

ESET Endpoint Security

Guia do Usuário

[Clique aqui para exibir a versão da Ajuda deste documento](#)

Direitos autorais ©2024 por ESET, spol. s r.o.

ESET Endpoint Security foi desenvolvido por ESET, spol. s r.o.

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

Todos os direitos reservados. Nenhuma parte desta documentação pode ser reproduzida, armazenada em um sistema de recuperação ou transmitida de qualquer forma ou por qualquer meio, eletrônico, mecânico, fotocópia, gravação, digitalização, ou de outra forma sem a permissão por escrito do autor.

A ESET, spol. s r.o. reserva-se o direito de alterar qualquer software aplicativo descrito sem prévio aviso.

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

REV. 12-04-2024

1 ESET Endpoint Security 9	1
1.1 Novidades nessa versão?	2
1.2 Requisitos do sistema	3
1.2 Idiomas compatíveis	4
1.3 Prevenção	5
1.4 Páginas de ajuda	6
2 Documentação para endpoints gerenciados remotamente	8
2.1 Introdução ao ESET PROTECT	8
2.2 Introdução ao ESET PROTECT Cloud	10
2.3 Configurações protegidas por senha	10
2.4 O que são políticas	11
2.4 Mesclagem de Políticas	12
2.5 Como os sinalizadores funcionam	12
3 Usando o ESET Endpoint Security por ele mesmo	13
3.1 Método de instalação	13
3.1 Instalação com o ESET AV Remover	14
3.1 ESET AV Remover	14
3.1 Desinstalação usando o ESET AV Remover terminou com erro	17
3.1 Instalação (.exe)	17
3.1 Mudar pasta de instalação (.exe)	19
3.1 Instalação (.msi)	19
3.1 Instalação avançada (.msi)	21
3.1 Instalação de módulos mínimos	23
3.1 Instalação da linha de comando	23
3.1 Instalação usando GPO ou SCCM	28
3.1 Atualização para uma versão mais recente	30
3.1 Atualizações de segurança e estabilidade	31
3.1 Problemas comuns de instalação	31
3.1 Falha na ativação	31
3.2 Ativação do produto	32
3.3 Escanear o computador	32
3.4 Guia do iniciante	32
3.4 A interface do usuário	32
3.4 Configuração da atualização	36
3.4 Configuração de zonas	37
3.4 Ferramentas de controle de web	38
4 Trabalhar com o ESET Endpoint Security	38
4.1 Computador	40
4.1 Mecanismo de detecção	42
4.1 Opções avançadas do mecanismo de detecção	46
4.1 Uma infiltração foi detectada	47
4.1 Proteção em tempo real do sistema de arquivos	49
4.1 Verificação da proteção em tempo real	51
4.1 Quando modificar a configuração da proteção em tempo real	51
4.1 O que fazer se a proteção em tempo real não funcionar	51
4.1 Escanear o computador	52
4.1 Iniciador de rastreamento personalizado	54
4.1 Progresso do rastreamento	55
4.1 Relatório de rastreamento do computador	57
4.1 Escaneamento de malware	57

4.1 Escaneamento em estado ocioso	58
4.1 Perfis de rastreamento	58
4.1 Alvos de rastreamento	59
4.1 Opções de rastreamento avançadas	60
4.1 Controle de dispositivo	60
4.1 Editor de regras do controle de dispositivos	61
4.1 Dispositivos detectados	62
4.1 Grupos do dispositivo	62
4.1 Adição de regras do controle de dispositivos	63
4.1 Sistema de prevenção de intrusos de host (HIPS)	66
4.1 Janela interativa HIPS	68
4.1 Comportamento de ransomware em potencial detectado	69
4.1 Gerenciamento de regras de HIPS	69
4.1 Configurações de regra HIPS	70
4.1 Configuração avançada HIPS	73
4.1 Drivers sempre com permissão para carregar	73
4.1 Modo de apresentação	73
4.1 Rastreamento na inicialização	74
4.1 Rastreamento de arquivos em execução durante inicialização do sistema	75
4.1 Proteção de documentos	75
4.1 Exclusões	76
4.1 Exclusões de desempenho	76
4.1 Adicionar ou editar exclusões de desempenho	77
4.1 Formato da exclusão do caminho	79
4.1 Exclusões de detecção	80
4.1 Adicionar ou Editar exclusão de detecção	83
4.1 Criar assistente de detecção de exclusão	84
4.1 Exclusões (7.1 e versões anteriores)	84
4.1 Exclusões de processos	85
4.1 Adicionar ou editar exclusões de processos	86
4.1 Exclusões HIPS	86
4.1 Parâmetros ThreatSense	86
4.1 Níveis de limpeza	89
4.1 Extensões de arquivo excluídas do rastreamento	90
4.1 Parâmetros adicionais do ThreatSense	91
4.2 Rede	91
4.2 Firewall	92
4.2 Modo de aprendizagem	94
4.2 Proteção de ataque a rede	96
4.2 Proteção contra ataque de força bruta	96
4.2 Regras	96
4.2 Exclusões	99
4.2 Opções de filtragem avançadas	99
4.2 Regras IDS	102
4.2 Ameaça suspeita bloqueada	103
4.2 Solução de problemas de proteção de rede	103
4.2 Redes conectadas	104
4.2 Redes conhecidas	105
4.2 Editor de redes conhecidas	105
4.2 Autenticação de rede - Configuração de servidor	108
4.2 Perfis do firewall	109

4.2 Perfis atribuídos a adaptadores de rede	109
4.2 Detecção de modificação de aplicativo	110
4.2 Aplicativos excluídos da detecção de modificação	110
4.2 Configuração e uso de regras	110
4.2 Lista de regras de firewall	111
4.2 Adicionar ou editar Regras de firewall	112
4.2 Regra de firewall – Local	114
4.2 Regra de firewall – Remoto	115
4.2 Lista de proibições temporária de endereço IP	116
4.2 Zona confiável	116
4.2 Configuração de zonas	117
4.2 Zonas de firewall	117
4.2 Relatório do firewall	118
4.2 Estabelecimento de uma conexão - detecção	118
4.2 Resolvendo problemas com o Firewall ESET	119
4.2 Assistente de solução de problemas	120
4.2 Registrando e criando regras ou exceções de log	120
4.2 Criar regra de log	120
4.2 Criando exceções de notificações do firewall	120
4.2 Registro em relatório avançado de proteção da rede	121
4.2 Resolvendo problemas com a filtragem de protocolo	121
4.3 Web e email	122
4.3 Filtragem de protocolos	124
4.3 Aplicativos excluídos	124
4.3 Endereços IP excluídos	125
4.3 SSL/TLS	126
4.3 Certificados	127
4.3 Tráfego de rede criptografado	128
4.3 Lista de certificados conhecidos	128
4.3 Lista de aplicativos SSL/TLS filtrados	129
4.3 Proteção do cliente de email	130
4.3 Protocolos de e-mail	131
4.3 Marcações de e-mail	132
4.3 Integração com clientes de email	133
4.3 Barra de ferramentas do Microsoft Outlook	133
4.3 Barra de ferramentas do Outlook Express e do Windows Mail	134
4.3 Caixa de diálogo de confirmação	135
4.3 Rastrear novamente mensagens	135
4.3 Proteção antispam	135
4.3 Catálogos de endereços antispam	137
4.3 Lista de proibições/Lista de permissões/Lista de exceções	138
4.3 Adicionar/Editar endereço da Lista de proibições/Lista de permissões/Lista de exceções	139
4.3 Proteção do acesso à Web	139
4.3 Configuração avançada de proteção de acesso à web	142
4.3 Protocolos da Web	142
4.3 Gerenciamento de endereços de URL	143
4.3 Lista de endereços URL	144
4.3 Criar nova lista	145
4.3 Como adicionar uma máscara de URL	146
4.3 Proteção antiphishing	147
4.3 Configuração avançada do Navegador protegido	148

4.3 Sites protegidos	149
4.3 Notificação no navegador	149
4.4 Controle de Web	150
4.4 Regras de controle de web	151
4.4 Adicionar regras de controle da Web	151
4.4 Grupos de categoria	153
4.4 Grupos de URL	154
4.4 Personalização de mensagem da página da web bloqueada	155
4.5 Atualização do programa	157
4.5 Configuração da atualização	161
4.5 Atualização de rollback	164
4.5 Atualizações de produto	166
4.5 Opção de conexão	166
4.5 Imagem de atualização	168
4.5 Servidor HTTP e SSL para a Imagem	170
4.5 Atualização através do mirror	170
4.5 Solução de problemas de atualização através da imagem	172
4.5 Como criar tarefas de atualização	173
4.6 Ferramentas	173
4.6 Relatórios	174
4.6 Filtragem de relatórios	177
4.6 Configuração do registro em relatório	178
4.6 Relatórios de auditoria	179
4.6 Agenda	180
4.6 ESET SysInspector	182
4.6 Proteção baseada em nuvem	183
4.6 Filtro de exclusões para Proteção baseada em nuvem	186
4.6 Processos em execução	186
4.6 Relatório de segurança	188
4.6 Conexões de rede	189
4.6 ESET SysRescue Live	191
4.6 Envio de amostras para análise	191
4.6 Selecionar amostra para análise - Arquivo suspeito	192
4.6 Selecionar amostra para análise - Site suspeito	192
4.6 Selecionar amostra para análise - Arquivo falso positivo	193
4.6 Selecionar amostra para análise - Site falso positivo	193
4.6 Selecionar amostra para análise - Outras	193
4.6 Quarentena	194
4.6 Configuração do servidor proxy	195
4.6 Segmentos de tempo	197
4.6 Microsoft Windows Update	197
4.6 Verificação de intervalo de licença	198
4.7 Interface do usuário	198
4.7 Elementos da interface do usuário	199
4.7 Configuração de acesso	200
4.7 Senha para Configuração avançada	201
4.7 Ícone da bandeja do sistema	202
4.7 Menu de contexto	203
4.7 Ajuda e suporte	203
4.7 Sobre o ESET Endpoint Security	204
4.7 Enviar dados de configuração do sistema	205

4.7 Suporte técnico	205
4.8 Notificações	206
4.8 Status de aplicativo	206
4.8 Notificações na área de trabalho	207
4.8 Janela de diálogo – notificações na área de trabalho	208
4.8 Personalização de notificações	208
4.8 Alertas interativos	208
4.8 Lista de alertas interativos	210
4.8 Mensagens de confirmação	211
4.8 Erro de conflito de configurações avançadas	212
4.8 Permitir continuar em um navegador padrão	212
4.8 Mídia removível	212
4.8 Requer reinicialização	213
4.8 Recomenda-se reiniciar	214
4.8 Encaminhamento	216
4.8 Gerenciador de perfil	218
4.8 Atalhos do teclado	219
4.8 Diagnóstico	219
4.8 Análise da linha de comandos	221
4.8 ESET CMD	223
4.8 Detecção em estado ocioso	225
4.8 Importar e exportar configurações	226
4.8 Reverter todas as configurações para o padrão	226
4.8 Reverter todas as configurações na seção atual	227
4.8 Erro ao salvar a configuração	227
4.8 Monitoramento e gerenciamento remoto	227
4.8 Linha de comando ERMM	228
4.8 Lista de comandos ERMM JSON	230
4.8 obter status de proteção	230
4.8 obter informações do aplicativo	231
4.8 obter informações da licença	234
4.8 obter relatórios	234
4.8 obter status de ativação	235
4.8 obter informações de rastreamento	236
4.8 obter configuração	237
4.8 obter status de atualização	238
4.8 iniciar rastreamento	239
4.8 iniciar ativação	239
4.8 iniciar desativação	240
4.8 iniciar atualização	241
4.8 definir configuração	241
5 Dúvidas comuns	242
5.1 FAQ de Atualizações automáticas	243
5.2 Como atualizar o ESET Endpoint Security	246
5.3 Como ativar o ESET Endpoint Security	246
5.3 Digitando sua chave de licença durante a ativação	247
5.3 Login no ESET Business Account	247
5.3 Como usar as credenciais de licença legado para ativar um produto endpoint da ESET mais novo	247
5.4 Como remover um vírus do meu PC	248
5.5 Como permitir comunicação para um determinado aplicativo	248
5.6 Como criar uma nova tarefa na Agenda	249

5.6 Como agendar um escanear semanal do computador	249
5.7 Como conectar o ESET Endpoint Security ao ESET PROTECT	250
5.7 Como usar o modo de Substituição	250
5.7 Como aplicar uma política recomendada para o ESET Endpoint Security	252
5.8 Como configurar uma imagem	254
5.9 Como atualizar para o Windows 10 com o ESET Endpoint Security	255
5.10 Como ativar o Monitoramento e gerenciamento remoto	255
5.11 Como bloquear o download de tipos de arquivo específicos da Internet	258
5.12 Como minimizar a interface do usuário do ESET Endpoint Security	259
5.13 Como resolver	259
6 Acordo de licença de usuário final	261
7 Política de Privacidade	268

ESET Endpoint Security 9

O ESET Endpoint Security 9 representa uma nova abordagem para a segurança do computador verdadeiramente integrada. A versão mais recente do mecanismo de rastreamento ESET LiveGrid®, combinada com nosso Firewall personalizado e os módulos antispam, utiliza velocidade e precisão para manter o computador seguro. O resultado é um sistema inteligente que está constantemente em alerta contra ataques e programas maliciosos que podem comprometer o funcionamento do computador.

O ESET Endpoint Security 9 é uma solução de segurança completa desenvolvida a partir do nosso esforço de longo prazo para combinar proteção máxima e impacto mínimo no sistema. As tecnologias avançadas, com base em inteligência artificial, são capazes de eliminar proativamente a infiltração por [vírus](#), spywares, cavalos de troia, worms, adwares, rootkits e outros [ataques via Internet](#) sem prejudicar o desempenho do sistema ou interromper a atividade do computador.

O ESET Endpoint Security 9 foi projetado principalmente para uso em estações de trabalho em um ambiente de negócios pequeno.

Na seção [Usando o ESET Endpoint Security por ele mesmo](#) você encontrará tópicos de ajuda divididos em diversos capítulos e subcapítulos para fornecer uma melhor orientação e contexto, inclusive para o [Download](#), [Instalação](#) e [Ativação](#).

[Usar o ESET Endpoint Security com ESET PROTECT](#) em um ambiente empresarial permite gerenciar facilmente qualquer número de estações de trabalho do cliente, aplicar políticas e regras, monitorar detecções e configurar remotamente clientes de qualquer computador em rede.

O capítulo [Perguntas mais frequentes](#) contém algumas perguntas e problemas mais frequentes encontrados.

Recursos e benefícios

Interface do usuário com novo design	A interface do usuário nesta versão foi redesenhada e simplificada significativamente com base em resultados de testes de usabilidade. Toda a linguagem da interface gráfica do usuário e das notificações foi revisada cuidadosamente e a interface agora é compatível com idiomas da direita para a esquerda, como hebreu e árabe. Ajuda on-line agora está integrada ao ESET Endpoint Security e oferece um conteúdo de suporte dinamicamente atualizado.
Antivírus e antispware	Detecta e limpa proativamente mais vírus, worms , cavalos de troia e rootkits conhecidos e desconhecidos. A heurística avançada sinalizada até mesmo malware nunca visto antes, protegendo você de ameaças desconhecidas e neutralizando-as antes que possam causar algum dano. A proteção de acesso à Web e proteção antiphishing funcionam monitorando a comunicação entre os navegadores da Internet e servidores remotos (incluindo SSL). A Proteção do cliente de email fornece controle da comunicação por email recebida através dos protocolos POP3(S) e IMAP(S).
Atualizações regulares	Atualizar o mecanismo de detecção (conhecido anteriormente como “banco de dados de assinatura de vírus”) e os módulos do programa periodicamente é a melhor forma de garantir o nível máximo de segurança em seu computador.
ESET LiveGrid® (Reputação potencializada pela nuvem)	Você pode verificar a reputação dos arquivos e dos processos em execução diretamente do ESET Endpoint Security.

Gerenciamento remoto	O ESET PROTECT permite a você gerenciar produtos ESET em estações de trabalho, servidores e dispositivos móveis em um ambiente de rede, de um local central. Usando o Web Console ESET PROTECT (Web Console ESET PROTECT) é possível implementar soluções ESET, gerenciar tarefas, implementar políticas de segurança, monitorar o status de sistema e responder rapidamente a problemas ou ameaças em computadores remotos.
Proteção de ataque a rede	Analisa o conteúdo do tráfego da rede e protege contra ataques de rede. Qualquer tráfego que seja considerado perigoso será bloqueado.
Controle de web (apenas ESET Endpoint Security)	O Controle de Web permite bloquear sites que possam conter material potencialmente ofensivo. Além disso, os empregadores ou administrador do sistema podem proibir o acesso para mais de 27 categorias de site predefinidas e mais de 140 subcategorias.

Novidades nessa versão?

O ESET Endpoint Security 9 foi lançado e está [disponível para download](#).

Atualizações automáticas

- garantem que você sempre use a versão do produto mais recente
- uma [solução inteligente](#) para reduzir a manutenção do ESET Endpoint Security para o mínimo necessário
- ativadas por padrão e usando a Atualização de componente de programa micro
- ele não reinstala o produto com todas as desvantagens, como cancelar o registro do sistema durante o processo, incluindo a transferência de configuração
- ele faz o download de menos dados (atualização diferencial)
- ele vem com um lembrete gentil ou que pode ser completamente suprimido para o usuário e é compatível com redes gerenciadas

Alterações associadas do Acordo de Licença para o Usuário Final (EULA)

- um novo EULA é apresentado independentemente do processo de instalação usando um elemento informativo no console ou na interface do usuário ESET Endpoint Security
- simplifica o processo de atualização automática do produto e melhora a experiência do usuário, pois você não precisará mais aceitar o EULA toda vez que seu produto ESET for atualizado para uma versão mais recente

Proteção contra ataque de força bruta

- como parte da Proteção contra ataque de rede repensada, a Proteção contra ataque de força bruta inspeciona o conteúdo do tráfego da rede e bloqueia tentativas de ataques sem senha
- tentativas repetidas com o endereço IP de origem são rastreadas e uma entrada de relatório é criada na lista de proibições de endereço IP temporário, que ajuda a monitorar a situação
- depois de um determinado período de tempo, o endereço IP de origem com esse comportamento pode ser liberado da lista de proibições se a conexão for legítima
- pode ser configurado em grandes redes

Build nativo ARM64

- a versão 9 oferece um build ARM64

Esta atualização vem com várias correções de bug e melhorias de desempenho.

Para mais informações e capturas de tela sobre os novos recursos no ESET Endpoint Security, leia o seguinte artigo na Base de conhecimento ESET:

- [Novidades do ESET Endpoint Security 9?](#)

Requisitos do sistema

Para uma operação sem interrupções do ESET Endpoint Security, o sistema deve atender aos seguintes requisitos de hardware e de software (configurações padrão do produto):

Processadores compatíveis

Processador Intel ou AMD, 32 bits (x86) com conjunto de instruções SSE2 ou 64 bits (x64), 1 GHz ou mais
processador baseado em ARM64, 1GHz ou mais

Sistemas operacionais

Microsoft® Windows® 11

Microsoft® Windows® 10



Para uma lista detalhada de versões compatíveis com o Microsoft® Windows® 10 e Microsoft® Windows® 11, consulte a [política de suporte ao sistema operacional Windows](#).



O suporte para a Assinatura de Código do Azure deve ser instalado em todos os sistemas operacionais Windows para instalar ou atualizar os produtos ESET lançados depois de julho de 2023. [Mais informações](#).

Microsoft® Windows® 8.1

Microsoft® Windows® 8

Microsoft® Windows® 7 SP1 com as atualizações do Windows mais recentes (no mínimo [KB4474419](#) e [KB4490628](#))



O ESET Endpoint Security versão 9.1 é a última compatível com o Windows 7 e Windows 8.1. [Mais informações](#).

O Windows XP e o Windows Vista [não são mais compatíveis](#).



Sempre tente manter seu sistema operacional atualizado.



O instalador ESET Endpoint Security criado no ESET PROTECT 8.1 e versões mais recentes é compatível com o Windows 10 Enterprise para Áreas de trabalho virtuais e o modo de várias sessões do Windows 10.

Outros

- Requisitos do sistema do sistema operacional e outros software instalado no computador são cumpridos

- 0,3 GB de memória do sistema livre (ver Nota 1)
- 1 GB de espaço livre em disco (ver Nota 2)
- Resolução mínima de exibição 1024x768
- Conexão com a Internet ou uma conexão com rede de área local para uma fonte (veja Nota 3) de atualizações do produto
- Dois programas antivírus sendo executados simultaneamente em um único dispositivo causam conflitos inevitáveis de recursos do sistema, como diminuir a velocidade do sistema até o ponto em que ele não consiga operar

Apesar de poder ser possível instalar e executar o produto em sistemas que não cumprem com esses requisitos, recomendamos um teste de usabilidade anterior a ser feito com base nos requisitos de desempenho.

- (1):** O produto pode usar mais memória se a memória fosse ser não usada, de outra forma, em um computador muito infectado ou quando grandes listas de dados estão sendo importadas para o produto (por exemplo lista de permissões de URL).
- (2):** O espaço em disco necessário para fazer download do instalador, instalar o produto e manter uma cópia do pacote de instalação nos dados do programa, assim como backups de atualizações do sistema para suportar o reversão de reversão. O produto pode usar mais espaço em disco em configurações diferentes (por exemplo quando mais versões de backup do produto estão armazenadas, despejos de memória ou altas quantidades de relatórios são mantidos) ou em um computador infectado (por exemplo devido ao recurso de quarentena). Recomendamos manter espaço em disco livre suficiente para suportar as atualizações do sistema operacional e para as atualizações de produtos ESET.
- (3):** Apesar de não ser recomendável, o produto pode ser atualizado manualmente de uma mídia removível.

Idiomas compatíveis

O ESET Endpoint Security está disponível para instalação e download nos seguintes idiomas.

Idioma	Código de idioma	LCID
Inglês (Estados Unidos)	en-US	1033
Árabe (Egito)	ar-EG	3073
Búlgaro	bg-BG	1026
Chinês simplificado	zh-CN	2052
Chinês tradicional	zh-TW	1028
Croata	hr-HR	1050
Tcheco	cs-CZ	1029
Estoniano	et-EE	1061
Finlandês	fi-FI	1035
Francês (França)	fr-FR	1036
Francês (Canadá)	fr-CA	3084
Alemão (Alemanha)	de-DE	1031
Grego	el-GR	1032
*Hebrew	he-IL	1037
Húngaro	hu-HU	1038
*Indonésio	id-ID	1057

Idioma	Código de idioma	LCID
Italiano	it-IT	1040
Japonês	ja-JP	1041
Cazaque	kk-KZ	1087
Coreano	ko-KR	1042
*Letão	lv-LV	1062
Lituano	lt-LT	1063
Nederlands	nl-NL	1043
Norueguês	nb-NO	1044
Polonês	pl-PL	1045
Português do Brasil	pt-BR	1046
Romeno	ro-RO	1048
Russo	ru-RU	1049
Espanhol (Chile)	es-CL	13322
Espanhol (Espanha)	es-ES	3082
Sueco (Suécia)	sv-SE	1053
Eslovaco	sk-SK	1051
Esloveno	sl-SI	1060
Tailandês	th-TH	1054
Turco	tr-TR	1055
Ucraniano (Ucrânia)	uk-UA	1058
*Vietnamita	vi-VN	1066

* O ESET Endpoint Security está disponível nesse idioma, mas o Guia do usuário on-line não está disponível (redirecionado para a versão em inglês).

Para alterar o idioma desse Guia do usuário on-line, veja a caixa de seleção de idioma (no canto superior direito).

Prevenção

Quando você trabalhar com o computador, e especialmente quando navegar na Internet, tenha sempre em mente que nenhum sistema antivírus do mundo pode eliminar completamente o risco de [detecções](#) e [ataques remotos](#). Para oferecer o máximo de proteção de conveniência, é essencial que você use sua solução antivírus corretamente e siga as seguintes regras úteis:

Atualização regular

De acordo com as estatísticas do ESET LiveGrid®, milhares de novas ameaças únicas são criadas todos os dias a fim de contornar as medidas de segurança existentes e gerar lucro para os seus autores - todas às custas dos demais usuários. Os especialistas no Laboratório de vírus da ESET analisam essas ameaças diariamente, preparam e publicam atualizações a fim de melhorar continuamente o nível de proteção de nossos usuários. Para garantir a máxima eficácia dessas atualizações, é importante que elas sejam configuradas devidamente em seu sistema. Para obter mais informações sobre como configurar as atualizações, consulte o capítulo [Configuração da atualização](#).

Download dos patches de segurança

Os autores dos softwares maliciosos frequentemente exploram as diversas vulnerabilidades do sistema a fim de aumentar a eficiência da disseminação do código malicioso. Considerado isso, as empresas de software vigiam de perto quaisquer vulnerabilidades em seus aplicativos para elaborar e publicar atualizações de segurança, eliminando as ameaças em potencial regularmente. É importante fazer o download dessas atualizações de segurança à medida que são publicadas. Microsoft Windows e navegadores da web, como o Internet Explorer, são dois exemplos de programas para os quais atualizações de segurança são lançadas regularmente.

Backup de dados importantes

Os escritores dos softwares maliciosos não se importam com as necessidades dos usuários, e a atividade dos programas maliciosos frequentemente leva ao mau funcionamento de um sistema operacional e à perda de dados importantes. É importante fazer o backup regular dos seus dados importantes e sensíveis para uma fonte externa como um DVD ou disco rígido externo. Isso torna mais fácil e rápido recuperar os seus dados no caso de falha do sistema.

Rastreie regularmente o seu computador em busca de vírus

A detecção de mais vírus, cavalos de troia e rootkits conhecidos e desconhecidos é realizada pelo módulo Proteção em tempo real do sistema de arquivos. Isso significa que sempre que você acessar ou abrir um arquivo, ele será rastreado quanto à atividade de malware. Recomendamos que você execute um rastreamento no computador inteiro pelo menos uma vez por mês, pois a assinatura de malware varia, assim como as atualizações do mecanismo de detecção são atualizadas diariamente.

Siga as regras básicas de segurança

Essa é a regra mais útil e eficiente de todas - seja sempre cauteloso. Hoje, muitas ameaças exigem a interação do usuário para serem executadas e distribuídas. Se você for cauteloso ao abrir novos arquivos, economizará tempo e esforço consideráveis que, de outra forma, seriam gastos limpando as ameaças. Aqui estão algumas diretrizes úteis:

- Não visite sites suspeitos com inúmeras pop-ups e anúncios piscando.
- Seja cuidadoso ao instalar programas freeware, pacotes codec. etc. Seja cuidadoso ao instalar programas freeware, pacotes codec. etc. Use somente programas seguros e somente visite sites da Internet seguros.
- Seja cauteloso ao abrir anexos de e-mail, especialmente aqueles de mensagens spam e mensagens de remetentes desconhecidos.
- Não use a conta do Administrador para o trabalho diário em seu computador.

Páginas de ajuda

Bem-vindo às páginas de ajuda do ESET Endpoint Security. As informações fornecidas aqui ajudarão você a se familiarizar com o produto e ajudar a tornar o computador mais seguro.

Introdução

Antes de iniciar o uso do ESET Endpoint Security, observe que nosso produto pode ser usado por [usuários conectados via ESET PROTECT](#) ou [sozinho](#). Além disso, recomendamos que você se familiarize com os vários [tipos de detecções](#) e [ataques remotos](#) que você pode encontrar ao usar seu computador.

Consulte [novos recursos](#) para saber mais sobre recursos introduzidos nesta versão do ESET Endpoint Security. Nós preparamos um guia para ajudá-lo a configurar e personalizar as configurações básicas do ESET Endpoint Security.


Como usar as páginas de ajuda do ESET Endpoint Security


Os tópicos de ajuda são divididos em diversos capítulos e subcapítulos para fornecer uma melhor orientação e contexto. Você pode encontrar as informações relacionadas navegando pela estrutura das páginas de ajuda.


Para saber mais sobre qualquer janela no programa, pressione **F1**. Será exibida a página de ajuda relacionada à janela que você está vendo.


Você pode pesquisar nas páginas de ajuda por palavra-chave ou digitando palavras ou frases. A diferença entre os dois métodos é que a palavra-chave pode ser logicamente relacionada às páginas de ajuda que não contenham aquela palavra-chave no texto. Usando as palavras ou frases pesquisará o conteúdo de todas as páginas e exibirá somente aquelas contendo a palavra ou a frase pesquisada.

Para fins de coerência e para evitar a confusão, a terminologia utilizada ao longo deste guia é baseada nos nomes de parâmetro do ESET Endpoint Security. Nós também usamos um conjunto uniforme de símbolos para destacar tópicos de interesse ou importância em particular.

 Uma nota é apenas uma observação curta. Apesar delas poderem ser omitidas, notas podem oferecer informações valiosas como recursos específicos ou um link para algum tópico relacionado.

 Isto requer a atenção, ignorar não é recomendado. Normalmente, fornece informações não críticas mas relevantes.

 Esta é uma informação que requer atenção e cautela adicionais. Os avisos são colocados especificamente para impedir você de cometer erros potencialmente nocivos. Leia e compreenda o texto colocado em parênteses de alerta, já que eles fazem referência a configurações do sistema altamente sensíveis ou a algo arriscado.

 Este é um caso de uso ou exemplo prático com o objetivo de ajudar a entender como uma determinada função ou recurso pode ser usado.

Convenção	Significado
Tipo negrito	Nomes de itens de interface, como caixas e botões de opção.
<i>Tipo itálico</i>	Espaços reservados para informações que você fornece. Por exemplo, nome do arquivo ou caminho significa que você digita o caminho ou nome de arquivo real.
Courier New	Amostras ou comandos de código.
Hyperlink	Fornece acesso rápido e fácil aos tópicos de referência cruzada ou locais externos da Web. Hyperlinks são destacados em azul e podem ser sublinhados.
%ProgramFiles%	O diretório do sistema do Windows onde os programas instalados no Windows estão armazenados.

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.

Documentação para endpoints gerenciados

remotamente

Os produtos empresariais da ESET, assim como o ESET Endpoint Security, podem ser gerenciados remotamente em estações de trabalho, servidores e dispositivos móveis do cliente em um ambiente de rede, de um local central. Administradores de sistema que gerenciam mais de 10 estações de trabalho do cliente podem considerar instalar uma das ferramentas de gerenciamento remoto da ESET para instalar soluções ESET, gerenciar tarefas, implementar [políticas de segurança](#), monitorar status do sistema e responder rapidamente a problemas ou ameaças em computadores remotos de um local central.

Ferramentas de gerenciamento remoto ESET

O ESET Endpoint Security pode ser gerenciado remotamente pelo ESET PROTECT ou pelo ESET Cloud Administrator.

- [Introdução ao ESET PROTECT](#)
- [Introdução ao ESET PROTECT Cloud](#)

Ferramentas de terceiros de gerenciamento remoto

- [Monitoramento e gerenciamento remoto \(RMM\)](#)

Melhores práticas

- [Conecte todos os endpoints com o ESET Endpoint Security para o ESET PROTECT](#)
- Proteja as [Definições de configuração avançada](#) nos computadores clientes conectados para evitar modificações não autorizadas
- Aplique [uma política recomendada](#) para implementar os recursos de segurança disponíveis
- [Minimizar a interface do usuário](#) – para reduzir ou limitar a interação do usuário com o ESET Endpoint Security

Guias de ação

- [Como usar o modo de Substituição](#)
- [Como instalar o ESET Endpoint Security usando GPO ou SCCM](#)

Introdução ao ESET PROTECT

O ESET PROTECT permite a você gerenciar produtos ESET em estações de trabalho, servidores e dispositivos móveis em um ambiente de rede, de um local central.

Usando o Web Console ESET PROTECT, você pode instalar soluções ESET, gerenciar tarefas, implementar políticas de segurança, monitorar o status do sistema e responder rapidamente a problemas ou detecções em computadores remotos. Veja também a [Visão geral de elementos de arquitetura e infraestrutura do ESET PROTECT](#), [Introdução ao Web Console ESET PROTECT](#) e [Ambientes de provisionamento de área de trabalho compatíveis](#).

O ESET PROTECT é feito dos seguintes componentes:

- [ESET PROTECT Servidor](#) - o Servidor ESET PROTECT pode ser instalado no Windows, assim como em

servidores Linux, e também vem como um Equipamento virtual. Ele lida com a comunicação com Agentes e coleta e armazena dados de aplicativo no banco de dados.

- [ESET PROTECT Console da web](#) - O Console da web ESET PROTECT é a interface primária que permite a você gerenciar os computadores cliente no seu ambiente. Ele exibe uma visão geral do status de clientes em sua rede e permite que você use soluções da ESET em computadores não gerenciados remotamente. Depois de instalar o Servidor ESET PROTECT, você pode acessar o Console da web usando seu navegador da web. Se escolher disponibilizar o servidor via Internet, você pode usar o ESET PROTECT de qualquer lugar e/ou dispositivo com uma conexão com a Internet.
- [Agente ESET Management](#) – o Agente ESET Management facilita a comunicação entre o Servidor ESET PROTECT e os computadores cliente. O Agente deve ser instalado em qualquer computador do cliente para estabelecer comunicação entre o computador e o Servidor ESET PROTECT. Como ele está localizado no computador cliente e pode armazenar vários cenários de segurança, o uso do Agente ESET Management diminui de forma significativa o tempo de reação a novas detecções. Usando o Web Console ESET PROTECT é possível [implementar o Agente ESET Management](#) para computadores não gerenciados identificados através do seu Active Directory ou o ESET [RD Sensor](#). Você também pode [instalar manualmente o Agente ESET Management](#) nos computadores cliente se necessário.
- [ESET Rogue Detection Sensor](#) - O ESET Rogue Detection (RD) Sensor detecta computadores não gerenciados presentes na sua rede e envia as informações ao Servidor ESET PROTECT. Isso permite que você adicione com facilidade novos computadores do cliente na sua rede segura. O RD Sensor lembrará dos computadores que já foram detectados e não enviará as mesmas informações duas vezes.
- [Proxy Apache HTTP](#) - É um serviço que pode ser usado em combinação com o ESET PROTECT para:
 - Distribuir atualizações para computadores cliente e pacotes de instalação para o Agente ESET Management.
 - Comunicação encaminhada dos Agentes ESET Management para o Servidor ESET PROTECT.
- [Mobile Device Connector](#) - é um componente que permite o Gerenciamento de dispositivo móvel com o ESET PROTECT, permitindo a você gerenciar dispositivos móveis (Android e iOS) e administrar o ESET Endpoint Security para Android.
- máquina virtualEquipamento Virtual [ESET PROTECT](#) - O ESET PROTECT VA é feito para usuários que queiram executar o ESET PROTECT em um ambiente virtualizado.
- [ESET PROTECT Virtual Agent Host](#) - Um componente do ESET PROTECT que virtualiza as entidades do agente para permitir o gerenciamento de máquinas virtuais sem agente. A solução permite a automação, uso de grupo dinâmico e o mesmo nível de gerenciamento de tarefa que um Agente ESET Management nos computadores físicos. O Agente Virtual coleta informações de máquinas virtuais e envia-as ao Servidor ESET PROTECT.
- [Ferramenta de imagem](#) - A ferramenta de imagem é necessária para atualizações off-line dos módulos. Se os computadores cliente não tiverem uma conexão à Internet, você pode usar a Ferramenta de imagem para fazer download de arquivos de atualização dos servidores de atualização ESET e armazená-los localmente.
- [ESET Remote Deployment Tool](#) - Esta ferramenta permite que você implante Pacotes Tudo-em-um criados pelo Console da Web <%PRODUCT%>. É uma forma conveniente de distribuir o Agente ESET Management com um produto ESET nos computadores de uma rede.
- [ESET Business Account](#) - O novo portal de licenciamento para produto empresarial ESET permite a você gerenciar licenças. Consulte a seção [ESET Business Account](#) deste documento para instruções sobre como ativar o produto, ou consulte o ESET Business Account [Guia do Usuário](#) para mais informações sobre o uso do ESET Business Account. Se você já tem um Usuário e Senha emitidos pela ESET que deseja converter para uma chave de licença, consulte a seção [Converter credenciais de licença de legado](#).
- [ESET 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.

Usando o Console web ESET PROTECT, você pode instalar soluções ESET, gerenciar tarefas, implementar [políticas de segurança](#), monitorar o status do sistema e responder rapidamente a problemas ou ameaças em computadores remotos.

 Para mais informações, consulte o [Guia do usuário on-line do ESET PROTECT](#).

Introdução ao ESET PROTECT Cloud

ESET PROTECT Cloud permite que você gerencie produtos ESET em estações de trabalho e servidores em um ambiente em rede a partir de um local central sem precisar ter um servidor físico ou virtual como o ESET PROTECT. Usando o (Console Web ESET PROTECT Cloud) é possível implementar soluções ESET, gerenciar tarefas, implementar políticas de segurança, monitorar o status de sistema e responder rapidamente a problemas ou ameaças em computadores remotos.

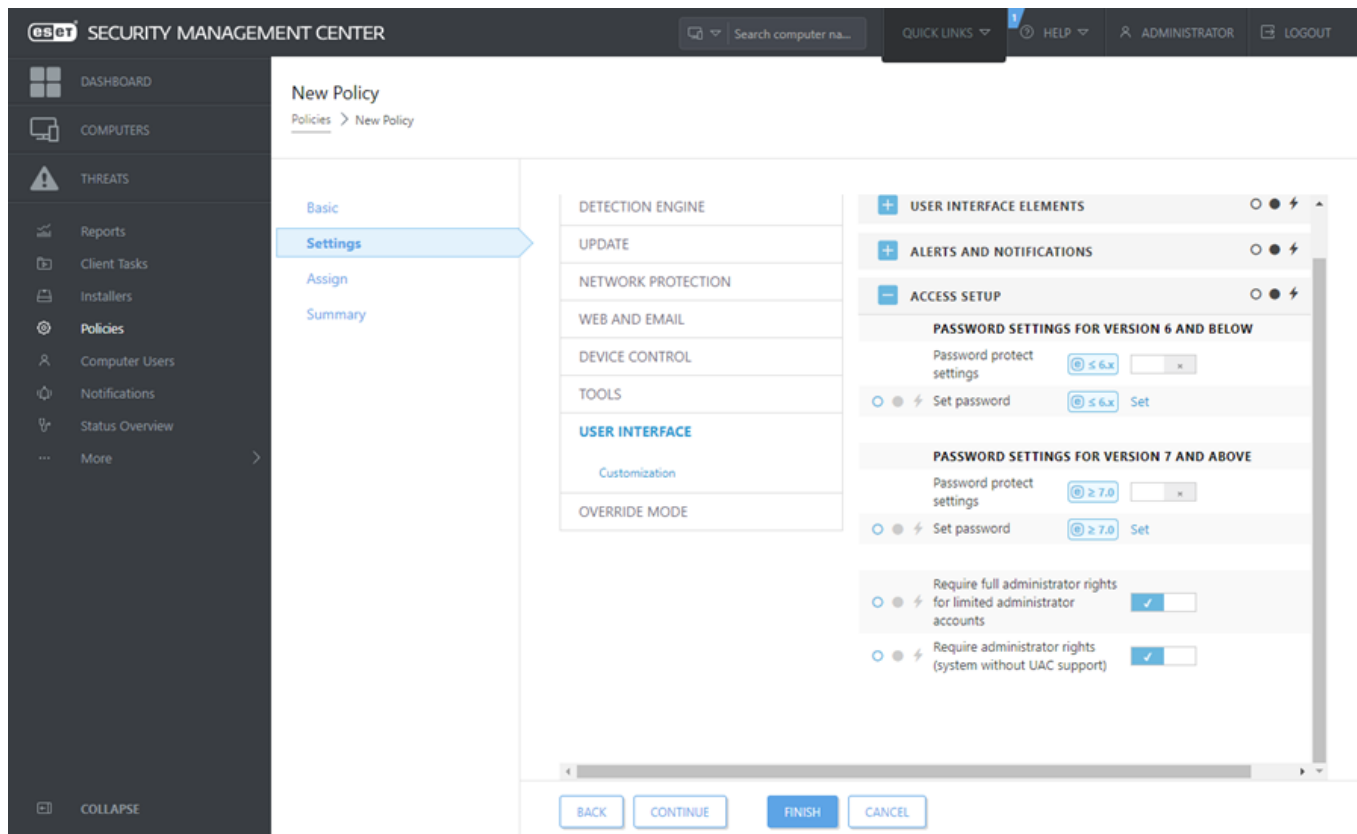
- [Leia mais sobre isso no Guia do usuário on-line do ESET PROTECT Cloud](#)

Configurações protegidas por senha

Para oferecer o máximo de segurança ao seu sistema, o ESET Endpoint Security precisa ser configurado corretamente. Qualquer alteração ou configuração não qualificada pode resultar em uma diminuição da segurança do cliente e do nível de proteção. Para limitar o acesso do usuário a uma configuração avançada, um administrador pode proteger as configurações por senha.

O administrador pode criar uma política para proteger com senha as configurações de Configuração avançada do ESET Endpoint Security nos computadores cliente conectados. Para criar uma nova política:

1. No Web Console ESET PROTECT, clique em **Políticas** no menu principal da esquerda.
2. Clique em **Nova política**.
3. Nomeie sua nova política e, opcionalmente, dê a ela uma pequena descrição. Clique no botão **Continuar**.
4. Da lista de produtos, selecione **ESET Endpoint para Windows**.
5. Clique em **Interface do usuário** na lista **Configurações** e abra a **Configuração de acesso**.
6. De acordo com a versão do ESET Endpoint Security, clique na barra deslizante para ativar **Proteger configurações com senha**. Observe que os produtos ESET Endpoint versão 7 oferecem uma proteção aprimorada. Se você tiver tanto a versão 7 quanto a versão 6 dos produtos Endpoint na rede, recomendamos criar duas políticas separadas com senhas diferentes para cada versão.
7. Na janela pop-up crie uma nova senha, confirme-a e clique em **OK**. Clique em **Continuar**.
8. Atribuir a política aos clientes. Clique em **Atribuir** e selecione os computadores ou grupos de computadores a serem protegidos por senha. Clique em **OK** para confirmar.
9. Verifique se todos os computadores cliente desejados estão na lista de destino e clique em **Continuar**.
10. Revise as configurações da política na seção resumo e clique em **Concluir** para aplicar a política.



O que são políticas

O administrador pode aplicar configurações específicas em produtos ESET sendo executados nos computadores cliente usando políticas do Console web ESET PROTECT. Uma política também pode ser aplicada diretamente aos computadores individuais, assim como a grupos de computadores. Você também pode atribuir várias políticas a um computador ou grupo.

Um usuário precisa das seguintes permissões para criar uma nova política: permissão de **Leitura** para ler a lista de políticas, permissão de **Uso** para atribuir políticas a computadores de destino e permissão de **Gravação** para criar, modificar ou editar políticas.

As políticas são aplicadas na ordem em que os grupos estáticos são organizados. Isso não é verdadeiro para Grupos dinâmicos, onde as políticas são aplicadas primeiro aos Grupos dinâmicos secundários. Isso permite a você aplicar políticas com maior impacto no topo da árvore do grupo e aplicar políticas mais específicas aos subgrupos. Usando [sinalizadores](#), um usuário ESET Endpoint Security com acesso aos grupos localizados mais acima na árvore poderá anular as políticas dos grupos inferiores. O algoritmo é explicado na [Ajuda on-line ESET PROTECT](#).



Recomendamos atribuir políticas mais genéricas (por exemplo, a política do 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](#)).



Mesclagem de Políticas

Uma política aplicada a um cliente normalmente é resultado de várias políticas sendo mescladas em uma política final. As políticas são mescladas uma a uma. Ao mesclar políticas, a regra geral é que a última política sempre substitui as configurações definidas pela política anterior. Para mudar esse comportamento, você pode usar os [sinalizadores de política](#) (Disponíveis para cada configuração).

Ao criar políticas você vai perceber que algumas configurações têm regras adicionais (substituir/inserir no começo/inserir no final) que você pode configurar.

- **Substituir** - a lista é substituída por inteiro, adiciona novos valores e remove a anterior.
- **Incluir no fim** - os itens são adicionados no final da lista aplicada no momento (deve ser outra política, a lista local é sempre sobrescrita).
- **Incluir no começo** - os itens são adicionados no começo da lista (a lista local é sempre sobrescrita).

ESET Endpoint Security é compatível com a mesclagem de configurações locais com as políticas remotas de uma nova forma. Se a configuração for uma lista (por exemplo, uma lista de sites bloqueados) e uma política remota estiver em conflito com uma configuração local existente, a política remota vai substituir a local. Você pode escolher como combinar as listas local e remota ao selecionar as regras de mesclagem diferentes para:




-  Configurações de mesclagem para políticas remotas.
-  Mesclagem de políticas remotas e locais - configurações locais com a política remota resultante.

Para saber mais sobre a mesclagem de políticas, siga o [Guia do usuário on-line do ESET PROTECT](#) e veja o [exemplo](#).

Como os sinalizadores funcionam

A política que é aplicada ao computador cliente normalmente é o resultado de várias políticas sendo mescladas em uma política final. Ao mesclar políticas, você pode ajustar o comportamento esperado da política final graças à ordem das políticas aplicadas, usando sinalizadores de políticas. Os sinalizadores definem como a política vai lidar com uma configuração em específico.

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 definida pela política, ela pode ser alterada por outras políticas aplicadas posteriormente.
 Aplicar	Configurações com o sinalizador Aplicar serão aplicadas ao computador do cliente. Porém, ao mesclar as políticas, isso pode ser sobrescrito por outras políticas aplicadas mais tarde. Quando uma política é enviada para um computador cliente contendo configurações marcadas com esse sinalizador, essas configurações vão alterar a configuração local do computador cliente. Como a configuração não é forçada, ela ainda pode ser alterada por outras políticas aplicadas posteriormente.
 Forçar	Configurações com o sinalizador Forçar têm prioridade e não podem ser sobrescritas por qualquer outra política aplicada posteriormente (mesmo se ela também tiver o sinalizador Forçar). Isso garante que outras políticas aplicadas mais tarde não conseguirão alterar essa configuração durante a mesclagem. Quando uma política é enviada para um computador cliente contendo configurações marcadas com esse sinalizador, essas configurações vão alterar a configuração local do computador cliente.

Cenário: O *Administrador* quer permitir que o usuário *John* crie ou edite políticas em seu grupo doméstico e veja as políticas criadas pelo *Administrador* inclusive Políticas com o sinalizador ⚡ **Forçar**. O *Administrador* quer que *John* seja capaz de ver todas as políticas, mas não de editar as políticas existentes criadas pelo *Administrador*. *John* só pode criar ou editar políticas dentro de seu Grupo doméstico, San Diego.

Solução: O *Administrador* deve seguir essas etapas:

Criar grupos estáticos e conjuntos de permissões personalizados

1. Criar um novo [Grupo estático](#) chamado *San Diego*.
2. Criar um novo [Conjunto de permissões](#) chamado *Política - Todos John* com acesso ao Grupo estático *Todos* e com permissão de **Leitura** para as **Políticas**.
3. Criar um novo [Conjunto de permissões](#) chamado *Política John* com acesso ao Grupo estático *San Diego*, com permissão para a funcionalidade de acesso **Gravação** para **Grupo e Computadores** e **Políticas**. Esse conjunto de permissões permite ao usuário *John* criar ou editar políticas em seu grupo inicial *San Diego*.
4. Criar um novo [usuário](#) *John* e na seção **Conjunto de Permissões** selecione *Política - Todos John* e *Política John*.

Criar políticas

5. Crie uma nova [política](#) *Todos - Ativar Firewall*, expanda a seção **Configurações**, selecione **ESET Endpoint para Windows**, navegue até **Firewall Pessoal > Básico** e aplique todas as configurações pelo sinalizador ⚡ **Forçar**. Abra 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 **Firewall Pessoal > Básico** e aplique todas as configurações pelo sinalizador ● **Aplicar**. Abra a seção **Atribuir** e selecione o Grupo estático *San Diego*.

Resultado

As Políticas criadas pelo *Administrador* serão aplicadas primeiro, já que os sinalizadores ⚡ **Forçar** foram aplicados nas configuração da política. As configurações com o sinalizador **Forçar** aplicado têm prioridade e não podem ser sobrescritas por outras política aplicada posteriormente. As políticas que são criadas pelo usuário *John* serão aplicadas depois das políticas criadas pelo *Administrador*.

Para ver a ordem final de política, vá para **Mais > Grupos > San Diego**. Selecione o computador e selecione **Mostrar detalhes**. Na seção **Configuração**, clique em **Políticas aplicadas**.

Usando o ESET Endpoint Security por ele mesmo

Esta seção e a seção [Trabalhar com o ESET Endpoint Security](#) do guia do usuário são feitas para usuários que estão utilizando o ESET Endpoint Security sem o ESET PROTECT ou ESET PROTECT Cloud. Todos os recursos e funcionalidades do ESET Endpoint Security estão totalmente acessíveis dependendo dos direitos da conta do usuário.

Método de instalação

Existem vários métodos de instalação do ESET Endpoint Security versão 9.x em uma estação de trabalho do cliente, a menos que você [instale o ESET Endpoint Security remotamente nas estações de trabalho do cliente via ESET PROTECT ou ESET PROTECT Cloud](#).

Métodos	Objetivo	Link de download
Instalação com o ESET AV Remover	A ferramenta ESET AV Remover ajudará você a remover os softwares antivírus instalados anteriormente no seu sistema antes de continuar com a instalação.	Download de 64-bit Download de 32-bit
Instalação (.exe)	Processo de instalação sem o ESET AV Remover.	N/A

Métodos	Objetivo	Link de download
Instalação (.msi)	Em ambientes comerciais, o instalador .msi é o pacote de instalação preferido. Isso acontece principalmente devido a instalações off-line e remotas que usar ferramentas variadas, como o ESET PROTECT.	Download de 64-bit Download de 32-bit
Instalação da linha de comando	O ESET Endpoint Security pode ser instalado localmente usando uma linha de comando, ou remotamente usando uma tarefa do cliente do ESET PROTECT.	N/A
Instalação usando GPO ou SCCM	Use ferramentas de gerenciamento como o GPO ou SCCM para instalar o ESET Management Agent e o ESET Endpoint Security nas estações de trabalho do cliente.	N/A
Instalação usando ferramentas RMM	Os plugins ESET DEM para a ferramenta de Gerenciamento e monitoramento remoto (RMM) permitem que você instale o ESET Endpoint Security em estações de trabalho do cliente.	N/A

O ESET Endpoint Security está [disponível em mais de 30 idiomas](#).

Instalação com o ESET AV Remover

Antes de continuar com o processo de instalação, é importante que outros aplicativos de segurança existentes no computador sejam desinstalados. Selecione a caixa de seleção ao lado de **Quero desinstalar aplicativos antivírus indesejados usando o ESET AV Remover** para que o ESET AV Remover rastreie seu sistema e remova qualquer [aplicativo de segurança compatível](#). Deixe a guia caixa de seleção desmarcada e clique em **Continuar** para instalar o ESET Endpoint Security sem executar o ESET AV Remover.

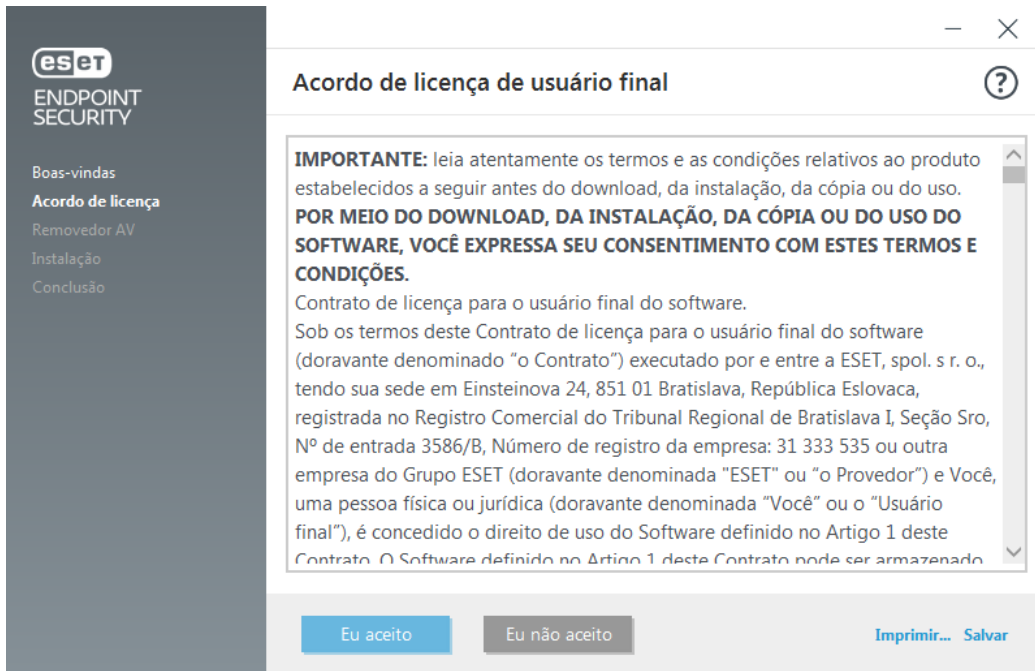


ESET AV Remover

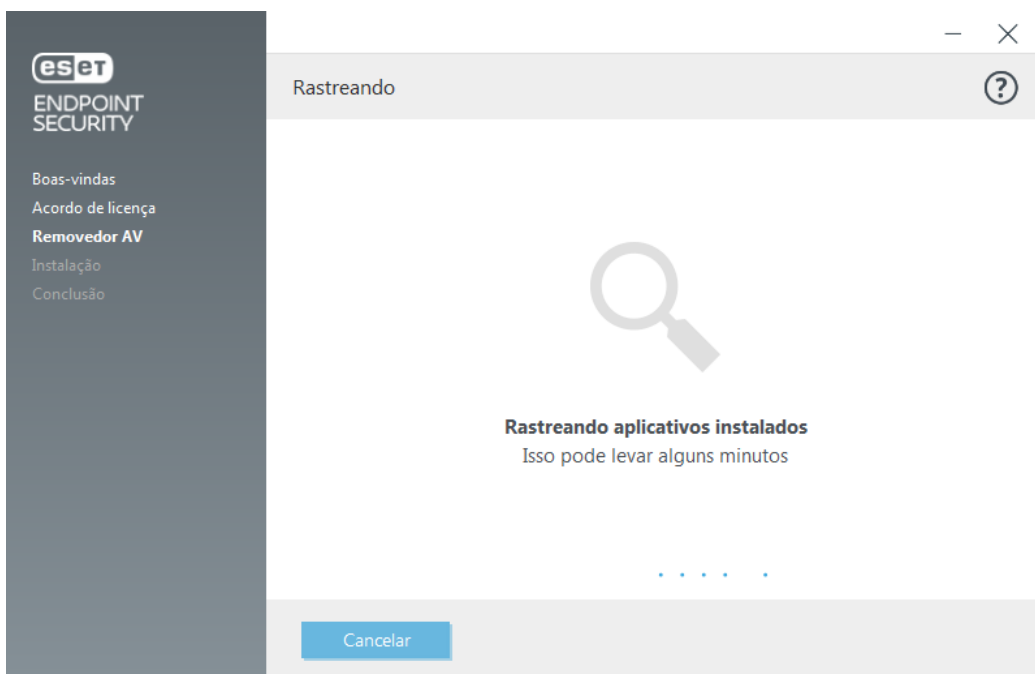
A ferramenta ESET AV Remover ajudará você a remover quase todos os software antivírus instalados anteriormente no seu sistema. Siga as instruções abaixo para remover um programa antivírus existente usando o

ESET AV Remover:

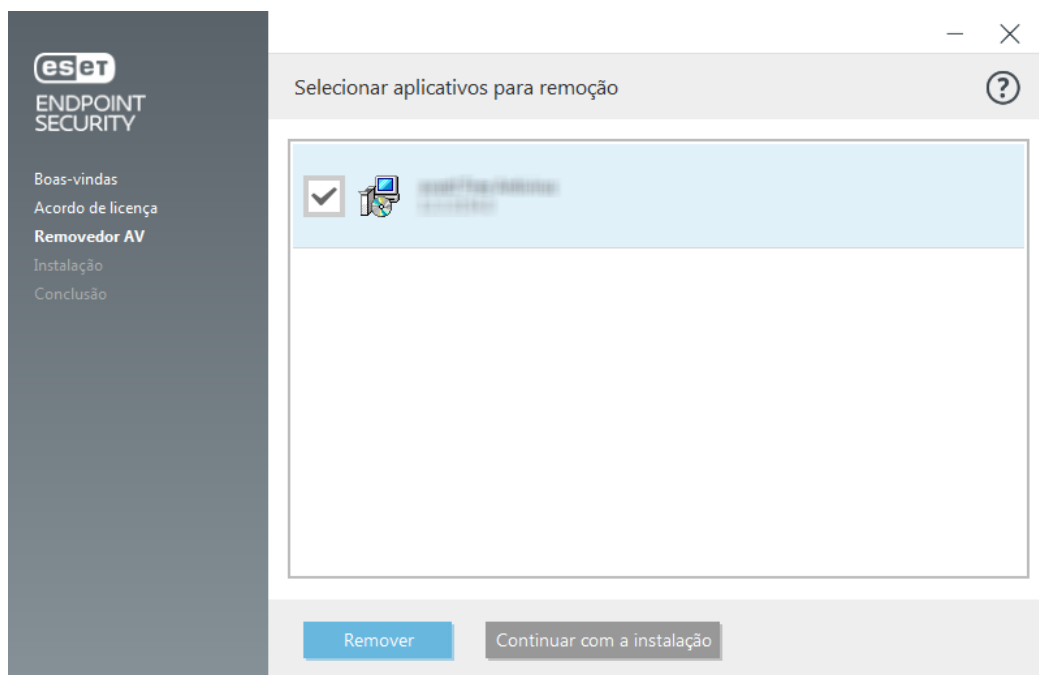
1. Para ver uma lista de software antivírus que o ESET AV Remover pode remover, [visite o Artigo na base de conhecimento ESET](#).
2. Leia o Acordo de Licença para o usuário final e clique em **Aceitar** para confirmar a sua aceitação. Clicar em **Eu não aceito** vai continuar com a instalação do ESET Endpoint Security sem remover qualquer aplicativo de segurança existente no computador.



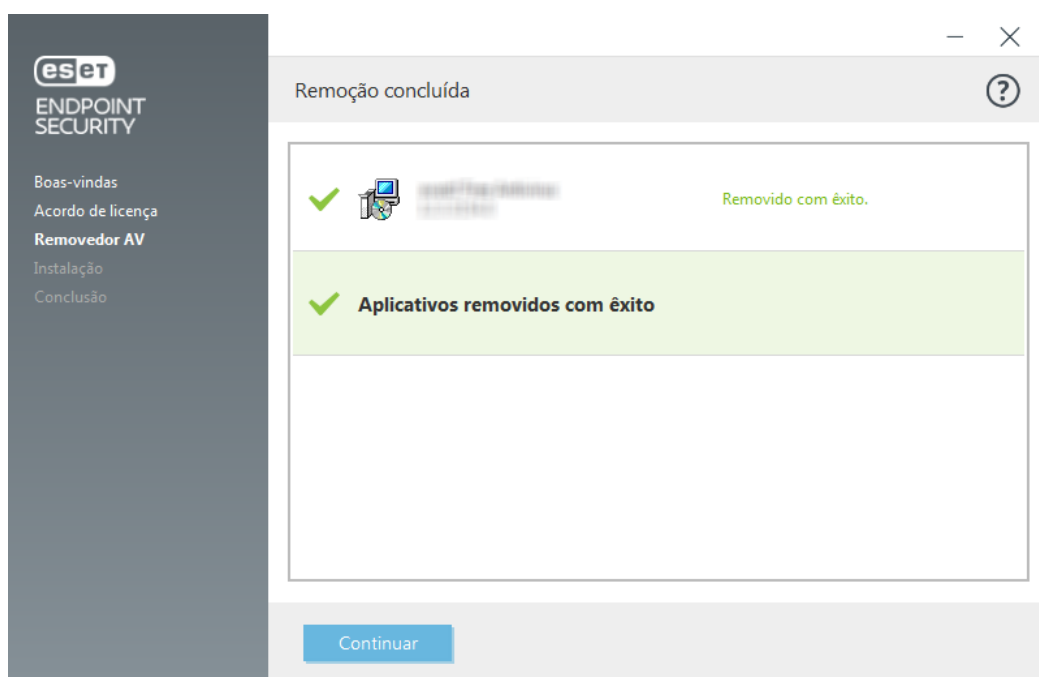
2. o ESET AV Remover começará a procurar por software antivírus no seu sistema.



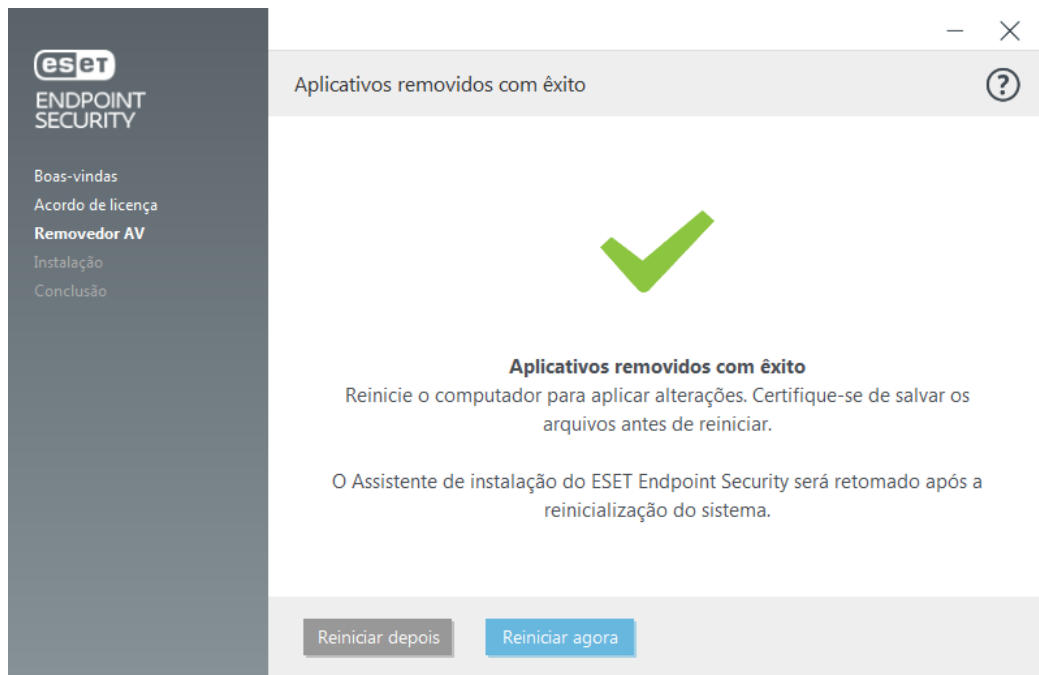
2. Selecione qualquer aplicativo antivírus listado e clique em **Remover**. A remoção pode levar alguns minutos.



2. Quando a remoção é bem sucedida, clique em **Continuar**.



6. Reinicie seu computador para aplicar as alterações e continue com a instalação do ESET Endpoint Security. Se a desinstalação não for bem sucedida, consulte a seção [Desinstalação com o ESET AV Remover terminou com erro](#) deste guia.



Desinstalação usando o ESET AV Remover terminou com erro

Se você não conseguir remover um programa antivírus usando o ESET AV Remover, você receberá uma notificação de que o aplicativo que está tentando remover pode não ser compatível com o ESET AV Remover. Visite a [lista de produtos compatíveis](#) ou [desinstaladores para software antivírus comuns do Windows](#) na Base de conhecimento ESET para ver se este programa específico pode ser removido.

Quando a desinstalação do produto de segurança não foi bem sucedida ou parte do seu componente foi desinstalado parcialmente, você é solicitado a **Reiniciar e escanear novamente**. Confirmar UAC depois da inicialização e continuar com o processo de escaneamento e desinstalação.

Se necessário, entre em contato com o [Suporte técnico ESET](#) para abrir uma solicitação de suporte e para que o arquivo **AppRemover.log** esteja disponível para ajudar os Técnicos da ESET. O arquivo **AppRemover.log** está localizado na pasta **eset**. Procure por **%TEMP%** no Windows Explorer para acessar esta pasta. O Suporte técnico ESET responderá o mais rápido possível para ajudar a resolver seu problema.

Instalação (.exe)

Depois de iniciar o instalador .exe, o assistente de instalação vai guiá-lo pelo processo de instalação.



Verifique se não há algum outro programa antivírus instalado no computador. Se duas ou mais soluções antivírus estiverem instaladas em um único computador, elas podem entrar em conflito umas com as outras. Recomendamos desinstalar outros programas antivírus do sistema. Consulte nosso [artigo da base de conhecimento](#) para obter uma lista de ferramentas de desinstalação para os softwares de antivírus comuns (disponível em inglês e vários outros idiomas).



1. Leia o Acordo de Licença para o Usuário final. Clique em **Permitir tudo e continuar** se quiser configurar a detecção de [Aplicativos potencialmente indesejados](#) e ativar o [sistema de feedback ESET LiveGrid®](#). O ESET LiveGrid® ajuda a garantir que a ESET seja informada imediata e continuamente sobre novas infiltrações, o que nos permite proteger melhor nossos clientes. O sistema permite que você envie novas ameaças para o Laboratório de vírus da ESET, onde elas serão analisadas, processadas e adicionadas ao mecanismo de detecção. Clique em **Continuar** para confirmar sua aceitação do Acordo de licença para o usuário final. Você pode instalar o ESET Endpoint Security em uma pasta específica clicando em [Alterar a pasta de instalação](#).



2. Depois da instalação ser concluída, você será solicitado a [ativar o ESET Endpoint Security](#).

Mudar pasta de instalação (.exe)

Depois de selecionar sua preferência para detecção de aplicativos potencialmente não desejados e clicar em **Alterar a pasta de instalação**, você será solicitado a selecionar um local para a pasta do produto ESET Endpoint Security de instalação. Por padrão, o programa é instalado no seguinte diretório:

C:\Program Files\ESET\ESET Security

Você pode especificar um local para dados e módulos de programa. Por padrão, eles são instalados nos seguintes diretórios:

C:\Program Files\ESET\ESET Security\Modules

C:\ProgramData\ESET\ESET Security

Clique em **Procurar** para alterar esses locais (não recomendado).

A imagem mostra a interface de instalação do ESET Endpoint Security. No lado esquerdo, há uma barra lateral com o logotipo ESET e as opções: 'Boas-vindas', 'Instalação' (destacada) e 'Conclusão'. O título principal da janela é 'Selecione a pasta de instalação'. Abaixo, há três seções para seleção de pastas:

- Pasta do produto:** Campo de texto com o caminho 'C:\Program Files\ESET\ESET Security\' e um botão 'Procurar...'.
- ☐ Quero especificar pastas diferentes para arquivos que mudam com frequência
- Pasta do módulo:** Campo de texto com o caminho 'C:\Program Files\ESET\ESET Security\Modules\' e um botão 'Procurar...'.
- Pasta de dados:** Campo de texto com o caminho 'C:\ProgramData\ESET\ESET Security\' e um botão 'Procurar...'.

Na base da janela, há três botões: 'Continuar' (em azul), 'Voltar' e 'Redefinir para padrão'.

Clique em **Voltar** e continue com o processo de instalação.

Instalação (.msi)

Depois de iniciar o instalador .ini, o assistente de instalação vai guiá-lo pelo processo de instalação.



Em ambientes comerciais, o instalador .msi é o pacote de instalação preferido. Isso acontece principalmente devido a instalações off-line e remotas que usar ferramentas variadas, como o ESET PROTECT.



Verifique se não há algum outro programa antivírus instalado no computador. Se duas ou mais soluções antivírus estiverem instaladas em um único computador, elas podem entrar em conflito umas com as outras. Recomendamos desinstalar outros programas antivírus do sistema. Consulte nosso [artigo da base de conhecimento](#) para obter uma lista de ferramentas de desinstalação para os softwares de antivírus comuns (disponível em inglês e vários outros idiomas).

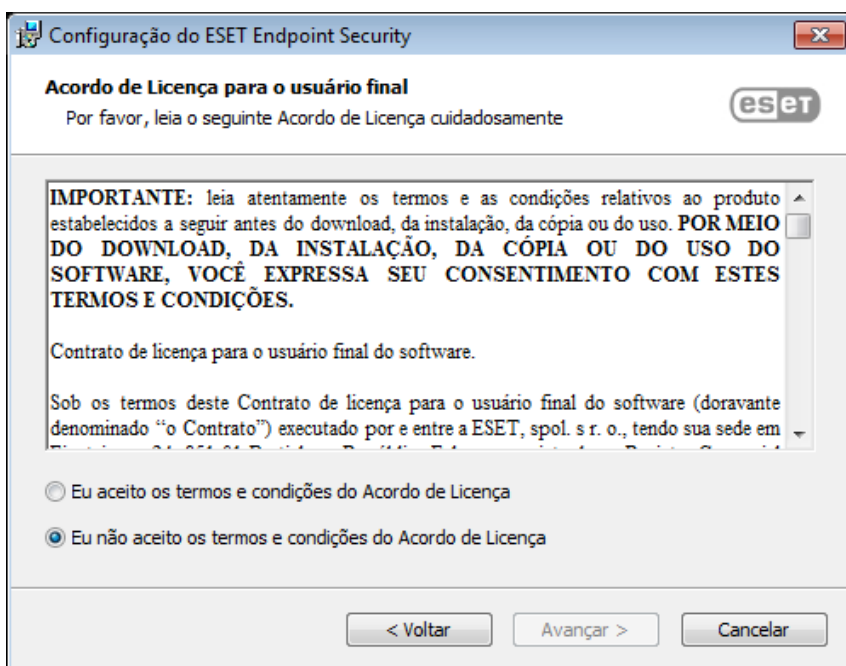


O instalador ESET Endpoint Security criado no ESET PROTECT 8.1 e versões mais recentes é compatível com o Windows 10 Enterprise para Áreas de trabalho virtuais e o modo de várias sessões do Windows 10.

1. Selecione o idioma desejado e clique em **Avançar**.

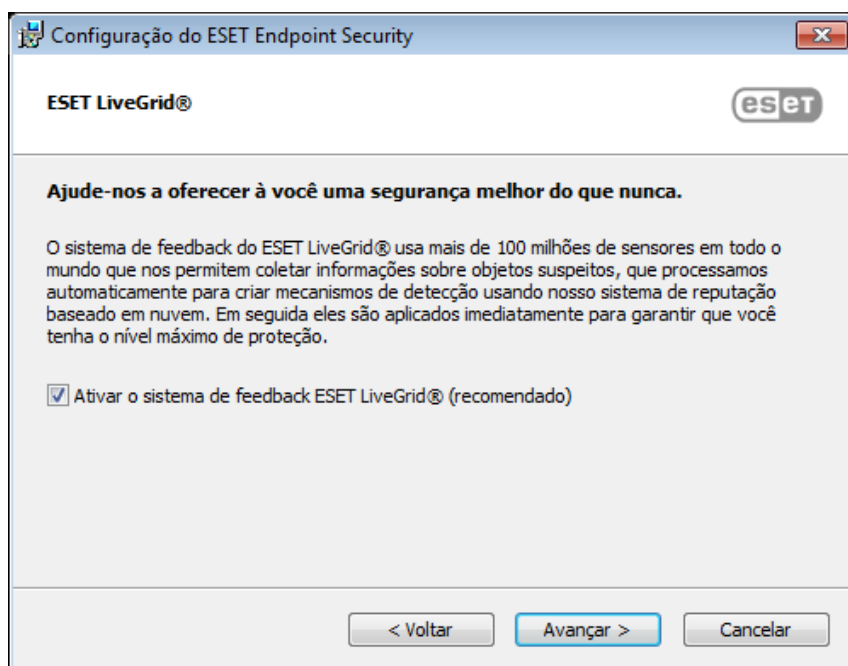


2. Leia o Acordo de Licença para o Usuário Final e clique em **Aceito os termos do Acordo de licença** para confirmar a sua aceitação do Acordo de licença para o usuário final. Clique em **Avançar** depois de aceitar os termos para continuar com a instalação.



3. Defina sua preferência para o [sistema de feedback ESET LiveGrid®](#). O ESET LiveGrid® ajuda a garantir que a ESET seja informada imediata e continuamente sobre novas infiltrações, para que possamos proteger

melhor nossos clientes. O sistema permite que você envie novas ameaças para o Laboratório de vírus da ESET, onde elas serão analisadas, processadas e adicionadas ao mecanismo de detecção. Clique em **Configurações avançadas** se quiser continuar com a [Instalação avançada \(.msi\)](#).



5. A etapa final é confirmar a instalação clicando em **Instalar**. Depois da instalação ser concluída, você será solicitado a [ativar o ESET Endpoint Security](#).

Instalação avançada (.msi)

A instalação avançada permitirá que você personalize vários parâmetros de instalação não disponíveis ao realizar uma instalação típica.

5. Depois de selecionar sua preferência para detecção de [aplicativos potencialmente indesejados](#) e clicar em **Configurações avançadas**, você será solicitado a selecionar um local para a pasta do produto ESET Endpoint Security de instalação. Por padrão, o programa é instalado no seguinte diretório:

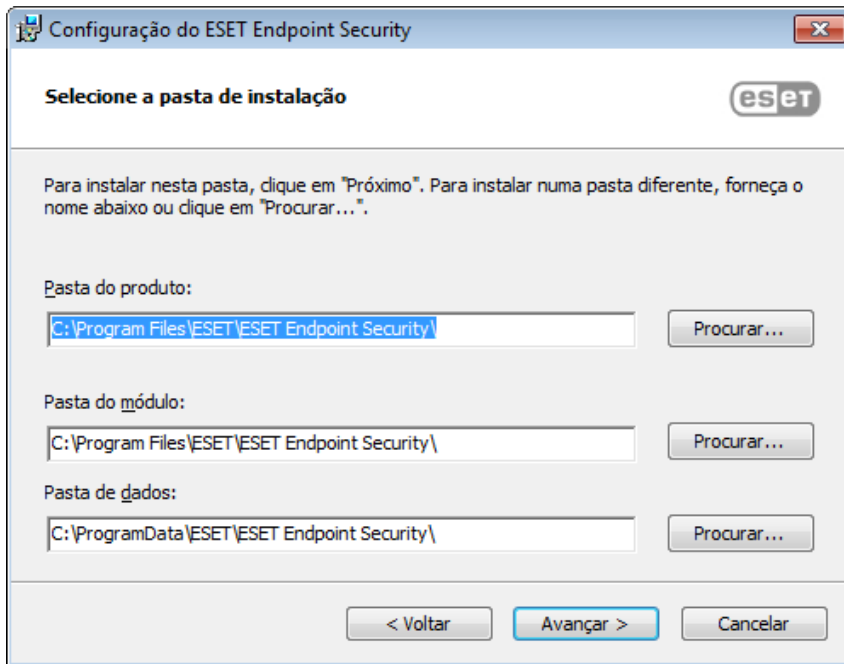
C:\Program Files\ESET\ESET Security

Você pode especificar um local para dados e módulos de programa. Por padrão, eles são instalados nos seguintes diretórios:

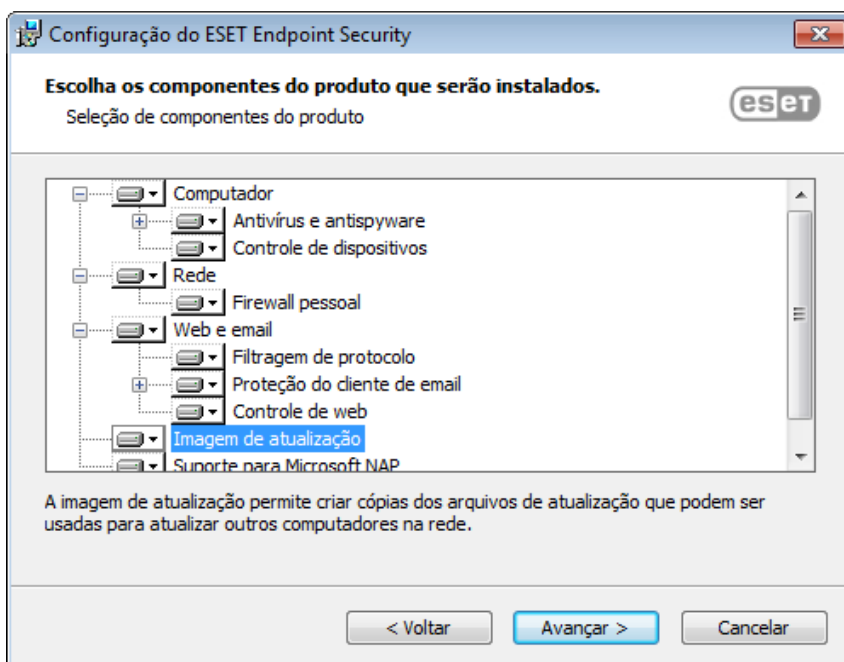
C:\Program Files\ESET\ESET Security\Modules

C:\ProgramData\ESET\ESET Security

Clique em **Procurar** para alterar esses locais (não recomendado).



6. Escolha quais componentes do produto serão instalados. Os componentes do produto na seção [Computador](#) incluem a Proteção em tempo real do sistema de arquivos, Escanear o computador, Proteção de documentos e Controle de dispositivos. Observe que os primeiros dois componentes são obrigatórios para o funcionamento de sua solução de segurança. A seção [Rede](#) oferece a opção de instalação do firewall ESET, que monitora todo o tráfego de entrada e saída na rede, e aplica regras para conexões individuais de rede. O Firewall também fornece proteção contra ataques de computadores remotos. A [Proteção contra ataques de rede \(IDS\)](#) analisa o conteúdo do tráfego de rede e protege contra ataques de rede. Qualquer tráfego que seja considerado perigoso será bloqueado. Componentes na seção [Web e email](#) são responsáveis pela sua proteção ao navegar na Internet e pela comunicação via email. O componente [Imagem de atualização](#) pode ser usado para atualizar outros computadores na sua rede. [Monitoramento e gerenciamento remoto \(RMM\)](#) é o processo de supervisionar e controlar sistemas de software usando um agente de instalação local que pode ser acessado por um provedor de serviço de gerenciamento.



7. A etapa final é confirmar a instalação clicando em **Instalar**.

Instalação de módulos mínimos

Para reduzir o tráfego da rede relacionado ao tamanho do instalador e economizar recursos, a ESET vem com um instalador de módulos mínimo. O instalador contém apenas módulos essenciais, e todos os outros módulos serão baixados durante a atualização de módulo inicial depois da ativação do produto. A principal vantagem é ter um instalador significativamente menor, e o ESET Endpoint Security faz download apenas dos módulos de aplicativo mais recentes quando você ativa o produto.

O instalador de módulo mínimo ainda contém os módulos a seguir:

- Carregadores
- Suporte ao módulo Anti-Stealth
- Módulo de comunicação Direct Cloud
- Módulo de suporte de tradução
- Módulo de configuração
- Módulo SSL

Depois da ativação do produto, você verá o status **Inicializando proteção** que vai informar sobre os recursos sendo inicializados.



No caso de um problema com o download dos módulos (p. ex. configurações de proxy, sem rede, etc.), será exibido um alerta de status do aplicativo **Atenção solicitada**. Na janela do programa principal, clique em **Atualizar > Verificar se há atualizações** para iniciar o processo de atualização novamente.

Depois de várias tentativas falhas, um status de aplicativo vermelho **Falha ao configurar proteção** será exibido.



Se os computadores cliente não possuem uma conexão à internet ou funcionam off-line e precisam de atualizações, use os métodos a seguir para fazer download dos arquivos de atualização dos servidores de atualização ESET:

- [Atualização através do mirror](#)
- [Uso da Ferramenta de imagem](#)



Se o processo de inicialização falhar e você ainda não conseguir fazer download dos módulos, faça o download dos instaladores MSI completos [aqui](#).

Instalação da linha de comando

Você pode instalar o ESET Endpoint Security localmente usando a linha de comando ou instalar remotamente usando uma tarefa de cliente do ESET PROTECT.

Parâmetros compatíveis

APPDIR=<path>

- Path - caminho de diretório válido
- Diretório de instalação de aplicativo.

APPDATADIR=<path>

- Path - caminho de diretório válido

- Dados do diretório de instalação de aplicativo.

MODULEDIR=<path>

- Path - caminho de diretório válido
- Diretório de instalação de módulo.

ADDLOCAL=<list>

- Instalação de componente - lista de recursos não obrigatórios a serem instalados localmente.
- Uso com os pacotes ESET .msi: `ees_nt64_ENU.msi /qn ADDLOCAL=<list>`
- Para obter mais informações sobre a propriedade **ADDLOCAL** veja <http://msdn.microsoft.com/en-us/library/aa367536%28v=vs.85%29.aspx>

ADDEXCLUDE=<list>

- A lista ADDEXCLUDE é uma lista separada por vírgula de todos os nomes de recursos que não devem ser instalados, substituindo o REMOVE obsoleto.
- Ao selecionar um recurso que não deve ser instalado, todo o caminho (ou seja, todos os seus sub-recursos) e recursos invisíveis relacionados devem estar explicitamente incluídos na lista.
- Uso com os pacotes ESET .msi: `ees_nt64_enu.msi /qn ADDEXCLUDE=Firewall,Network`

i O **ADDEXCLUDE** não pode ser usado junto com o **ADDLOCAL**.

Consulte a [documentação](#) para a versão do **msiexec** usada para as opções de linha de comando apropriadas.

Regras

- A lista **ADDLOCAL** é uma lista separada por vírgula de todos os nomes de recursos a serem instalados.
- Ao selecionar um recurso a instalar, todo o caminho (todos os recursos pai) devem ser explicitamente incluídos na lista.
- Consulte regras adicionais para o uso correto.

Componentes e recursos

i A instalação de componentes usando os parâmetros ADDLOCAL/ADDEXCLUDE não funcionará com o ESET Endpoint Antivirus.

Os recursos são divididos em 4 categorias:

- **Obrigatório** – O recurso será sempre instalado.
- **Opcional** – O recurso poderá ser desmarcado para que não seja instalado.
- **Invisível** - recurso lógico obrigatório para que outros recursos funcionem adequadamente
- **Espaço reservado** - recurso sem efeito no produto, mas que deve ser listado com os sub-recursos

O conjunto de recursos do ESET Endpoint Security é o seguinte:

Descrição	Nome do recurso	Recurso pai	Presença
Componentes do programa base	Computer		Espaço reservado
Mecanismo de detecção	Antivirus	Computer	Obrigatório

Descrição	Nome do recurso	Recurso pai	Presença
Mecanismo de detecção/Escaneamento de malware	Scan	Computer	Obrigatório
Mecanismo de detecção/Proteção em tempo real do sistema de arquivos	RealtimeProtection	Computer	Obrigatório
Mecanismo de detecção/Escaneamento de malware/Proteção de documento	DocumentProtection	Antivirus	Opcional
Controle de dispositivo	DeviceControl	Computer	Opcional
Proteção de rede	Network		Espaço reservado
Proteção da rede/Firewall	Firewall	Network	Opcional
Proteção da rede/Proteção contra ataque de rede/...	IdsAndBotnetProtection	Network	Opcional
Navegador protegido	OnlinePaymentProtection	WebAndEmail	Opcional
Web e email	WebAndEmail		Espaço reservado
Web e email/Filtragem de protocolo	ProtocolFiltering	WebAndEmail	Invisível
Web e email / Proteção do acesso à Web	WebAccessProtection	WebAndEmail	Opcional
Web e email / Proteção do cliente de email	EmailClientProtection	WebAndEmail	Opcional
Web e email/Proteção do cliente de email/Cientes de email	MailPlugins	EmailClientProtection	Invisível
Web e email / Proteção do cliente de email / Proteção antispam	Antispam	EmailClientProtection	Opcional
Web e email / Controle da web	WebControl	WebAndEmail	Opcional
Ferramentas/ESET RMM	Rmm		Opcional
Atualização/Perfis/Imagem de atualização	UpdateMirror		Opcional
Plugin do ESET Inspect	EnterpriseInspector		Invisível

Conjunto de recursos de grupo:

Descrição	Nome do recurso	Presença de recurso
Todos os recursos obrigatórios	_Base	Invisível
Todos os recursos disponíveis	ALL	Invisível

Permissões adicionais

- Se qualquer um dos recursos do **WebAndEmail** for selecionado para a instalação, o recurso **ProtocolFiltering** invisível deverá ser incluído na lista.
- Os nomes de todos os recursos diferenciam maiúsculas e minúsculas, por exemplo, UpdateMirror não é igual a UPDITEMIRROR.

Lista de propriedades de configuração

Propriedade	Valor	Recurso
CFG_POTENTIALLYUNWANTED_ENABLED=	0 – Desativado 1 – Ativado	Detecção de PUA
CFG_LIVEGRID_ENABLED=	Veja abaixo	Veja a propriedade LiveGrid abaixo
FIRSTSCAN_ENABLE=	0 – Desativado 1 – Ativado	Agendar e executar um Escaneamento do computador depois da instalação
CFG_PROXY_ENABLED=	0 – Desativado 1 – Ativado	Configurações do servidor proxy
CFG_PROXY_ADDRESS=	<ip>	Endereço IP do servidor proxy
CFG_PROXY_PORT=	<port>	Número de porta do servidor proxy
CFG_PROXY_USERNAME=	<username>	Nome de usuário para autenticação
CFG_PROXY_PASSWORD=	<password>	Senha para autenticação
ACTIVATION_DATA=	Veja abaixo	Ativação do produto, chave de licença ou arquivo de licença off-line
ACTIVATION_DLG_SUPPRESS=	0 – Desativado 1 – Ativado	Quando definido como "1", não exibir o diálogo de ativação do produto depois da primeira inicialização
ADMINCFG=	<path>	Caminho para a configuração XML exportada (valor padrão <i>cfg.xml</i>)

Propriedades de configuração apenas no ESET Endpoint Security

CFG_EPFW_MODE=	0 – Automático (padrão) 1 – Interativo 2 – Baseado em política 3 – Aprendizado	Modo de filtragem de Firewall***
CFG_EPFW_LEARNINGMODE_ENDTIME=	<timestamp>	Data final do Modo de aprendizagem como carimbo de data/hora de Unix

Propriedade [LiveGrid®](#)

Ao instalar o ESET Endpoint Security com o CFG_LIVEGRID_ENABLED, o comportamento do produto depois da instalação será:

Recurso	CFG_LIVEGRID_ENABLED=0	CFG_LIVEGRID_ENABLED=1
Sistema de reputação do ESET LiveGrid®	Ativar	Ativar
Sistema de feedback ESET LiveGrid®	Desativar	Ativar
Enviar estatísticas anônimas	Desativar	Ativar

Propriedade ACTIVATION_DATA

Formato	Métodos
ACTIVATION_DATA=key : AAAA - BBBB - CCCC - DDDD - EEEE	Ativação usando a Chave de licença ESET (é preciso ter uma conexão com a Internet ativa)

Formato	Métodos
ACTIVATION_DATA=offline:C:\ProgramData\ESET\ESET Security\license.lf	Ativação usando um arquivo de licença off-line

Propriedades de idioma

Idioma ESET Endpoint Security (é preciso especificar as duas propriedades).

Propriedade	Valor
PRODUCT_LANG=	LCID decimal (ID de local), por exemplo, 1033 para inglês (Estados Unidos), veja a lista de códigos de idioma .
PRODUCT_LANG_CODE=	String LCID (nome de idioma da cultura) em minúsculas, por exemplo, en-us para inglês dos Estados Unidos, veja a lista de códigos de idioma .

Reiniciar propriedades

Especifique os seguintes parâmetros para reiniciar o computador depois da instalação:

Propriedade	Valor	Recurso
REBOOT_WHEN_NEEDED=	0 – Desativado 1 – Ativado	Se estiver ativado, o computador será reiniciado depois da instalação.
REBOOT_CANCELABLE=	0 – Desativado 1 – Ativado	Se estiver ativado, o usuário poderá cancelar a reinicialização do computador.
REBOOT_POSTPONE=	valor em segundos	Quantidade máxima de tempo em segundos para o usuário adiar a reinicialização do computador.

i REBOOT_CANCELABLE e REBOOT_POSTPONE estão disponíveis apenas se REBOOT_WHEN_NEEDED estiver ativado.

Exemplos de instalação de linha de comando

! Certifique-se de ter lido o [Acordo de licença do usuário final](#) e de ter privilégios administrativos antes de executar a instalação.

✓ Exclua a seção **NetworkProtection** da instalação (você também deve especificar todos os recursos filho):
`msiexec /qn /i ees_nt64.msi ADDEXCLUDE=Network,Firewall,IdsAndBotnetProtection`

✓ Se quiser que o seu ESET Endpoint Security seja configurado automaticamente depois da instalação, você pode especificar os parâmetros de configuração básicos dentro do comando de instalação.
 Instalar o ESET Endpoint Security com o ESET LiveGrid® ativado:
`msiexec /qn /i ees_nt64.msi CFG_LIVEGRID_ENABLED=1`

✓ Instalar em um diretório de instalação de aplicativo diferente do [padrão](#).
`msiexec /qn /i ees_nt64_enu.msi APPDIR=C:\ESET\`

✓ Instalar e ativar o ESET Endpoint Security usando sua Chave de licença ESET.
`msiexec /qn /i ees_nt64_enu.msi ACTIVATION_DATA=key:AAAA-BBBB-CCCC-DDDD-EEEE`

✓ Instalação silenciosa com registro em relatório detalhado (útil para a solução de problemas), e RMM apenas com componentes obrigatórios:

```
msiexec /qn /i ees_nt64.msi /l*xv msi.log ADDLOCAL=_Base,Rmm
```

✓ Instalação completa silenciosa forçada com um [idioma específico](#).

```
msiexec /qn /i ees_nt64.msi ADDLOCAL=ALL PRODUCT_LANG=1033 PRODUCT_LANG_CODE=en-us
```

Opções de linha de comando pós-instalação

- [ESET CMD](#) – Importar um arquivo de configuração .xml ou ativar/desativar um recurso de segurança
- [Escaneador da linha de comando](#) – Execute um Escaneamento do computador da linha de comando

Instalação usando GPO ou SCCM

Além de [instalar o ESET Endpoint Security diretamente em uma estação de trabalho do cliente](#), você também pode instalar usando ferramentas de gerenciamento como o Objeto de política do grupo (GPO), Gerente de configuração do centro de software (SCCM), Symantec Altiris ou Puppet.

Gerenciado (recomendado)

Para computadores gerenciados, nós primeiro instalamos o Agente ESET Management, depois o ESET Endpoint Security via ESET PROTECT. O ESET PROTECT deve estar instalado na sua rede.

1. Faça o download do [instalador autônomo](#) para o Agente ESET Management.
2. [Preparar o script de instalação remota GPO/SCCM](#).
3. Instalar o Agente ESET Management usando o GPO ou o SCCM.
4. Certifique-se de que os [computadores clientes](#) foram adicionados ao ESET PROTECT.
5. [Instale e ative o ESET Endpoint Security aos seus computadores clientes](#).

Os artigos da Base de conhecimento da ESET a seguir podem estar disponíveis apenas em inglês:



- [Instale o ESET Management Agent via SCCM ou GPO](#)
- [Implantar o ESET Management Agent usando um Objeto de política de grupo \(GPO\)](#)

Não gerenciado

Para computadores não gerenciados, você pode instalar o ESET Endpoint Security diretamente nas estações de trabalho do cliente. Isso não é recomendado, pois você não conseguirá monitorar e implementar políticas para todos os seus produtos endpoint ESET nas estações de trabalho.

Por padrão, o ESET Endpoint Security não é ativado depois da instalação e, portanto, não é funcional.

Opção 1 (instalação de software)

1. [Faça o download do instalador .msi](#) para o ESET Endpoint Security.
2. Crie um pacote de transformação .mst do arquivo .msi (por exemplo, usando o editor Orca .msi) para incluir a propriedade de ativação do produto (consulte ACTIVATION_DATA em [Instalação da linha de comando](#)).

Exibir etapas para criar um .mst no Orca

1. Abrir Orca
2. Carregue o instalador .msi ao clicar em **File > Open**.
3. Clique em **Transform > New Transform**.
4. Clique em **Property** na seção **Tables** e depois clique no menu **Tables > Add row**.
5. Na janela **Add Row** digite ACTIVATION_DATA como **Property** e as informações de licença como **Value**.

The screenshot shows the Orca MSI editor window titled 'ees_nt32.msi (transformed by act.mst) - Orca'. The 'Tables' pane on the left has 'Property' selected. The main pane displays a table with three columns: 'Property', 'Value', and an empty third column. The first row is 'ACTIVATION_DATA' with the value 'key:AAAA-BBBB-CCCC-DDDD-EEEE'. Below it are various other properties like 'ACTIVATION_DLG_SUPPRESS', 'ALLUSERS', 'ARPNOREPAIR', etc.

Property	Value
ACTIVATION_DATA	key:AAAA-BBBB-CCCC-DDDD-EEEE
ACTIVATION_DLG_SUPPRESS	0
ALLUSERS	1
ARPNOREPAIR	1
ARPPRODUCTICON	Icon_Product
ApplicationCode	33686273
CHECK_NEW_VERSION	0
CLOUD_AGREE	1
CompatibleProductTypes	eav;eis;ess;essp;eea;ees;eavbe;essbe
DataDir	ESET\ESET Security\
DefaultUIFont	DlgStdFont
EPFW_PROXY_ENABLED	1
ERAProductCategory	1
EULATAG	4a25ec5f3fae5a774466f5f9991524b438c942bf
EULATAG_1026	4ff82b074b311d037fe051eadf6d42d2de00abf4
EULATAG_1028	205fb56b27259a729eced47de74a82ed6d80ba82
EULATAG_1029	014f233417984a324eadcab90b7ea46b2fc72414
EULATAG_1030	c75483d80bdc8381984918b8c0406fec55247fc
EULATAG_1031	3cf6614563807ce122021482475c01882de1d20a
EULATAG_1032	7f64744d3e9acfa7634af832b3f32bccd95c33d1
EULATAG_1033	e27bcea9073de912ce9e72c3176f1495410901f5
EULATAG_1035	b6a3cbdf825e409b2dd7c9dda3d5558db3492158
EULATAG_1036	3f953a8ff495167510d22df1b289c5a0f6faf3b2
EULATAG_1037	5cb62b1988ec4b5667a6c9a3067a3efca6421735
EULATAG_1038	df1b69e526fbd9c06fa10d79547b88b495ba4306
EULATAG_1040	cb63d6d62b38a9b50f3396cf1681b9eade12fa86
EULATAG_1041	01f931f203068d0a47d54f5ee9738c58ff82aff3
EULATAG_1042	44fde07b99660d4d28dafbb4d275693fd0a90b80

6. Clique em **Transformar > Gerar transformação** para salvar o arquivo .mst.

1. Opcional: para [importar](#) seu arquivo de configuração ESET Endpoint Security .xml personalizado (por exemplo, para ativar o RMM ou para configurar as configurações do servidor proxy), coloque o arquivo cfg.xml no mesmo local que o instalador .msi.
2. Instale o instalador .msi com o arquivo .mst remotamente usando um dos métodos a seguir: GPO (via instalação de software) ou SCCM.

Opção 2 (usando uma tarefa agendada)

1. [Faça o download do instalador .msi](#) para o ESET Endpoint Security.
2. Prepare um script de [Instalação da linha de comando](#) para incluir a propriedade de ativação do produto (consulte ACTIVATION_DATA).
3. Faça com que o instalador .msi e o script .cmd estejam acessíveis na rede para todas as estações de trabalho.
4. Opcional: para [importar](#) seu arquivo de configuração ESET Endpoint Security .xml personalizado (por exemplo, para ativar o RMM ou para configurar as configurações do servidor proxy), coloque o arquivo cfg.xml no mesmo local que o instalador .msi.
5. Aplique um script de instalação de linha de comando preparado usando o GPO ou o SCCM.
 - Para GPO, use as Preferências de política do grupo > Tarefas agendadas de política do grupo > Tarefa imediata

i Se não quiser usar o ESET PROTECT para gerenciar remotamente seus produtos endpoint ESET, o ESET Endpoint Security contém o plugin da ESET para o RMM, o que permite a você supervisionar e controlar sistemas de software usando um agente instalado localmente, que pode ser acessado por um prestador de serviços de gerenciamento.

- [Descubra mais informações](#)

Atualização para uma versão mais recente

Versões mais recentes do ESET Endpoint Security são lançadas para implementar aprimoramentos ou corrigir problemas que não podem ser resolvidos por meio de atualizações automáticas dos módulos de programa.

A atualização para uma versão mais recente pode ser feita de várias formas:

1. Automaticamente, usando o ESET PROTECT ou ESET PROTECT Cloud. O ESET Endpoint Security versão 9 não pode ser gerenciado pelo ESET Remote Administrator.
2. Automaticamente, [usando GPO ou SCCM](#).
3. Automaticamente, por meio de uma atualização do programa.
Como a atualização do programa é distribuída para todos os usuários e pode ter impacto em determinadas configurações do sistema, ela é lançada depois de um longo período de testes para garantir funcionalidade com todas as configurações de sistema possíveis. Se você precisar atualizar para uma versão mais recente imediatamente após ela ter sido lançada, use um dos métodos a seguir.
Certifique-se de ter ativado o **Modo de atualização** em **Configuração avançada (F5) > Atualizar > Perfis > Atualizações de produto**.
4. Manualmente, por meio de download e [instalação de uma versão mais recente](#) sobre a instalação anterior.

Cenários de atualização recomendados

Gerencio ou quero gerenciar meus produtos ESET remotamente

Se você gerenciar mais de 10 produtos ESET Endpoint, considere lidar com as atualizações usando o ESET PROTECT, ESET PROTECT Cloud.

Consulte a documentação a seguir:

- [ESET PROTECT | Atualizar o software ESET através de uma tarefa do cliente](#)
- [ESET PROTECT | Guia para empresas de pequeno e médio porte que gerenciam até 250 produtos ESET endpoint no Windows](#)
- [Introdução ao ESET PROTECT Cloud](#)

Atualização manual em uma estação de trabalho do cliente

Não instale a versão 9 sobre uma versão 4.x, similarmente, se você tiver um ESET Endpoint Security versão 5.x ou 6.x mais antiga/não funcional.

Se você está planejando lidar com atualizações manualmente em estações de trabalho de clientes individuais:

1. Verifique se o seu sistema operacional é [compatível](#) Windows Vista e Windows XP não é compatível com a versão.
2. Fazer download e [instalar uma versão mais recente](#) sobre a versão anterior.

Se quiser aumentar ao máximo as chances de uma atualização bem-sucedida para a [versão 9.x mais recente](#), atualize de uma das versões a seguir do ESET Endpoint Security:



- 5.0.2272.x
- 6.5.2132.x
- 7.3.2044.x

Caso contrário, desinstale seu ESET Endpoint Security primeiro. Para informações adicionais sobre a atualização do ESET Endpoint Security em uma estação de trabalho do cliente, leia o [artigo da Base de conhecimento ESET](#) a seguir.

Atualizações de segurança e estabilidade

A atualização do ESET Endpoint Security é uma parte essencial para manter a proteção completa contra códigos maliciosos. Cada nova versão do ESET Endpoint Security conta com vários aprimoramentos e soluções bugs. Recomendamos fortemente que você atualize periodicamente o ESET Endpoint Security para impedir vulnerabilidades e ameaças de segurança. O ESET Endpoint Security se encaixa em um estágio específico do ciclo de vida do produto como qualquer outro produto ESET.

Ler mais sobre:

[Política de Fim da vida útil \(Produtos empresariais\)](#)



[Atualizações de produto](#)

[Hotfixes de segurança e estabilidade](#)

Para informações adicionais sobre mudanças no ESET Endpoint Security, leia o [artigo da Base de conhecimento da ESET](#) a seguir.



Atualizações automáticas garantem a segurança e estabilidade máxima do seu produto. Não é possível desativar atualizações de segurança e estabilidade.

Problemas comuns de instalação

Se acontecer um problema durante a instalação, veja nossa lista de [erros e soluções comuns de instalação](#) para encontrar uma solução para seu problema.

Falha na ativação

Caso a ativação do ESET Endpoint Security não tenha sido bem-sucedida, os cenários possíveis mais comuns são:

- A Chave de licença já está em uso
- Chave de licença inválida. Erro no formulário de ativação do produto
- Informações adicionais necessárias para a ativação estão faltando ou são inválidas
- Erro na comunicação com o banco de dados de ativação. Tente ativar novamente em 15 minutos
- Sem conexão ou conexão desativada com os servidores de ativação ESET

Certifique-se de que você inseriu a Chave de licença ou adequada ou anexou uma Licença off-line e tente ativar novamente.

Se você não conseguir ativar, nosso pacote de boas-vindas apresentará a você as perguntas comuns, erros, problemas sobre a ativação e licenciamento (disponível em inglês e em vários outros idiomas).

- [Iniciar a solução de problemas de ativação do produto ESET](#)

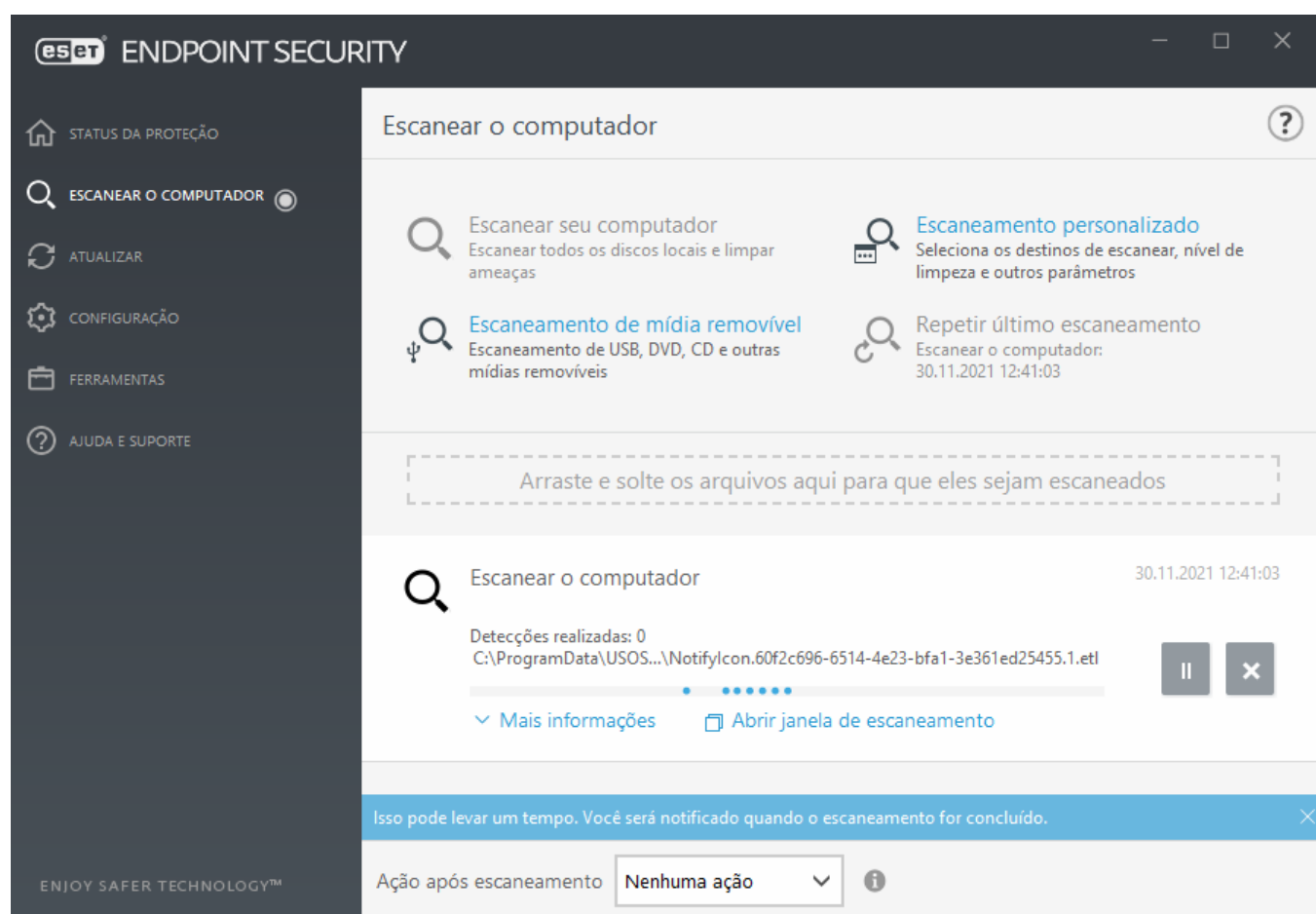
Ativação do produto

Após a conclusão da instalação, você será solicitado a ativar o produto.

Selecione um dos métodos disponíveis para ativar o ESET Endpoint Security. Para obter mais informações, consulte [Como ativar o ESET Endpoint Security](#).

Escanear o computador

Recomendamos que você realize rastreamentos regulares do computador ou [agende um rastreamento regular](#) para verificar se há ameaças. Na janela principal do programa, clique em **Escanear o computador** e, em seguida, clique em **Escanear seu computador**. Para obter mais informações sobre rastreamentos do computador, consulte [Rastrear o computador](#).



Guia do iniciante

Este capítulo fornece uma visão geral inicial do ESET Endpoint Security e de suas configurações básicas.

A interface do usuário

A janela principal do ESET Endpoint Security é dividida em duas seções principais. A primeira janela à direita exibe informações correspondentes à opção selecionada no menu principal à esquerda.

A seguir, há uma descrição das opções dentro do menu principal:

Status da proteção - Fornece informações sobre o status da proteção do ESET Endpoint Security.

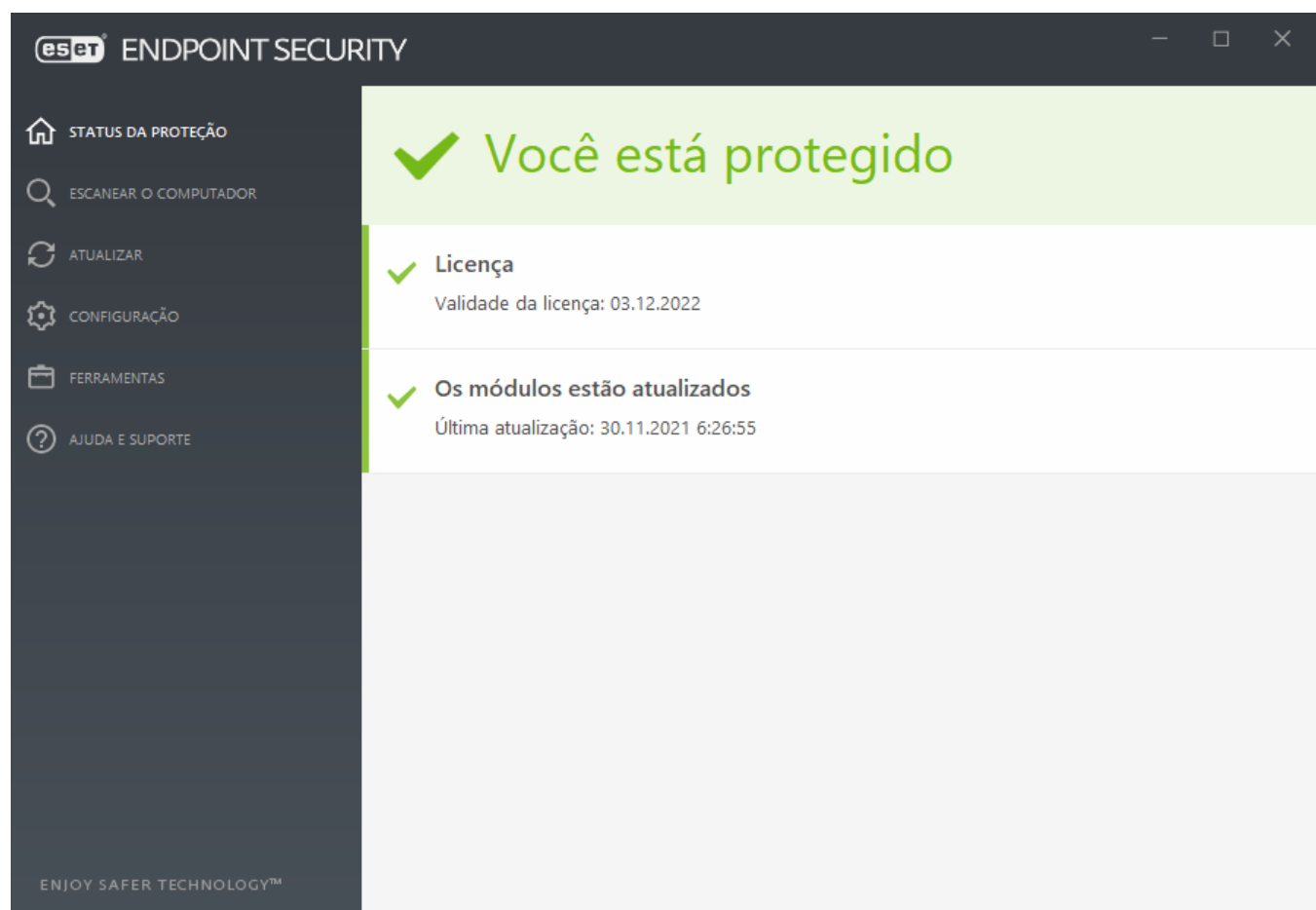
Escaneamento do computador – essa opção permite que você configure e inicie um escaneamento do seu computador, ou crie um escaneamento personalizado ou escaneamento de mídia removível. Você também pode repetir o último rastreamento que foi executado.

Atualizar – Exibe informações sobre o mecanismo de detecção e permite verificar manualmente a existência de atualizações.

Configuração - Selecione essa opção para ajustar configurações seu Computador, Rede ou Web e Email.

Ferramentas - Fornece acesso a Arquivos de relatório, Estatísticas de proteção, Monitorar atividade, Processos em execução, Agenda, Quarentena, conexões de rede, ESET SysInspector e ESET SysRescue para criar um CD de restauração. Você também pode enviar uma amostra para análise.

Ajuda e suporte – Fornece acesso a arquivos de ajuda, [base de conhecimento da ESET](#) e ao site da empresa ESET. Além disso, estão disponíveis links para abrir uma solicitação de suporte do Suporte técnico, ferramentas de suporte e informações sobre ativação do produto.

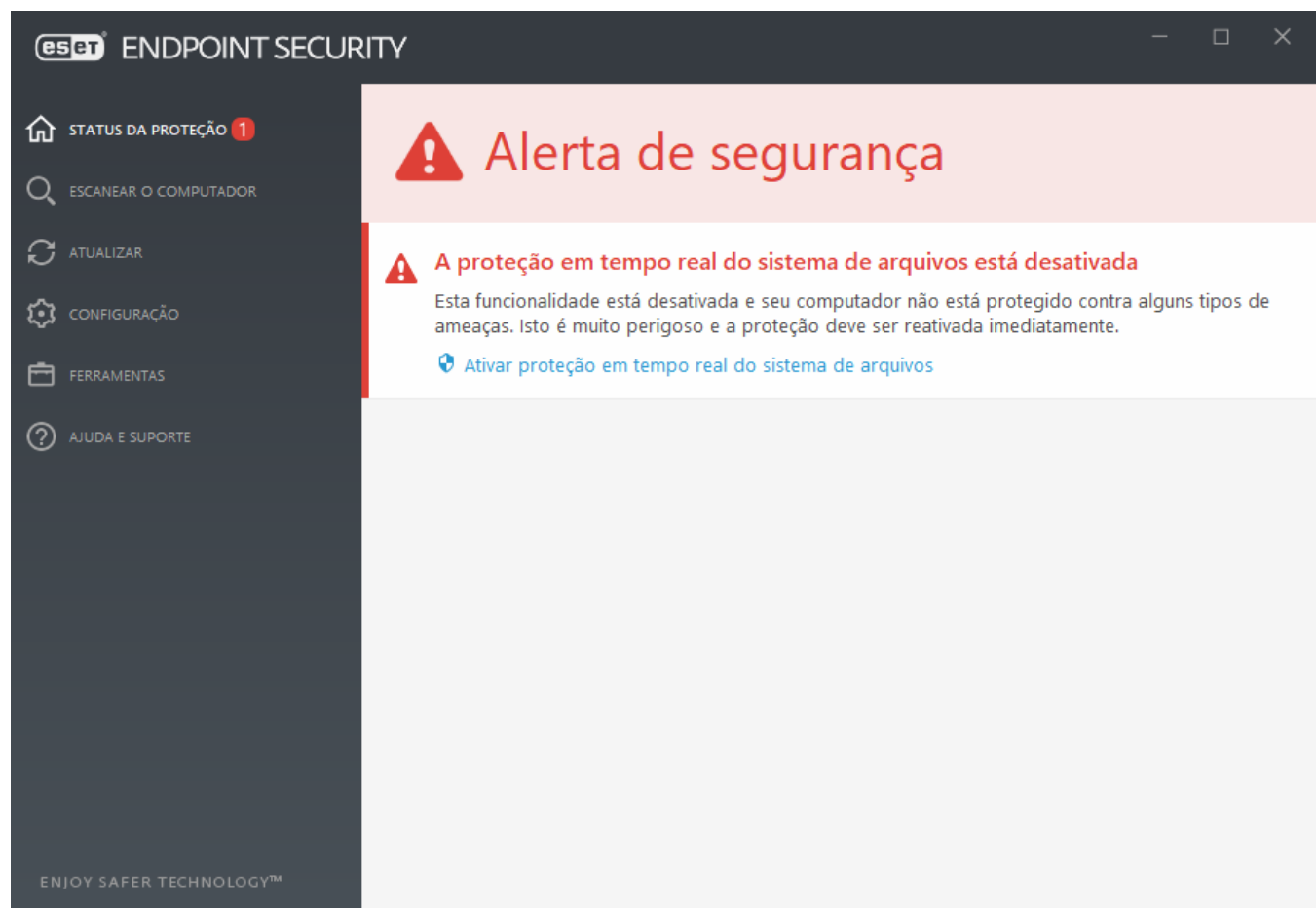


A tela **Status da proteção** informa sobre a segurança e o nível de proteção atual do seu computador. O ícone verde de status de **Proteção máxima** indica que a proteção máxima está garantida.

A janela de status também exibe os links rápidos para recursos mais usados do ESET Endpoint Security e informações sobre a última atualização.

O que fazer se o programa não funcionar adequadamente?

Uma marca de verificação verde será exibida ao lado dos módulos do programa que estão totalmente funcionais. Um ponto de exclamação vermelho ou um ícone de notificação laranja será exibido se um módulo precisar de atenção. Informações adicionais sobre o módulo, inclusive nossa recomendação sobre como restaurar a funcionalidade completa, serão mostradas na parte superior da janela. Para alterar o status de um módulo, clique em **Configuração** no menu principal e clique no módulo desejado.



O ícone do ponto de exclamação (!) vermelho indica que a proteção máxima do seu computador não está garantida. Você pode encontrar este tipo de notificação nos cenários a seguir:

- **Proteção antivírus e antispyware pausada** - Clique em **Iniciar todos os módulos de proteção de antivírus e antispyware** para reativar a proteção antivírus e antispyware no painel **Status da proteção** ou **Ativar proteção antivírus e antispyware** no painel **Configuração** da janela principal do programa.
- A proteção antivírus não está funcional - A inicialização do rastreador de vírus falhou. A maioria dos módulos ESET Endpoint Security não funcionará corretamente.
- **A Proteção antiphishing não está funcional** - Esta funcionalidade não está funcionando porque outros módulos de programa necessários não estão ativos.
- **O firewall da ESET está desativado** - Esse problema é indicado por um ícone vermelho e uma notificação de segurança próxima ao item **Rede**. Clique em **Ativar modo de filtragem** para reativar a proteção de rede.
- **Falha na inicialização do firewall** - O firewall está desativado por conta de problemas na integração do sistema. Reinicie seu computador o mais breve possível.
- **O mecanismo de detecção está desatualizado** - Esse erro aparecerá depois de diversas tentativas malsucedidas de atualizar o mecanismo de detecção (anteriormente chamado de banco de dados de assinatura de vírus). Recomendamos que você verifique as configurações de atualização. A razão mais

comum para esse erro é a inserção de [dados de autenticação](#) incorretos ou definições incorretas das [configurações de conexão](#).

- **Produto não ativado ou Licença expirada**– Isso é indicado pelo ícone do status da proteção que fica vermelho. O programa não pode ser atualizado após a licença expirar. Siga as instruções da janela de alerta para renovar sua licença.
- **O Sistema de prevenção de intrusos de host (HIPS) está desativado**- Este problema é indicado quando o HIPS é desativado na Configuração avançada. Seu computador não está protegido contra alguns tipos de ameaças e a proteção deve ser reativada imediatamente clicando em **Ativar HIPS**.
- **ESET LiveGrid® está desativado** - O problema é indicado quando o ESET LiveGrid® é desativado na Configuração avançada.
- **Sem atualizações regulares agendadas** - O ESET Endpoint Security não vai buscar ou receber atualizações importantes a menos que você agende uma tarefa de atualização.
- **Anti-Stealth está desativado** - Clique em **Ativar Anti-Stealth** para reativar esta funcionalidade.
- **Acesso de rede bloqueado** – Exibido quando a tarefa de cliente **Isolar computador da rede** da estação de trabalho do ESET PROTECT é acionada. Entre em contato com o administrador do sistema para mais informações.
- **A proteção do sistema de arquivos em tempo real está pausada** - A proteção em tempo real foi desativada pelo usuário. Seu computador não está protegido contra ameaças. Clicar em Ativar proteção em tempo real reativa essa funcionalidade.




O ícone laranja “!” indica que seu produto ESET requer atenção devido a um problema não crítico. As possíveis razões são:

- **Proteção do acesso à web desativada** - Clique na notificação de segurança para reativar a proteção do acesso à web ao clicar em **Ativar proteção do acesso à web**.
- **Sua licença expirará em breve** - Isso é indicado pelo ícone do status de proteção exibindo um ponto de exclamação. Depois que a licença expirar, o programa não poderá ser atualizado e o ícone do status da proteção ficará vermelho.
- **A Proteção botnet está pausada**- Clique em **Ativar proteção botnet** para ativar novamente este recurso.
- **Proteção de ataque a rede (IDS) pausada**- Clique em **Ativar proteção de ataque a rede (IDS)** para ativar novamente este recurso.
- **A Proteção antispam está pausada**- Clique em **Ativar proteção antispam** para ativar novamente este recurso.
- **O controle da Web está pausado**- Clique em **Ativar controle da web para ativar novamente este recurso**.
- **Substituição de política ativa** - A configuração definida pela política é substituída temporariamente, possivelmente até que a solução de problemas esteja concluída. Apenas um usuário autorizado pode substituir as configurações da política. Para mais informações consulte [Como usar o modo de Substituição](#).
- **O controle de dispositivos está pausado**- Clique em **Ativar controle de dispositivos** para ativar novamente este recurso.

Para ajustar a visibilidade de status do produto no primeiro painel do ESET Endpoint Security, consulte o [Status de aplicativo](#).

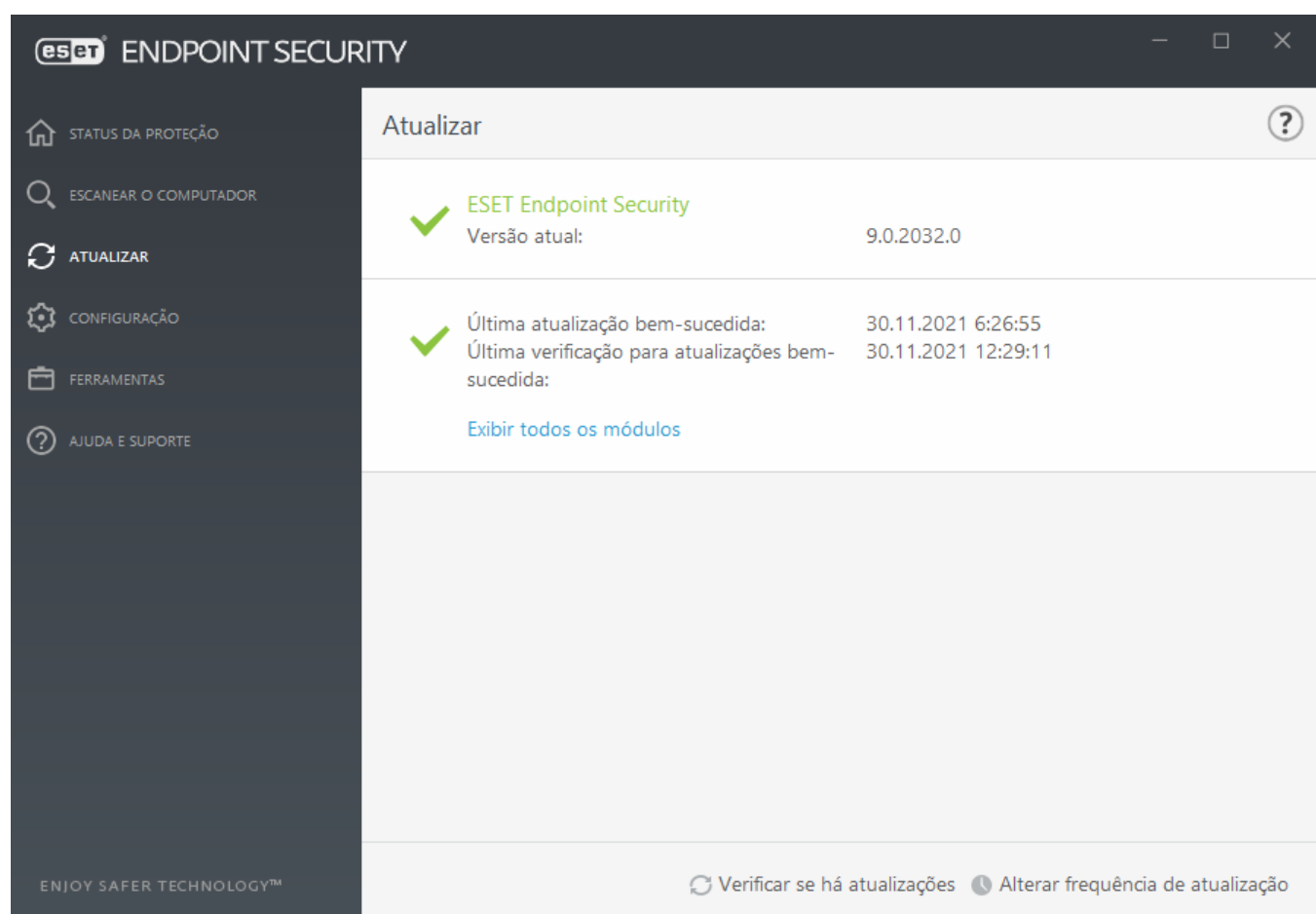
Se não for possível solucionar um problema com as soluções sugeridas, clique em **Ajuda e suporte** para acessar os arquivos de ajuda ou pesquisar na [Base de conhecimento da ESET](#). Se ainda precisar de ajuda, envie uma solicitação de Suporte técnico ESET. O Suporte Técnico da ESET responderá rapidamente às suas perguntas e ajudará você a encontrar uma solução.

 Se um status pertencem a um recurso que está bloqueado pela política ESET PROTECT, não será possível clicar no link.

Configuração da atualização

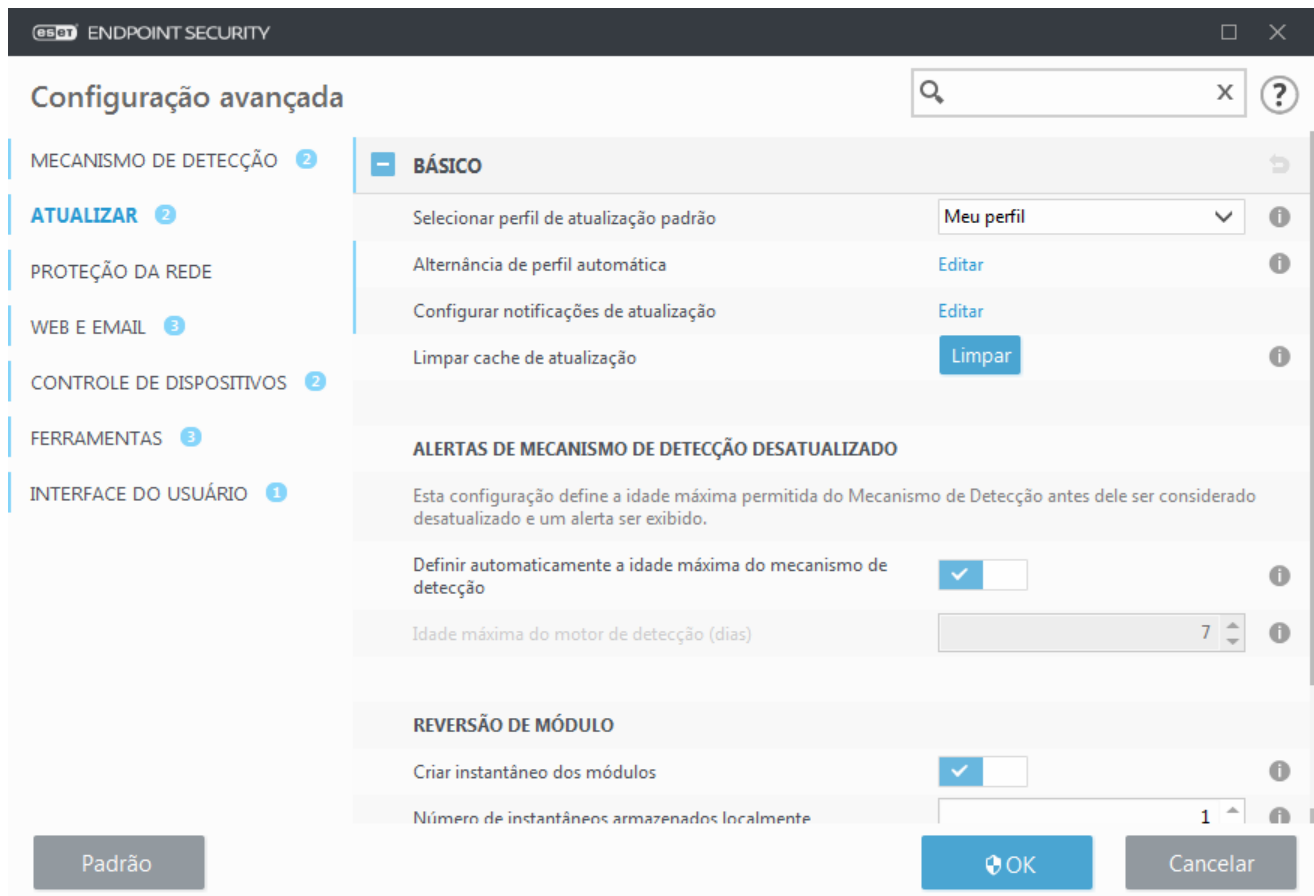
A atualização dos módulos é uma parte importante para manter a proteção completa contra códigos maliciosos. Preste bastante atenção na configuração de atualização e operação. No menu principal, selecione **Atualizar** > **Verificar se há atualizações** para verificar se há uma atualização de módulo mais recente.

Se a sua **Chave de licença** ainda não foi inserida, não será possível receber novas atualizações e você será solicitado a ativar seu produto.



A janela Configuração avançada (no menu principal, clique em **Configuração** > **Configuração avançada** ou pressione **F5** no teclado) contém opções de atualização adicionais. Para configurar opções avançadas de atualização como o modo de atualização, acesso ao servidor proxy, conexões de rede e configurações de criação de cópia do mecanismo de detecção, clique em **Atualizar** na árvore de Configuração avançada.

- Se você estiver tendo problemas com uma atualização, clique em **Limpar** para limpar o cache de atualização temporário.



- A opção **Escolher automaticamente** em **Perfis > Atualizações > Atualizações de módulos** está ativada por padrão. Ao usar um servidor de atualização ESET para receber atualizações, recomendamos que isso seja mantido assim.
- Se você não quiser que a notificação de atualização bem-sucedida da bandeja do sistema no canto inferior direito da tela apareça, abra **Perfis > Atualizações**, clique em **Editar** ao lado de **Selecionar as notificações de atualização recebidas** e ajuste as caixas de marcação para a notificação **Mecanismo de detecção atualizado com sucesso**.

Para obter a funcionalidade ideal, é importante que o programa seja atualizado automaticamente. Essa ação somente será possível se a **Chave de licença** correta for inserida em **Ajuda e suporte > Ativar produto**.

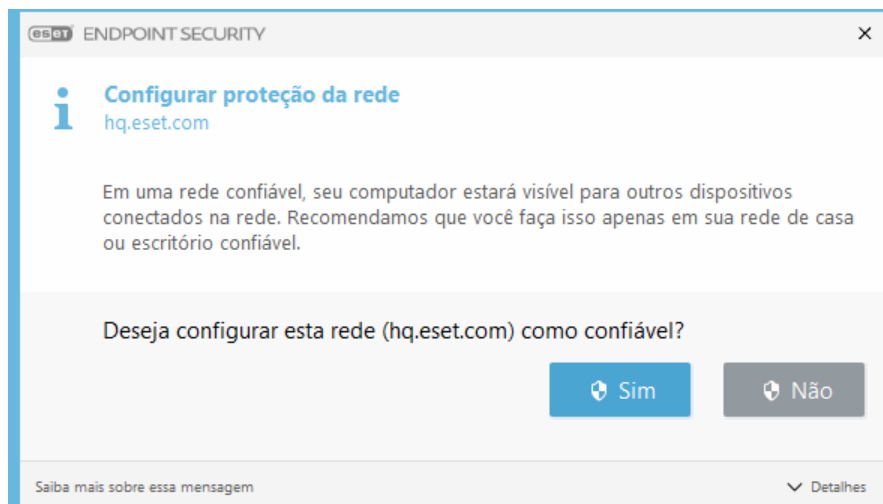
Se você não inseriu sua **chave de licença** após a instalação, poderá inseri-la a qualquer momento. Para obter informações mais detalhadas sobre a ativação, consulte [Como ativar o ESET Endpoint Security](#) e insira as credenciais recebidas com o produto de segurança ESET na janela **Detalhes da licença**.

Configuração de zonas

É necessário configurar zonas confiáveis para proteger o computador em um ambiente de rede. É possível permitir que outros usuários acessem o seu computador configurando a Zona confiável e permitindo o compartilhamento. Clique em **Configuração avançada (F5) > Proteção da rede > Firewall > Avançado > Zonas** para acessar as configurações de Zonas confiáveis.

A detecção de zona confiável ocorre após a instalação do ESET Endpoint Security e sempre que o seu computador se conectar a uma nova rede. Portanto, normalmente não há necessidade de definir Zonas confiáveis. Por padrão, há uma janela da caixa de diálogo exibida na detecção de uma nova zona que permite configurar o nível de

proteção dessa zona.



Uma configuração incorreta da zona confiável pode representar um risco de segurança para o seu computador.



Por padrão, as estações de trabalho de uma Zona confiável têm acesso garantido a arquivos e impressoras compartilhados, a comunicação RPC de entrada é ativada e o compartilhamento da área de trabalho remota é disponibilizado.

Para mais detalhes sobre este recurso, leia o seguinte artigo na Base de conhecimento ESET:

- [Nova conexão de rede detectada ESET Endpoint Security](#)

Ferramentas de controle de web

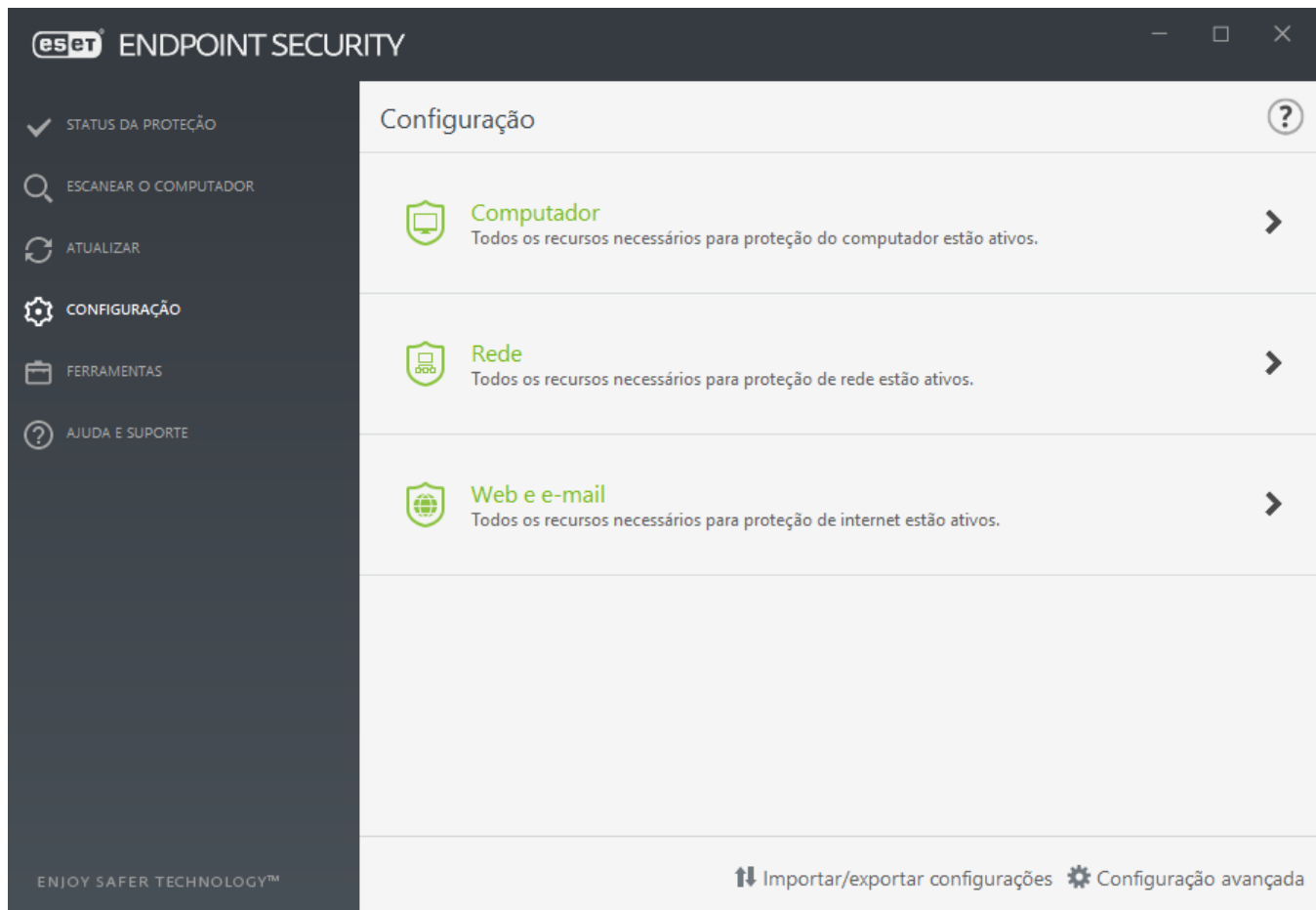
Se você já tiver ativado o Controle de web no ESET Endpoint Security, também deverá configurar o Controle de web para contas de usuário desejadas, a fim de que o Controle de web funcione devidamente. Consulte o capítulo [Controle de web](#) para obter instruções sobre como criar restrições específicas para suas estações de trabalho clientes, a fim de protegê-los de material potencialmente ofensivo.

Trabalhar com o ESET Endpoint Security

As opções de configuração do ESET Endpoint Security permitem ajustar o nível de proteção do computador, email e rede.



Ao criar uma política a partir do Console da Web ESET PROTECT você pode selecionar o sinalizador para cada configuração. 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 (por exemplo pelo usuário ou por políticas posteriores durante a mesclagem). Para obter mais informações consulte [Sinalizadores na Ajuda on-line ESET PROTECT](#).



O menu **Configurar** contém as seguintes seções:

- **Computador**
- **Rede**
- **Web e email**

A seção Computador permite a você ativar ou desativar os seguintes componentes:


- **Proteção em tempo real do sistema de arquivos** – Todos os arquivos são escaneados quanto a código malicioso no momento em que são abertos, criados ou executados.
- **Controle de dispositivos** – Fornece [controle](#) automático de dispositivos (CD/DVD/USB/...). Esse módulo permite bloquear ou ajustar filtros/permissões estendidos e define a capacidade de um usuário de acessar e trabalhar com um determinado dispositivo.
- **Host Intrusion Prevention System (HIPS)** - O sistema [HIPS](#) monitora os eventos que ocorrem dentro do sistema operacional e reage a eles de acordo com um conjunto de regras personalizado.
- **O Rastreamento de memória avançado** - funciona combinado com o Bloqueio de exploit para fortalecer a proteção contra malware feito para evitar a detecção por produtos antimalware através do uso de ofuscação ou criptografia. Por padrão, o scanner de memória avançado está ativado. Leia mais sobre esse tipo de proteção no [glossário](#).
- **Bloqueio de exploit** – feito para fortalecer tipos de aplicativos comumente explorados como navegadores da web, leitores de PDF, clientes de email e componentes do MS Office. Por padrão, o bloqueio de exploit está ativado. Leia mais sobre esse tipo de proteção no [glossário](#).
- **A Escudo Anti-ransomware** é outra camada de proteção que funciona como uma parte do recurso HIPS. Você deve ter o sistema de reputação ESET LiveGrid® ativado para a Proteção contra ransomware funcionar. [Leia mais sobre este tipo de proteção](#).


- **Modo de apresentação** - Um recurso para usuários que pretendem usar o seu software continuamente sem serem perturbados por janelas pop-up e que ainda pretendem reduzir o uso da CPU. Você receberá uma mensagem de aviso (risco potencial de segurança) e a janela do programa principal será exibida em laranja após a ativação do [Modo de apresentação](#).


A seção **Rede** permite a você configurar o [Firewall](#), Proteção contra ataque de rede (IDS) e [Proteção contra botnet](#).


A configuração da proteção de **Web e email** permite ativar ou desativar os seguintes componentes:


- **Navegador protegido** - Protege seus dados sensíveis ao navegar on-line (por exemplo, dados financeiros durante transações on-line).
- **Controle da Web** - Bloqueia páginas da Web que possam conter material potencialmente ofensivo. Além disso, os administradores do sistema podem especificar preferências de acesso para 27 categorias de sites predefinidas.
- **Proteção do acesso à Web** – Se ativada, todo o tráfego através de HTTP ou HTTPS será rastreado quanto a software malicioso.
- **Proteção do cliente de email** - Monitora a comunicação recebida através do protocolo POP3 e IMAP.
- **Proteção antispam** - Rastreia spam ou emails não solicitados.
- **Proteção antiphishing** - Protege você contra tentativas de adquirir senhas e outras informações confidenciais por sites ilegítimos disfarçados como sites legítimos.

Para desativar os módulos individuais temporariamente, clique na opção verde  ao lado do módulo desejado. Observe que essa ação pode diminuir o nível de proteção do seu computador.

Para reativar a proteção do componente de segurança desativado, clique na opção vermelha  para retornar um componente a seu estado ativado.

Quando a política ESET PROTECT é aplicada, você verá o ícone de cadeado  ao lado de um componente específico. A política aplicada ao ESET PROTECT pode ser substituída localmente depois da autenticação pelo usuário que fez login (por exemplo administrador). Para mais informações consulte a Ajuda on-line [ESET PROTECT](#).

 Todas as medidas protetivas desativadas dessa forma serão reativadas depois de uma reinicialização do computador.


Para acessar configurações detalhadas de um componente de segurança específico, clique no ícone de engrenagem  ao lado de qualquer componente.

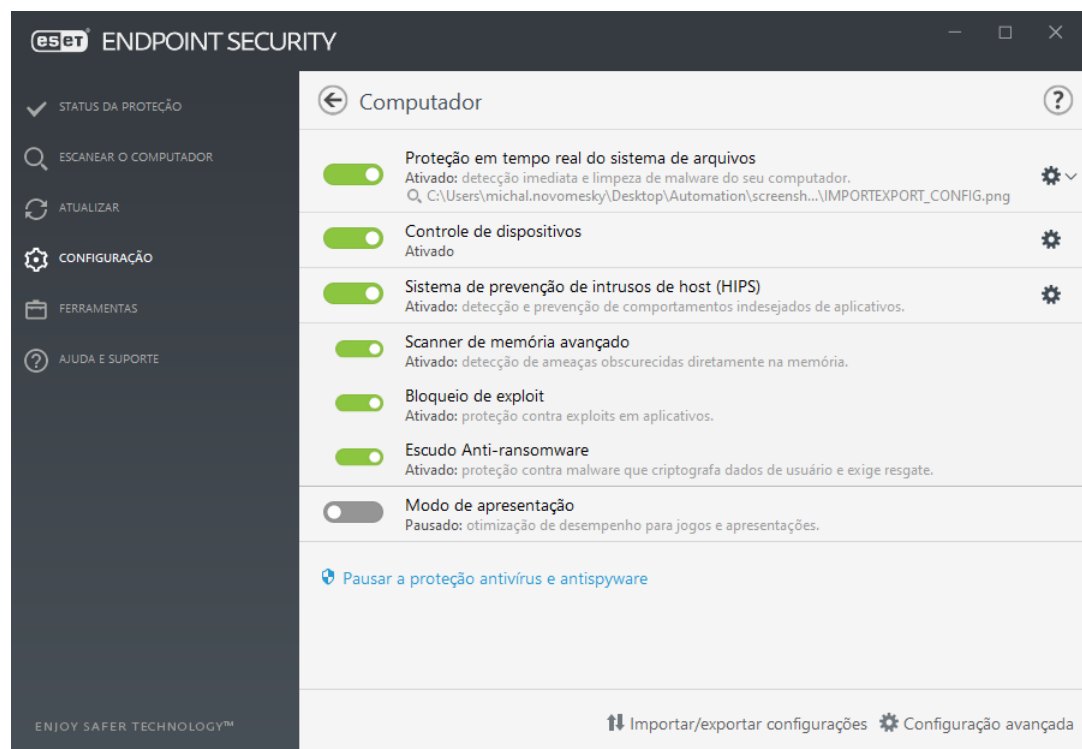
Existem opções adicionais na parte inferior da janela de configuração. Para carregar os parâmetros de configuração utilizando um arquivo de configuração *.xml* ou salvar os parâmetros atuais em um arquivo de configuração, use a opção **Importar e exportar configurações**. Para obter informações mais detalhadas, consulte [Importar/Exportar configurações](#).

Para opções com mais detalhes, clique em **Configuração avançada** ou pressione **F5**.

Computador

O módulo **Computador** pode ser encontrado em **Configuração > Computador**. Ele exibe uma visão geral dos módulos de proteção descritos no [capítulo anterior](#). Nesta seção, as seguintes configurações estão disponíveis:

Clique na engrenagem  ao lado de **Proteção em tempo real do sistema de arquivos** e clique em **Editar exclusões** para abrir a [janela de configuração de exclusão](#), que permite a exclusão de arquivos e pastas do escaneamento. Para abrir a configuração avançada da **Proteção em tempo real do sistema de arquivos**, clique em **Configurar**.



A seção **Computador** permite a você ativar ou desativar os seguintes componentes:

- **Proteção em tempo real do sistema de arquivos** - Todos os arquivos são verificados quanto a código malicioso no momento em que são abertos, criados ou executados no computador.
- **Controle de dispositivos** – Fornece [controle](#) automático de dispositivos (CD/DVD/USB/...). Esse módulo permite bloquear ou ajustar filtros/permissões estendidos e define a capacidade de um usuário de acessar e trabalhar com um determinado dispositivo.
- **Host Intrusion Prevention System (HIPS)** - O sistema [HIPS](#) monitora os eventos que ocorrem dentro do sistema operacional e reage a eles de acordo com um conjunto de regras personalizado.
- **O Rastreamento de memória avançado** - funciona combinado com o Bloqueio de exploit para fortalecer a proteção contra malware feito para evitar a detecção por produtos antimalware através do uso de ofuscação ou criptografia. Por padrão, o scanner de memória avançado está ativado. Leia mais sobre esse tipo de proteção no [glossário](#).
- **Bloqueio de exploit** – feito para fortalecer tipos de aplicativos comumente explorados como navegadores da web, leitores de PDF, clientes de email e componentes do MS Office. Por padrão, o bloqueio de exploit está ativado. Leia mais sobre esse tipo de proteção no [glossário](#).
- **A Escudo Anti-ransomware** é outra camada de proteção que funciona como uma parte do recurso HIPS. Você deve ter o sistema de reputação ESET LiveGrid® ativado para a Proteção contra ransomware funcionar. [Leia mais sobre este tipo de proteção](#).
- **Modo de apresentação** - Um recurso para usuários que pretendem usar o seu software continuamente sem serem perturbados por janelas pop-up e que ainda pretendem reduzir o uso da CPU. Você receberá uma mensagem de aviso (risco potencial de segurança) e a janela do programa principal será exibida em laranja após a ativação do [Modo de apresentação](#).

Pausar a Proteção antivírus e antispyware - A qualquer momento que você desativar temporariamente a Proteção antivírus e antispyware, você poderá selecionar o período de tempo para o qual deseja que o

componente selecionado seja desativado usando o menu suspenso e então clicar em **Aplicar** para desativar o componente de segurança. Para reativar a proteção, clique em **Ativar proteção antivírus e antispyware**.

Mecanismo de detecção

O mecanismo de detecção protege contra ataques maliciosos ao sistema controlando a comunicação de arquivos, e-mail e internet. Por exemplo, se um objeto classificado como malware for detectado, a correção será iniciada. O mecanismo de detecção pode eliminá-lo, primeiro bloqueando-o e, em seguida, limpando, removendo ou movendo-o para a quarentena.

Para definir as configurações do mecanismo de detecção em detalhes, clique em **Configuração avançada** ou pressione **F5**.

Nesta seção:

- [Categorias de Proteção em tempo real e Machine learning](#)
- [Escaneamento de malware](#)
- [Configuração de relatórios](#)
- [Configuração de proteção](#)
- [Melhores práticas](#)

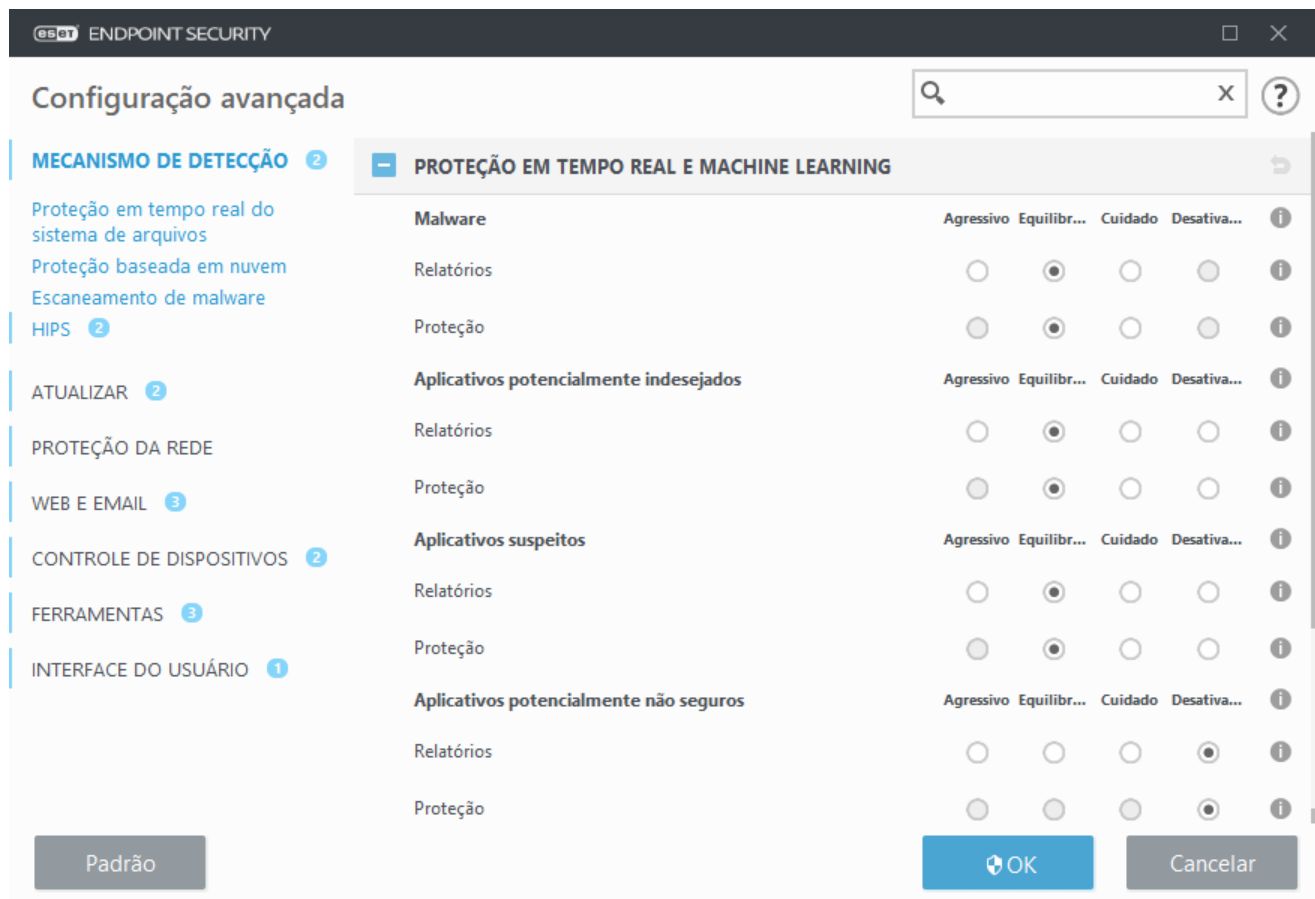
i A partir da versão 7.2, a seção do Mecanismo de detecção não oferece mais os botões Ligado/Desligado [como na versão 7.1 e versões anteriores](#). Os botões Ligado/Desligado foram substituídos por quatro limites: Agressivo, Equilibrado, Cuidadoso e Desligado.

Categorias de Proteção em tempo real e Machine learning

A **Proteção em tempo real e Machine Learning** para todos os módulos de proteção (por exemplo, Proteção em tempo real do sistema de arquivos, Proteção de acesso à web, ...) permite a você configurar os níveis de relatórios e proteção das categorias a seguir:

- **Malware** – Um vírus de computador é um pedaço de código malicioso que é anexado a arquivos existentes no seu computador. Porém, o termo "vírus" é frequentemente mal usado. "Malware" (software malicioso) é um termo mais preciso. A detecção de malware é realizada pelo módulo do mecanismo de detecção combinado com o componente de Machine learning.
Leia mais sobre esses tipos de aplicativos no [Glossário](#).
- **Aplicativo potencialmente indesejado** – Grayware ou Aplicativo potencialmente indesejado (PUA) é uma categoria ampla de software, cujo objetivo não é tão claramente nocivo quanto outros tipos de malware, como vírus ou trojans. Porém ele pode instalar software indesejado adicional, alterar o comportamento do dispositivo digital ou realizar atividades não aprovadas ou esperadas pelo usuário.
Leia mais sobre esses tipos de aplicativos no [Glossário](#).
- **Aplicativos potencialmente não seguros** – Refere-se a software comercial legítimo que tenha o potencial de ser usado indevidamente para fins maliciosos. Exemplos de aplicativos potencialmente inseguros (PUAs) incluem ferramentas de acesso remoto, aplicativos que descobrem senhas e registradores de teclado (programas que gravam cada pressão de tecla feita por um usuário).
Leia mais sobre esses tipos de aplicativos no [Glossário](#).

- **Aplicativos suspeitos** incluem programas compactados com [empacotadores](#) ou protetores. Esses tipos de protetores muitas vezes são explorados por autores de malware para evitar a detecção.



O Machine learning avançado agora faz parte do mecanismo de detecção como uma camada avançada de proteção que melhora a detecção baseada em machine learning. Leia mais sobre esse tipo de proteção no [Glossário](#).

Escaneamento de malware

As configurações do escaneador podem ser configuradas separadamente para o escaneador em tempo real e o [escaneador sob demanda](#). Por padrão, **Usar configurações de proteção em tempo real** está ativado. Quando ativadas, as configurações relevantes de Escaneamento sob demanda são herdadas da seção **Proteção em tempo real e Machine learning**.

Configuração de relatórios

Quando ocorre uma detecção (por exemplo, uma ameaça é encontrada e classificada como malware), informações são registradas no [Relatório de detecções](#) e [Notificações na área de trabalho](#) ocorrem se estiverem configuradas o ESET Endpoint Security.

O limite de relatório é configurado para cada categoria (chamado de "CATEGORIA"):

1. Malware
2. Aplicativos potencialmente indesejados
3. Potencialmente inseguro
4. Aplicativos suspeitos

Relatórios realizados com o mecanismo de detecção, inclusive o componente de machine learning. É possível definir um limite de relatório maior do que o limite de [proteção](#) atual. Essas configurações de relatório não influenciam o bloqueio, [limpeza](#) ou exclusão de [objetos](#).

Leia o seguinte antes de modificar um limite (ou nível) para um relatório de CATEGORIA:

Limite	Explicação
Agressivo	Relatório de CATEGORIA configurado para sensibilidade máxima. Mais detecções serão reportadas. A configuração Agressiva pode identificar erroneamente os objetos como CATEGORIA.
Equilibrado	Relatório de CATEGORIA configurado como equilibrado. Essa configuração está otimizada para equilibrar o desempenho e precisão das taxas de detecção, e o número de objetos erroneamente reportados.
Cuidadoso	Relatório de CATEGORIA configurado para minimizar objetos identificados erroneamente enquanto mantém um nível suficiente de proteção. Os objetos são reportados apenas quando a probabilidade é evidente e quando correspondem ao comportamento de CATEGORIA.
Desativar	O relatório de CATEGORIA não está ativo e as detecções deste tipo não serão encontradas, reportadas ou limpas. Como resultado, esta configuração desativará a proteção deste tipo de detecção. A opção Desativado não está disponível para relatórios de malware e é o valor padrão para aplicativos potencialmente não seguros.

[Disponibilidade de módulos de proteção ESET Endpoint Security](#)

A disponibilidade (ativado ou desativado) de um módulo de proteção para um limite de CATEGORIA selecionado é a seguinte:

	Agressivo	Equilibrado	Cuidadoso	Desligado**
Módulo de machine learning avançado*	✓ (modo agressivo)	✓ (modo conservador)	X	X
Módulo do mecanismo de detecção	✓	✓	✓	X
Outros módulos de proteção	✓	✓	✓	X

* Disponível no ESET Endpoint Security da versão 7.2 e versões posteriores.

** Não recomendado

[Determinar a versão do produto, versões do módulo de programa e datas de compilação](#)

1. Clique em **Ajuda e suporte > Sobre o ESET Endpoint Security**.
2. Na tela **Sobre**, a primeira linha de texto exibe o número de versão do seu produto ESET.
3. Clique em **Exibir módulos** para acessar informações sobre módulos específicos.

Informações essenciais

Algumas informações essenciais ao configurar um limite adequado para seu ambiente:

- O limite **Equilibrado** é recomendado para a maioria das configurações.
- O limite **Cuidadoso** representa um nível de proteção comparável com as versões anteriores do ESET

Endpoint Security (7.1 e versões anteriores). Ele é recomendado para ambientes onde a prioridade está em minimizar a identificação errônea de objetos pelo software de segurança.

- Quanto maior o limite de relatórios maior a taxa de detecção, mas também maior a chance de objetos serem identificados erroneamente.
- Partindo da perspectiva do mundo real, não há garantia de uma taxa de detecção de 100% nem uma chance de 0% de evitar a categorização incorreta de objetos limpos como malware.
- [Mantenha o ESET Endpoint Security e seus módulos atualizados](#) para maximizar o equilíbrio entre desempenho e precisão das taxas de detecção e o número de objetos reportados erroneamente.

Configuração de proteção

Se um objeto classificado como CATEGORIA for reportado, o programa bloqueia o objeto e depois [limpa](#), remove ou move o objeto para a [Quarentena](#).

Leia o seguinte antes de modificar um limite (ou nível) para a proteção CATEGORIA:

Limite	Explicação
Agressivo	As detecções de nível agressivo (ou inferior) relatadas são bloqueadas, e a correção automática (ou seja, limpeza) é iniciada. Essa configuração é recomendada quando todos os endpoints tiverem sido escaneados com configurações agressivas e objetos erroneamente reportados tiverem sido adicionados às exclusões de detecção.
Equilibrado	As detecções de nível equilibrado (ou inferior) relatadas são bloqueadas e a correção automática (ou seja, limpeza) é iniciada.
Cuidadoso	As detecções reportadas de nível de cuidado são bloqueadas e a correção automática (ou seja, limpeza) é iniciada.
Desativar	Útil para identificar e excluir objetos erroneamente reportados. A opção Desativado não está disponível para proteção contra malware e é o valor padrão para aplicativos potencialmente não seguros.

[Tabela de conversão de política ESET PROTECT para o ESET Endpoint Security 7.1 e versões anteriores](#)

A partir do ESET PROTECT o editor de política das configurações de escaneamento não tem mais as opções Ligado/Desligado para cada CATEGORIA. A tabela a seguir delinea uma conversão entre o limite de proteção e o estado final da [opção no ESET Endpoint Security 7.1 e versões anteriores](#).

Estado de limite da CATEGORIA	Agressivo	Equilibrado	Cuidadoso	Desativar
Opção de CATEGORIA aplicada	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>

Ao atualizar das versões 7.1 e versões anteriores para a versão 7.2 e versões posteriores, o novo estado do limite será o seguinte:

Opção de categoria antes da atualização	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Novo limite da CATEGORIA depois da atualização	Equilibrado	Desativar

Melhores práticas

NÃO GERENCIADO (estação de trabalho individual do cliente)

Mantém igual o valor recomendado padrão.

AMBIENTE GERENCIADO

Essas configurações geralmente são aplicadas às estações de trabalho por meio de uma [política](#).

1. Fase inicial

Essa fase pode levar até uma semana.

- Configure todos os limites de **Relatórios** como **Equilibrado**.
OBSERVAÇÃO: Se necessário, configure como **Agressivo**.
- Configure ou mantenha a **Proteção** contra malware como **Equilibrado**.
- Configure a **Proteção** para outras CATEGORIAS como **Cuidadoso**.
OBSERVAÇÃO: Não recomendamos configurar o limite de **Proteção** como **Agressivo** nesta fase, pois todas as detecções encontradas seriam corrigidas, inclusive as detecções identificadas erroneamente.
- Antes disso, identifique objetos identificados erroneamente do [Relatório de detecções](#) e adicione-os às [Exclusões de detecção](#).

2. Fase de transição

- Implemente a "Fase de produção" a algumas das estações de trabalho como um teste (não para todas as estações de trabalho da rede).

3. Fase de produção

- Configure todos os limites de **Proteção** como **Equilibrado**.
- Quando for feito o gerenciamento remoto, use uma [política pré-definida](#) de antivírus para o ESET Endpoint Security.
- O limite de proteção **Agressivo** pode ser configurado se as taxas de detecção mais altas forem necessárias e se os objetos identificados erroneamente forem aceitos.
- Confira o [Relatório de detecção](#) ou os relatórios do ESET PROTECT para possíveis detecções faltando.

Opções avançadas do mecanismo de detecção

A tecnologia **Anti-Stealth** é um sistema sofisticado que fornece a detecção de programas nocivos, como os [rootkits](#), que podem se auto-ocultar do sistema operacional. Isso significa que não é possível detectá-los usando técnicas comuns de testes.

Ativar rastreamento avançado via AMSI - A ferramenta Interface de Rastreando Microsoft Antimalware que dá aos desenvolvedores de aplicativos novas defesas contra malware (apenas Windows 10, 11).

Uma infiltração foi detectada

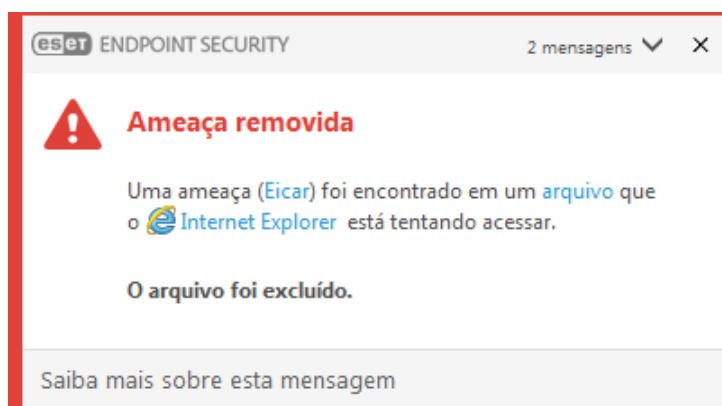
As ameaças podem alcançar o sistema a partir de vários pontos de entrada, tais como [páginas da web](#), pastas compartilhadas, via email ou [dispositivos removíveis](#) (USB, discos externos, CDs, DVDs, etc.).

Comportamento padrão

Como um exemplo geral de como as infiltrações são tratadas pelo ESET Endpoint Security, as infiltrações podem ser detectadas usando:

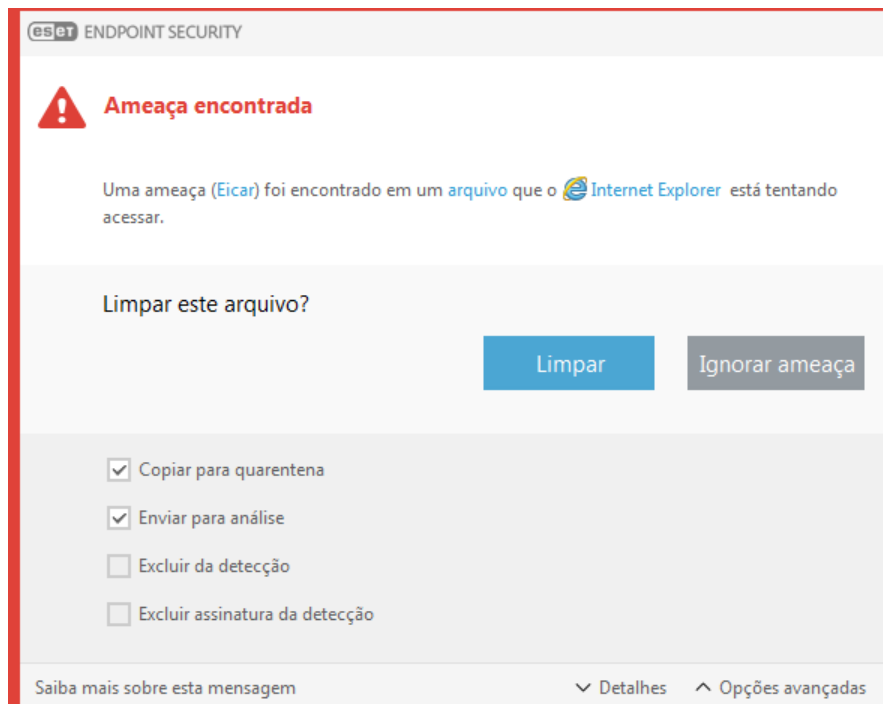
- [Proteção em tempo real do sistema de arquivos](#)
- [Proteção do acesso à Web](#)
- [Proteção do cliente de email](#)
- [Escaneamento sob demanda do computador](#)

Cada um usa o nível de limpeza padrão e tentará limpar o arquivo e movê-lo para a [Quarentena](#) ou encerrar a conexão. Uma janela de notificação é exibida na área de notificação, no canto inferior direito da tela. Para informações detalhadas sobre os objetos detectados/limpos, consulte os [Arquivos de relatório](#). Para obter mais informações sobre níveis de limpeza e de comportamento, consulte [Limpeza](#).



Limpeza e exclusão

Se não houver uma ação predefinida a ser adotada para a Proteção em tempo real do sistema de arquivos, você será solicitado a selecionar uma opção em uma janela de alerta. Geralmente as opções **Limpar**, **Excluir** e **Nenhuma ação** estão disponíveis. Não se recomenda selecionar **Nenhuma ação**, pois os arquivos infectados não serão limpos. A exceção a isso é quando você tem certeza de que um arquivo é inofensivo e foi detectado por engano.



Aplique a limpeza se um arquivo tiver sido atacado por um vírus que anexou um código malicioso a esse arquivo. Se esse for o caso, tente primeiro limpar o arquivo infectado a fim de restaurá-lo para o seu estado original. Se o arquivo for constituído exclusivamente por código malicioso, ele será excluído.

Se um arquivo infectado estiver "bloqueado" ou em uso por um processo do sistema, ele somente será excluído após ter sido liberado (normalmente após a reinicialização do sistema).

Restauração da Quarentena

A quarentena pode ser acessada da janela principal do programa do ESET Endpoint Security ao clicar em **Ferramentas > Quarentena**.

Os arquivos colocados em quarentena também podem ser restaurados para seu local original:

- Para isso, use o recurso **Restaurar**, que está disponível no menu de contexto clicando com o botão direito em um determinado arquivo na Quarentena.
- Se um arquivo for marcado como um [aplicativo potencialmente indesejado](#), a opção **Restaurar e excluir do escaneamento** é ativada. Veja também [Exclusões](#).
- O menu de contexto também oferece a opção **Restaurar para** que permite a você restaurar um arquivo para um local diferente daquele do qual ele foi removido.
- A funcionalidade de restauração não está disponível em alguns casos, por exemplo, para arquivos localizados em um compartilhamento de rede somente leitura.

Várias ameaças

Se quaisquer arquivos infectados não foram limpos durante um rastreamento de computador (ou o [nível de limpeza](#) estava configurado como **Sem limpeza**), será exibida uma janela de alerta solicitando a você que selecione a ação adequada para esses arquivos.

Exclusão de arquivos em arquivos compactados

No modo de limpeza Padrão, os arquivos compactados serão excluídos somente se contiverem arquivos infectados e nenhum arquivo limpo. Em outras palavras, os arquivos compactados não serão excluídos se eles contiverem também arquivos limpos inofensivos. Tenha cautela ao executar um rastreamento com Limpeza rígida, com esse tipo de limpeza ativado um arquivo compactado será excluído se contiver pelo menos um arquivo infectado, independentemente do status dos demais arquivos contidos no arquivo compactado.

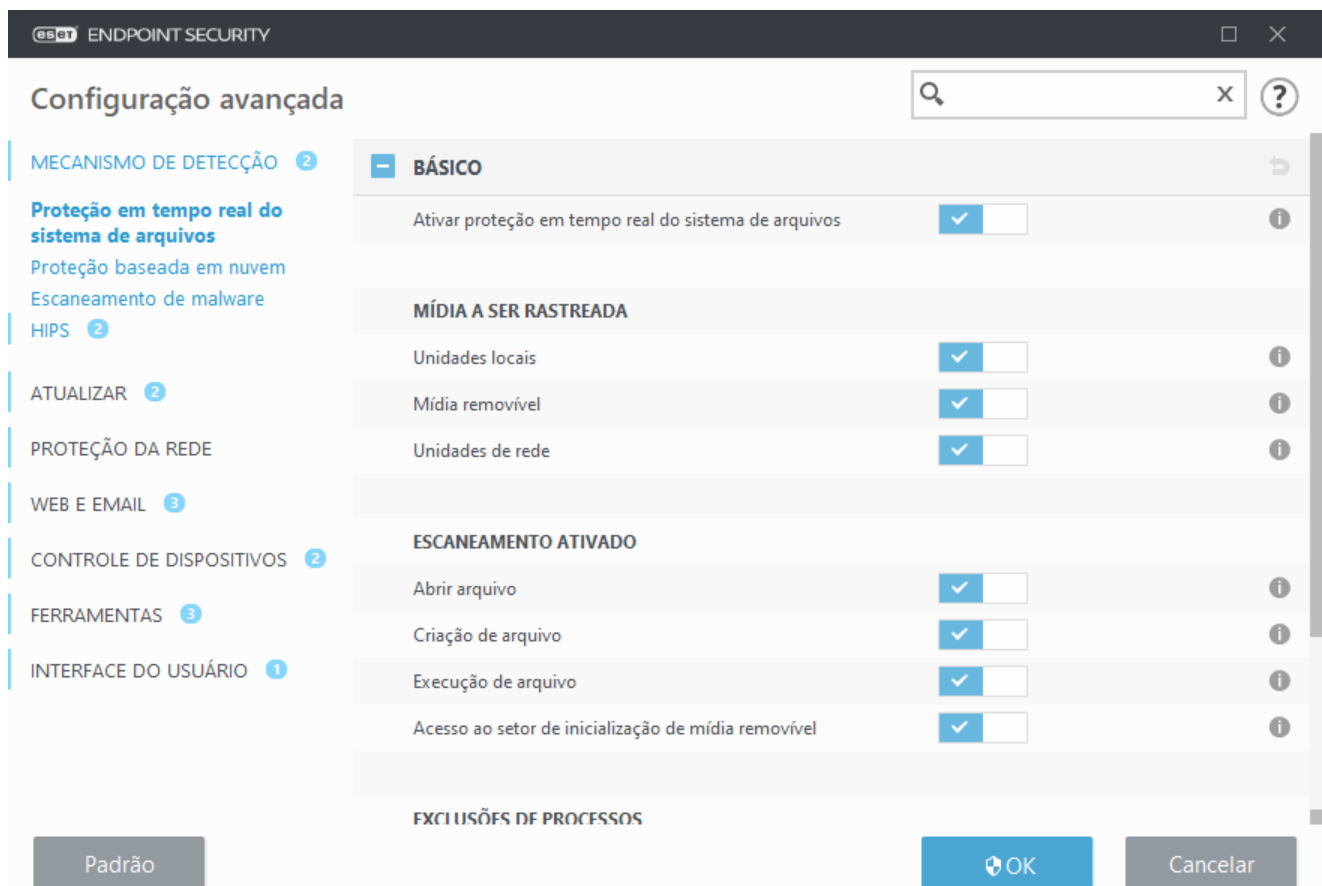
Se o seu computador estiver apresentando sinais de infecção por malware, por exemplo, estiver mais lento, travar com frequência, etc., recomendamos que você faça o seguinte:

- Abra o ESET Endpoint Security e clique em Rastrear o computador.
- Clique em **Rastreamento inteligente** (para obter mais informações, consulte [Rastrear o computador](#))
- Após a conclusão do rastreamento, revise o log para obter informações como o número de arquivos rastreados, infectados e limpos

Se desejar rastrear apenas uma determinada parte do seu disco, clique em **Rastreamento personalizado** e selecione os alvos a serem rastreados quanto a vírus.

Proteção em tempo real do sistema de arquivos

A Proteção em tempo real do sistema de arquivos controla todos os arquivos no sistema para código malicioso quando os arquivos são abertos, criados ou executados.



Por padrão, a Proteção em tempo real do sistema de arquivos é lançada na inicialização do sistema e oferece um

escaneamento sem interrupção. Não recomendamos desativá-la. **Ative a proteção em tempo real do sistema de arquivos** em **Configuração avançada** sob **Mecanismo de detecção** em **Proteção em tempo real do sistema de arquivos** > **Básico**.

Mídia a ser escaneada

Por padrão, todos os tipos de mídia são escaneadas quanto a potenciais ameaças:

- **Unidades locais** – Escaneia todo o sistema e discos rígidos fixos (por exemplo: *C:*, *D:*).
- **Mídia removível** – Escaneia CD/DVDs, armazenamento USB, cartões de memória, etc.
- **Unidades de rede** – Escaneia todas as unidades de rede mapeadas (por exemplo: *H:* como *\\store04*) ou unidades de rede de acesso direto (por exemplo: *\\store08*).

Recomendamos que você use as configurações padrão e as modifique somente em casos específicos, como quando o escaneamento de determinada mídia tornar muito lenta a transferência de dados.

Escaneamento ativado

Por padrão, todos os arquivos são verificados na abertura, criação ou execução. Recomendamos que você mantenha as configurações padrão, uma vez que elas fornecem o nível máximo de proteção em tempo real ao seu computador:

- **Abertura de arquivo** – Escaneia quando um arquivo é aberto.
- **Criação de arquivo** – Escaneia um arquivo criado ou modificado.
- **Execução de arquivo** – Escaneia quando um arquivo é executado.
- **Acesso ao setor de inicialização de mídia removível** – Quando uma mídia removível que contém um setor de inicialização é inserida no dispositivo, o setor de inicialização é escaneado imediatamente. Essa opção não ativa o escaneamento de arquivos em mídia removível. O escaneamento de arquivos em mídia removível está localizado em **Mídia a ser escaneada** > **Mídia removível**. Para que o **Acesso ao setor de inicialização de mídia removível** funcione corretamente, mantenha **Setores de inicialização/UEFI** ativado nos parâmetros ThreatSense.

Processos a serem excluídos do escaneamento – Leia mais sobre esse tipo de exclusão no capítulo [Exclusões de processos](#).

A proteção em tempo real do sistema de arquivos verifica todos os tipos de mídia e é acionada por vários eventos do sistema, tais como o acesso a um arquivo. Com a utilização dos métodos de detecção da tecnologia ThreatSense (descritos na seção Configuração de parâmetros do mecanismo [ThreatSense](#)), a proteção em tempo real do sistema de arquivos pode ser configurada para tratar arquivos recém-criados de forma diferente dos arquivos existentes. Por exemplo, é possível configurar a Proteção em tempo real do sistema de arquivos para monitorar mais de perto os arquivos recém-criados.

Para garantir o impacto mínimo no sistema ao usar a proteção em tempo real, os arquivos que já foram escaneados não são escaneados repetidamente (exceto se tiverem sido modificados). Arquivos são escaneados novamente imediatamente depois de cada atualização do mecanismo de detecção. Esse comportamento é controlado usando a **Otimização inteligente**. Se essa **Otimização inteligente** estiver desativada, todos os arquivos serão escaneados sempre que forem acessados. Para modificar essa configuração, pressione **F5** para abrir a Configuração avançada e expanda **Mecanismo de detecção** > **Proteção em tempo real do sistema de arquivos**. Clique em **Parâmetros do ThreatSense** > **Outro** e marque ou desmarque **Ativar otimização inteligente**.

Verificação da proteção em tempo real


Para verificar se a proteção em tempo real está funcionando e detectando vírus, use um arquivo de teste do eicar.com. Este arquivo de teste é inofensivo e detectável por todos os programas antivírus. O arquivo foi criado pela empresa EICAR (European Institute for Computer Antivirus Research) para testar a funcionalidade de programas antivírus.

O arquivo está disponível para download em <http://www.eicar.org/download/eicar.com>

Depois de inserir este URL no seu navegador, você deve ver uma mensagem dizendo que a ameaça foi removida.

Quando modificar a configuração da proteção em tempo real

A proteção do sistema de arquivos em tempo real é o componente mais essencial para a manutenção de um sistema seguro. Seja sempre cuidadoso ao modificar os parâmetros de proteção. Recomendamos que você modifique esses parâmetros apenas em casos específicos.

Após instalar o ESET Endpoint Security, todas as configurações serão otimizadas para proporcionar o nível máximo de segurança do sistema para os usuários. Para restaurar as configurações padrão, clique em  ao lado de cada guia na janela (**Configuração avançada > Mecanismo de detecção > Proteção do sistema de arquivos em tempo real**).

O que fazer se a proteção em tempo real não funcionar

Neste capítulo, descrevemos problemas que podem surgir quando usamos proteção em tempo real e como solucioná-las.

Proteção em tempo real desativada

Se um usuário inadvertidamente desativar a proteção em tempo real, você deve reativar o recurso. Para reativar a proteção em tempo real, vá para **Configuração** na janela principal do programa e clique em **Proteção do computador > Proteção em tempo real do sistema de arquivos**.

Se a proteção em tempo real não for ativada na inicialização do sistema, geralmente é porque **Ativar a proteção em tempo real do sistema de arquivos** está desativada. Para garantir que esta opção está ativada, navegue para **Configuração avançada (F5)** e clique em **Mecanismo de detecção > Proteção em tempo real do sistema de arquivos**.

Se a proteção em tempo real não detectar nem limpar infiltrações

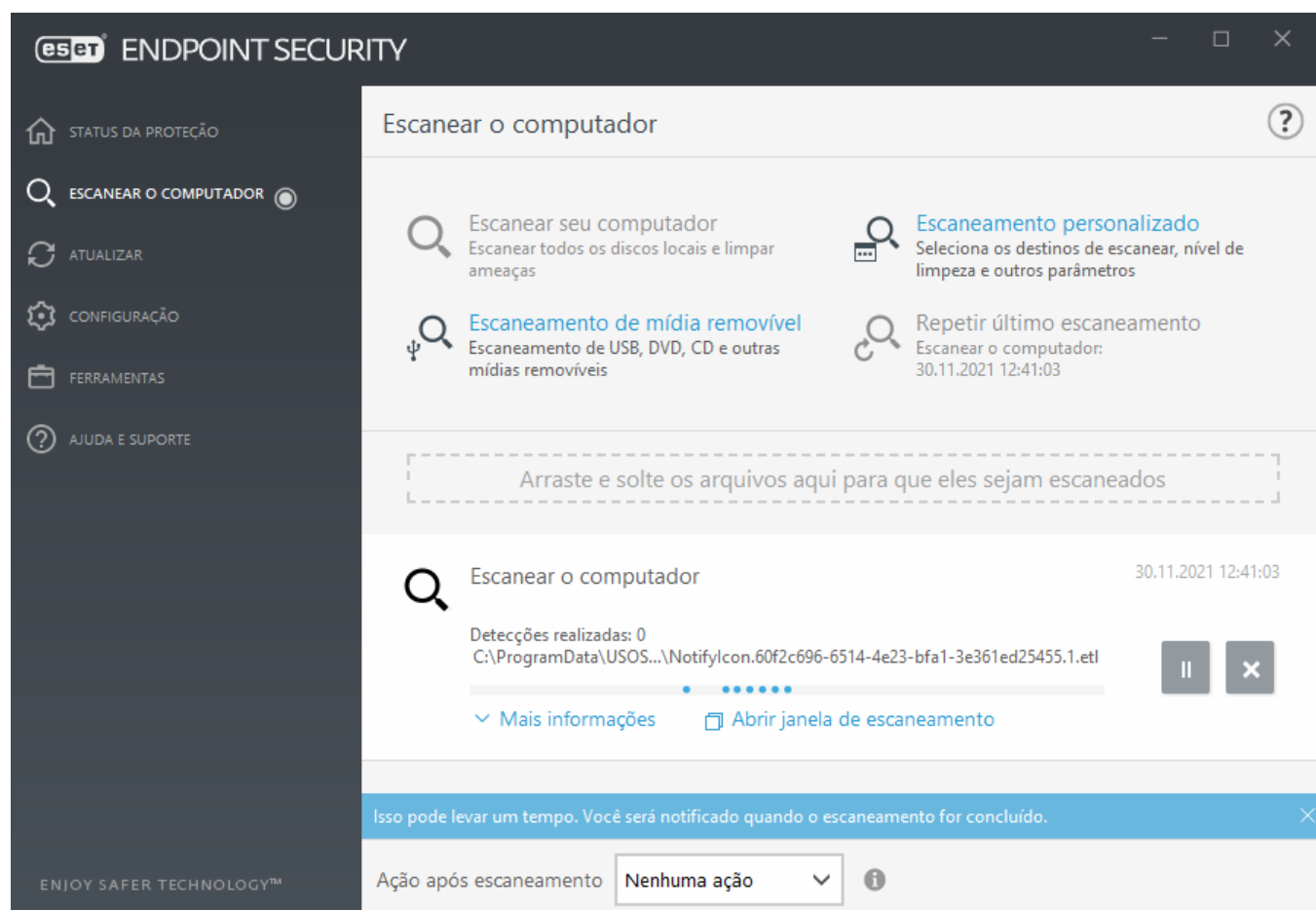
Verifique se não há algum outro programa antivírus instalado no computador. Se dois programas antivírus estiverem instalados ao mesmo tempo, eles podem entrar em conflito. Recomendamos desinstalar outros programas antivírus do sistema antes da instalação da ESET.

A proteção em tempo real não é iniciada

Se a proteção em tempo real não for iniciada na inicialização do sistema (e **Ativar a proteção em tempo real do sistema de arquivos** estiver ativado), isso pode ser devido a conflitos com outros programas. Para ajuda na resolução deste problema, entre em contato com o Suporte Técnico ESET. Criar um relatório do ESET SysInspector e enviar para o Suporte técnico ESET para análise pode ajudar a resolver o problema. Para mais informações, leia o seguinte [artigo da Base de conhecimento ESET](#).

Escanear o computador

O escaneador sob demanda é uma parte importante do ESET Endpoint Security. Ele é usado para realizar escaneamento nos arquivos e pastas do seu computador. Do ponto de vista da segurança, é fundamental que os escaneamento do computador não sejam executados apenas quando há suspeita de uma infecção, mas regularmente como parte das medidas usuais de segurança. Recomendamos que você realize rastreamentos detalhados regulares do sistema (por exemplo, uma vez por mês) para detectar vírus que não tenham sido capturados pela [Proteção em tempo real do sistema de arquivos](#). Isso pode acontecer se a Proteção em tempo real do sistema de arquivos estiver desativada no momento, se o mecanismo de detecção for obsoleto ou se o arquivo não for detectado como vírus ao ser salvo no disco.



Há dois tipos de **Escanejamento do computador** disponíveis. O **Escanear seu computador** escaneia rapidamente o sistema sem necessidade de mais configurações dos parâmetros de escaneamento. O **Escanejamento personalizado** permite selecionar qualquer perfil de escaneamento predefinido e definir destinos de escaneamento específicos.

Leia [Progresso do escaneamento](#) para obter mais informações sobre o processo de escaneamento.

Escanear seu computador

O Escaneamento inteligente permite que você inicie rapidamente um rastreamento 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 Escaneamento 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. Para obter informações mais detalhadas sobre os tipos de limpeza, consulte [Limpeza](#).

Escaneamento personalizado

O escaneamento personalizado é uma solução excelente, caso queira especificar parâmetros de escaneamento, como escaneamento de alvos e métodos de escaneamento. A vantagem do escaneamento personalizado é a capacidade de configurar os parâmetros detalhadamente. As configurações podem ser salvas nos perfis de escaneamento definidos pelo usuário, o que poderá ser útil se o escaneamento for executado repetidas vezes com os mesmos parâmetros.

Para selecionar os alvos de escaneamento, selecione **Escanear o computador > Escaneamento personalizado** e selecione uma opção no menu suspenso **Alvos de escaneamento** ou selecione alvos específicos na estrutura em árvore. Um alvo de escaneamento pode ser também especificado por meio da inserção do caminho da pasta ou arquivo(s) que você deseja incluir. Se você estiver interessado apenas no escaneamento do sistema, sem ações de limpeza adicionais, selecione **Escanear sem limpar**. Ao realizar um escaneamento você pode selecionar entre três níveis de limpeza clicando em **Configuração > Parâmetros Threatsense > Limpeza**.

A realização de escaneamentos de computador com o Escaneamento personalizado é adequada para usuários avançados com experiência anterior na utilização de programas antivírus.

Também é possível usar o recurso de **Escaneamento arrastar e soltar arquivos** para escanear um arquivo ou pasta manualmente ao clicar no arquivo ou pasta, mover o indicador do mouse para a área marcada enquanto mantém o botão do mouse pressionado, e então soltar. Depois disso, o aplicativo é movido para o primeiro plano.

Escaneamento de mídia removível

Semelhante ao **Escanear seu computador** - inicie rapidamente um escaneamento de mídia removível (como CD/DVD/USB) atualmente conectada ao computador. Isso pode ser útil quando você conectar uma unidade flash USB a um computador e quiser escanear seu conteúdo quanto a malware e ameaças em potencial.

Esse tipo de escaneamento também pode ser iniciado clicando em **Escaneamento personalizado** e selecionando **Mídia removível** no menu suspenso **Alvos de escaneamento** e clicando em **Escan**.

Repetir o último escaneamento

Permite iniciar rapidamente o rastreamento realizado anteriormente, usando as mesmas configurações com as quais foi executado antes.


Você pode selecionar **Nenhuma ação**, **Desligar**, **Reiniciar**, **Reiniciar se necessário**, **Forçar reinicialização se necessário** ou **Forçar reinicialização** do menu suspenso **Ação após o escaneamento**. As ações **Suspender** ou **Hibernar** estão disponíveis com base nas configurações de Energia e suspensão do sistema operacional do seu

computador ou das capacidades do seu computador/notebook. A ação selecionada será iniciada depois de todos os escaneamentos em execução serem concluídos. Quando **Desligar** for selecionado, uma caixa de diálogo de confirmação de produto do desligamento exibirá uma contagem regressiva de 30 segundos (clique em **Cancelar** para desativar o desligamento solicitado). Consulte as [Opções de escaneamento avançadas](#) para obter mais detalhes.



Recomendamos que execute um escaneamento do computador pelo menos uma vez por mês. O rastreamento pode ser configurado como uma tarefa agendada em **Ferramentas > Agenda**. [Como agendar um escaneamento semanal do computador?](#)

Iniciador de escaneamento personalizado

Se desejar verificar um alvo específico, você poderá usar a ferramenta Escaneamento personalizado clicando em **Escanear o computador > Escaneamento personalizado** e selecionar uma opção no menu suspenso  > **Alvos de escaneamento** ou selecionar alvos específicos na estrutura de pasta (em árvore).

A janela de destinos de escaneamento permite definir que objetos (memória, unidades, setores, arquivos e pastas) são escaneados em busca de infiltrações.

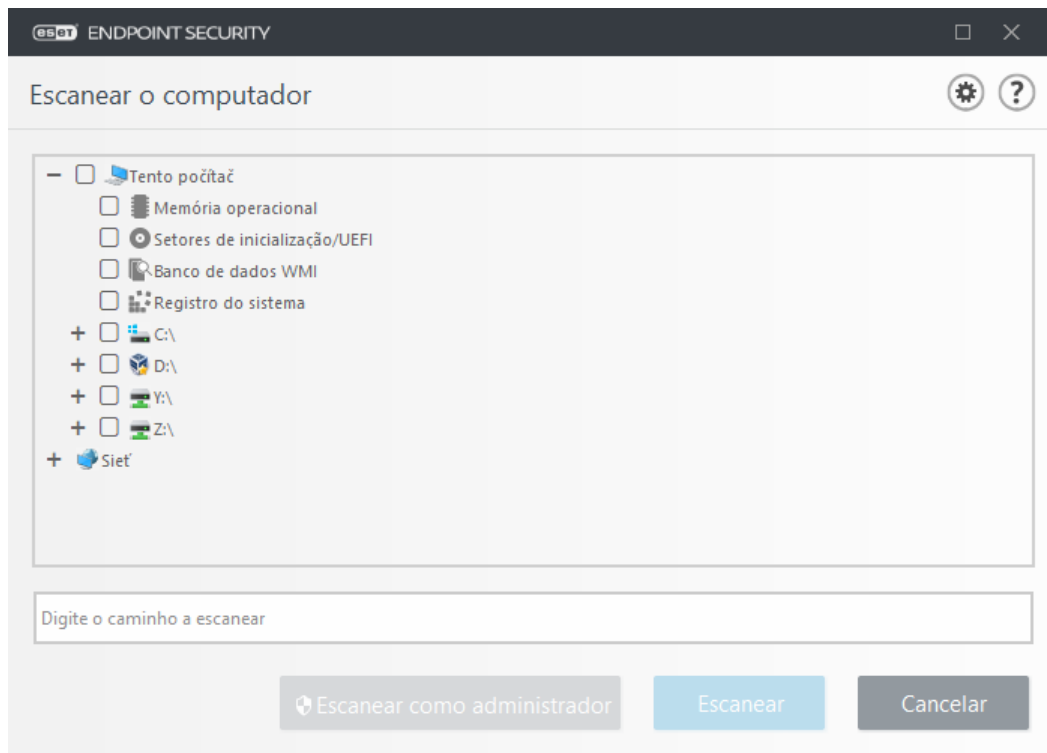
O menu suspenso **Destinos de escaneamento** permite a você selecionar destinos de escaneamento predefinidos.

- **Por configurações de perfil** - Seleciona destinos especificados pelo perfil de escaneamento selecionado.
- **Mídia removível** - Seleciona disquetes, dispositivos de armazenamento USB, CD/DVD.
- **Unidades locais** - Seleciona todas as unidades de disco rígido do sistema.
- **Unidades de rede** - Seleciona todas as unidades de rede mapeadas.
- **Seleção personalizada** – cancela todas as seleções anteriores.

A estrutura da pasta (árvore) também contém destinos de escaneamento específicos.

- **Memória operacional** – escaneia todos os processos e dados atualmente usados pela memória operacional.
- **Setores de inicialização/UEFI** – escaneia os setores de inicialização e UEFI quanto à presença de malware. Leia mais sobre o Escaneador UEFI no [glossário](#).
- **Banco de dados WMI** – Escaneia todo o banco de dados Windows Management Instrumentation WMI, todos os namespaces, todas as instâncias de classe e todas as propriedades. Pesquisa por referências a arquivos infectados ou malware incorporado como dados.
- **Registro do sistema** – escaneia todo o registro do sistema, todas as chaves e subchaves. Pesquisa por referências a arquivos infectados ou malware incorporado como dados. Ao limpar as detecções, a referência permanece no registro para se certificar de que nenhum dado importante será perdido.

Para navegar rapidamente até um destino de escaneamento (arquivo ou pasta), digite seu caminho no campo de texto abaixo da estrutura em árvore. O caminho diferencia minúsculas e maiúsculas. Para incluir o destino no escaneamento, selecione sua caixa de seleção na estrutura em árvore.



Itens infectados não são limpos automaticamente. O escaneamento sem a limpeza pode ser usado para obter uma visão geral do status de proteção atual. Além disso, você pode escolher entre três níveis de escaneamento clicando em **Configuração avançada > Mecanismo de detecção > Escaneamento sob demanda > Parâmetros ThreatSense > Limpeza**. Se você estiver interessado apenas no escaneamento do sistema, sem ações de limpeza adicionais, selecione **Escanear sem limpar**. O histórico de escaneamento é salvo no relatório do escaneamento.

Quando **Ignorar exclusões** estiver selecionado, arquivos com extensões que foram previamente excluídos da verificação serão escaneados sem exceção.

Você pode escolher um perfil no menu suspenso **Perfil de escaneamento** para ser usado para escaneamento dos destinos escolhidos. O perfil padrão é **Escaneamento inteligente**. Há mais três perfis de escaneamento predefinidos chamados de **Escaneamento do menu de contexto**, **Escaneamento detalhado** e **Escaneamento do computador**. Estes perfis de escaneamento usam [parâmetros ThreatSense](#) diferentes. As opções disponíveis são descritas em **Configuração avançada > Mecanismo de detecção > Escaneamentos de malware > Escaneamento sob demanda > [Parâmetros ThreatSense](#)**.

Clique em **Escaneamento** para executar o escaneamento com os parâmetros personalizados definidos.

Escaneamento como administrador permite que você execute o escaneamento usando a conta do administrador. Clique nessa opção se o usuário atual não tiver privilégios para acessar os arquivos apropriados para serem rastreados. Observe que esse botão não estará disponível se o usuário atual não puder acionar operações de UAC como Administrador.



Você pode exibir o relatório de rastreamento do computador quando o rastreamento for concluído clicando em [Exibir relatório](#).

Progresso do rastreamento

A janela de progresso do rastreamento mostra o status atual do rastreamento e informações sobre a quantidade de arquivos encontrados que contêm código malicioso.

Escaneamento de computador

?

Ameaças encontradas: 0

Setores de inicialização/UEFI

8/23/2018 2:40:59 PM

II

X

^

Menos informações

Usuário: John-PC\John

Objetos rastreados: 665

Duração: 0:00:36

Relatório do rastreamento

Versão do mecanismo de detecção: 17931 (20180823)

Data: 8/23/2018 Hora: 2:40:59 PM

Data: 8/23/2018 Hora: 2:40:59 PM

Discos, pastas e arquivos rastreados: Memória operacional;C:\Setores de inicialização/UEFI;C:\

Memória operacional = \\E:\yboxsn\VirtualBoxShare\Ranorex__EES\endpoint_65\endpoint_65\bin\Debug\Ranorex.Core.Resolver.dll - não foi possível abrir [4]

☒ Rolar relatório de escaneamento

Fechar

i É normal que alguns arquivos, como arquivos protegidos por senha ou arquivos exclusivamente utilizados pelo sistema (geralmente *pagefile.sys* e determinados arquivos de log), não possam ser rastreados.

Progresso do rastreamento - A barra de progresso mostra o status de objetos já rastreados em relação aos objetos ainda aguardando para serem rastreados. O status de progresso do rastreamento é derivado do número total de objetos incluídos no rastreamento.

Destino - O nome do objeto rastreado no momento e sua localização.

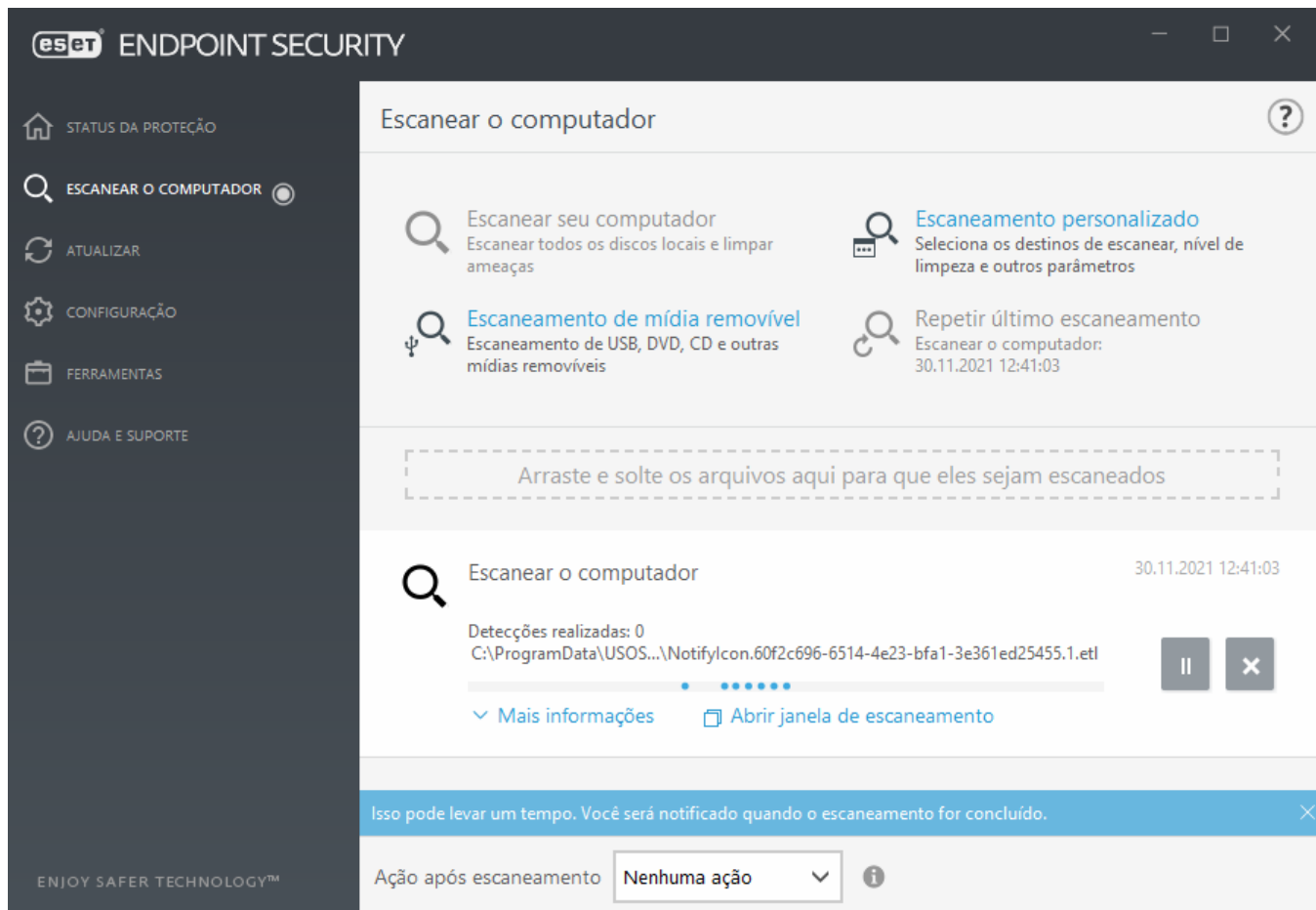
Ameaças encontradas - Mostra o número total de ameaças encontradas durante um rastreamento.

Pausa - Pausa um rastreamento.

Continuar - Essa opção torna-se visível quando o progresso do rastreamento é pausado. Clique em **Continuar** para dar continuidade ao rastreamento.

Parar - Termina o rastreamento.

Percorrer relatório de rastreamento - Se estiver ativado, o relatório de rastreamento rolará automaticamente para baixo à medida que novas entradas forem adicionadas para que as entradas mais recentes fiquem visíveis.



Relatório de escaneamento do computador

O [relatório de rastreamento do computador](#) dá informações gerais sobre o rastreamento, como:

- Data e hora do rastreamento
- Discos, pastas e arquivos rastreados
- Número de objetos rastreados
- Número de ameaças encontradas
- Hora da conclusão
- Tempo total do rastreamento

Escaneamento de malware

A seção **Escaneamento de malware** pode ser acessada no menu Configuração avançada. Pressionar a tecla **F5** e clicar em **Mecanismo de detecção > Escaneamento de malware** oferece as opções para selecionar parâmetros de escaneamento. Essa seção inclui as opções a seguir:

- **Perfil selecionado** – Um conjunto de parâmetros específicos usado pelo escaneador sob demanda. Para criar um novo perfil, clique em Editar ao lado de Lista de perfis. Consulte [Perfis de escaneamento](#) para mais detalhes.
- **Proteção sob demanda e de Machine learning** – Consulte [Mecanismo de detecção \(7.2 e versões posteriores\)](#).
- **Destinos para escaneamento** – Se você quiser escanear somente um destino específico, você pode clicar em **Edit** ao lado de **Destinos para escaneamento** e selecionar uma opção no menu suspenso ou

selecionar destinos específicos da estrutura de pastas (árvore). Consulte [Destinos para escaneamento](#) para mais detalhes.

- **Parâmetros do ThreatSense** – Opções de configuração avançada como, por exemplo, extensões de arquivo que você gostaria de controlar, métodos de detecção utilizados, etc., podem ser encontradas nesta seção. Clique para abrir uma guia com opções do escaneador avançado.

Escaneamento em estado ocioso

Você pode ativar o escaneador em estado ocioso na **Configuração avançada** sob **Mecanismo de detecção > Escaneamentos de malware > Escaneamento em estado ocioso**.

Escaneamento em estado ocioso

Defina a opção ao lado de **Ativar escaneamento em estado ocioso** como **Ativado** para ativar esse recurso. Quando o computador estiver em estado ocioso, um escaneamento do computador em segundo plano será realizado em todas as unidades locais.

Por padrão, o escaneamento em estado ocioso não será executado quando o computador estiver fazendo uso de bateria. Você pode substituir essa configuração ativando a chave ao lado de **Executar mesmo se o computador estiver na bateria** na Configuração avançada.

Ative a opção **Ativar registro** na Configuração avançada para registrar uma saída de rastreamento do computador na seção [Relatórios](#) (a partir da janela principal do programa, clique em **Ferramentas > Relatórios** e selecione **Rastreamento do computador** a partir do menu suspenso **Log**).

Detecção em estado ocioso

Veja [Acionadores de detecção em estado ocioso](#) para uma lista completa de condições que devem ser cumpridas para acionar o escaneamento em estado ocioso.

Clique na Configuração de parâmetros do mecanismo [ThreatSense](#) para modificar parâmetros de verificação (p. ex., métodos de detecção) para o scanner no estado ocioso.

Perfis de rastreamento

Há quatro perfis de escaneamento predefinidos no ESET Endpoint Security:

- **Escaneamento inteligente** – é o perfil de escaneamento avançado padrão. O perfil de Escaneamento inteligente usa a tecnologia de Otimização inteligente, que exclui os arquivos que foram detectados como limpos em um escaneamento anterior e não foram modificados desde esse escaneamento. Isso permite tempos de escaneamento mais baixos com um impacto mínimo na segurança do sistema.
- **Escaneamento do menu de contexto** – você pode iniciar um escaneamento sob demanda de qualquer arquivo no menu de contexto. O perfil de Escaneamento do menu de contexto permite que você defina uma configuração de escaneamento que será usada quando você acionar o escaneamento dessa forma.
- **Escaneamento detalhado** – O perfil de Escaneamento detalhado não usa a Otimização inteligente por padrão, portanto nenhum arquivo é excluído do escaneamento usando este perfil.
- **Escaneamento do computador** – este é o perfil padrão usado no escaneamento padrão do computador.

Os seus parâmetros de rastreamento favoritos podem ser salvos para rastreamento futuro. Recomendamos a criação de um perfil diferente (com diversos alvos de rastreamento, métodos de rastreamento e outros parâmetros) para cada rastreamento utilizado regularmente.

Para criar um novo perfil, abra a janela Configuração avançada (F5) e clique em **Mecanismo de detecção > Escaneamento de malware > Escaneamento sob demanda > Lista de perfis**. A janela **Gerenciador de perfil** inclui o menu suspenso **Perfil selecionado** que lista perfis de rastreamento existentes e a opção de criar um novo. Para ajudar a criar um perfil de rastreamento que atenda às suas necessidades, consulte a seção [Configuração de parâmetros do mecanismo ThreatSense](#) para obter uma descrição de cada parâmetro da configuração de rastreamento.



Suponhamos que você deseje criar seu próprio perfil de rastreamento e que a configuração **Rastrear seu computador** seja parcialmente adequada. Porém, você não deseja rastrear [empacotadores em tempo real](#) nem [aplicativos potencialmente inseguros](#) e também deseja aplicar a **Limpeza rígida**. Digite o nome do novo perfil na janela **Gerenciador de perfil** e clique em **Adicionar**. Selecione seu novo perfil do menu suspenso **Perfil selecionado** e ajuste os parâmetros restantes para atender aos seus requisitos e clique em **OK** para salvar seu novo perfil.

Alvos de rastreamento

A janela de destinos de escaneamento permite definir que objetos (memória, unidades, setores, arquivos e pastas) são escaneados em busca de infiltrações.

O menu suspenso **Destinos de escaneamento** permite a você selecionar destinos de escaneamento predefinidos.

- **Por configurações de perfil** - Seleciona destinos especificados pelo perfil de escaneamento selecionado.
- **Mídia removível** - Seleciona disquetes, dispositivos de armazenamento USB, CD/DVD.
- **Unidades locais** - Seleciona todas as unidades de disco rígido do sistema.
- **Unidades de rede** - Seleciona todas as unidades de rede mapeadas.
- **Seleção personalizada** – cancela todas as seleções anteriores.

A estrutura da pasta (árvore) também contém destinos de escaneamento específicos.

- **Memória operacional** – escaneia todos os processos e dados atualmente usados pela memória operacional.
- **Setores de inicialização/UEFI** – escaneia os setores de inicialização e UEFI quanto à presença de malware. Leia mais sobre o Escaneador UEFI no [glossário](#).
- **Banco de dados WMI** – Escaneia todo o banco de dados Windows Management Instrumentation WMI, todos os namespaces, todas as instâncias de classe e todas as propriedades. Pesquisa por referências a arquivos infectados ou malware incorporado como dados.
- **Registro do sistema** – escaneia todo o registro do sistema, todas as chaves e subchaves. Pesquisa por referências a arquivos infectados ou malware incorporado como dados. Ao limpar as detecções, a referência permanece no registro para se certificar de que nenhum dado importante será perdido.

Para navegar rapidamente até um destino de escaneamento (arquivo ou pasta), digite seu caminho no campo de texto abaixo da estrutura em árvore. O caminho diferencia minúsculas e maiúsculas. Para incluir o destino no escaneamento, selecione sua caixa de seleção na estrutura em árvore.

Opções de rastreamento avançadas

Nessa janela, é possível especificar opções avançadas para uma tarefa agendada de rastreamento do computador. Você pode definir uma ação a ser realizada automaticamente depois de um escaneamento terminar usando o menu suspenso:

- **Desligar** - O computador é desligado depois do rastreamento ser concluído.
- **Reinicializar** - Fecha todos os programas abertos e reinicia o computador depois da conclusão do rastreamento.
- **Reiniciar se necessário** – fecha todos os programas abertos e reinicia o computador, se necessário pelo escaneamento.
- **Suspender** - Salva sua sessão e coloca o computador em um estado de baixa energia para que você possa voltar a trabalhar rapidamente.
- **Hibernar** - Pega tudo que você tem sendo executado em RAM e move para um arquivo especial no seu disco rígido. Seu computador é desligado, mas vai voltar ao seu estado anterior da próxima vez que for iniciado.
- **Nenhuma ação** - Depois do fim do rastreamento, nenhuma ação será realizada.



Tenha em mente que um computador suspenso ainda é um computador ligado. Ele ainda está executando funções básicas e usando eletricidade quando seu computador está operando na bateria. Para economizar a vida da bateria, quando estiver trabalhando fora do escritório recomendamos usar a opção Hibernar.

Selecione **A ação não pode ser cancelada pelo usuário** para negar aos usuários não privilegiados a capacidade de interromper ações realizadas depois do rastreamento.

Selecione a opção **O rastreamento pode ser pausado pelo usuário por (min)** se quiser permitir que o usuário limitado pause o rastreamento do computador por um período de tempo específico.

Consulte também o capítulo [Progresso do rastreamento](#).

Controle de dispositivo

O ESET Endpoint Security fornece controle automático de dispositivos (CD/DVD/USB/...). Esse módulo permite bloquear ou ajustar filtros/permissões estendidos e define a capacidade de um usuário de acessar e trabalhar com um determinado dispositivo. Isso pode ser útil se a intenção do administrador do computador for evitar o uso de dispositivos com conteúdo não solicitado pelos usuários.

Dispositivos externos compatíveis:

- Armazenamento em disco (disco removível HDD, USB)
- CD/DVD
- impressora USB
- FireWire Armazenamento
- Dispositivo Bluetooth
- Leitor de cartão inteligente
- Dispositivo de criação de imagem
- Modem
- LPT/COM porta
- Dispositivo portátil (dispositivos movidos a bateria como reprodutor de mídias, smartphones, dispositivos

plug-and-play, etc.)

- Todos os tipos de dispositivo

As opções de configuração do controle de dispositivos podem ser modificadas em **Configuração avançada (F5) > Controle de dispositivos**.

Marcar a opção ao lado de **Habilitar o controle de dispositivo** ativa o recurso de Controle de dispositivos no ESET Endpoint Security, você precisará reiniciar o computador para que as alterações tenham efeito. Quando o Controle de dispositivos estiver ativado, as **Regras** ficarão ativas, permitindo abrir a janela do [Editor de regras](#).

Se um dispositivo bloqueado por uma regra existente for inserido, uma janela de notificação será exibida e o acesso ao dispositivo não será concedido.

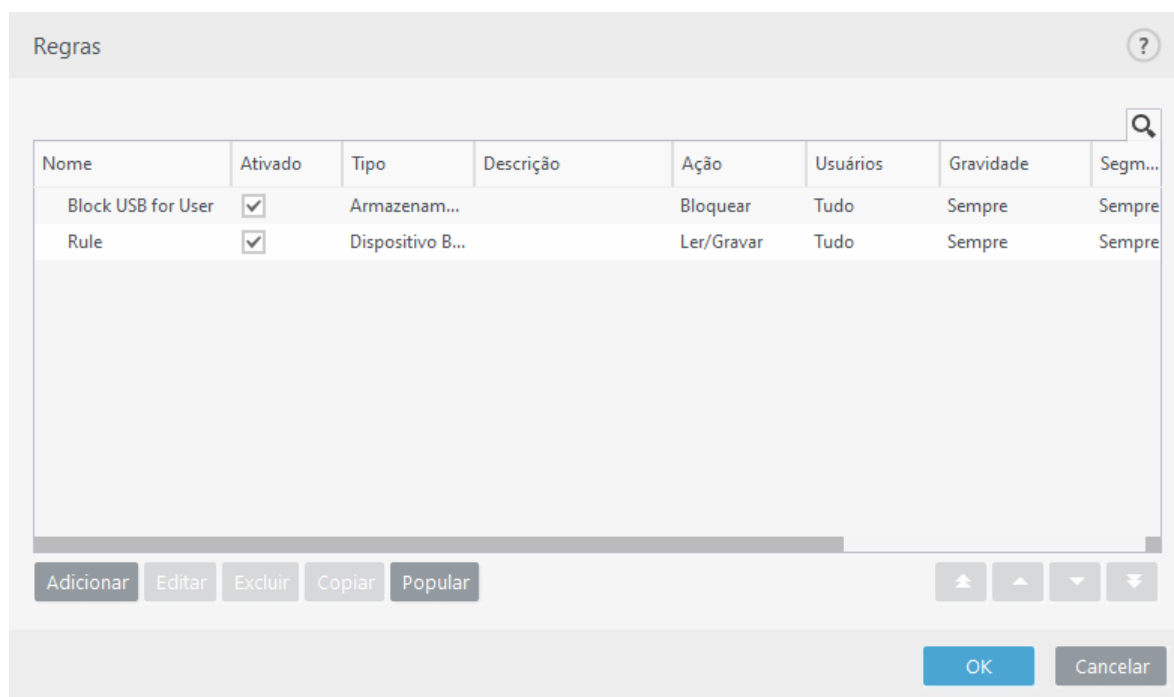
Editor de regras do controle de dispositivos

A janela **Editor de regras de controle de dispositivos** mostra as regras existentes e permite que se controle de forma precisa os dispositivos externos que os usuários conectam ao computador. Veja também [Adicionar regras de controle de dispositivo](#).



Os artigos da Base de conhecimento da ESET a seguir podem estar disponíveis apenas em inglês:

- [Adicione e modifique regras de controle de dispositivos usando os produtos ESET endpoint](#)







Determinados dispositivos podem ser permitidos ou bloqueados de acordo com seu usuário, grupo de usuários ou com base em vários parâmetros adicionais que podem ser especificados na configuração da regra. A lista de regras contém diversas descrições de uma regra, tais como nome, tipo de dispositivo externo, ação a ser realizada após conectar um dispositivo externo ao seu computador e a gravidade do relatório.

Clique em **Adicionar** ou **Editar** para gerenciar uma regra. Clique na caixa de seleção **Ativado** ao lado de uma regra para desativá-la até que você queira usá-la no futuro. Selecione uma ou mais regras e clique em **Excluir** para excluir as regras permanentemente.

Copiar - Cria uma nova regra com opções predefinidas usadas para outra regra selecionada.

Clique em **Preencher** para preencher automaticamente os parâmetros do dispositivo de mídia removível para dispositivos conectados ao computador.


As regras são listadas por ordem de prioridade, com regras de prioridade superior mais próximas do início. Regras podem ser movidas clicando em     **Topo/Cima/Baixo/Fundo** e podem ser movidas individualmente ou em grupos.

O relatório de controle de dispositivos registra todas as ocorrências nas quais o controle de dispositivos é acionado. As entradas de logs podem ser visualizadas a partir da janela principal do programa do ESET Endpoint Security em **Ferramentas** > [Relatórios](#).

Dispositivos detectados


O botão **Preencher** fornece uma visão geral de todos os dispositivos atualmente conectados com as informações sobre: tipo de dispositivo, sobre o fabricante do dispositivo, modelo e número de série (se disponível).

Selecione um dispositivo da lista de Dispositivos detectados e clique em **OK** para [adicionar uma regra de controle de dispositivos](#) com informações pré-definidas (todas as configurações podem ser ajustadas).

Dispositivos no modo de baixa energia (espera) são marcados com um ícone de alerta . Para ativar o botão **OK** e adicionar uma regra para este dispositivo:

- Reconectar o dispositivo.
- Use o dispositivo (por exemplo, inicie o aplicativo da Câmera no Windows para acordar a webcam).

Grupos do dispositivo

 O dispositivo conectado ao seu computador pode representar um risco de segurança.

A janela Grupo de dispositivo é dividida em duas partes. A parte da direita da janela contém uma lista de dispositivos que pertencem ao seu respectivo grupo e a parte da esquerda da janela contém os grupos criados. Selecione um grupo com uma lista de dispositivos que você deseja exibir no painel da direita.

Quando você abrir a janela Grupos do dispositivo e selecionar um grupo, poderá adicionar ou remover dispositivos da lista. Outra forma de adicionar dispositivos ao grupo é importá-los a partir de um arquivo. Alternativamente, você pode clicar no botão **Preencher** e todos os dispositivos conectados ao seu computador serão listados na janela **Dispositivos detectados**. Selecione um dispositivo da lista preenchida para adicioná-lo ao grupo ao clicar em **OK**.

Elementos de controle

Adicionar - Você pode adicionar um grupo ao inserir o nome, adicionar ou um dispositivo a um grupo existente (opcionalmente, é possível especificar detalhes como nome do fornecedor, modelo e número de série) dependendo de em qual parte da janela você clicou no botão.

Editar - Deixa você modificar o nome dos parâmetros do grupo ou dispositivo selecionado (fabricante, modelo, número de série).

Excluir - Exclui o grupo ou dispositivo selecionado dependendo de em qual parte da janela você clicou no botão.

Importar – importa uma lista de dispositivos de um arquivo de texto. Para importar dispositivos de um arquivo de texto é preciso ter a formatação:

- Cada dispositivo começa na nova linha.
- **Fabricante, Modelo e Número de série** devem estar presentes para cada dispositivo e separados por vírgula.

✓ Veja um exemplo do conteúdo do arquivo de texto:
Kingston,DT 101 G2,001CCE0DGRFC0371
04081-0009432,USB2.0 HD WebCam,20090101

Exportar – exporta uma lista de dispositivos para um arquivo.

O botão **Preencher** fornece uma visão geral de todos os dispositivos atualmente conectados com as informações sobre: tipo de dispositivo, sobre o fabricante do dispositivo, modelo e número de série (se disponível).

Quando você tiver concluído a personalização, clique em **OK**. Clique em **Cancelar** se quiser deixar a janela **Grupo do dispositivo** sem salvar alterações.

i É possível criar grupos diferentes de dispositivos para os quais regras diferentes serão aplicadas. Também é possível criar apenas um grupo de dispositivos para os quais a regra com ação **Ler/Gravar** ou **Apenas leitura** será aplicada. Isso garante o bloqueio de dispositivos não reconhecidos pelo Controle de dispositivos quando conectados ao seu computador.

Note que nem todas as ações (permissões) estão disponíveis para todos os tipos de dispositivos. Se for um dispositivo do tipo armazenamento, todas as quatro Ações estão disponíveis. Para dispositivos sem armazenamento, haverá somente duas (por exemplo, **Somente leitura** não estará disponível para Bluetooth, o que significa que dispositivos de Bluetooth poderão apenas ser permitidos, bloqueados ou alertados).

Adição de regras do controle de dispositivos

Uma Regra de controle de dispositivos define a ação a ser tomada quando um dispositivo que corresponde aos critérios da regra é conectado ao computador.

Editar regra

?

Nome

Rule

Regra ativada

☒

Aplicar durante

Sempre

▼

Tipo de dispositivo

Dispositivo Bluetooth

▼

Ação

Ler/Gravar

▼

Tipo de critério

Dispositivo

▼

Fabricante

Modelo

Número de série

Gravidade do registro em log

Sempre

▼

Lista de usuários

Editar

Notificar usuário

☒

OK

Insira uma descrição da regra no campo **Nome** para uma melhor identificação. Clique na opção ao lado de **Regra ativada** para ativar ou desativar esta regra. Isso pode ser útil caso não deseje excluir a regra permanentemente.

Aplicar durante – permite a você aplicar uma regra criada durante um certo tempo. Do menu suspenso, selecione o segmento de tempo criado. Veja mais informações [sobre Seções de tempo](#).

Tipo de dispositivo

Escolha o tipo de dispositivo externo no menu suspenso (Armazenamento em disco/Dispositivo portátil/Bluetooth/FireWire/...). As informações sobre o tipo de dispositivo são coletadas do sistema operacional e podem ser visualizados no Gerenciador de dispositivos do sistema se um dispositivo estiver conectado ao computador. Os dispositivos de armazenamento incluem discos externos ou leitores de cartão de memória convencionais conectados via USB ou FireWire. Leitores de cartões inteligentes abrangem todos os leitores de cartões inteligentes com um circuito integrado incorporado, como cartões SIM ou cartões de autenticação. Scanners e câmeras são exemplos de dispositivos de imagens. Como esses dispositivos oferecem apenas informações sobre suas ações e não oferecem informações sobre os usuários, eles só podem ser bloqueados de forma global.

i A lista de funcionalidade de usuário não está disponível para o tipo de dispositivo de modem. A regra será aplicada para todos os usuários e a lista atual de usuários será excluída.

Ação

O acesso a dispositivos que não sejam de armazenamento pode ser permitido ou bloqueado. Por outro lado, as regras de dispositivos de armazenamento permitem a seleção de uma das seguintes configurações de direitos:

- **Ler/Gravar** - Será permitido acesso total ao dispositivo.

- **Bloquear** - O acesso ao dispositivo será bloqueado.
- **Apenas leitura** - Será permitido acesso apenas para leitura ao dispositivo.
- **Alertar** - Cada vez que um dispositivo for conectado, o usuário será notificado se ele é permitido ou bloqueado, e um registro no relatório será feito. Dispositivos não são lembrados, uma notificação continuará a ser exibida com conexões subsequentes ao mesmo dispositivo.

Note que nem todas as ações (permissões) estão disponíveis para todos os tipos de dispositivos. Se for um dispositivo do tipo armazenamento, todas as quatro Ações estão disponíveis. Para dispositivos sem armazenamento, haverá somente duas (por exemplo, **Somente leitura** não estará disponível para Bluetooth, o que significa que dispositivos de Bluetooth poderão apenas ser permitidos, bloqueados ou alertados).

Tipo de critério

Selecione **Grupo do dispositivo** ou **Dispositivo**.

Outros parâmetros mostrados a seguir podem ser usados para ajustar as regras e adequá-las a dispositivos. Todos os parâmetros fazem diferenciação entre letras maiúsculas e minúsculas:

- **Fornecedor** - Filtragem por nome ou ID do fornecedor.
- **Modelo** - O nome específico do dispositivo.
- **Número de série** - Os dispositivos externos geralmente têm seus próprios números de série. No caso de CD/DVD, este é o número de série da mídia em si, e não o da unidade de CD.

i Se esses parâmetros estiverem indefinidos, a regra irá ignorar estes campos enquanto faz a correspondência. Os parâmetros de filtragem em todos os campos de texto fazem diferenciação de maiúsculas e minúsculas; caracteres curinga (*, ?) não são aceitos.

i Para ver informações sobre um dispositivo, crie uma regra para o tipo de dispositivos, conecte o dispositivo ao seu computador e, em seguida, verifique os detalhes do dispositivo no [Relatório de controle de dispositivos](#).

Gravidade do registro em relatório

- **Sempre** – Registra todos os eventos.
- **Diagnóstico** - Registra informações necessárias para ajustar o programa.
- **Informações**– Registra as mensagens informativas, incluindo as mensagens de atualizações bem-sucedidas e todos os registros mencionados anteriormente.
- **Avisos** - Registra mensagens de erros críticos e de aviso e envia-as para o ERA Server.
- **Nenhum** - Nenhum registro em relatório será feito.

As regras podem ser limitadas a determinados usuários ou grupos de usuários adicionando-os à **Lista de usuários**:

- **Adicionar** – Abre os **Tipos de objetos: Usuários ou Grupos** que permite selecionar os usuários desejados.
- **Remover** – Remove o usuário selecionado do filtro.

i Nem todos os dispositivos podem ser filtrados por regras do usuário (por exemplo, dispositivos de criação de imagem não fornecem informações sobre usuários, apenas sobre ações).

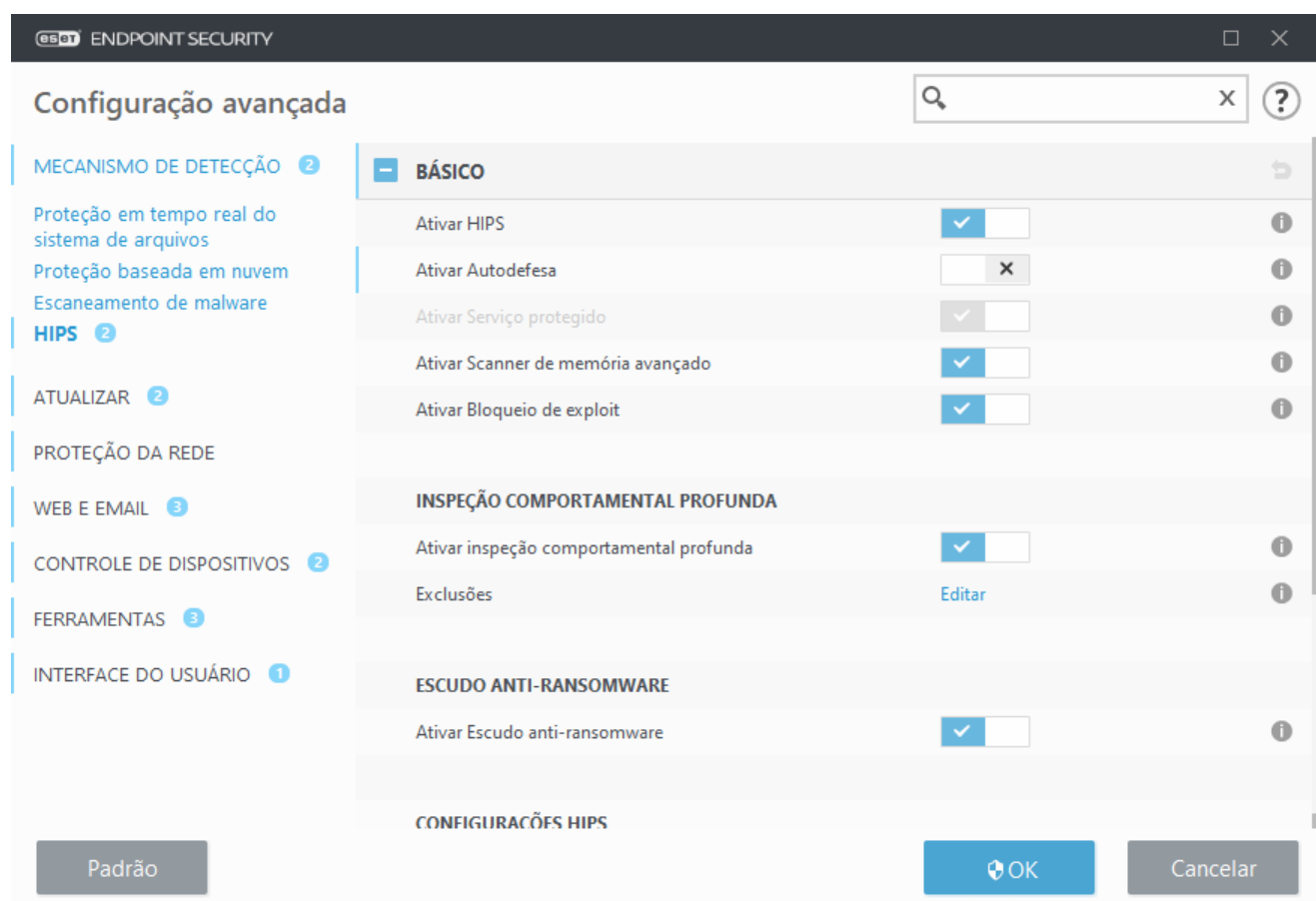
Sistema de prevenção de intrusos de host (HIPS)



Apenas um usuário experiente deve fazer alterações nas configurações do HIPS. A configuração incorreta das configurações HIPS pode causar instabilidade no sistema.

O **Sistema de prevenção de intrusos de host (HIPS)** protege o sistema de malware ou de qualquer atividade que tentar prejudicar a segurança do computador. Ele utiliza a análise comportamental avançada em conjunto com as capacidades de detecção de filtro de rede para monitorar processos em execução, arquivos e chaves de registro. O HIPS é separado da proteção em tempo real do sistema de arquivos e não é um firewall; ele monitora somente processos em execução no sistema operacional.

As configurações HIPS podem ser encontradas em **Configuração avançada (F5) > Mecanismo de detecção > HIPS > Básico**. O status do HIPS (ativado/desativado) é exibido na janela do programa principal do ESET Endpoint Security, em **Configuração > Computador**.



Básico

Ativar HIPS – O HIPS está ativado por padrão no ESET Endpoint Security. Desativar o HIPS vai desativar o restante dos recursos HIPS como o Bloqueio de Exploit.

Ativar Autodefesa – O ESET Endpoint Security usa a tecnologia de **Autodefesa** incorporada como parte do HIPS para impedir que o software malicioso danifique ou desabilite a proteção antivírus e antispymware. A Autodefesa protege sistemas cruciais e processos, chaves de registro e arquivos da ESET contra alterações maliciosas. O Agente ESET Management também é protegido, quando ele está instalado.

Ativar Serviço protegido – Ativa a proteção para o Serviço ESET (ekrn.exe). Quando ativado, o serviço é iniciado

como um processo protegido do Windows para defender ataques feitos por malware. Essa opção está disponível no Windows 8.1 e no Windows 10.

Ativar Advanced memory scanner – funciona combinado com o Bloqueio de exploit para fortalecer a proteção contra malware feito para evitar a detecção por produtos antimalware através do uso de ofuscação ou criptografia. Por padrão, o scanner de memória avançado está ativado. Leia mais sobre esse tipo de proteção no [glossário](#).

Ativar Bloqueio de exploit – feito para fortalecer tipos de aplicativos comumente explorados como navegadores da web, leitores de PDF, clientes de email e componentes do MS Office. Por padrão, o bloqueio de exploit está ativado. Leia mais sobre esse tipo de proteção no [glossário](#).

Inspeção comportamental profunda

Ativar inspeção comportamental profunda – outra camada de proteção que funciona como parte do recurso HIPS. Essa extensão do HIPS analisa o comportamento de todos os programas em execução no computador e avisa você se o comportamento do processo for malicioso.

[Exclusões HIPS da inspeção comportamental profunda](#) permitem que você exclua processos da análise.

Recomendamos que você crie exclusões somente quando for absolutamente necessário, a fim de garantir que todos os processos sejam escaneados para possíveis ameaças.

Proteção contra ransomware

Ativar escudo anti-ransomware – outra camada de proteção que funciona como uma parte do recurso HIPS. Você deve ter o sistema de reputação ESET LiveGrid® ativado para a Proteção contra ransomware funcionar. [Leia mais sobre este tipo de proteção](#).

Ativar modo de auditoria – Tudo que é detectado pelo Escudo Anti-ransomware não é bloqueado automaticamente, e sim [registrado com uma gravidade de alerta](#) e enviado para o console de gerenciamento com o sinalizador "MODO DE AUDITORIA". O administrador pode decidir excluir essa detecção para impedir detecções futuras ou mantê-la ativa, o que significa que depois que o Modo de auditoria terminar, ela será bloqueada e removida. A ativação/desativação do Modo de auditoria também será registrada no ESET Endpoint Security. Essa opção está disponível apenas no editor de configuração de política ESET PROTECT.

Configurações HIPS

O **modo de filtragem** pode ser executado em um dos modos a seguir:

Modo de filtragem	Descrição
Modo automático	As operações são ativadas, exceto aquelas bloqueadas por regras predefinidas que protegem o sistema.
Modo Smart	O usuário será notificado apenas sobre eventos muito suspeitos.
Modo interativo	O sistema solicitará que o usuário confirme as operações.
Modo com base em políticas	Bloqueia todas as operações que não são definidas por uma regra específica que permita essas operações.

Modo de filtragem	Descrição
Modo de aprendizagem	As operações são ativadas e uma regra é criada após cada operação. As regras criadas nesse modo podem ser visualizadas no editor de Regras HIPS , mas sua prioridade é menor que a prioridade das regras criadas manualmente ou das regras criadas no modo automático. Quando selecionar o Modo de aprendizagem do menu suspenso Modo de filtragem , a configuração Modo de aprendizagem vai terminar em ficará disponível. Selecione o período de tempo pelo qual você deseja que o módulo de aprendizado esteja ativado, a duração máxima é de 14 dias. Quando a duração especificada tiver terminado, você será solicitado a editar as regras criadas pelo HIPS enquanto ele estava no modo de aprendizagem. Você também pode escolher um modo de filtragem diferente, ou adiar a decisão e continuar usando o modo de aprendizagem.

Modo definido depois da expiração do modo de aprendizagem – Selecione o modo de filtragem que será usado após o modo de aprendizagem expirar. Depois da expiração, a opção **Perguntar ao usuário** requer privilégios de administrador para realizar uma mudança no modo de filtragem HIPS.

O sistema HIPS monitora os eventos dentro do sistema operacional e reage a eles de acordo com regras similares àquelas usadas no Firewall. Clique em **Editar** ao lado de **Regras** para abrir o editor de **regras do HIPS**. Na janela de regras HIPS é possível selecionar, adicionar, editar ou remover regras. Mais detalhes sobre a criação de regras e operação HIPS podem ser encontrados em [Editar uma regra HIPS](#).

Janela interativa HIPS

A janela da notificação HIPS permite que você crie uma regra com base em qualquer nova ação que o HIPS detectar e então defina as condições nas quais permitir ou negar essa ação.

As regras criadas da janela de notificação são consideradas iguais às regras criadas manualmente. Uma regra criada de uma janela de notificação pode ser menos específica que a regra que acionou a janela de diálogo. Isso significa que depois de criar uma regra na janela de diálogo, a mesma operação pode acionar a mesma janela. Para mais informações consulte [Prioridade para regras HIPS](#).

Se a ação padrão para uma regra estiver definida como **Perguntar todas as vezes**, uma janela de diálogo será exibida sempre que a regra for acionada. Você pode optar por **Negar** ou **Permitir** a operação. Se você não escolher uma ação no tempo determinado, uma nova ação será selecionada com base nas regras.

Lembrar até sair do aplicativo faz com que a ação (**Permitir/Negar**) seja utilizada até que ocorra uma alteração de regras ou o modo de filtragem ou ocorra uma atualização do módulo do HIPS ou reinicialização do sistema. Depois de qualquer uma dessas três ações, as regras temporárias serão excluídas.

A opção **Criar regra e lembrar permanentemente** criará uma nova regra HIPS que pode ser alterada posteriormente na seção [Gerenciamento de regras de HIPS](#) (requer privilégios de administração).

Clique em **Detalhes** na parte de baixo para ver qual aplicativo acionou a operação, qual é a reputação do arquivo ou qual tipo de operação você está sendo solicitado a permitir ou negar.

É possível acessar configurações para parâmetros de regra mais detalhados clicando em **Opções avançadas**. As opções abaixo estarão disponíveis se você escolher **Criar regra e lembrar permanentemente**:

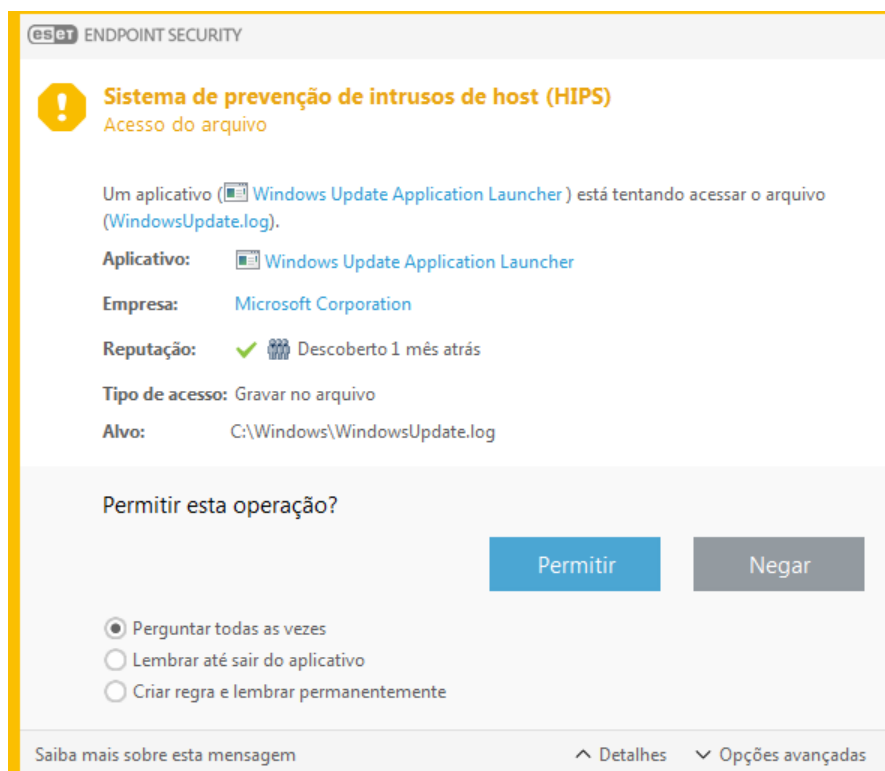
- **Criar uma regra válida apenas para este aplicativo** – Se você desmarcar esta caixa de seleção, a regra será criada para todos os aplicativos de origem.
- **Apenas para operação** – Escolhe a operação para a regra de arquivo/aplicativo/registro. [Veja a descrição](#)

[de todas as operações HIPS.](#)

- **Apenas para destino** – Selecione o(s) destino(s) de regra do arquivo/aplicativo/registro.



Para impedir que as notificações apareçam, mude o modo de filtragem para o **Modo automático** na **Configuração avançada (F5) > Mecanismo de detecção > HIPS > Básico.**



Comportamento de ransomware em potencial detectado

Esta janela interativa aparece quando o comportamento de ransomware em potencial é detectado. Você pode optar por **Negar** ou **Permitir** a operação.

Clique em **Detalhes** para ver os parâmetros de detecção específicos. A janela de diálogo permite a você **Enviar para análise** ou **Excluir da detecção**.



O ESET LiveGrid® deve estar ativado para que a [Proteção contra ransomware](#) funcione adequadamente.

Gerenciamento de regras de HIPS

Esta é uma lista de regras adicionadas automaticamente e definidas pelo usuário no sistema HIPS. Mais detalhes sobre a criação de regras e operações HIPS podem ser encontrados no capítulo [Configurações de](#)

[regras HIPS](#). Consulte também o [Princípio geral do HIPS](#).

Colunas

Regra - Nome da regra definida pelo usuário ou definida automaticamente.

Ativado – Desative esta opção se deseja manter a regra na lista, mas não deseja usá-la.

Ação – A regra especifica uma ação – **Permitir**, **Bloquear** ou **Perguntar** – que deve ser realizada se as condições forem cumpridas.

Fontes - A regra será utilizada apenas se o evento for acionado por um aplicativo(s).

Destinos - A regra será utilizada apenas se a operação estiver relacionada a um arquivo, aplicativo ou entrada de registro específico.

Gravidade do registro em relatório - Se você ativar essa opção, as informações sobre esta regra serão gravadas no [Registro em relatório HIPS](#).

Notificar – Se um evento for acionado, uma pequena notificação em pop-up será exibida no canto inferior direito.

Elementos de controle

Adicionar - Cria uma nova regra.

Editar - permite que você edite as entradas selecionadas.

Remover – Remove as entradas selecionadas.

Prioridade para as regras HIPS

Não há opções para ajustar o nível de prioridade das regras HIPS usando os botões início/fim (como nas [Regras de firewall](#) onde as regras são executadas do início para o fim).

- Todas as regras criadas por você têm a mesma prioridade
- Quanto mais específica a regra, mais alta sua prioridade (por exemplo, a regra para um aplicativo específico tem prioridade maior do que a regra para todos os aplicativos)
- Internamente, o HIPS contém regras com prioridade maior que não podem ser acessadas por você (por exemplo, você não pode substituir as regras definidas de Autodefesa)
- Uma regra criada por você que pode travar seu sistema operacional não será aplicada (ela terá a menor prioridade)

Configurações de regra HIPS

Consulte primeiro o [Gerenciamento de regras de HIPS](#).

Nome da regra - Nome da regra definida pelo usuário ou definida automaticamente.

Ação – Especifica uma ação – Permitir, Bloquear ou Perguntar – que deve ser realizada se as condições forem cumpridas.

Operações afetando - É preciso selecionar o tipo de operação para o qual a regra será aplicada. A regra será

utilizada apenas para esse tipo de operação e para o destino selecionado.

Ativado - Desative esta opção se deseja manter a regra na lista, mas não deseja aplicá-la.

Gravidade do registro em relatório - Se você ativar essa opção, as informações sobre esta regra serão gravadas no [Registro em relatório HIPS](#).

Notificar usuário - Se um evento for acionado, uma pequena janela pop-up será exibida no canto inferior direito.

A regra consiste em partes que descrevem as condições que acionam essa regra:

Aplicativos de origem - A regra será utilizada apenas se o evento for acionado por esse(s) aplicativo(s). Selecione **Aplicativos específicos** no menu suspenso e clique em **Adicionar** para adicionar novos arquivos, ou selecione **Todos os aplicativos** no menu suspenso para adicionar todos os aplicativos.

Arquivos de destino - A regra será utilizada apenas se a operação estiver relacionada a esse destino. Selecione **Arquivos específicos** no menu suspenso e clique em **Adicionar** para adicionar novos arquivos ou pastas, ou selecione **Todos os arquivos** no menu suspenso para adicionar todos os arquivos.

Aplicativos - A regra será utilizada apenas se a operação estiver relacionada a esse destino. Selecione **Aplicativos específicos** no menu suspenso e clique em **Adicionar** para adicionar novos arquivos ou pastas, ou selecione **Todos os aplicativos** no menu suspenso para adicionar todos os aplicativos.

Entradas do registro - A regra será utilizada apenas se a operação estiver relacionada a esse destino. Selecione **Entradas específicas** no menu suspenso e clique em **Adicionar** para adicionar novos arquivos ou pastas, ou selecione **Todas as entradas** no menu suspenso para adicionar todos os aplicativos.



Algumas operações de regras específicas predefinidas pelo HIPS não podem ser bloqueadas e são permitidas por padrão. Além disso, nem todas as operações de sistema são monitoradas pelo HIPS. O HIPS monitora operações que podem ser consideradas inseguras.



Ao especificar um caminho, o C:\example afeta ações com a própria pasta e o C:\example*.* afeta os arquivos na pasta.

Operações de aplicativo

- **Depurar outro aplicativo** - Anexa um depurador ao processo. Ao depurar um aplicativo, muitos detalhes de seu comportamento podem ser visualizados e alterados, e seus dados podem ser acessados.
- **Interceptar eventos de outro aplicativo** - O aplicativo de origem está tentando obter eventos direcionados a um aplicativo específico (por exemplo, um keylogger está tentando capturar eventos do navegador).
- **Finalizar/suspender outro aplicativo** - Suspende, retoma ou finaliza um processo (pode ser acessado diretamente pelo Explorador de Processos ou pelo painel Processos).
- **Iniciar novo aplicativo** - Iniciando novos aplicativos ou processos.
- **Modificar o estado de outro aplicativo** - O aplicativo de origem está tentando gravar na memória do aplicativo de destino ou executar um código em seu nome. Este recurso pode ser útil para proteger um aplicativo essencial, configurando-o como um aplicativo de destino em uma regra bloqueando o uso desta operação.



Não é possível interceptar as operações de processos em versões de 64 bits no Windows XP.

Operações de registro

- **Modificar configurações de inicialização** - Quaisquer alterações nas configurações, que definam quais aplicativos serão executados na inicialização do Windows. Esses aplicativos podem ser encontrados, por exemplo, pesquisando pela chave Run no registro do Windows.
- **Excluir do registro** - Exclui uma chave do registro ou seu valor.
- **Renomear chave do registro** - Renomeia chaves do registro.
- **Alterar registro** - Cria novos valores de chaves de registro, alterando os valores existentes, movendo dados na árvore de banco de dados ou configurando direitos de usuário ou de grupos para as chaves do registro.

Usando caracteres curinga nas regras

Um asterisco em uma regra só pode ser usado para substituir uma tecla em particular, por exemplo Um asterisco em uma regra só pode ser usado para substituir uma tecla em particular, por exemplo "HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet*\Start". Outras formas de usar os caracteres curinga não são possíveis.



Criar regras tendo como destino a tecla HKEY_CURRENT_USER

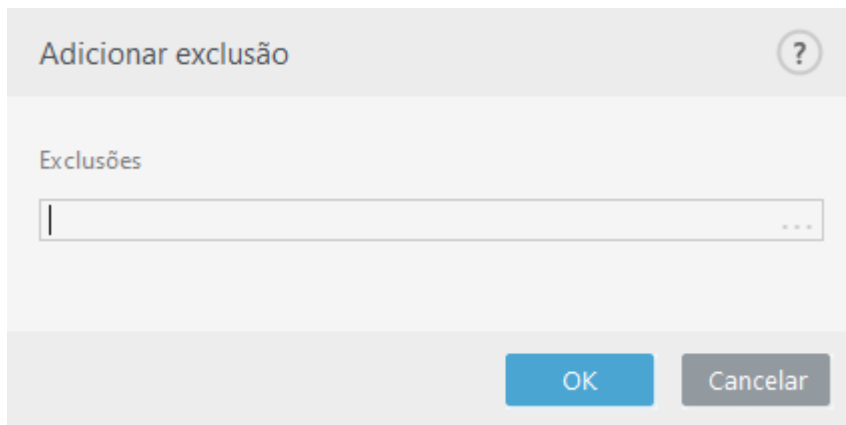
Esta chave é apenas um link para a subchave apropriada HKEY_USERS específica ao usuário SID identificado pelo (identificador seguro). Para criar uma regra apenas para o usuário atual, em vez de usar um caminho para HKEY_CURRENT_USER, use um caminho indo para HKEY_USERS\%SID%. Como SID você pode usar um asterisco para fazer com que a regra seja aplicável para todos os usuários.



Se você criar uma regra muito genérica, o alerta sobre este tipo de regra será exibido.

No exemplo a seguir, demonstraremos como restringir o comportamento indesejado de um aplicativo específico:

1. Nomeie a regra e selecione **Bloquear** (ou **Perguntar** se você preferir escolher posteriormente) do menu suspenso **Ação**.
2. Ative a opção **Notificar usuário** para exibir uma notificação sempre que uma regra for aplicada.
3. Selecione pelo menos uma operação para a qual a regra será aplicada na seção **Operações afetando**.
4. Clique em **Avançar**.
5. Na janela **Aplicativos de origem**, selecione **Aplicativos específicos** no menu suspenso para aplicar sua nova regra a todos os aplicativos que tentarem realizar qualquer uma das operações de aplicativo selecionadas nos aplicativos especificados.
6. Clique em **Adicionar** e em ... para selecionar um caminho para um aplicativo específico, então pressione **OK**. Adicione mais aplicativos se preferir.
Por exemplo: *C:\Program Files (x86)\Untrusted application\application.exe*
7. Selecione a operação **Gravar no arquivo**.
8. Selecione **Todos os arquivos** do menu suspenso. Isso vai bloquear qualquer tentativa de gravação em quaisquer arquivos feitas pelo(s) aplicativo(s) selecionado(s) na etapa anterior.
9. Clique em **Concluir** para salvar sua nova regra.



Configuração avançada HIPS

As opções a seguir são úteis para depurar e analisar o comportamento de um aplicativo:

Unidades sempre com permissão para carregar - As unidades selecionadas sempre tem permissão para carregar, independente do modo de filtragem configurado, a menos que explicitamente bloqueadas pela regra do usuário.

Relatar todas as operações bloqueadas – todas as operações bloqueadas serão gravadas no relatório HIPS. Use este recurso apenas quando estiver fazendo a solução de problemas ou quando for solicitada pelo Suporte técnico da ESET, pois ele pode gerar um relatório enorme e diminuir a velocidade do seu computador.

Notificar quando ocorrerem alterações nos aplicativos de Inicialização - Exibe uma notificação na área de trabalho toda vez que um aplicativo for adicionado ou removido da inicialização do sistema.

Drivers sempre com permissão para carregar

Os drivers exibidos nesta lista sempre terão permissão para carregar, independentemente do modo de filtragem HIPS, a menos que explicitamente bloqueado pela regra do usuário.

Adicionar - Adiciona uma nova unidade.

Editar - Edita a unidade selecionada.

Remover - Remove uma unidade da lista.

Redefinir - recarrega um conjunto de unidades do sistema.

i Clique em **Redefinir** se não quiser que os drivers adicionados manualmente sejam incluídos. Isso pode ser útil se você tiver vários drivers e não for possível excluí-los da lista manualmente.

Modo de apresentação

O modo de apresentação é um recurso para usuários que pretendem usar o seu software continuamente sem serem perturbados por janelas pop-up e que ainda pretendem reduzir o uso da CPU. Ele também pode ser utilizado durante apresentações que não podem ser interrompidas pela atividade do antivírus. Quando ativado,

todas as janelas pop-up são desativadas e tarefas agendadas não são executadas. A proteção do sistema ainda é executada em segundo plano, mas não requer interação com nenhum usuário.

Clique em **Configuração > Computador** e então clique na opção ao lado de **Modo de apresentação para ativar o modo de apresentação manualmente**. Na **Configuração avançada (F5)**, clique em **Ferramentas > Modo de apresentação** e clique na opção ao lado de **Ativar automaticamente o modo de apresentação ao executar aplicativos em tela cheia para que o ESET Endpoint Security ative o modo de apresentação automaticamente quando aplicativos em tela cheia forem executados**. Ativar automaticamente o modo de apresentação é um risco de segurança em potencial, pois o ícone do status de proteção na barra de tarefas ficará laranja e exibirá um aviso. Esse aviso também pode ser visto na janela do programa principal, onde a opção **Modo de apresentação ativado** será exibida em laranja.

Quando a opção **Ativar automaticamente o modo de apresentação ao executar aplicativos em tela cheia for marcada**, o modo de apresentação será iniciado depois que você iniciar um aplicativo em tela cheia e será interrompido automaticamente ao sair do aplicativo. Esse recurso é especialmente útil para iniciar o modo de apresentação logo após iniciar um jogo, abrir um aplicativo em tela cheia ou iniciar uma apresentação.

Você também pode selecionar **Desativar o modo de apresentação automaticamente após** para definir o período de tempo em minutos após o qual o modo de apresentação será desativado automaticamente.

i Se o firewall estiver no modo interativo e o modo de apresentação for ativado, você pode ter dificuldades para conectar-se à Internet. Isso pode ser um problema se você iniciar um jogo on-line. Normalmente, você será solicitado a confirmar tal ação (se não houver regras de comunicação ou exceções definidas), mas a interação com o usuário fará com que o modo de apresentação seja desativado. A solução é definir uma regra de comunicação para cada aplicativo que possa estar em conflito com esse comportamento ou usar outro [Modo de filtragem](#) no firewall. Tenha em mente que, se o modo de apresentação estiver ativado e você acessar uma página da web ou um aplicativo que possa ser considerado um risco à segurança, eles poderão ser bloqueados e nenhuma explicação ou aviso serão exibidos devido à desativação da interação com o usuário.

Rastreamento na inicialização

Por padrão a verificação automática de arquivo na inicialização será realizada na inicialização do sistema e durante a atualização dos módulos. Esse rastreamento depende das [Tarefas e configurações da agenda](#).

As opções de rastreamento na inicialização são parte de uma tarefa da agenda da **Rastreamento de arquivo na inicialização do sistema**. Para modificar suas configurações de rastreamento na inicialização, vá até **Ferramentas > Agenda**, clique em **Verificação automática de arquivos de inicialização** e então em **Editar....** Na última etapa, a janela [Rastreamento automático de arquivo na inicialização](#) será exibida (consulte o capítulo a seguir para obter mais detalhes).

Para obter mais instruções sobre o gerenciamento e a criação de tarefas da Agenda, consulte [Criação de novas tarefas](#).

Rastreamento de arquivos em execução durante

inicialização do sistema

Ao criar uma tarefa agendada de Rastreamento de arquivo na inicialização do sistema, você tem várias opções para ajustar os seguintes parâmetros:

O menu suspenso **Destino de rastreamento** especifica a profundidade do rastreamento para arquivos executados na inicialização do sistema com base em um algoritmo secreto e sofisticado. Os arquivos são organizados em ordem decrescente de acordo com os seguintes critérios:

- **Todos os arquivos registrados** (mais arquivos rastreados)
- **Arquivos usados raramente**
- **Arquivos usados comumente**
- **Arquivos usados com frequência**
- **Somente os arquivos mais frequentemente usados** (últimos arquivos rastreados)

Dois grupos específicos também estão inclusos:

- **Arquivos executados antes do logon do usuário** - Contém arquivos de locais que podem ser acessados sem que o usuário esteja conectado (inclui quase todos os locais de inicialização, tais como serviços, objetos auxiliares do navegador, notificação de Winlogon, entradas da Agenda do Windows, dlls conhecidos, etc.).
- **Arquivos executados após o logon do usuário** - Contém arquivos de locais que podem ser acessados após um usuário se conectar (inclui arquivos que são executados somente para um usuário específico, normalmente arquivos em `HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Run`).

As listas de arquivos a serem rastreados estão fixas para cada grupo anteriormente.

Prioridade do rastreamento - O nível de prioridade usado para determinar quando um rastreamento iniciará:

- **Quando em espera** - a tarefa será realizada somente quando o sistema estiver em espera,
- **Mais baixa** - quando a carga do sistema é a menor possível,
- **Baixa** - em uma carga baixa do sistema,
- **Normal** - em uma carga média do sistema.

Proteção de documentos

O recurso de proteção de documentos verifica os documentos do Microsoft Office antes de eles serem abertos, bem como arquivos obtidos por download automaticamente pelo Internet Explorer, tais como elementos do Microsoft ActiveX. A proteção de documentos fornece uma camada de proteção além da proteção do sistema de arquivos em tempo real, bem como pode ser desativada para aprimorar o desempenho em sistemas que não lidam com um alto volume de documentos do Microsoft Office.

Para ativar a Proteção de documentos, abra a janela **Configuração avançada** (pressione **F5**) > **Mecanismo de detecção** > **Escaneamento de malware** > **Proteção de documentos** e clique na chave **Habilitar proteção de documento**.



Este recurso é ativado por aplicativos que utilizam o Microsoft Antivirus API (por exemplo, Microsoft Office 2000 e superior ou Microsoft Internet Explorer 5.0 e superior).

Exclusões

As **Exclusões** permitem que você exclua [objetos](#) do mecanismo de detecção. Recomendamos que você crie exclusões somente quando for absolutamente necessário, para garantir que todos os objetos sejam escaneados. Situações em que você pode precisar excluir um objeto podem incluir entradas grandes do banco de dados de escaneamento que diminuiriam o desempenho do seu computador durante um escaneamento ou um software que entra em conflito com o escaneamento.

[Exclusões de desempenho](#) permitem a você excluir arquivos e pastas do escaneamento. Exclusões de desempenho são úteis para excluir o escaneamento em nível de arquivo de aplicativos de jogos ou quando um arquivo causa comportamento anormal do sistema ou para aumentar o desempenho.

[Exclusões de detecção](#) permite a você excluir objetos da limpeza usando o nome da detecção, o caminho ou o seu hash. As exclusões de detecção não excluem arquivos e pastas do escaneamento, como é feito pelas exclusões de desempenho. As exclusões de detecção excluem objetos apenas quando eles são detectados pelo mecanismo de detecção e uma regra apropriada está presente na lista de exclusão.

As [exclusões na versão 7.1 e versões anteriores](#) têm as Exclusões de desempenho e Exclusões de detecção unificadas como uma única exclusão.

Não confunda com outros tipos de exclusões:

- [Exclusões de processo](#) – Todas as operações de arquivo atribuídas a processos de aplicativos excluídos são excluídas do escaneamento (pode ser necessário para melhorar a velocidade do backup e a disponibilidade do serviço).
- [Extensões de arquivo excluídas](#)
- [Exclusões HIPS](#)
- [Filtro de exclusões para Proteção baseada em nuvem](#)

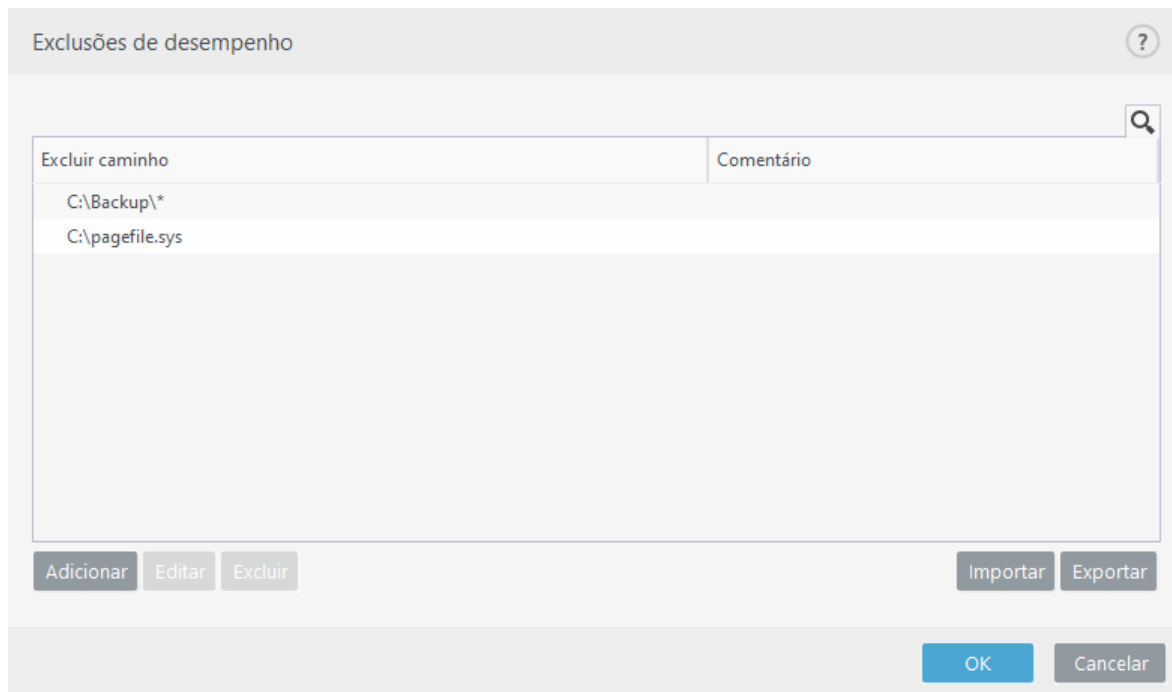
Exclusões de desempenho

Exclusões de desempenho permitem excluir arquivos e pastas do escaneamento.

Recomendamos que você crie exclusões somente quando for absolutamente necessário, para garantir que todos os objetos sejam escaneados contra ameaças. Entretanto, existem situações em que você pode precisar excluir um objeto, por exemplo, entradas extensas do banco de dados que diminuem o desempenho do computador durante um escaneamento ou um software que entra em conflito com o escaneamento.

Você pode adicionar arquivos e pastas para serem excluídos do escaneamento na lista de exclusões via **Configuração avançada (F5) > Mecanismo de detecção > Exclusões > Exclusões de desempenho > Editar**.

Para [excluir um objeto](#) (caminho: ameaça ou pasta) do escaneamento, clique em **Adicionar** e insira o caminho aplicável, ou selecione-o na estrutura em árvore.



Excluir caminho	Comentário
C:\Backup*	
C:\pagefile.sys	

i Uma ameaça em um arquivo não será detectada pelo módulo de **proteção em tempo real do sistema de arquivos** ou módulo de **rastreamento do computador** se um arquivo atender aos critérios para exclusão do rastreamento.

Elementos de controle

- **Adicionar** – Adiciona uma nova entrada para excluir objetos do escaneamento.
- **Editar** - permite que você edite as entradas selecionadas.
- **Remover** – Remove as entradas selecionadas (CTRL + clique para selecionar várias entradas).
- **Importar/Exportar** – A importação e exportação de exclusões de desempenho serão úteis caso você precise fazer backup das exclusões atuais para que ela possa ser utilizada posteriormente. A opção de exportação de configurações também é conveniente para os usuários em ambientes não gerenciados que desejam utilizar as suas configurações preferenciais em diversos sistemas, pois podem importar facilmente um arquivo .txt para transferir essas configurações.

 [Exibir exemplo do formato de arquivo de importação/exportação](#)

```
# {"product":"endpoint","version":"9.1.2060","path":"Settings.ExclusionsManagement.PerformanceExclusions","columns":["Path","Description"]}
```

```
C:\Backup\*,custom comment
```

```
C:\pagefile.sys
```

Adicionar ou editar exclusões de desempenho

Esse diálogo exclui um caminho específico (arquivo ou diretório) para este computador.



Para escolher um caminho apropriado, clique em ... no campo **Caminho**.
Ao inserir o caminho manualmente, veja mais [exemplos de formatos de exclusão](#) abaixo.

Você pode usar caracteres curinga para excluir um grupo de arquivos. Um ponto de interrogação (?) representa um caractere único e um asterisco (*) representa uma cadeia de caracteres, com zero ou mais caracteres.

- Se você deseja excluir todos os arquivos e subpastas em uma pasta, digite o caminho para a pasta e use a máscara *
- Se você deseja excluir somente arquivos doc, use a máscara *.doc
- Se o nome de um arquivo executável tiver um determinado número de caracteres (com caracteres que variam) e você souber somente o primeiro (digamos, "D"), use o seguinte formato: D?????.exe (os pontos de interrogação substituem os caracteres ausentes/desconhecidos)

Exemplos:

- C:\Tools* – O caminho deve terminar com a barra invertida (\) e o asterisco (*) para indicar que é uma pasta e que todo o conteúdo da pasta (arquivos e subpastas) será excluído.
- C:\Tools*. * – O mesmo comportamento que o C:\Tools*
- C:\Tools – A pasta Tools não será excluída. Da perspectiva do escaneador, Tools também pode ser um nome de arquivo.
- C:\Tools*.dat – Excluirá os arquivos .dat na pasta Tools.
- C:\Tools\sg.dat – Excluirá este arquivo em particular localizado no caminho exato.

Você pode usar variáveis do sistema como %PROGRAMFILES% para definir exclusões ao escaneamento.

- Para excluir a pasta de Arquivos de programa usando a variável do sistema, use o caminho %PROGRAMFILES%* (não se esqueça de adicionar a barra invertida e o asterisco no final do caminho) ao adicionar nas exclusões
- Para excluir todos os arquivos em um subdiretório %PROGRAMFILES%, use o caminho %PROGRAMFILES%\Excluded_Directory*

[Expandir a lista de variáveis do sistema suportadas](#)

As variáveis a seguir podem ser usadas no formato de exclusão de caminho:

- %ALLUSERSPROFILE%
- %COMMONPROGRAMFILES%
- %COMMONPROGRAMFILES(X86)%
- %COMSPEC%
- %PROGRAMFILES%
- %PROGRAMFILES(X86)%
- %SystemDrive%
- %SystemRoot%
- %WINDIR%
- %PUBLIC%

Variáveis do sistema específicas para o usuário (como %TEMP% ou %USERPROFILE%) ou variáveis do ambiente (como %PATH%) não são suportadas.

Usar caracteres curinga no meio de um caminho (por exemplo `C:\Tools*\Data\file.dat`) pode funcionar, mas não é oficialmente compatível com as exclusões de desempenho. Consulte o [artigo da Base de conhecimento](#) a seguir para mais informações.

Ao usar [exclusões de detecção](#), não há restrições quanto ao uso de caracteres curinga no meio de um caminho.

Ordem das exclusões:

- Não há opções para ajustar o nível de prioridade das exclusões usando os botões início/fim (como nas [Regras de firewall](#) onde as regras são executadas do início para o fim).
- ✓ • Quando houver uma correspondência com a primeira regra aplicável no escaneador, a segunda regra aplicável não será avaliada.
- Quanto menos regras, melhor o desempenho do escaneamento.
- Evite criar regras que rivalizem entre si.

Formato da exclusão do caminho

Você pode usar caracteres curinga para excluir um grupo de arquivos. Um ponto de interrogação (?) representa um caractere único e um asterisco (*) representa uma cadeia de caracteres, com zero ou mais caracteres.

- Se você deseja excluir todos os arquivos e subpastas em uma pasta, digite o caminho para a pasta e use a máscara *
- Se você deseja excluir somente arquivos doc, use a máscara *.doc
- Se o nome de um arquivo executável tiver um determinado número de caracteres (com caracteres que variam) e você souber somente o primeiro (digamos, "D"), use o seguinte formato: `D?????.exe` (os pontos de interrogação substituem os caracteres ausentes/desconhecidos)

Exemplos:

- ✓ • `C:\Tools*` – O caminho deve terminar com a barra invertida (\) e o asterisco (*) para indicar que é uma pasta e que todo o conteúdo da pasta (arquivos e subpastas) será excluído.
- `C:\Tools*. *` – O mesmo comportamento que o `C:\Tools*`
- `C:\Tools` – A pasta `Tools` não será excluída. Da perspectiva do escaneador, `Tools` também pode ser um nome de arquivo.
- `C:\Tools*.dat` – Excluirá os arquivos .dat na pasta `Tools`.
- `C:\Tools\sg.dat` – Excluirá este arquivo em particular localizado no caminho exato.

Você pode usar variáveis do sistema como `%PROGRAMFILES%` para definir exclusões ao escaneamento.

- Para excluir a pasta de Arquivos de programa usando a variável do sistema, use o caminho `%PROGRAMFILES%*` (não se esqueça de adicionar a barra invertida e o asterisco no final do caminho) ao adicionar nas exclusões
- Para excluir todos os arquivos em um subdiretório `%PROGRAMFILES%`, use o caminho `%PROGRAMFILES%\Excluded_Directory*`

☐ [Expandir a lista de variáveis do sistema suportadas](#)

As variáveis a seguir podem ser usadas no formato de exclusão de caminho:

- `%ALLUSERSPROFILE%`
- `%COMMONPROGRAMFILES%`
- `%COMMONPROGRAMFILES(X86)%`
- `%COMSPEC%`
- `%PROGRAMFILES%`
- `%PROGRAMFILES(X86)%`
- `%SystemDrive%`
- `%SystemRoot%`
- `%WINDIR%`
- `%PUBLIC%`

Variáveis do sistema específicas para o usuário (como `%TEMP%` ou `%USERPROFILE%`) ou variáveis do ambiente (como `%PATH%`) não são suportadas.

Exclusões de detecção

As exclusões de detecção permitem a você excluir objetos da [limpeza](#) ao filtrar por nome da detecção, caminho do objeto ou hash do objeto.

Exclusões de detecção não excluem arquivos e pastas do escaneamento, como é feito com as [Exclusões de desempenho](#). As exclusões de detecção excluem objetos apenas quando eles são detectados pelo mecanismo de detecção e uma regra apropriada está presente na lista de exclusão.

Por exemplo (veja a primeira linha da imagem abaixo), quando um objeto é detectado como Win32/Adware.Optmedia e o arquivo detectado é `C:\Recovery\file.exe`. Na segunda linha, cada arquivo com o hash SHA-1 apropriado sempre será excluído, independentemente do nome de detecção.

Exclusões de detecção

?

Q

Critérios do objeto	Excluir detecção	Comentário
C:\Recovery*.*	Win32/Adware.Optmedia	
2723cb8ca015209528d3fbdcaa801124f4f40ad4	Qualquer detecção	SuperApi.exe

Adicionar

Editar

Excluir

Importar

Exportar

OK

Cancelar

Para garantir que todas as ameaças são detectadas, recomendamos criar exclusões de detecção apenas quando absolutamente necessário.

Você pode adicionar arquivos e pastas na lista de exclusões, **Configuração avançada (F5) > Mecanismo de detecção > Exclusões > Exclusões de detecção > Editar**.

Para [excluir um objeto \(por seu nome de detecção ou hash\)](#) da limpeza, clique em **Adicionar**.

Para [Aplicativos potencialmente indesejados](#) e [Aplicativos potencialmente não seguros](#), também é possível criar a exclusão por seu nome de detecção:

- Na janela de alerta relatando a detecção (clique em **Exibir opções avançadas** e selecione **Excluir da detecção**).
- No menu de contexto do Arquivos de relatório usando o [assistente Criar exclusão de detecção](#).
- Ao clicar em **Ferramentas > Quarentena** e depois clicar com o botão direito no arquivo de quarentena e selecionar **Restaurar e excluir do escaneamento** no menu de contexto.

Critérios do objeto das exclusões de detecção

- **Caminho** – Limita uma exclusão de detecção para um caminho específico (ou para qualquer caminho).
- **Nome da detecção** –se houver um nome de uma [detecção](#) próximo a um arquivo excluído, significa que o arquivo só foi excluído para a determinada detecção, mas não completamente. Se o arquivo for infectado posteriormente com outro malware, ele será detectado.
- **Hash** – Exclui um arquivo com base em um hash específico SHA-1, independentemente do tipo de arquivo, sua localização, nome ou extensão.

Elementos de controle

- **Adicionar** – Adiciona uma nova entrada para excluir objetos da limpeza.

- **Editar** - permite que você edite as entradas selecionadas.
- **Remover** – Remove as entradas selecionadas (CTRL + clique para selecionar várias entradas).
- **Importar/Exportar** – A importação e exportação de exclusões de detecção serão úteis caso você precise fazer backup das exclusões atuais para que ela possa ser utilizada posteriormente. A opção de exportação de configurações também é conveniente para os usuários em ambientes não gerenciados que desejam utilizar as suas configurações preferenciais em diversos sistemas, pois podem importar facilmente um arquivo .txt para transferir essas configurações.

 [Exibir exemplo do formato de arquivo de importação/exportação](#)

```
# {"product":"endpoint","version":"9.1.2060","path":"Settings.ExclusionsManagement.DetectionExclusions","columns":["Id","Path","ThreatName","Description","FileHash"]}
```

```
4c59cd02-357c-4b20-a0ac-ca8400000001,,,SuperApi.exe,00117F70C86ADB0F979021391A8AEAA497C2C8DF
```

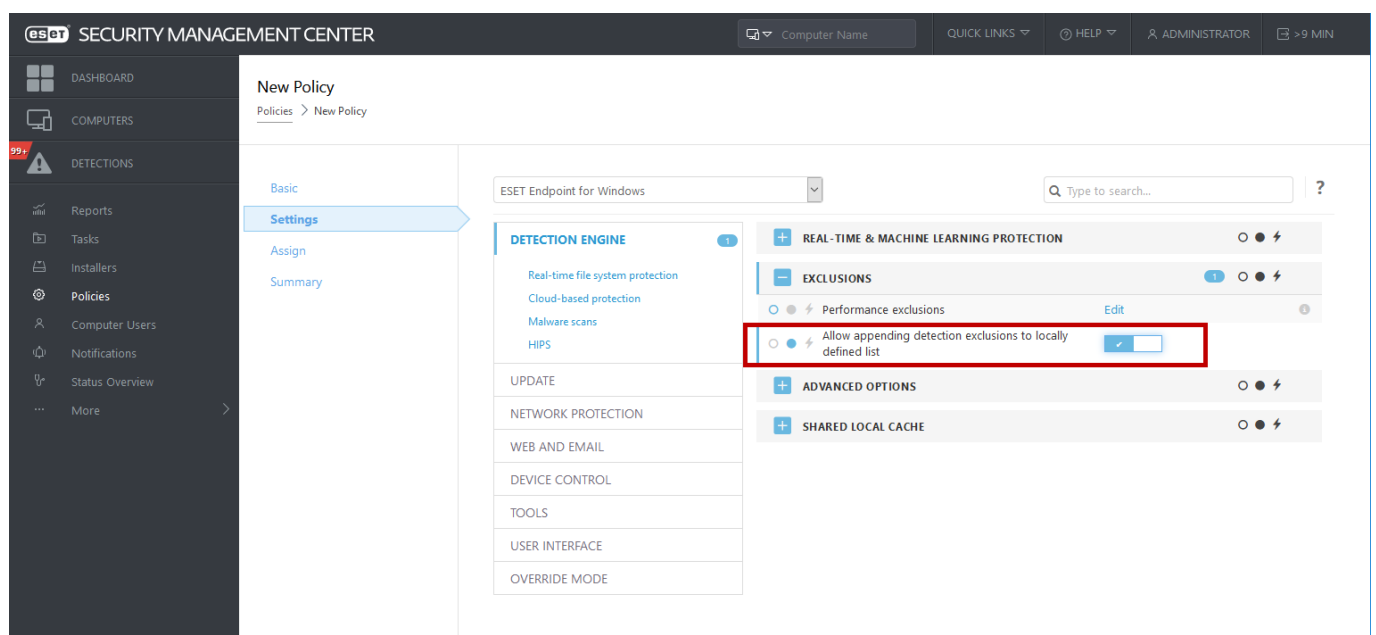
```
2c362ac8-a630-496e-9665-c76d00000001,C:\Recovery\*.*,Win32/Adware.Optmedia,
```

Configuração de exclusões de detecção no ESET PROTECT

O ESET PROTECT 8.0 inclui um [novo assistente para o gerenciamento de exclusões de detecção](#)— crie uma exclusão de detecção e aplique-a a mais computadores/grupos.

Possíveis substituições das exclusões de detecção do ESET PROTECT

Quando houver a presença existente de uma lista local de exclusões de detecção, o administrador deve aplicar uma política com **Permitir anexar exclusões de detecção na lista definida localmente**. Depois disso, anexar exclusões de política do ESET PROTECT vai funcionar conforme esperado.

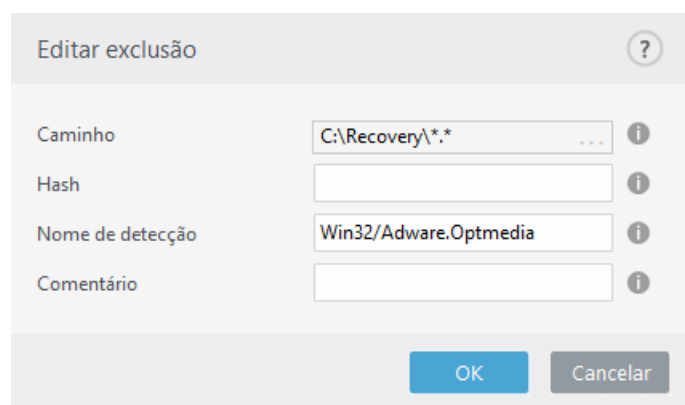


Adicionar ou Editar exclusão de detecção

Excluir detecção

Um nome válido de detecção ESET deve ser fornecido. Para encontrar um nome de detecção válido, consulte os [Arquivos de relatório](#) e selecione **Deteções** no menu suspenso Arquivos de relatório. Isso é útil quando uma [amostra com falso positivo](#) está sendo detectada no ESET Endpoint Security. Exclusões para infiltrações reais são muito perigosas, considere excluir apenas os arquivos/diretórios infectados, clicando em ... no campo **Caminho** e/ou apenas por um período de tempo limitado. As exclusões também são aplicáveis para [Aplicativos potencialmente indesejados](#), aplicativos potencialmente não seguros e aplicativos suspeitos.

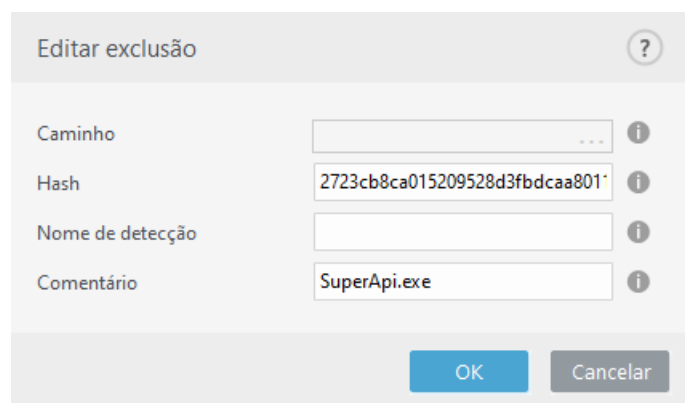
Veja também o [Formato da exclusão do caminho](#).



Veja o [exemplo de Exclusões de detecção](#) abaixo.

Excluir hash

Exclui um arquivo com base em um hash específico SHA-1, independentemente do tipo de arquivo, sua localização, nome ou extensão.



Para excluir uma ameaça específica por nome, digite um nome de detecção válido:

Win32/Adware.Optmedia

Você também pode usar o formato a seguir quando excluir uma detecção da janela de alerta do ESET



Endpoint Security:

@NAME=Win32/Adware.Optmedia@TYPE=ApplicUnwnt

@NAME=Win32/TrojanDownloader.Delf.QQI@TYPE=Trojan

@NAME=Win32/Bagle.D@TYPE=worm

Elementos de controle

- **Adicionar** - exclui objetos da detecção.
- **Editar** - permite que você edite as entradas selecionadas.
- **Remover** – Remove as entradas selecionadas (CTRL + clique para selecionar várias entradas).

Criar assistente de detecção de exclusão

Uma exclusão de detecção também pode ser criada do menu de contexto [Arquivos de relatório](#) (não disponível para detecções de malware):

1. Na janela principal do programa, clique em **Ferramentas > Arquivos de relatório**.
2. Clique com o botão direito em uma detecção no **Relatório de detecções**.
3. Clique em **Criar exclusão**.

Para excluir uma ou mais detecções com base nos **Critérios de exclusão**, clique em **Alterar critérios**:

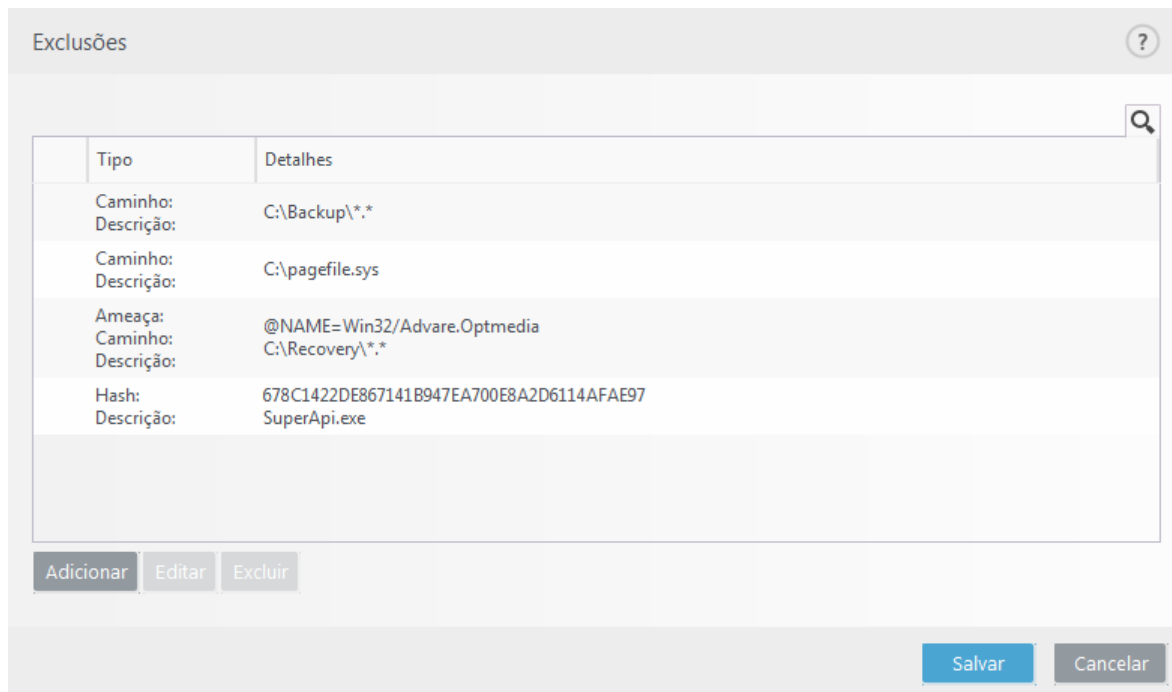
- **Arquivos exatos** – Exclui cada arquivo por seu hash SHA-1.
- **Detecção** – Exclui cada arquivo por seu nome de detecção.
- **Caminho + detecção** – Exclui cada arquivo por seu nome de detecção e caminho, incluindo o nome do arquivo (por exemplo, *file:///C:/Users/user/AppData/Local/Temp/34e1824e/ggdsfdgfd.pdf.exe*).

A opção recomendada é pré-selecionada com base no tipo de detecção.

Opcionalmente, você pode adicionar um **Comentário** antes de clicar em **Criar exclusão**.

Exclusões (7.1 e versões anteriores)

As exclusões na versão 7.1 e versões anteriores têm as [Exclusões de desempenho](#) e [Exclusões de detecção](#) unificadas como uma única exclusão.



Exclusões de processos

O recurso Exclusões de processos permite que você exclua processos de aplicativo da Proteção em tempo real do sistema de arquivos. Para melhorar a velocidade de backup, a integridade do processo e a disponibilidade do serviço, algumas técnicas que sabe-se que criam conflitos com a proteção de malware a nível de arquivo são usadas durante o backup. Problemas similares podem ocorrer ao tentar realizar migrações em tempo real de máquinas virtuais. A única forma eficiente de evitar ambas as situações é desativar o software Anti-Malware. Ao excluir processos específicos (por exemplo, os da solução de backup) todas as operações de arquivo atribuídas a tais processos excluídos são ignoradas e consideradas seguras, minimizando a interferência com o processo de backup. Recomendamos que você tenha cuidado ao criar exclusões. Uma ferramenta de backup que foi excluída pode acessar arquivos infectados sem acionar um alerta, que é o motivo pelo qual permissões estendidas são permitidas apenas no módulo de proteção em tempo real.

Exclusões de processos ajudam a minimizar o risco de conflitos em potencial e melhoram o desempenho de aplicativos excluídos, o que por sua vez tem um efeito positivo no desempenho e estabilidade geral do sistema operacional. A exclusão de um processo/aplicativo é uma exclusão de seu arquivo executável (.exe).

Você pode adicionar arquivos executáveis na lista de processos excluídos via **Configuração avançada (F5) > Mecanismo de detecção > Proteção em tempo real do sistema de arquivos > Exclusões de processos**.

Esse recurso foi feito para excluir ferramentas de backup. Excluir o processo de uma ferramenta de backup do escaneamento não só garante a estabilidade do sistema, como também não afeta o desempenho do backup, já que a velocidade do backup não diminui enquanto ele está em execução.

Clique em **Editar** para abrir a janela de gerenciamento **Exclusões de processos**, onde você pode [adicionar exclusões](#) e procurar por arquivo executável (por exemplo, *Backup-tool.exe*), que será excluído do escaneamento.



Assim que o arquivo .exe for adicionado às exclusões, a atividade desse processo não é monitorada pelo ESET Endpoint Security e nenhum escaneamento é realizado em qualquer operação de arquivo realizada por esse processo.

Se você não usar a função do navegador ao selecionar o executável do processo, será preciso inserir manualmente o caminho completo para o executável. Caso contrário, a exclusão não funcionará corretamente e o [HIPS](#) poderá reportar erros.

Você também pode **Editar** os processos existentes ou **Remover** esses processos das exclusões.

A [proteção de acesso à web](#) não leva em conta essa exclusão, portanto, se você excluir o arquivo executável do seu navegador da web, os arquivos baixados ainda serão escaneados. Assim, ainda será possível detectar uma infiltração. Esse cenário é apenas um exemplo, e não recomendamos criar exclusões para navegadores da web.

Adicionar ou editar exclusões de processos

Com esta janela de diálogo você poderá **adicionar** processos excluídos do mecanismo de detecção. Exclusões de processos ajudam a minimizar o risco de conflitos em potencial e melhoram o desempenho de aplicativos excluídos, o que por sua vez tem um efeito positivo no desempenho e estabilidade geral do sistema operacional. A exclusão de um processo/aplicativo é uma exclusão de seu arquivo executável (.exe).

Selecione o caminho de arquivo de um aplicativo com exceção ao clicar em ... (por exemplo *C:\Program Files\Firefox\Firefox.exe*). NÃO insira o nome do aplicativo.
✓ Assim que o arquivo .exe for adicionado às exclusões, a atividade desse processo não é monitorada pelo ESET Endpoint Security e nenhum escaneamento é realizado em qualquer operação de arquivo realizada por esse processo.

Se você não usar a função do navegador ao selecionar o executável do processo, será preciso inserir manualmente o caminho completo para o executável. Caso contrário, a exclusão não funcionará corretamente e o [HIPS](#) poderá reportar erros.

Você também pode **Editar** os processos existentes ou **Remover** esses processos das exclusões.

Exclusões HIPS

As exclusões possibilitam a você excluir processos da Inspeção comportamental profunda HIPS.

Para excluir um objeto, clique em **Adicionar** e insira o caminho para um objeto ou selecione-o na estrutura em árvore. Também é possível **Editar** ou **Remover** as entradas selecionadas.

[i](#) Consulte o capítulo [Exclusões](#).

Parâmetros ThreatSense

O ThreatSense é composto por vários métodos de detecção de ameaça complexos. Essa tecnologia é proativa, o que significa que ela também fornece proteção durante a propagação inicial de uma nova ameaça. Ela utiliza uma combinação de análise de código, emulação de código, assinaturas genéricas e assinaturas de vírus que funcionam em conjunto para otimizar significativamente a segurança do sistema. O mecanismo de rastreamento é capaz de controlar diversos fluxos de dados simultaneamente, maximizando a eficiência e a taxa de detecção. A tecnologia ThreatSense também elimina os rootkits com êxito.

As opções de configuração do motor ThreatSense permitem que você especifique diversos parâmetros de rastreamento:

- Tipos e extensões de arquivos que serão escaneados
- A combinação de diversos métodos de detecção
- Níveis de limpeza etc.

Para acessar a janela de configuração, clique em **parâmetros ThreatSense** na janela de Configuração avançada de qualquer módulo que use a tecnologia ThreatSense (consulte a seguir). Cenários de segurança diferentes podem precisar de configurações diferentes. Com isso em mente, o ThreatSense é individualmente configurável para os módulos de proteção a seguir:

- Proteção em tempo real do sistema de arquivos
- Rastreamento em estado ocioso
- Rastreamento na inicialização
- Proteção de documentos
- Proteção do cliente de email
- Proteção do acesso à Web
- Escanear o computador

Os parâmetros do ThreatSense são altamente otimizados para cada módulo, e modificá-los pode influenciar significativamente a operação do sistema. Por exemplo, alterar parâmetros para sempre verificar empacotadores em tempo real ou ativar a heurística avançada no módulo de Proteção em tempo real do sistema de arquivos pode resultar em maior utilização dos recursos (normalmente, somente arquivos recém-criados são verificados utilizando esses métodos). Recomendamos que mantenha os parâmetros padrão do ThreatSense inalterados para todos os módulos, exceto Escanear o computador.

Objetos a serem escaneados

Esta seção permite definir quais componentes e arquivos do computador serão rastreados quanto a infiltrações.

Memória operacional - Rastreia procurando ameaças que atacam a memória operacional do sistema.

Setores de inicialização/UEFI – Escaneia os setores de inicialização quanto à presença de malware no registro de inicialização principal. [Leia mais sobre UEFI no glossário.](#)

Arquivos de e-mail - O programa é compatível com as extensões a seguir: DBX (Outlook Express) e EML.

Arquivos – O programa é compatível com as extensões a seguir: ARJ, BZ2, CAB, CHM, DBX, GZIP, ISO/BIN/NRG, LHA, MIME, NSIS, RAR, SIS, TAR, TNEF, UUE, WISE, ZIP, ACE, e muito mais.

Arquivos de auto extração – Arquivos de auto extração (SFX) são arquivos que podem extrair a si mesmos.

Compactadores em tempo real – depois de serem executados, compactadores em tempo real (ao contrário dos arquivos compactados padrão) são descompactados na memória. Além dos empacotadores estáticos padrão (UPX, yoda, ASPack, FSG etc.), o scanner é compatível com o reconhecimento de vários tipos adicionais de empacotadores graças à emulação do código.

Opções de escaneamento

Selecione os métodos a serem utilizados durante o escaneamento do sistema para verificar infiltrações. As opções disponíveis são:

Heurística - Uma heurística é um algoritmo que analisa a atividade (maliciosa) dos programas. A principal

vantagem dessa tecnologia é a capacidade de identificar software malicioso que não existia ou que não era conhecido pela versão anterior do mecanismo de detecção. A desvantagem é uma probabilidade (muito pequena) de alarmes falsos.

Heurística avançada/assinaturas de DNA - A heurística avançada é um algoritmo heurístico exclusivo desenvolvido pela ESET, otimizado para a detecção de worms de computador e cavalos de troia e escritos em linguagens de programação de alto nível. O uso de heurística avançada aumenta muito as capacidades de detecção de ameaças de produtos ESET. As assinaturas podem detectar e identificar vírus com segurança. Usando o sistema de atualização automática, novas assinaturas são disponibilizadas em poucas horas depois da descoberta da ameaça. A desvantagem das assinaturas é que elas detectam somente os vírus que conhecem (ou suas versões levemente modificadas).

Limpeza

As [configurações de limpeza](#) determinam o comportamento do ESET Endpoint Security enquanto limpa os objetos.

Exclusões

Uma extensão é a parte do nome de arquivo delimitada por um ponto final. A extensão define o tipo e o conteúdo do arquivo. Essa seção de configuração de parâmetros do ThreatSense permite definir os tipos de arquivos a serem rastreados.

Outros

Ao configurar os parâmetros do mecanismo ThreatSense para um rastreamento sob demanda do computador, as seguintes opções na seção **Outro** também estarão disponíveis:

Rastrear fluxos dados alternativos (ADS) - Fluxos de dados alternativos usados pelo sistema de arquivos NTFS são associações de arquivos e pastas invisíveis às técnicas comuns de rastreamento. Muitas infiltrações tentam evitar a detecção disfarçando-se de fluxos de dados alternativos.

Executar escaneamento em segundo plano com baixa prioridade - Cada sequência de escaneamento consome determinada quantidade de recursos do sistema. Se você estiver trabalhando com programas que exigem pesados recursos do sistema, você poderá ativar o escaneamento em segundo plano prioridade em segundo plano e economizar recursos para os aplicativos.

Fazer relatório de todos os objetos – O [Relatório do escaneamento](#) exibirá todos os arquivos escaneados em arquivos de extração automática, mesmo aqueles que não estão infectados (pode gerar muitos dados de relatórios de escaneamento e aumentar o tamanho do arquivo do relatório do escaneamento).

Ativar otimização inteligente - Com a Otimização inteligente ativada, as configurações mais ideais são utilizadas para garantir o nível mais eficiente de escaneamento, mantendo simultaneamente a velocidade de rastreamento mais alta. Os diversos módulos de proteção fazem rastreamento de maneira inteligente, utilizando diferentes métodos de rastreamento e os aplicando a tipos específicos de arquivos. Se a Otimização inteligente estiver desativada, somente as configurações definidas pelo usuário no núcleo do ThreatSense do módulo particular serão aplicadas durante a realização de um escaneamento.

Manter último registro de acesso - Selecione essa opção para manter o tempo de acesso original dos arquivos escaneados, em vez de atualizá-lo (por exemplo, para uso com sistemas de backup de dados).

Limites

A seção Limites permite especificar o tamanho máximo de objetos e nível de compactação de arquivos compactados a serem rastreados:

Configurações do objeto


Tamanho máximo do objeto - Define o tamanho máximo de objetos a serem rastreados. O módulo antivírus determinado rastreará apenas objetos menores que o tamanho especificado. Essa opção apenas será alterada por usuários avançados que podem ter razões específicas para excluir objetos maiores do escaneamento. Valor padrão: sem limite.

Tempo máximo do escaneamento para objeto (seg) – define o valor de tempo máximo para o escaneamento de arquivos em um objeto de container (como um arquivo RAR/ZIP ou um e-mail com vários anexos). Esta configuração não é aplicável para arquivos autônomos. Se um valor definido pelo usuário for inserido e esse tempo tiver decorrido, um escaneamento será interrompido assim que possível, independentemente do escaneamento de cada arquivo em um objeto container ter sido concluído. No caso de um arquivo com arquivos grandes, o escaneamento não vai parar antes de um arquivo do arquivo ser extraído (por exemplo, quando uma variável definida pelo usuário é de 3 segundos, mas a extração de um arquivo leva 5 segundos). O resto dos arquivos no arquivo não será escaneado quando o tempo tiver decorrido. Para limitar o tempo de escaneamento, incluindo arquivos maiores, use o **Tamanho máximo do objeto** e o **tamanho máximo do arquivo no arquivo** (não recomendado devido a possíveis riscos de segurança). Valor padrão: sem limite.

Configuração de escaneamento de arquivo

Nível de compactação de arquivos - Especifica a profundidade máxima do escaneamento de arquivos compactados. Valor padrão: 10.

Tamanho máximo do arquivo no arquivo compactado - Essa opção permite especificar o tamanho máximo de arquivos para os arquivos contidos em arquivos compactados (quando são extraídos) a serem escaneados. O valor máximo é 3 GB.

 Não recomendamos alterar os valores padrão; sob circunstâncias normais, não haverá razão para modificá-los.

Níveis de limpeza

Para acessar as configurações de nível de limpeza para um módulo de proteção desejado, expanda os **Parâmetros ThreatSense** (por exemplo, **Proteção em tempo real do sistema de arquivos**) e clique em **Limpeza**.

A Proteção em tempo real e outros módulos de proteção têm os seguintes níveis de correção (ou seja, limpeza).

Correção no ESET Endpoint Security 9

Nível de limpeza	Descrição
Sempre corrigir a detecção	Tenta corrigir a detecção durante a limpeza dos objetos sem qualquer intervenção do usuário final. Em alguns casos raros (por exemplo, arquivos do sistema), se a detecção não puder ser corrigida, o objeto reportado será deixado em sua localização original. Sempre corrigir a detecção é a configuração padrão recomendada em um ambiente gerenciado .
Corrigir a detecção se for seguro, se não, manter	Tenta corrigir a detecção durante a limpeza dos objetos sem nenhuma intervenção do usuário final. Em alguns casos (por exemplo, arquivos do sistema ou arquivos contendo arquivos limpos e infectados), se a detecção não puder ser corrigida, o objeto reportado será deixado em sua localização original.
Corrigir a detecção se for seguro, se não, perguntar	Tenta corrigir a detecção durante a limpeza dos objetos. Em alguns casos, se nenhuma ação puder ser realizada, o usuário final recebe um alerta interativo e deve selecionar uma ação de correção (por exemplo, remover ou ignorar). Essa configuração é recomendada na maioria dos casos.
Sempre perguntar ao usuário final	O usuário final recebe uma janela interativa enquanto limpa os objetos e deve selecionar uma ação de correção (por exemplo, remover ou ignorar). Esse nível foi feito para usuários mais avançados que sabem qual etapa deve ser tomada no caso de uma detecção.



Extensões de arquivo excluídas do rastreamento

Uma extensão é a parte do nome de arquivo delimitada por um ponto final. A extensão define o tipo e o conteúdo do arquivo. Essa seção de configuração de parâmetros do ThreatSense permite definir os tipos de arquivos a serem rastreados.

i Não confunda com outros tipos de [Exclusões](#).

Por padrão, todos os arquivos são escaneados. Qualquer extensão pode ser adicionada à lista de arquivos excluídos do rastreamento.

A exclusão de arquivos será necessária algumas vezes se o rastreamento de determinados tipos de arquivos impedir o funcionamento correto do programa que está usando certas extensões. Por exemplo, pode ser aconselhável excluir as extensões `.edb`, `.eml` e `.tmp` ao usar os servidores Microsoft Exchange.

Para adicionar uma nova extensão à lista, clique em **Adicionar**. Digite a extensão no campo em branco (por exemplo `tmp`) e clique em **OK**. Quando você selecionar **Inserir valores múltiplos**, você poderá adicionar várias extensões de arquivos delimitadas por linhas, vírgulas ou ponto e vírgulas (por exemplo, escolha **Ponto e vírgula** do menu suspenso como separador, e digite `edb;eml;tmp`).

Você pode usar um símbolo especial `?` (ponto de interrogação). O ponto de interrogação representa qualquer símbolo (por exemplo `?db`).

i Para ver a extensão exata (se houver) de um arquivo em um sistema operacional Windows é preciso desmarcar a opção **Ocultar extensões para tipos de arquivos conhecidos** no **Painel de controle > Opções de pasta > Exibição** (guia) e aplicar esta alteração.

Parâmetros adicionais do ThreatSense


Parâmetros ThreatSense adicionais para arquivos criados e modificados recentemente - A probabilidade de infecção em arquivos criados ou modificados recentemente é comparativamente maior do que nos arquivos existentes. Por esse motivo, o programa verifica esses arquivos com parâmetros de rastreamento adicionais. Além dos métodos comuns de rastreamento baseados em assinaturas, também é usada a heurística avançada, que pode detectar novas ameaças antes do lançamento da atualização do mecanismo de detecção. Além dos arquivos recém-criados, o rastreamento é executado em arquivos de autoextração (.sfx) e em empacotadores em tempo real (arquivos executáveis compactados internamente). Por padrão, os arquivos compactados são rastreados até o décimo nível de compactação e são verificados, independentemente do tamanho real deles. Para modificar as configurações de rastreamento em arquivos compactados, desative **Configurações padrão de rastreamento em arquivos compactados**.

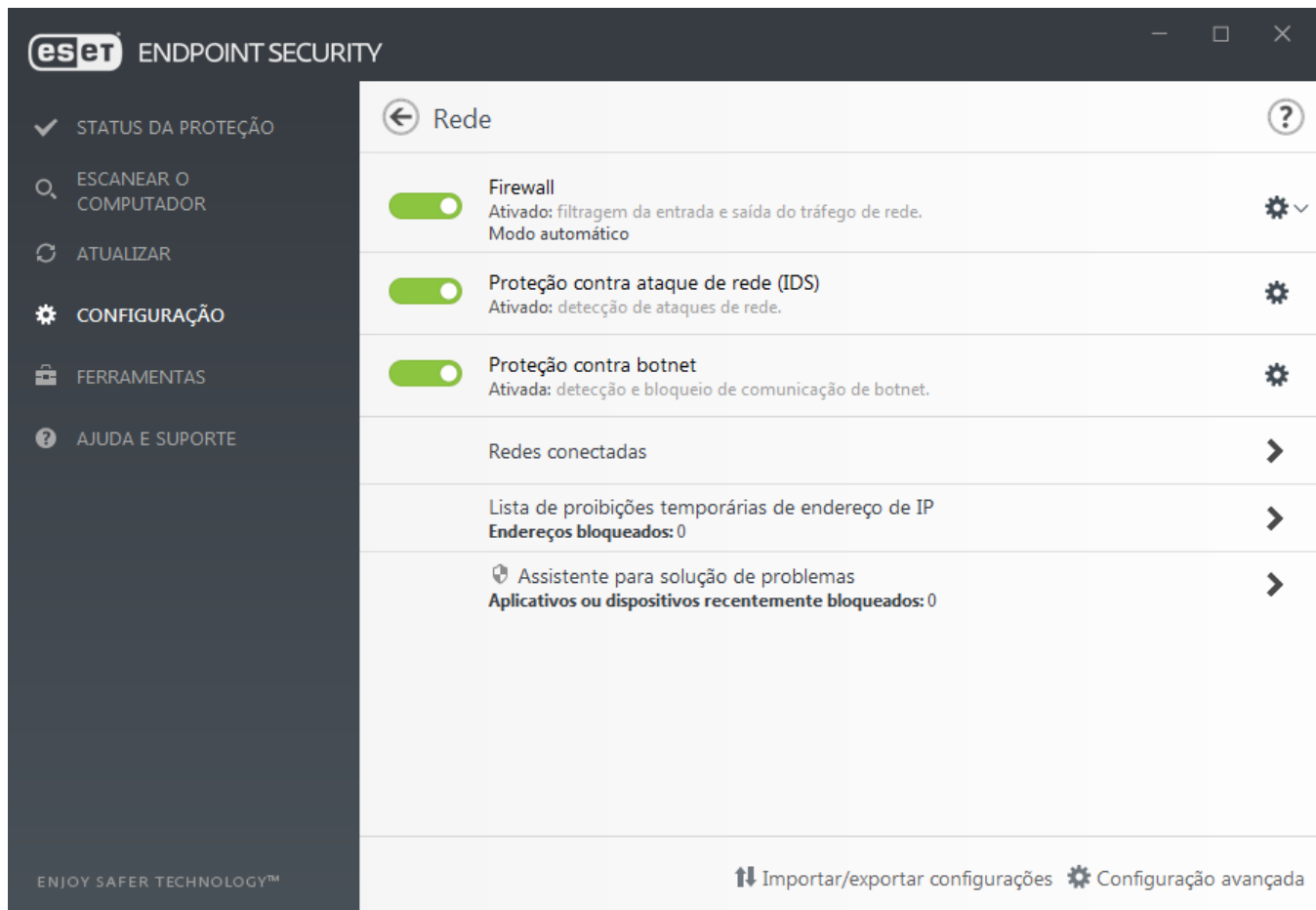
Para saber mais sobre Empacotadores em tempo real, Arquivos compactados de auto extração e Heurística avançada consulte a configuração de parâmetros do mecanismo do [ThreatSense](#).

ThreatSense Parâmetros adicionais para arquivos executados - por padrão, [Heurística avançada](#) é usada quando os arquivos são executados. Quando ativada, é altamente recomendado manter a [Otimização inteligente](#) e o ESET LiveGrid® ativados para minimizar o impacto no desempenho do sistema.

Rede

A seção **Rede** permite a você um acesso rápido aos componentes ou configurações a seguir na **Configuração avançada**:

- **Firewall** – Aqui você pode ajustar o modo de filtragem do [Firewall da ESET](#). Para acessar configurações mais detalhadas, clique na engrenagem ⚙ > **Configurar** ao lado de **Firewall**, ou pressione **F5** para acessar a **Configuração avançada**.
- [Proteção contra ataque de rede \(IDS\)](#) - Analisa o conteúdo do tráfego da rede e protege contra ataques de rede. Qualquer tráfego que seja considerado danoso será bloqueado. O ESET Endpoint Security vai informar você quando for feita uma conexão a uma rede sem fio não protegida ou a uma rede com proteção fraca.
- **Proteção contra botnet** – Identifica de forma rápida e precisa o malware no sistema. Para desativar a Proteção contra botnet por um período de tempo específico, clique em  (não recomendado).
- **Redes conectadas** - Mostra as redes às quais os adaptadores de rede estão conectados. Clique no ícone de engrenagem ⚙ para selecionar um tipo de proteção para a rede à qual você está conectado. Clique em **Redes conectadas** > **Adaptadores de rede** para ver cada adaptador de rede e seu perfil de firewall e zona confiável atribuídos. Para obter informações mais detalhadas, consulte [Adaptadores de rede](#).
- **Lista de proibições temporária de endereço IP** - Exibe uma lista de endereços de IP que foram detectados como a fonte de ataques e adicionados à lista de proibições para bloquear a conexão por um período de tempo. Para mais informações, clique nesta opção e pressione **F1**.
- **Assistente de solução de problemas** - O assistente de solução de problemas ajuda a resolver problemas de conectividade causados pelo Firewall ESET. Para obter informações mais detalhadas, consulte [Assistente de solução de problemas](#).



Clique na engrenagem  ao lado do **Firewall** para acessar as seguintes configurações:

- **Configurar** - Abre a janela Firewall na Configuração avançada, que permite definir como o firewall tratará a comunicação de rede.
- **Bloquear todo o tráfego** - Todas as comunicação de entrada e saída serão bloqueadas pelo Firewall. Utilize essa opção somente se suspeitar de riscos de segurança críticos que requeiram a desconexão do sistema da rede. Para restaurar o firewall para a operação normal enquanto a filtragem do tráfego de rede está no modo **Bloquear todo o tráfego**, clique em **Parar de bloquear todo o tráfego**.
- **Pausar firewall (permitir todo o tráfego)** - O contrário do bloqueio de todo o tráfego da rede. Se estiver selecionado, todas as opções de filtragem do Firewall serão desativadas, e todas as conexões de entrada e de saída serão permitidas. Para reativar o firewall enquanto a Filtragem de tráfego de rede está neste modo, clique em **Ativar firewall**.
- **Modo automático** - (quando outro modo de filtragem está ativado) - Clique para trocar o modo de filtragem para modo de filtragem automático (com regras definidas pelo usuário).
- **Modo interativo** - (quando outro modo de filtragem está ativado) - Clique para trocar o modo de filtragem para modo de filtragem interativo.

Firewall

O Firewall controla todo o tráfego de rede para e a partir do sistema. Isso é realizado através da permissão ou proibição de conexões individuais de rede, com base em regras de filtragem especificadas. Fornece proteção contra ataques de computadores remotos e pode bloquear alguns serviços possivelmente perigosos.

Básico

Ativar firewall

Recomendamos que deixe este recurso ativado para garantir a segurança do seu sistema. Com o firewall ativado, o tráfego de rede é rastreado em ambas as direções.

Avaliar também as regras do Windows Firewall

No modo automático, permitir também o tráfego de entrada permitido pelas regras do Windows Firewall, a menos que seja explicitamente bloqueado por regras ESET.

 Regras do Firewall do Windows configuradas usando a Política de Grupo (GPO) não são avaliadas.

Modo de filtragem

O comportamento do firewall é alterado com base no modo de filtragem. Os modos de filtragem também influenciam o nível de interação necessário do usuário.

Os modos de filtragem a seguir estão disponíveis para o Firewall do ESET Endpoint Security:

Modo de filtragem	Descrição
Modo automático	O modo padrão. Esse modo é adequado para usuários que preferem o uso fácil e conveniente do firewall sem necessidade de definir regras. Regras personalizadas e definidas pelo usuário podem ser criadas, mas não são exigidas no modo automático . O modo automático permite todo tráfego de saída para um determinado sistema e bloqueia a maioria do tráfego de entrada, exceto algum tráfego da zona confiável (como especificado em IDS e opções avançadas/serviços permitidos) e responde a comunicações de saída recente.
Modo interativo	Permite que você crie uma configuração personalizada para seu Firewall. Quando uma comunicação para a qual não há regras aplicadas for detectada, será exibida uma janela de diálogo com a informação de uma conexão desconhecida. A janela de diálogo dá a opção de permitir ou negar a comunicação, e a decisão de permitir ou negar pode ser salva como uma nova regra para o Firewall. Se o usuário escolher criar uma nova regra, todas as futuras conexões desse tipo serão permitidas ou bloqueadas de acordo com essa regra.
Modo com base em políticas	Bloqueia todas as conexões que não são definidas por uma regra específica que as permite. Esse modo permite que os usuários avançados definam as regras que permitem apenas as conexões desejadas e seguras. Todas as outras conexões não especificadas serão bloqueadas pelo Firewall.
Modo de aprendizagem	Cria e salva regras automaticamente, este modo é melhor usado para a configuração inicial do Firewall, mas não deve ser deixado ativado durante longos períodos de tempo. Nenhuma interação com o usuário é exigida, porque o ESET Endpoint Security salva as regras de acordo com os parâmetros predefinidos. O modo de aprendizagem não deve ser apenas usado até que todas as regras para as comunicações exigidas tenham sido criadas para evitar riscos de segurança.

[Perfis](#) podem ser usados para personalizar o comportamento do Firewall do ESET Endpoint Security ao especificar diferentes conjuntos de regras em diferentes situações.

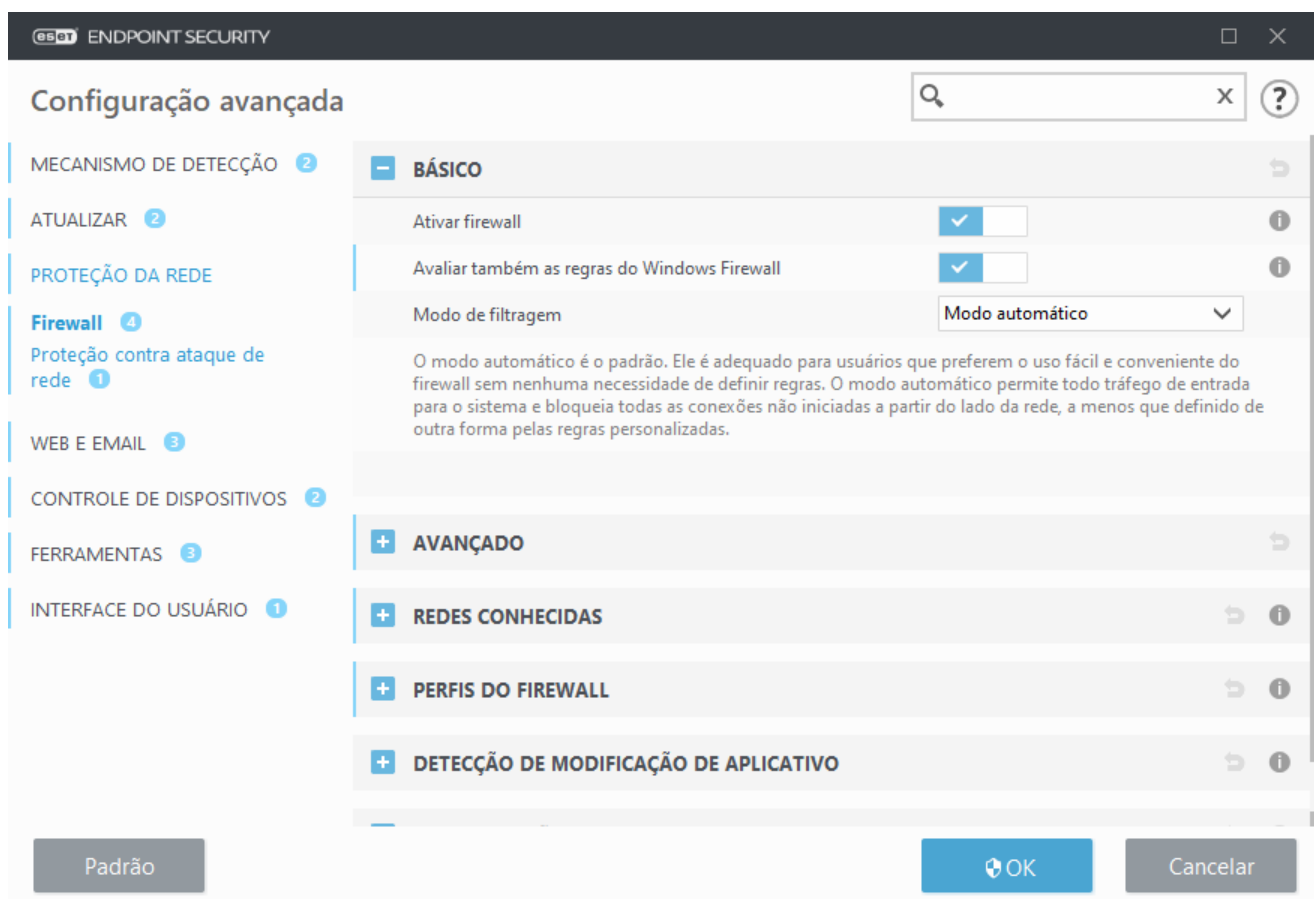
Avançado

Regras

A configuração de regras permite que você visualize todas as regras aplicadas ao tráfego gerado por aplicativos individuais nas zonas confiáveis e na Internet.

Zonas

Uma zona representa uma coleção de endereços de rede que criam um grupo lógico.



É possível criar uma regra IDS quando o [Botnet](#) atacar seu computador. Uma exceção pode ser modificada em **Configuração avançada (F5) > Proteção da rede > Proteção contra ataque de rede > Regras IDS** clicando em **Editar**.

Modo de aprendizagem

O modo de aprendizagem cria e salva automaticamente uma regra para cada comunicação que foi estabelecida no sistema. Nenhuma interação com o usuário é exigida, porque o ESET Endpoint Security salva as regras de acordo com os parâmetros predefinidos.

Esse modo pode expor seu sistema a risco e é recomendado somente para configuração inicial do Firewall.





Selecione **Modo de aprendizagem** do menu suspenso em **Configuração avançada (F5) > Firewall > Básico > Modo de filtragem** para ativar as **Opções do modo de aprendizagem**. Essa seção inclui os seguintes itens:



Enquanto está no Modo de aprendizagem, o Firewall não filtra a comunicação. Todas as comunicações de saída e de entrada são permitidas. Nesse modo, o seu computador não está totalmente protegido pelo Firewall.

Modo definido depois da expiração do modo de aprendizagem – Define para qual modo de filtragem o Firewall do ESET Endpoint Security vai ser revertido depois do período de tempo de aprendizagem terminar. Leia mais sobre [modos de filtragem](#). Depois da expiração, a opção Perguntar ao usuário exige privilégios de administrador para realizar uma alteração no modo de filtragem do firewall.

Tipo de comunicação - Selecione os parâmetros específicos de criação de regras para cada tipo de comunicação. Há quatro tipos de comunicação:

-  **Tráfego de entrada da Zona confiável** - Um exemplo de uma conexão de entrada na zona confiável seria um computador remoto a partir do qual a zona confiável está tentando estabelecer comunicação com um aplicativo local em execução no seu computador.
-  **Tráfego de saída para zona Confiável** - Um aplicativo local está tentando estabelecer uma conexão com outro computador na rede local ou em uma rede na zona confiável.
-  **Tráfego de entrada da Internet** - Um computador remoto tentando se comunicar com um aplicativo em execução no computador.
-  **Tráfego de saída da Internet** - Um aplicativo local está tentando estabelecer uma conexão com outro computador.

Cada seção permite que você defina parâmetros a serem adicionados às regras recém-criadas:

Adicionar porta local - Inclui o número da porta local da comunicação de rede. Para as comunicações de saída, números aleatórios são frequentemente gerados. Por essa razão, recomendamos a ativação dessa opção apenas para as comunicações de entrada.

Adicionar aplicativo – Inclui o nome do aplicativo local. Essa opção é adequada para regras de nível de aplicativo (regras que definem a comunicação para um aplicativo inteiro). Por exemplo, é possível ativar a comunicação apenas para um navegador da Web ou cliente de email.

Adicionar porta remota - Inclui o número da porta remota da comunicação de rede. Por exemplo, você pode permitir ou negar um serviço específico associado a um número de porta padrão (HTTP - 80, POP3 - 110, etc.).

Adicionar endereço IP remoto/Zona confiável - Um endereço IP ou uma zona remoto(a) pode ser utilizado(a) como um parâmetro para novas regras que definem todas as conexões de rede entre o sistema local e esse endereço/zona remoto(a). Essa opção é adequada se você desejar definir ações para determinado computador ou grupo de computadores conectados em rede.

Número máximo de regras diferentes para um aplicativo - Se um aplicativo comunicar por meio de diferentes portas para vários endereços IP etc., o firewall no modo de aprendizagem criará uma contagem apropriada de regras para esse aplicativo. Essa opção permite limitar o número de regras que podem ser criadas para um aplicativo.

Proteção de ataque a rede

Ativar Proteção de ataque a rede (IDS) - Analisa o conteúdo do tráfego da rede e protege contra ataques de rede. Qualquer tráfego que seja considerado perigoso será bloqueado.

Ativar proteção contra botnet - Detecta e bloqueia comunicação com comandos maliciosos e servidores de controle com base em padrões típicos quando o computador está infectado e um bot está tentando se comunicar. [Leia mais sobre a Proteção contra botnet no glossário.](#)

Regras IDS – Esta opção permite configurar opções avançadas de filtro para detectar vários tipos de ataques e vulnerabilidades que podem ser usados para danificar seu computador.

Proteção contra ataque de força bruta

A proteção contra ataque de força bruta bloqueia ataques sem senha para serviços RDP e SMB. Um ataque de força bruta é um método de descobrir uma senha específica ao tentar sistematicamente todas as combinações de letras, números e símbolos. Para configurar a Proteção contra ataque de força bruta, na [janela principal do programa](#), clique em **Configuração > Configuração avançada (F5) > Proteção da rede > Proteção contra ataque de rede > Proteção contra ataque de força bruta**.

Ativar proteção contra ataque de força bruta – o ESET Endpoint Security inspeciona o conteúdo do tráfego da rede e bloqueia tentativas de ataques sem senhas.

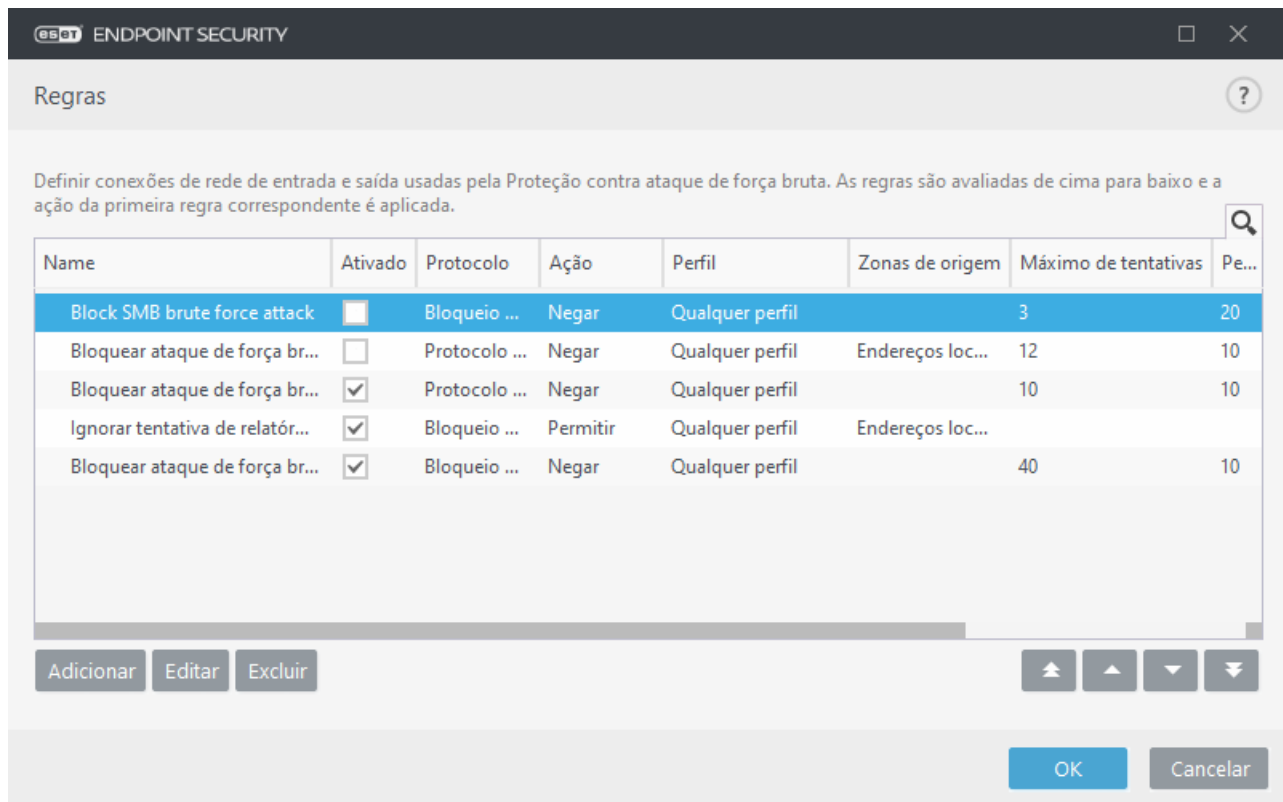
Regras – permite que você crie, edite e veja as regras para conexões de rede de entrada e saída. Para obter mais informações, consulte o [capítulo Regras](#).





Exclusões – lista de detecções excluídas definidas por um endereço IP ou caminho de aplicativo. Você pode criar e editar exclusões no seu console ESET PROTECT. Para obter mais informações, consulte o capítulo [Exclusões](#).

Regras

As regras de proteção contra ataque de força bruta permitem que você crie, edite e veja as regras para conexões de rede de entrada e saída. As regras pré-definidas não podem ser editadas ou removidas.

Gerenciar regras de Proteção contra ataque com força bruta



- **Adicionar** – clique para criar uma nova regra de proteção contra ataque de força bruta.
- **Editar** – clique para editar uma regra de proteção contra ataque de força bruta existente.
- **Remover** – selecione e clique se quiser remover uma exceção existente da lista de regras IDS.
-     **Início/Para cima/Final/Para baixo** – permite que você ajuste o nível de prioridade de regras.

i Para garantir a proteção mais alta possível, a regra de bloqueio com o menor valor de **Máximo de tentativas** é aplicada mesmo se a regra estiver posicionada mais baixo na lista de Regras quando várias regras de bloqueio são correspondentes às condições de detecção.

Editor de regras

Editar regra

Nome: Block SMB brute force attack

Ativado: ☒ X

Ação: Negar

Protocolo: Bloqueio de mensagem do servidor (SMB)

Perfil: Qualquer perfil

Máximo de tentativas: 3

Período de retenção na lista de proibições (min): 20

IP de origem:

Zonas de origem:

Adicionar Excluir

OK

Nome – nome da regra.

Ativado – desative a barra deslizante se deseja manter a regra na lista, mas não deseja aplicá-la.

Ação – escolha se quer **Negar** ou **Permitir** a conexão se as configurações de regra forem cumpridas.

Protocolo – o protocolo de comunicação que esta regra vai inspecionar.

Perfil – regras personalizadas podem ser definidas e aplicadas para perfis específicos.

Máximo de tentativas – O número máximo de tentativas permitidas de repetição de ataque até que o endereço IP seja bloqueado e adicionado à lista de proibições.

Período de retenção na lista de proibições (min) – define o tempo para a expiração do endereço da lista de proibições.

IP de origem – uma lista de endereços IP/intervalos/sub-redes. Vários endereços devem ser separados por vírgula.

Zonas de origem – permite adicionar uma zona pré-definida ou criada com um intervalo de endereços IP aqui clicando em **Adicionar**.

Exclusões

Exclusões de força bruta podem ser usadas para suprimir a detecção de Força bruta para critérios específicos. Essas exclusões são criadas com ESET PROTECT base na detecção de força bruta.

Colunas


- **Deteção** – tipo de detecção.
- **Aplicativo** – Selecione o caminho de arquivo de um aplicativo com exceção ao clicar em ... (por exemplo *C:\Program Files\Firefox\Firefox.exe*). NÃO insira o nome do aplicativo.
- **IP remoto** – Uma lista de endereço / intervalos / sub-redes IPv4 ou IPv6 remoto. Vários endereços devem ser separados por vírgula.


Gerenciamento de exclusões

As exclusões serão exibidas se um administrador [criar exclusões de Força bruta no Web Console ESET PROTECT](#). As exclusões podem ter apenas regras de permissão e serão avaliadas antes das regras IDS.

Opções de filtragem avançadas

As seções de Firewall e Proteção contra ataque de rede permitem a você configurar opções de filtragem avançadas para detectar vários tipos de ataques e vulnerabilidades que podem ser realizados contra seu computador.

 em alguns casos, você não receberá uma modificação de ameaça sobre comunicações bloqueadas. Consulte a seção [Registrando e criando regras ou exceções de relatório](#) para obter instruções para visualizar todas as comunicações bloqueadas no relatório do Firewall.

 A disponibilidade de opções em particular na **Configuração avançada (F5) > Proteção da rede > Firewall e Configuração avançada (F5) > Proteção da rede > Proteção contra ataque de rede** pode variar dependendo do tipo ou versão do seu módulo de firewall, e também da versão do seu sistema operacional.

Serviços permitidos

As configurações neste grupo têm como objetivo simplificar a configuração do acesso aos serviços deste computador a partir da zona confiável. Muitas delas ativam/desativam regras de firewall predefinidas.

- **Permitir compartilhamento de arquivos e impressoras na zona Confiável** - Permite que computadores remotos na zona confiável acessem seus arquivos e impressoras compartilhados.
- **Permitir UPnP para serviços do sistema na zona Confiável** - permite a entrada e saída de solicitações de protocolos UPnP para serviços do sistema. UPnP (Universal Plug and Play, também conhecido como Microsoft Network Discovery) é usado no Windows Vista e sistemas operacionais posteriores.
- **Permitir a entrada da comunicação RPC na zona Confiável** - Permite conexões TCP da Zona confiável, permitindo o acesso aos serviços MS RPC Portmapper e RPC/DCOM.
- **Permitir área de trabalho remota na Zona confiável** – permite conexões através do Microsoft Remote Desktop Protocol (RDP) e permite que computadores na [Zona confiável](#) acessem seu computador usando um programa que usa RDP (por exemplo, "Remote Desktop Connection"). Veja também como [permitir conexões RDP fora da Zona confiável](#).

- **Ativar o registro em relatório em grupos multicast por meio de IGMP** - Permite a entrada/saída IGMP e entrada de correntes UDP multicast, por exemplo fluxo de vídeos gerado por aplicativos que utilizam o protocolo IGMP (Internet Group Management Protocol).
- **Permitir comunicação para conexões em ponte** – Selecione essa opção para evitar o encerramento de conexões em ponte. A rede conectada em ponte conecta uma máquina virtual a uma rede usando o adaptador Ethernet do computador host. Se você usar redes conectadas em ponte, a máquina virtual pode acessar outros dispositivos na rede e vice-versa, como se fosse um computador físico na rede.
- **Permitir a Descoberta de Serviços Web (WSD) automática para serviços de sistema na zona Confiável** - Permite a entrada de solicitações de Descoberta de Serviços Web das Zonas confiáveis através do firewall. WSD é um protocolo usado para encontrar serviços em uma rede local.
- **Permitir a resolução de endereços multicast na zona Confiável (LLMNR)** - O LLMNR (Link-local Multicast Name Resolution) é um protocolo com base em pacotes DNS que permite aos hosts IPv4 e IPv6 executarem a resolução de nomes para hosts no mesmo link local sem a necessidade de um servidor DNS ou configuração do cliente DNS. Esta opção permite a entrada de solicitações DNS multicast a partir da Zona confiável através do firewall.
- **Grupo de Suporte Doméstico do Windows** - Ativa o grupo de suporte doméstico do Windows 7 e sistemas operacionais posteriores. Um Grupo de Suporte Doméstico pode compartilhar arquivos e impressoras em uma rede doméstica. Para configurar um Grupo doméstico, acesse **Iniciar > Painel de Controle > Rede e Internet > Grupo Doméstico**.

Detecção de intruso

- **Protocolo SMB** - Detecta e bloqueia vários problemas de segurança em protocolo SMB, a saber:
- **Detecção de ataque de autenticação no servidor por desafio por invasor** - Protege você contra um ataque que use um desafio de invasor durante a autenticação para obter credenciais de usuário.
- **Detecção de evasão do IDS durante abertura de pipe nomeado** - Detecção de técnicas conhecidas de evasão para abertura de pipes nomeados MSRPC no protocolo SMB.
- **Detecções de CVE** (Exposições e vulnerabilidades comuns) - Métodos de detecção implementados de vários ataques, formulários, vulnerabilidades de segurança e explorações em protocolo SMB. Consulte o [site de CVE em cve.mitre.org](https://cve.mitre.org) para pesquisar e obter informações mais detalhadas sobre identificadores de CVE (CVEs).
- **Protocolo RPC** - Detecta e bloqueia vários CVEs no sistema de chamada de procedimento remoto desenvolvido para o Distributed Computing Environment (DCE).
- **Protocolo RDP** - Detecta e bloqueia vários CVEs no protocolo RDP (veja acima).
- **Detecção de Ataque por envenenamento ARP** - Detecção de ataques por envenenamento ARP acionados por ataques "man-in-the-middle" (com envolvimento de pessoal) ou detecção de sniffing na chave de rede. ARP (Protocolo de resolução de endereço) é usado pelo aplicativo ou dispositivo de rede para determinar o endereço Ethernet.
- **Detecção de ataque de rastreamento de porta TCP/UDP** - Detecta ataques de software de rastreamento de porta - aplicativo projetado para investigar um host por portas abertas através do envio de pedidos de clientes a vários endereços de porta, com o objetivo de encontrar as portas ativas e explorar a vulnerabilidade do serviço. Leia mais sobre esse tipo de ataque no [glossário](#).
- **Bloquear endereço inseguro após detecção de ataque** - Endereços IP que foram detectados como fontes de ataques são adicionados à lista de proibições para impedir a conexão por um período de tempo.
- **Exibir notificação após detecção de ataque** - Ativa a notificação da bandeja do sistema no canto inferior direito da tela.

- **Exibir notificações também para ataques sendo recebidos contra buracos de segurança** - Alerta você se ataques contra buracos de segurança forem detectados ou se uma ameaça fizer uma tentativa de entrar no sistema desta forma.

Verificação do pacote

- **Permitir conexão de entrada aos compartilhamentos administrativos no protocolo SMB** - Os compartilhamentos administrativos (compartilhamentos administrativos) são os compartilhamentos padrão da rede que compartilham partições de disco rígido (*C\$, D\$, ...*) no sistema, junto com a pasta do sistema (*ADMIN\$*). Desabilitar conexão com compartilhamentos administrativos deve reduzir muitos riscos de segurança. Por exemplo, o worm Conficker realiza ataques de dicionário para conectar-se a compartilhamentos administrativos.
- **Negar dialetos SMB antigos (não compatíveis)** - Negar sessões SMB que usem um dialeto SMB anterior que não é aceito pelo IDS. Sistemas operacionais modernos do Windows suportam dialetos SMB antigos devido à compatibilidade retroativa com sistemas operacionais antigos, como o Windows 95. O agressor pode usar um dialeto antigo em uma sessão SMB para evitar inspeção de tráfego. Negar dialetos SMB antigos se o seu computador não precisa compartilhar arquivos (ou usar comunicação SMB em geral) com um computador com uma versão antiga do Windows.
- **Negar sessões SMB sem segurança estendida** - Segurança estendida pode ser usada durante a negociação de sessão SMB para proporcionar um mecanismo de autenticação mais seguro do que autenticação de LAN Manager Challenge/Response (LM). O esquema LM é considerado fraco e não é recomendado para uso.
- **Negar a abertura de arquivos executáveis em um servidor fora da zona Confiável no protocolo SMB** - Remove a conexão quando você está tentando abrir um arquivo executável (.exe, .dll) de uma pasta compartilhada no servidor que não pertence à zona Confiável no Firewall. Observe que copiar arquivos executáveis de fontes confiáveis pode ser legítimo; no entanto, essa detecção deve minimizar riscos de abrir sem querer um arquivo em um servidor malicioso (por exemplo, um arquivo aberto clicando em um hiperlink para um arquivo executável malicioso compartilhado).
- **Negar autenticação NTLM no protocolo SMB para conexão de um servidor dentro/fora da Zona confiável** - Protocolos que usam esquemas de autenticação NTLM (ambas as versões) estão sujeitos a ataques de encaminhamento de credenciais (conhecidos como ataque de relé SMB no caso de protocolo SMB). Negar autenticação NTLM com um servidor fora da Zona confiável devem mitigar os riscos de encaminhar credenciais por um servidor malicioso para fora da Zona confiável. Do mesmo modo, a autenticação NTLM pode ser negada com servidores da zona confiável.
- **Permitir comunicação com o serviço de Security Account Manager** - Para obter mais informações sobre este serviço consulte [\[MS-SAMR\]](#).
- **Permitir comunicação com o serviço Local Security Authority** - Para obter mais informações sobre este serviço consulte [\[MS-LSAD\]](#) e [\[MS-LSAT\]](#).
- **Permitir comunicação com o serviço de Remote Registry** - Para obter mais informações sobre este serviço consulte [\[MS-RRP\]](#).
- **Permitir comunicação com o serviço de Service Control Manager** - Para obter mais informações sobre este serviço consulte [\[MS-SCMR\]](#).
- **Permitir comunicação com o serviço de Servidor** - Para obter mais informações sobre este serviço consulte [\[MS-SRVS\]](#).
- **Permitir comunicação com outros serviços** - Outros serviços MSRPC. MSRPC é a implementação da Microsoft do mecanismo DCE RPC. Além disso, a MSRPC pode usar pipes nomeados levados para o protocolo de transporte (transporte ncacn_np) SMB (compartilhamento de arquivos de rede). Serviços MSRPC fornecem interfaces para acessar e gerenciar remotamente sistemas Windows. Várias

vulnerabilidades de segurança foram descobertas e exploradas no estado natural no sistema do Windows MSRPC (worm Conficker, worm Sasser...). Desativar comunicação com serviços MSRPC que não precisam ser fornecidos para mitigar muitos riscos de segurança (como execução de código remoto ou ataques de falha de serviço).

Regras IDS

Em algumas situações o [Serviço de detecção de intruso \(IDS\)](#) pode detectar a comunicação entre roteadores ou outros dispositivos de rede internos como um ataque em potencial. Por exemplo, você pode adicionar o endereço seguro conhecido à zona de Endereços excluídos de IDS para ignorar o IDS.

Os artigos da Base de conhecimento da ESET a seguir podem estar disponíveis apenas em inglês:




- [Criar regras IDS em estações de trabalho do cliente no ESET Endpoint Security](#)
- [Criar regras IDS para estações de trabalho do cliente no ESET PROTECT](#)

Colunas

- **Detecção** – tipo de detecção.
- **Aplicativo** – Selecione o caminho de arquivo de um aplicativo com exceção ao clicar em ... (por exemplo *C:\Program Files\Firefox\Firefox.exe*). NÃO insira o nome do aplicativo.
- **IP remoto** – Uma lista de endereço / intervalos / sub-redes IPv4 ou IPv6 remoto. Vários endereços devem ser separados por vírgula.
- **Bloquear** – Cada processo do sistema tem seu próprio comportamento padrão e ação atribuída (bloquear ou permitir). Para substituir o comportamento padrão do ESET Endpoint Security, você poderá selecionar bloqueá-lo ou permiti-lo usando o menu suspenso.
- **Notificar** – Selecione Sim para exibir as [Notificações na área de trabalho](#) no seu computador. Selecione Não se não quiser ter notificações na área de trabalho. Os valores disponíveis são Padrão/Sim/Não.
- **Relatório** – Selecione **Sim** para registrar eventos nos arquivos de relatório [ESET Endpoint Security](#). Selecione **Não** se não quiser registrar eventos. Os valores disponíveis são **Padrão/Sim/Não**.

Exclusões de guia serão exibidas se um administrador [criar exclusões IDS no Web Console ESET PROTECT](#). As exclusões IDS podem ter apenas regras de permissão e serão avaliadas antes das regras IDS.

Gerenciar regras IDS

- **Adicionar** – clique para criar uma nova regra IDS.
- **Editar** – clique para editar uma regra IDS existente.
- **Remover** – selecione e clique se quiser remover uma exceção existente da lista de regras IDS.
-  **Início/Para cima/Final/Para baixo** – permite que você ajuste o nível de prioridade de regras (exceções são avaliadas do início para o fim).

Se quiser exibir uma notificação e coletar um relatório toda vez que um evento ocorrer:

1. Clique em **Adicionar** para adicionar uma nova regra IDS.
2. Selecione o alerta em particular no menu suspenso **Deteção**.
3. Clique em ... e selecione o caminho de arquivo do aplicativo para o que você quer que a notificação seja aplicável.
4. Deixe como **Padrão** no menu suspenso **Bloquear**. Isso vai fazer com que seja herdada a ação padrão aplicada pelo ESET Endpoint Security.
5. Configure os menus suspensos **Notificar** e **Relatório** como **Sim**.
6. Clique em **OK** para salvar essa notificação.

Você quer remover uma notificação recorrente para um tipo de detecção que você não considera como uma ameaça:

1. Clique em **Adicionar** para adicionar uma nova exceção IDS.
2. Selecione o alerta em particular no menu suspenso **Deteção**, por exemplo **Sessão SMB sem extensões de segurança ataque de rastreamento de porta TCP**.
3. Selecione **Entrada** no menu suspenso de direção para o caso de uma comunicação de entrada.
4. Configure o menu suspenso **Notificar** como **Não**.
5. Configure o menu suspenso **Relatório** como **Sim**.
6. Deixe **Aplicativo** em branco.
7. Se a comunicação não estiver vindo de um endereço IP em particular, deixe **Endereço de IP remoto** em branco.
8. Clique em **OK** para salvar essa notificação.

Ameaça suspeita bloqueada

Esta situação pode acontecer quando um aplicativo no seu computador estiver tentando transmitir tráfego malicioso para outro computador da rede, explorando um buraco de segurança, ou se alguém estiver tentando rastrear as portas na sua rede.

Ameaça - Nome da ameaça.

Fonte – Fonte do endereço de rede.

Destino - Endereço de rede de destino.

Parar o bloqueio – cria uma regra IDS para a ameaça suspeita com configurações para permitir a comunicação.

Continuar com o bloqueio – bloqueia a ameaça detectada. Para criar uma regra IDS com configurações para bloquear a comunicação desta ameaça, selecione **Não quero ser notificado novamente**.

As informações exibidas nessa janela de notificação podem variar dependendo do tipo de ameaça detectada.



Para mais informações sobre ameaças e outros termos relacionados consulte [Tipos de ataques remotos](#) ou [Tipos de detecções](#).

Solução de problemas de proteção de rede

O assistente de solução de problemas ajuda a resolver problemas de conectividade causados pelo Firewall ESET. No menu suspenso, selecione um período de tempo durante o qual as comunicações foram bloqueadas. Uma lista de comunicações recentemente bloqueadas oferece um resumo sobre o tipo de aplicativo ou dispositivos, reputação e número total de aplicativos e dispositivos bloqueados durante aquele tempo específico. Para mais

detalhes sobre comunicações bloqueadas, clique em **Detalhes**. A próxima etapa é desbloquear o aplicativo ou dispositivo no qual você espera ter problemas de conectividade.

Ao clicar em **Desbloquear**, a comunicação anteriormente bloqueada será permitida. Se você continuar a ter problemas com um aplicativo, ou se o seu dispositivo não funcionar como esperado, clique em **O aplicativo ainda não funciona** e todas as comunicações bloqueadas anteriormente para aquele dispositivo passarão a ser permitidas. Se o problema continuar, reinicie o computador.

Clique em **Exibir alterações** para ver as regras criadas pelo assistente. Além disso, é possível ver as regras criadas pelo assistente em **Configuração avançada > Proteção da rede > Firewall > Avançado > Regras**.

Clique em **Desbloquear outro para solucionar os problemas de comunicação com um dispositivo ou aplicativo diferente**.

Redes conectadas

Você pode acessar a seção **Redes conectadas** na janela do programa principal do ESET Endpoint Security clicando em **Configuração > Rede > Redes conectadas**.

Essa seleção mostra as redes às quais os adaptadores de rede estão conectados. Depois de clicar no link abaixo do nome da rede, você será solicitado a selecionar um tipo de proteção (estrito ou permitido) para a rede à qual você está conectado via seu adaptador de rede. Clique na engrenagem (⚙️) para alterar essa seleção na **Configuração avançada**. Essa configuração define o quanto seu computador é acessível para outros computadores na rede.

Você pode se conectar a três tipos de localização de rede:

- **Rede não confiável** – Esse tipo de localização de rede é para locais públicos e não é confiável. Seu dispositivo não será visível na rede e você não conseguirá ver nenhum outro dispositivo na sua rede. A descoberta de rede está desativada por padrão para redes públicas.
- **Rede confiável** – ao contrário de uma rede pública, você pode compartilhar recursos com outros computadores no LAN em uma rede privada. Selecione **Rede de casa ou escritório** quando você conhecer e confiar nos dispositivos na rede.
- **Rede de domínio** – seu administrador de rede controla este tipo de localização de rede, e não é possível selecionar ou alterar esse tipo de rede. O tipo de localização de rede de domínio é detectado quando o computador local é membro de um Active Directory Domain Services. O computador local pode autenticar um controlador de domínio para esse domínio através de uma de suas conexões de rede.

Escolher um local de rede pode ajudar a garantir que seu computador esteja sempre configurado para um nível de segurança adequado.

Clicar em **Adaptadores de rede** no canto inferior direito da janela permite ver cada adaptador de rede e seu perfil de firewall e zona confiável atribuídos. Para obter informações mais detalhadas, consulte [Adaptadores de rede](#).



Quando você seleciona **Usar configuração do Windows** uma janela não aparecerá, e a rede na qual você está conectado será marcada automaticamente de acordo com as configurações do Windows. Essa configuração faz com que determinados recursos (por exemplo, compartilhamento de arquivos e área de trabalho remota) fiquem acessíveis de novas redes.

Redes conhecidas

Ao usar um computador que frequentemente se conecta a redes públicas ou redes fora de sua rede de trabalho normal, recomendamos que você verifique a credibilidade das novas redes às quais está se conectando. Assim que as redes forem definidas, o ESET Endpoint Security poderá reconhecer redes confiáveis (Residencial/comercial) usando vários parâmetros de rede configurados em **Identificação da rede**. Os computadores geralmente inserem redes com endereços IP semelhantes à rede confiável. Em tais casos, o ESET Endpoint Security pode considerar uma rede desconhecida como sendo confiável (Residencial/Comercial). Recomendamos que você use a **Autenticação de rede** para evitar esse tipo de situação.

Quando um adaptador de rede é conectado a uma rede ou suas configurações de rede são reconfiguradas, o ESET Endpoint Security pesquisará na lista de rede conhecida um registro que corresponda à nova rede. Se a **Identificação da rede** e a **Autenticação da rede** (opcional) corresponderem, a rede será marcada como conectada nesta interface. Quando nenhuma rede conhecida é encontrada, a configuração de identificação de rede criará uma nova conexão de rede para identificar a rede da próxima vez que você se conectar a ela. Por padrão, a nova conexão de rede usa o tipo de proteção **Rede pública**. A janela de diálogo **Nova conexão de rede detectada** irá pedir que você escolha entre o tipo de proteção **Rede não confiável**, **Rede confiável** ou **Usar configuração do Windows**. Se um adaptador de rede for conectado a uma rede conhecida e essa rede for marcada como **Rede confiável**, sub-redes locais do adaptador são adicionadas à Zona confiável.

Tipo de proteção de novas redes - Selecione uma das seguintes opções: Usar configuração do Windows, Perguntar ao usuário ou Marcar como público é usado por padrão para novas redes.

i Quando você seleciona **Usar configuração do Windows** uma caixa de diálogo do Windows não aparecerá e a rede na qual você está conectado será marcada automaticamente de acordo com as configurações do Windows. Isso fará com que determinados recursos (por exemplo, compartilhamento de arquivos e área de trabalho remota) fiquem acessíveis de novas redes.

Redes conhecidas podem ser configuradas manualmente na janela [Editor de redes conhecidas](#).

Editor de redes conhecidas

Redes conhecidas podem ser configuradas manualmente em **Configuração avançada > Proteção da rede > Básico > Redes conhecidas** clicando em **Editar** ao lado de **Redes conhecidas**.

Colunas

Nome – Nome da rede conhecida.

Tipo de proteção – mostra se a rede está definida para **Rede confiável**, **Rede não confiável** ou **Usar configuração do Windows**.

Perfil de firewall - Selecione o perfil no menu suspenso **Exibir regras usadas no perfil** para exibir o filtro de regras de perfis.

Atualizar perfil - Permite que você aplique o perfil de atualização criado quando estiver conectado a esta rede.

Elementos de controle

Adicionar – Cria uma nova rede conhecida.

Editar - Clique para editar uma rede conhecida existente.

Remover – Selecione uma rede e clique em **Remover** para removê-la da lista de redes conhecidas.



Início/Para cima/Final/Para baixo - Permite que você ajuste o nível de prioridade de redes conhecidas (redes são avaliadas do início para o fim).

Definições de configuração de rede são organizadas nas seguintes guias:

Rede

Aqui você pode definir o **Nome de rede** e selecionar o **Tipo de proteção** (Rede não confiável, Rede confiável ou Usar configuração do Windows) para a rede. Use o menu suspenso **Perfil de firewall** para selecionar o perfil para esta rede. Se a rede utilizar o tipo de proteção **Rede confiável**, todas as sub-redes de rede conectadas diretamente serão consideradas confiáveis. Por exemplo, se um adaptador de rede for conectado a esse tipo de rede com o endereço IP 192.168.1.5 e a máscara de sub-rede 255.255.255.0, a sub-rede 192.168.1.0/24 será adicionada à zona confiável desse adaptador. Se o adaptador tiver mais endereços/sub-redes, todos eles serão confiáveis, independentemente da configuração **Identificação de rede** da rede conhecida.

Além disso, endereços adicionados em **Endereços adicionais confiáveis** serão sempre adicionados à zona confiável de adaptadores conectados a essa rede (independentemente do tipo de proteção da rede).

Alertar sobre criptografia WiFi fraca – O ESET Endpoint Security vai informar quando você conectar a uma rede sem fio desprotegida ou uma rede com proteção fraca.

Perfil de firewall – Selecione o perfil de firewall que será aplicado quando conectado a esta rede.

Perfil de atualização – Selecione o perfil de atualização que será aplicado quando conectado a esta rede.

As seguintes condições devem ser atendidas para uma rede a ser marcada como conectada na lista de redes conectadas:

- **Identificação de rede** - Todos os parâmetros preenchidos devem corresponder aos parâmetros de conexão ativa.
- **Autenticação de rede** - se o servidor de autenticação for selecionado, a autenticação bem-sucedida com o servidor de autenticação ESET deverá ocorrer.

Identificação da rede

A identificação da rede é executada com base nos parâmetros do adaptador da rede local. Todos os parâmetros selecionados serão comparados em relação aos parâmetros reais de conexões de redes ativas. Endereços IPv4 e IPv6 serão permitidos.

Editar rede

Rede Identificação da rede Autenticação de rede

Quando o sufixo DNS atual for (exemplo: 'empresa.com') ☒

Quando o endereço IP do servidor WINS for ☐

Quando o endereço IP do servidor DNS for ☒

Quando o endereço IP local for ☒

Quando o endereço IP do servidor DHCP for ☒

OK Cancelar

Autenticação de rede

A autenticação de rede procura por um servidor específico na rede e usa uma criptografia assimétrica (RSA) para autenticar esse servidor. O nome da rede sendo autenticada deverá corresponder ao nome da zona definida em configurações do servidor de autenticação. O nome diferencia maiúsculas e minúsculas. Especifique um nome de servidor, uma porta de escuta do servidor e uma chave pública que corresponda à chave privada do servidor (consulte a seção [Autenticação de rede - Configuração de servidor](#)). O nome de servidor pode ser inserido na forma de um endereço IP, DNS ou nome NetBios e pode ser seguido por um caminho especificando o local da chave no servidor (por exemplo, server_name_/directory1/directory2/authentication). Você pode especificar servidores alternativos para uso acrescentando-os ao início do caminho, separados por ponto e vírgulas.

[Faça o download do Servidor de autenticação ESET.](#)

A chave pública pode ser importada usando qualquer um dos seguintes tipos de arquivos:

- Chave pública PEM codificada (.pem), essa chave pode ser gerada usando o servidor de autenticação ESET (consulte [Autenticação de rede - Configuração de servidor](#)).
- Chave pública codificada
- Certificado de chave pública (.crt)

Editar rede

Rede Identificação da rede Autenticação de rede

Nome do servidor ou endereço IP 10.1.1.24

Porta do servidor 80

Chave pública (codificação base64)

Adicionar Teste

OK Cancelar

Clique em **Testar** para testar suas configurações. Se a autenticação foi bem sucedida, A autenticação do servidor foi bem sucedida será exibido. Se a autenticação não estiver configurada corretamente, será exibida uma das seguintes mensagens de erro:

Falha na autenticação do servidor. Assinatura inválida ou sem correspondência.
A assinatura de servidor não corresponde à chave pública inserida.

Falha na autenticação do servidor. O nome da rede não corresponde.
O nome da rede configurada não corresponde ao nome da zona do servidor de autenticação. Verifique ambos os nomes e certifique-se de que sejam idênticos.

Falha na autenticação do servidor. Nenhuma resposta ou resposta inválida do servidor.
Uma resposta não será recebida se o servidor não estiver em execução ou não estiver acessível. Uma resposta inválida poderá ser recebida se outro servidor HTTP estiver em execução no endereço especificado.

Chave pública inválida inserida.
Verifique se o arquivo de chave pública inserido não está corrompido.

Autenticação de rede - Configuração de servidor

O processo de autenticação pode ser executado por qualquer computador/servidor conectado à rede que deva ser autenticado. O aplicativo Servidor de autenticação ESET precisa estar instalado em um computador/servidor que esteja sempre acessível para autenticação quando um cliente tentar se conectar à rede. O arquivo de instalação do aplicativo Servidor de autenticação ESET está disponível para download no site da ESET.

Depois de instalar o aplicativo Servidor de autenticação ESET, uma janela de diálogo será exibida (você pode acessar o aplicativo clicando em **Iniciar > Programas > ESET > Servidor de autenticação ESET**).

Para configurar o servidor de autenticação, insira o nome da rede de autenticação, a porta de escuta do servidor (o padrão é 80), bem como o local para armazenar o par de chaves pública e privada. Em seguida, gere as chaves pública e privada que serão utilizadas no processo de autenticação. A chave privada permanecerá no servidor, enquanto a chave pública precisará ser importada no lado do cliente na seção de autenticação da rede, ao definir uma rede na configuração do firewall.

Perfis de firewall

Perfil global padrão - Se não houver perfil da rede nem da configuração do adaptador, o perfil global padrão é usado.

Lista de perfis - Os perfis podem ser usados para controlar o comportamento do Firewall ESET Endpoint Security. Ao criar ou editar uma regra de Firewall, você pode atribuí-la a um perfil específico ou aplicá-la a cada perfil. Quando um perfil está ativo em uma interface de rede, apenas as regras globais (regras sem nenhum perfil especificado) e as regras que foram atribuídas a esse perfil são aplicadas a ele. Você pode criar vários perfis com regras diferentes atribuídas a adaptadores de rede ou atribuídas a redes para alterar com facilidade o comportamento do Firewall.

Perfis atribuídos a adaptadores de rede - Um adaptador de rede pode ser configurado para usar um perfil configurado para uma rede específica quando estiver conectado a essa rede.

Você também pode atribuir um perfil específico para usar quando estiver em uma determinada rede em **Configuração avançada (F5) > Firewall > Redes conhecidas**. Selecione uma rede da lista de **Redes conhecidas** e clique em **Editar** para atribuir um perfil de firewall para a rede específica no menu suspenso **Perfil de firewall**. Se essa rede não tiver um perfil atribuído, o perfil padrão do adaptador será usado. Se o adaptador for configurado para usar o perfil da rede, seu perfil padrão será usado, independentemente de à qual rede estiver conectado. Se não houver perfil da rede nem da configuração do adaptador, o perfil global padrão é usado. Para atribuir um perfil a um adaptador de rede, selecione o adaptador de rede, clique em **Editar** ao lado de **Perfis atribuídos a adaptadores de rede**, selecione o perfil do menu suspenso **Perfil de firewall padrão** e clique em **OK**.

Quando o Firewall alternar para outro perfil, uma notificação será exibida no canto inferior direito próximo ao relógio do sistema.

Perfis atribuídos a adaptadores de rede

Ao alternar perfis, você pode fazer rapidamente várias mudanças no comportamento do firewall. Regras personalizadas podem ser definidas e aplicadas para perfis específicos. Entradas do adaptador de rede para todos os adaptadores presentes na máquina são adicionadas automaticamente à lista de **Adaptadores de rede**.

Colunas

Nome - Nome do adaptador de rede.

Perfil de firewall padrão - O perfil padrão é usado quando a rede à qual você está conectado não tem um perfil configurado ou se o adaptador de rede estiver configurado para não usar o perfil de rede.

Perfil de rede preferido - O adaptador de rede pode usar um perfil de firewall configurado para a rede conectada conhecida. Se a rede não tiver um perfil configurado ou se o adaptador de rede estiver configurado para não usar o perfil de rede, então o perfil padrão do adaptador é usado.

Elementos de controle

Adicionar – Adiciona um novo adaptador de rede.

Editar – Deixa você editar um adaptador de rede existente.

Remover - Selecione um adaptador de rede e clique em Remover se quiser remover um adaptador de rede da lista.

OK/Cancelar - Clique em **OK** se quiser salvar alterações ou clique em **Cancelar** se quiser sair sem salvar.

Detecção de modificação de aplicativo

O recurso de detecção de verificação de aplicativo exibirá notificações se os aplicativos modificados, para os quais houver uma regra de firewall, tentarem estabelecer conexões. Isso é útil para evitar o uso incorreto de regras configuradas para algum aplicativo por outro aplicativo ao substituir temporariamente ou permanentemente o arquivo executável do aplicativo original por outro arquivo executável do aplicativo ou ao modificar maliciosamente o arquivo executável do aplicativo original.

Esteja ciente de que esse recurso não se destina a detectar modificações em qualquer aplicativo em geral. O objetivo é evitar o uso incorreto de regras de firewall e somente aplicativos para os quais há regras de firewall específicas são monitorados.

Ativar detecção de modificações em aplicativos - Se essa opção for selecionada, o programa monitorará os aplicativos para ver se há alterações (atualizações, infecções, outras modificações). Quando um aplicativo modificado tentar estabelecer uma conexão, você será notificado pelo Firewall.

Permitir modificação em aplicativos assinados (confiáveis) - Não notifique se o aplicativo tem a mesma assinatura digital válida antes e após a modificação.

Lista de aplicativos excluídos da verificação – Você pode adicionar ou remover aplicativos individuais para os quais modificações são permitidas sem notificação.

Aplicativos excluídos da detecção de modificação

O Firewall no ESET Endpoint Security detecta alterações em aplicativos para os quais há regras (consulte [Detecção de modificação de aplicativo](#)).

Em determinados casos, você pode não desejar utilizar essa funcionalidade para alguns aplicativos e desejar excluí-los da verificação pelo firewall.

Adicionar – Abre uma janela na qual você pode selecionar um aplicativo para adicionar à lista de aplicativos excluídos da detecção de modificação. Você pode escolher de uma lista de aplicativos em execução com comunicação de rede aberta, para a qual há uma regra de firewall ou adicionar um aplicativo específico.

Editar – abre uma janela na qual é possível alterar o local de um aplicativo que está na lista de aplicativos excluídos da detecção de modificação. Você pode escolher de uma lista de aplicativos em execução com comunicação de rede aberta, para a qual a regra de firewall existe, ou alterar o local manualmente.

Remover - Remove entradas da lista de aplicativos excluídos da detecção de modificação.

Configuração e uso de regras

As regras representam um conjunto de condições utilizadas para testar todas as conexões de rede e todas as ações atribuídas a essas condições. Usando regras de firewall, é possível definir a ação a ser feita quando

diferentes tipos de conexões de rede são estabelecidos. Para acessar a configuração de filtragem de regras, navegue até **Configuração avançada** (F5) > **Proteção da rede** > **Firewall** > **Avançado**. Algumas das regras predefinidas são vinculadas às caixas de seleção de **serviços permitidos** ([Serviços permitidos e opções avançadas](#)) e elas não podem ser desativadas diretamente; em vez disso, você pode usar essas caixas de seleção relacionadas para fazer isso.

Ao contrário da versão anterior do ESET Endpoint Security, regras são avaliadas do início para o fim. A ação da primeira regra correspondente é usada para cada conexão de rede sendo avaliada. Essa é uma alteração comportamental importante da versão anterior na qual a prioridade de regras era automática e regras mais específicas tinham prioridade superior do que as mais gerais.

As conexões podem ser divididas em conexões de entrada e de saída. As conexões de entrada são iniciadas por um computador remoto que tenta estabelecer uma conexão com o sistema local. As conexões de saída funcionam de maneira oposta - o sistema local contata um computador remoto.

Se uma nova comunicação desconhecida for detectada, considere cuidadosamente se vai permiti-la ou negá-la. As conexões não solicitadas, não seguras ou desconhecidas representam um risco de segurança para o sistema. Se tal conexão for estabelecida, recomenda-se que seja dada atenção especial ao computador remoto e ao aplicativo tentando conectar-se ao computador. Muitas infiltrações tentam obter e enviar dados particulares ou fazem download de outros aplicativos nocivos para estações de trabalho de host. O Firewall permite que o usuário detecte e finalize tais conexões.

Lista de regras de firewall

A Lista de regras de firewall pode ser encontrada em **Configuração avançada** (F5) > **Proteção da rede** > **Firewall** > **Básico** ao clicar em **Editar** ao lado de **Regras**.

Colunas

Nome – Nome da regra.

Ativado - Mostra se regras estão ativadas ou desativadas, a caixa de seleção correspondente deve ser selecionada para ativar uma regra.

Protocolo – O protocolo de internet para o qual esta regra é válida.

Perfil - Mostra o perfil de firewall para o qual esta regra é válida.

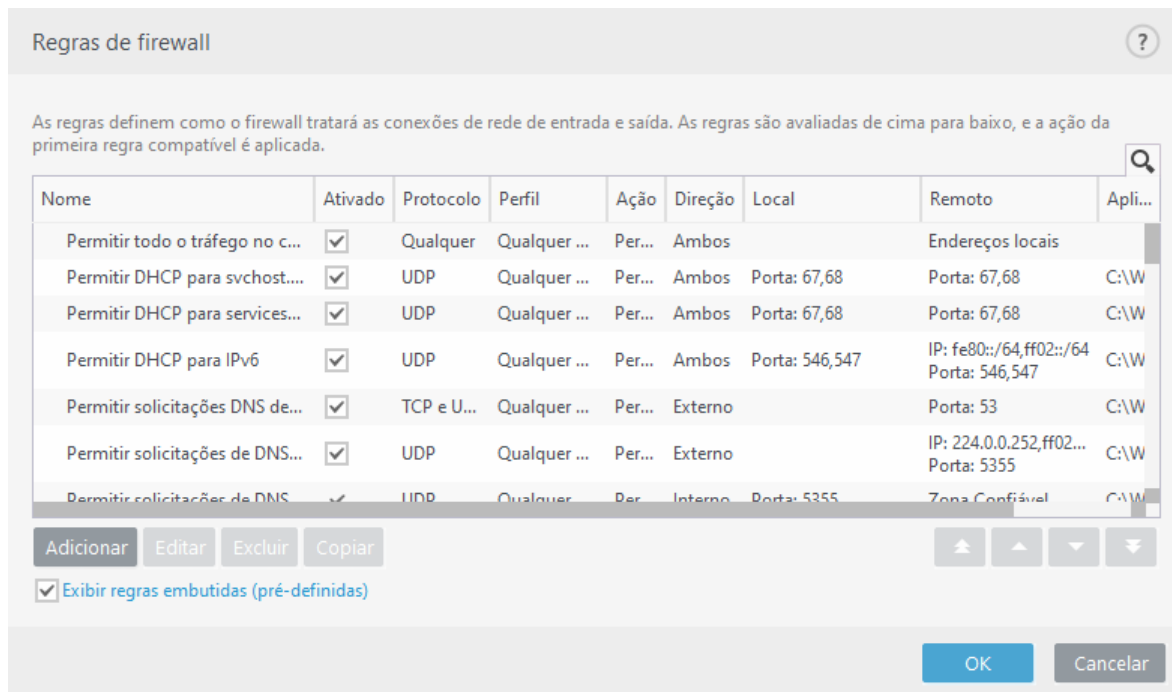
Ação - Mostra o status da comunicação (bloquear/permitir/perguntar).

Direção - Direção da comunicação (entrada/saída/ambas).

Local – Endereço/intervalo/subrede IPv4 ou IPv6 remoto e porta do computador local.

Remoto – Endereço/intervalo/subrede IPv4 ou IPv6 remoto e porta do computador remoto.

Aplicativos - Indica o aplicativo ao qual a regra se aplica.



Elementos de controle

Adicionar - [Cria uma nova regra](#).

Editar – Edita uma regra existente.

Remover – Remove uma regra existente.


Copiar - Cria uma cópia de uma regra selecionada.

Exibir regras embutidas (predefinidas) - Regras predefinidas por ESET Endpoint Security que permitem ou negam comunicações específicas. Você pode desativar essas regras, mas você não pode excluir uma regra predefinida.



Início/Para cima/Final/Para baixo - Permite que você ajuste o nível de prioridade de regras (regras são executadas do início para o fim).



Clique no ícone de pesquisa  no canto superior direito para pesquisar as regras por nome, protocolo ou porta.

Adicionar ou editar Regras de firewall

Editar ou adicionar regras de Firewall pode ser necessário quando as configurações de rede mudarem (por exemplo, o endereço de rede ou número de porta para o lado remoto forem alterados) para garantir a operação correta de um aplicativo afetado por uma regra.



Os artigos da Base de conhecimento da ESET a seguir podem estar disponíveis apenas em inglês:

- [Criar ou editar regras de firewall no ESET Endpoint Security](#)
- [Criar ou editar regras de firewall para estações de trabalho do cliente no ESET PROTECT](#)

A parte superior da janela contém três guias:

- **Geral** - Especifica um nome de regra, a direção da conexão, a ação (**Permitir, Negar, Perguntar**), o

protocolo e o perfil ao qual a regra se aplicará.

- **Local** - Exibe informações sobre o lado local da conexão, incluindo o número da porta local ou o intervalo de portas e o nome do aplicativo de comunicação. Permite adicionar uma zona pré-definida ou criada com um intervalo de endereços IP aqui clicando em **Adicionar**.
- **Remoto** - Esta guia contém informações sobre a porta remota (intervalo de portas). Permite que você defina uma lista de endereços IP remotos ou zonas para uma determinada regra. Permite adicionar uma zona pré-definida ou criada com um intervalo de endereços IP aqui clicando em **Adicionar**.

Ao criar uma nova regra, é preciso digitar o nome da regra no campo **Nome**. Selecione a direção para a qual a regra se aplica no menu suspenso **Direção** e a ação a ser executada quando um canal de comunicação encontra a regra no menu suspenso **Ação**.

Protocolo representa o protocolo de transferência usado para a regra. Selecione qual protocolo usar para determinada regra do menu suspenso.

Código/tipo ICMP representa uma mensagem ICMP identificada por um número (por exemplo, 0 representa "resposta Echo").

Por padrão, todas as regras estão ativadas para **Qualquer perfil**. Alternativamente, selecione um perfil de firewall personalizado usando o menu suspenso **Perfis**.

Se ativar o **Gravidade do registro em log**, a atividade conectada com a regra será registrada em um relatório. **Notificar usuário** exibe uma notificação quando a regra é aplicada.

Editar regra

Geral Local Remoto

Geral

Nome: Untitled

Ativado: ☒

Direção: Interno

Ação: Negar

Protocolo: TCP e UDP

Tipo/Código ICMP: 0

Perfil: Qualquer perfil

Gravidade do registro em log: Diagnóstico

OK



Relatórios de firewall com ação **Negar** e gravidade de registro de **Alerta** podem ser [coletados pelo ESET PROTECT](#).

Criamos uma nova regra para permitir que o aplicativo do navegador da web Firefox acesse o Internet / sites da rede local.

1. Na guia **Geral**, ative a comunicação de saída por meio dos protocolos TCP e DP.

✓ 2. Clique na guia **Local**.

3. Selecione o caminho de arquivo de um navegador da web usado por você ao clicar em ... (por exemplo *C:\Program Files\Firefox\Firefox.exe*). NÃO insira o nome do aplicativo.

4. Na guia **Remoto**, ative as portas número 80 e 443 se você deseja permitir navegação padrão na Internet.

i Regras pré-definidas podem ser modificadas de forma limitada.

Regra de firewall – Local

Especifique o nome do aplicativo local e a(s) porta(s) local(is) para a(s) qual(is) a regra se aplicará.

Porta – número(s) de porta(s) local(is). Se não forem fornecidos números, a regra será aplicada a todas as portas. Adiciona uma única porta de comunicação ou um intervalo de portas de comunicação.

IP - Permite que você adicione um endereço(s) remoto(s), intervalo de endereços ou sub-rede onde a regra é aplicada. Se não for fornecido um valor, a regra será aplicada a toda a comunicação.

Zonas – Lista de zonas adicionadas.

Adicionar - Adicione uma zona criada do menu suspenso. Para criar uma zona, use a guia [Configuração de zona](#).

Remover – Remove as zonas da lista.

Aplicativo - O nome do aplicativo para o qual a regra se aplica. Adicionar o local do aplicativo para o qual a regra será aplicada.

Serviço - O menu suspenso exibe os serviços do sistema.

✓ Você pode querer criar uma regra para sua Imagem que fornece atualização através da porta 2221 usando o serviço EHttpSrv para comunicação no menu suspenso.

Editar regra

Geral Local Remoto

Local

Porta 59654

IP 192.168.1.2

Zonas

Adicionar Editar Excluir Importar Exportar

Aplicativo C:\Program Files\Internet Explorer\

OK

Regra de firewall – Remoto

Porta – Número(s) de porta(s) remota(s). Se não forem fornecidos números, a regra será aplicada a todas as portas. Adiciona uma única porta de comunicação ou um intervalo de portas de comunicação.

IP - Permite que você adicione um endereço remoto, intervalo de endereços ou sub-rede. O endereço, intervalo/sub-rede ou zona remota para a qual a regra será aplicada. Se não for fornecido um valor, a regra será aplicada a toda a comunicação.

Zonas – Lista de zonas adicionadas.

Adicionar - Adicione uma zona selecionando-a do menu suspenso. Para criar uma zona, use a guia [Configuração de zona](#).

Remover – Remove as zonas da lista.

Editar regra

Geral Local Remoto

Remoto

Porta 21

IP 192.168.10.1/255.255.255.0

Zonas

Endereços locais

Adicionar Editar Excluir Importar Exportar

OK

Lista de proibições temporária de endereço IP

Para exibir endereços IP que foram detectados como fontes de ataques e que são adicionados à lista de proibições para bloquear a conexão por um período de tempo, de ESET Endpoint Security navegue até **Configuração > Rede > Lista de proibições temporária de endereço IP**. Endereços IP bloqueados temporariamente são bloqueados por 1 hora.

Colunas

Endereço IP - exibe um endereço IP que foi bloqueado.

Motivo de bloqueio - Exibe o tipo de ataque que foi impedido a partir do endereço (por exemplo Ataque de rastreamento de porta TCP).

Tempo de limite - Exibe a hora e data em que o endereço é excluído da lista de proibições.

Elementos de controle

Remover - clique para remover um endereço da lista de proibições antes de ele expirar.

Remover tudo - clique para remover todos os endereços da lista de proibições imediatamente.

Adicionar exceção - clique para adicionar uma exceção de firewall na filtragem IDS.

Zona confiável

A zona confiável representa um grupo de endereços de rede dos quais o firewall permite certo tráfego de entrada usando configurações padrão. Configurações para recursos, como compartilhamento de arquivos e área de

trabalho remota dentro da zona confiável, são determinadas em [Serviços permitidos e opções avançadas](#).

A zona confiável de fato é computada dinamicamente e separadamente de cada adaptador de rede com base em qual rede o computador está conectado no momento. Endereços definidos como na zona confiável no Editor de regras são sempre confiáveis. Se um adaptador de rede estiver conectado a uma rede conhecida, então os **Endereços confiáveis adicionais** configurados para essa rede serão adicionados à zona confiável do adaptador. Se uma rede tiver o tipo de proteção Doméstica/trabalho, todas as sub-redes diretamente conectadas serão incluídas na zona confiável. A zona confiável de fato para cada adaptador de rede pode ser visualizada da janela **Configuração** em **Rede > Adaptadores de rede**.

Configuração de zonas

Uma zona representa uma coleção de endereços de rede que criam um grupo lógico de endereços IP, úteis quando você precisa reutilizar o mesmo conjunto de endereços em várias regras. A cada endereço no grupo são atribuídas regras semelhantes definidas centralmente para todo o grupo. Um exemplo de tal grupo é a **Zona confiável**. Uma Zona confiável representa um grupo de endereços de rede que não são bloqueados pelo Firewall de maneira alguma. Essas zonas podem ser configuradas em **Configuração avançada > Proteção da rede > Básico > Zonas**, clicando em **Editar** ao lado de **Zonas**. Para adicionar uma nova zona, clique em **Adicionar**, insira um **Nome** para a zona, uma **Descrição** e adicione um endereço IP remoto no campo **Endereço do computador remoto (IPv4/IPv6, intervalo, máscara)**. Veja também [Zonas de firewall](#).

Zonas de firewall

Para mais informações sobre zonas, consulte a seção [Configurando zonas](#).

Colunas

Nome - Nome de um grupo de computadores remotos.

Endereços IP - Endereços IP remotos que pertencem à zona.

Elementos de controle

Ao **adicionar** ou **editar** uma zona, os campos a seguir estão disponíveis:

Nome - Nome de um grupo de computadores remotos.

Descrição - Uma descrição geral do grupo.

Endereço remoto do computador (IPv4, IPv6, intervalo, máscara) - Permite que você adicione um endereço remoto, intervalo de endereços ou sub-rede.

Excluir - Remove uma zona da lista.

i Esteja ciente de que zonas pré-definidas não podem ser removidas.

Relatório do firewall

O Firewall do ESET Endpoint Security salva eventos importantes em um arquivo de relatório, que pode ser exibido diretamente no menu principal. Clique em **Ferramentas > Relatórios** e em seguida selecione **Proteção da rede** no menu suspenso **Relatório**. Para ativar o registro em relatório de firewall, navegue para **Configuração avançada > Ferramentas > Relatórios** e defina o detalhamento mínimo de relatório como **Diagnóstico**. Todas as conexões negadas serão registradas.

Os relatórios podem ser usados para detectar erros e revelar intrusos no seu sistema. Os relatórios do Firewall ESET contêm os seguintes dados:

- **Hora** – Data e hora do evento.
- **Evento** – Nome do evento.
- **Fonte** – Fonte do endereço de rede.
- **Destino** - Endereço de rede de destino.
- **Protocolo** – Protocolo de comunicação de rede.
- **Nome da regra/worm** - Regra aplicada, ou nome do worm, se identificado.
- **Aplicativo** – Aplicativo envolvido.
- **Usuário** - Nome do usuário conectado no momento em que a infiltração foi detectada.

Uma análise completa desses dados pode ajudar a detectar tentativas de se comprometer a segurança do sistema. Muitos outros fatores indicam riscos de segurança potenciais e permitem que você reduza seus impactos. Alguns exemplos de possíveis indicadores de ameaças incluem conexões muito frequentes de locais desconhecidos, diversas tentativas para estabelecer conexões, aplicativos desconhecidos comunicando-se ou números de portas incomuns sendo utilizados.



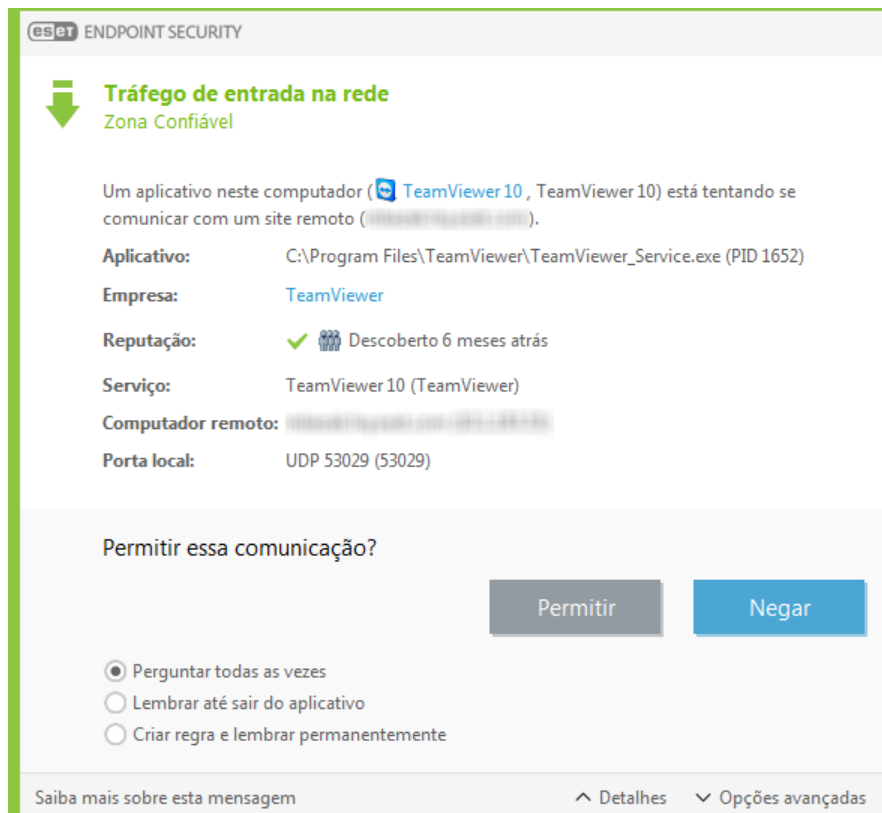
A mensagem da exploração de vulnerabilidade de segurança é registrada mesmo se a vulnerabilidade em particular já estiver corrigida, já que a tentativa de exploração é detectada e bloqueada no nível da rede antes que a exploração real possa acontecer.

Estabelecimento de uma conexão - detecção

O Firewall detecta cada conexão de rede recém-criada. O modo de firewall ativo determina quais ações serão executadas para a nova conexão. Se o **Modo automático** ou o **Modo com base em políticas** estiver ativado, o Firewall executará ações predefinidas sem nenhuma interação com o usuário.

O modo interativo exibe uma janela de informações que reporta a detecção de uma nova conexão de rede, suplementada com informações detalhadas sobre a conexão. O usuário pode escolher permitir a conexão ou recusá-la (bloqueio). Se houver necessidade de permitir várias vezes a mesma conexão na janela de diálogo, recomendamos que você crie uma nova regra para a conexão. Para isso, selecione **Lembrar ação (criar regra)** e salve a ação como uma nova regra para o Firewall. Se o firewall reconhecer a mesma conexão no futuro, ele aplicará a regra existente sem solicitar a interação do usuário.

Lembrar temporariamente ação para o processo faz com que a ação (**Permitir/Negar**) seja utilizada até que ocorra uma reinicialização do aplicativo, uma alteração de regras ou dos modos de filtragem ou ocorra uma atualização do módulo do Firewall ou reinicialização do sistema. Depois de qualquer uma dessas ações, as regras temporárias serão excluídas.



Tenha cuidado ao criar novas regras e permita apenas as conexões que você sabe que são seguras. Se todas as conexões forem permitidas, então o Firewall falhará em realizar seu propósito. Estes são os parâmetros importantes para as conexões:

- **Lado remoto** - Somente permita conexões para endereços confiáveis e conhecidos.
- **Aplicativo local** - Não é aconselhável permitir conexões para aplicativos e processos desconhecidos.
- **Número da porta** - Em circunstâncias normais, a comunicação em portas comuns (por exemplo, o tráfego da web - porta 80) deve ser permitida.

Para se proliferar, as ameaças de computador usam frequentemente a Internet e conexões ocultas para ajudar a infectar sistemas remotos. Se as regras forem configuradas corretamente, um Firewall se tornará uma ferramenta útil para a proteção contra diversos ataques de códigos maliciosos.

Resolvendo problemas com o Firewall ESET

Se você estiver tendo problemas de conectividade com o ESET Endpoint Security instalado, há várias formas de saber se o Firewall ESET está causando o problema. Além disso, o Firewall ESET pode ajudar você a criar novas regras ou exceções para resolver problemas de conectividade.

Consulte os seguintes tópicos para obter ajuda com a solução de problemas com o Firewall ESET:

- [Assistente de solução de problemas](#)
- [Registrando e criando regras ou exceções de log](#)
- [Criando exceções de notificações do firewall](#)
- [Registro em relatório avançado de proteção da rede](#)
- [Resolvendo problemas com a filtragem de protocolo](#)

Assistente de solução de problemas

O assistente de solução de problemas monitora em segundo plano todas as conexões bloqueadas. Ele o orienta no processo de solução de problemas para corrigir problemas de firewall com dispositivos ou aplicativos específicos. Depois disso, ele sugere um novo conjunto de regras a serem aplicadas caso você as aprove. O **Assistente de solução de problemas** pode ser acessado no menu principal em **Configuração > Rede**.



Os artigos da Base de conhecimento da ESET a seguir podem estar disponíveis apenas em inglês:

- [Adicionar uma exceção de firewall usando o Assistente de solução de problemas](#)

Registrando e criando regras ou exceções de log

Por padrão, o Firewall ESET não registra todas as conexões bloqueadas. Se você quiser ver o que foi bloqueado pelo firewall, ative o Registro em relatório avançado de Proteção da rede na seção **Diagnóstico** da **Configuração avançada** sob **Ferramentas > Diagnóstico**. Se você vir algo no relatório que não quiser que o firewall bloqueie, poderá criar uma regra ou regra IDS para isso clicando com o botão direito do mouse nesse item e selecionando **Não bloquear eventos similares no futuro**. Observe que o relatório de todas as conexões bloqueadas pode conter milhares de itens e pode dificultar a localização de uma conexão específica nesse relatório. Você pode desativar o registro em relatório depois de resolver o problema.

Para obter mais informações sobre o log, consulte [Relatórios](#).



Use o registro em relatório para ver o pedido no qual o Firewall bloqueou conexões específicas. Além disso, criar regras a partir do log permite que você crie regras que façam exatamente o que você deseja.

Criar regra de log

A nova versão do ESET Endpoint Security permite que você crie uma regra do relatório. No menu principal, clique em **Ferramentas > Arquivos de relatório**. Escolha **Proteção da rede** no menu suspenso, clique com o botão direito do mouse em sua entrada de relatório desejada e selecione **Não bloquear eventos similares no futuro** do menu de contexto. Uma janela de notificação exibirá sua nova regra.

Para permitir a criação de novas regras de relatório, o ESET Endpoint Security deve ser configurado com as seguintes configurações:

- define o detalhamento mínimo de registro em log como **Diagnóstico** em **Configuração avançada (F5) > Ferramentas > Relatórios**,
- ativar **Exibir notificações também para ataques sendo recebidos contra buracos de segurança** em **Configuração avançada (F5) > Proteção de rede > Proteção de ataque a rede > Opções avançadas > Detecção de intrusos**.

Criando exceções de notificações do firewall

Quando o Firewall ESET detectar atividade maliciosa na rede, uma janela de notificação descrevendo o evento será exibida. Esta notificação apresentará um link que permitirá que você saiba mais sobre o evento e configure uma exceção para ele caso queira.

i se um dispositivo ou aplicativo em rede não implementar padrões de rede corretamente ele poderá acionar notificações de IDS do firewall repetidas. Você pode criar uma exceção diretamente da notificação para impedir que o Firewall ESET detecte esse aplicativo ou dispositivo.

Registro em relatório avançado de proteção da rede

Esse recurso tem como objetivo fornecer arquivos de relatório mais complexos para o Suporte técnico ESET. Use esse recurso somente quando solicitado pelo Suporte técnico ESET, pois ele pode gerar um relatório enorme e deixar seu computador lento.

1. Navegue para **Configuração avançada > Ferramentas > Diagnóstico** e ative **Ativar registro em relatório avançado de proteção da rede**.
2. Tentativa de reproduzir o problema que você está tendo.
3. Desativar registro em relatório avançado de proteção da rede.
4. O arquivo de relatório PCAP criado pelo registro em relatório avançado de proteção da rede pode ser encontrado no mesmo diretório no qual despejos de memória de diagnóstico são gerados:
`C:\ProgramData\ESET\ESET Endpoint Security\Diagnostics\`

Resolvendo problemas com a filtragem de protocolo

Se você tiver problemas com seu navegador ou cliente de email, a primeira etapa é determinar se a filtragem de protocolo é responsável. Para fazer isso, tente desativar temporariamente a filtragem de protocolo na configuração avançada (lembre-se de ativá-la novamente depois de ter concluído; caso contrário, seu navegador e cliente de email ficarão desprotegidos). Se o problema desaparecer após desativá-la, há uma lista de problemas comuns e uma forma para resolvê-los:

Atualizar ou proteger problemas de comunicação

Se seu aplicativo avisar sobre a incapacidade de atualizar ou que um canal de comunicação não está seguro:

- Se você tiver filtragem de protocolo SSL ativada, tente desativá-la temporariamente. Se isso ajudar, você poderá continuar usando filtragem SSL e fazer o trabalho de atualização excluindo a comunicação problemática:
Altere o modo de filtragem de protocolo SSL para interativa. Execute a atualização novamente. Deve haver um diálogo informando você sobre tráfego de rede criptografado. Certifique-se de que o aplicativo corresponda ao que você está solucionando e o certificado pareça estar vindo do servidor do qual está atualizando. Em seguida, escolha lembrar a ação para esse certificado e clique em ignorar. Se não houver mais diálogos relevantes a serem exibidos, você poderá alternar o modo de filtragem de volta para automático e o problema deverá ser resolvido.
- Se o aplicativo em questão não for um navegador ou cliente de email, você poderá excluí-lo totalmente da filtragem de protocolo (fazer isso para o navegador ou cliente de email deixaria você exposto). Qualquer aplicativo que tenha tido sua comunicação filtrada anteriormente já deve estar na lista fornecida para você ao adicionar a exceção; portanto, fazer o acréscimo manualmente não deve ser necessário.

Problema ao acessar um dispositivo em sua rede

Se você não conseguir usar qualquer funcionalidade de um dispositivo em sua rede (isso poderia significar abrir uma página da Web de sua webcam ou reproduzir vídeo em um media player doméstico), tente adicionar os

respectivos IPv4 e IPv6 à lista de endereços excluídos.

Problemas com um site específico

Você pode excluir sites específicos de filtragem de protocolo usando o gerenciamento de endereços URL. Por exemplo, se você não conseguir acessar <https://www.gmail.com/intl/en/mail/help/about.html>, tente adicionar *gmail.com* à lista de endereços excluídos.

Erro "Alguns dos aplicativos capazes de importar o certificado raiz ainda estão em execução"

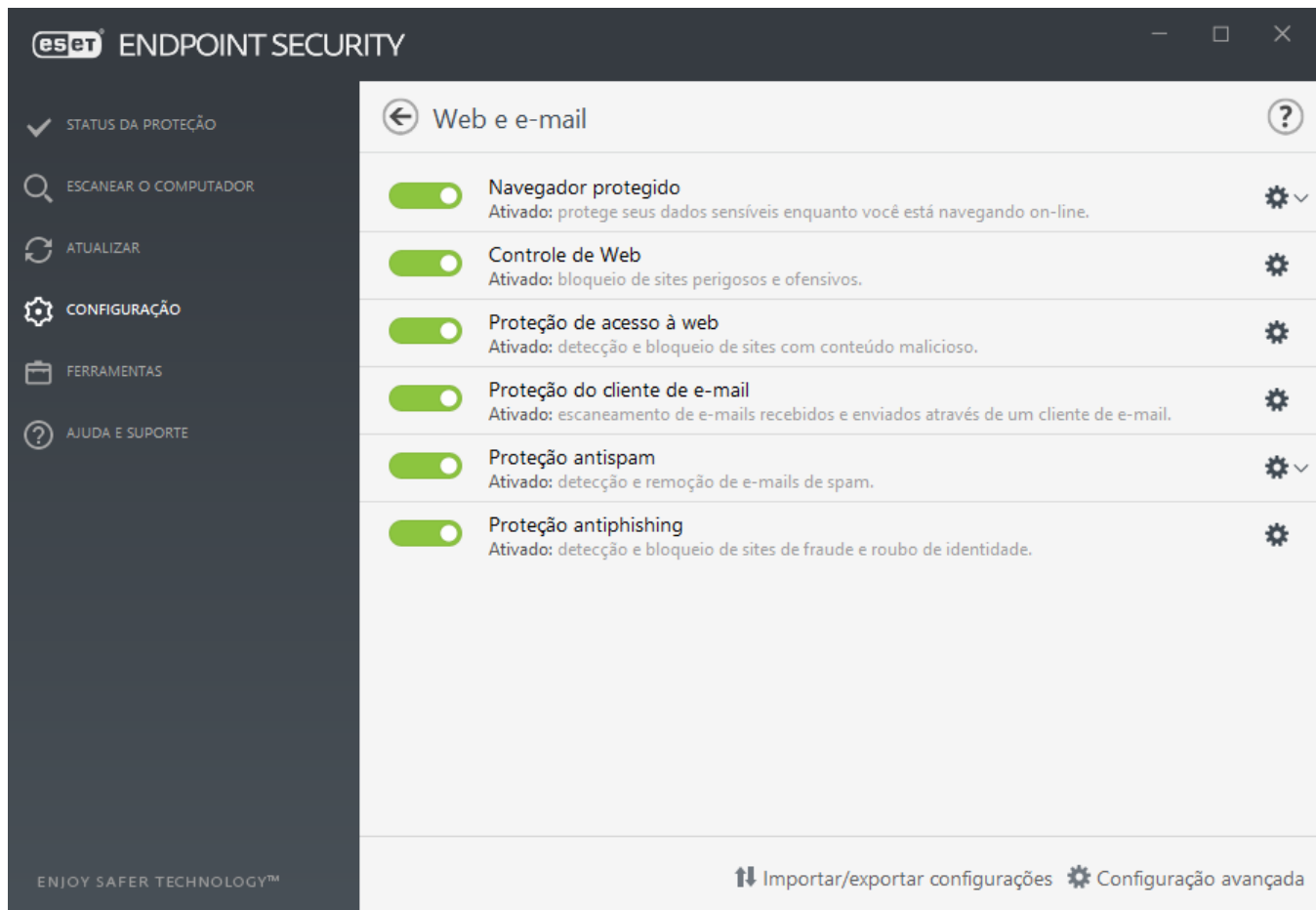
Quando você ativar a filtragem de protocolo SSL, o ESET Endpoint Security certifica-se de que aplicativos instalados confiem na forma como ele filtra protocolo SSL importando um certificado para a loja de certificados. Para alguns aplicativos, isso não é possível enquanto eles estiverem em execução. Isso inclui Firefox e Opera. Certifique-se de que nenhum deles esteja em execução (a melhor forma de fazer isso é abrir o Gerenciador de tarefas e certificar-se de que não haja firefox.exe ou opera.exe na guia Processos) e então tente novamente.

Erro sobre assinatura inválida ou emissor não confiável

Isso muito provavelmente significa que a importação descrita acima falhou. Primeiro, certifique-se de que nenhum dos aplicativos mencionados esteja em execução. Em seguida, desative a filtragem de protocolo SSL e a ative novamente. Isso executará novamente a importação.

Web e e-mail

Configuração de Web e email pode ser encontrada em **Configuração > Web e email**. A partir daqui, você pode acessar configurações mais detalhadas do programa.



Navegador protegido – Protege seus dados sensíveis enquanto você está navegando on-line.

O **módulo Controle de Web** permite configurar as definições, fornecendo aos administradores ferramentas automatizadas que ajudam a proteger as estações de trabalho e a definir restrições para navegação na internet. O objetivo da funcionalidade de controle da Web é impedir o acesso a páginas com conteúdos impróprios ou prejudiciais. Para obter mais informações, consulte [controle da Web](#).

A conectividade com a Internet é um recurso padrão em computadores pessoais. Infelizmente, a Internet tornou-se o meio principal de distribuição de códigos maliciosos. Por esse motivo, é essencial refletir com atenção sobre as suas configurações de [Proteção do acesso à Web](#).

A [Proteção do cliente de email](#) fornece controle da comunicação por email recebida através dos protocolos POP3(S) e IMAP(S). Usando o plug-in do cliente de email, o ESET Endpoint Security permite controlar todas as comunicações vindas através do cliente de email.


A [Proteção antispam](#) filtra mensagens de email não solicitadas.

Ao clicar na roda de engrenagem  ao lado de Proteção antispam, as seguintes opções estarão disponíveis:

Configurar - Abre configurações avançadas para proteção antispam de cliente de email.

Lista de endereços do usuário - Abre uma janela de diálogo onde pode adicionar, editar ou excluir endereços de email considerados seguros ou não seguros. De acordo com as regras definidas aqui, o email desses endereços não será rastreado nem será tratado como spam. Clique em Lista de exceções do usuário para abrir um diálogo onde é possível adicionar, editar ou excluir endereços de email que podem ser falsos e usados para o envio de spam. As mensagens de email de endereços relacionados na Lista de exceções serão sempre rastreadas quanto a spam.

Proteção antiphishing é outra camada de proteção que fornece um nível superior de defesa de sites ilegítimos que tentam adquirir senhas e outras informações confidenciais. A Proteção antiphishing pode ser encontrada no painel Configuração em Web e email. Para obter mais informações, consulte [Proteção antiphishing](#).

Você pode desativar o web/email/antiphishing/antispam temporariamente clicando em .

Filtragem de protocolos

A proteção antivírus para os protocolos dos aplicativos é fornecida pelo mecanismo de escaneamento ThreatSense, que integra perfeitamente todas as técnicas avançadas de escaneamento de malware. A filtragem de protocolo funciona automaticamente, independentemente do navegador da Internet ou do cliente de e-mail utilizado. Para editar configurações criptografadas (SSL), vá para **Configuração avançada (F5) > Web e e-mail > SSL/TLS**.

Ativar filtragem de conteúdo do protocolo de aplicativo - Essa opção pode ser usada para desativar a filtragem de protocolo. Observe que muitos componentes do ESET Endpoint Security (Proteção do acesso à Web, Proteção de protocolos de email, Antiphishing, Controle de Web) dependem disso e não funcionarão sem ele.

Aplicativos excluídos - Permite que você exclua aplicativos específicos da filtragem de protocolo. Útil quando a filtragem de protocolo causar problemas de compatibilidade.

Endereços IP excluídos - Permite que você exclua endereços remotos específicos da filtragem de protocolo. Útil quando a filtragem de protocolo causar problemas de compatibilidade.

Endereços IPv4 e máscara:

- **192.168.0.10** - Adiciona o endereço IP de um computador individual para o qual a regra é aplicada.
- **192.168.0.1 a 192.168.0.99** - Digite o início e o fim do endereço IP para especificar o intervalo IP (de vários computadores) para o qual a regra será aplicada.
- Sub-rede (um grupo de computadores) definida por um endereço IP e máscara. Por exemplo, **255.255.255.0** é a máscara de rede para o prefixo **192.168.1.0/24**, que significa o intervalo de endereços de **192.168.1.1 a 192.168.1.254**.

Endereços IPv6 e máscara:

- **2001:718:1c01:16:214:22ff:fec9:ca5** – O endereço IPv6 de um computador individual para o qual a regra é aplicada
- **2002:c0a8:6301:1::1/64** – Endereço IPv6 com o prefixo de comprimento de 64 bits, que significa **2002:c0a8:6301:0001:0000:0000:0000:0000 a 2002:c0a8:6301:0001:ffff:ffff:ffff:ffff**

Aplicativos excluídos

Para excluir da filtragem de protocolos a comunicação de aplicativos específicos que possuem direito de acesso à rede, adicione-os à lista. A comunicação HTTP/POP3/IMAP dos aplicativos selecionados não será verificada quanto a ameaças. Recomendamos que você use essa técnica somente em casos em que aplicativos não funcionarem devidamente com a filtragem de protocolos ativada.

Aplicativos e serviços que já tiverem sido afetados pela filtragem de protocolos serão automaticamente exibidos depois que você clicar em **Adicionar**.

Editar - Edite as entradas selecionadas da lista.

Remover – Remove as entradas selecionadas da lista.

Aplicativos excluídos

Adicionar

Editar

Excluir

Importar

Exportar

OK

Cancelar

C:\Windows\System32\svchost.exe
C:\Program Files\Notepad++\notepad++.exe

Endereços IP excluídos

Endereços IP nesta lista serão excluídos da filtragem de conteúdo de protocolo. A comunicação HTTP/POP3/IMAP de/para os endereços selecionados não será verificada quanto a ameaças. Recomendamos que use essa opção apenas para endereços conhecidos como sendo confiáveis.

Adicionar - Clique para adicionar um endereço IP/intervalo de endereços/sub-rede de um ponto remoto para o qual a regra é aplicada.

Editar - Edite as entradas selecionadas da lista.

Remover – Remove as entradas selecionadas da lista.

Endereços IP excluídos

Adicionar

Editar

Excluir

Importar

Exportar

OK

Cancelar

10.1.2.3
10.2.1.1-10.2.1.10
192.168.1.0/255.255.255.0
fe80::b434:b801:e878:5975
2001:21:420::/64

SSL/TLS

O ESET Endpoint Security é capaz de verificar se há ameaças em comunicações que usam o protocolo SSL. É possível usar vários modos de rastreamento para examinar comunicações protegidas por SSL com certificados confiáveis, certificados desconhecidos ou certificados excluídos da verificação das comunicações protegidas por SSL.

Ativar filtragem de protocolo SSL/TLS – A filtragem de protocolo está ativada como padrão. Você pode desativar a filtragem de protocolo SSL/TLS na **Configuração avançada > Web e email SSL/TLS** ou através da política. Se a filtragem de protocolo estiver desativada, o programa não escaneará as comunicações em SSL.

Modo de filtragem de protocolo SSL/TLS está disponível nas seguintes opções:


Modo de filtragem	Descrição
Modo automático	O modo padrão vai rastrear apenas aplicativos adequados como navegadores da Web e clientes de email. É possível cancelar selecionando os aplicativos para os quais as comunicações serão rastreadas.
Modo interativo	Se você entrar em um novo site protegido por SSL- (com um certificado desconhecido), uma caixa de diálogo de seleção de ação será exibida. Esse modo permite criar uma lista de certificados SSL / aplicativos que serão excluídos do rastreamento.
Modo de política	Selecione essa opção para rastrear todas as comunicações protegidas por SSL, exceto as comunicações protegidas por certificados excluídos da verificação. Se uma nova comunicação que utiliza um certificado desconhecido e assinado for estabelecida, você não será notificado e a comunicação será filtrada automaticamente. Ao acessar um servidor com um certificado não confiável marcado como confiável (ele está na lista de certificados confiáveis), a comunicação com o servidor será permitida e o conteúdo do canal de comunicação será filtrado.

A **Lista de aplicativos SSL/TLS filtrados** pode ser usada para personalizar o comportamento do ESET Endpoint Security para aplicativos específicos

A **Lista de certificados conhecidos** permite que você personalize o comportamento do ESET Endpoint Security para certificados SSL específicos.

Excluir comunicação com domínios confiáveis - Quando ativado, a comunicação com domínios confiáveis será excluída da verificação. A confiabilidade do domínio é determinada pela lista de permissões interna.

Bloquear comunicação criptografada utilizando o protocolo obsoleto SSL v2 - a comunicação que utiliza a versão anterior do protocolo SSL será bloqueada automaticamente.

 Os endereços não serão filtrados se a configuração **Excluir comunicação com domínios confiáveis** estiver ativada e o domínio for considerado como confiável.

Certificado raiz

Certificado raiz - Para que a comunicação SSL funcione adequadamente nos seus navegadores/clientes de email, é fundamental que o certificado raiz da ESET seja adicionado à lista de certificados raiz conhecidos (editores). **Adicionar o certificado raiz aos navegadores conhecidos** deve estar ativado. Selecione essa opção para adicionar automaticamente o certificado raiz da ESET aos navegadores conhecidos (por exemplo, Opera

e Firefox). Para navegadores que utilizam o armazenamento de certificação do sistema, o certificado será adicionado automaticamente (por exemplo, no Internet Explorer).

Para aplicar o certificado a navegadores não suportados, clique em **Exibir certificado > Detalhes > Copiar para arquivo** e importe-o manualmente para o navegador.


Validade do certificado

Ação se não for possível estabelecer a confiança do certificado – em alguns casos, um certificado de site não pode ser verificado usando o depósito de Autoridades de Certificação Raiz Confiáveis (TRCA) (por exemplo, certificado expirado, certificado não confiável, certificado não válido para o domínio específico ou assinatura que pode ser analisada, mas não assina o certificado corretamente). Sites legítimos sempre usarão certificados confiáveis. Se eles não estiverem fornecendo um, isso pode significar que um invasor está descriptografando sua comunicação ou o site está enfrentando dificuldades técnicas.

Se **Perguntar sobre validade do certificado** estiver selecionado (selecionado por padrão), o usuário será solicitado a selecionar uma ação a ser tomada quando for estabelecida a comunicação criptografada. Uma caixa de diálogo de seleção de ação será exibida, na qual você decidirá marcar o certificado como confiável ou excluído. Se o certificado não estiver presente na lista TRCA, a janela estará vermelha. Se o certificado estiver na lista TRCA, a janela estará verde.

Você pode selecionar **Bloquear comunicação que usa o certificado** para sempre encerrar uma conexão criptografada com um site que usa um certificado não confiável.

Ação para certificados corrompidos – um certificado corrompido significa que o certificado usa um formato não reconhecido pelo ESET Endpoint Security ou que foi recebido danificado (por exemplo, substituído por dados aleatórios). Nesse caso, recomendamos que você deixe **Bloquear a comunicação que utiliza o certificado** selecionado. Se **Perguntar sobre a validade do certificado** estiver selecionado, o usuário será solicitado a selecionar uma ação a ser tomada quando a comunicação criptografada for estabelecida.

 Os artigos da Base de conhecimento da ESET a seguir podem estar disponíveis apenas em inglês:

- [Notificações de certificado em produtos ESET](#)
- [“Tráfego de rede criptografado: certificado não confiável” é exibido ao visitar páginas da web](#)

Certificados

Para que a comunicação SSL funcione adequadamente nos seus navegadores/clientes de email, é fundamental que o certificado raiz da ESET seja adicionado à lista de certificados raiz conhecidos (editores). **Adicionar o certificado raiz aos navegadores conhecidos** deve estar ativado. Selecione essa opção para adicionar automaticamente o certificado raiz da ESET aos navegadores conhecidos (por exemplo, Opera e Firefox). Para navegadores que utilizam o armazenamento de certificação do sistema, o certificado será adicionado automaticamente (ou seja, Internet Explorer). Para aplicar o certificado a navegadores não suportados, clique em **Exibir certificado > Detalhes > Copiar para arquivo** e importe-o manualmente para o navegador.

Em alguns casos, o certificado não pode ser verificado utilizando o armazenamento de Autoridades de certificação raiz confiáveis (por exemplo, VeriSign). Isso significa que o certificado é assinado automaticamente por alguém (por exemplo, pelo administrador de um servidor Web ou uma empresa de pequeno porte) e considerar este certificado como confiável nem sempre é um risco. A maioria dos negócios de grande porte (por exemplo, bancos) usa um certificado assinado por TRCA. Se **Perguntar sobre validade do certificado** estiver selecionado (selecionado por padrão), o usuário será solicitado a selecionar uma ação a ser tomada quando for

estabelecida a comunicação criptografada. Uma caixa de diálogo de seleção de ação será exibida, na qual você decidirá marcar o certificado como confiável ou excluído. Se o certificado não estiver presente na lista TRCA, a janela estará vermelha. Se o certificado estiver na lista TRCA, a janela estará verde.

Você poderá selecionar **Bloquear a comunicação que utiliza o certificado** para terminar sempre uma conexão criptografada para o site que usa o certificado não verificado.


Se o certificado não for válido ou estiver corrompido, isso significa que o certificado expirou ou estava assinado incorretamente. Nesse caso, recomendamos o bloqueio da comunicação que usa o certificado.

Tráfego de rede criptografado

Se seu sistema estiver configurado para usar o rastreamento de protocolo SSL, em duas situações será exibida uma janela de diálogo solicitando que você escolha uma ação:

Primeiro, se um site usar um certificado inválido ou que não possa ser verificado e o ESET Endpoint Security estiver configurado para perguntar ao usuário nesses casos (por padrão, sim para certificados que não podem ser verificados e não para inválidos), uma caixa de diálogo perguntará ao usuário se ele deseja **Permitir** ou **Bloquear** a conexão. Se o certificado não for localizado no Trusted Root Certification Authorities store (TRCA), ele é considerado não confiável.

Depois, se o **modo de filtragem de protocolo SSL** estiver definido como **Modo interativo**, uma caixa de diálogo para cada site perguntará se você deseja **Rastrear** ou **Ignorar** o tráfego. Alguns aplicativos verificam se o tráfego SSL não foi modificado ou inspecionado por outra pessoa, sendo que em tais casos o ESET Endpoint Security deve **Ignorar** esse tráfego para manter o aplicativo funcionando.

-  Os artigos da Base de conhecimento da ESET a seguir podem estar disponíveis apenas em inglês:
- [Notificações de certificado em produtos ESET](#)
 - ["Tráfego de rede criptografado: certificado não confiável" é exibido ao visitar páginas da web](#)

Em ambos os casos, o usuário pode escolher lembrar a ação selecionada. Ações salvas serão armazenadas na [Lista de certificados conhecidos](#).

Lista de certificados conhecidos

A **Lista de certificados conhecidos** pode ser usada para personalizar o comportamento do ESET Endpoint Security para certificados SSL específicos, bem como para lembrar ações escolhidas se o **Modo interativo** estiver selecionado no **Modo de filtragem de protocolo SSL/TLS**. A lista pode ser visualizada e editada em **Configuração avançada** (F5) > **Web e email** > **SSL/TLS** > **Lista de certificados conhecidos**.

A janela **Lista de certificados conhecidos** consiste em:

Colunas

Nome - nome do certificado.

Emissor de certificado - nome do criador do certificado.

Assunto do certificado - o campo de assunto identifica a entidade associada à chave pública armazenada no campo de chave pública do assunto.

Acesso - Selecione **Permitir** ou **Bloquear como a Ação de acesso** para permitir/bloquear a comunicação garantida por este certificado, independentemente de sua confiabilidade. Selecione **Automático** para permitir certificados confiáveis e perguntar para não confiáveis. Selecione **Perguntar** para sempre perguntar ao usuário o que fazer.

Rastreamento - Selecione **Rastrear** ou **Ignorar** como a **Ação de rastreamento** para rastrear ou ignorar a comunicação protegida por este certificado. Selecione **Automático** para rastrear no modo automático e perguntar no modo interativo. Selecione **Perguntar** para sempre perguntar ao usuário o que fazer.

Elementos de controle

Adicionar - Um certificado pode ser carregado manualmente como um arquivo com extensão *.cer*, *.crt* ou *.pem*. Clique em **Arquivo** para carregar um certificado local ou clique em **URL** para especificar a localização de um certificado on-line.

Editar - Selecione o certificado que deseja configurar e clique em **Editar**.

Excluir - selecione o certificado que deseja excluir e clique em **Remover**.

OK/Cancelar - Clique em **OK** se quiser salvar alterações ou clique em **Cancelar** para sair sem salvar.

Lista de aplicativos SSL/TLS filtrados

A **Lista de aplicativos SSL/TLS filtrados** pode ser usada para personalizar o comportamento do ESET Endpoint Security para aplicativos específicos, bem como para lembrar ações escolhidas se o **Modo interativo** estiver selecionado no **Modo de filtragem de protocolo SSL/TLS**. A lista pode ser visualizada e editada na **Configuração avançada** (F5) > **Web e e-mail** > **SSL/TLS** > **Lista de aplicativos SSL/TLS filtrados**.

A janela da **Lista de aplicativos SSL/TLS filtrados** consiste em:

Colunas

Aplicativo - Escolha um arquivo executável na árvore de diretórios, clique na opção ... ou insira o caminho manualmente.

Ação de rastreamento – Selecione **Rastrear** ou **Ignorar**. Selecione **Automático** para rastrear no modo automático e perguntar no modo interativo. Selecione **Perguntar** para sempre perguntar ao usuário o que fazer.

Elementos de controle

Adicionar - Adicionar aplicativo filtrado.

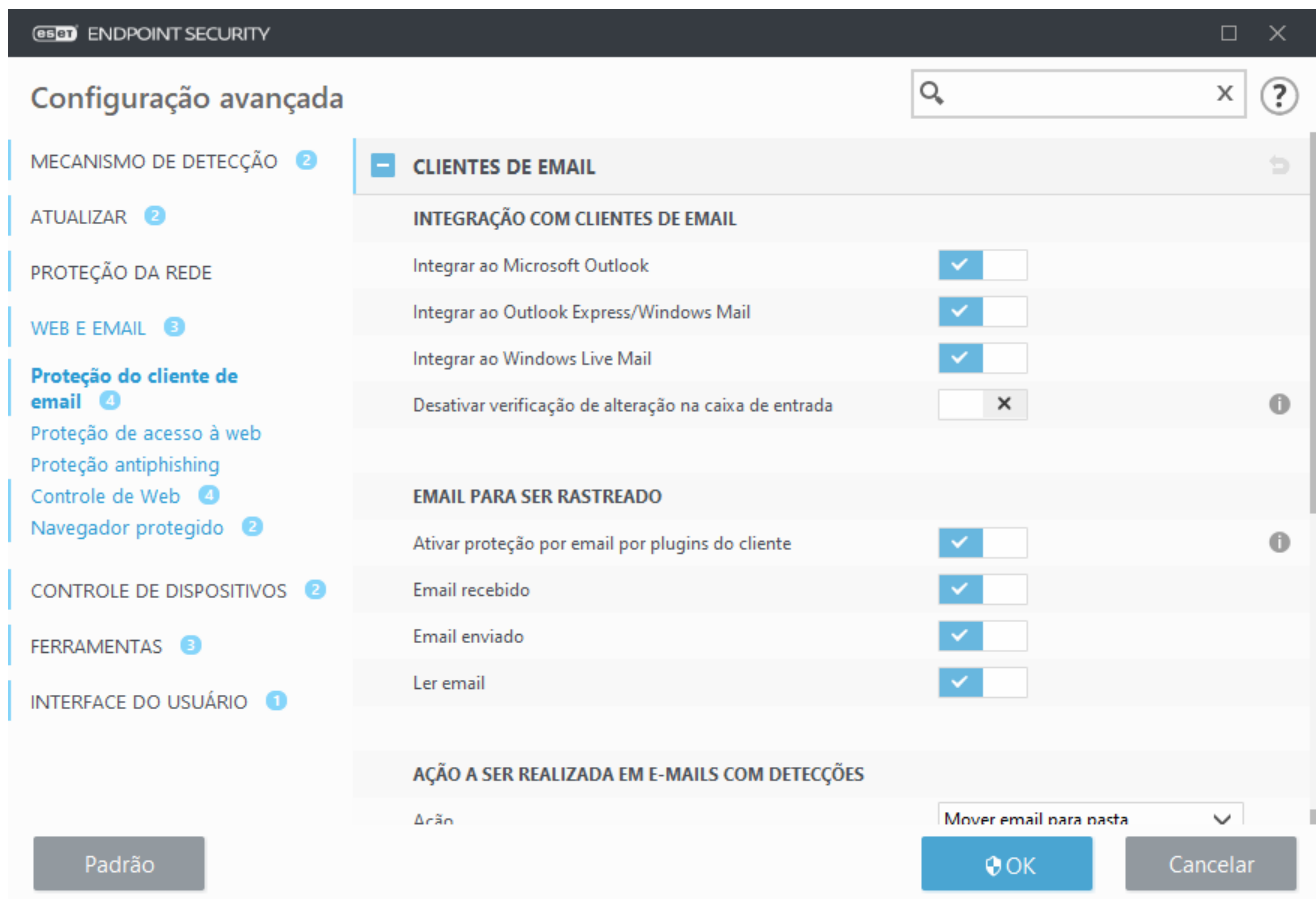
Editar - Selecione o certificado que deseja configurar e clique em **Editar**.

Excluir - selecione o certificado que deseja excluir e clique em **Remover**.

OK/Cancelar - Clique em **OK** se quiser salvar alterações ou clique em **Cancelar** se quiser sair sem salvar.

Proteção do cliente de e-mail

A integração do ESET Endpoint Security com seu cliente de e-mail aumenta o nível de proteção ativa em relação ao código malicioso nas mensagens de e-mail. Se o seu cliente de email for compatível, essa integração poderá ser ativada no ESET Endpoint Security. Quando integrado no seu cliente de email, a barra de ferramentas ESET Endpoint Security é inserida diretamente no cliente de email para uma proteção de email mais eficiente. Configurações de integração estão localizadas em **Configuração avançada (F5) > Web e email > Proteção do cliente de email > Clientes de email**.



Email para ser rastreado

Ativar proteção por e-mail por plugins do cliente – Quando desativado, a proteção por e-mail por plugins do cliente está desativada.

E-mail recebido – Verifica as mensagens de e-mail que são recebidas quando ativado.

E-mail enviado – Verifica as mensagens de e-mail que são enviadas quando ativado.

Ler email – Verifica as mensagens de e-mail que são lidas quando ativado.



Recomendamos manter a opção **Ativar proteção por e-mail por plugins do cliente** ativada. Mesmo se a integração não estiver ativada ou funcional, as comunicações por e-mail ainda estarão protegidas pela [Filtragem de protocolo](#) (IMAP/IMAPS e POP3/POP3S).

Ação que será executada no email infectado

Nenhuma ação – Se ativada, o programa identificará anexos infectados, mas não será tomada qualquer ação em relação aos emails.

Excluir email – O programa notificará o usuário sobre infiltrações e excluirá a mensagem.

Mover email para a pasta Itens excluídos - Os emails infectados serão movidos automaticamente para a pasta Itens excluídos.

Mover email para a pasta (ação padrão) – Os emails infectados serão movidos automaticamente para a pasta especificada.

Pasta - Especifique a pasta personalizada para a qual você deseja mover os emails infectados quando detectados.

Repetir o escaneamento após atualização – Faz um novo escaneamento dos e-mails infectados depois de uma atualização do mecanismo de detecção, quando ativado.

Aceitar resultados de escaneamento de outros módulos – Permite que o módulo de proteção de e-mail use os resultados de escaneamento recebidos de outros módulos de proteção em vez de fazer novamente o escaneamento.

Protocolos de e-mail

Os protocolos IMAP e POP3 são os protocolos mais amplamente utilizados para receber comunicação em um aplicativo cliente de e-mail. O IMAP (Internet Message Access Protocol) é outro protocolo de Internet para recuperação de e-mails. O IMAP tem algumas vantagens sobre o POP3, por exemplo, vários clientes podem se conectar simultaneamente à mesma caixa de entrada e gerenciar informações de estado das mensagens, tais como se a mensagem foi ou não lida, respondida ou removida. O módulo de proteção que fornece esse controle é iniciado automaticamente na inicialização do sistema e depois fica ativo na memória.

O ESET Endpoint Security fornece proteção para estes protocolos, independentemente do cliente de e-mail usado, sem necessidade de reconfiguração do cliente de e-mail. Por padrão, todas as comunicações feitas por meio dos protocolos POP3 e IMAP são escaneadas, independentemente dos números padrão de porta POP3/IMAP.

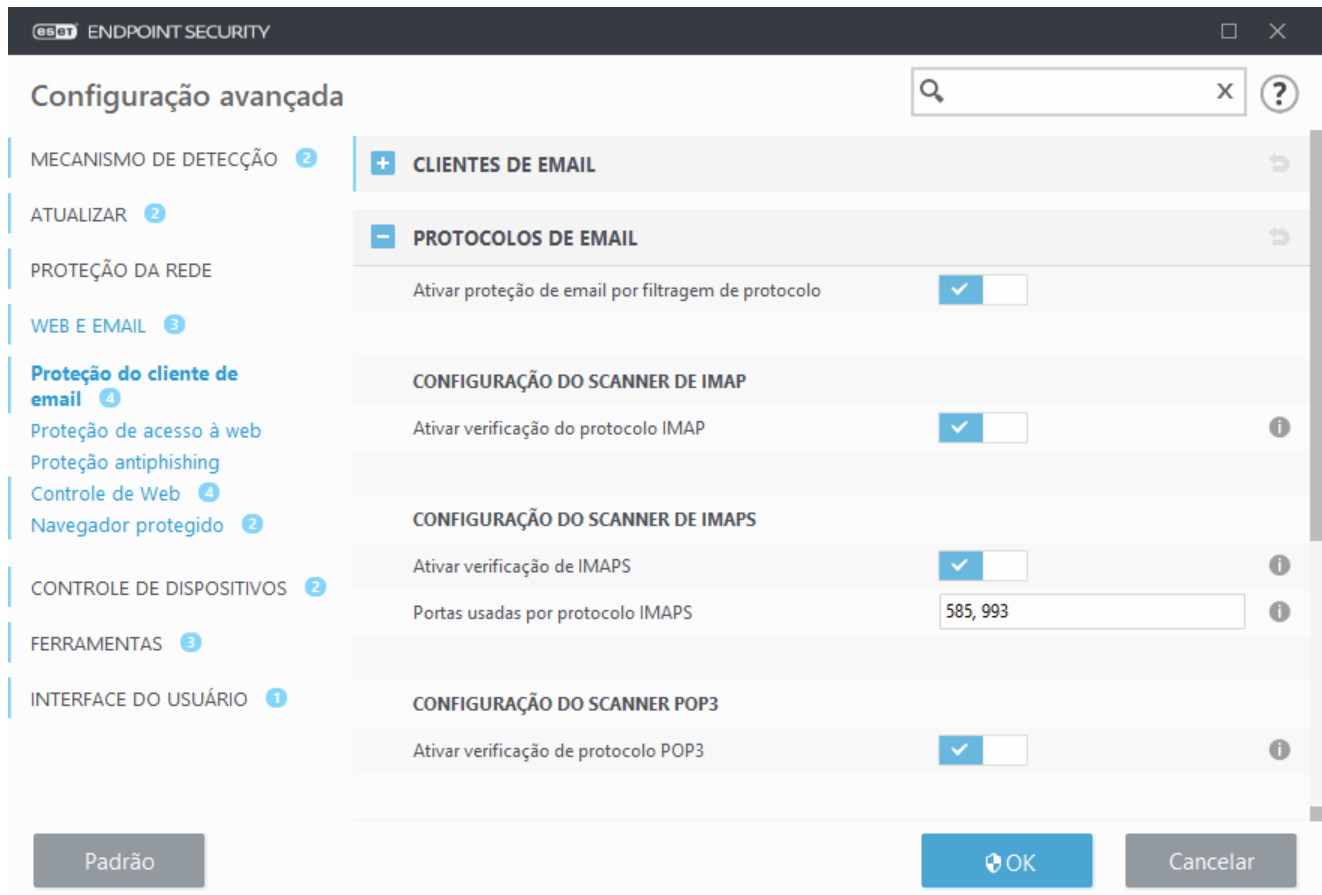
O protocolo MAPI não é escaneado. Porém, a comunicação com o servidor Microsoft Exchange pode ser escaneada pelo [módulo de integração](#) em clientes de e-mail como o Microsoft Outlook.

Recomendamos que você mantenha **Ativar proteção por e-mail por filtragem de protocolo** ativado. Para configurar a verificação de protocolo IMAP/IMAPS e POP3/POP3S, vá para Configuração avançada > **Web e e-mail** > **Proteção do cliente de e-mail** > **Protocolos de e-mail**.

O ESET Endpoint Security também é compatível com o escaneamento de protocolos IMAPS (585, 993) e POP3S (995), que utilizam um canal criptografado para transferir as informações entre servidor e cliente. O ESET Endpoint Security verifica as comunicações utilizando os protocolos SSL (Camada de soquete seguro) e TLS (Segurança da camada de transporte). O programa escaneará somente tráfego em portas definidas em **Portas usadas pelo protocolo IMAPS/POP3S**, independentemente da versão do sistema operacional. Podem ser adicionadas outras portas de comunicação, se necessário. Vários números das portas devem ser delimitados por vírgula.

A comunicação criptografada será escaneada por padrão. Para visualizar a configuração do escaneador, vá para

[SSL/TLS](#) na seção Configuração avançada, clique em **Web e email** > **SSL/TLS** e selecione a opção **Ativar filtragem de protocolo SSL/TLS**.



Marcações de e-mail

As opções dessa funcionalidade estão disponíveis em **Configuração avançada em Web e email** > **Proteção do cliente de email** > **Alertas e notificações**.

Depois que um e-mail foi verificado, uma notificação com o resultado do escaneamento pode ser anexada na mensagem. É possível selecionar **Acrescentar mensagem de marca nos e-mails recebidos e lidos** ou **Acrescentar mensagens de marca a e-mail enviado**. Esteja ciente que em algumas ocasiões raras as mensagens de marca podem ser omitidas em mensagens HTML problemáticas ou se mensagem forem forjadas por malware. As mensagens de marca podem ser adicionadas a um e-mail recebido e lido ou a um e-mail enviado, ou ambos. As opções disponíveis são:

- **Nunca** - nenhuma mensagem de marca será adicionada.
- **Quando ocorrer uma detecção** – Apenas mensagens contendo software malicioso serão marcadas como verificadas (padrão).
- **Todos os e-mails quando escaneados** – O programa vai incluir mensagens em todos os e-mails escaneados.

Atualizar assunto do e-mail enviado – Desative essa opção se você quiser que a proteção de e-mail inclua um alerta de vírus no assunto de um e-mail infectado. Esse recurso permite a filtragem simples de e-mail infectado com base em assunto (se isso for compatível com o seu programa de e-mail). Esse recurso aumenta o nível de credibilidade para os destinatários e, se nenhuma infiltração for detectada, ele fornece informações valiosas sobre o nível de ameaça do e-mail ou do remetente.

Texto a adicionar ao assunto de e-mail infectado – Edite esse modelo se quiser modificar o formato de prefixo do assunto de um e-mail infectado. Essa função substituirá o assunto da mensagem "Olá" com o seguinte formato: "[detecção %DETECTIONNAME%] Olá". A variável %DETECTIONNAME% representa a detecção.

Integração com clientes de email

Os clientes de email atualmente suportados incluem o [Microsoft Outlook](#), [Outlook Express](#), [Windows Mail](#) e Windows Live Mail. A proteção de email funciona como um plug-in para esses programas. A principal vantagem do plug-in é que ele não depende do protocolo usado. Quando o cliente de email recebe uma mensagem criptografada, ela é descriptografada e enviada para o scanner de vírus. Para obter uma lista completa dos clientes de email suportados e suas versões, consulte o seguinte artigo da [Base de conhecimento da ESET](#).

Configurações especiais

Otimização de tratamento de anexo – se a otimização estiver desativada, todos os anexos serão escaneados imediatamente. Quando desativado, isso pode diminuir a velocidade do desempenho do cliente de e-mail.

Processamento avançado do cliente de e-mail – se houver redução na velocidade do sistema ao trabalhar com o seu cliente de e-mail, desative esta opção.

Barra de ferramentas do Microsoft Outlook

A proteção do Microsoft Outlook funciona como um módulo de plug-in. Após a instalação do ESET Endpoint Security, essa barra de ferramentas contendo as opções de proteção de antivírus/antispam é adicionada ao Microsoft Outlook:

Spam – Marca as mensagens escolhidas como spam. Depois de marcar, uma "impressão digital" da mensagem será enviada a um servidor central que armazena as assinaturas de spam. Se o servidor receber mais "impressões digitais" semelhantes de vários usuários, a mensagem será classificada como spam no futuro.

Não é spam – Marca as mensagens escolhidas como não sendo spam.

Endereço de spam (lista de proibições, uma lista de endereços de spam) - Adiciona um novo endereço de remetente à [Lista de proibições](#). Todas as mensagens recebidas da lista serão automaticamente classificadas como spam.



Esteja atento à falsificação - forjar um endereço de remetente em mensagens de email para enganar os destinatários do email na leitura e na resposta.

Endereço confiável (lista de permissões, uma lista de endereços confiáveis) - Adiciona um novo endereço de remetente à Lista de permissões. Todas as mensagens recebidas de endereços da Lista de permissões nunca serão classificadas automaticamente como spam.

ESET Endpoint Security - Clique no ícone para abrir a janela do programa principal do ESET Endpoint Security.

Rastrear novamente mensagens – Permite iniciar o rastreamento de emails manualmente. Você pode especificar as mensagens que serão rastreadas e ativar o novo rastreamento do email recebido. Para obter mais informações, consulte [Proteção do cliente de email](#).

Configuração do scanner - exibe as opções de configuração da [Proteção do cliente de email](#).

Configuração do antispam - Exibe as opções de configuração da [Proteção antispam](#).

Catálogos de endereço - Abre a janela de proteção antispam, onde é possível acessar listas de endereços excluídos, confiáveis e de spam.

Barra de ferramentas do Outlook Express e do Windows Mail

A proteção do Outlook Express e do Windows Mail funciona como um módulo de plug-in. Após a instalação do ESET Endpoint Security, essa barra de ferramentas contendo as opções de proteção de antivírus/antispam é adicionada ao Outlook Express ou ao Windows Mail:

Spam – Marca as mensagens escolhidas como spam. Depois de marcar, uma "impressão digital" da mensagem será enviada a um servidor central que armazena as assinaturas de spam. Se o servidor receber mais "impressões digitais" semelhantes de vários usuários, a mensagem será classificada como spam no futuro.

Não é spam – Marca as mensagens escolhidas como não sendo spam.

Endereço de spam - Adiciona um novo endereço de remetente à [Lista de proibições](#). Todas as mensagens recebidas da lista serão automaticamente classificadas como spam.



Esteja atento à falsificação - forjar um endereço de remetente em mensagens de email para enganar os destinatários do email na leitura e na resposta.

Endereço confiável - Adiciona um novo endereço de remetente à Lista de permissões. Todas as mensagens recebidas de endereços da Lista de permissões nunca serão classificadas automaticamente como spam.

ESET Endpoint Security - Clique no ícone para abrir a janela do programa principal do ESET Endpoint Security.

Rastrear novamente mensagens – Permite iniciar o rastreamento de emails manualmente. Você pode especificar as mensagens que serão rastreadas e ativar o novo rastreamento do email recebido. Para obter mais informações, consulte [Proteção do cliente de email](#).

Configuração do scanner - exibe as opções de configuração da [Proteção de cliente de email](#).

Configuração do antispam - Exibe as opções de configuração da [Proteção antispam](#).

Interface do usuário

Personalizar aparência - A aparência da barra de ferramentas pode ser modificada para o seu cliente de email. Desmarque a opção para personalizar a aparência, independentemente dos parâmetros do programa de email.

Mostrar texto - Exibe as descrições dos ícones.

Texto à direita - as descrições da opção são movidas da parte inferior para o lado direito dos ícones.

Ícones grandes - Exibe ícones grandes para as opções de menu.

Caixa de diálogo de confirmação

Esta notificação serve para confirmar que o usuário realmente deseja realizar a ação selecionada, que deve eliminar possíveis erros.

Por outro lado, a caixa de diálogo também oferece a opção de desativar as confirmações.

Rastrear novamente mensagens

A barra de ferramentas do ESET Endpoint Security integrada em clientes de email permite que os usuários especifiquem diversas opções para a verificação de email. A opção **Rastrear novamente mensagens** fornece dois modos de rastreamento:

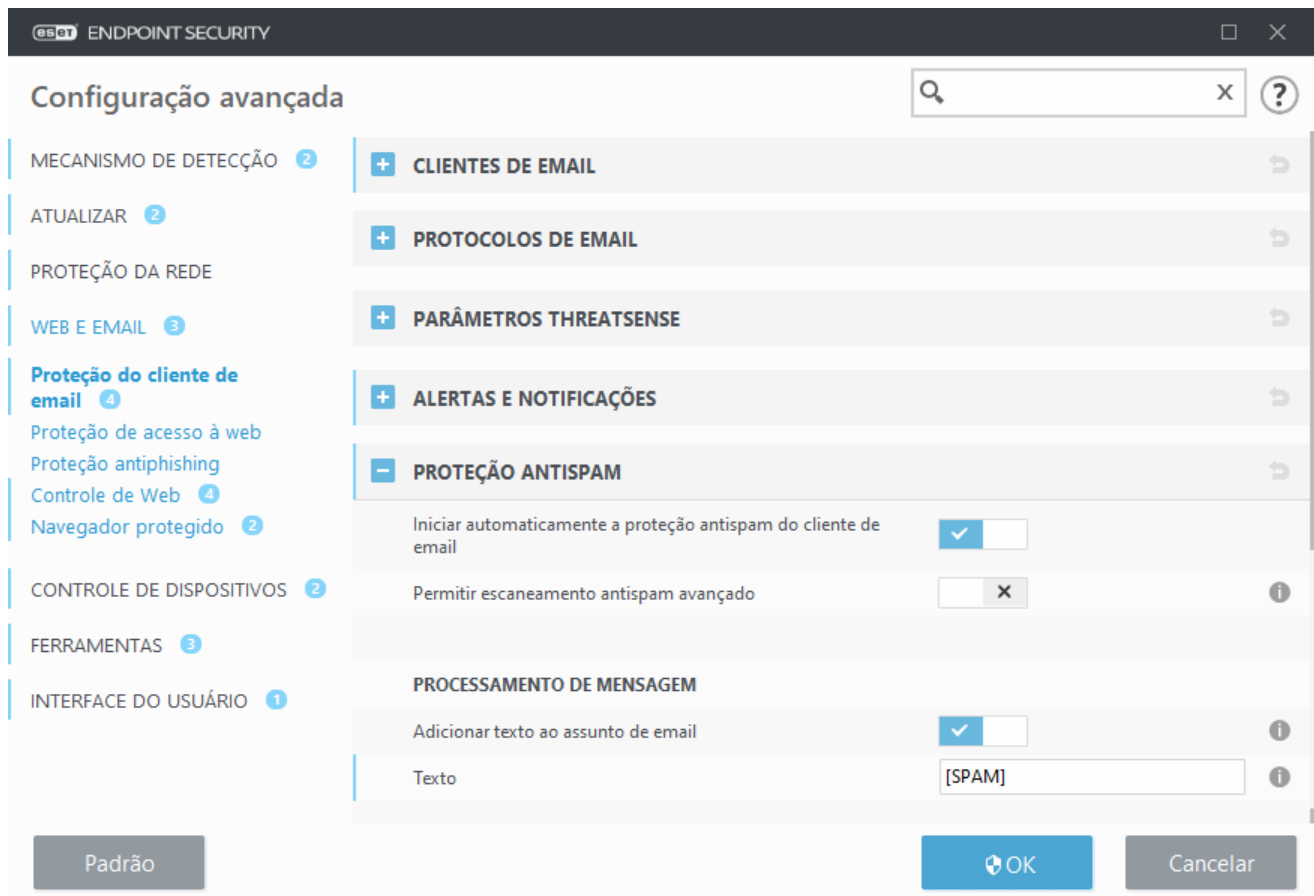
Todas as mensagens na pasta atual - rastreia as mensagens na pasta exibida no momento.

Apenas as mensagens selecionadas - Rastreia apenas as mensagens marcadas pelo usuário.

A caixa de seleção **Rastrear novamente as mensagens já rastreadas** possibilita ao usuário executar outro rastreamento nas mensagens que já foram rastreadas.

Proteção antispam

Os emails não solicitados, conhecidos como spams, estão entre os maiores problemas da comunicação eletrônica. Os spams representam até 50 por cento de toda a comunicação por email. A proteção Antispam serve para proteger contra esse problema. Combinando diversos princípios de segurança de -email, o módulo Antispam fornece filtragem superior para manter a caixa de entrada limpa.



Um princípio importante para a detecção do spam é a capacidade de reconhecer emails não solicitados com base em endereços confiáveis predefinidos (lista de permissões) e em endereços de spam (lista de proibições). Todos os endereços de sua lista de contatos são automaticamente acrescentados à lista de permissões, bem como todos os demais endereços marcados pelo usuário como seguros.

O principal método usado para detectar spam é o rastreamento das propriedades da mensagem de email. As mensagens recebidas são verificadas quanto aos critérios Antispam básicos (definições da mensagem, heurísticas estatísticas, reconhecimento de algoritmos e outros métodos únicos) e o valor do índice resultante determina se uma mensagem é spam ou não.

Iniciar automaticamente a proteção antispam do cliente de email - Quando ativada, a proteção antispam será ativada automaticamente na inicialização do sistema.

Permitir rastreamento antispam avançado - Dados antispam adicionais serão baixados periodicamente, aumentando as capacidades antispam e produzindo melhores resultados.

A proteção antispam no ESET Endpoint Security permite definir diferentes parâmetros para trabalhar com as listas de emails. As opções são:

Processamento de mensagens

Adicionar texto ao assunto de email - Permite adicionar uma cadeia de caracteres de prefixo personalizado à linha de assunto das mensagens classificadas como spam. O padrão é "[SPAM]".

Mover mensagens para pasta spam - Quando ativada, as mensagens de spam serão movidas para a pasta padrão de lixo eletrônico e as mensagens reclassificadas como não spam serão movidas para a caixa de entrada. Ao clicar com o botão direito em uma mensagem de email e selecionar ESET Endpoint Security no menu de contexto, é possível escolher das opções aplicáveis.

Usar a pasta – Especifique a pasta personalizada para a qual você deseja mover os emails infectados quando detectados.

Marcar mensagens de spam como lidas - Ative isto para marcar automaticamente spam como lido. Isso o ajudará a concentrar sua atenção em mensagens "limpas".

Marcar mensagens reclassificadas como não lidas - As mensagens originariamente classificadas como spam, mas posteriormente marcadas como "limpas" serão exibidas como não lidas.

Registro em relatório da pontuação de spam – o mecanismo antispam do ESET Endpoint Security atribui uma pontuação de spam a cada mensagem escaneada. A mensagem será registrada no [log de antispam](#) (ESET Endpoint Security > Ferramentas > Arquivos de relatório > Proteção antispam).

- **Nenhum** – A pontuação do rastreamento antispam não será registrada.
- **Reclassificado e marcado como spam** - Selecione isto se desejar registrar uma pontuação de spam para mensagens marcadas como SPAM.
- **Todas** - Todas as mensagens serão registradas no relatório com a pontuação de spam.

i Ao clicar em uma mensagem na pasta de email spam, é possível selecionar **Reclassificar mensagens selecionadas como NÃO spam** e a mensagem será movida para a caixa de entrada. Ao clicar em uma mensagem que você considera ser spam na caixa de entrada, selecione **Reclassificar mensagens como spam** e a mensagem será movida para a pasta de spam. Você pode selecionar várias mensagens e realizar a ação em todas elas ao mesmo tempo.

i o ESET Endpoint Security é compatível com a proteção antispam para Microsoft Outlook, Outlook Express, Windows Mail e Windows Live Mail.

Catálogos de endereços antispam

O recurso antispam no ESET Endpoint Security permite configurar diversos parâmetros para listas de endereços.

Catálogos de endereços

Permitir lista de endereços do usuário - Ative essa opção para ativar o catálogo de endereços criado por um usuário dentro de seu próprio cliente de email.

Permitir listas de endereços globais – Ative essa opção para ativar o catálogo de endereços global, que é compartilhado por todos os usuários nesta estação de trabalho, o serviço de diretórios dentro do sistema de e-mails. O GAL (Global Address List, catálogo de endereços global) contém informações de todos os usuários de e-mail, grupos de distribuição e recursos.

Lista de permissões do usuário - Lista de contatos onde você pode adicionar, editar ou excluir endereços de email considerados seguros, bem como dos quais o usuário deseja receber mensagens.

Lista de proibições do usuário - Lista de contatos onde você pode adicionar, editar ou excluir endereços de email não considerados seguros, bem como dos quais o usuário não deseja receber mensagens.

Lista de exceções do usuário - Essa lista de contatos contém endereços de email que podem ser falsificados e usados para o envio de spam. Consulte também a [lista de exceções](#).

Lista global de permissões/proibições/exceções – Essas listas são usadas para aplicar políticas globais antispam a todos os usuários que usam o ESET Endpoint Security nesta estação de trabalho. Quando o ESET Endpoint Security

é [gerenciado remotamente](#), a política ESET PROTECT/ECA será aplicada a todas as estações de trabalho atribuídas.

Adicionar automaticamente à lista de permissões do usuário

Adicionar endereços do catálogo de endereços - Adiciona endereços da sua lista de contatos à [Lista de permissões](#).

Adicionar endereços de destinatários de mensagens de saída - Adicione endereços de destinatários das mensagens enviadas à Lista de permissões.


Adicionar endereços de mensagens reclassificadas como NÃO spam - Adicione endereços de remetentes das mensagens reclassificadas como NÃO spam à Lista de permissões.

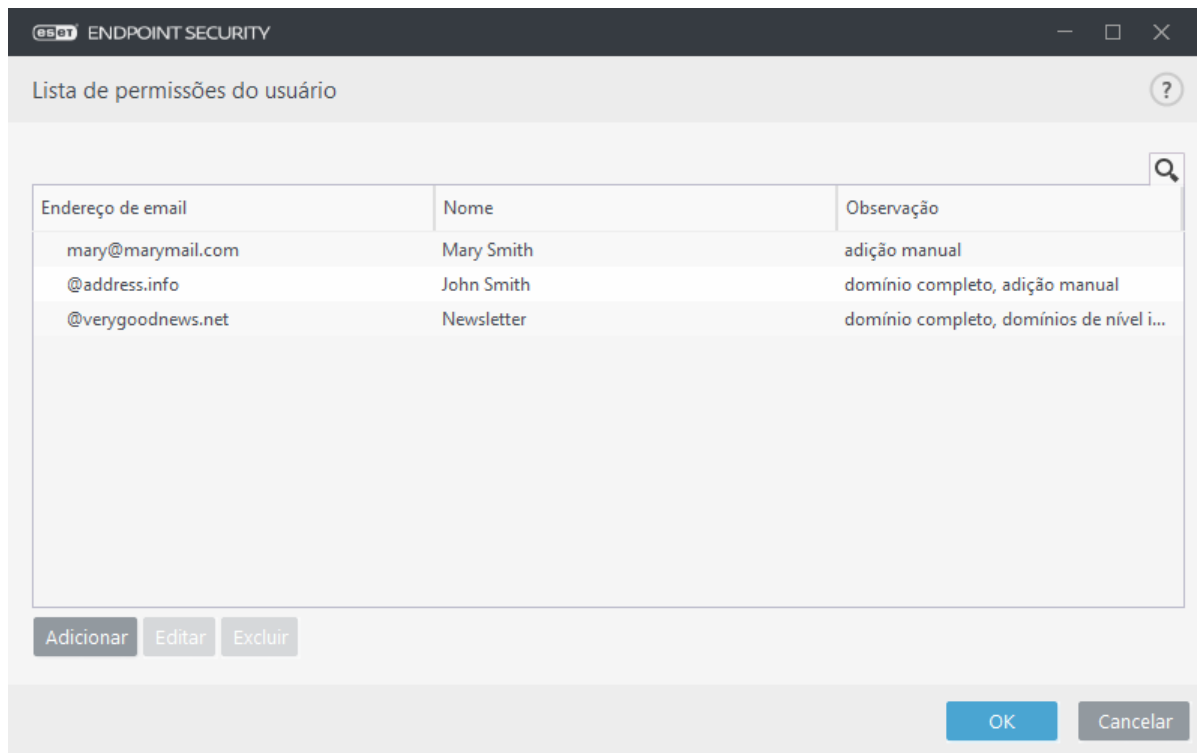
Adicionar automaticamente à lista de exceções do usuário

Adicionar endereços de contas próprias - Adiciona seus endereços das contas dos clientes de email existentes à [Lista de exceções](#).

Lista de proibições/Lista de permissões/Lista de exceções

Para fornecer proteção contra emails não solicitados, o ESET Endpoint Security permite classificar endereços de email usando listas especializadas. A [lista de permissões](#) contém endereços de email seguros. As mensagens de usuários na lista de permissões estão sempre disponíveis na pasta de email de entrada. A [lista de proibições](#) contém endereços de email classificados como spam, e todas as mensagens de remetentes na lista de proibições são marcadas de acordo. A lista de exceções contém endereços de email que são sempre verificados quanto a spam, mas também pode conter endereços de mensagens de email não solicitadas que podem não ser reconhecidas como spam inicialmente.

Todas as listas podem ser editadas da janela do programa principal do ESET Endpoint Security em **Configuração avançada > Web e e-mail > Proteção do cliente de e-mail > Catálogos de endereços antispam** usando os botões **Adicionar**, **Editar** e **Remover** em cada janela de diálogo da lista ou de **Configuração > Web e e-mail** depois que você clicar na roda de engrenagem  ao lado de **Proteção antispam**.



Por padrão, o ESET Endpoint Security adiciona à lista de permissões todos os endereços do catálogo de endereços de clientes de email compatíveis. Por padrão, a lista de proibições está vazia. Por padrão, a [lista de exceções](#) relaciona apenas os endereços de email do próprio usuário.

Adicionar/Editar endereço da Lista de proibições/Lista de permissões/Lista de exceções

Esta janela permite adicionar ou editar entradas na Lista de permissões ou na Lista de proibições. Abra a janela principal do programa do ESET Endpoint Security em **Configuração avançada > Web e e-mail > Proteção do cliente de e-mail > Livros de endereço antispam**.

Endereço de email - O endereço de email a ser adicionado/editado.

Nome - O nome da entrada.

Domínio completo - Selecione essa opção para a entrada a ser aplicada a todo o domínio do contato (não apenas ao endereço especificado no campo Endereço de email, mas em todos os endereços de email no domínio *address.info*).

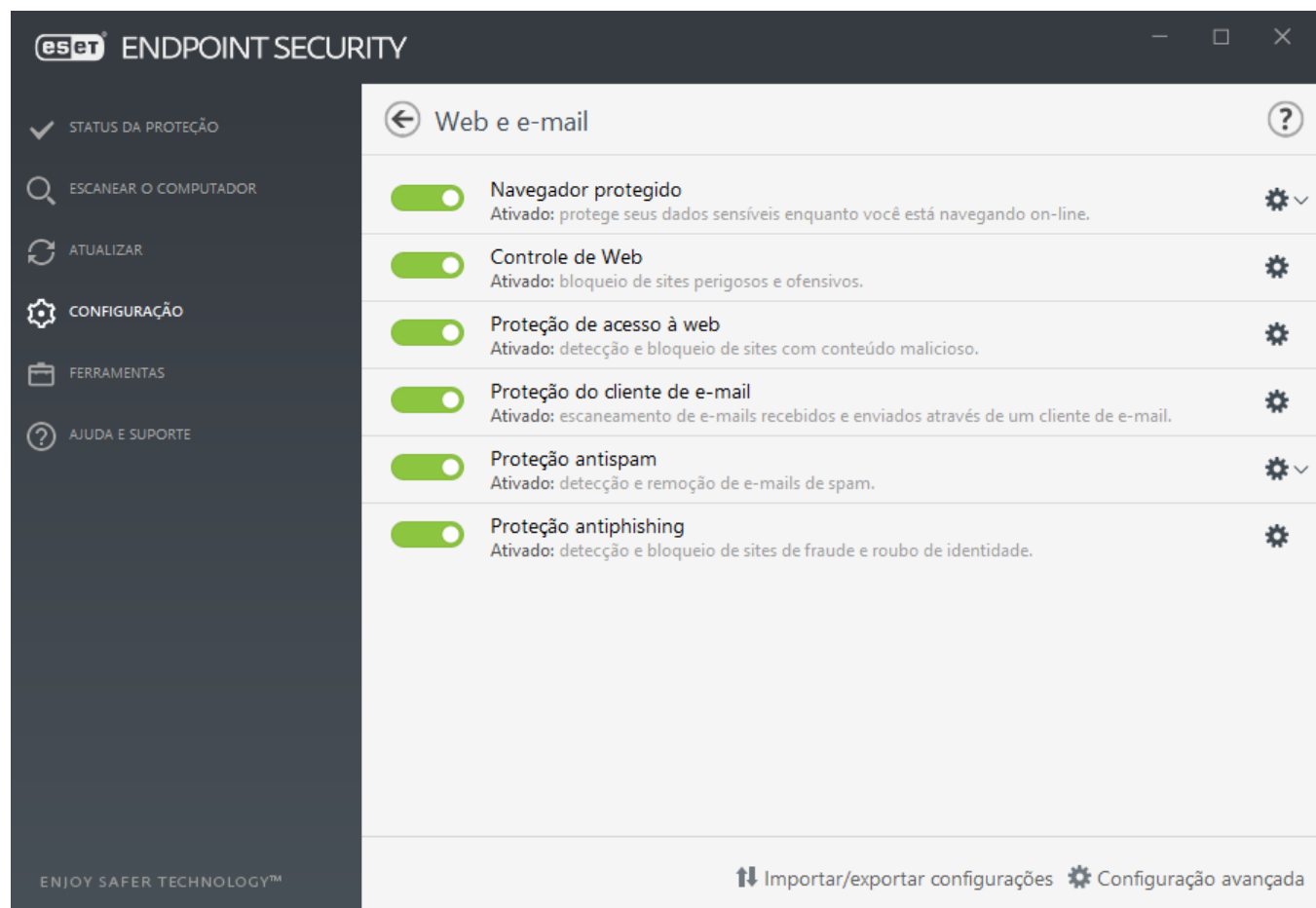
Domínios de nível inferior - Selecione essa opção para a entrada a ser aplicada ao domínio de nível inferior do contato (*address.info* representa um domínio e *my.address.info* representa um subdomínio).

Proteção de acesso à Web

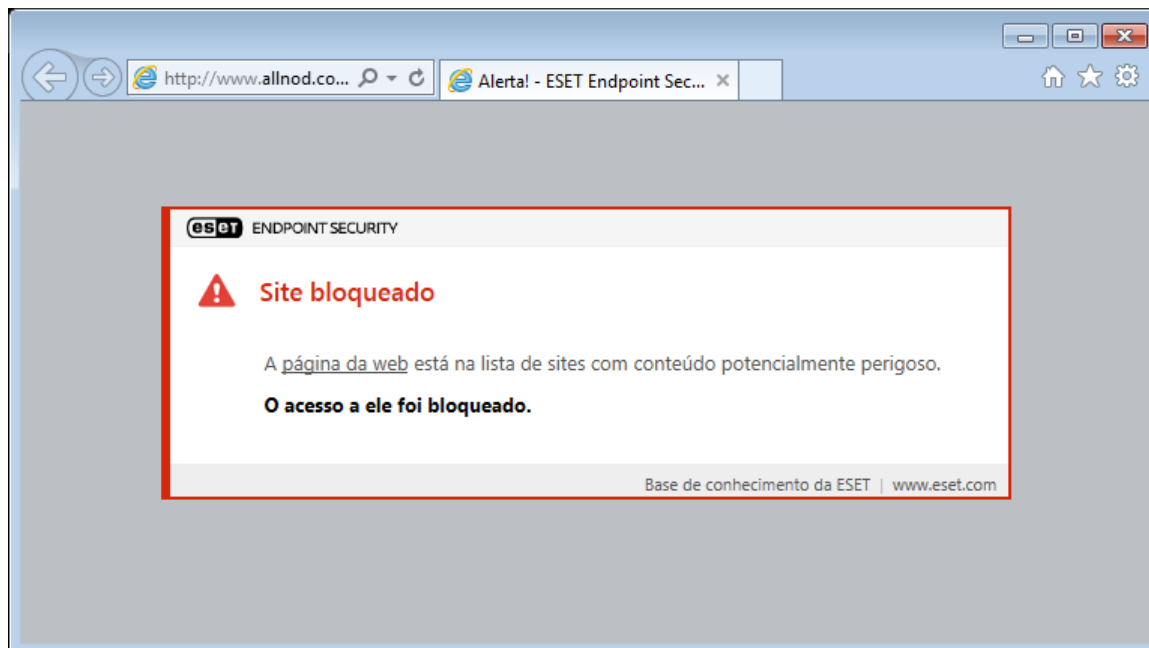
A conectividade com a Internet é um recurso padrão em um computador pessoal. Infelizmente, ela tornou-se o meio principal de transferência de códigos maliciosos. A proteção de acesso à Web funciona ao monitorar a comunicação entre os navegadores da web e servidores remotos e cumpre as regras do protocolo HTTP (Hypertext Transfer Protocol) e HTTPS (comunicação criptografada).

O acesso à páginas da Web conhecidas como tendo conteúdo malicioso é bloqueado antes que o conteúdo seja baixado. Todas as outras páginas da Web serão rastreadas pelo mecanismo de rastreamento ThreatSense quando forem carregadas e bloqueadas se conteúdo malicioso for detectado. A proteção do acesso à Web oferece dois níveis de proteção, bloqueio por lista de proibições e bloqueio por conteúdo.

Recomendamos enfaticamente que a proteção de acesso à Web seja ativada. Essa opção pode ser acessada a partir da janela principal do ESET Endpoint Security localizada em **Configuração > Proteção de internet > Proteção do acesso à Web**.



Quando o site for bloqueado, a proteção de acesso à web exibirá a mensagem a seguir no seu navegador:

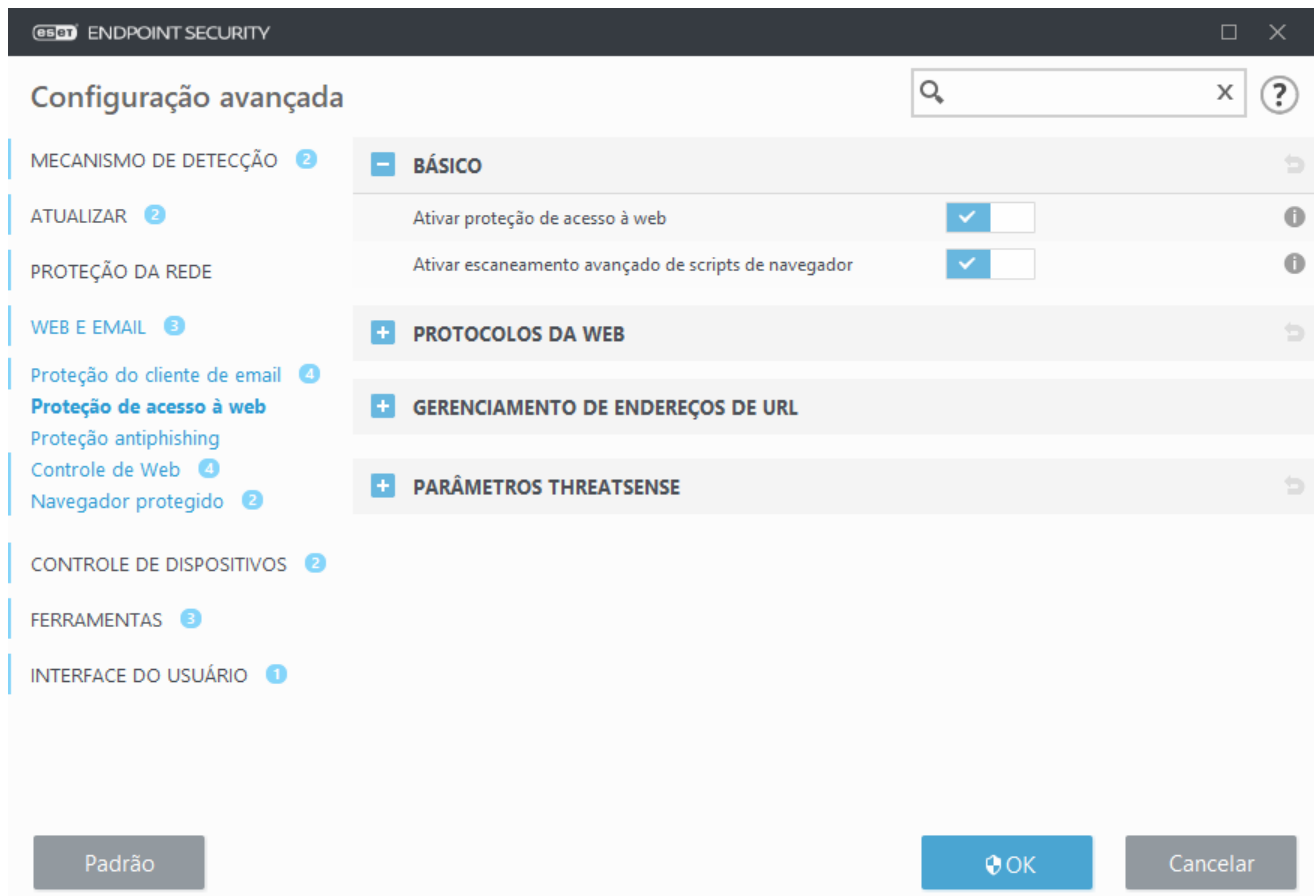


Os artigos da Base de conhecimento da ESET a seguir podem estar disponíveis apenas em inglês:

- [Desbloquear um site seguro em uma estação de trabalho individual no ESET Endpoint Security](#)

As seguintes opções estão disponíveis em **Configuração avançada (F5) > Web e email > Proteção de acesso Web**:

- **Básico** – Para ativar ou desativar esse recurso da Configuração avançada.
- **Protocolos da Web** – Permite que você configure o monitoramento para esses protocolos padrão, que são usados pela maioria dos navegadores de Internet.
- **Gerenciamento de endereços URL** – Permite especificar endereços URL a serem bloqueados, permitidos ou excluídos da verificação.
- **ThreatSense parâmetros** - Configuração avançada do rastreador de vírus - permite definir as configurações, como tipos de objetos para rastreamento (emails, arquivos, etc.), métodos de detecção para proteção do acesso à Web, etc.



Configuração avançada de proteção de acesso à web

As seguintes opções estão disponíveis em **Configuração avançada** (F5) > **Web e e-mail** > **Proteção de acesso à web** > **Básico**:

Ativar proteção do acesso à web – Quando desativada, a [Proteção de acesso à web](#) e [Proteção antiphishing](#) não serão executadas.

Ativar escaneamento avançado de scripts de navegador – Quando ativado, todos os programas JavaScript executados por navegadores da web serão verificados pelo mecanismo de detecção.

i Recomendamos enfaticamente que você mantenha a proteção de acesso à Web ativada.

Protocolos da Web

Por padrão, o ESET Endpoint Security é configurado para monitorar o protocolo HTTP usado pela maioria dos navegadores de Internet.

Configuração do scanner HTTP

O tráfego HTTP é sempre monitorado em todas as portas para todos os aplicativos.

Configuração do scanner HTTPS

O ESET Endpoint Security também oferece suporte à verificação do protocolo HTTPS. A comunicação HTTPS utiliza um canal criptografado para transferir as informações entre servidor e cliente. O ESET Endpoint Security verifica as comunicações utilizando os protocolos SSL (Camada de soquete seguro) e TLS (Segurança da camada de transporte). O programa rastreará somente tráfego em portas (443, 0-65535) definidas em **Portas usadas pelo protocolo HTTPS**, independentemente da versão do sistema operacional.

A comunicação criptografada será escaneada por padrão. Para visualizar a configuração do escaneador, vá para [SSL/TLS](#) na seção Configuração avançada, clique em **Web e email > SSL/TLS** e selecione a opção **Ativar filtragem de protocolo SSL/TLS**.

Gerenciamento de endereços de URL

O gerenciamento de endereços URL permite especificar endereços HTTP a serem bloqueados, permitidos ou excluídos do escaneamento de conteúdo.

A opção [Ativar filtragem de protocolo SSL/TLS](#) deve ser selecionada se você quiser filtrar endereços HTTPS além de páginas HTTP. Caso contrário, somente os domínios de sites HTTPS que você tenha visitado serão adicionados, não a URL completa.

Sites na **Lista de endereços bloqueados** não estarão acessíveis, exceto se também forem incluídos na **Lista de endereços permitidos**. Sites na **Lista de endereços excluídos do escaneamento de conteúdo** não serão escaneados quanto a código malicioso quando acessados.

Se você quiser bloquear todos os endereços HTTP, exceto endereços presentes na **Lista de endereços permitidos** ativa, adicione * à **Lista de endereços bloqueados** ativa.

Os símbolos especiais * (asterisco) e ? (ponto de interrogação) podem ser usados em listas. O asterisco substitui qualquer string de caracteres e o ponto de interrogação substitui qualquer símbolo. Tenha atenção especial ao especificar os endereços excluídos, uma vez que a lista deve conter os endereços seguros e confiáveis. De modo similar, é necessário assegurar que os símbolos * e ? sejam usados corretamente na lista. Consulte [Adicionar endereço HTTP/máscara de domínio](#) para saber como combinar com segurança um domínio completo, incluindo todos os subdomínios. Para ativar uma lista, selecione **Lista ativa**. Se você desejar ser notificado ao inserir um endereço da lista atual, selecione **Notificar ao aplicar**.



Os endereços não serão filtrados se a configuração **Web e e-mail > SSL/TLS > Excluir comunicação com domínios confiáveis** estiver ativada e o domínio for considerado como confiável.

Lista de endereços

?

Nome da lista

Tipos de endereços

Descrição da lista

Lista de endereços permitidos	Permitido	
Lista de endereços bloqueados	Bloqueado	
Lista de endereços excluídos do escaneamento de conteúdo	O malware encontrado ...	

Adicionar

Editar

Excluir

Importar

Exportar

Adicione um caractere curinga (*) à lista de endereços bloqueados para bloquear todos os URLs, exceto os incluídos em uma lista de endereços permitidos.

OK

Cancelar

Elementos de controle

Adicionar - Cria uma nova lista além das predefinidas. Isso pode ser útil se você quiser dividir logicamente diferentes grupos de endereços. Por exemplo, uma lista de endereços bloqueados pode conter endereços de uma lista pública externa de proibições e uma segunda pode conter sua própria lista de proibições, facilitando a atualização da lista externa enquanto mantém a sua intacta.

Editar - modifica listas existentes. Use isso para adicionar ou remover endereços.

Excluir - Exclui as listas existentes. Disponível somente para listas criadas com **Adicionar**, não para as padrão.

Lista de endereços URL

Nessa seção é possível especificar listas de endereços HTTP que serão bloqueados, permitidos ou excluídos da verificação.

Por padrão, as três listas a seguir estão disponíveis:

- **Lista de endereços excluídos do escaneamento de conteúdo** – Nenhuma verificação quanto a código malicioso será realizada para qualquer endereço adicionado a essa lista.
- **Lista de endereços permitidos** - Se Permitir acesso apenas a endereços HTTP na lista de endereços permitidos estiver ativada e a lista de endereços bloqueados tiver * (contém tudo), o usuário terá permissão para acessar apenas endereços especificados nessa lista. Os endereços nesta lista são permitidos mesmo se estiverem presentes na lista de endereços bloqueados.
- **Lista de endereços bloqueados** – O usuário não terá permissão para acessar endereços especificados nessa lista a menos que eles também estejam na lista de endereços permitidos.

Clique em **Adicionar** para criar uma nova lista. Para excluir as listas selecionadas, clique em **Remover**.

Lista de endereços

Nome da lista	Tipos de endereços	Descrição da lista
Lista de endereços permitidos	Permitido	
Lista de endereços bloqueados	Bloqueado	
Lista de endereços excluídos do escaneamento de conteúdo	O malware encontrado ...	

Adicionar Editar Excluir Importar Exportar

Adicione um caractere curinga (*) à lista de endereços bloqueados para bloquear todos os URLs, exceto os incluídos em uma lista de endereços permitidos.

OK Cancelar

i Os artigos da Base de conhecimento da ESET a seguir podem estar disponíveis apenas em inglês:

- [Desbloquear um site seguro em uma estação de trabalho individual no ESET Endpoint Security](#)

Para obter mais informações, consulte [Gerenciamento de endereços de URL](#).

Criar nova lista

Essa janela de diálogo permite configurar uma nova [lista de endereços URL/máscaras que serão bloqueados, permitidos ou excluídos](#) da verificação.

Você pode configurar as seguintes opções:

Tipo de lista de endereços - Três tipos de listas estão disponíveis:

- **O malware encontrado é ignorado** - Nenhuma verificação quanto a código malicioso será realizada para qualquer endereço adicionado a essa lista.
- **Bloqueado** – o acesso aos endereços especificados nesta lista será bloqueado.
- **Permitido** – o acesso aos endereços especificados nesta lista será permitido. Os endereços nesta lista são permitidos mesmo se estiverem na lista de endereços bloqueados.

Nome da lista - Especifique o nome da lista. Este campo estará indisponível ao editar uma das listas pré-definidas.

Descrição da lista - digite uma breve descrição para a lista (opcional). Indisponível ao editar uma da lista pré-definida.

Para ativar uma lista, selecione **Lista ativa** ao lado dessa lista. Se você quiser ser notificado quando uma lista específica for usada ao acessar sites, selecione **Notificar ao aplicar**. Por exemplo, você receberá uma notificação quando um site for bloqueado ou permitido por estar incluído na lista de endereços bloqueados ou permitidos. A notificação terá o nome da lista.

Gravidade do registro em relatório - Selecione a gravidade de registro em relatório no menu suspenso. Registros com detalhamento de Alerta podem ser coletados pelo ESET PROTECT.



As Informações e o Detalhamento do registro em relatório de alerta está disponível apenas para regras que contém pelo menos dois componentes sem caracteres curinga dentro do domínio. Por exemplo:

- *.domain.com/*
- *www.domain.com/*

Elementos de controle

Adicionar - Adiciona um novo endereço URL à lista (insira vários valores com separador).

Editar - Modifica endereço existente na lista. Disponível apenas para endereços criados com **Adicionar**.

Remover - Exclui endereços existentes na lista. Disponível apenas para endereços criados com **Adicionar**.

Importar - Importa um arquivo com endereços URL (separe os valores com uma quebra de linha, por exemplo, *.txt usando a codificação UTF-8).



Para informações, consulte o capítulo [Como adicionar uma máscara de URL](#).

Como adicionar uma máscara de URL

Consulte as instruções nesta caixa de diálogo antes de inserir o endereço/máscara de domínio desejado(a).

O ESET Endpoint Security possibilita que o usuário bloqueie o acesso a sites na Web especificados e evita que o navegador da Internet exiba o conteúdo deles. Além disso, ele permite que o usuário especifique os endereços que devem ser excluídos do rastreamento. Se o nome completo do servidor remoto for desconhecido ou o usuário desejar especificar um grupo total de servidores remotos, podem ser utilizadas para identificar tal grupo as denominadas "máscaras". As máscaras incluem os símbolos "?" e "*":

- utilize ? para substituir um símbolo
- utilize * para substituir uma string de texto.

Por exemplo *.c?m aplica-se a todos os endereços, em que a última parte começa com a letra c, termina com a letra m e contém um símbolo desconhecido entre elas (.com, .cam, etc.).

Por exemplo, a máscara *x? denota qualquer endereço com x como o último, mas um caractere. Para combinar com o domínio inteiro, digite-o na forma *.domain.com/*. Especificar o prefixo de protocolo *http://*, *https://* na máscara é opcional. Se isso for omitido, a máscara vai corresponder a qualquer protocolo. Uma sequência com um "*" na frente é tratada especialmente se for usada no começo de um nome de domínio. Primeiro, o caractere curinga * não corresponde ao caractere de barra ("/") neste caso. Isso é feito para evitar impedir a máscara, por exemplo a máscara *.domain.com não vai corresponder a *http://anydomain.com/anypath#.domain.com* (esse sufixo pode ser anexado a qualquer URL sem afetar o download). E, em segundo lugar, o "*" também corresponde a uma string vazia neste caso em especial. Isso acontece para permitir corresponder um domínio completo incluindo qualquer subdomínio usando uma única máscara. Por exemplo, a máscara *.domain.com também corresponde a *http://domain.com*. Usar *domain.com seria incorreto, já que isso também seria correspondente a *http://anotherdomain.com*.



As Informações e o Detalhamento do registro em relatório de alerta está disponível apenas para regras que contém pelo menos dois componentes sem caracteres curinga dentro do domínio. Por exemplo:

- *.domain.com/*
- *www.domain.com/*

Proteção antiphishing

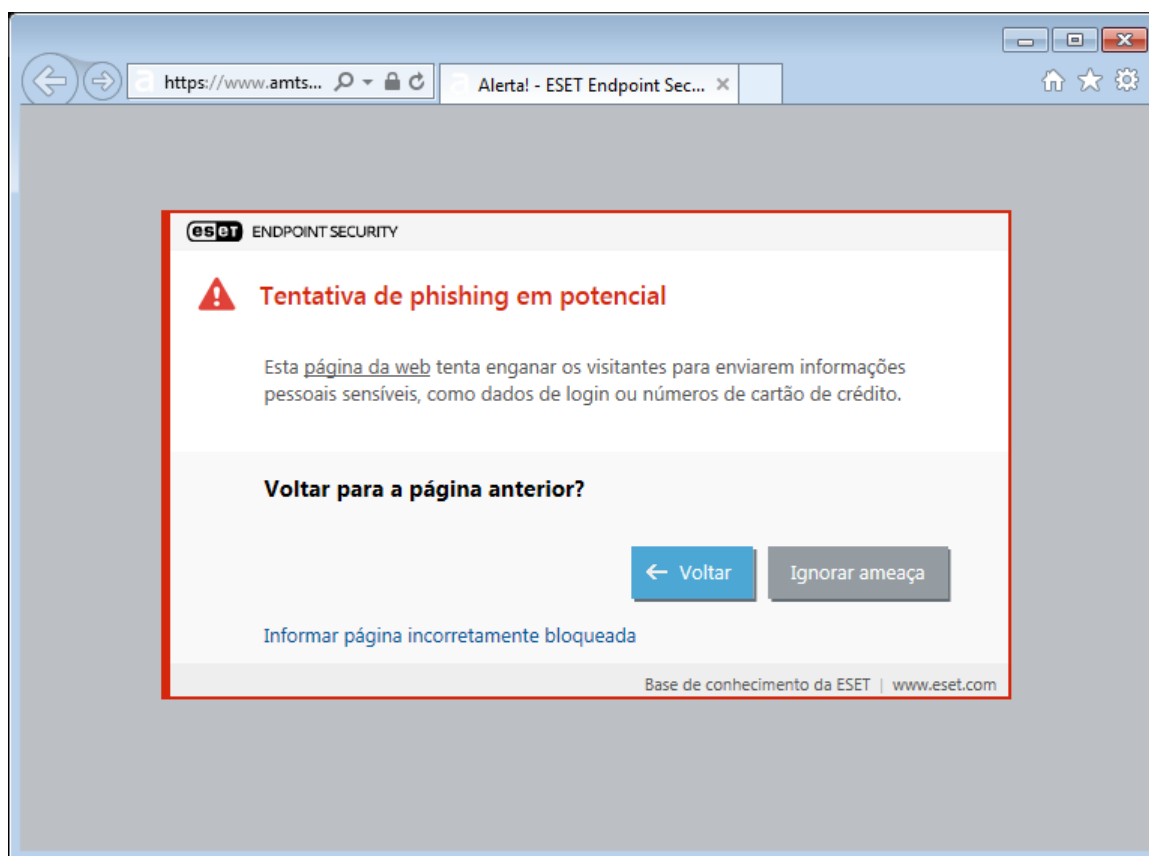
Phishing é uma atividade criminal que usa engenharia social (manipular os usuários para obter informações confidenciais). O phishing é usado para acessar dados confidenciais como números de contas bancárias, PINs, etc. Para mais informações, consulte o [glossário](#). O ESET Endpoint Security oferece proteção antiphishing; páginas da web conhecidas por distribuir esse tipo de conteúdo podem ser bloqueadas.

Por padrão, a proteção antiphishing está ativada. Esta configuração pode ser acessada na janela principal do programa > **Configuração avançada** (F5) > **Web e e-mail** > **Proteção antiphishing**.

Visite nosso [artigo da Base de conhecimento](#) para mais informações sobre a Proteção antiphishing no ESET Endpoint Security.

Acessando um site de roubo de identidade

Ao acessar um site reconhecido como sendo de phishing, seu navegador da web exibirá a caixa de diálogo a seguir. Se ainda quiser ter acesso ao site, clique em **Ignorar ameaça** (não recomendável).



Por padrão, sites de roubo de identidade em potencial que tiverem sido colocados na lista de permissões expirarão horas depois. Para permitir um site permanentemente, use a ferramenta de [gerenciamento de endereços de URL](#). A partir de **Configuração avançada** (F5) abra **Web e email** > **Proteção do acesso à Web** > **Gerenciamento de endereços URL** > **Lista de endereços**, clique em **Editar** e adicione o site que deseja editar na lista.

Denúncia de site de roubo de identidade

O link [Denunciar](#) permite que você denuncie um site de phishing/malicioso para análise da ESET.



antes de enviar um site para a ESET, certifique-se de que ele atenda a um ou mais dos seguintes critérios:

- o site não foi detectado,
- o site foi detectado incorretamente como uma ameaça. Nesse caso, é possível [relatar um site de phishing falso positivo](#).

Como alternativa, você pode enviar o site por email. Envie seu email para samples@eset.com. Lembre-se de incluir uma linha de assunto clara e o máximo de informações possível sobre o site (por exemplo, o site do qual você foi enviado, como ouviu falar sobre ele, etc.).

Configuração avançada do Navegador protegido

Essa configuração está disponível em **Configuração avançada (F5) > Web e email > Navegador protegido**.

– Básico

Ativar o Navegador protegido – quando estiver ativado, a lista de sites protegidos ficará ativa, permitindo abrir a janela de [Sites protegidos](#).

Redirecionamento de websites

Ativa o redirecionamento de sites protegidos - Se estiver ativado, sites de listas de sites protegidos e a lista interna de sites de banco serão redirecionados para o navegador protegido.

Sites protegidos - Uma lista de sites para os quais é possível selecionar qual navegador (normal ou protegido) será usado. Um logo ESET será exibido no seu navegador para mostrar que a navegação segura está ativada.

Proteção de páginas on-line seguras de atividades bancárias e pagamento – desativada por padrão. Além da lista nos [Sites protegidos](#), os sites na lista interna da ESET serão redirecionados para o navegador protegido da ESET. Os sites identificados pela ESET são atualizados regularmente.

Navegador protegido

Proteção de memória aprimorada - Se estiver ativado, a memória do navegador protegido será protegida da inspeção por outros processos.

Proteção do teclado – Se estiver ativado, as informações inseridas pelo teclado no navegador seguro ficarão ocultas de outros aplicativos. Isso aumenta a proteção contra [keyloggers](#).

Estrutura verde do navegador – Se estiver desativado, a estrutura verde ao redor da janela do seu navegador e a notificação no navegador relacionada serão exibidos brevemente durante a inicialização do navegador e desaparecerão. A estrutura verde indica que seu navegador está totalmente protegido.

Configurar alertas interativos do Navegador protegido – permite abrir a janela de [Alertas interativos](#).



Em algumas situações, um alerta interativo específico é usado apenas quando há um erro ao iniciar o Navegador protegido adequadamente. Para obter mais informações, consulte o capítulo [Alertas interativos](#).

Sites protegidos

O ESET Endpoint Security contém uma lista embutida de sites pré-definidos que vão acionar a abertura de um navegador protegido. É possível adicionar um site ou editar a lista de sites na configuração do produto.

A lista **Sites protegidos** pode ser vista e editada em **Configuração avançada (F5) > Web e email > Navegador protegido > Básico > Sites protegidos > Editar**.

A janela é composta por:

Colunas

Site – Site protegido.

Navegador protegido - O logo da ESET será exibido ao redor do canto do seu navegador durante a navegação protegida.

Navegador normal – selecione esta opção para continuar no seu navegador da web padrão (por exemplo, uma transação bancária).

Elementos de controle

Adicionar - Permite adicionar um site da lista de sites conhecidos.

Editar - Permite que você edite as entradas selecionadas.



Remove – Remove as entradas selecionadas.

Notificação no navegador

O navegador protegido informa sobre seu status atual por meio de notificações no navegador e da cor da estrutura do navegador.

Notificações no navegador são exibidas na guia no lado direito.



Para expandir a notificação no navegador, clique no ícone ESET . Para minimizar a notificação, clique no texto da notificação. Para dispensar a notificação, clique no ícone fechar .

Notificações no navegador

Tipo de notificação	Status
Notificação informativa e estrutura verde do navegador	A proteção máxima está assegurada e a notificação no navegador é minimizada por padrão.
Aviso e estrutura laranja do navegador	O navegador protegido requer sua atenção para um problema não crítico. Para obter mais informações sobre o problema ou uma solução, siga as instruções na notificação no navegador.

Tipo de notificação	Status
Alerta de segurança e estrutura vermelha do navegador	O navegador não está protegido pela proteção para bancos & pagamentos ESET. Reinicie o navegador para garantir que a proteção está ativa. Para resolver um conflito com os arquivos carregados no navegador, entre em contato com o Suporte Técnico ESET seguindo as instruções em nosso artigo da Base de conhecimento .

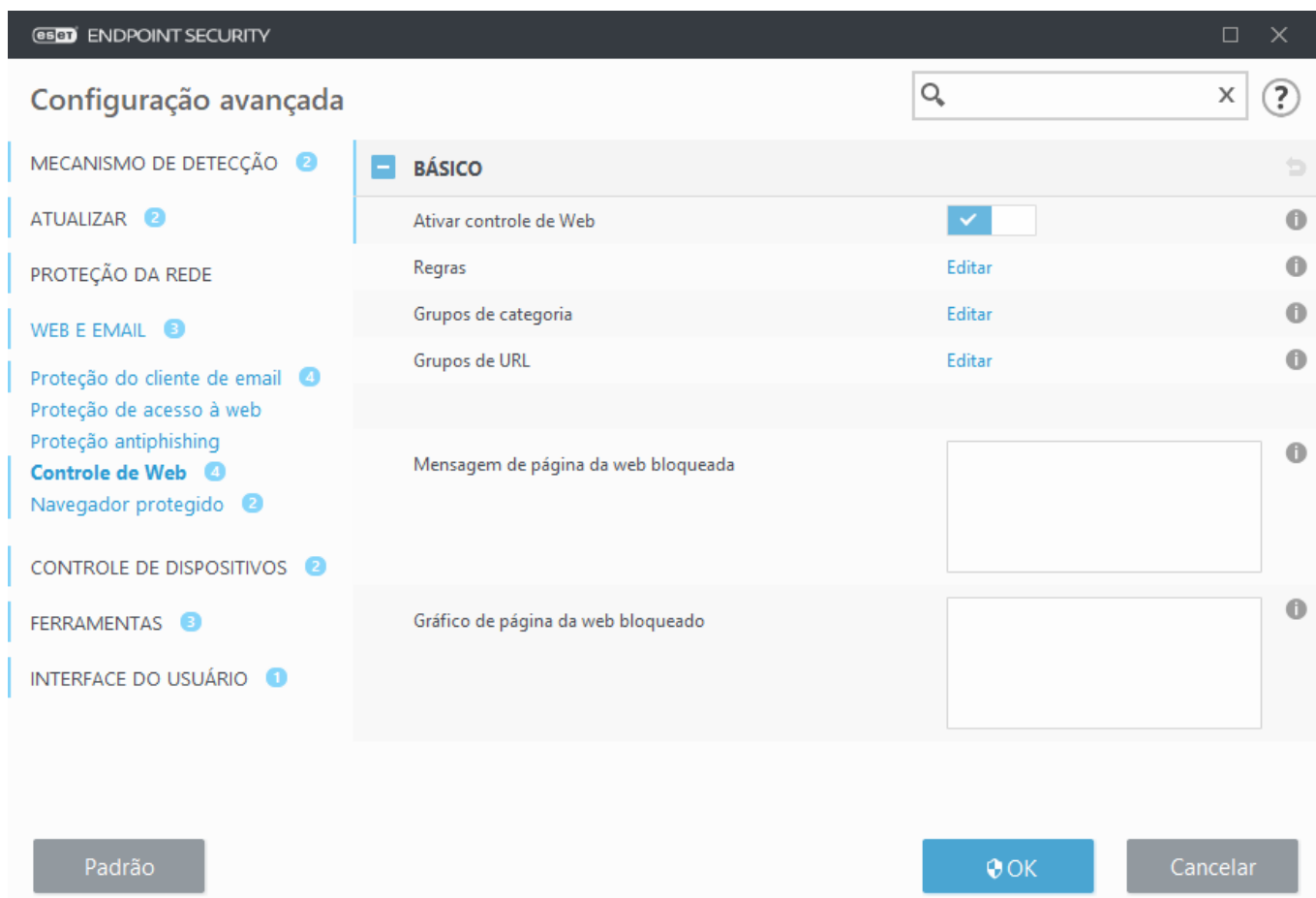
Controle de Web

A seção Controle de Web permite que você defina as configurações que protegem sua empresa do risco de responsabilidade legal. O Controle de Web pode regulamentar o acesso a sites que violem direitos de propriedade intelectual. O objetivo é impedir que os funcionários acessem páginas com conteúdo inadequado ou prejudicial, ou páginas que possam ter impacto negativo sobre a produtividade.

O Controle de Web permite bloquear sites que possam conter material potencialmente ofensivo. Além disso, os empregadores ou administrador do sistema podem proibir o acesso para mais de 27 categorias de site predefinidas e mais de 140 subcategorias.

Por padrão, o controle de web está desativado. Para ativar o controle de web:

1. Pressione **F5** para entrar na **Configuração avançada** e abra **Web e e-mail > Controle de web**.
2. Selecione **Ativar controle de web** para ativar o controle de web no ESET Endpoint Security.
3. Para configurar o acesso a páginas da web específicas, clique em **Editar** ao lado de **Regras** para acessar a janela do [Editor de regras de controle de web](#).



Os campos **Mensagem de página da web bloqueada** e **Gráfico de página da web bloqueada** permitem que você

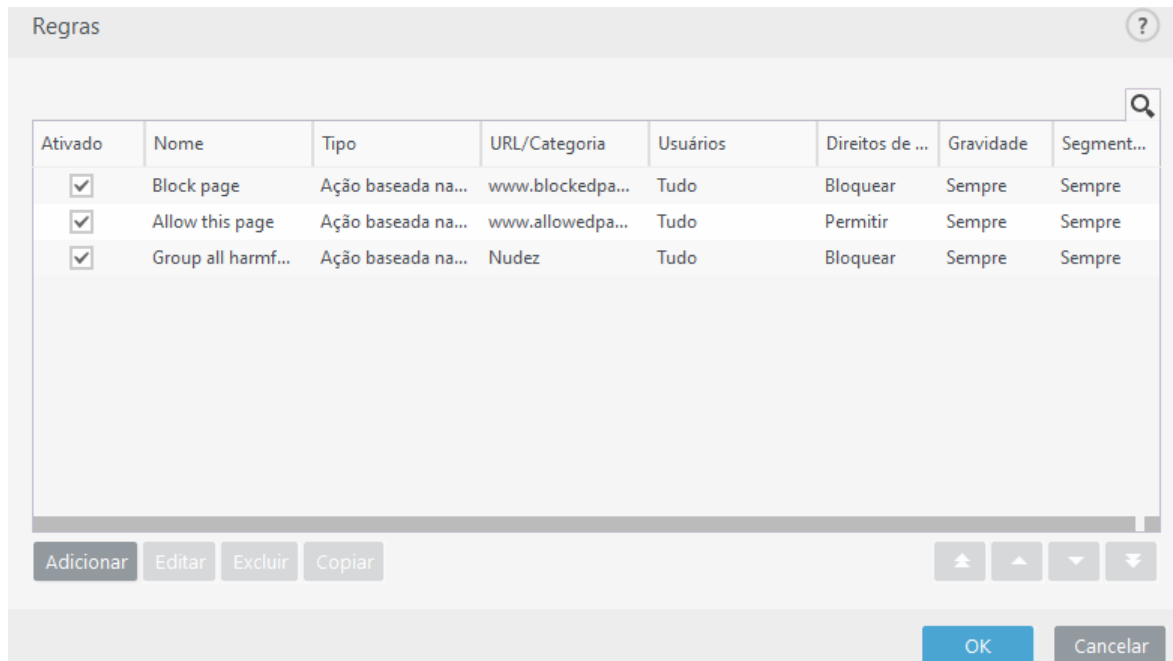
[personalize a mensagem exibida](#) quando um site for bloqueado.



Caso você queira bloquear todas as páginas da web e deixar apenas algumas disponíveis, use o [Gerenciamento de endereços de URL](#).

Regras de controle de web

A janela do editor de **Regras** exibe regras existentes com base em URL ou com base em categoria.



A lista de regras contém diversas descrições de uma regra, tais como nome, tipo de bloqueio, ação a ser realizada após a correspondência de uma regra de controle da Web e a gravidade do relatório.

Clique em **Adicionar** ou **Editar** para gerenciar uma regra. Clique em **Copiar** para criar uma nova regra com opções predefinidas usadas para outra regra selecionada. Ao pressionar **Ctrl** e clicar, você pode selecionar várias regras e remover todas as regras selecionadas. A caixa de seleção **Ativado** desativará ou ativará uma regra; isso pode ser útil caso não deseje excluir uma regra permanentemente se você pretende usá-la no futuro.

As regras são classificadas na ordem que determina sua prioridade, com as regras de prioridade mais alta no topo. Para alterar a prioridade de uma regra, selecione a regra e clique no botão de seta para aumentar ou diminuir a prioridade da regra. Clique na seta dupla para mover a regra para o topo ou para o fundo da lista.

Leia mais informações [sobre a criação de regras](#).

Adicionar regras de controle da Web

A janela Regras de controle da Web permite criar ou modificar manualmente uma regra de filtro do controle da Web existente.

Nome

Insira uma descrição da regra no campo **Nome** para uma melhor identificação.

Ativado

Clique na opção **Ativado** para ativar ou desativar esta regra. Isso pode ser útil caso não deseje remover a regra permanentemente.

Ação

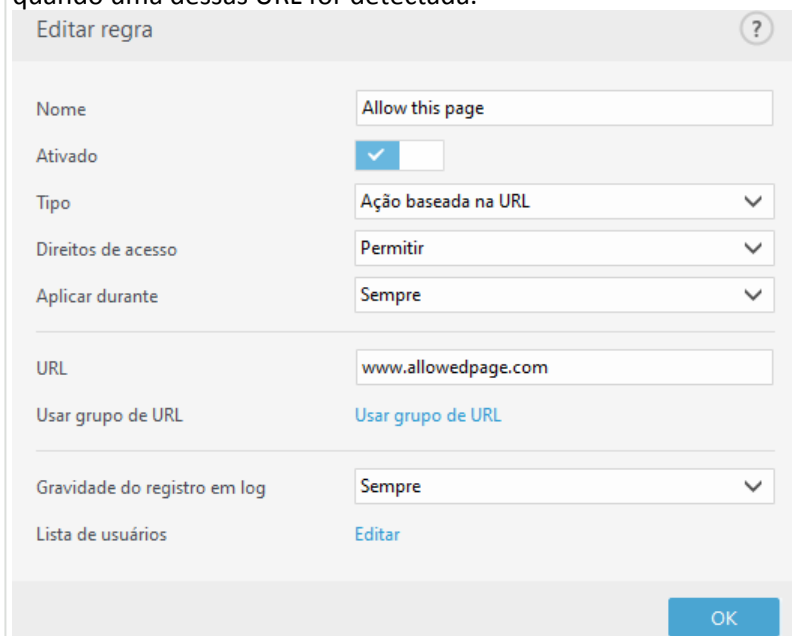
Escolha entre **Ação baseada no URL** ou **Ação baseada na categoria**:

[Ação baseada na URL](#)

Para regras que controlam acesso a um determinado site, insira o URL no campo **URL**.

Não é possível usar os símbolos especiais * (asterisco) e ? (ponto de interrogação) na lista de endereços de URL. Ao criar um grupo de URL que tenha um site com vários domínios de nível superior (TLDs), cada TLS deve ser adicionado separadamente. Se adicionar um domínio ao grupo, todo o conteúdo localizado neste domínio e em todos os subdomínios (por exemplo, *sub.paginaexemplo.com*) será bloqueado ou permitido de acordo com sua escolha de ação baseada na URL.

URL ou Usar grupo de URL - Use o link ou [grupo de links de URL](#) para permitir, bloquear ou alertar o usuário quando uma dessas URL for detectada.



[Ação baseada na categoria](#)

Quando isto estiver selecionado, defina a categoria para sua ação usando o menu suspenso.

Categoria do URL ou Usar grupo – Use a categoria do site ou categorias dos [Grupos de categoria](#) para permitir, bloquear ou alertar o usuário quando um desses grupos for detectado.

Direitos de acesso

- **Permitir** - O acesso ao endereço URL/categoria será concedido.
- **Alertar** - Alerta o usuário sobre o endereço URL/categoria.
- **Sempre alertar** – avisa o usuário sobre o endereço URL/categoria. Você pode continuar para o site, mas o administrador será notificado.
- **Bloquear** - Bloqueia o endereço URL/categoria.

Aplicar durante

Permite a você aplicar uma regra criada durante um certo tempo. Do menu suspenso, selecione o segmento de tempo criado.

- [Mais informações sobre Segmentos de tempo](#)

Gravidade do registro em relatório

- **Sempre** – Registra todas as comunicações on-line.
- **Diagnóstico** - Registra informações necessárias para ajustar o programa.
- **Informações**– Registra as mensagens informativas, incluindo as mensagens de atualizações bem-sucedidas e todos os registros mencionados anteriormente.
- **Aviso** – Registra mensagens de erros críticos e de aviso.
- **Nenhum** - Nenhum relatório será criado.



A gravidade do Registro em relatório pode ser configurada separadamente para cada lista. Registros com status de **Alerta** podem ser coletados pelo ESET PROTECT.

Lista de usuários

- **Adicionar** - Abre a janela de diálogo **Selecionar usuários ou grupos**, que permite que você selecione usuários desejados. Quando nenhum usuário for inserido, a regra será aplicada para todos os usuários.
- **Remover** – Remove o usuário selecionado do filtro.

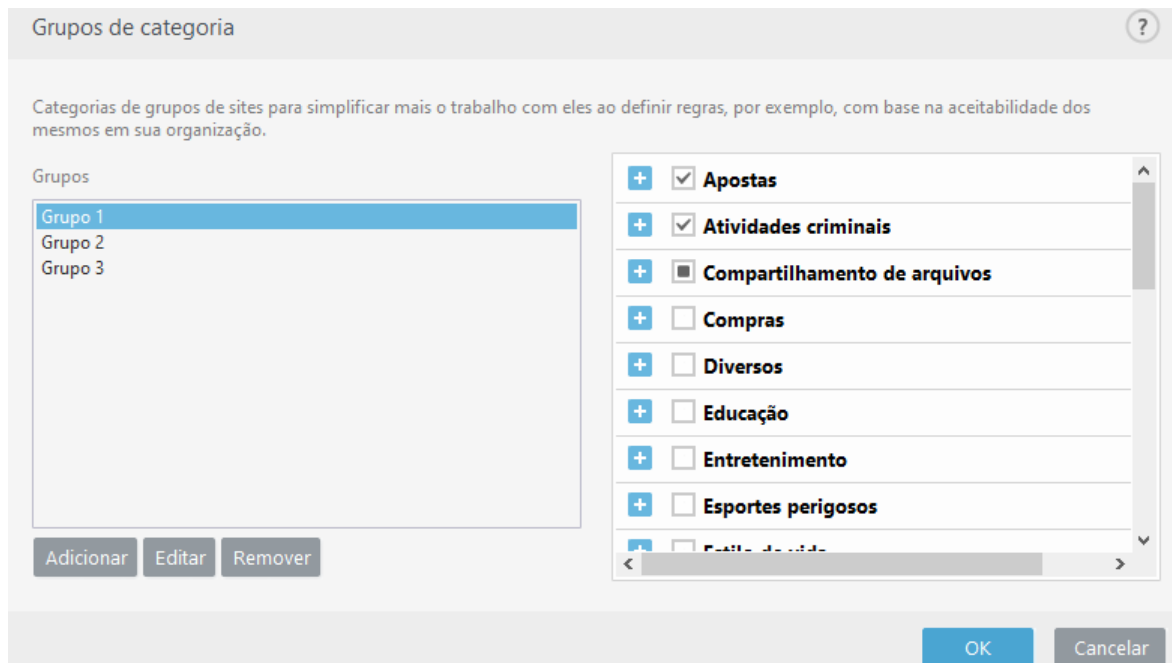
Grupos de categoria

A janela de grupos de Categoria é dividida em duas partes. A parte da esquerda da janela contém uma lista de grupos de Categoria.

- **Adicionar** – clique para criar um novo grupo de Categoria.
- **Editar** – clique para editar um grupo de Categoria existente.
- **Remover** – selecione e clique se quiser remover um grupo de Categoria existente da lista de grupos de categoria.

A parte da direita da janela contém uma lista de categorias e subcategorias. Selecione uma categoria na lista de Categorias para exibir as subcategorias. Cada grupo contém subcategorias geralmente inadequadas e/ou para adultos, bem como categorias consideradas geralmente aceitáveis. Quando você abrir a janela Grupos de categoria e clicar no primeiro grupo, poderá adicionar ou remover categorias/subcategorias da lista de grupos apropriados (por exemplo, violência ou armas). Páginas da web com conteúdo inadequado podem ser bloqueadas ou usuários podem ser informados depois que uma regra com ações predefinidas for criada.

Marque a caixa de seleção para adicionar ou remover uma subcategoria para um grupo específico.



Aqui estão alguns exemplos de categorias com as quais os usuários podem não estar familiarizados:

Diversos - Geralmente, endereços IP privados (locais), como intranet, 192.168.0.0/16, etc. Quando você recebe um código de erro 403 ou 404, o site também corresponderá a essa categoria.

Não solucionado - Esta categoria inclui páginas da web não solucionadas devido a um erro ao se conectar ao mecanismo do banco de dados do Controle da Web.

Não categorizado - Páginas web desconhecidas que ainda não estão no banco de dados do Controle da web.

Proxies - Páginas da Web, como anonimizadores, redirecionadores ou servidores proxy públicos, podem ser usadas para obter acesso (anônimo) a páginas da web que geralmente são proibidas pelo filtro do Controle da Web.

Compartilhamento de arquivos - Estas páginas da web contêm grandes quantidades de dados, como fotos, vídeos ou livros eletrônicos. Há um risco de que esses sites possam conter materiais potencialmente ofensivos ou de conteúdo adulto.

i Uma subcategoria pode pertencer a qualquer grupo. Existem algumas subcategorias que não estão incluídas nos grupos predefinidos (por exemplo, Jogos). Para corresponderem a uma subcategoria desejada usando o filtro de Controle de web, adicione-a a um grupo desejado.

Grupos de URL

O grupo de URL permite que você crie um grupo com vários links URL para os quais você deseja criar uma regra (permitir/bloquear certos sites).

Criar um novo grupo de URL

Para criar um novo grupo de URL clique em **Adicionar** e insira o nome do novo grupo de URL.

Usar um grupo de URL pode ser útil quando o administrador quer criar uma regra para mais páginas da web (bloqueadas ou permitidas, com base na sua escolha).

Adicionar endereços URL à lista do grupo de URL – manualmente

Para adicionar um novo endereço URL à lista, selecione um grupo de URL e clique em **Adicionar** no canto inferior direito da janela.

Não é possível usar os símbolos especiais * (asterisco) e ? (ponto de interrogação) na lista de endereços de URL.

Não é necessário inserir o nome completo do domínio com http:// ou https://.

Se você adicionar um domínio ao grupo, todo o conteúdo localizado nesse domínio e em todos os subdomínios (por exemplo, *sub.examplepage.com*) será bloqueado ou permitido com base na sua escolha de ação baseada no URL.

Se houver um conflito entre duas regras, no sentido de a primeira regra bloquear o domínio e a segunda regra permitir o mesmo domínio, o domínio ou endereço IP específico será bloqueado. Para mais informações sobre a criação de regras, [veja Ação baseada no URL](#).

Adicionar endereços URL à lista de grupo de URL – importar usando um arquivo .txt

Clique em **Importar** para importar um arquivo com uma lista de endereços URL (separe os valores com uma quebra de linha, por exemplo, um arquivo .txt usando codificação UTF-8). Não é possível usar os símbolos especiais * (asterisco) e ? (ponto de interrogação) na lista de endereços de URL.

Usar grupos de URL no controle de web

Se quiser configurar uma ação para ser realizada para um grupo de URL específico, abra o [Editor de regras do controle de web](#), selecione seu grupo de URL usando o menu suspenso, ajuste outros parâmetros e clique em **OK**.

i Bloquear ou permitir uma página da Web específica pode ser mais seguro do que bloquear ou permitir uma categoria inteira de páginas da Web. Tenha cuidado ao alterar essas configurações e adicionar uma página da Web ou categoria à lista.

Personalização de mensagem da página da web bloqueada

Os campos **Mensagem de página da web bloqueada** e **Gráfico de página da web bloqueada** permitem que você personalize a mensagem exibida quando um site for bloqueado.

Esta é a mensagem e o design padrão da notificação dentro do navegador quando o usuário tenta acessar um site bloqueado:

Uso

Vamos bloquear a categoria de site "Armas".

Um exemplo de mensagem de página da web bloqueada seria:

A página da web %URL_OR_CATEGORY% foi bloqueada pois é considerada inadequada ou com conteúdo prejudicial.
Entre em contato com seu administrador para detalhes.

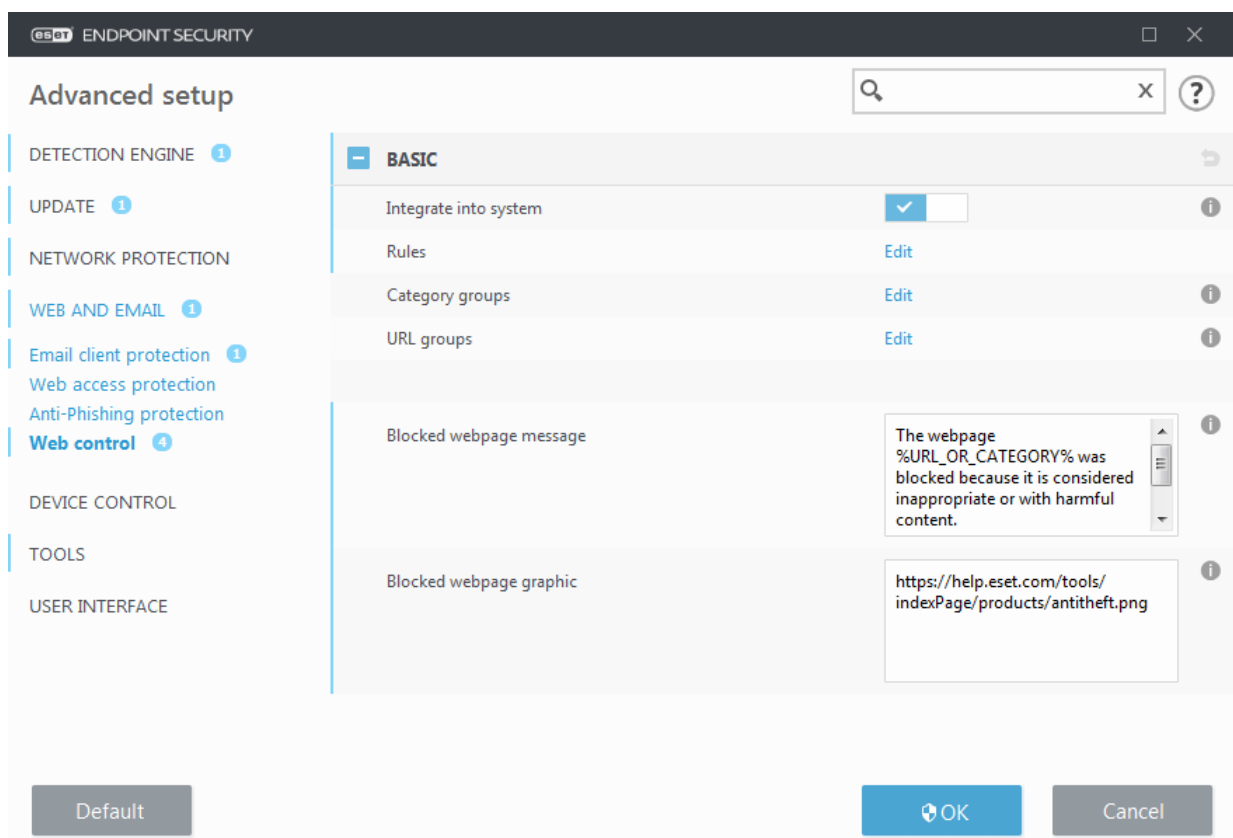
Variável	Descrição
%CATEGORY%	Categoria de controle de web bloqueada.
%URL_OR_CATEGORY%	Categoria ou site de controle de web bloqueado (depende da regra de bloqueio de controle de web).
%STR_GOBACK%	Valor do botão "Voltar".
%product_name%	Nome do produto ESET (ESET Endpoint Security)
%product_version%	Versão do produto ESET.

Um exemplo de gráfico para uma página da web bloqueada é o seguinte:

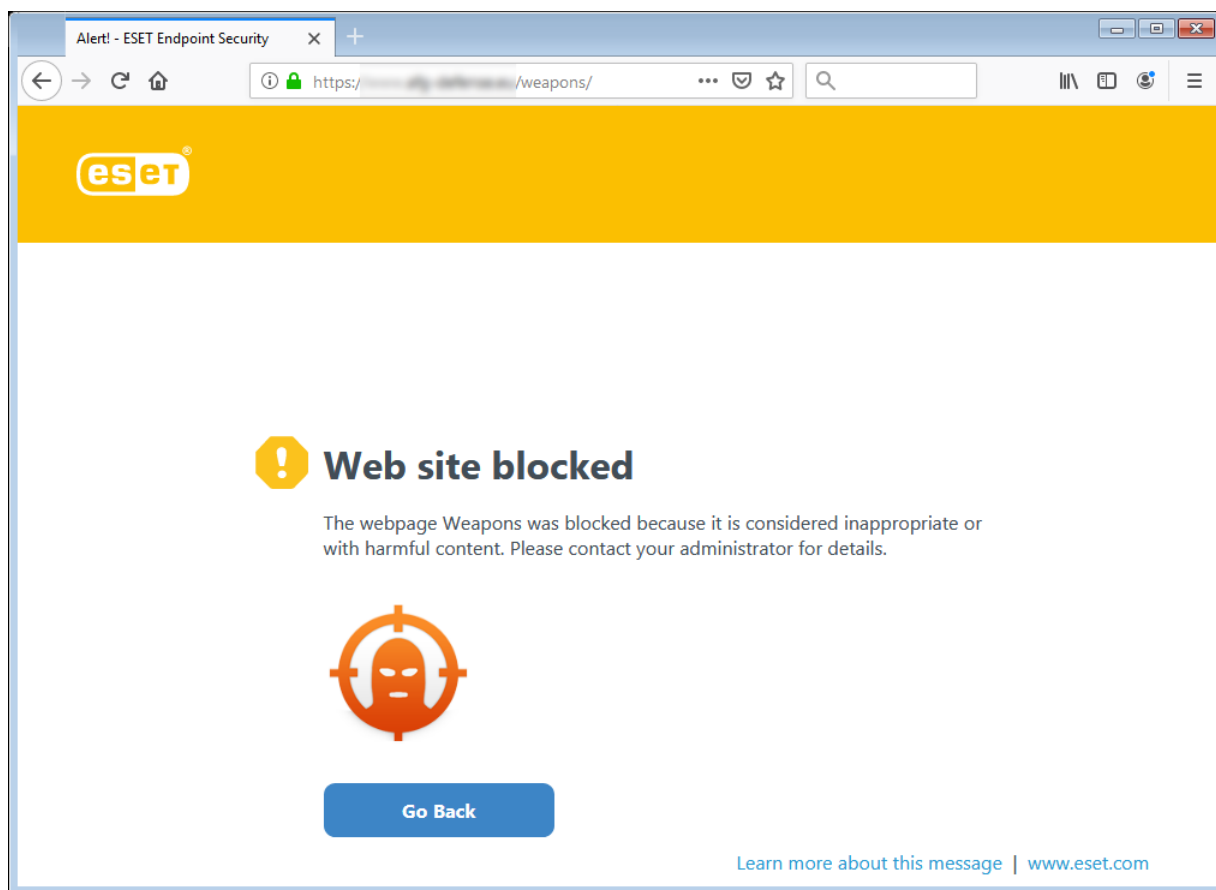
<https://help.eset.com/tools/indexPage/products/antitheft.png>

O tamanho da imagem (largura/altura) será colocado em escala automaticamente se o tamanho for muito grande.

A configuração no ESET Endpoint Security será a seguinte:



A notificação personalizada no navegador quando um usuário tenta acessar um site bloqueado será a seguinte:



Atualização do programa

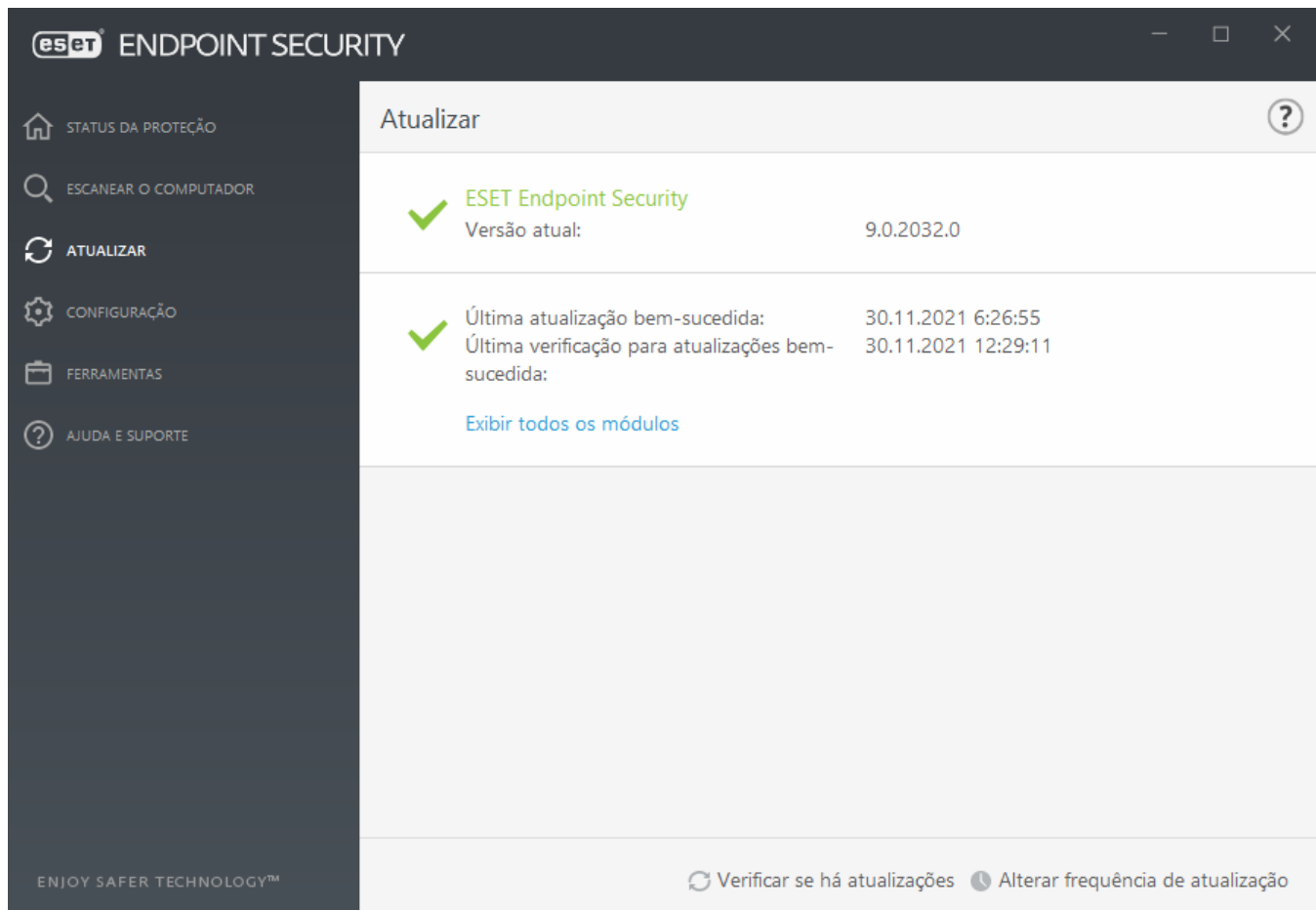
Atualizar o ESET Endpoint Security periodicamente é o melhor método para se obter o nível máximo de segurança em seu computador. O Módulo de atualização garante que o programa está sempre atualizado de duas maneiras, atualizando o mecanismo de detecção e atualizando os componentes do sistema. As atualizações são automáticas por padrão quando o programa está ativado.

Na janela principal do programa, ao clicar em **Atualizar**, você poderá localizar o status da atualização atual, incluindo o dia e a hora da última atualização bem-sucedida e se uma atualização será necessária. Também é possível clicar no link **Exibir todos os módulos** para abrir a lista de módulos instalados e verifique a versão e a última atualização de um módulo.

Além disso, a opção para iniciar manualmente o processo de atualização, **Verificar as atualizações**, está disponível. A atualização do mecanismo de detecção e a atualização dos componentes do programa são partes importantes da manutenção da proteção completa contra códigos maliciosos. Dê atenção especial à sua configuração e operação. Se você não inseriu os detalhes da licença durante a instalação, você poderá inserir sua chave de licença clicando em **Ativar produto** ao atualizar para acessar os servidores de atualização da ESET.

Se você ativar o ESET Endpoint Security com o Arquivo de licença off-line sem um Nome de usuário e Senha e tentar atualizar, a informação em vermelho **Falha na atualização do módulo** sinaliza que você só poderá fazer download de atualizações da imagem.

i Sua chave de licença é fornecida pela ESET após a compra do ESET Endpoint Security.



Versão atual– O número de compilação do ESET Endpoint Security.

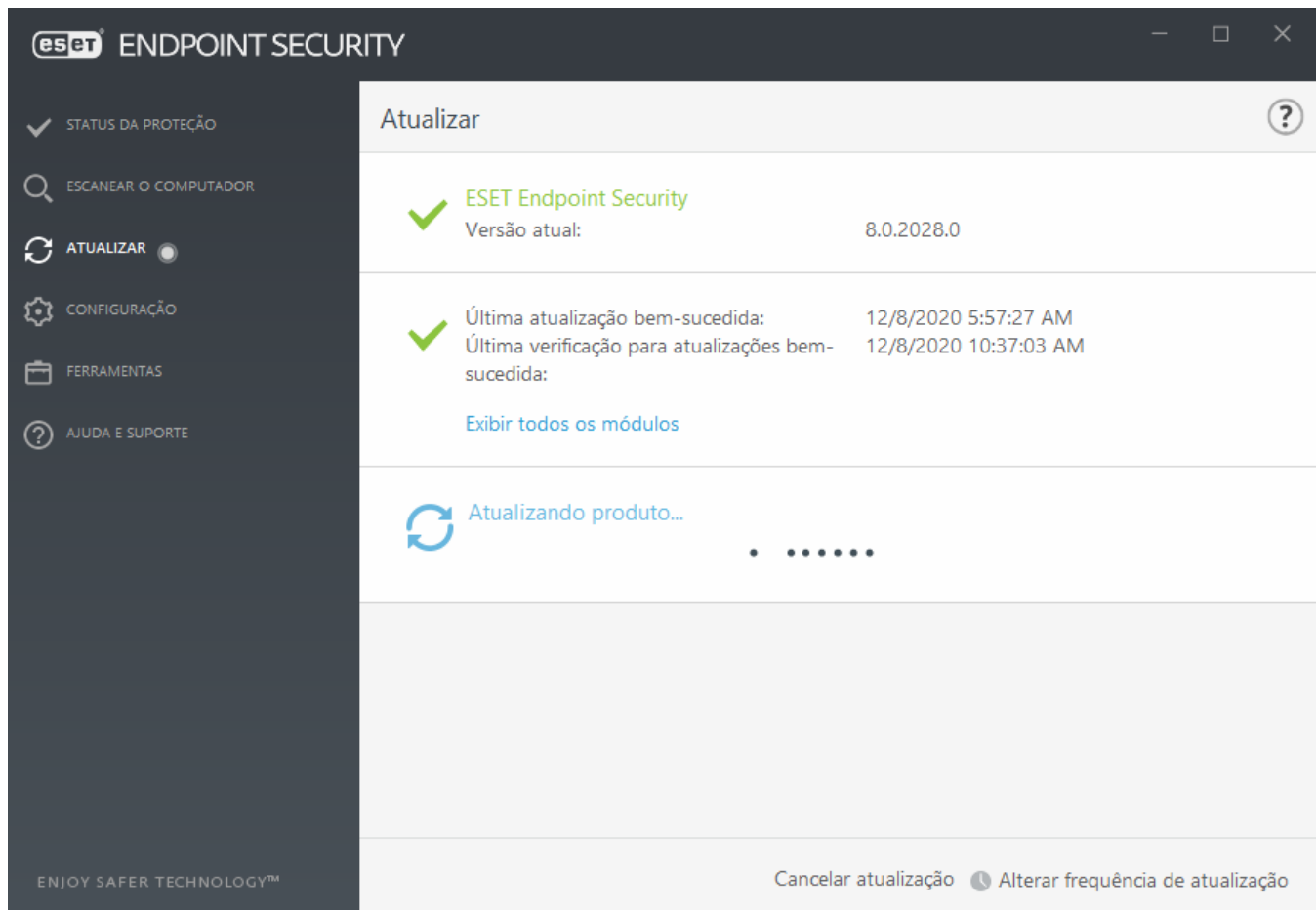
Última atualização bem-sucedida – A data e hora da última atualização bem-sucedida. Verifique se ela se refere a uma data recente, o que significa que o mecanismo de detecção está atualizado.

Última verificação por atualizações bem-sucedida – A data e hora da última tentativa bem-sucedida de atualizar módulos.

Exibir todos os módulos – Clique no link para abrir a lista de módulos instalados e verifique a versão e a última atualização de um módulo.

Processo de atualização

Depois de clicar em **Verificar se há atualizações**, o processo de download começará. A barra de progresso do download e o tempo restante do download serão exibidos. Para interromper a atualização, clique em **Cancelar atualização**.

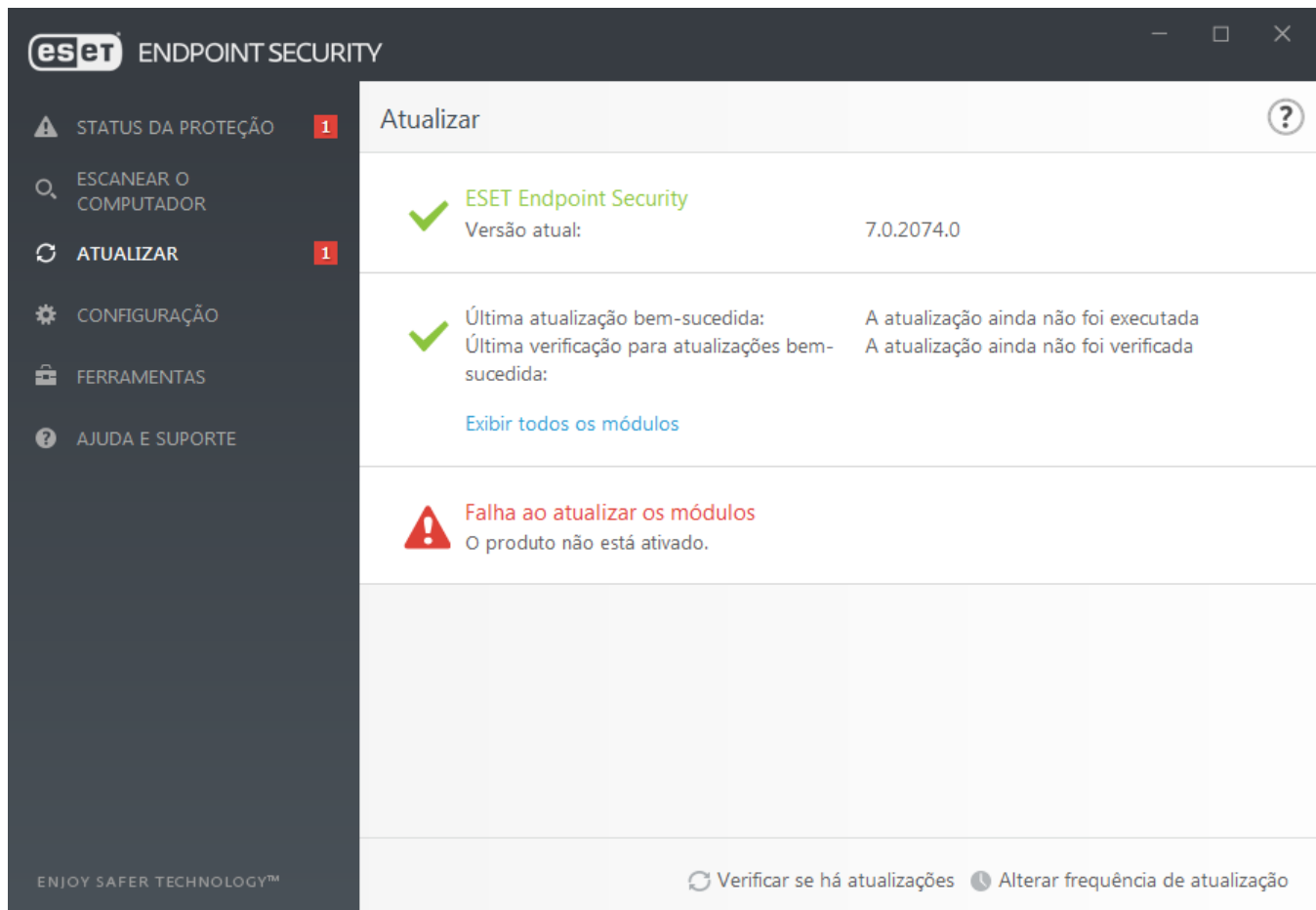


Sob circunstâncias normais os módulos são atualizados várias vezes por dia. Se esse não for o caso, o programa estará desatualizado e mais vulnerável a uma infecção. Atualize os módulos assim que for possível.

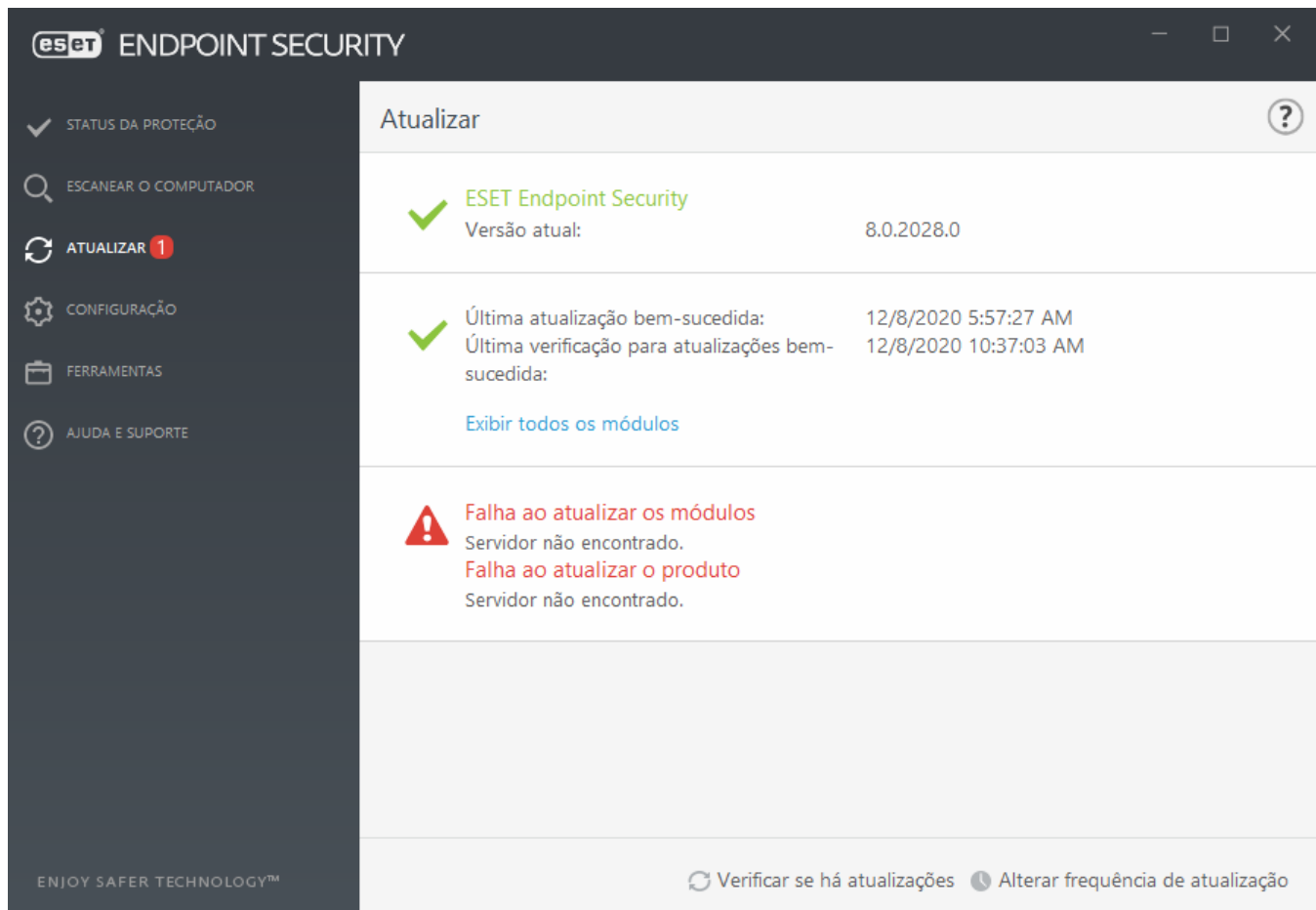
Mecanismo de detecção desatualizado – Esse erro aparecerá depois de diversas tentativas malsucedidas de atualizar os módulos. Recomendamos que você verifique as configurações de atualização. A razão mais comum para esse erro é a inserção de dados de autenticação incorretos ou definições incorretas das [configurações de conexão](#).


A notificação anterior está relacionada às duas mensagens **Falha na atualização dos módulos** a seguir sobre atualizações malsucedidas:

1. **Licença inválida** - A chave de licença foi inserida incorretamente na configuração da atualização. Recomendamos que você verifique os seus dados de autenticação. A janela Configuração avançada (no menu principal, clique em **Configuração** e depois em **Configuração avançada** ou pressione F5 no teclado) contém opções de atualização adicionais. Clique em **Ajuda e suporte** > **Alterar licença** a partir do menu principal para inserir uma nova chave de licença.



2. **Ocorreu um erro durante o download dos arquivos de atualização** - Uma possível causa do erro pode dever-se a [configurações de conexão à Internet](#) incorretas. Recomendamos que você verifique a conectividade da Internet (abrindo qualquer site em seu navegador da Web). Se o site não abrir, é provável que uma conexão com a Internet não tenha sido estabelecida ou que haja problemas de conectividade com o seu computador. Verifique com o seu provedor de serviços de Internet (ISP) se você não tiver uma conexão ativa com a Internet.



 Para obter mais informações, acesse este artigo da [Base de conhecimento ESET](#).

Configuração da atualização

Opções de configuração da atualização estão disponíveis na árvore de **Configuração avançada** (F5) sob **Atualização**. Esta seção especifica as informações da origem da atualização, como, por exemplo, os servidores de atualização e os dados de autenticação sendo usados para esses servidores.



Para que o download das atualizações seja feito de forma adequada, é fundamental preencher corretamente todos os parâmetros de atualização. Se você usar um firewall, certifique-se de que o programa da ESET tem permissão para comunicar com a Internet (por exemplo, comunicação HTTPS).

Básico

O perfil de atualização usado atualmente é exibido no menu suspenso **Selecionar perfil de atualização padrão**.

Para criar um novo perfil, consulte a seção [Perfis](#).

Alternância de perfil automática – Atribui um perfil de atualização de acordo com as Redes conhecidas no Firewall. A alternância de perfil automática permite alterar o perfil para uma rede específica dependendo da configuração na Agenda. Verifique as páginas de ajuda para mais informações

Configurar notificações de atualização – Clique em Editar para selecionar quais [notificações de aplicativo](#) são exibidas. Você pode escolher entre as opções Exibir na área de trabalho e/ou Enviar por email para as notificações.

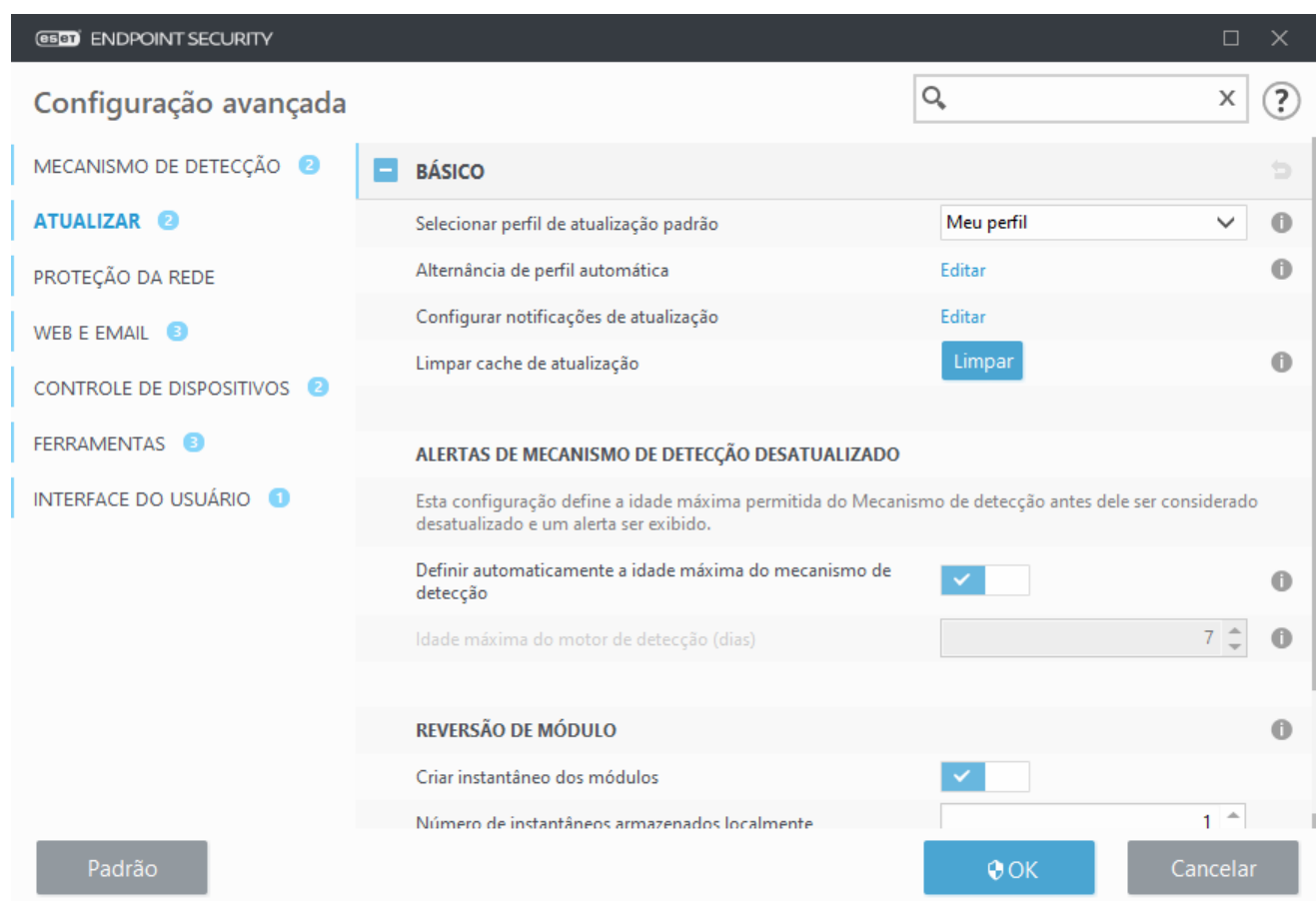
Se você está tendo dificuldade ao tentar fazer download das atualizações dos módulos, clique em **Limpar** ao lado de **Limpar cache de atualização** para limpar os arquivos/cache de atualização temporários.

Alertas de mecanismo de detecção desatualizado

Definir a idade máxima do mecanismo de detecção automaticamente – Permite definir o tempo máximo (em dias) depois do qual o mecanismo de detecção será relatado como desatualizado. O valor padrão da **Idade máxima do mecanismo de detecção (dias)** é 7.

Reversão de módulo

Caso suspeite que uma nova atualização do mecanismo de detecção e/ou módulos de programa esteja instável ou corrompida, será possível [reverter para a versão anterior](#) e desativar atualizações por um período de tempo definido.



Configuração avançada

MECANISMO DE DETECÇÃO 2

ATUALIZAR 2

PROTEÇÃO DA REDE

WEB E EMAIL 3

CONTROLE DE DISPOSITIVOS 2

FERRAMENTAS 3

INTERFACE DO USUÁRIO 1

BÁSICO

Selecionar perfil de atualização padrão: Meu perfil

Alternância de perfil automática: Editar

Configurar notificações de atualização: Editar

Limpar cache de atualização: Limpar

ALERTAS DE MECANISMO DE DETECÇÃO DESATUALIZADO

Esta configuração define a idade máxima permitida do Mecanismo de detecção antes dele ser considerado desatualizado e um alerta ser exibido.

Definir automaticamente a idade máxima do mecanismo de detecção: ☒

Idade máxima do motor de detecção (dias): 7

REVERSÃO DE MÓDULO

Criar instantâneo dos módulos: ☒

Número de instantâneos armazenados localmente: 1

Padrão OK Cancelar

Perfis

Os perfis de atualização podem ser criados para várias configurações e tarefas de atualização. A criação de perfis de atualização é especialmente útil para usuários móveis, que precisam de um perfil alternativo para propriedades de conexão à Internet que mudam regularmente.

O menu suspenso **Selecione o perfil a editar** exibe o perfil selecionado no momento, definido em **Meu perfil** por padrão.

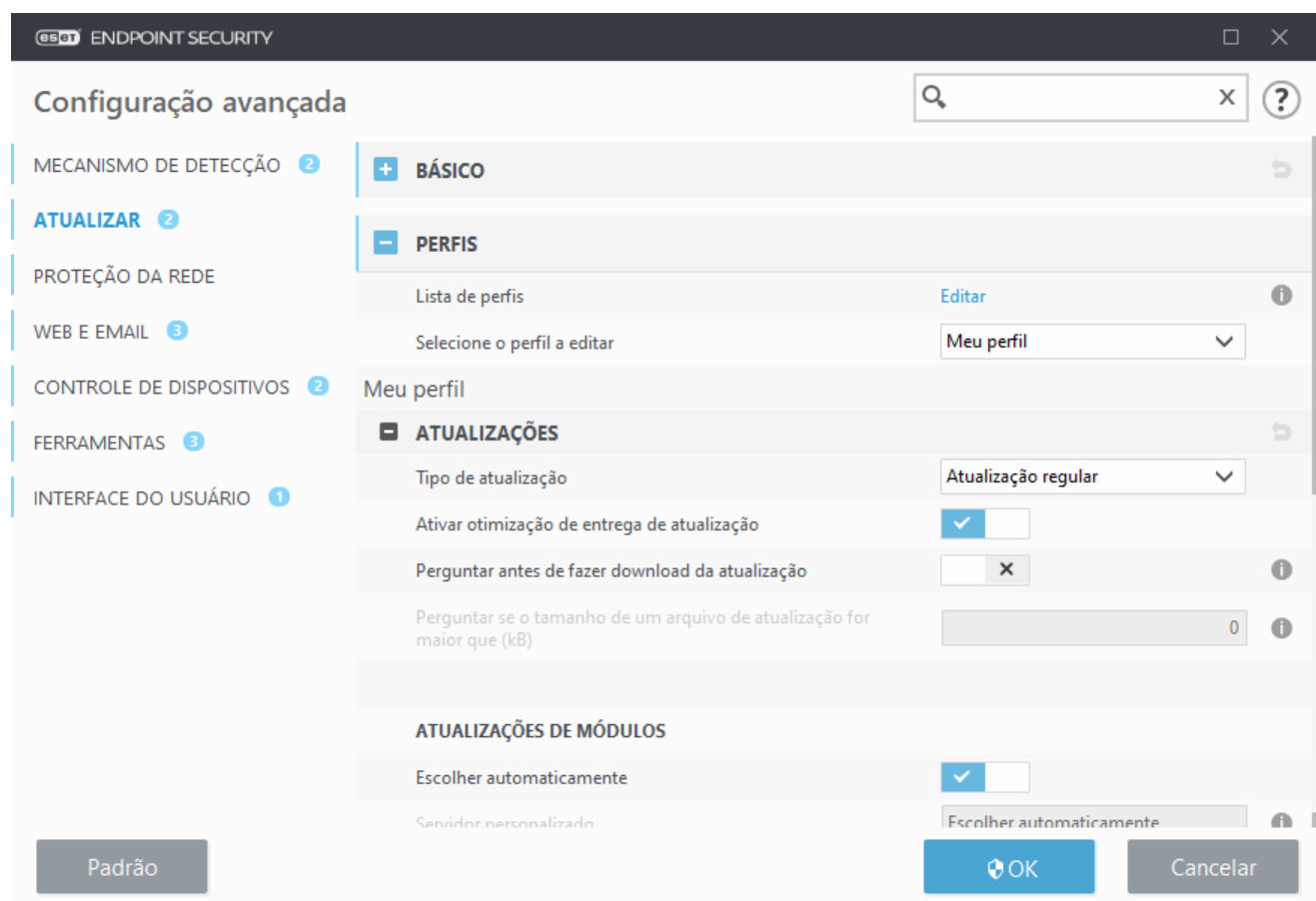
Para criar um novo perfil, clique em **Editar** ao lado de **Lista de perfis**, insira seu próprio **Nome de perfil** e então clique em **Adicionar**.

Atualizações

Por padrão, o Tipo de atualização é definido como Atualização regular para garantir que os arquivos de atualização são obtidos por download automaticamente do servidor da ESET com o menor tráfego de rede. Atualizações em modo de teste (a opção Modo de teste) são atualizações que passaram por testes internos e estarão disponíveis ao público geral em breve. Ao ativar as atualizações em modo de teste você pode se beneficiar do acesso aos métodos de detecção e correções mais recentes. No entanto, o atualização de pré-lançamento pode não ser sempre estável, e NÃO DEVE ser usado em servidores de produção e estações de trabalho em que é necessário ter a máxima disponibilidade e estabilidade. Atualização atrasada permite atualizar a partir de servidores especiais de atualização que fornecem novas versões do banco de dados de vírus com um atraso de, pelo menos, X horas (isto é, bancos de dados testados em um ambiente real e, por isso, considerados como estáveis).

Ativar otimização de entrega de atualização – Quando ativado, o download dos arquivos de atualização pode ser feito da CDN (content delivery network, rede de entrega de conteúdo). Desativar essa configuração pode causar interrupções no download e diminuições de velocidade quando os servidores de atualização da ESET estiverem sobrecarregados. Desativar é útil quando um firewall é limitado a acessar apenas os [endereços IP do servidor de atualização ESET](#) ou quando uma conexão com os serviços CDN não está funcionando.

Perguntar antes de fazer download da atualização – O programa vai exibir uma notificação onde você poderá escolher confirmar ou negar o download dos arquivos de atualização. Se o tamanho do arquivo de atualização for maior que o valor especificado no campo Perguntar se um arquivo de atualização for maior que (KB), o programa exibirá uma caixa de diálogo de confirmação. Se o tamanho do arquivo de atualização estiver definido como 0 KB, o programa sempre exibirá uma caixa de diálogo de confirmação.



Atualizações de módulos

A opção **Escolher automaticamente** está ativada por padrão. A opção **Servidor personalizado** é o local onde as atualizações são armazenadas. Se você usar um servidor de atualização da ESET, recomendamos que você deixe a opção padrão selecionada.

Ativar atualizações mais frequentes das assinaturas de detecção – As assinaturas de detecção serão atualizadas em um intervalo menor. Desativar essa configuração pode causar um impacto negativo na taxa de detecção.

Permitir atualizações de módulos a partir de mídias removíveis – Permite atualizar a partir de mídia removível se ela tiver uma imagem criada. Quando Automático estiver selecionado, a atualização será realizada em segundo plano. Se quiser exibir o diálogo de atualização selecione Sempre perguntar .

Ao usar um servidor HTTP local - também conhecido como Mirror - o servidor de atualização deve ser definido da seguinte forma:

`http://nome_computador_ou_seu_endereço_IP:2221`

Ao usar um servidor HTTP local com SSL - o servidor de atualização deve ser definido da seguinte forma:

`https://nome_computador_ou_seu_endereço_IP:2221`

Ao usar uma pasta compartilhada local - o servidor de atualização deve ser definido da seguinte forma:

`\\nome_computador_ou_seu_endereço_IP\pasta_compartilhada`



O número de porta do servidor HTTP especificado nos exemplos acima depende de qual porta seu servidor HTTP/HTTPS está escutando.

Atualizações de produto

Veja [Atualizações de produto](#).

Opção de conexão

Veja as [Opções de conexão](#).

Imagem de atualização

Veja a [Imagem de atualização](#).

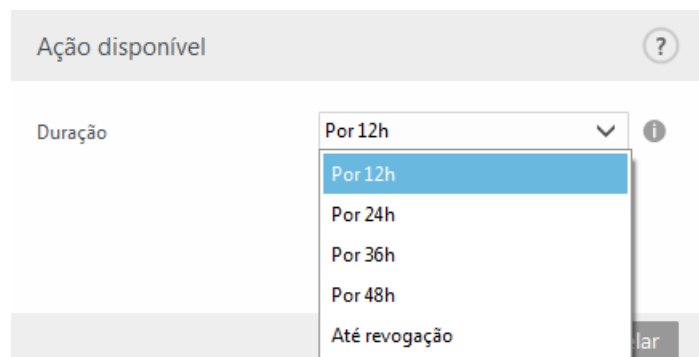
Atualização de rollback

Caso suspeite que uma nova atualização do mecanismo de detecção ou dos módulos de programa esteja instável ou corrompida, será possível reverter para a versão anterior e desativar atualizações. Alternativamente, será possível ativar atualizações desativadas anteriormente caso tenha as adiadas indefinidamente.

O ESET Endpoint Security registra instantâneos do mecanismo de detecção e dos módulos de programa para uso com o recurso de reversão. Para criar instantâneos do banco de dados de vírus, mantenha a opção **Criar instantâneos dos módulos** ativada. Quando **Criar instantâneos dos módulos** for ativado, o primeiro instantâneo será criado durante a primeira atualização. O próximo será criado depois de 48 horas. O campo **Número de instantâneos armazenados localmente** define o número de instantâneos do mecanismo de detecção armazenados.

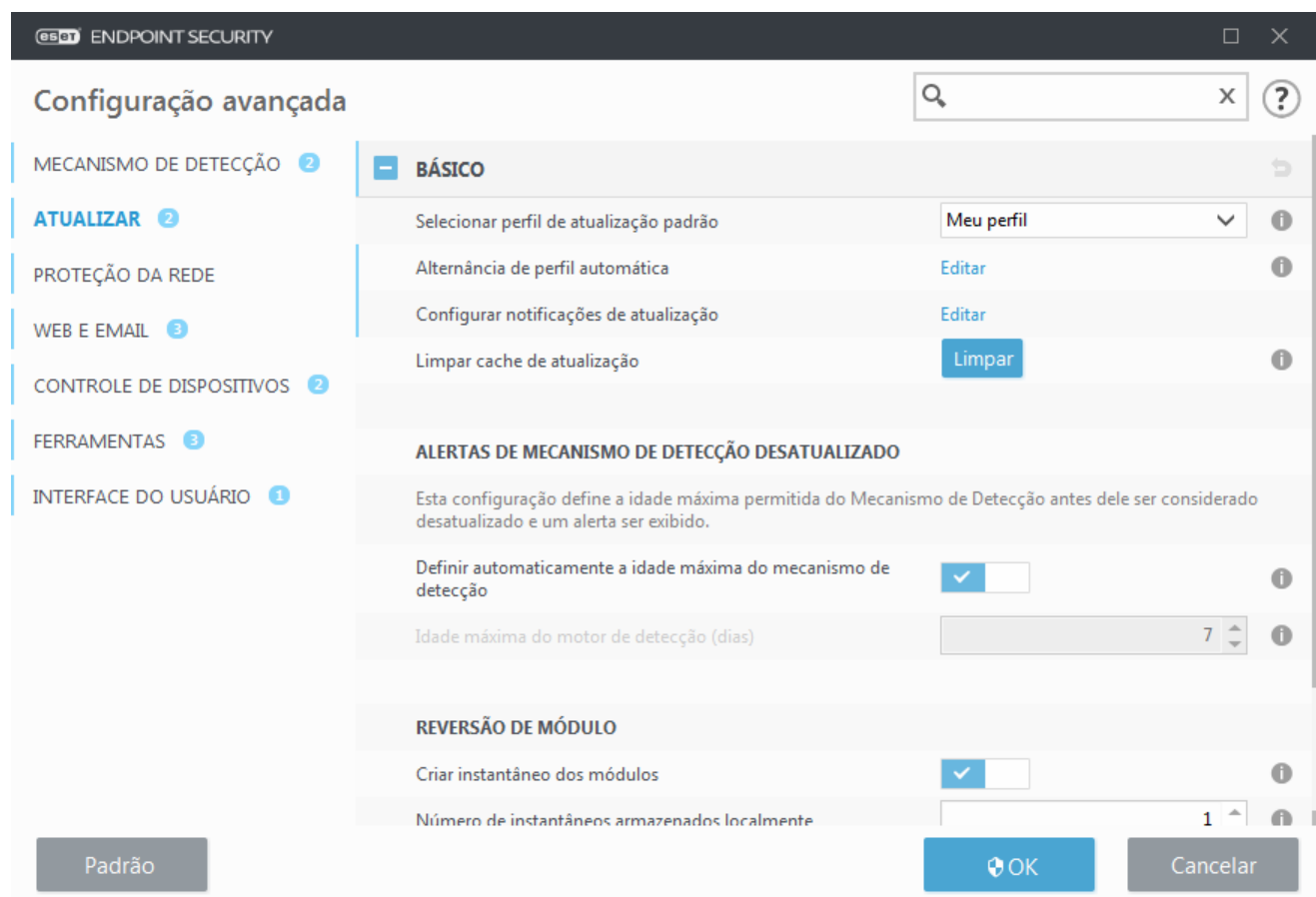
i Quando a quantidade máxima de instantâneos é alcançada (por exemplo, três), o instantâneo mais antigo é substituído por um novo instantâneo a cada 48 horas. O ESET Endpoint Security reverte as versões do mecanismo de detecção e atualização de módulos de programa para o instantâneo mais antigo.

Você deve selecionar um intervalo de tempo do menu suspenso **Duração** se clicar em **Reversão (Configuração avançada (F5) > Atualizar > Básico > Módulo de atualização)**.



Selecione **Até cancelado** para adiar atualizações regulares indefinidamente até restaurar a funcionalidade de atualização manualmente. Pois isso representa um risco de segurança em potencial, não recomendamos a seleção desta opção.

Se uma reversão for realizada, o botão **Reversão** muda para **Permitir atualizações**. Atualizações não são permitidas durante o intervalo de tempo selecionado no menu suspenso **Suspender atualizações**. A versão do mecanismo de detecção é desatualizada para a versão mais antiga disponível e armazenada como um instantâneo no sistema de arquivos do computador local.



Assuma que 22700 é o número de versão do mecanismo de detecção mais recente, e 22698 e 22696 estão armazenados como instantâneos do mecanismo de detecção. Note que o 22697 está indisponível. Neste exemplo, o computador foi desligado durante a atualização de 22697, e uma atualização mais recente foi disponibilizada antes do download de 22697. Se o campo **Número de instantâneos armazenados localmente** for dois e você clicar em **Reversão**, o mecanismo de detecção (incluindo os módulos de programa) será restaurado para a versão número 22696. Esse processo pode levar algum tempo. Verifique se a versão do mecanismo de detecção foi revertida na tela [Atualizar](#).

Atualizações de produto

A seção **Atualizações de produto** contém opções relacionadas às atualizações do produto. O programa permite que você predefinir seu comportamento quando uma nova atualização de produto estiver disponível.

As atualizações de produto oferecem novos recursos ou fazem alterações nos recursos já existentes de versões anteriores. Ela pode ser realizada automaticamente sem intervenção do usuário ou você pode escolher ser notificado. Depois das atualizações de produto serem instaladas, pode ser necessário reiniciar seu computador.

Atualizações automáticas – pausar atualizações automáticas para perfis de atualização específicos desativa temporariamente as atualizações de produto automáticas enquanto está conectado à internet usando outras redes ou conexões não relacionadas. Mantenha essa configuração habilitada para ter acesso constante aos recursos mais recentes e à maior proteção possível. Para mais informações sobre Atualizações automáticas, consulte o [FAQ de Atualizações automáticas](#).

Por padrão, o download das atualizações de produto é feito dos servidores do repositório ESET. Em ambientes grandes ou off-line, o tráfego pode ser distribuído para permitir o armazenamento em cache interno dos arquivos de produto.

[Definir o servidor personalizado para as atualizações de componentes de programa](#)

1. Defina o caminho para atualizações de produto no campo **Servidor personalizado**. Ele pode ser um link HTTP(S), um caminho de compartilhamento de rede do SMB, uma unidade de disco local ou um caminho de mídia removível. Para unidades de rede, use o caminho UNC no lugar da letra da unidade mapeada.
2. Deixe o **Nome de usuário** e **Senha** em branco, se não forem obrigatórios. Se necessário, defina aqui as credenciais apropriadas para a autenticação do HTTP no servidor web personalizado.
3. Confirme as alterações e teste a presença de uma atualização de produto usando uma atualização padrão do ESET Endpoint Security.

i A seleção da opção mais apropriada depende da estação de trabalho em que as configurações serão aplicadas. Esteja ciente de que há diferenças entre estações de trabalho e servidores; por exemplo, reiniciar o servidor automaticamente após uma atualização de produto pode provocar danos significantes à sua empresa.

Opção de conexão

Para acessar as opções de configuração do servidor proxy de determinado perfil de atualização, clique em **Atualizar** na árvore **Configuração avançada** (F5) e clique em **Perfis > Atualizações > Opções de conexão**.

Servidor proxy

Clique no menu suspenso **Modo proxy** e selecione uma das três opções a seguir:

- Não usar servidor proxy
- Conexão através de um servidor proxy
- Usar configurações globais de servidor proxy

Selecione **Usar configurações globais de servidor proxy** para usar as opções de configuração do servidor proxy já especificadas no galho **Ferramentas > Servidor proxy** da árvore Configuração avançada.

Selecione **Não usar servidor proxy** para especificar que nenhum servidor proxy será usado para atualizar o ESET Endpoint Security.

A opção **Conexão através de um servidor proxy** deve ser selecionada se:

- Um servidor proxy diferente do que está definido em **Ferramentas > Servidor proxy** é usado para atualizar o ESET Endpoint Security. Nesta configuração, as informações para o novo proxy deve ser especificadas no endereço **Servidor proxy**, **Porta** de comunicação (3128 por padrão), e **Usuário** e **Senha** para o servidor proxy, se necessário.
- As configurações do servidor proxy não são definidas globalmente, mas o ESET Endpoint Security irá estabelecer conexão com um servidor proxy para atualizações.
- Seu computador estabelece conexão com a Internet por meio de um servidor proxy. As configurações são obtidas do navegador durante a instalação do programa, mas se forem alteradas (por exemplo, se você mudar seu ISP), certifique-se as configurações de proxy listadas nesta janela estão corretas. Caso contrário, o programa não conseguirá estabelecer uma conexão com os servidores de atualização.

A configuração padrão para o servidor proxy é **Usar configurações globais de servidor proxy**.

Usar conexão direta se o proxy não estiver disponível - O Proxy será ignorado durante a atualização se não for possível acessá-lo.

Compartilhamento do Windows

Ao atualizar a partir de um servidor local com uma versão do sistema operacional Windows NT, a autenticação para cada conexão de rede é necessária por padrão.

Para configurar uma conta deste tipo, selecione a partir do menu suspenso **Conectar na rede como**:

- **Conta do sistema (padrão),**
- **Usuário atual,**
- **Usuário especificado.**

Selecione a opção **Conta do sistema (padrão)** para utilizar a conta do sistema para autenticação. De maneira geral, nenhum processo de autenticação ocorre normalmente se não houver dados de autenticação na seção principal de configuração de atualização.

Para assegurar que o programa é autenticado usando uma conta de usuário conectado no momento, selecione **Usuário atual**. A desvantagem dessa solução é que o programa não é capaz de conectar-se ao servidor de atualização se nenhum usuário tiver feito login no momento.

Selecione **Usuário especificado** se desejar que o programa utilize uma conta de usuário específica para autenticação. Use esse método quando a conexão com a conta do sistema padrão falhar. Lembre-se de que a conta do usuário especificado deve ter acesso ao diretório de arquivos de atualização no servidor local. Caso contrário, o programa não poderá estabelecer conexão e fazer download das atualizações.

As configurações **Nome de usuário** e **Senha** são opcionais.



Quando a opção **Usuário atual** ou **Usuário especificado** estiver selecionada, um erro poderá ocorrer ao alterar a identidade do programa para o usuário desejado. Recomendamos inserir os dados de autenticação da rede na seção principal de configuração da atualização. Nesta seção de configuração da atualização, os dados de autenticação devem ser inseridos da seguinte maneira: *nome_domínio\usuário* (se for um grupo de trabalho, insira o *nome_do_grupo_de_trabalho\nome*) e a senha. Ao atualizar da versão HTTP do servidor local, nenhuma autenticação é necessária.

Selecione **Desconectar** do servidor depois da atualização para forçar uma desconexão se uma conexão com o servidor permanecer ativa mesmo depois de fazer o download das atualizações.

Imagem de atualização

O ESET Endpoint Security permite criar cópias dos arquivos de atualização, que podem ser usadas para atualizar outras estações de trabalho na rede. Uso de uma “imagem” - uma cópia dos arquivos de atualização no ambiente de rede local é conveniente, pois os arquivos de atualização não precisam ser obtidos por download a partir do servidor de atualização do fabricante repetidamente e por cada estação de trabalho. O download das atualizações é feito para o servidor de imagem local e, em seguida, distribuído a todas as estações de trabalho, evitando assim o risco de sobrecarga potencial do tráfego da rede. A atualização das estações clientes a partir de uma Mirror otimiza o equilíbrio de carga da rede e economiza a largura de banda da conexão com a Internet.



Para minimizar o tráfego de Internet em redes onde o ESET PROTECT é usado para gerenciar um grande número de clientes, recomendamos usar o Proxy Apache HTTP em vez de configurar um cliente como imagem. O Proxy Apache HTTP pode ser instalado com o ESET PROTECT usando o instalador tudo-em-um ou como um componente autônomo. Para mais informações e diferenças entre o Proxy Apache HTTP, Ferramenta de imagem e conectividade direta, consulte nossa [página de Ajuda on-line do ESET PROTECT](#).

As opções de configuração do servidor local da Imagem estão localizadas em Configuração avançada em **Atualizar**. Para acessar esta seção, pressione **F5** para acessar a Configuração avançada, clique em **Atualizar > Perfis** e selecione a guia **Imagem de atualização**.

Configuração avançada

MECANISMO DE DETECÇÃO 1

ATUALIZAR 5

PROTEÇÃO DA REDE

WEB E EMAIL 3

CONTROLE DE DISPOSITIVOS 1

FERRAMENTAS 2

INTERFACE DO USUÁRIO 1

Criar imagem da atualização ☒

ACESSO PARA ATUALIZAR ARQUIVOS

Pasta de armazenamento
C:\ProgramData\ESET\ESET Smart Security Premium\mirror [Limpar](#)

Ativar servidor HTTP ☒

Nome de usuário

Senha

ATUALIZAÇÃO DE COMPONENTE DE PROGRAMA

Arquivos [Editar](#)

Atualizar componentes automaticamente ☒

Atualizar componentes agora [Atualizar](#)

SERVIDOR HTTP

OPÇÃO DE CONEXÃO

Padrão OK Cancelar

Para criar uma imagem na estação de trabalho do cliente, ative **Criar imagem da atualização**. Ativar essa opção ativa as outras opções de configuração da Imagem, como o modo em que os arquivos serão acessados e o caminho de atualização para os arquivos da imagem.

Acesso para atualizar arquivos

Ativar servidor HTTP – Se ativado, os arquivos de atualização podem ser [acessados através de HTTP](#), sem a necessidade de credenciais.


Os métodos de acesso do servidor de Imagem estão descritos em detalhes na seção [Atualização através do Imagem](#). Há dois métodos básicos para acessar a Imagem - a pasta com os arquivos de atualização pode ser apresentada como uma pasta de rede compartilhada ou os clientes podem acessar a imagem localizada em um servidor HTTP.

A pasta dedicada a armazenar os arquivos de atualização para a Imagem é definida na seção **Pasta para armazenar arquivos da imagem**. Para escolher uma pasta diferente clique em **Limpar** para excluir a pasta pré-definida *C:\ProgramData\ESET\ESET Endpoint Security\mirror* e clique em **Editar** para procurar uma pasta no computador local ou em uma pasta de rede compartilhada. Se a autorização para a pasta especificada for necessária, os dados de autenticação devem ser fornecidos nos campos **Nome de usuário** e **Senha**. Se a pasta de destino selecionada estiver localizada em um disco de rede que esteja executando o sistema operacional Windows NT/2000/XP, o nome de usuário e a senha especificados devem ter privilégios de gravação para a pasta selecionada. O nome de usuário e a senha devem ser inseridos no formato *Domínio/Usuário* ou *Grupo de trabalho/Usuário*. Lembre-se de fornecer as senhas correspondentes.

Servidor HTTP e SSL para a Imagem


Na seção **Servidor HTTP** da guia **Imagem**, é possível especificar a **Porta do servidor** em que o servidor HTTP escutará, bem como o tipo de **Autenticação** usada pelo servidor HTTP. Por padrão, a porta do servidor está definida em **2221**.

Autenticação - define o método de autenticação usado para acessar arquivos de atualização. As opções disponíveis são: **Nenhum**, **Básico** e **NTLM**. Selecione **Básico** para utilizar a codificação base64, com autenticação através de nome de usuário e senha. A opção **NTLM** utiliza um método de codificação seguro. Para autenticação, o usuário criado na estação de trabalho que compartilha os arquivos de atualização é utilizado. A configuração padrão é **Nenhum**, que garante acesso aos arquivos de atualização sem necessidade de autenticação.

 Dados de autenticação como **Nome de usuário** e **Senha** são destinados apenas para acessar o servidor HTTP da imagem. Preencha esses campos apenas se um nome de usuário e senha forem necessários.

Acrescente o **Arquivo de encadeamento do certificado** ou gere um certificado assinado automaticamente caso deseje executar o servidor HTTP com suporte HTTPS (SSL). Os seguintes **tipos de certificado** estão disponíveis: ASN, PEM e PFX. É possível fazer download dos arquivos de atualização através do protocolo HTTPS, que fornece mais segurança. É quase impossível rastrear transferências de dados e credenciais de login usando esse protocolo. A opção **Tipo de chave privada** é definida como **Integrada** por padrão, (portanto a opção de **Chave privada de arquivo** está desativada por padrão). Isso significa que a chave privada é uma parte do arquivo de encadeamento do certificado selecionado.

Certificados com autoassinatura para imagem HTTPS

 Se você estiver usando um servidor de imagem HTTPS, será preciso importar seu certificado para o armazenamento de raiz confiável em todas as máquinas do cliente. Veja [Instalação do certificado raiz confiável](#) no Windows.

Atualização através do mirror

Existem dois métodos básicos para configurar uma Imagem, que é essencialmente um repositório onde os clientes podem fazer download de arquivos de atualização. A pasta com os arquivos de atualização pode ser apresentada como uma pasta de rede compartilhada ou como um servidor HTTP.

Acesso à Mirror utilizando um servidor HTTP interno

Essa é a configuração padrão especificada na configuração do programa predefinida. Para permitir o acesso à Imagem utilizando o servidor HTTP, navegue até **Configuração avançada > Atualizar > Perfis > Imagem de atualização** e selecione **Criar imagem da atualização**.

Na seção **Servidor HTTP** da guia **Imagem**, é possível especificar a **Porta do servidor** em que o servidor HTTP escutará, bem como o tipo de **Autenticação** usada pelo servidor HTTP. Por padrão, a porta do servidor está definida em **2221**.

Autenticação - define o método de autenticação usado para acessar arquivos de atualização. As opções disponíveis são: **Nenhum**, **Básico** e **NTLM**. Selecione **Básico** para utilizar a codificação base64, com autenticação através de nome de usuário e senha. A opção **NTLM** utiliza um método de codificação seguro. Para autenticação, o usuário criado na estação de trabalho que compartilha os arquivos de atualização é utilizado. A configuração

padrão é **Nenhum**, que garante acesso aos arquivos de atualização sem necessidade de autenticação.



Se deseja permitir acesso aos arquivos de atualização através do servidor HTTP, a pasta Mirror deve estar localizada no mesmo computador que a instância do ESET Endpoint Security que os criou.



Um erro **Nome de usuário e/ou senha inválidos** aparecerá no Painel de atualização do menu principal após diversas tentativas mal sucedidas de atualizar a partir da Imagem. Recomendamos ir para **Configuração avançada > Atualizar > Perfis > Imagem de atualização** e verificar o Nome de usuário e a Senha. A razão mais comum para esse erro é a inserção de dados de autenticação incorretos.

Após concluir a configuração do servidor de Mirror, você deve adicionar o novo servidor de atualização em estações de trabalho clientes. Para fazer isso, siga as etapas a seguir:

- **Acesse Configuração avançada (F5)** e clique em **Atualizar > Perfis > Atualizações > Atualizações de módulo**.
- Desative **Escolher automaticamente** e adicione um novo servidor ao campo **Servidor de atualização** usando um dos formatos a seguir:
http://endereço_IP_do_seu_servidor:2221
https://IP_address_of_your_server:2221 (se SSL for usado)

Acesso à Mirror por meio de compartilhamentos de sistema

Primeiro, uma pasta compartilhada deve ser criada em um dispositivo de rede ou local. Ao criar a pasta para a Imagem, é necessário fornecer acesso de "gravação" para o usuário que salvará os arquivos de atualização na pasta e acesso de "leitura" para todos os usuários que atualizarão o ESET Endpoint Security a partir da pasta de Imagem.

Depois configure o acesso à Imagem na guia **Configuração avançada > Atualizar > Perfis > Imagem de atualização** desativando **Ativar servidor HTTP**. Essa opção está ativada por padrão no pacote de instalação do programa.

Se a pasta compartilhada estiver localizada em outro computador na rede, será necessário inserir os dados de autenticação para acessar o outro computador. Para inserir os dados de autenticação, abra a **Configuração avançada** do ESET Endpoint Security (F5) e clique em **Atualizar > Perfis > Atualizações > Opções de conexão > Compartilhamentos do Windows > Conectar na rede como**. Essa configuração é a mesma para a atualização, conforme descrito na seção [Conectar na rede como](#).

Para acessar a pasta de imagens, isso deve ser feito sob a mesma conta que a conta usada para fazer login no computador onde a imagem foi criada. Caso o computador seja um domínio, o nome de usuário "domínio\usuário" deve ser usado. Caso o computador não seja um domínio, "Endereço_IP_do_seu_servidor\usuário" ou "nomedehost\usuário" deve ser usado.

Após concluir a configuração da Mirror, prossiga até as estações de trabalho e configure `\\UNC\PATH` como o servidor de atualização usando estas etapas:

1. Abra ESET Endpoint Security **Configuração avançada** e clique em **Atualizar > Perfis > Atualizações**.
2. Desative **Escolher automaticamente** ao lado de **Atualizações do módulo** e um novo servidor para o campo **Servidor de atualização** usando o formato `\\UNC\PATH`.



Para o funcionamento correto das atualizações, o caminho para a pasta Mirror deve ser especificado como um caminho UNC. A atualização das unidades mapeadas pode não funcionar.

Criação da imagem usando a ferramenta de imagem

A ferramenta de imagem cria uma estrutura de pastas diferentes da que é feita pela imagem Endpoint. Cada pasta tem arquivos de atualização para um grupo de produtos. Você precisará especificar o caminho inteiro para a pasta correta nas configurações de atualização do produto usando a imagem.

Por exemplo, para atualizar o ESET PROTECT da imagem, configure o [Servidor de atualização](#) para (de acordo com sua localização raiz do servidor HTTP):

`http://your_server_address/mirror/eset_upd/era6`

A última seção controla os componentes do programa (PCUs). Por padrão, os componentes de programas baixados são preparados para copiar para a imagem local. Se **Atualizações de produto** estiver ativado, não é necessário clicar em **Atualizar** porque os arquivos são copiados para a imagem local automaticamente quando estiverem disponíveis. Consulte [Modo de atualização](#) para obter mais informações sobre as atualizações de produto.

Solução de problemas de atualização através da imagem

Na maioria dos casos, os problemas que ocorrem durante a atualização do servidor de imagem são causados por um ou mais dos seguintes itens: especificação incorreta das opções da pasta Mirror, dados de autenticação incorretos para a pasta Mirror, configuração incorreta nas estações de trabalho locais que tentam fazer download de arquivos de atualização a partir da Mirror ou por uma combinação das razões citadas. A seguir, é fornecida uma visão geral dos problemas mais frequentes que podem ocorrer durante uma atualização da Mirror:

O ESET Endpoint Security relata um erro ao conectar a um servidor de imagem - provavelmente provocado pela especificação incorreta do servidor de atualização (caminho de rede para a pasta Imagem), a partir do qual as estações de trabalho locais fazem download de atualizações. Para verificar a pasta, clique no menu **Iniciar** do Windows, clique em **Executar**, insira o nome da pasta e clique em **OK**. O conteúdo da pasta deve ser exibido.

O ESET Endpoint Security requer um nome de usuário e senha - Provavelmente provocado por dados de autenticação incorretos (nome de usuário e senha) na seção de atualização. O nome do usuário e a senha são utilizados para garantir acesso ao servidor de atualização, a partir do qual o programa se atualizará. Verifique se os dados de autenticação estão corretos e inseridos no formato correto. Por exemplo, Domínio/Nome de usuário ou Grupo de trabalho/Nome de usuário, além das senhas correspondentes. Se o servidor de imagem puder ser acessado por "Todos", esteja ciente de que isso não significa que o acesso é garantido a qualquer usuário. "Todos" não significa qualquer usuário não autorizado, apenas significa que a pasta pode ser acessada por todos os usuários do domínio. Como resultado, se a pasta puder ser acessada por "Todos", um nome de usuário e uma senha do domínio ainda precisarão ser inseridos na seção de configuração da atualização.

O ESET Endpoint Security relata um erro ao conectar a um servidor de imagem - A comunicação na porta definida para acessar a versão HTTP da Imagem está bloqueada.

O ESET Endpoint Security relata um erro ao fazer download dos arquivos de atualização - Provavelmente provocado pela especificação incorreta do servidor de atualização (caminho de rede para a pasta Imagem), a partir do qual as estações de trabalho locais fazem download de atualizações.

Como criar tarefas de atualização

As atualizações podem ser acionadas manualmente clicando em **Verificar se há atualizações** na janela primária, exibida depois de clicar em **Atualizar** no menu principal.

As atualizações também podem ser executadas como tarefas agendadas. Para configurar uma tarefa agendada, clique em **Ferramentas > Agenda**. Por padrão, as seguintes tarefas estão ativadas no ESET Endpoint Security:

- **Atualização automática de rotina**
- **Atualização automática após conexão dial-up**
- **Atualização automática após logon do usuário**

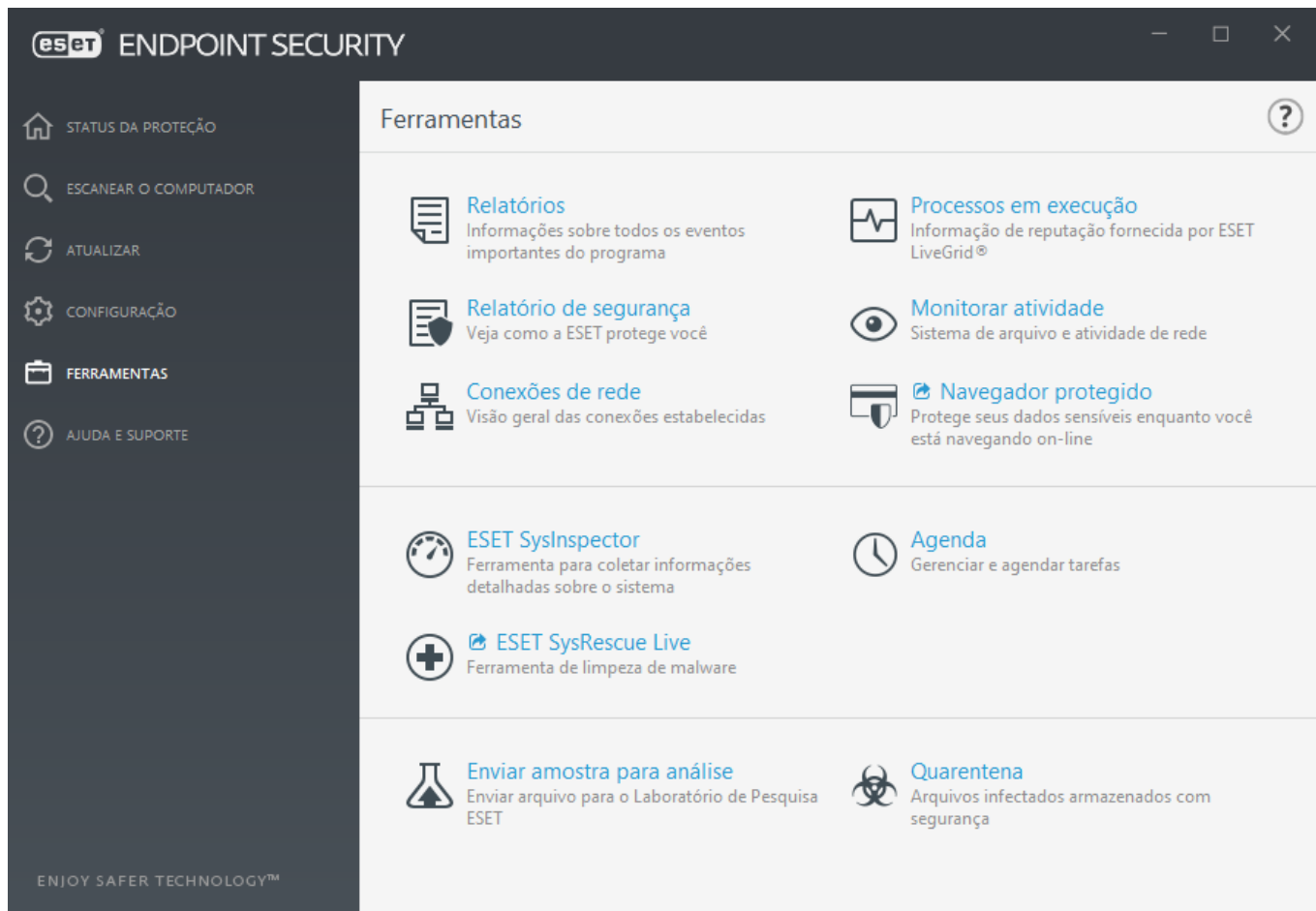
Toda tarefa de atualização pode ser modificada para atender às suas necessidades. Além das tarefas de atualização padrão, você pode criar novas tarefas de atualização com uma configuração definida pelo usuário. Para obter mais detalhes sobre a criação e a configuração de tarefas de atualização, consulte [Agenda](#).

Ferramentas

O menu **Ferramentas** inclui módulos que ajudam a simplificar a administração do programa e oferecem opções adicionais para usuários avançados.

Esse menu inclui as seguintes ferramentas:

- [Relatórios](#)
- [Processos em execução](#) (se o ESET LiveGrid® estiver ativado no ESET Endpoint Security)
- [Relatório de segurança](#) (para endpoints não gerenciados)
- [Conexões de rede](#) (se o [Firewall](#) estiver ativado no ESET Endpoint Security)
- [Navegador protegido](#) (desativado no ESET Endpoint Security por padrão)
- [ESET SysInspector](#)
- [Agenda](#)
- [ESET SysRescue Live](#) – Redireciona você para o site da ESET SysRescue Live, onde você pode fazer download da imagem do CD/DVD ESET SysRescue Live .iso.
- [Enviar amostra para análise](#) – Permite enviar um arquivo suspeito para análise para o Laboratório de pesquisa da ESET (pode não estar disponível com base em sua configuração do ESET LiveGrid®).
- [Quarentena](#)



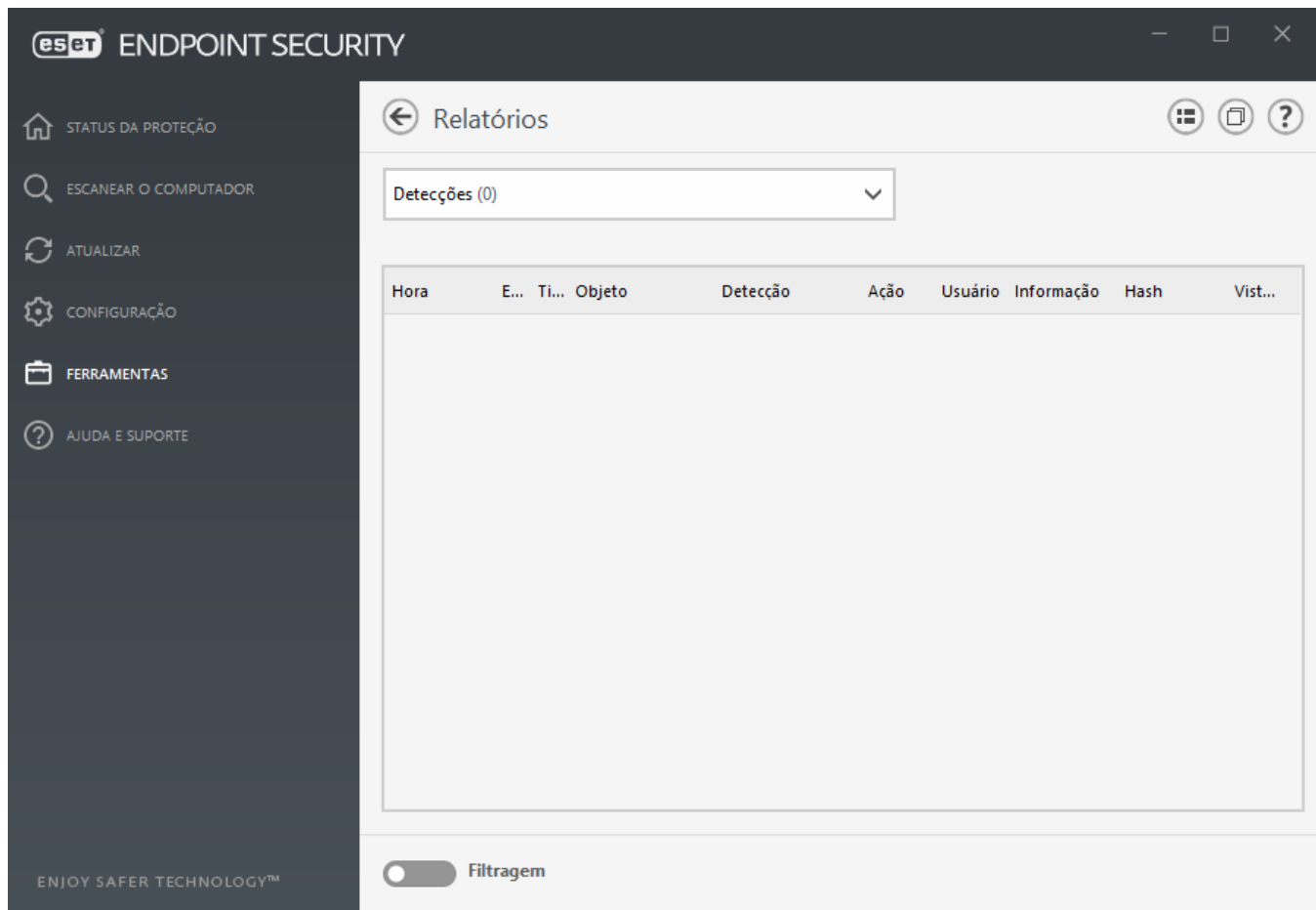
Relatórios

Os relatórios contêm informações sobre todos os eventos importantes do programa que ocorreram e fornecem uma visão geral das ameaças detectadas. O registro em log atua como uma ferramenta essencial na análise do sistema, na detecção de ameaças e na solução de problemas. O registro em relatório realiza-se ativamente em segundo plano, sem interação do usuário. As informações são registradas com base nas configurações atuais do detalhamento de relatórios. É possível visualizar mensagens de texto e logs diretamente do ambiente do ESET Endpoint Security. Bem como arquivar relatórios.

Os arquivos de log podem ser acessados na janela principal do programa, clicando em **Ferramentas > Arquivos de log**. Selecione o tipo de log desejado no menu suspenso **Log**. Os seguintes logs estão disponíveis:

- **Deteções** – Este relatório fornece informações detalhadas sobre as detecções e infiltrações detectadas pelos módulos do ESET Endpoint Security. As informações incluem a hora da detecção, nome da detecção, local, ação realizada e o nome do usuário conectado no momento em que a infiltração foi detectada. Clique duas vezes em qualquer entrada de relatório para exibir seus detalhes em uma janela separada. Infiltrações que não foram limpas sempre estão marcadas com um texto vermelho em um fundo vermelho claro, infiltrações limpas estão marcadas com um texto amarelo em um fundo branco. Aplicativos potencialmente não seguros ou PUAs não limpos são marcados com um texto amarelo em um fundo branco.
- **Eventos** - Todas as ações importantes executadas pelo ESET Endpoint Security são registradas no relatório de eventos. O log de eventos contém informações sobre eventos e erros que ocorreram no programa. Essa opção foi desenvolvida para ajudar administradores do sistema e usuários na solução de problemas. Muitas vezes as informações encontradas aqui podem ajudá-lo a encontrar uma solução para um problema no programa.

- **Rastreamento do computador** - Todos os resultados de rastreamento são exibidos nesta janela. Cada linha corresponde a um rastreamento no computador. Clique duas vezes em qualquer entrada para exibir os detalhes do respectivo escaneamento.
- **Arquivos bloqueados** – contém registros de arquivos bloqueados que não podem ser acessados quando conectado ao ESET Enterprise Inspector. O protocolo mostra o motivo e o módulo de origem que bloqueou o arquivo, assim como o aplicativo e o usuário que executaram o arquivo. Para mais informações, consulte o [Guia do usuário on-line do ESET Enterprise Inspector](#).
- **Arquivos enviados** – Contém registros de arquivos que foram enviados para o ESET LiveGrid® ou o [ESET LiveGuard](#) para análise.
- **Relatórios de auditoria** – Cada relatório contém informações sobre a data e hora em que a alteração foi realizada, o tipo de alteração, descrição, origem e usuário. Consulte [Relatórios de auditoria](#) para mais detalhes.
- **HIPS** - Contém registros de regras específicas que foram marcadas para registro. O protocolo exibe o aplicativo que acionou a operação, o resultado (se a regra foi permitida ou proibida) e o nome da regra criada.
- **Proteção de rede** – O relatório de firewall exibe todos os ataques remotos detectados pela [Proteção contra ataques de rede](#) ou [Firewall](#). Aqui, você vai encontrar informações sobre todos os ataques em seu computador. A coluna Evento lista os ataques detectados. A coluna Origem informa mais sobre quem atacou. A coluna Protocolo revela o protocolo de comunicação usado para o ataque. A análise do relatório de proteção do firewall pode ajudá-lo a detectar tentativas de infiltração do sistema a tempo de evitar o acesso sem autorização ao sistema. Para obter mais detalhes sobre ataques de rede específicos, consulte [Opções avançadas e IDS](#).
- **Sites filtrados** – Esta lista é útil se você quiser visualizar uma lista de sites que foram bloqueados pela [Proteção de acesso à Web](#) ou [Controle de Web](#). Nesses logs, você poderá ver o horário, URL, usuário e aplicativo que criaram uma conexão para o site específico.
- **Proteção antispam** - Contém registros relacionados com mensagens de email que foram marcadas como spam.
- **Controle da Web** - Mostra endereços URL bloqueados ou permitidos e detalhes sobre suas categorias. A coluna Ação executada mostra como as regras de filtragem foram aplicadas.
- **Controle de dispositivos** - Contém registros de dispositivos ou mídias removíveis que foram conectados ao computador. Apenas dispositivos com uma regra de controle de dispositivo serão registrados no relatório. Se a regra não coincidir com um dispositivo conectado, uma entrada de relatório para um dispositivo conectado não será criada. Aqui você também pode visualizar detalhes, como tipo de dispositivo, número de série, nome do fornecedor e tamanho da mídia (se disponível).



Selecione o conteúdo de qualquer relatório e pressione **Ctrl + C** para copiá-lo para a área de transferência. Pressione **Ctrl + Shift** para selecionar várias entradas.

Clique em  **Filtragem** para abrir a janela [Filtragem de relatórios](#) onde poderá definir os critérios de filtragem.

Clique com o botão direito em um registro específico para abrir o menu de contexto. As seguintes opções também estão disponíveis no menu de contexto.

- **Mostrar** - Mostra informações mais detalhadas sobre o relatório selecionado em uma nova janela.
- **Filtrar os mesmos registros** - Depois de ativar esse filtro, você só verá registros do mesmo tipo (diagnósticos, avisos...).
- **Filtrar** – Depois de clicar nessa opção, a janela [Filtragem de relatórios](#) permitirá que você defina critérios de filtragem para entradas de relatório específicas.
- **Ativar filtro** - Ativa configurações de filtro.
- **Desativar filtro** - Limpa todas as configurações de filtro (conforme descrito acima).
- **Copiar/Copiar tudo** - Copia informações sobre todos os registros na janela.
- **Excluir/Excluir tudo** - Exclui o(s) registro(s) selecionado(s) ou todos os exibidos - essa ação requer privilégios de administrador.
- **Exportar** – Exporta informações sobre o(s) registro(s) em formato XML.
- **Exportar todos** - Exporta informações sobre todos os registros em formato XML.
- **Encontrar/Encontrar próximo/Encontrar anterior** – depois de clicar nessa opção, você pode definir critérios de filtragem na janela de Filtragem de relatórios para destacar a entrada específica.
- **Criar exclusão** – Cria uma nova [Exclusão de detecção usando um assistente](#) (não disponível para detecções de malware).

Filtragem de relatórios

Clique em  **Filtragem** em **Ferramentas > Arquivos de relatório** para definir os critérios de filtragem.

O recurso de filtragem de relatório vai ajudá-lo a encontrar as informações que você está procurando, especialmente quando existirem muitos registros. Com ele você poderá limitar os registros de relatório, por exemplo, se você estiver procurando um tipo específico de evento, status ou período de tempo. Você pode filtrar os registros de relatório ao especificar certas opções de pesquisa, apenas registros relevantes (de acordo com tais opções de pesquisa) serão exibidos na janela Arquivo de relatório.

Digite a palavra chave que você está procurando no campo **Localizar texto**. Use o menu suspenso **Pesquisar nas colunas** para refinar sua pesquisa. Escolha um ou mais registros do menu suspenso **Tipos de relatório de registro**. Defina o **Período de tempo** para o qual você quer ver a exibição dos resultados. Você também pode usar outras opções de pesquisa, como **Coincidir apenas palavras inteiras** ou **Diferenciar maiúsculas e minúsculas**.

Localizar texto

Digite uma cadeia de caracteres (palavra ou parte de uma palavra). Apenas registros que contém a cadeia de caracteres serão exibidos. Outros registros serão omitidos.

Pesquisar nas colunas

Selecione quais colunas serão consideradas ao realizar a pesquisa. Você pode marcar uma ou mais colunas a serem usadas para a pesquisa.

Tipos de objetos

Escolha um ou mais tipos de relatórios de registro no menu suspenso:

- **Diagnóstico** – Registra informações necessárias para ajustar o programa e todos os registros mencionados anteriormente.
- **Informativos** – Registra as mensagens informativas, incluindo as mensagens de atualizações bem-sucedidas e todos os registros mencionados anteriormente.
- **Avisos** – Registra mensagens de erros críticos e de aviso.
- **Erros** – Erros como "Erro ao fazer download de arquivo" e erros críticos serão registrados.
- **Crítico** – Registra somente os erros críticos (como erro ao iniciar a proteção antivírus)

Período de tempo

Define o período de tempo no qual deseja que os resultados sejam exibidos.

- **Não especificado** (padrão) - Não faz uma pesquisa dentro de um período de tempo, pesquisa em todos os relatórios.
- **Último dia**
- **Última semana**
- **Último mês**
- **Período de tempo** - Você pode especificar o período de tempo exato (De: e Até:) para filtrar apenas os registros do período de tempo especificado.

Coincidir apenas palavras inteiras

Use essa caixa de seleção se você quiser pesquisar por palavras inteiras para obter resultados mais precisos.

Diferenciar maiúsculas de minúsculas

Ative essa opção se for importante para você usar letras em minúscula ou maiúscula ao realizar a filtragem. Depois de ter configurado suas opções de filtragem/pesquisa, clique em **OK** para exibir os registros de relatório filtrados ou em **Localizar** para começar a pesquisa. A pesquisa é feita de cima para baixo nos arquivos de relatório, começando com sua posição atual (o registro destacado). A pesquisa para quando encontra o primeiro registro correspondente. Pressione **F3** para pesquisar o próximo registro ou clique com o botão direito e selecione **Localizar** para refinar suas opções de pesquisa.

Configuração do registro em relatório

A configuração de logs do ESET Endpoint Security pode ser acessada na janela principal do programa. Clique em **Configuração > Configuração avançada > Ferramentas > Relatórios**. A seção de logs é utilizada para definir como os logs serão gerenciados. O programa exclui automaticamente os logs mais antigos a fim de economizar espaço no disco rígido. Você pode especificar as seguintes opções para logs:

Detalhamento mínimo de registro em relatório - Especifica o nível de detalhamento mínimo de eventos a serem registrados em relatório:

- **Diagnóstico** – Registra informações necessárias para ajustar o programa e todos os registros mencionados anteriormente.
- **Informativos** – Registra as mensagens informativas, incluindo as mensagens de atualizações bem-sucedidas e todos os registros mencionados anteriormente.
- **Avisos** – Registra mensagens de erros críticos e de aviso.
- **Erros** – Erros como "Erro ao fazer download de arquivo" e erros críticos serão registrados.
- **Crítico** – Registra somente os erros críticos (como erro ao iniciar a proteção antivírus, firewall integrado, etc.).

i Todas as conexões bloqueadas serão registradas ao selecionar o nível de detalhamento do **Diagnóstico**.

As entradas de logs anteriores ao número de dias especificado no campo **Excluir registros anteriores a (dias)** são automaticamente excluídas.

Otimizar automaticamente relatórios - Se selecionada, os relatórios serão automaticamente desfragmentados se a porcentagem for superior ao valor especificado no campo **Se o número de registros não utilizados excede (%)**.

Clique em **Otimizar** para começar a desfragmentar os relatórios. Todas as entradas de relatório vazias são removidas, o que melhora o desempenho e a velocidade de processamento de relatório. Essa melhoria pode ser observada particularmente quando os relatórios tiverem um grande número de entradas.

Ativar protocolo de texto permite a armazenagem de relatórios em outro formato de arquivo, separado dos [Relatórios](#):

- **Diretório de destino** - Selecione o diretório no qual relatórios serão armazenados (aplica-se somente a texto/CSV). É possível copiar o caminho ou selecionar outro diretório ao clicar em **Limpar**. Cada seção do relatório tem seu próprio arquivo com um nome de arquivo predefinido (por exemplo, *virlog.txt* para a

seção **Ameaças detectadas** dos relatórios, se você usar formato de arquivo de texto simples para armazenar relatórios).

- **Tipo** - Se você selecionar o formato de arquivo **Texto**, os relatórios serão armazenados em um arquivo de texto e os dados serão separados em tabelas. O mesmo se aplica a formato de arquivo **CSV** separado por vírgulas. Se você escolher **Evento**, os relatórios serão armazenados no relatório de eventos do Windows (pode ser visualizado usando o Visualizador de eventos no Painel de controle) ao contrário do arquivo.
- **Excluir todos os arquivos de relatório** - Apaga todos os relatórios armazenados atualmente selecionados no menu suspenso **Tipo**. Uma notificação sobre a exclusão bem sucedida dos relatórios será exibida.

Ativar o rastreamento de alterações de configuração no Relatório de auditoria – Informa sobre cada mudança de configuração. Veja os [Relatórios de auditoria](#) para mais informações.



Para ajudar a resolver problemas mais rapidamente, a ESET poderá solicitar que você forneça relatórios de seu computador. O ESET Log Collector facilita sua coleta das informações necessárias. Para obter mais informações sobre o ESET Log Collector, consulte nosso artigo da [Base de conhecimento ESET](#).

Relatórios de auditoria

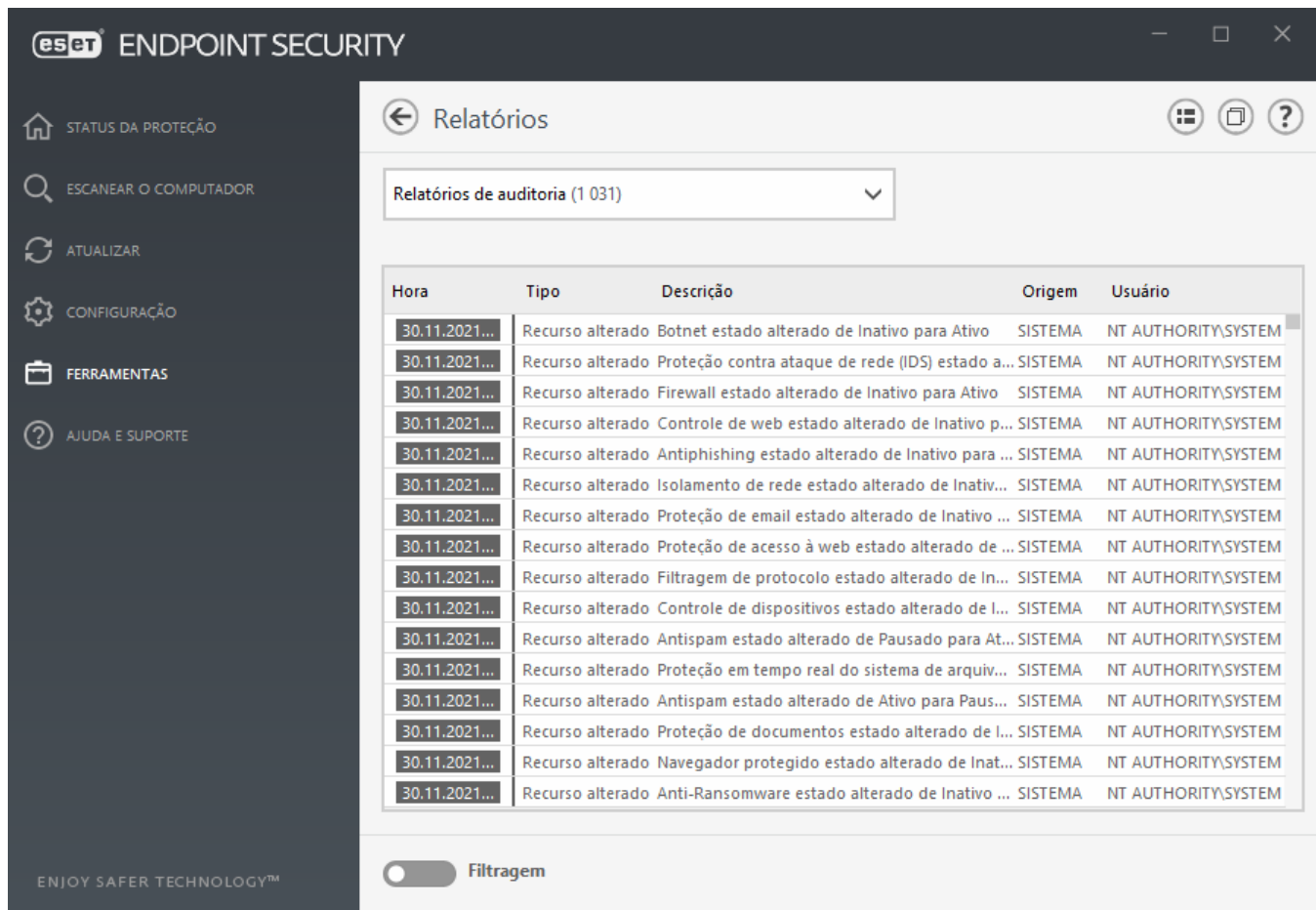
Em um ambiente empresarial, geralmente há vários usuários com direitos de acesso definidos para configurar endpoints. Como a modificação da configuração do produto pode afetar dramaticamente a forma como o produto opera, é essencial que os administradores acompanhem as alterações feitas por usuários para ajudar os administradores a identificarem, solucionarem e também impedirem, rapidamente, a ocorrência de problemas idênticos ou similares no futuro.

O Relatório de auditoria é um novo tipo de registro em relatório do ESET Endpoint Security versão 7.1 e uma solução para a identificação da origem do problema. O Relatório de auditoria acompanha as alterações na configuração ou no estado de proteção e registra instantâneos para referência posterior.

Para ver o **Relatório de auditoria**, clique em **Ferramentas** no menu principal e clique em **Arquivos de relatório** e selecione **Relatórios de auditoria** do menu suspenso.

O Relatório de auditoria contém informações sobre:

- Hora – quando a alteração foi realizada
- Tipo – que tipo de configuração ou recurso foi alterado
- Descrição – o que exatamente foi alterado e qual parte da configuração foi alterada, juntamente com o número de configurações alteradas
- Origem – qual a origem da alteração
- Usuário – quem fez a alteração



Clique com o botão direito do mouse em qualquer tipo de **Configurações alteradas** do relatório de auditoria na janela Arquivo de relatório e selecione **Exibir alterações** do menu de contexto para exibir informações detalhadas sobre a alteração realizada. Além disso, você pode restaurar uma alteração feita em uma configuração ao clicar em **Restaurar** do menu de contexto (indisponível em um produto gerenciado pelo ESET PROTECT). Se você selecionar **Remover tudo** do menu de contexto, o relatório com informações sobre essa ação será criado.

Se **Otimizar automaticamente relatórios** estiver ativado em **Configuração avançada > Ferramentas > Arquivos de relatório**, os Relatórios de auditoria serão desfragmentados automaticamente como outros relatórios.

se **Remover automaticamente registros anteriores a (dias)** estiver ativado em **Configuração avançada > Ferramentas > Arquivos de relatório**, entradas de relatório mais antigas do que o número de dias especificado serão removidas automaticamente.

Agenda

a Agenda gerencia e inicia tarefas agendadas com as configurações e propriedades predefinidas.

A Agenda pode ser acessada da janela principal do programa do ESET Endpoint Security ao clicar em **Ferramentas > Agenda**. A **Agenda** contém uma lista de todas as tarefas agendadas e suas propriedades de configuração, como a data e a hora predefinidas e o perfil de rastreamento utilizado.

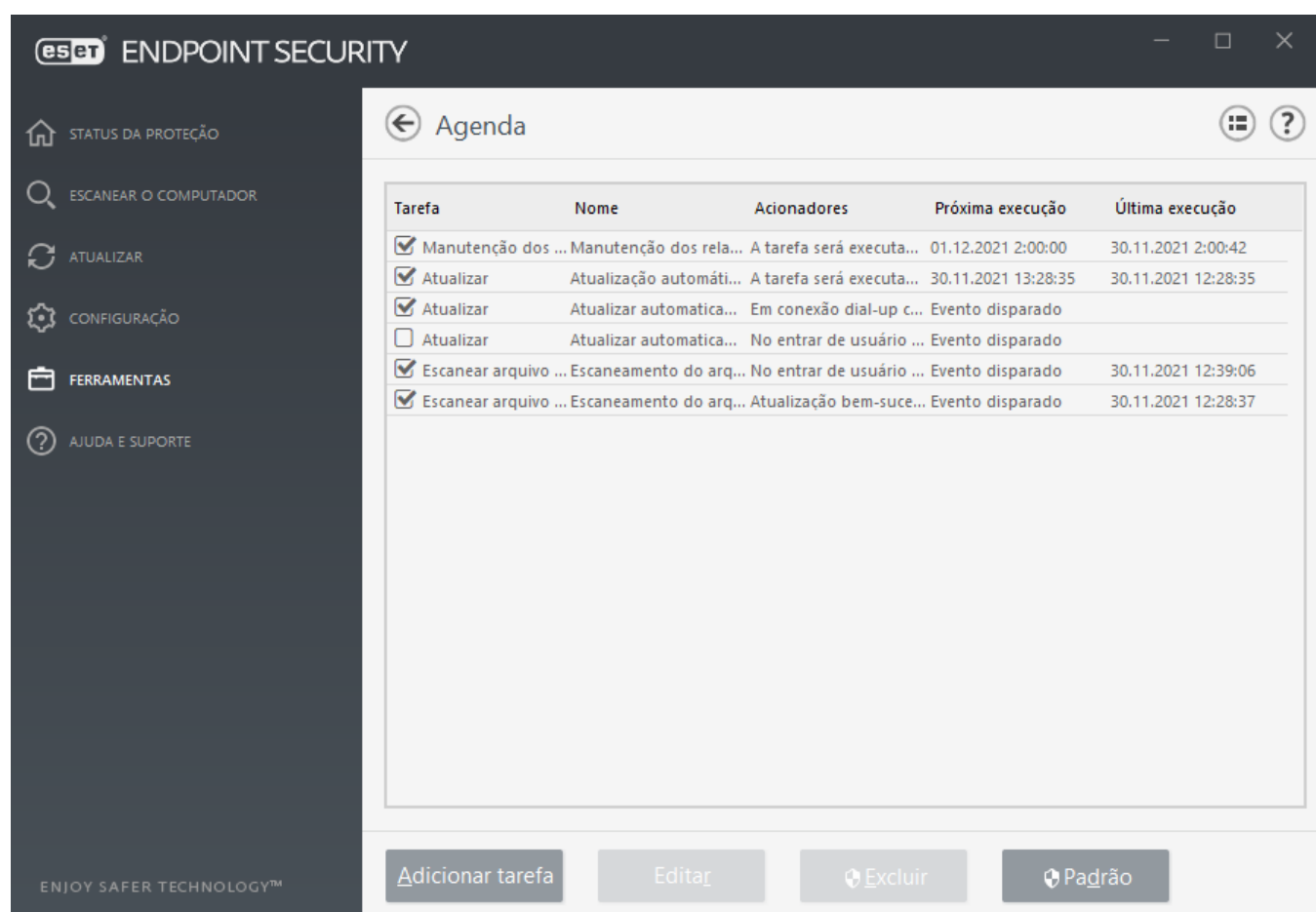
O Agendador serve para agendar as seguintes tarefas: atualização do mecanismo de detecção, tarefa de rastreamento, rastreamento de arquivos na inicialização do sistema e manutenção do relatório. Você pode adicionar ou excluir tarefas diretamente da janela principal da Agenda (clique em **Adicionar tarefa** ou **Excluir** na parte inferior). Clique com o botão direito em qualquer parte na janela de Agenda para realizar as seguintes

ações: exibir informações detalhadas, executar a tarefa imediatamente, adicionar uma nova tarefa e excluir uma tarefa existente. Use as caixas de seleção no início de cada entrada para ativar/desativar as tarefas.

Por padrão, as seguintes tarefas agendadas são exibidas na **Agenda**:

- **Manutenção de logs**
- **Atualização automática de rotina**
- **Atualização automática após conexão dial-up**
- **Atualização automática após logon do usuário**
- **Rastreamento de arquivos em execução durante inicialização do sistema** (após logon do usuário)
- **Verificação automática de arquivos durante inicialização** (depois da atualização de módulo bem sucedida)

Para editar a configuração de uma tarefa agendada existente (tanto padrão quanto definida pelo usuário), clique com o botão direito do mouse na tarefa e clique em **Editar** ou selecione a tarefa que deseja modificar e clique no botão **Editar**.



Adicionar uma nova tarefa

1. Clique em **Adicionar tarefa** na parte inferior da janela.
2. Insira o nome da tarefa.
3. Selecione a tarefa desejada no menu suspenso:

- **Executar aplicativo externo** – Agenda a execução de um aplicativo externo.
- **Manutenção de logs** - Os arquivos de log também contêm registros remanescentes excluídos. Essa tarefa otimiza regularmente os registros nos arquivos de log para funcionar de maneira eficiente.
- **Verificar arquivos na inicialização do sistema** - Verifica os arquivos que tem permissão para serem

executados no login ou na inicialização do sistema.

- **Criar um instantâneo do status do computador** - Cria um instantâneo do computador ESET SysInspector - coleta informações detalhadas sobre os componentes do sistema (por exemplo, drivers e aplicativos) e avalia o nível de risco de cada componente.
- **Rastrear o computador sob demanda** - Executa um rastreamento de arquivos e pastas em seu computador.
- **Atualização** - Agenda uma tarefa de atualização, atualizando o mecanismo de detecção e os módulos do programa.

4. Ative a opção **Ativado** se quiser ativar a tarefa (você pode fazer isso posteriormente marcando/desmarcando a caixa de seleção na lista de tarefas agendadas), clique em **Avançar** e selecione uma das opções de tempo:

- **Uma vez** - A tarefa será realizada na data e hora predefinidas.
- **Repetidamente** - A tarefa será realizada no intervalo de tempo especificado.
- **Diariamente** - A tarefa será executada repetidamente todos os dias no horário especificado.
- **Semanalmente** - A tarefa será realizada na data e hora selecionadas.
- **Evento disparado** - A tarefa será realizada após um evento especificado.

5. **Selecione Pular tarefa quando estiver executando na bateria** para minimizar os recursos do sistema enquanto o laptop estiver em execução na bateria. A tarefa será realizada uma vez somente na data e hora especificadas nos campos **Execução de tarefas**. Se não foi possível executar a tarefa em um horário predefinido, você pode especificar quando ela será executada novamente:

- **Na próxima hora agendada**
- **O mais breve possível**
- **Imediatamente, se o tempo depois da última execução ultrapassar um valor específico** (o intervalo pode ser definido utilizando a caixa de rolagem **Tempo depois da última execução**)

Você pode revisar a tarefa agendada clicando com o botão direito do mouse em **Mostrar detalhes da tarefa**.

Visão geral da tarefa agendada

Nome da tarefa

Atualizar automaticamente após login do usuário

Tipo de tarefa

Atualizar

Executar a tarefa

No login de usuário (uma vez por hora no máximo)

Ação a ser realizada se a tarefa não for executada na hora especificada

Na próxima hora agendada

OK

ESET SysInspector

O [ESET SysInspector](#) é um aplicativo que inspeciona completamente o computador, coleta informações detalhadas sobre os componentes do sistema, como os drivers e aplicativos, as conexões de rede ou entradas de

registro importantes, e avalia o nível de risco de cada componente. Essas informações podem ajudar a determinar a causa do comportamento suspeito do sistema, que pode ser devido a incompatibilidade de software ou hardware ou infecção por malware. [Consulte também o Guia do usuário on-line para o ESET SysInspector.](#)

A janela do SysInspector exibe as seguintes informações sobre os logs criados:

- **Hora** – A hora de criação do relatório.
- **Comentário** - Um comentário curto.
- **Usuário** - O nome do usuário que criou o relatório.
- **Status** – O status de criação do relatório.

As seguintes ações estão disponíveis:

- **Exibir** - abre o relatório criado. Também é possível clicar com o botão direito do mouse em um determinado relatório e selecionar **Exibir** no menu de contexto.
- **Criar** - Cria um novo log. Aguarde até que o ESET SysInspector tenha terminado (o status de relatório será exibido como **Criado**) antes de tentar acessar o relatório.
- **Excluir** - Exclui os relatórios selecionados da lista.

Os itens a seguir estão disponíveis no menu de contexto quando um ou mais relatórios são selecionados:

- **Exibir** - Abre o relatório selecionado no ESET SysInspector (igual a clicar duas vezes em um relatório).
- **Criar** - Cria um novo log. Aguarde até que o ESET SysInspector tenha terminado (o status de relatório será exibido como **Criado**) antes de tentar acessar o relatório.
- **Remover** – Remove o relatório selecionado.
- **Excluir tudo** – Exclui todos os relatórios.
- **Exportar** - Exporta o relatório para um arquivo .xml ou .xml compactado.

Proteção baseada em nuvem

ESET LiveGrid® (construído sobre o sistema de alerta precoce avançado ESET ThreatSense.Net) usa dados que os usuários ESET enviaram em todo o mundo e envia-os para o Laboratório de pesquisa ESET. Ao fornecer amostras suspeitas e metadados originais, o ESET LiveGrid® nos permite reagir imediatamente às necessidades de nossos clientes e manter a ESET sensível às ameaças mais recentes.

Existem três opções:

Opção 1: ativar o sistema de reputação do ESET LiveGrid®

O sistema de reputação ESET LiveGrid® oferece listas de permissões e listas de proibições baseadas em nuvem.

Verifique a reputação dos arquivos e dos [Processos em execução](#) diretamente da interface do programa ou no menu de contexto, com informações adicionais disponíveis no ESET LiveGrid®.

Opção 2: ativar o sistema de feedback do ESET LiveGrid®


Além do sistema de reputação ESET LiveGrid®, o sistema de feedback ESET LiveGrid® coletará informações sobre o seu computador relacionadas a ameaças recém-detectadas. Essas informações podem incluir uma amostra ou cópia do arquivo no qual a ameaça apareceu, o caminho para o arquivo, o nome do arquivo, a data e a hora, o

processo pelo qual a ameaça apareceu no computador e as informações sobre o sistema operacional do seu computador.

Por padrão, o ESET Endpoint Security é configurado enviar arquivos suspeitos ao Laboratório de vírus da ESET para análise detalhada. Arquivos com certas extensões como *.doc* ou *.xls* são sempre excluídos. Você também pode adicionar outras extensões se houver arquivos específicos que você ou sua organização deseja evitar enviar.

Opção 3: escolher não ativar o ESET LiveGrid®

Você não perderá nenhuma funcionalidade do software, mas, em alguns casos, o ESET Endpoint Security poderá responder mais rápido a novas ameaças do que a atualização do mecanismo de detecção quando o ESET LiveGrid® estiver ativado.

 Leia mais sobre ESET LiveGrid® no [glossário](#).
Confira nossas [instruções ilustradas](#) disponíveis em inglês e em vários outros idiomas sobre como ativar ou desativar o ESET LiveGrid® no ESET Endpoint Security.

Configuração da proteção baseada em nuvem na Configuração avançada

Para acessar as configurações do ESET LiveGrid®, pressione **F5** para entrar na Configuração avançada e abra **Mecanismo de detecção > Proteção baseada em nuvem**.

Ativar o sistema de reputação ESET LiveGrid® (recomendado) - O sistema de reputação do ESET LiveGrid® melhora a eficiência de soluções anti-malware da ESET ao comparar os arquivos rastreados com um banco de dados de itens na lista de proibições e permissões da nuvem.

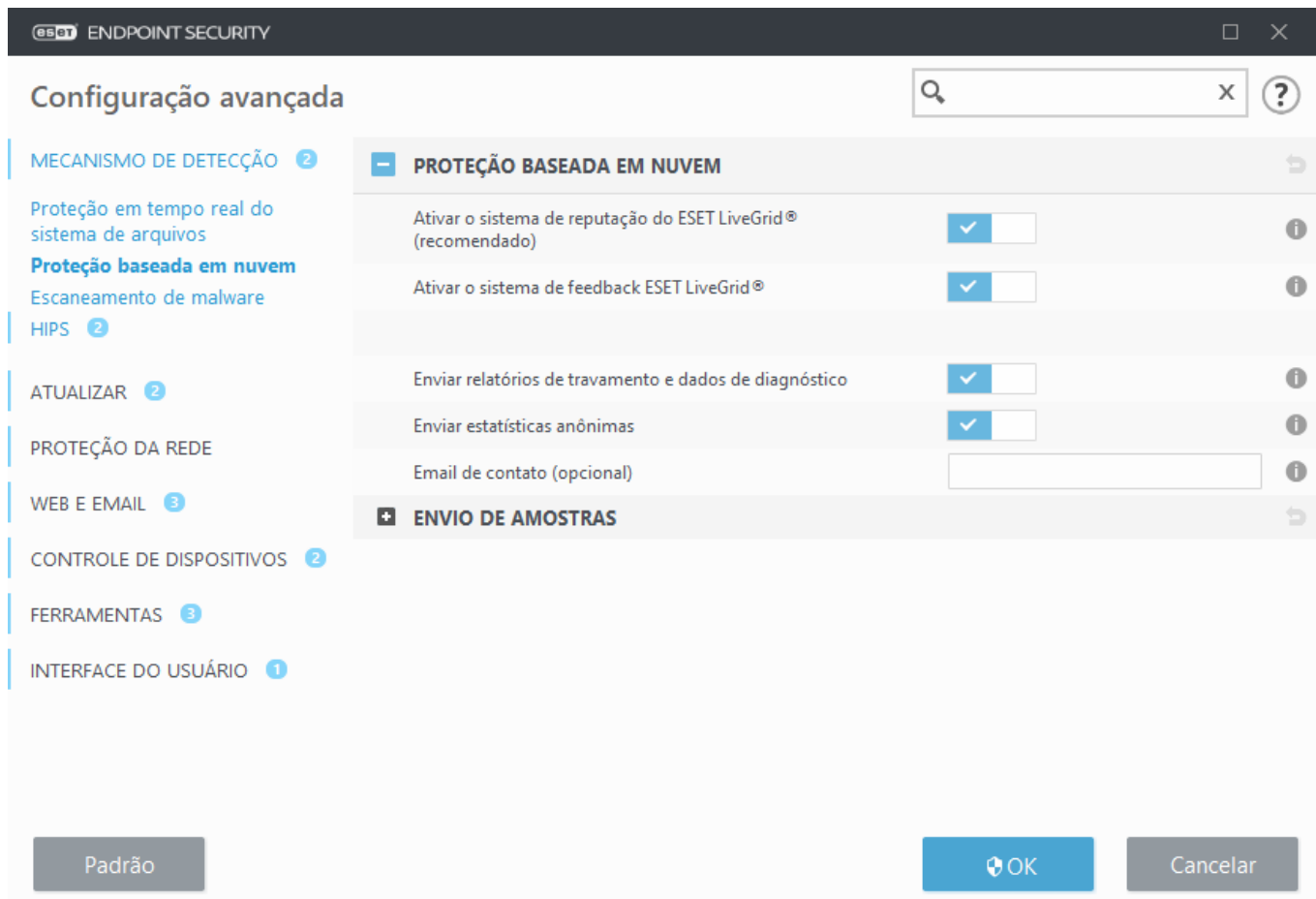
Ativar sistema de feedback ESET LiveGrid® – Envia os dados de envio relevantes (descritos na seção **Envio de amostras** abaixo) junto com os relatórios de travamento e estatísticas para o laboratório de pesquisas da ESET para análise posterior.

Ativar ESET LiveGuard (não visível no ESET Endpoint Security) – O ESET LiveGuard é um serviço pago fornecido pela ESET. Sua finalidade é adicionar uma camada de proteção desenvolvida especificamente para mitigar ameaças novas. Arquivos suspeitos são enviados automaticamente para a nuvem da ESET. Na nuvem, eles são analisados por nossos [mecanismos de detecção de malware avançados](#). O usuário que forneceu a amostra receberá um relatório de comportamento que fornece um resumo do comportamento observado da amostra.

Enviar relatórios de travamento e dados de diagnóstico – Envia dados de diagnóstico do ESET LiveGrid® relacionados, como relatórios de travamento e despejos de memória de módulos. Recomendamos manter ativado para ajudar a ESET a diagnosticar problemas, melhorar seus produtos e garantir uma proteção melhor ao usuário final.

Enviar estatísticas anônimas - Permite que a ESET colete informações sobre ameaças recém-detectadas como o nome, data e hora de detecção da ameaça, método de detecção e metadados associados, versão e configuração do produto, inclusive informações sobre seu sistema.

Email de contato (opcional) - Seu email de contato pode ser incluído com qualquer arquivo suspeito e ser utilizado para que possamos entrar em contato com você se precisarmos de mais informações para análise. Observe que você não receberá uma resposta da ESET, a menos que mais informações sejam necessárias.



Envio de amostras

Envio manual de amostras – permite enviar manualmente amostras para a ESET do menu de contexto, [Quarentena](#) ou [Ferramentas > Enviar amostras para análise](#).

Envio automático de amostras detectadas

Selecione qual tipo de amostras serão enviadas para a ESET para análise e para melhorar a detecção futura. As opções disponíveis são:

- **Todas as amostras detectadas** – Todos os [objetos](#) detectados pelo [Mecanismo de detecção](#) (inclusive aplicativos potencialmente indesejados, quando ativado nas configurações do escaneador).
- **Todas as amostras exceto documentos** – Todos os objetos detectados exceto **Documentos** (ver abaixo).
- **Não enviar** – Objetos detectados não serão enviados para a ESET.

Envio automático de amostras suspeitas

Essas amostras também serão enviadas para a ESET caso não sejam detectadas pelo mecanismo de detecção. Por exemplo, amostras que quase foram perdidas pela detecção, ou se um dos [módulos de proteção](#) do ESET Endpoint Security considerar essas amostras como suspeitas ou como tendo um comportamento incerto.

- **Executáveis** – Inclui arquivos como .exe, .dll, .sys.
- **Arquivos** – Inclui tipos de arquivo como .zip, .rar, .7z, .arch, .arj, .bzip, .gzip, .ace, .arc, .cab.
- **Scripts** – Inclui tipos de arquivo como .bat, .cmd, .hta, .js, .vbs, .ps1.
- **Outros** – Inclui tipos de arquivo como .jar, .reg, .msi, .sfw, .lnk.
- **Possíveis emails de spam** - Isto irá permitir o envio de possíveis emails de spam com anexo, parcial ou

totalmente, para a ESET para análise posterior. Ativar esta opção melhora a Detecção global de spam, incluindo melhoramentos na detecção de spam no futuro.

- **Documentos** – Inclui documentos Microsoft Office ou PDF com ou sem conteúdo ativo.

☐ [Abrir a lista de todos os tipos de arquivo de documento incluídos](#)

ACCDB, ACCDT, DOC, DOC_OLD, DOC_XML, DOCM, DOCX, DWFX, EPS, IWORK_NUMBERS, IWORK_PAGES, MDB, MPP, ODB, ODF, ODG, ODP, ODS, ODT, OLE2, OLE2_ENCRYPTED, OLE2_MACRO, OLE2_PROTECTED, ONE, ONEPKG, PDF, PPT, PPT_XML, PPTM, PPTX, PS, PSD, RTF, SYLK, THMX, VSD, VSD_XML, WPC, WPS, XLS, XLS_XML, XLSB, XLSM, XLSX, XPS

Exclusões

O [Filtro de exclusões](#) permite excluir determinados arquivos/pastas do envio. Por exemplo, pode ser útil excluir arquivos que podem conter informações sigilosas, como documentos ou planilhas. Os arquivos relacionados nunca serão enviados aos laboratórios da ESET para análise, mesmo se incluírem um código suspeito. Por padrão, os tipos mais comuns de arquivos são excluídos (.doc etc.). É possível adicioná-los à lista de arquivos excluídos, se desejar.



Para excluir arquivos baixados do download.domain.com, navegue até **Configuração avançada > Proteção baseada em nuvem > Envio de amostras > Exclusões** e adicione a exclusão *download.domain.com*.

ESET LiveGuard

Para ativar o serviço ESET LiveGuard em uma máquina do cliente usando o Web Console ESET PROTECT, veja a [configuração ESET LiveGuard para o ESET Endpoint Security](#).

Se já tiver usado o ESET LiveGrid® antes e o tiver desativado, ainda pode haver pacotes de dados a enviar. Mesmo depois da desativação, tais pacotes serão enviados à ESET. Assim que todas as informações atuais forem enviadas, não serão criados pacotes adicionais.

Filtro de exclusões para Proteção baseada em nuvem

O Filtro de exclusões permite excluir determinados arquivos ou pastas do envio de amostras. Os arquivos relacionados nunca serão enviados aos laboratórios da ESET para análise, mesmo se incluírem um código suspeito. Os tipos de arquivos comuns (como .doc, etc.) são excluídos por padrão.



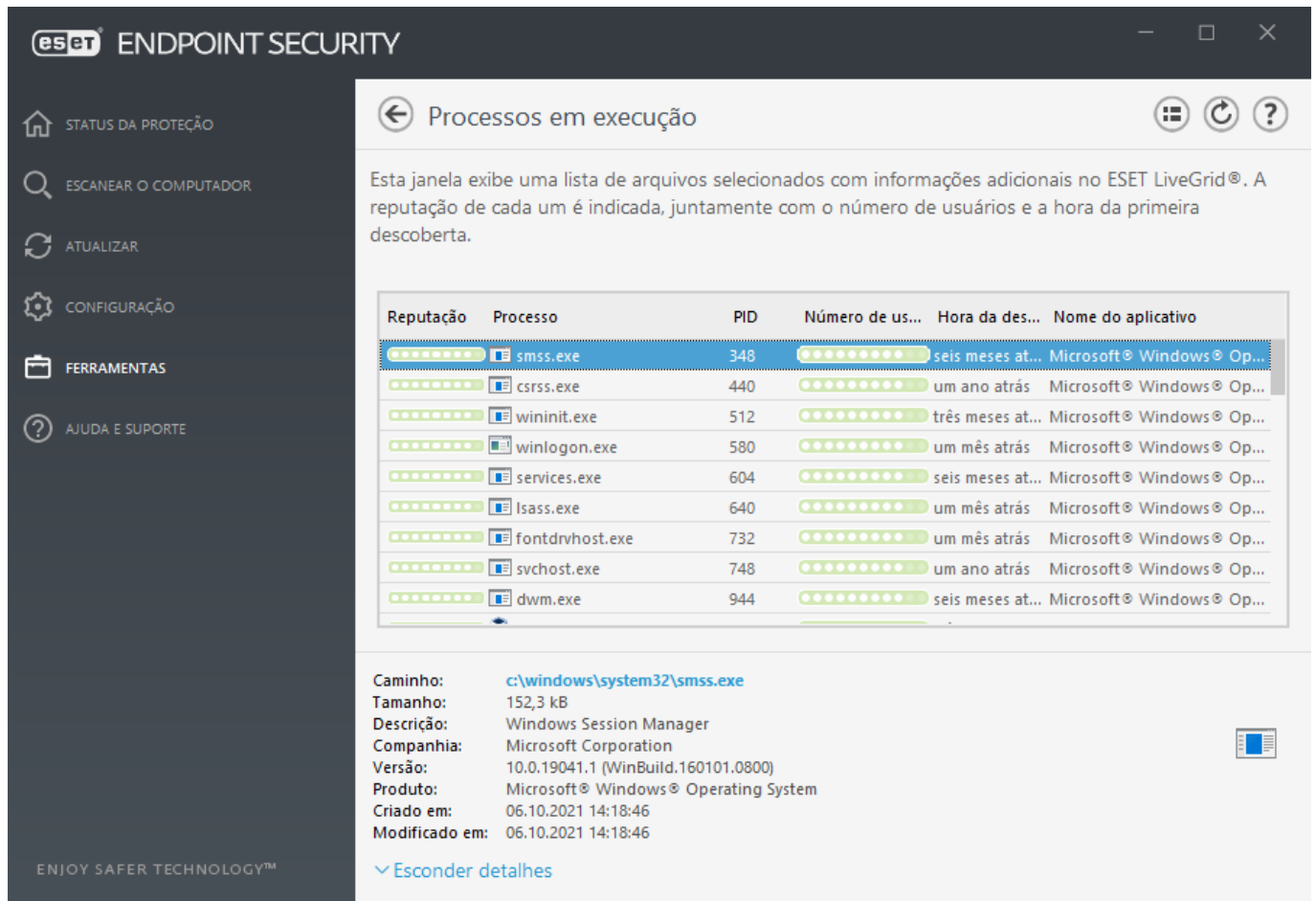
Este recurso é útil para excluir arquivos que podem conter informações sigilosas, como documentos ou planilhas.



Para excluir arquivos baixados do download.domain.com, navegue até **Configuração avançada > Proteção baseada em nuvem > Envio de amostras > Exclusões** e adicione a exclusão *download.domain.com*.

Processos em execução

Os processos em execução exibem os programas ou processos em execução no computador e mantêm a ESET imediatamente e continuamente informada sobre novas infiltrações. O ESET Endpoint Security oferece informações detalhadas sobre os processos em execução a fim de proteger os usuários com a tecnologia [ESET](#)



Reputação - Na maioria dos casos, o ESET Endpoint Security e a tecnologia ESET LiveGrid® atribuem níveis de risco aos objetos (arquivos, processos, chaves de registro etc.), utilizando uma série de regras de heurística que examinam as características de cada objeto e determinam o potencial para atividade maliciosa. Com base nessa heurística, atribui-se um nível de reputação aos objetos, que vai de 9 - Melhor reputação (verde) a 0 - Pior reputação (vermelho).

Processo - Nome da imagem do programa ou processo em execução no computador. Você também pode usar o Gerenciador de tarefas do Windows para ver todos os processos que estão em execução no computador. O Gerenciador de tarefas pode ser aberto clicando-se com o botão direito em uma área vazia da barra de tarefas e, em seguida, clicando na opção **Ctrl+Shift+Esc** no teclado.

PID - É um ID de processos em execução em sistemas operacionais Windows.

i Aplicativos conhecidos marcados como verde são limpos definitivamente (lista de permissões) e serão excluídos do escaneamento, pois isso melhorará a velocidade do escaneamento sob demanda do computador ou da Proteção em tempo real do sistema de arquivos no computador.

Número de usuários - O número de usuários que utilizam um determinado aplicativo. Estas informações são reunidas pela tecnologia ESET LiveGrid®.

Hora da descoberta - Período de tempo a partir do momento em que o aplicativo foi detectado pela tecnologia ESET LiveGrid®.

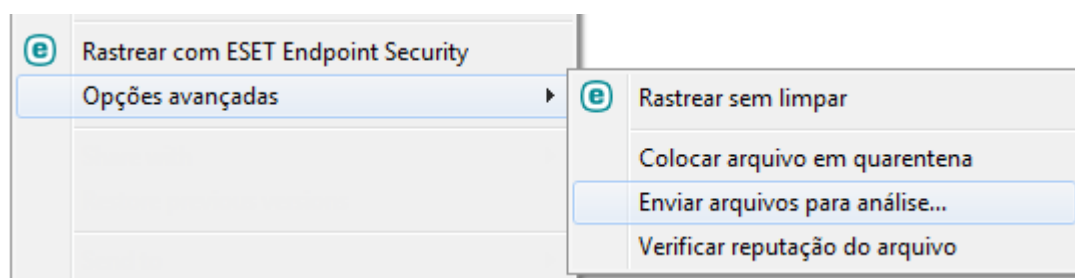
i Quando um aplicativo é marcado com o nível de segurança Desconhecido (laranja), não é necessariamente um software malicioso. Geralmente, é apenas um aplicativo mais recente. Se você não estiver certo em relação ao arquivo, use o recurso [enviar arquivo para análise](#) para enviar o arquivo para o Laboratório de vírus da ESET. Se for detectado que o arquivo é um aplicativo malicioso, sua detecção será adicionada em uma das atualizações posteriores do mecanismo de detecção.

Nome do aplicativo – O nome de um programa ou processo.

Ao clicar em um determinado aplicativo na parte inferior, as seguintes informações serão exibidas na parte inferior da janela:

- **Caminho** - Local de um aplicativo no computador.
- **Tamanho** - Tamanho do arquivo em kB (kilobytes) ou MB (megabytes).
- **Descrição** – Características do arquivo com base na descrição do sistema operacional.
- **Companhia** - Nome de processo do aplicativo ou do fornecedor.
- **Versão** – Informações do editor do aplicativo.
- **Produto** - Nome do aplicativo e/ou nome comercial.
- **Criado em** - Data e hora quando um aplicativo foi criado.
- **Modificado em** – data e hora quando um aplicativo foi modificado pela última vez.

i A reputação também pode ser verificada em arquivos que não agem como programas/processos em execução - marque os arquivos que deseja verificar, clique neles com o botão direito do mouse e, no [menu de contexto](#), selecione **Opções avançadas > Verificar reputação do arquivo usando o ESET LiveGrid®**.



Relatório de segurança

Esse recurso oferece uma visão geral das estatísticas para as categorias a seguir:

Páginas da web bloqueadas – Exibe o número de páginas da web bloqueadas (URL colocado na lista de proibições por PUA, phishing, roteador, IP ou certificado hackeados).

Objetos de e-mail detectados infectados – Exibe o número de [objetos](#) de e-mail infectados que foram detectados.

Páginas da web bloqueadas no controle de web – Exibe o número de páginas da web bloqueadas no [Controle de web](#).

PUA detectado - Exibe o número de [aplicativos potencialmente indesejados](#) (PUA) detectados.

Emails de spam detectados – Exibe o número de emails de spam detectados.

Documentos verificados – Exibe o número de objetos de documento escaneados.


Aplicativos escaneados – Exibe o número de objetos executáveis escaneados.

Outros objetos escaneados – Exibe o número de outros objetos escaneados.

Objetos de páginas da web escaneados – Exibe o número de objetos de página da web escaneados.

Objetos de email escaneados – Exibe o número de objetos de email escaneados.

A ordem dessas categorias é baseada no valor numérico, do mais alto para o mais baixo. As categorias com valor zero não são exibidas. Clique em **Mostrar mais** para expandir e exibir as categorias ocultas.

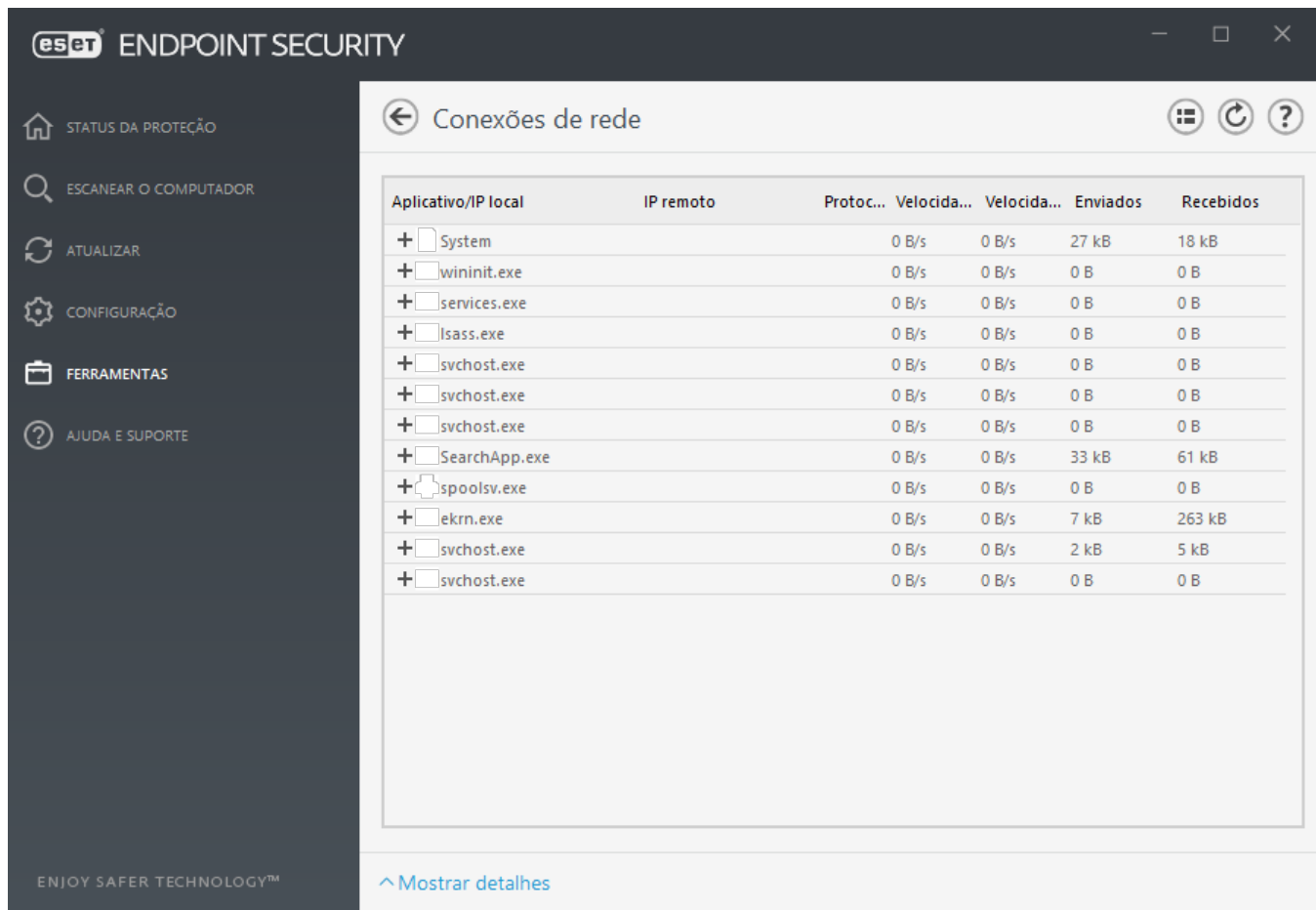
Clique na engrenagem  no canto superior direito para **Ativar/desativar notificações do relatório de segurança** ou selecione se os dados serão exibidos para os últimos 30 dias ou desde que o produto foi ativado. Se o ESET Endpoint Security estiver instalado há menos de 30 dias, apenas o número de dias a partir da instalação pode ser selecionado. O período de 30 dias está definido por padrão.



Redefinir dados vai limpar todas as estatísticas e remover os dados existentes para o Relatório de segurança. Essa ação deve ser confirmada, exceto se você desmarcar a opção **Perguntar antes de redefinir as estatísticas** na **Configuração avançada > Notificações > Alertas interativos > Mensagens de confirmação**.

Conexões de rede

Na seção Conexões de rede, você pode ver uma lista de conexões ativas e pendentes. Isso o ajuda a controlar todos os aplicativos que estabelecem conexões de saída.



A primeira linha exibe o nome do aplicativo e a velocidade de transferência dos dados. Para ver a lista de conexões feitas pelo aplicativo (bem como informações mais detalhadas), clique em +.

Colunas

Aplicativo/IP local - Nome do aplicativo, endereços IP locais e portas de comunicação.

IP remoto - Endereço IP e número de porta de um computador remoto específico.

Protocolo – Protocolo de transferência utilizado.

Velocidade de entrada/de saída - A velocidade atual dos dados de saída e entrada.

Enviados/Recebidos - Quantidade de dados trocados na conexão.

Mostrar detalhes - Escolha esta opção para exibir informações detalhadas sobre a conexão selecionada.

Selecione um aplicativo ou endereço IP na tela Conexões de rede e clique nele com o botão direito do mouse para exibir o menu de contexto com a seguinte estrutura:

Resolver nomes de host – Se possível, todos os endereços de rede serão exibidos no formato DNS, não no formato de endereço IP numérico.

Exibir somente conexões TCP - A lista só exibe conexões que pertencem ao pacote de protocolo TCP.

Mostrar conexões de escuta - Selecione essa opção para exibir somente conexões em que não haja comunicação atualmente estabelecida, mas o sistema tenha aberto uma porta e esteja aguardando por conexão.

Mostrar conexões no computador – Selecione essa opção para mostrar somente conexões nas quais o lado

remoto é um sistema local - as chamadas conexões de localhost.

Clique com o botão direito do mouse em uma conexão para visualizar as opções adicionais, que incluem:

Negar comunicação para a conexão - Finaliza a comunicação estabelecida. Essa opção só fica disponível depois que você clica em uma conexão ativa.

Velocidade de atualização - Escolha a frequência para atualizar as conexões ativas.

Atualizar agora - Recarrega a janela Conexões de rede.

As opções a seguir só ficam disponíveis depois que você clica em um aplicativo ou processo, não em uma conexão ativa:

Negar temporariamente comunicação para o processo - Rejeita as atuais conexões de determinado aplicativo. Se uma nova conexão for estabelecida, o firewall utilizará uma regra predefinida. Uma descrição das configurações pode ser encontrada na seção [Regras e zonas](#).

Permitir temporariamente comunicação para o processo - Permite as conexões atuais de determinado aplicativo. Se uma nova conexão for estabelecida, o firewall utilizará uma regra predefinida. Uma descrição das configurações pode ser encontrada na seção [Regras e zonas](#).

ESET SysRescue Live

ESET SysRescue Live é um utilitário gratuito que permite a você criar um CD/DVD de resgate que pode ser iniciado ou uma unidade USB. Você pode inicializar um computador infectado da sua mídia de resgate para escanear em busca de malware e limpar os arquivos infectados.

A principal vantagem do ESET SysRescue Live é o fato de ele ser executado de maneira independente do sistema operacional host, mas tem um acesso direto ao disco e ao sistema de arquivos. Isso possibilita remover as ameaças que não poderiam ser excluídas sob condições operacionais normais (por exemplo, quando o sistema operacional está em execução, etc.).

- [Ajuda on-line para o ESET SysRescue Live](#)

Envio de amostras para análise

Se você encontrar um arquivo suspeito no seu computador ou um site suspeito na internet, poderá enviá-lo para o Laboratório de pesquisa da ESET para análise (isso pode não estar disponível com base na sua configuração do ESET LiveGrid®).

Não envie uma amostra a menos que ela esteja de acordo com pelo menos um dos critérios a seguir:

- A amostra não foi detectada pelo seu produto ESET em absoluto
- A amostra foi detectada incorretamente como uma ameaça
- Não aceitamos seus arquivos pessoais (que você gostaria que fossem escaneados em busca de malware pela ESET) como amostras (o Laboratório de Pesquisa ESET não realiza escaneamentos sob demanda para os usuários)
- Inclua uma linha de assunto clara e o máximo de informações possível sobre o arquivo (por exemplo, uma captura de tela ou o site do qual fez o download).

O envio de amostra permite a você enviar um arquivo ou site para a ESET analisar usando um dos métodos a seguir:

1. A caixa de diálogo de envio de amostra pode ser encontrada em **Ferramentas > Enviar amostra para análise**.
2. Como alternativa, você pode enviar o arquivo por email. Se for esta sua opção, compacte o(s) arquivo(s) usando WinRAR/ZIP, proteja o arquivo com a senha "infected" (infectado) e envie-o para samples@eset.com.
3. Para reportar spam, falsos positivos de spam ou sites com a categorização errada no módulo do Controle de web, consulte nosso [artigo da base de conhecimento ESET](#).

Depois de abrir **Selecionar amostra para análise**, selecione a descrição no menu suspenso **Motivo para envio da amostra** mais adequada à sua mensagem:

- [Arquivo suspeito](#)
- [Site suspeito](#) (um site que está infectado por algum malware),
- [Arquivo falso positivo](#) (arquivo que é detectado como uma infecção, mas que não está infectado),
- [Site falso positivo](#)
- [Outros](#)

Arquivo/Site - O caminho do arquivo ou site que você pretende enviar.

Email de contato - O email de contato é enviado junto com arquivos suspeitos para a ESET e pode ser utilizado para contatar você se informações adicionais sobre os arquivos suspeitos forem necessárias para análise. É opcional inserir um email de contato. Selecione **Enviar anonimamente** para deixar o campo em branco.



Você não obterá uma resposta da ESET, a menos que mais informações sejam necessárias. A cada dia os nossos servidores recebem milhares de arquivos, o que torna impossível responder a todos os envios. Se for detectado que a amostra é um aplicativo ou site malicioso, sua detecção será adicionada em uma atualização posterior da ESET.

Selecionar amostra para análise - Arquivo suspeito

Sinais e sintomas de infecção por malware observados - Insira uma descrição do comportamento do arquivo suspeito observado em seu computador.

Origem do arquivo (endereço URL ou fabricante) - Informe a origem do arquivo (source) e como ele foi encontrado.

Observações e informações adicionais - Aqui você pode inserir informações adicionais ou uma descrição que ajudará no processo de identificação do arquivo suspeito.



O primeiro parâmetro - **Sinais e sintomas de infecção por malware observados** - é obrigatório, mas fornecer informações adicionais ajudará de maneira significativa nossos laboratórios a identificar e processar as amostras.

Selecionar amostra para análise - Site suspeito

Selecione uma das opções a seguir no menu suspenso **Qual o problema com o site**:

- **Infectado** - Um site que contenha vírus ou outro malware distribuído por vários métodos.
- **Roubo de identidade** - é frequentemente usado para obter acesso a dados sensíveis como números de

contas bancárias, códigos de PIN e outros. Leia mais sobre esse tipo de ataque no [glossário](#).

- **Fraude** - Uma fraude ou site fraudulento, especialmente para fazer um lucro rápido.
- Selecione **Outro** se as opções acima não estiverem relacionadas ao site que você vai enviar.

Observações e informações adicionais - Aqui você pode inserir informações adicionais ou uma descrição que ajudará a analisar o site suspeito.

Selecionar amostra para análise - Arquivo falso positivo

Solicitamos que você envie os arquivos que foram detectados como uma infecção, mas não estão infectados, para melhorar nosso mecanismo de antivírus e antispyware e ajudar na proteção de outros. Os casos de arquivos falsos positivos (FP) podem ocorrer quando um padrão de um arquivo corresponde ao mesmo padrão contido em um mecanismo de detecção.

Nome e versão do aplicativo - Nome do programa e sua versão (por exemplo, número, alias ou código).

Origem do arquivo (endereço URL ou fabricante) - Informe a origem do arquivo (source) e como ele foi encontrado.

Propósito dos aplicativos - Descrição geral do aplicativo, tipo de um aplicativo (por exemplo, navegador, media player etc.) e sua funcionalidade.

Observações e informações adicionais – Aqui você pode adicionar descrições ou informações adicionais que ajudarão no processamento do arquivo suspeito.

i Os primeiros três parâmetros são necessários para identificar os aplicativos legítimos e distingui-los do código malicioso. Forneça informações adicionais para ajudar nossos laboratórios de maneira significativa a processar e a identificar as amostras.

Selecionar amostra para análise - Site falso positivo

Solicitamos que você envie os sites que foram detectados como infectados, scam ou roubo de identidade, mas não são. Os casos de arquivos falsos positivos (FP) podem ocorrer quando um padrão de um arquivo corresponde ao mesmo padrão contido em um mecanismo de detecção. Forneça o site para melhorar nosso motor de antivírus e antiphishing e ajudar os outros a estarem protegidos.

Observações e informações adicionais – aqui você pode adicionar descrições ou informações adicionais que ajudarão no tratamento do site suspeito.

Selecionar amostra para análise - Outras

Utilize este formulário se o arquivo não puder ser categorizado como um **Arquivo suspeito** ou **Falso positivo**.

Motivo para envio do arquivo - Insira uma descrição detalhada e o motivo pelo qual está enviando o arquivo.

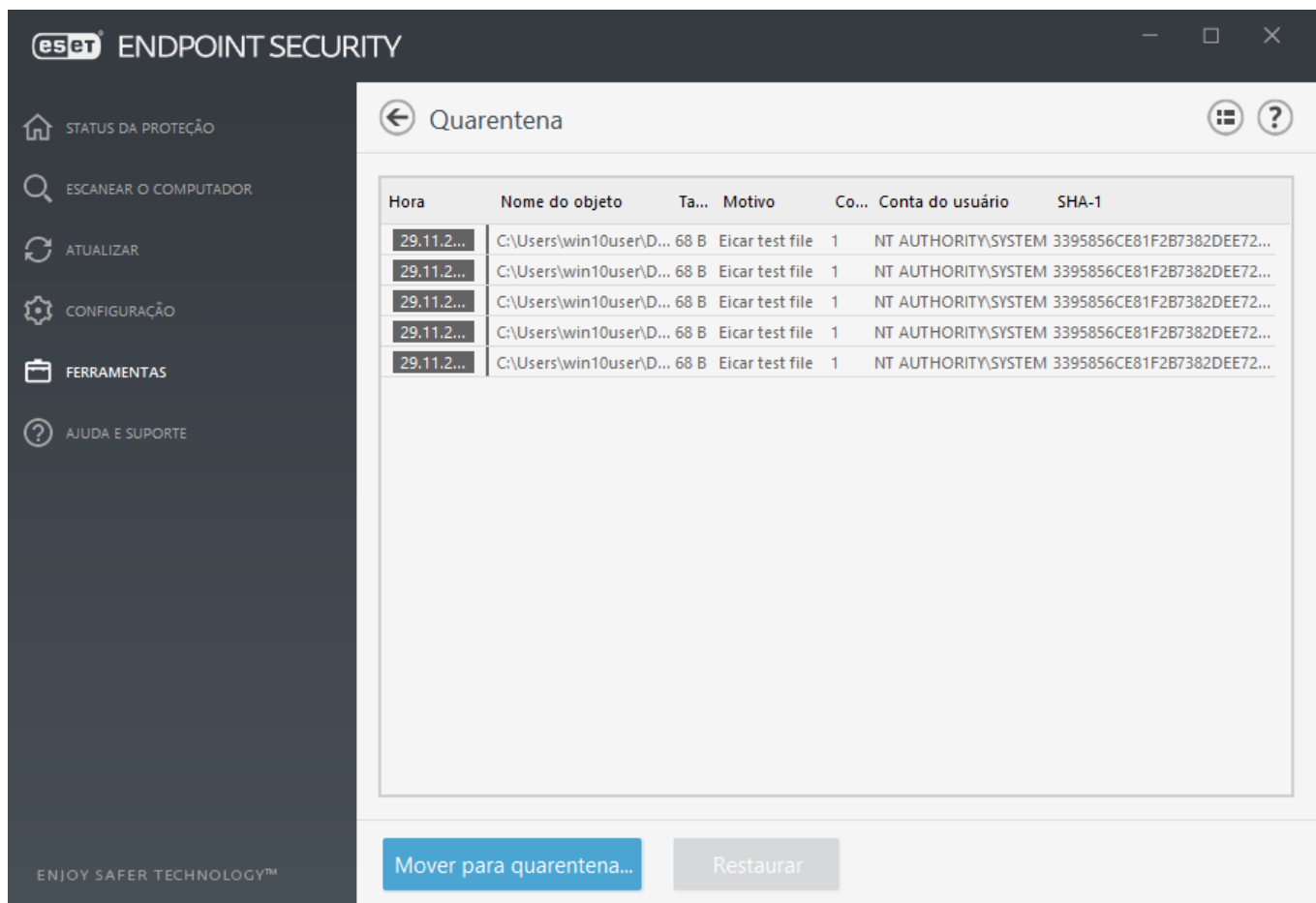
Quarentena

A principal função da quarentena é armazenar com segurança os objetos reportados (como malware, arquivos infectados ou aplicativos potencialmente indesejados).

A quarentena pode ser acessada da janela principal do programa do ESET Endpoint Security ao clicar em **Ferramentas > Quarentena**.

Os arquivos armazenados na pasta de quarentena podem ser visualizados em uma tabela que exibe:

- a data e a hora da quarentena,
 - o caminho para o local original do arquivo,
 - seu tamanho em bytes,
 - motivo (por exemplo, objeto adicionado pelo usuário),
 - e um número de detecções (por exemplo, detecções duplicadas do mesmo arquivo ou se for um arquivo compactado com vários infiltrações).
- [Gerencio a Quarentena em estações de trabalho do cliente remotamente](#)



Colocação de arquivos em quarentena

O ESET Endpoint Security automaticamente coloca os arquivos removidos em quarentena (se você não cancelou essa opção na [janela de alertas](#)).

Arquivos adicionais devem ser colocados em quarentena se:

- a. não puderem ser limpos,
- b. não for seguro nem aconselhável removê-los,
- c. eles forem erroneamente detectados pelo ESET Endpoint Security,
- d. ou se um arquivo se comportar de modo suspeito, mas não for detectado pelo [escaneador](#).

Para colocar um arquivo em quarentena, você tem várias opções:

- a. use o recurso arrastar e soltar arquivos para colocar em quarentena um arquivo manualmente ao clicar no arquivo, mover o indicador do mouse para a área marcada enquanto mantém o botão do mouse pressionado, e então soltar. Depois disso, o aplicativo é movido para o primeiro plano.
- b. Clique em **Mover para a quarentena** da janela principal do programa.
- c. O menu de contexto também pode ser usado para esse fim. Clique com o botão direito do mouse na janela **Quarentena** e selecione **Quarentena**.

Restauração da Quarentena

Os arquivos colocados em quarentena também podem ser restaurados para seu local original:

- Para isso, use o recurso **Restaurar**, que está disponível no menu de contexto clicando com o botão direito em um determinado arquivo na Quarentena.
- Se um arquivo for marcado como um [aplicativo potencialmente indesejado](#), a opção **Restaurar e excluir do escaneamento** é ativada. Veja também [Exclusões](#).
- O menu de contexto também oferece a opção **Restaurar para** que permite a você restaurar um arquivo para um local diferente daquele do qual ele foi removido.
- A funcionalidade de restauração não está disponível em alguns casos, por exemplo, para arquivos localizados em um compartilhamento de rede somente leitura.

Remover da Quarentena

Clique com o botão direito em um determinado item e selecione **Remover da quarentena**, ou selecione o item que você quer remover e pressione **Delete** no seu teclado. Também é possível selecionar vários itens e excluí-los juntos. Itens removidos serão removidos permanentemente do seu dispositivo e da quarentena.

Envio de um arquivo da Quarentena

Se você colocou em quarentena um arquivo suspeito não detectado pelo programa, ou se um arquivo foi determinado incorretamente como infectado (por exemplo, pela análise heurística do código) e colocado em quarentena, [envie a amostra para análise do Laboratório de pesquisa da ESET](#). Para enviar um arquivo, clique com o botão direito do mouse nele e selecione **Enviar para análise** no menu de contexto.

i Os artigos da Base de conhecimento da ESET a seguir podem estar disponíveis apenas em inglês:

- [Gerenciar a quarentena no ESET PROTECT](#)
- [Meu produto ESET notificou uma detecção, o que faço?](#)

Configuração do servidor proxy

Em grandes redes LAN, a comunicação entre seu computador e a Internet pode ser mediada por um servidor proxy. Usando esta configuração, as configurações a seguir precisarão ser definidas. Caso contrário, o programa não será capaz de atualizar a si mesmo automaticamente. No ESET Endpoint Security, a configuração do servidor

proxy está disponível a partir de duas seções diferentes na árvore Configuração avançada.

As configurações do servidor proxy podem ser definidas em **Configuração avançada**, em **Ferramentas > Servidor proxy**. A especificação do servidor proxy neste nível define as configurações globais do servidor proxy para todo o ESET Endpoint Security. Aqui os parâmetros serão utilizados por todos os módulos que exigem conexão com a Internet.

Para especificar as configurações do servidor proxy para esse nível, selecione **Usar servidor proxy** e digite o endereço do servidor proxy no campo **Servidor proxy**, junto com o número da **Porta** do servidor proxy.

Se a comunicação com o servidor proxy exigir autenticação, selecione **O servidor proxy requer autenticação** e digite um **Nome de usuário** e uma **Senha** válidos nos respectivos campos. Clique em **Detectar servidor proxy** para detectar e preencher automaticamente as configurações do servidor proxy. Os parâmetros especificados para seu sistema operacional serão copiados. Para encontrar as configurações de proxy no seu sistema operacional, pressione as teclas de atalho **Windows + I** e clique em **Rede e internet > Proxy**.

i É preciso inserir manualmente seu Nome de usuário e Senha nas configurações do **Servidor proxy**.

Usar conexão direta se o proxy não estiver disponível – Se o ESET Endpoint Security estiver configurado para conectar via proxy e não for possível acessar o proxy, o ESET Endpoint Security vai ignorar o proxy e se comunicar diretamente com os servidores da ESET.

Configurações do servidor proxy também podem ser estabelecidas na Configuração avançada de atualização (**Configuração avançada > Atualizar > Perfis > Atualizações > Opções de conexão** ao selecionar **Conexão através de um servidor proxy** no menu suspenso **Modo proxy**). Essa configuração será aplicada ao perfil de atualização especificado e é recomendada para laptops que recebem frequentemente atualizações do mecanismo de detecção de locais remotos. Para obter mais informações sobre essa configuração, consulte [Configuração avançada de atualização](#).

The screenshot shows the 'Configuração avançada' (Advanced Configuration) window. On the left is a sidebar with categories: MECANISMO DE DETECÇÃO, ATUALIZAR, PROTEÇÃO DA REDE, WEB E EMAIL, CONTROLE DE DISPOSITIVOS, FERRAMENTAS, and INTERFACE DO USUÁRIO. The 'FERRAMENTAS' category is expanded, showing 'Relatórios', 'Servidor proxy' (selected), 'Notificações por email', 'Modo de apresentação', and 'Diagnóstico'. The main area is titled 'SERVIDOR PROXY' and contains the following settings:

- Usar servidor proxy:** A toggle switch that is turned on (blue).
- Servidor proxy:** A text input field for the proxy address.
- Porta:** A text input field with the value '3128'.
- O servidor proxy requer autenticação:** A toggle switch that is turned off (grey).
- Nome de usuário:** A text input field for the proxy username.
- Senha:** A text input field for the proxy password.
- Detectar servidor proxy:** A blue button labeled 'Detectar'.
- Usar conexão direta se o proxy não estiver disponível:** A toggle switch that is turned on (blue).

At the bottom of the window are three buttons: 'Padrão' (Default), 'OK', and 'Cancelar' (Cancel).

Segmentos de tempo

Segmentos de tempo podem ser criados e depois atribuídos a regras para o **Controle de dispositivos** e **controle de Web**. A configuração **Segmentos de tempo** pode ser encontrado em **Configuração avançada > Ferramentas**. Ela permite a você definir segmentos de tempo usados mais normalmente (por exemplo horário de trabalho, finais de semana, etc.) e reutilizá-los com facilidade sem redefinir os intervalos de tempo para cada regra. O Segmento de tempo é aplicável a qualquer tipo relevante de regra que seja compatível com controle baseado em tempo.

Nome	Descrição
Work time	Weekdays 8:00-17:00
Off-work	Evenings & weekends

Adicionar Editar Excluir

OK Cancelar

Para criar um segmento de tempo, faça o seguinte:

1. Clique em **Editar > Adicionar**.
2. Digite o Nome e a **descrição** do segmento de tempo e clique em **Adicionar**.
3. Especifique o dia e hora de início/término do segmento de tempo ou selecione **Todo o dia**.
4. Clique em **OK** para confirmar.

Um único segmento de tempo pode ser definido com um ou mais intervalos de tempo baseado em dias e horários. Quando o intervalo de tempo é criado, ele será exibido no menu suspenso **Aplicar durante** na [janela do Editor de regras do controle de dispositivos](#) ou a [janela do editor de regras do Controle de Web](#).

Microsoft Windows Update

O recurso de atualização do Windows é um componente importante de proteção de usuários contra software malicioso. Por esse motivo, é extremamente importante manter as atualizações do Microsoft Windows em dia, instalando-as assim que forem disponibilizadas. O ESET Endpoint Security o notificará sobre as atualizações ausentes de acordo com o nível que você especificar. Os seguintes níveis estão disponíveis:

- **Nenhuma atualização** - Nenhuma atualização de sistema será proposta para download.
- **Atualizações opcionais** - Atualizações marcadas como de baixa prioridade e superiores serão propostas

para download.

- **Atualizações recomendadas** - Atualizações marcadas como comuns e superiores serão propostas para download.
- **Atualizações importantes** - Atualizações marcadas como importantes e superiores serão propostas para download.
- **Atualizações críticas** - Apenas atualizações críticas serão propostas para download.

Clique em **OK** para salvar as alterações. A janela Atualizações do sistema será exibida depois da verificação do status com o servidor de atualização. Assim, as informações sobre atualização de sistema podem não estar disponíveis imediatamente após as alterações serem salvas.

Verificação de intervalo de licença

O ESET Endpoint Security precisa se conectar aos servidores ESET automaticamente. Para alterar essa configuração, navegue até **Configuração avançada (F5) > Ferramentas > Licença**. Por padrão, a **Verificação de intervalo** está definida como **Automático**, e o servidor da Licença ESET verifica o produto algumas vezes a cada hora. Para o caso de um aumento no tráfego da rede, mude as configurações para **Limitado** para diminuir a sobrecarga. Quando **Limitado** estiver selecionado, o ESET Endpoint Security vai verificar o servidor de licença apenas uma vez por dia, ou quando o computador for reiniciado.



Se a configuração de **Verificação de intervalo** estiver definida como **Limitado**, todas as alterações relacionadas à licença feitas via ESET Business Account /ESET MSP Administrator podem levar até um dia para serem aplicadas nas configurações do ESET Endpoint Security.

Interface do usuário

A seção **Interface do usuário** permite configurar o comportamento da GUI (Graphical User Interface, interface gráfica do usuário) do programa.

Usando a ferramenta [Elementos da interface do usuário](#), é possível ajustar a aparência visual do programa e os efeitos usados.

Para obter a máxima segurança do seu software de segurança, você pode evitar quaisquer alterações não autorizadas usando a ferramenta [Configuração de acesso](#).

Ao configurar [Alertas e caixas de mensagens](#) e [Notificações](#), você poderá alterar o comportamento de alertas de detecção e notificações do sistema. Esses recursos poderão ser personalizados de acordo com suas necessidades.

Se você escolher não exibir algumas notificações, elas serão exibidas na área **Elementos da interface do usuário > Status de aplicativo**. Aqui é possível verificar o status ou, alternativamente, impedir a exibição dessas notificações.

A [Integração do menu de contexto](#) é exibida após um clique com o botão direito do mouse no objeto selecionado. Utilize essa ferramenta para integrar os elementos de controle do ESET Endpoint Security no menu de contexto.

O [Modo de apresentação](#) é útil para usuários que pretendem trabalhar com um aplicativo, sem serem interrompidos por janelas pop-up, tarefas agendadas ou quaisquer componentes que possam carregar o processador e a RAM.

Confira também [Como minimizar a interface do usuário do ESET Endpoint Security](#) (útil para ambientes

gerenciados).

Elementos da interface do usuário

As opções de configuração da interface do usuário no ESET Endpoint Security permitem que você ajuste o ambiente de trabalho para que ele atenda às suas necessidades. Essas opções de configuração são acessíveis na ramificação **Interface do usuário > Elementos da interface do usuário** da árvore Configuração avançada do ESET Endpoint Security.

Na seção **Elementos da interface do usuário**, é possível ajustar o ambiente de trabalho. Use o menu suspenso **Modo de início** para selecionar entre os seguintes modos de início da interface gráfica do usuário (GUI):

Completo - Toda a interface gráfica do usuário será exibida.

Mínimo – A interface gráfica do usuário está em execução, mas apenas as notificações são exibidas ao usuário.

Manual – A interface gráfica do usuário não foi iniciada automaticamente ao realizar login. Ela pode ser iniciada manualmente por qualquer usuário.

Silencioso – Nenhuma notificação ou alerta será exibido. A interface gráfica do usuário pode ser iniciada apenas pelo Administrador. Este modo pode ser útil em ambientes gerenciados ou em situações onde você precisa preservar os recursos do sistema.

i Quando o modo de início de interface gráfica do usuário mínima estiver selecionado e seu computador for reiniciado, serão exibidas notificações mas não a interface gráfica. Para voltar ao modo de interface gráfica do usuário completa, execute a interface gráfica do usuário no menu Iniciar em **Todos os programas > ESET > ESET Endpoint Security** como um administrador, ou faça isso através do ESET PROTECT usando uma [política](#).

Se desejar desativar a tela inicial do ESET Endpoint Security, desmarque a opção **Mostrar tela inicial na inicialização**.

Se você quiser que o ESET Endpoint Security reproduza um som quando ocorrerem eventos importantes durante um rastreamento, por exemplo quando uma ameaça é descoberta ou quando a verificação for concluída, selecione **Usar sinal sonoro**.

Integrar ao menu de contexto - Integra os elementos de controle do ESET Endpoint Security no menu de contexto.

Status

Status de aplicativo - Clique no botão **Editar** para gerenciar (desativar) status que são exibidos no painel **Status da proteção** no menu principal.

Informações da licença

Exibir informações da licença – Quando esta opção estiver desativada, não serão exibidas as informações de data de validade da licença na tela **Status da proteção** e **Ajuda e suporte**.

Exibir mensagens de licença e notificações - Quando estiver desativado, as notificações e mensagens só serão exibidas quando a licença tiver expirado.

i Configurações de informações de licença são aplicadas mas não estão acessíveis para o ESET Endpoint Security ativado com uma licença MSP.

The screenshot shows the 'Configuração avançada' (Advanced Configuration) window of ESET Endpoint Security. The left sidebar lists various configuration categories, with 'INTERFACE DO USUÁRIO' (User Interface) selected and numbered 1. The main panel is titled 'ELEMENTOS DA INTERFACE DO USUÁRIO' (User Interface Elements). It contains several settings:

- Modo de inicialização** (Startup mode): Set to 'Completo' (Full).
- Toda a interface gráfica do usuário será exibida.** (All user interface graphics will be displayed.): A descriptive text.
- Mostrar tela inicial na inicialização** (Show start screen on startup): A toggle switch that is turned on.
- Usar sinal sonoro** (Use sound signal): A toggle switch that is turned on.
- Integrar ao menu de contexto** (Integrate into context menu): A toggle switch that is turned on.
- STATUS** (Status): A section header.
- Status de aplicativo** (Application status): A button labeled 'Editar' (Edit).
- INFORMAÇÕES DA LICENÇA** (License information): A section header.
- Exibir informações da licença** (Show license information): A toggle switch that is turned on.
- Exibir mensagens de licença e notificações** (Show license and notification messages): A toggle switch that is turned on.

At the bottom of the window, there are three buttons: 'Padrão' (Default), 'OK', and 'Cancelar' (Cancel).

Configuração de acesso

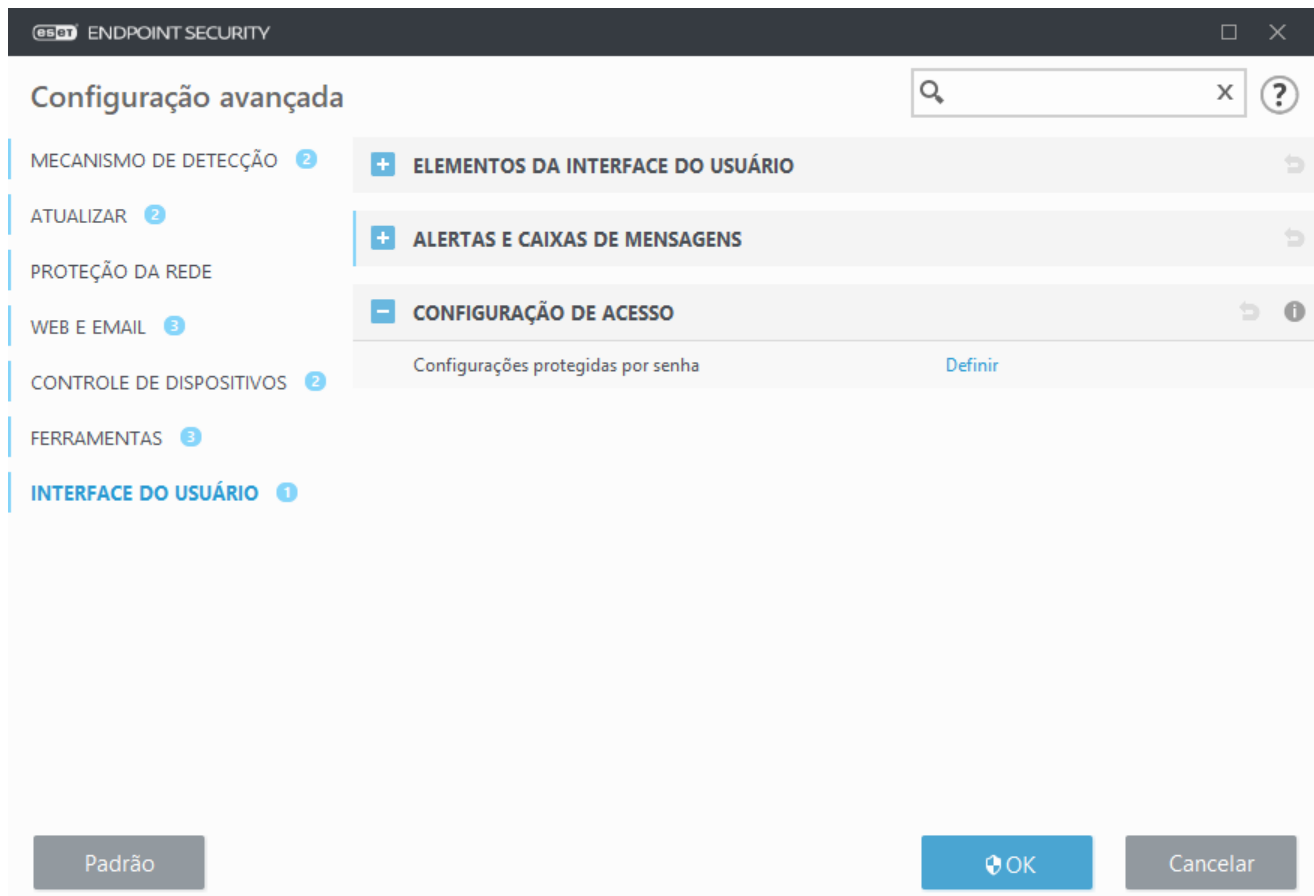
Para fornecer segurança máxima ao seu sistema, é fundamental que o ESET Endpoint Security seja configurado corretamente. Qualquer alteração não qualificada pode resultar em perda de dados importantes. Para evitar modificações não autorizadas, os parâmetros de configuração do ESET Endpoint Security podem ser protegidos por senha.

Ambientes gerenciados

O administrador pode criar uma política para proteger com senha as configurações do ESET Endpoint Security nos computadores cliente conectados. Para criar uma nova política consulte [Configurações protegidas por senha](#).

Não gerenciado

As configurações para proteção de senha estão localizadas na **Configuração avançada (F5)** sob **Interface do usuário > Configuração de acesso**.



Configurações protegidas por senha - Indica as configurações de senha. Clique para abrir a janela Configuração de senha.

Para definir uma senha para proteger os parâmetros de configuração, clique em **Definir**.

Senha para Configuração avançada

Para proteger os parâmetros de configuração do ESET Endpoint Security para evitar modificação não autorizada, uma nova senha deve ser definida.

Ambientes gerenciados

O administrador pode criar uma política para proteger com senha as configurações do ESET Endpoint Security nos computadores cliente conectados. Para criar uma nova política consulte [Configurações protegidas por senha](#).

Não gerenciado

Quando quiser alterar uma senha existente:

1. Digite sua antiga senha no campo **Senha antiga**.
2. Insira sua nova senha nos campos **Nova senha** e **Confirmar senha**.
3. Clique em **OK**.


Esta senha será solicitada em todas as modificações futuras no ESET Endpoint Security.


Se você esquecer sua senha, o acesso às configurações avançadas pode ser restaurado.

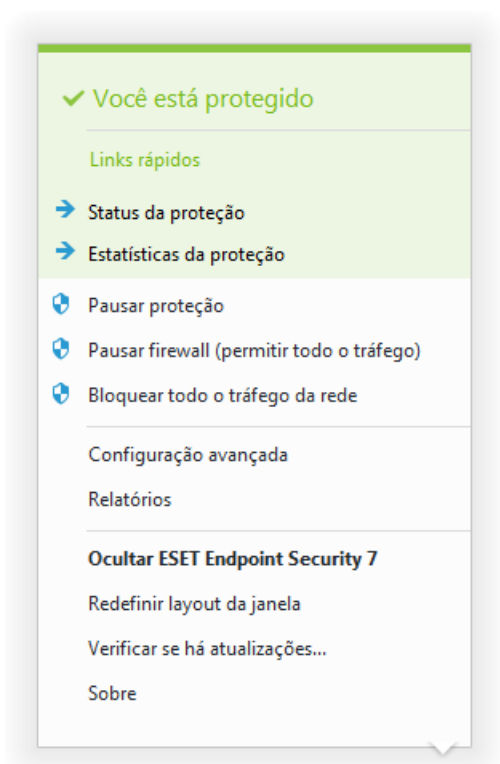
- [Restaure usando o método "Restaurar senha" \(versão 7.1 e versões posteriores\)](#)
- [Restaure usando a Ferramenta de desbloqueio ESET \(versão 7.0 e versões anteriores\)](#)

Leia mais informações caso tenha esquecido sua [Chave de licença emitida pela ESET](#), a data de expiração da sua licença ou outras informações de licença para o ESET Endpoint Security.

Ícone da bandeja do sistema

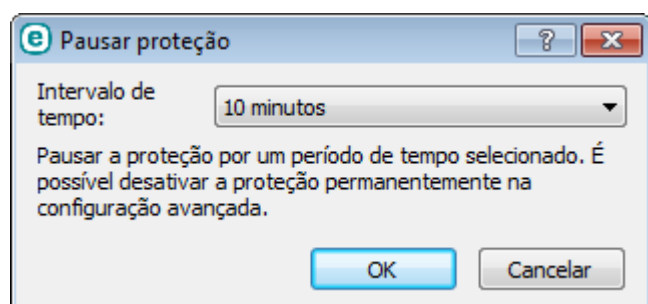
Estão disponíveis alguns dos recursos e opções de configuração mais importantes clicando com o botão direito do mouse no ícone da bandeja do sistema .

 Para acessar o menu de ícones da bandeja do sistema, certifique-se de que o modo de início dos [Elementos da interface do usuário](#) está definido como Completo.



Pausar proteção – Exibe a caixa de diálogo de confirmação que desativa o [Mecanismo de detecção](#), que protege contra ataques controlando arquivos e a comunicação via web e email.

O menu suspenso **Intervalo de tempo** representa o período de tempo em que a proteção será desativada.



Pausar firewall (permitir todo o tráfego) - Alterna o firewall para o estado inativo. Para obter mais informações, consulte [Rede](#).

Bloquear todo o tráfego da rede - O firewall bloqueará todo o tráfego de entrada / saída da rede e da Internet. É possível reativar clicando em **Parar de bloquear todo o tráfego de rede**.

Configuração avançada - Selecione esta opção para entrar na árvore de **Configuração avançada**. Você também pode acessar a Configuração avançada pressionando a tecla F5 ou acessando **Configuração > Configuração avançada**.

Arquivo de relatório – Os [Arquivos de relatório](#) contêm informações sobre todos os eventos importantes do programa que ocorreram e fornecem uma visão geral das detecções.

Abrir o ESET Endpoint Security – Abre a janela principal de programa do ESET Endpoint Security do ícone da bandeja.

Redefinir layout da janela - Redefine a janela do ESET Endpoint Security para seu tamanho e posição padrão na tela.

Verificar se há atualizações - Inicia a atualização dos módulos do programa para garantir seu nível de proteção em relação ao código malicioso.

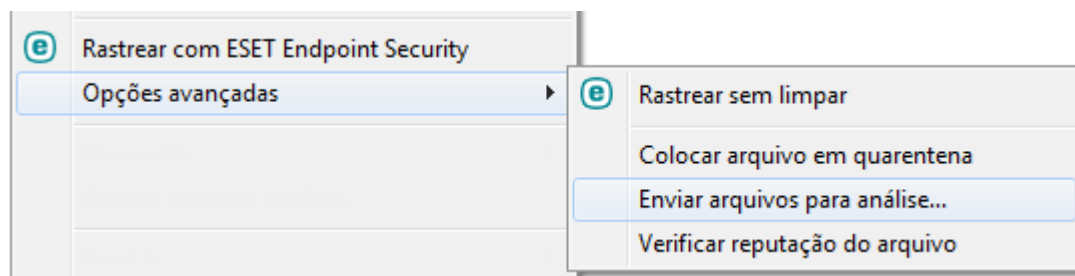
Sobre - Fornece informações do sistema, detalhes sobre a versão instalada do ESET Endpoint Security e os componentes do programa instalados, bem como a data de expiração de sua licença. Informações sobre seu sistema operacional e recursos do sistema podem ser encontradas no final da página.

Menu de contexto

O menu de contexto é exibido após um clique com o botão direito do mouse em um objeto (arquivo). O menu relaciona todas as ações que você pode realizar em um objeto.

É possível integrar os elementos de controle do ESET Endpoint Security no menu de contexto. A opção de configuração está disponível para essa funcionalidade na árvore Configuração avançada em **Interface do usuário > Elementos da interface do usuário**.

Integrar ao menu de contexto - Integra os elementos de controle do ESET Endpoint Security no menu de contexto.



Ajuda e suporte

O ESET Endpoint Security contém ferramentas de solução de problemas e informações de suporte que o ajudarão a solucionar eventuais problemas.



Produto instalado

- **Sobre o ESET Endpoint Security** – Exibe informações sobre sua cópia do [ESET Endpoint Security](#).
- **[Solução de problemas do produto](#)** – clique neste link para encontrar soluções para os problemas mais frequentemente encontrados.
- **[Solução de problemas de licença](#)** – clique neste link para encontrar soluções para problemas com a ativação ou alteração de licença.
- **[Alterar licença](#)** - Clique para iniciar a janela de ativação e ativar seu produto.



Página de ajuda - Clique nesse link para iniciar as páginas de ajuda do ESET Endpoint Security.



[Suporte técnico](#)

- **Solicitar suporte** – se não encontrar a resposta para o seu problema, você pode usar o formulário no site da ESET para entrar em contato rapidamente com o departamento de Suporte técnico. Com base em suas configurações, a janela [enviar seus dados de configuração do sistema](#) será exibida antes de preencher o formulário da web.
- **Detalhes para Suporte técnico** – Quando solicitado, você pode copiar e enviar informações ao Suporte técnico ESET (como nome do produto, versão do produto, sistema operacional e tipo de processador).
- **ESET Log Collector** – Links para o artigo da [Base de conhecimento ESET](#), na qual você pode baixar o ESET Log Collector, aplicativo que coleta automaticamente informações e relatórios de um computador para ajudar a resolver problemas mais rapidamente. Para obter mais informações, consulte o [ESET Log Collector guia on-line do usuário](#).
- Ative o [Registro em relatório avançado](#) para criar relatórios avançados para todos os recursos disponíveis para ajudar os desenvolvedores a diagnosticarem e resolverem problemas. Detalhamento mínimo de registro em relatório definido para o nível Diagnóstico. O registro em relatório avançado será desativado automaticamente depois de duas horas, a menos que ele seja interrompido antes disso clicando em Parar registro em relatório avançado. Quando todos os relatórios são criados, a janela de notificação é exibida fornecendo acesso direto à pasta de diagnóstico com os relatórios criados.

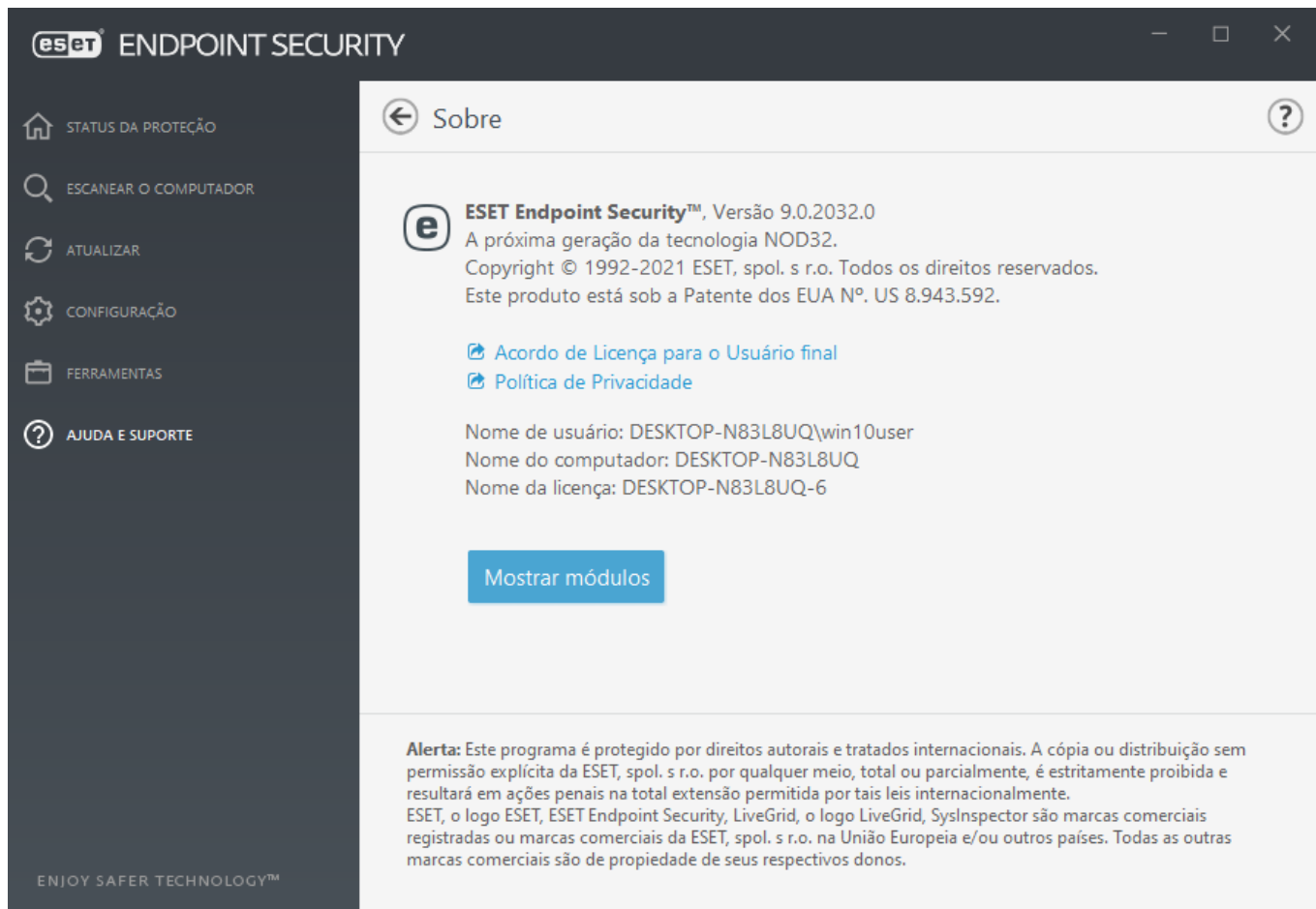


Base de conhecimento - A [Base de conhecimento da ESET](#) contém as respostas à maioria das perguntas mais frequentes e as soluções recomendadas para diversos problemas. A atualização regular feita pelos especialistas técnicos da ESET tornam a base de conhecimento a ferramenta mais poderosa para a solução de diversos problemas.

Sobre o ESET Endpoint Security

Esta janela fornece detalhes sobre a versão instalada do ESET Endpoint Security, seu sistema operacional e recursos do sistema.

Clique em **Mostrar módulos** para ver informações sobre a lista de módulos de programas instalados e suas versões. Você pode copiar informações sobre os módulos para a área de transferência clicando em **Copiar**. Isso pode ser útil durante a solução de problemas ou ao entrar em contato com o Suporte técnico.



Enviar dados de configuração do sistema

Para fornecer ajuda com a maior rapidez e precisão possíveis, a ESET solicita informações sobre a configuração do ESET Endpoint Security, informações detalhadas do sistema e processos em execução ([relatório do ESET SysInspector](#)) e dados do registro. A ESET usará estes dados apenas para fornecer assistência técnica ao cliente.

Quando enviar o formulário da web, seus dados de configuração do sistema serão enviados para a ESET. Selecione **Sempre enviar estas informações** se quiser lembrar desta ação para este processo. Para enviar o formulário sem mandar qualquer dado, clique em **Não enviar dados** e você pode entrar em contato com o Suporte técnico ESET usando o formulário de suporte on-line.

Esta configuração também pode ser feita em **Configuração avançada > Ferramentas > Diagnóstico > Suporte técnico**.

i Se você decidiu enviar dados do sistema é necessário preencher e enviar o formulário da web, caso contrário seu bilhete não será criado e os dados do seu sistema serão perdidos.

Suporte técnico

Entrar em contato com o Suporte técnico

Solicitar suporte – se não encontrar a resposta para o seu problema, você pode usar o formulário no site da ESET para entrar em contato rapidamente com o departamento de Suporte técnico da ESET. Com base em suas

configurações, a janela [enviar seus dados de configuração do sistema](#) será exibida antes de preencher o formulário da web.

Obter informações para o Suporte técnico

Detalhes para Suporte técnico – quando solicitado, você pode copiar e enviar informações ao Suporte técnico ESET (como os detalhes da licença, nome do produto, versão do produto, sistema operacional e informações do computador).

ESET Log Collector – Links para o artigo da [Base de conhecimento ESET](#), na qual você pode baixar o ESET Log Collector, aplicativo que coleta automaticamente informações e relatórios de um computador para ajudar a resolver problemas mais rapidamente. Para obter mais informações, consulte o [ESET Log Collector guia on-line do usuário](#).

Ative o [Registro em relatório avançado](#) para criar relatórios avançados para todos os recursos disponíveis para ajudar os desenvolvedores a diagnosticarem e resolverem problemas. Detalhamento mínimo de registro em relatório definido para o nível **Diagnóstico**. O registro em relatório avançado será desativado automaticamente depois de duas horas, a menos que ele seja interrompido antes disso clicando em **Parar registro em relatório avançado**. Quando todos os relatórios são criados, a janela de notificação é exibida fornecendo acesso direto à pasta de diagnóstico com os relatórios criados.

Notificações

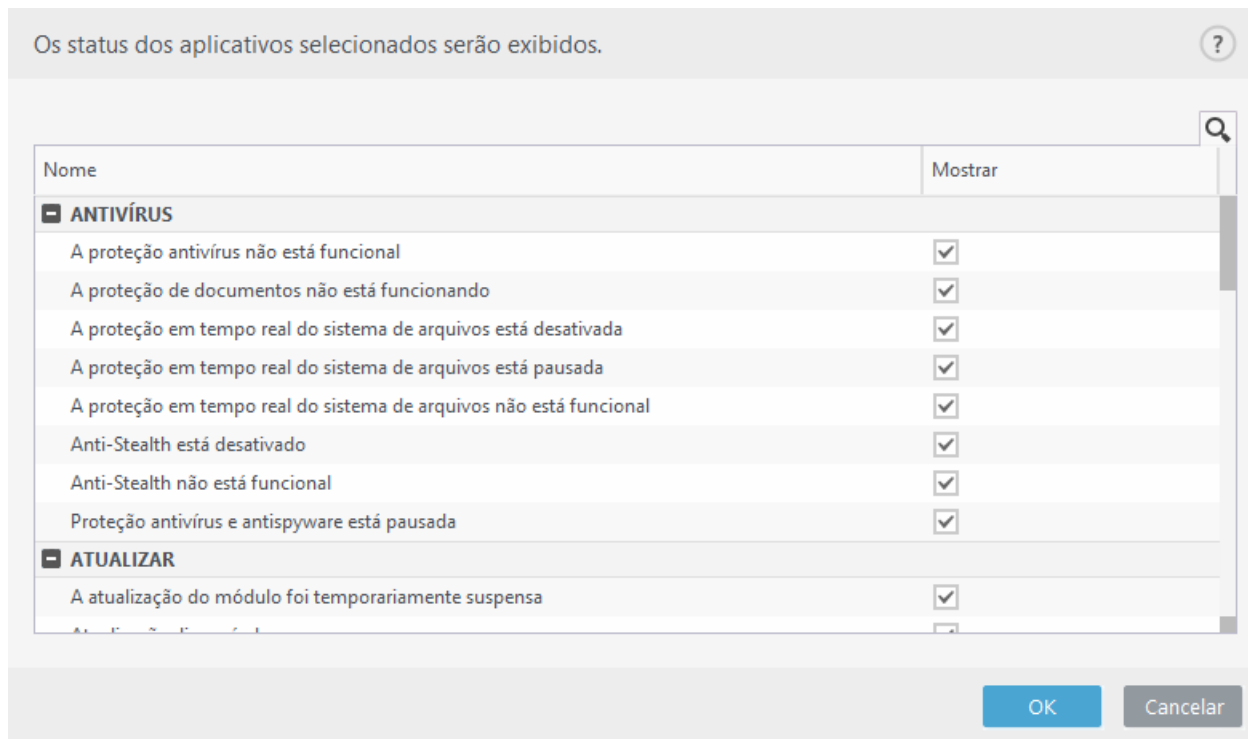
Para gerenciar as notificações ESET Endpoint Security, abra a **Configuração avançada (F5) > Notificações**. Você pode configurar os seguintes tipos de notificações:

- [Status de aplicativo](#) – clique em **Editar** para selecionar quais status de aplicativos serão exibidos na seção inicial da [janela principal do programa](#).
- [Notificações na área de trabalho](#) – pequenas janelas pop-up ao lado da barra de tarefas do sistema.
- [Personalização de notificações](#) – Adicione uma mensagem personalizada a, por exemplo, uma notificação na área de trabalho.
- [Alertas interativos](#) – janelas de alerta e caixas de mensagens que exigem interação do usuário.
- [Encaminhamento](#) (notificações por email) – Notificações por email são enviadas ao endereço de email especificado.

Status de aplicativo

Para configurar quais status de aplicativos serão exibidos (por exemplo, quando você pausar a Proteção antivírus e antispyware ou ativar o Modo gamer), abra a **Configuração avançada (F5) > Notificações** e clique em **Editar** para selecionar quais status de aplicativo serão exibidos na seção inicial da [janela principal do programa](#).

O status do aplicativo também será exibido se o produto não estiver ativado ou se sua licença tiver expirado. Essa configuração pode ser alterada através das [políticas ESET PROTECT](#).



Notificações na área de trabalho

A notificação na área de trabalho é representada por uma pequena janela pop-up ao lado da barra de tarefas do sistema. Por padrão, ela está configurada para ser exibida por 10 segundos e, depois, desaparecer lentamente. Essa é a maneira principal do ESET Endpoint Security comunicar-se com o usuário, com notificações sobre atualizações de produto bem-sucedidas, novos dispositivos conectados, tarefas de escaneamento de vírus concluídas ou novas ameaças encontradas.

Exibir notificações na área de trabalho – recomendamos manter essa opção ativada para que o produto possa informar quando um novo evento ocorrer.

Notificações na área de trabalho – clique em **Editar** para ativar ou desativar as [Notificações na área de trabalho](#) específicas.

Não exibir notificações ao executar aplicativos em tela cheia – suprime todas as notificações não interativas ao executar aplicativos em modo tela cheia.

Limite de tempo em segundos – define a duração de visibilidade da notificação. O valor deve estar entre 3 a 30 segundos.

Transparência – define a porcentagem de transparência da notificação. O intervalo possível é de 0 (sem transparência) a 80 (transparência muito alta).

Detalhamento mínimo de eventos para exibir – define o nível de gravidade de notificação inicial exibido. No menu suspenso, selecione uma das seguintes opções:

- **Diagnóstico** – Registra informações necessárias para ajustar o programa e todos os registros mencionados anteriormente.
- **Informativos** - Registra as mensagens informativas como eventos de rede fora do padrão, incluindo as mensagens de atualizações bem-sucedidas e todos os registros mencionados anteriormente.
- **Avisos** - Registra mensagens de erros críticos e de aviso (o Anti-Stealth não está sendo executado)

corretamente ou a atualização falhou).

- **Erros** - Erros (proteção de documentos não iniciada) e erros críticos serão registrados.
- **Crítico** - Registra somente os erros críticos como erro ao iniciar a proteção antivírus ou sistema infectado.

Em sistemas com vários usuários, exibir notificações na tela deste usuário – permite que as contas selecionadas recebam notificações na área de trabalho. Por exemplo, se você não usa a conta do Administrador, digite o nome completo da conta e as notificações na área de trabalho serão exibidas para a conta especificada. Apenas uma conta de usuário pode receber as notificações na área de trabalho.

Permitir que as notificações se concentrem na tela – as notificações vão se concentrar na tela e podem ser acessadas com Alt+Tab.

Janela de diálogo – notificações na área de trabalho

Para ajustar a visibilidade das notificações na área de trabalho (exibidas no canto inferior direito da tela), abra a **Configuração avançada (F5) > Notificações > Notificações na área de trabalho**. Clique em **Editar** ao lado de **Notificações na área de trabalho** e selecione a caixa de seleção adequada **Exibir na área de trabalho**.

i Se quiser configurar notificações de **Arquivo analisado** e **Arquivo não analisado** ao usar o ESET LiveGuard, a [Proteção proativa](#) deve ser configurada para **Bloquear a execução até o recebimento do resultado da análise**.

Personalização de notificações

Nesta janela você pode personalizar a mensagem usada nas notificações.

Mensagem de notificação padrão - Uma mensagem padrão a ser exibida no rodapé das notificações.


Detecções

Ativar **Não fechar notificações de malware automaticamente** para que as notificações de malware continuem na tela até que sejam fechadas manualmente.

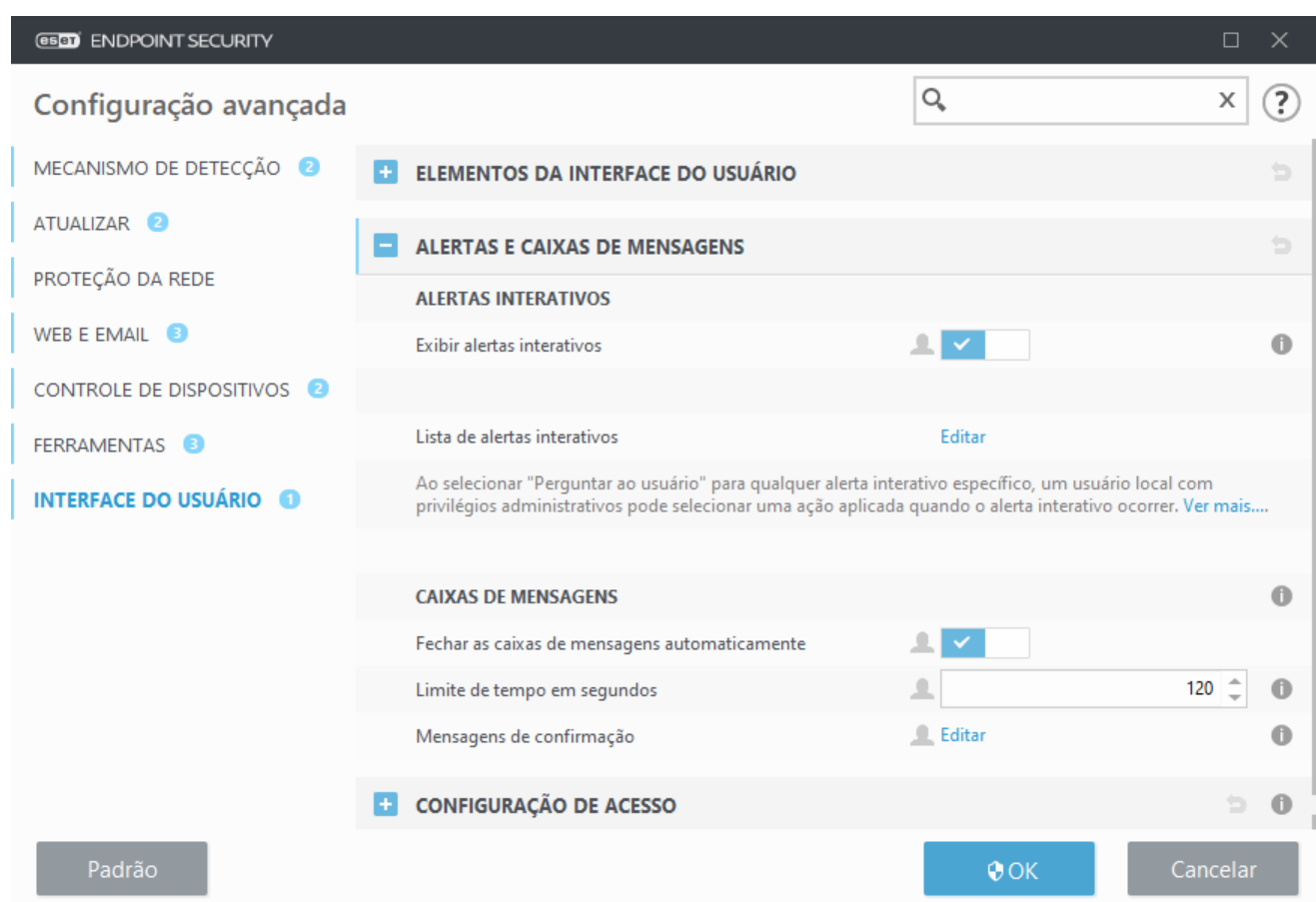
Desative **Usar mensagem padrão** e digite sua própria mensagem no campo **Mensagem de notificação de detecção** para usar uma mensagem de notificação personalizada.

Alertas interativos

Buscando informações sobre alertas e notificações comuns?

- [Ameaça encontrada](#)
- [O endereço foi bloqueado](#)
- [O produto não está ativado](#)
- [Atualização gratuita disponível](#)
-  As informações de atualização não são consistentes
- [Solução de problemas para a mensagem "Falha na atualização dos módulos"](#)
- ["Arquivo corrompido" ou "Falha ao renomear arquivo"](#)
- [Certificado de site revogado](#)
- [Ameaça na rede bloqueada](#)
- [Arquivo bloqueado devido a análise](#)

A seção **Alertas interativos** sob **Notificações** permite a você configurar como as detecções são tratadas pelo ESET Endpoint Security, quando é preciso que uma decisão seja feita por um usuário (por exemplo, sites de phishing em potencial).



Alertas interativos

As janelas de alertas interativos são exibidas se a detecção for encontrada ou se for necessária uma intervenção do usuário.

Exibir alertas interativos

- Para usuários não gerenciados, recomendamos que essa opção seja mantida em sua configuração padrão (ativado).
- Para usuários gerenciados, mantenha a configuração ativada e selecione uma ação pré-definida para usuários na [Lista de alertas interativos](#).

Desativar **Exibir alertas interativos** vai ocultar todas as janelas de alerta e diálogos no navegador. Uma ação padrão pré-definida será selecionada automaticamente (por exemplo, "site de phishing em potencial" será bloqueado).

Caixas de mensagens

Para fechar as janelas pop-up automaticamente após um certo período de tempo, selecione a opção **Fechar caixas de mensagens automaticamente**. Se não forem fechadas manualmente, as janelas de alertas serão fechadas automaticamente após o período de tempo especificado expirar.

Mensagens de confirmação - mostra a você uma [lista de mensagens de confirmação](#) que você pode selecionar para serem exibidas ou não.

Lista de alertas interativos

Esta seção delinea várias janelas de alerta interativo que o ESET Endpoint Security vai exibir antes de qualquer ação ser realizada.

Para ajustar o comportamento para alertas interativos configuráveis, vá para a **Notificações > Alertas interativos** da Árvore de configuração avançada do ESET Endpoint Security e clique em **Editar**.

i Útil para ambientes gerenciados onde o administrador pode desmarcar **Perguntar ao usuário** em todos os lugares e selecionar uma ação pré-definida aplicada quando janelas de alerta interativo são exibidas. Veja também os [status de aplicativo](#) no produto.

Selecionar qual alerta interativo será exibido

Nome	Perguntar ao usuário	Ação aplicada quando não exibida
ALERTAS DO NAVEGADOR DA WEB		
Conteúdo potencialmente indesejado encontrado	<input checked="" type="checkbox"/>	Bloquear
Site bloqueado devido a phishing	<input checked="" type="checkbox"/>	Bloquear
ATUALIZAÇÃO		
Atualização gratuita disponível	<input checked="" type="checkbox"/>	Nenhum
COMPUTADOR		
Reiniciar computador (obrigatório)	<input checked="" type="checkbox"/>	Nenhum
Reiniciar computador (recomendado)	<input checked="" type="checkbox"/>	Nenhum
MÍDIA REMOVÍVEL		

OK Cancelar

Confira outras seções de ajuda para referências a janelas de alerta interativo específicas:

Mídia removível

- [Novo dispositivo detectado](#)

Navegador protegido

- [Permitir continuar em um navegador padrão](#)

Proteção de rede

- [Acesso de rede bloqueado](#) é exibido quando a tarefa de cliente **Isolar computador da rede** da estação de trabalho do ESET PROTECT é acionada.
- [Comunicação de rede bloqueada](#)
- [Ameaça na rede bloqueada](#)

Alertas do navegador da web

- [Conteúdo potencialmente indesejado encontrado](#)
- [Site bloqueado devido a phishing](#)

Computador

A presença dos alertas a seguir vai fazer com que a interface do usuário fique laranja:

- [Reiniciar computador \(obrigatório\)](#)
- [Reiniciar computador \(recomendado\)](#)



Alertas interativos não contém janelas interativas do Mecanismo de detecção, HIPS ou Firewall, pois seu comportamento pode ser configurado individualmente no recurso específico.

Mensagens de confirmação

Para ajustar mensagens de confirmação navegue até **Interface do usuário > Alertar e caixas de mensagem > Mensagens de confirmação** da árvore de Configuração avançada ESET Endpoint Security e clique em **Editar**.

As mensagens selecionadas serão exibidas

☒ Exibir caixa de diálogo de confirmação de produto para clientes de email Outlook Express e Windows Mail

☒ Exibir caixa de diálogo de confirmação do produto para o cliente de email Outlook

☒ Exibir caixa de diálogo de confirmação do produto para o cliente de email Windows Live Mail

☒ Exibir notificações de resultado de processamento Antispam

☒ Exibir notificações de resultado de processamento Antispam para clientes de email

☒ Perguntar antes de deixar todas as ameaças encontradas sem limpar de uma janela de alerta

☐ Perguntar antes de descartar configurações na Configuração avançada

☒ Perguntar antes de excluir objeto da Quarentena

☒ Perguntar antes de excluir os relatórios do ESET SysInspector

☒ Perguntar antes de excluir todos os relatórios do ESET SysInspector

☒ Perguntar antes de executar uma tarefa agendada na Agenda

OK

Cancelar

Esta janela de diálogo exibe mensagens de confirmação que o ESET Endpoint Security exibirá antes de qualquer ação ser realizada. Marque ou desmarque a caixa de seleção ao lado de cada mensagem de confirmação para permiti-la ou desativá-la.

Saiba mais sobre o recurso específico relacionado a mensagens de confirmação:

- [Perguntar antes de excluir relatórios do ESET SysInspector](#)
- [Perguntar antes de excluir todos os relatórios do ESET SysInspector](#)
- [Perguntar antes de excluir objeto da Quarentena](#)
- Perguntar antes de descartar configurações na Configuração avançada
- [Perguntar antes de deixar todas as ameaças encontradas sem limpar de uma janela de alerta](#)
- [Perguntar antes de remover um registro de um relatório](#)
- [Perguntar antes de remover uma tarefa agendada na Agenda](#)
- [Perguntar antes de remover todos os registros de relatórios](#)
- [Perguntar antes de redefinir as estatísticas](#)
- [Perguntar antes de restaurar objetos da quarentena](#)
- [Perguntar antes de restaurar objetos da quarentena e de excluí-los do escaneamento](#)
- [Perguntar antes de executar uma tarefa agendada na Agenda](#)
- [Exibir notificações de resultado de processamento Antispam](#)
- [Exibir notificações de resultado de processamento Antispam para clientes de email](#)
- [Exibir caixa de diálogo de confirmação de produto para clientes de email Outlook Express e Windows Mail](#)
- [Exibir caixa de diálogo de confirmação do produto para o cliente de email Windows Live Mail](#)
- [Exibir caixa de diálogos de confirmação do produto para o cliente de email Outlook](#)

Erro de conflito de configurações avançadas

Esse erro pode acontecer se algum componente (por exemplo HIPS ou Firewall) e o usuário cria as regras no modo interativo ou de aprendizagem ao mesmo tempo.



Recomendamos alterar o modo de filtragem para o **Modo automático** padrão se quiser criar suas próprias regras. Leia mais sobre [Modo de aprendizagem do ESET Firewall](#). Leia mais sobre [HIPS e modos de filtragem HIPS](#).

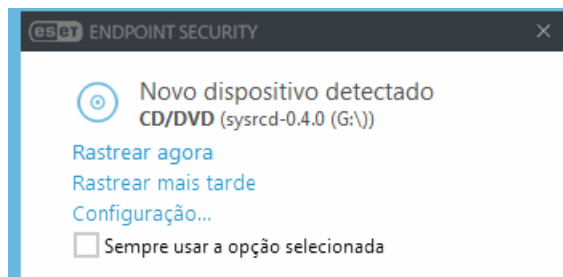
Permitir continuar em um navegador padrão

Um alerta interativo específico é usado apenas quando há um erro ao iniciar o Navegador protegido adequadamente.

Mídia removível

O ESET Endpoint Security fornece escaneamento automático de mídia removível (CD/DVD/USB/...) quando ela é inserida em um computador. Isso pode ser útil se a intenção do administrador do computador for evitar que os usuários usem uma mídia removível com conteúdo não solicitado.

Quando uma mídia removível for inserida e **Mostrar opções de escaneamento** estiver configurado em ESET Endpoint Security, a caixa de diálogo a seguir será exibida:



Opções para esta caixa de diálogo:

- **Rastrear agora** - Isto vai acionar o rastreamento da mídia removível.
- **Não escanear** – nenhuma ação será realizada.

Além disso, o ESET Endpoint Security conta com a funcionalidade de Controle de dispositivos, onde você pode definir regras para dispositivos externos em um determinado computador. Acesse a seção [Controle de dispositivos](#) para obter mais detalhes sobre o controle de dispositivos.

Para acessar as configurações de escaneamento de mídia removível, abra Configuração avançada (F5) > **Interface do usuário** > **Alertas e caixas de mensagens** > **Alertas interativos** > **Lista de alertas interativos** > **Editar** > **Novo dispositivo detectado**.

Se **Perguntar ao usuário** não estiver selecionado, escolha a ação a realizar ao inserir uma mídia removível em um computador:

- **Não escanear** – Nenhuma ação será executada e a janela **Novo dispositivo detectado** não será aberta.
- **Escaneamento automático de dispositivo** – Um escaneamento do computador do dispositivo de mídia removível inserido será executado.
- **Escaneamento forçado do dispositivo** – um escaneamento do computador do dispositivo de mídia removível inserido será executado e não pode ser cancelado.
- **Mostrar opções de escaneamento** – Abre a seção de configuração de **Alertas interativos**.

Requer reinicialização

Se as máquinas endpoint estiverem recebendo o alerta vermelho "Requer reinicialização", você pode desativar a exibição dos alertas.

Para desativar o alerta "Requer reinicialização" ou "Recomenda-se reiniciar", siga as etapas abaixo:

1. Pressione a tecla **F5** para acessar a Configuração avançada e abra a seção **Alertas e caixas de mensagens**.
2. Clique em **Editar** ao lado da **Lista de alertas interativos**. Na seção **Computador**, desmarque as caixas de marcação ao lado de **Reiniciar computador (obrigatório)** e **Reiniciar computador (recomendado)**.

Select which interactive alert will be displayed

Name	Ask user	Action applied when not displayed
+ Removable media		
+ Network protection		
+ Web browser alerts		
- Computer		
Restart computer (required)	<input type="checkbox"/>	None
Restart computer (recommended)	<input type="checkbox"/>	None

OK Cancel

3. Clique em **OK** para salvar suas alterações em ambas as janelas abertas.
4. Os alertas não aparecerão mais na máquina do endpoint.
5. (opcional) Para desativar o status de aplicativo na janela principal do programa do ESET Endpoint Security, em [Janela do programa principal](#) desmarque as caixas de marcação ao lado de **Requer reinicialização do computador** e **Recomenda-se reiniciar o computador**.

Selected application statuses will be displayed

Name	Show
- Device control	
Device control is not fully functional	<input checked="" type="checkbox"/>
Device control is paused	<input checked="" type="checkbox"/>
- GENERAL	
Computer restart recommended	<input type="checkbox"/>
Computer restart required	<input type="checkbox"/>
ESET LiveGrid® is disabled	<input checked="" type="checkbox"/>
ESET LiveGrid® is not accessible	<input checked="" type="checkbox"/>
Policy override active	<input checked="" type="checkbox"/>
Presentation mode is enabled	<input checked="" type="checkbox"/>
Settings password has to be updated	<input checked="" type="checkbox"/>
Windows updates available	<input checked="" type="checkbox"/>

OK Cancel

Recomenda-se reiniciar

Se as máquinas endpoint estiverem recebendo o alerta amarelo "Recomenda-se reiniciar", você pode desativar a exibição dos alertas.

Para desativar o alerta "Requer reinicialização" ou "Recomenda-se reiniciar", siga as etapas abaixo:

1. Pressione a tecla **F5** para acessar a Configuração avançada e abra a seção **Alertas e caixas de mensagens**.
2. Clique em **Editar** ao lado da **Lista de alertas interativos**. Na seção **Computador**, desmarque as caixas de marcação ao lado de **Reiniciar computador (obrigatório)** e **Reiniciar computador (recomendado)**.

Select which interactive alert will be displayed ?

Name	Ask user	Action applied when not displayed
Removable media		
Network protection		
Web browser alerts		
Computer		
Restart computer (required)	<input type="checkbox"/>	None
Restart computer (recommended)	<input type="checkbox"/>	None

OK Cancel

3. Clique em **OK** para salvar suas alterações em ambas as janelas abertas.
4. Os alertas não aparecerão mais na máquina do endpoint.
5. (opcional) Para desativar o status de aplicativo na janela principal do programa do ESET Endpoint Security, em [Janela do programa principal](#) desmarque as caixas de marcação ao lado de **Requer reinicialização do computador** e **Recomenda-se reiniciar o computador**.

Selected application statuses will be displayed ?

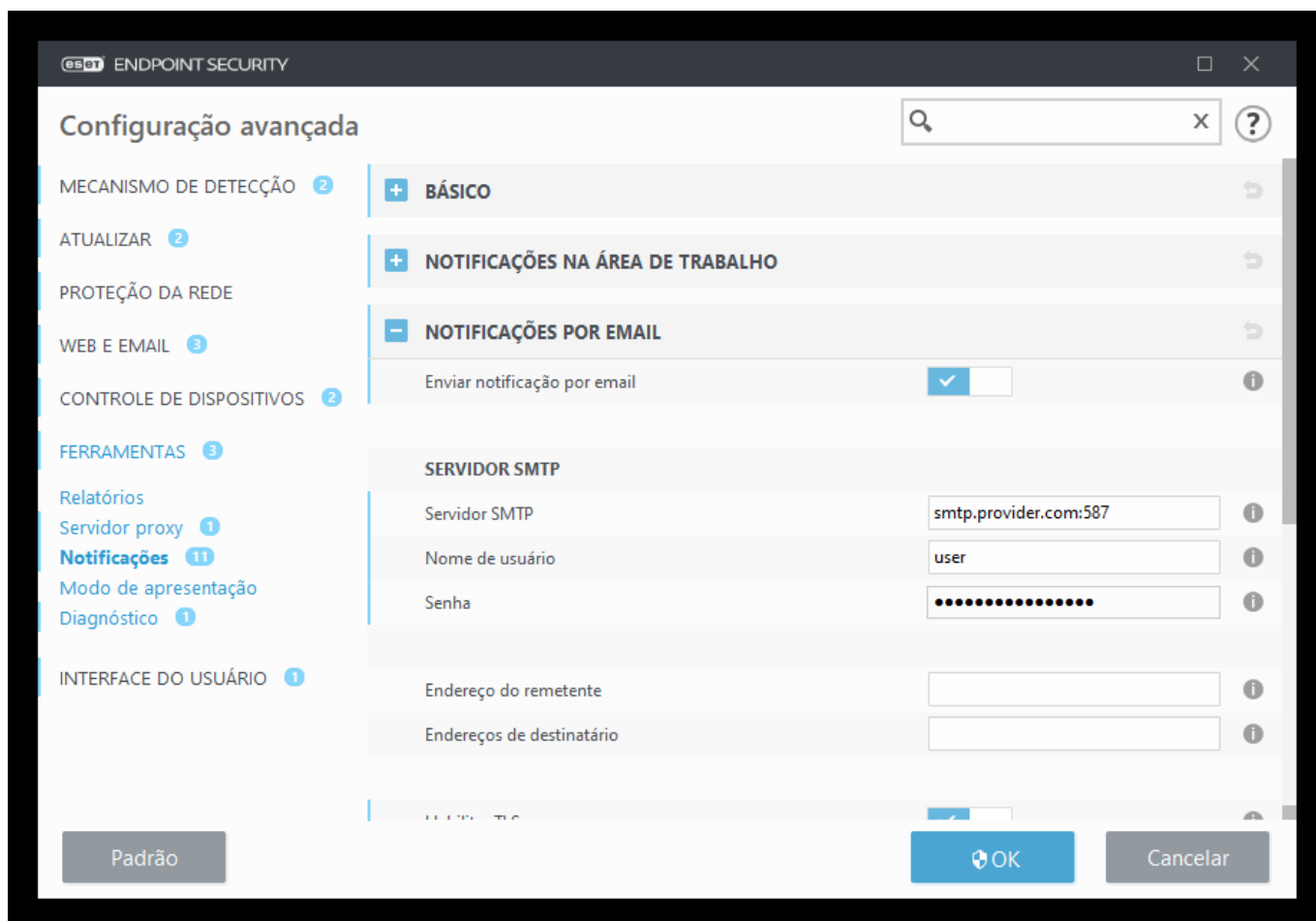
Name	Show
Device control	
Device control is not fully functional	<input checked="" type="checkbox"/>
Device control is paused	<input checked="" type="checkbox"/>
GENERAL	
Computer restart recommended	<input type="checkbox"/>
Computer restart required	<input type="checkbox"/>
ESET LiveGrid® is disabled	<input checked="" type="checkbox"/>
ESET LiveGrid® is not accessible	<input checked="" type="checkbox"/>
Policy override active	<input checked="" type="checkbox"/>
Presentation mode is enabled	<input checked="" type="checkbox"/>
Settings password has to be updated	<input checked="" type="checkbox"/>
Windows updates available	<input checked="" type="checkbox"/>

OK Cancel

Encaminhamento

O ESET Endpoint Security pode enviar e-mails de notificação automaticamente se um evento com o nível de detalhamento selecionado ocorrer. Na seção **Configuração avançada > Notificações > Encaminhamento > Encaminhar para e-mail**, ative **Encaminhar notificações por e-mail** para ativar as notificações por e-mail.

Notificações encaminhadas – selecione quais notificações na área de trabalho são encaminhadas para o e-mail.



Servidor SMTP

Servidor SMTP - O servidor SMTP usado para o envio de notificações (por exemplo *smtp.provider.com:587*, a porta predefinida é 25).

i Os servidores SMTP com criptografia TLS são compatíveis com o ESET Endpoint Security.

Nome de usuário e senha - Se o servidor SMTP exigir autenticação, esses campos devem ser preenchidos com nome de usuário e senha válidos para conceder acesso ao servidor SMTP.

Endereço do remetente - Esse campo especifica o endereço do remetente que será exibido no cabeçalho dos emails de notificação.

Endereços dos destinatários - Esse campo especifica o endereço do destinatário que será exibido no cabeçalho dos emails de notificação. Use um ponto e vírgula “;” para separar vários endereços de email.

Ativar TLS - Ativa o envio de mensagens de alerta e notificação compatíveis com a criptografia TLS.

Configurações de email

No menu suspenso **Detalhamento mínimo de notificações**, é possível selecionar o nível de gravidade inicial das notificações a serem enviadas.

- **Diagnóstico** – Registra informações necessárias para ajustar o programa e todos os registros mencionados anteriormente.
- **Informativos** - Registra as mensagens informativas como eventos de rede fora do padrão, incluindo as mensagens de atualizações bem-sucedidas e todos os registros mencionados anteriormente.
- **Avisos** - Registra mensagens de erros críticos e de aviso (o Anti-Stealth não está sendo executado corretamente ou a atualização falhou).
- **Erros** - Erros (proteção de documentos não iniciada) e erros críticos serão registrados.
- **Crítico** - Registra somente os erros críticos como erro ao iniciar a proteção antivírus ou sistema infectado.

Enviar cada notificação em um email separado - Quando ativado, o destinatário receberá um novo email para cada notificação individual. Isso pode resultar em um grande número de emails recebidos em um curto período de tempo.

Intervalo depois do qual cada novo email de notificação será enviado (min) - Intervalo em minutos depois do qual cada nova notificação será enviada por email. Se configurar este valor como 0, as notificações serão enviadas imediatamente.

Formato de mensagem

As comunicações entre o programa e um usuário remoto ou administrador do sistema são feitas por meio de e-mails ou mensagens de rede local (usando o serviço de mensagens do Windows). O formato padrão das mensagens de alerta e notificações será o ideal para a maioria das situações. Em algumas circunstâncias, você pode precisar alterar o formato de mensagens de evento.

Formato de mensagens de eventos - O formato de mensagens de eventos que são exibidas em computadores remotos.

Formato das mensagens de aviso de ameaça - Mensagens de alerta de ameaça e notificação têm um formato padrão predefinido. Não aconselhamos alterar esse formato. No entanto, em algumas circunstâncias (por exemplo, se você tiver um sistema de processamento de email automatizado), você pode precisar alterar o formato da mensagem.

Conjunto de caracteres – Converte uma mensagem de e-mail para a codificação de caracteres ANSI com base nas configurações regionais do Windows (por exemplo, windows-1250, Unicode (UTF-8), ACSII 7-bit ou japonês (ISO-2022-JP)). Como resultado, "á" será alterado para "a" e um símbolo desconhecido para "?".

Usar codificação Quoted-printable - A origem da mensagem de email será codificada para o formato Quoted-printable (QP) que usa caracteres ASCII e pode transmitir caracteres nacionais especiais por email no formato de 8 bits (áéíóú).

As palavras-chave (cadeias de caractere separadas por sinais %) são substituídas na mensagem pelas informações reais conforme especificadas. As palavras-chave disponíveis são:

- **%TimeStamp%** – Data e hora do evento
- **%Scanner%** – Módulo relacionado
- **%ComputerName%** – Nome do computador no qual o alerta ocorreu
- **%ProgramName%** – Programa que gerou o alerta
- **%InfectedObject%** – Nome do arquivo e mensagem infectados etc

- **%VirusName%** – Identificação da infecção
- **%Action%** - Ação realizada sobre a infiltração
- **%ErrorDescription%** - Descrição de um evento não vírus

As palavras-chave **%InfectedObject%** e **%VirusName%** são usadas somente em mensagens de alerta de ameaça, enquanto **%ErrorDescription%** é usada somente em mensagens de evento.

Gerenciador de perfil

O gerenciador de perfil é usado em duas seções no ESET Endpoint Security - **Rastreamento sob demanda do computador** e **Atualizar**.

Escaneamento sob demanda do computador

Os seus parâmetros de rastreamento favoritos podem ser salvos para rastreamento futuro. Recomendamos a criação de um perfil diferente (com diversos alvos de rastreamento, métodos de rastreamento e outros parâmetros) para cada rastreamento utilizado regularmente.

Para criar um novo perfil, abra a janela Configuração avançada (F5) e clique em **Antivírus > Rastreamento sob demanda do computador** e em **Editar** ao lado de **Lista de perfis**. O menu suspenso **Atualizar perfil** que lista os perfis de rastreamento existentes. Para ajudar a criar um perfil de rastreamento que atenda às suas necessidades, consulte a seção [Configuração de parâmetros do mecanismo ThreatSense](#) para obter uma descrição de cada parâmetro da configuração de rastreamento.

i Suponhamos que você deseje criar seu próprio perfil de rastreamento e que a configuração **Rastrear seu computador** seja parcialmente adequada. Porém, você não deseja rastrear [empacotadores em tempo real](#) nem [aplicativos potencialmente inseguros](#) e também deseja aplicar a **Limpeza rígida**. Digite o nome do novo perfil na janela **Gerenciador de perfil** e clique em **Adicionar**. Selecione seu novo perfil do menu suspenso **Perfil selecionado** e ajuste os parâmetros restantes para atender aos seus requisitos e clique em **OK** para salvar seu novo perfil.

Atualizar

O editor de perfil na seção de configuração da Atualização permite que os usuários criem novos perfis de atualização. Crie e use os seus próprios perfis personalizados (isto é, outros que não sejam o padrão **Meu perfil**) somente se o seu computador usar diversos modos de conexão com os servidores de atualização.

Por exemplo, um laptop que normalmente se conecta ao servidor local (Mirror) na rede local, mas faz os downloads das atualizações diretamente dos servidores de atualização da ESET quando está desconectado da rede local (em viagem de negócios, por exemplo) pode usar dois perfis: o primeiro para conectar ao servidor local; o segundo para conectar aos servidores da ESET. Quando esses perfis estiverem configurados, navegue até **Ferramentas > Agenda** e edite os parâmetros da tarefa de atualização. Designe um perfil como primário e outro como secundário.

Perfil de atualização - O perfil de atualização atualmente usado. Para mudar, escolha um perfil no menu suspenso.

Lista de perfis - Crie novos perfis de atualização ou remova os existentes.

Atalhos do teclado

Para uma melhor navegação no ESET Endpoint Security, os seguintes atalhos de teclado podem ser utilizados:

Atalhos do teclado	Ação realizada
F1	abre as páginas da Ajuda
F5	abre a Configuração avançada
Up/Down	permite a navegação no produto por itens
TAB	move o cursor em uma janela
Esc	fecha a janela da caixa de diálogo ativa
Ctrl+U	exibe informações sobre a licença ESET e seu computador (detalhes para o Atendimento ao cliente)
Ctrl+R	redefine a janela do produto para seu tamanho e posição padrão na tela

Diagnóstico

O diagnóstico fornece despejos de memória de aplicativos dos processos da ESET (por exemplo, ekrn). Se um aplicativo falhar, um despejo será gerado. Isso poderá ajudar os desenvolvedores a depurar e a corrigir vários problemas da ESET Endpoint Security.

Clique no menu suspenso ao lado de **Tipo de despejo** e selecione uma das três opções disponíveis:

- Selecione **Desativar** para desativar esse recurso.
- **Mini** (padrão) - Registra o menor conjunto de informações úteis que podem ajudar a identificar porque o aplicativo parou inesperadamente. Este tipo de arquivo de despejo pode ser útil quando o espaço é limitado, no entanto, devido às informações limitadas incluídas, os erros que não foram causados diretamente pelo encadeamento que estava em execução no momento em que o problema ocorreu, podem não ser descobertos por uma análise desse arquivo.
- **Completo** - Registra todo o conteúdo da memória do sistema quando o aplicativo para inesperadamente. Um despejo de memória completo pode conter dados de processos que estavam em execução quando o despejo de memória foi coletado.

Diretório de destino - Diretório no qual o despejo durante a falha será gerado.

Abrir pasta de diagnóstico - Clique em **Abrir** para abrir esse diretório em uma nova janela do *Windows explorer*.

Criar liberação de diagnóstico - Clique em **Criar** para criar arquivos de liberação de diagnóstico no **Diretório de destino**.

Registro em relatório avançado

Ativar registro avançado do mecanismo Antispam – Registra todos os eventos que ocorrem durante o escaneamento do antispam. Isto pode ajudar os desenvolvedores a diagnosticar e solucionar problemas relacionados ao mecanismo do ESET Antispam.

Ativar registro em relatório avançado do escaneamento do computador – registra todos os eventos que acontecem ao escanear arquivos e pastas ao Escanear o computador ou na Proteção em tempo real do sistema

de arquivos.

Ativar registro avançado do Controle de dispositivos – Registra todos os eventos que ocorrem no Controle de dispositivos. Isto pode ajudar os desenvolvedores a diagnosticar e solucionar problemas relacionados ao Controle de dispositivos.

Ativar registro em relatório avançado do Direct Cloud – Registra toda a comunicação do produto entre o produto e os servidores Direct Cloud.

Habilitar Registro em relatório avançado da proteção de documento – Registra todos os eventos que ocorrem na Proteção de documentos para permitir o diagnóstico e a resolução de problemas.

Ativar registro em relatório avançado de Kernel – Registra todos os eventos que ocorrem no serviço de kernel da ESET (ekrn) para permitir o diagnóstico e a resolução de problemas (disponível na versão 7.2 e versões posteriores).

Ativar registro em relatório avançado do mecanismo de Licenciamento – Registra toda a comunicação do produto com a ativação da ESET e os servidores ESET Business Account.

Ativar o escaneamento de memória – Registre todos os eventos que ajudarão os desenvolvedores a diagnosticar vazamentos de memória.

Ativar registro em relatório avançado de proteção de rede - Registra todos os dados de rede que passam pelo firewall no formato PCAP para ajudar os desenvolvedores a diagnosticar e solucionar problemas relacionados ao firewall.

Ativar o registro em relatório avançado do Sistema operacional – Informações adicionais sobre o Sistema operacional como os processos em execução, atividade de CPU e operações de disco serão coletadas. Isto pode ajudar os desenvolvedores a diagnosticar e solucionar problemas relacionados ao produto ESET sendo executado em seu sistema operacional.

Ativar registro em relatório avançado de Filtragem de protocolo - Registra todos os dados passando pelo mecanismo de Filtragem de protocolo em formato PCAP para ajudar os desenvolvedores a diagnosticar e solucionar problemas relacionados a Filtragem de protocolo.

Ativar registro em relatório avançado de mensagens por push – Registra todos os eventos que ocorrem durante o envio de mensagens para permitir diagnóstico e solução de problemas.

Ativar o registro em relatório avançado da Proteção em tempo real do sistema de arquivos – registrar todos os eventos que ocorrem na Proteção em tempo real do sistema de arquivos para permitir o diagnóstico e a resolução de problemas.

Ativar o registro em relatório avançado do Navegador protegido – Registre todos os eventos que ocorrem no Navegador protegido para permitir o diagnóstico e a resolução de problemas.

Ativar registro avançado do Mecanismo de atualização – Registra todos os eventos que acontecem durante o processo de atualização. Isto pode ajudar os desenvolvedores a diagnosticarem e solucionarem problemas relacionados ao mecanismo de Atualização.

Ativar registro avançado do Controle da web – Registra todos os eventos que ocorrem no Controle de web. Isso pode ajudar os desenvolvedores a diagnosticar e solucionar problemas relacionados ao Controle de web.

Localização dos arquivos de relatório

C:\ProgramData\ESET\ESET Endpoint Security\Diagnostics

Análise da linha de comandos

O módulo antivírus do ESET Endpoint Security pode ser iniciado pela linha de comando – manualmente (com o comando "ecls") ou com um arquivo em lotes ("bat").

Uso do escaneador de linha de comando da ESET:

```
ecls [OPTIONS..] FILES..
```

Os seguintes parâmetros e chaves podem ser utilizados ao executar o scanner sob demanda na linha de comando:

Opções

/base-dir=PASTA	carregar módulos da PASTA
/quar-dir=PASTA	PASTA de quarentena
/exclude=MÁSCARA	excluir arquivos que correspondem à MÁSCARA do rastreamento
/subdir	rastrear subpastas (padrão)
/no-subdir	não rastrear subpastas
/max-subdir-level=NÍVEL	subnível máximo de pastas dentro de pastas para rastrear
/symlink	seguir links simbólicos (padrão)
/no-symlink	ignorar links simbólicos
/ads	rastrear ADS (padrão)
/no-ads	não rastrear ADS
/log-file=ARQUIVO	registrar o relatório em ARQUIVO
/log-rewrite	substituir arquivo de saída (padrão - acrescentar)
/log-console	registrar saída para console (padrão)
/no-log-console	não registrar saída para console
/log-all	também registrar arquivos limpos
/no-log-all	não registrar arquivos limpos (padrão)
/auid	mostrar indicador de atividade
/auto	rastrear e limpar automaticamente todos os discos locais

Opções do scanner

/files	rastrear arquivos (padrão)
/no-files	não rastrear arquivos
/memory	rastrear memória
/boots	rastrear setores de inicialização
/no-boots	não rastrear setores de inicialização (padrão)

/arch	rastrear arquivos compactados (padrão)
/no-arch	não rastrear arquivos compactados
/max-obj-size=TAMANHO	rastrear apenas arquivos com menos de TAMANHO megabytes (padrão 0 = sem limite)
/max-arch-level=NÍVEL	subnível máximo de arquivos dentro de arquivos (arquivos aninhados) para rastrear
/scan-timeout=LIMITE	rastrear arquivos pelo LIMITE máximo de segundos
/max-arch-size=TAMANHO	rastrear apenas os arquivos em um arquivo compactado se eles tiverem menos de TAMANHO (padrão 0 = sem limite)
/max-sfx-size=TAMANHO	rastrear apenas os arquivos em um arquivo compactado de auto-extração se eles tiverem menos de TAMANHO megabytes (padrão 0 = sem limite)
/mail	rastrear arquivos de email (padrão)
/no-mail	não rastrear arquivos de email
/mailbox	rastrear caixas de correio (padrão)
/no-mailbox	não rastrear caixas de correio
/sfx	rastrear arquivos compactados de auto-extração (padrão)
/no-sfx	não rastrear arquivos compactados de auto-extração
/rtp	rastrear empacotadores em tempo real (padrão)
/no-rtp	não rastrear empacotadores em tempo real
/unsafe	rastrear por aplicativos potencialmente inseguros
/no-unsafe	não rastrear por aplicativos potencialmente inseguros (padrão)
/unwanted	rastrear por aplicativos potencialmente indesejados
/no-unwanted	não rastrear por aplicativos potencialmente indesejados (padrão)
/suspicious	rastrear aplicativos suspeitos (padrão)
/no-suspicious	não rastrear aplicativos suspeitos
/pattern	usar assinaturas (padrão)
/no-pattern	não usar assinaturas
/heur	ativar heurística (padrão)
/no-heur	desativar heurística
/adv-heur	ativar heurística avançada (padrão)
/no-adv-heur	desativar heurística avançada
/ext-exclude=EXTENSÕES	excluir do escaneamento EXTENSÕES de arquivo delimitadas por dois pontos
/clean-mode=MODO	<p>utilizar MODO de limpeza para objetos infectados</p> <p>As opções disponíveis são:</p> <ul style="list-style-type: none"> • none (padrão) - não ocorrerá nenhuma limpeza automática. • standard - o ecls.exe tentará limpar ou excluir automaticamente os arquivos infectados. • strict (rígida) - o ecls.exe tentará limpar ou excluir automaticamente todos os arquivos infectados sem intervenção do usuário (você não será avisado antes de os arquivos serem excluídos). • rigorous (rigorosa) - o ecls.exe excluirá arquivos sem tentar limpá-los, independentemente de quais arquivos sejam. • delete (excluir) - o ecls.exe excluirá arquivos sem tentar limpá-los, mas não excluirá arquivos importantes, como arquivos do sistema Windows.

/quarantine	copiar arquivos infectados para Quarentena (completa a ação realizada enquanto ocorre a limpeza)
/no-quarantine	não copiar arquivos infectados para Quarentena

Opções gerais

/help	mostrar ajuda e sair
/version	mostrar informações de versão e sair
/preserve-time	manter último registro de acesso

Códigos de saída

0	nenhuma ameaça encontrada
1	ameaça encontrada e removida
10	alguns arquivos não puderam ser rastreados (podem conter ameaças)
50	ameaça encontrada
100	erro

i Os códigos de saída maiores que 100 significam que o arquivo não foi rastreado e, portanto, pode estar infectado.

ESET CMD

Este é um recurso que permite comandos ecmd avançados. Isso permite a você exportar e importar configurações usando a linha de comando (ecmd.exe). Até agora era possível exportar e importar configurações apenas usando a [Interface gráfica do usuário](#). A configuração do ESET Endpoint Security pode ser exportada para um arquivo .xml.

Quando você ativa o ESET CMD, existem dois métodos de autorização disponíveis:

- **Nenhum** - sem autorização. Não recomendamos esse método porque ele permite importar qualquer configuração não assinada, o que é um risco em potencial.
- **Senha da configuração avançada** - uma senha é necessária para importar a configuração de um arquivo .xml, esse arquivo deve ser assinado (veja a assinatura do arquivo de configuração .xml mais abaixo). A senha especificada em [Configuração de acesso](#) deve ser fornecida antes de ser possível importar a nova configuração. Se você não tiver a configuração de acesso ativada, a senha não combina ou o arquivo de configuração .xml não está assinado, a configuração não será importada.

Assim que o ESET CMD estiver ativado, você pode usar a linha de comando para exportar ou importar as configurações do ESET Endpoint Security. Isso pode ser feito manualmente ou você pode criar um script para a automação.



Para usar comandos ecmd avançados, será preciso que eles sejam executados com privilégios de administrador, ou abra o Prompt de Comando do Windows (cmd) usando **Executar como administrador**. Caso contrário, você terá a mensagem **Error executing command**. Além disso, ao exportar a configuração, a pasta de destino deve existir. O comando de exportação ainda funciona quando a configuração do ESET CMD está desligada.

i Comandos `ecmd` avançados só podem ser executados localmente. A pausa de comandos `ecmd` só pode ser realizada através da tarefa de cliente **Executar comando** usando ESET PROTECT.

Comando de exportar configurações:
`ecmd /getcfg c:\config\settings.xml`

Comando importar configurações:
`ecmd /setcfg c:\config\settings.xml`

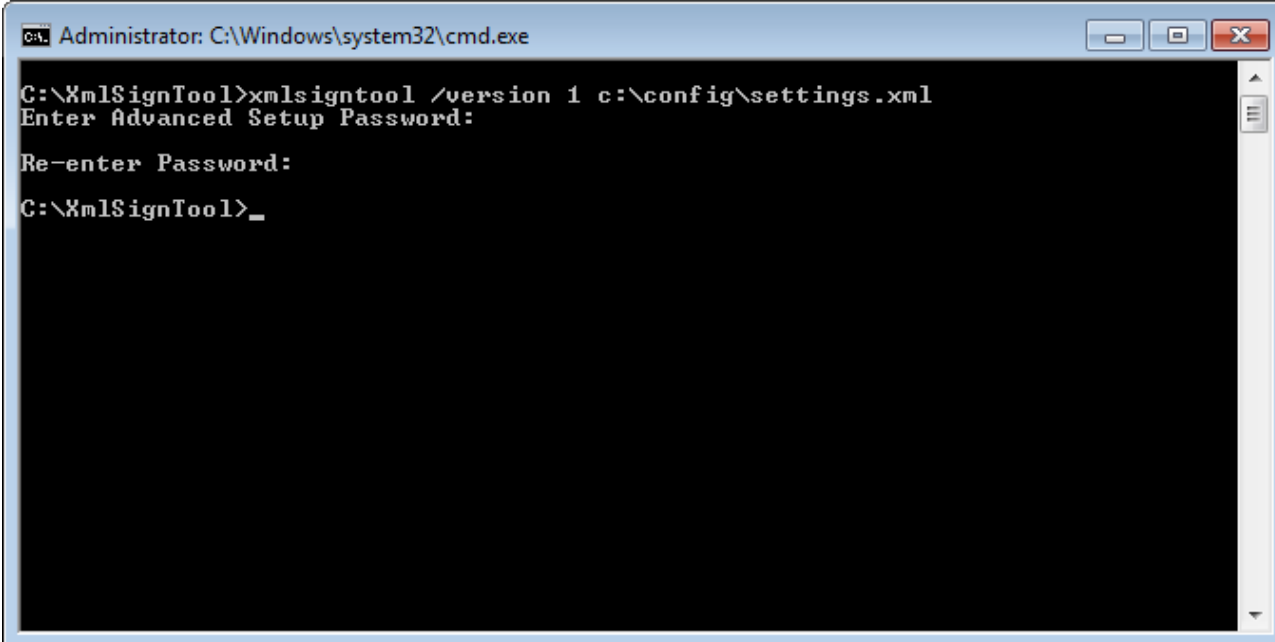
Assinando um arquivo de configuração `.xml`:

1. Faça o download do executável [XmlSignTool](#).
2. Abra o Prompt de Comando do Windows (`cmd`) usando **Executar como administrador**.
3. Navegue até a localização salva do `xmlsigntool.exe`
4. Execute um comando para assinar o arquivo de configuração `.xml`, uso: `xmlsigntool /version 1|2 <xml_file_path>`


! O valor do parâmetro `/version` depende da sua versão do ESET Endpoint Security. Use o `/version 2` para versões 7 e posteriores.

5. Digite e digite novamente a senha da [Configuração avançada](#) quando solicitado pelo XmlSignTool. Seu arquivo de configuração `.xml` agora está assinado e pode ser usado para importar outra instância do ESET Endpoint Security com o ESET CMD usando o método de autorização de senha.

Assinar o comando de arquivo de configuração exportado:
`xmlsigntool /version 2 c:\config\settings.xml`



i Se sua senha da [Configuração de acesso](#) mudar e você quiser importar a configuração que foi assinada anteriormente com uma senha antiga, você precisa assinar o arquivo de configuração `.xml` novamente usando sua senha atual. Isso permite a você usar o arquivo de configuração antigo sem precisar exportá-lo para outra máquina executando o ESET Endpoint Security antes da importação.

 Ativar o ESET CMD sem uma autorização não é recomendado, já que isso vai permitir a importação de qualquer configuração não assinada. Defina a senha em **Configuração avançada > Interface do usuário > Configuração de acesso** para impedir a modificação não autorizada por usuários.

Lista de comandos ecmd

Recursos de segurança individuais podem ser ativados e desativados temporariamente com o comando Executar tarefa do cliente ESET PROTECT. Os comandos não substituem as configurações de política, e quaisquer configurações pausadas serão revertidas de volta ao seu estado original depois de o comando ter sido executado ou depois de uma reinicialização do dispositivo. Para usar esse recurso, especifique a linha de comando a ser executada no campo de mesmo nome.

Revise a lista de comandos para cada recurso de segurança abaixo:

Recurso de segurança	Pausar o comando temporariamente	Ativar comando
Proteção em tempo real do sistema de arquivos	ecmd /setfeature onaccess pause	ecmd /setfeature onaccess enable
Proteção de documentos	ecmd /setfeature document pause	ecmd /setfeature document enable
Controle de dispositivo	ecmd /setfeature devcontrol pause	ecmd /setfeature devcontrol enable
Modo de apresentação	ecmd /setfeature presentation pause	ecmd /setfeature presentation enable
Tecnologia Anti-Stealth	ecmd /setfeature antistealth pause	ecmd /setfeature antistealth enable
Firewall pessoal	ecmd /setfeature firewall pause	ecmd /setfeature firewall enable
Proteção contra ataque de rede (IDS)	ecmd /setfeature ids pause	ecmd /setfeature ids enable
Proteção contra botnet	ecmd /setfeature botnet pause	ecmd /setfeature botnet enable
Controle de Web	ecmd /setfeature webcontrol pause	ecmd /setfeature webcontrol enable
Proteção do acesso à Web	ecmd /setfeature webaccess pause	ecmd /setfeature webaccess enable
Proteção do cliente de email	ecmd /setfeature email pause	ecmd /setfeature email enable
Proteção antispam	ecmd /setfeature antispam pause	ecmd /setfeature antispam enable
Proteção antiphishing	ecmd /setfeature antiphishing pause	ecmd /setfeature antiphishing enable

Detecção em estado ocioso

As configurações de detecção em estado ocioso podem ser feitas em **Configuração avançada** em **Mecanismo de detecção > Escaneamento de malware > Escaneamento em estado ocioso > Detecção em estado ocioso**. Essas configurações especificam um acionador para o [Escaneamento em estado ocioso](#), quando:

- a proteção de tela estiver em execução,
- o computador estiver bloqueado,
- um usuário efetuar logoff.

Use as opções de cada estado para ativar ou desativar os diferentes acionadores de detecção de estado ocioso.

Importar e exportar configurações

Você pode importar ou exportar seu arquivo de configuração .xml personalizado do ESET Endpoint Security do menu **Configuração**.

A importação e a exportação dos arquivos de configuração serão úteis caso precise fazer backup da configuração atual do ESET Endpoint Security para que ela possa ser utilizada posteriormente. A opção de exportação de configurações também é conveniente para os usuários que desejam utilizar as suas configurações preferenciais em diversos sistemas. Os usuários podem importar facilmente um arquivo .xml para transferir essas configurações.

A importação de uma configuração é muito fácil. Na janela principal do programa, clique em **Configuração > Importar/exportar configurações** e selecione **Importar configurações**. Digite o nome do arquivo de configuração ou clique no botão ... para procurar o arquivo de configuração que deseja importar.

As etapas para exportar uma configuração são muito semelhantes. Na janela principal do programa, clique em **Configuração > Importar/exportar configurações**. Selecione a opção **Exportar configurações** e insira o nome de arquivo do arquivo de configuração (ou seja, *export.xml*). Utilize o navegador para selecionar um local no computador no qual deseja salvar o arquivo de configuração.



Você pode encontrar um erro ao exportar configurações se não tiver direitos suficientes para gravar o arquivo exportado no diretório especificado.

ESET ENDPOINT SECURITY

Importar e exportar configurações

A configuração atual pode ser salva em um arquivo XML e, quando necessário, poderá ser restaurada posteriormente.

☒ Importar configurações
☐ Exportar configurações

Caminho completo do arquivo com nome:
C:\Backup\settings.xml

Importar Fechar

Reverter todas as configurações para o padrão

Clique em **Padrão** na Configuração avançada (F5) para reverter todas as configurações do programa, para todos os módulos. Elas serão redefinidas para o status que teriam após uma nova instalação.

Veja também [Importar e exportar configurações](#).

Reverter todas as configurações na seção atual

Clique na seta curva ↶ para reverter todas as configurações na seção atual para as configurações padrão definidas pela ESET.

Observe que quaisquer alterações feitas serão perdidas depois que você clicar em **Reverter para padrão**.

Reverter conteúdo de tabelas - Quando essa opção for ativada, as regras, tarefas ou perfis adicionados manualmente ou automaticamente serão perdidos.

Veja também [Importar e exportar configurações](#).

Erro ao salvar a configuração

Essa mensagem de erro indica que as configurações não foram salvas corretamente devido a um erro.

Isso normalmente significa que o usuário que tentou modificar os parâmetros do programa:

- tem direitos de acesso insuficientes ou não tem os privilégios do sistema operacional necessários para modificar os arquivos de configuração e o registro do sistema.
> Para realizar as modificações desejadas, o administrador do sistema deve entrar.
- ativou recentemente o Modo de aprendizagem no HIPS ou Firewall e tentou fazer alterações na Configuração avançada.
> Para salvar a configuração e evitar o conflito de configurações, feche a Configuração avançada sem salvar e tente fazer as mudanças desejadas novamente.

O segundo caso mais comum pode ser que o programa não funciona mais devidamente, está corrompido e, portanto, precisa ser reinstalado.

Monitoramento e gerenciamento remoto

O Monitoramento e Gerenciamento Remoto (RMM) é o processo de supervisionar e controlar sistemas de software usando um agente instalado localmente que pode ser acessado por um prestador de serviço de gerenciamento.

ERMM – plugin da ESET para RMM

- A instalação padrão ESET Endpoint Security contém o arquivo `ermm.exe` localizado no aplicativo Endpoint dentro do diretório:
`C:\Program Files\ESET\ESET Security\ermm.exe`
- `ermm.exe` é um utilitário de linha de comando feito para facilitar o gerenciamento de produtos endpoint e comunicações com qualquer plugin RMM.
- O `ermm.exe` troca dados com o plugin RMM, que se comunica com o Agente RMM vinculado a um Servidor RMM. Por padrão, a ferramenta ESET RMM está desativada.

Recursos adicionais

- [Linha de comando ERM](#)
- [Lista de comandos ERM JSON](#)
- [Como ativar o Monitoramento e gerenciamento remoto ESET Endpoint Security](#)

Plugins ESET Direct Endpoint Management para soluções RMM de terceiros

O Servidor RMM está sendo executado como um serviço em um servidor de terceiros. Para mais informações veja os guias de usuário on-line do ESET Direct Endpoint Management a seguir:

- [Plugin do ESET Direct Endpoint Management para ConnectWise Automate](#)
- [Plugin do ESET Direct Endpoint Management para DattoRMM](#)
- [ESET Direct Endpoint Management para Solarwinds N-Central](#)
- [ESET Direct Endpoint Management para NinjaRMM](#)

Linha de comando ERM

Remote monitoring management is run using the command line interface. The default ESET Endpoint Security installation contains the file ermm.exe located in the Endpoint application within the directory *c:\Program Files\ESET\ESET Security*.

Run the Command Prompt (cmd.exe) as an Administrator and navigate to the mentioned path. (To open Command Prompt, press Windows button + R on your keyboard, type a cmd.exe into the Run window and press Enter.)

The command syntax is: `ermm context command [options]`

Also note that the log parameters are case sensitive.

```

C:\WINDOWS\system32\cmd.exe
C:\Program Files\ESET\ESET Security>ermm
Invalid arguments.

Usage: eRmm context command [options]

Contexts: get, start, set

Commands for specified contexts with options:

get: get information about products
  application-info: get information about application
  license-info: get information about license
  protection-status: get protection status
  logs: get logs: all, virlog, warnlog, scanlog ...
    -N [--name] arg=all (retrieve all logs) name of log to retrieve
    -S [--start-date] arg start time from which logs should be retrieved (YYYY-MM-DD [HH-mm-SS])
    -E [--end-date] arg end time until which logs should be retrieved (YYYY-MM-DD [HH-mm-SS])
  scan-info: get information about scan
    -I [--id] arg id of scan to retrieve
  configuration: get product configuration
    -F [--file] arg path where configuration file will be saved
    -O [--format] arg=json format of configuration: json, xml
  update-status: get information about update
  activation-status: get information about last activation

start: start task
  scan: Start on demand scan
    -P [--profile] arg scanning profile
    -T [--target] arg scan target
  activation: Start activation
    -K [--key] arg activation key
    -O [--offline] arg path to offline file
    -T [--token] arg activation token
  deactivation: start deactivation of product
  update: start update of product

set: set configuration to product
  configuration: set product configuration
    -V [--value] arg configuration data (encoded in base64)
    -F [--file] arg path to configuration xml file
    -P [--password] arg password for configuration

Application parameters:
  -H [--help] help
  -L [--log] log application
--debug display input json

Example: eRmm start scan --target C:\ -p "@Smart scan"

C:\Program Files\ESET\ESET Security>_

```

ermm.exe uses three basic contexts: Get, Start and Set. In the table below you can find examples of commands syntax. Click the link in the Command column to see the further options, parameters, and usage examples. After successful execution of command, the output part (result) will be displayed. To see an input part, add parameter --debug at the of the command.

Context	Command	Description
get	Get information about products	
	application-info	Get information about product
	license-info	Get information about license
	protection-status	Get protection status
	logs	Get logs
	scan-info	Get information about running scan
	configuration	Get product configuration
	update-status	Get information about update
	activation-status	Get information about last activation
start	Start task	
	scan	Start on demand scan

Context	Command	Description
	activation	Start activation of product
	deactivation	Start deactivation of product
	update	Start update of product
set		Set options for product
	configuration	Set configuration to product

In the output result of every command, the first information displayed is result ID. To understand better the result information, check the table of IDs below.

Error ID	Error	Description
0	Success	
1	Command node not present	"Command" node not present in input json
2	Command not supported	Particular command is not supported
3	General error executing the command	Error during execution of command
4	Task already running	Requested task is already running and has not been started
5	Invalid parameter for command	Bad user input
6	Command not executed because it's disabled	RMM isn't enabled in advanced settings or isn't started as an administrator

Lista de comandos ERMM JSON

- [get protection-status](#)
- [get application-info](#)
- [get license-info](#)
- [get logs](#)
- [get activation-status](#)
- [get scan-info](#)
- [get configuration](#)
- [get update-status](#)
- [start scan](#)
- [start activation](#)
- [start deactivation](#)
- [start update](#)
- [set configuration](#)

get protection-status

Get the list of application statuses and the global application status

Command line

```
ermm.exe get protection-status
```

Parameters

None

Example

call

```
{
  "command": "get_protection_status",
  "id": 1,
  "version": "1"
}
```

result

```
{
  "id": 1,
  "result": {
    "statuses": [{
      "id": "EkrrnNotActivated",
      "status": 2,
      "priority": 768,
      "description": "Product not activated"
    }],
    "status": 2,
    "description": "Security alert"
  },
  "error": null
}
```

get application-info

Get information about the installed application

Command line

```
ermm.exe get application-info
```

Parameters

None

Example

call

```
{
  "command": "get_application_info",
  "id": 1,
  "version": "1"
}
```

result

```

{
  "id":1,
  "result":{
    "description":"ESET Endpoint Antivirus",
    "version":"6.6.2018.0",
    "product":"eea",
    "lang_id":1033,
    "modules":[{
      "id":"SCANNER32",
      "description":"Detection engine",
      "version":"15117",
      "date":"2017-03-20"
    },{
      "id":"PEGASUS32",
      "description":"Rapid Response module",
      "version":"0734",
      "date":"2017-03-20"
    },{
      "id":"LOADER32",
      "description":"Update module",
      "version":"1009",
      "date":"2016-12-05"
    },{
      "id":"PERSEUS32",
      "description":"Antivirus and antispysware scanner module",
      "version":"1513",
      "date":"2017-03-06"
    },{
      "id":"ADVHEUR32",
      "description":"Advanced heuristics module",
      "version":"1176",
      "date":"2017-01-16"
    },{
      "id":"ARCHIVER32",
      "description":"Archive support module",
      "version":"1261",
      "date":"2017-02-22"
    },{
      "id":"CLEANER32",
      "description":"Cleaner module",
      "version":"1132",
      "date":"2017-03-15"
    },{
      "id":"ANTISTEALTH32",
      "description":"Anti-Stealth support module",
      "version":"1106",
      "date":"2016-10-17"
    },{
      "id":"SYSTEMSTATUS32",
      "description":"ESET SysInspector module",
      "version":"1266",
      "date":"2016-12-22"
    },{
      "id":"TRANSLATOR32",
      "description":"Translation support module",
      "version":"1588B",
      "date":"2017-03-01"
    },{
      "id":"HIPS32",
      "description":"HIPS support module",
      "version":"1267",
      "date":"2017-02-16"
    },{
      "id":"PROTOSCAN32",
      "description":"Internet protection module",
      "version":"1300",
      "date":"2017-03-03"
    },{
      "id":"DBLITE32",
      "description":"Database module",
      "version":"1088",
      "date":"2017-01-05"
    },{
      "id":"CONFENG32",
      "description":"Configuration module (33)",
      "version":"1496B",
      "date":"2017-03-17"
    },{
      "id":"IRIS32",
      "description":"LiveGrid communication module",
      "version":"1022",
      "date":"2016-04-01"
    },{
      "id":"SAURON32",
      "description":"Rootkit detection and cleaning module",
      "version":"1006",
      "date":"2016-07-15"
    },{
      "id":"SSL32",
      "description":"Cryptographic protocol support module",
      "version":"1009",
      "date":"2016-12-02"
    }
  ],
  "error":null
}

```

get license-info

Get information about the license of the product

Command line

```
ermm.exe get license-info
```

Parameters

None

Example

call

```
{
  "command": "get_license_info",
  "id": 1,
  "version": "1"
}
```

result

```
{
  "id": 1,
  "result": {
    "type": "NFR",
    "expiration_date": "2020-12-31",
    "expiration_state": "ok",
    "public_id": "3XX-7ED-7XF",
    "seat_id": "6f726793-ae95-4e04-8ac3-e6a20bc620bf",
    "seat_name": "M"
  },
  "error": null
}
```

get logs

Get logs of the product

Command line

```
ermm.exe get logs --name warnlog --start-date "2017-04-04 06-00-00" --end-date "2017-04-04 12-00-00"
```

Parameters

Name	Value
name	{ all, virlog, warnlog, scanlog, blocked, hipslog, urllog, devctrllog } : log to retrieve
start-date	start date from which logs should be retrieved (YYYY-MM-DD [HH-mm-SS])
end-date	end time until which logs should be retrieved (YYYY-MM-DD [HH-mm-SS])

Example

```
call
{
  "command": "get_logs",
  "id": 1,
  "version": "1",
  "params": {
    "name": "warnlog",
    "start_date": "2017-04-04 06-00-00",
    "end_date": "2017-04-04 12-00-00"
  }
}
```

```
result
{
  "id": 1,
  "result": {
    "warnlog": {
      "display_name": "Events",
      "logs": [
        {
          "Time": "2017-04-04 06-05-59",
          "Severity": "Info",
          "PluginId": "ESET Kernel",
          "Code": "Malware database was successfully updated to version 15198 (20170404).",
          "UserData": ""
        },
        {
          "Time": "2017-04-04 11-12-59",
          "Severity": "Info",
          "PluginId": "ESET Kernel",
          "Code": "Malware database was successfully updated to version 15199 (20170404).",
          "UserData": ""
        }
      ]
    }
  },
  "error": null
}
```

get activation-status

Get information about the last activation. Result of status can be {

success, running, failure }

Command line

```
ermm.exe get activation-status
```

Parameters

None

Example

call

```
{
  "command": "get_activation_status",
  "id": 1,
  "version": "1"
}
```

result

```
{
  "id": 1,
  "result": {
    "status": "success"
  },
  "error": null
}
```

get scan-info

Get information about running scan.

Command line

```
ermm.exe get scan-info
```

Parameters

None

Example

call

```
{
  "command": "get_scan_info",
  "id": 1,
  "version": "1"
}
```

result

```
{
  "id":1,
  "result":{
    "scan-info":{
      "scans":[{
        "scan_id":65536,
        "timestamp":272,
        "state":"finished",
        "pause_scheduled_allowed":false,
        "pause_time_remain":0,
        "start_time":"2017-06-20T12:20:33Z",
        "elapsed_tickcount":328,
        "exit_code":0,
        "progress_filename":"Operating memory",
        "progress_arch_filename":"",
        "total_object_count":268,
        "infected_object_count":0,
        "cleaned_object_count":0,
        "log_timestamp":268,
        "log_count":0,
        "log_path":"C:\\ProgramData\\ESET\\ESET Security\\Logs\\eScan\\ndl31494.dat",
        "username":"test-PC\\test",
        "process_id":3616,
        "thread_id":3992,
        "task_type":2
      }],
      "pause_scheduled_active":false
    }
  },
  "error":null
}
```

get configuration

Get the product configuration. Result of status may be { success, error }

Command line

```
ermm.exe get configuration --file C:\\tmp\\conf.xml --format xml
```

Parameters

Name	Value
file	the path where the configuration file will be saved
format	format of configuration: json, xml. Default format is xml

Example

```
call
```

```
{
  "command": "get_configuration",
  "id": 1,
  "version": "1",
  "params": {
    "format": "xml",
    "file": "C:\\tmp\\conf.xml"
  }
}
```

result

```
{
  "id": 1,
  "result": {
    "configuration": "PD94bWwgdmVyc2lvbj0iMS4w=="
  },
  "error": null
}
```

get update-status

Get information about the update. Result of status may be { success, error }

Command line

```
ermm.exe get update-status
```

Parameters

None

Example

call

```
{
  "command": "get_update_status",
  "id": 1,
  "version": "1"
}
```

result

```
{
  "id": 1,
  "result": {
    "last_update_time": "2017-06-20 13-21-37",
    "last_update_result": "error",
    "last_successful_update_time": "2017-06-20 11-21-45"
  },
  "error": null
}
```

start scan

Start scan with the product

Command line

ermm.exe start scan --profile "profile name" --target "path"

Parameters

Name	Value
profile	Profile name of On-demand computer scan defined in product
target	Path to be scanned

Example

```
call
{
  "command": "start_scan",
  "id": 1,
  "version": "1",
  "params": {
    "profile": "Smart scan",
    "target": "c:\\\"
  }
}
```

```
result
{
  "id": 1,
  "result": {
    "task_id": 458752
  },
  "error": null
}
```

start activation

Start activation of product

Command line

ermm.exe start activation --key "activation key" | --offline "path to offline file"

Parameters

Name	Value
------	-------

key	Activation key
offline	Path to offline file

Example

call
<pre>{ "command": "start_activation" "id": 1, "version": "1", "params": { "key": "XXXX-XXXX-XXXX-XXXX-XXXX" } }</pre>

result
<pre>{ "id": 1, "result": { }, "error": null }</pre>

start deactivation

Start deactivation of the product

Command line

```
ermm.exe start deactivation
```

Parameters

None

Example

call
<pre>{ "command": "start_deactivation", "id": 1, "version": "1" }</pre>

result
<pre>{ "id": 1, "result": { }, "error": null }</pre>

start update

Start update of the product. Only one update may be running in the product so in case the update is already running, "Task already running" error code is returned

Command line

```
ermm.exe start update
```

Parameters

None

Example

call
<pre>{ "command": "start_update", "id": 1, "version": "1" }</pre>
result
<pre>{ "id": 1, "result": { }, "error": { "id": 4, "text": "Task already running." } }</pre>

set configuration

Set configuration to the product. Result of status may be { success, error }

Command line

```
ermm.exe set configuration --file C:\tmp\conf.xml --format xml --password pass
```

Parameters

Name	Value
file	the path where the configuration file will be saved

password	password for configuration
value	configuration data from the argument (encoded in base64)

Example

call

```
{
  "command": "set_configuration",
  "id": 1,
  "version": "1",
  "params": {
    "format": "xml",
    "file": "C:\\tmp\\conf.xml",
    "password": "pass"
  }
}
```

result

```
{
  "id": 1,
  "result": {
  },
  "error": null
}
```

Dúvidas comuns

Este capítulo contém algumas perguntas e problemas mais frequentes encontrados. Clique em um título do capítulo para descobrir como solucionar o seu problema:

- [Como atualizar o ESET Endpoint Security](#)
- [Como ativar o ESET Endpoint Security](#)
- [Como usar credenciais atuais para ativar um novo produto](#)
- [Como remover um vírus do meu PC](#)
- [Como permitir comunicação para um determinado aplicativo](#)
- [Como criar uma nova tarefa na Agenda](#)
- [Como agendar um escanear semanal do computador](#)
- [Como gerenciar notificações e alertas interativos](#)
- [Como conectar meu produto ao ESET PROTECT](#)
 - [Como usar o modo de Substituição](#)
 - [Como aplicar uma política recomendada para o ESET Endpoint Security](#)
- [Como configurar uma imagem](#)
- [Como atualizar para o Windows 10 com o ESET Endpoint Security](#)
- [Como ativar o Monitoramento e gerenciamento remoto](#)
- [Como bloquear o download de tipos de arquivo específicos da Internet](#)
- [Como minimizar a interface do usuário do ESET Endpoint Security](#)

Se o seu problema não estiver incluído na lista das páginas de ajuda acima, tente pesquisar por palavra-chave ou digite uma frase descrevendo seu problema nas páginas de ajuda do ESET Endpoint Security.

Se não conseguir encontrar a solução para o seu problema/pergunta dentro das páginas de Ajuda, poderá acessar nossa [Base de conhecimento ESET](#) onde estão disponíveis respostas para perguntas e problemas comuns.

- [Melhores práticas para proteger contra malware Filecoder \(ransomware\)](#)
- [FAQ do ESET Endpoint Security e ESET Endpoint Antivirus](#)
- [Quais endereços e portas em meu firewall de terceiros devo abrir para permitir a funcionalidade total para meu produto ESET?](#)

Se necessário, você pode contatar nosso centro de suporte técnico on-line com as suas perguntas ou problemas. O link para nosso formulário de contato on-line pode ser encontrado no painel **Ajuda e Suporte** na janela do programa principal.

FAQ de Atualizações automáticas



Para informações adicionais sobre atualizações de produto no ESET Endpoint Security, leia o artigo da Base de conhecimento da ESET a seguir:

- [Quais são os diferentes tipos de atualização de produto da ESET e lançamentos?](#)

Os computadores serão atualizados automaticamente? O download da atualização é feito antes ou depois da reinicialização?

O download acontece antes da reinicialização, e os arquivos atualizados também são preparados nesta etapa. Depois da reinicialização, os arquivos atualizados ainda estão apenas preparados para uso, e a versão instalada no momento oferece proteção continuada. As alterações são aplicadas depois do próximo início do produto ESET Endpoint.

Eu tenho aproximadamente 3000 computadores. Todos os computadores vão fazer download das atualizações ao mesmo tempo? Posso usar o proxy para Atualizações automáticas com muitos computadores?

A ESET oferece a Ferramenta de imagem e soluções de proxy para redes maiores, portanto, o download das atualizações é feito apenas uma vez da internet e depois distribuído localmente. As atualizações são pequenas, geralmente de 5 a 10 MB e a ESET vai liberá-las durante as primeiras semanas de disponibilidade. Portanto, nem todos os clientes vão iniciar o download simultaneamente quando conectados diretamente aos servidores ESET.

Posso decidir quantos ou quais computadores serão atualizados automaticamente? Não quero fazer download de mais de dez computadores por hora, ou só quero atualizar dez computadores agora e outro computador depois de alguns dias.

Ambientes gerenciados têm uma política de atualização automática onde você pode especificar a versão mais recente desejada. O uso de curingas (por exemplo, 9.0.2032.*) também é possível. Para obter mais informações, visite o capítulo de Atualizações automáticas na ajuda on-line do [ESET PROTECT](#) ou [ESET PROTECT Cloud](#). Infelizmente, não há outras opções para limitar as atualizações automáticas disponíveis no momento. Você pode atribuir várias políticas para vários grupos.

As atualizações automáticas são configuradas apenas através da política? Posso desativar a política se não quiser que o produto ESET seja atualizado?

Se houver um hotfix de Segurança e Estabilidade para o produto ESET Endpoint, o produto será atualizado mesmo

quando as atualizações automáticas estão desativadas, de acordo com os termos definidos no Acordo de Licença para o Usuário Final aplicável. A ESET usa [Hotfixes de Segurança e Estabilidade](#) para lidar com problemas críticos e garantir o máximo de segurança e estabilidade para seu produto ESET.

Você pode atribuir uma política de atualização automática a qualquer grupo de endpoints, independentemente de sua configuração atual de atualização automática. Em ambientes não gerenciados, o usuário pode configurar localmente as atualizações automáticas na tela de Configuração avançada de um produto ESET endpoint.

E se eu configurar uma política para usar a versão mais antiga disponível? Mesmo assim, a ESET vai atualizar meus produtos?

Hotfixes e hotfixes críticos (atualizações de segurança e estabilidade) são categorias de atualização ligeiramente diferentes. Quando as configurações do usuário são aceitas, hotfixes regulares são atribuídos a atualizações automáticas com uma prioridade padrão. Hotfixes críticos são aplicados com prioridade máxima, independentemente das configurações do usuário.

Como as atualizações vão funcionar em cenários off-line? Quando os usuários estão usando o repositório off-line?

O repositório off-line também contém arquivos .dup e .fup. O download da seção do repositório deve ser feito pela Ferramenta de imagem, não pela atualização de módulo. Para mais informações, leia o [artigo da Base de conhecimento da ESET](#) a seguir.

Como os produtos ESET sabem que a atualização é necessária? Do repositório? Existem dados enviados para os servidores? Se a ESET planeja fazer uma atualização um mês depois do lançamento da versão, os servidores ESET podem lidar com um lançamento mundial?

O produto ESET faz download de atualizações automáticas do repositório. Os servidores estão prontos para isso, pois atualizações críticas têm apenas alguns kilobytes de tamanho. A ESET não vai lançar atualizações críticas em servidores do repositório. Porém, há uma opção de lançar atualizações em servidores se as atualizações automáticas forem maiores. A tabela abaixo mostra o exemplo de tamanhos de hotfix no caso de uma atualização automática diferencial:

Versão anterior	Nova versão	Tamanho
9.0.2032.2	9.0.2032.6	420 KB
8.1.2037.2	9.0.2032.2	6.5 MB
8.0.2028.0	9.0.2032.2	11.5 MB

Se uma atualização automática diferencial, seu produto ESET pode iniciar uma atualização completa. Ela ainda é uma atualização automática com uma garantia de funcionalidade, mas em vez de um arquivo .dup, será feito o download de um .fup, que é um arquivo maior. Para a versão 9.0.2032.2, o arquivo é de 27MB. Porém, tal cenário é raro.

O ESET Endpoint Security/ESET Endpoint Antivirus será atualizado com throttling? Se sim, por quanto tempo o

throttling acontece depois do lançamento?

A ESET lança atualizações parciais pelas primeiras semanas depois de uma nova versão ser lançada para reduzir a carga em nossos servidores e distribuir a nova versão de forma balanceada.

Atualizações automáticas vão se tornar um dos principais métodos de atualização. Como ela funciona, em detalhes?

O objetivo da ESET é ter o máximo de clientes possível usando atualizações automáticas. É difícil disponibilizar suporte para muitas versões de produto antigas. O recurso Atualizações automáticas funciona de forma simples – é feito o download de arquivos .dup durante a primeira verificação de atualização de módulo. Durante o procedimento de atualização, o produto está totalmente funcional e protege o computador em todos os momentos. A nova versão é ativada depois da reinicialização. No ESET PROTECT (do lado do servidor), você pode usar uma política para especificar a versão mais recente para a qual deseja atualizar, ou usar caracteres curinga. Para obter mais informações, visite o capítulo de Atualizações automáticas na ajuda on-line do [ESET PROTECT](#) ou [ESET PROTECT Cloud](#).

Está correto que as atualizações automáticas funcionam em 1/10? Estou usando o ESET Endpoint Security 8.0.2028.1 agora. Se as atualizações automáticas forem executadas, para qual versão ele será atualizado?

A atualização de produtos usando atualizações automáticas pode ser atrasada devido a um throttling em servidores de repositório. Se uma atualização de produto for lançada com throttling, as verificações automáticas de atualização podem não receber essa atualização imediatamente. Se a atualização for considerada segura e estável, o lançamento parcial pode ser reduzido ou removido completamente para que todos os clientes restantes recebam a atualização.

O procedimento de throttling pode levar um tempo diferente para cada atualização. Ele varia dependendo de quantos clientes solicitarem a atualização, o tráfego em nossos servidores e outros fatores. Esse procedimento está sempre em evolução e mudanças acontecem a todo o momento. Além disso, como o recurso de Atualizações automáticas é novo, provavelmente vamos ajustar esse procedimento no futuro para melhorar a experiência do cliente.

Quando as atualizações automáticas serão executadas, se eu iniciar um computador às 08:45 e desligar às 17:00?

Na próxima atualização de módulo agendada bem-sucedida, no máximo uma vez a cada 24 horas.

Quando a atualização será executada da próxima vez, se o computador for desligado enquanto as atualizações automáticas estão em execução?

A atualização será realizada na próxima janela de atualização agendada. Há um mecanismo robusto à prova de falhas para o procedimento de atualização automática (anteriormente uPCU). Depois de fazer download da atualização e reiniciar o computador, os arquivos atualizados ainda estão preparados para uso, e a versão instalada no momento oferece uma proteção continuada. As alterações são aplicadas depois do próximo início do produto ESET endpoint.

Como executar as atualizações automáticas imediatamente sem aguardar uma conexão regular a cada 24 horas? Existe outra forma de clicar em Verificar se há atualizações?

Você pode iniciar o procedimento de atualização automática manualmente apenas quando você abrir a janela principal do programa e clicar em **Atualizar > Verificar se há atualizações**. Todas as outras formas de iniciar atualizações de módulo refletem a política da Agenda de atualização automática de 24 horas. No momento, não é possível iniciar remotamente um download de atualização automática. Adicionaremos este recurso em uma atualização futura.

Como atualizar o ESET Endpoint Security

A atualização do ESET Endpoint Security pode ser executada de forma manual ou automática. Para acionar a atualização, clique em **Atualizar** na janela principal do programa e em seguida clique em **Buscar atualizações**.

A configuração de instalação padrão cria uma tarefa de atualização automática que é executada a cada hora. Para alterar o intervalo, vá para **Ferramentas > Agenda** (consulte [mais informações sobre a Agenda](#)).

Como ativar o ESET Endpoint Security

Após a conclusão da instalação, você será solicitado a ativar o produto.

Há vários métodos para ativar seu produto. A disponibilidade de um cenário de ativação específico na janela de ativação pode variar conforme o país, assim como os meios de distribuição (página da web da ESET, instalador tipo .msi ou .exe, etc.).

Para ativar sua cópia do ESET Endpoint Security diretamente do programa, abra a janela principal do programa ESET Endpoint Security e, no menu principal, clique em **Ajuda e suporte > Ativar produto** ou **Status de proteção > Ativar produto**.


Você pode usar qualquer um dos seguintes métodos para ativar o ESET Endpoint Security:


- **Use uma Chave de licença comprada** - Uma sequência exclusiva no formato XXXX-XXXX-XXXX-XXXX-XXXX, que é usada para identificação do proprietário da licença e para ativação da licença.
- **ESET Business Account** – Uma conta criada no portal [ESET Business Account](#) com credenciais (endereço de email + senha). Esse método permite que você gerencie várias licenças de um local.
- **Licença offline** - Um arquivo gerado automaticamente que será transferido para o produto da ESET para fornecer informações de licença. Se uma licença permitir que você baixe um arquivo de licença off-line (.lf), esse arquivo poderá ser usado para realizar a ativação off-line. O número de licenças off-line será subtraído do número total de licenças disponíveis. Para mais detalhes sobre a geração de um arquivo off-line consulte o Guia do Usuário do [ESET Business Account](#).

Clique em **Ativar mais tarde** se seu computador for um membro da rede gerenciada e seu administrador for realizar a ativação remota via ESET PROTECT. Você também pode usar esta opção se quiser ativar este cliente em posteriormente.

Se você tem um Nome de usuário e Senha usados para a ativação de produtos ESET mais antigos e não sabe como ativar o ESET Endpoint Security, [converta suas credenciais de legado para uma Chave de licença](#).

[Falha na ativação do produto?](#)

Você pode alterar sua licença de produto a qualquer momento. Para isso, clique em **Ajuda e suporte > Alterar licença** na janela principal do programa. Você verá o ID público de licença usado para identificar sua licença para o Suporte ESET. O Nome de usuário sob o qual seu computador está registrado é armazenado na seção **Sobre**, que pode ser vista clicando com o botão direito do mouse no ícone da bandeja do sistema .

 O ESET PROTECT 7.2 ou ESET PROTECT 9 pode ativar computadores do cliente em segundo plano usando licenças disponibilizadas pelo administrador. Para instruções sobre como fazer isso, consulte a [Ajuda on-line ESET PROTECT](#).

Digitando sua chave de licença durante a ativação

Atualizações automáticas são importantes para sua segurança. O ESET Endpoint Security vai receber atualizações apenas depois de ativado usando sua **Chave de licença**.

Se você não digitou sua Chave de licença depois da instalação, o produto não será ativado. Você pode alterar sua licença na janela principal do programa. Para fazer isso, clique em **Ajuda e suporte > Ativar licença** e digite os dados da licença que você recebeu com seu produto de segurança ESET na janela de Ativação do produto.

Ao digitar sua **Chave de licença**, é importante digitar exatamente como ela está escrita:

- Sua Chave de licença é uma sequência exclusiva no formato XXXX-XXXX-XXXX-XXXX-XXXX, que é usada para identificação do proprietário da licença e ativação da licença.

Recomendamos que copie e cole sua chave de licença do seu email de registro para garantir a precisão.

Login no ESET Business Account

A conta do admin de segurança é uma conta criada no portal do ESET Business Account com seu **endereço de email e senha**, que é capaz de ver todas as autorizações de licença. Uma conta de administrador de segurança permite que você gerencie várias licenças. Se você não tiver uma conta de administrador de segurança, clique em **Criar conta** e você será redirecionado para o portal do ESET Business Account, onde poderá se registrar com suas credenciais.

Se você tiver esquecido sua senha, clique em **Esqueci minha senha** e você será redirecionado para o portal ESET Business Account. Insira seu endereço de email e clique em **Entrar** para confirmar. Depois disso, você receberá uma mensagem com instruções sobre como redefinir sua senha.

Como usar as credenciais de licença legado para ativar um produto endpoint da ESET mais novo

Se você já tiver seu Nome de usuário e Senha e quiser receber uma Chave de licença, acesse o [portal do ESET Business Account](#), onde você poderá converter suas credenciais em uma nova chave de licença.

Como remover um vírus do meu PC

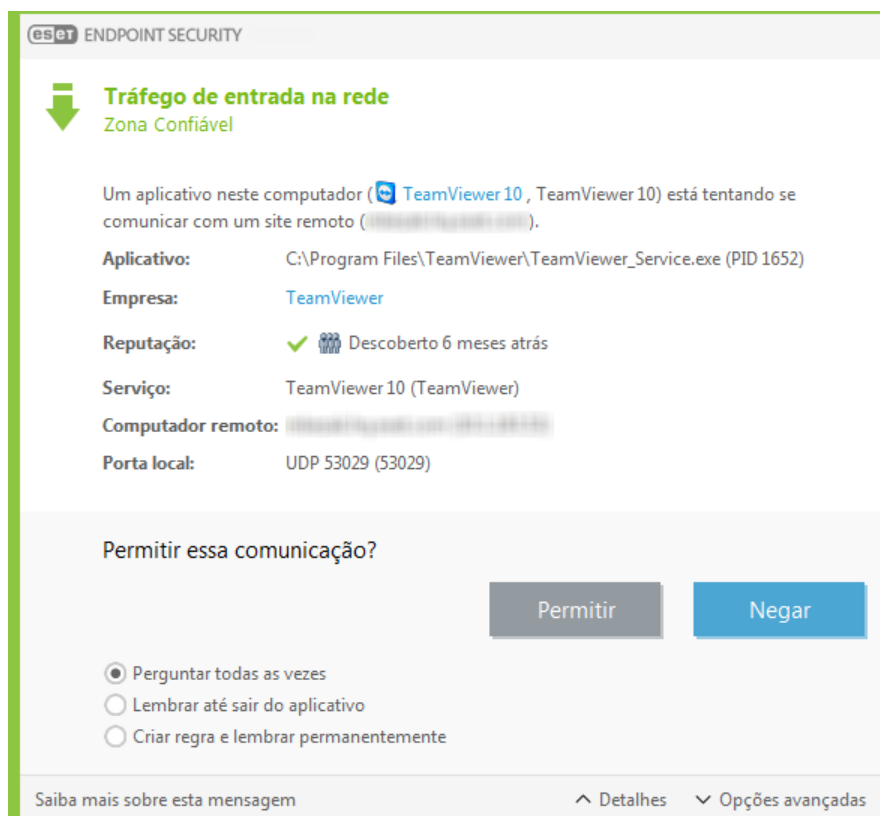
Se o seu computador estiver mostrando sintomas de uma infecção por código malicioso, como, por exemplo, estiver mais lento, congelar com frequência, recomendamos que você faça o seguinte:

1. Na janela do programa principal, clique em **Rastrear o computador**.
2. Clique em **Rastreamento inteligente** para começar o rastreamento do sistema.
3. Após a conclusão do rastreamento, revise o log com o número de arquivos verificados, infectados e limpos.
4. Se desejar rastrear apenas uma determinada parte do seu disco, clique em **Rastreamento personalizado** e selecione os alvos a serem rastreados quanto a vírus.

Para informações adicionais consulte nosso [artigo na Base de conhecimento ESET](#) atualizado regularmente.

Como permitir comunicação para um determinado aplicativo

Se uma nova conexão for detectada no modo interativo e se não houver uma regra correspondente, será solicitado que você permita ou negue a conexão. Se desejar executar a mesma ação toda vez que o ESET Endpoint Security tentar estabelecer conexão, marque a caixa de seleção **Lembrar ação (criar regra)**.



Você pode criar novas regras de firewall para aplicativos antes que eles sejam detectados pelo ESET Endpoint Security na janela de configuração do firewall, abra a janela principal do programa > **Configuração** > **Rede** > **Firewall** > clique na engrenagem > **Configurar...** > **Avançado** > **Regras** clicando em **Editar**.

Clique em **Adicionar** para adicionar a regra. Na guia **Geral**, insira o nome, a direção e o protocolo de comunicação para a regra. A janela permite que você defina a ação a ser tomada quando a regra for aplicada.

Insira o caminho para o executável do aplicativo e a porta de comunicação local na guia **Local**. Clique na guia **Remoto** para inserir o endereço remoto e a porta (se aplicável). A regra recém-criada será aplicada assim que o aplicativo tentar comunicar novamente.

Como criar uma nova tarefa na Agenda

Para criar uma nova tarefa em **Ferramentas > Agenda**, clique em **Adicionar tarefa** ou clique com o botão direito do mouse e selecione **Adicionar** no menu de contexto. Cinco tipos de tarefas agendadas estão disponíveis:

- **Executar aplicativo externo** – Agenda a execução de um aplicativo externo.
- **Manutenção de logs** - Os arquivos de log também contêm registros remanescentes excluídos. Essa tarefa otimiza regularmente os registros nos arquivos de log para funcionar de maneira eficiente.
- **Verificar arquivos na inicialização do sistema** - Verifica os arquivos que tem permissão para serem executados no login ou na inicialização do sistema.
- **Criar um instantâneo do status do computador** - Cria um instantâneo do computador ESET SysInspector - coleta informações detalhadas sobre os componentes do sistema (por exemplo, drivers e aplicativos) e avalia o nível de risco de cada componente.
- **Rastrear o computador sob demanda** - Executa um rastreamento de arquivos e pastas em seu computador.
- **Atualização** - Agenda uma tarefa de atualização, atualizando os módulos.

Como **Atualizar** é uma das tarefas agendadas usadas com mais frequência, explicaremos a seguir como adicionar uma nova tarefa de atualização:

No menu suspenso **Tarefa agendada**, selecione **Atualizar**. Insira o nome da tarefa no campo **Nome da tarefa** e clique em **Próximo**. Selecione a frequência da tarefa. As opções disponíveis são: **Uma vez**, **Repetidamente**, **Diariamente**, **Semanalmente** e **Acionado por evento**. **Selecione Pular tarefa quando estiver executando na bateria** para minimizar os recursos do sistema enquanto o laptop estiver em execução na bateria. A tarefa será realizada uma vez somente na data e hora especificadas nos campos **Execução de tarefas**. Depois defina a ação a ser tomada se a tarefa não puder ser executada ou concluída na hora agendada. As opções disponíveis são:

- **Na próxima hora agendada**
- **O mais breve possível**
- **Imediatamente, se o tempo depois da última execução ultrapassar um valor específico** (o intervalo pode ser definido utilizando a caixa de rolagem **Tempo depois da última execução**)

Na próxima etapa, uma janela de resumo com informações sobre a tarefa agendada atual é exibida. Clique em **Concluir** quando tiver concluído as alterações.

Uma janela de diálogo será exibida permitindo selecionar perfis a serem utilizados para a tarefa agendada. Aqui é possível especificar um perfil primário e um alternativo. Que será usado caso a tarefa não possa ser concluída utilizando o perfil primário. Confirme clicando em **Concluir** e a nova tarefa agendada será adicionada à lista de tarefas agendadas no momento.

Como agendar um escanear semanal do computador

Para agendar uma tarefa regular, abra a janela do programa principal e clique em **Ferramentas > Agenda**. A seguir está um pequeno guia sobre como agendar uma tarefa que escaneará suas unidades locais toda semana. Consulte nosso [artigo da Base de conhecimento](#) para instruções mais detalhadas.

Para agendar uma tarefa de rastreamento:

1. Clique em **Adicionar** na tela principal do módulo Agenda.
2. Selecione **Rastreamento sob demanda do computador** no menu suspenso.
3. Escolha um nome para a tarefa e selecione **Semanalmente para a frequência da tarefa**.
4. Configure a data e hora em que a tarefa será executada.
5. Selecione **Executar a tarefa tão logo quanto possível** para realizar a tarefa mais tarde se a tarefa programada não começar por qualquer motivo (por exemplo, o computador estava desligado).
6. Revise o resumo da tarefa agendada e clique em **Fim**.
7. No menu suspenso **Alvos**, selecione **Unidades locais**.
8. Clique em **Concluir** para aplicar a tarefa.

Como conectar o ESET Endpoint Security ao ESET PROTECT

Quando você tiver instalado o ESET Endpoint Security no seu computador e quiser conectar via ESET PROTECT, certifique-se de também ter instalado o Agente ESET Management na sua estação de trabalho cliente. Ele é uma parte essencial de qualquer solução do cliente que se comunica com o Servidor ESET PROTECT.

- [Instalar o Agente ESET Management nas estações de trabalho do cliente](#)

Veja também:

- [Documentação para endpoints gerenciados remotamente](#)
- [Como usar o modo de Substituição](#)
- [Como aplicar uma política recomendada para o ESET Endpoint Security](#)


Como usar o modo de Substituição

Usuários com produtos ESET endpoint (versão 6.5 e mais recente) do Windows instalados em sua máquina podem usar o recurso Substituição. O modo de substituição permite que os usuários no nível do computador do 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 certos usuários AD, ou pode ser protegido por senha. A função não pode ser ativada por mais de quatro horas por vez.

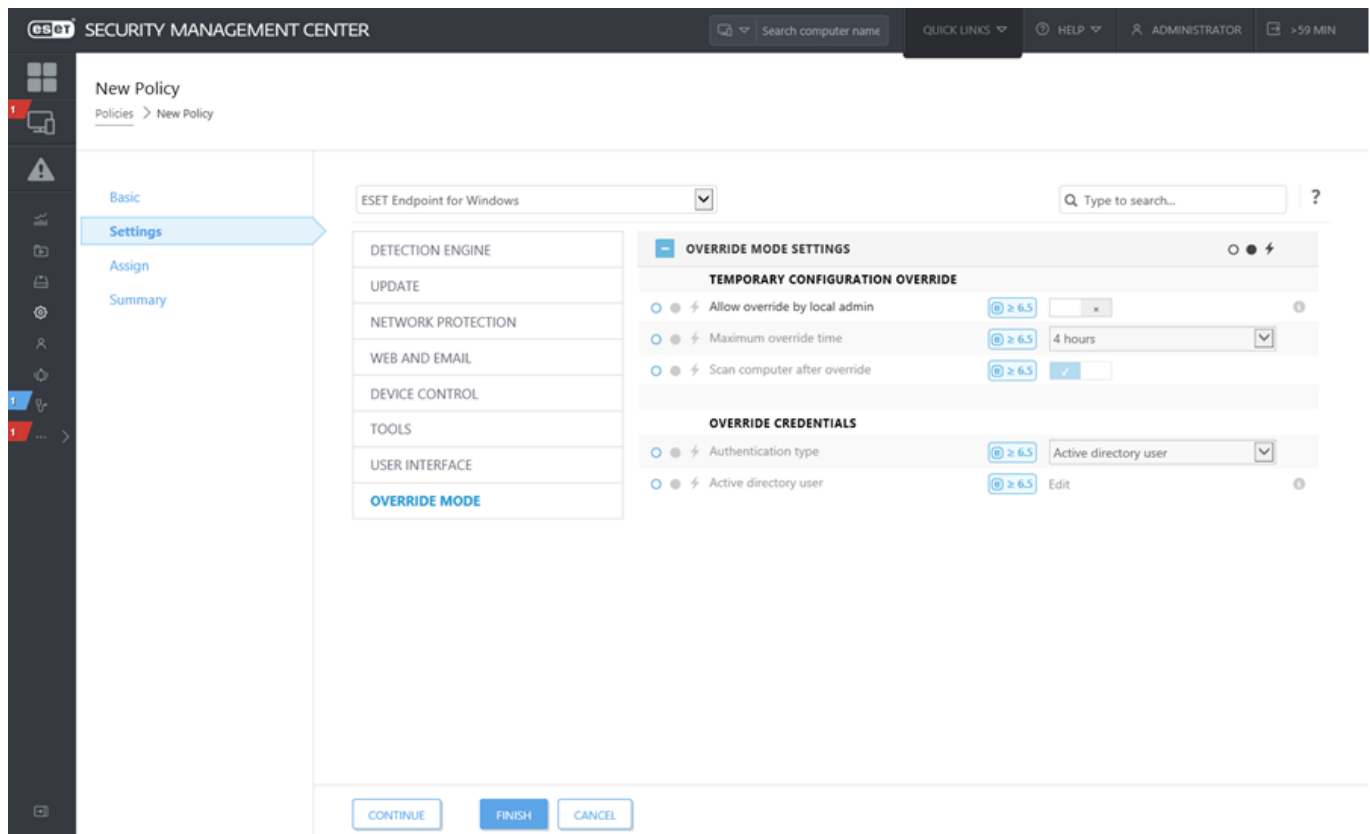


- Não é possível parar o modo de substituição do Console web ESET PROTECT depois dele estar ativado. O modo de substituição será desativado automaticamente quando o período de tempo de substituição expirar. Ele também pode ser desligado na máquina do cliente.
- O usuário que está usando o Modo de substituição também precisa ter direitos de administrador do Windows. Caso contrário, o usuário não poderá salvar as alterações nas configurações do ESET Endpoint Security.
- A autenticação em grupo do Active Directory é compatível para o ESET Endpoint Security versão 7.0.2100.4 e versões posteriores.

Para definir o **Modo de Substituição**:

1. Navegue até  **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 até **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 **Exibir 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.


Como aplicar uma política recomendada para o ESET Endpoint Security

A melhor prática depois de conectar o ESET Endpoint Security ao ESET PROTECT é aplicar uma [política recomendada](#) ou aplicar uma política personalizada.


O ESET Endpoint Security tem várias políticas internas:

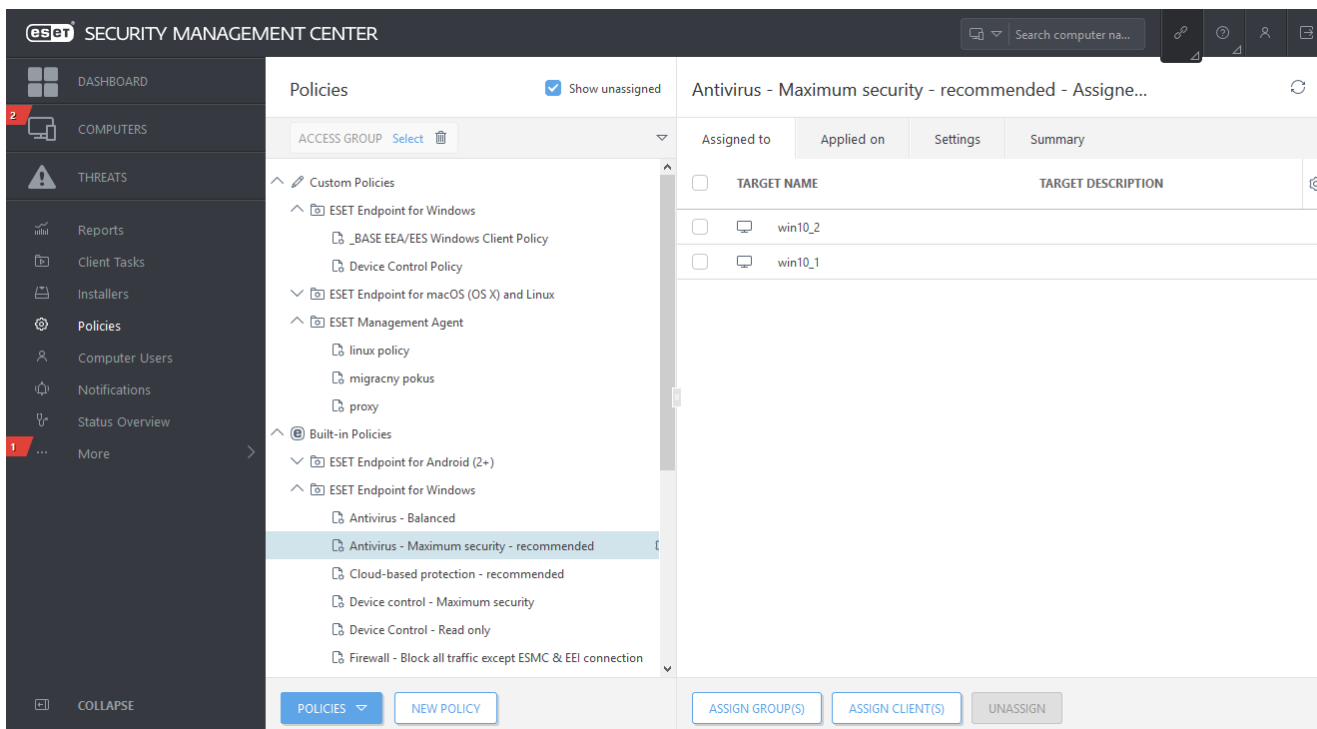
Política	Descrição
Antivírus - Balanceado	Configuração de segurança recomendada para a maioria das configurações.
Antivírus – Segurança máxima	Utilizando aprendizado de máquina, inspeção comportamental profunda e filtragem SSL. A detecção de aplicativos potencialmente indesejados, não seguros e suspeitos é afetada.
Sistema de reputação e feedback baseado em nuvem	Ativa o sistema de reputação e feedback baseado em nuvem ESET LiveGrid® para melhorar a detecção de ameaças recentes e ajudar a compartilhar ameaças maliciosas ou desconhecidas em potencial para uma análise mais aprofundada.
Controle de dispositivo - Segurança máxima	Todos os dispositivos estão bloqueados. Quando qualquer dispositivo quiser se conectar, ele precisará ser permitido por um administrador.
Controle de dispositivo - Somente leitura	Todos os dispositivos podem ser somente leitura. Não é permitido gravação.
Firewall – Bloquear todo o tráfego, exceto a conexão com o ESET PROTECT e o ESET Inspect	Bloquear todo o tráfego exceto a conexão ao ESET PROTECT e ESET Inspect Server (apenas ESET Endpoint Security).
Registro - Registro em relatório de diagnóstico completo	Esse modelo garantirá que o administrador tenha todos os relatórios disponíveis quando ele precisar. Tudo será registrado, desde o detalhamento mínimo, incluindo HIPS e parâmetros Threatsense , firewall. Os relatórios serão automaticamente removidos depois de 90 dias.
Registro - Registrar somente eventos importantes	A política garante que avisos, erros e eventos críticos sejam registrados. Os registros são automaticamente excluídos após 90 dias.
Visibilidade - Balanceado	Configuração padrão de visibilidade. Status e notificações estão ativados.
Visibilidade - Modo invisível	Notificações, alertas, GUI , integração ao menu contexto desativados. Nenhum egui.exe será executado. Adequado para gerenciamento apenas do ESET PROTECT Cloud .
Visibilidade - Interação reduzida com usuário	Status desativado, notificações desativadas, GUI apresentada.

Para configurar a política nomeada como **Antivírus – Segurança máxima**, que executa mais de 50 configurações recomendadas para o ESET Endpoint Security instaladas nas suas estações de trabalho, siga estas etapas:

-  Os artigos da Base de conhecimento da ESET a seguir podem estar disponíveis apenas em inglês:
- [Aplique uma política recomendada ou pré-definida para o ESET Endpoint Security usando o ESET PROTECT](#)

1. Abra o Web Console ESET PROTECT.

2. Navegue até  **Políticas** e abra **Políticas internas > ESET Endpoint para Windows**.
3. Clique em **Antivírus – Segurança máxima – recomendado**.
4. Na guia **Atribuído a** clique em **Atribuir cliente(s)** ou **Atribuir grupo(s)** e selecione os computadores apropriados nos quais você deseja aplicar essa política.



Para ver quais configurações serão aplicadas nessa política, clique na guia **Configurações** e abra a árvore de Configuração avançada.

- O ponto azul representa uma configuração alterada para essa política
- O número no quadro azul representa um número de configurações alteradas por essa política
- [Leia mais sobre políticas ESET PROTECT](#)

Como configurar uma imagem

O ESET Endpoint Security pode ser configurado para armazenar cópias de arquivos de atualização do mecanismo de detecção e distribuir atualizações para outras estações de trabalho com o ESET Endpoint Security ou o ESET Endpoint Antivirus em execução.

Configurando o ESET Endpoint Security como um servidor de imagem para fornecer atualizações via servidor HTTP interno

1. Pressione **F5** para acessar a Configuração avançada e abra **Atualização > Perfis > Imagem de atualização**.
2. Abra **Atualizações** e certifique-se de ter ativada a opção **Escolher automaticamente** sob **Atualizações de módulos**.
3. Abra a **Imagem de atualização** e ative **Criar imagem da atualização** e **Ativar servidor HTTP**.

Para mais informações, consulte:

- [Imagem de atualização](#)
- [Atualização através do mirror](#)

Configurando um servidor de Mirror para fornecer atualizações através de uma pasta de rede compartilhada

1. Crie uma pasta compartilhada em um dispositivo local ou em rede. Esta pasta deve ser lida por todos os usuários executando soluções de segurança da ESET e gravável da conta SYSTEM local.
2. Ative **Criar imagem da atualização** em **Configuração avançada > Atualização > Perfis > Imagem de atualização**.
3. Escolha uma **Pasta de armazenamento** adequada clicando ao **Limpar** e depois em **Editar**. Procure e selecione a pasta compartilhada criada.



Se não quiser fornecer atualizações de módulo através do servidor interno HTTP, desative **Criar imagem da atualização**.

Como atualizar para o Windows 10 com o ESET Endpoint Security



É altamente recomendável que você atualize para a versão mais recente do seu produto ESET, e em seguida faça o download dos módulos mais recentes, antes de atualizar para o Windows 10. Isso vai garantir a proteção máxima e preservar as configurações do programa e informações de licença durante a atualização para o Windows 10.

Versão 7.x:

Clique no link apropriado abaixo para fazer download e instalar a versão mais recente para preparar para a atualização para o Microsoft Windows 10:

[Download do ESET Endpoint Security 7 32-bit](#) [Download do ESET Endpoint Antivirus 7 32-bit](#)

[Download do ESET Endpoint Security 7 64-bit](#) [Download do ESET Endpoint Antivirus 7 64-bit](#)

Versão 5.x:



Produtos ESET Endpoint na versão 5 estão atualmente no [Fim da vida útil](#). Isso significa que as compilações não estão mais disponíveis publicamente para download. Recomendamos fortemente que você faça a atualização para a [versão mais recente dos produtos ESET Endpoint](#).

Versões em outros idiomas:

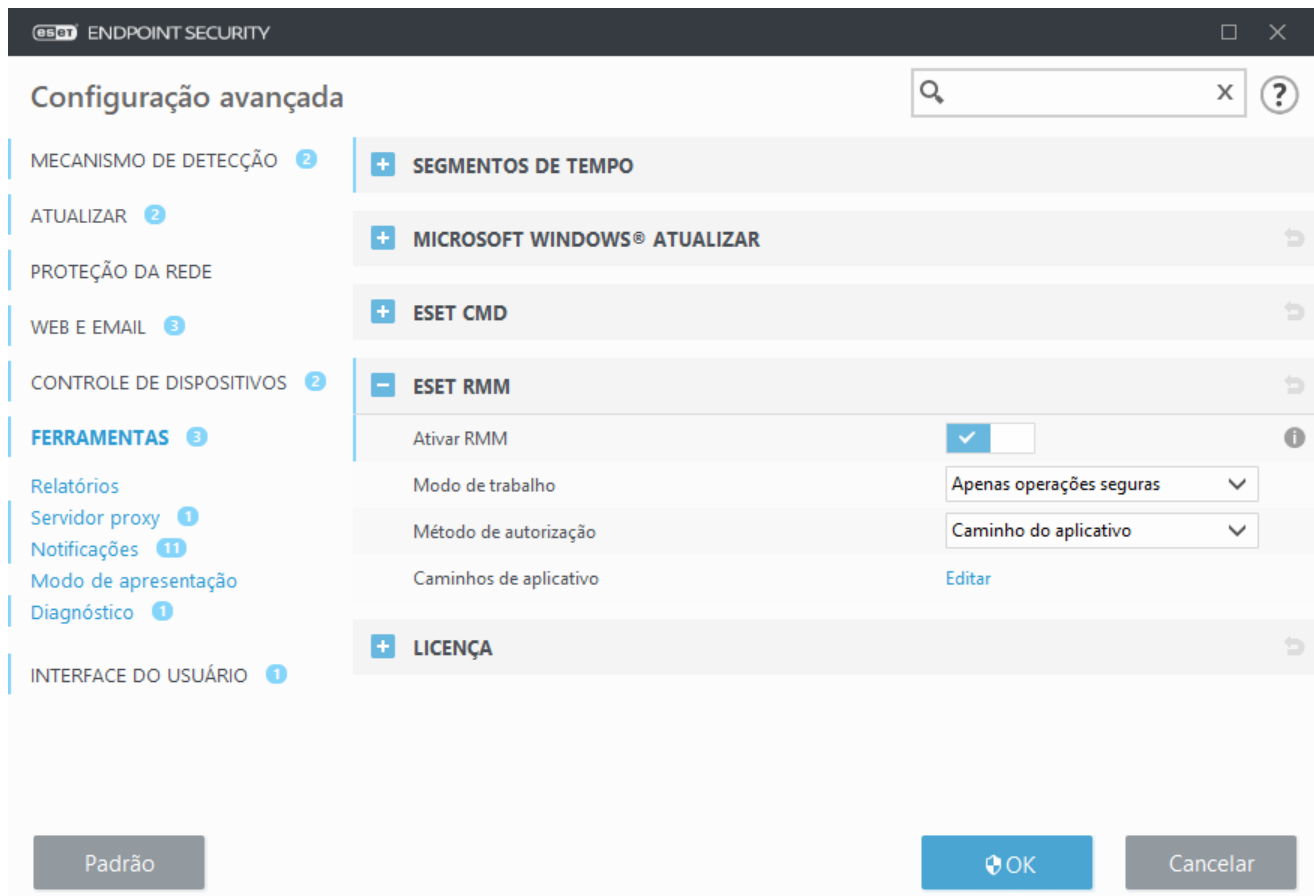
Se você está procurando por uma versão em outro idioma do seu produto ESET endpoint, [visite nossa página de download](#).



[Mais informações sobre a compatibilidade dos produtos empresariais ESET com o Windows 10.](#)

Como ativar o Monitoramento e gerenciamento remoto

O Monitoramento e Gerenciamento Remoto (RMM) é o processo de supervisionar e controlar sistemas de software (como aqueles em áreas de trabalho, servidores e dispositivos móveis) usando um agente instalado localmente que pode ser acessado por um prestador de serviço de gerenciamento. O ESET Endpoint Security pode ser gerenciado por RMM a partir da versão 6.6.2028.0.



Por padrão, o ESET RMM está desativado. Para ativar o ESET RMM, pressione **F5** para acessar a Configuração avançada, clique em **Ferramentas**, abra o **ESET RMM** e ative a chave ao lado de **Ativar RMM**.

Modo de trabalho – Selecione **Apenas operações seguras** se quiser permitir a interface RMM para operações seguras e somente leitura. Selecione **Todas as operações** se quiser ativar a interface RMM para todas as operações.

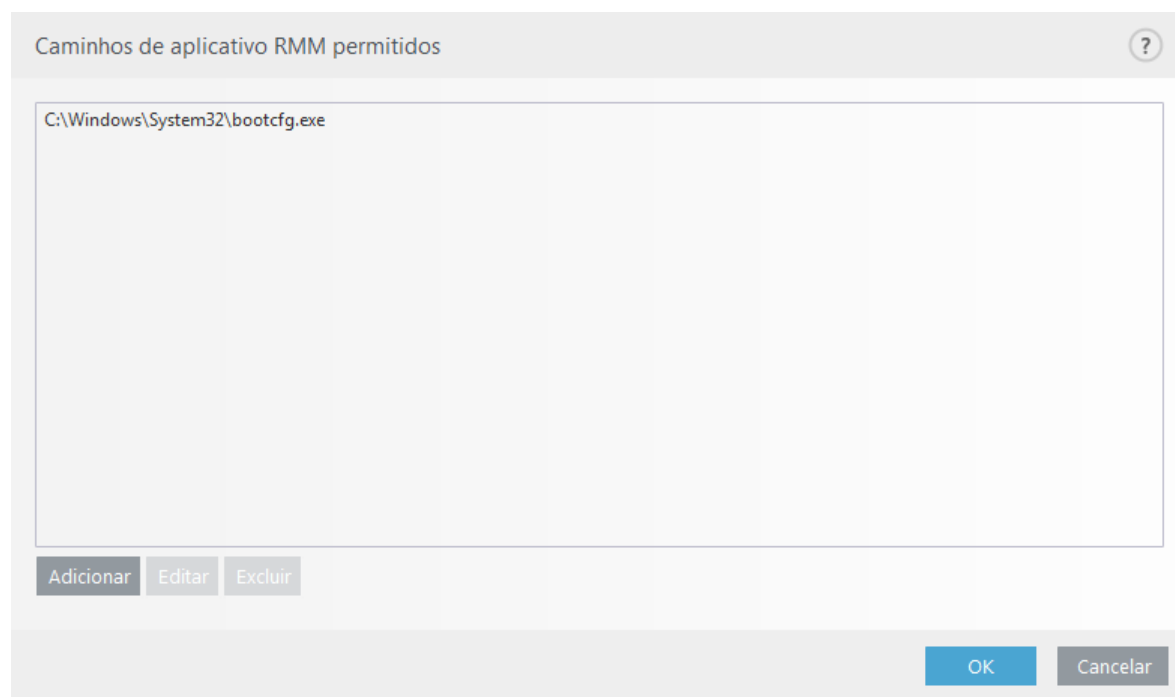
Operação	Modo Apenas operações seguras	Modo Todas as operações
Obter informações do aplicativo	✓	✓
Obter configuração	✓	✓
Obter informações de licença	✓	✓
Obter relatórios	✓	✓
Obter status da proteção	✓	✓
Obter status da atualização	✓	✓
Definir configuração		✓
Iniciar ativação		✓
Iniciar rastreamento	✓	✓
Iniciar atualização	✓	✓

Método de autorização – Defina o método de autorização RMM. Para a autorização de uso, selecione **Caminho de aplicativo** no menu suspenso, ou selecione **Nenhum**.



O RMM sempre deve usar a autorização para impedir que software malicioso desative ou desvie da proteção do ESET Endpoint.

Caminhos de aplicativo – Aplicativo específico que tem permissão para executar o RMM. Se você selecionou **Caminho de aplicativo** como um método de autorização, clique em **Editar** para abrir a janela de configuração **Caminho de aplicativo RMM permitido**.



Adicionar - Cria um novo caminho de aplicativo RMM. Insira o caminho ou clique no botão ... para selecionar um executável.

Editar – Modifica um caminho existente permitido. Use **Editar** se a localização do executável tiver sido alterada para outra pasta.

Excluir – Excluir um caminho existente permitido.

A instalação padrão ESET Endpoint Security contém o arquivo ermm.exe localizado no diretório do aplicativo Endpoint (caminho padrão *C:\Program Files\ESET\ESET Security*). O ermm.exe troca dados com o Plug-in RMM, que se comunica com o Agente RMM, vinculado a um Servidor RMM.

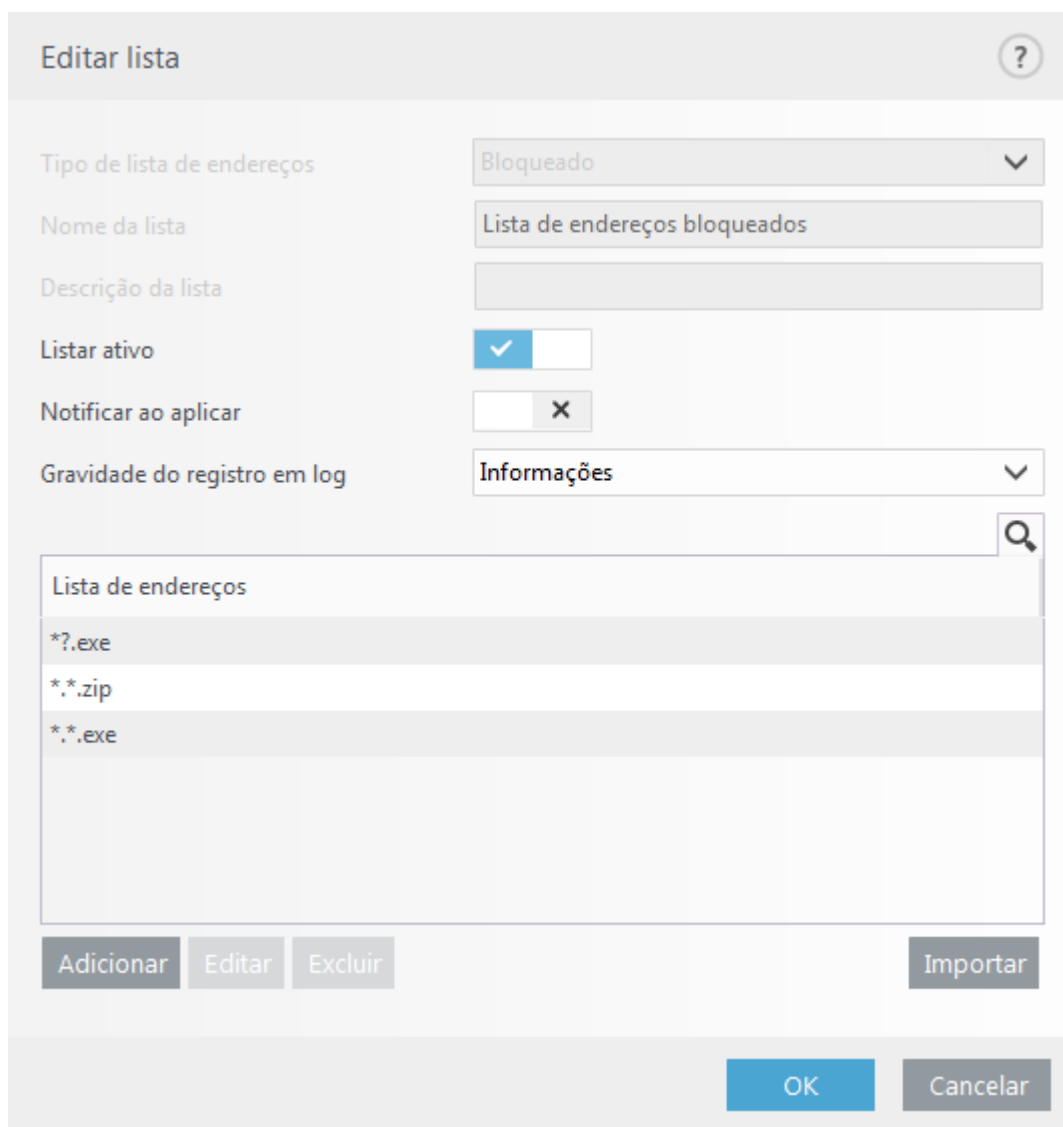
- ermm.exe – utilidade de linha de comando desenvolvida pela ESET que permite o gerenciamento de produtos Endpoint e a comunicação com qualquer Plug-in RMM.
- O Plug-in RMM é um aplicativo de terceiros sendo executado localmente no sistema Windows Endpoint. O plug-in foi projetado para se comunicar com o Agente RMM específico (por exemplo apenas Kaseya) e com o ermm.exe.
- O Agente RMM é um aplicativo de terceiros (por exemplo da Kaseya) sendo executado localmente no sistema Windows Endpoint. O Agente se comunica com o Plug-in RMM e com o Servidor RMM.

Como bloquear o download de tipos de arquivo

específicos da Internet

Se você não quiser permitir o download de um tipo específico de arquivo (por exemplo exe, pdf ou zip) da internet, use [Gerenciamento de endereços de URL](#) com uma combinação de caracteres curingas. Pressione a tecla F5 para acessar a **Configuração avançada**. Clique em **Web e Email > Proteção de acesso à web** e abra o **Gerenciamento de endereços de URL**. Clique em **Editar** ao lado da **Lista de endereços**.

Na janela da **Lista de endereços**, selecione a **Lista de endereços bloqueados** e clique em **Editar**, ou clique em **Adicionar** para criar uma nova lista. Uma nova janela será aberta. Se você estiver criando uma nova lista, selecione **Bloqueado** no menu suspenso de **Tipo de lista de endereços** e nomeie a lista. Se quiser ser notificado ao acessar um tipo de arquivo da lista atual, ative a barra deslizante **Notificar ao aplicar**. Selecione a **Gravidade de registro em relatório** no menu suspenso. O Administrador remoto pode coletar registros com Detalhamento de **Aviso**.



Editar lista

Tipo de lista de endereços: Bloqueado

Nome da lista: Lista de endereços bloqueados

Descrição da lista:

Listar ativo: ☒

Notificar ao aplicar: ☐

Gravidade do registro em log: Informações

Lista de endereços

- *?.exe
- *.*.zip
- *.*.exe

Adicionar Editar Excluir Importar OK Cancelar

Clique em **Adicionar** para inserir uma máscara que especifica os tipos de arquivo que você quer bloquear do download. Insira o URL inteiro se quiser bloquear o download de um arquivo específico de um site específico, por exemplo *http://example.com/file.exe*. Você pode usar caracteres curinga para abranger um grupo de arquivos. Um ponto de interrogação (?) representa um caractere de variável único e um asterisco (*) representa uma cadeia de caracteres variável, com zero ou mais caracteres. Por exemplo, a máscara **/*.*.zip* bloqueia todos os arquivos comprimidos de zip para o download.

Observe que você pode bloquear o download de tipos de arquivo específicos usando esse método quando a extensão do arquivo fizer parte do URL do arquivo. Se a página da web usar URLs para o download de arquivos, por exemplo, www.example.com/download.php?fileid=42, o download de qualquer arquivo localizado nesse link será feito, mesmo se ele tiver uma extensão que foi bloqueada.

Como minimizar a interface do usuário do ESET Endpoint Security

Quando o gerenciamento for remoto, você pode aplicar uma [política pré-definida de "Visibilidade"](#).

Se não, faça as etapas a seguir manualmente:

1. Pressione **F5** para acessar a Configuração avançada e abra a **Interface do usuário > Elementos da interface do usuário**.
2. Definir o **Modo de inicialização** no valor desejado. [Mais informações sobre modos de inicialização](#).
3. Desativar **Mostrar tela inicial na inicialização** e **Usar sinal sonoro**.
4. Configurar [Notificações](#).
5. Configurar [Status de aplicativo](#).
6. Configurar [Mensagens de confirmação](#).
7. Configurar [Alertas e caixas de mensagens](#).

Como resolver "Não foi possível redirecionar o Navegador protegido para a página da web solicitada"

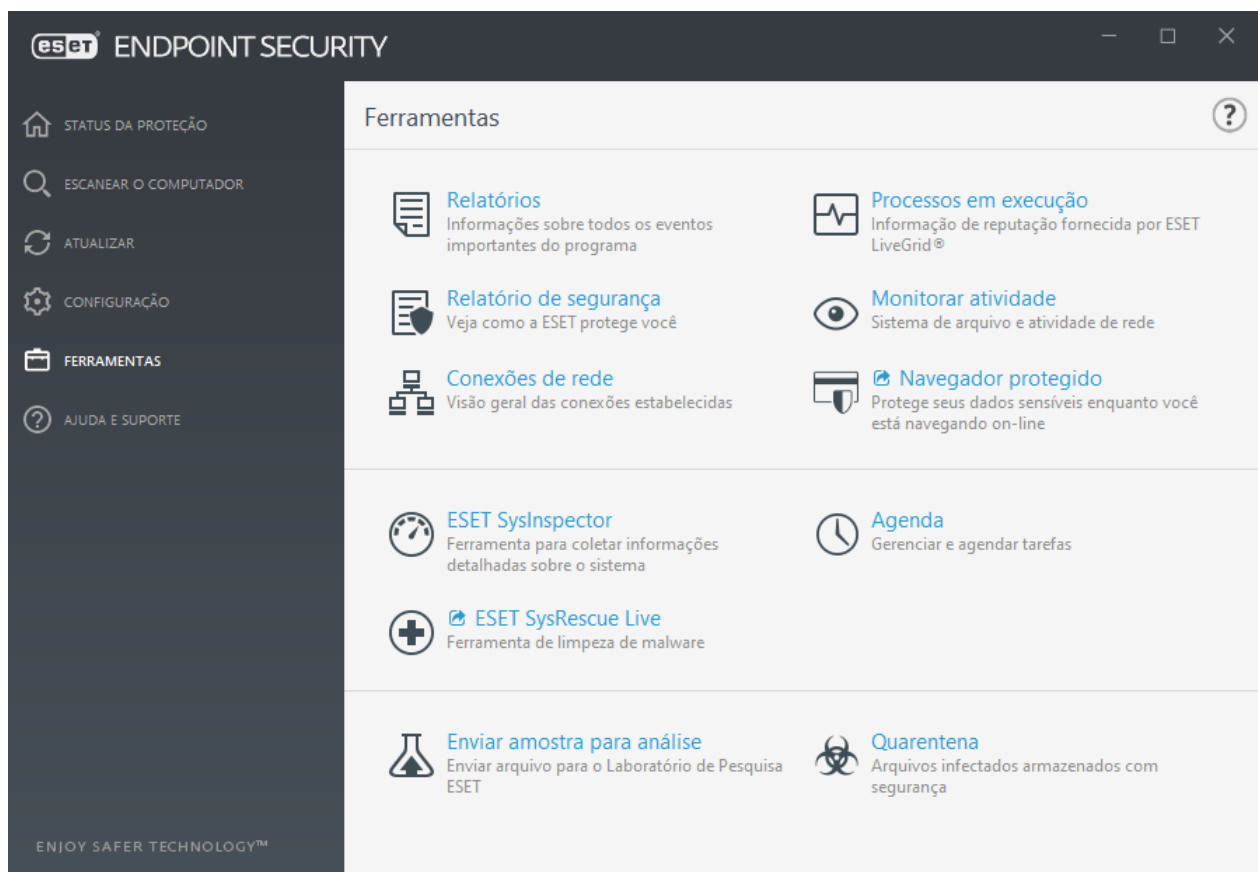
Para resolver esse erro siga as instruções abaixo:

Depois de concluir cada etapa, verifique para ver se o Navegador protegido está funcionando



Se a janela do navegador ainda não estiver funcionando, conclua a próxima etapa até que ela esteja funcionando novamente.


1. Reinicie seu computador.
2. Certifique-se de estar usando a versão mais recente do seu sistema operacional Windows e do seu produto comercial ESET Windows: [Confira a versão mais recente dos seus produtos empresariais ESET](#)



3. Você pode estar experimentando um conflito com seu software de segurança ou firewall de terceiros. Considere a remoção e desinstalação desse software de terceiros na janela Adicionar/Remover programas. Clique em **Ferramentas > Navegador protegido**. Com a janela do Navegador protegido aberta, continue para a próxima etapa.
4. Desativar todas as extensões do navegador de terceiros.
5. Limpe o armazenamento em cache do navegador. Como [limpar o armazenamento em cache do Firefox](#) ou [limpar o armazenamento em cache do Google Chrome](#) no meu navegador?
6. Certifique-se de que seu navegador padrão não está sendo excluído em **Configuração avançada > Web e email > Filtragem de protocolo > Aplicativos excluídos**.
7. Se você não atualizou seu produto ESET nas etapas anteriores, [desinstale e instale novamente seu produto ESET](#). Depois de reiniciar seu computador, [desative o Navegador protegido](#) e reinicie seu computador novamente. Ative de novo o Navegador protegido e tente iniciar a janela do Navegador protegido.

A Navegador protegido é uma camada adicional de proteção projetada para proteger seus dados financeiros durante transações online.

Na maioria dos casos, o Navegador protegido é iniciado no seu navegador padrão depois de você visitar um site de atividade bancária conhecido. Para acessar diretamente o navegador protegido, clique em **Ferramentas** no

ESET Endpoint Security e clique em  **Navegador protegido**.

Para mais detalhes sobre os recursos da Navegador protegido, leia o seguinte artigo na Base de conhecimento ESET disponível em inglês e em vários outros idiomas:

- [Como usar o Navegador protegido ESET?](#)
- [Ativar ou desativar o ESET Proteção para bancos & pagamentos para um site específico](#)
- [Pausar ou desativar a Proteção para bancos & pagamentos nos produtos domésticos ESET Windows](#)

- [Proteção para bancos & pagamentos ESET — erros comuns](#)
 - [Glossário ESET | Proteção para bancos & pagamentos](#)
-

Se você ainda não conseguir resolver o problema, envie um email para o [Suporte técnico da ESET](#).

Acordo de licença de usuário final

Em vigor a partir de 19 de outubro de 2021.

IMPORTANTE: leia atentamente os termos e as condições relativos ao produto estabelecidos a seguir antes do download, da instalação, da cópia ou do uso. **POR MEIO DO DOWNLOAD, DA INSTALAÇÃO, DA CÓPIA OU DO USO DO SOFTWARE, VOCÊ EXPRESSA SEU CONSENTIMENTO COM ESTES TERMOS E CONDIÇÕES E RECONHECE A [POLÍTICA DE PRIVACIDADE](#).**

Acordo de Licença do Usuário Final

Sob os termos deste Contrato de licença para o usuário final ("Contrato") executado por e entre a ESET, spol. s r. o., tendo sua sede em Einsteinova 24, 85101 Bratislava, Slovak Republic, registrada no Registro Comercial do Tribunal Regional de Bratislava I, Seção Sro, Nº de entrada 3586/B, Número de registro da empresa: 31333532 ("ESET" ou "Provedor") e Você, uma pessoa física ou jurídica ("Você" ou "Usuário final"), recebe o direito de uso do Software definido no Artigo 1 deste Contrato. O Software definido no Artigo 1 deste Contrato pode ser armazenado em um carregador de dados, enviado por e-mail, obtido por download da Internet, obtido por download de servidores do Provedor ou obtido de outras fontes, sujeito aos termos e às condições especificados a seguir.

ESTE É UM CONTRATO SOBRE DIREITOS DO USUÁRIO FINAL E NÃO UM CONTRATO DE VENDA. O Provedor permanece o proprietário da cópia de Software e da mídia física fornecida na embalagem comercial e de todas as outras cópias a que o Usuário final tiver direito nos termos deste Contrato.

Ao clicar na opção "Eu aceito" ou "Eu aceito..." durante a instalação, download, cópia ou uso do Software, Você concorda com os termos e condições deste Contrato e reconhece a Política de Privacidade. Se Você não concordar com os termos e as condições deste Contrato e/ou com a Política de Privacidade, clique imediatamente na opção para cancelar, cancele a instalação ou o download, ou destrua ou devolva o Software, a mídia de instalação, a documentação que vem com o produto e o recibo de vendas para o Provedor ou a loja onde Você adquiriu o Software.

VOCÊ CONCORDA QUE SEU USO DO SOFTWARE CONFIRMA QUE VOCÊ LEU ESTE CONTRATO, QUE O COMPREENDEU E CONCORDA EM ESTAR VINCULADO A ELE POR MEIO DE SEUS TERMOS E CONDIÇÕES.

1. Software. Conforme usado neste Contrato, o termo "Software" significa: (i) o programa de computador acompanhado por este Contrato e todos os seus componentes; (ii) todos os conteúdos de discos, CD-ROMs, DVDs, e-mails e anexos, ou outras mídias nas quais este Contrato é fornecido, inclusive o formulário de código de objeto do Software fornecido no transportador de dados, através de correio eletrônico ou baixado na Internet; (iii) qualquer material explicativo por escrito relacionado e qualquer outra documentação possível em relação ao Software, sobretudo qualquer descrição do Software, suas especificações, qualquer descrição das propriedades ou operação do Software, qualquer descrição do ambiente operacional no qual o Software é usado, instruções para o uso ou instalação do Software ou qualquer descrição sobre como usar o Software ("Documentação"); (iv) cópias do Software, patches para possíveis erros no Software, adições ao Software, extensões ao Software, versões modificadas do Software e atualizações de componentes do Software se houverem, são licenciadas a

Você pelo Provedor de acordo com o Artigo 3 deste Contrato. O Software será fornecido exclusivamente na forma de código de objeto executável.

2. Instalação, Computador e uma Chave de Licença. O Software fornecido em um carregador de dados, enviado por email eletrônico, obtido por download da Internet, obtido por download de servidores do Provedor ou obtido de outras fontes requer instalação. Você deve instalar o Software em um Computador configurado corretamente que, pelo menos, esteja de acordo com os requisitos definidos na Documentação. A metodologia de instalação é descrita na Documentação. Nenhum computador ou hardware que possa ter um efeito adverso no Software pode ser instalado no Computador no qual Você instalar o Software. Computer significa hardware, incluindo sem limitação computadores pessoais, notebooks, estações de trabalho, computadores tipo palmtop, smartphones, dispositivos eletrônicos manuais ou outros dispositivos eletrônicos para os quais o Software foi projetado, no qual ele será instalado e/ou usado. Chave de licença significa a sequência exclusiva de símbolos, letras, números ou sinais especiais fornecidos ao Usuário Final para permitir o uso legal do Software, sua versão específica ou extensão do termo da Licença em conformidade com esse Contrato.

3. Licença. Desde que Você tenha concordado com os termos deste Contrato e cumprido com todos os termos e condições estabelecidos neste documento, o Provedor deverá conceder a Você os seguintes direitos ("a Licença"):

a) Instalação e uso. Você deverá ter o direito não exclusivo e não transferível para instalar o Software no disco rígido de um computador ou outra mídia permanente para armazenamento dos dados, instalação e armazenamento do Software na memória de um sistema computacional e para implementar, armazenar e exibir o Software.

b) Estipulação do número de licenças. O direito de utilizar o Software deverá estar vinculado ao número de Usuários finais. Um Usuário final deverá ser selecionado para referir-se ao seguinte: (i) instalação do Software em um sistema computacional; ou (ii) se a extensão de uma licença estiver vinculada ao número de caixas de email, então um Usuário final deverá ser selecionado para referir-se a um usuário de computador que aceita e-mail através de um Agente de usuário de email ("MUA"). Se um MUA aceitar e-mail e, subsequentemente, distribuí-lo de forma automática a vários usuários, então o número de Usuários finais deverá ser determinado de acordo com o número real de usuários para os quais o e-mail será distribuído. Se um servidor de email executar a função de um portal de email, o número de Usuários finais deverá ser igual ao número de servidores de email para o qual esse portal oferece serviços. Se um número não especificado de endereços de emails eletrônicos for direcionado para um usuário e aceito por ele (por exemplo, por meio de alias) e as mensagens não forem automaticamente distribuídas pelo cliente para um número maior de usuários, uma licença para um computador será exigida. Você não deve usar a mesma Licença ao mesmo tempo em mais de um computador. O Usuário Final tem o direito de inserir a Chave de Licença para o Software apenas até a extensão em que o Usuário Final tem o direito de usar o Software de acordo com a limitação criada pelo número de Licenças oferecido pelo Provedor. A Chave de licença é considerada confidencial, Você não deve compartilhar a Licença com terceiros ou permitir que terceiros usem a Chave de licença a menos que isso seja permitido por esse Contrato ou pelo Provedor. Se sua Chave de licença for comprometida, notifique o Provedor imediatamente.

c) Home/Business Edition. Uma versão Home Edition do Software será usada exclusivamente em ambientes particulares e/ou não comerciais apenas para uso familiar e doméstico. Uma versão Business Edition do Software deve ser obtida para uso em ambiente comercial, assim como para usar o Software em servidores de e-mail, relés de e-mail, gateways de e-mail ou gateways de Internet.

d) Vigência da licença. O direito de utilizar o Software deverá estar limitado a um período.

e) Software OEM. O Software classificado como "OEM" deve estar limitado ao Computador com o qual Você obteve o software. Ele não pode ser transferido para um computador diferente.

f) Software NFR, AVALIAÇÃO. Software classificado como "Não para revenda", NFR ou AVALIAÇÃO não pode ser

atribuído para pagamento e deve ser usado apenas para demonstração ou teste dos recursos do Software.

g) Término da licença. A Licença deverá terminar automaticamente no final do período para o qual ela foi concedida. Se Você deixar de cumprir qualquer das cláusulas deste Contrato, o Provedor terá o direito de retirar-se do Contrato, sem prejuízo de qualquer direito ou solução jurídica abertos ao Provedor em tais eventualidades. No caso de cancelamento da Licença, Você deve excluir, destruir ou devolver imediatamente, às suas custas, o Software e todas as cópias de backup para a ESET ou loja em que Você obteve o Software. Mediante a rescisão da Licença o Provedor também estará autorizado a cancelar o direito do Usuário Final de usar as funções do Software que exigem conexão aos servidores do Provedor ou servidores de terceiros.

4. Funções com coleta de dados e requisitos de conexão com a internet. Para operar corretamente, o Software exige conexão com a Internet e deve conectar-se em intervalos regulares aos servidores do Provedor ou a servidores de terceiros e a coleta de dados aplicáveis de acordo com a Política de Privacidade. A conexão com a Internet e coleta de dados aplicáveis é necessária para os seguintes recursos do Software:

a) Atualizações para o Software. O Provedor deverá, de tempos em tempos, 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.

b) Encaminhamento de infiltrações e informações ao Provedor. O Software contém funções que coletam amostras de vírus de computador e outros programas maliciosos de computador e objetos suspeitos, problemáticos, potencialmente indesejados ou potencialmente inseguros como arquivos, URLs, pacotes de IP e quadros de ethernet ("Infiltrações") e então envia-os ao Provedor, incluindo mas não limitado a informações sobre o processo de instalação, o Computador e/ou a plataforma na qual o Software está instalado, e informações sobre as operações e funcionalidades do Software (as "Informações"). As Informações e Infiltrações podem conter dados (inclusive dados pessoais obtidos de forma aleatória ou acidental) sobre o Usuário Final ou outros usuários do computador no qual o Software está instalado, e arquivos afetados por Infiltrações com os metadados associados.

Informação e Infiltrações podem ser coletadas pela funções de Software a seguir:

i. A função do Sistema de Reputação LiveGrid inclui a coleta e envio de hashes unidirecionais relacionadas a Infiltrações para o Provedor. Esta função é ativada nas configurações padrão do software.

ii. A função do Sistema de Feedback LiveGrid inclui a coleta e envio de Infiltrações com metadados e Informação associados para o Provedor. Esta função pode ser ativada pelo usuário final durante o processo de instalação do Software.

O Provedor deverá usar apenas as Informações e Infiltrações recebidas para o objetivo de análise e pesquisa de infiltrações, melhoria de Software e verificação de autenticidade da Licença, e deverá tomar as medidas adequadas para garantir que as Infiltrações e Informações recebidas permaneçam seguras. Ao ativar esta função do Software, Infiltrações e Informações podem ser coletadas e processadas pelo Provedor como especificado na Política de Privacidade e de acordo com os regulamentos legais relevantes. Estas funções podem ser desativadas a qualquer momento.

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 contrárium.

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 importadas 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.

EULAID: EULA-PRODUCT-LG; 3537.0

Política de Privacidade

ESET, spol. s r. o., com sede em Einsteinova 24, 851 01 Bratislava, República Eslovaca, registrada no Registro Comercial administrado pela Corte Distrital Bratislava I, Seção Sro, Registro Nº. 3586/B, Número de Registro Comercial: 31333532 como o Controlador de Dados ("ESET" ou "Nós") deseja ser transparente quando ao processamento de dados pessoais e privacidade de nossos clientes. Para isso, estamos publicando essa Política de Privacidade com o objetivo exclusivo de informar nosso cliente ("Usuário Final" ou "Você") sobre os tópicos a seguir:

- Processamento de dados pessoais,
- Confidencialidade de Dados,
- Direitos do sujeito dos dados.

Processamento de dados pessoais

Serviços prestados pela ESET e implementados em nosso produto são fornecidos sob os termos do Acordo de Licença para o Usuário Final ("EULA"), mas alguns deles podem precisar de atenção específica. Gostaríamos de fornecer a Você mais detalhes sobre a coleta de dados em relação à prestação de nossos serviços. Nós prestamos vários serviços descritos no EULA e na documentação de produtos como o serviço de atualização, ESET LiveGrid®, proteção contra o uso errôneo de dados, suporte, etc. Para que tudo funcione, precisamos coletar as informações a seguir:

- Atualização e outras estatísticas cobrindo informações sobre o processo de instalação e seu computador, incluindo a plataforma na qual seu produto está instalado e informações sobre as operações e funcionalidades de seus produtos, como o sistema operacional, informações de hardware, IDs de instalação, ID de licença, endereço IP, endereço MAC, definições de configuração do produto.
- Hashes de via única relacionados a infiltrações como parte do sistema de reputação do ESET LiveGrid® que melhora a eficiência de nossas soluções anti-malware ao comparar os arquivos escaneados com um banco de dados de itens na lista de proibições e permissões da nuvem.
- Amostras suspeitas e metadados originais como parte do Sistema de Feedback ESET LiveGrid® permite que a ESET reaja imediatamente às necessidades de nossos usuários finais e nos mantém sensível às ameaças mais recentes. Nós dependemos de Você enviando

o infiltrações como amostras potenciais de vírus e outros programas nocivos e suspeitos; objetos problemáticos, potencialmente indesejados ou potencialmente inseguros como arquivos executáveis, mensagens de email reportadas por Você como spam ou marcadas pelo nosso produto;

- informações sobre dispositivos na rede local como tipo, fornecedor, modelo e/ou nome do dispositivo;
- informações sobre o uso da internet como endereço IP e informações geográficas, pacotes de IP, URL e quadros ethernet;
- arquivos de despejo de parada e informações contidas neles.

Não queremos coletar seus dados além desse escopo, mas isso pode ser impossível de impedir algumas vezes. Dados coletados acidentalmente podem estar incluídos no próprio malware (coletados sem seu conhecimento ou aprovação) ou como parte de nomes de arquivos ou URL e não pretendemos que eles façam parte de nossos sistemas ou processos para os fins declarados nessa Política de Privacidade.

- 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 email, 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.

Confidencialidade de dados

A ESET é uma empresa que opera no mundo todo através de entidades afiliadas ou parceiros como parte de nossa rede de distribuição, serviço e suporte. Informações processadas pela ESET podem ser transferidas de e para entidades afiliadas ou parceiros para o desempenho do Acordo de Licença para o usuário final, como o fornecimento de serviços ou suporte ou cobrança. Com base em sua localização e no serviço que Você escolhe usar, Nós podemos precisar transferir seus dados para um país que não tenha uma decisão de adequação pela Comissão Europeia. Mesmo nesse caso, toda transferência de informação está sujeita a uma regulação de legislação de proteção de dados e acontece apenas se for necessária. Cláusulas Contratuais Padrão, Regras Corporativas Vinculantes ou outra proteção adequada deve ser estabelecida sem exceção.

Estamos fazendo nosso melhor para impedir que os dados sejam armazenados por mais tempo do que o necessário enquanto fornecemos produtos e serviços sob o Acordo de Licença para o usuário final. Nosso período de retenção pode ser mais longo do que a validade de sua licença, apenas para dar a você um tempo para fazer a renovação de forma fácil e confortável. Estatísticas minimizadas e com pseudônimos e outros dados do ESET LiveGrid® podem ser processados ainda mais para fins estatísticos.

A ESET implementa medidas técnicas e organizacionais adequadas para garantir um nível de segurança que seja apropriado para os riscos potenciais. Estamos fazendo nosso melhor para garantir a confidencialidade, integridade, disponibilidade e resiliência constante de sistemas de processamento e serviços. Porém, em caso de violação de dados resultando em um risco aos seus direitos e liberdades, estamos prontos para notificar uma autoridade supervisora assim como os sujeitos dos dados. Como um sujeito de dados, Você tem o direito de enviar uma queixa à autoridade supervisora.

Direitos do sujeito dos dados

A ESET é sujeita ao regulamento das leis eslovacas e estamos vinculados pela legislação de proteção de dados como parte da União Europeia. Sujeito às condições estabelecidas pelas leis aplicáveis de proteção de dados, Você tem o direito ao seguinte como um titular dos dados:

- o direito de solicitar acesso aos seus dados pessoais da ESET,
- direito a uma retificação dos seus dados pessoais se estiverem incorretos (Você também tem o direito de

completar dados pessoais incompletos),

- direito de solicitar que seus dados pessoais sejam apagados,
- direito de solicitar a restrição do processamento de seus dados pessoais
- direito a uma objeção ao processamento
- direito a fazer uma queixa assim como o
- direito à portabilidade de dados.

Acreditamos que todas as informações que processamos são valiosas e necessárias para os fins de nossos interesses legítimos, que são o oferecimento de serviços e produtos aos nossos clientes.

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