

# ESET NOD32 Antivirus

## Guia do Usuário

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

Direitos autorais ©2023 por ESET, spol. s r.o.

ESET NOD32 Antivirus 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. 19-03-2023

<b>1 ESET NOD32 Antivirus</b> .....	<b>1</b>
<b>1.1 O que há de novo?</b> .....	<b>2</b>
<b>1.2 Qual produto eu tenho?</b> .....	<b>2</b>
<b>1.3 Requisitos do sistema</b> .....	<b>3</b>
1.3 Sua versão do Windows 7 está desatualizada .....	4
1.3 O Windows 7 não é mais compatível com a Microsoft .....	4
1.3 O Windows Vista não é mais compatível .....	5
<b>1.4 Prevenção</b> .....	<b>5</b>
<b>1.5 Páginas de ajuda</b> .....	<b>6</b>
<b>2 Instalação</b> .....	<b>8</b>
<b>2.1 Instalador Live</b> .....	<b>8</b>
<b>2.2 Instalação off-line</b> .....	<b>9</b>
<b>2.3 Ativação do produto</b> .....	<b>11</b>
2.3 Digitando sua chave de licença durante a ativação .....	12
2.3 Usar ESET HOME conta .....	12
2.3 Ativar a licença de avaliação .....	13
2.3 Chave de licença ESET gratuita .....	14
2.3 Falha na ativação - cenários comuns .....	15
2.3 Falha na ativação devido a uma licença usada em excesso .....	15
2.3 Atualização da licença .....	16
2.3 Atualização do produto .....	17
2.3 Downgrade da licença .....	17
2.3 Downgrade do produto .....	18
<b>2.4 Solução de problemas de instalação</b> .....	<b>19</b>
<b>2.5 Primeiro rastreamento depois da instalação</b> .....	<b>19</b>
<b>2.6 Atualização para uma versão mais recente</b> .....	<b>20</b>
2.6 Atualização automática de produto legado .....	21
<b>2.7 Indicando um produto ESET para um amigo</b> .....	<b>21</b>
2.7 ESET NOD32 Antivirus será instalado .....	22
2.7 Alterar para uma linha de produtos diferente .....	22
2.7 Registro .....	22
2.7 Progresso da ativação .....	22
2.7 Ativação bem-sucedida .....	22
<b>3 Guia do iniciante</b> .....	<b>23</b>
<b>3.1 Conectar ao ESET HOME</b> .....	<b>23</b>
3.1 Entrar no ESET HOME .....	24
3.1 Falha ao entrar - erros comuns .....	25
3.1 Adicionar dispositivo em ESET HOME .....	26
<b>3.2 Janela do programa principal</b> .....	<b>26</b>
<b>3.3 Atualizações</b> .....	<b>29</b>
<b>4 Trabalhando com o ESET NOD32 Antivirus</b> .....	<b>30</b>
<b>4.1 Proteção do computador</b> .....	<b>32</b>
4.1 Mecanismo de detecção .....	33
4.1 Opções avançadas do mecanismo de detecção .....	38
4.1 Uma infiltração foi detectada .....	38
4.1 Proteção em tempo real do sistema de arquivos .....	40
4.1 Níveis de limpeza .....	42
4.1 Quando modificar a configuração da proteção em tempo real .....	43
4.1 Verificação da proteção em tempo real .....	43
4.1 O que fazer se a proteção em tempo real não funcionar .....	43

4.1 Exclusões de processos .....	44
4.1 Adicionar ou editar exclusões de processos .....	45
4.1 Proteção baseada em nuvem .....	45
4.1 Filtro de exclusões para Proteção baseada em nuvem .....	48
4.1 Escanear o computador .....	48
4.1 Iniciador de rastreamento personalizado .....	51
4.1 Progresso do rastreamento .....	52
4.1 Relatório de rastreamento do computador .....	54
4.1 Escaneamento de malware .....	56
4.1 Escaneamento em estado ocioso .....	56
4.1 Perfis de rastreamento .....	57
4.1 Alvos de rastreamento .....	58
4.1 Controle de dispositivo .....	58
4.1 Editor de regras do controle de dispositivos .....	59
4.1 Dispositivos detectados .....	60
4.1 Grupos do dispositivo .....	61
4.1 Adição de regras do controle de dispositivos .....	62
4.1 Sistema de prevenção de intrusos de host (HIPS) .....	64
4.1 Janela interativa HIPS .....	66
4.1 Comportamento de ransomware em potencial detectado .....	68
4.1 Gerenciamento de regras de HIPS .....	69
4.1 Configurações de regra HIPS .....	70
4.1 Adicionar caminho de registro/aplicativo para HIPS .....	73
4.1 Configuração avançada HIPS .....	73
4.1 Drivers sempre com permissão para carregar .....	74
4.1 Modo jogador .....	74
4.1 Rastreamento na inicialização .....	74
4.1 Rastreamento de arquivos em execução durante inicialização do sistema .....	75
4.1 Proteção de documentos .....	76
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 .....	82
4.1 Criar assistente de detecção de exclusão .....	83
4.1 Exclusões HIPS .....	84
4.1 Parâmetros ThreatSense .....	84
4.1 Extensões de arquivo excluídas do rastreamento .....	88
4.1 Parâmetros adicionais do ThreatSense .....	88
<b>4.2 Proteção de internet .....</b>	<b>89</b>
4.2 Filtragem de protocolos .....	90
4.2 Aplicativos excluídos .....	91
4.2 Endereços IP excluídos .....	92
4.2 Adicionar endereço IPv4 .....	93
4.2 Adicionar endereço IPv6 .....	93
4.2 SSL/TLS .....	93
4.2 Certificados .....	95
4.2 Tráfego de rede criptografado .....	95
4.2 Lista de certificados conhecidos .....	96
4.2 Lista de aplicativos SSL/TLS filtrados .....	97

4.2 Proteção do cliente de email .....	97
4.2 Integração com clientes de email .....	98
4.2 Barra de ferramentas do Microsoft Outlook .....	98
4.2 Barra de ferramentas do Outlook Express e do Windows Mail .....	99
4.2 Caixa de diálogo de confirmação .....	99
4.2 Rastrear novamente mensagens .....	99
4.2 Protocolos de email .....	100
4.2 Filtro POP3, POP3S .....	101
4.2 Marcações de e-mail .....	102
4.2 Proteção do acesso à Web .....	102
4.2 Configuração avançada de proteção de acesso à web .....	105
4.2 Protocolos da Web .....	105
4.2 Gerenciamento de endereços de URL .....	106
4.2 Lista de endereços URL .....	107
4.2 Criar nova lista de endereços de URL .....	108
4.2 Como adicionar uma máscara de URL .....	109
4.2 Proteção antiphishing .....	109
<b>4.3 Atualização do programa .....</b>	<b>111</b>
4.3 Configuração da atualização .....	114
4.3 Atualização de rollback .....	116
4.3 Intervalo de tempo de reversão .....	118
4.3 Atualizações de produto .....	118
4.3 Opção de conexão .....	118
4.3 Como criar tarefas de atualização .....	119
4.3 Janela de diálogo - Reinicialização necessária .....	120
<b>4.4 Ferramentas .....</b>	<b>120</b>
4.4 Ferramentas no ESET NOD32 Antivirus .....	120
4.4 Relatórios .....	121
4.4 Filtragem de relatórios .....	123
4.4 Configuração do registro em relatório .....	125
4.4 Processos em execução .....	126
4.4 Relatório de segurança .....	128
4.4 ESET SysInspector .....	129
4.4 Agenda .....	130
4.4 Opções de escaneamento programado .....	133
4.4 Visão geral da tarefa agendada .....	134
4.4 Detalhes da tarefa .....	134
4.4 Tempo da tarefa .....	134
4.4 Tempo da tarefa - única .....	135
4.4 Tempo da tarefa - diária .....	135
4.4 Tempo da tarefa - semanal .....	135
4.4 Tempo da tarefa - acionada por evento .....	135
4.4 Tarefa ignorada .....	135
4.4 Detalhes da tarefa - atualizar .....	136
4.4 Detalhes da tarefa - executar aplicativo .....	136
4.4 Limpeza do sistema .....	137
4.4 ESET SysRescue Live .....	138
4.4 Quarentena .....	138
4.4 Servidor proxy .....	141
4.4 Selecionar amostra para análise .....	142
4.4 Selecionar amostra para análise - Arquivo suspeito .....	143

4.4 Selecionar amostra para análise - Site suspeito .....	143
4.4 Selecionar amostra para análise - Arquivo falso positivo .....	144
4.4 Selecionar amostra para análise - Site falso positivo .....	144
4.4 Selecionar amostra para análise - Outras .....	144
4.4 Microsoft Windows® update .....	145
4.4 Janela de diálogo - Atualizações do sistema .....	145
4.4 Atualizar informações .....	145
<b>4.5 Interface do usuário .....</b>	<b>145</b>
4.5 Elementos da interface do usuário .....	146
4.5 Configuração de acesso .....	147
4.5 Senha para Configuração avançada .....	147
4.5 Ícone da bandeja do sistema .....	148
4.5 Compatibilidade com leitor de tela .....	149
4.5 Ajuda e suporte .....	149
4.5 Sobre o ESET NOD32 Antivirus .....	150
4.5 Notícias ESET .....	151
4.5 Enviar dados de configuração do sistema .....	151
4.5 Suporte técnico .....	152
<b>4.6 Notificações .....</b>	<b>152</b>
4.6 Janela de diálogo - status de aplicativo .....	153
4.6 Notificações na área de trabalho .....	153
4.6 Lista de notificações na área de trabalho .....	155
4.6 Alertas interativos .....	156
4.6 Mensagens de confirmação .....	158
4.6 Mídia removível .....	159
4.6 Encaminhamento .....	160
<b>4.7 Configurações de privacidade .....</b>	<b>162</b>
<b>4.8 Perfis .....</b>	<b>163</b>
<b>4.9 Atalhos do teclado .....</b>	<b>164</b>
<b>4.10 Diagnóstico .....</b>	<b>165</b>
4.10 Suporte técnico .....	166
4.10 Importar e exportar configurações .....	167
4.10 Reverter todas as configurações na seção atual .....	167
4.10 Reverter para configurações padrão .....	168
4.10 Erro ao salvar a configuração .....	168
<b>4.11 Análise da linha de comandos .....</b>	<b>168</b>
<b>4.12 ESET CMD .....</b>	<b>171</b>
<b>4.13 Detecção em estado ocioso .....</b>	<b>172</b>
<b>5 Dúvidas comuns .....</b>	<b>173</b>
<b>5.1 Como atualizar o ESET NOD32 Antivirus .....</b>	<b>173</b>
<b>5.2 Como remover um vírus do meu PC .....</b>	<b>174</b>
<b>5.3 Como criar uma nova tarefa na Agenda .....</b>	<b>174</b>
<b>5.4 Como agendar um escanear semanal do computador .....</b>	<b>175</b>
<b>5.5 Como desbloquear a Configuração avançada .....</b>	<b>175</b>
<b>5.6 Como resolver a desativação do produto do ESET HOME .....</b>	<b>176</b>
5.6 Produto desativado, dispositivo desconectado .....	176
5.6 O produto não está ativado .....	177
<b>6 Programa de melhoria da experiência do cliente .....</b>	<b>177</b>
<b>7 Acordo de licença de usuário final .....</b>	<b>178</b>
<b>8 Política de Privacidade .....</b>	<b>189</b>

# ESET NOD32 Antivirus

O ESET NOD32 Antivirus representa uma nova abordagem para a segurança do computador verdadeiramente integrada. A versão mais recente do mecanismo de rastreamento ESET LiveGrid® utiliza velocidade e precisão para manter a segurança do seu computador. 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 NOD32 Antivirus é uma solução de segurança completa que combina proteção máxima e impacto mínimo no sistema. Nossas tecnologias avançadas usam inteligência artificial para impedir infiltração por vírus, spywares, cavalos de troia, worms, adwares, rootkits e outras ameaças sem prejudicar o desempenho do sistema ou interromper a atividade do computador.

## Recursos e benefícios

<b>Interface do usuário com novo design</b>	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 NOD32 Antivirus e oferece um conteúdo de suporte dinamicamente atualizado.
<b>Antivírus e antispyware</b>	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).
<b>Atualizações regulares</b>	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.
<b>ESET LiveGrid® (Reputação potencializada pela nuvem)</b>	Você pode verificar a reputação dos arquivos e dos processos em execução diretamente do ESET NOD32 Antivirus.
<b>Controle de dispositivo</b>	Rastreia automaticamente todas as unidades flash USB, cartões de memória e CDs/DVDs. Bloqueia mídia removível com base no tipo de mídia, fabricante, tamanho e outros atributos.
<b>Funcionalidade do HIPS</b>	Você pode personalizar o comportamento do sistema em mais detalhes; especifique regras para o registro do sistema, processos e programas ativos e ajuste sua postura de segurança.
<b>Modo jogador</b>	Adia todas as janelas pop-up, atualizações ou outras atividades que exijam muitos recursos do sistema, a fim de conservar recursos do sistema para jogos e outras atividades de tela inteira.

Uma licença precisa estar ativa para que os recursos do ESET NOD32 Antivirus estejam operacionais. Recomendase que você renove sua licença várias semanas antes de a licença do ESET NOD32 Antivirus expirar.

# O que há de novo?

## Novidades do ESET NOD32 Antivirus 15

### ESET HOME (anteriormente myESET)

Fornecer maior visibilidade e controle sobre sua segurança. Instale a proteção para novos dispositivos, adicione e compartilhe licenças e receba notificações importantes através do aplicativo móvel e do portal da web. Para mais informações, visite o [ESET HOME Guia de Ajuda on-line](#).

### Sistema de prevenção de intrusos de host (HIPS) aprimorado

Escaneia a memória que pode ser modificada por técnicas sofisticadas de injeção de malware. As melhorias estendem sua capacidade de detectar intrusos de malware mais sofisticados.

---

Para imagens e informações adicionais sobre os novos recursos no ESET NOD32 Antivirus, veja [Novidades na versão mais recente dos produtos domésticos da ESET](#).



Para desativar as notificações de **Novidades**, clique em **Configuração avançada > Notificações > Notificações da área de trabalho**. Clique em **Editar** ao lado de **Notificações na área de trabalho** e desmarque a caixa de seleção **Exibir notificações de novidades**. Para mais informações sobre notificações, consulte a seção [Notificações](#).

## Qual produto eu tenho?

A ESET oferece várias camadas de segurança com novos produtos, desde solução antivírus potente e rápida até uma solução de segurança tudo-em-um com pegada mínima no sistema:

- ESET NOD32 Antivirus
- ESET Internet Security
- ESET Smart Security Premium

Para determinar qual produto você instalou abra a [janela principal do programa](#) e você verá o nome do produto na parte superior da janela (veja o [artigo da Base de Conhecimento](#)).

---

A tabela abaixo detalha os recursos disponíveis em cada produto específico.

	ESET NOD32 Antivirus	ESET Internet Security	ESET Smart Security Premium
Mecanismo de detecção	✓	✓	✓
Aprendizado de máquina avançado	✓	✓	✓
Bloqueio de Exploit	✓	✓	✓
Proteção contra ataque baseado em script	✓	✓	✓
Antiphishing	✓	✓	✓

	ESET NOD32 Antivírus	ESET Internet Security	ESET Smart Security Premium
Proteção do acesso à Web	✓	✓	✓
HIPS (incluindo Escudo Anti-ransomware)	✓	✓	✓
Antispam		✓	✓
Firewall		✓	✓
Inspetor de rede		✓	✓
Proteção da webcam		✓	✓
Proteção contra ataque de rede		✓	✓
Proteção contra botnet		✓	✓
Proteção para bancos & pagamentos		✓	✓
Controle dos pais		✓	✓
Antifurto		✓	✓
Password Manager			✓
ESET Secure Data			✓
ESET LiveGuard			✓

 Alguns dos produtos acima podem não estar disponíveis para o seu idioma/região.

## Requisitos do sistema

Seu sistema deve atender aos seguintes requisitos de hardware e software para executar o ESET NOD32 Antivírus de forma otimizada:

### 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 compatíveis\*

Microsoft® Windows® 11

Microsoft® Windows® 10

Microsoft® Windows® 8.1

Microsoft® Windows® 8

[Microsoft® Windows® 7 SP1 com as atualizações do Windows mais recentes](#)

Microsoft® Windows® Home Server 2011 64-bit

 Sempre tente manter seu sistema operacional atualizado.

### Outros

É preciso ter uma conexão com a internet para que a ativação e as atualizações do ESET NOD32 Antivírus funcionem adequadamente.

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.

\* A ESET não pode fornecer proteção para sistemas operacionais incompatíveis desde de fevereiro de 2021.

## Sua versão do Windows 7 está desatualizada

### Problema

Você está executando uma versão desatualizada do sistema operacional. Para manter-se protegido, sempre tente manter o sistema operacional atualizado.

### Solução

Você instalou o ESET NOD32 Antivirus sendo executado no {GET\_OSNAME} {GET\_BITNESS}.

Verifique se você instalou o Windows 7 Service Pack 1 (SP1) com as atualizações do Windows mais recentes (no mínimo [KB4474419](#) e [KB4490628](#)).

Se o seu Windows 7 não estiver configurado para ser atualizado automaticamente, clique no **Menu Iniciar > Painel de controle > Sistema e segurança > Windows Update > Verificar se há atualizações** e clique em **Instalar atualizações**.

Consulte também [O Windows 7 não é mais compatível com a Microsoft](#).

## O Windows 7 não é mais compatível com a Microsoft

### Problema

A compatibilidade da Microsoft para o Windows 7 terminou em 14 de janeiro de 2020. [O que isso significa?](#)

Se você continuar a usar o Windows 7 após o término da compatibilidade seu PC continuará funcionando, mas poderá se tornar mais vulnerável a riscos de segurança e vírus. Seu PC não receberá mais atualizações do Windows (incluindo atualizações de segurança).

### Solução

#### Está atualizando do Windows 7 para o Windows 10? Atualizar seu produto ESET

O processo de atualização é relativamente fácil e, em muitos casos, ele pode ser feito sem perder os arquivos. Antes de atualizar para o Windows 10:

1. [Verifique/atualize seu produto ESET](#)
2. Backup de dados importantes
3. Leia as [Perguntas frequentes da atualização para o Windows 10](#) da Microsoft e atualize seu sistema operacional Windows

## Obtendo um novo computador ou dispositivo? Transfira o produto ESET

Se você vai comprar ou já comprou um novo computador ou dispositivo, aprenda a [transferir seu produto ESET para um novo dispositivo](#).

**i** Veja também que o [Suporte para o Windows 7 chegou ao fim](#).

# O Windows Vista não é mais compatível

## Problema

Devido a limitações técnicas no Windows Vista, o ESET NOD32 Antivirus não poderá fornecer proteção depois de **fevereiro de 2021**. O produto ESET se tornará **não funcional**. Isso pode fazer com que seu sistema fique vulnerável a infiltrações.

O suporte da Microsoft para o Windows Vista terminou em 11 de abril de 2017. [O que isso significa?](#)

Se você continuar a usar o Windows Vista após o término da compatibilidade seu PC continuará funcionando, mas poderá se tornar mais vulnerável a riscos de segurança e vírus. Seu PC não receberá mais atualizações do Windows (incluindo atualizações de segurança).

## Solução

### Está atualizando do Windows Vista para o Windows 10? Obtenha um novo computador ou dispositivo e transfira o produto ESET

Antes de atualizar para o Windows 10:

1. Backup de dados importantes
2. Leia as [Perguntas frequentes da atualização para o Windows 10](#) da Microsoft e atualize seu sistema operacional Windows
3. Instale ou [transfira seu produto ESET existente para um novo dispositivo](#).

**i** Veja também que o [Suporte para o Windows Vista chegou ao fim](#).

## 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 pesquisa 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 a 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 ao guia do usuário ESET NOD32 Antivirus. As informações fornecidas aqui ajudarão você a se familiarizar com o produto e ajudar a tornar o computador mais seguro.

# Introdução

Antes de usar o ESET NOD32 Antivirus, recomendamos que você se familiarize com os vários [tipos de detecções](#) e [ataques remotos](#) que pode encontrar ao usar seu computador.

Também compilamos uma lista de [novos recursos](#) introduzidos no ESET NOD32 Antivirus, e um guia para ajudá-lo a definir as configurações básicas.

## Como usar as páginas de ajuda do ESET NOD32 Antivirus

Os tópicos de ajuda estão divididos em vários capítulos e sub-capítulos. Pressione **F1** para exibir informações sobre a janela onde você está.

O programa permite pesquisar por um tópico de ajuda pela(s) palavra(s)-chave(s) ou pesquisar pelo conteúdo 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 no texto real.

Para fins de coerência e para evitar a confusão, a terminologia utilizada ao longo deste guia é baseada nos nomes de parâmetro do ESET NOD32 Antivirus. 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
<b>Tipo negrito</b>	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.
<a href="#">Hyperlink</a>	Fornecer acesso rápido e fácil aos tópicos de referência cruzada ou locais externos da Web. Hyperlinks são destacados em azul e podem ser sublinhados.
<code>%ProgramFiles%</code>	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.

# Instalação

Há vários métodos para a instalação do ESET NOD32 Antivírus em seu computador. Os métodos de instalação podem variar dependendo do país e meio de distribuição:

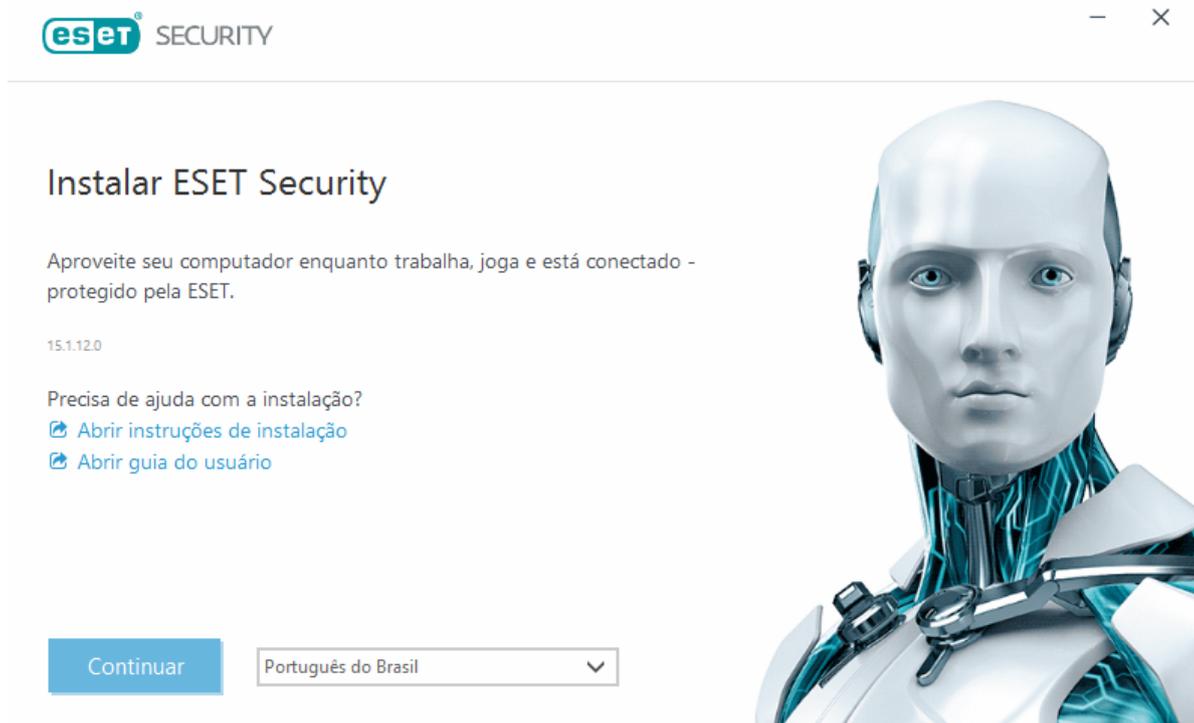
- [Instalador](#) – o download é feito do site da ESET ou do CD/DVD. O pacote de instalação é universal para todos os idiomas (escolha o idioma adequado). O Instalador é um arquivo pequeno; arquivos adicionais necessários para instalar o ESET NOD32 Antivírus são baixados automaticamente.
- [Instalação off-line](#) – usa um arquivo .exe maior do que o arquivo do Instalador e não precisa de uma conexão com a internet ou arquivos adicionais para concluir a instalação.

Verifique se não há algum outro programa antivírus instalado no computador antes de instalar o ESET NOD32 Antivírus. 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 da ESET](#) para obter uma lista de ferramentas de desinstalação para os softwares de antivírus comuns (disponível em inglês e vários outros idiomas).

## Instalador Live

Depois de ter feito o download do [Pacote de instalação do Instalador](#) clique duas vezes no arquivo de instalação e siga as instruções passo a passo na janela do Assistente do instalador.

! Para esse tipo de instalação, você deverá estar conectado à Internet.



1. Selecione o idioma adequado no menu suspenso e clique em **Continuar**.

**i** Se você estiver instalando uma versão mais recente sobre a versão anterior com as configurações protegidas por senha, digite sua senha. Você pode configurar a senha de configuração na [Configuração de acesso](#).

2. Selecione sua preferência para os recursos a seguir, leia o [Acordo de licença para o usuário final](#) e a [Política de Privacidade](#) e clique em **Continuar**, ou clique em **Permitir tudo e continuar** para ativar todos os recursos:

- [sistema de feedback ESET LiveGrid®](#)
- [Aplicativos potencialmente indesejados](#)
- [Programa de melhoria da experiência do cliente](#)

**i** Ao clicar em **Continuar** ou **Permitir tudo e continuar**, você aceita o Acordo de Licença para o Usuário Final e reconhece a Política de Privacidade.

3. Para ativar, gerenciar e visualizar a segurança do dispositivo usando o ESET HOME, [conecte seu dispositivo à conta ESET HOME](#). Clique em **Ignorar login** para continuar sem conectar ao ESET HOME. Você pode [conectar seu dispositivo à sua conta ESET HOME](#) mais tarde.

4. Se você continuar sem se conectar o ESET HOME, escolha uma [opção de ativação](#). Se você estiver instalando uma versão mais recente em uma versão anterior, sua Chave de licença será inserida automaticamente.

5. O Assistente de instalação determina qual produto ESET está instalado com base na sua licença. A versão com mais recursos de segurança é sempre pré-selecionada. Clique em **Alterar produto** se quiser [instalar uma versão diferente do produto ESET](#). Clique em **Continuar** para iniciar o processo de instalação. Pode levar alguns momentos.

**i** Se houver algo remanescente (arquivos ou pastas) dos produtos ESET desinstalados no passado, você será solicitado a permitir a remoção deles. Clique em **Instalar** para continuar.

6. Clique em **Concluído** para sair do Assistente de instalação.

### **!** [Solução de problemas de instalação.](#)

**i** Depois do produto ser instalado e ativado, os módulos vão iniciar o download. A proteção está sendo inicializada e alguns recursos podem não ser totalmente funcionais a menos que o download seja concluído.

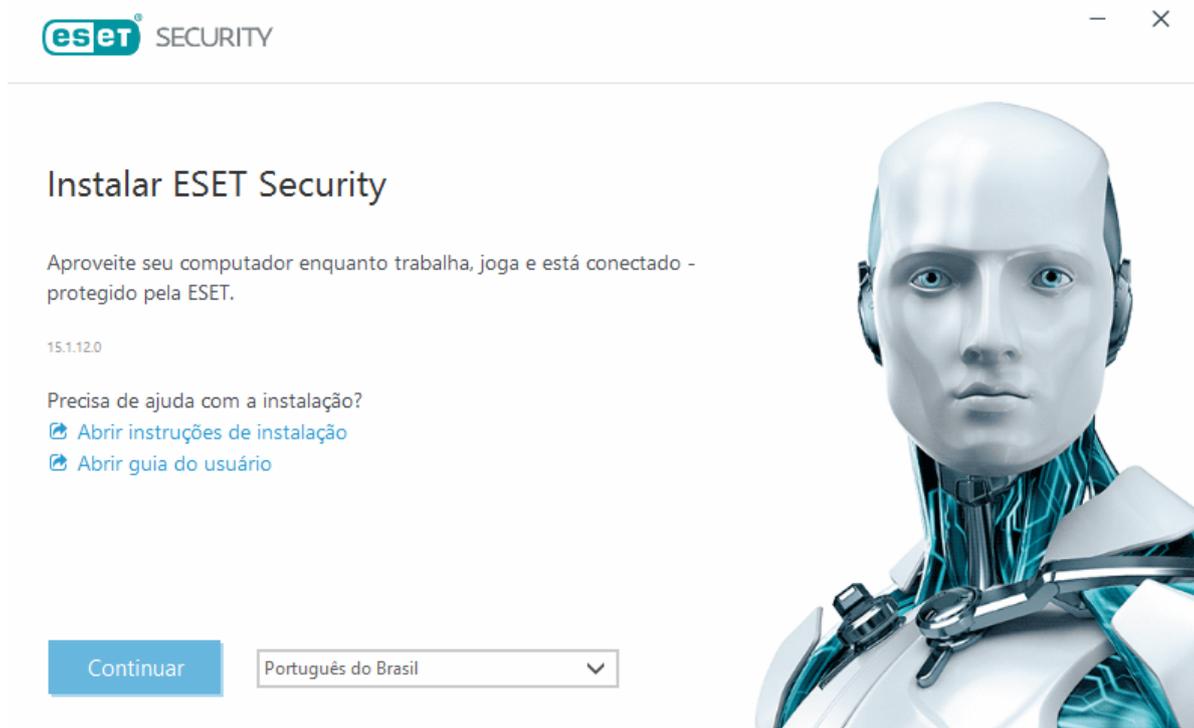
## Instalação off-line

Faça o download e instale seu produto doméstico ESET Windows usando o instalador off-line (.exe) abaixo. [Escolha qual versão você vai fazer download do produto inicial da ESET](#) (32-bit, 64-bit ou ARM).

ESET NOD32 Antivírus	ESET Internet Security	ESET Smart Security Premium
<a href="#">Download de 64 bits</a>	<a href="#">Download de 64 bits</a>	<a href="#">Download de 64 bits</a>
<a href="#">Download de 32 bits</a>	<a href="#">Download de 32 bits</a>	<a href="#">Download de 32 bits</a>
<a href="#">Download ARM</a>	<a href="#">Download ARM</a>	<a href="#">Download ARM</a>

**!** Se você tiver uma conexão com a internet ativa, [instale seu produto ESET usando um Instalador](#).

Ao iniciar o instalador off-line (.exe), o Assistente de instalação o guiará pelo processo de configuração.



1. Selecione o idioma adequado no menu suspenso e clique em **Continuar**.

**i** Se você estiver instalando uma versão mais recente sobre a versão anterior com as configurações protegidas por senha, digite sua senha. Você pode configurar a senha de configuração na [Configuração de acesso](#).

2. Selecione sua preferência para os recursos a seguir, leia o [Acordo de licença para o usuário final](#) e a [Política de Privacidade](#) e clique em **Continuar**, ou clique em **Permitir tudo e continuar** para ativar todos os recursos:

- [sistema de feedback ESET LiveGrid®](#)
- [Aplicativos potencialmente indesejados](#)
- [Programa de melhoria da experiência do cliente](#)

**i** Ao clicar em **Continuar** ou **Permitir tudo e continuar**, você aceita o Acordo de Licença para o Usuário Final e reconhece a Política de Privacidade.

3. Clique em **Ignorar login**. Quando você tiver uma conexão com a internet, poderá [conectar seu dispositivo à sua conta ESET HOME](#).

4. Clique em **Ignorar ativação**. O ESET NOD32 Antivirus deve ser ativado depois da instalação estar totalmente funcional. A [Ativação do produto](#) requer uma conexão com a internet ativa.

5. O Assistente de instalação mostra quais produtos ESET serão instalados com base no instalador off-line baixado. Clique em **Continuar** para iniciar o processo de instalação. Pode levar alguns momentos.

**i** Se houver algo remanescente (arquivos ou pastas) dos produtos ESET desinstalados no passado, você será solicitado a permitir a remoção deles. Clique em **Instalar** para continuar.

6. Clique em **Concluído** para sair do Assistente de instalação.

 [Solução de problemas de instalação.](#)

## Ativação do produto

Há vários métodos disponíveis para ativar seu produto. A disponibilidade de um cenário específico de ativação na janela de ativação pode variar conforme o país e meios de distribuição (CD/DVD, página da web da ESET etc.):

- Se você comprou uma versão do produto em uma caixa no varejo ou recebeu um e-mail com detalhes da licença, ative seu produto clicando em **Usar uma Chave de licença comprada**. A Chave de licença normalmente está localizada no interior ou na parte posterior da embalagem do produto. Para uma ativação bem-sucedida, a Chave de licença deve ser digitada conforme fornecida. Chave de licença – uma sequência de caracteres exclusiva no formato XXXX-XXXX-XXXX-XXXX-XXXX ou XXXX-XXXXXXXX, que é usada para identificação do proprietário da licença e para ativação da licença.
- Depois de selecionar [Usar conta ESET HOME](#), você será solicitado a entrar em sua conta ESET HOME.
- Se desejar avaliar o ESET NOD32 Antivirus antes de fazer uma aquisição, selecione a opção [Avaliação gratuita](#). Insira seu endereço de email e país para ativar o ESET NOD32 Antivirus por um período limitado. Sua licença de avaliação será enviada para seu email. As licenças de avaliação podem ser ativadas apenas uma vez por cliente.
- Se você não tem uma licença e deseja adquirir uma, clique em **Comprar licença**. Isso o redirecionará para o site do seu distribuidor local da ESET. As licenças completas para produtos domésticos ESET Windows [não são gratuitas](#).

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.

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 NOD32 Antivirus, [converta suas credenciais de legado para uma Chave de licença](#).

 [Falha na ativação do produto?](#)

Escolha uma opção de ativação



#### Use uma Chave de licença comprada

Use uma licença comprada on-line ou em uma loja.



#### Usar a conta ESET HOME

Entre no ESET HOME e escolha uma licença para ativar o produto ESET no seu dispositivo.



#### Comprar licença

Entre em contato com seu revendedor para comprar uma licença. Se você não tem certeza de quem é seu revendedor, [entre em contato com nosso suporte](#).

## Digitando sua chave de licença durante a ativação

Atualizações automáticas são importantes para sua segurança. O ESET NOD32 Antivirus vai receber atualizações apenas depois de ativado.

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.

Se você não digitou sua Chave de licença depois da instalação, o produto não será ativado. Você pode ativar o ESET NOD32 Antivirus na [janela principal do programa](#) > **Ajuda e suporte** > **Ativar licença**.

As licenças completas para produtos domésticos ESET Windows [não são gratuitas](#).

## Usar ESET HOME conta

Conecte seu dispositivo ao [ESET HOME](#) para visualizar e gerenciar todas as suas licenças e dispositivos ESET ativados. Você pode renovar, atualizar ou estender sua licença e exibir detalhes importantes da licença. No portal de gerenciamento ESET HOME ou aplicativo móvel, você pode adicionar licenças diferentes, fazer download de produtos no seu dispositivo, verificar o status de segurança do produto ou compartilhar licenças através do e-mail. Para mais informações, visite as [páginas de Ajuda on-line do ESET HOME](#).

Entre em sua conta ESET HOME

 Continuar com o Google

 Continuar com a Apple

 Ler código QR



eSet<sup>®</sup> HOME

Endereço de e-mail



Senha



[Esqueci minha senha](#)

 Efetuar login

Cancelar

Não tem uma conta? [Criar conta](#)

Depois de selecionar **Usar conta ESET HOME** como um método de ativação ou ao conectar na conta ESET HOME durante a instalação:

1. [Entre em sua conta ESET HOME](#).

**i** Se você não tem uma conta ESET HOME, clique em **Criar conta** para se registrar ou ver as instruções na [ESET HOME Ajuda on-line](#).  
Se você esqueceu sua senha, clique em **Esqueci minha senha** e siga as etapas na tela ou veja as instruções da [ESET HOME Ajuda on-line](#).

2. Defina um **Nome do dispositivo** para seu dispositivo que será usado em todos os serviços ESET HOME e clique em **Continuar**.
3. Escolha uma licença para ativação ou [adicione uma nova licença](#). Clique em **Continuar** para ativar o ESET NOD32 Antivirus.

## Ativar a licença de avaliação

Para ativar sua versão de avaliação do ESET NOD32 Antivirus, insira um endereço de e-mail válido no campo **Endereço de e-mail** e **Confirmar endereço de e-mail**. Depois da ativação, sua licença ESET será gerada e enviada para seu e-mail. Esse endereço de e-mail também será usado para as notificações de expiração do produto e outras comunicações com a ESET. A versão de avaliação pode ser ativada apenas uma vez.

Selecione o país no menu suspenso **País** para registrar o ESET NOD32 Antivirus junto ao seu distribuidor local, que fornecerá suporte técnico.

# Chave de licença ESET gratuita

A licença completa para o ESET NOD32 Antivirus não é gratuita.

A Chave de licença ESET é uma sequência única de letras e números separados por um traço fornecida pela ESET para permitir o uso legalizado do ESET NOD32 Antivirus de acordo com o [Acordo de licença para o Usuário final](#). Todo Usuário final tem o direito de usar a Chave de licença apenas na extensão em que tem o direito de usar o ESET NOD32 Antivirus com base no número de licenças fornecidas pela ESET. A Chave de licença é considerada confidencial e não pode ser compartilhada, mas você pode [compartilhar as licenças usando o ESET HOME](#).

Existem fontes gratuitas na Internet que podem oferecer a você uma chave de licença ESET "gratuita", mas não se esqueça:

- Clicar em uma propaganda de "Licença ESET gratuita" pode comprometer seu computador ou dispositivo e pode causar uma infecção com malware. O malware pode estar escondido em conteúdo não oficial da web (por exemplo, vídeos), sites que exibem anúncios para ganhar dinheiro com base em suas visitas, etc. Normalmente, eles são uma armadilha.
- A ESET pode desativar e realmente desativa licenças pirateadas.
- Ter uma chave de licença pirateada não está de acordo com o [Acordo de Licença para o Usuário final](#) que você deve aceitar para instalar o ESET NOD32 Antivirus.
- Compre licenças ESET apenas através de canais oficiais, como o [www.eset.com](http://www.eset.com), distribuidores ou revendedores ESET (não compre licenças de sites de terceiros não oficiais, como o eBay, ou licenças compartilhadas de um terceiro).
- [O download](#) de um ESET NOD32 Antivirus é gratuito, mas a ativação durante a instalação necessita de uma chave de licença ESET válida (você pode fazer o download e instalar, mas ele não funcionará sem a ativação).
- Não compartilhe sua licença na Internet ou em mídias sociais (ela pode ser espalhada).

Para identificar e reportar uma licença ESET pirateada, [visite nosso artigo da Base de conhecimento](#) para instruções.

---

Se você ainda não tiver certeza se deseja comprar um produto de segurança ESET, você poderá usar uma versão de avaliação enquanto decide:

1. [Ativar o ESET NOD32 Antivirus usando uma licença de avaliação gratuita](#)
2. [Participar do Programa beta da ESET](#)
3. [Instale o ESET Mobile Security](#) se estiver usando um dispositivo móvel Android, ele é um freemium.

Para obter um desconto/prolongar sua licença:

- [Indique o ESET NOD32 Antivirus a um amigo](#)
- [Renove sua licença ESET](#) (se você tinha uma licença ativa antes) ou ative por um período mais longo

# Falha na ativação – cenários comuns

Se a ativação do ESET NOD32 Antivirus não for bem-sucedida, os cenários mais comuns são:

- A chave de licença já está sendo usada
- 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

Verifique se você ativou a chave de licença adequada e tente ativá-la novamente. Se você usar a conta ESET HOME para ativação, consulte [Gerenciamento de licenças ESET HOME – Ajuda on-line](#).

Se você ainda não conseguir ativar, a [Solução de problemas de ativação ESET](#) o acompanha pelas perguntas, erros e problemas comuns sobre a ativação e licenciamento (disponível em inglês e em vários outros idiomas).

## Falha na ativação devido a uma licença usada em excesso

### Problema

- Sua licença pode estar sendo usada em excesso ou abusada
- Falha na ativação devido a uma licença usada em excesso

### Solução

Há mais dispositivos usando esta licença do que ela permite. Você pode ser uma vítima de pirataria de software ou falsificação. A licença não pode ser usada para ativar qualquer outro produto ESET. Você pode resolver esse problema diretamente se você tem permissão para gerenciar a licença na sua conta ESET HOME ou se você comprou a licença de uma fonte legítima. Se você ainda não tem uma conta, crie uma.

Se você é um proprietário de licença e não foi solicitado a inserir seu endereço de e-mail:

1. Para gerenciar sua licença ESET, abra um navegador da web e navegue até <https://home.eset.com>. Acessar ESET License Manager e remova ou desative as licenças. Para obter mais informações, veja [O que fazer no caso de uma licença usada em excesso](#).
2. Para identificar e reportar uma licença ESET pirateada, [visite nosso artigo Identificar e reportar licenças ESET pirateadas](#) para instruções.
3. Se você não tiver certeza, clique em **Voltar** e [mande um e-mail para o Suporte técnico da ESET](#).

Se você não for um proprietário de licença, entre em contato com o proprietário desta licença e informe que você não consegue ativar o produto ESET devido ao excesso de uso da licença. O proprietário pode resolver o

problema no portal [ESET HOME](#).

Se for solicitado a confirmar seu endereço de e-mail (apenas para vários casos), digite o endereço de e-mail usado originalmente para comprar ou ativar seu ESET NOD32 Antivirus.

## Atualização da licença

Essa janela de notificação aparece quando a licença usada para ativar seu produto ESET foi alterada. Sua licença alterada permite ativar um produto com mais recursos de segurança. Se nenhuma alteração tiver sido executada, o ESET NOD32 Antivirus o vai exibir uma janela de alerta uma vez, chamada **Alterar para um produto com mais recursos**.

**Sim (recomendado)** – vai instalar automaticamente o produto com mais recursos de segurança.

**Não, obrigado** – nenhuma alteração será feita e a notificação desaparecerá permanentemente.

Para alterar o produto mais tarde, consulte nosso [artigo da Base de conhecimento ESET](#). Para obter mais informações sobre licenças ESET, consulte a [FAQ de Licenciamento](#).

A tabela abaixo detalha os recursos disponíveis em cada produto específico.

	ESET NOD32 Antivirus	ESET Internet Security	ESET Smart Security Premium
Mecanismo de detecção	✓	✓	✓
Aprendizado de máquina avançado	✓	✓	✓
Bloqueio de Exploit	✓	✓	✓
Proteção contra ataque baseado em script	✓	✓	✓
Antiphishing	✓	✓	✓
Proteção do acesso à Web	✓	✓	✓
HIPS (incluindo Escudo Anti-ransomware)	✓	✓	✓
Antispam		✓	✓
Firewall		✓	✓
Inspetor de rede		✓	✓
Proteção da webcam		✓	✓
Proteção contra ataque de rede		✓	✓
Proteção contra botnet		✓	✓
Proteção para bancos & pagamentos		✓	✓
Controle dos pais		✓	✓
Antifurto		✓	✓
Password Manager			✓
ESET Secure Data			✓
ESET LiveGuard			✓

## Atualização do produto

Você fez o download de um instalador padrão e decidiu alterar o produto a ser ativado, ou deseja alterar seu produto instalado para um com mais recursos de segurança.

[Alterar produto durante a instalação.](#)

A tabela abaixo detalha os recursos disponíveis em cada produto específico.

	ESET NOD32 Antivírus	ESET Internet Security	ESET Smart Security Premium
Mecanismo de detecção	✓	✓	✓
Aprendizado de máquina avançado	✓	✓	✓
Bloqueio de Exploit	✓	✓	✓
Proteção contra ataque baseado em script	✓	✓	✓
Antiphishing	✓	✓	✓
Proteção do acesso à Web	✓	✓	✓
HIPS (incluindo Escudo Anti-ransomware)	✓	✓	✓
Antispam		✓	✓
Firewall		✓	✓
Inspetor de rede		✓	✓
Proteção da webcam		✓	✓
Proteção contra ataque de rede		✓	✓
Proteção contra botnet		✓	✓
Proteção para bancos & pagamentos		✓	✓
Controle dos pais		✓	✓
Antifurto		✓	✓
Password Manager			✓
ESET Secure Data			✓
ESET LiveGuard			✓

## Downgrade da licença

Essa janela de diálogo aparece quando a licença usada para ativar seu produto ESET foi alterada. Sua licença alterada pode ser usada apenas com um produto ESET diferente com menos recursos de segurança. O produto foi alterado automaticamente para evitar a perda de proteção.

Para obter mais informações sobre licenças ESET, consulte a [FAQ de Licenciamento](#).

A tabela abaixo detalha os recursos disponíveis em cada produto específico.

	ESET NOD32 Antivírus	ESET Internet Security	ESET Smart Security Premium
Mecanismo de detecção	✓	✓	✓

	ESET NOD32 Antivírus	ESET Internet Security	ESET Smart Security Premium
Aprendizado de máquina avançado	✓	✓	✓
Bloqueio de Exploit	✓	✓	✓
Proteção contra ataque baseado em script	✓	✓	✓
Antiphishing	✓	✓	✓
Proteção do acesso à Web	✓	✓	✓
HIPS (incluindo Escudo Anti-ransomware)	✓	✓	✓
Antispam		✓	✓
Firewall		✓	✓
Inspetor de rede		✓	✓
Proteção da webcam		✓	✓
Proteção contra ataque de rede		✓	✓
Proteção contra botnet		✓	✓
Proteção para bancos & pagamentos		✓	✓
Controle dos pais		✓	✓
Antifurto		✓	✓
Password Manager			✓
ESET Secure Data			✓
ESET LiveGuard			✓

## Downgrade do produto

O produto instalado no momento tem mais recursos de segurança do que aquele que você está prestes a ativar.

A tabela abaixo detalha os recursos disponíveis em cada produto específico.

	ESET NOD32 Antivírus	ESET Internet Security	ESET Smart Security Premium
Mecanismo de detecção	✓	✓	✓
Aprendizado de máquina avançado	✓	✓	✓
Bloqueio de Exploit	✓	✓	✓
Proteção contra ataque baseado em script	✓	✓	✓
Antiphishing	✓	✓	✓
Proteção do acesso à Web	✓	✓	✓
HIPS (incluindo Escudo Anti-ransomware)	✓	✓	✓
Antispam		✓	✓
Firewall		✓	✓
Inspetor de rede		✓	✓
Proteção da webcam		✓	✓
Proteção contra ataque de rede		✓	✓
Proteção contra botnet		✓	✓

	ESET NOD32 Antivírus	ESET Internet Security	ESET Smart Security Premium
Proteção para bancos & pagamentos		✓	✓
Controle dos pais		✓	✓
Antifurto		✓	✓
Password Manager			✓
ESET Secure Data			✓
ESET LiveGuard			✓

## Solução de problemas de instalação

Se ocorrerem problemas durante a instalação, o Assistente de instalação fornece um solução de problemas que resolverá o problema, se possível.

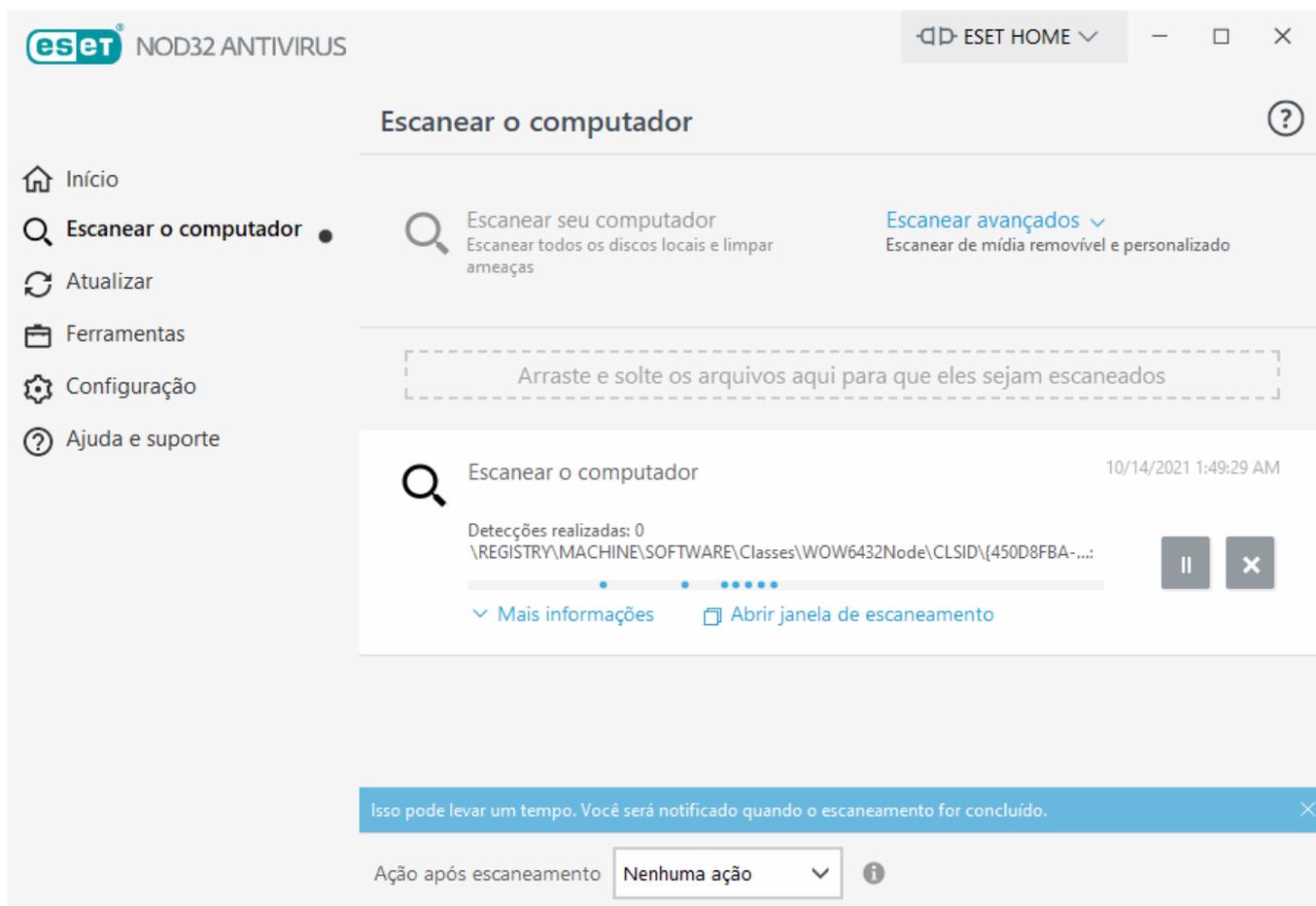
Clique em **Executar a solução de problemas** para iniciar a solução de problemas. Quando a solução de problemas for concluída, siga a solução recomendada.

Se o problema persistir, veja a lista de [erros de instalação comuns e resoluções](#).

## Primeiro rastreamento depois da instalação

Depois de instalar o ESET NOD32 Antivírus, um rastreamento do computador será iniciado automaticamente depois da primeira atualização bem-sucedida, para verificar a existência de código malicioso.

Você também pode iniciar um rastreamento no computador manualmente a partir da [janela principal do programa](#), clicando em **Escanear o computador > Rastrear seu computador**. Para obter mais informações sobre os rastreamentos do computador, consulte a seção [Escanear o computador](#).



## Atualização para uma versão mais recente

Versões mais recentes do ESET NOD32 Antivirus 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, 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 a **Atualização de recursos do aplicativo** em **Configuração avançada (F5) > Atualização > Perfis > Atualizações**.

2. Manualmente na [janela do programa principal](#), clicando em **Verificar se há atualizações** na seção **Atualizações**.

3. Manualmente, por meio de download e [instalação de uma versão mais recente](#) sobre a instalação anterior.

Para informações adicionais e instruções ilustradas, consulte:

- [Atualizar produtos ESET — busque os módulos de produto mais recentes](#)
- [Quais são os diferentes tipos de atualização de produto da ESET e lançamentos?](#)

# Atualização automática de produto legado

Sua versão do produto ESET não é mais compatível, e seu produto foi atualizado para a versão mais recente.

## [Problemas comuns de instalação](#)

 Cada nova versão dos produtos ESET tem muitas soluções bugs e melhorias. Clientes existentes com uma licença válida para um produto ESET podem atualizar para a versão mais recente do mesmo produto gratuitamente.

Para concluir a instalação:

1. Clique em **Aceitar e continuar** para aceitar o [Acordo de licença para o usuário final](#) e reconhecer a [Política de privacidade](#). Se você não concordar com o Acordo de licença para o usuário final, clique em **Desinstalar**. Não é possível reverter para a versão anterior.
2. Clique em **Permitir tudo e continuar** para permitir o [Sistema de feedback ESET LiveGrid®](#) e o [Programa de melhoria da experiência do cliente](#) ou clique em **Continuar** se não quiser participar.
3. Depois de ativar o novo produto ESET com sua Chave de licença, a página de Início será exibida. Se suas informações de licença não forem encontradas, continue com uma nova licença de avaliação. Se sua licença usada no produto anterior não for válida, [ative seu produto ESET](#).
4. É necessário reiniciar o dispositivo para concluir a instalação.

## Indicando um produto ESET para um amigo

Essa versão do ESET NOD32 Antivirus agora oferece bônus de indicação, portanto você pode compartilhar sua experiência com produtos ESET com seus familiares ou amigos. Você pode até mesmo compartilhar indicações de um produto ativado com uma licença de avaliação. Quando você é um usuário de avaliação, para cada indicação bem sucedida enviada por você que resultar em uma ativação do produto, tanto você quanto seu amigo receberão um mês adicional de proteção completa na licença de avaliação.

Você pode indicar usando seu ESET NOD32 Antivirus instalado. O produto que você pode indicar depende do produto de onde você está indicando, consulte a tabela abaixo.

Seu produto instalado	Produto que você pode indicar
ESET NOD32 Antivirus	ESET Internet Security
ESET Internet Security	ESET Internet Security
ESET Smart Security Premium	ESET Smart Security Premium

## Indicando um produto

Para enviar um link de indicação, clique em **Indicar um amigo** no menu principal do ESET NOD32 Antivirus. Clique em **Compartilhar link de indicação**. Seu produto vai gerar um link de indicação que será exibido em uma nova janela. Copie o link e envie-o para seus familiares e amigos. Você pode compartilhar seu link de indicação diretamente do seu produto ESET usando as opções **Compartilhar no Facebook**, **Indicar aos contatos do Gmail** e **Compartilhar no Twitter**.

Quando seu amigo clicar no link de indicação que você enviou, ele será redirecionado para uma página da web onde poderá fazer download do produto e usá-lo para uma proteção adicional GRATUITA de um mês. Como um usuário de avaliação, você receberá uma notificação para cada link de indicação que for ativado com sucesso e sua licença será estendida automaticamente por mais um mês de proteção GRATUITA. Assim você pode estender sua proteção GRATUITA por até 5 meses. Você pode verificar o número de links de indicação ativados com sucesso na janela **Indique seu amigo** do seu produto ESET.

**i** O recurso de indicação pode não estar disponível para seu idioma/região.

## ESET NOD32 Antivirus será instalado

Esta janela de diálogo pode ser exibida:

- Durante o processo de instalação – clique em **Continuar** para instalar o ESET NOD32 Antivirus.
- Ao alterar uma licença no ESET NOD32 Antivirus – clique em **Ativar** para alterar a licença e ativar o ESET NOD32 Antivirus.

A opção **Alterar produto** permite a você trocar entre vários produtos domésticos da ESET Windows de acordo com sua licença ESET. Consulte [Qual produto eu tenho?](#) para obter mais informações.

## Alterar para uma linha de produtos diferente

De acordo com sua licença ESET, você pode trocar entre vários produtos domésticos da ESET Windows. Consulte [Qual produto eu tenho?](#) para obter mais informações.

## Registro

Registre sua licença preenchendo os campos no formulário de registro e clicando em Ativar. Os campos marcados como necessários entre parênteses são obrigatórios. Estas informações serão usadas apenas para questões que envolvam sua licença ESET.

## Progresso de ativação

Aguarde por alguns segundos para que o processo de ativação seja concluído (o tempo necessário pode variar dependendo da velocidade de sua conexão com a Internet ou do seu computador).

## Ativação bem-sucedida

O processo de ativação foi concluído.

Uma atualização de módulo irá começar em alguns segundos. Atualizações regulares do ESET NOD32 Antivirus serão iniciadas imediatamente.

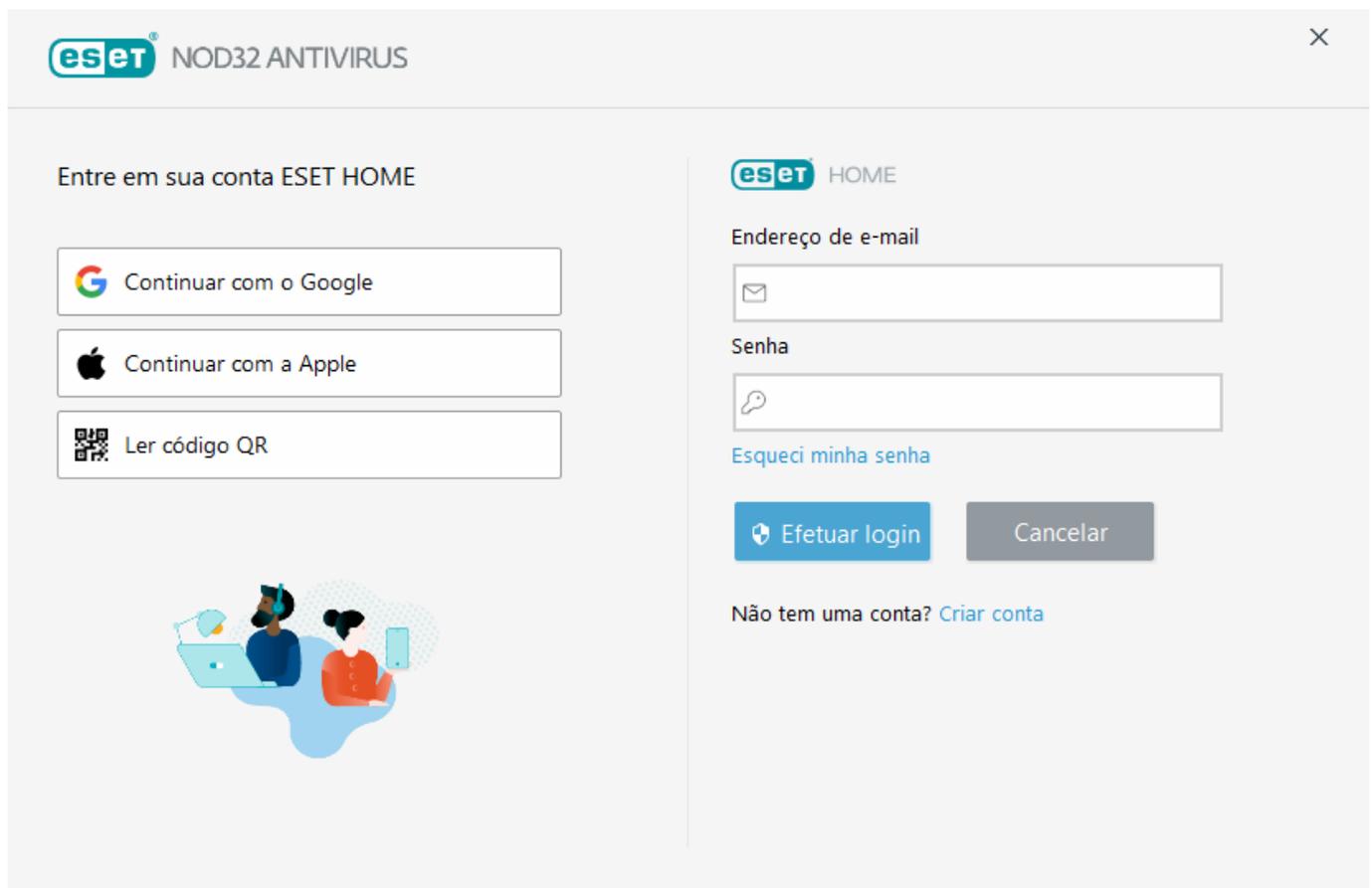
Um escaneamento inicial irá começar automaticamente dentro de 20 minutos depois da atualização de módulo.

# Guia do iniciante

Este capítulo fornece uma visão geral inicial do ESET NOD32 Antivirus e de suas configurações básicas.

## Conectar ao ESET HOME

Conecte seu dispositivo ao [ESET HOME](#) para visualizar e gerenciar todas as suas licenças e dispositivos ESET ativados. Você pode renovar, atualizar ou estender sua licença e exibir detalhes importantes da licença. No portal de gerenciamento ESET HOME ou aplicativo móvel, você pode adicionar licenças diferentes, fazer download de produtos no seu dispositivo, verificar o status de segurança do produto ou compartilhar licenças através do e-mail. Para mais informações, visite as [páginas de Ajuda on-line do ESET HOME](#).



Conecte seu dispositivo ao ESET HOME:

- i** Se você estiver conectando ao ESET HOME durante a instalação ou ao selecionar **Usar conta ESET HOME** como um método de ativação, siga as instruções no tópico [Usar conta ESET HOME](#). Se você já tiver o ESET NOD32 Antivirus instalado e ativado com uma licença adicionada na sua conta ESET HOME, é possível conectar seu dispositivo ao ESET HOME usando o portal ESET HOME. Siga as instruções no [ESET HOME guia de Ajuda on-line](#) e [permita a conexão no ESET NOD32 Antivirus](#).

1. Na [janela principal do programa](#), clique em **ESET HOME > Conectar ao ESET HOME** ou clique em **Conectar ao ESET HOME** na notificação **Conectar este dispositivo a uma conta ESET HOME**.
2. [Entre em sua conta ESET HOME](#).

-  Se você não tem uma conta ESET HOME, clique em **Criar conta** para se registrar ou ver as instruções na [ESET HOME Ajuda on-line](#).
-  Se você esqueceu sua senha, clique em **Esqueci minha senha** e siga as etapas na tela ou veja as instruções da [ESET HOME Ajuda on-line](#).

3. Defina um **Nome de dispositivo** e clique em **Continuar**.

4. Depois de uma conexão bem-sucedida, uma janela de detalhes é exibida. Clique em **Concluído**.

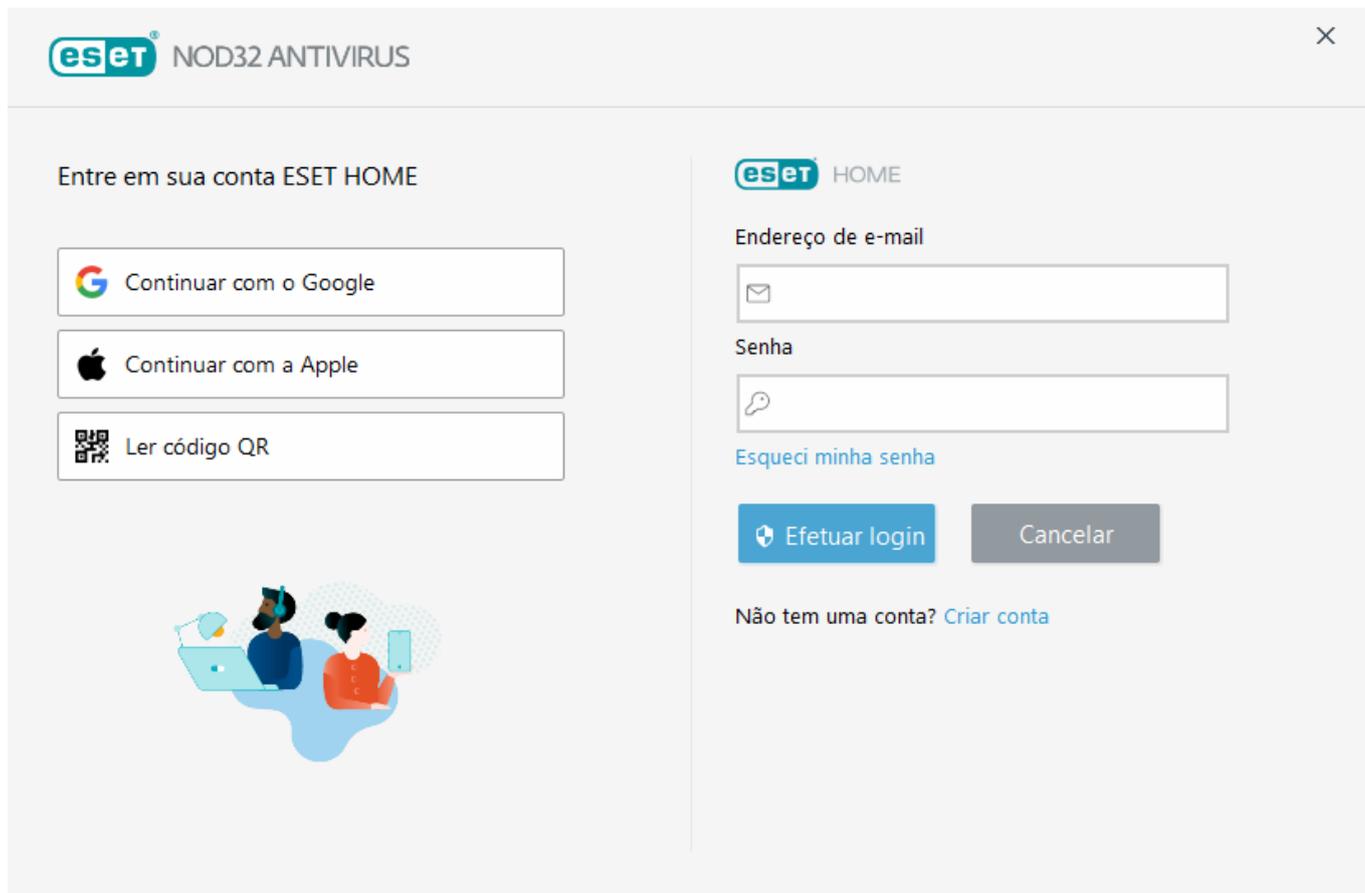
## Entrar no ESET HOME

Há vários métodos disponíveis para entrar em sua conta ESET HOME:

- **Use seu endereço de e-mail ESET HOME e senha** – digite o **Endereço de e-mail** e **Senha** usados para criar sua conta ESET HOME e clique em **Entrar**.
- **Use sua conta Google /AppleID** – clique em **Continuar com Google** ou **Continuar com Apple** e entre na conta adequada. Depois de um login bem-sucedido, você será redirecionado para a página da web de confirmação ESET HOME. Para continuar, volte para a janela do seu produto ESET. Para obter mais informações sobre a conta Google/login AppleID, consulte as instruções em [ESET HOME Ajuda on-line](#).
- **Leitura de código QR** – clique em **Ler código QR** para exibir o código QR. Abra seu aplicativo móvel ESET HOME e leia o código QR ou aponte a câmera do seu dispositivo para o código QR. Para obter mais informações, consulte as instruções em [ESET HOME Ajuda on-line](#).

-  Se você não tem uma conta ESET HOME, clique em **Criar conta** para se registrar ou ver as instruções na [ESET HOME Ajuda on-line](#).
-  Se você esqueceu sua senha, clique em **Esqueci minha senha** e siga as etapas na tela ou veja as instruções da [ESET HOME Ajuda on-line](#).

 [Falha ao entrar – erros comuns](#).



## Falha ao entrar – erros comuns

### Não conseguimos encontrar uma conta que corresponde ao endereço de e-mail inserido

O endereço de e-mail inserido não combina com nenhuma conta ESET HOME. Clique em **Voltar** e digite o endereço de e-mail e a senha corretos.

Para entrar é preciso criar uma ESET HOME conta. Se você não tem uma conta ESET HOME, clique em **Voltar** > **Criar conta** ou veja [Criar uma nova conta ESET HOME](#).

### O nome de usuário e senha não combinam

A senha inserida não combina com o endereço de e-mail inserido. Clique em **Voltar**, digite a senha correta e certifique-se de que o endereço de e-mail inserido está correto. Se você ainda não conseguir entrar, clique em **Voltar** > **Esqueci minha senha** para redefinir sua senha e siga as etapas na tela, ou consulte [Esqueci minha senha ESET HOME](#).

### A opção de login selecionada não é correspondente com sua conta

Sua conta está vinculada à sua conta de mídia social. Para entrar no ESET HOME, clique em **Continuar com o Google** ou **Continuar com o Apple** e entre na conta adequada. Depois de um login bem-sucedido, você será redirecionado para a página da web de confirmação do ESET HOME. Você pode desconectar sua conta de mídia social ESET HOME da sua conta no portal ESET HOME.

## Senha incorreta

Esse erro pode acontecer se o seu ESET NOD32 Antivirus já estiver conectado ao ESET HOME e você estiver fazendo alterações que exigem que você entre (por exemplo, desativar o Anti-Theft) e a senha inserida não corresponde com a senha da sua conta. Clique em **Voltar** e digite a senha correta. Se você ainda não conseguir entrar, clique em **Voltar** > **Esqueci minha senha** para redefinir sua senha e siga as etapas na tela, ou consulte [Esqueci minha senha ESET HOME](#).

## Adicionar dispositivo em ESET HOME

Se você já instalou o ESET NOD32 Antivirus e ativou com uma licença adicionada na sua conta ESET HOME, é possível conectar seu dispositivo ao ESET HOME usando o portal ESET HOME:

1. [Envie uma solicitação de conexão ao seu dispositivo](#).
2. O ESET NOD32 Antivirus exibe a janela de diálogo **Conectar este dispositivo a uma conta ESET HOME** com um nome da conta ESET HOME. Clique em **Permitir** para conectar o dispositivo à conta ESET HOME mencionada.

**i** Se não houver interação, a solicitação de conexão será cancelada automaticamente depois de aproximadamente 30 minutos.

## Janela do programa principal

A janela principal do ESET NOD32 Antivirus é dividida em duas seções principais. A primeira janela à direita exibe informações correspondentes à opção selecionada no menu principal à esquerda.

### Instruções ilustradas

**i** Consulte [Abrir a janela principal do programa dos produtos ESET Windows](#) para instruções ilustradas disponíveis em inglês e em vários outros idiomas.

**ESET HOME** – [conecte seu dispositivo ao ESET HOME](#). Use o [ESET HOME](#) para visualizar e gerenciar seu ativar licenças e dispositivos ESET.

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

**Início** - Fornece informações sobre o status da proteção do ESET NOD32 Antivirus.

**Rastreamento do computador** - Configure e inicie um rastreamento do seu computador ou crie um rastreamento personalizado.

**Atualizar** - Exibe informações sobre atualizações do mecanismo de detecção.

**Ferramentas** – Fornece acesso aos módulos que ajudam a simplificar a administração do programa e oferecem opções adicionais para usuários avançados. Para mais informações, consulte [Ferramentas no ESET NOD32 Antivirus](#).

**Configuração** - Selecione essa opção para ajustar o nível de segurança para seu computador, internet.

**Ajuda e suporte** – Fornece acesso aos arquivos de ajuda, [Base de conhecimento ESET](#), ao site da ESET e a links para enviar uma solicitação de suporte.



A tela **Inicial** contém informações importantes sobre o nível de proteção atual do seu computador. A janela de status exibe os recursos mais usados do ESET NOD32 Antivirus. Informações sobre o produto instalado e a data de expiração da licença também são encontradas aqui. Clique em **ESET NOD32 Antivirus** se quiser instalar outra versão do produto ESET. [Mais informações sobre os recursos estão em cada produto específico.](#)



O ícone verde e status de **Você está protegido** verde indica que a proteção máxima está garantida.

## O que fazer se o programa não funcionar adequadamente?

Se um módulo de proteção ativa estiver funcionando corretamente, seu ícone do status de proteção estará verde. Um ponto de exclamação vermelho ou um ícone de notificação laranja indica que a máxima proteção não está garantida. Serão exibidas informações adicionais sobre o status de proteção de cada módulo, bem como soluções sugeridas para a restauração da proteção total em **Início**. Para alterar o status de módulos individuais, clique em **Configuração** e selecione o módulo desejado.



O ícone vermelho e o status de **Alerta de segurança** vermelho indicam problemas críticos. Há várias razões para esse status poder ser exibido, por exemplo:

- **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.
- **Mecanismo de detecção desatualizado** - Esse erro aparecerá após diversas tentativas malsucedidas de atualizar o mecanismo de detecção. 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 proteção em tempo real do sistema de arquivos está desativada** – 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.
- **Proteção antivírus e antispyware desativada** - Você pode reativar a proteção antivírus e antispyware clicando em **Ativar proteção antivírus e antispyware**.



O ícone laranja indica proteção limitada. Por exemplo, pode haver um problema com a atualização do programa ou a data de expiração da sua licença está se aproximando.

Há várias razões para esse status poder ser exibido, por exemplo:

- **Modo de jogador ativo** - Ativar o [Modo de jogador](#) é um risco de segurança em potencial. Ativar este recurso desativa todas as janelas de pop-up e interrompe qualquer tarefa agendada.
- **Sua licença expirará em breve** - Isso é indicado pelo ícone do status de proteção exibindo um ponto de exclamação ao lado do relógio do sistema. Depois que a licença expirar, o programa não poderá ser

atualizado e o ícone do status da proteção ficará vermelho.

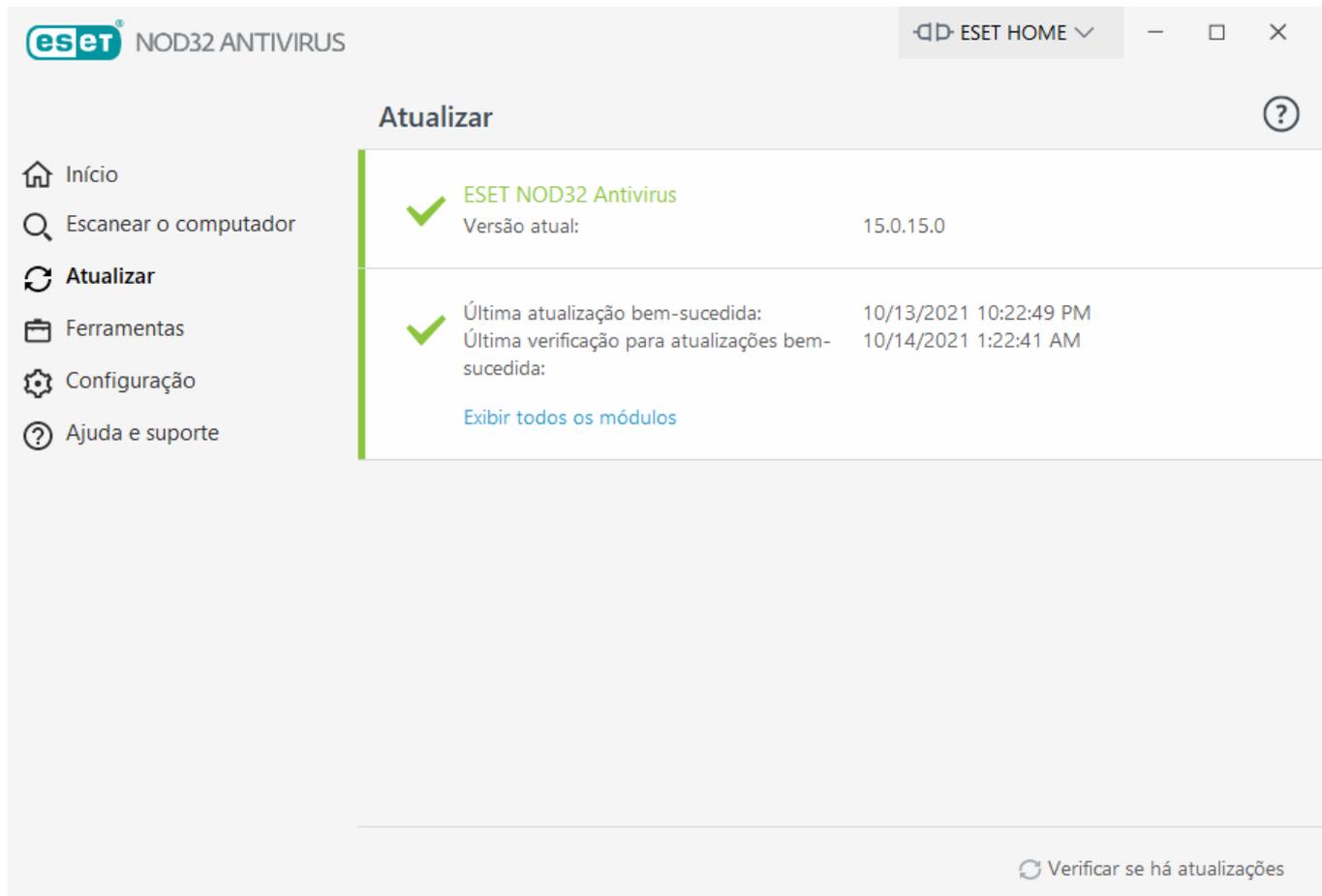
Se não for possível solucionar um problema com as soluções sugeridas, clique em **Ajuda e suporte** para acessar os arquivos de ajuda ou pesquisar na [Base de conhecimento da ESET](#). Se precisar de assistência, envie uma solicitação de suporte. O Suporte técnico ESET responderá rapidamente às suas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

## Atualizações

Atualizar o ESET NOD32 Antivirus periodicamente é o melhor método para se garantir o nível máximo de segurança em seu computador. O módulo de Atualização garante que tanto os módulos do programa quanto os componentes do sistema estejam sempre atualizados.

Na [janela principal do programa](#), ao clicar em **Atualizar**, você poderá visualizar o status da atualização atual, incluindo o dia e a hora da última atualização bem-sucedida, e se uma atualização será necessária.

Além de atualizações automáticas, você pode clicar em **Verificar se há atualizações** para acionar uma atualização manual.



The screenshot shows the ESET NOD32 Antivirus interface. The title bar reads "eSet NOD32 ANTIVIRUS" and "ESET HOME". The main window is titled "Atualizar" (Update) and displays the following information:

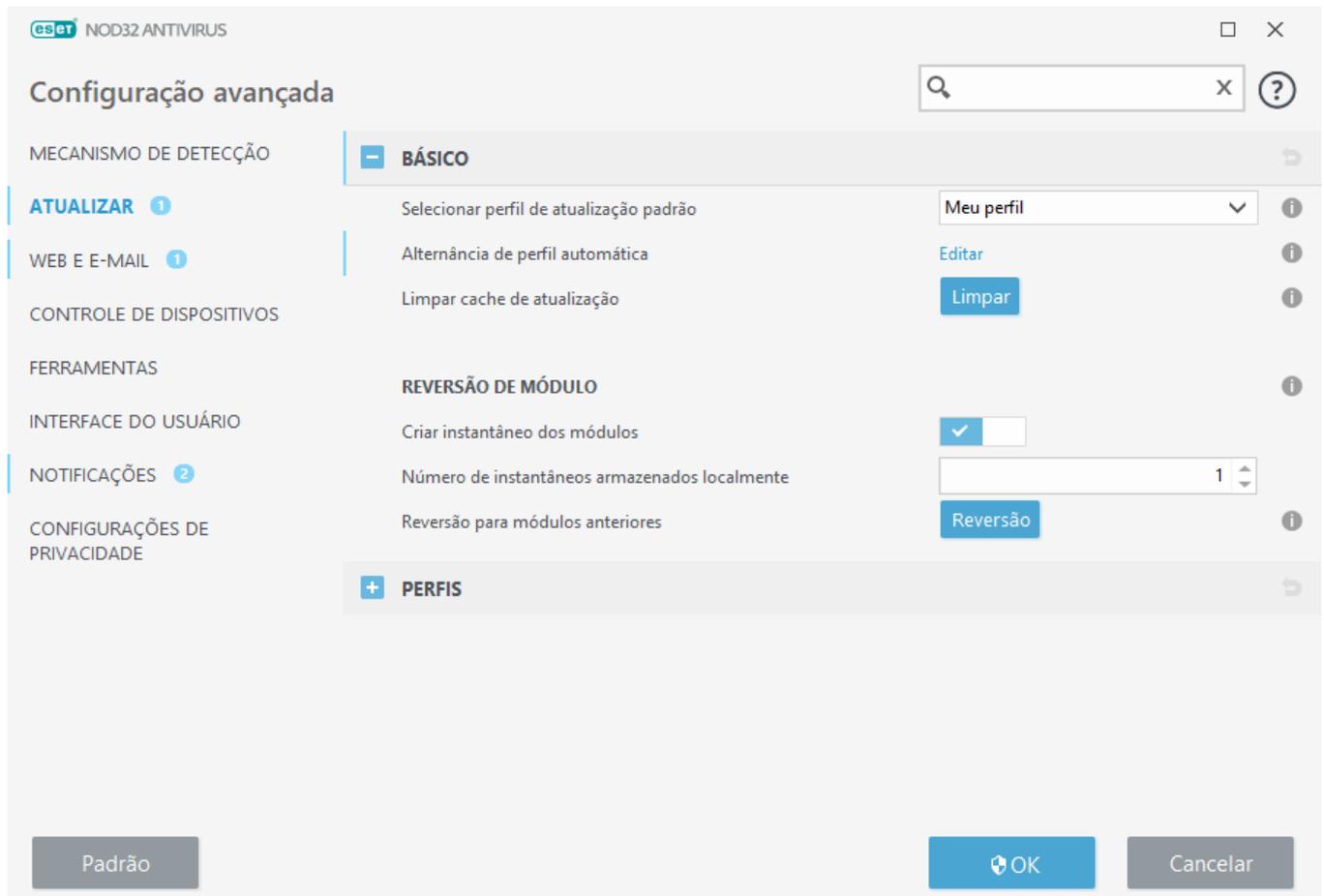
- ESET NOD32 Antivirus** (indicated by a green checkmark)
- Versão atual: 15.0.15.0
- Última atualização bem-sucedida: 10/13/2021 10:22:49 PM
- Última verificação para atualizações bem-sucedida: 10/14/2021 1:22:41 AM
- Link: [Exibir todos os módulos](#)

At the bottom right, there is a button labeled "Verificar se há atualizações" (Check for updates).

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. Para configurar opções avançadas de atualização como o modo de atualização, acesso ao servidor proxy e as conexões de rede, clique em **Atualizar** na árvore de configuração avançada.

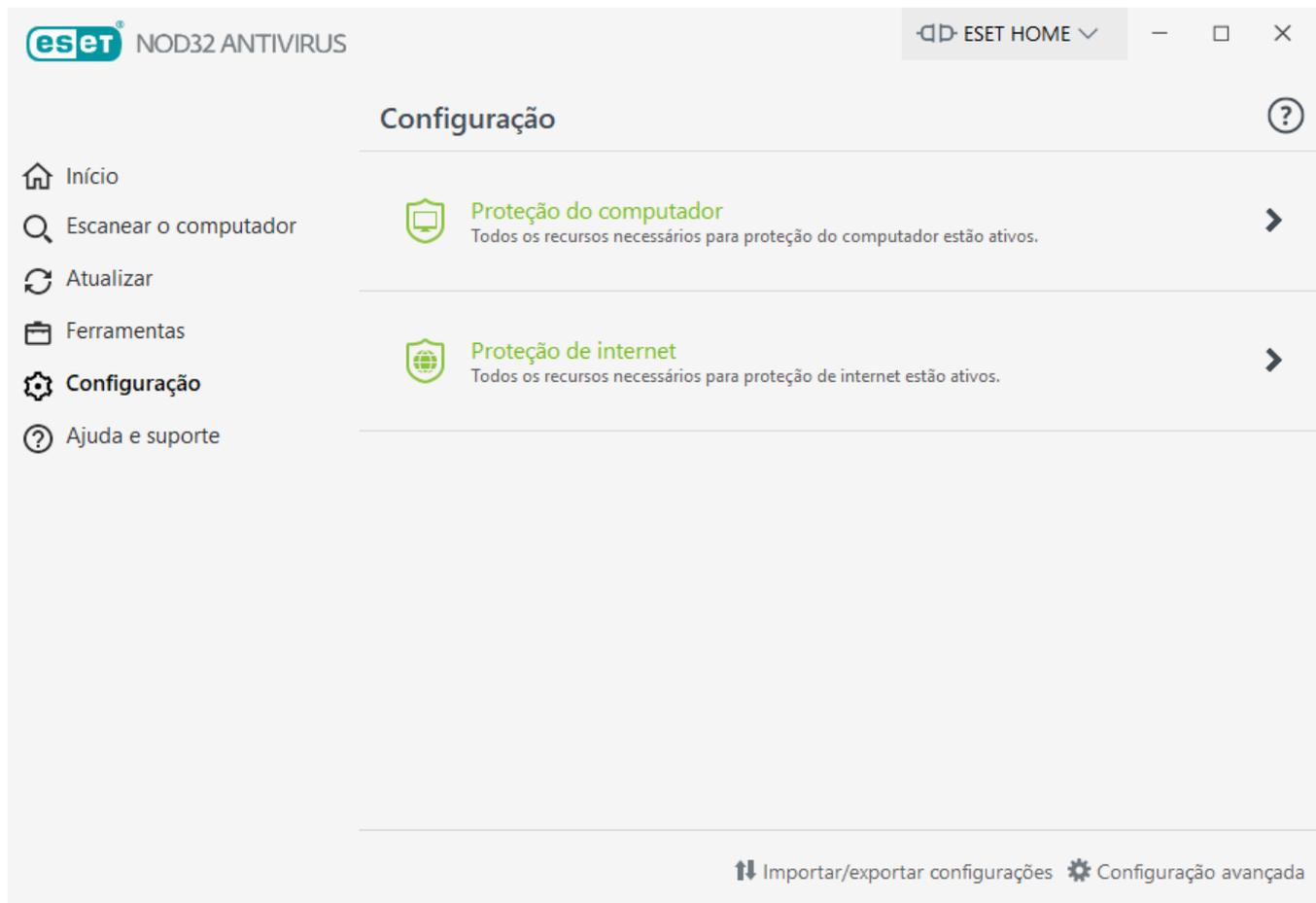
Se você estiver tendo problemas com uma atualização, clique em **Limpar** para limpar o cache de atualização. Se você ainda não conseguir atualizar os módulos de programa, consulte a seção de [Solução de problemas para a](#)

[mensagem "Falha na atualização dos módulos"](#).



## Trabalhando com o ESET NOD32 Antivirus

As opções de configuração ESET NOD32 Antivirus permitem que você ajuste os níveis de proteção do seu computador.



O menu **Configurar** é dividido pelas seguintes seções:

 **Proteção do computador**

 **Proteção para internet**

Clique em um componente para ajustar as configurações avançadas do módulo de proteção correspondente.

A configuração da proteção do **Computador** permite 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** - Esse módulo permite rastrear, bloquear ou ajustar filtros/permisões estendidos e seleciona como o usuário pode acessar e usar um determinado dispositivo (CD/DVD/USB...).
- **HIPS** – O sistema [HIPS](#) monitora os eventos dentro do sistema operacional e reage a eles de acordo com um conjunto de regras personalizado.
- **Modo de jogador** – Ativa ou desativa o [Modo de jogador](#). Você receberá uma mensagem de aviso (risco potencial de segurança) e a janela principal será exibida em laranja após a ativação do Modo de jogos.

A configuração da proteção de **Internet** permite ativar ou desativar os seguintes componentes:

- **Proteção do acesso à Web** – Se ativada, todo o tráfego através de HTTP ou HTTPS será escaneado quanto

a software malicioso.

- **Proteção do cliente de email** – Monitora a comunicação recebida através do protocolo POP3(S) e IMAP(S).
- **Proteção Antiphishing** - Filtra sites suspeitos de distribuir conteúdo com objetivo de manipular usuários para que enviem informações confidenciais.

Para reativar a proteção do componente de segurança desativado, clique no controle deslizante  para que ele exiba uma marca de verificação verde .

**i** Ao desabilitar a proteção usando este método, todos os módulos com proteção desativada serão ativados depois da reinicialização do computador.

Existem opções adicionais disponíveis na parte inferior da janela de configuração. Use o link de **Configuração avançada** para configurar parâmetros mais detalhados para cada módulo. Use **Configurações importar/exportar** para carregar os parâmetros de configuração utilizando um arquivo de configuração .xml ou salvar seus parâmetros atuais em um arquivo de configuração.

## Proteção do computador

Clique em **Proteção do computador** na janela **Configuração** para ver uma visão geral de todos os módulos de proteção:

- [Proteção em tempo real do sistema de arquivos](#)
- [Controle de dispositivos](#)
- [Sistema de prevenção de intrusos de host \(HIPS\)](#)
- [Modo jogador](#)

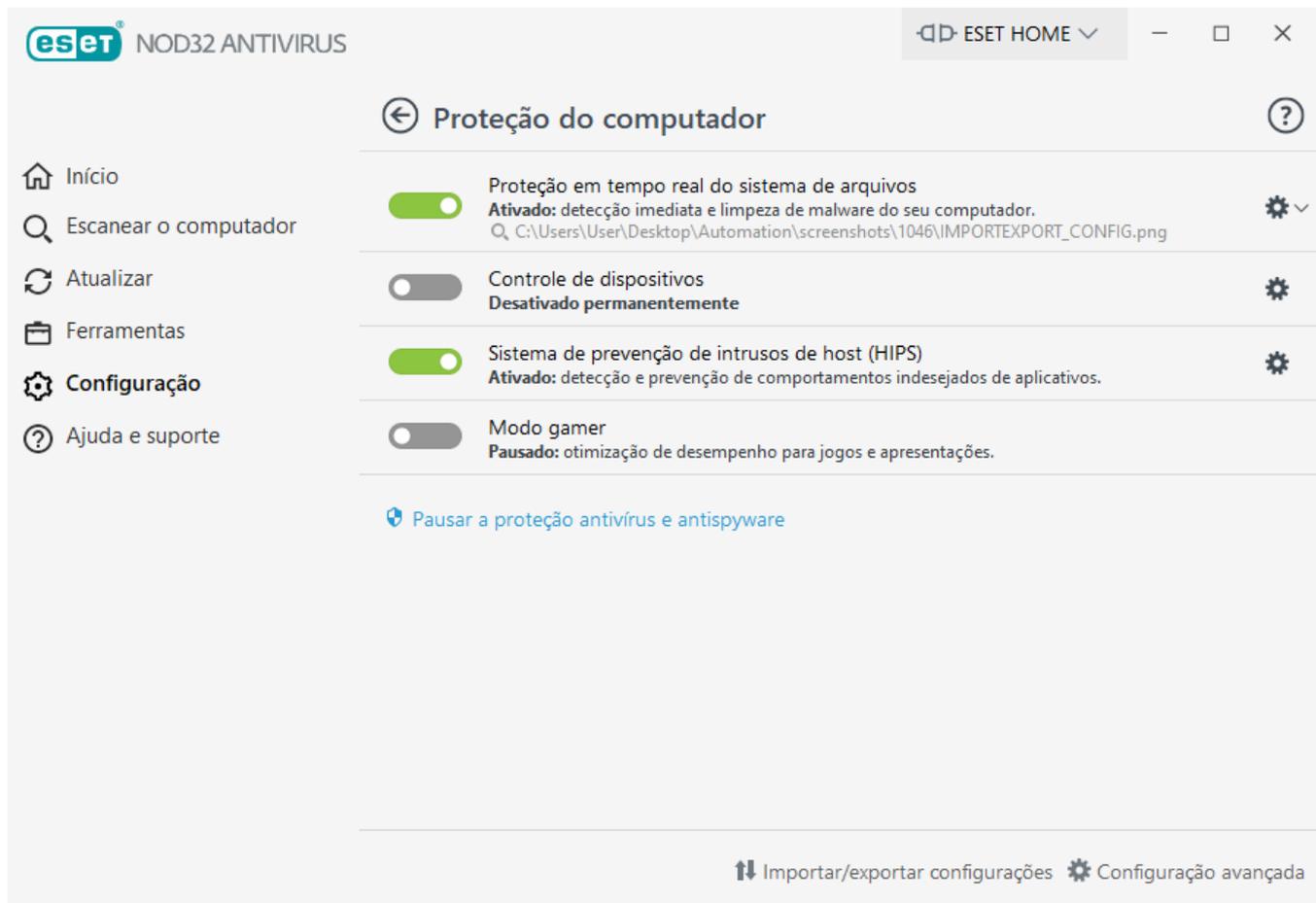
Para pausar ou desativar os módulos de proteção individuais, clique no ícone da barra deslizante .

**!** Desligar os módulos de proteção pode diminuir o nível de proteção do seu computador.

Clique no ícone de engrenagem  ao lado de um módulo de proteção para acessar as configurações avançadas daquele módulo.

Para a **Proteção em tempo real do sistema de arquivos**, clique no ícone de engrenagem  e escolha uma das seguintes opções:

- **Configurar** – abre a Configuração avançada da Proteção em tempo real do sistema de arquivos.
- **Editar exclusões** – abre a [janela de Configuração de exclusão](#) para que você possa excluir arquivos e pastas do escaneamento.



**Pausar a proteção antivírus e antispyware** – desativa todos os módulos de proteção antivírus e antispyware. Quando você desativar a proteção, uma janela será aberta para determinar por quanto tempo a proteção será desativada usando o menu suspenso **Intervalo de tempo**. Use apenas se você for um usuário experiente ou instruído pelo Suporte técnico da ESET.

## 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**.



As alterações nas configurações do Mecanismo de detecção devem ser feitas apenas por um usuário experiente. A configuração incorreta das configurações pode levar a um nível de proteção reduzido.

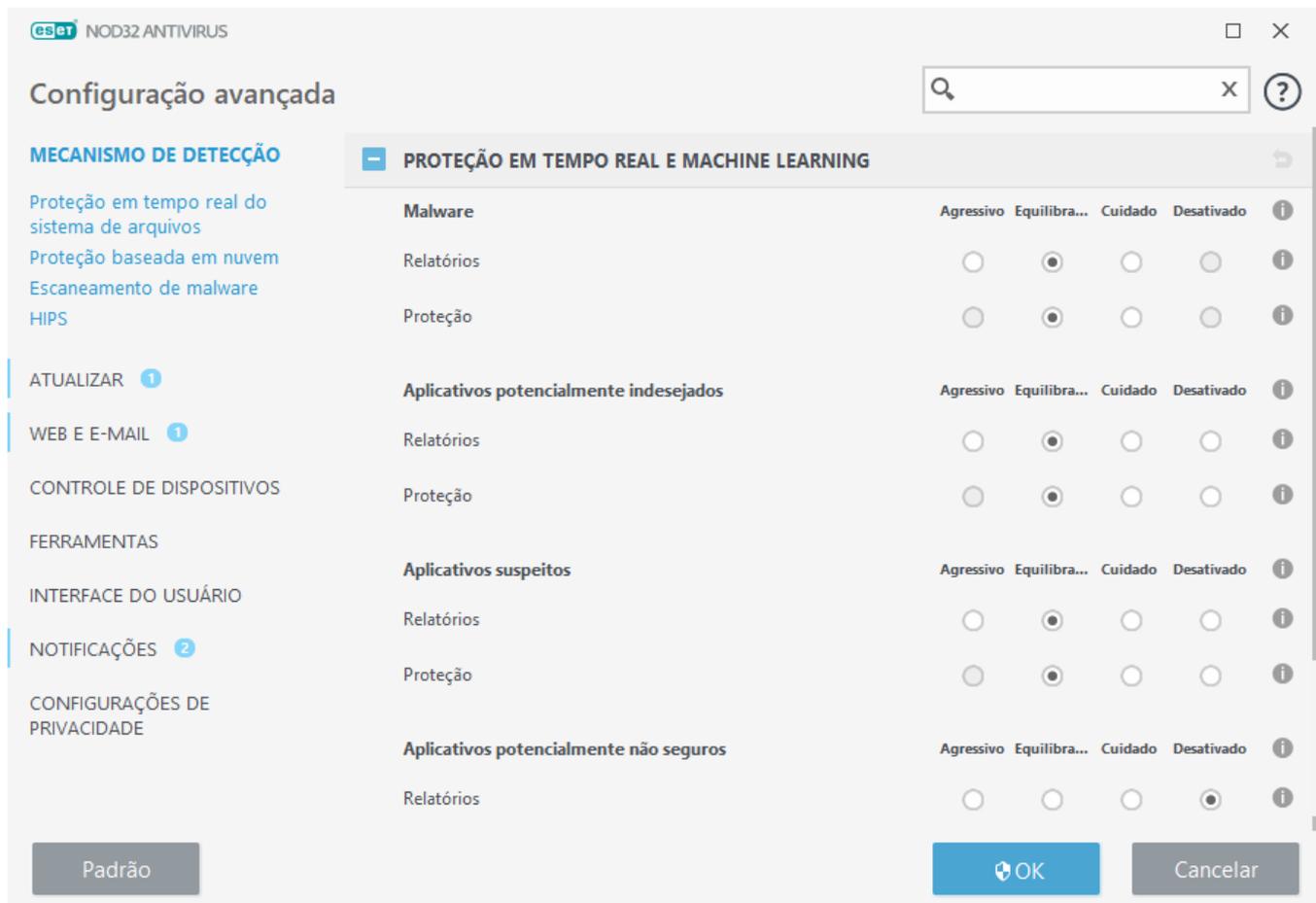
Nesta seção:

- [Categorias de Proteção em tempo real e Machine learning](#)
- [Escanear o computador](#)
- [Configuração de relatórios](#)

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



### Proteção aprimorada

**i** 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**. Para mais informações, consulte [escaneamentos de malware](#).

## 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 NOD32 Antivirus.

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
<b>Agressivo</b>	Relatório de CATEGORIA configurado para sensibilidade máxima. Mais detecções serão reportadas. A configuração <b>Agressiva</b> pode identificar erroneamente os objetos como CATEGORIA.
<b>Equilibrado</b>	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.
<b>Cuidadoso</b>	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.
<b>Desativar</b>	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 NOD32 Antivirus](#)

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 NOD32 Antivirus da versão 13.1 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 NOD32 Antivirus**.
2. Na tela **Sobre**, a primeira linha de texto exibe o número de versão do seu produto ESET.
3. Clique em **Componentes instalados** 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 NOD32 Antivirus (13.0 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 NOD32 Antivirus 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
<b>Agressivo</b>	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.
<b>Equilibrado</b>	As detecções de nível equilibrado (ou inferior) relatadas são bloqueadas e a correção automática (ou seja, limpeza) é iniciada.
<b>Cuidadoso</b>	As detecções reportadas de nível de cuidado são bloqueadas e a correção automática (ou seja, limpeza) é iniciada.
<b>Desativar</b>	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 para o ESET NOD32 Antivirus 13.0 e versões anteriores](#)

Ao atualizar das versões 13.0 e versões anteriores para a versão 13.1 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

# 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 Rastreamento Microsoft Antimalware que dá aos desenvolvedores de aplicativos novas defesas contra malware (apenas Windows 10).

## Uma infiltração foi detectada

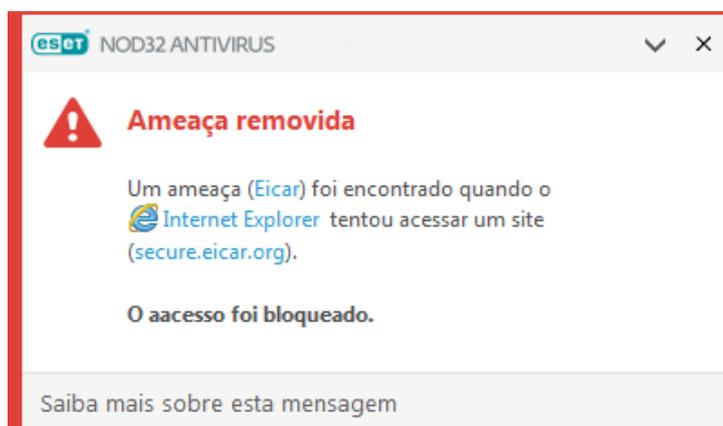
As ameaças podem alcançar o sistema a partir de vários pontos de entrada, tais como [páginas da web](#), pastas compartilhadas, via email ou [dispositivos removíveis](#) (USB, discos externos, CDs, DVDs, etc.).

## Comportamento padrão

Como um exemplo geral de como as infiltrações são tratadas pelo ESET NOD32 Antivirus, 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 [Nível de limpeza](#).



## Escaneando o computador em busca de arquivos infectados

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:

1. Abra o ESET NOD32 Antivirus e clique em **Escanear o computador**.

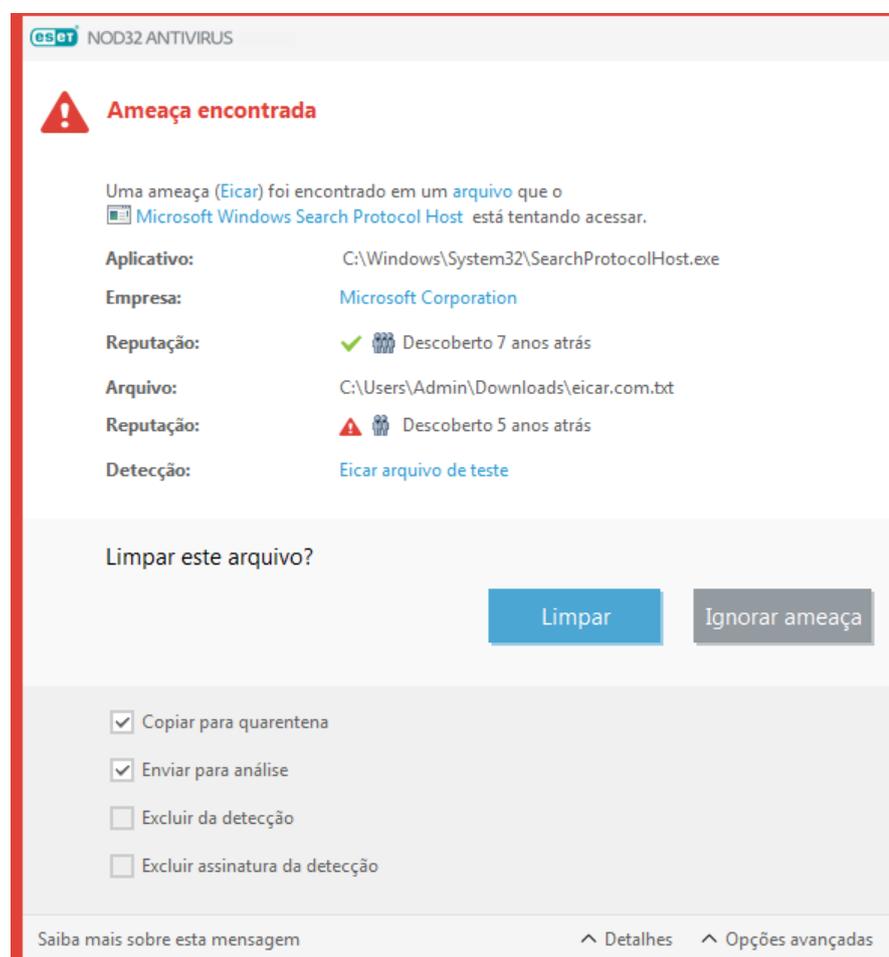
2. Clique em **Rastrear seu computador** (para obter mais informações, consulte [Escanear o computador](#)).

3. Após o rastreamento ter terminado, revise o relatório para obter informações como o número dos arquivos verificados, 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.

## 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 NOD32 Antivirus 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

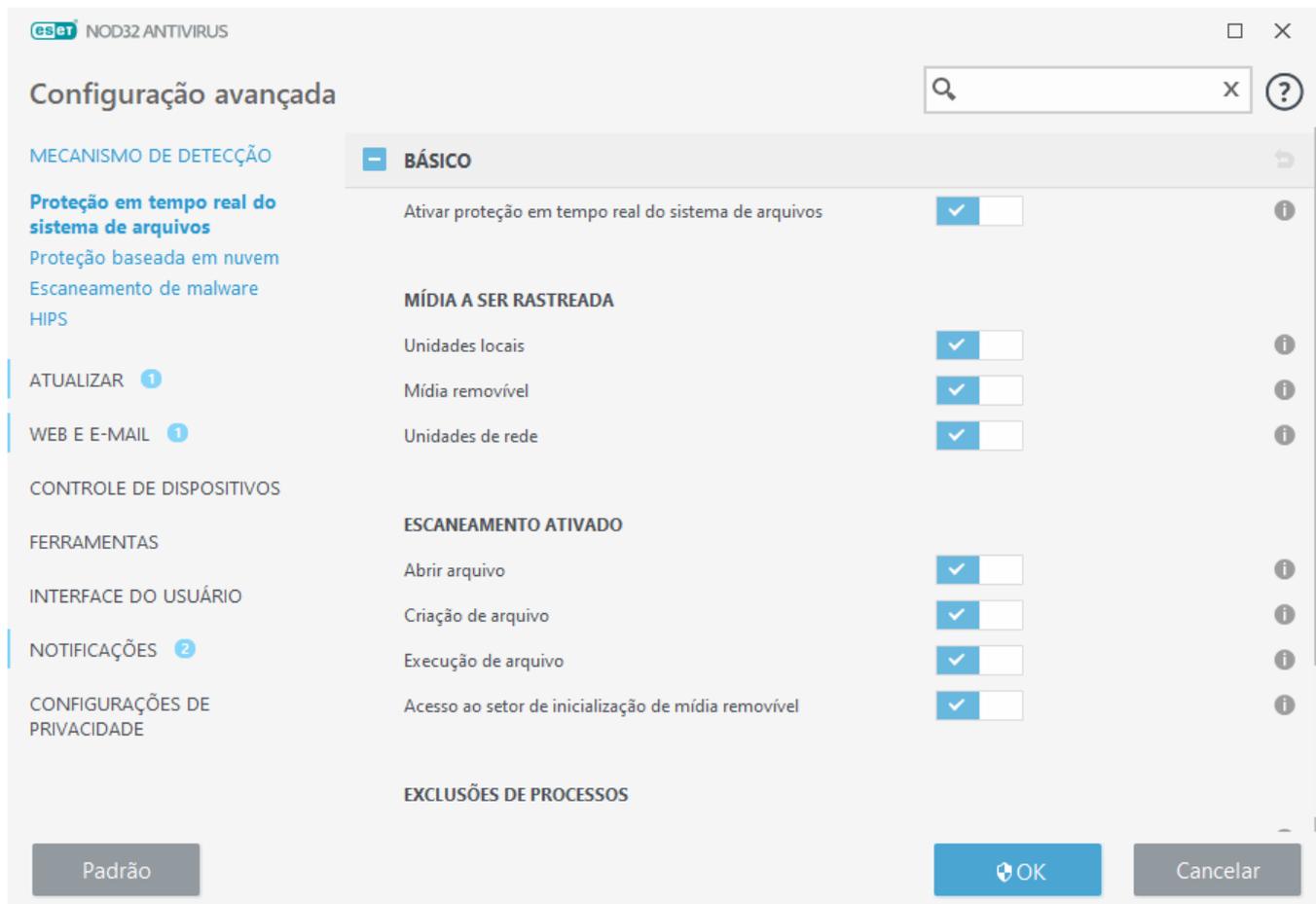
Se quaisquer arquivos infectados não foram limpos durante um rastreamento de computador (ou o [nível de limpeza](#) estava configurado como **Sem limpeza**), será exibida uma janela de alerta solicitando a você que selecione as ações adequadas para esses arquivos. Selecione ações para os arquivos (as ações são definidas individualmente para cada arquivo na lista) e clique em **Fim**.

## 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.

## 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 rastreadas 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.

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). Os arquivos são rastreados novamente logo após 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 **Parâmetro do ThreatSense > Outro** e marque ou desmarque **Ativar otimização inteligente**.

## 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 localize **Limpeza > Nível de limpeza**.

Os parâmetros do ThreatSense têm os seguintes níveis de correção (ou seja, limpeza).

### Correção no ESET NOD32 Antivirus

Nível de limpeza	Descrição
<b>Sempre corrigir a detecção</b>	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.
<b>Corrigir a detecção se for seguro, se não, manter</b>	Tenta corrigir a detecção durante a limpeza dos <a href="#">objetos</a> 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.
<b>Corrigir a detecção se for seguro, se não, perguntar</b>	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.

Nível de limpeza	Descrição
<b>Sempre perguntar ao usuário final</b>	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.

## Quando modificar a configuração da proteção em tempo real

A proteção 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 NOD32 Antivirus, 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**).

## 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 [www.eicar.com](http://www.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.

## 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 resolver o problema, [crie um Relatório do SysInspector e envie-o para o Suporte técnico ESET para análise](#).

## 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. 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.

**i** Não confunda isso com as [Extensões de arquivo excluídas](#), [Exclusões HIPS](#), [Exclusões de detecção](#) ou [Exclusões de desempenho](#).

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 NOD32 Antivirus 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.

**i** 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 NOD32 Antivirus 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.

## 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, o ESET LiveGrid® nos permite reagir imediatamente às necessidades de nossos clientes e manter a ESET sensível às ameaças mais recentes.

As opções disponíveis são:

### Ativa o sistema de reputação 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®.

### Ativar o sistema de feedback ESET LiveGrid®

Além do sistema de reputação ESET LiveGrid®, o sistema de feedback ESET LiveGrid® coletará informações sobre seu computador relacionadas a ameaças recém-detectadas. Essas informações podem incluir:

- Amostra ou cópia do arquivo no qual a ameaça apareceu
- Caminho para o arquivo
- Nome do arquivo

- Data e hora
- O processo pelo qual a ameaça apareceu em seu computador
- Informações sobre o sistema operacional do seu computador

Por padrão, o ESET NOD32 Antivirus é configurado enviar arquivos suspeitos ao Laboratório de vírus da ESET para análise detalhada. Os arquivos com certas extensões, como *.doc* ou *.xls*, são sempre excluídos. Você também pode adicionar outras extensões se houver arquivos específicos cujo envio você ou sua empresa desejam impedir.

**i** Leia mais sobre o envio dos dados relevantes na [Política de Privacidade](#).

## Você pode escolher não ativar o ESET LiveGrid®

Você não perderá nenhuma funcionalidade do software, mas, em alguns casos, o ESET NOD32 Antivirus poderá responder mais rápido a novas ameaças quando o ESET LiveGrid® estiver ativado. 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.

**i** Leia mais sobre ESET LiveGrid® no [glossário](#).  
Veja nossas [instruções ilustradas](#) disponíveis em inglês e em vários outros idiomas para a ativação ou desativação do ESET LiveGrid® no ESET NOD32 Antivirus.

## Configuração da proteção baseada em nuvem na Configuração avançada

Para acessar as configurações do ESET LiveGrid®, abra a **Configuração avançada (F5) > 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.
- **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](#).

### Envio automático de amostras detectadas

Selecione qual tipo de amostras serão enviadas para a ESET para análise e para melhorar a detecção futura (o tamanho máximo de amostra padrão é 64 MB). 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 se não forem detectadas pelo mecanismo de detecção. Por exemplo, amostras que quase foram perdidas pela detecção, ou se um dos [módulos de proteção](#) do ESET NOD32 Antivirus considerar essas amostras como suspeitas ou como tendo um comportamento incerto (o tamanho máximo de amostra padrão é 64 MB).

- **Executáveis** – Inclui arquivos executáveis 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 de script 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 para uma lista de todos os tipos de arquivo de documento incluídos](#)

ACCDB, ACCDT, DOC, DOC\_OLD, DOC\_XML, DOCM, DOCX, DWF, 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, XLST, XLSTML, 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 > Mecanismo de detecção > Proteção baseada em nuvem > Envio de amostras** e clique em **Editar** ao lado de **Exclusões**. Adicione a exclusão `.download.domain.com`.

**Tamanho máximo das amostras (MB)** – Define o tamanho máximo das amostras (1-64 MB).

## Filtro de exclusões para Proteção baseada em nuvem

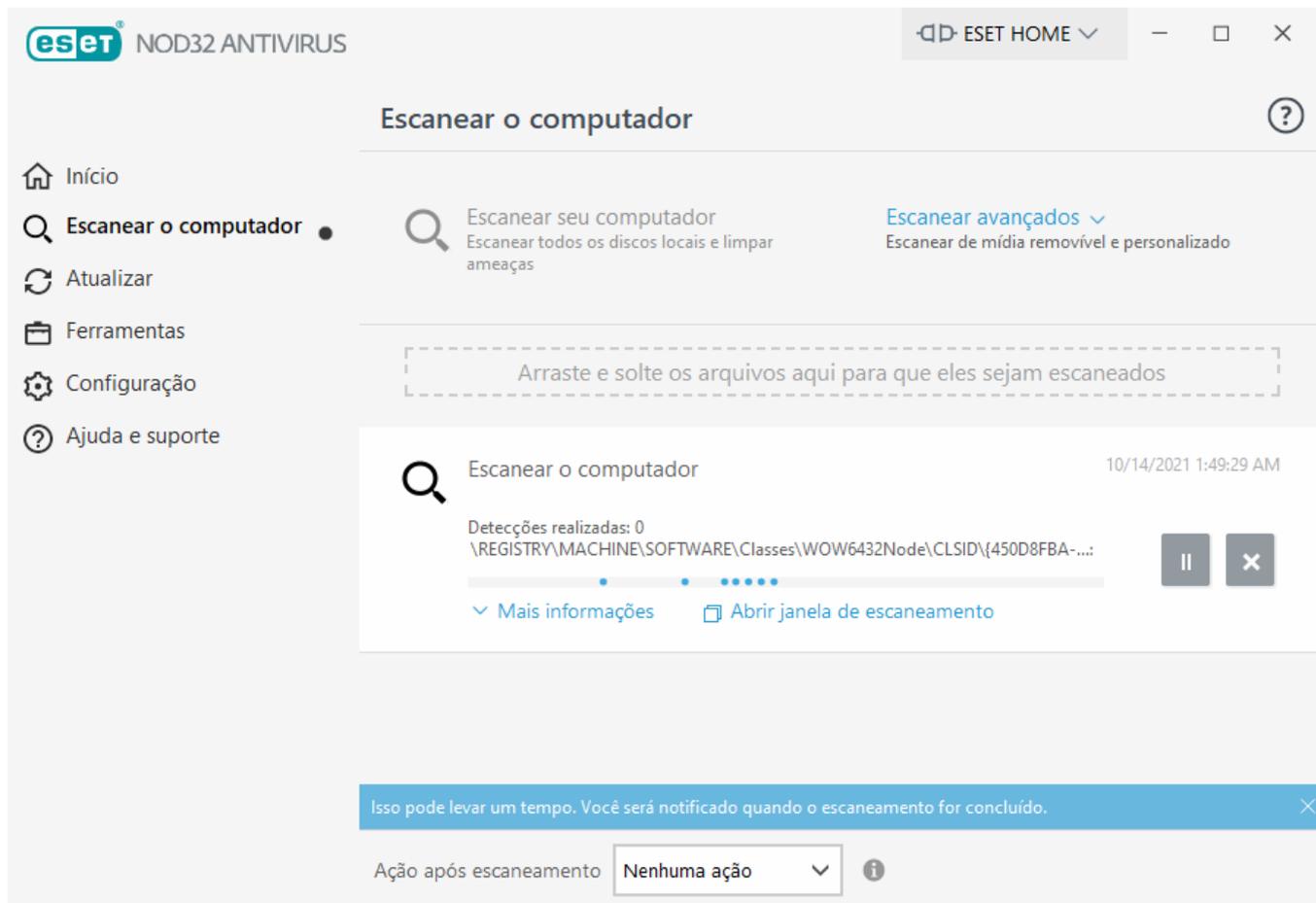
O Filtro de exclusões permite excluir determinados arquivos ou pastas do envio de amostras. Os arquivos relacionados nunca serão enviados aos laboratórios da ESET para análise, mesmo se incluírem um código suspeito. Os tipos de arquivos comuns (como `.doc`, etc.) são excluídos por padrão.

**i** Este recurso é útil para excluir arquivos que podem conter informações sigilosas, como documentos ou planilhas.

✓ Para excluir arquivos baixados de `download.domain.com`, clique em **Configuração avançada > Mecanismo de detecção > Proteção baseada em nuvem > Envio de amostras > Exclusões** e adicione a exclusão `*download.domain.com*`.

## Escanear o computador

O escaneador sob demanda é uma parte importante da sua solução antivírus. Ele é usado para realizar escaneamento nos arquivos e pastas do seu computador. Do ponto de vista da segurança, é fundamental que os escaneamentos do computador sejam executados regularmente como parte das medidas usuais de segurança, não apenas quando há suspeita de uma infecção. Recomendamos que você realize escaneamentos detalhados regulares do sistema para detectar vírus que não tenham sido capturados pela [Proteção em tempo real do sistema de arquivos](#) quando foram gravados no disco. 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 o arquivo não for detectado como vírus ao ser salvo no disco.



Há dois tipos de **Escaneamento do computador** disponíveis. **Escanear seu computador** escaneia rapidamente o sistema sem especificar os parâmetros de escaneamento. O **Escaneamento personalizado** (sob Escaneamento avançado) permite selecionar qualquer perfil de escaneamento predefinido para locais de destino específicos, e também permite escolher destinos de escaneamento específicos.

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

Por padrão, o ESET NOD32 Antivirus tenta limpar ou remover automaticamente as detecções encontradas durante o escaneamento do computador. Em alguns casos, se nenhuma ação puder ser realizada, você receberá um alerta interativo e deverá selecionar uma ação de limpeza (por exemplo, remover ou ignorar). Para alterar o nível de limpeza e para informações mais detalhadas, consulte [Limpeza](#). Para revisar os escaneamentos anteriores, consulte [Arquivos de relatório](#).

## Escanear seu computador

**Escan seu computador** permite que você inicie rapidamente um escanear o computador e limpe arquivos infectados, sem a necessidade de intervenção do usuário. A vantagem de **Escan seu computador** é que ele é fácil de operar e não requer configuração de rastreamento detalhada. Este rastreamento 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](#).

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.

As opções de rastreamento a seguir estão disponíveis em **Escaneamentos avançados**:



## Escaneamento personalizado

O **escaneamento personalizado** permite especificar parâmetros de escaneamento, como destinos de escaneamento e métodos. A vantagem do **Escaneamento personalizado** é que você pode 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.



## 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 rastreamento também pode ser iniciado clicando em **Escaneamento personalizado**, selecionando **Mídia removível** no menu suspenso **Alvos de escaneamento** e clicando em **Escanear**.



## Repetir o último escaneamento

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

O menu suspenso **Ação após escaneamento** permite definir uma ação a ser realizada automaticamente depois do escaneamento ser finalizado:

- **Nenhuma ação** - Depois do fim do rastreamento, nenhuma ação será realizada.
- **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** – o computador será reiniciado se necessário apenas para concluir a limpeza das ameaças detectadas.
- **Forçar reinicialização** – força o encerramento de todos os programas abertos sem esperar pela interação do usuário e reinicia o computador depois do fim do escaneamento.
- **Forçar reinicialização se necessário** – o computador será reiniciado se necessário apenas para concluir a limpeza das ameaças detectadas.
- **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. Sua computador é desligado, mas vai voltar ao seu estado anterior da próxima vez que for iniciado.

**i** As ações de **Suspender** ou **Hibernar** estão disponíveis com base nas configurações do sistema operacional de Energia e hibernação ou das capacidades do seu computador/notebook. Lembre-se 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.

A ação selecionada será iniciada depois de todos os escaneamentos em execução serem concluídos. Quando você seleciona **Desligar** ou **Reiniciar**, uma janela de diálogo de confirmação exibirá uma contagem regressiva de 30 segundos (clique em **Cancelar** para desativar a ação solicitada).

**i** 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

Você pode usar o Escaneamento personalizado para escanear a memória operacional, a rede ou partes específicas de um disco, em vez de todo o disco. Para fazer isso, clique em **Escaneamentos avançados > Escaneamento personalizado** e selecione destinos específicos da estrutura de pasta (árvore).

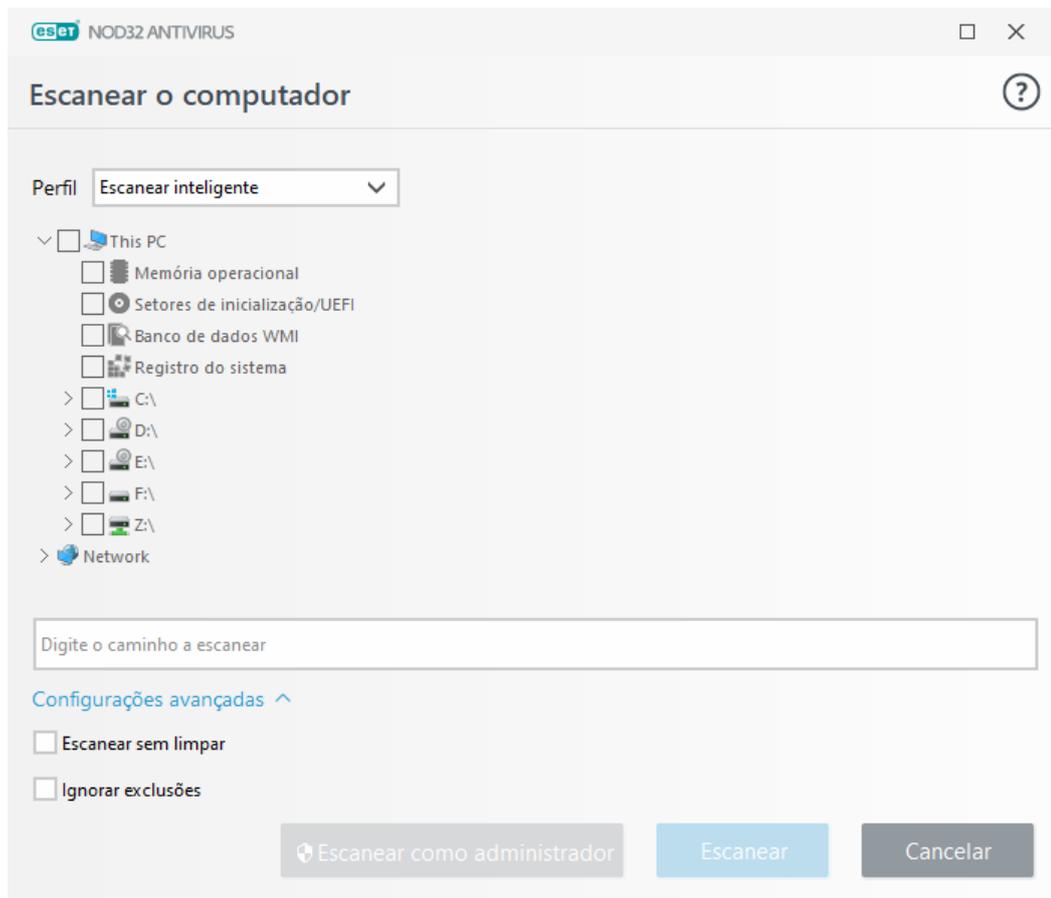
Você pode escolher um perfil no menu suspenso **Perfil** para ser usado durante o escaneamento dos alvos específicos. O perfil padrão é **Escaneamento inteligente**. Há mais três perfis de escaneamento predefinidos chamados de **Escaneamento detalhado** e **Escaneamento do menu de contexto** e **Escaneamento do computador**. Estes perfis de escaneamento usam [parâmetros ThreatSense](#) diferentes. As opções disponíveis são descritas em **Configuração avançada (F5) > Mecanismo de detecção > Escaneamentos de malware > Escaneamento sob demanda > [Parâmetros ThreatSense](#)**.

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.

**i** [Como agendar um escanear semanal do computador](#)  
Para agendar uma tarefa regular, leia o capítulo [Como agendar um escaneamento do computador semanal](#).



Você pode configurar os parâmetros de limpeza para o escaneamento em **Configuração avançada (F5) > Mecanismo de detecção > Escaneamento sob demanda > Parâmetros ThreatSense > Limpeza**. Para executar um escaneamento sem ação de limpeza, clique em **Configurações avançadas** e 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 excluídas escaneados sem exceção.

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

**Rastrear como administrador** permite que você execute o rastreamento usando a conta do administrador. Use isso se o usuário atual não tem privilégios para acessar os arquivos que você deseja rastrear. Esse botão não estará disponível se o usuário atual não puder acionar operações de UAC como Administrador.

**i** 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.

**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. Mais detalhes podem ser encontrados em nosso [artigo da Base de conhecimento](#).



## Como agendar um escanear semanal do computador

Para agendar uma tarefa regular, leia o capítulo [Como agendar um escaneamento do computador semanal](#).

**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 arquivos rastreados, ameaças encontradas e ameaças limpas 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.



Clique na lupa ou seta para mostrar detalhes sobre o escaneamento que está atualmente em execução. Você pode executar outro escaneamento paralelo clicando em **Escanear seu computador** ou **Escaneamentos avançados > Escaneamento personalizado**.

The screenshot displays the ESET NOD32 ANTIVIRUS interface. The main window is titled "Escanear o computador". On the left, there is a navigation menu with options: "Início", "Escanear o computador" (selected), "Atualizar", "Ferramentas", "Configuração", and "Ajuda e suporte". The main content area shows two scanning options: "Escanear seu computador" (Escanear todos os discos locais e limpar ameaças) and "Escanear avançados" (Escanear de mídia removível e personalizado). Below these is a dashed box with the text "Arraste e solte os arquivos aqui para que eles sejam escaneados". A progress bar is visible with the text "Escanear o computador" and "10/14/2021 1:49:29 AM". The progress bar shows "Detecções realizadas: 0" and a list of registry paths: "\REGISTRY\MACHINE\SOFTWARE\Classes\WOW6432Node\CLSID\{450D8FBA-...:". There are buttons for "Mais informações" and "Abrir janela de escaneamento". At the bottom, there is a notification bar that says "Isso pode levar um tempo. Você será notificado quando o escaneamento for concluído." and a dropdown menu for "Ação após escaneamento" set to "Nenhuma ação".

O menu suspenso **Ação após escaneamento** permite definir uma ação a ser realizada automaticamente depois do

escaneamento ser finalizado:

- **Nenhuma ação** - Depois do fim do rastreamento, nenhuma ação será realizada.
- **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** – o computador será reiniciado se necessário apenas para concluir a limpeza das ameaças detectadas.
- **Forçar reinicialização** – força o encerramento de todos os programas abertos sem esperar pela interação do usuário e reinicia o computador depois do fim do escaneamento.
- **Forçar reinicialização se necessário** – o computador será reiniciado se necessário apenas para concluir a limpeza das ameaças detectadas.
- **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. Sua computador é desligado, mas vai voltar ao seu estado anterior da próxima vez que for iniciado.

**i** As ações de **Suspender** ou **Hibernar** estão disponíveis com base nas configurações do sistema operacional de Energia e hibernação ou das capacidades do seu computador/notebook. Lembre-se 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.

A ação selecionada será iniciada depois de todos os escaneamentos em execução serem concluídos. Quando você seleciona **Desligar** ou **Reiniciar**, uma janela de diálogo de confirmação exibirá uma contagem regressiva de 30 segundos (clique em **Cancelar** para desativar a ação solicitada).

## Relatório de escaneamento do computador

Quando o escaneamento for concluído, o [Relatório do escaneamento do computador](#) será aberto com todas as informações relevantes relacionadas ao escaneamento em particular. O relatório do escaneamento fornece informações como:

- Versão do mecanismo de detecção
- Data e hora de início
- Lista de discos, pastas e arquivos escaneados
- Nome do escaneamento programado (apenas [escaneamento programado](#))
- Status do escaneamento
- Número de objetos rastreados

- Número de detecções encontradas
- Hora da conclusão
- Tempo total do rastreamento

**i** Um novo início de uma [tarefa agendada de escaneamento do computador](#) será ignorado se a mesma tarefa agendada que foi executada anteriormente ainda estiver em execução. A tarefa de escaneamento programado ignorada vai criar um relatório do escaneamento do computador com 0 objetos escaneados e o status **Escaneamento não iniciado porque o escaneamento anterior ainda estava em execução**.

Para encontrar relatórios do escaneamento anteriores, no [janela do programa principal](#) selecione **Ferramentas > Arquivos de relatório**. No menu suspenso, selecione **Escaneamento do computador** e clique duas vezes no registro desejado.

ESET NOD32 ANTIVIRUS

## Escaneamento do computador

Relatório do escaneamento

Versão do mecanismo de detecção: 22237 (20201030)

Data: 10/30/2020 Hora: 11:58:16 AM

Discos, pastas e arquivos rastreados: Memória operacional; C:\Setores de inicialização/UEFI; C:\Banco de dados WMI; Registro do sistema

Escaneamento finalizado pelo usuário.

Número de objetos rastreados: 1160

Número de detecções: 0

Hora de conclusão: 11:58:28 AM Tempo total do escaneamento: 12 s (00:00:12)

Filtragem

**i** Para saber mais sobre registros "não é possível abrir", "erro ao abrir" e/ou "arquivo danificado", consulte nosso [artigo da Base de conhecimento ESET](#).

Clique no ícone da barra deslizante  **Filtragem** para abrir a janela de [Filtragem de relatórios](#) onde você pode detalhar sua busca por meio de critérios personalizados. Para ver o menu de contexto, clique com o botão direito em uma entrada de relatório específica:

Ação	Uso
Filtrar os mesmos registros	Ativa a filtragem de relatórios. O relatório exibirá apenas registros do mesmo tipo que o registro selecionado.
Filtro	Essa opção abre a janela Filtragem de relatórios e permite a você definir critérios para entradas de relatório específicas. Atalho: <code>Ctrl+Shift+F</code>
Ativar filtro	Ativa as configurações de filtro. Se você ativar o filtro pela primeira vez, será preciso definir as configurações e a janela de Filtragem de relatórios abrirá.
Desativar filtro	Desativa o filtro (assim como clicar na opção na parte de baixo).
Copiar	Copia os registros destacados para a área de transferência. Atalho: <code>Ctrl+C</code>
Copiar tudo	Copia todos os registros na janela.
Exportar	Exporta os registros destacados na área de transferência para um arquivo XML.
Exportar todos	Essa opção exporta todos os registros na janela para um arquivo XML.
Descrição da detecção	Abre a Enciclopédia de ameaças da ESET, que contém informações detalhadas sobre os perigos e os sinais da infiltração destacada.

## Escaneamento de malware

A seção **Escaneamento de malware** pode ser acessada em **Configuração avançada (F5) > Mecanismo de detecção > Escaneamento de malware** e oferece opções para selecionar parâmetros de escaneamento. Essa seção inclui os seguintes itens:

**Perfil selecionado** – Um conjunto particular de parâmetros usados pelo escaneador sob demanda. Para criar um novo, clique em **Editar** ao lado de **Lista de perfis**. Consulte [Perfis de escaneamento](#) para mais detalhes.

**Destinos para escaneamento** – Se você quiser escanear somente um destino específico, poderá clicar em **Editar** ao lado de **Destinos para escaneamento** e escolher 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

Habilite a barra deslizante ao lado de **Ativar escaneamento em estado ocioso** 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 habilitando a barra deslizante ao lado de **Executar mesmo se o computador estiver na bateria** na Configuração avançada.

Habilite a barra deslizante ao lado de **Ativar registro em relatório** na Configuração avançada para gravar uma saída de escaneamento do computador na seção [Arquivos de relatórios](#) (na [janela principal do programa](#), clique em **Ferramentas > Arquivos de relatórios** e em seguida selecione **Escanear o computador** no menu suspenso **Relatório**).

## 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 NOD32 Antivirus:

- **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.

**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 **Sempre corrigir detecção**. 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

O menu suspenso **Alvos** permite selecionar alvos de rastreamento 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.

## Controle de dispositivo

O ESET NOD32 Antivirus fornece controle automático de dispositivos (CD/DVD/USB/...). Esse módulo permite bloquear ou ajustar filtros/permisões 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 (HDD, disco removível USB)
- CD/DVD
- Impressora USB
- FireWire Armazenamento

- BluetoothDispositivo
- Leitor de cartão inteligente
- Dispositivo de criação de imagem
- Modem
- LPT/COM porta
- Dispositivo portátil
- Todos os tipos de dispositivo

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

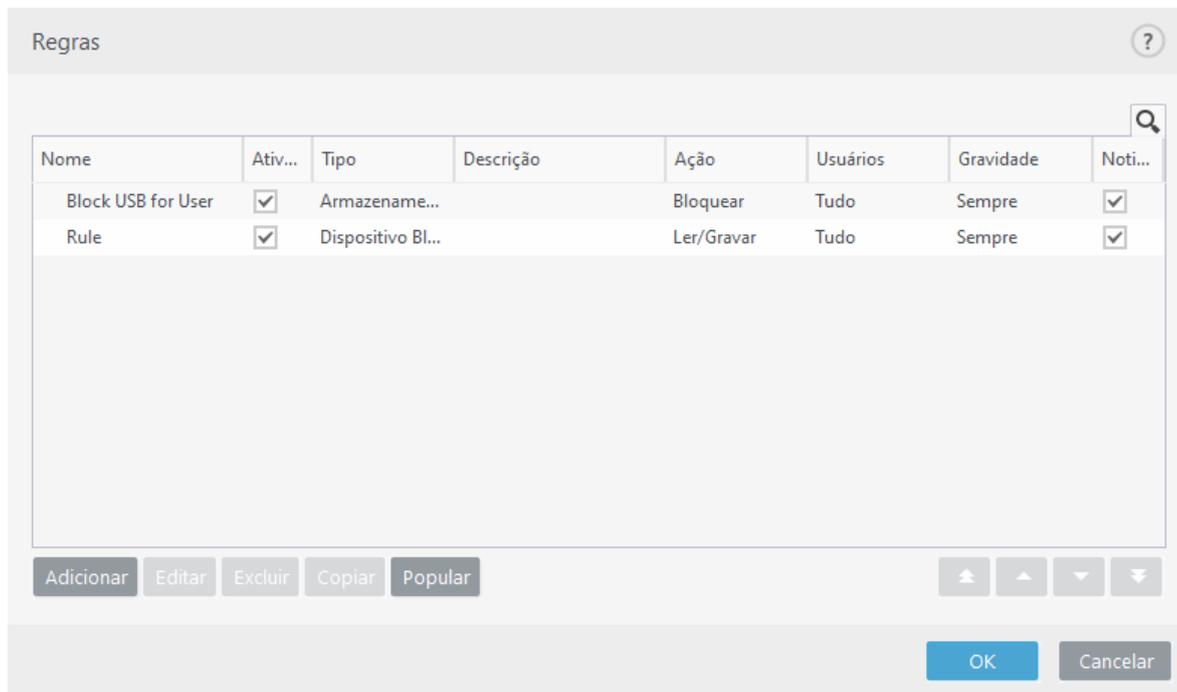
Habilite a barra deslizante ao lado de **Habilitar o controle de dispositivo** para ativar o recurso de Controle de dispositivos no ESET NOD32 Antivirus, você precisará reiniciar o computador para que as alterações tenham efeito. Quando o Controle de dispositivos estiver ativado, as **Regras** ficarão ativas, permitindo abrir a janela do [Editor de regras](#).

**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.

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.



Determinados dispositivos podem ser permitidos ou bloqueados por usuário ou grupo de usuários e com base em parâmetros de dispositivos 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. Veja também [Adicionar regras de controle de dispositivo](#).

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. As cadeias XML exibidas ao clicar em uma regra podem ser copiadas para a área de transferência para ajudar os administradores do sistema a exportarem/importarem esses dados e usá-los.

Ao pressionar **CTRL** e clicar, é possível selecionar mais de uma regra e aplicar as ações, tais como excluí-las ou movê-las para cima e para baixo na lista, em 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.

O controle é realizado por regras classificadas na ordem que determina sua prioridade, com regras de prioridade mais alta na parte superior.

As entradas de relatórios podem ser visualizadas a partir da janela principal do ESET NOD32 Antivirus em **Ferramentas > Relatórios**.

O relatório de controle de dispositivos registra todas as ocorrências nas quais o controle de dispositivos é acionado.

## 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.

A imagem mostra a interface de usuário para editar uma regra. O formulário contém os seguintes campos:

- Nome:** Campo de texto com o valor "Block USB for User".
- Regra ativada:** Botão de alternância com uma seta para cima e para baixo, atualmente em posição "ativada".
- Tipo de dispositivo:** Menu suspenso com o valor "Armazenamento em disco".
- Ação:** Menu suspenso com o valor "Bloquear".
- Tipo de critério:** Menu suspenso com o valor "Dispositivo".
- Fabricante:** Campo de texto vazio.
- Modelo:** Campo de texto vazio.
- Número de série:** Campo de texto vazio.
- Gravidade do registro em log:** Menu suspenso com o valor "Sempre".
- Lista de usuários:** Botão "Editar".
- Notificar usuário:** Botão de alternância com uma seta para cima e para baixo, atualmente em posição "ativada".

Um botão "OK" azul está localizado no canto inferior direito do formulário.

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

### 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.

## 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 não 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 não 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

O ESET NOD32 Antivirus salva eventos importantes em um arquivo de relatório, que pode ser exibido diretamente no menu principal. Clique em **Ferramentas > Arquivos de relatório** e então selecione **Controle de dispositivos** no menu suspenso **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.
- **Aviso** – Registra mensagens de erros críticos e de aviso.
- **Nenhum** - Nenhum registro em relatório será feito.

## Lista de usuários

As regras podem ser limitadas a determinados usuários ou grupos de usuários adicionando-os à Lista de usuários ao clicar em **Editar** ao lado da **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.

### Limitações da lista de usuário

A Lista de usuários não pode ser definida para regras com [Tipos de dispositivos](#) específicos:



- Impressora USB
- Dispositivo Bluetooth
- Leitor de cartão inteligente
- Dispositivo de imagens
- Modem
- Porta LPT/COM

**Notificar usuário** – se um dispositivo bloqueado por uma regra existente for inserido, uma janela de notificação será exibida.

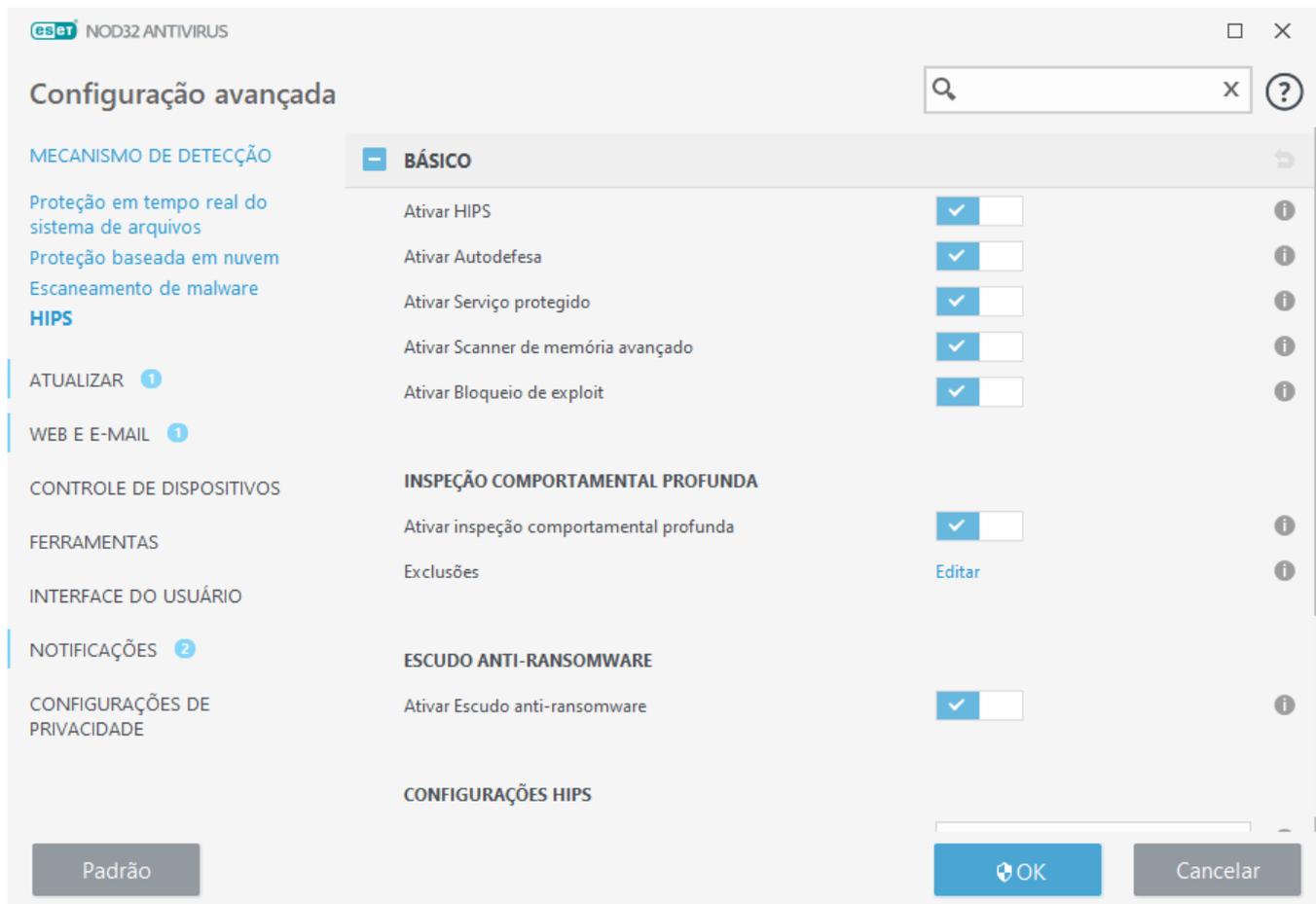
## Sistema de prevenção de intrusos de host (HIPS)



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.

Configurações HIPS podem ser encontradas em **Configuração avançada (F5) > Mecanismo de detecção > HIPS > Básico**. O estado HIPS (ativado/desativado) é mostrado na [janela principal do programa](#) ESET NOD32 Antivirus, em **Configuração > Proteção do computador**.



## Básico

**Ativar HIPS** – O HIPS está ativado por padrão no ESET NOD32 Antivirus. Desativar o HIPS vai desativar o restante dos recursos HIPS como o Bloqueio de Exploit.

**Ativar Autodefesa** – O ESET NOD32 Antivirus 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.

**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 versões posteriores.

**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.](#)

## Configurações HIPS

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

Modo de filtragem	Descrição
<b>Modo automático</b>	As operações são ativadas, exceto aquelas bloqueadas por regras predefinidas que protegem o sistema.
<b>Modo Smart</b>	O usuário será notificado apenas sobre eventos muito suspeitos.
<b>Modo interativo</b>	O sistema solicitará que o usuário confirme as operações.
<b>Modo com base em políticas</b>	Bloqueia todas as operações que não são definidas por uma regra específica que permita essas operações.
<b>Modo de aprendizagem</b>	As operações são ativadas e uma regra é criada após cada operação. As regras criadas nesse modo podem ser visualizadas no editor de <b>Regras HIPS</b> , mas sua prioridade é menor que a prioridade das regras criadas manualmente ou das regras criadas no modo automático. Quando selecionar o <b>Modo de aprendizagem</b> do menu suspenso <b>Modo de filtragem</b> , a configuração <b>Modo de aprendizagem vai terminar em</b> 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.

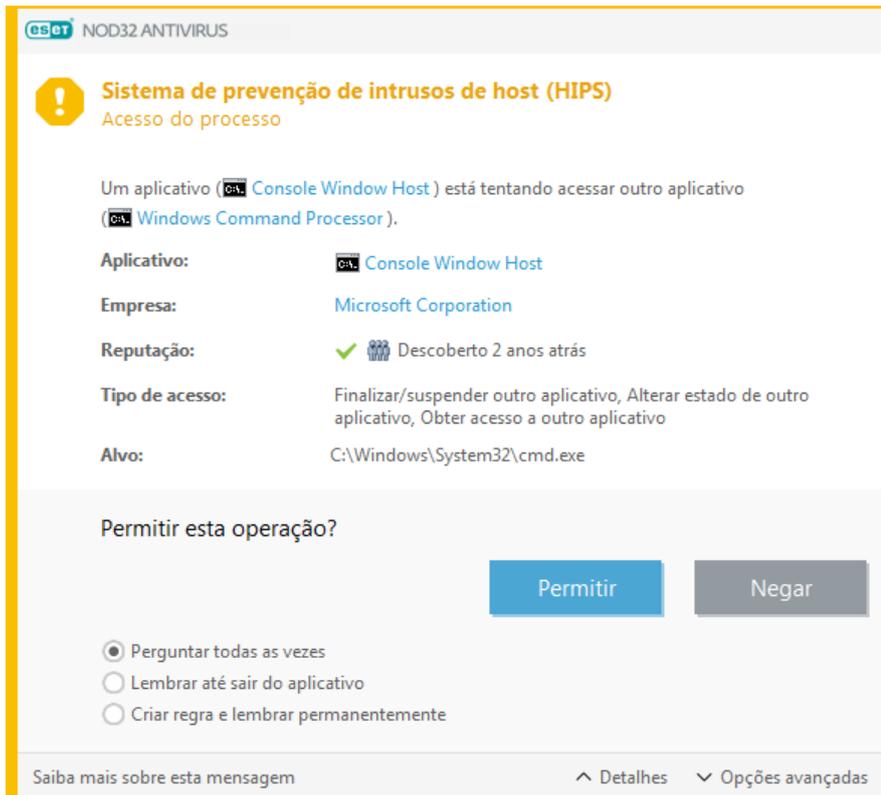
É possível acessar configurações para parâmetros de regra mais detalhados clicando em **Opções avançadas**. As opções abaixo estarão disponíveis se você escolher **Criar regra e lembrar permanentemente**:

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

#### Notificações do HIPS infinitas?

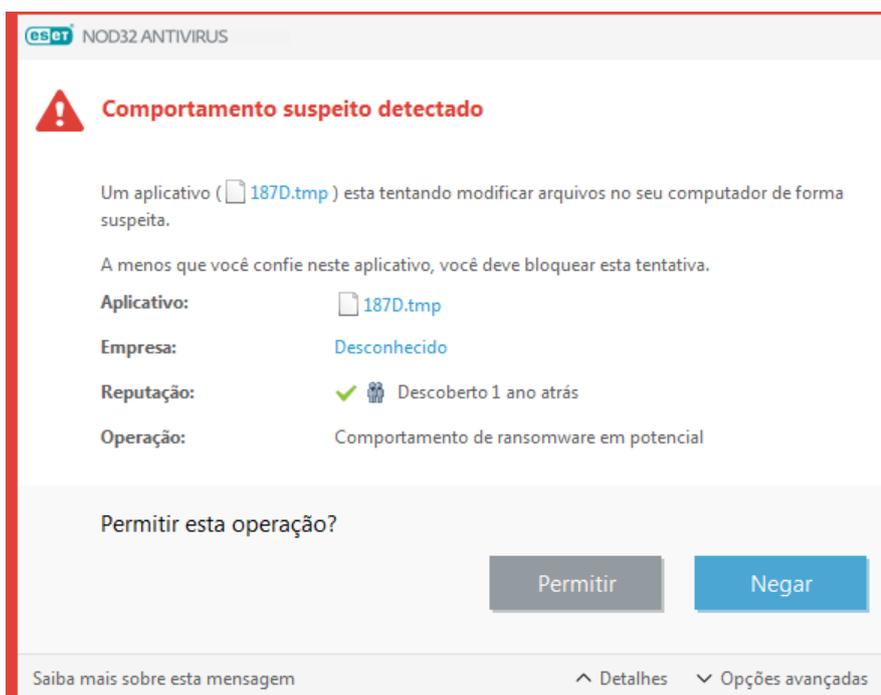


Para impedir que as notificações apareçam, mude o modo de filtragem para o **Modo automático** na **Configuração avançada (F5) > Mecanismo de detecção > HIPS > Básico**.



## 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

Uma lista de regras adicionadas automaticamente e definidas pelo usuário do 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 a barra deslizante 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 janela 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.

- 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)

# Editar uma regra HIPS

Consulte primeiro o [gerenciamento de regras do 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 a barra deslizante 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 digitar manualmente, ou clique em **Abrir o editor do registro** para selecionar uma chave no Registro. Também é possível selecionar **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.

Descrição de operações importantes:

## Operações de arquivo

- **Excluir arquivo** - O aplicativo está solicitando permissão para excluir o arquivo de destino.
- **Gravar no arquivo** - O aplicativo está solicitando permissão para gravar no arquivo de destino.
- **Acesso direto ao disco** - O aplicativo está tentando ler do disco ou gravar no disco de forma não padrão, o

que poderá impedir procedimentos comuns do Windows. Isso pode resultar na alteração de arquivos sem a aplicação das regras correspondentes. Essa operação poderá ser causada por um malware que está tentando impedir a detecção, um software de backup tentando realizar uma cópia exata de um disco ou um gerenciador de partição tentando reorganizar volumes do disco.

- **Instalar vínculo global** – Refere-se à chamada da função SetWindowsHookEx da biblioteca do MSDN.
- **Carregar unidade** - Instalação e carregamento de unidades no sistema.

## 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.

**i** 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.

Ao informar um destino, você poderá utilizar caracteres curingas, mas com certas restrições. Em vez de uma chave específica, o símbolo \* (asterisco) pode ser utilizado nos caminhos do registro. Por exemplo `HKEY_USERS\*\software` pode significar `HKEY_USER\.default\software`, mas não `HKEY_USERS\S-1-2-21-2928335913-73762274-491795397-7895\.default\software`.

**i** `HKEY_LOCAL_MACHINE\system\ControlSet*` não é um caminho válido de chave de registro. Um caminho de chave de registro que contém \\* significa que "este caminho ou qualquer caminho em qualquer nível após esse símbolo". Esta é a única forma de usar os curingas em destinos de arquivo. Primeiro, a parte específica de um caminho será avaliada e, em seguida, o caminho após o símbolo curinga (\*).

 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. Habilite a barra do controle deslizante ao lado de **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.

**eset** NOD32 ANTIVIRUS

Configurações de regra HIPS

Nome da regra: Sem título

Ação: Permitir

Operações afetando:

- Arquivos de destino:  X
- Aplicativos:  X
- Entradas do registro:  X

Ativado:

Gravidade do registro em log: Nenhum

Notificar usuário:  X

Voltar Avançar Cancelar

## Adicionar caminho de registro/aplicativo para HIPS

Selecione o caminho de aplicativo do arquivo clicando na opção .... Ao selecionar uma pasta, todos os aplicativos que constam nesse local serão incluídos.

A opção **Abrir o editor do registro** abrirá o editor do registro do Windows (regedit). Ao adicionar um caminho de registro, insira o local correto no campo **Valor**.

Exemplos de caminho de arquivo ou registro:

- *C:\Program Files\Internet Explorer\iexplore.exe*
- *HKEY\_LOCAL\_MACHINE\system\ControlSet*

## 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 jogador

O modo jogador 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. Ao ativar esse recurso, todas as janelas pop-up são desativadas e a atividade da agenda será completamente interrompida. A proteção do sistema ainda é executada em segundo plano, mas não requer interação com nenhum usuário.

É possível ativar ou desativar o Modo gamer na [janela principal do programa](#) em **Configuração > Proteção do computador** clicando em  ou  ao lado de **Modo gamer**. Ativar automaticamente o Modo gamer é um risco de segurança em potencial, pois o ícone do status da 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 gamer ativado** será exibida em laranja.

Ative o **Ativar automaticamente o modo de jogador ao executar aplicativos em tela cheia** em **Configuração avançada (F5) > Ferramentas > Modo de jogador** para que o Modo de jogador seja iniciado sempre que você iniciar um aplicativo em tela cheia e pare depois que você sair do aplicativo.

Ative **Desativar o modo jogador automaticamente após** para definir o período de tempo após o qual o modo de jogador será desativado automaticamente.

## Rastreamento na inicialização

Por padrão a verificação automática de arquivo na inicialização será realizada na inicialização do sistema e durante a atualização do mecanismo de detecção. 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 alterar suas configurações, vá para **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 escaneados estão fixas para cada grupo acima. Se você escolher uma profundidade inferior do escaneamento para arquivos executados na inicialização do sistema, os arquivos não escaneados serão escaneados ao serem abertos ou executados.

**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 (F5) > Mecanismo de detecção > Escaneamento de malware > Proteção de documentos** e clique na barra deslizante ao lado de **Habilitar proteção de documento**.

**i** 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 detecção 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.

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**.

**i** Não confunda isso com as [Exclusões de detecção](#), [Extensões de arquivo excluídas](#), [Exclusões HIPS](#) ou [Exclusões de processos](#).

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.

A imagem mostra a janela de configuração 'Exclusões de desempenho'. No topo, há um ícone de ajuda (?). Abaixo, há uma barra de pesquisa. O conteúdo principal é uma tabela com duas colunas: 'Excluir caminho' e 'Comentário'. A tabela contém duas entradas: 'C:\Backup\\*' e 'C:\pagefile.sys'. Na base da janela, há botões para 'Adicionar', 'Editar', 'Excluir', 'Importar', 'Exportar', 'OK' e 'Cancelar'.

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

## Adicionar ou editar exclusões de desempenho

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

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

Editar exclusão

Caminho: C:\Backup\\*

Comentário:

OK Cancelar

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.

### Formato da exclusão

- Se você desejar excluir todos os arquivos e subpastas em uma pasta, digite o caminho para a pasta e use a máscara \*
- Se você desejar 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.

### Variáveis do sistema nas exclusões

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.

### Não é possível colocar caracteres curinga no meio de um caminho

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.
- ✓ 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.

### Formato da exclusão

- 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.

## Variáveis do sistema nas exclusões

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.

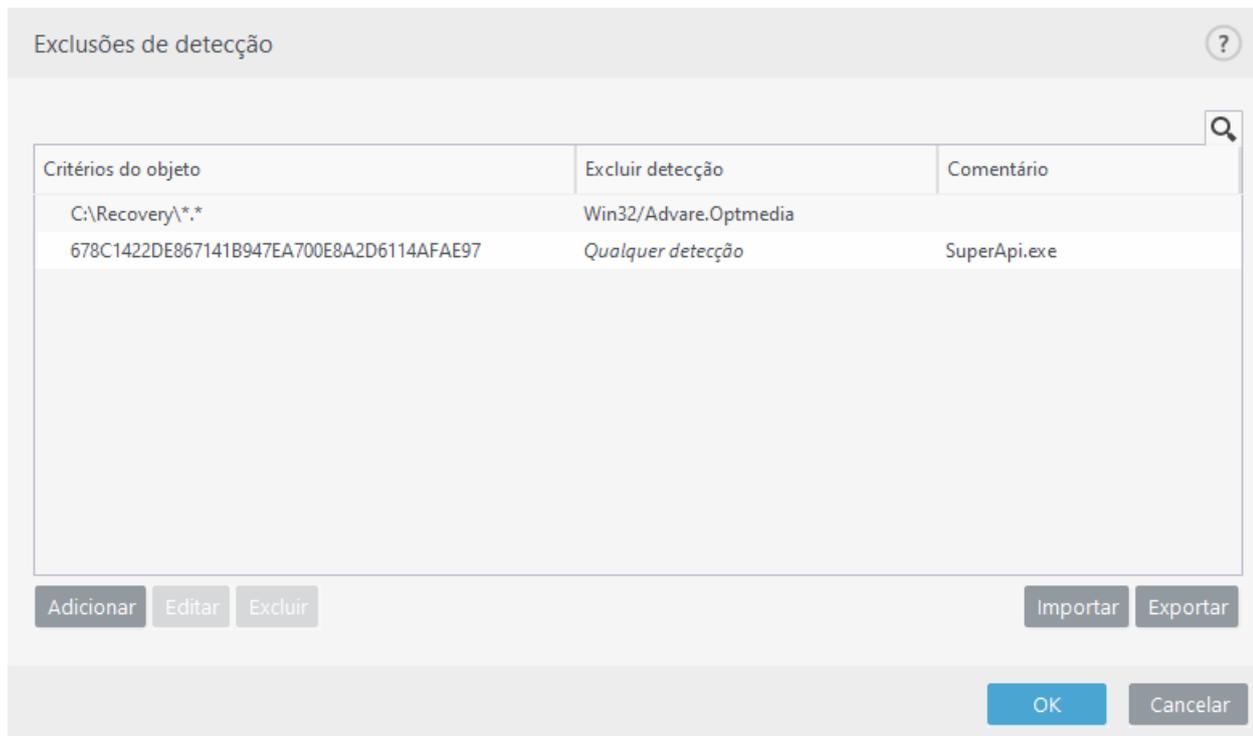
## Exclusões de detecção

As exclusões de detecção permitem a você excluir objetos da detecção ao filtrar por nome da detecção, caminho do objeto ou hash do objeto.

### Como as exclusões de detecção funcionam

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.



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, navegue para **Configuração avançada (F5) > Mecanismo de detecção > Exclusões > Exclusões de detecção > Editar**.

**i** Não confunda isso com as [Exclusões de desempenho](#), [Extensões de arquivo excluídas](#), [Exclusões HIPS](#) ou [Exclusões de processos](#).

Para [excluir um objeto \(por seu nome de detecção ou hash\)](#) do mecanismo de detecção, 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 clicando com o botão direito no arquivo de quarentena e selecionando **Restaurar e excluir do escaneamento** no menu de contexto.

## Critérios do objeto das exclusões de detecção

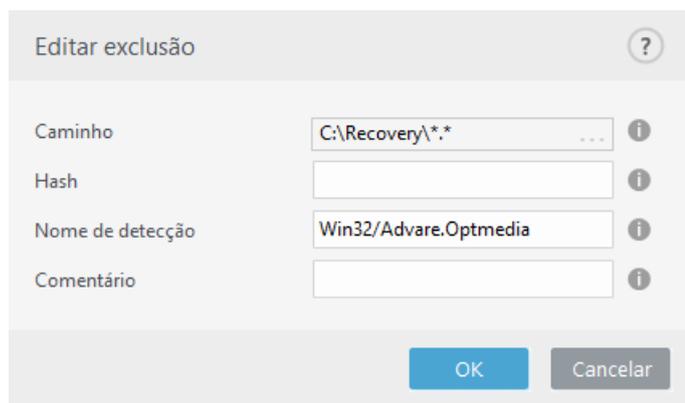
- **Caminho** – Limita uma exclusão de detecção para um caminho específico (ou para qualquer caminho).
- **Nome da detecção** – se houver um nome de uma [detecção](#) próximo a um arquivo excluído, significa que o arquivo só foi excluído para a determinada detecção, mas não completamente. Se o arquivo 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.

# 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 **Deteccões** no menu suspenso Arquivos de relatório. Isso é útil quando uma [amostra com falso positivo](#) está sendo detectada no ESET NOD32 Antivirus. 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](#).



Editar exclusão

Caminho: C:\Recovery\\*.\*

Hash:

Nome de detecção: Win32/Adware.Optmedia

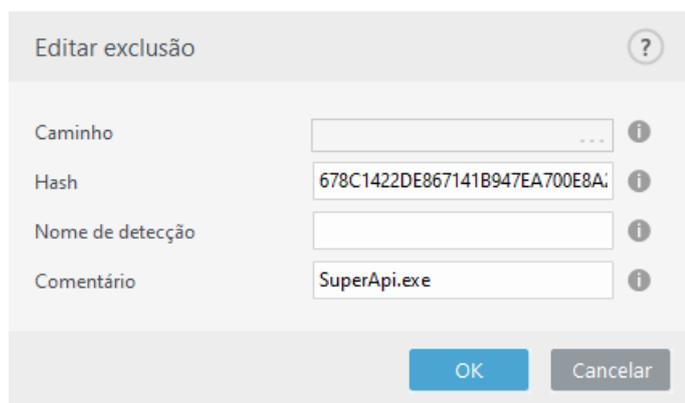
Comentário:

OK Cancelar

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.



Editar exclusão

Caminho:

Hash: 678C1422DE867141B947EA700E8A:

Nome de detecção:

Comentário: SuperApi.exe

OK Cancelar

### Exclusões por nome de detecção

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 NOD32 Antivirus:

@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):

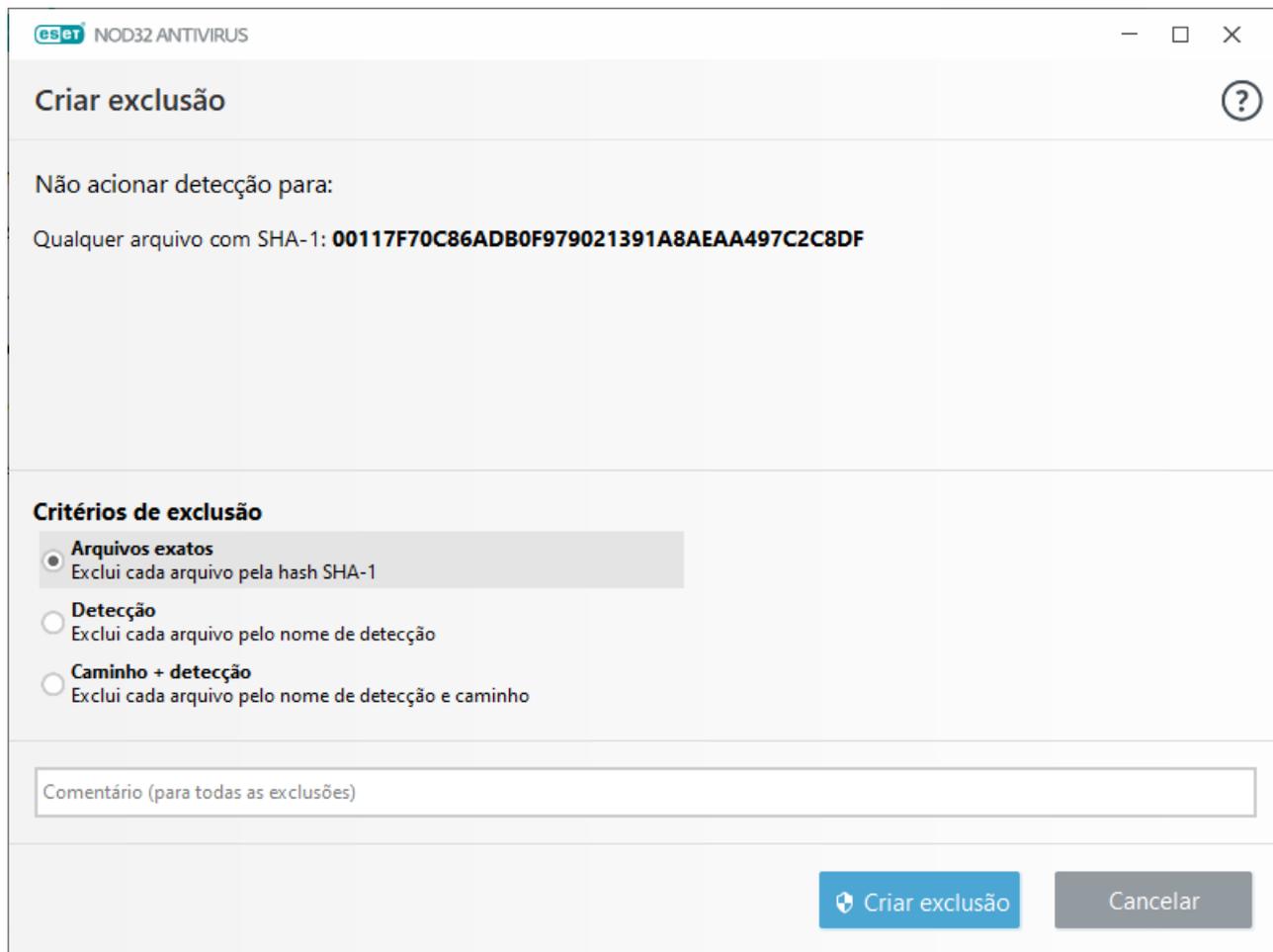
1. Na [janela do programa principal](#), clique em **Ferramentas > Arquivos de relatório**.
2. Clique com o botão direito em uma detecção no **Relatório de detecções**.
3. Clique em **Criar exclusão**.

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 HIPS

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

Para editar exclusões HIPS, navegue até **Configuração avançada (F5) > Mecanismo de detecção > HIPS > Básico > Exclusões > Editar**.

**i** Não confunda isso com as [Extensões de arquivo excluídas](#), [Exclusões de detecção](#), [Exclusões de desempenho](#) ou [Exclusões de processo](#).

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.

## 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 rastreados
- 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 email** - 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 NOD32 Antivirus enquanto limpa os objetos. Existem quatro níveis de limpeza:

Os parâmetros do ThreatSense têm os seguintes níveis de correção (ou seja, limpeza).

## Correção no ESET NOD32 Antivirus

Nível de limpeza	Descrição
<b>Sempre corrigir a detecção</b>	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.
<b>Corrigir a detecção se for seguro, se não, manter</b>	Tenta corrigir a detecção durante a limpeza dos <a href="#">objetos</a> 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.
<b>Corrigir a detecção se for seguro, se não, perguntar</b>	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.
<b>Sempre perguntar ao usuário final</b>	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.

## 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 rastreamento consome determinada quantidade de recursos do sistema. Se você estiver trabalhando com programas que exigem pesados recursos do sistema, você poderá ativar o rastreamento de baixa 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 rastreamento.

**Manter último registro de acesso** - Selecione essa opção para manter o tempo de acesso original dos arquivos rastreados, 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**.

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

## Extensões de arquivo excluídas do rastreamento

Extensões de arquivo excluídas são parte dos [parâmetros ThreatSense](#). Para configurar as extensões de arquivo excluídas, clique em **parâmetros ThreatSense** na janela Configuração avançada para qualquer [módulo que use a tecnologia ThreatSense](#).

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 isso com as [Exclusões de processos](#), [Exclusões HIPS](#) ou [Exclusões de arquivo/pasta](#).

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 extensões 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

Para editar essas configurações navegue até **Configuração avançada (F5) > Mecanismo de detecção > Proteção em tempo real do sistema de arquivos > Parâmetros adicionais do ThreatSense**.

## Parâmetros adicionais do ThreatSense para arquivos criados e modificados recentemente

A probabilidade de infecção em arquivos criados ou modificados recentemente é muito mais alta que nos arquivos existentes. Por esse motivo, o programa verifica esses arquivos com parâmetros de escaneamento adicionais. O ESET NOD32 Antivirus usa heurística avançada, que pode detectar novas ameaças antes do lançamento da atualização do mecanismo de detecção com métodos de escaneamento baseados em assinatura.

Além dos arquivos recém-criados, o escaneamento também é executado em **Arquivos de autoextração (.sfx)** e em **Compactadores em tempo real** (arquivos executáveis compactados internamente). Por padrão, os arquivos compactados são escaneados até o décimo nível de compactação e são verificados, independentemente do tamanho real deles. Para modificar as configurações de escaneamento em arquivos compactados, desmarque **Configurações padrão de escaneamento de arquivo**.

## Parâmetros adicionais do ThreatSense para arquivos executados

**Heurística avançada na execução de arquivos** - 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.

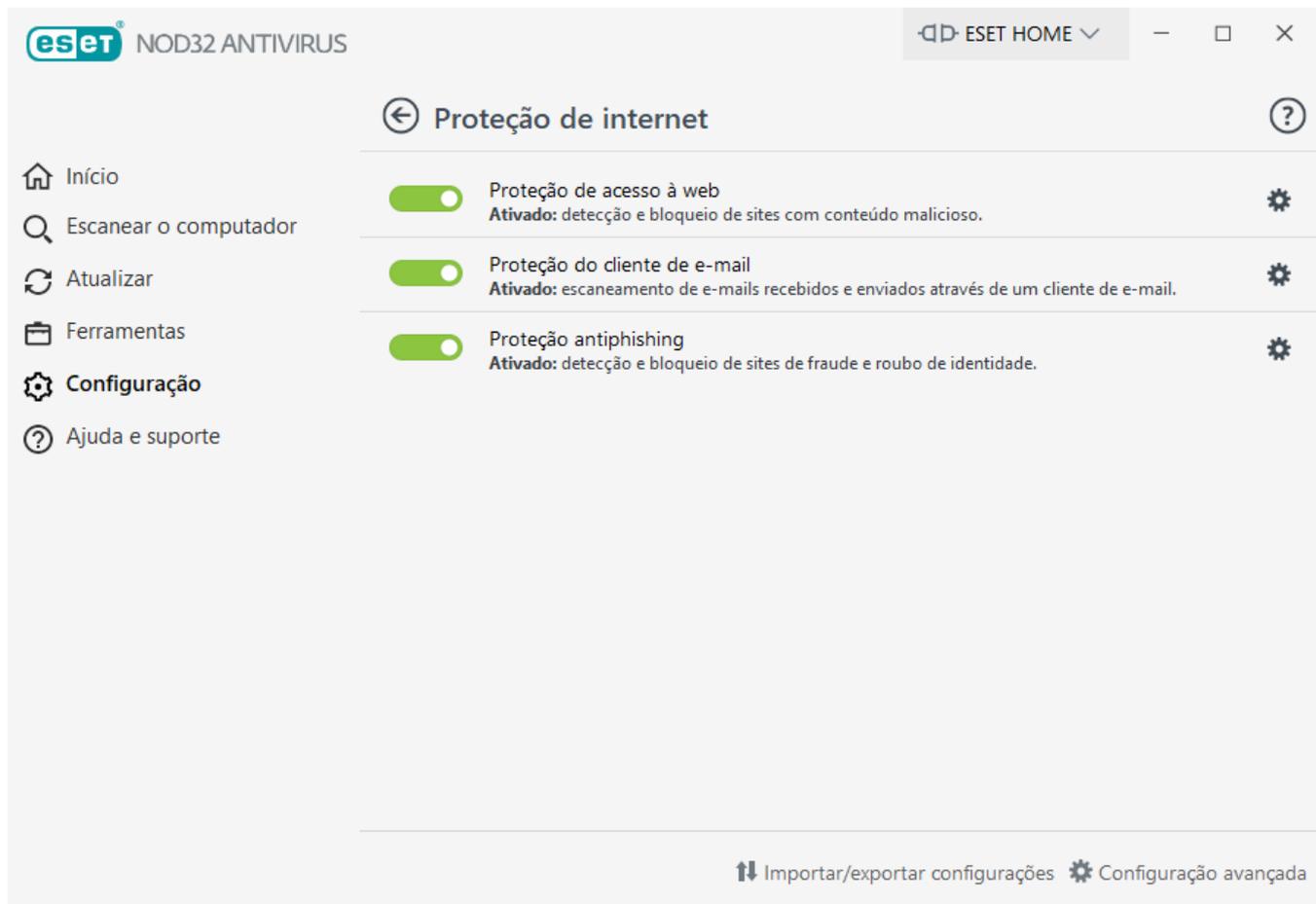
**Heurística avançada na execução de arquivos da mídia removível** - A heurística avançada emula um código em um ambiente virtual e avalia seu comportamento antes do código poder ser executado a partir de uma mídia removível.

## Proteção de internet

Para configurar a Proteção à web e e-mail, clique em **Proteção para internet** na janela **Configuração**. A partir daqui, você pode acessar configurações mais detalhadas do programa.

Para pausar ou desativar os módulos de proteção individuais, clique no ícone da barra deslizante .

 Desligar os módulos de proteção pode diminuir o nível de proteção do seu computador.



Clique no ícone de engrenagem  para abrir a web/e-mail/Antiphishing configurações de proteção em Configuração avançada.

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 NOD32 Antivirus permite controlar todas as comunicações vindas através do cliente de email.

A [Proteção Antiphishing](#) permite bloquear páginas na web que são conhecidas como distribuindo conteúdo de roubo de identidade. Recomendamos que você deixe o Antiphishing ativado.

## 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/TLS), 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 NOD32 Antivirus (Proteção do acesso à Web, Proteção de protocolos de email, Antiphishing, Controle dos pais) 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.

Adiciona (por exemplo *2001:718:1c01:16:214:22ff:fec9:ca5*).

**Sub-rede** - A sub-rede (um grupo de computadores) é definida por um endereço IP e máscara (por exemplo, *2002:c0a8:6301:1::1/64*).

### Exemplo de endereços IP excluídos

#### 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*.

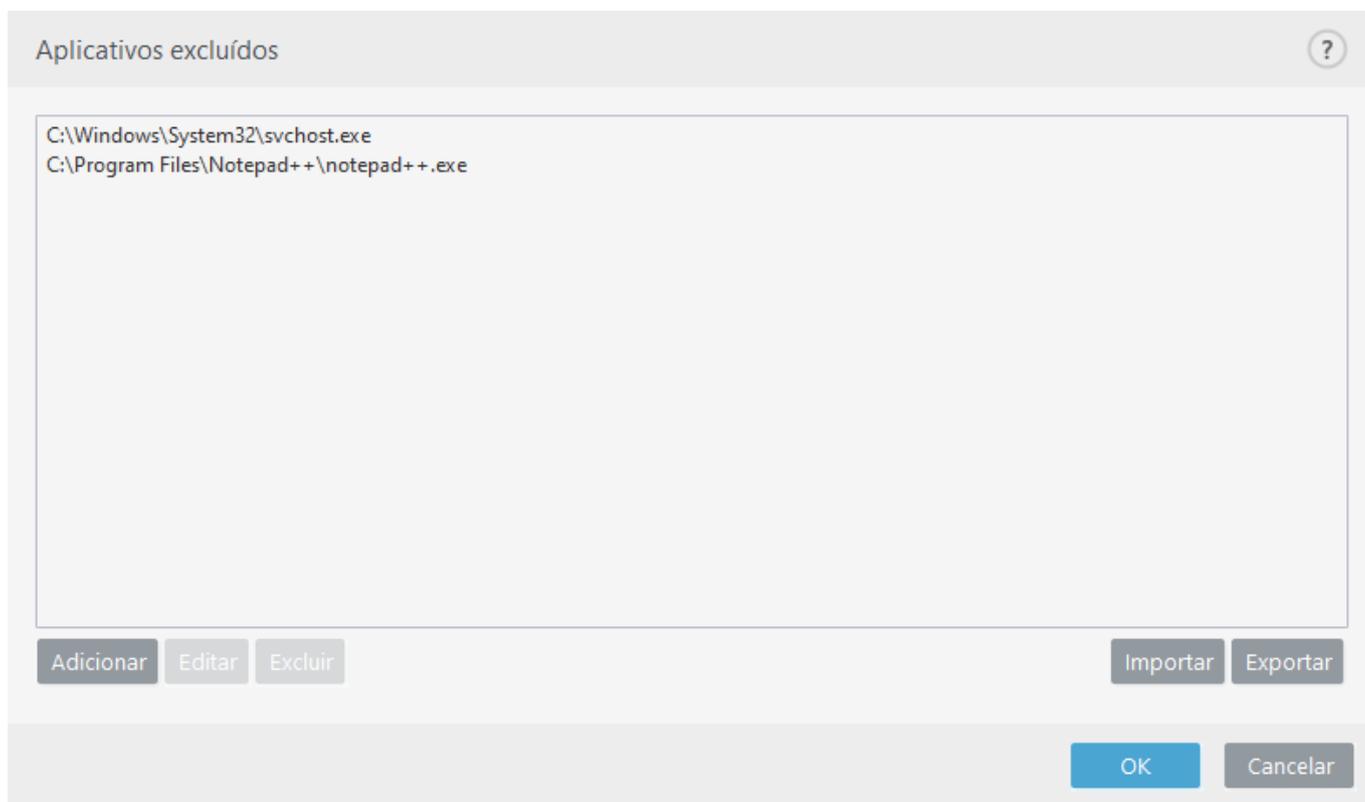
#### Endereços IPv6 e máscara:

- *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 conteúdos a comunicação de aplicativos específicos que possuem direito de acesso à rede, selecione-os na lista. A comunicação HTTP/POP3/IMAP dos aplicativos selecionados não será verificada quanto a ameaças. Recomendamos usar isto apenas para aplicativos que não funcionam corretamente se as suas comunicações estiverem sendo rastreadas.

A execução de aplicativos e serviços estará disponível automaticamente. Clique em **Adicionar** para adicionar um aplicativo manualmente se ele não for exibido na lista de filtragem de protocolo.

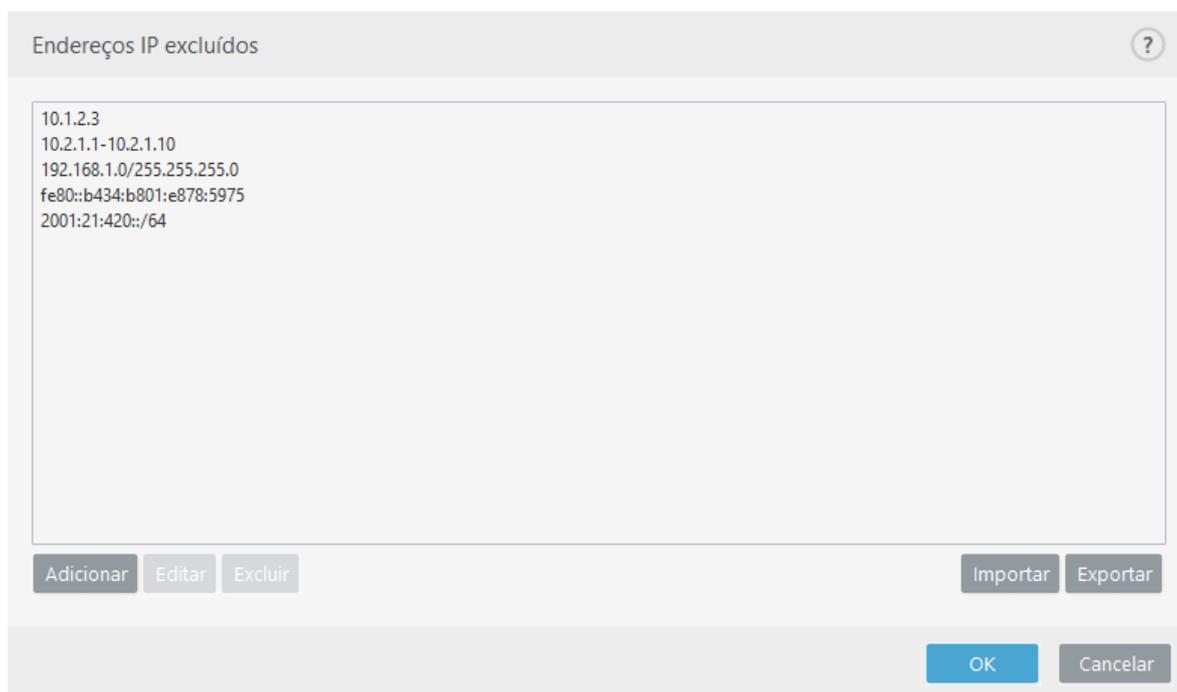


## Endereços IP excluídos

As entradas na lista serão excluídas da filtragem de conteúdos do 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.

Clique em **Adicionar** para excluir um endereço IP/intervalo de endereço/subrede de um ponto remoto para que não seja exibido na lista de filtragem de protocolo.

Clique em **Remover** para remover as entradas selecionadas da lista.



## Adicionar endereço IPv4

Isso permite que você adicione um endereço IP/intervalo de endereços/sub-rede de um ponto remoto para o qual a regra é aplicada. A versão 4 do IP (Internet Protocol) é a versão mais antiga, mas ainda é a mais amplamente utilizada.

**Endereço único** - Adiciona o endereço IP de um computador individual para o qual a regra será aplicada (por exemplo, *192.168.0.10*).

**Intervalo de endereços** - Digite o início e o fim do endereço IP para especificar o intervalo IP (de vários computadores) para o qual a regra será aplicada (por exemplo, *192.168.0.1* a *192.168.0.99*).

**Sub-rede** - 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*.

## Adicionar endereço IPv6

Permite adicionar um endereço/sub-rede IPv6 de um ponto remoto para o qual a regra deve ser aplicada. É a versão mais recente do protocolo do IP (Internet Protocol) e substituirá a versão 4 mais antiga.

**Endereço único** - Adiciona o endereço IP de um computador individual para o qual a regra é aplicada (por exemplo, *2001:718:1c01:16:214:22ff:fec9:ca5*).

**Sub-rede** - A sub-rede (um grupo de computadores) é definida por um endereço IP e máscara (por exemplo: *2002:c0a8:6301:1::1/64*).

## SSL/TLS

O ESET NOD32 Antivirus é capaz de verificar se há ameaças em comunicações que usam o protocolo SSL. É possível usar vários modos de filtragem 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** - Se a filtragem de protocolo estiver desativada, o programa não rastreará as comunicações em SSL.

**Modo de filtragem de protocolo SSL/TLS** está disponível nas seguintes opções:

Modo de filtragem	Descrição
<b>Modo automático</b>	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.
<b>Modo interativo</b>	Se você entrar em um novo site protegido por SSL (com um certificado desconhecido), uma <a href="#">caixa de diálogo de seleção de ação</a> será exibida. Esse modo permite criar uma lista de certificados SSL / aplicativos que serão excluídos do rastreamento.

Modo de filtragem	Descrição
<b>Modo de política</b>	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 NOD32 Antivirus para aplicativos específicos

**Lista de certificados conhecidos** - permite que você personalize o comportamento do ESET NOD32 Antivirus 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.

## Certificado raiz

**Adicionar o certificado raiz aos navegadores conhecidos** – Para que a comunicação do SSL funcione adequadamente nos seus navegadores/clientes de e-mail, é fundamental que o certificado raiz da ESET seja adicionado à lista de certificados raiz conhecidos (editores). Quando ativado, o ESET NOD32 Antivirus vai adicionar automaticamente o certificado ESET SSL Filter CA aos navegadores conhecidos (por exemplo, Opera). Para navegadores que utilizam o armazenamento de certificação do sistema, o certificado será adicionado automaticamente. Por exemplo, o Firefox é configurado automaticamente para confiar em Autoridades raiz no armazenamento de certificação do sistema.

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

**Caso a confiança do certificado não seja estabelecida** – em alguns casos, o certificado do site não pode ser verificado utilizando o depósito de Autoridades de certificação raiz confiáveis (TRCA). Portanto, alguém (por exemplo, o administrador de um servidor da web ou uma empresa de pequeno porte) assinou o certificado 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. Você pode selecionar **Bloquear a comunicação que utiliza o certificado** para sempre encerrar conexões criptografadas para sites com certificados não verificados.

**Se o certificado estiver corrompido** – isso significa que o certificado foi assinado incorretamente ou está danificado. Nesse caso, a ESET recomenda 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.

## Exemplos ilustrados



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

- [Notificações de certificado em produtos domésticos ESET Windows](#)
- ["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 NOD32 Antivirus 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 NOD32 Antivirus deve **Ignorar** esse tráfego para manter o aplicativo funcionando.

## Exemplos ilustrados

- i** Os artigos da Base de conhecimento da ESET a seguir podem estar disponíveis apenas em inglês:
- [Notificações de certificado em produtos domésticos ESET Windows](#)
  - ["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 NOD32 Antivirus 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** – Adiciona um novo certificado e ajusta suas configurações relacionadas a opções de acesso e de rastreamento.

**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.

# Lista de aplicativos SSL/TLS filtrados

A **Lista de aplicativos SSL/TLS filtrados** pode ser usada para personalizar o comportamento do ESET NOD32 Antivirus para aplicativos específicos, bem como para lembrar ações escolhidas quando o **Modo de filtragem de protocolo SSL/TLS** estiver no **Modo interativo**. 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** para rastrear ou ignorar a comunicação. 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 aplicativo que deseja configurar e clique em **Editar**.

**Remover** – selecione o aplicativo que deseja remover e clique em **Remover**.

**Importar/Exportar** – importa aplicativos de um arquivo ou salvar sua lista atual de aplicativos em um arquivo.

**OK/Cancelar** - Clique em **OK** se quiser salvar alterações ou clique em **Cancelar** se quiser sair sem salvar.

# Proteção do cliente de email

Veja a [Integração do ESET NOD32 Antivirus com seu cliente de e-mail](#) para configurar a integração.

Configurações de cliente de email estão localizadas em **Configuração avançada (F5) > Web e email > Proteção do cliente de email > Clientes de email**.

## Clientes de email

**Ativar proteção por e-mail por plugins do cliente** – Quando desativado, a proteção por e-mail por plugins do cliente está desativada.

### Email para ser rastreado

Selecione e-mails para escanear:

- Email recebido
- Email enviado

- Ler email
- E-mail modificado

**i** 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.

## Integração com clientes de email

A integração do ESET NOD32 Antivirus 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 NOD32 Antivirus. Quando integrado no seu cliente de email, a barra de ferramentas ESET NOD32 Antivirus 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 > 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 e-mail funciona como um plugin 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](#).

Desative a **Otimização de tratamento de anexo** e o **Processamento avançado do cliente de e-mail** se a velocidade do sistema diminuir ao recuperar e-mails.

## Barra de ferramentas do Microsoft Outlook

A proteção do Microsoft Outlook funciona como um módulo de plug-in. Após a instalação do ESET NOD32 Antivirus, essa barra de ferramentas contendo as opções de proteção de antivírus/ é adicionada ao Microsoft Outlook:

**ESET NOD32 Antivirus** – Clique duas vezes no ícone para abrir a janela principal do ESET NOD32 Antivirus.

**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](#).

## 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 NOD32 Antivirus, essa barra de ferramentas contendo as opções de proteção de antivírus/ é adicionada ao Outlook Express ou ao Windows Mail:

**ESET NOD32 Antivirus** – Clique duas vezes no ícone para abrir a janela principal do ESET NOD32 Antivirus.

**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](#).

### 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

Essa notificação serve para verificar se o usuário realmente deseja executar a ação selecionada, que deve eliminar possíveis enganos.

Por outro lado, a caixa de diálogo também oferece a opção de desativar as confirmações.

## Rastrear novamente mensagens

A barra de ferramentas do ESET NOD32 Antivirus 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.

## Protocolos de email

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 NOD32 Antivirus 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 IMAP 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 NOD32 Antivirus 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 NOD32 Antivirus 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 ver a configuração do escaneador, abra a Configuração avançada > **Web e e-mail > [SSL/TLS](#)**.



## Filtro POP3, POP3S

O protocolo POP3 é o protocolo mais amplamente utilizado para receber comunicação em um aplicativo cliente de email. O ESET NOD32 Antivirus fornece proteção a esse protocolo, independentemente do cliente de email usado.

O módulo de proteção que fornece esse controle é iniciado automaticamente na inicialização do sistema e depois fica ativo na memória. Para que o módulo funcione corretamente, verifique se ele está ativado - a verificação do protocolo POP3 é feita automaticamente, sem necessidade de reconfiguração do cliente de email. Por padrão, todas as comunicações através da porta 110 são rastreadas, mas podem ser adicionadas outras portas de comunicação, se necessário. Os vários números das portas devem ser delimitados por vírgula.

A comunicação criptografada será escaneada por padrão. Para ver a configuração do escaneador, abra a Configuração avançada > **Web e e-mail** > [SSL/TLS](#).

Nesta seção, é possível configurar a verificação dos protocolos POP3 e POP3S.

**Ativar verificação do protocolo POP3** - Se estiver ativada, todo o tráfego por meio do POP3 será monitorado quanto a software malicioso.

**Portas usadas pelo protocolo POP3** - Uma lista de portas utilizadas pelo protocolo POP3 (110 por padrão).

O ESET NOD32 Antivirus oferece também suporte à verificação do protocolo POP3S. Esse tipo de comunicação utiliza um canal criptografado para transferir as informações entre servidor e cliente. O ESET NOD32 Antivirus verifica as comunicações utilizando os métodos de criptografia SSL (Camada de soquete seguro) e TLS (Segurança da camada de transporte).

**Não utilizar a verificação de POP3S** - A comunicação criptografada não será verificada.

**Utilizar a verificação de protocolo POP3S para as portas selecionadas** - Selecione essa opção para permitir a verificação de POP3S apenas para as portas definidas em **Portas utilizadas pelo protocolo POP3S**.

**Portas utilizadas pelo protocolo POP3S** - Uma lista de portas POP3S a serem verificadas (por padrão, 995).

## 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.

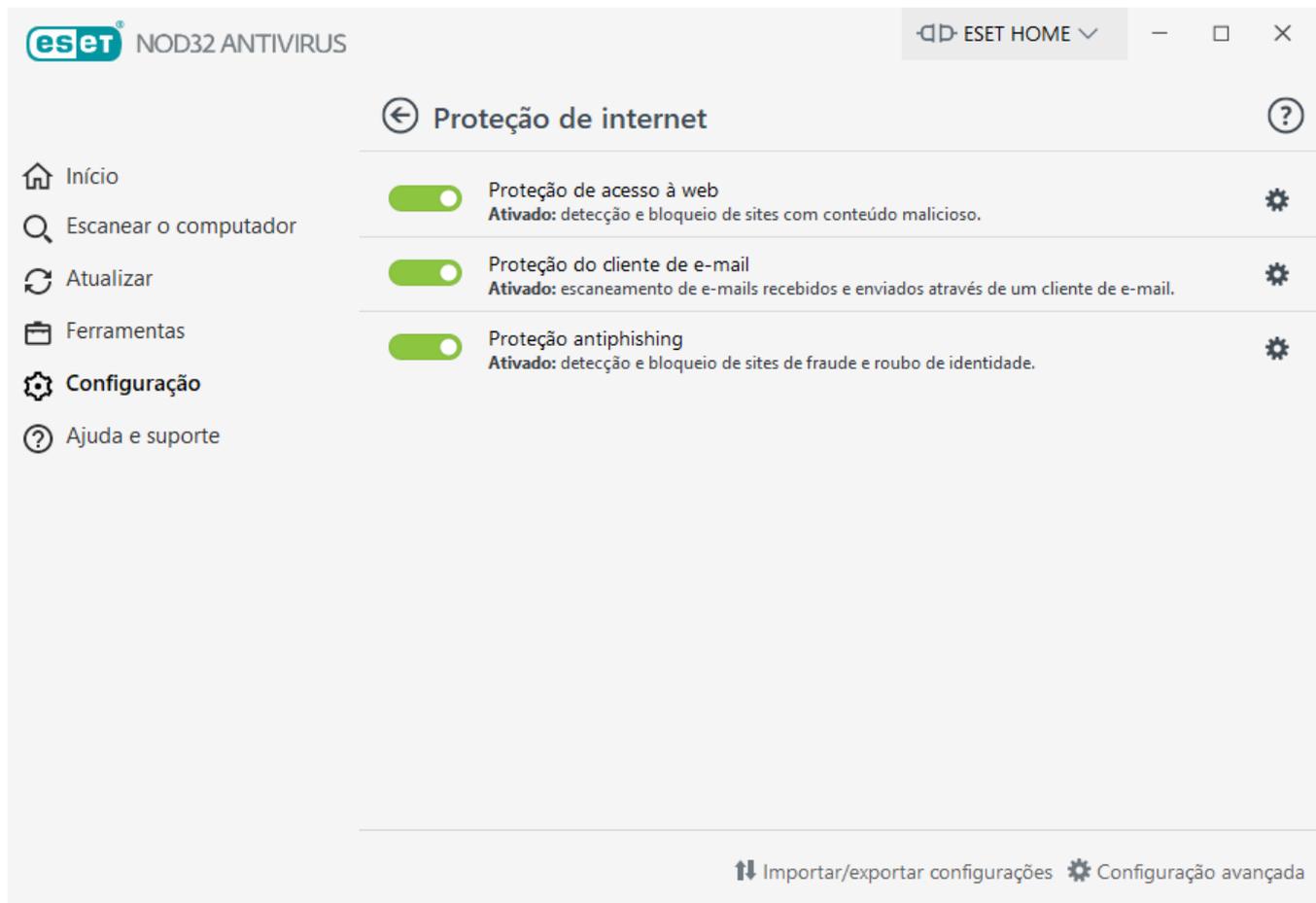
**Texto a adicionar ao assunto de e-mail infectado** – Edite esse modelo se quiser modificar o formato de prefixo do assunto de um e-mail infectado. Essa função substituirá o assunto da mensagem "Olá" com o seguinte formato: "[detecção %DETECTIONNAME%] Olá". A variável %DETECTIONNAME% representa a detecção.

## Proteção do acesso à Web

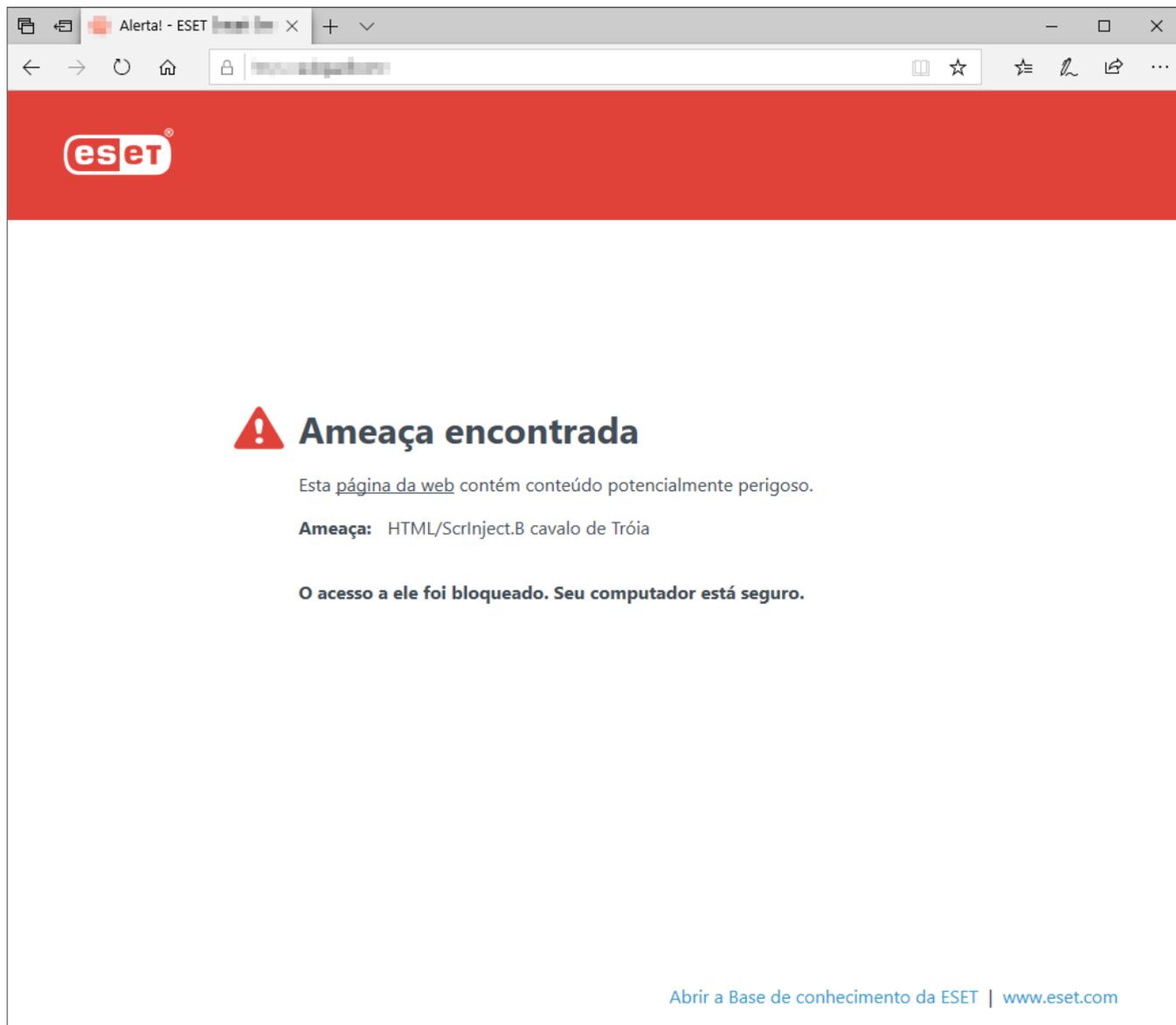
A conectividade com a Internet é um recurso padrão em um computador pessoal. Infelizmente, ela tornou-se o meio principal de transferência de códigos maliciosos. A proteção de acesso à Web funciona ao monitorar a comunicação entre os navegadores da web e servidores remotos e cumpre as regras do protocolo 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 da [janela principal do programa](#) > **Configuração** > **Proteção para 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:



### Instruções ilustradas

- i** Os artigos da Base de conhecimento da ESET a seguir podem estar disponíveis apenas em inglês:
- [Excluir um site seguro de ser bloqueado pela Proteção de acesso à web](#)
  - [Bloquear um site usando o ESET NOD32 Antivirus](#)

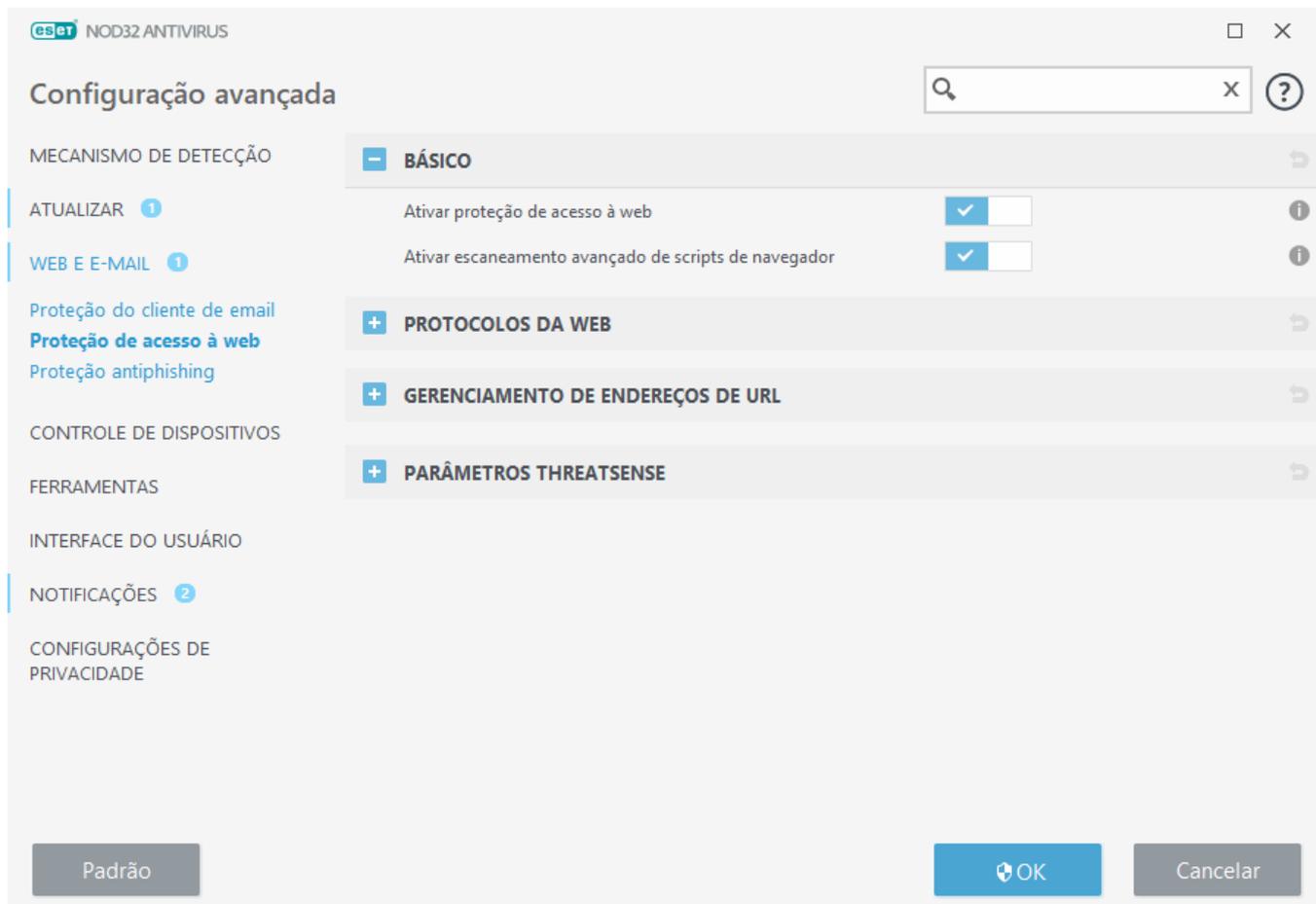
As seguintes opções estão disponíveis em **Configuração avançada (F5) > Web e email > Proteção de acesso Web:**

[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. Essa opção está disponível apenas quando a filtragem de protocolo SSL/TLS está ativada.

**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 NOD32 Antivirus 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 NOD32 Antivirus 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 NOD32 Antivirus 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 ver a configuração do escaneador, abra a Configuração avançada > **Web e e-mail** > [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.

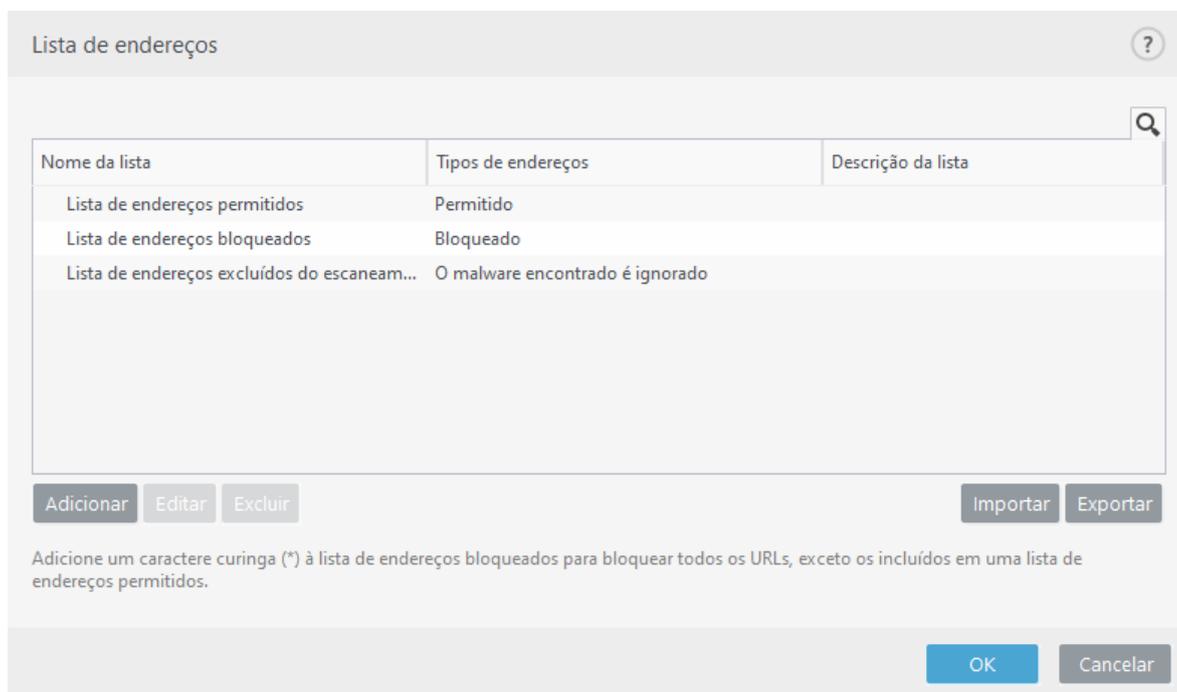
Sites na **Lista de endereços bloqueados** não estarão acessíveis, exceto se também forem incluídos na **Lista de endereços permitidos**. Sites na **Lista de endereços excluídos do escaneamento de conteúdo** não serão escaneados quanto a código malicioso quando acessados.

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**.

### Domínios confiáveis

**i** 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.



## 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 escaneam...	O malware encontrado é ignorado	

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

### Instruções ilustradas

- i** Os artigos da Base de conhecimento da ESET a seguir podem estar disponíveis apenas em inglês:
- [Excluir um site seguro de ser bloqueado pela Proteção de acesso à web](#)
  - [Bloquear um site usando os produtos domésticos ESET Windows](#)

Para obter mais informações, consulte [Gerenciamento de endereços de URL](#).

## Criar nova lista de endereços de URL

Essa seção permite especificar listas de endereços URL/máscaras que serão bloqueados, permitidos ou excluídos da verificação.

Ao criar uma nova lista, as seguintes opções estão disponíveis para configuração:

**Tipo de lista de endereços** - Três tipos de listas estão disponíveis:

- **Excluídos da verificação** - Nenhuma verificação quanto a código malicioso será realizada para qualquer endereço adicionado a essa lista.
- **Bloqueado** - O usuário não terá permissão para acessar endereços especificados nessa lista.
- **Permitido** - Se a opção 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 também estiverem presentes na lista de endereços bloqueados.

**Nome da lista** - Especifique o nome da lista. Esse campo estará esmaecido ao editar uma das três listas predefinidas.

**Descrição da lista** - digite uma breve descrição para a lista (opcional). Esse campo estará esmaecido ao editar uma das três listas predefinidas.

Para ativar uma lista, selecione **Lista ativa** ao lado dessa lista. Se você quiser ser notificado quando uma lista específica for usada em avaliação de um site HTTP que você acessou, selecione **Notificar ao aplicar**. Por exemplo, uma notificação será emitida se um site for bloqueado ou permitido, pois está incluída na lista de endereços bloqueados ou permitidos. A notificação terá o nome da lista contendo o site especificado.

## Elementos de controle

**Adicionar** - Adiciona um novo endereço URL à lista (insira vários valores com separador).

**Editar** - Modifica endereço existente na lista. Somente possível para endereços criados com **Adicionar**.

**Remover** - Exclui endereços existentes na lista. Somente possível 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).

## 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 NOD32 Antivirus 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.)

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*.

## Proteção antiphishing

O termo roubo de identidade define uma atividade criminal que usa engenharia social (a manipulação de usuários para obter informações confidenciais). O roubo de identidade é usado para obter acesso a dados sensíveis como números de contas bancárias, códigos de PIN e outros. Leia mais sobre essa atividade no [glossário](#). O ESET NOD32 Antivirus oferece proteção antiphishing; páginas da web conhecidas por distribuir esse tipo de conteúdo podem ser bloqueadas.

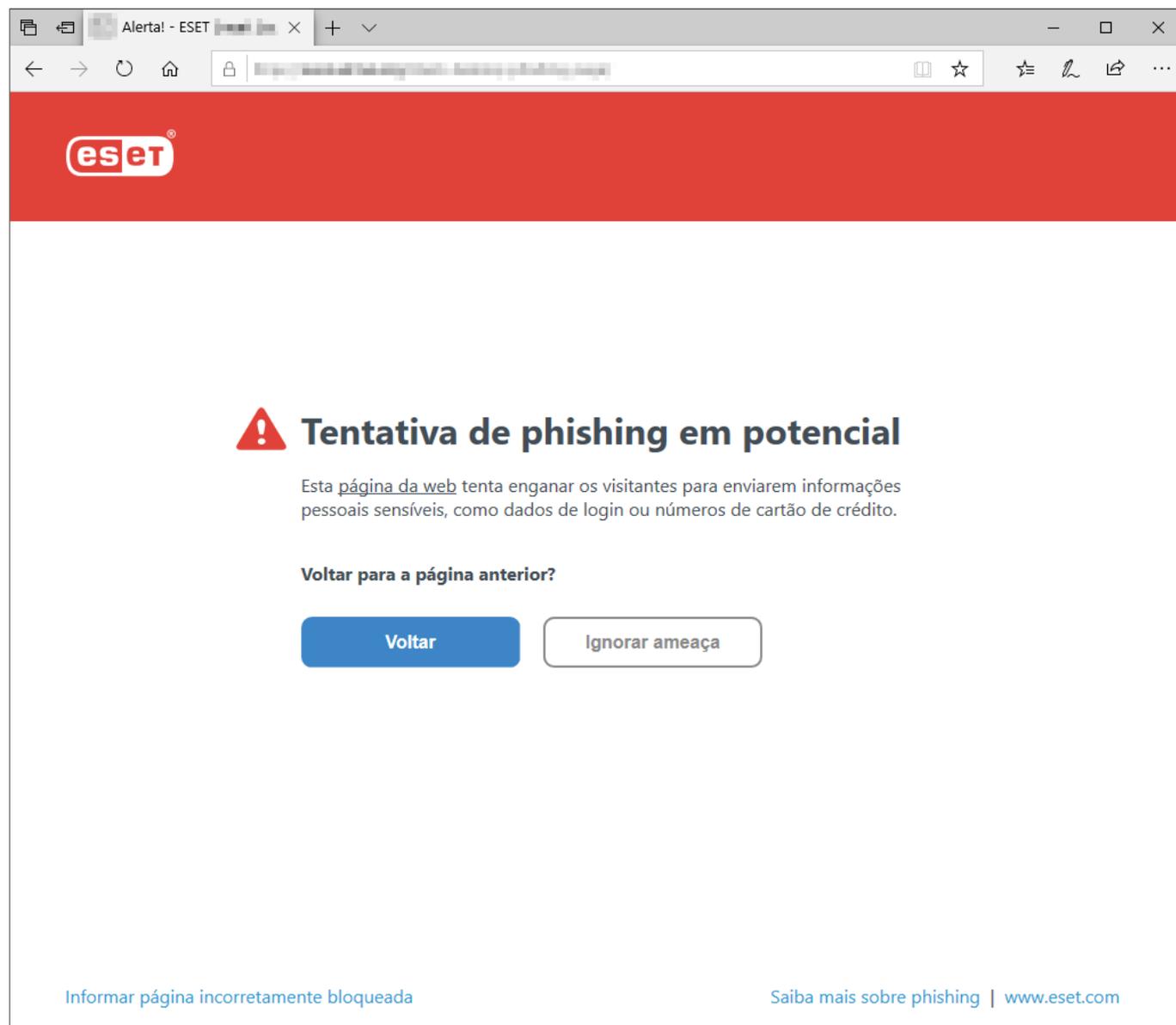
Recomendamos que você ative a proteção antiphishing no ESET NOD32 Antivirus. Para isso, abra a **Configuração**

avançada (F5) e vá para **Web e email > Proteção antiphishing**.

Visite nosso [artigo da Base de conhecimento](#) para mais informações sobre a Proteção antiphishing no ESET NOD32 Antivirus.

## Acessando um site de roubo de identidade

Ao acessar um site de phishing reconhecido, você verá a caixa de diálogo a seguir no seu navegador da web. 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](#). Em **Configuração avançada (F5) > Web e e-mail > Proteção de acesso à Web > Gerenciamento de endereços URL > Lista de endereços > Editar**, 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, você pode [Informar página incorretamente bloqueada](#).

Como alternativa, você pode enviar o site por email. Envie seu email para [samples@eset.com](mailto: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.).

## Atualização do programa

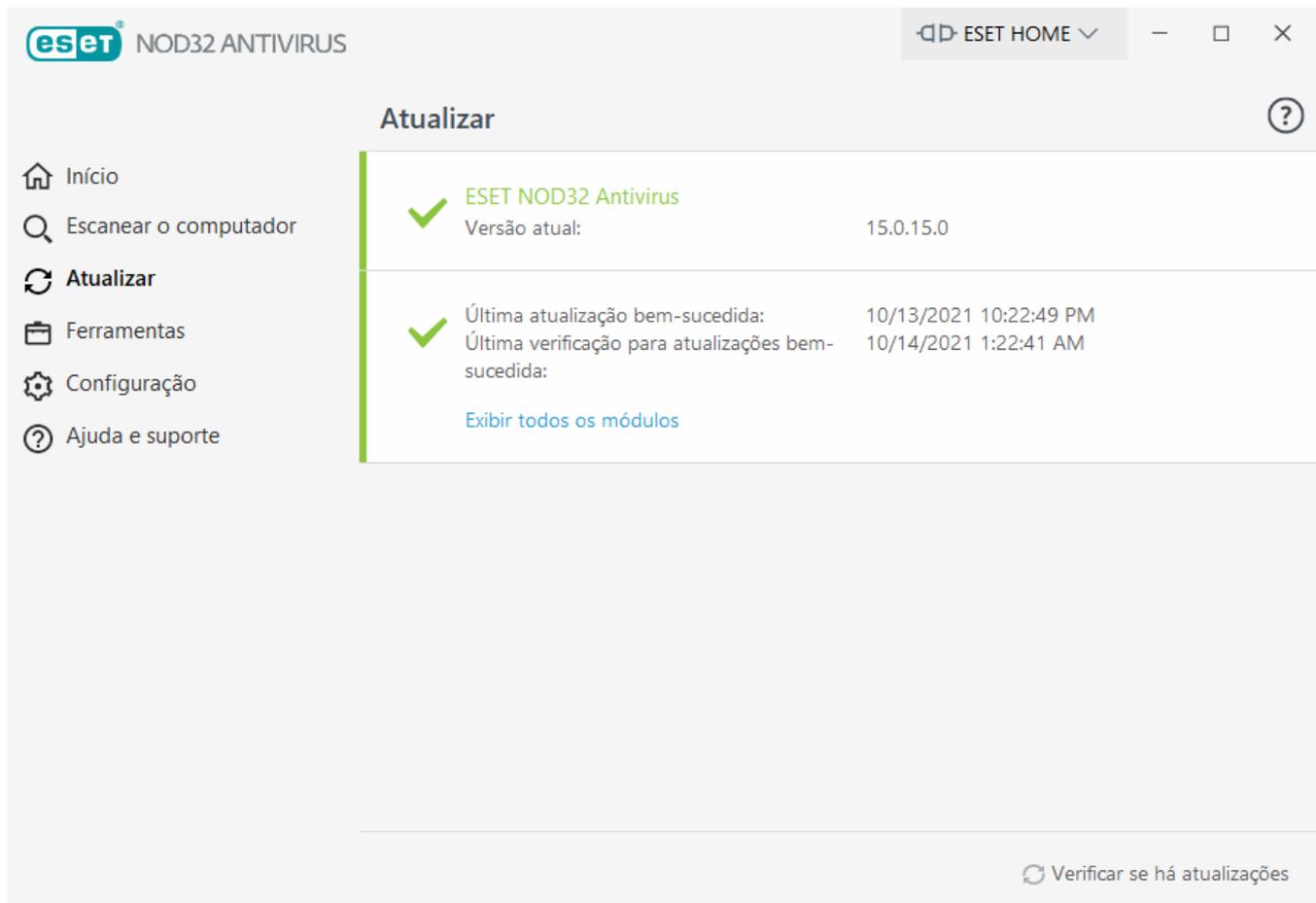
Atualizar o ESET NOD32 Antivirus periodicamente é o melhor método para se garantir o nível máximo de segurança em seu computador. O módulo de Atualização garante que tanto os módulos do programa quanto os componentes do sistema estejam sempre atualizados.

Na [janela principal do programa](#), ao clicar em **Atualizar**, você poderá visualizar o status da atualização atual, incluindo o dia e a hora da última atualização bem-sucedida, e se uma atualização será necessária.

Além de atualizações automáticas, você pode clicar em **Verificar se há atualizações** para acionar uma atualização manual. A atualização regular dos módulos e componentes do programa é uma parte importante para manter a proteção completa contra códigos maliciosos. Dê atenção especial à configuração e operação dos módulos do produto. É preciso ativar seu produto usando a Chave de licença para receber atualizações. Se você não fez isso durante a instalação, você precisará inserir sua chave de licença para ativar o produto para acessar os servidores de atualização da ESET durante a atualização.



Sua chave de licença foi enviada em um email da ESET após a compra do ESET NOD32 Antivirus.



**Versão atual** – Mostra o número de versão da versão de produto atual que você tem instalado.

**Última atualização bem-sucedida** - Mostra a data da última atualização bem-sucedida. Se você não vir uma data recente, seus módulos de produto podem não estar atuais.

**Última verificação por atualizações bem-sucedida** - A data da última verificação bem-sucedida de atualizações.

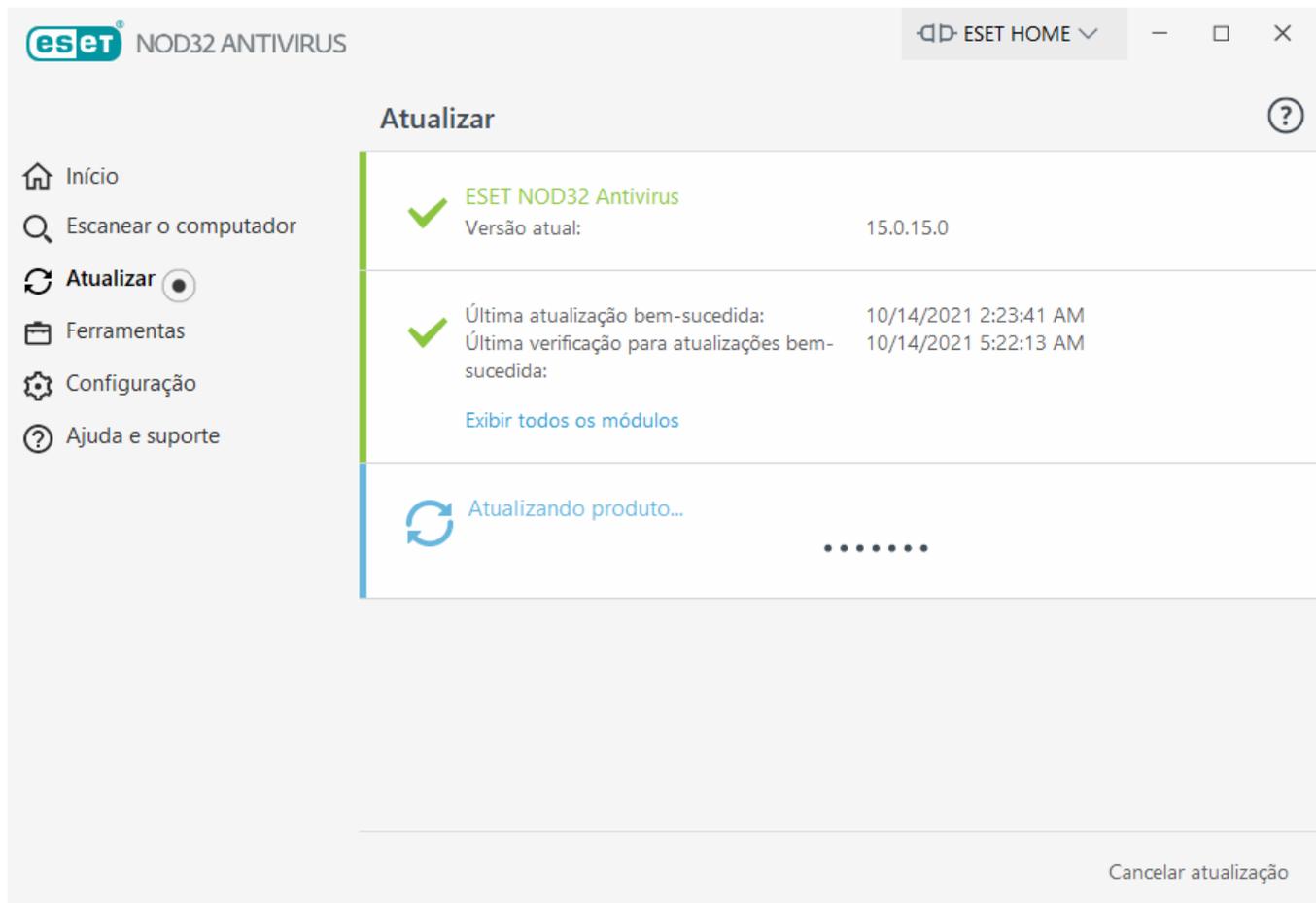
**Mostrar todos os módulos** - Mostra a lista de módulos de programas instalados.

Clique em **Verificar atualizações** para detectar a versão disponível do ESET NOD32 Antivirus mais recente.

---

## 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**.



Em circunstâncias normais, é possível ver a marca de verificação verde na janela **Atualização** indicando que o programa está atualizado. Se não for possível ver a marca de verificação verde, o programa estará desatualizado e mais vulnerável a uma infecção. Atualize os módulos do programa tão logo quanto possível.

## Falha na atualização

Se você receber uma mensagem de falha na atualização dos módulos, ela pode ter sido causada pelos problemas a seguir:

1. **Licença inválida** – a licença usada para a ativação é inválida ou expirou. Na [janela do programa principal](#), clique em **Ajuda e suporte** > **Alterar licença** e insira uma nova chave de licença.
2. **Ocorreu um erro ao fazer download de arquivos de atualização** - Isso pode ser causado pelas [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.

Recomendamos reiniciar seu computador depois de uma atualização bem-sucedida do ESET NOD32 Antivirus para uma nova versão do produto para garantir que todos os módulos do programa foram atualizados corretamente. Não é necessário reiniciar seu computador depois de atualizações de módulos regulares.

Para obter mais informações, visite [a mensagem Solução de problemas para "Falha na atualização do módulo"](#).

## Configuração da atualização

As opções de configuração da atualização estão disponíveis na árvore **Configuração avançada** (tecla F5) em **Atualizar > Básico**. 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.

### - Básico

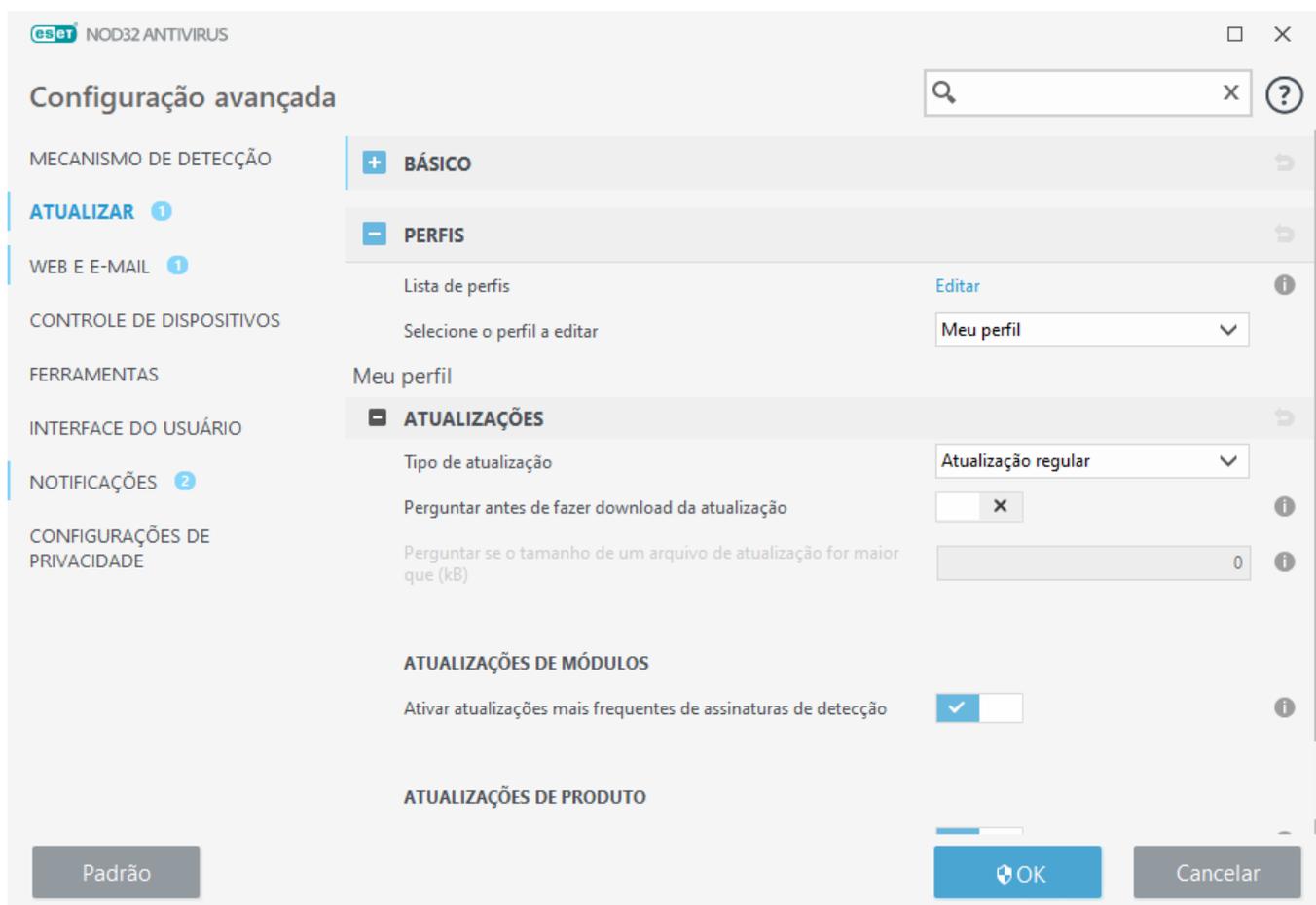
O Perfil de atualização usado atualmente (a menos que seja usado um específico, configurado em **Configuração avançada > Firewall > Redes conhecidas**) é exibido no menu suspenso **Perfil de atualização**.

Para criar um novo perfil, consulte a seção [Perfis de atualização](#).

Se você está tendo dificuldade ao tentar fazer download das atualizações do mecanismo de detecção ou de módulo, clique em **Limpar** para limpar os arquivos/cache de atualização temporários.

## Reversão do 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.



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 HTTP).

### 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.

**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.

**Perguntar se o tamanho de um arquivo de atualização for maior que (kB)** – O programa exibirá um diálogo de confirmação se o tamanho do arquivo de atualização for maior que o valor especificado. Se o tamanho do arquivo de atualização estiver definido como 0 kB, o programa sempre exibirá uma caixa de diálogo de confirmação.

**Desativar notificação sobre atualização concluída com êxito** - desativa a notificação na bandeja do sistema, na parte inferior direita da tela. A seleção dessa opção será útil se um aplicativo ou jogo de tela inteira estiver em execução. Observe que o Modo jogador vai desligar todas as notificações.

## Atualizações do módulo

**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.

## Atualizações de produto

**Atualizações de recursos do aplicativo** – instala automaticamente novas versões do ESET NOD32 Antivirus.

### Opção de conexão

Para usar um servidor proxy para fazer download das atualizações, consulte a seção [Opções de conexão](#).

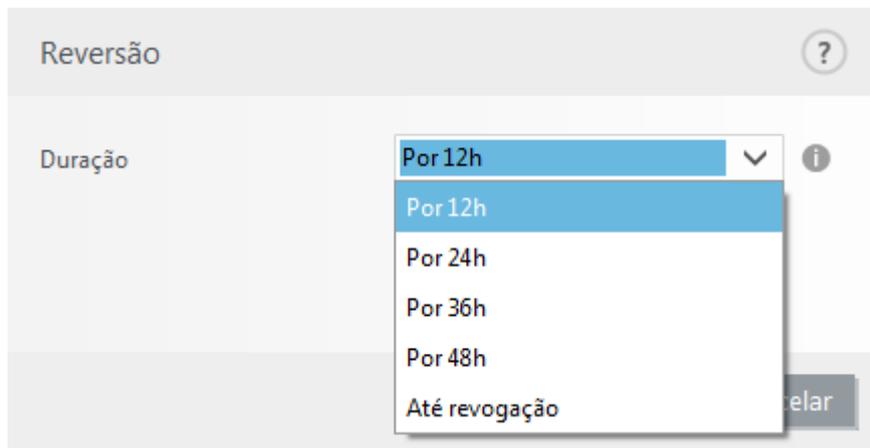
## Atualização de rollback

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 adiado indefinidamente.

O ESET NOD32 Antivirus 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.

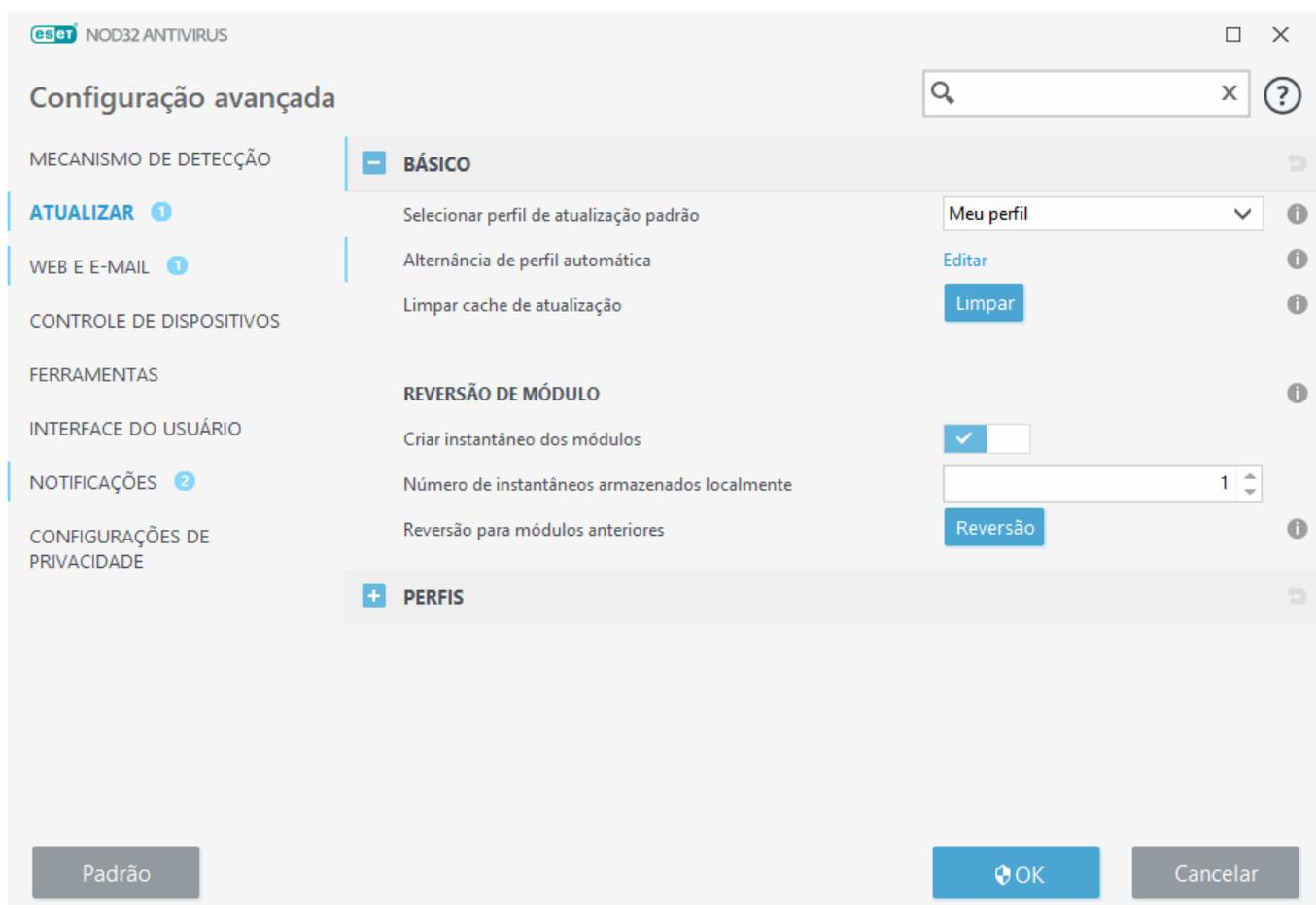
 Quando a quantidade máxima de instantâneos é alcançada (por exemplo, três), o instantâneo mais antigo é substituído por um novo instantâneo a cada 48 horas. O ESET NOD32 Antivirus reverte as versões do mecanismo de detecção e atualização de módulos de programa para o instantâneo mais antigo.

Se você clicar em **Reversão (Configuração avançada (F5) > Atualização > Geral)**, você tem que selecionar um intervalo de tempo do menu suspenso **Duração** que representa o período de tempo que o mecanismo de detecção e atualizações dos módulos de programas serão pausados.



Selecione **Até cancelado** para adiar atualizações regulares indefinidamente até restaurar a funcionalidade de atualização manualmente. A ESET não recomenda a seleção desta opção, pois isso representa um risco de segurança em potencial.

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](#).

## Intervalo de tempo de reversão

Se você clicar em **Reversão (Configuração avançada (F5) > Atualização > Geral)**, você tem que selecionar um intervalo de tempo do menu suspenso **Duração** que representa o período de tempo que o mecanismo de detecção e atualizações dos módulos de programas serão pausados.



Selecione **Até cancelado** para adiar atualizações regulares indefinidamente até restaurar a funcionalidade de atualização manualmente. A ESET não recomenda a seleção desta opção, pois isso representa um risco de segurança em potencial.

## Atualizações de produto

A seção **Atualizações de produto** permite que você instale automaticamente novas atualizações de recursos quando disponíveis.

Atualizações de recursos do aplicativo trazem novos recursos ou alteram os recursos que já existem de versões anteriores. Ela pode ser realizada automaticamente sem intervenção do usuário ou você pode escolher ser notificado. Depois de uma atualização de recurso de aplicativo ser instalada, pode ser necessário reiniciar o computador.

**Atualizações de recursos do aplicativo** – quando ativado, as atualizações de recursos do aplicativo serão realizadas automaticamente.

## 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**. 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 NOD32 Antivirus.

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 NOD32 Antivirus. 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 NOD32 Antivirus 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 Internet Explorer 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.

**i** Os campos **Nome de usuário** e **Senha** nesta seção são específicos para o servidor proxy. Preencha esses campos somente se um nome de usuário e uma senha forem necessários para acessar o servidor proxy. Esses campos devem ser fornecidos somente se você souber que precisa de senha para acessar a Internet por meio de um servidor proxy.

## 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 NOD32 Antivirus:

- **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 a seção [Agenda](#).

## Janela de diálogo – Reinicialização necessária

É necessário reiniciar o computador depois de atualizar o ESET NOD32 Antivirus para uma nova versão. Versões novas do ESET NOD32 Antivirus são emitidas para implementar melhorias ou corrigir problemas que as atualizações automáticas dos módulos de programa não conseguem resolver.

A nova versão do ESET NOD32 Antivirus pode ser instalada automaticamente, com base nas suas [configurações de atualização do programa](#), ou manualmente ao [fazer o download e instalar uma versão mais recente](#) sobre a versão anterior.

Clique em **Reiniciar agora** para reiniciar seu computador. Se você planeja reiniciar seu computador mais tarde, clique em **Lembrar mais tarde**. Mais tarde você pode reiniciar seu computador manualmente da seção **Início** na [janela do programa principal](#).

## Ferramentas

O menu **Ferramentas** inclui módulos que ajudam a simplificar a administração do programa e oferecem opções adicionais para usuários avançados.

Consulte as [Ferramentas no ESET NOD32 Antivirus](#) para obter mais informações.

## Ferramentas no ESET NOD32 Antivirus

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](#)



[Relatório de segurança](#)



[Processos em execução](#) (se o ESET LiveGrid® estiver ativado no ESET NOD32 Antivirus)



[ESET SysInspector](#)



[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.



[Agenda](#)



[Limpeza do sistema](#) – Ajuda você a restaurar o computador para um estado de uso depois de limpar a

ameaça.



[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](#)

**eSet** NOD32 ANTIVIRUS

ESET HOME

### Ferramentas

- Início**
- Escanear o computador**
- Atualizar**
- Ferramentas**
- Configuração**
- Ajuda e suporte**

**Relatórios**  
Informações sobre todos os eventos importantes do programa

**Processos em execução**  
Informação de reputação fornecida por ESET LiveGrid®

**Relatório de segurança**  
Veja como a ESET protege você

**ESET SysInspector**  
Ferramenta para coletar informações detalhadas sobre o sistema

**Agenda**  
Gerenciar e agendar tarefas

**ESET SysRescue Live**  
Ferramenta de limpeza de malware

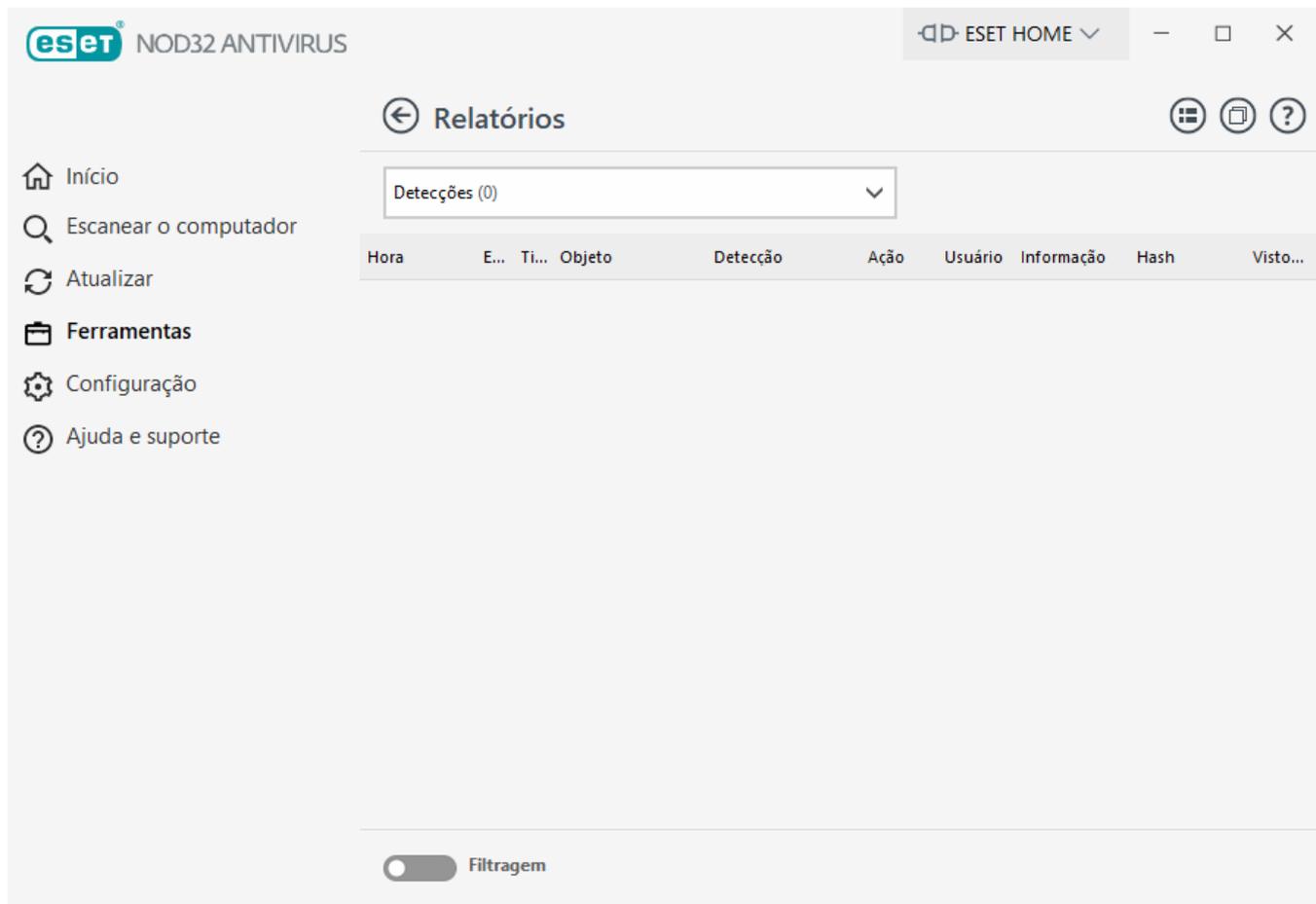
**Limpeza do sistema**  
Ferramenta de limpeza do sistema

**Enviar amostra para análise**  
Enviar arquivo para o Laboratório de Pesquisa ESET

**Quarentena**  
Arquivos infectados armazenados com segurança

## Relatórios

Os relatórios contêm informações sobre os eventos importantes do programa que ocorreram e fornecem uma visão geral das ameaças detectadas. O registro em log é uma parte essencial na análise do sistema, na detecção de ameaças e na solução de problemas. O registro em log 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 relatórios diretamente do ambiente do ESET NOD32 Antivirus, bem como arquivar relatórios.



Os relatórios podem ser acessados na [janela principal do programa](#), clicando em **Ferramentas > Arquivos de relatório**. Selecione o tipo de log desejado no menu suspenso **Log**. Os seguintes logs estão disponíveis:

- **Detecções** – este relatório fornece informações detalhadas sobre as detecções e infiltrações detectadas pelo ESET NOD32 Antivirus. As informações de relatório incluem a hora da detecção, tipo de escaneador, tipo de objeto, local do objeto, nome da detecção, ação realizada, nome do usuário conectado no momento em que a infiltração foi detectada, hash e primeira ocorrência. 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 NOD32 Antivirus 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 a solução de problemas de administradores do sistema e de usuários. Muitas vezes as informações encontradas aqui podem ajudá-lo a encontrar uma solução para um problema no programa.
- **Escaneamento do computador** – Os resultados de todos os escaneamentos concluídos são exibidos nessa janela. Cada linha corresponde a um escaneamento no computador. Clique duas vezes em qualquer entrada para exibir os [detalhes do selecionado escaneamento](#).
- **HIPS** - Contém registros de regras específicas [HIPS](#) 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.
- **Sites filtrados** – Esta lista é útil se você quiser visualizar uma lista de sites que foram bloqueados pela [Proteção de acesso à web](#). Cada relatório inclui o horário, endereço URL, usuário e aplicativo que criaram uma conexão para o site específico.

- **Controle de dispositivos** - Contém registros de dispositivos ou mídias removíveis que foram conectados ao computador. Apenas dispositivos com Regras de controle de dispositivo respectivas serão registrados no arquivo de log. Se a regra não coincidir com um dispositivo conectado, uma entrada de log para um dispositivo conectado não será criada. 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** e **SHIFT** para selecionar várias entradas.

Clique em  **Filtragem** para abrir a janela de [Filtragem de relatórios](#) onde você pode definir 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 os registros selecionados na janela.
- **Remover/Remover tudo** – Exclui os registros selecionados ou todos os registros exibidos. Essa ação requer privilégios de administrador.
- **Exportar/Exportar tudo** – exporta informações sobre os registros selecionados ou todos os registros em formato XML.
- **Encontrar/Encontrar próximo/Encontrar anterior** – depois de clicar nessa opção, você pode definir critérios de filtragem para destacar a entrada específica usando a janela Filtragem de relatório.
- **Descrição da detecção** – abre a Enciclopédia de ameaças da ESET, que contém informações detalhadas sobre os perigos e os sinais da infiltração registrada.
- **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 NOD32 Antivirus 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, 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 arquivos de relatório** - Se selecionado, os arquivos de relatório 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 logs vazias são removidas durante esse processo, o que melhora o desempenho e a velocidade de processamento de logs. Essa melhoria pode ser observada especialmente se os logs 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** – O diretório no qual relatórios serão armazenados (aplica-se somente a texto/CSV). Cada seção do relatório tem seu próprio arquivo com um nome de arquivo predefinido (por exemplo, virlog.txt para a seção **Deteções** 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 relatórios** - Apaga todos os relatórios armazenados atualmente selecionados no menu suspenso **Tipo**. Uma notificação sobre a exclusão bem sucedida dos relatórios será exibida.

**i** 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](#).

## 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 NOD32 Antivirus oferece informações detalhadas sobre os processos em execução a fim de proteger os usuários com a tecnologia [ESET LiveGrid®](#).

**eset** NOD32 ANTIVIRUS

ESET HOME

### Processos em execução

Esta janela exibe uma lista de arquivos selecionados com informações adicionais no ESET LiveGrid®. A reputação de cada um é indicada, juntamente com o número de usuários e a hora da primeira descoberta.

Reputação	Processo	PID	Número de usu...	Hora da desc...	Nome do aplicativo
●●●●●●●●	smss.exe	356	●●●●●●●●	três meses atrás	Microsoft® Windows® Oper...
●●●●●●●●	csrss.exe	452	●●●●●●●●	um ano atrás	Microsoft® Windows® Oper...
●●●●●●●●	wininit.exe	524	●●●●●●●●	um mês atrás	Microsoft® Windows® Oper...
●●●●●●●●	services.exe	572	●●●●●●●●	seis meses atrás	Microsoft® Windows® Oper...
●●●●●●●●	winlogon.exe	616	●●●●●●●●	um mês atrás	Microsoft® Windows® Oper...
●●●●●●●●	lsass.exe	660	●●●●●●●●	seis meses atrás	Microsoft® Windows® Oper...
●●●●●●●●	svchost.exe	748	●●●●●●●●	um ano atrás	Microsoft® Windows® Oper...
●●●●●●●●	fontdrvhost.exe	760	●●●●●●●●	um mês atrás	Microsoft® Windows® Oper...
●●●●●●●●	dwm.exe	980	●●●●●●●●	seis meses atrás	Microsoft® Windows® Oper...
●●●●●●●●	vboxservice.exe	1412	●●●●●●●●	um ano atrás	Oracle VM VirtualBox Guest A...
●●●●●●●●	wudfhost.exe	1472	●●●●●●●●	um ano atrás	Microsoft® Windows® Oper...

**Caminho:** c:\windows\system32\smss.exe  
**Tamanho:** 152,3 kB  
**Descrição:** Windows Session Manager  
**Companhia:** Microsoft Corporation  
**Versão:** 10.0.19041.1 (WinBuild.160101.0800)  
**Produto:** Microsoft® Windows® Operating System  
**Criado em:** 5/12/2021 12:02:49 AM  
**Modificado em:** 5/12/2021 12:02:49 AM

Esconder detalhes

**Reputação** – Na maioria dos casos, o ESET NOD32 Antivirus 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 risco aos objetos, que vai de 1 – Aceitável (verde) a 9 – Perigoso (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. Para abrir o Gerenciador de Tarefas, clique com o botão direito em uma área vazia na barra de tarefas e clique em **Gerenciador de tarefas** ou pressione **Ctrl+Shift+Esc** no seu teclado.

**i** Aplicativos conhecidos marcados como Bom (verde) estão definitivamente limpos (na lista de permissões) e serão excluídos do rastreamento para melhorar o desempenho.

**PID** - O número identificador do processo pode ser usado como um parâmetro em várias chamadas de função como ajustar a prioridade do processo.

**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®.

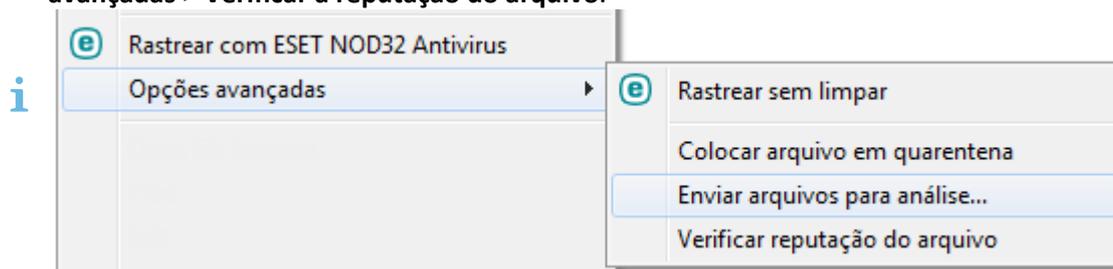
**i** Um aplicativo marcado como Desconhecido (laranja) não é necessariamente software malicioso. Geralmente, é apenas um aplicativo mais recente. Se você não tem certeza sobre o arquivo, você pode [enviar o arquivo para análise](#) no ESET Research Lab. Se for detectado que o arquivo é um aplicativo malicioso, sua detecção será adicionada em uma das atualizações posteriores.

**Nome do aplicativo** – O nome de um programa ou processo.

Clique em um aplicativo para exibir os seguintes detalhes do aplicativo:

- **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/Modificado em** - Data e hora da criação (modificação).

Você também pode verificar a reputação de arquivos que não agem como programas/processos em execução. Para fazer isso, clique neles com botão direito em um explorador de arquivos e selecione **Opções avançadas > Verificar a reputação do arquivo**.



# 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.
- **PUA detectado** - Exibe o número de [aplicativos potencialmente indesejados](#) (PUA) detectados.
- **Documentos verificados** – Exibe o número de objetos de documento escaneados.
- **Aplicativos escaneados** – Exibe o número de objetos executáveis escaneados.
- **Outros objetos verificados** – 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.

Depois que o recurso é ativado, ele não é mais exibido como não estando funcional no relatório de Segurança.

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 NOD32 Antivírus 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 > Mensagem de confirmação > Editar**.

## 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. Para aprender a usar o ESET SysInspector, consulte a [ESET SysInspector Ajuda on-line](#).

A janela ESET SysInspector exibe as seguintes informações sobre os relatórios:

- **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 selecionado em ESET SysInspector. Também é possível clicar com o botão direito

do mouse em um determinado relatório e selecionar **Exibir** no menu de contexto.

- **Comparar** - Compara dois relatórios existentes.
- **Criar** - Cria um novo log. Aguarde até ESET SysInspector ser gerado (status **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).
- **Comparar** - Compara dois relatórios existentes.
- **Criar** - Cria um novo log. Aguarde até ESET SysInspector ser gerado (status **Criado**) antes de tentar acessar o relatório.
- **Excluir** - Exclui os relatórios selecionados da lista.
- **Excluir tudo** – Exclui todos os relatórios.
- **Exportar** - Exporta o relatório para um arquivo .xml ou .xml compactado. O relatório é exportado para C:\ProgramData\ESET\ESET Security\SysInspector.

## 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 NOD32 Antivirus 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 de módulos, tarefa de rastreamento, verificação 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). Você pode reverter a lista de tarefas agendadas para o padrão e excluir todas as alterações clicando em **Padrão**. 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** (após a atualização bem sucedida do mecanismo de detecção)

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 em **Editar**.

Tarefa	Nome	Acionadores	Próxima execução	Última execução	
<input checked="" type="checkbox"/>	Manutenção dos r...	Manutenção dos relat...	A tarefa será executad...	10/14/2021 2:00:00 AM	10/13/2021 10:22:12 PM
<input checked="" type="checkbox"/>	Atualizar	Atualização automáti...	A tarefa será executad...	10/14/2021 2:22:40 AM	10/14/2021 1:22:40 AM
<input checked="" type="checkbox"/>	Atualizar	Atualizar automaticam...	Em conexão dial-up co...	Evento disparado	
<input type="checkbox"/>	Atualizar	Atualizar automaticam...	No entrar de usuário (...)	Evento disparado	
<input checked="" type="checkbox"/>	Escanear arquivo ...	Escaneamento do arqu...	No entrar de usuário A...	Evento disparado	10/14/2021 1:45:34 AM
<input checked="" type="checkbox"/>	Escanear arquivo ...	Escaneamento do arqu...	Atualização bem-suced...	Evento disparado	10/14/2021 1:42:55 AM

## Adicionar uma nova tarefa

1. Clique em **Adicionar tarefa** na parte inferior da janela.
2. Insira um 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 os módulos.

4. Clique na barra deslizante ao lado de **Ativado** para 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 (horas)** – representa o tempo decorrido desde a primeira vez que a tarefa foi ignorada. Se este tempo for ultrapassado, a tarefa será executada imediatamente. Defina a hora usando a chave de cabeça abaixo.

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**  
Manutenção dos relatórios

**Tipo de tarefa**  
Manutenção dos relatórios

**Executar a tarefa**  
A tarefa será executada todos os dias às 3:00:00 AM.

**Ação a ser realizada se a tarefa não for executada na hora especificada**  
O mais breve possível

OK

# Opções de escaneamento programado

Nesta janela, você pode especificar opções avançadas para uma tarefa agendada de escaneamento do computador.

Para executar um escaneamento sem nenhuma ação de limpeza, clique em **Configurações avançadas** e 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 definir uma ação a ser realizada automaticamente depois de um escaneamento terminar usando o menu suspenso:

- **Nenhuma ação** - Depois do fim do rastreamento, nenhuma ação será realizada.
- **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** – o computador será reiniciado se necessário apenas para concluir a limpeza das ameaças detectadas.
- **Forçar reinicialização** – força o encerramento de todos os programas abertos sem esperar pela interação do usuário e reinicia o computador depois do fim do escaneamento.
- **Forçar reinicialização se necessário** – o computador será reiniciado se necessário apenas para concluir a limpeza das ameaças detectadas.
- **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. Sua computador é desligado, mas vai voltar ao seu estado anterior da próxima vez que for iniciado.

**i** As ações de **Suspender** ou **Hibernar** estão disponíveis com base nas configurações do sistema operacional de Energia e hibernação ou das capacidades do seu computador/notebook. Lembre-se 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 **O escaneamento não pode ser cancelado** para negar aos usuários não privilegiados a capacidade de interromper ações realizadas depois do escaneamento.

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.

Veja também o [Progresso do escaneamento](#).

# Visão geral da tarefa agendada

Esta janela de diálogo exibe informações detalhadas sobre a tarefa agendada selecionada quando você clicar duas vezes em uma tarefa personalizada ou clicar com o botão direito do mouse em uma tarefa do agendador personalizado e clicar em **Mostrar detalhes da tarefa**.

## Detalhes da tarefa

Digite o **Nome da tarefa**, selecione uma das opções de **Tipo da tarefa** e clique em **Avançar**:

- **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.

## Tempo da tarefa

A tarefa será realizada repetidamente no intervalo de tempo especificado. Selecione uma das opções de intervalo de tempo:

- **Uma vez** - A tarefa será realizada somente uma vez, na data e hora predefinidas.
- **Repetidamente** - A tarefa será realizada no intervalo de tempo especificado (em horas).
- **Diariamente** - A tarefa será realizada diariamente na hora especificada.
- **Semanalmente** - A tarefa será realizada uma ou mais vezes por semana, no(s) dia(s) e hora selecionados.
- **Acionado por evento** - A tarefa será realizada após um evento especificado.

**Pular tarefa quando estiver executando na bateria** - Uma tarefa não será iniciada se o computador estiver utilizando bateria no momento que a tarefa deveria ser iniciada. Isso também se aplica a computadores que são executados em UPS.

## Tempo da tarefa – única

**Execução de tarefas** - A tarefa especificada será realizada uma vez somente na data e hora especificadas.

## Tempo da tarefa – diária

A tarefa será realizada diariamente na hora especificada.

## Tempo da tarefa – semanal

A tarefa será executado repetidamente a cada semana nos dias e hora selecionados.

## Tempo da tarefa – acionada por evento

A tarefa será acionada por um dos seguintes eventos:

- **Sempre que o computador for iniciado**
- **Na primeira vez em que o computador for iniciado diariamente**
- **Conexão dial-up com a Internet/VPN**
- **Atualização de módulo bem sucedida**
- **Atualização de produto bem sucedida**
- **Após logon do usuário**
- **Detecção de ameaças**

Ao agendar uma tarefa acionada por um evento, você pode especificar o intervalo mínimo entre as duas conclusões da tarefa. Por exemplo, se você fizer logon no seu computador várias vezes ao dia, escolha 24 horas para realizar a tarefa somente no primeiro logon do dia e, em seguida, no dia seguinte.

## Tarefa ignorada

É possível [ignorar uma tarefa se o computador estiver desligado ou sendo executado na bateria](#). Selecione quando a tarefa ignorada deve ser executada a partir de uma dessas opções e clique em **Avançar**:

- **Na próxima hora agendada** – a tarefa será realizada se o computador estiver ligado na próxima hora agendada.
- **O mais breve possível** – a tarefa será executado quando o computador estiver ligado.
- **Imediatamente, se o tempo depois da última operação agendada ultrapassar (horas)** – representa o tempo decorrido desde a primeira execução ignorada da tarefa. Se este tempo for ultrapassado, a tarefa será executada imediatamente.

## Imediatamente, se o tempo depois da última execução agendada ultrapassar (horas) – exemplos

Uma tarefa de exemplo é configurada para ser executada repetidamente a cada hora. A opção **Imediatamente, se o tempo depois da última operação agendada ultrapassar (horas)** será selecionada e o tempo ultrapassado é definido como duas horas. A tarefa é executado às 13:00 e, quando terminada, o computador é suspenso:

- O computador acordará às 15:30. A primeira vez que a tarefa foi ignorada foi às 14:00. Apenas 1,5 horas se passaram desde as 14:00, então a tarefa será executado às 16:00.
- O computador acordará às 16:30. A primeira vez que a tarefa foi ignorada foi às 14:00. Duas horas e meia se passaram desde as 14:00, então a tarefa será executada imediatamente.

## Detalhes da tarefa – atualizar

Se você deseja atualizar o programa a partir de dois servidores de atualização, é necessário criar dois perfis de atualização diferentes. Se o primeiro falhar em fazer download dos arquivos de atualização, o programa alterna para o outro. Isso é útil para notebooks por exemplo, os quais normalmente são atualizados de um servidor de atualização de rede local, mas seus proprietários frequentemente conectam-se à Internet usando outras redes. Portanto, se o primeiro perfil falhar, o segundo automaticamente fará download dos arquivos de atualização dos servidores de atualização da ESET.

## Detalhes da tarefa – executar aplicativo

Essa tarefa agenda a execução de um aplicativo externo.

### Detalhes da tarefa ?

Executar aplicativo

Arquivo executável	<input type="text" value="C:\Program Files\Internet Explorer\iexplore.exe"/>
Pasta de trabalho	<input type="text" value="Internet Explorer"/>
Parâmetros	<input type="text" value="www.eset.com"/>

**Arquivo executável** - Escolha um arquivo executável na árvore de diretórios, clique na opção ... ou insira o caminho manualmente.

**Pasta de trabalho** - Defina o diretório de trabalho do aplicativo externo. Todos os arquivos temporários do

**arquivo executável** selecionado serão criados neste diretório.

**Parâmetros** - Parâmetros da linha de comando do aplicativo (opcional).

Clique em **Concluir** para aplicar a tarefa.

## Limpeza do sistema

A Limpeza do sistema é uma ferramenta que ajuda você a restaurar o computador para um estado de uso depois de limpar a ameaça. Malware pode desativar utilitários do sistema como o Editor de registro, Gerenciador de tarefas ou Atualizações do Windows. A Limpeza do sistema restaura os valores e configurações padrão para um determinado sistema em um único clique.

A Limpeza do sistema emite relatórios de cinco categorias de configuração:

- **Configurações de segurança:** mudanças nas configurações que podem causar um aumento da vulnerabilidade do seu computador, como uma Atualização do Windows
- **Configurações do sistema:** alterações nas configurações do sistema que podem alterar o comportamento de seu computador, como associações de arquivos
- **Aparência do sistema:** configurações que afetam a aparência do seu sistema, como o papel de parede da sua área de trabalho
- **Recursos desativados:** recursos e aplicativos importantes que podem estar desativados
- **Restauração do Sistema Windows:** configurações para o recurso de Restauração do Sistema Windows, que permite a você reverter seu sistema para um estado anterior

A Limpeza do sistema pode ser solicitada:

- quando uma ameaça for encontrada
- quando um usuário clicar em **Redefinir**

Você pode revisar as mudanças e redefinir as configurações se for apropriado.



**i** Apenas um usuário com direitos de Administrador pode realizar ações na Limpeza do sistema.

## 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](#)

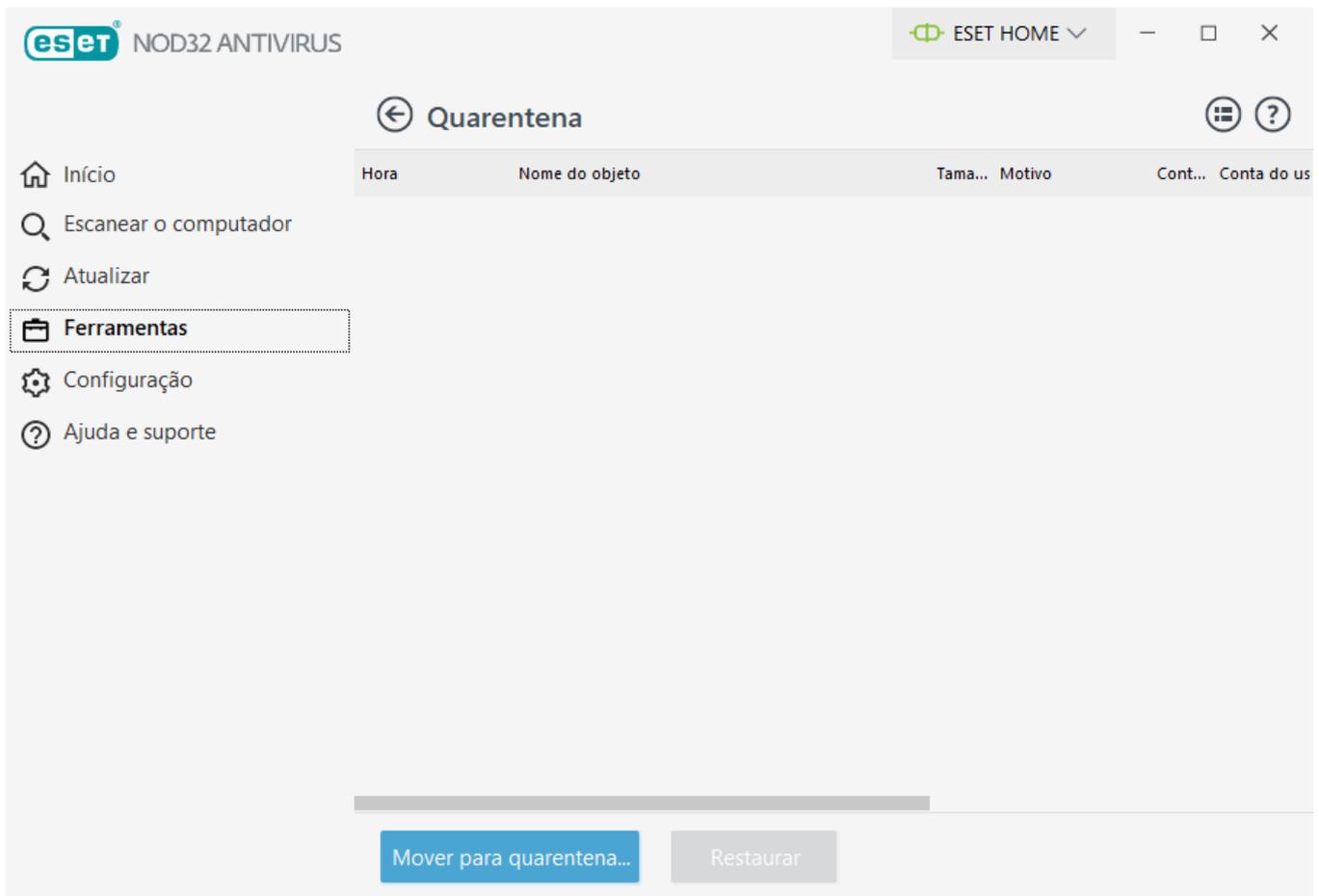
## Quarentena

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 NOD32 Antivirus ao clicar em **Ferramentas > Quarentena**.

Os arquivos armazenados na pasta de quarentena podem ser visualizados em uma tabela que exhibe:

- 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).



## Colocação de arquivos em quarentena

O ESET NOD32 Antivirus 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 NOD32 Antivirus,
- 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 com o botão direito do mouse no arquivo > clique em **Opções avançadas > Arquivo em quarentena**.

c. Clique em **Mover para quarentena** da janela **Quarentena**.

d. 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.

## Descrição da detecção

Clique com o botão direito em um item e clique em **Descrição da detecção** para abrir a Enciclopédia de ameaças da ESET, que contém informações detalhadas sobre os perigos e os sinais da infiltração registrada.

## Instruções ilustradas

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

- [Restaurar um arquivo colocado em quarentena no ESET NOD32 Antivirus](#)
- [Remover um arquivo colocado em quarentena no ESET NOD32 Antivirus](#)
- [Meu produto ESET notificou uma detecção, o que faço?](#)

## Falha na quarentena

Os motivos pelos quais arquivos específicos não podem ser movidos para a Quarentena são os seguintes:

- **Você não tem permissões de leitura** – significa que você não pode visualizar o conteúdo de um arquivo.
- **Você não tem permissões de gravação** – significa que não é possível modificar o conteúdo do arquivo, ou seja, adicionar novo conteúdo ou remover o conteúdo existente.
- **O arquivo que você está tentando colocar em quarentena é muito grande** – você precisa reduzir o tamanho do arquivo.

Quando você receber uma mensagem de erro "Falha na quarentena", clique em **Mais informações**. A janela da lista de erros de quarentena aparece e você verá o nome do arquivo e o motivo pelo qual o arquivo não pode ser colocado em quarentena.

## 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 precisam ser definidas. Caso contrário, o programa não será capaz de atualizar a si mesmo automaticamente. No ESET NOD32 Antivirus, 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 NOD32 Antivirus. 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.

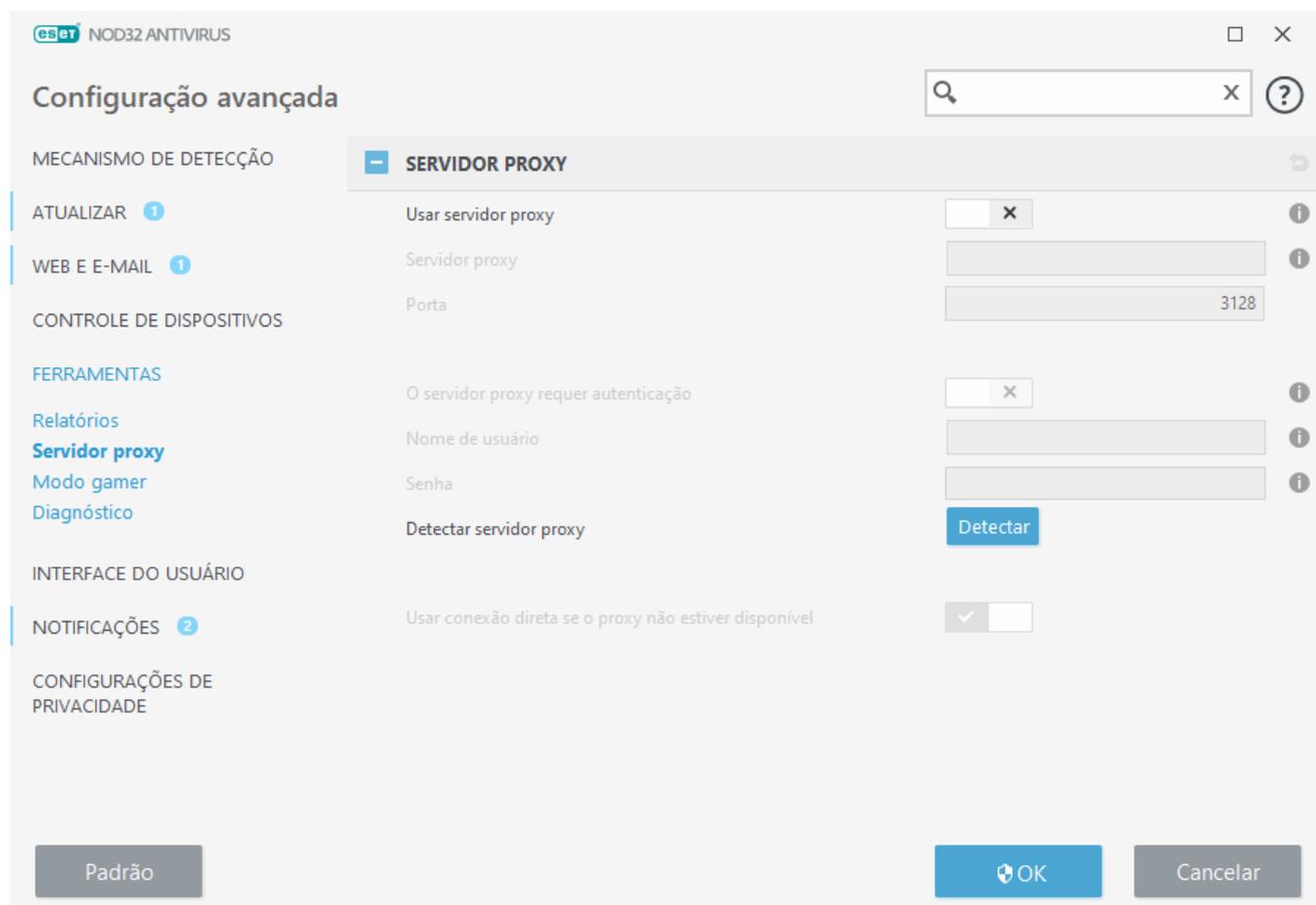
Se a comunicação com o servidor proxy exigir autenticação, selecione **O servidor proxy requer autenticação** e digite um **Nome de usuário** e uma **Senha** válidos nos respectivos campos. Clique em **Detectar servidor proxy** para detectar e preencher automaticamente as configurações do servidor proxy. Os parâmetros especificados nas opções de Internet para o Internet Explorer ou Google Chrome serão copiados.

**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 NOD32 Antivirus estiver configurado para conectar via proxy e não for possível acessar o proxy, o ESET NOD32 Antivirus 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 de assinatura de vírus de locais remotos. Para obter mais informações sobre essa configuração, consulte [Configuração avançada de atualização](#).



## Selecionar amostra 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®).

### Antes de enviar amostras para a ESET

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).

Você pode enviar uma amostra (um arquivo ou site) para a ESET analisar usando um dos métodos a seguir:

1. Use o formulário de envio de amostra no seu produto. Ele está localizado em **Ferramentas > Enviar amostra para análise**. O tamanho máximo de uma amostra enviada é de 256 MB.

2. Como alternativa, você pode enviar o arquivo por email. Se for esta sua opção, compacte o(s) arquivo(s) usando WinRAR/WinZIP, proteja o arquivo com a senha "infected" (infectado) e envie-o para [samples@eset.com](mailto:samples@eset.com).

3. Para reportar spam ou falsos positivos de spam, consulte nosso [artigo da base de conhecimento ESET](#).

No formulário **Selecionar amostra para análise**, selecione a descrição mais adequada à sua mensagem no menu suspenso **Motivo para envio da amostra**:

- [Arquivo suspeito](#)
- [Site suspeito](#) (um site que está infectado por algum malware),
- [Site falso positivo](#)
- [Arquivo falso positivo](#) (arquivo que é detectado como uma infecção, mas que não está infectado),
- [Outros](#)

**Arquivo/Site** - O caminho do arquivo ou site que você pretende enviar.

**Email de contato** – O email de contato será enviado junto com arquivos suspeitos para a ESET e poderá 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 pode não receber uma resposta da ESET

**i** 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 processamento de identificação do arquivo suspeito.

**i** 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 antispymware 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.

# 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 NOD32 Antivirus 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.

## Janela de diálogo – Atualizações do sistema

Se houver alguma atualização para seu sistema operacional disponível, a janela Início do ESET NOD32 Antivirus vai exibir a notificação. Clique em **Mais informações** para abrir a janela de Atualizações do sistema.

A janela Atualizações do sistema mostra a lista de atualizações disponíveis prontas para serem obtidas por download e instaladas. O tipo da atualização é mostrado próximo ao nome da atualização.

Clique duas vezes em qualquer linha de atualização para exibir a janela das [Informações de atualização](#) com informações adicionais.

Clique em **Executar atualização do sistema** para iniciar o download e a instalação de atualizações do sistema operacional.

## Atualizar informações

Informações sobre atualizações do Windows. O nome e o número da atualização são exibidos na parte superior da janela, seguidos pela prioridade e pela descrição do problema solucionado pela atualização.

## Interface do usuário

Para configurar o comportamento da interface gráfica do usuário (GUI) do programa, na [janela principal do programa](#), clique em **Configuração > Configuração avançada (F5) > Interface do usuário**.

Você pode ajustar a aparência visual do programa e os efeitos usados na tela de configuração avançada [Elementos da interface do usuário](#).

Para obter a máxima segurança do seu software, você pode evitar desinstalação ou quaisquer alterações não autorizadas protegendo as configurações com uma senha com a ajuda da ferramenta [Configuração de acesso](#).

**i** Para configurar o comportamento de notificações do sistema, alertas de detecção e status de aplicativos, consulte a seção [Notificações](#).

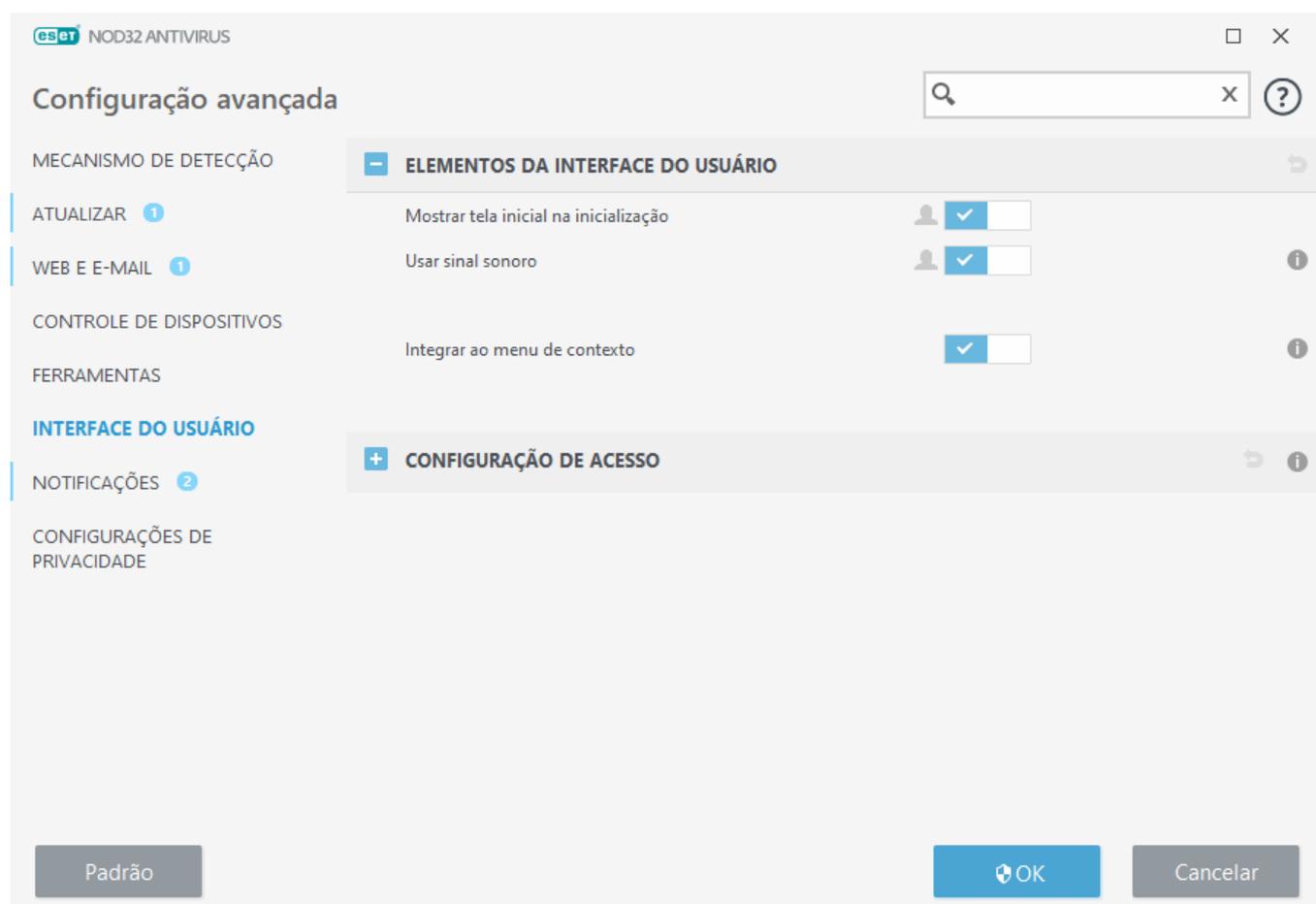
## Elementos da interface do usuário

As opções de configuração da interface do usuário no ESET NOD32 Antivirus permitem que você ajuste o ambiente de trabalho para que ele atenda às suas necessidades. Essas opções de configuração são acessíveis em **Configuração avançada (F5) > Interface do usuário > Elementos da interface do usuário**.

Se desejar desativar a tela inicial do ESET NOD32 Antivirus, desmarque a opção **Mostrar tela inicial na inicialização**.

**Usar sinal sonoro** – o ESET NOD32 Antivirus reproduz um som quando ocorrerem eventos importantes durante um escaneamento, por exemplo quando uma ameaça é descoberta ou quando o escaneamento for concluído.

**Integrar ao menu de contexto** - Integra os elementos de controle do ESET NOD32 Antivirus no menu de contexto.



# Configuração de acesso

As configurações do ESET NOD32 Antivirus são uma parte essencial de sua política de segurança. Modificações não autorizadas podem colocar em risco a estabilidade e a proteção do seu sistema. Para evitar modificações não autorizadas, os parâmetros de configuração e desinstalação do ESET NOD32 Antivirus podem ser protegidos por senha.

Para definir uma senha para proteger os parâmetros de configuração e desinstalação do ESET NOD32 Antivirus, clique em **Definir** ao lado de **Configurações protegidas por senha**.

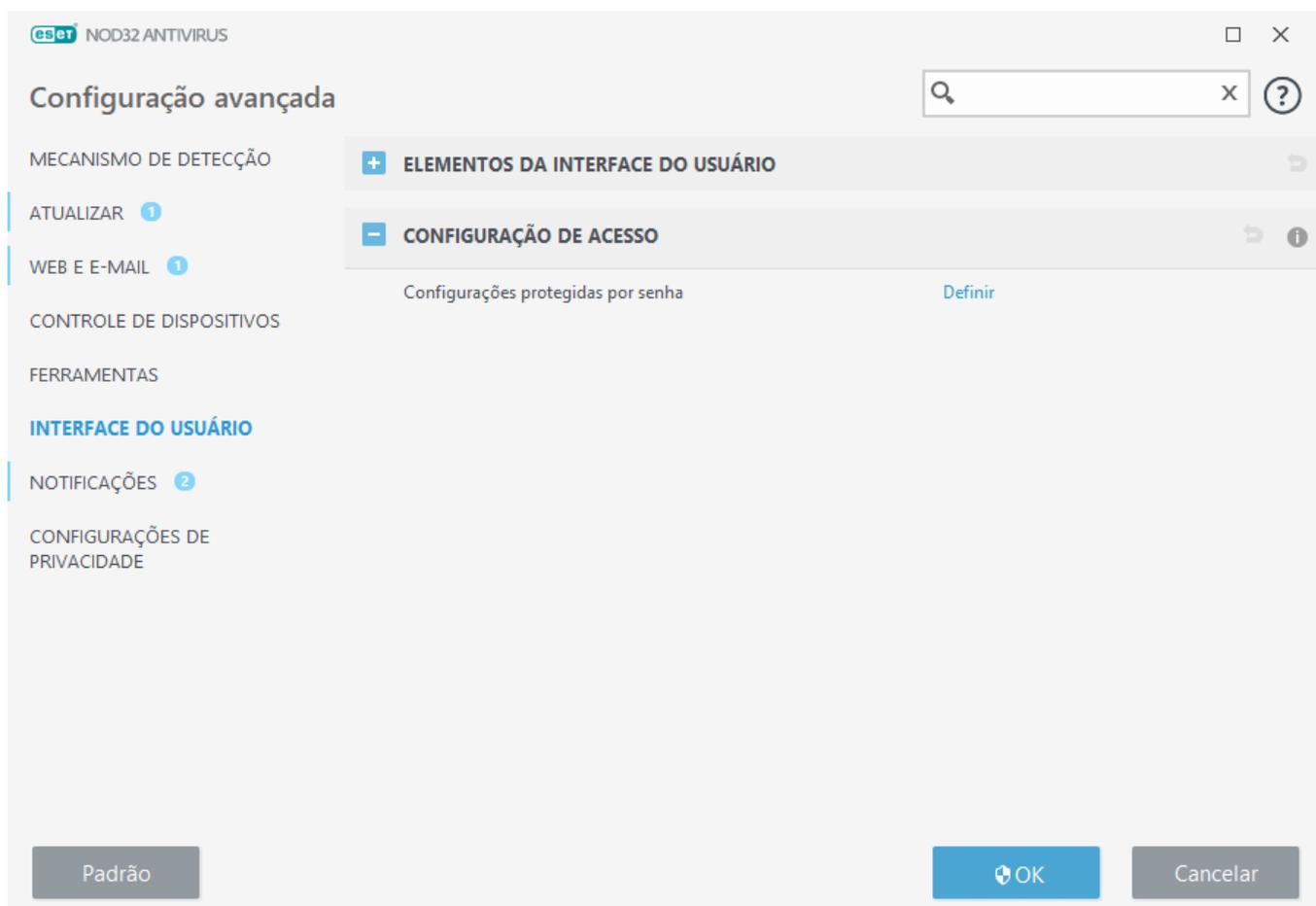


Quando você quiser acessar a definição da Configuração avançada, será exibida a janela onde digitar a senha. Se esquecer ou perder sua senha, clique na opção **Restaurar senha** abaixo e insira o endereço de email usado para seu registro de licença. A ESET vai enviar a você um email com o código de verificação e instruções sobre como redefinir sua senha.

- [Como desbloquear a Configuração avançada](#)

Para alterar sua senha, clique em **Alterar senha** ao lado de **Configurações protegidas por senha**.

Para remover sua senha, clique em **Remover** ao lado de **Configurações protegidas por senha**.



## Senha para Configuração avançada

Para proteger a configuração avançada do ESET NOD32 Antivirus para evitar modificação não autorizada, uma nova senha deve ser definida.

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**.

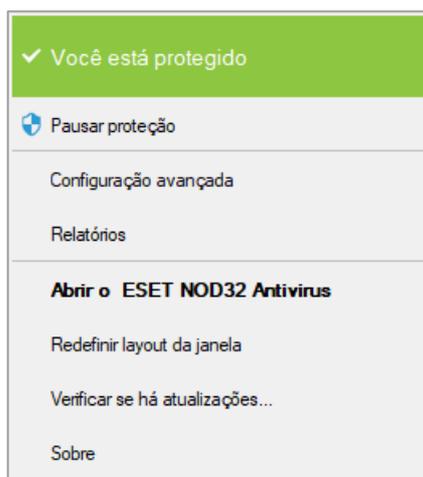
Esta senha será solicitada em todas as modificações futuras no ESET NOD32 Antivirus.

Se você esqueceu sua senha, o acesso às configurações avançadas pode ser [restaurado usando o método "Restaurar senha"](#).

Para recuperar sua chave de licença ESET perdida, a data de expiração de sua licença ou outras informações de licença do ESET NOD32 Antivirus, consulte nosso [artigo da Base de conhecimento](#).

## 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 .



**Pausar proteção** – Exibe a caixa de diálogo de confirmação que desativa o [Mecanismo de detecção](#), que protege contra ataques maliciosos ao sistema 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.



### Desativar proteção antivírus e antispyware?

Desativar a Proteção antivírus e antispyware vai desativar a Proteção em tempo real, Proteção de documentos, Proteção do acesso à web, Proteção do cliente de e-mail e a Proteção antiphishing. Isto deixará seu computador vulnerável a uma ampla gama de ameaças.

Pausar por 10 minutos ▾

Aplicar

Cancelar

**Configuração avançada** - Selecione esta opção para entrar na árvore de **Configuração avançada**. Existem também

outras formas de abrir as Configurações avançadas, como, por exemplo, pressionando a tecla F5 ou navegando até **Configuração > Configuração avançada**.

**Arquivos de relatório** – Os [arquivos de relatório](#) contêm informações sobre os eventos importantes do programa que ocorreram e fornecem uma visão geral das detecções.

**Abrir o ESET NOD32 Antivirus** – Abre a [janela principal de programa](#) do ESET NOD32 Antivirus do ícone da bandeja.

**Redefinir layout da janela** - Redefine a janela do ESET NOD32 Antivirus para seu tamanho e posição padrão na tela.

**Verificar se há atualizações** - Inicia a atualização do mecanismo de detecção (conhecido anteriormente como “banco de dados de assinatura de vírus”) para garantir seu nível de proteção em relação ao código malicioso.

**Sobre** - Fornece informações do sistema, detalhes sobre a versão instalada do ESET NOD32 Antivirus e os componentes do programa instalados. Aqui, você também pode encontrar a data de expiração de licença e informações sobre o sistema operacional e os recursos do sistema.

## Compatibilidade com leitor de tela

O ESET NOD32 Antivirus pode ser usado junto com leitores de tela para permitir que usuários da ESET com deficiência visual naveguem no produto ou para configurar as configurações. Os leitores de tela a seguir são compatíveis com o (JAWS, NVDA, Narrator).

Para se certificar de que o software leitor de tela pode acessar a interface gráfica do usuário do ESET NOD32 Antivirus corretamente, siga as instruções em nosso [artigo da Base de conhecimento](#).

## Ajuda e suporte

O ESET NOD32 Antivirus contém ferramentas de solução de problemas e informações de suporte que o ajudarão a solucionar eventuais problemas.



### Licença

- [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. Se o seu dispositivo estiver [conectado ao ESET HOME](#), escolha uma licença da sua conta ESET HOME ou adicione uma nova.



### Produto instalado

- [O que há de novo](#) – clique aqui para abrir a janela de informações sobre os recursos novos e aprimorados.
- [Sobre o ESET NOD32 Antivirus](#) – Exibe informações sobre sua cópia do ESET NOD32 Antivirus.
- [Solução de problemas do produto](#) – clique neste link para encontrar soluções para os problemas mais frequentemente encontrados.

- **Alterar produto** – Clique para ver se o ESET NOD32 Antivirus pode ser alterado para uma [linha de produto diferente](#) com a licença atual.



**Página de ajuda** - Clique nesse link para iniciar as páginas de ajuda do ESET NOD32 Antivirus.



**SupORTE técnico**



**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 NOD32 Antivirus

Esta janela fornece detalhes sobre a versão instalada do ESET NOD32 Antivirus e seu computador.

**e** **ESET NOD32 Antivirus™**, Versão 15.0.15.0  
A próxima geração da tecnologia NOD32.  
Copyright © 1992-2021 ESET, spol. s r.o. Todos os direitos reservados.  
Este produto está sob a Patente dos EUA N°. US 8.943.592.

[Acordo de Licença para o Usuário final](#)  
[Política de Privacidade](#)

Nome de usuário: DESKTOP-ILTJID9\User  
Nome do computador: DESKTOP-ILTJID9  
Nome da licença: DESKTOP-ILTJID9

[Mostrar módulos](#)

**Alerta:** Este programa é protegido por direitos autorais e tratados internacionais. A cópia ou distribuição sem permissão explícita da ESET, spol. s r.o. por qualquer meio, total ou parcialmente, é estritamente proibida e resultará em ações penais na total extensão permitida por tais leis internacionalmente. ESET, o logo ESET, ESET NOD32 Antivirus, LiveGrid, o logo LiveGrid, SysInspector são marcas comerciais registradas ou marcas comerciais da ESET, spol. s r.o. na União Europeia e/ou outros países. Todas as outras marcas comerciais são de propriedade de seus respectivos donos.

Clique em **Exibir módulos** para ver informações sobre a lista de módulos de programa carregados.

- 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.
- Clique em **Mecanismo de detecção** na janela de Módulos para abrir o radar de Vírus ESET, que contém informações sobre cada versão do Mecanismo de Detecção ESET.

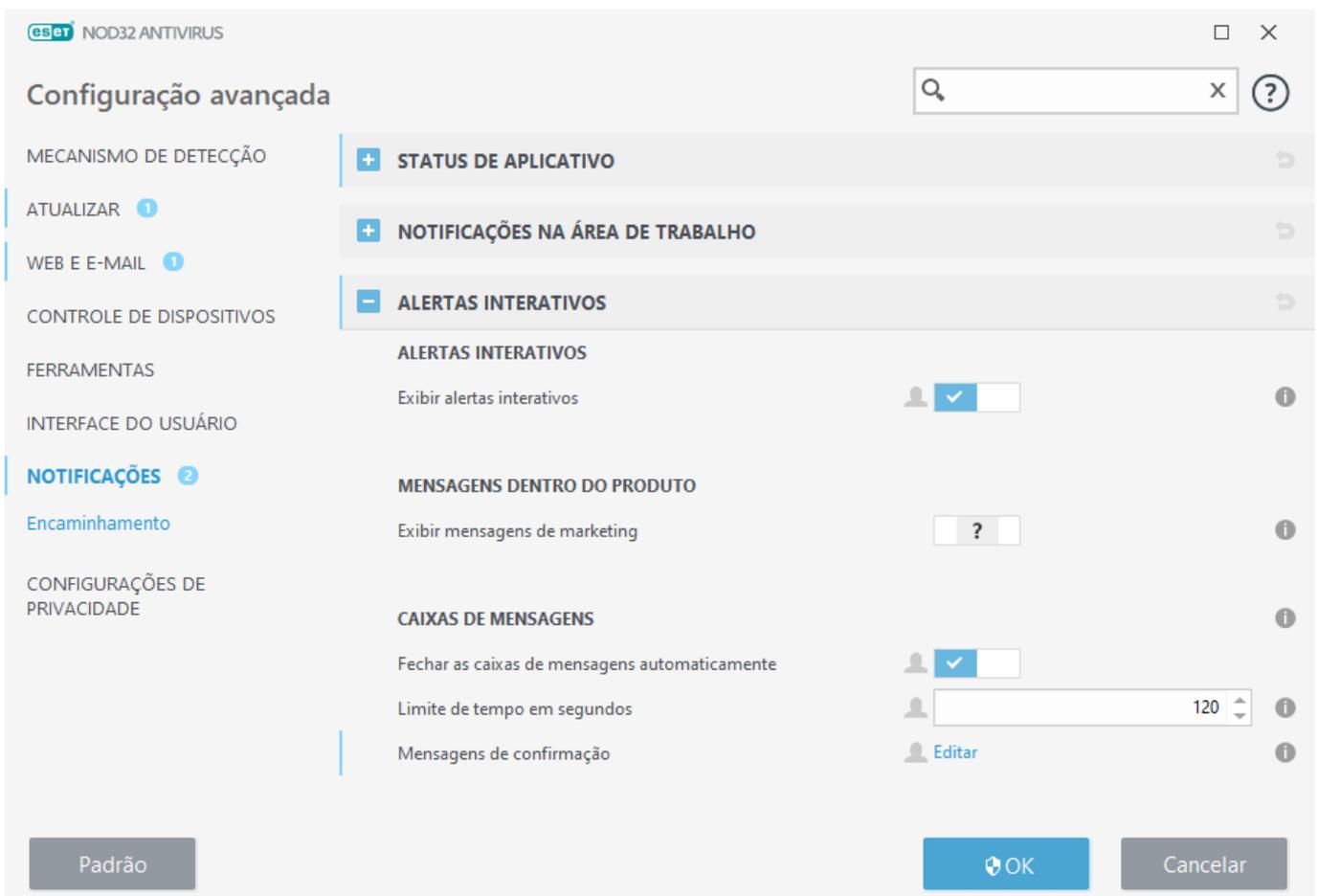
# Notícias ESET

Nesta janela o ESET NOD32 Antivirus informa as notícias ESET regularmente.

As mensagens dentro do produto foram feitas para informar os usuários ESET sobre novidades e outras comunicações. Para enviar mensagens de marketing é preciso ter o consentimento de um usuário. Portanto, mensagens de marketing não são enviadas a um usuário por padrão. Ao ativar essa opção você concorda em receber as mensagens de marketing da ESET. Se você não estiver interessado em receber o material de marketing da ESET, desative a opção **Exibir mensagens de marketing**.

Para ativar ou desativar o recebimento de mensagens de marketing via janela pop-up, siga as instruções abaixo.

1. Abra a janela do principal do seu produto ESET.
2. Pressione a tecla **F5** para acessar a **Configuração avançada**.
3. Clique em **Notificações > Alertas interativos**.
4. Modifique a opção **Exibir mensagens de marketing**.



## 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 NOD32 Antivirus, 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.

Ao 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

Na [janela do programa principal](#), clique em **Ajuda e Suporte > 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](#).

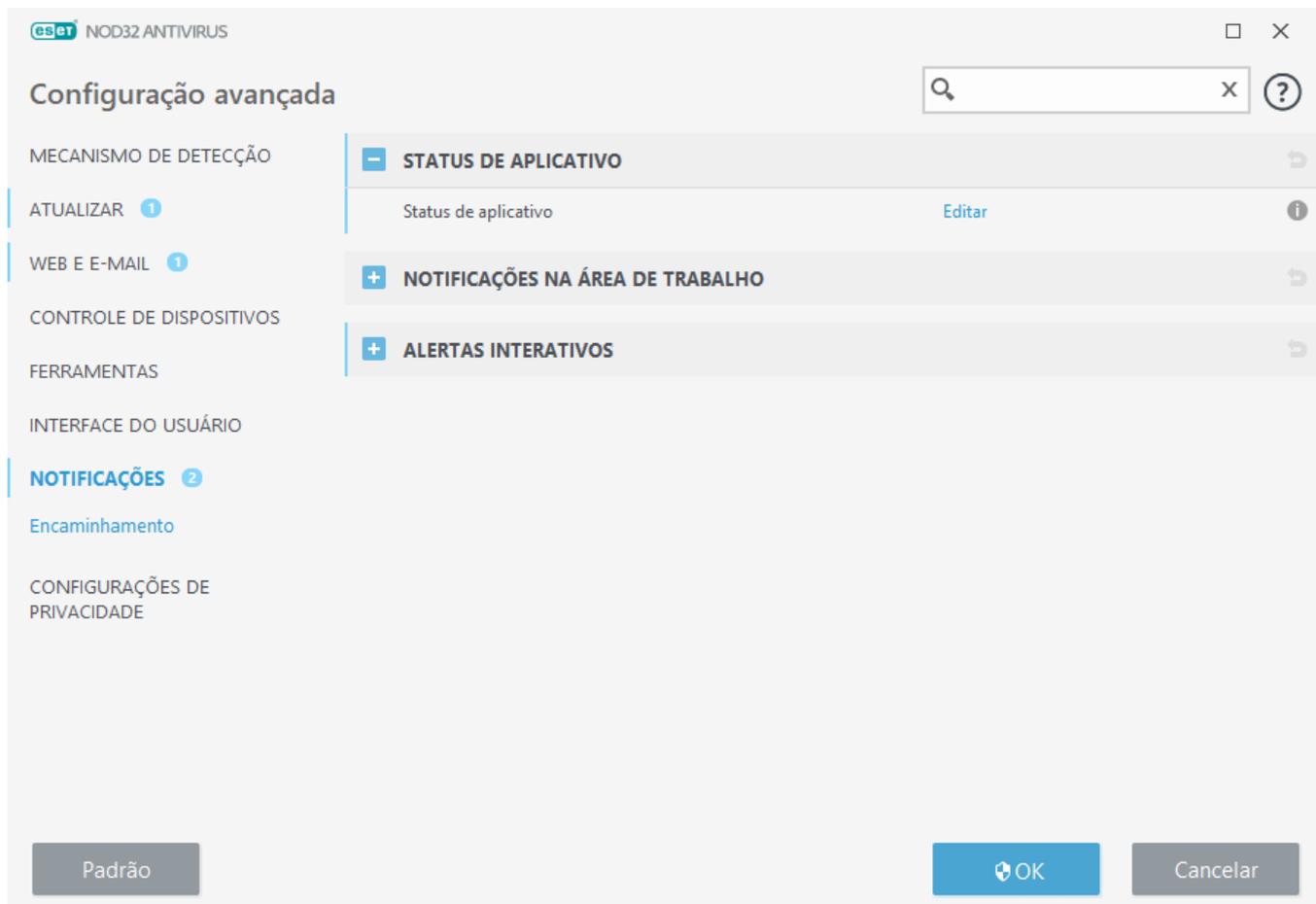
Ative o [Registro em relatório avançado](#) para criar relatórios avançados para todos os recursos disponíveis para ajudar os desenvolvedores a diagnosticarem e resolverem problemas. Detalhamento mínimo de registro em relatório definido para o nível **Diagnóstico**. O registro em relatório avançado será 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 NOD32 Antivirus, abra a **Configuração avançada (F5) > Notificações**. Você pode configurar os seguintes tipos de notificações:

- Status de aplicativo – notificações exibidas 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.

- [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**

**Status de aplicativo** – clique em **Editar** para selecionar quais status de aplicativos serão exibidos na seção inicial da [janela principal do programa](#).

## **Janela de diálogo – status de aplicativo**

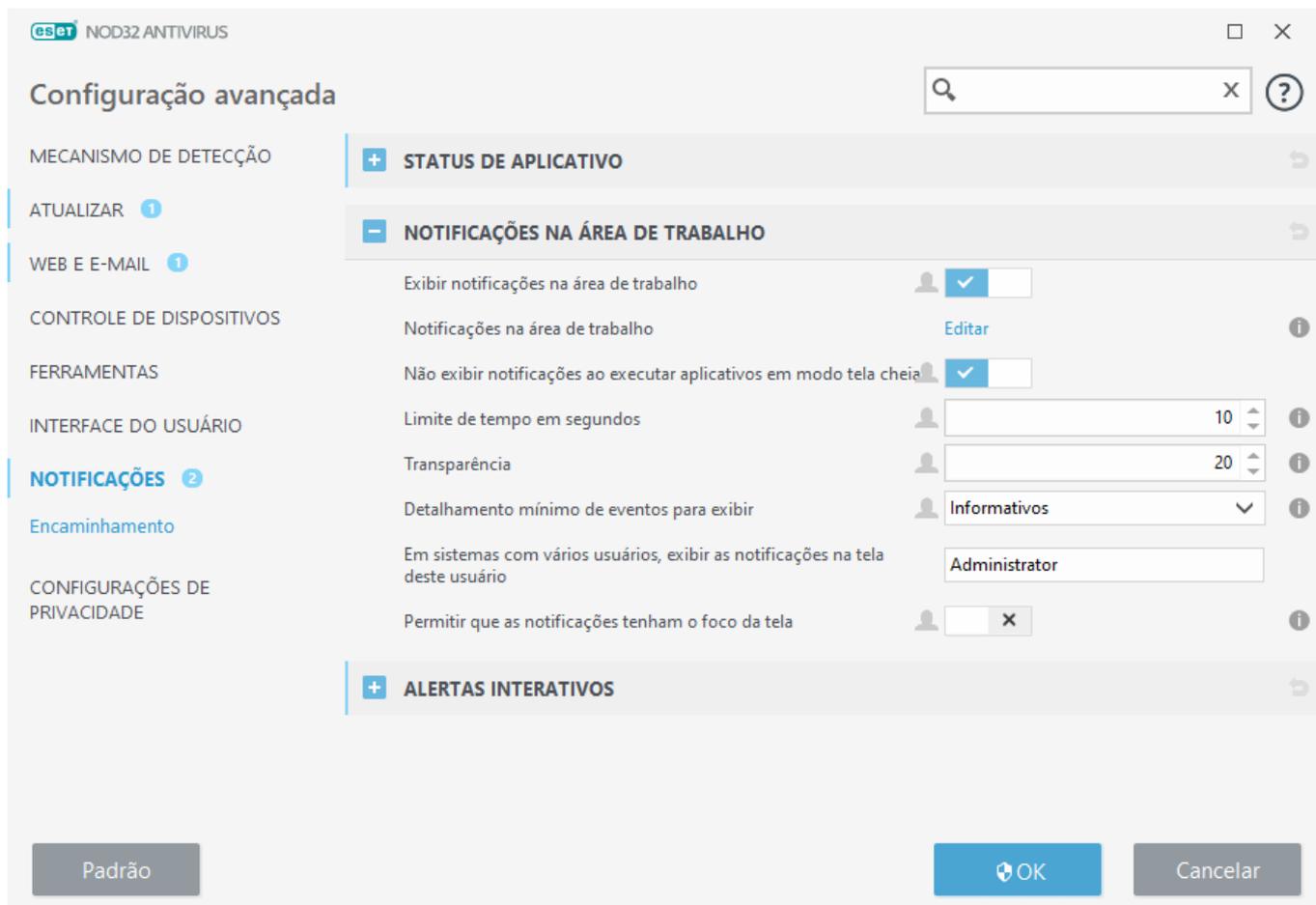
Nesta janela de diálogo, você pode selecionar quais status de aplicativos serão exibidos. Por exemplo, quando você pausa a Proteção antivírus e antispymware ou ativa o Modo gamer.

O status do aplicativo também será exibido se o produto não estiver ativado ou se sua licença tiver expirado.

## **Notificações na área de trabalho**

As notificações na área de trabalho são representadas por uma pequena janela pop-up ao lado da barra de tarefas do sistema. Por padrão, elas são exibidas por 10 segundos e depois desaparecem lentamente. As notificações incluem atualizações de produtos bem-sucedidas, novos dispositivos conectados, conclusão da tarefa

de escaneamento de vírus 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:

**O Diagnóstico** – exibe informações necessárias para ajustar o programa e todos os registros mencionados anteriormente.

**O Informativos** – exibe as mensagens informativas como eventos de rede fora do padrão, incluindo as mensagens de atualizações bem-sucedidas e todos os registros mencionados anteriormente.

**O Avisos** – exibe mensagens de aviso, erros e erros críticos (por exemplo, o Antisteach não está sendo

executado corretamente ou falha de atualização).

**O Erros** – exibe erros (por exemplo, proteção de documentos não iniciada) e erros críticos.

**O Crítico** – exibe somente os erros críticos (erro ao iniciar a proteção antivírus ou sistema infectado, etc.).

**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** – permite que as notificações se concentrem na tela e podem ser acessadas no menu **ALT + Tab**.

## Lista de notificações na área de trabalho

Para ajustar a visibilidade das notificações na área de trabalho (exibidas no canto inferior direito da tela), abra **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 **Exibir** apropriada.

Nome	Exibir na área de trabalho
<b>ATUALIZAÇÃO</b>	
A atualização de aplicativo está pronta	<input type="checkbox"/>
O Mecanismo de detecção foi atualizado com sucesso	<input type="checkbox"/>
Os módulos foram atualizados com sucesso	<input type="checkbox"/>
<b>GERAL</b>	
Exibir notificações das Novidades	<input checked="" type="checkbox"/>
Exibir notificações de relatório de segurança	<input checked="" type="checkbox"/>
O arquivo foi enviado para análise	<input type="checkbox"/>

### Geral

**Exibir notificações do relatório de segurança** – receba uma notificação quando um novo [Relatório de segurança](#) é gerado.

**Exibir notificações das Novidades** – notificações sobre todos os recursos novos e aprimorados da versão do produto mais recente.

**O arquivo foi enviado para análise** – receba uma notificação toda vez que o ESET NOD32 Antivirus enviar um arquivo para análise.

## Atualizar

**A atualização de aplicativo está pronta** – receba uma notificação quando houver uma atualização para uma nova versão do ESET NOD32 Antivirus preparada.

**O Mecanismo de Detecção foi atualizado com sucesso** – receba uma notificação quando o produto atualizar os módulos do Mecanismo de detecção.

**Os módulos foram atualizados com sucesso** – receba uma notificação quando o produto atualizar os componentes do programa.

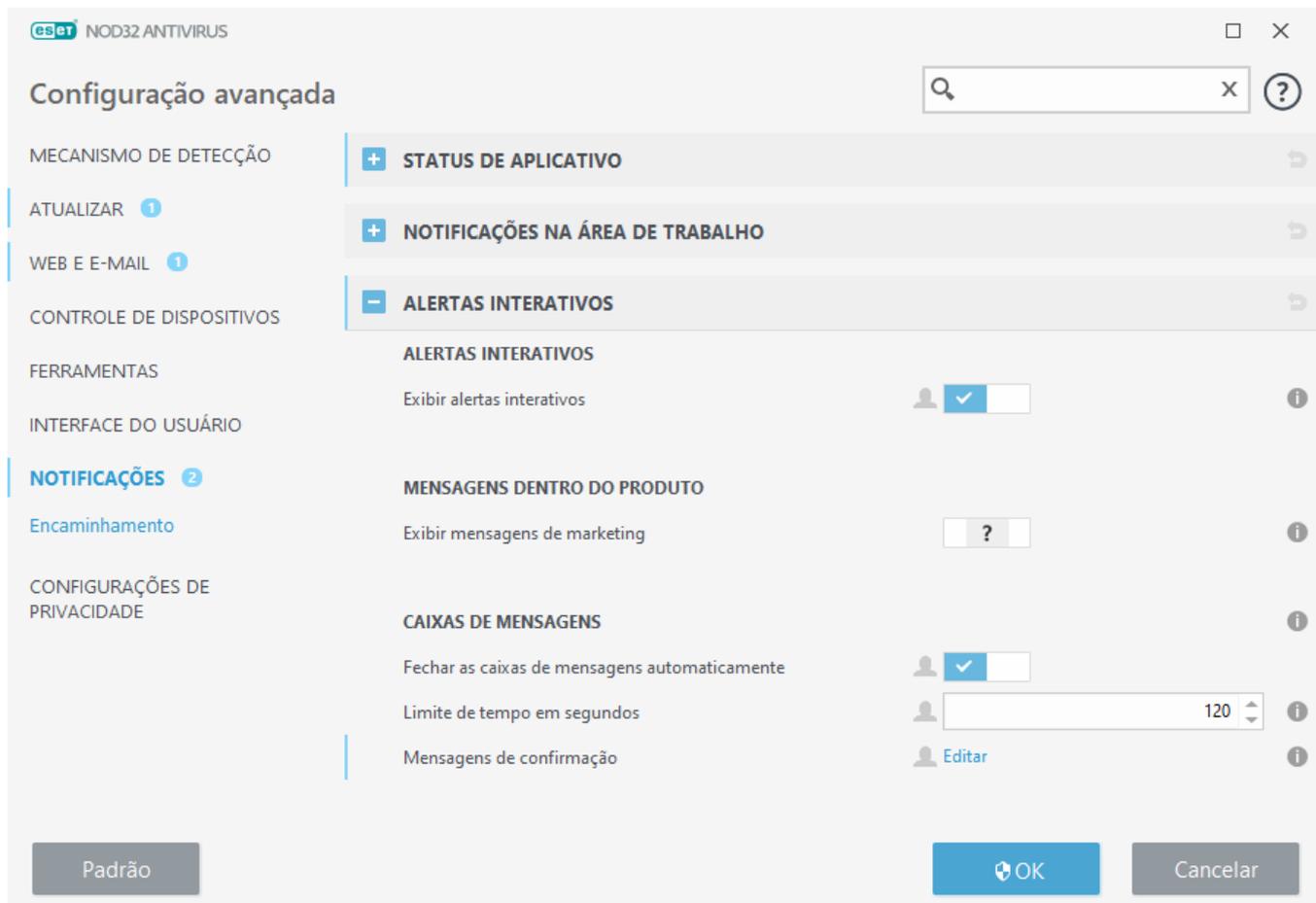
Para definir as configurações feais para Notificações na área de trabalho, por exemplo, por quanto tempo a mensagem será exibida ou o detalhamento mínimo dos eventos a serem exibidos, consulte [Notificações na área de trabalho](#) em **Configuração avançada (F5) > Notificações**.

## Alertas interativos

### Buscando informações sobre alertas e notificações comuns?

- [Ameaça encontrada](#)
- [O endereço foi bloqueado](#)
- [O produto não está ativado](#)
- [Alterar para um produto com mais recursos](#)
- [Mudar para uma linha de produtos mais básica](#)
- [Atualização gratuita disponível](#)
- [As informações de atualização não são consistentes](#)
- [Solução de problemas para a mensagem "Falha na atualização dos módulos"](#)
- [Solucionar erros de atualização dos módulos](#)
- [Certificado de site revogado](#)

A seção **Alertas interativos** em **Configuração avançada (F5) > Notificações** permite que você configure como as caixas de mensagens e alertas interativos para detecções, nas quais um usuário precisa tomar uma decisão (por exemplo, site de phishing em potencial), são tratados pelo ESET NOD32 Antivirus.



## Alertas interativos

Desativar a opção **Exibir alertas interativos** ocultará todas as janelas de alerta e caixas de diálogo no navegador, e é adequado apenas para uma quantidade limitada de situações específicas. A ESET recomenda que essa opção seja mantida com a configuração ativada.

## Mensagens dentro do produto

As mensagens dentro do produto foram feitas para informar os usuários ESET sobre novidades e outras comunicações. Para enviar mensagens de marketing é preciso ter o consentimento de um usuário. Portanto, mensagens de marketing não são enviadas a um usuário por padrão. Ao ativar essa opção você concorda em receber as mensagens de marketing da ESET. Se você não estiver interessado em receber o material de marketing da ESET, desative a opção **Exibir mensagens de marketing**.

## Caixas de mensagens

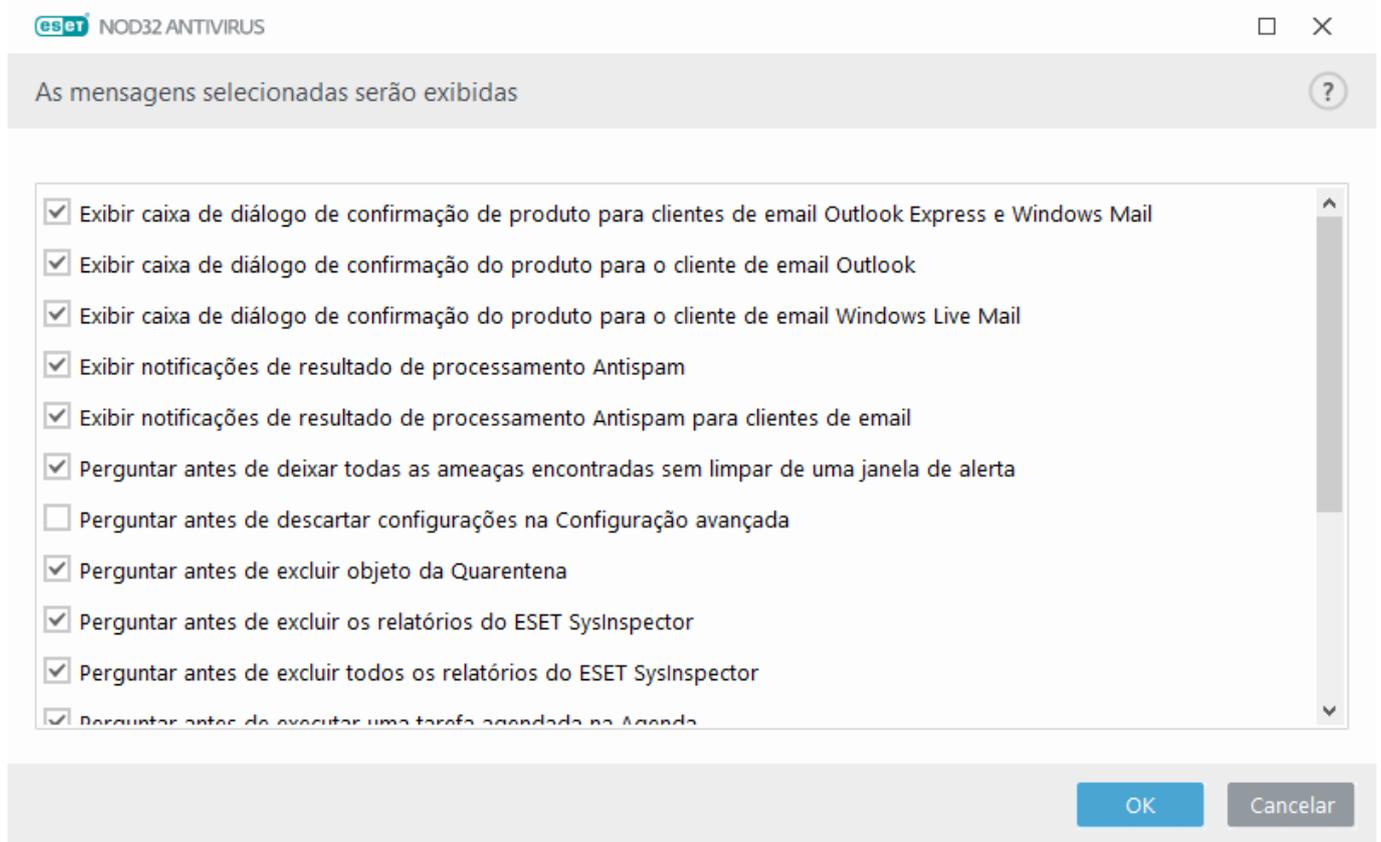
Para fechar as caixas de mensagem automaticamente após um certo tempo, selecione a opção **Fechar caixas de mensagens automaticamente**. Se não forem fechadas manualmente, as janelas de alertas serão fechadas automaticamente após o tempo especificado expirar.

**Limite de tempo em segundos** – define a duração de visibilidade do alerta. O valor deve estar entre 10 a 999 segundos.

**Mensagens de confirmação** – Clique em **Editar** para exibir uma [lista de mensagens de confirmação](#) que você pode selecionar para serem exibidas ou não.

# Mensagens de confirmação

Para ajustar as mensagens de confirmação, navegue para **Configuração avançada (F5) > Notificações > Alertas interativos** e clique em **Editar** ao lado de **Mensagens de confirmação**.



Esta janela de diálogo exibe mensagens de confirmação que o ESET NOD32 Antivirus 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:

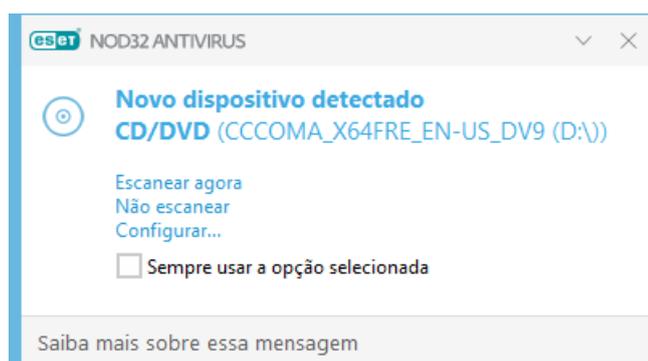
- [Perguntar antes de excluir os relatórios do ESET SysInspector](#)
- [Perguntar antes de excluir todos os relatórios do ESET SysInspector](#)
- [Perguntar antes de excluir objeto da Quarentena](#)
- Perguntar antes de descartar configurações na Configuração avançada
- [Perguntar antes de deixar todas 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 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](#)

## Mídia removível

O ESET NOD32 Antivirus fornece escaneamento automático de mídia removível (CD/DVD/USB/...) no momento da inserção 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 NOD32 Antivirus, 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** – a mídia removível não será escaneada.
- **Configuração** – Abre a seção de **Configuração avançada**.
- **Sempre usar a opção selecionada** - Quando estiver selecionado, a mesma ação será executada quando uma mídia removível for inserida outra vez.

Além disso, o ESET NOD32 Antivirus tem o recurso de Controle de dispositivos, que permite que você defina regras de utilização de 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 para o escaneamento de mídia removível, abra Configuração avançada (F5) > Mecanismo de detecção > Escaneamentos de malware > Mídia removível.

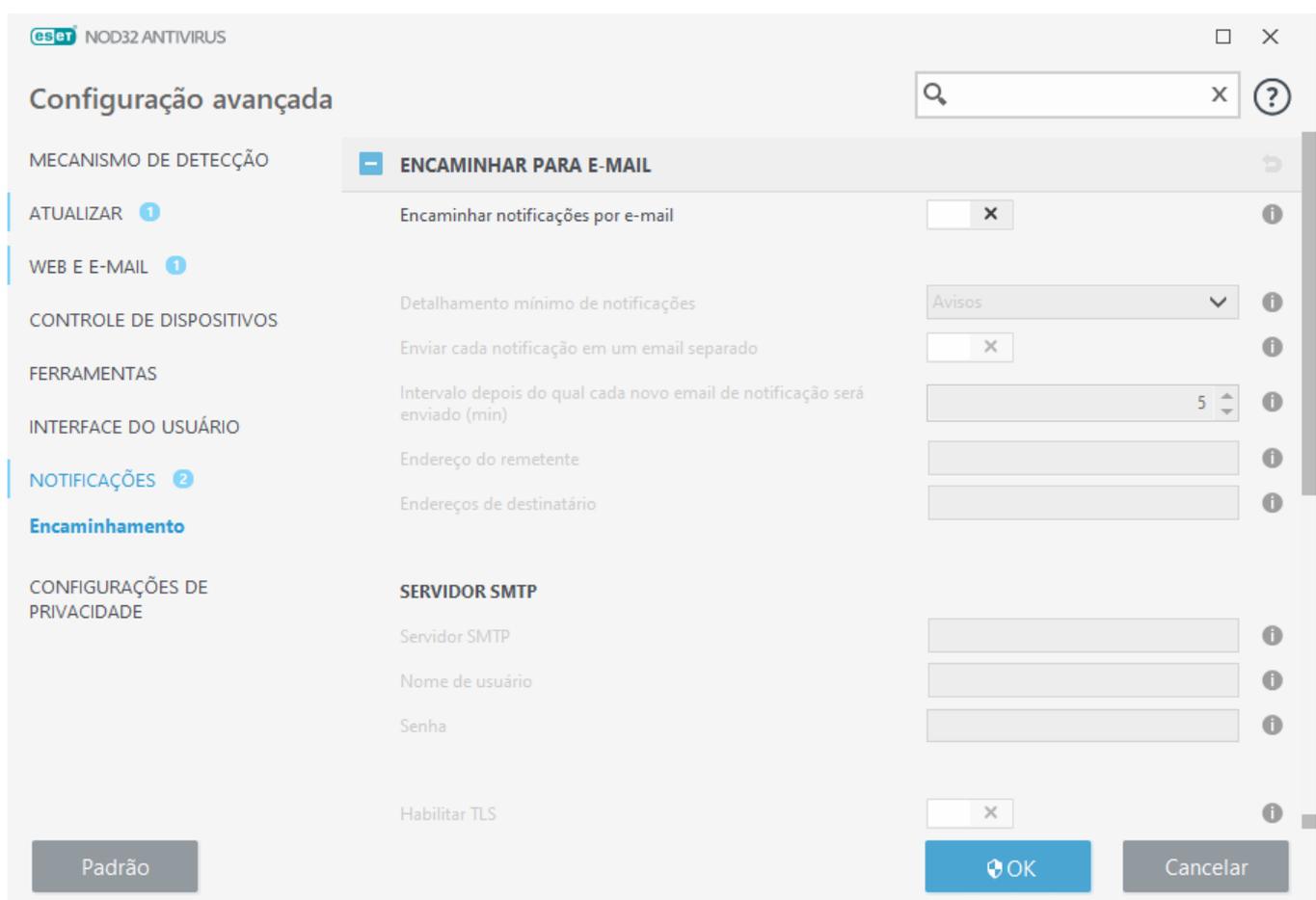
**Ação a ser executada após inserção da mídia removível**– Selecione a ação padrão que será desenvolvida quando

um dispositivo de mídia removível for inserido no computador (CD/DVD/USB). Escolha a ação desejada 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.
- **Exibir opções de rastreamento** - Abre a seção de configuração da **mídia removível**.

## Encaminhamento

O ESET NOD32 Antivirus pode enviar e-mails de notificação automaticamente se um evento com o nível de detalhamento selecionado ocorrer. Abra a **Configuração avançada (F5) > Notificações > Encaminhamento** e ative **Encaminhar notificações por e-mail** para ativar as notificações por e-mail.



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 (por exemplo, Erro ao iniciar a proteção antivírus ou Ameaça encontrada).

**Enviar cada notificação em um e-mail separado** – quando ativado, o destinatário receberá um novo e-mail para cada notificação. Isso pode resultar em muitos e-mails 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.

**Endereço do remetente** - Especifica o endereço do remetente que será exibido no cabeçalho dos emails de notificação.

**Endereços dos destinatários** – define os endereços do destinatário que serão exibidos no cabeçalho dos e-mails de notificação. Vários valores são compatíveis. Use o ponto e vírgula ";" como um separador.

## Servidor SMTP

**Servidor SMTP** – O servidor SMTP usado para enviar notificações (por exemplo smtp.provider.com:587, a porta pré-definida é 25).

**i** os servidores SMTP com criptografia TLS são compatíveis com o ESET NOD32 Antivirus.

**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.

**Ativar TLS** – Secure Alert e notificações usando a criptografia TLS.

**Testar conexão SMTP** – Um e-mail de teste serão enviado ao endereço de e-mail do destinatário. É preciso preencher o servidor SMTP, Nome de usuário, Senha, Endereço do remetente e Endereços de destinatário.

## 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 "?".

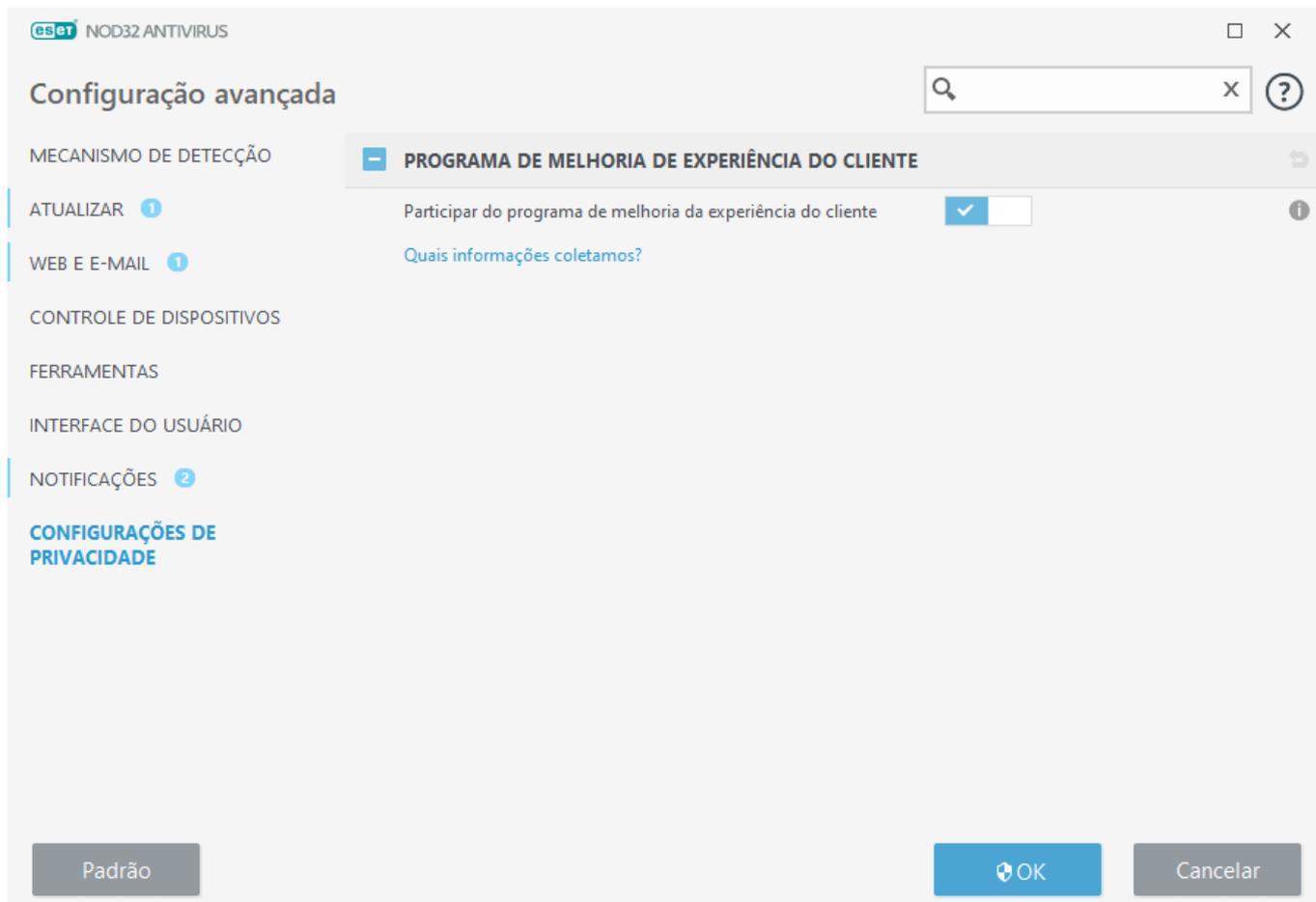
**Usar codificação Quoted-printable** - A origem da mensagem de email será codificada para o formato Quoted-printable (QP) que usa caracteres ASCII e pode transmitir caracteres nacionais especiais por email no formato de 8 bits (áéíóú).

- **%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.

## Configurações de privacidade

Na [janela principal do programa](#), clique em **Configuração > Configuração avançada (F5) > Configurações de privacidade**.



## Programa de melhoria da experiência do cliente

Ative a barra deslizante ao lado de **Participar do Programa de melhoria da experiência do cliente** para entrar no Programa de melhoria da experiência do cliente. Ao entrar, você fornece para a ESET informações anônimas relacionadas ao uso dos produtos ESET. Os dados coletados vão nos ajudar a melhorar sua experiência nunca serão compartilhados com terceiros. [Quais informações coletamos?](#)

## Perfis

O gerenciador de perfil é usado em duas seções no ESET NOD32 Antivirus - **Rastreamento sob demanda do computador** e **Atualizar**.

## Escanear o computador

Há quatro perfis de escaneamento predefinidos no ESET NOD32 Antivirus:

- **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.

**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 **Sempre corrigir detecção**. 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 NOD32 Antivirus, você pode usar os seguintes atalhos de teclado:

Atalhos do teclado	Ação
F1	abre as páginas da Ajuda
F5	abre a Configuração avançada
Seta para cima/Seta para baixo	navegação nos itens de menu suspensos

Atalhos do teclado	Ação
TAB	mover para o próximo elemento da interface gráfica do usuário em uma janela
Shift+TAB	mover para o elemento anterior da interface gráfica do usuário 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
ALT + Seta da esquerda	voltar a navegação
ALT + Seta da direita	avançar a navegação
ALT+Home	navegar para o início

Você também pode usar os botões de mouse para trás ou para a frente para navegação.

## 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 NOD32 Antivirus.

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 o registro em relatório avançado em mensagens de marketing** – registra todos os eventos relacionados a mensagens de marketing dentro do produto.

**Ativar registro em relatório avançado do escaneamento do computador** – registra todos os eventos que acontecem ao escanear arquivos e pastas ao Escanear o computador.

**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 todos os eventos que ocorrem no ESET LiveGrid®. Isto pode ajudar os desenvolvedores a diagnosticar e solucionar problemas relacionados ao ESET LiveGrid®.

**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 o registro em relatório avançado da Proteção do cliente de e-mail** – registra todos os eventos que ocorrem no plugin do cliente de e-mail e no cliente de e-mail para permitir o diagnóstico e a resolução de problemas.

**Ativar registro em relatório avançado de Kernel** – registra todos os eventos que ocorrem no kernel da ESET (ekrn).

**Ativar registro em relatório avançado do mecanismo de Licenciamento** – Registra toda a comunicação do produto com a ativação da ESET ou os servidores ESET License Manager.

**Ativar o escaneamento de memória** – registre todos os eventos que ajudarão os desenvolvedores a diagnosticar vazamentos de memória.

**Ativar o registro em relatório avançado do Sistema operacional** – registre informações adicionais sobre o Sistema operacional como os processos em execução, atividade de CPU e operações de disco. 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 por push.

**Ativar registro em relatório avançado da Proteção em tempo real do sistema de arquivos** – registra todos os eventos que acontecem ao escanear arquivos e pastas na Proteção em tempo real do sistema de arquivos.

**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.

Os arquivos de relatório estão localizados em *C:\ProgramData\ESET\ESET Security\Diagnostics\*.

## Suporte técnico

Ao [entrar em contato com o Suporte Técnico ESET](#) do ESET NOD32 Antivirus, você pode enviar dados de configuração do sistema. Selecione **Sempre enviar** do menu suspenso **Enviar dados de configuração do sistema** para enviar os dados automaticamente, ou selecione **Perguntar antes de enviar** para ser solicitado antes de enviar os dados.

# Importar e exportar configurações

Você pode importar ou exportar seu arquivo de configuração .xml personalizado do ESET NOD32 Antivirus do menu **Configuração**.

## Instruções ilustradas

**i** Veja [Importar ou exportar configurações ESET usando um arquivo .xml](#) para instruções ilustradas disponíveis em inglês e em vários outros idiomas.

A importação e a exportação dos arquivos de configuração serão úteis caso precise fazer backup da configuração atual do ESET NOD32 Antivirus para que ela possa ser utilizada posteriormente. A opção de exportação de configurações também é conveniente quando você quer utilizar as suas configurações preferenciais em vários sistemas. Você pode importar facilmente um arquivo .xml para transferir essas configurações.

Para importar uma configuração, 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.

Para exportar uma configuração, clique na [janela principal do programa](#), clique em **Configurar > Importar/exportar configurações**. Selecione **Exportar configurações** e digite o caminho de arquivo completo com o nome. Clique em ... para navegar para uma localização no seu computador para salvar o arquivo de configuração.

**i** Você pode encontrar um erro ao exportar configurações se não tiver direitos suficientes para gravar o arquivo exportado no diretório especificado.



## 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](#).

## Reverter para configurações 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](#).

## 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.

## Análise da linha de comandos

O módulo antivírus do ESET NOD32 Antivirus 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)
/aind	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	utilizar MODO de limpeza para objetos infectados  As opções disponíveis são: <ul style="list-style-type: none"> <li>• <code>none</code> (padrão) - não ocorrerá nenhuma limpeza automática.</li> <li>• <code>standard</code> - o ecls.exe tentará limpar ou excluir automaticamente os arquivos infectados.</li> <li>• <code>strict</code> (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).</li> <li>• <code>rigorous</code> (rigorosa) - o ecls.exe excluirá arquivos sem tentar limpá-los, independentemente de quais arquivos sejam.</li> <li>• <code>delete</code> (excluir) - o ecls.exe excluirá arquivos sem tentar limpá-los, mas não excluirá arquivos importantes, como arquivos do sistema Windows.</li> </ul>
/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 NOD32 Antivirus 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 NOD32 Antivirus. 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 uma configuração, a pasta de destino deve existir. O comando de exportação ainda funciona quando a configuração do ESET CMD está desligada.

Comando de exportar configurações:  
`ecmd /getcfg c:\config\settings.xml`



Comando importar configurações:  
`ecmd /setcfg c:\config\settings.xml`

**i** Comandos `ecmd` avançados só podem ser executados localmente.

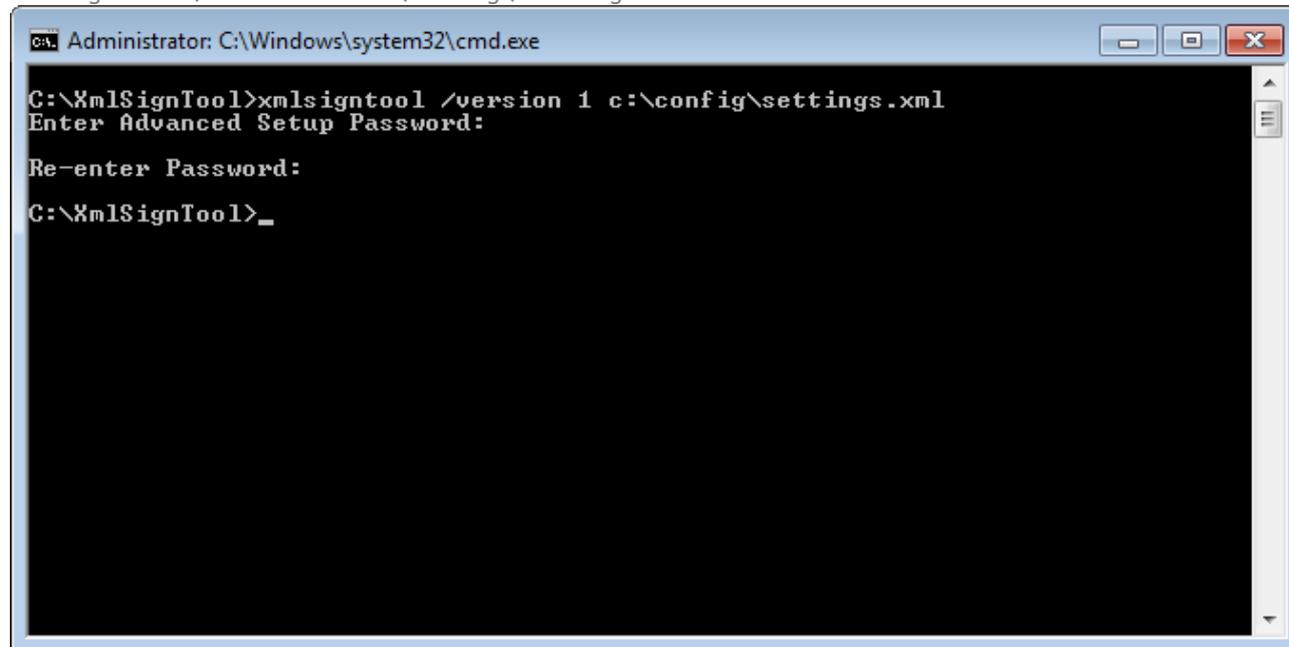
Assinando um arquivo de configuração `.xml`:

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 NOD32 Antivirus. Use o `/version 1` para versões do ESET NOD32 Antivirus anteriores a 11.1. Use o `/version 2` para a versão atual do ESET NOD32 Antivirus.

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 NOD32 Antivirus 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`



```
Administrator: C:\Windows\system32\cmd.exe
C:\XmlSignTool>xmlsigntool /version 1 c:\config\settings.xml
Enter Advanced Setup Password:
Re-enter Password:
C:\XmlSignTool>_
```



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 NOD32 Antivirus 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.

## 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](#):

- Tela desligada ou protetor de tela
- Computador bloqueado
- Logoff de usuário

Use as barras deslizantes de cada estado para ativar ou desativar os diferentes acionadores de detecção de estado ocioso.

# Dúvidas comuns

Você pode encontrar algumas perguntas frequentes e problemas encontrados abaixo. Clique no título do capítulo para descobrir como solucionar o seu problema:

- [Como atualizar o ESET NOD32 Antivirus](#)
- [Como remover um vírus do meu PC](#)
- [Como criar uma nova tarefa na Agenda](#)
- [Como agendar uma tarefa de escaneamento \(semanalmente\)](#)
- [Como desbloquear a Configuração avançada](#)
- [Como resolver a desativação do produto do ESET HOME](#)

Se o seu problema não estiver incluído na lista acima, tente pesquisar na Ajuda on-line do ESET NOD32 Antivirus.

Se você não conseguir encontrar a solução para o seu problema/pergunta na Ajuda on-line do ESET NOD32 Antivirus, poderá acessar nossa [Base de conhecimento ESET](#) on-line, atualizada regularmente. Links para nossos artigos mais populares na Base de conhecimento estão incluídos abaixo:

- [Como renovar minha licença?](#)
- [Recebi um erro de ativação durante a instalação do meu produto ESET. O que isso significa?](#)
- [Ativar meu produto doméstico ESET Windows usando meu Nome de usuário, Senha ou Chave de licença](#)
- [Desinstalar ou reinstalar meu produto doméstico ESET](#)
- [Eu recebo a mensagem de que minha instalação ESET terminou prematuramente](#)
- [O que eu preciso fazer depois de renovar minha licença? \(Usuários Home\)](#)
- [E se eu mudar o meu endereço de email?](#)
- [Transferir meu produto ESET para um novo computador ou dispositivo](#)
- [Como iniciar o Windows em modo de segurança ou Modo de segurança com rede](#)
- [Excluir um site seguro de ser bloqueado](#)
- [Permitir acesso de software de leitura de tela para a interface gráfica do usuário da ESET](#)

Se necessário, você pode [entrar em contato com nosso Suporte técnico](#) com as suas perguntas ou problemas.

## Como atualizar o ESET NOD32 Antivirus

A atualização do ESET NOD32 Antivirus 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. Se precisar alterar o intervalo, acesse **Ferramentas** > [Agenda](#).

## 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 **Rastrear seu computador** 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 verificar se há vírus em apenas uma certa parte do seu disco, clique em **Rastreamento personalizado** e selecione os alvos a serem rastreados em busca de vírus.

Para informações adicionais consulte nosso [artigo na Base de conhecimento ESET](#) atualizado regularmente.

## Como criar uma nova tarefa na Agenda

Para criar uma nova tarefa em **Ferramentas** > **Agenda**, clique em **Adicionar** 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 relatórios** - Os arquivos de relatório 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 (horas)**)

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. Insira um nome para a tarefa e selecione **Escaneamento do computador sob demanda** no menu suspenso **Tipo de tarefa**.
3. Selecione **Semanalmente** como 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 desbloquear a Configuração avançada protegida por senha

Quando você quiser acessar a definição protegida da Configuração avançada, será exibida a janela onde digitar a senha. Se esquecer ou perder sua senha, clique em **Restaurar senha** e insira o endereço de e-mail usado para seu registro de licença. A ESET vai enviar um e-mail com o código de verificação. Digite o código de verificação e escreva e confirme a senha nova. O código de verificação é válido por sete dias.

**Restaurar a senha através da sua conta ESET HOME** – use esta opção se a licença usada para ativação estiver associada à sua conta ESET HOME. Digite o endereço de e-mail que você usa para entrar na sua conta [ESET HOME](#).

Se você não conseguir se lembrar do seu endereço de e-mail ou tiver dificuldades para restaurar a senha, clique em **Entrar em contato com o Suporte técnico**. Você será redirecionado ao site da ESET para entrar em contato com nosso departamento de Suporte técnico.

**Gerar código para Suporte técnico** – Essa opção gera um código para o Suporte técnico. Copie o código fornecido pelo Suporte técnico e clique em **Eu tenho um código de verificação**. Digite o código de verificação e escreva e confirme a nova senha. O código de verificação é válido por sete dias.

Para mais informações, consulte [Desbloquear sua senha de configuração nos produtos domésticos ESET Windows](#).

## Como resolver a desativação do produto do ESET HOME

### O produto não está ativado

Essa mensagem de erro aparece quando o proprietário da licença desativa seu ESET NOD32 Antivirus do portal ESET HOME ou a licença compartilhada com sua conta ESET HOME não é mais compartilhada. Para resolver esse problema:

- Clique em **Ativar** e use um dos [Métodos de ativação](#) para ativar o ESET NOD32 Antivirus.
- Entre em contato com o proprietário da licença com informações que seu ESET NOD32 Antivirus foi desativado pelo proprietário da licença ou a licença não é mais compartilhadas com você. O proprietário pode resolver o problema no [ESET HOME](#).

### Produto desativado, dispositivo desconectado

Esta mensagem de erro aparece após a [remoção de um dispositivo da conta ESET HOME](#). Para resolver esse problema:

- Clique em **Ativar** e use um dos [Métodos de ativação](#) para ativar o ESET NOD32 Antivirus.
- Entre em contato com o proprietário da licença com informações de que seu ESET NOD32 Antivirus foi desativado e que o dispositivo foi desconectado do ESET HOME.
- Se você é o proprietário da licença e não sabe das alterações, revise seu [Feed de atividade do ESET HOME](#). Se você encontrar qualquer atividade suspeita, [altere a senha da conta ESET HOME](#) e entre em contato com o [Suporte técnico ESET](#).

### Produto desativado, dispositivo desconectado

Esta mensagem de erro aparece após a [remoção de um dispositivo da conta ESET HOME](#). Para resolver esse problema:

- Clique em **Ativar** e use um dos [Métodos de ativação](#) para ativar o ESET NOD32 Antivirus.

- Entre em contato com o proprietário da licença com informações de que seu ESET NOD32 Antivirus foi desativado e que o dispositivo foi desconectado do ESET HOME.
- Se você é o proprietário da licença e não sabe das alterações, revise seu [Feed de atividade do ESET HOME](#). Se você encontrar qualquer atividade suspeita, [altere a senha da conta ESET HOME](#) e entre em contato com o [Suporte técnico ESET](#).

## O produto não está ativado

Essa mensagem de erro aparece quando o proprietário da licença desativa seu ESET NOD32 Antivirus do portal ESET HOME ou a licença compartilhada com sua conta ESET HOME não é mais compartilhada. Para resolver esse problema:

- Clique em **Ativar** e use um dos [Métodos de ativação](#) para ativar o ESET NOD32 Antivirus.
- Entre em contato com o proprietário da licença com informações que seu ESET NOD32 Antivirus foi desativado pelo proprietário da licença ou a licença não é mais compartilhadas com você. O proprietário pode resolver o problema no [ESET HOME](#).

## Programa de melhoria da experiência do cliente

Ao participar do Programa de melhoria da experiência do cliente, você fornece para a ESET informações anônimas relacionadas ao uso dos nossos produtos. Mais informações sobre o processamento de dados estão disponíveis em nossa Política de privacidade.

### Seu consentimento

A participação no Programa é voluntária e baseada no seu consentimento. Depois de entrar no programa sua participação será passiva, o que significa que você não precisará realizar mais nenhuma ação. Você pode revogar seu consentimento a qualquer momento, ao alterar as configurações do produto. Fazer isso vai nos impedir de continuar processando seus dados anônimos.

Você pode revogar seu consentimento a qualquer momento, ao alterar as configurações do produto:

- [Alterar as configurações do Programa de melhoria da experiência do cliente nos produtos domésticos ESET Windows](#)

## Quais tipos de informações coletamos?

### Dados sobre a interação com o produto

Essas informações nos falam mais sobre como nossos produtos são usados. Graças a isso sabemos, por exemplo, quais funcionalidades são usadas com frequência, quais configurações são modificadas pelo usuário e quanto tempo eles passam usando o produto.

### Dados sobre os dispositivos

Coletamos essas informações para entendermos onde e em quais dispositivos nossos produtos são usados. Exemplos típicos são o modelo do dispositivo, país, versão e nome do sistema operacional.

## Dados de diagnóstico de erro

Informações sobre erros e situações de parada também são coletados. Por exemplo, qual erro ocorreu e quais ações levaram até ele.

## Por que coletamos essas informações?

Com essas informações anônimas podemos melhorar nossos produtos para você, nosso usuário. Elas nos ajudam a ser o mais relevante, fácil de usar e livre de problemas possível.

## Quem controla essas informações?

ESET, spol. s r.o. é o único controlador de dados coletados no Programa. Essa informação não é compartilhada com terceiros.

# 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\\_home](https://go.eset.com/eol_home). 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 automaticamente 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 contrário.

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.

## **ADENDO AO CONTRATO**

**Avaliação de segurança de dispositivos conectados na rede.** Provisões adicionais são aplicáveis à Avaliação de segurança de dispositivos conectados na rede da seguinte forma:

O Software contém uma função para verificar a segurança da rede local do Usuário Final e a segurança dos dispositivos em uma rede local, que requer o nome da rede local e informações sobre dispositivos na rede local como presença, tipo, nome, endereço IP e endereço AC do dispositivo na rede local, em conexão com informações de licença. As informações também incluem tipo de segurança sem fio e tipo de criptografia sem fio para dispositivos roteadores. Essa função também pode fornecer informações sobre a disponibilidade de soluções de software de segurança para dispositivos seguros na rede local.

**Proteção contra o uso errôneo de dados.** Provisões adicionais são aplicáveis à Proteção contra o uso errôneo de dados da seguinte forma:

O Software contém uma função que impede a perda ou uso errôneo de dados crítico em conexão direta com o furto de um Computador. Essa função é desligada sob as configurações padrão do Software. A Conta ESET HOME precisa ser criada para que isso seja ativado, e através disso a função ativa a coleta de dados no caso de furto do computador. Se você escolher ativar essa função do Software, os dados sobre o Computador furtado serão coletados e enviados ao Provedor, que pode incluir dados sobre a localização de rede do computador, dados sobre o conteúdo exibido na tela do Computador, dados sobre a configuração do Computador e/ou dados registrados por uma câmera conectada ao Computador (doravante denominado "Dados"). O Usuário Final terá o direito de usar os Dados obtidos por essa função e fornecidos através da Conta ESET HOME exclusivamente para retificar uma situação adversa causada pelo furto de um Computador. Apenas para os fins desta função, o Provedor processa os Dados conforme especificado na Política de Privacidade e de acordo com os regulamentos legais relevantes. O Provedor deve permitir que o Usuário Final acesse os Dados pelo período necessário para alcançar o objetivo pelo qual os dados foram obtidos, que não deve ultrapassar o período de retenção especificado na Política de Privacidade. A proteção contra o uso errôneo de dados deve ser usada exclusivamente com Computadores e contas aos quais o Usuário Final tenha acesso legítimo. Qualquer uso ilegal será reportado à autoridade competente. O Provedor cumprirá as leis relevantes e auxiliará autoridades de execução da lei no caso de uso errôneo. Você concorda e reconhece que é responsável pela proteção da senha de acesso da Conta ESET HOME e concorda que não revelará sua senha para nenhum terceiro. O Usuário Final é responsável por qualquer atividade usando a função de Proteção Contra Uso Indevido de Dados e a Conta ESET HOME, de forma autorizada ou não. Se a Conta ESET HOME for comprometida, notifique o Provedor imediatamente. Provisões adicionais são

aplicáveis à Proteção Contra Uso Errôneo de Dados exclusivamente para Usuários Finais do ESET Internet Security e ESET Smart Security Premium.

**ESET Secure Data.** Provisões adicionais são aplicáveis ao ESET Secure Data da seguinte forma:

1. Definições. Nessas provisões adicionais do ESET Secure Data as palavras a seguir têm os significados correspondentes:

- a) “Informações” qualquer informação ou dados criptografados ou descriptografados usando o software;
- b) “Produtos” o software ESET Secure Data e a documentação;
- c) “ESET Secure Data” o software(s) usado para criptografar e descriptografar dados eletrônicos;

Todas as referências para o plural incluem o singular e todas as referências para o masculino incluem o feminino e neutro e vice-versa. Palavras sem definição específica serão usadas de acordo com as definições estipuladas no Contrato.

2. Declaração adicional do Usuário Final. Você reconhece e aceita que:

- a) é sua responsabilidade proteger, manter e fazer back-up das Informações;
- b) você deve fazer back-up completo de todas as informações e dados (incluindo sem limitação quaisquer informações e dados críticos) no seu computador antes da instalação do ESET Secure Data;
- c) Você deve manter um registro seguro de quaisquer senhas ou outras informações utilizadas para configurar e usar o ESET Secure Data, você também deve fazer back-up de todas as chaves de criptografia, códigos de licença, arquivos chave e outros dados gerados em meios de armazenamento separados;
- d) Você é responsável pelo uso dos Produtos. O Provedor não será responsável por qualquer perda, reclamação ou danos sofridos em consequência de qualquer criptografia ou descriptografia não autorizada ou equivocada de Informações ou dados onde e como essas Informações ou dados forem armazenados;
- e) Enquanto o Provedor tomou todas as medidas razoáveis para garantir a integridade e segurança do ESET Secure Data, os Produtos (ou qualquer um deles) não devem ser usados em qualquer área que dependa de um nível de segurança à prova de falhas ou que seja potencialmente perigosa, incluindo, sem limitação, instalações nucleares, navegação de aeronaves, sistemas de controle ou comunicação, sistemas de armas e de defesa e sistemas de apoio à vida ou monitoramento de vida;
- f) É responsabilidade do Usuário Final garantir que o nível de segurança e criptografia fornecida pelos produtos seja adequado para suas necessidades;
- g) Você é responsável por seu uso dos Produtos, incluindo, sem limitação, por garantir que esse uso está em conformidade com todas as leis e regulamentos da República Eslovaca ou de qualquer outro país, região ou estado aplicáveis onde o Produto é utilizado. Você deve garantir que, antes de qualquer uso dos Produtos, você garantiu que tal uso não está violando qualquer embargo governamental (na República Eslovaca ou outro local);
- h) O ESET Secure Data pode entrar em contato com os servidores do Provedor de vez em quando, para verificar informações de licença, patches disponíveis, pacotes de serviço e outras atualizações que podem melhorar, manter, modificar ou melhorar o funcionamento do ESET Secure Data e ele poderá enviar informações gerais do sistema relacionadas ao funcionamento de acordo com a Política de Privacidade.
- i) O Provedor não será responsável por qualquer perda, dano, despesa ou reclamação resultante da perda, roubo, uso indevido, corrupção, dano ou destruição de senhas, informações de configuração, chaves de criptografia,

códigos de ativação de licença e outros dados gerados ou armazenados durante o uso do software.

Provisões adicionais são aplicáveis ao ESET Secure Data exclusivamente para Usuários Finais ESET Smart Security Premium.

**Password Manager Software.** Provisões adicionais são aplicáveis ao Software do Password Manager da seguinte forma:

1. Declaração adicional do Usuário Final. Você reconhece e aceita que Você não pode:

a) usar o Software Password Manager para operar qualquer aplicativo de missão crítica onde a vida humana ou bens possam estar em jogo. Você entende que o Software Password Manager não é feito para tais fins e que sua falha em tais casos pode levar à morte, ferimentos pessoais ou danos materiais ou ambientais graves pelos quais o Provedor não é responsável.

O SOFTWARE PASSWORD MANAGER NÃO FOI PROJETADO, PRETENDIDO OU AUTORIZADO PARA USO EM AMBIENTES PERIGOSOS QUE EXIJAM CONTROLES À PROVA DE FALHAS INCLUINDO, SEM LIMITAÇÃO, O PROJETO, CONSTRUÇÃO, MANUTENÇÃO OU OPERAÇÃO DE INSTALAÇÕES NUCLEARES, NAVEGAÇÃO AÉREA OU SISTEMAS DE COMUNICAÇÃO, CONTROLE DE TRÁFEGO AÉREO E SUPORTE A VIDA OU SISTEMAS DE ARMAS. O PROVEDOR RENUNCIA ESPECIFICAMENTE QUALQUER GARANTIA EXPRESSA OU IMPLÍCITA DE ADEQUAÇÃO PARA TAIS FINS.

b) Usar o Software Password Manager de forma contrária a este contrato ou às leis da República Eslovaca ou sua jurisdição. Especificamente, você não pode usar o Software Password Manager para realizar ou promover quaisquer atividades ilegais, incluindo o carregamento de dados de conteúdo nocivo ou conteúdo que pode ser usado para quaisquer atividades ilegais ou que de alguma forma viola a lei ou os direitos de terceiros (incluindo qualquer direito de propriedade intelectual), incluindo mas não limitado a quaisquer tentativas de obter acesso a contas no Depósito (para os fins destes termos adicionais do Software Password Manager, "Depósito" significa o espaço de armazenamento de dados gerenciado pelo Provedor ou por um terceiro que não seja o Provedor e o usuário para fins de ativar a sincronização e backup dos dados do usuário) ou quaisquer contas e dados de outros usuários do Software Password Manager ou Depósito. Se você violar qualquer uma destas disposições, o Provedor tem o direito de rescindir imediatamente este acordo e transferir a Você o custo de qualquer recurso necessário, assim como tomar as medidas necessárias para impedir a continuação do uso do Software Password Manager sem a possibilidade de reembolso.

2. LIMITAÇÃO DE RESPONSABILIDADE. O SOFTWARE PASSWORD MANAGER É FORNECIDO "COMO ESTÁ". NENHUMA GARANTIA DE QUALQUER TIPO É EXPRESSA OU IMPLÍCITA. VOCÊ USA O SOFTWARE POR SUA CONTA E RISCO. O PRODUTOR NÃO É RESPONSÁVEL POR PERDA DE DADOS, DANOS, LIMITAÇÃO DE DISPONIBILIDADE DO SERVIÇO, INCLUINDO QUAISQUER DADOS ENVIADOS ATRAVÉS DO SOFTWARE PASSWORD MANAGER PARA ARMAZENAMENTO EXTERNO PARA OS FINS DE SINCRONIZAÇÃO E BACKUP DE DADOS. CRIPTOGRAFAR OS DADOS USANDO O SOFTWARE PASSWORD MANAGER NÃO IMPLICA EM QUALQUER RESPONSABILIDADE DO PROVEDOR EM RELAÇÃO À SEGURANÇA DE TAIS DADOS. VOCÊ CONCORDA EXPRESSAMENTE QUE OS DADOS ADQUIRIDOS, USADOS, CRIPTOGRAFADOS, ARMAZENADOS, SINCRONIZADOS OU ENVIADOS COM O SOFTWARE PASSWORD MANAGER TAMBÉM PODEM SER ARMAZENADOS EM SERVIDORES DE TERCEIROS (APLICÁVEL APENAS AO USO DO SOFTWARE PASSWORD MANAGER ONDE OS SERVIÇOS DE SINCRONIZAÇÃO E BACKUP FORAM ATIVADOS). SE O PROVEDOR A SEU CRITÉRIO EXCLUSIVO ESCOLHER USAR TAL ARMAZENAMENTO, SITE, PORTAL DA WEB, SERVIDOR OU SERVIÇO DE TERCEIROS, O PROVEDOR NÃO É RESPONSÁVEL PELA QUALIDADE, SEGURANÇA OU DISPONIBILIDADE DE TAL SERVIÇO DE TERCEIROS E EM NENHUM MOMENTO O FORNECEDOR É RESPONSÁVEL PERANTE A VOCÊ POR QUALQUER VIOLAÇÃO DAS OBRIGAÇÕES CONTRATUAIS OU JURÍDICAS POR TERCEIROS NEM POR DANOS, PERDA DE LUCROS, DANOS FINANCEIROS OU NÃO-FINANCEIROS, OU QUALQUER OUTRO TIPO DE PERDA AO USAR ESTE SOFTWARE. O PROVEDOR NÃO É RESPONSÁVEL PELO CONTEÚDO DE QUALQUER DADO ADQUIRIDO, USADO, CRIPTOGRAFADO, ARMAZENADO, SINCRONIZADO OU ENVIADO USANDO O SOFTWARE PASSWORD MANAGER OU NO DEPÓSITO. VOCÊ RECONHECE QUE O PROVEDOR NÃO TEM ACESSO AO CONTEÚDO DOS DADOS ARMAZENADOS E NÃO É CAPAZ DE MONITORÁ-LO OU REMOVER LEGALMENTE

QUALQUER CONTEÚDO NOCIVO.

O Provedor detém todos os direitos a melhorias, atualizações e dificuldades relacionadas ao Software Password Manager (“Melhorias”), mesmo no caso de tais melhorias terem sido criadas com base no feedback, ideias ou sugestões enviadas por você de qualquer forma. Você não terá direito a qualquer compensação, incluindo quaisquer direitos autorais relativos a tais Melhorias.

ENTIDADES E LICENCIADOS DO PROVEDOR NÃO SERÃO RESPONSÁVEIS POR RECLAMAÇÕES E RESPONSABILIDADES DE QUALQUER TIPO DECORRENTES DE OU DE QUALQUER FORMA RELACIONADAS AO USO DO SOFTWARE PASSWORD MANAGER POR VOCÊ OU POR TERCEIROS, AO USO OU NÃO USO DE QUALQUER CORRETORA OU REVENDEDOR, OU À COMPRA OU VENDA DE QUALQUER TÍTULO, SENDO TAIS RECLAMAÇÕES E RESPONSABILIDADES BASEADAS EM QUALQUER TEORIA LEGAL OU EQUIVALENTE.

ENTIDADES E LICENCIADOS DO PROVEDOR NÃO SÃO RESPONSÁVEIS POR TODO E QUALQUER DANO DIRETO, ACIDENTAL, ESPECIAL, INDIRETO OU RESULTANTE SURGINDO DE OU RELACIONADO A QUALQUER SOFTWARE DE TERCEIROS, QUAISQUER DADOS ACESSADOS ATRAVÉS DO SOFTWARE PASSWORD MANAGER, SEU USO OU INCAPACIDADE DE USAR OU ACESSAR O SOFTWARE PASSWORD MANAGER OU QUAISQUER DADOS FORNECIDOS ATRAVÉS DO SOFTWARE PASSWORD MANAGER, SENDO TAIS RECLAMAÇÕES DE DANOS CRIADAS SOB QUALQUER TEORIA DE LEI OU EQUIDADE. DANOS EXCLUÍDOS POR ESTA CLÁUSULA INCLUEM, SEM LIMITAÇÃO, AQUELES POR PERDA DE LUCROS, DANO A PESSOA OU PROPRIEDADE, INTERRUPÇÃO DE NEGÓCIOS, PERDA DE NEGÓCIOS OU INFORMAÇÕES PESSOAIS. ALGUMAS JURISDIÇÕES NÃO PERMITEM A LIMITAÇÃO DE DANOS INCIDENTAIS OU EMERGENTES PORTANTO ESTA RESTRIÇÃO PODE NÃO SE APLICAR A VOCÊ. NESSE CASO, A EXTENSÃO DA RESPONSABILIDADE DO PROVEDOR SERÁ O MÍNIMO PERMITIDO PELA LEGISLAÇÃO APLICÁVEL.

INFORMAÇÕES FORNECIDAS ATRAVÉS DO SOFTWARE PASSWORD MANAGER, INCLUINDO COTAÇÕES DE AÇÕES, ANÁLISE, INFORMAÇÕES DE MERCADO, NOTÍCIAS E DADOS FINANCEIROS, PODEM SER ATRASADOS, IMPRECIOSOS OU CONTER ERROS OU OMISSÕES, E ENTIDADES E LICENCIADOS DO PROVEDOR NÃO TERÃO RESPONSABILIDADE SOBRE ISSO. O PROVEDOR PODE ALTERAR OU INTERROMPER QUALQUER ASPECTO OU RECURSO DO SOFTWARE PASSWORD MANAGER OU O USO DE TODO E QUALQUER RECURSO OU TECNOLOGIA NO SOFTWARE PASSWORD MANAGER A QUALQUER MOMENTO, SEM AVISO PRÉVIO AO USUÁRIO.

SE AS DISPOSIÇÕES NESTE ARTIGO FOREM ANULADAS POR QUALQUER MOTIVO OU SE O PROVEDOR FOR CONSIDERADO RESPONSÁVEL POR PERDAS, DANOS ETC. DE ACORDO COM LEIS APLICÁVEIS, AS PARTES CONCORDAM QUE A RESPONSABILIDADE DO PROVEDOR PERANTE A VOCÊ SERÁ LIMITADA AO VALOR TOTAL DAS TAXAS DE LICENÇA PAGAS POR VOCÊ.

VOCÊ CONCORDA EM INDENIZAR, DEFENDER E ISENTAR DE RESPONSABILIDADE O PROVEDOR E SEUS FUNCIONÁRIOS, SUBSIDIÁRIAS, AFILIADAS, REPOSICIONAMENTO DE MARCA E OUTROS PARCEIROS DE E CONTRA TODA E QUALQUER REIVINDICAÇÃO, RESPONSABILIDADE, DANOS, PERDAS, CUSTOS, DESPESAS, TAXAS DE TERCEIROS (INCLUINDO OS PROPRIETÁRIOS DO DISPOSITIVO OU PARTES CUJOS DIREITOS FORAM AFETADOS PELOS DADOS USADOS NO SOFTWARE PASSWORD MANAGER OU DEPÓSITO) QUE TAIS PARTES POSSAM INCORRER COMO RESULTADO DO SEU USO DO SOFTWARE PASSWORD MANAGER.

3. Dados no Software Password Manager. A menos que declarado em contrário, e explicitamente selecionado por você, todos os dados inseridos por você que são salvos em um banco de dados do Software Password Manager são armazenados em formato criptografado no seu computador, ou outro dispositivo de armazenamento, conforme definido por você. Você entende que, no caso de exclusão de, ou dano a, qualquer banco de dados no Software Password Manager ou outros arquivos, todos os dados contidos nele serão irreversivelmente perdidos e você entende e aceita o risco de tal perda. O fato de que seus dados pessoais são armazenados em formato criptografado no computador não significa que as informações não podem ser roubadas ou usadas erroneamente por alguém que descubra a Senha mestre ou ganhe acesso ao dispositivo de ativação definido pelo cliente para abrir o banco de dados. Você é responsável por manter a segurança de todos os métodos de acesso.

4. Transmissão de dados pessoais ao Provedor ou Depósito. Se você selecionar isso e apenas com o objetivo de garantir a sincronização de dados e backup em tempo útil, o Software Password Manager transmite ou envia dados pessoais do banco de dados do Software Password Manager - ou seja, senhas, informações de login, Contas e Identidades - através da Internet para o Depósito. Os dados são transmitidos exclusivamente criptografados. O uso do Software Password Manager para o preenchimento de formulários on-line com senhas, logins e outros dados pode exigir que a informação seja enviada através da Internet para o site identificado por você. Esta transmissão de dados não é iniciada pelo Software Password Manager e, portanto, o Provedor não pode ser responsabilizado pela segurança de tais interações com qualquer site compatível com vários provedores. Quaisquer transações pela Internet, sendo ou não em conjunto com o Software Password Manager, são feitas por sua própria conta e risco, e você será o único responsável por qualquer dano ao seu sistema de computadores ou perda de dados resultantes da transferência e/ou uso de tal material ou serviço. Para minimizar o risco de perder dados valiosos, o Provedor recomenda que os clientes executem backup periódico do banco de dados e outros arquivos sensíveis em unidades externas. O Provedor não pode fornecer a você nenhuma assistência na recuperação de dados perdidos ou danificados. Se o Provedor fornece serviços de backup de arquivos de banco de dados do usuário em caso de dano ou exclusão dos arquivos nos PCs dos usuários, tal serviço de backup é feito sem qualquer garantia e não implica em qualquer responsabilidade do Provedor a você.

Ao usar o Software Password Manager, você concorda que o software pode entrar em contato com os servidores do Provedor de vez em quando, para verificar informações de licença, patches disponíveis, pacotes de serviço e outras atualizações que podem melhorar, manter, modificar ou melhorar o funcionamento do Software Password Manager. O software poderá enviar informações gerais do sistema relacionadas ao funcionamento do Software Password Manager.

5. Informações e instruções de desinstalação. Qualquer informação que você gostaria de manter no banco de dados deve ser exportada antes de desinstalar o Software Password Manager.

Provisões adicionais são aplicáveis ao Software Password Manager exclusivamente para Usuários Finais do ESET Smart Security Premium.

**ESET LiveGuard.** Provisões adicionais são aplicáveis ao ESET LiveGuard da seguinte forma:

O Software contém uma função de análise adicional dos arquivos enviados pelo Usuário Final. O Provedor deverá usar apenas os arquivos enviados pelo Usuário Final e os resultados da análise de acordo com a Política de Privacidade e de acordo com os regulamentos legais relevantes.

Provisões adicionais são aplicáveis ao ESET LiveGuard exclusivamente para Usuários Finais ESET Smart Security Premium.

EULAID: EULA-PRODUCT-LG-EHSW; 3537.0

## Política de Privacidade

A proteção de dados pessoais é de importância particular para a ESET, spol. s r. o., com sede em Einsteinova 24, 851 01 Bratislava, Slovak Republic, registrada no Registro Comercial administrado pela Corte Distrital Bratislava I, Seção Sro, Registro Nº. 3586/B, Número de Registro Comercial: 31333532 como um Responsável pelo Tratamento de Dados ("ESET" ou "Nós"). Queremos cumprir com o requisito de transparência conforme legalmente protegido pelo Regulamento Geral de Proteção de Dados ("RGPD") da UE. Para isso, estamos publicando essa Política de Privacidade com o objetivo exclusivo de informar nosso cliente ("Usuário Final" ou "Você") como titular dos dados sobre os tópicos de dados pessoais a seguir:

- Base jurídica do tratamento de dados pessoais,

- Compartilhamento de dados e confidencialidade,
- Segurança de dados,
- Seus direitos como titular dos dados,
- Tratamento de seus Dados pessoais
- Informações de contato.

## Base jurídica do tratamento de dados pessoais

Existem apenas algumas bases jurídicas para o tratamento de dados que Nós usamos de acordo com a estrutura legislativa aplicável relacionada à proteção de dados pessoais. O tratamento de dados pessoais na ESET é principalmente necessário para o desempenho do [Acordo de Licença para o usuário final](#) ("EULA") com o Usuário Final (Art. 6 (1) (b) LGPD), que é aplicável para o fornecimento de produtos ou serviços ESET, a menos que explicitamente declarado o contrário, por exemplo:

- Base jurídica de interesse legítimo (Art. 6 (1) (f) LGPD), que nos permite processar dados sobre como nossos clientes usam nossos Serviços e sua satisfação para fornecer aos nossos usuários a melhor proteção, suporte e experiência que podemos oferecer. Mesmo o marketing é reconhecido pela legislação aplicável como um interesse legítimo, portanto normalmente contamos com isso para a comunicação de marketing com nossos clientes.
- Consentimento (Art. 6 (1) (a) LGPD), que podemos solicitar de Você em situações específicas quando consideramos essa base jurídica como a mais adequada ou se for exigido por lei.
- Conformidade com obrigações legais (Art. 6 (1) (c) LGPD), por exemplo estipulando requisitos para comunicação eletrônica, retenção para faturamento ou documentos de cobrança.

## Compartilhamento de dados e confidencialidade

Não compartilhamos seus dados com terceiros. Porém, a ESET é uma empresa que opera no mundo todo através de empresas afiliadas ou parceiros como parte de nossa rede de vendas, serviço e suporte. Informações de licenciamento, cobrança e suporte técnico processadas pela ESET podem ser transferidas de e para afiliadas ou parceiros com o objetivo de cumprir com o Acordo de Licença para o Usuário Final, como o fornecimento de serviços ou suporte.

A ESET prefere processar seus dados na União Europeia (UE). Porém, dependendo de sua localização (uso de nossos produtos e/ou serviços fora da UE) e/ou do serviço escolhido por você, pode ser necessário transferir seus dados para um país fora da UE. Por exemplo, usamos serviços de terceiros em conexão com a computação em nuvem. Nesses casos, selecionamos cuidadosamente nossos provedores de serviço e garantimos um nível apropriado de proteção de dados através de medidas contratuais, técnicas e organizacionais. Como regra, concordamos com as cláusulas contratuais padrão da UE, se necessário, com regulamentos contratuais suplementares.

Para alguns países fora da UE, como o Reino Unido e Suíça, a UE já determinou um nível de proteção de dados comparável. Devido ao nível comparável de proteção de dados, a transferência de dados para esses países não requer qualquer autorização ou acordo especial.

## Segurança de dados

A ESET implementa medidas técnicas e organizacionais adequadas para garantir um nível de segurança que seja apropriado para os riscos potenciais. Estamos fazendo nosso melhor para garantir a confidencialidade, integridade, disponibilidade e resiliência constante de sistemas de processamento e serviços. Porém, em caso de violação de dados resultando em um risco aos seus direitos e liberdades, estamos prontos para notificar uma autoridade supervisora relevante, assim como os Usuários Finais afetados como titulares dos dados.

## Direitos do sujeito dos dados

Os direitos de todos os Usuários Finais são importantes e gostaríamos de informar que todos os Usuários Finais (de qualquer país da UE ou que não da UE) têm os seguintes direitos garantidos na ESET. Para exercer seus direitos de titular dos dados, você pode entrar em contato conosco através do formulário de suporte ou por e-mail em [dpo@eset.sk](mailto:dpo@eset.sk). Para fins de identificação, pedimos as informações a seguir: Nome, endereço de e-mail e, se disponível, chave de licença ou número do cliente e filiação da empresa. Não envie nenhum outro dado pessoal, como a data de nascimento. Destacamos que, para ser capaz de processar sua solicitação, assim como para fins de identificação, vamos processar seus dados pessoais.

**Direito de retirar o consentimento.** O direito de retirar o consentimento é aplicável no caso de tratamento baseado apenas no consentimento. Se processarmos seus dados pessoais com base em seu consentimento, você tem o direito de retirar o consentimento a qualquer momento sem dar motivos. A retirada do seu consentimento só é eficaz para o futuro e não afeta a legalidade dos dados processados antes da retirada.

**Direito a uma objeção.** O direito de objeção ao tratamento é aplicável no caso de tratamento com base no interesse legítimo da ESET ou de terceiros. Se tratarmos seus dados pessoais para proteger um interesse legítimo, Você como o titular dos dados tem o direito de objeção aos interesses legítimos nomeados por Nós e ao tratamento de seus dados pessoais a qualquer momento. Sua objeção só é eficaz para o futuro e não afeta a legalidade dos dados processados antes da objeção. Se processarmos seus dados pessoais para fins de marketing direto, não é necessário dar motivos para sua objeção. Isso também se aplica a criação de perfis, na medida em que está conectado a tal marketing direto. Em todos os outros casos, solicitamos que você nos informe brevemente sobre suas queixas contra o interesse legítimo da ESET para tratar seus dados pessoais.

Observe que, em alguns casos, apesar de sua retirada de consentimento, temos o direito de continuar com o tratamento de seus dados pessoais com base em outra base jurídica, por exemplo, para a execução de um contrato.

**Direito de acesso.** Como um titular dos dados, você tem o direito de obter informações sobre seus dados armazenados pela ESET gratuitamente a qualquer momento.

**Direito a retificação.** Se inadvertidamente tratarmos dados pessoais incorretos sobre você, você tem o direito de corrigir isso.

**Direito a exclusão e direito a restrição do tratamento.** Como um titular dos dados, você tem o direito de solicitar a exclusão ou restrição do tratamento de seus dados pessoais. Se tratarmos seus dados pessoais, por exemplo, com seu consentimento, você retirará esse consentimento e se não houver outra base jurídica, por exemplo, um contrato, removeremos seus dados pessoais imediatamente. Seus dados pessoais também serão removidos assim que não forem mais necessários para os fins declarados para eles no final do nosso período de retenção.

Se usarmos seus dados pessoais com o objetivo exclusivo de marketing direto e você tiver revogado seu consentimento ou feito uma objeção ao interesse legítimo subjacente da ESET, restringiremos o tratamento de seus dados pessoais na medida em que incluirmos seus dados de contato em nossa lista de proibições interna para evitar contato não solicitado. Caso contrário, seus dados pessoais serão removidos.

Note que Nós podemos ser obrigados a armazenar seus dados até a expiração das obrigações de retenção e períodos emitidos pelas autoridades legisladoras ou supervisoras. Obrigações e períodos de retenção também podem ser resultado da legislação eslovaca. Depois disso, os dados correspondentes serão removidos rotineiramente.

**Direito à portabilidade de dados.** Será um prazer fornecer a Você, como um titular dos dados, os dados pessoais processados pela ESET no formato xls.

**Direito de fazer uma queixa.** Como um titular dos dados, Você tem o direito de enviar uma queixa à autoridade supervisora a qualquer momento. A ESET é sujeita ao regulamento das leis eslovacas e estamos vinculados pela legislação de proteção de dados como parte da União Europeia. A autoridade supervisora de dados relevante é o Gabinete de Proteção de Dados Pessoais da República Eslovaca, localizado em Hraničná 12, 82007 Bratislava 27, Slovak Republic.

## Tratamento de seus Dados pessoais

Serviços prestados pela ESET e implementados em nosso produto são fornecidos sob os termos do [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. Prestamos vários serviços descritos no Acordo de Licença para o Usuário Final e na documentação [documentação](#). Para que tudo funcione, precisamos coletar as informações a seguir:

**Dados de licenciamento e cobrança.** O nome, endereço de e-mail, chave de licença e (se aplicável), endereço, filiação da empresa e dados de pagamento são coletados e processados pela ESET para facilitar a ativação da licença, entrega de chaves de licença, lembretes sobre a expiração, solicitações de suporte, verificação da autenticidade da licença, fornecimento de nosso serviço e outras notificações, inclusive mensagens de marketing de acordo com a legislação aplicável ou com o Seu consentimento. A ESET é legalmente obrigada a manter as informações de cobrança pelo período de 10 anos, mas as informações de licenciamento serão transformadas em anônimas no máximo 12 meses depois da expiração da licença.

**Atualização e outras estatísticas.** As informações processadas incluem 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 são processadas para fins de fornecimento de serviços de atualização e manutenção, segurança e melhoria de nossa infraestrutura de backend.

Essas informações são mantidas além das informações de identificação necessárias para os fins de licenciamento e cobrança, já que não requerem a identificação do Usuário Final. O período de retenção é de até 4 anos.

**ESET LiveGrid® Sistema de reputação.** Hashes de via única relacionados a infiltrações são processados para os fins do Sistema de Reputação ESET LiveGrid®, o que melhora a eficiência de nossas soluções antimalware ao comparar os arquivos escaneados com um banco de dados de itens na lista de permissões e na lista de proibições na nuvem. O Usuário Final não é identificado durante esse processo.

**ESET LiveGrid® Sistema de feedback.** 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

- 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 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.

Todas as informações obtidas e processadas através do Sistema de feedback ESET LiveGrid® são feitas para serem usadas sem a identificação do Usuário Final.

**Avaliação de segurança de dispositivos conectados na rede.** Para fornecer a função de avaliação de segurança, processamos o nome da rede local e as informações sobre os dispositivos em sua rede local, como presença, tipo, nome, endereço IP e endereço MAC do dispositivo em sua rede local em conexão com as informações de licença. As informações também incluem tipo de segurança sem fio e tipo de criptografia sem fio para dispositivos roteadores. As informações de licença que identifiquem o Usuário Final não serão anonimizadas até 12 meses depois da expiração da licença.

**Suporte técnico.** As informações de contato e licenciamento 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. Os dados processados para suporte técnico são armazenados por 4 anos.

**Proteção contra o uso errôneo de dados.** Se a Conta ESET HOME em <https://home.eset.com> for criada e a função em conexão com o furto do computador for ativada pelo Usuário Final, as informações a seguir serão coletadas e processadas: dados de localização, capturas de tela, dados sobre a configuração do computador e dados registrados pela câmera do computador. Os dados coletados são armazenados em nossos servidores ou nos servidores de nossos provedores de serviço com um período de retenção de 3 meses.

**Password Manager.** Se Você escolher ativar a função do Password Manager, os dados relacionados aos seus detalhes de login serão armazenados criptografados apenas no seu computador ou em outro dispositivo designado. Se Você ativar o serviço de sincronização, os dados criptografados serão armazenados em nossos servidores ou nos servidores de nossos prestadores de serviço, para garantir cada serviço. Nem a ESET nem o prestador de serviço têm acesso aos dados criptografados. Apenas Você tem a chave para retirar a criptografia dos dados. Os dados serão removidos mediante a desativação da função.

**ESET LiveGuard.** Se Você escolher ativar o ESET LiveGuard, a função requer o envio de amostras, como arquivos pré-definidos e selecionados pelo Usuário Final. As amostras que Você escolher para a análise remota serão enviadas para o serviço ESET e o resultado da análise será enviado de volta ao seu computador. Quaisquer amostras suspeitas são processadas na forma de informações coletadas pelo Sistema de feedback ESET LiveGrid®.

**Programa de melhoria da experiência do cliente.** Se Você escolheu ativar o [Programa de melhoria da experiência do cliente](#), as informações anônimas de telemetria relacionadas ao uso de Nossos produtos serão coletadas e usadas, com base no Seu consentimento.

Observe que, se a pessoa usando nossos produtos e serviços não for o Usuário Final que comprou o produto ou serviço e concordou no Acordo de Licença para o Usuário Final conosco (por exemplo, um funcionário do Usuário Final, um membro da família ou uma pessoa autorizada a usar o produto ou serviço pelo Usuário Final de acordo com o Acordo de Licença para o Usuário Final), o tratamento dos dados é realizado no interesse legítimo da ESET, dentro do significado do Art. 6 (1) (f) LGPD para permitir ao usuário autorizado pelo Usuário Final usar os

produtos e serviços fornecidos por Nós de acordo com o Acordo de Licença para o Usuário Final.

## **Informações de contato**

Se Você quiser exercer seus direitos como sujeito de dados ou se tiver uma pergunta ou dúvida, envie uma mensagem para:

ESET, spol. s r.o.  
Data Protection Officer  
Einsteinova 24  
85101 Bratislava  
Slovak Republic  
dpo@eset.sk