ESET PROTECT

Guia do Usuário

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

1 Introdução ao ESET PROTECT 1
1.1 Sobre a ajuda 3
1.1 Legenda de ícones 4
1.2 Novos recursos no ESET PROTECT 5
1.3 Notas de lançamento 6
1.4 Navegadores da Web, produtos de segurança ESET e idiomas compatíveis 30
1.5 Sistemas operacionais compatíveis 32
1.6 Pré-requisitos de rede 33
1.7 Disponibilidade do serviço 34
1.8 Diferenças entre o console de gerenciamento local e na nuvem 35
2 Introdução ao ESET PROTECT 36
2.1 Criar uma nova instância ESET PROTECT usando o ESET Business Account 37
2.2 Criar um novo usuário ESET PROTECT no ESET Business Account 40
2.3 Console da Web ESET PROTECT 43
2.3 Tela de login 47
2.3 Tour ESET PROTECT 48
2.3 Configurar proteção 49
2.3 Configurações do usuário 52
2.3 Filtros e personalização de layout 54
2.3 Marcações 57
2.3 Importar CSV 60
2.3 Solução de problemas - Console da Web 61
2.3 Recursos de visualização 63
2.4 Sincronizar o ESET PROTECT com o Active Directory 63
2.5 Como gerenciar produtos Endpoint a partir do ESET PROTECT 67
2.6 Serviço de notificação por push da ESET 69
3 VDI, clonagem e detecção de hardware 70
3.1 Resolver questões de clonagem 74
3.2 Identificação de hardware 76
3.3 Mestre para clonagem 77
4 ESET BridgeProxy HTTP - 79
5 ESET Management Implantação do agente 79
5.1 Adicionar computadores usando o RD sensor 80
5.1 Instalação do Sensor RD 81
5.1 Configurações de política do ESET Rogue Detection Sensor 83
5.2 Implantação local 84
5.2 Criar instalador do Agente e produto de segurança ESET 84
5.2 Live Installer comportamento 89
5.2 Criar instalador de script do Agente 90
5.2 Implantação do Agente – Linux 91
5.2 Implantação do agente – macOS 93
5.3 Implantação remota 94
5.3 Implantação do agente usando GPO ou SCCM 95
5.3 Etapas de implementação - SCCM 96
5.3 ESET Remote Deployment Tool 113
5.3 Pré-requisitos da ferramenta de instalação remota ESET 114
5.3 Selecione computadores a partir do Active Directory 114
5.3 Rastrear a rede local para computadores 117
5.3 Importar uma lista de computadores 119
5.3 Adicionar computadores manualmente 121

5.3 ESET Remote Deployment Tool – solução de problemas ... 123
5.4 Proteção do agente ... 123
5.5 Configurações do Agente ESET Management ... 124
5.5 Criar uma política para ativar a proteção de senha do Agente ESET Management ... 125
5.6 Solução de problemas - conexão de Agente ... 127
6 ESET PROTECT Menu principal ... 128
6.1 Painel ... 129
6.1 Detalhamento ... 135
6.2 Clientes gerenciados ... 137
6.3 Computadores ... 137
6.3 Detalhes do computador ... 140
6.3 Visualização do computador ... 146
6.3 Remover computador do gerenciamento ... 147
6.3 Tráfego alto incomum de computadores gerenciados ... 149
6.3 Grupos ... 149
6.3 Ações do grupo ... 150
6.3 Detalhes do grupo ... 150
6.3 Grupos estáticos ... 151
6.3 Crie um Novo grupo estático ... 152
6.3 Exportar grupos estáticos ... 154
6.3 Importar grupos estáticos ... 155
6.3 Árvore do grupo estático para ESET Business Account / ESET MSP Administrator ... 157
6.3 Grupos dinâmicos ... 159
6.3 Criar novo Grupo dinâmico ... 159
6.3 Mover grupo estático ou dinâmico ... 161
6.3 Atribuir Tarefa do cliente a um Grupo ... 163
6.3 Atribuir política a um grupo ... 164
6.4 Detecções ... 165
6.4 Gerenciar detecções ... 168
6.4 Visualização de detecção ... 169
6.4 Criar exclusão ... 170
6.4 Produtos de segurança ESET compatíveis com exclusões ... 173
6.4 Escudo contra ransomware ... 173
6.4 ESET Inspect ... 174
6.5 Vulnerabilidades ... 175
6.5 Aplicativos cobertos por Vulnerabilidades ... 179
6.6 Gerenciamento de patch ... 179
6.6 Aplicativos cobertos pelo Gerenciamento de patch ... 183
6.7 Relatórios ... 183
6.7 Criar um novo modelo de relatório ... 185
6.7 Gerar relatório ... 189
6.7 Agendar um relatório ... 190
6.7 ESET MDR ... 191
6.7 Arquivo de Relatórios MDR ... 193
6.7 Aplicativos desatualizados ... 195
6.7 Exibidor de Relatório SysInspector ... 195
6.7 Inventário de hardware ... 197
6.7 Relatório de auditoria. ... 199
6.8 Tarefas ... 199
6.8 Visão geral de tarefas ... 202
6.8 Indicador de progresso ... 203

6.8 Ícone de status ... 204
6.8 Detalhes da tarefa ... 204
6.8 Tarefas de cliente ... 207
6.8 Acionadores de tarefa do cliente ... 209
6.8 Atribuir Tarefa do cliente a um Grupo ou Computador(es) ... 210
6.8 Ações Antifurto ... 212
6.8 Verificar se há atualização do produto ... 214
6.8 Diagnóstico ... 215
6.8 Exibição de mensagem ... 217
6.8 Parar com o isolamento do computador ... 218
6.8 Exportar configuração de produtos gerenciados ... 219
6.8 Isolar computador da rede ... 220
6.8 Sair ... 221
6.8 Atualização de módulos ... 222
6.8 Reversão de atualização dos módulos ... 224
6.8 Rastreamento sob demanda ... 225
6.8 Atualização de sistema operacional ... 227
6.8 Gerenciamento de quarentena ... 229
6.8 Ativação do produto ... 231
6.8 Redefinir agente clonado ... 232
6.8 Redefinição de banco de dados do Rogue Detection Sensor ... 233
6.8 Executar comando ... 234
6.8 Executar script do SysInspector ... 236
6.8 Enviar arquivo para ESET LiveGuard ... 237
6.8 Escaneamento de servidor ... 237
6.8 Desligar computador ... 238
6.8 Instalação de software ... 239
6.8 Software Safetica ... 243
6.8 Desinstalação de software ... 244
6.8 Interromper gerenciamento (desinstalar agente ESET Management) ... 246
6.8 Solicitação de relatório do SysInspector (apenas Windows) ... 247
6.8 Atualizar Agente ... 248
6.8 Carregar arquivo em quarentena ... 250
6.8 Tarefas do servidor ... 251
6.8 Excluir computadores não conectando ... 253
6.8 Gerar relatório ... 254
6.8 Renomear computadores ... 256
6.8 Tipos de acionadores de tarefas ... 257
6.8 Intervalo de Expressão CRON ... 259
6.8 Configurações avançadas - Alternância ... 261
6.8 Exemplos de alternância ... 265
6.9 Instaladores ... 267
6.10 Políticas ... 270
6.10 Assistente de Políticas ... 272
6.10 Sinalizadores ... 274
6.10 Gerenciar políticas ... 276
6.10 Como as Políticas são aplicadas aos clientes ... 276
6.10 Ordenação de Grupos ... 277
6.10 Enumeração de Políticas ... 278
6.10 Mesclagem de Políticas ... 279
6.10 Exemplo de cenário da mesclagem de políticas ... 280

6.10 Configuração de um produto de ESET PROTECT 284
6.10 Atribuir uma política a um grupo 285
6.10 Atribuir uma política a um Cliente 286
6.10 Como usar o modo de Substituição 288
6.11 Notificações 290
6.11 Gerenciar notificações 291
6.11 Eventos em computadores ou grupos gerenciados 293
6.11 Alterações de status do servidor 294
6.11 Alterações no grupo dinâmico 295
6.11 Distribuição 295
6.12 Visão geral do status 297
6.13 Soluções ESET 299
6.13 Ativar o ESET LiveGuard Advanced 300
6.13 Ativar o ESET Full Disk Encryption 302
6.14 Mais 304
6.14 Arquivos enviados 304
6.14 Exclusões 306
6.14 Quarentena 308
6.14 Usuários do computador 309
6.14 Adicionar novos usuários 310
6.14 Editar usuários 312
6.14 Criar novo grupo de usuário 315
6.14 Modelos de grupo dinâmico 316
6.14 Novo modelo de grupo dinâmico 317
6.14 Regras para um modelo de grupo dinâmico 318
6.14 Operações 319
6.14 Regras e conectivos lógicos 319
6.14 Avaliação de Permissões de Modelo 321
6.14 Modelo de grupo dinâmico - exemplos 324
6.14 Grupo dinâmico - um produto de segurança está instalado 324
6.14 Grupo dinâmico - uma versão de software específica está instalada 325
6.14 Grupo dinâmico - uma versão específica de um software não está instalada 326
6.14 Grupo dinâmico - uma versão específica de um software não está instalada, mas existe outra versão 327
6.14 Grupo dinâmico - um computador está em uma subrede específica 328
6.14 Grupo dinâmico - versão instalada mas não ativada do produto de segurança do servidor 329
6.14 Como automatizar ESET PROTECT 329
6.14 Gerenciamento de licenças 331
6.14 Licenças elegíveis para a nuvem 335
6.14 Direitos de acesso 335
6.14 Usuários 336
6.14 Ações do usuário e detalhes do usuário 339
6.14 Usuários mapeados 340
6.14 Atribuir um conjunto de permissões a um usuário 343
6.14 Definições de permissão 345
6.14 Gerenciar definições de permissão 347
6.14 Lista de permissões 349
6.14 Relatório de auditoria 353
6.14 Configurações 355
6.14 Exportar relatórios para Syslog 357
6.14 Servidor Syslog 357
6.14 Restrições de segurança e limites Syslog 358

6.14 Eventos exportados para o formato JSON 359
6.14 Eventos exportados para o formato LEEF 367
6.14 Eventos exportados para o formato CEF 368
7 ESET PROTECT para Provedores de serviço gerenciados 376
7.1 Recursos do ESET PROTECT para usuários MSP 377
7.2 Criar um novo usuário ESET PROTECT no ESET MSP Administrator 379
7.3 Processo de implantação para MSP 381
7.3 Implantação local do Agente 382
7.3 Implantação remota do Agente 382
7.4 Licenças MSP 383
7.5 Iniciar configuração do cliente MSP 384
7.6 Ignorar configuração do cliente MSP 389
7.7 Criar instalador personalizado 389
7.8 Usuários MSP 391
7.9 Marcação de objetos MSP 393
7.10 Visão geral do status MSP 394
8 Gestão de dispositivo móvel de nuvem 395
8.1 Inscrição – adicionar dispositivos móveis 396
8.1 Inscrição do dispositivo Android 400
8.1 Inscrição do Android – proprietário do dispositivo 411
8.1 Inscrição do dispositivo iOS 417
8.1 Inscrição do Microsoft Entra ID (Android ou iOS) 426
8.1 Sincronização do Microsoft Intune (Android) 428
8.1 Sincronização do VMware Workspace ONE (Android) 430
8.1 Sincronização de Apple Business Manager (ABM) (iOS) 434
8.2 Gerenciar dispositivos móveis 438
8.2 Controle de web para Android 439
8.2 Gerenciamento de atualização do sistema operacional 440
8.2 Criar uma política para iOS - Conta Exchange ActiveSync 441
8.2 Criar uma política para aplicar restrições no iOS e adicionar conexão de Wi-Fi 446
8.2 Perfis de configuração Cloud MDM 450
8.3 Migração para o Cloud MDM (do ESET PROTECT On-prem) 451
9 ESET PROTECT Cenários de migração 452
9.1 Migração parcial do ESET PROTECT on-prem para ESET PROTECT 454
9.2 Migração dentro da nuvem—de ESET PROTECT para outro ESET PROTECT 468
10 Como remover o ESET PROTECT da sua rede 472
10.1 Expiração da última licença ESET PROTECT 474
11 Atualizações automáticas 475
11.1 Atualização automática do Agente ESET Management 476
11.2 Atualização automática de produtos de segurança ESET 476
11.2 Configurar atualizações de produto automáticas 479
12 Sobre o ESET PROTECT 480
13 ESET Connect (API) 480
14 Perguntas frequentes do gerenciamento de patch e de vulnerabilidade 481
15 Segurança para ESET PROTECT 483
16 Termos de uso 488
16.1 Acordo de licença para o usuário final do Agente ESET Management 492
16.2 Contrato de processamento de dados 499
16.3 Cláusulas contratuais padrão 501
17 Política de Privacidade 525

Introdução ao ESET PROTECT

Bem-vindo ao ESET PROTECT. O ESET PROTECT permite que você gerencie produtos ESET em estações de trabalho e servidores em um ambiente em rede com até 50.000 dispositivos 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 ameaças 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.

Para começar a usar o ESET PROTECT, veja a Introdução ao ESET PROTECT.

As seguintes soluções de segurança empresarial ESET foram renomeadas:

Nome antigo:	Novo nome:	Renomeado na versão:
ESET PROTECT	ESET PROTECT On-Prem	11.0
ESET PROTECT Cloud	ESET PROTECT	5.0
ESET Inspect	ESET Inspect On-Prem	2.0
ESET Inspect Cloud	ESET Inspect	

O ESET PROTECT é composto dos seguintes componentes:

ESET PROTECT como um serviço

Console da Web ESET PROTECT

- O Console web interpreta os dados armazenados no banco de dados ESET PROTECT. Ele visualiza as grandes quantidades de dados em painéis e relatórios claros, e também aplica políticas e executa tarefas em agentes e outros aplicativos da ESET.

Live Installer

- É um pequeno aplicativo composto pelo Agente ESET Management e uma opção para conter um produto empresarial endpoint em um pacote aprimorado e fácil de usar.

- O Agente ESET Management é um aplicativo pequeno sem interface do usuário gráfica que executa os comandos de ESET PROTECT em clientes conectados. Ele executa as tarefas, coleta relatórios de aplicativos ESET, interpreta e aplica políticas e executa outras tarefas válidas, como instalação de software e monitoramento geral de computadores.

- É um pacote pré-configurado e fácil de fazer download, contendo um agente e produto de segurança, na forma de um instalador aprimorado que vai conectar automaticamente à instância da nuvem adequada e ativar a si mesmo com uma licença válida com necessidade mínima de interação com o usuário. O instalador vai identificar a plataforma correta e fazer download do pacote do produto de segurança adequado.

- O agente é um aplicativo leve que facilita a comunicação entre o produto de segurança ESET em um computador do cliente e o ESET PROTECT.

Produtos de Segurança ESET

- Os produtos de segurança ESET protegem os computadores e servidores do cliente contra ameaças.
- ESET PROTECT é compatível com os seguintes produtos de segurança ESET.

ESET Business Account

- Ponto de entrada central para clientes empresariais, ou um fornecedor de identidade para o ESET PROTECT.
- Serve como um login único para clientes empresariais poderem ver suas licenças, ativarem serviços, realizarem o gerenciamento de usuários, etc.
- Uma ESET business account é necessária para ativar a instância ESET PROTECT.
- Consulte a Ajuda on-line ESET Business Account para mais informações.

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.

ESET Remote Deployment Tool

- Uma ferramenta que pode instalar o Live Installer remotamente na rede.
- Tem a capacidade de mapear remotamente a rede e sincronizar com AD, ou suportar os destinos de importação nos quais o produto será instalado.

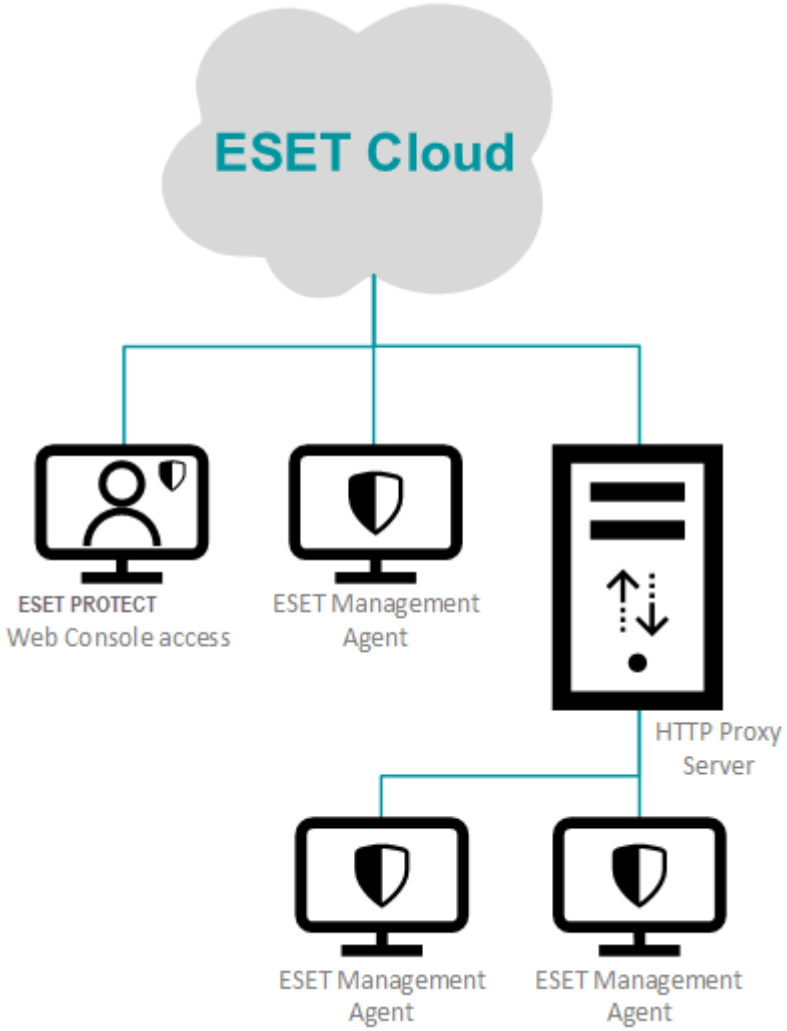
ESET Bridge (Proxy HTTP) –Você pode usar o ESET Bridge com o ESET PROTECT como um serviço de Proxy para:

- 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.

Escaneador do Active Directory ESET – sincroniza computadores e usuários do Active Directory com o Web Console ESET PROTECT.

O ESET Cloud Mobile Device Management (Cloud MDM) – fornece gerenciamento de dispositivo móvel Android e iOS e administração de segurança móvel.

O diagrama abaixo mostra a arquitetura ESET PROTECT simplificada:



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.
- Os tópicos neste guia são divididos em vários capítulos e subcapítulos. Você pode encontrar informações relevantes usando o campo Pesquisar no topo.
- 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 – inscreva novamente 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.

Ícone de status	Descrições
	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 chamada para acordar - O Servidor ESET PROTECT 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 Servidor ESET PROTECT. Por exemplo, quando quiser que uma Tarefa de cliente seja executada imediatamente em clientes ou se quiser que uma Política seja aplicada já.
	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 Relatórios/Políticas que deseja importar.
	Exportar – selecione Relatórios/Políticas 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
	Servidor de gateway
	Servidor de colaboração
	Agente ESET Management
	Conector de dispositivo móvel
	Sensor Rogue Detection
	ESET Bridge
	Tipo de detecção de **antivírus**. Veja todos os tipos de detecção em Detecções. Clique em um computador e selecione **Soluções** > **Ativar produto de segurança** para ativar 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.
	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.
	Vulnerabilidades
	Gerenciamento de patch

Novos recursos no ESET PROTECT

Painel MDR e relatório semanal

Para nossos clientes que usam o serviço ESET MDR, estamos felizes em apresentar o novo painel do MDR. Este painel reúne e exibe todos os dados importantes em tempo real relacionados ao monitoramento e caça a ameaças 24 horas por dia, 7 dias por semana. Além disso, você receberá relatórios semanais regulares com os instantâneos de dados mais recentes diretamente em sua caixa de entrada. Esses relatórios também podem ser acessados na seção Relatórios e são arquivados automaticamente para sua conveniência. Saiba mais

Inscrição de dispositivos móveis com Microsoft Entra ID

Adicionamos a opção de registrar dispositivos móveis no ESET PROTECT por meio do Microsoft Entra ID. Graças a esse método de inscrição simplificada, não é mais necessário gerar códigos exclusivos por dispositivo. Agora, você pode facilmente inscrever todos os dispositivos móveis usando um único link ou código QR, facilmente distribuído por e-mail ou através de seu canal preferido. Saiba mais

Outras melhorias e correções de bugs

Descubra o que mais foi melhorado no registro de mudanças.

Notas de lançamento

Notas de lançamento estão disponíveis apenas em inglês.

ESET PROTECT 5.2

Release date: April, 2024

- ADDED: MDR dashboard that displays real-time data for customers with the ESET MDR service
- ADDED: Weekly MDR report email sent automatically to customers with the ESET MDR service
- ADDED: Archive of MDR reports for customers with the ESET MDR service
- ADDED: Ability to enroll all mobile devices with one enrollment link or QR code via Microsoft Entra ID enrollment
- IMPROVED: Post-installation restart is not required for Linux products (ESET Endpoint Antivirus for Linux and ESET Server Security for Linux)
- IMPROVED: Using Google Play version of ESET Endpoint Security for Android instead of a web version when enrolling a mobile device in Device Owner mode
- FIXED: Error message displayed when opening the details or editing a server task with a trigger other than "Generate report"
- FIXED: Incorrect headline displayed in the webhook notifications sent to Microsoft Teams
- FIXED: Displaying "Product not installed" alert for "Common features" policies in some instances
- FIXED: No information about the mobile network is displayed when the device has multiple SIMs/eSIMs
- Other minor improvements and bug fixes

ESET PROTECT 5.1

Release date: February, 2024

- ADDED: Vulnerability & Patch Management for Windows servers (requires ESET Server Security for Microsoft Windows Server version 11.0 and later)
- ADDED: Enhanced ESET LiveGuard behavioral reports with detailed behavior of the sample (available for customers with ESET Inspect)
- IMPROVED: Migration of static group hierarchies from on-premises to cloud in large and MSP environments
- IMPROVED: Ability to send "ESET Inspect incidents" notification for all incident authors

- IMPROVED: Clarified wording related to Vulnerability & Patch Management
- FIXED: Incorrect installation date reported for Linux product
- FIXED: Table scrolling does not work after opening Details
- FIXED: Incorrect display of license time remaining before expiration next to the license end date in Computer Details
- Other minor improvements and bug fixes

ESET PROTECT 5.0

Release date: December, 2023

- ADDED: Name change for ESET PROTECT Cloud to ESET PROTECT
- ADDED: Enable automatic operating system updates (part of Vulnerability & Patch Management)
- ADDED: New preset policy with automatic operating system updates (part of Vulnerability & Patch Management)
- ADDED: Ability to download ESET LiveGuard behavioral reports
- ADDED: Option to send a notification to non-activated devices enrolled via Workspace ONE or Microsoft Intune (MDM)
- IMPROVED: Patch management restarts added to the Automatic problem resolving setting
- IMPROVED: Users with access to server settings can delegate access rights to other users for viewing and modifying the server settings
- IMPROVED: Devices API contains information about the BIOS serial number
- IMPROVED: New version of AV Remover in the Management Agent
- FIXED: Incorrect Dynamic Groups evaluation behavior on Agent startup
- FIXED: Devices API does not report installed security products
- REMOVED: Support for macOS Sierra (10.12), High Sierra (10.13) and Mojave (10.14)
- REMOVED: Support for Windows 7, 8 and 8.1
- Other minor improvements and bug fixes

ESET PROTECT Cloud 4.7

Release date: October, 2023

- ADDED: New REST API for ESET PROTECT Cloud
- IMPROVED: New information for MSP administrators about the MSP managing company in the All-in-one

installer

- FIXED: Agents lost connection after migration, followed by an upgrade
- FIXED: Agent service fails to stop in time, or system restart takes longer than expected in specific cases
- FIXED: Agent for macOS is not correctly reporting the system build number in specific cases
- Other minor improvements and bug fixes

ESET PROTECT Cloud 4.6

Release date: August, 2023

- ADDED: Setting time slots in Dynamic groups
- ADDED: Enrolling Android mobile devices from Workspace ONE
- IMPROVED: Added new setting in the ESET LiveGuard Basic built-in policy regarding the automatic document submissions (set to OFF by default)
- IMPROVED: Visual enhancements in the patches list in Patch Management
- IMPROVED: Added language settings for the mobile device enrollment email
- Other minor improvements and bug fixes

ESET PROTECT Cloud 4.5

Release date: July, 2023

- ADDED: ESET Vulnerability & Patch Management - a new protection layer monitoring vulnerabilities with the ability to patch all endpoints managed through our platform (requires ESET Endpoint Antivirus/Security for Windows version 10.1 and later)
- ADDED: New setting in "Set up your protection" wizard regarding ESET LiveGuard for new and existing customers
- ADDED: New Client task - Check for product update (requires ESET Endpoint Antivirus/Security for Windows version 10.1 and above)
- ADDED: The ability to test send email and webhook notifications
- ADDED: Webhook authentication to verify the credibility of the webhook notification
- IMPROVED: New version of the Log Collector in the Management Agent
- FIXED: Negative filter applied to the list of computers still visible after clearing the filters
- Other minor improvements and bug fixes

ESET PROTECT Cloud 4.4

Release date: June, 2023

- ADDED: New dashboard for customers using ESET Cloud Office Security
- ADDED: Data filter per customer for MSP administrators in the Dashboard section
- ADDED: New section for MSP administrators, "Managed Customers", offering an overview of all managed customers
- ADDED: Ability for MSP administrators to filter report templates per customer when creating scheduled reports
- ADDED: New delivery method for notifications - webhooks
- ADDED: New branding visuals within the console
- IMPROVED: Easier search within the console with no need to first choose a category
- IMPROVED: Ability to filter policies by name
- IMPROVED: Information about the creation and download of installers added to the Audit Log
- IMPROVED: MSP customers ready for a set up distinguished by an icon
- IMPROVED: Asynchronous sending of enrollment emails during the mobile device enrollment
- IMPROVED: Wi-fi settings available via QR code during Device owner enrollment (MDM)
- IMPROVED: New version of the AV Remover and Log Collector in the Management Agent
- CHANGED: The "Auto-updates" policy will become a part of the "Common features" policy when the new Configuration module is released (planned for July)
- FIXED: Creating a dynamic group template based on a value "LiveGuard is not working due to a license problem" not functioning properly
- FIXED: Dynamic group template based on a value "macOS is preventing the ESET security product from accessing some folders" not working properly
- Other minor improvements and bug fixes

ESET PROTECT Cloud 4.3

Release date: April, 2023

- ADDED: An MDR Report Template for offices and partners delivering ESET Services
- ADDED: A column for mobile device IMEIs in the device list and the possibility to filter the devices by IMEI
- ADDED: The ability to combine Computer name, Database version and Last connection in one report

- IMPROVED: Extended certificate validity for mobile devices - devices do not need to connect to an MDM server frequently to stay protected
- FIXED: Issues with displaying the Product Tour in the Safari browser
- FIXED: Various localization bugs
- Other minor improvements and bug fixes

ESET PROTECT Cloud 4.2

Release date: February, 2023

- ADDED: Detections are grouped by common attributes
- ADDED: Migration of mobile devices to cloud MDM
- ADDED: Syslog includes the operating system of a computer, and the full hierarchy and description of a static group
- ADDED: Product Navigator has a link to ESET Cloud Office Security (available later in April 2023)
- IMPROVED: Active Directory Synchronization (time of last sync, ability to deactivate and regenerate token)
- FIXED: Incorrect filter behavior when multiple license statuses are selected
- Various other minor improvements and bug fixes

ESET PROTECT Cloud 4.1

Release date: January, 2023

- ADDED: Enrollment support for Android mobile devices via Microsoft Intune Management Console
- ADDED: Column "Investigated by ESET" in incident overview in the ESET Inspect dashboard
- ADDED: Ability to add column FQDN and Serial Number in the Computers section
- IMPROVED: Size values in Submitted Files
- FIXED: Inability to resolve/unresolve detections when the parent group is selected in the tree
- FIXED: Incorrect encryption process (EFDE) status in the ESET Solutions section
- FIXED: Wrong ESET LiveGuard license was shown while editing the existing software install task
- Various other minor improvements and bug fixes

ESET PROTECT Cloud 4.0

Release date: November, 2022

- ADDED: Basic incident overview in the ESET Inspect dashboard

- ADDED: CEF format for Syslog
- ADDED: Reporting of absolute and relative free space for hard drives in HW inventory
- ADDED: Log out action in the Computer context menu (under Power)
- ADDED: Log out Client Task
- ADDED: Ability to filter Computers by FQDN
- ADDED: Ability to filter Computers by Serial Number
- ADDED: Last boot time in computer details
- ADDED: Ability to deploy LiveGuard on all devices in a static group via context menu action
- ADDED: Ability to reset default filters
- ADDED: Static Group name in Syslog events
- ADDED: Ability to see the progress of removing client tasks
- ADDED: Ability to filter unassigned policies in the Policies section
- ADDED: Ability to sort policies in the "Last Modified By" column
- ADDED: Support for time-elapsed (duration) filters in Dynamic Groups
- ADDED: Comma separator for thousands place in table numbers
- IMPROVED: Table numbers are now aligned right
- IMPROVED: Selecting a product from the repository in the Software Install task
- IMPROVED: "Deploy ESET LiveGuard" through the computer's or group's context menu now leverages a better mechanism that is used in the dedicated ESET Solutions section
- IMPROVED: Filtering by Detection Type
- IMPROVED: New version of Log Collector (version 4.6.0.0) in Management Agent
- IMPROVED: Solutions deployment supports computers in site/company location based on hierarchy
- IMPROVED: Example section in the "Select time interval" filter
- CHANGED: Limit from 100 to 1000 when opening selected objects
- CHANGED: Disabled optional use OPAL in built-in encryption policy "Encrypt all disks - Recommended"
- FIXED: The license list occasionally disappears when scrolling through a long License Management list
- FIXED: The date/time filter does not work correctly on the localized web console
- FIXED: All policies are hidden except auto-update when logging in to the console for the first time

- FIXED: Info message about default value for time-based criteria in Notifications is shown when it is not mandatory
- FIXED: Network adapter(s) screen informs that the latest version of an agent is required, even though the latest version is installed
- FIXED: Default presets for Computers/Detections sections are overwritten in a special scenario
- FIXED: Inaccurate problem count in License Management badge in specific scenarios
- FIXED: Missing limit for quarantine management actions, which causes an error message in some cases
- FIXED: HW inventory reports the TPM manufacturer version instead of the specification version
- Various other minor improvements and bug fixes

ESET PROTECT Cloud 3.5

Release date: September, 2022

- ADDED: Initial configuration (Set up protection)
- ADDED: Dark theme
- ADDED: Ability to switch between Absolute and Relative time in tables
- ADDED: Ability to add column Hash in Detections section
- ADDED: Ability to search by Hash in the Detections section
- ADDED: Ability to search by Object in the Detections section
- ADDED: Ability to distinguish, whether BitLocker is activated on a particular machine
- ADDED: Filtering options in Computer details - Installed Applications screen
- ADDED: Computer preview - the ability to reset displayed sections into default
- ADDED: Ability to modify Computer name and Description directly from the Computer preview panel
- ADDED: Ability to mute/unmute Computer directly from the Computer preview panel
- ADDED: Section name as a prefix in the browser tab title
- IMPROVED: VDI support (mostly improvements around instant clones)
- IMPROVED: Network Adapters (part of Computer details - Details - Hardware) are more readable in the case of IPv4/IPv6
- IMPROVED: Multiplatform support when deploying or enabling features via Solutions in the Computer context menu
- IMPROVED: Displaying of Inspect button is now dependent on the permission set "Access to ESET Inspect"

- IMPROVED: Filter Advisor remembers item sorting
- IMPROVED: Information in the Detection type column was split into two separate columns Detection Category and Type
- IMPROVED: Creation of New Report Template for newly created Report category
- FIXED: Save filter set is not working correctly in all sections
- FIXED: Specific scenario causes license sync breakage (if static group below company has the same name as a site that is going to be created in EBA)
- FIXED: When you load a saved filter set, it is not applied unless you edit it (various sections)
- FIXED: Filter "≤ # OF ALERTS" is not working correctly (Computers section)
- Various other minor improvements and bug fixes

ESET PROTECT Cloud 3.4

Release date: June, 2022

- ADDED: Advanced Filters in the Computers section
- ADDED: Native ARM64 support for ESET Management Agent for macOS
- ADDED: "Waiting" state in the Component version status section on Status Overview for better communication of auto-updates (available from ESET Endpoint Antivirus/Security for Windows version 9.1)
- ADDED: Site structure from ESET Business Account synchronizes in the static group tree
- ADDED: New rebooting option-administrator can set up reboots in a way that the end-users can postpone them (available from ESET Endpoint Antivirus/Security for Windows version 9.1)
- ADDED: Information on how many more devices can enable ESET LiveGuard on the ESET LiveGuard Dashboard
- ADDED: Dark Theme preview feature
- ADDED: Limited-input device-simple enrollment flow for Android-based devices that do not have access to emails or a camera for scanning QR codes
- ADDED: Support for deployment of the latest version in the software installation task (the latest version at the moment of task execution, it is not necessary to select a specific version anymore)
- ADDED: Creation date column in the Installers section
- ADDED: Reset functionality for columns in tables
- ADDED: Warning to Audit log access right
- ADDED: "Installation Date" column in Computer details - Installed Applications screen
- ADDED: Ability to select multiple monitored static groups in a single notification

- ADDED: Reporting human-readable Windows operating system version is displayed in the OS Service Pack column in the Computers section
- ADDED: OS build version collected from macOS is displayed in the OS Service Pack column in the Computers section
- ADDED: Agents tile in the Status Overview section for better identification of unmanaged computers
- ADDED: Instance ID is available in the console's About section (previously only available in ESET Business Account)
- ADDED: Console users can deploy ESET Full Disk Encryption (EFDE) on recommended (portable) devices in the ESET Solutions screen
- IMPROVED: EFDE does not deploy to devices using BitLocker for drive encryption
- IMPROVED: Reboot and shut down experience on macOS (user is notified about restart and can cancel it in 60 seconds)
- IMPROVED: Tasks planned ASAP are executed in the order in which they were created in the console
- IMPROVED: Admin password is not required when enrolling a new mobile device. However, ESET strongly recommends you use an admin password for the full functionality of certain features
- IMPROVED: Every ASAP trigger created by the user in the console must have an expiration set (less than six months)
- IMPROVED: HIPS detections now contain user and hash
- IMPROVED: New version of AVRemover and Log Collector in the Management Agent
- FIXED: Several functionality problems with the dynamic group template selector
- FIXED: Scheduled client tasks without "Invoke ASAP If Event Missed" pre-selected could be executed with the wrong timing if the computer woke up from sleep or hibernation
- FIXED: Tags assigned to a "Client Task" are automatically assigned to applicable computers
- FIXED: Unavailable EDR element in the Component version status section on the Status Overview screen
- Various other minor improvements and bug fixes

ESET PROTECT Cloud 3.3

Release date: April, 2022

- ADDED: Manage up to 50,000 devices (according to purchased license)
- ADDED: Support for ESET Inspect Cloud (EDR solution)
- ADDED: Easy trial, deployment and purchase of ESET Full Disk Encryption (EFDE)
- ADDED: Preview feature - Advanced Filters in the Computers section

- ADDED: New buttons under the table in the Computers section and Detection section
- ADDED: Right-click tables to open the context menu
- ADDED: Enrollment link expiration and device certificate renewal information to the enrollment email
- ADDED: Built-in policies for V7 product for macOS and HTTP proxy
- ADDED: Ability to turn on the "Remote Host" column in the Computers section
- ADDED: Console users can configure (in Settings) the behavior of newly enrolled devices deduplication in the console
- ADDED: Console users receive an email notification that contains a link that redirects the user into the Computer details section in the console
- IMPROVED: Console users receive a notification about multiple detections occurring on managed computers aggregated in one email message
- IMPROVED: Remove button was moved behind the gear icon in the ESET Solutions section
- IMPROVED: Console users can click the chart in the ESET Solutions section and will be redirected to the Computers section
- IMPROVED: The latest versions of each product are prioritized in the product selection section of the software installation task
- IMPROVED: UI elements in tables
- CHANGED: ESET Dynamic Threat Defense to ESET LiveGuard in management consoles
- CHANGED: Remove tags icon in the Tags panel
- FIXED: Trigger for scheduled Reports cannot be edited
- FIXED: Exclusions table shows the "Occurred" column, but it is labeled as "Created on"
- FIXED: "Export table as" now exports all data, not just data on the page
- FIXED: Trigger via CRON shows different time after opening details of a specific trigger
- REMOVED: "Auto-loading" option in the Clients and Detections screen paging menu
- Various other minor bug fixes, security and performance improvements

ESET PROTECT Cloud 3.2

Release date: February, 2022

- ADDED: Easier enrollment for mobile devices
- ADDED: Easier deployment mechanism also extended for MSPs
- ADDED: New product tour

- ADDED: ESET Product Navigator to the header
- ADDED: New context menu action "Deploy ESET security product" (in Computers section)
- ADDED: AD user sync tool for ESET PROTECT Cloud
- ADDED: AD user sync-based features enabled for iOS devices
- IMPROVED: Context menu in Computers section
- IMPROVED: Installer creation Wizard
- IMPROVED: Email enrollment progress bar to indicate whether the task has been finished
- IMPROVED: Computer with IP column was divided into two columns in Submitted Files
- IMPROVED: Retention policy dialog is more user-friendly and upper limits are communicated in the Online Help guide
- FIXED: Last scan time in computer details
- FIXED: When "Module update failed" occurs, the computer is not moved to the related Dynamic Group, if the Dynamic Group was created
- FIXED: Policies under "Manage policies" over a group do not display for users with an administrator permission set
- FIXED: "Restart required" and "Inbound Communication" columns in the Detections list display incorrect values

ESET PROTECT Cloud 3.1.5

Release date: January, 2022

- ADDED: Easier deployment - the new simplified dialog for installer download, and reworked wizard for creation of the customized installer
- ADDED: Dynamic groups for mobile devices
- ADDED: Easy trial, deploy and purchase of ESET Dynamic Threat Defense (EDTD) also for MSP customers
- ADDED: Hide and Show action for EDTD Dashboard
- ADDED: Possibility to add Group Name column in the Detections section (not displayed by default)
- CHANGED: Default message contents (Computer first connected, Computer identity recovered, Computer cloning question created)
- IMPROVED: EDTD status (enabled/disabled) is reported properly to the console (requires ESET Endpoint Antivirus/Security for Windows version 9.0 and above) and leveraged in various sections (for example, action Enable is not offered for endpoint where the feature is already enabled)
- IMPROVED: Computer description can be multiline

- IMPROVED: User can define more than one naming pattern for VDI master image
- IMPROVED: Hover effect (Inverted color) on the cell with Computer name (in Computers section) and on the cell with Detection type (in Detections section)
- IMPROVED: Computer name and IP is now in separate columns in the Detection section
- FIXED: Multiple sorting does not work as expected when the top priority is assigned to the Alerts column
- FIXED: The overall status of the license might not be shown correctly in specific cases
- FIXED: Various other bug fixes, security, and performance improvements

ESET PROTECT Cloud 3.0

Release date: October, 2021

- ADDED: Support for Automatic Product Updates (available from ESET Endpoint Antivirus/Security for Windows version 9.0)
- ADDED: Management for brute-force attack protection (available from ESET Endpoint Antivirus/Security for Windows version 9.0)
- ADDED: Easy trial, deploy and purchase of ESET Dynamic Threat Defense (EDTD)
- ADDED: Web control for Android devices
- ADDED: System updates management for Android
- ADDED: New column Logged users in Computers table
- ADDED: Windows OS build number is reported as a separate symbol (possibility to use it in Dynamic groups)
- ADDED: List of submitted files (EDTD) in Computer details, Detection and Quarantine section
- ADDED: New product categories in Component version status section on Status Overview
- ADDED: Full path to a computer in received notifications
- ADDED: Possibility disable the triggering of notifications for muted computers
- ADDED: Possibility to manage session protection (e.g., disable blocking requests from different IP addresses)
- CHANGED: Reducing and re-organizing columns in the Computers section
- IMPROVED: ESET Dynamic Threat Defense perception (added information of what was originally detected by EDTD)
- IMPROVED: Operating system update - allowing the user to postpone the required reboot
- IMPROVED: Operating system update task accessible not only from context menu over a group but also over a single device
- IMPROVED: Now is possible to visually distinguish locked policies in policies and computer details screens

(padlock icon)

- IMPROVED: When users create new permission sets, some checkboxes can grey out based on their permission (users can not give higher permission that they have)
- IMPROVED: Automatically selected newly created permission set when creating a new user
- IMPROVED: Basic support of installer file caching in script-based Agent Live Installers
- IMPROVED: Date and Time displayed in format according to language
- IMPROVED: Faster displaying of the planned flag on client tasks also after assigning to the significant amount of targets
- IMPROVED: The enrollment URL link is visible below the QR code, and the user can copy it in the enrollment wizard
- IMPROVED: New version of Log Collector in Management Agent
- FIXED: Idle session timeout was not matching settings in ESET Business Account
- FIXED: Triggers - infinite loading in some cases when the user changes trigger type
- FIXED: Unwanted machines moved during computers import
- FIXED: Missing notification about scheduled restart (macOS - osascript)
- FIXED: License is randomly changed when the software install task is edited
- FIXED: Notifications - Message preview is not displaying properly
- FIXED: macOS Big Sur, specific protections statuses are missing in dynamic groups and report templates
- FIXED: Users without access to an EDTD license cannot see the data on the EDTD Dashboard
- FIXED: Multiple sorting does not sort correctly
- FIXED: Performance issue when deleting a large number of exclusions
- FIXED: EDTD Deployment on Dynamic Group ends with error
- FIXED: Various other bug fixes, security, and performance improvements

ESET PROTECT Cloud 2.4

Release date: August, 2021

- ADDED: Ability to manage up to 25,000 devices (according to purchased license)
- ADDED: New ESET Dynamic Threat Defense dashboard
- ADDED: Preview feature - Easy trial, deploy and purchase of ESET Dynamic Threat Defense
- ADDED: Ability to create a new trigger in client task details

- ADDED: Indicator of last connection status of managed computer (connected in last replication interval)
- ADDED: Computer preview - by clicking on computer name will be displayed side panel with the most important computer details
- ADDED: Detections preview - by clicking on detection type will be displayed side panel with the most important detection details
- CHANGED: Existing ESET Dynamic Threat Defense dashboard name change
- CHANGED: Triggers for server tasks and client tasks with frequencies lower than 15 minutes will not be allowed
- CHANGED: More granular communication of managed applications versions
- CHANGED: Automatic application of retention policy after the grace period
- CHANGED: After de-enrollment, ABM devices no longer offer the re-enroll task option
- IMPROVED: A user or a computer can only be assigned to 200 users or computers in one operation to retain adequate service responsiveness
- FIXED: Actions in the context menu for devices were disabled incorrectly (Enable ESET Dynamic Threat Defense, Network Isolation)
- FIXED: Licenses without an expiration date (for example, subscription licenses) were counted as expired in the Status Overview
- FIXED: Automatic update of company name in the console when changed in ESET Business Account or ESET MSP Administrator
- FIXED: Discrepancy in "Total number of devices" on the Dashboard compared to the total count of devices shown in the Computers tab
- FIXED: FaceID screen is now correctly skipped during ABM enrollment when selected in the wizard as one of the items to be skipped
- FIXED: "Title" in the properties of the exported PDF report

ESET PROTECT Cloud 2.3

Release date: June, 2021

- ADDED: Management of Apple devices running iOS and iPadOS, including Apple Business Manager
- ADDED: Native ARM64 support for ESET Management Agent for Windows
- ADDED: Support for VMWare Instant Clones
- ADDED: New audit information on the policy screen (Modification time, Last modified by, and Creation time)
- ADDED: Upgrade outdated operating systems in a computer group
- ADDED: Ability to copy a license Public ID to the clipboard via the context menu in license management

- ADDED: Ability to filter licenses on the license management screen based on the Public ID
- ADDED: Automatic resolution of HIPS logs
- ADDED: Computer description as a new attribute in Device Identifiers under computer details
- ADDED: Support for migration and backup of ESET Full Disk Encryption (EFDE) recovery data
- ADDED: New client task "Generate new FDE Recovery password" (available from EFDE client version 1.3 (EFDE - purchased separately))
- ADDED: Ability to retry encryption from the console if encryption fails (available from EFDE client version 1.3 (EFDE - purchased separately))
- IMPROVED: Preview feature – Computer preview (added new sections and the possibility to click on some elements and navigate to relevant details)
- IMPROVED: The Syslog export now also supports the information log level
- IMPROVED: The ESET Full Disk Encryption status now provides more details
- IMPROVED: Extended Hardware inventory details for the device with encryption-related fields
- IMPROVED: Disabled computers are not synced or deleted by the Active Directory scanner
- IMPROVED: Various UI and UX improvements
- CHANGED: Retention policy enforcement notification
- CHANGED: The CRON trigger can be planned for LOCAL or UTC time only
- CHANGED: The Wipe task has been dropped because it does not work properly in newer versions of Android. The Factory Reset task remains the only task for both Apple and Android devices
- CHANGED: Adjustments related to managed products name changes
- FIXED: Mobile device management allows manual selection of a suitable platform in case of unrecognized mobile devices
- FIXED: The License Owner name is not updated in License Management after changing it in ESET Business Account
- FIXED: A Client task cannot be scheduled for managed computer local time (only for browser time)
- FIXED: Various other bug fixes, security, and performance improvements

ESET PROTECT Cloud 2.2

Release date: April, 2021

- NEW: New concept–Option to preview certain features
- NEW: Preview feature–Support for iOS / iPadOS (without ABM enrollment)

- NEW: Preview feature–Computer preview
- ADDED: Upgrade outdated products in a computer group
- ADDED: Default filter in the Detection screen (unresolved detections first)
- ADDED: Ability to use a second license to activate ESET Dynamic Threat Defense in a software installation task when an eligible endpoint product is selected
- ADDED: User management for users with global "write" access
- ADDED: Expiration time for client task triggers (Triggers tab)
- ADDED: New report–Computer Hardware Overview
- ADDED: Enabled non-root administration (other than the instance creator) to manage the security of other managed accounts (depends on the upcoming EBA release planned for April 2020)
- IMPROVED: Pause a task for ESET Full Disk Encryption (capability to select an exact date and time)
- IMPROVED: The encryption status tile is now more interactive
- IMPROVED: Extended information in detection details
- IMPROVED: A recommendation message is displayed when the Administrator tries to run a client task on more than 1,000 clients (using a group is recommended)
- IMPROVED: Assigning a policy to more than 200 individual devices is permitted (using a group is recommended)
- IMPROVED: Various performance improvements
- FIXED: Licenses with over 10,000 seats were displayed as infinite
- FIXED: In some cases, the "Planned" flag In a client task remained active after a task was executed
- FIXED: The license usage number did not display the correct number when a license was overused
- FIXED: Subunits were not used by percentage usage enumeration for mail security products
- FIXED: The operating system name (Big Sur) for macOS 11.1 and 11.2 was missing
- FIXED: Various other bug fixes and improvements

ESET PROTECT Cloud 2.1

Release date: February, 2021

- ADDED: Ability to look up specific computer based on the last logged user parameter
- ADDED: Support for policy-based migration from on-premises console to cloud console
- FIXED: Issue with opening/reading PDF reports sent by email (base64-encoded)

- FIXED: Non-root user with write permission rights for ESET PROTECT Cloud in ESET Business Account cannot import or create dynamic group templates
- FIXED: Device filters on Dashboards display different values than in tables
- FIXED: In some cases, Detail in the "Audit Log" overlapping other lines
- FIXED: Product deactivation fails with timeout (in certain cases) if started by "Delete not connected computers" server task
- FIXED: User cannot delete objects in some cases even with correct access rights
- FIXED: Name of the file is garbled when Japanese characters are used
- FIXED: Various other bug fixes and minor improvements

ESET PROTECT Cloud 2.0.148.0

Release date: December, 2020

- CHANGED: ESET Cloud Administrator renamed to ESET PROTECT Cloud
- ADDED: Ability to manage and protect Android mobile devices
- ADDED: Ability to manage FileVault (macOS) native encryption when an eligible license is present
- ADDED: Increased device management limit (up to 10,000 - dependent on purchased license size)
- ADDED: One-click deployment of ESET Dynamic Threat Defense if an eligible license is present
- ADDED: Ability to manage dynamic groups
- ADDED: Ability to manage notifications
- ADDED: Ability to define specific permission sets for selected users
- ADDED: Active Directory synchronization (Computers only)
- ADDED: Syslog log exporting
- ADDED: New “Audit log” section provides detailed information about specific actions
- ADDED: Ability to mass deploy the management agent to macOS devices
- ADDED: Second-level menu for advanced options
- ADDED: Secure Browser management
- ADDED: Support for sites (ESET Business Account) licenses including new "License user" column
- ADDED: Renew a license in the “License Management” screen
- ADDED: Ability to drill-down from expiring license issues in “Dashboards” and “Reports” to obtain more information in the “License Management” screen

- ADDED: New “Manage license” context menu
- ADDED: EULA update notifications that support auto-upgrade (uPCU) of endpoint products in managed environments
- ADDED: New ESET Full Disk Encryption (EFDE) management actions directly from “Computer details”
- ADDED: New EFDE Dynamic groups and Reports
- ADDED: Detection details (LiveGrid, Observed in organization, Virus Total)
- ADDED: One-click access to client task triggers
- ADDED: Unsupported browser warning
- ADDED: New "Seats allocated to sites" present in dedicated license report
- ADDED: Multi-line command scripts for Run Command task
- ADDED: Option to create a Computer user group in the “Add computer user” wizard
- CHANGED: Management Agent - supported operating systems
- CHANGED: Retention policy defaults
- CHANGED: License unit/sub-units visualization changed to "used/total" for online licenses and "X offline" for offline licenses
- CHANGED: Access to behavior reports (when EDTD is purchased and enabled) are available (in the UI) only if an eligible license is present
- IMPROVED: Ability to define a retention policy for certain logs
- IMPROVED: Exclusions mechanism extended to firewall threats
- IMPROVED: Computer details now directly accessible by clicking the computer name
- IMPROVED: One-click Network isolation
- IMPROVED: Columns ordering
- IMPROVED: Pop-up with search option
- IMPROVED: Hierarchical Dynamic groups tree
- IMPROVED: Multi-select in pop-up (modal) windows
- IMPROVED: Ability to create one exclusion from multiple detentions with standard exclusion criteria(s)
- IMPROVED: Breadcrumbs for better navigation in Wizards
- IMPROVED: Various other performance and security improvements
- FIXED: “Delete task action” removes all client tasks, not just selected items in a task list for a specific group

- FIXED: Status filter not visible for server tasks (only in client tasks)
- FIXED: Failed to send a wake-up call from the client task details executions
- FIXED: Incorrect target group type displays when editing a client trigger
- FIXED: “Status update” type notifications fail to save if they contain the “$” character
- FIXED: Import of policies with large file sizes
- FIXED: Infinite units or subunits in tooltips for licenses in the License Management screen display incorrectly
- FIXED: License-related notifications (for example, expiration/overuse) trigger when a license is suspended
- FIXED: Policy does not block the selected Scan profile
- FIXED: Filters previously set are not saved
- FIXED: Various other bug fixes

ESET Cloud Administrator 1.2.118.0

- Added: Support for ESET Dynamic Thread Defense (Sold separately. Available for purchase in upcoming weeks)
- Added: Submitted files screen
- ADDED: Ability to pause ESET Full Disk Encryption available from EFDE client version 1.2 (EFDE - purchased separately)
- ADDED: Automatic resolution of firewall logs and filtered websites
- ADDED: Ukrainian language
- ADDED: New filtering options
- ADDED: Many other performance, usability, and security improvements
- IMPROVED: Discontinued the default limit for the number of displayed static groups
- IMPROVED: Performance improvements in the “groups” tree on the “Computers” and “Detections” screens
- IMPROVED: Selected screens redesign: Users, scheduled reports and edit updates in the navigation bar
- IMPROVED: Unified table design for task selection, computers selection, and other features
- IMPROVED: Second-level menu added under "Change assignments" in the policy screen
- FIXED: Delay of product version status shown in the main web console
- FIXED: System applications are not reported on macOS 10.15
- FIXED: Language detection on macOS Catalina

- FIXED: Table sorting behavior: Clicking column headers adds columns to multi-sorting until it has been clicked 3 times
- FIXED: Last scan time in “computer details” screen won’t impact the computer security status tile
- FIXED: User cannot resolve detections when the “Resolved” column is not shown in the “detections” table
- FIXED: The side panel does not remember the expanded/collapsed state after log-out and log-in
- FIXED: Some threats cannot be marked as resolved
- FIXED: After moving computers from a specific group, the view is changed to the group "ALL."

ESET Cloud Administrator - ESET Management Agent release- June

- ADDED: New version of ESET Management Agent
- ADDED: Updating ESET Management Agent to the latest version can be deployed centrally alongside the cloud service update
- ADDED: Agent compatibility with H1/2021 Windows version 10

ESET Cloud Administrator 1.2.82.0

- IMPROVED: Email domain validation when sending live installer link was discontinued
- IMPROVED: Checkbox "automatically reboot when needed" not checked by default when activating EFDE from encryption tile
- IMPROVED: Dozens of usability, security, performance and stability improvements
- FIXED: Clicking column headers adds columns to multi-sorting until it has been clicked 3 times
- FIXED: Last Scan Time should note trigger red security status
- FIXED: Not possible to resolve detections when "Resolution" column is not shown
- FIXED: The side panel doesn't remember expanded/collapsed state after log-out and log-in
- FIXED: Agents stop connecting to cloud service under some circumstances
- FIXED: Recipients not visible in notifications emails
- FIXED: Computer with outdated OS are not visible in appropriate dynamic group
- FIXED: Ability to create hash exclusion without a hash present
- FIXED: ESET Full Disk Encryption not included within the selective export task configuration

ESET Cloud Administrator 1.2

- NEW: ESET Full Disk Encryption

- NEW: Tagging - mark all relevant objects (e.g., computers) using user-defined tags
- NEW: Support for the newest generation of Linux products, starting with ESET File Security for Linux v7
- NEW: Centralized Exclusions and wizard
- ADDED: Option to automatically delete computers that are not connecting
- ADDED: Option to rename computers based on defined criteria
- ADDED: Computer isolation task
- ADDED: Unified table design with new navigation elements
- ADDED: Ability to export tables across all the main screens to different formats
- ADDED: New "empty screen states" for simpler object creation
- ADDED: Detections view is now aggregated by time and other criteria to simplify operations and to resolve them
- ADDED: Execute one click actions from the "task executions" screen
- ADDED: Create a combined installer including ESET Full Disk Encryption
- ADDED: Option to deactivate individual products
- ADDED: New dynamic groups related to newly introduced products
- ADDED: Search by group name in computer screens and search bar
- ADDED: Option to save dashboard layout as preset for other users
- ADDED: Generate defined reports filtered to a selected group
- ADDED: Indonesian language support
- ADDED: New ESET Management Agent version (Windows) supports the latest security products
- IMPROVED: Many UI Improvements & other usability changes
- IMPROVED: Context menu now applies for all selected rows
- IMPROVED: Filtering panel has many new options such as autocomplete
- IMPROVED: New column selector element for primary tables
- IMPROVED: Layout of detections (previously "threats") screen with new detection details
- IMPROVED: Reports screen layout includes a one click report generation option
- IMPROVED: Task section was updated and triggers are now displayed in a separate view of "task details"
- IMPROVED: Layout of policies screen, with simpler orientation and navigation

- IMPROVED: Layout of notifications screen with notification details
- IMPROVED: Quick links menu
- IMPROVED: AV remover (part of management agent) supports auto update
- IMPROVED: Download speeds from the repositories were significantly improved
- IMPROVED: Management agent file size significantly reduced
- CHANGED: "Threats" section was renamed to "Detections"
- CHANGED: Management agent compatibility update related to macOS 10.7 and 10.8 support (see the documentation for more details)
- CHANGED: ESET Cloud Administrator ends support for Endpoint and Server Security versions 6.4 and earlier
- FIXED: Various other bug fixes and internal performance improvements

ESET Cloud Administrator 1.1.360.0

- Added: Full support for endpoint version 7.1 products
- Fixed: Various bugs

ESET Cloud Administrator 1.1.359.0

- Improved: Internal performance improvements

ESET Cloud Administrator 1.1.358.0

- Improved: Overall performance improvements
- Changed: Updated copyright information
- Fixed: ESET Cloud Administrator (ECA) server does not receive all "Web protection" threats
- Fixed: "Web protection" threat details view in the webconsole displays an unexpected error
- Fixed: An uncaught exception occurs when working with ECA
- Fixed: Indonesian language support is missing in product installation filters
- Fixed: Server Device Status chart is missing

ESET Cloud Administrator 1.1.356.0

- FIXED: Issue with too many notifications send from one incident

ESET Cloud Administrator 1.1.350.0

- New version of ESET Management Agent fixing various installation/upgrade/repair issues
- Internal service performance improvements
- Fixed invalid installer CA certificate encoding in GPO installer script

ESET Cloud Administrator 1.1.349

- Various minor performance improvements

ESET Cloud Administrator 1.1.345

- Various minor bug fixes
- Wrong information is displayed under "Policy Product" column while creating the ECA Live installer

ESET Cloud Administrator 1.1.343.0

- One-click actions
- New one-click action - One click upgrade option – even from aggregated data
- New One-click actions to resolve "resolvable" actions – activate, reboot, update OS, or various protection issues
- Hardware inventory
- Redesigned client details section
- New "incident overview" dashboard, with new types of graphical elements, and one-click navigation to threats
- Improved Automatic resolving of handled threats
- Option to generate live installer without security product selected
- New status overview section
- Live installer now support offline cache to speed up the deployment
- Overall UI improvements (polished UI, new vector icons, updated menus)
- Updated "overview" dashboard with one click navigation & Configurable RSS feed
- Redesigned quick links & help links
- New layout for wizard elements
- Ability to switch ECA do different language in EBA (support for NEW languages)

- Automatic detection of "machine cloning"
- Ability to send e-mail directly from ECA when sending installer
- Automatic log-outs
- New more streamlined way when adding computers or using introductory wizard
- Redesigned "filter bar" with the option to remove / reset / save filter presets + "category filter" moved to "filters"
- New columns for number / highest severity of alerts, cloning questions, and hardware detection reliability status
- Enhanced filtering options by product name, version, number of alerts, policies, threats, & other options
- New "remove computer from management" wizard, showing clear steps how to correctly remove devices from ECA
- Redesigned task wizard
- New task types - Diagnostic (enable diagnostic / Log Collector)
- Section "logs" now includes tabs to display "Log Collector" and new section for "diagnostic logs"
- Alerts - Alert (problem) details are reported from the supported security products
- New dynamic groups for desktops and servers
- Questions to resolve conflicts
- Possible to locate threats detected by the same scan
- Added current detection engine version and a hash value
- Possibility to filter by cause, threat type, scan, scanner and define more granular criteria for the time filter in threats
- Possibility to collapse and expand all reports in one click
- Software installation task executes a "pre-execution check", and reports "task failed" with further details
- New report template categories Hardware Inventory, Cloning Detection
- Restyled report creation wizard
- Extended options for filtering for specific values
- Redesigned installer generation flow
- Ability to configure LiveGrid and PUA settings when creating live installer
- Ability to configure Live Installer proxy settings during the installer creation

- Support for GPO (Group policy)
- New filter to "hide not-assigned policies"
- Policy details showing "assigned to" (combines computers / groups) and "applied on" (actually applied targets)
- New predefined policies for optimal usage of ESET Live Grid, and few tweaks to existing recommended templates for maximum protection
- Possibility to allow "local lists"
- Possible to edit multiple notifications at once
- New announcement channel to inform users about planned outages and other important events
- Improved migration from ERA6 (ESMC) managed environment when executing live installers

Navegadores da Web, produtos de segurança ESET e idiomas compatíveis

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

Recomendamos usar a versão mais recente do Agente ESET Management para gerenciar totalmente a versão mais recente dos produtos de segurança ESET e seus recursos.

Produto	Versão do produto
ESET Endpoint Security para Windows	7.3+
ESET Endpoint Antivirus para Windows	7.3+
ESET Endpoint Security para macOS	6.10+
ESET Endpoint Antivirus para macOS	6.10+
ESET File Security para Windows Server	7.3+
ESET Server Security para Microsoft Windows Server	7.3+

Produto	Versão do produto
ESET Mail Security para Microsoft Exchange Server	7.3+
ESET Security para Microsoft SharePoint Server	7.3+
ESET Mail Security para IBM Domino Server	7.3+
ESET File Security para Linux	7.2+
ESET Server Security para Linux	7.2, 8.1, 9.x, 10.x
ESET Endpoint Antivirus para Linux	7.1, 8.1, 9.x, 10.x
ESET Endpoint Security para Android	3.3+
ESET Inspect Connector	1.8+
ESET Full Disk Encryption para Windows	
ESET Full Disk Encryption para macOS	
ESET LiveGuard Advanced	

Idiomas compatíveis

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

Sistemas operacionais compatíveis

As tabelas a seguir mostram os sistemas operacionais compatíveis para cada componente do ESET PROTECT:

Controle de versão e suporte do Agente ESET Management

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

- As versões compatíveis com o Agente ESET Management são 9.x–11.x.
- Cada versão do Agente ESET Management recebe seis meses de Suporte completo e dois anos de Suporte limitado. Em seguida, a versão transita para o Fim da vida útil.

A versão mais recente do Agente ESET Management compatível é a 11.x. Recomendamos usar a versão mais recente do Agente ESET Management para gerenciar totalmente a versão mais recente dos produtos de segurança ESET e seus recursos.

Windows

Sistema operacional	Agente	Sensor RD
Windows Server 2012 x64	9.x—10.x, 11.x	✔
Windows Server 2012 CORE x64	9.x—10.x, 11.x	✔
Windows Server 2012 R2 x64	9.x—10.x, 11.x	✔
Windows Server 2012 R2 CORE x64	9.x—10.x, 11.x	✔
Windows Storage Server 2012 R2 x64	9.x—10.x, 11.x	✔
Windows Server 2016 x64	9.x—10.x, 11.x	✔
Windows Storage Server 2016 x64	9.x—10.x, 11.x	✔
Windows Server 2019 x64	9.x—10.x, 11.x	✔
Windows Server 2022 x64	9.x—10.x, 11.x	✔
Windows Server 2022 CORE x64	11.x	

Sistema operacional	Agente	Sensor RD
Windows 10 x86	9.x—10.x, 11.x	✔
Windows 10 x64 (todos os lançamentos oficiais)	9.x—10.x, 11.x	✔
Windows 10 no ARM	9.x—10.x, 11.x	
Windows 11 x64	9.x (21H2) 10.x, 11.x (21H2,22H2) 10.1, 11.x (23H2)	✔
Windows 11 no ARM	10.x, 11.x	

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

Linux

Sistema operacional	Agente	Sensor RD
Ubuntu 18.04.1 LTS x64 Desktop	9.x—10.x, 11.x	✔
Ubuntu 18.04.1 LTS x64 Server	9.x—10.x, 11.x	✔
Ubuntu 20.04 LTS x64	9.x—10.x, 11.x	✔
Ubuntu 22.04 LTS x64	10.x, 11.x	✔
Linux Mint 20	10.x, 11.x	✔
Linux Mint 21	10.1, 11.x	✔
RHEL Server 7 x64	9.x—10.x, 11.x	✔
RHEL Server 8 x64	9.x—10.x, 11.x	
RHEL Server 9 x64	9.x—10.x, 11.x	✔
CentOS 7 x64	9.x—10.x, 11.x	✔
SLED 15 x64	9.x—10.x, 11.x	✔
SLES 12 x64	9.x—10.x, 11.x	✔
SLES 15 x64	9.x—10.x, 11.x	✔
Debian 9 x64	9.x—10.x, 11.x	✔
Debian 10 x64	9.x—10.x, 11.x	✔
Debian 11 x64	9.x—10.x, 11.x	✔
Debian 12 x64	10.1, 11.x	✔
Oracle Linux 8	9.x—10.x, 11.x	✔
Amazon Linux 2	9.x—10.x, 11.x	✔
Alma Linux 9	10.1, 11.x	✔
Rocky Linux 8	10.1, 11.x	
Rocky Linux 9	10.1, 11.x	

O Agente ESET Management foi testado e executado nas últimas versões secundárias das distribuições Linux listadas.

Mac

Sistema operacional	Agente
macOS Catalina (10.15)	9.x—10.x, 11.x
macOS Big Sur (11.0)	9.x—10.x, 11.x
macOS Monterey (12.0)	9.x—10.x, 11.x
macOS Ventura (13.0)	9.x—10.x, 11.x
macOS Sonoma (14.0)	10.1, 11.x

Móvel

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

* O iOS ABM só está disponível em países selecionados.

Pré-requisitos de rede

Permita que os pré-requisitos de rede a seguir no seu firewall do ESET PROTECT funcionem corretamente.

Domínios e portas

Domínio	Protocolo	Porta	Serviço/componente	Descrição
eba.eset.com	TCP	443	ESET Business Account	
msp.eset.com	TCP	443	ESET MSP Administrator	
identity.eset.com	TCP	443	ESET Identity Server	
protect.eset.com	TCP	443	ESET PROTECT	

Domínio	Protocolo	Porta	Serviço/componente	Descrição
eu02.protect.eset.com	TCP	443	Console da Web ESET PROTECT	Local: Europa
us02.protect.eset.com	TCP	443		Local: EUA
jp02.protect.eset.com	TCP	443		Local: Japão
*.a.ecaserver.eset.com	TCP	443	Conexão entre o Agente e o ESET PROTECT	
edf.eset.com	TCP	443	Live Installer	
redirector.eset.systems	TCP	443		
repository.eset.com	TCP	80		Repositório necessário para instalação.
epns.eset.com	TCP	8883	Conexão para o serviço EPNS (chamadas para despertar)	
eu.mdm.eset.com (EUROPA) us.mdm.eset.com (EUA) jp.mdm.eset.com (JAPÃO)	TCP	443	Cloud MDM	Inscrição
checkin.eu.eset.com (EUROPA) checkin.us.eset.com (EUA) checkin.jp.eset.com (JAPAN)	TCP	443		Check-in
mdmcomm.eu.eset.com (EUROPA) mdmcomm.us.eset.com (EUA) mdmcomm.jp.eset.com (JAPAN)	TCP	443		Comunicação
mdm.eset.com (GLOBAL)	TCP	443		Inscrição limitada de dispositivo de entrada
	TCP	139	ESET PROTECT Remote Deployment Tool (Porta de destino do ponto de vista do Remote Deployment Tool)	Usando o compartilhamento ADMIN$
	TCP	445		Acesso direto a recursos compartilhados usando TCP/IP durante a instalação remota (uma alternativa para TCP 139)
	UDP	137		Resolução de nome durante a instalação remota
	UDP	138		Procurar durante a instalação remota

Endereços IP

Endereço IP	Serviço	Descrição
20.82.100.209	Conexão entre o ESET Management Agente e o ESET PROTECT	Local: Europa
20.245.38.118		Local: EUA
20.194.197.189		Local: Japão
13.69.61.76	Conexão do Web Console ESET PROTECT	Local: Europa
23.99.91.144		Local: EUA
20.46.163.70		Local: Japão

Encontre os pré-requisitos de rede para o **ESET Connect** na Ajuda on-line do ESET Connect.

Disponibilidade do serviço

Disponibilidade

Nossa meta é fornecer uma disponibilidade de serviço de 99,5%. Nosso esforço interno e processos bem definidos orientam esse empreendimento. No caso de uma interrupção do serviço ESET PROTECT, os endpoints permanecerão seguros e não serão afetados.

O Portal de Status ESET exibe o status atual dos serviços de nuvem da ESET, interrupções programadas e incidentes passados. Se você estiver enfrentando um problema com um serviço suportado pela ESET e não o vir listado no Portal de Status, entre em contato com o Suporte Técnico ESET.

As equipes de monitoramento verificam possíveis problemas internamente e os incidentes confirmados são publicados e atualizados manualmente para manter alta credibilidade e precisão. Portanto, eles aparecem no Portal de Status com um pequeno atraso. Incidentes com curta duração podem não ser publicados se forem resolvidos antes de serem confirmados manualmente.

Manutenção

O serviço ESET PROTECT está sujeito a procedimentos de manutenção de rotina. Todas as janelas de manutenção que ultrapassam 15 minutos são anunciadas para os administradores do console antecipadamente. Paralisações durante as janelas de manutenção não afetam nossa meta de disponibilidade. A manutenção será realizada durante os fins de semana e fora do horário de trabalho (centro de dados dos EUA: durante o horário da noite nos EUA. Centro de dados da UE: durante o horário da noite da UE. Centro de dados do Japão: durante o horário da noite do Japão).

Diferenças entre o console de gerenciamento local e na nuvem

O ESET PROTECT inclui todos os principais recursos e funcionalidades que você conhece do ESET PROTECT On-Prem, mas foi ajustado para atender às necessidades de um gerenciamento baseado em nuvem. Você pode migrar do ESET PROTECT on-prem para o ESET PROTECT.

A tabela abaixo contém descrições das principais diferenças entre o ESET PROTECT e o ESET PROTECT On-Prem.

Diferença geral	ESET PROTECT	ESET PROTECT On-Prem
Hospedagem	É executado no ambiente de nuvem mantido pela ESET.	É executado em seu ambiente físico ou virtualizado.
Limitação de dispositivos gerenciáveis	50.000 dispositivos do cliente.	A limitação depende das limitações de hardware do servidor.
Versões de produtos compatíveis	• Produtos empresariais versão 6 e versões posteriores	• Produtos empresariais versão 4 e versões posteriores
Componentes	• Agente ESET Management • Sensor RD • Ferramenta de implantação • CloudMDM	• Agente ESET Management • Sensor RD • Ferramenta de implantação • MDM
Active Directory	A sincronização Active Directory está disponível com o uso do Escaneador ESET Active Directory.	A sincronização Active Directory está disponível.
Gestão de dispositivo móvel	• Por padrão, o gerenciamento de dispositivo móvel está disponível via CloudMDM. • A inscrição de entrada limitada para dispositivos Android está disponível como uma opção de inscrição.	• O gerenciamento de dispositivo móvel está disponível via ESET PROTECT On-Prem MDM. ⚠ O componente gerenciamento de dispositivo móvel ESET PROTECT/conector (MDM/MDC) (somente local) chegou ao fim da vida útil em janeiro de 2024. Ler mais. Recomendamos que você migre para o gerenciamento de dispositivo móvel em nuvem.
Certificados	O gerenciamento de certificados é tratado pela ESET.	O usuário pode criar, editar ou importar/exportar Certificados e Autoridades de certificação

Diferença geral	ESET PROTECT	ESET PROTECT On-Prem
Direitos de acesso	O gerenciamento de Direitos de acesso foi movido para ESET Business Account mas você pode especificar o acesso a recursos específicos do ESET PROTECT para um usuário com permissões personalizadas.	Modelo de segurança avançado de direitos de acesso multi-inquilino que pode ser gerenciado da interface ESET PROTECT On-Prem
Gerenciamento de licenças	O gerenciamento de licenças foi totalmente movido para o ESET Business Account.	O gerenciamento de licenças está parcialmente no ESET PROTECT On-Prem e parcialmente no ESET Business Account.
Como adicionar computadores	Computadores podem ser adicionados através da sincronização Sincronização do Active Directory, de um relatório do sensor RD e usando scripts do instalador GPO e SCCM.	Computadores podem ser adicionados via Active Directory sync, de um relatório de sensor RD, usando os scripts de instalador GPO e SCCM, manualmente adicionando um novo dispositivo com a adição de uma Tarefa de instalação do agente ou instalando o Agente localmente.
Camadas de proteção adicionais	• ESET Gerenciamento de patch e de vulnerabilidade • ESET LiveGuard • ESET Full Disk Encryption • ESET Inspect O ESET PROTECT não é compatível com ESET Inspect On-Prem mas é compatível com o ESET Inspect. Se você migrar do ESET PROTECT On-Prem para o ESET PROTECT, você não será capaz de gerenciar o ESET Inspect On-Prem do ESET PROTECT, mas poderá gerenciar o ESET Inspect do ESET PROTECT.	• ESET LiveGuard • ESET Full Disk Encryption • ESET Inspect Local

Introdução ao ESET PROTECT

ESET PROTECT é a solução de fábrica para gerenciar os produtos ESET Security em sua rede comercial pequena e média. Ele representa uma nova abordagem, ampliando a antiga solução ESET no local e introduzindo um novo serviço mais flexível, baseado em nuvem, hospedado e mantido pela ESET.

Essa solução oferece uso imediato e abre mão das etapas de instalação e configuração exigidas pelas soluções locais. O ESET PROTECT é construído para ser fácil de instalar e de usar. Este novo serviço hospedado na nuvem vem com um console de administração contemporâneo baseado na web (Console Web ESET PROTECT), ao qual você pode se conectar de praticamente qualquer lugar e/ou dispositivo com uma conexão com a internet adequada.

As seções a seguir detalham os recursos do Console da Web ESET PROTECT e como usá-los. Você pode criar instaladores e instalar o Agente ESET Management e produtos de segurança ESET em computadores do cliente. Após a instalação do Agente ESET Management você pode gerenciar grupos, criar e atribuir políticas e configurar notificações e relatórios.

Introdução ao ESET PROTECT

Estou usando o ESET Business Account

1.Criar uma nova instância ESET PROTECT.

2.Configurar usuários ESET PROTECT no ESET Business Account.

3.Abrir o Console Web ESET PROTECT. Veja também o Tour do ESET PROTECT e a visão geral do Web Console ESET PROTECT.

4.Mapear usuários do ESET Business Account no Web Console ESET PROTECT.

5.Adicione computadores cliente na sua rede à estrutura ESET PROTECT.

6.Gerencie produtos Endpoint do ESET PROTECT.

Estou usando o ESET MSP Administrator

1.Criar uma nova instância ESET PROTECT.

2.Configurar usuários ESET PROTECT no ESET MSP Administrator.

3.Abrir o Console Web ESET PROTECT. Veja também o Tour do ESET PROTECT e a visão geral do Web Console ESET PROTECT.

4.Adicione usuários ESET MSP Administrator ao Web Console ESET PROTECT durante a configuração do cliente MSP.

5.Adicione computadores cliente na sua rede à estrutura ESET PROTECT.

6.Gerencie produtos Endpoint do ESET PROTECT.

Criar uma nova instância ESET PROTECT usando o ESET Business Account

Pré-requisitos

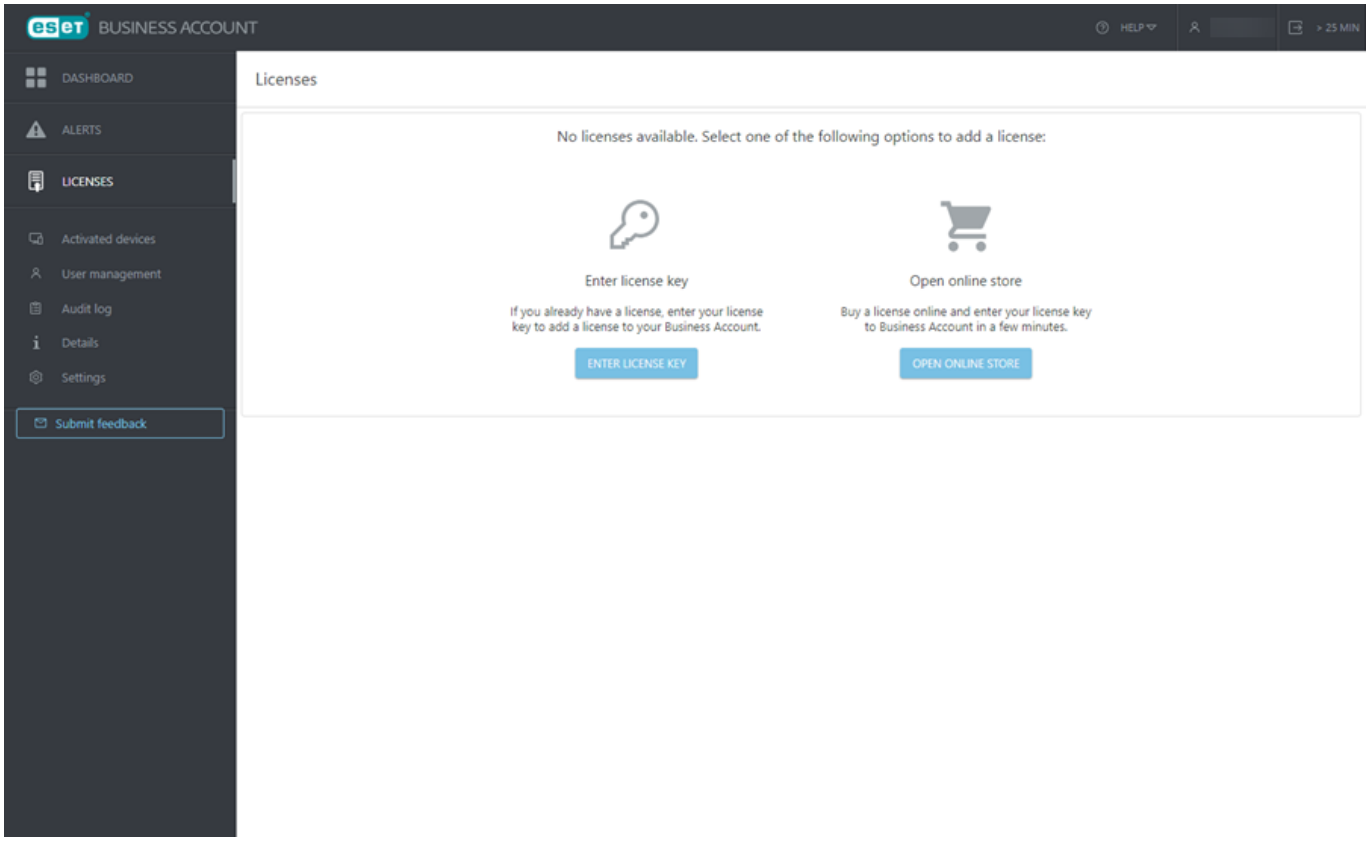
- Uma conta de Superusuário no ESET Business Account.
- Uma licença elegível para o ESET PROTECT.

Se as suas contas EBA e EMA2 estiverem registradas no mesmo endereço de e-mail, o ESET PROTECT pode ser ativado de apenas uma conta. A conta (EBA ou EMA2) para a qual você escolher criar a instância ESET PROTECT será a única que você pode usar para ativar ou remover a instância.

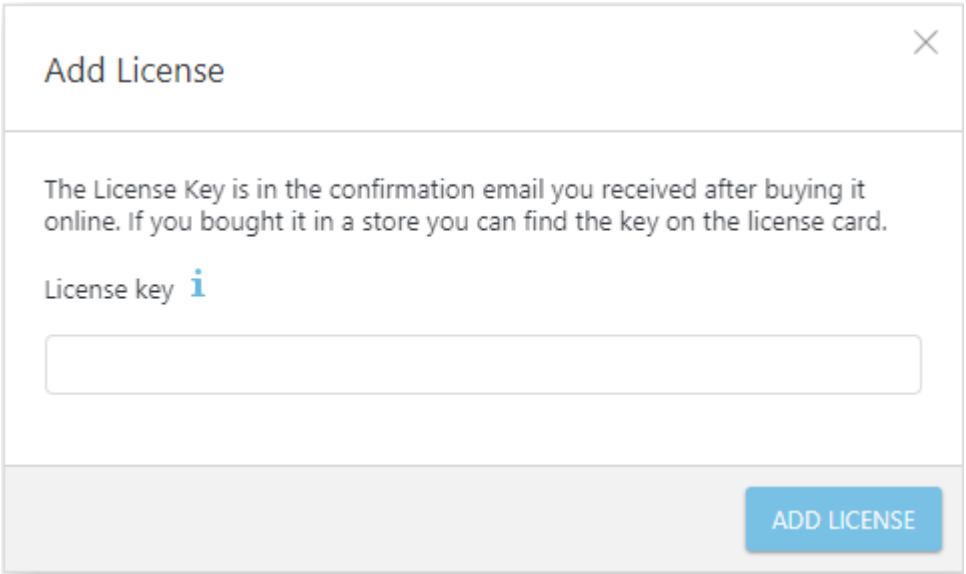
Criar uma nova instância ESET PROTECT

1. Abra o ESET Business Account e entre (ou crie uma nova conta).

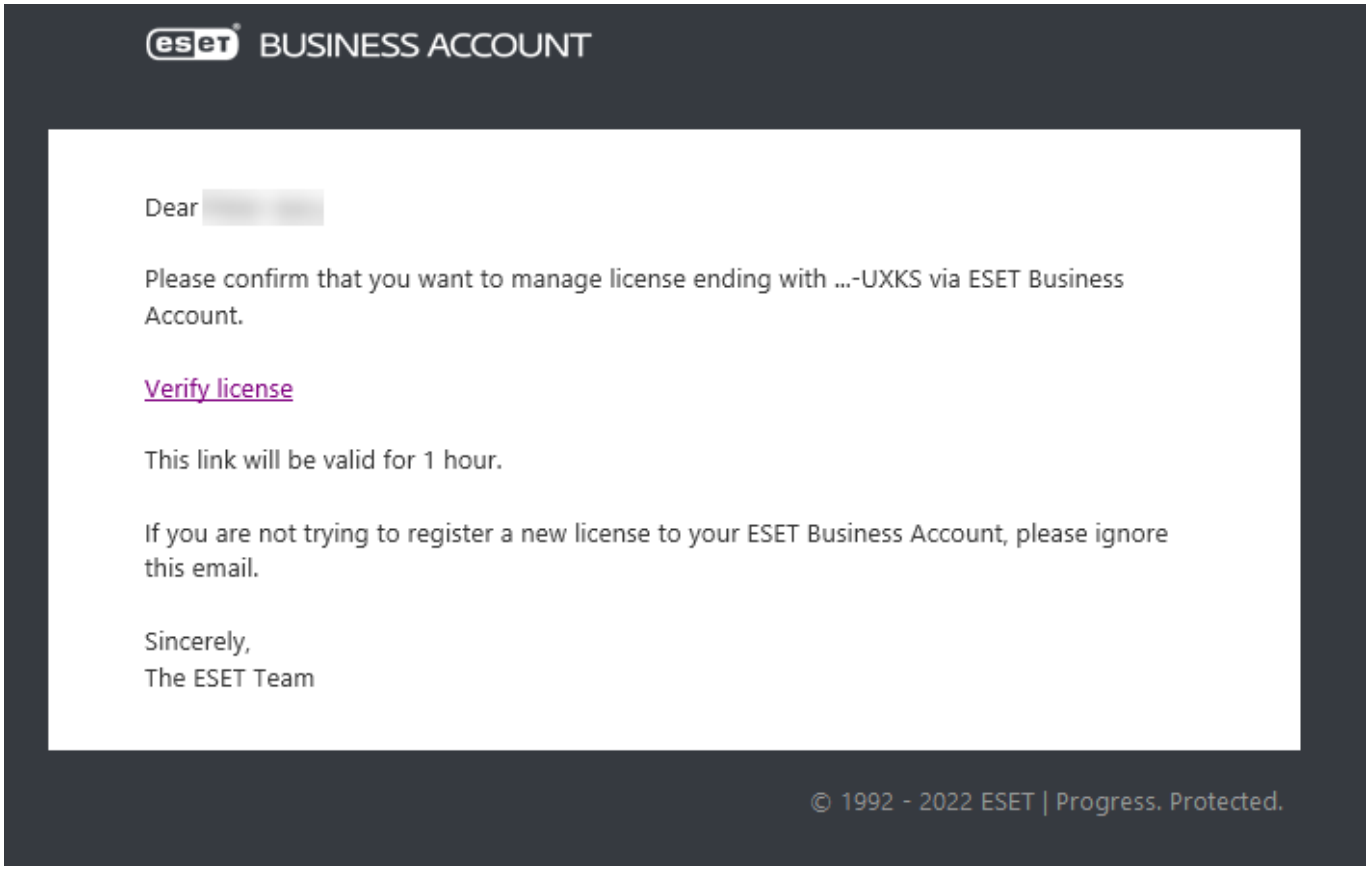
2. Clique em **Licenças** > **Inserir chave de licença**.



3. Na janela **Adicionar licença**, insira sua **Chave de licença** ESET PROTECT e clique em **Adicionar licença**.



4. Você receberá um e-mail de verificação (se não receber o e-mail, siga as instruções do artigo da Base de conhecimento). Clique em **verificar licença**.



5. No **Painel** clique em **Ativar** sob **ESET PROTECT**.

⚠ Verifique a configuração de idioma do seu ESET Business Account. Alguns elementos da janela principal do programa do ESET PROTECT são definidos na primeira vez que você define o idioma nas configurações de idioma ESET Business Account e não podem ser alterados posteriormente.

6. Uma janela **Ativar ESET PROTECT** será aberta. Leia os Termos de uso e marque a caixa de seleção se você concordar.

7. Selecione um local do centro de dados para sua instância do ESET PROTECT que seja o mais próximo do local de sua rede gerenciada e clique em **Continuar**.

⚠ Depois de selecionado você não conseguirá alterar a localização do centro de dados da sua instância ESET PROTECT.

8. Sua instância ESET PROTECT será criada. Você pode aguardar alguns minutos até que ele seja criado ou você pode sair e você será notificado por email assim que a instância do ESET PROTECT estiver disponível.

9. Clique em **Continuar**. Alternativamente, clique em **Painel**, clique em **Abrir** no bloco ESET PROTECT para abrir uma nova guia com o Web Console ESET PROTECT.

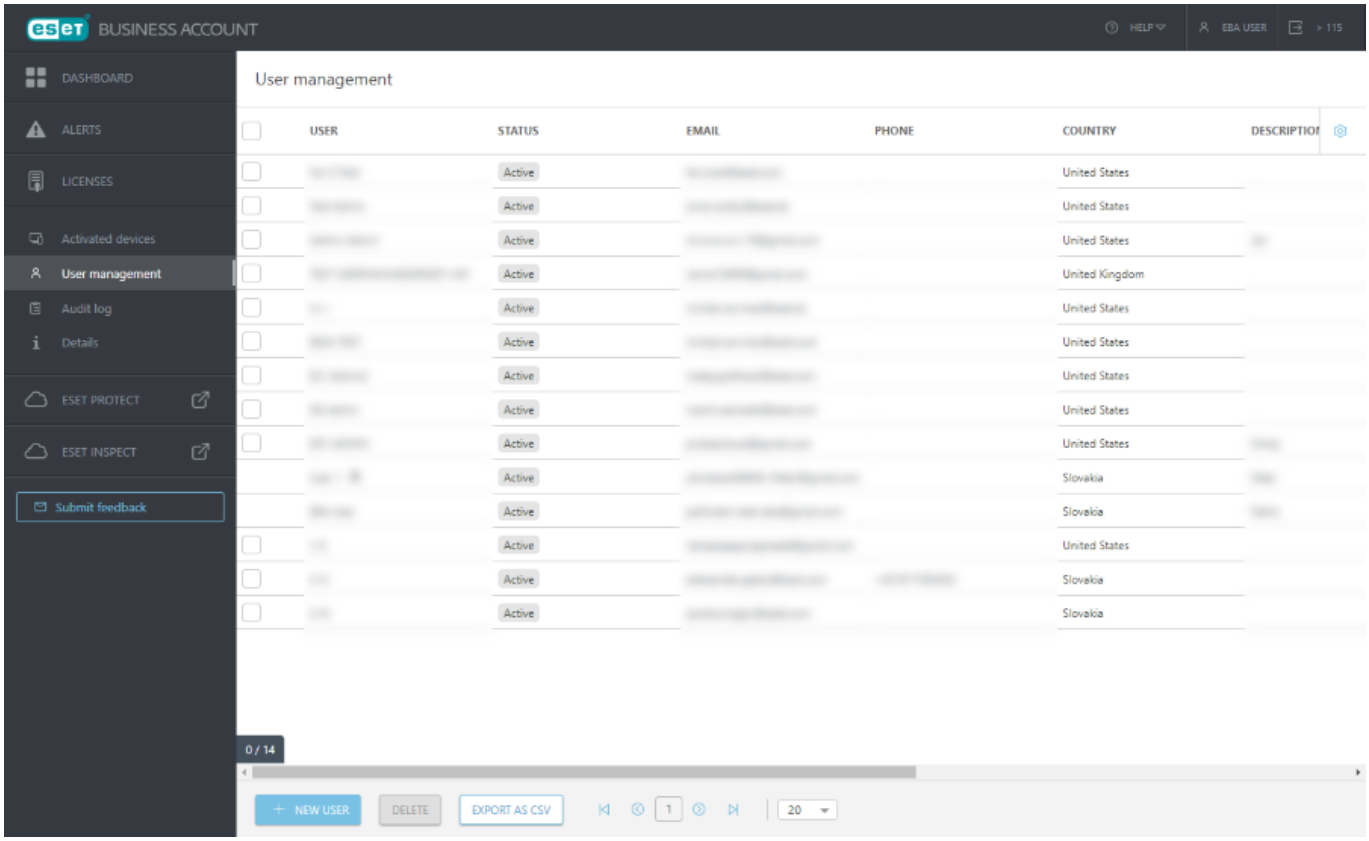
O ESET PROTECT sincroniza sua estrutura ESET Business Account com a árvore do Grupo estático em **Computadores** no Web Console.

Criar um novo usuário ESET PROTECT no ESET Business Account

Siga as etapas abaixo para criar um novo usuário ESET PROTECT no ESET Business Account e mapear a conta do usuário no ESET PROTECT:

1. Entre em sua conta ESET Business Account.

2. Selecione **Gerenciamento de usuário** > **Novo usuário**.



3. Preencha os campos necessários (leia mais na ajuda on-line ESET Business Account):

I.**Geral** – fornece informações básicas sobre o usuário

II.**Direitos de acesso**:

a)**Acesso da empresa** – selecione o nível de acesso da empresa do usuário: **Gravação**, **Leitura**, **Acesso somente para os sites selecionados**.

> Um usuário deve ter **Acesso de gravação da Empresa** para ver outros usuários ESET Business Account no ESET PROTECT.

b)**Acesso de gerenciamento de usuário** – selecione a caixa de seleção para permitir ao usuário gerenciar outros usuários no ESET Business Account.

c)**Acesso do ESET PROTECT e ESET Inspect**:

- **Gravação** – o usuário tem acesso completo ao ESET PROTECT e ESET Inspect.

- **Leitura** – o usuário pode apenas visualizar os dados no ESET PROTECT e ESET Inspect.
- **Personalizado** – é possível definir o acesso do usuário mais tarde no ESET PROTECT em Conjunto de permissões.
- **Sem acesso** – O usuário não tem acesso ao ESET PROTECT e ESET Inspect.

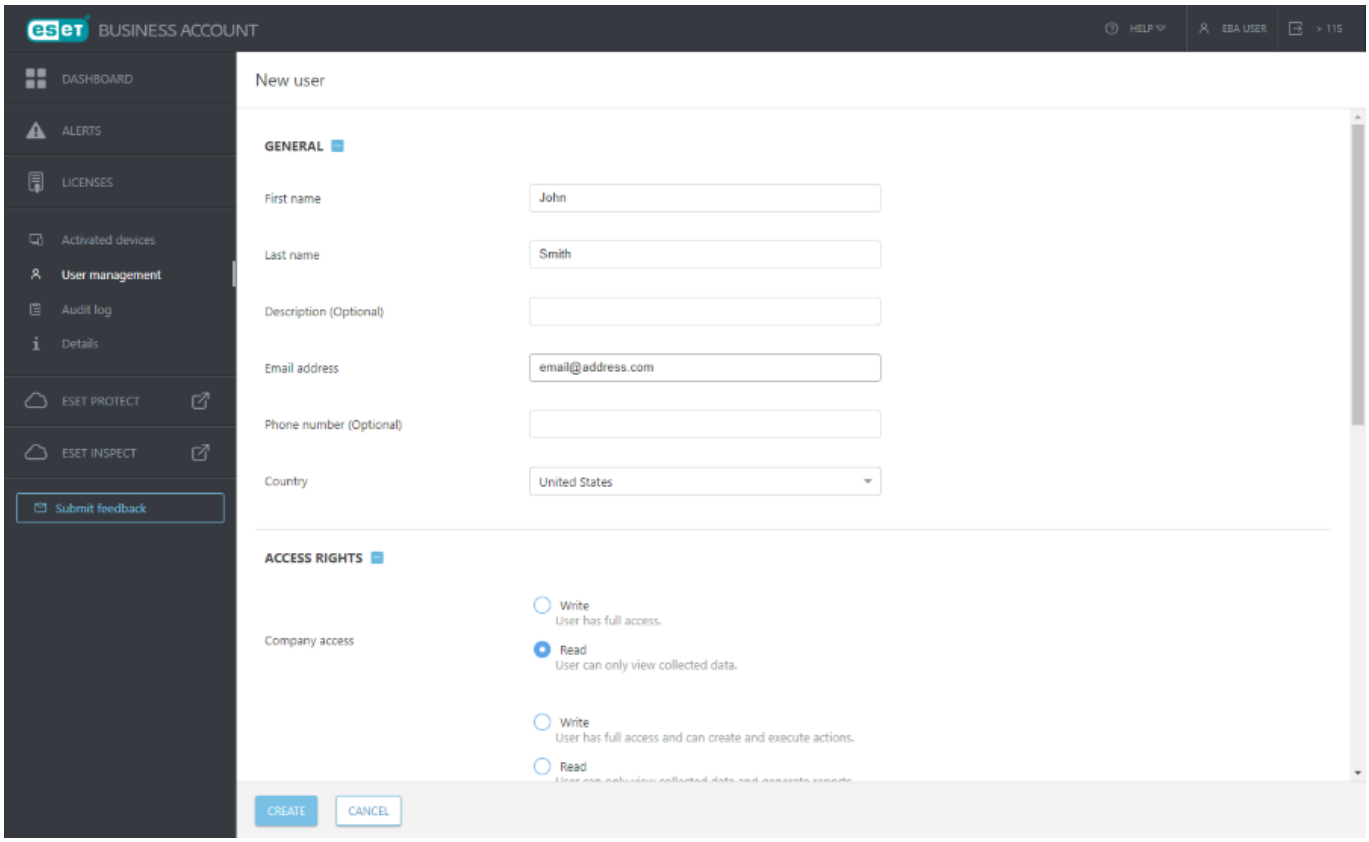
Para acessar ESET PROTECT, um usuário deve ter direitos de acesso de **Gravação** ou **Leitura** para pelo menos uma empresa com licença ESET PROTECT elegível (ativa).

- Para um usuário do site, selecione **Personalizado** em **ESET PROTECT Acesso**.
- Para criar outro usuário com direitos de acesso do Administrador, siga as etapas para criar um segundo Administrador no ESET PROTECT.

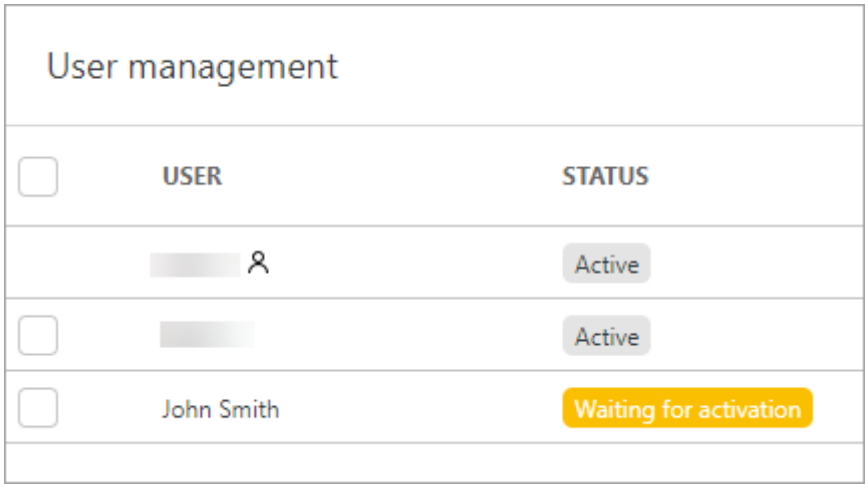
III. **Preferências** – define o idioma do usuário para o ESET Business Account e o ESET PROTECT e define o fuso horário.

IV. **Segurança** – ajusta as configurações de segurança para o usuário (expiração da senha, tempo limite de sessão ociosa, verificação em dois fatores).

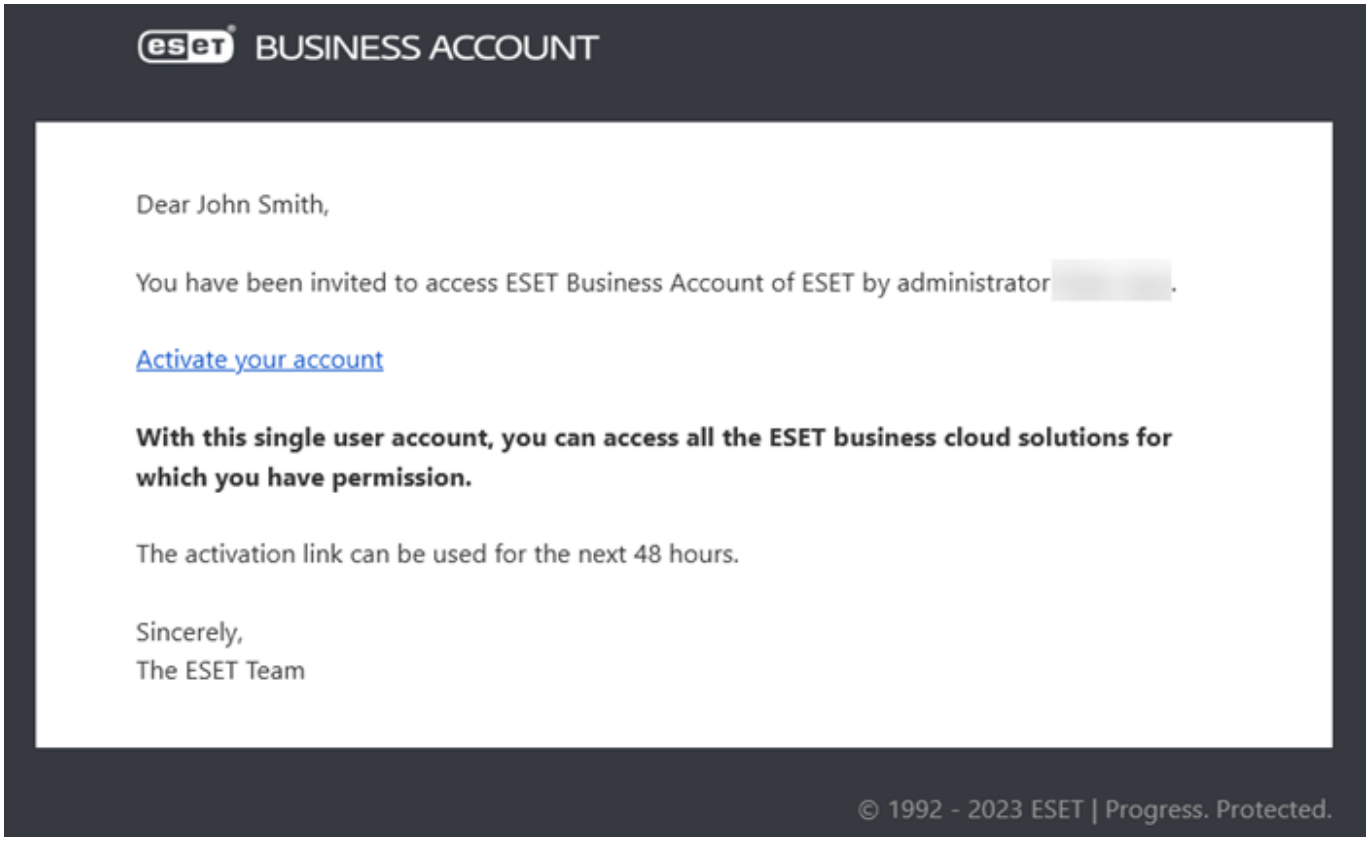
Clique em **Criar** para criar o usuário.



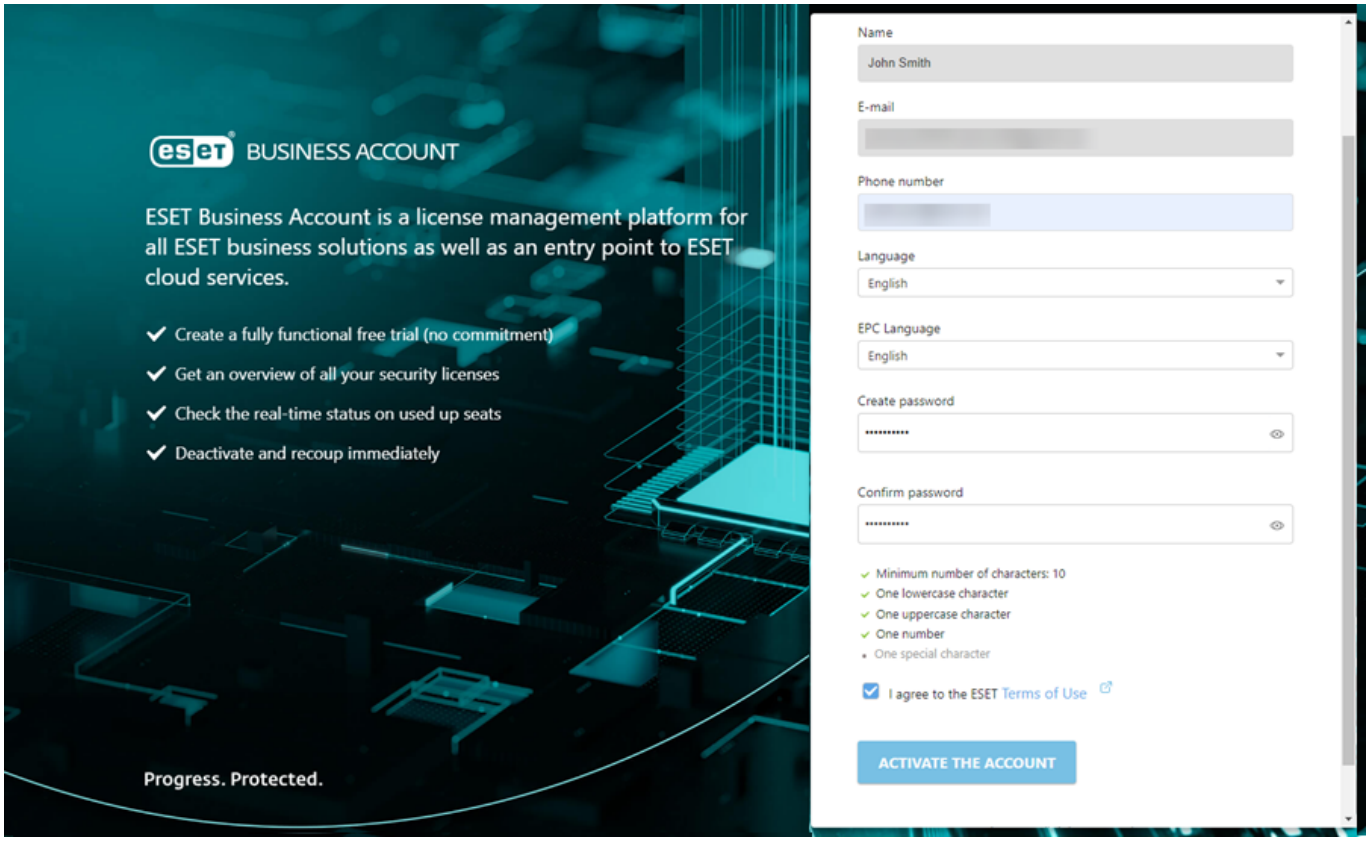
4. O novo usuário aparece no Gerenciamento de usuários com o rótulo **Aguardando ativação**.



5. O usuário receberá um e-mail de ativação (para o endereço de e-mail que você especificou ao criar o usuário). O usuário deve clicar em **Ativar sua conta**.



6. O usuário precisa ajustar as configurações de usuário e digitar a senha duas vezes (**Criar senha** e **Confirmar senha**), selecionar a caixa de seleção **Concordo com os Termos de uso da ESET** e clicar em **Ativar a conta**.



7. Mapeie o usuário no Web Console ESET PROTECT.

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 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 do 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 **Logout** para efetuar logout a qualquer momento. Quando a sessão atingir o limite de tempo (devido à inatividade do usuário), você deverá entrar novamente. 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.

- Você pode usar a ferramenta Pesquisar no topo do Web Console ESET PROTECT. Digite no mínimo 3 e no máximo 30 caracteres no campo de pesquisa para pesquisar estas categorias: **Nome do computador**, **Descrição do computador**, **Endereço IP do computador**, **Nome do grupo estático**, **Causa da detecção**,

Usuários do computador e **Contas mapeadas**. Você pode encontrar no máximo 3 resultados em cada categoria. Clique no resultado para exibir os detalhes e clique em **Todos os resultados** para exibir a seção específica do Web Console com o filtro de categoria aplicado.

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

Links rápidos
Configurar seus dispositivos
• Dispositivos Windows
• Dispositivos macOS
• Dispositivos Linux
• Dispositivos móveis
Gerenciar dispositivos
• Criar tarefa de cliente
• Criar nova política
• Atribuir política
• Fazer download da Política de migração
• Configurar proteção
Gerenciar conta
• Abrir o ESET Business Account
• Gerenciar direitos de acesso
• Gerenciar licenças
Outras
• Recursos de visualização

- 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, ESET MSP Administrator, ESET Cloud Office Security (você pode ver os respectivos produtos com base na sua licença e nos direitos de acesso)

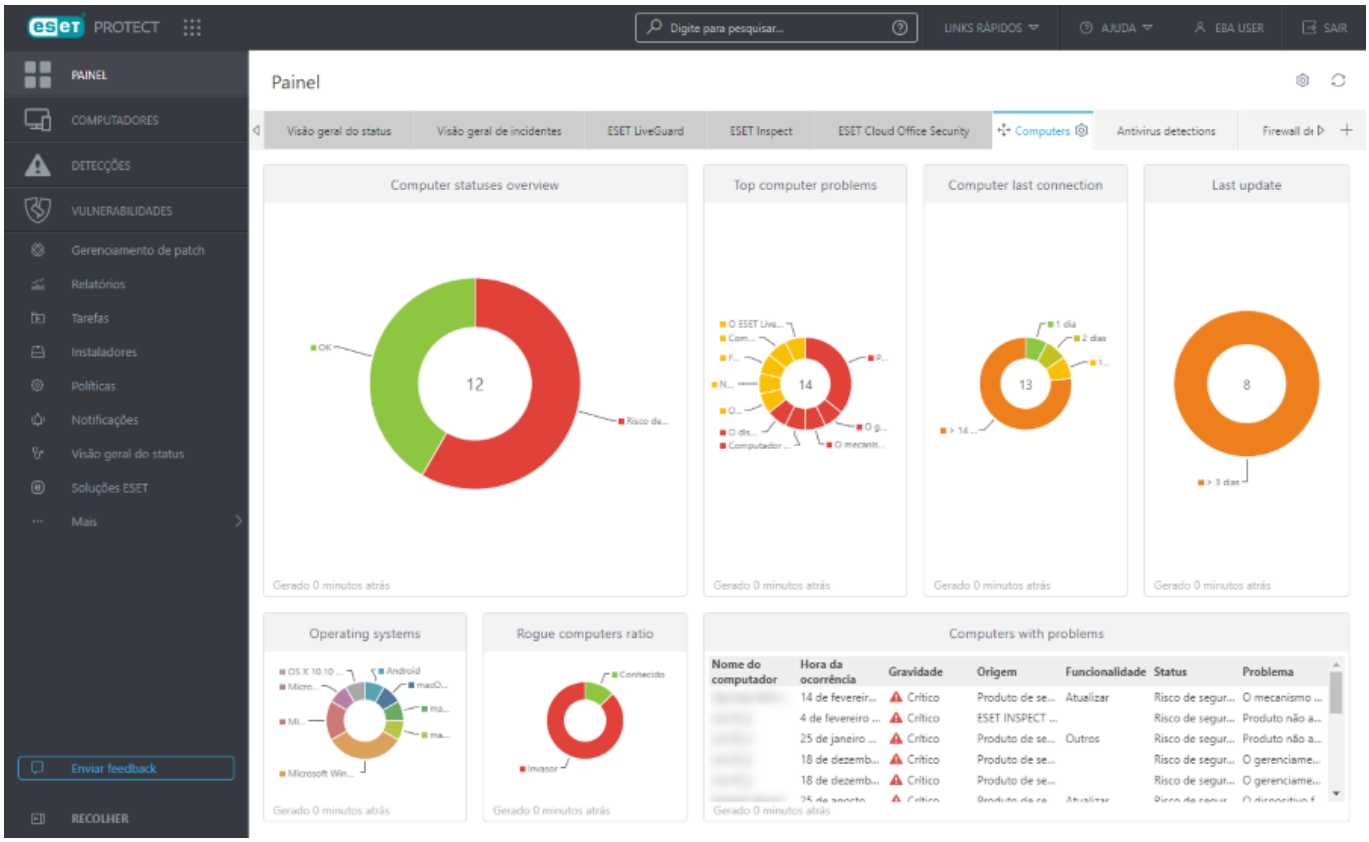
- O ícone de **Engrenagem**  sempre denota um menu de contexto.

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

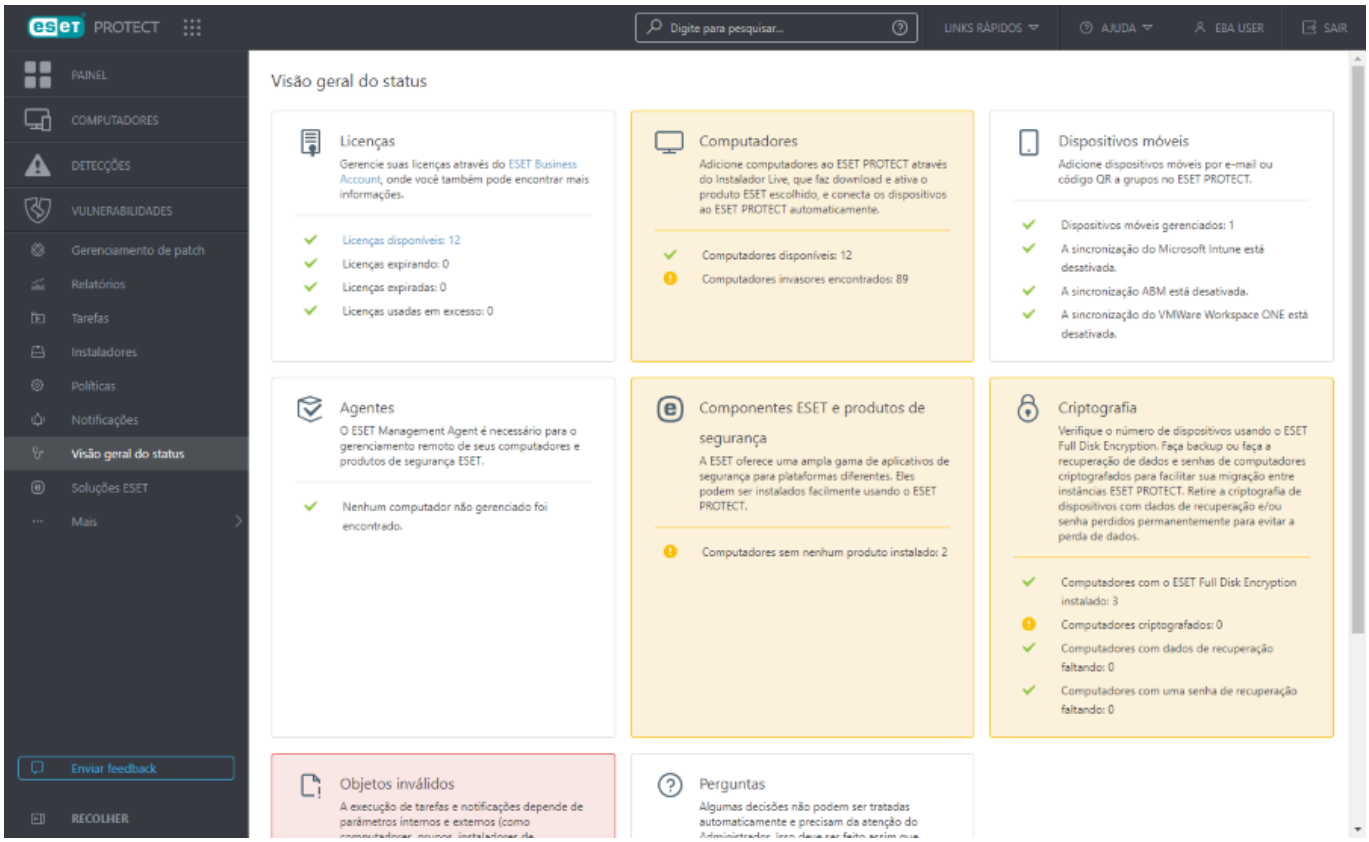
- Os botões na parte inferior da página são exclusivos para cada seção e função, e são descritos em detalhes em seus respectivos capítulos.

- O Web Console ESET PROTECTinforma o administrador sobre os Acordos de Licença de Usuário Final atualizados dos produtos de segurança ESET gerenciados ou sobre o tráfego excepcionalmente alto de computadores gerenciados

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

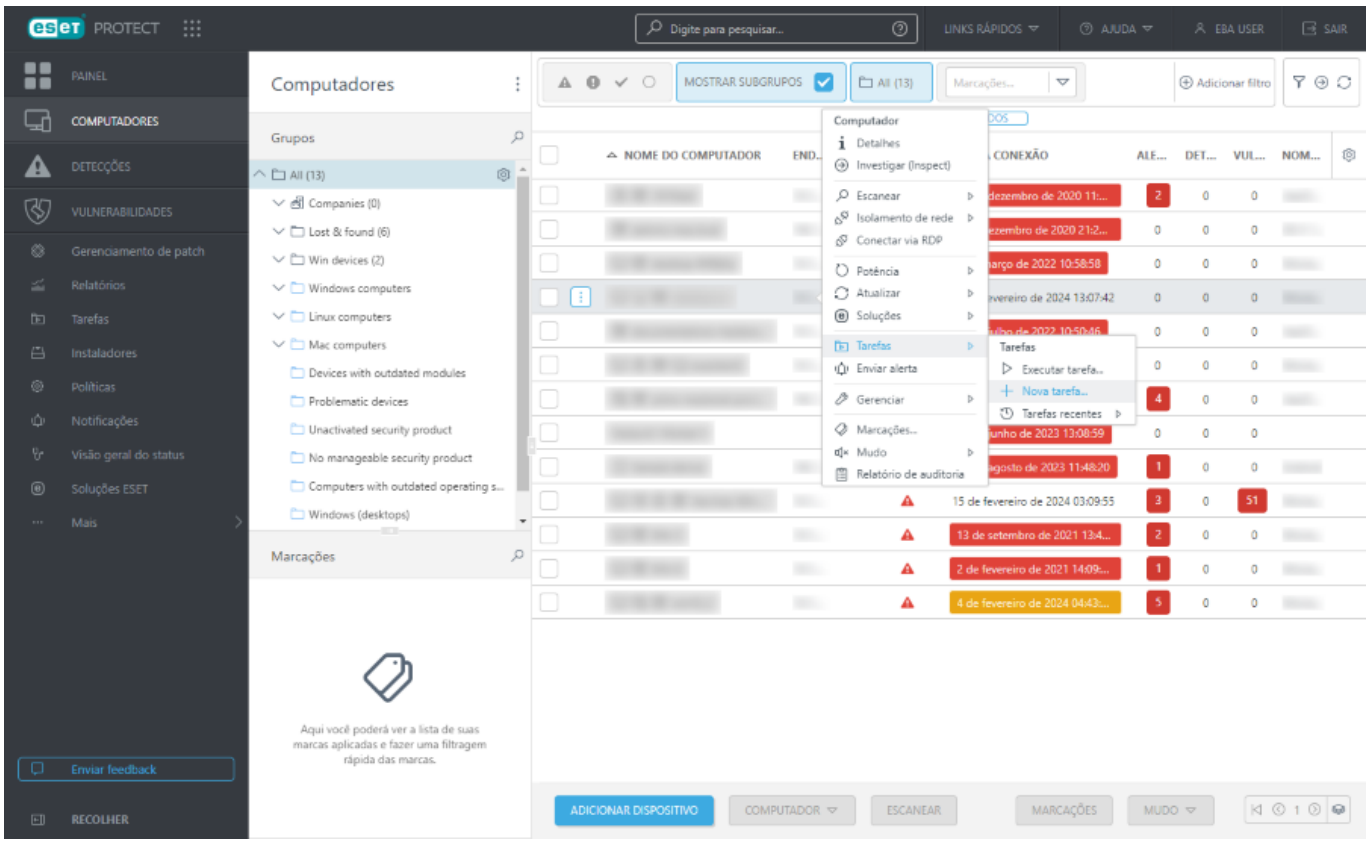


Visão geral do status mostra como obter o máximo do ESET PROTECT. Isso vai orientá-lo pelas etapas recomendadas.



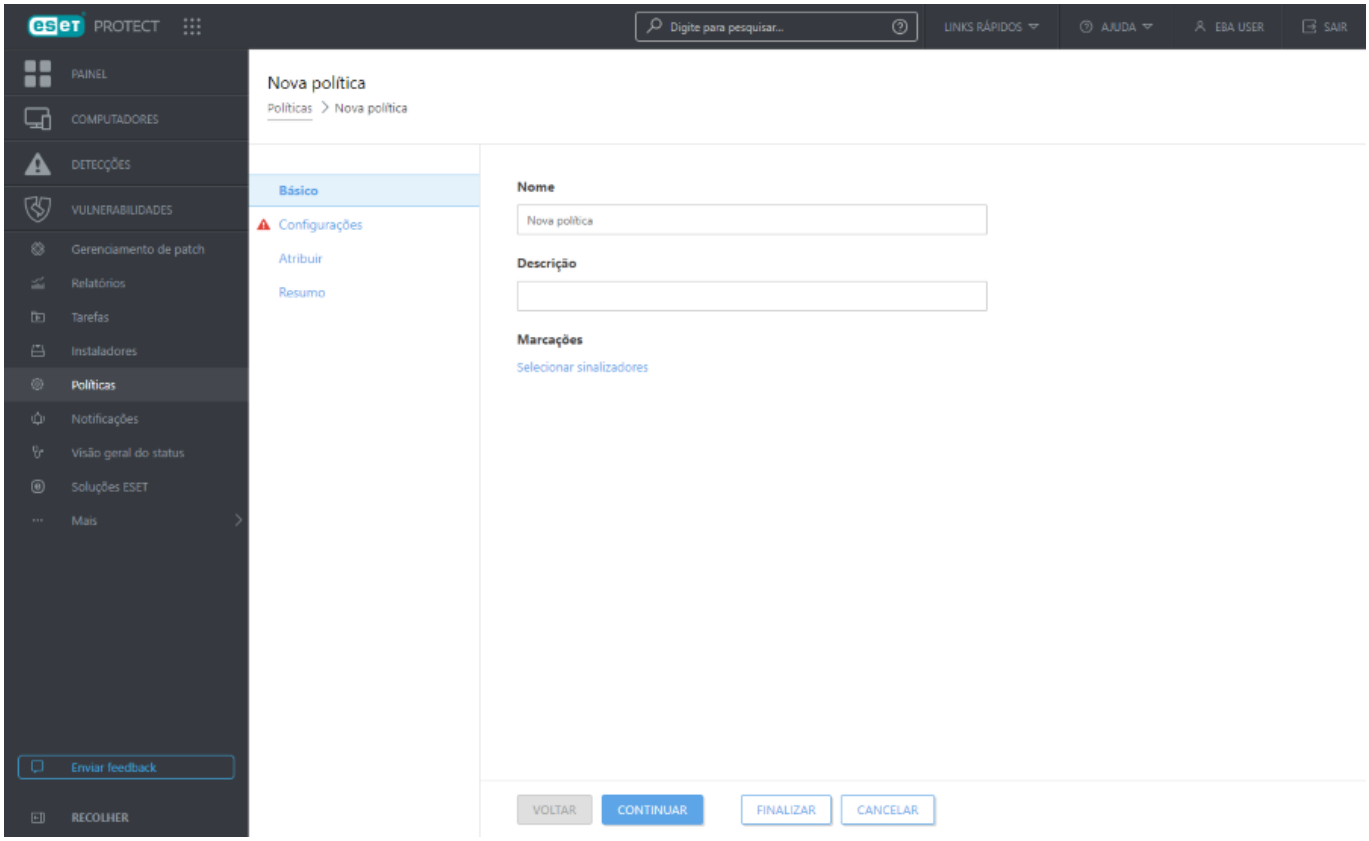
As telas com árvores têm controles específicos. A árvore em si fica à esquerda com ações abaixo. Clique em um item na árvore para exibir as opções.

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, e a etapa do assistente contendo dados inválidos também é marcada
- A opção **Concluir** não está disponível até que todos os dados de entrada estejam corretos.



Tela de login

Recomendamos fazer login no ESET PROTECT via ESET Business Account. Do ESET Business Account você pode abrir o ESET PROTECT diretamente.. Este é o método de login recomendado porque assim você estará logado no ESET Business Account e ESET PROTECT simultaneamente. Embora também seja possível entrar no ESET PROTECT diretamente do login ESET PROTECT, você pode ter problemas com determinadas funções que exigem que você tenha entrado no ESET Business Account.

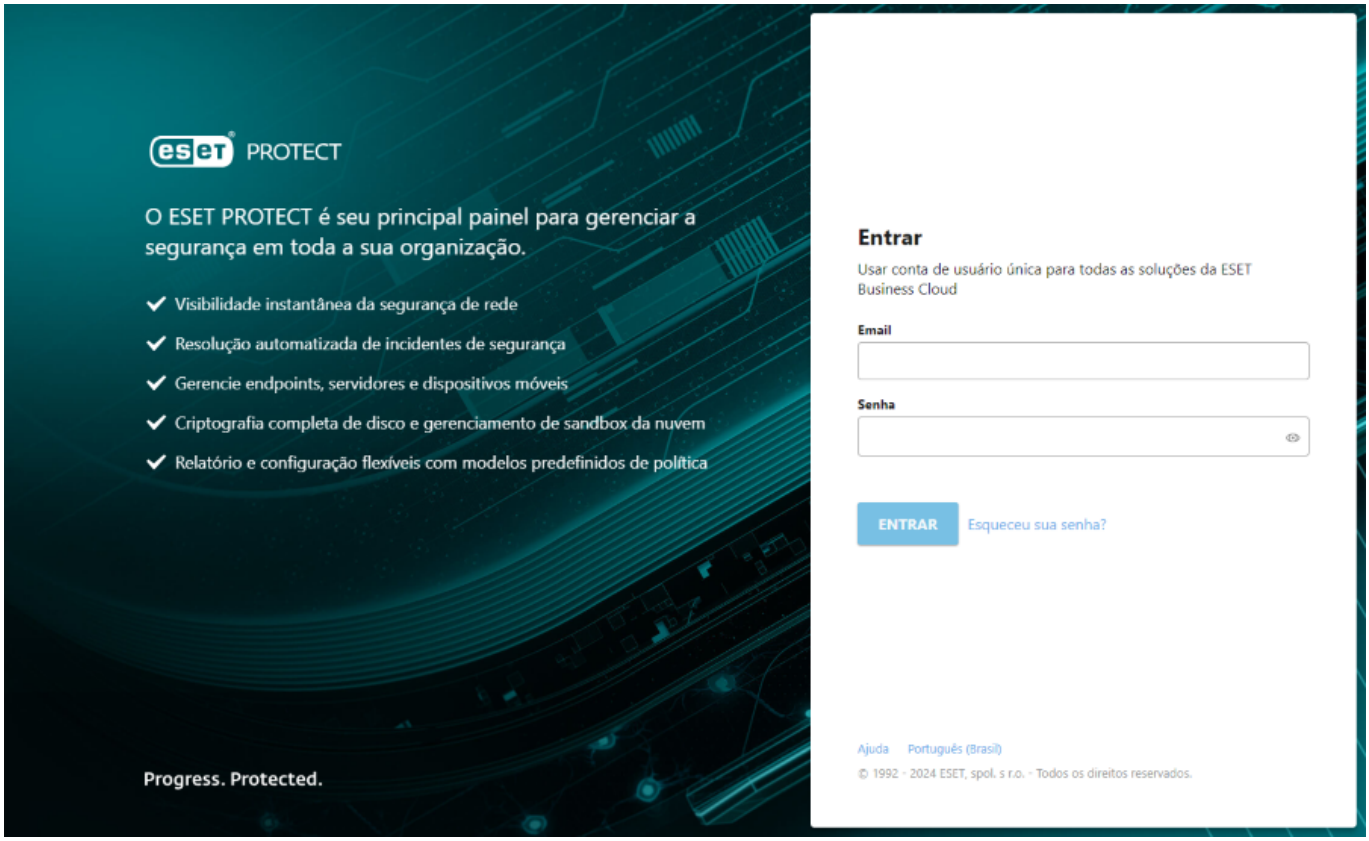
Credenciais de login ESET Business Account (nome de usuário e senha) são usadas para ambos os métodos mencionados acima.

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.

O idioma da tela de login e do Console Web ESET PROTECT pode ser alterado em ESET Business Account **Configurações do usuário** > **Idioma**.

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 configuração inicial da sua instância ESET PROTECT e seu idioma não pode ser alterado.

Senha esquecida permite a você recuperar uma senha esquecida em sua conta.



Gerenciamento de sessão e medidas de segurança:

Bloqueio de login do endereço IP

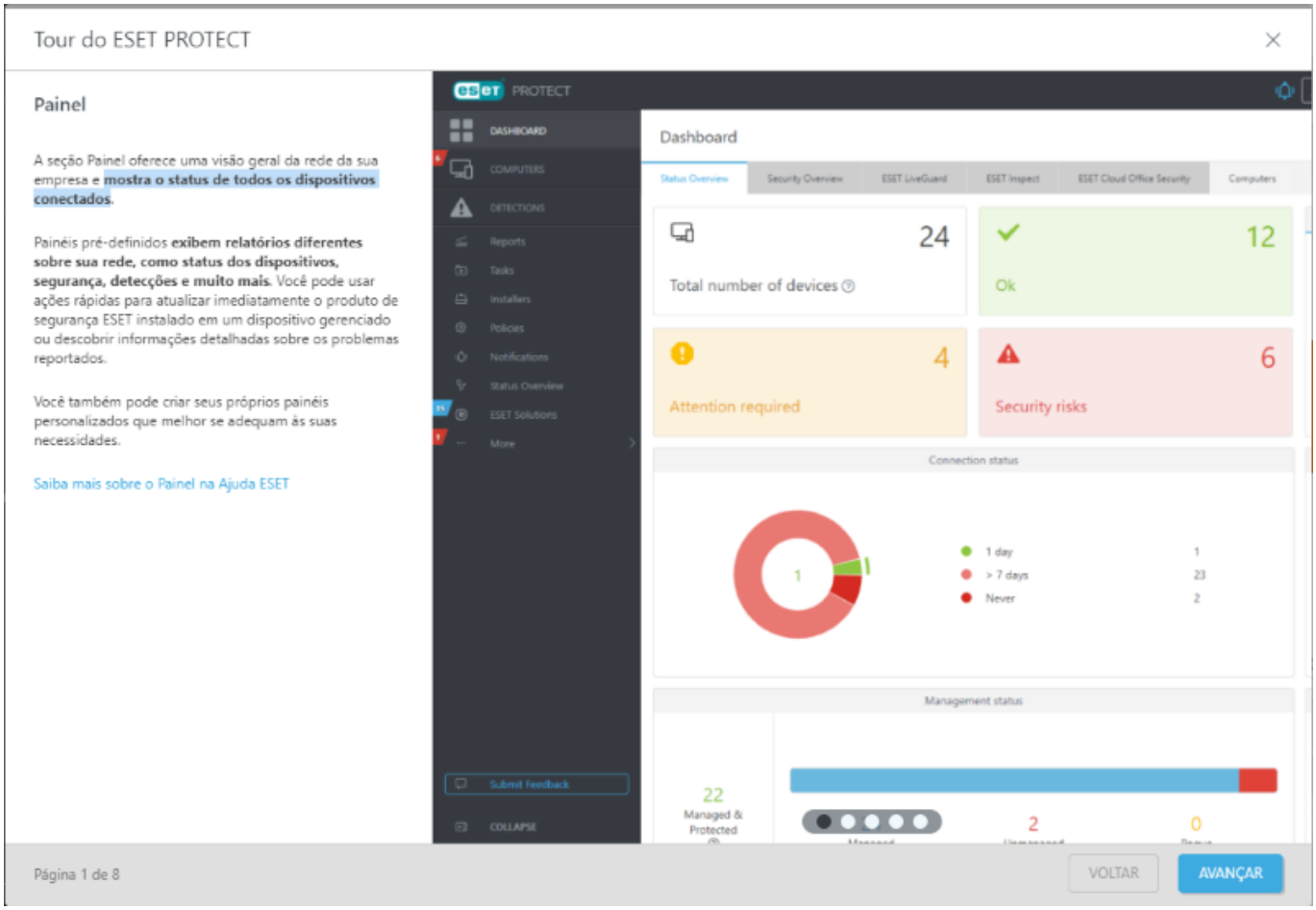
Depois de 10 tentativas mal sucedidas de entrar do mesmo endereço IP (por exemplo, usando credenciais de login incorretas), outras tentativas de entrar feitas por esse endereço IP serão bloqueadas temporariamente. Depois de 15 minutos, entre usando as credenciais corretas. O bloqueio de endereço IP em tentativas de login não afeta sessões existentes.

Tour ESET PROTECT

Quando você entrar no Web Console pela primeira vez, o **Tour do 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 **Tour do ESET PROTECT** 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 **Tour do ESET PROTECT**. O console web ESET PROTECT será aberto. O **Tour do ESET PROTECT** não vai aparecer na próxima vez que você entrar no Web Console ESET PROTECT.

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

Configurar proteção

A configuração a seguir é válida apenas para usuários ESET Business Account com ESET PROTECT.

Quando você entrar no Web Console, o assistente **Configurar sua proteção** aparece. Você pode configurar facilmente configurações de segurança específicas globalmente por toda a rede sem usar políticas ou grupos dinâmicos.

Opcionalmente, você pode abrir o assistente em:

- **Links rápidos** > clique em **Configurar proteção**.
- **Computadores** > clique no ícone de engrenagem ao lado de **Todos** em Grupos > clique em **Configurar proteção**.
- **Políticas** > clique na política **Configuração da proteção – através da configuração de proteção** > clique em **Configurar proteção**.
- **Visão geral do status** > clique no bloco **Componentes e produtos de segurança ESET** > clique no botão **Configurar proteção** .

Você precisa dos seguintes direitos de acesso para exibir o assistente de **Configuração da proteção**:
- Acesso de leitura – todo o grupo estático
- Acesso de leitura – Políticas

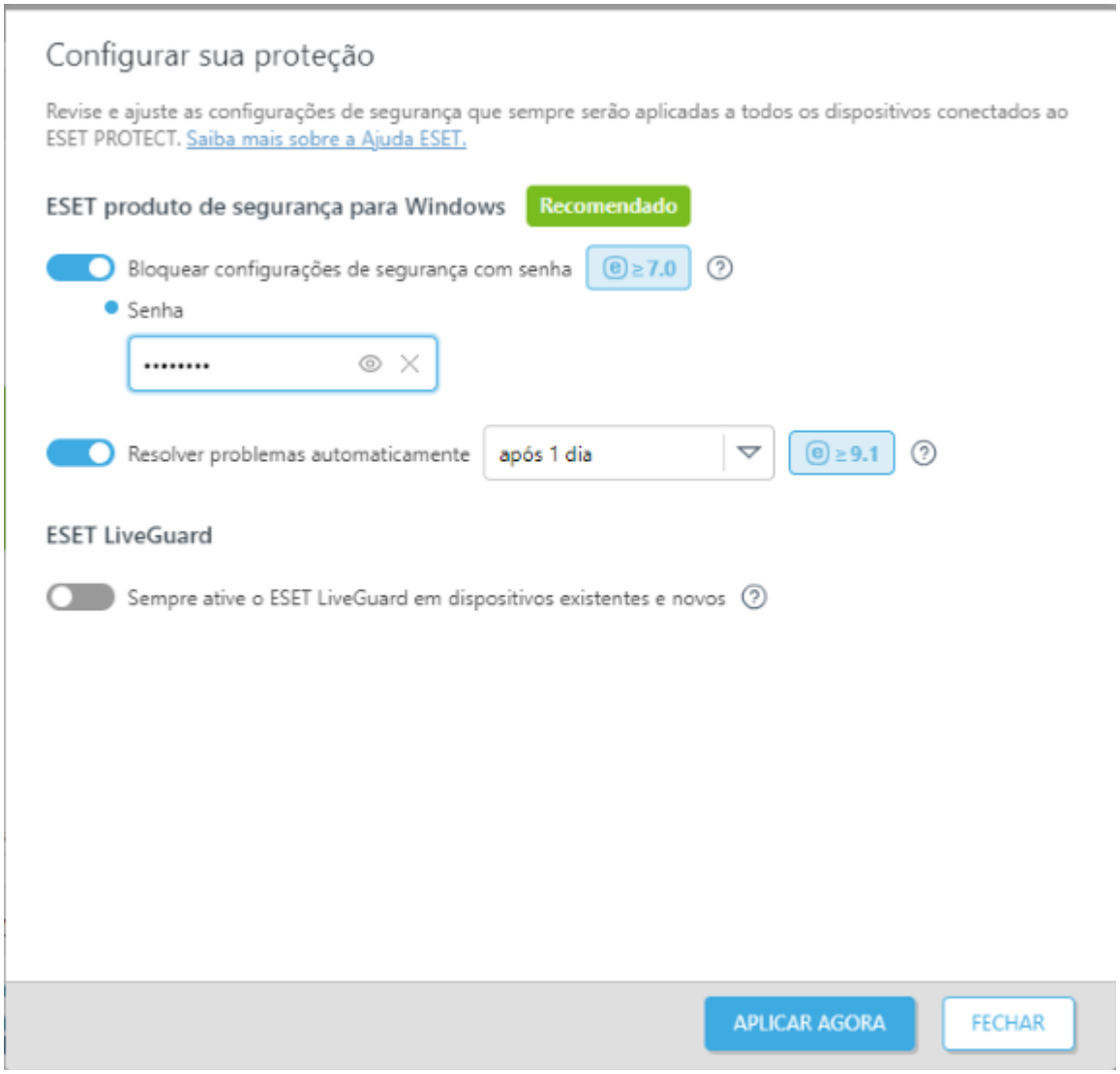
Você precisa dos seguintes direitos de acesso para editar o assistente de **Configuração da proteção**:
ESET produto de segurança para Windows parte:
- Acesso de uso – todo o Grupo estático
- Acesso de gravação – Políticas

Se você não tiver os direitos de acesso necessários, o **produto de segurança ESET para Windows** será desativado.
ESET LiveGuard parte:
- Acesso de uso – todo o Grupo estático
- Acesso de uso – licenças
- Acesso de gravação – tarefa do cliente de ativação do produto

Se você não tiver os direitos de acesso necessários, a parte **ESET LiveGuard** será desativada.
Se você não tiver a licença ESET LiveGuard Advanced, a parte **ESET LiveGuard** não estará disponível.

Quando sua licença ESET LiveGuard Advanced expirar, suas configurações para implantação automática serão armazenadas, mas não serão exibidas. Quando você renova sua licença, suas configurações são ativadas e exibidas novamente.

O assistente solicita que você aumente o nível de segurança para os dispositivos conectados ao ESET PROTECT.



ESET produto de segurança para Windows

1. Ative as **configurações de bloqueio de segurança com senha** para criar uma senha que impede os usuários finais de alterarem as políticas nos dispositivos conectados sem saber a senha.

A configuração é compatível com:
- ESET Endpoint Security para Windows 7.0 e versões posteriores:
- ESET Server Security for Microsoft Windows Server, ESET File Security for Microsoft Windows Server
- ESET Mail Security for Microsoft Exchange Server
- ESET Mail Security for IBM Domino
- ESET Security for Microsoft SharePoint Server

2. Digite uma senha com no mínimo 8 caracteres em **Senha**.

A senha criada é sempre aplicada automaticamente a todos os seus dispositivos conectados. Lembrar a senha. Se você esquecer a senha, poderá substituí-la por uma nova do ESET PROTECT, mas não poderá recuperar a senha anterior.

3. Ative **Resolver problemas automaticamente** para ativar a reinicialização automática dos dispositivos conectados necessários depois da atualização de um produto de segurança ESET.

Se um usuário final ou administrador não resolver essa reinicialização manualmente até um intervalo de tempo definido, o dispositivo será reiniciado automaticamente.

A configuração é compatível no ESET Endpoint Security para Windows 9.1 e versões posteriores. Ela não está disponível para produtos do servidor.

4. Selecione um intervalo de tempo para reinicialização automática do menu suspenso:

- Não foi possível adiar
- Depois de 1 a 5 horas
- Após 1 – 30 dias

ESET LiveGuard

5. Ative **Sempre ativar o ESET LiveGuard em dispositivos existentes e novos** para ativar a implantação automática do ESET LiveGuard Advanced em dispositivos existentes e recém-conectados com um produto de segurança ESET compatível instalado.

Recomendamos selecionar **Proteção ideal** para atribuir novas políticas com a proteção ideal. Você pode alterar sua seleção também na seção **ESET LiveGuard Advanced** em Soluções ESET.

6. Clique em **Aplicar agora** para aplicar as configurações de segurança.

Você pode ver as configurações em **Políticas** > **Configuração da proteção – via configuração da proteção**. Não é possível editar ou remover essas políticas, mas você pode alterar a atribuição delas (por padrão, elas são atribuídas ao Grupo estático **Todos**).

Desativar configurações

Você pode desativar as configurações com a alternância .

Se você desativar **Bloquear configurações de segurança com senha**, isso vai substituir as políticas atuais de senha nos seus dispositivos conectados. Se uma senha protegia as configurações de segurança nesses dispositivos, a senha não será mais necessária.

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:

- **Claro (padrão)**
- **Escuro**
- **Tema do sistema operacional** – a cor do Web Console corresponde à cor do sistema operacional.

Selecione o tema no menu suspenso:

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

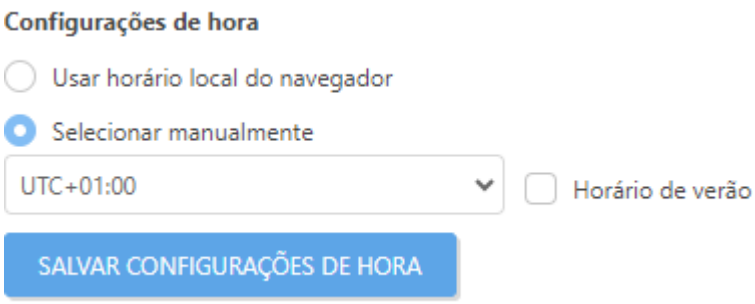
Configurações de hora

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.

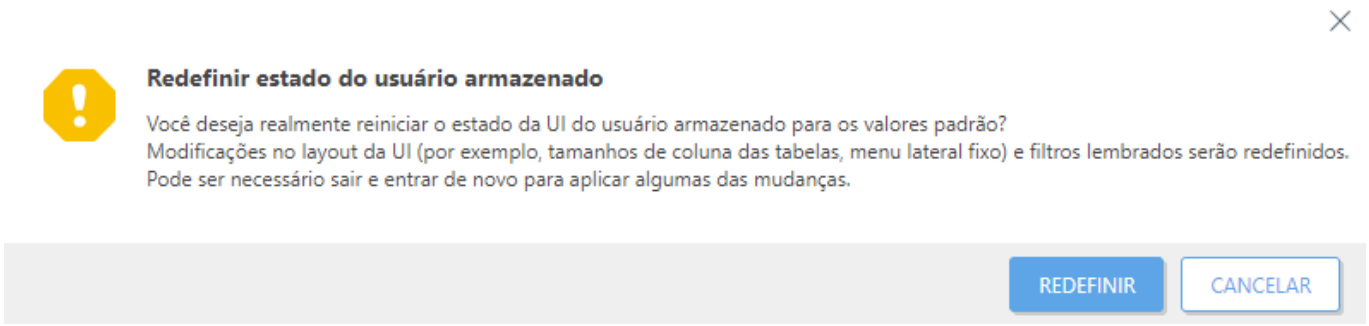


Em alguns casos, a opção de usar um fuso horário diferente será disponibilizada. Ao configurar um acionador, o fuso horário do Web Console ESET PROTECT é usado por padrão. Alternativamente, você pode selecionar a caixa de seleção **Usar horário local do destino** para usar o fuso horário local do dispositivo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

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

Estado do usuário armazenado

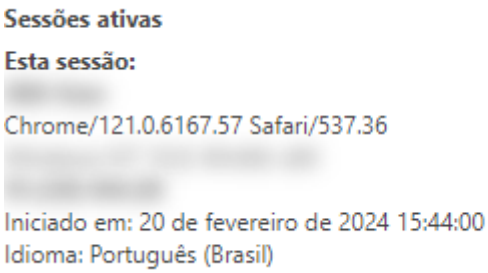
Você pode redefinir o estado da interface do usuário armazenada do usuário para o padrão clicando em **Redefinir estado do usuário armazenado**. Isso inclui o Tour do ESET PROTECT, tamanhos das colunas da tabela, filtros lembradas, menu lateral fixado, etc.



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.
- 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**.

Filtros e personalização de layout

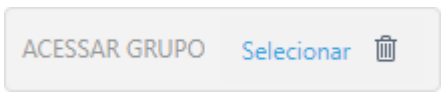
O console web ESET PROTECT permite a você personalizar o layout dos itens exibidos nas seções principais (por exemplo, **Computadores**, **Tarefas** etc.) de várias formas:

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.

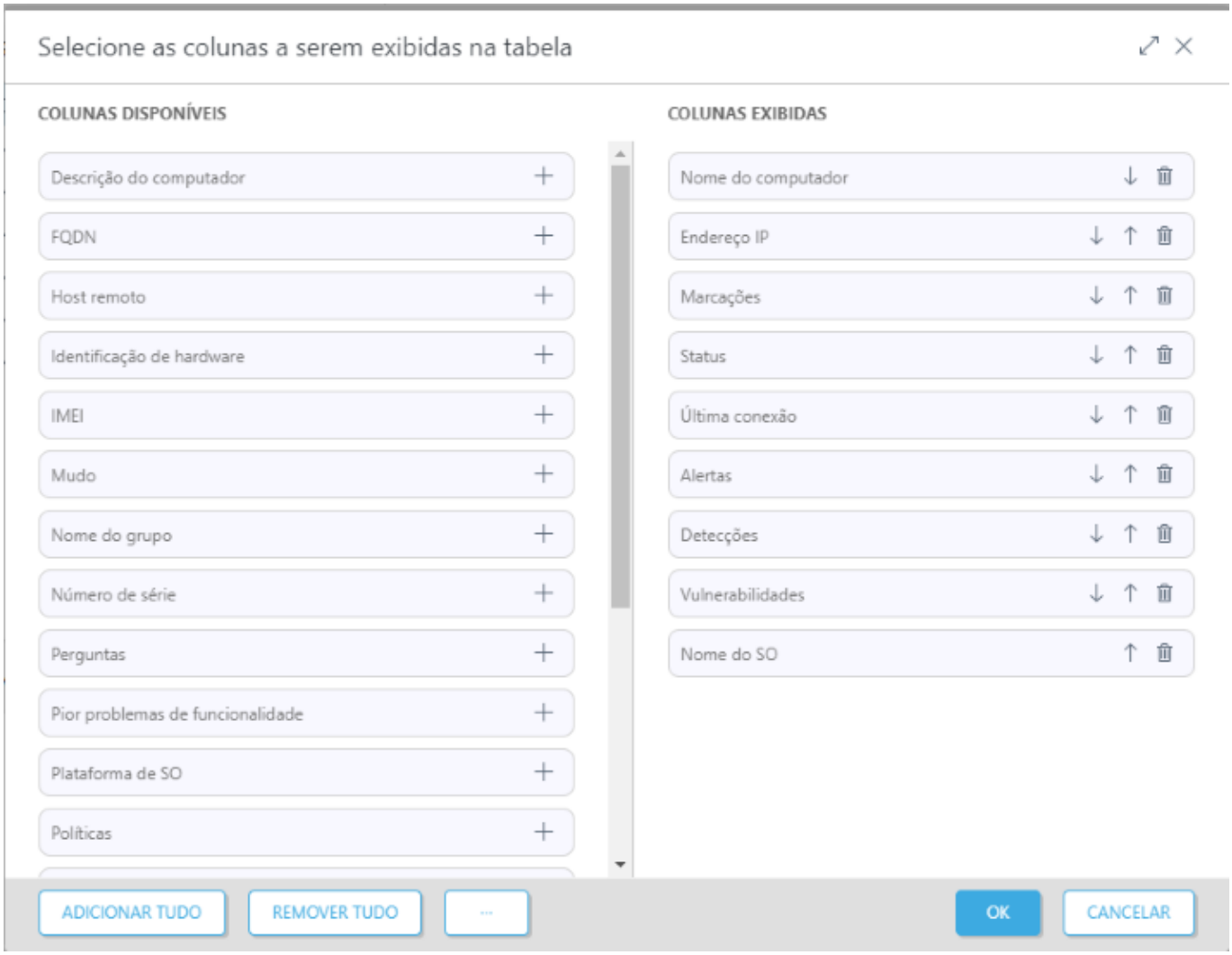
Para classificar por uma única coluna, clique no cabeçalho da coluna para classificar as linhas da tabela com base nos dados na coluna selecionada.

- 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.

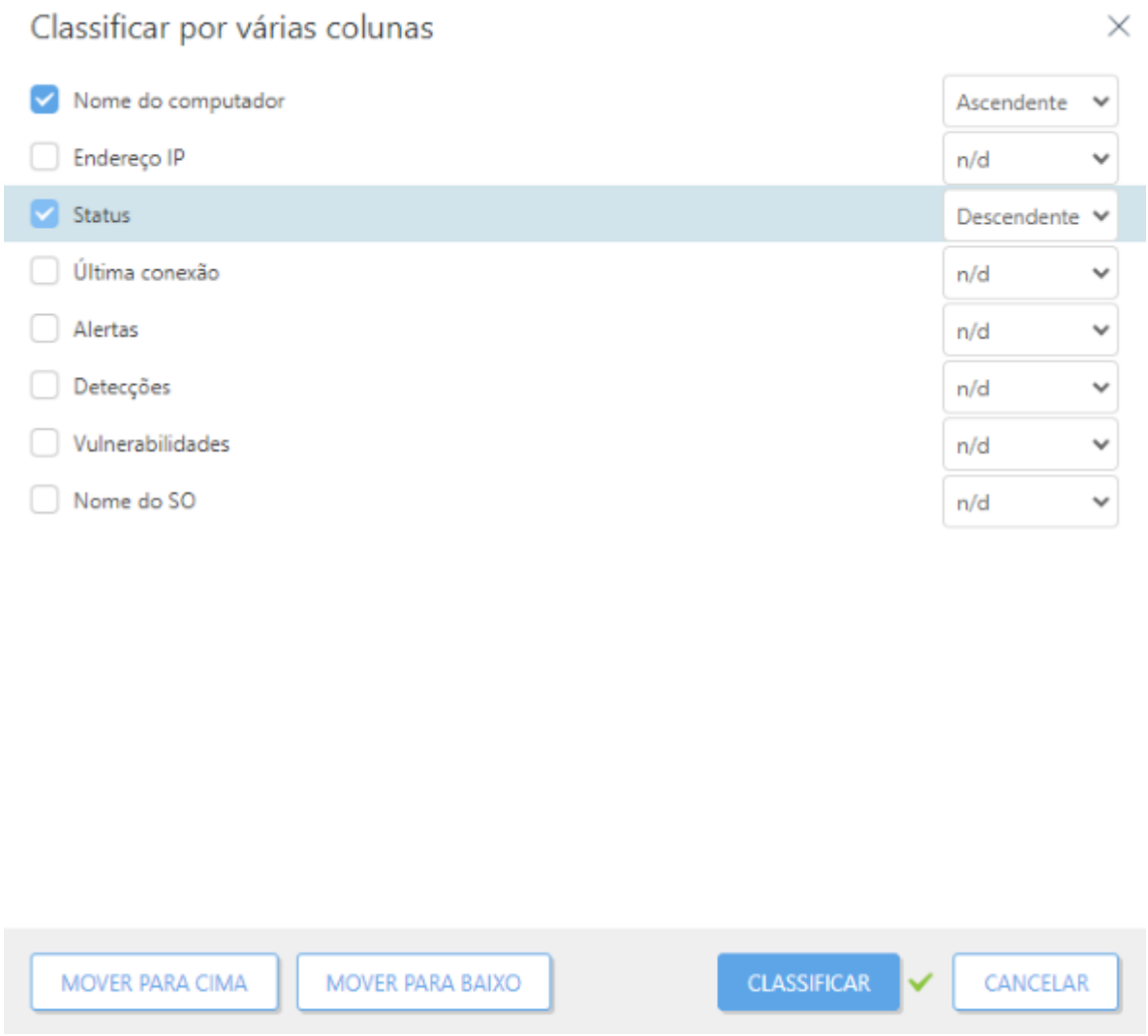
Classificação de tabela

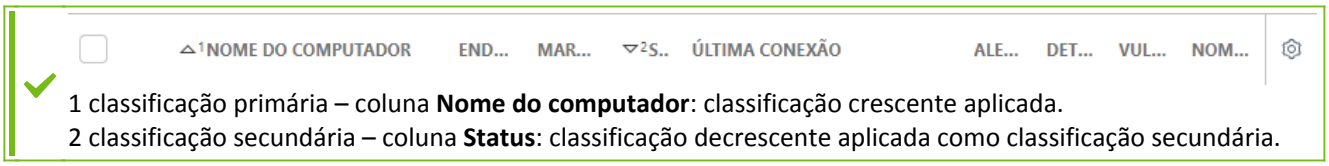
• **Redefinir classificação** – redefine a classificação da coluna.

• **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.





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:

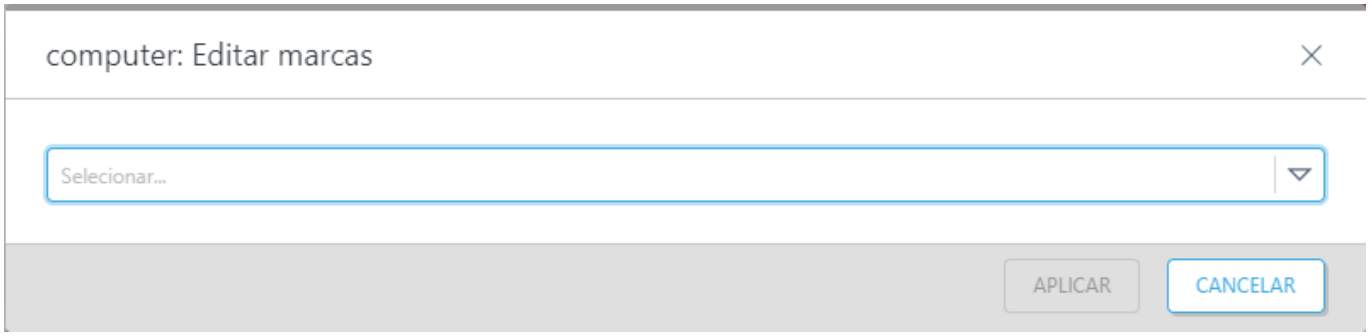
Permissões para gerenciamento de marcações

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.

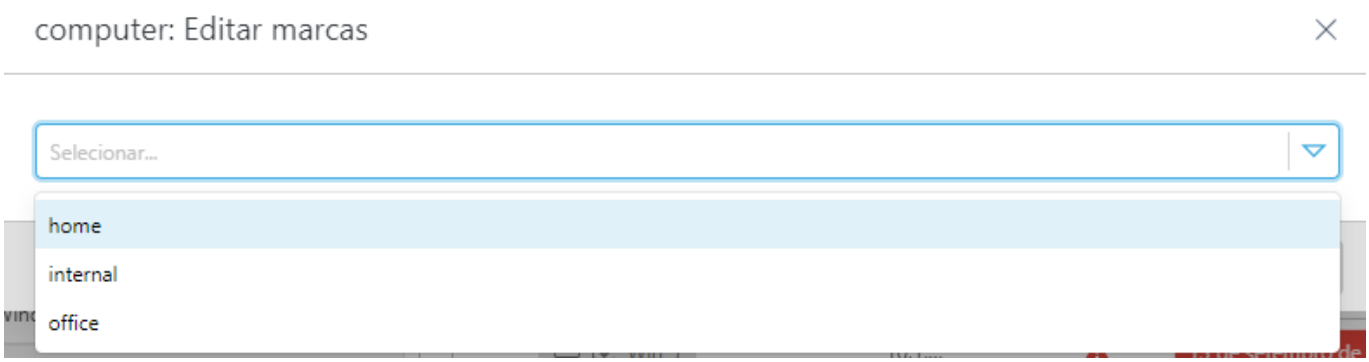
Atribuir marcações

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**:

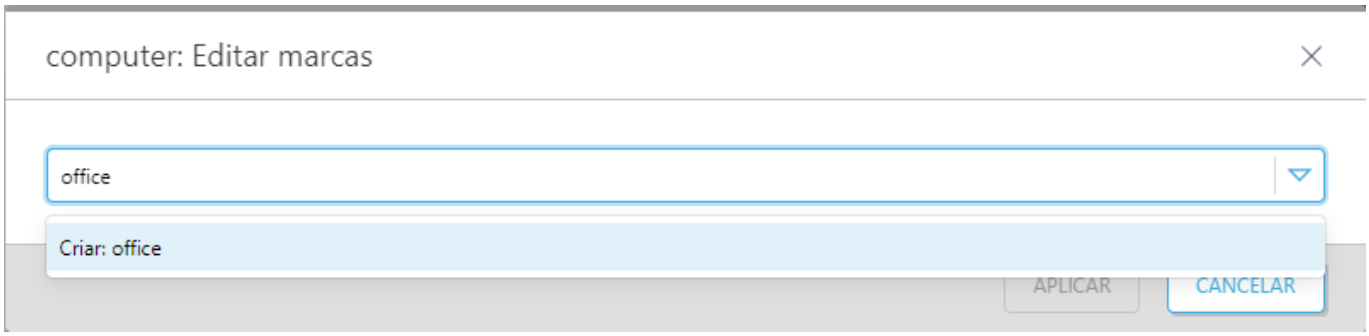


Para atribuir marcações já existentes, clique no campo de digitação em uma marcação da lista e clique em **Aplicar**.



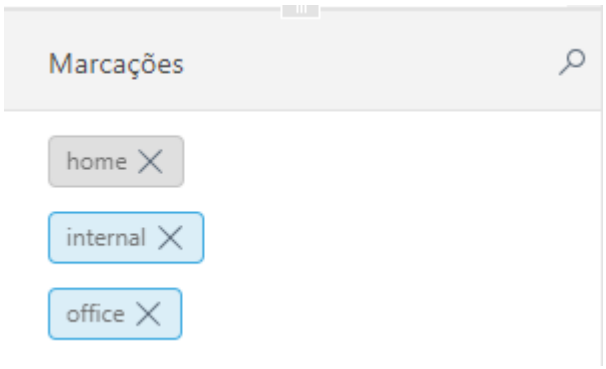
Criar uma nova marcação

Para criar uma nova marcação, digite o nome da marcação, selecione **Criar "tag_name"** e clique em **Aplicar**. Não é possível editar o nome de um sinalizador existente.



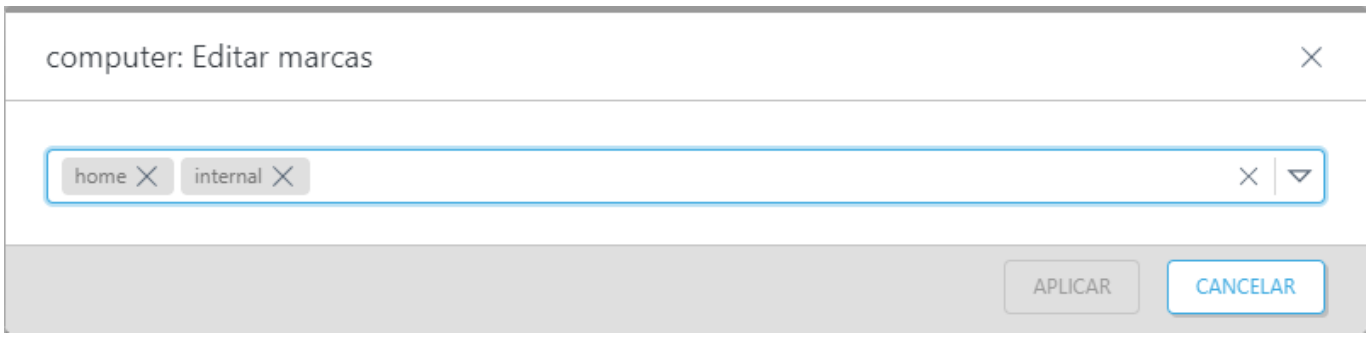
Filtrar objetos por marcações

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



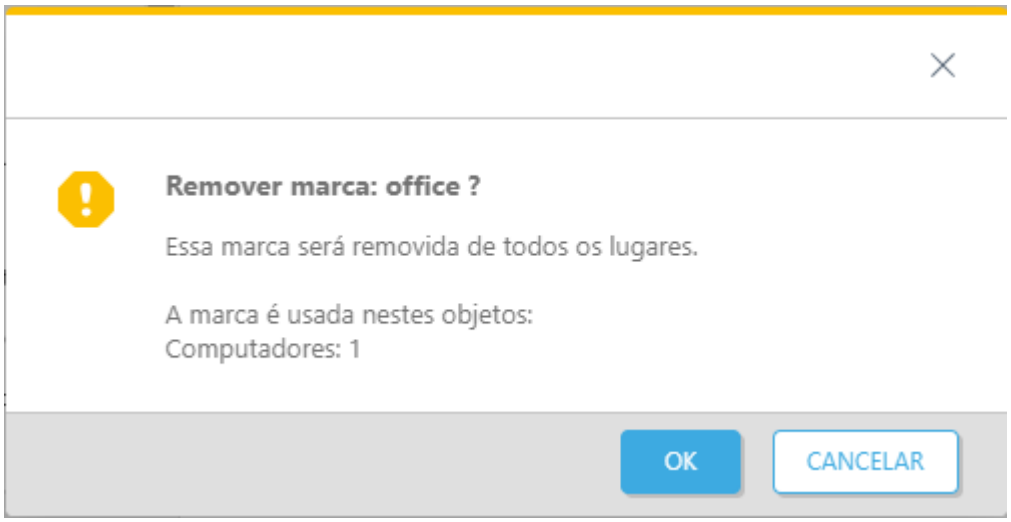
Cancelar atribuição de marcações

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**.

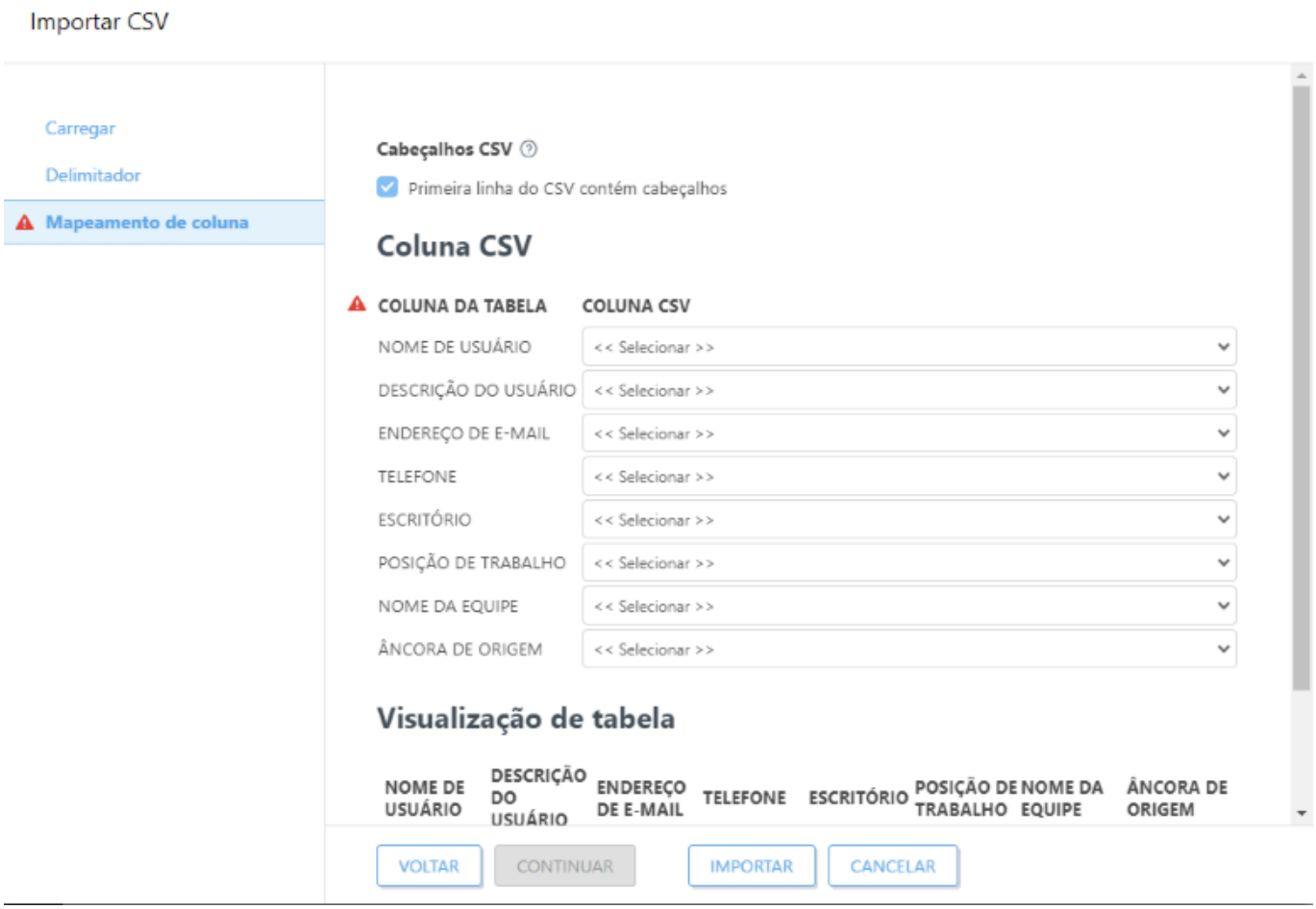
2.**Carregar** – clique em **Escolher arquivo** e procure o arquivo *.csv* (com a codificação UTF-8) que você gostaria de **Carregar**.

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

Como o ESET PROTECT está hospedado na nuvem, a maioria dos erros que podem acontecer durante o login podem ser resolvidos seguido essas etapas gerais de solução de problemas:

- Limpe o cache do navegador e atualize a página de login.
- Se o problema persistir, aguarde alguns minutos e tente efetuar login novamente ou tente um navegador diferente (navegadores compatíveis).
- Se o problema não for resolvido entre em contato com o Suporte ESET.

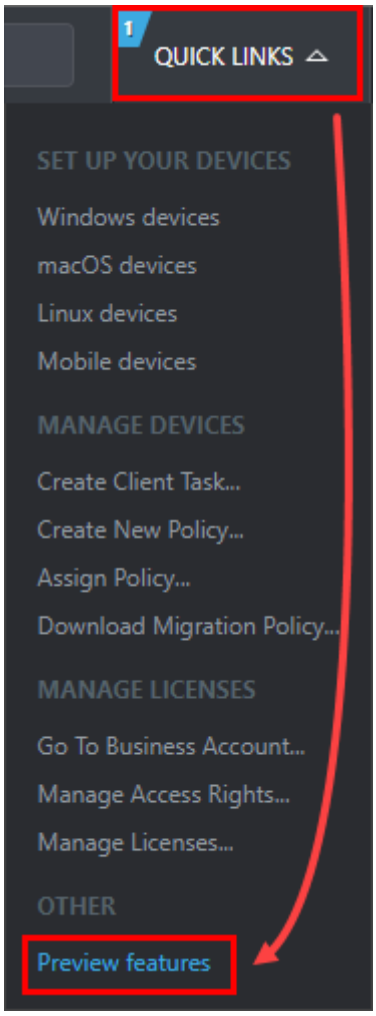
A tabela abaixo fornece algumas informações sobre as massagens e status de erros de login do console Web mais comuns, o que elas significam e algumas etapas adicionais de solução de problemas:

Mensagem de erro	Causa possível
⚠ Falha no login: A comunicação do seu endereço foi bloqueada temporariamente	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 15 minutos, entre usando as credenciais corretas.
⚠ Falha no login: Erro de autenticação ⚠ Falha no login: Falha de autenticação no servidor	O servidor recebeu um token de autenticação danificado ou incompleto. Certifique-se de estar usando as credenciais de login corretas e de que sua conexão com a página de login é segura. Se o problema continuar, tente limpar os cookies.
⚠ Falha no login: Falha na conexão com estado 'Não conectado' ⚠ Falha no login: Erro de comunicação ⚠ Falha no login: Tempo limite de conexão	Verifique a conexão de rede e as configurações de firewall para se certificar de que o seu dispositivo pode chegar ao Console Web ESET PROTECT.
⚠ Falha no login: O usuário não tem direitos de acesso atribuídos	A conta do usuário na qual você está tentando fazer login não tem nenhum direito de acesso atribuído. Faça login como administrador e edite a conta de usuário, atribuindo as permissões apropriadas para esse usuário. Se você não tiver acesso à conta do administrador, entre em contato com o administrador com essa solicitação.
O JavaScript está desativado. Ative o JavaScript no seu navegador.	JavaScript é necessário para que a página de login funcione corretamente. Ative o JavaScript ou atualize seu navegador da web.
Você não visualiza a tela de login ou quando a tela de login aparecer ela parece estar constantemente sendo carregada.	Verifique a conexão de rede e as configurações de firewall para se certificar de que o seu dispositivo pode chegar ao Console Web ESET PROTECT. O Portal de Status ESET exibe o status atual dos serviços de nuvem da ESET, interrupções programadas e incidentes passados. Se você estiver enfrentando um problema com um serviço suportado pela ESET e não o vir listado no Portal de Status, entre em contato com o Suporte Técnico ESET. As equipes de monitoramento verificam possíveis problemas internamente e os incidentes confirmados são publicados e atualizados manualmente para manter alta credibilidade e precisão. Portanto, eles aparecem no Portal de Status com um pequeno atraso. Incidentes com curta duração podem não ser publicados se forem resolvidos antes de serem confirmados manualmente.
"Ocorreu um erro inesperado" ou "Ocorreu uma exceção que não foi pega"	Este erro pode ocorrer quando você está acessando o Console Web ESET PROTECT de um navegador que não é compatível com o Console web ESET PROTECT, veja os navegadores da web compatíveis.
SEC_ERROR_INADEQUATE_KEY_USAGE (apenas Mozilla Firefox).	O Mozilla Firefox tem um depósito de certificado corrompido.

Recursos de visualização

Recursos de visualização permitem que o usuário experimente novos recursos individuais no ESET PROTECT.

Você pode acessar o menu **Recursos de visualização** do menu suspenso **Links rápidos**.



No menu de recursos de visualização, o administrador pode encontrar todos os recursos de visualização disponíveis com uma breve descrição de cada funcionalidade de recursos de visualização. O administrador pode então **Ativar** ou **Desativar** cada um dos recursos de visualização e também **Enviar feedback** para cada um dos recursos de visualização disponíveis.

Depois da ativação, o recurso de visualização está disponível instantaneamente no console de gerenciamento.

Os recursos de visualização mais recentes disponíveis no seu console de gerenciamento são:

Não há recursos de Visualização disponíveis para o lançamento atual.

Sincronizar o ESET PROTECT com o Active Directory

Use o **Escaneador ESET Active Directory** para sincronizar os computadores e usuários Active Directory com o Web Console ESET PROTECT.

A ESET atualiza regularmente o Escaneador Active Directory para melhorar sua funcionalidade. Você pode encontrar mais detalhes no registro de alterações.

Pré-requisitos

• Execute o Escaneador Active Directory como um usuário Active Directory em um computador conectado ao Active Directory.

• Sistemas operacionais compatíveis (compatibilidade com o HTTP/2): Windows 10, Windows Server 2016 e versões posteriores.

• Faça o download e instale o .NET Core Runtime.

• Preparar arquivo de configuração do usuário (*config.json*) para a sincronização do usuário Active Directory. *config.json* está incluído no arquivo zip do Escaneador **Active Directory**.

• Permissão de direitos de acesso do usuário para o **Token de acesso do Escaneador AD**: **Gravação**

Usando o Escaneador Active Directory

1. No Web Console ESET PROTECT, crie o script de implantação GPO do Agente.

2. Entre em um computador no seu Active Directory com uma conta de usuário Active Directory. Certifique-se de que ele cumpre com os pré-requisitos listados acima.

3. Faça o download do escaneador do Active Directory mais recente no computador.

4. Descompacte o arquivo do download.

5. Faça o download do script de implantação GPO do Agente (criado na etapa 1) e copie-o para a pasta *ActiveDirectoryScanner* (uma pasta que contém todos os arquivos do Escaneador do Active Directory).

Sincronização de computador do Active Directory

1. No Web Console ESET PROTECT, vá para **Computadores** e selecione o grupo estático onde deseja sincronizar a estrutura do Active Directory.
2. Clique no ícone de **engrenagem** ao lado do grupo estático selecionado e selecione **Escaneador** do **Active Directory**.
3. Clique em **Gerar** para obter o token de acesso.

Cada grupo estático tem um token. O token identifica o grupo estático onde o Active Directory será sincronizado.
Para invalidar o token atual por razões de segurança, clique em **Regenerar** para criar um novo token. Se a sincronização Active Directory com o ESET PROTECT já estiver sendo executada, a sincronização será interrompida depois da alteração do token de segurança. Você deve executar o Escaneador do Active Directory com o novo token para reabilitar a sincronização do Active Directory.
Para remover o token por motivos de segurança, clique em **Desativar token**. Para confirmar a desativação do token, clique em **Desativar**.

4. Execute o Escaneador do Active Directory (substitua `token_string` pelo token copiado na etapa anterior).

```
ActiveDirectoryScanner.exe --token token_string
```

Por padrão, o Escaneador Active Directory mais recente não sincroniza computadores Active Directory desativados. Para sincronizar computadores Active Directory desativados, use o parâmetro `--disabled-computers`:

```
ActiveDirectoryScanner.exe --token token_string --disabled-computers
```

5. Quando solicitado, digite a senha do usuário do Active Directory.
6. Depois do Escaneador do Active Directory concluir a sincronização, sua estrutura Active Directory (unidades organizacionais com computadores) aparecerá em **Computadores** no Web Console ESET PROTECT como Grupos estáticos com computadores.

Incluir ou excluir a estrutura da unidade organizacional

Para incluir ou excluir a estrutura da unidade organizacional, determine o caminho (por exemplo: `"Users/Bratislava/TechDepartment"`).
`"ExcludeByID"` funciona com `sid` por padrão.
Um exemplo da sintaxe:

```
"Include": [
    "path"
            ],
            "Exclude": [
    "path"
            ],
            "ExcludeByID": [
    "sid1", "sid2"...
            ],
```

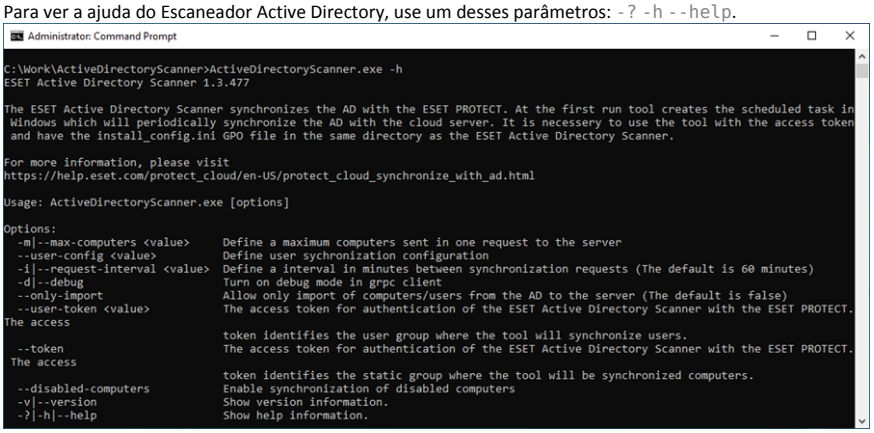
Exemplo: `"Include" "path" "Users/Bratislava/TechDepartment"` tem mais subunidades, você pode excluir qualquer subunidade com `"exclude" "path" "Users/Bratislava/TechDepartment/Test"`

O Escaneador do Active Directory cria uma tarefa de **Sincronização Active Directory** na Agenda de tarefas do Windows com um acionador de intervalo de repetição definido como 1 hora. Você pode ajustar o intervalo de sincronização Active Directory na Agenda de tarefas com base em sua preferência. Qualquer alteração futura na estrutura Active Directory será refletida no Web Console ESET PROTECT depois da próxima sincronização.

Limitações de sincronização do Active Directory:

- O Escaneador do Active Directory sincroniza apenas unidades organizacionais do Active Directory que contêm computadores com nomes DNS. Unidades organizacionais que não contenham nenhum computador não serão sincronizadas.
- Se o nome da unidade organizacional mudar no Active Directory, um novo grupo estático com o novo nome será criado no Web Console ESET PROTECT depois da próxima sincronização. O Grupo estático correspondente ao nome da unidade organizacional anterior continuará a ser o Web Console ESET PROTECT e será deixado em branco, os computadores incluídos vão mudar para o grupo estático com o novo nome.
- Se você remover uma unidade organizacional no Active Directory, todos os computadores nela serão removidos do Grupo estático correspondente no Web Console ESET PROTECT.
- Se você excluir um computador Active Directory sincronizado do Web Console ESET PROTECT, ele não será exibido novamente depois da próxima sincronização, mesmo se ele continuar no Active Directory.

Para ver a ajuda do Escaneador Active Directory, use um desses parâmetros: `-? -h --help`.



Para solucionar os problemas, veja os relatórios localizados em *C:\ProgramData\ESET\ActiveDirectoryScanner\Logs*.

Se você remover um computador do Active Directory, o computador também será removido do Web Console ESET PROTECT.

Sincronização do Usuário do Active directory

1. No Web Console ESET PROTECT, vá para **Mais** > **Usuários do computador** e selecione o Grupo de usuários onde deseja sincronizar a estrutura do Active Directory.
2. Clique no ícone de **engrenagem** ao lado do Grupo usuário selecionado, selecione **Escaneador Active Directory** e copie o token de acesso gerado.
3. Clique em **Gerar** para obter o token de acesso.

Cada Grupo estático tem seu token. O token identifica o grupo estático onde o Active Directory será sincronizado.
Para invalidar o token atual por razões de segurança, clique em **Regenerar** para criar um novo token. Se a sincronização Active Directory com o ESET PROTECT já estiver sendo executada, a sincronização será interrompida depois da alteração do token de segurança. Você deve executar o Escaneador do Active Directory com o novo token para reabilitar a sincronização do Active Directory.
Para remover o token por motivos de segurança, clique em **Desativar token**. Para confirmar a desativação do token, clique em **Desativar**.

3. Execute o Escaneador do Active Directory (substitua `token_string` pelo token copiado na etapa anterior).

```
ActiveDirectoryScanner.exe --user-token token_string --user-config config.json
```

`--user-token` e `--token` podem ser usados simultaneamente. A ferramenta vai então sincronizar computadores e usuários.

As recomendações do arquivo de configuração do usuário (config.json)

Siga as recomendações de formatação para configurar o arquivo *config.json* (localizado na mesma pasta que *ActiveDirectoryScanner.exe*). Faça backup do arquivo antes de editá-lo (você pode fazer download de uma nova cópia novamente, se necessário).

- Remova os comentários, eles servem apenas como instruções.
- Use os campos `"Include"` e `"Exclude"` para especificar os grupos incluídos ou excluídos para sincronização.
- De acordo com as instruções no arquivo *config.json*, recomendamos identificar grupos usando o `objectGUID` em vez do `Distinguished Name`.
- Digite os valores `objectGUID` no seguinte formato:

```
"Include": [ "{objectGUID1}", "{objectGUID2}", ... ],
"Exclude": [ "{objectGUID3}", "{objectGUID4}", ... ],
```

- Substitua `{objectGUID}` pelos valores `objectGUID` reais dos grupos que você deseja incluir ou excluir. Cada `objectGUID` um deve estar no formato de uma cadeia hexadecimal cercada por chaves. Por exemplo, se você tiver dois grupos com valores `objectGUID` de `"12345678-1234-5678-1234-1234567890AB"` e `"98765432-4321-8765-4321-0987654321AB"`, a seção `Include` será da seguinte forma:

```
"Include": [ "{12345678-1234-5678-1234-1234567890AB}", "{98765432-4321-8765-4321-0987654321AB}" ],
```

- Para excluir um grupo com `objectGUID` `"55555555-5555-5555-5555-555555555555"`, a seção `Exclude` ficaria assim:

```
"Exclude": [ "{55555555-5555-5555-5555-555555555555}" ],
```

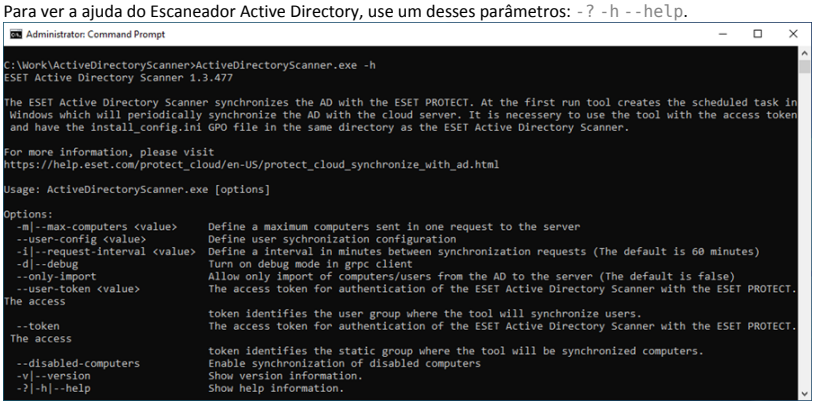
4. Quando solicitado, digite a senha do usuário do Active Directory.
5. Depois do Escaneador Active Directory concluir a sincronização, sua estrutura Active Directory (unidades organizacionais com computadores/usuários) aparecerá em **Computadores/Usuários do computador** como Grupos estáticos com computadores do Web Console ESET PROTECT e/ou **Grupos de usuários** com Usuários em **Usuários do computador**.

O Escaneador do Active Directory cria uma tarefa de **Sincronização Active Directory** na Agenda de tarefas do Windows com um acionador de intervalo de repetição definido como 1 hora. Você pode ajustar o intervalo de sincronização Active Directory na Agenda de tarefas com base em sua preferência. Qualquer alteração futura na estrutura Active Directory será refletida no Web Console ESET PROTECT depois da próxima sincronização.

Limitações de sincronização do Active Directory:

- O Escaneador do Active Directory sincroniza apenas unidades organizacionais do Active Directory que contêm usuários. Unidades organizacionais que não contenham nenhum usuário não serão sincronizadas.
- Se você remover uma unidade organizacional no Active Directory, todos os usuários nela serão removidos do Grupo de usuários correspondente no Web Console ESET PROTECT. Grupos sincronizados vazios também são removidos.
- Se você remover um usuário do Active Directory sincronizado do Web Console ESET PROTECT, ele não será exibido de novo depois da próxima sincronização, mesmo se ele continuar no Active Directory até que algumas das propriedades sincronizadas sejam alteradas no Active Directory de origem.

Para ver a ajuda do Escaneador Active Directory, use um desses parâmetros: `-? -h --help`.



Para fins de solução de problemas, veja os relatórios localizados no *C:\ProgramData\ESET\ActiveDirectoryScanner\Logs*.

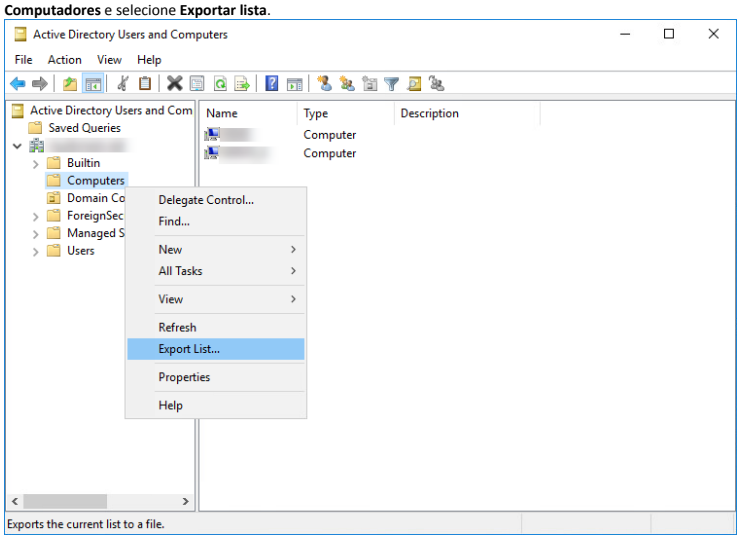
Soluções alternativas

Você também pode usar uma das soluções alternativas abaixo:
- Exportar a lista de computadores do Active Directory e importá-la para o ESET PROTECT
- Implantar o Agente ESET Management em computadores do Active Directory usando um Objeto de política de grupo

Exportar a lista de computadores do Active Directory e importá-la para o ESET PROTECT

Esta solução fornece apenas uma sincronização única do Active Directory e não sincroniza quaisquer alterações futuras do Active Directory.

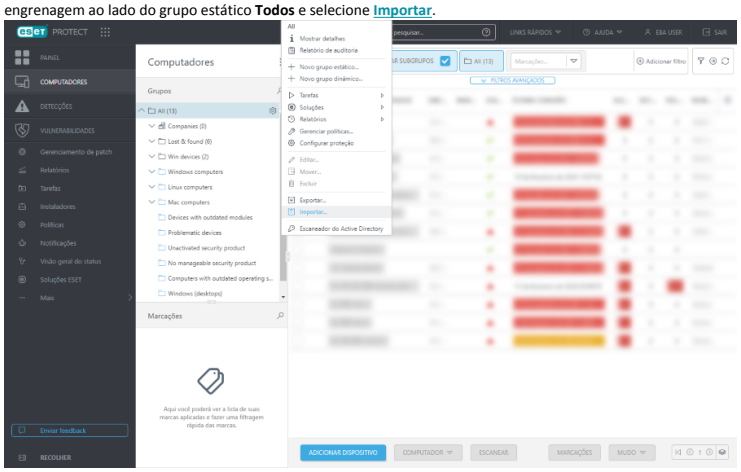
1. Exporte a lista de computadores do Active Directory. Você pode usar várias ferramentas, dependendo de como você gerencia o Active Directory. Por exemplo, abra os **Usuários e computadores** do **Active Directory** e, em seu domínio, clique com o botão direito do mouse em **Computadores** e selecione **Exportar lista**.



2. Salve a lista de computadores do Active Directory exportados como um arquivo *.txt*.
3. Modifique a lista de computadores para que seu formato seja aceitável para a importação ESET PROTECT. Certifique-se de que cada linha contém um computador e tem o formato a seguir:

```
\GROUP\SUBGROUP\Computer name
```

4. Salve o arquivo *.txt* atualizado com a lista de computadores.
5. Importe a lista de computadores do Active Directory para o Web Console ESET PROTECT. Clique em **Computadores** > clique no ícone de engrenagem ao lado do grupo estático **Todos** e selecione **Importar**.



Implantar o Agente ESET Management em computadores do Active Directory usando um Objeto de política de grupo

1. Crie o Script de implantação GPO do Agente.
2. Implante o Agente ESET Management usando um Objeto de política de grupo (GPO). Comece na etapa 3 em nosso artigo da Base de conhecimento.
3. Depois da implantação bem sucedida do Agente ESET Management via GPO, o Agente ESET Management será instalado em computadores do Active Directory e os computadores vão aparecer na tela ESET PROTECT Web Console **Computadores**.
Sempre que você adicionar um novo computador ao Active Directory no futuro, ele vai aparecer na tela ESET PROTECT Web Console **Computadores**.

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 PROTECTAssistente 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 importar sua licença no ESET Business Account 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** > **Ativar produto de segurança** para ativar 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 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 Servidor ESET PROTECT. Todos os relatórios dos Endpoints ou outros produto de segurança ESET são enviados ao Servidor ESET PROTECT.

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

O O **ESET Push Notification Service** (EPNS) serve para receber mensagens do ESET PROTECT, se o ESET PROTECT 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 Servidor ESET PROTECT e os Agentes ESET Management.

Detalhes da conexão

Para configurar sua rede local para permitir a comunicação com o EPNS, os Agentes ESET Management precisam ser capazes de se conectar ao servidor EPNS. Se você não conseguir estabelecer uma conexão com o EPNS para seus Agentes, apenas as Chamadas para despertar serão afetadas. Certifique-se de que o firewall permite a conexão com o servidor EPNS (consulte a tabela abaixo).

Protocolo de segurança criptográfico	TLS – a versão TLS mais recente compatível com o sistema operacional do computador gerenciado
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).

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 Servidor ESET PROTECT. 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.

- Somente os sistemas operacionais Windows são compatíveis.

- Você pode usar o ESET Full Disk Encryption em um ambiente virtual, mas o ESET Full Disk Encryption não deve ser clonado

- Dispositivos móveis gerenciados via Cloud 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 é capaz de analisar o hardware de forma confiável

- Ver a lista de configurações compatíveis:

- Citrix PVS 7.15+ com máquinas físicas
- Citrix PVS 7.15+ com máquinas virtuais no Citrix XenServer 7.15+
- Citrix PVS 7.15+ e Citrix XenDesktop com Citrix XenServer 7.15+
- Serviços de criação de máquina Citrix
- (sem PVS) Citrix XenDesktop com Citrix XenServer 7.15+
- VMware Horizon 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, sinalize o computador Mestre em Detalhes do computador > **Virtualização** antes de criar o pool, em seguida selecione **Marcar como Mestre para clonagem** > **Fazer correspondência com o computador existente**

- Se o computador mestre for removido do ESET PROTECT, a recuperação de sua identidade (clonagem) será proibida e novas máquinas do pool obterão uma nova identidade a cada vez (uma nova entrada de máquina será criada no Web Console)

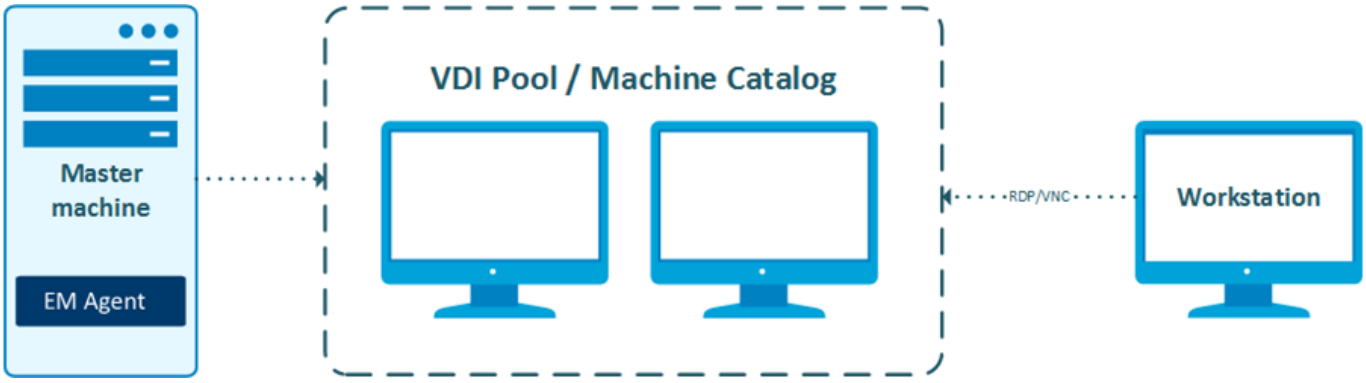
- Quando uma máquina do pool VDI conecta pela primeira vez, é obrigatório ter um intervalo de conexão de 1 minuto. Depois das primeiras replicações o intervalo de conexão é herdado do mestre

- 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.

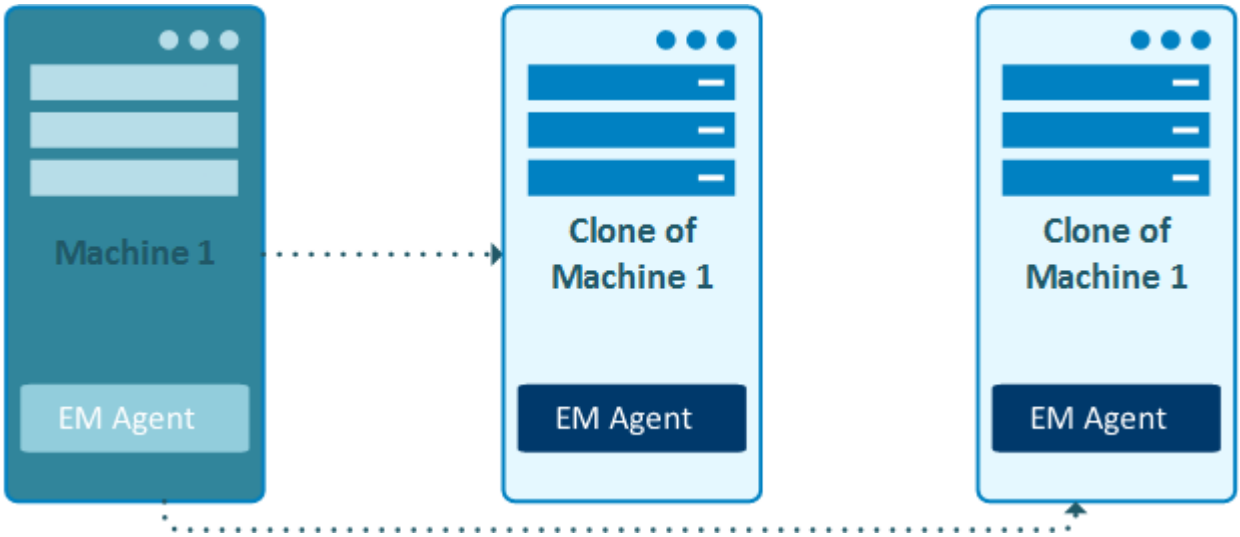
Grupo padrão para máquinas VDI

Novas máquinas clonadas do Mestre aparecem no grupo estático definido no **Grupo doméstico de computadores clonados** na janela Mestre para clonagem.



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:

Criar um novo computador

Criar uma nova máquina no ESET PROTECT depois de cada implantação de imagem.

Quando um clone é detectado, o sistema pode reagir de duas maneiras:

- Manualmente – resolva cada novo computador manualmente em Perguntas e selecione **Criar um novo computador todas as vezes**.
- Automaticamente – sinalize a máquina Mestre antes de clonar e selecione **Marcar como Mestre para clonagem** > **Criar novos computadores**.

Combinar com computador existente

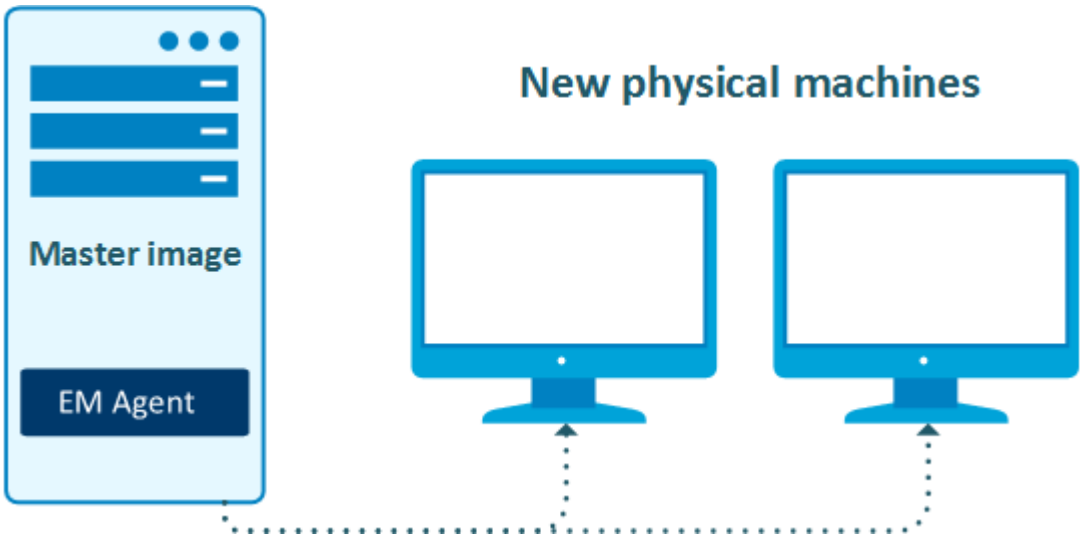
Se a imagem for instalada novamente em uma máquina com histórico anterior no ESET PROTECT (que já tinha o Agente ESET Management instalado), essa máquina é conectada à sua identidade anterior no ESET PROTECT. Se não houver uma correspondência de identidade anterior, o sistema cria uma nova máquina no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

Quando um clone é detectado, o sistema pode reagir de duas maneiras:

- Manualmente – resolva cada novo computador manualmente em Perguntas e selecione **Corresponder com um computador existente todas as vezes**.

- Automaticamente – sinalize a máquina Mestre antes de clonar e 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 de atualizar ou reinstalar qualquer componente ESET na máquina mestre.



Replicação paralela

O Servidor ESET PROTECT 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 de um clique disponível no alerta – os computadores serão divididos e a detecção de hardware será desativada permanentemente

- Em casos raros, até mesmo computadores com detecção de hardware desligado podem entrar em conflito – se isso acontecer, a tarefa Redefinir agente clonado é a única opção

- Execute a tarefa Redefinir agente clonado na máquina. Isso evitará que você precise desabilitar a detecção de hardware

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 Servidor ESET PROTECT detectar um dos seguintes:

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

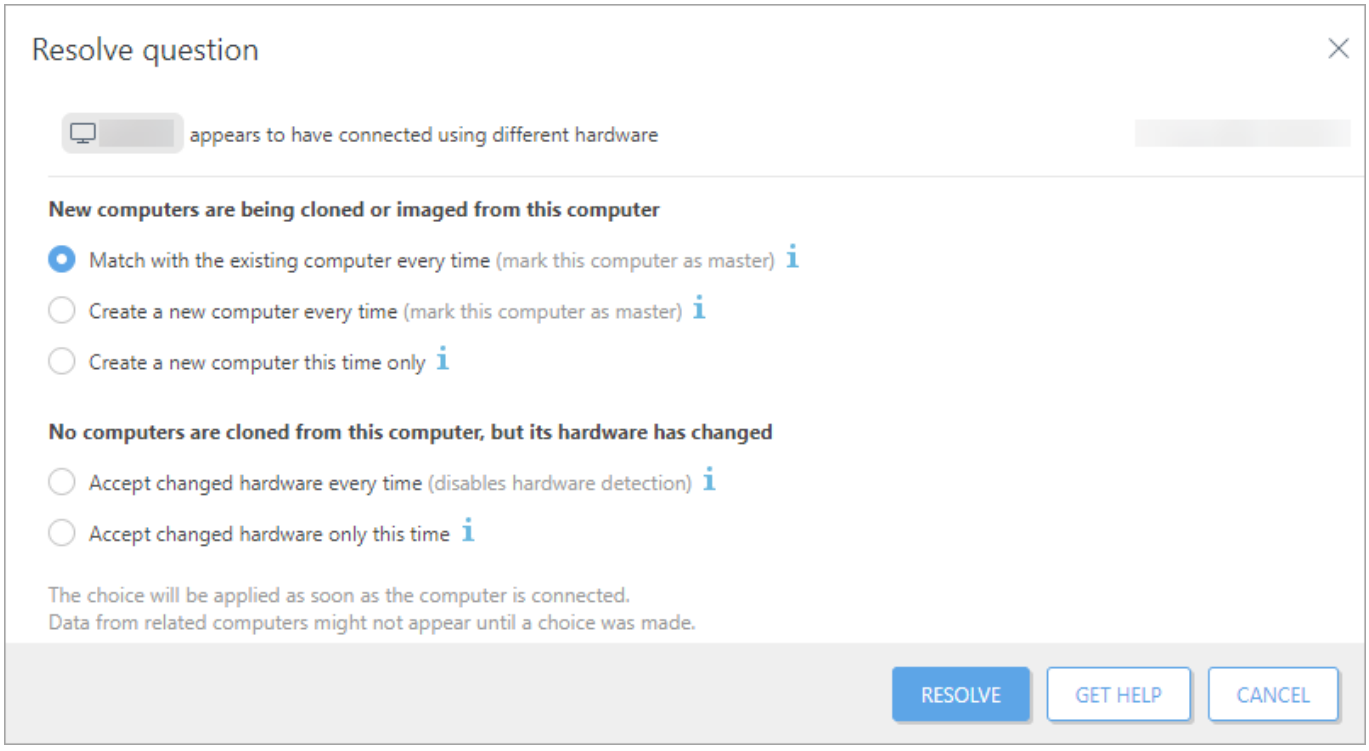
A detecção de Impressão digital de hardware não é compatível com:
- Linux, macOS, Android, iOS
- máquinas sem o Agente ESET Management

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. A questão da clonagem será resolvida na próxima vez que o computador clonado se conectar ao ESET PROTECT.



Se você não resolver uma questão em 30 dias, a opção **Criar um novo computador somente desta vez** será selecionada automaticamente.

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. A janela de diálogo **Perguntas** não lida com essa situação. 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 Web Console. 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 resolver esse problema 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 ativar produtos ESET e entre em contato com a ESET para modificar sua licença.

Notificações para computadores clonados

Um usuário pode escolher entre três notificações preparadas para ações relacionadas à clonagem. Para configurar uma notificação, selecione o menu **Notificações** no Web Console.

- **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 em seu hardware, se o computador foi clonado de uma máquina mestre ou 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.

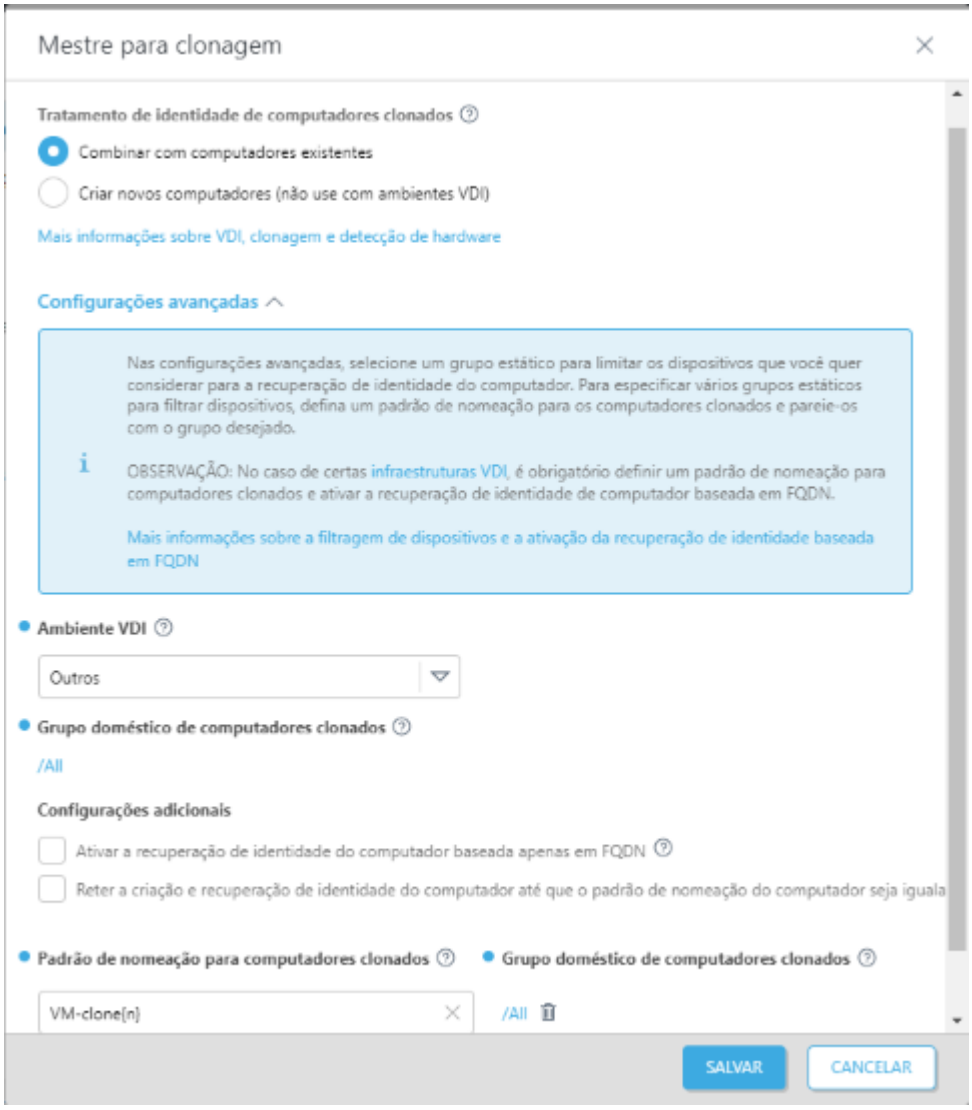
Identificação de hardware

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**.

ESET BridgeProxy HTTP -

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

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

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

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

Apache HTTP Proxy usuários
Começando com o ESET PROTECT 4.0 (lançado em novembro de 2022), o ESET Bridge substitui o Apache HTTP Proxy. O Apache HTTP Proxy agora está com Suporte limitado. Se você usar o Apache HTTP Proxy, recomendamos migrar para o ESET Bridge.

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 Servidor ESET PROTECT exclusivamente por meio do Agente.

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.

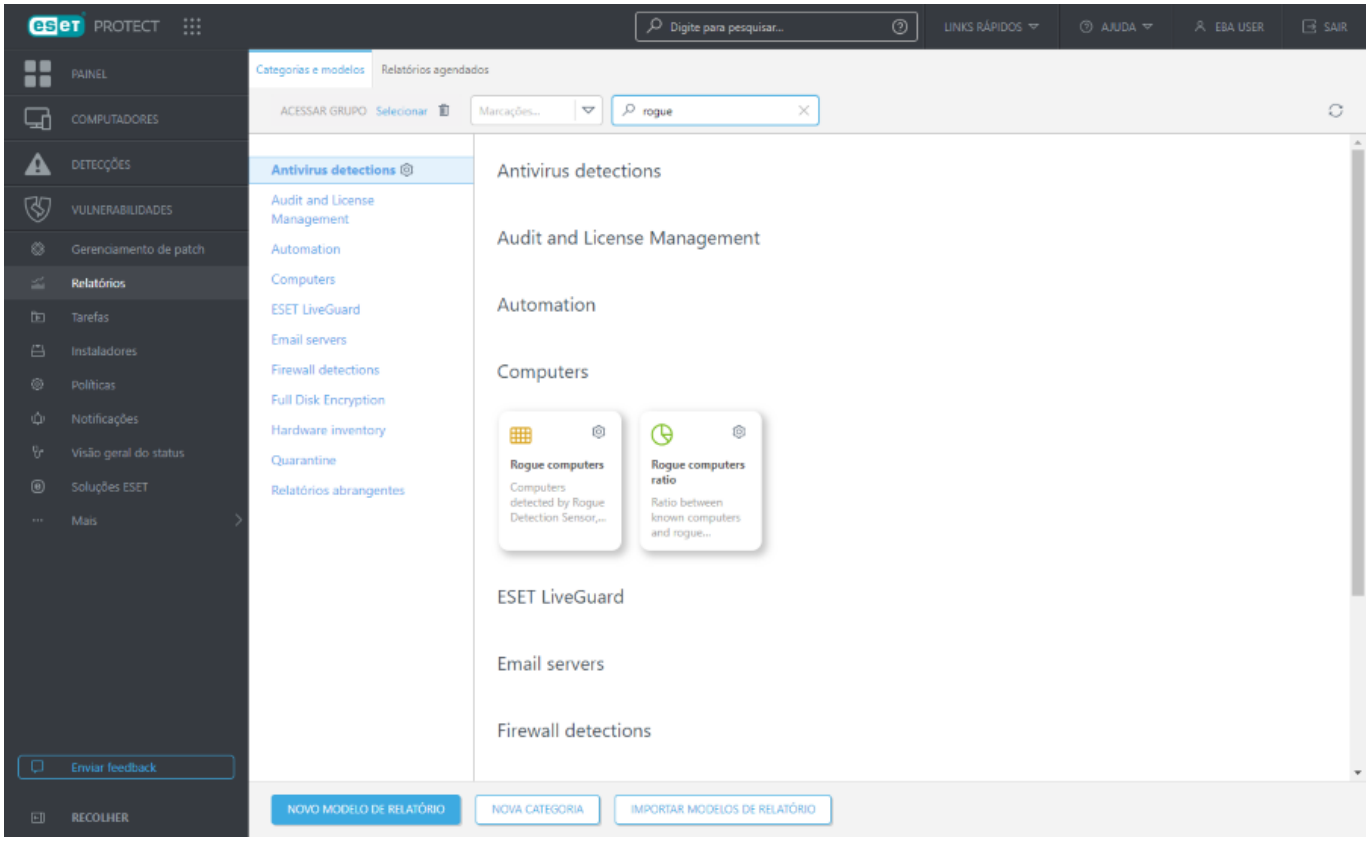
Recomendamos que você use a implantação local apenas se você tiver uma rede pequena (até 50 computadores). Para redes maiores, é possível Implantar o Agente ESET Management usando GPO ou SCCM.

- 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 o RD sensor

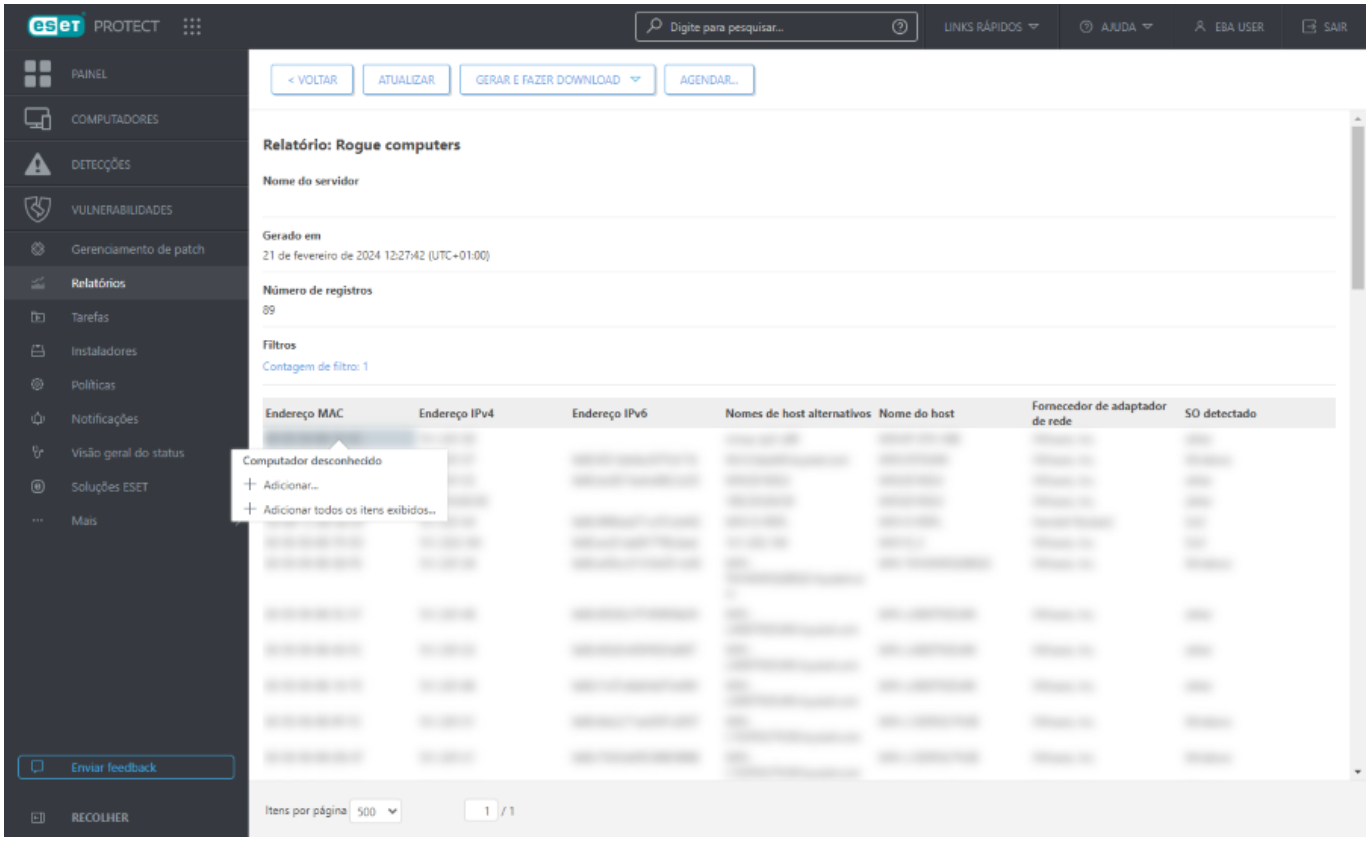
A forma mais fácil de encontrar um computador não gerenciado em sua estrutura de rede é usar o RD Sensor. O RD Sensor monitora a rede na qual ele está implantado e, quando um novo dispositivo sem um Agente se conecta à rede, ele reporta essas informações para o ESET PROTECT. O componente do RD Sensor não pode ser implantado com Live Installer. Para implantar o RD Sensor na sua rede, siga as etapas de instalação do RD Sensor.

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.

Para adicionar computadores encontrados pelo RD Sensor ao ESET PROTECT, faça o download do relatório no formato *.csv* e use essa lista na Ferramenta de implantação na opção Importar lista de 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

Instalação do Sensor RD

Você pode instalar o ESET Rogue Detection Sensor no Windows ou Linux.

Pré-requisitos

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

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

- A instância ESET PROTECTestá acessível

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

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

Instalação no Windows

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

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

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

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

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

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

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

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

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

Instalação no Linux

Siga as etapas abaixo para instalar o componente do Sensor RD no Linux usando o comando Terminal:

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

1. Visite a seção de download ESET PROTECT para fazer download de um instalador autônomo para este componente ESET PROTECT (*rdsensor-linux-i386.sh* ou *rdsensor-linux-x86_64.sh*).

2. Defina o arquivo de instalação do Sensor RD como um executável: `chmod +x rdsensor-linux-x86_64.sh`

3. Use o seguinte comando para executar o arquivo de instalação como sudo:

```
sudo ./rdsensor-linux-x86_64.sh
```

4. Leia o Acordo de licença de usuário final. Use a **barra de espaço** para ir para a próxima página do EULA. O instalador irá solicitar que você especifique se aceita o acordo. Pressione **Y** no seu teclado se concordar. Caso contrário, pressione **N**.

5. Pressione **Y** se você concordar em participar do Programa de melhoria do produto. Caso contrário, pressione **N**.

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

7. Para verificar se a instalação foi bem-sucedida, verifique se o serviço está em execução ao executar o comando a seguir:

```
sudo systemctl status rdsensor
```

Você pode encontrar aqui o arquivo de relatório do Rogue Detection Sensor:
/var/log/eset/RogueDetectionSensor/trace.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.

Navegue até a seção Instaladores e selecione o pacote de instalador desejado.

A implantação local pode ser realizada dessas maneiras:

- Criar instalador do Agente e produto de segurança ESET – (Windows, macOS)
- Criar instalador de script do Agente (Linux, macOS)

O Agente ESET Management vem pré-configurado para conexão adequada ao ESET PROTECT, portanto apenas modificações limitadas para as configurações do Agente ESET Management estão disponíveis via Política do Agente ESET Management.

Criar Live Installer – Agente e produto de segurança ESET – Windows/macOS

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

- **Links rápidos** > **Dispositivos Windows** ou **dispositivos macOS**
- **Instaladores** > **Criar instalador** > **Windows** ou **macOS**
- ESET PROTECT Tour

1. **Configurações de proteção e instalação** – Selecione a caixa de seleção ao lado da configuração para ativá-la para o instalador:

- Windows apenas:

  oAtivar o sistema de feedback ESET LiveGrid® (recomendado)

  oAtivar a detecção de aplicativos potencialmente indesejados – leia mais em nosso artigo da Base de conhecimento.

- 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. Selecione a caixa de seleção **Eu aceito o Acordo de licença de usuário final 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.

3. Clique em **Download** para fazer download do pacote do instalador ou selecionar outras opções de distribuição de pacote do instalador.

Clique em **Personalizar instalador** para personalizar o pacote do instalador:

4. **Distribuição** – selecione **Fazer download ou enviar instalador ou usar a ESET Remote Deployment Tool** (Windows) ou **Fazer download ou enviar instalador** (macOS).

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

5. **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. Não é possível desmarcar o produto de segurança ESET em um instalador macOS.

- Windows apenas: **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.

- Windows apenas: **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.

6. 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).

7. **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.

8. Personalizar mais configurações

- Digite o **Nome** e a **Descrição do instalador** (opcional).
- Clique em **Selecionar marcações** para atribuir marcações.
- **Configuração inicial (opcional)** – use essa 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 Servidor ESET PROTECT. O campo **Host** é o endereço da máquina que executa 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 Servidor ESET PROTECT não é compatível com a autenticação. Qualquer solução de proxy usada para encaminhar a comunicação do Agente para o Servidor ESET PROTECT e que precise de autenticação não funcionará.

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 desabilitar a configuração usando uma Política de AgenteESET Management:
- Durante a criação do instalador – inclua a política na **Configuração inicial**.
- Depois da instalação do Agente ESET Management – atribua a política ao computador.

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

10. 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.
b. Windows apenas: 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 **Eu aceito o Acordo de licença de usuário final 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**).
o**Configuração** Opcionalmente, você pode selecionar uma **Política** que será aplicada ao produto de segurança ESET durante sua instalação.
o Windows apenas: **Executar o ESET AV Remover** – selecione a caixa de seleção para desinstalar ou remover completamente outros programas antivírus no dispositivo de destino.

Windows apenas: 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 **Eu aceito o Acordo de licença de usuário final 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**).

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 **Eu aceito o Acordo de licença de usuário final 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**).
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.

11. Clique em **Concluir**.

12. Você pode distribuir o pacote Live Installer de várias formas:

- Clique em para copiar o link de download do pacote Live Installer, distribuir o link para os usuários e deixá-los fazer download e instalar o pacote Live Installer.

- Você também pode **Fazer download** do pacote Live Installer e distribuí-lo pessoalmente, ou carregá-lo para um local compartilhado para acesso dos usuários.

- Apenas Windows Use o Remote Deployment Tool para implantar remotamente o pacote Live Installer.

- Clique em para usar o servidor SMTP ESET PROTECT para entregar uma mensagem de e-mail com o link de download do pacote Live Installer para usuários especificados.

  oPara adicionar um usuário, clique em **Adicionar** > preencha o campo **Endereço de e-mail** > pressione **Enter** ou clique em . Opcionalmente, clique em **Criar usuário** > digite o **Nome** do usuário > clique em **Salvar**. Você pode editar detalhes do usuário nos Usuários do computador. Clique em **Ver visualização de e-mail**, selecione o **Idioma do e-mail** no menu suspenso e clique em **Salvar**.

  oPara 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).

Depois de ser criado, o Live Installer vai se comportar de acordo com esta tabela.
O Live Installer requer uma conexão com a internet e não funciona em um computador off-line.
O Live Installer no macOS requer uma conexão com a internet direta (para conectar aos servidores ESET) e não funciona em um computador macOS conectado à internet via Proxy sem conexão direta com a internet.

O ESET PROTECT é compatível com a atualização automática de Agentes ESET Management em computadores gerenciados.

13. Execute o arquivo do pacote de instalação em um computador cliente. O pacote Live Installer vai fazer download do Agente ESET Management e do produto de segurança ESET compatíveis com a plataforma do sistema operacional do computador (x86, x64, ARM64). Ele vai instalar o Agente ESET Management e o produto de segurança ESET no dispositivo e conectar o dispositivo ao ESET PROTECT. O instalador do ESET Endpoint Antivirus/Security criado no ESET PROTECT é compatível com o Windows 10 Enterprise para Desktops virtuais e com o modo de várias sessões do Windows 10. Para instruções passo a passo, veja o assistente de configuração para Windows ou macOS.

Live Installer comportamento

Depois do Live Installer ser criado, ele é armazenado no ESET PROTECT e vai se comportar como descrito na tabela abaixo.

Ação	Comportamento do link de download Live Installer	Comportamento do Live Installer depois do download
Live Installer é removido de ESET PROTECT.	O link de download está desativado.	Foi feito do download de Live Installer cópias antes da exclusão parar de funcionar.
Live InstallerO não está mais presente no repositório.	O link de download está desativado. **O pacote selecionado não está no repositório** é exibido ao lado do instalador.	Foi feito do download de Live Installer cópias antes da edição parar de funcionar.
Política que faz parte do Live Installer é editada.	A alteração na Política não será refletida nas cópias existentes do Live Installer e o link de download vai oferecer ao instalador as políticas definidas quando ele foi criado inicialmente. Se você quiser que as alterações sejam refletidas no instalador, será preciso criar um novo instalador com esta Política atualizada.	O instalador vai funcionar, mas vai instalar seu produto ESET com políticas definidas quando ele foi criado inicialmente.
Política que faz parte do Live Installer é removida	**A política referenciada não está acessível**, o aviso será exibido ao lado do instalador e o link de download será desativado. Duplicar o instalador e atribuir uma nova política para ele.	Foi feito do download de Live Installer cópias antes da exclusão parar de funcionar.
Grupo que faz parte do Live Installer é editado.		Essa alteração não vai afetar os instaladores existentes e o computador será atribuído ao grupo atualizado/movido quando se conectar ao ESET PROTECT.
Grupo que faz parte do Live Installer é removido.		O instalador vai se comportar como se não houvesse nenhum grupo atribuído ao instalador. Ele será atribuído ao grupo padrão **Perdido e encontrado**.

Ação	Comportamento do link de download Live Installer	Comportamento do Live Installer depois do download
Live Installervida útil	Instaladores Live Installer são válidos por 6 meses depois de serem criados. Para atualizar o link de download de um instalador existente, navegue até **Instaladores**, selecione o instalador existente e selecione **Mostrar link de download**. Faça o download de um instalador válido do novo link de download.	

Criar instalador de script do Agente – 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).

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

- **Links rápidos** > **Dispositivos macOS** ou **dispositivos Linux**
- **Instaladores** > **Criar instalador** > **macOS** ou **Linux**
- ESET PROTECT Tour

Clique em **Personalizar instalador** > **Implantar primeiro o Agente (instalador de script do Agente)**.

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. Personalizar mais configurações

- Digite o **Nome** e a **Descrição do instalador** (opcional).
- Clique em **Selecionar marcações** para atribuir marcações.
- **Configuração inicial (opcional)** – use essa 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 Servidor ESET PROTECT. O campo **Host** é o endereço da máquina que executa 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 Servidor ESET PROTECT não é compatível com a autenticação. Qualquer solução de proxy usada para encaminhar a comunicação do Agente para o Servidor ESET PROTECT e que precise de autenticação não funcionará.

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 desabilitar a configuração usando uma Política de AgenteESET 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 **Salvar e Fazer download**.

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

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

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

> O ESET PROTECT é compatível com a atualização automática de Agentes 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:
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 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 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 relate o inventário de hardware corretamente.

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

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

```
yum install policycoreutils-devel
```

Instalação

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

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

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 de Agentes 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. Permitir acesso total ao disco para o Terminal:

   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** > e adicione o **Terminal** à lista de aplicativos na pasta de **Acesso total ao disco**.

   e)Bloqueie as configurações no canto inferior esquerdo.

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

```
cd Desktop
sudo bash PROTECTAgentInstaller.sh
```

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

7. Permitir acesso total ao disco para o Agente ESET Management:

Localmente:

   a)Abra as **Preferências do sistema** > **Privacidade e segurança** > **Privacidade**.

   b)Desbloqueie as configurações no canto inferior esquerdo.

   c)Clique em **Acesso total ao disco**.

   d)Clique em **+** > **Aplicativo** > **ESET** > **Abrir** e adicione o Agente ESET Management à lista de aplicativos na

pasta de **Acesso total ao disco**.

e)Bloqueie as configurações no canto inferior esquerdo.

Remotamente:

a)Faça o download do arquivo de configuração da lista .plist.

b)Gere dois UUIDs com um gerador UUID de sua escolha e use um editor de texto para substituir cadeias de caracteres pelo texto. Insira seu UUID 1 e UUID 2 no perfil de configuração baixado.

c)Implante o arquivo do perfil de configuração .plist usando o servidor de gerenciamento de dispositivo móvel. Seu computador precisa estar inscrito no servidor de gerenciamento de dispositivo móvel para implantar perfis de configuração em computadores.

8. 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 de Agentes ESET Management em computadores gerenciados.

Instalação e solução de problemas do Agente

Verifique se o Agente está em execução: Clique em **Ir** > **Utilitários** e clique duas vezes no **Monitor de atividade**. Clique na guia **Energia** ou na guia **CPU** e localize o processo chamado **ERAAgent**.

O relatório do Agente ESET Management pode ser encontrado aqui:

/Library/Application Support/com.eset.remoteadministrator.agent/Logs/
/Users/%user%/Library/Logs/EraAgentInstaller.log

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

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.

Caso você tenha problemas com a implementação do Agente ESET Management remotamente, consulte Solução de problemas – conexão do Agente.

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.

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

1. Clique em **Windows** > **Personalizar instalador** > **Usar 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. Personalizar mais configurações

- Digite o **Nome** e a **Descrição do instalador** (opcional)
- Clique em **Selecionar marcações** para atribuir marcações.
- **Configuração inicial (opcional)** – use essa 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 Servidor ESET PROTECT. O campo **Host** é o endereço da máquina que executa 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 Servidor ESET PROTECT não é compatível com a autenticação. Qualquer solução de proxy usada para encaminhar a comunicação do Agente para o Servidor ESET PROTECT e que precise de autenticação não funcionará.

  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 desabilitar a configuração usando uma Política de AgenteESET 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 **Concluir**.

6. 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.

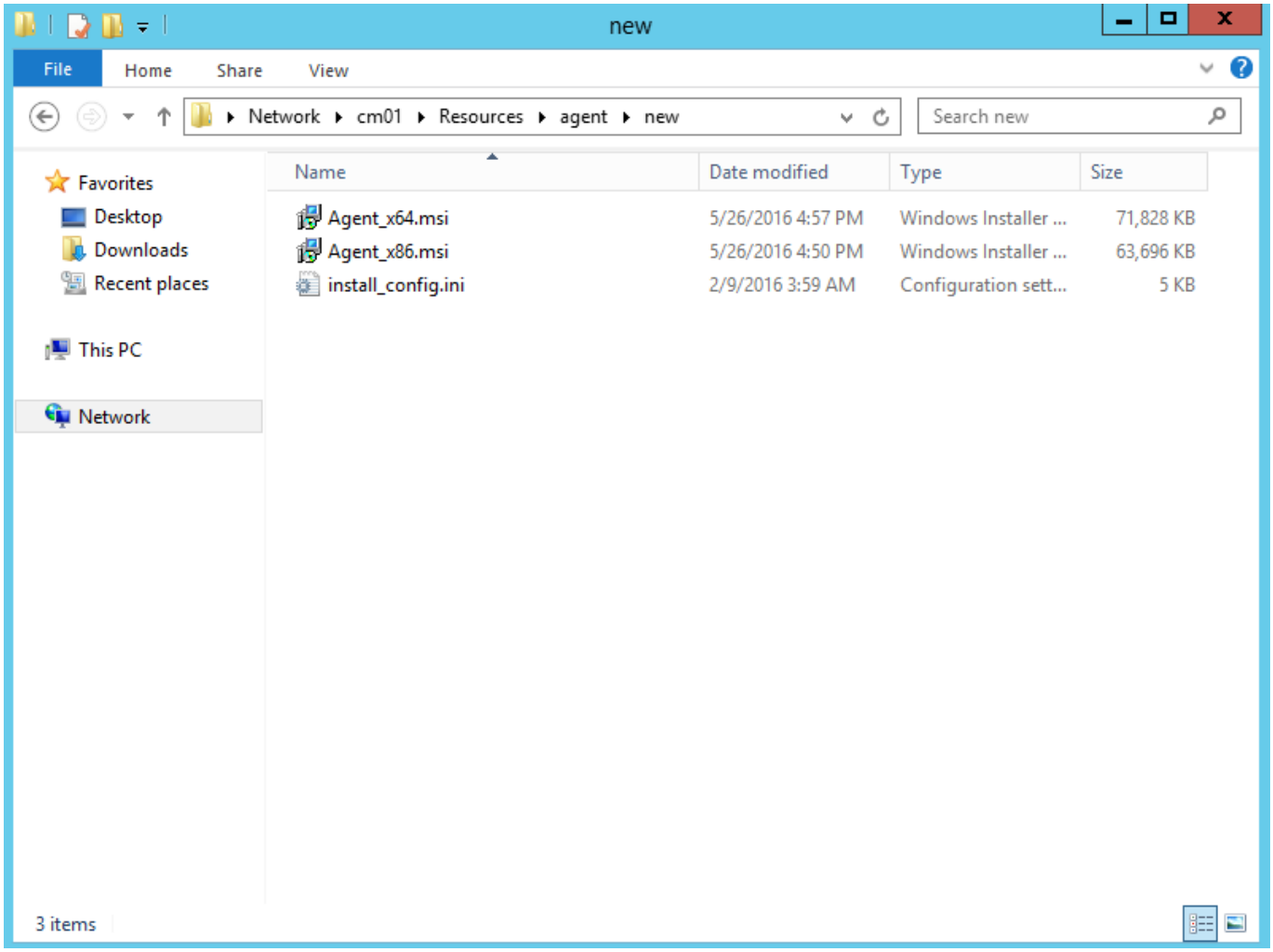
Clique no link adequado abaixo para ver instruções passo-a-passo para dois métodos populares de implantação remota do Agente ESET Management:

- 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)

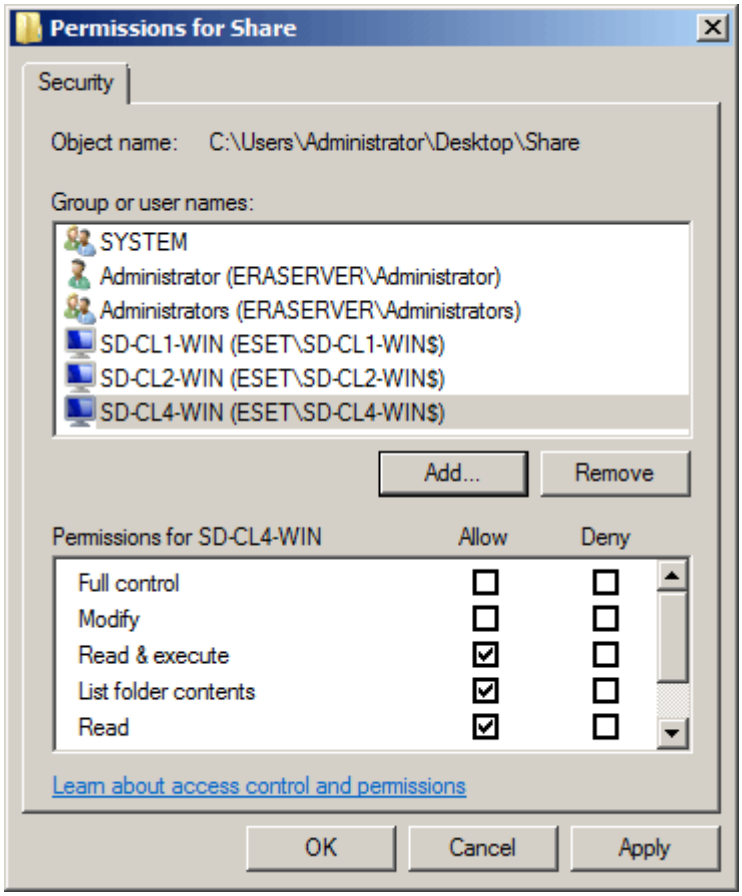
Etapas de implementação - SCCM

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

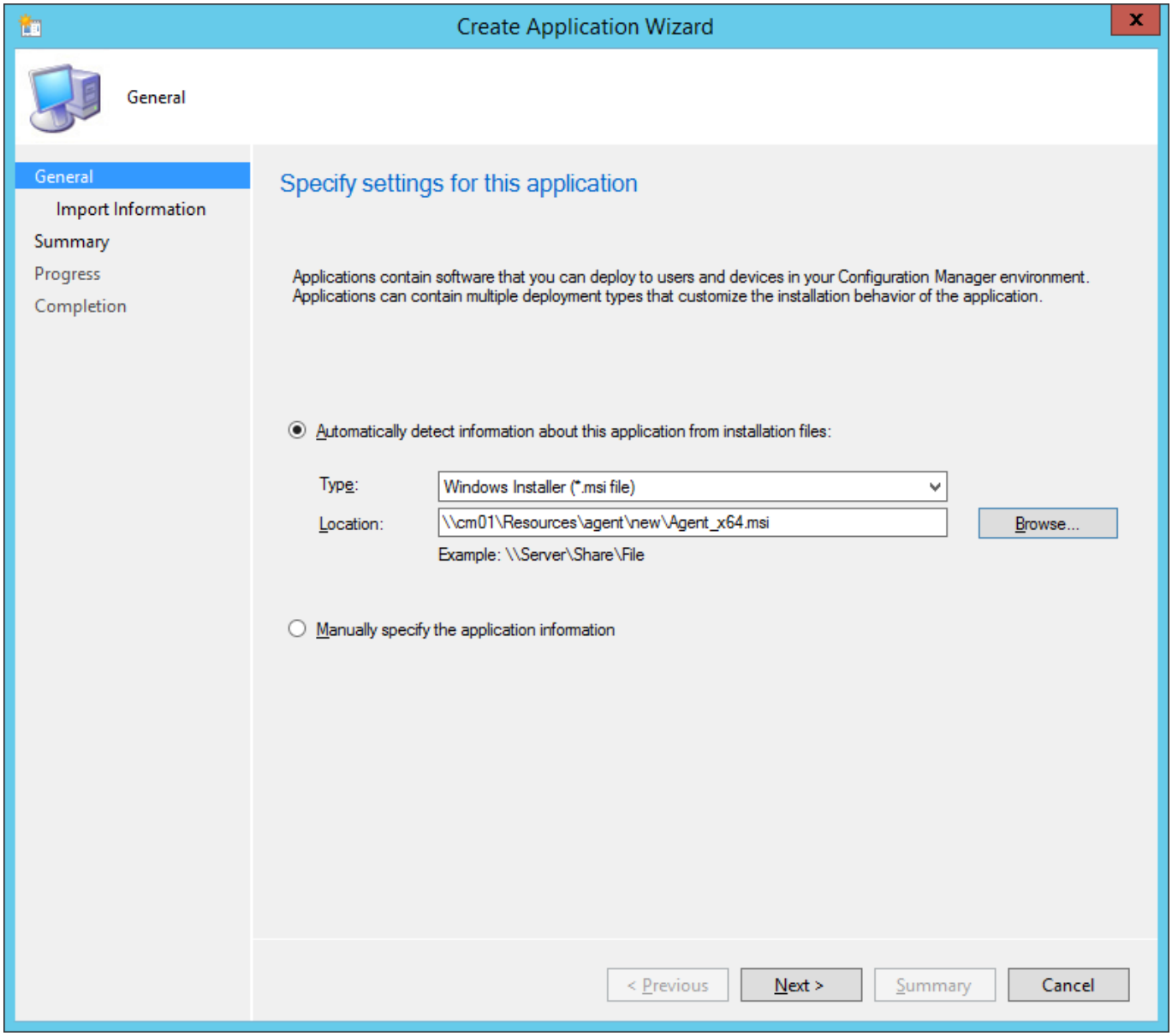
1. Coloque os arquivos *.msi* do instalador do Agente ESET Management e arquivo *install_config.ini* em uma pasta compartilhada.



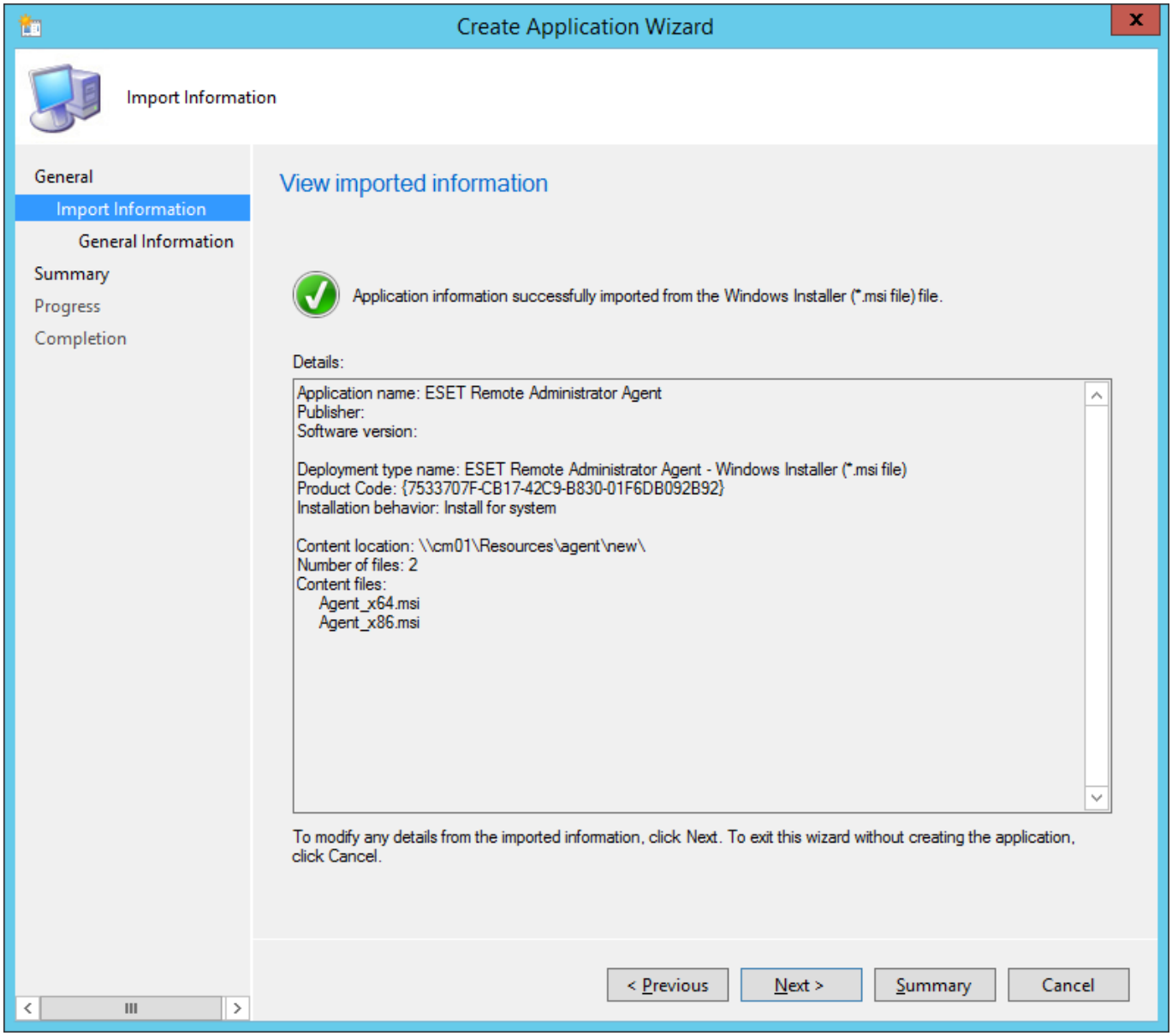
Computadores do cliente vão precisar de acesso de leitura/execução para esta pasta compartilhada.



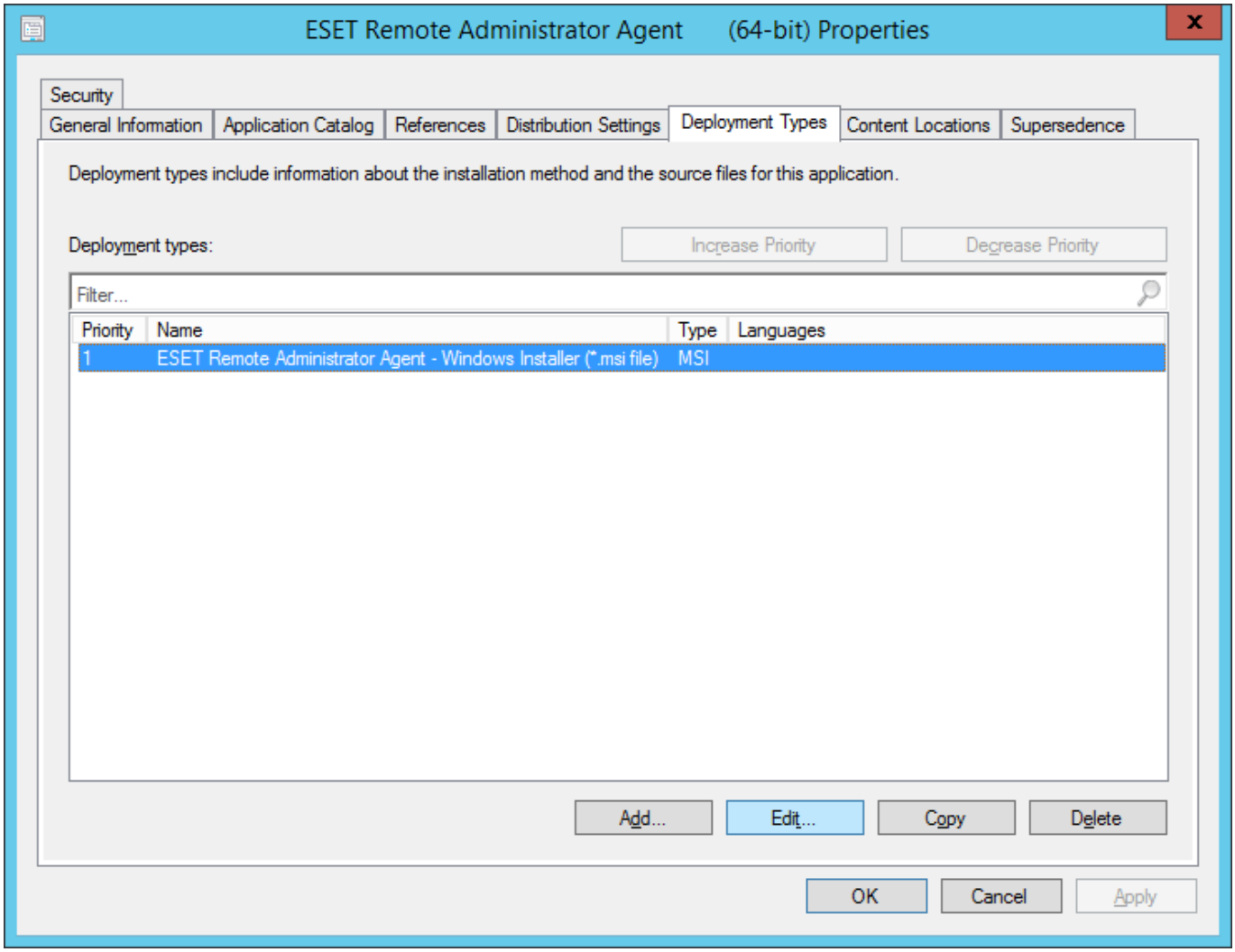
2. Abra o console SCCM e clique em **Biblioteca de software**. Em **Gestão de aplicativo** clique com o botão direito em **Aplicativos** e selecione **Criar aplicativo**. Escolha **Windows Installer (arquivo *.msi)**.



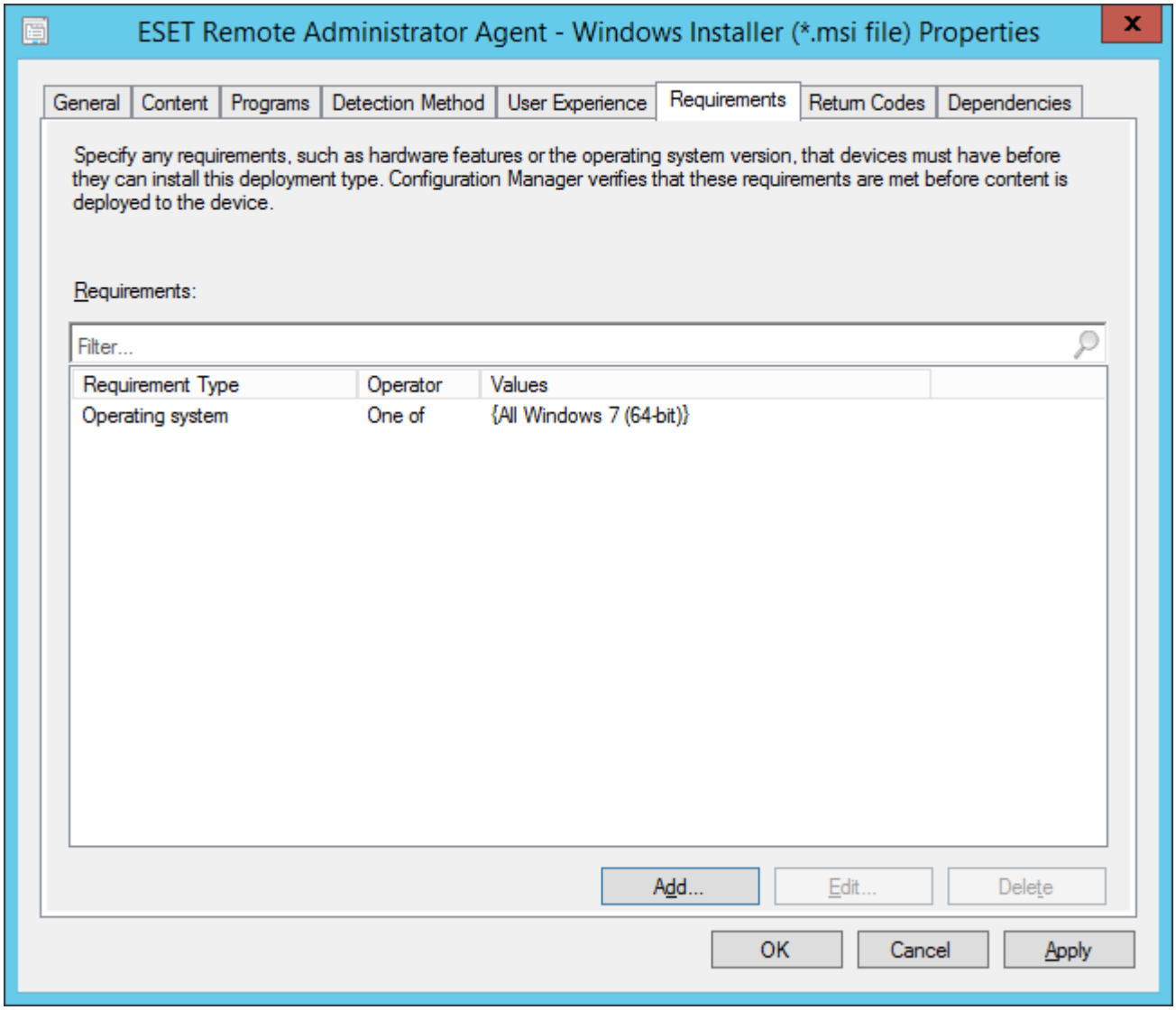
3. Especifique todas as informações necessárias sobre o aplicativo e clique em **Avançar**.

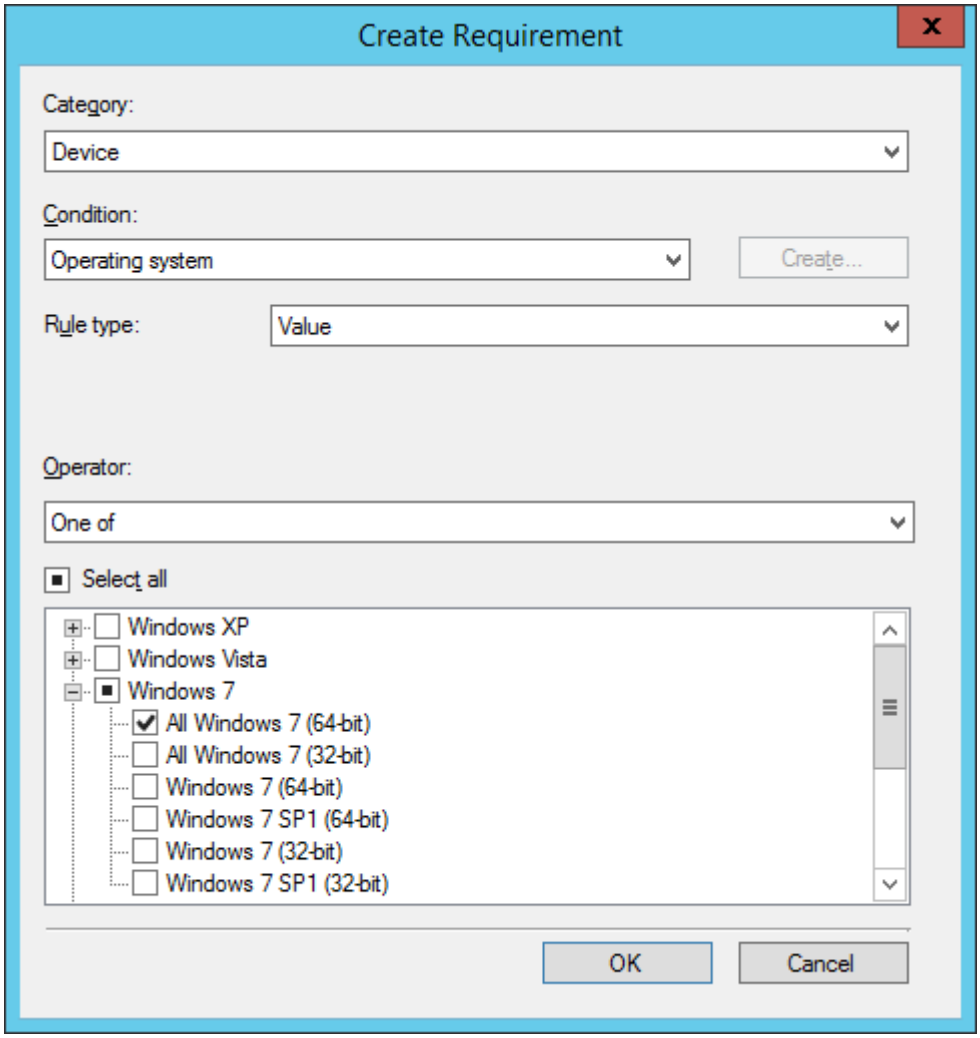


4. Clique com o botão direito no Aplicativo do Agente ESET Management, clique na guia **Tipos de implementação**, selecione a única implementação existente e clique em **Editar**.

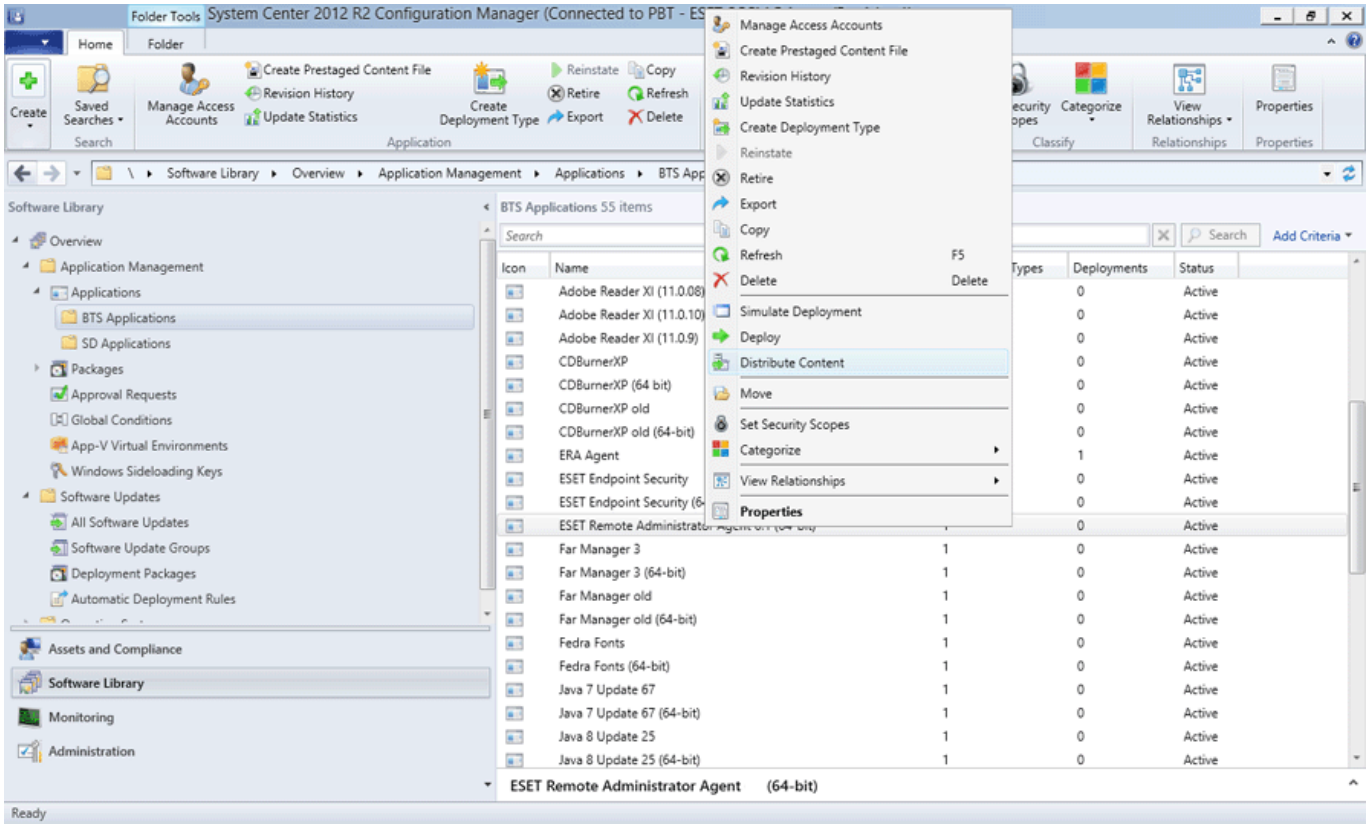


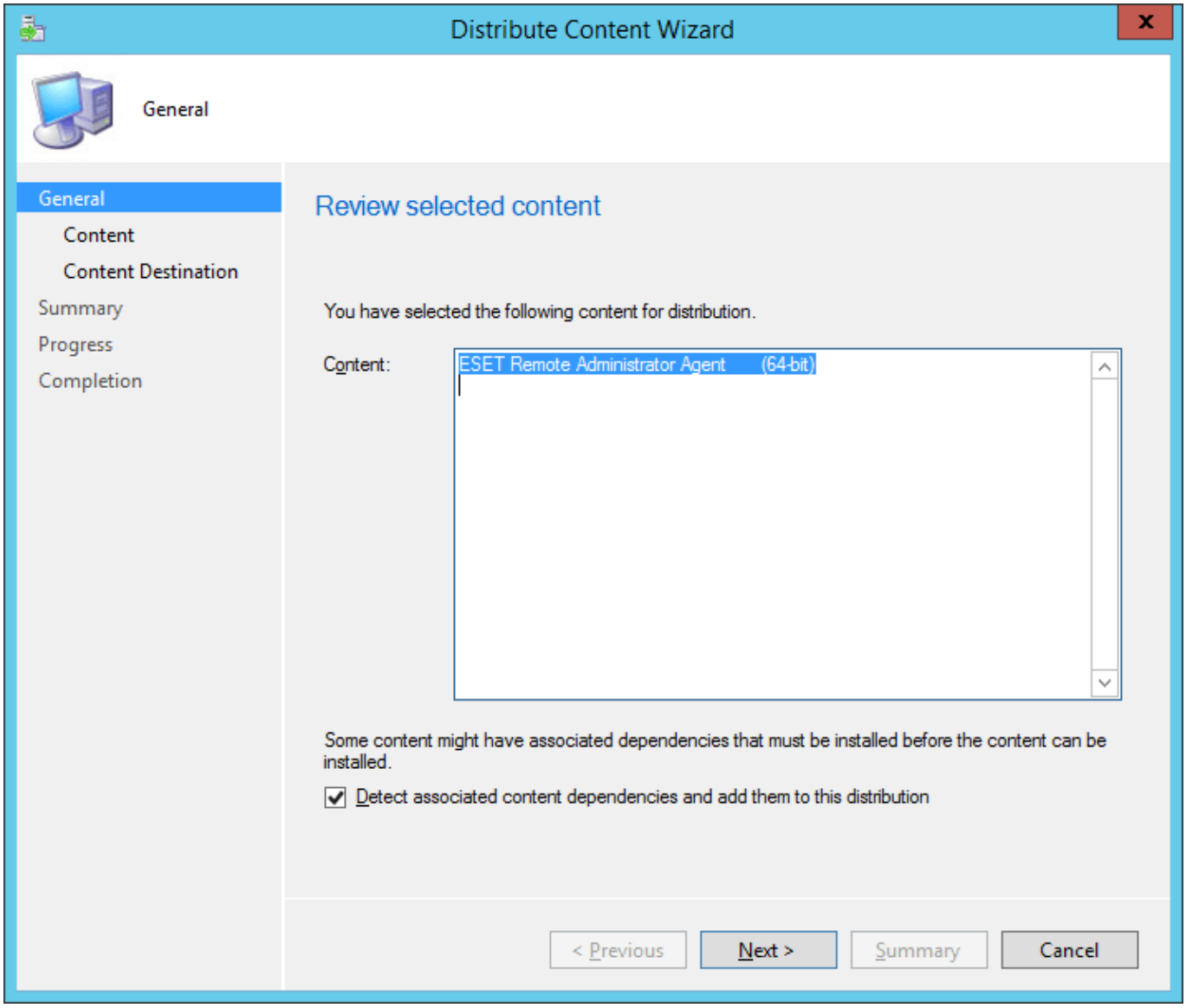
5. Clique na guia **Requisitos** e clique em **Adicionar**. Selecione o **sistema operacional** do menu suspenso **Condição**, selecione **Um** no menu suspenso **Operador** e depois especifique os sistemas operacionais que serão instalados ao marcar as caixas de seleção adequadas. Clique em **OK** quando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

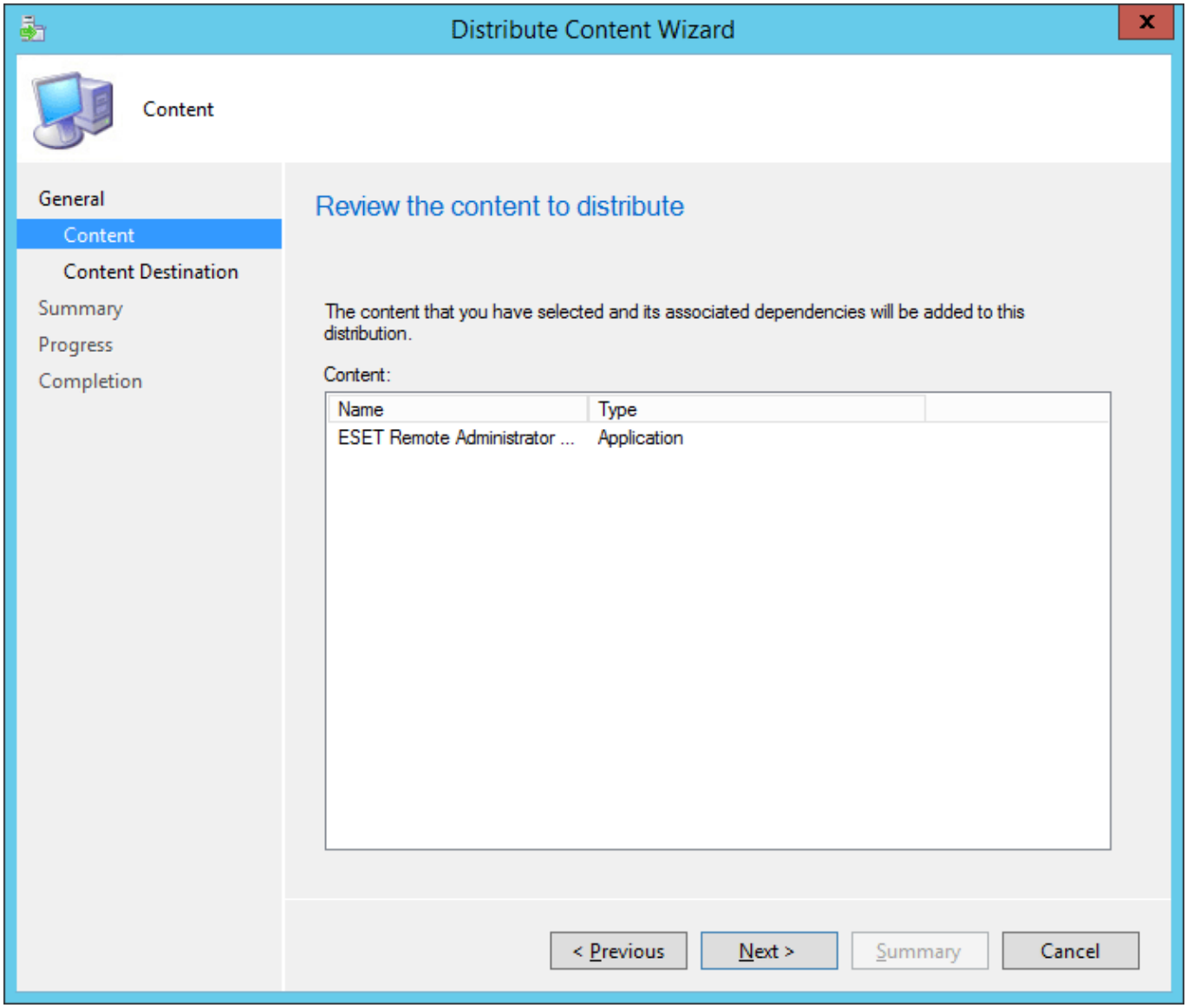

ESET Remote Administrator Agent - Windows Installer (*.msi file) Properties
General
Content
Programs
Detection Method
User Experience
Requirements
Return Codes
Dependencies
Specify any requirements, such as hardware features or the operating system version, that devices must have before they can install 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



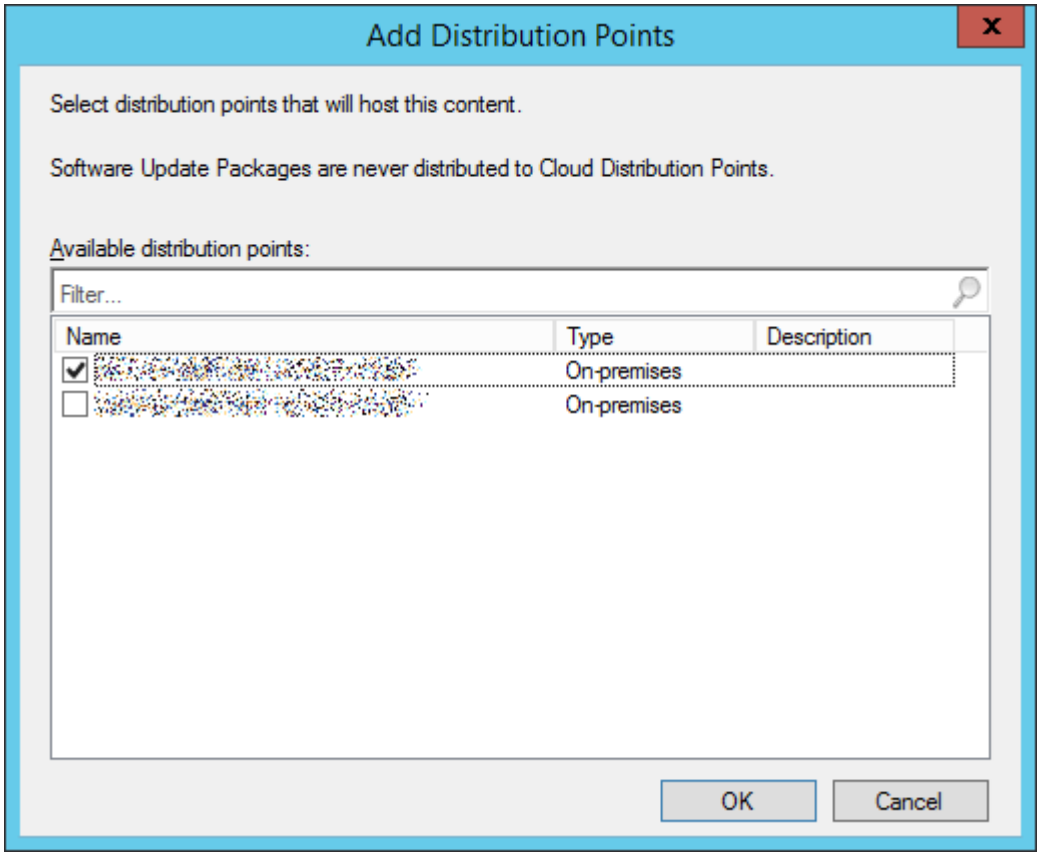
6. Na biblioteca central de software do sistema, clique com o botão direito em seu novo aplicativo e selecione **Distribuir conteúdo** no menu de contexto. Siga as instruções do Assistente de Implementação de Software para concluir a implementação do aplicativo.

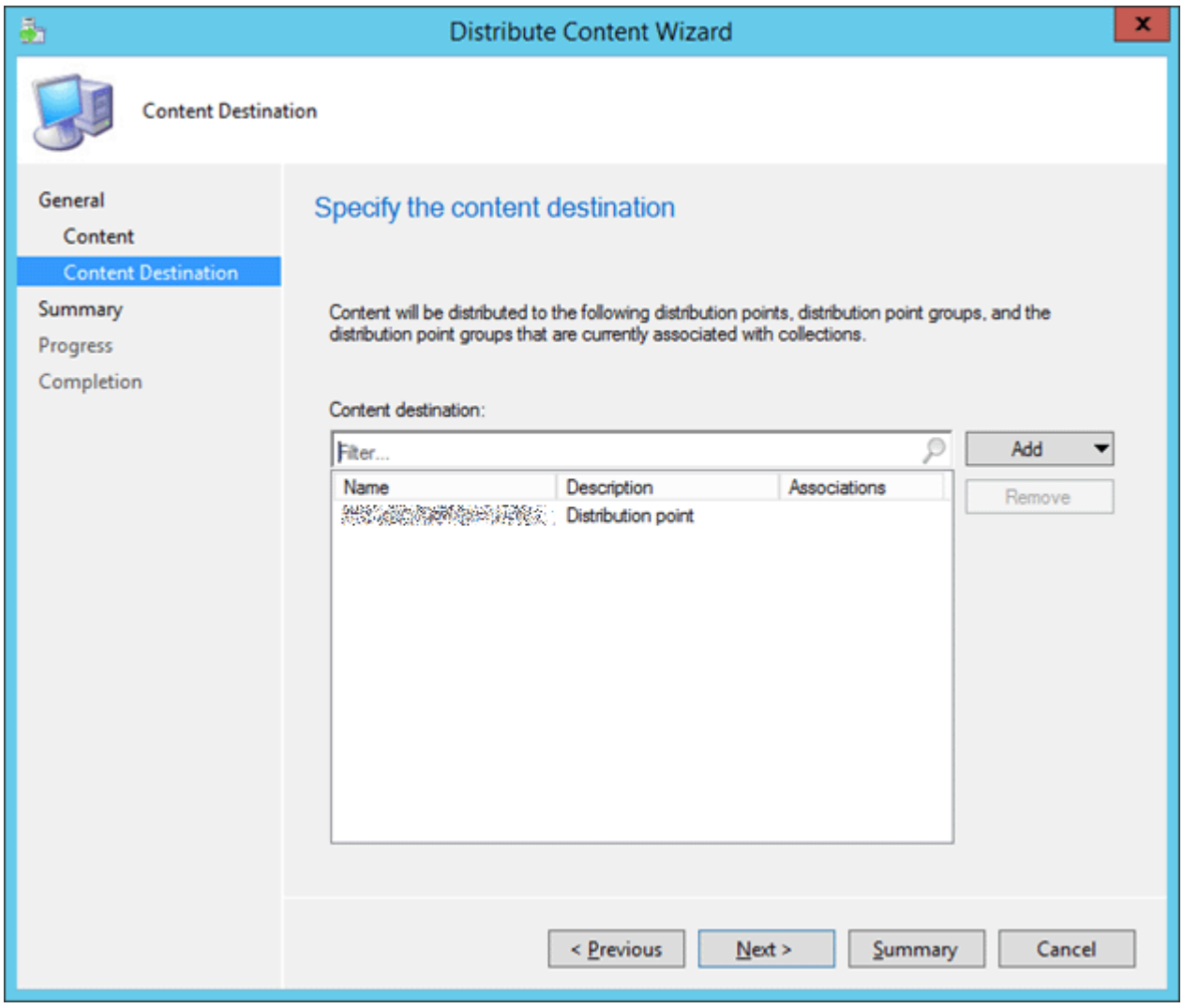

Folder Tools
System Center 2012 R2 Configuration Manager (Connected to PBT - ES
Home
Folder
Create
Saved Searches
Manage Access Accounts
Create Prestaged Content File
Revision History
Update Statistics
Create Deployment Type
Reinstate
Retire
Export
Copy
Refresh
Delete
Search
Application
Categorize
View Relationships
Properties
Classify
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

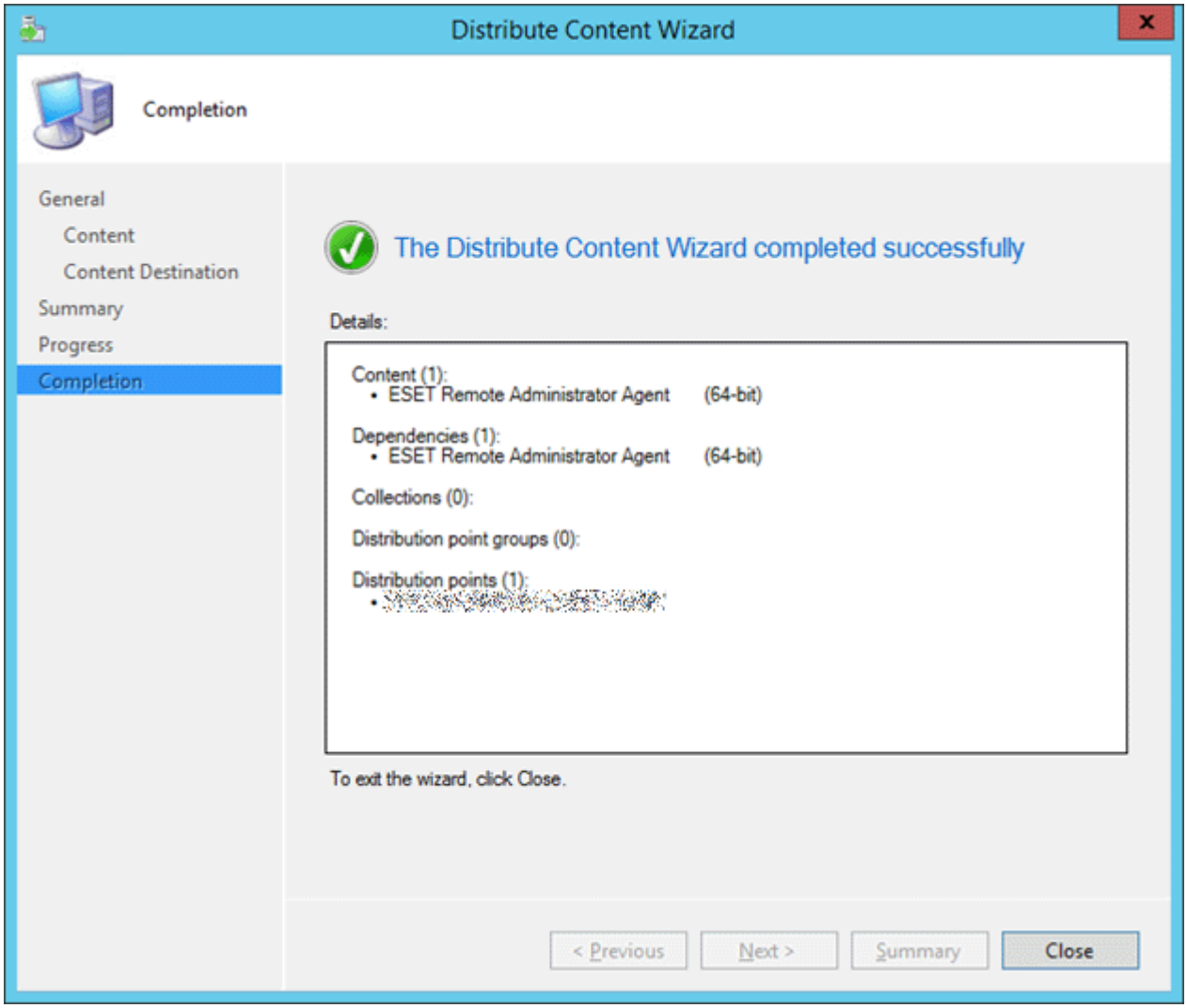

Distribute Content Wizard
General
General
Content
Content Destination
Summary
Progress
Completion
Review selected content
You have selected the following content for distribution.
Content:
ESET Remote Administrator Agent (64-bit)
Some content might have associated dependencies that must be installed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

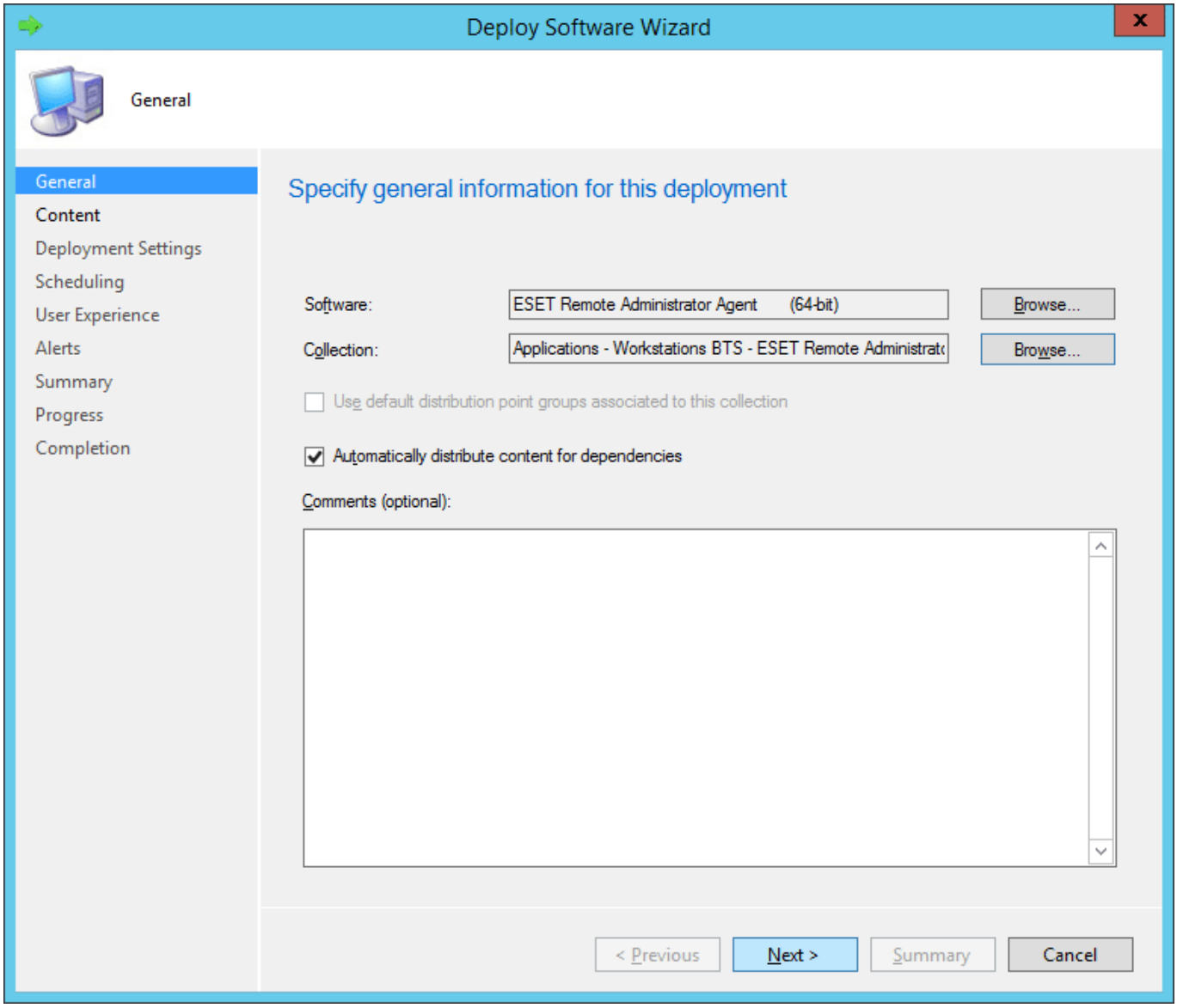


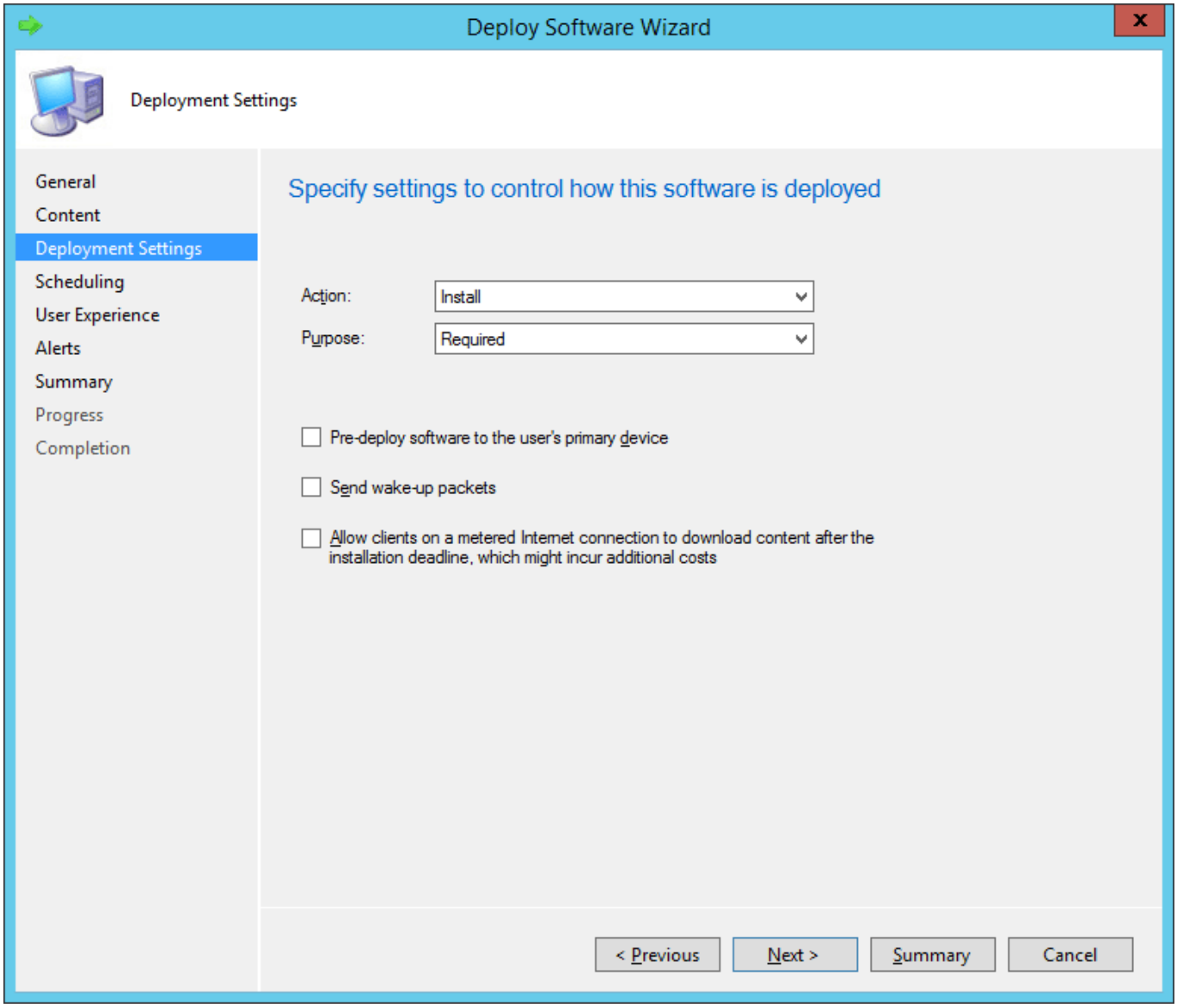
7. Clique com o botão direito no aplicativo e selecione **Implantar**. Siga o assistente e selecione a coleção e o destino para onde deseja implantar o agente.

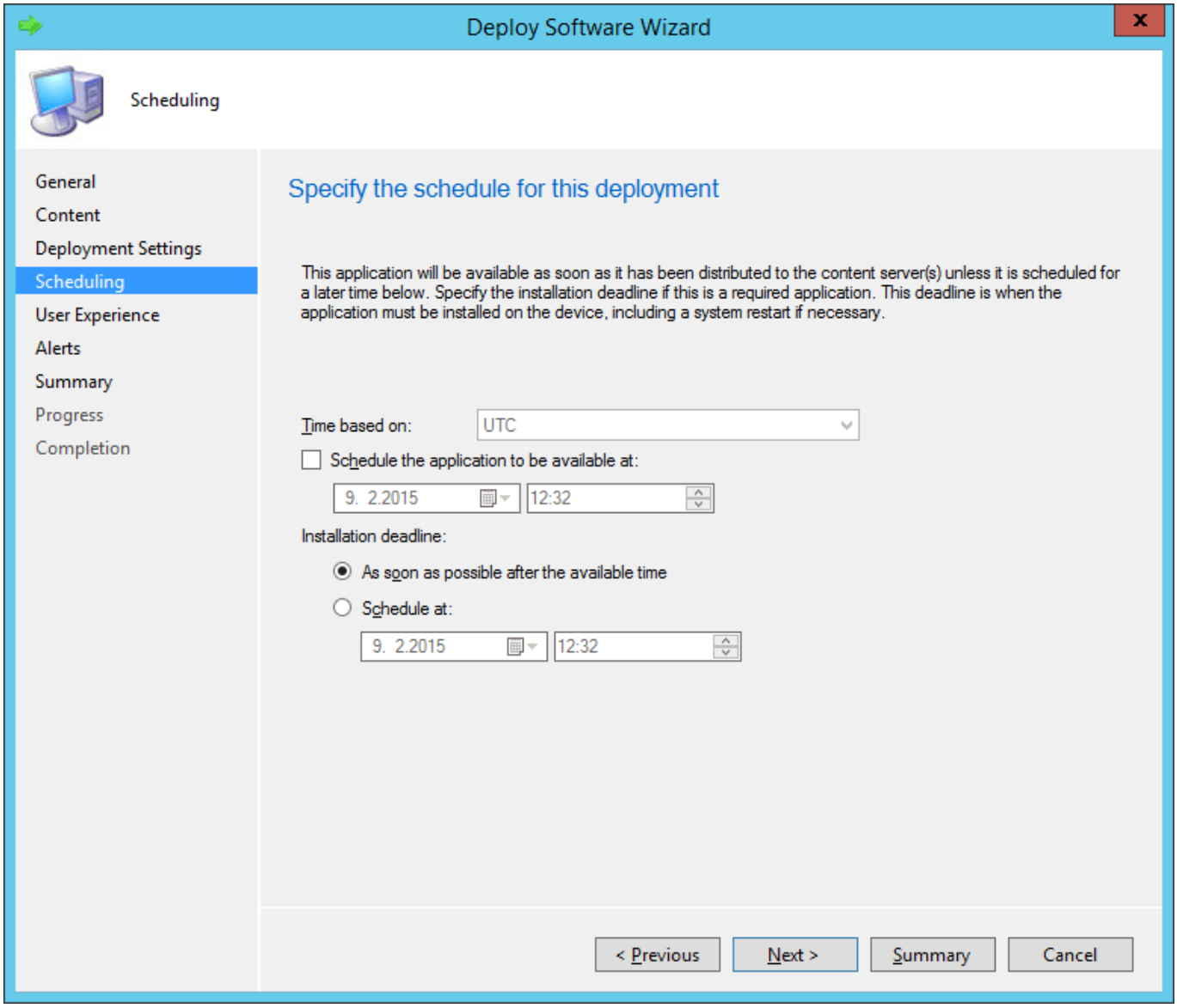

Add Distribution Points
Select distribution points that will host this content.
Software Update Packages are never distributed to Cloud Distribution Points.
Available distribution points:
Filter...
Name
Type
Description
On-premises
On-premises
OK
Cancel

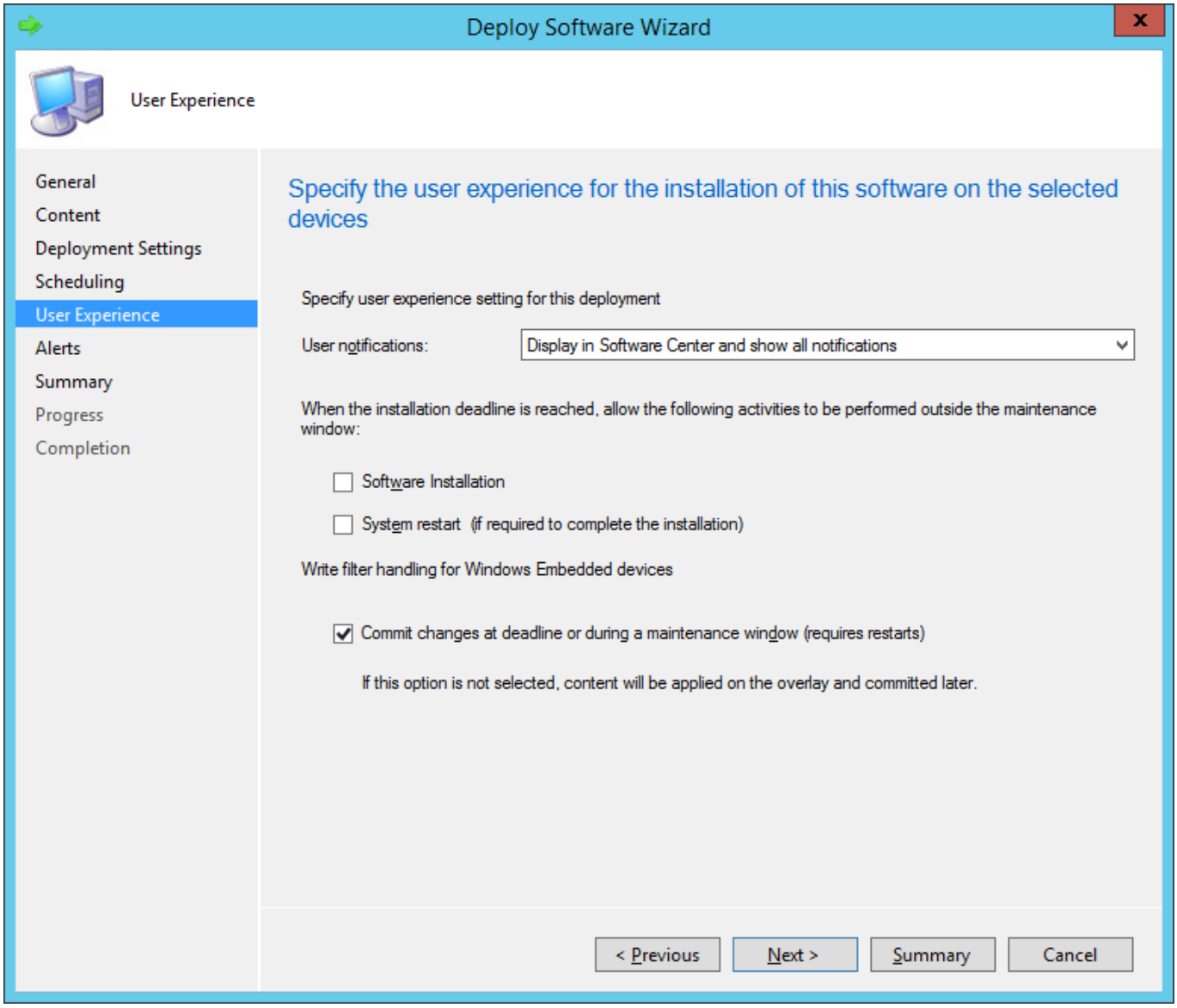

Distribute Content Wizard
Content Destination
General
Content
Content Destination
Summary
Progress
Completion
Specify the content destination
Content will be distributed to the following distribution points, distribution point groups, and the distribution point groups that are currently associated with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

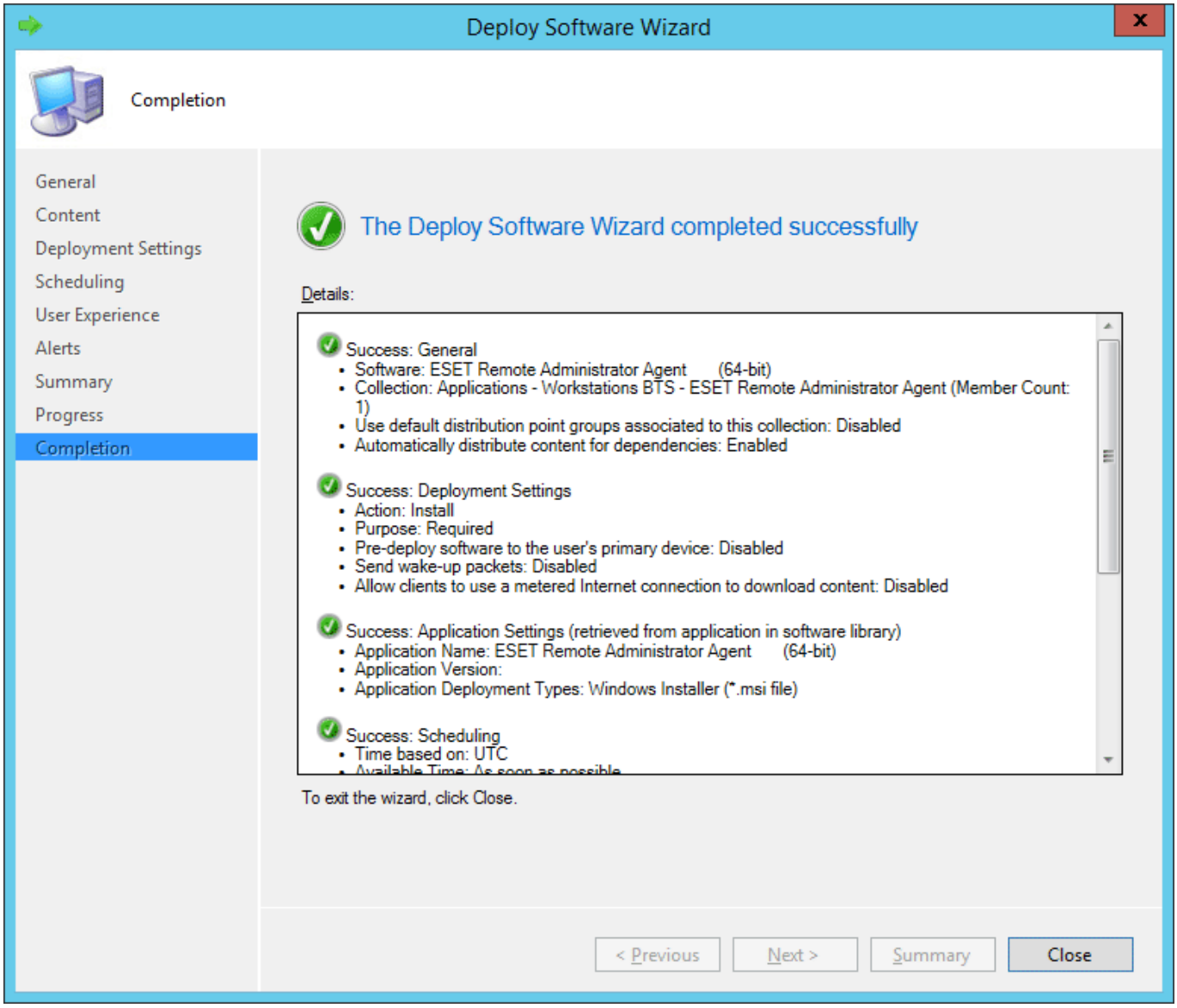

Distribute Content Wizard
Completion
General
Content
Content Destination
Summary
Progress
Completion
The Distribute Content Wizard completed successfully
Details:
Content (1):
• ESET Remote Administrator Agent (64-bit)
Dependencies (1):
• ESET Remote Administrator Agent (64-bit)
Collections (0):
Distribution 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.

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

O Agente ESET Management vem pré-configurado para conexão adequada ao ESET PROTECT, portanto apenas modificações limitadas para as configurações do Agente ESET Management estão disponíveis via Política do Agente ESET Management.

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.

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 A instância ESET PROTECT deve ter sido criada e estar funcionando.

• A porta adequada deve ser aberta. Veja as portas do Remote Deployment Tool ESET PROTECT.

• Uma Live Installer deve ser criada e seu download deve ser feito na unidade local do dispositivo do qual você vai realizar a instalação remota com a Ferramenta de Instalação.

A implantação pode falhar devido a vários motivos. No caso de qualquer problema com a implantação, leia o capítulo de Solução de problemas.

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).

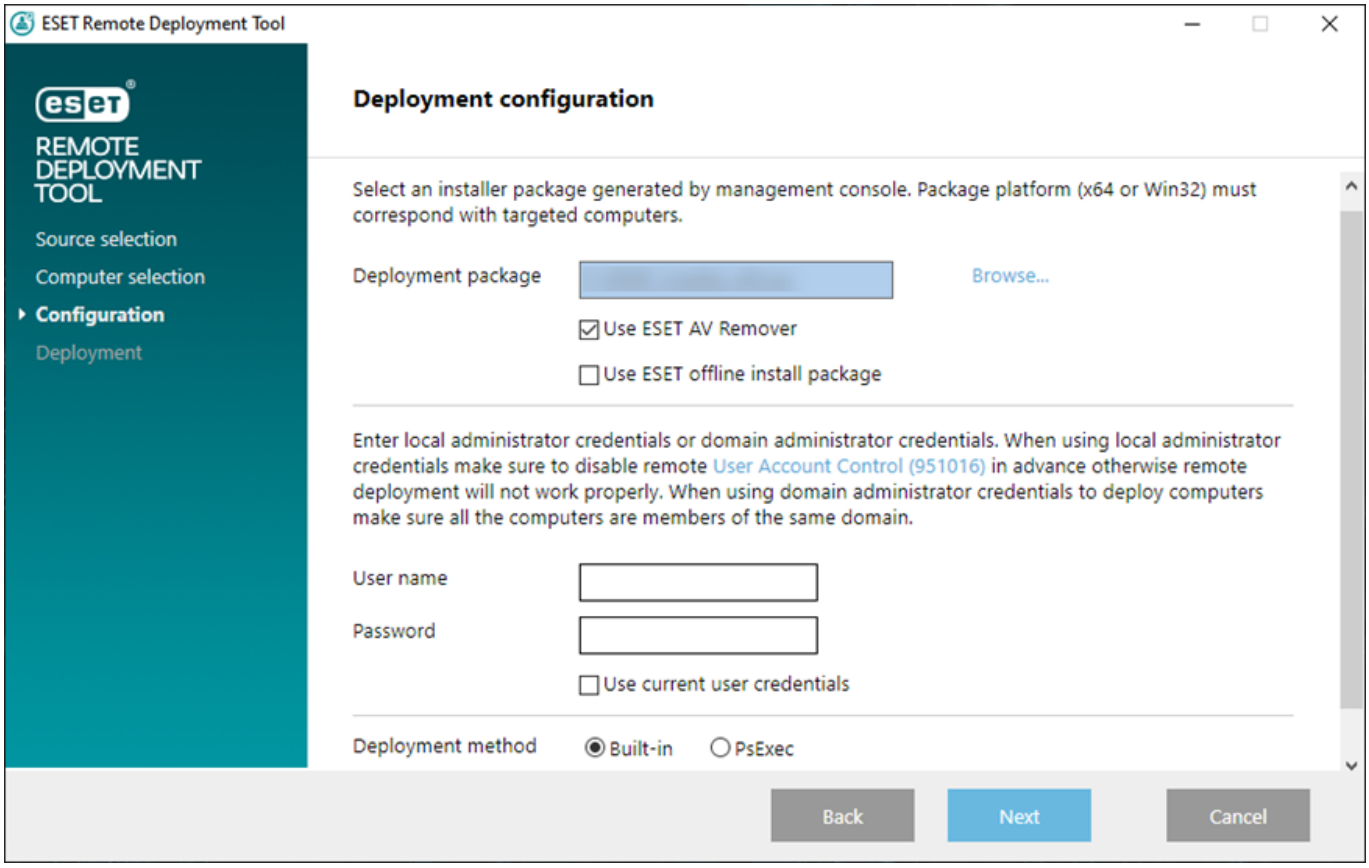
7. Clique em **Procurar** e selecione o pacote de instalação do pacote que você criou no Web Console ESET PROTECT (local ou na nuvem).

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

- 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.

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.

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).

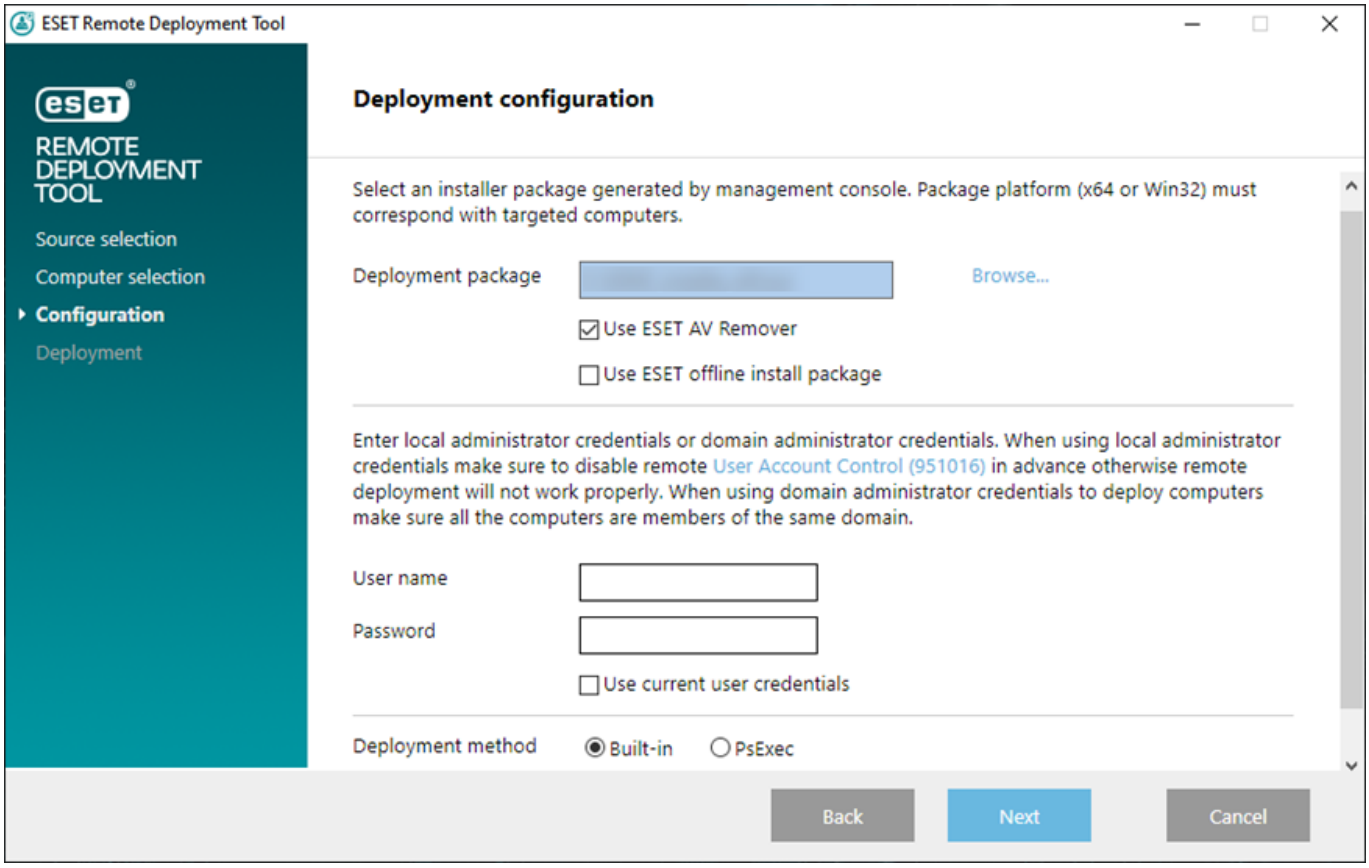
7. Clique em **Procurar** e selecione o pacote de instalação do pacote que você criou no Web Console ESET PROTECT (local ou na nuvem).

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

- 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.

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).

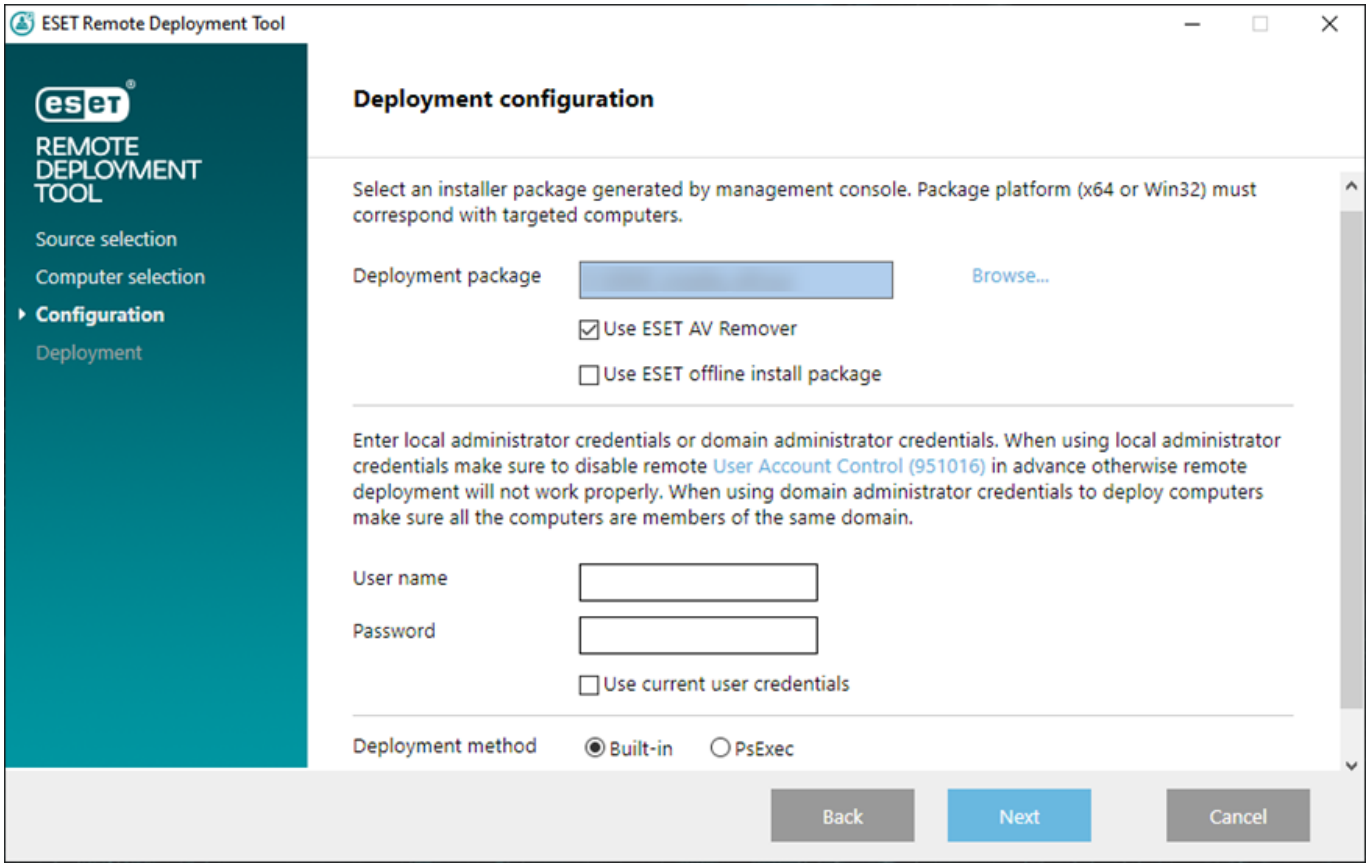
5. Clique em **Procurar** e selecione o pacote de instalação do pacote que você criou no Web Console ESET PROTECT (local ou na nuvem).

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

   • 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.

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**.

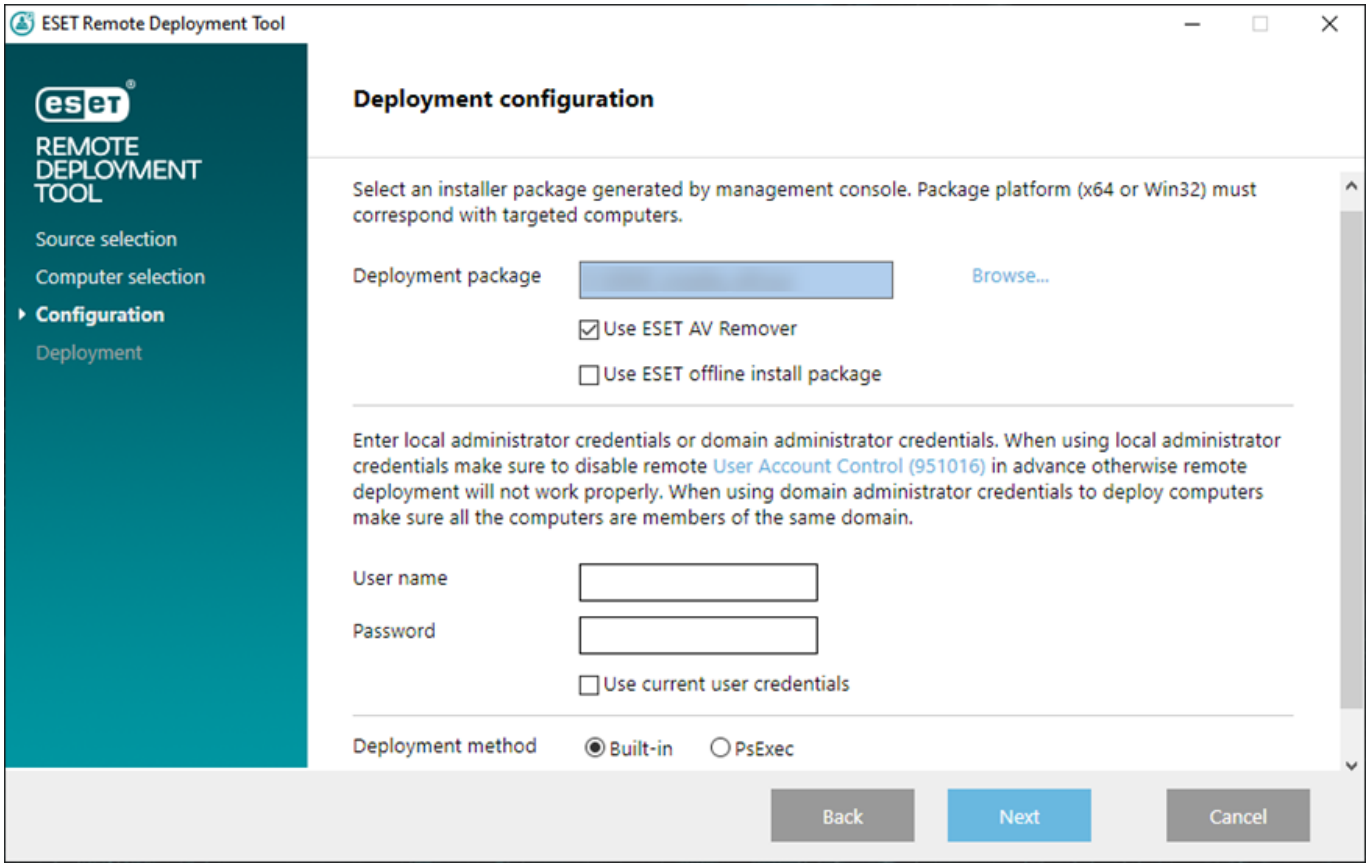
4. Clique em **Procurar** e selecione o pacote de instalação do pacote que você criou no Web Console ESET PROTECT (local ou na nuvem).

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

- 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.

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.

> A ESET Remote Deployment Tool é dedicada a implantar o Agente ESET Management apenas em computadores clientes com 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	Acesse o cliente a partir do Servidor ESET PROTECT; se 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. A conta de usuário Administrador deve ser ativada para executar a tarefa de instalação 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 11 faça o seguinte: • Clique em **Iniciar**, digite `Explorador de arquivos` na caixa **Pesquisar** e clique em **Opções do explorador de arquivos**. 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). Para definir uma senha do Agente ESET Management é preciso criar uma política para o Agente ESET Management adequada.

Se o Agente ESET Management estiver protegido por senha, você deverá fornecer a senha para desinstalar, reparar ou atualizar (com alterações).

Configurações do Agente ESET Management

Você pode definir configurações específicas do Agente ESET Management usando uma política do Agente ESET Management.

Não há políticas predefinidas para o Agente ESET Management. Para criar uma política do Agente ESET Management, clique em **Políticas** > **Nova política** e na seção **Configurações** selecione **Agente ESET Management**, onde você pode ajustar as seguintes configurações:

Configuração

A Configuração protegida por senha é um recurso de proteção do Agente ESET Management (somente para Windows). Clique em **Configurar** ao lado de **Configuração protegida por senha** para habilitar a proteção por senha de configuração do Agente ESET Management.

- A configuração protegida por senha foi aprimorada na versão 10.1. Defina a senha separadamente para a versão 10.0 do Agente e para versões anteriores, 10.1 e versões posteriores.
- Registre a senha em um local seguro. Se o Agente ESET Management estiver protegido por senha, você deverá fornecer a senha para desinstalar, reparar ou atualizar (com alterações).

Configurações avançadas

- **Proxy HTTP** – use um servidor proxy para facilitar o tráfego na internet de clientes da sua rede. 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.

- **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.

- **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:

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**.

Você pode solicitar a configuração do Agente em um computador gerenciado para ver as configurações de política do Agente aplicadas: Clique em **Computadores** > clique em um computador > **Detalhes** > **Configuração** > Solicitar configuração.

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.

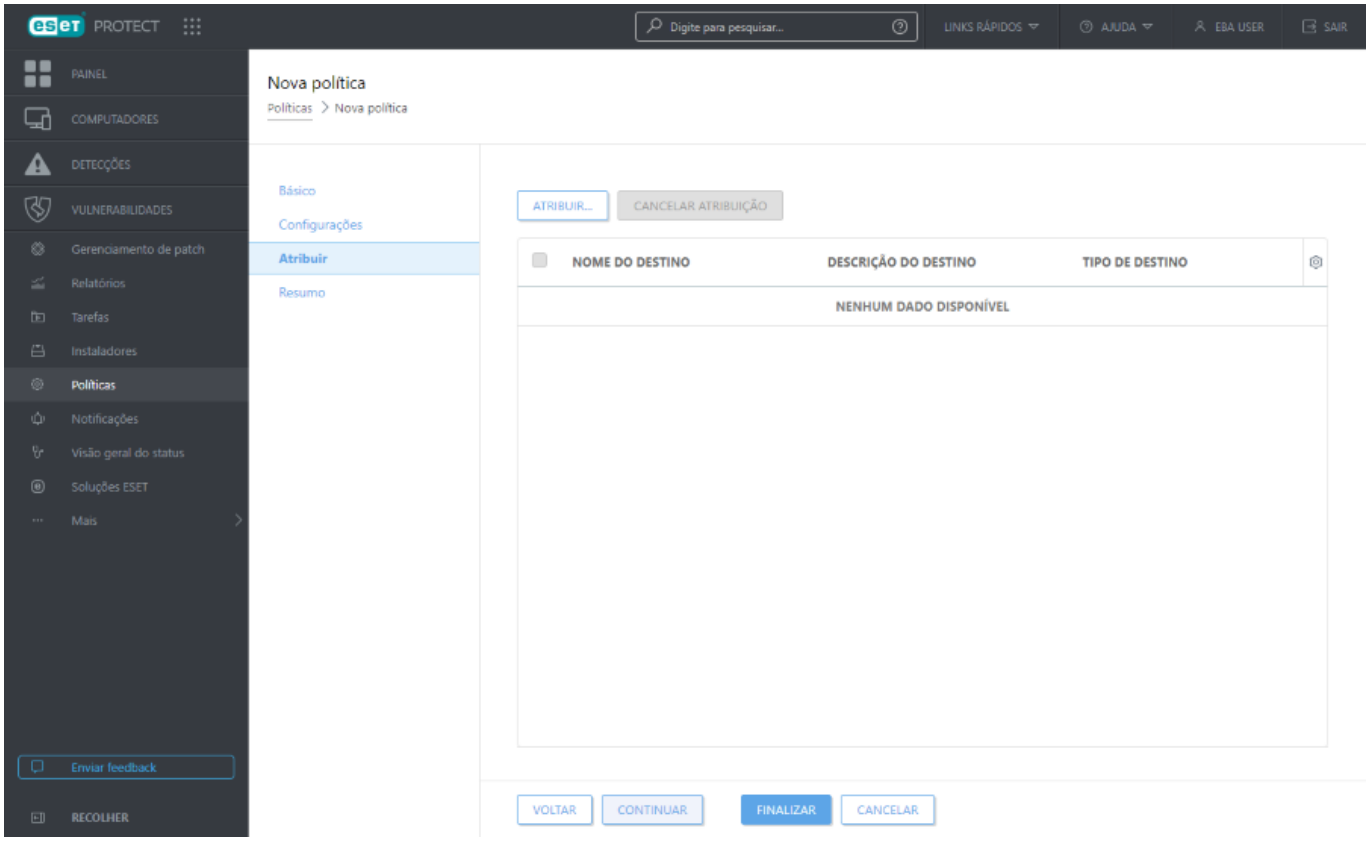
Configurações

Selecione **Agente ESET Management** na lista suspensa > abra **Configuração** > clique em **Configurar** ao lado de **Configuração protegida por senha** e digite a senha. Esta senha será necessária se alguém estiver tentando desinstalar ou reparar o Agente ESET Management em um computador cliente.

Registre a senha em um local seguro. Se o Agente ESET Management estiver protegido por senha, você deverá fornecer a senha para desinstalar, reparar ou atualizar (com alterações).

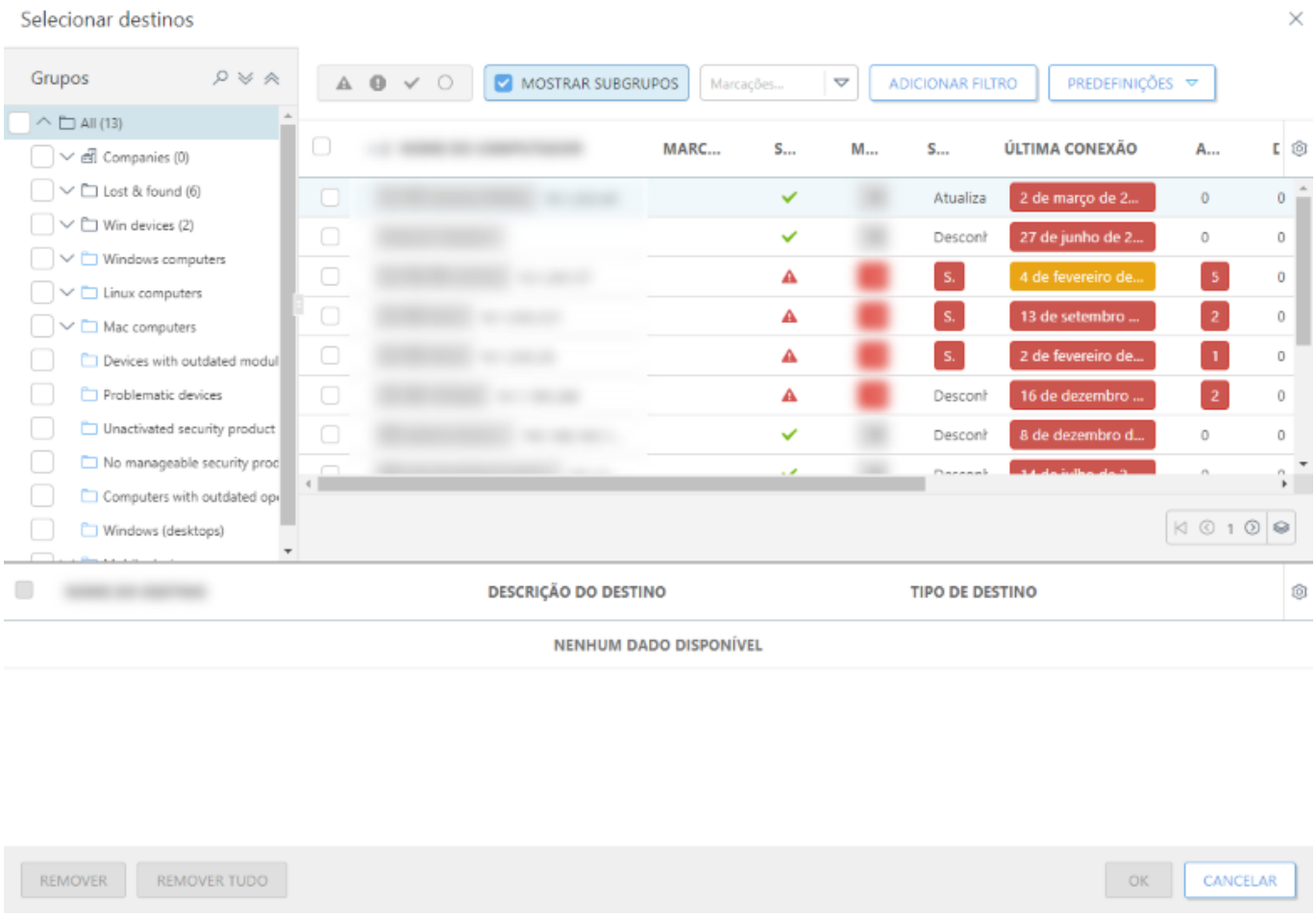
Atribuir

Especifique os clientes (computadores individuais 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 ESET PROTECT.

> 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 conectando ao seu Servidor ESET PROTECT, recomendamos que você solucione problemas do Agente ESET Management localmente na máquina do cliente.

Por padrão, o Agente ESET Management sincroniza com o ESET PROTECT a cada 10 minutos.

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 Servidor ESET PROTECT. 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.

Os problemas mais comuns que podem impedir o Agente ESET Management de se conectar ao ESET PROTECT é que o DNS não está funcionando adequadamente ou as portas foram bloqueadas por um firewall - consulte nossa lista de portas usadas pelo ESET PROTECT. Consulte nosso artigo da Base de Conhecimento para resolver o alerta **Dispositivo usando uma conexão de failover**.

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
Clientes gerenciados
Computadores
Detecções
Vulnerabilidades
Gerenciamento de patch
Relatórios
Tarefas
Instaladores
Políticas
Notificações
Visão geral do status
Soluções ESET
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.
- Os Usuários do MSP podem clicar em **Selecionar** ao lado do **Cliente MSP** para filtrar a exibição do painel do cliente selecionado.

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**, **ESET LiveGuard** e **ESET Inspect**.

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.

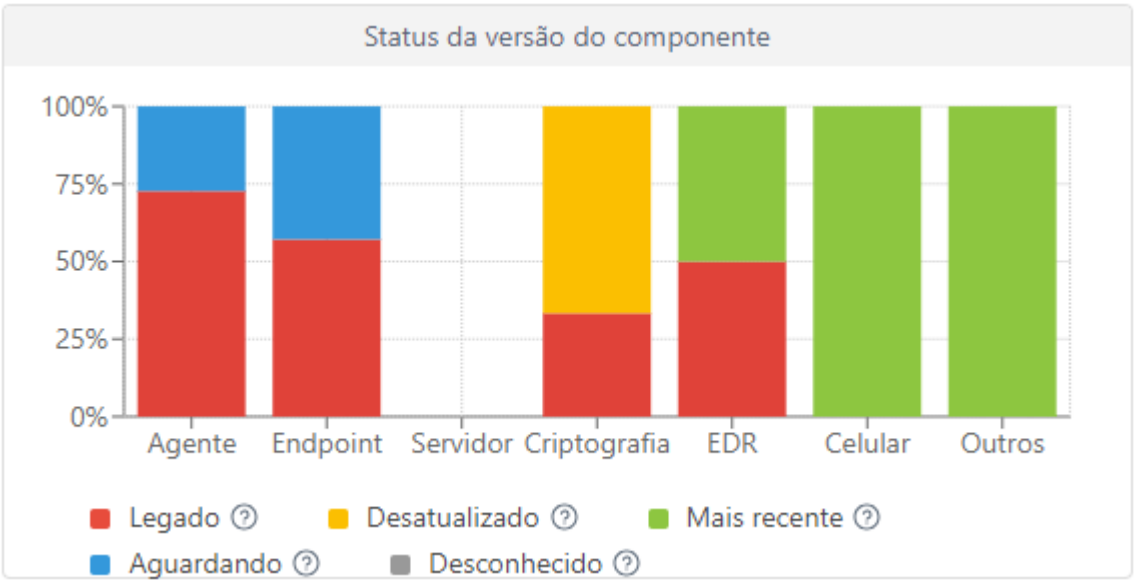
Status do dispositivo - Exibe o número de dispositivos gerenciados com base no tipo de produto de segurança instalado nas respectivas guias. Se nenhum produto de segurança daquele grupo está implantado, a guia vai exibir

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**.
> Como alternativa, você pode usar a Tarefa do cliente Atualizar do Agente para atualizar os 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.

ESET Inspect

Se você estiver usando o ESET Inspect esse painel oferece uma visão geral de dados estatísticos substanciais do ESET Inspect. Clique em um bloco para abrir o console ESET Inspect e ir de lá. Clique no ícone de engrenagem em cima (ao lado de) e selecione **Ocultar/Exibir ESET Inspect** para ocultar/exibir o painel.

Os blocos ESET Inspect mostram as informações a seguir:

- **Detecções não resolvidas por gravidade** – o número total de detecções não resolvidas e detecções não resolvidas por nível de gravidade – Informação, Aviso ou Crítico.

- **Detecções por gravidade nos últimos 7 dias** – um gráfico de linha composto pelo número de detecções por gravidade nos últimos sete dias.

- **10 principais computadores com detecções nos últimos 7 dias** - o nome do computador, o número de computadores por nível de gravidade de detecção (vermelho - crítico, amarelo - alerta, azul - informação) e o número total de detecções.

• **Computadores por gravidade de detecção** – um gráfico de rosca com o número de computadores por nível de gravidade de detecção – Crítico, Alerta e Informação.

• **Incidentes** – o número de incidentes (criados em ESET Inspect) por status (**Aberto**, **Em andamento**, **Em espera**, **Resolvido**, **Fechado** e **Inválido**). Clique em um número ao lado de um status de incidente para ver mais detalhes no ESET Inspect. Quando o Representante de Serviço ESET editar o incidente no ESET Inspect, você poderá ver o incidente marcado como **Investigado pela ESET**.

ESET Cloud Office Security

Se você usar o ESET Cloud Office Security, este painel fornecerá uma visão geral de dados estatísticos substanciais do ESET Cloud Office Security. Clique em um bloco para abrir o console ESET Cloud Office Security e ir de lá. Clique no ícone de engrenagem em cima (ao lado do ícone atualizar) e selecione **Ocultar/Exibir ESET Cloud Office Security** para ocultar/exibir o painel.

Os blocos ESET Cloud Office Security incluem as seguintes informações:

• **Usuários protegidos** – o número de usuários protegidos

• **Uso de licenças** – o número de licenças usadas e não usadas

• **Sites protegidos SharePoint** – o número de sites protegidos pelo SharePoint

• **Grupos protegidos Teams** – o número de grupos protegidos pelo Teams

• **10 usuários com mais detecções nos últimos 30 dias** – o nome e o e-mail com o número de detecções de e-mails e arquivos para os 10 usuários com mais detecções

• **Detecções nos últimos 30 dias** – im gráfico de histograma com o número de detecções nos serviços específicos (**Teams**, **SharePoint**, **E-mail**, **Drive**) nos últimos 30 dias. Clique em qualquer serviço no gráfico de histograma para abrir a página Detecções no ESET Cloud Office Security

• **Objetos em quarentena** – o número de objetos em quarentena nos serviços específicos nos últimos 7 e 30 dias. Clique em qualquer linha de serviço para exibir a página Quarentena no ESET Cloud Office Security

Computadores

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

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 aplicativos ESET instalados.

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).

ESET MDR

O ESET MDR fornece uma visão geral de incidentes e detecções do ESET Inspect. Para usar o ESET MDR, você precisa de uma licença do ESET Inspect e do nível **ESET PROTECT MDR**.

> **Disponibilidade do ESET MDR por país**
> O ESET MDR está disponível nos seguintes países: EUA, Canadá, Japão, Reino Unido, Holanda, França, Itália, países do DACH (Alemanha, Áustria, Suíça), países nórdicos (Suécia, Noruega, Dinamarca, Finlândia, Islândia), Eslováquia, República Tcheca, Ucrânia.

O serviço ESET MDR abrange todos os dispositivos gerenciados que executam o ESET Inspect. Siga as etapas abaixo para selecionar os dispositivos para os quais você deseja gerenciar a segurança independentemente do serviço ESET MDR:

1. Abra ESET PROTECT e navegue até **Computadores**.
2. Clique no ícone de engrenagem ao lado do grupo pai estático existente e selecione **Novo grupo estático.**
3. Digite `exempt` no campo **Nome** e clique em **Concluir**.
4. Selecione o grupo pai e selecione os dispositivos que você deseja incluir no grupo isento.
5. Clique no botão **Computador** > **Gerenciar** > **Mover para Grupo** e selecione o grupo `exempt`.

Os dispositivos no grupo `exempt` estão sob seu gerenciamento — você pode lidar com incidentes manualmente sem as ações de resposta aplicadas automaticamente.

> Você precisa dos seguintes conjuntos de permissões para exibir **ESET MDR** no Painel:
> • **ESET MDR relatórios**—Usar
> • **Acesso somente leitura ao ESET Inspect** – Leitura
> Você pode ver dados em blocos com base em seus Conjuntos de Permissões personalizados em ESET Inspect e ESET PROTECT.

Clique em um bloco para abrir o ESET Inspect Web Console prossiga a partir daí.

Os blocos **ESET MDR** mostram as informações a seguir:

• **Incidentes**: o número de incidentes por nível de gravidade nos últimos sete dias —**Total**, **Alto**, **Médio** e **Baixo**

• **Principais incidentes não resolvidos**: uma lista do maior número de incidentes nos últimos sete dias — **Nome do incidente**, **Autor**, **Data de criação**, **Dispositivos afetados**, **Status** e **Atribuído a**

• **Status do incidente**: um gráfico de rosca com o número de incidentes por status nos últimos sete dias — **Aberto**, **Em andamento**, **Em espera**, **Resolvido**, **Fechado** e **Inválido**

• **Principais dispositivos afetados**: uma lista do maior número de dispositivos afetados por seu nível de

gravidade nos últimos sete dias —**Nome do dispositivo**, **Incidentes** (nível de gravidade —**Informativo**, **Aviso** ou **Crítico**), **Nome do grupo** e **Última visualização**

• **Ações de resposta**: um gráfico de rosca com o número de ações de resposta a um incidente nos últimos sete dias —**Bloquear**, **Limpar e bloquear**, **Isolar** e **Encerrar o processo**

• **Pipeline de incidentes**: **número total de detecções**, **Número de detecções relacionadas a incidentes** e **Número de incidentes criados** nos últimos sete dias

• **Incidentes no tempo**: um gráfico de linhas com o número de incidentes encontrados nos últimos sete dias por nível de gravidade —**Alto**, **Médio** e **Baixo**

Em cada bloco, você pode clicar no botão ⋮ para:

• **Exibir tudo**: clique para entrar no ESET Inspect Web Console. Você será redirecionado para a página específica com o filtro definido (Tempo de criação de 7 dias)

• **Atualizar**: clique para atualizar o bloco específico

Veja também o relatório ESET MDR.

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 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, gerar relatórios com base em modelos de relatório e ler seu painel
> • **Uso**: o usuário pode modificar seu painel com modelos de relatório disponíveis
> • **Gravação**: criar/modificar/remover modelos 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:

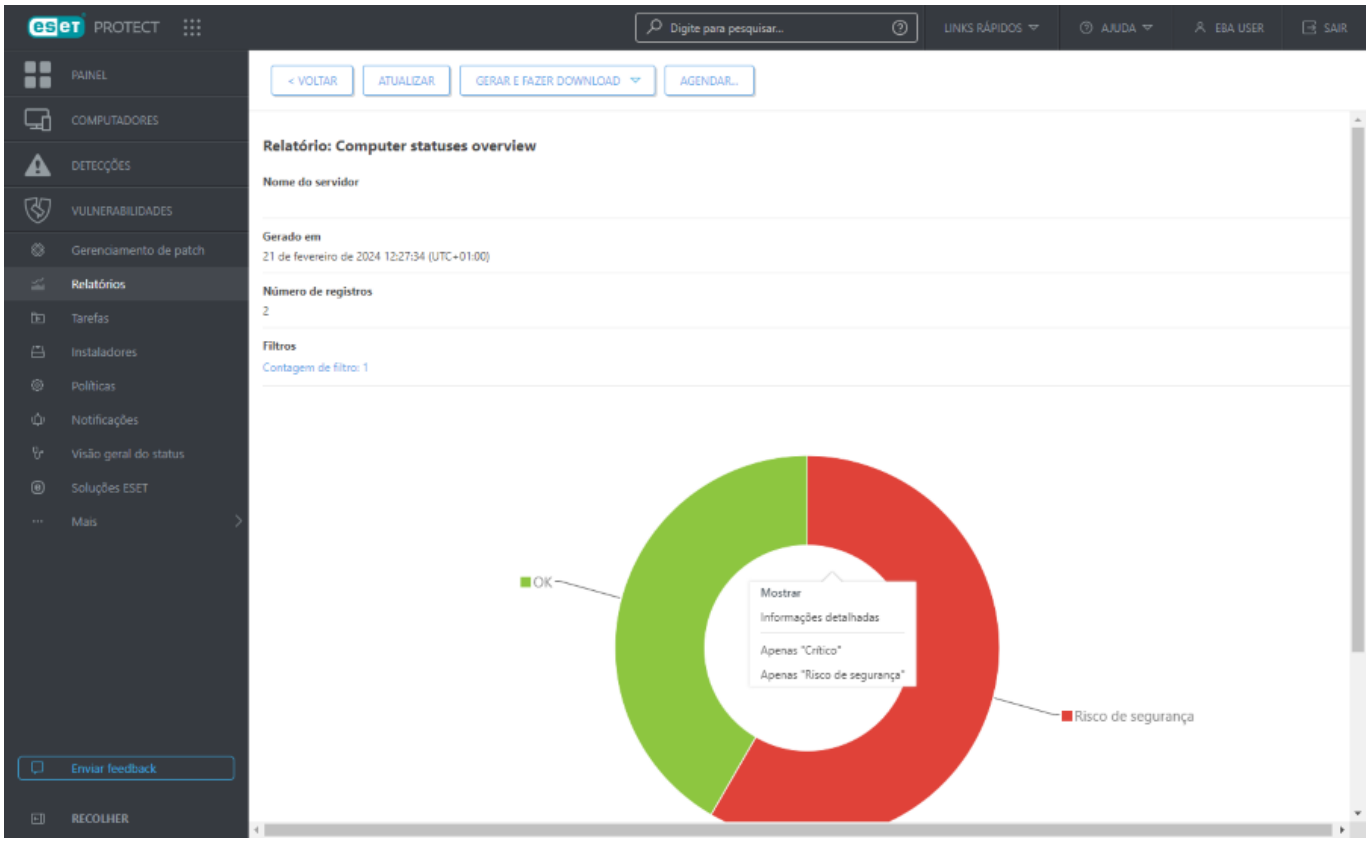
  - Gerenciar políticas

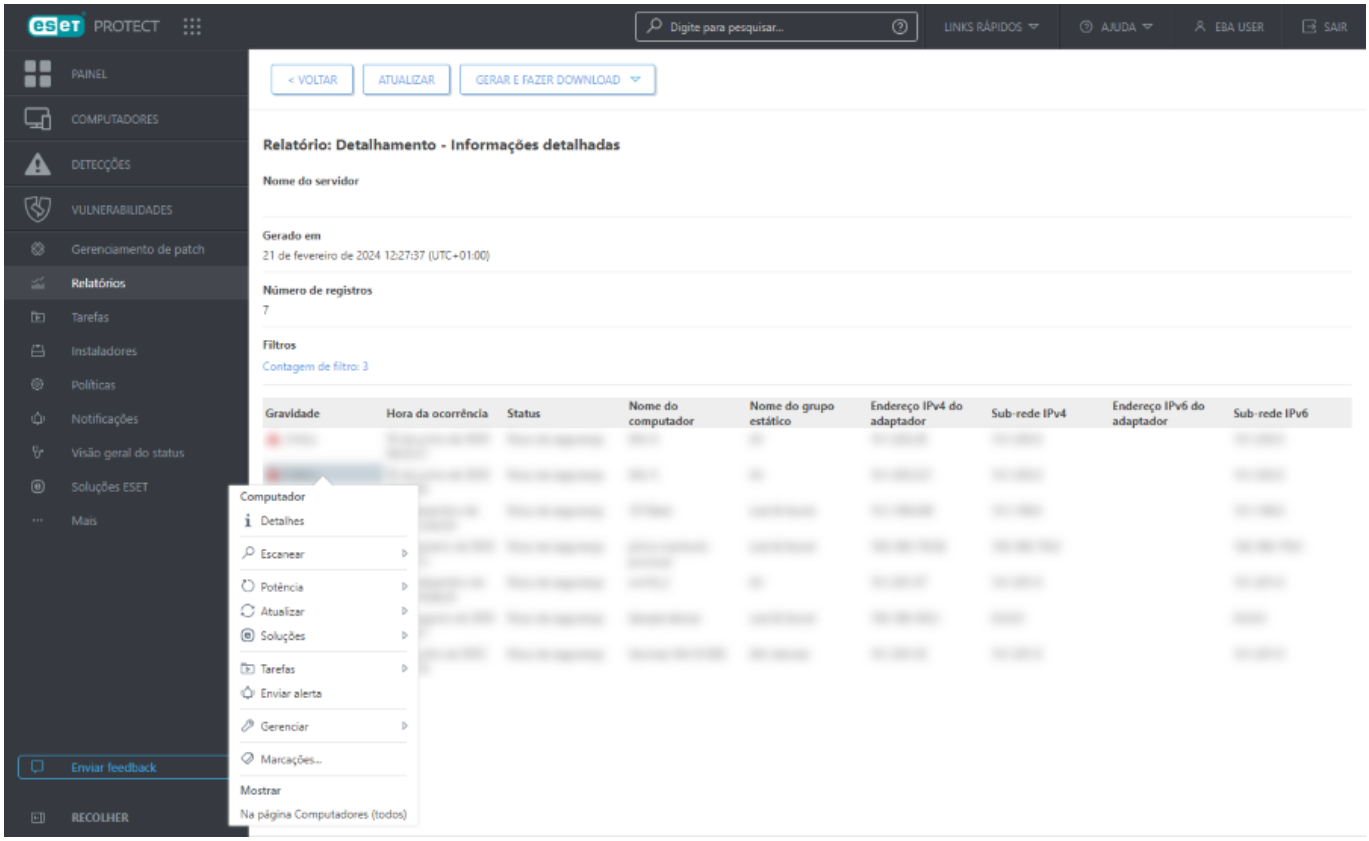
  - **Nova política**

- **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.





Clientes gerenciados

A seção **Clientes Gerenciados** no menu principal ESET PROTECT está disponível somente para os usuários do Provedor de Serviços Gerenciados (MSP).

Na seção **Clientes gerenciados**, o usuário MSP pode ver a lista de clientes gerenciados:

- Clique no nome do cliente para ver os detalhes do cliente – esses são detalhes do grupo estático porque os grupos estáticos no ESET PROTECT representam os clientes
- Clique em um número na tabela para obter detalhes sobre os dispositivos, detecções (não resolvidas) e licenças do cliente

Você pode personalizar a tabela principal (ajustar as colunas visíveis, adicionar ou remover colunas).

Filtrando clientes gerenciados

Você pode filtrar os clientes gerenciados pelo nome do cliente:

- Em **Clientes gerenciados** –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 também pode usar as predefinições de filtro
- Em outras seções do Web Console – Painel, ao agendar ou gerar um relatório

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.

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.

> Os dispositivos móveis inscritos devem se conectar ao ESET PROTECT a cada 120 dias para evitar problemas de conexão. Você pode ver essas informações no link do e-mail de inscrição ou no código QR.
> Não inscreva um dispositivo sobressalente com antecedência. Recomendamos inscrever apenas um dispositivo sobressalente que será usado dentro de 120 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.

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.

  - **Protegido pela ESET** – protegido por um produto ESET – Desktop, Mobile, Servidor, Servidor de e-mail, Servidor de gateway, Servidor de colaboração, Servidor de arquivos.

  - **ESET PROTECT** – componentes ESET PROTECT individuais – Agente ESET Management, Rogue Detection Sensor.

  - **Outros** – ESET LiveGuard, ESET Inspect Connector, ESET Full Disk Encryption, ESET Bridge, Gerenciamento de patch e de vulnerabilidade ESET.

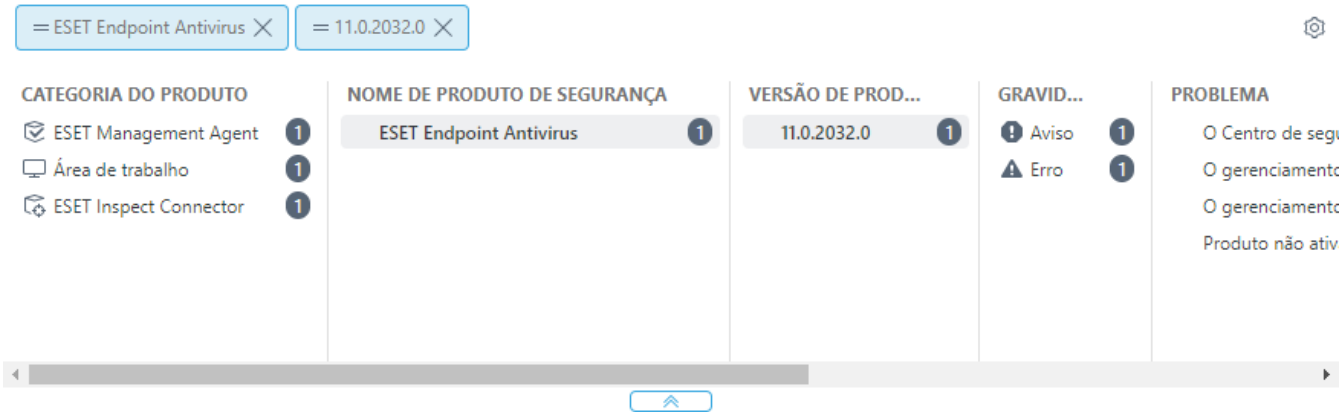
- Caixa de seleção **Exibir Subgrupos** - mostra subgrupos do grupo atualmente selecionado.

- 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.

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
- **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:

oAmarelo (erro) – O computador não conecta há 2-14 dias.

oVermelho (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.

Você precisa da licença ESET LiveGuard Advanced para ativar o ESET LiveGuard Advanced.

Ações disponíveis:

• **Ativar** – Clique em **Ativar** para configurar a tarefa de ativação e política para o produto ESET LiveGuard Advanced na máquina atual. Alternativamente, clique em um computador ou ícone de engrenagem ao

lado de um grupo estático e selecione **Soluções** > **Ativar ESET LiveGuard**. Na janela de configuração, selecione o nível de proteção e clique em **Ativar**.

- **Proteção ideal (recomendado)** – arquivos em risco, incluindo tipos de documentos compatíveis com macros, serão enviados a um servidor seguro do ESET para o escaneamento automatizado e análise comportamental. O acesso aos arquivos é limitado até que eles tenham sido avaliados como seguros.
- **Proteção básica** – o ESET LiveGuard Advanced vai escanearum conjunto limitado de arquivos.

- Arquivos enviados – a lista de todos os arquivos enviados aos servidores ESET.

Depois de ativar o ESET LiveGuard Advanced:

- O painel ESET LiveGuard exibirá os relatórios aprimorados do ESET LiveGuard Advanced da sua rede gerenciada.
- Cada dispositivo com o ESET LiveGuard Advanced terá o Sistema de Reputação ESET LiveGrid® e Sistema de Feedback ESET LiveGrid® habilitados. Verifique as políticas do seu dispositivo.

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 Servidor ESET PROTECT 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 Servidor ESET PROTECT. 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** > **Desligar** para parar o modo de Diagnóstico.

> O limite de tamanho de arquivo para entrega do relatório por dispositivo é de 15 MB. Você pode acessar relatórios do Web Console na seção **Detalhes** > **Relatórios**. Se os relatórios coletados pela tarefa forem maiores que 15 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.

Se você gerencia dispositivos Android e aplicou uma política para permitir as exceções do aplicativo (**Controle de aplicações** > **Ativar controle de aplicações** > **Ativar bloqueio** > **Exceções**):

- gerenciamento de dispositivo móvel local (ESET PROTECT On-Prem) – os aplicativos na lista são destacados e têm o status de segurança **Permitido por exceção**.

• Gerenciamento de dispositivo móvel na nuvem (ESET PROTECT) – os aplicativos na lista não são destacados e não têm nenhum status de segurança.

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 ESET Management estiver protegido por senha, você deverá fornecer a senha para desinstalar, reparar ou atualizar (com alterações). Recomendamos redefinir algumas configurações que você não quer manter (por exemplo, proteção por senha) para as configurações padrão usando uma política antes do dispositivo ser removido do gerenciamento.
• Todas as tarefas sendo executadas no agente serão abandonadas. O status de execução **Em execução**, **Concluído** ou **Com falha** dessa tarefa poderá não ser exibido com precisão no console da Web ESET PROTECT, dependendo da replicação de dados.
• Depois do Agente ser desinstalado é possível gerenciar seu produto de segurança através da EGUI integrada ou do eShell.

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 de Agentes 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**, **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.

- **Arquivos enviados** – uma lista de todos os arquivos enviados aos servidores ESET.

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:

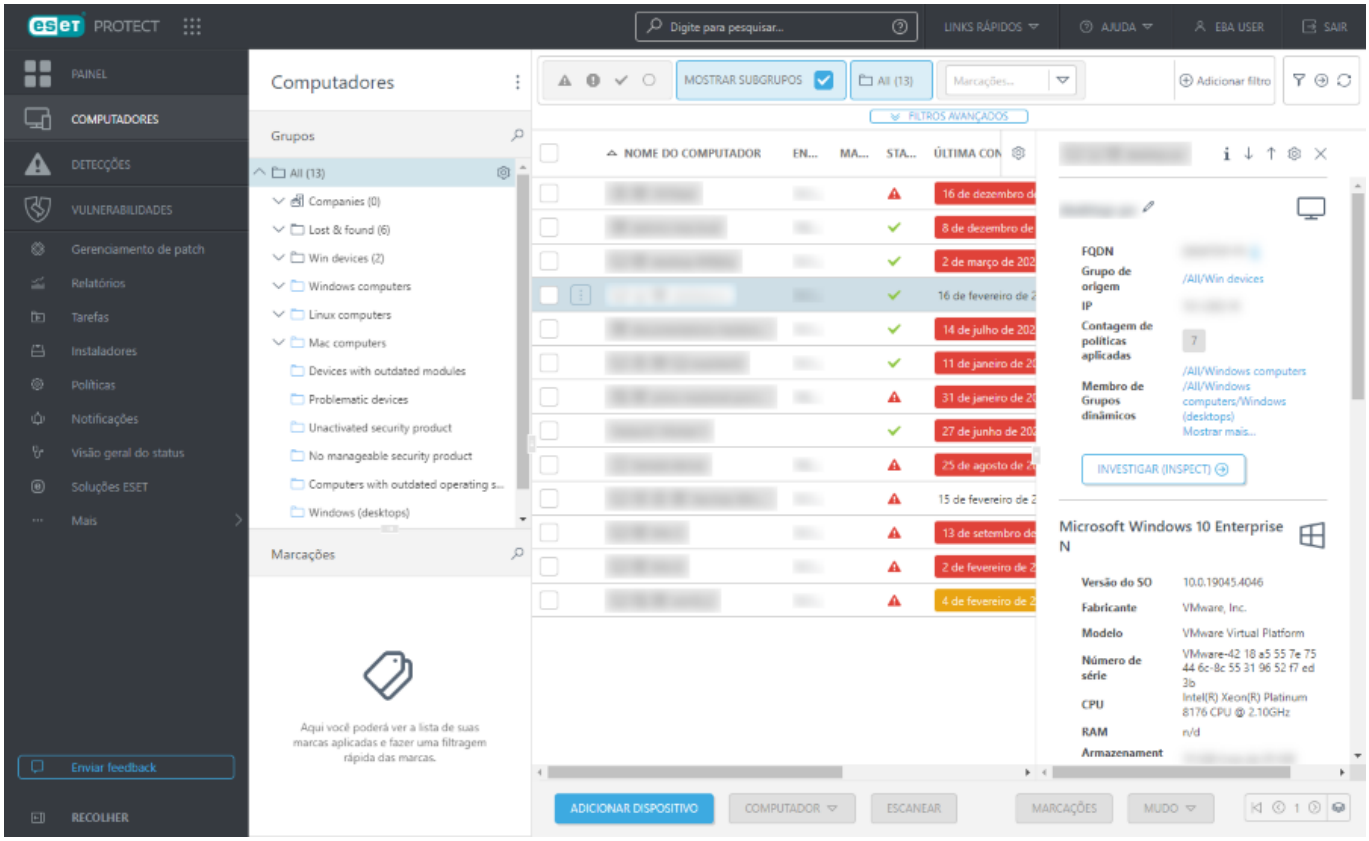
- **Mostrar detalhes** – abre o menu Detalhes do computador

- **Próximo** – mostrar o próximo dispositivo no painel lateral de visualização do computador.

- **Anterior** – exibe o dispositivo anterior no painel lateral de Visualização do computador.

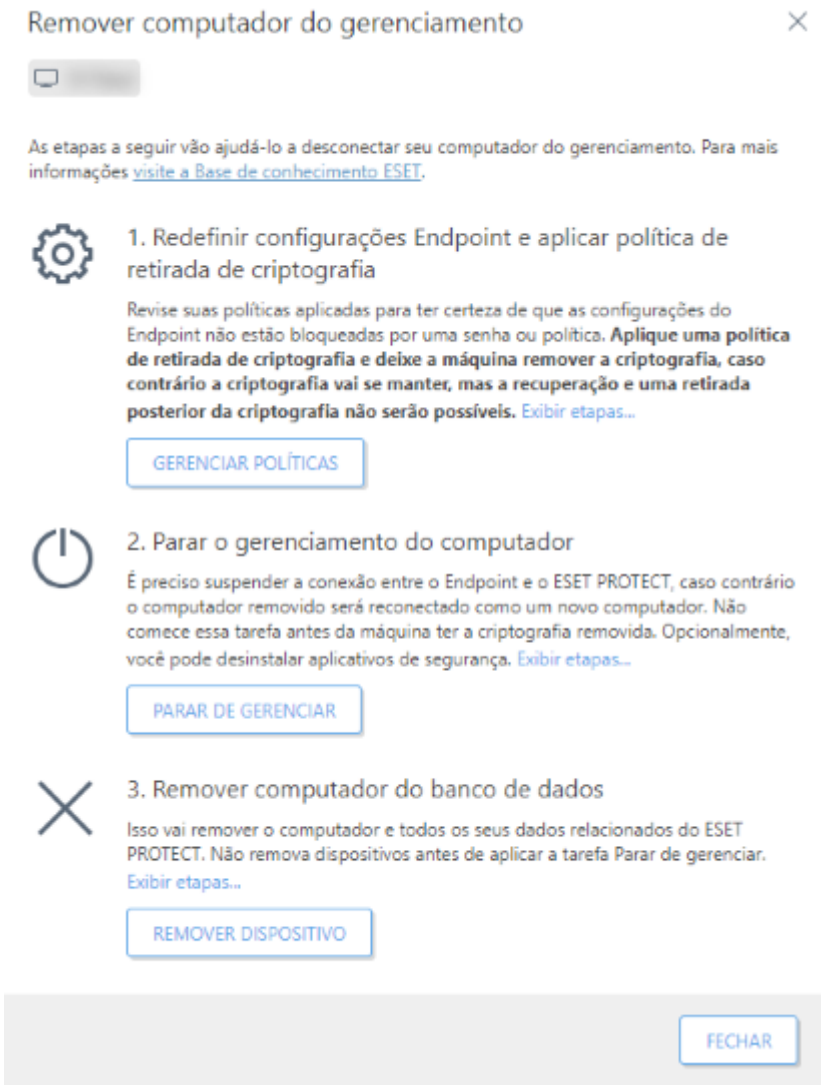
- **Gerenciar conteúdo para Detalhes do computador** – você pode gerenciar quais seções do painel lateral de visualização do computador serão exibidas e em qual ordem.

- **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 uma senha estiver definida para acessar a configuração do produto Endpoint, clique em **Desabilitar senha** para atribuir a política **Desabilitar proteção por senha** ao computador selecionado. Alternativamente, você pode criar uma nova política para remover a senha (selecione para definir uma senha, mas não digite nenhuma senha) e atribuí-la ao computador. Para computadores criptografados com ESET Full Disk Encryption, siga as etapas de remoção da criptografia.

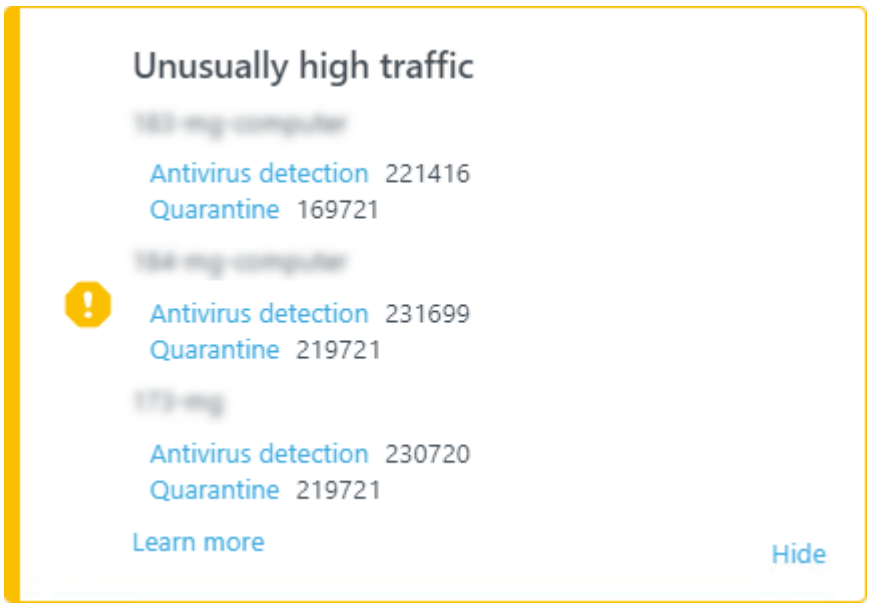
2. **Interromper gerenciamento do computador** - Execute uma tarefa Interromper gerenciamento ou desinstale o Agente ESET Management ou produto de segurança ESET localmente em um computador. Isso suspende a conexão entre o computador e o ESET PROTECT.

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.

Tráfego alto incomum de computadores gerenciados

Quando o administrador do Web Console entrar, ele pode ver um aviso de janela de um tráfego alto incomum de computadores gerenciados.



A sobrecarga de relatórios deixa a rede mais lenta entre os computadores gerenciados e o ESET PROTECT:

- Dados dos computadores gerenciados levam mais tempo para serem enviados para o ESET PROTECT.
- O Web Console pode não exibir o estado atual dos computadores gerenciados afetados.

O administrador do Web Console deve resolver relatórios de tráfego alto incomuns (por exemplo, um arquivo na quarentena detectado no Endpoint ou no ESET PROTECT).

A janela desaparece quando o número de relatórios de tráfego alto incomum diminui.

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	✔
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** – inscreva novamente 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. **Habilitar Gerenciamento de patch e de vulnerabilidade** – Clique em ao lado de um grupo estático e selecione **Soluções** > **Habilitar o Gerenciamento de patch e de vulnerabilidade** para habilitar o Gerenciamento de patch e de vulnerabilidade no computador.	✔	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
Escaneador do Active Directory	Use o token de acesso gerado para autenticar o Escaneador do ESET Active Directory para conectar ao ESET PROTECT e sincronizar o Active Directory com o grupo estático selecionado.	✔	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:

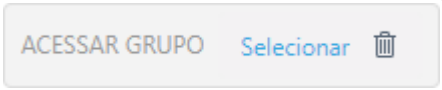
- **Todos** - Este é um grupo principal de todos os computadores na Servidor ESET PROTECT. Todos os objetos criados pelo administrador estão contidos neste grupo (por padrão). É sempre exibido e não pode ser renomeado. O acesso a este grupo dá aos usuários acesso a todos os subgrupos, portanto ele deve ser distribuído com cuidado.

- **Perdido e encontrado** - um grupo secundário do grupo **Todos**. Cada novo computador que se conecta ao Servidor ESET PROTECT pela primeira vez é automaticamente exibido nesse 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

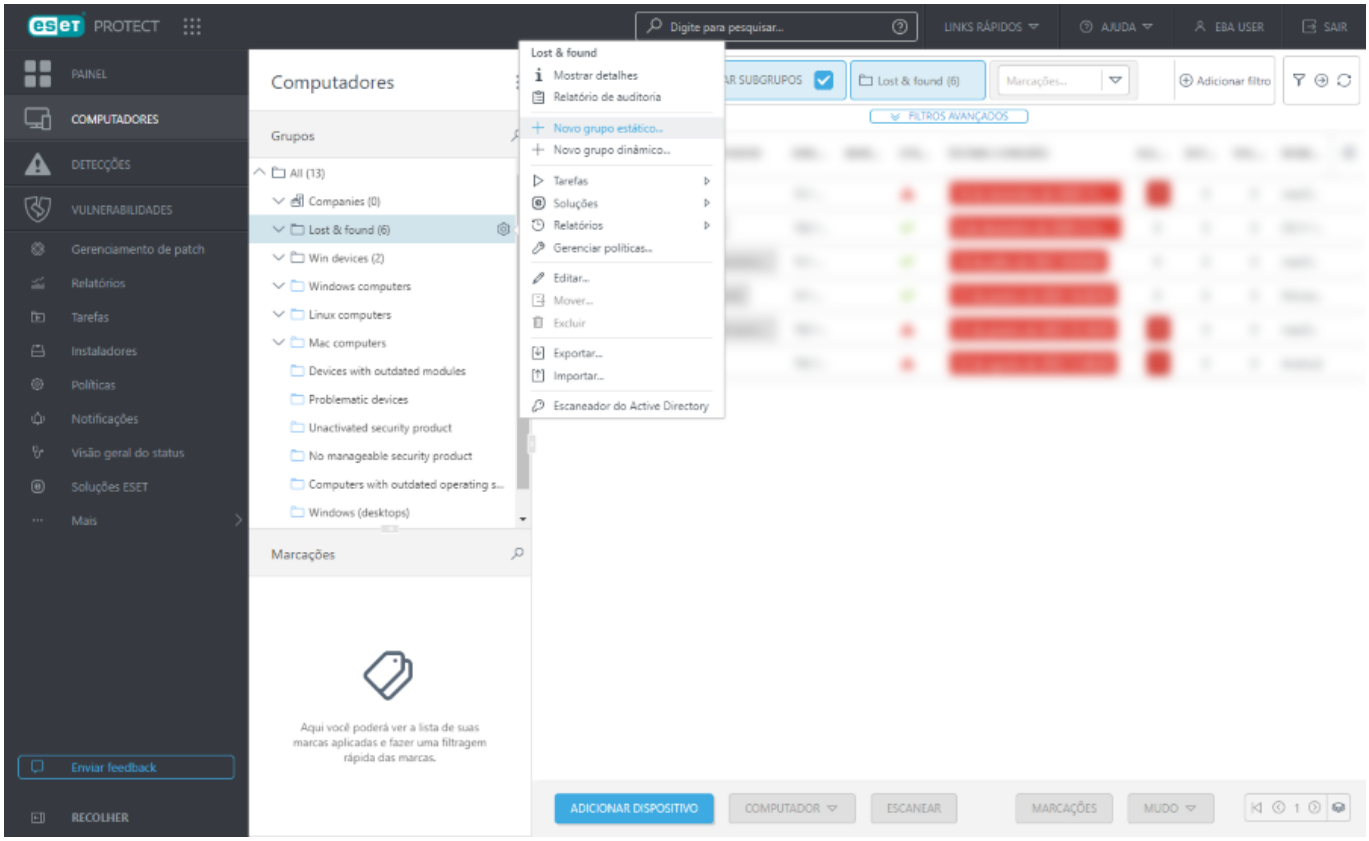
Se ainda existirem alguns objetos no grupo estático, a operação vai falhar. Há um botão de filtro do **Grupo de acesso** localizado em cada menu (por exemplo, **Instaladores**) com objetos.



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**.



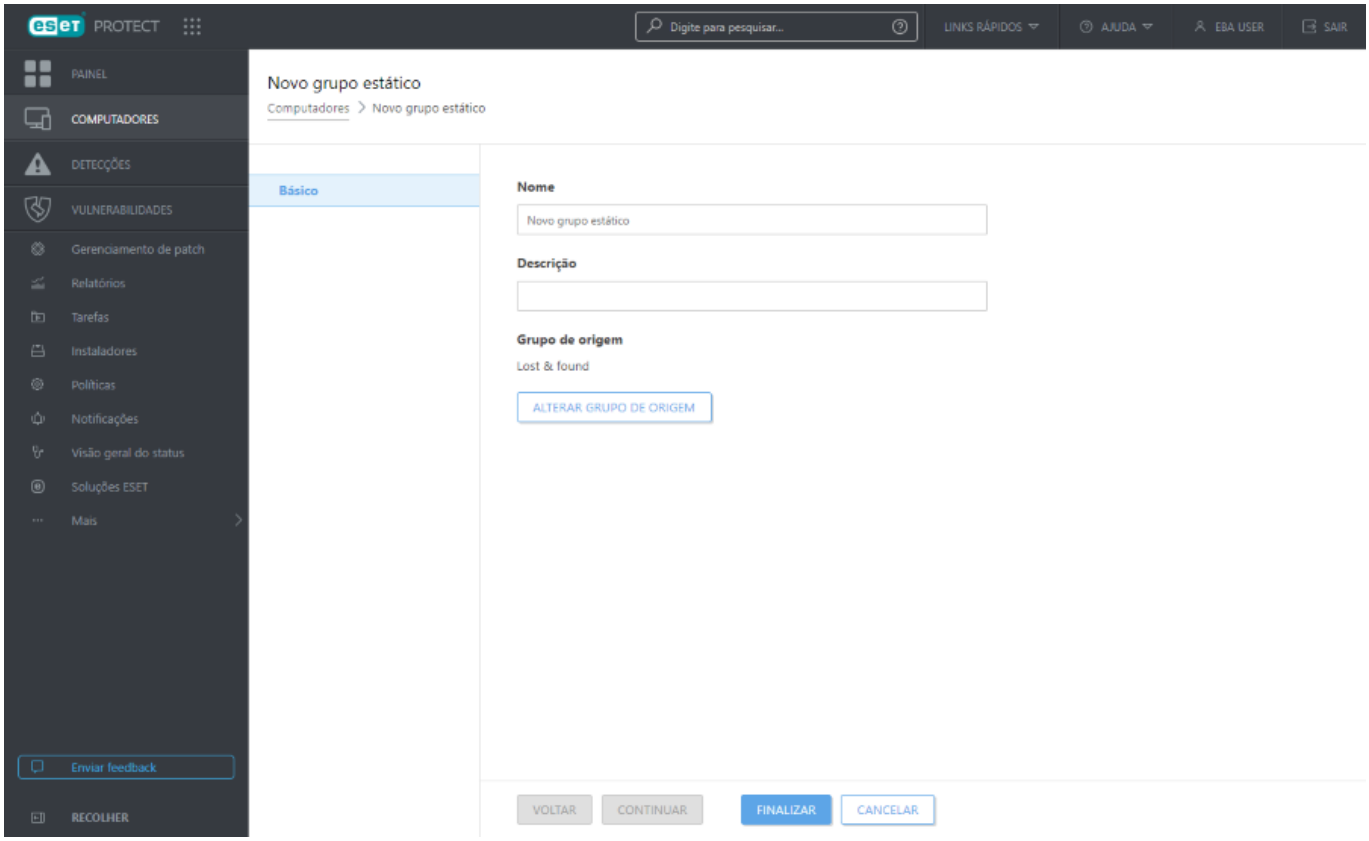
Básico

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.

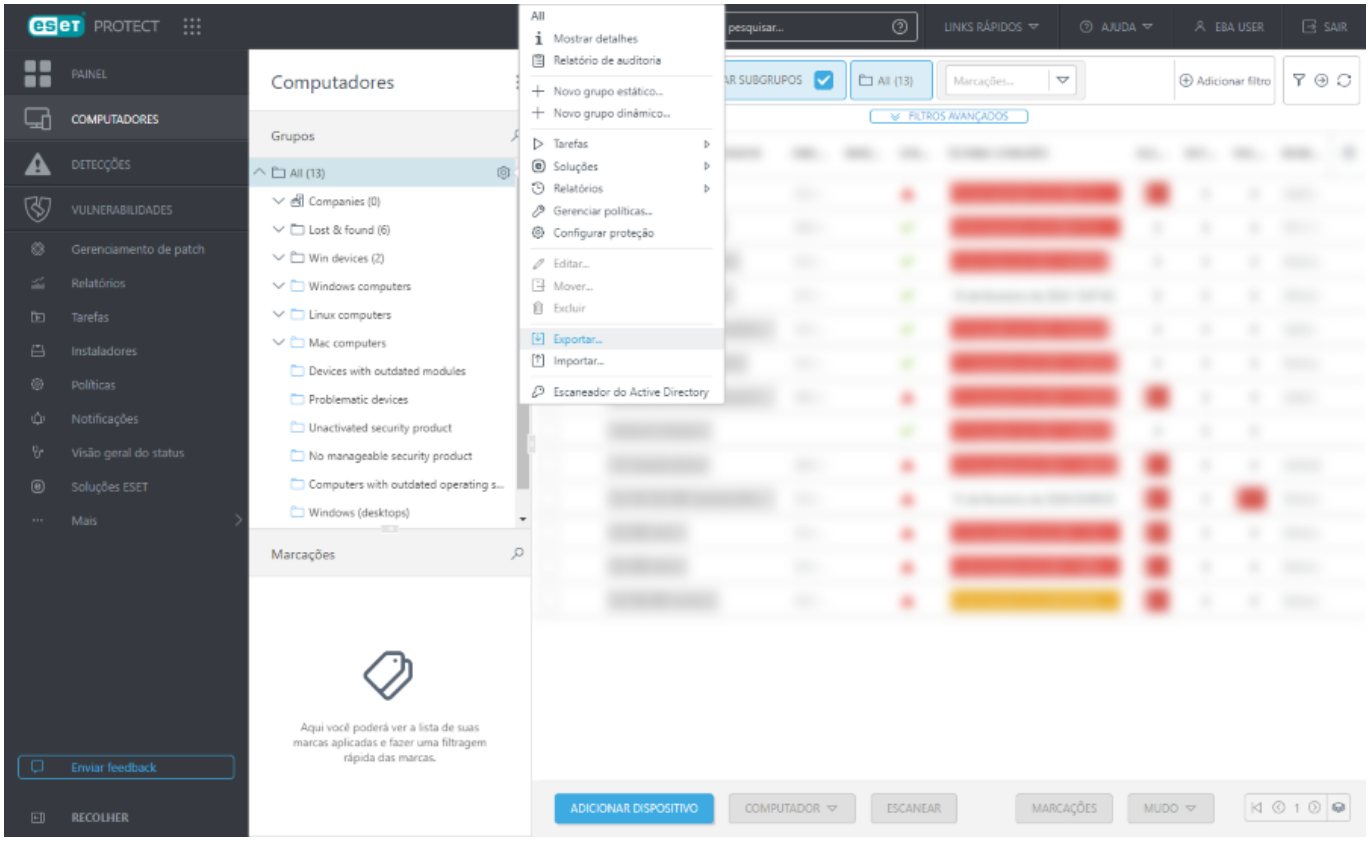


Exportar grupos estáticos

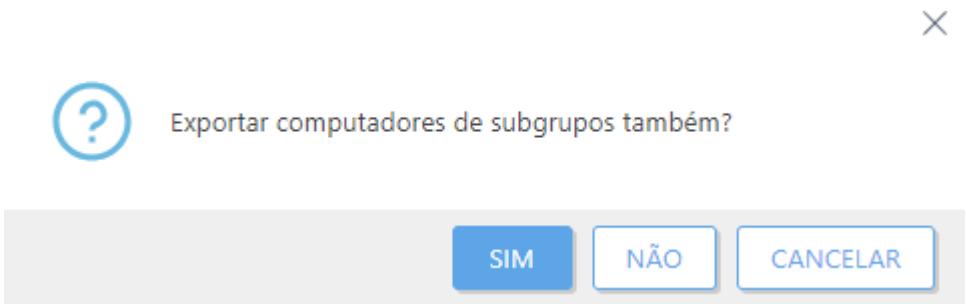
A exportação de uma lista de computadores que estejam na estrutura ESET PROTECT é simples. Você pode exportar a lista e armazená-la como um backup, a fim de que possa importar a lista de volta no futuro, por exemplo, se quiser restaurar a estrutura de grupo.

> 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.

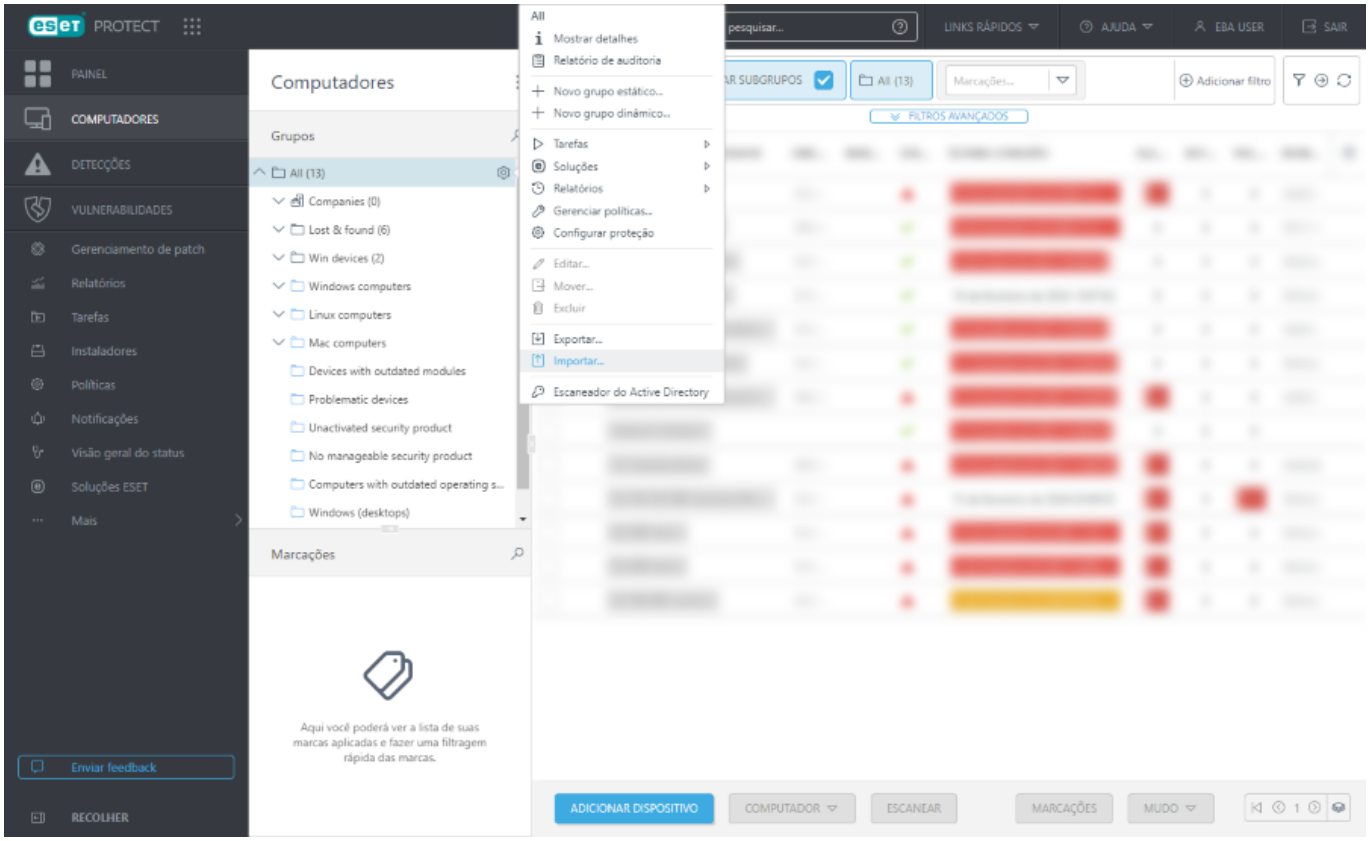


4. O arquivo será salvo em formato *.txt*.

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 **Escolher arquivo** e navegue até o arquivo *.txt*. Cada linha no arquivo deve conter um caminho completo para o nome do computador/endereço IP (com uma barra invertida como separador). Por exemplo:

```
All\Lost & found\Computer_Name
All\Lost & found\10.20.30.40
```

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.

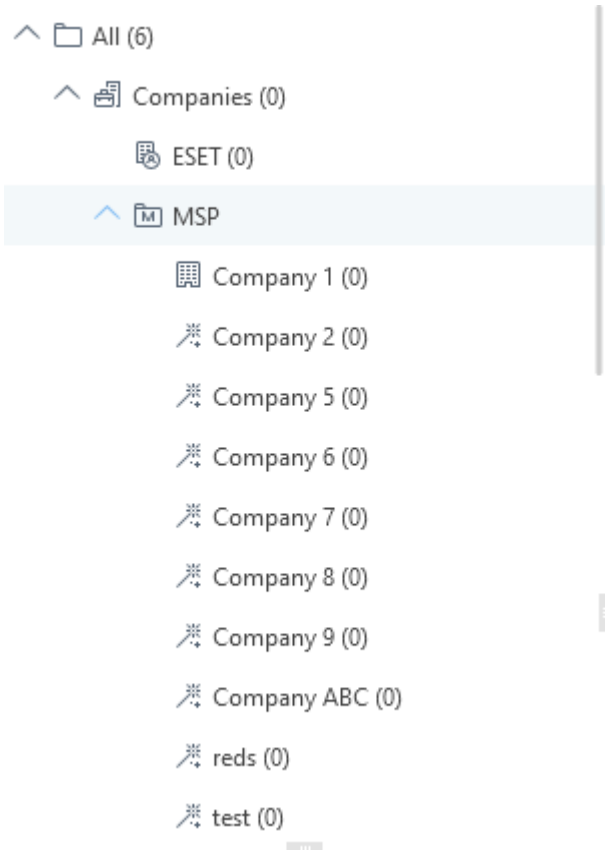
Árvore do grupo estático para ESET Business Account / ESET MSP Administrator

Se você implantou o ESET PROTECT do ESET Business Account, a estrutura ESET Business Account da sua empresa (incluindo sites) aparecerá na árvore do Grupo estático (um novo recurso no ESET PROTECT versão 3.4).

Se você implantou o ESET PROTECT do ESET MSP Administrator, a estrutura ESET MSP Administrator aparecerá 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**.



Em **Empresas**, você pode ver:

- ESET Business Account empresa – se você implantou o ESET PROTECT de ESET Business Account.
- ESET MSP Administrator árvore – se você implantou o ESET PROTECT de ESET MSP Administrator.
- Ambas as árvores – se você implantou o ESET PROTECT de uma conta mista.

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 com acesso **Personalizado** ESET PROTECT 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 vários Grupos dinâmicos pré-definidos para seus computadores e dispositivos móveis disponíveis depois de ter criado 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.

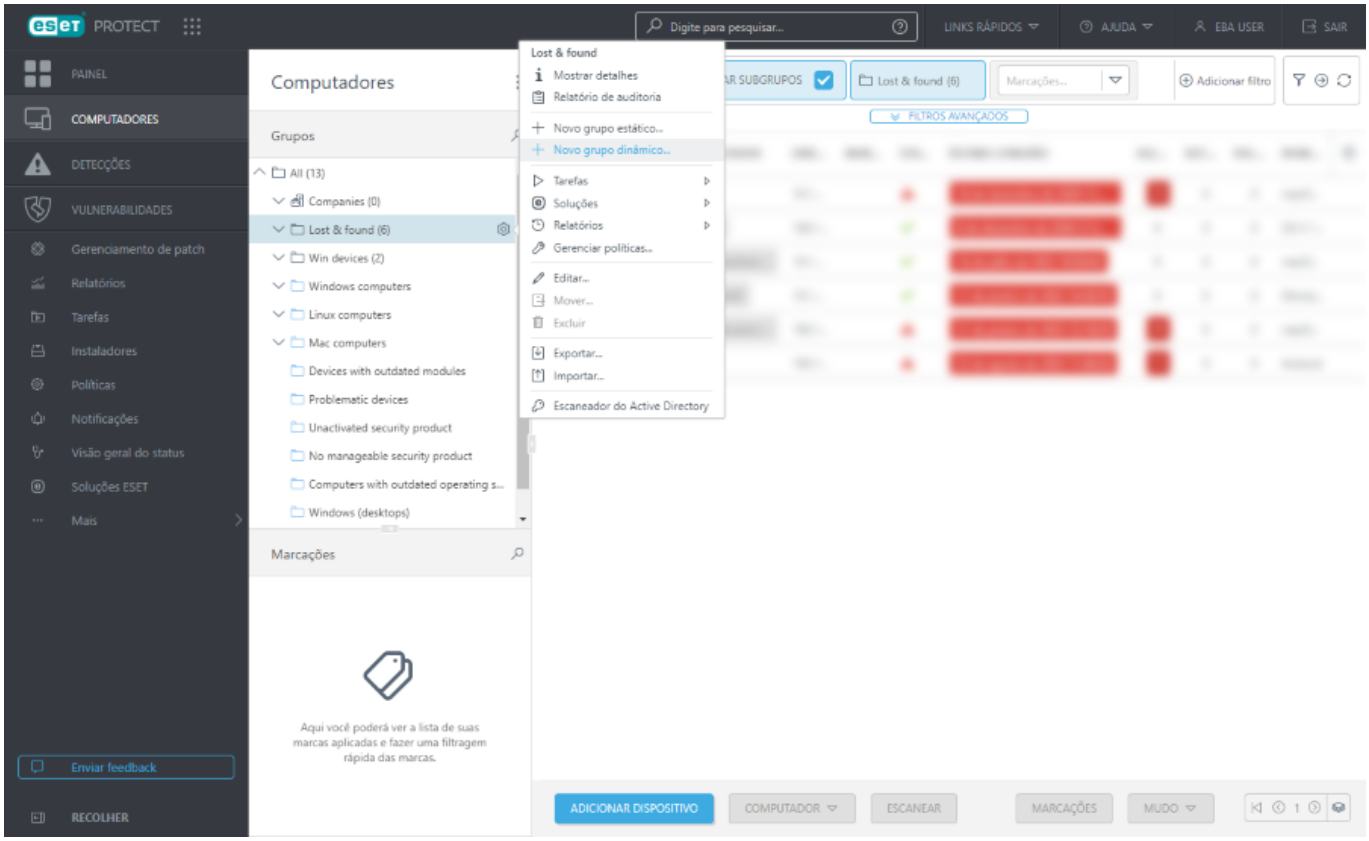
Um grupo dinâmico pode estar dentro de (sob) um grupo estático ou grupos dinâmicos. Porém o grupo estático não pode estar dentro de um grupo dinâmico. Todos os Grupos dinâmicos sob um certo Grupo estático filtram apenas os dispositivos daquele Grupo estático. Se um Grupo dinâmico estiver dentro de outro 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

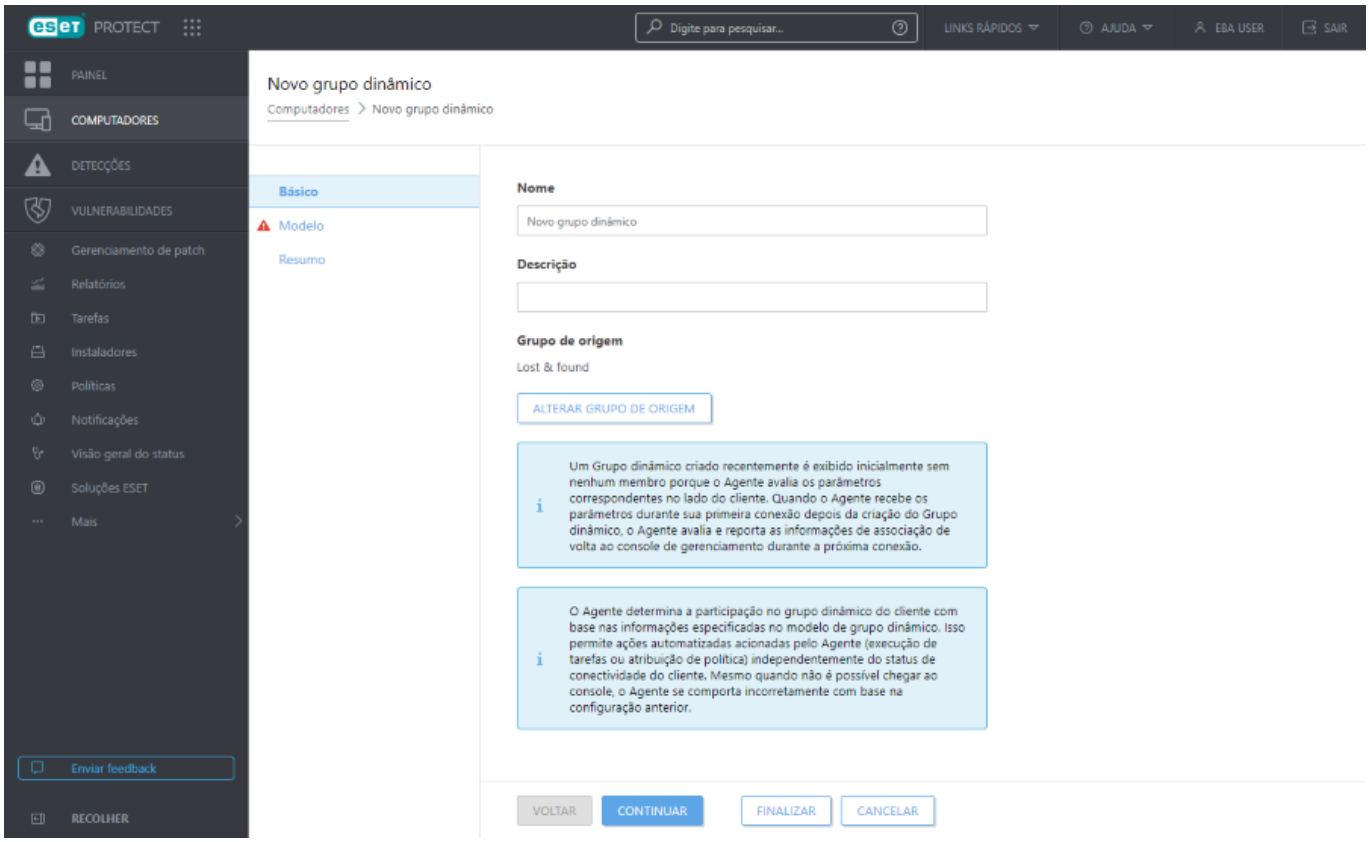
Para criar um Novo grupo dinâmico, siga as etapas abaixo.

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**.



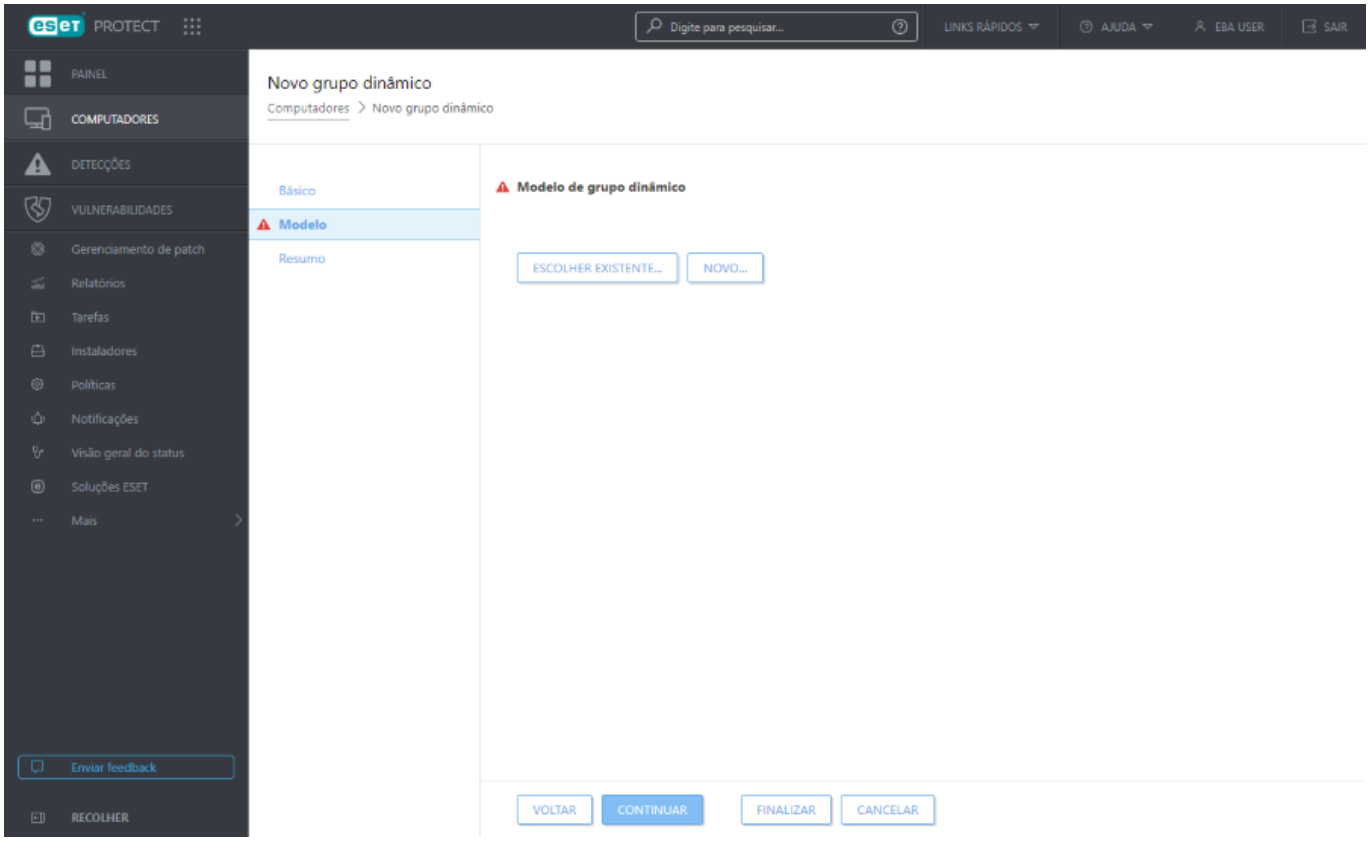
4. Clique em **Modelo**. Todo Grupo dinâmico é criado de um Modelo que define como o grupo filtra os computadores do cliente. Um número ilimitado de Grupos dinâmicos pode ser criado a partir de um modelo.

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

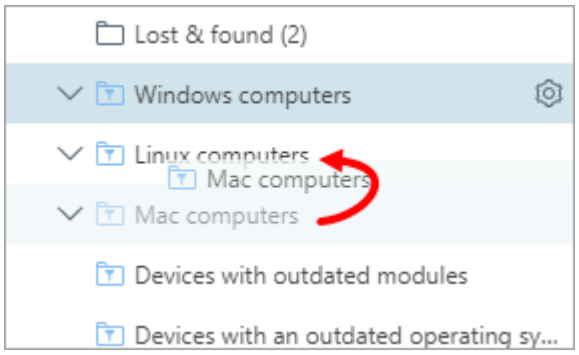
Um Grupo dinâmico pode ser membro de qualquer outro grupo, inclusive de Grupos estáticos. Um Grupo estático não pode ser movido para dentro de um Grupo dinâmico. Também não é permitido mover Grupos estáticos pré-definidos (por exemplo, o grupo estático **Perdido e encontrado**) para qualquer outro grupo. 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.

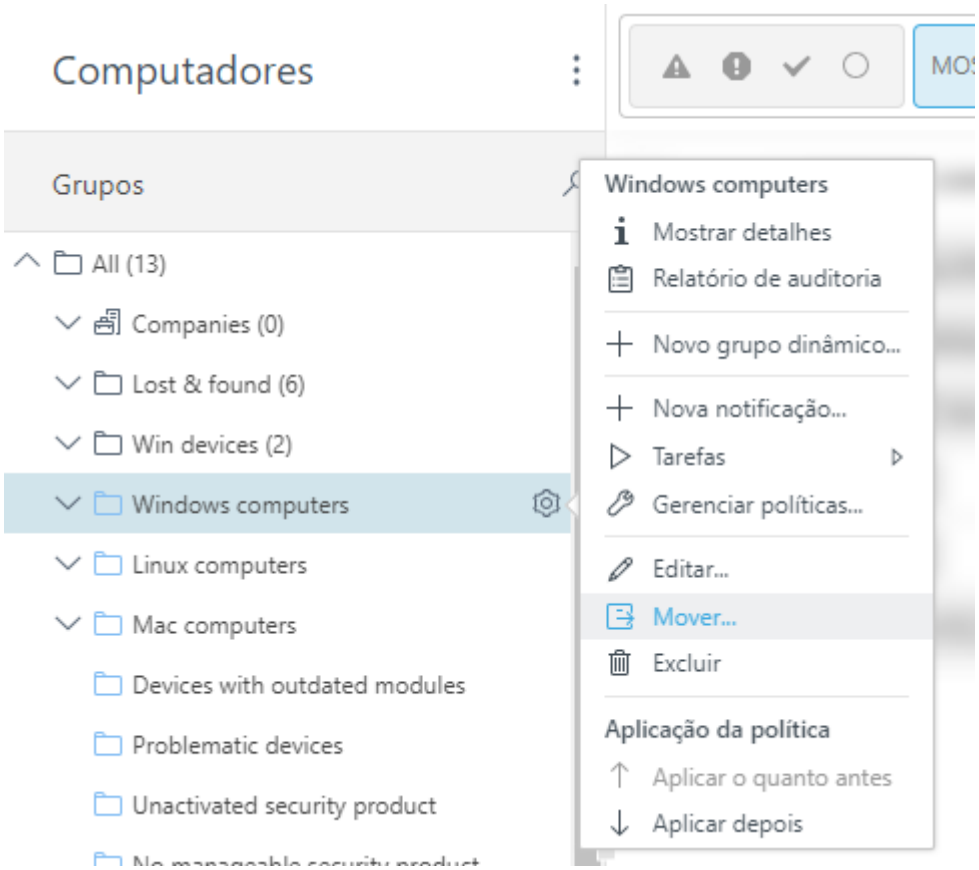
> O Grupo dinâmico em uma nova posição começa a filtrar os computadores (com base no modelo) sem qualquer relação com sua localização anterior.

Existem 3 métodos para mover um grupo:

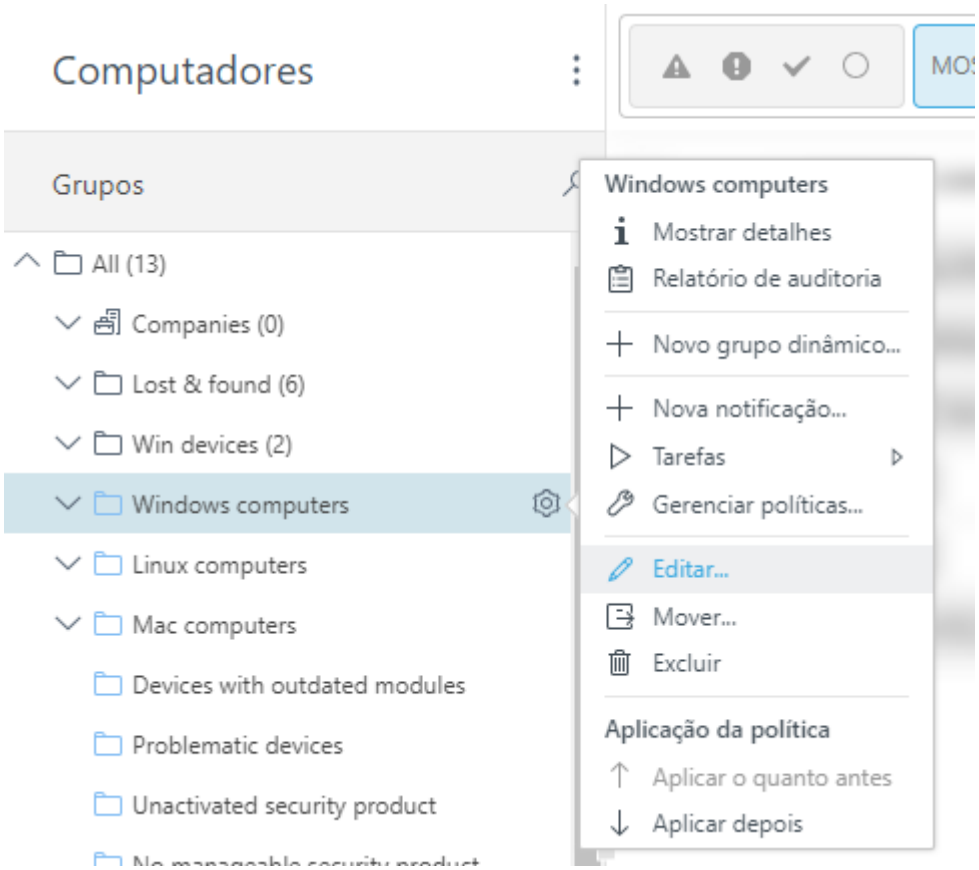
- **Arrastar e soltar** - clique e segure o grupo que deseja mover e solte-o sobre o novo grupo principal.



- Clique no ícone de engrenagem > **Mover** > selecione um novo grupo principal da lista e clique em **OK**.

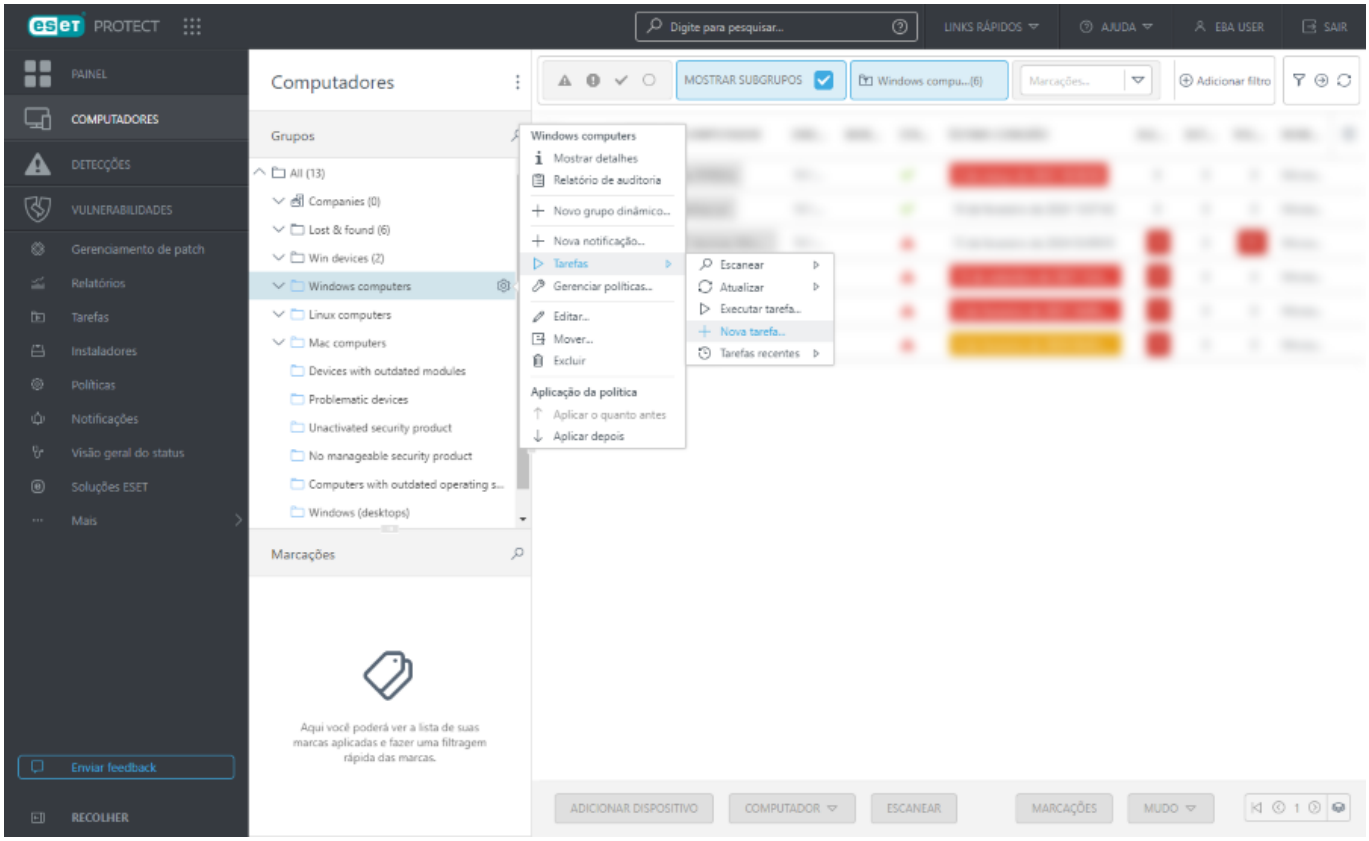


- Clique no ícone de engrenagem > **Editar >** selecione **Alterar grupo principal**. Selecione um novo grupo principal da lista e clique em **OK**.



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.

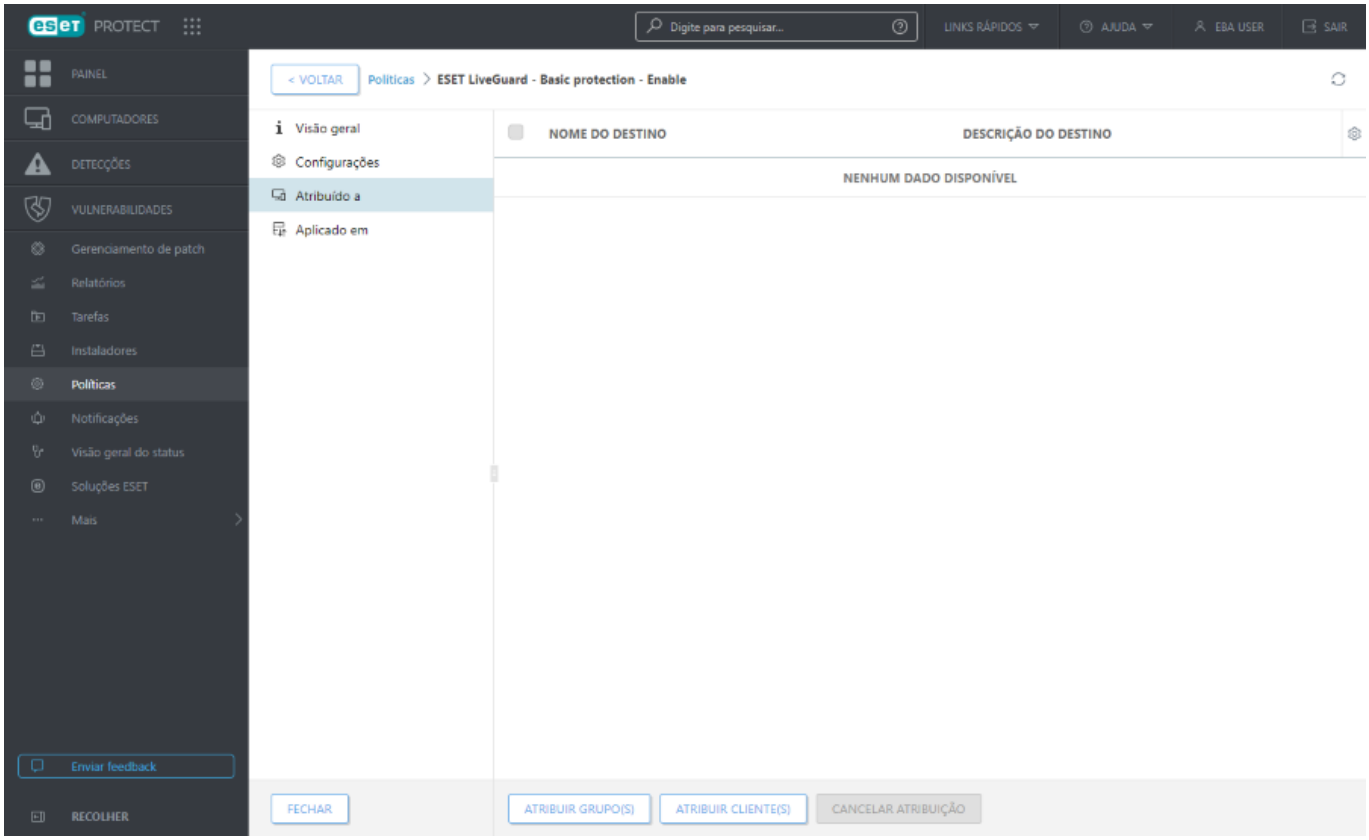


Atribuir política a um grupo

Depois que uma política é criada, você pode atribuí-la a um **grupo estático** ou **grupo dinâmico**. Existem duas maneiras de atribuir uma política:

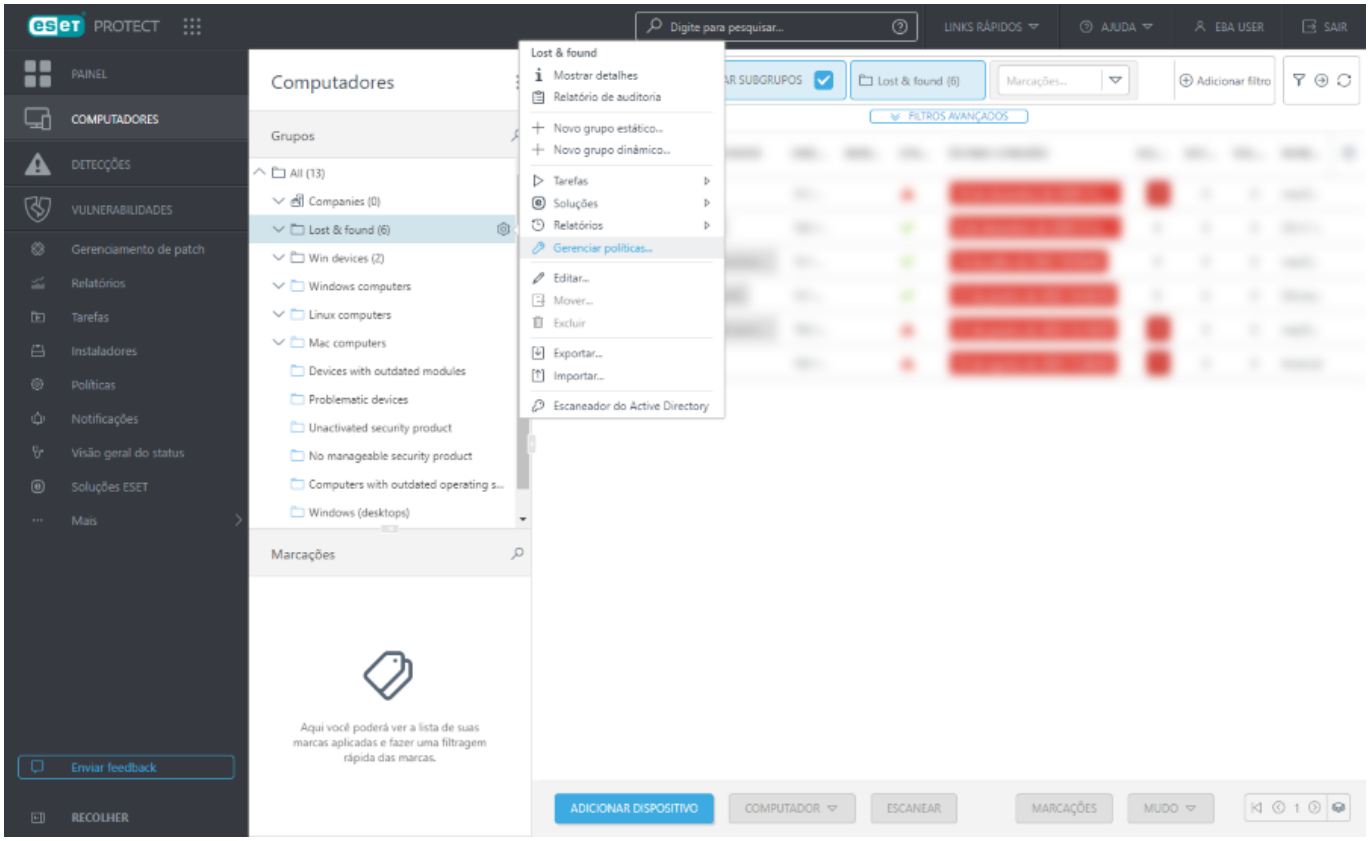
Método I.

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.

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.

Agrupamento de detecções

Para agrupar detecções, selecione no menu suspenso:

- **Desagroupado** – visualização padrão
- **Agrupado por computador** – detecções agrupadas por um nome de computador
- **Agrupados por categoria** – detecções agrupadas por uma categoria de detecção
- **Agrupados por tipo** – detecções agrupadas por uma categoria de detecção e seu tipo de detecção
- **Agrupado por hash** – detecções agrupadas por um hash
- **Agrupado por causa** – detecções agrupadas por uma causa
- **Agrupado por usuário** – detecções agrupadas por um usuário

Para ver todas as detecções agrupadas em uma fileira específica, clique em qualquer fileira e clique em **Abrir lista de detecção**. Então, informações sobre o grupo de detecção serão exibidas no topo da página. Clique no ícone de **Seta para baixo** para navegar entre as detecções agrupadas. Clique no ícone de **Seta voltar** para voltar aos grupos de detecção.

Para uma visualização mais específica, você pode adicionar outros filtros, como:

- **Categoria de detecção** – **Antivírus**, **Arquivos bloqueados**, **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.

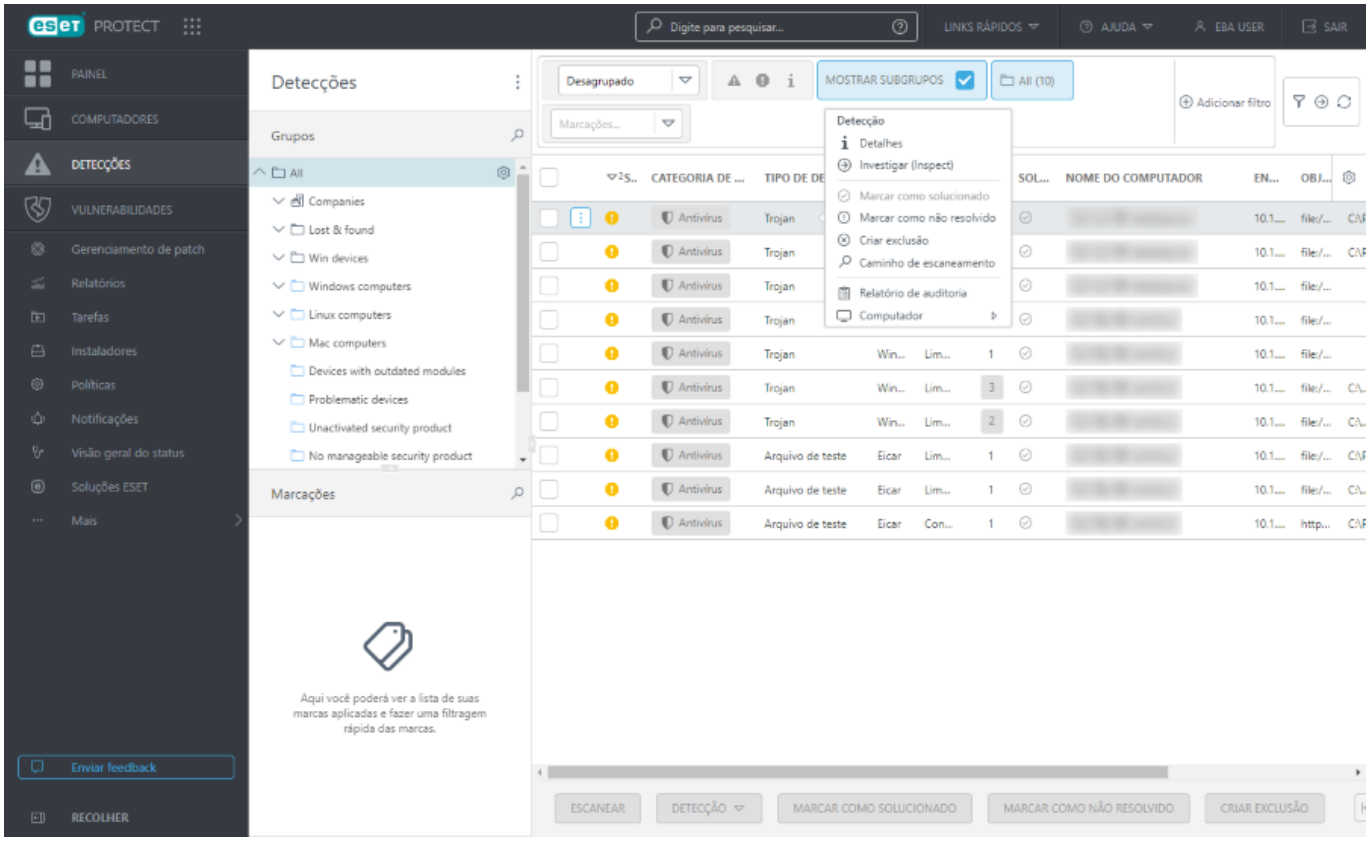
  ➢ Nas configurações do mecanismo de detecção do produto de segurança ESET, o nível de **Proteção** para a categoria de detecção é definido abaixo do nível de **Relatório**.

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** ou **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.

- **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:

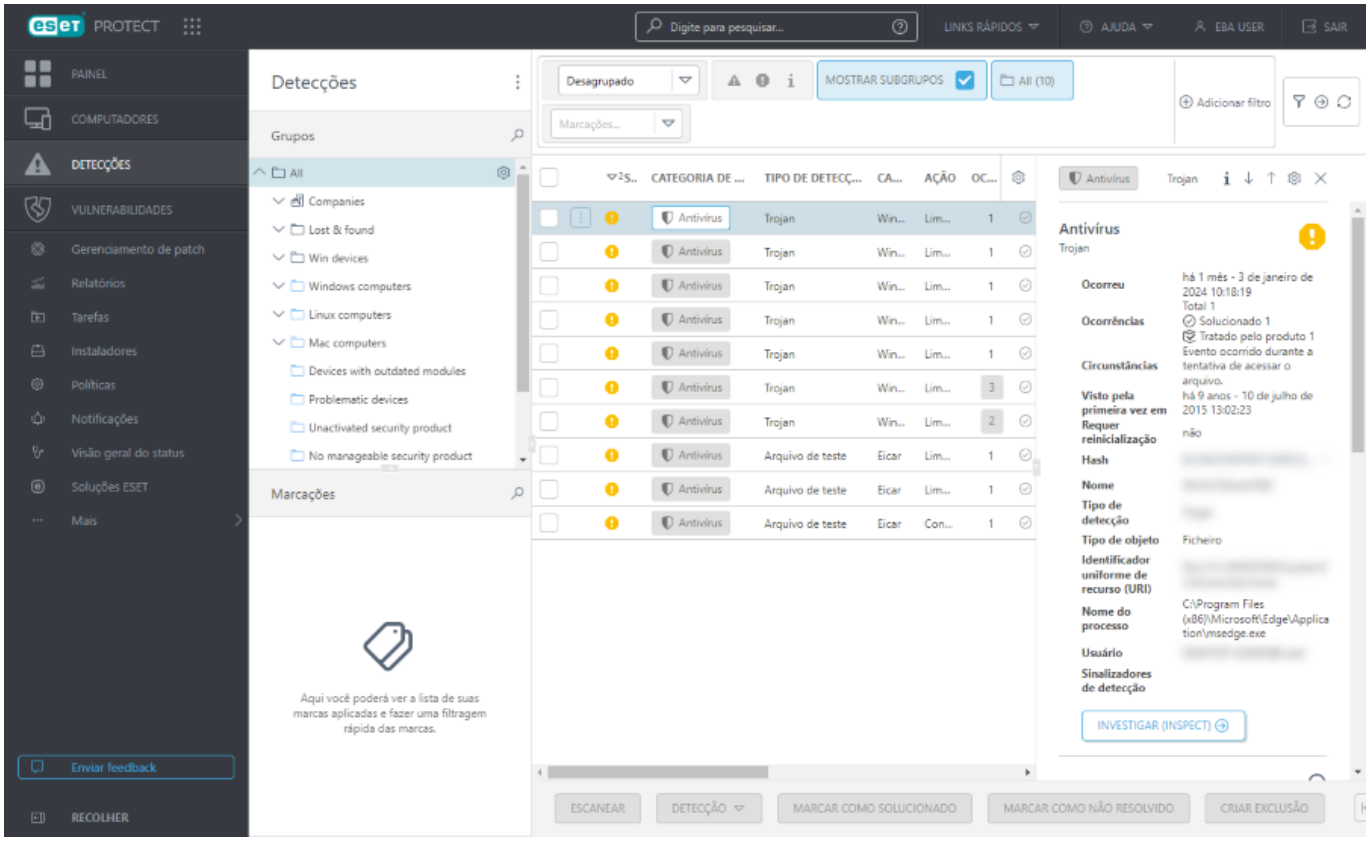
- **Mostrar detalhes** – abre os Detalhes da detecção.

- **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**:

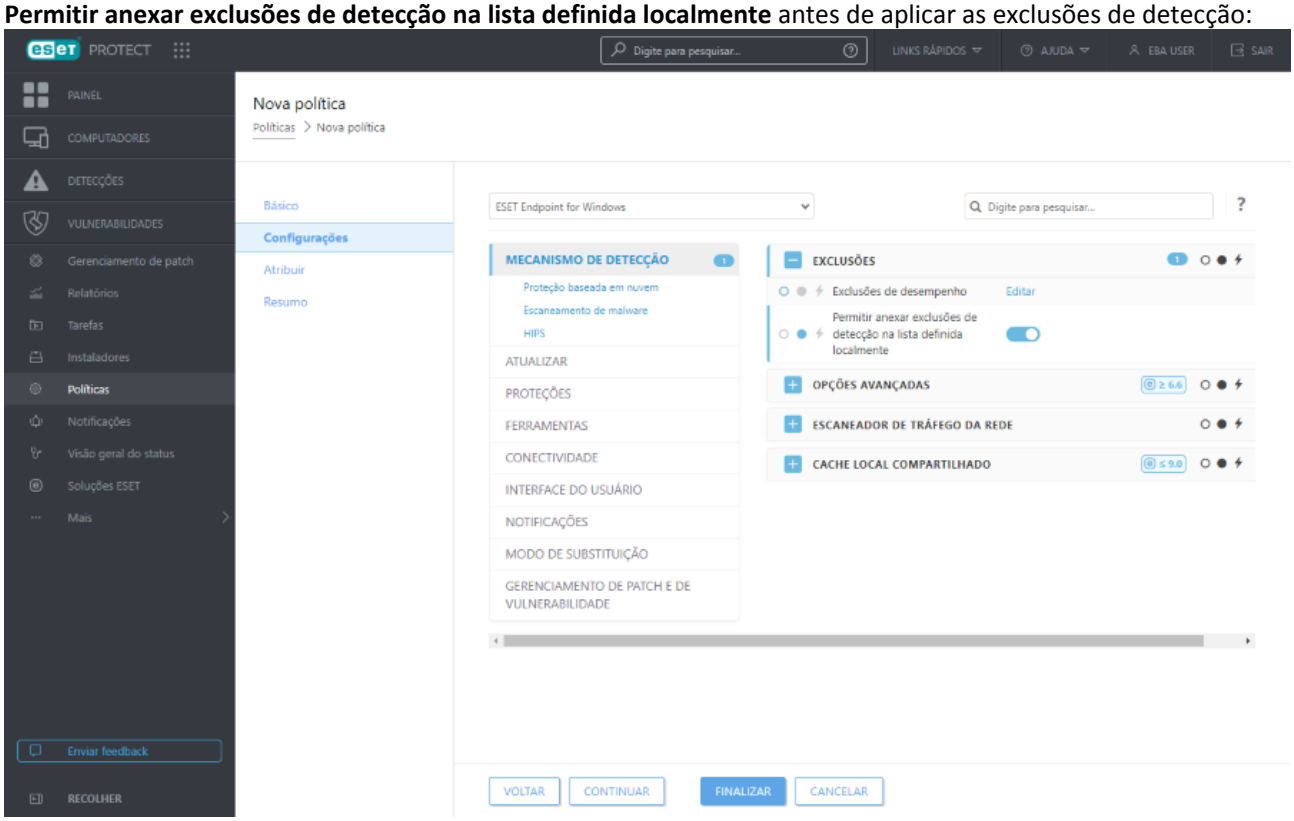
- **Exclusões de desempenho** – exclusões de arquivos e pastas definidas por um caminho. Elas podem ser criadas por meio de uma Política. Veja também o formato e os exemplos de exclusões de desempenho.

- **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 e gerenciar 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 relatada 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.

As seguintes soluções de segurança empresarial ESET foram renomeadas:

Nome antigo:	Novo nome:	Renomeado na versão:
ESET PROTECT	ESET PROTECT On-Prem	11.0
ESET PROTECT Cloud	ESET PROTECT	5.0
ESET Inspect	ESET Inspect On-Prem	2.0
ESET Inspect Cloud	ESET Inspect	

Configuração do ESET Inspect

Você pode ativar o ESET Inspect de ESET Business Account. Você precisa de uma licença ESET Inspect para ativar o 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.

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

O ESET PROTECT não armazena nem exibe detecções ESET Inspect em Detecções. Você pode visualizar as estatísticas de detecções ESET Inspect no **ESET PROTECT** > **Painel** > **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).

Clique na detecção e selecione **Investigar (Inspect)** para ver os detalhes da detecção no Web Console ESET Inspect.

Vulnerabilidades

A seção **Vulnerabilidades** fornece uma visão geral das vulnerabilidades detectadas em computadores. O computador é escaneado para detectar qualquer software instalado vulnerável a riscos de segurança. O escaneamento automatizado com relatórios instantâneos para o console permite que você priorize vulnerabilidades com base na gravidade, gerencie riscos de segurança e aloque recursos de forma eficaz. Uma ampla gama de opções de filtragem permite que você identifique e se concentre em problemas críticos de segurança.

Pré-requisitos

Para visualizar e habilitar o ESET Gerenciamento de patch e de vulnerabilidade, certifique-se de ter uma das seguintes camadas:

- ESET PROTECT Elite
- ESET PROTECT Complete
- ESET PROTECT MDR

Você pode habilitar o ESET Gerenciamento de patch e de vulnerabilidade somente em computadores Windows que executam:

- Versão do Agente ESET Management 10.1+
- ESET Endpoint Security para Windows versão 10.1+
- ESET Endpoint Antivirus para Windows versão 10.1+
- ESET Server Security para Microsoft Windows Server versão 11.0+

ESET Vulnerability & Patch Management não é compatível com processadores ARM.

Ativar gerenciamento de patch e de vulnerabilidade

1. Clique em **Computadores**.
2. Selecione o computador/grupo onde você deseja habilitar o Gerenciamento de patch e de vulnerabilidade.
3. Selecione **Soluções** e clique em **Ativar Gerenciamento de patch e de vulnerabilidade**.
4. Na janela **Ativar gerenciamento de patch e de vulnerabilidade**:

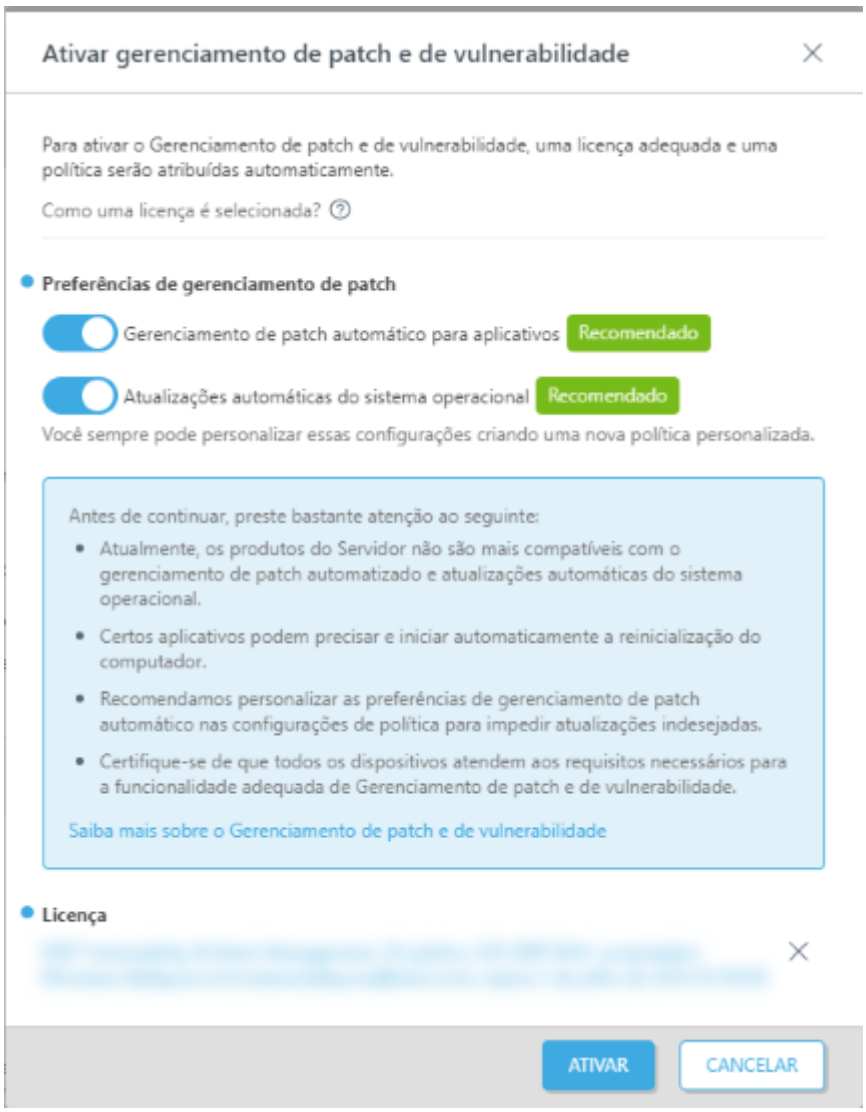
   a.Verifique se a opção **Gerenciamento automático de patches para aplicativos** está habilitada para aplicar automaticamente os patches ausentes aos computadores selecionados.

   b.Verifique se a opção de **Atualizações automáticas do sistema operacional** está habilitada para aplicar automaticamente as atualizações do sistema operacional aos computadores selecionados.

   As atualizações automáticas do sistema operacional só estão disponíveis para o ESET Endpoint para Windows 11.0 e versões posteriores.

   c.A licença é pré-selecionada.

   d.Clique no botão **Ativar**.



Quando o Gerenciamento de patch e de vulnerabilidade está habilitado:

- O ícone Vulnerabilidades aparece ao lado do nome do computador.
- Você pode ver o bloco **Gerenciamento de patch e de vulnerabilidade** com o status **Ativo** nos detalhes do computador.

> Alguns aplicativos exigem uma reinicialização do computador e podem reiniciar os computadores automaticamente após uma atualização.

> Alguns aplicativos (por exemplo, TeamViewer) podem ser licenciados para uma versão específica. Revise seus aplicativos. Para evitar uma atualização desnecessária, defina a **Estratégia de patch automático** > **Corrigir todos exceto os aplicativos excluídos** ao criar uma política.

Exibir Vulnerabilidades

Você pode ver as **Vulnerabilidades** vindo de vários lugares:

- Clique em **Vulnerabilidades** no menu principal para abrir a seção **Vulnerabilidades** e exibir uma lista de vulnerabilidades.
- Clique em **Computadores** > clique no computador e clique em **Detalhes** > no bloco **Gerenciamento de**

patch e de vulnerabilidade, clique em **Mostrar vulnerabilidades** para abrir a seção **Vulnerabilidades**.

• Clique em **Computadores** > na coluna **Vulnerabilidades** e clique no número de vulnerabilidades no computador selecionado para abrir a seção **Vulnerabilidades**.

Agrupamento de vulnerabilidades

Para agrupar vulnerabilidades, selecione no menu suspenso:

• **Desagroupado** – visualização padrão

• **Agrupar por nome de aplicativo** – as vulnerabilidades são agrupadas por nome de aplicativo vulnerável, com números de **Dispositivos afetados** e **Vulnerabilidades**. Quando agrupado, clique em uma linha de aplicativo e clique em **Mostrar vulnerabilidades** para exibir as vulnerabilidades para o aplicativo selecionado.

• **Agrupar por CVE** – as vulnerabilidades são agrupadas pelo número CVE (vulnerabilidades e exposição comuns). Um CVE é um número de identificação de uma vulnerabilidade. Quando agrupadas, clique em uma linha CVE e clique em **Mostrar dispositivos** para exibir os dispositivos (computadores) com a vulnerabilidade.

Filtragem de visualização

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.

• **Nome do aplicativo** – o nome do aplicativo com a vulnerabilidade

• **Versão do aplicativo** – a versão do aplicativo

• **Fornecedor do aplicativo** – o fornecedor do aplicativo com a vulnerabilidade

• **Pontuação de risco** – pontuação de risco da vulnerabilidade de 0 a 100

• **CVE** – um número CVE (vulnerabilidades e exposição comuns), que é um número de identificação de uma vulnerabilidade

• **Nome do computador** – o nome do computador afetado. Clique no nome do computador para exibir os detalhes do computador com a vulnerabilidade

• **Categoria** – Categoria da vulnerabilidade:

  ○Vulnerabilidade do aplicativo

  ○Vulnerabilidade do sistema operacional

• **Visto pela primeira vez** – a data e a hora em que a vulnerabilidade foi detectada pela primeira vez no dispositivo

Pontuação de risco – avalia a gravidade das vulnerabilidades de segurança do sistema de computador. Uma pontuação de risco é calculada com base no seguinte:

- CVSSv2/CVSSv3
- Popularidade CVE – indica o nível de atividade da vulnerabilidade
- Taxa de risco comprometido – indica o número de dispositivos com vulnerabilidade confirmada
- Ciclo de vida CVE – indica o tempo decorrido desde que a vulnerabilidade foi relatada pela primeira vez

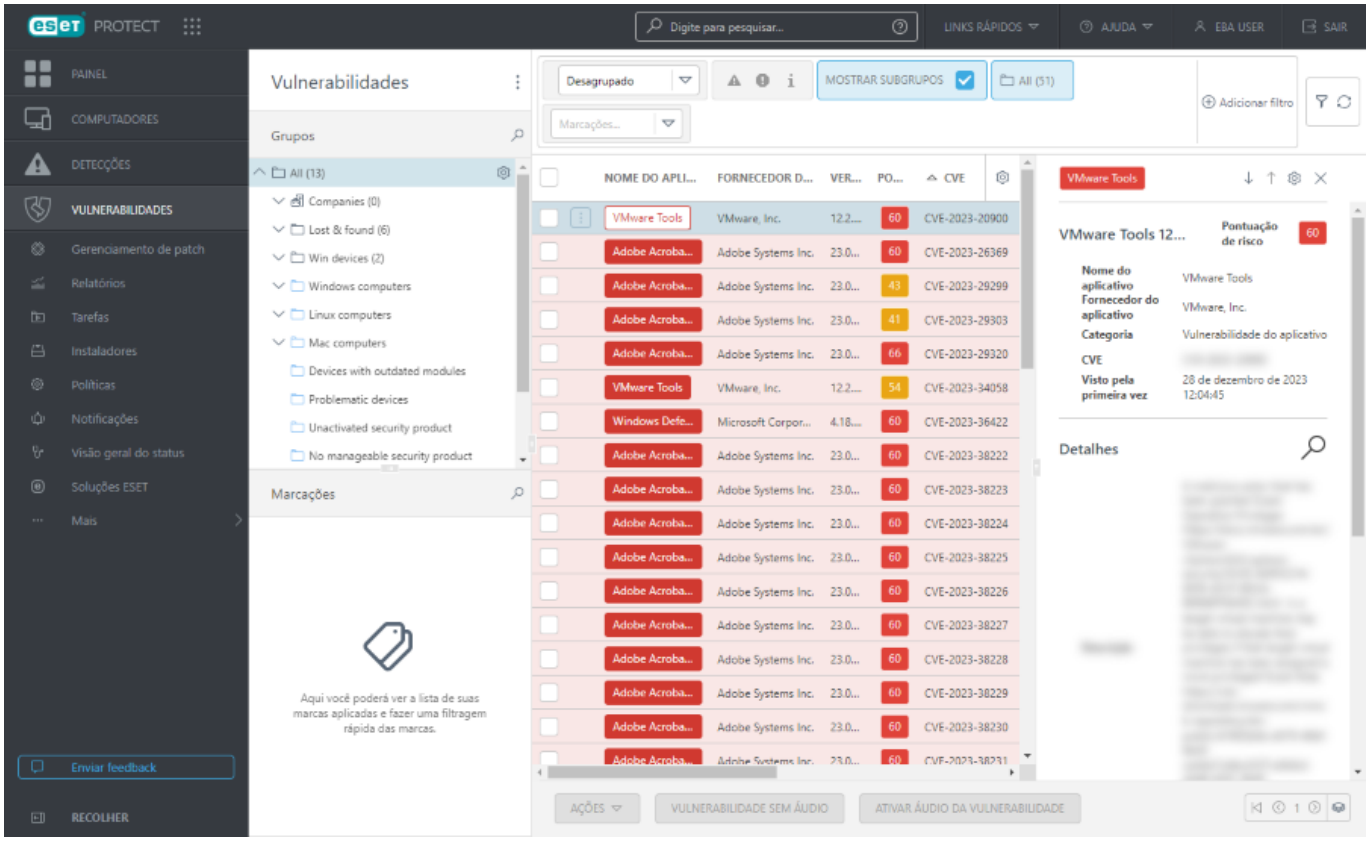
Uma pontuação de risco é indicada em:

- cinza (0–29) – baixa gravidade
- amarelo (30–59) – gravidade média
- vermelho (60–100) – gravidade crítica

Pré-visualização da vulnerabilidade

Clique no nome de um aplicativo para exibir os detalhes da vulnerabilidade em um painel lateral. A manipulação de visualização de vulnerabilidades inclui:

- **Avançar** – exibe a próxima vulnerabilidade no painel lateral de visualização de vulnerabilidades
- **Anterior** – exibe a vulnerabilidade anterior no painel lateral de visualização da vulnerabilidade
- **Gerenciar conteúdo para detalhes da vulnerabilidade** – gerencia como as seções do painel lateral de visualização da vulnerabilidade são exibidas e em que ordem
- **Fechar** – fecha o painel lateral de visualização de vulnerabilidades



Para obter mais informações, consulte a lista de aplicativos cobertos em Vulnerabilidades.

Ativar/desativar áudio da vulnerabilidade

Você pode ativar ou desativar o som da vulnerabilidade nos dispositivos:

- Clique na linha do computador e clique em **Silenciar vulnerabilidade/Ativar o som da vulnerabilidade**
- Selecione o computador e clique no botão **Silenciar vulnerabilidade/Ativar o som da vulnerabilidade** na parte inferior da página
- Selecione o computador e clique no botão **Ações** e, em seguida, selecione **Silenciar vulnerabilidade/Ativar o som da vulnerabilidade**

Escaneamento de vulnerabilidade

Você pode iniciar a verificação imediata de vulnerabilidades e patches ausentes em um dispositivo selecionado:

- Clique na linha do computador e selecione **Computador** > **Verificar** > **Verificação de vulnerabilidade**
- Selecione o computador e clique no botão **Ações** e, em seguida, selecione **Computador** > **Verificar** > **Verificação de vulnerabilidade**
- Selecione qualquer grupo, clique em e selecione **Tarefas** > **Verificação** > **Verificação de vulnerabilidade**

A tarefa **Iniciar verificação de vulnerabilidade** está programada para ser executada o mais rápido possível.

A tarefa pode ter uma demanda maior nos recursos do dispositivo por até 10 minutos.

Você pode criar um modelo de relatório com dados de vulnerabilidade e, em seguida, adicionar o relatório ao Painel.

Para obter mais informações, consulte Perguntas frequentes sobre o Gerenciamento de patch e de vulnerabilidade.

Aplicativos cobertos por Vulnerabilidades

A lista de aplicativos cobertos por Vulnerabilidades só está disponível em inglês.

Gerenciamento de patch

O gerenciamento de patch ajuda a garantir que os sistemas e aplicativos estejam seguros contra vulnerabilidades e explorações conhecidas. A seção Gerenciamento de patch lista todos os patches disponíveis que corrigem as vulnerabilidades detectadas e facilita o processo de correção por meio de atualizações automatizadas de software. Com as opções de aplicação de patches, você pode garantir prontamente que seus endpoints sejam atualizados com os patches de segurança mais recentes.

Pré-requisitos

Para visualizar e habilitar o ESET Gerenciamento de patch e de vulnerabilidade, certifique-se de ter uma das seguintes camadas:

- ESET PROTECT Elite
- ESET PROTECT Complete
- ESET PROTECT MDR

Você pode habilitar o ESET Gerenciamento de patch e de vulnerabilidade somente em computadores Windows que executam:

- Versão do Agente ESET Management 10.1+
- ESET Endpoint Security para Windows versão 10.1+
- ESET Endpoint Antivirus para Windows versão 10.1+
- ESET Server Security para Microsoft Windows Server versão 11.0+

ESET Vulnerability & Patch Management não é compatível com processadores ARM.

ESET Bridge usuários

O ESET Bridge bloqueia o tráfego da rede do gerenciamento de patch por padrão. O ESET Bridge não afeta o relatório de vulnerabilidades.

Para habilitar o tráfego da rede do gerenciamento de patch, desabilite as regras da Lista de controle de acesso (ACL) no arquivo de configuração ESET Bridge:

1.Abra o arquivo de configuração ESET Bridge*restrict.conf.template* em um editor de texto:
*o*Windows: *C:\ProgramData\ESET\Bridge\Proxies\Nginx\Conf\restrict.conf.template*
*o*Linux: */var/opt/eset/bridge/nginx/conf/restrict.conf.template*
2.Mude `set $valid_host 0;` para `set $valid_host 1;`.
3.Salve o arquivo *restrict.conf.template*.
4.Reinicie o serviço ESET Bridge.

Desabilitar regras de ACL permite o roteamento de todo o tráfego da rede via ESET Bridge (ESET Bridge torna-se um proxy aberto).

O Gerenciamento de patch é habilitado durante a ativação do Gerenciamento de patch e vulnerabilidades.

Exibir Gerenciamento de patch

Você pode visualizar o Gerenciamento de patch de vários lugares:

- Clique em **Gerenciamento de patch** no menu principal para abrir a seção **Gerenciamento de patch** e exibir uma lista de patches

- Clique em **Computadores** > selecione **Detalhes** > no bloco **Gerenciamento de patch e de vulnerabilidade**, clique em **Mostrar patches** para abrir a seção **Gerenciamento de patch**

Agrupando a visualização

Para agrupar patches, selecione no menu suspenso:

- **Desagroupado** – visualização padrão

- **Agrupar por nome do aplicativo** – quando agrupado, clique em uma linha do aplicativo e clique em **Mostrar dispositivos** para exibir dispositivos (computadores) onde um patch será aplicado

Filtragem de visualização

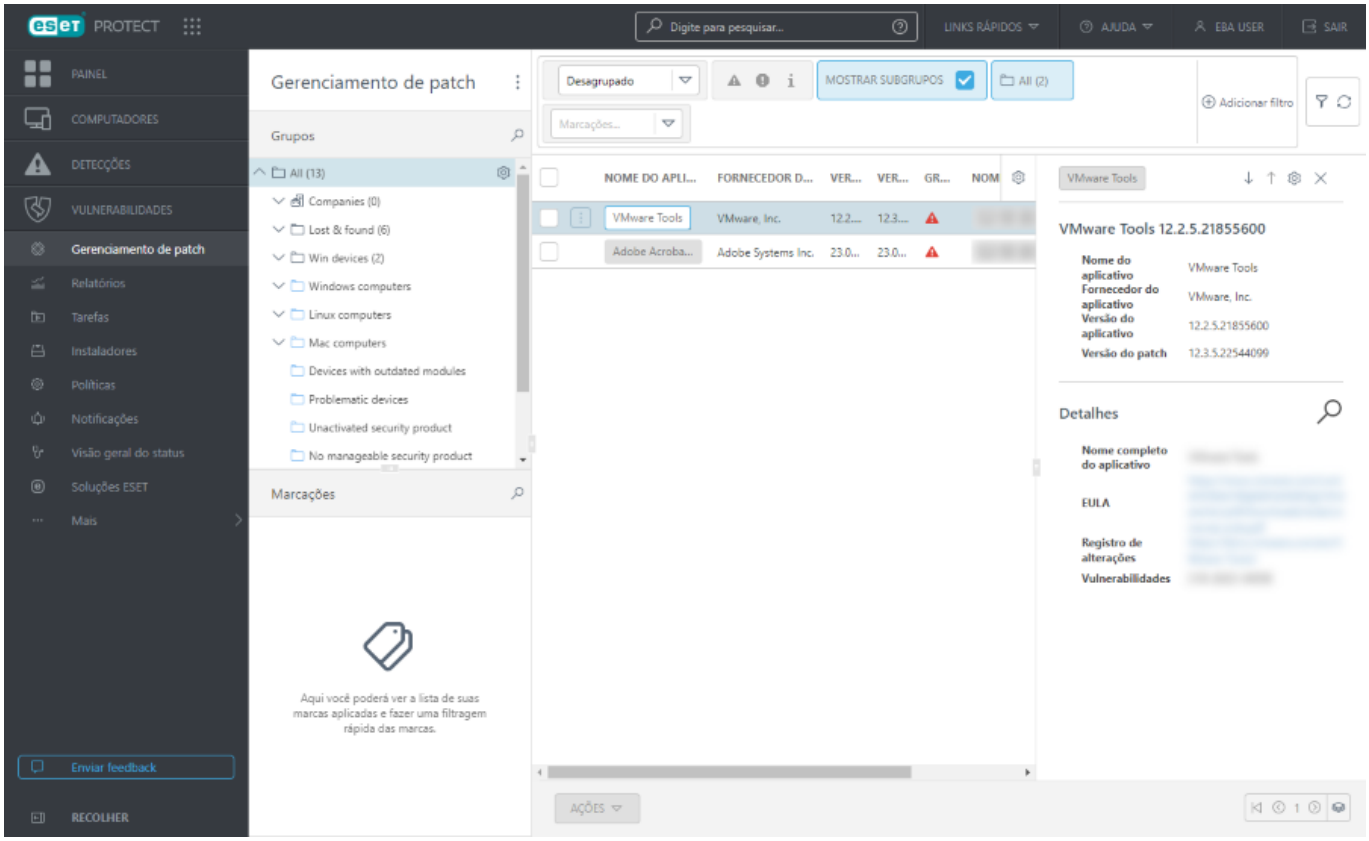
Para adicionar critérios de filtragem, clique em **Adicionar filtro** e selecione um item da lista. Digite as strings de pesquisa ou selecione os itens no menu suspenso no(s) campo(s) de filtro(s) e pressione **Enter**. Filtros ativos são destacados em azul.

- **Nome do aplicativo** – o nome do aplicativo com a vulnerabilidade
- **Versão do aplicativo** – a versão do aplicativo que está causando a vulnerabilidade
- **Versão do patch** – a versão do patch
- **Gravidade** – nível de gravidade, incluindo para informação, aviso ou crítico
- **Nome do computador** – o nome do computador afetado
- **Fornecedor do aplicativo** – o nome do fornecedor do aplicativo

Painel lateral com detalhes

Clique no nome de um aplicativo para exibir os detalhes do aplicativo em um painel lateral. Manipulação de visualização de aplicativo:

- **Avançar** – exibe os detalhes do próximo aplicativo no painel lateral
- **Anterior** – exibe os detalhes do aplicativo anterior no painel lateral
- **Gerenciar conteúdo para Detalhes do patch** – gerencia como as seções do painel lateral são exibidas e em que ordem
- **Fechar** – fecha o painel lateral



Implantar patches

Você pode fazer patch apenas em aplicativos selecionados.

Recomendamos que você habilite o gerenciamento de patch automático por meio de uma política.

Você pode habilitar as atualizações automáticas do sistema operacional e selecionar os níveis de gravidade para aplicar atualizações do sistema operacional por meio de uma política.
As atualizações automáticas do sistema operacional só estão disponíveis para o ESET Endpoint para Windows 11.0 e versões posteriores.

Quando o patch automatizado é configurado, a solução aplica patches automaticamente nos aplicativos durante as janelas de manutenção.

Alguns aplicativos exigem uma reinicialização do computador e podem reiniciar os computadores automaticamente após uma atualização.

Alguns aplicativos (por exemplo, TeamViewer) podem ser licenciados para uma versão específica. Revise seus aplicativos. Para evitar uma atualização desnecessária, defina a **Estratégia de patch automático** > **Corrigir todos exceto os aplicativos excluídos** ao criar uma política.

Como alternativa, você pode implantar patches via:

- Selecione os aplicativos onde deseja implantar patches > clique no botão **Ações** e clique em **Atualizar**.
- Para aplicar um patch em um aplicativo em todos os dispositivos afetados, aplique a visualização **Agrupar por nome do aplicativo**, selecione a linha com o nome do aplicativo, clique em ⋮ e clique em **Atualizar**.

Depois de implantar patches com o botão **Atualizar**, uma nova tarefa do cliente **Aplicar patch de aplicativo** será

criada automaticamente em Tarefas. Para endpoints, os patches serão aplicados com base na agenda do Gerenciamento de patch e de vulnerabilidade definida nas Políticas. Para servidores, os patches serão instalados após uma contagem regressiva de 60 segundos, sem opção de adiamento.

Para obter mais informações, consulte Perguntas frequentes sobre o Gerenciamento de patch e de vulnerabilidade.

Aplicativos cobertos pelo Gerenciamento de patch

A lista de aplicativos cobertos pelo Gerenciamento de patch só está disponível em inglês.

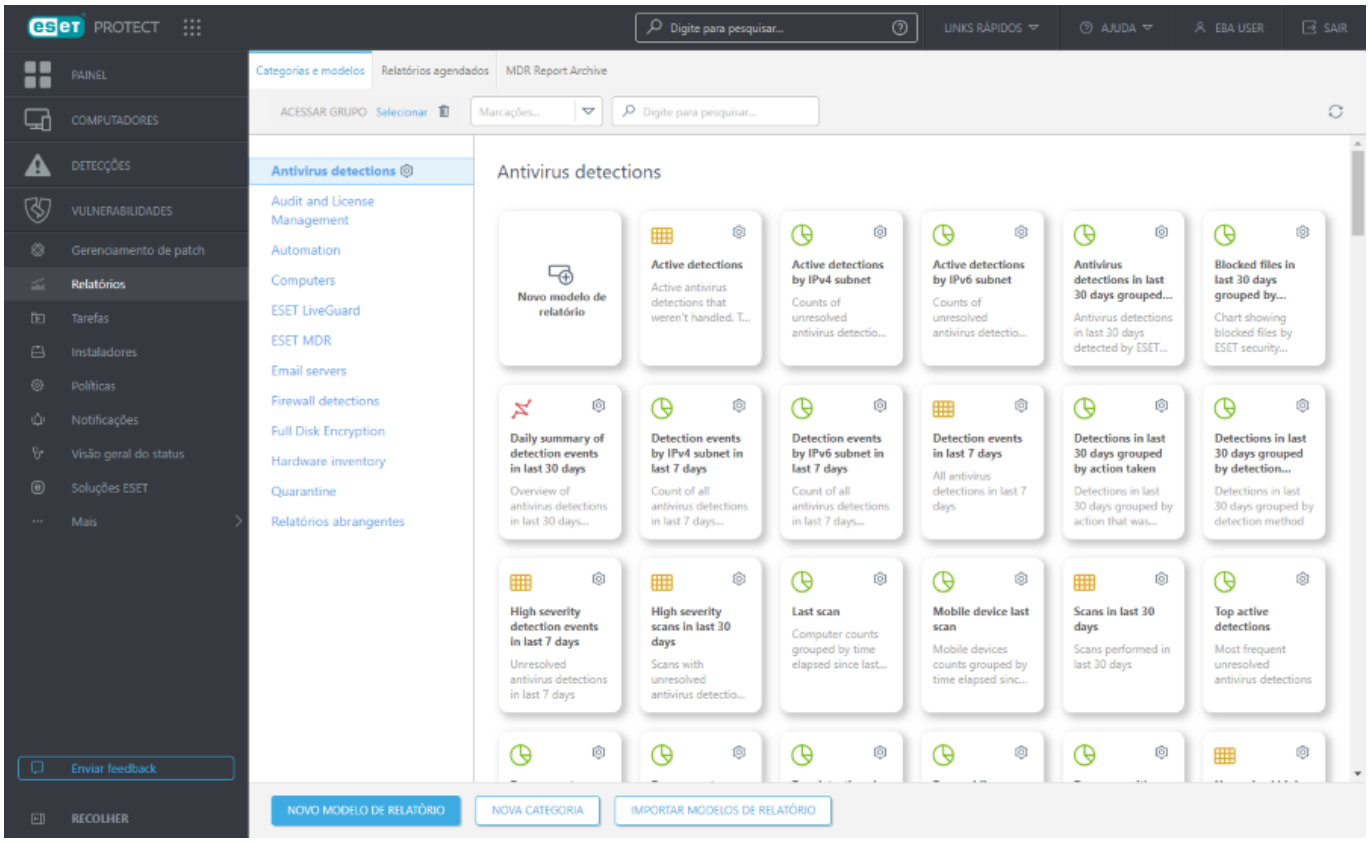
Relatórios

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.

- **MDR Arquivo de relatórios**: esta guia fornece uma visão geral dos ESET MDR relatórios.

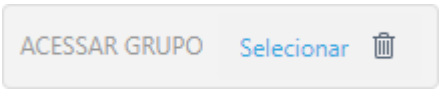


Os relatórios são gerados a partir de modelos que são categorizados por tipo de relatório. Um relatório pode ser

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.

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 Servidor 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.

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

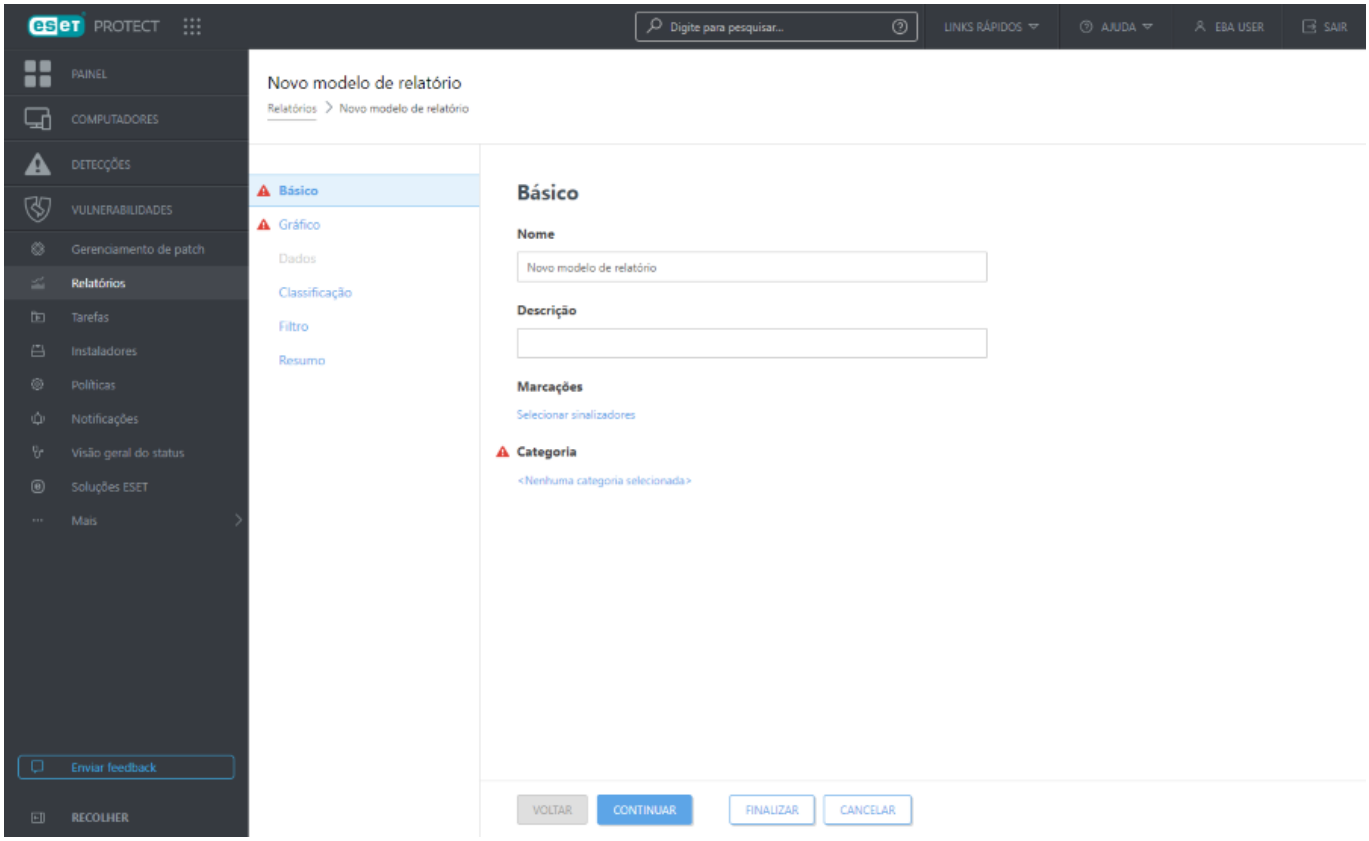
Relatórios são objetos estáticos que residem em uma estrutura de objetos no banco de dados ESET PROTECT. Cada novo modelo de relatório é armazenado no grupo inicial do usuário que o criou. Para acessar um relatório você precisa de permissões com a funcionalidade **Relatórios e Painel**. Você também precisa 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, gerar relatórios com base em modelos de relatório e ler seu painel
- **Uso**: o usuário pode modificar seu painel com modelos de relatório disponíveis
- **Gravação**: criar/modificar/remover modelos e suas categorias

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

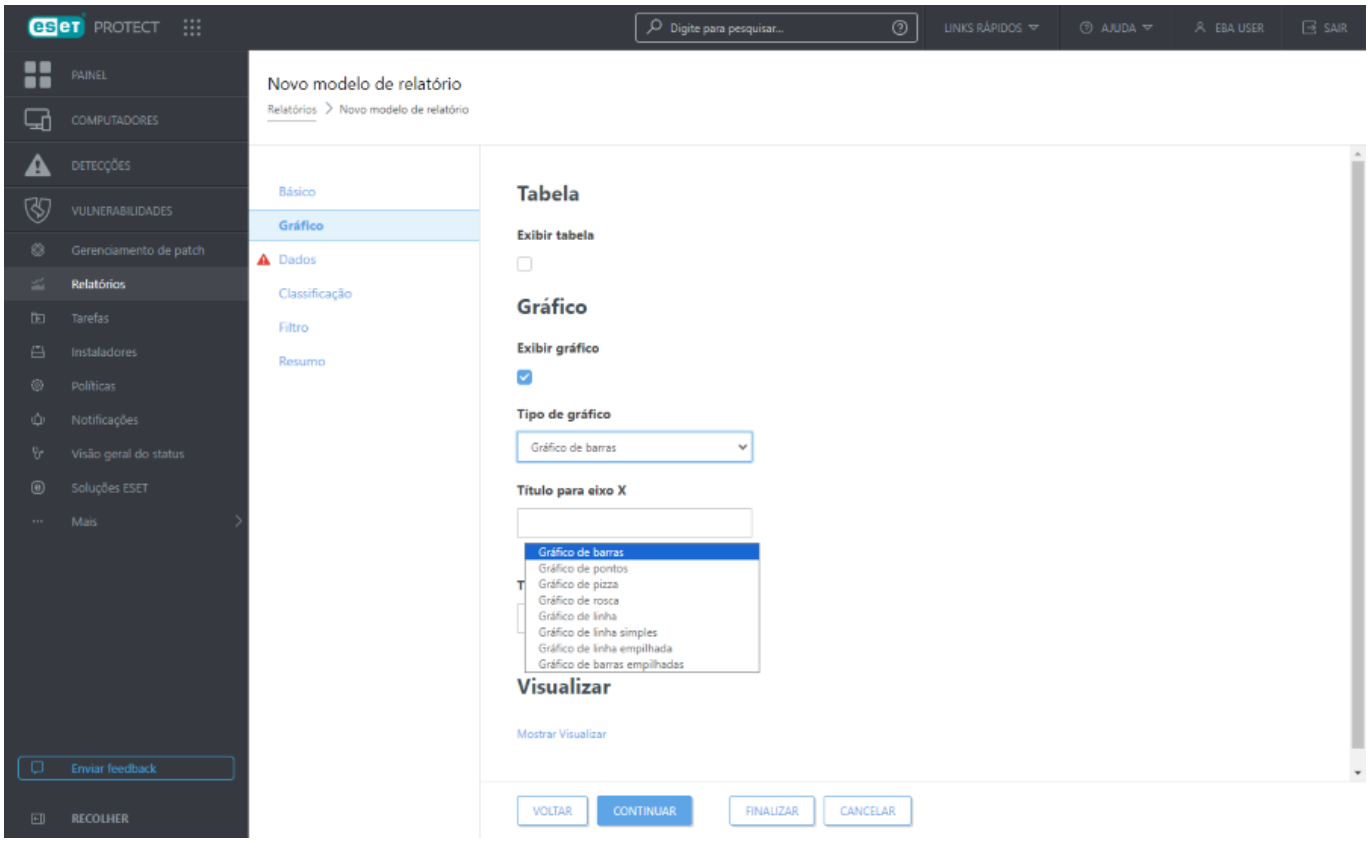
Criar um novo modelo de relatório

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

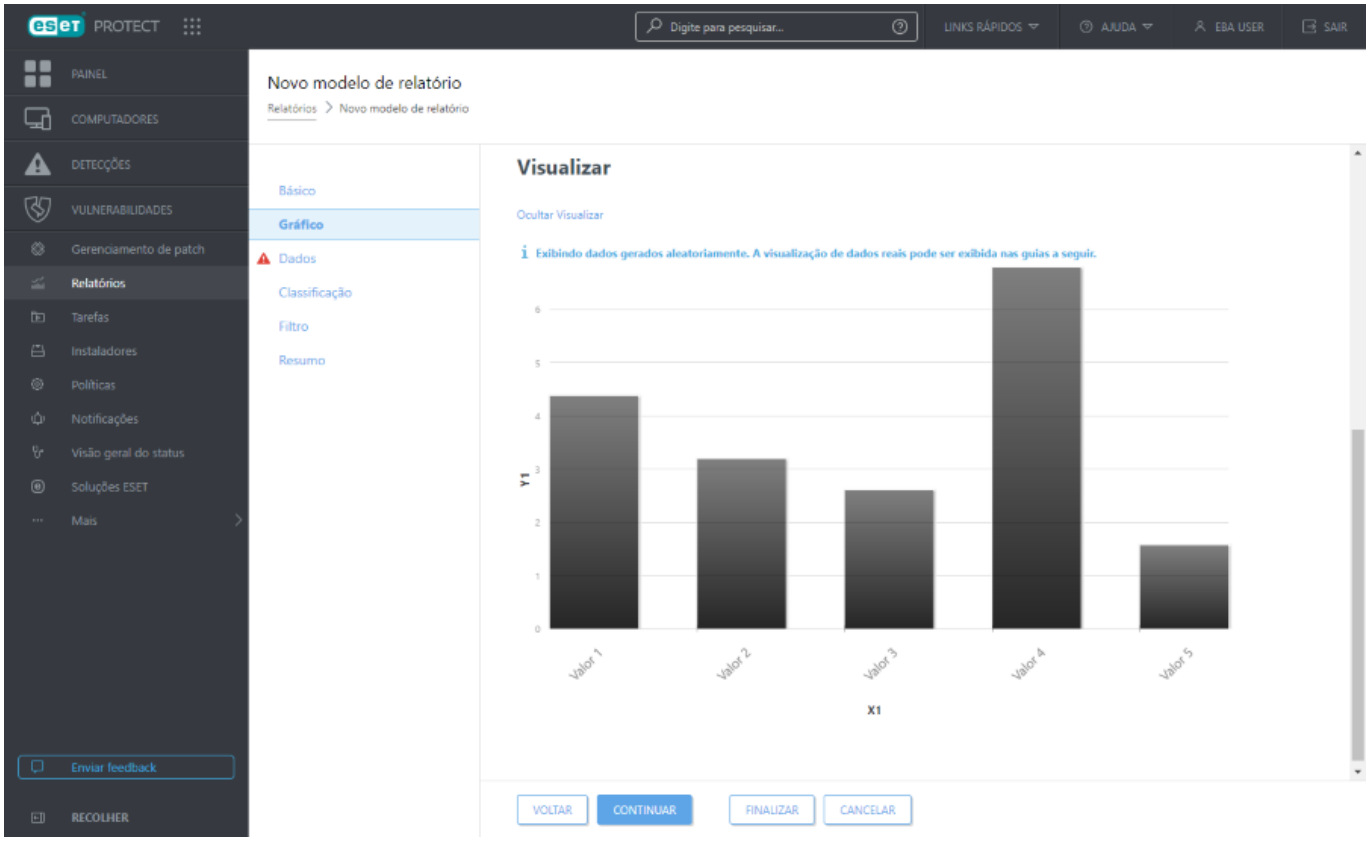
Na seção **Gráfico**, selecione o tipo **Relatório**. Uma **Tabela**, onde as informações são classificadas em linhas e colunas, ou um **Gráfico**, que representa dados usando um eixo X e Y.

> 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:

- 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.
  - Defina 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.

Modelo de relatório MDR

O relatório MDR é um relatório de segurança para Provedores de detecção e resposta gerenciados.

Você precisa de uma licença do ESET Inspect para gerar o relatório MDR. Um usuário precisa de um conjunto de permissões com a funcionalidade **Relatórios abrangentes** (conjunto de permissões de Administrador/Revisor/personalizado) para gerar o Modelo do Relatório MDR:

1. Clique em **Relatórios** e selecione a guia **Categorias e Modelos**.
2. Clique em **Relatórios Abrangentes** e clique em **MDR Modelo de Relatório**.
3. Clique em **Gerar e fazer download**. Você pode gerar o MDR Modelo de Relatório somente como arquivo .odt.

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.
- Os Usuários do MSP podem filtrar o relatório selecionando o cliente.
- Defina a entrega do relatório em um e-mail.
- Opcionalmente define os parâmetros de acionador e alternância.

O tamanho máximo de e-mail permitido pela infraestrutura ESET PROTECT é de 30 MB.

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.

ESET MDR

O ESET MDR fornece uma visão geral de incidentes e detecções do ESET Inspect. Para usar o ESET MDR, você precisa de uma licença do ESET Inspect e do nível **ESET PROTECT MDR**.

> **Disponibilidade do ESET MDR por país**
> O ESET MDR está disponível nos seguintes países: EUA, Canadá, Japão, Reino Unido, Holanda, França, Itália, países do DACH (Alemanha, Áustria, Suíça), países nórdicos (Suécia, Noruega, Dinamarca, Finlândia, Islândia), Eslováquia, República Tcheca, Ucrânia.

O serviço ESET MDR abrange todos os dispositivos gerenciados que executam o ESET Inspect. Siga as etapas abaixo para selecionar os dispositivos para os quais você deseja gerenciar a segurança independentemente do serviço ESET MDR:

1. Abra ESET PROTECT e navegue até **Computadores**.
2. Clique no ícone de engrenagem ao lado do grupo pai estático existente e selecione **Novo grupo estático.**
3. Digite `exempt` no campo **Nome** e clique em **Concluir**.
4. Selecione o grupo pai e selecione os dispositivos que você deseja incluir no grupo isento.
5. Clique no botão **Computador** > **Gerenciar** > **Mover para Grupo** e selecione o grupo `exempt`.

Os dispositivos no grupo `exempt` estão sob seu gerenciamento — você pode lidar com incidentes manualmente sem as ações de resposta aplicadas automaticamente.

> Consulte também o ESET MDR painel.

Relatório ESET MDR

O relatório **ESET MDR** é um resumo semanal de informações relevantes para a segurança de várias fontes em toda a rede.

Você precisa dos seguintes conjuntos de permissões para agendar o ESET MDR relatório:
- **ESET MDR relatórios**: Gravar
- **Tarefas e Gatilhos do Servidor**: **Gerar Relatório**—Usar, Gravar

Depois de ativar a licença doESET PROTECT MDR, uma tarefa do servidor é agendada automaticamente com o e-mail atribuído pelo administrador.

Os destinatários receberão o **ESET MDR Relatório Semanal** automaticamente.

1. Clique em **Relatórios** e selecione a guia **Categorias e Modelos** > **ESET MDR**.
2. Clique no ícone de engrenagem **Ações** no **ESET MDR Relatório Semanal** e clique em **Agendar**.
3. Clique em **Selecionar marcações** para atribuir marcações. Clique em **Continuar**.
4. Selecione o idioma preferido do relatório no menu suspenso **Localidade** e selecione seu fuso horário no menu suspenso **Fuso horário**. O menu suspenso **Tipo de gatilho** está desabilitado. A opção semanal (todas as segundas-feiras) é selecionada automaticamente.
5. Digite o endereço de email do destinatário no campo **Enviar para** .
6. Você também pode selecionar **Personalizar mensagem** e digitar seu **Assunto** e o corpo da **Mensagem**.
7. Clique em **Concluir**.

Como alternativa, você pode criar o **ESET MDR Relatório Semanal** executando uma tarefa Gerar Relatório do servidor:

1. Selecione **Tarefas** > **, Nova** > **Tarefa do Servidor**.
2. Selecione **Gerar Relatório** no menu suspenso **Tarefa** e clique em **Continuar**.
3. Clique em **Adicionar modelo de relatório** e selecione **ESET MDR Relatório Semanal**.
4. Digite o endereço de email do destinatário no campo **Enviar para**.
5. Você também pode selecionar **Personalizar mensagem** e digitar seu **Assunto** e o corpo da **Mensagem**.
6. Clique em **Continuar**.
7. Selecione o idioma preferido do relatório no menu suspenso **Localidade** e selecione seu fuso horário no menu suspenso **Fuso horário**. O menu suspenso **Tipo de gatilho** está desabilitado. A opção semanal (todas as segundas-feiras) é selecionada automaticamente.
8. Clique em **Continuar**.
9. Verifique suas configurações em **Resumo** e clique em **Concluir**.

Você receberá o ESET MDR Relatório Semanal como um arquivo .pdf.
O ESET MDR Relatório Semanal é gerado todas as segundas-feiras com um nível ESET PROTECT MDR ativo.

Arquivo de Relatórios MDR

O **MDR Arquivo de Relatórios** contém todos os relatórios do ESET MDR enviados por e-mail. Você receberá um e-mail com um link para o seu relatório, e poderá retornar a qualquer relatório do ESET MDR gerado no último ano.

Você pode exibir o ESET MDR arquivo morto de relatórios na guia **Relatórios** > **MDR Arquivo Morto de Relatórios**.

Pré-requisitos
Você pode exibir o Arquivo Morto de Relatório quando tiver definido um direito de **Uso** nos Conjuntos de permissões para Relatórios do **ESET MDR** e:
- ter ativado a licença do ESET PROTECT MDR e ESET Inspect
- sua licença do ESET PROTECT MDR está vencida, mas você tem pelo menos um relatório agendado e entregue no último ano

Layout do painel lateral

Clique no ícone ⋮ ao lado do nome do **MDR Arquivo Morto de Relatórios** e ajuste o layout do painel lateral usando o menu de contexto:

- **Ocultar painel lateral**
- **Marcações**

Filtrar o MDR Arquivo Morto de Relatórios

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 adicionar:

- **Período de**: clique no campo para selecionar a data de início do filtro
- **Período até**: clique no campo para selecionar a data de fechamento do filtro

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.

Gerenciar o MDR Arquivo Morto Relatórios

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

Para classificar por uma única coluna, (**Hora de criação**/**Período de**/**Período até**), 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.

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/Tempo Absoluto de Exibição** Altere o formato de exibição dos dados da **Hora de criação**; passe o mouse sobre os dados da **Hora de criação** para ver o tempo relativo/absoluto.

Classificação de tabela

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

MDR Colunas do Arquivo Morto de Relatórios

O MDR Arquivo Morto de Relatórios contém as seguintes colunas:

Tipo de relatório: o tipo de relatório (semanal)

Usuários notificados: o endereço de e-mail do usuário que recebeu o ESET MDR relatório

Localidade: o ESET MDR idioma do relatório

Hora de criação: a data em que o ESET MDR relatório foi gerado

Período de: a data de início dos dados registrados no ESET MDR relatório

Período até: a data de encerramento dos dados registrados no ESET MDR relatório

Fuso horário: o fuso horário do ESET MDR relatório

Ações do Arquivo Morto de relatórios

Clique no relatório para selecionar uma das ações:

- **Download**: baixe o relatório como um *.pdf* arquivo
- **Enviar por e-mail**: envie o relatório como um anexo com um e-mail. Você pode selecionar **Idioma do e-mail** no menu suspenso e clicar no botão **Adicionar** para adicionar os **Endereços de e-mail** para escolher os destinatários. Como alternativa, clique no botão **Mais** para **Adicionar usuários** (adicionar o endereço do usuário dos Usuários do computador), **Importar CSV** (importar uma lista personalizada de endereços de um arquivo *.csv* estruturado com delimitadores) ou **Colar da Área de Transferência** (importar uma lista personalizada de endereços separados com delimitadores personalizados; esse recurso funciona de forma semelhante à importação CSV). Depois de clicar no botão **Enviar**, o relatório será enviado como um anexo para o endereço de e-mail selecionado.

> **Registros no MDR Arquivo Morto de Relatórios**
> ESET MDR os relatórios estão presentes no MDR Arquivo Morto de Relatórios há um ano.

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 do cliente Atualizar Agente para atualizar o Agente ESET Management.
- 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**.

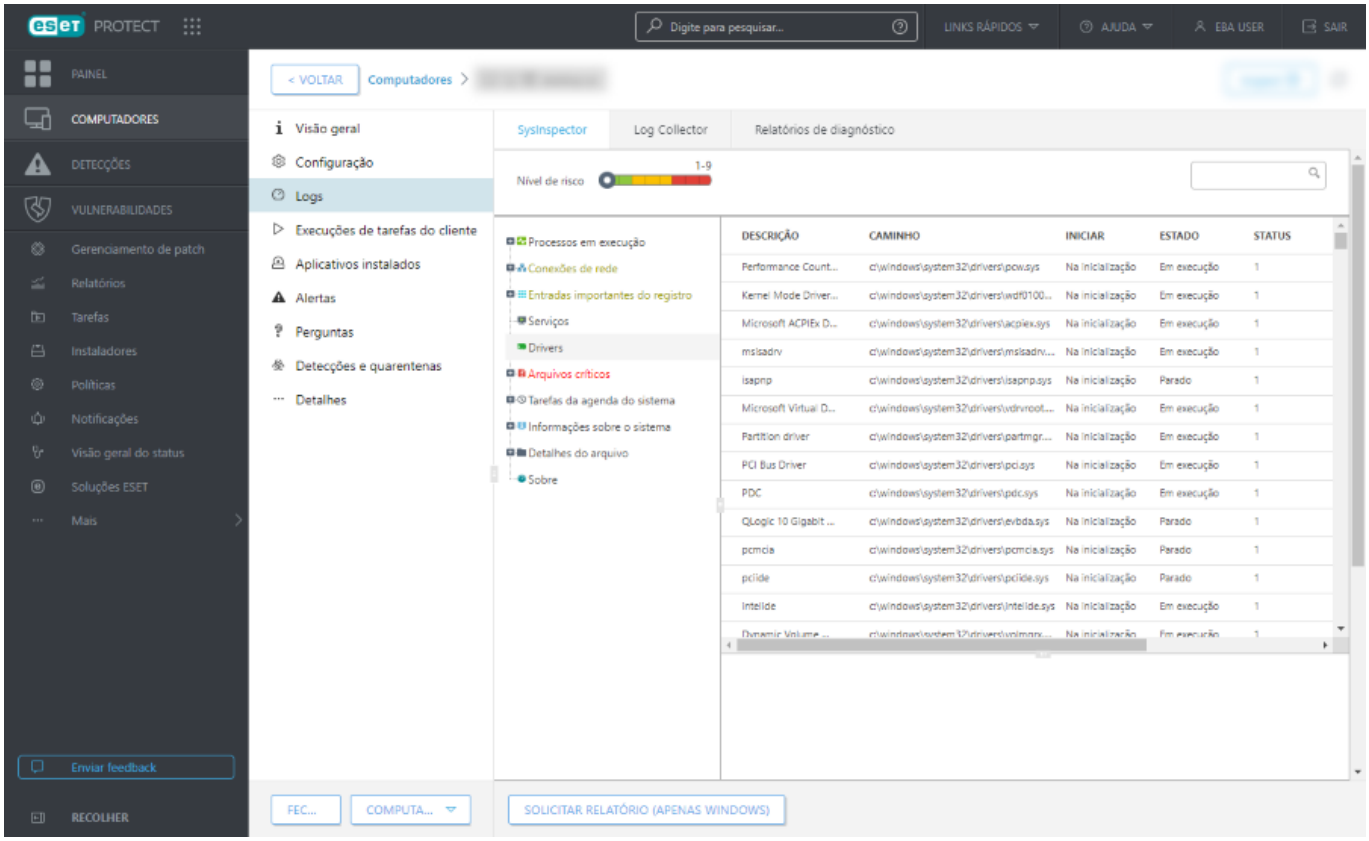
3.Abra o relatório, selecione um computador e selecione **Abrir visualização de relatório SysInspector** no menu suspenso.

Do menu Computadores

1.Navegar para Computadores.

2.Selecione um computador no Grupo Estático ou Dinâmico e clique em **Mostrar Detalhes**.

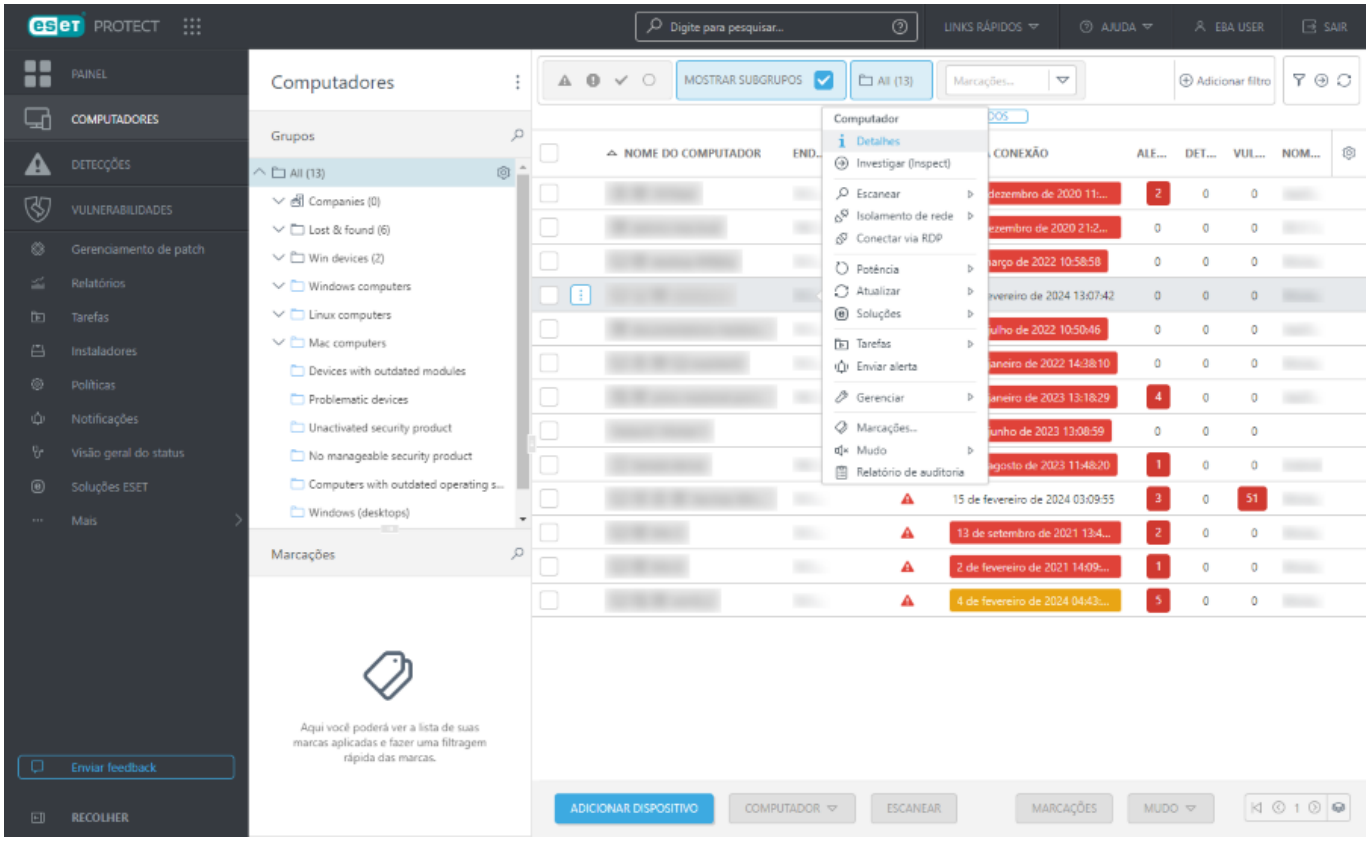
3.Navegue para a seção **Relatórios** > guia **SysInspector**, clique em uma entrada de lista e selecione **Abra o exibidor de Visualizador do Relatório do Sysinspector**.



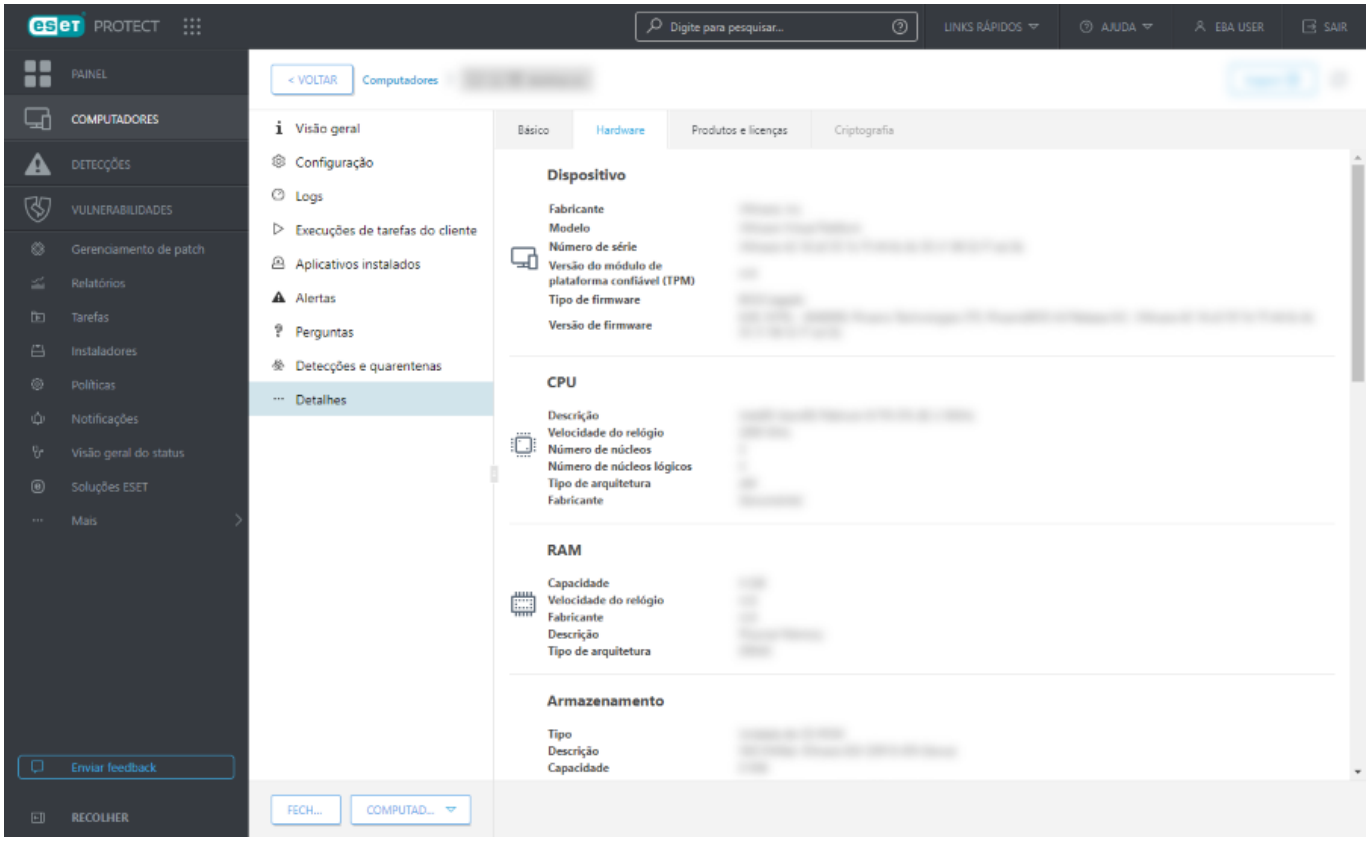
Inventário de hardware

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 Servidor ESET PROTECT.

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 as **Tarefas** para gerenciar o Servidor ESET PROTECT, computadores 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 Servidor ESET PROTECT. Por isso, pode levar algum tempo para os resultados de uma execução de tarefa serem comunicados ao Servidor ESET PROTECT.

- As tarefas do servidor são executadas pelo Servidor ESET PROTECT em si próprio 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

Verificar se há atualização do produto
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
Interromper gerenciamento (desinstalar agente ESET Management)
Atualizar Agente

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)

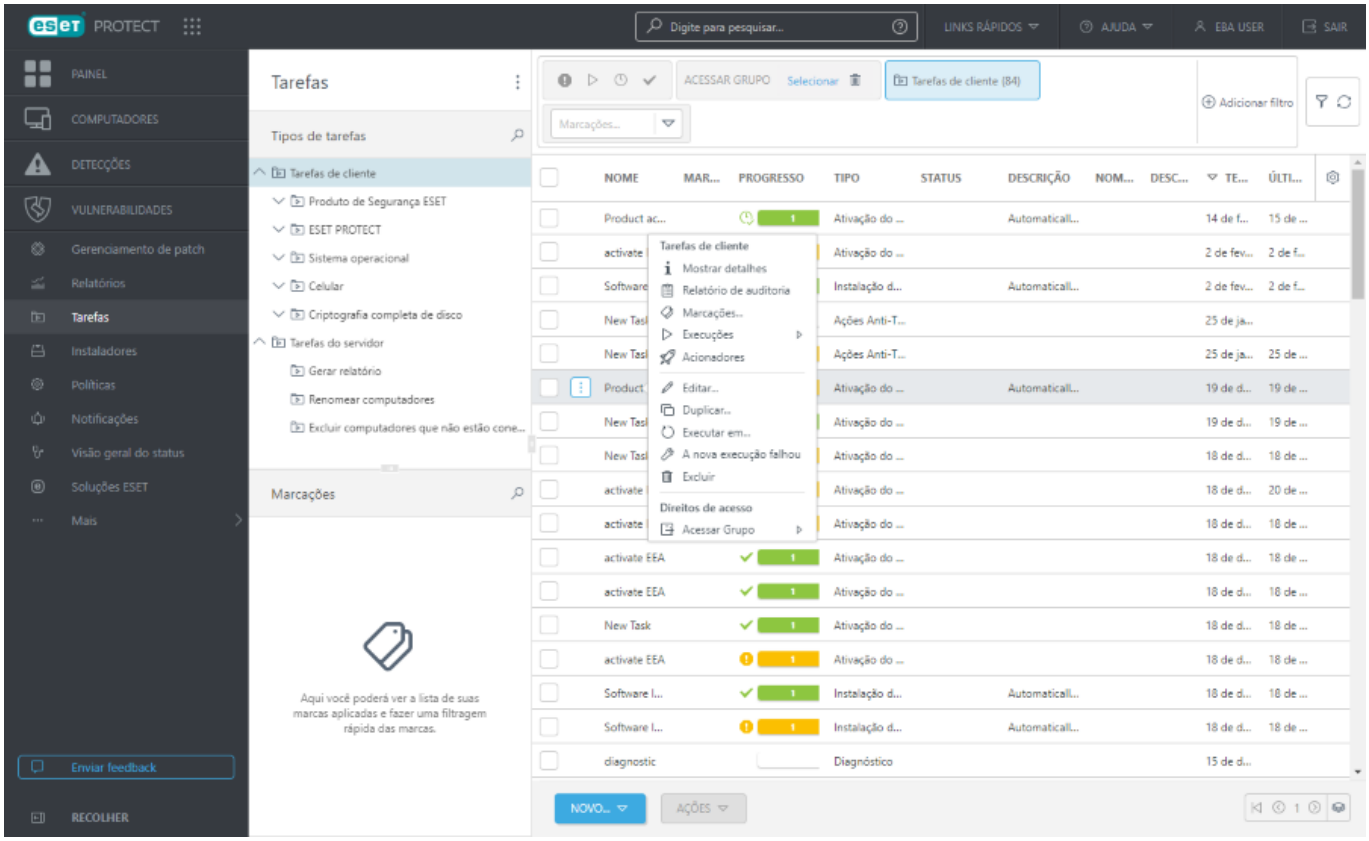
Tarefas do servidor

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.

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:

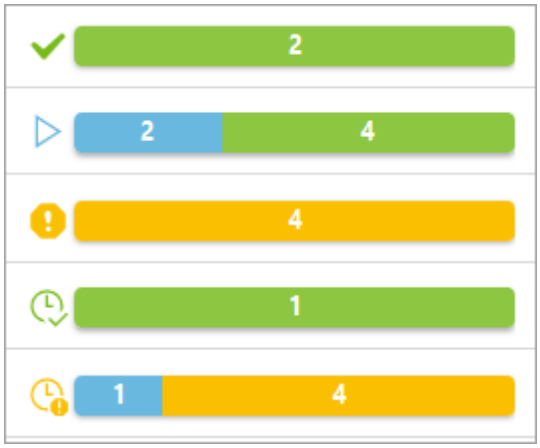
Em execução (azul)

Concluído com sucesso (verde)

Falha (laranja)

Tarefa criada recentemente (branco) - pode levar algum tempo até que o indicador mude de cor, o Servidor ESET PROTECT precisa 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 Servidor ESET PROTECT. 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**

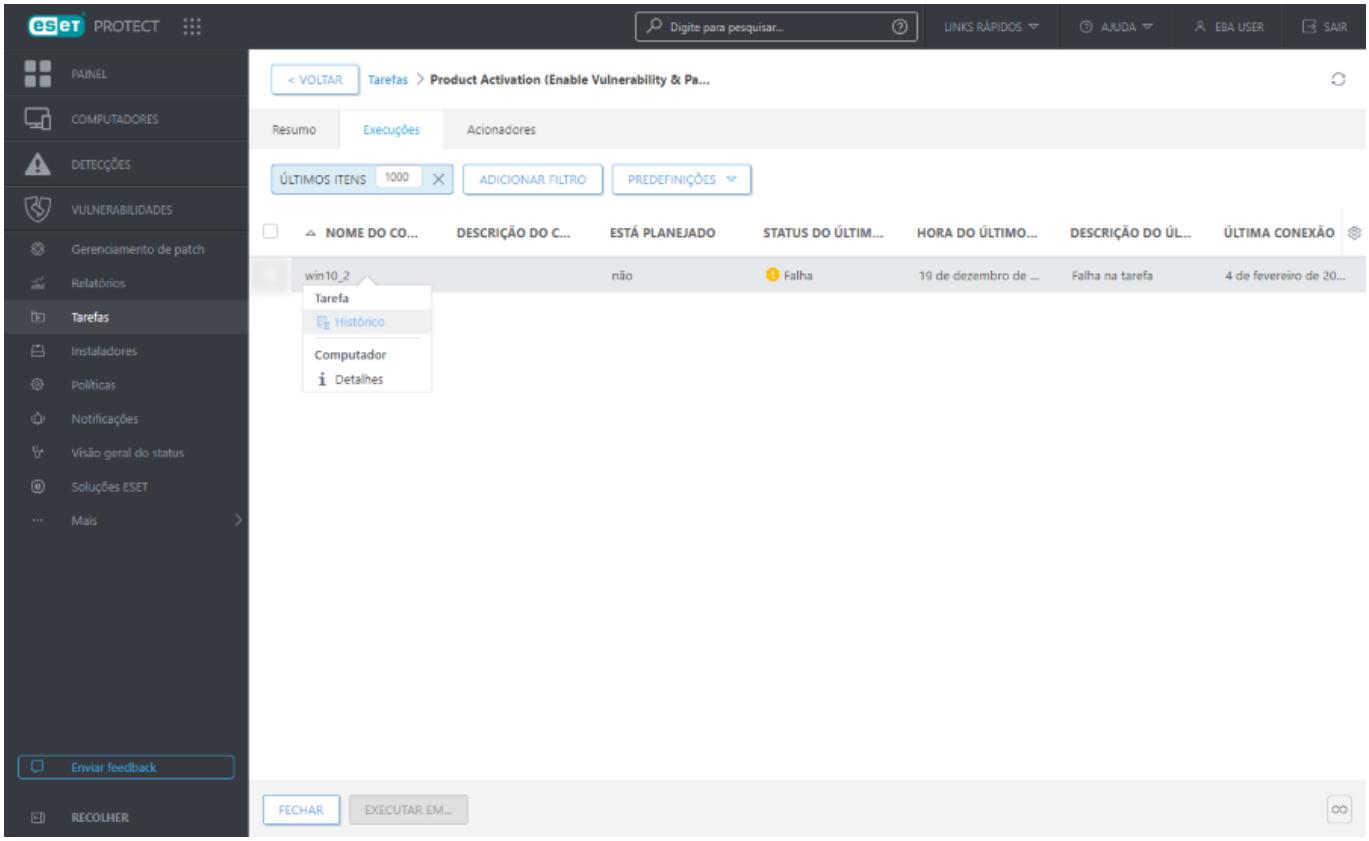
Você pode modificar o filtro ou desligá-lo para ver todos os computadores, independentemente do seu último status.

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**.

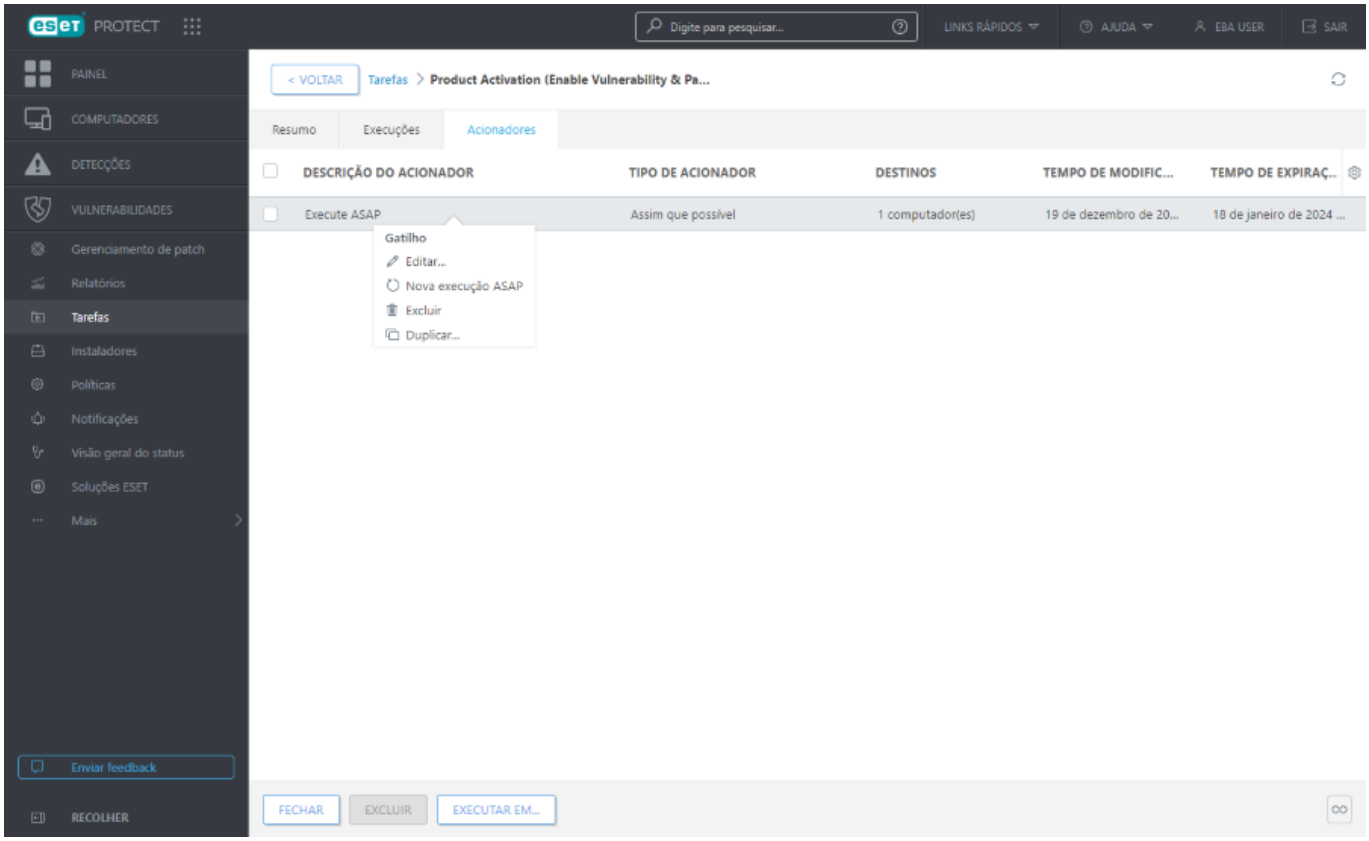
- **Detalhes** – exibir detalhes para o computador selecionado.



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:

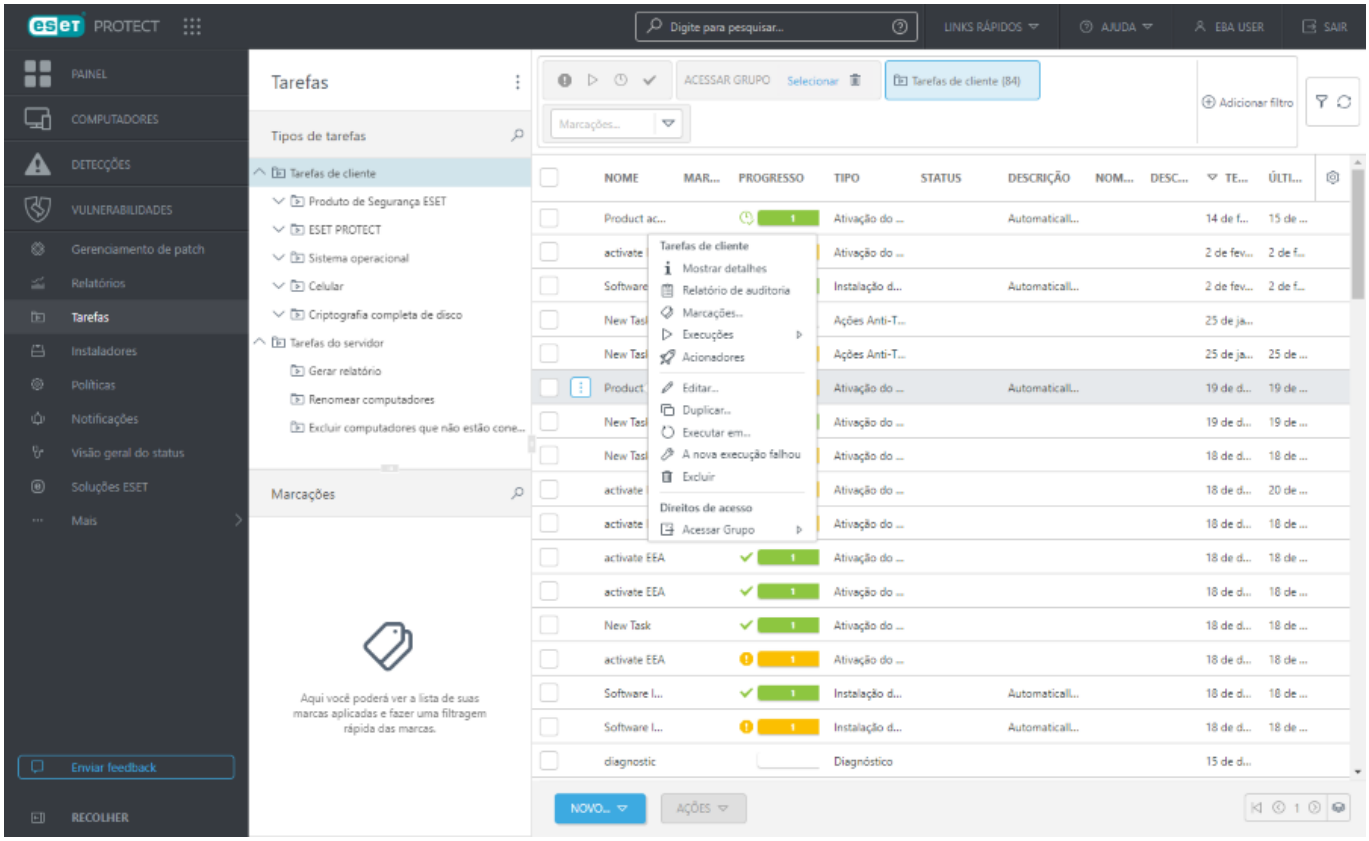
Editar	Editar o Acionador selecionado.
Nova execução ASAP	Executar novamente a tarefa do cliente (assim que possível) usando um Acionador existente logo em seguida sem nenhuma modificação.
Excluir	Remove completamente o acionador selecionado. Para remover vários acionadores, marque as caixas de seleção 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 Servidor ESET PROTECT. Por isso, pode levar algum tempo para os resultados de uma execução de tarefa serem comunicados ao Servidor ESET PROTECT.

Em **Tarefas** você pode ver a barra de indicadores de progresso, o ícone de status e os detalhes para cada tarefa criada.



Encontre mais informações sobre tarefas do cliente (processo de eliminação) criadas no ESET Connect. Você pode ver os resumos de tarefas do cliente; no entanto, você não pode editá-los ou criá-los.

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.

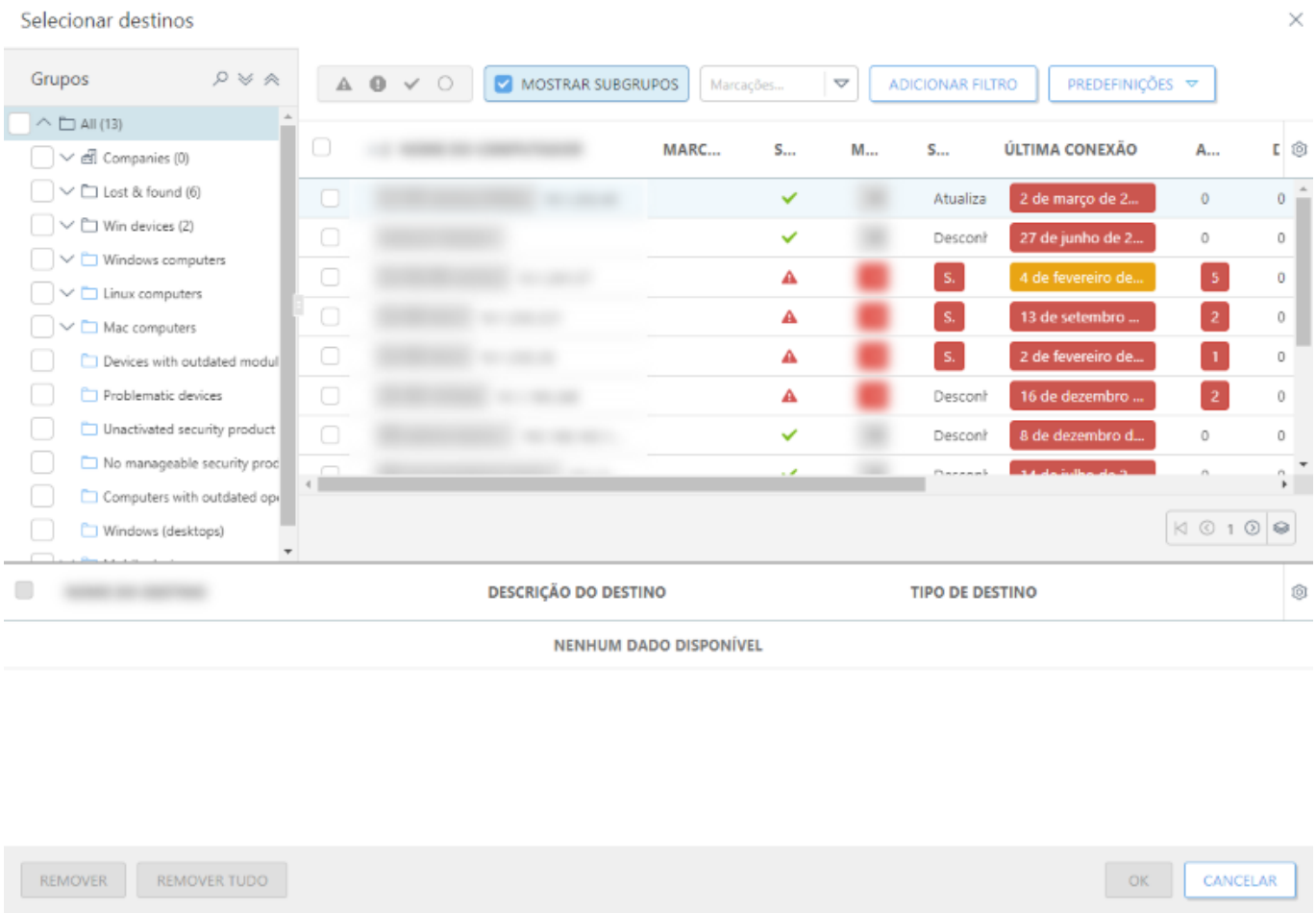
Básico

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. Você pode definir a data de expiração para até 6 meses da data atual.
- **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.

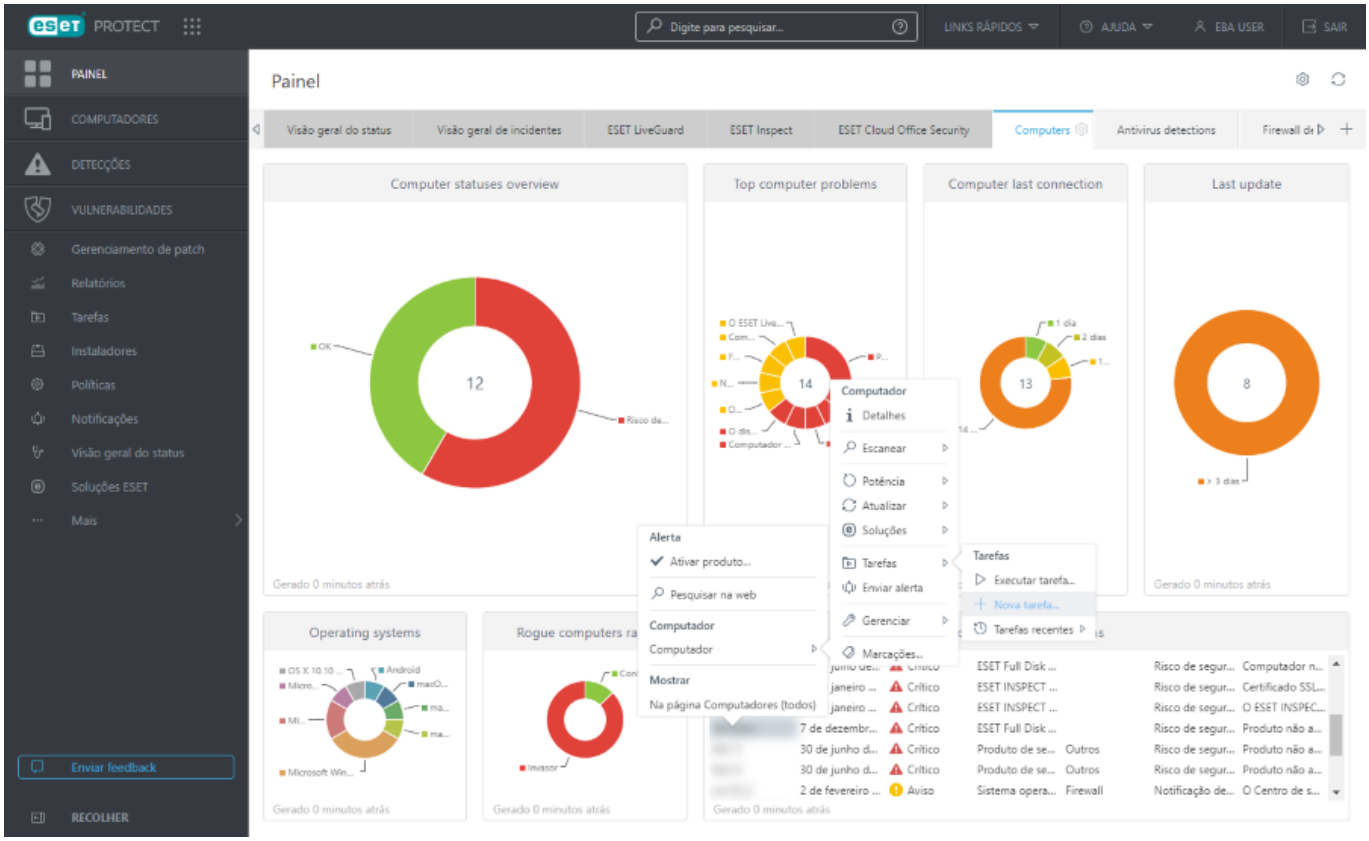
Clique em **Concluir** quando tiver definido os destinatários dessa tarefa e os acionadores que executam a tarefa.

Atribuir Tarefa do cliente a um Grupo ou Computador(es)

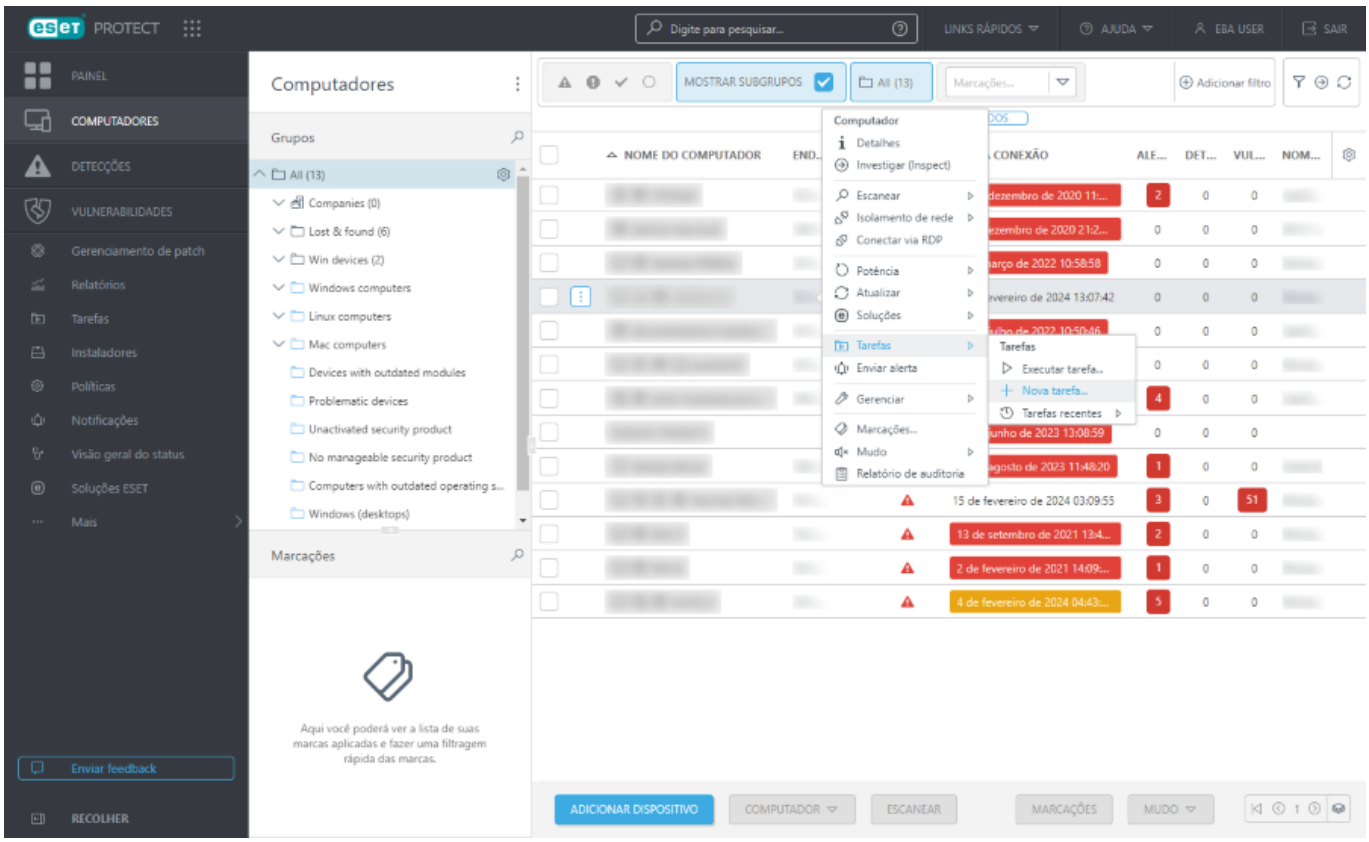
Leia aqui como Atribuir uma tarefa do cliente a um grupo.

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**.

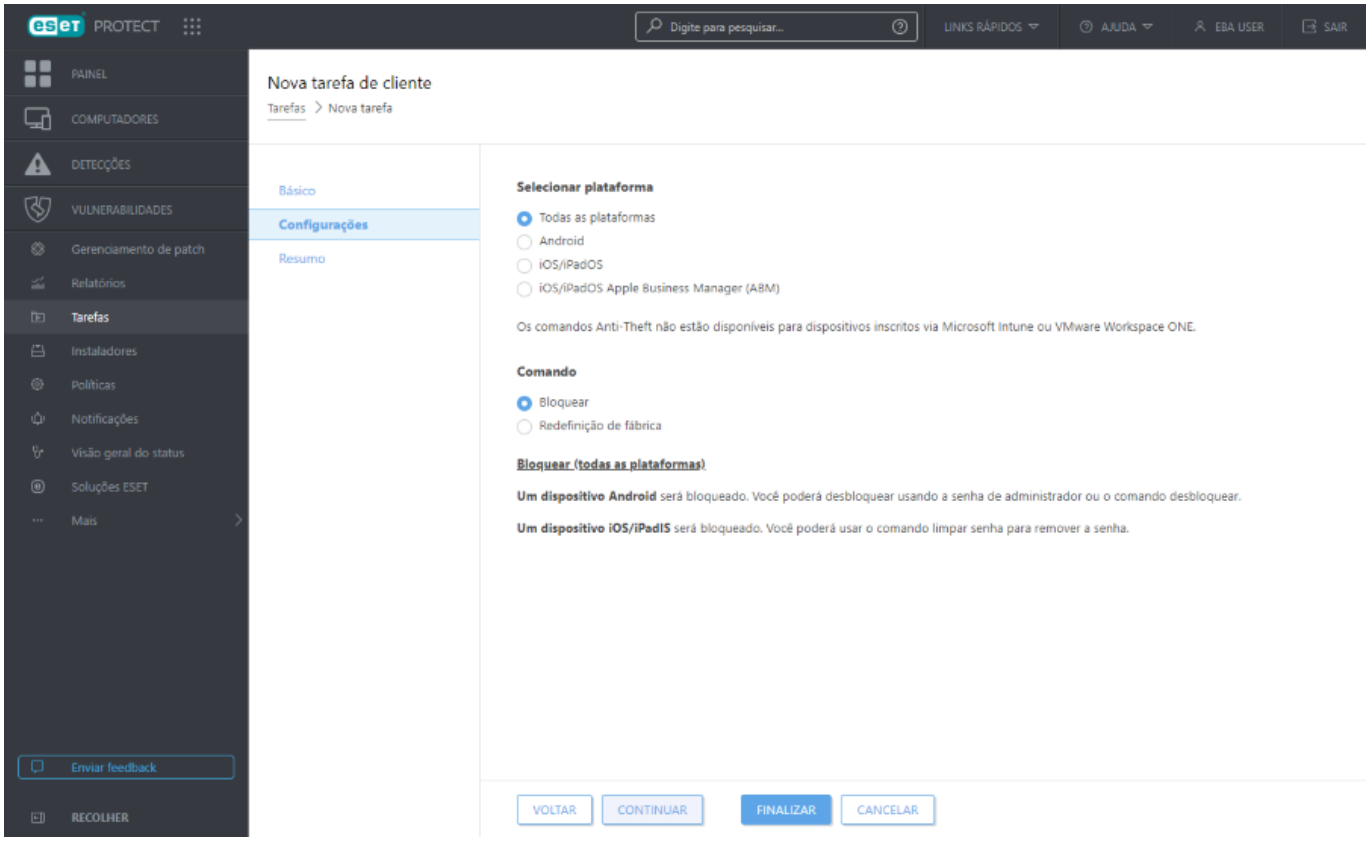
Básico

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.

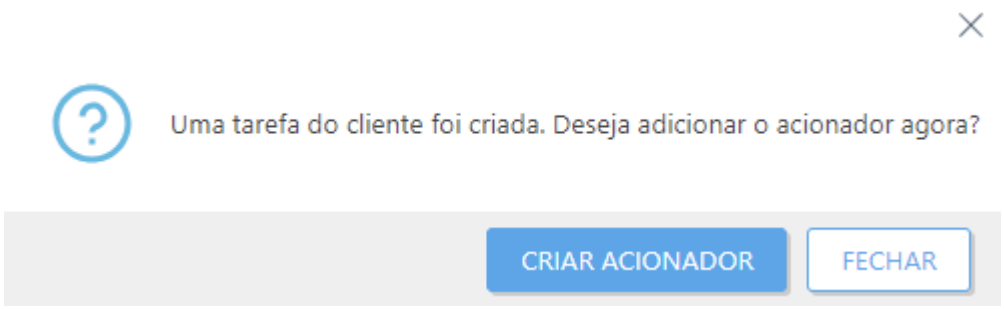
Ação	Comportamento em sistemas operacionais móveis	Descrição
Redefinição de fábrica		Todos os dados acessíveis no dispositivo serão apagados (cabeçalhos de arquivos serão destruídos) e o dispositivo será redefinido para suas configurações padrão de fábrica. Isso pode demorar vários minutos.
		Todas as configurações e informações serão removidas e o dispositivo será definido para suas configurações padrão de fábrica. Isso pode demorar vários minutos.
Ativar o Modo perdido 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.

> **Gatilhos de tarefas do cliente de dispositivo móvel**
> Você pode usar apenas esses gatilhos para tarefas de cliente de dispositivo móvel:
> • Assim que possível
> • Gatilho de grupo dinâmico ingressado
> As tarefas do cliente com gatilhos diferentes dos acima falharão com a mensagem **Tipo de gatilho sem suporte**.

Verificar se há atualização do produto

A tarefa **Verificar atualização de produto** impõe a verificação de atualizações de produtos de segurança ESET (atualizações automáticas) em computadores gerenciados:

> Os produtos de segurança ESET compatíveis:
> • ESET Endpoint Antivirus/Security para Windows versão 10.1 e versões posteriores
> • ESET Server Security para Microsoft Windows Server versão 11.0 e versões posteriores

- Se uma versão posterior do produto de segurança ESET estiver disponível, ela será baixada.

- A atualização do produto de segurança ESET requer uma reinicialização do computador, mas não imediatamente (a reinicialização não é imposta). O administrador ESET PROTECT pode impor a atualização do computador e reiniciar remotamente a partir do Web Console usando a caixa de seleção Encerrar tarefa de cliente do computador com a caixa de seleção **Reinicializar computador(es)** marcada.

- O produto de segurança ESET anterior permanece totalmente funcional até a reinicialização. A atualização ocorre após a próxima reinicialização do computador.

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.

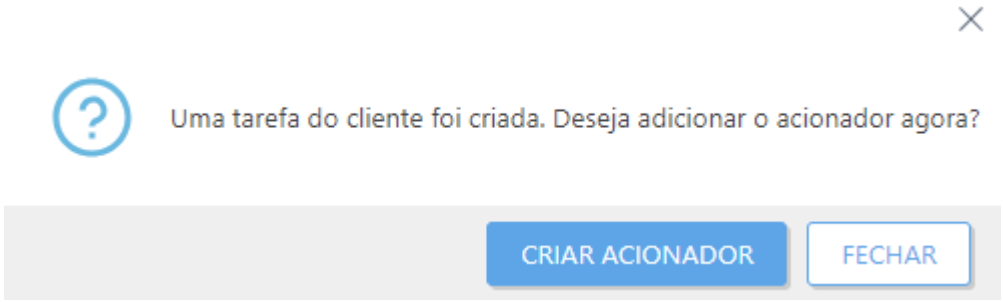
Configurações

> 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.

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 entrega do relatório por dispositivo é de 15 MB. Você pode acessar relatórios do Web Console na seção **Detalhes** > **Relatórios**. Se os relatórios coletados pela tarefa forem maiores que 15 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.

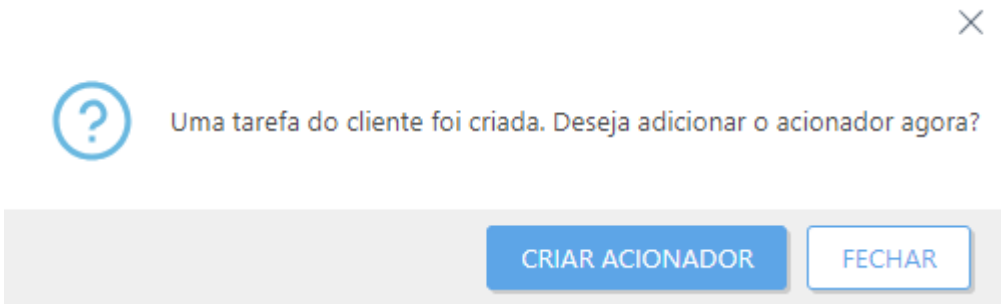
Relatórios de diagnóstico com mais de 24 horas são removidos todos os dias durante a limpeza da meia noite. Isso protege o banco de dados ESET PROTECT de uma sobrecarga.

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.

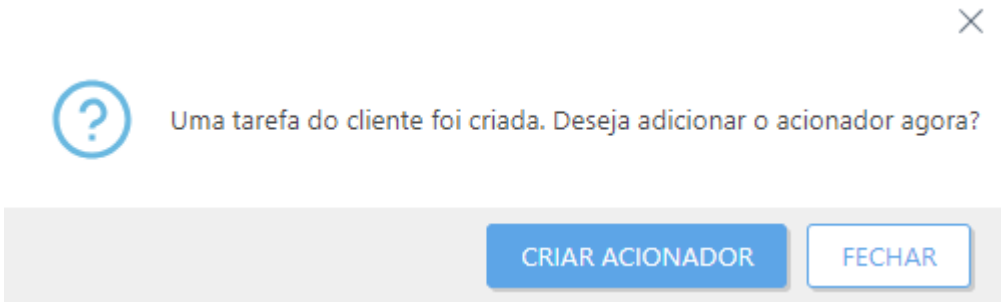
Configurações

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

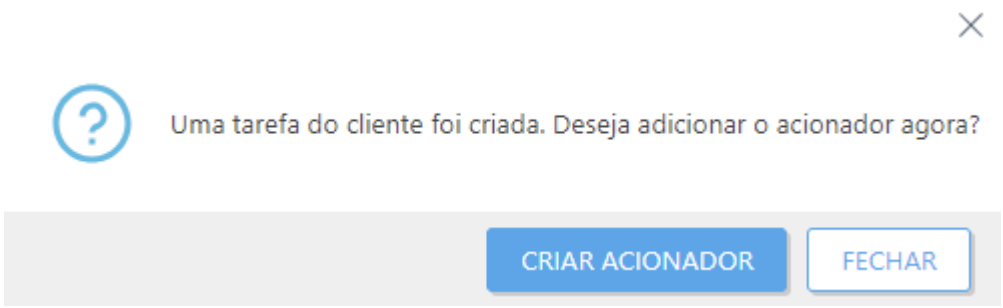
Na seção **Básico**, insira informações básicas sobre a tarefa, como **Nome e Descrição (opcional)**. Clique em **Selecionar marcações** para atribuir marcações.
No menu suspenso **Tarefa**, selecione o tipo de tarefa que deseja criar e configurar. Se você selecionou um tipo de tarefa específico antes 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

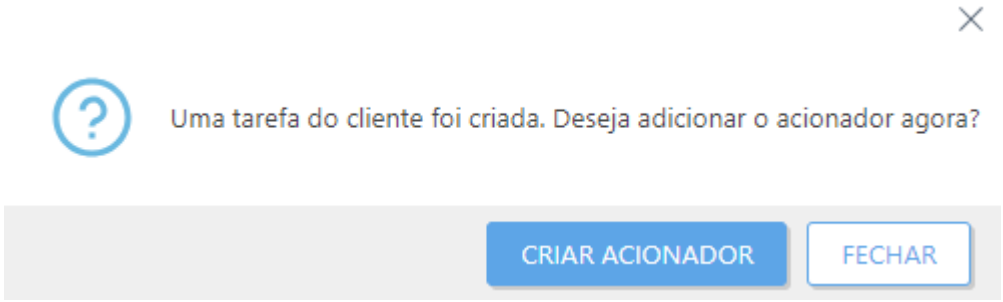
Exportar definições de configuração de produtos gerenciados.

- **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).
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.

Sistemas operacionais compatíveis

O isolamento de rede está disponível para dispositivos Windows e macOS.

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

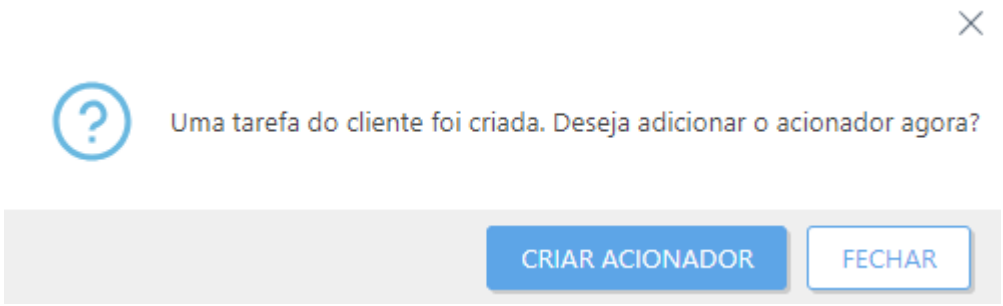
Na seção **Básico**, insira informações básicas sobre a tarefa, como **Nome e Descrição (opcional)**. Clique em **Selecionar marcações** para atribuir marcações.
No menu suspenso **Tarefa**, selecione o tipo de tarefa que deseja criar e configurar. Se você selecionou um tipo de tarefa específico antes 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

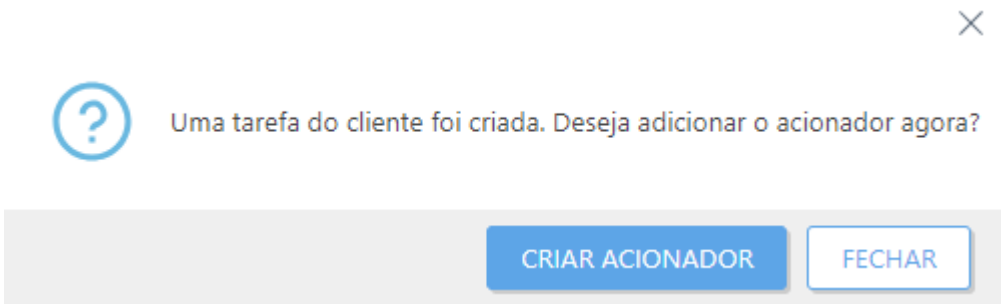
Na seção **Básico**, insira informações básicas sobre a tarefa, como **Nome e Descrição (opcional)**. Clique em **Selecionar marcações** para atribuir marcações.
No menu suspenso **Tarefa**, selecione o tipo de tarefa que deseja criar e configurar. Se você selecionou um tipo de tarefa específico antes 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.

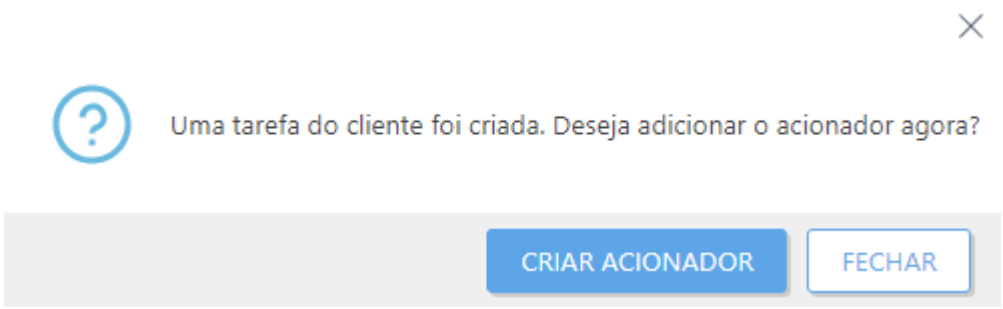
Configurações

- **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

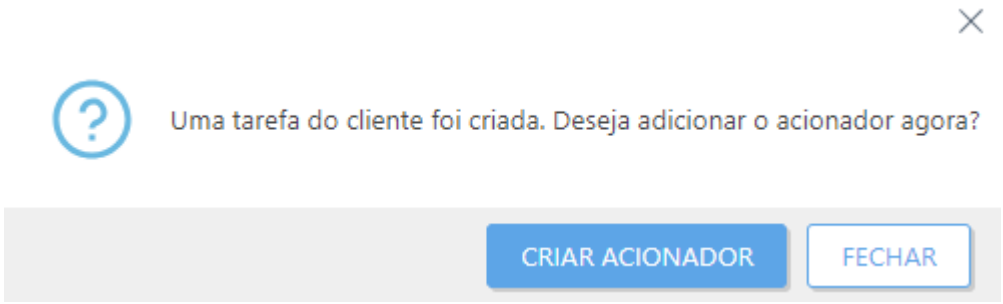
- **Ativar atualizações** - As atualizações estão ativadas e o cliente receberá a próxima atualização do módulo.
- **Reverter e desativar atualizações da próxima vez** - As atualizações são desativadas pelo período de tempo especificado no menu suspenso **Desativar intervalo** (12, 24, 36, 48 horas ou 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 **Escaneamento 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 escaneamento personalizado permite especificar parâmetros de escaneamento, como o escaneamento de destinos e métodos de escaneamento. 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).

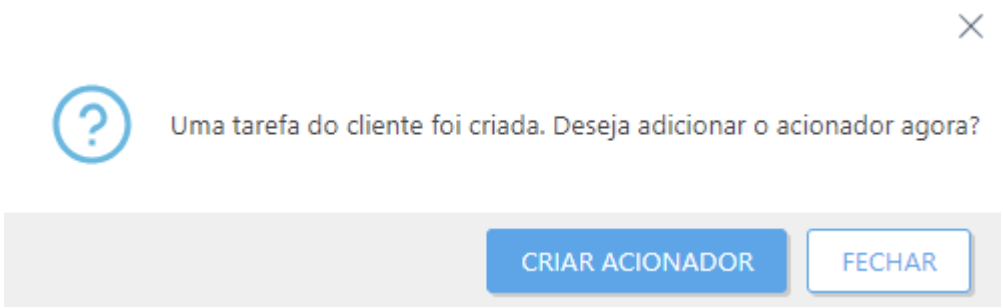
Abaixo mostramos alguns exemplos de como usar os parâmetros de destino de **Rastreamento sob demanda**:
■Arquivo: *C:\Users\Data.dat*
■Pasta *C:\MyFolder*
■Caminho Unix ou arquivo */usr/data*
■Local Windows UNC *\\server1\scan_folder*
■String predefinida `${Memory}`

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:

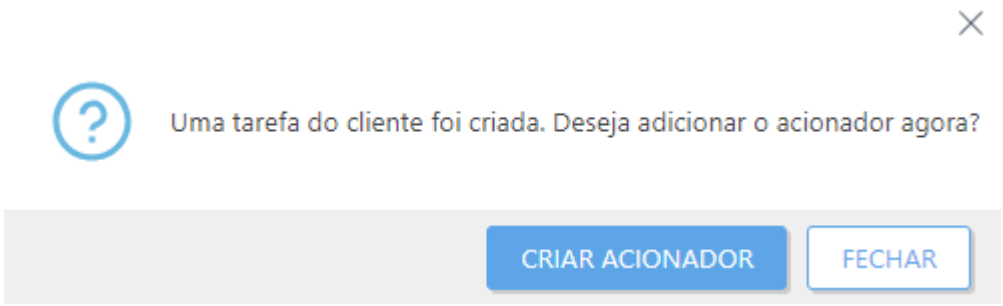
- O Windows vai notificar o usuário do computador sobre a reinicialização forçada planejada 4 horas antes da reinicialização e 10 minutos antes da reinicialização.
- O macOS será reiniciado imediatamente depois da atualização.

- 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.

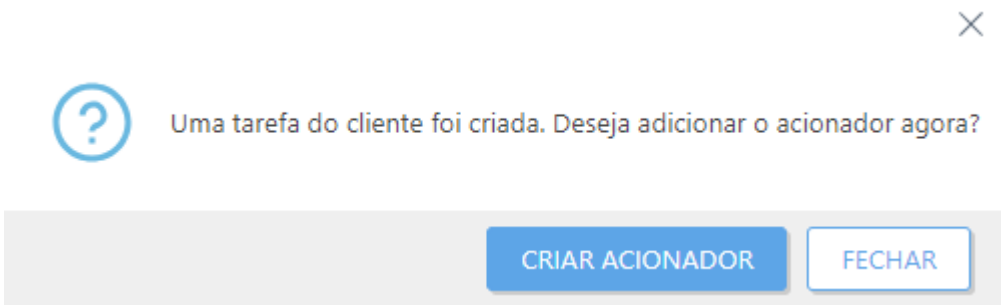
Configurações de filtro:

- **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.

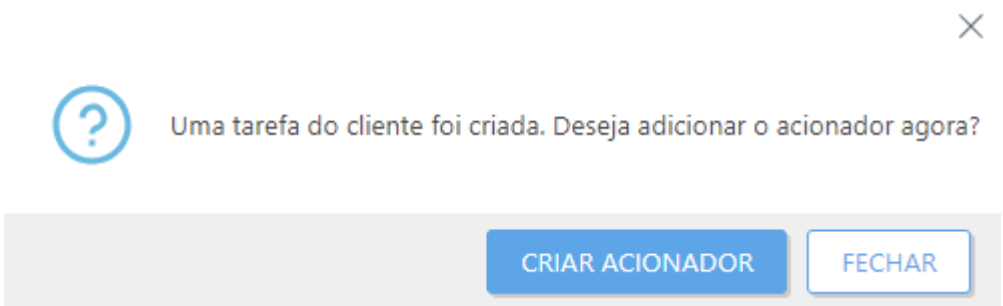
Configurações

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**).

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.

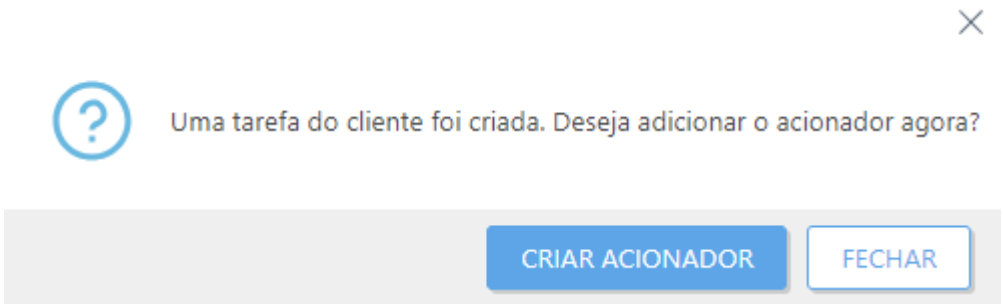
Execute a tarefa com cuidado. Depois do Agente ESET Management atual ser redefinido, todas as tarefas sendo executadas nele serão abandonadas. O status de execução **Em execução**, **Concluído** ou **Falha** desta tarefa pode não ser observado, dependendo da replicação de dados.

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.

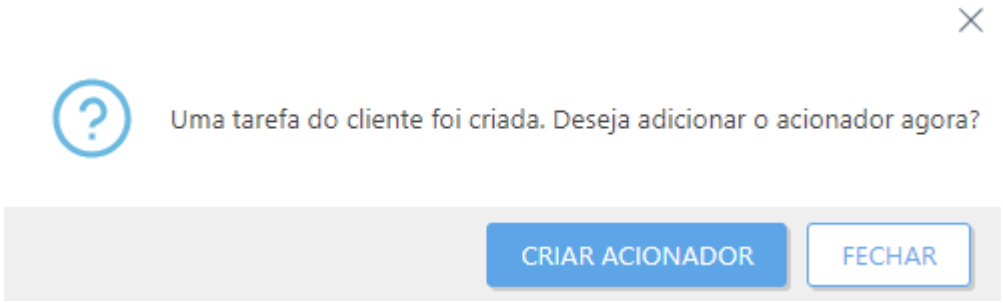
Ao criar um acionador para esta tarefa, tenha como destino um computador no qual o Sensor RD está instalado.

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):

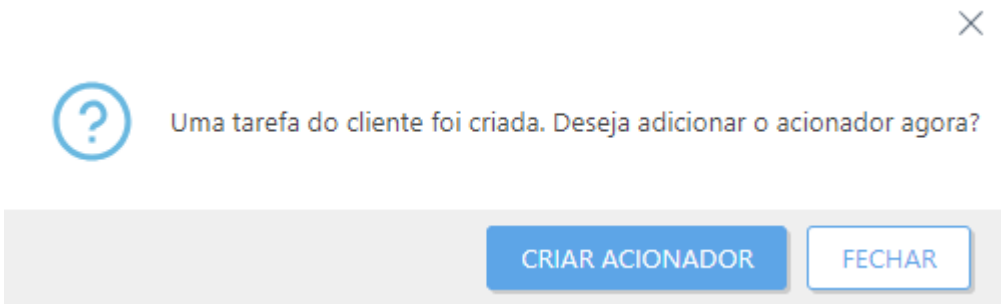
```
net stop service_name
net start service_name
```

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.

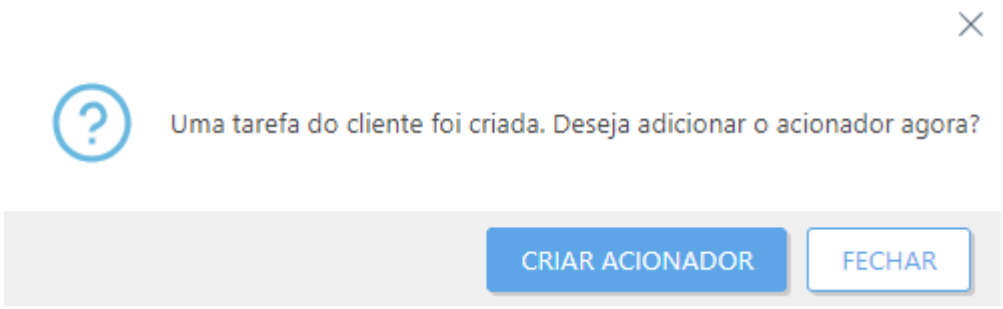
Configurações

- **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 Web 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.

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.
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 Verificado** e selecione um computador com o produto de segurança do servidor ESET instalado. 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 escaneamento ESET Management**:

- **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.

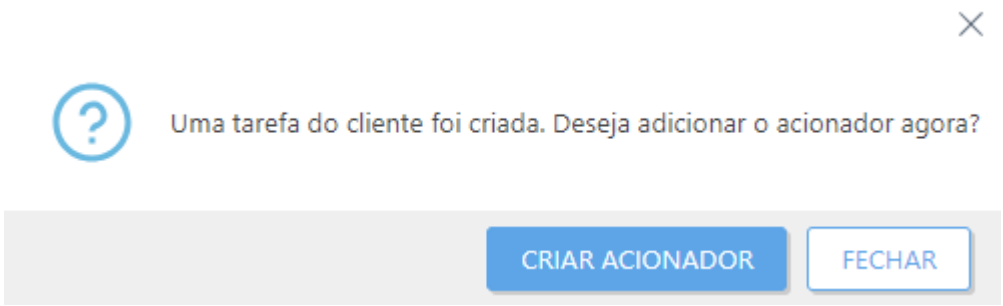
Você pode configurar o comportamento de reinicialização/desligamento dos computadores gerenciados. O computador deve executar um Agente ESET Management 9.1 e um produto de segurança ESET compatível com esta configuração.

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** > **Ativar produto de segurança** para ativar 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.

Tanto o Servidor ESET PROTECT quanto 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 Agentes ESET Management. Em vez disso, use a tarefa Atualizar 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.

Configurações

Pacote a instalar – existem duas opções:

- **Instalar pacote de repositório**

  oEscolher sistema operacional – selecione o sistema operacional para a instalação do produto.

  oEscolher 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**.

oInstalar 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**).

• 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 **Eu aceito o Acordo de licença de usuário final 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.

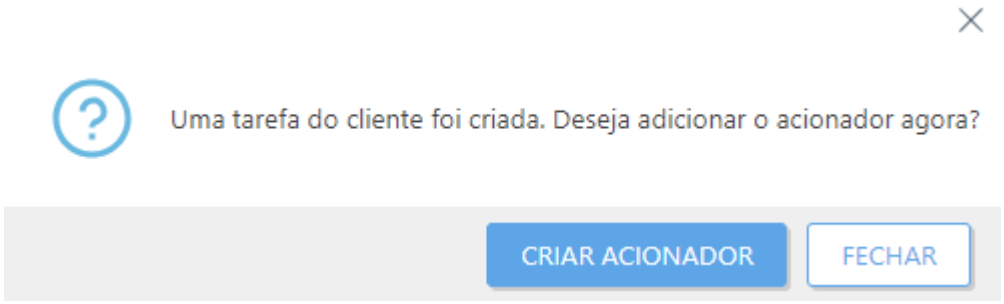
Você quer instalar o software no Linux usando o arquivo *install_script.sh* que tem dois parâmetros: `-a` é o primeiro parâmetro, `-b` é o segundo parâmetro.
Instalação no terminal (como usuário root na pasta onde o *install_script.sh está localizado*):
```
./install_script.sh -a parameter_1 -b parameter_2
```
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

Selecione uma opção no menu suspenso **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 ESET Management estiver protegido por senha, você deverá fornecer a senha para desinstalar, reparar ou atualizar (com alterações). Recomendamos redefinir algumas configurações que você não quer manter (por exemplo, proteção por senha) para as configurações padrão usando uma política antes do dispositivo ser removido do gerenciamento.
• Todas as tarefas sendo executadas no agente serão abandonadas. O status de execução **Em execução**, **Concluído** ou **Com falha** dessa tarefa poderá não ser exibido com precisão no console da Web ESET PROTECT, dependendo da replicação de dados.
• Depois do Agente ser desinstalado é possível gerenciar seu produto de segurança através da EGUI integrada ou do eShell.

• **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.

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.

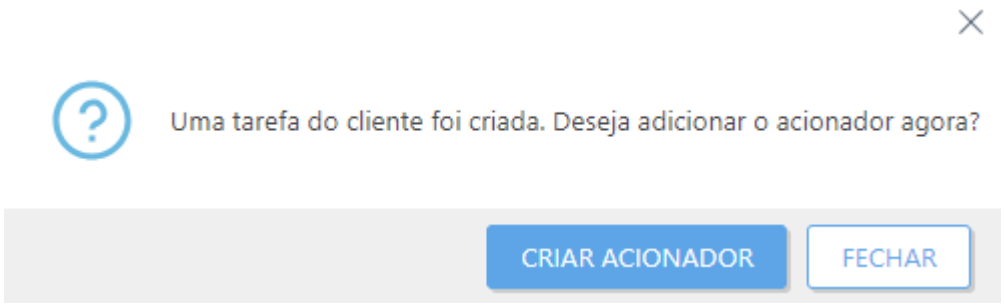
Resumo

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 ESET Management estiver protegido por senha, você deverá fornecer a senha para desinstalar, reparar ou atualizar (com alterações). Recomendamos redefinir algumas configurações que você não quer manter (por exemplo, proteção por senha) para as configurações padrão usando uma política antes do dispositivo ser removido do gerenciamento.
- Todas as tarefas sendo executadas no agente serão abandonadas. O status de execução **Em execução**, **Concluído** ou **Com falha** dessa tarefa poderá não ser exibido com precisão no console da Web ESET PROTECT, dependendo da replicação de dados.
- Depois do Agente ser desinstalado é possível gerenciar seu produto de segurança através da EGUI integrada ou do eShell.

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

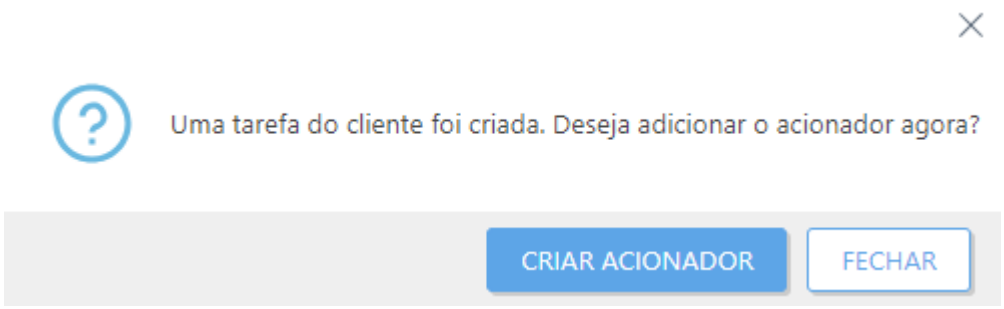
Na seção **Básico**, insira informações básicas sobre a tarefa, como **Nome e Descrição (opcional)**. Clique em **Selecionar marcações** para atribuir marcações.
No menu suspenso **Tarefa**, selecione o tipo de tarefa que deseja criar e configurar. Se você selecionou um tipo de tarefa específico antes 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

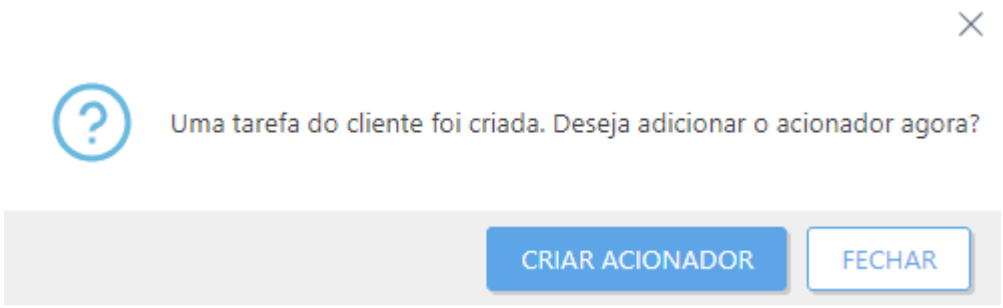
- **Armazenar registro em cliente** - selecione isso se quiser armazenar o log do SysInspector no cliente, bem como no Servidor ESET PROTECT. Por exemplo, quando um cliente tiver o ESET Endpoint Security instalado, o relatório geralmente será armazenado em *C:\Program Data\ESET\ESET Security\SysInspector*.

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.

Atualizar Agente

Você pode usar a tarefa **Atualizar Agente** para atualizar o Agente ESET Management para a versão mais recente.

O ESET PROTECT é compatível com a atualização automática de Agentes ESET Management em computadores

gerenciados.

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**.

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)

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

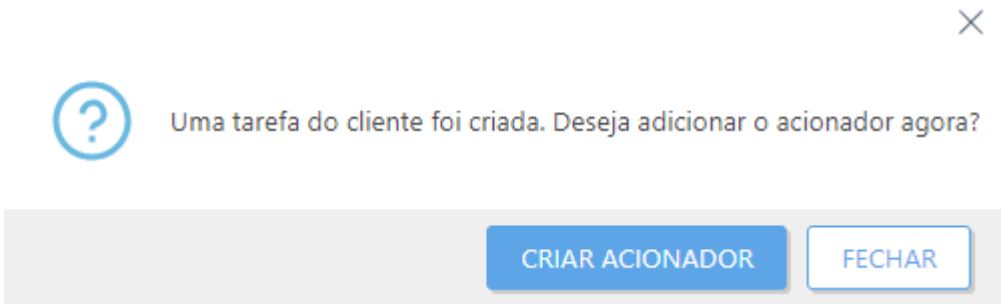
Selecione a caixa de seleção **Eu aceito o Acordo de licença de usuário final e reconheço a Política de Privacidade**. Consulte o Acordo de Licença para o Usuário Final (EULA), Termos de Uso e Política de Privacidade dos produtos ESET.

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.

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

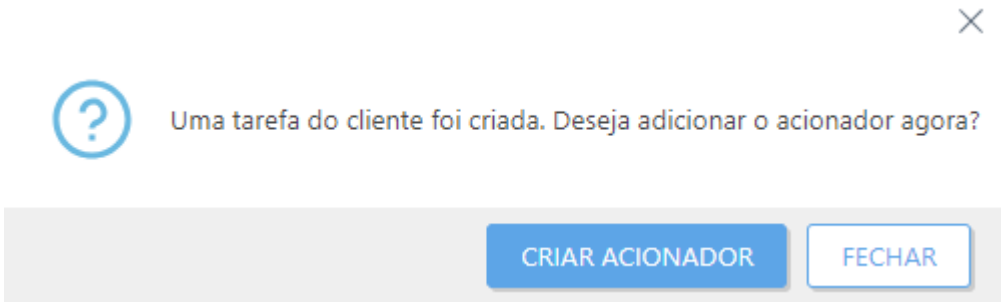
- **Objeto em quarentena** - selecione um objeto específico da quarentena.
- **Senha do objeto** - insira uma senha para criptografar o objeto por motivos de segurança. Note que a senha será exibida no relatório correspondente.
- **Carregar caminho** - insira um caminho para um local no qual deseja carregar 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 Servidor ESET PROTECT em si próprio 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.

Tarefas do servidor

- Excluir computadores não conectando
- Gerar relatório
- Renomear computadores

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.

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.

Os Usuários do MSP podem filtrar o relatório selecionando o cliente.

- **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.

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.

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.

Gatilhos de tarefas do cliente de dispositivo móvel

Você pode usar apenas esses gatilhos para tarefas de cliente de dispositivo móvel:
- Assim que possível
- Gatilho de grupo dinâmico ingressado

As tarefas do cliente com gatilhos diferentes dos acima falharão com a mensagem **Tipo de gatilho sem suporte**.

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. Você pode definir a data de expiração para até 6 meses da data atual.

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 Web 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**).

Outro

• **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

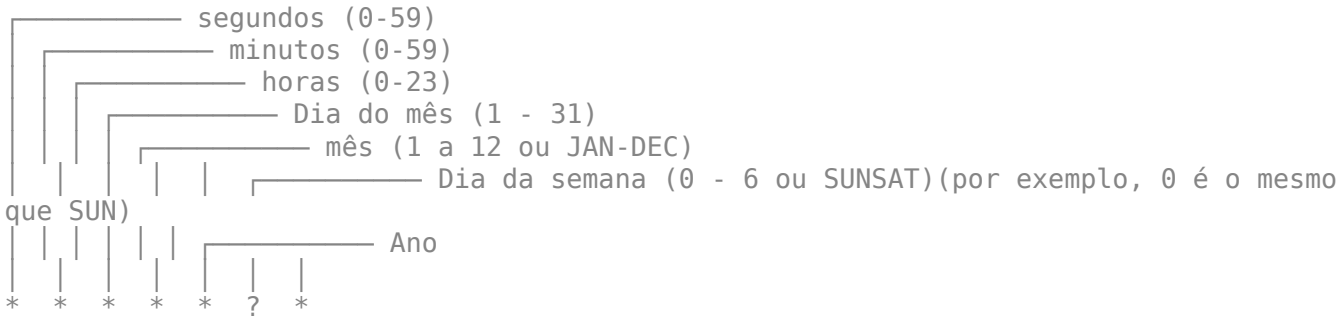
Uma expressão CRON é usada para configurar instâncias específicas de um acionador. Principalmente para o acionamento repetitivo agendado. É uma string composta de 6 ou 7 campos que representam valores individuais da agenda. Esses campos são separados por um espaço e contém qualquer um dos valores permitidos 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:



- 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 Servidor ESET PROTECT.

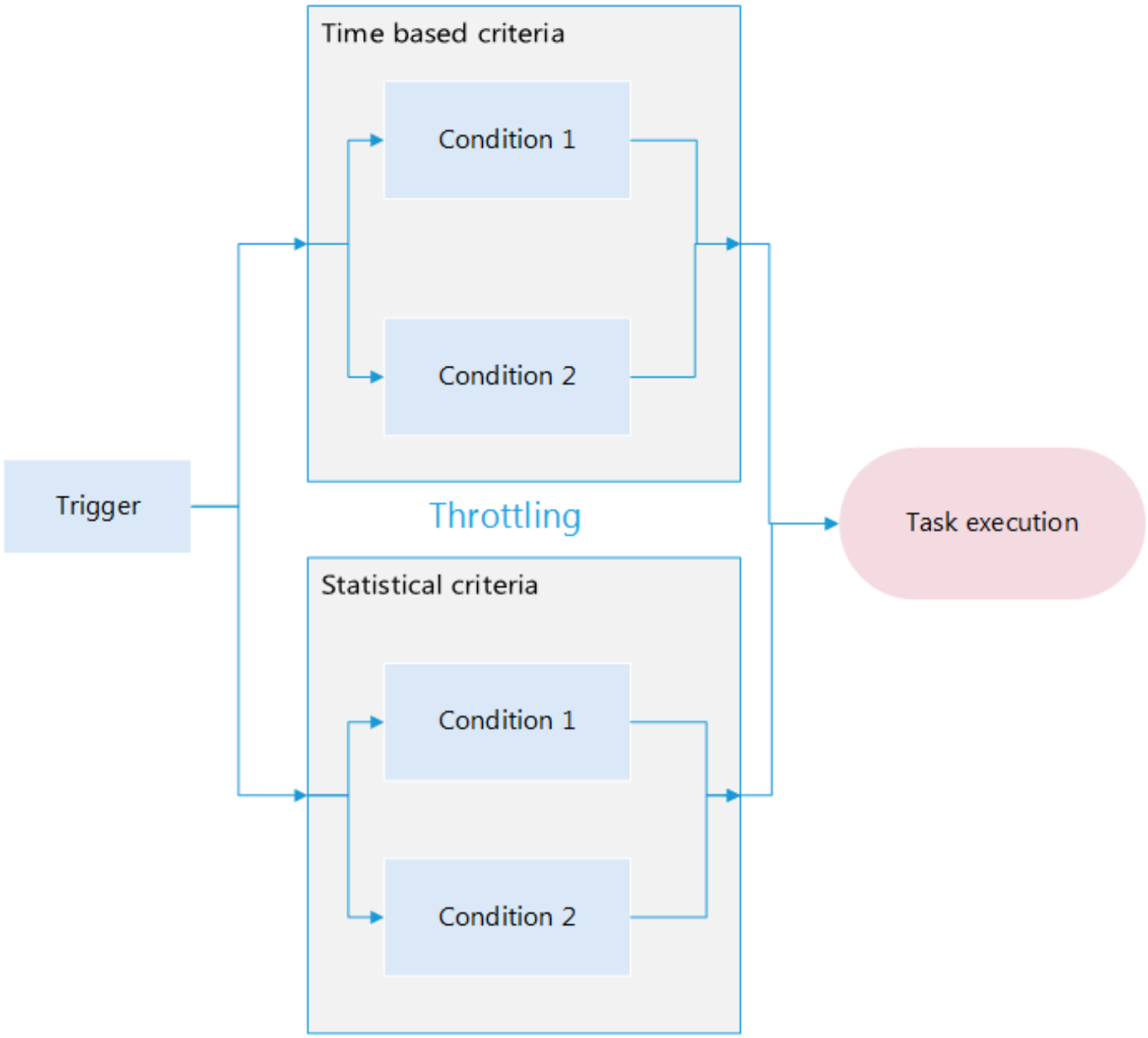
Exemplos reais que ilustram algumas variações da Expressão CRON:

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 Servidor ESET PROTECT forem reiniciados. 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.

Você deve configurar o throttling com critérios baseados em tempo para restringir a execução da tarefa a no máximo uma vez a cada 15 minutos e as notificações a no máximo uma vez a cada 1 minuto (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***.

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

Hora	00	01	02	03	04	05	06	Acionador é modificado	07	08	09	10	11	12	13
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

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
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 Web Console ESET PROTECT e você pode fazer download deles novamente quando necessário.

Clique em **Instaladores** > **Criar Instalador** e selecione o sistema operacional.

Selecione as configurações do instalador, aceite o Acordo de Licença para o Usuário Final e selecione uma das opções de distribuição do instalador (as configurações do instalador e opções de distribuição podem variar de acordo com o sistema operacional):

- Clique em **Download** para fazer download do pacote do instalador.
- Clique no ícone **Copiar** para copiar o link do instalador para sua área de transferência.
- Clique no ícone **E-mail** para enviar um e-mail com um link para o pacote do instalador.

Ou clique em **Personalizar instalador** para acessar mais opções antes de fazer download do pacote do instalador:

Windows

- Fazer download ou enviar instalador ou usar a ESET Remote Deployment Tool – o pacote do 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, além da capacidade de selecionar um Grupo principal. Você pode implantar o instalador de forma local ou remota (usando o ESET Remote Deployment Tool).

- 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.

- 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).

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).

Android ou iOS/iPadOS

Inscrever dispositivos móveis no Web Console da nuvem.

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**.

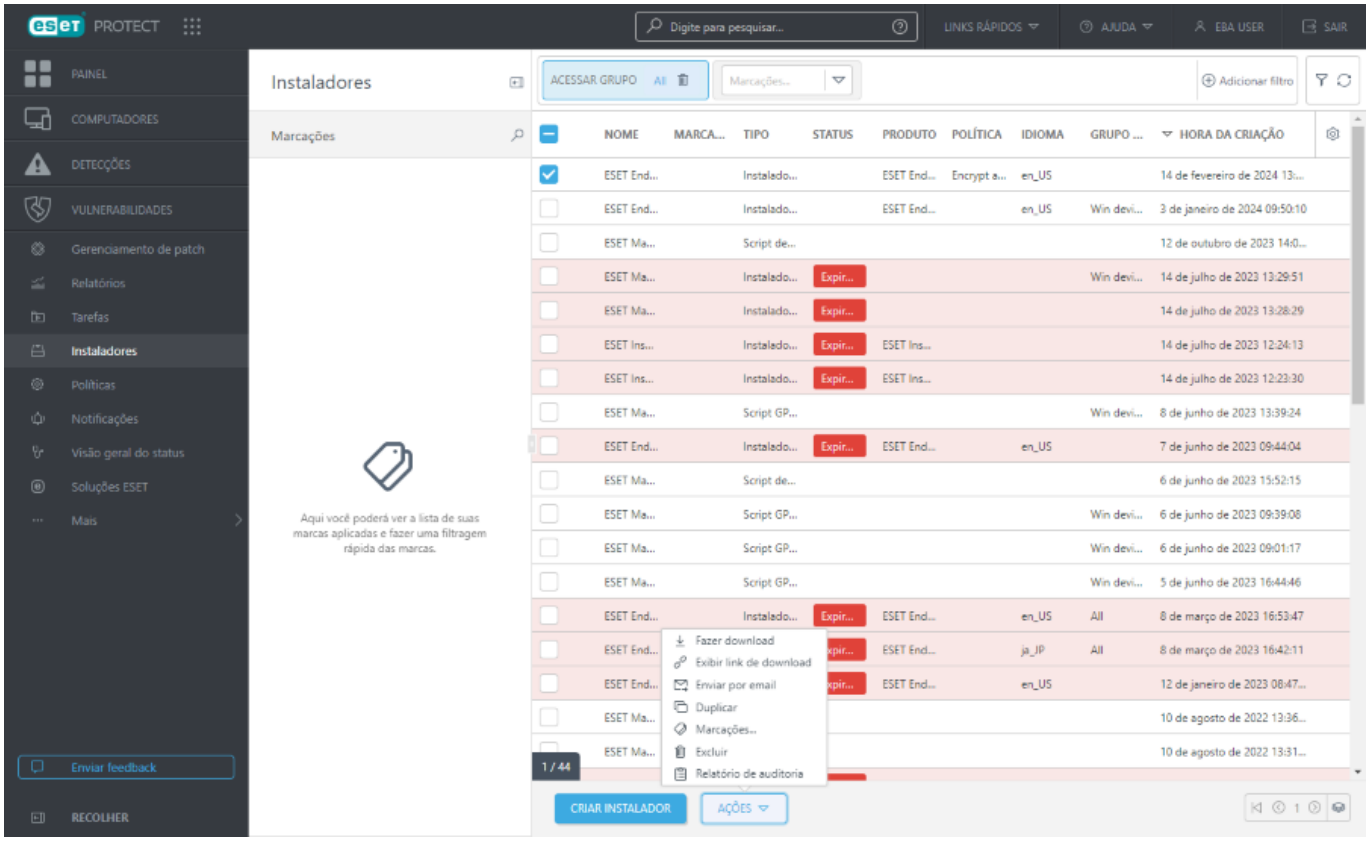
Para fazer download dos instaladores já criados, um usuário precisa de permissão de **Uso** para **Grupos e Computadores** e **Instaladores armazenados.**

- 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.

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 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 **Ações** > **Download**.

4.Você pode encontrar o pacote de instalação na pasta onde seu navegador da web salva os arquivos baixados.

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:

- Quando você remove uma política ou seleciona o sinalizador **Não aplicar***, a configuração volta automaticamente para os valores locais anteriores. 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. Esse comportamento se aplica a:

Produtos de Segurança ESET Windows	versão 7 e posterior
Produtos de Segurança ESET macOS	versão 7 e posterior
Produtos de Segurança ESET Linux	versão 8.1 e posterior

- Produtos de segurança ESET anteriores (do que os listados acima): 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.

Mesclagem de Políticas

Uma política aplicada a um cliente normalmente é resultado de várias políticas sendo mescladas em uma política final.

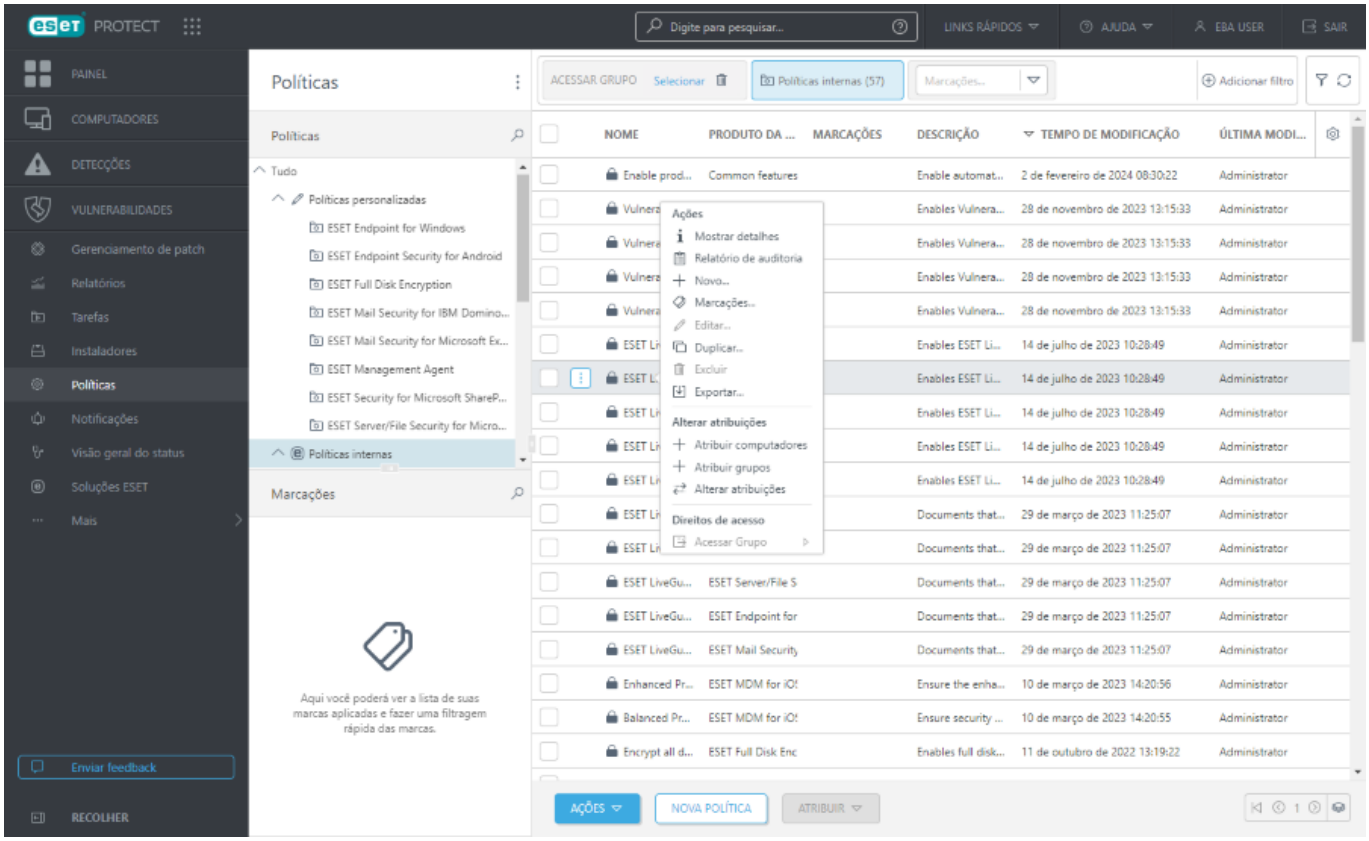
> Recomendamos atribuir políticas mais genéricas (por exemplo, o servidor de atualização) para grupos que estão mais alto na árvore de grupos. Políticas mais específicas (por exemplo, configurações de controle de dispositivos) devem ser atribuídas em locais mais baixos na árvore de grupo. A política 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 o sinalizador **Não aplicar** para excluir regras aplicadas aos itens na seção atual.

Veja também as regras de remoção de política.

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.Crie o novo usuário *John* e, na seção **Conjuntos de Permissões**, selecione *Política – Todas 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**.

ORDE...	PRODUTO DA ...	NOME DA POLÍ...	DESCRIÇÃO DE...
1 (aplicado prime...	Common features	Enable produ...	Enable automatic...
2	ESET Endpoint fo...	Protection se...	This policy enabl...

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.

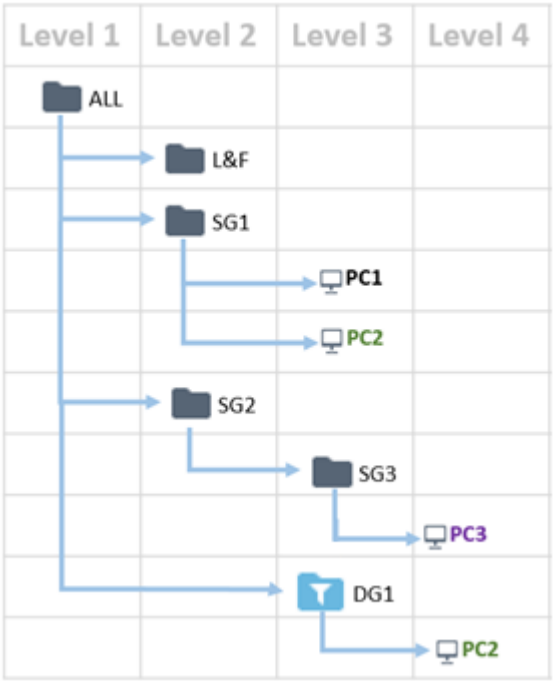
Regra 2: Em cada nível, os grupos estáticos desse nível são verificados em primeiro lugar na ordem em que aparecem na árvore (o que também é chamado pesquisa com a “largura primeiro”).

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: 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:

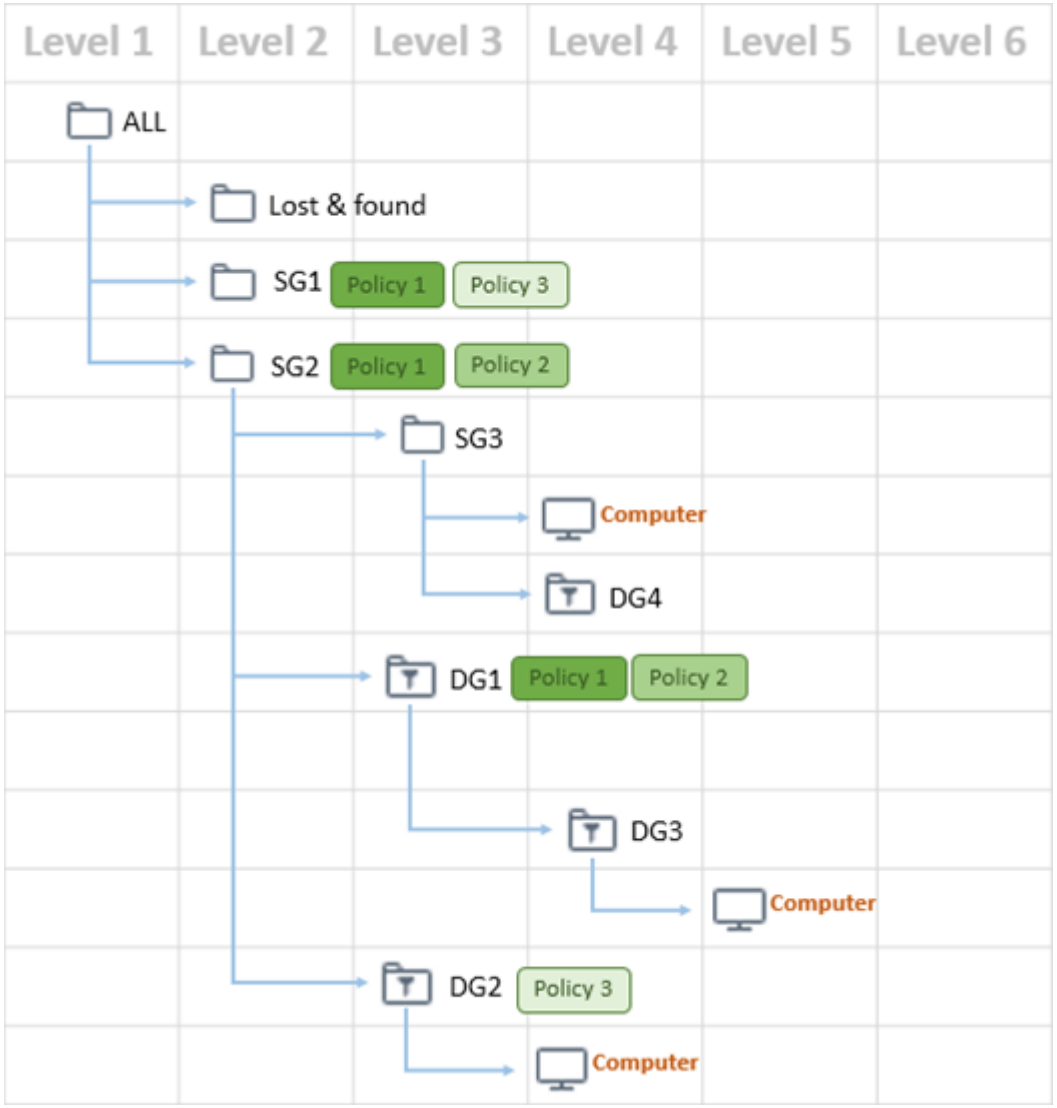
PC1:	PC2:	PC3:
1.ALL 2.SG1 3.PC1	1.ALL 2.SG1 3.DG1 4.PC2	1.ALL 2.SG2 3.SG3 4.PC3

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, ESET Endpoint Security, 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. 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.

- **Incluir no fim** – 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.

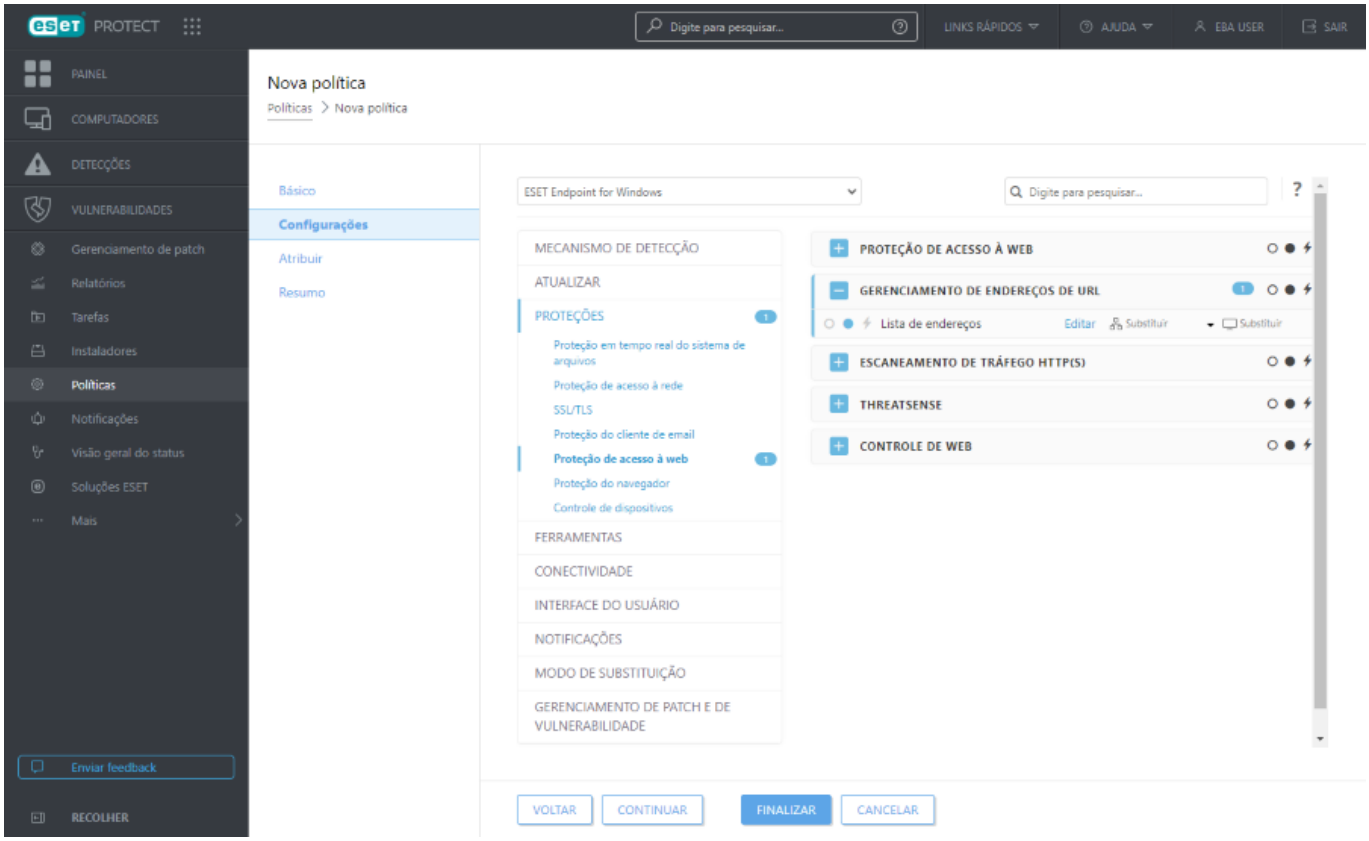
• **Incluir no começo** – Ao aplicar a mesma configuração em mais de uma política, você pode anexar no final as configurações com esta regra. A configuração será colocada no começo da lista que foi criada ao mesclar políticas.

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**.



Veja também as regras de remoção de política.

Exemplo de cenário da mesclagem de políticas

Este exemplo descreve:

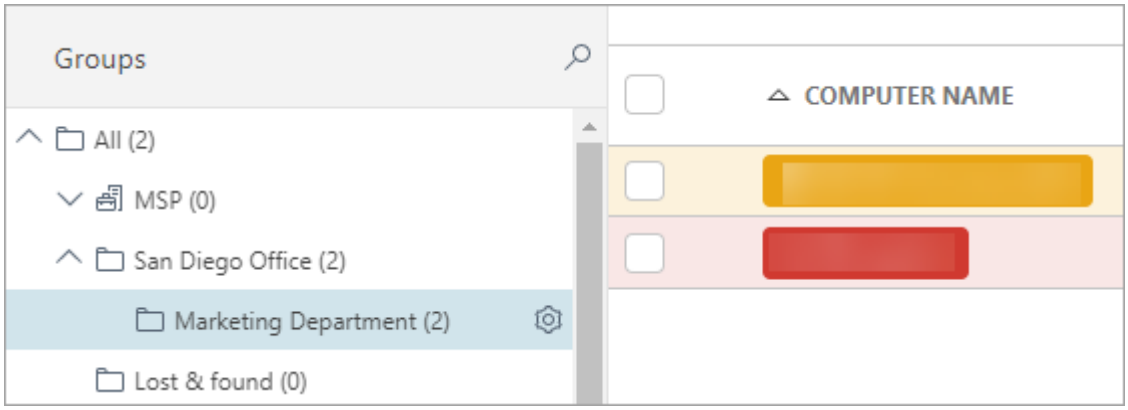
• Instruções sobre como aplicar configurações de política aos produtos de segurança ESET Endpoint

• 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)Navegue até **Proteções** > **Proteção de acesso à web** > **Gerenciamento de lista de URL**

   iv)Clique no botão **Aplicar** política e edite a **Lista de endereços** clicando em **Editar**

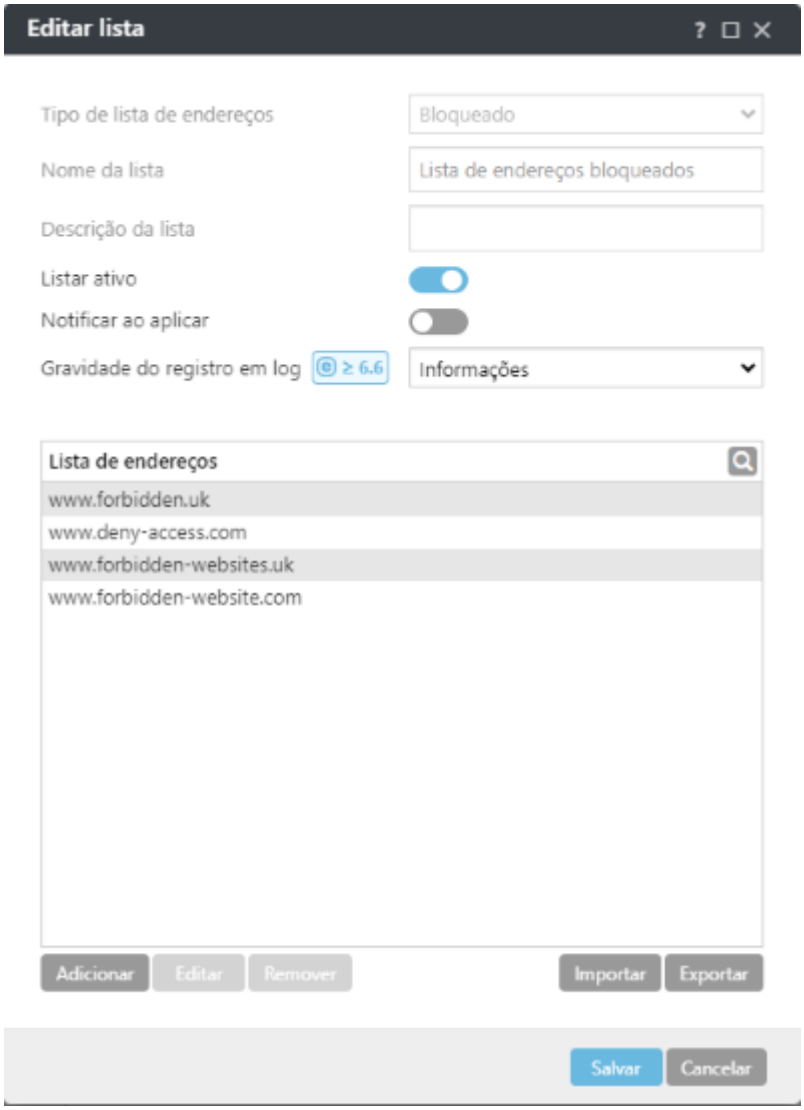
   v)Clique na **Lista de endereços bloqueados** e selecione **Editar**.

   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.

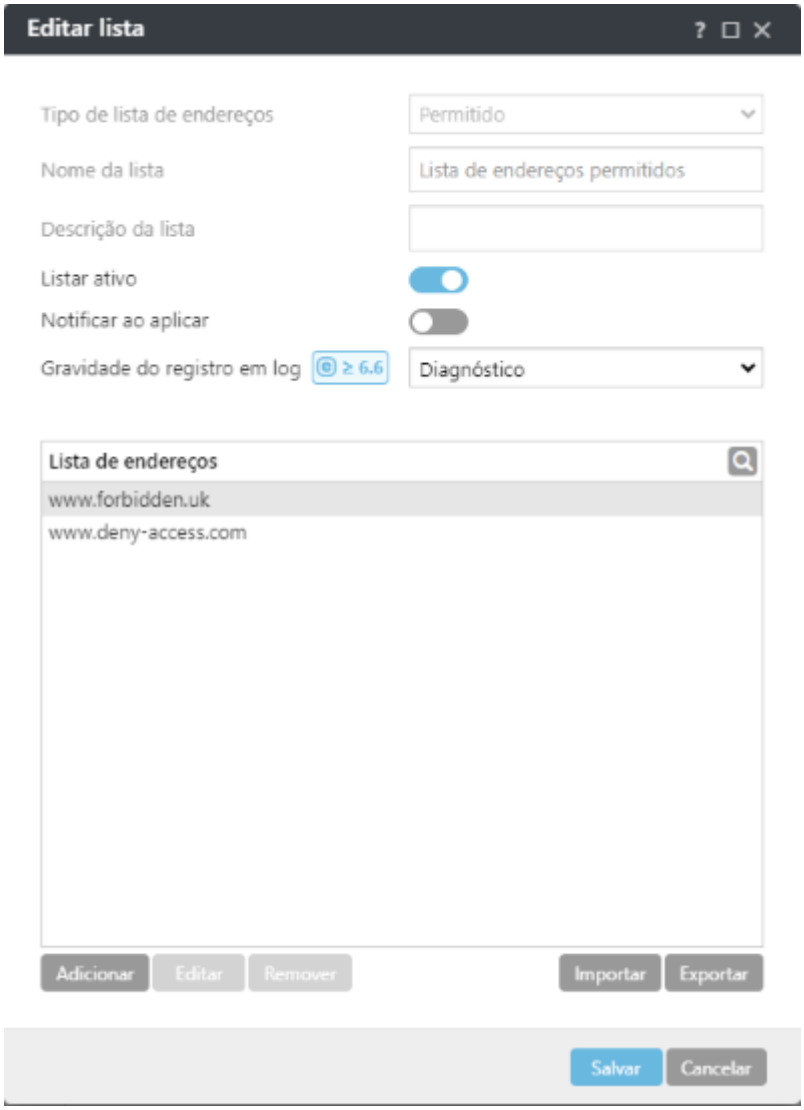


3. Navegue para **Políticas** e crie uma nova política:

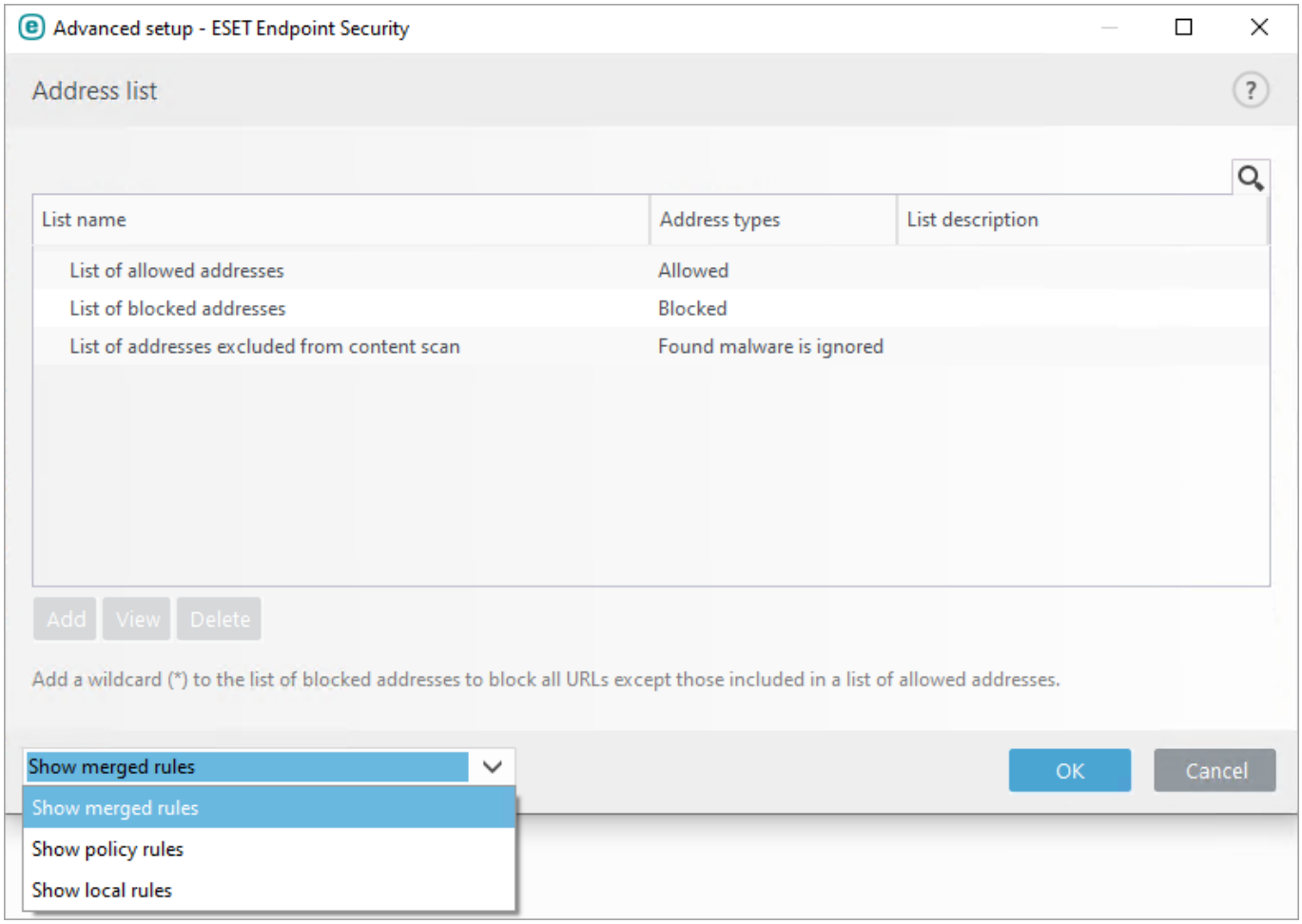
   i)Chamado *Departamento de Marketing*.
   ii)Expanda as **Configurações** e selecione **ESET Endpoint para Windows**
   iii)Navegue até **Proteções** > **Proteção de acesso à web** > **Gerenciamento de lista de URL**
   iv)Clique no botão **Aplicar** política, selecione Anexar regra e edite a **Lista 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 **ESET Endpoint Security** e navegue até **Configuração** > **Configuração avançada** > **Proteções** > **Proteção de acesso à web** > abra o **Gerenciamento de lista de URLs**. A configuração final do produto Endpoint será exibida.



A configuração final inclui:

- Lista de endereços da política do *Escritório de San Diego*
- 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:

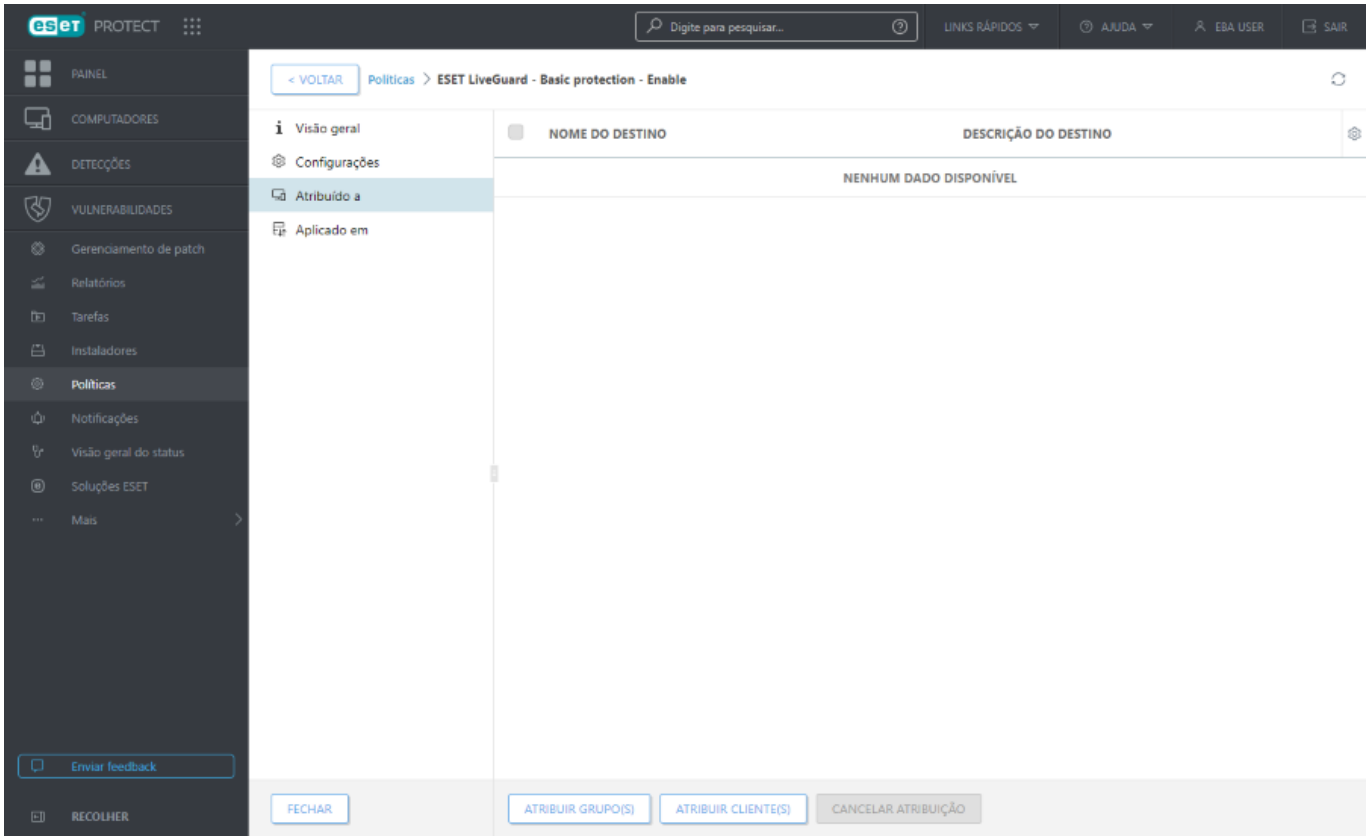
- ESET ManagementConfigurações de política do Agente
- Configurações de política do ESET Rogue Detection Sensor

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:

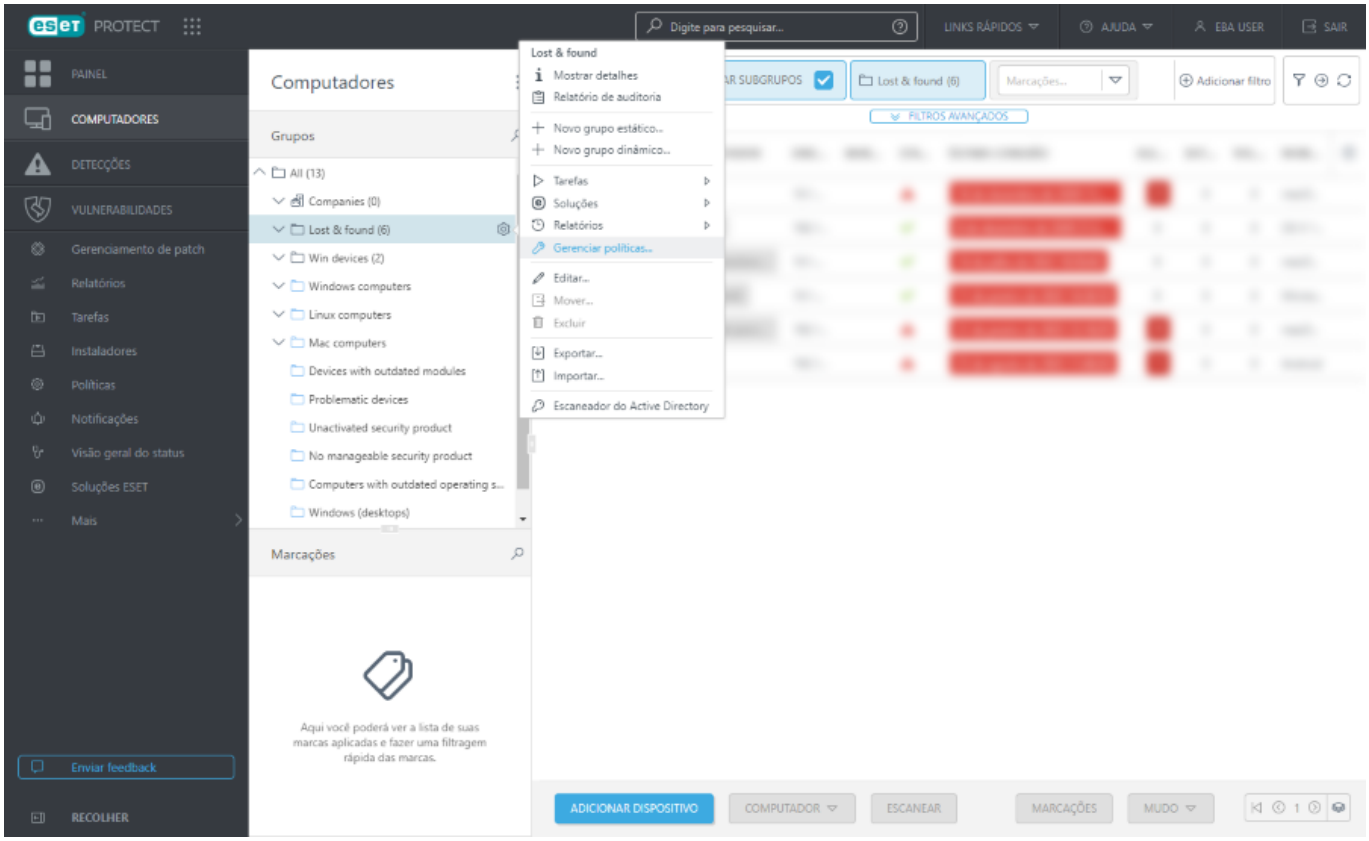
Método I.

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.

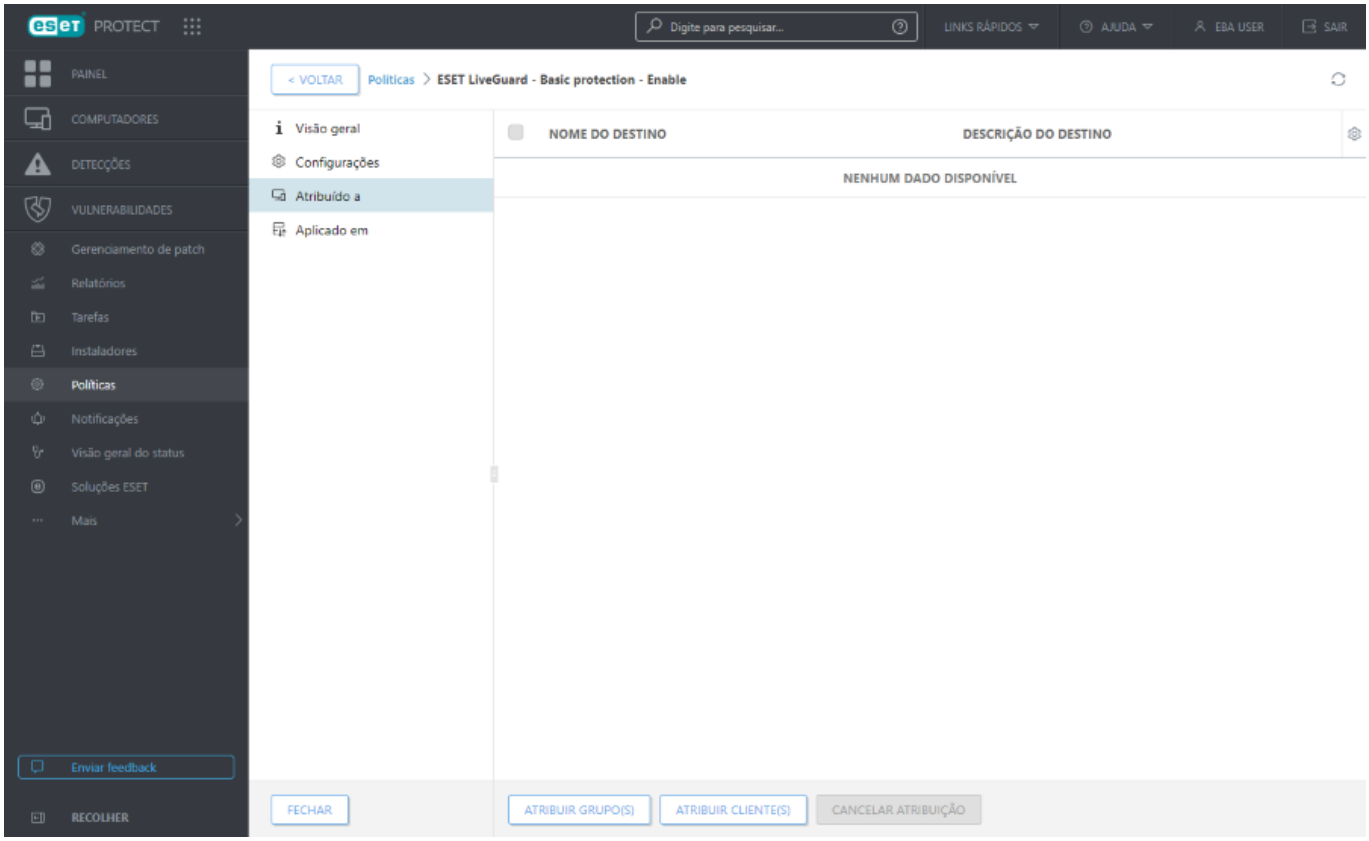
Para ver quais grupos estão atribuídos a uma política específica, selecione a política e clique em **Mostrar Detalhes** > **Aplicado em**.

Para obter mais informações sobre políticas, consulte o capítulo Políticas.

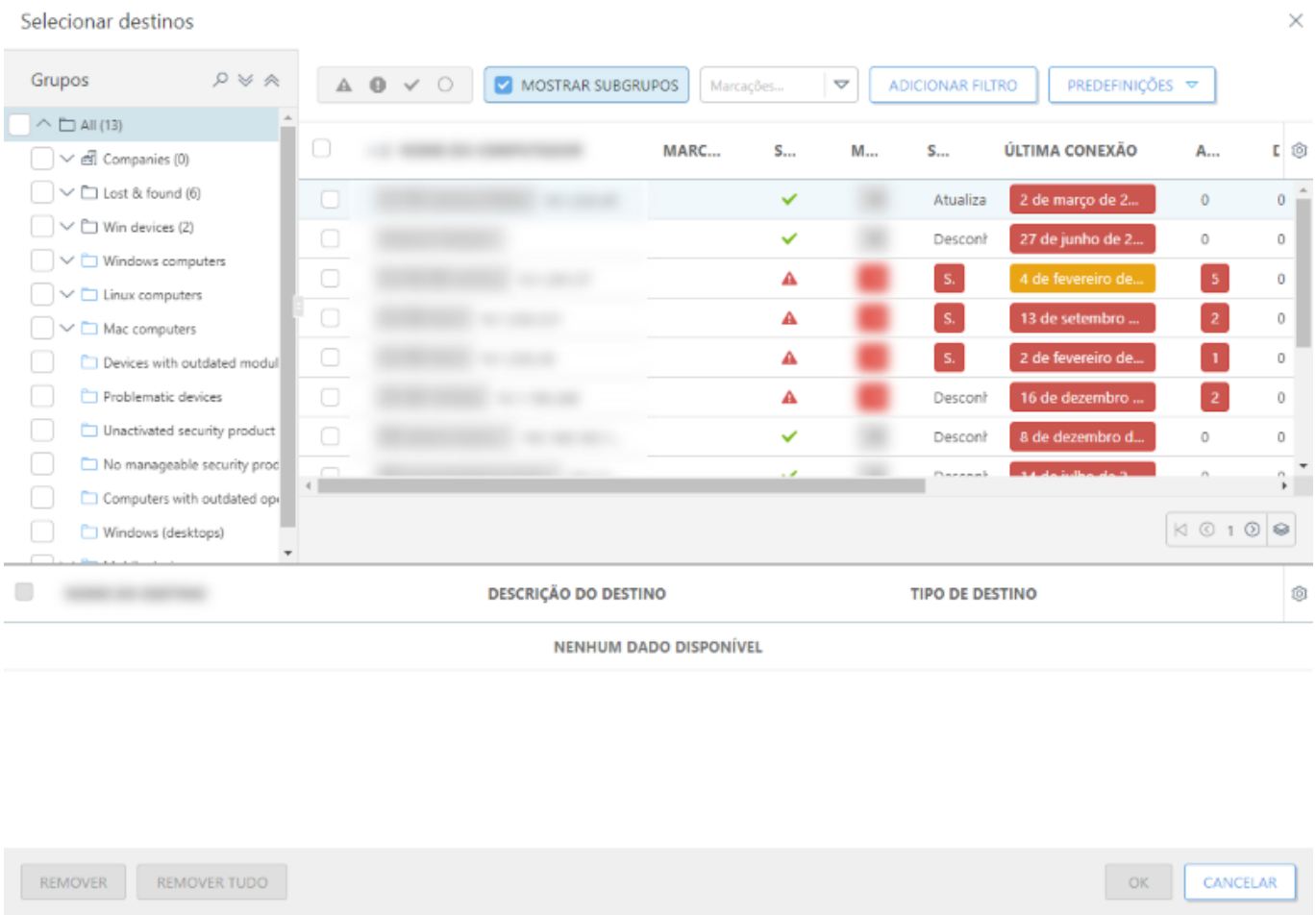
Atribuir uma política a um Cliente

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

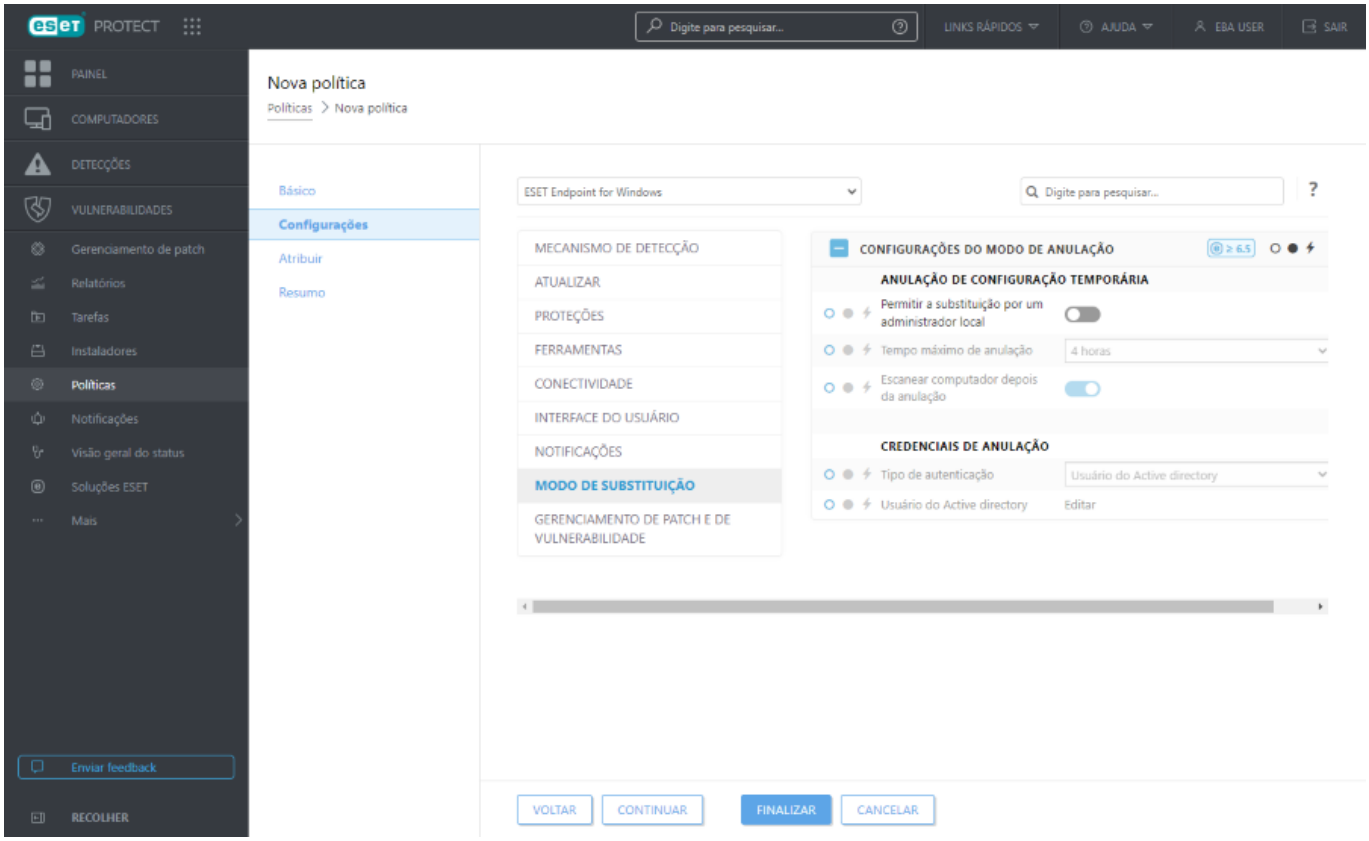
Usuários com produtos ESET endpoint do Windows instalados em sua máquina podem usar o recurso Substituição. Você pode ativar o modo de Substituição no Web Console ESET PROTECT apenas remotamente. O modo de substituição permite que os usuários no nível do computador cliente alterem as configurações no 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:
  - ESET Endpoint Security
  - ESET Server Security para Microsoft Windows Server (anteriormente ESET File Security para Microsoft Windows Server)
  - ESET Mail Security para IBM Domino
  - ESET Mail Security para Microsoft Exchange Server

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.

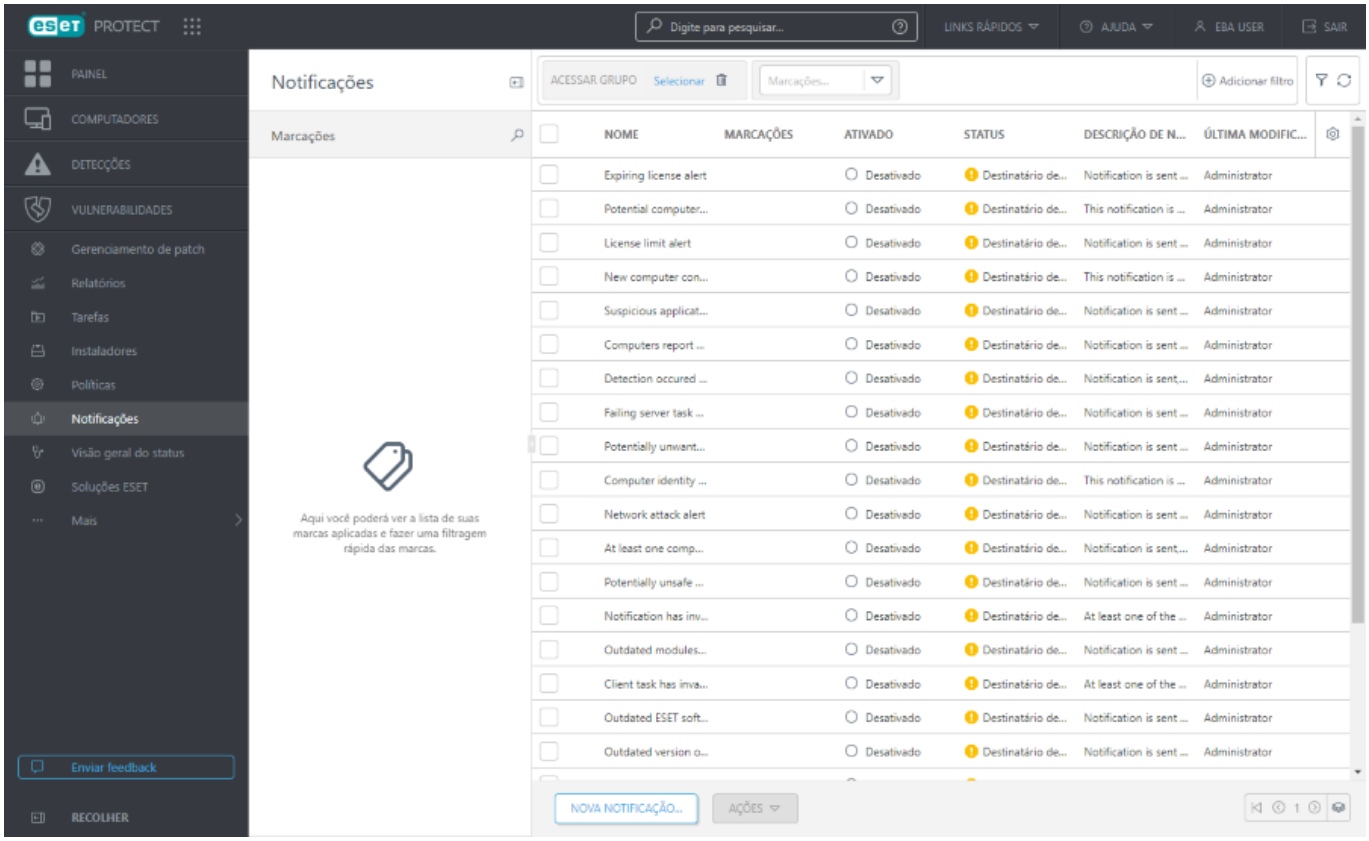
12. Na seção **Atribuir** você pode atribuir esta política ao *computador do John* (ou outros).

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 sua configuração de notificação), você será notificado através de um e-mail para o endereço de e-mail especificado e você pode responder de acordo. O servidor SMTP necessário para enviar as notificações é configurado automaticamente, portanto nenhuma modificação adicional é necessária. 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 e vão acionar um email para notificar o usuário.

Criar 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 - o usuário deve ter permissões de **Gravação** para notificações em um grupo onde a notificação está localizada.

Remover 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.

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.

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**
- **ESET Inspect incidentes**

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.

O conteúdo padrão da mensagem tem uma finalidade informativa, não é possível personalizá-lo. Você pode personalizar a mensagem entregue por meio de uma notificação na seção Distribuição.

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
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.
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.

O conteúdo padrão da mensagem tem uma finalidade informativa, não é possível personalizá-lo. Você pode personalizar a mensagem entregue por meio de uma notificação na seção Distribuição.

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.

> Você pode selecionar ambos os meios de distribuição – **Enviar e-mail** e **Enviar webhook** e, em seguida:
> 1.Preencha as **Configurações de distribuição de e-mail**.
> 2.Preencha as **Configurações de distribuição de webhook**.

Enviar email

Se **Enviar e-mail** estiver selecionado, insira pelo menos um destinatário de e-mail.Por padrão, o e-mail de notificação está em formato HTML com um logotipo ESET PROTECT no cabeçalho.

Configurações de distribuição de e-mail

- **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.

Incluir um link no e-mail – selecione a caixa de seleção para incluir um link para o Web Console com detalhes sobre o evento da notificação.

Enviar e-mail de teste – Clique no botão **Enviar** para enviar um e-mail de teste para o endereço acima.

Enviar webhook

Você pode usar o ESET PROTECT para enviar notificações como webhooks. Você pode receber notificações do ESET PROTECT como mensagens no seu canal de comunicação principal.

- **URL do Webhook** – digite o URL do webhook do canal de comunicação

> ✓ Veja um exemplo do URL do webhook de equipe abaixo:
> *https://xxxxx.webhook.office.com*
> Depois de digitar o URL do webhook Teams, a **carga JSON** não é exibida.

  - **Incluir um link no conteúdo do webhook** – selecione a caixa de seleção para incluir um link para o Web Console com detalhes sobre o evento da notificação. Esse recurso é válido para webhooks Teams
  - Ao digitar seu URL de webhook personalizado (que não seja do Teams ou Slack), você pode definir a Autenticação

- **Carga JSON** – digite o JSON válido. Você pode usar variáveis. Clique em **Adicionar variável** e selecione a variável: **Assunto**, **Conteúdo**, **Link**
  - Ao preencher o **Assunto** e o **Conteúdo** na **Visualização da mensagem**, os valores das variáveis serão usados automaticamente na **carga JSON**
  - Para criar uma carga JSON personalizada para um canal de comunicação de terceiros, consulte a ajuda oficial de tal canal, por exemplo, Discord

- **Autenticação** – exibida quando você digita um link de webhook personalizado. Proteja seus dados e melhore

a segurança com a autenticação de webhook. Selecionar:

- **Sem autenticação** – selecione esta opção quando o receptor do webhook não tiver nenhum esquema de autenticação. Recomendamos adicionar autenticação para proteger os dados e aumentar a segurança.
- **Token do portador** – digite token ao portador no campo **Token do portador**.
- **Autenticação básica** – digite o **Nome de usuário** e **Senha** nos campos.

- **Enviar webhook de teste** – Clique no botão **Enviar** para enviar um webhook de teste para o link de webhook fornecido.

Campos básicos na distribuição

- **Visualização da mensagem** – uma visualização da mensagem que aparece na notificação, contendo configurações definidas em formato 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. Isso é opcional, mas recomendado para uma filtragem melhor.
  - **Assunto** – o assunto de uma mensagem de notificação. Clique no ícone editar para editar o conteúdo, um assunto preciso pode melhorar a classificação e a filtragem de mensagens
  - **Conteúdo** – clique no ícone de editar para editar o conteúdo, depois disso, você pode clicar no ícone de redefinição 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**
  - **Localidade** – idioma da mensagem padrão. O conteúdo da mensagem não é traduzido
  - **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 uma nova notificação com base no modelo que você está editando.

Visão geral do status

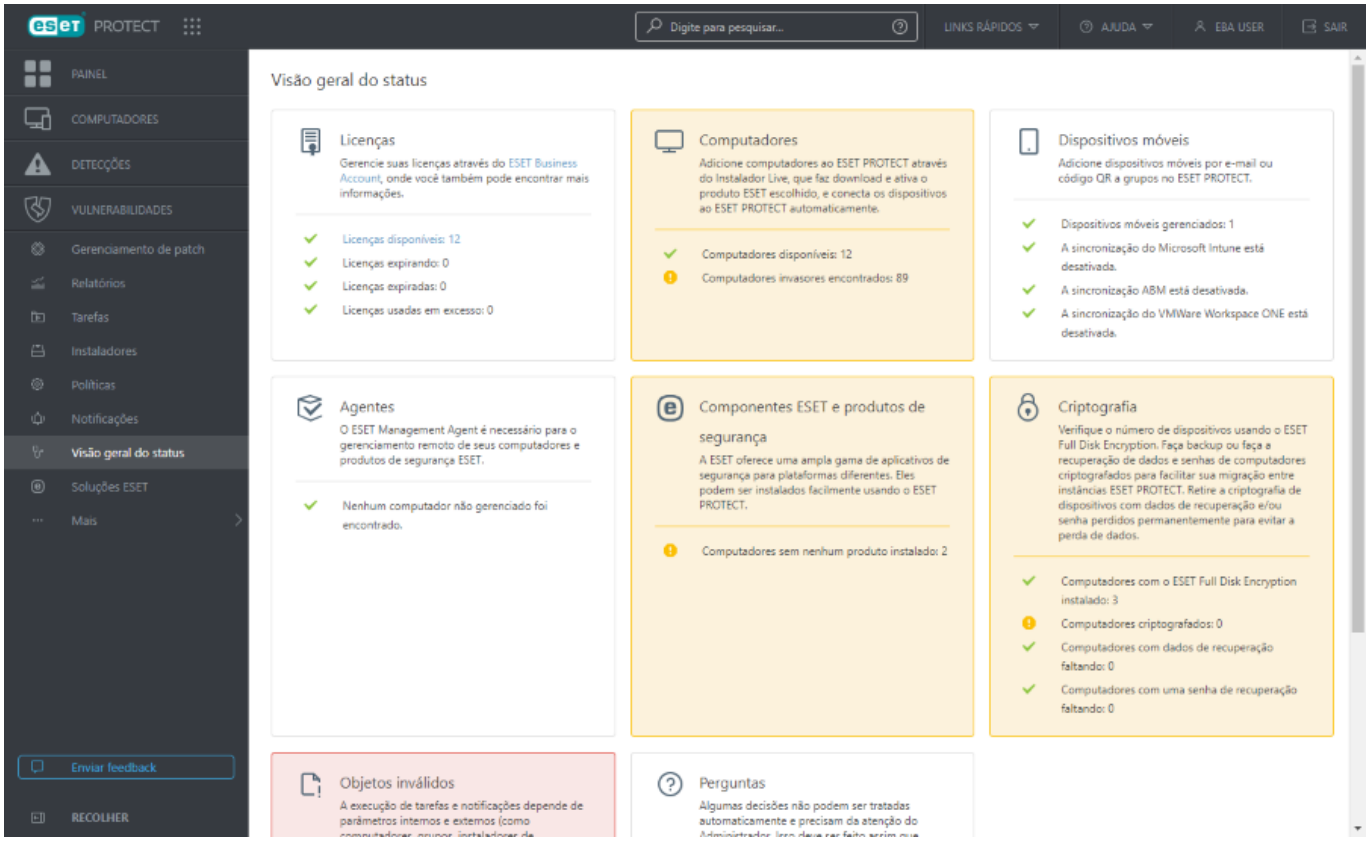
O Servidor ESET PROTECT realiza verificações de diagnóstico periódicas. Use a **Visão geral do status** para ver as estatísticas de uso e o status geral do seu ESET PROTECT. Também pode ajudá-lo com a configuração inicial do ESET PROTECT. Clique em **Visão geral do status** para ver as informações detalhadas 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 Web 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:

Licenças	ESET PROTECT usa o sistema de licenciamento ESET. Para o gerenciamento de licenças, vá para sua ESET Business Account.
Computadores	• **Adicionar computador** – adiciona computadores na sua rede à estrutura ESET PROTECT.
Dispositivos móveis	**Adicionar dispositivos móveis** – Inscrever dispositivos móveis. • **Microsoft Entra ID Configurações de inscrição** – configure a inscrição Microsoft Entra ID. • **Microsoft Intune sincronização** – configurar a sincronização do Microsoft Intune. • **Sincronização ABM** – configure a sincronização do Apple Business Manager (ABM). • **sincronizaçãoVMware Workspace ONE** – configure a sincronização do VMware Workspace ONE.
Agentes	• **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. • **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). • **Configurar Proteção** – revise e ajuste as configurações de segurança aplicadas a todos os dispositivos conectados ao ESET PROTECT.
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.
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	Status MSP estão disponíveis em instâncias com uma conta MSP.



Soluções ESET

Esta seção permite a implantação simplificada dos produtos a seguir:

- **ESET LiveGuard Advanced**
- **ESET Full Disk Encryption**

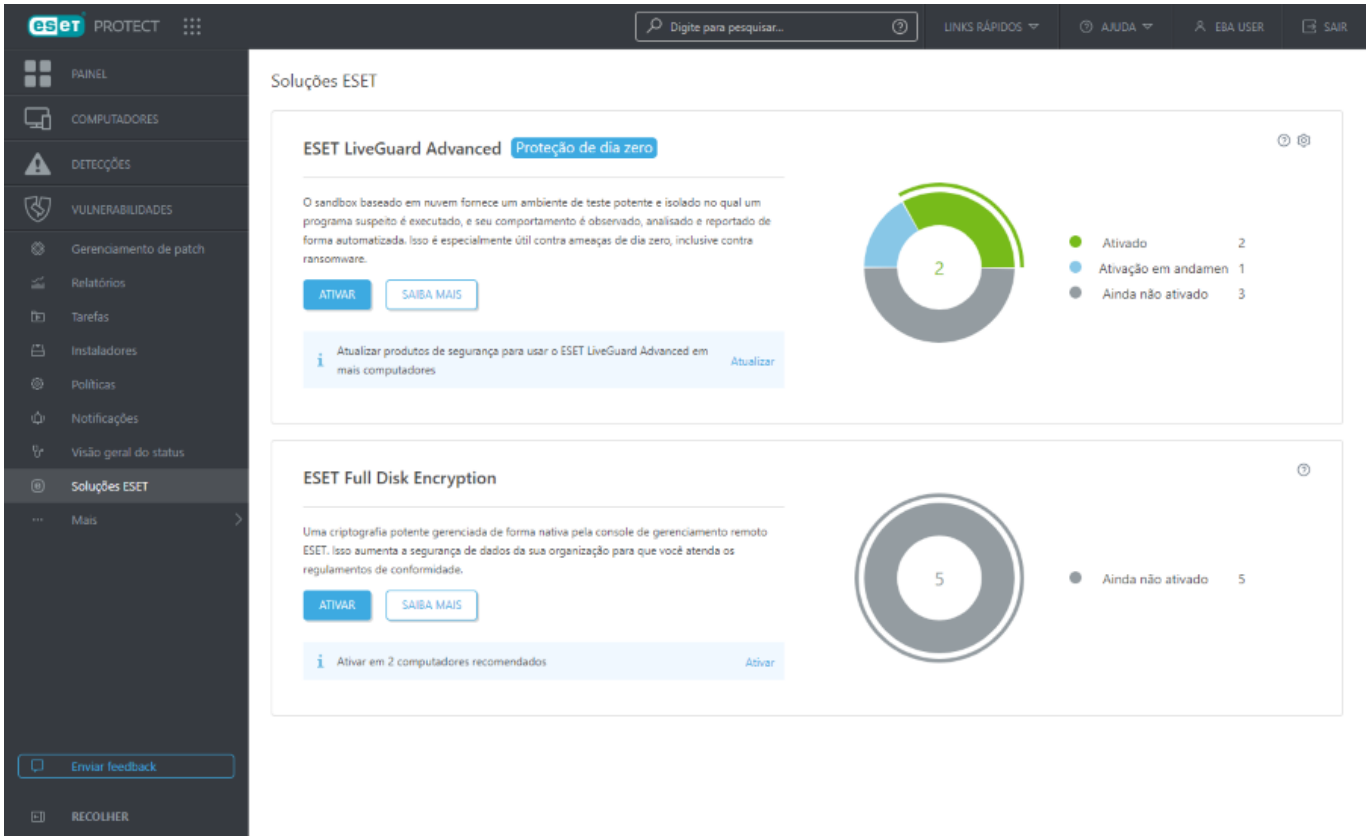
Para cada um dos produtos você pode selecionar uma das opções a seguir:

- **Experimentar** – solicite uma licença de avaliação para um produto selecionado se você tiver usuários não licenciados.
- **Comprar** – compra uma licença para o produto selecionado.
- **Ativar** – ativa o produto selecionado para todos os dispositivos qualificados. Para mais detalhes, consulte as subseções para cada produto.
- Clique no **ícone de engrenagem** > **Remover** para remover o ESET LiveGuard Advanced ou o ESET Full Disk Encryption de todos os dispositivos.
- **Saiba mais** – abre uma pequena página informativa sobre o produto selecionado.

Você também pode acessar o **detalhamento** do gráfico para cada categoria representada e exibir os 100 primeiros dispositivos.

Limitações de implantação

- A conta de usuário precisa de Permissão de **gravação** para ativar esta funcionalidade.
- Existe uma opção única para experimentar essa funcionalidade por uma Empresa MSP.



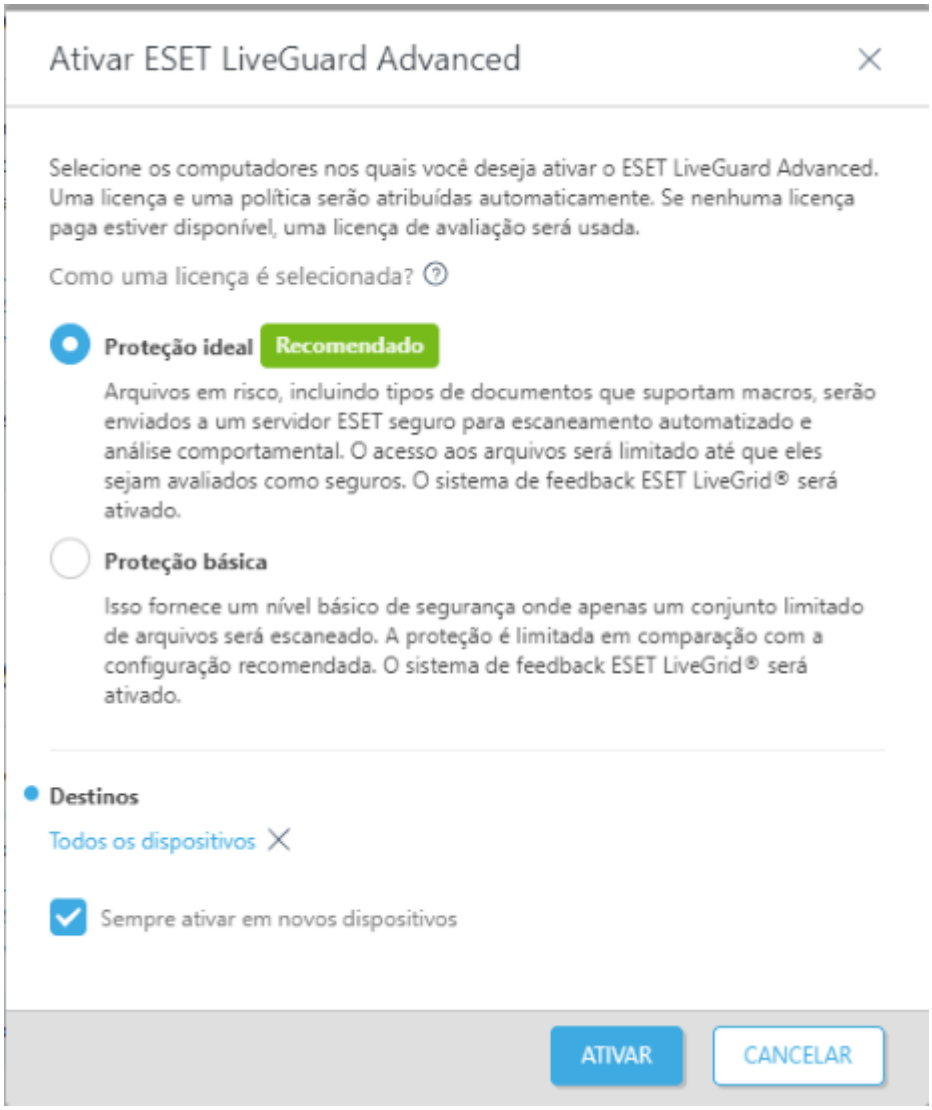
Ativar o ESET LiveGuard Advanced

Selecione a seção **Soluções ESET**; em **ESET LiveGuard Advanced** clique em **Comprar** para ser redirecionado para o procedimento de atualização do seu nível de licença ESET PROTECT. Depois de concluir o procedimento de atualização, você pode implementar e ativar a funcionalidade do ESET LiveGuard Advanced em sua rede gerenciada.

Licença de avaliação

Se você já tem uma licença de avaliação ativa e comprar uma licença completa do produto, uma nova opção vai aparecer para migrar os dispositivos para a licença completa.

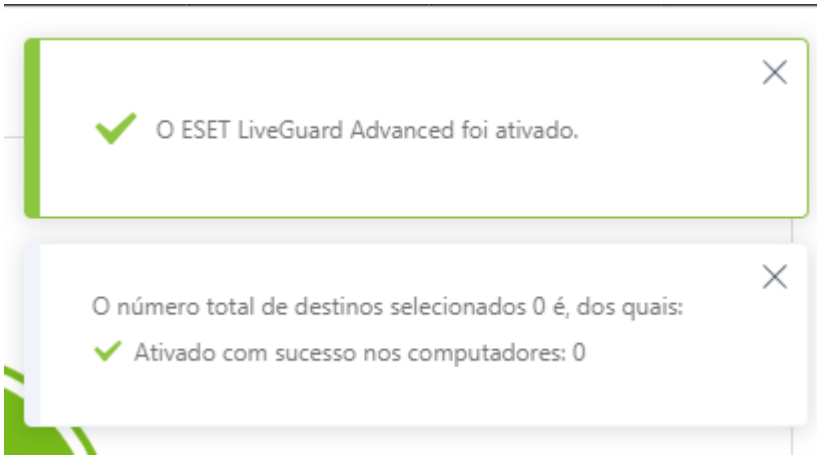
Se você selecionar **Implantar**, uma nova janela aparecerá. Aqui, você pode selecionar **Proteção ideal** (recomendada) ou **Proteção básica**. Selecione os **Destinos** da implantação. Você pode ser deixar para a seleção padrão de **Todos os dispositivos**, ou pode selecionar manualmente os dispositivos de destino e os grupos estáticos ou dinâmicos. Quando você mantém a seleção padrão **Todos os dispositivos**, você pode marcar a caixa de seleção **Sempre ativar em novos dispositivos** para ativar a implantação automática do ESET LiveGuard Advanced em todos os novos dispositivos que serão gerenciados pelo ESET PROTECT no futuro. Em seguida, confirme sua decisão selecionando **Ativar**.



Proteção básica A implantação é executado com uma política interna **ESET LiveGuard – ativar**.
Proteção ideal A implantação é executada com uma política interna **ESET LiveGuard – proteção ideal – ativar**.

ESET PROTECT executará a Tarefa de ativação para o ESET LiveGuard Advanced em todos os dispositivos gerenciados selecionados.

Uma pequena notificação será exibida no lado direito, mostrando os detalhes de implantação.

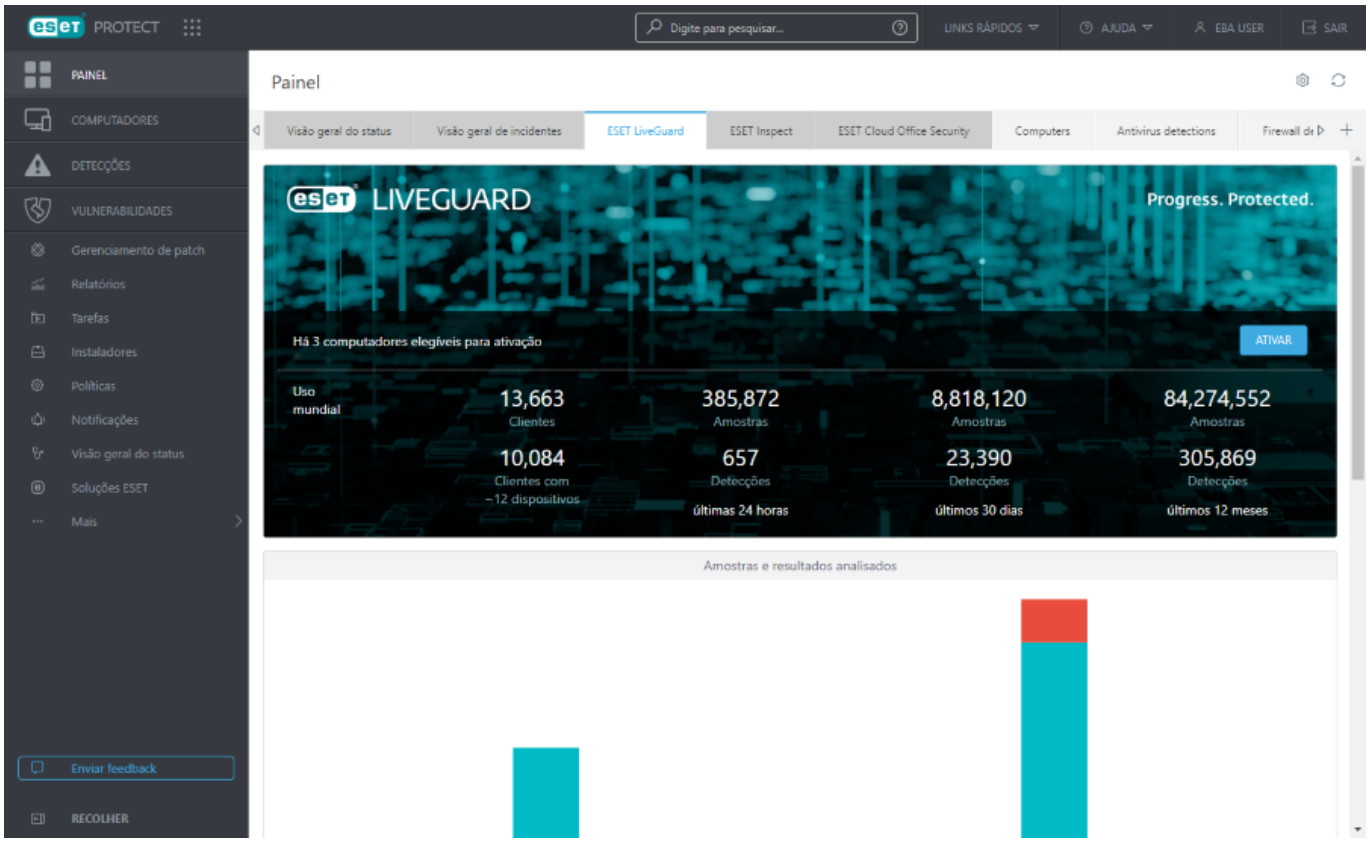


Você pode revisar o progresso em **Soluções ESET**.

Depois de ativar o ESET LiveGuard Advanced:

- O painel ESET LiveGuard exibirá os relatórios aprimorados do ESET LiveGuard Advanced da sua rede gerenciada.

- Cada dispositivo com o ESET LiveGuard Advanced terá o Sistema de Reputação ESET LiveGrid® e Sistema de Feedback ESET LiveGrid® habilitados. Verifique as políticas do seu dispositivo.



Remover o ESET LiveGuard Advanced

Clique no ícone de engrenagem na parte superior direita do bloco **ESET LiveGuard Advanced** e selecione **Remover ESET LiveGuard Advanced** para remover o ESET LiveGuard Advanced dos dispositivos gerenciados. ESET PROTECT vai desativar o ESET LiveGuard Advanced, retirar a criptografia de todos os discos criptografados e remover a criptografia de todos os discos criptografados e remover a opção de política correspondente de todos os dispositivos selecionados.

Desativar implantação automática

Clique no ícone de engrenagem na parte superior direita do bloco **ESET LiveGuard Advanced** e selecione **Desativar a implantação automática** para desativar a implantação automática em novos dispositivos.

Ativar o ESET Full Disk Encryption

Selecione a seção **Soluções ESET**; em **ESET Full Disk Encryption** clique em **Comprar** para ser redirecionado para o procedimento de atualização do seu nível de licença ESET PROTECT. Depois de concluir o procedimento de atualização, você será capaz de implementar e ativar a produto ESET Full Disk Encryption em sua rede gerenciada.

Selecione a opção **Ativar** e uma nova janela aparecerá:

1.**Destinos** – mantenha o padrão (**todos os dispositivos**) ou selecione os destinos (dispositivos, grupos estáticos ou dinâmicos).

2.**Idioma** – selecione um idioma do ESET Full Disk Encryption que será implantado em todos os dispositivos selecionados.

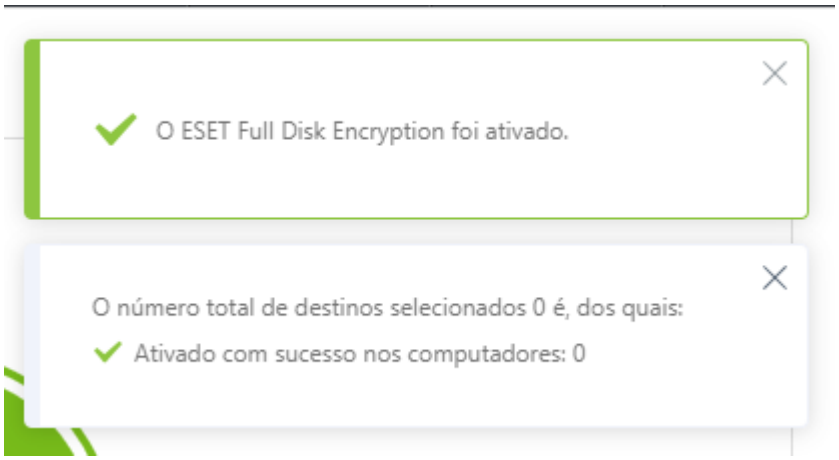
3.Selecione a caixa de seleção **Eu aceito o Acordo de licença de usuário final e reconheço a Política de Privacidade**. Consulte o Acordo de Licença para o Usuário Final (EULA), Termos de Uso e Política de Privacidade dos produtos ESET.

4.Clique em **Ativar**. O ESET PROTECT executará a Tarefa de ativação e a Tarefa de instalação de software para o ESET Full Disk Encryption em todos os dispositivos gerenciados selecionados.

A implantação é executado com uma política incorporada **Criptografar todos os discos – TPM usado se disponível – OPAL não usado**.

Uma pequena notificação será exibida no lado direito, mostrando os detalhes de implantação.

O usuário do dispositivo gerenciado deve realizar mais etapas para a implantação bem-sucedida do ESET Full Disk Encryption. Siga as etapas descritas na documentação ESET Full Disk Encryption.



Você pode revisar o progresso em **Soluções ESET**.

Remover o ESET Full Disk Encryption

Clique no **ícone de engrenagem** na parte superior direita do bloco **ESET Full Disk Encryption** e selecione **Remover ESET Full Disk Encryption** para remover o ESET Full Disk Encryption dos dispositivos gerenciados. ESET PROTECT vai desativar o ESET Full Disk Encryption, remover a criptografia de todos os discos criptografados e remover a opção de política correspondente de todos os dispositivos selecionados.

A remoção é executado com a política interna **Remover a criptografia de todos os discos**.

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 oArquivos enviados oExclusões oQuarentena
Computadores oUsuários do computador oModelos de grupo dinâmico
Licenças oGerenciamento de licenças
Direitos de acesso oUsuários oDefinições de permissão
Auditoria de atividade oRelatório de auditoria
Admin oConfigurações

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.

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.

Relatório de exportação	Faça o download do 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 ou em **Exportar relatório** para baixar o relatório. 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:

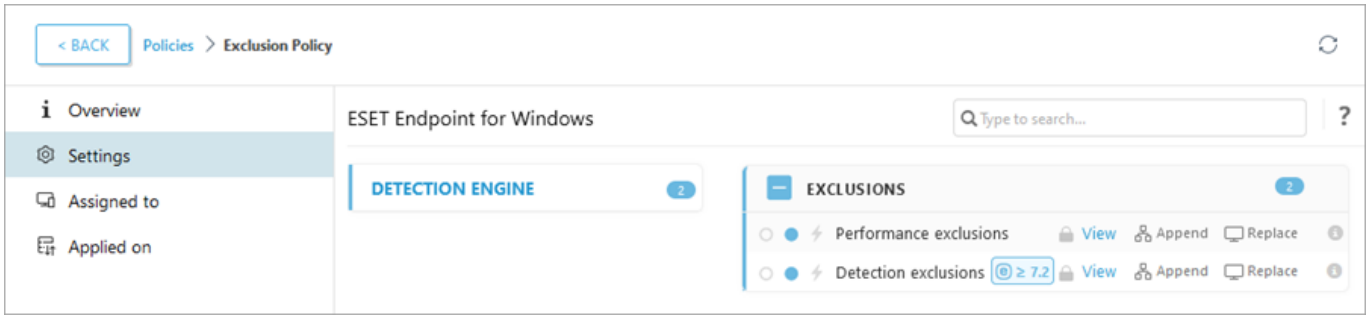
- **Alterar atribuição** – Altera os computadores de destino nos quais a exclusão será aplicada.
- **Mostrar computadores afetados** – Veja os computadores aos quais a exclusão é aplicada.
- **Relatório de auditoria** – mostrar o Relatório de auditoria para a exclusão selecionada.
- **Remover** – Remove 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.

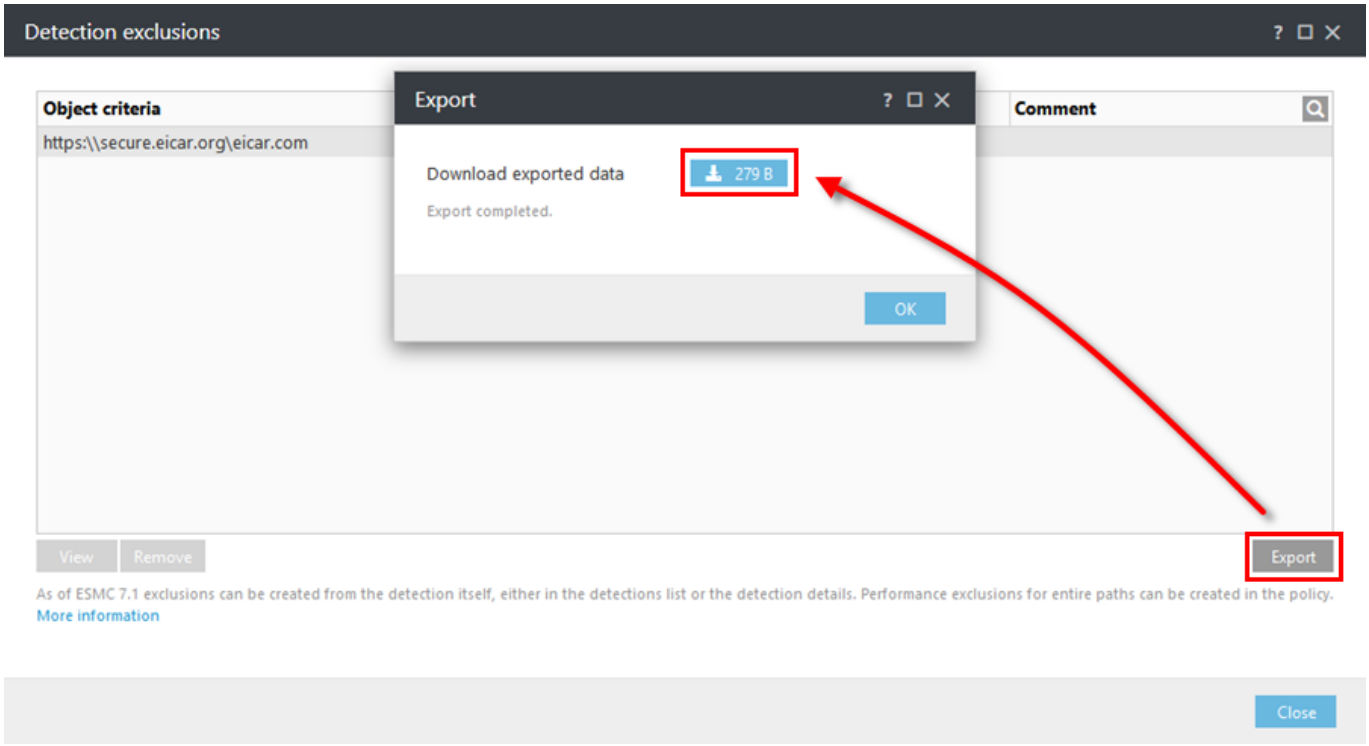
Migrar exclusões de uma política

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**.

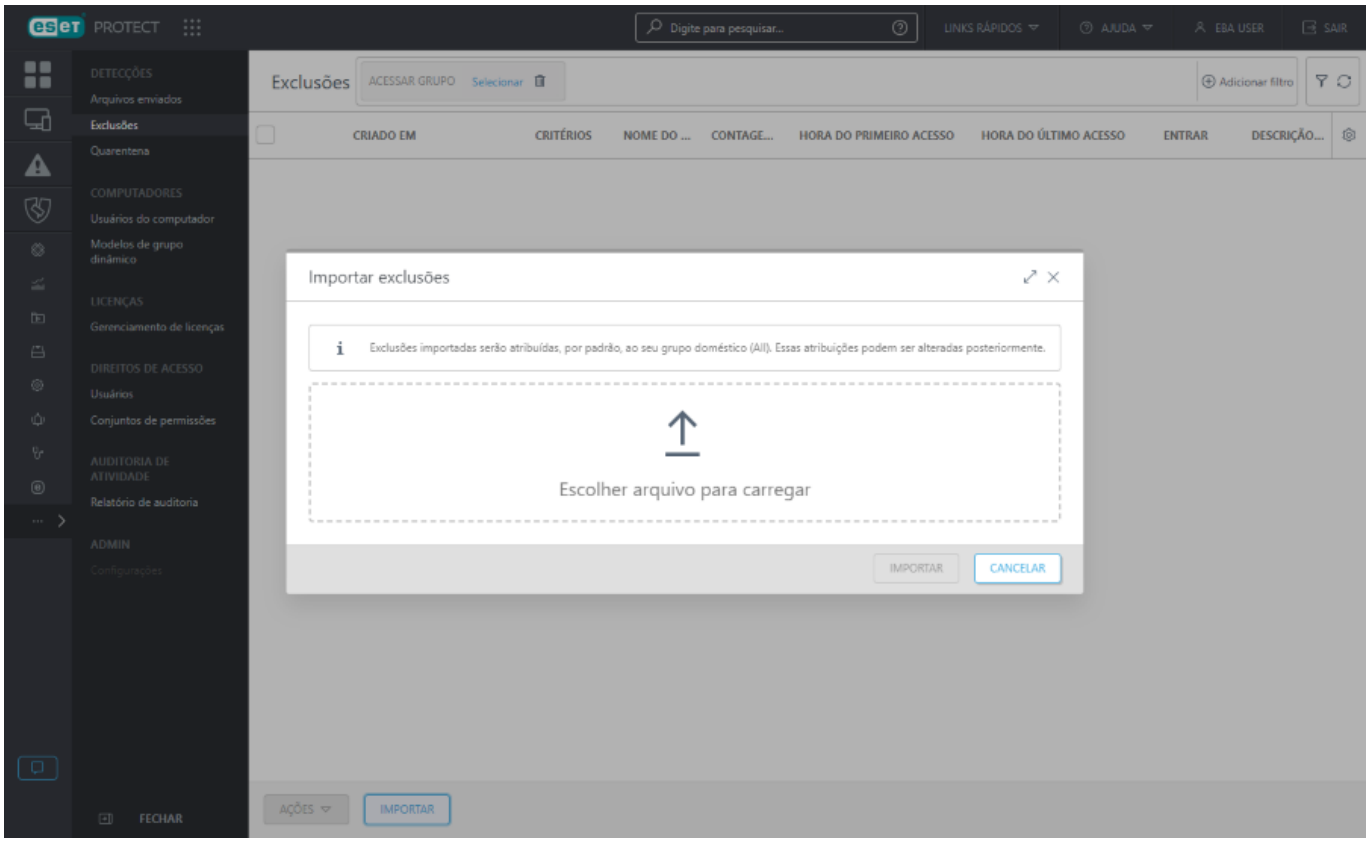


4. Clique no botão **Exportar** e, em seguida, clique no botão ao lado de **Fazer download dos dados exportados** e salve o arquivo *export.txt*. Clique em **OK**.



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

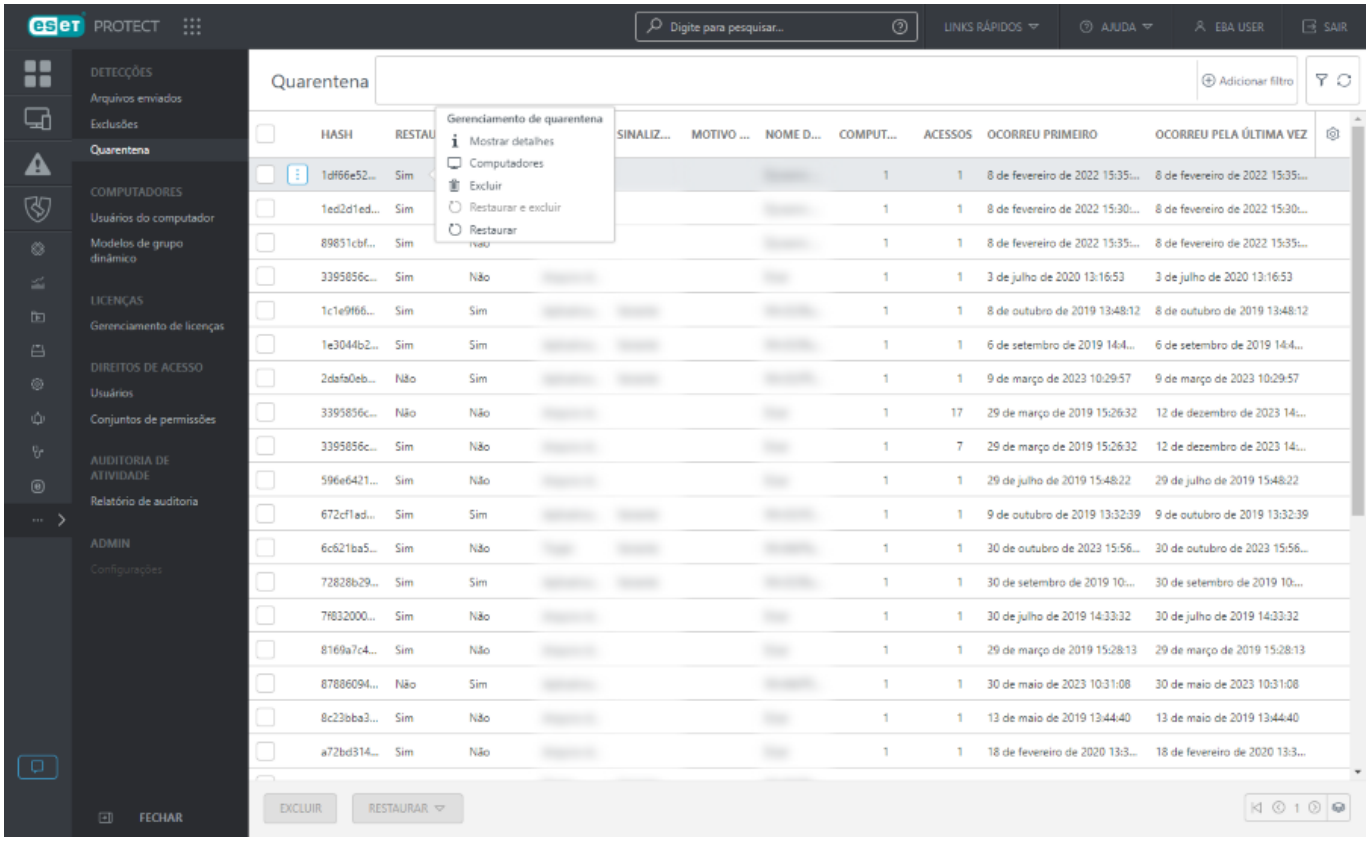
Você pode personalizar a exibição da tela atual do console web:

- 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 que você sincronize os Usuários com o Active Directory primeiro. 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 Web Console ESET PROTECT**. A seção Usuários do computador permite a você parear um usuário com um dispositivo para sincronizar algumas configurações específicas do usuário. Para gerenciar os usuários do console Web ESET PROTECT e conjuntos de permissões navegue até ESET Business Account.

- Os usuários destacados não têm 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 de gerenciamento de dispositivo móvel do iOS.

Filtros e personalização de layout

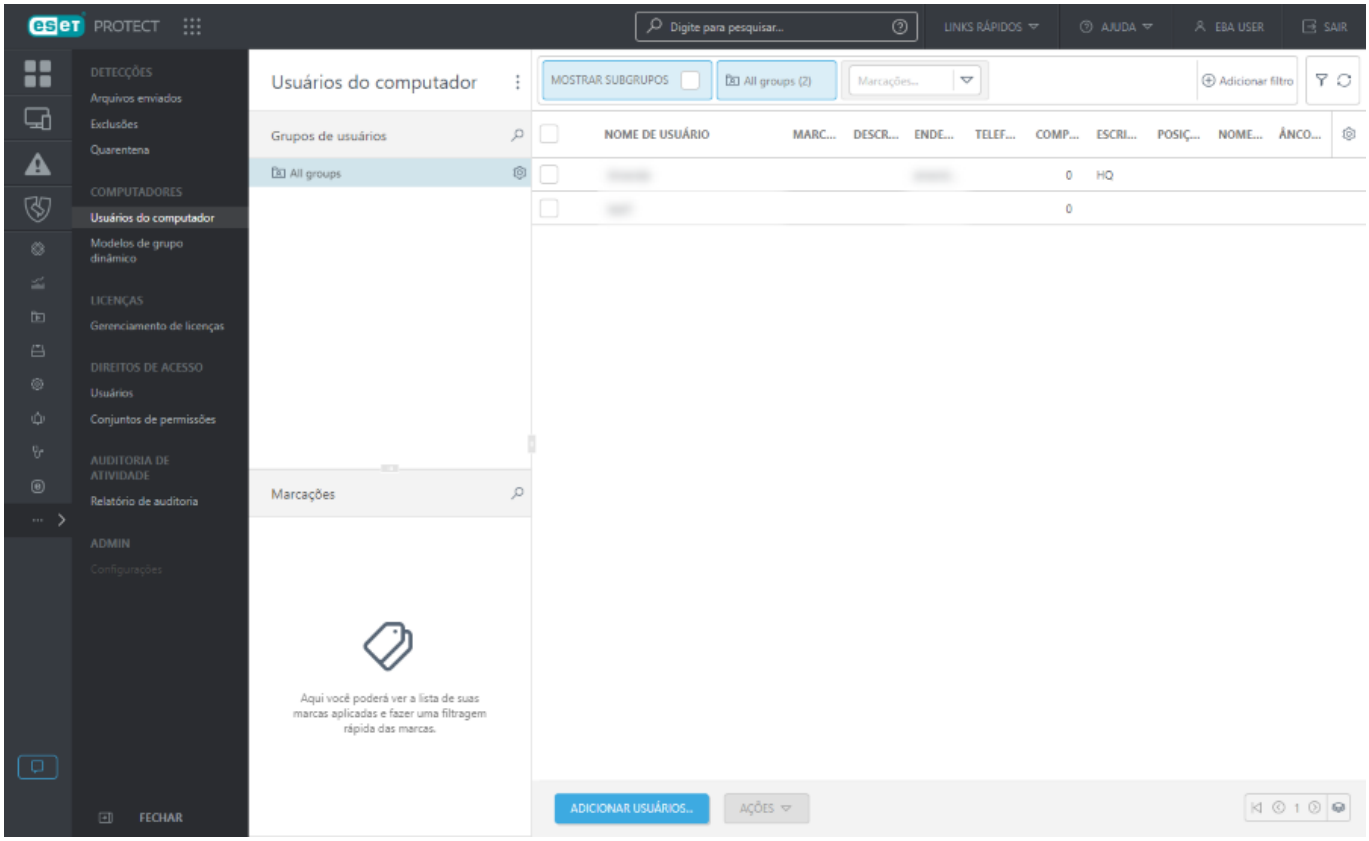
Você pode personalizar a exibição da tela atual do console web:

- 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 usuários.



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.

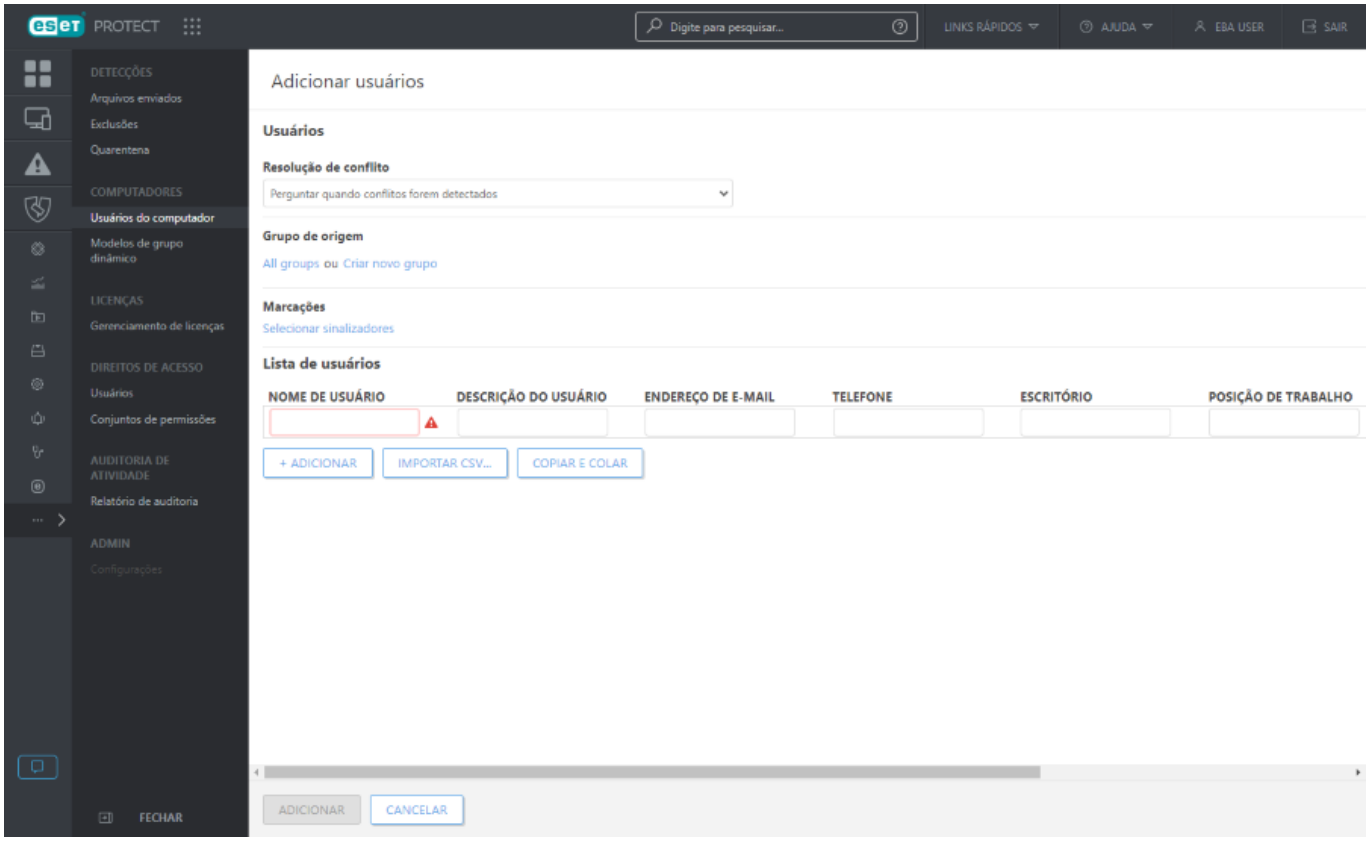
5. Use o menu suspenso de **Resolução de conflito** para selecionar a ação a ser realizada se um usuário sendo adicionado já existir no ESET PROTECT:

- **Perguntar quando conflitos forem detectados** – Quando um conflito for detectado, o programa pedirá que você selecione uma ação (veja as opções a seguir).

- **Pular 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.



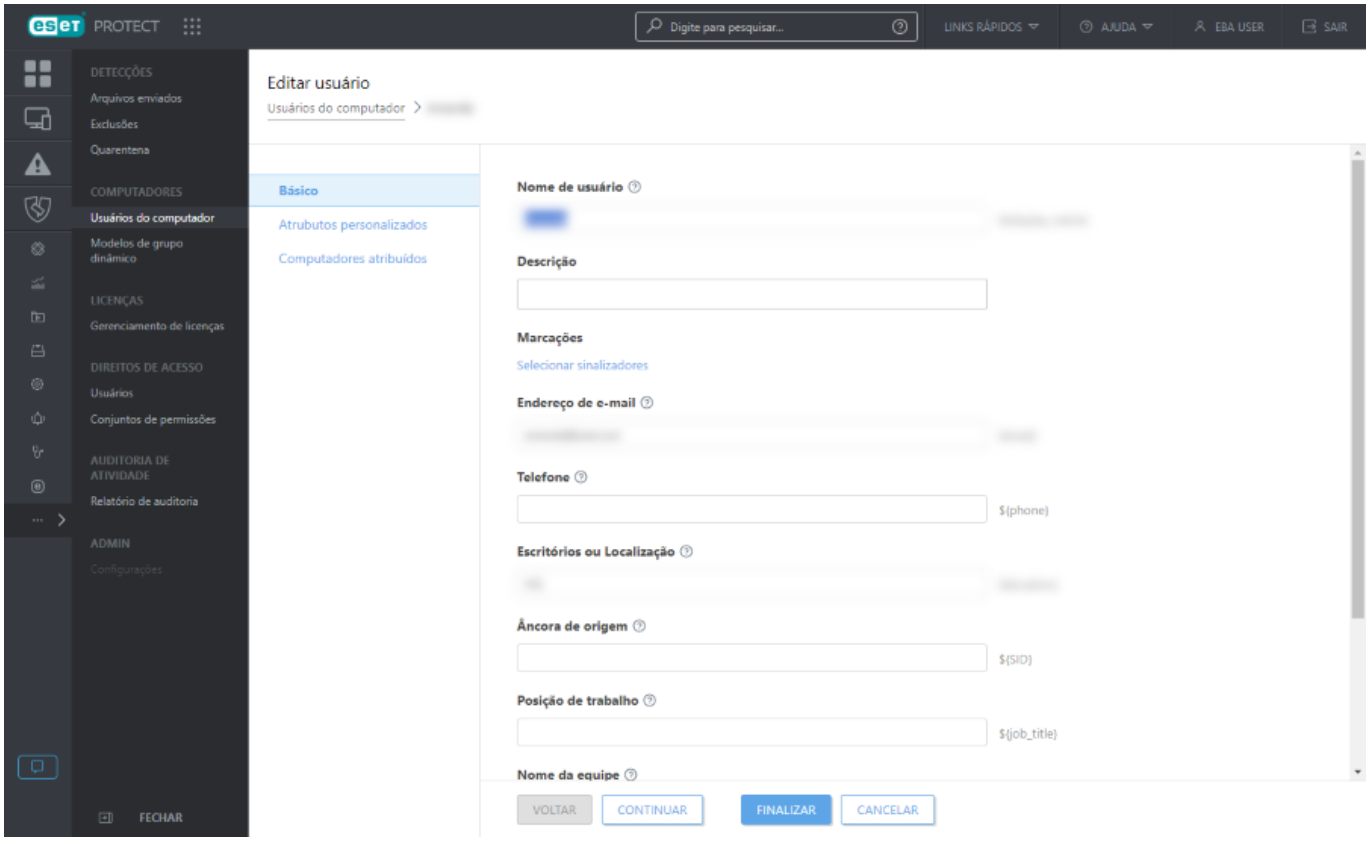
Editar usuários

Você pode modificar os detalhes do usuário como informações **Básicas** e **Computadores atribuídos**.

Básico

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.
- **Âncora de origem**: 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.

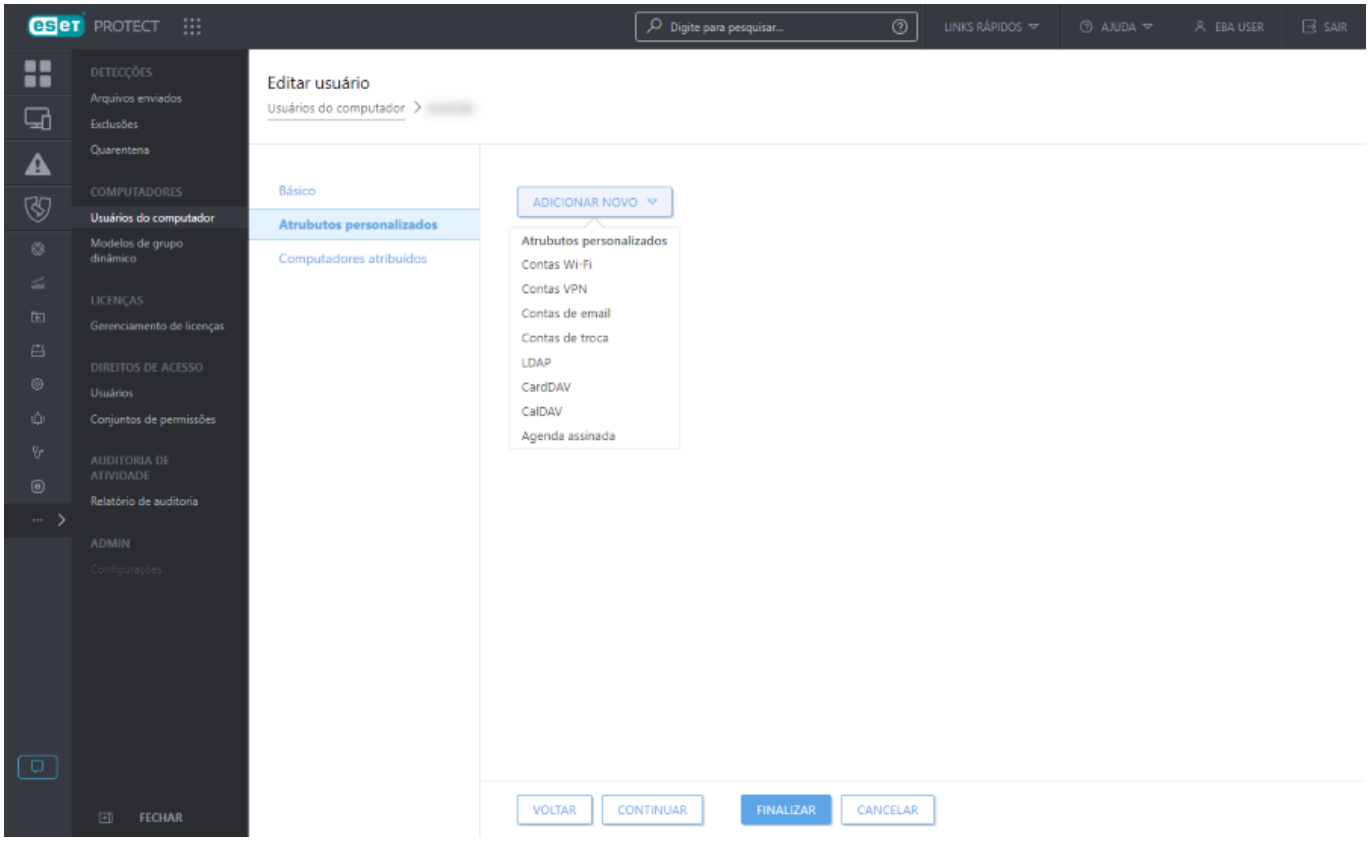
- **LDAP (Alias de atributo)** – Isto é especialmente útil se a sua empresa usa LDAP para contatos. Você pode mapear os campos de contato nos campos de contato iOS correspondentes.

- **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.

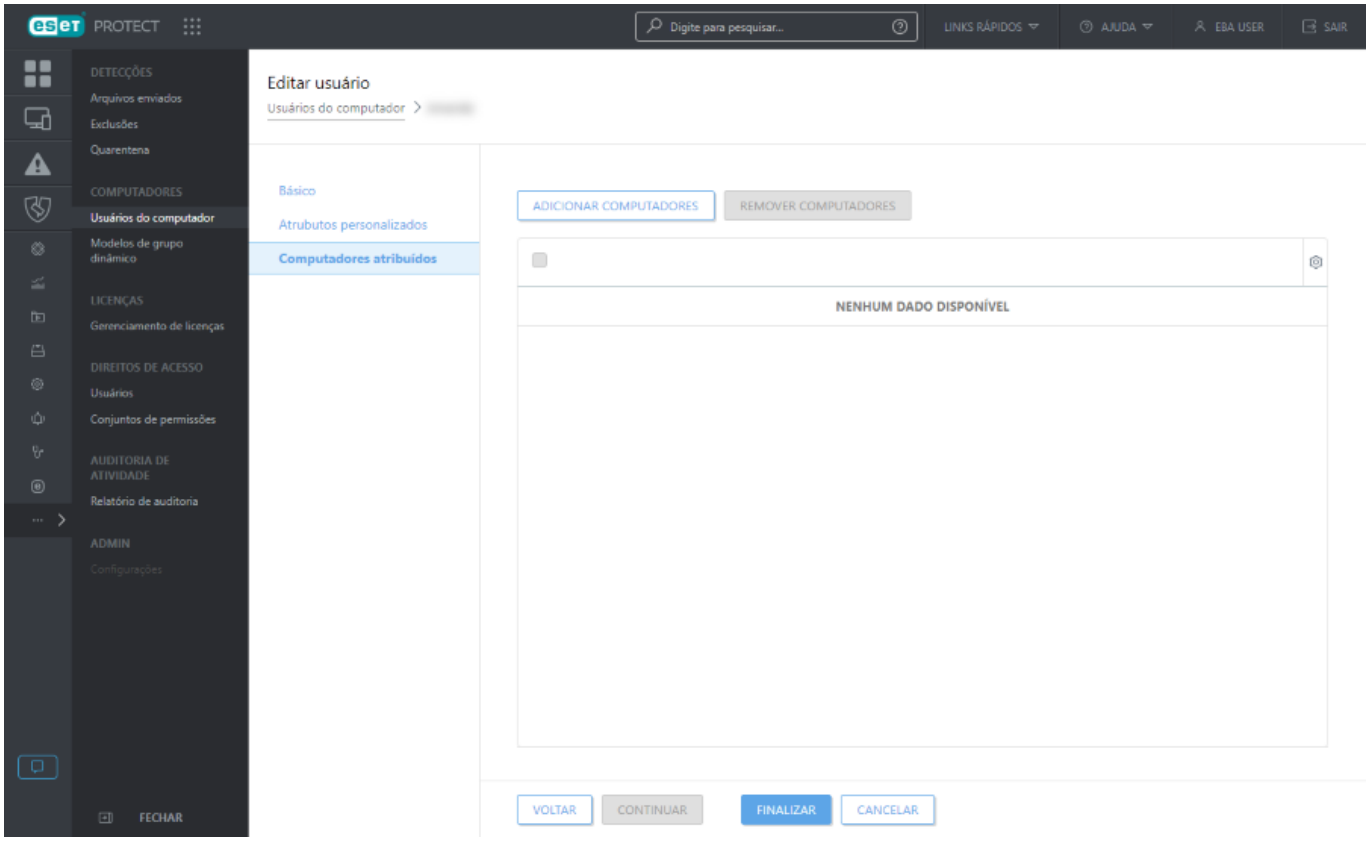
Alguns dos campos vão se tornar um atributo que pode ser usado ao criar uma política para dispositivo móvel iOS como uma variável (espaço reservado). Por exemplo, Login `${exchange_login/exchange}` ou Endereço de email `${exchange_email/exchange}`.



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.

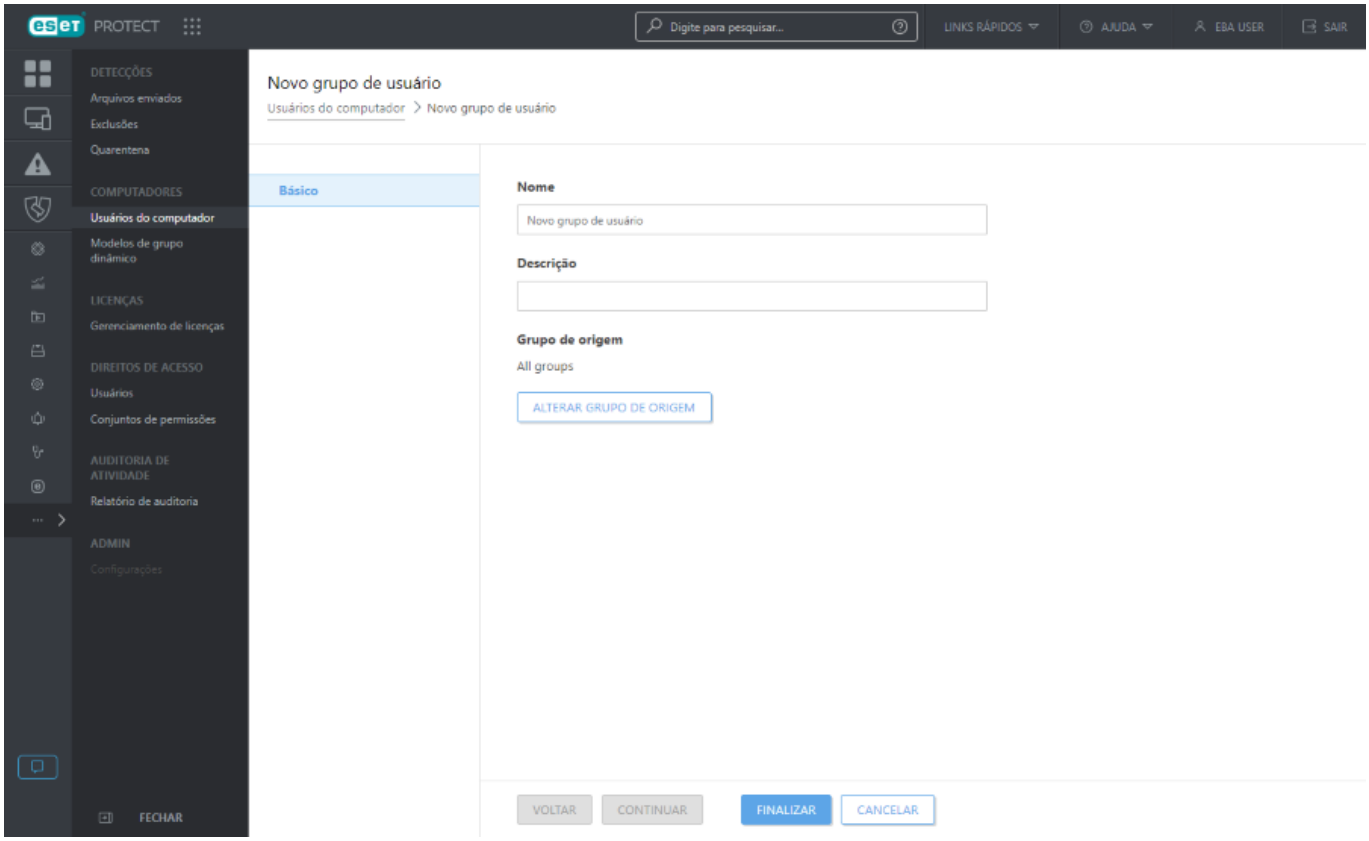


Criar novo grupo de usuário

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.



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.

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

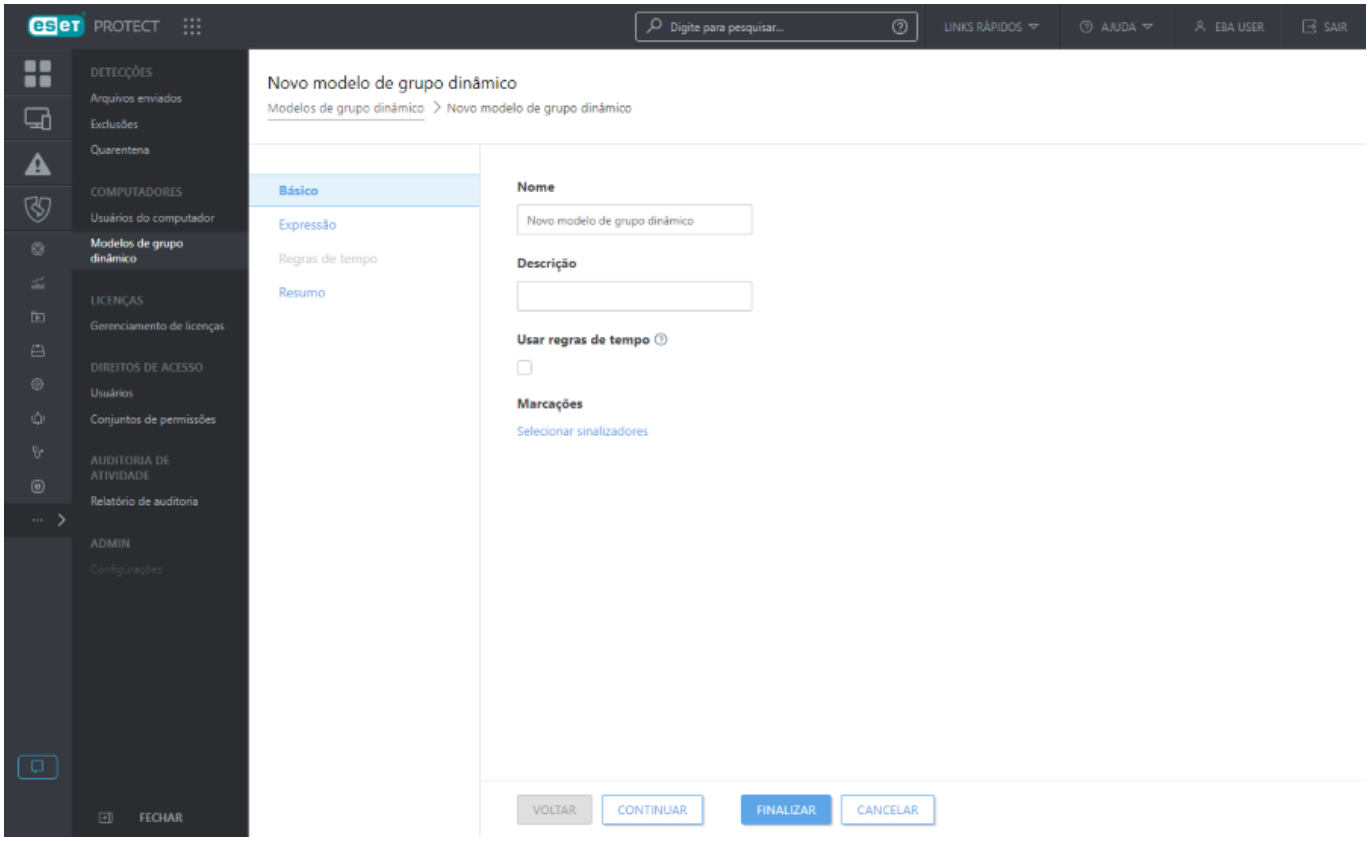
Insira um **Nome** e uma **Descrição** para o novo modelo de grupo dinâmico.

Selecione **Usar regras de tempo** para ativar as **Regras de tempo** e defina um horário específico durante o qual a correspondência de grupo dinâmico está ativada.

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.



Regras de tempo

Defina um intervalo de tempo para o novo modelo de grupo dinâmico. Clique no botão **Adicionar**. Clique no campo de hora e selecione **Hora de início** e **Hora de término** no menu suspenso. Selecione a frequência (Todos os dias, Dia útil, Fim de semana) ou o dia da semana e horário. O tempo selecionado deve ser de mais de 1 minuto e menos de 24 horas. Depois de definir a **Hora de início** e a **Hora de término**, a coluna **Duração** exibe a duração da hora definida. Você pode adicionar mais intervalos de tempo.

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 de Permissões de Modelo é feita pelo Agente ESET Management, não pelo Servidor ESET PROTECT (somente o resultado é enviado para o Servidor ESET PROTECT). 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 11 Enterprise	10.0.22621	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 11 Enterprise	10.0.22621	2048	ESET Endpoint Security

Adaptadores de rede - endereço IP	Adaptadores de rede - endereço MAC	Nome do SO	Versão do SO	HW - tamanho de RAM em MB	Aplicativo instalado
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 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 11 Enterprise	10.0.22621	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 11 Enterprise	10.0.22621	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.

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.

Selecione **Usar regras de tempo** para ativar as **Regras de tempo** e defina um horário específico durante o qual a correspondência de grupo dinâmico está ativada.

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.

Regras de tempo

Defina um intervalo de tempo para o novo modelo de grupo dinâmico. Clique no botão **Adicionar**. Clique no campo de hora e selecione **Hora de início** e **Hora de término** no menu suspenso. Selecione a frequência (Todos os dias, Dia útil, Fim de semana) ou o dia da semana e horário. O tempo selecionado deve ser de mais de 1 minuto e menos de 24 horas. Depois de definir a **Hora de início** e a **Hora de término**, a coluna **Duração** exibe a duração da hora definida. Você pode adicionar mais intervalos de tempo.

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.

Selecione **Usar regras de tempo** para ativar as **Regras de tempo** e defina um horário específico durante o qual a correspondência de grupo dinâmico está ativada.

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*

Regras de tempo

Defina um intervalo de tempo para o novo modelo de grupo dinâmico. Clique no botão **Adicionar**. Clique no campo de hora e selecione **Hora de início** e **Hora de término** no menu suspenso. Selecione a frequência (Todos os dias, Dia útil, Fim de semana) ou o dia da semana e horário. O tempo selecionado deve ser de mais de 1 minuto e menos de 24 horas. Depois de definir a **Hora de início** e a **Hora de término**, a coluna **Duração** exibe a duração da hora definida. Você pode adicionar mais intervalos de tempo.

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.

Selecione **Usar regras de tempo** para ativar as **Regras de tempo** e defina um horário específico durante o qual a correspondência de grupo dinâmico está ativada.

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*

Regras de tempo

Defina um intervalo de tempo para o novo modelo de grupo dinâmico. Clique no botão **Adicionar**. Clique no campo de hora e selecione **Hora de início** e **Hora de término** no menu suspenso. Selecione a frequência (Todos os dias, Dia útil, Fim de semana) ou o dia da semana e horário. O tempo selecionado deve ser de mais de 1 minuto e menos de 24 horas. Depois de definir a **Hora de início** e a **Hora de término**, a coluna **Duração** exibe a duração da hora definida. Você pode adicionar mais intervalos de tempo.

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.

Selecione **Usar regras de tempo** para ativar as **Regras de tempo** e defina um horário específico durante o qual a correspondência de grupo dinâmico está ativada.

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*

Regras de tempo

Defina um intervalo de tempo para o novo modelo de grupo dinâmico. Clique no botão **Adicionar**. Clique no campo de hora e selecione **Hora de início** e **Hora de término** no menu suspenso. Selecione a frequência (Todos os

dias, Dia útil, Fim de semana) ou o dia da semana e horário. O tempo selecionado deve ser de mais de 1 minuto e menos de 24 horas. Depois de definir a **Hora de início** e a **Hora de término**, a coluna **Duração** exibe a duração da hora definida. Você pode adicionar mais intervalos de tempo.

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.

Selecione **Usar regras de tempo** para ativar as **Regras de tempo** e defina um horário específico durante o qual a correspondência de grupo dinâmico está ativada.

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*

Regras de tempo

Defina um intervalo de tempo para o novo modelo de grupo dinâmico. Clique no botão **Adicionar**. Clique no campo de hora e selecione **Hora de início** e **Hora de término** no menu suspenso. Selecione a frequência (Todos os dias, Dia útil, Fim de semana) ou o dia da semana e horário. O tempo selecionado deve ser de mais de 1 minuto e menos de 24 horas. Depois de definir a **Hora de início** e a **Hora de término**, a coluna **Duração** exibe a duração da hora definida. Você pode adicionar mais intervalos de tempo.

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.

Selecione **Usar regras de tempo** para ativar as **Regras de tempo** e defina um horário específico durante o qual a correspondência de grupo dinâmico está ativada.

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**

Regras de tempo

Defina um intervalo de tempo para o novo modelo de grupo dinâmico. Clique no botão **Adicionar**. Clique no campo de hora e selecione **Hora de início** e **Hora de término** no menu suspenso. Selecione a frequência (Todos os dias, Dia útil, Fim de semana) ou o dia da semana e horário. O tempo selecionado deve ser de mais de 1 minuto e menos de 24 horas. Depois de definir a **Hora de início** e a **Hora de término**, a coluna **Duração** exibe a duração da hora definida. Você pode adicionar mais intervalos de tempo.

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.

Gerenciamento de licenças

Você pode gerenciar facilmente suas licenças através do ESET PROTECT no menu principal sob **Mais** > **Gerenciamento de licenças**. Você pode ver aqui licenças sincronizadas do ESET Business Account que você usou para implantação do ESET PROTECT.

Para usar licenças do outro ESET Business Account, é preciso mover as licenças para o ESET Business Account que você usou para a implantação do ESET PROTECT.

Você pode ativar seu produto empresarial ESET usando o ESET PROTECT.

Consulte também as Perguntas frequentes de licenciamento (usuários corporativos).

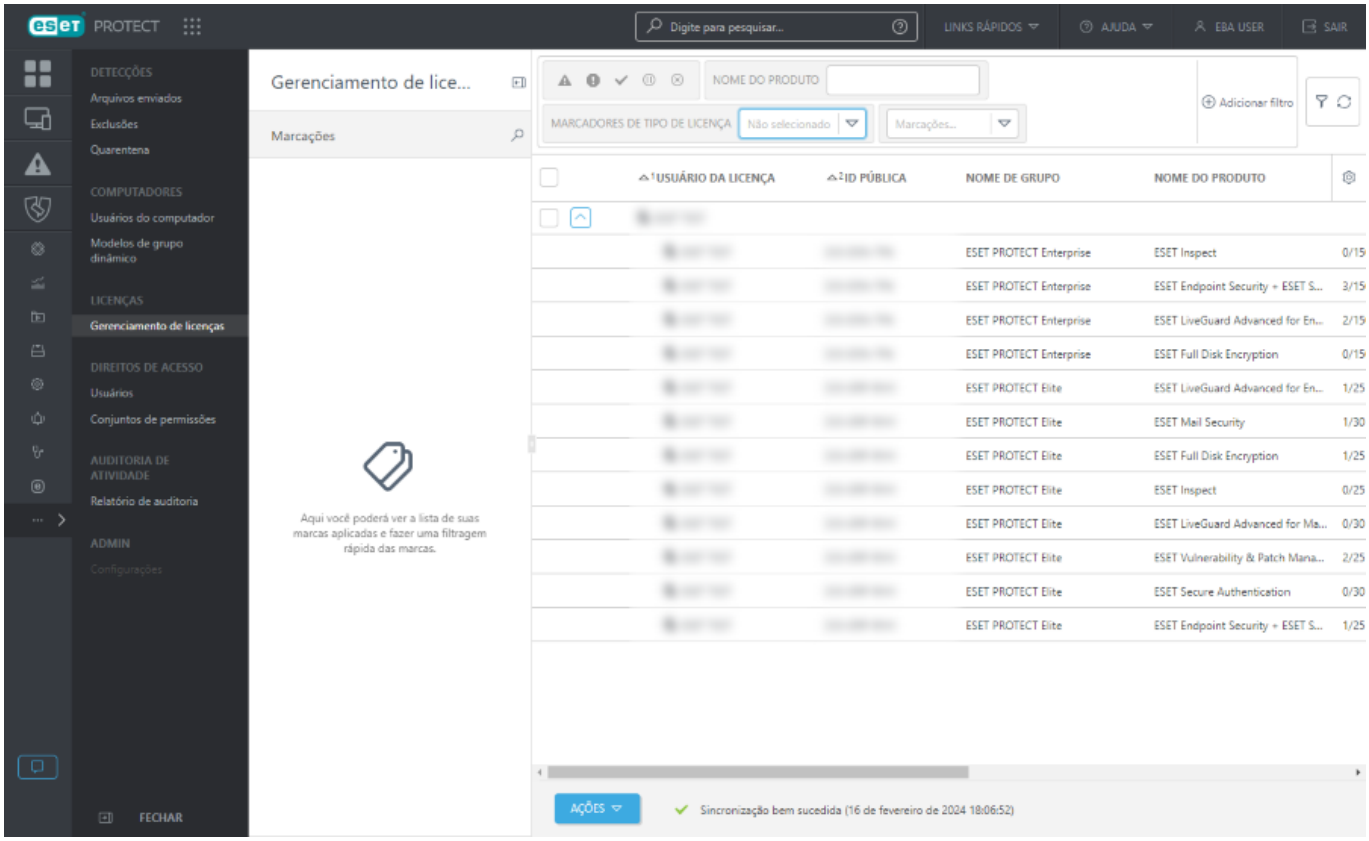
Permissões para gerenciamento de licenças

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 de pacote** para o qual os produtos ESET são destinados. Leia mais sobre os níveis de proteção ESET.

- 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 **Validade** representa 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).
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 em ESET Business Account ou ESET MSP Administrator.
Atualizar licença	Atualize a licença de avaliação em 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. Você pode verificar a validade da sua assinatura em **Gerenciamento de licenças** na coluna **Validade** ou em **Computadores** > Detalhes.

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 não pode usar a licença ESET PROTECT para ativação dos produtos de segurança ESET em endpoints gerenciados. Para ativar produtos de segurança ESET individuais, use as licenças para esses produtos.

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.

Licenças elegíveis para a nuvem

Licenças elegíveis para a nuvem são licenças que podem ser usadas com o ESET PROTECT. Leia mais sobre os níveis de proteção ESET.

Não é possível usar os níveis de proteção local do ESET PROTECT na nuvem ESET PROTECT.

Veja na tabela abaixo quais licenças podem ser usadas para criar uma instância ESET PROTECT e quais níveis são usados apenas para ativar recursos específicos do produto.

Nome da camada	Elegível para criar uma instância ESET PROTECT no ESET Business Account	Elegível para criar uma instância ESET PROTECT no ESET MSP Administrator
ESET PROTECT Essential	✔	
ESET PROTECT Entry (anteriormente: ESET Endpoint Protection Advanced Cloud)	✔	✔
ESET Secure Business Cloud	✔	
ESET PROTECT Advanced (anteriormente: ESET Remote Workforce Offer)	✔	✔
ESET PROTECT Complete	✔	✔
ESET PROTECT Enterprise	✔	✔
ESET PROTECT Mail Plus	✔	✔
ESET PROTECT Elite	✔	✔
ESET PROTECT MDR	✔	
ESET Security for Microsoft SharePoint Server (Per Server)	✔	
ESET LiveGuard Advanced		
ESET LiveGuard Advanced for Endpoint Security + ESET Server Security (ESET File Security)		
ESET LiveGuard Advanced for Mail Security		
ESET Full Disk Encryption para ECA		

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

Direitos de acesso

Os direitos de acesso permitem gerenciar os usuários do Web Console ESET PROTECT e suas permissões.

O modelo de segurança

Essas configurações de direitos de acesso são aplicadas aos usuários apenas quando uma **Permissão personalizada** é definida no gerenciamento de contas ESET Business Account (EBA). **Permissões personalizadas** podem ser adicionadas no Web Console ESET PROTECT apenas por uma conta com permissões de **Superusuário** no portal ESET Business Account.

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 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.

- Ações do usuário e detalhes do usuário
- Usuários mapeados
- Atribuir um conjunto de permissões a um usuário

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.
b)**Conjunto de permissões** chamado de *Conjunto de permissões San Diego*, com o grupo estático *Escritório San Diego*, e com permissões de acesso total.
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 **Licenças**
- **Gravação** para **Notificações**

3.Crie o novo usuário *John* no escritório do grupo doméstico *San Diego*, atribuído aos conjuntos de permissões *conjunto de permissões de San Diego* e *Todos os Grupos/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:

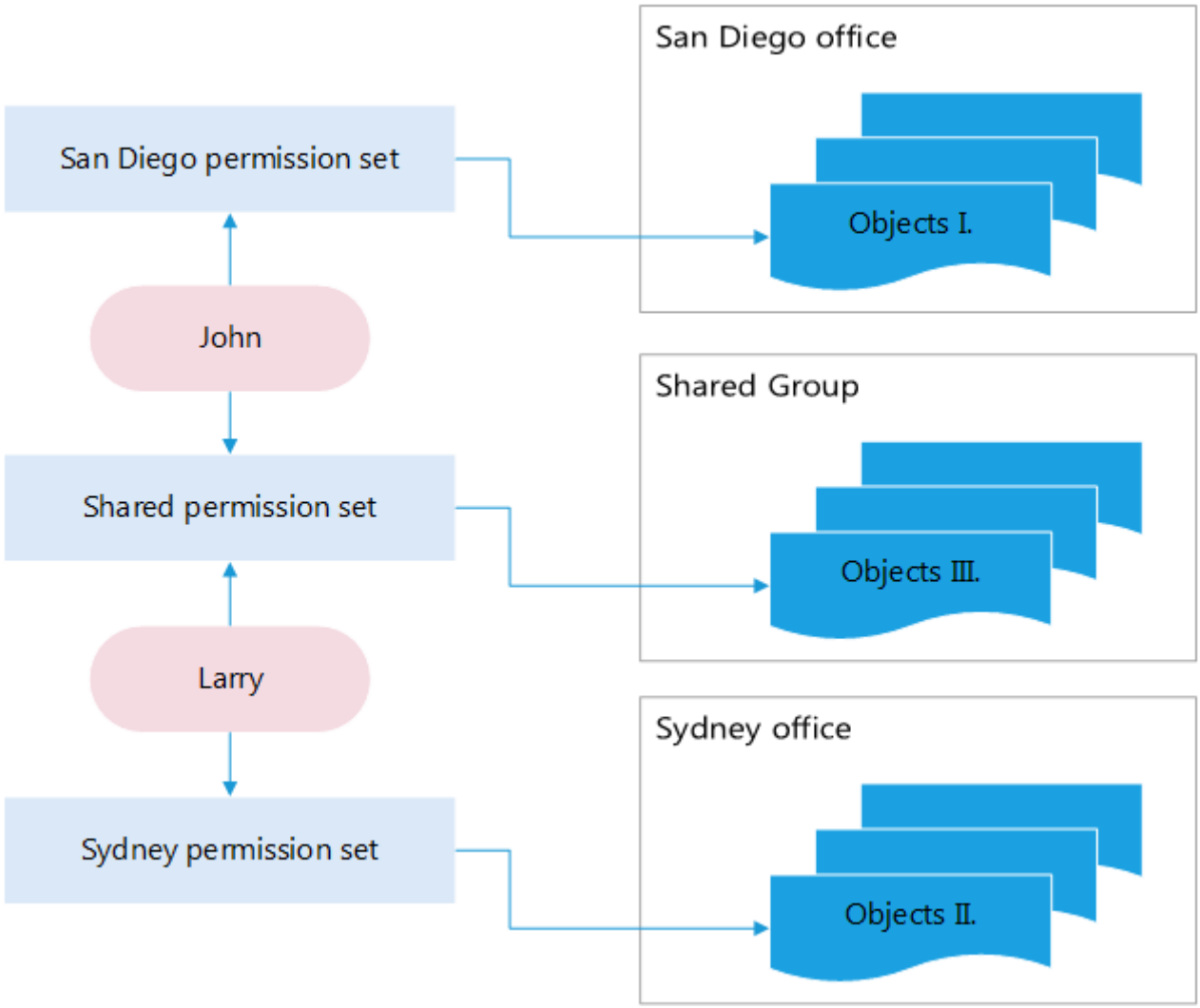
- Mova esses objetos para os grupos compartilhados

- 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.

Ações do usuário e detalhes do usuário

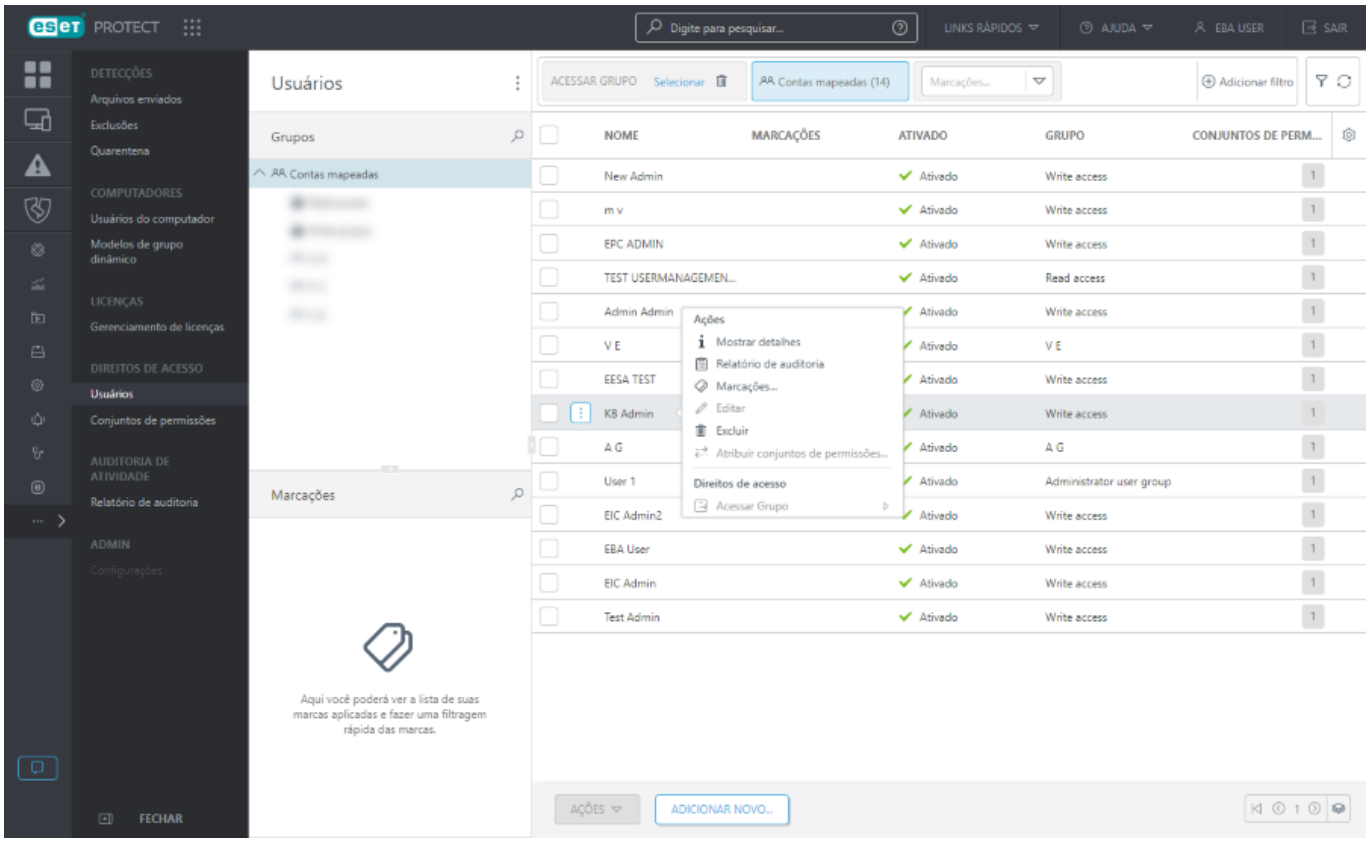
Para gerenciar um usuário, selecione o usuário aplicável e selecione uma das ações disponíveis:

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.

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:

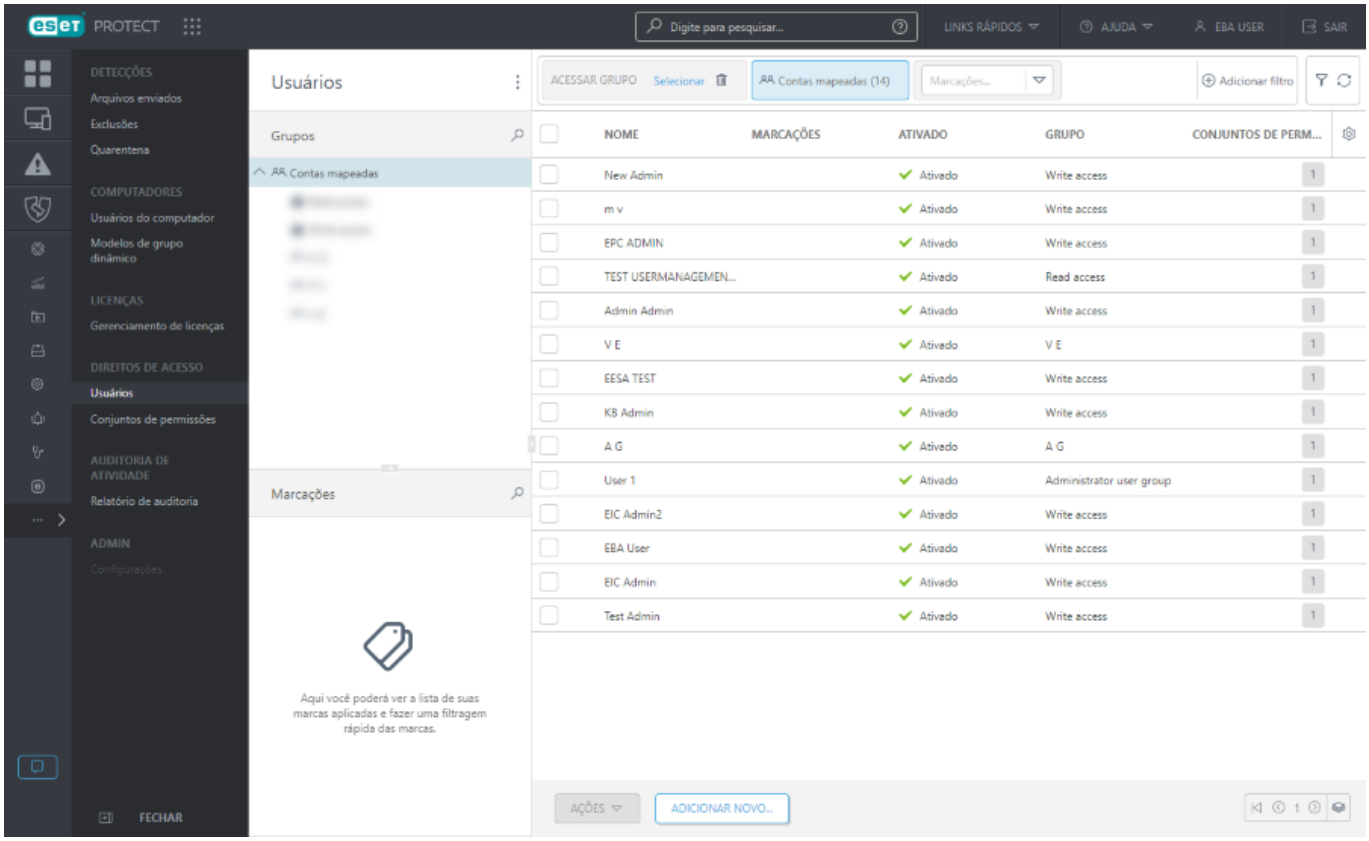
- **Visão geral** – informações básicas sobre o usuário. Você pode gerenciar o usuário usando o botão **Ações** na parte inferior.
- **Conjuntos de permissão** – a lista de conjuntos de permissões atribuídos ao usuário. Clique em um conjunto de permissões para gerenciá-lo.

Mapear usuários do ESET Business Account

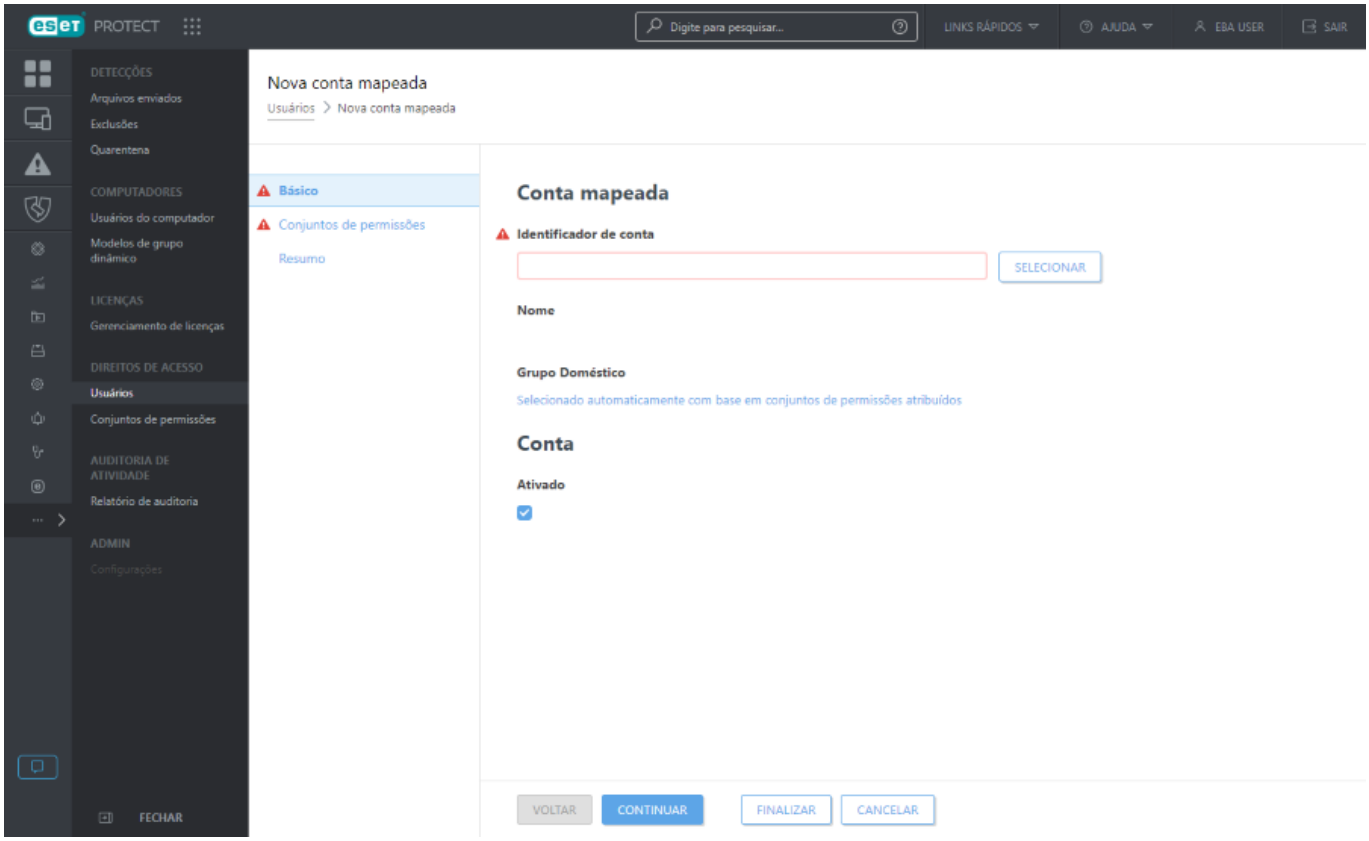
Siga as etapas abaixo para mapear um usuário do ESET Business Account no ESET PROTECT:

1. Entre no seu ESET Business Account com a conta do usuário usada ao criar um novo usuário no ESET Business Account; não use a conta de usuário recém-criada no momento.

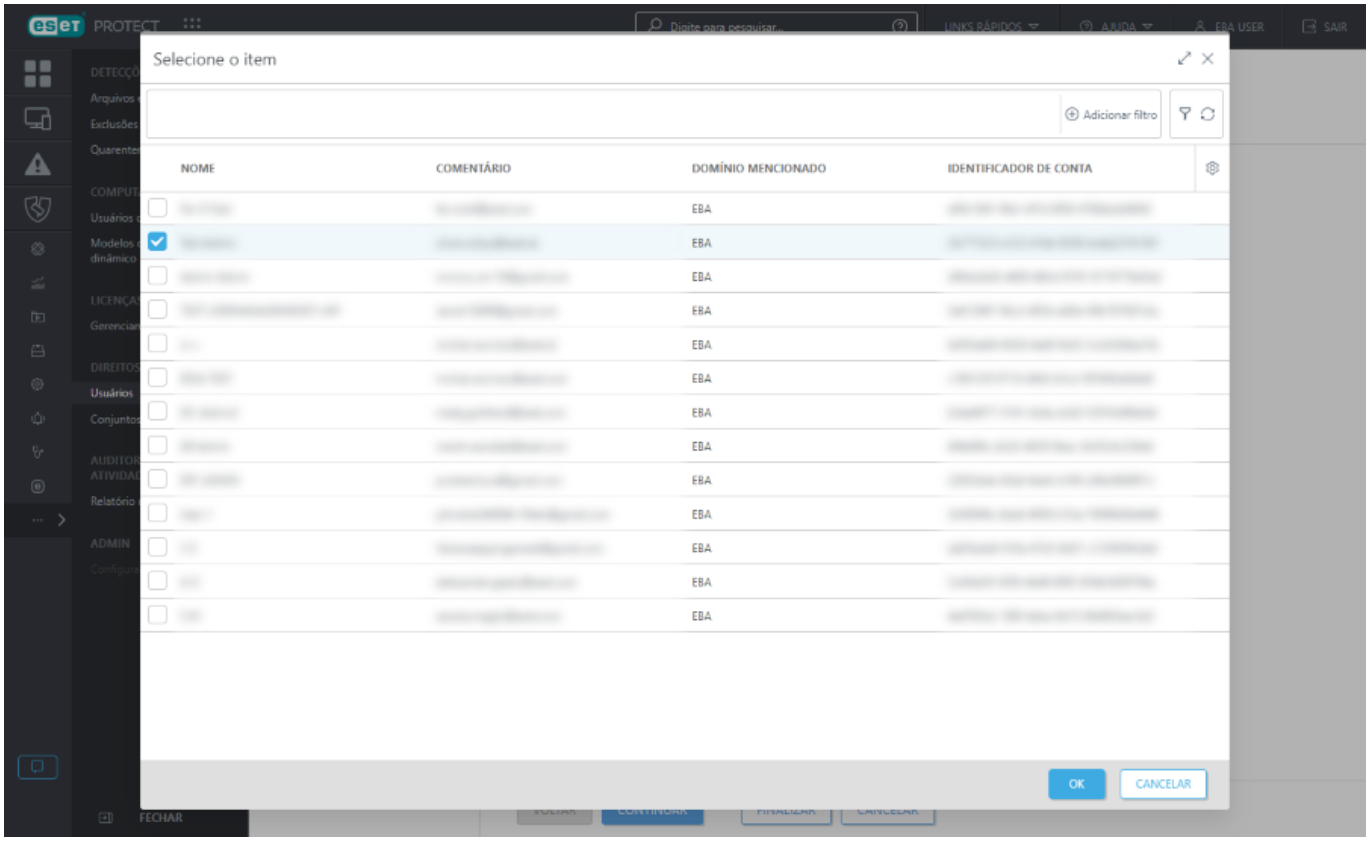
2. Abrir o Console Web ESET PROTECT. Clique em **Mais** > **Usuários** > selecione **Contas mapeadas** > clique no botão **Adicionar novo**.



3. Clique em **Selecionar** sob **Identificador de conta**.



4. Selecione o usuário [criado em ESET Business Account](#) e clique em **OK**.



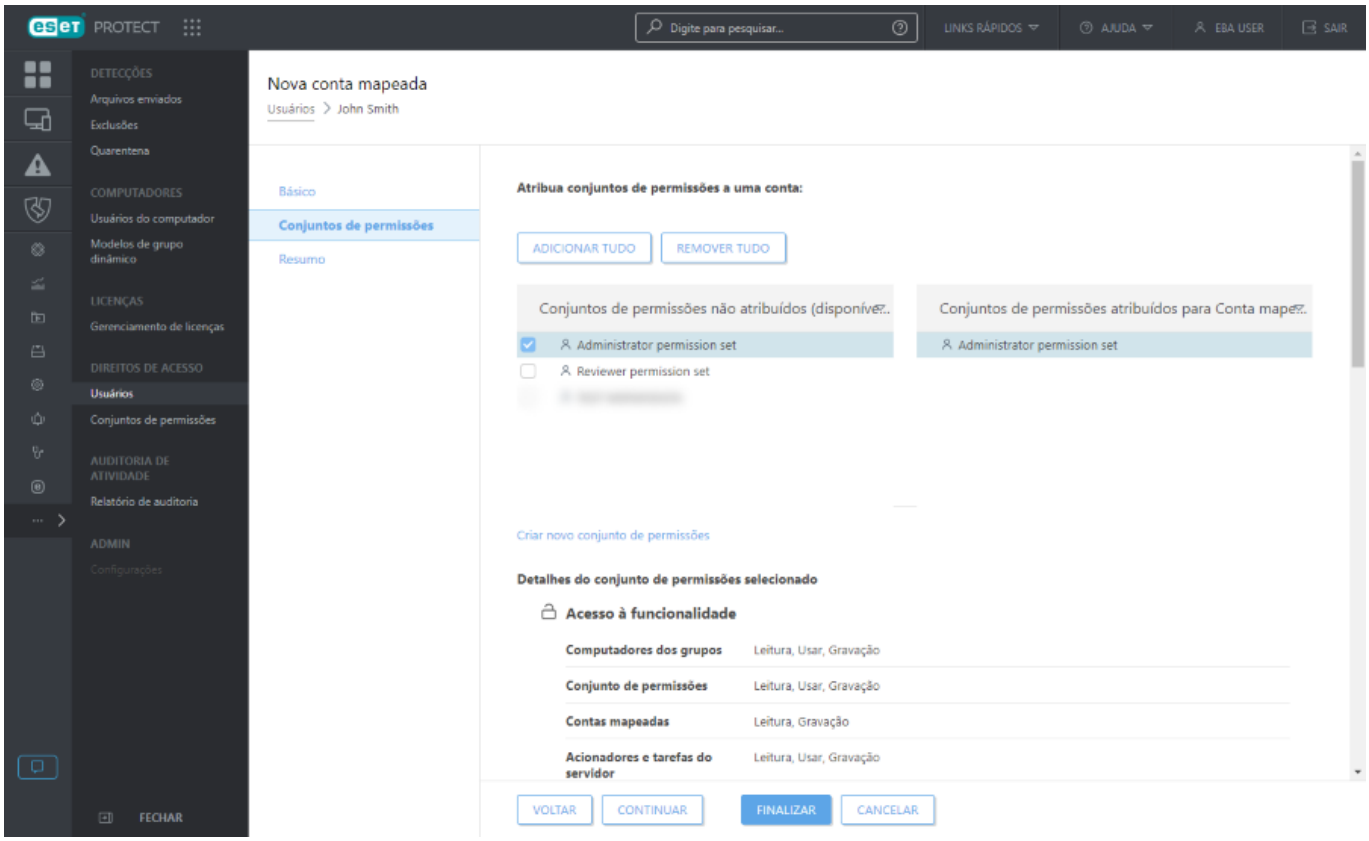
5. **Grupo doméstico** – O grupo doméstico é detectado automaticamente com base no conjunto de permissões atribuído do usuário atualmente ativo.

Exemplo de cenário:

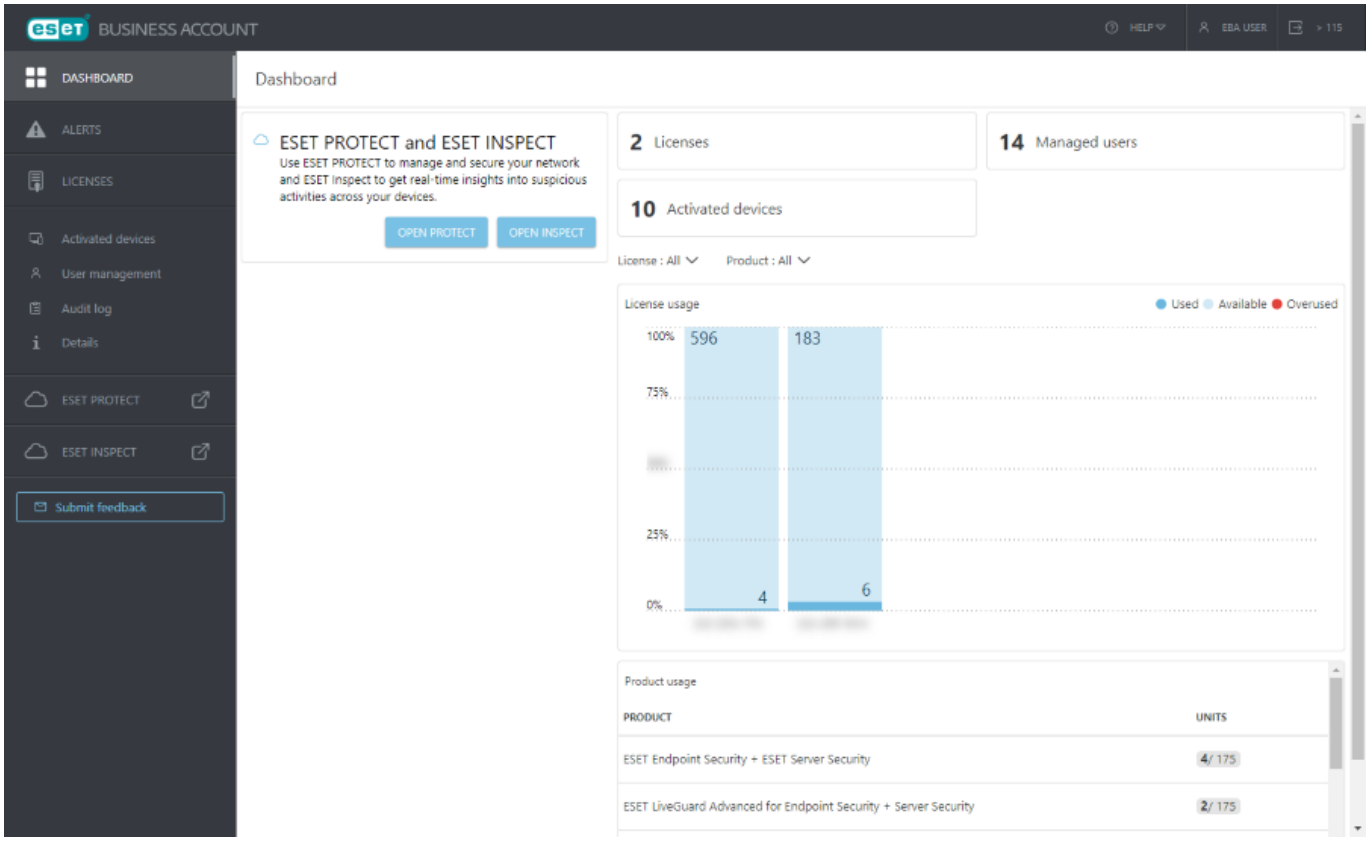
A conta de usuário atualmente ativa tem o direito de acesso de **Gravação** para a **Tarefa de cliente de Instalação de software** e a conta do **Grupo doméstico** é "Department_1". Quando o usuário criar uma nova **Tarefa de cliente de instalação de software**, "Department_1" será selecionado automaticamente 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.

6. Em **Conjuntos de permissões**, você pode ver o nível de permissões atribuído ao usuário ao criar o usuário no ESET Business Account. Se você selecionou **Acesso personalizado ao ESET PROTECT**, precisará atribuir um conjunto de permissões para o usuário (um existente, ou você poderá criar um novo conjunto de permissões). Clique em **Concluir**.



7. Os usuários que receberam o acesso ao ESET PROTECT vão ver a opção de abrir o ESET PROTECT no seu ESET Business Account.

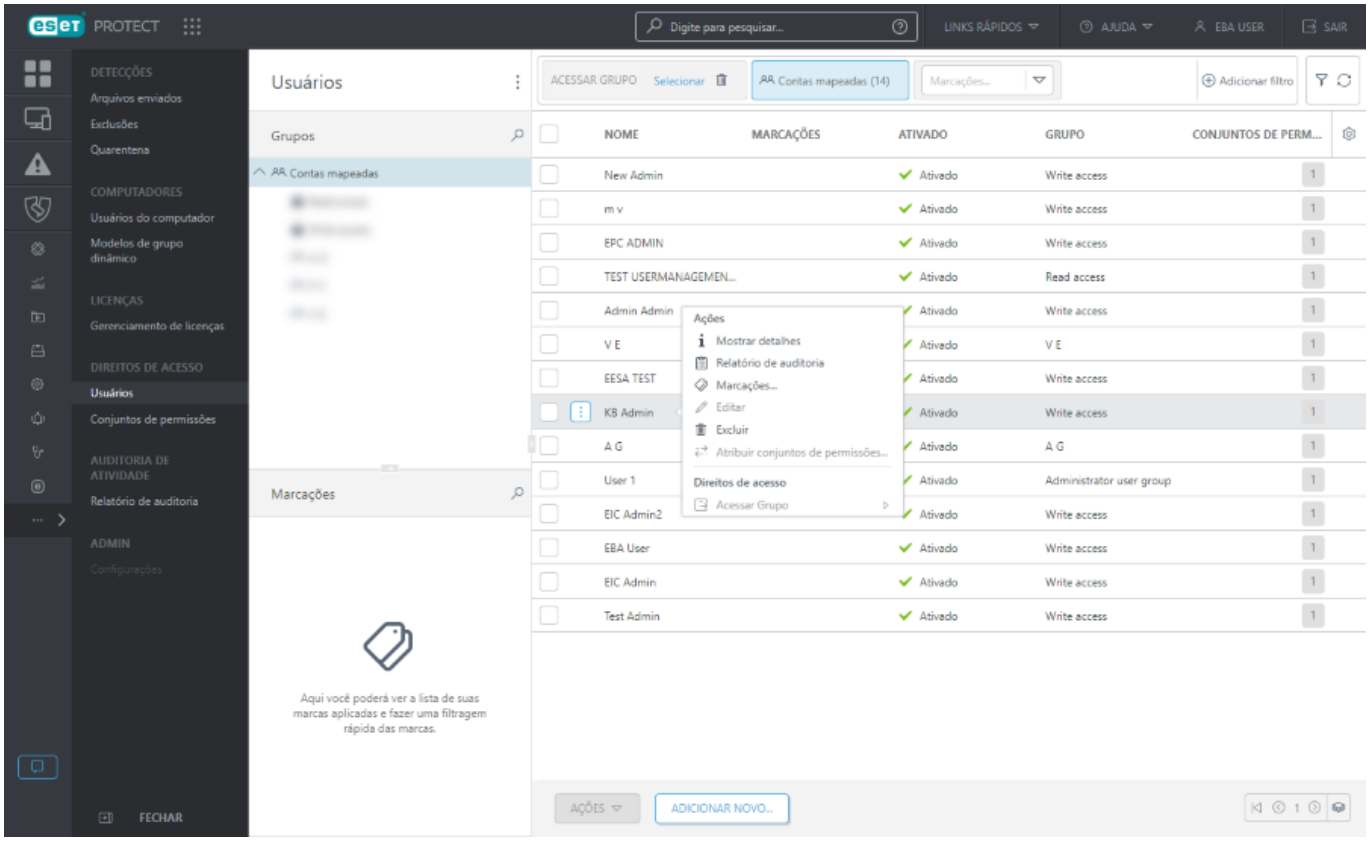


Atribuir um conjunto de permissões a um usuário

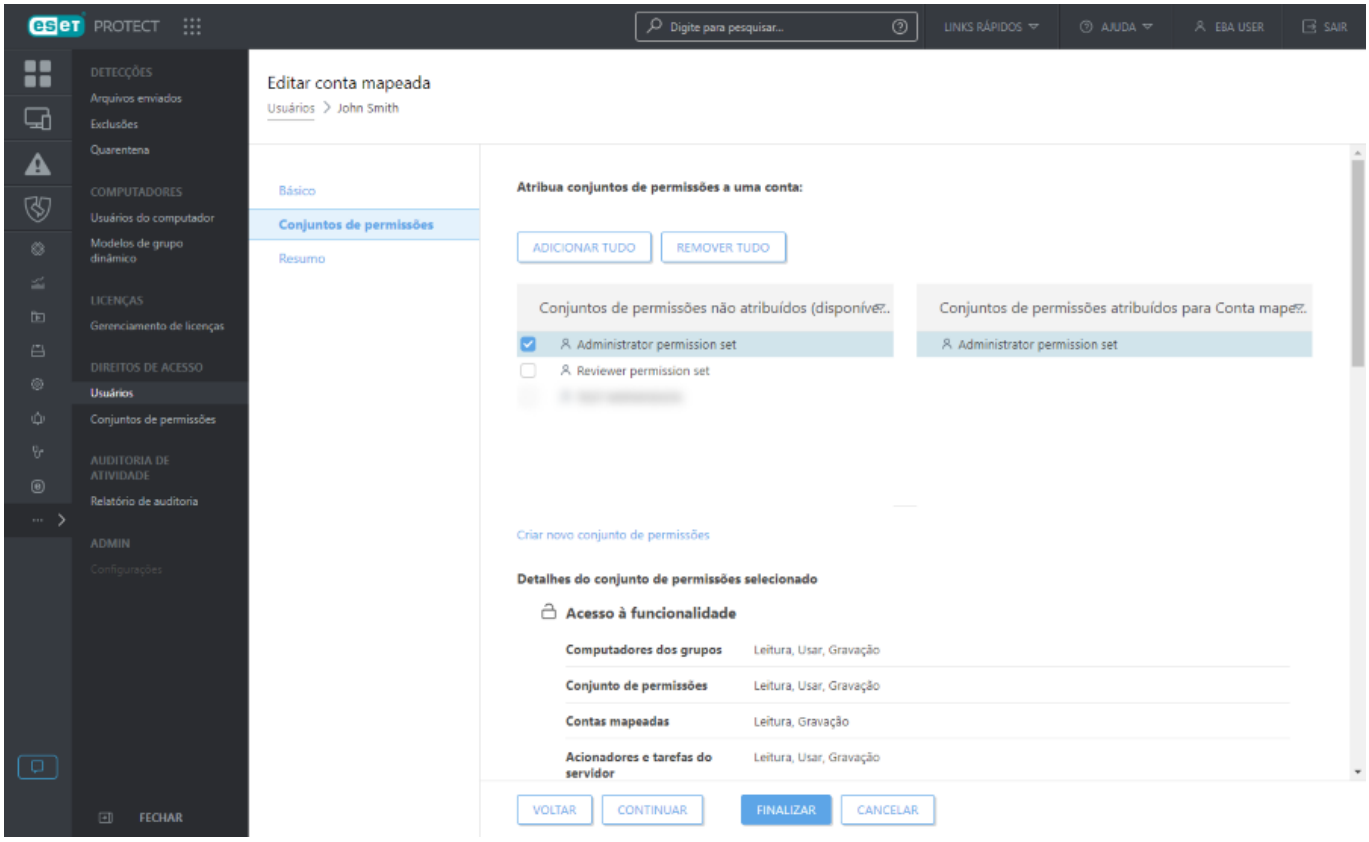
1. Há duas formas de atribuir um conjunto de permissões a um usuário:

   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.



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. 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).

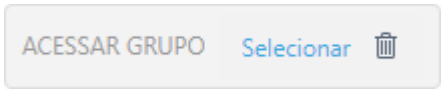
Um usuário pode receber a atribuição de um conjunto de permissões mesmo sem ser capaz de vê-lo. Um conjunto de permissões também é um objeto que é automaticamente armazenado no grupo inicial do usuário que o criou. Quando uma conta de usuário é criada, o usuário é armazenado como objeto no grupo inicial 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

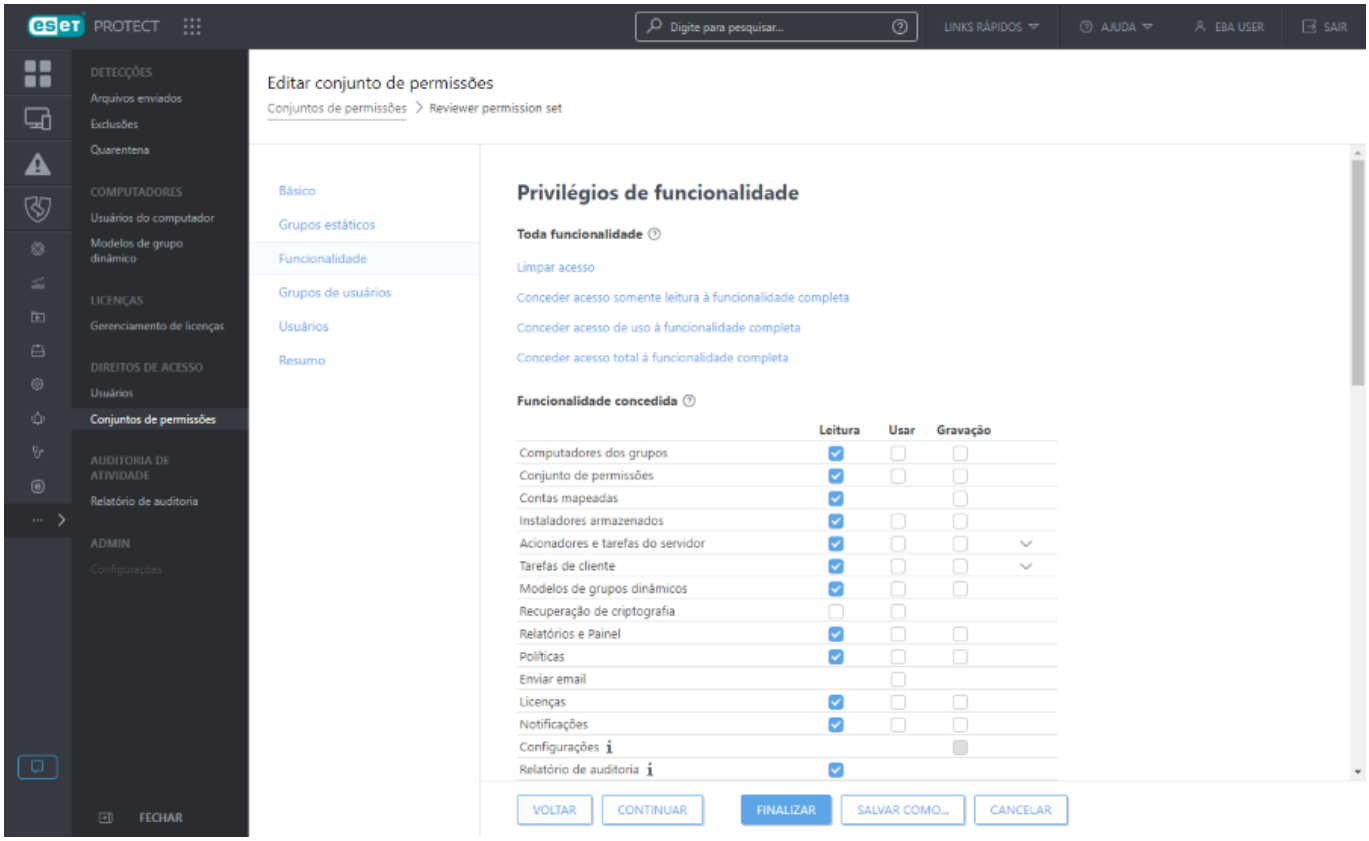
O acesso final que um usuário tem a um objeto é o resultado da combinação de todos os conjuntos de permissões atribuídos ao usuário. Por exemplo, um usuário que tenha dois conjuntos de permissões, um para um grupo doméstico com permissões totais e outro para um grupo com computadores, com permissões 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:
• Considere restringir o acesso para as **Tarefas de cliente** > **Executar comando** - é uma tarefa muito potente que pode ser mal utilizada.
• Os usuários de nível não administrativo não devem ter permissões para **Conjuntos de permissões** e **Contas mapeadas**.
• 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.

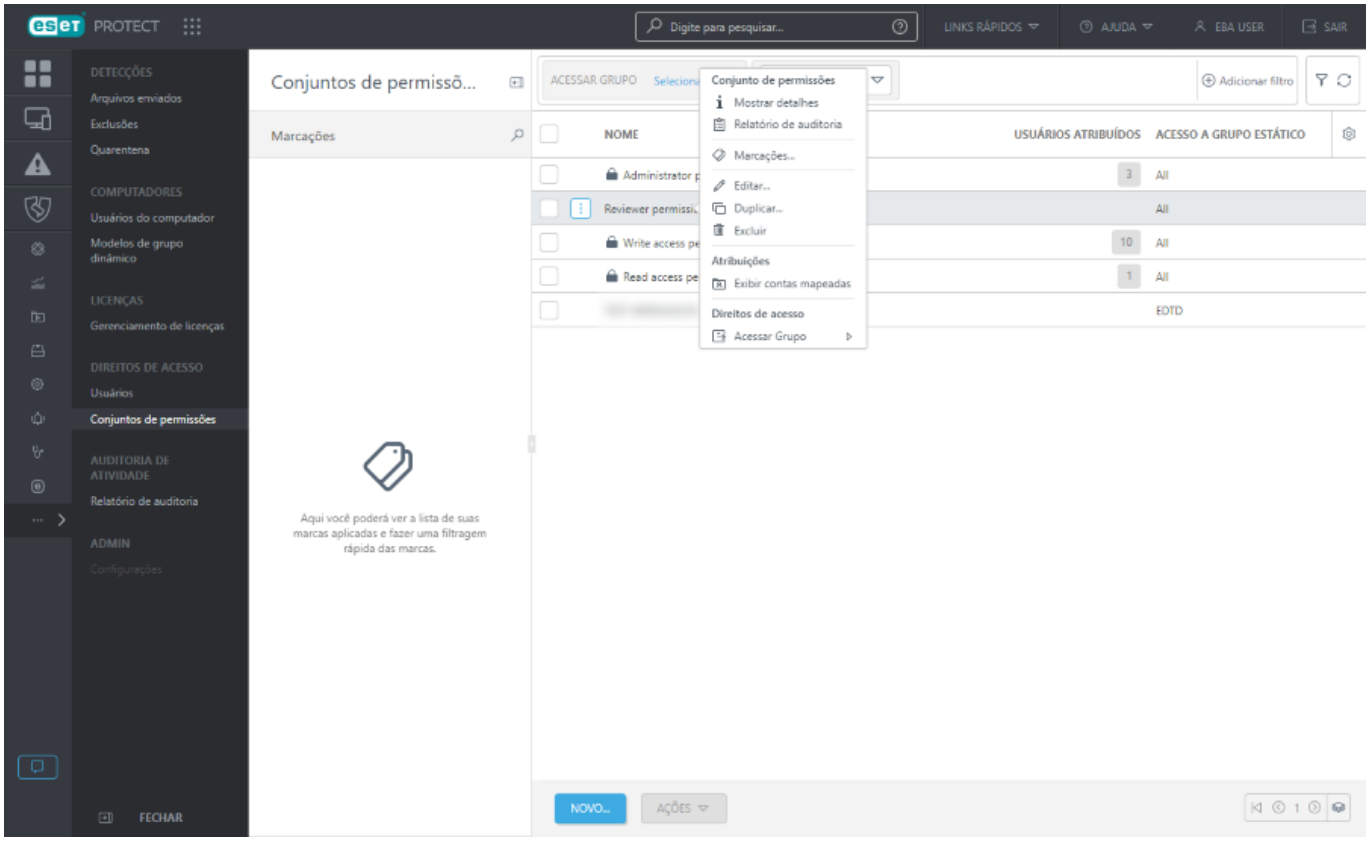
Diferença entre Uso e Gravação

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 contas mapeadas** – exibe a lista de contas mapeadas atribuídas.

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, 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**
- **Token de acesso do Escaneador AD**
- **Relatórios abrangentes**
- **Relatórios ESET MDR**

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.

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 cancelar a atribuição de) um conjunto de permissões a um usuário, a permissão **Gravação** é necessária para **Contas mapeadas**.

Contas mapeadas

Leitura – lista contas mapeadas.

Gravação - Permite a concessão/anulação de conjuntos de permissões.

Instaladores armazenados

Leitura - Lista os instaladores armazenados.

Uso - Exportar o instalador armazenado.

Gravação - Criar/modificar/remover instaladores armazenados.

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.)

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.

Uso – atribuir marcações.

Gravação - Criar, modificar, remover notificações.

Configurações

Gravação - Modificar ESET PROTECT configurações.

Relatório de auditoria

Leitura – exibir o Relatório de auditoria e ler o Relatório de auditoria.

Token de acesso do Escaneador AD

Leitura

Gravação – necessária para sincronização do AD.

Relatórios abrangentes

Uso - gerar o MDR Modelo de Relatório.

Relatórios ESET MDR

Uso - necessário para MDR Arquivamento de Relatórios.

Gravar - gerar os ESET MDR relatórios.

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.

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.

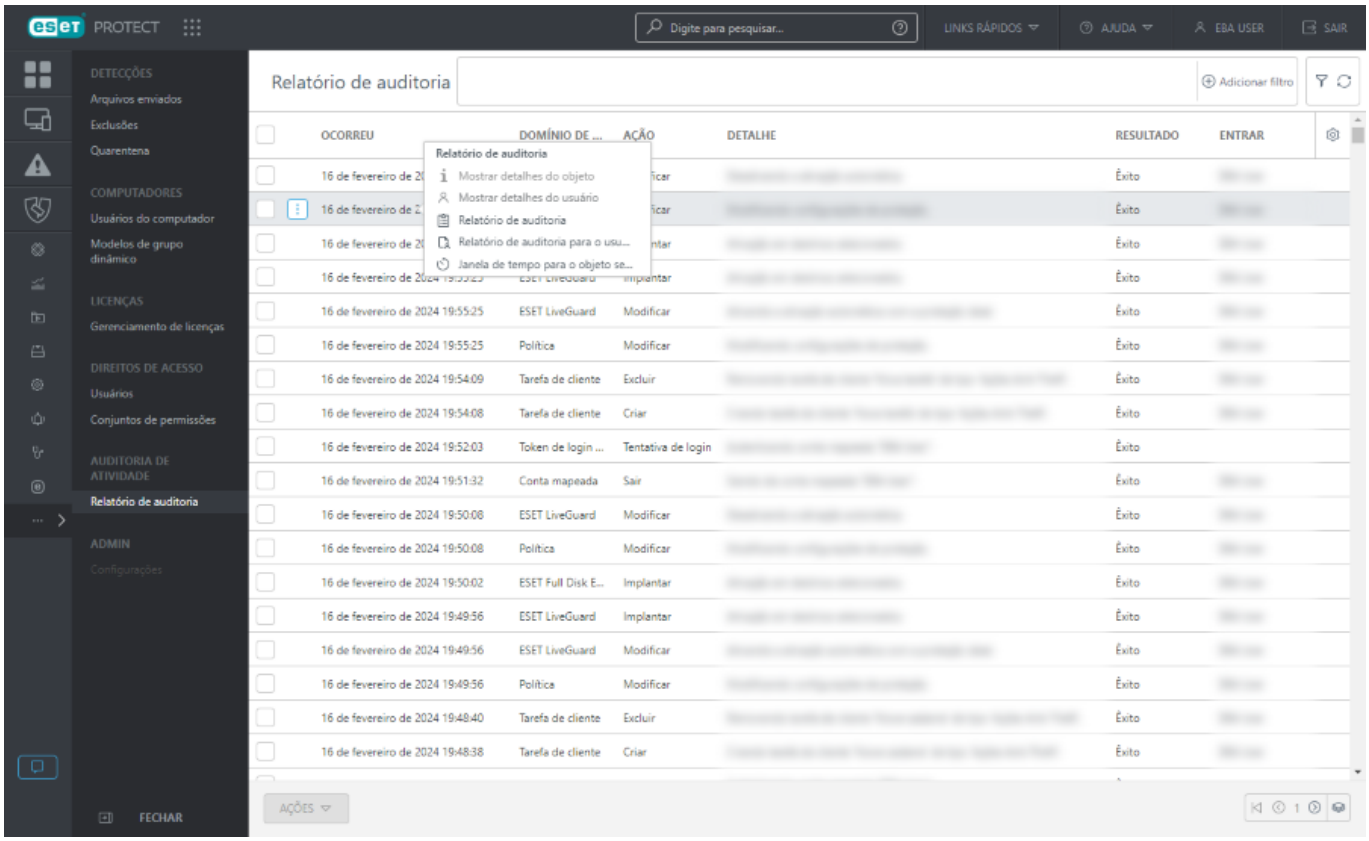
O Relatório de auditoria é uma nova tela disponível no ESET PROTECT. O Relatório de auditoria contém as mesmas informações que o Relatório de auditoria, mas permite uma conveniente filtragem dos dados exibidos. Você também pode visualizar diretamente o relatório de auditoria filtrado para vários objetos 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

A seção Configurações permite que o administrador ajuste as propriedades de entrega das informações Syslog para seu servidor Syslog e especifique a política de retenção de dados para os relatórios do console da nuvem.

A seção **Configurações** está disponível apenas para um usuário com permissões suficientes (por exemplo, conta de Superusuário (ESET Business Account) / Root User (ESET MSP Administrator)).

Geral

Syslog

Ative 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.

Retenção de dados

Especifique o período de limpeza para tipos específicos de relatórios armazenados no console da nuvem. Indica o número de dias/semanas/meses/anos pelos quais os relatórios serão armazenados no servidor para cada categoria. 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 • 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.

Limites de armazenamento:

Tipo de log	Mínimo	Padrão	Máximo
Relatórios de detecção	1 dia	90 dias	365 dias
Relatórios de gerenciamento	1 dia	30 dias	30 dias
Relatórios de auditoria	1 dia	180 dias	730 dias

Tipo de log	Mínimo	Padrão	Máximo
Relatórios de monitoramento	1 dia	30 dias	30 dias

Você pode aprender mais sobre o que acontece com os dados armazenados depois da expiração da última licença elegível .

Proteção de sessão para o Web Console

Bloquear solicitações de endereços IP diferentes:

- **Ativar**: se você quiser limitar o intervalo de endereços IP que podem acessar seu Web Console.
- **Desativar**:
  - **Desativar permanentemente** – isto permitirá que os usuários acessem seu intervalo de endereços IP não filtrado do Web Console.
  - **Desativar por** – seleciona um período de tempo pelo qual a limitação de acesso ao endereço IP será desativada.

Grupos estáticos

Parear automaticamente computadores encontrados – se estiver **Ativado**, esta configuração ativa o pareamento automático de computadores encontrados com computadores já presentes em grupos estáticos com base no nome de host reportado pelo Agente ESET Management.

- Se o pareamento falhar, o computador será colocado no grupo Achados e perdidos.
- Se o Agente não reportar com confiança o nome de host, recomendamos desativar o pareamento automático.

Gestão de dispositivo móvel

Inscrição Microsoft Entra ID

Confira Inscrição do Microsoft Entra ID (Android ou iOS).

Sincronização de Apple Business Manager (ABM)

Confira Sincronização de Apple Business Manager (ABM) (iOS).

Sincronização do Microsoft Intune

Confira Sincronização do Microsoft Intune (Android).

VMware Workspace ONE Sincronização

Consulte Sincronização do VMware Workspace One (Android).

Migração de dispositivos móveis de ESET PROTECT (lokal)

Veja mais detalhes na Ferramenta de migração de gerenciamento de dispositivo móvel.

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 habilitar o servidor Syslog, clique em **Mais** > **Configurações** > **Syslog** > **Habilitar envio Syslog**.

Todos os relatórios exportados estão disponíveis para usuários Syslog sem limitações.

2. 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.

Para ativar o servidor Syslog:

1. Clique em **Mais** > **Configurações** > **Syslog** e clique na alternância ao lado de **Ativar envio Syslog**.

2. Especifique as configurações obrigatórias a seguir:

   a. **Formato da carga**: – JSON, LEEF ou CEF

   b. **Formato do envelope** do relatório – **BSD** (especificação), **Syslog** (especificação)

   c. **Nível de relatório mínimo** – **informações**, **aviso**, **erro** ou **crítico**

   d. **Tipo de evento de relatórios** – selecione o tipo de relatórios que deseja incluir (**Antivírus**, **HIPS**, **Firewall**, **Proteção da web**, **Relatório de auditoria**, **Arquivos bloqueados Alertas do ESET Inspect**).

   e. **IP de destino ou FQDN do servidor syslog compatível com TLS** – endereço IPv4 ou nome de host do

destino para mensagens Syslog

f.**Validar certificados raiz CA de conexões TLS** – clique na alternância se quiser ativar a validação de certificado para a conexão entre seu servidor Syslog e o ESET PROTECT. Depois que a validação estiver ativada um novo campo de texto será exibido, onde você poderá copiar e colar a cadeia de certificado necessária. O certificado do servidor deve atender aos requisitos a seguir:

- Toda a cadeia de certificado no formato PEM é carregada e salva na configuração de exportação Syslog (isso inclui a CA raiz, já que não há certificados confiáveis internos)
- O certificado do seu servidor Syslog fornece extensão de Nome alternativo para o assunto (DNS=/IP=), onde qual pelo menos um registro corresponde à configuração do nome de host FQDN/IP.

> Você precisa da autoridade de certificação versão 3 (e posterior) com a extensão de certificado Restrições Básicas para ser aprovado na validação.
> A validação de conexões TLS é aplicável apenas aos certificados. Desativar a validação não afeta as configurações TLS do ESET PROTECT.

Depois de fazer as alterações aplicáveis, clique em **Aplicar configurações**. A configuração entra em vigor em 10 minutos.

> 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.

Restrições de segurança e limites Syslog

Devido aos requisitos de segurança para conexão com o servidor Syslog, as configurações a seguir são fixas e não podem ser alteradas:

- Protocolo de transporte: TLS
- Porta TCP: 6514

Pelas mesmas razões, existem requisitos adicionais no servidor Syslog de recebimento:

- Endereço IP: Endereço IPv4 que pode ser roteado globalmente
- Nomes IDN: Deve usar representação ASCII ("xn--")
- FQDN: Deve traduzir para um endereço IPv4 fixo único.

> Usando FQDN
> Se o seu servidor Syslog operar sob vários computadores/endereços IP (CDN), não há garantia sobre quando e com que frequência o FQDN é solucionado novamente. Porém, garantimos que a primeira solução FQDN seja concluída em uma janela de 10 minutos depois da inicialização do servidor, desde que a exportação Syslog esteja ativada e configurada corretamente.

Configurações de segurança adicionais

O administrador deve configurar seu firewall do servidor Syslog para permitir a entrada de eventos de Exportação Syslog apenas dos seguintes intervalos de IP:

- Endereços IP de saída do ESET PROTECT na região da Europa: 51.136.106.164/30
- Endereços IP de saída do ESET PROTECT na região EUA: 40.81.8.148/30
- Endereços IP de saída do ESET PROTECT na região do Japão: 20.78.10.184/30

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.
hostname	string		Nome do host 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`
group_name	string		O caminho completo para o grupo estático do computador gerando o evento. Se o caminho for maior que 255 caracteres o group_name vai ter apenas o nome do grupo estático.
group_description	string		Descrição do grupo estático.
os_name	string		Informações sobre o sistema operacional do computador.

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_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": "All/Lost & found",
    "os_name": "Microsoft Windows 11 Pro",
    "group_description": "Lost & found static group",
    "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 a replicação de Agente ESET Management/Servidor ESET PROTECT. 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

event	string	opcional	Nome do evento
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 Servidor ESET PROTECT e o Agente ESET Management gerente
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": "All/Lost & found",
     "os_name": "Microsoft Windows 11 Pro",
     "group_description": "Lost & found static group",
 "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 Servidor ESET PROTECT e o Agente ESET Management gerente
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": "All/Lost & found",
    "os_name": "Microsoft Windows 11 Pro",
    "group_description": "Lost & found static group",
    "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\\ja
va.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": "All/Lost & found",
        "os_name": "Microsoft Windows 11 Pro",
        "group_description": "Lost & found static group",
        "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:

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": "All/Lost & found",
     "os_name": "Microsoft Windows 11 Pro",
     "group_description": "Lost & found static group",
 "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": "All/Lost & found",
     "os_name": "Microsoft Windows 11 Pro",
     "group_description": "Lost & found static group",
 "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:

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 caminho completo para o grupo estático do computador gerando o evento. Se o caminho for maior que 255 caracteres o deviceGroupName vai ter apenas o nome do grupo estático. O atributo deviceOSName contém informações sobre o sistema operacional do computador, e o atributo deviceGroupDescription contém a descrição do grupo estático.

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	ProtectCloud	
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 • 2 – Informações • 3 – Aviso • 5 – Alerta • 7 – Erro • 8 – Crítico • 10 – Fatal

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.
rt	Jun 04 2017 14:10:0	Hora UTC de ocorrência do evento. O formato é %b %d %Y %H:%M:%S
ESETProtectDeviceGroupName	All/Lost & found	O caminho completo para o grupo estático do computador gerando o evento. Se o caminho for maior que 255 caracteres o ESETProtectDeviceGroupName vai ter apenas o nome do grupo estático.
ESETProtectDeviceOsName	Microsoft Windows 11 Pro	Informações sobre o sistema operacional do computador.
ESETProtectDeviceGroupDescription	Lost & found static group	Descrição do grupo estático.

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	

Nome da extensão	Exemplo	Descrição
cs4	Real-time file system protection	ID do Scanner
cs4Label	Scanner ID	
cs5	virlog.dat	ID de rastreamento
cs5Label	Scan ID	
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

Nome da extensão	Exemplo	Descrição
sprod	C:\\7-Zip\\7z.exe	O nome do processo de origem do evento
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

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 ESETProtectDeviceGroupName=All/Lost & found ESETProtectDeviceOsName=Microsoft Windows 11 Pro ESETProtectDeviceGroupDescription=Lost & found static group 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	

Nome da extensão	Exemplo	Descrição
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)
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 ESETProtectDeviceGroupName=All/Lost & found ESETProtectDeviceOsName=Microsoft Windows 11 Pro ESETProtectDeviceGroupDescription=Lost & found static group 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	

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

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 ESETProtectDeviceGroupName=All/Lost & found ESETProtectDeviceOsName=Microsoft Windows 11 Pro ESETProtectDeviceGroupDescription=Lost & found static group 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	

Nome da extensão	Exemplo	Descrição
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	
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 ESETProtectDeviceGroupName=All/Lost & found
ESETProtectDeviceOsName=Microsoft Windows 11 Pro ESETProtectDeviceGroupDescription=Lost & found static
group 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

Nome da extensão	Exemplo	Descrição
cs2	Blocked by Administrator	Causa
cs2Label	Cause	

Exemplo de relatório CEF de evento de arquivos bloqueados:

```
CEF:0|ESET|Protect|10.0.0.0|600|Blocked File Event|5|dvchost=test_lrghlbjyoa
deviceExternalId=432a30af-6ac7-4b61-ae5c-5141bfc5d878 ESETProtectDeviceGroupName=All/Lost & found
ESETProtectDeviceOsName=Microsoft Windows 11 Pro ESETProtectDeviceGroupDescription=Lost & found static
group 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:0|ESET|Protect|10.0.0.0|716|Filtered Website Event|5|dvchost=test_lrghlbjyoa
deviceExternalId=432a30af-6ac7-4b61-ae5c-5141bfc5d878 ESETProtectDeviceGroupName=All/Lost & found
ESETProtectDeviceOsName=Microsoft Windows 11 Pro ESETProtectDeviceGroupDescription=Lost & found static
group 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
```

ESET PROTECT para Provedores de serviço gerenciados

Quem é um MSP

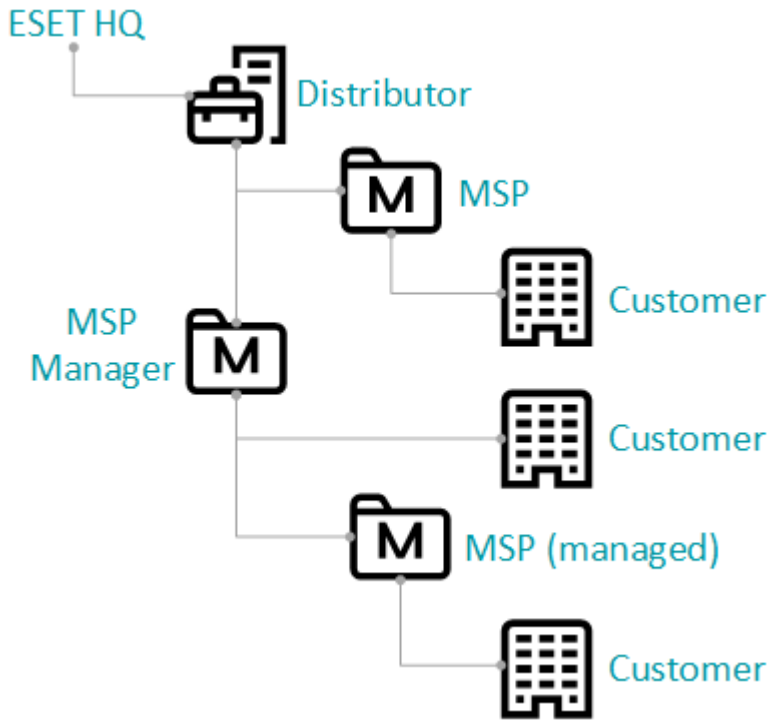
A abreviação MSP significa "Managed Service Provider", "Provedor de Serviço Gerenciado". Os usuários MSP geralmente fornecem serviços de TI a seus clientes, por exemplo, o gerenciamento de produtos de segurança (por exemplo, ESET Endpoint Antivirus).

- 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. O cliente pode ter status diferentes marcados por um ícone:

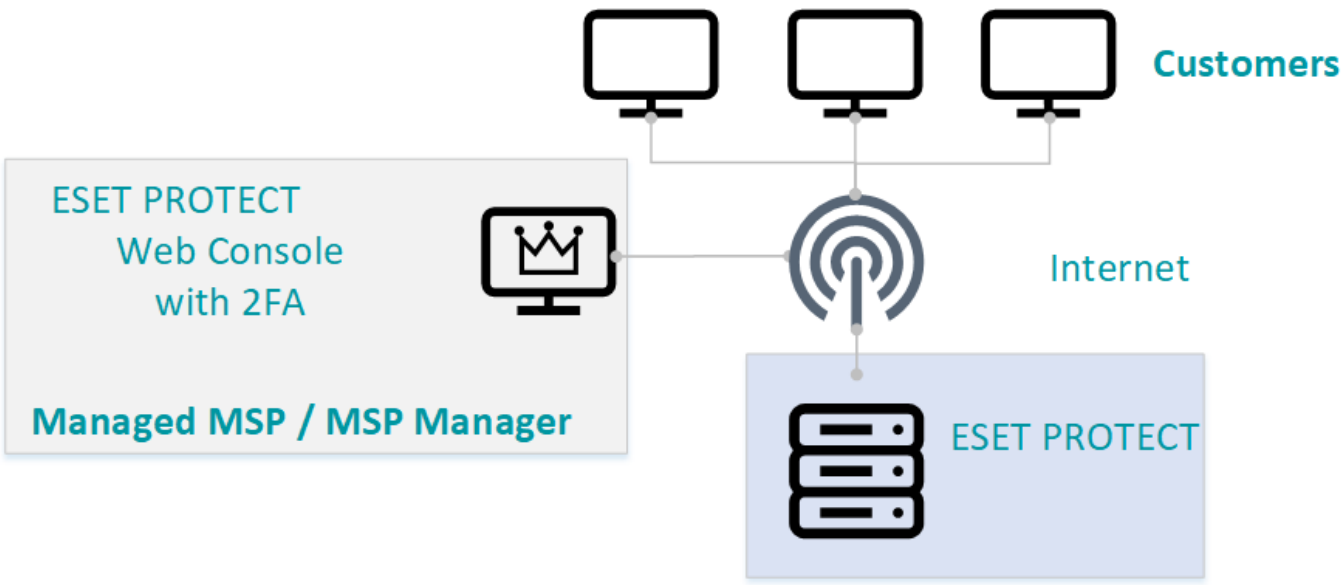
- – o cliente ainda não foi configurado.
- – o cliente foi configurado ou você ignorou a configuração do cliente.
- – O cliente foi removido.

> Depois de sincronizar a conta MSP, o usuário MSP pode ver a lista de clientes gerenciados na seção Clientes gerenciados no menu principal do ESET PROTECT.

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. Os Agentes ESET Management instalados nos computadores dos clientes precisam ter conectividade com o ESET PROTECT por meio da Internet pública. Certifique-se de abrir determinadas portas para tornar o ESET PROTECT visível.

A configuração padrão do MSP tem a estrutura a seguir:



ESET PROTECT implantado de uma conta mista

Uma conta mista usa as mesmas credenciais para acessar o ESET Business Account e o ESET MSP Administrator. Nesse caso, você pode criar o ESET PROTECT a partir de cada uma delas. Depois da criação da instância, você pode acessar a mesma instância de ambos os serviços (EMA 2 e EBA). O direito de remover a instância ESET PROTECT é reservado para o serviço que criou a instância.

Recursos do ESET PROTECT para usuários MSP

O ESET PROTECT oferece um conjunto de recursos focados nos usuários MSP. Os recursos do MSP estão disponíveis para usuários que implantaram a instância ESET PROTECT de:

- Conta ESET MSP Administrator (EMA 2)

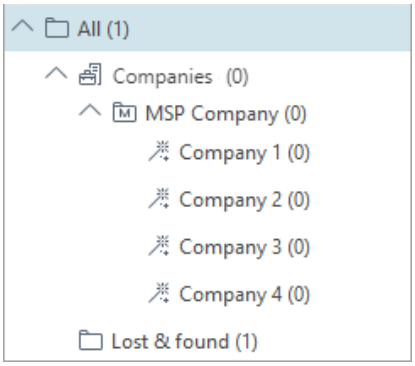
- ESET Business Account (EBA) enquanto tem uma conta EMA 2 sob as mesmas credenciais

Assistente de configuração do cliente

O recurso principal do MSP no ESET PROTECT é a configuração do cliente MSP. Esse recurso ajuda você a criar um instalador personalizado do Agente ESET Management para seu cliente.

Árvore MSP

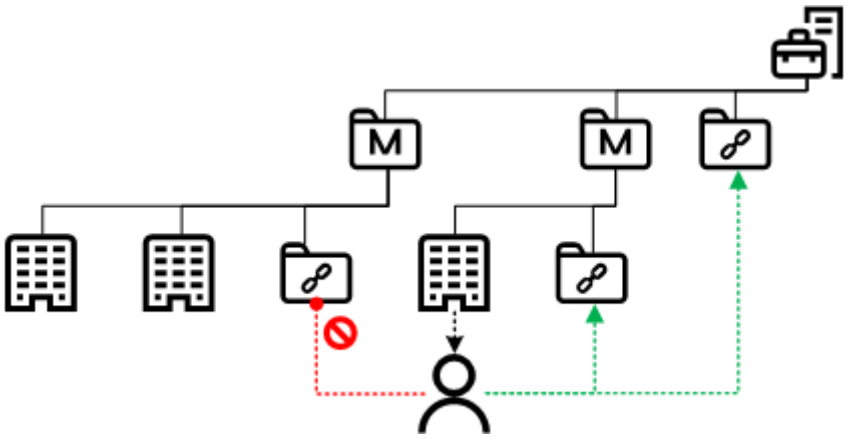
O ESET PROTECT sincroniza com o Portal ESET MSP (EMA 2) e cria a Árvore MSP. A Árvore MSP é uma estrutura no menu Computadores, que representa a estrutura das empresas na sua conta EMA 2. Os itens na Árvore MSP usam ícones diferentes dos dispositivos e grupos ESET PROTECT padrão. Não é possível modificar a estrutura da árvore MSP no Web Console.



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.



Clientes gerenciados

Depois de sincronizar a conta MSP, o usuário MSP pode ver a lista de clientes gerenciados na seção Clientes gerenciados no menu principal do ESET PROTECT.

MSP na Visão geral do status

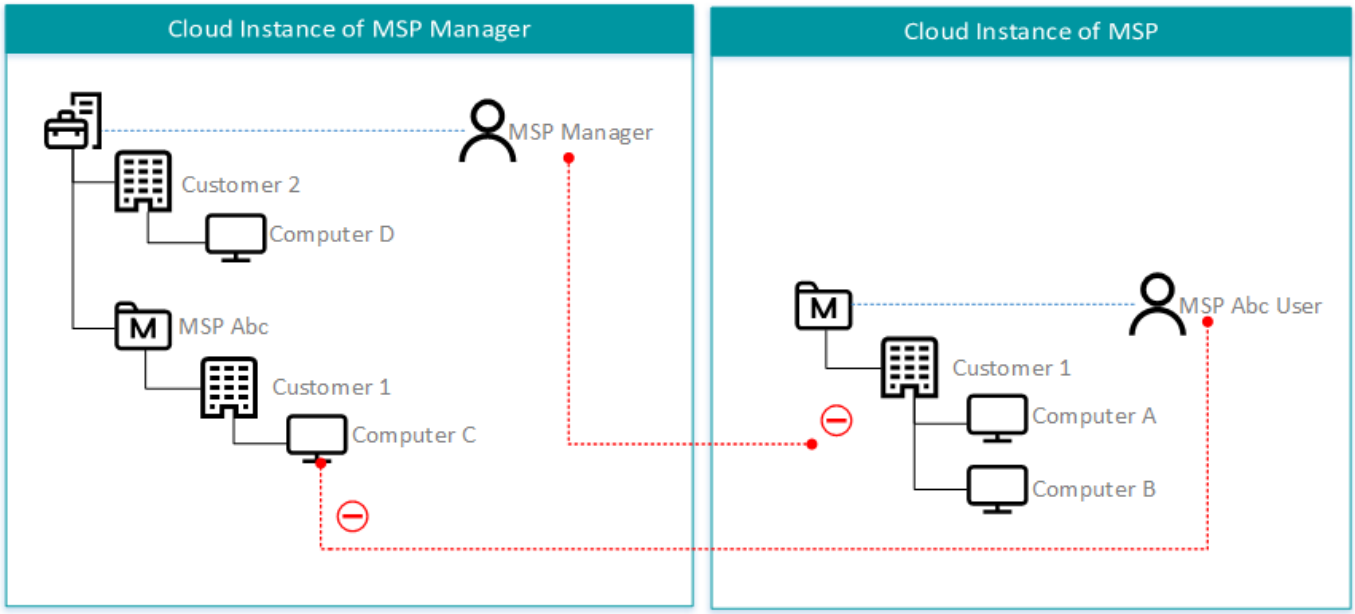
Você obtém acesso ao novo bloco MSP na Visão geral do status. O bloco MSP exibe informações básicas sobre sua conta.

Ter várias instâncias do ESET PROTECT em uma estrutura MSP

Se você usar a instância da nuvem implantada de uma conta MSP, ela é separada de outras instâncias MSP. A instância do seu Gerente MSP não está conectada. Eles compartilham a mesma estrutura da empresa (árvore MSP), mas não compartilham computadores ou outros objetos, como tarefas ou políticas. As licenças são a única exceção. Elas são compartilhados hierarquicamente, da mesma forma que no ESET MSP Administrator. O Gerente MSP pode acessar as licenças dentro do Web Console e atribuí-las a máquinas.

Veja o exemplo a seguir:

O usuário MSP não tem acesso a computadores na instância do Gerente MSP, mesmo se esses computadores estiverem no grupo estático dos clientes MSP. Isso acontece porque as instâncias da nuvem são separadas.



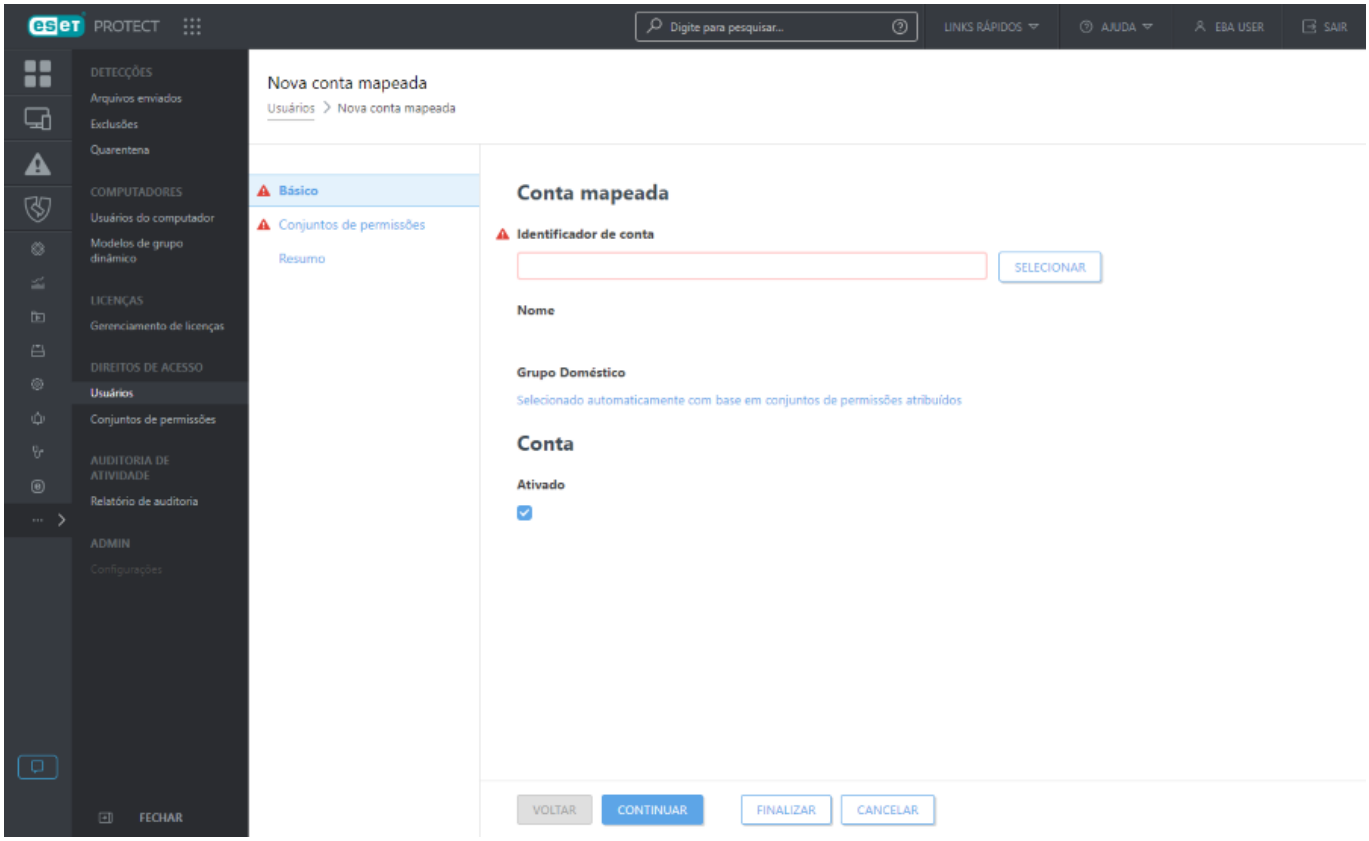
Criar um novo usuário ESET PROTECT no ESET MSP Administrator

Para criar um novo usuário para o Web Console ESET PROTECT, este usuário deve ser criado primeiro no ESET MSP Administrator (EMA 2). Consulte a Ajuda on-line do EMA 2 para um guia passo-a-passo. Você pode adicionar o novo usuário durante a configuração do cliente MSP ou seguindo as etapas abaixo.

- Veja como as permissões de usuário funcionam no EMA 2 e no ESET PROTECT na Ajuda on-line do EMA 2.
- Veja o guia passo a passo sobre como criar a instância ESET PROTECT.

1. Abrir o Console Web.

2. Navegue até **Usuários**.

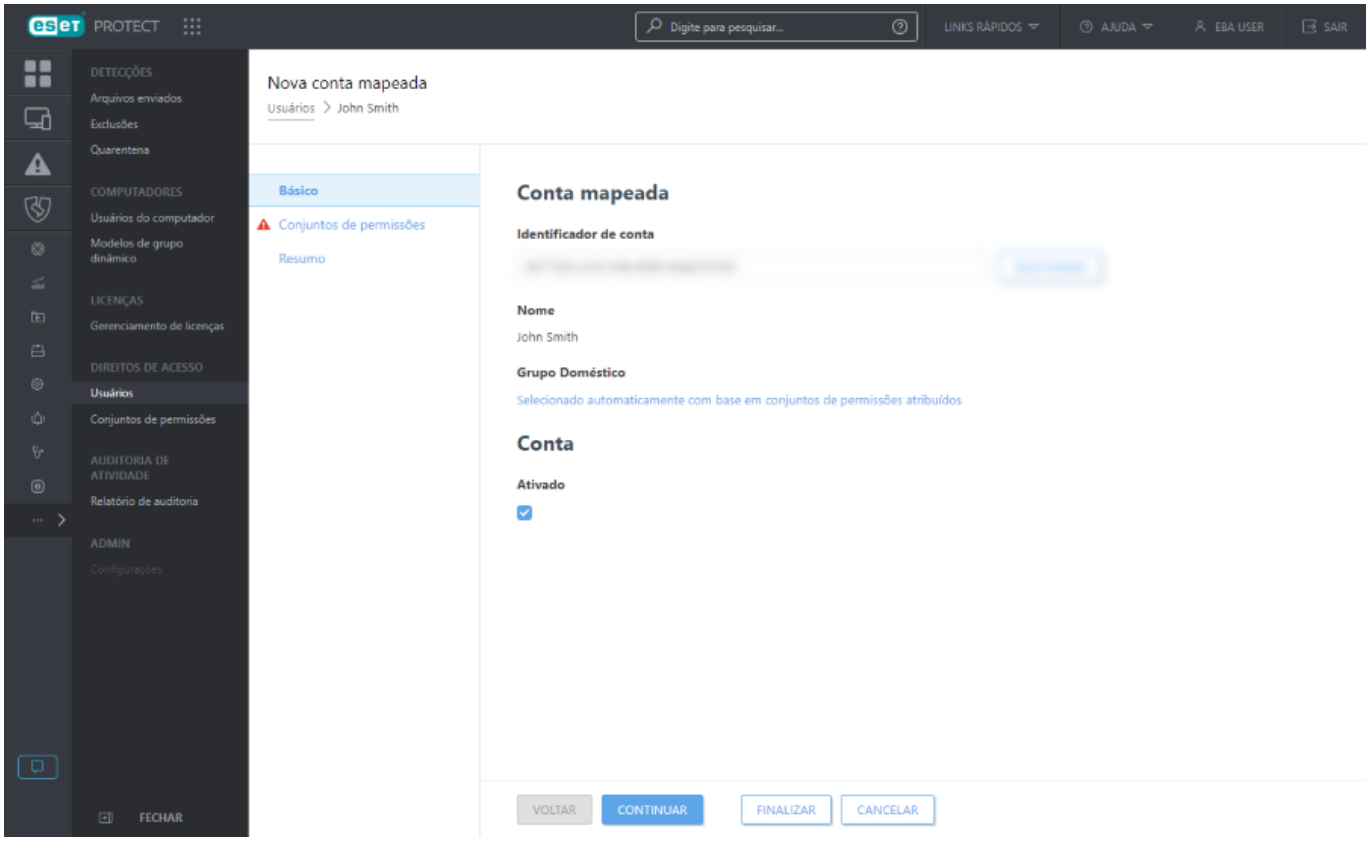


3. Clique em **Selecionar** ao lado do campo **Identificador de conta** e selecione o usuário que deseja ativar no ESET PROTECT.

4. Você pode adicionar marcas novas ou existentes ao usuário.

5. Clique em **Selecionar** ao lado do campo **Grupo doméstico**. O grupo doméstico é o grupo estático onde os objetos criados pelo usuário são armazenados por padrão.

6. Clique em **Conjuntos de permissões**.



7. Selecione um conjunto de permissões para o novo usuário. Um conjunto de permissões determina os direitos de acesso do usuário. Cada conjunto de permissões dá ao usuário direitos em um determinado grupo estático. Os grupos são definidos em cada conjunto de permissões. Um usuário pode ser atribuído a um ou vários conjuntos. Você pode selecionar um dos conjuntos de permissões oferecidos ou criar um novo.

> **Conjunto de permissões do grupo doméstico**
> Adicione conjuntos de permissões ao grupo doméstico selecionado para o usuário. Sem os direitos de acesso ao grupo doméstico, o usuário não pode acessar ou criar objetos no grupo doméstico.

8. Clique em **Concluir** para salvar as alterações.

O novo usuário agora pode entrar no Web Console ESET PROTECT usando suas credenciais EMA 2.

Processo de implantação para MSP

1. Conclua a Configuração do cliente MSP. Quando solicitado, selecione o instalador **Apenas Agente**.
2. Distribua e instale o instalador do Agente ESET Management de maneira local ou remota.
3. 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 (*.exe* para Windows ou *.sh* para Linux) contém todas as informações necessárias para uma máquina cliente fazer o download e instalar o Agente ESET Management. Certifique-se de que a máquina Linux 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 (*.exe* para Windows ou *.sh* para Linux) contém todas as informações necessárias para uma máquina cliente fazer o download e instalar o Agente ESET Management. Certifique-se de que a máquina Linux 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 instalador.

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

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.

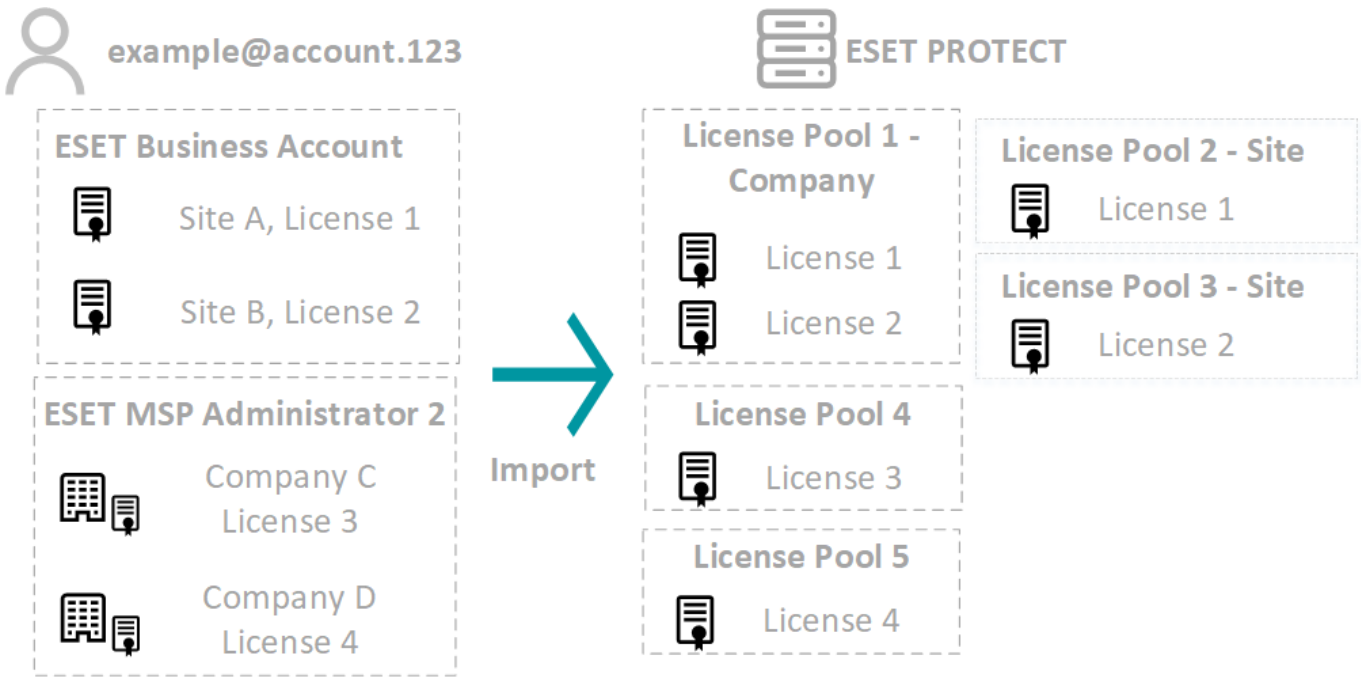
• Se houver uma empresa em sua estrutura MSP que não possua licenças no momento da sincronização, ela será sincronizada apenas com a Árvore MSP do computador, e não com a Árvore MSP dentro do Gerenciamento de licenças.

• 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.

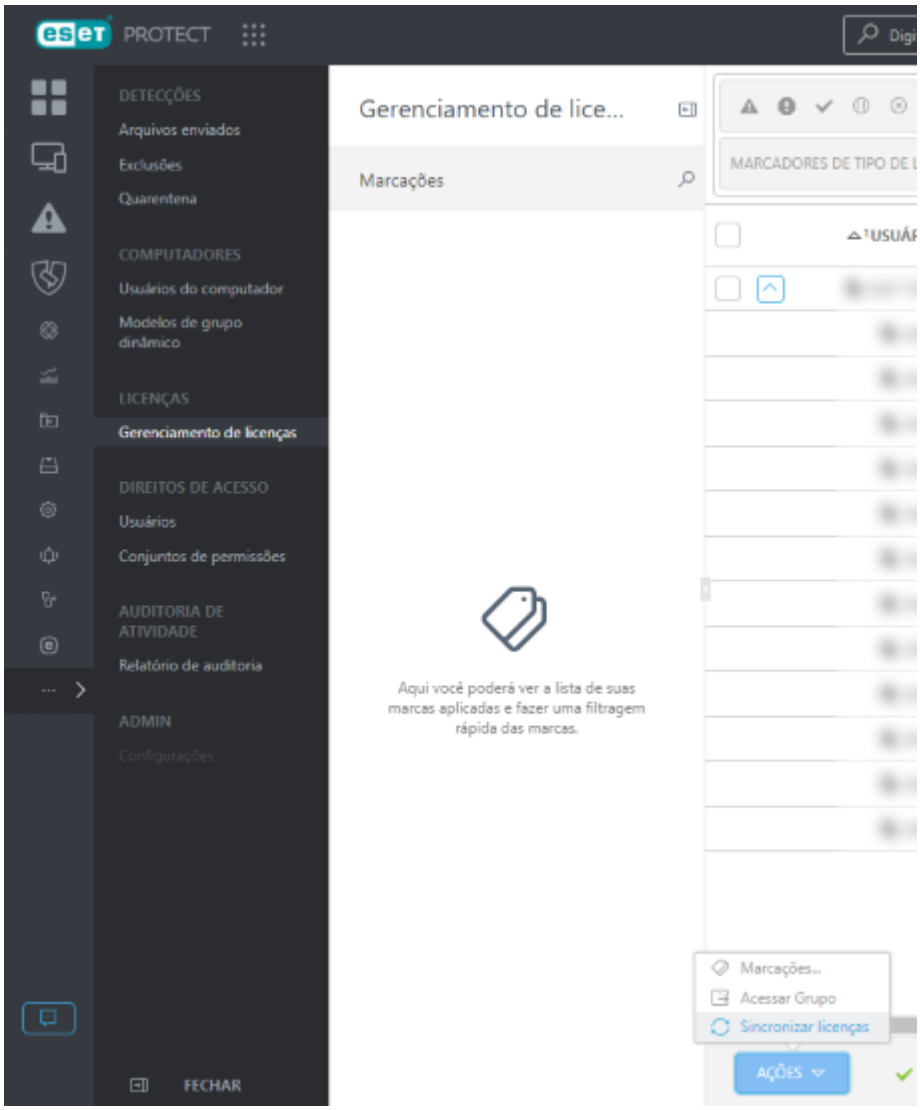
• Você pode encontrar nomes de empresa e sites na coluna **Usuário da licença** no Gerenciamento de licenças. Você pode usar os dados do **Usuário da licença** ao criar um relatório.

• 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.



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**.



Iniciar configuração do cliente MSP

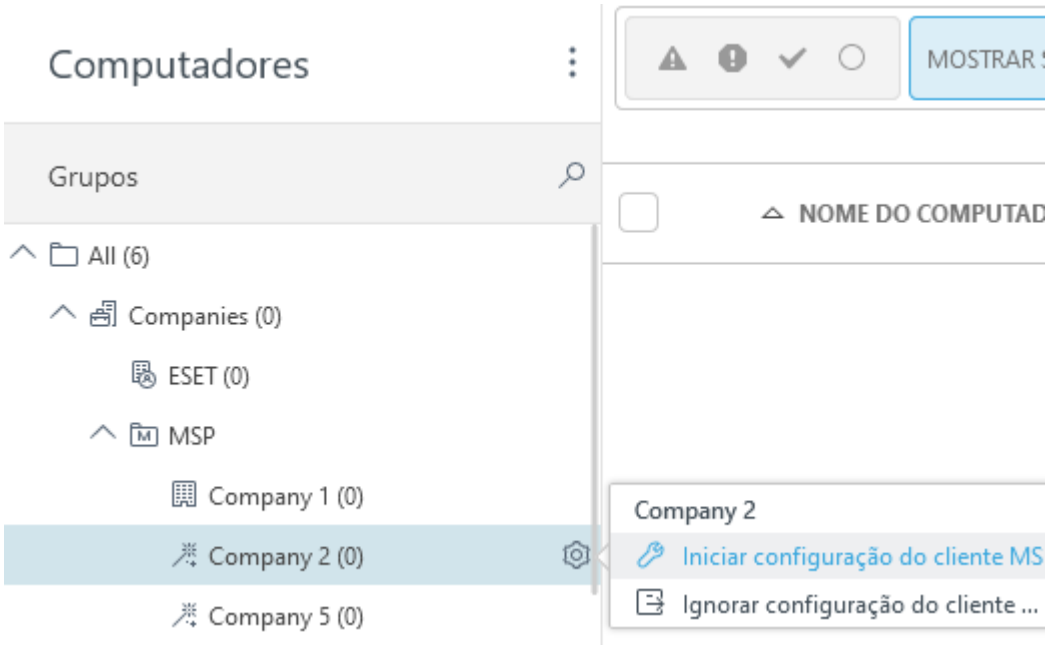
Depois de criar sua instância ESET PROTECT usando uma conta MSP, a árvore MSP é sincronizada e você pode começar a configurar empresas. A configuração do cliente MSP cria:

- 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.

Você também pode ignorar a configuração do cliente MSP, mas recomendamos que a instalação do MSP seja concluída.

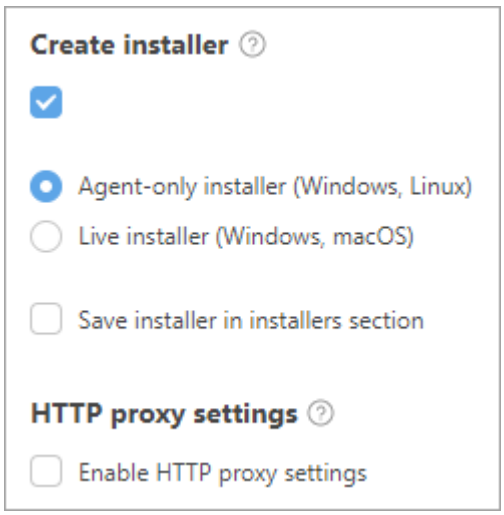
Você pode configurar apenas uma empresa com pelo menos 1 unidade de licença válida.

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 (Windows, Linux)**.
- **Instalador tudo-em-um (Windows, MacOS)** – o instalador é constituído pelo Agente ESET Management e pelo produto de segurança ESET Business selecionado.

Instalador tudo-em-um (Windows, macOS)

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 **Eu aceito o Acordo de licença de usuário final 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**.

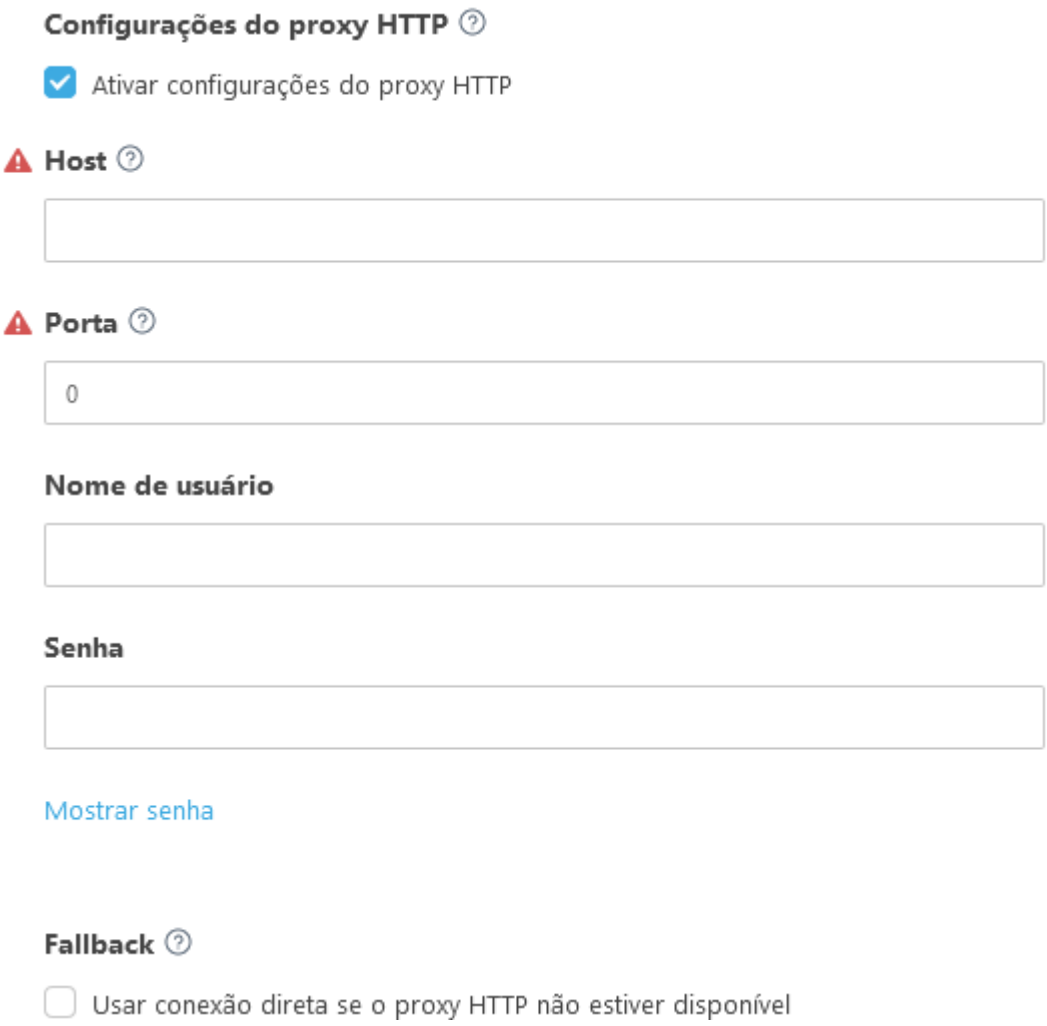
Ativar configurações do proxy http

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 Servidor ESET PROTECT. O campo **Host** é o endereço da máquina que executa 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 Servidor ESET PROTECT não é compatível com a autenticação. Qualquer solução de proxy usada para encaminhar a comunicação do Agente para o Servidor ESET PROTECT e que precise de autenticação não funcionará.

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 desabilitar a configuração usando uma Política de AgenteESET Management:

- Durante a criação do instalador – inclua a política na **Configuração inicial**.
- Depois da instalação do Agente ESET Management – atribua a política ao computador.



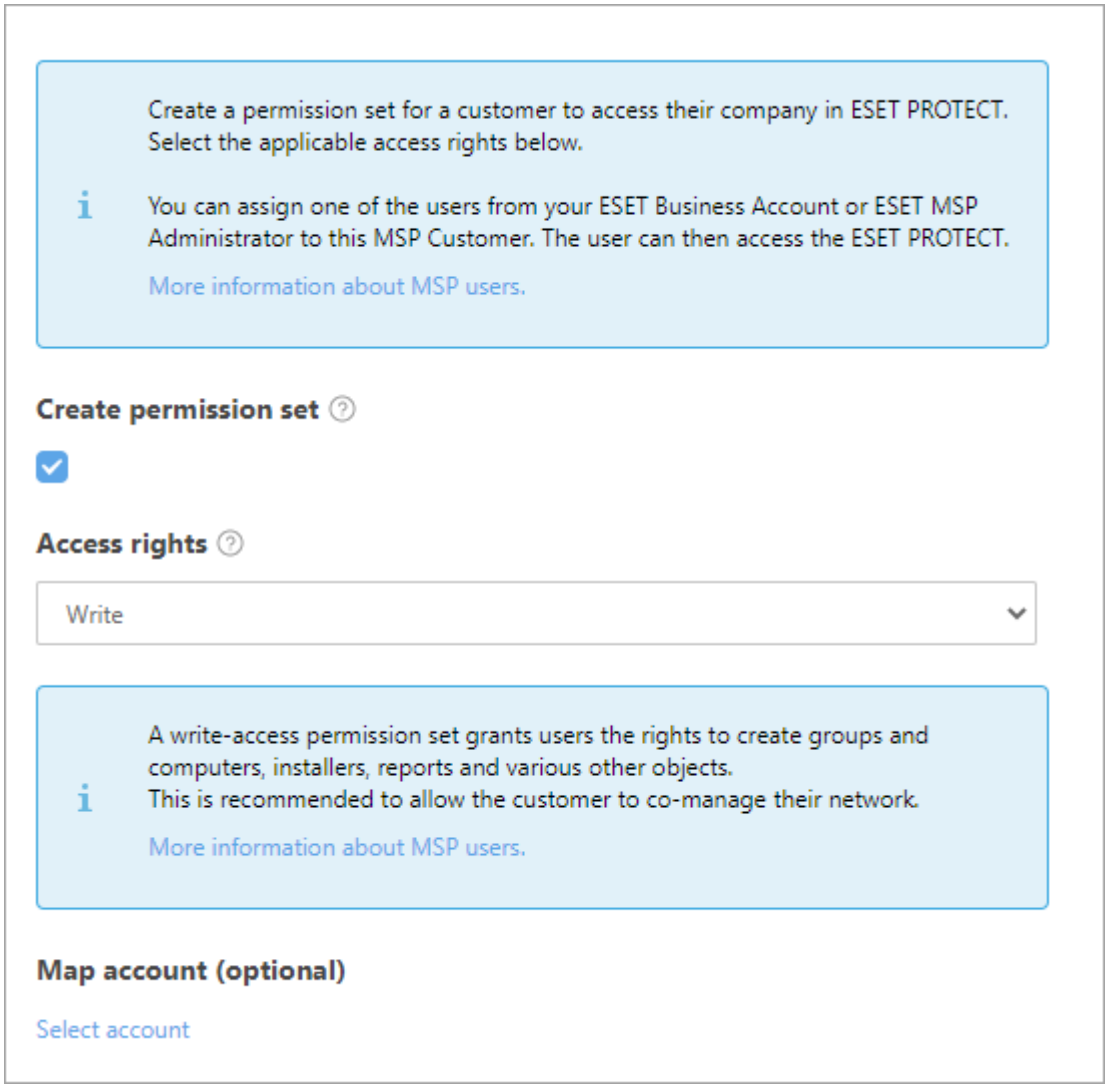
5. Clique em **Continuar** para ir para a seção **Usuário**.

6. Você pode selecionar um usuário do seu EMA 2 e deixar o usuário gerenciar o ESET PROTECT.

a) Selecione a caixa de seleção em **Criar conjunto de permissões**.

b) **Direitos de acesso** – O usuário pode entrar no console web e gerenciar os dispositivos da empresa. Selecione o nível de direitos de acesso **Leitura** ou **Gravação**.

c)**Mapear conta (opcional)** – clique em **Selecionar conta** e mapeie uma das contas disponíveis.



Problemas para criar um usuário? Certifique-se de ter as permissões necessárias.

Clique em **Concluir** para preparar os instaladores. Você também pode fazer novamente o download o instalador no menu Instaladores, se tiver selecionado salvar o instalador.Você pode distribuir o pacote Live Installer de várias formas:

- Clique em para copiar o link de download do pacote Live Installer, distribuir o link para os usuários e deixá-los fazer download e instalar o pacote Live Installer.

- Você também pode **Fazer download** do pacote Live Installer e distribuí-lo pessoalmente, ou carregá-lo para um local compartilhado para acesso dos usuários.

- Apenas Windows Use o Remote Deployment Tool para implantar remotamente o pacote Live Installer.

- Clique em para usar o servidor SMTP ESET PROTECT para entregar uma mensagem de e-mail com o link de download do pacote Live Installer para usuários especificados.

  - Para adicionar um usuário, clique em **Adicionar** > preencha o campo **Endereço de e-mail** > pressione **Enter** ou clique em . Opcionalmente, clique em **Criar usuário** > digite o **Nome** do usuário > clique em **Salvar**. Você pode editar detalhes do usuário nos Usuários do computador. Clique em **Ver visualização de e-mail**, selecione o **Idioma do e-mail** no menu suspenso e clique em **Salvar**.

- 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).

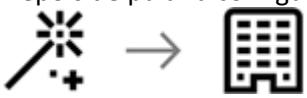
Depois de ser criado, o Live Installer vai se comportar de acordo com esta tabela.
O Live Installer requer uma conexão com a internet e não funciona em um computador off-line.
O Live Installer no macOS requer uma conexão com a internet direta (para conectar aos servidores ESET) e não funciona em um computador macOS conectado à internet via Proxy sem conexão direta com a internet.

Leia como implantar o Agente ESET Management de maneira local ou remota.

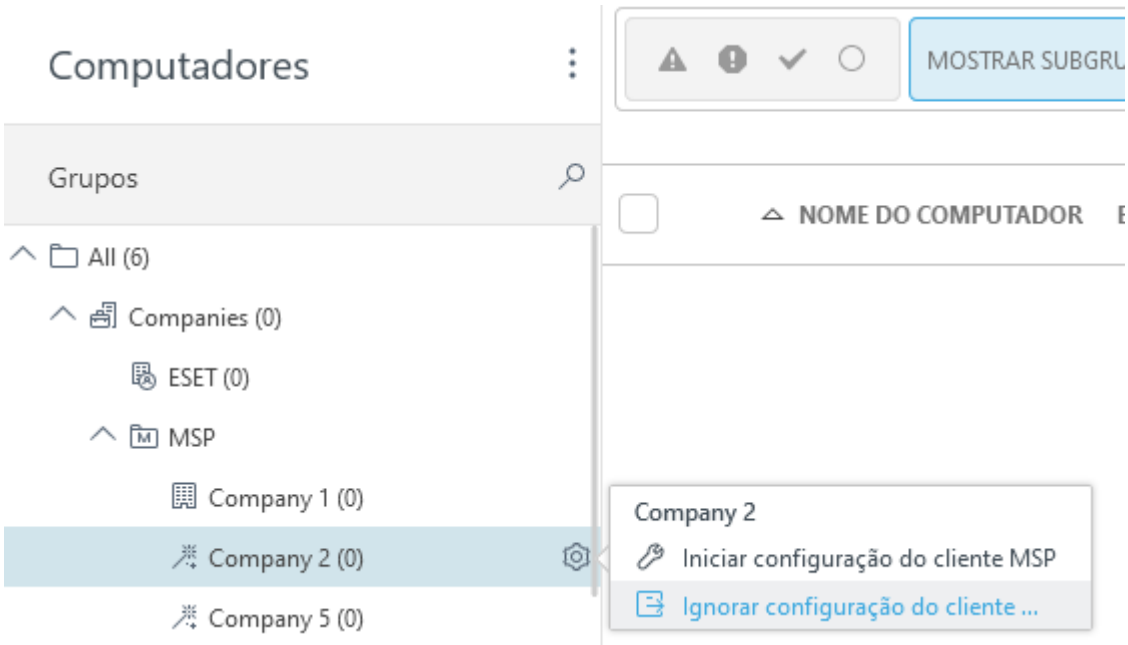
Ignorar configuração do cliente MSP

Você pode **Ignorar a configuração do cliente MSP** se não desejar configurá-la. Opcionalmente, você pode criar um instalador mais tarde. Não recomendamos ignorar a configuração.

Depois de pular a configuração, o ícone da empresa será alterado como se tivesse sido configurado:



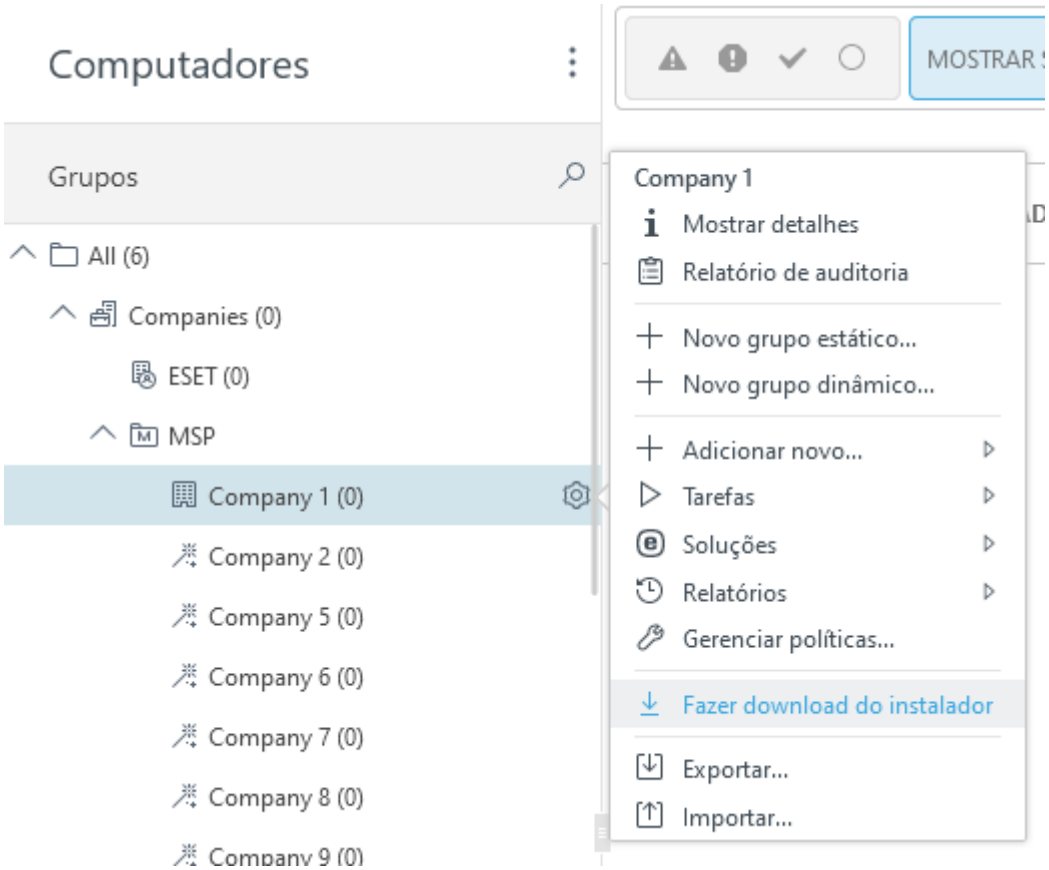
Se você ignorar a configuração, não poderá executar o assistente de configuração para a empresa novamente na mesma instância do ESET PROTECT.



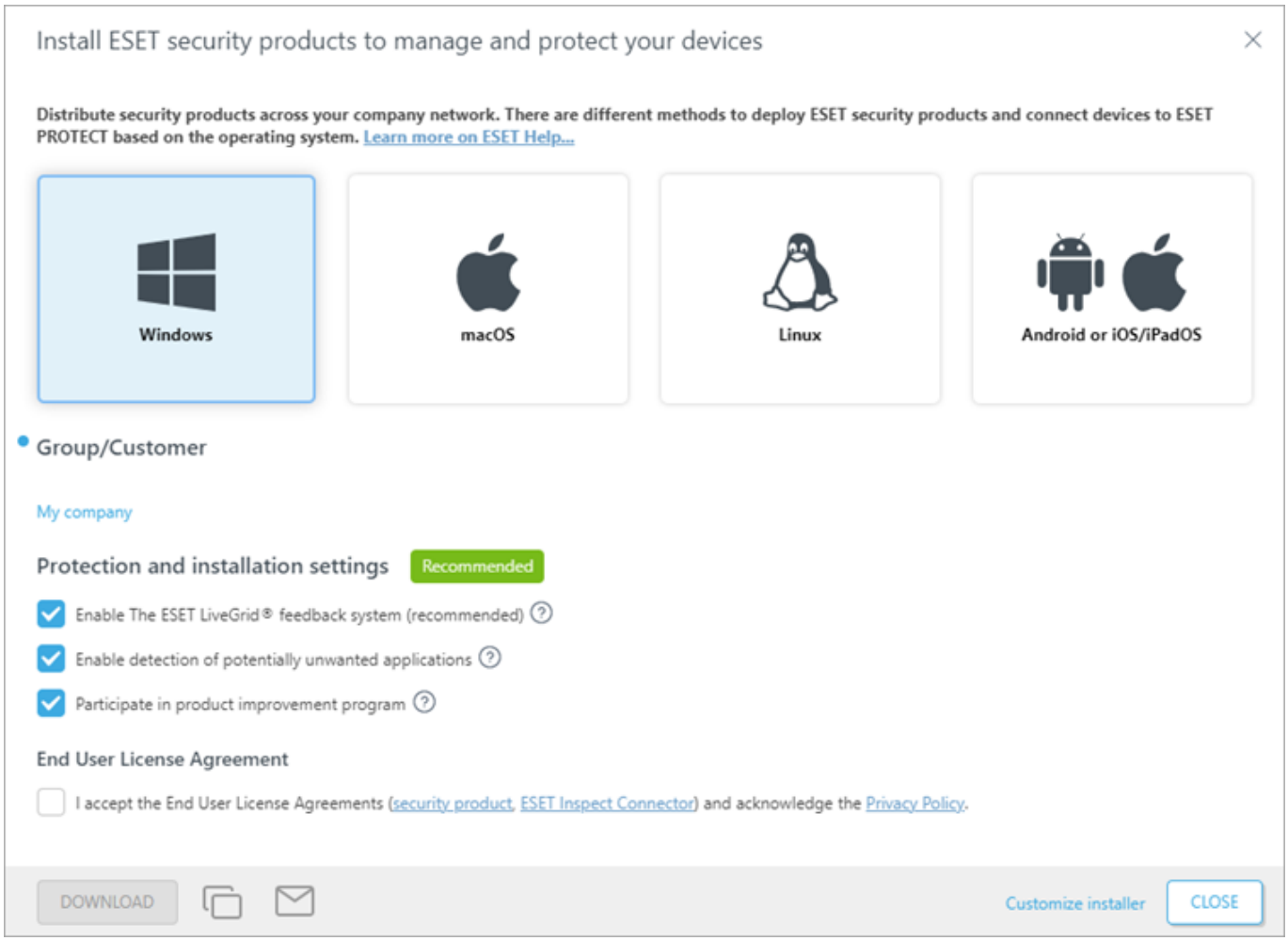
Criar instalador personalizado

1. No console web, 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. Crie e personalize o instalador e faça o download dele.



Usuários MSP

Durante a configuração de um cliente MSP, você pode adicionar um usuário existente do EMA2 ou do EBA ao ESET PROTECT. Para revisar e editar o usuário navegue até o menu **Mais** > **Direitos de acesso** > **Usuários**.

Permissões necessárias

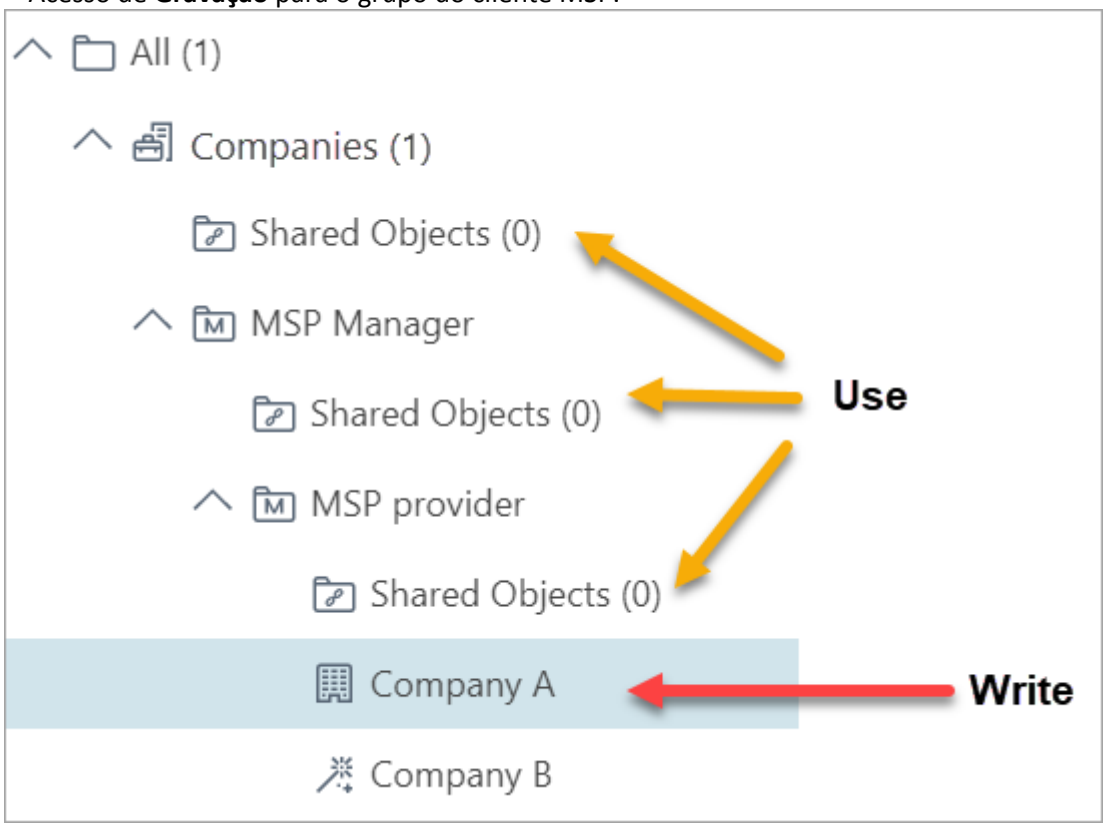
Para criar o novo usuário na configuração do cliente MSP, você precisará ter direitos de acesso para a empresa configurada e para os grupos de **Objetos compartilhados**.

Esquema de permissão detalhado

Configurar uma única empresa

Direitos de acesso necessários para criar um usuário durante a configuração da *Empresa A*:

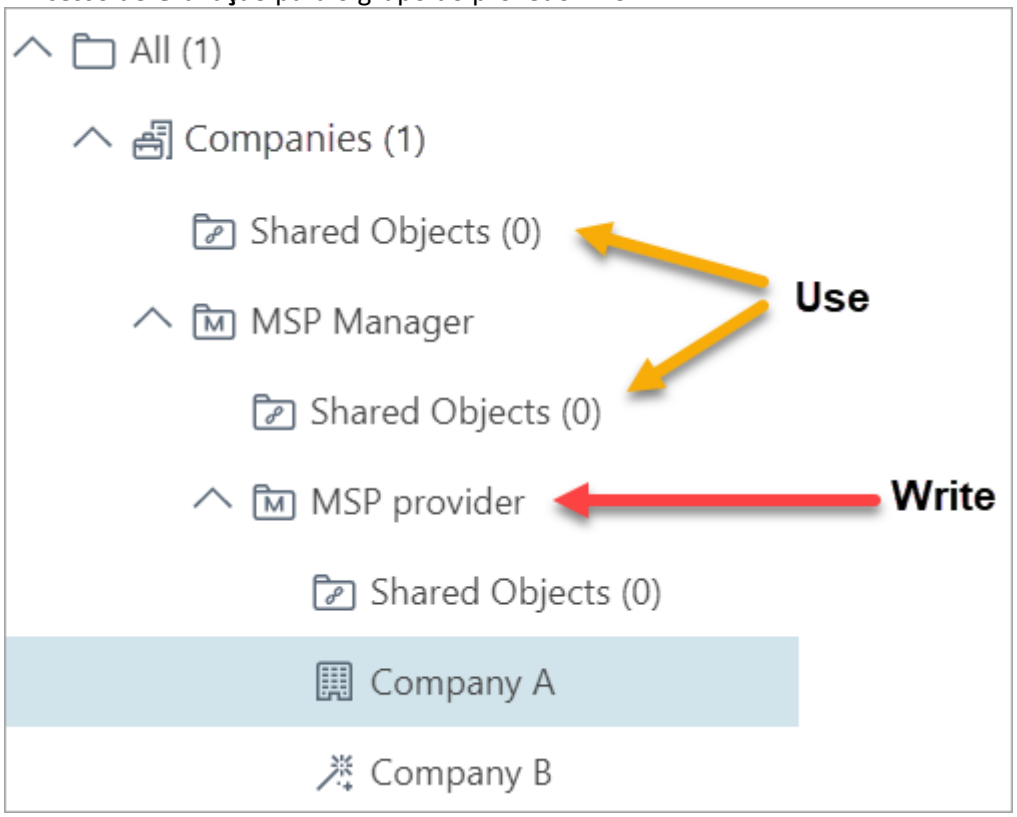
- Acesso de **Uso** para todos os grupos de **Objetos compartilhados**.
- Acesso de **Gravação** para o grupo do cliente MSP.



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.

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**.

Marcação de objetos MSP

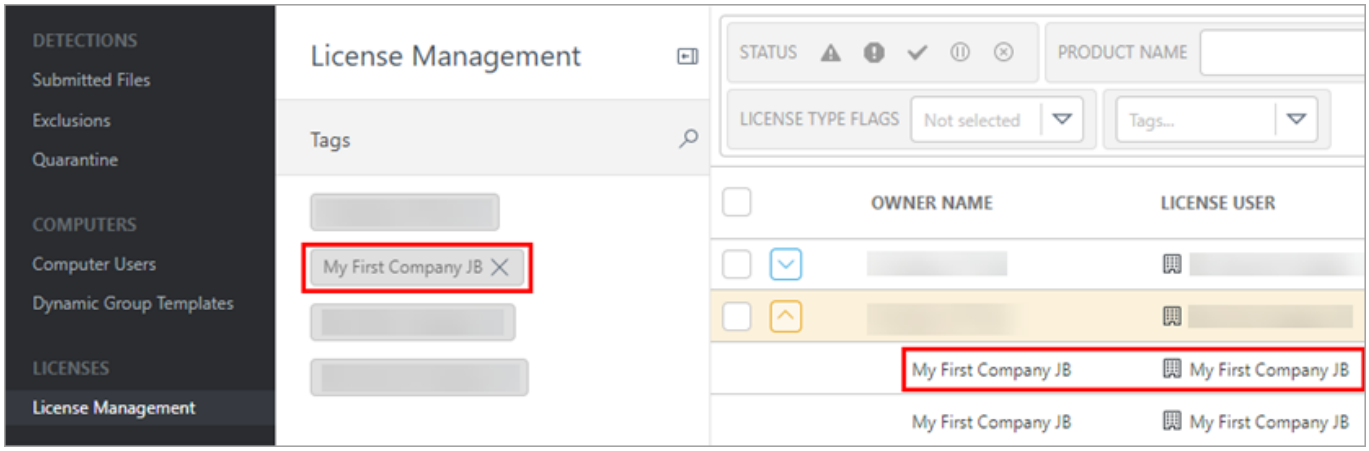
Se você usar o ESET PROTECT com uma conta EMA 2, habilitará a marcação automática de objetos MSP. Os seguintes objetos são marcados automaticamente:

- 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**.



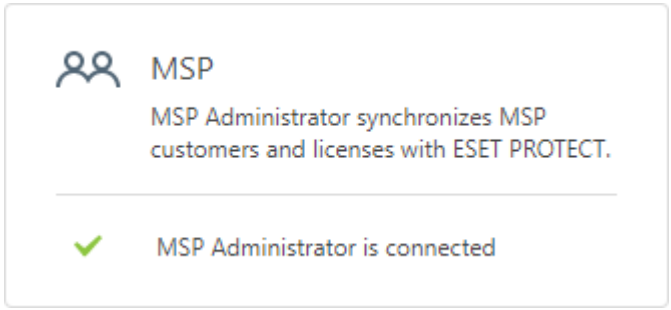
Visão geral do status MSP

A seção Visão geral do status fornece informações complexas sobre o seu status do ESET PROTECT. Se você criar sua instância ESET PROTECT usando uma conta EMA 2 ou mista (EMA 2 e EBA), existe um bloco MSP disponível com informações relacionadas ao MSP.

Status MSP

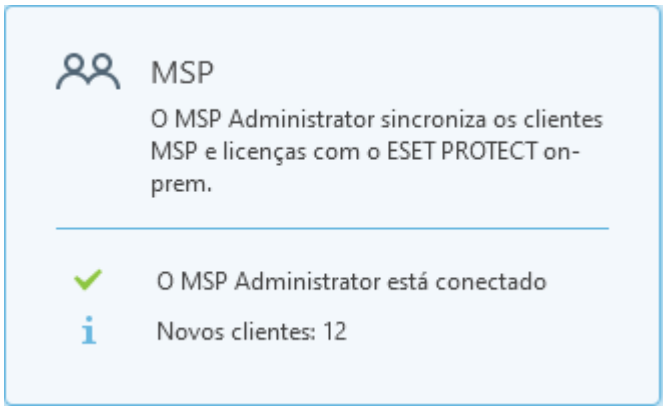
Conta sincronizada

Sua conta está sincronizada e nenhuma ação é necessária.



Sincronização em andamento

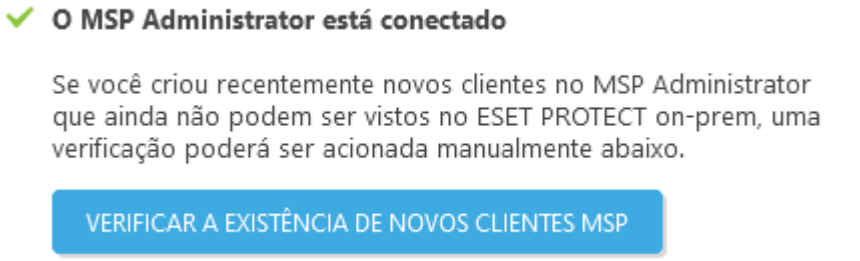
Há uma sincronização em andamento da conta MSP sendo executada em segundo plano. A sincronização pode levar várias horas para contas grandes. O bloco ficará branco após a sincronização.



Ações disponíveis

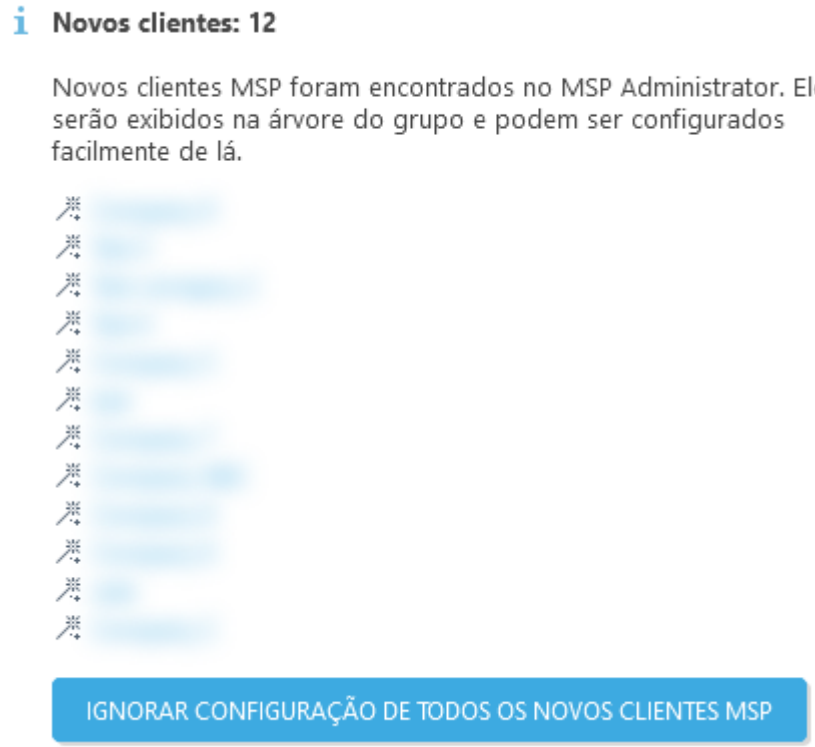
Clique no bloco MSP para ver mais detalhes.

- **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.



Gestão de dispositivo móvel de nuvem

O ESET Cloud Mobile Device Management (Cloud MDM) é um recurso complementar nativo do ESET PROTECT. O ESET Cloud MDM fornece gerenciamento de dispositivo móvel Android e iOS e administração de segurança móvel.

O ESET Cloud MDM fornece uma solução sem agente onde o Agente de gerenciamento não está sendo executado diretamente no dispositivo móvel (para economizar bateria e desempenho do dispositivo móvel). Em vez disso, o agente de gerenciamento para o dispositivo móvel é virtualizado na nuvem da ESET.

Todo o gerenciamento de certificado de segurança e conexão é gerenciado pela ESET, então o administrador não precisa se preocupar com o processo de renovação de certificado ou se os certificados estão ativos para os padrões de segurança mais recentes.

Verifique se a versão do sistema operacional do seu dispositivo móvel é compatível com o gerenciamento Cloud MDM e se você atende aos requisitos de rede.

> Os dispositivos móveis inscritos devem se conectar ao ESET PROTECT a cada 120 dias para evitar problemas de conexão. Você pode ver essas informações no link do e-mail de inscrição ou no código QR.
> Não inscreva um dispositivo sobressalente com antecedência. Recomendamos inscrever apenas um dispositivo sobressalente que será usado dentro de 120 dias.

O processo de gerenciamento de dispositivo móvel é composto pelas partes a seguir:

- Inscrição de dispositivo móvel – com base no tipo de dispositivos móveis que você planeja gerenciar e em que modo, você deve concluir diferentes etapas antes de começar a gerenciar os dispositivos móveis. O Cloud MDM é compatível com estes tipos de inscrições de dispositivos móveis:
  - Inscrição Android
  - Inscrição do proprietário do dispositivo Android
  - Inscrição do Microsoft Entra ID (Android ou iOS)
  - Sincronização do Microsoft Intune (Android)
  - Sincronização do VMware Workspace ONE (Android)
  - Inscrição iOS
  - Sincronização de Apple Business Manager (ABM) (iOS)
- Gerenciamento de dispositivos móveis – depois de inscrever seus dispositivos móveis Android, você pode começar a gerenciá-los.

Inscrição – adicionar dispositivos móveis

Para gerenciar um dispositivo móvel, inscreva o dispositivo no console web de nuvem clicando em **Computadores** > **Adicionar dispositivo** > **Android ou iOS/iPadOS**.

Acordo de Licença para o Usuário Final – selecione a caixa de seleção se você aceitar o Acordo de Licença para o Usuário Final e a Política de privacidade.

a)Clique em **Inscrever com código QR** para gerar o código QR de inscrição:

1.Na nova janela especifique o **Nome do dispositivo** para o novo dispositivo móvel que você deseja inscrever e clique em **Gerar código QR**.

2.Escaneie o código QR exibido com o dispositivo móvel que você deseja inscrever.

3.Depois da inscrição bem sucedida do dispositivo móvel selecionado, clique em **Inscrever o próximo** para gerar outro código QR para outro dispositivo móvel ou clique em **Fechar** quando tiver concluído a inscrição de dispositivos móveis.

b)Clique em ✉ para abrir a janela **Inscrever um dispositivo móvel por e-mail**:

Especifique os dispositivos móveis para inscrição, você pode usar as seguintes funções para adicionar dispositivos móveis:

- **Adicionar** – entrada única – você deve digitar manualmente um nome de dispositivo e um endereço de e-mail associado ao dispositivo móvel. (No caso de entrega de e-mail, o e-mail de inscrição será enviado para este endereço.) 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 em **Mais** > Usuários do computador. Se você quiser adicionar outro dispositivo móvel, clique em **Adicionar** novamente e envie as informações solicitadas.

- **Mais**:

- **Adicionar usuários** – você pode adicionar dispositivos selecionando as caixas de verificação adequadas listadas em **Mais** > Usuários do computador.

- **Importar CSV** – use esta opção para adicionar muitos dispositivos móveis com facilidade. 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 especificar o **Nome do dispositivo** em cada entrada ao usar método **Importar CSV**. Ele será visto como **Nome do computador** em **Computadores**. Se você deixar o campo **Nome do dispositivo** vazio, o endereço de e-mail será usado no lugar do nome e aparecerá como **Nome do computador** em **Computadores** e **Grupos**. Evite usar o mesmo endereço de e-mail para inscrever vários dispositivos, pois este endereço de e-mail irá aparecer várias vezes e impedi-lo de conseguir distinguir os dispositivos.

Clique em **Personalizar e-mail** para ver a visualização do e-mail e personalizar o **Assunto** e o **Conteúdo**.

c)Clique em **Personalizar inscrição** para um assistente de inscrição mais detalhado (veja abaixo).

Básico

Selecione um tipo de inscrição:

- **Android ou iOS/iPadOS** – este é um procedimento de inscrição padrão para dispositivos Android ou iOS/iPadOS.

- **Proprietário do dispositivo Android** – assumir controle total do dispositivo Android gerenciado.

- **Dispositivos Android com opções de entrada limitadas** – procedimento de inscrição alternativo para inscrição de dispositivos Android sem uma câmera (limitando a inscrição de código QR) ou sem serviço de e-mail (limitando a inscrição por e-mail).

> Consulte também as etapas de sincronização para:
> - Dispositivos Android e iOS gerenciados pelo Microsoft Entra ID
> - Dispositivos Android gerenciados pelo Microsoft Intune
> - Dispositivos iOS gerenciados pelo ABM
> - Dispositivos Android gerenciados pelo VMware Workspace ONE

Distribuição

Na seção **Distribuição** você pode escolher o método de entrega do link de inscrição adequado para os dispositivos com base em sua acessibilidade e número de dispositivos.

- **Enviar e-mail** – Inscrição em massa de dispositivos móveis por email. Esta opção é mais adequada se você precisa inscrever muitos dispositivos móveis ou dispositivos móveis existentes aos quais você não tem acesso físico. Usar esta opção requer participação ativa do usuário/proprietário do dispositivo móvel.

- **Escanear código QR** – inscrição de um único dispositivo móvel. Você pode inscrever um dispositivo móvel por vez e terá que repetir o mesmo processo para cada dispositivo. Recomendamos essa opção somente quando você tiver menos dispositivos móveis para se 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 tiver novos dispositivos móveis e se eles forem ser entregues aos usuários depois de configurar os dispositivos.

- **Inserir o código de segurança** – inscrição de um único dispositivo móvel especificamente usada se um dispositivo móvel Android não tiver câmera ou cliente de e-mail.

Grupo de origem – selecione o grupo de origem inicial ao qual o dispositivo móvel será atribuído depois da inscrição.

Personalizar mais configurações

Licença – Selecione a licença adequada para ativação do produto de segurança móvel.

Marcações – selecione ou adicione uma marcação adequada para identificar o dispositivo móvel.

Configuração do produto

Selecione a caixa de seleção **Eu aceito o Acordo de licença de usuário final 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.

Você pode definir configurações adicionais para o proprietário do dispositivo Android:

- Marque a caixa de seleção **Manter aplicativos do sistema instalados em dispositivos móveis** para manter os aplicativos pré-instalados pela operadora móvel.

- Marque a caixa de seleção **Configurar rede Wi-Fi** para configurar a conexão Wi-Fi do dispositivo. Digite o **SSID** (nome) e selecione o **Tipo de segurança** – **Nenhum**, **WPA** ou **WEP**. Se você selecionou WPA ou WEP, digite a **Senha**.

Não compartilhe ou armazene o código QR, ele contém a senha do Wi-Fi.

Lista

Especifique os dispositivos móveis para inscrição, você pode usar as seguintes funções para adicionar dispositivos móveis:

- **Adicionar** – entrada única – você deve digitar manualmente um nome de dispositivo e um endereço de e-mail associado ao dispositivo móvel. (No caso de entrega de e-mail, o e-mail de inscrição será enviado para este endereço.) 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 em **Mais** > Usuários do computador. Se você quiser adicionar outro dispositivo móvel, clique em **Adicionar** novamente e envie as informações solicitadas.

- **Mais**:

  - **Adicionar usuários** – você pode adicionar dispositivos selecionando as caixas de verificação adequadas listadas em **Mais** > Usuários do computador.

  - **Importar CSV** – use esta opção para adicionar muitos dispositivos móveis com facilidade. Carregue um

arquivo *.csv* contendo uma lista de dispositivos a serem adicionados, veja Importar CSV para mais detalhes.

o**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 especificar o **Nome do dispositivo** em cada entrada ao usar método **Importar CSV**. Ele será visto como **Nome do computador** em **Computadores**. Se você deixar o campo **Nome do dispositivo** vazio, o endereço de e-mail será usado no lugar do nome e aparecerá como **Nome do computador** em **Computadores** e **Grupos**. Evite usar o mesmo endereço de e-mail para inscrever vários dispositivos, pois este endereço de e-mail irá aparecer várias vezes e impedi-lo de conseguir distinguir os dispositivos.

Clique em **Personalizar e-mail** para ver a visualização do e-mail e personalizar o **Assunto** e o **Conteúdo**.

Inscrição

Você pode revisar todos os parâmetros do processo de inscrição nesta seção.

> O link de inscrição no e-mail ou código QR é válido por 14 dias.

• **Enviar e-mail** – veja a lista de dispositivos com seus respectivos endereços de e-mail. Clique em **Visualizar e-mail** para ver o modelo do e-mail que será entregue a cada um dos endereços de e-mail na lista. Clique em **Enviar** para enviar o e-mail para os endereços de e-mail especificados. Clique em **Ver mais** na janela de confirmação para ver a lista de endereços de e-mail para os quais enviou o e-mail de inscrição. Clique em **Exportar** para exportar a lista de dispositivos e e-mails como um CSV.

• **Escanear código QR** – veja a lista de dispositivos para inscrição. No lado direito da tela, você pode ver o código QR específico para o dispositivo selecionado na lista.

• **Inserir código de segurança** – insira o código de segurança gerado no dispositivo móvel que você deseja inscrever.

> Os dispositivos móveis inscritos devem se conectar ao ESET PROTECT a cada 120 dias para evitar problemas de conexão. Você pode ver essas informações no link do e-mail de inscrição ou no código QR.
> Não inscreva um dispositivo sobressalente com antecedência. Recomendamos inscrever apenas um dispositivo sobressalente que será usado dentro de 120 dias.

Para concluir a inscrição do dispositivo móvel, siga estas etapas:

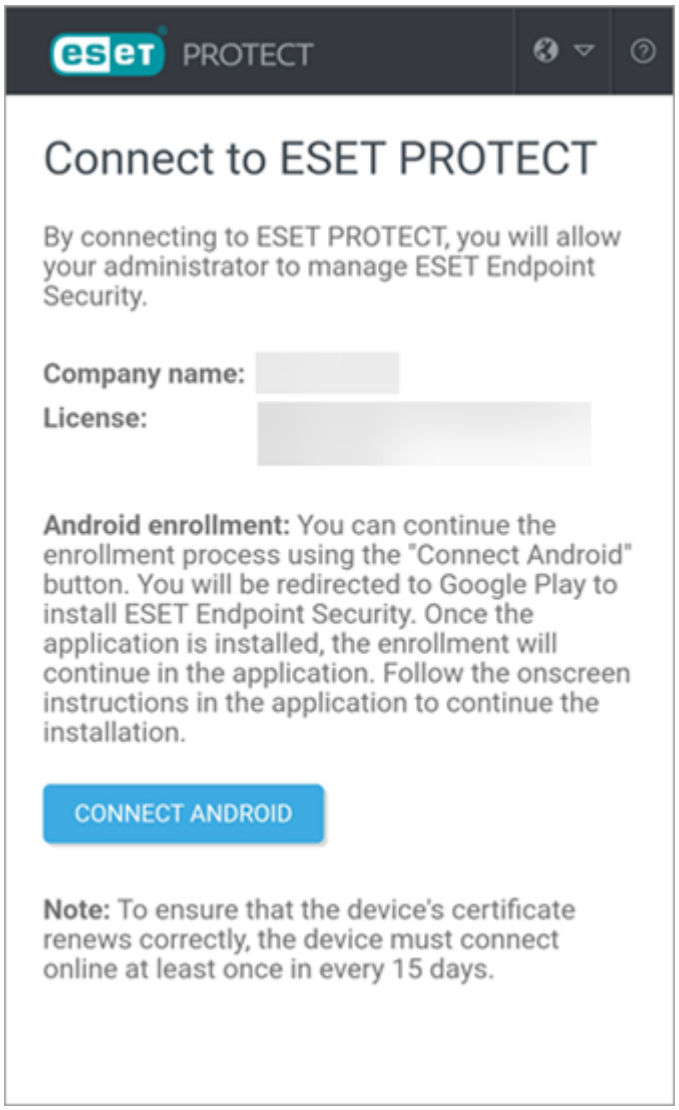
- Inscrição do dispositivo Android
- Inscrição do Android – proprietário do dispositivo
- Inscrição do dispositivo iOS

Inscrição do dispositivo Android

Siga as etapas abaixo para registrar um dispositivo Android no ESET PROTECT:

Os dispositivos móveis inscritos devem se conectar ao ESET PROTECT a cada 120 dias para evitar problemas de conexão. Você pode ver essas informações no link do e-mail de inscrição ou no código QR.
Não inscreva um dispositivo sobressalente com antecedência. Recomendamos inscrever apenas um dispositivo sobressalente que será usado dentro de 120 dias.

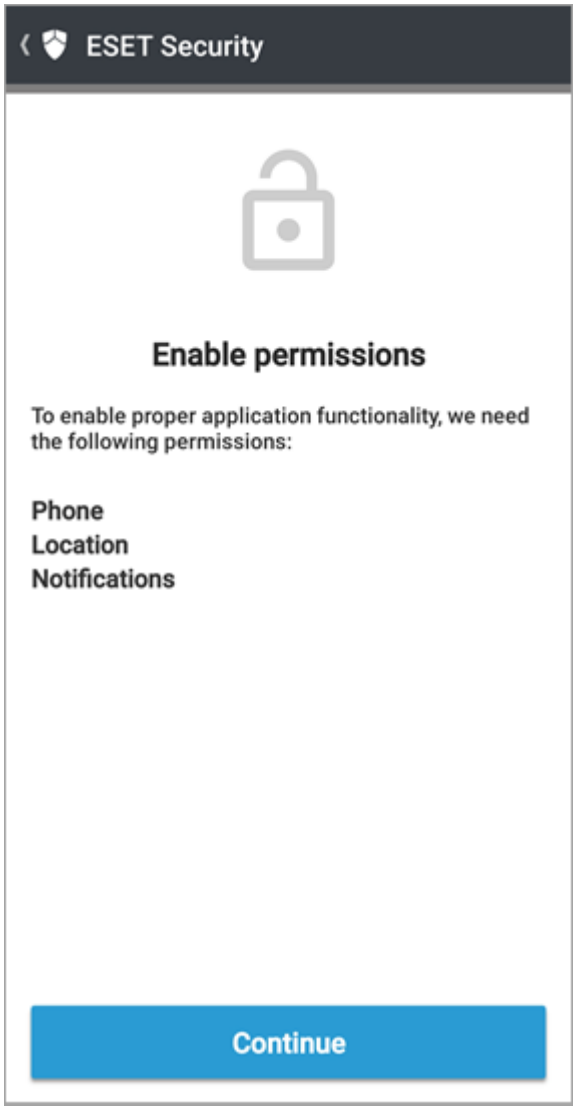
1. Abra o link de inscrição de um e-mail ou código QR e toque em **Conectar Android**.



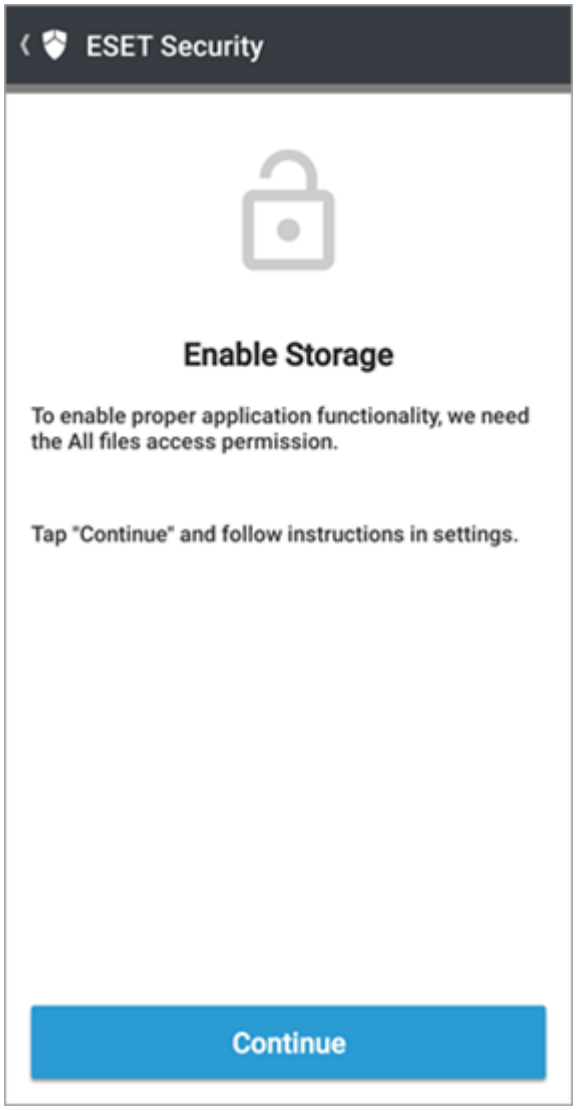
Se você não tiver o ESET Endpoint Security para Android instalado no dispositivo móvel, você será redirecionado automaticamente para a loja do Google Play para fazer download do aplicativo.

Se você receber a notificação **Nenhum aplicativo encontrado para abrir URL**, tente abrir o link de inscrição no navegador da Web padrão Android.

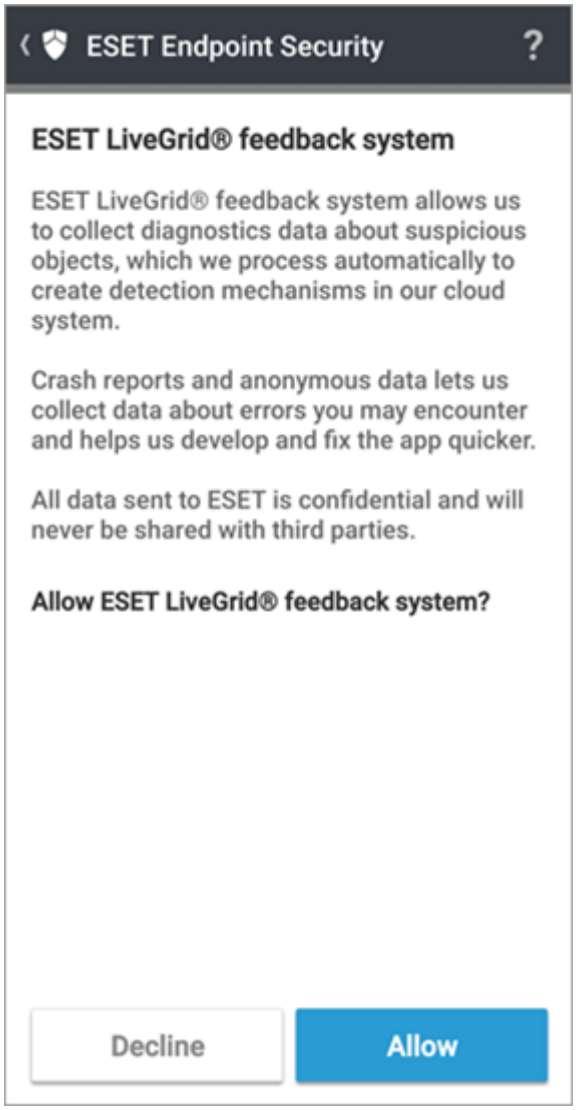
2. Toque em **Continuar** para ativar as permissões necessárias de **Telefone**, **Localização** e **Notificações**:



3. Toque em **Continuar** para ativar a permissão de acesso a Todos os arquivos.

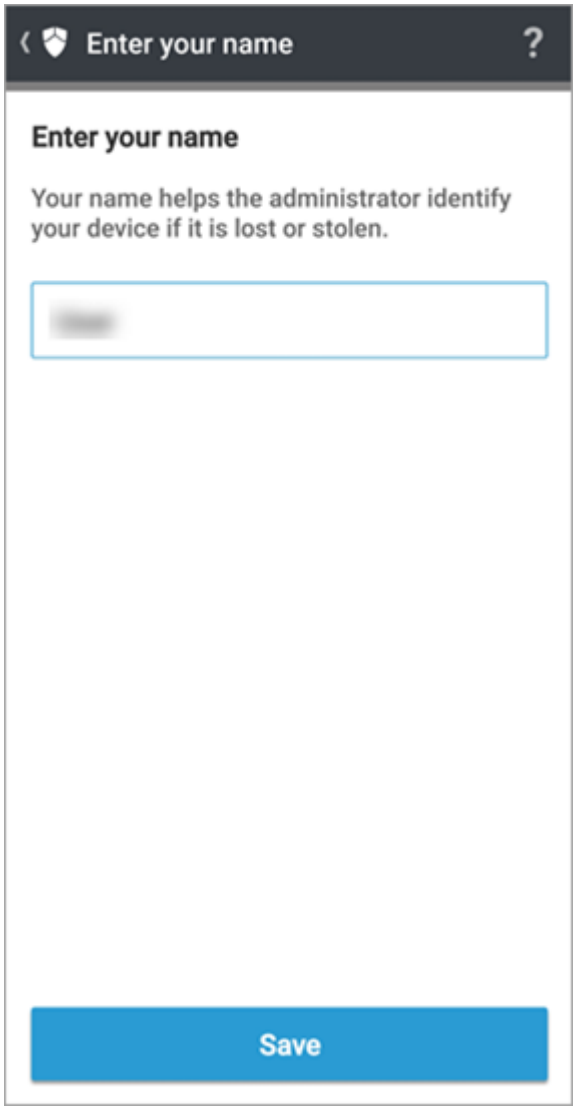


4. Toque em **Permitir** ou **Recusar** para ativar o ESET LiveGrid®.

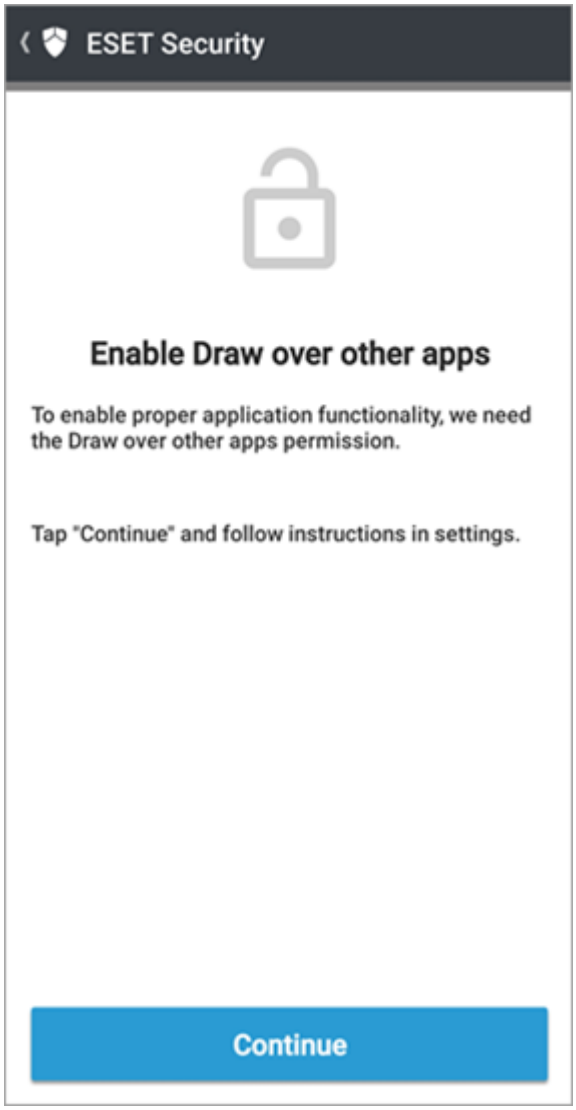


5. Digite seu nome e toque em **Salvar**.

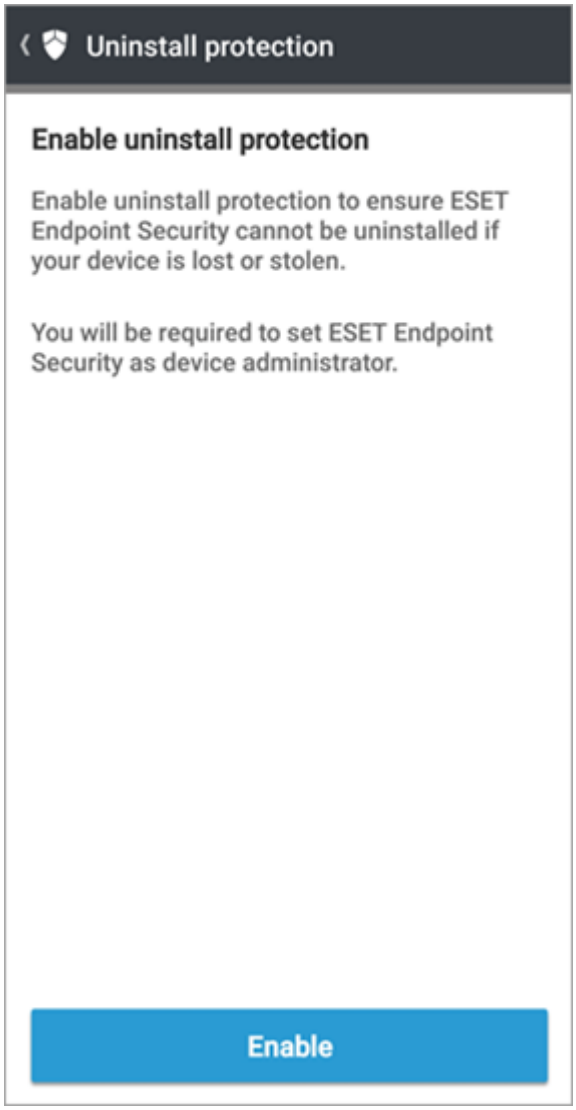
O nome não é visível no ESET PROTECT e é usado para fins de registro de diagnóstico e do Anti-Theft.



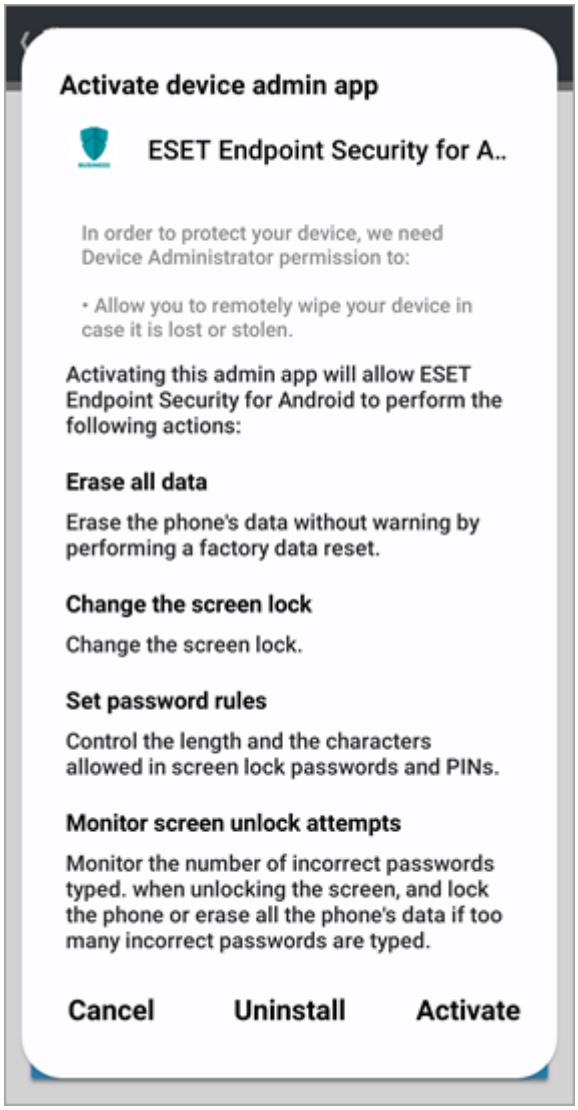
6. Toque em **Continuar** para ativar a permissão Sobrepor outros apps.



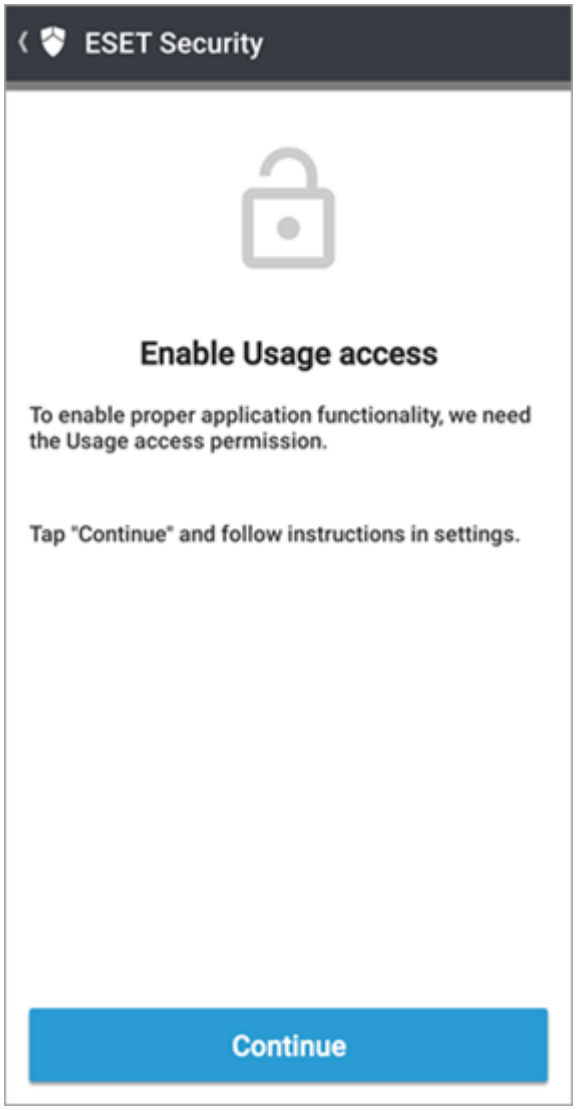
7. Toque em **Ativar** para ativar a proteção contra desinstalação para ter certeza de que o ESET Endpoint Security para Android não poderá ser desinstalado se o dispositivo for perdido ou roubado.



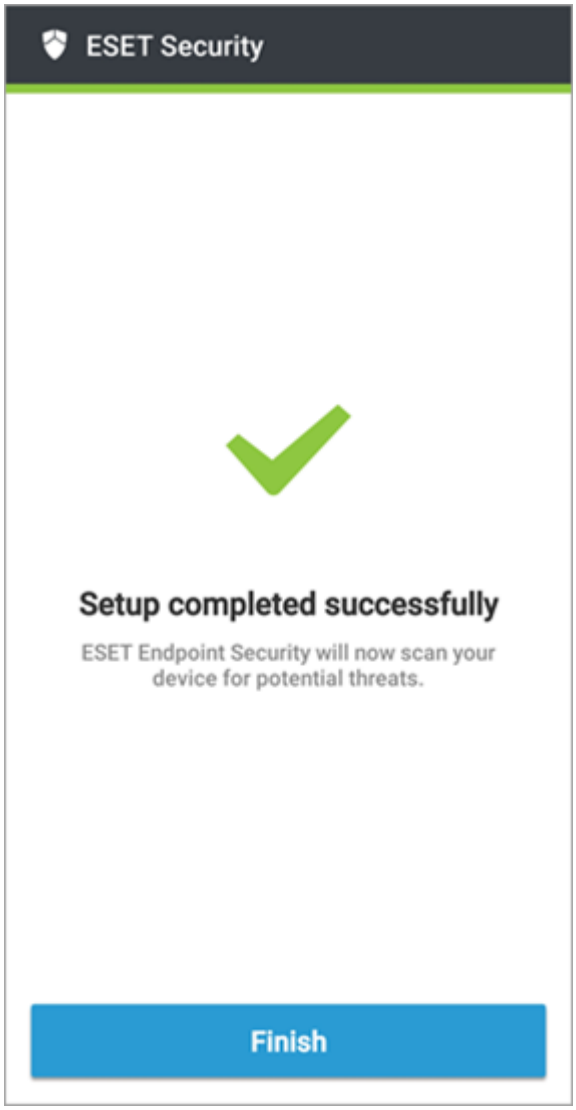
8. Toque em **Ativar** para ativar a permissão de administrador do dispositivo para o ESET Endpoint Security para Android.



9. Toque em **Continuar** para ativar a permissão de acesso de uso.



10. Toque em **Concluir**.



O ESET Endpoint Security para Android abre e o ESET PROTECT agora gerencia o dispositivo móvel.

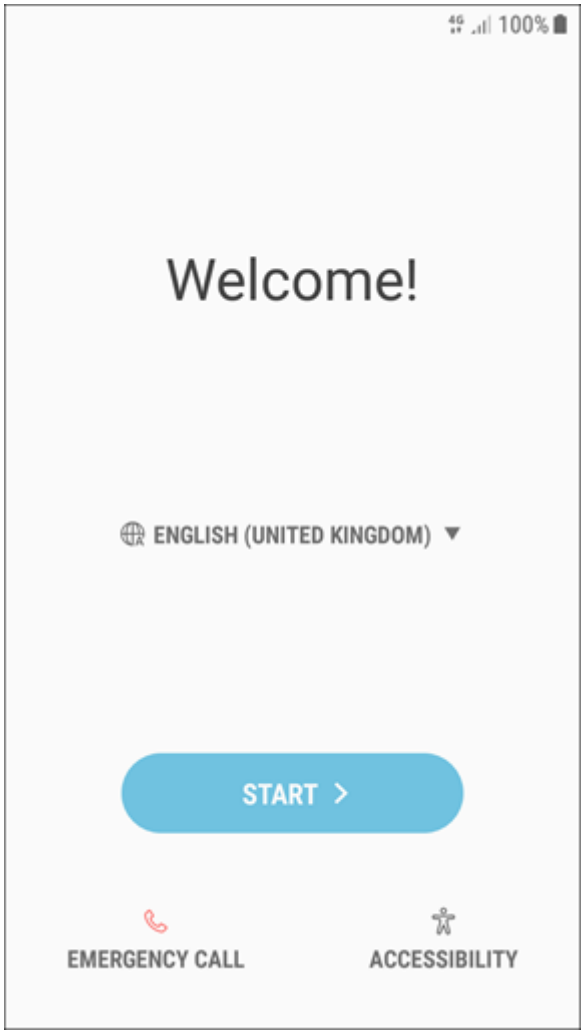
Inscrição do Android – proprietário do dispositivo

O tipo de registro do proprietário do dispositivo está disponível apenas para dispositivos Android com Android 7 e versões posteriores.
O dispositivo Android deve estar logo depois de uma limpeza/redefinição de fábrica ou ter acabado de sair da caixa para as etapas de inscrição a seguir.

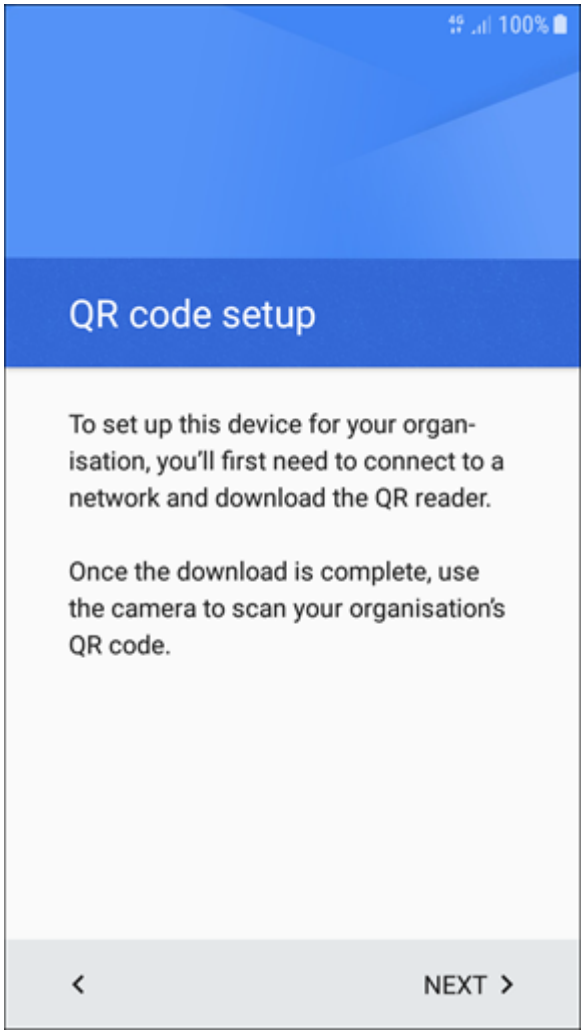
1. Ative o dispositivo móvel.

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.

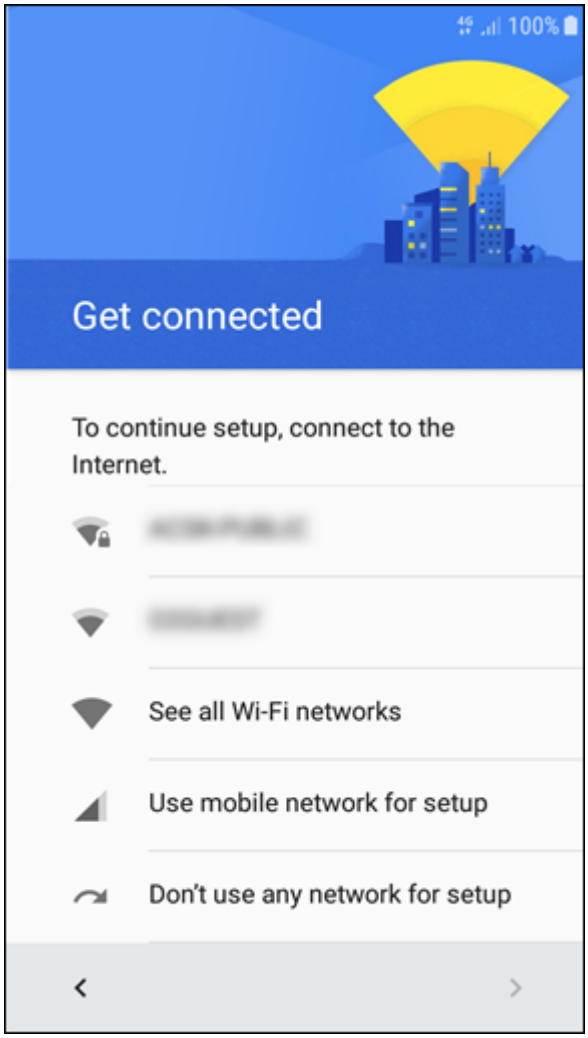


4. Uma tela de **configuração de código QR** será exibida. Toque em **Avançar** para continuar.



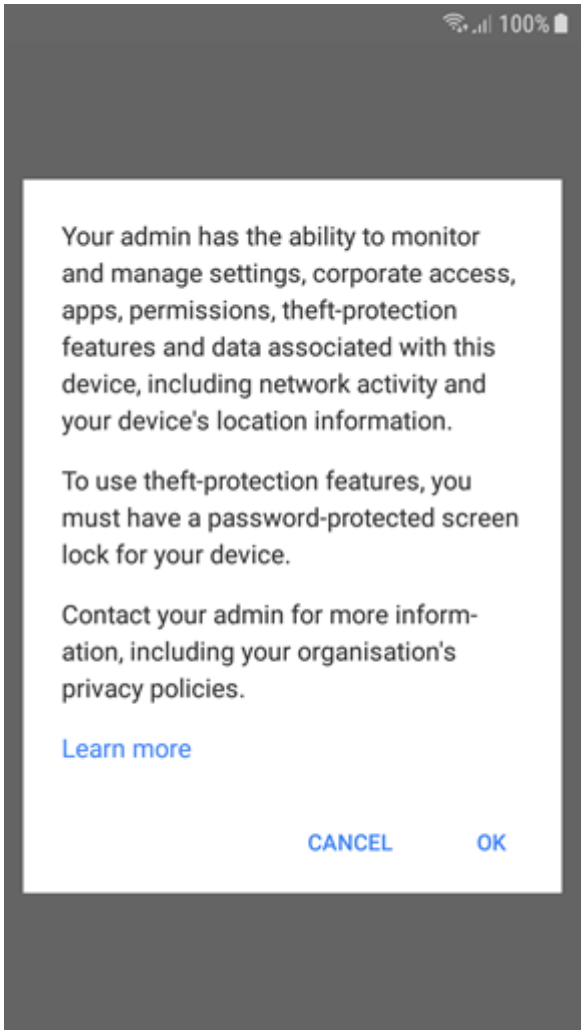
Alguns dispositivos podem exigir que você criptografe o armazenamento do dispositivo (às vezes, também é necessário conectar o carregador). Selecione o tipo de criptografia que você quer e continue de acordo com as instruções na tela.

5. Selecione uma conexão com a internet para baixar o leitor de código QR necessário para a próxima etapa.

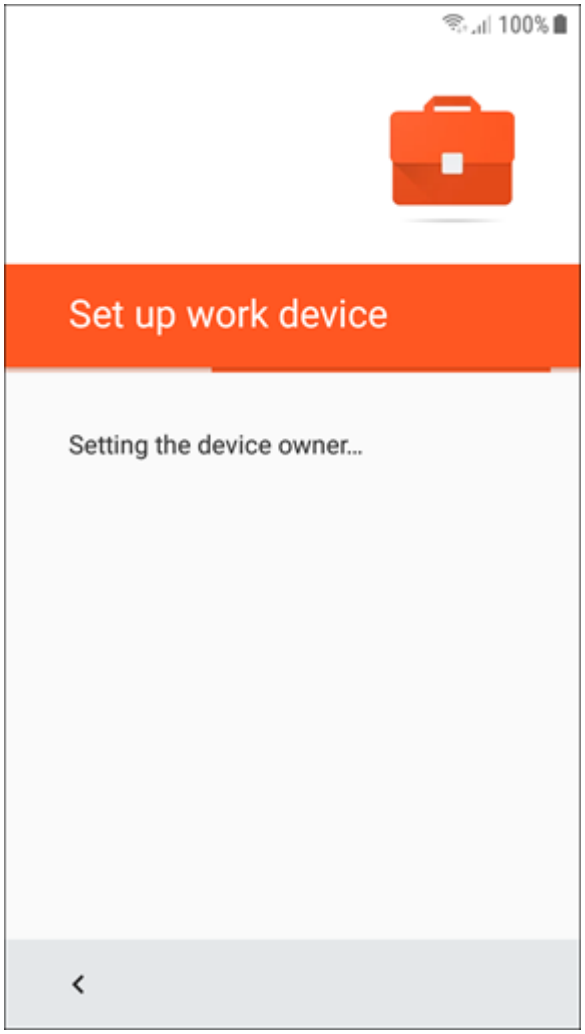


6. Agora o leitor de código QR será instalado. Depois do fim da instalação, escaneie o código QR que foi gerado no console da Web ESET PROTECT.

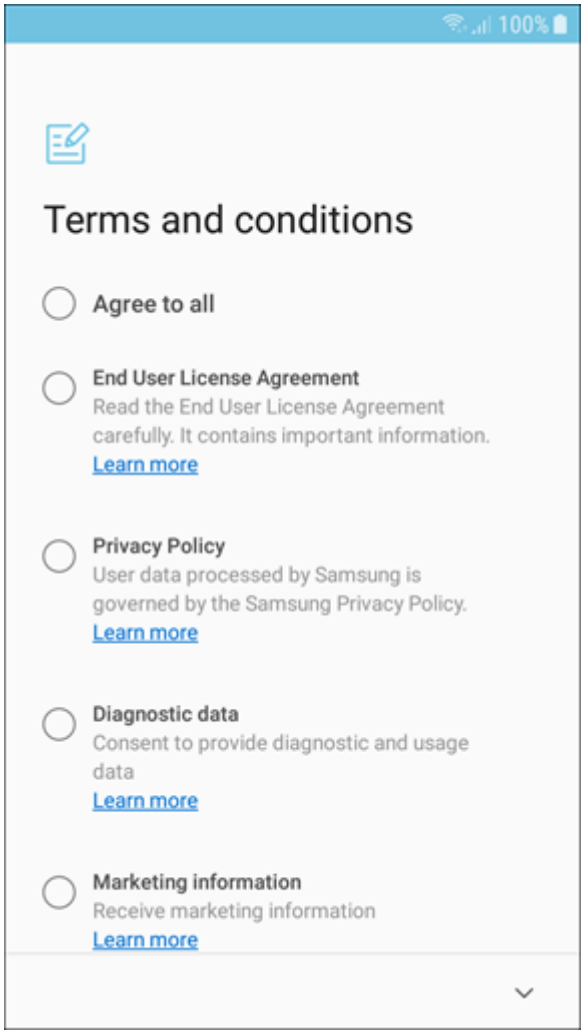
7. Será preciso que você confirme que entende que está concedendo direitos elevados de Proprietário de dispositivo ao Administrador. Toque em **OK** para continuar.



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.



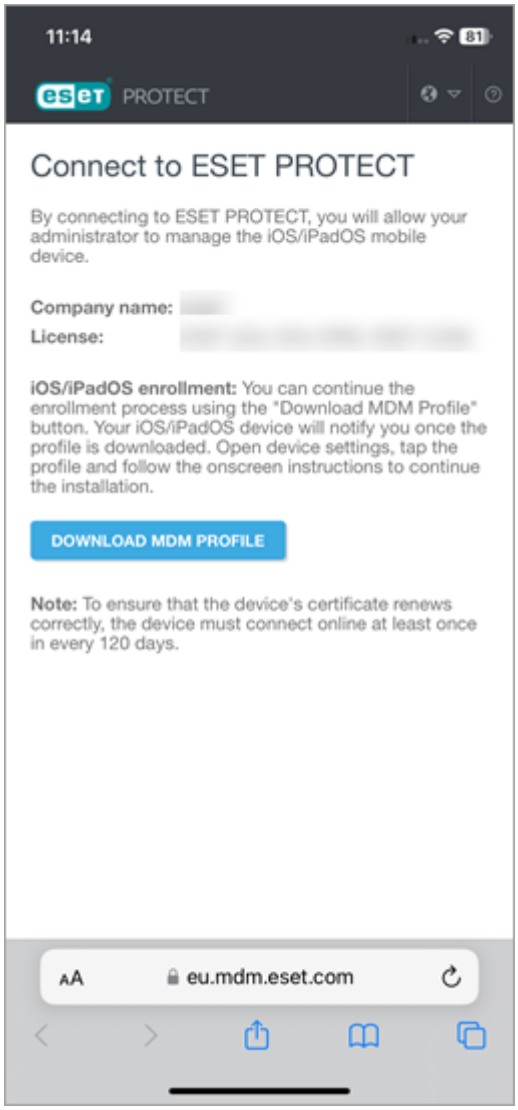
10. O dispositivo agora está inscrito no modo de Proprietário de dispositivo.

Inscrição do dispositivo iOS

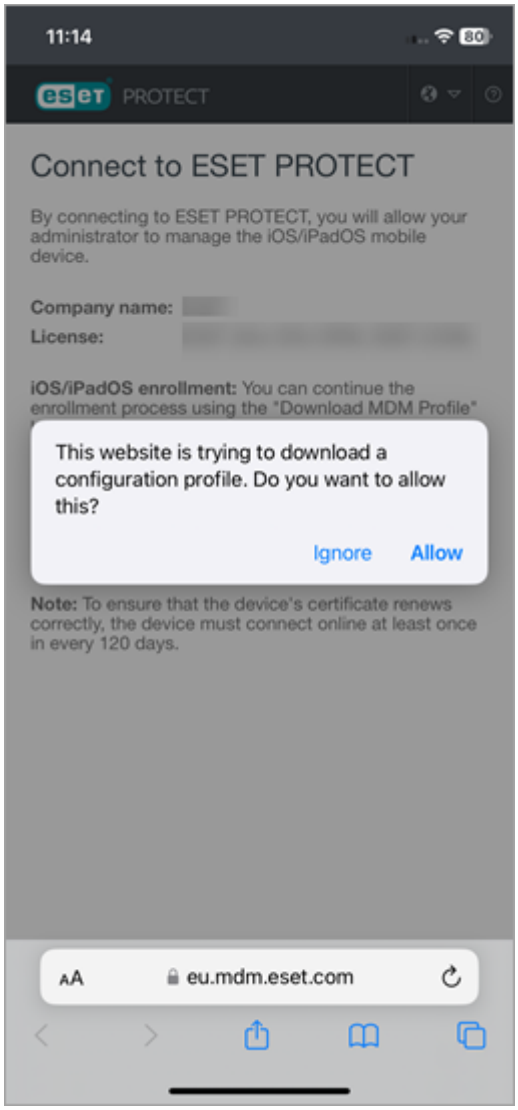
Siga as etapas abaixo para inscrever um dispositivo iOS no ESET PROTECT:

> Os dispositivos móveis inscritos devem se conectar ao ESET PROTECT a cada 120 dias para evitar problemas de conexão. Você pode ver essas informações no link do e-mail de inscrição ou no código QR.
> Não inscreva um dispositivo sobressalente com antecedência. Recomendamos inscrever apenas um dispositivo sobressalente que será usado dentro de 120 dias.

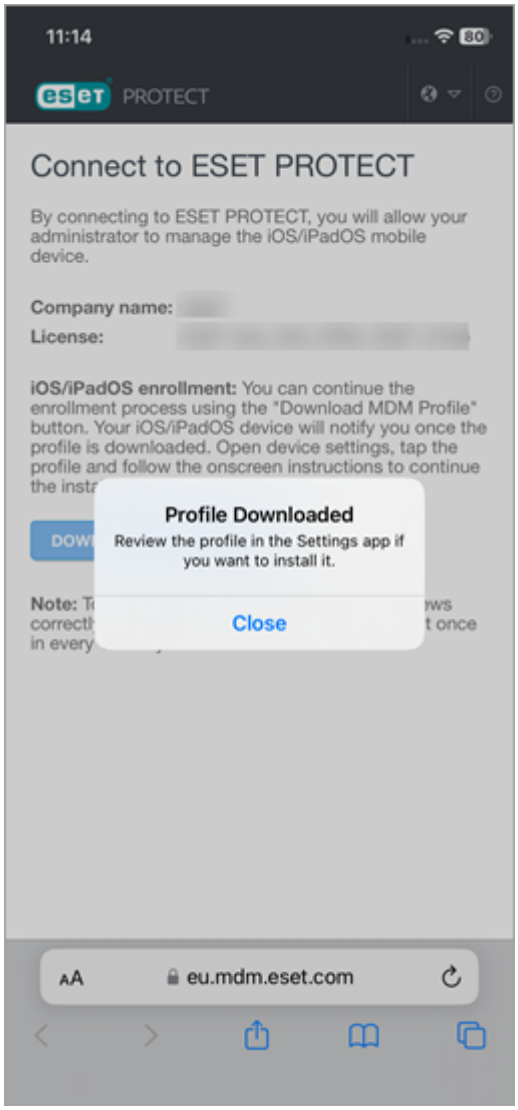
1. Abra o link de inscrição de um e-mail ou código QR e toque em **Fazer download do perfil MDM**.



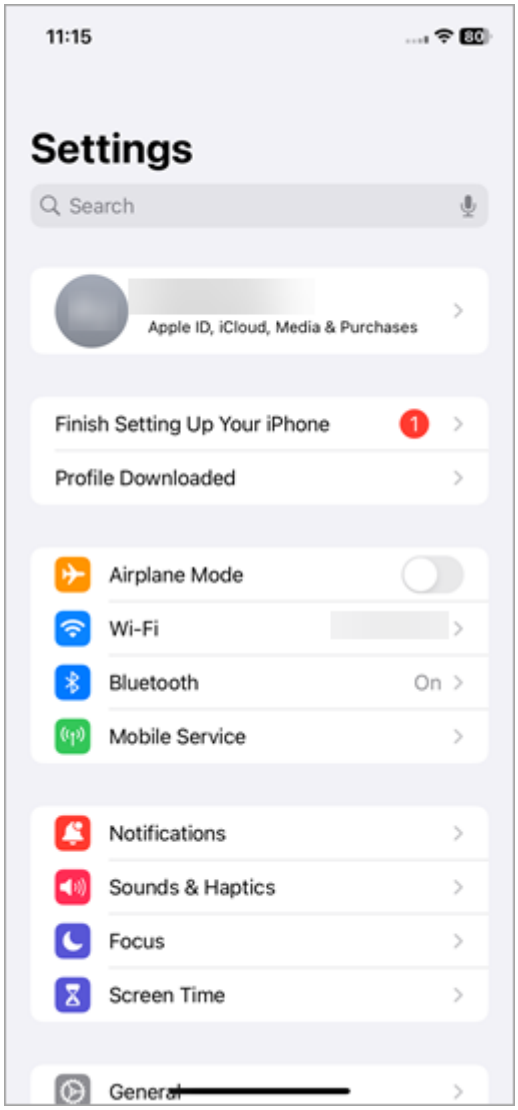
2. Toque em **Permitir**.



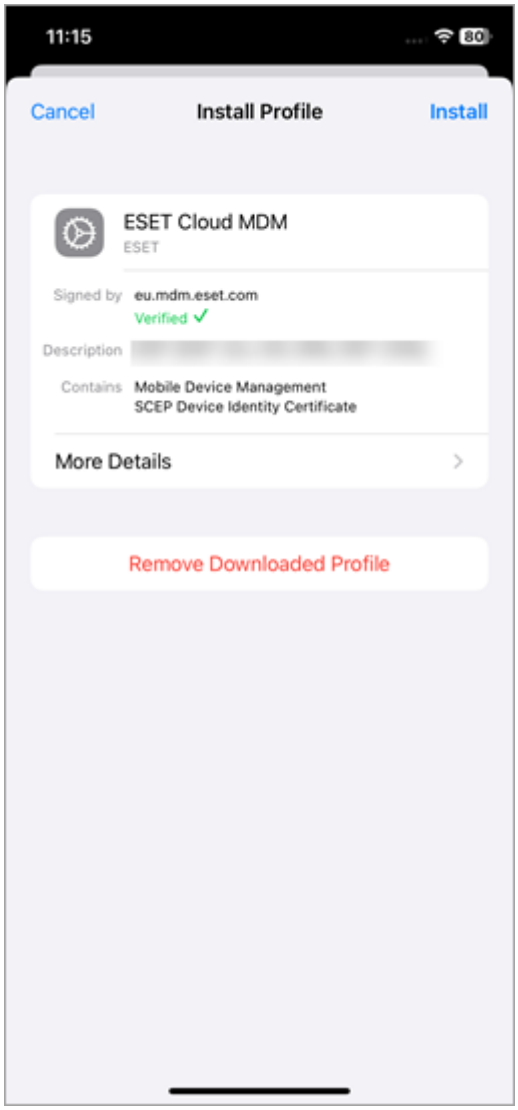
3. Toque em **Fechar**.



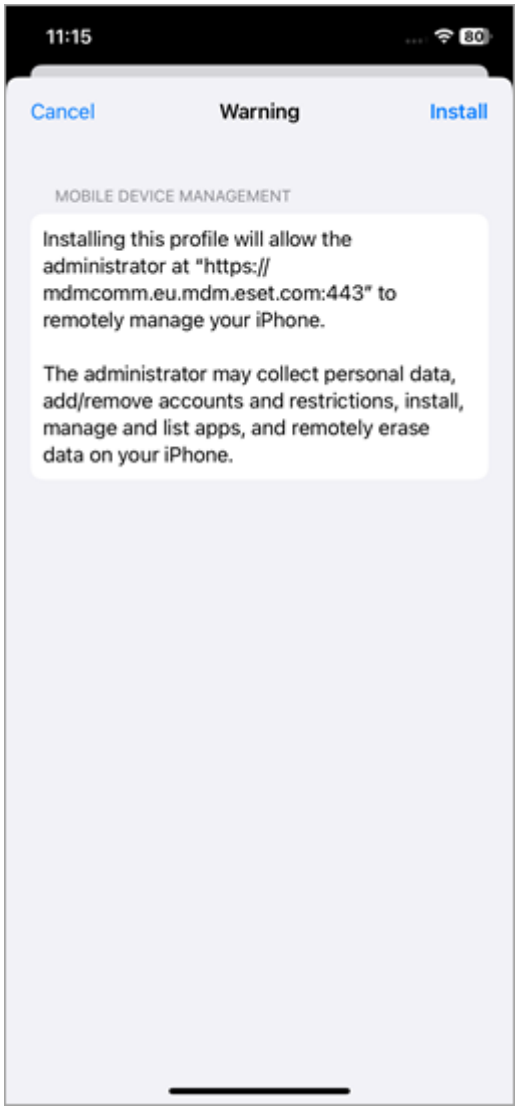
4. Abra o aplicativo **Configurações** e toque em **Perfil baixado**.



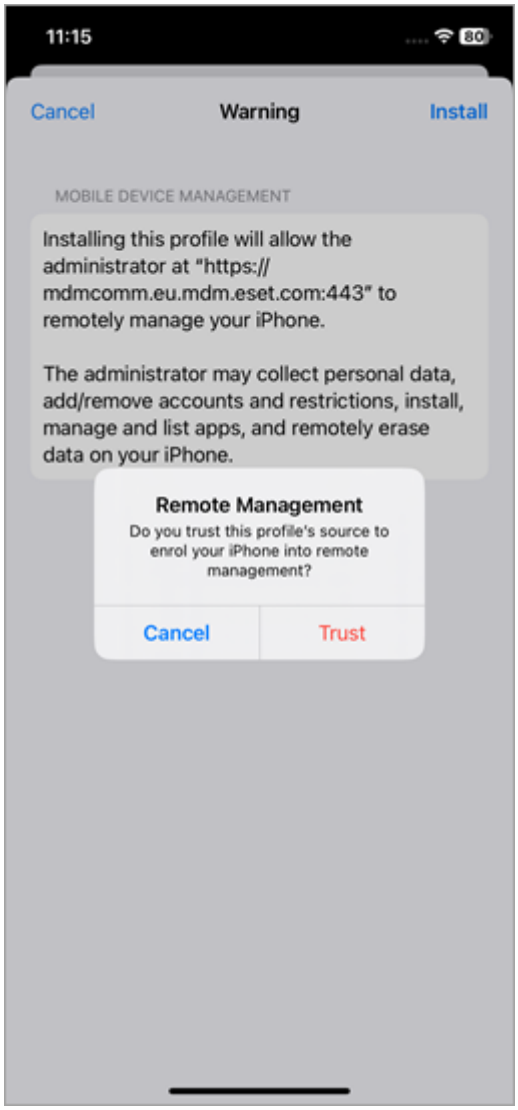
5. Toque em **Instalar** para instalar o perfil do ESET Cloud MDM.



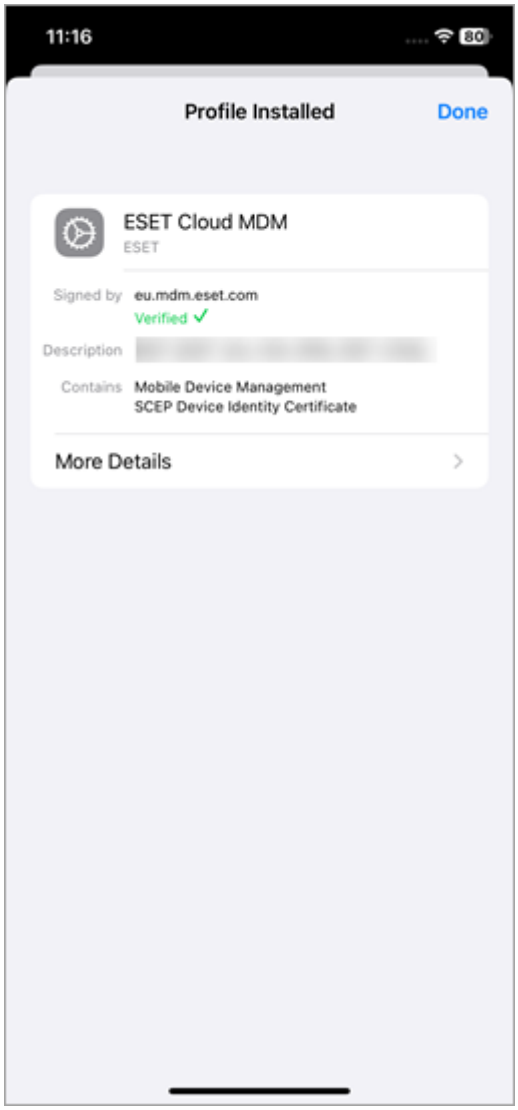
6. Toque em **Instalar**.



7. Toque em **Confiar** para instalar o novo perfil.



8. Toque em **Concluído**.

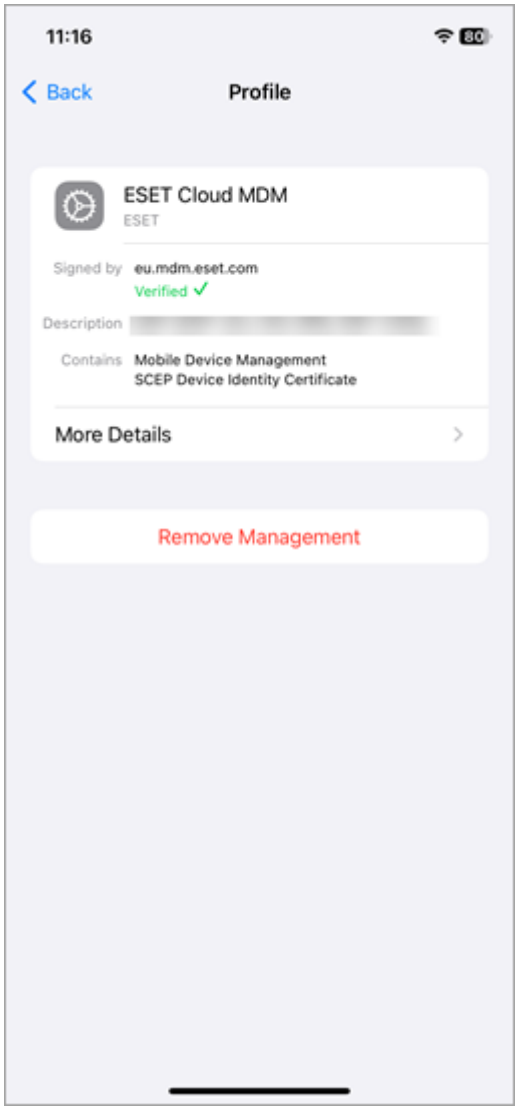


Agora o ESET PROTECT gerencia o dispositivo móvel. Este perfil de inscrição permite configurar dispositivos e definir políticas de segurança para usuários ou grupos. Os detalhes do perfil estão no aplicativo **Configurações** > **Geral** > **Gerenciamento de dispositivos e VPN**.

Remover o perfil de inscrição

Para remover o perfil de inscrição, abra o aplicativo **Configurações** > **Geral** > **Gerenciamento de dispositivos e VPN** > toque em **Remover gerenciamento**.

Remover o perfil de inscrição remove todas as configurações da empresa (E-mail, Agenda, Contatos, etc.) e dispositivo móvel iOS do gerenciamento. O dispositivo para de se conectar ao ESET PROTECT e o status do dispositivo muda para um sinal de aviso e, em seguida, um alerta vermelho depois de 14 dias.



Inscrição do Microsoft Entra ID (Android ou iOS)

Você pode verificar um usuário Microsoft Entra ID (anteriormente Azure Active Directory) para inscrever os dispositivos móveis Android ou iOS no ESET PROTECT.

Você precisa de uma conta de usuário do Microsoft Entra ID para esse tipo de inscrição de dispositivo móvel.
Você pode inscrever todos os dispositivos móveis por meio de um link.

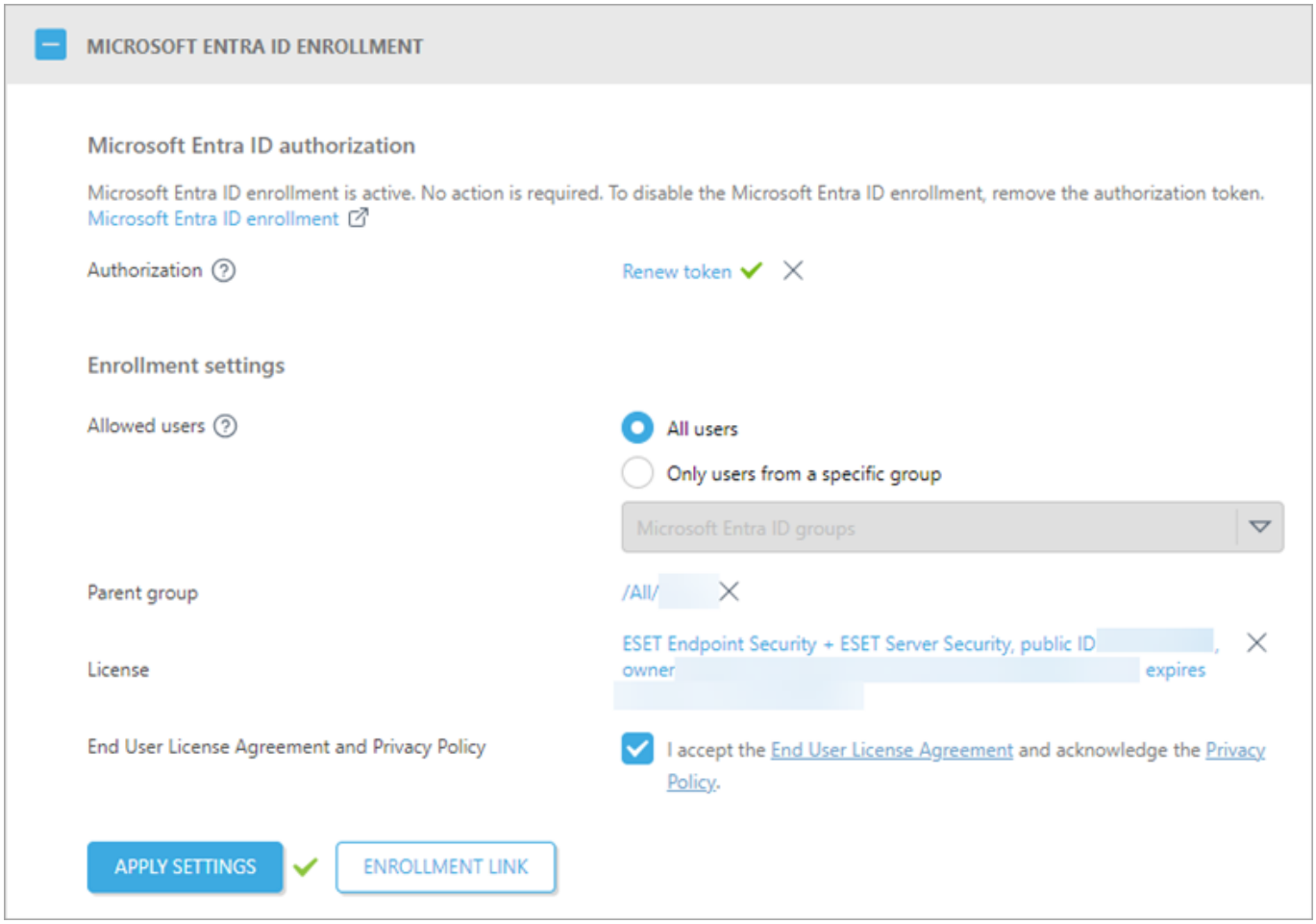
1. No Web Console ESET PROTECT clique em **Mais** > **Configurações** > **Microsoft Entra IDInscrição**.
2. Clique em **Obter token** para obter um token de autorização.
3. Entre com sua conta Microsoft Entra ID e aceite a permissão solicitada.
4. Em **Usuários permitidos**, selecione os usuários Microsoft Entra ID que podem inscrever dispositivos móveis:
   - **Todos os usuários** – todos os usuários do Microsoft Entra ID podem se inscrever.
   - **Somente usuários de um grupo específico** – selecione um grupo Microsoft Entra ID do qual os usuários podem se inscrever.

5. Selecione um **Grupo principal** ao qual os dispositivos móveis inscritos vão pertencer depois da inscrição.

6. Selecione a **Licença** para ativar os dispositivos móveis inscritos.

7. Selecione a caixa de seleção **Eu aceito o Acordo de licença de usuário final 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.

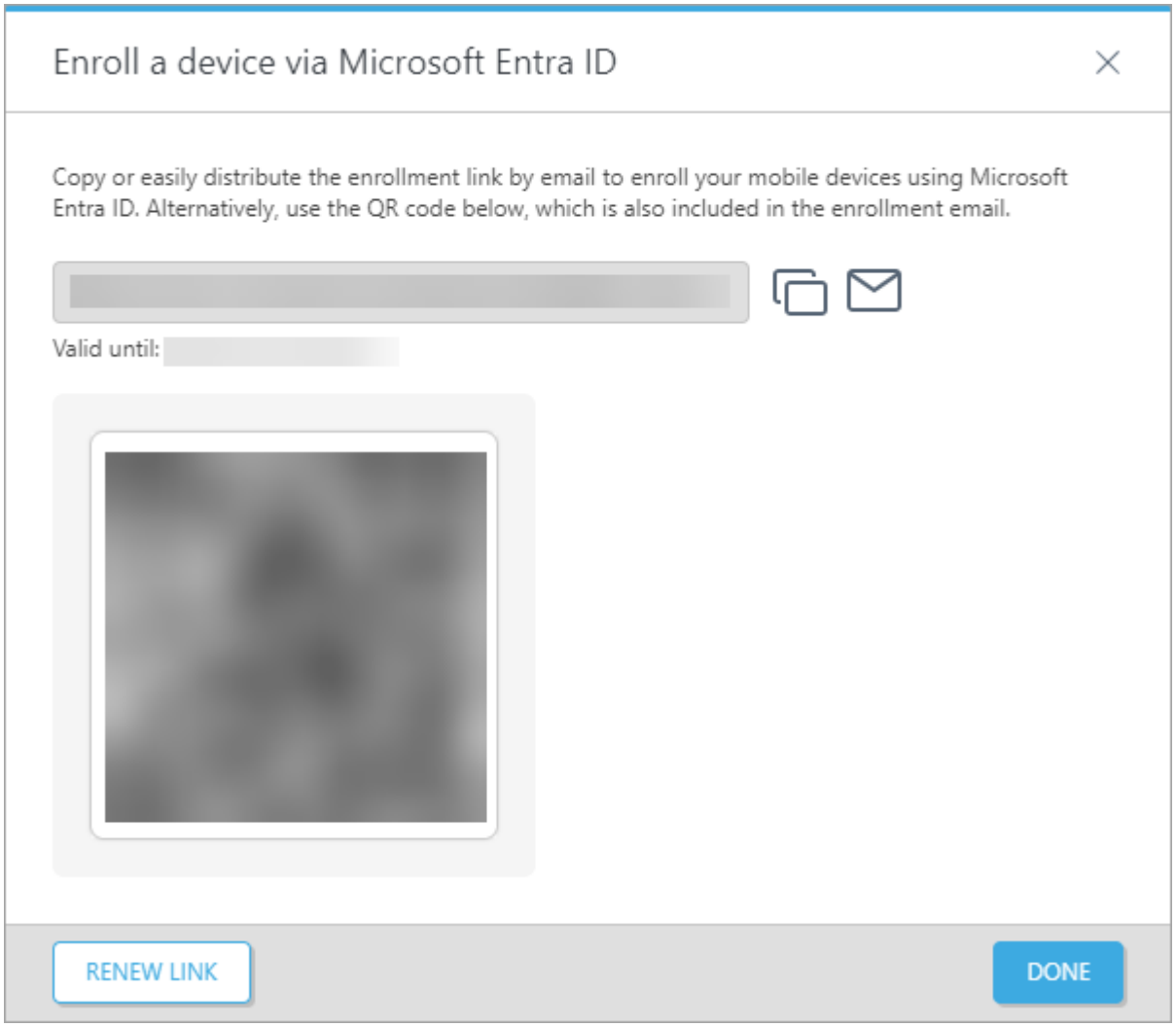
8. Clique em **Aplicar configurações** para salvar e aplicar todos os parâmetros de inscrição selecionados. Seus dispositivos móveis Microsoft Entra ID aparecerão no Web Console ESET PROTECT em **Computadores** com os mesmos nomes de dispositivo. Você pode renomear um dispositivo nos detalhes do dispositivo.



9. Clique em **Link de inscrição** para mostrar um link de inscrição:

- Você pode copiar o link, escaneá-lo usando um código QR ou enviá-lo por e-mail. Há um link de inscrição – ele não é específico do usuário.

- O link de inscrição é válido por um ano. Clique em **Renovar link** para renovar o link de inscrição.



10. Abra o link de inscrição em um dispositivo móvel, entre em sua conta Microsoft Entra ID e aceite a permissão solicitada. Em seguida, siga as etapas de inscrição para o Android ou iOS.

> Para inscrever dispositivos Android com opções de entrada limitadas:
> 1.Abra o link de inscrição em um navegador da web em um computador.
> 2.Insira o código de segurança gerado no aplicativo ESET Endpoint Security para Android no dispositivo móvel que você deseja inscrever.
> 3.Conclua a inscrição.

11. Agora você pode gerenciar os dispositivos móveis Microsoft Entra ID no ESET PROTECT.

Todos os Microsoft Entra ID dispositivos móveis estão em grupos dinâmicos dedicados —**Microsoft Entra ID inscrição** (Android dispositivos) e **Microsoft Entra ID dispositivos** (iOS dispositivos).

Sincronização do Microsoft Intune (Android)

Se você estiver usando o Microsoft Intune, é possível sincronizar sua conta Microsoft Intune com o ESET PROTECT para gerenciar seus dispositivos Android Microsoft Intune com o ESET PROTECT.

Pré-requisitos

- Prepare seu Microsoft Intune para a inscrição do Android.
- Conecte seu Microsoft Intune com sua conta do Google Play gerenciada.
- Inscreva os dispositivos como Android Enterprise.
- Migre os dispositivos inscritos como **Administrador de dispositivos Android** antes da inscrição.

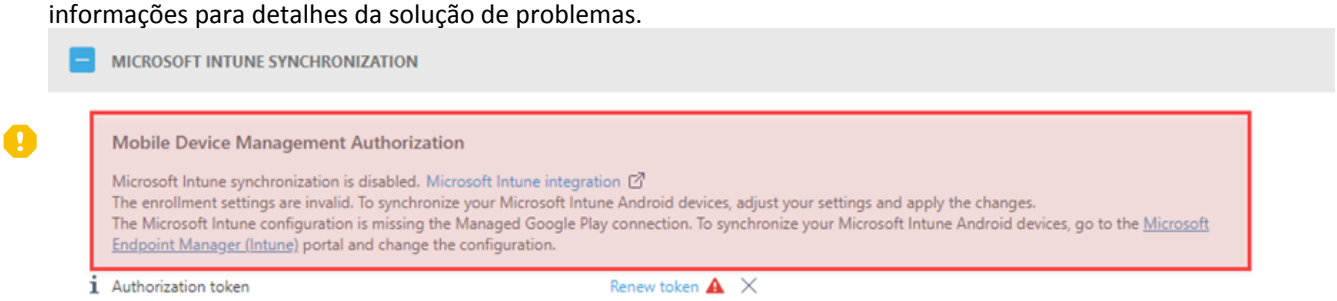
1. No Web Console ESET PROTECT, clique em **Mais** > **Configurações** > **Sincronização do Microsoft Intune**.

2. Clique em **Obter token**.

3. Entre com sua conta Microsoft Intune.

4. Depois de um login bem-sucedido, uma **Solicitação de permissão** é necessária para o ESET PROTECT. Revise as informações fornecidas e clique em **Aceitar** para continuar e adicionar um token de autenticação válido à sua instância ESET PROTECT.

Se houver qualquer problema com o processo de importação do Token de autorização, consulte a caixa de informações para detalhes da solução de problemas.



5. Em **Configurações de inscrição**, selecione um dos métodos de inscrição:

- **Inscrever todos os dispositivos Android** – todos os dispositivos Android Microsoft Intune serão inscritos automaticamente no seu ESET PROTECT.
- **Inscrever dispositivos Android para todos os usuários** – inscreve apenas dispositivos Android com o usuário atribuído no Microsoft Intune para seu ESET PROTECT.
- **Inscrever dispositivos Android dos grupos Microsoft Intune** – inscreve apenas dispositivos Android que fazem parte dos grupos selecionados Microsoft Intune no seu ESET PROTECT.

6. Selecione a **Licença** usada para ativar os dispositivos Android inscritos.

7. Selecione um **Grupo principal** ao qual os dispositivos Android inscritos vão pertencer depois da inscrição.

8. **Notificações** (habilitadas por padrão) – envia notificações automaticamente para cada dispositivo quando a proteção não tiver sido ativada. As notificações informam aos usuários que a proteção está instalada em seus dispositivos e eles devem ativá-la abrindo o aplicativo ESET Endpoint Security em seu perfil de trabalho. O dispositivo pode receber até três notificações: cinco dias, sete dias e nove dias após a inscrição. Clique em **Personalizar** para personalizar a mensagem de notificação.

9. **Aplique as configurações de inscrição** para salvar e aplicar todos os parâmetros de inscrição selecionados.

Dispositivos Microsoft Intune agora estão disponíveis para gerenciamento no ESET PROTECT e no Microsoft Intune.

Quando você registra um dispositivo com Android 9 e posteriormente via Microsoft Intune ou VMware Workspace ONE, o ESET Endpoint Security para Android versão 3.5 e posterior ignora as seguintes configurações de política:

- Segurança do dispositivo
- Controle de aplicações
- Anti-Theft

Sincronização do VMware Workspace ONE (Android)

Se você gerencia dispositivos Android com o VMware Workspace ONE (consulte Registrando o Android com o VMware Workspace ONE), poderá sincronizar sua conta VMware Workspace ONE com o ESET PROTECT para proteger os dispositivos Android VMware Workspace ONE. Siga as etapas abaixo para configurar a sincronização:

I. Habilite o acesso à API REST em VMware Workspace ONE

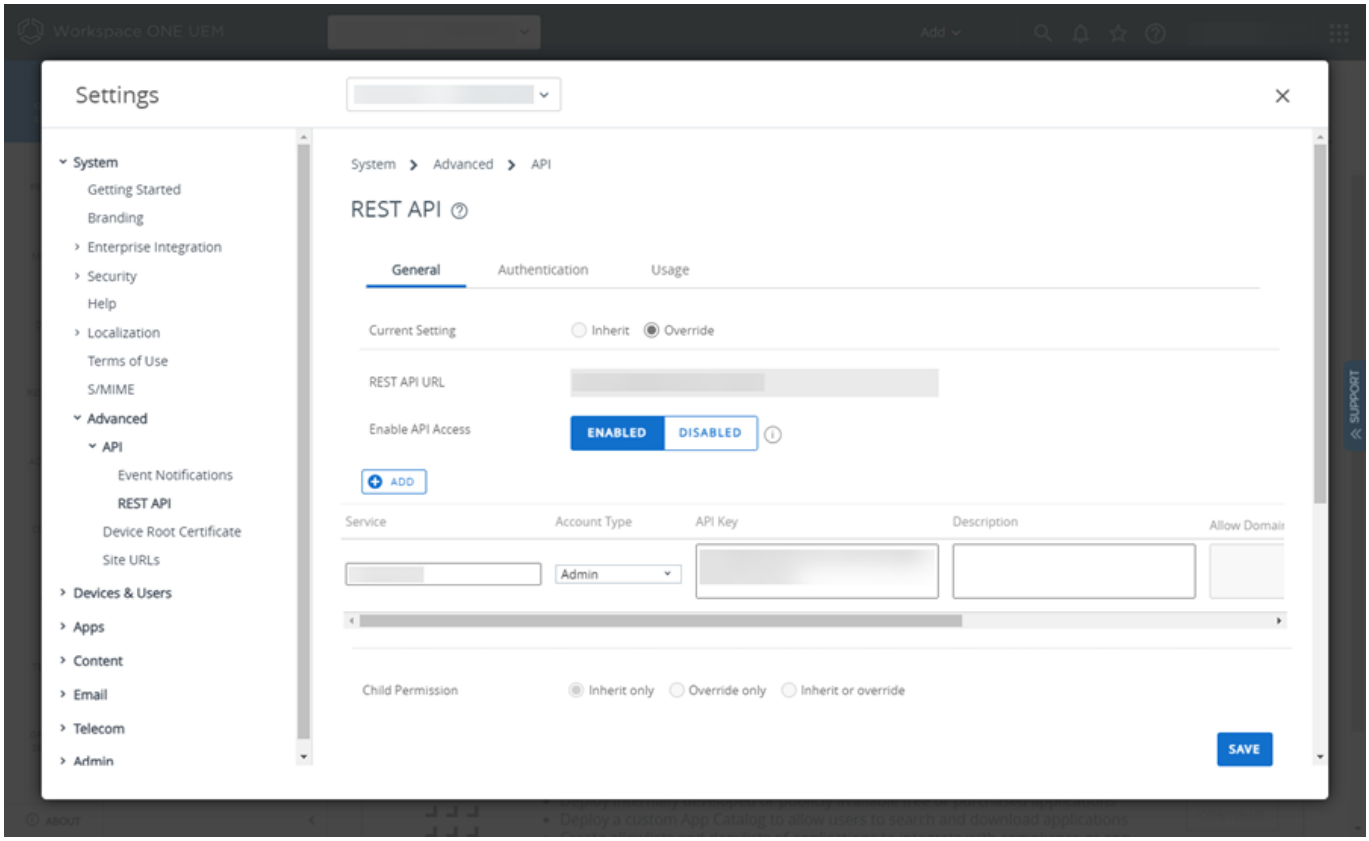
II. Crie um cliente OAuth em VMware Workspace ONE

III. Sincronizar ESET PROTECT com VMware Workspace ONE

I. Habilite o acesso à API REST em VMware Workspace ONE

1. Entre no VMware Workspace ONE:
2. Clique em **Introdução** > **Configurações**.
3. Clique em **Avançado** > **API** > **REST API**.
4. Copie o **URL da API REST**.
5. Selecione **Habilitado** ao lado de **Habilitar acesso à API**.
6. Clique em **Adicionar**, digite o nome do **Serviço** e copie a **chave da API**.
7. Clique em **Salvar**.

Leia mais sobre a API REST para VMware Workspace ONE.



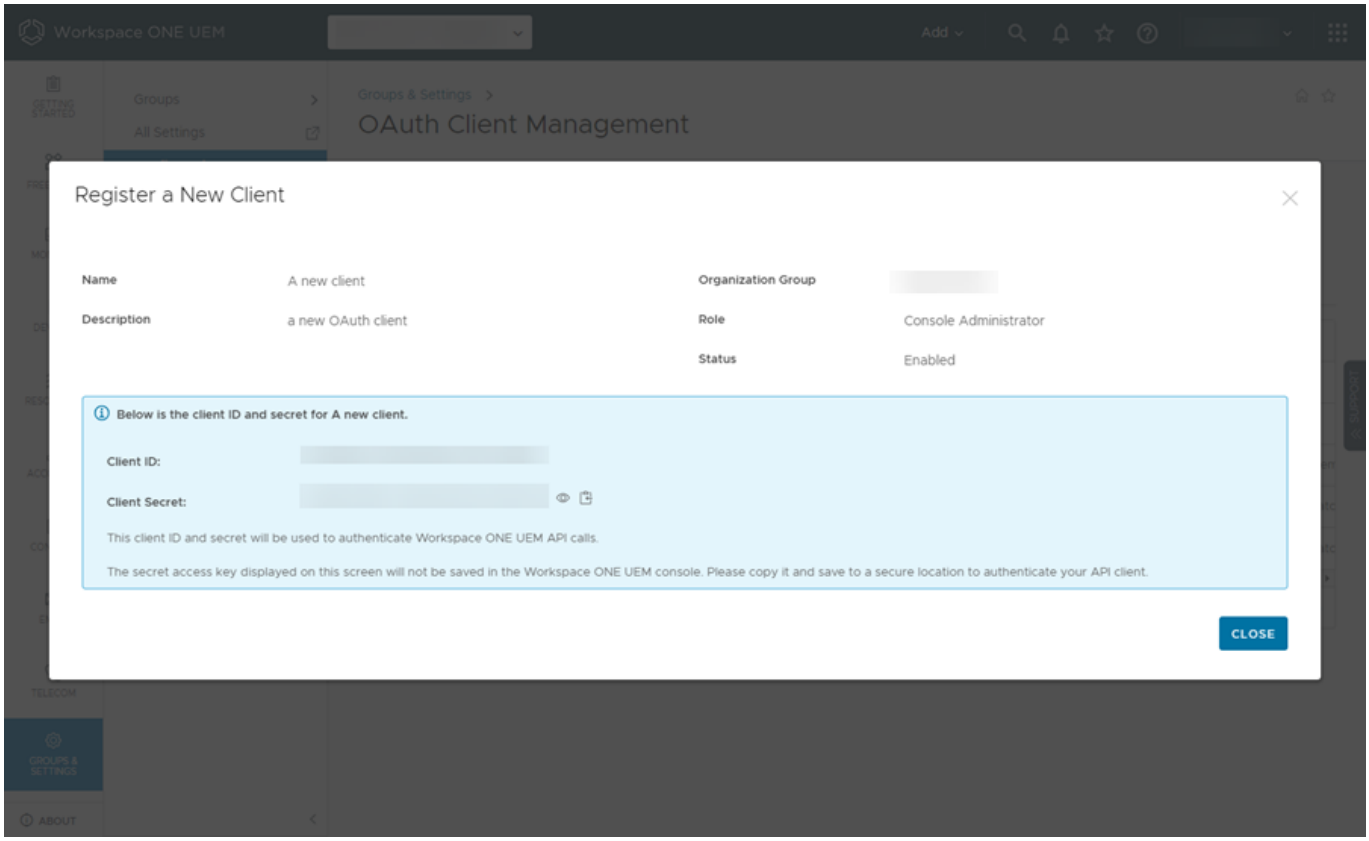
II. Crie um cliente OAuth em VMware Workspace ONE

1. Clique em **Grupos e configurações** > **Configurações**.
2. Digite **OAuth** na caixa de pesquisa **Digite um nome ou categoria**.
3. Clique em **Gerenciamento de cliente OAuth**.
4. Clique em **Adicionar**.
5. Na janela **Registrar um novo cliente**:
   a. Digite o **Nome**, **Descrição** e **Grupo de Organização**.
   b. Selecione o **Administrador do console** no menu suspenso **Função**.
   c. Verifique se a opção **Status** está **Habilitada**.
   d. Clique em **Salvar**.
6. Copie o **ID do cliente** e o **Segredo do cliente**.

> Certifique-se de ter copiado e salvo o **ID do cliente** e o **Segredo do cliente** antes de fechar a janela. Não é possível recuperar o **ID do cliente** e o **Segredo do cliente** depois de clicar em **Fechar**.

7. Clique em **Fechar**.

> Leia mais sobre como gerenciar clientes OAuth na documentação VMware Workspace ONE.



III. Sincronizar ESET PROTECT com VMware Workspace ONE

1. No console da Web ESET PROTECT clique em **Mais** > **Configuração**.

2. Expanda a **sincronização VMware Workspace ONE**.

3. Clique em **Configurar** ao lado de **Autorização**.

4. Digite ou cole as configurações de autorização necessárias:

    a.**URL da API REST** – digite ou cole o link copiado na etapa 4 da seção I acima.

    b.**REST API KEY** – digite ou cole a **chave de API** copiada na etapa 6 da seção I acima.

    c.**ID do cliente OAuth** – digite ou cole o **ID do cliente** que você copiou na etapa 6 da seção II acima.

    d.**Segredo do cliente OAuth** – digite ou cole o **Cegredo do cliente** que você copiou na etapa 6 da seção II acima.

5. Clique em **Configurar**. Quando as configurações de autorização estiverem corretas, você verá **Atualizar** ✔ com uma marca de seleção verde ao lado de **Autorização**.

6. Em **Atribuições**, selecione os dispositivos Android a serem sincronizados:

    a.**Inscrever todos os dispositivos Android** – sincronize todos os dispositivos Android do seu VMware Workspace ONE.

A opção **Inscrever todos os dispositivos Android** cria a opção **Todos os dispositivos Android protegidos pela ESET** com o Grupo inteligente VMware Workspace ONE com todos os dispositivos Android. A **atribuição de proteção ESET** vai instalar o ESET Endpoint Security para Android em dispositivos móveis no grupo. Se, posteriormente, você selecionar a opção **Inscrever somente dispositivos Android de um grupo específico**, a opção **Todos os dispositivos Android protegidos pela ESET** com o Grupo inteligente será removida.

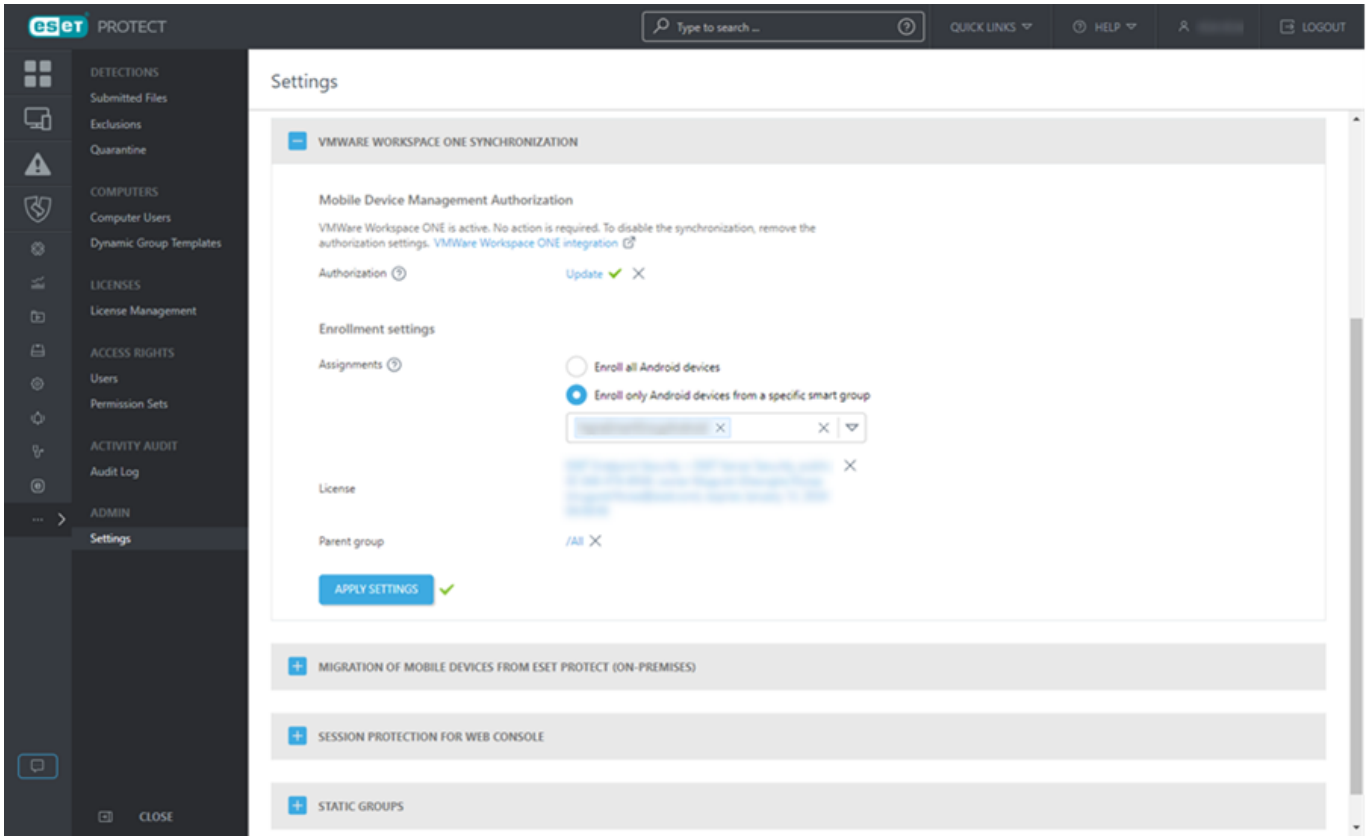
b. **Inscrever apenas dispositivos Android de um grupo inteligente específico** – sincronize os dispositivos Android dos Grupos inteligentes VMware Workspace ONE selecionados no menu suspenso.

7. **Licença** – a licença apropriada está pré-selecionada. Você pode selecionar outra licença. A licença ativará o ESET Endpoint Security para Android durante a instalação.

8. **Grupo de origem** – selecione o Grupo de origem ESET PROTECT onde os dispositivos Android serão sincronizados.

9. **Notificações** (habilitadas por padrão) – envia notificações automaticamente para cada dispositivo quando a proteção não tiver sido ativada. As notificações informam aos usuários que a proteção está instalada em seus dispositivos, e eles devem ativá-la abrindo o aplicativo ESET Endpoint Security em seu perfil de trabalho ou tocando no link na notificação. O dispositivo pode receber até três notificações: cinco dias, sete dias e nove dias após a inscrição. Clique em **Personalizar** para personalizar a mensagem de notificação.

10. Clique em **Aplicar configurações**.



Os dispositivos Android do seu VMware Workspace ONE aparecerão na seção Computadores sob o grupo de origem selecionado, e você pode gerenciar o ESET Endpoint Security para Android instalado por meio de uma política.

Quando você registra um dispositivo com Android 9 e posteriormente via Microsoft Intune ou VMware Workspace ONE, o ESET Endpoint Security para Android versão 3.5 e posterior ignora as seguintes configurações de política:

- Segurança do dispositivo
- Controle de aplicações
- Anti-Theft

Sincronização de Apple Business Manager (ABM) (iOS)

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.

Antes de executar a inscrição do ABM do iOS, você deve habilitar a sincronização do ABM no Web Console ESET PROTECT. Para fazer isso, navegue até **Mais** > **Configurações** > **Sincronização Apple Business Managed (ABM)**.

Sincronize seu ESET PROTECT MDM com o servidor Apple ABM

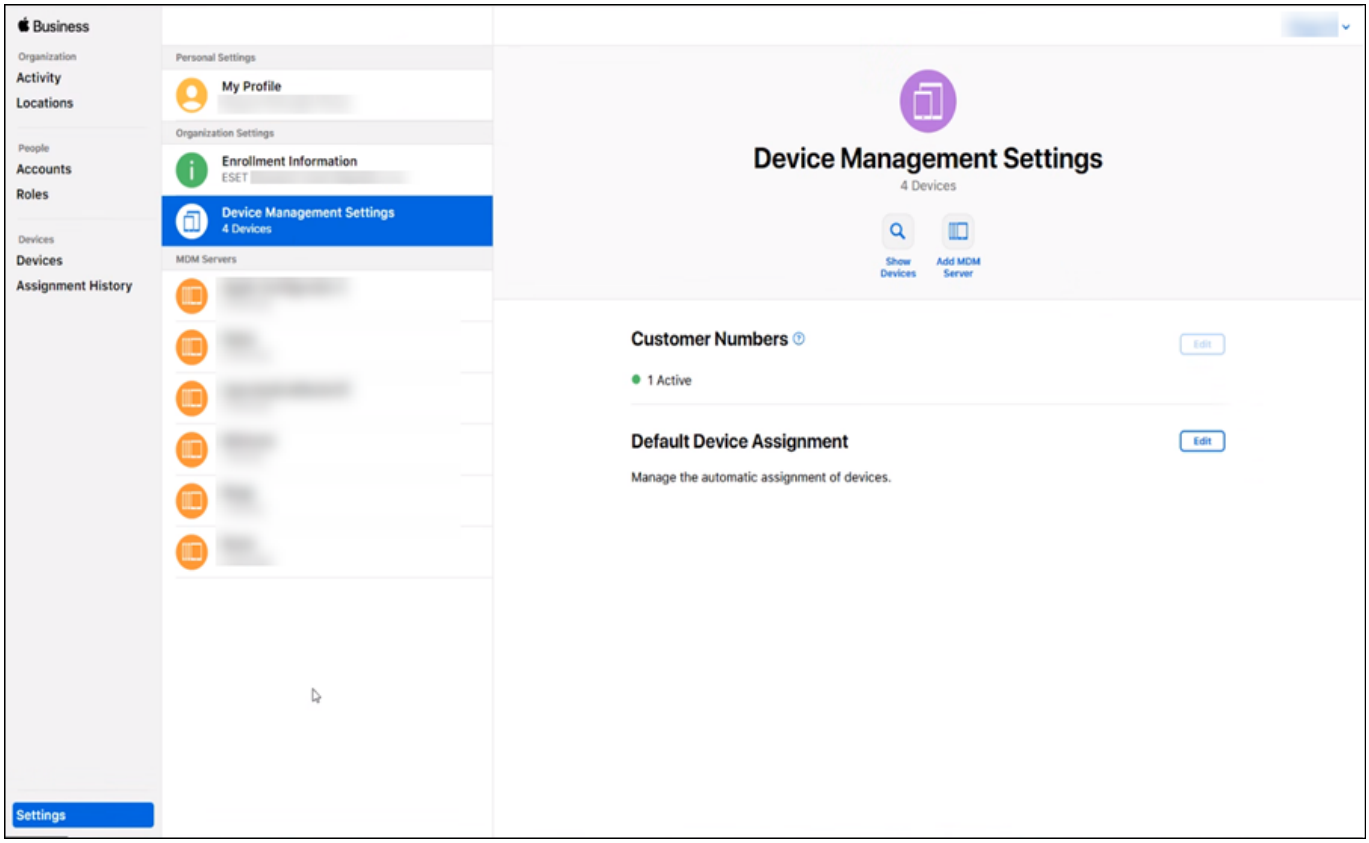
1. Verifique se todos os Requisitos Apple ABM são cumpridos para os requisitos da conta e os requisitos do dispositivo.

Conta ABM:

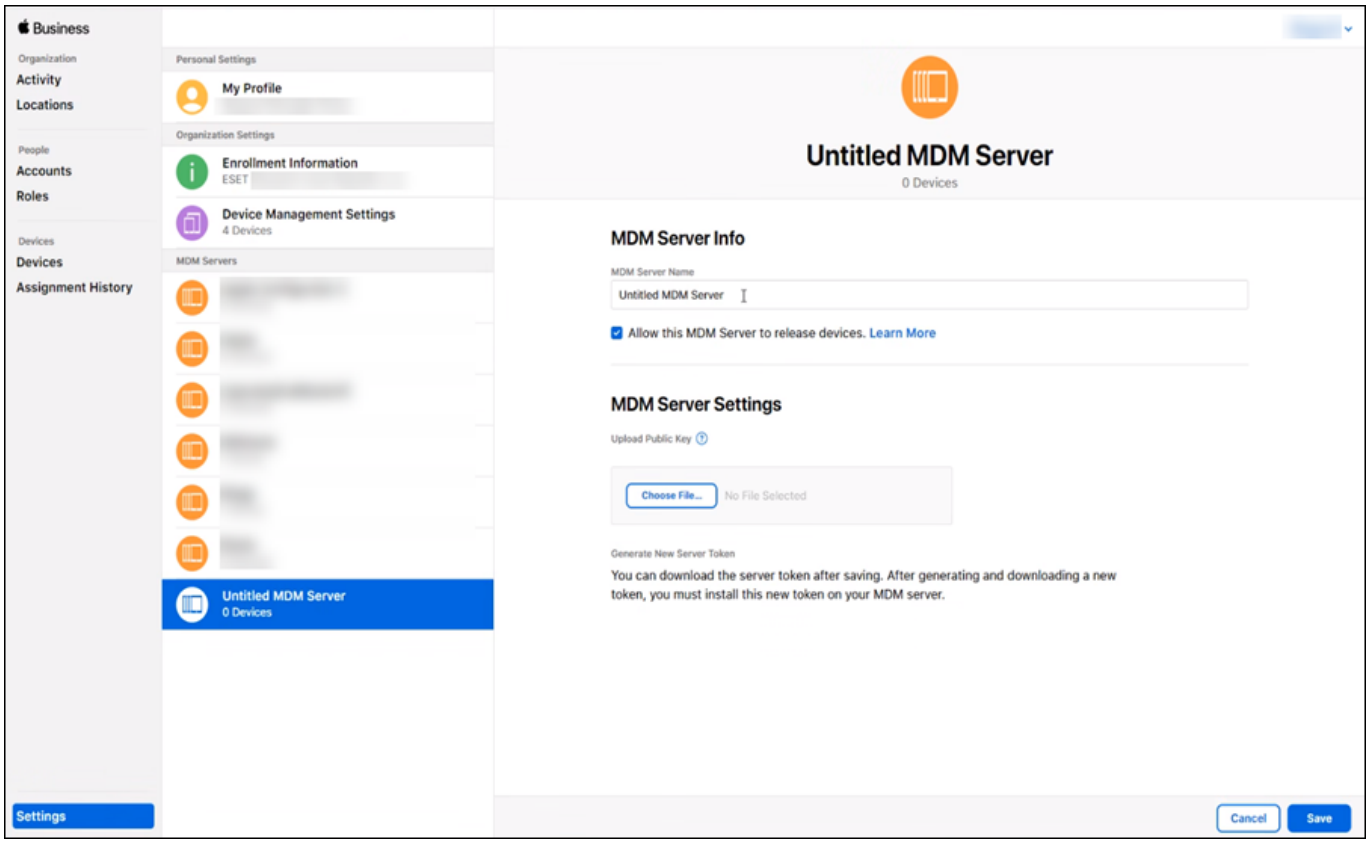
- Este programa está disponível somente em certos países. Visite a página da web Apple ABM para ver se o ABM está disponível no seu país.
- Os requisitos da Conta Apple ABM podem ser encontrados nesses sites: Requisitos do programa de implantação Apple e requisitos do Programa de inscrição de dispositivo Apple.
- Veja os requisitos detalhados de dispositivo ABM.

2. Entre em sua Conta Apple ABM (Se você não tiver uma Conta Apple ABM, poderá criar uma).

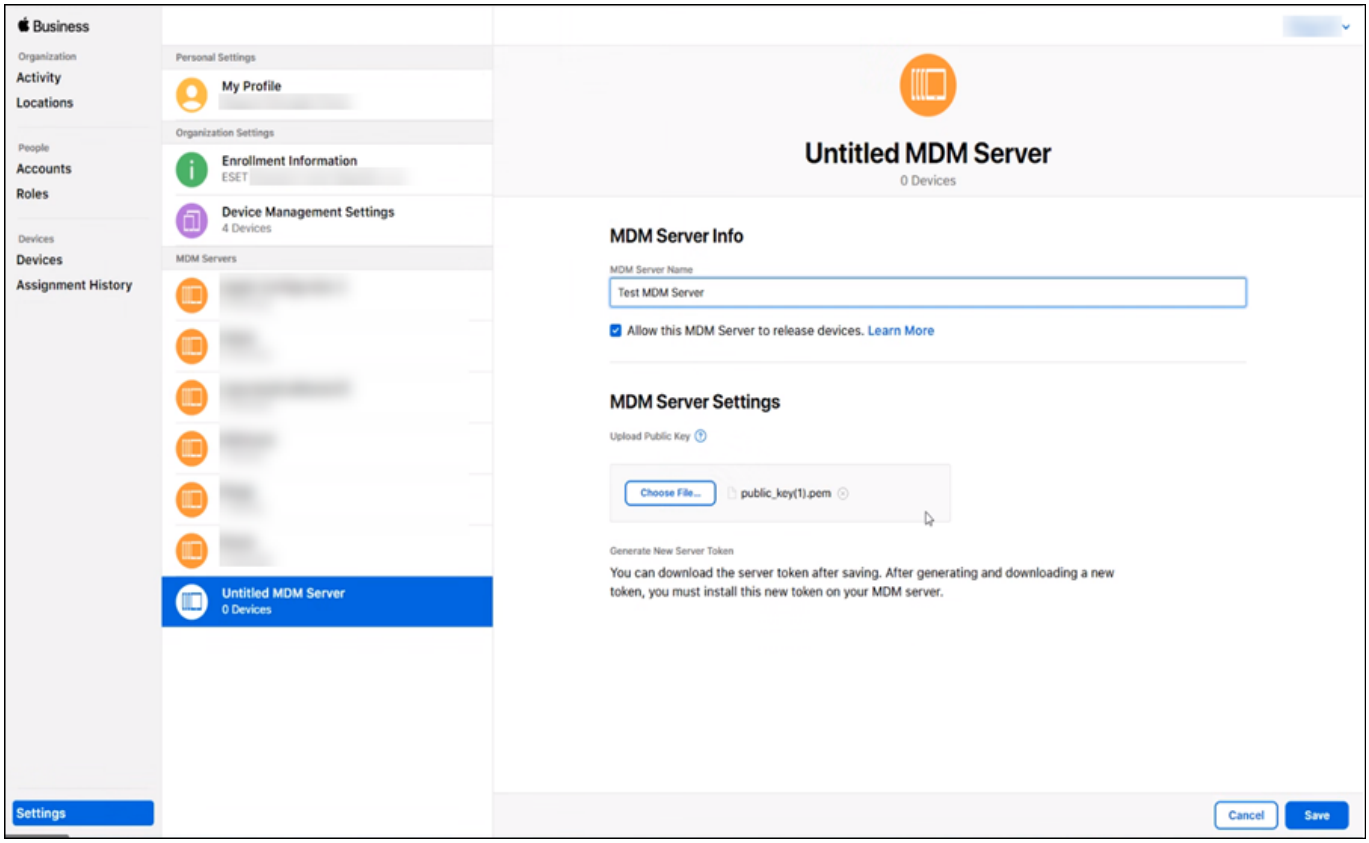
3. Na seção **Configurações de gerenciamento de dispositivo** selecione **Adicionar servidor MDM**.



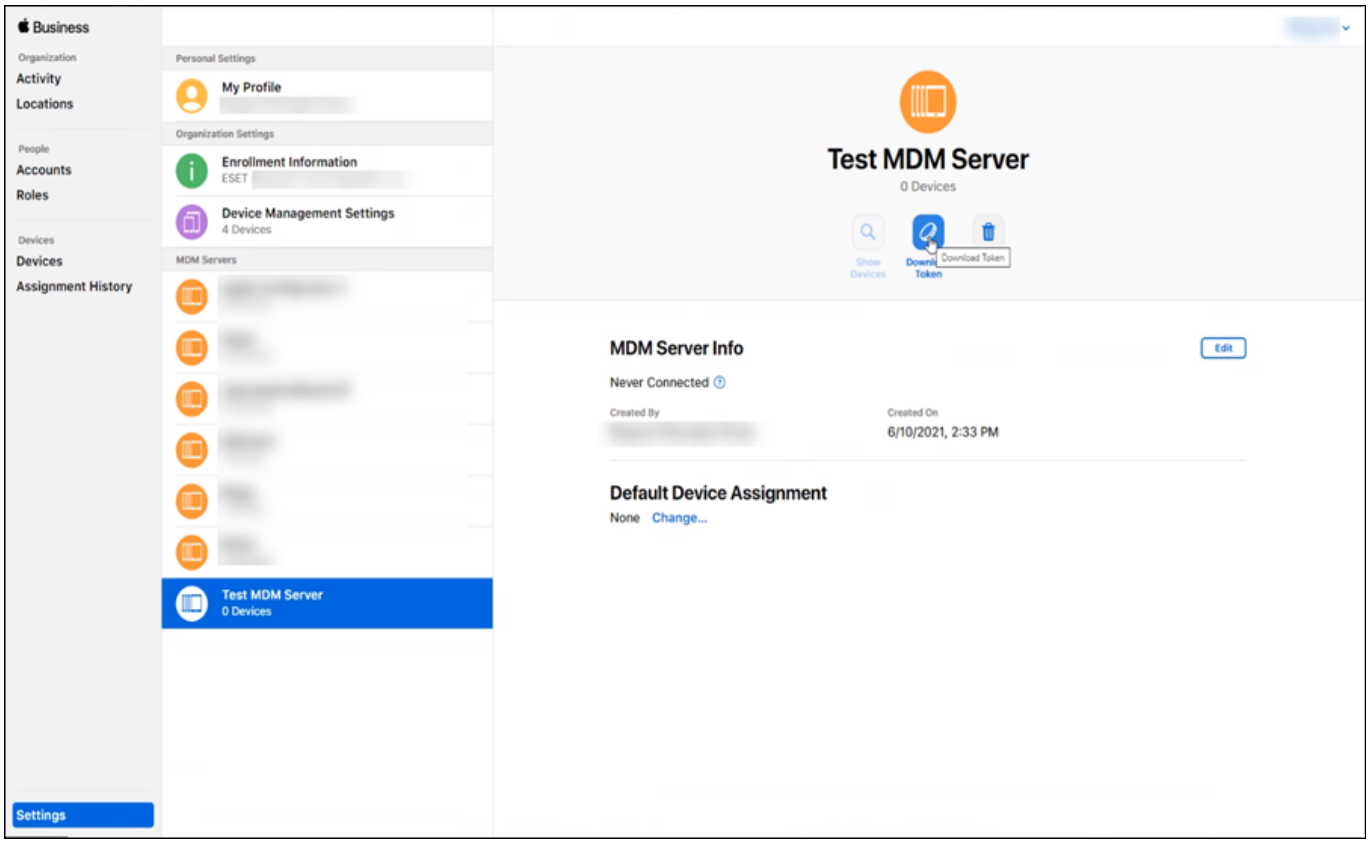
4. Na tela do Servidor MDM sem título, digite seu **Nome de servidor MDM**, por exemplo: "MDM_Server,".



5. Carregue sua chave pública para o portal ABM. Clique em **Escolher arquivo** e selecione o arquivo de chave pública (este é o arquivo de chave pública que você faz o download da tela de configurações ABM no ESET PROTECT) e clique em **Salvar**.



6. Agora clique no **Token de download** para fazer download do seu Token Apple ABM. Esse arquivo será carregado nas Configurações ESET PROTECT em **Token do Servidor ABM** > **Carregar**.

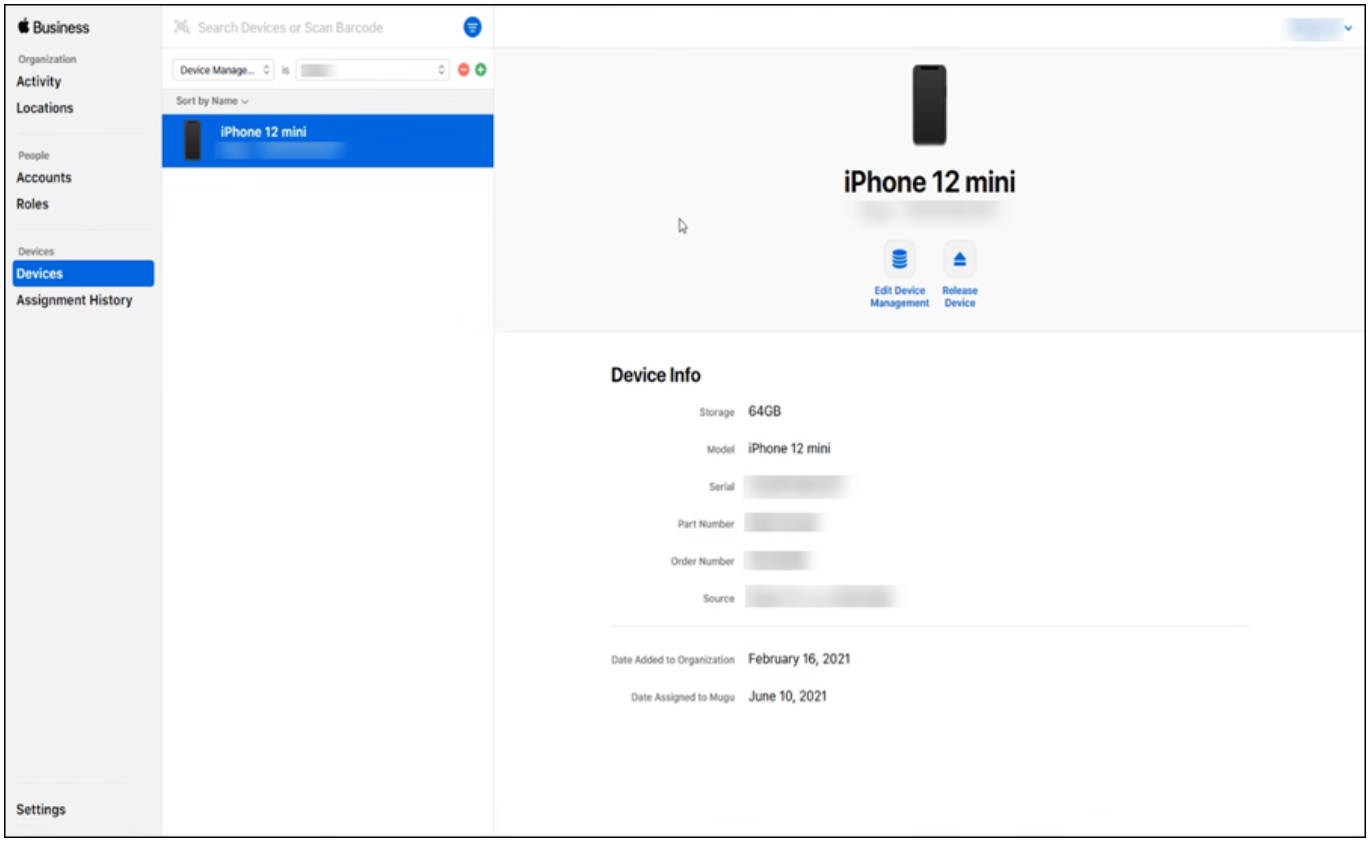


Adicionar dispositivo iOS no Apple ABM

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.

O intervalo de sincronização da Nuvem MDM está definido para 30 minutos, então você precisará aguardar esse período de tempo para que o dispositivo Apple apareça no ESET PROTECT.

Solução de problemas — adicionar novamente um dispositivo ABM removido

Se você removeu um dispositivo ABM da lista de dispositivos no ESET PROTECT Console da Web, siga as etapas abaixo para adicionar novamente o dispositivo ao ESET PROTECT Console da Web:

1. Cancele a atribuição do dispositivo do MDM Server no ABM. Não desconecte o dispositivo no portal ABM.

2. Aguarde 30 minutos.

3. Atribua o dispositivo ao MDM Server novamente.

Gerenciar dispositivos móveis

Depois de inscrever seus dispositivos móveis Android, você pode começar a gerenciá-los.

Além do gerenciamento de endpoint padrão disponível para todos os dispositivos endpoint, o gerenciamento de dispositivo móvel oferece vários recursos disponíveis apenas para o gerenciamento de dispositivo móvel.

Gerenciar dispositivos móveis por meio de tarefas do cliente

Ações Anti-Theft (aplica-se a dispositivos Android e iOS) – essas tarefas estão disponíveis apenas para dispositivos móveis gerenciados, como Localizar, Bloquear e Redefinição de fábrica. As tarefas permitem que o administrador localize o dispositivo móvel remotamente, bloqueie-o e, se a situação exigir, limpe o dispositivo móvel.

Veja todas as tarefas do cliente para dispositivos móveis.

> **Gatilhos de tarefas do cliente de dispositivo móvel**
> Você pode usar apenas esses gatilhos para tarefas de cliente de dispositivo móvel:
> • Assim que possível
> • Gatilho de grupo dinâmico ingressado
> As tarefas do cliente com gatilhos diferentes dos acima falharão com a mensagem **Tipo de gatilho sem suporte**.

Gerenciar dispositivos Android por meio de políticas

Atribua a política **ESET Endpoint Security for Android**, que permite a você personalizar cada uma das configurações de gerenciamento disponíveis do Android. Por exemplo:

- Controle de Web
- Gerenciamento de atualização do sistema operacional
- Instalação de aplicativo remoto – você pode forçar remotamente o dispositivo móvel a instalar os aplicativos necessários adicionando-os à lista na política:

    1.Navegue até sua política **ESET Endpoint Security for Android** aplicada (ou crie uma nova política para essa finalidade).

    2.Em **Controle de aplicações**, ative a configuração **Ativar controle de aplicações**.

    3.Clique em **Lista de aplicativos** e adicione os aplicativos que você deseja instalar remotamente no dispositivo móvel depois de aplicar a política.

Quando você registra um dispositivo com Android 9 e posteriormente via Microsoft Intune ou VMware Workspace ONE, o ESET Endpoint Security para Android versão 3.5 e posterior ignora as seguintes configurações de política:

- Segurança do dispositivo
- Controle de aplicações
- Anti-Theft

Gerenciar dispositivos iOS por meio de políticas

O gerenciamento do dispositivos iOS permite que a funcionalidade CloudMDM também inscreva e gerencie dispositivos iOS no ESET PROTECT no modo padrão ou de inscrição ABM.

Atribua a política **ESET MDM para iOS/iPadOS**, onde você pode personalizar cada uma das configurações de gerenciamento iOS disponíveis. Por exemplo:

- Configurar a conta Exchange ActiveSync
- Impor restrições no iOS

Controle de web para Android

Use o ESET Endpoint Security for 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 for Android**.
3. Na seção **Proteção da Web** da política, expanda o Controle de web e habilite a alternância **Controle de web**.
4. Links ou categorias específicos da lista de permissões e da lista de proibições. 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.

> Essa funcionalidade requer o ESET Endpoint Security for Android versão 3.0, Android versão 8.x e posterior, e o dispositivo Android deve estar inscrito em um 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 for Android**.
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**:
  - **Automático** – A atualização do sistema operacional Android será executada sem atraso.
  - **Com janela** – A atualização do sistema operacional Android será executada apenas durante uma janela de

manutenção especificada configuração **Janela de manutenção diária**.

o**Adiado 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.

Criar uma política para iOS - 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 que representa a versão do iOS, por exemplo, a versão 11.0 e posterior do iOS 

.

- 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.

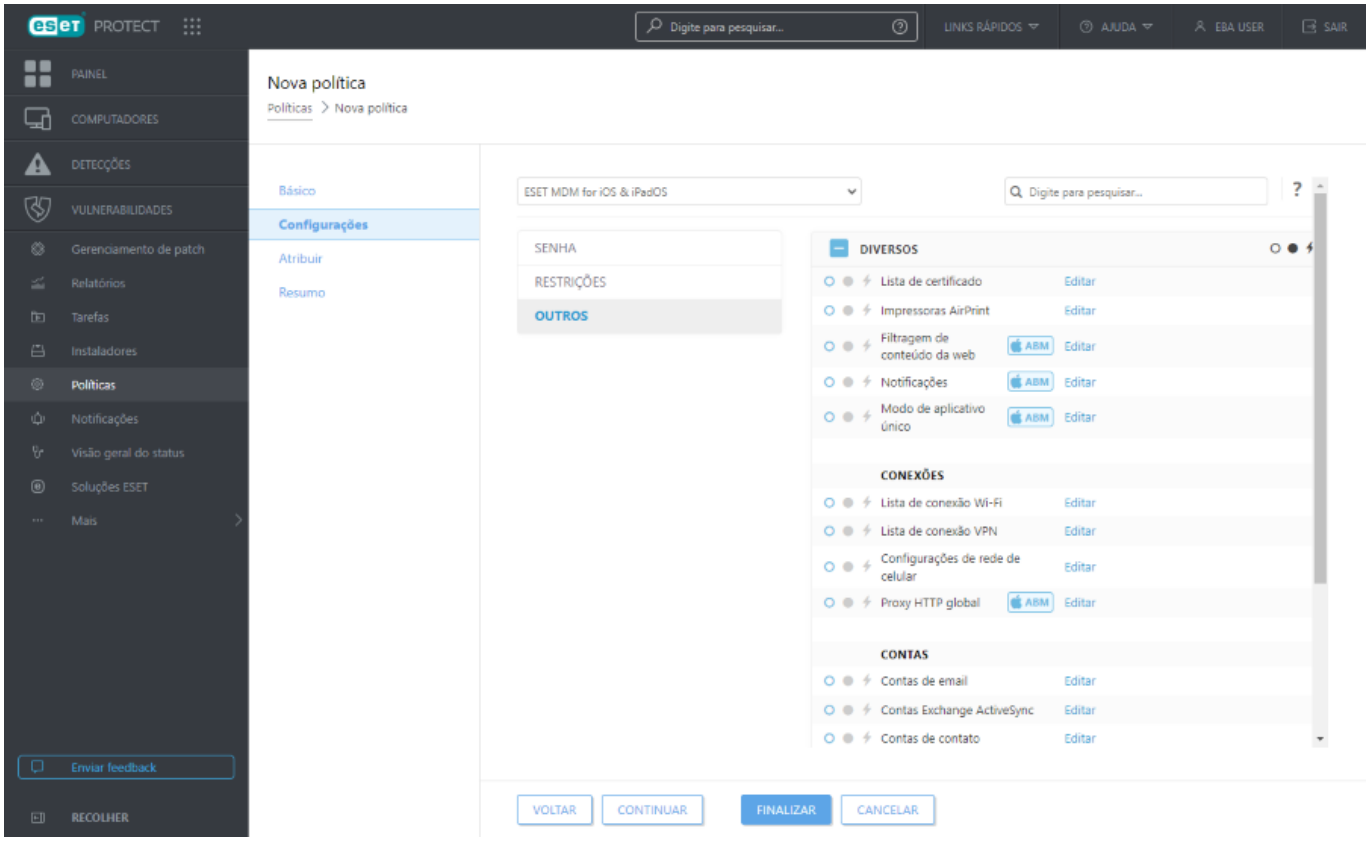
> Antes de começar a configurar essa política, verifique se você já executou as etapas descritas em inscrição de dispositivo móvel.

Básico

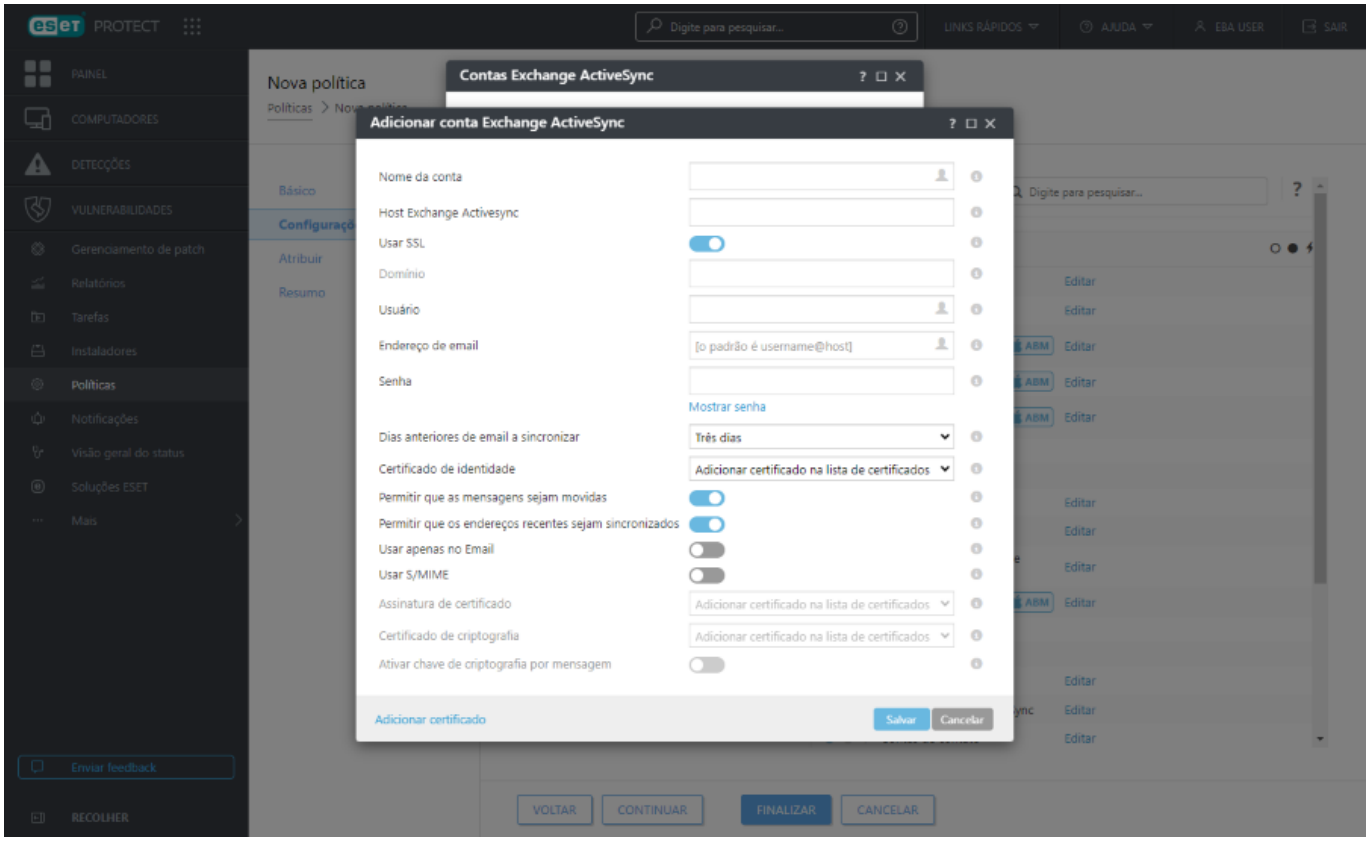
Digite um **Nome** para a política. O campo **Descrição** é opcional.

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.

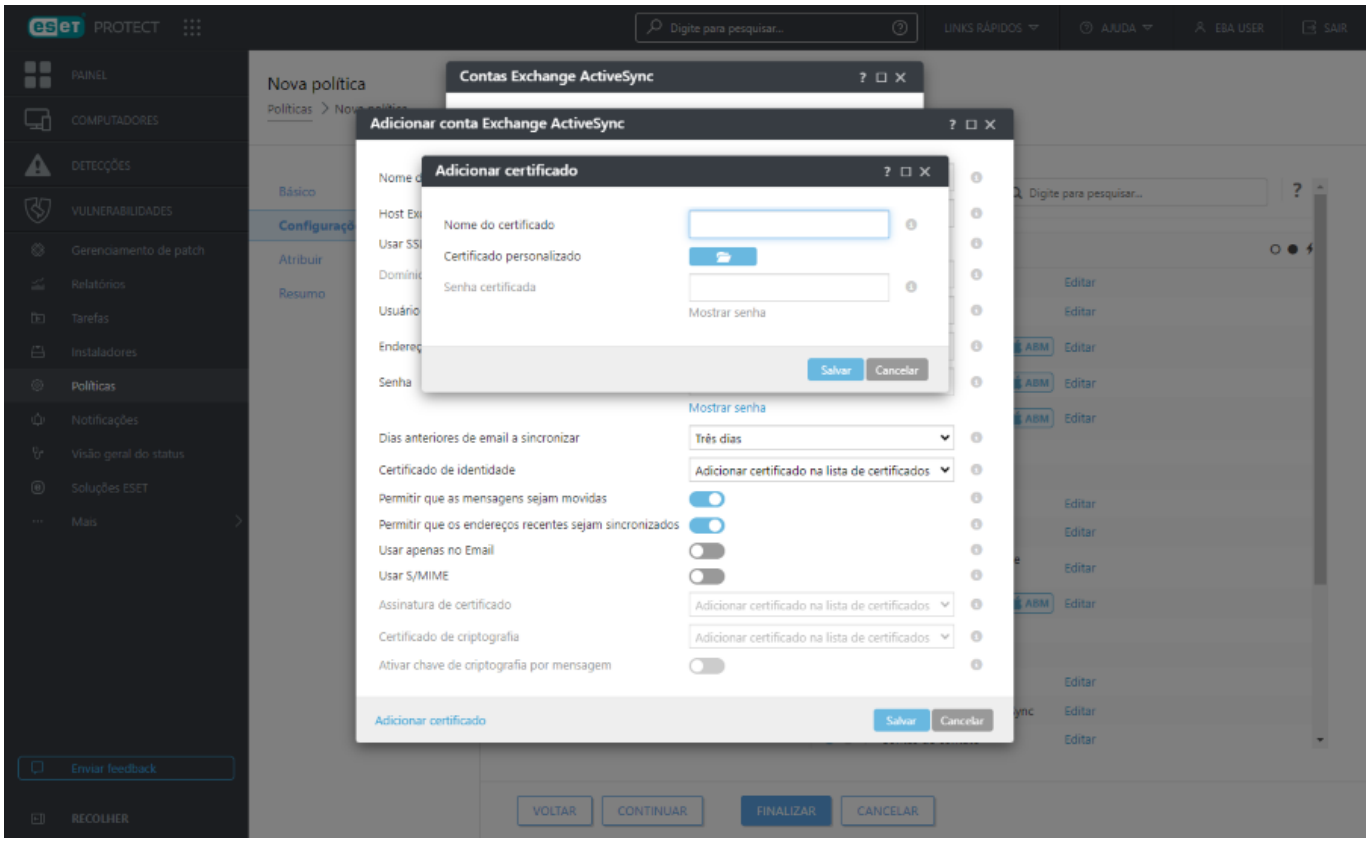
• **Permitir que os endereços recentes sejam sincronizados** - Se esta opção for ativada, o usuário pode sincronizar endereços usados recentemente em dispositivos diferentes.

• **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**.

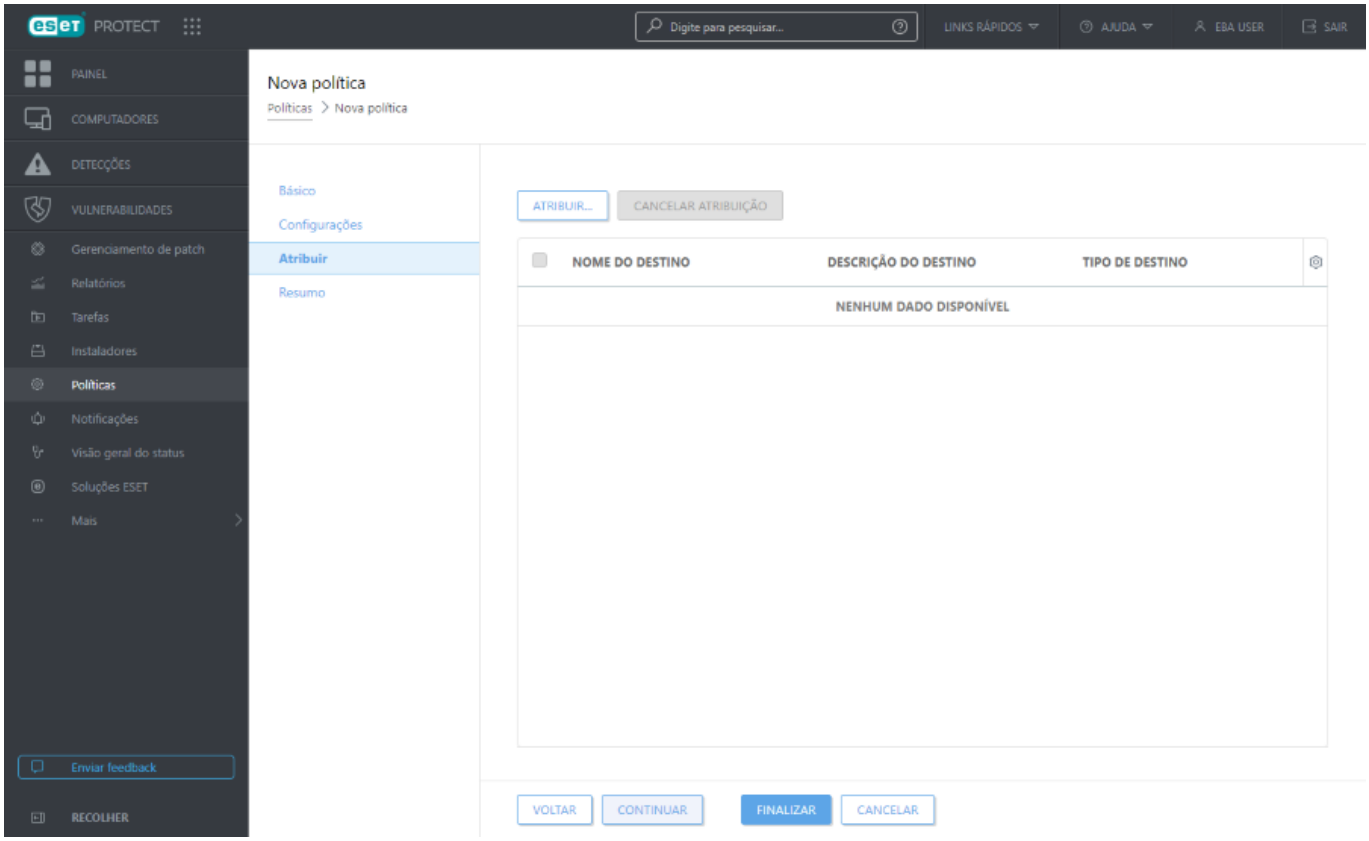


- **Adicionar certificado**- É possível adicionar certificados Exchange específicos (Identidade do usuário, Assinatura digital ou Certificado de criptografia) se necessário.

> 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.

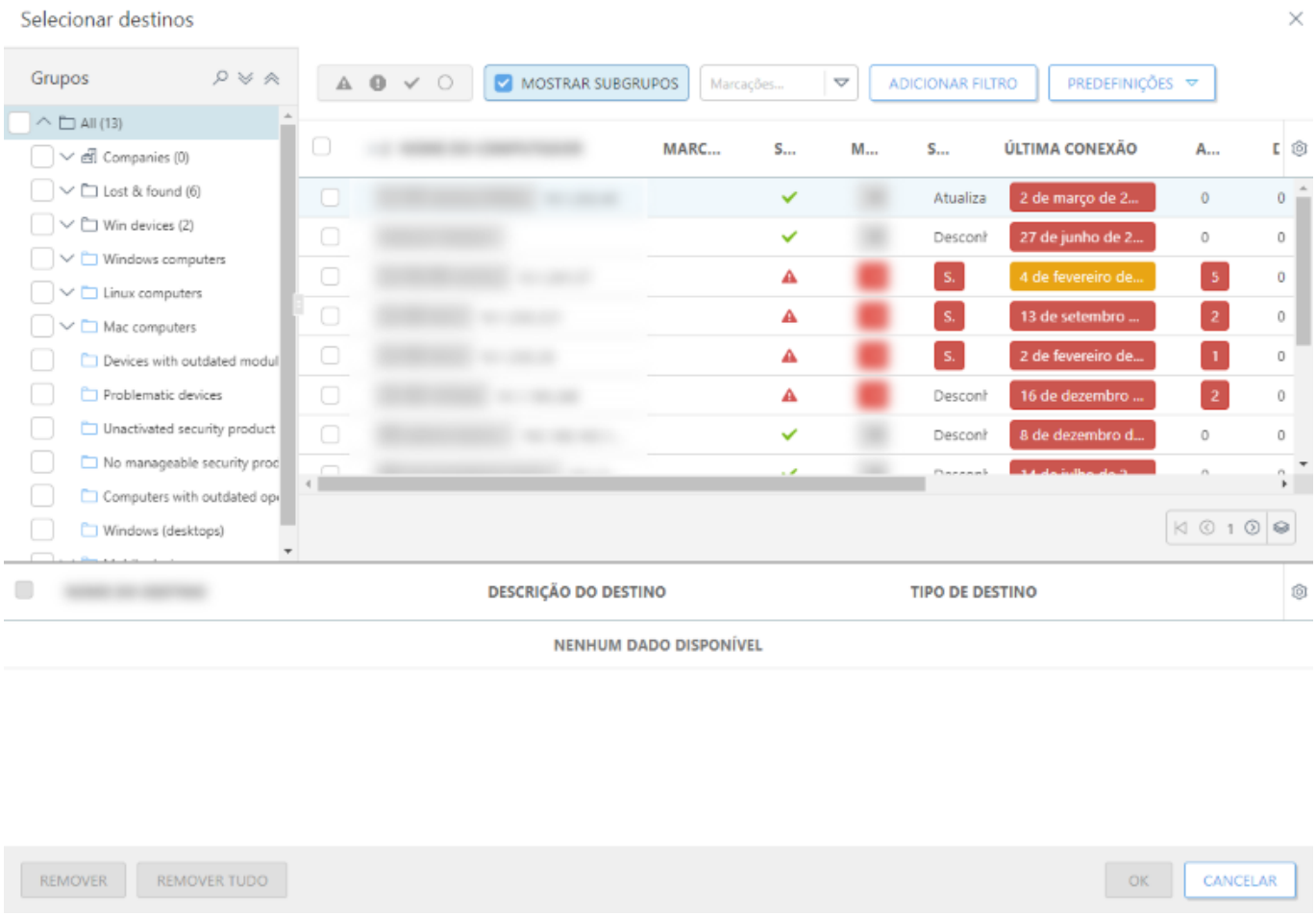
Atribuir

Especifique os clientes (computadores individuais 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 ESET PROTECT.

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 às 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.

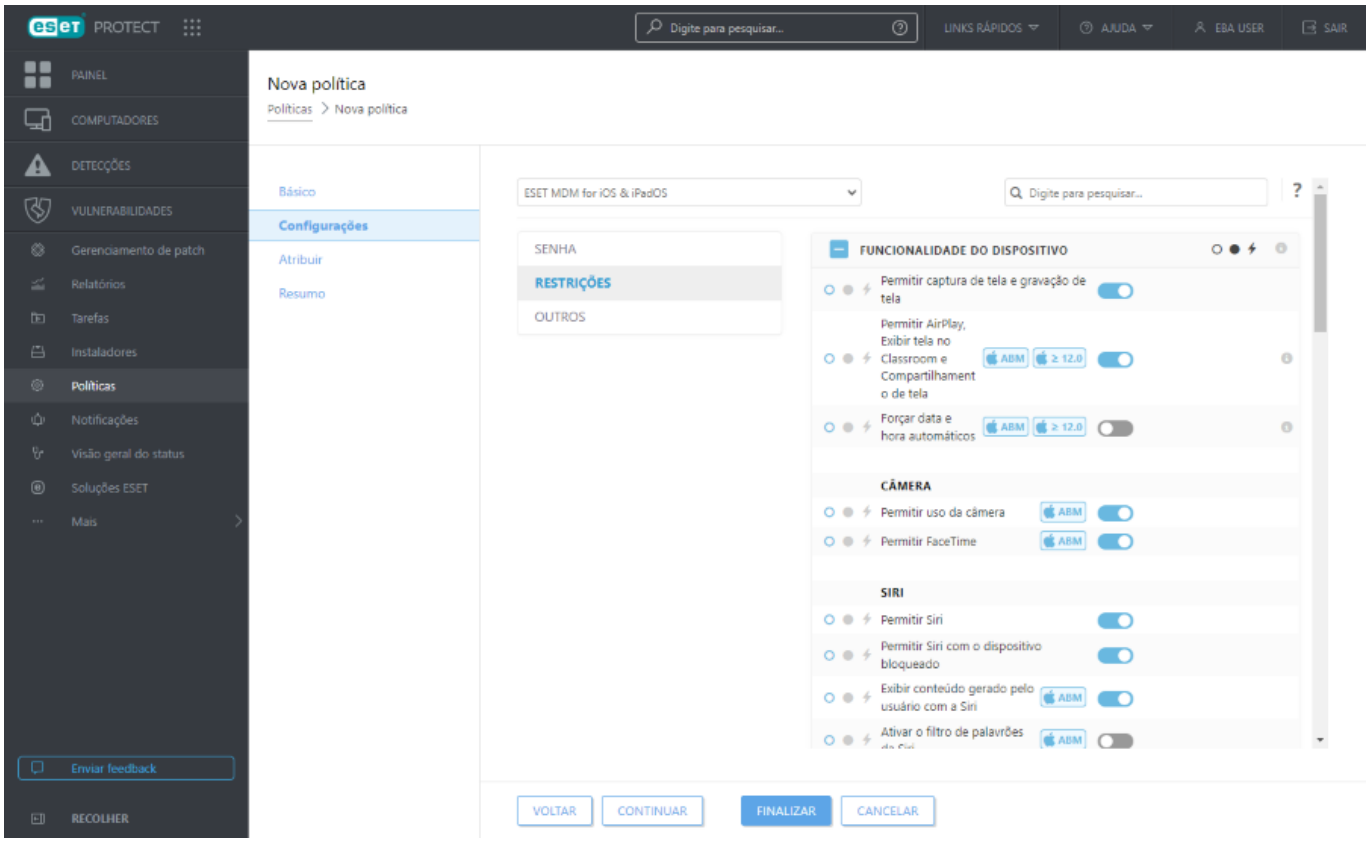
O seguinte é um exemplo de como desabilitar os **aplicativos** de **câmera e** FaceTime e adicionar detalhes da conexão Wi-Fi na lista, para que o dispositivo móvel iOS conecte a uma rede Wi-Fi sempre que a rede for detectada. Se você usar a opção Ingressar automaticamente, dispositivos móveis iOS serão conectados a essa rede por padrão. A configuração de política irá substituir a seleção manual de uma rede Wi-Fi por um usuário.

Básico

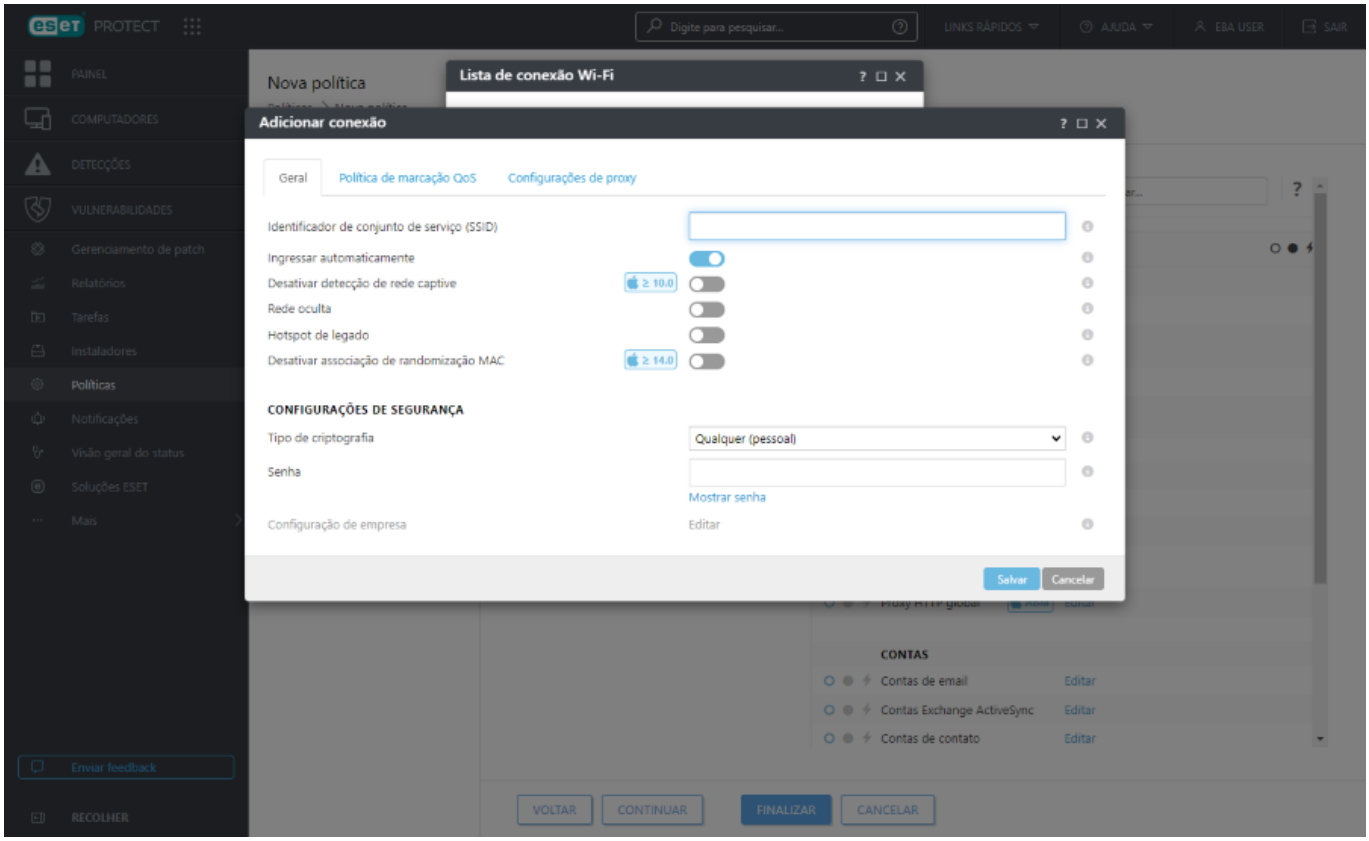
Digite um **Nome** para a política. O campo **Descrição** é opcional.

Configurações

Selecione **ESET MDM para iOS e iPadOS**, clique em **Restrições** para ver as 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

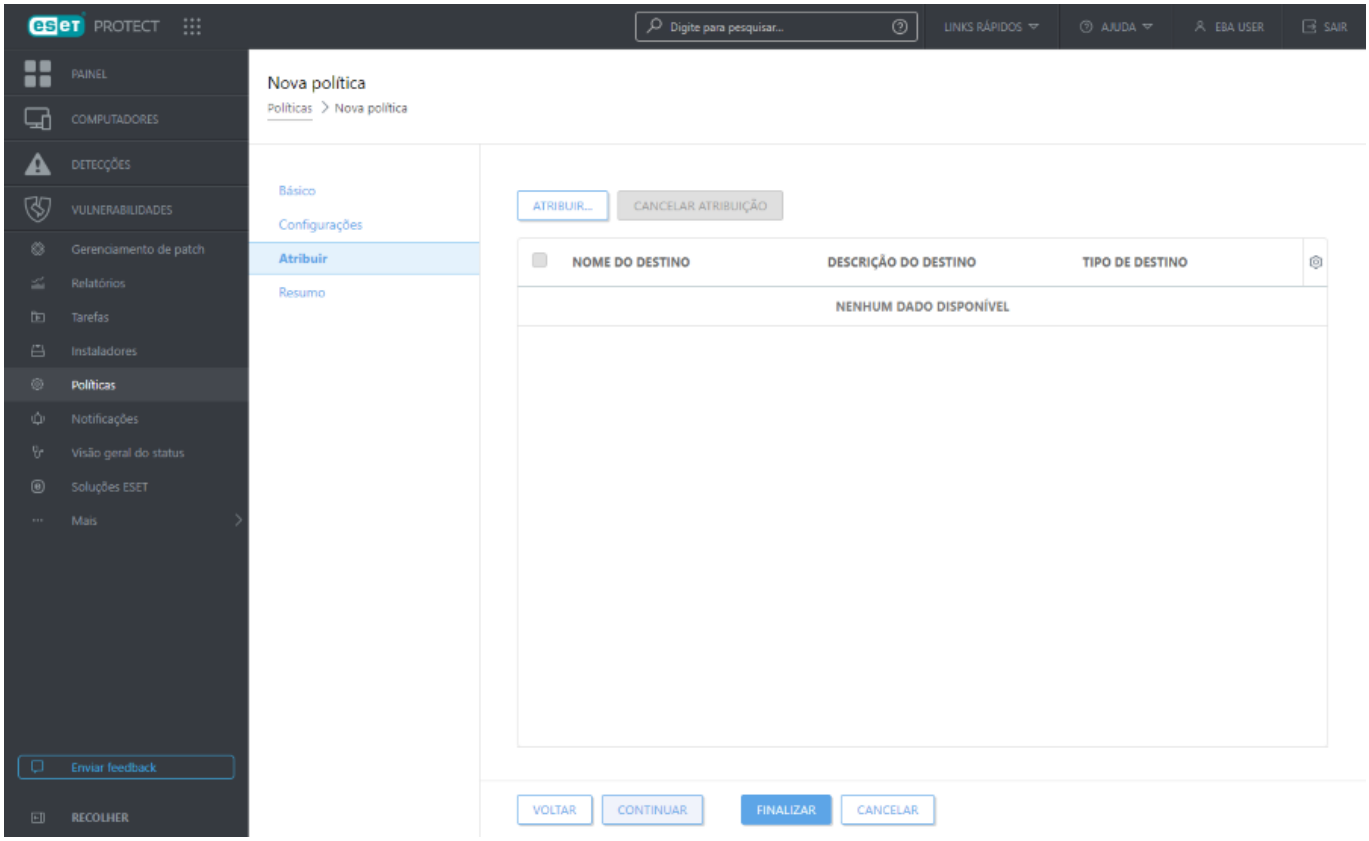
- **Tipo de criptografia** - Selecione a criptografia adequada na lista suspensa, certifique-se de que esse valor combina exatamente com as capacidades da rede Wi-Fi.

- **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.

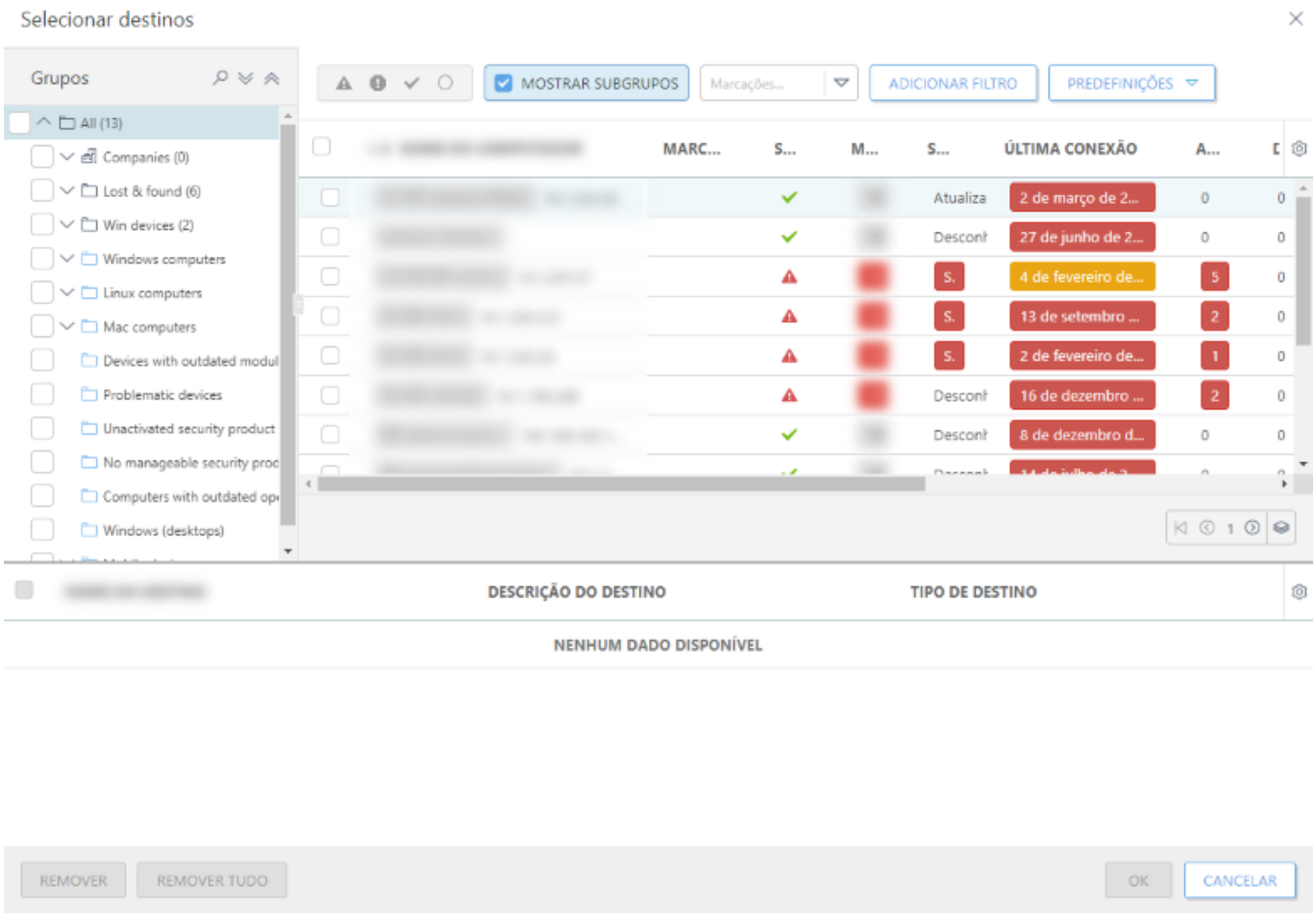
Atribuir

Especifique os clientes (computadores individuais 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 ESET PROTECT.

Perfis de configuração Cloud 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	Os perfis de Wi-Fi enviam as configurações de Wi-Fi corporativo diretamente para dispositivos gerenciados para 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	Os perfis do Exchange ActiveSync permitem que os usuários finais acessem a infraestrutura corporativa de e-mail por 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.

Migração para o Cloud MDM (do ESET PROTECT On-prem)

As etapas a seguir vão ajudar você a migrar dispositivos móveis do ESET PROTECT On-Prem para o ambiente ESET PROTECT:

Pré-requisitos

- Ambiente ESET PROTECT On-Prem funcionando com o componente de Gerenciamento de dispositivo móvel
- Ambiente de trabalho ESET PROTECT
- Conta ESET PROTECT 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 On-Prem versão 10.0+
- A migração de dispositivos gerenciados iOS requer a remoção manual da inscrição no ESET PROTECT On-Prem e a inscrição no ESET PROTECT

1. Abrir o Console Web ESET PROTECT.

2. Clique em **Mais** > **Configurações** > **Migração de dispositivos móveis do ESET PROTECT On-Prem**.

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. Abrir o Console Web ESET PROTECT On-Prem.

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 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. Depois que o dispositivo móvel for migrado, ele será conectado ao ESET PROTECT, e será visível na seção **Computadores** do Web Console ESET PROTECT.

16. Depois de migrar o dispositivo para o ambiente ESET PROTECT com segurança, ele poderá ser removido com segurança do Web Console ESET PROTECT On-Prem.

17. Depois de migrar com sucesso todos os dispositivos móveis para o ambiente ESET PROTECT, você poderá desativar com segurança o componente de Gerenciamento de dispositivo móvel.

ESET PROTECT Cenários de migração

Cenários de migração para migração para o ESET PROTECT.

Nesta seção vamos revisar os cenários de migração para a transição de outros produtos ESET para o ESET PROTECT. Clique no link abaixo que melhor descreve seu cenário.

1. Eu tenho produtos de segurança ESET Endpoint não gerenciados na minha rede e quero começar a gerenciá-los com o ESET PROTECT.

2. Atualmente gerencio minha rede com o ESET PROTECT on-prem e quero migrar para o ESET PROTECT.

3. Atualmente gerencio minha rede com o ESET PROTECT e quero migrar para o ESET PROTECT.

Se você gerenciar dispositivos criptografados com o ESET Full Disk Encryption, siga essas etapas para evitar a perda de dados de recuperação.
1.Antes da migração – navegue para **Visão geral do status** > **Criptografia**. Aqui você pode **Exportar** seus **Dados de recuperaçãoESET Full Disk Encryption** atuais.
2.Depois da migração – **Importar** os **Dados de recuperação ESET Full Disk Encryption** no seu novo console de gerenciamento.
Se você não conseguir realizar essas etapas, será preciso remover a criptografia dos dispositivos gerenciados antes da migração. Depois da migração, você pode criptografar os dispositivos gerenciados do Web Console ESET PROTECT.

Eu tenho produtos ESET Endpoint não gerenciados na minha rede e quero começar a gerenciá-los com o ESET PROTECT.

Não é possível atualizar a versão 4.5 ou versões anteriores de produtos ESET Server com o Live Installer. Você deve ter produtos ESET versão 6 ou versões posteriores instalados para atualizar para o ESET PROTECT.

Siga as etapas abaixo para encontrar e adicionar produtos não gerenciados no ESET PROTECT:

1. Crie sua instância ESET PROTECT.

2. Criar um novo Instalador e selecionar o produto a ser instalado com base em quais produtos Endpoint estão presentes na sua rede no momento.

3. As configurações de políticas e grupos para clientes podem ser definidas no instalador. Se nenhuma política for selecionada como parte do instalador e nenhuma política for aplicada a qualquer grupo no ESET PROTECT, a configuração atual de seus produtos Endpoint não será sobrescrita e pode ser exportada e convertida posteriormente em uma política.

4. Use os instaladores na sua rede. O Live Installer vai instalar o Agente ESET Management e atualizar seus produtos Endpoint existentes.

O Live Installer requer uma conexão direta com a internet para fazer download dos componentes necessários. Depois da instalação ser concluída você pode alterar a conexão a ser encaminhada via proxy.

5. Depois da instalação ser concluída com sucesso e dos dispositivos estarem conectados ao ESET PROTECT, você pode começar a gerenciá-los com seu ESET PROTECT.

6. Se nenhuma política fazia parte do instalador ou se aplicava a qualquer grupo no ESET PROTECT, agora você pode exportar a configuração de seus Produtos Endpoint.

7. Para fazer isso, navegue até **Tarefas** e crie uma nova Tarefa de definição de configuração do produto gerenciado de exportação.

8. Na parte **Configurações** selecione**Produto: Todos** e como **Destino** selecione todos os dispositivos dos quais você quer exportar a configuração.

9. Aguarde até que a tarefa seja executada em todos os dispositivos selecionados.

10. Navegue até **Detalhes** > **Configuração** do dispositivo específico e abra a configuração específica do produto Endpoint.

11. Aqui você pode revisar as configurações exportadas e, se estiver satisfeito, selecionar **Converter para Política**.

12. O assistente de política será aberto e lá você poderá editar o **Nome** para revisão da política e ajustar algumas das configurações, se necessário, e clicar em **Concluir** para salvar.

13. Repita este procedimento para cada produto Endpoint.

14. Depois de todas as configurações de produto serem convertidas você pode continuar ao aplicar a política aos respectivos dispositivos do cliente, de forma que a configuração será bloqueada e o usuário do dispositivo não será capaz de alterá-la.

Migração parcial do ESET PROTECT on-prem para ESET PROTECT

A migração do Servidor ESET PROTECT local para o ESET PROTECT é parcial — consulte a tabela abaixo:

Você pode migrar:	Não é possível migrar:
• Agentes ESET Management (computadores gerenciados) • grupos estáticos • políticas • modelos de grupo dinâmico • modelos de relatório • dispositivos móveis (somente Android)	• todo o banco de dados • Grupos dinâmicos (mas você pode migrar modelos de grupo dinâmico) • detecções • relatórios de auditoria • notificações • tarefas e acionadores • instaladores • relatórios agendados/gerados (mas você pode migrar modelos de relatório) • marcações • iOS dispositivos móveis

O ESET PROTECT não é compatível com ESET Inspect On-Prem mas é compatível com o ESET Inspect. Se você migrar do ESET PROTECT On-Prem para o ESET PROTECT, você não será capaz de gerenciar o ESET Inspect On-Prem do ESET PROTECT, mas poderá gerenciar o ESET Inspect do ESET PROTECT.

Siga as etapas abaixo para migrar do Servidor ESET PROTECT local para o ESET PROTECT:

Se você tiver uma conta MSP, siga as etapas para a Migração MSP para a nuvem.

I. Crie uma nova instância do ESET PROTECT

II. Migrar políticas do ESET PROTECT On-Prem para o ESET PROTECT

III. Migrar modelos de grupo dinâmico do ESET PROTECT On-Prem para o ESET PROTECT

IV. Migrar modelos de relatório do ESET PROTECT On-Prem para o ESET PROTECT

V. Migrar computadores gerenciados do ESET PROTECT On-Prem para o ESET PROTECT

V.I. Migrar a estrutura de grupo estático usando a ferramenta de exportação de computadores

V.II. Migrar os computadores gerenciados (Agentes ESET Management) usando a política de migração

VI. Migrar dispositivos móveis

VII. Configurar usuários ESET PROTECT no ESET Business Account.

VIII. Adicionar usuários ESET Business Account ao Web Console ESET PROTECT

IX. Descomissionar o Servidor ESET PROTECT local

Solução de problemas após a migração

Se você gerenciar dispositivos criptografados com o ESET Full Disk Encryption, siga essas etapas para evitar a perda de dados de recuperação.
1.Antes da migração – navegue para **Visão geral do status** > **Criptografia**. Aqui você pode **Exportar** seus **Dados de recuperaçãoESET Full Disk Encryption** atuais.
2.Depois da migração – **Importar** os **Dados de recuperação ESET Full Disk Encryption** no seu novo console de gerenciamento.
Se você não conseguir realizar essas etapas, será preciso remover a criptografia dos dispositivos gerenciados antes da migração. Depois da migração, você pode criptografar os dispositivos gerenciados do Web Console ESET PROTECT.

Não exportar nenhuma política do Agente ESET Management.
Certifique-se de cancelar totalmente a atribuição de todas as políticas ativas do Agente antes da migração.

I. Crie uma nova instância do ESET PROTECT

Pré-requisitos

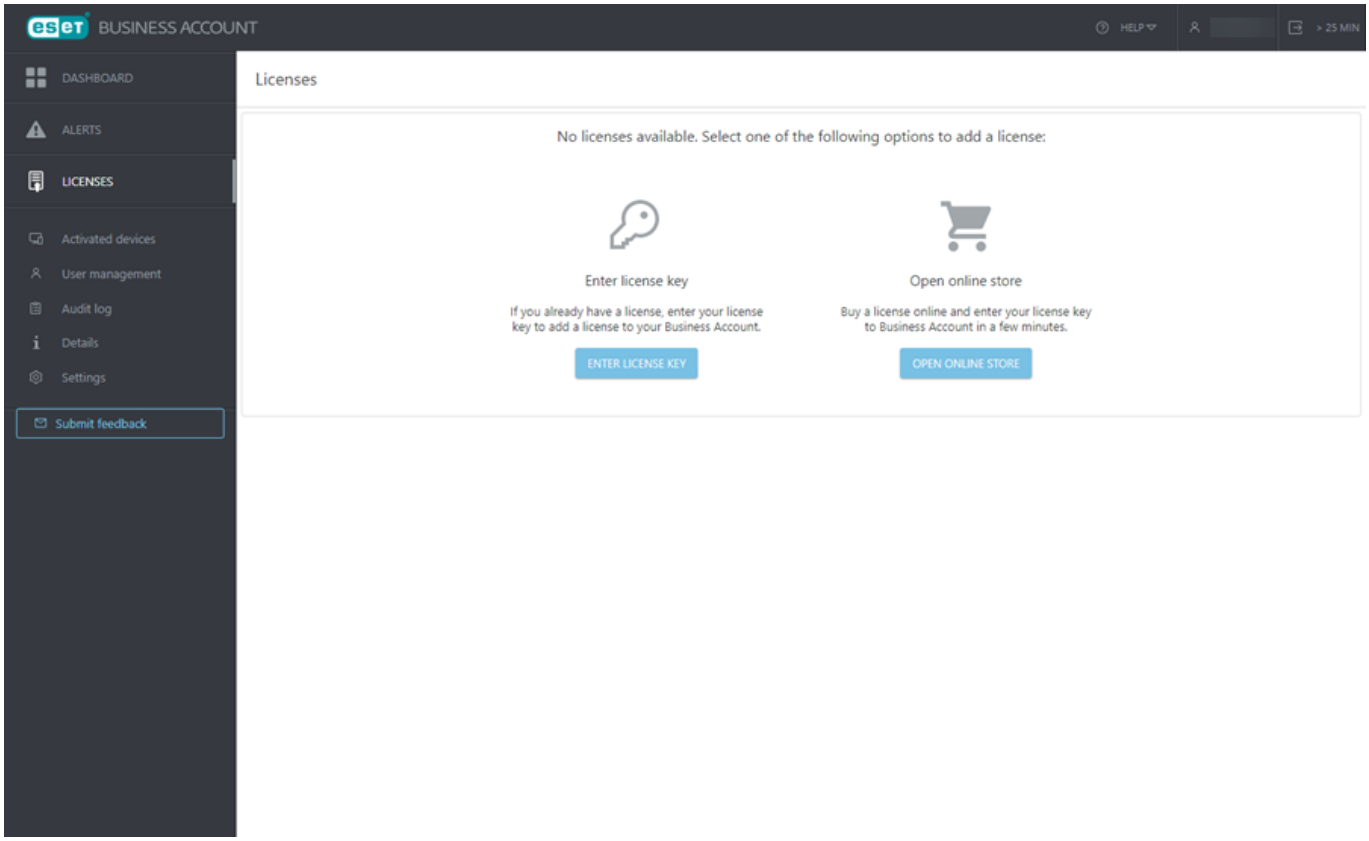
- Uma conta de Superusuário no ESET Business Account.
- Uma licença elegível para o ESET PROTECT.

Se as suas contas EBA e EMA2 estiverem registradas no mesmo endereço de e-mail, o ESET PROTECT pode ser ativado de apenas uma conta. A conta (EBA ou EMA2) para a qual você escolher criar a instância ESET PROTECT será a única que você pode usar para ativar ou remover a instância.

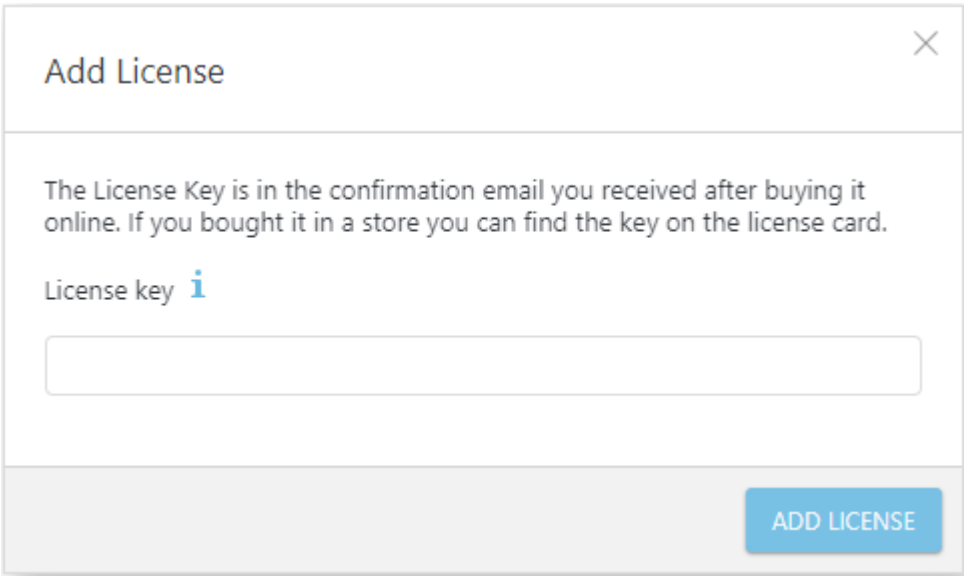
Criar uma nova instância ESET PROTECT

1. Abra o ESET Business Account e entre (ou crie uma nova conta).

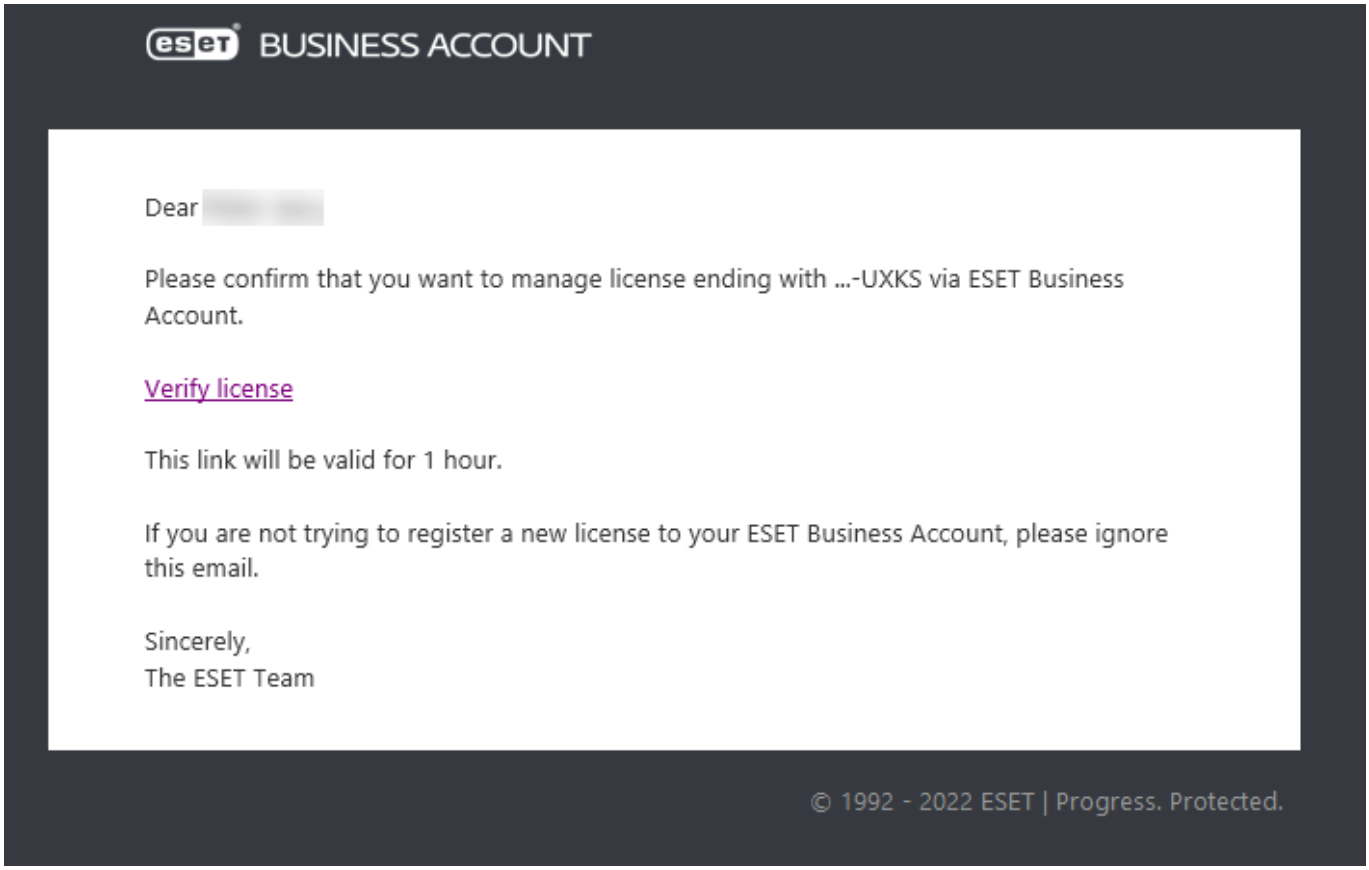
2. Clique em **Licenças** > **Inserir chave de licença**.



3. Na janela **Adicionar licença**, insira sua **Chave de licença** ESET PROTECT e clique em **Adicionar licença**.



4. Você receberá um e-mail de verificação (se não receber o e-mail, siga as instruções do artigo da Base de conhecimento). Clique em **verificar licença**.



5. No **Painel** clique em **Ativar** sob **ESET PROTECT**.

Verifique a configuração de idioma do seu ESET Business Account. Alguns elementos da janela principal do programa do ESET PROTECT são definidos na primeira vez que você define o idioma nas configurações de idioma ESET Business Account e não podem ser alterados posteriormente.

6. Uma janela **Ativar ESET PROTECT** será aberta. Leia os Termos de uso e marque a caixa de seleção se você concordar.

7. Selecione um local do centro de dados para sua instância do ESET PROTECT que seja o mais próximo do local de sua rede gerenciada e clique em **Continuar**.

Depois de selecionado você não conseguirá alterar a localização do centro de dados da sua instância ESET PROTECT.

8. Sua instância ESET PROTECT será criada. Você pode aguardar alguns minutos até que ele seja criado ou você pode sair e você será notificado por email assim que a instância do ESET PROTECT estiver disponível.

9. Clique em **Continuar**. Alternativamente, clique em **Painel**, clique em **Abrir** no bloco ESET PROTECT para abrir uma nova guia com o Web Console ESET PROTECT.

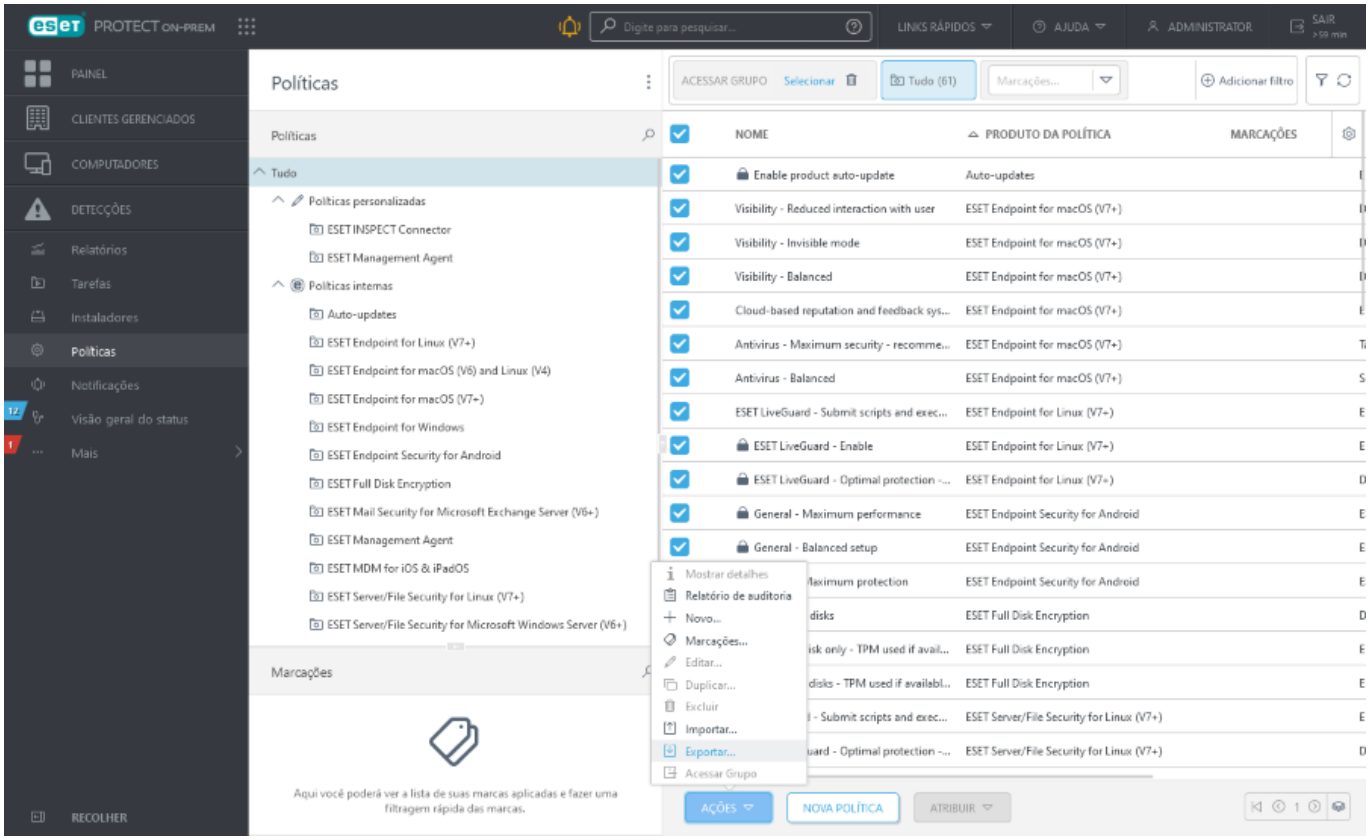
O ESET PROTECT sincroniza sua estrutura ESET Business Account com a árvore do Grupo estático em **Computadores** no Web Console.

II. Migrar políticas do ESET PROTECT On-Prem para o ESET PROTECT

1. Entre no seu ESET PROTECT On-Prem.

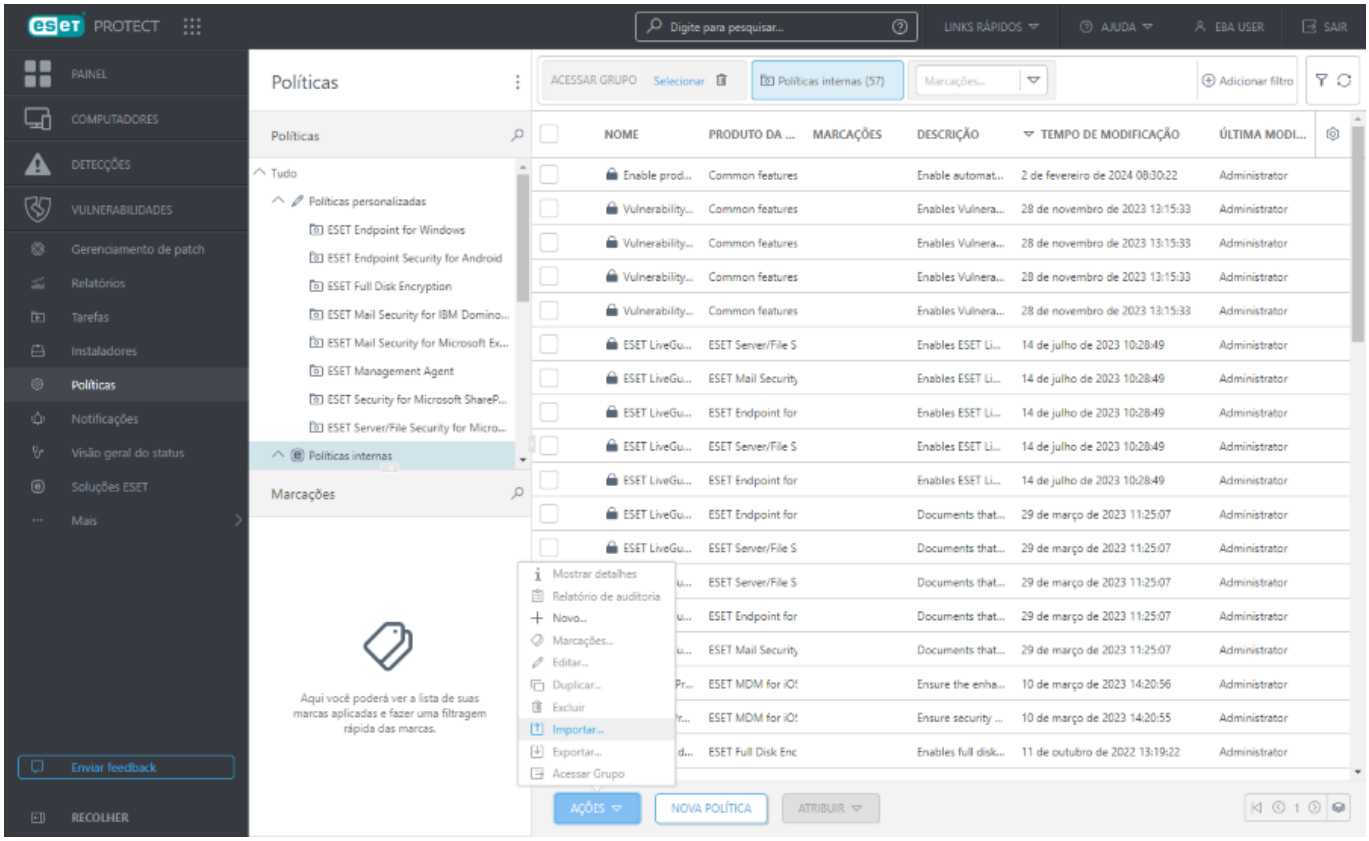
2. Em seu ESET PROTECT On-Prem, selecione **Políticas** > **Todas** > marque a caixa de seleção no cabeçalho da tabela (ou selecione as caixas de seleção ao lado das políticas que deseja exportar) e clique em **Ações** > **Exportar**.

Não exportar nenhuma política do Agente ESET Management.
Certifique-se de cancelar totalmente a atribuição de todas as políticas ativas do Agente antes da migração.



3. Salve o arquivo *.dat* com a lista de Políticas.

4. Em ESET PROTECT, clique em **Políticas** > **Ações** > **Importar** e selecione o arquivo *.dat* com a lista de políticas exportada do ESET PROTECT On-Prem na etapa 2 e, em seguida, clique em **Importar** para importar para o ESET PROTECT.



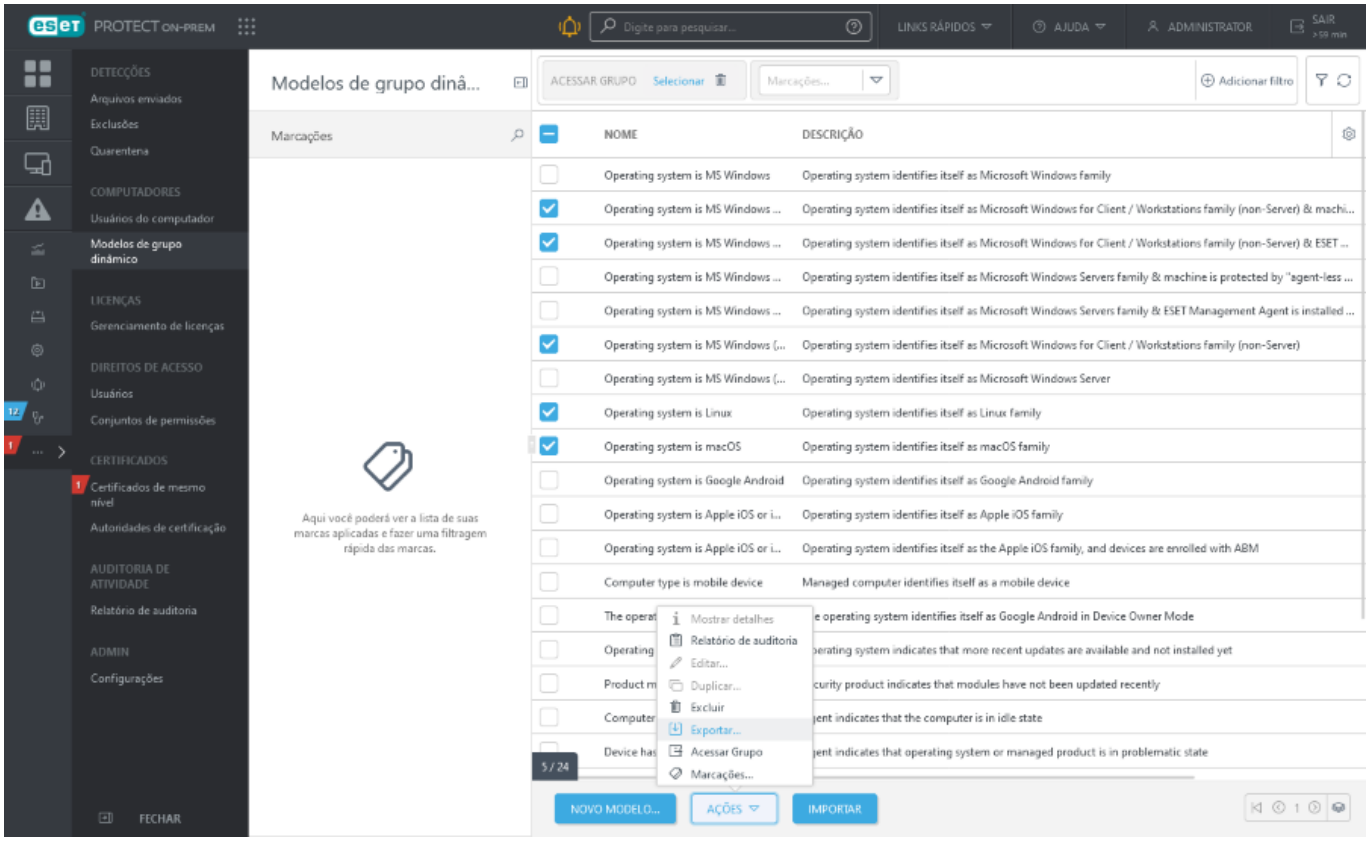
5. As políticas importadas vão aparecer sob **políticas personalizadas**. Depois da migração de computadores do ESET PROTECT On-Prem para o ESET PROTECT, as políticas que foram atribuídas aos computadores no ESET PROTECT On-Prem não serão preservadas. Depois de importar as Políticas para o ESET PROTECT, você pode atribuí-las aos computadores importados no ESET PROTECT.

Tenha cuidado ao aplicar políticas a computadores:
a)No seu ESET PROTECT On-Prem: Faça a lista de políticas aplicadas e sua ordem para cada computador gerenciado.
b)Interno ESET PROTECT: Aplique as políticas a cada computador com base na configuração de política do ESET PROTECT On-Prem.

III. Migrar modelos de grupo dinâmico do ESET PROTECT On-Prem para o ESET PROTECT

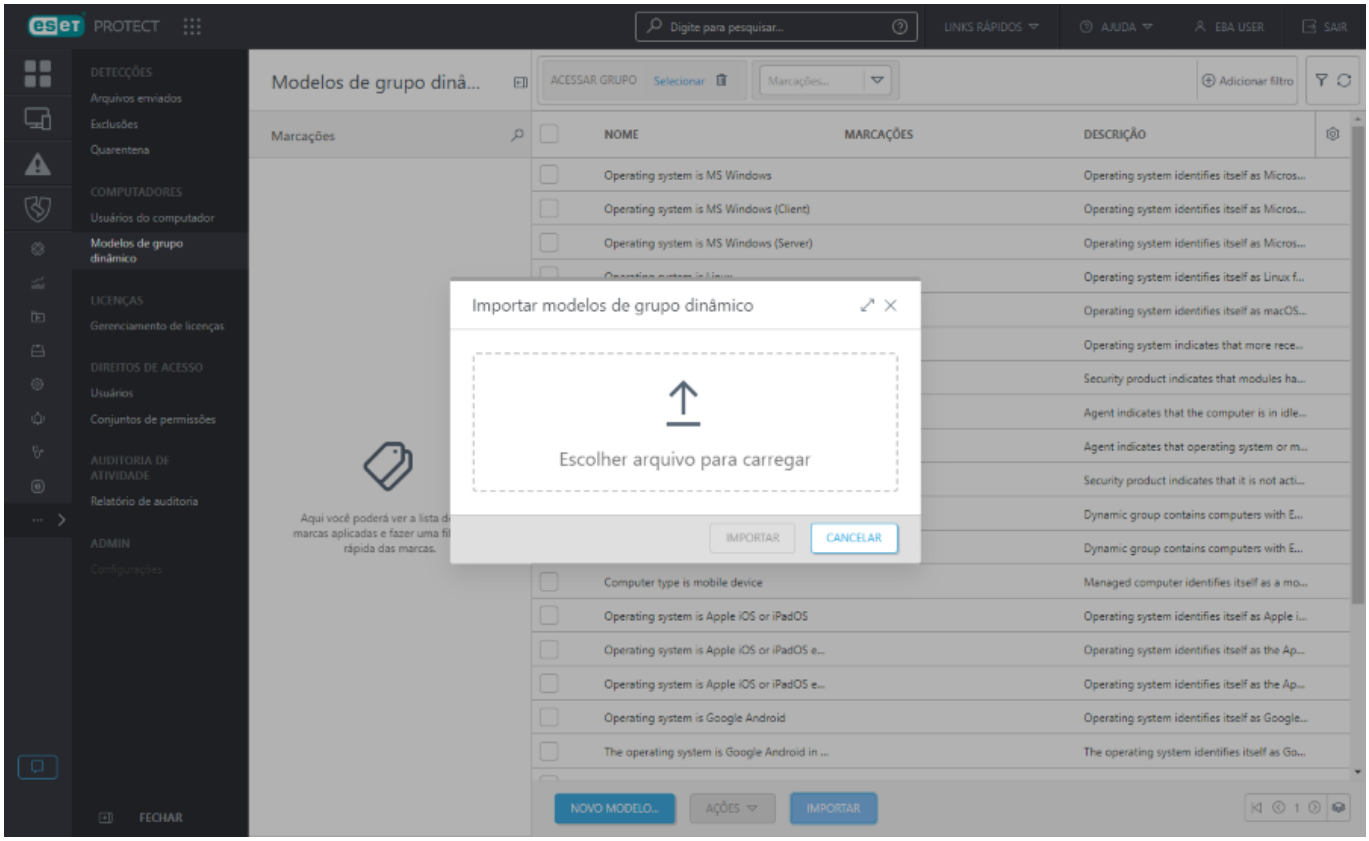
1. No ESET PROTECT On-Prem, selecione **Mais** > **Modelos de grupo dinâmico**.

2. Marque as caixas de seleção ao lado dos modelos de grupo dinâmico que você deseja exportar e clique em **Ações** > **Exportar**.



3. Salve o arquivo *.dg* com os modelos de grupo dinâmico exportados.

4. No ESET PROTECT, clique em **Mais** > **Modelos de grupo dinâmico** > **Importar** e selecione o arquivo *.dg* com os modelos de grupo dinâmico exportados do ESET PROTECT On-Prem e clique em **Importar** para importá-los para o ESET PROTECT.



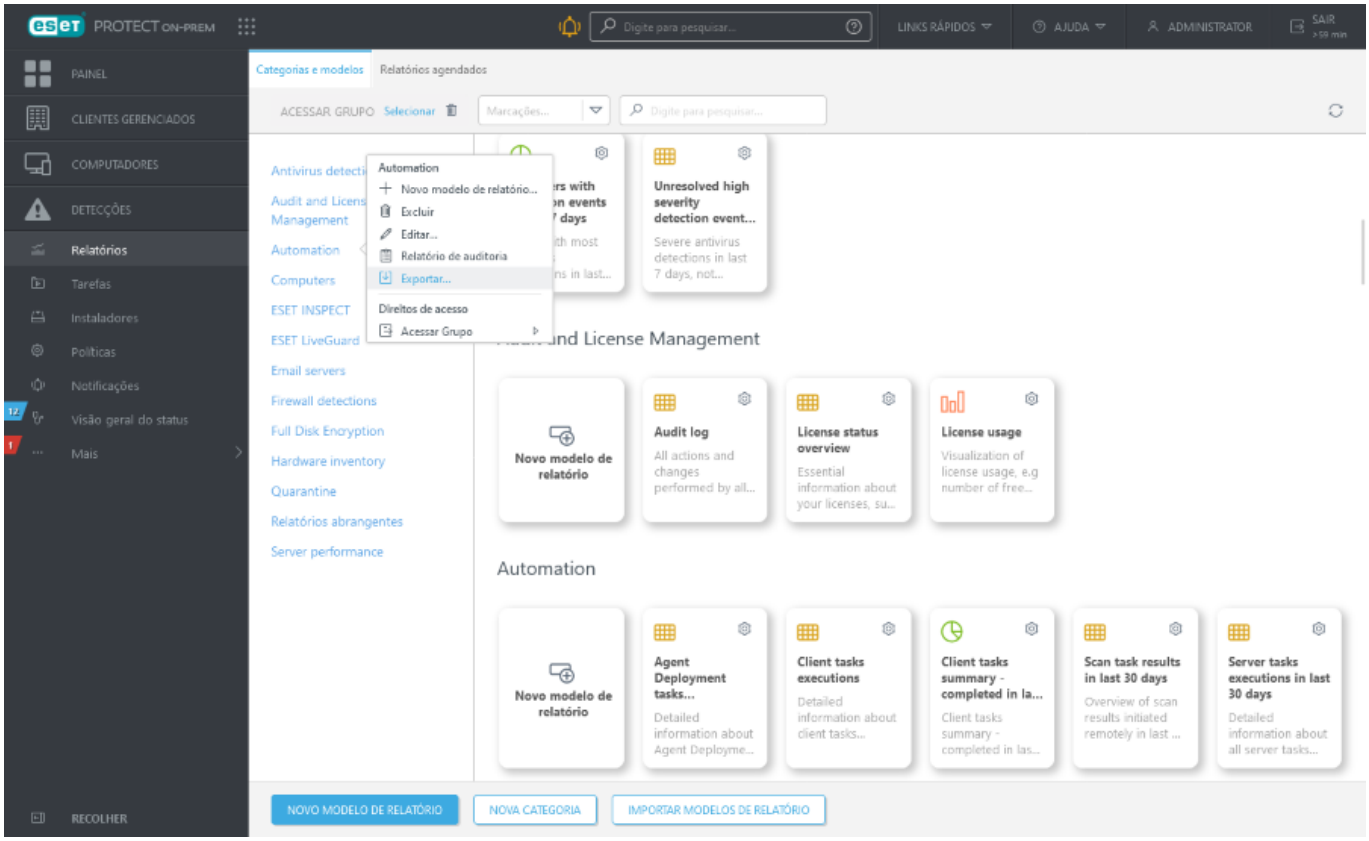
5. Os modelos de grupo dinâmico importados aparecerão na lista de todos os modelos de grupo dinâmico e

você poderá usá-los para criar grupos dinâmicos (não é possível migrar grupos dinâmicos).

IV. Migrar modelos de relatório do ESET PROTECT On-Prem para o ESET PROTECT

1. No ESET PROTECT On-Prem, selecione **Relatórios**.

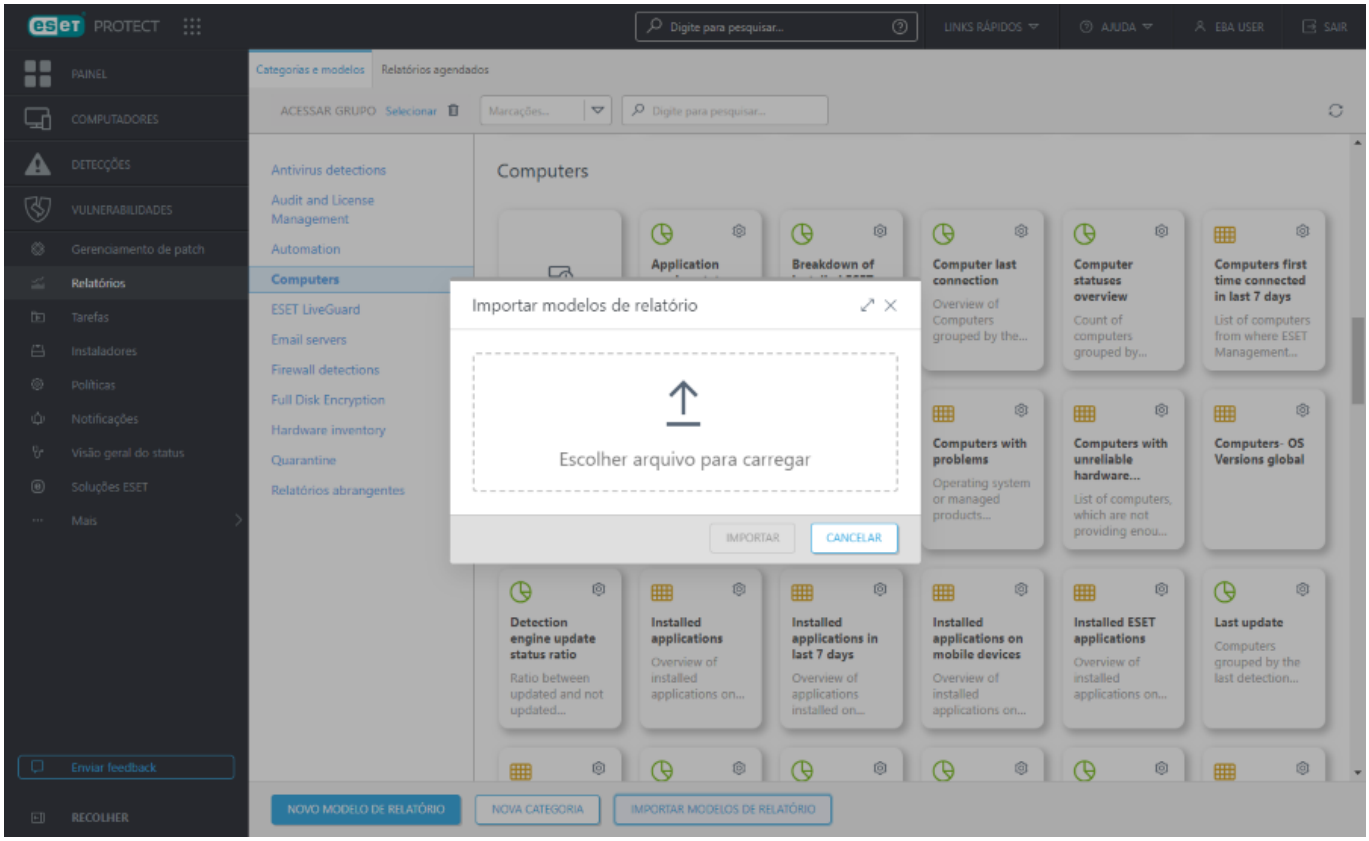
2. Clique no ícone de engrenagem ao lado de uma categoria de relatório ou de um modelo de relatório individual e clique em **Exportar**.



3. Salve o arquivo *.dat* com os modelos de relatório exportados.

4. No ESET PROTECT, clique em **Relatórios** > **Importar modelos de relatório** e selecione o arquivo *.dat* com os modelos de relatório exportados do ESET PROTECT On-Prem e clique em **Importar** para importá-los para o ESET PROTECT.

Repita as etapas acima para migrar mais modelos de relatório individuais ou mais categorias de relatório.



5. Os modelos de relatório importados aparecerão em **Relatórios**. Você pode usar os modelos de relatório para agendar e gerar relatórios.

V. Migrar computadores gerenciados do ESET PROTECT On-Prem para o ESET PROTECT

V.I. Migrar a estrutura de grupo estático usando a ferramenta de exportação de computadores

A ferramenta de exportação de computadores pode exportar a estrutura de grupo estático (não-MSP ou MSP) do ESET PROTECT On-Prem. Em seguida, você pode importar a estrutura de grupo estático para o ESET PROTECT.

⚠ Se você decidir não usar a ferramenta de exportação de computadores:
- Continue com a migração usando a política de migração.
- Depois da migração, todos os computadores vão aparecer no Grupo estático **achados e perdidos** no ESET PROTECT.

Pré-requisitos para executar a ferramenta de exportação de computadores:

- Windows ou Linux de 64 bits
- Python (versão 3.9 e posteriores) – você pode verificar se o Python está instalado e verificar sua versão executando o seguinte comando:
  - Prompt de comando do Windows: `python --version`
  - Terminal Linux: `python3 --version`

Você pode fazer download e instalar o Python de https://www.python.org/. Certifique-se de marcar a caixa de seleção **Add python.exe to PATH** durante a instalação no Windows.

- Verifique se a porta do Web Console (2223 ou uma porta personalizada) está acessível na rede.

1. Faça o download da ferramenta de exportação de computadores para o computador.

2. Descompacte o arquivo *computers_export_tool.zip* do download.

3. Abra a pasta *computers_export_tool* no prompt de comando do Windows ou na janela do Terminal Linux.

4. Execute o seguinte comando:

   - Windows: `python computers_export_tool.py`
   - Linux: `python3 computers_export_tool.py`

5. Em **Hostname [localhost]**, digite o nome do host ESET PROTECT On-Prem e pressione Enter. Se você executar a ferramenta de exportação de computadores no servidor ESET PROTECT, pressione Enter para usar o valor padrão `localhost`.

6. No **Port [2223]**, pressione Enter se o ESET PROTECT On-Prem usa a porta padrão do Web Console (2223) ou digite a porta personalizada do Web Console e pressione Enter.

7. Em **Username**, digite o nome de usuário do Web Console e pressione Enter.

Use o usuário do Web Console com privilégios de administrador que tem acesso a todos os grupos estáticos ESET PROTECT On-Prem para garantir a exportação de todos os grupos estáticos.

8. Em **Password**, digite a senha do usuário do Web Console (você não verá os sinais digitados) e pressione Enter.

9. A ferramenta gera um arquivo *computers.csv* (localizado na mesma pasta: *computers_export_tool*). O arquivo *computers.csv* contém a estrutura de grupo estático ESET PROTECT On-Prem com nomes de computador. Nota: Se você executar a ferramenta novamente, ela substituirá o arquivo *computers.csv*.

Um grande número de computadores gerenciados

A importação de um grande número de computadores pode levar muito tempo. Se houver mais de 30.000 computadores gerenciados no ESET PROTECT On-Prem, siga estas etapas:
1.Usando um editor de texto simples, divida o *computers.csv* arquivo *.csv* em vários arquivos com até 30.000 linhas em cada arquivo.
2.Importe cada arquivo *.csv* no ESET PROTECT repetindo as etapas abaixo.

10. No Web Console ESET PROTECT da nuvem, clique em **Computadores** > clique no ícone de engrenagem ao lado do Grupo Estático **Todos** > selecione **Importar**.

11. Clique em **Escolher arquivo** > selecione o arquivo *computers.csv* e clique em **Abrir**.

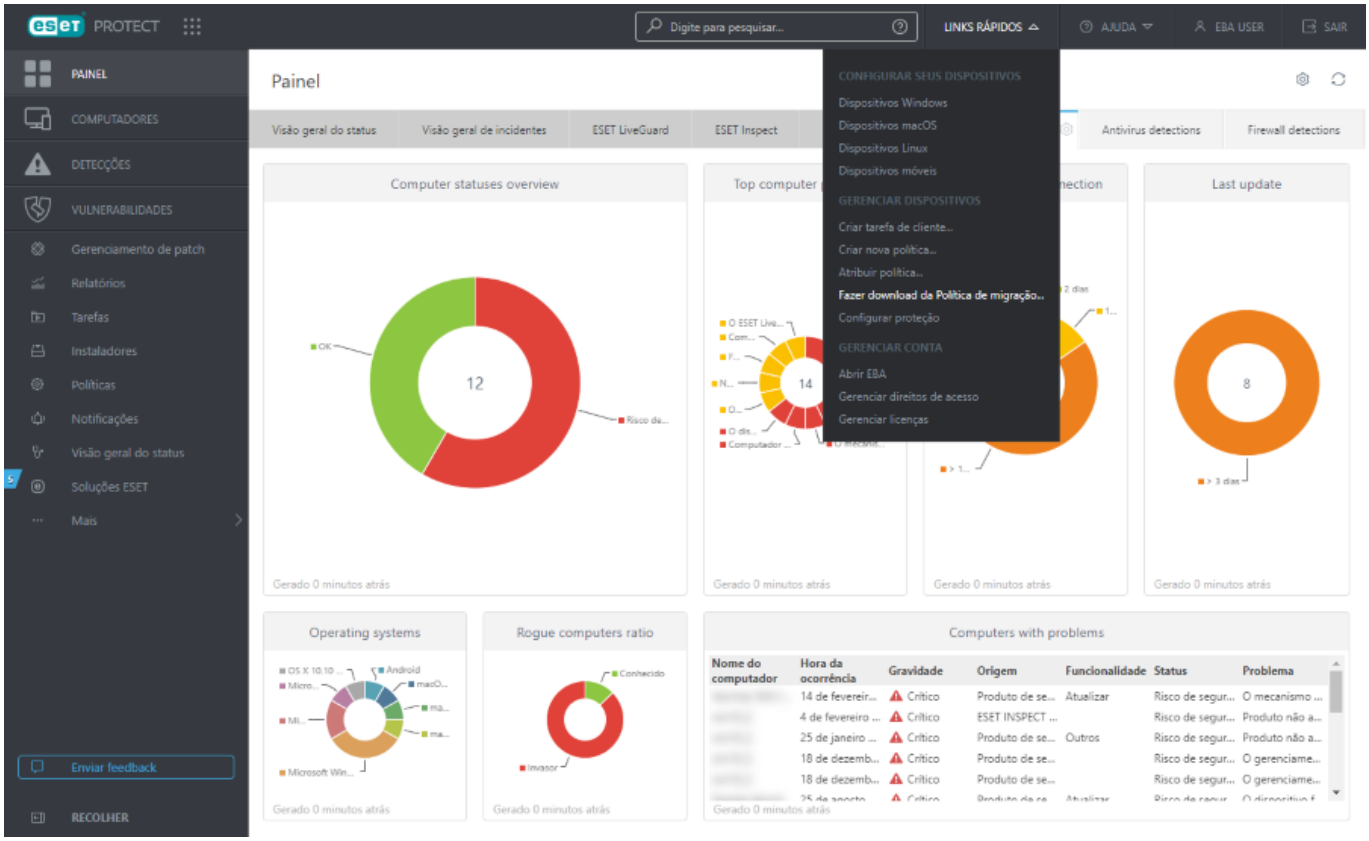
12. Clique em **Importar**. O ESET PROTECT importará a estrutura de grupo estático do ESET PROTECT On-Prem do arquivo *computers.csv*. Você pode fechar a janela de importação e continuar trabalhando com o ESET PROTECT.

13. Após a conclusão da importação, a estrutura Grupo Estático com nomes de computador do ESET PROTECT On-Prem aparecerá em **Computadores** no Web Console ESET PROTECT na nuvem. Continue com as etapas abaixo – use a política de migração para migrar os computadores gerenciados (Agentes ESET Management).

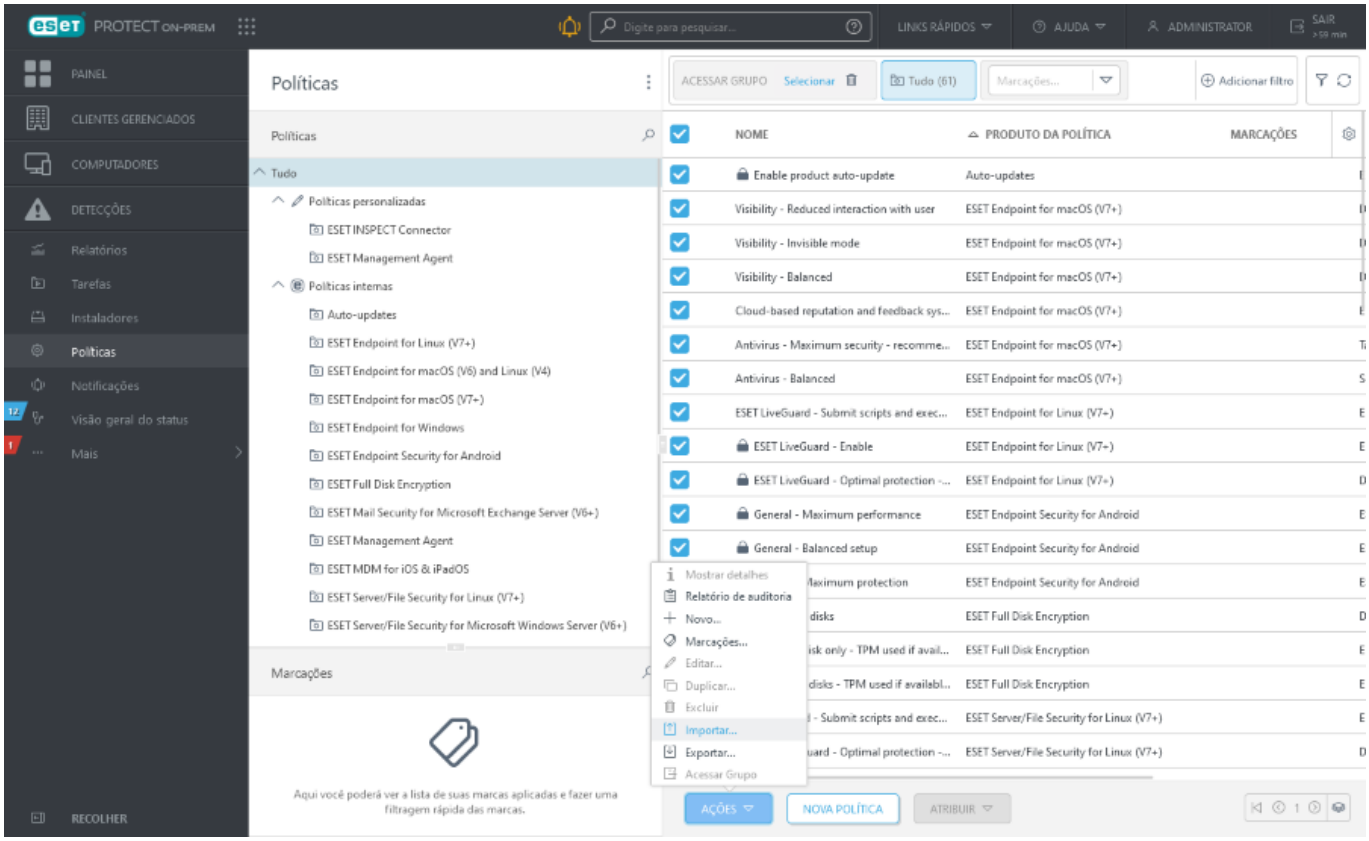
V.II. Migrar os computadores gerenciados (Agentes ESET Management) usando a política de migração

Antes da migração dos Agentes, verifique se as configurações do firewall atendem aos ESET PROTECT pré-requisitos de rede.

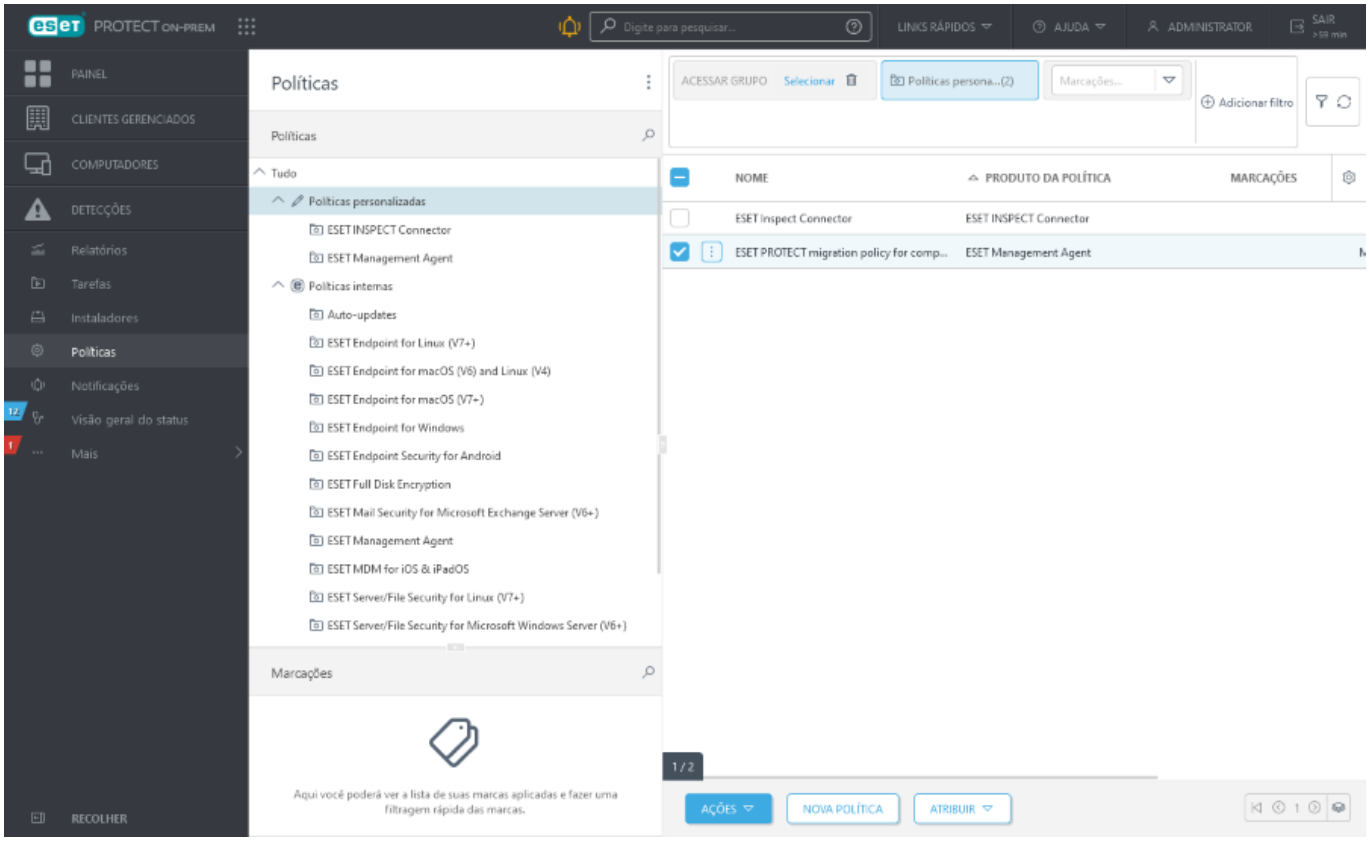
1. No Web Console ESET PROTECT, clique em **Links rápidos** > **Fazer download da política de migração** e salve o arquivo *.dat*.



2. No ESET PROTECT On-Prem, selecione **Políticas** > **Importar**. Selecione o arquivo de download *.dat* da etapa anterior e clique em **Importar**.



3. Navegue para **Políticas personalizadas** e selecione sua política de migração importada.



4. Clique na política de migração > **Editar**.

5. Em **Configurações** > **Conexão**, defina o sinalizador **Forçar** para **Servidores se conectarem** e **Certificado**.

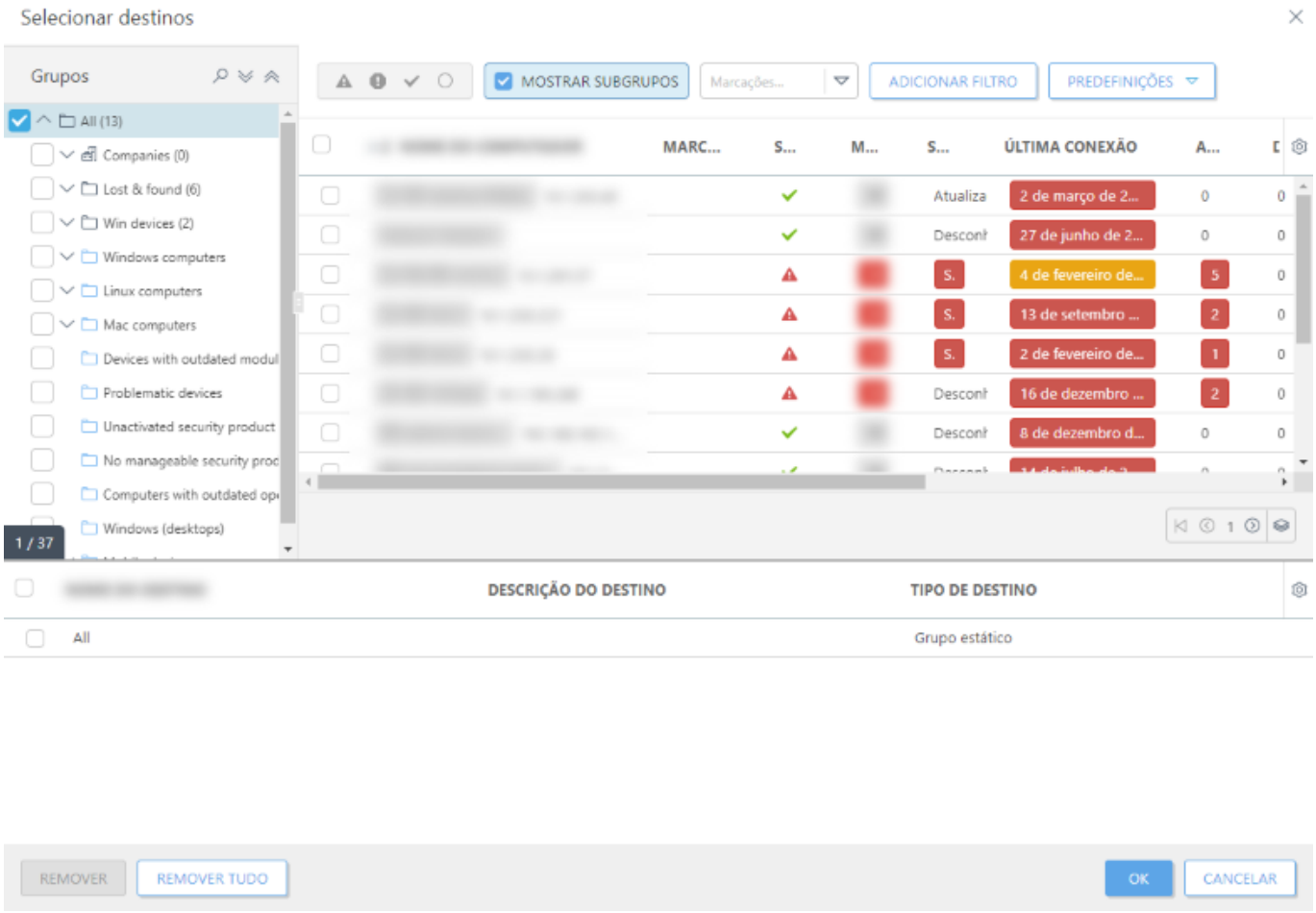
6. Clique em **Concluir**.

Teste a migração em algumas máquinas
Recomendamos migrar alguns computadores aos quais você tem acesso físico. Certifique-se de que eles conseguem se conectar ao ESET PROTECT e, em seguida, migre todos os computadores.

7. Clique em **Atribuir** > **Atribuir grupos**.

8. Selecione o grupo estático **Rodos** e clique em **OK**.

Aplique a política de migração ao grupo estático **Todos** para garantir que você migre os computadores gerenciados.

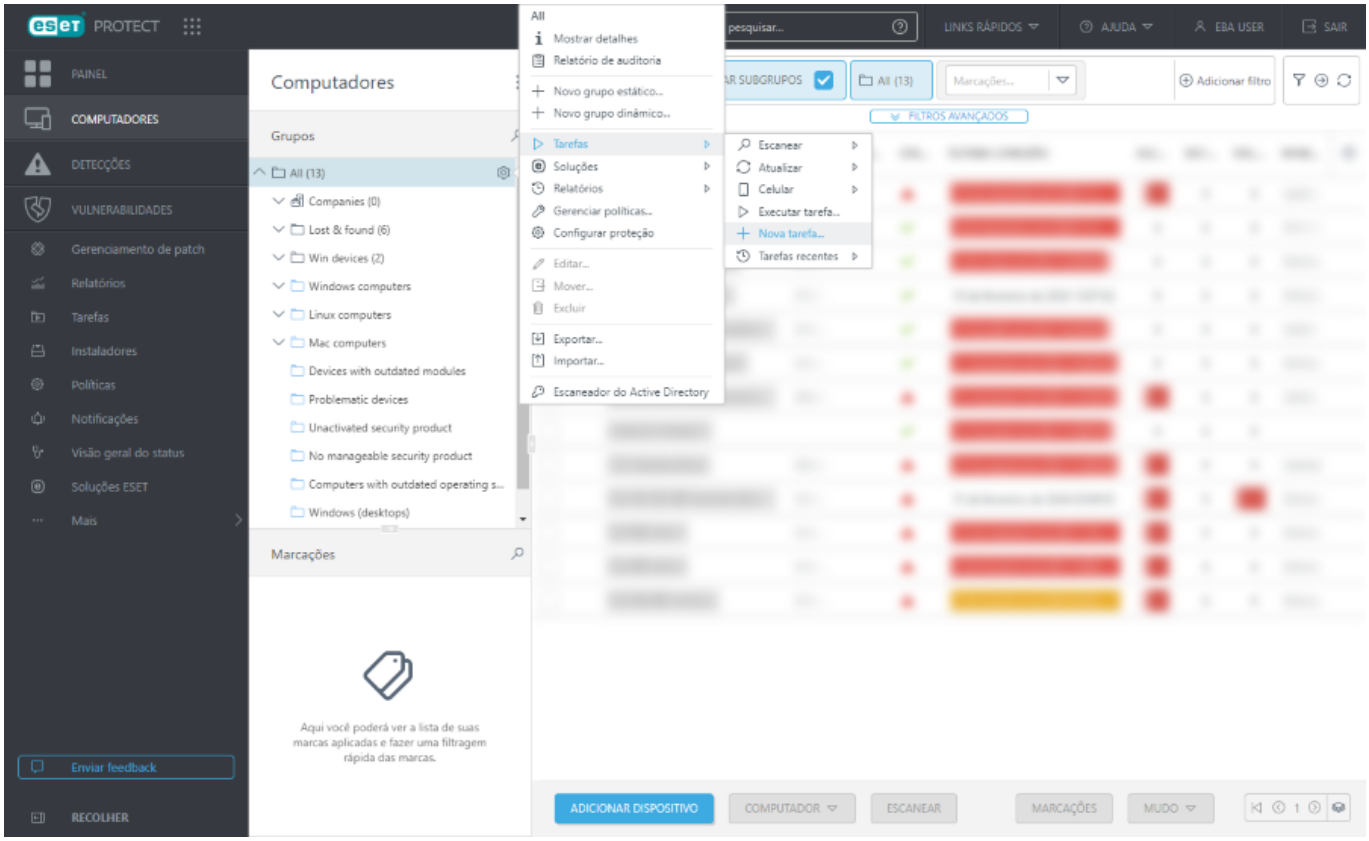


9. Clique em **Concluir** para aplicar a política.

10. Entre no seu console da Web ESET PROTECT. Em **Computadores**, você verá os computadores migrados do ESET PROTECTOn-Prem. Pode ser preciso aguardar alguns minutos até que todos os computadores do ESET PROTECT On-Prem comecem a conectar ao ESET PROTECT.

11. Depois de migrar os computadores do ESET PROTECT On-Prem para o ESET PROTECT, você deve reativar os produtos de segurança ESET nos computadores gerenciados com licenças de nuvem gerenciadas pelo ESET PROTECT:

a.No Web Console ESET PROTECT, clique em **Computadores** > clique no ícone de engrenagem ao lado de **Todo** o Grupo Estático > selecione **Tarefas** > **Nova Tarefa**.



b.Selecione **Ativação do produto** no menu suspenso **Tarefa**.

c.Selecione a licença do produto de segurança ESET em **Configurações**, revise os computadores de destino em **Destino** e clique em **Concluir**.

Se os computadores executarem vários produtos de segurança ESET, você deve repetir as etapas de ativação e selecionar a licença apropriada para cada categoria de produto de segurança ESET.

d.Aguarde alguns minutos até que os produtos de segurança ESET sejam ativados.

VI. Migrar dispositivos móveis

VII. Configurar usuários ESET PROTECT no ESET Business Account.

VIII. Adicionar usuários ESET Business Account ao Web Console ESET PROTECT

IX. Descomissionar o Servidor ESET PROTECT local

Depois de migrar com êxito para o ESET PROTECT, descomissione o Servidor ESET PROTECT.

Se você mantiver o Servidor ESET PROTECT local, desative a tarefa Remover computadores não conectados para evitar a possível desativação dos produtos de segurança ESET em computadores gerenciados pelo ESET PROTECT.

Solução de problemas após a migração

Consulte nosso artigo da Base de Conhecimento para resolver o alerta **Dispositivo usando uma conexão de failover**.

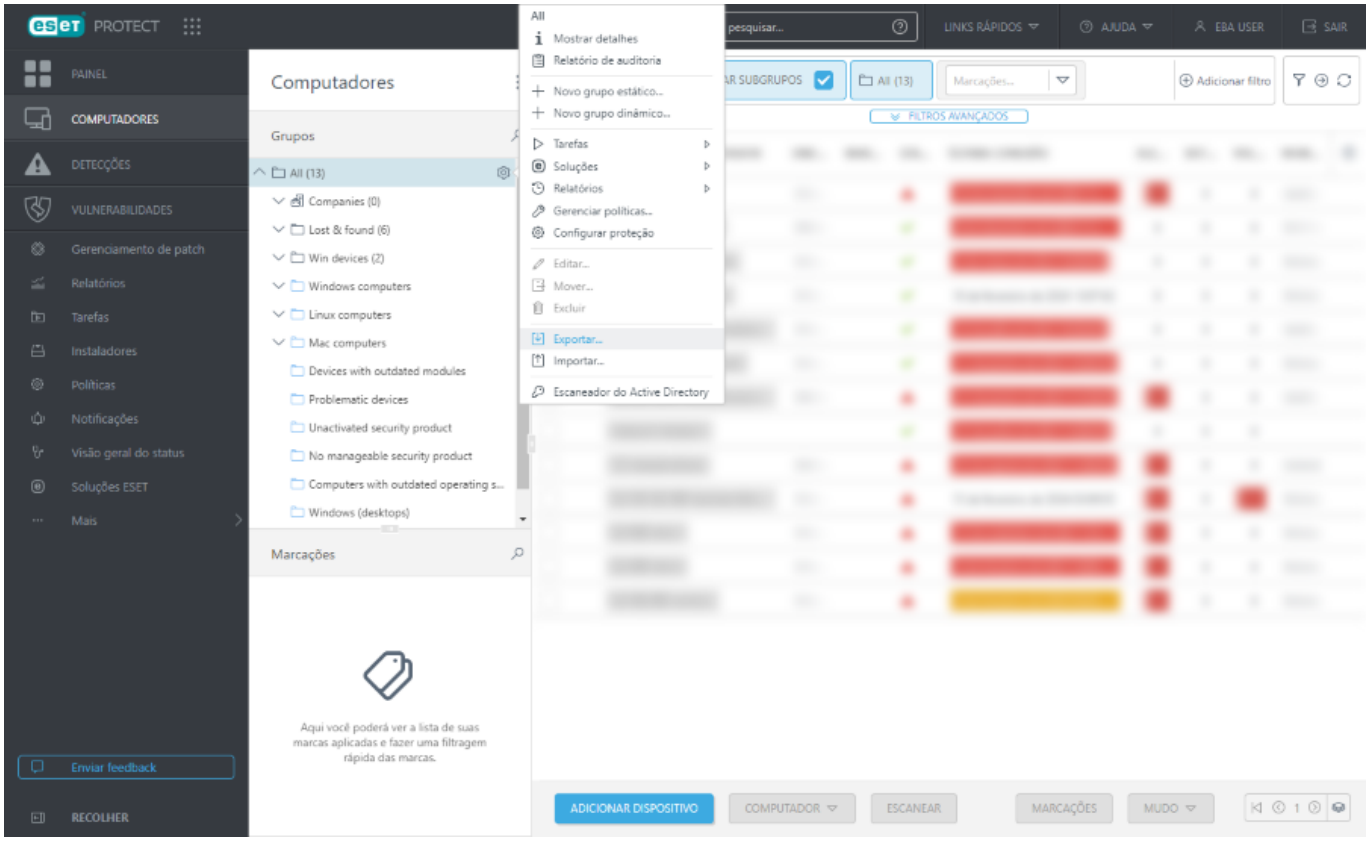
Migração dentro da nuvem—de ESET PROTECT para outro ESET PROTECT

Siga as etapas abaixo para migrar de ESET PROTECT (nomeado **ESET PROTECT 1** abaixo) para outro ESET PROTECT (nomeado **ESET PROTECT 2** abaixo) usando a política de migração:

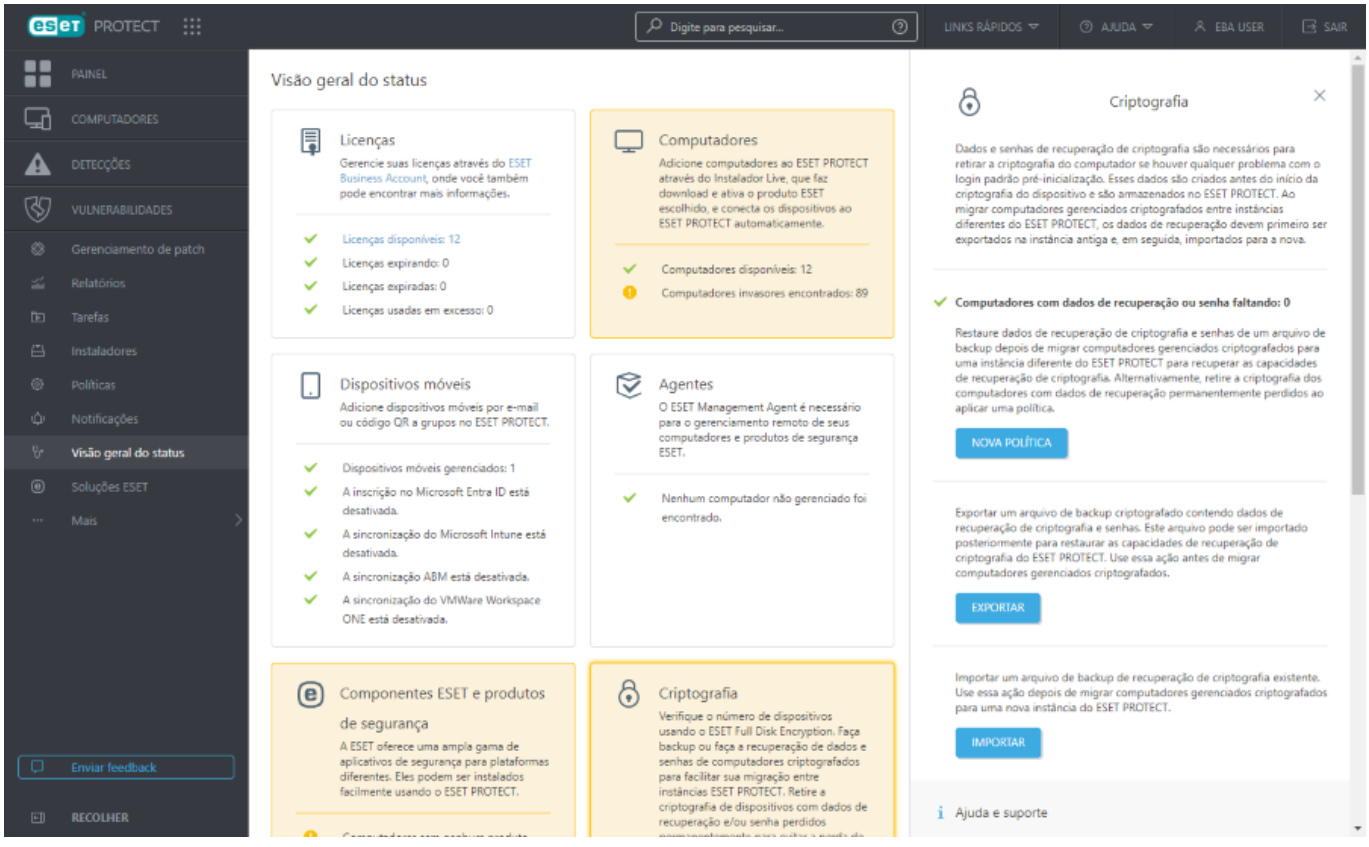
> **ESET PROTECT 1** contém grupos estáticos personalizados, conectando ESET Management Agentes, dispositivos gerenciados com produtos de segurança da ESET instalados e ativados e dispositivos criptografados.

Você pode migrar:	Não é possível migrar:
• computadores gerenciados (ESET Management Agentes e ESET Inspect Conectores) • grupos estáticos • políticas • modelos de grupo dinâmico • modelos de relatório	• todo o banco de dados • Grupos dinâmicos (mas você pode migrar modelos de grupo dinâmico) • detecções • relatórios de auditoria • notificações • tarefas e acionadores • instaladores • relatórios agendados/gerados (mas você pode migrar modelos de relatório) • marcações • dispositivos móveis (mas você pode registrá-los novamente)

1. **ESET PROTECT 1**—Clique em **Computadores** >, clique no ícone de engrenagem ao lado do grupo estático > **Todos** > selecione **Exportar** > clique em **Sim** para exportar computadores de subgrupos > salve o arquivo *TXT*.

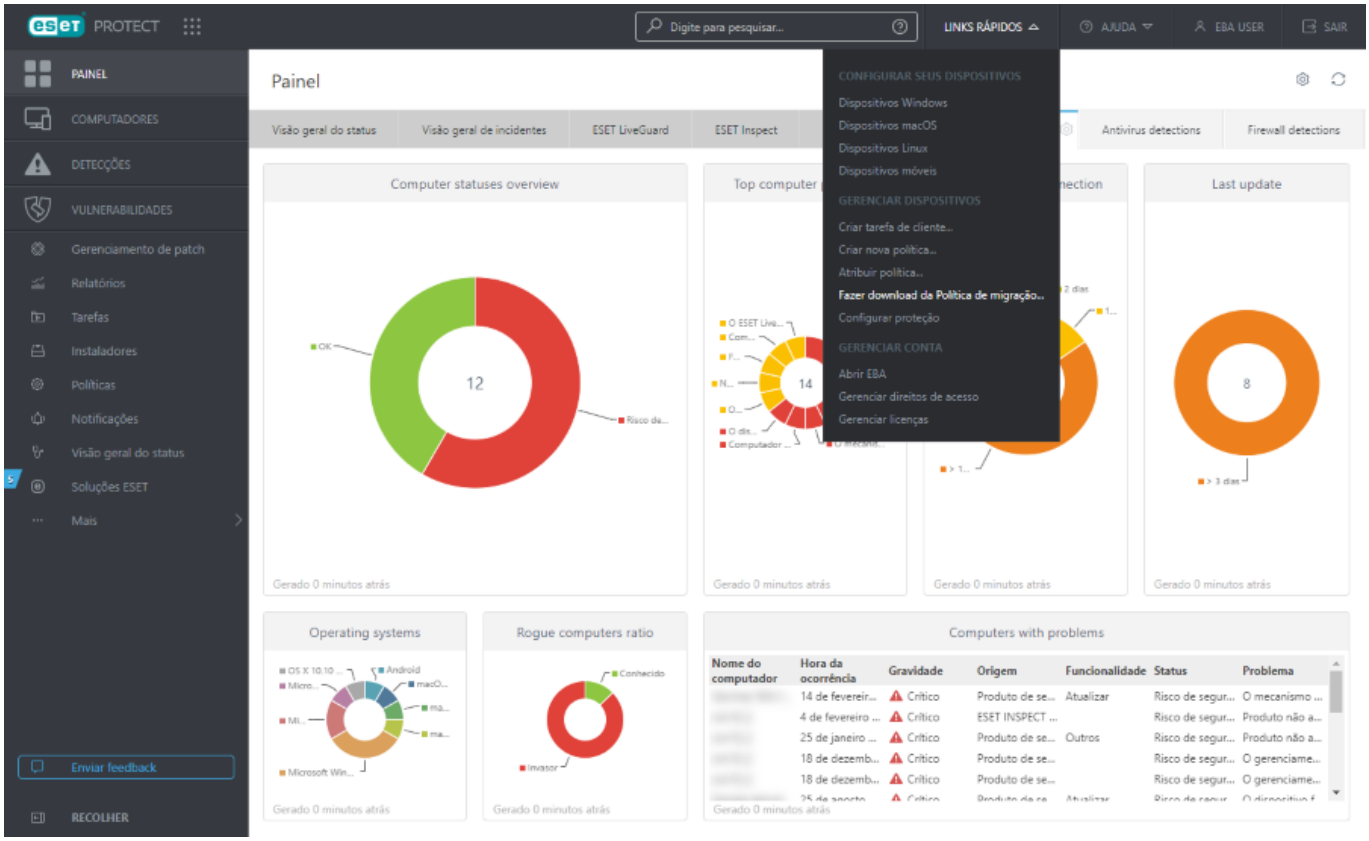


2. **ESET PROTECT 1**—Clique em **Visão Geral do Status** > clique no bloco > **Criptografia** > clique em **Exportar** para exportar os dados de criptografia e as senhas > salve o arquivo **efdeRecoveryExport.dat**.

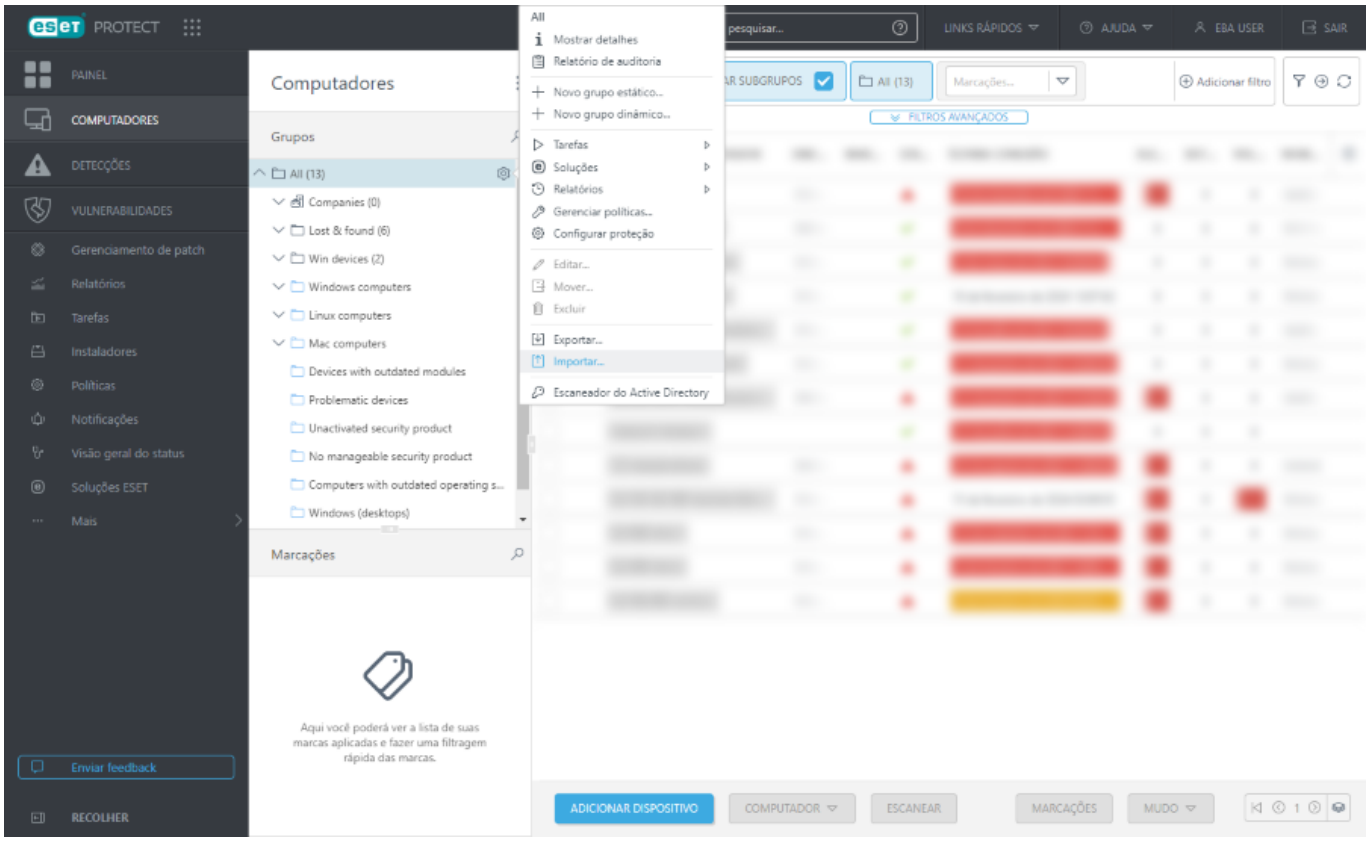


3. Crie um novo ESET PROTECT (**ESET PROTECT 2**).

4. **ESET PROTECT 2**— Clique em **Links Rápidos** > **Baixar Política de Migração** > salve o arquivo *CloudMigrationPolicy {timestamp}.dat*.



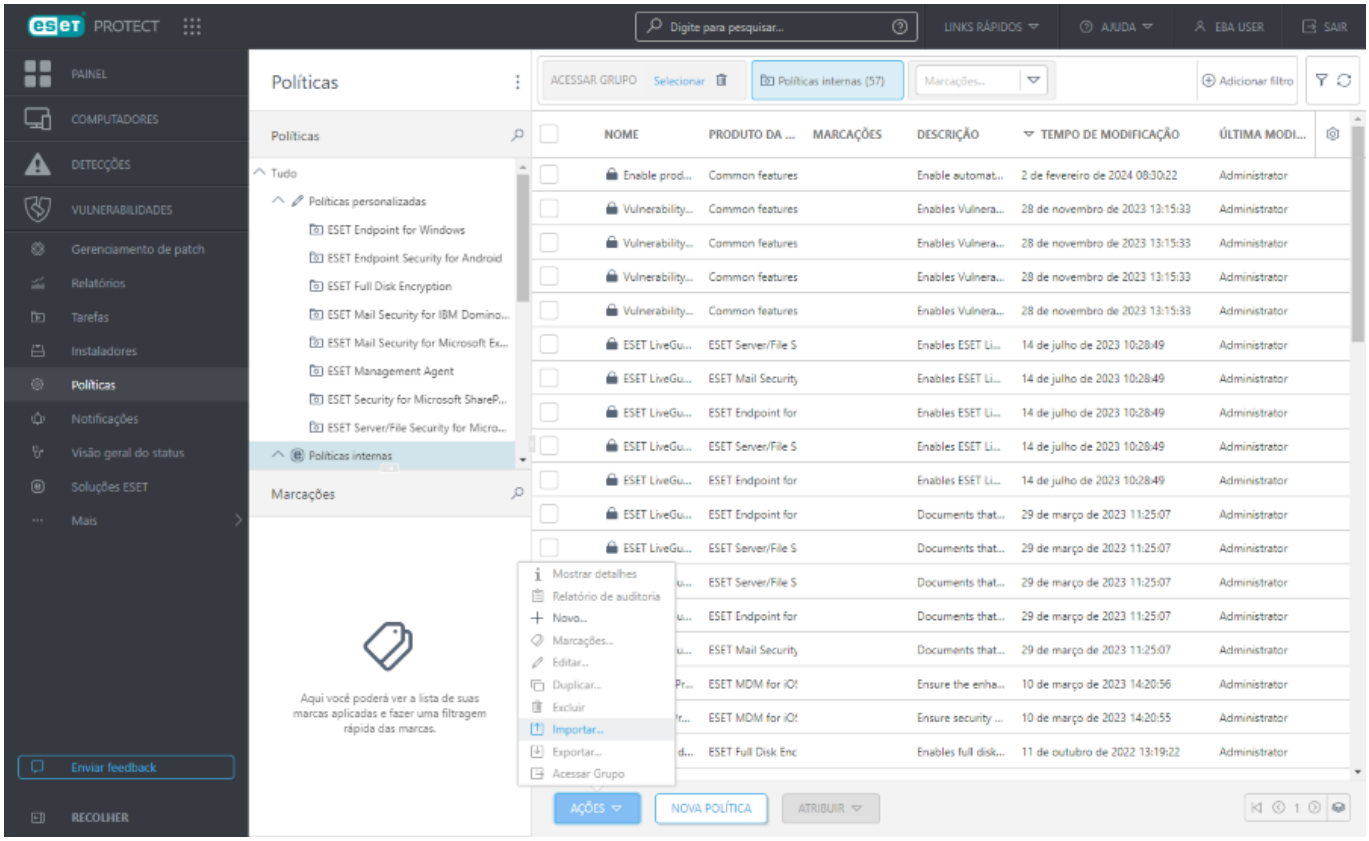
5. **ESET PROTECT 2—Clique em Computadores** > clique no ícone de engrenagem ao lado do grupo estático > **Todos** > selecione **Importar** > importar os grupos estáticos usando o arquivo *TXT* exportado de **ESET PROTECT 1** na etapa 1 acima.



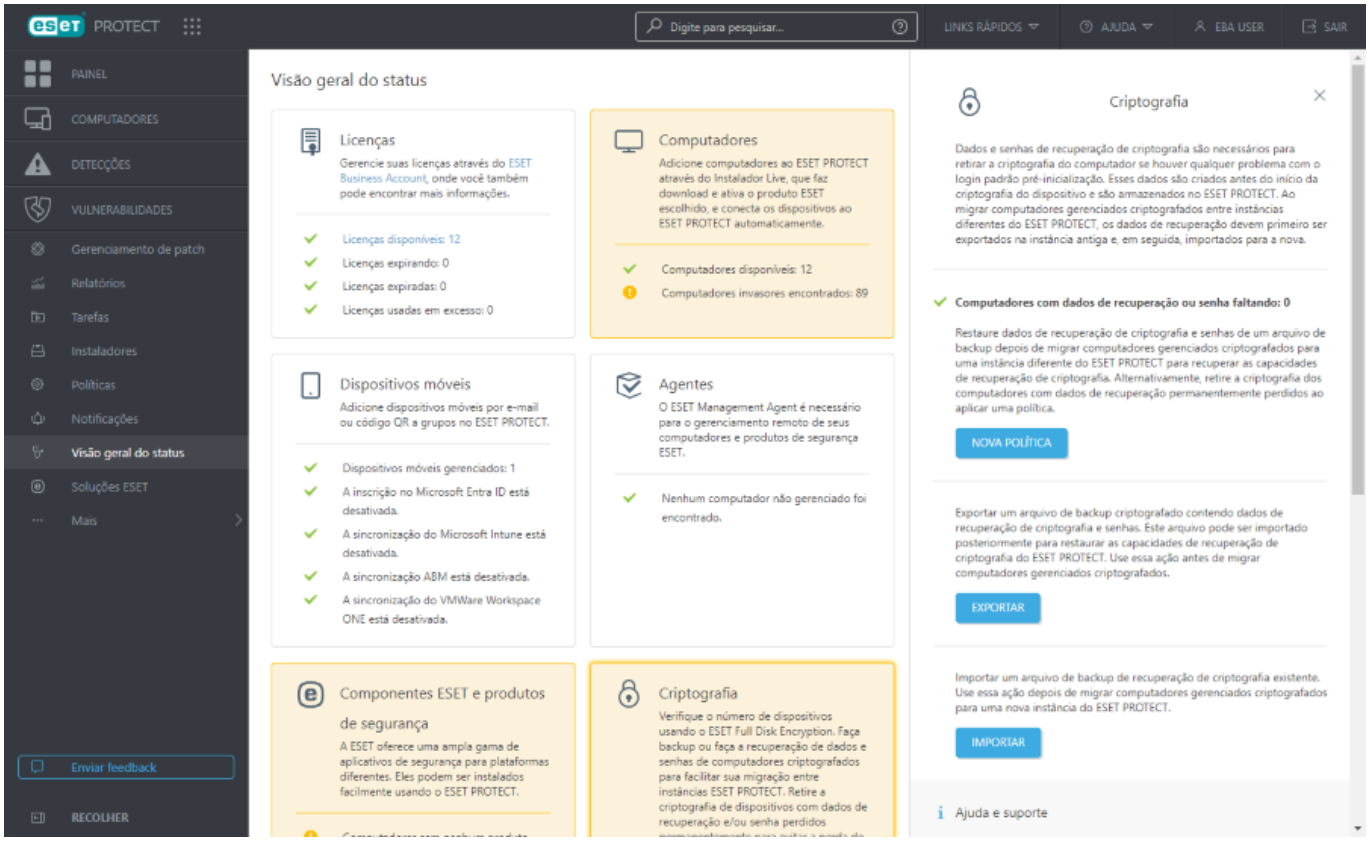
6. **ESET PROTECT 1**—Clique em **Políticas** > **Ações** >**Importar** > importe o arquivo de política de migração *DAT* exportado de **ESET PROTECT 2** na etapa 4 acima > atribua a política de migração ao grupo estático **Todos**. Os

computadores gerenciados se conectarão a **ESET PROTECT 2**.

> Se você usar ESET Inspect, os ESET Inspect Conectores nos computadores gerenciados se conectarão ao novo ESET Inspect.



7. **ESET PROTECT 2**—Clique em **Visão geral do status** > clique no bloco > **Criptografia** > clique em **Importar** para importar os dados de criptografia e senhas do arquivo *DAT* exportado de **ESET PROTECT 1** na etapa 2 acima.



8. Da mesma forma que migrar de ESET PROTECT On-Prem para ESET PROTECT, execute a migração de **ESET PROTECT** 1 para **ESET PROTECT 2** para:

   - políticas
   - modelos de grupo dinâmico
   - modelos de relatório

> **Migração de dispositivos móveis**
> Para migrar os dispositivos móveis gerenciados, cancele a inscrição deles de **ESET PROTECT 1** e inscreva-os em **ESET PROTECT 2**.

Como remover o ESET PROTECT da sua rede

Existem duas formas corretas de parar de gerenciar sua rede com o ESET PROTECT:

a) Remover completamente todos os produtos ESET Security e o Agentes ESET Management e então desmontar a instância ESET PROTECT.

b) Continuar a usar os produto de segurança ESET mas remover o Agente ESET Management e a instância ESET PROTECT. (Nesse cenário, ignore Remover Agente ESET Management abaixo).

Remover produtos de Segurança ESET da sua rede

1. Redefinir para padrão ou desbloquear as configurações do cliente nas políticas.

   a. Remova todas as **Políticas personalizadas** aplicadas atualmente aos clientes.

b.Para todsa as **Políticas internas** selecione a política e clique na guia **Clientes** para ver se alguma dessas políticas está atribuída a computadores na sua rede.

2. Mude as configurações de senha nos clientes no valor padrão.

a.Crie uma nova política e navegue para **Política do produto de segurança > Interface do usuário > Configuração do acesso**.

b.Deixar as **Configurações protegidas por senha** desativadas e usar **Forçar** ao lado da configuração **Definir senha**.

c.Atribua essa política a todos os dispositivos na sua rede. Isso removerá a proteção por senha das configurações avançadas dos seus produtos Endpoint Security.

3. Remover a criptografia de qualquer estação de trabalho criptografada com o ESET Full Disk Encryption.

Se qualquer estação de trabalho ainda estiver criptografada depois da instância do ESET PROTECT ser removida, não haverá outra forma de retirar a criptografia da estação de trabalho (se você não tiver feito o download dos dados de recuperação de criptografia anteriormente). Nem mesmo a ESET poderá ajudar nesse caso.

4. Remova o produto de segurança dos dispositivos do cliente, se desejar. Você pode deixar os produtos de segurança instalados e eles continuarão a oferecer proteção, mesmo que não sejam gerenciados.

Para desinstalar todos os produtos de segurança na sua rede use a tarefa de Desinstalação de software.

a.Navegue para **Tarefas** > **Nova**.

b.No Assistente de criação de tarefas na seção **Básico**, preencha o Nome e a Descrição e selecione **Desinstalação do software** no menu suspenso **Tarefa**.

c.Na seção **Configurações** selecione o aplicativo a ser desinstalado no menu suspenso **Desinstalar**. Em **Nome do pacote** clique em **Selecionar pacote a desinstalar**, selecione o produto de segurança que quer desinstalar e clique em **OK**.

d.Em **Versão do pacote**, clique em **Desinstalar todas as versões do pacote** para evitar problemas ao desinstalar diferentes versões de produtos de segurança nos computadores clientes da sua rede.

e.Selecione a caixa de seleção ao lado de **Reinicialização automática quando necessário** para garantir que o processo de desinstalação foi totalmente concluído e depois clique em **Concluir** para criar a tarefa.

f.Clique em **Criar acionador** para selecionar um Destino para a tarefa. Clique em **Adicionar grupos** e selecione o grupo **Todos** como destino. Selecione o acionador apropriado e clique em **Concluir** para executar.

Verifique se a tarefa foi executada com sucesso em todos os dispositivos e repita o processo para cada tipo de produto de segurança em sua rede.

Remova o Agente ESET Management da sua rede.

Para uma remoção mais eficiente de todas as Agentes ESET Management na sua rede, verifique se todos os dispositivos afetados estão ligados e conectados ao ESET PROTECT.

1. Reverta a definição de configuração protegida por senha (somente Windows).

   a.Criando uma nova política para o Agente ESET Management.

   b.Navegue até **Configurações avançadas** e, em **Configuração**, defina um marcador **Forçar** ao lado da definição **Configuração protegida por senha**.

   c.Atribua a política ao grupo **Todos** e clique em **Concluir** para aplicar.

2. Verifique se a política é aplicada. Depois da política ser aplicada a todos os clientes, remova o Agente ESET Management dos computadores na sua rede. Você pode usar a tarefa Interromper gerenciamento (desinstalar Agente ESET Management) para isso. Atribui a tarefa a todos os computadores na sua rede.

3. Aguarde até que a tarefa seja executada em todos os dispositivos da sua rede.

4. Remova todos os dispositivos na seção **Computadores** do ESET PROTECT.

Se nenhum dos dispositivos reaparecer no console pelos próximos 10 minutos, você removeu com sucesso todos os Agentes ESET Management da sua rede.

Remover instância do ESET PROTECT

1. Abra sua conta ESET Business Account.

2. Na seção principal do **Painel**, navegue até o bloco ESET PROTECT.

3. Clique no ícone de engrenagem no bloco ESET PROTECT e selecione **Remover ESET PROTECT**.

4. Digite sua senha e clique em **Remover**. Sua instância ESET PROTECT será removida.

Expiração da última licença ESET PROTECT

Este tópico descreve os seguintes cenários relacionados a licença:

- O que acontece com uma instância ESET PROTECT antes e depois da última licença elegível ESET PROTECT expirar.
- O que acontece depois que a última licença elegível ESET PROTECT é removida do ESET Business Account.

O que acontece com uma instância ESET PROTECT antes e depois da expiração da última licença elegível ESET PROTECT?

Quando sua licença estiver perto de expirar, um alerta será exibido na interface ESET Business Account.

- Se a data de expiração passar e você não renovar sua licença ou ativar uma nova licença, o alerta de licença expirada será exibido em ESET Business Account.
- Se não houver uma licença elegível uma notificação de que sua licença será suspensa em 14 dias será exibida no ESET Business Account e você receberá um e-mail no endereço especificado na sua conta de

administrador.

Você tem um período de carência de 14 dias para renovar depois que sua licença expirar. Você será notificado no ESET Business Account e por email no meio do período de carência. Depois de 14 dias o uso do seu ESET PROTECT será suspenso.

A instância vai se tornar inacessível e não-funcional. Uma instância ESET PROTECT suspensa será armazenada e pode ser acessada novamente adicionando uma licença elegível para ESET PROTECT ao ESET Business Account. **Sua instância ESET PROTECT pode permanecer em um estado suspenso por até 30, depois desse período a instância e todos os dados relacionados a ela serão removidos permanentemente**.

Se sua instância entrar em um estado suspenso você será notificado no ESET Business Account e por email quando houver 14 dias antes de sua instância ser removida. Você deve ativar uma nova licença elegível ESET PROTECT para restaurar o acesso a sua instância ESET PROTECT.

O que acontece depois que a última licença elegível ESET PROTECT é removida do ESET Business Account?

Se nenhuma licença elegível ESET PROTECT estiver presente no ESET Business Account, sua instância ESET PROTECT será suspensa.

A instância vai se tornar inacessível e não-funcional. Uma instância ESET PROTECT suspensa será armazenada e pode ser acessada novamente adicionando uma licença elegível para ESET PROTECT ao ESET Business Account. **Sua instância ESET PROTECT pode permanecer em um estado suspenso por até 30, depois desse período a instância e todos os dados relacionados a ela serão removidos permanentemente**.

Se sua instância entrar em um estado suspenso você será notificado no ESET Business Account e por email quando houver 14 dias antes de sua instância ser removida. Você deve ativar uma nova licença elegível ESET PROTECT para restaurar o acesso a sua instância ESET PROTECT.

Atualizações automáticas

Há vários tipos de atualizações automáticas de produtos ESET:

- Atualização automática do Agente ESET Management
- Atualização automática de produtos de segurança ESET

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 Mirror Tool 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.

Como a atualização automática do Agente ESET Management funciona

- A atualização automática do Agente está ativada por padrão e não pode ser desativada.

- 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.
> Como alternativa, você pode usar a Tarefa do cliente Atualizar Agente.

- 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 Mirror Tool 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 inclui um recurso para manter os produtos de segurança ESET atualizados para a versão mais recente em seus computadores gerenciados.

As atualizações de produto automáticas são habilitadas automaticamente em uma instância recém-implantada do 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 Mirror Tool 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.

Há duas maneiras de atualizar os produtos de segurança ESET para a versão mais recente:

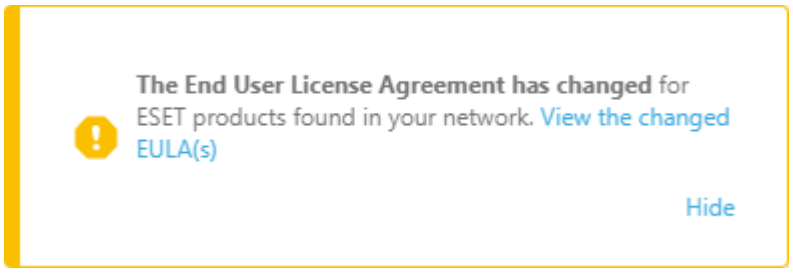
- Tarefa do cliente de instalação de software
- Recurso de atualização automática

Diferenças entre a Tarefa do cliente de Instalação de software e o recurso de Atualizações automáticas:

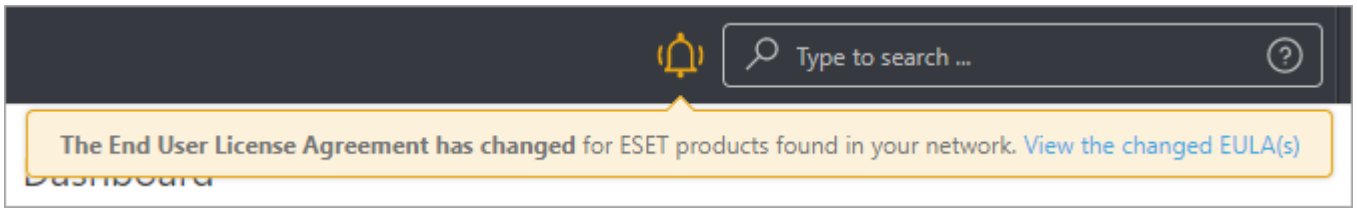
	Processo de atualização	Reiniciar depois da atualização	Atualizações futuras
Tarefa do cliente de instalação de software	O processo de atualização inclui a reinstalação do produto de segurança ESET.	A atualização do produto de segurança ESET requer a reinicialização imediata do computador por motivos 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 uma reinicialização do computador, mas não imediatamente (a reinicialização não é imposta). O administrador ESET PROTECT pode impor a atualização do computador e reiniciar remotamente a partir do Web Console usando a caixa de seleção Encerrar tarefa de cliente do computador com a caixa de seleção **Reinicializar computador(es)** marcada.	Automático – atualizações automáticas de produtos de segurança ESET compatíveis quando uma nova versão é lançada (a atualização é atrasada por motivos de estabilidade). Você pode impor manualmente a verificação de atualizações de produtos de segurança ESET usando a Tarefa Verificar atualização de produto.

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.

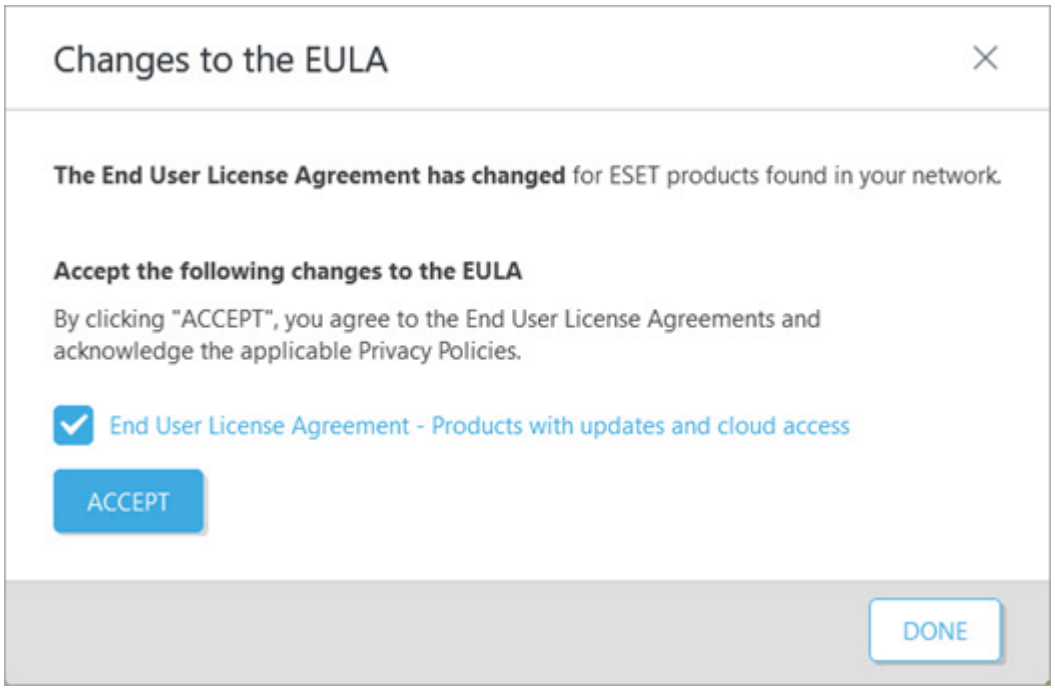


Clique em **Exibir o(s) EULA(s) alterado(s)** para ver os detalhes ou em **Ocultar** para mover a notificação sob um ícone de sino amarelo na barra de ferramentas superior.



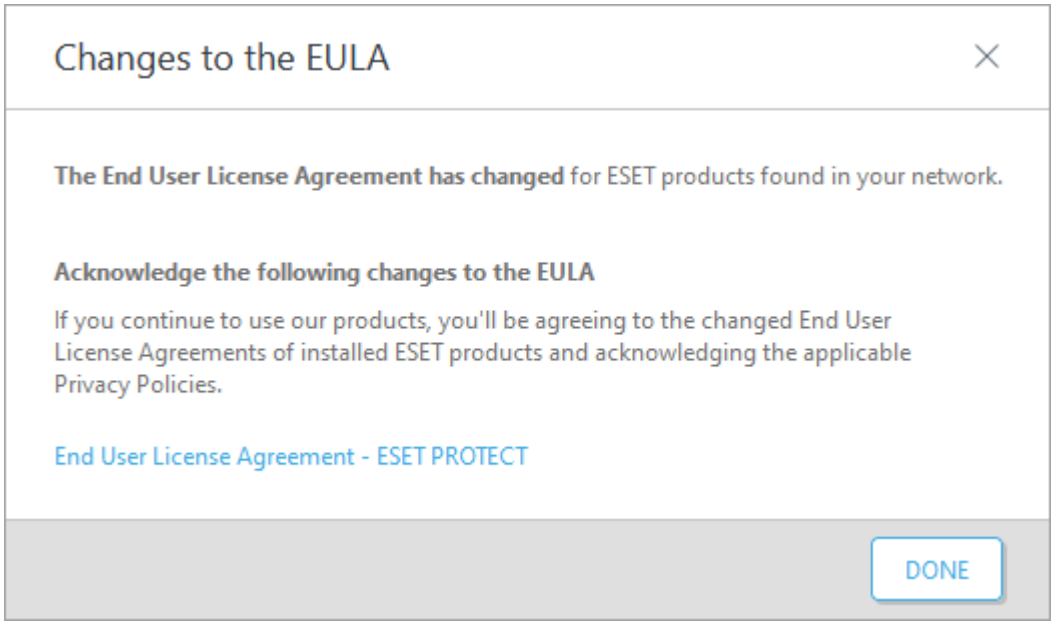
Quando você clica em **Exibir o(s) EULA(s) alterado(s)**, uma nova janela será exibida com detalhes sobre o produto de segurança ESET e suas alterações do Acordo de Licença para o Usuário Final:

- 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.



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 **Recursos comuns** > **Atualização** no menu suspenso e defina as configurações de política:
   - **Alternância automática de perfil** – clique em **Editar** e atribua um perfil de atualização de acordo com os perfis de conexão de rede.
   - **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** > **Selecionar versão** – 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.

ℹ 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**.

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.

ℹ Se você estiver em contato com o Suporte ESET, identifique sua instância ESET PROTECT fornecendo o número UUID de sua instância ESET PROTECT. O número UUID de sua instância pode ser encontrado em **Ajuda** > **Sobre** > **ID**, ou em **ESET Business Account** ou no portal **ESET MSP Administrator** em **Ajuda** > **Sobre** > **ESET PROTECT ID**.

ESET Connect (API)

O ESET Connect é um gateway REST API entre um cliente e uma coleção de serviços de backend ESET. O ESET Connect atua como um proxy reverso para aceitar todas as chamadas de interface de programação de aplicativos (API), agregar os serviços necessários para cumpri-las e retornar o resultado apropriado.

APIs ESET e integrações API construídas sobre o gateway API permitem a automação de atividades de monitoramento, segurança e administração.

ℹ ESET Connnect está disponível apenas em inglês.
Para obter mais informações, consulte a Ajuda on-line do ESET Connect.

Perguntas frequentes do gerenciamento de patch e de vulnerabilidade

Veja abaixo as perguntas frequentes relacionadas ao Gerenciamento de patch e de vulnerabilidade (V&PM:

Lista de aplicativos

Com que frequência os aplicativos cobertos pela lista de vulnerabilidades são atualizados?	• V&PM pode detectar software recém-adicionado com base no banco de dados atualizado algumas vezes por semana. • A lista é atualizada diariamente com base nos dados do provedor.
Os aplicativos que não são cobertos na lista de aplicativos compatíveis são escaneados em Vulnerabilidades?	Não, a lista é definitiva. Os aplicativos não cobertos no banco de dados não serão detectados.
O V&PM exibe e corrige apenas versões anteriores de aplicativos vulneráveis ou também pode corrigir apenas versões desatualizadas e não vulneráveis de aplicativos?	O V&PM não corrige aplicativos sem CVE.

Política

Os **aplicativos permitidos** e os **aplicativos excluídos** na política de **recursos comuns** do V&PM são classificados com base no que pode ser corrigido automaticamente?	Estas são listas seguras e listas de negação para gerenciamento de patches automáticos com base na configuração da **Estratégia de patch automático**.

Agenda do gerenciamento de patch e de vulnerabilidade

Como exatamente o escaneamento V&PM é acionado?	O escaneamento V&PM é acionado uma vez por dia pela agenda V&PM com base nas configurações feitas pelo administrador na política.
O que acontece durante a janela de tempo selecionada?	O escaneamento é feito uma vez por dia nesse período de tempo especificado. O escaneamento é iniciado quando um computador é ligado dentro desse período de tempo.
Uma tarefa de escaneamento e uma tarefa de patch estão interligadas? Às 15:50, vou definir a agenda para iniciar às 16:00 – 19:00. Ela acionará apenas uma tarefa de escaneamento ou uma tarefa de patch também? Se apenas uma tarefa de escaneamento for acionada às 16:00, quando a próxima tarefa de patch será acionada?	O escaneamento e o patch não estão interconectados. Se forem 15:50 e você aplicar a política, o escaneamento será executado às 16:00 e o patch será executado em um horário aleatório entre 16:30 e 18:30. Mas se você estiver fora da janela de manutenção, o patch automático será executado da próxima vez. O gerenciamento de patch não aplica patches fora desse horário.
Se um computador ligar às 19:00, a tarefa de escaneamento/patch será acionada imediatamente ou ela vai esperar até as 9:00? Está definido na tarefa da agenda que se o horário agendado for ignorado, o patch será iniciado imediatamente após isso?	Se as configurações de diretiva forem executar essas tarefas entre 17:00 e 9:00 e você abrir o computador às 19:00, o escaneamento será executado o mais rápido possível e um patch será executado também somente se a hora escolhida aleatoriamente quando essa tarefa foi criada for antes das 19:00, se não ela aguardará a hora selecionada.

Se um agenda não estiver definida em uma política, quando o escaneamento e a aplicação de patches serão acionados? A política predefinida é das 17:00 às 09:00. Isso significa que o escaneamento/patch será acionado 17:00 + 30min ou 9:00 - 30 min se não houver uma política definida?	Sim, o intervalo de tempo do agendamento é o mesmo da política predefinida das 17:00 às 09:00.
Como exatamente e quando uma atualização de aplicativos é acionada (quando a disponibilidade na agenda é definida para todos os dias e todo o ciclo de 24 horas)?	O patch automático é uma tarefa executada pela agenda, mas o tempo de execução é um valor aleatório entre a **Hora de início** + 30 min e **Hora de término** - 30 min. Por exemplo: se o administrador define o horário de início da segunda-feira na agenda como 1:00 e o horário de término para 11:00. Quando a política é aplicada em um endpoint, temos um algoritmo que cria a tarefa de patch automático para a agenda selecionando um valor aleatório entre 1:30 e 10:30, por exemplo, 4:21 foi selecionado. Isso significa que o patch automático será executado todas as segundas-feiras, às 4:21. O mesmo fluxo também é usado quando todos os dias são selecionados e o horário de início é 0:00 e 12:00. (24h); um valor é selecionado entre essas horas, por exemplo, se 1:23 foi selecionado, então, em todos os dias, o patch automático será executado às 13:23.
O tempo de escaneamento depende das configurações na agenda V&PM (por exemplo, o escaneamento pode ser forçado manualmente editando as configurações da agenda) ou apenas a agenda determina a hora em que o patch é aplicado?	O escaneamento não pode ser forçado manualmente, ele é executado apenas pela agenda.
Existe um tempo definido para o escaneamento ou o período de tempo é aleatório?	A tarefa de escaneamento é executada para os dias da semana selecionados usando o valor de hora de início. Por exemplo, na segunda e sexta-feira a **Hora de início** é 1:00. A **Hora de término** é às 11:00, o que significa que o escaneamento será executado na segunda-feira à 1:00 e na sexta-feira à 1:00.

Processo

Devo esperar ver vulnerabilidades do sistema operacional na página Vulnerabilidades?	O V&PM pode detectar vulnerabilidades de aplicativos e vulnerabilidades do sistema operacional.
Como é feito o escaneamento?	Nenhuma verificação ativa da capacidade de exploração é executada. As versões do software instalado são comparadas àquelas listadas no banco de dados como vulneráveis.
Quando a tarefa de aplicação de patches diz que foi concluída, o que isso significa? O patch foi aplicado na máquina com sucesso ou a solicitação de patch foi enviada com sucesso? Por que as tarefas de atualização parecem ser aplicadas com sucesso enquanto nenhum patch foi realmente aplicado?	O produto de endpoint inicia o comando no sistema operacional. Não há outra maneira de acompanhar os resultados da operação msiexec; portanto, se o comando for transmitido com sucesso, a tarefa será concluída com um resultado bem-sucedido.

Relatórios de diagnóstico e ELC?	Para coletar relatórios avançados V&PM: 1.Pressione F5 > clique em Ferramentas > Diagnóstico > Habilitar o Gerenciamento de patch e de vulnerabilidade para habilitar o registro em relatório avançado de diagnóstico do V&PM. 2.Reproduza o problema. 3.Desative o registro em relatório avançado (caso contrário, os dados coletados não serão gravados no relatório). 4.Colete relatórios ELC + SysInspector com ELC 4.9.0 e posterior.
Onde posso encontrar um relatório de patches aplicados e com falha?	Você pode criar seu relatório com a lista de computadores do par CVE/patch, mas, no momento, não é possível criar um relatório com tarefas com falha, nem mesmo para ver os resultados da tarefa em que a aplicação de patches em um sistema operacional é feita e também registrada pelo sistema operacional.
Quanto tempo um comando de atualização manual leva para corrigir um aplicativo para ser aplicado no endpoint?	O patch manual será executado assim que o Agente se conectar. O comando Atualizar criará uma tarefa Aplicar patch de aplicativo que será acionada imediatamente.
Se a reinicialização ocorrer quando nem todos os patches foram aplicados, o processo continuará após a reinicialização?	Temos apenas uma tarefa de patch que itera por todos os aplicativos e patches um por um, se um deles exigir uma reinicialização, a mensagem de reinicialização será exibida após a conclusão da iteração. A reinicialização não acontece sem qualquer notificação e durante a iteração através da lista de aplicativos a terem patches aplicados. Embora alguns aplicativos sejam reiniciados diretamente após a aplicação do patch sem nos informar que uma reinicialização é necessária, e já temos um ticket aberto, isso não deve acontecer. Mas se ele reiniciar, o patch não continuará de onde saiu, mesmo que estejamos no intervalo de tempo certo; ele será executado na próxima vez.
Existe uma maneira de instalar uma versão específica dos aplicativos? Não só a versão mais recente?	Não é possível aplicar patch no software compatível apenas para a versão mais recente.
Como será o download de pacotes de instalação de patches? Ele será hospedado pela ESET ou apenas armazenado em cache?	Download direto somente da máquina de endpoint.
A reinicialização do computador tem algum efeito na atualização/gerenciamento de patches do aplicativo?	Não, reiniciar é necessário apenas se a aplicação de patches no final do patch exigir uma reinicialização e, neste caso, notificaremos o usuário de que uma reinicialização é necessária.

Segurança para ESET PROTECT

Introdução

O objetivo deste documento é controlar as práticas de segurança e os controles de segurança aplicados dentro do ESET PROTECT Cloud. As práticas e controles de segurança são feitos para proteger a confidencialidade, integridade e disponibilidade das informações do cliente. Observe que as práticas e controles de segurança podem mudar.

Escopo

O escopo deste documento é ampliar as práticas de segurança e controles de segurança para infraestrutura do ESET PROTECT Cloud, ESET Business Account (doravante chamado de "EBA"), e infraestrutura do ESET MSP Administrator (doravante chamado de "EMA"), organização, pessoal e processos operacionais. Práticas e controles de segurança incluem:

1. Políticas de segurança da informação
2. Organização da segurança da informação
3. Segurança de recursos humanos
4. Gerenciamento de ativos
5. Controle de Acesso
6. Criptografia
7. Segurança física e ambiental
8. Segurança de operações
9. Segurança de comunicações
10. Aquisição, desenvolvimento e manutenção do sistema
11. Relação de fornecedor
12. Gerenciamento de incidentes de segurança de informações
13. Aspectos de segurança de informação do gerenciamento de continuidade dos negócios
14. Compliance

Conceito de segurança

A empresa ESET s.r.o. é certificada pela ISO 27001:2013 com o escopo de sistema de gerenciamento integrado explicitamente cobrindo ESET PROTECT Cloud, EBA e serviços EMA.

Portanto, o conceito de segurança da informação usa a estrutura ISO 27001 para implementar uma estratégia de defesa de segurança em camadas ao aplicar controles de segurança na camada de rede, sistemas operacionais, bancos de dados, aplicativos, pessoal e processos operacionais. As práticas de segurança aplicadas e controles de segurança têm como objetivo se sobrepor e se complementar.

Práticas e controles de segurança

1. Políticas de segurança da informação

A ESET usa políticas de segurança da informação para cobrir todos os aspectos do padrão ISO 27001, incluindo a governança da segurança da informação e controles e práticas de segurança. As políticas são revisadas anualmente e atualizadas depois de alterações significativas para garantir sua adequação e eficácia contínuas.

A ESET realiza revisões anuais desta política e verificações de segurança internas para garantir a coerência com esta política. A não conformidade com as políticas de segurança da informação está sujeita a ações disciplinares para os funcionários da ESET ou penalidades contratuais até a rescisão do contrato para os fornecedores.

2. Organização da segurança da informação

A organização da segurança da informação para ESET PROTECT Cloud é composta por várias equipes e pessoas envolvidos na segurança da informação e de TI, incluindo:

- Gerenciamento executivo da ESET
- Equipes de segurança interna da ESET

- Equipes de TI de aplicativos empresariais
- Outras equipes de apoio

As responsabilidades de segurança da informação são alocadas alinhadas com as políticas de segurança da informação implementadas. Processos internos são identificados e avaliados para qualquer risco de modificação não autorizada ou não intencional ou uso indevido dos ativos ESET. Atividades perigosas ou sensíveis de processos internos adotam o princípio da separação de deveres para mitigar o risco.

A equipe jurídica da ESET é responsável por contatos com autoridades do governo, incluindo reguladores eslovacos sobre cibersegurança e proteção de dados pessoais. A equipe de Segurança Interna da ESET é responsável por entrar em contato com grupos de interesse especiais como ISACA. A equipe do laboratório de pesquisa da ESET é responsável pela comunicação com outras empresas de segurança e pela comunidade de cibersegurança em geral.

A segurança de informações é contada no gerenciamento de projeto usando a estrutura de gerenciamento de projeto aplicada, desde a concepção do projeto até sua conclusão.

O trabalho remoto e a troca de dados são cobertos pelo uso de uma política implementada em dispositivos móveis, que inclui o uso de uma forte proteção criptográfica de dados em dispositivos móveis enquanto viajam por redes não confiáveis. Controles de segurança em dispositivos móveis são projetados para funcionar independentemente das redes internas e dos sistemas internos da ESET.

3. Segurança de recursos humanos

A ESET usa práticas padrão de recursos humanos, incluindo políticas projetadas para ajudar na segurança da informação. Essas práticas cobrem todo o ciclo de vida dos funcionários, e são aplicadas a todas as equipes que acessam o ambiente ESET PROTECT Cloud.

4. Gerenciamento de ativos

A infraestrutura ESET PROTECT Cloud é incluída nas responsabilidades da ESET com propriedade rígida e regras aplicadas de acordo com o tipo de modelo e sensibilidade. A ESET tem um esquema de classificação interna definido. Todos os dados e configurações do ESET PROTECT Cloud são classificados como confidenciais.

5. Controle de Acesso

A política de Controle de acesso da ESET governa todos os acessos no ESET PROTECT Cloud. O controle de acesso é definido na infraestrutura, serviços de rede, sistema operacional, banco de dados e nível de aplicativo. O gerenciamento completo do acesso do usuário no nível do aplicativo é autônomo. O login único do ESET PROTECT Cloud e ESET Business Account é governado por um provedor de identidade central, que garante que o usuário possa acessar apenas o locatário autorizado. O aplicativo usa permissões padrão do ESET PROTECT Cloud para aplicar o controle de acesso baseado em função para o locatário.

O acesso ao backend da ESET é estritamente limitado a pessoas e funções autorizadas. Processos padrão da ESET para (des)registro de usuário, (de)provisionamento, gerenciamento de privilégios e revisão dos direitos de acesso do usuário são usados para gerenciar o acesso de funcionários da ESET à infraestrutura e às redes do ESET PROTECT Cloud.

Uma autenticação forte está implementada para proteger o acesso a todos os dados do ESET PROTECT Cloud.

6. Criptografia

Para proteger os dados do ESET PROTECT Cloud, uma criptografia forte é usada para criptografar dados em

descanso e em trânsito. Uma autoridade de certificação geralmente confiável é usada para emitir certificados para serviços públicos. A infraestrutura interna de chave pública ESET é usada para gerenciar chaves dentro da infraestrutura do ESET PROTECT Cloud. Os dados armazenados no banco de dados são protegidos por chaves de criptografia geradas pela nuvem. Todos os dados de backup são protegidos por chaves gerenciadas pela ESET.

7. Segurança física e ambiental

Como o ESET PROTECT Cloud e o ESET Business Account são baseados na nuvem, contamos com o Microsoft Azure para a segurança física e ambiental. O Microsoft Azure usa centros de dados certificados com medidas robustas de segurança física. A localização física do centro de dados depende da escolha da região do cliente. Uma criptografia forte é usada para proteger dados do cliente durante o transporte fora do local do ambiente de nuvem (por exemplo, em conjunto com um armazenamento de dados de backup físico).

8. Segurança de operações

O serviço ESET PROTECT Cloud é operado através de meios automatizados com base em procedimentos operacionais e modelos de configuração estritos. Todas as alterações, incluindo alterações de configuração e nova implantação de pacote, são aprovadas e testadas em um ambiente de teste dedicado antes da implantação para a produção. Ambientes de desenvolvimento, teste e produção são separados um do outro. Os dados ESET PROTECT Cloud estão localizados apenas no ambiente de produção.

O ambiente ESET PROTECT Cloud é supervisionado usando o monitoramento operacional para identificar problemas e fornecer capacidade suficiente para todos os serviços na rede e nos níveis de host.

Todos os dados de configuração são armazenados em nossos repositórios de backup regulares para permitir a recuperação automatizada da configuração de um ambiente. Os backups de dados ESET PROTECT Cloud são armazenados no local e fora do local.

Backups são criptografados e testados regularmente para capacidade de recuperação como parte de testes de negócios.

A auditoria em sistemas é realizada de acordo com padrões e diretrizes internos. Relatórios e eventos da infraestrutura, sistema operacional, banco de dados, servidores de aplicativo e controles de segurança são coletados continuamente. Os relatórios são processados ainda mais por equipes de TI e segurança interna para identificar anomalias operacionais e de segurança e incidentes de segurança de informações.

A ESET usa um processo geral de gerenciamento de vulnerabilidades técnicas para lidar com a ocorrência de vulnerabilidades na infraestrutura ESET, incluindo ESET PROTECT Cloud e outros produtos ESET. Esse processo inclui o escaneamento proativo de vulnerabilidade e testes repetitivos de segurança de infraestrutura, produtos e aplicativos.

A ESET declara diretrizes internas para a segurança da infraestrutura interna, redes, sistemas operacionais, bancos de dados, servidores de aplicativos e aplicativos. Essas diretrizes são verificadas através do monitoramento de conformidade técnica e do nosso programa interno de auditoria de segurança de informações.

9. Segurança de comunicações

O ambiente ESET PROTECT Cloud é segmentado através da segmentação de nuvem nativa com acesso de rede limitado apenas aos serviços necessários entre os segmentos de rede. A disponibilidade de serviços de rede é realizada através de controles nativos da nuvem como zonas de disponibilidade, balanceamento de carga e redundância. Componentes dedicados de balanceamento de carga são implantados para fornecer endpoints específicos para roteamento de instância do ESET PROTECT Cloud que aplicam a autorização de tráfego e balanceamento de carga. O tráfego da rede é monitorado continuamente em busca de anomalias operacionais e

de segurança. Os potenciais ataques podem ser resolvidos usando controles nativos de nuvem ou soluções de segurança implantadas. Toda a comunicação de rede é criptografada através de técnicas geralmente disponíveis, incluindo IPsec e TLS.

10. Aquisição, desenvolvimento e manutenção do sistema

O desenvolvimento de sistemas ESET PROTECT Cloud é realizado de acordo com a política de desenvolvimento de software seguro da ESET. Equipes de segurança interna são incluídas no projeto de desenvolvimento do ESET PROTECT Cloud desde a fase inicial e supervisionam todas as atividades de desenvolvimento e manutenção. A equipe de segurança interna define e verifica o cumprimento dos requisitos de segurança em diversos momentos do desenvolvimento do software. A segurança de todos os serviços, incluindo os recentemente desenvolvidos, é testada continuamente depois do lançamento.

11. Relação de fornecedor

Uma relação de fornecedor relevante é conduzida de acordo com diretrizes válidas da ESET, que cobrem o gerenciamento de relacionamento por completo e os requisitos contratuais da perspectiva de segurança da informação e privacidade. A qualidade e a segurança dos serviços prestados pelo provedor de serviço crítico são avaliados regularmente.

Além disso, a ESET utiliza o princípio de portabilidade para o ESET PROTECT Cloud para evitar o bloqueio do fornecedor.

12. Gerenciamento de segurança de informações

O gerenciamento de incidentes de segurança de informações no ESET PROTECT Cloud é realizado de forma similar a outras infraestruturas da ESET e conta com procedimentos de resposta a incidentes definidos. As funções dentro da resposta a incidentes são definidas e alocadas em várias equipes, incluindo TI, segurança, jurídico, recursos humanos, relações públicas e gerenciamento executivo. A equipe de resposta a incidentes para um incidente é estabelecida com base na triagem de incidentes pela equipe de segurança interna. Essa equipe fornecerá ainda mais informações sobre outras equipes lidando com o incidente. A equipe de segurança interna também é responsável pela coleta de provas e por lições aprendidas. A ocorrência e a resolução de incidentes são comunicadas às partes afetadas. A equipe jurídica da ESET é responsável por notificar os corpos regulatórios se necessário, de acordo com o Regulamento Geral de Proteção de Dados (GDPR) e com a Lei de Cibersegurança que transpõe a Diretiva de Segurança da Informação e Rede (NIS).

13. Aspectos de segurança de informação do gerenciamento de continuidade dos negócios

A continuidade de negócios do serviço ESET PROTECT Cloud é codificada na arquitetura robusta usada para aumentar ao máximo a disponibilidade dos serviços fornecidos. A restauração completa de dados de backup e configuração fora do local é possível no caso de uma falha total de todos os nós redundantes para componentes do ESET PROTECT Cloud ou o serviço ESET PROTECT Cloud. O processo de restauração é testado regularmente.

14. Compliance

A conformidade com os requisitos regulatórios e contratuais do ESET PROTECT Cloud é regularmente avaliada e revisada de maneira semelhante a outras infraestruturas e processos da ESET, e as medidas necessárias são realizadas continuamente para garantir a conformidade. A ESET está registrada como um provedor de serviço digital para o serviço digital de Computação em nuvem, que cobre vários serviços ESET, inclusive o ESET PROTECT Cloud. Observe que as atividades de conformidade da ESET não necessariamente significam que os requisitos gerais de conformidade dos clientes estão cumpridos como tal.

Termos de uso

Em vigor a partir de 29 de setembro de 2023 | Veja uma versão anterior dos Termos de Uso | Comparar alterações

Este Termo de Uso ("Termos") constitui o acordo especial entre a ESET, spol. s r. o., tendo sua sede em Einsteinova 24, 85101 Bratislava, Slovak Republic, Número de registro da empresa: 31333532 ("ESET" ou "Provedor") e você, uma pessoa física ou jurídica ("Você" ou "Usuário") que acessa uma conta para administração, ESET PROTECT Cloud e que usa serviços on-line de propriedade de e fornecidos pela ESET ("Conta") que estão todos especificados na documentação aplicável que pode ser acessada na Ajuda on-line ESET ("documentação"). Se você usar a Conta em nome de uma organização, então estará concordando com estes Termos para essa organização e estará garantindo que tem a autoridade para vincular essa organização a estes Termos. Nesse caso, Você e Usuário se referirão a essa organização. Leia esses Termos com cuidado. Eles se relacionam também aos serviços prestados pela ESET através de ou em relação à Conta. As condições específicas para o uso de serviços individuais além desses Termos são declaradas em cada serviço, com a aceitação fazendo parte do processo de ativação do serviço.

Segurança e Proteção de dados

A Conta oferece acesso aos serviços fornecidos pela ESET. O nome completo do usuário, nome da empresa, país, endereço de email válido, número de telefone, dados de licenciamento e estatísticas são necessários para o registro e uso da Conta e para o fornecimento e manutenção dos serviços acessados através da Conta. Você doravante concorda que dados sejam coletados e transferidos para os servidores do Provedor ou de seus parceiros, sendo a finalidade disso garantir a funcionalidade e a autorização para usar os serviços do Software e a proteção dos direitos do Provedor. Seguindo a conclusão destes Termos, o Provedor ou qualquer de seus parceiros comerciais terão o direito de transferir, processar e armazenar dados essenciais que identifiquem Você para fins de suporte e para os fins da execução destes Termos. Você está autorizado a usar a Conta apenas para os fins e para a forma pretendidos sob esses Termos, termos de serviço individuais e documentação.

Você é responsável por manter a segurança da sua Conta e das credenciais necessárias para fazer login. A ESET não será responsável por quaisquer perdas ou danos resultantes da sua falha em cumprir com esta obrigação de manter a segurança. O Usuário também é responsável por qualquer atividade relacionada ao uso da Conta, autorizada ou não. Se a Conta for comprometida você deve notificar o Provedor imediatamente.

Para fornecer o serviço de administração da Conta, é necessária a coleta de dados em relação aos dispositivos gerenciados junto com as informações de administração (doravante os “Dados”). Dados são fornecidos a Você pela ESET apenas para os fins do fornecimento de serviço de administração da Conta. Os Dados serão processados e armazenados de acordo com as políticas e práticas de segurança da ESET, assim como de acordo com a Política de Privacidade.

Dados, assim como outros relatórios relacionados à Conta, devem ser armazenados de acordo com a Política de retenção de relatórios.

Detalhes sobre a privacidade, proteção de dados pessoais e direitos como sujeito de dados podem ser encontrados na Política de Privacidade.

Segurança de dados da API

Ao usar a Interface de Programação de Aplicativo ("API"), Você reconhece e concorda que quaisquer dados ou informações transmitidas ou recebidas pela API podem sair da ou entrar na infraestrutura segura da ESET. Isso inclui, sem limitação, instruções, solicitações, comandos ou diretrizes recebidas de sistemas ou redes de terceiros.

Você entende que a ESET não pode garantir a segurança ou confidencialidade dos dados ou informações transmitidos para ou recebidos pela API, e a ESET não será responsabilizada por qualquer acesso não autorizado, divulgação, perda, danos ou uso errôneo de tais dados ou informações.

Você declara e garante que implementou medidas de segurança apropriadas para proteger os dados e as informações transmitidas para a API, e para quaisquer instruções recebidas de terceiros por meio da API. Você aceita ser o único responsável pela segurança e confidencialidade dos dados e informações assim que elas saírem da ou entrarem na infraestrutura da ESET, assim como pela interpretação e execução de quaisquer instruções recebidas por meio da API. Você reconhece que assume todos os riscos associados com a interação da API com sistemas ou redes de terceiros, incluindo sem limitação os riscos de interferência maliciosa.

Política de Uso Justo

Você é obrigado a cumprir com as limitações técnicas estipuladas na documentação. Você concorda que Você somente usará a Conta e suas funções de uma forma que não limite as possibilidades de outros Usuários acessarem esses serviços. O Provedor reserva o direito de limitar o escopo de serviços oferecidos para os Usuários individuais, para habilitar o uso de serviços pelo número mais alto possível de Usuários. A limitação do escopo de serviços também deve significar a eliminação total da possibilidade de usar qualquer uma das funções da Conta e exclusão dos Dados e informação.

O Provedor também reserva o direito de limitar a quantidade de dispositivos gerenciados sob a Conta. Você pode adicionar e gerenciar até 50000 dispositivos endpoint.

Limitação de Uso

O uso da Conta é estritamente limitado ao gerenciamento do produto ativado com as Licenças elegíveis para nuvem. O ESET Full Disk Encryption deve ser usado apenas nos endpoints com produtos de segurança endpoint instalados e ativados por Licenças elegíveis para nuvem ou separadamente, sem ultrapassar o número total de licenças elegíveis para nuvem obtidas. O Provedor também reserva o direito de limitar o número de produtos gerenciados sob a Conta caso Você não cumpra com esta limitação.

Localização

O Provedor pode permitir que você escolha entre os locais de hospedagem disponíveis para a Conta, incluindo a localização recomendada escolhida pelo Provedor. Você reconhece que, ao escolher outro local que não o recomendado, sua experiência de usuário pode ser afetada. Com base no local escolhido, poderão ser aplicáveis o Contrato de Proteção de Dados incluído no Anexo nº. 2 desse Contrato e as Cláusulas Contratuais Padrão incluídas no Anexo nº. 3 desse Contrato. A ESET reserva-se o direito de alterar um local específico a qualquer momento, sem aviso prévio, com o objetivo de aprimorar os serviços prestados pela ESET, em conformidade com Suas preferências de local (por exemplo, União Europeia).

Software

A ESET ou seus respectivos fornecedores possuem ou podem exercer direitos autorais em todos os softwares disponíveis nos sites da Conta (doravante denominados "Software"). O Software pode ser usado somente de acordo com o Acordo de licença do Usuário Final (doravante denominado “EULA”). O EULA é fornecido juntamente com o Software, ou faz parte dele. O software fornecido com o EULA não pode ser instalado sem o consentimento do usuário com o EULA. Outras informações sobre licenças, direitos autorais, documentação e marcas registradas estão estipuladas no Informações legais.

Restrições

Você não pode copiar, distribuir, extrair componentes ou produzir trabalhos derivativos da Conta. Ao usar a Conta, Você é obrigado a cumprir as seguintes restrições:

(a) Você não pode usar, modificar, traduzir ou reproduzir a Conta ou transferir direitos para uso da Conta ou seus componentes de qualquer forma que não conforme expressamente fornecido nestes Termos.

(b) Você não pode vender, sublicenciar, arrendar ou alugar ou emprestar a Conta ou usar a Conta para a prestação de serviços comerciais.

(c) Você não pode fazer engenharia reversa, reverter a compilação ou desmontar a Conta ou tentar descobrir de outra maneira o código fonte da Conta, exceto na medida em que essa restrição for expressamente proibida por lei.

(d) Você concorda que Você usará a Conta somente de uma maneira que esteja de acordo com todas as leis aplicáveis na jurisdição em que Você usa a Conta, incluindo sem limitação, restrições aplicáveis relacionadas a direitos autorais e a outros direitos de propriedade intelectual.

Aviso de isenção de responsabilidade

COMO O USUÁRIO, VOCÊ RECONHECE QUE A CONTA, ASSIM COMO OS SERVIÇOS, SÃO FORNECIDOS "NA CONDIÇÃO EM QUE SE ENCONTRAM", 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 A CONTA OU SERVIÇO NÃO INFRINGIRÁ QUAISQUER PATENTES DE TERCEIROS, DIREITOS AUTORAIS, MARCAS COMERCIAIS OU OUTROS DIREITOS. NÃO HÁ GARANTIA DO PROVEDOR OU QUALQUER OUTRA PARTE DE QUE A CONTA OU OS SERVIÇOS ATENDERÃO SEUS REQUISITOS OU QUE A OPERAÇÃO DA CONTA OU DOS SERVIÇOS NÃO SERÁ INTERROMPIDA E NÃO TERÁ ERROS. VOCÊ ASSUME TOTAL RESPONSABILIDADE E RISCO PELA SELEÇÃO E USO DA CONTA E DOS SERVIÇOS PARA ATINGIR OS RESULTADOS PRETENDIDOS E OBTIDOS A PARTIR DELA.

Estes Termos não criam obrigações por parte do Provedor e de seus licenciadores diferentes daquelas especificamente definidas neste documento.

Limitação de Responsabilidade

ATÉ A EXTENSÃO MÁXIMA PERMITIDA PELA LEGISLAÇÃO APLICÁVEL, EM NENHUMA HIPÓTESE, O PROVEDOR, SEUS FUNCIONÁRIOS OU CONTRATADOS 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 DO USO OU DA INCAPACIDADE DE USAR A CONTA, MESMO QUE O PROVEDOR, SEUS CONTRATADOS 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, CONTRATADOS OU AFILIADOS, NESSES CASOS, DEVERÁ ESTAR LIMITADA À SOMA QUE VOCÊ PAGOU PELO SERVIÇO OU CONTA EM QUESTÃO.

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 esses Termos 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 esses Termos 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 da seção (a) desta cláusula de Conformidade com o controle comercial desses Termos; 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 esses Termos poderia resultar na ESET ou suas Filiais violarem, ou estarem sujeitas a consequências negativas sob, as Leis de Controle Comercial.

(c) Nada nesses Termos 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.

Legislação governante e idioma

Esses Termos serão governados por e construídos de acordo com a legislação eslovaca. O Usuário Final e o Provedor concordam que as disposições conflitantes da legislação reguladora e a Convenção das Nações Unidas sobre Contratos de Venda Internacional de Bens não deverão se aplicar a este Contrato. Se Você é um consumidor com residência habitual na UE, Você também tem proteção adicional concedida a Você pelas disposições obrigatórias da lei aplicável em seu país de residência.

Você concorda expressamente que a jurisdição exclusiva para qualquer reivindicação ou disputa com o Provedor ou relacionada de qualquer forma ao seu uso do Software, da Conta ou dos Serviços ou que surja desses Termos ou Termos Especiais (se aplicável) reside no Tribunal Regional de Bratislava I, Eslováquia, e você também concorda e consente expressamente com o exercício da jurisdição pessoal no Tribunal Regional de Bratislava I em conexão com tal disputa ou reivindicação. Se Você é um consumidor e tem residência habitual na UE, Você também pode fazer uma reivindicação para aplicar seus direitos de consumidor no lugar de jurisdição exclusiva ou no país da UE em que Você vive. Além disso, Você também pode usar uma plataforma de solução de disputas on-

line, que pode ser acessada aqui: https://ec.europa.eu/consumers/odr/. Porém, considere entrar em contato conosco primeiro antes de criar qualquer reivindicação oficialmente.

Se ocorrer qualquer discrepância entre as versões de idiomas destes Termos, a versão em inglês disponível aqui deverá sempre prevalecer.

Disposições gerais

A ESET reserva o direito de revisar estes Termos e documentação ou qualquer parte deles, a qualquer momento atualizando o documento relevante para refletir alterações na legislação ou alterações na Conta. Você será notificado sobre qualquer revisão desses Termos através da sua Conta. Se você não concordar com as alterações destes Termos, você pode cancelar sua Conta. A menos que Você cancele sua Conta depois de ser notificado sobre as mudanças, Você estará vinculado a quaisquer aditamentos ou revisões desses Termos. Você é incentivado a visitar periodicamente esta página para verificar os Termos atualizado que se aplicam ao seu uso da Conta.

Avisos

Todos os avisos devem ser entregues a: ESET, spol. s r. o., Einsteinova 24, 85101 Bratislava, Slovak Republic.

Anexo nº. 1

EULA do ESET Management Agent

Anexo nº. 2

Contrato de processamento de dados

Anexo nº. 3

Cláusulas contratuais padrão

Acordo de licença para o usuário final do Agente ESET Management

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 importas 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

Dados de Comunicação e Gerenciamento. Provisões adicionais são aplicáveis aos Dados de Comunicação e Gerenciamento da seguinte forma:

O Software contém uma função que permite a transferência de informações entre o Computador 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 serão determinados pelas configurações do software instalado no Computador. O conteúdo das instruções do software de gerenciamento será determinado pelas configurações do software de gerenciamento remoto.

EULAID: EULA-PRODUCT-AGENT; 3537.0

Contrato de processamento de dados

Em conformidade com os requisitos do Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho de 27 de abril de 2016, relativo à proteção das pessoas físicas no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados, revogando a Diretiva 95/46/EC (referido doravante como "GDPR"), o Provedor (referido doravante como o "Processador") e Você (referido doravante como "Controlador") estão entrando no relacionamento contratual de processamento de dados para definir os termos e condições para o processamento de dados pessoais, a maneira de sua proteção, e também para definir outros direitos e obrigações de ambas as partes no processamento de dados pessoais de titulares de dados em nome do Controlador durante o curso da execução do objeto destes Termos como o contrato principal.

1. **Tratamento de dados pessoais.** Os serviços prestados em conformidade com estes Termos incluem o tratamento de informações relacionadas a uma pessoa física identificada ou identificável listada na Política de Privacidade (doravante os "Dados Pessoais").

2. **Autorização.** O Responsável pelo Tratamento autoriza o Subcontratante para processar Dados Pessoais, incluindo as instruções a seguir:

(i) "Finalidade do processamento" significa a prestação de serviços em conformidade com estes Termos. O Subcontratante só pode processar Dados Pessoais em nome do Responsável pelo Tratamento em relação à prestação de serviços solicitados pelo Responsável pelo Tratamento. Todas as informações coletadas para fins adicionais serão processadas fora da relação contratual Responsável pelo Tratamento-Subcontratante.

(ii) período de processamento significa o período iniciado quando se inicia a cooperação sob estes Termos e terminando na rescisão dos serviços,

(iii) Escopo e Categorias de Dados pessoais. Os Serviços são pretendidos apenas para o tratamento de dados

pessoais. Porém, o Responsável pelo Tratamento é o único responsável pela determinação do escopo de dados pessoais.

(iv) “Titular dos dados” significa a pessoa física como usuário autorizado dos dispositivos do Controlador,

(v) operações de processamento são todas e quaisquer operações necessárias para o processamento,

(vi) “Instruções documentadas” significa instruções descritas nestes Termos, seus Anexos, na Política de Privacidade e na documentação do serviço. O Responsável pelo Tratamento será responsável pela responsabilidade legal do processamento de Dados Pessoais pelo Subcontratante em relação às respectivas disposições aplicáveis da lei de proteção de dados.

3. **Obrigações do Subcontratante.** O Processador será obrigado a:

(i) processar Dados Pessoais apenas com base nas Instruções documentadas e para os fins definidos nos Termos, seus Anexos, na Política de Privacidade e na documentação de serviço,

(ii) instruir as pessoas autorizadas a processar os Dados Pessoais (doravante as "Pessoas Autorizadas") sobre seus direitos e deveres de acordo com o GDPR, sobre sua responsabilidade em caso de violação e garantir que as Pessoas Autorizadas comprometeram-se a manter a confidencialidade e a seguir as instruções Documentadas,

(iii) implementar e seguir as medidas descritas nos Termos, seus Anexos, na Política de Privacidade e na documentação de serviço,

(iv) auxiliar o Responsável pelo Tratamento a responder a solicitações dos Titulares dos Dados relacionadas aos seus direitos. O Subcontratante não deve corrigir, remover ou restringir o tratamento de Dados Pessoais sem as instruções do Responsável pelo Tratamento. Todas as solicitações do Titular dos Dados relacionadas a Dados Pessoais processados em nome do Responsável pelo Tratamento serão encaminhadas ao Responsável pelo Tratamento sem atraso.

(v) auxiliar o Responsável pelo Tratamento com a notificação de violação de dados pessoais à autoridade supervisora e ao Titular dos Dados, O Subcontratante notificará o Responsável pelo Tratamento sobre qualquer violação do processamento de dados pessoais ou da segurança dos dados pessoais imediatamente após tal descoberta. O Subcontratante deve cooperar de forma razoável em uma investigação e correção de tal violação e tomar medidas razoáveis para limitar outras implicações negativas.

(vi) por escolha do Responsável pelo Tratamento remover ou devolver todos os Dados Pessoais ao Responsável pelo Tratamento após o fim do Período de Tratamento. O Responsável pelo Tratamento se compromete a informar o Subcontratante sobre sua decisão no prazo de dez (10) dias após o término do Período de Processamento. Essa disposição não afetará o direito do Subcontratante de manter os Dados Pessoais na extensão necessária para fins de arquivamento no interesse público, fins de pesquisa científica, fins estatísticos ou para o estabelecimento, exercício ou defesa de reivindicações judiciais.

(vii) manter um registro atualizado de todas as categorias de atividades de processamento que ele realizou em nome do Controlador,

(viii) disponibilizar todas as informações necessárias para demonstrar conformidade como parte dos Termos, seus Anexos, da Política de Privacidade e da documentação de serviço disponíveis ao Responsável pelo Tratamento. No caso de auditoria ou controle do processamento de Dados Pessoais do lado do Responsável pelo Tratamento, o Responsável pelo Tratamento será obrigado a informar o Subcontratante por escrito pelo menos dez (30) dias antes da auditoria ou controle planejado.

4. **Contratação de outro Subcontratante.** O Subcontratante tem o direito de contratar outro subcontratante para

realizar atividades de tratamento específicas, como o fornecimento de armazenamento em nuvem e infraestrutura para o serviço, em conformidade com estes Termos, seus Anexo, a Política de Privacidade e a documentação do serviço. Atualmente, a Microsoft fornece armazenamento em nuvem e infraestrutura como parte do Azure Cloud Service. Mesmo neste caso, o Processador permanecerá o único ponto de contato e a parte responsável pela conformidade. O Subcontratante se compromete a informar o Responsável pelo Tratamento sobre qualquer adição ou substituição de outro subcontratante para fins da possibilidade de contestar tal alteração.

5. **Território de processamento.** O Processador garante que o processamento ocorra no Espaço Econômico Europeu ou em um país designado como seguro por decisão da Comissão Europeia, com base na decisão do Controlador. As Cláusulas Contratuais Padrão serão aplicadas em caso de transferências e tratamentos localizados fora do Espaço Econômico Europeu ou de um país designado como seguro por decisão da Comissão Europeia, por solicitação do Responsável pelo Tratamento.

6. **Segurança.** O Processador é certificado pela ISO 27001:2013 e usa a estrutura da ISO 27001 para implementar uma estratégia de defesa de segurança em camadas ao aplicar controles de segurança na camada de rede, sistemas operacionais, bancos de dados, aplicativos, pessoal e processos operacionais. A conformidade com os requisitos regulatórios e contratuais é regularmente avaliada e revisada de maneira semelhante a outras infraestruturas e operações do Processador, e as medidas necessárias são realizadas continuamente para garantir a conformidade. O Subcontratante organizou a segurança de dados usando ISMS com base em ISO 27001. A documentação de segurança inclui principalmente documentos de política para segurança da informação, segurança física e segurança de equipamentos, gerenciamento de incidentes, tratamento de vazamentos de dados e incidentes de segurança, etc.

7. **Medidas Técnicas e Organizacionais**. O Subcontratante deve proteger os Dados Pessoais contra danos e destruição casuais e ilegais, perda casual, mudança, acesso não autorizado e divulgação. Para cumprir este objetivo, o Subcontratante deverá adotar as medidas técnicas e organizativas adequadas ao modo de tratamento e ao risco que representa o tratamento dos direitos dos Titulares dos Dados em conformidade com os requisitos do GDPR. Uma descrição detalhada das medidas técnicas e organizacionais consta da Política de Segurança.

8. **Informações de contato do Subcontratante.** Todas as notificações, solicitações, demandas e outras comunicações relacionadas à proteção de dados pessoais devem ser endereçadas à ESET, spol. s.r.o., aos cuidados de: Data Protection Officer, Einsteinova 24, 85101 Bratislava, Slovak Republic, email: dpo@eset.sk.

Cláusulas contratuais padrão

SECTION I

Clause 1 Purpose and scope

(a) The purpose of these standard contractual clauses is to ensure compliance with the requirements of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) (1) for the transfer of personal data to a third country.

(b) The Parties:

(i) the natural or legal person(s), public authority/ies, agency/ies or other body/ies (hereinafter ‘entity/ies’) transferring the personal data, as listed in Annex I.A (hereinafter each ‘data exporter’), and

(ii) the entity/ies in a third country receiving the personal data from the data exporter, directly or indirectly via another entity also Party to these Clauses, as listed in Annex I.A (hereinafter each 'data importer')

have agreed to these standard contractual clauses (hereinafter: 'Clauses').

(c) These Clauses apply with respect to the transfer of personal data as specified in Annex I.B.

(d) The Appendix to these Clauses containing the Annexes referred to therein forms an integral part of these Clauses.

Clause 2 Effect and invariability of the Clauses

(a) These Clauses set out appropriate safeguards, including enforceable data subject rights and effective legal remedies, pursuant to Article 46(1) and Article 46(2)(c) of Regulation (EU) 2016/679 and, with respect to data transfers from controllers to processors and/or processors to processors, standard contractual clauses pursuant to Article 28(7) of Regulation (EU) 2016/679, provided they are not modified, except to select the appropriate Module(s) or to add or update information in the Appendix. This does not prevent the Parties from including the standard contractual clauses laid down in these Clauses in a wider contract and/or to add other clauses or additional safeguards, provided that they do not contradict, directly or indirectly, these Clauses or prejudice the fundamental rights or freedoms of data subjects.

(b) These Clauses are without prejudice to obligations to which the data exporter is subject by virtue of Regulation (EU) 2016/679.

Clause 3 Third-party beneficiaries

(a) Data subjects may invoke and enforce these Clauses, as third-party beneficiaries, against the data exporter and/or data importer, with the following exceptions:

(i) Clause 1, Clause 2, Clause 3, Clause 6, Clause 7;

(ii) Clause 8 – Module One: Clause 8.5 (e) and Clause 8.9(b); Module Two: Clause 8.1(b), 8.9(a), (c), (d) and (e); Module Three: Clause 8.1(a), (c) and (d) and Clause 8.9(a), (c), (d), (e), (f) and (g); Module Four: Clause 8.1 (b) and Clause 8.3(b);

(iii) Clause 9 – Module Two: Clause 9(a), (c), (d) and (e); Module Three: Clause 9(a), (c), (d) and (e);

(iv) Clause 12 – Module One: Clause 12(a) and (d); Modules Two and Three: Clause 12(a), (d) and (f);

(v) Clause 13;

(vi) Clause 15.1(c), (d) and (e);

(vii) Clause 16(e);

(viii) Clause 18 – Modules One, Two and Three: Clause 18(a) and (b); Module Four: Clause 18.

(b) Paragraph (a) is without prejudice to rights of data subjects under Regulation (EU) 2016/679.

Clause 4 Interpretation

(a) Where these Clauses use terms that are defined in Regulation (EU) 2016/679, those terms shall have the same meaning as in that Regulation.

(b) These Clauses shall be read and interpreted in the light of the provisions of Regulation (EU) 2016/679.

(c) These Clauses shall not be interpreted in a way that conflicts with rights and obligations provided for in Regulation (EU) 2016/679.

Clause 5 Hierarchy

In the event of a contradiction between these Clauses and the provisions of related agreements between the Parties, existing at the time these Clauses are agreed or entered into thereafter, these Clauses shall prevail.

Clause 6 Description of the transfer(s)

The details of the transfer(s), and in particular the categories of personal data that are transferred and the purpose(s) for which they are transferred, are specified in Annex I.B.

Clause 7 – Optional Docking clause

(a) An entity that is not a Party to these Clauses may, with the agreement of the Parties, accede to these Clauses at any time, either as a data exporter or as a data importer, by completing the Appendix and signing Annex I.A.

(b) Once it has completed the Appendix and signed Annex I.A, the acceding entity shall become a Party to these Clauses and have the rights and obligations of a data exporter or data importer in accordance with its designation in Annex I.A.

(c) The acceding entity shall have no rights or obligations arising under these Clauses from the period prior to becoming a Party.

SECTION II – OBLIGATIONS OF THE PARTIES

Clause 8 Data protection safeguards

The data exporter warrants that it has used reasonable efforts to determine that the data importer is able, through the implementation of appropriate technical and organisational measures, to satisfy its obligations under these Clauses.

MODULE ONE: Transfer controller to controller

8.1 Purpose limitation

The data importer shall process the personal data only for the specific purpose(s) of the transfer, as set out in Annex I.B. It may only process the personal data for another purpose:

(i) where it has obtained the data subject's prior consent;

(ii) where necessary for the establishment, exercise or defence of legal claims in the context of specific administrative, regulatory or judicial proceedings; or

(iii) where necessary in order to protect the vital interests of the data subject or of another natural person.

8.2 Transparency

(a) In order to enable data subjects to effectively exercise their rights pursuant to Clause 10, the data importer shall inform them, either directly or through the data exporter:

(i) of its identity and contact details;

(ii) of the categories of personal data processed;

(iii) of the right to obtain a copy of these Clauses;

(iv) where it intends to onward transfer the personal data to any third party/ies, of the recipient or categories of recipients (as appropriate with a view to providing meaningful information), the purpose of such onward transfer and the ground therefore pursuant to Clause 8.7.

(b) Paragraph (a) shall not apply where the data subject already has the information, including when such information has already been provided by the data exporter, or providing the information proves impossible or would involve a disproportionate effort for the data importer. In the latter case, the data importer shall, to the extent possible, make the information publicly available.

(c) On request, the Parties shall make a copy of these Clauses, including the Appendix as completed by them, available to the data subject free of charge. To the extent necessary to protect business secrets or other confidential information, including personal data, the Parties may redact part of the text of the Appendix prior to sharing a copy, but shall provide a meaningful summary where the data subject would otherwise not be able to understand its content or exercise his/her rights. On request, the Parties shall provide the data subject with the reasons for the redactions, to the extent possible without revealing the redacted information.

(d) Paragraphs (a) to (c) are without prejudice to the obligations of the data exporter under Articles 13 and 14 of Regulation (EU) 2016/679.

8.3 Accuracy and data minimisation

(a) Each Party shall ensure that the personal data is accurate and, where necessary, kept up to date. The data importer shall take every reasonable step to ensure that personal data that is inaccurate, having regard to the purpose(s) of processing, is erased or rectified without delay.

(b) If one of the Parties becomes aware that the personal data it has transferred or received is inaccurate, or has become outdated, it shall inform the other Party without undue delay.

(c) The data importer shall ensure that the personal data is adequate, relevant and limited to what is necessary in relation to the purpose(s) of processing.

8.4 Storage limitation

The data importer shall retain the personal data for no longer than necessary for the purpose(s) for which it is processed. It shall put in place appropriate technical or organisational measures to ensure compliance with this obligation, including erasure or anonymisation (2) of the data and all back-ups at the end of the retention period.

8.5 Security of processing

(a) The data importer and, during transmission, also the data exporter shall implement appropriate technical and organisational measures to ensure the security of the personal data, including protection against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access (hereinafter 'personal data breach'). In assessing the appropriate level of security, they shall take due account of the state of the art, the costs of implementation, the nature, scope, context and purpose(s) of processing and the risks involved in the processing for the data subject. The Parties shall in particular consider having recourse to

encryption or pseudonymisation, including during transmission, where the purpose of processing can be fulfilled in that manner.

(b) The Parties have agreed on the technical and organisational measures set out in Annex II. The data importer shall carry out regular checks to ensure that these measures continue to provide an appropriate level of security.

(c) The data importer shall ensure that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

(d) In the event of a personal data breach concerning personal data processed by the data importer under these Clauses, the data importer shall take appropriate measures to address the personal data breach, including measures to mitigate its possible adverse effects.

(e) In case of a personal data breach that is likely to result in a risk to the rights and freedoms of natural persons, the data importer shall without undue delay notify both the data exporter and the competent supervisory authority pursuant to Clause 13. Such notification shall contain i) a description of the nature of the breach (including, where possible, categories and approximate number of data subjects and personal data records concerned), ii) its likely consequences, iii) the measures taken or proposed to address the breach, and iv) the details of a contact point from whom more information can be obtained. To the extent it is not possible for the data importer to provide all the information at the same time, it may do so in phases without undue further delay.

(f) In case of a personal data breach that is likely to result in a high risk to the rights and freedoms of natural persons, the data importer shall also notify without undue delay the data subjects concerned of the personal data breach and its nature, if necessary in cooperation with the data exporter, together with the information referred to in paragraph (e), points ii) to iv), unless the data importer has implemented measures to significantly reduce the risk to the rights or freedoms of natural persons, or notification would involve disproportionate efforts. In the latter case, the data importer shall instead issue a public communication or take a similar measure to inform the public of the personal data breach.

(g) The data importer shall document all relevant facts relating to the personal data breach, including its effects and any remedial action taken, and keep a record thereof.

8.6 Sensitive data

Where the transfer involves personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, or biometric data for the purpose of uniquely identifying a natural person, data concerning health or a person's sex life or sexual orientation, or data relating to criminal convictions or offences (hereinafter 'sensitive data'), the data importer shall apply specific restrictions and/or additional safeguards adapted to the specific nature of the data and the risks involved. This may include restricting the personnel permitted to access the personal data, additional security measures (such as pseudonymisation) and/or additional restrictions with respect to further disclosure.

8.7 Onward transfers

The data importer shall not disclose the personal data to a third party located outside the European Union (3) (in the same country as the data importer or in another third country, hereinafter 'onward transfer') unless the third party is or agrees to be bound by these Clauses, under the appropriate Module. Otherwise, an onward transfer by the data importer may only take place if:

(i) it is to a country benefitting from an adequacy decision pursuant to Article 45 of Regulation (EU) 2016/679 that covers the onward transfer;

(ii) the third party otherwise ensures appropriate safeguards pursuant to Articles 46 or 47 of Regulation (EU) 2016/679 with respect to the processing in question;

(iii) the third party enters into a binding instrument with the data importer ensuring the same level of data protection as under these Clauses, and the data importer provides a copy of these safeguards to the data exporter;

(iv) it is necessary for the establishment, exercise or defence of legal claims in the context of specific administrative, regulatory or judicial proceedings;

(v) it is necessary in order to protect the vital interests of the data subject or of another natural person; or

(vi) where none of the other conditions apply, the data importer has obtained the explicit consent of the data subject for an onward transfer in a specific situation, after having informed him/her of its purpose(s), the identity of the recipient and the possible risks of such transfer to him/her due to the lack of appropriate data protection safeguards. In this case, the data importer shall inform the data exporter and, at the request of the latter, shall transmit to it a copy of the information provided to the data subject.

Any onward transfer is subject to compliance by the data importer with all the other safeguards under these Clauses, in particular purpose limitation.

8.8 Processing under the authority of the data importer

The data importer shall ensure that any person acting under its authority, including a processor, processes the data only on its instructions.

8.9 Documentation and compliance

(a) Each Party shall be able to demonstrate compliance with its obligations under these Clauses. In particular, the data importer shall keep appropriate documentation of the processing activities carried out under its responsibility.

(b) The data importer shall make such documentation available to the competent supervisory authority on request.

MODULE TWO: Transfer controller to processor

8.1 Instructions

(a) The data importer shall process the personal data only on documented instructions from the data exporter. The data exporter may give such instructions throughout the duration of the contract.

(b) The data importer shall immediately inform the data exporter if it is unable to follow those instructions.

8.2 Purpose limitation

The data importer shall process the personal data only for the specific purpose(s) of the transfer, as set out in Annex I.B, unless on further instructions from the data exporter.

8.3 Transparency

On request, the data exporter shall make a copy of these Clauses, including the Appendix as completed by the Parties, available to the data subject free of charge. To the extent necessary to protect business secrets or other confidential information, including the measures described in Annex II and personal data, the data exporter may

redact part of the text of the Appendix to these Clauses prior to sharing a copy, but shall provide a meaningful summary where the data subject would otherwise not be able to understand the its content or exercise his/her rights. On request, the Parties shall provide the data subject with the reasons for the redactions, to the extent possible without revealing the redacted information. This Clause is without prejudice to the obligations of the data exporter under Articles 13 and 14 of Regulation (EU) 2016/679.

8.4 Accuracy

If the data importer becomes aware that the personal data it has received is inaccurate, or has become outdated, it shall inform the data exporter without undue delay. In this case, the data importer shall cooperate with the data exporter to erase or rectify the data.

8.5 Duration of processing and erasure or return of data

Processing by the data importer shall only take place for the duration specified in Annex I.B. After the end of the provision of the processing services, the data importer shall, at the choice of the data exporter, delete all personal data processed on behalf of the data exporter and certify to the data exporter that it has done so, or return to the data exporter all personal data processed on its behalf and delete existing copies. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit return or deletion of the personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process it to the extent and for as long as required under that local law. This is without prejudice to Clause 14, in particular the requirement for the data importer under Clause 14(e) to notify the data exporter throughout the duration of the contract if it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under Clause 14(a).

8.6 Security of processing

(a) The data importer and, during transmission, also the data exporter shall implement appropriate technical and organisational measures to ensure the security of the data, including protection against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access to that data (hereinafter 'personal data breach'). In assessing the appropriate level of security, the Parties shall take due account of the state of the art, the costs of implementation, the nature, scope, context and purpose(s) of processing and the risks involved in the processing for the data subjects. The Parties shall in particular consider having recourse to encryption or pseudonymisation, including during transmission, where the purpose of processing can be fulfilled in that manner. In case of pseudonymisation, the additional information for attributing the personal data to a specific data subject shall, where possible, remain under the exclusive control of the data exporter. In complying with its obligations under this paragraph, the data importer shall at least implement the technical and organisational measures specified in Annex II. The data importer shall carry out regular checks to ensure that these measures continue to provide an appropriate level of security.

(b) The data importer shall grant access to the personal data to members of its personnel only to the extent strictly necessary for the implementation, management and monitoring of the contract. It shall ensure that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

(c) In the event of a personal data breach concerning personal data processed by the data importer under these Clauses, the data importer shall take appropriate measures to address the breach, including measures to mitigate its adverse effects. The data importer shall also notify the data exporter without undue delay after having become aware of the breach. Such notification shall contain the details of a contact point where more information can be obtained, a description of the nature of the breach (including, where possible, categories and approximate number of data subjects and personal data records concerned), its likely consequences and the measures taken or proposed to address the breach including, where appropriate, measures to mitigate its possible adverse effects. Where, and in so far as, it is not possible to provide all information at the same time, the initial notification shall

contain the information then available and further information shall, as it becomes available, subsequently be provided without undue delay.

(d) The data importer shall cooperate with and assist the data exporter to enable the data exporter to comply with its obligations under Regulation (EU) 2016/679, in particular to notify the competent supervisory authority and the affected data subjects, taking into account the nature of processing and the information available to the data importer.

8.7 Sensitive data

Where the transfer involves personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, or biometric data for the purpose of uniquely identifying a natural person, data concerning health or a person's sex life or sexual orientation, or data relating to criminal convictions and offences (hereinafter 'sensitive data'), the data importer shall apply the specific restrictions and/or additional safeguards described in Annex I.B.

8.8 Onward transfers

The data importer shall only disclose the personal data to a third party on documented instructions from the data exporter. In addition, the data may only be disclosed to a third party located outside the European Union (4) (in the same country as the data importer or in another third country, hereinafter 'onward transfer') if the third party is or agrees to be bound by these Clauses, under the appropriate Module, or if:

(i) the onward transfer is to a country benefitting from an adequacy decision pursuant to Article 45 of Regulation (EU) 2016/679 that covers the onward transfer;

(ii) the third party otherwise ensures appropriate safeguards pursuant to Articles 46 or 47 Regulation of (EU) 2016/679 with respect to the processing in question;

(iii) the onward transfer is necessary for the establishment, exercise or defence of legal claims in the context of specific administrative, regulatory or judicial proceedings; or

(iv) the onward transfer is necessary in order to protect the vital interests of the data subject or of another natural person.

Any onward transfer is subject to compliance by the data importer with all the other safeguards under these Clauses, in particular purpose limitation.

8.9 Documentation and compliance

(a) The data importer shall promptly and adequately deal with enquiries from the data exporter that relate to the processing under these Clauses.

(b) The Parties shall be able to demonstrate compliance with these Clauses. In particular, the data importer shall keep appropriate documentation on the processing activities carried out on behalf of the data exporter.

(c) The data importer shall make available to the data exporter all information necessary to demonstrate compliance with the obligations set out in these Clauses and at the data exporter's request, allow for and contribute to audits of the processing activities covered by these Clauses, at reasonable intervals or if there are indications of non-compliance. In deciding on a review or audit, the data exporter may take into account relevant certifications held by the data importer.

(d) The data exporter may choose to conduct the audit by itself or mandate an independent auditor. Audits may include inspections at the premises or physical facilities of the data importer and shall, where appropriate, be

carried out with reasonable notice.

(e) The Parties shall make the information referred to in paragraphs (b) and (c), including the results of any audits, available to the competent supervisory authority on request.

MODULE THREE: Transfer processor to processor

8.1 Instructions

(a) The data exporter has informed the data importer that it acts as processor under the instructions of its controller(s), which the data exporter shall make available to the data importer prior to processing.

(b) The data importer shall process the personal data only on documented instructions from the controller, as communicated to the data importer by the data exporter, and any additional documented instructions from the data exporter. Such additional instructions shall not conflict with the instructions from the controller. The controller or data exporter may give further documented instructions regarding the data processing throughout the duration of the contract.

(c) The data importer shall immediately inform the data exporter if it is unable to follow those instructions. Where the data importer is unable to follow the instructions from the controller, the data exporter shall immediately notify the controller.

(d) The data exporter warrants that it has imposed the same data protection obligations on the data importer as set out in the contract or other legal act under Union or Member State law between the controller and the data exporter (5).

8.2 Purpose limitation

The data importer shall process the personal data only for the specific purpose(s) of the transfer, as set out in Annex I.B., unless on further instructions from the controller, as communicated to the data importer by the data exporter, or from the data exporter.

8.3 Transparency

On request, the data exporter shall make a copy of these Clauses, including the Appendix as completed by the Parties, available to the data subject free of charge. To the extent necessary to protect business secrets or other confidential information, including personal data, the data exporter may redact part of the text of the Appendix prior to sharing a copy, but shall provide a meaningful summary where the data subject would otherwise not be able to understand its content or exercise his/her rights. On request, the Parties shall provide the data subject with the reasons for the redactions, to the extent possible without revealing the redacted information.

8.4 Accuracy

If the data importer becomes aware that the personal data it has received is inaccurate, or has become outdated, it shall inform the data exporter without undue delay. In this case, the data importer shall cooperate with the data exporter to rectify or erase the data.

8.5 Duration of processing and erasure or return of data

Processing by the data importer shall only take place for the duration specified in Annex I.B. After the end of the provision of the processing services, the data importer shall, at the choice of the data exporter, delete all personal data processed on behalf of the controller and certify to the data exporter that it has done so, or return to the data exporter all personal data processed on its behalf and delete existing copies. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws

applicable to the data importer that prohibit return or deletion of the personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process it to the extent and for as long as required under that local law. This is without prejudice to Clause 14, in particular the requirement for the data importer under Clause 14(e) to notify the data exporter throughout the duration of the contract if it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under Clause 14(a).

8.6 Security of processing

(a) The data importer and, during transmission, also the data exporter shall implement appropriate technical and organisational measures to ensure the security of the data, including protection against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access to that data (hereinafter 'personal data breach'). In assessing the appropriate level of security, they shall take due account of the state of the art, the costs of implementation, the nature, scope, context and purpose(s) of processing and the risks involved in the processing for the data subject. The Parties shall in particular consider having recourse to encryption or pseudonymisation, including during transmission, where the purpose of processing can be fulfilled in that manner. In case of pseudonymisation, the additional information for attributing the personal data to a specific data subject shall, where possible, remain under the exclusive control of the data exporter or the controller. In complying with its obligations under this paragraph, the data importer shall at least implement the technical and organisational measures specified in Annex II. The data importer shall carry out regular checks to ensure that these measures continue to provide an appropriate level of security.

(b) The data importer shall grant access to the data to members of its personnel only to the extent strictly necessary for the implementation, management and monitoring of the contract. It shall ensure that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

(c) In the event of a personal data breach concerning personal data processed by the data importer under these Clauses, the data importer shall take appropriate measures to address the breach, including measures to mitigate its adverse effects. The data importer shall also notify, without undue delay, the data exporter and, where appropriate and feasible, the controller after having become aware of the breach. Such notification shall contain the details of a contact point where more information can be obtained, a description of the nature of the breach (including, where possible, categories and approximate number of data subjects and personal data records concerned), its likely consequences and the measures taken or proposed to address the data breach, including measures to mitigate its possible adverse effects. Where, and in so far as, it is not possible to provide all information at the same time, the initial notification shall contain the information then available and further information shall, as it becomes available, subsequently be provided without undue delay.

(d) The data importer shall cooperate with and assist the data exporter to enable the data exporter to comply with its obligations under Regulation (EU) 2016/679, in particular to notify its controller so that the latter may in turn notify the competent supervisory authority and the affected data subjects, taking into account the nature of processing and the information available to the data importer.

8.7 Sensitive data

Where the transfer involves personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, or biometric data for the purpose of uniquely identifying a natural person, data concerning health or a person's sex life or sexual orientation, or data relating to criminal convictions and offences (hereinafter 'sensitive data'), the data importer shall apply the specific restrictions and/or additional safeguards set out in Annex I.B.

8.8 Onward transfers

The data importer shall only disclose the personal data to a third party on documented instructions from the

controller, as communicated to the data importer by the data exporter. In addition, the data may only be disclosed to a third party located outside the European Union (6) (in the same country as the data importer or in another third country, hereinafter 'onward transfer') if the third party is or agrees to be bound by these Clauses, under the appropriate Module, or if:

(i) the onward transfer is to a country benefitting from an adequacy decision pursuant to Article 45 of Regulation (EU) 2016/679 that covers the onward transfer;

(ii) the third party otherwise ensures appropriate safeguards pursuant to Articles 46 or 47 of Regulation (EU) 2016/679;

(iii) the onward transfer is necessary for the establishment, exercise or defence of legal claims in the context of specific administrative, regulatory or judicial proceedings; or

(iv) the onward transfer is necessary in order to protect the vital interests of the data subject or of another natural person.

Any onward transfer is subject to compliance by the data importer with all the other safeguards under these Clauses, in particular purpose limitation.

8.9 Documentation and compliance

(a) The data importer shall promptly and adequately deal with enquiries from the data exporter or the controller that relate to the processing under these Clauses.

(b) The Parties shall be able to demonstrate compliance with these Clauses. In particular, the data importer shall keep appropriate documentation on the processing activities carried out on behalf of the controller.

(c) The data importer shall make all information necessary to demonstrate compliance with the obligations set out in these Clauses available to the data exporter, which shall provide it to the controller.

(d) The data importer shall allow for and contribute to audits by the data exporter of the processing activities covered by these Clauses, at reasonable intervals or if there are indications of non-compliance. The same shall apply where the data exporter requests an audit on instructions of the controller. In deciding on an audit, the data exporter may take into account relevant certifications held by the data importer.

(e) Where the audit is carried out on the instructions of the controller, the data exporter shall make the results available to the controller.

(f) The data exporter may choose to conduct the audit by itself or mandate an independent auditor. Audits may include inspections at the premises or physical facilities of the data importer and shall, where appropriate, be carried out with reasonable notice.

(g) The Parties shall make the information referred to in paragraphs (b) and (c), including the results of any audits, available to the competent supervisory authority on request.

MODULE FOUR: Transfer processor to controller

8.1 Instructions

(a) The data exporter shall process the personal data only on documented instructions from the data importer acting as its controller.

(b) The data exporter shall immediately inform the data importer if it is unable to follow those instructions,

including if such instructions infringe Regulation (EU) 2016/679 or other Union or Member State data protection law.

(c) The data importer shall refrain from any action that would prevent the data exporter from fulfilling its obligations under Regulation (EU) 2016/679, including in the context of sub-processing or as regards cooperation with competent supervisory authorities.

(d) After the end of the provision of the processing services, the data exporter shall, at the choice of the data importer, delete all personal data processed on behalf of the data importer and certify to the data importer that it has done so, or return to the data importer all personal data processed on its behalf and delete existing copies.

8.2 Security of processing

(a) The Parties shall implement appropriate technical and organisational measures to ensure the security of the data, including during transmission, and protection against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access (hereinafter 'personal data breach'). In assessing the appropriate level of security, they shall take due account of the state of the art, the costs of implementation, the nature of the personal data (7), the nature, scope, context and purpose(s) of processing and the risks involved in the processing for the data subjects, and in particular consider having recourse to encryption or pseudonymisation, including during transmission, where the purpose of processing can be fulfilled in that manner.

(b) The data exporter shall assist the data importer in ensuring appropriate security of the data in accordance with paragraph (a). In case of a personal data breach concerning the personal data processed by the data exporter under these Clauses, the data exporter shall notify the data importer without undue delay after becoming aware of it and assist the data importer in addressing the breach.

(c) The data exporter shall ensure that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

8.3 Documentation and compliance

(a) The Parties shall be able to demonstrate compliance with these Clauses.

(b) The data exporter shall make available to the data importer all information necessary to demonstrate compliance with its obligations under these Clauses and allow for and contribute to audits.

Clause 9 Use of sub-processors

MODULE TWO: Transfer controller to processor

(a) The data importer has the data exporter's general authorisation for the engagement of sub-processor(s) from an agreed list. The data importer shall specifically inform the data exporter in writing of any intended changes to that list through the addition or replacement of sub-processors at least [Specify time period] in advance, thereby giving the data exporter sufficient time to be able to object to such changes prior to the engagement of the sub-processor(s). The data importer shall provide the data exporter with the information necessary to enable the data exporter to exercise its right to object.

(b) Where the data importer engages a sub-processor to carry out specific processing activities (on behalf of the data exporter), it shall do so by way of a written contract that provides for, in substance, the same data protection obligations as those binding the data importer under these Clauses, including in terms of third-party beneficiary rights for data subjects. (8) The Parties agree that, by complying with this Clause, the data importer fulfils its obligations under Clause 8.8. The data importer shall ensure that the sub-processor complies with the

obligations to which the data importer is subject pursuant to these Clauses.

(c) The data importer shall provide, at the data exporter's request, a copy of such a sub-processor agreement and any subsequent amendments to the data exporter. To the extent necessary to protect business secrets or other confidential information, including personal data, the data importer may redact the text of the agreement prior to sharing a copy.

(d) The data importer shall remain fully responsible to the data exporter for the performance of the sub-processor's obligations under its contract with the data importer. The data importer shall notify the data exporter of any failure by the sub-processor to fulfil its obligations under that contract.

(e) The data importer shall agree a third-party beneficiary clause with the sub-processor whereby – in the event the data importer has factually disappeared, ceased to exist in law or has become insolvent – the data exporter shall have the right to terminate the sub-processor contract and to instruct the sub-processor to erase or return the personal data.

MODULE THREE: Transfer processor to processor

(a) The data importer has the controller's general authorisation for the engagement of sub-processor(s) from an agreed list. The data importer shall specifically inform the controller in writing of any intended changes to that list through the addition or replacement of sub-processors at least [Specify time period] in advance, thereby giving the controller sufficient time to be able to object to such changes prior to the engagement of the sub-processor(s). The data importer shall provide the controller with the information necessary to enable the controller to exercise its right to object. The data importer shall inform the data exporter of the engagement of the sub-processor(s).

(b) Where the data importer engages a sub-processor to carry out specific processing activities (on behalf of the controller), it shall do so by way of a written contract that provides for, in substance, the same data protection obligations as those binding the data importer under these Clauses, including in terms of third-party beneficiary rights for data subjects. (9) The Parties agree that, by complying with this Clause, the data importer fulfils its obligations under Clause 8.8. The data importer shall ensure that the sub-processor complies with the obligations to which the data importer is subject pursuant to these Clauses.

(c) The data importer shall provide, at the data exporter's or controller's request, a copy of such a sub-processor agreement and any subsequent amendments. To the extent necessary to protect business secrets or other confidential information, including personal data, the data importer may redact the text of the agreement prior to sharing a copy.

(d) The data importer shall remain fully responsible to the data exporter for the performance of the sub-processor's obligations under its contract with the data importer. The data importer shall notify the data exporter of any failure by the sub-processor to fulfil its obligations under that contract.

(e) The data importer shall agree a third-party beneficiary clause with the sub-processor whereby – in the event the data importer has factually disappeared, ceased to exist in law or has become insolvent – the data exporter shall have the right to terminate the sub-processor contract and to instruct the sub-processor to erase or return the personal data.

Clause 10 Data subject rights

MODULE ONE: Transfer controller to controller

(a) The data importer, where relevant with the assistance of the data exporter, shall deal with any enquiries and requests it receives from a data subject relating to the processing of his/her personal data and the exercise of

his/her rights under these Clauses without undue delay and at the latest within one month of the receipt of the enquiry or request. (10) The data importer shall take appropriate measures to facilitate such enquiries, requests and the exercise of data subject rights. Any information provided to the data subject shall be in an intelligible and easily accessible form, using clear and plain language.

(b) In particular, upon request by the data subject the data importer shall, free of charge:

(i) provide confirmation to the data subject as to whether personal data concerning him/her is being processed and, where this is the case, a copy of the data relating to him/her and the information in Annex I; if personal data has been or will be onward transferred, provide information on recipients or categories of recipients (as appropriate with a view to providing meaningful information) to which the personal data has been or will be onward transferred, the purpose of such onward transfers and their ground pursuant to Clause 8.7; and provide information on the right to lodge a complaint with a supervisory authority in accordance with Clause 12(c)(i);

(ii) rectify inaccurate or incomplete data concerning the data subject;

(iii) erase personal data concerning the data subject if such data is being or has been processed in violation of any of these Clauses ensuring third-party beneficiary rights, or if the data subject withdraws the consent on which the processing is based.

(c) Where the data importer processes the personal data for direct marketing purposes, it shall cease processing for such purposes if the data subject objects to it.

(d) The data importer shall not make a decision based solely on the automated processing of the personal data transferred (hereinafter 'automated decision'), which would produce legal effects concerning the data subject or similarly significantly affect him/her, unless with the explicit consent of the data subject or if authorised to do so under the laws of the country of destination, provided that such laws lays down suitable measures to safeguard the data subject's rights and legitimate interests. In this case, the data importer shall, where necessary in cooperation with the data exporter:

(i) inform the data subject about the envisaged automated decision, the envisaged consequences and the logic involved; and

(ii) implement suitable safeguards, at least by enabling the data subject to contest the decision, express his/her point of view and obtain review by a human being.

(e) Where requests from a data subject are excessive, in particular because of their repetitive character, the data importer may either charge a reasonable fee taking into account the administrative costs of granting the request or refuse to act on the request.

(f) The data importer may refuse a data subject's request if such refusal is allowed under the laws of the country of destination and is necessary and proportionate in a democratic society to protect one of the objectives listed in Article 23(1) of Regulation (EU) 2016/679.

(g) If the data importer intends to refuse a data subject's request, it shall inform the data subject of the reasons for the refusal and the possibility of lodging a complaint with the competent supervisory authority and/or seeking judicial redress.

MODULE TWO: Transfer controller to processor

(a) The data importer shall promptly notify the data exporter of any request it has received from a data subject. It shall not respond to that request itself unless it has been authorised to do so by the data exporter.

(b) The data importer shall assist the data exporter in fulfilling its obligations to respond to data subjects' requests

for the exercise of their rights under Regulation (EU) 2016/679. In this regard, the Parties shall set out in Annex II the appropriate technical and organisational measures, taking into account the nature of the processing, by which the assistance shall be provided, as well as the scope and the extent of the assistance required.

(c) In fulfilling its obligations under paragraphs (a) and (b), the data importer shall comply with the instructions from the data exporter.

MODULE THREE: Transfer processor to processor

(a) The data importer shall promptly notify the data exporter and, where appropriate, the controller of any request it has received from a data subject, without responding to that request unless it has been authorised to do so by the controller.

(b) The data importer shall assist, where appropriate in cooperation with the data exporter, the controller in fulfilling its obligations to respond to data subjects' requests for the exercise of their rights under Regulation (EU) 2016/679 or Regulation (EU) 2018/1725, as applicable. In this regard, the Parties shall set out in Annex II the appropriate technical and organisational measures, taking into account the nature of the processing, by which the assistance shall be provided, as well as the scope and the extent of the assistance required.

(c) In fulfilling its obligations under paragraphs (a) and (b), the data importer shall comply with the instructions from the controller, as communicated by the data exporter.

MODULE FOUR: Transfer processor to controller

The Parties shall assist each other in responding to enquiries and requests made by data subjects under the local law applicable to the data importer or, for data processing by the data exporter in the EU, under Regulation (EU) 2016/679.

Clause 11 Redress

(a) The data importer shall inform data subjects in a transparent and easily accessible format, through individual notice or on its website, of a contact point authorised to handle complaints. It shall deal promptly with any complaints it receives from a data subject.

MODULE ONE: Transfer controller to controller

MODULE TWO: Transfer controller to processor

MODULE THREE: Transfer processor to processor

(b) In case of a dispute between a data subject and one of the Parties as regards compliance with these Clauses, that Party shall use its best efforts to resolve the issue amicably in a timely fashion. The Parties shall keep each other informed about such disputes and, where appropriate, cooperate in resolving them.

(c) Where the data subject invokes a third-party beneficiary right pursuant to Clause 3, the data importer shall accept the decision of the data subject to:

(i) lodge a complaint with the supervisory authority in the Member State of his/her habitual residence or place of work, or the competent supervisory authority pursuant to Clause 13;

(ii) refer the dispute to the competent courts within the meaning of Clause 18.

(d) The Parties accept that the data subject may be represented by a not-for-profit body, organisation or association under the conditions set out in Article 80(1) of Regulation (EU) 2016/679.

(e) The data importer shall abide by a decision that is binding under the applicable EU or Member State law.

(f) The data importer agrees that the choice made by the data subject will not prejudice his/her substantive and procedural rights to seek remedies in accordance with applicable laws.

Clause 12 Liability

MODULE ONE: Transfer controller to controller

MODULE FOUR: Transfer processor to controller

(a) Each Party shall be liable to the other Party/ies for any damages it causes the other Party/ies by any breach of these Clauses.

(b) Each Party shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages that the Party causes the data subject by breaching the third-party beneficiary rights under these Clauses. This is without prejudice to the liability of the data exporter under Regulation (EU) 2016/679.

(c) Where more than one Party is responsible for any damage caused to the data subject as a result of a breach of these Clauses, all responsible Parties shall be jointly and severally liable and the data subject is entitled to bring an action in court against any of these Parties.

(d) The Parties agree that if one Party is held liable under paragraph (c), it shall be entitled to claim back from the other Party/ies that part of the compensation corresponding to its/their responsibility for the damage.

(e) The data importer may not invoke the conduct of a processor or sub-processor to avoid its own liability.

MODULE TWO: Transfer controller to processor

MODULE THREE: Transfer processor to processor

(a) Each Party shall be liable to the other Party/ies for any damages it causes the other Party/ies by any breach of these Clauses.

(b) The data importer shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data importer or its sub-processor causes the data subject by breaching the third-party beneficiary rights under these Clauses.

(c) Notwithstanding paragraph (b), the data exporter shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data exporter or the data importer (or its sub-processor) causes the data subject by breaching the third-party beneficiary rights under these Clauses. This is without prejudice to the liability of the data exporter and, where the data exporter is a processor acting on behalf of a controller, to the liability of the controller under Regulation (EU) 2016/679 or Regulation (EU) 2018/1725, as applicable.

(d) The Parties agree that if the data exporter is held liable under paragraph (c) for damages caused by the data importer (or its sub-processor), it shall be entitled to claim back from the data importer that part of the compensation corresponding to the data importer's responsibility for the damage.

(e) Where more than one Party is responsible for any damage caused to the data subject as a result of a breach of these Clauses, all responsible Parties shall be jointly and severally liable and the data subject is entitled to bring an action in court against any of these Parties.

(f) The Parties agree that if one Party is held liable under paragraph (e), it shall be entitled to claim back from the other Party/ies that part of the compensation corresponding to its/their responsibility for the damage.

(g) The data importer may not invoke the conduct of a sub-processor to avoid its own liability.

Clause 13 Supervision

MODULE ONE: Transfer controller to controller

MODULE TWO: Transfer controller to processor

MODULE THREE: Transfer processor to processor

(a) [Where the data exporter is established in an EU Member State:] The supervisory authority with responsibility for ensuring compliance by the data exporter with Regulation (EU) 2016/679 as regards the data transfer, as indicated in Annex I.C, shall act as competent supervisory authority.

[Where the data exporter is not established in an EU Member State, but falls within the territorial scope of application of Regulation (EU) 2016/679 in accordance with its Article 3(2) and has appointed a representative pursuant to Article 27(1) of Regulation (EU) 2016/679:] The supervisory authority of the Member State in which the representative within the meaning of Article 27(1) of Regulation (EU) 2016/679 is established, as indicated in Annex I.C, shall act as competent supervisory authority.

[Where the data exporter is not established in an EU Member State, but falls within the territorial scope of application of Regulation (EU) 2016/679 in accordance with its Article 3(2) without however having to appoint a representative pursuant to Article 27(2) of Regulation (EU) 2016/679:] The supervisory authority of one of the Member States in which the data subjects whose personal data is transferred under these Clauses in relation to the offering of goods or services to them, or whose behaviour is monitored, are located, as indicated in Annex I.C, shall act as competent supervisory authority.

(b) The data importer agrees to submit itself to the jurisdiction of and cooperate with the competent supervisory authority in any procedures aimed at ensuring compliance with these Clauses. In particular, the data importer agrees to respond to enquiries, submit to audits and comply with the measures adopted by the supervisory authority, including remedial and compensatory measures. It shall provide the supervisory authority with written confirmation that the necessary actions have been taken.

SECTION III – LOCAL LAWS AND OBLIGATIONS IN CASE OF ACCESS BY PUBLIC AUTHORITIES

Clause 14 Local laws and practices affecting compliance with the Clauses

MODULE ONE: Transfer controller to controller

MODULE TWO: Transfer controller to processor

MODULE THREE: Transfer processor to processor

MODULE FOUR: Transfer processor to controller (where the EU processor combines the personal data received from the third country-controller with personal data collected by the processor in the EU)

(a) The Parties warrant that they have no reason to believe that the laws and practices in the third country of destination applicable to the processing of the personal data by the data importer, including any requirements to

disclose personal data or measures authorising access by public authorities, prevent the data importer from fulfilling its obligations under these Clauses. This is based on the understanding that laws and practices that respect the essence of the fundamental rights and freedoms and do not exceed what is necessary and proportionate in a democratic society to safeguard one of the objectives listed in Article 23(1) of Regulation (EU) 2016/679, are not in contradiction with these Clauses.

(b) The Parties declare that in providing the warranty in paragraph (a), they have taken due account in particular of the following elements:

(i) the specific circumstances of the transfer, including the length of the processing chain, the number of actors involved and the transmission channels used; intended onward transfers; the type of recipient; the purpose of processing; the categories and format of the transferred personal data; the economic sector in which the transfer occurs; the storage location of the data transferred;

(ii) the laws and practices of the third country of destination– including those requiring the disclosure of data to public authorities or authorising access by such authorities – relevant in light of the specific circumstances of the transfer, and the applicable limitations and safeguards (12);

(iii) any relevant contractual, technical or organisational safeguards put in place to supplement the safeguards under these Clauses, including measures applied during transmission and to the processing of the personal data in the country of destination.

(c) The data importer warrants that, in carrying out the assessment under paragraph (b), it has made its best efforts to provide the data exporter with relevant information and agrees that it will continue to cooperate with the data exporter in ensuring compliance with these Clauses.

(d) The Parties agree to document the assessment under paragraph (b) and make it available to the competent supervisory authority on request.

(e) The data importer agrees to notify the data exporter promptly if, after having agreed to these Clauses and for the duration of the contract, it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under paragraph (a), including following a change in the laws of the third country or a measure (such as a disclosure request) indicating an application of such laws in practice that is not in line with the requirements in paragraph (a). [For Module Three: The data exporter shall forward the notification to the controller.]

(f) Following a notification pursuant to paragraph (e), or if the data exporter otherwise has reason to believe that the data importer can no longer fulfil its obligations under these Clauses, the data exporter shall promptly identify appropriate measures (e.g. technical or organisational measures to ensure security and confidentiality) to be adopted by the data exporter and/or data importer to address the situation [for Module Three:, if appropriate in consultation with the controller]. The data exporter shall suspend the data transfer if it considers that no appropriate safeguards for such transfer can be ensured, or if instructed by [for Module Three: the controller or] the competent supervisory authority to do so. In this case, the data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses. If the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise. Where the contract is terminated pursuant to this Clause, Clause 16(d) and (e) shall apply.

Clause 15 Obligations of the data importer in case of access by public

authorities

MODULE ONE: Transfer controller to controller

MODULE TWO: Transfer controller to processor

MODULE THREE: Transfer processor to processor

MODULE FOUR: Transfer processor to controller (where the EU processor combines the personal data received from the third country-controller with personal data collected by the processor in the EU)

15.1 Notification

(a) The data importer agrees to notify the data exporter and, where possible, the data subject promptly (if necessary with the help of the data exporter) if it:

(i) receives a legally binding request from a public authority, including judicial authorities, under the laws of the country of destination for the disclosure of personal data transferred pursuant to these Clauses; such notification shall include information about the personal data requested, the requesting authority, the legal basis for the request and the response provided; or

(ii) becomes aware of any direct access by public authorities to personal data transferred pursuant to these Clauses in accordance with the laws of the country of destination; such notification shall include all information available to the importer.

[For Module Three: The data exporter shall forward the notification to the controller.]

(b) If the data importer is prohibited from notifying the data exporter and/or the data subject under the laws of the country of destination, the data importer agrees to use its best efforts to obtain a waiver of the prohibition, with a view to communicating as much information as possible, as soon as possible. The data importer agrees to document its best efforts in order to be able to demonstrate them on request of the data exporter.

(c) Where permissible under the laws of the country of destination, the data importer agrees to provide the data exporter, at regular intervals for the duration of the contract, with as much relevant information as possible on the requests received (in particular, number of requests, type of data requested, requesting authority/ies, whether requests have been challenged and the outcome of such challenges, etc.). [For Module Three: The data exporter shall forward the information to the controller.]

(d) The data importer agrees to preserve the information pursuant to paragraphs (a) to (c) for the duration of the contract and make it available to the competent supervisory authority on request.

(e) Paragraphs (a) to (c) are without prejudice to the obligation of the data importer pursuant to Clause 14(e) and Clause 16 to inform the data exporter promptly where it is unable to comply with these Clauses.

15.2 Review of legality and data minimisation

(a) The data importer agrees to review the legality of the request for disclosure, in particular whether it remains within the powers granted to the requesting public authority, and to challenge the request if, after careful assessment, it concludes that there are reasonable grounds to consider that the request is unlawful under the laws of the country of destination, applicable obligations under international law and principles of international comity. The data importer shall, under the same conditions, pursue possibilities of appeal. When challenging a request, the data importer shall seek interim measures with a view to suspending the effects of the request until the competent judicial authority has decided on its merits. It shall not disclose the personal data requested until

required to do so under the applicable procedural rules. These requirements are without prejudice to the obligations of the data importer under Clause 14(e).

(b) The data importer agrees to document its legal assessment and any challenge to the request for disclosure and, to the extent permissible under the laws of the country of destination, make the documentation available to the data exporter. It shall also make it available to the competent supervisory authority on request. [For Module Three: The data exporter shall make the assessment available to the controller.]

(c) The data importer agrees to provide the minimum amount of information permissible when responding to a request for disclosure, based on a reasonable interpretation of the request.

SECTION IV – FINAL PROVISIONS

Clause 16 Non-compliance with the Clauses and termination

(a) The data importer shall promptly inform the data exporter if it is unable to comply with these Clauses, for whatever reason.

(b) In the event that the data importer is in breach of these Clauses or unable to comply with these Clauses, the data exporter shall suspend the transfer of personal data to the data importer until compliance is again ensured or the contract is terminated. This is without prejudice to Clause 14(f).

(c) The data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses, where:

(i) the data exporter has suspended the transfer of personal data to the data importer pursuant to paragraph (b) and compliance with these Clauses is not restored within a reasonable time and in any event within one month of suspension;

(ii) the data importer is in substantial or persistent breach of these Clauses; or

(iii) the data importer fails to comply with a binding decision of a competent court or supervisory authority regarding its obligations under these Clauses.

In these cases, it shall inform the competent supervisory authority [for Module Three: and the controller] of such non-compliance. Where the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise.

(d) [For Modules One, Two and Three: Personal data that has been transferred prior to the termination of the contract pursuant to paragraph (c) shall at the choice of the data exporter immediately be returned to the data exporter or deleted in its entirety. The same shall apply to any copies of the data.] [For Module Four: Personal data collected by the data exporter in the EU that has been transferred prior to the termination of the contract pursuant to paragraph (c) shall immediately be deleted in its entirety, including any copy thereof.] The data importer shall certify the deletion of the data to the data exporter. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit the return or deletion of the transferred personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process the data to the extent and for as long as required under that local law.

(e) Either Party may revoke its agreement to be bound by these Clauses where (i) the European Commission adopts a decision pursuant to Article 45(3) of Regulation (EU) 2016/679 that covers the transfer of personal data to which these Clauses apply; or (ii) Regulation (EU) 2016/679 becomes part of the legal framework of the country

to which the personal data is transferred. This is without prejudice to other obligations applying to the processing in question under Regulation (EU) 2016/679.

Clause 17 Governing law

MODULE ONE: Transfer controller to controller

MODULE TWO: Transfer controller to processor

MODULE THREE: Transfer processor to processor

These Clauses shall be governed by the law of one of the EU Member States, provided such law allows for third-party beneficiary rights. The Parties agree that this shall be the law as defined in Terms.

MODULE FOUR: Transfer processor to controller

These Clauses shall be governed by the law of a country allowing for third-party beneficiary rights. The Parties agree that this shall be the law as defined in Terms.

Clause 18 Choice of forum and jurisdiction

MODULE ONE: Transfer controller to controller

MODULE TWO: Transfer controller to processor

MODULE THREE: Transfer processor to processor

(a) Any dispute arising from these Clauses shall be resolved by the courts of an EU Member State.

(b) The Parties agree that those shall be the courts as defined in Terms.

(c) A data subject may also bring legal proceedings against the data exporter and/or data importer before the courts of the Member State in which he/she has his/her habitual residence.

(d) The Parties agree to submit themselves to the jurisdiction of such courts.

MODULE FOUR: Transfer processor to controller

Any dispute arising from these Clauses shall be resolved by the courts as defined in Terms.

APPENDIX

EXPLANATORY NOTE: It must be possible to clearly distinguish the information applicable to each transfer or category of transfers and, in this regard, to determine the respective role(s) of the Parties as data exporter(s) and/or data importer(s). This does not necessarily require completing and signing separate appendices for each transfer/category of transfers and/or contractual relationship, where this transparency can achieved through one appendix. However, where necessary to ensure sufficient clarity, separate appendices should be used.

ANNEX I

A. LIST OF PARTIES

MODULE ONE: Transfer controller to controller

MODULE TWO: Transfer controller to processor

MODULE THREE: Transfer processor to processor

MODULE FOUR: Transfer processor to controller

Data exporter(s): [Identity and contact details of the data exporter(s) and, where applicable, of its/their data protection officer and/or representative in the European Union]

1. Controller as defined in Data Processing Agreement

2. Processor as defined in Data Processing Agreement

(based on the flow of data)

Data importer(s): [Identity and contact details of the data importer(s), including any contact person with responsibility for data protection]

1. Controller as defined in Data Processing Agreement

2. Processor as defined in Data Processing Agreement

(based on the flow of data)

B. DESCRIPTION OF TRANSFER

MODULE ONE: Transfer controller to controller

MODULE TWO: Transfer controller to processor

MODULE THREE: Transfer processor to processor

MODULE FOUR: Transfer processor to controller

Categories of data subjects whose personal data is transferred: As defined in Data Processing Agreement.

Categories of personal data transferred: As defined in Data Processing Agreement and Privacy Policy.

Sensitive data transferred (if applicable) and applied restrictions or safeguards that fully take into consideration the nature of the data and the risks involved, such as for instance strict purpose limitation, access restrictions (including access only for staff having followed specialised training), keeping a record of access to the data, restrictions for onward transfers or additional security measures: As defined in Data Processing Agreement and Privacy Policy.

The frequency of the transfer (e.g. whether the data is transferred on a one-off or continuous basis): Continuous basis.

Nature of the processing: Automated.

Purpose(s) of the data transfer and further processing: Provision of service as defined in Terms, its Annexes, Privacy Policy, and service documentation.

The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine

that period: As defined in Data Processing Agreement.

For transfers to (sub-) processors, also specify subject matter, nature and duration of the processing: As defined in Data Processing Agreement.

C. COMPETENT SUPERVISORY AUTHORITY

MODULE ONE: Transfer controller to controller

MODULE TWO: Transfer controller to processor

MODULE THREE: Transfer processor to processor

Identify the competent supervisory authority/ies in accordance with Clause 13: As defined in Privacy Policy

ANNEX II TECHNICAL AND ORGANISATIONAL MEASURES INCLUDING TECHNICAL AND ORGANISATIONAL MEASURES TO ENSURE THE SECURITY OF THE DATA

MODULE ONE: Transfer controller to controller

MODULE TWO: Transfer controller to processor

MODULE THREE: Transfer processor to processor

EXPLANATORY NOTE: The technical and organisational measures must be described in specific (and not generic) terms. See also the general comment on the first page of the Appendix, in particular on the need to clearly indicate which measures apply to each transfer/set of transfers.

Description of the technical and organisational measures implemented by the data importer(s) (including any relevant certifications) to ensure an appropriate level of security, taking into account the nature, scope, context and purpose of the processing, and the risks for the rights and freedoms of natural persons: As defined in Security Policy

For transfers to (sub-) processors, also describe the specific technical and organisational measures to be taken by the (sub-) processor to be able to provide assistance to the controller and, for transfers from a processor to a sub-processor, to the data exporter

ANNEX III LIST OF SUB-PROCESSORS

MODULE TWO: Transfer controller to processor

MODULE THREE: Transfer processor to processor

EXPLANATORY NOTE: This Annex must be completed for Modules Two and Three, in case of the specific authorisation of sub-processors (Clause 9(a), Option 1).

The controller has authorised the use of the following sub-processors: As defined in Data Processing Agreement

References:

(1) Where the data exporter is a processor subject to Regulation (EU) 2016/679 acting on behalf of a Union institution or body as controller, reliance on these Clauses when engaging another processor (sub-processing) not subject to Regulation (EU) 2016/679 also ensures compliance with Article 29(4) of Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC (OJ L 295, 21.11.2018, p. 39), to the extent these Clauses and the data protection obligations as set out in the contract or other legal act between the controller and the processor pursuant to Article 29(3) of Regulation (EU) 2018/1725 are aligned. This will in particular be the case where the controller and processor rely on the standard contractual clauses included in Decision 2021/915.

(2) This requires rendering the data anonymous in such a way that the individual is no longer identifiable by anyone, in line with recital 26 of Regulation (EU) 2016/679, and that this process is irreversible.

(3) The Agreement on the European Economic Area (EEA Agreement) provides for the extension of the European Union's internal market to the three EEA States Iceland, Liechtenstein and Norway. The Union data protection legislation, including Regulation (EU) 2016/679, is covered by the EEA Agreement and has been incorporated into Annex XI thereto. Therefore, any disclosure by the data importer to a third party located in the EEA does not qualify as an onward transfer for the purpose of these Clauses.

(4) The Agreement on the European Economic Area (EEA Agreement) provides for the extension of the European Union's internal market to the three EEA States Iceland, Liechtenstein and Norway. The Union data protection legislation, including Regulation (EU) 2016/679, is covered by the EEA Agreement and has been incorporated into Annex XI thereto. Therefore, any disclosure by the data importer to a third party located in the EEA does not qualify as an onward transfer for the purpose of these Clauses.

(5) See Article 28(4) of Regulation (EU) 2016/679 and, where the controller is an EU institution or body, Article 29(4) of Regulation (EU) 2018/1725.

(6) The Agreement on the European Economic Area (EEA Agreement) provides for the extension of the European Union's internal market to the three EEA States Iceland, Liechtenstein and Norway. The Union data protection legislation, including Regulation (EU) 2016/679, is covered by the EEA Agreement and has been incorporated into Annex XI thereto. Therefore, any disclosure by the data importer to a third party located in the EEA does not qualify as an onward transfer for the purposes of these Clauses.

(7) This includes whether the transfer and further processing involves personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data or biometric data for the purpose of uniquely identifying a natural person, data concerning health or a person's sex life or sexual orientation, or data relating to criminal convictions or offences.

(8) This requirement may be satisfied by the sub-processor acceding to these Clauses under the appropriate Module, in accordance with Clause 7.

(9) This requirement may be satisfied by the sub-processor acceding to these Clauses under the appropriate Module, in accordance with Clause 7.

(10) That period may be extended by a maximum of two more months, to the extent necessary taking into account the complexity and number of requests. The data importer shall duly and promptly inform the data subject of any such extension.

(11) The data importer may offer independent dispute resolution through an arbitration body only if it is

established in a country that has ratified the New York Convention on Enforcement of Arbitration Awards.

(12) As regards the impact of such laws and practices on compliance with these Clauses, different elements may be considered as part of an overall assessment. Such elements may include relevant and documented practical experience with prior instances of requests for disclosure from public authorities, or the absence of such requests, covering a sufficiently representative time-frame. This refers in particular to internal records or other documentation, drawn up on a continuous basis in accordance with due diligence and certified at senior management level, provided that this information can be lawfully shared with third parties. Where this practical experience is relied upon to conclude that the data importer will not be prevented from complying with these Clauses, it needs to be supported by other relevant, objective elements, and it is for the Parties to consider carefully whether these elements together carry sufficient weight, in terms of their reliability and representativeness, to support this conclusion. In particular, the Parties have to take into account whether their practical experience is corroborated and not contradicted by publicly available or otherwise accessible, reliable information on the existence or absence of requests within the same sector and/or the application of the law in practice, such as case law and reports by independent oversight bodies.

Política de Privacidade

Em vigor a partir de 19 de julho de 2023 | Ver uma versão anterior da Política de Privacidade | Comparar alterações

A proteção de dados pessoais é de importância particular para a ESET, spol. s r. o., com sede em Einsteinova 24, 851 01 Bratislava, Slovak Republic, registrada no Registro Comercial administrado pela Corte Distrital Bratislava I, Seção Sro, Registro Nº. 3586/B, Número de Registro Comercial: 31333532 como um Responsável pelo Tratamento de Dados ("ESET" ou "Nós"). Queremos cumprir com o requisito de transparência conforme legalmente protegido pelo Regulamento Geral de Proteção de Dados ("RGPD") da UE. Para isso, estamos publicando essa Política de Privacidade com o objetivo exclusivo de informar nosso cliente ("Usuário Final" ou "Você") como titular dos dados sobre os tópicos de dados pessoais a seguir:

- Base jurídica do tratamento de dados pessoais,
- Compartilhamento de dados e confidencialidade,
- Segurança de dados,
- Seus direitos como titular dos dados,
- Tratamento de seus Dados pessoais
- Informações de contato.

Base jurídica do tratamento de dados pessoais

Existem apenas algumas bases jurídicas para o tratamento de dados que Nós usamos de acordo com a estrutura legislativa aplicável relacionada à proteção de dados pessoais. O tratamento de dados pessoais na ESET é principalmente necessário para o desempenho do Termos de uso ("Termos") com o Usuário Final (Art. 6 (1) (b) LGPD), que é aplicável para o fornecimento de produtos ou serviços ESET, a menos que explicitamente declarado o contrário, por exemplo:

- Base jurídica de interesse legítimo (Art. 6 (1) (f) LGPD), que nos permite processar dados sobre como nossos clientes usam nossos Serviços e sua satisfação para fornecer aos nossos usuários a melhor proteção, suporte e experiência que podemos oferecer. Mesmo o marketing é reconhecido pela legislação aplicável como um interesse legítimo, portanto normalmente contamos com isso para a comunicação de marketing com nossos clientes.
- Consentimento (Art. 6 (1) (a) LGPD), que podemos solicitar de Você em situações específicas quando consideramos essa base jurídica como a mais adequada ou se for exigido por lei.

- Conformidade com obrigações legais (Art. 6 (1) (c) LGPD), por exemplo estipulando requisitos para comunicação eletrônica, retenção para faturamento ou documentos de cobrança.

Compartilhamento de dados e confidencialidade

Não compartilhamos seus dados com terceiros. Porém, a ESET é uma empresa que opera no mundo todo através de empresas afiliadas ou parceiros como parte de nossa rede de vendas, serviço e suporte. Informações de licenciamento, cobrança e suporte técnico processadas pela ESET podem ser transferidas de e para afiliadas ou parceiros com o objetivo de cumprir com o Acordo de Licença para o Usuário Final, como o fornecimento de serviços ou suporte.

A ESET prefere processar seus dados na União Europeia (UE). Porém, dependendo de sua localização (uso de nossos produtos e/ou serviços fora da UE) e/ou do serviço escolhido por você, pode ser necessário transferir seus dados para um país fora da UE. Por exemplo, usamos serviços de terceiros em conexão com a computação em nuvem. Nesses casos, selecionamos cuidadosamente nossos provedores de serviço e garantimos um nível apropriado de proteção de dados através de medidas contratuais, técnicas e organizacionais. Como regra, concordamos com as cláusulas contratuais padrão da UE, se necessário, com regulamentos contratuais suplementares.

Para alguns países fora da UE, como o Reino Unido e Suíça, a UE já determinou um nível de proteção de dados comparável. Devido ao nível comparável de proteção de dados, a transferência de dados para esses países não requer qualquer autorização ou acordo especial.

Contamos com serviços de terceiros relacionados à computação em nuvem fornecida pela Microsoft como um provedor de serviços de nuvem.

Segurança de dados

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 relevante, assim como os Usuários Finais afetados como titulares dos dados.

Direitos do sujeito dos dados

Os direitos de todos os Usuários Finais são importantes e gostaríamos de informar que todos os Usuários Finais (de qualquer país da UE ou que não da UE) têm os seguintes direitos garantidos na ESET. Para exercer seus direitos de titular dos dados, você pode entrar em contato conosco através do formulário de suporte ou por e-mail em dpo@eset.sk. Para fins de identificação, pedimos as informações a seguir: Nome, endereço de e-mail e, se disponível, chave de licença ou número do cliente e filiação da empresa. Não envie nenhum outro dado pessoal, como a data de nascimento. Destacamos que, para ser capaz de processar sua solicitação, assim como para fins de identificação, vamos processar seus dados pessoais.

Direito de retirar o consentimento. O direito de retirar o consentimento é aplicável no caso de tratamento baseado apenas no consentimento. Se processarmos seus dados pessoais com base em seu consentimento, você tem o direito de retirar o consentimento a qualquer momento sem dar motivos. A retirada do seu consentimento só é eficaz para o futuro e não afeta a legalidade dos dados processados antes da retirada.

Direito a uma objeção. O direito de objeção ao tratamento é aplicável no caso de tratamento com base no interesse legítimo da ESET ou de terceiros. Se tratarmos seus dados pessoais para proteger um interesse legítimo,

Você como o titular dos dados tem o direito de objeção aos interesses legítimos nomeados por Nós e ao tratamento de seus dados pessoais a qualquer momento. Sua objeção só é eficaz para o futuro e não afeta a legalidade dos dados processados antes da objeção. Se processarmos seus dados pessoais para fins de marketing direto, não é necessário dar motivos para sua objeção. Isso também se aplica a criação de perfis, na medida em que está conectado a tal marketing direto. Em todos os outros casos, solicitamos que você nos informe brevemente sobre suas queixas contra o interesse legítimo da ESET para tratar seus dados pessoais.

Observe que, em alguns casos, apesar de sua retirada de consentimento, temos o direito de continuar com o tratamento de seus dados pessoais com base em outra base jurídica, por exemplo, para a execução de um contrato.

Direito de acesso. Como um titular dos dados, você tem o direito de obter informações sobre seus dados armazenados pela ESET gratuitamente a qualquer momento.

Direito a retificação. Se inadvertidamente tratarmos dados pessoais incorretos sobre você, você tem o direito de corrigir isso.

Direito a exclusão e direito a restrição do tratamento. Como um titular dos dados, você tem o direito de solicitar a exclusão ou restrição do tratamento de seus dados pessoais. Se tratarmos seus dados pessoais, por exemplo, com seu consentimento, você retirará esse consentimento e se não houver outra base jurídica, por exemplo, um contrato, removeremos seus dados pessoais imediatamente. Seus dados pessoais também serão removidos assim que não forem mais necessários para os fins declarados para eles no final do nosso período de retenção.

Se usarmos seus dados pessoais com o objetivo exclusivo de marketing direto e você tiver revogado seu consentimento ou feito uma objeção ao interesse legítimo subjacente da ESET, restringiremos o tratamento de seus dados pessoais na medida em que incluirmos seus dados de contato em nossa lista de proibições interna para evitar contato não solicitado. Caso contrário, seus dados pessoais serão removidos.

Note que Nós podemos ser obrigados a armazenar seus dados até a expiração das obrigações de retenção e períodos emitidos pelas autoridades legisladoras ou supervisoras. Obrigações e períodos de retenção também podem ser resultado da legislação eslovaca. Depois disso, os dados correspondentes serão removidos rotineiramente.

Direito à portabilidade de dados. Será um prazer fornecer a Você, como um titular dos dados, os dados pessoais processados pela ESET no formato xls.

Direito de fazer uma queixa. Como um titular dos dados, Você tem o direito de enviar uma queixa à autoridade supervisora a qualquer momento. A ESET é sujeita ao regulamento das leis eslovacas e estamos vinculados pela legislação de proteção de dados como parte da União Europeia. A autoridade supervisora de dados relevante é o Gabinete de Proteção de Dados Pessoais da República Eslovaca, localizado em Hraničná 12, 82007 Bratislava 27, Slovak Republic.

Tratamento de seus Dados pessoais

Serviços fornecidos pela ESET implementados em nosso produto baseado na web são oferecidos sob os Termos de Uso (“ToU”), mas alguns deles podem precisar de uma atenção específica. Gostaríamos de fornecer a Você mais detalhes sobre o processamento de dados em relação ao fornecimento de nossos produtos e prestação de nossos serviços. Prestamos vários serviços descritos no Termos Especiais e no produto documentação. Para que tudo funcione, precisamos coletar as informações a seguir:

- O gerenciamento dos produtos de segurança ESET requer informações como ID da unidade de licença e nome, nome do produto, informações da licença, informações de ativação e expiração, informações de

hardware e software a respeito dos dispositivos gerenciados com o produto de segurança ESET 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.

- Outras informações processadas podem incluir informações sobre o processo de instalação, inclusive a plataforma na qual nosso produto está instalado, e informações sobre as operações e funcionalidade de nossos produtos ou dispositivos gerenciados, como impressão digital de hardware, IDs de instalação, IDs de licença, endereço IP, endereço MAC, endereços de e-mail usados, coordenadas GPS de um dispositivo móvel ou definições de configuração do produto.
- Para a segurança da infraestrutura e para fins de relatório, informações de telemetria precisam ser processadas inclusive o número de usuários, políticas, logins, tarefas, notificações, dispositivos gerenciados, ameaças, etc. assim como cabeçalhos HTTP.
- 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.
- Para a Avaliação de Vulnerabilidade e para recursos do Gerenciamento de Patch, mais informações serão processadas. As informações relacionadas ao nome e identificador da vulnerabilidade, gravidade e pontuação de impacto de dispositivos gerenciados serão coletadas e processadas para a Avaliação de Vulnerabilidade. O recurso de Gerenciamento de Patch também precisa do nome, versão e fornecedor do aplicativo, a versão do patch faltando no dispositivo e o identificador do patch faltando.
- 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.
- O feedback do cliente pode ser fornecido por Você através de um formulário da web e para fins de acompanhamento seu email pode ser solicitado, assim como informações de licença e o número de dispositivos gerenciados.

Observe que, se a pessoa usando nossos produtos e serviços não for o Usuário Final que comprou o produto ou serviço e concordou nos Termos conosco (por exemplo, um funcionário do Usuário Final, um membro da família ou uma pessoa autorizada a usar o produto ou serviço pelo Usuário Final de acordo com o Acordo de Licença para o Usuário Final), o tratamento dos dados é realizado no interesse legítimo da ESET, dentro do significado do Art. 6 (1) (f) LGPD para permitir ao usuário autorizado pelo Usuário Final usar os produtos e serviços fornecidos por Nós de acordo com o Acordo de Licença para o Usuário Final.

Informações de contato

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