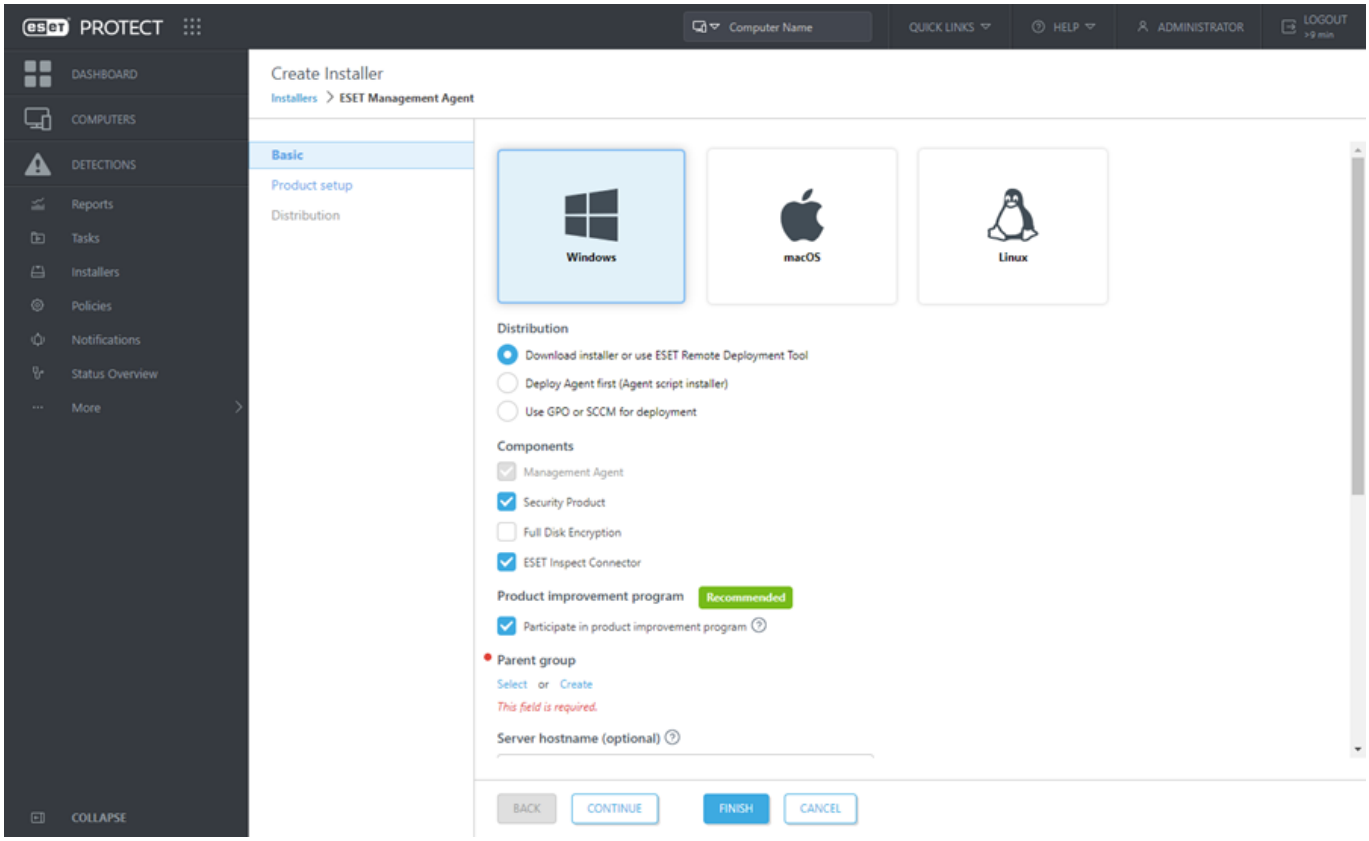
- Use GPO ou SCCM para implantação –Use esta opção para implantação em massa do Agente ESET Management em computadores do cliente.

macOS

- O pacote do Fazer download ou enviar instalador instalador do Agente e do produto de segurança ESET permite opções de configuração avançadas, inclusive configurações de Política para o Agente ESET Management e produtos ESET, Nome do host e Porta do Servidor , além da capacidade de selecionar um Grupo principal.

Linux

- Implantar primeiro o Agente (instalador de script do Agente) –Esse tipo de implantação do Agente é útil quando as opções de implantação remota e local não são adequadas para você. Você pode distribuir o instalador de script do Agente por e-mail e permitir que o usuário o implante. Você também pode executar o Instalador de script do agente de uma mídia removível (uma unidade USB, por exemplo).



Instaladores e permissões

Um usuário pode criar ou editar instaladores contidos em grupos onde o usuário tem permissão de **Gravação** para **Grupos e Computadores** e **Instaladores armazenados**.

Para fazer download dos instaladores já criados, um usuário precisa de permissão de **Uso** para **Grupos e Computadores** e **Instaladores armazenados.**

- Atribua a permissão **Uso** a um usuário para as **Políticas** que estão selecionadas em **Avançado** > **Configuração inicial do instalador** > **Tipo de configuração** ao criar um Instalador Tudo-em-um, instalador GPO ou script SCCM.
- Atribuir permissão de **Uso** a um usuário para **Licenças** se a licença para o grupo estático estiver especificada.
- Selecionar o Grupo principal durante a criação do instalador não afeta a localização do instalador. Depois de criar o instalador, ele é colocado no Grupo de acesso do usuário atual. O Grupo de acesso define o grupo estático do objeto e o acesso ao objeto com base nos direitos de acesso do usuário.
- Tenha em mente que o usuário será capaz de trabalhar com os Certificados ao criar instaladores. Atribua a permissão de **Uso** a um usuário para os **Certificados** com o acesso ao grupo estático onde os certificados estão contidos. Se um usuário quiser implantar um Agente ESET Management, esse usuário precisará ter permissão de **Uso** para a Autoridade de certificação onde o certificado de servidor real é assinado. Para informações sobre dividir o acesso a Certificados e Autoridade de certificação, leia este exemplo.

Grupo doméstico – O grupo doméstico é detectado automaticamente com base no conjunto de permissões atribuído do usuário atualmente ativo.

Exemplo de cenário:

A conta de usuário atualmente ativa tem o direito de acesso de **Gravação** para a **Tarefa de cliente de Instalação de software** e a conta do **Grupo doméstico** é "Department_1". Quando o usuário criar uma nova **Tarefa de cliente de instalação de software**, "Department_1" será selecionado automaticamente como o **Grupo doméstico** da tarefa de cliente.

Se o Grupo doméstico pré-selecionado não atender às suas expectativas, você pode selecionar o Grupo doméstico manualmente.

Como permitir ao usuário criar instaladores

O *Administrador* quer permitir ao usuário *John* criar ou editar novos instaladores no *Grupo do John*. O *Administrador* deve seguir essas etapas:

1.Criar um novo Grupo estático chamado *Grupo do John*

2.Criar novo Conjunto de permissões

a.Nomeie o novo conjunto de Permissões *Permissões para John – criar Instaladores*

b.Adicione o grupo *Grupo do John* na seção **Grupos estáticos**

c.Na seção **Funcionalidade**, selecione

- **Gravação** para **Instaladores armazenados**
- **Uso** para **Certificados**
- **Gravação** para **Grupos e Computadores**

d.Clique em **Concluir** para salvar o conjunto de permissões

3.Criar novo Conjunto de permissões

a.Nomeie o novo conjunto de Permissões *Permissões para John – Certificados*

b.Adicione o grupo *Todos* na seção **Grupos estáticos**

c.Na seção **Funcionalidade** selecione **Uso** para **Certificados**.

d.Clique em **Concluir** para salvar o conjunto de permissões

Essas permissões são os requisitos mínimos para o uso completo (criação e edição) do instalador.

4.Criar um novo usuário

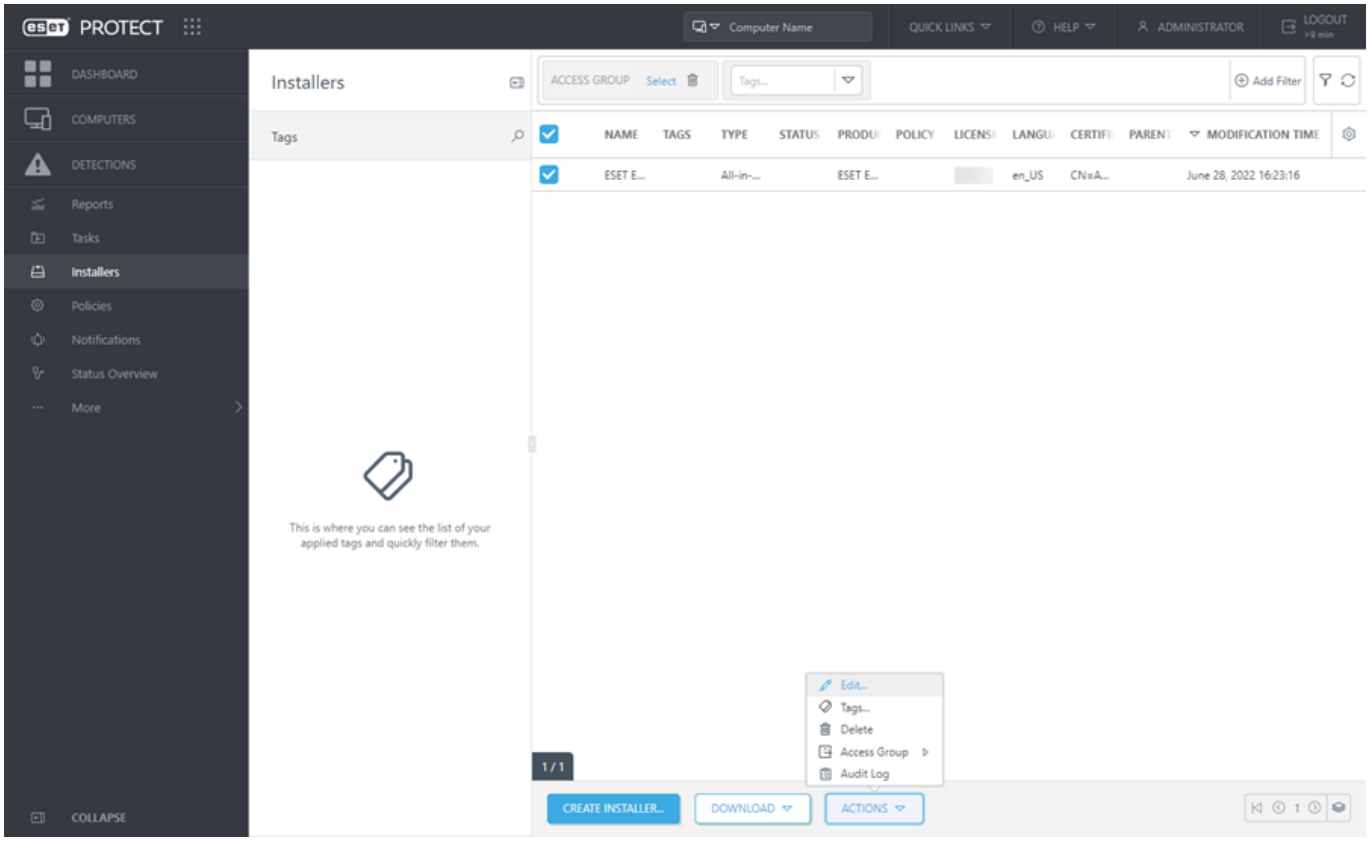
a.Nomeie o novo usuário *John*

b.Na seção **Básico** selecione *Grupo do John* como o Grupo inicial

c.Defina a senha para o usuário *John*

d.Na seção **Conjunto de Permissões** selecione *Permissões para John - Certificados* e *Permissões para John - Criar instaladores*

e.Clique em **Concluir** para salvar o usuário



Como fazer download dos instaladores a partir do menu de instaladores

1.Clique em **Instaladores**.

2.Selecione a caixa de seleção ao lado do instalador que deseja baixar.

3.Clique em **Download** e escolha o pacote de instalação correto (com base no número de bits ou no sistema operacional). Se uma versão posterior de um produto ESET no instalador estiver disponível (produto de segurança ESET, Conector ESET Inspect ou ESET Full Disk Encryption), uma janela será exibida. Selecione a caixa de seleção **Eu aceito o Acordo de licença de usuário final e reconheço a Política de Privacidade** e clique em **Atualizar e fazer download** para atualizar o instalador e fazer download dele.

Como editar instaladores do menu de instaladores

1.Clique em **Instaladores**.

2.Selecione a caixa de seleção ao lado do instalador que deseja editar.

3.Clique em **Ações** > **Editar** para modificar o pacote do instalador.

Filtros e personalização de layout

Você pode personalizar a exibição da tela atual do console web:

- Gerenciar o painel lateral e a tabela principal.
- Adicionar filtro e predefinições de filtro. Você pode usar marcações para filtrar os itens exibidos.

Políticas

Políticas são usadas para enviar configurações específica aos produtos ESET sendo executados nos computadores do cliente. Isso permite que você não precise configurar cada produto ESET no cliente manualmente. Uma política pode ser aplicada diretamente em Computadores individuais, e também como grupos (Estático e Dinâmico). Também é possível atribuir várias políticas a um computador ou grupo.

Políticas e permissões

O usuário precisa ter permissões suficientes para criar e atribuir políticas. Permissões necessárias para certas ações de Políticas:

- Para ler a lista de políticas e sua configuração um usuário precisa da permissão **Leitura**.
- Para atribuir políticas a destinos, um usuário precisa de permissão de **Uso**.
- Para criar, modificar ou editar políticas, um usuário precisa da permissão de **Gravação**.

Veja a lista de permissões para obter mais informações sobre os direitos de acesso.

Há um ícone de cadeado ao lado de políticas bloqueadas (não editáveis) – políticas internas específicas (por exemplo, a política de Atualizações automáticas ou as políticas ESET LiveGuard) ou políticas onde o usuário tem a permissão de **Leitura**, mas não de **Gravação**.

- Se o usuário *John* precisar apenas ler as políticas criadas por ele mesmo, a permissão **Leitura** para **Políticas** é necessária.
- Se o usuário *John* quiser atribuir determinadas políticas para computadores, ele precisa da permissão de **Uso** para **Políticas** e permissão de **Uso** para **Grupos e Computadores**.
- Para permitir que *John* tenha acesso total para as políticas, o *Administrador* deve definir a permissão de **Gravação** para as **Políticas**.

Aplicação da política

As políticas são aplicadas na ordem em que os grupos estáticos são organizados. Isso não é verdadeiro para Grupos dinâmicos, onde os Grupos dinâmicos secundários são verificados primeiro. Isso permite que você aplique políticas com mais impacto no topo da árvore de grupos e aplique políticas mais específicas para subgrupos. Usando sinalizadores, um usuário ESET PROTECT com acesso a grupos localizados mais alto na árvore pode anular políticas de grupos mais baixos. O algoritmo é explicado detalhadamente em Como as Políticas são aplicadas aos clientes.

Regras de remoção de política

Quando você tem uma política em vigor e decide removê-la mais tarde, a configuração resultante dos computadores cliente vai depender da versão do produto de segurança ESET instalado nos computadores gerenciados:

- Produtos de Segurança ESET versão 6 e versões posteriores: A configuração não volta automaticamente para as configurações originais quando a política é removida. A configuração permanecerá acordo com a última política que foi aplicada aos clientes. O mesmo acontece quando um computador torna-se membro de um Grupo dinâmico no qual uma certa política é aplicada e ela altera as configurações do computador.

Essas configurações permanecem mesmo se o computador deixar o grupo dinâmico. Portanto, recomendamos que você crie uma política com as configurações padrão e atribua-a ao grupo root (**Todos**) para que as configurações voltem para o padrão em tal situação. Assim, quando um computador sair de um grupo dinâmico que mudou suas configurações, este computador vai voltar para as configurações padrão.

• Produtos de Segurança ESET versão 7 e versões posteriores: Quando uma política é removida, a configuração voltará automaticamente para a última política que foi aplicada aos clientes. Quando um computador sair de um Grupo dinâmico onde uma configuração de política em particular estava implementada, essas configurações de política serão removidas do computador. O sinalizador **Não aplicar** transforma políticas de configurações individuais no estado padrão em computadores do cliente.

Mesclagem de Políticas

Uma política aplicada a um cliente normalmente é resultado de várias políticas sendo mescladas em uma política final.

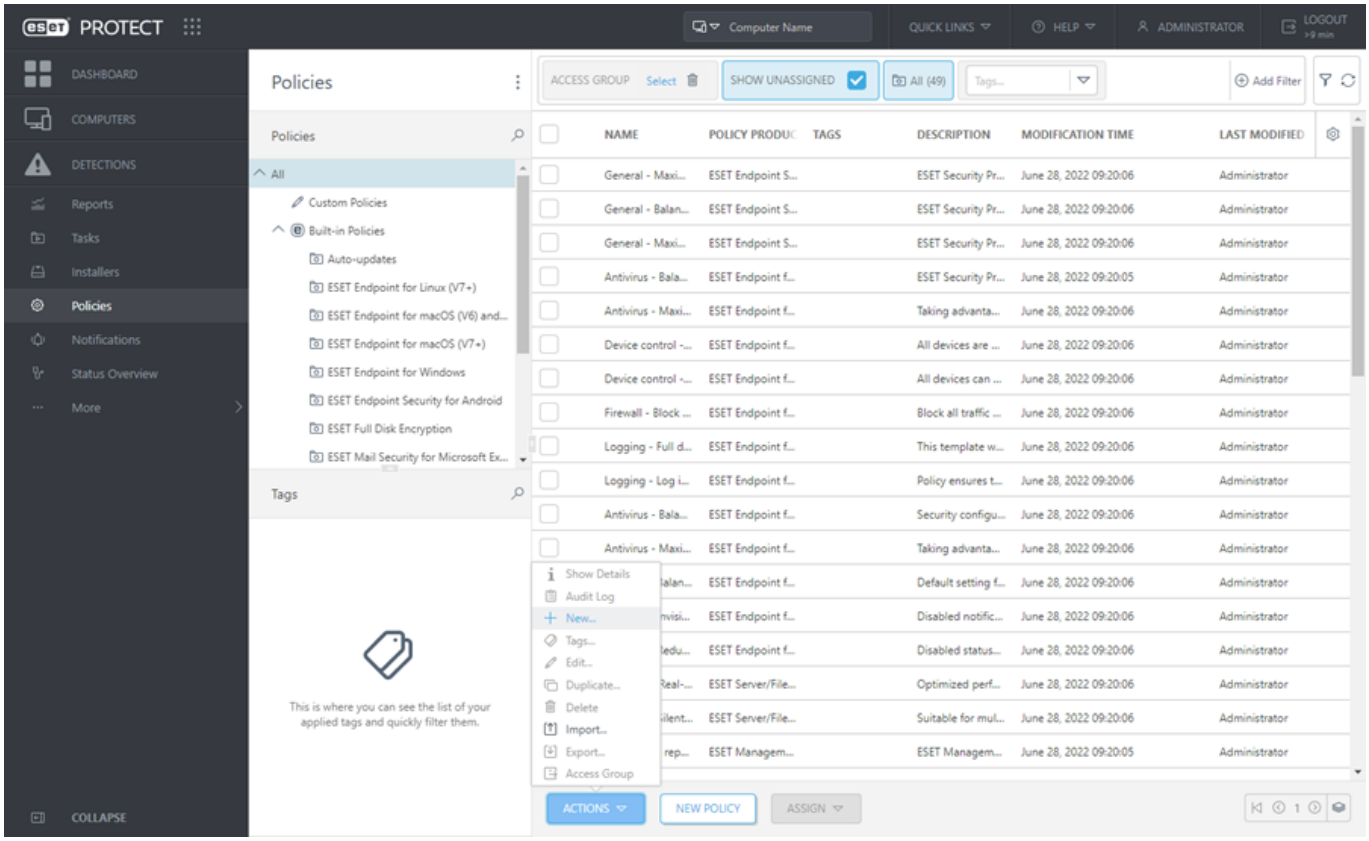
> Recomendamos atribuir políticas mais genéricas (por exemplo, o servidor de atualização) para grupos que estão mais alto na árvore de grupos. Políticas mais específicas (por exemplo, configurações de controle de dispositivos) devem ser atribuídas em locais mais baixos na árvore de grupo. A política mais baixa geralmente anula as configurações das políticas mais altas quando mescladas (a menos que seja definido de outra forma com sinalizadores de política).

Assistente de Políticas

As políticas são agrupadas/categorizadas por produto ESET. **Políticas incorporadas** contém políticas predefinidas e **Políticas personalizadas** listam as categorias de todas as políticas criadas ou modificadas manualmente por você.

Use políticas para configurar seu produto ESET da mesma forma que você faria de dentro da janela de Configuração avançada da interface gráfica do usuário do produto. Ao contrário de políticas no Active Directory, Políticas ESET PROTECT não podem carregar nenhum script ou série de comandos.

Digite para pesquisar um item na Configuração avançada (por exemplo, HIPS). Todas as configuração HIPS serão exibidas. Quando você clica no ícone no canto superior direito, uma página de Ajuda on-line para a configuração em particular será exibida.



Filtros e personalização de layout

Você pode personalizar a exibição da tela atual do console web:

- Gerenciar o painel lateral e a tabela principal.
- Adicionar filtro e predefinições de filtro. Você pode usar marcações para filtrar os itens exibidos.

Criando uma nova política

1.Clique em **Ações** > **Novo**.

2.Insira informações básicas sobre a política, como o **Nome** e **Descrição** (opcional). Clique em **Selecionar marcações** para atribuir marcações.

3.Selecione o produto correto na seção **Configurações**.

4.Use sinalizadores para adicionar configurações que serão processadas pela política.

5.Especifique os clientes que receberão essa política. Clique em **Atribuir** para exibir todos os grupos estáticos e dinâmicos e seus membros. Selecione o computador no qual você deseja aplicar uma política e clique em **OK**.

6.Verifique as configurações para esta política e clique em **Concluir**.

Sinalizadores

Ao mesclar políticas você pode alterar o comportamento usando sinalizadores de política. Os sinalizadores definem como uma configuração será processada pela política.

Para cada configuração você pode selecionar um dos sinalizadores a seguir:

Não aplicar - Qualquer configuração com este sinalizador não é definida pela política. Como a configuração não é forçada, ela pode ser alterada por outras políticas mais tarde.

Aplicar - configurações com esse sinalizador serão enviadas para o cliente. Porém, ao mesclar políticas, isso pode ser sobrescrito por uma política posterior. Quando uma política é aplicada a um computador de um cliente e uma configuração em particular tem este sinalizador, a configuração é alterada independentemente da configuração local no cliente. Como a configuração não é forçada, ela pode ser alterada por outras políticas mais tarde.

Forçar - Configurações com um sinalizador forçar terão prioridade e não poderão ser sobrescritas por uma política posterior (mesmo se a política posterior tiver um sinalizador Forçar). Isso garante que essa configuração não será alterada com políticas posteriores durante a mesclagem.

Para que a navegação seja mais fácil, todas as regras são contadas. O número de regras definidas em uma seção particular será exibido automaticamente. Além disso, você verá um número ao lado do nome de categoria na árvore na esquerda. Isto mostra uma soma de regras em todas as suas seções. Assim, você verá rapidamente onde e quantas configurações/regras estão definidas.

Também é possível usar as sugestões a seguir para tornar a edição de políticas mais simples:

- Uso para definir Aplicar sinalizador a todos os itens em uma seção atual
- Use para excluir as regras aplicadas aos itens na seção atual

Produtos de Segurança ESET versão 7 e versões posteriores:
O sinalizador **Não aplicar** transforma políticas de configurações individuais no estado padrão em computadores do cliente.

Como o Administrador pode permitir que os usuários vejam todas as políticas

O *Administrador* quer que o usuário *John* crie e edite políticas em seu grupo inicial e permitir que *John* veja as políticas que são criadas pelo *Administrador*. Políticas criadas pelo *Administrador* incluem sinalizadores **Forçar**. O usuário *John* pode ver todas as políticas, mas não pode editar políticas criadas pelo *Administrador* porque a permissão **Leitura** para as **Políticas** com acesso ao Grupo estático *Todos* está definida. O usuário *John* pode criar ou editar políticas em seu grupo inicial *San Diego*.
O *Administrador* deve seguir essas etapas:
Criar ambiente
1.Criar um novo Grupo estático chamado *San Diego*.
2.Criar um novo Conjunto de permissões chamado *Política - Todos John* com acesso ao Grupo estático *Todos* e com permissão de **Leitura** para as **Políticas**.
3.Criar um novo Conjunto de permissões chamado *Política John* com acesso ao Grupo estático *San Diego*, com permissão para a funcionalidade de acesso **Gravação** para **Grupo e Computadores** e **Políticas**. Esse conjunto de permissões permite ao usuário *John* criar ou editar políticas em seu grupo inicial *San Diego*.
4.Criar um novo usuário *John* e na seção **Conjunto de** Permissões selecione *Política - Todos John* e *Política John*.
Criar políticas
5.Crie uma nova política *Todos - Ativar firewall*, expanda a seção **Configurações**, selecione **ESET Endpoint para Windows**, navegue até **Proteção da rede** > **Firewall** > **Básico** e aplique todas as configurações pelo sinalizador **Forçar**. Expanda a seção **Atribuir** e selecione o Grupo estático *Todos*.
6.Crie uma nova política *Grupo John - Ativar Firewall*, expanda a seção **Configurações**, selecione **ESET Endpoint para Windows**, navegue até **Proteção da rede Firewall** > **Básico** e aplique todas as configurações pelo sinalizador **Aplicar**. Expanda a seção **Atribuir** e selecione o Grupo estático *San Diego*.
Resultado
Políticas criadas pelo *Administrador* serão aplicadas primeiro pois estão atribuídas ao grupo *Todos*. Configurações com um sinalizador **Forçar** terão prioridade e não poderão ser sobrescritas por uma política posterior. Então as políticas criadas pelo usuário *John* serão aplicadas.
Vá até **Mais** > **Grupos** > **San Diego**, clique no computador e selecione **Detalhes**. A ordem de aplicação da política final está em **Configuração** > **Políticas aplicadas**.

POLICY OF	POLICY PRODUC	POLICY NAME	POLICY DESCR
1 (applied first)	Auto-updates	Enable produ...	Enable automa
2	ESET Endpoint fo...	ESET LiveGua...	Enables ESET Li

A primeira política é criada pelo *Administrador* e a segunda é criada pelo usuário *John*.

Grupo doméstico – O grupo doméstico é detectado automaticamente com base no conjunto de permissões atribuído do usuário atualmente ativo.

Exemplo de cenário:
A conta de usuário atualmente ativa tem o direito de acesso de **Gravação** para a **Tarefa de cliente de Instalação de software** e a conta do **Grupo doméstico** é "Department_1". Quando o usuário criar uma nova **Tarefa de cliente de instalação de software**, "Department_1" será selecionado automaticamente como o **Grupo doméstico** da tarefa de cliente.

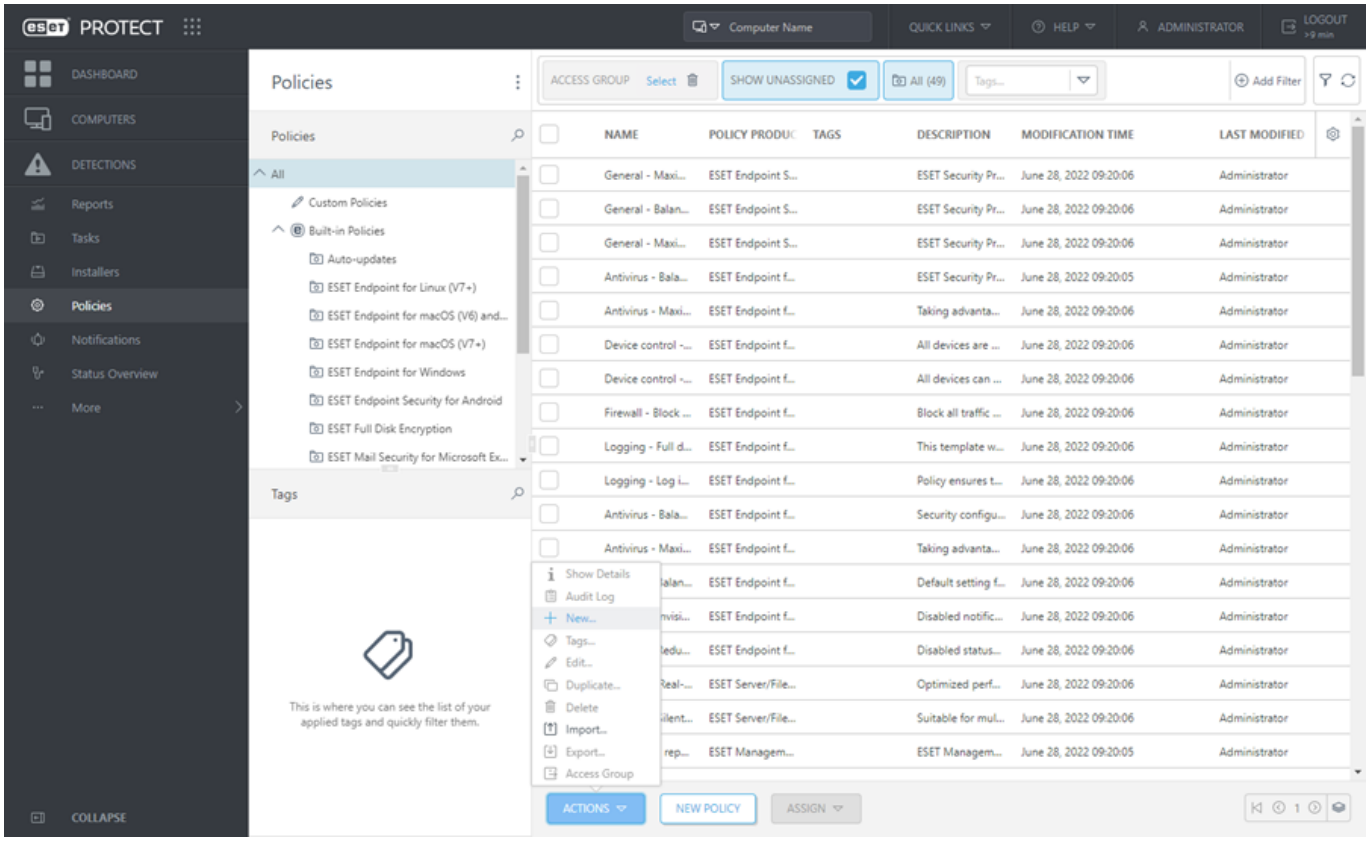
Se o Grupo doméstico pré-selecionado não atender às suas expectativas, você pode selecionar o Grupo doméstico manualmente.

Gerenciar políticas

As políticas são agrupadas/categorizadas por produto ESET. **Políticas incorporadas** contém políticas predefinidas e Políticas personalizadas listam as categorias de todas as políticas criadas ou modificadas manualmente por você.

Ações disponível para políticas:

Mostrar detalhes	Mostrar detalhes da política.
Relatório de auditoria	Exibe o Relatório de auditoria para o item selecionado.
Novo	Criando uma nova política.
Marcações	Editar marcações (atribuir, remover atribuição, criar, remover).
Editar	Modifica uma política existente.
Duplicar	Cria uma nova política com base em uma política existente selecionada por você. A política duplicada precisa de um novo nome.
Alterar atribuições	Atribui uma política a um cliente ou grupos.
Excluir	Excluir uma política. Veja também as regras de remoção de política.
Importar	Clique em **Políticas** > **Importar**, clique em **Escolher arquivo** e vá até o arquivo que você quer importar. Você pode importar apenas um arquivo *.dat* que contenha as políticas exportadas do console da Web ESET PROTECT. Não é possível importar um arquivo *.xml* que contenha políticas exportadas do produto de segurança ESET. As políticas importadas vão aparecer sob **políticas personalizadas**.
Exportar	Marque as caixas de seleção ao lado das políticas que deseja exportar da lista e clique em **Ações** > **Exportar**. As políticas serão exportadas para um arquivo *.dat*. Para exportar todas as políticas da categoria selecionada, selecione a caixa de seleção no cabeçalho da tabela.
Grupo de acesso > **Mover**	Mova o objeto para outro grupo estático onde ele está disponível para usuários com direitos suficientes para o grupo de destino. Alterar o Grupo de acesso é útil ao resolver problemas de acesso com outros usuários. O Grupo de acesso define o grupo estático do objeto e o acesso ao objeto com base nos direitos de acesso do usuário.



Como as Políticas são aplicadas aos clientes

Grupos e Computadores podem ter várias políticas atribuídas a eles. Além disso, um computador pode estar em um grupo profundamente aninhada, cujos grupos principais têm suas próprias políticas.

A coisa mais importante para a aplicação de políticas é sua ordem. Isto é derivado da ordem do grupo e da ordem de políticas atribuídas ao grupo.

Para ver todas as políticas aplicadas a um computador selecionado, consulte Políticas aplicadas nos detalhes do computador.

Siga as etapas abaixo para determinar a política ativa para qualquer cliente:

1. Encontre a ordem dos grupos onde o cliente reside
2. Substituir grupos com políticas atribuídas
3. Mesclar Políticas para obter configurações finais

Ordenação de Grupos

Políticas podem ser atribuídas a grupos **e são aplicadas em uma ordem específica. As regras escritas abaixo determinar a ordem na qual as políticas são aplicadas aos clientes**.

Regra 1: Grupos estáticos são verificados a partir do Grupo estático (**Todos**) de raiz.

Regra 2: Em cada nível, os grupos estáticos desse nível são verificados em primeiro lugar na ordem em que aparecem na árvore (o que também é chamado pesquisa com a “largura primeiro”).

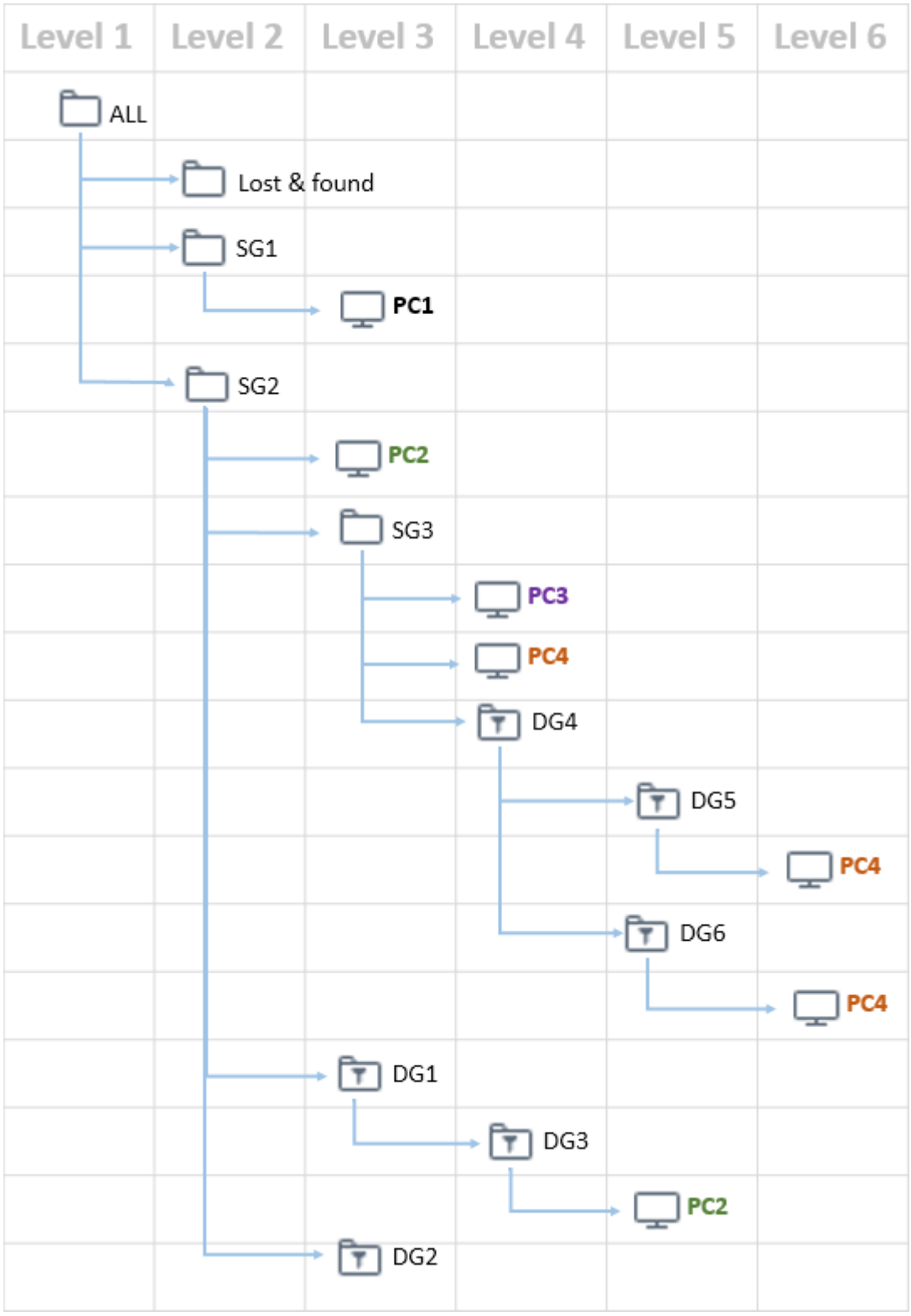
Regra 3: Depois de todos os grupos estáticos em um certo nível estarem registrados, os grupos dinâmicos são verificados.

Regra 4: Em cada grupo dinâmico, todos os seus grupos secundários são verificados na ordem em que aparecem na lista.

Regra 5: Em qualquer nível de um Grupo Dinâmico, qualquer secundário é listado e outros secundários são pesquisados. Quando não há mais secundários, os próximos grupos dinâmicos no nível principal são listados (isso também é chamado de pesquisa “com profundidade primeiro”).

Regra 6: A verificação termina em um computador.

A política será aplicada ao computador. Isso significa que o transversal terminal no computador onde você quer aplicar a política.



Usando as regras escritas acima, a ordem na qual as políticas serão aplicadas em computadores individuais seria a seguinte:

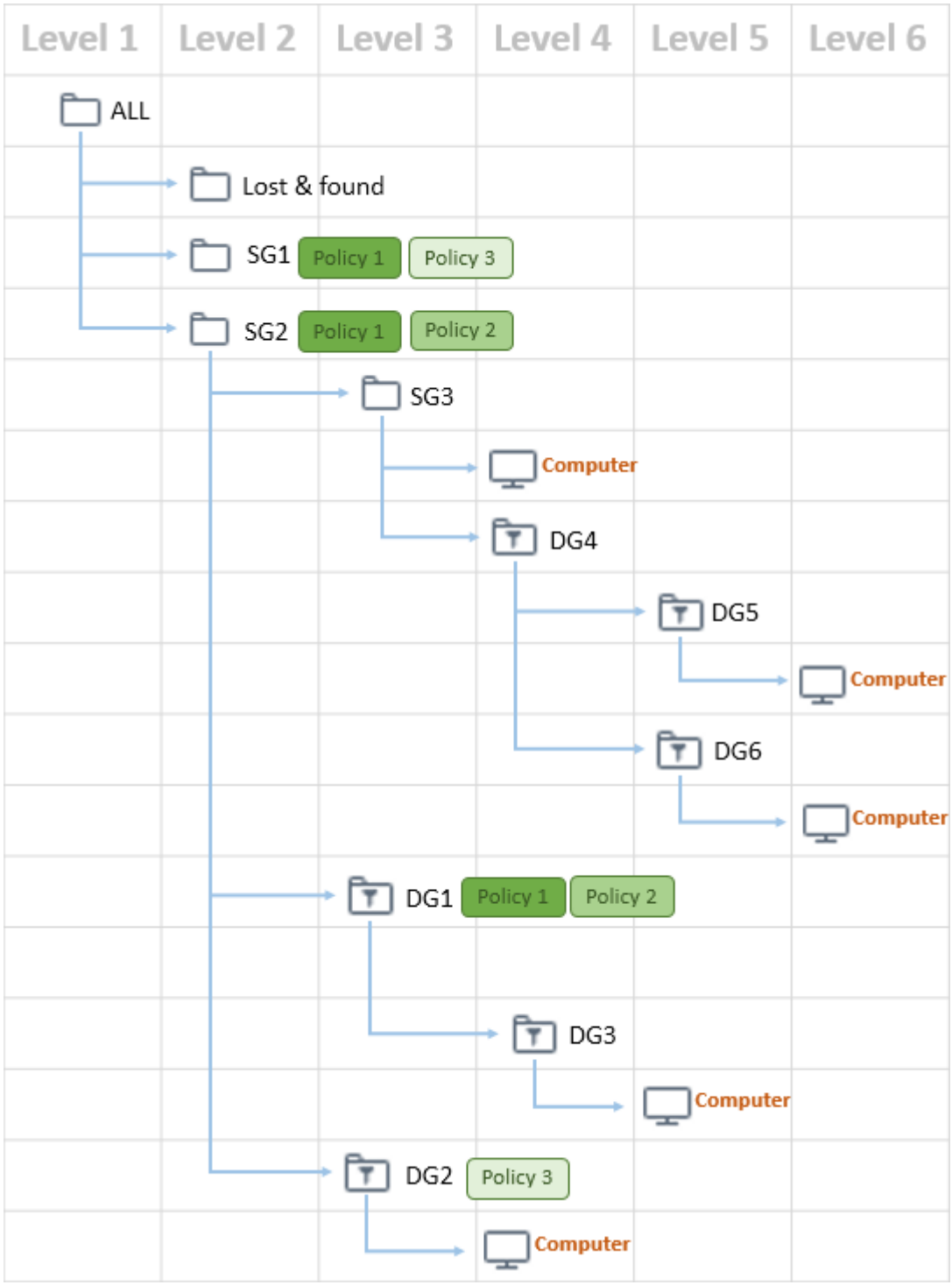
PC1:	PC2:	PC3:	PC4:
1.ALL 2.SG1 3.PC1	1.ALL 2.SG2 3.DG1 4.DG3 5.PC2	1.ALL 2.SG2 3.SG3 4.PC3	1.ALL 2.SG2 3.SG3 4.DG4 5.DG5 6.DG6 7.PC4

Enumeração de Políticas

Quando a ordem dos grupos for conhecida, o próximo passo é substituir cada grupo com as políticas atribuídas a ele. As políticas estão listadas na mesma ordem em que são atribuídas a um grupo. É possível editar a prioridade de políticas para um grupo com mais políticas atribuídas. Cada política configura apenas um produto (Agente ESET Management, EES, etc.).

Um grupo sem uma Política é removido da lista.

Temos três políticas aplicadas a grupos estáticos e dinâmicos(ver imagem abaixo):



A ordem na qual as políticas serão aplicadas no Computador

A lista abaixo exibe os grupos e políticas aplicadas a eles:

1.Todos – removido, sem Política aqui

2.SG 2 -> Política 1, Política 2

3.SG 3 -> removido para sem Política

4.DG 1 – Política 1, Política 2

5.DG 3 – removido, sem Política

6.DG 2 – Política 1, Política 3

7.DG 4 – removido, sem Política

8.DG 5 – removido, sem Política

9.DG 6 – removido, sem Política

10. Computador – removido, sem Política

A lista final de Políticas é:

1.Política 1

2.Política 2

3.Política 1

4.Política 2

5.Política 3

Mesclagem de Políticas

Quando você aplica uma política a um produto de segurança ESET onde outra política já foi aplicada, as configurações sobrepostas da política são mescladas. As políticas são mescladas uma por uma. Ao mesclar políticas, a regra geral é que a última política sempre substitui as configurações definidas pela política anterior. Para alterar esse comportamento, você pode usar sinalizadores de política (disponíveis para todas as configurações). Algumas configurações têm outra regra (substituir / anexar no começo / anexar no final) que você pode configurar.

Tenha em mente que a estrutura dos Grupos (sua hierarquia) e a sequência de políticas determina como as políticas são mescladas. Mesclar duas políticas quaisquer pode ter resultado diferentes dependendo de sua ordem.

Ao criar políticas você vai perceber que algumas configurações têm regras adicionais que você pode configurar. Essas regras permitem que você reorganize as mesmas configurações em várias políticas.

- **Substituir**: A regra padrão usada ao mesclar políticas. Ele substitui as configurações definidas pela política anterior.

- **Anexar**: Ao aplicar a mesma configuração em mais de uma política, você pode anexar no começo as configurações com esta regra. A configuração será colocada no final da lista que foi criada ao mesclar políticas.

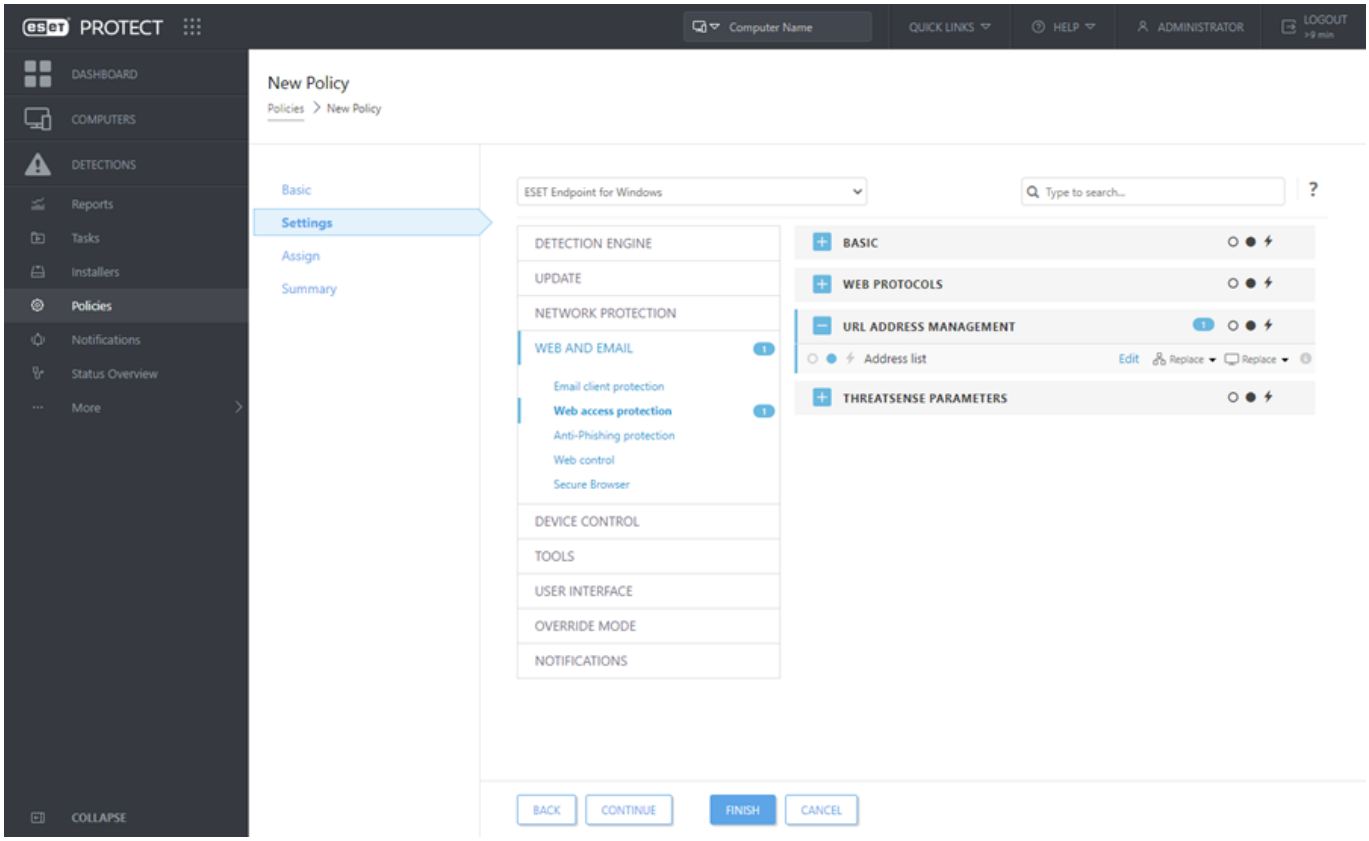
- **Anexar no final**: Ao aplicar a mesma configuração em mais de uma política, você pode anexar no final as configurações com esta regra. A configuração será colocada no começo da lista que foi criada ao mesclar políticas.

Mesclagem de listas local e remota

Os produto de segurança ESET recentes (consulte as versões compatíveis na tabela abaixo) são compatíveis com a mesclagem de configurações remotas com políticas remotas de uma nova forma. Se a configuração for uma lista (por exemplo, uma lista de sites) e uma política remota estiver em conflito com uma configuração local existente, a política remota vai substituir a local. É possível escolher como combinar listas locais e remotas. Você pode selecionar regras de mesclagem diferentes para:

- Configurações de mesclagem para políticas remotas.
- Mesclagem de políticas remotas e locais - configurações locais com a política remota resultante.

As opções são as mesmas descritas acima: **Substituir**, **Incluir no fim**, **Incluir no começo**.



Remoção de política nos produtos de segurança ESET versão 7

Quando uma política é removida, a configuração voltará automaticamente para a última política que foi aplicada aos clientes.

O sinalizador **Não aplicar** transforma políticas de configurações individuais no estado padrão em computadores do cliente.

Exemplo de cenário da mesclagem de políticas

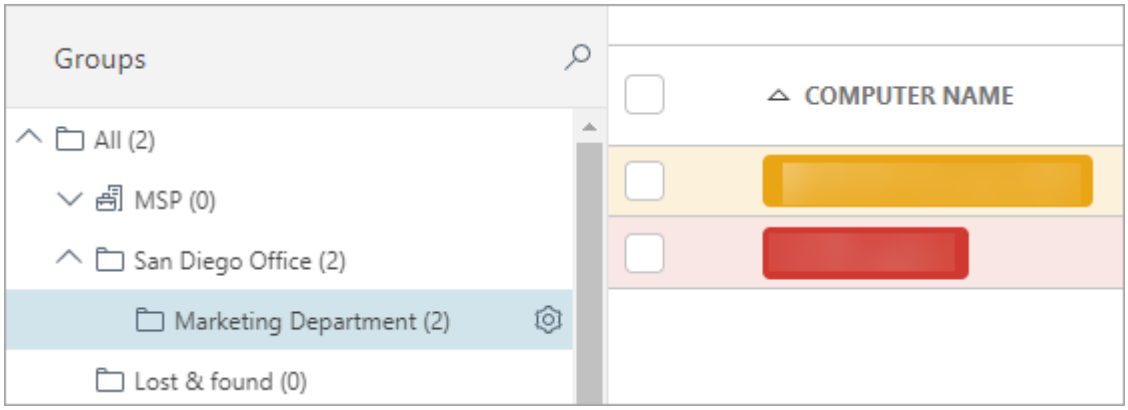
Este exemplo descreve:

- Instruções sobre como aplicar configurações de política aos produtos de segurança ESET Endpoint
- Como as políticas são mescladas ao aplicar sinalizadores e regras

Em situações onde o *Administrador* quer:

- Negue acesso do *Escritório San Diego* para os sites *www.forbidden.uk, www.deny-access.com, www.forbidden-websites.uk* e *www.forbidden-website.com*

- Permita o acesso do *Departamento de Marketing* para os sites *www.forbidden.uk, www.deny-access.com*



O *Administrador* deve seguir essas etapas:

1.Criar um novo grupo estático *escritório San Diego* e o *Departamento de Marketing* como subgrupo do grupo estático *escritório San Diego*.

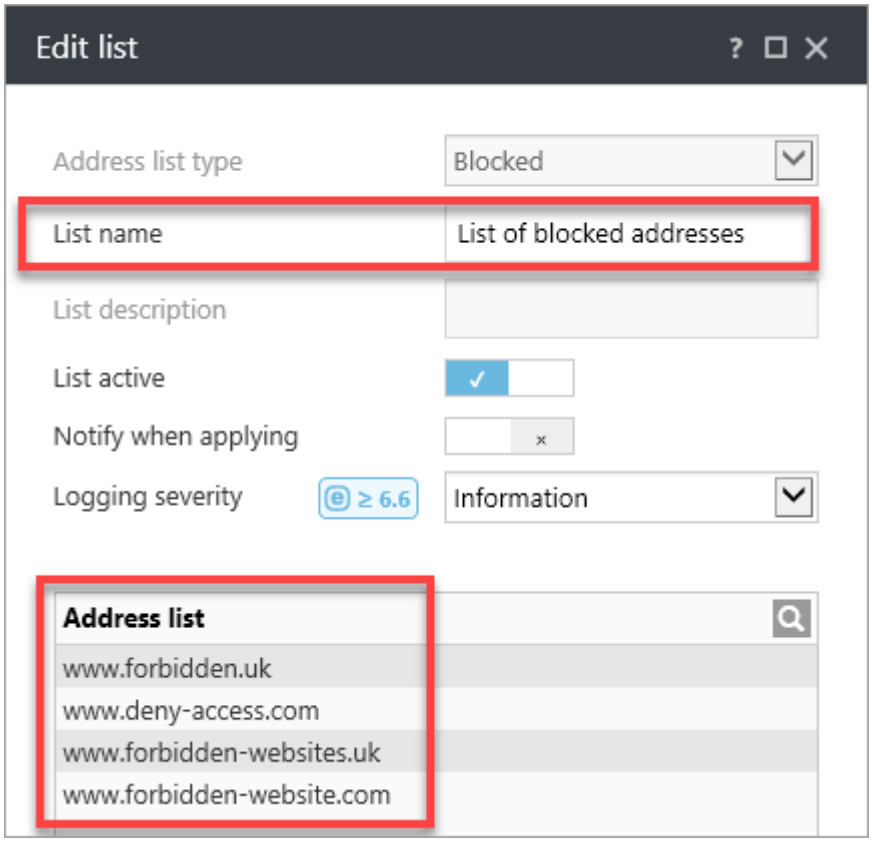
2.Navegue para **Políticas** e crie uma nova política da seguinte forma:

i.Chamado *escritório de San Diego*.
ii.Expanda as **Configurações** e selecione **ESET Endpoint para Windows**
iii.Vá para **Web e email** > **Proteção de acesso à web** > **Gerenciamento de endereços de URL**
iv.Clique no botão **Aplicar** política e edite a **Lista de endereços** clicando em **Editar**
v.Clique na **Lista de endereços bloqueados** e selecione **Editar**.

vi.Adicione os seguintes endereços da web: *www.forbidden.uk, www.deny-access.com, www.forbidden-websites.uk* e *www.forbidden-website.com*. Salve a lista de endereços bloqueados e a lista de endereços.

vii. Expanda **Atribuir** e atribua a política ao *Escritório de San Diego* e seu subgrupo *Departamento de Marketing.*
viii. Clique em **Concluir** para salvar a política.

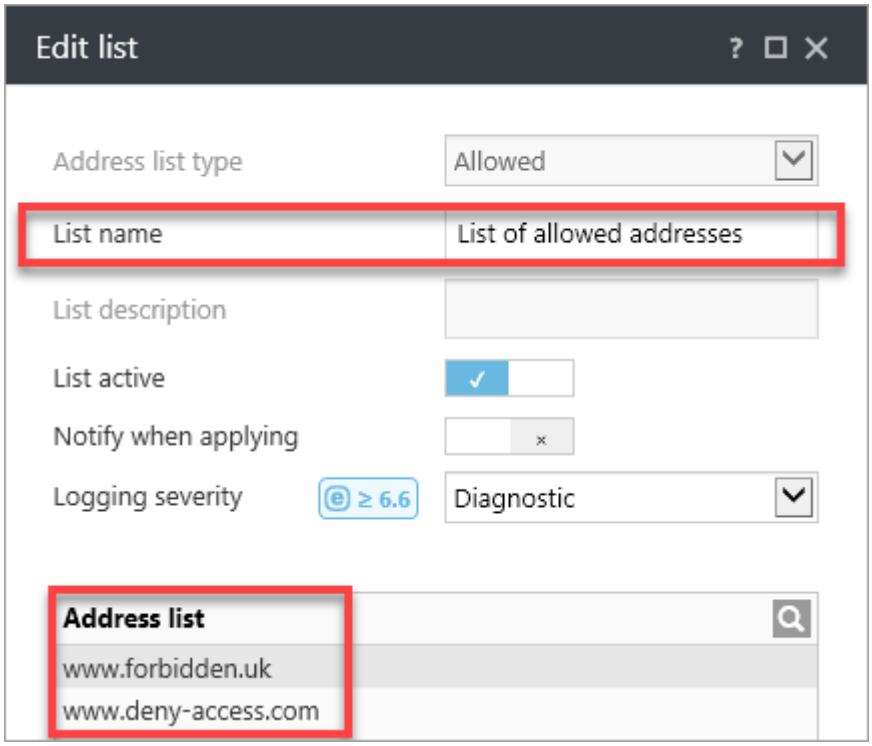
Esta política será aplicada ao *Escritório San Diego* e *Departamento de Marketing* e vai bloquear os sites como exibido abaixo.



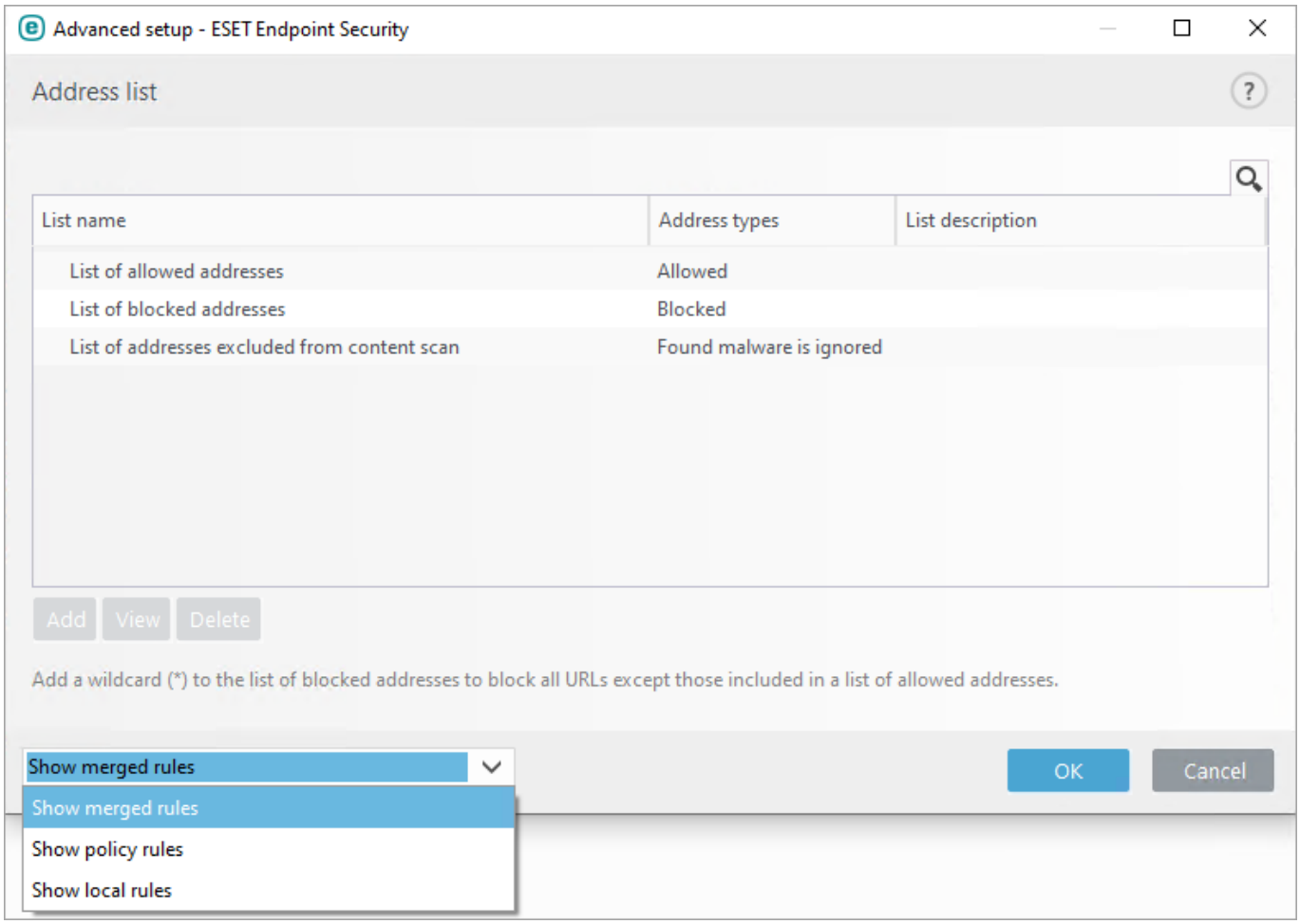
3.Navegue para **Políticas** e crie uma nova política:

i.Chamado *Departamento de Marketing*.
ii.Expanda as **Configurações** e selecione **ESET Endpoint para Windows**
iii.Vá para a seção **Web e email** > **Proteção de acesso à web** > **Gerenciamento de endereços de URL**
iv.Clique no botão **Aplicar** política, selecione Anexar regra e edite a **Lista de endereços** clicando em **Editar**. Anexar Regra ao Final faz com que a lista de Endereços seja colocada no final ao mesclar políticas.
v.Clique na **Lista de endereços permitidos** > **Editar**.
vi.Adicione os seguintes endereços da web: k*www.forbidden.uk*, *www.deny-access.com*. Salve a lista de endereços permitidos e a lista de endereços.
vii. Expanda **Atribuir** e atribua a política ao *Departamento de Marketing*
viii. Clique em **Concluir** para salvar a política.

Esta política será aplicada ao *Departamento de Marketing* e permitirá acesso aos sites como exibidos abaixo.



4.A política final vai incluir ambas as políticas aplicadas ao *Escritório San Diego* e *Departamento de Marketing*. Abra o **produto Endpoint Security** e navegue até **Configuração** > **Web e email** > **Configuração avançada**, selecione a guia **Web e email** > **Proteção do acesso à Web** e abra o **Gerenciamento de endereço URL**. A configuração final do produto Endpoint será exibida.



A configuração final inclui:

1. Lista de endereços da política do *Escritório de San Diego*

2. Lista de endereços da política do *Departamento de marketing*

Configuração de um produto de ESET PROTECT

É possível usar políticas para configurar seu produto ESET da mesma forma que você faria de dentro da janela de Configuração avançada da interface gráfica do usuário do produto. Ao contrário de políticas no Active Directory, Políticas ESET PROTECT não podem carregar nenhum script ou série de comandos.

Para a Versão 6 e produtos ESET mais recentes é possível definir certos status para serem reportados no cliente ou no console da Web. Isso pode ser definido em uma política para produto v6 sob **Interface do usuário** > **Elementos de interface do usuário** > **Status**:

- **Mostrar** - o status é reportado na interface gráfica do usuário do cliente
- **Enviar** - status reportado para ESET PROTECT

Exemplos de uso de política para configurar produtos ESET:

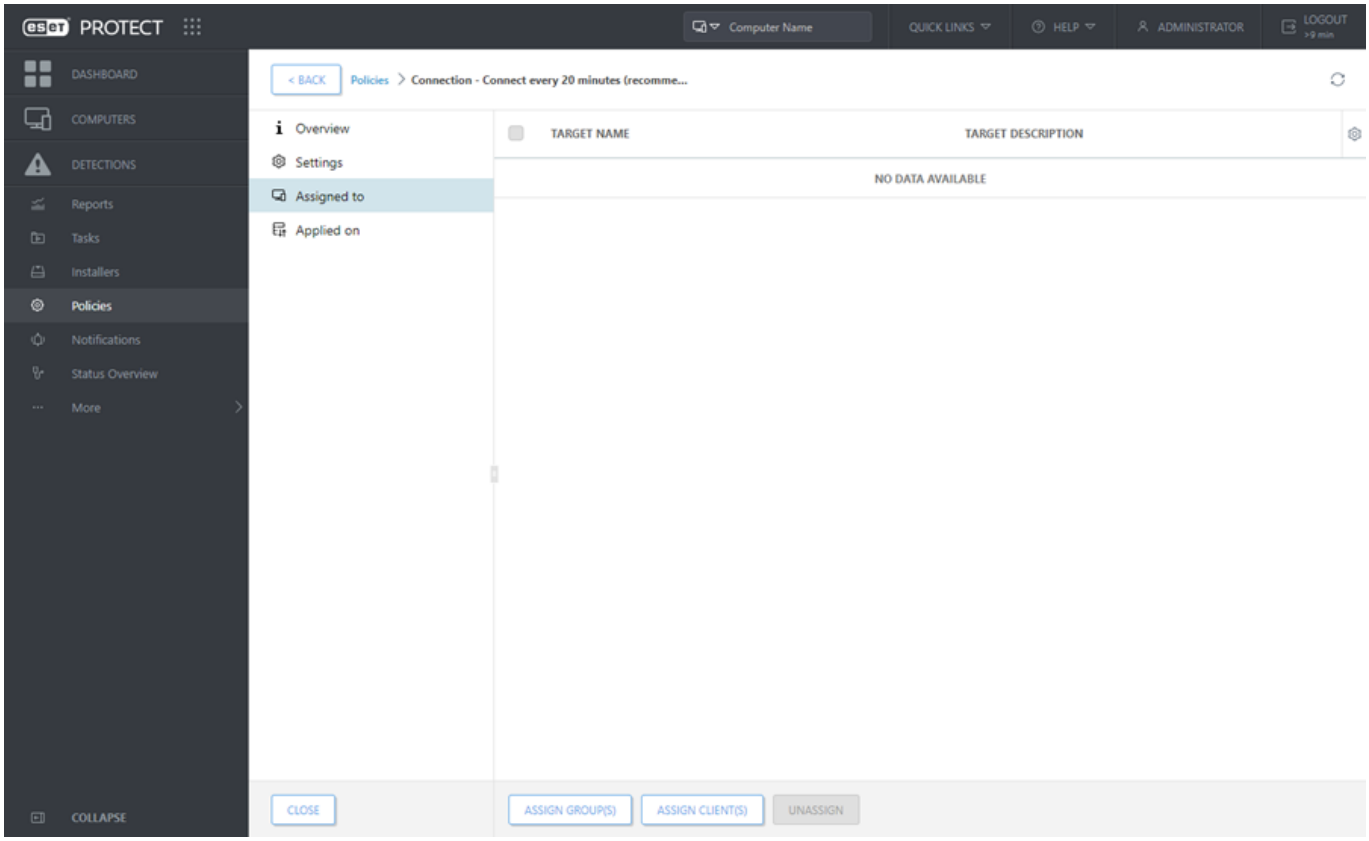
- ESET ManagementConfigurações de política do Agente
- Configurações de política do ESET Rogue Detection Sensor
- Criar uma política para iOS MDM - Conta Exchange ActiveSync
- Criar uma política para MDC para ativar APNS para inscrição iOS

Atribuir uma política a um grupo

Depois que uma política é criada, você pode atribuí-la a um **grupo estático** ou **grupo dinâmico**. Existem duas maneiras de atribuir uma política:

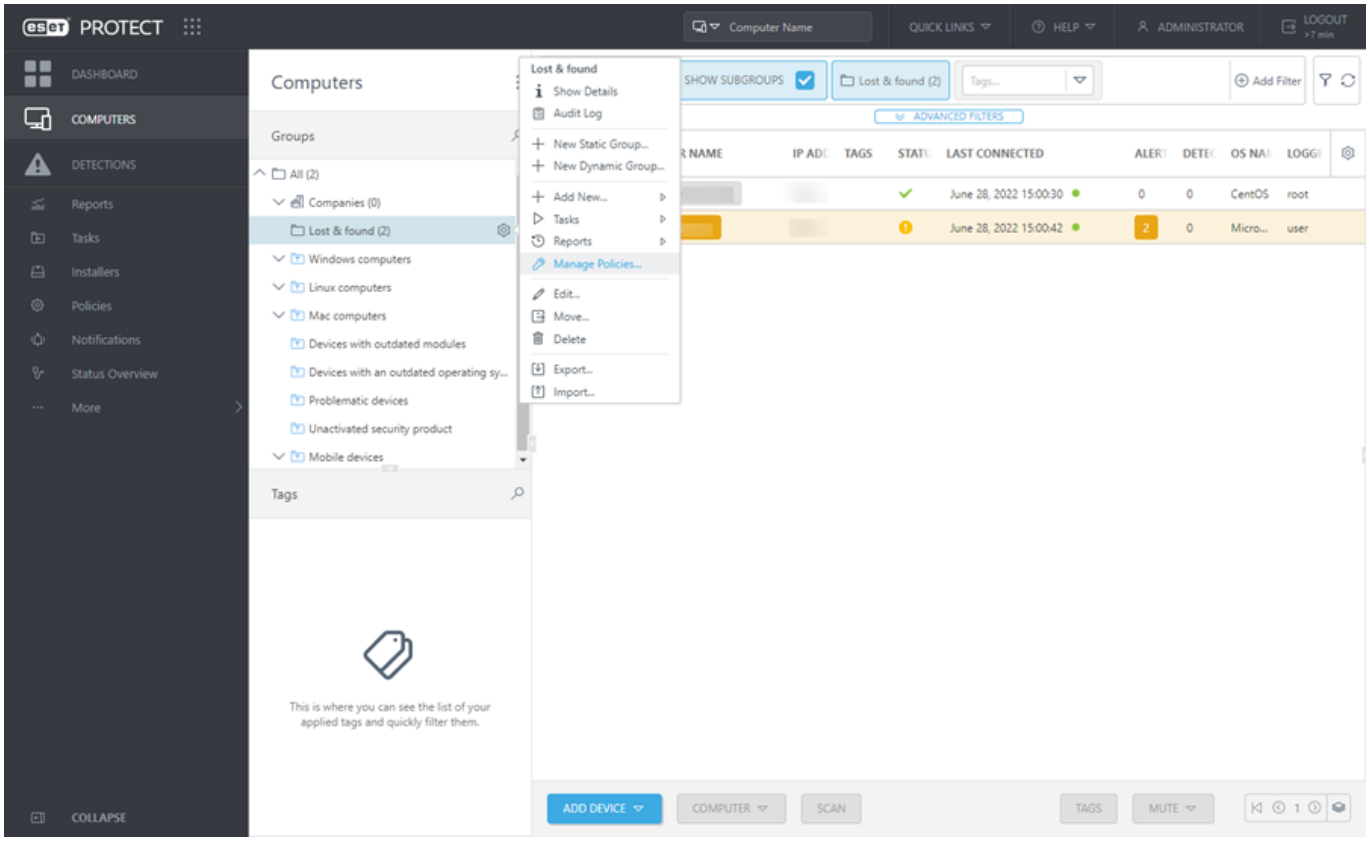
Método I.

Em **Políticas**, selecione uma política e clique em **Ações** > **Mostrar detalhes** > **Atribuído a** > **Atribuir grupo(s)**. Selecione um grupo estático ou dinâmico da lista (é possível selecionar mais grupos) e clique em **OK**.



Método II.

1. Clique em **Computadores**, clique no ícone de engrenagem ao lado do nome do grupo e selecione **Gerenciar políticas**.



2. Na janela **Ordem de aplicação de política** clique em **Adicionar política**.

3. Marque a caixa de seleção ao lado das políticas que deseja atribuir a esse grupo e clique em **OK**.

4. Clique em **Fechar**.

Para ver quais políticas estão atribuídas a um grupo em particular, selecione aquele grupo e clique na guia **Políticas** para ver uma lista de políticas atribuídas ao grupo.

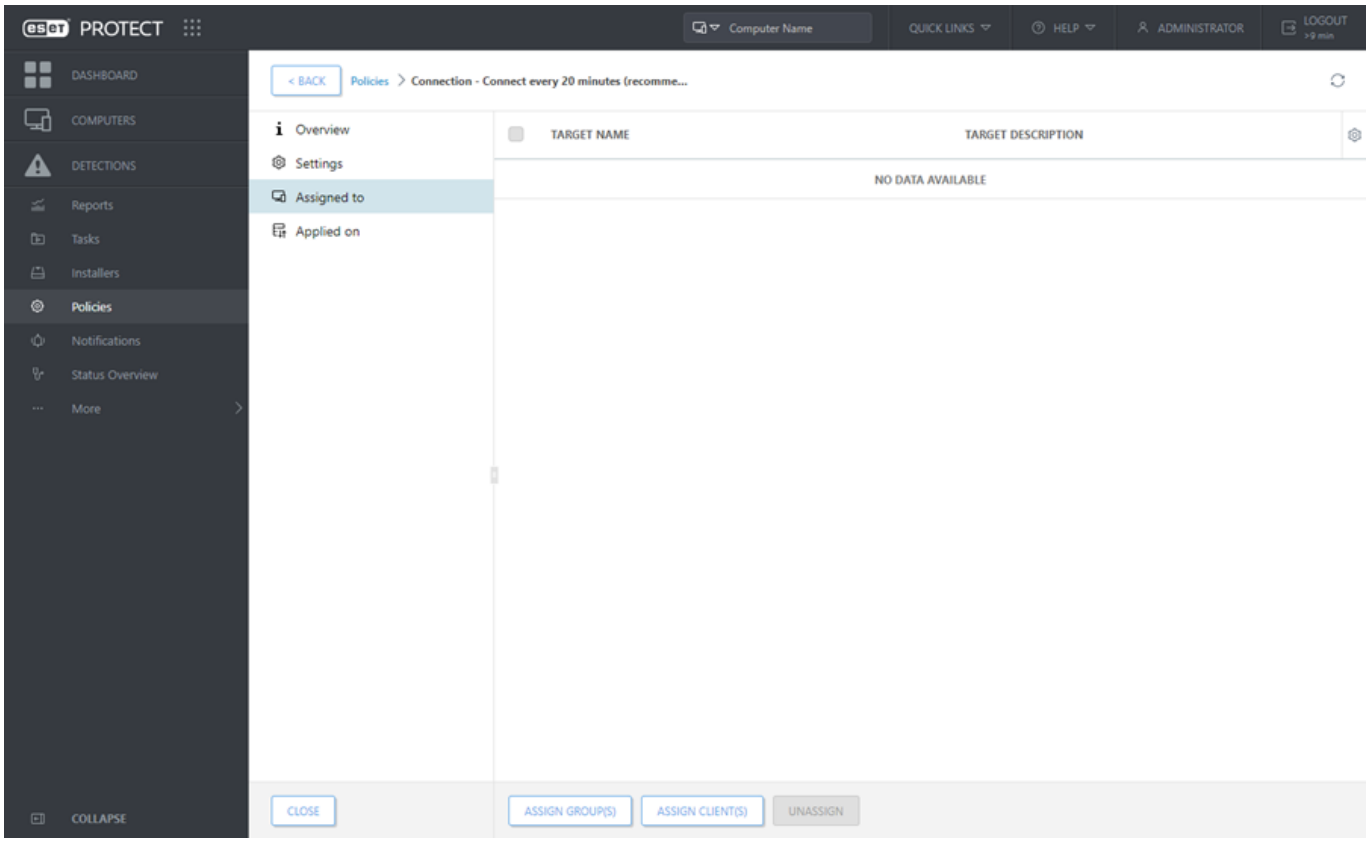
Para ver quais grupos estão atribuídos a uma política específica, selecione a política e clique em **Mostrar Detalhes** > **Aplicado em**.

Para obter mais informações sobre políticas, consulte o capítulo Políticas.

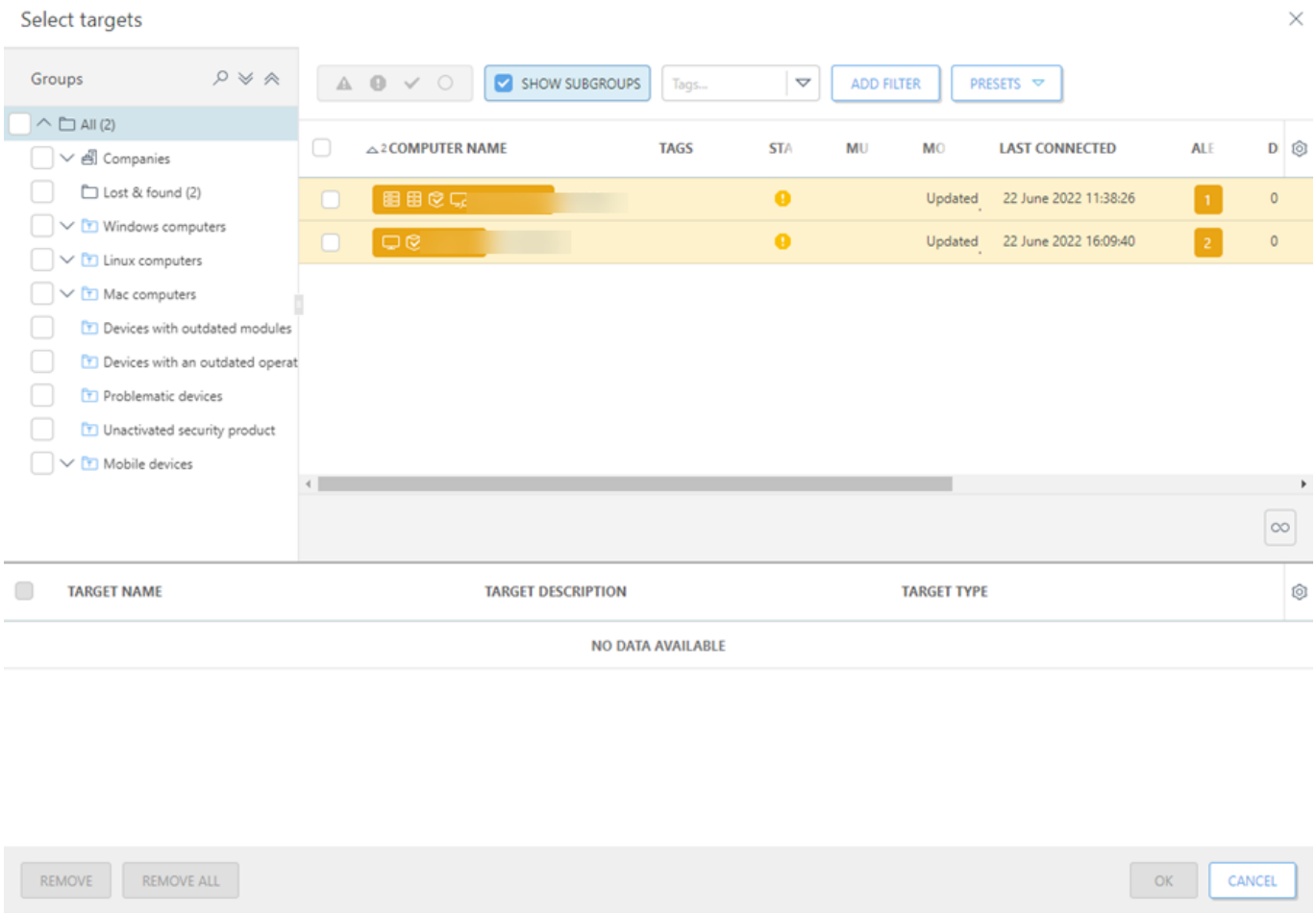
Atribuir uma política a um Cliente

Para atribuir uma política a uma estação de trabalho do cliente, clique em **Políticas** selecione uma política e clique em **Ações** > **Mostrar detalhes** > **Atribuído a** > **Atribuir cliente(s)**.

Para atribuir todos os computadores em um grupo, atribua o grupo em vez de computadores individuais para impedir que a velocidade do Web Console diminua.
O Web Console exibirá um aviso se você selecionar um grande número de computadores.



Selecione seu computador de destino do cliente e clique em **OK**. A política será atribuída a todos os computadores selecionados.



Para ver quais clientes são atribuídos a uma política em particular, selecione a política e consulte a primeira guia **Atribuído a**.

Como usar o modo de Substituição

Usuários com produtos ESET endpoint (versão 6.5 e mais recente) do Windows instalados em sua máquina podem usar o recurso Substituição. Você pode ativar o modo de Substituição no Web Console ESET PROTECT apenas remotamente. O modo de substituição permite que os usuários no nível do computador cliente alterem as configurações no produto ESET instalado, mesmo se houver uma política aplicada a essas configurações. O modo de substituição pode ser ativado para usuários AD, ou pode ser protegido por senha. A função não pode ser ativada por mais de quatro horas por vez.

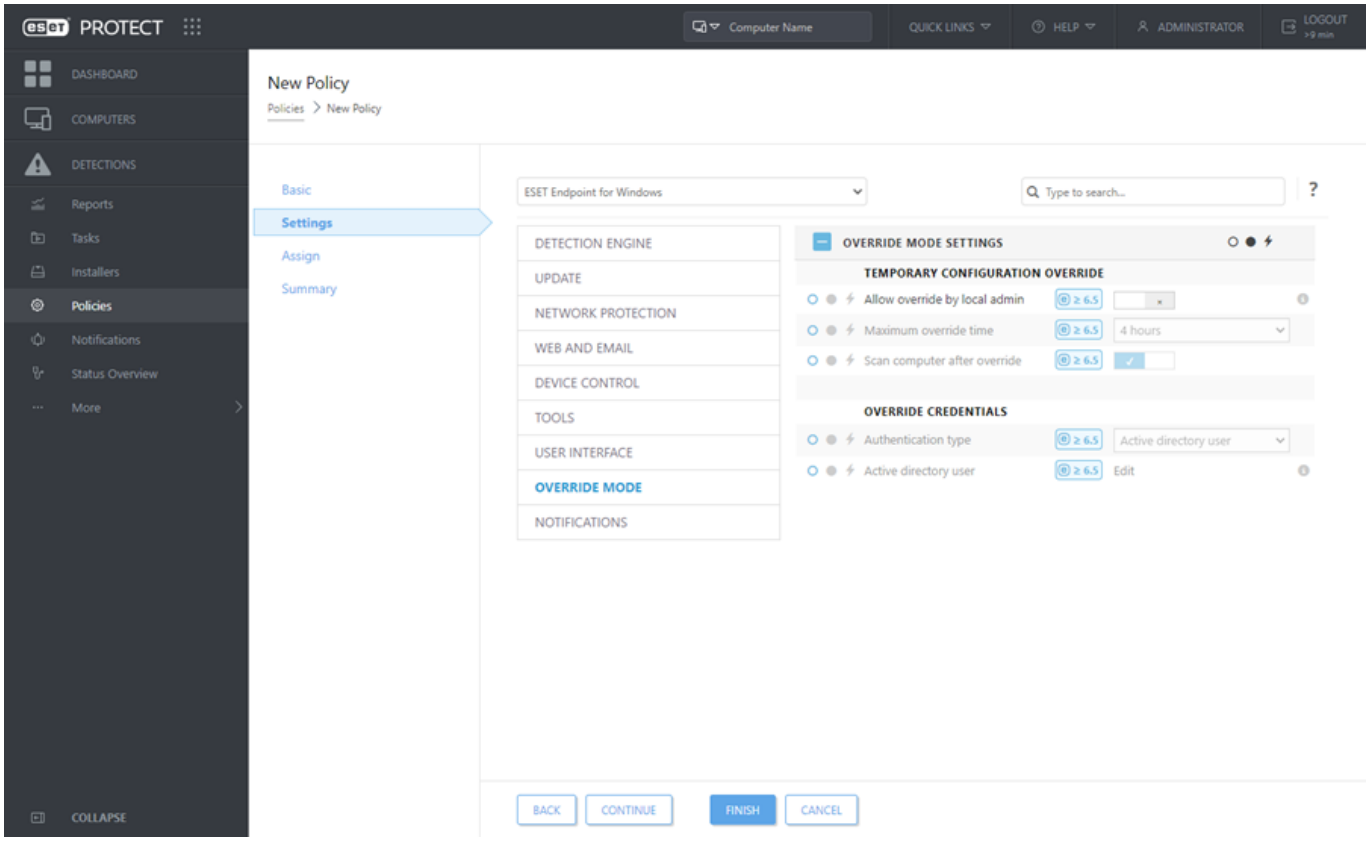
Limitações do modo de substituição

- Não é possível interromper o modo de substituição a partir do Console da Web ESET PROTECT depois dele ser ativado. A substituição é desativada somente depois que o tempo de substituição expirar, ou depois de ser desligada pelo próprio cliente.
- O usuário que está usando o Modo de substituição precisa também ter direitos de administrador do Windows. Caso contrário, o usuário não pode salvar as alterações nas configurações do produto ESET.
- A autenticação de grupo do Active Directory é compatível com produtos gerenciados selecionados da versão:

ESET Endpoint Security	7.0.2100.4 e versões posteriores.
ESET File Security para Microsoft Windows Server	6.5.12013.0 e versões posteriores.
ESET Mail Security para IBM Domino	6.5.14020.0 e versões posteriores.
ESET Mail Security para Microsoft Exchange Server	6.5.10019.1 e versões posteriores.
ESET Server Security para Windows	8.0 e versões posteriores.

Para definir o **Modo de Substituição**:

1. Navegue para **Políticas** > **Nova política**.
2. Na seção **Básico**, digite um **Nome** e **Descrição** para esta política.
3. Na seção **Configurações**, selecione **ESET Endpoint for Windows**.
4. Clique em **Modo de Substituição** e configure as regras para o modo de substituição.
5. Na seção **Atribuir**, selecione o computador ou grupo de computadores nos quais esta política será aplicada.
6. Revise as configurações na seção **Resumo** e clique em **Concluir** para aplicar a política.



Se *John* tiver um problema com suas configurações endpoint bloqueando alguma funcionalidade importante ou acesso à web em sua máquina, o Administrador pode permitir que *John* substitua sua política endpoint existente e ajuste as configurações manualmente em sua máquina. Depois disso, essas novas configurações podem ser solicitadas pela ESET PROTECT para que o Administrador possa criar uma nova política a partir delas.

Para fazer isso, siga as etapas a seguir:

1.Navegue para **Políticas** > **Nova política**.

2.Preencha os campos **Nome** e **Descrição**. Na seção **Configurações**, selecione **ESET Endpoint for Windows**.

3.Clique em **Modo de Substituição**, ative o modo de substituição por uma hora e selecione *John* como o usuário AD.

4.Atribua a política ao *computador do John* e clique em **Concluir** para salvar a política.

5.*John* precisa ativar o **Modo de Substituição** em seu endpoint ESET e alterar as configurações manualmente em sua máquina.

6.No Console da Web ESET PROTECT, navegue até **Computadores**, selecione *computador do John* e clique em **Mostrar detalhes**.

7.Na seção **Configuração**, clique em **Solicitar configuração** para agendar uma tarefa de cliente para obter a configuração do cliente assim que for possível.

8.Depois de um curto tempo, a nova configuração vai aparecer. Clique no produto cujas configurações você deseja salvar e clique em **Abrir Configuração**.

9.Você pode revisar as configurações e em seguida clicar em **Converter para Política**.

10. Preencha os campos **Nome** e **Descrição**.

11. Na seção **Configurações** é possível modificar as configurações, se necessário.

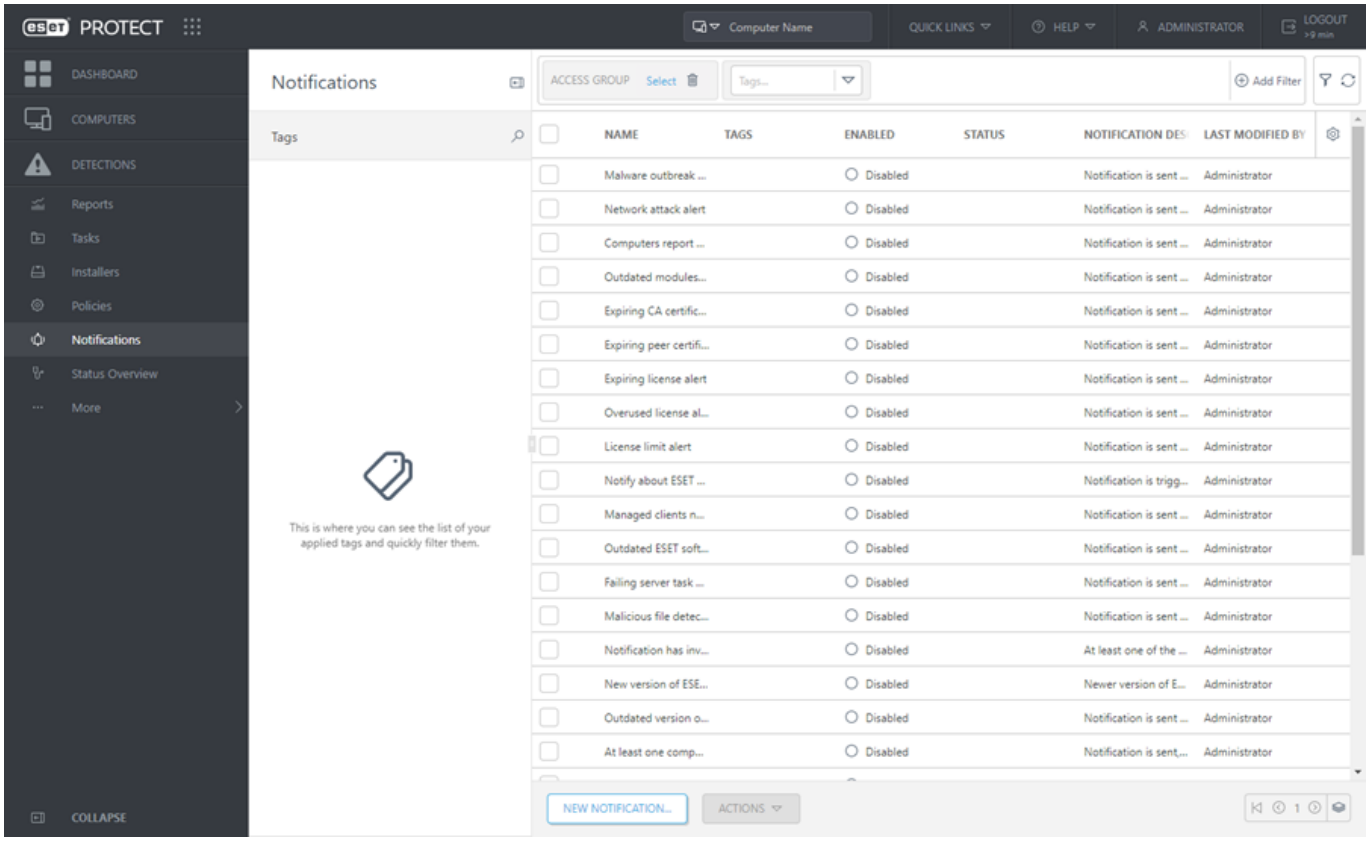
12. Na seção **Atribuir** você pode atribuir esta política ao *computador do John* (ou outros).

13. Clique em **Concluir** para salvar as configurações.

14. Não esqueça de remover a política de substituição assim que ela não for mais necessária.

Notificações

Notificações são essenciais para manter o controle do estado geral da sua rede. Quando um novo evento ocorre (com base na configuração de notificação), você será notificado através de um método definido (uma interceptação SNMP ou mensagem por e-mail ou se for enviado para o servidor syslog), e você pode responder de acordo. Você pode configurar notificações automáticas com base em eventos específicos, como detecções, endpoints desatualizados, e muito mais. Veja a Descrição da notificação para mais informações sobre uma notificação específica e seu acionador.



Para criar uma nova notificação, clique em **Nova notificação** na parte inferior da página.

Selecione uma notificação existente e clique em **Ações** para gerenciar a notificação.

Para adicionar critérios de filtragem, clique em **Adicionar filtro** e selecione um item da lista. Digite as strings de pesquisa ou selecione os itens no menu suspenso no(s) campo(s) de filtro(s) e pressione **Enter**. Filtros ativos são destacados em azul.

Notificações, usuários e permissões

O uso das Notificações é restrito pelas permissões do usuário atual. Cada vez que a notificação é executada, existe um usuário executando cujas permissões são levadas em conta. O usuário executando sempre é aquele que editou a notificação pela última vez. Um usuário só pode ver notificações que estejam contidas em um grupo para o qual ele tenha permissões de **Leitura**.

Para que a notificação funcione bem, é necessário que o usuário executando tenha permissões suficientes para todos os objetos referenciados (dispositivos, grupos, modelos). Tipicamente, permissões **Leitura** e **Uso** são necessárias. Se o usuário não tiver essas permissões, ou se vier a perdê-las, a notificação vai falhar. Notificações com falha são destacadas com laranja e vão acionar um email para notificar o usuário.

Criar notificação - Para criar uma notificação o usuário deve ter permissões de **Gravação** para notificações em seu grupo inicial. Uma nova notificação é criada no grupo inicial do usuário.

Modificar notificação - Para ser capaz de modificar uma notificação, o usuário deve ter permissões de **Gravação** para notificações em um grupo onde a notificação está localizada.

Remover notificação - Para ser capaz de excluir uma notificação, o usuário deve ter permissões de **Gravação** para notificações em um grupo onde a notificação está localizada.

John, cujo **Grupo inicial** é o *Grupo do John*, quer remover (ou modificar) a *Notificação 1*. A notificação foi originalmente criada por *Larry*, portanto está automaticamente contida no grupo inicial de Larry, o *Grupo do Larry*. As seguintes condições devem ser atendidas para que *John* remova (ou modifique) a *Notificação 1*:
- *John* deve receber a atribuição de um conjunto de permissões com permissões de **Gravação** para as **notificações**
- O conjunto de permissões deve ter o *Grupo do Larry* sob os **Grupos estáticos**

Grupo doméstico – O grupo doméstico é detectado automaticamente com base no conjunto de permissões atribuído do usuário atualmente ativo.

Exemplo de cenário:
A conta de usuário atualmente ativa tem o direito de acesso de **Gravação** para a **Tarefa de cliente de Instalação de software** e a conta do **Grupo doméstico** é "Department_1". Quando o usuário criar uma nova **Tarefa de cliente de instalação de software**, "Department_1" será selecionado automaticamente como o **Grupo doméstico** da tarefa de cliente.

Se o Grupo doméstico pré-selecionado não atender às suas expectativas, você pode selecionar o Grupo doméstico manualmente.

Clonagem e VDI

Existem três notificações preparadas para notificar o usuário sobre eventos relacionados a clonagem, ou o usuário pode criar uma nova notificação personalizada.

Filtros e personalização de layout

Você pode personalizar a exibição da tela atual do console web:

- Gerenciar o painel lateral e a tabela principal.
- Adicionar filtro e predefinições de filtro. Você pode usar marcações para filtrar os itens exibidos.

Gerenciar notificações

As notificações são gerenciadas na seção **Notificações**. Você pode realiza as ações a seguir:

- Clique em **Nova notificação** para criar uma nova notificação.
- Clique em uma notificação existente e selecione uma ação no menu suspenso:

Mostrar detalhes	Mostrar detalhes da notificação, incluindo sua configuração e configurações de distribuição. Clique em **Ver visualização de mensagem** para ver a visualização da notificação.
Relatório de auditoria	Exibe o Relatório de auditoria para o item selecionado.
Marcações	Editar marcações (atribuir, remover atribuição, criar, remover).
Ativar / Desativar	Alterar o status da notificação. A notificação desativada não é avaliada. Todas as notificações estão configuradas como **Desativado** por padrão.
Editar	Configuração e distribuição da notificação.
Duplicar	Criar uma notificação duplicada em seu grupo inicial.
Excluir	Remover a notificação.
Grupo de acesso > **Mover**	Mova o objeto para outro grupo estático onde ele está disponível para usuários com direitos suficientes para o grupo de destino. Alterar o Grupo de acesso é útil ao resolver problemas de acesso com outros usuários. O Grupo de acesso define o grupo estático do objeto e o acesso ao objeto com base nos direitos de acesso do usuário.

O ESET Enterprise Inspector e o ESET Dynamic Threat Defense foram renomeados para ESET Inspect e ESET LiveGuard Advanced.
Você pode precisar resolver os problemas causados pela renomeação se você atualizou do ESET PROTECT 9.0 e versões anteriores e tem relatórios, grupos dinâmicos, notificações ou outros tipos de regras que filtram por ESET Dynamic Threat Defense ou ESET Enterprise Inspector.

Nova notificação

Básico

Insira um **Nome** e **Descrição** para sua notificação para fazer com que seja mais fácil filtrar entre diferentes notificações.

Se você estiver editando uma notificação ativada e quiser desativar a notificação, clique na alternância e ela vai mudar o status para **Desativado**.

Configuração

Evento – Existem três tipos básicos de evento que podem acionar uma notificação. Cada tipo de evento oferece opções diferentes na seção **Configurações**. Selecione um dos seguintes tipos de evento:

- Eventos em computadores ou grupos gerenciados
- Alterações de status do servidor
- Alterações no grupo dinâmico

Configurações avançadas - Alternância

A alternância permite a você configurar regras avançadas que determinam quando uma notificação é acionada. Consulte alternância para obter mais informações.

Distribuição

Configure as configuração de distribuição para as notificações. Configure seu servidor SMTP se quiser enviar notificações por email.

Eventos em computadores ou grupos gerenciados

Esta opção é usada para as notificações não associadas a um grupo dinâmico, e sim baseadas em eventos de sistema filtrados do registro do evento. Selecione uma categoria de relatório na qual a notificação será baseada e um operador lógico para filtros.

Categoria - Escolha entre as categorias de evento a seguir:

- **Detecção de firewall**
- **Detecção de antivírus**
- **Rastrear**
- **HIPS**
- **ESET Inspect alertas**
- **Arquivo bloqueado**
- **Computador conectado pela primeira vez**
- **Identidade do computador recuperada**
- **Pergunta de clonagem de computador criada**
- **Novo cliente MSP encontrado**

De acordo com a categoria selecionada, existe uma lista de eventos disponíveis em **Configurações** > **Filtrar por**. Os valores nos filtros são comparados diretamente com os eventos enviados por clientes. Não há uma lista definida de valores disponíveis.

Grupos estáticos monitorados – clique em **Selecionar** ou **Criar novo grupo** e selecione grupos estáticos para limitar os dispositivos monitorados sobre os que você deseja ser notificado. Se você não selecionar nenhum grupo estático, você receberá notificações de todos os dispositivos aos quais você tem acesso.

Ignorar dispositivos colocados em mudo – se você selecionar essa caixa de seleção, você não receberá notificações de computadores colocados em mudo (computadores colocados em mudo serão excluídos das notificações).

Configurações

Em **Configurações**, selecione um **Operador** e valores para o filtro (**Filtrar por**). Apenas um operador pode ser selecionado e todos os valores serão avaliados juntos usando aquele operador. Clique em **Adicionar filtro** para adicionar um novo valor para o filtro.

Alterações de status do servidor

Essa opção notifica alterações do estado do objeto. O intervalo de notificação depende da **Categoria**selecionada. Você pode selecionar uma das configurações existentes ou definir seus próprios parâmetros.

Carregar configurações pré-definidas - Clique em Selecionar para escolher entre as configurações existentes, ou deixe em branco. Clique em Limpar para limpar a seção de Configurações.

Categoria - Selecione uma categoria de objetos. De acordo com uma categoria selecionadas, os objetos são exibidos na seção Configurações abaixo.

Grupos estáticos monitorados – para categorias onde a notificação está relacionada a um cliente (Clientes gerenciados, software instalado) você pode clicar em **Selecionar** ou **Criar novo grupo** e selecionar grupos estáticos para limitar os dispositivos monitorados sobre os quais você deseja ser notificado. Se você não selecionar nenhum grupo estático, você receberá notificações de todos os dispositivos aos quais você tem acesso.

Configurações

Selecione um **Operador** e valores para o filtro (**Filtrar por**). Apenas um operador pode ser selecionado e todos os valores serão avaliados juntos usando aquele operador. Clique em **Adicionar filtro** para adicionar um novo valor para o filtro. Se mais filtros estiverem selecionados, a execução de uma notificação é avaliada com o operador *AND* (a notificação é enviada apenas se todos os campos do filtro forem avaliados como *verdadeiros*).

> Alguns filtros podem causar uma notificação muito frequente. Recomendamos usar a Alternância para agregar as notificações.

Lista de valores de filtro disponíveis

Categoria	Valor	Comentário
Certificados CA	Intervalo de tempo relativo (Autoridade de certificação válida até, Certificado de mesmo nível válido até)	Selecione um intervalo de tempo relativo.
Certificados de mesmo nível		
Clientes gerenciados	Intervalo de tempo relativo (Última conexão)	Selecione um intervalo de tempo a ser monitorado para **Conectado pela última vez**.
	Porcentagem de computadores não conectando	Um valor entre 0 e 100. Ele pode ser usado apenas combinado com o filtro **Intervalo de tempo relativo**.
Licenças	Intervalo de tempo relativo (Data de expiração de licença)	Selecione um intervalo de tempo a ser monitorado para a expiração da licença.
	Porcentagem de uso da licença	Um valor entre 0 e 100 foi calculado com base nas **Unidades** de licença usadas para ativação. Para produtos ESET Mail Security, o uso da licença é calculado com base nas **Subunidades** usadas para ativação.
	Tipo de usuário de licença	Selecione **Empresa**, **Cliente MSP** ou **Site**.
Tarefas de cliente	Tarefa	Selecione as tarefas para o filtro de validade. Se nada estiver selecionado, tudo será considerado.
	A tarefa é inválida	Selecione **Sim** / **Não**. Se você selecionar **Não**, a notificação será acionada quando pelo menos uma das tarefas da seleção (filtro **Tarefa**) for inválida.
Tarefas do servidor	Contagem (Falhou)	Número de falhas de tarefas selecionadas.
	Último status	Último status reportado da tarefa selecionada.
	Tarefa	Selecione tarefas para esse filtro. Se nada estiver selecionado, tudo será considerado.
	A tarefa é inválida	Selecione **Sim** / **Não**. Se você selecionar **Não**, a notificação será acionada quando pelo menos uma das tarefas da seleção (filtro **Tarefa**) for inválida.
	Intervalo de tempo relativo (Hora da ocorrência)	Selecione um intervalo de tempo a ser monitorado.
Software instalado	Nome do aplicativo	Nome completo do aplicativo Se mais um aplicativo for monitorado, use o operador **in** e adicione mais campos.
	Fornecedor do aplicativo	Nome completo do fornecedor Se mais fornecedores forem monitorados, use o operador **in** e adicione mais campos.
	Verificar status da versão	Se uma **Versão desatualizada** for selecionada, a notificação é acionada quando pelo menos um aplicativo está desatualizado.
Pares de rede	Mesmo nível	Se você tiver mais Servidores ESET PROTECT na sua rede, selecione um deles.
	Estado do Servidor	Se o Servidor ESET PROTECT estiver sobrecarregado pela gravação de relatórios, ele muda de estado: • **Normal** - Resposta imediata do servidor • **Limitado** - o servidor responde ao agente uma vez em uma hora • **Sobrecarregado** - o servidor não está respondendo aos agentes
Notificações	Notificação	Selecione a notificação para este filtro. Se nada estiver selecionado, tudo será considerado.
	A notificação está ativada	Selecione **Sim** / **Não**. Se tiver selecionado **Não**, a notificação é acionada quando pelo menos uma notificação da seleção (filtro **Notificação**) estiver desativada.
	A notificação é válida	Selecione **Sim** / **Não**. Se tiver selecionado **Não**, a notificação é acionada quando pelo menos uma notificação da seleção (filtro **Notificação**) for inválida.

Alterações no grupo dinâmico

A notificação será enviada quando a condição for cumprida. Só é possível selecionar uma condição a ser monitorada para um determinado grupo dinâmico.

Grupo dinâmico - Selecione um grupo dinâmico a ser avaliado.

Configurações - Condições

Selecione o tipo de condição que vai acionar uma notificação.

- **Notificar sempre que o conteúdo do grupo dinâmico for alterado** – Ative para ser notificado quando membros do grupo selecionado forem adicionados, removidos ou alterados.

> O ESET PROTECT verifica o Grupo dinâmico uma vez a cada 20 minutos.
> Por exemplo, se a primeira verificação acontece às 10:00, as outras verificações são realizadas às 10:20, 10:40, 11:00. Se o conteúdo do Grupo dinâmico mudar às 10:05 e depois mudar de novo às 10:13, durante a próxima verificação realizada às 10:20 o ESET PROTECT não reconhece a mudança anterior e ela não é notificada.

- **Notificar quando o tamanho do grupo ultrapassar um número específico** – selecione o operador de tamanho do grupo e o limite para a notificação:
  - **Maior que** - Envia uma notificação quando o tamanho do grupo é maior que o limite.
  - **Menor que** - Envia uma notificação quando o tamanho do grupo é menor que o limite.
- **Notificar quando o crescimento do grupo ultrapassar uma taxa específica** – define um limite e período de tempo que vai acionar uma notificação. Você pode definir um número de clientes ou uma porcentagem de clientes (membros do grupo dinâmico). Define o período de tempo (em minutos, horas ou dias) para a comparação com o novo estado. Por exemplo, há sete dias havia 10 clientes com produtos de segurança desatualizados, mas o Limite estava definido como 20. Se o número de clientes com um produto de segurança desatualizado chegar a 30, você será notificado.
- **Notificar quando o número de clientes no grupo dinâmico mudar em comparação com outro grupo** – se o número de clientes em um Grupo Dinâmico observado for alterado de acordo com um grupo de comparação (estático ou dinâmico), uma notificação será enviada. L - Define um limite que vai acionar o envio de uma notificação.

> Você pode atribuir uma notificação apenas ao Grupo dinâmico onde você tem permissões suficientes. Para ver um grupo dinâmico é preciso ter permissão de **Leitura** para seu grupo estático principal.

Distribuição

Você precisa escolher pelo menos um meio de distribuição.

Enviar interceptação SNMP

Envia uma interceptação SNMP. A interceptação SNMP notifica o servidor usando uma mensagem SNMP não

solicitada. Para mais informações, consulte Como configurar um Serviço de interceptação SNMP.

Enviar email

Envia uma mensagem de email com base em suas configurações de email. Por padrão, o e-mail de notificação está em formato HTML com um logotipo ESET PROTECT no cabeçalho. Você pode ter um logotipo personalizado e diferentes posições de logotipo de acordo com suas configurações de personalização (**logotipo claro em segundo plano**).

Se **Enviar email** estiver selecionado, insira pelo menos um destinatário de email.

- **Endereços de email** - Insira o endereço de email dos destinatários das mensagens de notificação.
- Clique em + adiciona um novo campo de endereço.
- Para adicionar vários usuários de uma vez, clique em **Mais** > **Adicionar usuários** (adicione o endereço do usuário dos Usuários do computador) ou em **Mais** > **Importar CSV** ou **Colar da área de transferência** (Importe uma lista personalizada de endereços de um arquivo CSV estruturado com delimitadores).
- **Mais** > **Copiar da área de transferência** – Importa uma lista personalizada de endereços separados por delimitadores personalizados. Esse recurso funciona de forma similar à importação de CSV.

Enviar Syslog

Você pode usar o ESET PROTECT para enviar notificações e mensagens de eventos para o servidor Syslog. Além disso, exportar relatórios de um produto ESET do computador cliente e enviá-los ao servidor Syslog. **Gravidade do Syslog** - Escolha o nível de gravidade no menu suspenso. Então, notificações vão aparecer com a gravidade selecionada no servidor Syslog.

Campos básicos na distribuição

- **Visualização de mensagem** - Uma visualização de mensagem que vai aparecer na notificação. A visualização contém configurações definidas em forma de texto. Você pode personalizar o conteúdo e o assunto da mensagem e usar variáveis que serão convertidas em valores reais quando a notificação for gerada. Isto é opcional, mas é recomendado para uma melhor filtragem de notificações e para uma visão geral.
  - **Assunto** - O assunto de uma mensagem de notificação. Clique no ícone para editar o conteúdo. Um assunto preciso pode melhorar a classificação e filtragem da mensagem.
  - **Conteúdo** - Clique no ícone para editar o conteúdo. Depois de editar o conteúdo, você pode clicar no ícone para redefinir o conteúdo padrão da mensagem.

> Para **Eventos em computadores ou grupos gerenciados**, você pode adicionar variáveis ao **Assunto** e **Conteúdo** para incluir informações específicas na notificação. Clique em **Adicionar variável** ou comece a digitar $ para exibir a lista de variáveis.

- **Geral**
  - **Local** – Idioma da mensagem padrão. O conteúdo da mensagem não é traduzido.

o**Fuso horário** - Define o fuso horário para a variável **Hora de ocorrência** `${timestamp}`, que pode ser usado na mensagem personalizada.

Se o evento acontece às 3:00 do horário local, o horário local é UTC+2, o fuso horário selecionado é UTC+4, o horário reportado na notificação será 5:00.

Clique em **Concluir** para criar um novo modelo com base no modelo que você está editando.

Como configurar um Serviço de interceptação SNMP

Para receber mensagens SNMP com sucesso, o serviço de intercepção SNMP precisa estar configurado. Siga as etapas de configuração abaixo conforme for apropriado para seu sistema operacional:

WINDOWS

Pré-requisitos

- O serviço do **Protocolo de gerenciamento de rede simples** deve ser instalado na máquina onde o Servidor ESET PROTECT está instalado, assim como na máquina onde o software de intercepção SNMP será instalado.
- Ambos os computadores (acima) devem estar na mesma subrede.
- O serviço SNMP deve ser configurado no computador do Servidor ESET PROTECT.

Configuração de Serviço SNMP (Servidor ESET PROTECT)

1.Pressione a tecla Windows + R para abrir uma caixa de diálogo, digite Services.msc no campo **Abrir** e pressione **Enter**. Pesquise pelo SNMP Service.

2.Abra a guia **Intercepções**, digite **público** no campo **Nome da comunidade** e clique em **Adicionar à lista**.

3.Clique em **Adicionar**, digite o **Nome do host, endereço IP ou IPX** do computador onde o software de bloqueio SNMP está instalado no campo apropriado e clique em **Adicionar**.

4.Continue para a guia **Segurança**. Clique em **Adicionar** para exibir a janela **Configuração de serviço SNMP**. Digite **público** no campo **Nome da comunidade** e clique em **Adicionar**. Os direitos serão definidos para **SOMENTE LEITURA** e isso é ok.

5.Certifique-se de que **Aceitar pacotes SNMP de qualquer host** está selecionado e clique em **OK** para confirmar. O serviço SNMP não é configurado.

Configuração de software de interceptação SNMP (cliente)

1.Certifique-se de que o Serviço SNMP está instalado na máquina do cliente.

2.Instale um aplicativo de intercepção do receptor.

3.Configure o aplicativo de intercepção do receptor para receber intercepções SNMP do Servidor ESET PROTECT (isso pode incluir endereço IP do Servidor ESET PROTECT e configurações de porta).

4.Certifique-se de que o firewall nas máquinas do cliente permitem a comunicação de rede para comunicação SNMP definida na etapa anterior.

5.O aplicativo de intercepção do receptor agora permite o recebimento de mensagens do Servidor ESET PROTECT.

A Intercepção SNMP não é compatível com o Equipamento Virtual ESET PROTECT.

LINUX

1. Instale o pacote snmpd ao executar um dos comandos a seguir:
`apt-get install snmpd snmp`(distribuições Debian, Ubuntu)
`yum install net-snmp` (Distribuições Red Hat, CentOS)

2. Abra o arquivo */etc/default/snmpd* e faça as edições de atributo a seguir:

```
#SNMPDOPTS='-Lsd -Lf /dev/null -u snmp -g snmp -I -smux -p /var/run/snmpd.pid'
```

Adicionar # vai desativar esta linha completamente.

```
SNMPDOPTS='-Lsd -Lf /dev/null -u snmp -I -smux -p /var/run/snmpd.pid -
c /etc/snmp/snmpd.conf'
```

Adicione esta linha para o arquivo.

```
TRAPDRUN=yes
```
Altere o atributo do trapdrun para yes.

3. Criar um backup do arquivo snmpd.conf original. O arquivo será editado mais tarde.

```
mv /etc/snmp/snmpd.conf /etc/snmp/snmpd.conf.original
```

4. Crie um novo arquivo snmpd.conf e adicione essas linhas:

```
rocommunity public
syslocation "Testing ESET PROTECT"
syscontact admin@PROTECT.com
```

5. Abra o arquivo */etc/snmp/snmptrapd.conf* e adicione a linha a seguir no final do arquivo:

```
authCommunity log,execute,net public
```

6. Digite o seguinte comando para iniciar os serviços do gerenciador SNMP e fazer o registro em relatório de intercepções realizadas:

```
/etc/init.d/snmpd restart
```

ou

```
service snmpd restart
```

7. Para verificar se a intercepção está funcionando e coletando as mensagens, execute o comando a seguir:

```
tail -f /var/log/syslog | grep -i TRAP
```

Visão geral do status

ESET PROTECT Servidor realiza verificações de diagnóstico periódicas. Use a **Visão geral do status** para ver as estatísticas de uso e o status geral do seu ESET PROTECT. Também pode ajudá-lo com a configuração inicial do ESET PROTECT. Clique em **Visão geral do status** para ver as informações detalhadas de status sobre o ESET PROTECT.

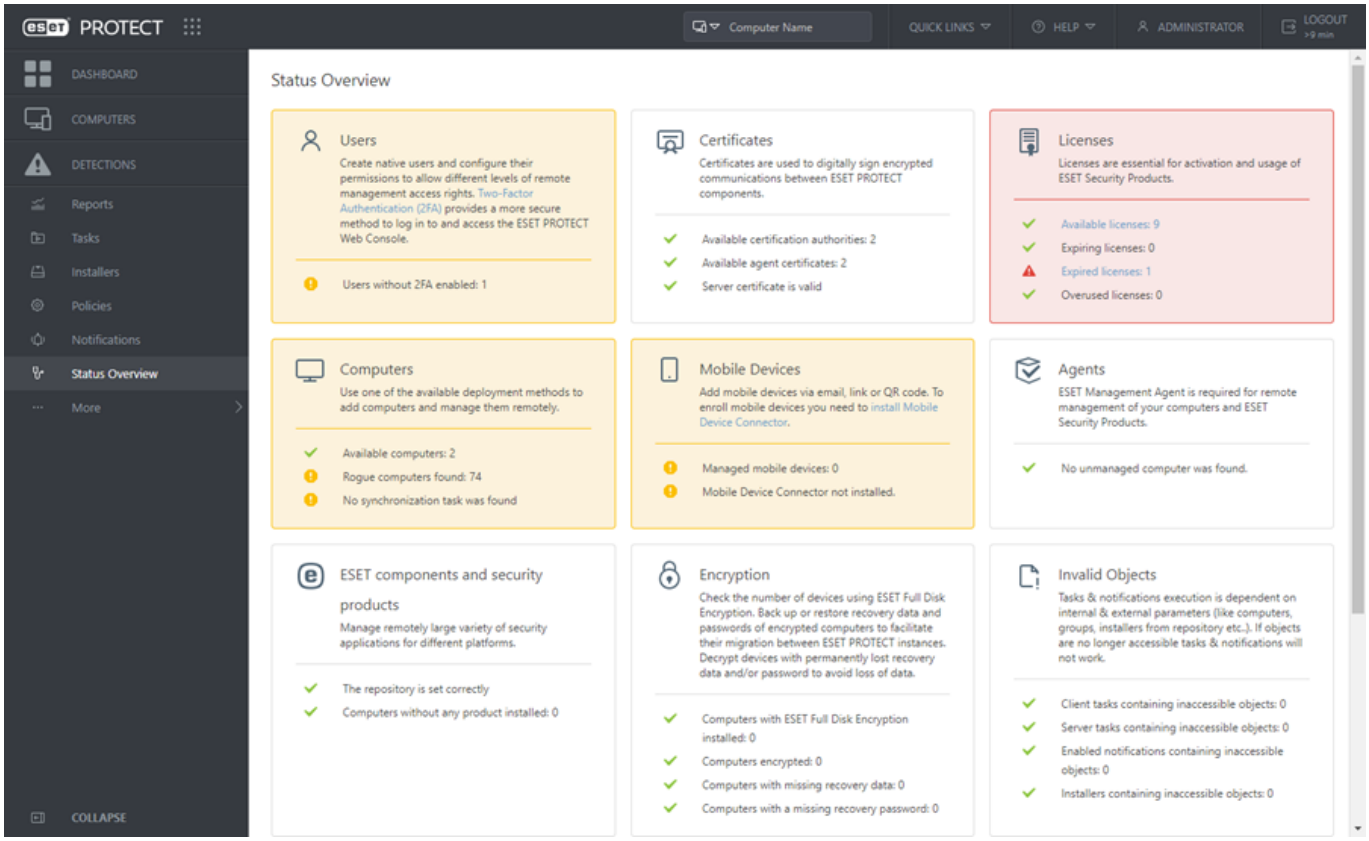
Clique em um bloco de seção para exibir uma barra de tarefas na direita com as ações. Cada bloco de seção pode ter uma de várias cores, com base no status de gravidade mais alto dos itens incluídos:

Cor	Ícone	Significado do ícone	Descrição
Verde		OK	Todos os itens na seção não tem nenhum problema.
Amarelo		Alerta	Pelo menos um item na seção está marcado com um alerta
Vermelho		Erro	Pelo menos um item na seção está marcado com um erro.
Cinza		Conteúdo indisponível	O conteúdo está indisponível devido a direitos de acesso insuficientes do usuário do Console ESET PROTECT. O administrador precisa definir permissões adicionais para o usuário, ou você pode fazer login como outro usuário com os direitos de acesso adequados.
Azul		Informações	Há uma pergunta relacionada aos computadores conectados (consulte a descrição da seção **Perguntas** abaixo).

Visão geral do status contém as seções a seguir:

Usuários	Cria usuários diferentes e configura suas permissões para permitir níveis diferentes de gerenciamento no ESET PROTECT. A conta padrão do Administrator ESET PROTECT foi criada durante a instalação. Não recomendamos usar a conta de Administrador ESET PROTECT padrão como uma conta de usuário normal. Clique em **Exibir usuários** e crie uma nova conta de usuário nativo com autenticação em dois fatores e use-a como a conta padrão no ESET PROTECT.
Certificados	Se quiser usar certificados diferentes do que os padrão fornecidos pela ESET PROTECT, você pode criar Autoridades de Certificação e Certificados de mesmo nível para componentes individuais ESET PROTECT para permitir a comunicação com o Servidor ESET PROTECT.
Licenças	ESET PROTECT usa o sistema de licenciamento ESET. Selecione o método que deseja usar para adicionar Licença(s) para ativação dos componentes ESET PROTECT e produtos de segurança ESET em computadores do cliente.
Computadores	• **Adicionar computador** – adiciona computadores na sua rede à estrutura ESET PROTECT. Você pode Adicionar computadores e Dispositivos móveis manualmente ou importar uma lista de dispositivos. • **Adicionar computadores invasores** - Importa automaticamente os computadores usando o ESET RD Sensor. • **Nova tarefa de sincronização** - Execute a Sincronização de grupo estático com o Active Directory, LDAP, VMware, etc.
Dispositivos móveis	• **Download** – Se o MDC não estiver instalado, você poderá fazer o download do instalador do Mobile Device Connector na página web da ESET. • **Adicionar dispositivos móveis** – Registre os dispositivos móveis por e-mail, por link ou código QR ou como Proprietário do dispositivo.

Agentes	• **Nova política** – Cria uma nova política para o Agente ESET Management para alterar o intervalo de conexão. • **Implantar Agente** – Existem várias formas de implantar o Agente ESET Management em computadores do cliente na sua rede.
Componentes ESET e produtos de segurança	• **Nova política** - Crie uma nova política para alterar a configuração do produto de segurança da ESET instalado nos computadores do cliente. • **Configurar repositório** - Muda as Configurações do ESET PROTECT servidor. • **Instalar software** - com o Agente ESET Management implantado, você pode instalar o software diretamente do repositório ESET ou especificar o local de um pacote de instalação (URL ou uma pasta compartilhada).
Criptografia	Se você gerenciar dispositivos criptografados com ESET Full Disk Encryption, use essas opções para evitar a perda de dados de recuperação: • **Exportar** – exporta seus dados de recuperação ESET Full Disk Encryption atuais antes de migrar computadores gerenciados criptografados. • **Importar** – importar os dados de recuperação ESET Full Disk Encryption depois de migrar computadores gerenciados criptografados para uma nova instância ESET PROTECT.
Objetos inválidos	Contém a lista de tarefas do cliente e servidor, acionadores, notificações ou instaladores com referências a objetos inacessíveis ou inválidos. Clique em qualquer um dos campos de resultado para ver um menu com a lista de objetos selecionados.
Serviços externos	ESET PROTECT pode ser configurado para conectar a serviços externos para oferecer a funcionalidade completa. • **Configurar repositório** – O repositório contém arquivos do instalador para outros produtos de segurança ESET que você pode instalar usando a tarefa de instalação. O repositório é configurado em Mais > Configurações. Se for necessário, você pode criar um repositório off-line. • **Configurar atualizações** - Atualizações são necessárias para manter o ESET PROTECT atualizado. As atualizações estão disponíveis apenas se o ESET PROTECT tiver importado uma licença de produto comercial não expirada. Você pode alterar suas configurações de atualização em **Mais** > Configurações. • **Configurações SMTP** - Configure o ESET PROTECT para usar seu Servidor SMTP existente para enviar mensagens de email, por exemplo, Notificações, emails de inscrição de dispositivo móvel, Relatórios, etc.
Perguntas	Quando um dispositivo clonado ou uma alteração de hardware é detectada em um dispositivo do cliente, uma pergunta é listada. Leia mais sobre resolver computadores clonados.
Status MSP	Se você importar uma conta MSP, há um bloco com status MSP disponível.



Mais

A seção ⋯ **Mais** é o componente de configuração avançada do ESET PROTECT. Esta seção contém ferramentas que o administrador pode usar para gerenciar soluções de segurança de cliente, bem como as Configurações ESET PROTECT. Você pode usar essas ferramentas para configurar o ambiente de rede de maneira que não exija muita manutenção.

A seção ⋯ **Mais** contém os itens a seguir:

Detecções
- Arquivos enviados
- Exclusões
- Quarentena

Computadores
- Usuários do computador
- Modelos de grupo dinâmico

Licenças
- Gerenciamento de licenças

Direitos de acesso
- Usuários
- Definições de permissão

Certificados
- Certificados de mesmo nível
- Autoridades de certificação

Auditoria de atividade
- Relatório de auditoria

Admin
o Configurações

Arquivos enviados

O ESET LiveGuard Advanced é um serviço que fornece proteção avançada contra detecções nunca antes vistas. Um usuário do ESET PROTECT pode enviar arquivos para análise de malware no ambiente de nuvem e receber um relatório sobre o comportamento da amostra. Consulte o Guia do Usuário ESET LiveGuard Advanced para instruções passo a passo. Você pode enviar remotamente um arquivo diretamente do console web ESET PROTECT em **Detecções** > clique em um item da categoria **Arquivos bloqueados** > **Enviar arquivo para ESET LiveGuard**.

A janela **Arquivos enviados** oferece uma lista de todos os arquivos enviados para os servidores ESET. Isso inclui arquivos enviados automaticamente para o ESET LiveGrid® de computadores clientes (caso o ESET LiveGrid® esteja ativado no produto de segurança ESET) e arquivos enviados para o ESET LiveGuard Advanced manualmente do console web ESET PROTECT.

Janela de arquivos enviados

Você pode ver a lista de arquivos enviados e informações relacionadas a esses arquivos, como o usuário que enviou o arquivo e a data de envio. Clique em um arquivo enviado e selecione uma ação no menu suspenso.

Mostrar detalhes	Clique para ver a guia **envio mais recente**.
Exibir comportamento	Veja o relatório de análise comportamental para uma determinada amostra. Esta opção está disponível apenas para arquivos enviados para o ESET LiveGuard Advanced.
Criar exclusão	Selecione um ou mais arquivos e clique em **Criar Exclusão** para adicionar uma exclusão de detecção para os arquivos selecionados a uma política existente.

Janela de detalhes do arquivo

A janela de Detalhes do arquivo contém uma lista de detalhes do arquivo para o arquivo selecionado. Se um arquivo for enviado várias vezes, os detalhes do envio mais recente são exibidos.

Status	Resultado da análise de malware. **Desconhecido** - o arquivo não foi analisado. **Limpo** - nenhum dos mecanismos de detecção avaliou o arquivo como malware. **Suspeito**, **Altamente suspeito** - O arquivo exibe comportamento suspeito mas pode não ser malware. **Nocivo** - o arquivo exibe comportamento perigoso.
Estado	Estado da análise. O status **Reanalisando** significa que o resultado está disponível, mas pode mudar depois de mais análise.
Processado pela última vez em	Um arquivo pode ser enviado para análise várias vezes, de mais de um computador. Essa é a data e hora da última análise.
Enviado em	A hora do envio.
Comportamentos	Clique em Exibir comportamento para ver a análise do ESET LiveGuard Advanced. Isso só é válido se o computador que enviou o arquivo tiver uma licença ESET LiveGuard Advanced válida.

Computador	O nome do computador de onde o arquivo foi enviado.
Usuário	Usuário do computador que enviou o arquivo.
Motivo	O motivo pelo qual o arquivo foi enviado.
Enviado para	Parte da nuvem ESET que recebeu o arquivo. Nem todo arquivo enviado é analisado em busca de malware.
Hash	Hash SHA1 do arquivo enviado.
Tamanho	Tamanho do arquivo enviado.
Categoria	Categoria do arquivo. A categoria pode não seguir a extensão do arquivo.

Para obter mais informações sobre relatórios comportamentais ESET LiveGuard Advanced, consulte a documentação.

Filtros e personalização de layout

Você pode personalizar a exibição da tela atual do console web:

- Gerenciar o painel lateral e a tabela principal.
- Adicionar filtro e predefinições de filtro. Você pode usar marcações para filtrar os itens exibidos.

Exclusões

Nesta seção, você pode ver a lista de todas as exclusões criadas para detecções **Antivírus** e regras de **Firewall** IDS. Esta nova seção contém todas as exclusões, aumenta sua visibilidade e simplifica seu gerenciamento.

Clique em uma exclusão ou selecione mais exclusões e clique no botão **Detecção** para gerenciar as exclusões:

- **Alterar atribuição** – Altera os computadores de destino nos quais a exclusão será aplicada.
- **Mostrar computadores afetados** – Veja os computadores aos quais a exclusão é aplicada.
- **Relatório de auditoria** – mostrar o Relatório de auditoria para a exclusão selecionada.
- **Remover** – Remove a exclusão.
- **Grupo de acesso** > **Mover** – Mova o objeto para outro grupo estático onde ele está disponível para usuários com direitos suficientes para o grupo de destino. Alterar o Grupo de acesso é útil ao resolver problemas de acesso com outros usuários. O Grupo de acesso define o grupo estático do objeto e o acesso ao objeto com base nos direitos de acesso do usuário.

Se a ação excluída de detecção ou firewall aparecer novamente nos computadores gerenciados, a coluna **Contagem de correspondências** exibe o número de vezes que a exclusão foi aplicada.

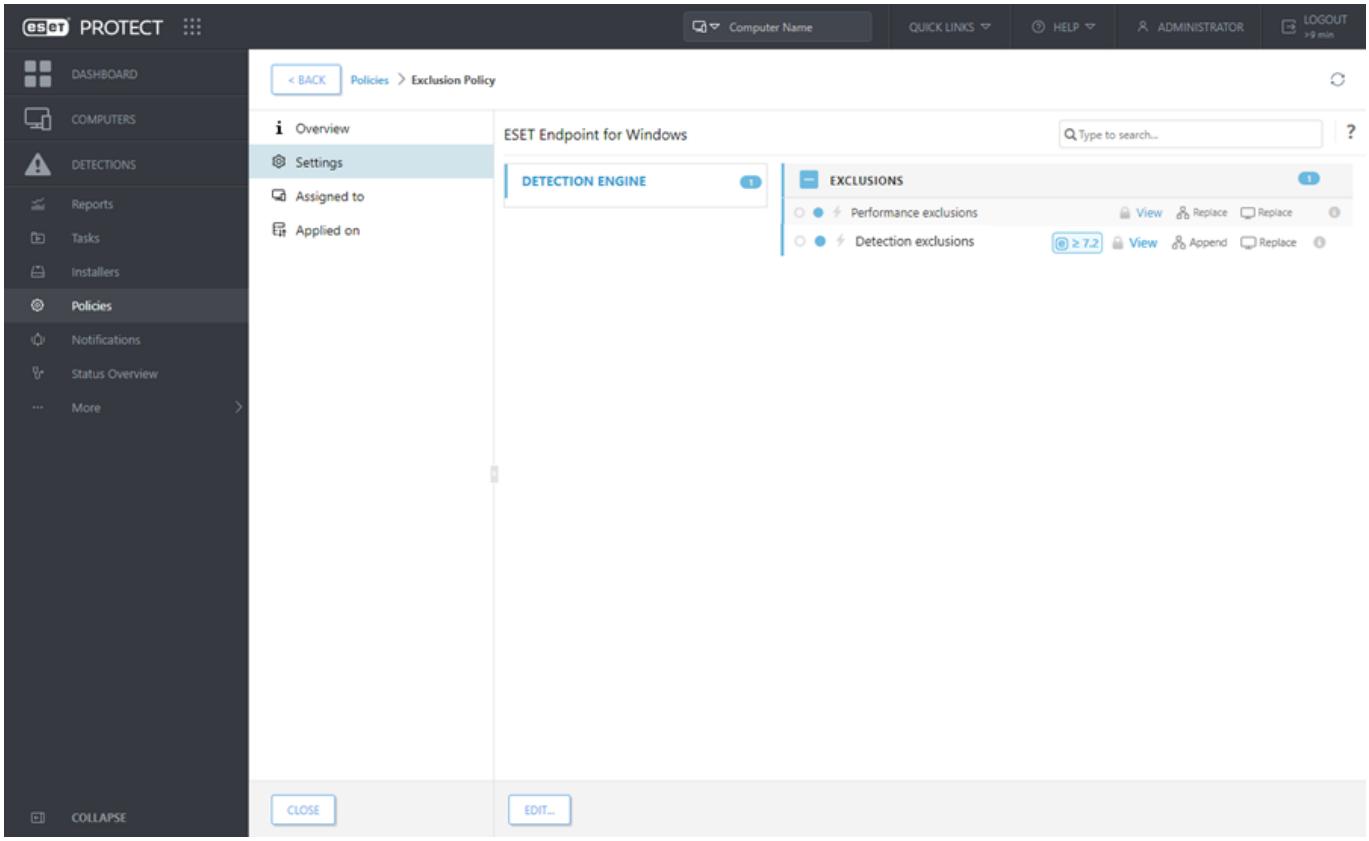
Migrar exclusões de uma política

No ESET PROTECT não é possível criar exclusões de detecção Antivírus por meio de uma Política. Se as suas políticas tinham exclusões anteriormente, siga as etapas abaixo para migrar exclusões das Políticas para a lista **Exclusões** no ESET PROTECT:

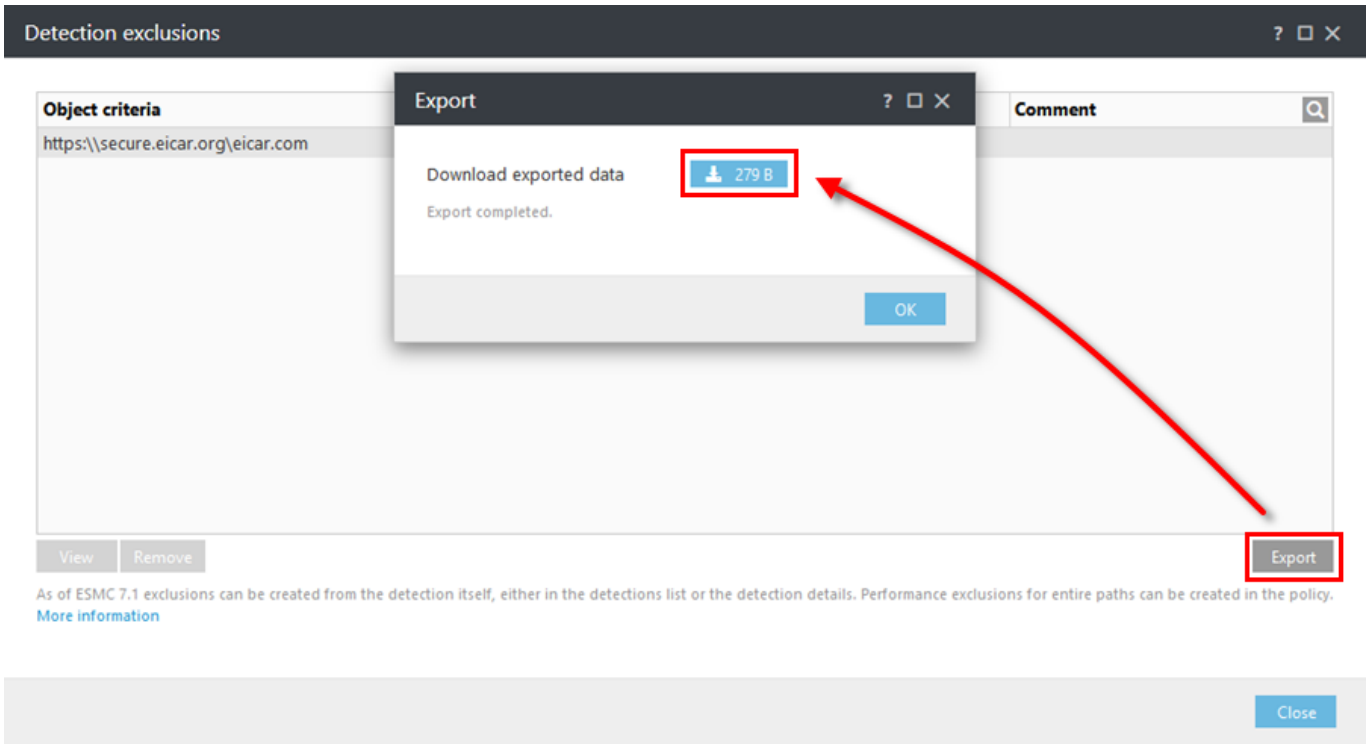
1.Navegue para **Políticas** e clique na política que contém exclusões e selecione **Mostrar detalhes**.

2.Clique em **Configurações** > **Mecanismo** de **detecção**.

3.Clique em **Exibir** ao lado de **Exclusões de detecção**.

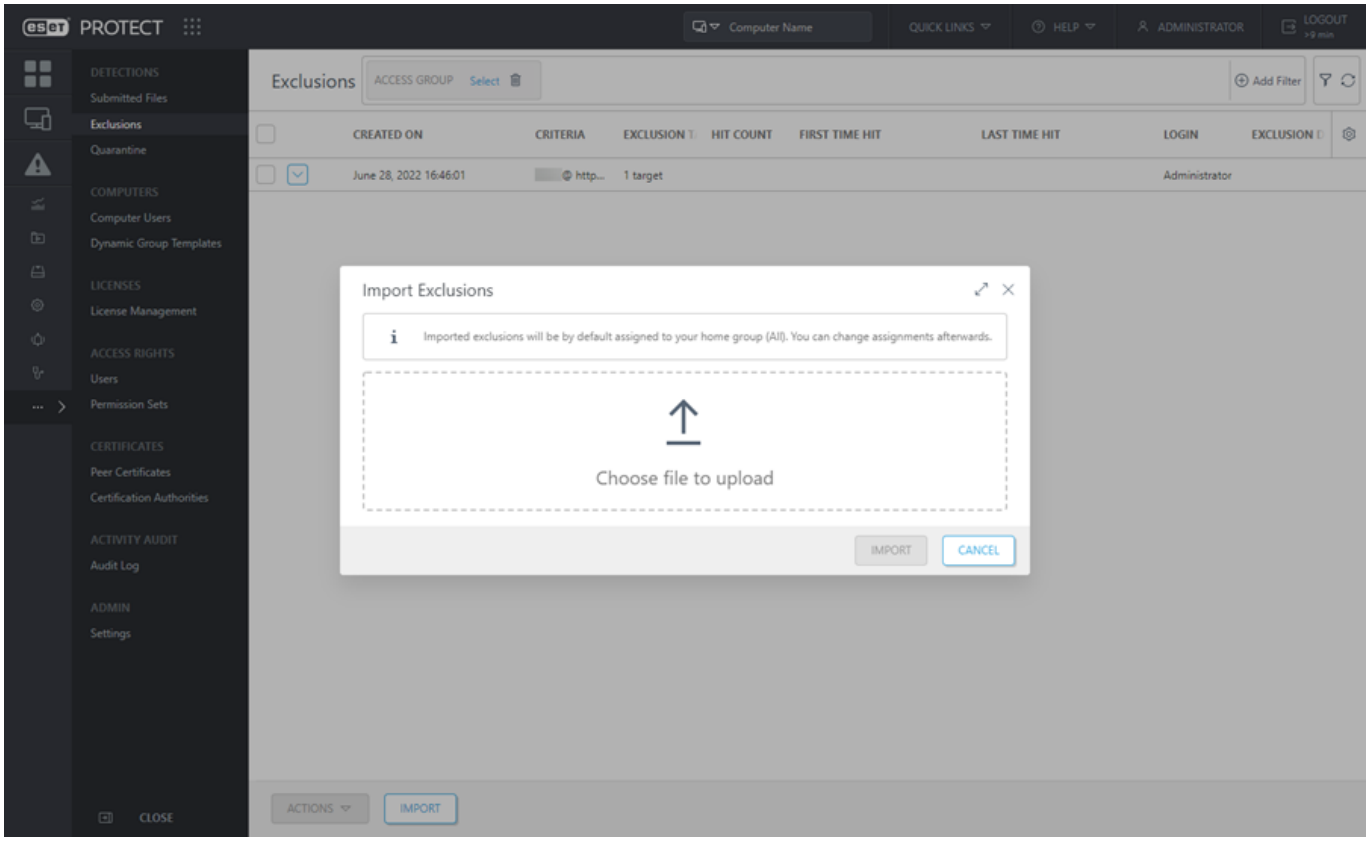


4.Clique no botão **Exportar** e, em seguida, clique no botão ao lado de **Fazer download dos dados exportados** e salve o arquivo *export.txt*. Clique em **OK**.

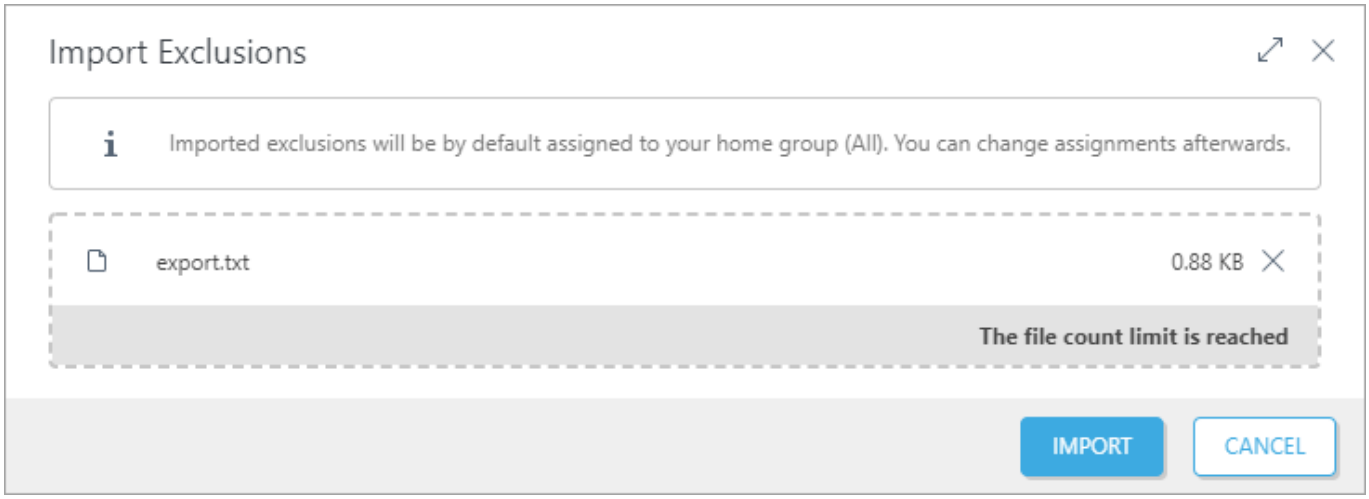


5.No console web ESET PROTECT, navegue para **Mais** > **Exclusões**.

6.Clique no botão **Importar** para importar as exclusões de detecção de um arquivo. Clique em **Escolher arquivo para carregar** e navegue até o arquivo *export.txt* ou arraste e solte o arquivo.



7.Clique no botão **Importar** para importar as exclusões de detecção. As exclusões de detecção importadas aparecerão na lista de exclusões.



Limitações de atribuição de exclusões

- As atribuições de exclusão originais não são preservadas. As exclusões de detecção importadas são, por padrão, atribuídas aos computadores em seu grupo doméstico. Para alterar a atribuição de exclusão, clique na exclusão e selecione **Alterar atribuição**.
- Você pode atribuir exclusões (para ameaças de **Antivírus** e regras IDs de **Firewall**) somente a computadores com um produto de segurança ESET compatível instalado. Exclusões não serão aplicadas a produtos de segurança ESET incompatíveis e serão ignoradas neles.

Filtros e personalização de layout

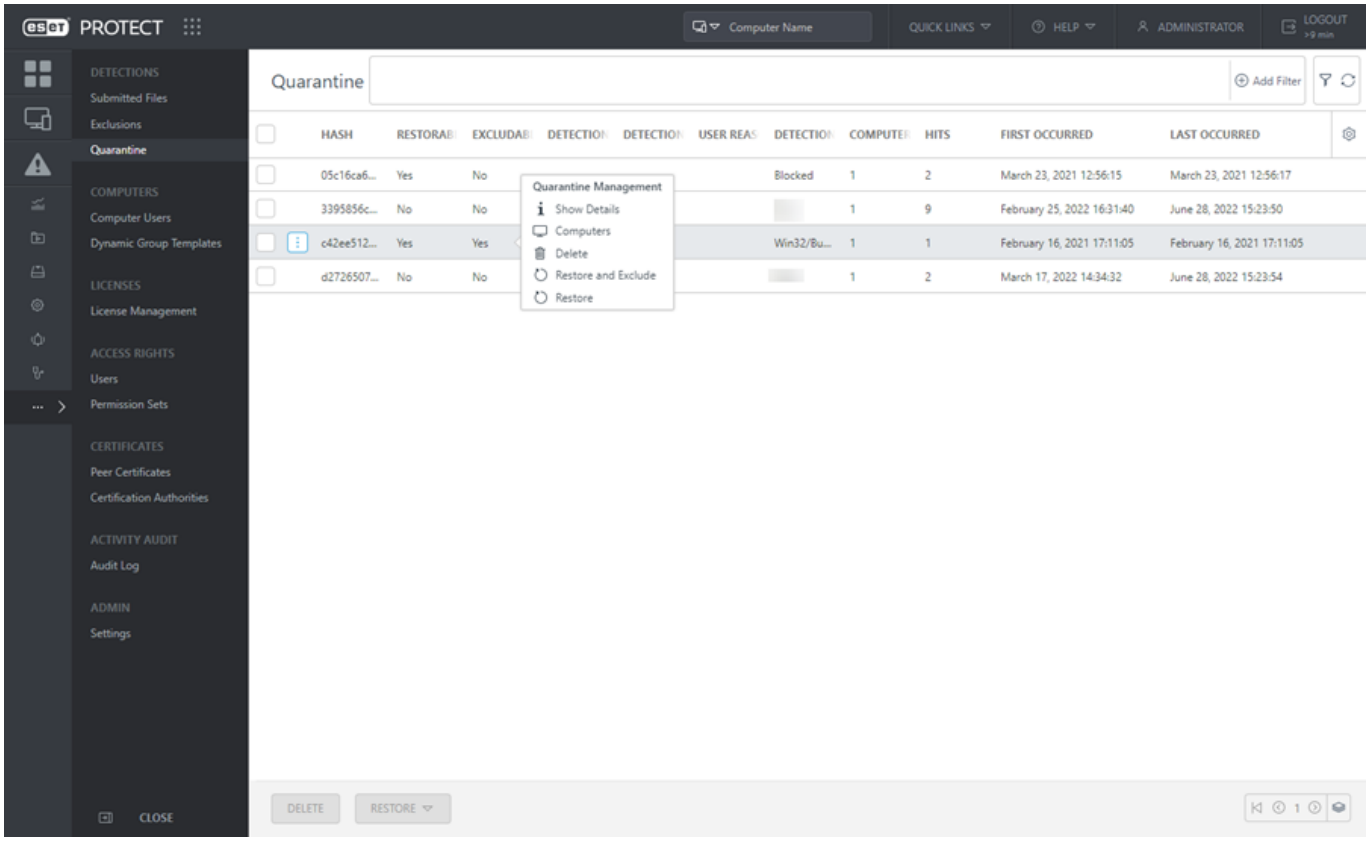
Você pode personalizar a exibição da tela atual do console web:

- Gerenciar o painel lateral e a tabela principal.
- Adicionar filtro e predefinições de filtro. Você pode usar marcações para filtrar os itens exibidos.

Quarentena

Essa seção mostra todos os arquivos colocados em quarentena nos dispositivos do cliente. Os arquivos devem ser colocados em quarentena se não puderem ser limpos, se não for seguro nem aconselhável excluí-los ou se eles estiverem sendo falsamente detectados por um produto ESET.

> Nem todas as detecções encontradas em dispositivos clientes são movidas para a quarentena. Detecções que não são colocadas em quarentena incluem:
> • Detecções que não se pode remover
> • Detecções que são suspeitas com base em seu comportamento, mas que não são detectadas como malware, por exemplo, PUAs.



Você pode **Excluir** o arquivo em quarentena ou **Restaurar** para sua localização anterior. Você pode usar **Restaurar e Excluir** no arquivo em quarentena para impedi-lo de ser reportado novamente pelo produto ESET.

Você pode usar vários filtros para filtrar a lista de arquivos em quarentena.

Há duas maneiras de acessar a **Quarentena**:

1. **Mais** > **Quarentena**.

2. **Detalhes do computador** > **Detecções e quarentena** > guia Quarentena.

Se você clicar em um item na seção **Quarentena** vai abrir o menu do **Gerenciamento de quarentena**.

Mostrar Detalhes – Exibe o dispositivo de origem, nome e tipo de detecção, nome do objeto com o caminho de arquivo completo, hash, tamanho, etc.

Computadores - Abre a seção **Computadores** com dispositivos filtrados conectados ao arquivo de quarentena.

Excluir - Remove o arquivo da quarentena e o dispositivo afetado.

Restaurar - Restaurar o arquivo para sua localização original.

Restaurar e Excluir - Restaura o arquivo para sua localização original e exclui o arquivo do rastreamento.

Carregar - Abre a tarefa Carregar arquivo em quarentena. Esta ação está disponível depois que você clica em **Mostrar detalhes**.

A função **Carregar** é recomendada apenas para usuários experientes. Se quiser investigar mais o arquivo colocado em quarentena, ele pode ser **Carregado** para um diretório compartilhado.

Filtros e personalização de layout

Você pode personalizar a exibição da tela atual do console web:

- Gerenciar o painel lateral e a tabela principal.
- Adicionar filtro e predefinições de filtro. Você pode usar marcações para filtrar os itens exibidos.

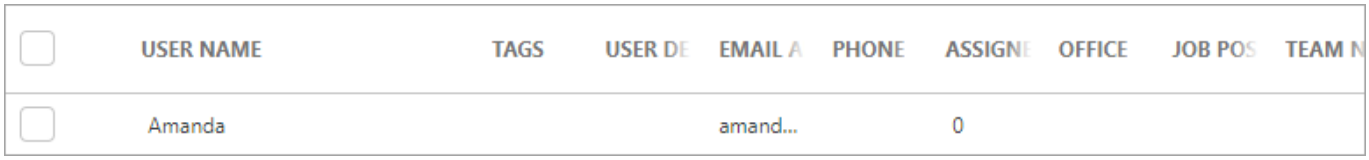
Usuários do computador

A seção Usuários do computador permite que você gerencie Usuários e Grupos de usuários. Você pode parear um usuário com um dispositivo para sincronizar algumas configurações específicas do usuário. Recomendamos primeiro sincronizar Usuários com o Active Directory. Após a criação de um novo computador, você pode parear o computador com um usuário específico. Você pode então procurar o usuário para visualizar detalhes sobre os computadores atribuídos a eles e suas atividades.

Você também pode gerenciar Usuários e Grupos de usuários para fins de Gerenciamento de dispositivo móvel iOS com o uso de políticas atribuídas a dispositivos iOS. Em seguida, você pode modificar os usuários ou adicionar Atributos personalizados.

Usuários do computador são diferentes dos **usuários do Console da web ESET PROTECT**. Para gerenciar os usuários do console da Web ESET PROTECT e conjuntos de permissões navegue até **Mais** > **Usuários**.

- Usuários destacados em laranja não terão nenhum dispositivo atribuído a eles. Clique no usuário, selecione Editar e clique em**Computadores atribuídos** para ver os detalhes daquele usuário. Clique em **Adicionar computadores** para atribuir dispositivos a este usuário.



- Você também pode adicionar ou remover **Usuários atribuídos** de dentro dos Detalhes do computador. Quando você estiver em **Computadores**, selecione um dispositivo e clique em **Mostrar detalhes**. O usuário pode ser atribuído a mais de um dispositivo. Você também pode usar **Atribuir Usuário** para atribuir um usuário diretamente para o(s) dispositivo(s) selecionado(s). Se houver um dispositivo atribuído a um usuário, você pode clicar no nome do dispositivo para ver detalhes sobre aquele dispositivo.

- Você pode Arrastar e Soltar usuários e grupos de usuários. Selecione o usuário (ou grupo), segure o botão do mouse e mova para o outro grupo.

Ações de gerenciamento de usuários

Selecione um usuário para abrir um menu suspenso onde você pode executar ações. Consulte a legenda de Ícones para detalhes sobre as ações.

Mostrar detalhes – o menu exibe informações como **Endereço de e-mail**, **Escritório ou local** e **Computadores atribuídos**. O usuário pode ter mais de um dispositivo atribuído. Você pode alterar o **nome** de usuário, **descrição** ou o **grupo principal**. Você pode usar os **Atributos personalizados** ao criar políticas MDM iOS.

Filtros e personalização de layout

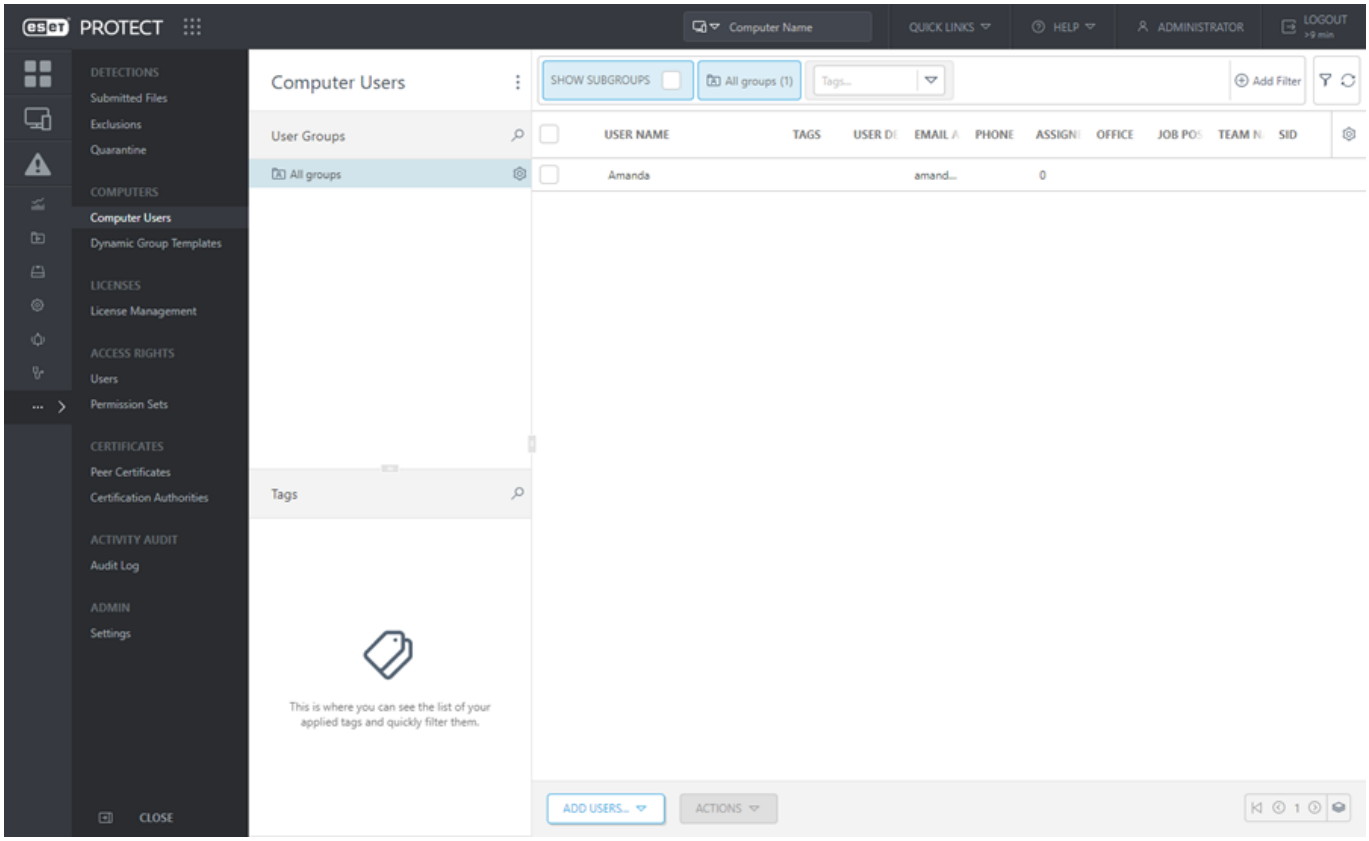
Você pode personalizar a exibição da tela atual do console web:

- Gerenciar o painel lateral e a tabela principal.

- Adicionar filtro e predefinições de filtro. Você pode usar marcações para filtrar os itens exibidos.

Adicionar novos usuários

1. Clique em **Usuários do computador** > **Adicionar usuários** para adicionar usuários. Use essa opção para adicionar usuários que não foram encontrados ou adicionados automaticamente durante a Sincronização de usuário.



2. Digite o nome do usuário que deseja adicionar no campo **Nome de usuário**. Clique em + **Adicionar** para adicionar usuários. Se quiser adicionar vários usuários ao mesmo tempo, clique em Importar CSV para carregar um arquivo *.csv* contendo uma lista de usuários a serem adicionados. Clique em **Copiar e colar** para importar uma lista personalizada de endereços separados por delimitadores personalizados (esse recurso funciona de forma similar ao Importar CSV). Opcionalmente, você pode digitar uma **Descrição** dos usuários para facilitar a identificação.

3. Você pode selecionar um **Grupo de origem** existente ou criar um novo grupo.

4. Clique em **Selecionar marcações** para atribuir marcações.

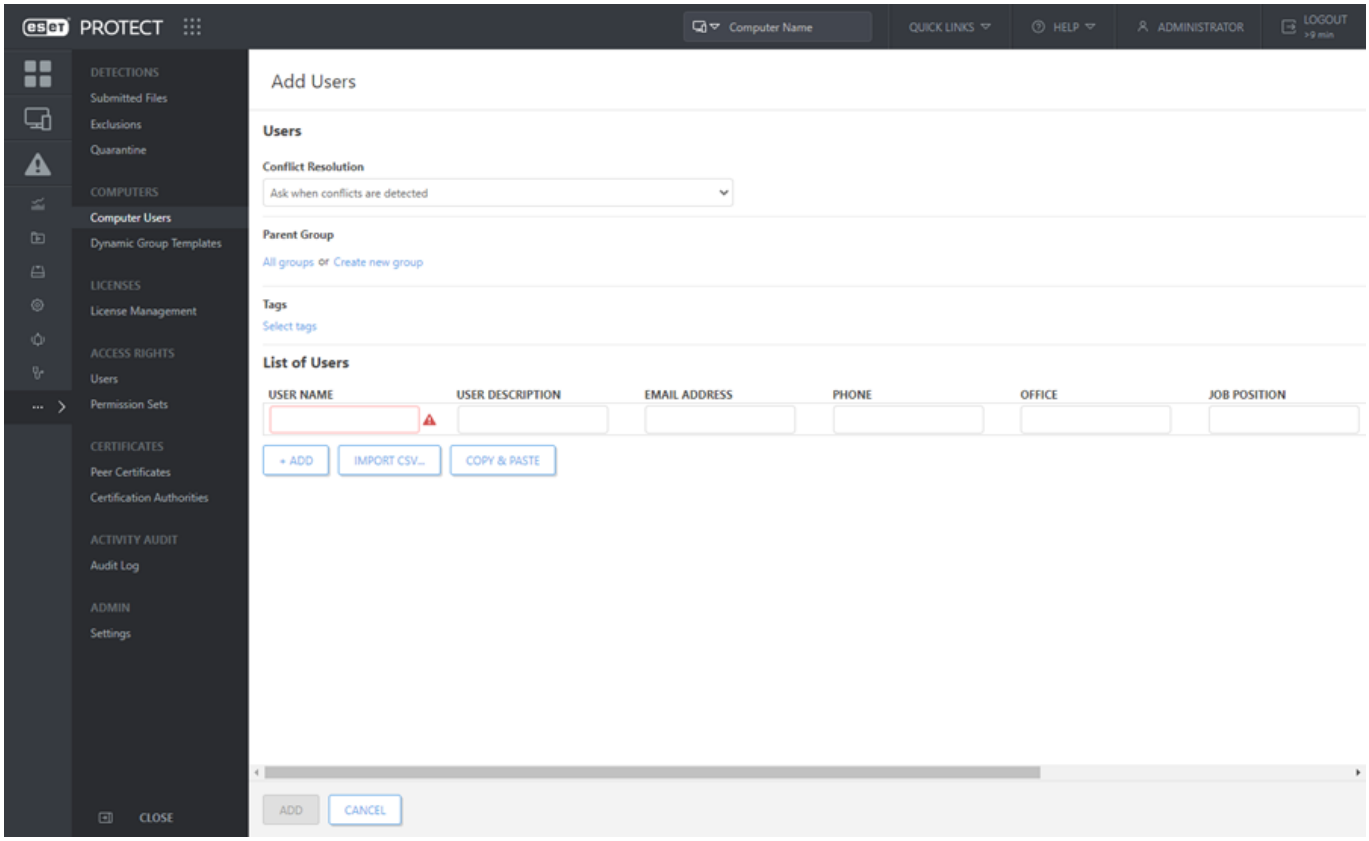
5. Use o menu suspenso de **Resolução de conflito** para selecionar a ação a ser realizada se um usuário sendo adicionado já existir no ESET PROTECT:

- **Perguntar quando conflitos forem detectados**: Quando um conflito for detectado, o programa pedirá que você selecione uma ação (veja as opções a seguir).

- **Ignorar usuários em conflito:** Não serão adicionados usuários com o mesmo nome. Isso também garante que os atributos personalizados de usuário existentes no ESET PROTECT serão preservados (não serão substituídos por dados do Active Directory).

- **Sobrescrever usuários em conflito:** Os usuários existentes no ESET PROTECT são sobrescritos pelos usuários do Active Directory. Se dois usuários tiverem o mesmo SID, o usuário existente no ESET PROTECT é removido do seu local anterior (mesmo se o usuário estava em um grupo diferente).

6. Clique em **Adicionar** quando tiver concluído as alterações. Os Usuários vão aparecer no grupo principal especificado.



Editar usuários

Você pode modificar os detalhes do usuário como informações **Básicas** e **Computadores atribuídos**.

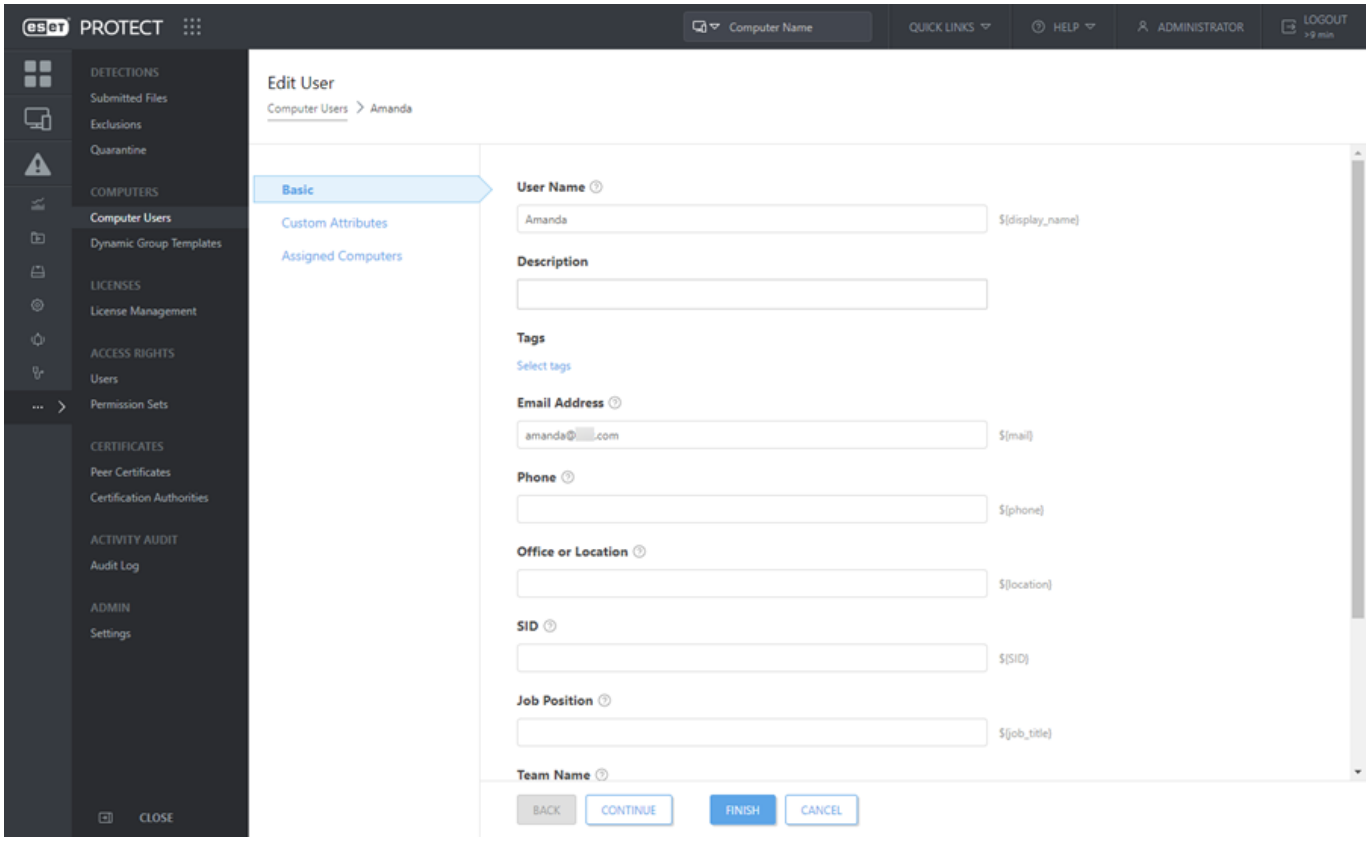
> Ao realizar uma tarefa de Sincronização de usuário para usuários com atributos personalizados definidos, defina **Processamento de colisão na criação de usuário** como **Ignorar**. Se não, os dados do usuário serão substituídos por dados do seu Active Directory.

Básico

Se você usou uma tarefa de Sincronização de usuário para criar o usuário e alguns campos estão em brancos, é possível especificar esses campos manualmente conforme for necessário.

Aqui você pode editar detalhes do usuário como:

- **Nome de usuário** e **Descrição** – apenas para fins informativos.
- **Marcações** - Editar marcações (atribuir, remover atribuição, criar, remover).
- **Endereço de e-mail –** pode ser usado como endereço do destinatário para a entrega de notificações.
- **Telefone** e **Escritório ou local –** apenas para fins informativos.
- **SID** Pode estar associado a várias funções ESET PROTECT que exigem essas informações AD (por exemplo, o Modo de Substituição da Política Endpoint).



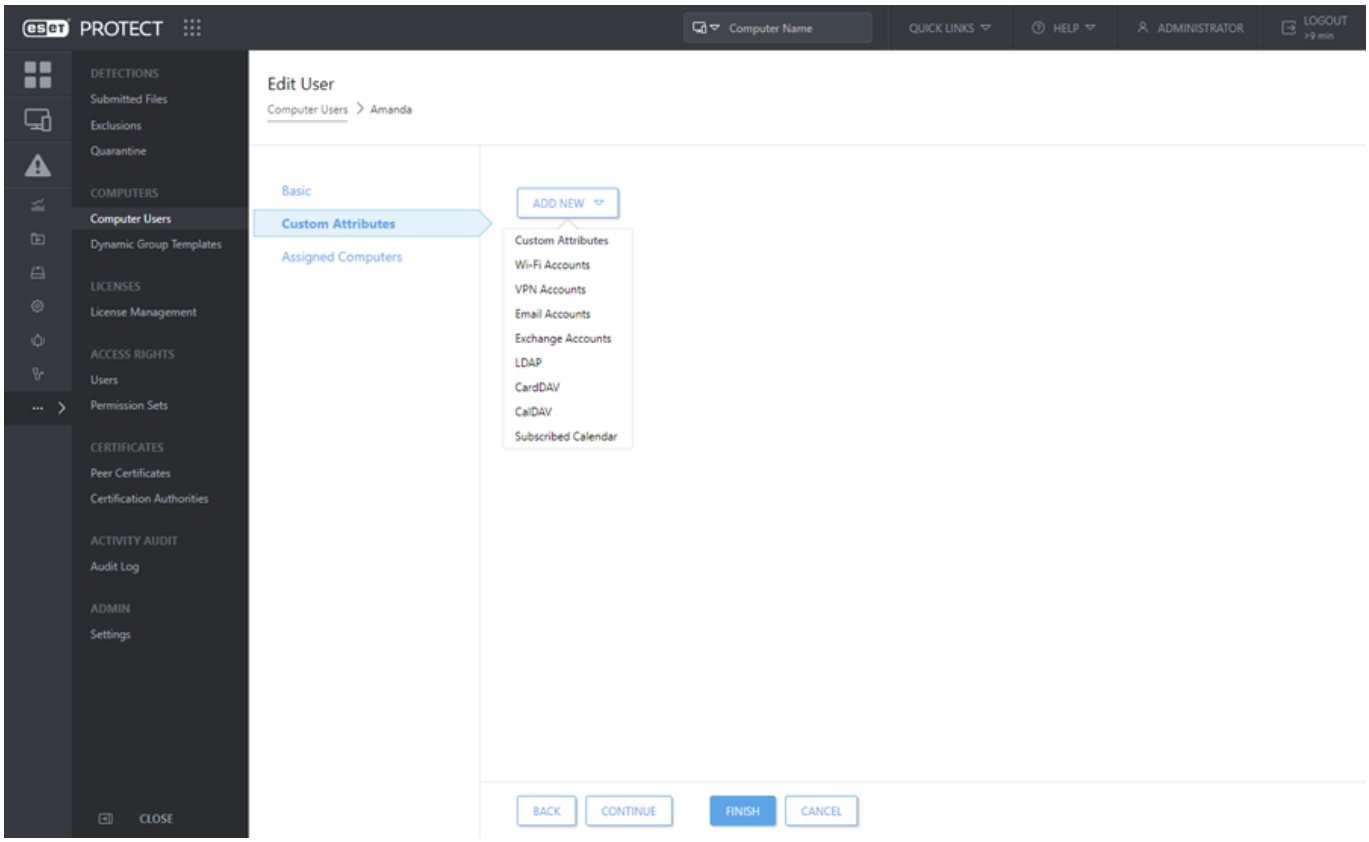
Atributos personalizados

Você pode editar atributos personalizados existentes ou adicionar novos atributos. Para adicionar novos, clique em **Adicionar novo** e escolha a partir das categorias:

- **Contas Wi-Fi:** Perfis podem ser usados para enviar configurações de Wi-Fi corporativo diretamente para dispositivos gerenciados.
- **Contas VPN:** Você pode configurar um VPN junto com as credenciais, certificados e outras informações necessárias para tornar o VPN facilmente acessíveis para os usuários.
- **Contas de Email**: Isto é usado para qualquer conta de email que usa especificações IMAP ou POP3. Se você usar um servidor Exchange, use as configurações Exchange ActiveSync abaixo.
- **Contas do Exchange**: Se a sua empresa usar o Microsoft Exchange, você pode criar todas as configurações aqui, para minimizar o tempo de configuração para o acesso dos seus usuários ao email, agenda e contatos.
- **LDAP (Alias de atributo):** Isto é especialmente útil se a sua empresa usa LDAP para contatos. Você pode mapear os campos de contato nos campos de contato iOS correspondentes.
- **CalDAV:** Isso contém as definições para qualquer calendário que usa as especificações CalDAV.
- **CardDAV:** Para qualquer contato sincronizado através da especificação CardDAV, as informações para sincronização podem ser estabelecidas aqui.
- **Agenda assinada**: Se qualquer agenda CalDAV for configurada, é aqui onde é possível definir acesso somente leitura a agendas de outros.

Alguns dos campos vão se tornar um atributo que pode ser usado ao criar uma política para dispositivo móvel iOS

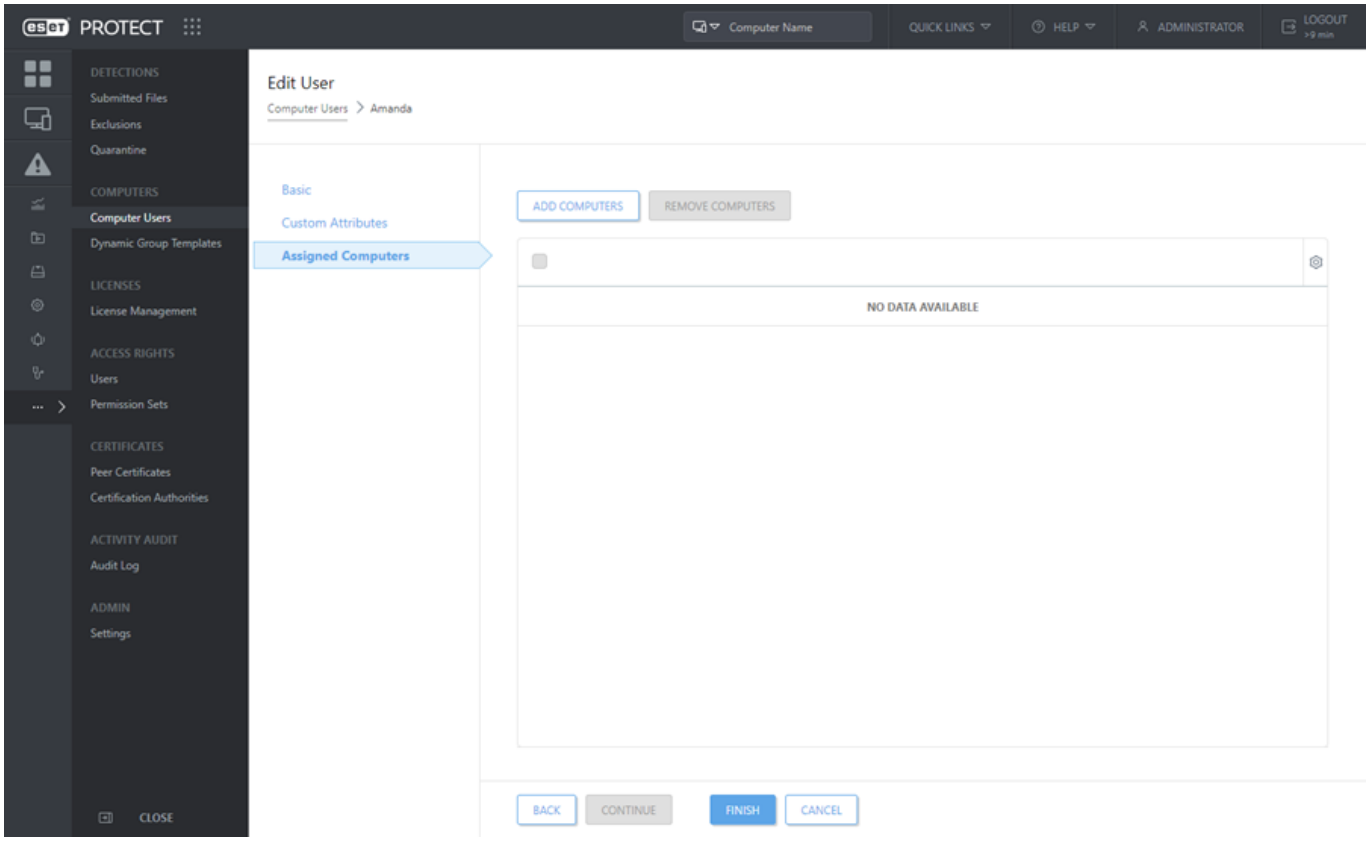
como uma variável (espaço reservado). Por exemplo, Login `${exchange_login/exchange}` ou Endereço de email `${exchange_email/exchange}`.



Computadores atribuídos

Aqui é possível selecionar dispositivos individuais. Para fazer isso, clique em **Adicionar computadores -** todos os grupos estáticos e dinâmicos e seus membros serão listados. Use as caixas de seleção para fazer sua seleção e clique em **OK**.

Um usuário só pode ser atribuído a no máximo 200 computadores em uma operação.

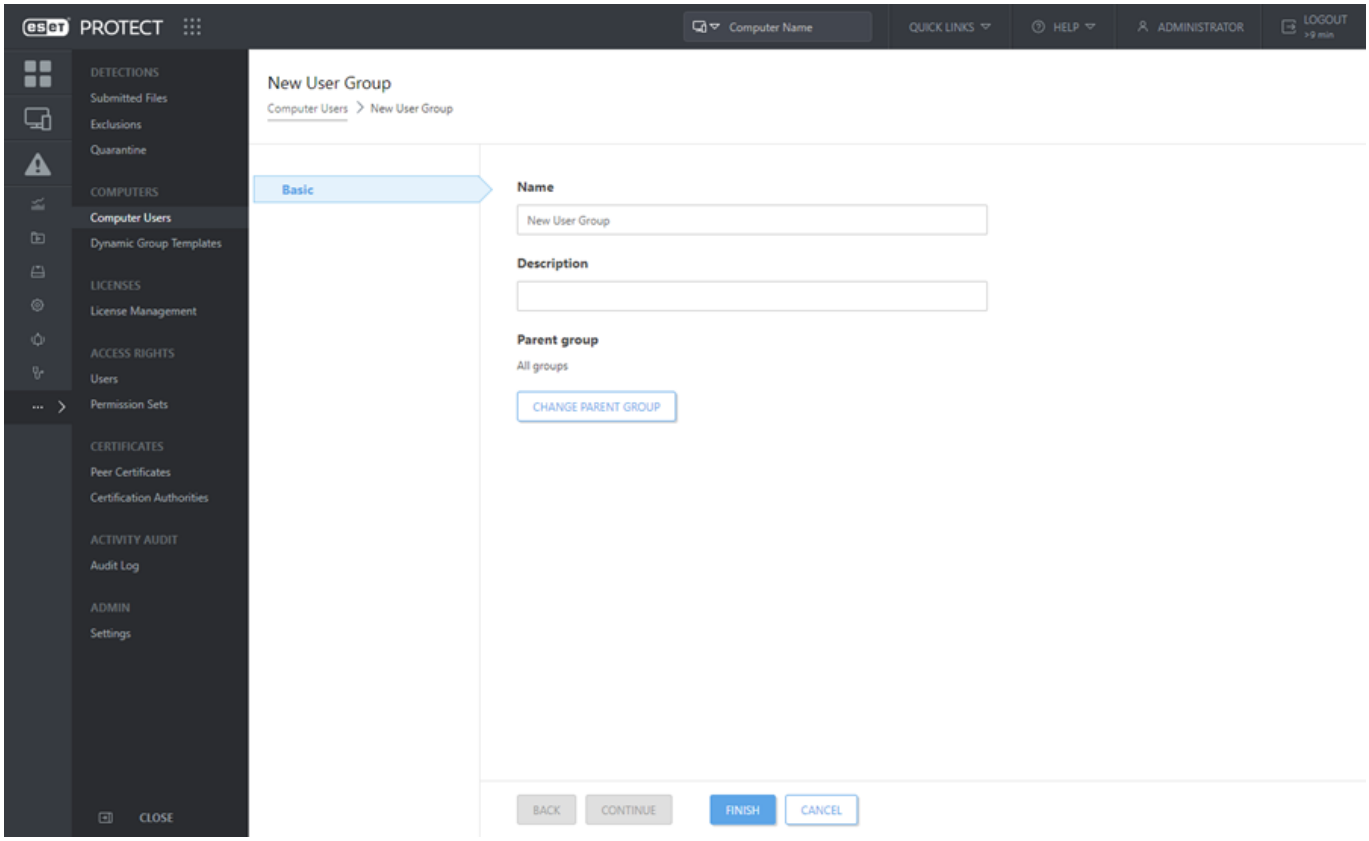


Criar novo grupo de usuário

Clique em **Usuários do computador** > ⚙ e selecione + **Novo grupo de usuário**

Básico

Insira um **Nome e uma Descrição** (opcional) para o novo grupo de usuário. Por padrão, o grupo principal é o grupo que você selecionou quando começou a criar o novo grupo de usuário. Se quiser trocar seu grupo principal, clique em **Alterar grupo principal** e selecione o grupo principal da árvore. Clique em **Concluir** para criar o novo grupo de usuários.



Você pode atribuir permissões específicas para esse grupo de usuários de dentro dos Direitos de Acesso usando Definições de permissão (consulte a seção **Grupos de usuários**). Assim, você pode especificar quais usuários específicos do Console ESET PROTECT podem gerenciar quais Grupos de usuários específicos. Você pode até restringir o acesso desses usuários para outras funções ESET PROTECT usando políticas, se desejar. Esses usuários vão, então, gerenciar apenas Grupos de usuários.

Modelos de grupo dinâmico

Modelos de grupo dinâmico estabelecem os critérios que os computadores devem atender para serem colocados em um grupo dinâmico. Quando esses critérios são cumpridos por um cliente, o cliente será automaticamente transferido para o grupo dinâmico apropriado.

Um modelo é um objeto estático armazenado em um grupo estático. Usuários devem ter as permissões apropriadas para acessar os modelos. Um usuário precisa de permissões de acesso para ser capaz de trabalhar com modelos de Grupo dinâmico. Todos os modelos predefinidos estão localizados no grupo estático **Todos** e por padrão estão disponíveis apenas ao Administrador. Outros usuários precisam receber permissões adicionais. Como resultado, os usuários podem não conseguir ver ou usar os modelos padrão. Os modelos podem ser movidos para um grupo onde os usuários têm permissões.
Para duplicar um modelo o usuário precisa receber a atribuição de permissões de **Uso** (para modelos do Grupo dinâmico) para o grupo onde o modelo original está localizado, e permissões de **Gravação** para o grupo inicial do usuário (onde a duplicata será armazenada). Veja o exemplo de duplicação de objeto.

- Criar novo modelo de grupo dinâmico
- Regras para um modelo de grupo dinâmico
- Modelo de grupo dinâmico - exemplos

Gerenciar modelos de grupo dinâmico

Modelos podem ser gerenciados em **Mais** > **Modelos de grupo dinâmico**.

Novo modelo	Clique para criar um Novo modelo em seu grupo inicial.
Mostrar detalhes	Veja o resumo de informações sobre o modelo selecionado.
Relatório de auditoria	Exibe o Relatório de auditoria para o item selecionado.
Marcações	Editar marcações (atribuir, remover atribuição, criar, remover).
Editar	Editar modelo selecionado. Clique em **Salvar como** se quiser manter seu modelo existente e criar um novo com base no modelo que você está editando. Quando solicitado, especifique o nome para seu novo modelo.
Duplicar	Criar um novo Modelo de grupo dinâmico com base no modelo selecionado. Um novo nome será necessário para a tarefa duplicada. O modelo duplicado será armazenado em seu grupo inicial.
Excluir	Remova o modelo permanentemente.
Importar	Importar modelos de grupo dinâmico de um arquivo. Durante a importação, a estrutura do arquivo está sendo verificada para garantir que o arquivo não esteja corrompido.
Exportar	Exportar os modelos de grupo dinâmico selecionados para um arquivo para fins de backup ou migração. Não recomendamos fazer edições no arquivo – elas podem tornar os dados inutilizáveis.
Grupo de acesso > **Mover**	Mova o objeto para outro grupo estático onde ele está disponível para usuários com direitos suficientes para o grupo de destino. Alterar o Grupo de acesso é útil ao resolver problemas de acesso com outros usuários. O Grupo de acesso define o grupo estático do objeto e o acesso ao objeto com base nos direitos de acesso do usuário.

O ESET Enterprise Inspector e o ESET Dynamic Threat Defense foram renomeados para ESET Inspect e ESET LiveGuard Advanced.
Você pode precisar resolver os problemas causados pela renomeação se você atualizou do ESET PROTECT 9.0 e versões anteriores e tem relatórios, grupos dinâmicos, notificações ou outros tipos de regras que filtram por ESET Dynamic Threat Defense ou ESET Enterprise Inspector.

Filtros e personalização de layout

Você pode personalizar a exibição da tela atual do console web:

- Gerenciar o painel lateral e a tabela principal.
- Adicionar filtro e predefinições de filtro. Você pode usar marcações para filtrar os itens exibidos.

Novo modelo de grupo dinâmico

Clique em **Novo modelo** em **Mais** > **Modelos de grupo dinâmico**.

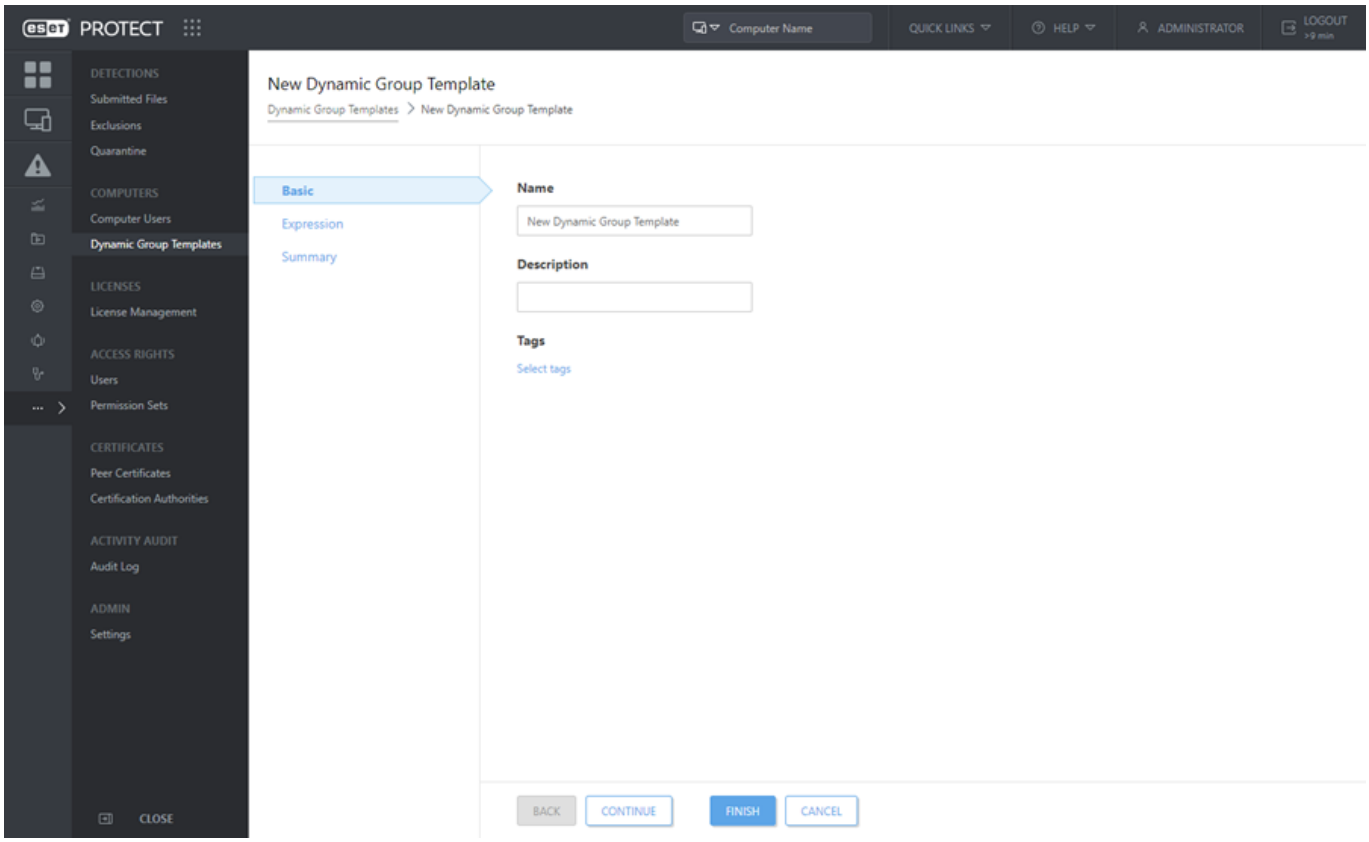
Básico

Insira um **Nome** e uma **Descrição** para o novo modelo de grupo dinâmico.

Clique em **Selecionar marcações** para atribuir marcações.

Expressão

Veja nossos exemplos ilustrados com instruções passo-a-passo para amostras de como usar grupos dinâmicos em sua rede.



Resumo

Revise as configurações definidas e clique em **Concluir** para criar o modelo. Este novo modelo será adicionado na lista de todos os modelos e pode ser usado mais tarde para criar um novo Grupo dinâmico.

Regras para um modelo de grupo dinâmico

Quando você define regras para um modelo de grupo dinâmico, você pode usar diferentes operadores para diferentes condições para chegar ao seu cenário desejado.

Os capítulos a seguir explicam as regras e operações usadas nos modelos de Grupo dinâmico:

- Operações
- Regras e conectivos lógicos

- Avaliação de Permissões de Modelo
- Como criar automação no ESET PROTECT
- Modelos de grupo dinâmico
- Casos de uso - criar um modelo específico de grupo dinâmico

Operações

Se você especificar várias regras (condições), é preciso selecionar qual operação deve ser usada para combinar as regras. Dependendo do resultado, um computador cliente será adicionado ou não a um Grupo dinâmico que usar esse Modelo.

- A **Operação** selecionada funciona não só ao combinar mais regras, mas também quando existe apenas uma regra.
- Não é possível combinar as operações. Apenas uma operação é usada pelo Modelo de grupo dinâmico e se aplica a todas as suas regras.

AND (Todas as condições precisam ser verdadeiras)	Verifique se todas as condições são avaliadas positivamente - o computador deve cumprir com todos os parâmetros necessários.
OR (Pelo menos uma condição precisa ser verdadeira)	Verifique se pelo menos uma das condições é avaliada positivamente - o computador deve cumprir com pelo menos um dos parâmetros necessários.
NAND (Pelo menos uma condição precisa ser falsa)	Verifique se pelo menos uma das condições não pode ser avaliada positivamente - o computador não deve cumprir com pelo menos um parâmetro.
NOR (Todas as condições precisam ser falsas)	Verifique se todas as condições não podem ser avaliadas positivamente - o computador não cumpre com nenhum os parâmetros necessários.

Regras e conectivos lógicos

Uma regra é composta de um item, conector lógico (operador lógico) e valor definido.

Quando você clica em **+ Adicionar** regra uma janela abrirá com uma lista de itens divididos em categorias. Por exemplo:

Software instalado > **Nome do aplicativo**

Adaptadores de rede > **Endereço MAC**

Edição do sistema operacional > **nome do sistema operacional**

Você pode navegar pela lista de todas as regras disponíveis neste artigo da Base de conhecimento da ESET.

Para criar uma regra selecione um item, escolha um operador lógico e especifique um valor. A regra será avaliada de acordo com o valor que você especificou e o operador lógico usado.

Tipos de valor aceitáveis incluem números, strings, enumerações, endereços IP, máscaras de produto e IDs de computadores. Cada tipo de valor tem operadores lógicos diferentes associados e p console da Web ESET PROTECT mostrará automaticamente apenas aqueles que são compatíveis.

• **"= (igual)"** - O valor do símbolo e o valor do modelo devem ser iguais. Strings são comparadas sem diferenciação de maiúsculas e minúsculas.

• **"> (mais de)"** - O valor do símbolo deve ser maior do que o valor de modelo. Também pode ser usado para criar uma comparação em intervalo para símbolos de endereço IP.

• **"≥ (mais ou igual)"** - O valor do símbolo deve ser mais que ou igual ao valor do modelo. Também pode ser usado para criar uma comparação em intervalo para símbolos de endereço IP.

• **"< (menos de)"** - O valor do símbolo deve ser menor do que o valor de modelo. Também pode ser usado para criar uma comparação em intervalo para símbolos de endereço IP.

• **"≤ (menor ou igual)"** - O valor do símbolo deve ser menos que ou igual ao valor do modelo. Também pode ser usado para criar uma comparação em intervalo para símbolos de endereço IP.

• **"contém"** - O valor do símbolo contém o valor do modelo. No caso de strings, isso procura uma sub-string. A pesquisa é feita sem sensibilidade para letras maiúsculas ou minúsculas.

• **"tem prefixo"** - O valor do símbolo tem o mesmo prefixo de texto como valor de modelo. Strings são comparadas sem diferenciação de maiúsculas e minúsculas. Define os primeiros caracteres da sua sequência de pesquisa, por exemplo string "Microsoft Visual C++ 2010 x86 Redistributable - 10.0.30319", o prefixo é "Micros" ou "Micr" ou “Microsof” etc.

• **"tem sufixo"** - O valor do símbolo tem o mesmo sufixo de texto como valor de modelo. Strings são comparadas sem diferenciação de maiúsculas e minúsculas. Define os primeiros caracteres da sua string de pesquisa, por exemplo para "Microsoft Visual C++ 2010 x86 Redistributable - 10.0.30319", o sufixo é "319" ou "0.30319", etc.

• **"tem máscara"** - O valor do símbolo deve combinar com a máscara definida em um modelo. A formatação de máscara permite todos os caracteres, símbolos especiais '*' - zero, um ou muitos caracteres e '?' exatamente um caractere, por exemplo: "6.2.*" ou "6.2.2033.?".

• **“regex"** - O valor do símbolo deve combinar com a expressão regular (regex) de um modelo. O regex deve ser escritos no formato **Perl**.

Uma expressão regular, *regex* ou *regexp* é uma sequência de caracteres que define um padrão de busca. Por exemplo, *gray|grey* e *gr(a|e)y* são padrões equivalentes que combinam com as duas palavras a seguir: "*gray*", "*grey*".

• **“faz parte de”** - O valor do símbolo deve combinar com qualquer valor de uma lista em um modelo. Para adicionar um item, clique em **+ Adicionar**. Cada linha em um novo item na lista. Strings são comparadas sem diferenciação de maiúsculas e minúsculas.

• **“faz parte de (máscara da string)”** - O valor do símbolo deve combinar com qualquer máscara de uma lista em um modelo. As strings são comparadas com diferenciação de maiúsculas e minúsculas. Exemplos: *endpoint-pc*, *Endpoint-PC*.

• **“com valor”**

As regras de tempo permitem selecionar a caixa de seleção **Medir tempo decorrido** para criar um modelo de Grupo dinâmico com base no tempo decorrido desde um evento específico. O computador gerenciado deve executar o Agente ESET Management 10.0 e versões posteriores.

Operadores negados:

Operadores de negação devem ser usados com cuidado, porque no caso relatórios de várias linhas como “Aplicativo instalado”, todas as linhas são testadas contra essas condições. Consulte os exemplos incluídos (Avaliação de regras de modelo e Modelo de grupo dinâmico - exemplos) para ver como operadores de negação ou operações negadas deve ser usados para obter os resultados esperados.

- **"= (desigual)"** - O valor do símbolo e o valor do modelo não devem ser iguais. Strings são comparadas sem diferenciação de maiúsculas e minúsculas.
- **"não contém"** - O valor do símbolo não contém o valor do modelo. A pesquisa é feita sem sensibilidade para letras maiúsculas ou minúsculas.
- **"não tem prefixo"** - O valor do símbolo não tem um prefixo de texto como valor de modelo. Strings são comparadas sem diferenciação de maiúsculas e minúsculas.
- **"não tem sufixo"** - O valor do símbolo não tem um sufixo de texto como valor de modelo. Strings são comparadas sem diferenciação de maiúsculas e minúsculas.
- **"não tem máscara"** - O valor do símbolo não deve combinar com a máscara definida em um modelo.
- **“não regex"** - O valor do símbolo não deve combinar com a expressão regular (regex) de um modelo. O regex deve ser escritos no formato **Perl**. A operação de negação é fornecida como ajudante para negar correspondentes em expressões regulares sem regravações.
- **“não é um de”** - O valor do símbolo não deve combinar com qualquer valor de uma lista em um modelo. Strings são comparadas sem diferenciação de maiúsculas e minúsculas.
- **“não em um de (máscara da cadeia)"** - O valor do símbolo não deve combinar com qualquer máscara de uma lista em um modelo.
- **“sem valor”**

Avaliação de Permissões de Modelo

A avaliação das regras de modelo é feita pelo Agente ESET Management, não pelo ESET PROTECT Servidor (apenas o resultado é enviado para o ESET PROTECT Servidor). O processo de avaliação acontece de acordo com as regras que estão configuradas em um modelo. Veja abaixo alguns exemplos do processo de avaliação das regras de modelo.

É preciso distinguir entre um teste para existência (algo que não existe dentro daquele valor) e um teste para diferença (algo que existe mas com um valor diferente). Aqui estão algumas regras básicas para fazer essa distinção:
• Para verificar a existência: Operação sem negação (**AND**, **OR**) e operador sem negação (**=**, **>**, **<**, **contém**,...).
• Para verificar a existência de um valor diferente: Operação **AND** e operadores incluindo pelo menos uma negação (**=**, **>**, **<**, **contém**, **não contém**,...).
• Para verificar a não existência de um valor: Operações sem negação (**NAND**, **NOR**) e operadore sem negação (**=**, **>**, **<**, **contém**,...).
Para verificar a presença de uma lista de itens (por exemplo, uma lista específica de aplicativos instalados em um computador), é preciso criar um modelo de Grupo dinâmico separado para cada item na lista e atribuir o modelo a um Grupo dinâmico separado, com cada Grupo dinâmico sendo um subgrupo de outro Grupo dinâmico. Os computadores com a lista de itens estão no último subgrupo.

Status é um agrupamento com várias informações. Algumas fontes oferecem mais de um status dimensional por máquina (por exemplo: sistema operacional, tamanho de RAM, etc.), outras fornecem informações multidimensionais de status (por exemplo: endereço IP, aplicativo instalado, etc.).

Veja abaixo uma representação visual do status de um cliente:

Adaptadores de rede - endereço IP	Adaptadores de rede - endereço MAC	Nome do SO	Versão do SO	HW - tamanho de RAM em MB	Aplicativo instalado
192.168.1.2	4A-64-3F-10-FC-75	Windows 7 Enterprise	6.1.7601	2048	ESET Endpoint Security
10.1.1.11	2B-E8-73-BE-81-C7				Leitor de PDF
124.256.25.25	52-FB-E5-74-35-73				Conjunto Office
					Previsão do tempo

O status é feito de grupos de informações. Um grupo de dados sempre fornece informações coerentes organizadas em fileiras. O número de fileiras por grupo pode variar.

As condições são avaliadas por grupo e por fileira - se houverem mais condições em relação às colunas de um grupo, apenas os valores da mesma fileira são considerados.

Exemplo 1:

Para este exemplo, considere a condição a seguir:

```
Adaptadores de rede.Endereço IP = 10.1.1.11 AND Adaptadores de rede.Endereço MAC = 4A-64-3F-10-FC-75
```

Essa permissão não é compatível com nenhum computador, pois não há uma fileira onde ambas as condições sejam verdadeiras.

Adaptadores de rede - endereço IP	Adaptadores de rede - endereço MAC	Nome do SO	Versão do SO	HW - tamanho de RAM em MB	Aplicativo instalado
192.168.1.2	4A-64-3F-10-FC-75	Windows 7 Enterprise	6.1.7601	2048	ESET Endpoint Security
10.1.1.11	2B-E8-73-BE-81-C7				Leitor de PDF

Adaptadores de rede - endereço IP	Adaptadores de rede - endereço MAC	Nome do SO	Versão do SO	HW - tamanho de RAM em MB	Aplicativo instalado
124.256.25.25	52-FB-E5-74-35-73				Conjunto Office
					Previsão do tempo

Exemplo 2:

Para este exemplo, considere a condição a seguir:

```
Adaptadores de rede.Endereço IP = 192.168.1.2 AND Adaptadores de rede.Endereço MAC =
 4A-64-3F-10-FC-75
```

Desta vez, ambas as condições são compatíveis com células na mesma fileira e, portanto, a permissão como um todo é avaliada como VERDADEIRO. O computador é selecionado.

Adaptadores de rede - endereço IP	Adaptadores de rede - endereço MAC	Nome do SO	Versão do SO	HW - tamanho de RAM em MB	Aplicativo instalado
192.168.1.2	4A-64-3F-10-FC-75	Windows 7 Enterprise	6.1.7601	2048	ESET Endpoint Security
10.1.1.11	2B-E8-73-BE-81-C7				Leitor de PDF
124.256.25.25	52-FB-E5-74-35-73				Conjunto Office
					Previsão do tempo

Exemplo 3:

Para condições com o operador OR (pelo menos uma condição deve ser VERDADEIRO), como:

```
Adaptadores de rede.Endereço IP = 10.1.1.11 OR Adaptadores de rede.Endereço MAC = 4A
-64-3F-10-FC-75
```

A permissão é VERDADEIRO para duas fileiras, pois apenas uma das condições deve ser cumprida. O computador é selecionado.

Adaptadores de rede - endereço IP	Adaptadores de rede - endereço MAC	Nome do SO	Versão do SO	HW - tamanho de RAM em MB	Aplicativo instalado
192.168.1.2	4A-64-3F-10-FC-75	Windows 7 Enterprise	6.1.7601	2048	ESET Endpoint Security
10.1.1.11	2B-E8-73-BE-81-C7				Leitor de PDF
124.256.25.25	52-FB-E5-74-35-73				Conjunto Office
					Previsão do tempo

Modelo de grupo dinâmico - exemplos

Você pode encontrar modelos úteis de Grupo dinâmico predefinidos em **Mais** > **Modelos de grupo dinâmico**.

Os modelos do Grupo Dinâmico de amostra e seus exemplos de uso neste guia demonstram algumas das maneiras que você pode usar Grupos dinâmicos para gerenciar sua rede:

Grupo dinâmico que detecta se um produto de segurança está instalado
Grupo dinâmico que detecta se uma versão específica de um software está instalada
Grupo dinâmico que detecta se uma versão específica do software não está instalada
Grupo dinâmico que detecta se uma versão específica do software não está instalada, mas existe uma outra versão
Grupo dinâmico que detecta se um computador está em uma subrede específica
Grupo dinâmico que detecta versões instaladas mas não ativadas dos produtos de segurança do servidor
Automaticamente produtos ESET em áreas de trabalho do Windows recentemente conectadas
Forçar a política baseada em localização

Consulte também nossos **artigos da Base de conhecimento** com exemplos de modelos de Grupos dinâmicos e seu uso:

Exemplos úteis de modelos de Grupo dinâmico no ESET PROTECT - exemplos de como você pode usar detalhes do Inventário HW para criar regras para um Grupo dinâmico que podem conter os dispositivos que cumprem com os critérios HW selecionados.
Configure o ESET PROTECT para instalar automaticamente produtos ESET endpoint em computadores não protegidos
Configure endpoints para usarem configurações de atualização diferentes dependendo da rede na qual estão conectados usando o ESET PROTECT
Crie um novo certificado para novas estações de trabalho para entrar automaticamente em um Grupo dinâmico no ESET PROTECT

Artigos da Base de conhecimento podem não estar disponíveis no seu idioma.

Naturalmente, existem muitos outros objetivos que podem ser alcançados com Modelos de grupos dinâmicos com uma combinação de regras. As possibilidades são quase infinitas.

O ESET Enterprise Inspector e o ESET Dynamic Threat Defense foram renomeados para ESET Inspect e ESET LiveGuard Advanced.
Você pode precisar resolver os problemas causados pela renomeação se você atualizou do ESET PROTECT 9.0 e versões anteriores e tem relatórios, grupos dinâmicos, notificações ou outros tipos de regras que filtram por ESET Dynamic Threat Defense ou ESET Enterprise Inspector.

Grupo dinâmico - um produto de segurança está instalado

Este grupo dinâmico pode ser usado para executar uma tarefa imediatamente depois do produto de segurança ESET ser instalado em uma máquina: Ativação, Rastreamento personalizado, etc.

Você pode criar um **Novo modelo** sob **Mais** > **Modelos de grupo dinâmico** e criar um novo Grupo dinâmico com modelo.

Básico

Insira um **Nome** e uma **Descrição** para o novo modelo de grupo dinâmico.

Expressão

1.Selecione um operador lógico no menu Operação: **AND** (todas as condições precisam ser verdadeiras).

2.Clique em **+ Adicionar regra** e selecione uma condição. Selecione **Computador** > **Máscara de produtos gerenciados** > **é um dos** > **Protegido pela ESET: Área de trabalho**. Você também pode escolher diferentes produtos da ESET.

Resumo

Revise as configurações definidas e clique em **Concluir** para criar o modelo. Este novo modelo será adicionado na lista de todos os modelos e pode ser usado mais tarde para criar um novo Grupo dinâmico.

Grupo dinâmico - uma versão de software específica está instalada

Este grupo dinâmico pode ser usado para detectar software de segurança ESET instalado em uma máquina. Então você será capaz de executar, por exemplo, uma tarefa de atualização ou executar o comando personalizado nessas máquinas. Operadores diferentes como **“contém"** ou **“tem prefixo"** podem ser usados.

Você pode criar um **Novo modelo** sob **Mais** > **Modelos de grupo dinâmico** e criar um novo Grupo dinâmico com modelo.

Básico

Insira um **Nome** e uma **Descrição** para o novo modelo de grupo dinâmico.

Expressão

1.Selecione um operador lógico no menu Operação: **AND** (todas as condições precisam ser verdadeiras).

2.Clique em **+ Adicionar regra** e selecione uma condição:

- **Software instalado** > **Nome do aplicativo** > **= (igual)** > *ESET Endpoint Security*
- **Software instalado** > **Versão do aplicativo** > **= (igual)** > *6.2.2033.0*

Resumo

Revise as configurações definidas e clique em **Concluir** para criar o modelo. Este novo modelo será adicionado na

lista de todos os modelos e pode ser usado mais tarde para criar um novo Grupo dinâmico.

Grupo dinâmico - uma versão específica de um software não está instalada

Este grupo dinâmico pode ser usado para detectar software de segurança ESET faltando em uma máquina. As configurações desse exempli incluirão máquinas que não contêm o software ou máquinas com versões diferentes da especificada.

Esse grupo é útil porque você será capaz de executar tarefas de instalação do software nos computadores para instalar ou atualizar. Operadores diferentes como **“contém"** ou **“tem prefixo"** podem ser usados.

Clique em **Novo modelo** em **Mais** > **Modelos de grupo dinâmico**.

Básico

Insira um **Nome** e uma **Descrição** para o novo modelo de grupo dinâmico.

Expressão

1.Selecione um operador lógico no menu Operação: **NAND** (pelo menos uma condição precisa ser falsa).

2.Clique em **+ Adicionar regra** e selecione uma condição:

- **Software instalado** > **Nome do aplicativo** > **= (igual)** > *ESET Endpoint Security*
- **Software instalado** > **Versão do aplicativo** > **= (igual)** > *6.2.2033.0*

Resumo

Revise as configurações definidas e clique em **Concluir** para criar o modelo. Este novo modelo será adicionado na lista de todos os modelos e pode ser usado mais tarde para criar um novo Grupo dinâmico.

Grupo dinâmico - uma versão específica de um software não está instalada, mas existe outra versão

Este grupo dinâmico pode ser usado para detectar um software que está instalado, mas com uma versão diferente da que você está solicitando. Este grupo é útil porque você será capaz de executar tarefas de atualização nas máquinas onde a versão necessária está faltando. Operadores diferentes podem ser usados, mas certifique-se que o teste de versão é feito com o operador de negação.

Clique em **Novo modelo** em **Mais** > **Modelos de grupo dinâmico**.

Básico

Insira um **Nome** e uma **Descrição** para o novo modelo de grupo dinâmico.

Expressão

1.Selecione um operador lógico no menu Operação: **AND** (todas as condições precisam ser verdadeiras).

2.Clique em **+ Adicionar regra** e selecione uma condição:

- **Software instalado** > **Nome do aplicativo** > **= (igual)** > *ESET Endpoint Security*
- **Software instalado** > **Versão do aplicativo**> **≠ (desigual)** > *6.2.2033.0*

Resumo

Revise as configurações definidas e clique em **Concluir** para criar o modelo. Este novo modelo será adicionado na lista de todos os modelos e pode ser usado mais tarde para criar um novo Grupo dinâmico.

Grupo dinâmico - um computador está em uma subrede específica

Este grupo dinâmico pode ser usado para detectar uma subrede específica. Então isso pode ser usado para aplicar uma política personalizada para o controle da web ou atualização. Você pode especificar intervalos diferentes.

Clique em **Novo modelo** em **Mais** > **Modelos de grupo dinâmico**.

Básico

Insira um **Nome** e uma **Descrição** para o novo modelo de grupo dinâmico.

Expressão

1.Selecione um operador lógico no menu Operação: **AND** (todas as condições precisam ser verdadeiras).

2.Clique em **+ Adicionar regra** e selecione uma condição:

- **Endereços IP de rede** > **Endereço IP do adaptador** > **≥ (mais ou igual)** > *10.1.100.1*
- **Endereços IP de rede** > **Endereço IP do adaptador** > **≤ (menor ou igual)** > *10.1.100.254*
- **Endereços IP de rede** > **Máscara do adaptador subrede** > **= (igual)** > *255.255.255.0*

Resumo

Revise as configurações definidas e clique em **Concluir** para criar o modelo. Este novo modelo será adicionado na lista de todos os modelos e pode ser usado mais tarde para criar um novo Grupo dinâmico.

Grupo dinâmico - versão instalada mas não ativada do produto de segurança do servidor

Este grupo dinâmico pode ser usado para detectar produtos de servidor inativos. Assim que esses produtos forem detectados, você pode atribuir uma tarefa de cliente para este grupo, para ativar computadores cliente com a licença adequada. Neste exemplo apenas o ESET Mail Security for Microsoft Exchange Server é detectado, mas você pode especificar vários produtos.

Clique em **Novo modelo** em **Mais** > **Modelos de grupo dinâmico**.

Básico

Insira um **Nome** e uma **Descrição** para o novo modelo de grupo dinâmico.

Expressão

1.Selecione um operador lógico no menu Operação: **AND** (todas as condições precisam ser verdadeiras).

2.Clique em **+ Adicionar regra** e selecione uma condição:

- **Computador** > **Máscara de produtos gerenciados** > **é um dos** > **Protegido pela ESET: Servidor de email**
- **Problemas de proteção/funcionalidade**> **Fonte** > **= (igual)** > **Produto de segurança**
- **Problemas de proteção/funcionalidade** > **Problema** > = **(igual)** > **Produto não ativado**

Resumo

Revise as configurações definidas e clique em **Concluir** para criar o modelo. Este novo modelo será adicionado na lista de todos os modelos e pode ser usado mais tarde para criar um novo Grupo dinâmico.

Como automatizar ESET PROTECT

Usando técnicas como no exemplo abaixo, você pode automatizar várias ações, desde atualizações de produtos e sistema operacional, rastreamento, ativações automáticas de produtos adicionados recentemente com licenças pré-selecionadas, até a solução de incidentes sofisticados.

Automaticamente produtos ESET em áreas de trabalho do Windows recentemente conectadas

⚠ Este exemplo deve ser realizado apenas em clientes sem software de segurança de terceiros ou o software de segurança ESET do segmento doméstico (p. ex. ESET Smart Security). A instalação de produtos ESET em clientes com software de segurança de terceiros não é recomendada. Você pode usar o ESET AV Remover Para remover outros programas de antivírus do seu computador.

1. Cria um grupo dinâmico chamado *Sem produto de segurança*.
a.Torne-o um grupo secundário do grupo predefinido **Computadores Windows** > **Windows (desktops)**.
b.Clique em **Novo modelo**.
c.Adicione a regra a seguir: **Computador** > **Máscara de produtos gerenciados**.
d.Como operador, selecione **desigual**.
e.Selecione a máscara **protegida pela ESET: Área de trabalho**
f.Clique em **Concluir** para salvar o grupo.
2. Navegue para **Tarefas** > **Nova** > **Tarefa de cliente**.
a.Selecione **Instalação de software** no menu suspenso Tarefa e digite o nome da tarefa em **Nome.**
b.Escolha o pacote na seção **Configurações** e defina outros parâmetros, se necessário.
c.Clique em **Concluir** > **Criar acionador**.
d.Na seção **Destino**, clique em **Adicionar grupos** e selecione *Sem o produto de segurança*.
e.Na seção **Acionador**, selecione **Acionador de grupo dinâmico ingressado**.
f.Clique em **Concluir** para salvar a tarefa e o acionador.
Esta tarefa será executada em clientes conectados ao grupo dinâmico a partir deste momento. Você precisará executar essa tarefa manualmente em clientes que estavam no grupo dinâmico antes da tarefa ser criada.

Forçar a política baseada em localização

1. Cria um grupo dinâmico chamado *Subrede 120*.
a.Faça um grupo secundário do grupo **Todos**.
b.Clique em **Novo modelo**.
c.Adicionar regra: **Endereços IP de rede** > **IP da subrede.**
d.Como operador, selecione **igual**.
e.Insira a subrede que deseja filtrar, por exemplo, 10.1.120.0 (o último número precisa ser 0 para filtrar todos os endereços IP da subrede 10.1.120.).
f.Clique em **Concluir** para salvar o grupo.
2. Navegue para **Políticas**.
a.Clique em **Nova política** e dê um **Nome** para a política.
b.Na seção **Configurações**, selecione Agente **ESET Management**.
c.Faça a alteração da política; por exemplo, altere o **Intervalo de conexão** para 5 minutos.
d.Na seção **Atribuir**, clique em **Atribuir** e selecione a caixa de seleção ao lado da *Subrede 120* do seu grupo e clique em **OK** para confirmar.
e.Clique em **Concluir** para salvar a política.
Esta política será aplicada em clientes conectados ao grupo dinâmico a partir deste momento.

Consulte as regras de remoção de política para verificar o que acontece para as configurações de política aplicadas quando a máquina do cliente sai do grupo dinâmico (as condições que atendem aos critérios de participação no grupo dinâmico não são mais válidas).

Veja outros exemplos de Modelos de grupo dinâmico.

O ESET Enterprise Inspector e o ESET Dynamic Threat Defense foram renomeados para ESET Inspect e ESET LiveGuard Advanced.
Você pode precisar resolver os problemas causados pela renomeação se você atualizou do ESET PROTECT 9.0 e versões anteriores e tem relatórios, grupos dinâmicos, notificações ou outros tipos de regras que filtram por ESET Dynamic Threat Defense ou ESET Enterprise Inspector.

Gerenciamento de licenças

Ao adquirir qualquer produto de licenciamento comercial da ESET, você receberá automaticamente acesso ao ESET PROTECT. Você pode gerenciar facilmente suas licenças através do ESET PROTECT no menu principal sob **Mais** > **Gerenciamento de licenças**.Se você já tem um Usuário e Senha emitidos pela ESET que deseja converter para uma chave de licença, consulte Converter credenciais de licença de legado. O Nome de usuário e Senha foram substituídos por uma Chave de licença/ID pública. Uma Chave de licença é uma sequência única usada para identificar o proprietário da licença e a própria ativação.

Você pode ativar seu produto empresarial ESET usando o ESET PROTECT.

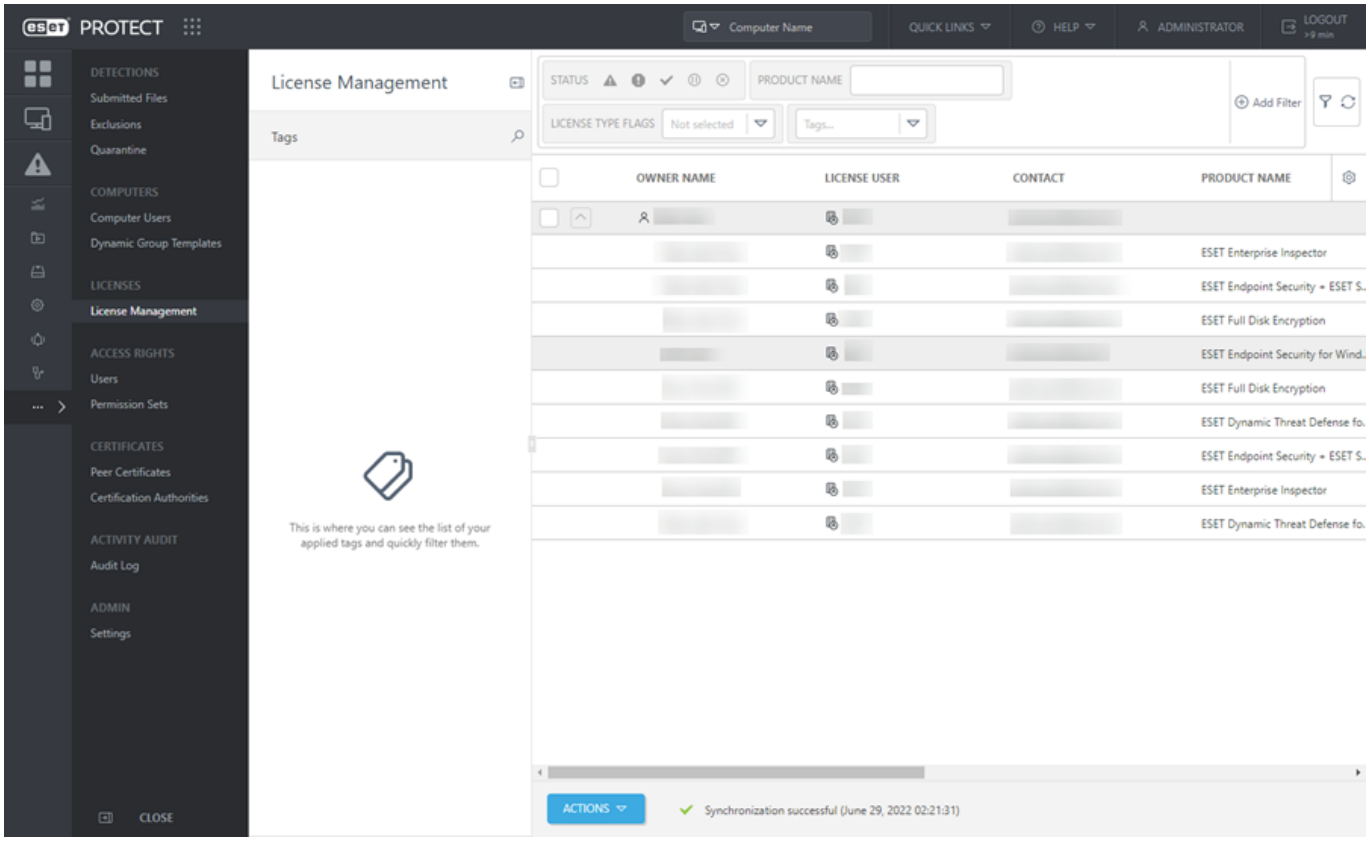
Permissões para gerenciamento de licenças

Cada usuário pode receber a atribuição de uma permissão para Licenças. As permissões são válidas apenas para licenças contidas no grupo estático para onde aquele conjunto de permissões foi atribuído. Cada tipo de permissão permite ao usuário realizar ações diferentes.

Apenas administradores cujo grupo inicial está definido como **Todos**, com permissão de **Gravação** em licenças no grupo inicial, podem adicionar ou remover licenças. Cada licença é identificada por seu **ID Público** e pode ter uma ou mais unidades. As licenças podem ser distribuídas pelo Administrador apenas para outros usuários com permissões suficientes. Uma licença não está registrada.

As licenças do ESET MSP Administrator 2 são divididas em um pool para cada empresa. Você não pode mover uma licença para fora do pool.

Gerenciamento de licenças no console web



As licenças do mesmo usuário ESET Business Account ou da mesma empresa são agrupadas em conjuntos de

licenças. Clique em para expandir o pool de licenças e ver os detalhes da licença.

No ESET Business Account e ESET PROTECT, cada licença é identificada por meio de:

- **ID pública**
- **Tipo de licença** – **Business** (licença paga), **Trial** (licença de avaliação), **MSP** (licença do provedor de serviços gerenciados) e **NFR** (licença com revenda proibida).

Informações adicionais da licença incluem:

- O **Nome do proprietário** da licença e **Contato**.
- O nome e tipo da **Licença do usuário**: **Empresa**, **Site**, **Cliente MSP**.
- O **Nome do produto** de segurança para o qual a licença se destina.
- O **Status** da licença (se a licença estiver expirada, usada em excesso ou com risco de expiração ou uso em excesso, uma mensagem de alerta será exibida aqui).
- O número de **Unidades** que podem ser ativadas com esta licença e número de unidades off-line. Para produtos ESET Mail Security, o uso da licença é calculado com base nas **Subunidades** usadas para ativação.
- O número de **Subunidades** de produtos do servidor ESET (caixas de correio, proteção de gateway, conexões).
- A **data** de expiração da licença.
  - Licenças de assinatura podem não ter uma data de validade.

Você pode filtrar licenças por seu **Status**:

OK – Verde	Sua licença foi ativada com sucesso.
Erro(s) – Vermelho	A licença não está registrada, expirou ou foi usada em excesso.
Aviso(s) – Laranja	Laranja - sua licença ainda está esgotada ou está prestes a expirar (a expiração acontecerá em 30 dias).
Desativado ou suspenso	Sua licença foi desativada ou suspensa.
Obsoleto	A sua licença expirou.

As licenças expiradas e usadas em excesso (no estado de **Erro** ou **Obsoleto**) não estão visíveis na lista de licenças disponíveis no Assistente do instalador tudo-em-um, tarefa do cliente de Ativação do produto e tarefa do cliente de Instalação de software.

Clique no botão **Ações** para gerenciar o(s) pool(s) de licenças selecionado(s):

Marcações	Editar marcações (atribuir, remover atribuição, criar, remover).

Adicionar licenças	Clique em **Adicionar licenças** e selecione o método que deseja usar para adicionar suas novas licenças: 1.**ESET Business Account ou ESET MSP Administrator** – conecte um ESET Business Account ou EMA 2 e adicione todas as suas licenças à seção **Gerenciamento de licenças**. 2.**Chave de licença** - Insira uma chave de licença para uma licença válida e clique em **Adicionar licenças**. A chave de licença será verificada no servidor de ativação e adicionada à lista. 3.**Arquivo de licença off-line** - Adicione um arquivo de licença (*.lf*) e clique em **Adicionar licença**. O arquivo de licença será verificado e a licença será adicionada à lista. Você pode ver como a licença foi adicionada com base no ícone na coluna **Nome do proprietário**: **Arquivo de licença off-line**, **Chave de licença** ou **ESET Business Account ou ESET MSP Administrator**.
Remover licenças	Remove o pool de licença selecionado. Será solicitada confirmação dessa ação. A remoção da licença não inicia a desativação do produto. Seu produto ESET continuará ativado mesmo depois da licença ser removida no **Gerenciamento de licenças** ESET PROTECT.
Grupo de acesso > **Mover**	Mova o objeto para outro grupo estático onde ele está disponível para usuários com direitos suficientes para o grupo de destino. Alterar o Grupo de acesso é útil ao resolver problemas de acesso com outros usuários. O Grupo de acesso define o grupo estático do objeto e o acesso ao objeto com base nos direitos de acesso do usuário.
Sincronizar licenças	Atualizar informações da licença no ESET PROTECT imediatamente. As licenças são sincronizadas automaticamente uma vez por dia com os servidores de licença da ESET. Se você estiver usando o ESET Business Account, ou ESET MSP Administrator, as licenças serão sincronizadas automaticamente uma vez por dia também com esses serviços.
Abrir EBA	Abra o portal ESET Business Account. Esta ação está disponível apenas se você adicionou licenças de ESET Business Account.
Abrir EMA	Abra o portal ESET MSP Administrator. Esta ação está disponível apenas se você adicionou licenças de ESET MSP Administrator.

Expanda um pool de licenças e clique em uma licença para executar as seguintes ações. O conjunto de ações depende do tipo de licença selecionada:

Use a licença para ativação	Executar a Tarefa de ativação do produto usando essa licença.
Marcações	Editar marcações (atribuir, remover atribuição, criar, remover).
Gerenciar licenças	Se a licença for sincronizada do ESET Business Account ou ESET MSP Administrator, você poderá gerenciar a licença. Se a licença estiver sendo usada em excesso, você pode aumentar a capacidade da licença ou desativar alguns dos seus dispositivos.
Renovar licença	Renove a licença expirando, expirada, suspensa ou desativada no ESET Business Account ou ESET MSP Administrator.
Atualizar licença	Atualize a licença de avaliação no ESET Business Account ou ESET MSP Administrator.
Relatório de auditoria	Exibe o Relatório de auditoria para o item selecionado.
Copiar ID público de licença	Copie o ID da licença pública para a área de transferência.

Licenças de assinatura

O ESET PROTECT é compatível com o gerenciamento de licenças de assinatura. Essas licenças podem ser adicionadas usando o ESET Business Account ou ESET MSP Administrator ou uma Chave de licença. Você pode verificar a validade da sua assinatura em **Gerenciamento de licenças** na coluna **Validade** ou em **Computadores** >

Detalhes. Não é possível criar um arquivo de licença off-line de uma licença de assinatura.

Suporte para sites ESET Business Account

Agora você pode importar a estrutura completa do seu ESET Business Account, incluindo a distribuição de licenças entre os locais.

Ativação de produtos empresariais ESET

Você pode distribuir licenças para produtos ESET do ESET PROTECT usando duas tarefas:

- A tarefa de instalação de software
- A tarefa de ativação de produtos

Desativação de produtos empresariais ESET

Você pode desativar o produto empresarial ESET (remover a licença do produto) de várias maneiras usando o Console web ESET PROTECT:

- em **Computadores**, selecione o(s) computador(es) e selecione **Desativar produto** – remove a licença de todos os dispositivos selecionados através do servidor de licença da ESET. O produto é desativado mesmo se ele não foi ativado do ESET PROTECT ou se a licença não é gerenciada pelo ESET PROTECT.

> Se você selecionar apenas um computador com mais produtos ESET instalados (por exemplo, produto endpoint ESET e Connector do ESET Inspect), poderá optar por desativar produtos individuais.

- Remover computador do gerenciamento
- Crie a tarefa Remover computadores não conectando com a opção **Desativar licença**.

Filtros e personalização de layout

Você pode personalizar a exibição da tela atual do console web:

- Gerenciar o painel lateral e a tabela principal.
- Adicionar filtro e predefinições de filtro. Você pode usar marcações para filtrar os itens exibidos.

Compartilhar licenças entre os administradores de filiais

Existem três usuários e um Administrador, cada usuário tem seu próprio grupo inicial:
• *John*, *San Diego*
• *Larry*, *Sydney*
• *Makio*, *Tóquio*
O Administrador importa 3 licenças. Elas estão contidas no grupo estático Todos e não podem ser usadas por outros usuários.
Para atribuir uma licença a outro usuário, o administrador pode selecionar a caixa de seleção ao lado do pool de licença que deseja atribuir a outro usuário, clicar no botão **Ações** e depois clicar em **Grupo de acesso** > **Mover** e selecionar o grupo onde aquele usuário tem permissão. Para o usuário *John*, selecione no grupo *San Diego*. *John* precisa ter a **Permissão de** uso para **Licenças** no grupo *San Diego* para usar a licença.
Quando o usuário *John* faz login ele pode ver e usar apenas a licença que foi movida para seu grupo. O administrador deve repetir o processo para *Larry* e *Makio*, depois disso, os usuários conseguem ver apenas suas próprias licenças enquanto o Administrador pode ver todas as licenças.

ESET Business Account ou ESET MSP Administrator

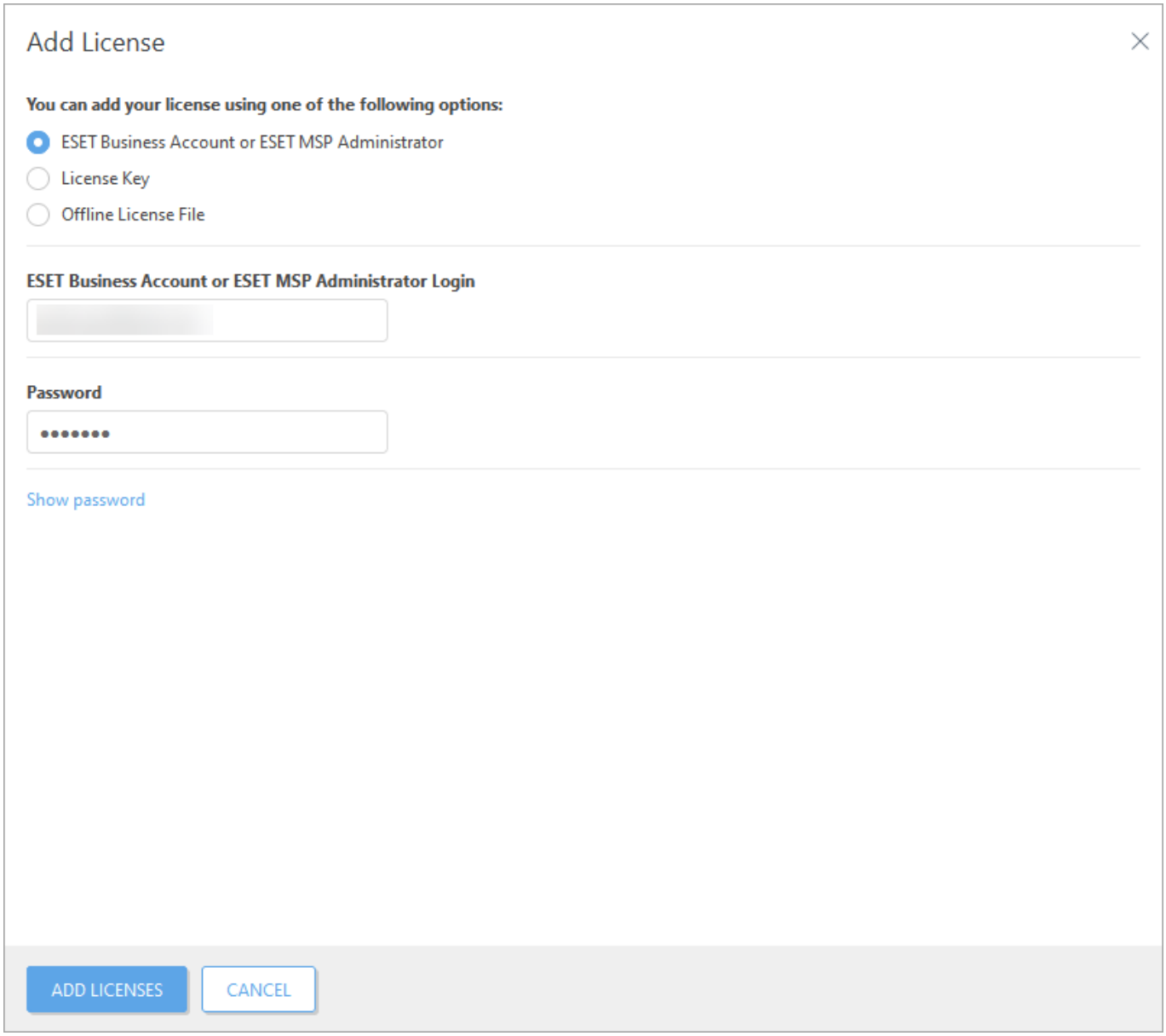
Apenas administradores cujo grupo inicial está definido como **Todos**, com permissão de **Gravação** em licenças no grupo inicial, podem adicionar ou remover licenças. Cada licença é identificada por seu **ID Público** e pode ter uma ou mais unidades. As licenças podem ser distribuídas pelo Administrador apenas para outros usuários com permissões suficientes. Uma licença não está registrada.

ESET Business Account ou ESET MSP Administrator

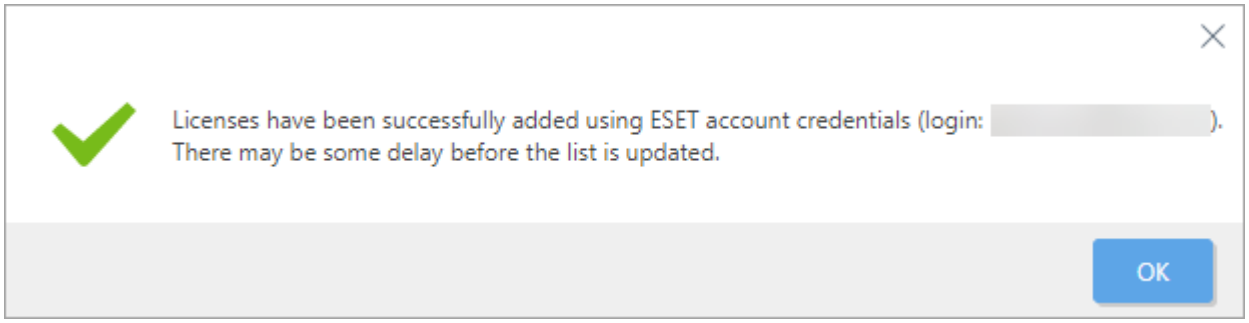
1. Clique em **Mais** > **Gerenciamento de licenças** > **Ações** e clique em **Adicionar licença**.

2. Selecione **ESET Business Account ou ESET MSP Administrator**.

3. Insira as credencias **ESET Business Account ou ESET MSP Administrator 2** (o ESET PROTECT vai exibir todas as licenças delegadas no Gerenciamento de licenças ESET PROTECT).



4. Clique em **Adicionar licenças** para confirmar.



5. O ESET PROTECT agora sincroniza sua estrutura ESET MSP Administrator ou ESET Business Account com a árvore do Grupo estático em **Computadores** no Web Console.

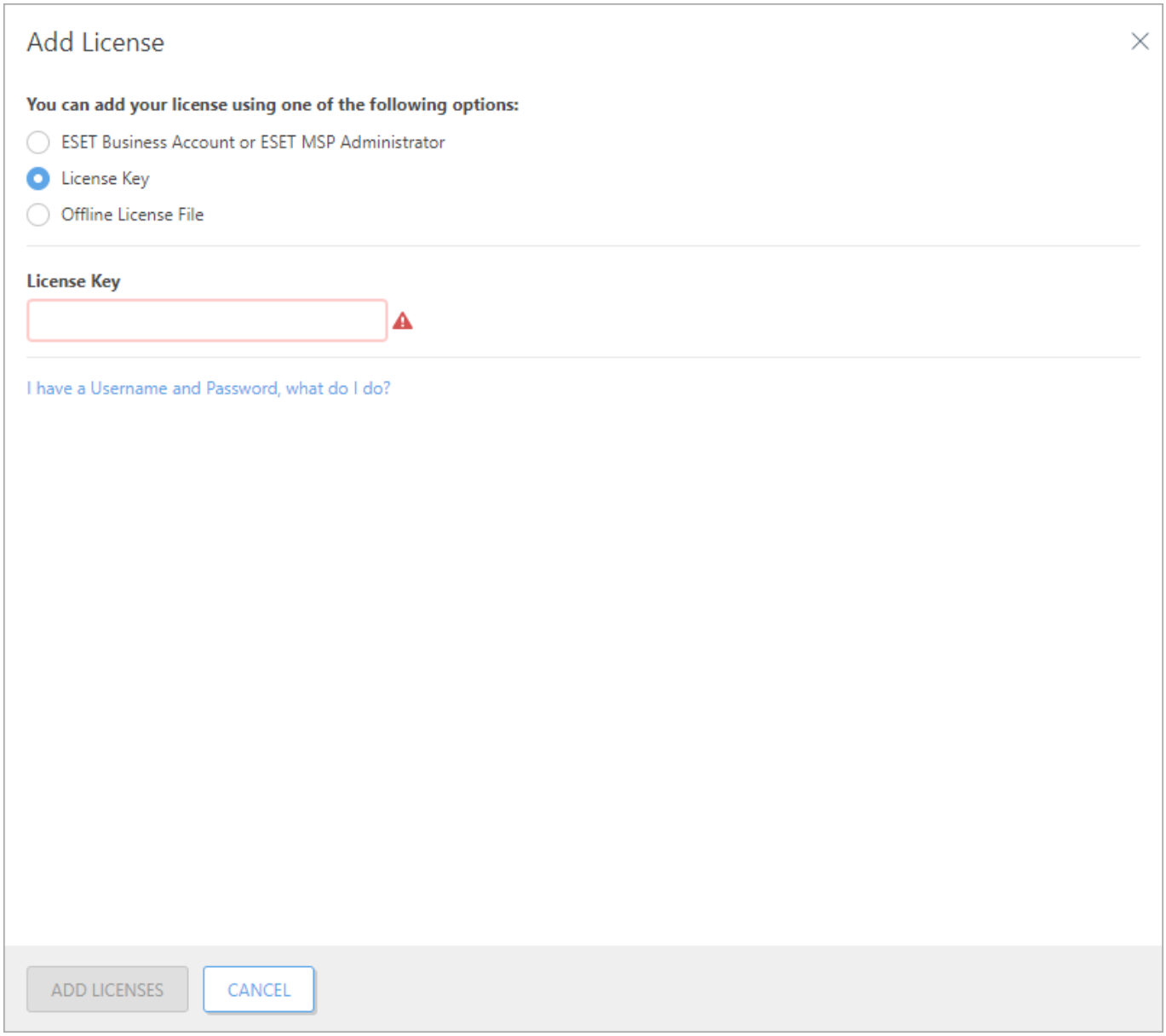
Adicionar Licença - Chave de Licença

Apenas administradores cujo grupo inicial está definido como **Todos**, com permissão de **Gravação** em licenças no grupo inicial, podem adicionar ou remover licenças. Cada licença é identificada por seu **ID Público** e pode ter uma ou mais unidades. As licenças podem ser distribuídas pelo Administrador apenas para outros usuários com permissões suficientes. Uma licença não está registrada.

Chave de licença

Digite ou copie e cole a **Chave de licença** que você recebeu quando comprou sua solução de segurança da ESET no campo **Chave de licença** e clique em **Adicionar licenças**.

Se você estiver usando credenciais de licença de legado (um nome de usuário e senha), converta as credenciais em uma chave de licença. Se uma licença não for registrada, ela irá acionar o processo de registro, que será feito no portal EBA (ESET PROTECT fornecerá um URL válido para registro com base na origem na licença).



Ativação off-line

Você pode usar um arquivo de licença do portal ESET Business Account para ativar o ESET PROTECT e outros produtos de segurança ESET.

- Cada arquivo de licença off-line é gerado para apenas um produto, por exemplo o ESET Endpoint Security.

- A licença off-line deve ser usada apenas para clientes que nunca vão ter acesso aos servidores de licença ESET (mesmo se um cliente estiver conectado à internet via proxy com acesso limitado apenas a serviços ESET, não use a licença off-line).

- Não é possível criar um arquivo de licença off-line de uma licença de assinatura.

Para substituir uma licença off-line existente, você precisará

1. Remover a licença antiga no ESET PROTECT e o arquivo de licença no ESET Business Account.

2. Criar nova licença off-line no ESET Business Account.
3. Importar uma nova licença para o ESET PROTECT

4. Reativar produtos com a licença nova.

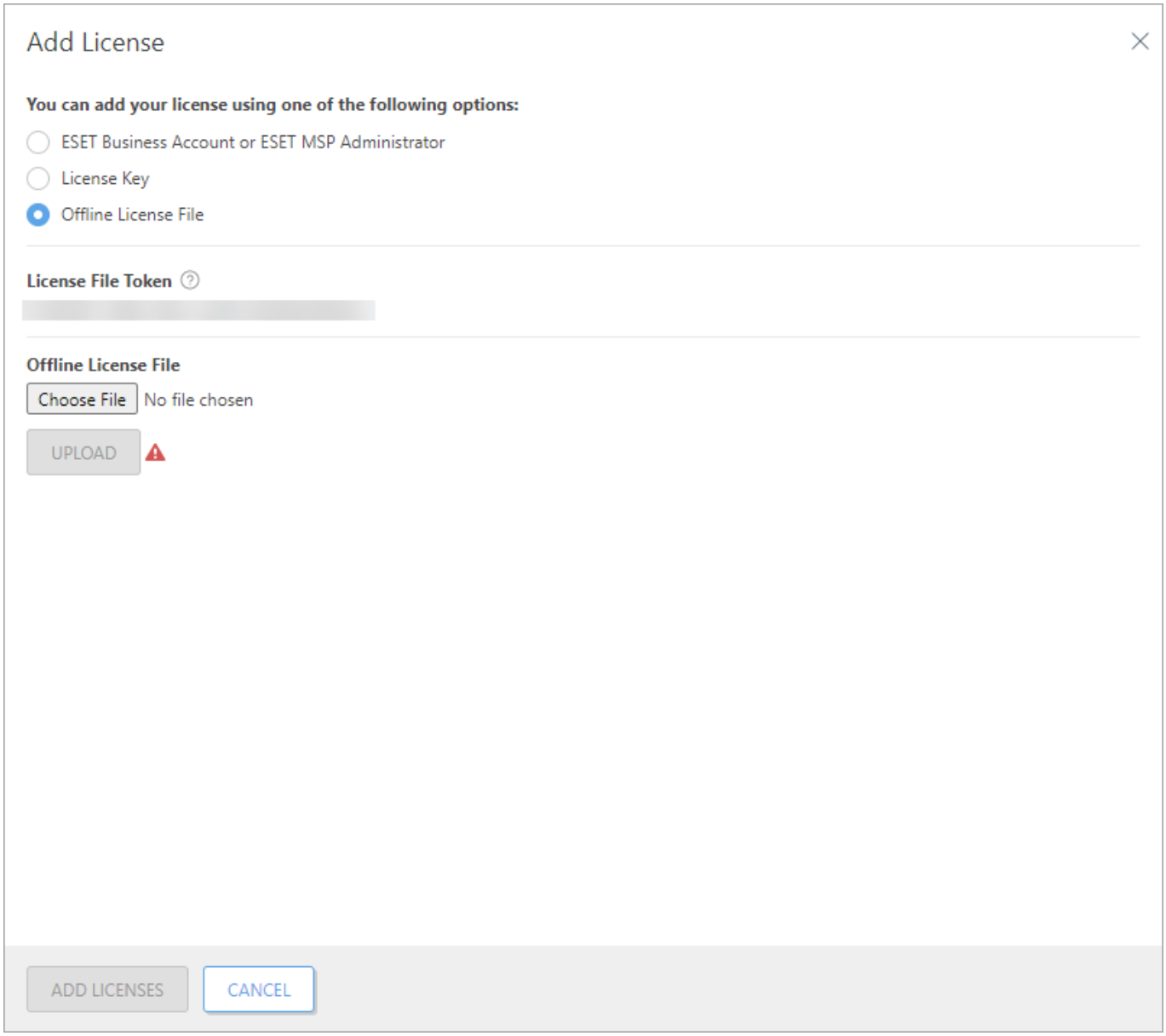
Apenas administradores cujo grupo inicial está definido como **Todos**, com permissão de **Gravação** em licenças no grupo inicial, podem adicionar ou remover licenças. Cada licença é identificada por seu **ID Público** e pode ter uma ou mais unidades. As licenças podem ser distribuídas pelo Administrador apenas para outros usuários com permissões suficientes. Uma licença não está registrada.

Arquivo de licença off-line

Para criar e importar um arquivo de licença off-line, siga esse procedimento:

1. Abra o ESET PROTECT **Gerenciamento de licenças** e clique em **Ações** > **Adicionar licenças**.

2. Selecione o **Arquivo de licença off-line** e copie um **Token de arquivo de licença** específico.

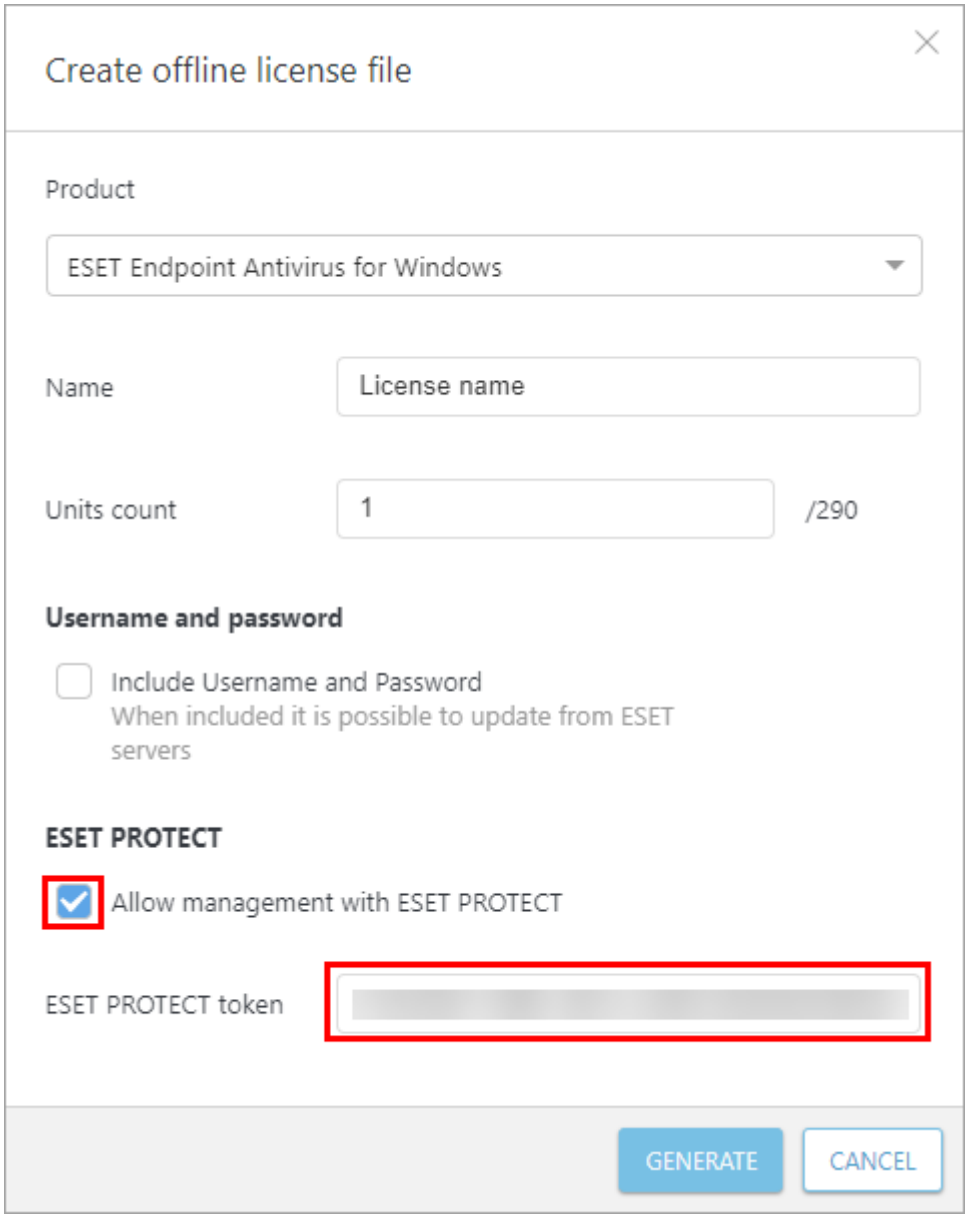


3.Entre na sua ESET Business Account onde você importou sua licença.

4.Selecione a licença que deseja exportar e selecione **Criar arquivos off-line**.

5.Selecione um produto para esse arquivo de licença, insira o **Nome** do arquivo e sua **Contagem de unidade** (número de unidades de licença exportados para o arquivo de licença).

6.Selecione a caixa de verificação ao lado de **Permitir o gerenciamento com o ESET PROTECT** e digite o **Token ESET PROTECT** (**Token do arquivo de licença** do ESET PROTECT).



7.Clique em **Gerar**.

Para fazer download do arquivo siga este procedimento:

1.Selecione a licença e clique em **Mostrar detalhes**.

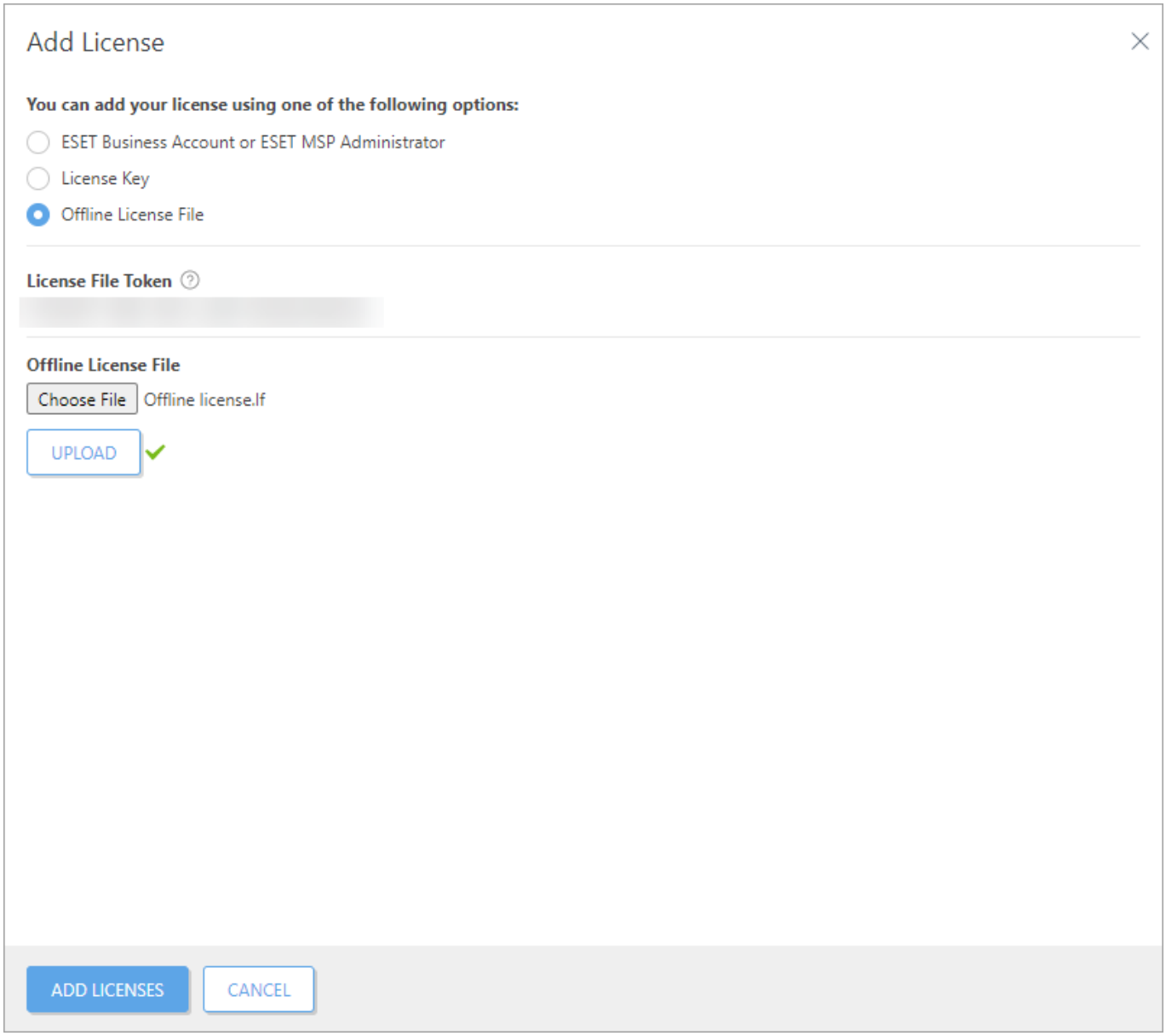
2.Selecione a guia **Arquivos off-line**.

3.Clique no arquivo de licença criado, ele pode ser separado por nome, e selecione **Download**.

Volte para o ESET PROTECT **Gerenciamento de licença**:

1.Clique em **Escolher arquivo** e selecione o arquivo de licença off-line que você exportou no ESET Business Account.

2.Clique em **Carregar** e, em seguida, clique em **Adicionar licenças**.



Direitos de acesso

Direitos de acesso permitem que você gerencie os usuários do console da Web ESET PROTECT e suas permissões.

O modelo de segurança

Estes são os termos principais usados do modelo de segurança:

Termo	Explicação
Grupo inicial	O Grupo inicial é o grupo onde todos os objetos (dispositivos, tarefas, modelos, etc.) criados por um usuário são armazenados automaticamente. Cada usuário deve ter apenas um grupo inicial.
Objeto	Os objetos estão localizados em **Grupos estáticos**. O acesso aos objetos por grupos, não usuários (fornecer acesso por grupos faz com que seja mais fácil acomodar vários usuários, por exemplo, se um usuário estiver de férias). Tarefas do servidor e notificações são exceções que precisam de um usuário "executando".
Grupo de Acesso	O Grupo de acesso define o grupo estático do objeto e o acesso ao objeto com base nos direitos de acesso do usuário.
Administrator	Um usuário com grupo inicial **Todos** e conjunto de permissões total sobre este grupo é efetivamente um administrador.
Direitos de acesso	O direito de acessar um objeto ou executar uma tarefa é atribuído com um Conjunto de permissão. Veja a lista de todos os direitos de acesso e suas funções para mais detalhes.
Conjunto de permissão	Um conjunto de permissões representa as permissões para usuários que acessam o console da Web ESET PROTECT. Elas definem o que o usuário pode fazer ou visualizar no Console da Web ESET PROTECT. Um usuário pode receber a atribuição de vários conjuntos de permissões. Conjuntos de permissões são aplicados apenas em objetos dentro de grupos definidos. Esses **Grupos estáticos** são definidos na seção **Grupos estáticos** ao criar ou editar um conjunto de permissões.
Funcionalidade	Uma funcionalidade é um tipo de objeto ou ação. Normalmente as funcionalidades recebem esses valores: **Leitura**, **Gravação**, **Uso**. A combinação de funcionalidades aplicadas a um Grupo de acesso é chamada de Conjunto de permissão.

Lista de exemplos relacionados de direitos de acesso

Existem vários exemplos em todo o guia de Administração em relação aos direitos de acesso. A lista é essa:

- Como duplicar políticas
- Diferença entre Uso e Gravação
- Como criar uma solução para administradores de filiais
- Como compartilhar objetos através da duplicação
- Como dividir acesso a certificados e autoridades
- Como permitir ao usuário criar instaladores
- Como remover notificações
- Como criar políticas
- Permitir que os usuários vejam todas as políticas
- Compartilhar licenças entre os administradores de filiais

Usuários

O gerenciamento de usuários faz parte da seção **Mais** do console da Web ESET PROTECT.

- Criar um usuário nativo
- Ações do usuário e detalhes do usuário
- Alterar senha do usuário
- Usuários mapeados
- Atribuir um conjunto de permissões a um usuário

Há dois tipos de usuário:

- Usuários nativos - contas de usuário criadas e gerenciadas a partir do console da Web ESET PROTECT.
- Grupos de segurança de domínio mapeado - Contas de usuário gerenciadas e autenticadas pelo Active Directory.

Uma configuração nova do ESET PROTECT tem o **Administrador** (Usuário nativo com o grupo doméstico **Todos** e acesso a tudo) como o único usuário.

• Não recomendamos usar essa Conta do usuário regularmente. Aconselhamos vivamente que crie outra conta administrator ou use os Administradores dos Grupos de segurança de domínio mapeado com a Permissão definida do administrador atribuída a eles. Use a conta padrão do Administrador apenas como uma opção de backup.

• Você também pode criar usuários adicionais com direitos de acesso mais específicos com base nas competências desejadas.

• Opcionalmente, você pode configurar a Autenticação de dois fatores para usuários nativos e grupos de segurança do domínio mapeado. Isto irá aumentar a segurança ao fazer login e acessar o console da Web ESET PROTECT.

Solução de administradores da filial

Se uma empresa tiver dois escritórios, cada um com administradores locais, eles precisar receber mais conjuntos de permissões para grupos diferentes.

Digamos que temos os administradores *John* em *San Diego* e *Larry* em *Sydney*. Ambos precisam cuidar apenas de seus computadores locais, use **Painel, Políticas, Relatórios** e **Modelos de grupos dinâmicos** com suas máquinas. O *Administrador* principal deve seguir estas etapas:

1.Criar novos Grupos estáticos: *Escritório de San Diego*, *Escritório de Sydney.*

2.Crie um novo Conjunto de permissões:

a)**Conjunto de permissões** chamado de *Conjunto de permissões Sydney*, com o grupo estático *Escritório Sydney*, e com permissões de acesso total (excluir **Configurações do servidor**).

b)**Conjunto de permissões** chamado de *Conjunto de permissões San Diego*, com o grupo estático *Escritório San Diego*, e com permissões de acesso total (excluir **Configurações do servidor**).

c)**Conjunto de permissões** chamado de *Grupo Todos / Painel*, com o Grupo estático *Todos*, com as permissões a seguir:

• **Leitura** para **Tarefas de cliente**
• **Uso** para **Modelos de grupo dinâmico**
• **Uso** para **Relatórios e Painel**
• **Uso** para **Políticas**
• **Uso** para **Enviar email**
• **Uso** para **Enviar interceptação SNMP**
• **Uso** para **Exportar relatório para arquivo**
• **Uso** para **Licenças**
• **Gravação** para **Notificações**

3.Criar novo usuário *John* com grupo inicial *escritório San Diego,* atribuído com os conjuntos de permissões *conjunto de permissões San Diego* e *Grupo Todos / Painel*.

4.Criar novo usuário *Larry* com grupo inicial *escritório Sydney,* atribuído com os conjuntos de permissões *conjunto de permissões Sydney* e *Grupo Todos / Painel*.

Se as permissões forem definidas dessa forma, *John* e *Larry* poderão usar as mesmas tarefas e políticas, relatórios e painel, usar os modelos de grupo dinâmico sem restrições, mas cada um deles só pode usar os modelos para máquinas contidas dentro de seus grupos iniciais.

Compartilhando objetos

Se um Administrador quiser compartilhar objetos, como modelos de grupo dinâmico, modelos de relatório ou políticas, as opções a seguir estarão disponíveis:

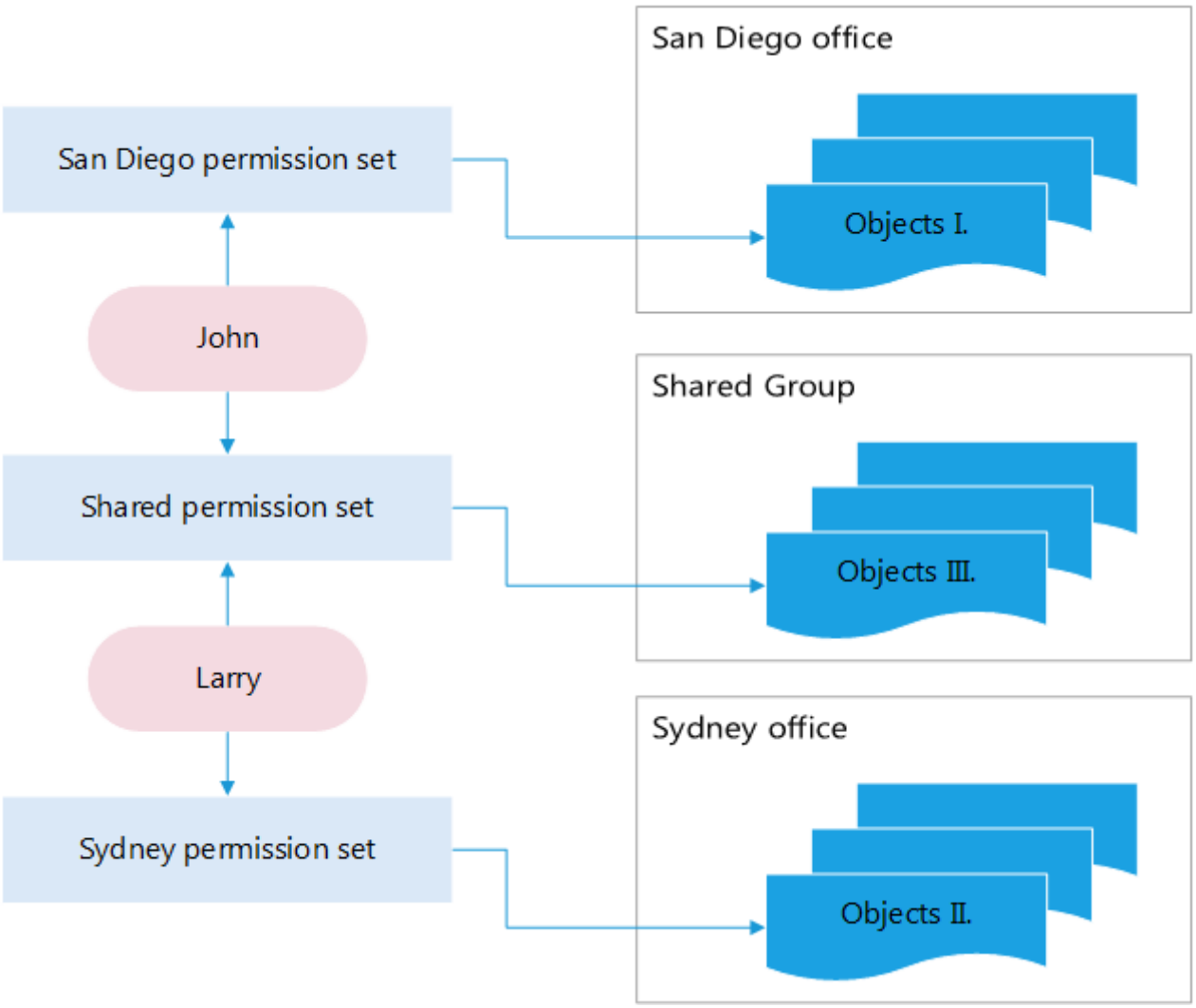
• Mova esses objetos para os grupos compartilhados

• Crie objetos duplicados e mova-os para os grupos estáticos que podem ser acessados por outros usuários (veja o exemplo abaixo)

Para uma duplicação de objeto é preciso que o usuário tenha uma permissão de **Leitura** no objeto original e permissão de **Gravação** em seu **Grupo inicial** para este tipo de ação.
O *Administrador*, cujo grupo inicial é *Todos,* quer compartilhar o *Modelo especial* com o usuário *John*. O modelo foi criado originalmente pelo *Administrador*, portanto ele está automaticamente no grupo *Todos*.
O *Administrator* vai seguir essas etapas:
1.Navegue para **Mais** > **Modelos de grupo dinâmico**.
2.Selecione o *Modelo especial* e clique em **Duplicado**, se necessário, defina o nome e descrição e clique em **Concluir**.
3.O modelo duplicado estará no grupo inicial do *Administrador*, grupo *Todos*.
4.Vá para **Mais** > **Modelos de grupo dinâmico** e selecione o modelo duplicado, clique em **Grupo de acesso** > **Mover** e selecione o grupo estático de destino (onde *John* tem permissão). Clique em **OK**.

Como compartilhar objetos entre mais usuários através do Grupo compartilhado

Para entender melhor como o novo modelo de segurança funciona, veja o esquema abaixo. Existe uma situação onde são dois usuários criados pelo administrador. Cada usuário tem seu próprio grupo inicial com objetos criados por ele. *Conjunto de permissões San Diego* dá a *John* os direitos de manipular *Objetos* em seu grupo inicial. A situação é similar para *Larry*. Se esses usuários não precisarem compartilhar alguns objetos (por exemplo computadores) esses objetos devem ser movidos para o *Grupo compartilhado* (um Grupo estático). É preciso atribuir a ambos os usuários o *Conjunto de permissões compartilhadas* que tem o *Grupo compartilhado* listado na seção **Grupos estáticos**.



Filtros e personalização de layout

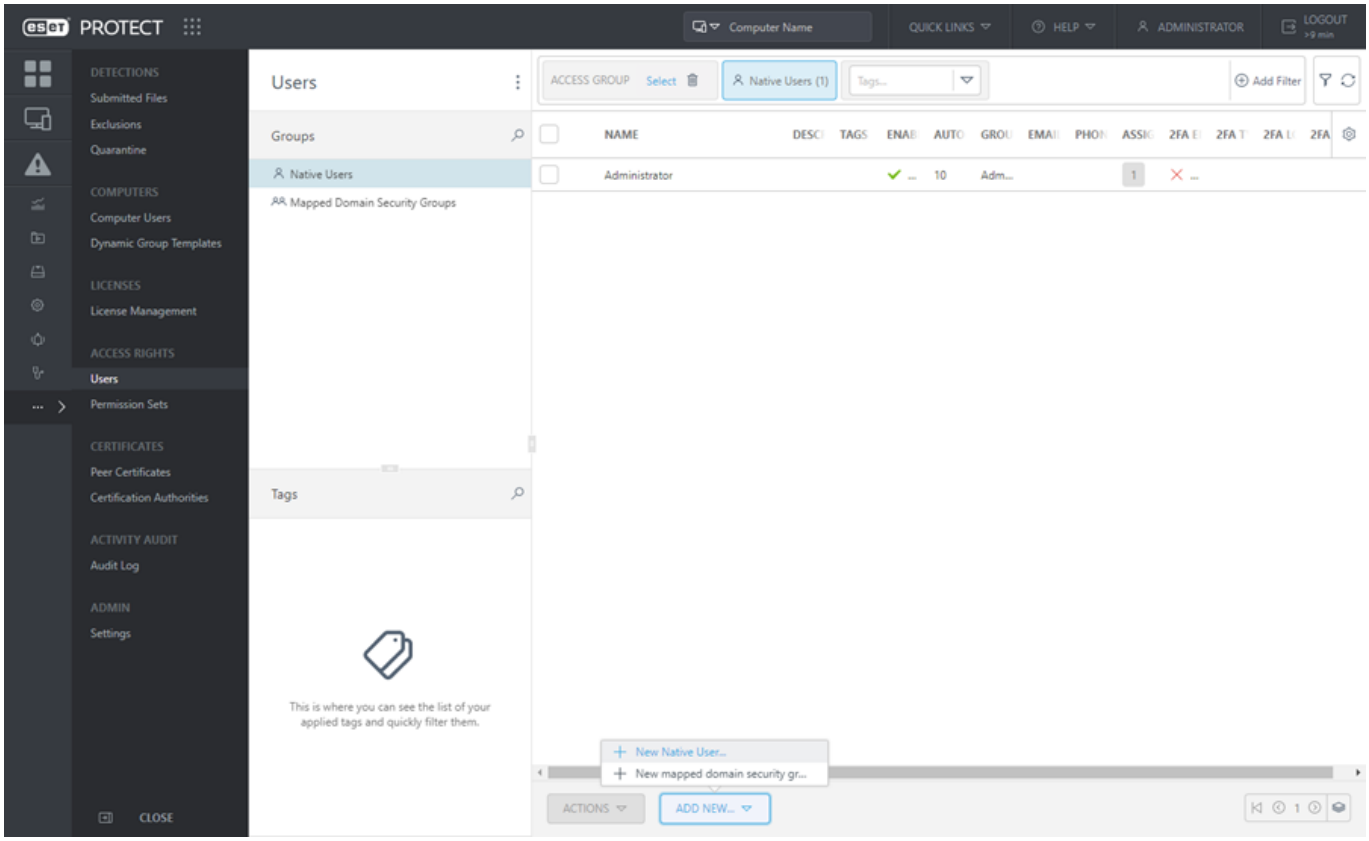
Você pode personalizar a exibição da tela atual do console web:

- Adicionar filtro e predefinições de filtro.
- Você pode usar marcações para filtrar os itens exibidos.

Criar um usuário nativo

Para criar um novo usuário nativo, clique em **Mais** > **Usuários** > **Adicionar novo** > **Novo usuário nativo**.

> Para criar o usuário adequadamente, recomendamos que você siga essas etapas:
> 1.Decida qual grupo estático será o grupo inicial do usuário. Se necessário, crie o grupo.
> 2.Decida qual conjunto de permissões seria o melhor para o usuário. Se necessário, crie um novo conjunto de permissões.
> 3.Siga este capítulo e crie o usuário.



Básico

Insira um nome de **Usuário** e uma **Descrição** opcional para o novo usuário.

Clique em **Selecionar marcações** para atribuir marcações.

Selecionar **Grupo inicial**. Este é o grupo estático onde todos os objetos criados por esse usuário estarão contidos automaticamente.

Grupo doméstico – O grupo doméstico é detectado automaticamente com base no conjunto de permissões atribuído do usuário atualmente ativo.

> Exemplo de cenário:
> A conta de usuário atualmente ativa tem o direito de acesso de **Gravação** para a **Tarefa de cliente de Instalação de software** e a conta do **Grupo doméstico** é "Department_1". Quando o usuário criar uma nova **Tarefa de cliente de instalação de software**, "Department_1" será selecionado automaticamente como o **Grupo doméstico** da tarefa de cliente.

Se o Grupo doméstico pré-selecionado não atender às suas expectativas, você pode selecionar o Grupo doméstico manualmente.

Definir senha

A senha do usuário deve ter pelo menos oito caracteres. A senha não deve conter o nome de usuário.

Conta

Ativado - Selecione esta opção, exceto se quiser que a conta esteja inativa (com o propósito de uso posterior).

É necessário alterar senha – selecione esta opção para forçar o usuário a alterar sua senha na primeira vez que ele entrar no Web Console ESET PROTECT.

Expiração de senha (dias) – essa opção define o número de dias pelos quais a senha é válida (será preciso alterar a senha depois dela expirar).

Logout automático (mín.) - Esta opção define o período de tempo ocioso (em minutos), depois do qual o usuário é desconectado do console da Web. Digite **0** (zero) para desativar o logout automático para o usuário.

Nome completo, **Contato por email** e **Contato telefônico** podem ser definidos para ajudar a identificar o usuário.

Definições de permissão

Você pode atribuir vários conjuntos de permissões a um usuário.

Você pode selecionar uma competência pré-definida (listada abaixo) ou você pode usar um conjunto de permissões personalizado.

- **Conjunto de permissões de revisor** - direitos somente leitura para o grupo **Todos**.
- **Conjunto de permissões do Administrator** - acesso total ao grupo **Todos**.
- **Conjunto de permissões de instalação auxiliada por servidor** - direitos de acesso mínimos necessários para a instalação auxiliada por servidor.
- **Conjunto de permissões de revisor do ESET Inspect** – no mínimo os direitos de acesso somente leitura (para o grupo **Todos**) são necessários para um usuário ESET Inspect.
- **Conjunto de permissões do servidor do ESET Inspect** – direitos de acesso (para o grupo **Todos**) são necessários para o processo de instalação do ESET Inspect e sincronização automática posterior entre o ESET Inspect e o ESET PROTECT.
- **Conjunto de permissões do usuário do ESET Inspect** – direitos de acesso de gravação (para o grupo **Todos**) são necessários para um usuário ESET Inspect.

Cada conjunto de permissões fornece permissões apenas para os objetos contidos nos **Grupos estáticos** selecionados no conjunto de permissões.

Usuários sem nenhum conjunto de permissões não conseguirá fazer login no Console da Web.

> ⚠ Todos os conjuntos de permissões predefinidos têm o grupo **Todos** na seção de **Grupos estáticos**. Esteja ciente disso ao atribuir a um usuário. Os usuários terão essas permissões sobre todos os objetos no ESET PROTECT.

Resumo

Verifique as definições configuradas para este usuário e clique em **Concluir** para criar o usuário.

Ações do usuário e detalhes do usuário

Para gerenciar um usuário, selecione o usuário aplicável e selecione uma das ações disponíveis:

Ações

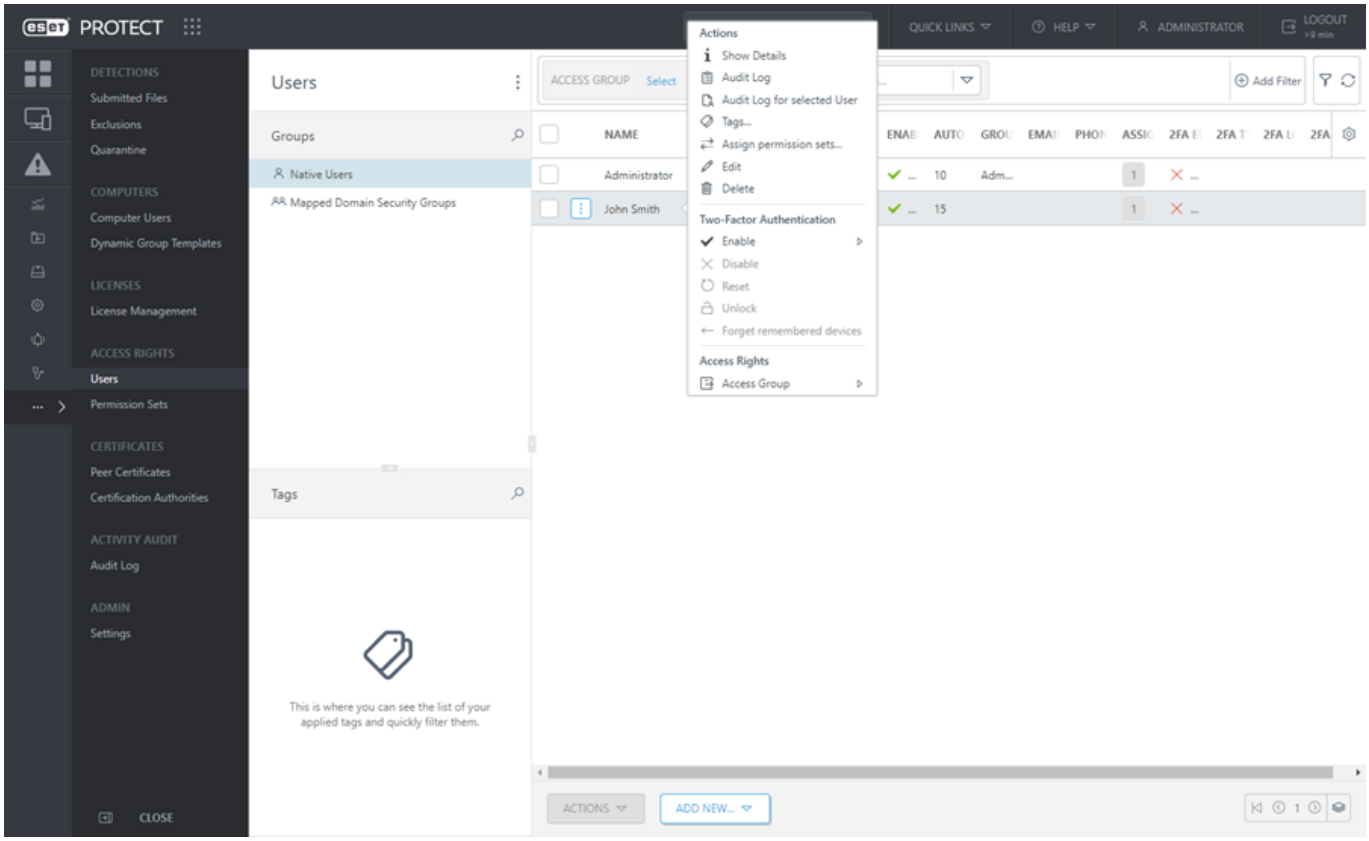
- **Mostrar detalhes** – exibe os detalhes do usuário.
- **Relatório de auditoria** – exibe o Relatório de auditoria para todos os usuários.
- **Relatório de auditoria para o usuário selecionado** – exibe o Relatório de auditoria para o usuário selecionado.
- **Marcações** - Editar marcações (atribuir, remover atribuição, criar, remover).
- **Atribuir conjuntos de permissões** – atribui um conjunto de permissões ao usuário.
- **Editar** – edita as configurações do usuário.
- **Remover** – remove o usuário.

Autenticação em dois fatores

- **Ativar** – ativa a Autenticação em dois fatores para o usuário.
- **Desativar** – desativa a Autenticação em dois fatores existente para o usuário.
- **Redefinir** – redefine as configurações da Autenticação em dois fatores para o usuário.
- **Desbloquear** – se o usuário foi bloqueado, você pode desbloquear o usuário usando esta configuração.
- **Esquecer dispositivos lembrados** – requer a autenticação em dois fatores nos dispositivos lembrados do usuário.

Direitos de acesso

- **Grupo de acesso** > **Mover** – Mova o objeto para outro grupo estático onde ele está disponível para usuários com direitos suficientes para o grupo de destino. Alterar o Grupo de acesso é útil ao resolver problemas de acesso com outros usuários. O Grupo de acesso define o grupo estático do objeto e o acesso ao objeto com base nos direitos de acesso do usuário.



Detalhes do usuário

Há duas seções nos detalhes do usuário:

- **Visão geral** – informações básicas sobre o usuário. Você pode gerenciar o usuário usando as **Ações** e os botões de **Autenticação em dois fatores** na parte de baixo.

- **Conjuntos de permissão** – a lista de conjuntos de permissões atribuídos ao usuário. Clique em um conjunto de permissões para gerenciá-lo.

Alterar senha do usuário

Você pode alterar a senha para qualquer usuário ao qual tenha direitos de acesso. Você deve ter permissões de Gravação para o grupo estático onde o usuário está armazenado. O usuário é armazenado no grupo doméstico do usuário de origem.

1. Clique em **Mais** > **Usuários**.

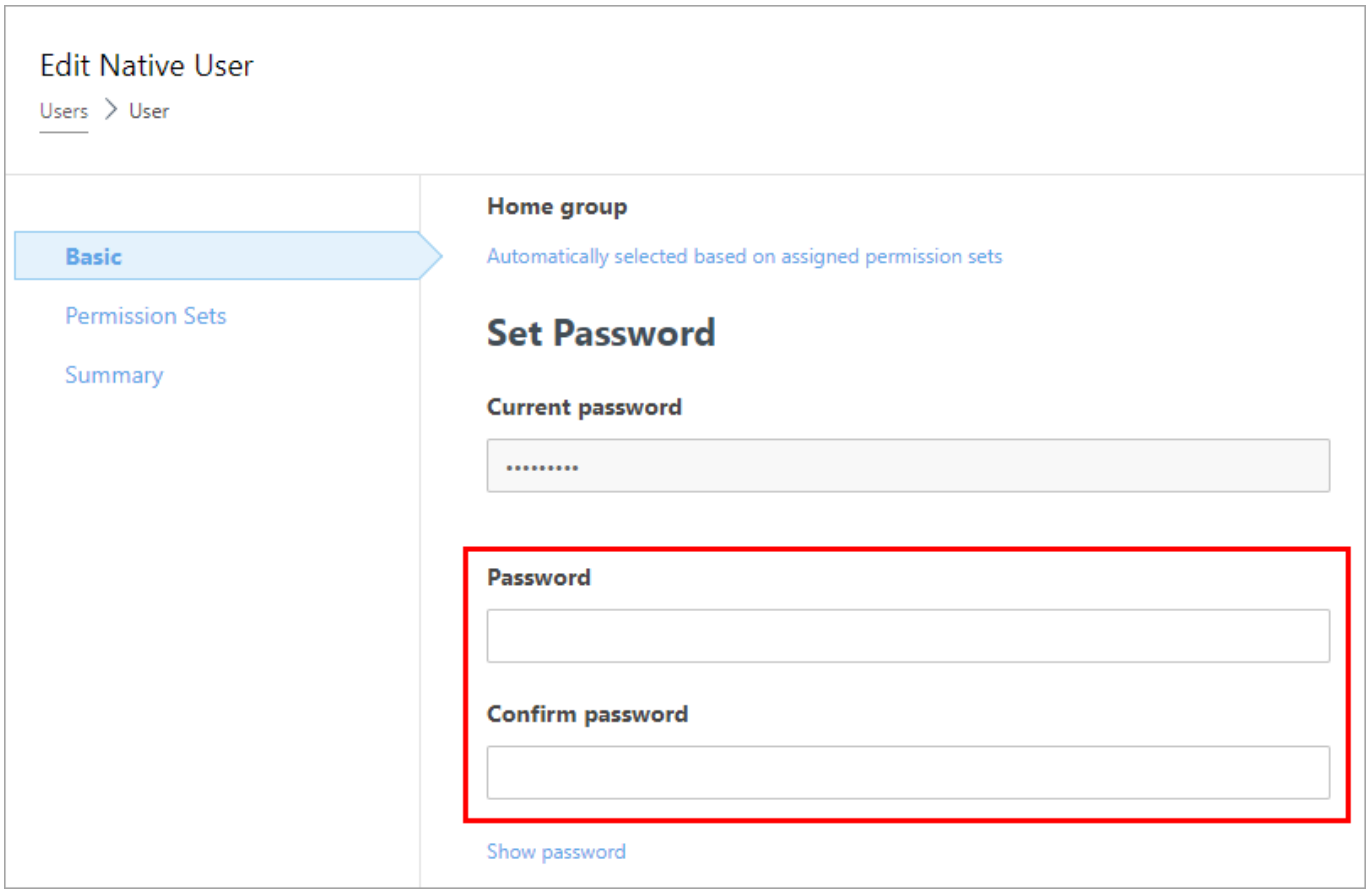
2. Selecione o usuário e clique em **Editar**.

3. Na seção **Básico**, role para **Definir senha**.

4. Se você estiver editando o usuário conectado, é preciso inserir a **Senha atual**. Ao editar outros usuários, o campo **Senha atual** é pré-preenchido.

5.Insira a nova senha nos campos **Senha** e **Confirmar senha**.

6.Clique em **Concluir**.

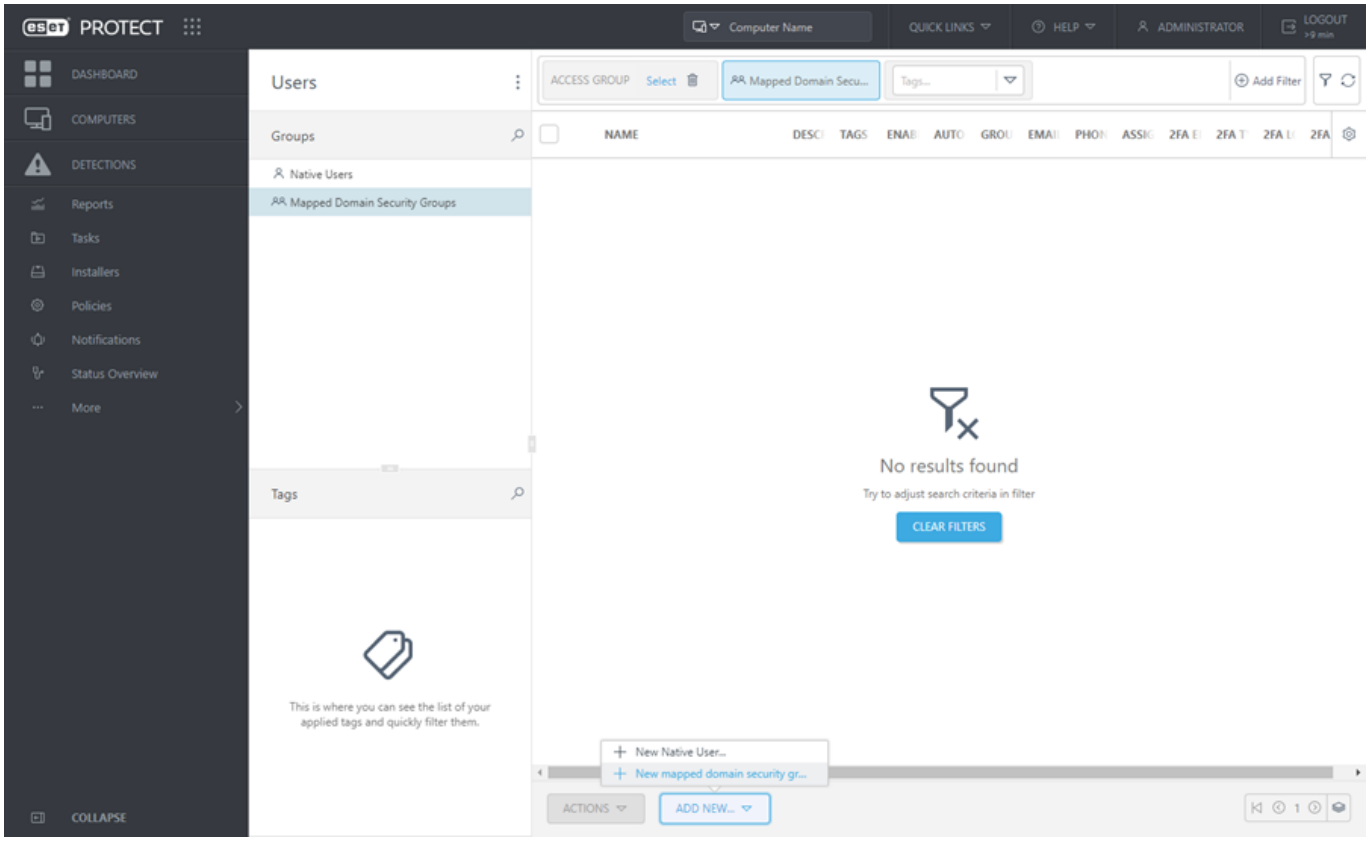


Mapear usuários do Grupo de segurança do domínio

Você pode mapear um grupo de segurança de domínio para o Servidor ESET PROTECT e permitir que usuários existentes (membros desses grupos de segurança de domínio) se tornem usuários do console da Web ESET PROTECT.

Este recurso está disponível apenas para sistemas com o Active Directory.

Para acessar o **Assistente de grupo de segurança do domínio mapeado**, vá para **Mais** > **Usuários** > **Adicionar novo** > **Novo grupo de segurança do domínio mapeado**.



Básico

Grupo de domínio

Digite um **nome** para o grupo. Você também pode digitar uma **Descrição** do grupo.

Clique em **Selecionar marcações** para atribuir marcações.

Selecionar **Grupo inicial**. Este é o grupo estático onde todos os objetos criados por usuários deste grupo de domínio estarão contidos automaticamente.

Grupo doméstico – O grupo doméstico é detectado automaticamente com base no conjunto de permissões atribuído do usuário atualmente ativo.

> ✓ Exemplo de cenário:
> A conta de usuário atualmente ativa tem o direito de acesso de **Gravação** para a **Tarefa de cliente de Instalação de software** e a conta do **Grupo doméstico** é "Department_1". Quando o usuário criar uma nova **Tarefa de cliente de instalação de software**, "Department_1" será selecionado automaticamente como o **Grupo doméstico** da tarefa de cliente.

Se o Grupo doméstico pré-selecionado não atender às suas expectativas, você pode selecionar o Grupo doméstico manualmente.

Este grupo de domínio será definido por um **SID do grupo** (identificador de segurança). Clique em **Selecionar** para selecionar um grupo na lista e em **OK** para confirmar. Seu Servidor ESET PROTECT precisa ser unido no domínio, ou então não existirão grupos na lista. Se estiver usando um Equipamento Virtual, consulte o capítulo relacionado.

- Se o LDAPS não estiver disponível, você pode mapear o grupo de segurança do domínio da seguinte forma:
  - desativando temporariamente as configurações do Active Directory em **Mais** > Configurações > **Configurações avançadas** > **Active Directory**.
  - digitando o SID do grupo manualmente.
- Se você continuar recebendo uma mensagem de erro depois de clicar em Selecionar e se o AD estiver bem configurado, o processo em segundo plano poderá ter passado do limite de tempo. Você pode:
  - Inserir o SID manualmente para evitar este problema
  - Inserir suas credenciais AD em **Mais** > Configurações > **Configurações avançadas** > **Active Directory**. O ESET PROTECT, então, usará uma maneira diferente e mais rápida de recuperar a lista de SIDs.

Conta

Ativado - Selecione esta opção, exceto se quiser que a conta esteja inativa (se quiser usar posteriormente).

Logout automático (mín.) - Esta opção define o período de tempo ocioso (em minutos), depois do qual o usuário é desconectado do console da Web.

Contato de email e **Contato telefônico** podem ser definidos para ajudar a identificar o grupo.

Definições de permissão

Atribua competências (direitos) aos usuários deste grupo.

Os conjuntos de permissões são definidos para o grupo de segurança do domínio do Active Directory (em vez de ser para usuários individuais, como no caso do **Usuário nativo**).

Você pode atribuir vários conjuntos de permissões a um grupo de segurança do domínio.

Você pode selecionar uma competência pré-definida (listada abaixo) ou você pode usar um conjunto de permissões personalizado.

- **Conjunto de permissões de revisor** - direitos somente leitura para o grupo **Todos**.
- **Conjunto de permissões do Administrator** - acesso total ao grupo **Todos**.
- **Conjunto de permissões de instalação auxiliada por servidor** - direitos de acesso mínimos necessários para a instalação auxiliada por servidor.
- **Conjunto de permissões de revisor do ESET Inspect** – no mínimo os direitos de acesso somente leitura (para o grupo **Todos**) são necessários para um usuário ESET Inspect.
- **Conjunto de permissões do servidor do ESET Inspect** – direitos de acesso (para o grupo **Todos**) são necessários para o processo de instalação do ESET Inspect e sincronização automática posterior entre o ESET Inspect e o ESET PROTECT.
- **Conjunto de permissões do usuário do ESET Inspect** – direitos de acesso de gravação (para o grupo **Todos**) são necessários para um usuário ESET Inspect.

Cada conjunto de permissões fornece permissões apenas para os objetos contidos nos **Grupos estáticos** selecionados no conjunto de permissões.

Usuários sem nenhum conjunto de permissões não conseguirá fazer login no Console da Web.

> ⚠ Todos os conjuntos de permissões predefinidos têm o grupo **Todos** na seção de **Grupos estáticos**. Esteja ciente disso ao atribuir a um usuário. Os usuários terão essas permissões sobre todos os objetos no ESET PROTECT.

Resumo

Verifique as definições configuradas para este usuário e clique em **Concluir** para criar o grupo.

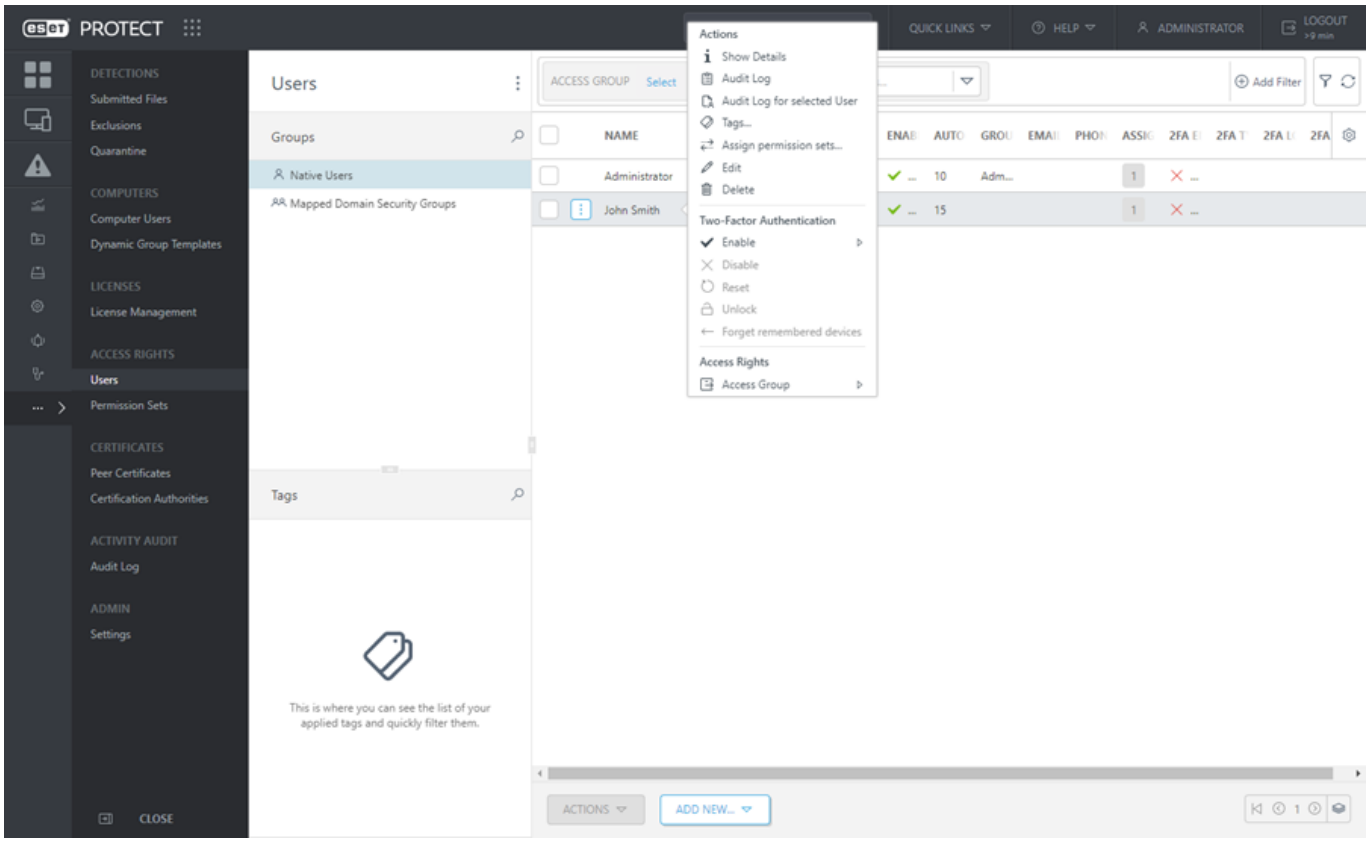
Os usuários vão aparecer nos **Grupos de segurança do domínio mapeados** depois de entrarem pela primeira vez.

Atribuir um conjunto de permissões a um usuário

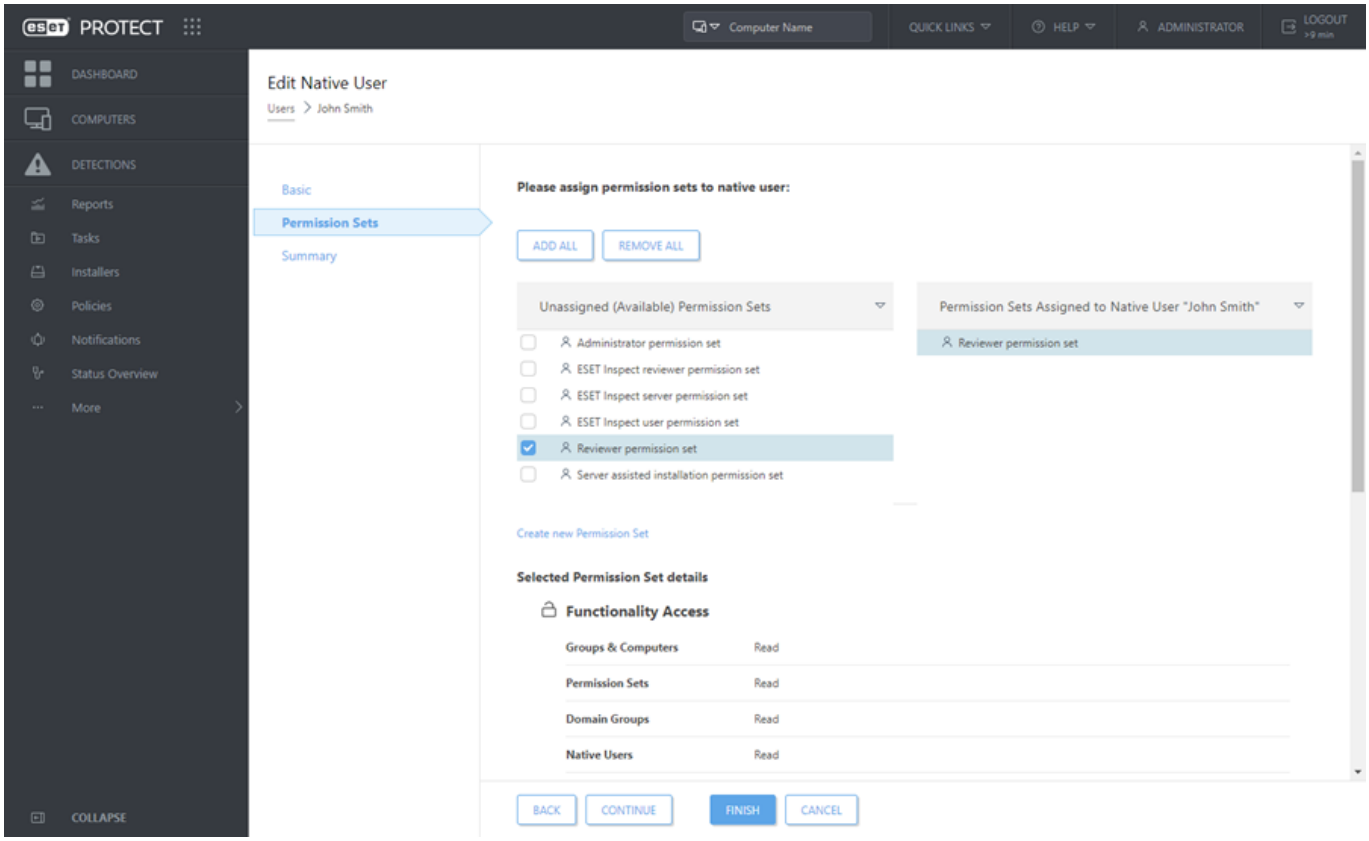
1. Há duas formas de atribuir um conjunto de permissões a um usuário:

   a)Clique em **Mais** > **Usuários** > clique em um usuário e selecione **Atribuir conjuntos de permissões** para atribuir conjuntos de permissões específicos ao usuário.

   b)Na seção **Usuários**, edite um usuário específico clicando em **Editar**.



2. Marque a caixa de seleção ao lado de um Conjuntos de permissão específico na seção **Conjuntos de permissão não atribuídos (disponíveis)**. Veja Gerenciar definições de permissão para mais detalhes.



Autenticação em dois fatores

Autenticação de dois fatores (2FA) fornece um método mais seguro para fazer login e acessar o console da web ESET PROTECT. Usuários com autenticação em dois fatores ativada serão obrigados a entrar no ESET PROTECT usando o ESET Secure Authentication ou um autenticador de terceiros.

- Não há limite para o número de usuários que podem fazer login no ESET PROTECT através de 2FA.
- Configurações de **Proxy HTTP** não são aplicadas para comunicação com servidores de Autenticação Segura (2FA).
- Você pode habilitar a 2FA também para a conta de Administrador.

Pré-requisitos

- Para ativar a autenticação em dois fatores para outro usuário, o usuário atual precisa da permissão de **Gravação** sobre aquele usuário. Quando a autenticação em dois fatores está ativada, o usuário precisa configurar a autenticação em dois fatores por si próprio antes de entrar. Os usuários receberão um link via mensagem de texto (SMS) que eles podem abrir no navegador da web do seu telefone para ver as instruções para configurar 2FA.
- O 2FA não funciona sem acesso direto da rede para os servidores ESET 2FA. É preciso permitir pelo menos os servidores 2FA específicos no firewall. Se o proxy for configurado em **Mais** > **Configurações** > **Configurações avançadas** > **Proxy HTTP**, ele não é aplicável para 2FA.

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

Ativar a Autenticação em dois fatores para um usuário do console da Web

1. Criar um novo usuário ou usar um usuário existente.

2. Clique em **Mais** > **Usuários** no console da Web ESET PROTECT.

3. Clique no usuário e selecione **Autenticação em dois fatores** > **Ativar** e selecione a opção que deseja usar:

   • **ESET Secure Authentication** – autenticação em dois fatores fornecida pela ESET usando a tecnologia ESET Secure Authentication. Você não precisa implantar ou instalar o ESET Autenticação Segura dentro de seu ambiente, o ESET PROTECT conecta automaticamente para os servidores ESET para autenticar os usuários que estão fazendo login no seu console da Web ESET PROTECT.

   • **Autenticador de terceiros** – no ESET PROTECT 9.1 e versões posteriores, você pode usar um cliente de autenticação de terceiros compatível com o protocolo TOTP necessário. Testamos os seguintes aplicativos: Google Authenticator, Microsoft Authenticator ou Authy.

4. Quando o usuário entrar na próxima vez, digite o número de telefone do usuário quando for solicitado.

5. Instale o aplicativo móvel ESET Secure Authentication ou um aplicativo de autenticação de terceiros no celular do usuário usando o link do SMS ou o código QR.

6. Quando você instala o aplicativo usando o token, sua instância do ESET PROTECT é adicionada ao aplicativo.

7. Continue para o login e digite a senha única do aplicativo móvel no console da Web quando solicitado. Uma nova senha única é gerada a cada 30 segundos.

8. Opcionalmente, selecione a caixa de seleção **Lembrar este dispositivo** para autorizar seu dispositivo a não solicitar a autenticação em dois fatores para cada login.

> Você pode esquecer os dispositivos lembrados para o usuário ativo nas Configurações do usuário.

9. Clique em **Enviar**.

Solução de problemas

O usuário será bloqueado depois de digitar a senha única incorretamente dez vezes. O Administrador pode desbloquear o usuário em **Mais** > **Usuários** > clique no usuário e selecione **Desbloquear**.

Se um usuário do Web Console não conseguir entrar no Web Console com a autenticação em dois fatores, siga essas etapas:

1. Backup de banco de dados ESET PROTECT.

2. Selecione a opção aplicável:

   • O número de telefone definido para a autenticação em dois fatores pode ser acessado:

   a)Ao entrar no Web Console, clique em **Redefinir token** na janela autenticação em dois fatores.

   b)Um SMS de verificação é enviado para o número de telefone definido para a autenticação em dois fatores.

Não é possível alterar o número de telefone armazenado no banco de dados ESET PROTECT. Se o telefone não estiver acessível, siga as etapas abaixo.

• O número de telefone definido para a autenticação em dois fatores está inacessível (o telefone foi perdido, está danificado, etc.)

a)Redefina a senha do Web Console para desativar a autenticação em dois fatores na conta do Administrador.

O estado da autenticação em dois fatores de outras contas de usuário ESET PROTECT não é afetado.

b)O usuário pode entrar no Web Console sem a autenticação em dois fatores e reabilitar a autenticação em dois fatores depois de fazer login.

Definições de permissão

Um conjunto de permissões representa as permissões para usuários que acessam o console da Web ESET PROTECT. Elas definem o que o usuário pode fazer ou visualizar no Console da Web. Usuários nativos têm suas próprias permissões, enquanto usuários de domínio têm permissões do seu grupo de segurança mapeado. Cada conjunto de permissões tem seu domínio de aplicativo (grupos estáticos). Permissões que estão selecionadas na seção **Funcionalidade** serão aplicáveis em objetos nos grupos que estão definidos na seção de **Grupos estáticos** para cada usuário atribuído por este conjunto de permissões. Ter acesso a um determinado Grupo estático automaticamente significa acesso a cada um de seus subgrupos. Com a configuração adequada de grupos estáticos é possível construir braços separados para administradores locais (veja o exemplo).

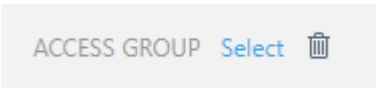
Um usuário pode receber a atribuição de um conjunto de permissões mesmo sem ser capaz de vê-lo. Um conjunto de permissões também é um objeto que é automaticamente armazenado no grupo inicial do usuário que o criou. Quando uma conta de usuário é criada, o usuário é armazenado como objeto no grupo inicial do usuário criador. Normalmente o Administrador cria usuários, então eles são armazenados no grupo *Todos*.

Os conjuntos de permissões são cumulativos. Se você atribuir mais conjuntos de permissões a um único usuário, a soma de todos os conjuntos de permissões será o acesso real do usuário.

Combinação de mais conjuntos de permissões

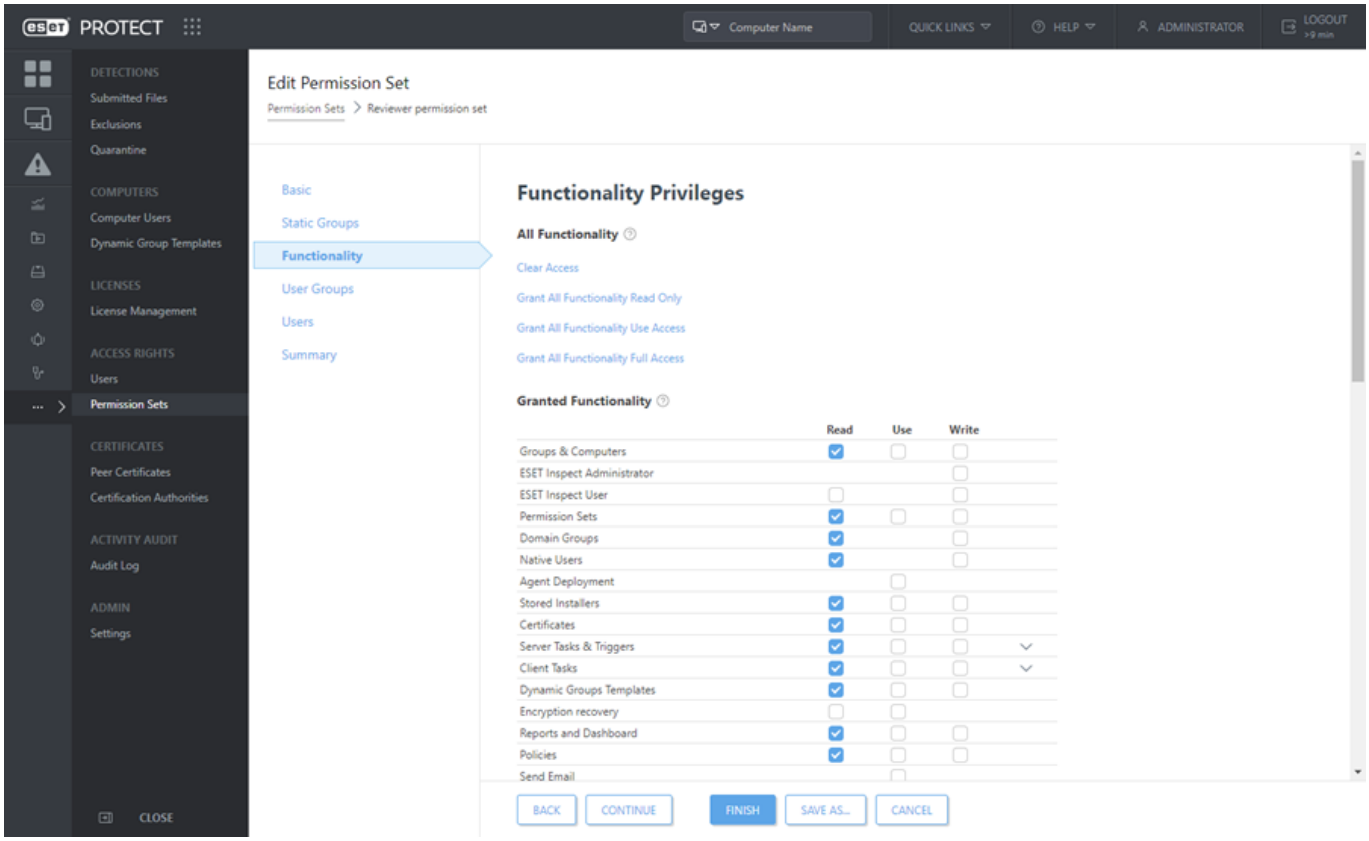
O acesso final que um usuário tem a um objeto é o resultado da combinação de todos os conjuntos de permissões atribuídos ao usuário. Por exemplo, um usuário que tenha dois conjuntos de permissões, um para um grupo doméstico com permissões totais e outro para um grupo com computadores, com permissões de Leitura e Uso para Computadores e grupos. Este usuário pode executar todas as tarefas do grupo doméstico nos computadores do outro grupo.

Em geral, um usuário pode executar objetos de um grupo estático sobre objetos em outro grupo estático, se o usuário tiver permissões para um determinado tipo de objeto em um determinado grupo.



O botão de filtro do **Grupo de acesso** permite aos usuários selecionarem um grupo estático e filtrar os objetos visualizados de acordo com o grupo onde estão contidos.

Você pode usar marcações para filtrar os itens exibidos.



Boa prática para trabalhar com permissões:
• Nunca dê acesso para as ESET PROTECT Configurações do servidor a usuários inexperientes - apenas o Administrador deve ter esse acesso.
• Considere restringir o acesso para as **Tarefas de cliente** > **Executar comando** - é uma tarefa muito potente que pode ser mal utilizada.
• Usuários de um nível que não seja do administrador não devem ter permissões para os **Conjuntos de permissões**, **Usuários nativos**, **Configurações**.
• Se um modelo de permissões mais complexo for necessário, não hesite em criar mais conjuntos de permissões e atribuí-los de acordo.

A permissão do Relatório de auditoria permite que o usuário veja as ações registradas de todos os outros usuários e domínios, mesmo aquelas relacionadas aos ativos que o usuário não tem direitos suficientes para visualizar.

Depois de definir permissões para a funcionalidade ESET PROTECT, é possível atribuir acesso de **Leitura**, **Uso** e **Gravação** aos Grupos de usuários.

Duplicação

Para uma duplicação de objeto é preciso que o usuário tenha uma permissão de **Leitura** no objeto original e permissão de **Gravação** em seu **Grupo inicial** para este tipo de ação.
John, cujo grupo inicial é o *Grupo do John,* quer duplicar a *Política 1,* que foi originalmente criada por *Larry*, portanto a política está automaticamente contida no grupo inicial de Larry, o *Grupo do Larry*.
1.Crie um novo Grupo estático. Dê o nome, por exemplo, de *Políticas compartilhadas*.
2.Atribua para *John* e *Larry* as permissões de **Leitura** para **Políticas** no grupo *Políticas compartilhadas*.
3.*Larry* move a *Política 1* para o grupo de *Políticas compartilhadas*.
4.Atribua para *John* as permissões de **Gravação** para **Políticas** em seu grupo inicial.
5.*John* agora pode **Duplicar** a *Política 1* - a duplicada vai aparecer em seu grupo inicial.

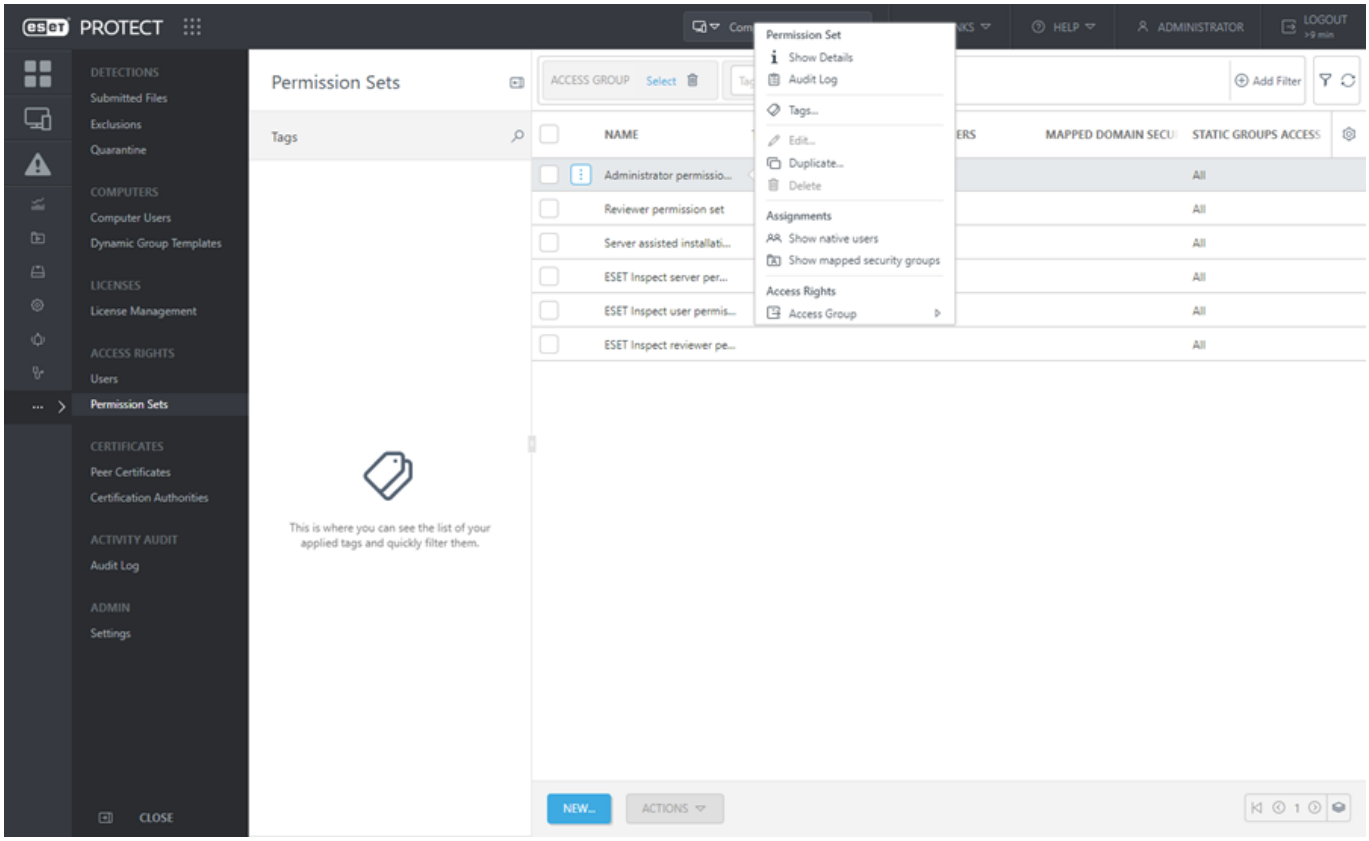
Diferença entre Uso e Gravação

Se o *Administrador* não quiser permitir que o usuário *John* modifique as políticas no grupo *Políticas compartilhadas*, ele teria que criar um conjunto de permissões com:

- Políticas de **Funcionalidade**: Permissões **Leitura** e **Uso** selecionadas
- **Grupos estáticos**: Políticas compartilhadas

Com essas permissões atribuídas a *John*, *John* consegue executar essas políticas mas não consegue editar, criar novas ou remover as políticas. Se um administrador fosse adicionar a permissão **Gravação**, John poderia criar, editar e remover políticas dentro do grupo estático selecionado (*Políticas compartilhadas*).

Gerenciar definições de permissão



Para gerenciar um conjunto de permissões, clique no conjunto de permissões e selecione uma das ações disponíveis:

Conjunto de permissão

- **Mostrar detalhes** – exibe detalhes do conjunto de permissões.
- **Relatório de auditoria** - Exibe o Relatório de auditoria para o item selecionado.
- **Marcações** - Editar marcações (atribuir, remover atribuição, criar, remover).
- **Editar** – edita o conjunto de permissões.
- **Duplicar** – cria um conjunto de permissões duplicado para que você possa modificar e atribuir a um usuário específico. A duplicada será armazenada no grupo inicial do usuário que a duplicou.

- **Remover** – remove o conjunto de permissões.

Atribuições

- **Exibir usuários nativos** – exibe a lista de usuários nativos atribuídos.
- **Exibir grupos de segurança mapeado** – exibe a lista de grupos de segurança do domínio mapeados atribuídos.

Direitos de acesso

- **Grupo de acesso** > **Mover** – Mova o objeto para outro grupo estático onde ele está disponível para usuários com direitos suficientes para o grupo de destino. Alterar o Grupo de acesso é útil ao resolver problemas de acesso com outros usuários. O Grupo de acesso define o grupo estático do objeto e o acesso ao objeto com base nos direitos de acesso do usuário.

Todos os conjuntos de permissões predefinidos têm o grupo **Todos** na seção de **Grupos estáticos**. Esteja ciente disso ao atribuir a um usuário. Os usuários terão essas permissões sobre todos os objetos no ESET PROTECT.

Criar ou editar um conjunto de permissões

Para criar um novo conjunto de permissões, clique em **Novo**. Para editar um conjunto de permissões existente, selecione o conjunto de permissões aplicável e clique em **Editar**.

Básico

Insira um **Nome** para o conjunto (configuração obrigatória). Você também pode inserir uma **Descrição** e **Marcações**.

Clique em **Selecionar marcações** para atribuir marcações.

Grupos estáticos

Você pode **Selecionar** um Grupo estático (ou vários Grupos estáticos) ou **Criar novo grupo** que terão essa competência. Permissões que estão marcadas na seção **Funcionalidade** serão aplicáveis a objetos contidos em grupos selecionados nesta seção.

Funcionalidade

Selecione módulos individuais para os quais deseja conceder acesso. O Usuário com essa competência terá acesso a essas tarefas específicas. Também é possível definir permissões diferentes para cada tipo de tarefa do servidor e tarefa de cliente. Existem quatro conjuntos de funcionalidade pré-definidos. Selecione um dos quatro ou selecione manualmente as caixas de marcação de funcionalidade.

Conceder permissão de **Gravação** automaticamente concede a permissão de **Uso** e direitos de **Leitura**; conceder direitos de **Uso** automaticamente concede direitos de **Leitura**.

Grupos de usuários

Você pode adicionar um Grupo de usuários (ou vários Grupos de usuários) cujos parâmetros de usuário podem ser usados dentro de uma política (por exemplo ESET Mobile Device Management para iOS ou Modo de substituição).

Usuários

Escolha um usuário ao qual atribuir este conjunto de permissões. Todos os usuários disponíveis são relacionados à esquerda. Selecione usuários específicos ou selecione todos os usuários utilizando o botão **Adicionar tudo**. Os usuários atribuídos são relacionados à direita. Não é obrigatório atribuir um usuário, isso pode ser feito posteriormente.

Resumo

Verifique as definições configuradas para esta competência e clique em **Concluir**. O conjunto de permissões é armazenado no grupo inicial do usuário que o criou.

Clique em **Salvar como** para criar um novo conjunto de permissões com base no conjunto de permissões que você está editando. Será necessário escolher um nome para o novo conjunto de permissões.

Lista de permissões

Tipos de permissão

Ao criar ou editar um conjunto de permissões em **Mais** > **Conjuntos de permissão** > **Novo / Editar** > **Funcionalidade** há uma lista de todas as permissões disponíveis. As permissões do Web Console ESET PROTECT são divididas em categorias, por exemplo **Grupos e Computadores**, **Políticas**, **Tarefas de cliente**, **Relatórios**, **Notificações** e assim por diante. Um determinado conjunto de permissões pode autorizar o acesso **Leitura**, **Uso** ou **Gravação**. Em geral:

Permissões **Leitura** são boas para usuários de auditoria. Eles podem ver os dados mas não podem fazer alterações.

As permissões de Uso permitem aos usuários usarem objetos, executarem tarefas, mas não modificar ou excluir.

As permissões de **Gravação** permitem que os usuários modifique e/ou duplique os respectivos objetos.

Certos tipos de permissões (listadas abaixo) controlam um processo, não um objeto. É por isso que eles trabalham em um nível global, portanto não importa em qual grupo estático a permissão é aplicada, ela vai funcionar independentemente disso. Se o processo for permitido para um usuário ele pode usá-lo apenas em usuários sobre os quais ele tem permissões suficientes. Por exemplo, a permissão **Exportar relatório para arquivo** ativa a funcionalidade de exportação, mas os dados contidos no relatório são determinados por outras permissões.

Leia nosso artigo da Base de conhecimento com exemplos de tarefas e conjuntos de permissões que o usuário precisa para realizar as tarefas com sucesso.

Funcionalidades às quais o usuário atual não tem direitos de acesso estão indisponíveis (acinzentadas).

Usuários podem receber a atribuição de permissões para os processos a seguir:

- **Implantação do agente**
- **Relatórios e Painel** (apenas a funcionalidade do Painel estará disponível, mas os modelos de relatório usáveis ainda dependem de grupos estáticos acessíveis)
- **Enviar email**
- **Exportar relatório para arquivo**
- **Enviar interceptação SNMP**
- **Configurações do servidor**
- **ESET Inspect Administrator**
- **ESET Inspect Usuário**

Tipos de funcionalidade:

Grupos e Computadores

Leitura - Lista computadores, grupos e computadores dentro de um grupo.

Uso - Usar um computador/grupo como destino para uma política ou tarefa.

Gravação - Cria, modifica e remove computadores. Isso também inclui renomear um computador ou grupo.

ESET Inspect Administrator

Gravação - Realizar funções administrativas no ESET Inspect.

ESET Inspect Usuário

Leitura – acesso somente leitura ao ESET Inspect. Um usuário do Web Console precisa de permissão de **Leitura** ou acima para **Acessar o ESET Inspect** ou permissão de **Leitura** ou acima para o **Usuário ESET Inspect**.

Gravação - Acesso de leitura e gravação ao ESET Inspect.

Definições de permissão

Leitura - Lê a lista de conjuntos de permissões e a lista de direitos de acesso dentro deles.

Uso - Atribui/remove conjuntos de permissões existentes para os usuários.

Gravação - Cria, modifica e remove conjuntos de permissões.

Ao atribuir (ou retirar a atribuição) um conjuntos de permissões para um usuário, a permissão **Gravação** é necessária para **Grupos do domínio** e **Usuários nativos**.

Grupos de domínio

Leitura - Lista os grupos de domínio.

Usar

Gravação - Permite a concessão/anulação de conjuntos de permissões. Criar/modificar/remover grupos de domínio.

Usuários nativos

Leitura - Lista os usuários nativos.

Usar

Gravação - Permite a concessão/anulação de conjuntos de permissões. Criar/modificar/remover usuários nativos.

Implantação do agente

Uso - Permitir acesso para implantar o Agente através de **Links Rápidos** ou adicionar computadores cliente manualmente no Console da Web ESET PROTECT.

Instaladores armazenados

Leitura - Lista os instaladores armazenados.

Uso - Exportar o instalador armazenado.

Gravação - Criar/modificar/remover instaladores armazenados.

Certificados

Leitura - Leia a lista de Certificados de mesmo nível e da Autoridade de certificação.

Uso - Exportar certificado de mesmo nível e Autoridades de certificação e usá-los em instaladores ou tarefas.

Gravação - Criar e anula novos certificados de mesmo nível ou Autoridade de certificação.

Acionadores e tarefas do servidor

Ler - Ler a lista de tarefas e suas configurações (exceto por campos sensíveis como senhas).

Uso - Executa uma tarefa existente com Executar agora (como o usuário que atualmente fez login no Console da Web).

Gravação - Cria, modifica e remove tarefas do servidor.

É possível abrir as categorias clicando no sinal  e um tipo único ou múltiplo de tarefas de servidor pode ser selecionado.

Tarefas de cliente

Ler - Ler a lista de tarefas e suas configurações (exceto por campos sensíveis como senhas).

Uso - Agendar execução de Tarefas de cliente existentes ou cancelar sua execução. Note que para a atribuição de tarefas (ou cancelamento da atribuição) em destinos (computadores ou grupos) o acesso de Uso adicional é necessário para os destinos afetados.

Gravação - Criar, modificar ou remover a Tarefa de cliente existente. Note que para a atribuição de tarefas (ou cancelamento da atribuição) em destinos (computadores ou grupos) o acesso de **Uso** adicional é necessário para os objetos de destino afetados.

É possível abrir as categorias clicando no sinal de mais  e um tipo único ou múltiplo de tarefas de cliente pode ser selecionado.

Modelos de grupos dinâmicos

Leitura - Leia a lista de modelos de Grupos dinâmicos.

Uso - Uso de modelos existentes para grupos dinâmicos.

Gravação - Cria, modifica e remove modelos de Grupo dinâmico.

Recuperação de criptografia

Leitura

Uso – gerencia o processo de recuperação de criptografia.

Relatórios e Painel

Leitura - Lista modelos de relatório e suas categorias. Gerar relatórios com base nos modelos de relatório. Leia seus próprios painéis com base nos painéis padrão.

Uso - Modificar seus próprios painéis com modelos de relatório disponíveis.

Gravação - Cria, modifica, remove modelos de relatório existentes e suas categorias. Modificando os painéis padrão.

Políticas

Leitura - Leia a lista de políticas e configurações dentro delas.

Uso - Atribui políticas existentes aos destinos (ou cancela sua atribuição). Note que para os destinos afetados o acesso de **Uso** adicional é necessário.

Gravação - Cria, modifica e remove políticas.

Enviar email

Uso - Enviar emails. (Útil para tarefas do servidor Notificações e Gerar relatório.)

Enviar interceptação SNMP

Uso - Permite enviar interceptação SNMP (útil para Notificações).

Exportar relatório para arquivo

Uso - Permite que você armazene relatórios no sistema de arquivos da máquina do Servidor ESET PROTECT. Útil com as tarefas do servidor Gerar relatório.

Licenças

Leitura - Leia a lista de licenças e suas estatísticas de uso.

Uso - Use a licença para ativação.

Gravação - Adiciona e remove licenças. (O usuário deve ter o grupo inicial definido como Todos. Por padrão somente o Administrador pode fazer isso.)

Notificações

Leitura - Leia a lista de notificações e suas configurações.

Gravação - Criar, modificar, remover notificações. Para o tratamento adequado de notificações, direitos de acesso de **Uso** adicionais podem ser necessários para **Enviar interceptação SNMP** ou **Enviar email** dependendo da configuração da notificação.

Configurações do servidor

Leitura - Leitura das ESET PROTECT configurações do servidor.

Gravação - Modificar ESET PROTECT configurações do servidor.

Relatório de auditoria

Leitura – exibir o Relatório de auditoria e ler o Relatório de auditoria.

ESET Inspect Funcionalidade concedida

Esta é uma lista de funcionalidades individuais do ESET Inspect às quais um usuário terá acesso. Para mais detalhes, consulte o Guia do Usuário ESET Inspect. Um usuário do Web Console precisa de permissão de **Leitura** ou acima para **Acessar o ESET Inspect** ou permissão de **Leitura** ou acima para o **Usuário ESET Inspect**.

Certificados

Os certificados são uma parte importante do ESET PROTECT, eles são necessários para a comunicação segura entre os componentes do ESET PROTECT e o Servidor ESET PROTECT e também para estabelecer uma conexão segura com o Web Console ESET PROTECT.

Para certificar-se de que todos os componentes podem se comunicar de forma correta, todos os certificados de mesmo nível precisam ser válidos e assinados pela mesma Autoridade de Certificação.

Leia mais sobre certificados no ESET PROTECT no nosso artigo da Base de conhecimento.

Você tem algumas opções em relação aos certificados:

- Você pode usar certificados que foram criados automaticamente durante a ESET PROTECT instalação.
- Você pode criar uma nova Autoridade de certificação (CA) ou Importar chave pública que você usará para assinar o Certificado de mesmo nível para cada um dos componentes (Agente ESET Management, Servidor ESET PROTECT, ESET PROTECT MDM).
- É possível usar seu certificado e autoridade de certificação personalizados.

Se você planeja migrar do Servidor ESET PROTECT para uma nova máquina de servidor, é preciso exportar/fazer backup de todas as Autoridades de certificação que está usando, e também do Certificado do Servidor ESET PROTECT. Caso contrário, nenhum dos componentes do ESET PROTECT será capaz de comunicar com seu novo Servidor ESET PROTECT.

Você pode criar uma nova **Autoridade de Certificação** e **Certificado de mesmo nível** no console da Web ESET PROTECT, siga as instruções neste guia para:

- Criar uma nova Autoridade de Certificação
  - Importar uma chave pública
  - Exportar uma chave pública
  - Exportar uma chave pública no formato BASE64
- Criar um Certificado de mesmo nível
  - Criar um Certificado
  - Exportar Certificado
  - Criar um certificado APN/ABM
  - Revogar um certificado
  - Certificar uso
  - Definir novo certificado do Servidor ESET PROTECT
  - Certificados personalizados com ESET PROTECT
  - Certificado expirando - relatório e substituição

macOS / OS X não é compatível com Certificados com data de validade em 19 de janeiro de 2038 e posterior. O Agente ESET Management sendo executado no macOS / OS X não será capaz de conectar ao Servidor ESET PROTECT.

Para todos os Certificados e Autoridades de Certificação criados durante a instalação dos componentes ESET PROTECT, o valor Válido de é definido para 2 dias antes da criação do certificado.
Para todos os Certificados e Autoridades de Certificação criados no Console da Web ESET PROTECT, o valor Válido de é definido para 1 dia antes da criação do certificado. O motivo disso é cobrir todas as discrepâncias de tempo possíveis entre os sistemas afetados.
Por exemplo, uma Autoridade de certificação e Certificado criados em 12 de janeiro de 2017 durante a instalação terão um valor Válido de pré-definido como 10 de janeiro de 2017 00:00:00, e uma Autoridade de certificação e Certificado criados em 12 de janeiro de 2017 no Console da Web ESET PROTECT terão o valor Válido de pré-definido de 11 de janeiro de 2017 00:00:00.

Certificados de mesmo nível

Se uma Autoridade de certificação estiver presente em seu sistema, você deve criar um certificado de mesmo nível de componentes individuais do ESET PROTECT. Cada componente (Agente ESET Management e Servidor ESET PROTECT) requer um certificado específico.

Novo

Esta opção é usada para criar um novo certificado. Esses certificados são usados pelo Agente ESET Management e servidor ESET PROTECT.

Certificado APN/ABM

Esta opção é usada para criar um novo certificado APN/ABM. Este certificado é usado pelo MDM. Esta ação requer uma licença válida.

Certificar uso

Você também pode verificar quais clientes estão usando esse certificado ESET PROTECT.

Marcações

Editar marcações (atribuir, remover atribuição, criar, remover).

Editar

Selecione esta opção para editar uma **descrição** de um certificado existente da lista.

Relatório de auditoria

Exibe o Relatório de auditoria para o item selecionado.

Exportar / **Exportar como Base64**

Exporte um certificado como um arquivo *.pfx* ou arquivo *.txt* (Base64). Este arquivo é necessário se você instalar o Agente ESET Management de forma local em um computador, ou ao instalar o MDM.

Revogar

Se não quiser mais usar um certificado, selecione **Revogar**. Esta opção invalida o certificado permanentemente, o certificado é colocado na lista de proibições. Essa informação é enviada aos Agentes ESET Management durante a próxima conexão. Certificados revogados não serão aceitos pelo ESET PROTECT.

Certifique-se que não há agentes ESET Management restantes (ou outros componentes) que ainda estejam usando este certificado antes de removê-lo. Quando o certificado for revogado, os componentes não serão capazes de conectar ao Servidor ESET PROTECT. Reinstale os componentes usando um certificado válido para restaurar a funcionalidade.

Grupo de Acesso

Um certificado ou autoridade de certificado pode ser movido para o outro grupo. Então isso se torna disponível para usuários com direitos suficientes para este grupo. Para localizar com facilidade o grupo inicial de um certificado, selecione o certificado e clique em **Grupo de acesso** no menu suspenso. O grupo inicial do certificado é exibido na primeira linha do menu pop-up (por exemplo, /Todos/San Diego. Veja nosso cenário de amostra para aprender mais sobre compartilhar certificados).

Você verá apenas os certificados localizados em seu grupo doméstico (assumindo que você tem permissão de **gravação** para os certificados). Certificados que são criados durante a instalação ESET PROTECT estão localizados no grupo **Todos** e apenas os administradores têm acesso a eles.

Clique no botão **Exibir revogado** para visualizar todos os certificados revogados.

Certificado de agente para instalação auxiliada por servidor - Este certificado é gerado durante a instalação de servidor, desde que você tenha selecionado a opção **Gerar certificados**.

Filtros e personalização de layout

Você pode personalizar a exibição da tela atual do console web:

- Gerenciar o painel lateral e a tabela principal.
- Adicionar filtro e predefinições de filtro. Você pode usar marcações para filtrar os itens exibidos.

Criar um novo Certificado

Como parte do processo de instalação, o ESET PROTECT requer que seja criada uma autoridade de certificação de mesmo nível para Agentes. Esses certificados são usados para autenticar a comunicação entre o Agente no dispositivo cliente e o Servidor ESET PROTECT.

Existe uma exceção, um **Certificado de agente para instalação auxiliada por servidor** não pode ser criado manualmente. Este certificado é gerado durante a instalação do servidor, desde que **Gerar certificados** esteja selecionado.

Para criar um novo certificado no **ESET PROTECT Console da Web**, vá até **Mais** > **Certificados** e clique em **Ações** > **Novo**.

Básico

Descrição – digite a descrição para o certificado.

Clique em **Selecionar marcações** para atribuir marcações.

Produto - Selecione o tipo de certificado que quer criar a partir do menu suspenso.

Host - 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.

Ao criar o certificado MDM, preencha o endereço IP ou Nome de host do dispositivo de Host MDM. O valor padrão (um asterisco) não é válido para esse tipo de certificado.

Código - Recomendamos deixar este campo em branco, mas você pode definir um código para o certificado que será exigido quando os clientes tentarem ativar.

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

Atributos (assunto)

Esses campos não são obrigatórios, mas você pode usá-los para incluir informações mais detalhadas sobre este certificado.

Nome comum - Este valor deve ter a string “Agente” ou “Servidor”, de acordo com o **Produto** selecionado. Se quiser, é possível inserir informações de descrição sobre o certificado. Insira os valores **Válido de** e **Válido até** para ter certeza de que o certificado é válido.

> Para todos os Certificados e Autoridades de Certificação criados durante a instalação dos componentes ESET PROTECT, o valor Válido de é definido para 2 dias antes da criação do certificado.
> Para todos os Certificados e Autoridades de Certificação criados no Console da Web ESET PROTECT, o valor Válido de é definido para 1 dia antes da criação do certificado. O motivo disso é cobrir todas as discrepâncias de tempo possíveis entre os sistemas afetados.
> Por exemplo, uma Autoridade de certificação e Certificado criados em 12 de janeiro de 2017 durante a instalação terão um valor Válido de pré-definido como 10 de janeiro de 2017 00:00:00, e uma Autoridade de certificação e Certificado criados em 12 de janeiro de 2017 no Console da Web ESET PROTECT terão o valor Válido de pré-definido de 11 de janeiro de 2017 00:00:00.

Assinar

Selecione de dois métodos de assinatura:

- **Autoridade de certificação** - Se quiser assinar usando a **ESET PROTECTAutoridade de Certificação** (CA criada durante a instalação ESET PROTECT).
  - Selecione a **ESET PROTECTautoridade de certificação** na lista de autoridade de certificação
  - Criar uma nova Autoridade de Certificação
- **Arquivo pfx personalizado** - Para usar um arquivo *.pfx* personalizado, clique em **Procurar**, navegue até seu arquivo *.pfx* personalizado e clique em **OK**. Selecione **Carregar** para carregar este certificado no Servidor. Você não pode usar o certificado personalizado.

> Se você quiser assinar um novo certificado usando o ESET PROTECT CA (criado durante a instalação ESET PROTECT) no Equipamento Virtual ESET PROTECT, é preciso preencher o campo **Senha da autoridade de certificação. Esta é a** senha especificada durante a configuração ESET PROTECT VA.

Resumo

Revise as informações de certificado fornecidas e clique em **Concluir**. O certificado foi criado com sucesso e estará disponível na lista **Certificados** para usar ao instalar o Agente. O certificado será criado em seu grupo inicial.

> Como uma alternativa para criar um novo certificado, você pode Importar uma chave pública, Exportar uma chave pública ou Exportar certificado de mesmo nível.

Exportar certificado de mesmo nível

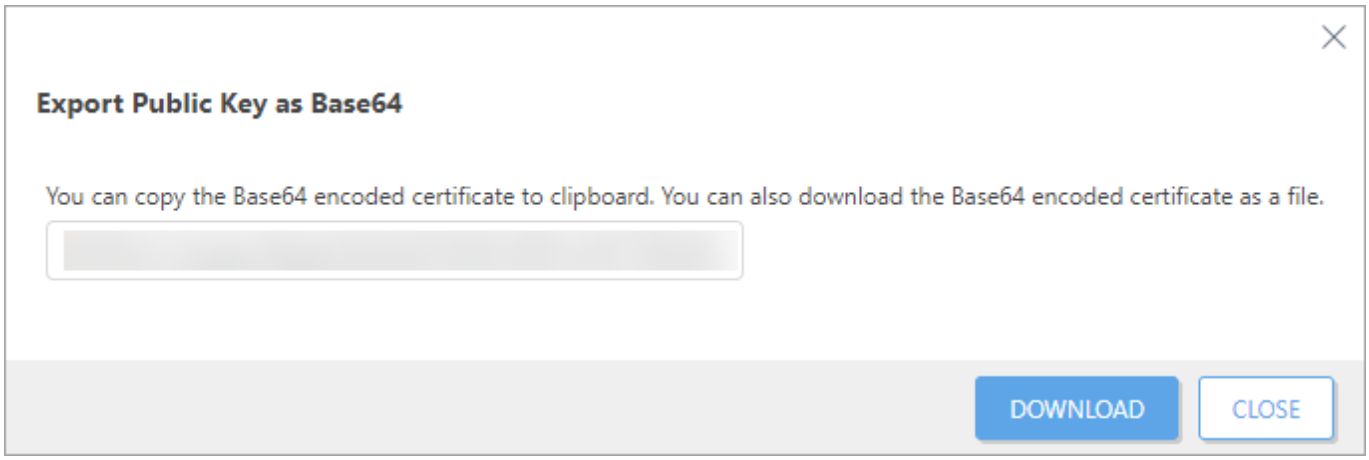
Exportar certificados de mesmo nível

1. Selecione os **Certificados de mesmo nível** que deseja usar a partir da lista e selecione a caixa de seleção ao lado dela.

2.No menu de contexto selecione **Exportar**. O certificado será exportado (incluindo a chave privada) como um arquivo *.pfx*. Digite um nome para o seu certificado e clique em **Salvar**.

Exportar como Base64 a partir de Certificados de mesmo nível

Certificados para componentes ESET PROTECT estão disponíveis no console da Web. Para copiar o conteúdo de um certificado no formato Base64, clique em **Mais** > **Certificado de mesmo nível**, selecione um certificado e selecione **Exportar como Base64**. Também é possível fazer download do certificado codificado Base64 como um arquivo. Repita este passo para outros certificados de componentes, assim como para sua Autoridade de Certificação.



Para exportar um certificado é preciso que o usuário tenha direitos de **Uso** sobre os **Certificados**. Veja a lista completa de direitos de acesso para obter mais informações.

Certificado APN/ABM

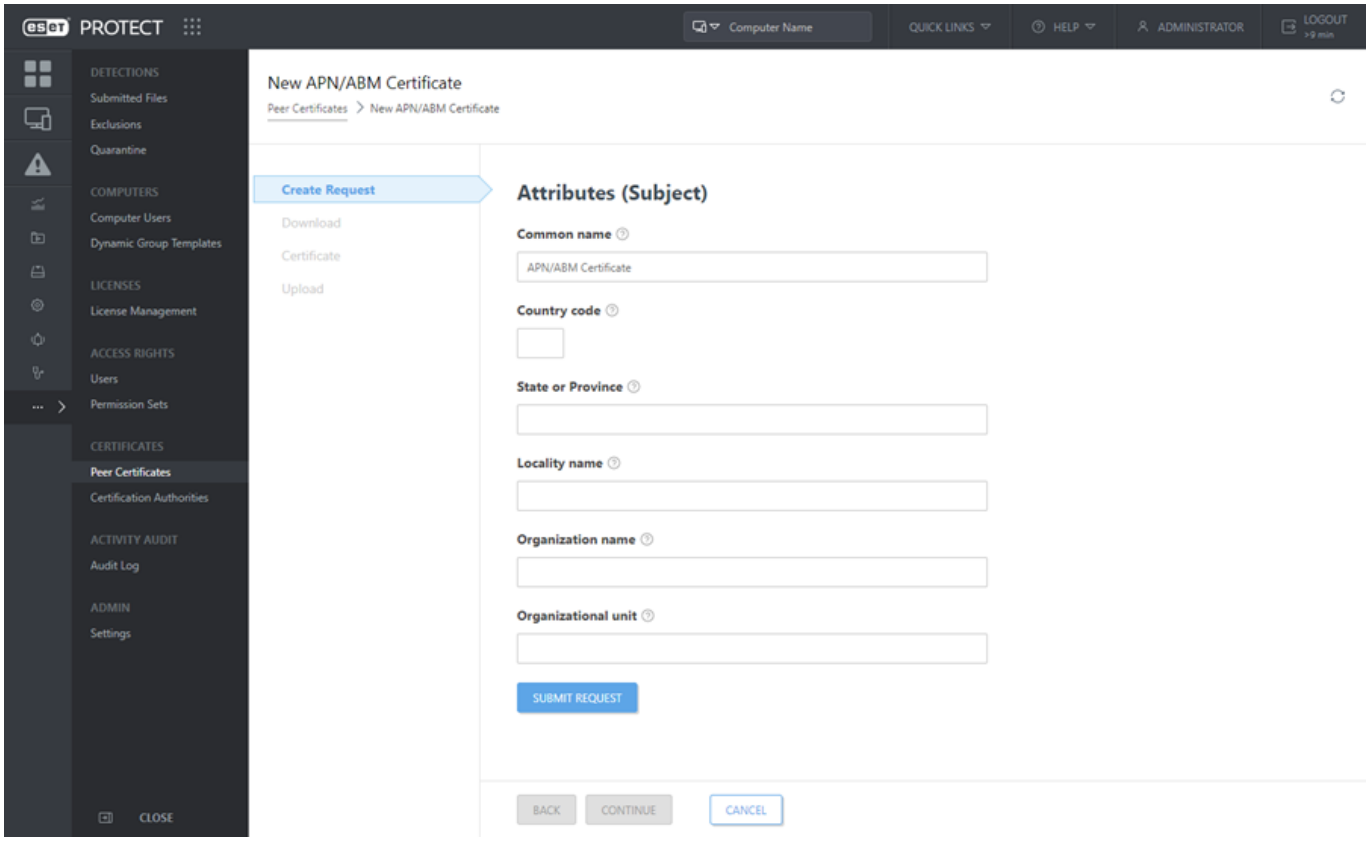
Um certificado APN (Notificação Push da Apple)/ABM (Apple Business Manager) é usado pelo ESET PROTECT MDM para inscrição do dispositivo iOS. Você precisa criar um **certificado de push fornecido pela Apple** e tê-lo assinado pela Apple para poder inscrever dispositivos iOS no ESET PROTECT. Certifique-se também de ter uma licença válida para o ESET PROTECT.

Clique na guia **Mais** > **Certificados de mesmo nível**, clique em **Novo e** selecione **Certificado APN/ABM**.

Para adquirir um certificado APN, você precisará de um Apple ID. Este ID é necessário para a Apple assinar o certificado.
O Certificado APN tem validade de 1 ano. Se o seu certificado estiver perto de expirar, siga as etapas abaixo e na parte de Certificado etapa 2 selecione **Renovar**.
Para adquirir um token de inscrição ABM, você precisará de uma Conta Apple ABM.

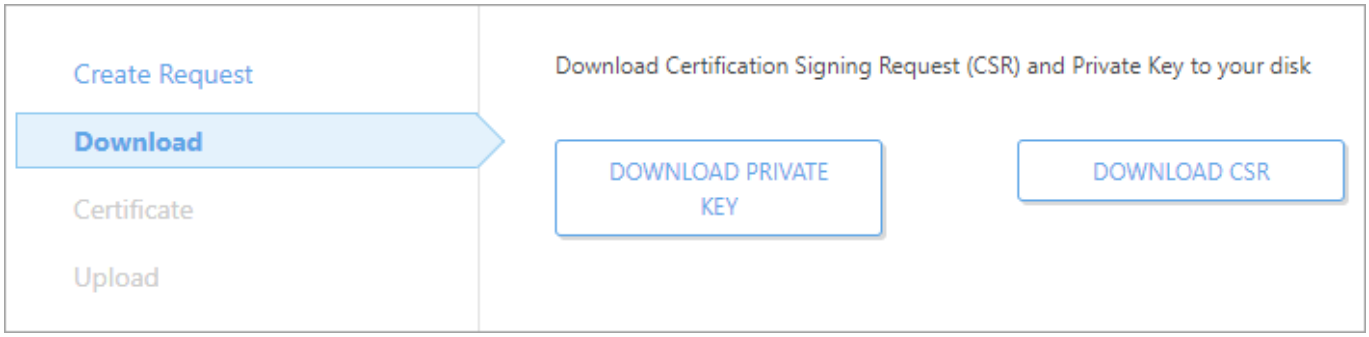
Criar solicitação

Especifique os atributos do certificado (Código de país, Nome da organização, etc.) e clique em **Enviar solicitação**.



Download

Faça download da sua **CSR** (Solicitação de Assinatura de Certificado) e **chave privada**.



Certificado

1.Abra o Portal de Certificados Push da Apple e faça login usando seu ID Apple.

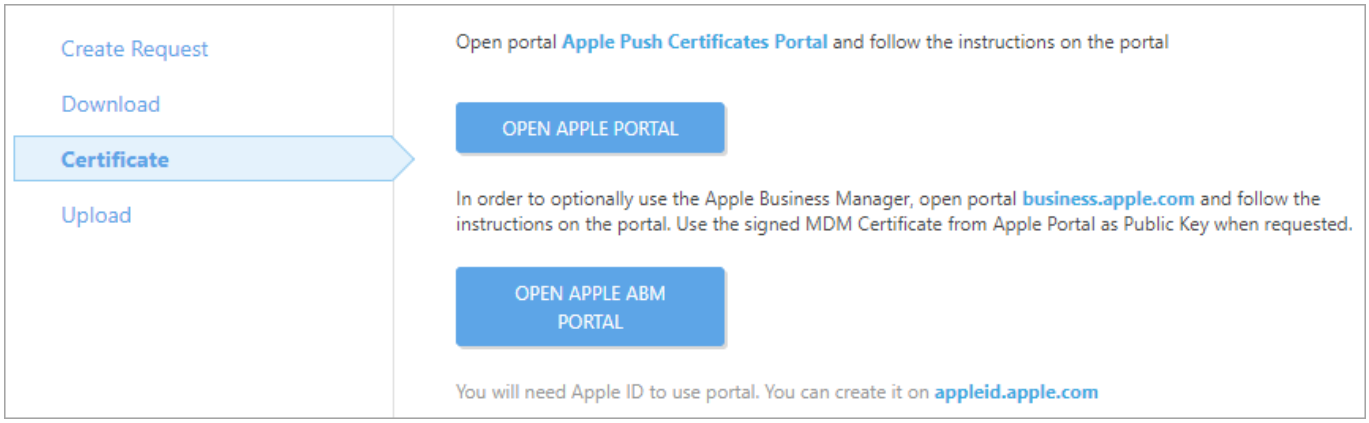
2.Clique em **Criar um Certificado**.

3.Preencha a nota (opcional). Clique em **Escolher arquivo**, carregue o arquivo CSR que você baixou em uma etapa anterior e clique em **Carregar**.

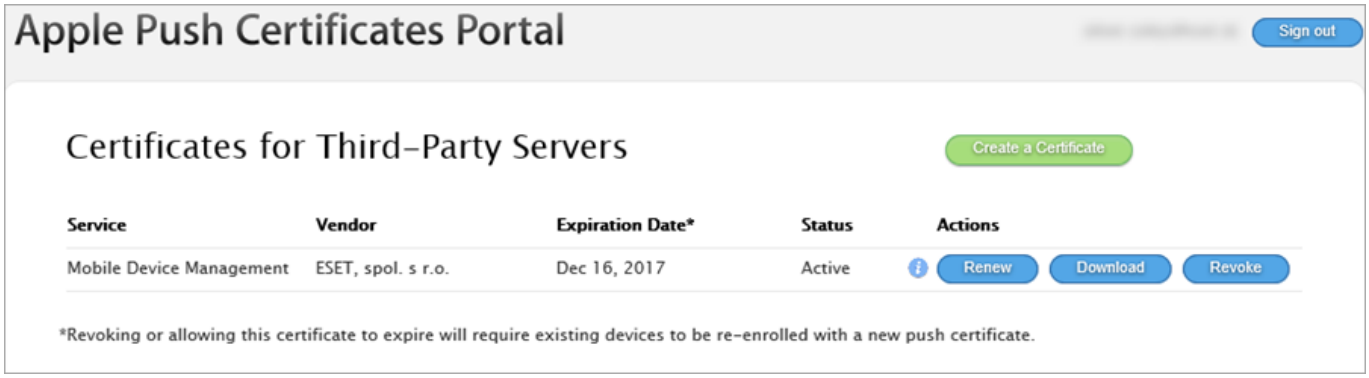
4.Depois de um tempo você verá uma nova tela de confirmação com a notificação de que seu certificado APNS para o servidor de Gerenciamento de dispositivo móvel ESET foi criado com sucesso.

5.Clique em **Download** e salve o arquivo *.pem* no seu computador.

6.Feche o Portal de Certificado Push da Apple e continue para a seção Carregar abaixo.

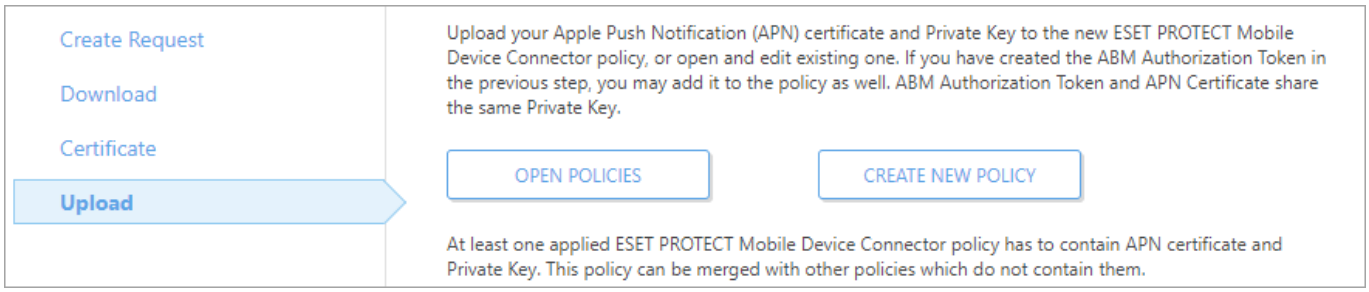


O certificado APNS é necessário para a política MDM ABM e não ABM. Siga essas instruções para criar um certificado de Inscrição ABM.



Carregar

Assim que tiver concluído todas as etapas acima, você pode criar uma Política para MDC para ativar APNS para inscrição iOS. Você pode então Inscrever qualquer dispositivo iOS visitando *https://<mdmcore>:<enrollmentport>/unique_enrollment_token* a partir do navegador do dispositivo.

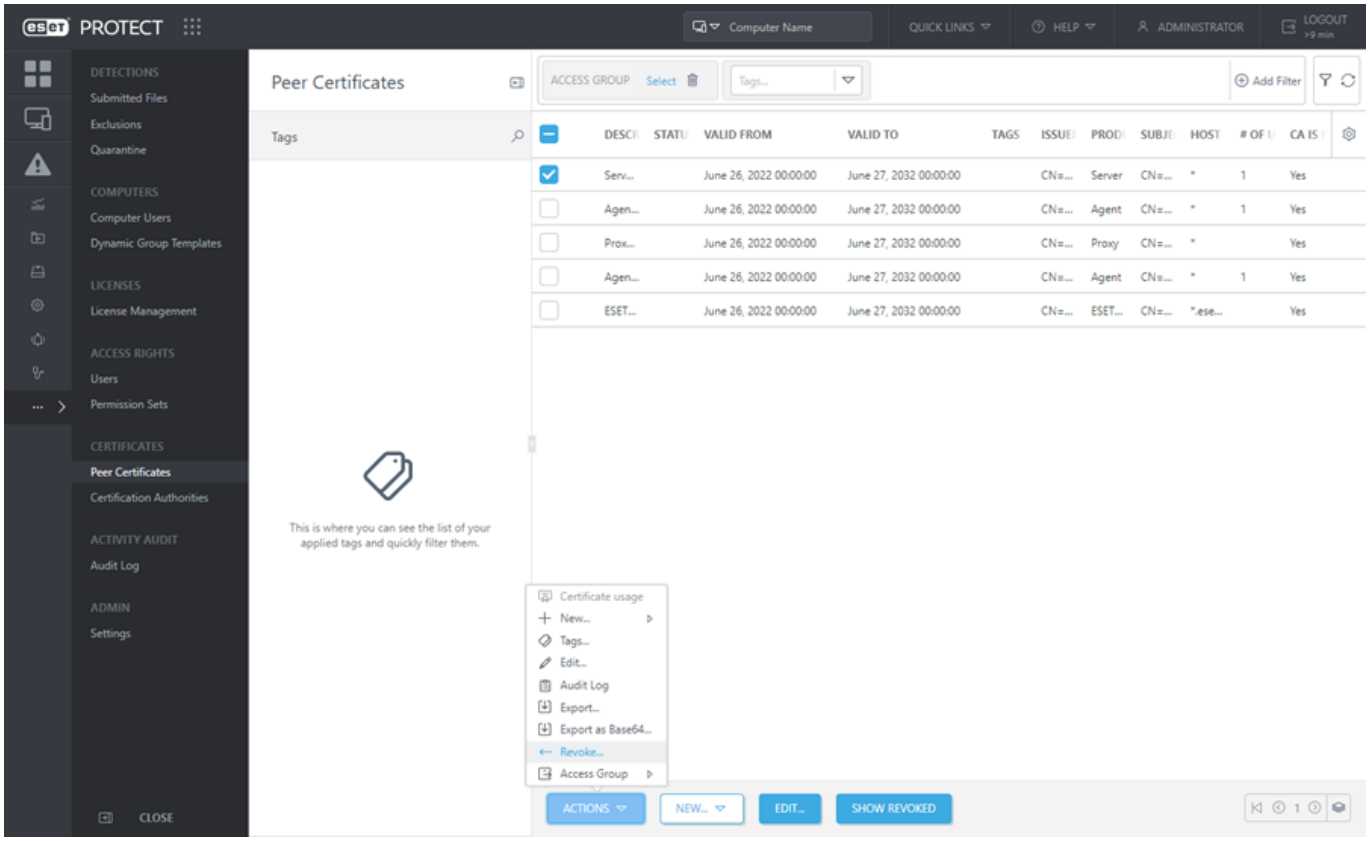


Exibir revogado

Esta lista exibe todos os certificados que foram criados e depois invalidados pelo Servidor ESET PROTECT. Certificados revogados serão automaticamente removidos da tela principal de **certificado de mesmo nível**. Clique em **Exibir revogados para ver os** certificados que foram revogados da janela principal.

Para revogar um certificado, siga as etapas abaixo:

1. Vá para **Mais** > **Certificados de mesmo nível** > selecione um certificado e clique em **Revogar**.



2. Especifique o **Motivo** da revogação e clique em **Revogar**.

3. Clique em **OK**. O certificado desaparecerá da lista de certificados de mesmo nível. Para ver certificados revogados anteriormente, clique no botão **Exibir revogados**.

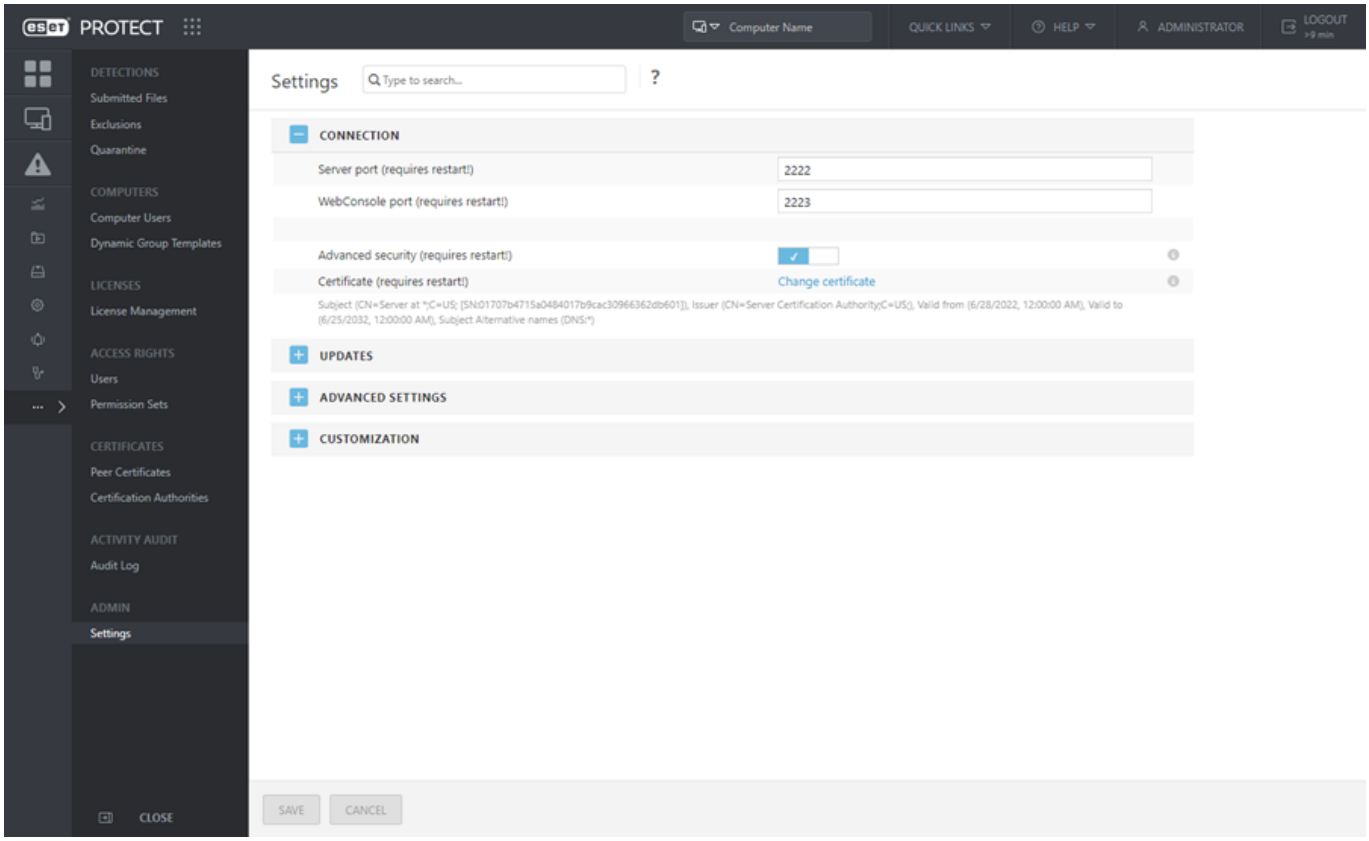
Definir novo certificado do Servidor ESET PROTECT

Seu certificado do Servidor ESET PROTECT é criado durante a instalação e distribuído aos agentes ESET Management e outros componentes para permitir a comunicação com o Servidor ESET PROTECT.

- Se necessário, você pode configurar o Servidor ESET PROTECT para usar um certificado de mesmo nível diferente. Você pode usar o certificado do Servidor ESET PROTECT (gerado automaticamente durante a instalação) ou um **Certificado personalizado**.

- OESET PROTECT Certificado do servidor é necessário para uma autenticação e conexão TLS segura. O certificado do Servidor é usado para se certificar de que agentes ESET Management e proxies ESET PROTECT não conectam a um servidor ilegítimo.

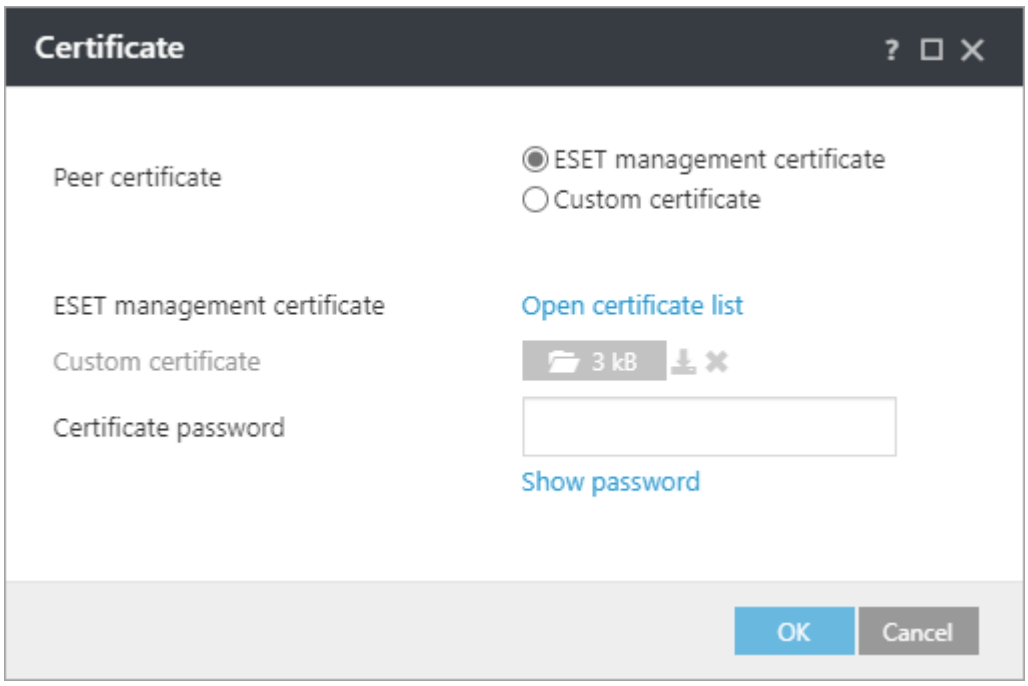
1.Clique em **Mais** > **Configurações** > abra a seção **Conexão**, selecione **Alterar certificado**.



2.Escolha a partir dos dois tipos de certificado de mesmo nível:

• **Certificado do ESET Management** - clique em **Abrir lista de certificados** e selecione o certificado a ser usado.

• **Certificado personalizado** – navegue para o seu certificado personalizado e clique em **OK** e **Salvar**. Se você estiver realizando uma migração, selecione o arquivo de certificado *.pfx* do Servidor ESET PROTECT exportado do seu Servidor ESET PROTECT antigo.



3.**Reinicie** o serviço do Servidor ESET PROTECT, consulte nosso artigo da Base de Conhecimento.

Certificados personalizados com ESET PROTECT

Se você tem seu próprio PKI (infraestrutura de chave pública) dentro do seu ambiente e quer que o ESET PROTECT use seus certificados personalizados para comunicação entre os componentes, veja o exemplo abaixo. Esse exemplo é executado em um Windows Server 2012 R2. Capturas de tela podem variar em outras versões do windows, mas o procedimento geral permanece o mesmo.

- Não use certificados com validade curta (por exemplo, Let's Encrypt que são válidos por 90 dias) para evitar o procedimento complexo de uma substituição frequente.
- Se você gerenciar dispositivos móveis, não recomendamos usar certificados assinados com assinatura própria (incluindo certificados assinados pela CA ESET PROTECT) porque nem todos os dispositivos móveis permitem que os usuários aceitem certificados assinados com assinatura própria. Recomendamos usar um certificado personalizado fornecido por uma Autoridade de certificação de terceiros.

Você pode usar o OpenSSL para criar novos certificados com assinatura própria. Veja nosso artigo da Base de conhecimento para obter mais informações.

Funções de servidor necessárias:

- Serviços de domínio do Active Directory.
- Certificado de Serviço do Active Directory com o CA de Raiz Autônomo instalado.

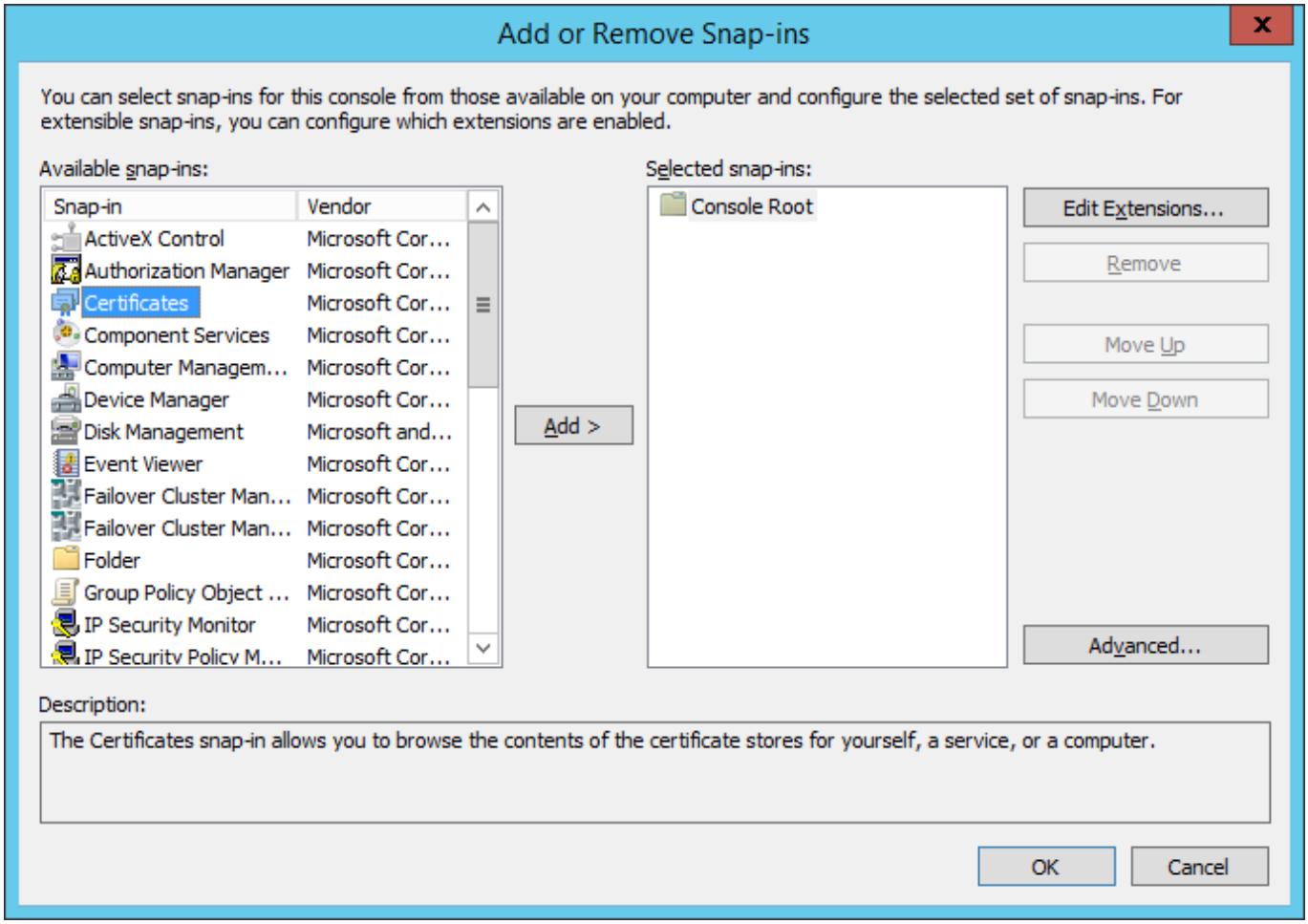
1. Abra o **Console de gerenciamento** e adicione snap-ins de **Certificados**:

   a)Faça logon no servidor como membro do grupo Administrador local.

   b)Execute o mmc.exe para abrir o Console de gerenciamento.

   c)Clique em **Arquivo** e selecione **Adicionar/remover Snap-in...** (ou pressione **CTRL+M**).

   d)Selecione **Certificados** no painel da esquerda e clique no botão **Adicionar**.



e)Selecione **Conta de computador** e clique em **Avançar**.

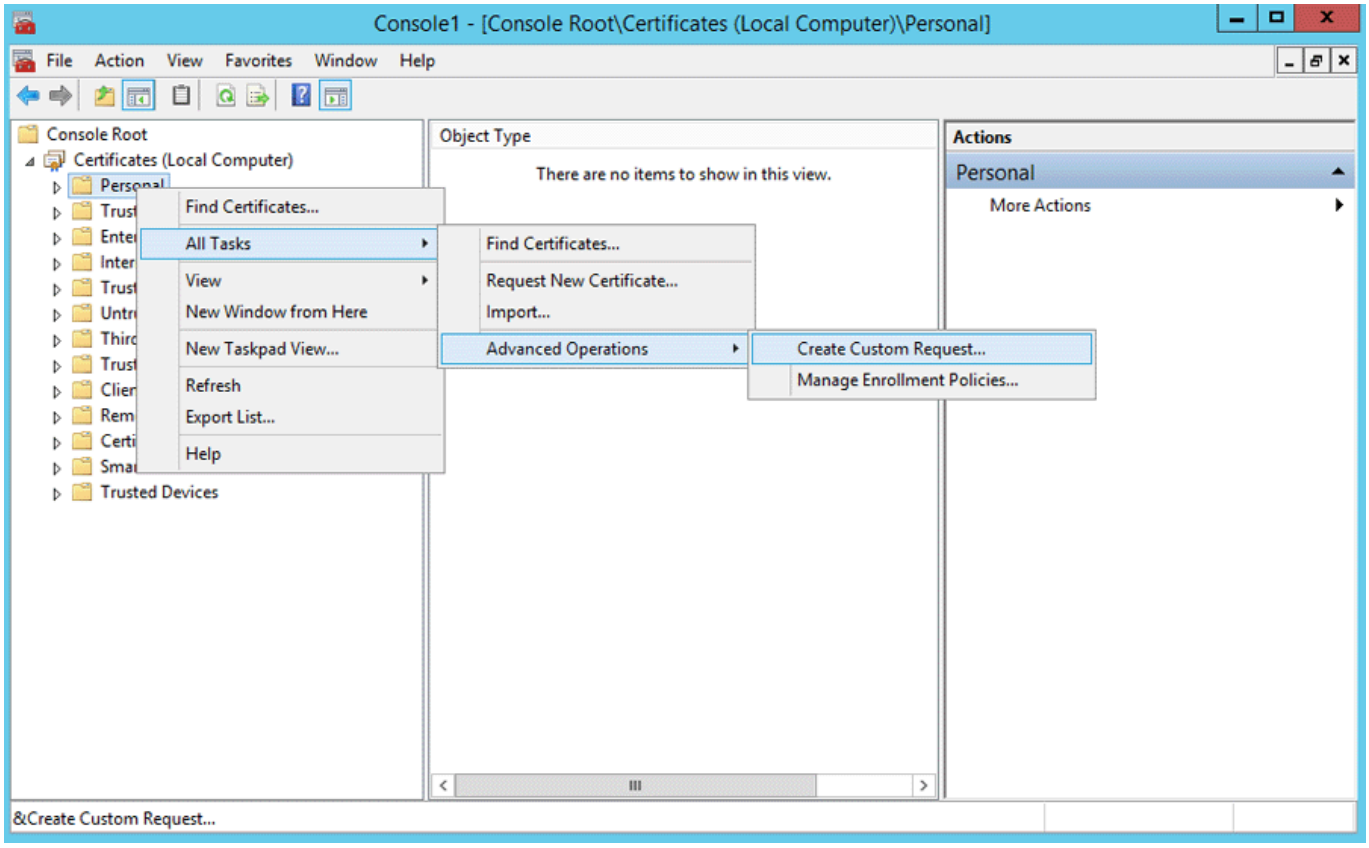
f)Certifique-se que o **Computador Local** está selecionado (padrão) e clique em **Concluir**.

g)Clique em **OK**.

2. Criar uma **Solicitação de certificado personalizado**:

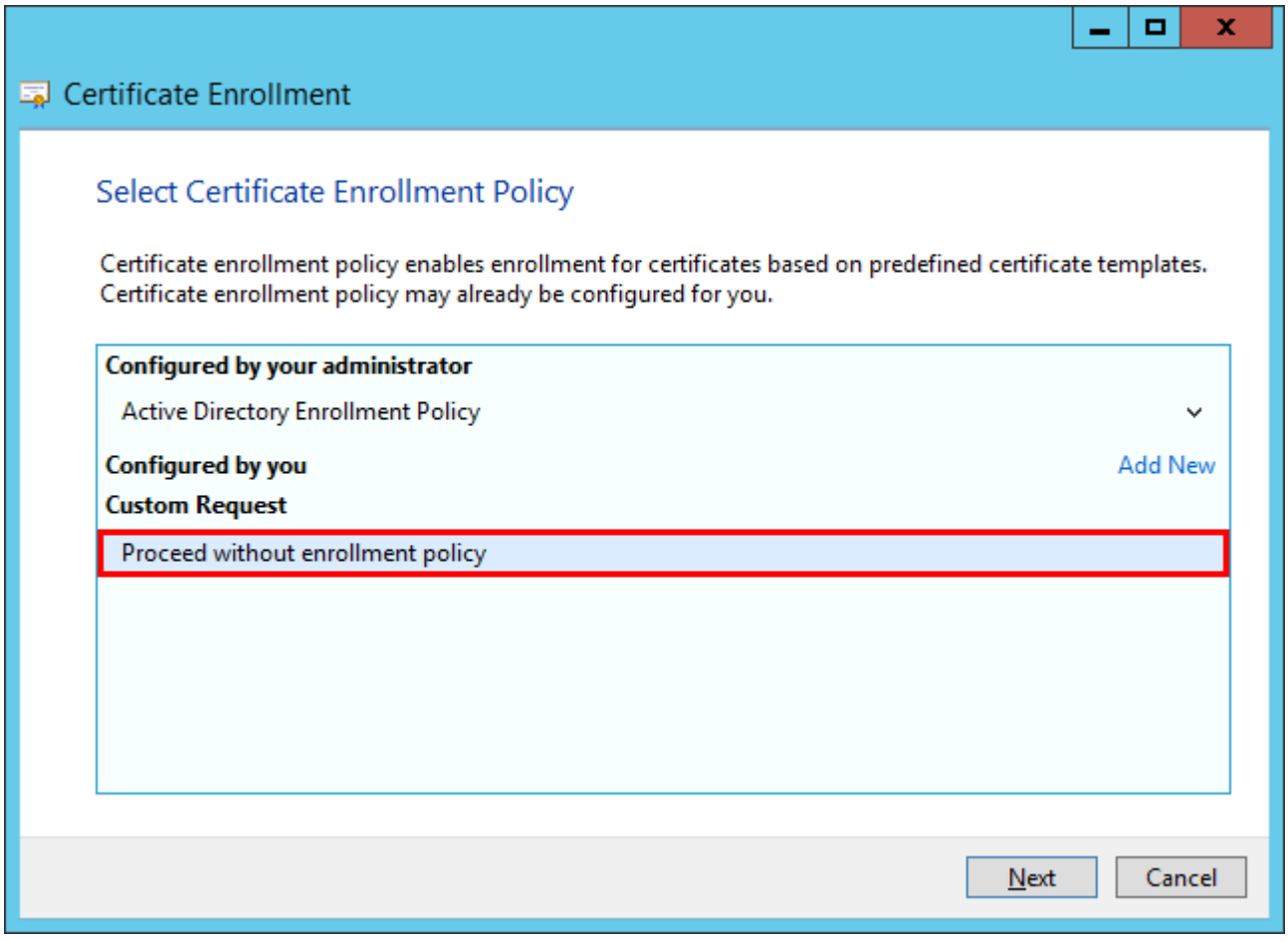
a)Clique duas vezes em **Certificados (Computador local)** para expandir.

b)Clique duas vezes em Pessoal para expandir. Clique com o botão direito em Certificados e selecione Todas as tarefas > Operações avançadas e escolha Criar solicitação personalizada

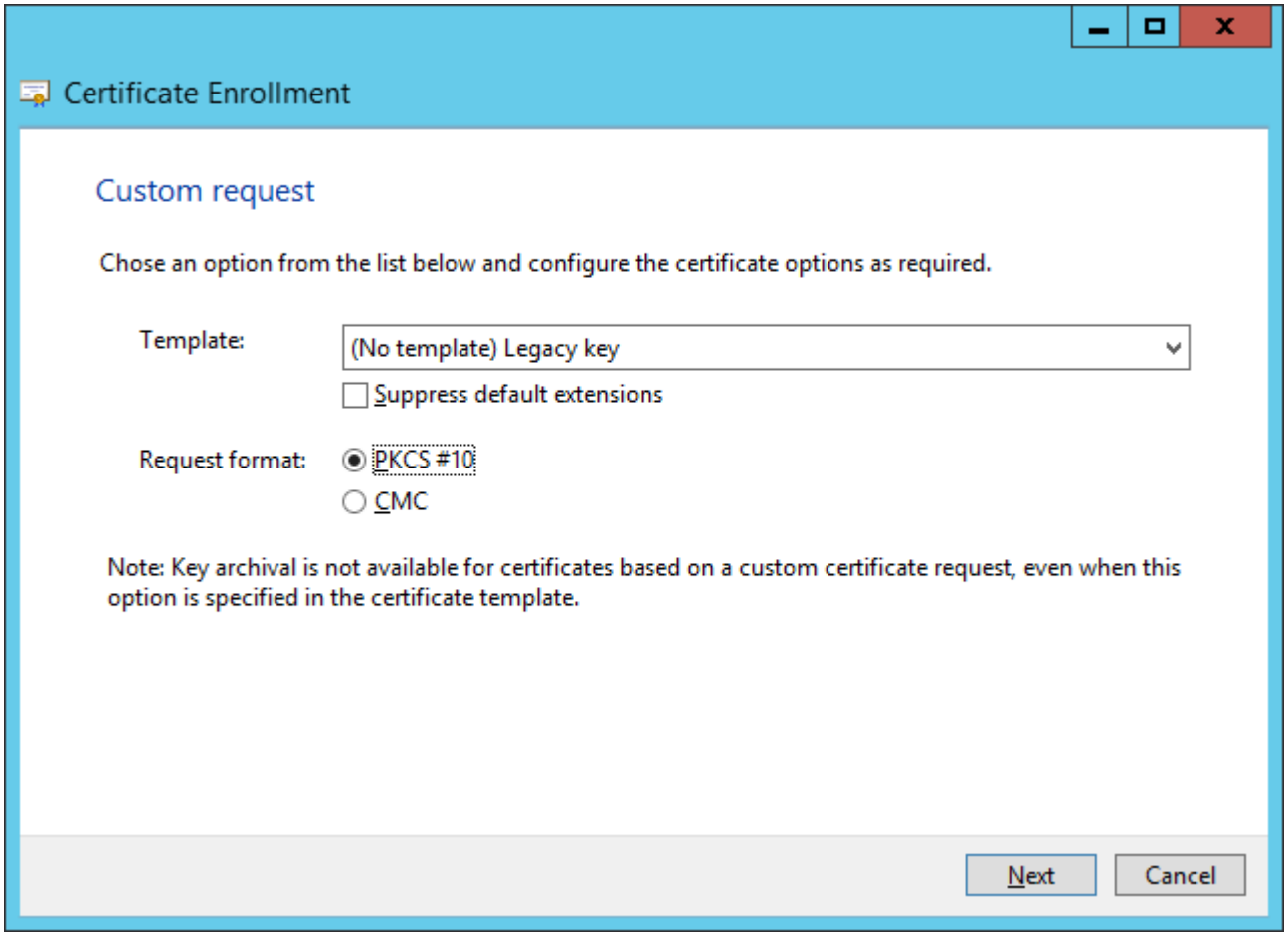


c)A janela do assistente de Inscrição de certificado vai abrir, clique em **Avançar**.

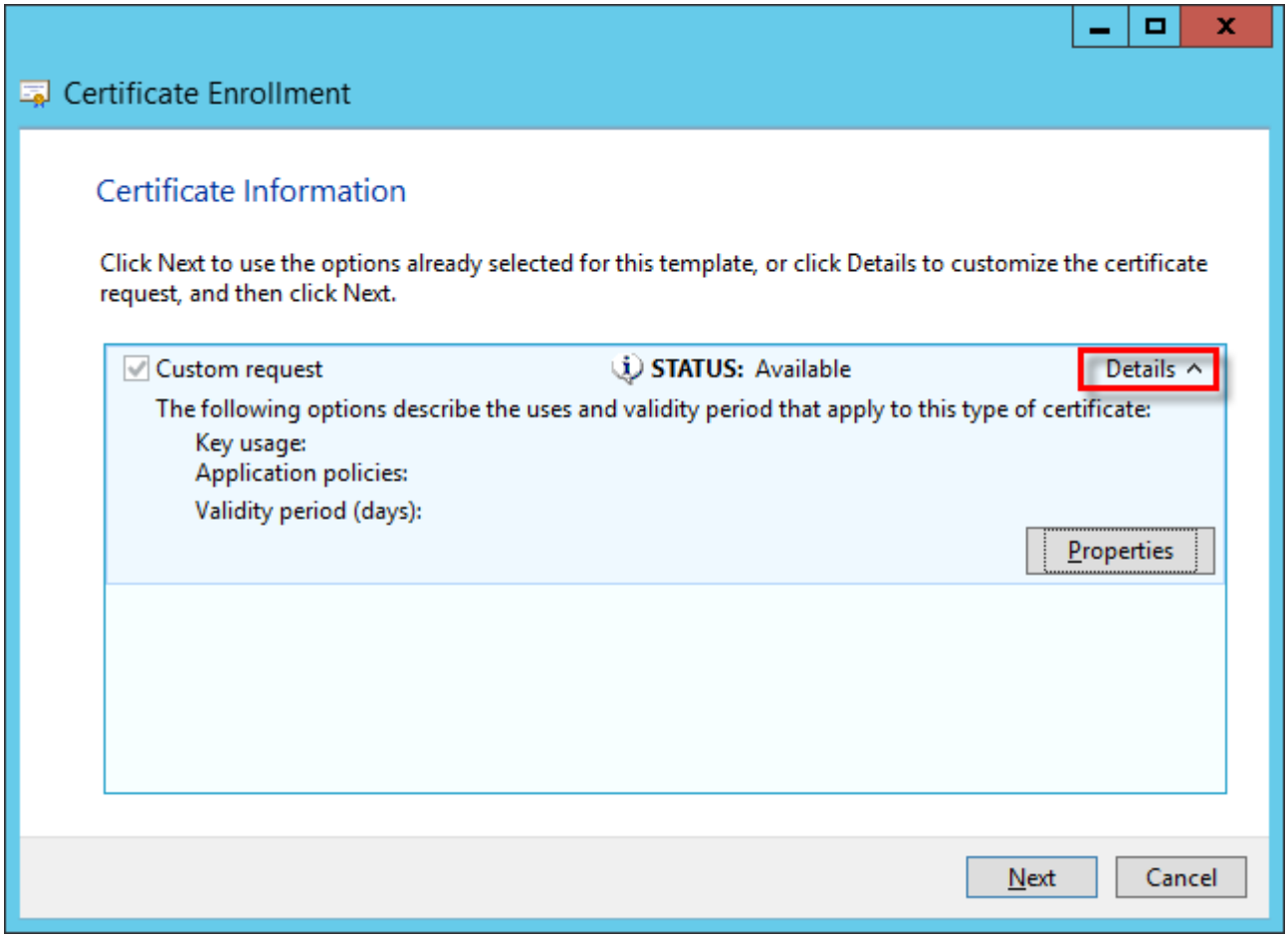
d)Selecione **Continuar sem política de inscrição** e clique em **Avançar** para continuar.



e)Escolha **(Sem modelo) Chave de legado** da lista suspensa e certifique-se de que o formato de solicitação **PKCS #10** foi selecionado. Clique em **Avançar**.



f)Clique na seta para abrir a seção **Detalhes** e clique em **Propriedades**.



g)Na guia **Geral**, digite o **Nome amigável** do seu certificado, você também pode digitar a Descrição (opcional).

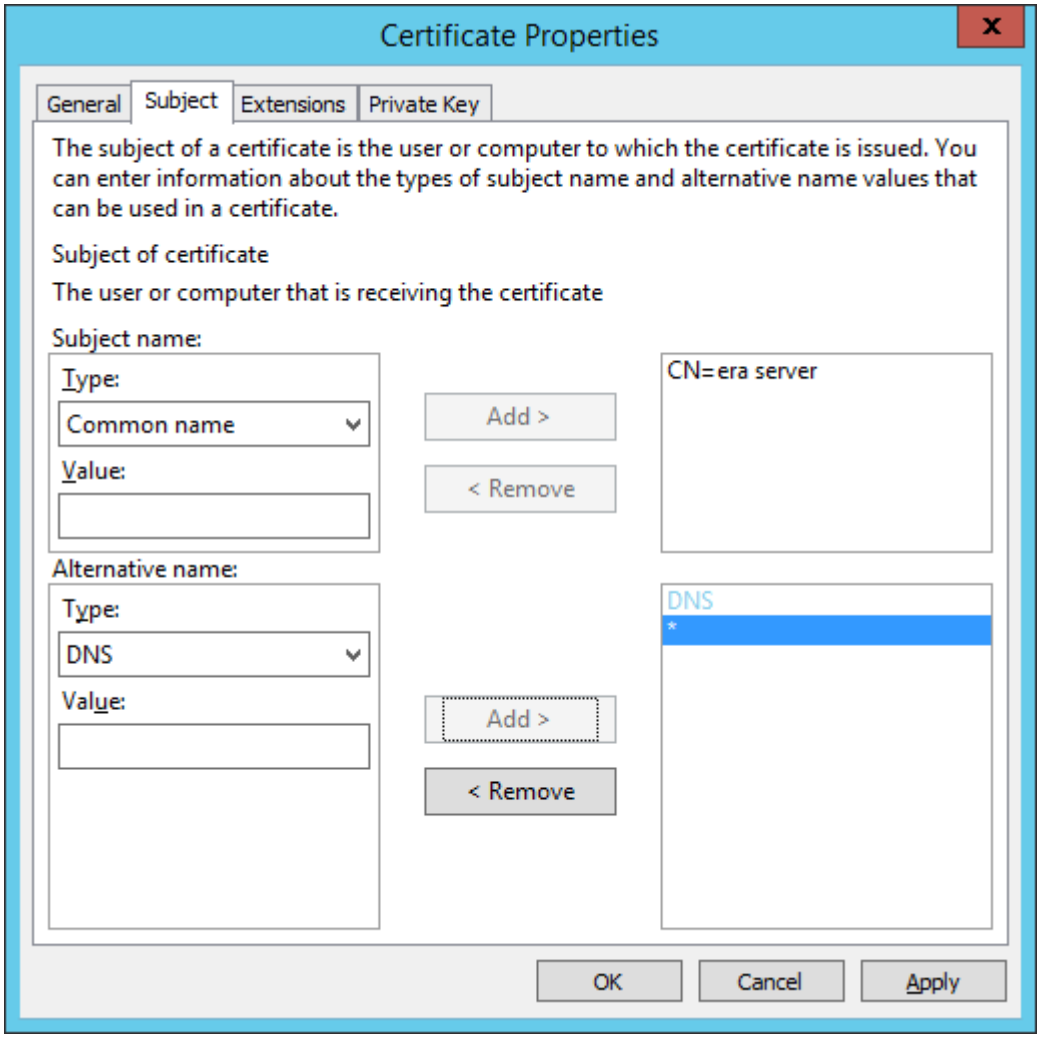
h)Na guia **Assunto**, faça o seguinte:

Na seção **Nome do assunto**, selecione **Nome comum** na lista suspensa em **Tipo** e digite `era server` no campo **Valor**, então clique em **Adicionar**. O **CN=era server** vai aparecer na caixa de informações na direita. Se você estiver criando uma solicitação de certificado para o Agente ESET Management digite `era agent` no campo de valor de nome comum.

O nome comum deve conter uma dessas strings: "**servidor**" ou "**agente**", dependendo de qual Solicitação de certificado você quer criar.

i)Na seção **Nome alternativo**, escolha **DNS** da lista suspensa em **Tipo** e digite * (asterisco) no campo **Valor**, então clique no botão **Adicionar**.

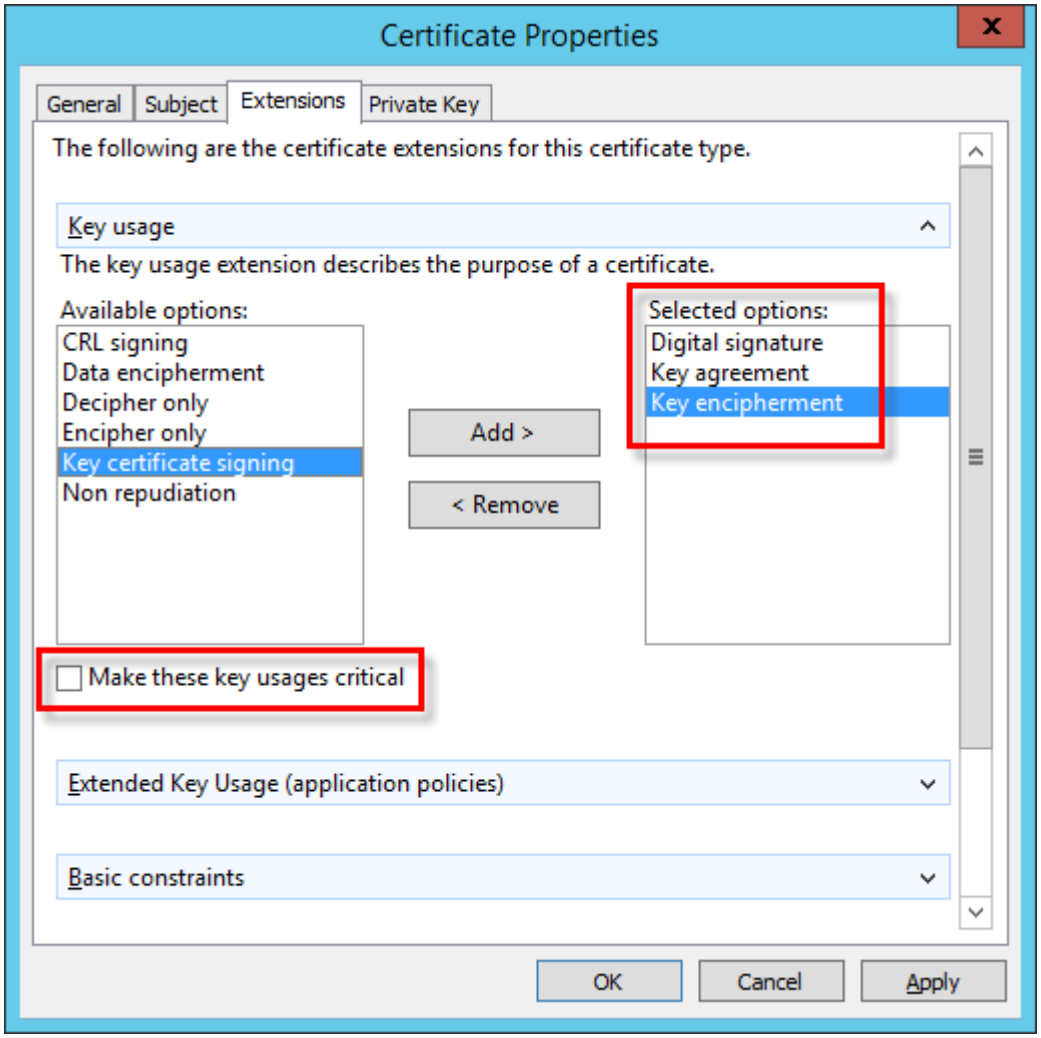
O Nome alternativo para o assunto (Subject Alternative Name – SAN) deve ser definido como "DNS:*" para o Servidor ESET PROTECT e para todos os agentes.



j)Na guia **Extensões**, abra a seção **Uso de chave** clicando na seta. Adicione o seguinte das Opções disponíveis: **Assinatura digital**, **Combinação de chave**, **Criptografia de chave**. Desmarque a opção **Tornar o uso dessas chaves crítico**.

Certifique-se de selecionar as três opções sob **Uso da chave** > **Assinatura de certificado da chave**:

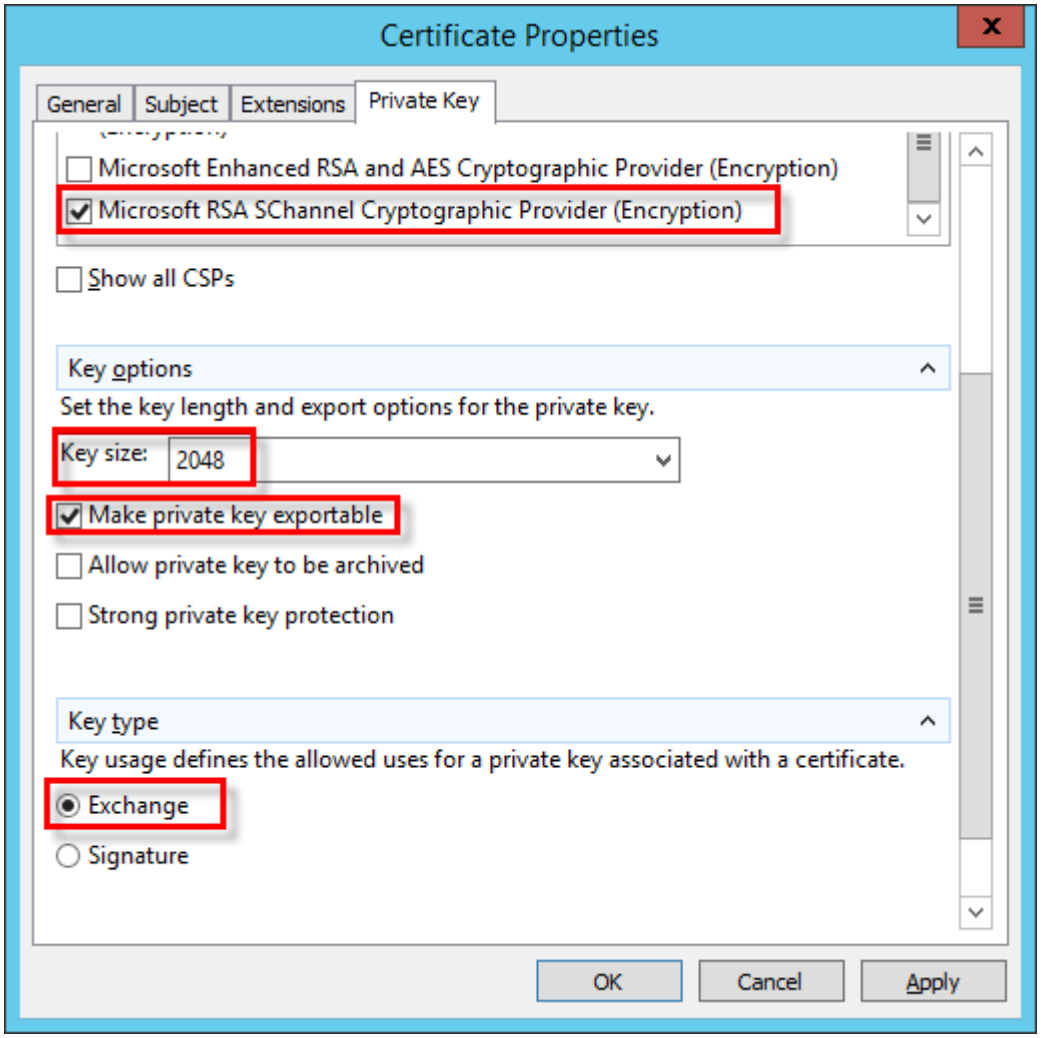
- **Assinatura digital**
- **Acordo de chave**
- **Criptografia de chave**



k)Na guia **Chave privada**, faça o seguinte:

i.Abra a seção **Provedor de serviço criptográfico** clicando na seta. Uma lista de todos os provedores de serviços de criptografia (CSP) será exibida. Certifique-se de que somente **Microsoft RSA SChannel Cryptographic Provider (Encryption)** está selecionado.

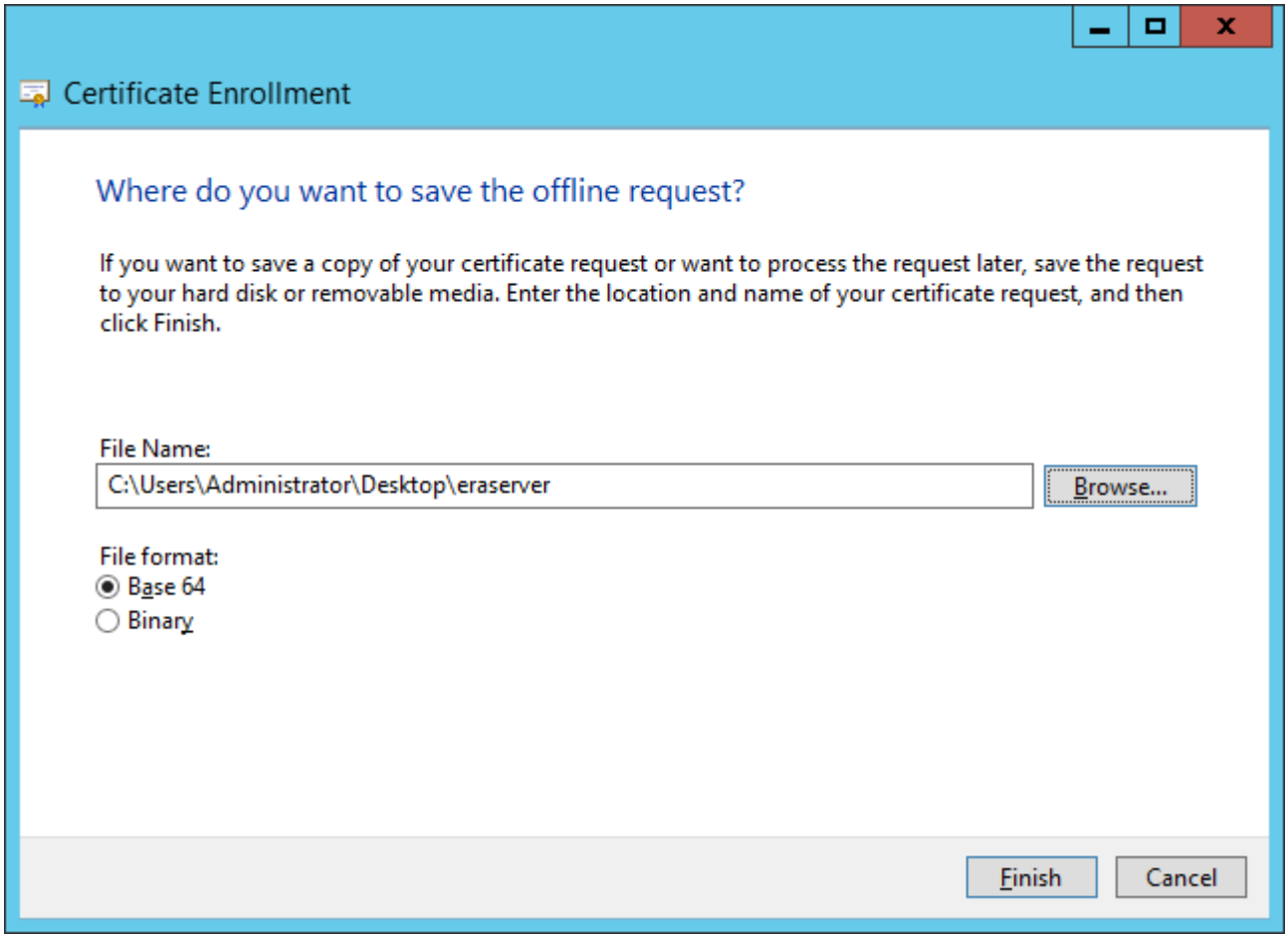
Desmarcar todos os CSPs que não sejam o **Microsoft RSA SChannel Cryptographic Provider (Criptografia)**.



i.Abra a seção **Chave Opções**. No menu **Tamanho da chave**, defina um valor de pelo menos **2048**. Selecione **Tornar chave privada exportável**.

ii.Abra a seção **Tipo de chave** e selecione **Exchange**. Clique em **Aplicar** e verifique suas configurações.

l)Clique em **OK**. Informações do certificado serão exibidas. Clique no botão **Avançar** para continuar. Clique em **Procurar** para selecionar o local onde a solicitação de assinatura de certificado (CSR) será salva. Digite o nome do arquivo e certifique-se de que **Base 64** está selecionado.

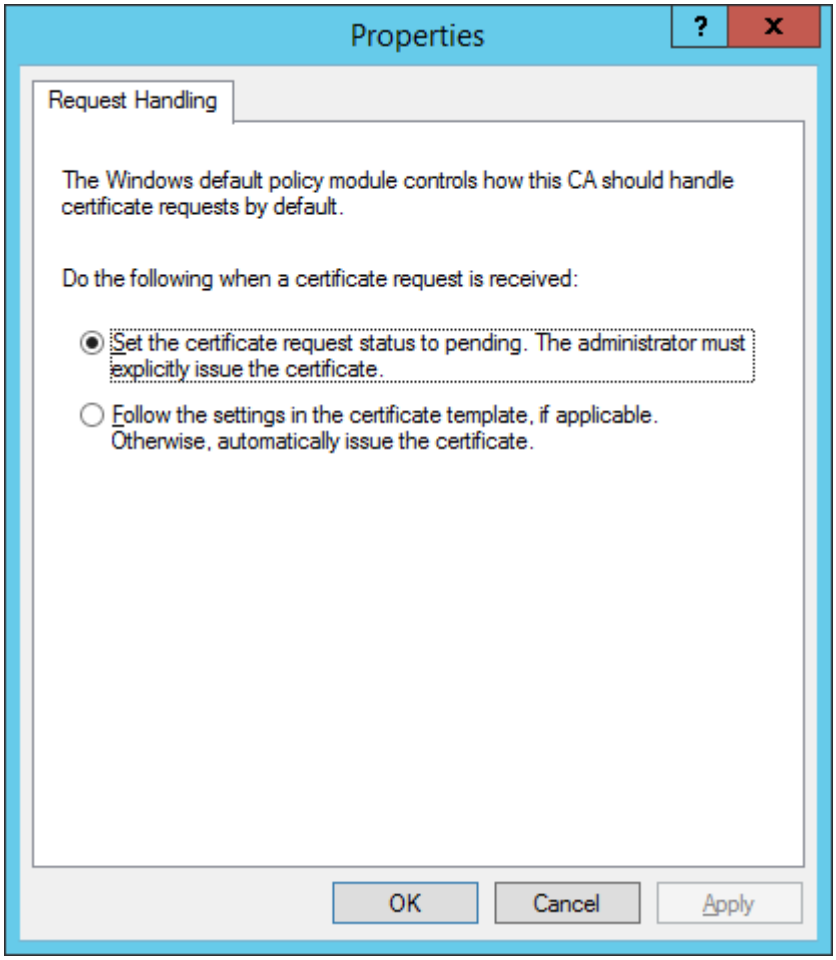


m)Clique em **Concluir** para gerar o CSR.

3. Para importar sua solicitação de certificado personalizado, siga as etapas abaixo:

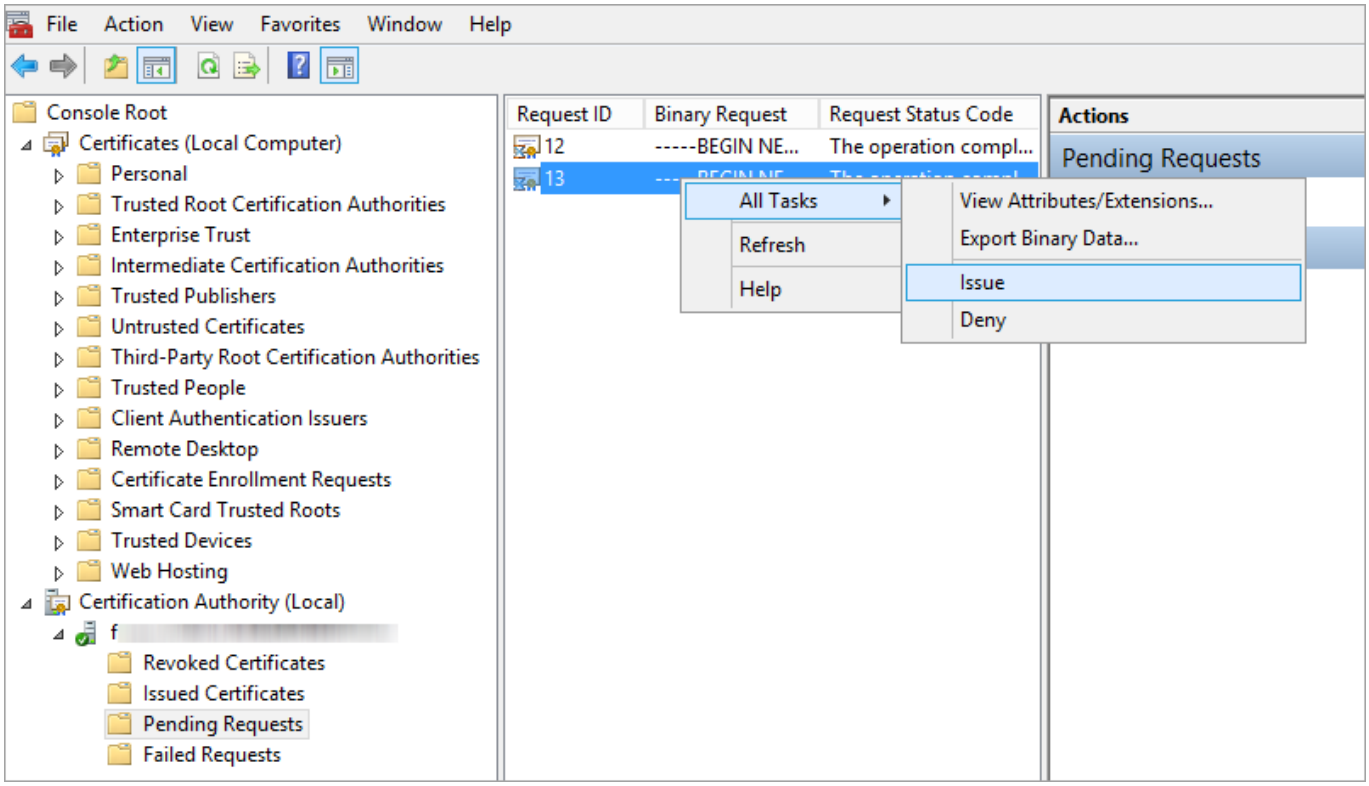
a)Abra o Gerenciador de servidor e clique em **Ferramentas** > **Autoridade de Certificação**.

b)Na árvore **Autoridade de Certificação (Local)**, selecione **Seu servidor** (geralmente FQDN) > **Propriedades** e selecione a guia **Módulo de Política**. Clique em **Propriedades** e selecione **Definir o status da solicitação de certificado como pendente. O administrador deve emitir explicitamente o certificado**. Caso contrário, ele não vai funcionar adequadamente. Você precisará reiniciar os serviços de certificados do Active Directory se precisar alterar essa configuração.



c)Na árvore **Autoridade de Certificação (Local)**, selecione **Seu servidor (geralmente FQDN)** > **Todas as tarefas** > **Enviar nova solicitação** e vá para o arquivo **CSR** gerado anteriormente na etapa 2.

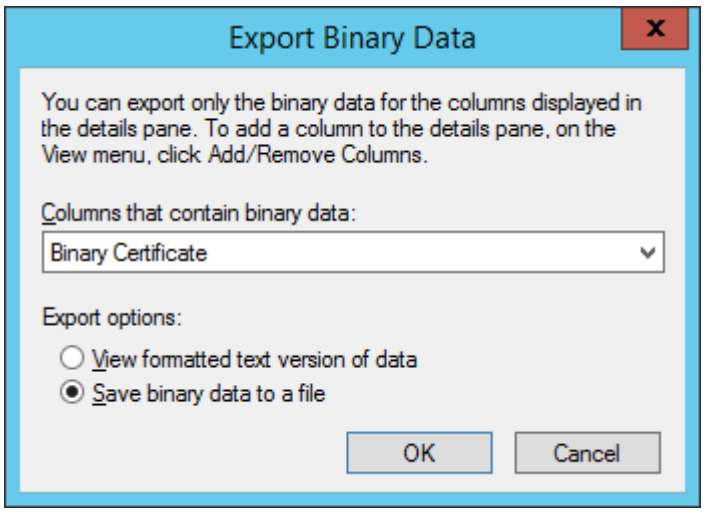
d)O certificado será adicionado a **Solicitações pendentes**. Selecione o **CSR** no painel de navegação da direita. No menu **Ação**, selecione **Todas as tarefas** > **Emitir**.



4. Exportar **Certificado personalizado emitido** para o arquivo *.tmp*.

a)Selecione Certificados **Emitidos** no painel da esquerda. Clique com o botão direito no certificado que você deseja exportar e clique em **Todas as tarefas** > **Exportar dados binários**.

b)No diálogo **Exportar dados binários**, escolha **Certificado binário** da lista suspensa. Em **Opções de exportação**, clique em **Salvar dados binários para um arquivo** e clique em **OK**.



c)Na caixa de diálogo Salvar dados binários, vá para o local do arquivo onde deseja salvar o certificado e clique em **Salvar**.

5. Importar o arquivo *..tmp*.

a)Vá para Certificado (Computador local) > clique com o botão direito em Pessoal, selecione Todas as tarefas > Importar.

b)Clique em **Avançar**.

c)Localize seu arquivo binário *.tmp* salvo anteriormente usando **Procurar** e clique em **Abrir**. Selecione Colocar todos os certificados no armazenamento a seguir > **Pessoal**. Clique em **Avançar**.

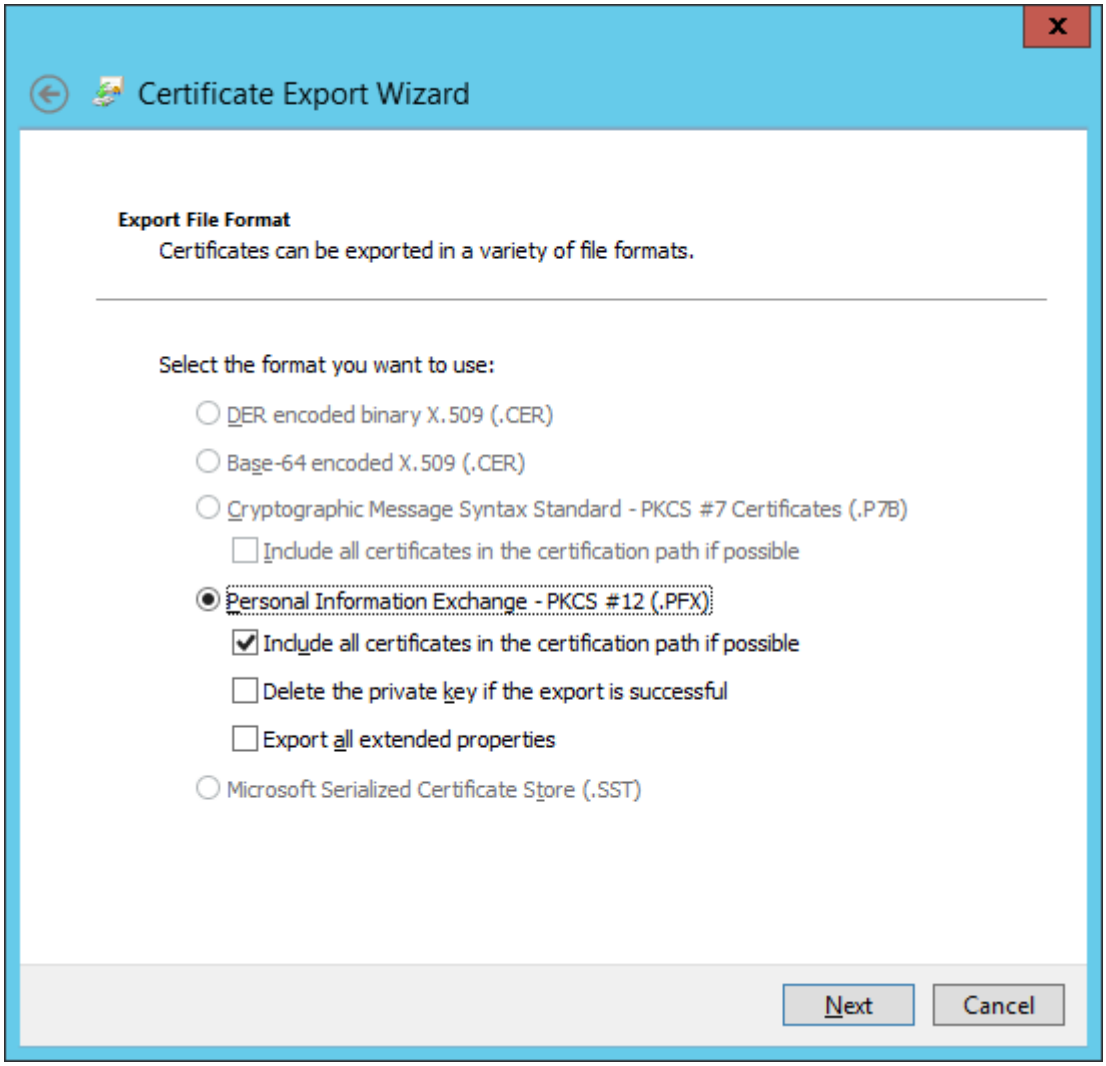
d)Clique em **Concluir** para importar o certificado.

6. Exporte o Certificado incluindo uma chave privada para o arquivo *.pfx*.

a)Em **Certificados (computador local)** abra **Pessoal** e clique em **Certificados**, selecione o certificado criado que você deseja exportar, no menu **Ação**, aponte para **Todas as tarefas** > **Exportar**.

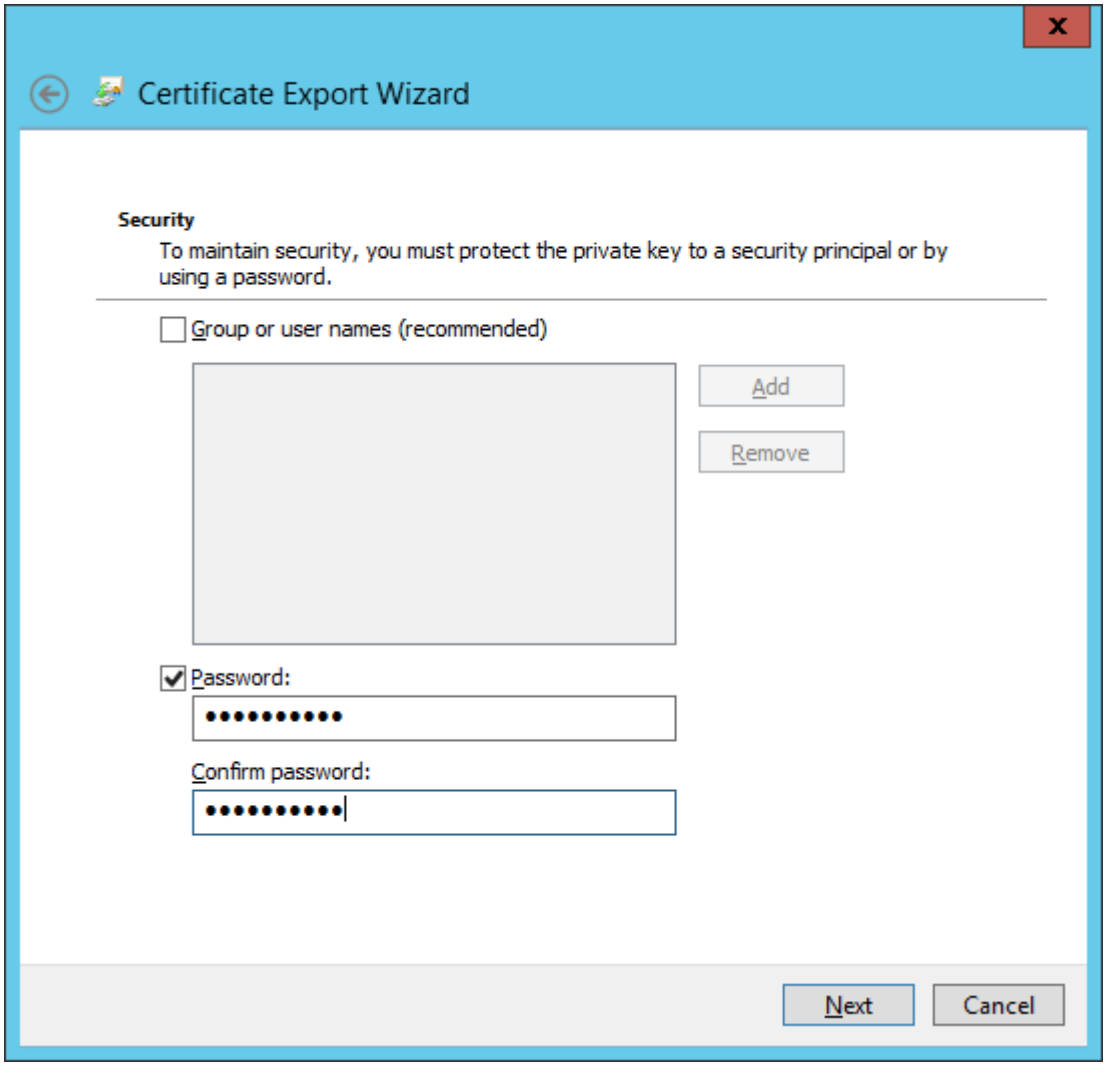
b)No **Assistente de exportação de certificados**, clique em **Sim, exportar a chave privada**. (Esta opção vai aparecer somente se a chave privada for marcada como de exportação possível e se você tiver acesso à chave privada.)

c)Em Formato de arquivo de exportação, selecione **Personal Information Exchange -PKCS #12 (.PFX)**, selecione a caixa de marcação ao lado de **Incluir todos os certificados no caminho de certificação se possível** e clique em **Avançar**.



d)**Senha**, digite uma senha para criptografar a chave privada que você está exportando. No campo **Confirmar senha**, digite a mesma senha novamente e clique em **Avançar**.

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



e)**Nome do arquivo**, digite um nome de arquivo e caminho para o arquivo *.pfx* que vai armazenar o certificado exportado e a chave privada. Clique em **Avançar** e depois em **Concluir**.

> O exemplo acima mostra como criar o certificado de um Agente ESET Management. Repita as mesmas etapas para os certificados do Servidor ESET PROTECT.
> Não é possível usar esse certificado para assinar outro novo certificado no console da Web.

7. Exportar Autoridade de certificação:

a)Abra o Gerenciador de servidor e clique em **Ferramentas** > **Autoridade de Certificação**.

b)Na árvore **Autoridade de Certificação (Local)**, selecione **Seu servidor (geralmente FQDN)** > **Propriedades** > **Geral** e selecione a guia **Exibir certificado**.

c)Na guia **Detalhes**, clique em **Copiar para o arquivo**. O **Assistente de exportação do certificado** vai abrir.

d)Na janela **Formato de exportação do arquivo**, selecione **binário codificado DER X.509 (.CER)** e clique em **Avançar**.

e)Clique em **Procurar** para selecionar o local onde o arquivo *.cer* será salvo e clique em **Avançar**.

f)Clique em **Concluir** para exportar a autoridade de certificação.

Para instruções passo a passo sobre o uso de certificados personalizados no ESET PROTECT, consulte o próximo capítulo.

Como usar o certificado personalizado com ESET PROTECT

Para continuar do capítulo anterior:

1. Importe sua Autoridade de certificação de terceiros para o Web Console ESET PROTECT.

2. Defina o novo certificado de servidor personalizado no console da Web ESET PROTECT.

Se você já tiver um Agente ESET Management conectando ao Servidor ESET PROTECT, aplique uma política para alterar o certificado personalizado para os Agentes ESET Management:
1. Abra o console da Web ESET PROTECT.
2. Clique em **Políticas** > **Nova**. Digite um nome para a política.
3. Abra as **Configurações** e selecione Agente **ESET Management** do menu suspenso.
4. Abra a **Conexão** e clique em **Alterar certificado** ao lado de **Certificado**.
5. Clique em **Certificado personalizado** e selecione o certificado personalizado para o Agente ESET Management.
6. Digite a senha do certificado e clique em **OK**.
7. Atribua essa política a todos os clientes.

3. Navegue para **Iniciar** > **Programas e Recursos**, clique com o botão direito em **ESET Management Agente** e selecione **Alterar**.

4. Clique no botão **Avançar** e execute **Reparar**.

5. Não altere as configurações do Host do servidor e Porta do servidor e clique em **Avançar**.

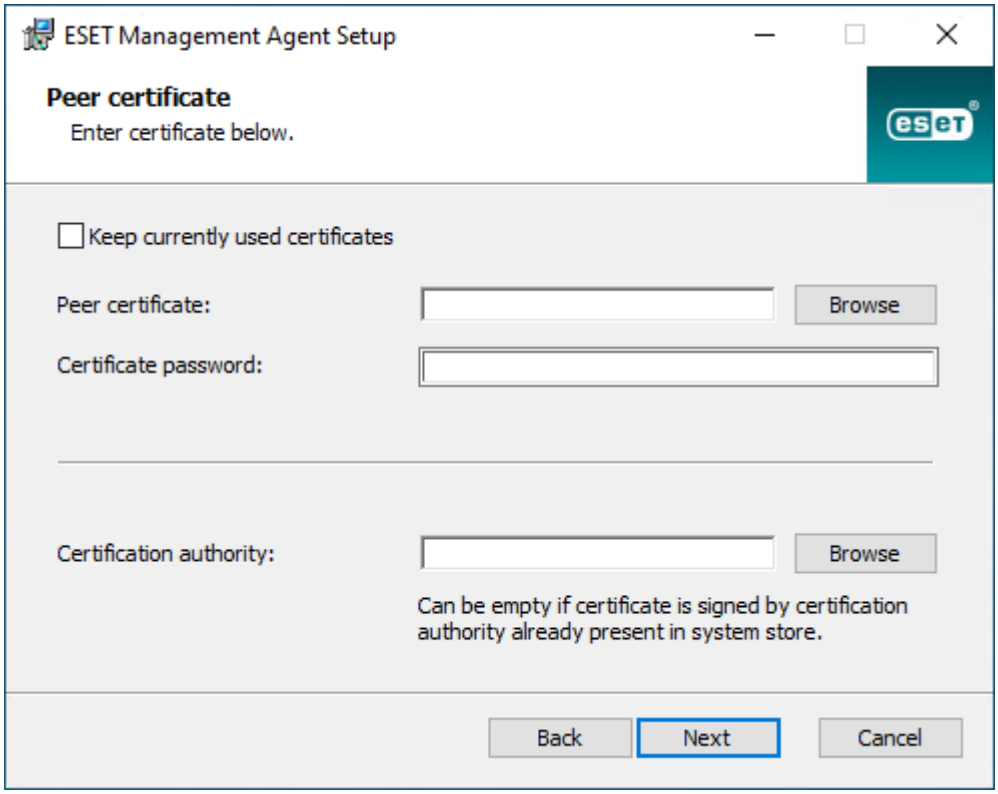
6. Clique em **Procurar** ao lado de **Certificado de mesmo nível** e localize o arquivo personalizado de certificado *.pfx*.

7. Digite a senha do certificado que você especificou na etapa 6.

8. Clique em **Procurar** ao lado de **Autoridade de certificação e selecione o arquivo** .der (chave pública) exportado do console web. Deve ser a chave pública que assina o certificado personalizado.

9. Clique em **Avançar** e conclua o reparo.

10. O Agente ESET Management agora está usando um certificado personalizado.*pfx*.



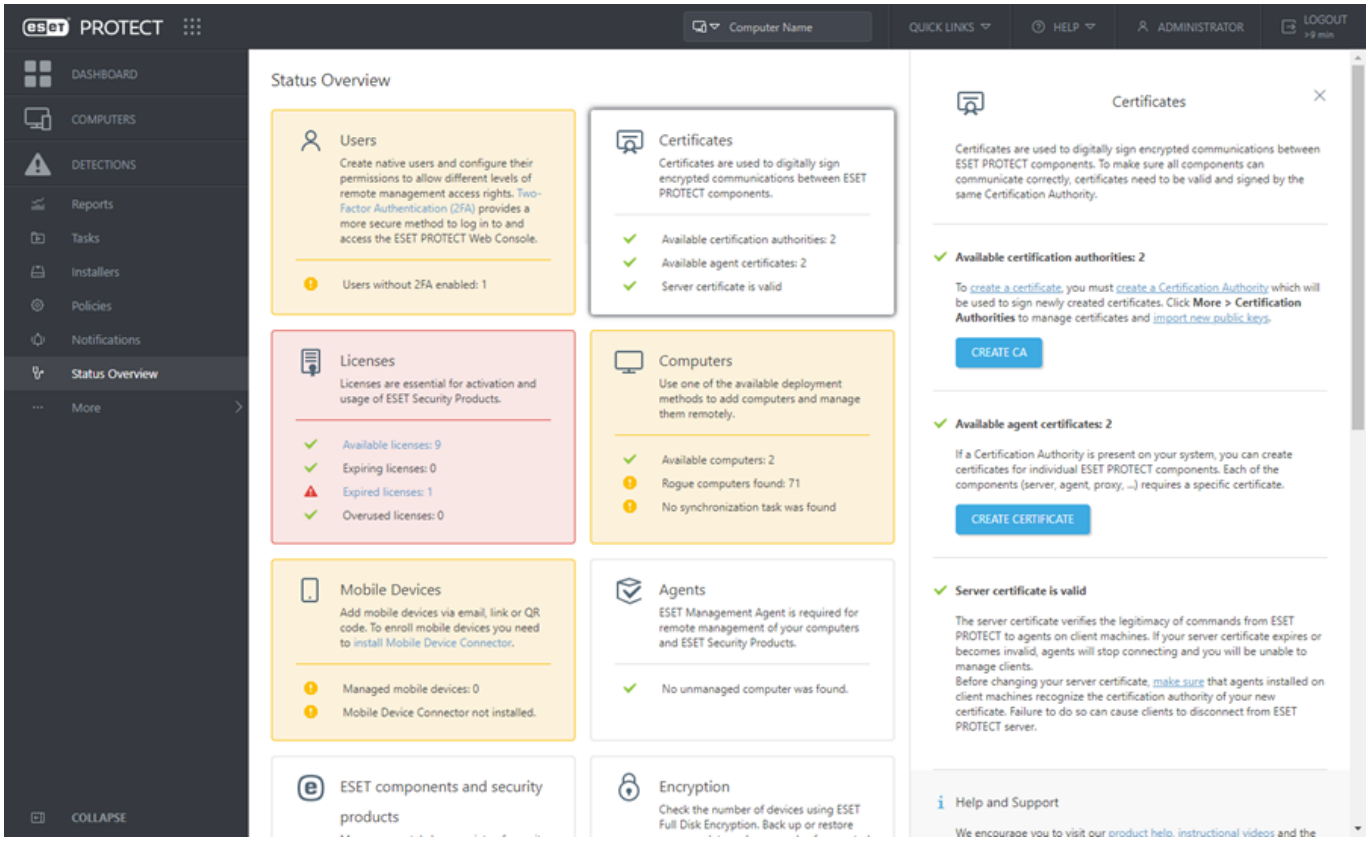
Certificado expirando - relatório e substituição

O ESET PROTECT é capaz de notificar sobre um Certificado ou autoridade de certificação que vai expirar. Existem **Notificações** pré-configuradas para o Certificado ESET PROTECT e para a Autoridade de certificação ESET PROTECT na guia **Notificações**.

Para ativar este recurso, clique em **Editar notificação** e detalhes específicos na seção Distribuição, como endereço de email e intercepção SNMP. Cada usuário é capaz de ver as notificações apenas para os certificados que estão em seu grupo inicial (considerando que o usuário tenha atribuído permissões de **Leitura** para os **Certificados**).

> Certifique-se de primeiro ter configurado as definições de conexão SMTP em **Mais** > **Configurações**. Depois disso, você pode editar a notificação para adicionar os Endereços de email de distribuição.

Se um computador tiver um certificado prestes a expirar, suas informações de status vão mudar automaticamente. O status será reportado para a guia Painel, lista de Computadores , Visão geral do status e Certificado:



Para substituir a Autoridade de certificação ou Certificado expirando, siga essas etapas:

1.Criar uma nova Autoridade de Certificação com o novo período de validade (caso o antigo vá expirar), de preferência definindo para que ele seja válido imediatamente.

2.Criar um novo Certificado de mesmo nível para o Servidor ESET PROTECT e outros componentes (Agente/MDM) dentro do período de validade da sua nova Autoridade de certificação.

3.Criar políticas para definir novos Certificados de mesmo nível. Aplique as políticas aos componentes ESET PROTECT, MDM e ao Agente ESET Management em todos os computadores do cliente da sua rede.

4.Espere até que a nova Autoridade de Certificação e Certificados de mesmo nível sejam aplicados e os clientes sejam replicados.

Recomendamos que você aguarde 24 horas ou verifique se todos os seus componentes ESET PROTECT (Agentes) foram replicados pelo menos duas vezes. Você pode aplicar a replicação do Agente em **Computadores** clicando no computador e selecionando **Enviar chamada para acordar**.

5.Substitua o Certificado do servidor nas Configurações do Servidor ESET PROTECT para que os clientes consigam autenticar usando seus novos Certificados de mesmo nível.

6.Reinicie o serviço do Servidor ESET PROTECT.

7.Assim que tiver concluído todas as etapas acima, e que todos os clientes estiverem se conectando ao ESET PROTECT e funcionando como esperado, revogue os Certificados de mesmo nível antigos e exclua a Autoridade de certificação antiga.

Autoridades de certificação

Autoridades de certificação são listadas e gerenciadas na seção **Autoridades de certificação**. Se você tiver várias autoridades de certificação, é possível aplicar um filtro para classificá-las.

> Autoridades de certificação e certificados são acessados usando as mesmas permissões para a função **Certificados**. Certificados e autoridades criados durante a instalação, e os criados depois pelo administrador, estão contidos no grupo estático **Todos**. Veja a lista de permissões para obter mais informações sobre os direitos de acesso.

Clique em **Ações** para gerenciar a Autoridade de certificação selecionada:

- **Nova** – Criar uma nova Autoridade de certificação
- **Marcações** - Editar marcações (atribuir, remover atribuição, criar, remover).
- **Editar** – edite a descrição da autoridade de certificação.
- **Relatório de auditoria** - Exibe o Relatório de auditoria para o item selecionado.
- **Remover** – Remove a Autoridade de certificação selecionada.
- Importar chave pública
- Exportar chave pública – use essa opção para fazer backup das suas Autoridades de certificação.
- **Grupo de acesso** > **Mover** – Mova o objeto para outro grupo estático onde ele está disponível para usuários com direitos suficientes para o grupo de destino. Alterar o Grupo de acesso é útil ao resolver problemas de acesso com outros usuários. O Grupo de acesso define o grupo estático do objeto e o acesso ao objeto com base nos direitos de acesso do usuário.

Filtros e personalização de layout

Você pode personalizar a exibição da tela atual do console web:

- Gerenciar o painel lateral e a tabela principal.
- Adicionar filtro e predefinições de filtro. Você pode usar marcações para filtrar os itens exibidos.

Como dividir acesso a certificados e autoridades
Se o *Administrador* não quiser permitir que o usuário *John* acesse as Autoridades de Certificação ESET PROTECT, mas precisa que ele seja capaz de trabalhar com os certificados, o administrador precisa seguir essas etapas:
1.Criar um novo Grupo estático chamado *Certificados*.
2.Crie novo Conjunto de permissões.
a.Nomeie este conjunto de permissões como *Permissões para certificados*.
b.Adicione um grupo chamado *Certificados* na seção **Grupos estáticos**.
c.Na seção **Funcionalidade**, selecione **Gravação** para **Certificados**.
d.Na seção **Usuários**, clique em **Usuários nativos** e selecione *John.*
e.Clique em **Concluir** para salvar o conjunto de permissões.
3.Mova os certificados do grupo **Todos** para o grupo recém criado **Certificados***:*
a.Vá para **Mais** > **Certificados de mesmo nível**.
b.Selecione as caixas de seleção ao lado dos certificados que deseja mover.
c.Clique em **Ações** > **Grupo de acesso**, selecione o grupo **Certificados** e clique em **OK**.
Agora *John* pode modificar e usar os certificados movidos. Porém, as Autoridades de Certificação estão armazenadas com segurança fora do alcance do usuário. *John* não poderá nem mesmo usar as autoridades existentes (do grupo **Todos**) para assinar nenhum certificado.

Criar uma nova Autoridade de Certificação

Para criar uma nova Autoridade de certificação:, navegue para **Mais** > **Autoridade de Certificação** e clique em **Ação** > **Novo** na parte inferior da página.

Autoridade de certificação

Insira uma **descrição** da Autoridade de Certificação e selecione uma **Senha**. Esta **Senha** deve conter no mínimo 12 caracteres.

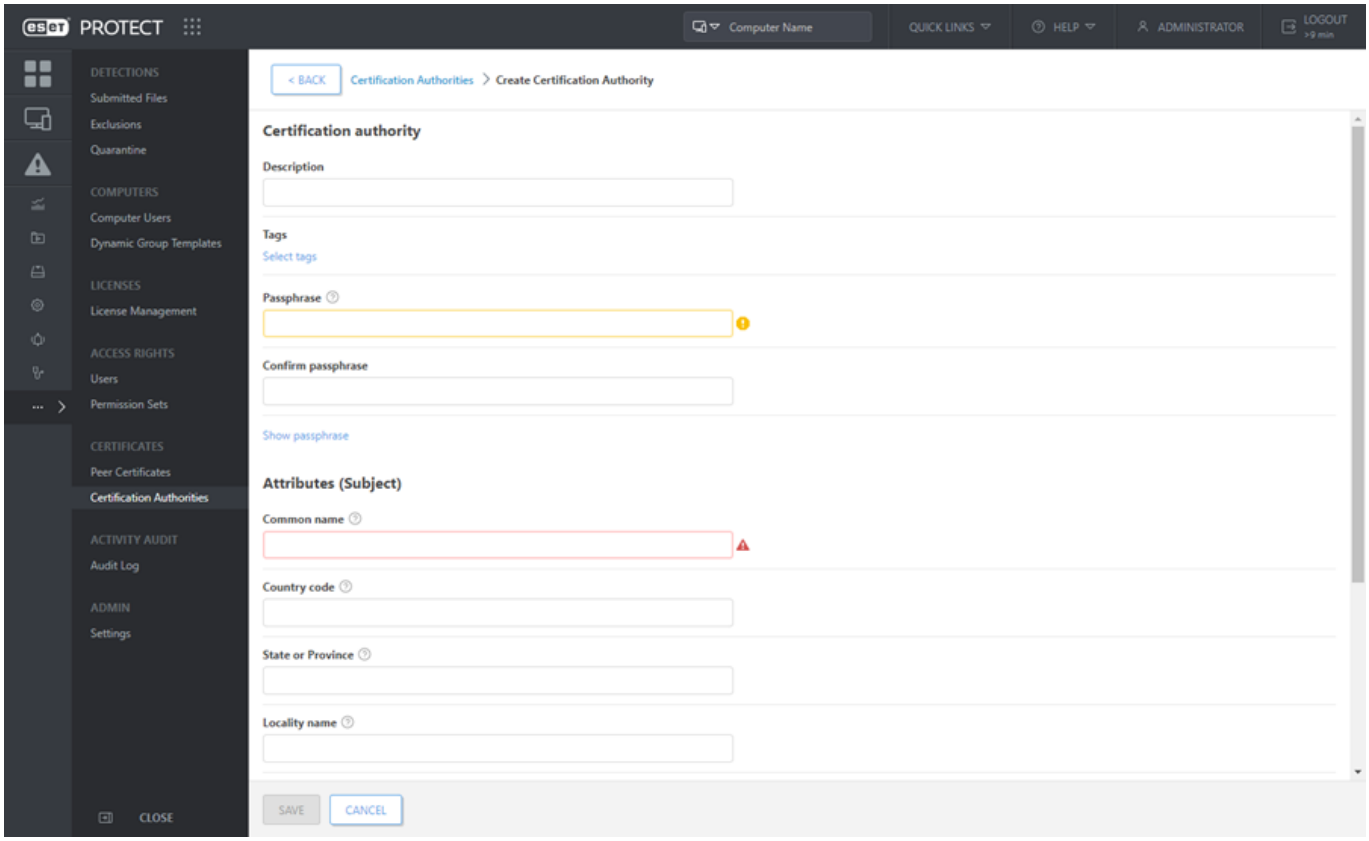
Atributos (assunto)

1.Insira um **Nome comum** (nome) da Autoridade de Certificação. Selecione um nome único para diferenciar várias Autoridades de certificação. Opcionalmente, é possível inserir informações de descrição sobre a Autoridade de certificação.

2.Insira os valores **Válido de** e **Válido até** para ter certeza de que o certificado é válido.

Para todos os Certificados e Autoridades de Certificação criados durante a instalação dos componentes ESET PROTECT, o valor Válido de é definido para 2 dias antes da criação do certificado.
Para todos os Certificados e Autoridades de Certificação criados no Console da Web ESET PROTECT, o valor Válido de é definido para 1 dia antes da criação do certificado. O motivo disso é cobrir todas as discrepâncias de tempo possíveis entre os sistemas afetados.
Por exemplo, uma Autoridade de certificação e Certificado criados em 12 de janeiro de 2017 durante a instalação terão um valor Válido de pré-definido como 10 de janeiro de 2017 00:00:00, e uma Autoridade de certificação e Certificado criados em 12 de janeiro de 2017 no Console da Web ESET PROTECT terão o valor Válido de pré-definido de 11 de janeiro de 2017 00:00:00.

3.Clique em **Salvar** para salvar sua nova Autoridade de Certificação. Agora será listado na lista de Autoridade de Certificação sob **Mais** > **Autoridades de Certificação**, e está pronto para ser usado. A autoridade de certificação é criada no grupo inicial do usuário que a criou.



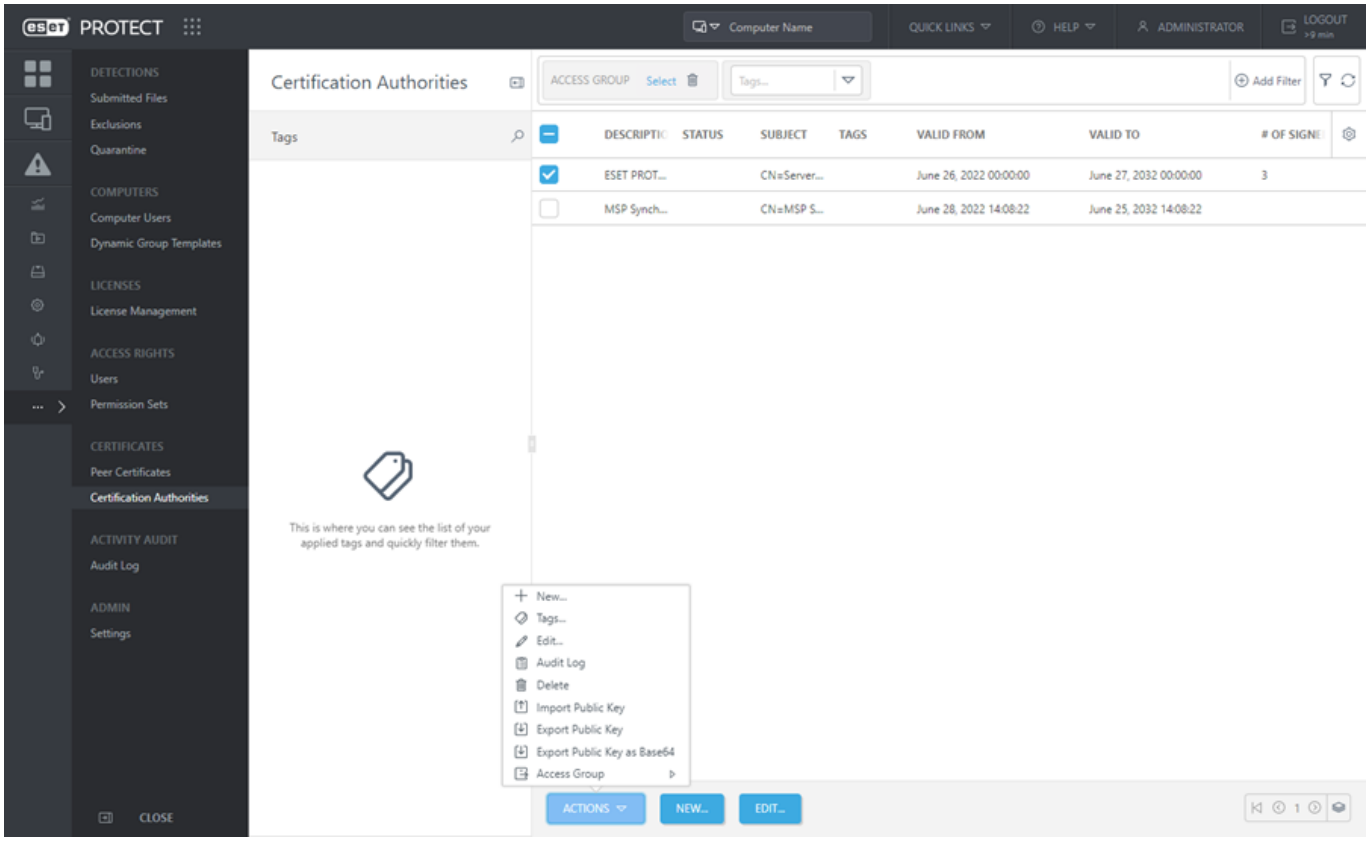
Para gerenciar a Autoridade de Certificação, marque a **caixa de seleção** ao lado de Autoridade de Certificação na lista e use o menu de contexto (clique com o botão esquerdo na Autoridade de Certificação) ou o botão **Ação** na parte inferior da página. As opções disponíveis são Importar chave pública e Exportar chave pública ou **Editar** a Autoridade de Certificação.

Exportar uma chave pública

Para exportar uma Autoridade de certificação, clique em **Mais** > **Autoridades de Certificação**.

> Para exportar uma chave pública, é preciso que o usuário tenha direitos de Uso sobre os Certificados. Veja a lista completa de direitos de acesso para obter mais informações.

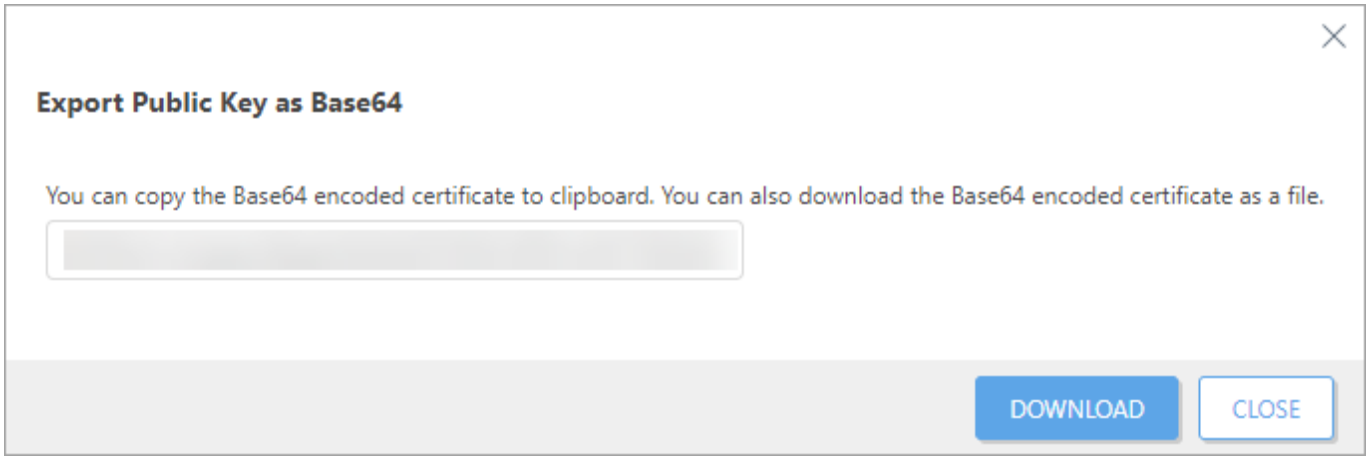
1. Selecione a Autoridade de Certificação que deseja usar a partir da lista e selecione a caixa de seleção ao lado dela.



2. Selecione uma das opções de exportação:

a.Selecione **Ações** > **Exportar chave pública**. Selecione esta opção se quiser importar a Chave pública para outra instalação do ESET PROTECT (migração de um servidor para outro). Digite um nome para a chave pública e clique em **Salvar**. A chave pública será exportada como um arquivo *.der*.

b.Selecione **Ações** > **Exportar chave pública como Base64**. Você pode copiar a string de certificado codificada do Base64 ou clicar em **Download** para fazer download do certificado codificado do Base64 como um arquivo.



Se você excluir a Autoridade de certificação ESET PROTECT padrão e criar uma nova, isto não irá funcionar. Antes de substituir a CA, você precisa criar e distribuir Certificados de mesmo nível assinados pela nova CA. Você também precisa alterar o certificado do Servidor nas **Mais** > Configurações e em seguida reiniciar o serviço do Servidor ESET PROTECT.

Importar uma chave pública

Para importar uma autoridade de certificação de terceiros, clique em **Mais** > **Autoridades de Certificação**.

1.Clique no botão **Ações** e selecione **Importar Chave Pública**.

2.**Escolher arquivo para carregar**: clique em **Navegar** e vá ao arquivo que você deseja importar. Você pode importar apenas um arquivo *.der*.

3.Insira uma **Descrição** para o certificado e clique em **Importar**. A Autoridade de Certificação foi importada com sucesso.

Relatório de auditoria

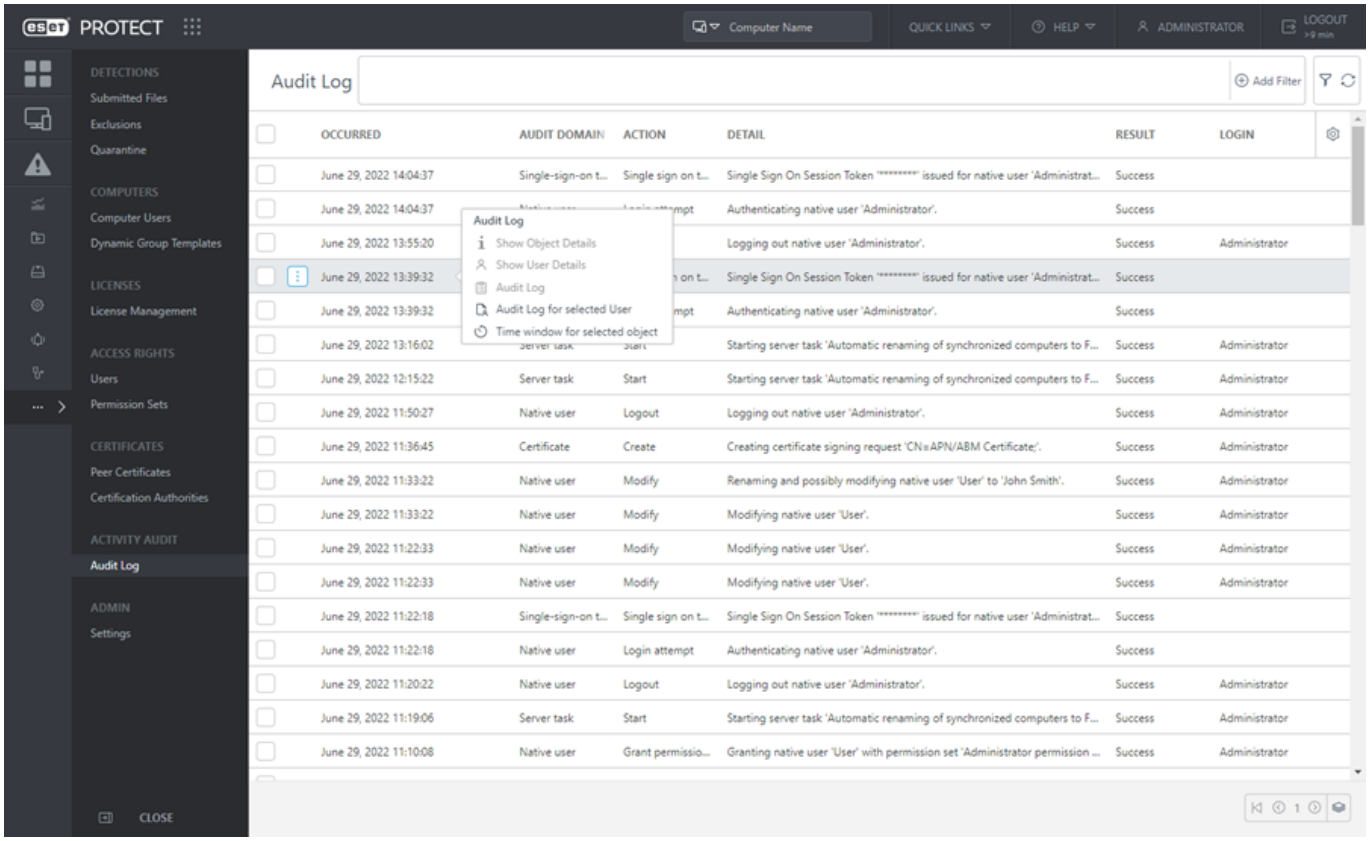
Quando um usuário realizar uma ação no Web Console ESET PROTECT, a ação será registrada. Os relatórios de auditoria serão criados se um objeto do Web Console ESET PROTECT (por exemplo: computador, política, detecção, etc.) for criado ou modificado.

O Relatório de auditoria é uma nova tela disponível no ESET PROTECT. O Relatório de auditoria contém as mesmas informações que o Relatório de auditoria, mas permite uma conveniente filtragem dos dados exibidos. Você também pode visualizar diretamente o relatório de auditoria filtrado para vários objetos do Web Console clicando no objeto do Web Console e selecionando **Relatório de auditoria**.

O Relatório de auditoria permite ao Administrador inspecionar as atividades realizadas no Web Console ESET PROTECT, especialmente se houver mais usuários do Web Console.

Para ver o Relatório de auditoria, o usuário do Web Console deve ter um conjunto de permissões com a funcionalidade ***Relatório de auditoria.

A permissão do Relatório de auditoria permite que o usuário veja as ações registradas de todos os outros usuários e domínios, mesmo aquelas relacionadas aos ativos que o usuário não tem direitos suficientes para visualizar.



Ao clicar em uma linha no Relatório de auditoria você pode realizar as ações a seguir:

Mostrar detalhes do objeto	Mostrar os detalhes do objeto auditado.
Mostrar detalhes do usuário	Mostrar detalhes do usuário que executou a ação no objeto.
Relatório de auditoria	Mostrar o Relatório de auditoria para o objeto selecionado.
Relatório de auditoria para o usuário selecionado	Mostrar o Relatório de auditoria para o usuário selecionado.
Janela de tempo para o objeto selecionado	Mostrar o Relatório de auditoria para o objeto selecionado com um filtro ativado de tempo de ocorrência.

Clique em **Adicionar filtro** para filtrar o modo de exibição da tabela por vários critérios:

- **<= Ocorreu** – define a data e hora antes da qual a ação ocorreu.
- **>= Ocorreu** – define a data e hora depois da qual a ação ocorreu.
- **Ação** – seleciona a ação realizada.
- **Domínio de auditoria** – seleciona o objeto modificado do Web Console.
- **Usuário da auditoria** – seleciona o usuário do Web Console que realizou a ação.
- **Resultado** – seleciona o resultado da ação.

Configurações

Nesta seção, você pode definir configurações específicas do próprio Servidor ESET PROTECT. Essas configurações são similares às Políticas, mas são aplicadas diretamente no Servidor ESET PROTECT.

Conexão

Porta do servidor (requer reinicialização) – Essa é a porta para a conexão entre o Servidor ESET PROTECT e o(s) Agente(s). Alterar essa opção exigirá a reinicialização do Serviço do Servidor ESET PROTECT para que a alteração seja implementada. Para alterar a porta pode ser necessário realizar alterações nas configurações de firewall.

Porta do console web (requer reinicialização) – Porta para a conexão entre o Console web ESET PROTECT e o Servidor ESET PROTECT. Para alterar a porta pode ser necessário realizar alterações nas configurações de firewall.

Segurança avançada (requer reinicialização!) – Essa configuração ativa a segurança avançada de uma comunicação de rede de componentes ESET PROTECT.

Certificado (requer reinicialização) – Aqui você pode gerenciar certificados do Servidor ESET PROTECT. Clique em Alterar certificado e selecione qual certificado do Servidor ESET PROTECT deve ser usado pelo servidor ESET PROTECT. Para obter mais informações consulte Certificados de mesmo nível.

Essas mudanças exigem uma reinicialização do serviço ESET PROTECT Server. Visite nosso artigo da Base de conhecimento para instruções.

Atualizações

Intervalo de atualização - intervalo no qual as atualizações serão recebidas. Você pode selecionar um Intervalo regular e definir as configurações ou usar uma expressão CRON.

Servidor de atualização – servidor de atualização do qual o Servidor ESET PROTECT recebe atualizações de versões de produtos ESET e componentes ESET PROTECT. Para atualizar o ESET PROTECT 10.0 de uma imagem (Ferramenta de imagem), defina o endereço completo da pasta de atualização `era6` (de acordo com a localização raiz do seu servidor HTTP). Por exemplo:

```
http://your_server_address/mirror/eset_upd/era6
```

Tipo de atualização - selecione o tipo de atualizações do módulo do Servidor ESET PROTECT que deseja receber. Você pode encontrar a versão atual dos módulos do Servidor ESET PROTECT instalado em **Ajuda** > **Sobre**.

Atualização regular	O download das atualizações do módulo do Servidor ESET PROTECT será feito automaticamente do servidor ESET com o menor tráfego de rede. Configuração padrão.
Atualização teste	Essas atualizações passaram pelo teste interno e estarão disponíveis em breve para o público em geral. Você pode se beneficiar de ativar as atualizações de teste ao obter acesso às atualizações mais recentes dos módulos do Servidor ESET PROTECT. Atualizações de teste podem ajudar a resolver um problema com o Servidor ESET PROTECT em alguns casos. Porém, as atualizações de pré-lançamento podem não ser estáveis o bastante a todos os momentos e não devem ser usadas em servidores de produção onde é preciso ter o máximo de disponibilidade e estabilidade. Atualizações de teste estão disponíveis apenas com AUTOSELECT definido no parâmetro do **Servidor de atualização**.

Configurações avançadas

Proxy HTTP - Use um servidor proxy para facilitar o tráfego na internet de clientes da sua rede. Se você instalar o ESET PROTECT usando o Instalador tudo-em-um, o proxy HTTP está ativado por padrão. Configurações de Proxy HTTP não são aplicadas para comunicação com servidores de Autenticação Segura (2FA).

Chamada para despertar – O Servidor ESET PROTECT pode executar uma replicação instantânea do Agente ESET Management em uma máquina via EPNS. Isso é útil quando você não quer aguardar o intervalo regular quando o Agente ESET Management se conecta ao Servidor ESET PROTECT. Por exemplo, quando quiser que uma Tarefa seja executada imediatamente em clientes ou se quiser que uma Política seja aplicada já.

Wake on LAN - Configure os **Endereços Multicast** se quiser enviar chamadas Wake on LAN para um ou mais endereço IP.

Servidor SMTP – Usa um Servidor SMTP para deixar o Servidor ESET PROTECT enviar mensagens de e-mail (por exemplo, e-mails de notificação ou relatórios). Especifique detalhes de seu servidor SMTP.

Active Directory – Você pode predefinir suas configurações do AD. O ESET PROTECT usa suas credencias por padrão nas tarefas de sincronização do Active Directory (sincronização do usuário, sincronização de grupo estático). Quando os campos relacionados são deixados em branco na configuração de tarefas, o ESET PROTECT usa as credenciais predefinidas. Use um usuário AD somente leitura, o ESET PROTECT não faz qualquer alteração na estrutura AD.

Se você estiver executando o Servidor ESET PROTECT no Linux (ou máquina virtual), precisará ter um arquivo de configuração *Kerberos* configurado corretamente. Você pode configurar o *Kerberos* para sincronizar com vários domínios.

Se o Servidor ESET PROTECT estiver sendo executado em uma máquina Windows conectada a um domínio, apenas o **Host** arquivado é necessário. A sincronização entre mais domínios é possível se os domínios tiverem estabelecido confiança entre eles.

- **Host** - Digite o nome do servidor ou endereço IP do seu controlador de domínio.
- **Nome de usuário** - Digite o nome de usuário para seu controlador de domínio no formato a seguir:
  - `DOMAIN\username` (Servidor ESET PROTECT em execução no Windows)
  - `username@FULL.DOMAIN.NAME` ou `username` (Servidor ESET PROTECT em execução no Linux).

> Não se esqueça de digitar o domínio em letras maiúsculas. Esta formatação é necessária para fazer a autenticação adequada de consultas no servidor do Active Directory.

- **Senha** - Digite a senha usada para fazer login no seu controlador de domínio.
- **Container de raiz** - Digite o identificador completo de um container AD, por exemplo: `CN=John,CN=Users,DC=Corp`. Ela age como um **Nome diferenciado** predeterminado. Recomendamos que você copie e cole este valor de uma tarefa do servidor para ter certeza de que você tem o valor correto (copie o valor do campo **Nome diferenciado**, quando ele estiver selecionado).

O Servidor ESET PROTECT no Windows usa o protocolo LDAPS criptografado (LDAP sobre SSL) por padrão para todas as conexões com o Active Directory (AD). Você também pode Configurar LDAPS na máquina virtual ESET PROTECT.
Para uma conexão AD bem-sucedida no LDAPS, configure o seguinte:
1. O controlador de domínio deve ter um certificado de máquina instalado. Para emitir um certificado para seu controlador de domínio, siga as etapas abaixo:
a)Abra o **Gerenciador de servidor**, clique em **Gerenciar** > **Adicionar funções e recursos** e instale os **Serviços de certificados do Active Directory** > **Autoridade de certificação**. Uma nova Autoridade de certificação será criada em **Autoridades de certificação raiz confiáveis**.
b)Navegue até **Início** > digite `certmgr.msc` e pressione **Enter** para executar o snap-in do Console de Gerenciamento da Microsoft **Certificados** > **Certificados – computador local** > **Pessoal** > clique com o botão direito na janela vazia > **Todas as tarefas** > **Solicitar novo certificado** > função **Inscrever controlador de domínio**.
c)Verifique se o certificado emitido contém o FQDN do controlador de domínio.
d)No seu servidor ESMC, importe a CA gerada para o depósito de certificados (usando a ferramenta `certmgr.msc`) para a pasta de CAs confiáveis.

2. Ao fornecer as configurações de conexão ao servidor AD, digite o FQDN do controlador de domínio (conforme fornecido no certificado do controlador de domínio) no campo **Servidor** ou **Host**. O endereço IP não é mais suficiente para o LDAPS.
Para ativar o fallback para o protocolo LDAP, selecione a caixa de seleção **Usar LDAP em vez do Active Directory** na tarefa de Sincronização de grupo estático ou Sincronização de usuário.

Servidor syslog - Você pode ter o ESET PROTECT enviando notificações e mensagens de evento para seu Servidor Syslog. Além disso, exportar relatórios de um produto ESET do computador cliente e enviá-los ao servidor Syslog.

Grupos estáticos - Ativa o pareamento automático de computadores encontrados aos computadores já presentes em grupos estáticos. O pareamento funciona no nome de host reportado pelo Agente ESET Management e, se não for possível confiar nele, ele deve ser desativado. Se o pareamento falhar um computador será colocado no grupo Achados e perdidos.

Repositório - local do repositório no qual todos os arquivos de instalação são armazenados.

- O repositório padrão da ESET é definido como **AUTOSELECT** (ele aponta para: *http://repository.eset.com/v1*). Ele determina automaticamente o servidor do repositório com a melhor conexão, baseado na localização geográfica (endereço IP) do Servidor ESET PROTECT (usando CDN - Rede de fornecimento de conteúdo). Portanto, não é preciso alterar as configurações de repositório.
- Opcionalmente, você pode configurar um repositório que use apenas os servidores ESET: *http://repositorynocdn.eset.com/v1*
- Nunca use um endereço IP para acessar o repositório ESET.
- Você pode criar e usar um repositório off-line.

Participar do programa de melhoria do produto – ative ou desative o envio de relatórios de travamento se você não concordar em 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).

Registro em relatório > **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).

Os relatórios mais recentes do Servidor ESET PROTECT podem ser encontrados aqui:

- Windows: *C:\ProgramData\ESET\RemoteAdministrator\Server\EraServerApplicationData\Logs*

- Linux: */var/log/eset/RemoteAdministrator/Server/*

Você pode configurar a exportação de relatórios para o Syslog aqui.

Limpeza de banco de dados - para impedir a sobrecarga de um banco de dados, você pode usar essa opção para limpar relatórios regularmente. A limpeza de banco de dados exclui esses tipos de relatórios: Relatórios do SysInspector, relatórios de diagnóstico, relatórios que não são mais coletados (relatórios de dispositivos removidos, relatórios de modelos de relatório removidos). O processo de limpeza do banco de dados é executado toda meia-noite por padrão. Alterações nessa configuração vão ter efeito depois da próxima limpeza. É possível configurar o intervalo de limpeza para cada um desses tipos de relatórios:

Tipo de log	Exemplo de tipo de relatório
Relatórios de detecção	• Antivírus • Arquivos bloqueados • ESET Inspect Alertas: • Firewall • HIPS • Proteção da web (sites filtrados)
Relatórios de gerenciamento	• Tarefas • Acionadores • Configuração exportada • Inscrição
Relatórios de auditoria	• Relatório de auditoria e relatório do Relatório de auditoria.
Relatórios de monitoramento	• Controle de dispositivos • Controle de Web • Usuários conectados

Os relatórios de diagnóstico são limpos todos os dias. O usuário não pode alterar o intervalo de limpeza.

Durante a limpeza do banco de dados, os itens em Detecções correspondentes aos relatórios de Incidentes limpos também são removidos (independentemente do status da detecção). Por padrão, o período de limpeza para relatórios de Incidente (e Detecções) está definido para 6 meses. Você pode alterar o intervalo em **Mais** > Configurações.

Personalização

Personalizar interface do usuário – você pode adicionar um logotipo personalizado ao Web Console ESET PROTECT, os relatórios gerados através da Tarefa do servidor e notificações por e-mail.

	Web Console	Relatórios	Notificações
Nenhuma	Design básico, sem logotipo personalizado	Logotipo ESET PROTECT no lado esquerdo do rodapé.	Logotipo ESET PROTECT no lado esquerdo do cabeçalho.
Co-branding	Logotipo personalizado para o Web Console	Um logotipo personalizado no rodapé do relatório – o logotipo ESET PROTECT está na esquerda e seu logotipo na direita.	Um logotipo personalizado no cabeçalho de notificação – o logotipo ESET PROTECT está na esquerda e seu logotipo na direita.
Rotulação com permissão (requer licença MSP)	Logotipo personalizado para o Web Console	Um logotipo personalizado no rodapé do relatório – sem logotipo ESET PROTECT, apenas seu logotipo na esquerda.	Um logotipo personalizado no cabeçalho de notificação – no lado esquerdo. Ao lado dele, está **Powered by ESET PROTECT**.

Logotipo da empresa

- **Logotipo de segundo plano escuro** (cabeçalho do Console da Web) - Este logotipo será exibido no canto superior esquerdo do Console da Web.

- **Logotipo claro de segundo plano** – esse logotipo será exibido no cabeçalho (para proprietários de licença MSP) ou rodapé (configuração de co-branding) dos relatórios gerados através da Tarefa do servidor e no cabeçalho de notificações por e-mail.

Clique em  para selecionar um logo. Clique em  para fazer o download do logotipo atual. Clique em  para remover o logotipo atual.

Relatórios e notificações

- **Personalizar relatórios** – Ative essa opção para usar o logotipo selecionado nos relatórios e/ou para adicionar um texto de rodapé.

- **Texto de rodapé do relatório** – Digite o texto que será adicionado no canto inferior direito dos relatórios gerados no formato PDF.

Um logo personalizado não pode ser usado junto com o texto de rodapé personalizado. O logotipo tem a mesma posição que o texto do rodapé. Se o logotipo e o rodapé forem usados simultaneamente, apenas o logotipo será visível. Ao usar a configuração **Colocação na lista de permissões**, o logotipo personalizado vai aparecer no canto superior esquerdo de um relatório, um logotipo menor **powered by ESET** será colocado no canto inferior direito, no lugar do texto do rodapé.

Segurança avançada

A segurança avançada inclui uma comunicação de rede segura entre os componentes ESET PROTECT:

- Certificados recém criados e autoridades de certificação vão usar SHA-256 (em vez de SHA-1).

- O servidor ESET PROTECT usa a maior segurança possível (TLS 1.3 ou 1.2) para comunicação com agentes, Syslog e comunicação SMTP.

- Usuários MDM: O Servidor ESET PROTECT usa TLS 1.2 para comunicação com o servidor MDM. A comunicação entre o servidor MDM e os dispositivos móveis não é afetada.

A segurança avançada funciona com todos os sistemas operacionais compatíveis:

- Windows

- Linux – Recomendamos que você **use a versão mais recente do OpenSSL1.1.1**. O Servidor/gerenciamento de dispositivo móvel ESET PROTECT não são compatíveis com o OpenSSL 3.x. 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`

- macOS

A segurança avançada está ativada por padrão em todas as novas instalações do ESET PROTECT 8.1 e versões posteriores.
Se você usar o ESMC ou ESET PROTECT 8.0 com a Segurança avançada desativada e atualizar para o ESET PROTECT e 8.1 e versões posteriores, a Segurança avançada permanecerá desativada. Recomendamos que você ative seguindo as etapas abaixo.

Ativar e aplicar a Segurança avançada na sua rede

- Quando você ativa a segurança avançada, precisa reiniciar o servidor ESET PROTECT para começar a usar o recurso.
- A segurança avançada não influencia as Autoridades de certificação (CAs) e certificados existentes. A segurança avançada inclui apenas os novos CAs e certificados criados depois que a segurança avançada é ativada. Para aplicar a segurança avançada na infraestrutura ESET PROTECT atual, é preciso substituir os certificados existentes.
- Se você quiser usar a Segurança avançada, é altamente recomendável configurá-la **antes** de importar a conta MSP.

1. Clique em **Mais** > **Configurações** > **Conexão** e clique na alternância ao lado de **Segurança avançada (requer reinicialização!)**.
2. Clique em **Salvar** para aplicar a configuração.
3. Feche o console e reinicie o serviço do Servidor ESET PROTECT.
4. Aguarde alguns minutos depois do início do serviço e entre no console da Web.
5. Verifique se todos os computadores ainda estão se conectando e se nenhum outro problema aconteceu.
6. Clique em **Mais** > **Autoridades de Certificação Novo** e criar nova CA. O novo CA é enviado automaticamente para todos os computadores cliente durante a próxima conexão Agente - Servidor.
7. Criar novos certificados de mesmo nível assinados com esse mesmo CA. Criar um certificado para Agente ou Servidor (você pode selecionar no menu suspenso **Produto** no assistente).
8. Altere seu certificado de Servidor ESET PROTECT atual para um novo.
9. Criar uma nova política de Agente ESET Management para configurar seus Agentes para usarem o novo certificado de Agente.
a.Na seção **Conexão**, clique em **Certificado** > **Abrir lista de certificados** e selecione o novo certificado de mesmo nível.
b.Atribuir a política a computadores onde você quer usar a Segurança avançada.
c.Clique em **Concluir**.
10. Quando todos os dispositivos estiverem se conectando ao novo certificado, você pode excluir seu CA antigo e revogar os certificados antigos.

Não exclua seu CA antigo ou revogue certificados antigos se você tiver aplicado a Segurança avançada em apenas alguns (e não em todos) computadores cliente conectados.

Para aplicar a segurança avançada ao componente Mobile Device Management (MDM), crie um novo MDM e certificados de proxy assinados pela nova CA e atribua-os através de uma política para o servidor MDM da seguinte forma:
- Clique em Política do ESET Mobile Device Connector > **Geral** > Certificado HTTPS. Importar o novo certificado MDM.
- Clique em Política do ESET Mobile Device Connector > **Conexão** > **Certificado** = Certificado de proxy.

Servidor SMTP

O ESET PROTECT pode enviar automaticamente relatórios de email e notificação. Ative **Usar Servidor SMTP**, clique em **Mais** > **Configurações** > **Configurações avançadas** > **Servidor SMTP** e especifique o seguinte:

- **Host** - Nome de host ou endereço IP do seu servidor SMTP.
- **Porta –** O SMTP usa a porta 25 por padrão, mas você pode alterá-la caso seu servidor SMTP use uma porta diferente.
- **Nome de usuário** - Se o seu servidor SMTP precisar de autenticação, especifique o nome da conta do usuário SMTP (não inclua o domínio, pois isso não vai funcionar).
- **Senha** - A senha associada à conta de usuário SMTP.
- **Tipo de conexão de segurança** - Especifica o tipo de conexão, o padrão é **Não protegido**, mas se o seu servidor SMTP permite conexões seguras, escolha TLS ou STARTTLS. Se você quiser tornar sua conexão mais segura, use uma extensão STARTTLS ou SSL/TLS, pois elas usam uma porta separada para a comunicação criptografada.
- **Tipo de autenticação** – o padrão está definido como **Sem autenticação**. Porém, você pode selecionar o Tipo de autenticação apropriado na lista suspensa (por exemplo, Login, CRAM-MD5, CRAM-SHA1, SCRAM-SHA1, NTLM ou Automática)
- **Endereço do remetente** - Especifica o endereço do remetente que será exibido no cabeçalho dos emails de notificação (De:)
- **Testar servidor SMTP** – Isto é feito para garantir que as configurações SMTP estão corretas. Clique em **Enviar e-mail de teste** para abrir uma nova janela. Insira o endereço de e-mail do destinatário e a mensagem de e-mail de teste que será enviada através do servidor SMTP para este endereço. Verifique a caixa de entrada do destinatário para verificar se o e-mail de teste foi entregue.

Computadores pareados encontrados automaticamente

Se houver uma ocorrência de várias instâncias do mesmo computador em ESET PROTECT (por exemplo, se o Agente ESET Management for reinstalado em um computador cliente que já é gerenciado), o recurso **Parear automaticamente computadores encontrados** cuida disso e pareia essas instâncias em uma. Isso deve eliminar a necessidade de verificação manual e classificação dos computadores encontrados.

O pareamento funciona no nome de host reportado pelo Agente ESET Management e, se não for possível confiar nele, recomendamos que você desative **Parear automaticamente computadores encontrados**. Se o pareamento falhar um computador será colocado no grupo **Achados e perdidos**. A ideia é que sempre que um Agente ESET Management for reinstalado em um computador já gerenciado, ele seria pareado automaticamente e, assim, colocados corretamente no ESET PROTECT sem sua intervenção. Além disso, o novo Agente ESET Management irá obter imediatamente suas políticas e tarefas.

- Quando **desativado**, os computadores que devem ser colocados no grupo **Perdido e encontrado** serão pareados com o primeiro computador não gerenciado encontrado (espaço reservado, ícone do círculo)

localizado em qualquer lugar na árvore ESET PROTECT. Se não existir nenhum espaço reservado com o mesmo nome, o computador será colocado em Perdido e encontrado.

• Quando **ativado (padrão)**, computadores que devem ser colocados no **Perdido e encontrado** serão pareados com o primeiro computador não gerenciado encontrado (espaço reservado, ícone do círculo) localizado em qualquer lugar na árvore ESET PROTECT. Se não houver nenhum espaço reservado com o mesmo nome, o computador vai ser pareado com o primeiro computador gerenciado encontrado (ícone de alerta ou verificação) localizado em qualquer lugar na árvore ESET PROTECT. Se este pareamento também falhar, o computador será colocado em Perdido e encontrado.

Se você considerar o pareamento automático como indesejada, desative-o. Você sempre pode verificar e classificar computadores manualmente.

Exportar relatórios para Syslog

O ESET PROTECT pode exportar certos relatórios/eventos e enviá-los ao seu Servidor Syslog. Eventos das seguintes categorias de relatório estão sendo exportados para o servidor Syslog: Detecção, Firewall, HIPS, Auditoria e ESET Inspect. Eventos são gerados em qualquer computador cliente gerenciado executando o produto ESET (por exemplo, ESET Endpoint Security). Esses eventos podem ser processados por qualquer solução SIEM (Informações de Segurança e Gerenciamento de Eventos - Security Information and Event Management) capaz de importar eventos de um servidor Syslog. Os eventos são escritos no servidor Syslog pelo ESET PROTECT.

1.Para ativar o Servidor Syslog, clique em **Mais** > **Configurações** > **Configurações avançadas** > **Servidor Syslog** > **Usar servidor Syslog**.

2.Para ativar a exportação, clique em **Mais** > **Configurações** > **Configurações avançadas** > **Registro em relatório** > **Exportar relatórios para o Syslog**.

Todos os relatórios exportados estão disponíveis para usuários Syslog sem limitações. Todas as mensagens de relatório de auditoria são exportadas para o Syslog.

3.Escolha um dos seguintes formatos para mensagens de eventos:

- JSON (Notação de Objeto do JavaScript)
- LEEF (Formato de relatório de evento estendido) - formato usado pelo aplicativo QRadar da IBM.
- CEF (Formato de evento comum)

Para filtrar os relatórios de evento enviados para o Syslog, crie uma notificação de categoria de relatório com um filtro definido.

Servidor Syslog

Se você tiver um servidor Syslog sendo executado em sua rede, você pode Exportar relatórios para o Syslog para receber determinados eventos (Evento de detecção, Evento de Firewall agregado, Evento de HIPS agregado, etc.) de computadores cliente executando o ESET Endpoint Security. É possível configurar o ESET PROTECT para enviar Notificações ao seu servidor Syslog.

Para ativar o servidor Syslog:

1.Navegue até **Mais** > **Configurações** > **Configurações avançadas** > **Servidor syslog** e clique na alternância ao lado de **Usar servidor syslog**.

2.Especifique as configurações obrigatórias a seguir:

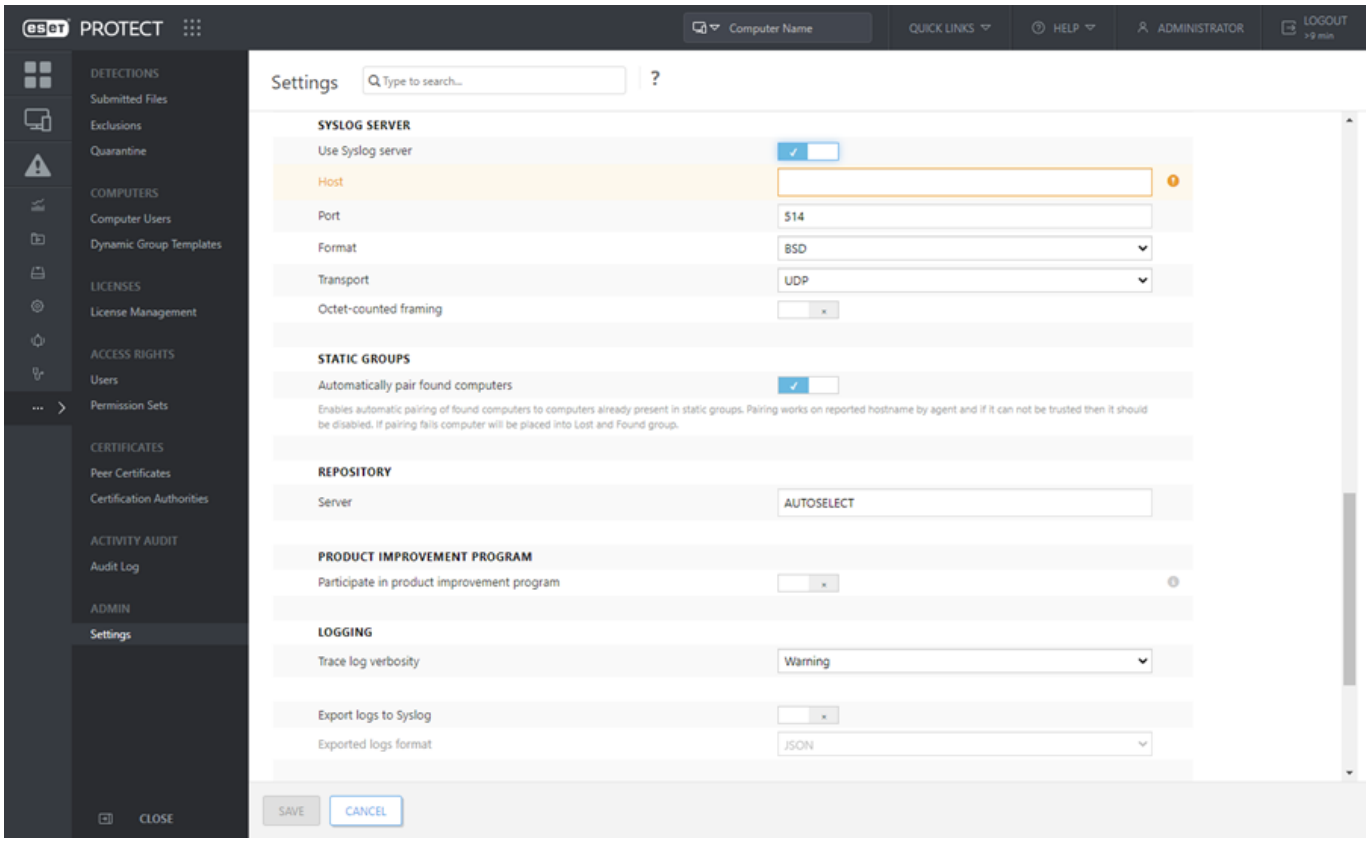
a.**Host** (endereço IP ou nome de host do destino para mensagens Syslog)

b.Número de **Porta** (o valor padrão é 514).

c.**Formato** do relatório: **BSD** (especificação), **Syslog** (especificação)

d.Protocolo de **transporte** para o envio de mensagens ao Syslog (**UDP**, **TCP**, **TLS**)

Depois de fazer alterações, clique em **Salvar**.



É feita uma gravação regular no arquivo de relatório do aplicativo. O syslog serve apenas como meio para exportar certos eventos assíncronos como notificações ou vários eventos do computador cliente.

Eventos exportados para o formato JSON

O JSON é um formato leve para troca de dados. É construído em uma coleção de pares de nome / valor e uma lista ordenada de valores.

Eventos exportados

Esta seção contém detalhes sobre o formato e significado de atributos de todos os eventos exportados. A mensagem de evento está na forma de um objeto JSON com algumas chaves obrigatórias e outras opcionais. Cada evento exportado vai ter a chave a seguir:

event_type	string		Tipo de eventos exportados: • Threat_Event (detecções de **Antivírus**) • FirewallAggregated_Event (detecções de **Firewall**) • HipsAggregated_Event (detecções de **HIPS**) • Audit_Event (Relatório de auditoria) • FilteredWebsites_Event (sites filtrados – **Proteção da web**) • EnterpriseInspectorAlert_Event (ESET Inspect Alertas) • BlockedFiles_Event (Arquivos bloqueados)
ipv4	string	opcional	Endereço IPv4 do computador gerando o evento.
ipv6	string	opcional	Endereço IPv6 do computador gerando o evento.
group_name	string		O grupo estático do computador gerando o evento.
source_uuid	string		UUID do computador gerando o evento.
occurred	string		Hora UTC de ocorrência do evento. O formato é %d-%b-%Y %H:%M:%S
severity	string		Gravidade do evento. Valores possíveis (do menos ao mais grave) são: `Informação`, `Aviso`, `Alerta`, `Erro`, `Crítico`, `Fatal`

Todos os tipos de evento listados abaixo com todos os níveis de gravidade são reportados ao servidor Syslog. Para filtrar os relatórios de evento enviados para o Syslog, crie uma notificação de categoria de relatório com um filtro definido.
Os valores reportados dependem do produto de segurança ESET (e sua versão) instalado no computador gerenciado, e o ESET PROTECT reporta apenas os dados recebidos. Portanto, a ESET não pode fornecer uma lista completa de todos os valores. Recomendamos observar sua rede e filtrar os relatórios com base nos valores recebidos.

Teclas personalizadas de acordo com o event_type:

Threat_Event

Todos os eventos de Detecção **Antivírus** gerados por endpoints gerenciados serão encaminhados para o Syslog. Chave de evento específica de Detecção:

threat_type	string	opcional	Tipo de detecção
threat_name	string	opcional	Nome da detecção
threat_flags	string	opcional	Sinalizadores de detecção relacionados
scanner_id	string	opcional	ID do Scanner
scan_id	string	opcional	ID de rastreamento
engine_version	string	opcional	Versão do mecanismo de escaneamento
object_type	string	opcional	Tipo de objeto relacionado a este evento
object_uri	string	opcional	URI do objeto
action_taken	string	opcional	Ação realizada pelo Endpoint
action_error	string	opcional	Mensagem de erro se a "ação" não for bem sucedida

threat_type	string	opcional	Tipo de detecção
threat_handled	bool	opcional	Indica se a detecção foi resolvida ou não
need_restart	bool	opcional	Indica se era necessário reiniciar ou não
username	string	opcional	Nome da conta de usuário associada ao evento
processname	string	opcional	Nome do processo associado ao evento
circumstances	string	opcional	Descrição breve do que causou o evento
hash	string	opcional	SHA1 hash do fluxo de dados (detecção).
firstseen	string	opcional	Data e hora de quando a detecção foi detectada pela primeira vez na máquina. O ESET PROTECT usa formatos de data-hora diferentes para o atributo firstseen (e qualquer outro atributo de data-hora) dependendo do formato de saída do relatório (JSON ou LEEF): • JSON formato:"%d-%b-%Y %H:%M:%S" • LEEF formato:"%b %d %Y %H:%M:%S"

Exemplo de relatório JSON Threat_Event:


```
Jun 21 11: 46: 40 030 - MG ERAServer[5648]: {
    "event_type": "Threat_Event",
    "ipv4": "192.168.30.30",
    "hostname": "030-mg",
    "group_name": "Lost & found",
    "source_uuid": "1361a9f6-1d45-4561-b33a-b5d6c62c71e0",
    "occured": "21-Jun-2021 09:46:15",
    "severity": "Warning",
    "threat_type": "Virus",
    "threat_name": "XF/Gydhex.A",
    "scanner_id": "Real-time file system protection",
    "scan_id": "virlog.dat",
    "engine_version": "23497 (20210621)",
    "object_type": "file",
    "object_uri": "file:///C:/Users/Administrator/Downloads/xls/YICT080714.xls",
    "action_taken": "Deleted",
    "threat_handled": true,
    "need_restart": false,
    "username": "030-MG\\Administrator",
    "processname": "C:\\Program Files\\WinRAR\\WinRAR.exe",
```

```
    "circumstances": "Event occurred on a newly created file.",
    "firstseen": "21-Jun-2021 09:46:14",
    "hash": "5B97884A45C6C05F93B22C4059F3D9189E88E8B7"
}
```


FirewallAggregated_Event

Relatórios de evento gerados pelo Firewall da ESET (detecções de **Firewall**) são agregados pelo Agente ESET Management gerente, para evitar o desperdício de banda durante Agente ESET Management/ ESET PROTECT. Servidor replicação. Chave de evento específico de Firewall:

event	string	opcional	Nome do evento
source_address	string	opcional	Endereço da origem do evento
source_address_type	string	opcional	Tipo de endereço da origem do evento
source_port	número	opcional	Porta de origem do evento
target_address	string	opcional	Endereço do destino do evento
target_address_type	string	opcional	Tipo de endereço do destino do evento
target_port	número	opcional	Porta de destino do evento
protocol	string	opcional	Protocolo
account	string	opcional	Nome da conta de usuário associada ao evento
process_name	string	opcional	Nome do processo associado ao evento
rule_name	string	opcional	Nome da regra
rule_id	string	opcional	ID de regra
inbound	bool	opcional	Indica se a conexão era de entrada ou não
threat_name	string	opcional	Nome da detecção
aggregate_count	número	opcional	Quantas mensagens exatamente iguais foram geradas pelo endpoint entre duas replicações consecutivas entre o ESET PROTECT Servidor e gerenciamento do Agente ESET Management
action	string	opcional	Ação realizada
handled	string	opcional	Indica se a detecção foi resolvida ou não

Exemplo de relatório JSON FirewallAggregated_Event:


```
Jun 21 3: 54: 07 030 - MG ERAServer[5648]: {
 "event_type": "FirewallAggregated_Event",
 "ipv4": "192.168.30.30",
 "hostname": "w16test",
     "group_name": "Lost & found",
 "source_uuid": "d9477661-8fa4-4144-b8d4-e37b983bcd69",
```

```
 "occured": "21-Jun-2021 13:10:04",

 "severity": ""Warning",

 "event": "Security vulnerability exploitation attempt",

 "source_address": "127.0.0.1",

 "source_address_type": "IPv4",

 "source_port": 54568,

 "target_address": "127.0.0.1",

 "target_address_type": "IPv4",

 "target_port": 80,

 "protocol": "TCP",

 "account": "NT AUTHORITY\\NETWORK SERVICE",

 "process_name": "C:\\Program Files\\Apache Software Foundation\\apache-
tomcat-9.0.41\\bin\\tomcat9.exe",

 "inbound": true,

 "threat_name": "CVE-2017-5638.Struts2",

 "aggregate_count": 1

}
```


HIPSAggregated_Event

Eventos do Sistema de Prevenção de intruso Baseado em Host (detecções de **HIPS**) são filtrados por **gravidade** antes de serem enviados como mensagens Syslog. Os atributos específicos HIPS são os seguintes:

application	string	opcional	Nome do aplicativo
operation	string	opcional	Operação
target	string	opcional	Destino
action	string	opcional	Ação realizada
action_taken	string	opcional	Ação realizada pelo Endpoint
rule_name	string	opcional	Nome da regra
rule_id	string	opcional	ID de regra
aggregate_count	número	opcional	Quantas mensagens exatamente iguais foram geradas pelo endpoint entre duas replicações consecutivas entre o ESET PROTECT Servidor e gerenciamento do Agente ESET Management
handled	string	opcional	Indica se a detecção foi resolvida ou não

Exemplo de relatório JSON HipsAggregated_Event:


```
Jun 21 13: 54: 07 030 - MG ERAServer[5648]: {
```

```
    "event_type": "HipsAggregated_Event",
    "ipv4": "192.168.30.181",
    "hostname": "test-w10-uefi",
    "group_name": "Lost & found",
    "source_uuid": "5dbe31ae-4ca7-4e8c-972f-15c197d12474",
    "occured": "21-Jun-2021 11:53:21",
    "severity": "Critical",
    "application": "C:\\Users\\Administrator\\Desktop\\es_pack_to_test\\test\\java.exe",
    "operation": "Attempt to run a suspicious object",
    "target": "C:\\Users\\Administrator\\Desktop\\es_pack_to_test\\test\\trojan.exe",
    "action": "blocked",
    "handled": true,
    "rule_id": "Suspicious attempt to launch an application",
    "aggregate_count": 2
}
```


Audit_Event

O ESET PROTECT encaminha as mensagem de relatório de auditoria internas para o Syslog. Os atributos específicos são os seguintes:

domain	string	opcional	Domínio de relatório de auditoria
action	string	opcional	Ação sendo realizada
target	string	opcional	Ação de destino no qual está operando
detail	string	opcional	Descrição detalhada da ação
user	string	opcional	Usuário de segurança envolvido
result	string	opcional	Resultado da ação

Exemplo de relatório Audit_Event:


```
Jun 21 11: 42: 00 030 - MG ERAServer[5648]: {
    "event_type": "Audit_Event",
    "ipv4": "192.168.30.30",
    "hostname": "030-MG",
```

```
    "group_name": "Lost & found",
    "source_uuid": "72cdf05f-f9c8-49cc-863d-c6b3059a9e8e",
    "occured": "21-Jun-2021 09:42:00",
    "severity": "Information",
    "domain": "Native user",
    "action": "Login attempt",
    "target": "Administrator",
    "detail": "Authenticating native user 'Administrator'.",
    "user": "",
    "result": "Success"
}
```


FilteredWebsites_Event

O ESET PROTECT encaminha os sites filtrados (detecções da **Proteção da web**) para o Syslog. Os atributos específicos são os seguintes:

hostname	string	opcional	Nome de host do computador com o evento
processname	string	opcional	Nome do processo associado ao evento
username	string	opcional	Nome da conta de usuário associada ao evento
hash	string	opcional	Hashs SHA1 do objeto filtrado
event	string	opcional	Tipo do evento
rule_id	string	opcional	ID de regra
action_taken	string	opcional	Ação realizada
scanner_id	string	opcional	ID do Scanner
object_uri	string	opcional	URI do objeto
target_address	string	opcional	Endereço do destino do evento
target_address_type	string	opcional	Tipo de endereço do destino do evento (25769803777 = IPv4; 25769803778 = IPv6)
handled	string	opcional	Indica se a detecção foi resolvida ou não

Exemplo de relatório JSON FilteredWebsites_Event:


```
Jun 21 3: 56: 03 020 - MG ERAServer[5648]: {
 "event_type": "FilteredWebsites_Event",
 "ipv4": "192.168.30.30",
 "hostname": "win-test",
```

```
    "group_name": "Lost & found",
 "source_uuid": "d9477661-8fa4-4144-b8d4-e37b983bcd69",
 "occured": "21-Jun-2021 03:56:20",
 "severity": "Warning",
 "event": "An attempt to connect to URL",
 "target_address": "192.255.255.255",
 "target_address_type": "IPv4",
 "scanner_id": "HTTP filter",
 "action_taken": "blocked",        "object_uri": "https://test.com",
 "hash": "ABCDAA625E6961037B8904E113FD0C232A7D0EDC",
 "username": "WIN-TEST\\Administrator",
 "processname": "C:\\Program Files\\Web browser\\brwser.exe",
 "rule_id": "Blocked by PUA blacklist"
}
```


EnterpriseInspectorAlert_Event

O ESET PROTECT encaminha os alarmes ESET Inspect para o syslog. Os atributos específicos são os seguintes:

processname	string	opcional	Nome do processo causando esse alarme
username	string	opcional	Proprietário do processo
rulename	string	opcional	Nome da regra acionando este alarme
count	número	opcional	Número de alertas desse tipo gerados desde o último alarme
hash	string	opcional	Hash SHA1 do alarme
eiconsolelink	string	opcional	Link para o alarme no console ESET Inspect
eialarmid	string	opcional	ID da subparte do link de alarme ($1 no ^http.*/alarm/([0-9]+)$)
computer_severity_score	número	opcional	Pontuação de gravidade do computador
severity_score	número	opcional	Pontuação de gravidade da regra

Exemplo de relatório JSON EnterpriseInspectorAlert_Event:


```
Jun 16 16:19:00 Win2016Std ERAServer[2772]: {
 "event_type": "EnterpriseInspectorAlert_Event",
 "ipv4": "192.168.30.30",
 "hostname": "shdsolec.vddjc",
    "group_name": "Lost & found",
```

```
 "source_uuid": "csd77ad2-2453-42f4-80a4-d86dfa9d0543",
 "occured": "13-Jun-2021 07:45:00",
 "severity": "Warning",
 "processname": "ProcessName",
 "username": "UserName",
 "rulename": "RuleName2",
 "count": 158,
 "eiconsolelink": "http://eiserver.tmp/linkToConsole",
 "computer_severity_score": "1",
 "severity_score": "1"
}
```


BlockedFiles_Event

O ESET PROTECT encaminha os arquivos bloqueados ESET Inspect ao Syslog. Os atributos específicos são os seguintes:

hostname	string	opcional	Nome de host do computador com o evento
processname	string	opcional	Nome do processo associado ao evento
username	string	opcional	Nome da conta de usuário associada ao evento
hash	string	opcional	Hash SHA1 do arquivo bloqueado
object_uri	string	opcional	URI do objeto
action	string	opcional	Ação realizada
firstseen	string	opcional	Hora e data em que a detecção foi encontrada pela primeira vez na máquina (formato de data e hora).
cause	string	opcional	
description	string	opcional	Descrição do arquivo bloqueado
handled	string	opcional	Indica se a detecção foi resolvida ou não

Eventos exportados para o formato LEEF

Para filtrar os relatórios de evento enviados para o Syslog, crie uma notificação de categoria de relatório com um filtro definido.

O formato LEEF é um formato de evento personalizado para o IBM® Security QRadar®. Os eventos têm atributos personalizados e padrão:

- o ESET PROTECT usa alguns dos atributos padrões descritos na documentação oficial da IBM.
- Atributos personalizados são os mesmos que no formato JSON. O atributo deviceGroupName contém o grupo estático do computador gerando o evento.

Categorias de evento:

- Detecções de antivírus
- Firewall
- Sites filtrados – Proteção da web
- HIPS
- Auditoria
- ESET Inspect Alertas
- Arquivos bloqueados

Você pode encontrar mais informações sobre o Log Event Extended Format (LEEF) no site oficial da IBM.

Eventos exportados para o formato CEF

Para filtrar os relatórios de evento enviados para o Syslog, crie uma notificação de categoria de relatório com um filtro definido.

CEF é um formato de relatório baseado em texto desenvolvido por ArcSight™. O formato CEF inclui um cabeçalho CEF e uma extensão CEF. A extensão contém uma lista de pares de valor de chave.

Cabeçalho CEF

Cabeçalho	Exemplo	Descrição
Device Vendor	ESET	
Device Product	Protect	
Device Version	10.0.5.1	ESET PROTECT versão
Device Event Class ID (Signature ID):	109	Identificador exclusivo da categoria de evento do dispositivo: • 100 – Evento de ameaça 199 • 200 – Evento de firewall 299 • 300399 HIPS evento • 400–499 evento de auditoria • 500–599 ESET Inspect evento • 600 – Evento de arquivos bloqueados 699 • 700 – Evento de sites filtrados 799
Event Name	Detected port scanning attack	Uma breve descrição do que aconteceu no evento
Severity	5	Gravidade 0–10

Extensões CEF comuns para todas as categorias

Nome da extensão	Exemplo	Descrição
cat	ESET Threat Event	Categoria de evento: • ESET Threat Event • ESET Firewall Event • ESET HIPS Event • ESET RA Audit Event • ESET Inspect Event • ESET Blocked File Event • ESET Filtered Website Event
dvc	10.0.12.59	Endereço IPv4 do computador gerando o evento.
c6a1	2001:0db8:85a3:0000:0000:8a2e:0370:7334	Endereço IPv6 do computador gerando o evento.
c6a1Label	Device IPv6 Address	
dvchost	COMPUTER02	Nome de host do computador com o evento
deviceExternalId	39e0feee-45e2-476a-b17f-169b592c3645	UUID do computador gerando o evento.
flexString1	Lost & Found	O nome do grupo do computador gerando o evento
flexString1Label	Device Group Name	
rt	Jun 04 2017 14:10:0	Hora UTC de ocorrência do evento. O formato é %b %d %Y %H:%M:%S

Extensões CEF por categoria de evento

Eventos de ameaça

Nome da extensão	Exemplo	Descrição
cs1	W97M/Kojer.A	Nome da ameaça encontrada
cs1Label	Threat Name	
cs2	25898 (20220909)	Versão do mecanismo de detecção
cs2Label	Engine Version	
cs3	Virus	Tipo de detecção
cs3Label	Threat Type	
cs4	Real-time file system protection	ID do Scanner
cs4Label	Scanner ID	
cs5	virlog.dat	ID de rastreamento
cs5Label	Scan ID	

Nome da extensão	Exemplo	Descrição
cs6	Failed to remove file	Mensagem de erro se a "ação" não for bem sucedida
cs6Label	Action Error	
cs7	Event occurred on a newly created file	Descrição breve do que causou o evento
cs7Label	Circumstances	
cs8	0000000000000000000000000000000000000000	SHA1 hash do fluxo de dados (detecção).
cs8Label	Hash	
act	Cleaned by deleting file	A ação foi realizada pelo endpoint
filePath	file:///C:/Users/Administrator/Downloads/doc/000001_5dc5c46b.DOC	Objeto URI
fileType	File	Tipo de objeto relacionado ao evento
cn1	1	A detecção foi tratada (1) ou não foi tratada (0)
cn1Label	Handled	
cn2	0	É necessário reiniciar (1) ou não é necessário reiniciar (0)
cn2Label	Restart Needed	
suser	172-MG\\Administrator	Nome da conta de usuário associada ao evento
sprod	C:\\7-Zip\\7z.exe	O nome do processo de origem do evento
deviceCustomDate1	Jun 04 2019 14:10:00	

Nome da extensão	Exemplo	Descrição
deviceCustomDate1Label	FirstSeen	A hora e a data em que a detecção foi encontrada pela primeira vez na máquina. O formato é %b %d %Y %H:%M:%S

Exemplo de relatório CEF de evento de ameaça:

CEF:O|ESET|Protect|10.0.0.0|183|File scanner cleaned a virus|5|deviceExternalId=e9d26759-fd21-47f1-9751-d2e7194c41a8 flexString1=Lost & found flexString1Label=Device Group Name cat=ESET Threat Event rt=Jun 04 2017 14:10:00 cs1=W97M/Kojer.A cs1Label=Threat Name cs2=25898 (20220909) cs2Label=Engine Version cs3=Virus cs3Label=Threat Type cs4=Real-time file system protection cs4Label=Scanner ID cs5=virlog.dat cs5Label=Scan ID act=Cleaned by deleting fileType=File filePath=file:///C:/Users/Administrator/Downloads/doc/000001_5dc5c46b.DOC cn1=1 cn1Label=Handled suser=172-MG\\Administrator sprod=C:\\7-Zip\\7z.exe cs7=Event occurred on a newly created file. cs7Label=Circumstances eviceCustomDate1=Jun 04 2019 14:10:00 deviceCustomDate1Label=FirstSeen cs8=0000000000000000000000000000000000000000 cs8Label=Hash

Eventos de firewall

Nome da extensão	Exemplo	Descrição
msg	TCP Port Scanning attack	Nome do evento
src	127.0.0.1	Endereço de origem do evento IPv4
c6a2	2001:0db8:85a3:0000:0000:8a2e:0370:7334	Endereço de origem do evento IPv6
c6a2Label	Source IPv6 Address	
spt	36324	Porta de origem do evento
dst	127.0.0.2	Endereço IPv4 de destino do evento
c6a3	2001:0db8:85a3:0000:0000:8a2e:0370:7335	Endereço IPv6 de destino do evento
c6a3Label	Destination IPv6 Address	
dpt	24	Porta de destino de evento
proto	http	Protocolo
act	Blocked	Ação realizada
cn1	1	A detecção foi tratada (1) ou não foi tratada (0)
cn1Label	Handled	
suser	172-MG\\Administrator	Nome da conta de usuário associada ao evento
deviceProcessName	someApp.exe	Nome do processo associado ao evento
deviceDirection	1	A conexão era de entrada (0) ou saída (1)

Nome da extensão	Exemplo	Descrição
cnt	3	O número das mesmas mensagens geradas pelo endpoint entre duas replicações consecutivas entre o ESET PROTECT e o Agente ESET Management
cs1		ID de regra
cs1Label	Rule ID	
cs2	custom_rule_12	Nome da regra
cs2Label	Rule Name	
cs3	Win32/Botnet.generic	Nome da ameaça
cs3Label	Threat Name	

Exemplo de relatório CEF de evento de firewall:

```
CEF:O|ESET|Protect|10.0.0.0|109|Detected port scanning attack|5|deviceExternalId=39e0feee-45e2-476a-b07f-169b592c3645 flexString1=Lost & found flexString1Label=Device Group Name cat=ESET Firewall Event rt=Jun 04 2017 14:10:00 msg=TCP Port Scanning attack src=127.0.0.1 spt=36324 dpt=21 dst=127.0.0.2 proto=http act=Blocked cnt=1 cn1=1 cn1Label=Handled suser=myAccount deviceProcessName=someApp.exe cs2=rule_118882389 cs2Label=Rule Name deviceDirection=0 cs3=Win32/Botnet.generic cs3Label=Threat Name
```

HIPS eventos

Nome da extensão	Exemplo	Descrição
cs1	Suspicious attempt to launch an application	ID de regra
cs1Label	Rule ID	
cs2	custom_rule_12	Nome da regra
cs2Label	Rule Name	
cs3	C:\\someapp.exe	Nome do aplicativo
cs3Label	Application	
cs4	Attempt to run a suspicious object	Operação
cs4Label	Operation	
cs5	C:\\somevirus.exe	Destino
cs5Label	Target	
act	Blocked	Ação realizada
cs2	custom_rule_12	Nome da regra
cn1	1	A detecção foi tratada (1) ou não foi tratada (0)
cn1Label	Handled	
cnt	3	O número das mesmas mensagens geradas pelo endpoint entre duas replicações consecutivas entre o ESET PROTECT e o Agente ESET Management

Exemplo de relatório CEF de evento HIPS:

CEF:O|ESET|Protect|10.0.0.0|303|Attempt to run a suspicious object Blocked|5|dvchost=test_bcmcjkbpgp deviceExternalId=82e114a8-9070-4868-8ee2-1e87b7b85ee3 flexString1=Lost & found flexString1Label=Device Group Name cat=ESET HIPS Event rt=Jun 04 2019 14:10:00 cs3=C:\\someapp.exe cs3Label=Application cs4=Attempt to run a suspicious object cs4Label=Operation cs5=C:\\somevirus.exe cs5Label=Target act=Blocked cn1=1 cn1Label=Handled cs1=Suspicious attempt to launch an application cs1Label=Rule ID cnt=1

Eventos de auditoria

Nome da extensão	Exemplo	Descrição
act	Login attempt	Ação sendo realizada
suser	Administrator	Usuário de segurança envolvido
duser	Administrator	Usuário de segurança de destino (por exemplo, para tentativas de login)
msg	Authenticating native user 'Administrator'	Uma descrição detalhada da ação
cs1	Native user	Domínio de relatório de auditoria
cs1Label	Audit Domain	
cs2	Success	Resultado da ação
cs2Label	Result	

Exemplo de relatório CEF de evento de auditoria:

CEF:O|ESET|Protect|10.0.0.0|449|Native user login|2|dvc=10.15.172.133 dvchost=BRNH00006D deviceExternalId=db4a82c0-e1c6-49be-8bac-a436136ed1f4 cat=ESET RA Audit Event rt=Sep 21 2022 13:10:23 cs1=Native user cs1Label=Audit Domain act=Login attempt duser=Administrator msg=Authenticating native user 'Administrator'. cs2=Success cs2Label=Result

ESET Inspect eventos

Nome da extensão	Exemplo	Descrição
deviceProcessName	c:\\imagepath_bin.exe	Nome do processo causando esse alarme
suser	HP\\home	Proprietário do processo
cs2	custom_rule_12	Nome da regra acionando este alarme
cs2Label	Rule Name	
cs3	78C136C80FF3F46C2C98F5C6B3B5BB581F8903A9	Alarme de hash SHA1
cs3Label	Hash	
cs4	https://inspect.eset.com:443/console/alarm/126	Link para o alarme no Web Console ESET Inspect
cs4Label	EI Console Link	
cs5	126	ID da subparte do link de alarme ($1 no ^http.*/alarm/([0-9]+)$)
cs5Label	EI Alarm ID	
cn1	275	Pontuação de gravidade do computador
cn1Label	ComputerSeverityScore	

Nome da extensão	Exemplo	Descrição
cn2	60	Pontuação de gravidade da regra
cn2Label	SeverityScore	
cnt	3	O número de alertas do mesmo tipo gerados desde o último alarme

Exemplo de relatório CEF de evento ESET Inspect:

```
CEF:O|ESET|Protect|10.0.0.0|500|ESET Inspect Alert|5|dvchost=test_lrghlbjyoa
deviceExternalId=432a30af-6ac7-4b61-ae5c-5141bfc5d878 flexString1=Lost & found flexString1Label=Device
Group Name cat=ESET Inspect Alert rt=Sep 21 2022 07:31:55
deviceProcessName=c:\\mother_process_info_imagepath_dir\\mother_process_info_imagepath_bin.exe
suser=HP\\home cs2=9_1_0addd4e8baf8e87d4bc4ed77fadc cs2Label=Rule Name
cs3=78C136C80FF3F46C2C98F5C6B3B5BB581F8903A9 cs3Label=Hash
cs4=https://dev-inspect.eset.com:443/console/alarm/126 cs4Label=EI Console Link cs5=126 cs5Label=EI Alarm
ID cn1=275 cn1Label=ComputerSeverityScore cn2=60 cn2Label=SeverityScore
```

Eventos de arquivos bloqueados

Nome da extensão	Exemplo	Descrição
act	Execution blocked	Ação realizada
cn1	1	A detecção foi tratada (1) ou não foi tratada (0)
cn1Label	Handled	
suser	HP\\home	Nome da conta de usuário associada ao evento
deviceProcessName	C:\\Windows\\explorer.exe	Nome do processo associado ao evento
cs1	78C136C80FF3F46C2C98F5C6B3B5BB581F8903A9	Hash SHA1 do arquivo bloqueado
cs1Label	Hash	
filePath	C:\\totalcmd\\TOTALCMD.EXE	Objeto URI
msg	ESET Inspect	Descrição do arquivo bloqueado
deviceCustomDate1	Jun 04 2019 14:10:00	
deviceCustomDate1Label	FirstSeen	A hora e a data em que a detecção foi encontrada pela primeira vez na máquina. O formato é %b %d %Y %H:%M:%S
cs2	Blocked by Administrator	Causa
cs2Label	Cause	

Exemplo de relatório CEF de evento de arquivos bloqueados:

CEF:O|ESET|Protect|10.0.0.0|600|Blocked File Event|5|dvchost=test_lrghlbjyoa deviceExternalId=432a30af-6ac7-4b61-ae5c-5141bfc5d878 flexString1=Lost & found flexString1Label=Device Group Name cat=ESET Blocked File Event rt=Sep 21 2022 07:31:55 act=Execution blocked cn1=1 cn1Label=Handled suser=HP\\home deviceProcessName=C:\\Windows\\explorer.exe cs1=78C136C80FF3F46C2C98F5C6B3B5BB581F8903A9 cs1Label=Hash filePath=C:\\totalcmd\\TOTALCMD.EXE deviceCustomDate1=Sep 21 2022 07:31:55 deviceCustomDate1Label=FirstSeen cs2=Blocked by Administrator cs2Label=Cause msg=ESET Inspect

Eventos de site filtrados

Nome da extensão	Exemplo	Descrição
msg	An attempt to connect to URL	Tipo do evento
act	Blocked	Ação realizada
cn1	1	A detecção foi tratada (1) ou não foi tratada (0)
cn1Label	Handled	
suser	Peter	Nome da conta de usuário associada ao evento
deviceProcessName	Firefox	Nome do processo associado ao evento
cs1	Blocked by PUA blacklist	ID de regra
cs1Label	Rule ID	
requestUrl	https://kenmmal.com/	URL de solicitação bloqueada
dst	172.17.9.224	Endereço de destino do evento IPv4
c6a3	2001:0db8:85a3:0000:0000:8a2e:0370:7335	Endereço de destino do evento IPv6
c6a3Label	Destination IPv6 Address	
cs2	HTTP filter	ID do Scanner
cs2Label	Scanner ID	
cs3	8EECCDD290BE2E99183290FDBE4172EBE3DC7EC5	Hashs SHA1 do objeto filtrado
cs3Label	Hash	

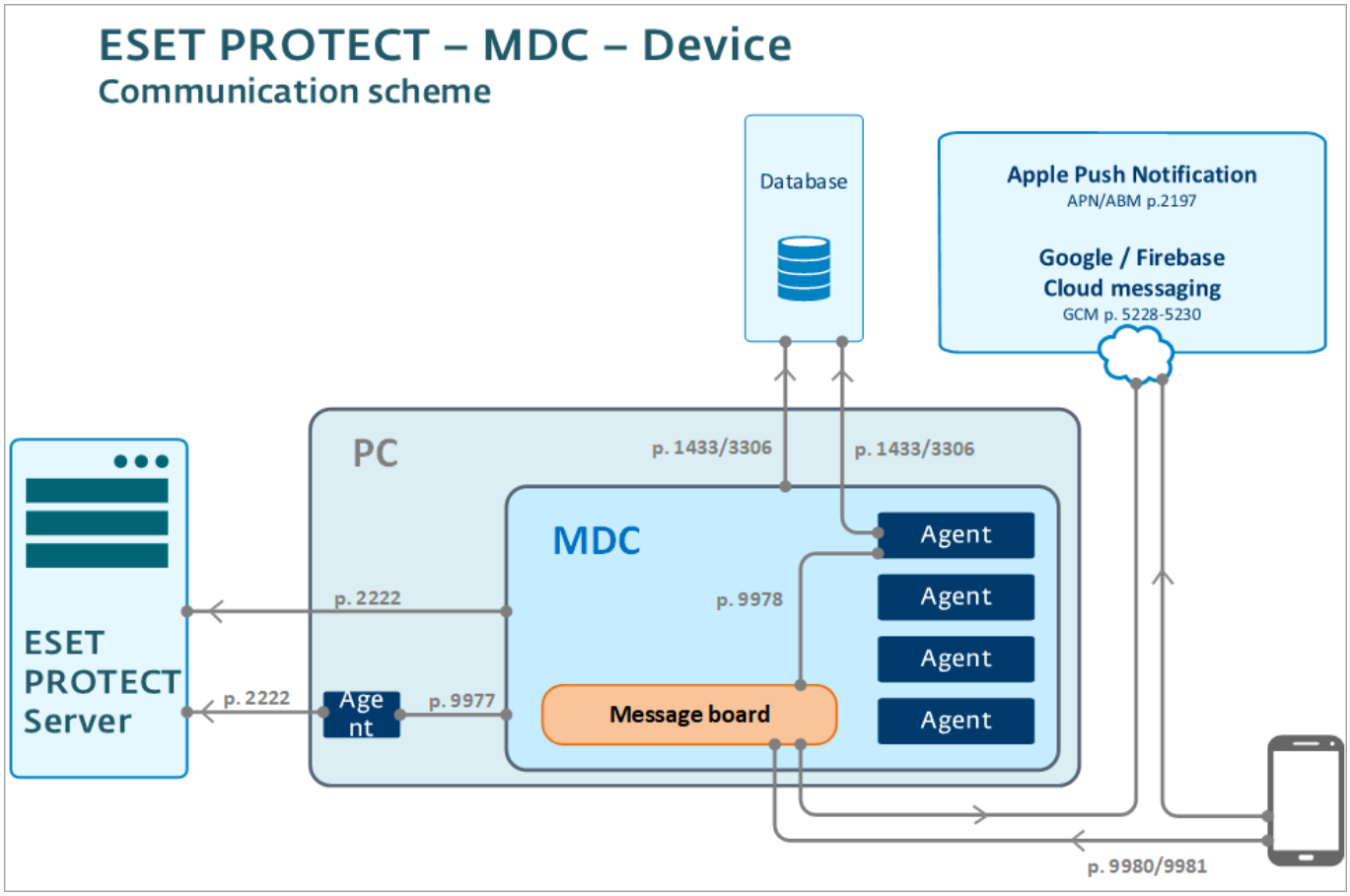
Exemplo de relatório CEF de evento de site filtrado:

CEF:O|ESET|Protect|10.0.0.0|716|Filtered Website Event|5|dvchost=test_lrghlbjyoa deviceExternalId=432a30af-6ac7-4b61-ae5c-5141bfc5d878 flexString1=Lost & found flexString1Label=Device Group Name cat=ESET Filtered Website Event rt=Sep 21 2022 07:31:55 msg=An attempt to connect to URL dst=172.17.9.224 cs2=HTTP filter cs2Label=Scanner ID act=Blocked cn1=1 cn1Label=Handled requestUrl=https://kenmmal.com cs3=8EECCDD290BE2E99183290FDBE4172EBE3DC7EC5 cs3Label=Hash suser=Peter deviceProcessName=Firefox cs1=Blocked by PUA blacklist cs1Label=Rule ID

Gestão de dispositivo 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.

O diagrama a seguir demonstra a comunicação entre os componentes ESET PROTECT e um dispositivo móvel:



Clique para ver a imagem maior

Recomendação de segurança para MDM: O dispositivo de host MDM precisa de acesso à internet. Recomendamos que o dispositivo de host MDM esteja atrás de um firewall e que apenas as portas necessárias para o MDM estejam abertas. Você também pode usar um IDS/IPS para monitorar a rede em busca de anomalias.

O Conector de dispositivo móvel (MDC) é um componente ESET PROTECT que permite a Gestão de dispositivo móvel com o ESET PROTECT, permitindo o gerenciamento de dispositivos móveis Android e iOS e a administração da segurança móvel.

O MDC oferece uma solução sem agende onde os Agentes não estão sendo executados diretamente em dispositivos móveis (para economizar bateria e desempenho do dispositivo móvel). O MDM serve como host para esses agentes virtuais. O MDC armazena dados de/para dispositivos móveis em seu banco de dados SQL dedicado.

O certificado HTTPS é necessário para autenticar a comunicação entre o dispositivo móvel e o MDC. Para autenticar a comunicação entre o Servidor ESET PROTECT e o MDC, um certificado de Proxy é usado.

O gerenciamento de dispositivos Apple tem alguns requisitos adicionais. Usar o ESET PROTECT MDC para gerenciar o dispositivo iOS requer o certificado do serviço de notificação por push da Apple. O serviço APN ativa o ESET MDC para se comunicar com segurança com dispositivos móveis Apple. Esse certificado deve ser assinado diretamente pela Apple (usando o Portal de Certificados Push da Apple) e entregue para o MDC através da política. Depois disso, os dispositivos iOS podem ser inscritos no ESET PROTECT MDC.

Em determinados países, o Apple Business Manager (ABM) está disponível. O ABM é um novo método potente para inscrição de dispositivos iOS corporativos. Com o ABM você pode inscrever os dispositivos iOS automaticamente no MDC sem nenhum contato direto com o dispositivo e também com interação mínima do usuário. O ABM estende dramaticamente as capacidades do iOS MDM e permite a personalização completa da configuração do dispositivo.

Depois de uma instalação e configuração bem sucedida do Conector de dispositivo móvel, os dispositivos móveis podem ser inscritos. Depois de uma inscrição bem-sucedida, o dispositivo móvel pode ser gerenciado do console da Web ESET PROTECT.

Configuração e definição 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 aproveitar o componente de Gestão de dispositivo móvel no ESET PROTECT, realize as etapas a seguir para depois da instalação do MDM para poder inscrever e gerenciar dispositivos móveis.

1. Instalar o **Conector de dispositivo móvel** (MDC) usando o Instalador Tudo-em-um ou executar uma instalação de componentes para o Windows ou Linux. Você também pode implantar o MDM como uma Máquina virtual. Certifique-se de ter cumprido com os pré-requisitos antes da instalação.

Se você estiver instalando o MDC usando o Instalador tudo-em-um, o certificado HTTPS assinado pela CA ESET PROTECT é gerado automaticamente durante o processo de instalação. O certificado é protegido por senha (com uma senha gerada aleatoriamente) e o certificado não está visível em **Mais** > **Certificados de mesmo nível**.
Para instalar o ESET PROTECT com o instalador Tudo-em-um e usar um certificado HTTPS de terceiros, instale o ESET PROTECT primeiro e depois altere seu certificado HTTPS usando a Política (em **Política de Conector de dispositivo móvel do ESET Mobile Device** > **Geral** > **Alterar certificado** > **Certificado personalizado**).
Se estiver instalando o componente MDC por si próprio, você pode usar:
a) certificado assinado pelo ESET PROTECT CA (**Básico** > **Produto**: Conector de dispositivo móvel; **Host**: Nome de host/Endereço IP do MDC; **Assinar** > **Assinar Método**: Autoridade de certificação; **Autoridade de certificação**: ESET PROTECT Autoridade de certificação
b) Corrente de certificado HTTPS de terceiro assinado por uma CA de confiança da Apple (lista de CA de confiança da Apple).

2. Ative o ESET PROTECT MDC usando a tarefa de cliente Ativação do produto. O procedimento é o mesmo que ao ativar qualquer produto de segurança ESET em um computador do cliente (uma unidade de licença não será usada).

3. Executar uma tarefa de servidor Sincronização de usuário (Recomendado). Isso permite que você sincronize automaticamente os usuários com o Active Directory ou LDAP para fins de Usuários do computador.

Se estiver planejando em gerenciar apenas dispositivos baseados em **Android** (nenhum dispositivos iOS será gerenciado), pule para a etapa 7.

4. Criar um certificado APN/ABM. Este certificado é usado pelo ESET PROTECT MDM para inscrição do dispositivo iOS. Certificados que serão adicionados ao seu perfil de inscrição também devem ser adicionados ao seu perfil ABM.

5. Criar uma nova política para o Conector de dispositivo móvel ESET para ativar o APNS.

Siga essas instruções para realizar a inscrição de dispositivos iOS com o Apple Business Manager (ABM).

6. Inscrever dispositivos móveis usando uma Inscrição de dispositivo. Configure a tarefa para inscrever dispositivos para Android e/ou iOS. Isso também pode ser feito da guia **Computadores** ou **Grupo** clicando em **Adicionar novo** > **Dispositivos móveis** enquanto tem um **Grupo estático** selecionado (**Adicionar novo** não pode ser usado em Grupos Dinâmicos).

7. Se você não tiver fornecido a licença durante a Inscrição de dispositivos, ative os Dispositivos móveis usando a Tarefa de cliente de ativação do produto - escolha uma licença ESET Endpoint Security. Uma unidade de licença será usada para cada dispositivo móvel.

A tarefa de **Ativação do produto** pode ativar um produto móvel, ESET Endpoint para Android, usando também uma licença off-line.
A tarefa de ativação não pode ativar os produtos ESET do versão 4 e 5 com a licença off-line. É preciso ativar o produto manualmente ou usar uma versão compatível do produto (Recomendamos usar a versão mais recente).

8. Você pode editar Usuários para configurar Atributos personalizados e Atribuir dispositivos móveis se você não atribuiu usuários durante a Inscrição de dispositivos.

9. Agora você pode começar a aplicar políticas e gerenciar dispositivos móveis. Por exemplo, Criar uma política para iOS MDM - Conta Exchange ActiveSync, que vai configurar automaticamente a Conta de email, Contatos e Agenda em dispositivos iOS. Você também pode aplicar restrições em um dispositivo iOS e/ou adicionar uma conexão Wi-Fi.

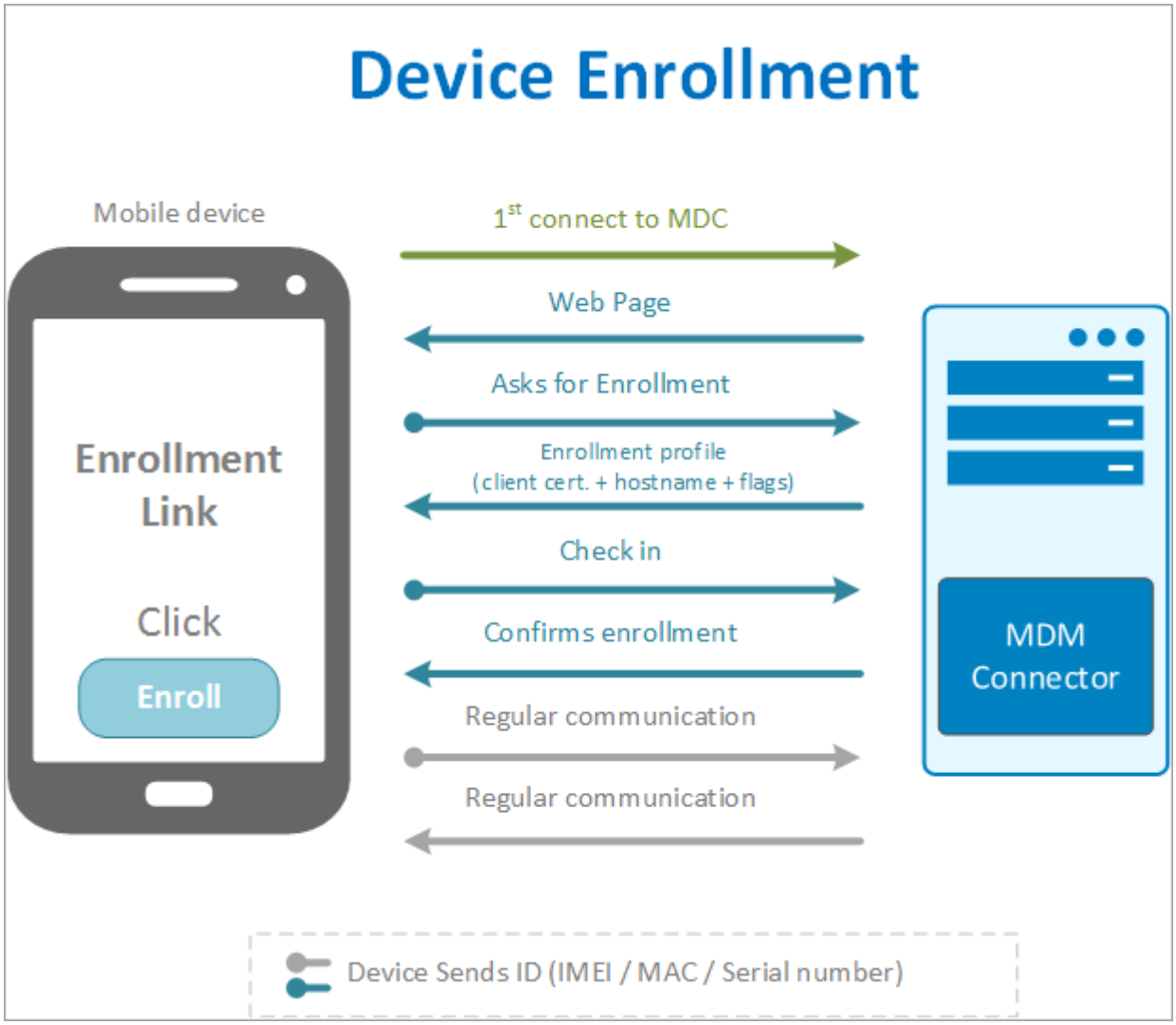
Solução de problemas

- Você pode usar **Inscrever novamente** em um dispositivo móvel que foi corrompido ou apagado. O link de nova inscrição será enviado via email.
- A tarefa Parar de gerenciar (Desinstalar Agente ESET Management) irá cancelar a inscrição MDM de um dispositivo móvel e removê-lo do ESET PROTECT.
- Para atualizar o MDC, use a tarefa Atualização de componentes ESET PROTECT.
- Veja também a solução de problemas MDM

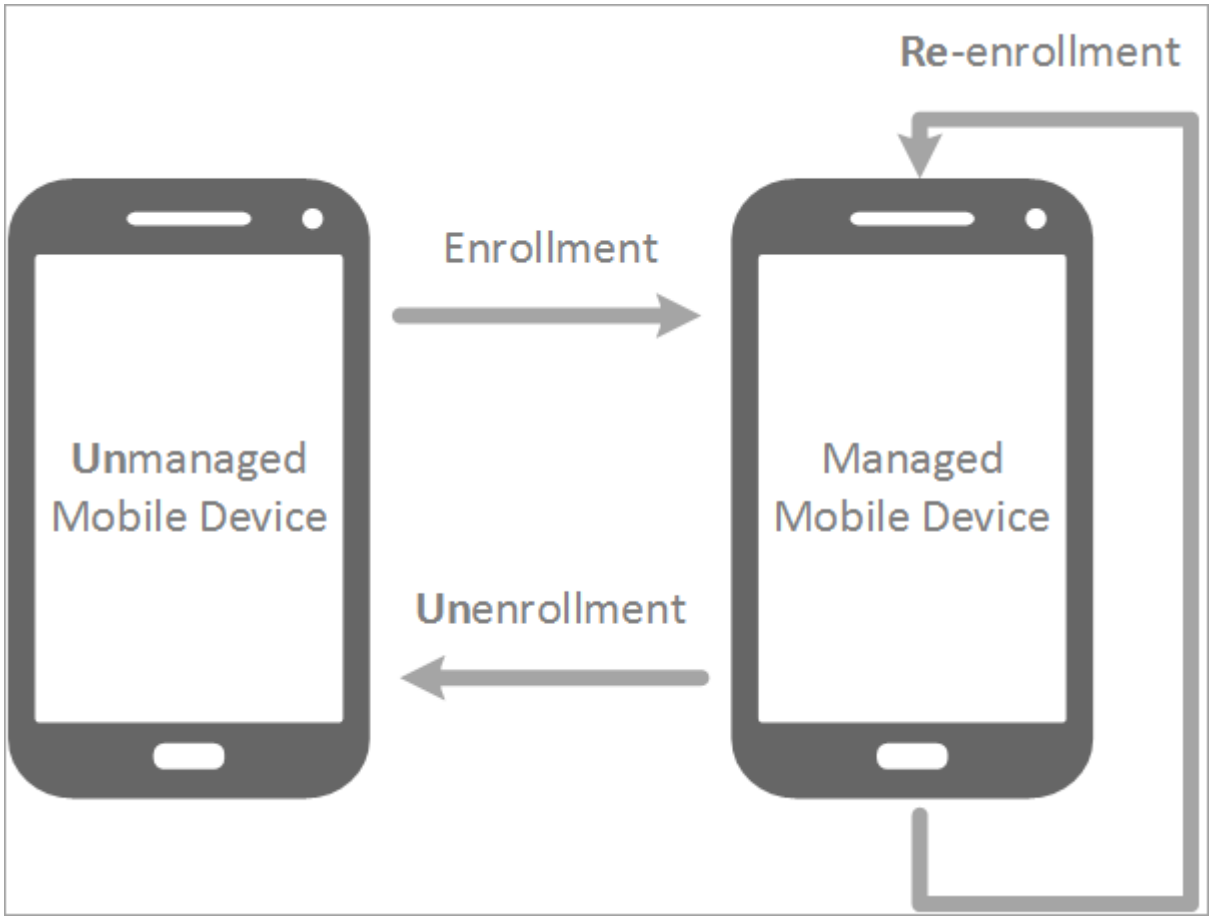
Inscrição de dispositivos

Os dispositivos móveis podem ser gerenciados através do ESET PROTECT e do produto de segurança ESET em execução no dispositivo móvel. Para começar a gerenciar dispositivos móveis, é necessário inscrevê-los no ESET PROTECT (não é mais necessário inserir o IMEI ou outros números de identificação no dispositivo móvel).

O diagrama abaixo ilustra como um dispositivo móvel se comunica com o Conector de dispositivo móvel durante o processo de inscrição:



Este diagrama explica quando a inscrição, reinscrição e retirada da inscrição podem ser usados e explica a diferença entre dispositivo gerenciado e não gerenciado.



- **Inscrição**: A inscrição só pode ser usada quando o dispositivo não é gerenciado pelo MDM. Neste caso, o dispositivo não existe na seção **Computadores**. Excluir um dispositivo do console da web não faz com que não seja gerenciado e o dispositivo aparecerá no console da web depois de uma replicação bem sucedida. Apenas o processo de retirada da inscrição pode remover um dispositivo do status gerenciado. Cada token de inscrição é único e de uso único, então ele só pode ser usado uma vez. Assim que um token é usado ele não pode ser usado de novo.

- **Reinscrição**: A reinscrição só pode ser usada quando o dispositivo é gerenciado. O token de reinscrição é sempre diferente do token de inscrição e também pode ser usado apenas uma vez.
Para reinscrever um dispositivo abra a seção **Computadores** e selecione o dispositivo móvel que quer reinscrever. Abra o menu **Computador** e selecione **Móvel > Reinscrição**.

- **Retirada da inscrição**: A retirada da inscrição é a maneira correta de parar de gerenciar um dispositivo. A retirada da inscrição é realizada usando uma tarefa de cliente Parar de gerenciar. Se o dispositivo não estiver respondendo pode levar até 3 dias para que o dispositivo seja realmente removido. Se quiser remover o dispositivo apenas para inscrevê-lo de novo, use a reinscrição.

> Siga essas instruções para realizar a inscrição de dispositivos iOS com o Apple Business Manager (ABM).

Você pode inscrever dispositivos móveis na seção **Computadores** ou sob Mais > Grupos. Selecione o **Grupo estático** ao qual você quer adicionar dispositivos móveis, clique em **Adicionar dispositivo** > **Dispositivos móveis** e selecione um dos seguintes métodos de inscrição:

- **Android ou iOS/iPadOS** – existem dois métodos de inscrição:

  - Enviar e-mail – Inscrição em massa de dispositivos móveis por email. Esta opção é mais adequada se você precisa inscrever um grande número de dispositivos móveis ou caso você tenha dispositivos móveis

existentes aos quais você não tem acesso físico. Usar esta opção requer participação ativa do usuário/proprietário do dispositivo móvel.

oEscanear código QR – inscrição de um único dispositivo móvel. Você será capaz de inscrever um dispositivo móvel de cada vez e terá que repetir o mesmo processo para cada dispositivo. Recomendamos que você use essa opção somente quando tiver um número pequeno de dispositivos móveis para inscrever. Esta opção é adequada se você não quiser que os usuários/proprietários de dispositivos móveis façam nada e que todas as tarefas de inscrição sejam feitas por você. Além disso, você pode usar esta opção se você tem novos dispositivos móveis que serão entregues aos usuários assim que os dispositivos forem todos configurados.

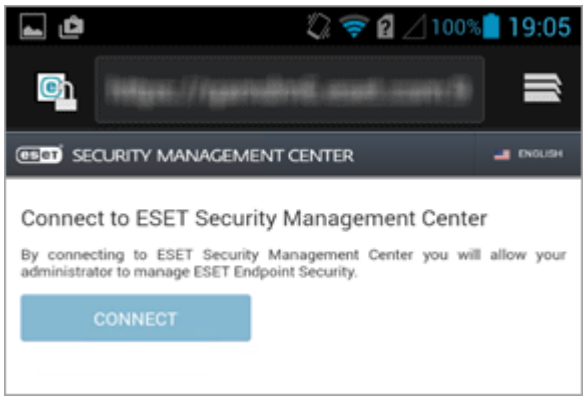
- **Inscrição individual como Proprietário do dispositivo (apenas Android 7 e versões superiores)** - inscrição de dispositivo móvel única apenas para dispositivos Android. Você será capaz de inscrever um dispositivo móvel de cada vez e terá que repetir o mesmo processo para cada dispositivo móvel. Esse processo de inscrição é possível apenas em dispositivos móveis novos (saídos da caixa) ou depois de uma limpeza/redefinição de fábrica. Esse processo de inscrição vai oferecer direitos de gerenciamento elevados para o administrador sobre os direitos de gerenciamento do usuário do dispositivo móvel.

Inscrição de dispositivo Android

Há dois cenários para a inscrição, quando o ESET Endpoint Security para Android (EESA) é ativado no dispositivo móvel. Você pode ativar o EESA no dispositivo móvel usando uma tarefa de cliente de Ativação de Produto (recomendado). O outro cenário é para dispositivos móveis com o aplicativo ESET Endpoint Security para Android já ativado.

EESA já ativado - siga as etapas abaixo para inscrever o seu dispositivo:

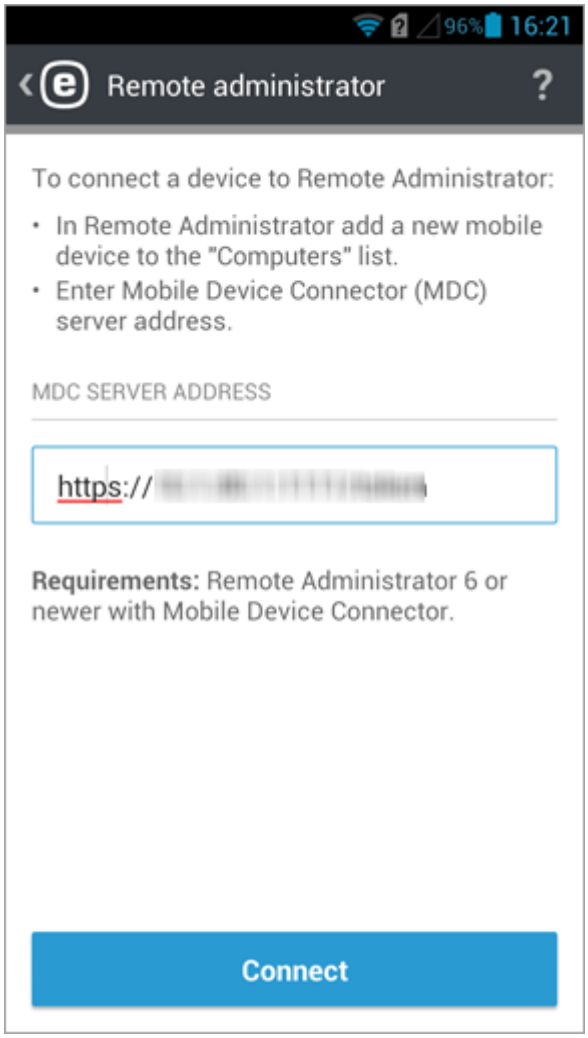
1. Toque no URL do link de inscrição (incluindo o número de porta) e digite-o no navegador manualmente (por exemplo, *https://eramdm:9980/<token>*). Você pode ser solicitado a aceitar um certificado SSL, clique em **Aceitar** se você concordar e depois em **Conectar**.



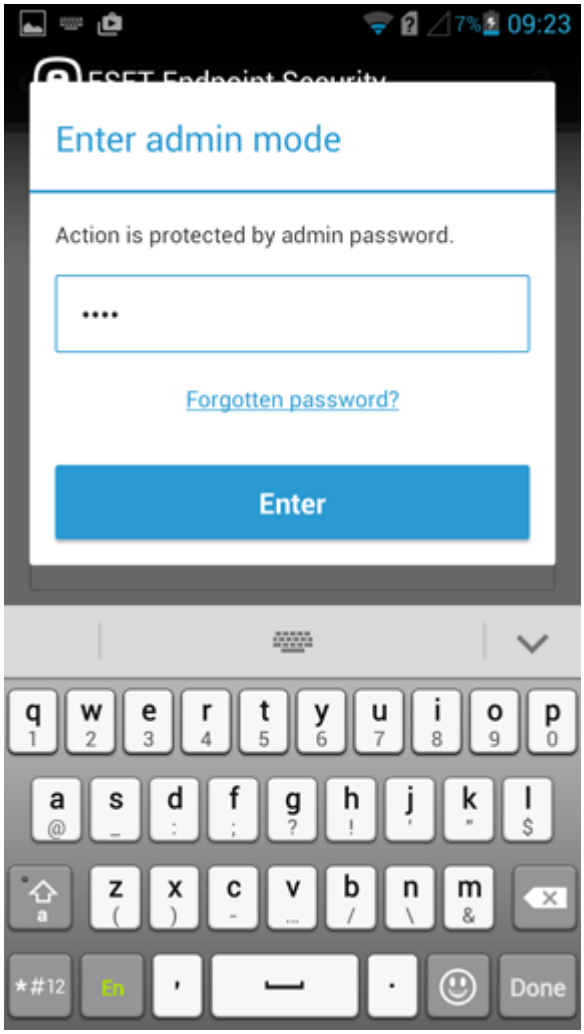
Se você não tiver o ESET Endpoint Security instalado no dispositivo móvel, você será redirecionado automaticamente para a loja do Google Play, onde é possível fazer download do aplicativo.

Se você receber a notificação **Não foi possível localizar o aplicativo para abrir este link**, tente abrir o link de inscrição no navegador web padrão do Android.

2. Confira seus detalhes da conexão (endereço e porta do servidor do Conector de dispositivo móvel) e clique em **Conectar**.



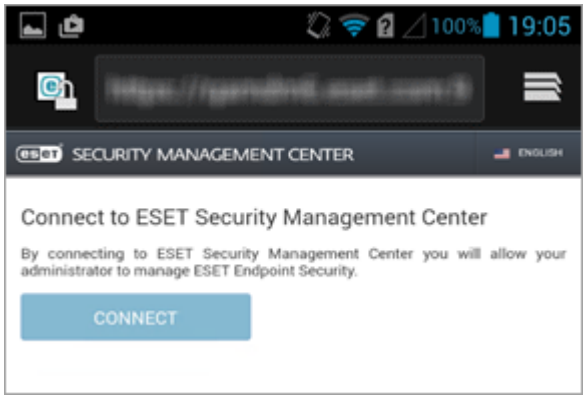
3. Digite a senha do modo de administrador do ESET Endpoint Security no campo em branco e toque em **Enter**.



4. Este dispositivo móvel agora está sendo gerenciado por ESET PROTECT, toque em **Concluir**.

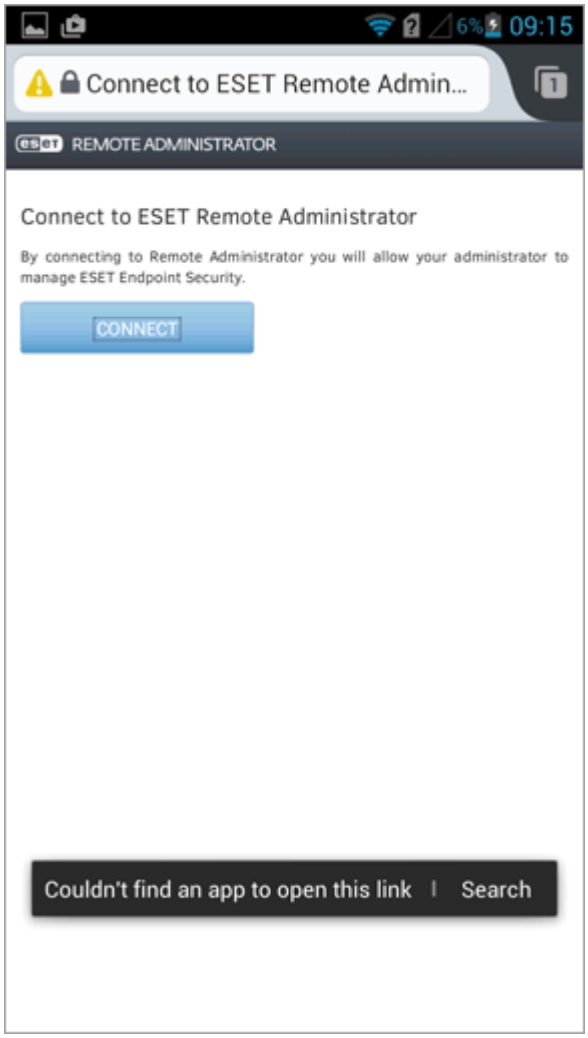
EESA ainda não ativado - siga as etapas abaixo para ativar o produto e inscrever seu dispositivo:

1. Toque no URL do link de inscrição (incluindo o número de porta) e digite-o no navegador manualmente (por exemplo, *https://esmcmdm:9980/<token>*) ou você pode usar o **Código QR** fornecido. Você pode ser solicitado a aceitar um certificado SSL, clique em **Aceitar** se você concordar e depois em **Conectar**.

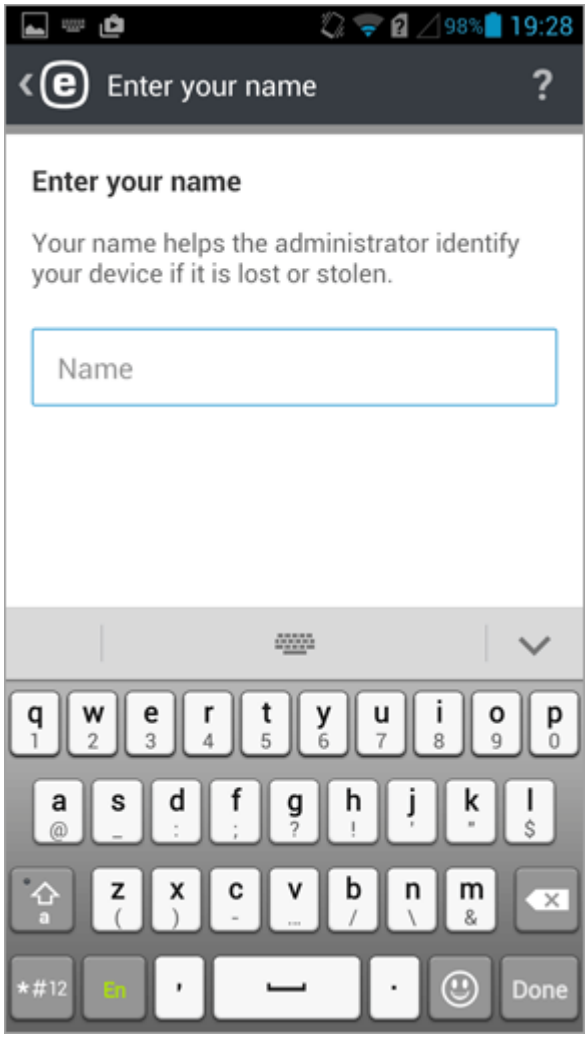


Se você não tiver o ESET Endpoint Security instalado no dispositivo móvel, você será redirecionado automaticamente para a loja do Google Play, onde é possível fazer download do aplicativo.

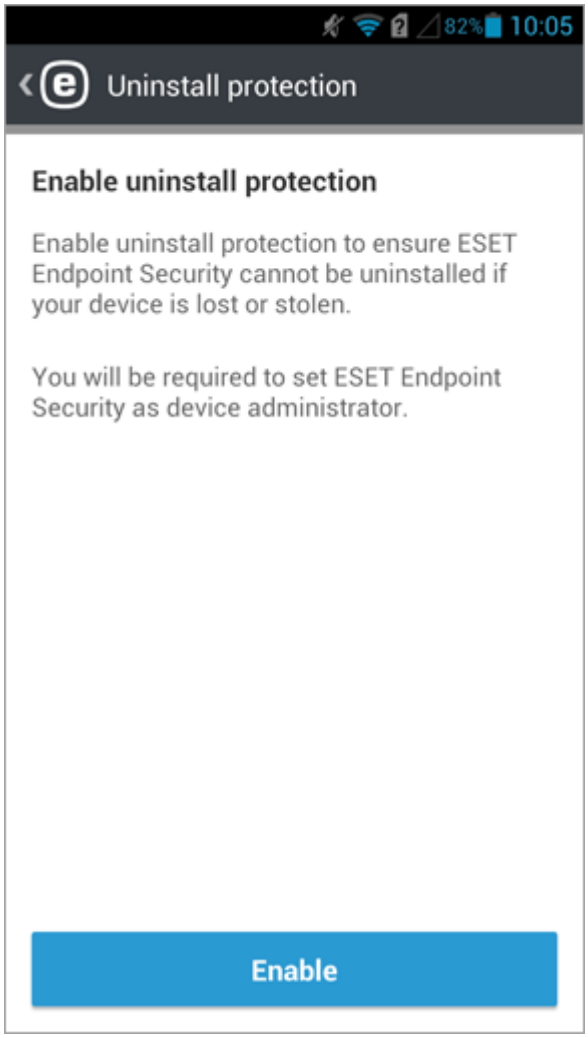
Se você receber a notificação **Não foi possível localizar o aplicativo para abrir este link**, tente abrir o link de inscrição no navegador web padrão do Android.



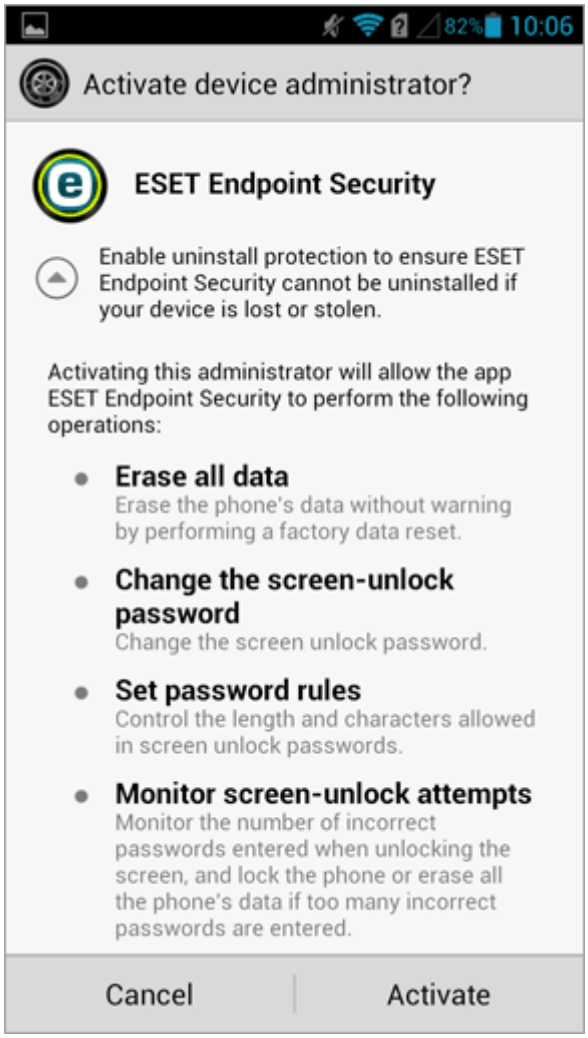
2. Insira o nome do dispositivo móvel. (Esse nome não é visível no ESET PROTECT. Só é relevante para Antifurto e para fins de relatório de diagnóstico.)



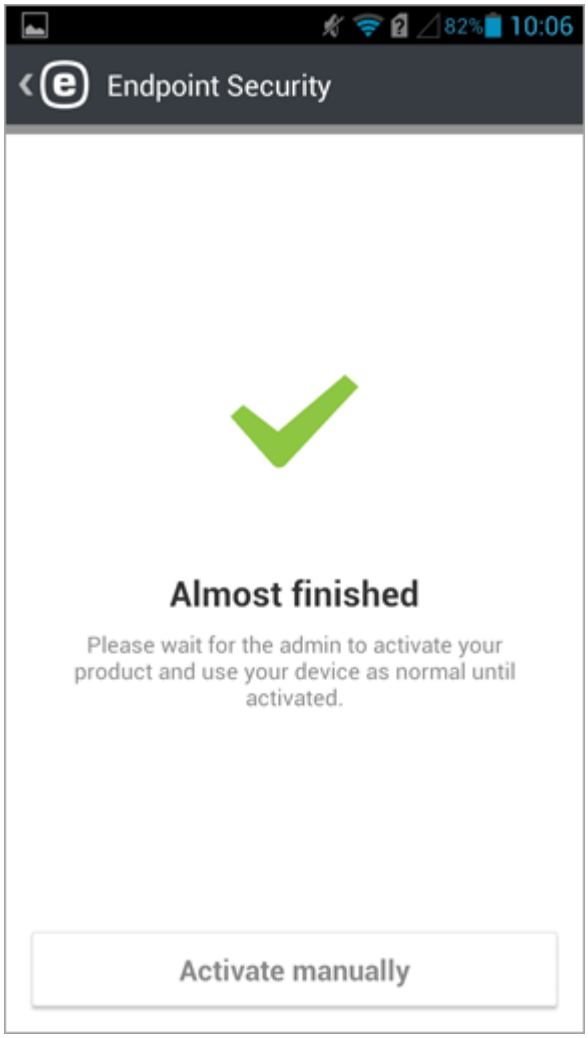
3. Toque **Habilitar** para ativar a proteção contra desinstalação.



4. Toque em **Ativar** para ativar o administrador do dispositivo.

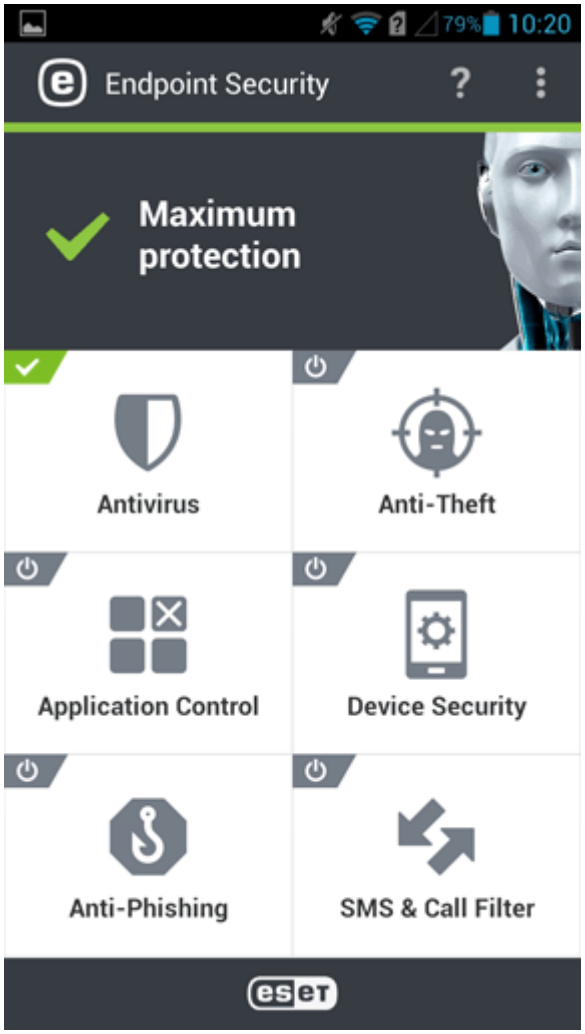


5. Neste ponto, você pode sair do aplicativo ESET Endpoint Security para Android no dispositivo móvel e abrir o console da Web ESET PROTECT.



6. No console da Web ESET PROTECT, vá para **Tarefas de clientes** > **Móvel** > Ativação de Produtos e clique em **Novo**.

Pode levar algum tempo para a tarefa do cliente de Ativação de Produtos ser executada no dispositivo móvel. Quando a tarefa for executada com sucesso, o aplicativo ESET Endpoint Security para Android é ativado e o dispositivo móvel está sendo gerenciado pelo ESET PROTECT. O usuário agora será capaz de usar o aplicativo ESET Endpoint Security para Android. Quando o aplicativo ESET Endpoint Security para Android estiver aberto, o menu principal será exibido:



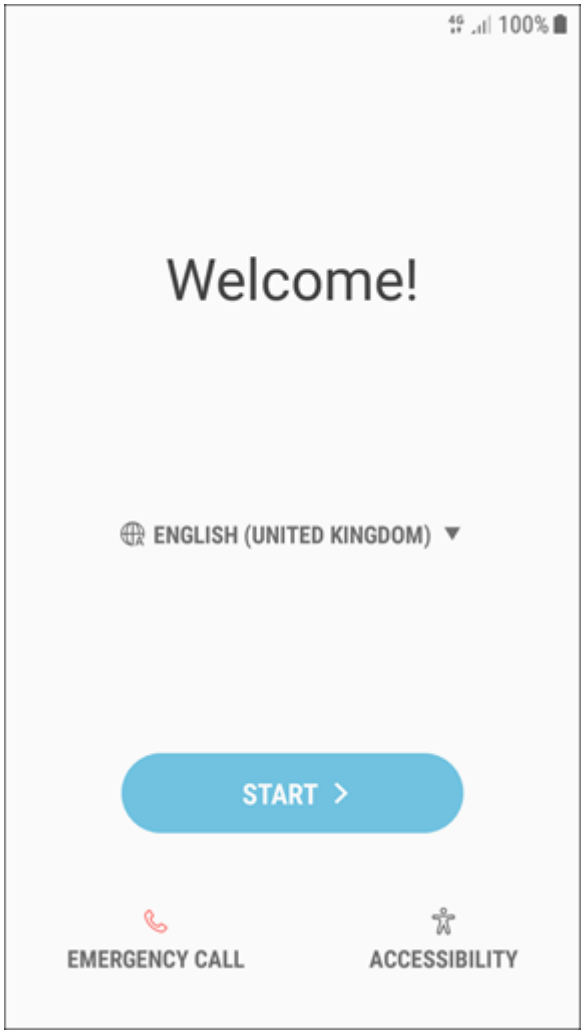
Inscrição de dispositivo Android como Proprietário do dispositivo

Esse tipo de inscrição está disponível apenas para dispositivos Android com Android v7 e versões superiores.
O dispositivo Android deve estar logo depois de uma limpeza/redefinição de fábrica ou ter acabado de sair da caixa para que possa realizar as etapas de inscrição a seguir.

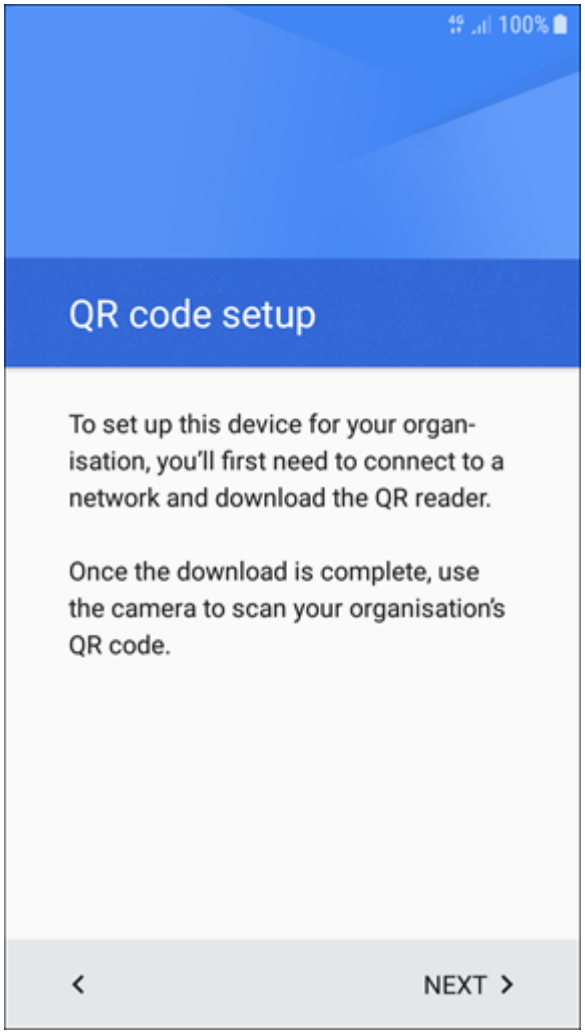
1. Ative o dispositivo móvel.

2. Insira o pin do cartão SIM.

3. Na tela de Boas-vindas, selecione o idioma preferido e toque na tela seis (6) vezes em algum lugar ao redor do texto “Bem-vindo” para iniciar a configuração do código QR.

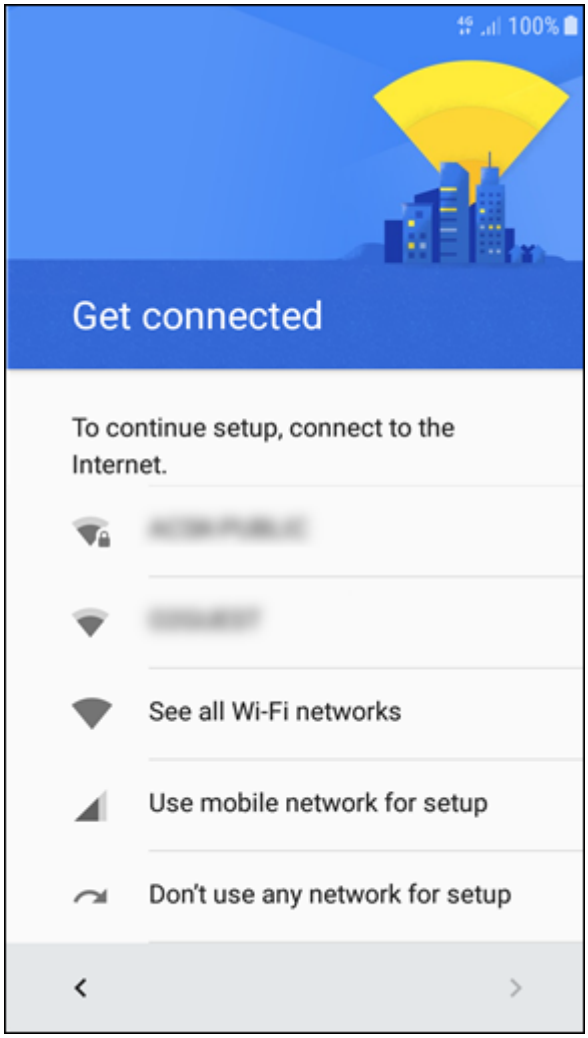


4. Se você tiver realizado a etapa anterior corretamente, uma tela de **configuração de código QR** será exibida. Toque em **AVANÇAR** para continuar.



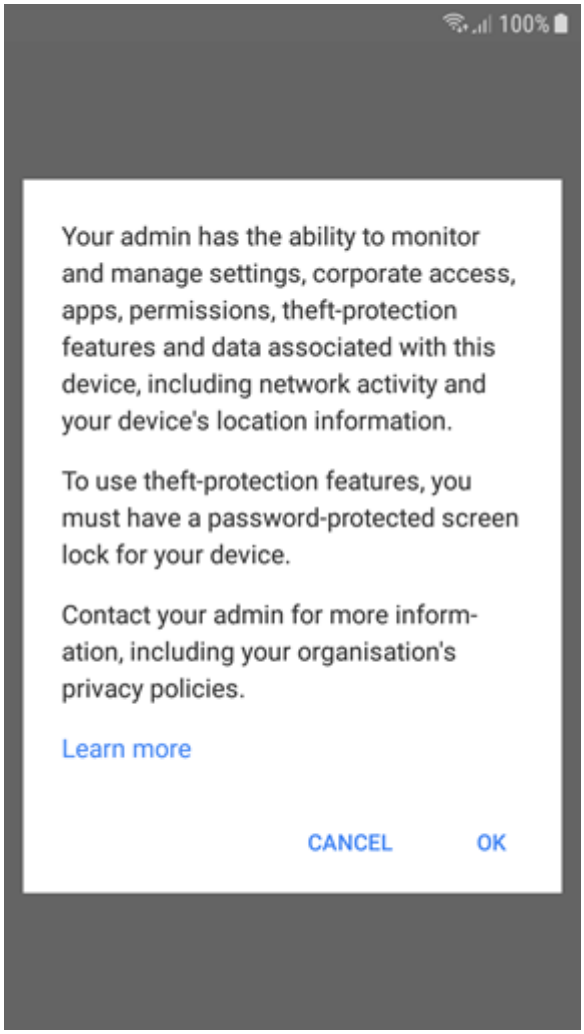
Para alguns dispositivos pode ser necessário realizar uma criptografia do armazenamento do dispositivo (as vezes também é necessário conectar o carregador). Selecione o tipo de criptografia que você quer e continue de acordo com as instruções na tela.

5. Selecione uma conexão com a internet. Isso será usado para fazer download do leitor de código QR necessário para a próxima etapa.

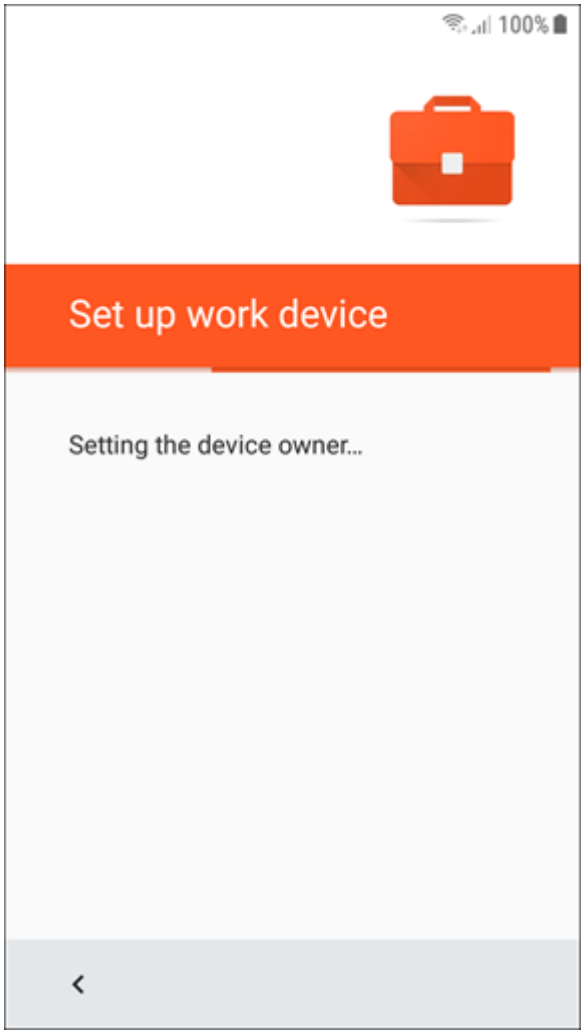


6. Agora o leitor de código QR será instalado. Depois do fim da instalação, escaneie o código QR que foi gerado no console da Web ESET PROTECT.

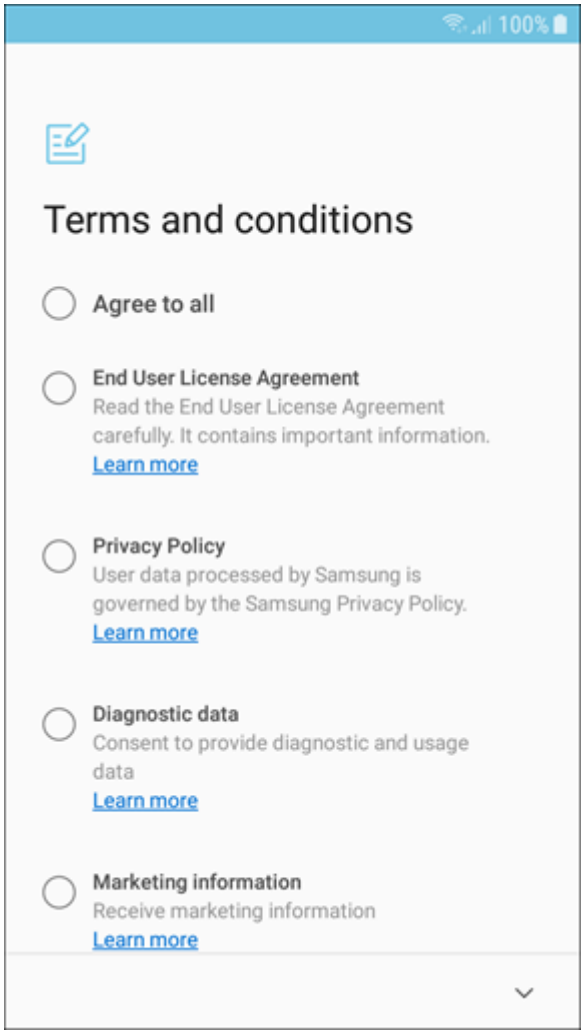
7. Será preciso que você confirme que entende que está concedendo direitos elevados de Proprietário de dispositivo ao Administrador. Toque em **OK** para continuar.



8. O aplicativo ESET Endpoint Security para Android agora poderá ser instalado e as permissões necessárias serão aplicadas.



9. Toque em **Concordo com tudo** para concordar com o EULA, Política de Privacidade e transferência de dados de diagnóstico e marketing.



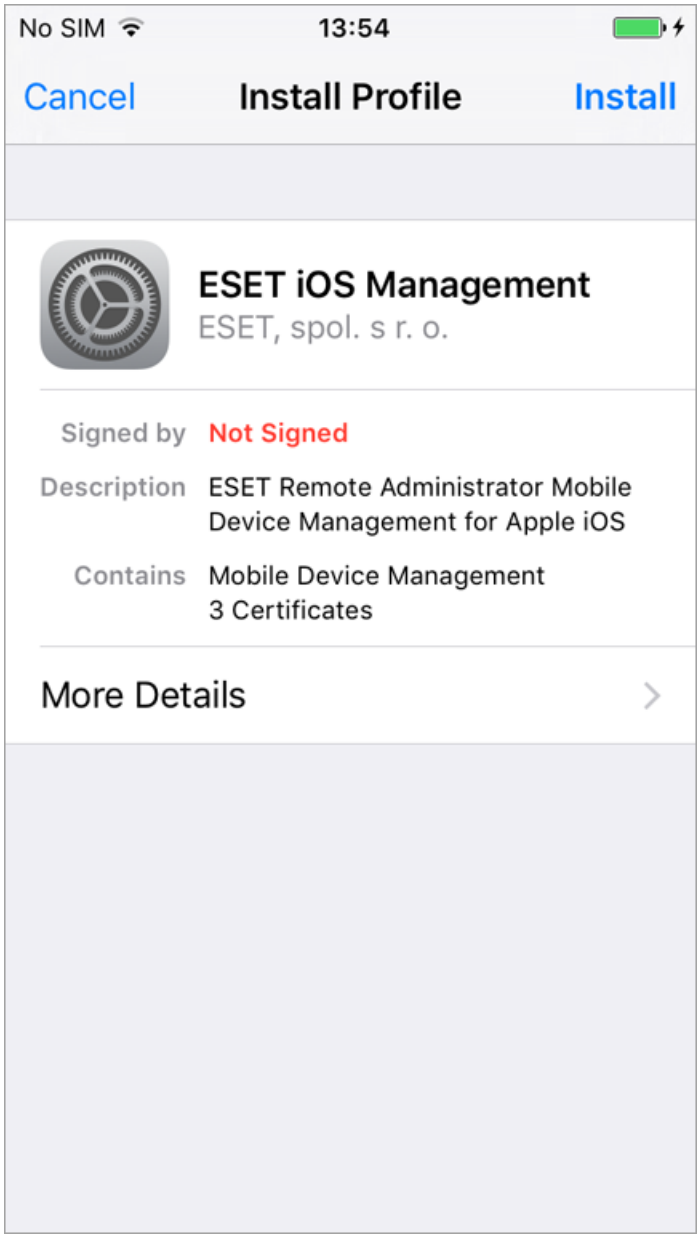
10. O dispositivo agora está inscrito no modo de Proprietário de dispositivo.

Inscrição de dispositivo iOS

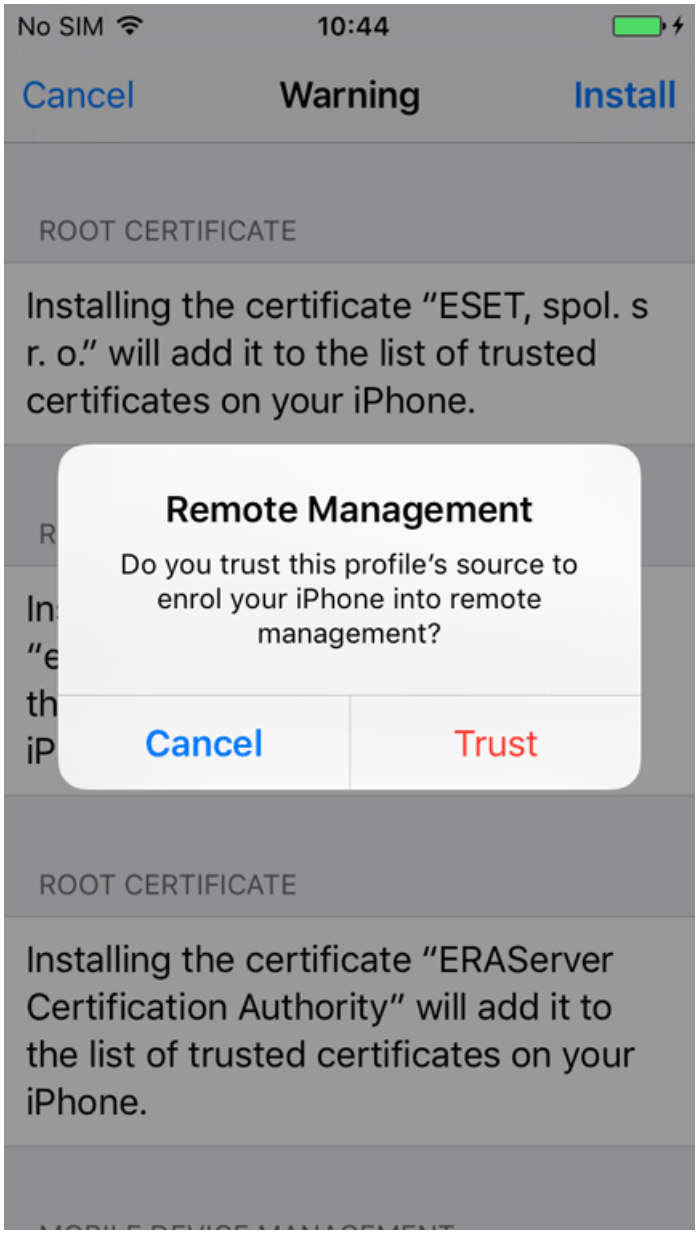
Siga essas instruções para realizar a inscrição de dispositivos iOS com o Apple Business Manager (ABM).

1. Toque no URL do link de inscrição (incluindo o número de porta) e digite-o no navegador manualmente (por exemplo, *https://eramdm:9980/<token>*) ou você pode usar o **Código QR** fornecido.

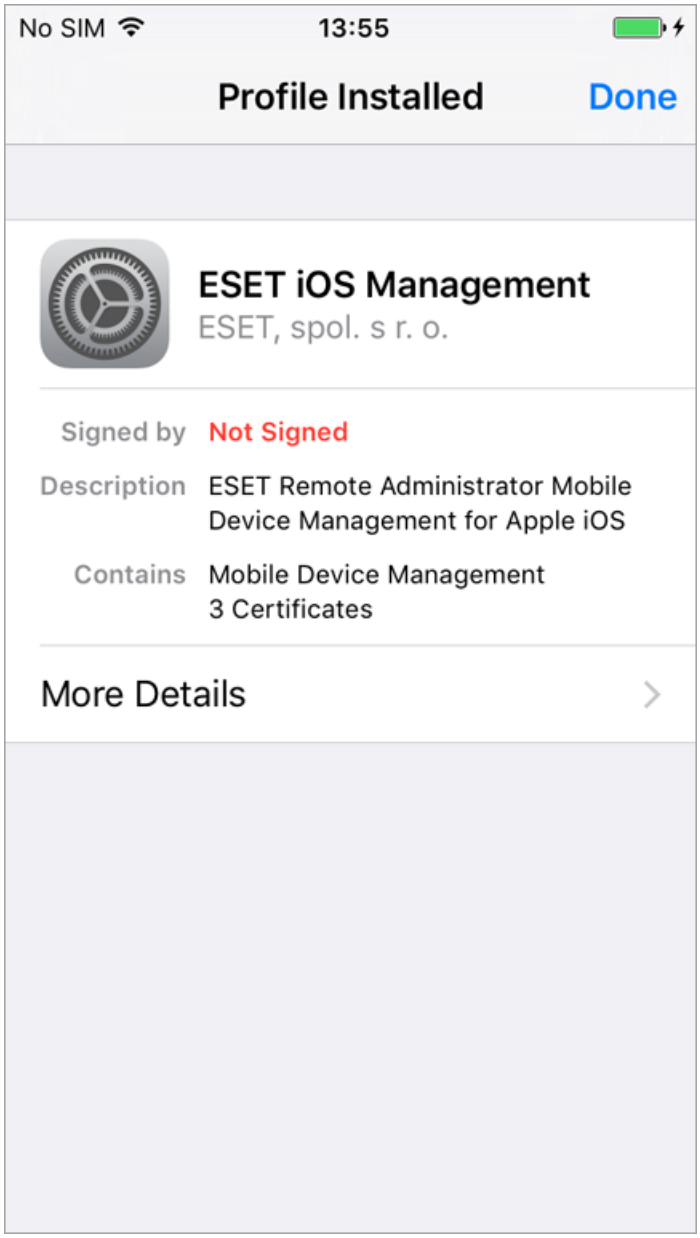
2. Toque em **Instalar** para continuar na tela Inscrição de MDM **Instalar perfil**.



3. Toque em **Confiar** para permitir a instalação do novo perfil.

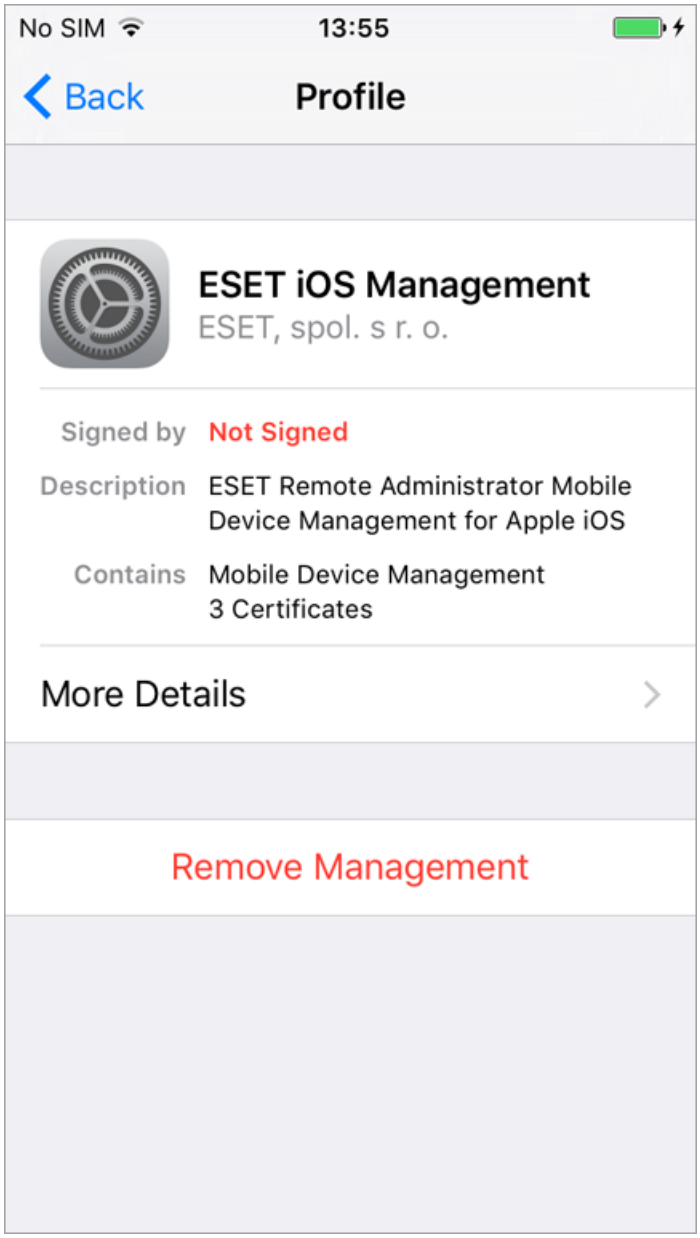


4. Depois de instalar o novo perfil, o campo **Assinado por** vai exibir que o perfil é **Não assinado**. Isso acontece porque o iOS não reconhece o certificado. Para ter um perfil de inscrição assinado, use o certificado HTTPS assinado pelo CA confiável da Apple. Ou você pode usar seu próprio certificado de inscrição HTTPS para assinar a inscrição.



5. Este perfil de inscrição permite configurar dispositivos e definir políticas de segurança para usuários ou grupos.

Remover o perfil de inscrição remove todas as configurações da empresa (Email, Agenda, Contatos, etc.) e o dispositivo móvel iOS não será gerenciado. Se um usuário retirar seu perfil de inscrição, o ESET PROTECT não saberá disso e o status do dispositivo vai mudar para e mais tarde para depois de 14 dias porque o dispositivo não está se conectando. Não será dada nenhuma outra indicação de que o perfil de inscrição foi removido.



Inscrição de dispositivos iOS com ABM

O Apple Business Manager (ABM) é o novo método da Apple para a inscrição de dispositivos iOS corporativos. Com o ABM você pode inscrever os dispositivos iOS sem nenhum contato direto com o dispositivo e também com interação mínima do usuário. A inscrição Apple ABM dá aos administradores a opção de personalizar o processo de configuração do dispositivo por completo. Ele também oferece a opção de impedir que os usuários removam o perfil MDM do dispositivo. Você pode inscrever seus dispositivos iOS existentes (se eles estiverem de acordo com os requisitos de dispositivos iOS ABM) e todos os dispositivos iOS que você comprar no futuro. Para obter mais informações sobre o Apple ABM consulte o Guia Apple ABM e a Documentação Apple ABM.

Sincronize seu ESET PROTECT MDM com o servidor Apple ABM:

1. Verifique se todos os Requisitos Apple ABM são cumpridos para os requisitos da conta e os requisitos do dispositivo.

- Conta ABM:
  - Este programa está disponível somente em certos países. Visite a página da web Apple ABM para ver se

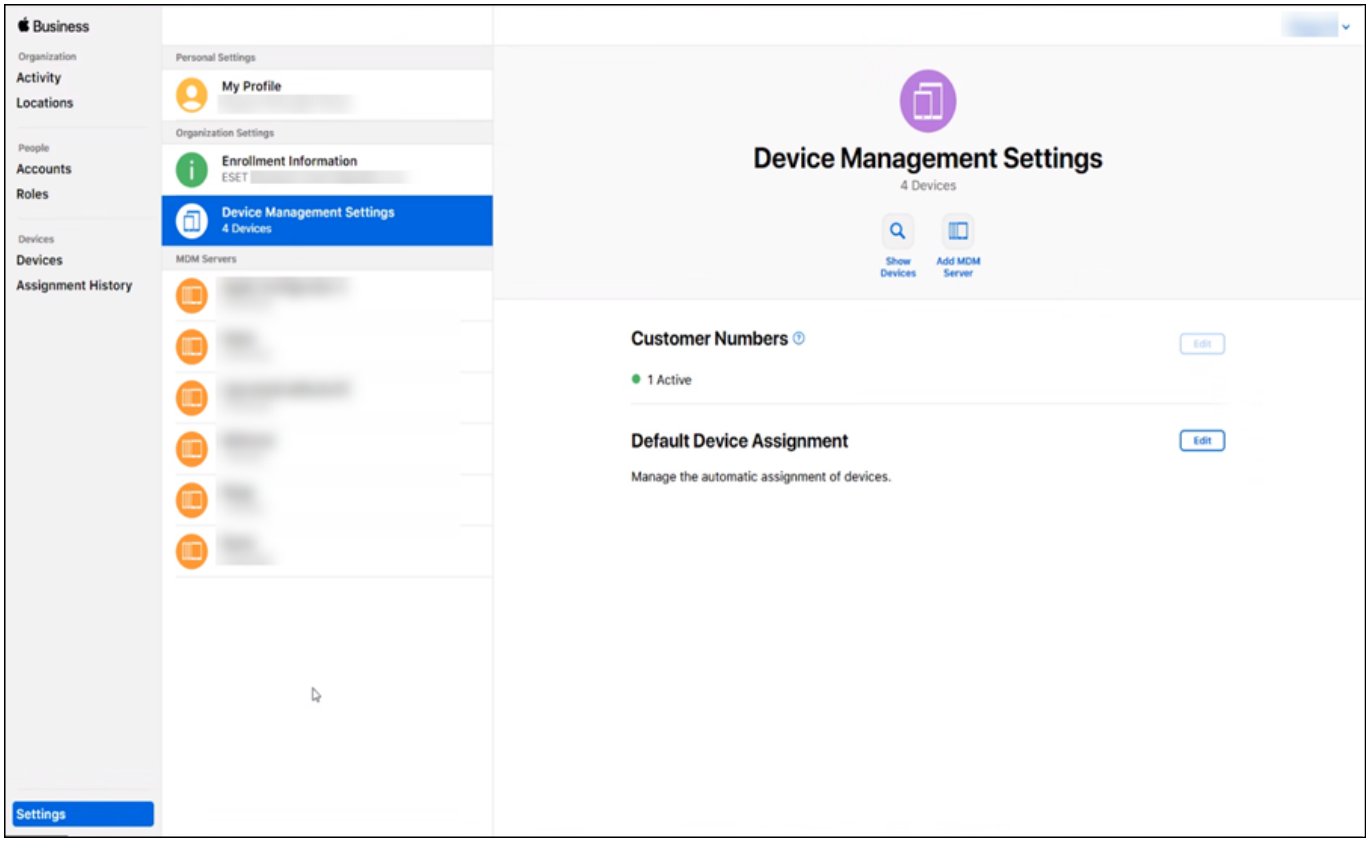
o ABM está disponível no seu país.

oOs requisitos da Conta Apple ABM podem ser encontrados nesses sites: Requisitos do programa de implantação Apple e requisitos do Programa de inscrição de dispositivo Apple.

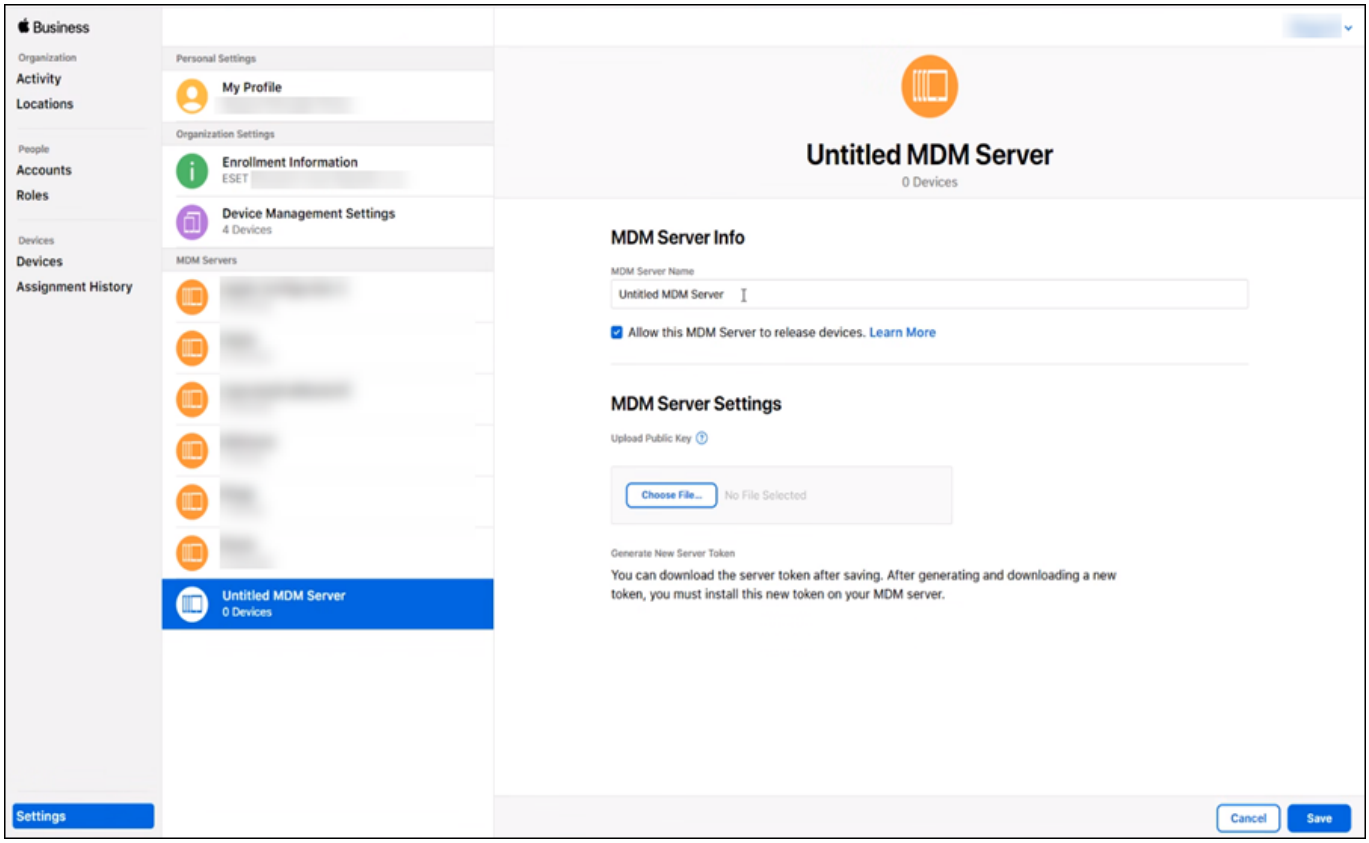
oVeja os requisitos detalhados de dispositivo ABM.

2.Entre em sua Conta Apple ABM (Se você não tiver uma Conta Apple ABM, poderá criar uma).

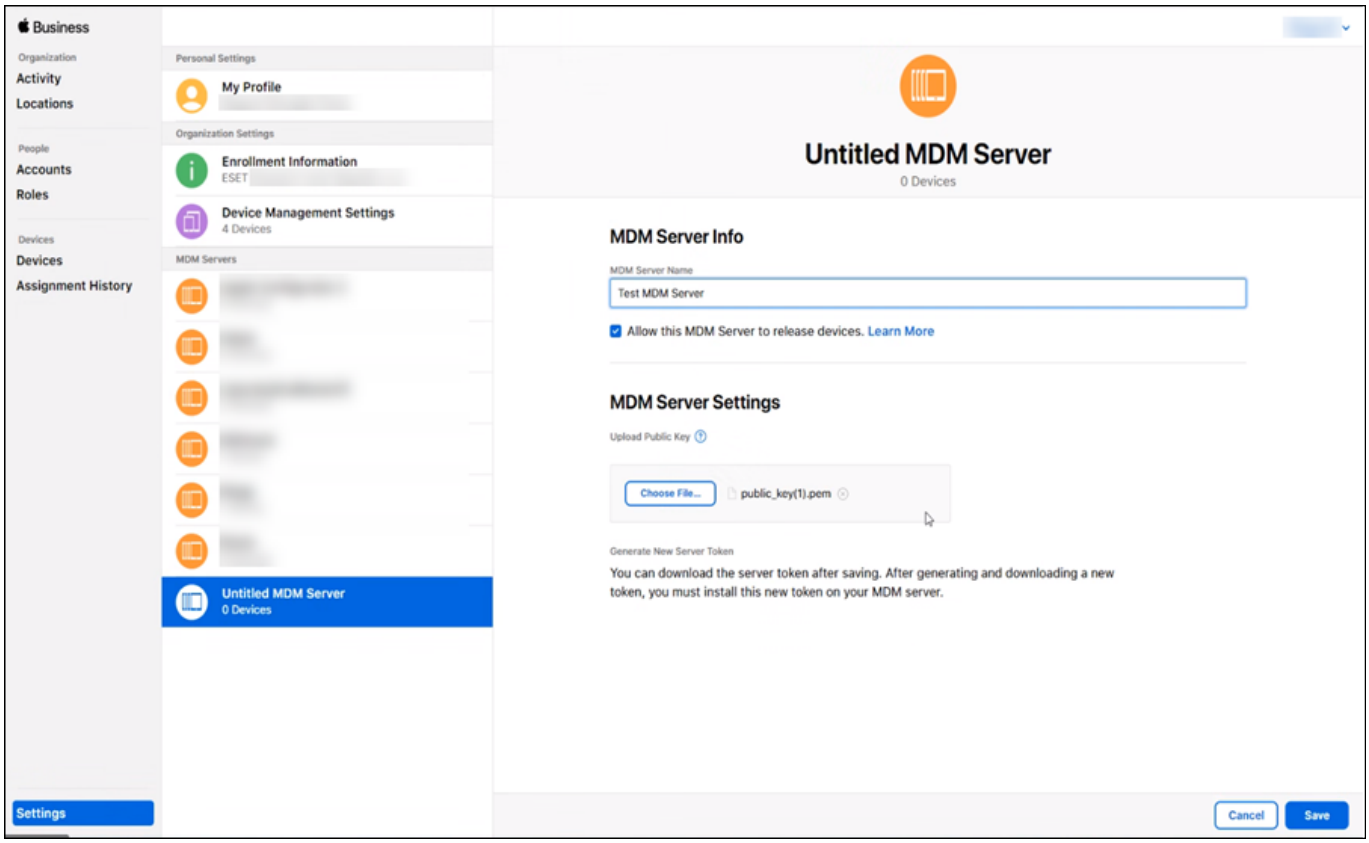
3.Na seção **Configurações de gerenciamento de dispositivo** selecione **Adicionar servidor MDM**.



4.Na tela do Servidor MDM sem título, digite seu **Nome de servidor MDM**, por exemplo: "MDM_Server,".

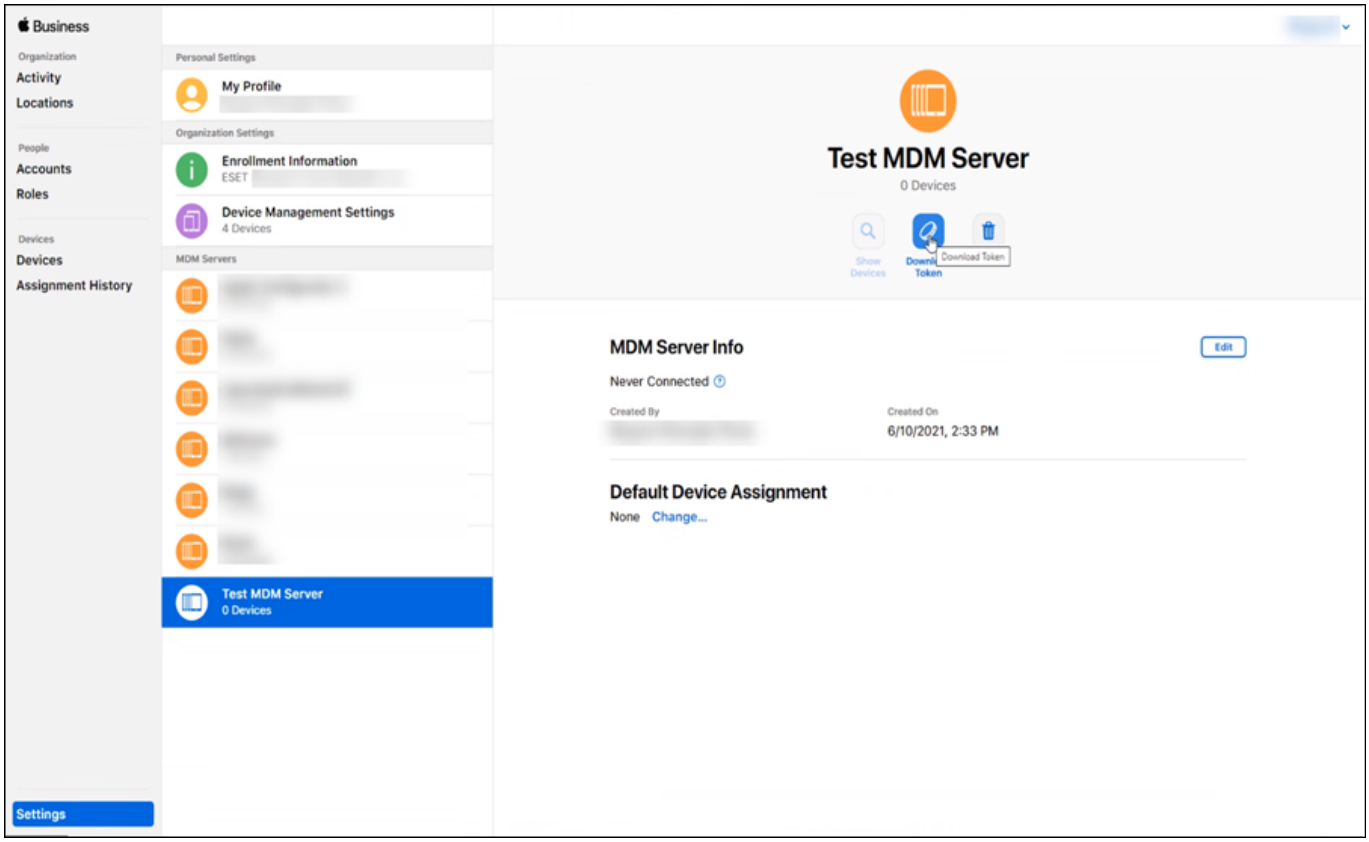


5.Carregue sua chave pública para o portal ABM. Clique em **Escolher arquivo** e selecione o arquivo da chave pública (este é o certificado APNS que você baixou do Portal de Certificado Push da Apple) e clique em **Salvar**.



6.Agora clique no **Token de download** para fazer download do seu Token Apple ABM. Este arquivo deve ser carregado na Política ESET PROTECT MDC sob **Apple Business Manager (ABM)** > **Carregar token de**

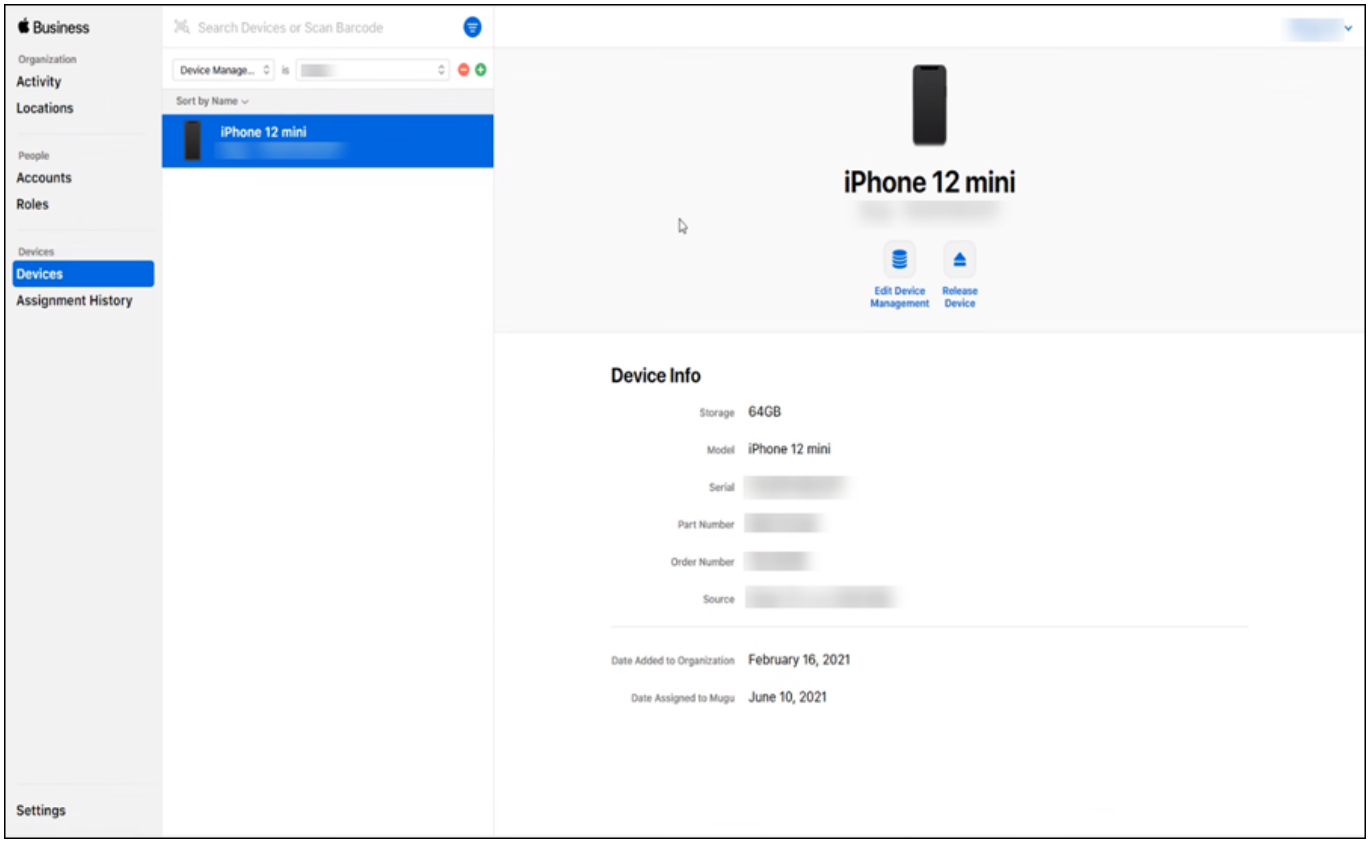
autorização.



Adicionar dispositivo iOS no Apple ABM:

A próxima etapa é atribuir dispositivos iOS ao seu Servidor MDM virtual dentro do portal Apple ABM. Você pode atribuir seus dispositivos iOS por número de série, número de pedido ou carregando uma lista de Números de série para dispositivos de destino no formato CSV. De qualquer forma, você deve Atribuir o dispositivo iOS ao Servidor MDM virtual (criado nas etapas anteriores).

1. Navegue até a seção **Dispositivos** do portal ABM e selecione o dispositivo que deseja atribuir e clique em **Editar gerenciamento de dispositivo**.



2. Depois de selecionar sua lista do servidor MDM, confirme sua seleção e o dispositivo móvel será atribuído ao seu servidor MDM.

Assim que um dispositivo for removido do portal ABM ele é removido permanentemente e não pode ser adicionado de novo.

Depois disso você pode sair do portal Apple ABM e continuar no Web Console ESET PROTECT.

Se você estiver inscrevendo dispositivos iOS que estão atualmente em uso (e que cumprem com os requisitos do dispositivo) novas configurações de política serão aplicadas a eles depois de uma redefinição de fábrica do dispositivo de destino.

Para concluir o processo de inscrição você precisa carregar o certificado APNS na Política MDC que vai ser atribuída ao Servidor MDM. (Esta Política MDC vai cumprir a função das Configurações do servidor MDM).

Se o seu dispositivo iOS exibir a mensagem de que ele não foi capaz de fazer download do perfil da ESET durante a inscrição, verifique se o servidor MDM dentro do ABM está configurado corretamente (possui os certificados corretos) e que você atribuiu o dispositivo iOS correto para seu servidor ESET PROTECT MDM selecionado dentro do Apple ABM.

Inscrição por email

Este método é ideal para a inscrição em massa de dispositivos móveis. Você pode enviar um link de inscrição a qualquer número de dispositivos por email. Cada dispositivo móvel receberá um token exclusivo de uso único vez com base no endereço de email.

É obrigatório configurar um servidor SMTP para inscrição em massa via email. Vá para **Mais** > Configurações, abra **Configurações avançadas** e especifique os Detalhes do servidor SMTP.

1.Para adicionar novos dispositivos móveis, vá para a seção **Computadores**. Selecione o **Grupo estático** ao qual você quer adicionar dispositivos móveis e clique em **Adicionar dispositivo** > **Dispositivos móveis**.

2.Navegue até a seção **Básico**.

3.**Selecionar tipo** – selecione **Android ou iOS/iPadOS**.

4.**Distribuição –** selecione **Enviar e-mail**.

5.**Grupo principal** - se você não tiver um grupo estático específico para dispositivos móveis, recomendamos criar um **Novo grupo estático** (chamado **Dispositivos móveis**, por exemplo). Se você já tem um grupo existente, clique em **All** e uma janela será aberta, onde você pode escolher o Grupo estático.

6.**Personalizar mais configurações**

- O **Mobile Device Connector** será selecionado automaticamente. Se você tiver mais de um MDC, selecione o FQDN do MDC que quer usar. Se você ainda não tiver um conector de dispositivo móvel instalado, consulte os capítulos Instalação do conector de dispositivo móvel - Windows ou Linux deste guia para obter instruções de instalação.

- **Licença** - clique em **Selecionar** e escolha a licença que será usada para ativação. Uma tarefa do cliente de Ativação de Produtos será criada para o dispositivo móvel. Uma unidade de licença será usada (uma para cada dispositivo móvel).

- **Marcações –** selecione ou adicione uma marcação adequada para identificar o dispositivo móvel.

7.Navegue até **Configuração do produto**.

8. Selecione a caixa de seleção **Aceito os termos do Contrato de licença para o usuário final do aplicativo e reconheço a Política de Privacidade**. Consulte o Acordo de Licença para o Usuário Final (EULA), Termos de Uso e Política de Privacidade dos produtos ESET.

9. Navegue até **Lista**.

10. **Lista de dispositivos** - especifique os dispositivos móveis para inscrição, você pode usar as seguintes funções para adicionar dispositivos móveis:

- **Adicionar –** entrada única, você precisa digitar manualmente um endereço de e-mail associado ao dispositivo móvel para onde o e-mail de inscrição será enviado. Se você atribuir um usuário ao dispositivo móvel clicando em **Parear com um usuário existente** e selecionando o usuário, o endereço de e-mail será substituído pelo endereço especificado na tela **Mais** > Usuários do computador. Se você quiser adicionar outro dispositivo móvel, clique em **Adicionar** novamente e envie as informações solicitadas.

- **Adicionar usuário –** você pode adicionar dispositivos selecionando as caixas de verificação adequadas listadas em **Mais** > Usuários do computador. Clique em **Desfazer o par** para fazer correções na lista de dispositivos móveis para inscrição. Assim que você tiver retirado a pareação de um usuário atribuído, o usuário será notado como não pareado. Clique em **Parear** para selecionar o usuário desejado para um dispositivo não pareado. Clique no ícone da **Lixeira** para excluir uma entrada.

• **Importar CSV** - um método que faz com que seja fácil adicionar um grande número de dispositivos móveis. Carregue um arquivo *.csv* contendo uma lista de dispositivos a serem adicionados, veja Importar CSV para mais detalhes.

• **Copiar da área de transferência** – Importa uma lista personalizada de endereços separados por delimitadores personalizados (esse recurso funciona de forma similar ao importar CSV).

> Recomendamos atribuir pelo menos um usuário para um dispositivo móvel. Se quiser usar políticas personalizadas no iOS o usuário deve ser atribuído a um dispositivo.
> Recomendamos especificar o **Nome do dispositivo** em cada entrada ao usar método Importar CSV. Este é o nome do dispositivo exibido na seção **Computadores**. Se você deixar o campo **Nome do dispositivo** vazio, o endereço de email será usado no lugar do nome e aparecerá como Nome do dispositivo em **Computadores** e **Grupos**. Isto pode causar alguma confusão, especialmente caso você use o mesmo endereço de email para inscrever vários dispositivos. Este endereço de email irá aparecer várias vezes e impedi-lo de conseguir distinguir os dispositivos.

11. Navegue até o **Inscrição**.

12. **Visualização de e-mail** – um modelo de mensagem pré-definido contém detalhes necessários para a inscrição por parte do usuário. **Instruções** são mostradas abaixo do **Conteúdo** no email de inscrição e vão conter um **Nome de dispositivo** (ou um endereço de email) com o link de inscrição (URL). Se você usa um endereço de email para inscrever vários dispositivos móveis, uma lista de dispositivos será exibida, cada uma com seu próprio link de inscrição (URL) atribuído. Também existem instruções que o usuário do dispositivo móvel (iOS e Android) deve executar para concluir a inscrição.

13. Ao clicar em **Enviar**, um email será enviado a cada endereço de email com os links de inscrição apropriados e instruções.

14. Para completar a inscrição do dispositivo móvel, siga estas etapas ou peça que os usuários/proprietários dos dispositivos móveis executem as etapas:

- Inscrição de dispositivo Android
- Inscrição de dispositivo iOS

Inscrição individual por link ou código QR

Quando estiver inscrevendo um dispositivo móvel usando o link de inscrição ou código QR, você precisará de acesso físico ao dispositivo. Além disso, para usar o código QR, você precisa ter um aplicativo Leitor/Scanner de código QR instalado no dispositivo móvel.

> Para números grandes de dispositivos móveis, recomendamos usar a Inscrição via email.

1.Para adicionar novos dispositivos móveis, vá para a seção **Computadores**. Selecione o **Grupo estático ao qual você quer adicionar dispositivos móveis** e clique em **Adicionar dispositivo** > **Dispositivos móveis**.

2.Navegue até a seção **Básico**.

3.**Selecionar tipo** – selecione **Android ou iOS/iPadOS**.

4.**Distribuição –** selecione **Escanear código QR**.

5.**Grupo principal** - se você não tiver um grupo estático específico para dispositivos móveis, recomendamos criar um **Novo grupo estático** (chamado **Dispositivos móveis**, por exemplo). Se você já tem um grupo existente, clique em **All** e uma janela será aberta, onde você pode escolher o Grupo estático.

6.**Personalizar mais configurações**

- O **Mobile Device Connector** será selecionado automaticamente. Se você tiver mais de um MDC, selecione o FQDN do MDC que quer usar. Se você ainda não tiver um conector de dispositivo móvel instalado, consulte os capítulos Instalação do conector de dispositivo móvel - Windows ou Linux deste guia para obter instruções de instalação.

- **Licença** - clique em **Selecionar** e escolha a licença que será usada para ativação. Uma tarefa do cliente de Ativação de Produtos será criada para o dispositivo móvel. Uma unidade de licença será usada (uma para cada dispositivo móvel).

- **Marcações –** selecione ou adicione uma marcação adequada para identificar o dispositivo móvel.

7.Navegue até **Configuração do produto**.

8. Selecione a caixa de seleção **Aceito os termos do Contrato de licença para o usuário final do aplicativo e reconheço a Política de Privacidade**. Consulte o Acordo de Licença para o Usuário Final (EULA), Termos de Uso e Política de Privacidade dos produtos ESET.

9. Navegue até **Lista**.

10. **Lista de dispositivos** - especifique os dispositivos móveis para inscrição, você pode usar as seguintes funções para adicionar dispositivos móveis:

- **Adicionar** – entrada única, você precisa digitar manualmente um endereço de e-mail associado ao dispositivo móvel para onde o e-mail de inscrição será enviado. Se você atribuir um usuário ao dispositivo móvel clicando em **Parear com um usuário existente** e selecionando o usuário, o endereço de e-mail será substituído pelo endereço especificado na tela **Mais** > Usuários do computador. Se você quiser adicionar outro dispositivo móvel, clique em **Adicionar** novamente e envie as informações solicitadas.

- **Adicionar usuário** – você pode adicionar dispositivos selecionando as caixas de verificação adequadas listadas em **Mais** > Usuários do computador. Clique em **Desfazer o par** para fazer correções na lista de dispositivos móveis para inscrição. Assim que você tiver retirado a pareação de um usuário atribuído, o usuário será notado como não pareado. Clique em **Parear** para selecionar o usuário desejado para um dispositivo não pareado. Clique no ícone da **Lixeira** para excluir uma entrada.

- **Importar CSV** - um método que faz com que seja fácil adicionar um grande número de dispositivos móveis. Carregue um arquivo *.csv* contendo uma lista de dispositivos a serem adicionados, veja Importar CSV para mais detalhes.

- **Copiar da área de transferência** – Importa uma lista personalizada de endereços separados por delimitadores personalizados (esse recurso funciona de forma similar ao importar CSV).

11. Depois de clicar em **Continuar**, uma lista de dispositivos será exibida com o **Link** de inscrição (URL) correspondente e o **código QR**. Digite toda a URL no navegador da web do dispositivo móvel manualmente (por exemplo *https://eramdm:9980/token*, o token será diferente para cada dispositivo móvel) ou envie esta URL para o dispositivo móvel por outros meios. Alternativamente, você pode usar um **Código QR**

fornecido, que pode ser mais conveniente do que digitar o URL, mas requer um Leitor/Scanner de código QR no dispositivo móvel.

12. Depois de ter concluído a inscrição de todos os dispositivos selecionados, clique em **Concluir**.

13. Para realizar a inscrição real dos dispositivos móveis, siga estas instruções passo-a-passo:

- Inscrição de dispositivo Android
- Inscrição de dispositivo iOS

Proprietário do dispositivo Android (apenas Android 7 e versões superiores)

Quando estiver inscrevendo um dispositivo móvel Android usando o link de inscrição ou código QR, você precisará de acesso físico ao dispositivo. Além disso, essa inscrição é possível apenas em um dispositivo depois de uma limpeza/redefinição de fábrica ou que acabou de sair da caixa.

> Não é possível usar a Inscrição por email para a inscrição em massa de dispositivos Android como um Proprietário de dispositivo.

1.Para adicionar novos dispositivos móveis, vá para a seção **Computadores**. Selecione o **Grupo estático ao qual você quer adicionar dispositivos móveis** e clique em **Adicionar dispositivo** > **Dispositivos móveis**.

2.Navegue até a seção **Básico**.

3.**Selecionar tipo** – Selecione **Proprietário do dispositivo Android (apenas Android 7 e versões superiores)**.

4.**Distribuição –** selecione **Escanear código QR**.

5.**Grupo principal** - se você não tiver um grupo estático específico para dispositivos móveis, recomendamos criar um **Novo grupo estático** (chamado **Dispositivos móveis**, por exemplo). Se você já tem um grupo existente, clique em **All** e uma janela será aberta, onde você pode escolher o Grupo estático.

6.**Personalizar mais configurações**

- O **Mobile Device Connector** será selecionado automaticamente. Se você tiver mais de um MDC, selecione o FQDN do MDC que quer usar. Se você ainda não tiver um conector de dispositivo móvel instalado, consulte os capítulos Instalação do conector de dispositivo móvel - Windows ou Linux deste guia para obter instruções de instalação.
- **Licença** - clique em **Selecionar** e escolha a licença que será usada para ativação. Uma tarefa do cliente de Ativação de Produtos será criada para o dispositivo móvel. Uma unidade de licença será usada (uma para cada dispositivo móvel).
- **Marcações –** selecione ou adicione uma marcação adequada para identificar o dispositivo móvel.

7.Navegue até **Configuração do produto**.

8. Selecione a caixa de seleção **Aceito os termos do Contrato de licença para o usuário final do aplicativo e reconheço a Política de Privacidade**. Consulte o Acordo de Licença para o Usuário Final (EULA), Termos de Uso e Política de Privacidade dos produtos ESET.

9. Navegue até **Lista**.

10. **Lista de dispositivos** - especifique os dispositivos móveis para inscrição, você pode usar as seguintes funções para adicionar dispositivos móveis:

- **Adicionar** – entrada única, você precisa digitar manualmente um endereço de e-mail associado ao dispositivo móvel para onde o e-mail de inscrição será enviado. Se você atribuir um usuário ao dispositivo móvel clicando em **Parear com um usuário existente** e selecionando o usuário, o endereço de e-mail será substituído pelo endereço especificado na tela **Mais** > Usuários do computador. Se você quiser adicionar outro dispositivo móvel, clique em **Adicionar** novamente e envie as informações solicitadas.

- **Adicionar usuário** – você pode adicionar dispositivos selecionando as caixas de verificação adequadas listadas em **Mais** > Usuários do computador. Clique em **Desfazer o par** para fazer correções na lista de dispositivos móveis para inscrição. Assim que você tiver retirado a pareação de um usuário atribuído, o usuário será notado como não pareado. Clique em **Parear** para selecionar o usuário desejado para um dispositivo não pareado. Clique no ícone da **Lixeira** para excluir uma entrada.

- **Importar CSV** - um método que faz com que seja fácil adicionar um grande número de dispositivos móveis. Carregue um arquivo *.csv* contendo uma lista de dispositivos a serem adicionados, veja Importar CSV para mais detalhes.

- **Copiar da área de transferência** – Importa uma lista personalizada de endereços separados por delimitadores personalizados (esse recurso funciona de forma similar ao importar CSV).

11. Depois de clicar em **Continuar**, uma lista de dispositivos será exibida com o **Link** de inscrição (URL) correspondente e o **código QR**. Digite toda a URL no navegador da web do dispositivo móvel manualmente (por exemplo *https://eramdm:9980/token*, o token será diferente para cada dispositivo móvel) ou envie esta URL para o dispositivo móvel por outros meios. Alternativamente, você pode usar um **Código QR** fornecido, que pode ser mais conveniente do que digitar o URL, mas requer um Leitor/Scanner de código QR no dispositivo móvel.

12. Depois de ter concluído a inscrição de todos os dispositivos selecionados, clique em **Concluir**.

13. Siga essas etapas no dispositivo Android para realizar o processo de inscrição.

Criar uma política para iOS MDM - Conta Exchange ActiveSync

Esta política governa todas as configurações para o dispositivo iOS. Essas configurações se aplicam para dispositivos iOS ABM e não ABM.

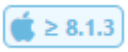
- As configurações apenas ABM são denotadas com um ícone ABM 

. Essas configurações são aplicáveis apenas aos dispositivos iOS inscritos no portal Apple ABM. Recomendamos que você não personalize essas configurações apenas ABM ao criar uma política para dispositivos iOS que não são ABM.

• Algumas configurações só podem ser aplicadas para um dispositivo iOS com uma determinada versão do iOS. Essas configurações são marcadas por um ícone representando a versão iOS.

  o iOS versão 9.0 e versões superiores 

  o iOS versão 9.3 e versões superiores 

  o iOS versão 8.1.3 e versões superiores 

  oiOS versão 11.0 e versões superiores 

• Se ambos os ícones (ícone ABM e ícone da versão iOS) estiverem presentes ao lado de uma configuração específica, o dispositivo deve cumprir com ambos os requisitos ou o gerenciamento da configuração vai falhar.

Veja o cenário de amostra abaixo que explica como usar a política MDM iOS quando você quiser criar uma conta de Email Microsoft Exchange:

Você pode usar essa política para configurar uma conta de email, contatos e calendário do Microsoft Exchange em dispositivos móveis iOS do usuário. A vantagem de usar essa política é você só precisa criar uma política que então pode ser aplicada a muitos dispositivos móveis iOS sem precisar configurar cada um separadamente. Isso é possível usando os atributos de usuário do Active Directory. Você precisa especificar uma variável, por exemplo `${exchange_login/exchange}` e isto será substituído por um valor do AD para um usuário em particular.

Se você não usar o Microsoft Exchange ou Exchange ActiveSync, é possível configurar manualmente cada serviço (**Contas de email**, **Contas de contato**, **Contas LDAP**, **Contas de agenda** e **Contas de agenda inscritas**).

O seguinte é um exemplo de como criar e aplicar uma nova política para definir automaticamente o Email, Contatos e Calendário para cada usuário no dispositivo móvel iOS usando o protocolo Exchange ActiveSync (EAS) para sincronizar esses serviços.

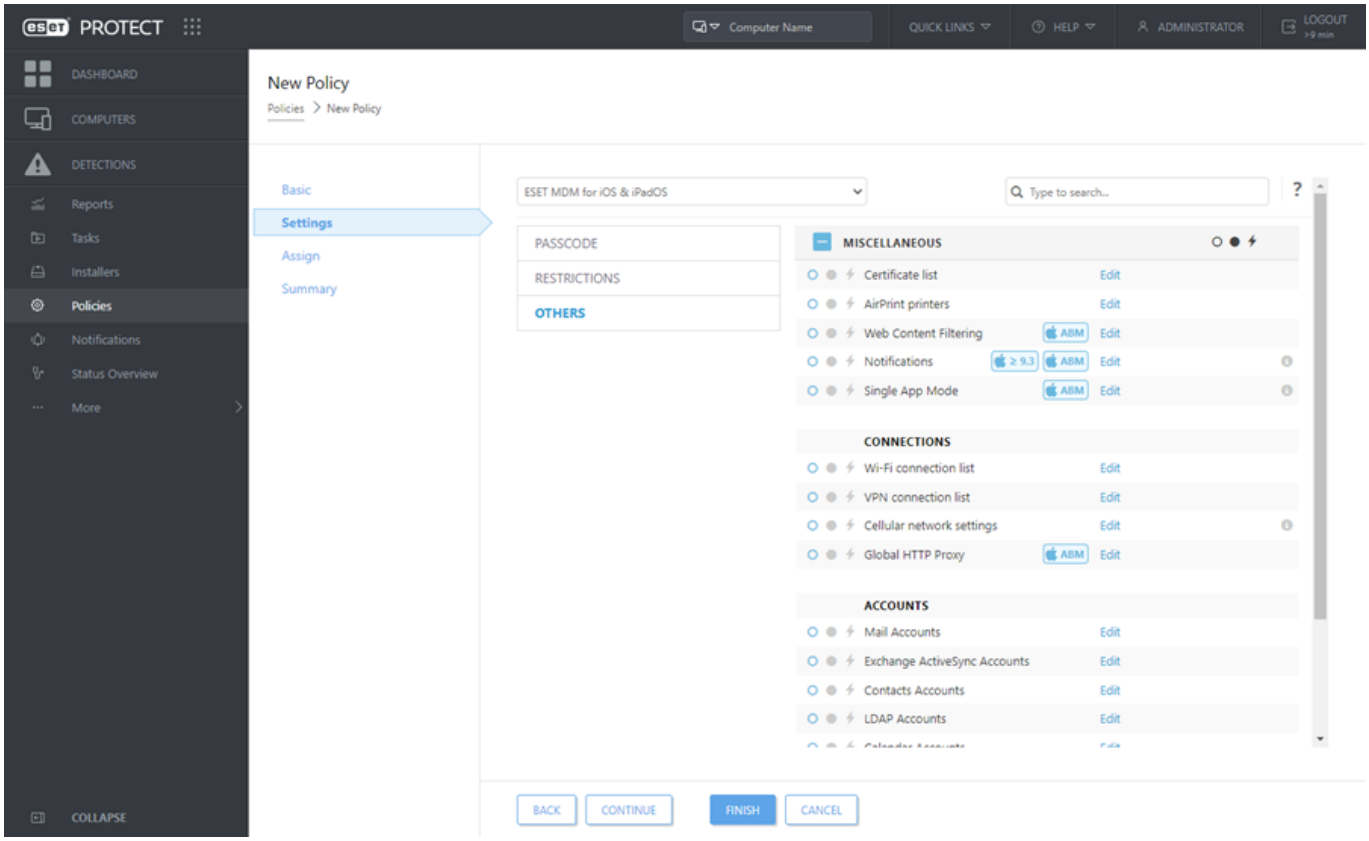
> Antes de começar a configurar essa política, certifique-se de já ter realizado as etapas descritas em Gestão de dispositivo móvel.

Básico

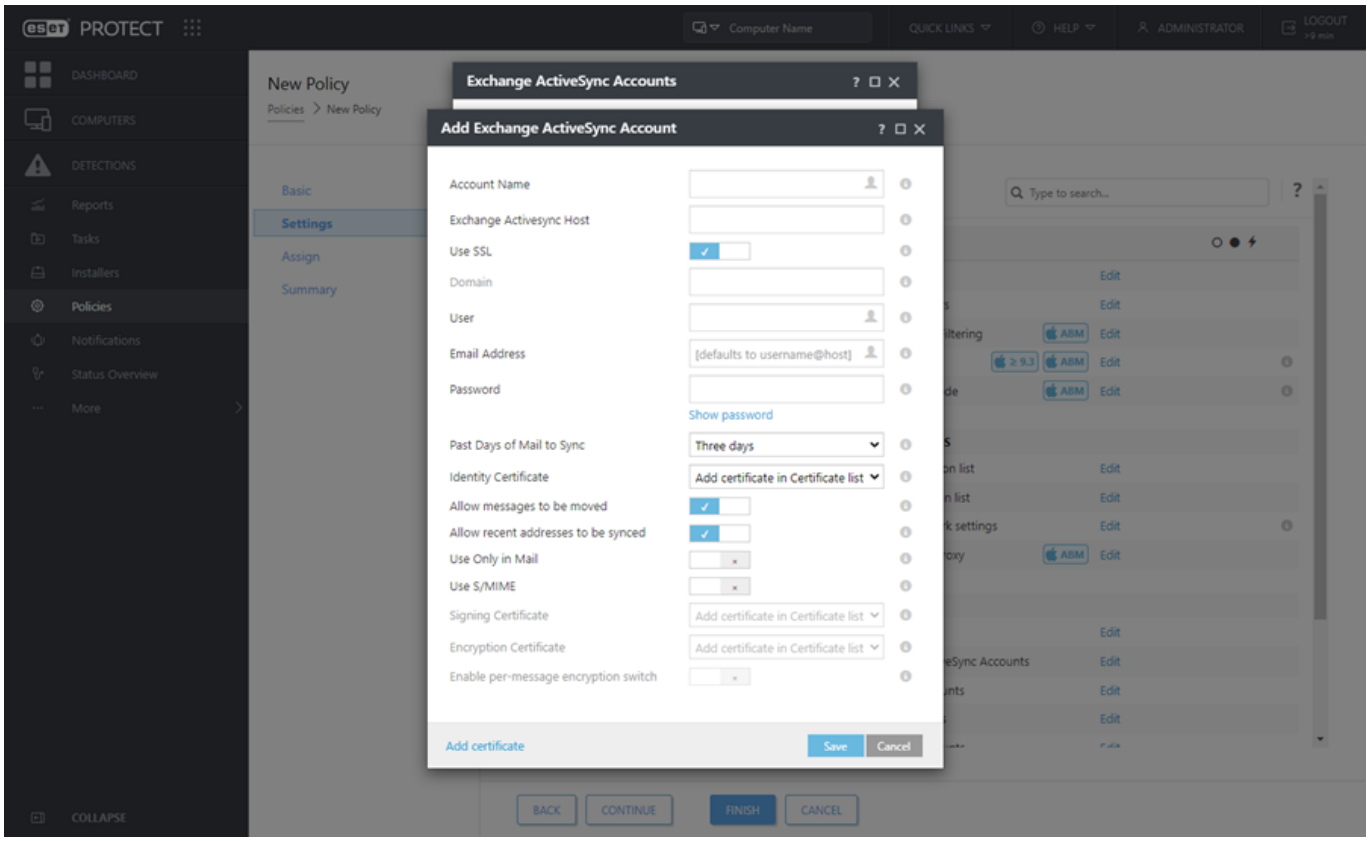
Digite um **Nome** para a política. O campo **Descrição** é opcional.

Configurações

Selecione **MDM ESET para iOS/iPadOS** da lista suspensa, clique em **Outros** para abrir categorias e clique em **Editar** ao lado de **Contas Exchange ActiveSync**.



Clique em **Adicionar** e especifique os detalhes da sua conta Exchange ActiveSync. Você pode usar variáveis para certos campos (selecione a partir da lista suspensa), como Usuário ou Endereço de email. Eles serão substituídos por valores reais de Usuários do computador quando uma política é aplicada.



- **Nome da conta** - Digite o nome da conta Exchange.
- **Host do Exchange ActiveSync** - Especifique o nome de host do servidor Exchange ou seu endereço IP.

• **Usar SSL** - Essa opção está ativada por padrão. Isso especifica se o Exchange Server usa Secure Sockets Layer (SSL) para autenticação.

• **Domínio** - Este campo é obrigatório. Você pode inserir o domínio ao qual essa conta pertence.

• **Usuário** - Nome de login do Exchange. Selecione a variável adequada na lista suspensa para usar um atributo do seu Active Directory para cada usuário.

• **Endereço de email** - Selecione a variável adequada na lista suspensa para usar um atributo do seu Active Directory para cada usuário.

• **Senha** - Opcional. Recomendamos que você deixe esse campo vazio. Se isso ficar vazio os usuários serão solicitados a criarem suas próprias senhas.

• **Dias anteriores de email a sincronizar** - Selecione o número de dias anteriores de email a sincronizar na lista suspensa.

• **Certificado de identidade** - Credenciais para conexão ao ActiveSync.

• **Permitir que as mensagens sejam movidas** - Se ativado, as mensagens podem ser movidas de uma conta para outra.

• **Permitir que os endereços recentes sejam sincronizados** - Se esta opção for ativada, o usuário pode sincronizar endereços usados recentemente em dispositivos diferentes.

• **Usar apenas no Email** - Ative esta opção se você deseja permitir que apenas o aplicativo Email envie emails a partir desta conta.

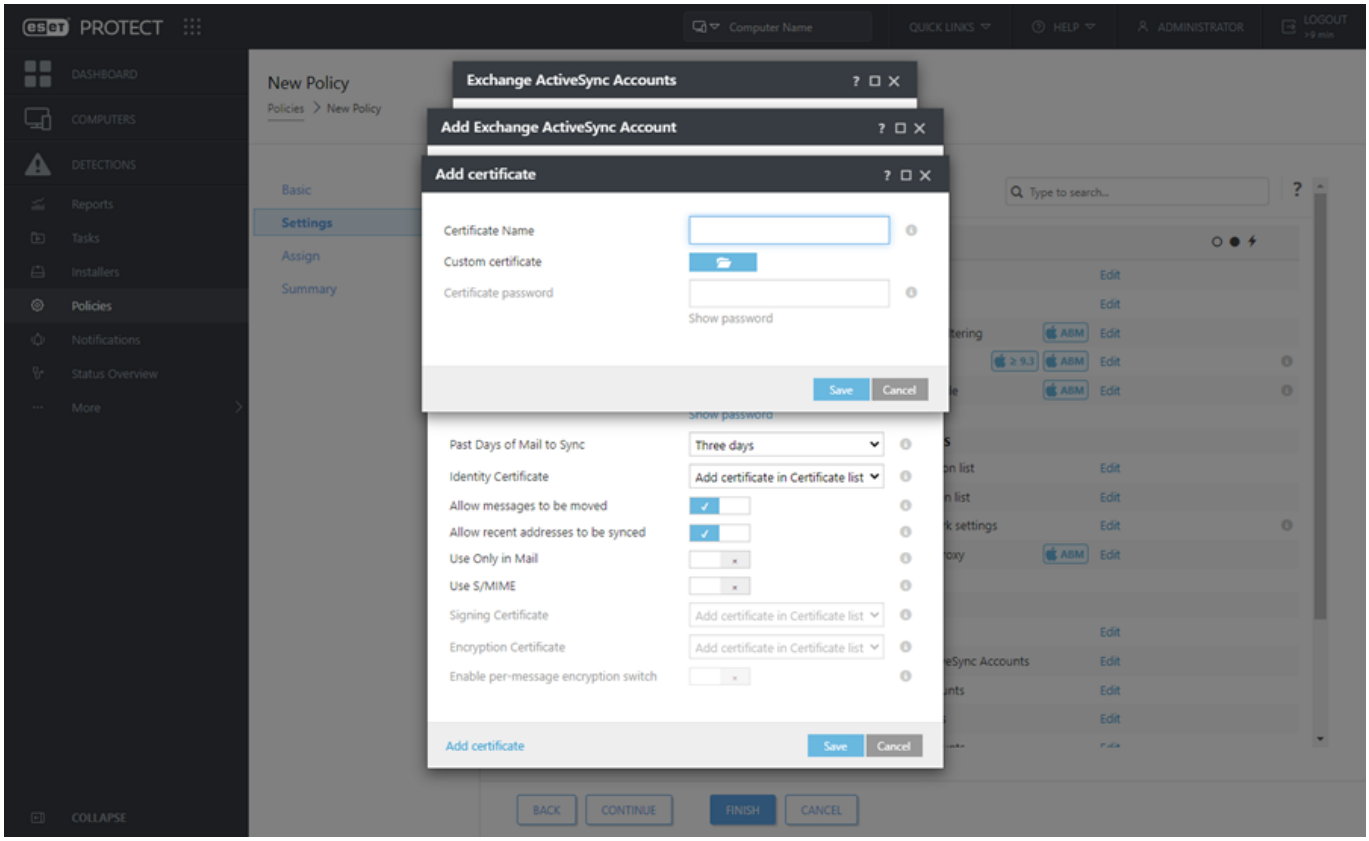
• **Usar S/MIME** - Ative essa opção para usar a criptografia S/MIME para mensagens de email enviadas.

• **Assinatura de certificado** - Credencias para assinatura de dados MIME.

• **Certificado de criptografia** - Credencias para criptografia de dados MIME.

• **Ativar alternância de criptografia por mensagem** – permite ao usuário escolher se vai criptografar cada mensagem.

> Se você não especificar um valor e deixar o campo em branco, os usuários de dispositivos móveis serão solicitados a inserir esse valor. Por exemplo, uma **Senha**.

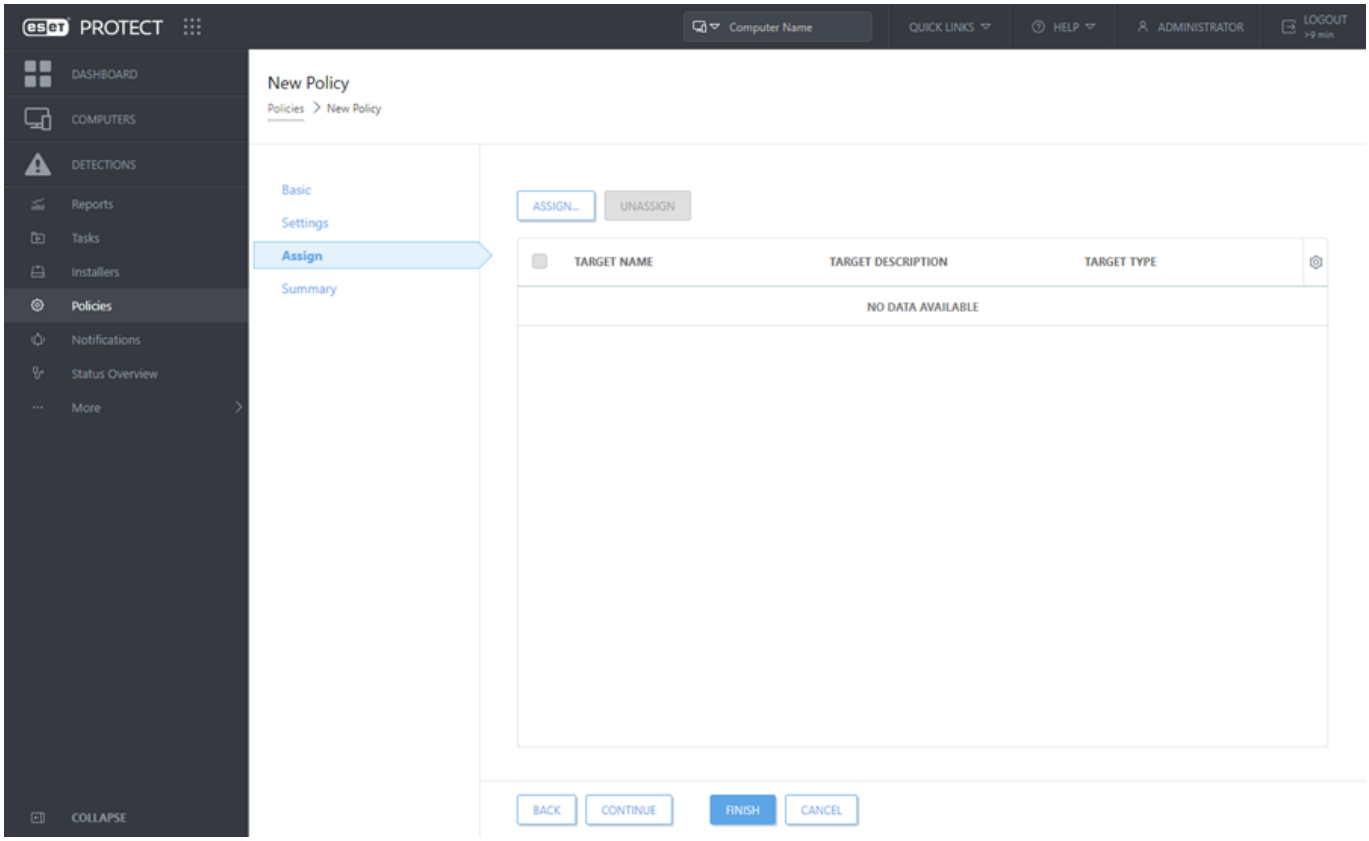


- **Adicionar certificado**- É possível adicionar certificados Exchange específicos (Identidade do usuário, Assinatura digital ou Certificado de criptografia) se necessário.

> Usando as etapas acima, você pode adicionar várias contas do Exchange ActiveSync, se desejar. Assim, haverá mais contas configuradas em um dispositivo móvel. Você também pode editar contas existentes, se necessário.

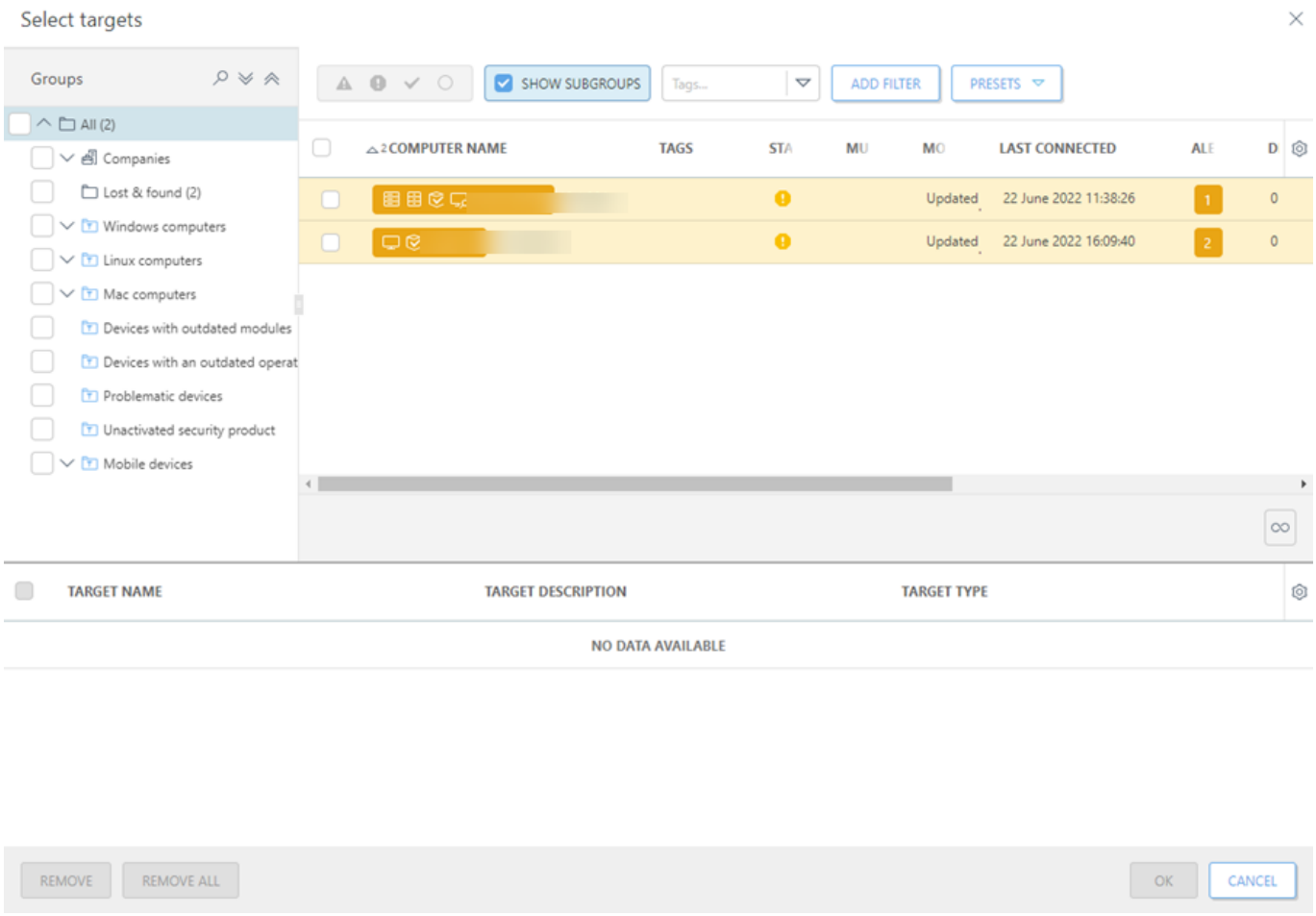
Atribuir

Especifique os clientes (computadores individuais/dispositivos móveis ou grupos inteiros) que serão os destinatários dessa política.



Clique em **Atribuir** para exibir todos os grupos estáticos e dinâmicos e seus membros. Selecione seus computadores ou grupos desejados e clique em **OK**.

Para atribuir todos os computadores em um grupo, atribua o grupo em vez de computadores individuais para impedir que a velocidade do Web Console diminua.
O Web Console exibirá um aviso se você selecionar um grande número de computadores.



Resumo

Verifique as configurações para esta política e clique em **Concluir**. A política é aplicada aos destinos depois da próxima conexão com o Servidor ESET PROTECT (dependendo do intervalo de conexão do agente).

Criar uma política para MDC para ativar APN/ABM para inscrição iOS

Ao alterar o certificado https usado em sua política para o MDC, siga as etapas abaixo para evitar desconectar os dispositivos móveis do seu MDM:
1. Criar e aplicar a nova política que usa o novo certificado https.
2. Permitir que os dispositivos verifiquem o servidor MDM e recebam a nova política.
3. Verifique se os dispositivos estão usando o novo certificado https (a troca de certificado https foi concluída).
4. Permitir pelo menos 72 horas para que seus dispositivos recebam a nova política. Depois de todos os dispositivos terem recebido a nova política (o alerta MDM Core “Alteração de certificado HTTPS ainda em andamento. O certificado antigo ainda está sendo usado” não é mais exibido na guia Alertas), você pode excluir a política antiga.

Este é um exemplo de como criar uma nova política para o Conector de dispositivo móvel ESET para ativar o APNS (Serviços de notificação por push da Apple) e o recurso do programa de inscrição de dispositivo móvel iOS. Isto é necessário para a inscrição de dispositivo iOS. Antes de configurar essa política, crie um novo certificado APN e faça com que ele seja assinado pela Apple no Portal de Certificados Push da Apple para que se torne um

certificado assinado ou **Certificado APN**. Para instruções passo a passo veja a seção Certificado APN.

Básico

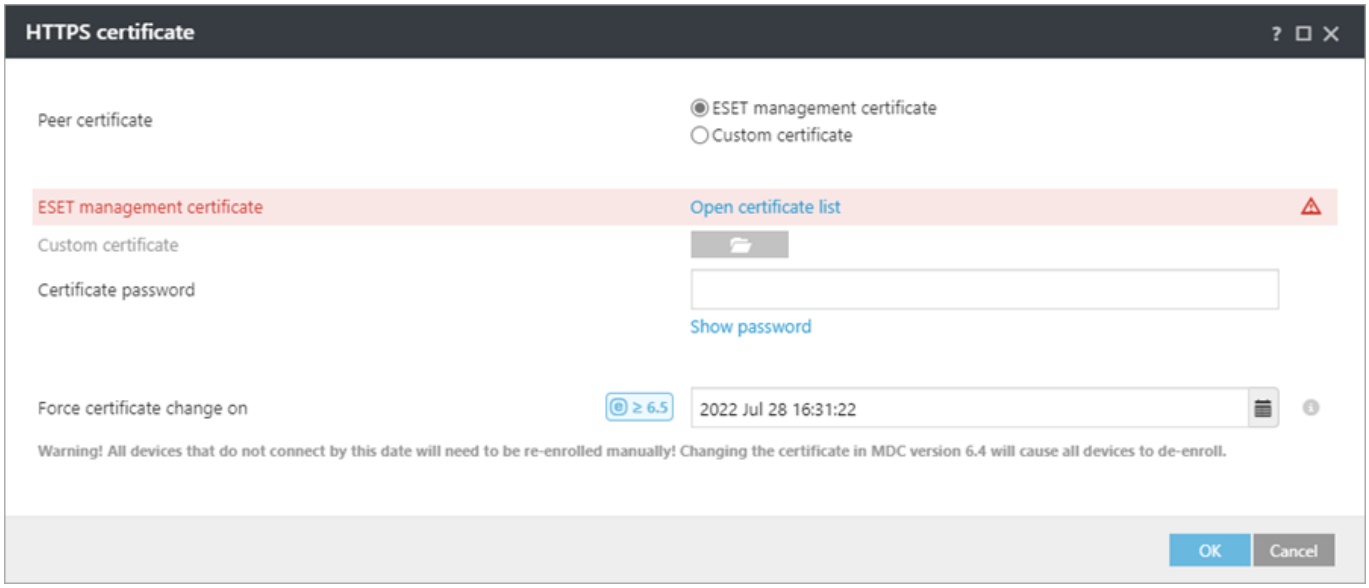
Digite um **Nome** para a política. O campo **Descrição** é opcional.

Configurações

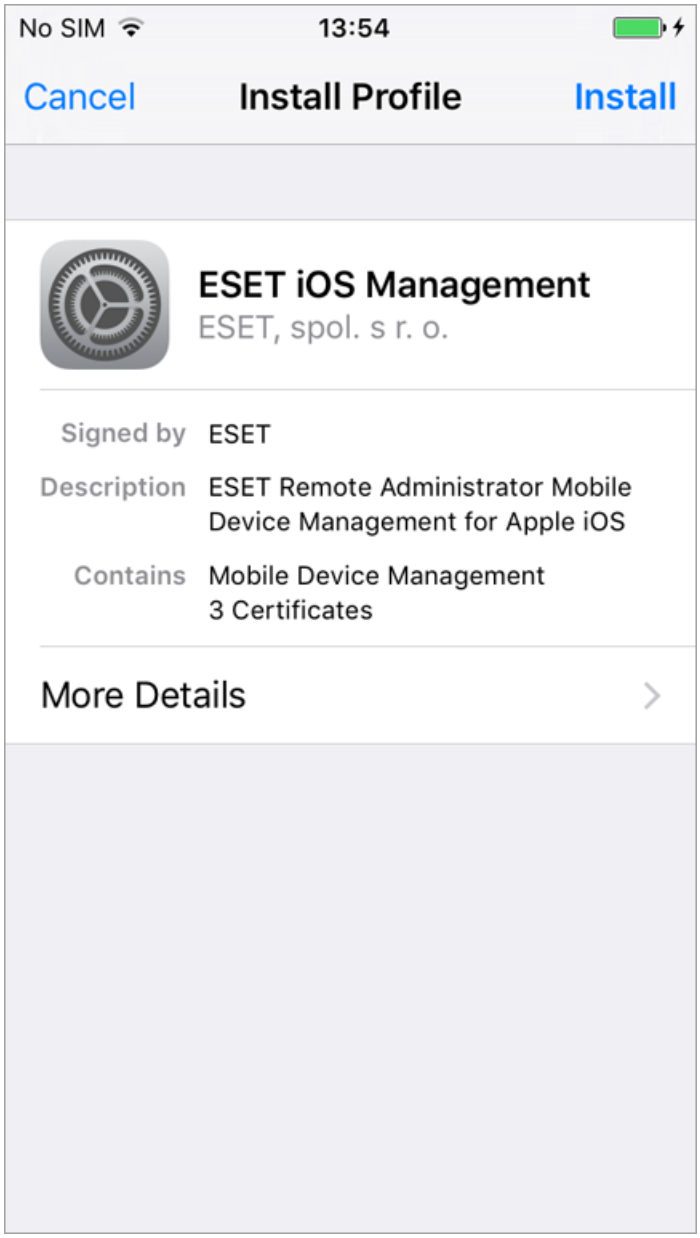
Selecione **Conector de dispositivo móvel** da lista suspensa.

Se você instalou o Servidor MDM com o Instalador Tudo-em-um (não como autônomo e não como componente) o certificado HTTPS será gerado automaticamente durante a instalação. Para todos os outros casos você precisará aplicar um certificado HTTPS personalizado. Você pode encontrar mais informações anotadas seguindo a etapa um do tópico de Gerenciamento de dispositivo móvel.
Você pode usar o Certificado ESET PROTECT (assinado pela ESET PROTECT CA) ou seu certificado personalizado. Você também pode especificar a data para **Forçar alteração de certificado**. Clique na dica de ferramentas ao lado desta configuração para obter mais informações.

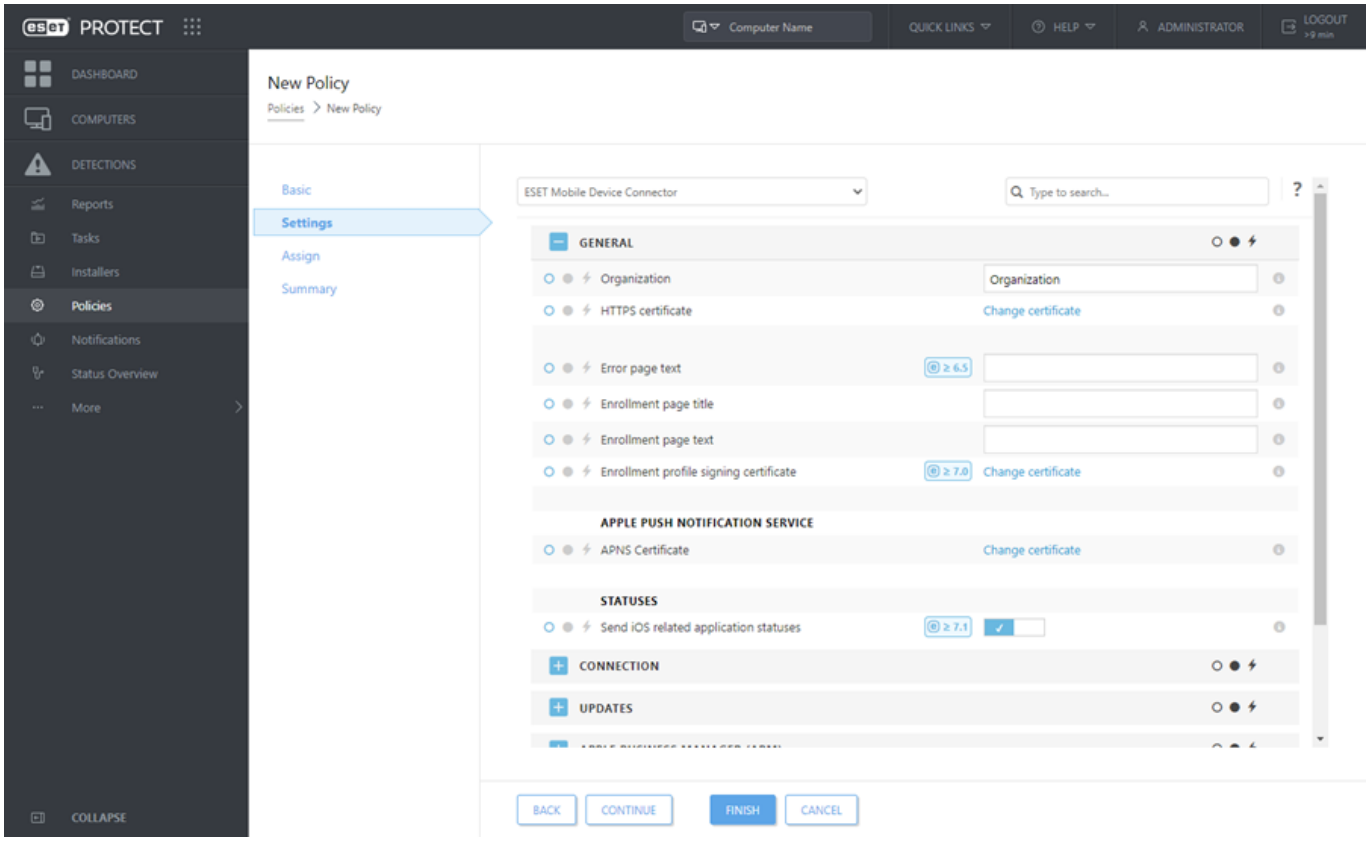
Digite seu nome de organização real na string **Organização**. Isto é usado pelo gerador de perfil de inscrição para incluir esta informação no perfil.



Em **Geral**, você pode opcionalmente carregar seu certificado HTTPS para inscrição no **Certificado de assinatura de perfil de inscrição** (isso afeta apenas a inscrição não ABM). Isso vai permitir que a página de inscrição para dispositivos iOS que foram visitadas durante o processo de inscrição sejam assinadas e que elas estarão visíveis em **Assinado por** preenchido com base no certificado.

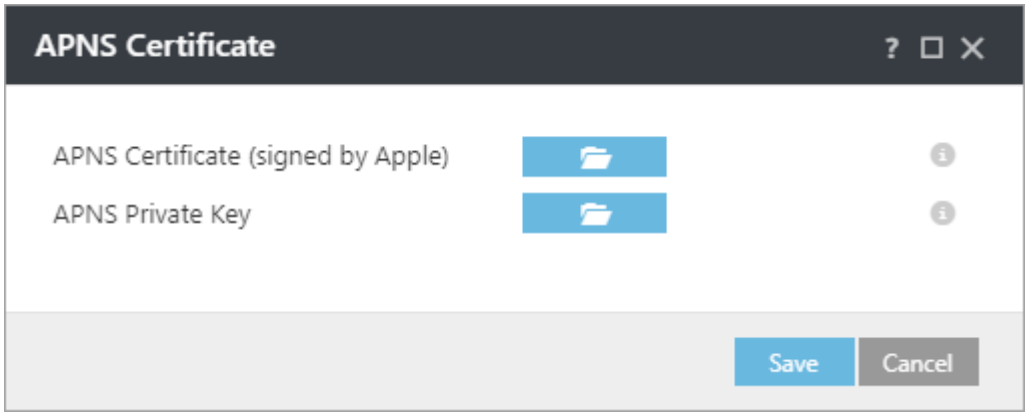


Carregar os certificados Apple para inscrição iOS – vá para o Serviço de notificação por push da Apple e carregue o Certificado APNS e uma Chave privada APNS.



Certificado APNS (assinado pela Apple) - clique no ícone de pasta e procure o Certificado APNS para fazer o upload dele. O Certificado APNS o arquivo que você fez o download do Portal de Certificados Push da Apple.

Chave privada APNS - clique no ícone de pasta e procure a Chave privada APNS para fazer o upload dela. A Chave privada APNS é o arquivo que você fez o download durante a criação do Certificado APN/ABM.



Programa de melhoria do produto - Ativa ou desativa a transmissão de relatórios de parada e dados de telemetria anônimos para a ESET.

Registro em relatório > **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).

Se você estiver criando esta política para inscrição iOS com o Apple ABM, vá até o **Apple Business Manager (ABM)**.

Apple Business Manager (ABM) – essas configurações são apenas para ABM. ABM

Depois da configuração inicial, se qualquer uma dessas configurações tiver que ser alterada, para aplicar as alterações você precisará fazer uma redefinição de fábrica e inscrever novamente todos os dispositivos iOS afetados.

Carregar token de autorização – clique no ícone de pasta e procure o token de servidor ABM. O token de servidor ABM é o arquivo que você fez download quando criou o servidor virtual MDM no portal Apple ABM.

Instalação obrigatória - o usuário não conseguirá usar o dispositivo sem instalar o perfil MDM.

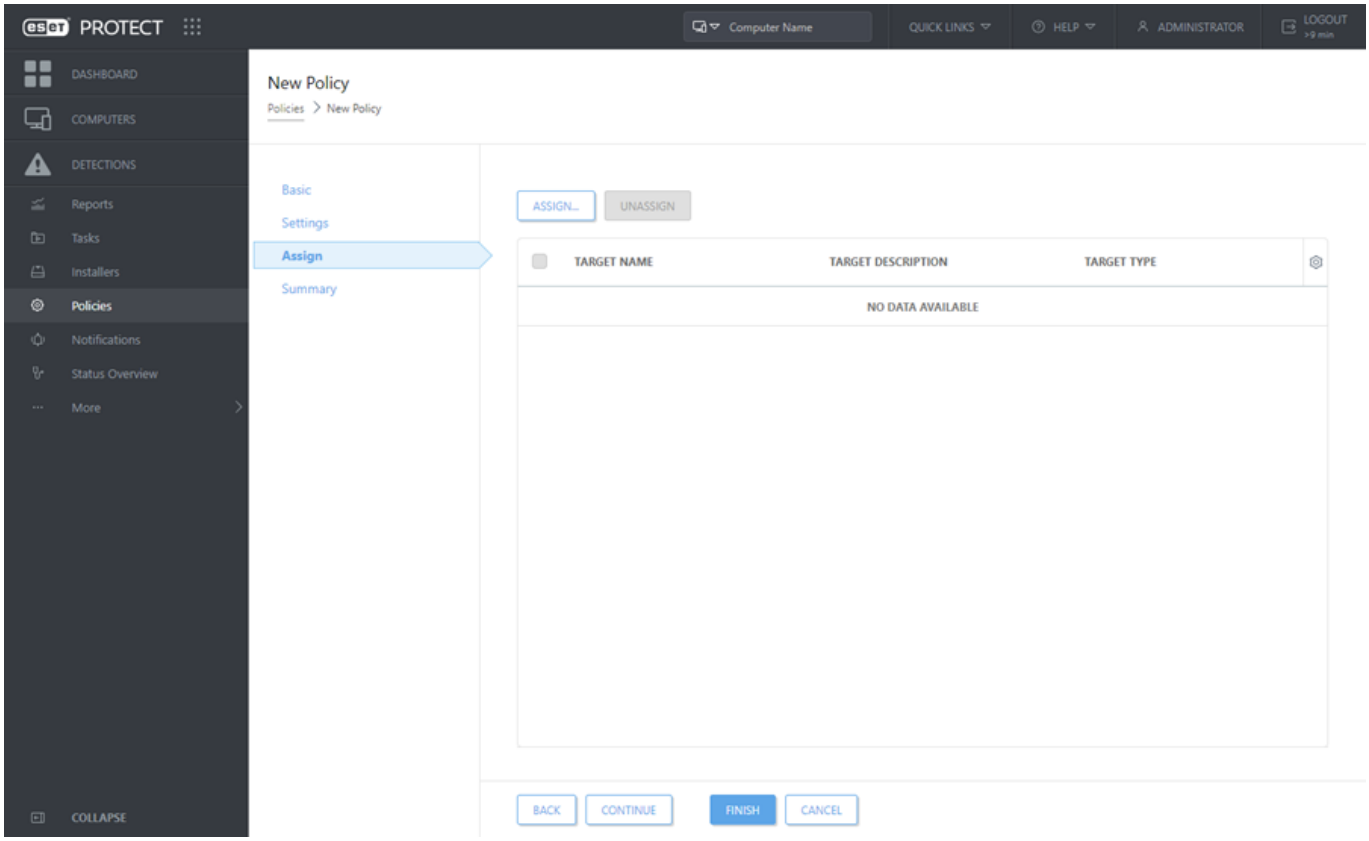
Permitir que o usuário remova o perfil MDM - o dispositivo deve estar no modo supervisionado para impedir o usuário de remover o perfil MDM.

Requer login de domínio - o usuário precisará usar credenciais válidas de domínio no assistente de configuração do dispositivo.

Ignorar itens de configuração - essa configuração permite a você escolher qual das etapas da configuração inicial durante a configuração iOS serão ignoradas. Você pode encontrar mais informações sobre cada uma dessas etapas no artigo da Base de conhecimento Apple.

Atribuir

Selecione o dispositivo que é host do servidor MDM da política de destino.



Clique em **Atribuir** para exibir todos os grupos estáticos e dinâmicos e seus membros. Selecione a instância do Conector de dispositivo móvel na qual você deseja aplicar a política e clique em **OK**.

Resumo

Verifique as configurações para esta política e clique em **Concluir**.

Criar uma política para aplicar restrições no iOS e adicionar conexão de Wi-Fi

Você pode criar uma política para dispositivos móveis iOS para aplicar certas restrições. Você também pode definir várias conexões Wi-Fi para que, por exemplo, os usuários sejam automaticamente conectados à rede Wi-Fi corporativa em diferentes localizações de escritórios. O mesmo se aplica a conexões VPN.

Restrições que podem ser aplicadas ao dispositivo móvel iOS estão listadas em categorias. Por exemplo, você pode desativar o FaceTime e o uso da câmera, desativar certos recursos do iCloud, ajustar as opções de Segurança e privacidade ou desativar aplicativos selecionados.

> Restrições que podem ou não podem ser aplicadas dependem da versão do iOS usada por dispositivos do cliente. iOS 8.x e mais recente são compatíveis.

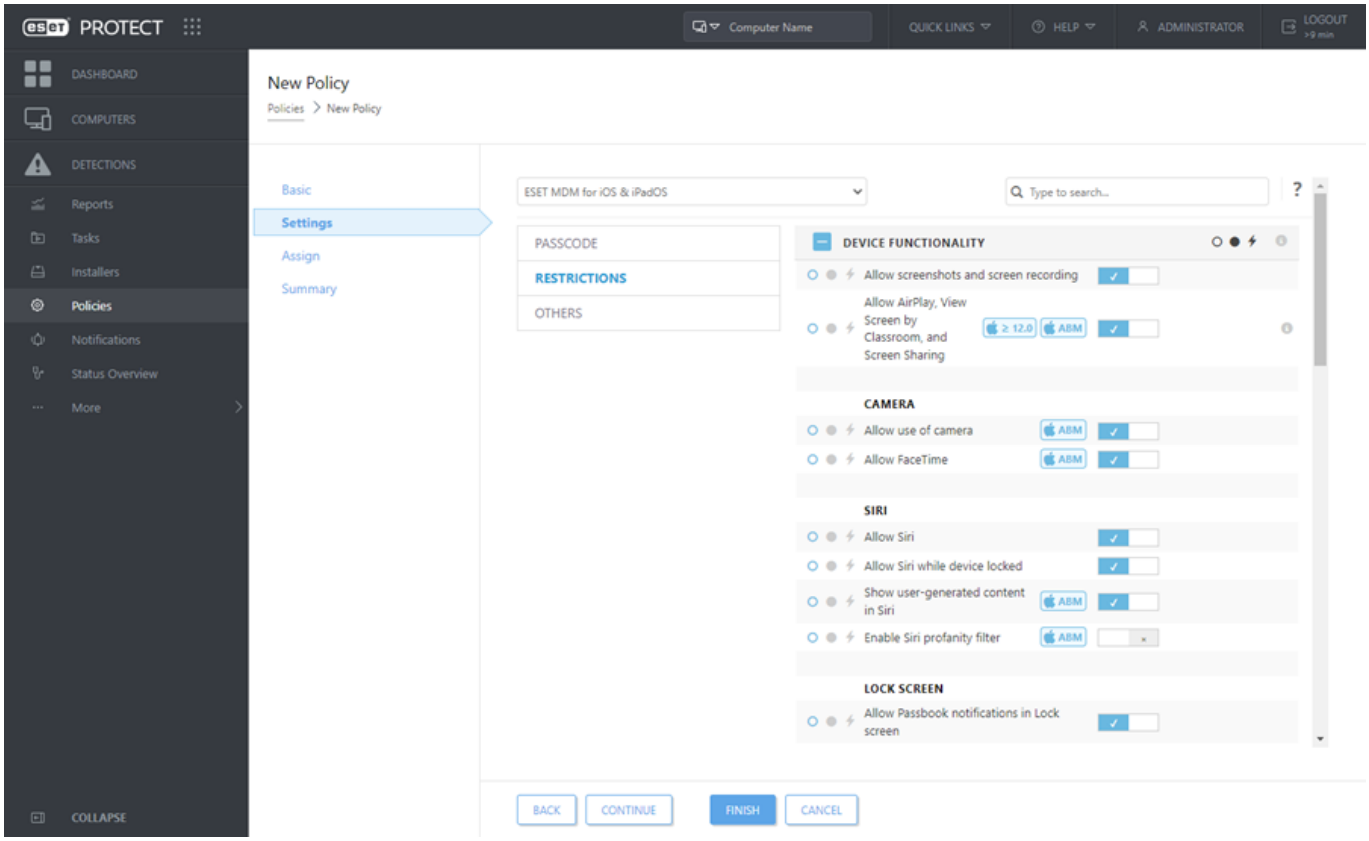
O seguinte é um exemplo de como desabilitar os **aplicativos** de **câmera e** FaceTime e adicionar detalhes da conexão Wi-Fi na lista, para que o dispositivo móvel iOS conecte a uma rede Wi-Fi sempre que a rede for detectada. Se você usar a opção Ingressar automaticamente, dispositivos móveis iOS serão conectados a essa rede por padrão. A configuração de política irá substituir a seleção manual de uma rede Wi-Fi por um usuário.

Básico

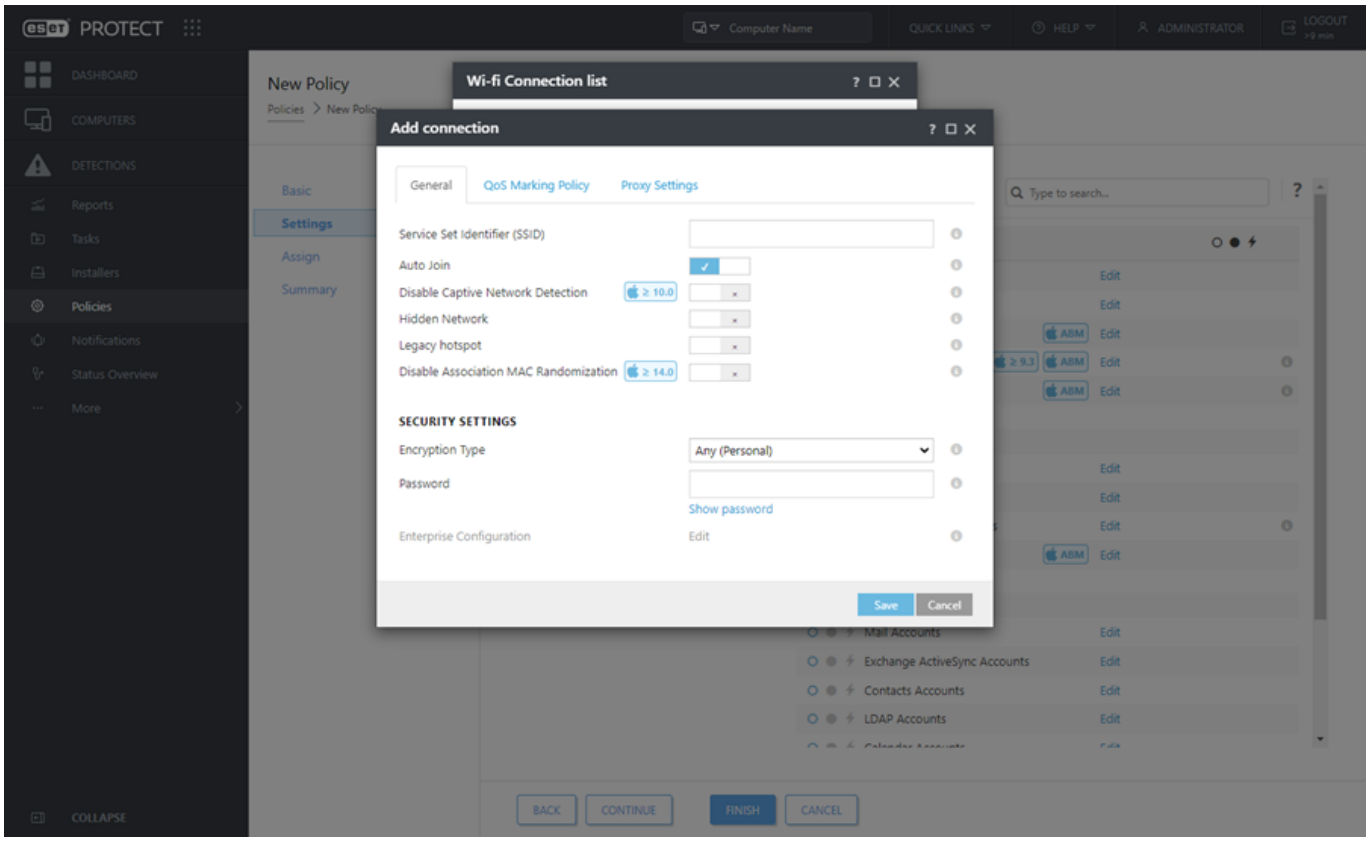
Digite um **Nome** para a política. O campo **Descrição** é opcional.

Configurações

Selecione **Gestão de dispositivo móvel ESET para iOS**, clique em **Restrições** para ver categorias. Use a alternância ao lado de **Permitir uso da câmera** para desativar. Como a câmera está desativada, o FaceTime será automaticamente desativado também. Se quiser desativar apenas o FaceTime, deixe a câmera ativada e use a alternância ao lado de **Permitir FaceTime** para que ele seja desativado.



Depois de ter configurado as **Restrições**, clique em **Outros** e depois em **Editar** ao lado da **Lista de conexão Wi-Fi**. Será aberta uma janela com a lista de conexões wi-fi. Clique em **Adicionar** e especifique detalhes de conexão para a rede Wi-Fi que você deseja adicionar. Clique em **Salvar**.



- **Identificador de conjunto de serviço (SSID)** - SSID da rede Wi-Fi a ser usada.
- **Ingressar automaticamente** - opcional (ativado por padrão), o dispositivo ingressa na rede

automaticamente.

Configurações de segurança:

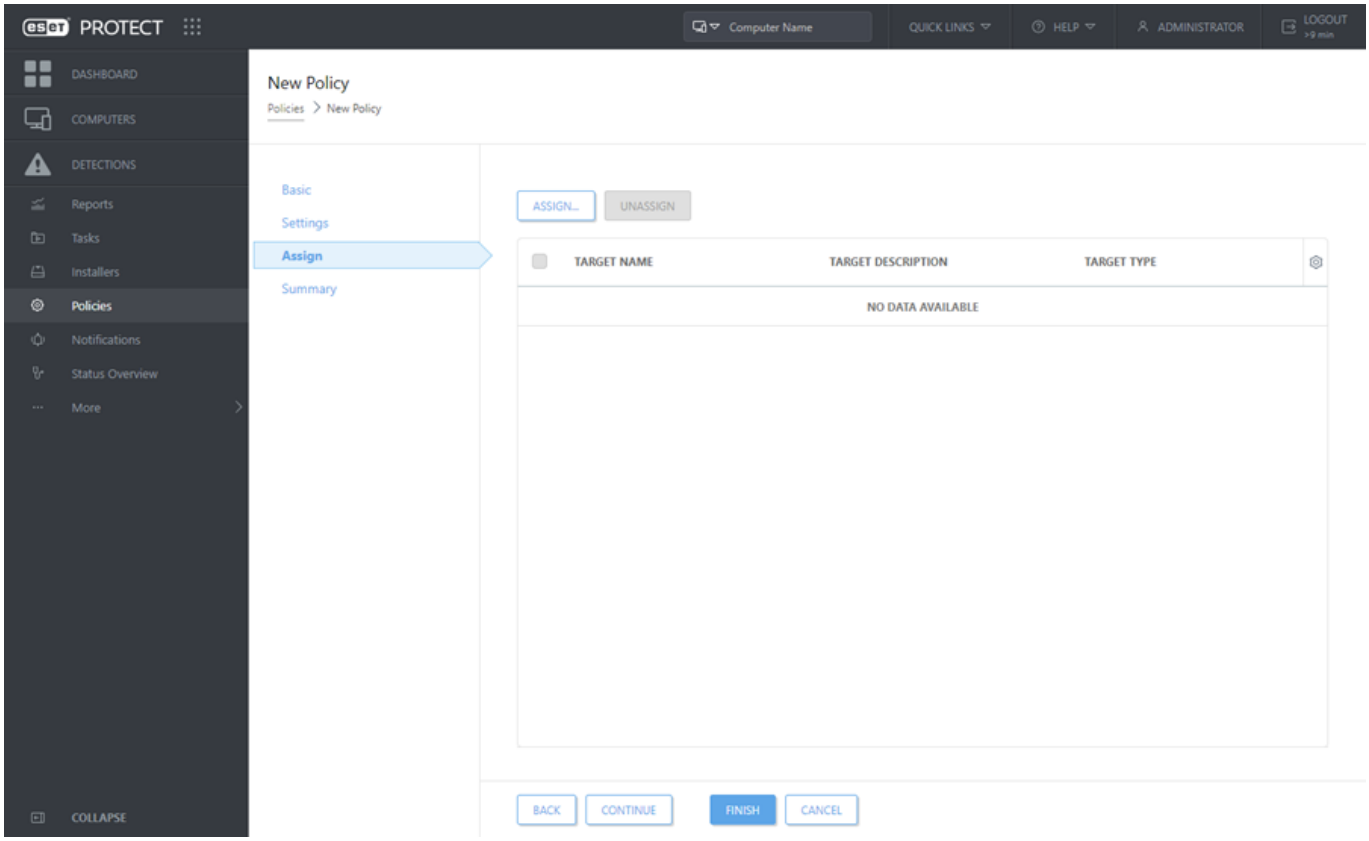
- **Tipo de criptografia** - Selecione a criptografia adequada na lista suspensa, certifique-se de que esse valor combina exatamente com as capacidades da rede Wi-Fi.

- **Senha** - Insira a senha que será usada para autenticar ao conectar na rede Wi-Fi.

Configurações de proxy - Opcionais. Se sua rede usar um Proxy, especifique os valores de acordo.

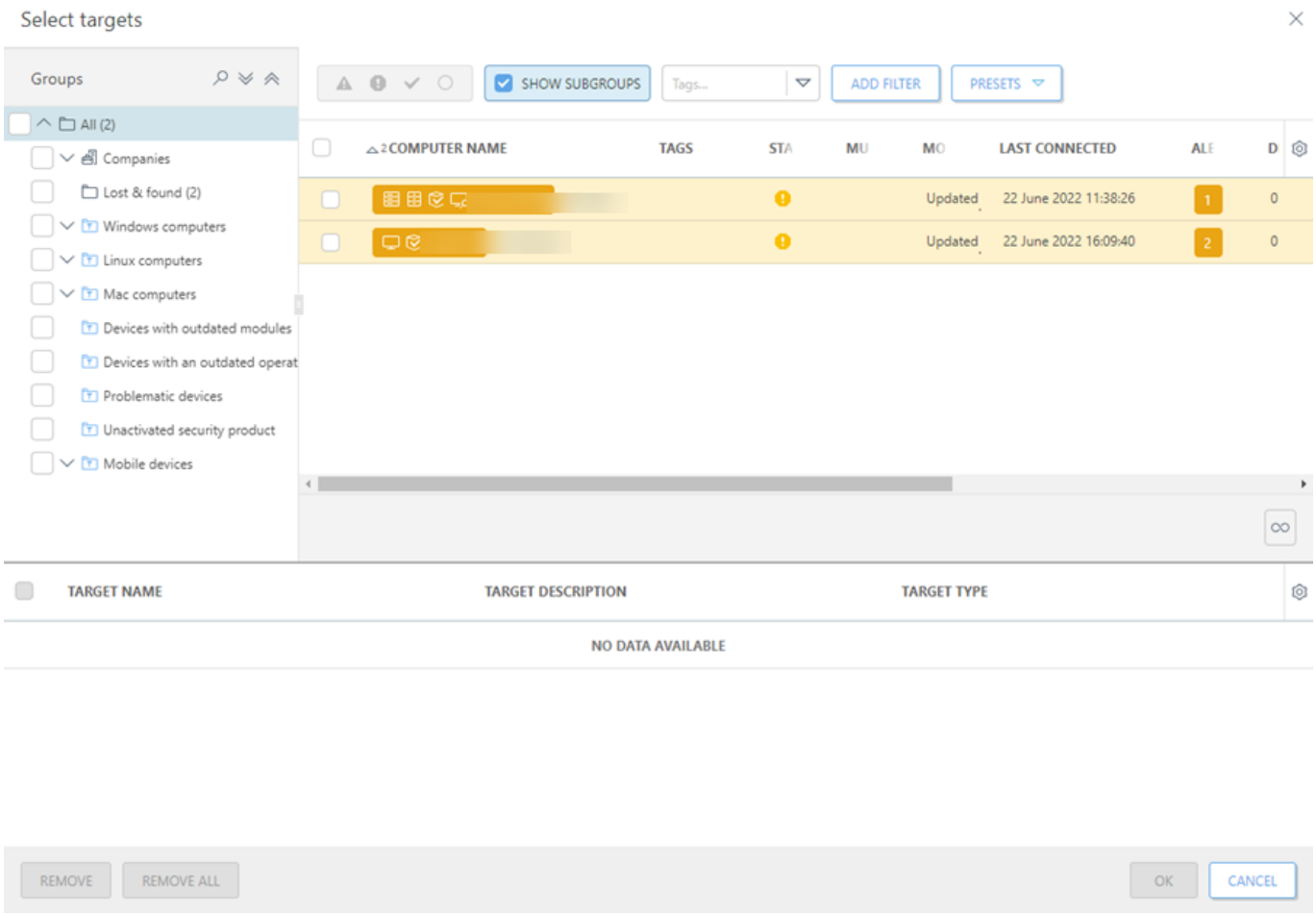
Atribuir

Especifique os clientes (computadores individuais/dispositivos móveis ou grupos inteiros) que serão os destinatários dessa política.



Clique em **Atribuir** para exibir todos os grupos estáticos e dinâmicos e seus membros. Selecione seus computadores ou grupos desejados e clique em **OK**.

Para atribuir todos os computadores em um grupo, atribua o grupo em vez de computadores individuais para impedir que a velocidade do Web Console diminua.
O Web Console exibirá um aviso se você selecionar um grande número de computadores.



Resumo

Verifique as configurações para esta política e clique em **Concluir**. A política é aplicada aos destinos depois da próxima conexão com o Servidor ESET PROTECT (dependendo do intervalo de conexão do agente).

Perfis de configuração MDM

Você pode configurar o perfil para impor políticas e restrições no dispositivo móvel gerenciado.

Nome do perfil	Descrição breve
Senha	Requer que os usuários finais protejam seus dispositivos com senhas cada vez que eles retornam do estado ocioso. Isso garante que todas as informações corporativas confidenciais em dispositivos gerenciados permanecem protegidas. Se vários perfis aplicarem senhas em um único dispositivo, a política mais restritiva é aplicada.
Restrições	Perfis de restrição limitam os recursos disponíveis para os usuários de dispositivos gerenciados ao restringir o uso de permissões específicas relacionadas com a funcionalidade de dispositivos, aplicativos, iCloud, segurança e privacidade.
Lista de conexão Wi-Fi	Perfis Wi-Fi empurram configurações de Wi-Fi corporativo diretamente para dispositivos gerenciados para um acesso instantâneo.

Nome do perfil	Descrição breve
Lista de conexão VPN	Perfis VPN empurram as configurações de rede virtual privada corporativa para dispositivos corporativos, para que os usuários possam acessar de forma segura a infraestrutura corporativa em locais remotos. **Nome de conexão** - Veja o nome da conexão exibido no dispositivo. **Tipo de conexão** - Escolha o tipo de conexão ativada por este perfil. Cada tipo de conexão possibilita capacidades diferentes. **Servidor** - Insira o nome de host ou endereço IP do servidor ao qual está se conectando.
Contas de email	Permite que o administrador configure as contas IMAP/POP3.
Contas do Exchange ActiveSync	Perfis do Exchange ActiveSync permitem que usuários finais tenham acesso a uma infraestrutura de email corporativo baseada em push. Observe que existem campos de consulta de valor e opções pré-preenchidos que são aplicáveis apenas ai iOS 5+ .
CalDAV - Contas do calendário	O CalDAV fornece opções de configuração para permitir que usuários finais façam sincronização sem fio com o servidor empresarial CalDAV.
CardDAV - Contas de contato	Esta seção permite a configuração específica de serviços CardDAV.
Contas de calendários inscritas	Calendários assinados fornecem configuração de calendário.

Gerenciamento de atualização do sistema operacional

O ESET Endpoint Security para Android permite que um administrador gerencie as atualizações do sistema operacional Android em dispositivos Android gerenciados.

> Esta funcionalidade requer o ESET Endpoint Security para Android versão 3.0 e o dispositivo Android deve estar inscrito no modo de Proprietário do dispositivo.

Para gerenciar as atualizações do sistema operacional em dispositivos gerenciados, crie uma nova política:

1. Clique em **Políticas** > **Nova política**.

2. Nas **Configurações**, selecione **ESET Endpoint Security para Android (2+)**.

3. Na **Segurança do dispositivo**, selecione **Segurança do dispositivo** e ative a configuração **Ativar segurança do dispositivo**.

4. Para ativar a funcionalidade de gerenciamento de sistema operacional, navegue até **Gerenciamento de atualizações do sistema** e **ative Gerenciar atualizações do sistema**.

A partir desta seção você pode definir regras diferentes do sistema operacional Android atualizadas em seus dispositivos Android gerenciados:

- **Política de atualização do sistema**

  oAutomático: A atualização do sistema operacional Android será executada sem atraso.

  oCom janela: A atualização do sistema operacional Android será executada apenas durante uma janela de manutenção especificada configuração **Janela de manutenção diária**.

  oAdiado por 30 dias: A atualização do sistema operacional Android será executada 30 dias depois de sua data

de lançamento.

- **Janela de manutenção diária:** Defina um tempo específico para que a atualização do sistema operacional seja executada no dispositivo Android gerenciado.
- **Períodos de parada:** Especifique vários períodos de tempo que os dispositivos não podem ser atualizados.

Controle de web para Android

Use o ESET Endpoint Security para Android para regular o acesso a sites nos seus dispositivos Android gerenciados. O controle de web pode regulamentar o acesso a sites que podem violar direitos de propriedade intelectual e proteger sua empresa do risco de responsabilidade legal. O objetivo é impedir que os funcionários acessem páginas com conteúdo inadequado ou nocivo, e páginas que podem afetar negativamente a produtividade.

> O controle de web para Android é compatível com o ESET Endpoint Security para Android versão 3.0 e versões posteriores.

Por padrão, o controle de web está desativado. Para ativar, você precisará criar uma nova política:

1. Clique em **Políticas** > **Nova política**.
2. Na janela **Nova Política**, navegue até **Configurações** e selecione **ESET Endpoint Security para Android (2+)**.
3. Na seção **Proteção da Web** da política, ative o **Controle de Web**.
4. Links ou categorias específicos da lista de permissões e da lista de proibições.

Regras de controle de web

Use a política de Controle de web para especificar uma lista de URLs para três categorias diferentes:

- **Lista de proibições** – bloqueia o URL sem nenhuma opção ou acesso
- **Lista de permissões** – permite acesso ao URL
- **Aviso** – avisa o usuário sobre o URL, mas dá a opção de acessar

Cada uma dessas seções pode ser gerenciada pelas ações a seguir:

- **Adicionar** – adicionar um novo registro com um endereço URL específico
- **Editar** – editar um endereço URL existente
- **Remover** – remover um relatório existente de um endereço URL
- **Importar** – importar uma lista de novos endereços URL para a categoria
- **Exportar** – exportar uma lista de endereços URL da categoria selecionada

Para regras que controlam acesso a um determinado site, insira o URL completo no campo **URL**.
Os símbolos especiais * (asterisco) e ? (ponto de interrogação) podem ser usados no campo URL.
Ao adicionar um endereço de domínio, todo o conteúdo localizado neste domínio e em todos os subdomínios (por exemplo `subdomain.domain.com`) serão bloqueados ou permitidos com base na ação escolhida.

Outra opção é Permitir/Bloquear um conjunto inteiro de URLs com base em sua categoria de acordo com as **Regras de categoria**.

Na janela **Regras de categoria**, selecione uma ação para uma categoria específica de URLs e especifique qual sub-categoria deve ser afetada:

- **Permitir** – permitir acesso ao URL de uma categoria selecionada
- **Bloquear** – bloquear acesso ao URL de uma categoria selecionada
- **Alertar** – alertar o usuário sobre o URL de uma categoria selecionada

Gerenciamento de atualização do sistema operacional

O ESET Endpoint Security para Android permite que um administrador gerencie as atualizações do sistema operacional Android em dispositivos Android gerenciados.

Esta funcionalidade requer o ESET Endpoint Security para Android versão 3.0 e o dispositivo Android deve estar inscrito no modo de Proprietário do dispositivo.

Para gerenciar as atualizações do sistema operacional em dispositivos gerenciados, crie uma nova política:

1. Clique em **Políticas** > **Nova política**.
2. Nas **Configurações**, selecione **ESET Endpoint Security para Android (2+)**.
3. Na **Segurança do dispositivo**, selecione **Segurança do dispositivo** e ative a configuração **Ativar segurança do dispositivo**.
4. Para ativar a funcionalidade de gerenciamento de sistema operacional, navegue até **Gerenciamento de atualizações do sistema** e **ative Gerenciar atualizações do sistema**.

A partir desta seção você pode definir regras diferentes do sistema operacional Android atualizadas em seus dispositivos Android gerenciados:

- **Política de atualização do sistema**

  oAutomático: A atualização do sistema operacional Android será executada sem atraso.

  oCom janela: A atualização do sistema operacional Android será executada apenas durante uma janela de manutenção especificada configuração **Janela de manutenção diária**.

  oAdiado por 30 dias: A atualização do sistema operacional Android será executada 30 dias depois de sua data de lançamento.

- **Janela de manutenção diária:** Defina um tempo específico para que a atualização do sistema operacional

seja executada no dispositivo Android gerenciado.

- **Períodos de parada:** Especifique vários períodos de tempo que os dispositivos não podem ser atualizados.

Solução de problemas MDM

Configuração e arquivos de relatório MDMCore

Veja também arquivos de relatório de outros componentes do ESET PROTECT.

Localização	Detalhes do arquivo
Windows: *%ProgramData%\ESET\RemoteAdministrator\MDMCore\Configuration* Linux: */etc/opt/eset/RemoteAdministrator/MDMCore*	• *startupconfiguration.ini* (Windows), *startupconfiguration.ini* (Linux) – as informações de conexão do banco de dados. • *loggerLevel.cfg* – uma única linha especificando um nível de relatório de substituição para registro em relatório. Esse arquivo tem prioridade sobre a configuração em qualquer política (e pode ser usado em casos em que a política não pode ser entregue). Se for reconhecido, a linha "Setting log level from loggerLevel.cfg override file to XYZ" é o resultado do relatório de rastreamento (nível de informações). Valores reconhecidos: all, trace, debug, information, warning, error, critical, fatal. Quando definido como all, ele também registra toda a comunicação com os telefones. • *shouldLogPhoneComm.cfg* – uma única linha especifica se a comunicação com os telefones deve ser registrada em um arquivo de relatório separado. Valores reconhecidos: 1, true, log. • *skipPnsCertCheck.cfg* – uma única linha especificando se o certificado de serviço PNS deve ser validado.
Windows: *%ProgramData%\ESET\RemoteAdministrator\MDMCore\Data\MultiAgent* Linux: */var/opt/eset/RemoteAdministrator/MDMCore/MultiAgent*	Rastrear relatórios de agentes individuais nas subpastas por agente.
Windows: *%ProgramData%\ESET\RemoteAdministrator\MDMCore\Dumps* Linux: */var/opt/eset/RemoteAdministrator/MDMCore/Dumps*	Crashdumps que ainda não foram enviados para o serviço ESET CrashReporting.
Windows: *%ProgramData%\ESET\RemoteAdministrator\MDMCore\Logs* Linux: */var/log/eset/RemoteAdministrator/MDMCore*	• *trace.log, trace.log.<N>.gz* – o relatório de rastro do MDMCore. Os arquivos compactados e numerados são os conteúdos mais antigos do relatório.
Windows: *%ProgramData%\ESET\RemoteAdministrator\MDMCore\Logs\Proxy* Linux: */var/log/eset/RemoteAdministrator/MDMCore/Proxy*	• *trace.log, trace.log.<N>.gz* – o relatório de rastro do componente MultiProxy do MDMCore. Os arquivos compactados e numerados são os conteúdos mais antigos do relatório.
Windows: *%ProgramData%\ESET\RemoteAdministrator\MDMCore\Modules* Linux: */var/opt/eset/RemoteAdministrator/MDMCore/Modules*	• *em*.dat* – módulos do Mecanismo de config e Carregador.
Windows: *%ProgramFiles%\ESET\RemoteAdministrator\MDMCore* Linux: */opt/eset/RemoteAdministrator/MDMCore*	Todos os arquivos executáveis necessários pelo MDMCore.

Mensagens de erro MDM

O token de Inscrição já está sendo usado ou não é válido

É provável que você esteja tentando fazer a nova inscrição com um token de inscrição antigo. Crie um novo token de reinscrição no console da web e use-o. Também é possível que você esteja tentando uma segunda reinscrição muito cedo depois da primeira. Verifique se o token de reinscrição é diferente do primeiro. Se não, aguarde alguns minutos e tente gerar um novo token de reinscrição novamente.

Falha na validação de certificado de serviço

Essa mensagem de erro indica que existe um problema com seu certificado de serviço APNS ou FCM. Isso é anunciado no Console da Web ESET PROTECT como um dos alertas a seguir sob os alertas do MDM Core:

- **Falha na validação de certificado de serviço FCM** (0x0000000100001002)
- **Falha na validação de certificado de serviço APNS** (0x0000000100001000)
- **Falha na validação de certificado de serviço de Feedback APNS** (0x0000000100001004)

Certifique-se de ter a autoridade de certificado correta disponível em seu sistema:

- Autoridade de certificação APNS: **Confiar na Autoridade de certificação**, necessário para validar o certificado de gateway.push.apple.com:2195;

- Autoridade de certificação do Feedback APNS: **Confiar na Autoridade de certificação**, necessário para validar o certificado de feedback.push.apple.com:2196;
- Autoridades de certificação FCM: **GeoTrust Global CA**, necessário para validar o certificado de android.googleapis.com:443.

A autoridade de certificação desejada deve ser incluída no depósito de certificado na máquina host do MDM. Em um sistema Windows você pode pesquisar “Gerenciar Certificação Raiz Confiável". Em um sistema Linux a localização do certificado depende da distribuição que você está usando. Alguns exemplos de destinos de armazenamento de certificado incluem:

- no Debian, CentOS: */usr/lib/ssl/cert.pem*, */usr/lib/ssl/certs*;
- no Red Hat: */usr/share/ssl/cert.pem*, */usr/share/ssl/certs*;
- o comando `openssl version -d` geralmente retorna com o caminho desejado.

Se a autoridade de certificação desejada não for instalada no sistema onde o MDM Core está sendo executado, instale-a. Depois da instalação, reinicie o serviço ESET PROTECT MDC.

Tenha cuidado, a validação de certificado é um recurso de segurança, portanto se ocorrer um alerta no console da web isso também pode indicar uma ameaça de segurança.

Ferramenta de migração de gerenciamento de dispositivo móvel

As etapas a seguir vão ajudar você a migrar dispositivos móveis do ESET PROTECT (local) para o ambiente ESET PROTECT Cloud:

Pré-requisitos

- Ambiente ESET PROTECT funcionando (local) com o componente de Gerenciamento de dispositivo móvel
- Ambiente de trabalho ESET PROTECT Cloud
- Conta ESET PROTECT Cloud com privilégios de **superusuário**

Limitações

- Esta migração está disponível apenas para dispositivos Android
- Essa migração requer o ESET Endpoint Security para Android versão 3.5+ e o ESET PROTECT versão 10.0+
- A migração de dispositivos gerenciados iOS requer a remoção manual da inscrição no ESET PROTECT e a inscrição no ESET PROTECT Cloud

1. Abrir o Console Web ESET PROTECT Cloud.

2. Clique em **Mais** > **Configurações** > **Migração de dispositivos móveis do ESET PROTECT (local)**.

3. Selecione a **Licença** que deseja usar para a ativação de dispositivos móveis gerenciados depois do fim da migração.

4. Selecione o **Grupo principal** para o posicionamento inicial dos dispositivos depois da migração.

5. **Limite de uso do token** – você pode limitar o número de dispositivos para migração com o token de migração.

Se você gerenciar um grande número de dispositivos móveis, recomendamos primeiro experimentar o processo de migração com um pequeno número de dispositivos para monitorar a migração, para que ela não tenha problemas. Depois disso você poderá continuar com a migração dos dispositivos móveis gerenciados restantes.

6. Selecione **Gerar token** para gerar um token de migração com parâmetros definidos para o processo de migração.

O token gerado é válido por 14 dias e está disponível apenas enquanto você permanece nesta página. Não feche ou atualize a página antes de copiar o token pela primeira vez.

7. O token de migração aparece como uma string de caracteres no campo abaixo. Copie-a em um editor de texto.

8. Abra o Web Console ESET PROTECT (local).

9. Clique em **Políticas** > **Nova política**.

10. Na seção **Básico**, preencha o **Nome** e a **Descrição** da política. Essa política vai migrar os dispositivos móveis gerenciados no momento do ambiente no local para o ambiente de nuvem.

11. Na seção **Configurações**, selecione **ESET Mobile Device Connector**.

12. Em **Migração** > **ESET PROTECT Cloud geral**, colar o token de migração no campo **de texto do token de migração**.

13. Na seção **Atribuir**, selecione o dispositivo executando o Mobile Device Connector.

14. Depois da política ser aplicada, o processo de migração começará.

O servidor vai aplicar a política de migração a todos os dispositivos móveis gerenciados que serão conectados a partir deste momento. Certifique-se de que todos os seus dispositivos móveis gerenciados são capazes de se conectar ao servidor enquanto o token de migração é válido (pelos próximos 14 dias). Se um dispositivo móvel gerenciado não se conectar ao servidor nesse período, ele não será migrado e você precisará repetir o procedimento de migração.

15. Você pode monitorar o processo de migração no Web Console ESET PROTECT Cloud. Depois que o dispositivo móvel for migrado, ele será conectado ao ESET PROTECT Cloud, e será visível na seção **Computadores** do Web Console ESET PROTECT Cloud.

16. Depois de migrar o dispositivo para o ambiente ESET PROTECT Cloud com segurança, ele poderá ser removido com segurança do Web Console ESET PROTECT (local).

17. Depois de migrar com sucesso todos os dispositivos móveis para o ambiente ESET PROTECT Cloud, você poderá desativar com segurança o componente de Gerenciamento de dispositivo móvel.

ESET PROTECT para Provedores de serviço gerenciados

Quem é um MSP

A abreviação MSP significa "Managed Service Provider", "Provedor de Serviço Gerenciado". Os usuários MSP

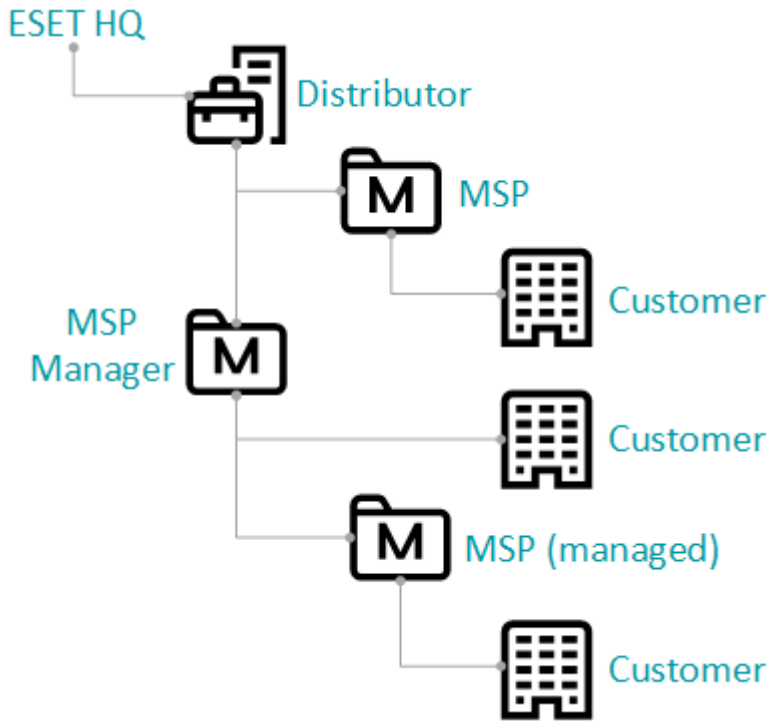
geralmente fornecem serviços de TI a seus clientes, por exemplo, o gerenciamento de produtos de segurança (por exemplo, ESET Endpoint Antivirus).

- Os usuários MSP têm requisitos diferentes e outras formas de usar o ESET PROTECT do que, por exemplo, usuários corporativos ou SMB (empresas pequenas e médias). Veja os cenários de implantação recomendados para o MSP.

- Para obter mais informações sobre o programa MSP ESET, entre em contato com seu parceiro ESET local ou visite a página do Programa do provedor de serviço gerenciado ESET.

A estrutura das entidades no MSP

O ESET PROTECT sincroniza sua estrutura ESET MSP Administrator com a árvore do Grupo estático em **Computadores** no Web Console.



- **Distribuidor** – Um distribuidor é um parceiro da ESET e um MSP ou parceiro do Gerente MSP.

- **Gerente MSP** – Gerencia várias empresas de MSP. Um Gerente MSP também pode ter clientes diretos.

- **MSP** – O público-alvo deste guia. Um MSP fornece serviços aos seus clientes. Por exemplo, MSPs: gerenciam remotamente os computadores dos clientes, instalam e gerenciam os produtos ESET.

- **MSP gerenciado** – Semelhante ao MSP, mas o MSP gerenciado é gerenciado por um Gerente MSP.

- **Cliente** – o usuário final das licenças de produto ESET. O cliente não deve interagir com os produtos da ESET.

Especificidades do ambiente MSP

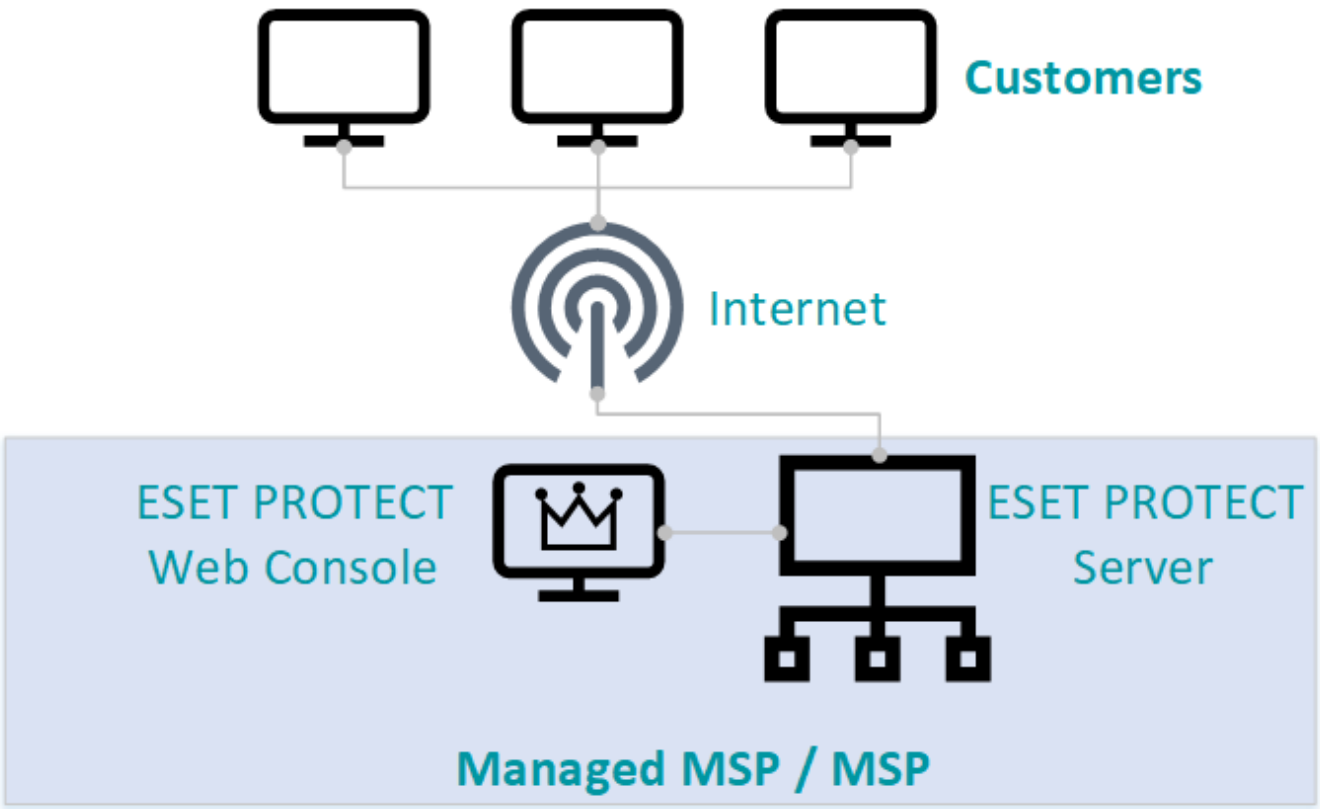
O modelo de negócios MSP usa uma configuração de infraestrutura diferente de uma empresa ou SMB. No ambiente MSP, os clientes geralmente estão localizados fora da rede da empresa MSP. O próprio Servidor ESET PROTECT também pode ser hospedado fora da empresa MSP. Os Agentes ESET Management precisam ter

conectividade direta com o Servidor ESET PROTECT pela Internet pública. As configurações recomendadas do Servidor ESMC para MSPs são:

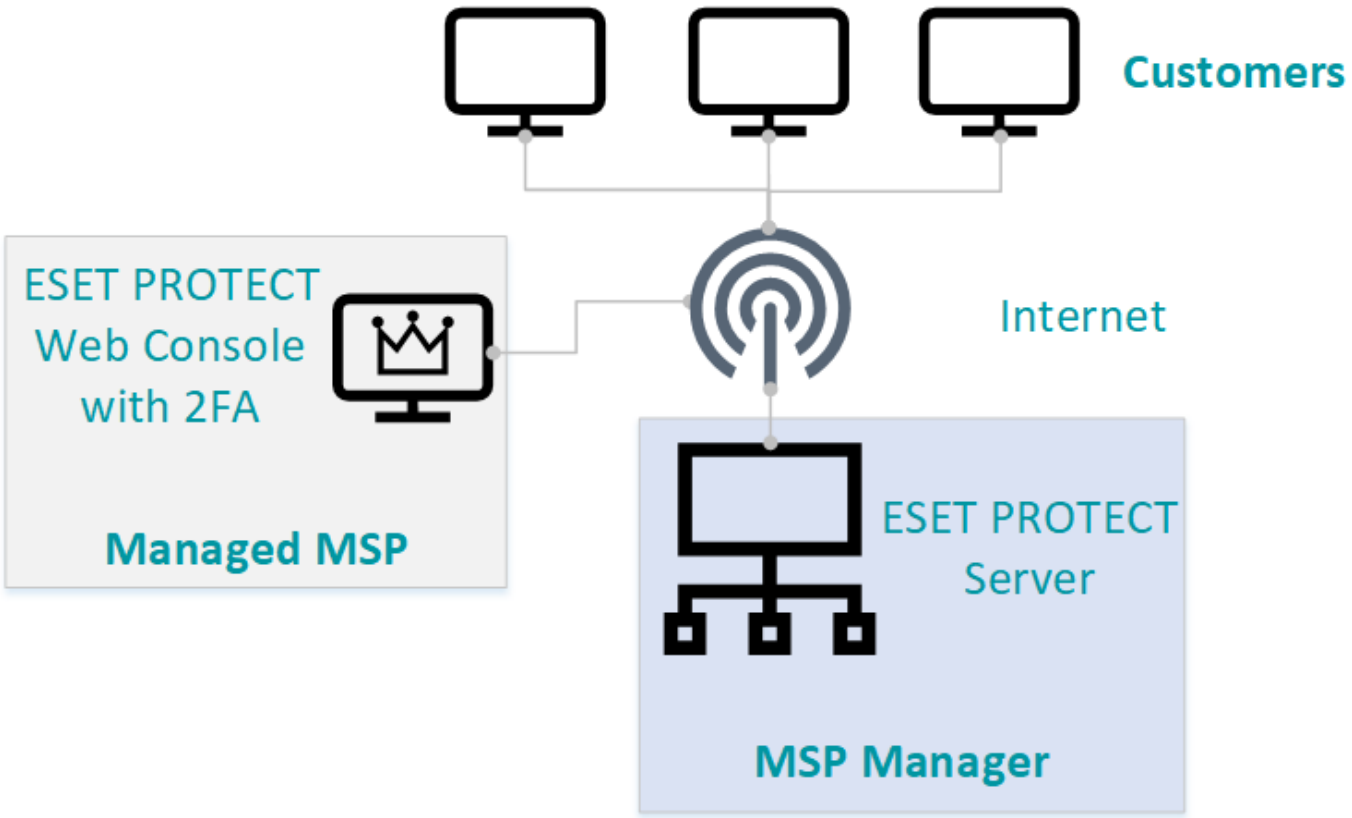
- Hospedado em uma nuvem pública.
- Hospedado na nuvem privada de um MSP. (Você precisa abrir certas portas para tornar o ESET PROTECT visível na Internet)
- Hospedado em uma rede privada MSP. (Use o Proxy HTTP para encaminhar as conexões da Internet, se o Servidor não estiver diretamente visível.)

Configurações básicas

- **Configuração centralizada** – os clientes acessam o Servidor ESET PROTECT pela Internet. O Web Console ESET PROTECT pode ser acessado apenas da rede da empresa MSP.



- **Configuração distribuída** – os clientes acessam o Servidor ESET PROTECT pela Internet. O Web Console ESET PROTECT pode ser acessado pelo MSP via internet. Se você fizer com que o Web Console possa ser acessado via internet, certifique-se de ativar a 2FA.



Migração de ESMC 7.2

Usuários com a conta EMA 2 importada que estão fazendo atualização do ESMC 7.2, a árvore MSP e a estrutura de grupo não são afetadas.

Recursos do ESET PROTECT para usuários MSP

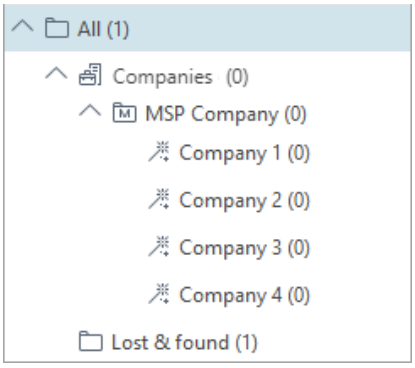
O ESET PROTECT oferece um conjunto de recursos focados nos usuários MSP. Todos os recursos relacionados do MSP são ativados depois de você importar uma conta EMA 2 para o ESET PROTECT.

Assistente de configuração do cliente

O recurso principal do MSP no ESET PROTECT é a configuração do cliente MSP. Esse recurso ajuda a criar um usuário e um instalador de Agente ESET Management personalizado para o seu cliente.

Árvore MSP

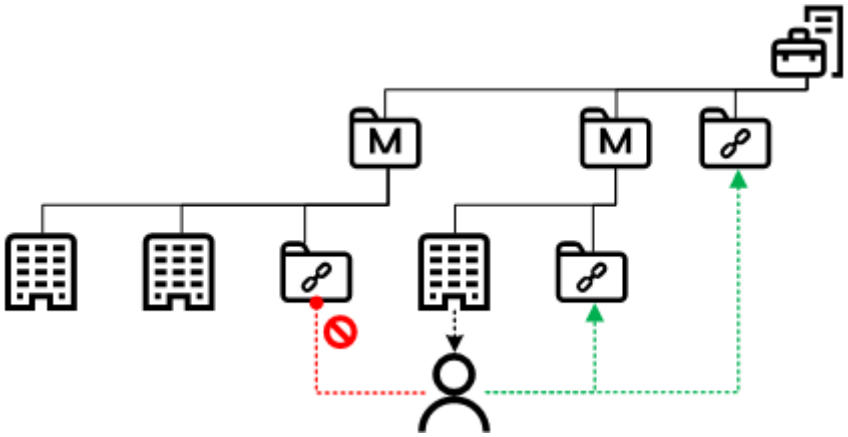
Depois de importar a conta EMA 2, o ESET PROTECT sincroniza com o Portal ESET MSP (EMA 2) e cria a Árvore MSP. A Árvore MSP é uma estrutura no menu Computadores, que representa a estrutura das empresas na sua conta EMA 2. Os itens na Árvore MSP usam ícones diferentes dos dispositivos e grupos ESET PROTECT padrão. Não é possível modificar a estrutura da árvore MSP no Web Console. Somente depois de remover a conta EMA 2 do Gerenciamento de licenças será possível começar a editar e remover clientes da árvore. Suspender uma empresa no EMA 2 não remove a empresa da Árvore MSP no ESET PROTECT.



Grupo de objetos compartilhados

Depois da sincronização da conta MSP, o ESET PROTECT criará a árvore MSP. Há um grupo de acesso: de **Objetos compartilhados** para cada MSP e gerente de MSP. O Grupo de acesso define o grupo estático do objeto e o acesso ao objeto com base nos direitos de acesso do usuário. Você não pode armazenar computadores nos **Objetos compartilhados**. **Objetos compartilhados** não são visíveis sob **Grupos** nos **computadores**. MSPs podem compartilhar objetos como políticas e tarefas por meio do grupo de Acesso **Objetos compartilhados**.

Cada usuário MSP criado usando o assistente de configuração da empresa tem acesso de leitura e uso a todos os grupos de **Objetos compartilhados** acima do usuário. Você pode inspecionar os Conjuntos de permissões atribuídos ao usuário para ver a lista de grupos de acesso. Os usuários podem acessar apenas grupos de Objetos compartilhados acima deles, não grupos de gerentes de MSP paralelos.



ESET PROTECT certificados e MSP

Quando você importa a conta EMA 2 no ESET PROTECT, seu Servidor ESET PROTECT cria uma nova Autoridade de certificação (CA) MSP. A CA MSP é armazenada no grupo estático **Objetos compartilhados**, no grupo raiz MSP. Existe apenas uma CA MSP, mesmo se você importar várias contas. Se você remover a CA MSP, o ESET PROTECT cria uma nova CA MSP depois da próxima sincronização com os servidores de licença. A sincronização ocorre automaticamente uma vez por dia.

ESET PROTECT cria um novo certificado de agente de mesmo nível depois que uma empresa é configurada usando o assistente de configuração do cliente. A CA MSP assina esses certificados de mesmo nível. Cada certificado é marcado com o nome da empresa. Criar um certificado separado para cada empresa melhora a segurança geral.

Se você quiser usar a Segurança avançada, é altamente recomendável configurá-la **antes** de importar a conta MSP.

Se você remover uma CA, todos os computadores que usam certificados assinados por essa CA não conseguirão mais se conectar ao Servidor ESET PROTECT. Seria necessário fazer a reimplantação manual do Agente ESET Management.

MSP na Visão geral do status

Você obtém acesso ao novo bloco MSP na Visão geral do status depois de importar a conta EMA 2. O bloco MSP exibe informações básicas sobre sua conta.

Processo de implantação para MSP

Se você não tiver o ESET PROTECT instalado, recomendamos usar o Instalador tudo-em-um Windows e seguir o guia de instalação, levando em consideração as seguintes recomendações:

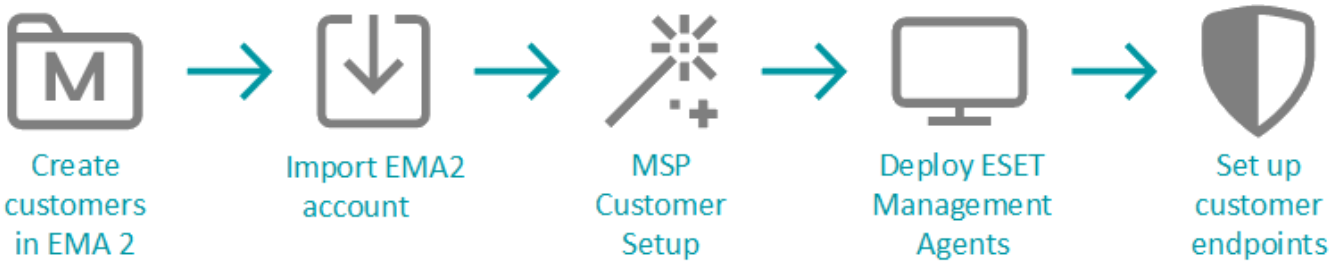
- Não escolha a opção a instalar **ESET Bridge** (Proxy HTTP). Seus clientes entrarão em contato diretamente com os servidores ESET (para downloads, ativações, atualizações). Clientes maiores podem ter sua própria solução local de Proxy HTTP. Essa configuração pode ser feita mais tarde.

- O Servidor ESET PROTECT também deve ter conectividade com o servidor ESET (para sincronizar com o EMA 2, fazer download de atualizações, etc.).

Depois de instalar o Servidor ESET PROTECT, siga o processo abaixo:

1. Certifique-se de que você tem uma conta elegível para o EMA 2.
2. Prepare um cliente com pelo menos uma licença. Você também pode usar um cliente existente.
3. Importe sua conta do EMA 2 para o ESET PROTECT.
4. Conclua a Configuração do cliente MSP. Quando solicitado, selecione o instalador **Apenas Agente**.
5. Distribua e instale o instalador do Agente ESET Management de maneira local ou remota.
6. Instale os produtos de segurança ESET e configure as políticas.

O esquema abaixo é uma descrição de alto nível do processo de inscrição do cliente MSP.



Implantação local do Agente

Implantação local do instalador apenas do Agente

O **instalador apenas do Agente** é um script (*.bat* para Windows e *.sh* Linux e macOS) que contém todas as informações necessárias para uma máquina cliente fazer o download e instalar o Agente ESET Management. Se você estiver instalando em uma máquina Linux, verifique se a máquina atende aos pré-requisitos.

Você pode executar o instalador localmente ou de uma mídia removível (uma unidade USB, por exemplo).

A máquina cliente precisa ter conexão com a Internet para efetuar o download do pacote de instalação do Agente e conectar com o ESET PROTECT.

Você pode editar o script manualmente para ajustar determinadas configurações, se necessário. Recomendamos

isso apenas para usuários avançados.

Implantação local do Instalador tudo-em-um

O instalador Tudo-em-um contém um produto de segurança ESET escolhido por você e um instalador pré-configurado do Agente ESET Management.

Consulte o manual do instalador para obter instruções detalhadas.

Implantação remota do Agente

Implantação remota do instalador apenas do Agente

O **instalador apenas do Agente** é um script (*.bat* para Windows e *.sh* Linux e macOS) que contém todas as informações necessárias para uma máquina cliente fazer o download e instalar o Agente ESET Management. Se você estiver instalando em uma máquina Linux, verifique se a máquina atende aos pré-requisitos. Você pode distribuir o instalador por e-mail e permitir que o usuário o implante. Se disponível, use uma ferramenta de gerenciamento remoto de terceiros para distribuir e executar o script.

A máquina cliente precisa ter conexão com a Internet para efetuar o download do pacote de instalação do Agente e conectar com o ESET PROTECT.

Implantação remota do Instalador tudo-em-um

O instalador Tudo-em-um pode ser instalado remotamente, dentro de uma rede local, usando a ESET Remote Deployment Tool. Consulte a documentação da ESET Remote Deployment Tool para obter instruções detalhadas.

Licenças MSP

Contas elegíveis

Para ativar os recursos MSP no ESET PROTECT, você precisa importar sua conta MSP no Gerenciamento de licenças ESET PROTECT.

- Você pode importar os seguintes tipos de contas EMA 2: MSP, MSP gerenciado e Gerente MSP.
- Qualquer conta precisa ter pelo menos permissão de leitura para pelo menos uma empresa, que pode ser sua empresa principal ou um cliente.
- O acesso à empresa principal não é necessário.
- A conta do distribuidor não pode ser importada.

Informações sobre licenças e empresas

- Licenças importadas da sua conta MSP são marcadas com o nome da empresa. Se a empresa for renomeada mais tarde, as marcações não serão renomeadas automaticamente. Isso pode ser editado manualmente.

• Todas as licenças são importadas de maneira compatível com o modelo de segurança ESET PROTECT. Cada usuário criado usando a configuração do Cliente MSP pode apenas ver e usar suas licenças.

• Se houver uma empresa em sua estrutura MSP que não possua licenças no momento da sincronização, ela será sincronizada apenas com a Árvore MSP do computador, e não com a Árvore MSP dentro do Gerenciamento de licenças.

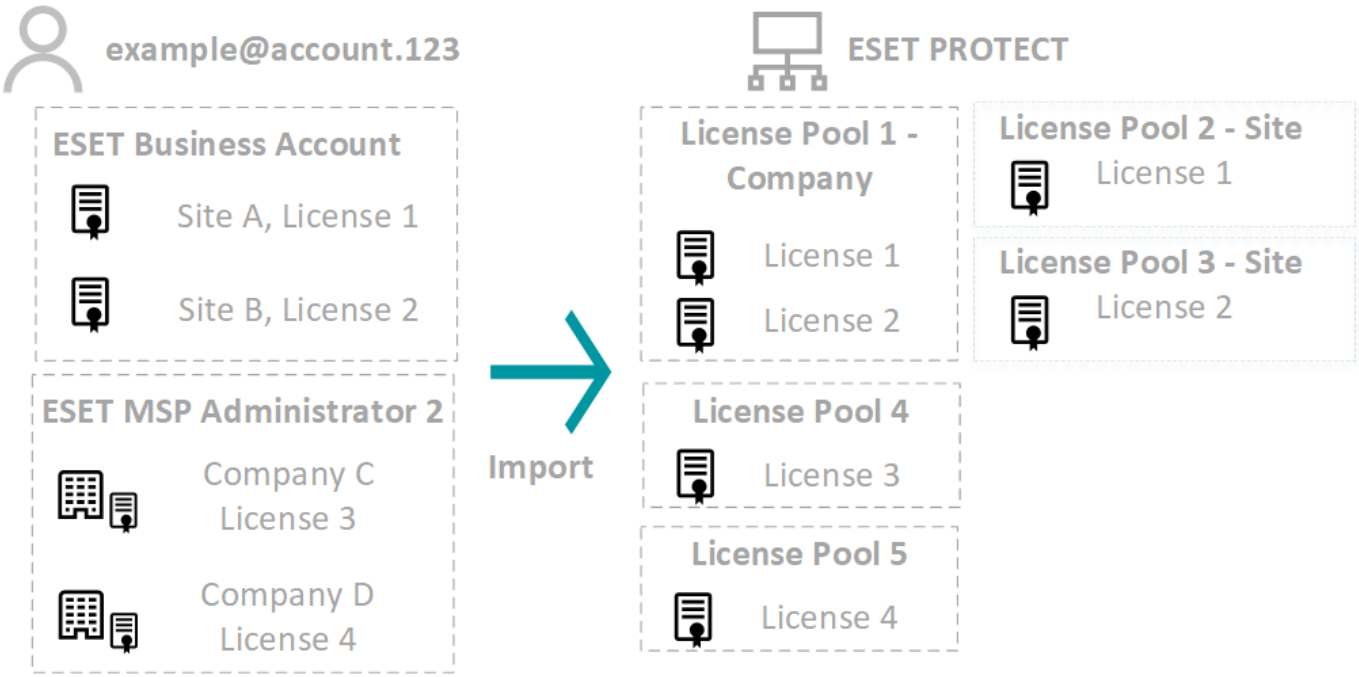
• Se você adicionar uma nova empresa no ESET MSP Administrator 2, o ESET PROTECT adiciona a empresa à Árvore MSP depois da próxima sincronização de licença.

• As licenças do ESET MSP Administrator 2 são divididas em um pool para cada empresa. Você não pode mover uma licença para fora do pool.

• Você pode encontrar nomes de empresa e sites na coluna **Usuário da licença** no Gerenciamento de licenças. Você pode usar os dados do **Usuário da licença** ao criar um relatório.

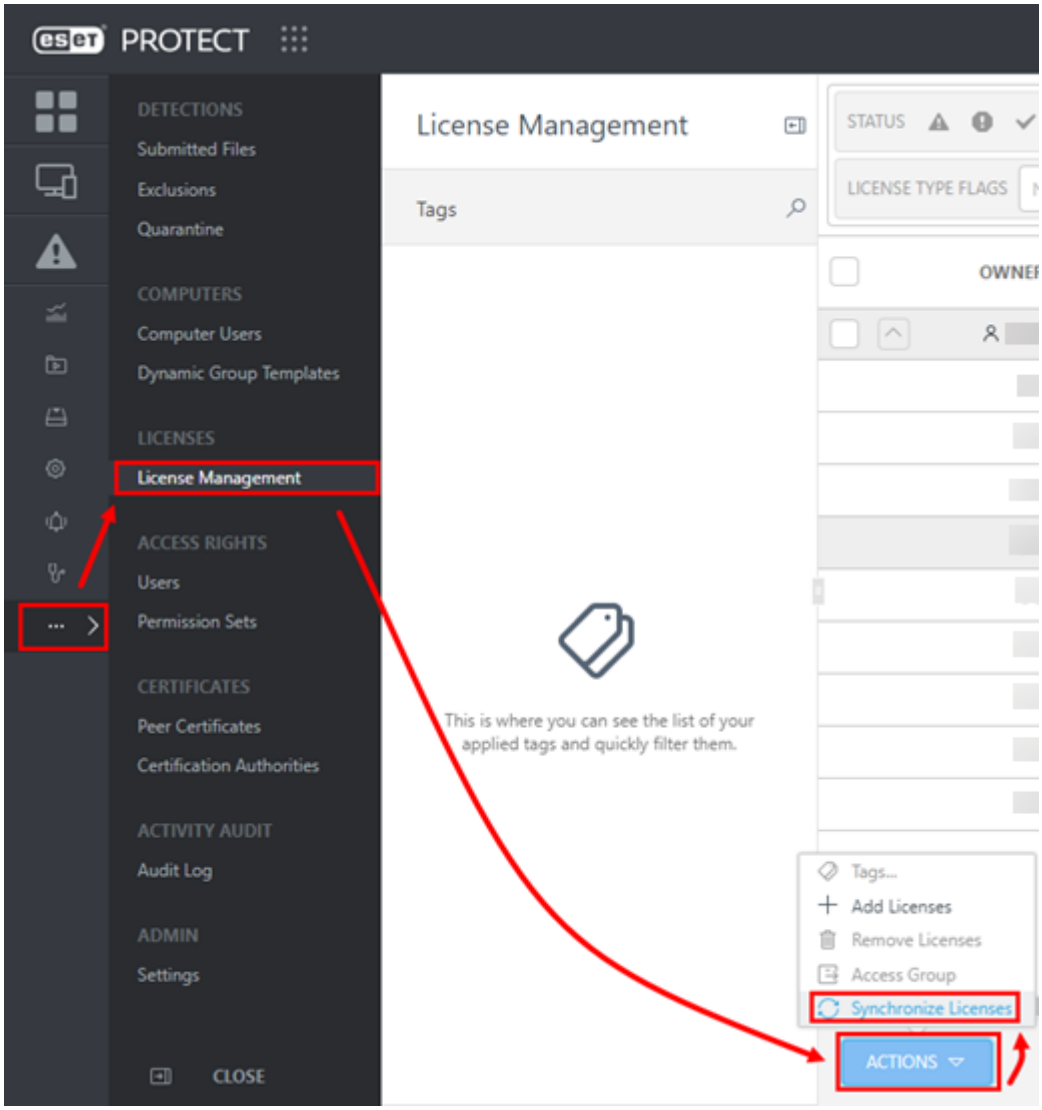
• Se você tiver licenças no ESET Business Account e no ESET MSP Administrator 2 sob as mesmas credenciais, o ESET PROTECT sincroniza todas as licenças de ambas as contas. Todas as licenças ESET Business Account são salvas em vários conjuntos de licenças. As licenças do ESET MSP Administrator 2 são divididas em um pool para cada empresa. Desde a versão 8.0 o ESET PROTECT é compatível com Sites ESET Business Account para dividir as licenças.

• Ao remover qualquer pool de licenças, você remove automaticamente todos os outros pools de licenças associados à mesma conta. Leia mais sobre como remover uma empresa.



Sincronização sob demanda

O ESET PROTECT sincroniza com os servidores de licença uma vez por dia. Se você fez alterações na sua conta MSP e deseja atualizar a tela de licença e a árvore MSP, navegue até **Gerenciamento de licenças** > **Ações** e clique em **Sincronizar licenças**.



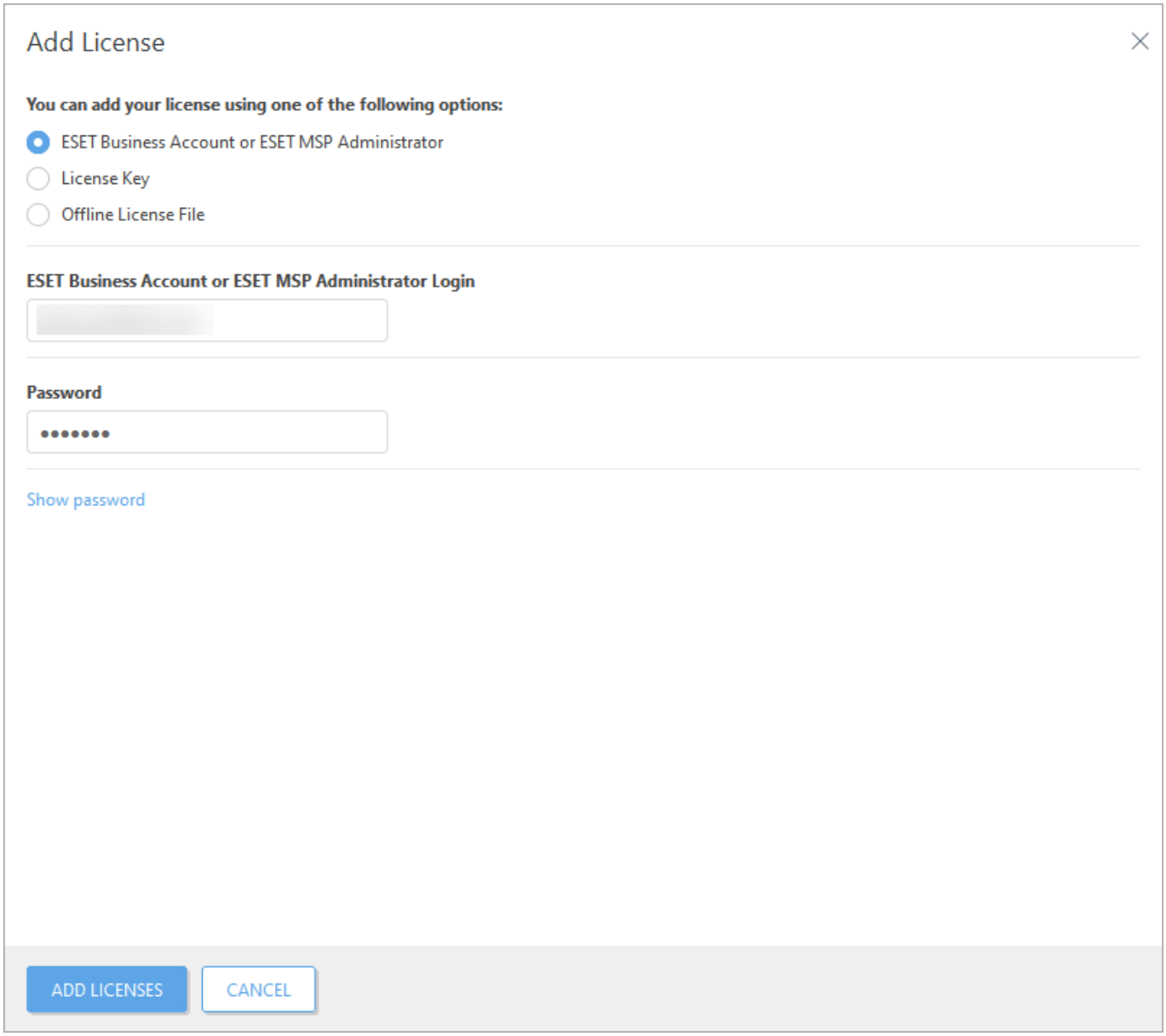
Importação de uma conta MSP

Se você quiser usar a Segurança avançada, é altamente recomendável configurá-la **antes** de importar a conta MSP.

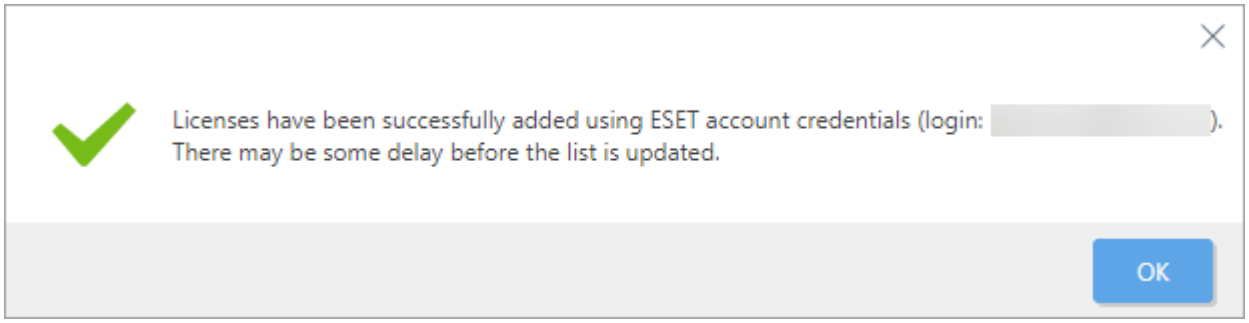
1. Entre no console web e navegue até **Mais** > **Gerenciamento de licenças**.

2. Clique em **Ações** > **Adicionar licenças**.

3. Selecione a opção **ESET Business Account ou ESET MSP Administrator**. Digite suas credenciais MSP (login do EMA 2) nos campos **Login** e **Senha** abaixo.



4. Clique em **Adicionar licenças** para confirmar.



5. Agora o ESET PROTECT sincroniza sua estrutura do portal MSP para a árvore de Grupo estático com o menu **Computadores** no Web Console. A estrutura sincronizada é chamada de *Árvore MSP*.

Importar uma conta MSP com um grande número de clientes (milhares) pode levar muito tempo, até mesmo horas.

Iniciar configuração do cliente MSP

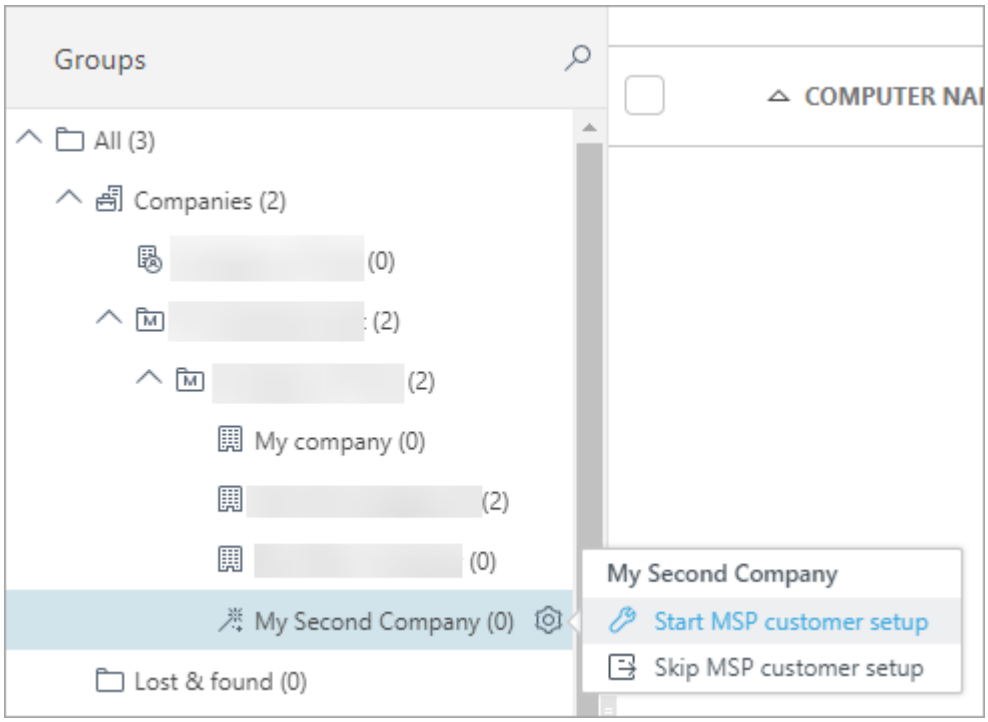
Depois de importar sua conta MSP e da árvore MSP ser sincronizada, você poderá começar a configurar empresas. A configuração do cliente MSP cria:

- Um ESET Management personalizado ou instalador do conjunto de Agente e produto de segurança ESET. A configuração do cliente MSP não é compatível com a criação de instaladores ESET Full Disk Encryption ou instaladores do Conector ESET Inspect.
- Um usuário MSP que pode gerenciar os computadores da empresa usando o console web.

Você também pode ignorar a configuração do cliente MSP, mas recomendamos que a instalação do MSP seja concluída.

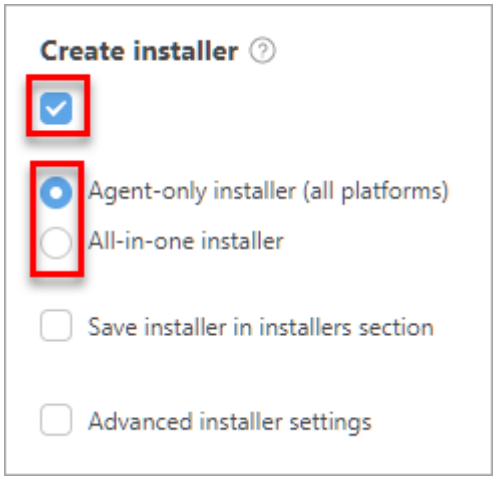
Você pode configurar apenas uma empresa com pelo menos 1 unidade de licença válida.

1. Na janela **Computadores**, clique no ícone de engrenagem ao lado da empresa que você deseja configurar e selecione **Iniciar configuração do cliente MSP**.



2. Se quiser salvar esta configuração como configuração padrão, marque a caixa de seleção em **Lembrar configurações**. Clique em **Continuar**.

3. Se você quiser criar um instalador personalizado durante a configuração (recomendado), marque a caixa de seleção em **Criar instalador**.



4. Você pode criar dois tipos de instaladores:

• **Instalador apenas do Agente (todas as plataformas)** – você pode instalar este Instalador de script do agente nos computadores Windows, MacOS e Linux.

• **Instalador tudo-em-um** – o instalador é constituído pelo Agente ESET Management e pelo produto de segurança ESET Business selecionado (Windows).

Se você não ver a opção **Instalador único**, certifique-se de que uma licença esteja atribuída à empresa.

^ Selecionei o Instalador tudo-em-um

Produto/versão – selecione um produto de segurança ESET que será instalado junto com o Agente ESET Management. Por padrão, a versão mais recente está selecionada (recomendado). Você pode selecionar uma versão anterior.
Selecione o idioma no menu suspenso **Idioma**.
Selecione a caixa de seleção **Aceito os termos do Contrato de licença para o usuário final do aplicativo e reconheço a Política de Privacidade**. Consulte o Acordo de Licença para o Usuário Final (EULA), Termos de Uso e Política de Privacidade dos produtos ESET.

Para salvar o instalador em Instaladores para uso futuro, selecione a caixa de seleção ao lado de **Salvar instalador na seção instaladores**.

^ Configurações avançadas do instalador (recomendado)

Nome do host do servidor é o endereço onde os Agentes ESET Management se conectam ao Servidor ESET PROTECT. Selecione uma porta diferente para a comunicação entre Agente e Servidor, se necessário. Se você alterar a porta, precisará alterá-la para todos os agentes de conexão e também nas **Mais** > Configurações. Certifique-se de que todos os dispositivos clientes que usarão o instalador podem alcançar o endereço do **Nome de host do servidor**. Consulte as Recomendações do ambiente MSP.

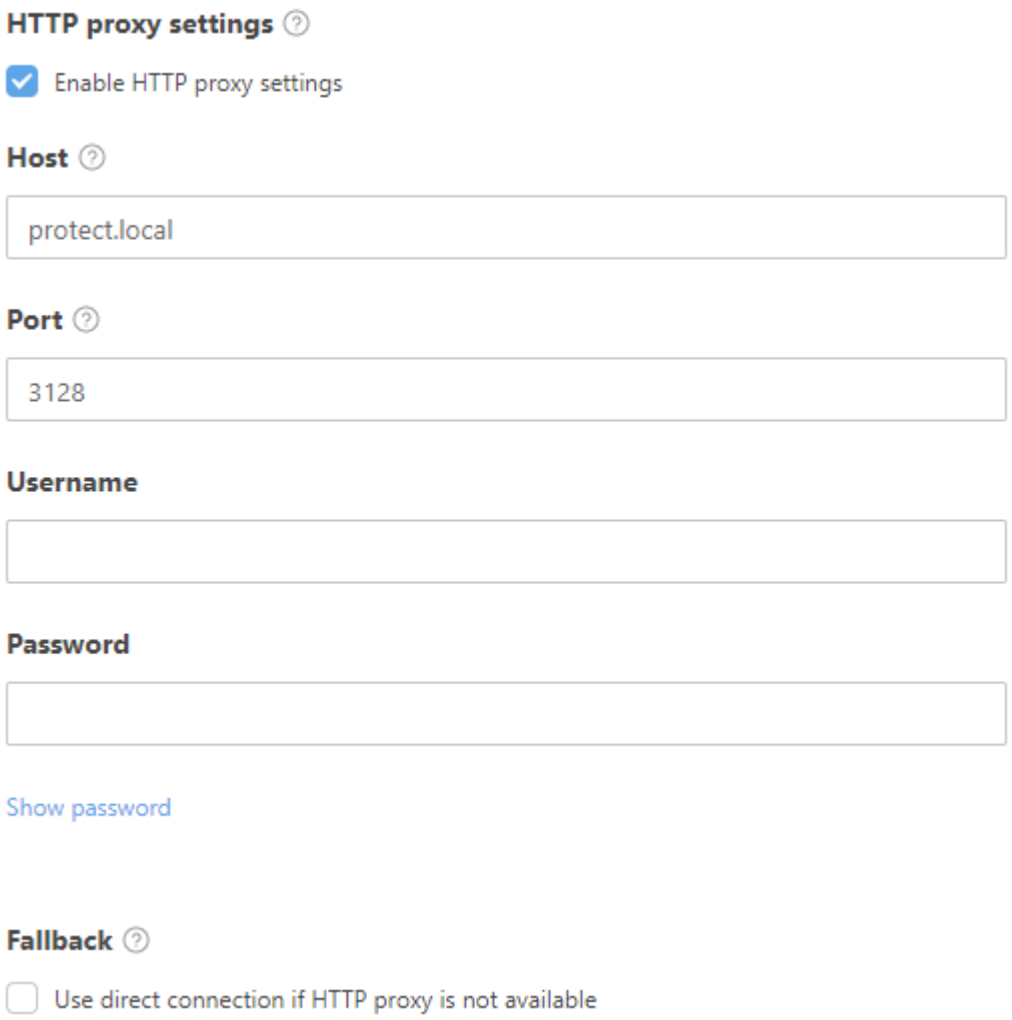
Ativar configurações do proxy http

Se você usa um Proxy HTTP (recomendamos usar o ESET Bridge), marque a caixa de seleção **Ativar configurações de proxy HTTP** e especifique as configurações de Proxy (**Host**, **Porta**, **Nome de usuário** e **Senha**) para fazer o download do instalador via Proxy e configurar uma conexão do Agente ESET Management com o Proxy, para permitir o encaminhamento de comunicação entre o Agente ESET Management e o ESET PROTECT. Servidor. O campo **Host** é o endereço da máquina executando o Proxy HTTP. O ESET Bridge usa a porta 3128 por padrão. Você pode definir uma porta diferente, se necessário. Certifique-se de definir a mesma porta também na configuração do Proxy HTTP (veja Política ESET Bridge).

> O protocolo de comunicação entre o Agente e o ESET PROTECT Servidor não é compatível com autenticação. Qualquer solução de proxy usada para encaminhar a comunicação do Agente para o ESET PROTECT Servidor que precise de autenticação não funcionará.

A caixa de verificação **Usar conexão direta se o proxy HTTP não estiver disponível** está pré-selecionada. O assistente aplica a configuração como um fallback para o instalador – não é possível desmarcar a caixa de seleção. Você pode desativar a configuração usando uma Política do Agente ESET Management:

- Durante a criação do instalador – inclua a política na **Configuração inicial**.
- Depois da instalação do Agente ESET Management – atribua a política ao computador.

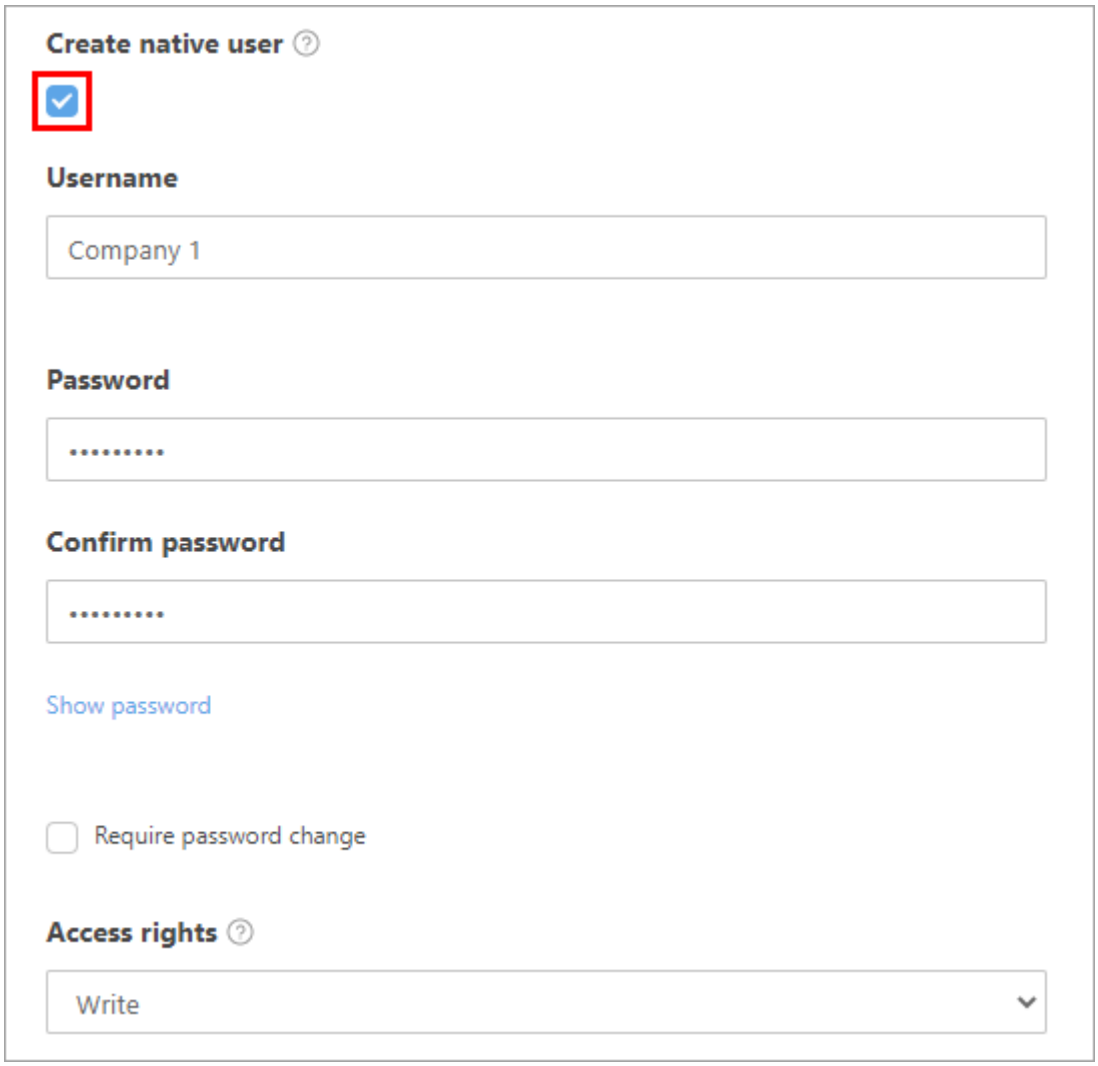


5. Clique em **Continuar** para ir para a seção **Usuário**.

6. Se quiser criar um novo usuário para a empresa (recomendado), marque a caixa de seleção ao lado de **Criar usuário nativo**. O usuário pode entrar no console web e gerenciar os dispositivos da empresa. Digite um nome de usuário (que não contenha os caracteres , ; ") e senha válidos para o novo usuário.

a.**Exigir alteração de senha** – O usuário precisa alterar sua senha depois de entrar pela primeira vez.

b.**Direitos de acesso** – Selecione se o usuário tem acesso de **Leitura e Uso** ou **Gravação** para os objetos da empresa (computadores, políticas, tarefas).



A sincronização do AD não está disponível para usuários criados usando a configuração da empresa MSP.

Problemas para criar um usuário? Certifique-se de ter as permissões necessárias.

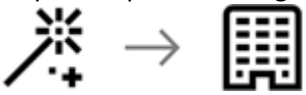
Clique em **Concluir** para preparar os instaladores. Clique no link e faça o download do instalador que você precisa. Você também pode fazer novamente o download o instalador no menu Instaladores, se tiver selecionado salvar o instalador.

Leia como implantar o Agente ESET Management de maneira local ou remota.

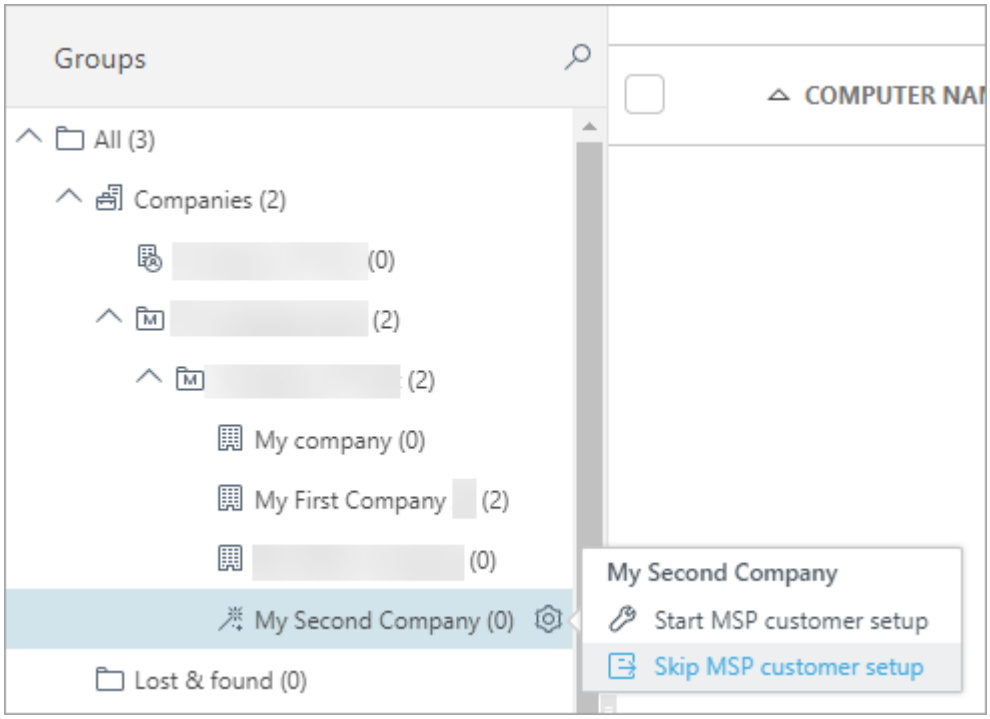
Ignorar configuração do cliente MSP

Você pode **Ignorar a configuração do cliente MSP** se não desejar configurá-la. Opcionalmente, você pode criar um instalador e um novo usuário posteriormente. Não recomendamos ignorar a configuração.

Depois de pular a configuração, o ícone da empresa será alterado como se tivesse sido configurado:



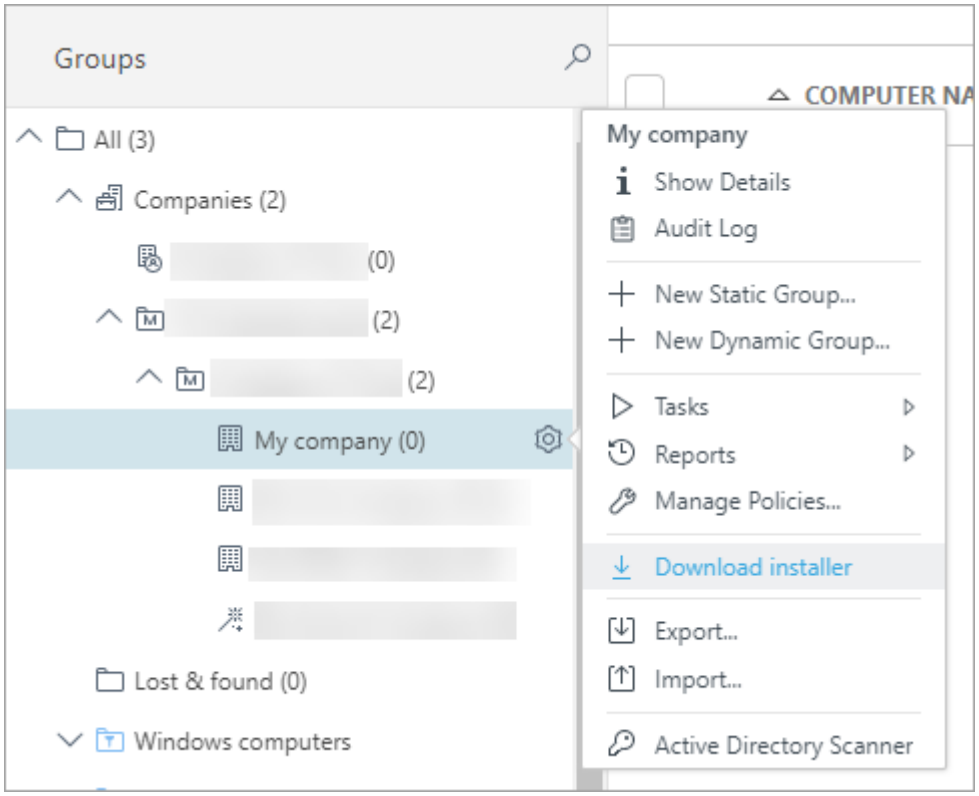
Se você ignorar a configuração, não poderá executar o assistente de configuração para a empresa novamente na mesma instância do ESET PROTECT.



Criar instalador personalizado

1. No console web ESMC, navegue até o menu **Computadores**.

2. Clique no ícone de engrenagem ao lado da empresa para a qual deseja criar o instalador e selecione **Fazer download do instalador**.



3. Você pode criar dois tipos de instaladores:

   • **Instalador apenas do Agente (todas as plataformas)** – você pode instalar este Instalador de script do agente nos computadores Windows, MacOS e Linux.

   • **Instalador tudo-em-um** – o instalador é constituído pelo Agente ESET Management e pelo produto de segurança ESET Business selecionado (Windows).

Se você não ver a opção **Instalador único**, certifique-se de que uma licença esteja atribuída à empresa.

Selecionei o Instalador tudo-em-um

Produto/versão – selecione um produto de segurança ESET que será instalado junto com o Agente ESET Management. Por padrão, a versão mais recente está selecionada (recomendado). Você pode selecionar uma versão anterior.
Selecione o idioma no menu suspenso **Idioma**.
Selecione a caixa de seleção **Aceito os termos do Contrato de licença para o usuário final do aplicativo e reconheço a Política de Privacidade**. Consulte o Acordo de Licença para o Usuário Final (EULA), Termos de Uso e Política de Privacidade dos produtos ESET.

Para salvar o instalador em Instaladores para uso futuro, selecione a caixa de seleção ao lado de **Salvar instalador na seção instaladores**.

Configurações avançadas do instalador (recomendado)

Nome do host do servidor é o endereço onde os Agentes ESET Management se conectam ao Servidor ESET PROTECT. Selecione uma porta diferente para a comunicação entre Agente e Servidor, se necessário. Se você alterar a porta, precisará alterá-la para todos os agentes de conexão e também nas **Mais** > Configurações. Certifique-se de que todos os dispositivos clientes que usarão o instalador podem alcançar o endereço do **Nome de host do servidor**. Consulte as Recomendações do ambiente MSP.

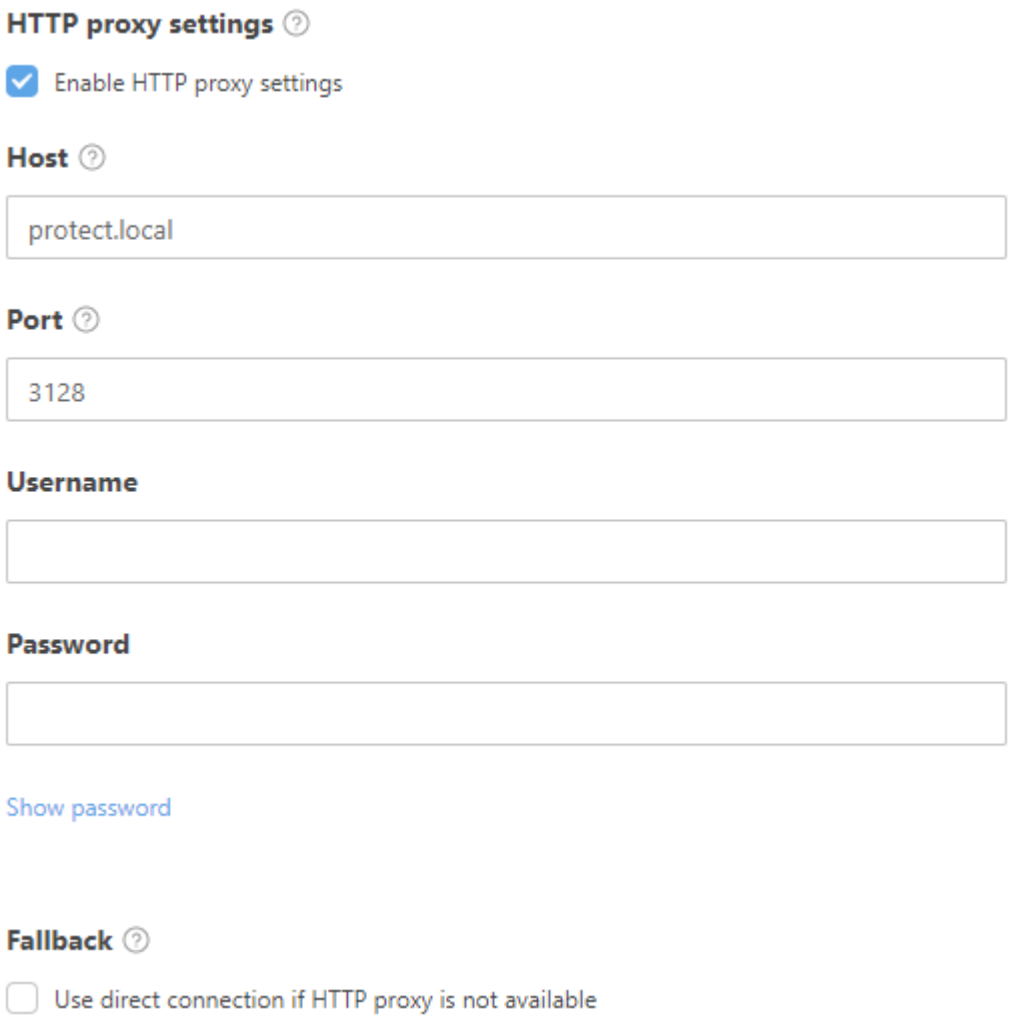
Ativar configurações do proxy http

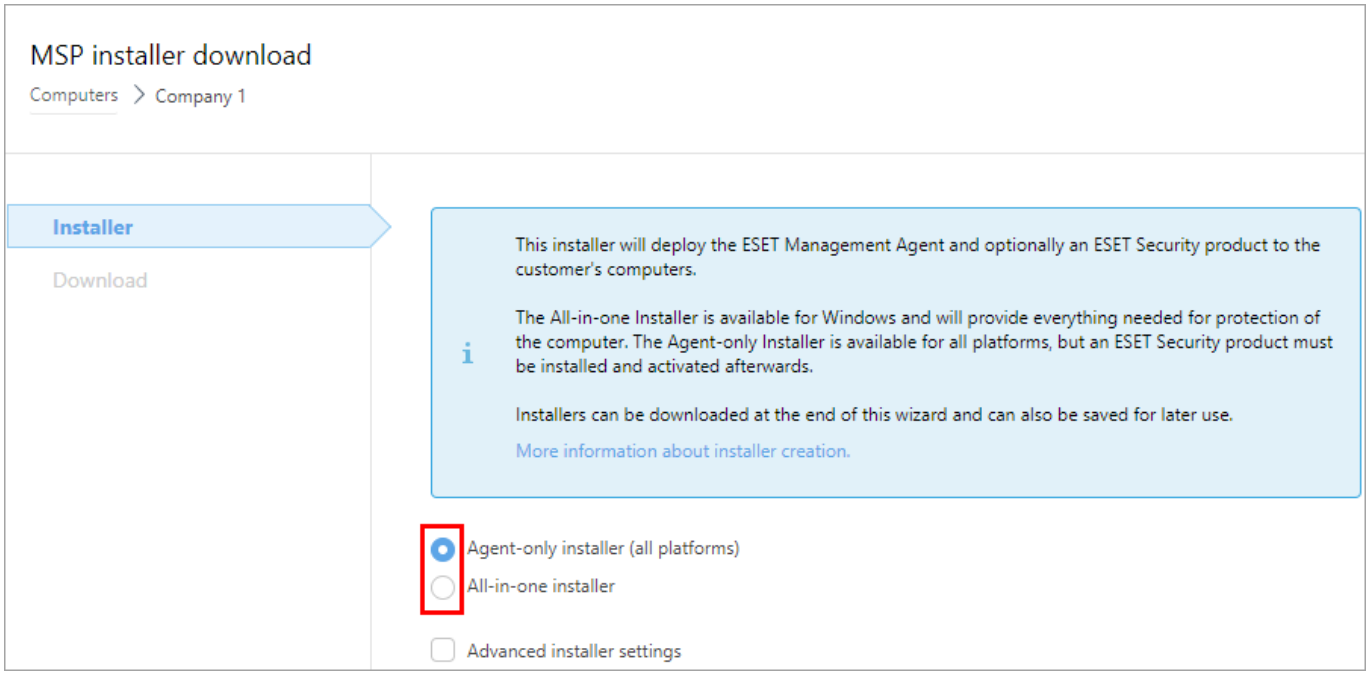
Se você usa um Proxy HTTP (recomendamos usar o ESET Bridge), marque a caixa de seleção **Ativar configurações de proxy HTTP** e especifique as configurações de Proxy (**Host**, **Porta**, **Nome de usuário** e **Senha**) para fazer o download do instalador via Proxy e configurar uma conexão do Agente ESET Management com o Proxy, para permitir o encaminhamento de comunicação entre o Agente ESET Management e o ESET PROTECT. Servidor. O campo **Host** é o endereço da máquina executando o Proxy HTTP. O ESET Bridge usa a porta 3128 por padrão. Você pode definir uma porta diferente, se necessário. Certifique-se de definir a mesma porta também na configuração do Proxy HTTP (veja Política ESET Bridge).

> O protocolo de comunicação entre o Agente e o ESET PROTECT Servidor não é compatível com autenticação. Qualquer solução de proxy usada para encaminhar a comunicação do Agente para o ESET PROTECT Servidor que precise de autenticação não funcionará.

A caixa de verificação **Usar conexão direta se o proxy HTTP não estiver disponível** está pré-selecionada. O assistente aplica a configuração como um fallback para o instalador – não é possível desmarcar a caixa de seleção. Você pode desativar a configuração usando uma Política do Agente ESET Management:

- Durante a criação do instalador – inclua a política na **Configuração inicial**.
- Depois da instalação do Agente ESET Management – atribua a política ao computador.





4. Clique em **Criar** para criar o instalador.

5. Clique no link e faça o download do instalador que você precisa.

Usuários MSP

Se você configurar sua empresa usando a configuração de cliente MSP, poderá criar um tipo especial de usuário nativo (Usuário MSP). Para revisar e editar o usuário navegue até o menu **Mais** > **Direitos de acesso** > **Usuários**.

Você também pode criar um usuário MSP personalizado, por exemplo, para um MSP ou um revendedor.

Permissões necessárias

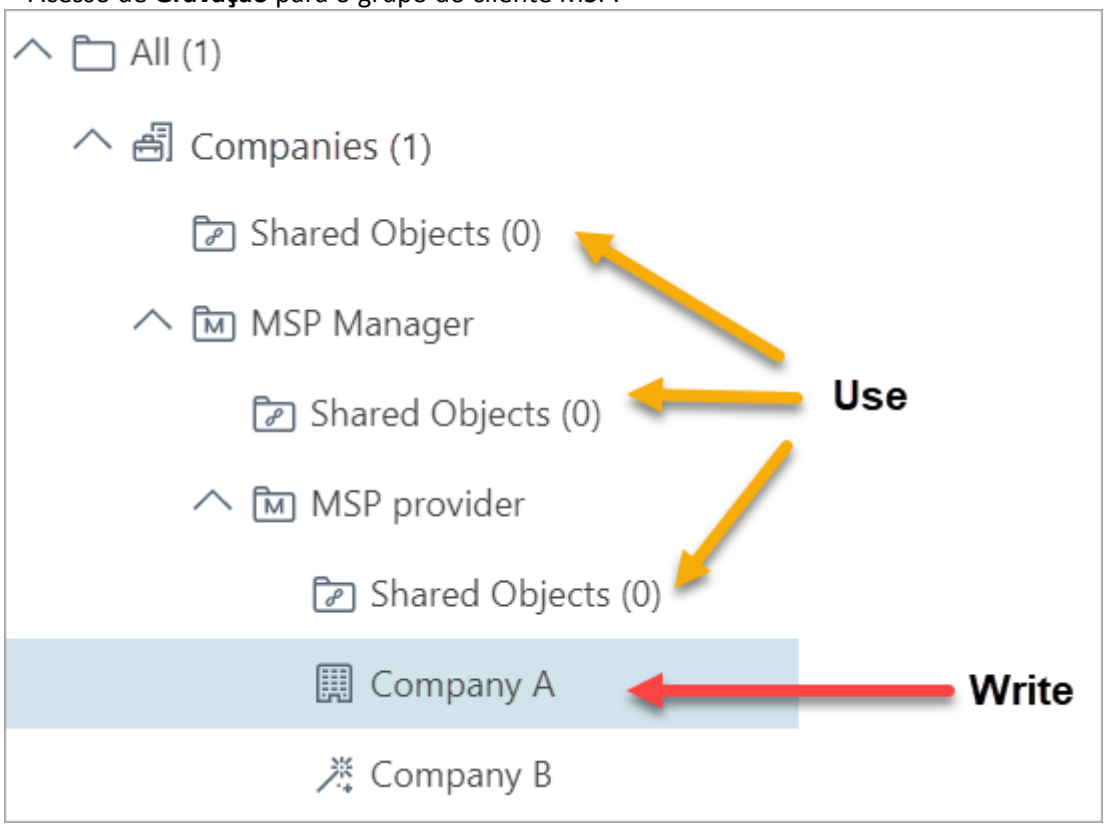
Para criar o novo usuário na configuração do cliente MSP, você precisará ter direitos de acesso para a empresa configurada e para os grupos de **Objetos compartilhados**.

Esquema de permissão detalhado

Configurar uma única empresa

Direitos de acesso necessários para criar um usuário durante a configuração da *Empresa A*:

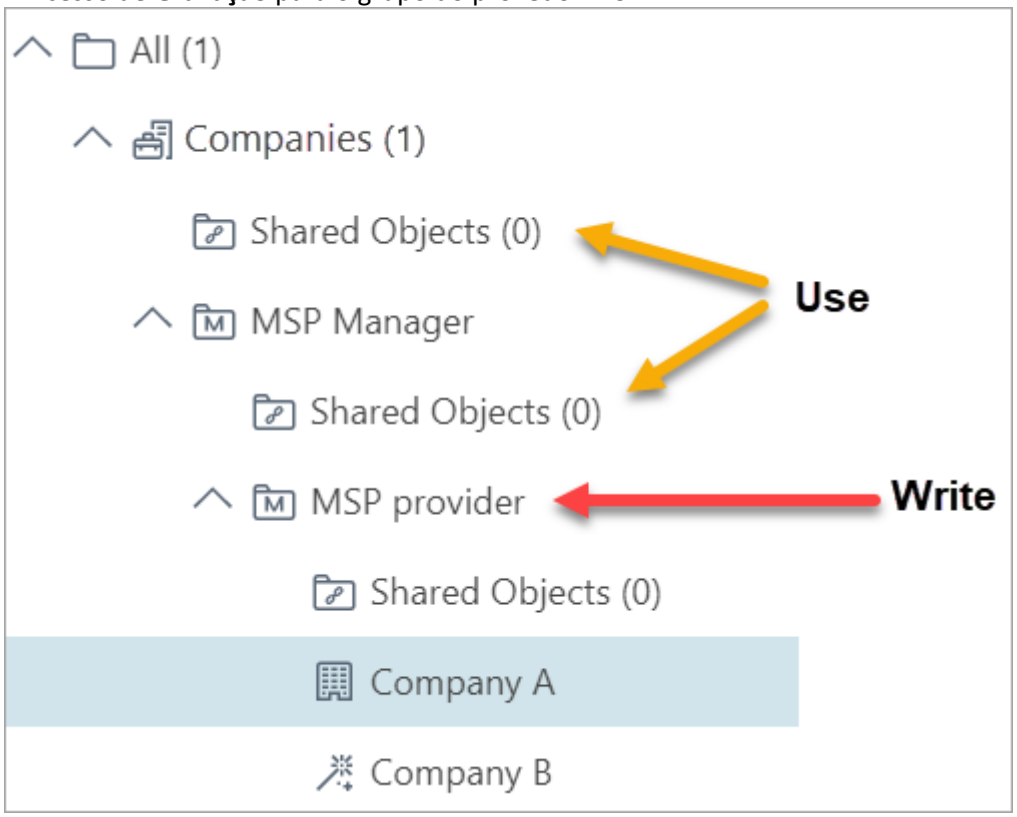
- Acesso de **Uso** para todos os grupos de **Objetos compartilhados**.
- Acesso de **Gravação** para o grupo do cliente MSP.



Configurar todas as empresas de um MSP

Direitos de acesso necessários para criar usuários para todas as empresas que pertencem ao *provedor MSP:*

- Acesso de **Uso** para todos os grupos de **Objetos compartilhados**.
- Acesso de **Gravação** para o grupo do provedor MSP.



Ter direitos de acesso significa que o usuário atual (agindo) tem conjuntos de permissões atribuídos com acesso sobre os grupos, conforme mencionado acima. Se você não tiver os direitos de acesso necessários, a configuração do cliente MSP terminará com um erro.

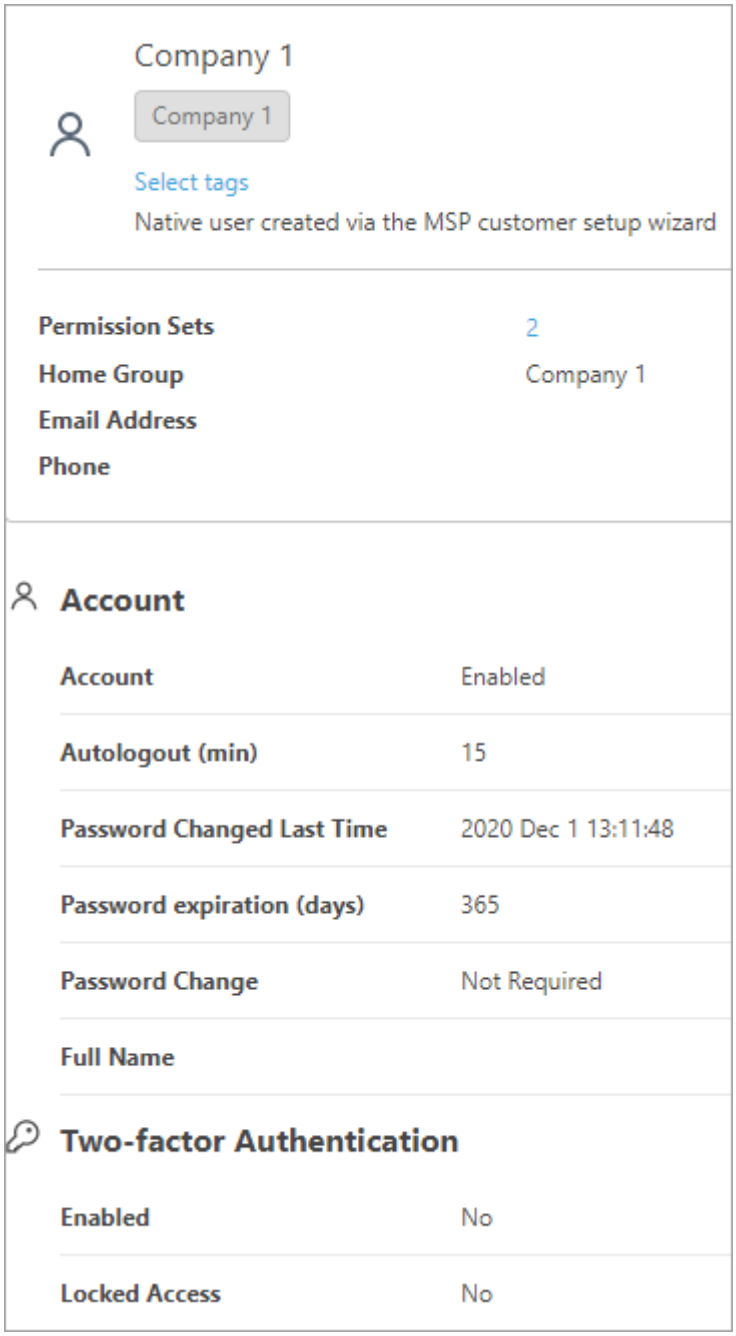
Recursos do usuário MSP

- Eles podem entrar no console web ESET PROTECT e gerenciar dispositivos e outros objetos sobre os quais tenham direitos de acesso.
- Eles podem criar outro usuário nativo com as mesmas permissões ou menos.
- Eles não podem criar Usuários do computador. Se for necessário criar um Usuário do computador, um administrador precisará fazer isso.

A sincronização do AD não está disponível para usuários criados usando a configuração da empresa MSP.

O ESET PROTECT possui as seguintes configurações para cada novo usuário MSP:

- **Descrição** – Usuário nativo criado por meio do assistente de configuração do cliente MSP
- **Marcações** – O usuário é marcado com o nome da empresa
- **Grupo doméstico** – Grupo estático da empresa
- **Sair automaticamente** – 15 minutos
- A conta está ativada e a alteração de senha não é necessária
- **Conjuntos de permissões** – Cada Usuário MSP tem 2 conjuntos de permissões. Um para seu grupo doméstico e outro para os grupos de **Objetos compartilhados**.



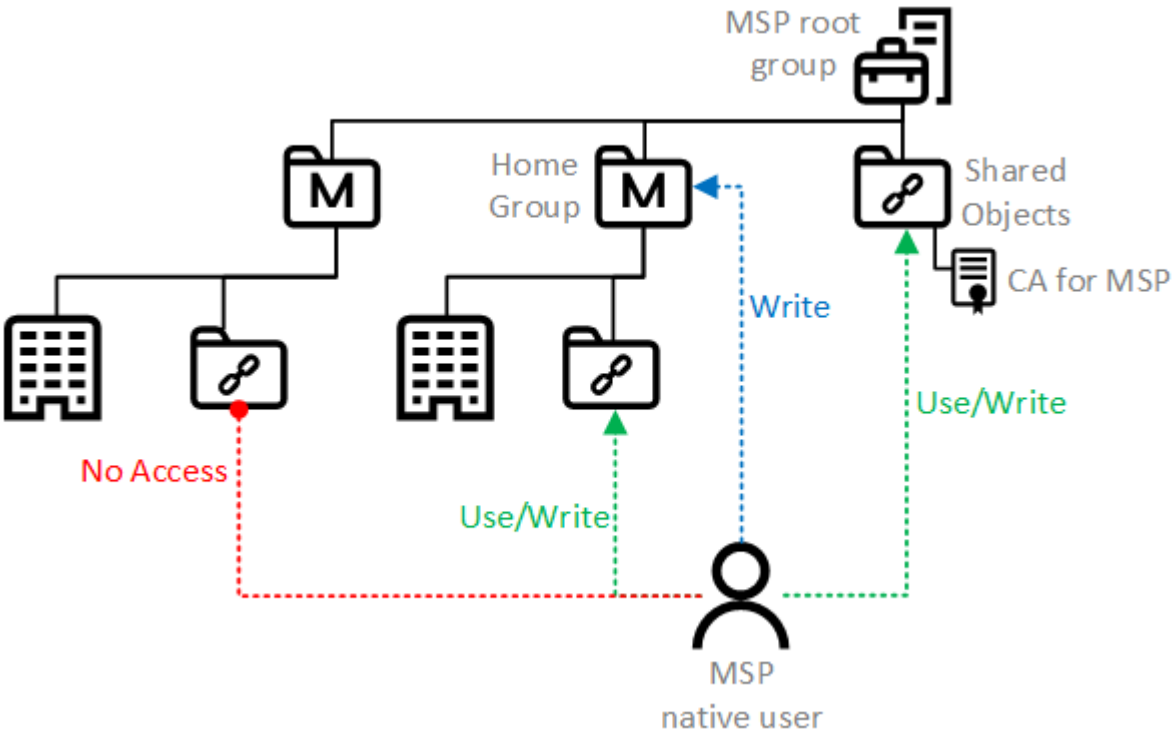
Criar um usuário MSP personalizado

Você pode criar usuários nativos do console web para gerenciar clientes, por exemplo, para um MSP ou um revendedor.

1. Você precisa ter a empresa MSP criada no EMA 2.
2. Verifique se a empresa MSP está sincronizada na árvore MSP.
3. Criar um usuário nativo. Configurações críticas para um usuário MSP personalizado:
    a. O grupo doméstico do usuário está definido para o grupo estático MSP correspondente.
    b. Crie e atribua os seguintes conjuntos de permissões ao usuário:
        i. Permissões de **Gravação** para o grupo doméstico.

ii.**Use** ou **Grave** permissões para os grupos de **Objetos compartilhados**.

> O grupo superior de **Objetos compartilhados** contém a CA do MSP. O acesso à CA do MSP é necessário para o usuário criar um instalador.



Esquema de acesso para um usuário MSP personalizado.

O usuário MSP personalizado criado usando essas etapas é elegível para gerenciar dispositivos do cliente e criar instaladores, mas o usuário não pode gerenciar o Servidor ESET PROTECT ou importar licenças.

Marcação de objetos MSP

Se você importar uma conta MSP válida no ESET PROTECT, você ativa a marcação automática de objetos MSP. Os seguintes objetos são marcados automaticamente:

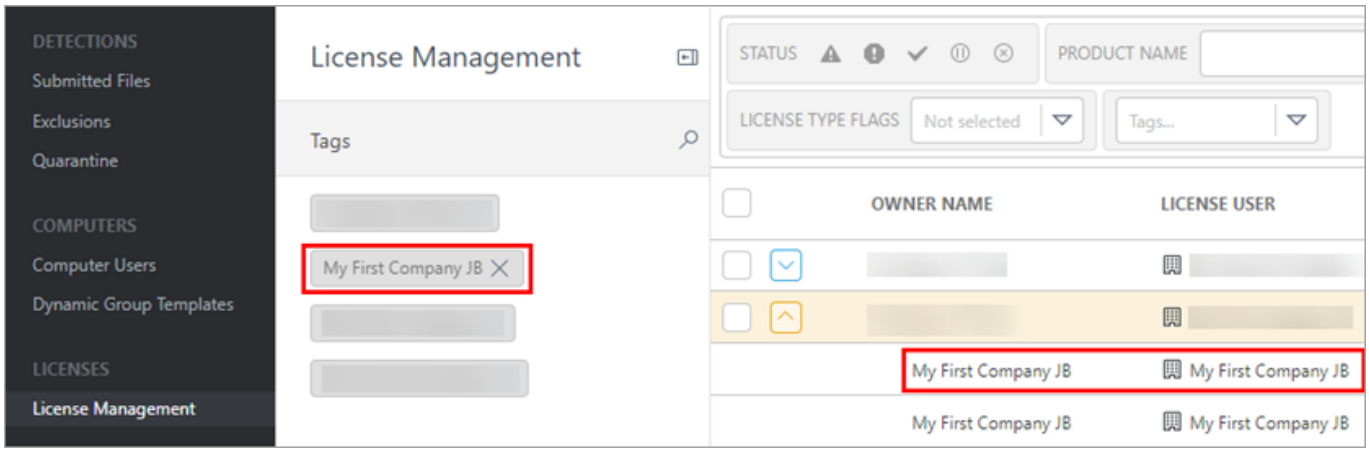
- Licenças importadas por meio da conta MSP
- Instaladores
- Usuários e seus Conjuntos de permissões criados usando a configuração do cliente MSP

A marcação é uma forma de rótulo usada para melhorar a filtragem de objetos.

- O nome da marcação automática é igual ao **Usuário da licença** (Nome da empresa no EMA 2, exceto os caracteres , " que o ESET PROTECT retira da marcação).
- Se você renomear o Cliente no EMA 2 depois da sincronização, as marcações não serão atualizadas.

- Você pode adicionar mais marcações personalizadas a qualquer objeto, se quiser.
- Você pode remover as marcas sem afetar os objetos marcados.

Clique no ícone expandir para visualizar a guia **Marcações**.



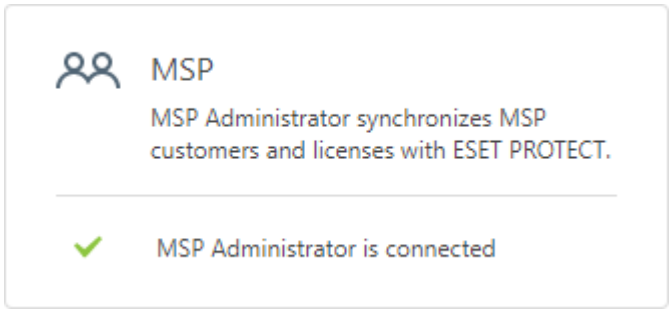
Visão geral do status MSP

A seção Visão geral do status fornece informações complexas sobre o seu status do ESET PROTECT. Se você importar uma conta MSP, há um bloco MSP disponível com informações relacionadas ao MSP.

Status MSP

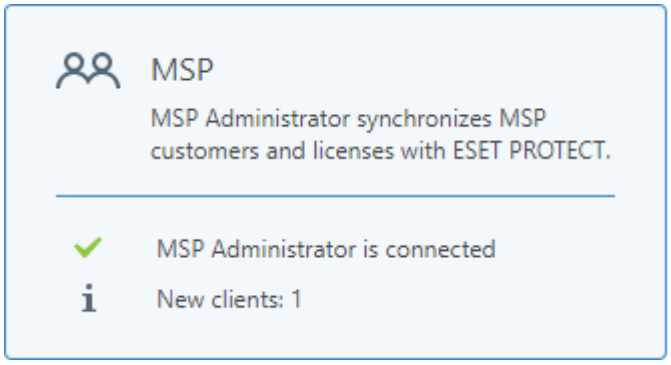
Conta sincronizada

Sua conta está sincronizada e nenhuma ação é necessária.



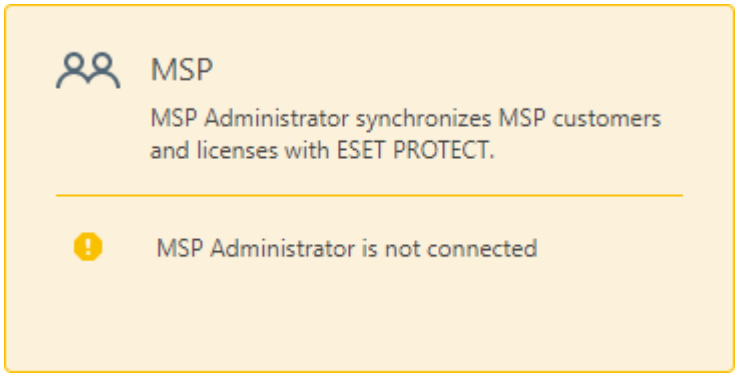
Sincronização em andamento

Há uma sincronização em andamento da conta MSP sendo executada em segundo plano. A sincronização pode levar várias horas para contas grandes. O bloco ficará branco após a sincronização.



Conta desconectada

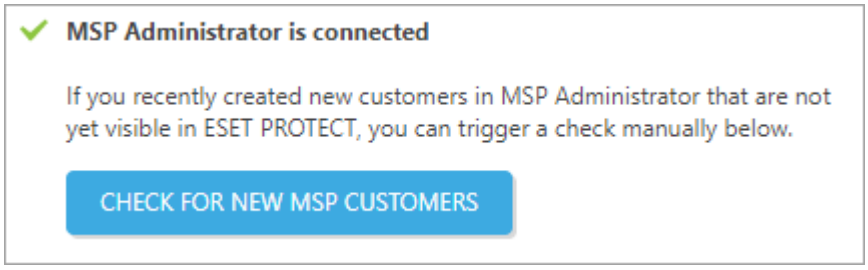
Existem alguns grupos MSP (partes da árvore MSP) na sua Estrutura de grupos estáticos, mas não há uma conta MSP correspondente importada. Isso pode ocorrer se você remover sua conta MSP do Gerenciamento de licença.



Ações disponíveis

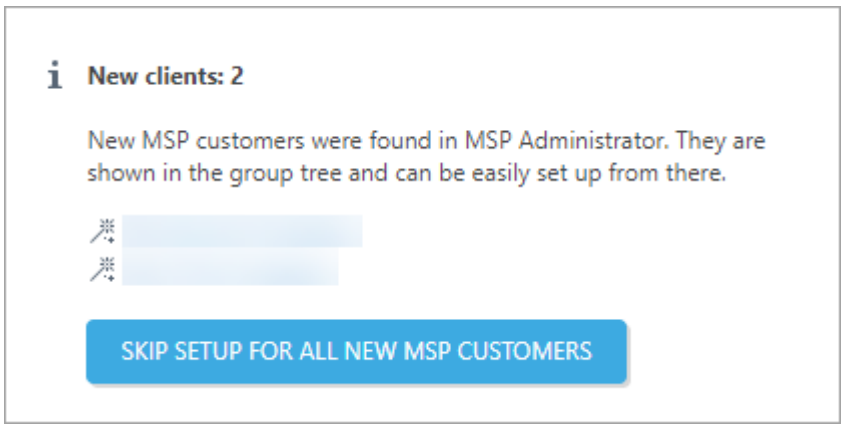
Clique no bloco MSP para ver mais detalhes.

- **Verifique se há novos clientes MSP** – Execute a sincronização de licença sob demanda (atualize a árvore MSP).

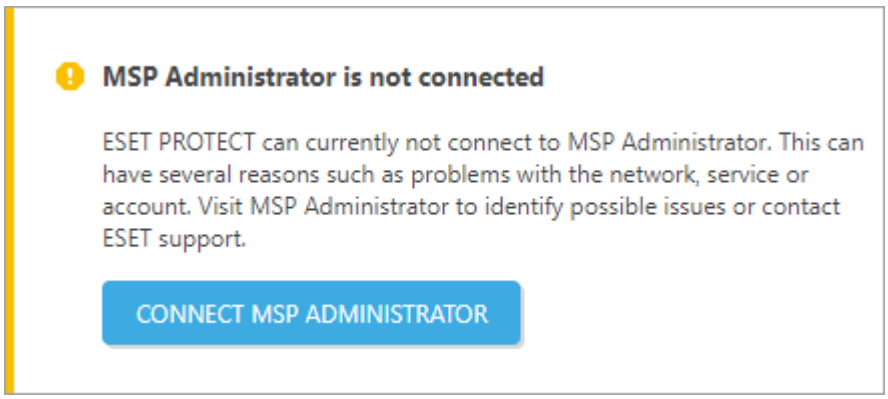


- **Novos clientes** – Se algumas empresas não estiverem configuradas, clique nelas e siga o assistente de configuração do cliente.

- **Ignorar configuração para todos os novos clientes MSP** – Ignorar assistentes de configuração para todas as empresas que não estão configuradas.



• **Conectar Administrador MSP** – Você pode adicionar sua conta MSP para importar suas licenças e estrutura MSP.



Removendo uma empresa

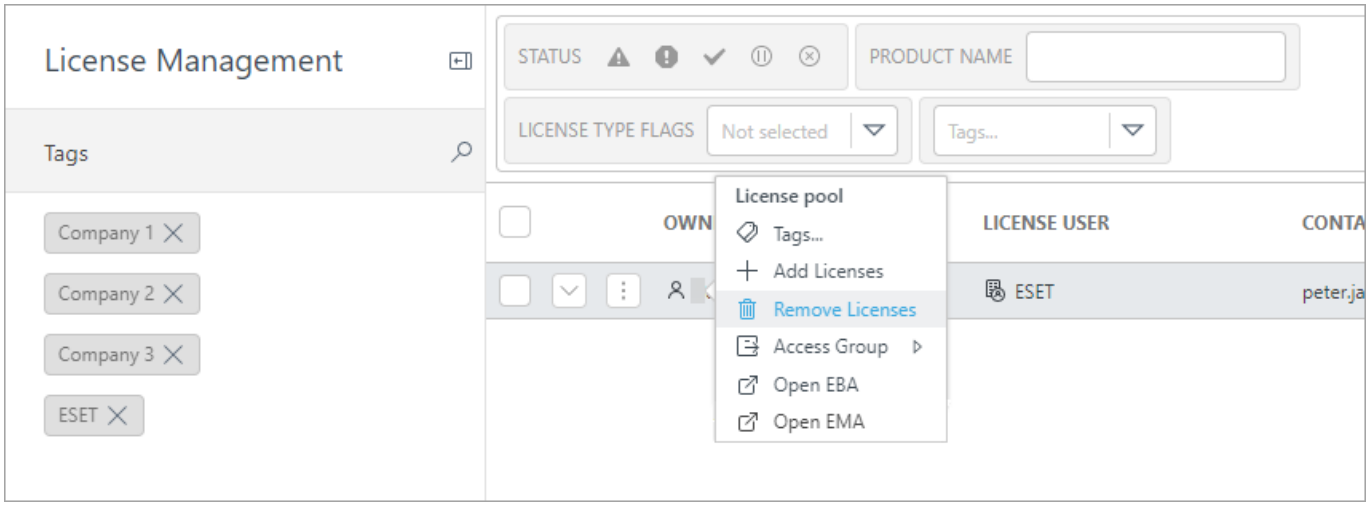
A árvore MSP é sincronizada com a conta MSP. Você precisa remover a conta MSP do Gerenciamento de licenças para desbloquear a árvore MSP. Depois de remover a conta, todas as empresas gerenciadas por essa conta são desvinculadas da árvore MSP.

Se você parar de gerenciar uma empresa, remova os Agentes ESET Management dos computadores dessa empresa. Não é possível remover a empresa da árvore MSP sem remover toda a conta MSP do seu gerenciamento de licenças.
O grupo estático MSP é persistente. Depois de sincronizar a árvore MSP, você nunca pode remover o grupo raiz MSP, apenas seus grupos secundários.

Como remover a conta MSP e as empresas da árvore MSP

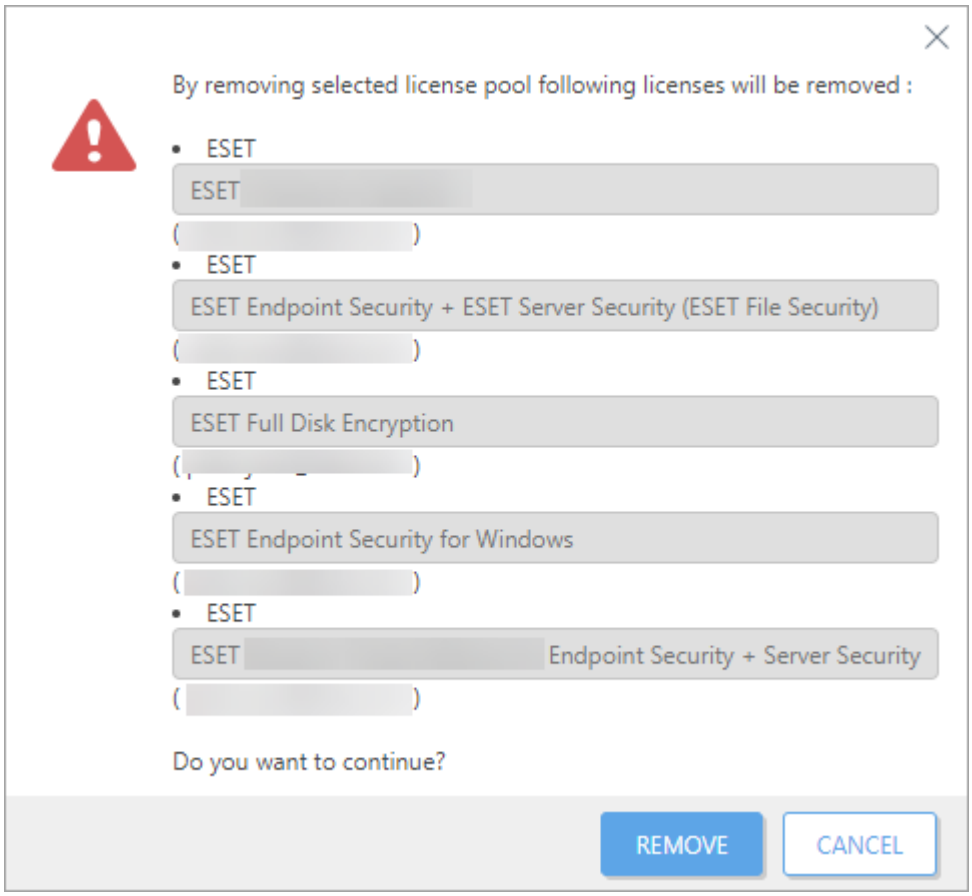
1. Entre no console web ESET PROTECT e navegue até **Mais** > **Gerenciamento de licença**.

2. Clique na licença que você deseja remover > **Remover licenças**. Lembre-se de que, se você remover qualquer licença vinculada a uma conta MSP, a conta inteira e suas licenças vinculadas serão removidas do ESET PROTECT.



3. Confirme sua escolha de remover (desvincular) as licenças listadas do Gerenciamento de licença.

Ao remover qualquer pool de licenças, você remove automaticamente todos os outros pools de licenças associados à mesma conta.
Por exemplo, as licenças da *Empresa X* foram importadas usando as credenciais joe@test.me do EMA 2. Se um usuário remover as licenças da *Empresa X*, todas as licenças importadas das contas EBA e EMA 2 joe@test.me serão removidas do Gerenciamento de licença.



4. Aguarde alguns momentos depois da ação e navegue até o menu **Computadores**.

5. Agora você pode clicar e **Remover** qualquer empresa que fazia parte da Árvore MSP. Você só pode remover uma empresa (seu grupo estático) se o grupo estiver vazio.

Depois de remover a conta MSP do Gerenciamento de licenças, você receberá o status **O Administrador MSP não está conectado** na Visão geral do status. Você precisa remover todos os grupos da sua antiga árvore MSP (no menu **Computadores**) para desativar esse status.

Atualizações automáticas

Há vários tipos de atualizações automáticas de produtos ESET:

- Atualização automática do Agente ESET Management
- Atualização automática de produtos de segurança ESET
- Atualizar ESET PROTECT
- Atualizar componentes de terceiros

Veja também a política de Fim da vida útil ESET para produtos empresariais.
Veja também Quais são os diferentes tipos de atualização de produto ESET e lançamentos?
As atualizações automáticas não funcionarão se você usar um repositório off-line que não contenha metadados (por exemplo, se você copiou instaladores em uma unidade de rede compartilhada). Use a Ferramenta de imagem para criar um repositório off-line compatível com atualizações automáticas. O repositório off-line da Ferramenta de imagem distribui as atualizações automáticas simultaneamente por toda a rede (um repositório on-line distribui gradualmente as atualizações automáticas).

Atualização automática do Agente ESET Management

ESET PROTECT oferece uma atualização automática (auto-atualização) do Agente ESET Management em computadores gerenciados.

Requisitos de atualização automática do Agente ESET Management

- Agente ESET Management 8.1 e versões posteriores.
- A atualização automática do Agente começa a funcionar depois de instalar a versão do servidor ESET PROTECT posterior a 8.1 (ou atualizar para a versão do servidor ESET PROTECT posterior a 8.1).

Como a atualização automática do Agente ESET Management funciona

- O Agente atualiza para a versão mais recente compatível com o servidor ESET PROTECT instalado. Essa normalmente é a versão do servidor ESET PROTECT instalado (por exemplo, 10.0).

• A atualização automática do Agente está ativada por padrão. Ela pode ser desabilitada em Política do Agente ESET Management > **Atualizações** > desativar a alternância **Ativar atualização automática**.

• A atualização automática do Agente ESET Management é acionada em torno de duas semanas depois da versão mais recente do Agente ESET Management ser lançada no repositório.

Quando uma nova versão do Agente ESET Management estiver disponível e a atualização automática ainda não tiver ocorrido, você pode iniciar a atualização do Agente manualmente do **Painel** > Status da versão do componente.
Alternativamente, você pode usar a tarefa do cliente ESET PROTECT Atualização de componentes.

• O design da atualização automática garante um processo de atualização em fases distribuído durante um período maior, para impedir um maior impacto na rede e nos computadores gerenciados.

• As atualizações automáticas não funcionarão se você usar um repositório off-line que não contenha metadados (por exemplo, se você copiou instaladores em uma unidade de rede compartilhada). Use a Ferramenta de imagem para criar um repositório off-line compatível com atualizações automáticas. O repositório off-line da Ferramenta de imagem distribui as atualizações automáticas simultaneamente por toda a rede (um repositório on-line distribui gradualmente as atualizações automáticas).

Atualização automática de produtos de segurança ESET

O ESET PROTECT versão 9.0 inclui um recurso para manter os produtos de segurança ESET atualizados para a versão mais recente nos seus computadores gerenciados.

Atualizações de produtos automáticas são ativadas automaticamente em uma nova instalação ESET PROTECT.

• Você deve ter um produto de segurança ESET elegível para usar o recurso Atualizações automáticas. Veja a lista de produtos empresariais ESET compatíveis com as atualizações automáticas. Outros produtos de segurança ESET não são compatíveis com atualizações automáticas e a ESET vai adicionar esse recurso a eles no futuro.
• Você pode configurar atualizações automáticas através de uma Política.
• Veja também o FAQ de Atualizações automáticas. A primeira atualização automática vai acontecer quando uma versão futura da versão 9.x lançada inicialmente for lançada (por exemplo, 9.1 ou 9.0.xxxx.y, onde xxxx é superior à primeira versão 9.x). Para garantir o máximo de estabilidade de atualização, as atualizações de produtos automáticas têm uma distribuição atrasada depois do lançamento global de uma nova versão do produto de segurança ESET. Enquanto isso, o Web Console pode reportar o produto de segurança ESET como desatualizado.
• Veja também Quais são os diferentes tipos de atualização de produto ESET e lançamentos?
• As atualizações automáticas não funcionarão se você usar um repositório off-line que não contenha metadados (por exemplo, se você copiou instaladores em uma unidade de rede compartilhada). Use a Ferramenta de imagem para criar um repositório off-line compatível com atualizações automáticas. O repositório off-line da Ferramenta de imagem distribui as atualizações automáticas simultaneamente por toda a rede (um repositório on-line distribui gradualmente as atualizações automáticas).

Siga uma das opções abaixo para atualizar os produtos de segurança ESET em sua rede para uma versão compatível com atualizações automáticas:

- Use a ação em um clique em **Painel** > **Visão geral do status** > **Status da versão do componente** > clique no gráfico de barras e selecione **Atualizar componentes ESET instalados**.
- Em **Computadores**, clique no ícone de engrenagem ao lado do Grupo estático **Todos** e selecione **Tarefas** > **Atualizar** > **Atualizar produtos ESET**.
- Use a Tarefa do cliente de Instalação de software.
- Se você atualizou do ESET PROTECT 8.x ou ESMC 7.2, você pode usar a atualização com um clique na janela **Atualizações de produtos automáticas**.

Há duas maneiras de atualizar os produtos de segurança ESET para a versão mais recente:

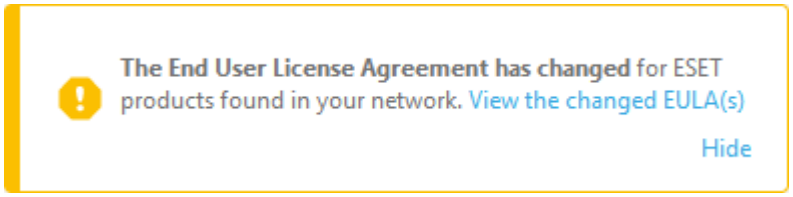
- Tarefa do cliente de instalação de software
- Recurso de atualização automática

Diferenças entre a Tarefa do cliente de Instalação de software e o recurso de Atualizações automáticas:

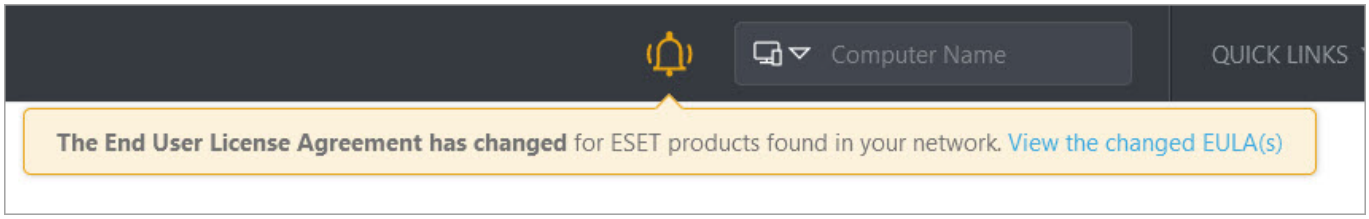
	Processo de atualização	Reiniciar depois da atualização	Atualizações futuras
Tarefa do cliente de instalação de software	O processo de atualização inclui a reinstalação do produto de segurança ESET.	A atualização do produto de segurança ESET requer a reinicialização imediata do computador por motivos de segurança (para garantir a funcionalidade completa do produto de segurança ESET atualizado).	Manual – o administrador deve iniciar cada atualização futura executando a Tarefa do cliente de instalação de software. Veja as opções disponíveis acima.
Atualizações automáticas	O processo de atualização não inclui a reinstalação do produto de segurança ESET.	A atualização do produto de segurança ESET requer a reinicialização do computador, mas não imediatamente. A atualização acontece depois da próxima reinicialização do computador. O administrador ESET PROTECT pode aplicar a atualização do computador e reiniciar remotamente a partir do Web Console usando a Tarefa do cliente Desligar computador com a caixa de seleção **Reiniciar computador** selecionada.	Automático – atualizações automáticas de produtos de segurança ESET compatíveis quando uma nova versão é lançada (a atualização é atrasada por motivos de estabilidade).

Acordo de licença para o usuário final atualizado de produtos de segurança ESET gerenciados

O Web Console ESET PROTECT notifica o administrador se um Acordo de licença para o usuário final (EULA) atualizado de um produto de segurança ESET gerenciado estiver disponível.

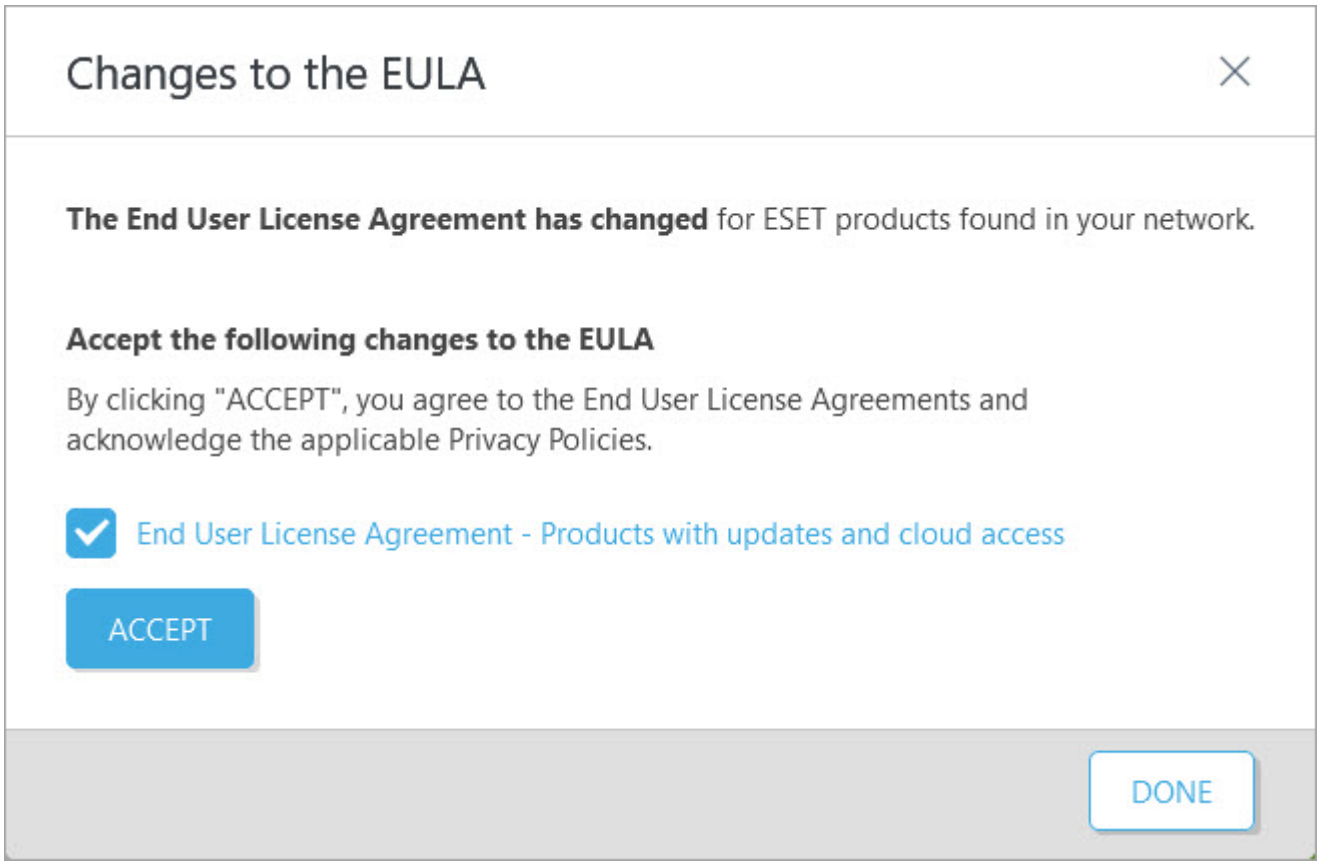


Clique em **Exibir o(s) EULA(s) alterado(s)** para ver os detalhes ou em **Ocultar** para mover a notificação sob um ícone de anel amarelo na barra de ferramentas superior.



Quando você clica em **Exibir o(s) EULA(s) alterado(s)**, uma nova janela será exibida com detalhes sobre o produto de segurança ESET e suas alterações do Acordo de Licença para o Usuário Final:

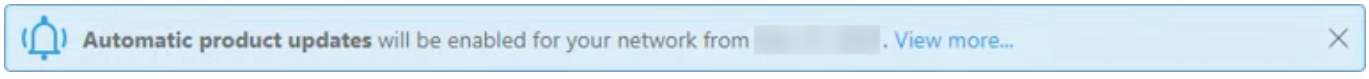
- Se você tiver versões anteriores de produtos de segurança ESET que não são compatíveis com atualizações automáticas (por exemplo, ESET endpoint 8.x e versões anteriores), clique em **Aceitar** para aceitar o Acordo de Licença para o Usuário Final atualizado e ative a atualização para uma versão que é compatível com atualizações automáticas.



- Se você tiver produtos empresariais ESET que são compatíveis com atualizações automáticas (por exemplo, versão do ESET endpoint 9 e versões posteriores), você receberá uma notificação sobre o Acordo de Licença para o Usuário Final atualizado, mas não precisará aceitar (o botão **Aceitar** não estará disponível) para atualizar os produtos de segurança ESET para versões posteriores.

Depois da atualização a partir de uma versão anterior do ESET PROTECT

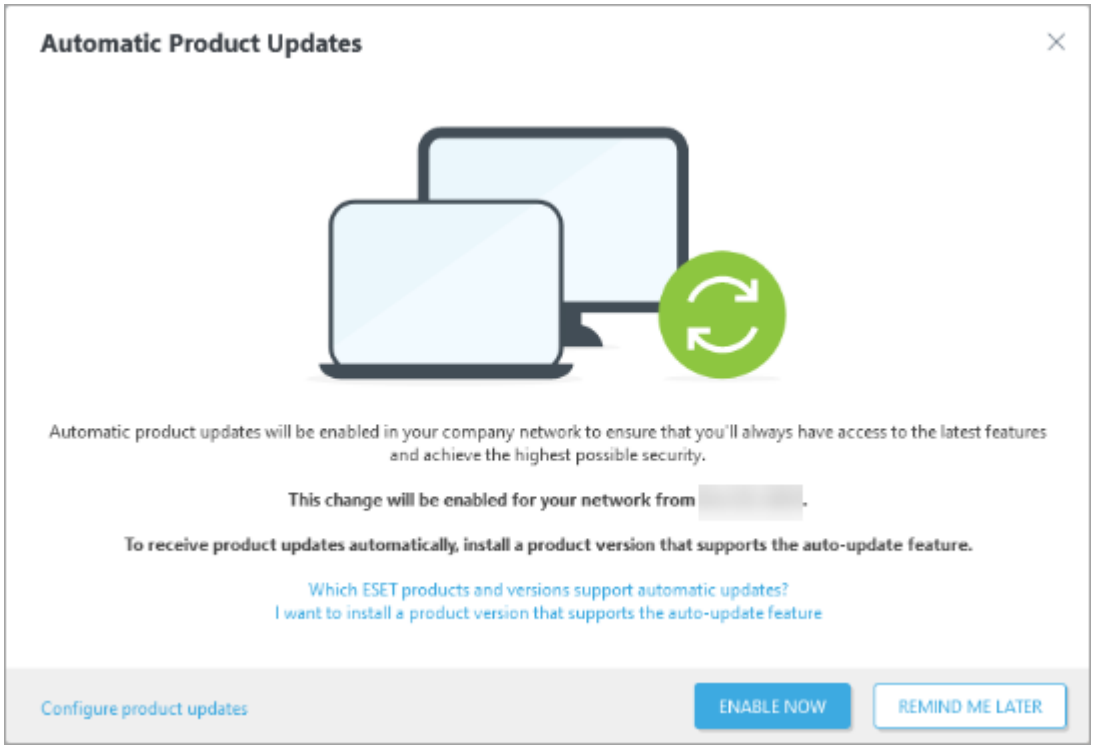
Se você atualizou de uma versão anterior do ESET PROTECT (ou do ESMC 7.2) para o ESET PROTECT 10.0, o Web Console vai exibir a notificação de **Atualizações de produto automáticas**.



Atualizações de produtos automáticas serão ativadas automaticamente em todos os computadores gerenciados

(**Grupo estático** Todos) 60 dias a partir do dia em que a notificação aparecer. Se você desativar as atualizações automáticas a notificação não desaparecerá, mas você poderá desconsiderá-la.

Clique em **Exibir mais** para configurar atualizações automáticas de produtos e a janela **Atualizações de produtos automáticas** vai aparecer:



Clique em **Ativar agora** para ativar atualizações automáticas em todos os computadores gerenciados (Grupo estático **Todos**) imediatamente.

Clique em **Configurar atualizações de produto** para configurar a política de atualizações automáticas.

Clique em **Quero instalar uma versão do produto compatível com o recurso de atualização automática** na janela **Atualizações de produto automáticas** e o ESET PROTECT exibirá uma opção de atualização com um clique (uma Tarefa do cliente de instalação de software).

Configurar atualizações de produto automáticas

Você pode configurar atualizações automáticas através da política do recurso **Atualizações automáticas** cobrindo produtos de segurança ESET compatíveis com o Grupo estático **Todos** como destino padrão.

Alterar os destinos internos da política de Atualizações automáticas

No Web Console ESET PROTECT, clique em **Políticas** > abra **Políticas internas** > clique na política > selecione **Alterar atribuições** > ajuste os destinos > clique em **Concluir**.

Configurar atualizações automáticas

Criar uma nova política de **Atualizações automáticas** para configurar atualizações automáticas.

1. Web Console ESET PROTECT, clique em **Políticas** > **Nova política** > **Configurações**.

2. Selecione **Atualizações automáticas** do menu suspenso e configure as configurações de política:

- **Atualizações automáticas** – as atualizações automáticas estão ativadas por padrão.

Para desativar atualizações automáticas, desligue a alternância **Atualizações automáticas**. Veja também Desabilitar atualizações automáticas.

- **Parar atualizações em** – opcionalmente, você pode definir a versão do produto de segurança ESET que vai parar de atualizar automaticamente:
  - Clique em **Selecionar do repositório** e selecione a versão.
  - Digite a versão – você pode usar * como um caractere curinga, por exemplo, 9.*/9.0.*/9.0.2028.*.

Por exemplo, se você digitar 9.0.*, todas as correções da versão secundária 9.0 serão instaladas.

Essa configuração não se aplica a atualizações de segurança e estabilidade instaladas automaticamente independentemente da versão definida ou do estado de configuração de atualizações automáticas. Veja também Quais são os diferentes tipos de atualização de produto ESET e lançamentos?

3. Clique em **Atribuir** para selecionar destinos de política (grupos ou computadores individuais).

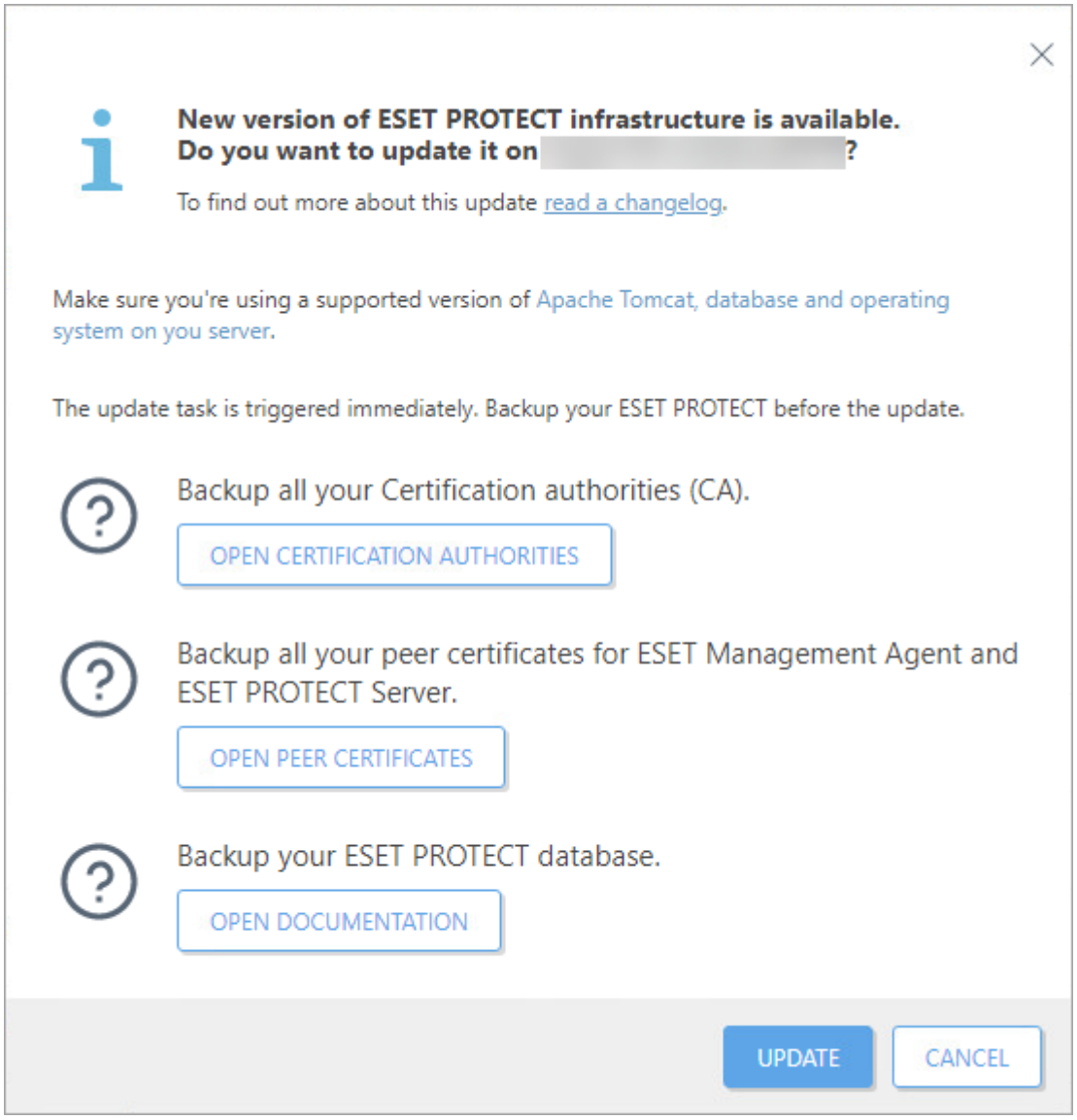
Certifique-se de que a política de atualizações automáticas interna não substitui as configurações de política de atualizações automáticas criadas. Leia mais sobre a aplicação de políticas em clientes.

4. Clique em **Concluir**.

Atualizar ESET PROTECT

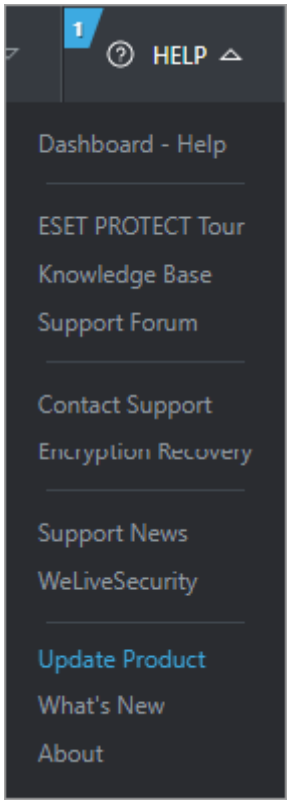
O Servidor ESET PROTECT verifica regularmente se há atualizações disponíveis para a infraestrutura ESET PROTECT.

Quando uma atualização está disponível, uma janela aparece:



Você pode ler sobre as mudanças na atualização do ESET PROTECT disponível clicando em **ler um relatório de mudanças**.

Se você não selecionar a atualização, é possível exibir a janela de atualização clicando em **Ajuda** > **Atualizar produto**:



Apenas usuários que podem executar a tarefa de cliente ESET PROTECT Atualização dos componente podem ver a notificação de atualização.

Certifique-se de estar executando uma versão compatível do Apache Tomcat, banco de dados e sistema operacional no seu servidor.

1. Clique no botão **Abrir Autoridades de certificação** e faça o backup de todas as suas CAs.

2. Clique no botão **Abrir certificados de mesmo nível** e faça backup de todos os seus certificados.

3. Clique no botão **Abrir documentação** e faça backup do banco de dados ESET PROTECT.

4. Clique no botão **Atualizar**.

5. Selecione a caixa de seleção **Aceito os termos do Contrato de licença para o usuário final do aplicativo e reconheço a Política de Privacidade**. Consulte o Acordo de Licença para o Usuário Final (EULA), Termos de Uso e Política de Privacidade dos produtos ESET.

6. Clique no botão **Atualizar**. Uma atualização do seu Servidor ESET PROTECT está agendada – nas **Tarefas do cliente** é possível encontrar uma nova tarefa do cliente que atualiza os componentes do ESET PROTECT no computador onde o Servidor ESET PROTECT está instalado. Você será desconectado do Web Console quando a atualização começar. Você poderá entrar depois da atualização ser concluída.

Para atualizar componentes ESET PROTECT nos dispositivos conectados ao Servidor ESET PROTECT para a versão mais recente, é possível acionar a tarefa de ESET PROTECTAtualização de componentes diretamente da janela de atualização.

Nem todos os componentes do ESET PROTECT são atualizados automaticamente – alguns componentes precisam de uma atualização manual.

O ESET PROTECT é compatível com a atualização automática do Agente ESET Management em computadores gerenciados.

Atualizar 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:
Microsoft SQL Server	2019 (compilação 15.0.4261.0)	Determine sua versão e edição do Mecanismo de banco de dados do SQL Server e instale a atualização cumulativa mais recente.
MySQL	8.0.0.0	Clique em **Ajuda** > **Sobre** no Web Console ESET PROTECT para ver a versão do banco de dados instalado.
Sistema operacional	Windows Server 2016	O ESET PROTECT não reporta as atualizações disponíveis para o Linux.
Apache Tomcat	9.0.65	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`
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`

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.

Siga as instruções de atualização para componentes de terceiros:

- Servidor do banco de dados
- Sistema operacional
- Apache Tomcat
- Java Runtime Environment

Apache HTTP Proxy usuários
A partir do ESET PROTECT 10.0, o ESET Bridge substitui o Apache HTTP Proxy. O Apache HTTP Proxy chegou a Suporte limitado. Se você usar o Apache HTTP Proxy, recomendamos migrar para o ESET Bridge.

FAQ

Lista de perguntas

Como resolver o erro Falha no login: Falha na conexão com estado **'não conectado'**?

Verifique se o serviço do Servidor ESET PROTECT está em execução ou o serviço do Microsoft SQL Server. Se não, inicie. Se não, inicie. Se estiver em execução reinicie o serviço, atualize o console da web e tente fazer login novamente. Para mais informações, consulte Solução de problemas de login.

Para que o grupo "**Achados e Perdidos**" é usado?

Cada computador que se conecta ao servidor ESET PROTECT e não é membro de um grupo estático é exibido automaticamente nesse grupo. Você pode trabalhar com o grupo e os computadores dentro deles como se fossem computadores em qualquer outro grupo estático. O grupo pode ser renomeado, copiado ou movido sob outro grupo mas não pode ser excluído.

Como criar um perfil de atualização duplo?

Consulte nosso artigo da Base de conhecimento ESET para instruções passo a passo.

Como atualizar as informações em uma página ou em uma seção da página sem atualizar toda a janela do navegador?

Clique em **Atualizar** no menu de contexto no canto superior direito de uma seção da página.

Como executar uma instalação silenciosa do Agente ESET Management?

Os métodos a seguir permitem a você realizar uma instalação silenciosa:

- Script GPO ou SCCM
- Tarefa Implantação do Agente
- ESET Remote Deployment Tool

O RD Sensor não detecta todos os clientes na rede.

O Sensor RD escuta passivamente a comunicação de rede na rede. Se os PCs não estiverem se comunicando, eles não estão listados pelo Sensor RD. Verifique suas configurações DNS para se certificar de que os problemas com busca de DNS não estão impedindo a comunicação.

Como redefinir a Contagem de detecções ativas mostrada no ESET PROTECT depois de limpar as detecções?

Para redefinir o número de detecções ativas, um (escaneamento detalhado) completo precisa ser iniciado através do ESET PROTECT no computador de destino. Se você limpou uma detecção manualmente, pode marcá-la como resolvida.

Como configurar a expressão CRON para o intervalo de conexão do Agente ESET Management?

P_REPLICATION_INTERVAL aceita uma expressão CRON.

O padrão é "R R/20 * * * ? *" que significa conectar em um segundo aleatório (R = 0-60) a cada 20 minutos aleatórios (por exemplo, 3, 23, 43 ou 17, 37, 57). Valores aleatórios devem ser usados para o equilíbrio de carga com o tempo. Assim, todos os agentes ESET Management estão se conectando em um tempo aleatório diferente. Se um CRON preciso for usado, por exemplo "0 * * * *? *", todos os agentes com esta configuração vão se conectar ao mesmo tempo (a cada minuto no segundo :00) haverá picos de carga no servidor neste momento. Para mais informações, consulte Intervalo de expressão CRON.

Como posso criar um novo grupo dinâmico para implantação automática?

Consulte nosso artigo da Base de conhecimento para instruções passo a passo.

Ao importar um arquivo contendo uma lista de computadores a adicionar ao ESET PROTECT, qual é o formato requerido para o arquivo?

Arquivo com as linhas a seguir:

Tudo\Grupo1\GrupoN\Computador1
Tudo\Grupo1\GrupoM\ComputadorX

Tudo é o nome obrigatório do grupo de raiz.

Quais certificados de terceiros podem ser usados para assinar certificados ESET PROTECT?

O certificado deve ser um certificado CA (ou CA intermediário) com o sinalizador 'keyCertSign' da restrição 'keyUsage'. Isto significa que ele pode ser usado para assinar outros certificados.

Como faço para **redefinir a senha do administrador** para o console da Web (a senha inserida durante a configuração no sistema operacional Windows)?

É possível redefinir a senha executando o instalador do servidor e escolhendo **Reparar**. Note que você pode precisar da senha para o banco de dados ESET PROTECT se você não usou a autenticação do Windows durante a criação do banco de dados. Consulte o artigo da Base de conhecimento sobre esse tópico.

- Tenha cuidado, algumas das opções de reparo potencialmente causam a remoção de dados armazenados.
- A redefinição de senha desativa a 2FA.

Como faço para **redefinir a senha do administrador** para o console da Web (Linux, inserida durante a instalação)?

Se você tiver outro usuário no ESET PROTECT com direitos suficientes, você deve ser capaz de redefinir a senha da conta de administrador. Mas, se o administrador for a única conta (já que ele é criado no momento da instalação) no sistema, você não pode redefinir a senha. Consulte o artigo da Base de conhecimento sobre esse tópico.

Como solucionar problemas se o **Sensor RD** não está detectando nada?

Se seu sistema operacional for detectado como um dispositivo de rede, ele não será enviado para o ESET PROTECT como um computador. Dispositivos de rede (impressoras, roteadores) são filtrados. O Sensor RD foi compilado com o *libpcap version 1.3.0*, verifique se você possui essa versão instalada no seu sistema. O segundo requisito é uma rede em ponte da sua máquina virtual onde Sensor RD está instalado. Se estes requisitos forem cumpridos, execute nmap com detecção de sistema operacional (http://nmap.org/book/osdetect-usage.html) para ver se ele pode detectar o sistema operacional em seu computador.

Por que não consigo ver os itens na janela de Modelos de grupos dinâmicos?

Muito provavelmente seus usuários não têm permissões suficientes. Os usuários podem ver modelos apenas se eles estiverem contidos em um grupo estático onde o usuário recebeu a atribuição de pelo menos permissões de **Leitura** *** para Modelos de grupo dinâmico.

Por que não consigo ver nenhuma informação na janela do Painel?

Muito provavelmente seus usuários não têm permissões suficientes. Os usuários precisam de permissões sobre computadores e também que o Painel tenha os dados exibidos. Veja o exemplo de conjunto de permissões.

Como atualizar meu Produto de Segurança ESET?

Use a tarefa de Instalação de software e selecione o produto a atualizar.

Como posso alterar o sufixo no endereço do console web

Se o endereço do seu console web for, por exemplo, *10.1.0.5/era* e você quiser alterar o sufixo *era*, nunca renomeie a própria pasta. Não recomendamos alterar o endereço, mas se isso for necessário, crie um link na pasta *webapps* com um nome diferente.

Por exemplo, no Linux ou Máquina virtual você pode usar o comando a seguir:

```
ln -sf /var/lib/tomcat/webapps/era/ /var/lib/tomcat/webapps/esmc
```

Depois de executar o comando no terminal, seu Console web também pode ser acessado em 10.1.0.5/esmc (altere o endereço IP para seu próprio endereço).

Sobre o ESET PROTECT

Para abrir a janela **Sobre**, vá para **Ajuda** > **Sobre**. Esta janela fornece detalhes sobre a versão do ESET PROTECT. A janela superior contém informações sobre o número de dispositivos cliente conectando e o número de licenças ativas. Além disso, você verá a lista de módulos de programa instalados, seu sistema operacional e uma licença usada pelo ESET PROTECT para fazer download das atualizações de módulo (a mesma licença usada para ativar o ESET PROTECT). Informações sobre o banco de dados, como o nome, versão, tamanho, nome de host e usuário, são exibidos nessa janela.

Para obter instruções sobre como descobrir a qual versão do ESET PROTECT um componente pertence, consulte nosso artigo da Base de Conhecimento.

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