

# ESET Mobile Security

## Guia do Usuário

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

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

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

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

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

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

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

REV. 12-04-2024

1	Introdução .....	1
<b>1.1</b>	<b>Novidades .....</b>	<b>1</b>
<b>1.2</b>	<b>Requisitos mínimos do sistema .....</b>	<b>1</b>
2	Instalação .....	2
3	Assistente inicial .....	3
4	Recursos de licença gratuitas e premium .....	6
5	Ativação .....	7
6	Desinstalação .....	8
7	Conectando ao ESET HOME .....	9
8	Antivírus .....	12
<b>8.1</b>	<b>Logs de escaneamento .....</b>	<b>15</b>
<b>8.2</b>	<b>Configurações avançadas .....</b>	<b>15</b>
<b>8.3</b>	<b>Adware Detector .....</b>	<b>17</b>
9	Relatório de segurança .....	17
10	Relatório de atividades .....	19
11	Anti-Theft .....	20
<b>11.1</b>	<b>Configurações Anti-Theft .....</b>	<b>21</b>
<b>11.2</b>	<b>Otimização .....</b>	<b>22</b>
<b>11.3</b>	<b>Portal da Web .....</b>	<b>23</b>
<b>11.4</b>	<b>ESET HOME senha .....</b>	<b>23</b>
12	Antiphishing .....	24
<b>12.1</b>	<b>Proteção de notificação e SMS .....</b>	<b>26</b>
13	Bloqueio de aplicativo .....	27
<b>13.1</b>	<b>Esqueci meu código PIN de Bloqueio de aplicativo .....</b>	<b>28</b>
14	Proteção de pagamento .....	29
15	Filtro de Chamadas .....	30
<b>15.1</b>	<b>Adicionar uma nova regra .....</b>	<b>31</b>
16	Inspetor de rede .....	32
17	Auditoria de segurança .....	33
<b>17.1</b>	<b>Monitoramento do Dispositivo .....</b>	<b>33</b>
<b>17.2</b>	<b>Auditoria do Aplicativo .....</b>	<b>33</b>
18	Códigos de indicação .....	34
<b>18.1</b>	<b>Indique um amigo .....</b>	<b>34</b>
<b>18.2</b>	<b>Resgatar código .....</b>	<b>34</b>
19	Configurações .....	35
20	Atendimento ao cliente .....	36
21	Acordo de licença de usuário final .....	37
22	Política de Privacidade .....	45

# Introdução

O ESET Mobile Security é uma solução de segurança completa que protege seu dispositivo contra ameaças emergentes e páginas de phishing e permite que você tome controle do seu dispositivo remotamente no caso de perda ou furto.

Os recursos principais incluem:

- [Antivírus](#)
- [Anti-Theft](#)
- [Antiphishing](#)
- [Integração com o portal ESET HOME](#)
- [Filtro de Chamadas](#)
- [Auditoria de segurança](#)
- [Relatório de segurança](#)
- [Inspetor de rede](#)
- [Bloqueio de aplicativo](#)
- [Proteção de pagamento](#)

## Novidades

Novos recursos no ESET Mobile Security versão 8:

### Adicionado

- Suporte para Android 13
- [Antismishing \(proteção por SMS e proteção de notificação\)](#)

### Aprimorado

- Novo design da tela inicial
- Novo design do menu principal

## Requisitos mínimos do sistema

Para instalar o ESET Mobile Security, seu dispositivo Android deve atender aos requisitos mínimos do sistema a seguir:

- Sistema operacional:  Android 6 (Marshmallow) ou posterior
- Resolução da tela de toque: mínimo 240x320 px
- CPU: 500+ MHz ARM7+
- RAM: 512+ MB
- Conexão com a Internet

### Exclusões de suporte

- Dispositivos com SIM duplo e root não são compatíveis. Os recursos do Anti-Theft e Filtro de Chamadas não estão disponíveis em tablets que não suportam chamadas e mensagens.
- O Android Go não é suportado
- O ESET Mobile Security precisa que os serviços do Google Play funcionem corretamente. O ESET Mobile Security não é compatível com dispositivos sem serviços do Google Play, como alguns dispositivos Huawei.
- O recurso Anti-Theft de cartão SIM confiável não está disponível em dispositivos CDMA.
- Algumas funções dependem da versão do sistema operacional.

## Instalação

Existem três formas de instalar o ESET Mobile Security:

1. **Google Play Store** – abra o aplicativo do Google Play Store em seu dispositivo Android e procure ESET Mobile Security (ou apenas ESET):



2. **Código QR** – leia o código QR abaixo usando seu dispositivo móvel e um aplicativo de leitura de QR:



3. **Da conta ESET HOME** – no seu ESET HOME, faça o download do instalador ESET Mobile Security para seu dispositivo ou envie o instalador para outro dispositivo.

### Observação

- Para obter instruções visuais, visite nosso [guia de instalação passo a passo](#) (este artigo não está disponível em todos os idiomas).

Quando o ESET Mobile Security estiver instalado, toque em **Abrir** para iniciar o [assistente de inicialização](#)

Para proteger suas informações pessoais e os recursos do seu dispositivo Android, o ESET Mobile Security precisará ter acesso às funções do seu dispositivo e, em alguns casos, ter controle sobre elas. Para explicações detalhadas sobre cada tipo de permissão e como eles são usados, consulte a tabela nesse [artigo da Base de conhecimento](#). (O artigo não está disponível em todos os idiomas.)

## Assistente inicial

Depois da instalação, siga os avisos na tela do assistente de inicialização:

### Ativar permissões para o ESET Mobile Security



Este guia é baseado nas configurações de ações do Android. O processo de ativação de permissão pode ser diferente com base no fabricante do seu dispositivo.

1. Toque em **País** e selecione o país aplicável.
2. Toque em **Idioma** e selecione o idioma aplicável.
3. Toque em **Avançar** e concorde com o [Acordo de licença de usuário final](#) e a [Política de privacidade](#).

4. Se aplicável, permita as opções a seguir e toque em **Avançar**.

- **Permitir ESET LiveGrid©** – para ler mais sobre o sistema de feedback ESET LiveGrid©, [visite a seção Configurações avançadas](#).
- **Permitir análise para ajudar a tornar nossos produtos melhores** – o ESET Mobile Security enviará informações anônimas do aplicativo (desempenho, estatísticas operacionais) que vão nos ajudar a melhorar nossos aplicativos e serviços. Para ler mais sobre as informações que coletamos, visite o capítulo [Política de privacidade](#).
- **Permitir o uso de dados para fins de marketing**
- **Permitir o envio de descontos promocionais e novidades sobre produtos da ESET** – você receberá novidades no produto e as ofertas mais recentes da ESET.

5. Revise seus detalhes de ativação quando tiver instalado o ESET Mobile Security do link de download enviado para seu endereço de e-mail [da conta ESET HOME](#). Toque em **Continuar** e [siga as instruções para ativar o ESET Mobile Security com a conta ESET HOME](#). Se você não concorda, toque em **Negar** e siga as etapas abaixo.

6. Entre na sua conta ESET HOME para conectar seu dispositivo móvel à sua conta e ativar o ESET Mobile Security.

### ✓ [Continuar com o Google.](#)

a. Selecione sua conta Google.

b. Se você estiver conectando pela primeira vez a uma conta ESET HOME existente com sua conta Google, será solicitado que você digite sua senha ESET HOME. Toque em **Confirmar senha**.

### ✓ [Continuar com a Apple.](#)

- a. Digite seu ID Apple e senha.
- b. Toque em **Entrar**.
- c. Digite o código enviado para seu dispositivo Apple.
- d. Toque em **Continuar**.
- e. Se você confia no seu navegador da web, clique em **Confiar**.
- f. Toque em **Continuar** para acessar o ESET HOME com seu ID Apple.
- g. Toque no ícone **X** no canto superior esquerdo para retornar ao ESET Mobile Security.

✓ [Ler código QR](#)

Esta opção requer outro dispositivo com o aplicativo ESET HOME.

- a. Abra o aplicativo ESET HOME em outro dispositivo.
- b. Toque no botão do menu  > **Escanear um código QR**.
- c. Toque em **Ler código QR**. Você pode ser solicitado a permitir que o ESET HOME tire fotos e grave vídeos. Toque em **Enquanto estiver usando o aplicativo** ou **Somente dessa vez**.
- d. Use sua câmera para escanear o código QR.
- e. Toque em **Conectar dispositivo**.
- f. Toque em **Concluir** no seu ESET Mobile Security.

✓ [Criar conta ou entrar](#)

### Criar uma conta ESET HOME

- a. Digite seu endereço de e-mail e senha.



#### Requisitos de senha

A senha precisa ter pelo menos 10 caracteres e pelo menos um caractere em letras maiúsculas, um caractere em letras minúsculas e um número.

- b. Toque em **Criar conta** para receber um link de confirmação por e-mail.
- c. Crie um nome para seu dispositivo e toque em **Avançar**.
- d. Para trabalhar com o ESET Mobile Security corretamente, toque em **Continuar** para permitir a permissão de acesso a Todos os arquivos.
- e. Toque em **Iniciar primeiro escaneamento**.
- f. Para concluir o registro, toque no link no e-mail de confirmação.

## Entre no ESET HOME

a. Toque em **Entrar** sob o botão **Criar conta**.

b. Digite seu e-mail e senha.

c. Toque em **Entrar**.

Depois de entrar na sua conta ESET HOME, você precisará criar um apelido para seu dispositivo. Isso vai ajudar você a identificar este dispositivo na sua conta ESET HOME. Digite o apelido e toque em **Avançar**.

### ✓ [Ignorar](#)

Se você não tem uma conta ESET HOME, ou se não quiser conectar seu dispositivo móvel à sua conta ESET HOME, toque em **Ignorar**. Você pode entrar em sua conta ESET HOME mais tarde no aplicativo ESET Mobile Security.

Se você ignorar essa etapa, você será solicitado a selecionar a conta de e-mail que vai receber o registro da licença ESET e os e-mails do Suporte técnico. Toque em **Selecione seu endereço de e-mail** para exibir a lista de contas de e-mail disponíveis. Selecione o email da lista de contas ou toque em **Adicionar Conta** para adicionar uma nova conta de email ao seu dispositivo. Toque em **OK** para continuar. Para usar uma conta de e-mail diferente sem adicionar a conta ao seu dispositivo, toque em **Selecione seu endereço de e-mail > Cancelar**. Repita esta ação duas vezes. Digite seu e-mail e toque em **Selecionar** para continuar.

7. As últimas etapas do assistente de inicialização variaram de acordo com a versão do Android do seu dispositivo.

### ✓ [Android 6–10](#)

a. Para ativar o escaneamento do dispositivo, o ESET Mobile Security precisa ter várias permissões. Revise as permissões do ESET Mobile Security na tela **Permitir acesso** e toque em **Continuar**.

b. Toque em **Permitir** para permitir o acesso ao ESET Mobile Security. Se você tocar em **Ignorar**, o ESET Mobile Security não conseguirá escanear seu dispositivo em busca de ameaças até que essas permissões sejam autorizadas e você receberá uma notificação de Risco de segurança.

### ✓ [Android 11 e versões posteriores](#)

a. Toque em **Continuar**.

b. Selecionar ESET Mobile Security.

c. Ative na alterância ao lado de ESET Mobile Security.

d. O Assistente de inicialização está concluído. Toque em **Iniciar primeiro escaneamento**.

### Protetor de bateria

Muitos fabricantes de dispositivos introduziram opções de proteção de bateria ou economia de bateria em dispositivos do Android 6 e versões posteriores. Quando ativado, este recurso desliga a funcionalidade do Antiphishing no ESET Mobile Security. Em dispositivos com este recurso, será necessário criar uma exceção para permitir que a funcionalidade Antiphishing do ESET Mobile Security funcione com o recurso de economia de bateria ativado. Para criar uma exceção consulte a documentação do fabricante do seu dispositivo.

## Recursos de licença gratuitas e premium

O ESET Mobile Security tem duas versões disponíveis:

- Gratuito – recursos básicos de uso gratuito por tempo ilimitado
- Premium - os recursos premium são ativados até sua licença expirar.

Essa tabela indica quais recursos estão disponíveis nas versões Gratuita e Premium:

	Gratuito	Premium
Antivírus	✓	✓
Antivírus - rastreamentos automáticos		✓
Atualizações automáticas de módulos de detecção		✓
Bloqueio de aplicativo		✓
Antifurto - portal da web		✓
Antifurto - Proteção SIM		✓
Inspetor de rede		✓
Antiphishing		✓
Filtro de Chamadas		✓
Proteção de pagamento		✓
Auditoria de segurança		✓
Relatório de segurança	✓	✓

Selecione seu período de assinatura. Você pode ser cobrado mensalmente ou anualmente. E selecione sua versão de licença de assinatura.

Tipo de licença	Uso da licença
Celular	Você pode usar a licença para o ESET Mobile Security em até cinco dispositivos Android com o ESET Mobile Security e o ESET Smart TV Security sob a mesma conta Google.
PC/Mac/Mobile	Você receberá uma licença do ESET Internet Security que pode ser usada para proteger três dispositivos. Uma licença será alocada automaticamente para o ESET Mobile Security no dispositivo para o qual você comprou a licença. Como em uma licença móvel, você pode usar essa licença para ativar até cinco dispositivos Android com o ESET Mobile Security e o ESET Smart TV Security sob a mesma conta Google.

### Exemplo de uso de licença móvel

O Sam usa um smartphone Android, tablet Android e uma smart TV Android. Em todos esses dispositivos o Sam entrou com a mesma conta Google.

- i O Sam comprou uma Assinatura móvel para o ESET Mobile Security via smartphone. Depois da compra, Sam recebe uma chave de licença no e-mail associado à conta Google do Sam. Sam pode usar essa licença para ativar o ESET Mobile Security no tablet Android e o ESET Smart TV Security na Smart TV via ESET HOME ou usando a chave de licença.

## Ativação

Para desbloquear os recursos da versão premium, é preciso ativar o ESET Mobile Security.

Há várias maneiras de ativar o ESET Mobile Security. A disponibilidade de um determinado método de ativação pode variar dependendo do seu país e dos meios de distribuição (página da ESET, Google Play).

### Se você ainda não tem uma licença

1. Toque no botão do menu  para abrir o menu principal.
2. Toque em **Licença** no menu principal.
3. Na seção **Sua licença** toque em **Atualizar para a versão premium**.
4. Selecione um plano de assinatura **Mensal** ou **Anual**. Toque no botão **Atualizar para versão Premium** para confirmar o plano selecionado. Sua licença Premium será renovada automaticamente dependendo do seu intervalo de assinatura selecionado.
5. Você será direcionado para concluir a compra através do Google Play.
6. Você receberá um recibo de pedido do Google Play com seu número de Pedido no endereço de email associado à sua conta Google Play. Você também receberá um email da ESET (não responda) com suas informações de licença nesta mesma conta de email. Salve esses e-mails para futuras referências.
7. Seu produto será ativado automaticamente assim que a compra do Google Play for bem-sucedida.

### Se você comprou licença através do ESET.com:

Uma chave de licença é uma string única com a formatação: XXXX-XXXX-XXXX-XXXX-XXXX que é usada para identificar o proprietário da licença. Isso pode ser encontrado no email recebido da ESET ou no cartão de licença incluído na caixa de compra.

#### Disponibilidade de recursos



Alguns recursos como Códigos de indicação estão disponíveis apenas para proprietários de licença do Google Play, esses recursos ficarão inativos se o produto for ativado com uma licença comprada da eset.com.

### Se você já tem uma licença

## Ative o ESET Mobile Security com uma licença já associada ao ESET HOME

Siga as etapas de ativação abaixo se você já tem uma licença ESET Mobile Security presente na sua conta ESET HOME e também quando tiver instalado o ESET Mobile Security do e-mail de verificação enviado [da conta ESET HOME de outra pessoa](#):

1. Revise seus detalhes de ativação no aplicativo ESET Mobile Security e toque em **Continuar** para concordar que o endereço de e-mail exibido vai gerenciar seu dispositivo.

### Detalhes da ativação

- i** Quando alguém enviar a você a proteção ESET por e-mail, o ESET Mobile Security será gerenciado pela conta ESET HOME do remetente. Se você concordar, desconecte o dispositivo da sua conta ESET HOME primeiro. Se você não concorda, toque em **Negar** e continue no [Assistente de inicialização com a etapa 4](#).

2. Crie um nome para seu dispositivo e toque em **Avançar**.
3. Quando sua ativação for bem-sucedida, toque em **Concluir**.
4. Toque em **Iniciar primeiro escaneamento**.
5. Para trabalhar com o ESET Mobile Security corretamente, toque em **Continuar** para permitir a permissão de acesso a Todos os arquivos.

Se um problema aparecer e você não for capaz de associar o ESET Mobile Security com sua conta ESET HOME, visite o tópico [Conectando ao ESET HOME](#).

## Ativação sem o ESET HOME

1. Vá para o menu principal ao tocar no botão de menu .
2. Toque em **Licença** na tela inicial do ESET Mobile Security e selecione **Inserir uma chave de licença**.
3. Digite sua chave de licença no campo e toque em **Ativar**.
4. Quando a verificação de licença estiver concluída, você verá **Ativação bem-sucedida**.
5. Toque em **Concluir** para fechar a janela.

## Desinstalação

O ESET Mobile Security pode ser desinstalado usando o assistente de **Desinstalação** disponível no menu principal em ESET Mobile Security.

1. Toque em Menu .
2. Toque em **Configurações**.
3. Toque em **Desinstalar**.
4. Se a proteção Anti-Theft estiver ativada, você precisará inserir sua senha/padrão de segurança do ESET

Mobile Security ou impressão digital.

5. Toque em **Desinstalar**.

Alternativamente, siga as etapas abaixo para instalar manualmente o produto:

## Android 7 e versões posteriores:

1. Vá para Configurações e toque em **Gerenciar aplicativos > ESET Mobile Security > Desinstalar**. Se a proteção Anti-Theft estiver ativada, você pode ser solicitado a desativar o Administrador do dispositivo do ESET Mobile Security antes de desinstalar.

Ou

1. No ESET Mobile Security, toque no botão do menu principal  para abrir o menu principal.

2. Selecione **Configurações**.

3. Toque em **Desinstalar**.

4. Toque em **Desinstalar** novamente para confirmar sua decisão.

## Android 6,

1. Toque no ícone do Iniciador  na tela inicial do Android (ou navegue até **Início > Menu**) e toque em **Configurações > Segurança > Administradores do dispositivo**. Selecione **ESET Mobile Security** e toque em **Desativar**. Toque em **Desbloquear** e digite sua senha/padrão de segurança. Você pode ignorar esta etapa se o aplicativo não estiver mais definido como um administrador de dispositivo.

2. Volte para **Configurações** e toque em **Gerenciar aplicativos > ESET Mobile Security > Desinstalar**.

## Conectando ao ESET HOME

Para usar esse recurso, atualize para o ESET Mobile Security versão 6.3 ou posterior.

### Ativando o ESET Mobile Security via ESET HOME

 Se quiser ativar um dispositivo via ESET HOME pela segunda vez (por exemplo, depois da reinstalação do ESET Mobile Security), será preciso remover manualmente o dispositivo da licença no ESET HOME antes de continuar. Caso contrário, você não conseguirá ativar este dispositivo via ESET HOME.

## Conecte seu dispositivo a uma conta ESET HOME existente

1. Toque no botão do menu .

2. Toque em **conta ESET HOME**.

✓ [Continuar com o Google.](#)

a. Selecione sua conta Google.

b. Se você estiver conectando pela primeira vez a uma conta ESET HOME existente com sua conta Google, será solicitado que você digite sua senha ESET HOME. Toque em **Confirmar senha**.

✓ [Continuar com a Apple.](#)

a. Digite seu ID Apple e senha.

b. Toque em **Entrar**.

c. Digite o código enviado para seu dispositivo Apple.

d. Toque em **Continuar**.

e. Se você confia no seu navegador da web, clique em **Confiar**.

f. Toque em **Continuar** para acessar o ESET HOME com seu ID Apple.

g. Toque no ícone **X** no canto superior esquerdo para retornar ao ESET Mobile Security.

✓ [Ler código QR](#)

Esta opção requer outro dispositivo com o aplicativo ESET HOME.

a. Abra o aplicativo ESET HOME em outro dispositivo.

b. Toque no botão do menu  > **Escanear um código QR**.

c. Toque em **Ler código QR**. Você pode ser solicitado a permitir que o ESET HOME tire fotos e grave vídeos. Toque em **Enquanto estiver usando o aplicativo** ou **Somente dessa vez**.

d. Use sua câmera para escanear o código QR.

e. Toque em **Conectar dispositivo**.

f. Toque em **Concluir** no seu ESET Mobile Security.

✓ [Continuar com o e-mail](#)

a. Digite seu e-mail e senha.

b. Toque em **Entrar**.

3. Se você estiver entrando em sua conta ESET HOME pela primeira vez com este dispositivo, crie um nome para seu dispositivo para ajudar a identificar o dispositivo no ESET HOME. Toque em **Avançar**.

4. Se você usar uma licença de avaliação ou gratuita e tiver uma licença disponível no ESET HOME, será oferecido que você ative o ESET Mobile Security.

a. Selecione a licença aplicável.

b. Toque em **Ativar**.

5. Toque em **Concluir**.

---

## Crie uma conta ESET HOME e conecte seu dispositivo a ela

1. Toque no botão do menu .
2. Toque em **conta ESET HOME**.
3. Toque em **Criar conta**.
4. Digite seu endereço de e-mail e senha.



### Requisitos de senha

A senha precisa ter pelo menos 10 caracteres e ter pelo menos um caractere em letras maiúsculas, um caractere em letras minúsculas e um número.

5. Toque em **Criar conta** para receber um link de confirmação por e-mail.
  6. Crie um nome para seu dispositivo e toque em **Avançar**.
  7. Para trabalhar com o ESET Mobile Security corretamente, toque em **Continuar** para permitir a permissão de acesso a Todos os arquivos.
  8. Toque em **Iniciar primeiro escaneamento**.
  9. Para concluir o registro, toque no link no e-mail de confirmação.
- 

## Desconectar seu dispositivo do ESET HOME

1. Toque no botão do menu .
2. Toque em **conta ESET HOME**.
3. Toque em **Desconectar dispositivo**. Esta opção não estará disponível se seu dispositivo não estiver conectado ao ESET HOME.
4. Use sua impressão digital ou digite seu PIN.
5. Toque em **Desconectar**.

# Antivírus

O módulo Antivírus protege seu dispositivo contra códigos maliciosos ao bloquear as ameaças que chegam e depois limpando tais ameaças.



Descubra e elimine ameaças com profundidades variadas de escaneamento.

🔍 Escanear dispositivo

### Escaneamentos automáticos



Escaneamento no carregador  
Ativado



Escaneamento programado  
Desativado



### Atualização



Atualizar módulos de detecção  
Versão: 27121 (atualizado)

## Proteção em tempo real

A proteção em tempo real do sistema de arquivos controla todos os arquivos nas pastas de download em busca de 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 desativar a Proteção em tempo real do sistema de arquivos na seção **Antivírus**. Se você precisar ir para as configurações da Proteção em tempo real, toque nos três pontos  na seção **Antivírus > Configurações avançadas > Proteção em tempo real**.

## Rastrear dispositivo

Você pode realizar o escaneamento sob demanda a qualquer momento ao tocar no botão **Escanear dispositivo** na seção **Antivírus**. Por padrão, o nível de escaneamento está definido para o Escaneamento inteligente. Você pode alterar o nível de escaneamento nas **configurações avançadas** do antivírus. Toque no botão de três pontos  > **Configurações avançadas > Nível de rastreamento**.

Há dois níveis de rastreamento para escolher:

- **Inteligente** — O rastreamento inteligente irá rastrear aplicativos instalados, arquivos DEX (arquivos executáveis do sistema operacional Android), arquivos SO (bibliotecas), arquivos com uma profundidade de rastreamento máxima de 3 arquivos aninhados e conteúdo do cartão SD.
- **Profundo** - O rastreamento profundo vai examinar todos os tipos de arquivos, independentemente da extensão, na memória interna e no cartão SD.

Um breve resumo do escaneamento será salvo em um arquivo de relatório disponível na seção [Relatórios do escaneamento](#). Se quiser anular o escaneamento já em andamento, toque em **Cancelar**. O resultado e as estatísticas do escaneamento serão exibidos durante o escaneamento no painel de configuração do **Antivírus**.

### Escaneamento do cartão de memória

 O ESET Mobile Security não é compatível com o escaneamento de cartões de memória em dispositivos com o Android 6 e versões posteriores.

## Ameaças não solucionadas

Depois que o ESET Mobile Security detecta uma ameaça, essa opção estará disponível até que você selecione uma ação de resposta para a ameaça. As ações de resposta disponíveis são remover ou ignorar a ameaça.

## Ignorar ameaças

Depois de escolher Ignorar uma ameaça, a opção **Ignorar ameaças** vai aparecer. Esta opção ainda permitirá que você remova uma ameaça ignorada mais tarde.

## Rastreamento no carregador

Quando esta opção estiver selecionada, um escaneamento será iniciado automaticamente quando o dispositivo

estiver no estado ocioso, totalmente carregado e conectado a um carregador.

## Rastreamento programado

O rastreamento programado permite que você agende o rastreamento de Dispositivo para ser executado automaticamente, em um horário predefinido. Para agendar um rastreamento, toque em ao lado de **Rastreamento programado** e especifique as datas e horários para que o rastreamento seja iniciado.

## Atualizar módulos de detecção

Por padrão, o ESET Mobile Security inclui uma tarefa para garantir que o programa seja atualizado regularmente. Para executar a atualização manualmente, toque em **Atualizar módulos de detecção**.

### Carregamento de transferência de dados

**i** Para evitar o uso desnecessário da largura de banda, as atualizações são emitidas apenas quando necessário. As atualizações são gratuitas, mas a operadora poderá cobrar pela transferência de dados.

Para mais informações sobre rastreamentos, consulte os links a seguir:

- [Logs de escaneamento](#)
- [Configurações avançadas](#)

## Relatórios de escaneamento

A seção Relatórios de rastreamento contém dados abrangentes sobre cada rastreamento agendado ou rastreamento de dispositivo acionado manualmente.

Cada relatório contém:

- Data e hora do rastreamento
- Nível de rastreamento (Inteligente ou Detalhado)
- Duração do rastreamento
- Número de arquivos rastreados
- Resultado do rastreamento ou erros ocorridos durante o rastreamento
- Número de ameaças encontradas e lista de ameaças encontradas

## Configurações avançadas

### Nível de rastreamento

Há dois níveis de rastreamento para escolher:

- **Inteligente** — O rastreamento inteligente irá rastrear aplicativos instalados, arquivos DEX (arquivos executáveis do sistema operacional Android), arquivos SO (bibliotecas), arquivos com uma profundidade de rastreamento máxima de 3 arquivos aninhados e conteúdo do cartão SD.
- **Profundo** - O rastreamento profundo vai examinar todos os tipos de arquivos, independentemente da extensão, na memória interna e no cartão SD.

## Proteção em tempo real

O escaneamento em tempo real é iniciado automaticamente na inicialização do sistema e escaneia os arquivos com os quais você interage. Ele escaneia automaticamente a pasta Download e os aplicativos instalados ou atualizados.

## ESET LiveGrid© sistema de reputação

O ESET LiveGrid© é um sistema preventivo projetado para fornecer ao seu dispositivo níveis adicionais de segurança. Ele monitora constantemente os programas e processos em execução do seu sistema contra as últimas informações coletadas de milhões de usuários da ESET em todo o mundo. Isso nos permite oferecer proteção proativa melhor e mais precisa e velocidade de escaneamento melhor para todos os usuários ESET. Recomendamos que você ative este recurso.

## ESET LiveGrid© sistema de feedback

Esse sistema de feedback nos permite coletar estatísticas anônimas, relatórios de travamento e dados de diagnóstico sobre objetos suspeitos, que processamos automaticamente para criar um mecanismo de detecção em nosso sistema de nuvem.

## Mídia removível

O ESET Mobile Security escaneia todas as mídias removíveis conectadas ao seu dispositivo (unidades USB, discos rígidos externos, etc.).

## Detectar Aplicativos Potencialmente Indesejados

Um aplicativo potencialmente indesejado é um programa que contém adware, instala barras de ferramentas, rastreia seus resultados de pesquisa ou tem outros objetivos pouco claros. Podem existir algumas situações em que você acredita que os benefícios oferecidos pelo aplicativo potencialmente indesejado superam os riscos. Por isso, a ESET atribui a essa categoria de aplicativo um risco menor se comparado ao software malicioso.

## Detectar aplicativos potencialmente não seguros

Há muitos aplicativos legítimos com a função de simplificar a administração dos dispositivos conectados em rede. Essa classificação inclui programas como ferramentas de acesso remoto, aplicativos que descobrem senhas e registradores de teclado. Aplicativos potencialmente inseguros é uma classificação usada para software comercial legítimo. Porém, eles podem ser usados indevidamente para fins maliciosos se estiverem em mãos erradas. Ative a opção **Detectar aplicativos potencialmente inseguros** para monitorar essa categoria de aplicativos e bloqueá-los, se você preferir.

## Servidor de atualização

Esta opção permite a você habilitar atualizações no seu dispositivo a partir do **servidor de pré-lançamento**. Atualizações de pré-lançamento passaram por testes internos e estarão disponíveis em breve para o público em geral. Você pode se beneficiar do acesso antecipado aos métodos de detecção e correções mais recentes. Porém as atualizações pré-lançamento podem não ser totalmente estáveis em todos os momentos. Para verificar as versões dos módulos de programa atuais, toque nos três pontos  na tela principal do ESET Mobile Security e toque em **Sobre > ESET Mobile Security**. Recomendamos que os usuários básicos deixem a opção **Servidor de lançamento** selecionada por padrão.

## Adware Detector

O Adware Detector é a resposta da ESET para os aplicativos adware. Aplicativos adware podem ser aplicativos legítimos ou aplicativos que tentam se apresentar como legítimos (como Calculadora ou lanterna). Esses aplicativos então exibem anúncios em tela cheia mesmo quando o aplicativo estiver fechado. Portanto, o usuário não pode detectar qual aplicativo está exibindo essas telas de anúncio.

O Adware Detector ajuda você a identificar esses aplicativos adware. Para usá-lo, faça o seguinte depois que uma tela de anúncio for exibida:

1. Abrir ESET Mobile Security.
2. Na tela principal do ESET Mobile Security, toque em **Antivírus**.
3. Toque em  no canto superior direito para exibir o menu.
4. Toque em **Adware Detector** no menu.
5. Depois que o Adware Detector exibir um guia para detectar aplicativos adware, toque em **Continuar**.

O Adware Detector exibirá aplicativos que foram abertos nos últimos cinco minutos. Identifique os aplicativos suspeitos e toque em **Remover** para removê-los do seu dispositivo. Um aplicativo suspeito normalmente é um que você não queria abrir ou que não estava usando no momento.

## Relatório de segurança

Relatórios de segurança fornecem uma visão geral abrangente de cada módulo do programa e seu respectivo status e estatísticas. Também é possível ativar módulos que atualmente não estejam ativados na tela do **Relatório de segurança**. Cada seção de módulo de programa contém as informações a seguir.

Se algumas informações não estiverem presentes, significa que zero ocorrências aconteceram.

### Antivírus

- Escaneamentos de aplicativos
- Ameaças encontradas
- Atualizações do banco de dados

- Detecção realizada
- Arquivos escaneados
- Aplicativos atualizados

## **Bloqueio de aplicativo**

- Número de aplicativos protegidos
- Número de desbloqueios de aplicativo bem sucedidos
- Número de tentativas falhas de desbloquear

## **Antiphishing**

- Links escaneados
- Notificações escaneadas
- Ameaças detectadas

## **Filtro de Chamadas**

- Chamadas enviadas
- Chamadas recebidas
- Chamadas bloqueadas

## **Proteção de pagamento**

- Número de aplicativos protegidos
- Número de escaneamentos de aplicativos protegidos
- Número de problemas encontrados
- Número de quantas vezes você iniciou o aplicativo bancário ou de pagamento do Iniciador seguro

## **Auditoria de segurança**

- Alertas de roaming representam o número de vezes que você foi alertado sobre estar conectado a uma rede de roaming
- Avisos de WiFi aberta

## **Inspetor de rede**

- Escaneamentos de rede

- Dispositivos encontrados
- Vulnerabilidades encontradas

ESET Mobile Security vai exibir uma mensagem curta de relatório mensal na barra de notificações do Android todos os meses. Se você não quiser receber essas notificações, ative a opção **Não exibir a notificação de relatório mensal**.

## Relatório de atividades

O Relatório de atividades exibe as atividades diárias do ESET Mobile Security na tela principal do aplicativo ESET Mobile Security. O Relatório de Atividades contém informações sobre os sites escaneados pelo ESET Mobile Security, ESET Mobile Security atualizações, atualizações de aplicativo, aplicativos instalados, ESET Mobile Security escaneamentos e muito mais.

Para exibir o histórico completo do Relatório de atividades, toque no ícone > ao lado do Relatório de atividades. No relatório completo do Relatório de atividades, você pode usar **Filtros** para filtrar atividades por status ou recurso do ESET Mobile Security. Por exemplo: Alerta, Risco, Antifurto e Licença. Você também pode filtrar as atividades pela data de ocorrência por mais recente ou mais antigo.

Para limpar o histórico do Relatório de atividades:

1. Abrir ESET Mobile Security.
2. Deslize a tela inicial para baixo.
3. Toque no ícone > ao lado do **Relatório de atividades**.
4. Toque no ícone do menu .
5. Toque em **Limpar tudo**.

Para remover registros individuais do histórico do Relatório de atividades:

1. Abrir ESET Mobile Security.
2. Deslize a tela inicial para cima.
3. Toque no ícone > ao lado do **Relatório de atividades**.
4. Passe o registro adequado para a esquerda.
5. Toque em **Remover**.

# Anti-Theft

O recurso ESET Anti-Theft protege seu dispositivo móvel contra acesso não autorizado, permite que você monitore atividades estranhas e rastreia a localização do dispositivo. Você também pode exibir uma mensagem para quem encontrou o dispositivo se ele estiver perdido.

o ESET Anti-Theft precisa das seguintes permissões:

- Acesso à câmera para tirar fotos de um intruso.
- Editar acesso aos arquivos para remover dados sensíveis remotamente.
- Acesso aos dados de localização para rastrear seu dispositivo se ele for perdido.
- Acesso de atividade física para reconhecer quando seu dispositivo for movido.
- Acesso de localização em segundo plano para rastrear seu dispositivo se ele for perdido, mesmo quando o ESET Mobile Security estiver fechado ou não estiver em uso. Ao conceder essa permissão, selecione **Permitir sempre** para garantir a proteção completa.
- Acesso de uso para permitir o recebimento de chamadas no seu dispositivo se ele for bloqueado.
- Acesso de administrador do dispositivo para impedir a desinstalação não autorizada do ESET Mobile Security. Depois de ativar o administrador do dispositivo, você será solicitado a criar um PIN para proteger as configurações importantes no ESET Mobile Security.
- Ler informações do telefone para detectar a remoção do cartão SIM. Seu dispositivo será bloqueado quando o cartão SIM for removido.

Visite nosso [artigo da Base de conhecimento Configurar proteção Anti-Theft no ESET Mobile Security for Android](#) para configurar a proteção Anti-Theft no ESET Mobile Security (os artigos da Base de conhecimento não estão disponível em todos os idiomas).

## Bloquear dispositivo automaticamente

Além de bloquear seu dispositivo do portal ESET HOME, você pode configurar o ESET Mobile Security para bloquear automaticamente seu dispositivo quando uma das ações a seguir for realizada:

- **Um cartão SIM é removido** – se o cartão SIM confiável for removido do dispositivo, o dispositivo será bloqueado. Para remover e inspecionar cartões SIM confiáveis, toque em **Gerenciar cartões SIM confiáveis**, selecione o cartão SIM que deseja remover e toque no ícone da lixeira . Para adicionar um cartão SIM confiável, insira o cartão SIM. Se o Bloqueio automático estiver ativado, será preciso desbloquear o dispositivo. O ESET Mobile Security vai pedir que você confirme que o novo cartão SIM adicionado é confiável.

### Suporte do bloqueio automático mediante remoção do cartão SIM

- **O recurso de bloqueio automático mediante remoção do cartão SIM não está disponível em dispositivos CDMA, WCDMA e apenas Wi-Fi.**

- **Depois de [X] tentativas de desbloqueio** – Quando ativado, seu dispositivo será bloqueado depois de um número determinado de tentativas de desbloqueio falhas. O número de tentativas de desbloqueio falhas antes do bloqueio do dispositivo pode ser definido nas configurações do Anti-Theft. Se a sua tentativa falha foi por

engano, ela poderá ser corrigida em 30 segundos e não será considerada como uma tentativa falha. Você pode alterar o tempo para uma correção nas configurações do Anti-Theft, na opção **Tempo para correção**. O tempo para correção também pode ser desativado, e o dispositivo será bloqueado imediatamente depois do número determinado de tentativas falhas.

Quando o dispositivo está bloqueado, você pode exibir as informações para entrar em contato com o proprietário do dispositivo. Também pode permitir que o dispositivo tire fotos com ambas as câmeras para obter fotos da pessoa que está tentando desbloquear seu dispositivo.

## Depois do dispositivo ser bloqueado

Você pode definir o seguinte para acontecer depois do seu dispositivo ser bloqueado:

- A opção **Mostrar detalhes de contato** exibe os detalhes do **Proprietário do contato** quando um código de bloqueio de tela incorreto é inserido. Toque em **Editar detalhes de contato** para digitar seus detalhes de contato para serem exibidos quando o dispositivo for perdido. Seu e-mail ESET HOME está digitado por padrão.
- A opção **Tirar uma foto** salva as fotos da câmera traseira e frontal na Galeria do dispositivo e no portal Anti-Theft no caso de uma tentativa falha de desbloqueio ou uma remoção do cartão SIM.

## Como desbloquear meu dispositivo móvel

Se você bloqueou seu dispositivo móvel via portal ESET Anti-Theft ou se o ESET Mobile Security for Android tiver bloqueado seu dispositivo móvel, você precisará acessar sua senha ESET HOME.

### Desbloquear seu dispositivo gerenciado por outra pessoa



Se o seu ESET Mobile Security for Android for gerenciado pela conta ESET HOME de outra pessoa, digite a senha para que a conta desbloqueie seu dispositivo.

Para instruções visuais sobre como desbloquear seu dispositivo móvel, leia o seguinte artigo na [Base de conhecimento ESET](#) (disponível em inglês e em vários outros idiomas).

## Configurações Anti-Theft

### Bloquear após tentativas que falharam

Selecione o número de tentativas falhas de desbloqueio permitidas antes do dispositivo ser bloqueado. Para definir o número de tentativas falhas de desbloqueio toque em na tela do Anti-Theft, selecione **Configurações**, toque em **Bloquear após tentativas que falharam** e selecione o número de tentativas falhas que você deseja.

### Tempo para correção

Se você ativou Bloquear após tentativas que falharam, seu dispositivo será bloqueado após o número definido de tentativas falhas. Desative o Tempo para correção para bloquear o dispositivo imediatamente depois de alcançar o número de tentativas falhas, ou defina um período de tempo para desbloquear seu dispositivo com sucesso antes de ele ser bloqueado ao chegar ao número definido de tentativas falhas.

### Exemplo

- Bloquear após tentativas que falharam** está ativado e o número de tentativas falhas está definido como 3.
- i** O **Tempo para correção** está definido como 15 segundos.
- Depois de inserir o padrão de desbloqueio errado no dispositivo três vezes, você tem 15 segundos para inserir o padrão de desbloqueio correto para impedir que o ESET Mobile Security bloqueie o dispositivo.

## Editar detalhes do contato

Se um dispositivo for marcado como perdido no ESET Anti-Theft, ou depois de um número definido de tentativas falhas de desbloqueio, as informações dos **Detalhes de contato** serão exibidas na tela do seu dispositivo bloqueado para que a pessoa que encontrar seu dispositivo possa entrar em contato com você.

Estas informações podem incluir:

- Mensagem exibida (opcional)
- Seu nome (opcional)
- Número de telefone (que não o seu)
- Endereço de e-mail (opcional)

## Gerenciar cartões SIM confiáveis

Essa opção permite que você remova ou renomeie o cartão SIM inserido. Para adicionar um novo cartão SIM confiável, insira o cartão SIM no dispositivo. O dispositivo será bloqueado. Desbloqueie o dispositivo com seu código de segurança. Você será solicitado a adicionar o cartão SIM recém-inserido à lista de cartões SIM confiáveis. Se você não adicionar este cartão SIM à lista, a proteção SIM ficará desativada.

## Alterar tipo de bloqueio

Selecione uma forma de desbloquear o ESET Anti-Theft. Um código PIN é definido como uma opção padrão durante a configuração do Anti-Theft. Você pode alterar isso para uma opção de padrão de desbloqueio.

## Usar impressão digital

Quando ativado, você pode usar a impressão digital salva no dispositivo para desbloquear a opção Anti-Theft.

## Otimização

A otimização do ESET Anti-Theft é uma avaliação técnica mensurável do estado de segurança de seu dispositivo. A proteção Anti-Theft examinará seu sistema em busca dos problemas listados abaixo.

Para cada problema de segurança, é possível tocar em **Alterar Configurações** para navegar até a tela onde o problema específico pode ser resolvido. Se não quiser que o ESET Mobile Security reporte um problema, toque em **Ignorar este problema**.

- **Serviços de localização desligados** - para ligar, vá até as configurações do Android > **Serviços de**

**localização** e selecione **Usar redes sem fio**

- **Satélites GPS não utilizados** - acesse esta configuração nas configurações do Android > **Localização** > **Modo** > **Alta precisão**
- **Bloqueio de tela não protegido** - para proteger seu dispositivo com um código de bloqueio de tela, senha, PIN ou padrão, vá até as configurações do Android > **Tela de bloqueio ; Bloqueio de tela** e selecione uma das opções disponíveis. A maioria dos dispositivos Android oferece Swipe, Movimento, Desbloqueio por face, Face e voz, Padrão, PIN ou Senha. Se alguém tentar desbloquear o dispositivo usando um código errado, o ESET Anti-Theft irá notificá-lo sobre a atividade suspeita no portal ESET HOME.
- **Dados móveis desativados** - acesse esta configuração nas configurações do Android > **Redes sem fio e redes** > **Redes móveis** > **Dados**.
- **Serviços do Google Play não presentes** - O ESET Anti-Theft usa os Serviços do Google Play para fornecer comandos ao seu dispositivo em tempo real e exibir notificações push. Se esses serviços estiverem desativados ou faltando em seu dispositivo, as funções do ESET Anti-Theft gerenciadas a partir do ESET HOME serão limitadas.

## Portal da Web

O ESET Mobile Security é integrado completamente com a proteção do ESET Anti-Theft com o novo [portal ESET HOME](#). Do portal ESET Anti-Theft você será capaz de monitorar as atividades do seu dispositivo, bloquear o dispositivo, enviar mensagens personalizadas para o localizador do dispositivo, acionar um alarme alto ou limpar os dados do dispositivo remotamente.

Para criar uma conta ESET HOME, toque em **Criar nova conta** e preencha o formulário de registro. Verifique sua caixa de entrada para a confirmação da conta e clique no link dentro da mensagem para ativar sua conta. Depois da ativação da conta, você pode gerenciar remotamente o recurso de segurança ESET Anti-Theft dos dispositivos conectados por meio do portal ESET HOME. Se você já tem uma conta ESET HOME, toque em **Entrar** e digite seu email e senha. Assim que essas etapas estiverem completas, você pode associar o dispositivo com sua conta ESET HOME.

Para mais orientações sobre como usar os recursos do ESET Anti-Theft, consulte o [guia do usuário Anti-Theft](#) ou toque no ícone de **Ajuda** no canto superior direito do portal ESET HOME.

## ESET HOME senha

### Altere sua senha esquecida:

1. Visite <https://login.eset.com/LostPassword>.
2. Insira o endereço de e-mail que você usou para se registrar no ESET HOME e clique em **Enviar**.
3. Entre na sua conta de e-mail, abra o e-mail **Redefinição de senha da conta ESET HOME** e clique no link no e-mail.
4. Digite e confirme uma nova senha e clique em **Confirmar alteração**.

5. Insira a nova senha no seu dispositivo e toque em **Desbloquear** para desbloquear seu dispositivo.

## Altere sua senha ESET HOME:

1. Vá para o site [ESET HOME](#).
2. Entre usando seu endereço de e-mail e senha atual.
3. Clique no seu e-mail ao lado da seta para baixo  no canto superior direito.
4. Clique em **Alterar senha**.
5. Digite sua senha atual.
6. Digite sua nova senha e confirme.
7. Clique em **Salvar alterações**.

## Antiphishing

Phishing descreve uma atividade criminal que envolve manipular usuários para que eles forneçam informações confidenciais em um site que parece verdadeiro mas não é. Esse tipo de manipulação é conhecida como engenharia social. O phishing é utilizado frequentemente para obter acesso a dados confidenciais como números de contas bancárias, números de cartões de pagamento, PINs ou nomes de usuários e senhas.

O Antiphishing no ESET Mobile Security protege contra sites considerados maliciosos ou perigosos.

Recomendamos manter o **Antiphishing** ativado. Quando está ativado, todos os potenciais ataques de phishing que vêm de sites ou domínios listados no banco de dados de malware da ESET serão bloqueados e uma notificação de alerta será exibida informando sobre a tentativa de ataque.

O Antiphishing pode ser integrado com os navegadores e aplicativos de redes sociais mais comuns disponíveis no sistema operacional Android. O Chrome e navegadores padrão que vêm pré-instalados em dispositivos Android (normalmente chamados de *Internet* ou *Navegador*). Outros navegadores podem estar listados como Desprotegidos, pois eles não fornecem integração suficiente para o Antiphishing. Para usar totalmente a funcionalidade Antiphishing, recomendamos não usar navegadores incompatíveis.



Para a integração Antiphishing adequada com navegadores da web, recomendamos usar o Android 6 (Marshmallow) ou uma versão posterior.

**Melhorar funcionalidade** – o ESET Mobile Security avisa você se a Proteção Antiphishing exigir permissões adicionais concedidas pelo sistema operacional Android. Toque em **Permitir** para abrir as configurações de Acessibilidade do sistema e considere que as opções disponíveis fornecem suporte a mais navegadores e ativar a proteção ao navegar no modo privado (anônimo). Se não quiser que esse problema seja reportado como um problema, toque em **Ignorar este problema (não recomendado)**.

Para desativar o Antiphishing, toque nos três pontos  na seção Antiphishing e toque em **Desativar**.

## Permitir a permissão de acessibilidade no ESET Mobile Security instalado

## do arquivo .APK no Android 13

### Observação

Por motivos de segurança, o Android 13 restringe o uso de permissões de acessibilidade para aplicativos instalados de arquivos .apk para impedir o acesso desinformado a essas permissões.

#### **i** Como o ESET Mobile Security usa essas permissões

Usamos essa permissão para acessar os URLs dos sites que você visitar. Analisamos esses sites para fins maliciosos, como phishing, malware ou outras atividades perigosas.

O site é bloqueado quando uma ameaça é detectada para proteger você e seus dados sensíveis.

Os dados acessados através da permissão de acessibilidade não são compartilhados com terceiros.

Para resolver o problema de acessibilidade:

### Habilitar permissões de acessibilidade

**i** Para as instruções ilustradas, leia nosso [artigo da base de conhecimento](#) (pode estar disponível apenas em inglês).

1. Abra **Configurações > Acessibilidade > Fazer download de aplicativos** e o ESET Mobile Security está indisponível.
2. Toque no aplicativo ESET Mobile Security e a caixa de diálogo **Configuração restrita** será aberta.
3. Toque em **'OK'**.
4. Vá para **Configurações > Aplicativos > ESET Mobile Security** para abrir as **Informações do aplicativo**.
5. Toque no ícone de três pontos do menu  no canto superior direito > **Permitir configurações restritas**.

As configurações restritas agora estão permitidas e você pode [começar a usar o aplicativo com segurança](#).

### **i** Antiphishing no Samsung DeX

O Antiphishing não é compatível com dispositivos conectados à estação Samsung DeX.

## Navegadores protegidos

- Chrome
- Chrome Beta
- Firefox
- Firefox Beta
- Opera
- Opera Beta
- Opera Mini
- Opera Mini Beta
- Navegador Opera TV

- Internet Samsung
- Mint
- Navegador Yandex
- DuckDuckGo (no ESET Mobile Security versão 6.1 e versões posteriores)
- Navegador Kiwi
- Edge
- Silk em dispositivos da Amazon
- Navegador Mi
- Navegador Xiaomi Mi
- Vewd no Android TV

### **Aplicativos de redes sociais protegidos**

- Facebook
- Facebook Lite
- Messenger
- Messenger Lite
- Instagram
- Aplicativos de rede social que usam componentes de navegador protegidos para visualização da web também estão protegidos.

## **Proteção de notificação e SMS**

A Proteção de notificação e SMS protege você contra esse smishing.

O smishing vem da combinação das palavras phishing e SMS (Serviço de mensagem curta). As vezes, isso pode ser chamado de phishing por SMS. Os agressores usam mensagens de SMS, já que as pessoas não confiam nas mensagens mais do que no e-mail.

A proteção por SMS protege você contra smishing transmitido por meio de mensagem SMS. Mas a ameaça também pode ser transmitida por qualquer plataforma de envio de mensagens. É aqui onde a Proteção de notificação entra. Quando você recebe um SMS ou uma notificação (por exemplo, depois de receber uma mensagem do Whatsapp), o ESET Mobile Security analisa o link. Com base na análise, existem três possíveis resultados:

- Nenhuma ameaça encontrada.
- Conteúdo potencialmente indesejado é encontrado. O conteúdo da mensagem ou notificação pode não representar um risco direto. A intenção não é tão inequivocamente maliciosa quanto outros tipos de malware,

como vírus ou trojan. Porém, ele pode instalar software indesejado adicional, alterar o comportamento do dispositivo digital ou realizar atividades não aprovadas ou esperadas pelo usuário.

- Conteúdo perigoso encontrado. Esta mensagem ou notificação contém links perigosos ou de phishing. Recomendamos que você não abra o conteúdo e remova a mensagem ou notificação.

### Removendo mensagens e notificações



Por motivos de segurança, o ESET Mobile Security não consegue remover mensagens e notificações para você. Você precisa remover o conteúdo perigoso manualmente.

## Como o smishing funciona

1. Um invasor envia uma mensagem contendo um link para um site.
2. O link normalmente leva a um site de phishing que pode tentar fazer você fornecer suas informações pessoais. Elas podem ser usadas, por exemplo, para roubar dinheiro de você ou cometer outras fraudes. O link também pode levar a um site malicioso que contém malware ou tenta enganar você para que o malware seja baixado.

## Sinais de smishing

- Um número de telefone suspeito, por exemplo, um número estrangeiro ou com comprimento não padrão.
- A mensagem contém arquivos ou links desconhecidos.
- Mensagens smishing geralmente têm um tom urgente.
- Mensagens smishing muitas vezes agem como se tivessem informações sobre prêmios.

## Bloqueio de aplicativo

O Bloqueio de aplicativo permite que você proteja o acesso a aplicativos selecionados (emails, mensagens, agenda, etc.) com um código PIN ou impressão digital. O Bloqueio de Aplicativo impede o acesso não autorizado a aplicativos selecionados mesmo quando o dispositivo está desbloqueado.

### Recomendação



Ativar as permissões de **Sobreposição (Aplicativos que podem aparecer no topo)** para o ESET Mobile Security para uma melhor funcionalidade.

Para configurar o Bloqueio de aplicativo no seu dispositivo:

1. Toque em **Bloqueio de aplicativo** na tela principal do ESET Mobile Security.
2. Toque em **Ativar**.
3. Habilite a permissão de acesso de Uso e clique em **Continuar**.
4. Digite seu PIN, que desbloqueia os aplicativos.
5. Confirme seu PIN digitando-o novamente.

6. Toque em um aplicativo para bloquear ou desbloquear.

## Definir as configurações do Bloqueio de aplicativo

Para acessar as configurações do Bloqueio de aplicativo, abra o menu  no canto superior direito e clique em **Configurações**:

- **Bloquear novos aplicativos** - Quando o Bloqueio de aplicativo está ativado, depois de instalar um novo aplicativo vamos perguntar se você deseja bloquear o novo aplicativo.
- **Bloquear aplicativo novamente** - Você pode configurar o Bloqueio de aplicativo para bloquear um aplicativo imediatamente quando ele for fechado, depois da tela desligar ou depois de um minuto ter passado.
- **Tipo de bloqueio** - Você pode bloquear seu aplicativo usando o PIN ou um padrão.
- **Desbloqueio com impressão digital** - Essa opção só está disponível se uma impressão digital verificada está salva em seu dispositivo. Quando ativado, você pode desbloquear aplicativos usando a impressão digital salva no seu dispositivo. Você ainda conseguirá desbloquear o aplicativo usando o PIN. Para isso, toque em **Usar PIN** ao abrir um aplicativo bloqueado.
- **Alerta de intruso** - Depois de uma série de tentativas mal sucedidas de desbloqueio, o ESET Mobile Security tira uma foto do intruso. A foto é exibida depois do próximo desbloqueio bem sucedido do aplicativo.

## Desativar Bloqueio de aplicativo

1. Vá para o recurso de Bloqueio de aplicativo no ESET Mobile Security.
2. Digite o PIN do seu Bloqueio de aplicativo.
3. Toque no menu  no canto superior direito.
4. Toque em **Desativar**.

## Ativar o Modo noturno

Você pode ativar o Modo noturno na Tela de bloqueio do seu aplicativo para que a experiência seja mais agradável para seus olhos tocando no ícone do modo noturno no canto superior direito.

## Esqueci meu PIN de Bloqueio de aplicativo

Se você esquecer o PIN do Bloqueio de aplicativo e não tiver uma impressão digital salva no seu dispositivo, você tem duas opções para desbloquear um aplicativo bloqueado, dependendo das suas configurações do Anti-Theft:

- Se você ativou o recurso Anti-Theft no ESET Mobile Security:
  1. Abrir ESET Mobile Security.
  2. Vá para o recurso Bloqueio de aplicativo.
  3. Digite seu PIN. **Toque em Esqueceu seu PIN?** no meio da tela.

4. Se o recurso Anti-Theft estiver ativo, será solicitado que você digite sua senha ESET HOME. Digite a senha no campo **Senha** e toque em **Enter**.

5. Digite seu novo PIN e toque em  para confirmar.

6. Digite o mesmo PIN novamente para confirmar. Toque em  quando terminar.

- Se você não ativou o recurso Anti-Theft, [desinstale o ESET Mobile Security](#) e instale-o novamente.

## Proteção de pagamento



A Proteção de pagamento é uma camada adicional projetada para proteger seus dados financeiros em dispositivos Android contra o phishing avançado e outras ameaças. A Proteção de pagamento impede que outros aplicativos percebam a inicialização de seus aplicativos protegidos, além de evitar que eles substituam informações ou leiam informações na tela do seu aplicativo protegido. A proteção de pagamento escaneia todos os aplicativos que estão em sua lista de aplicativos protegidos. Depois de ativar a Proteção de pagamento, você vai adicionar automaticamente alguns aplicativos de operações bancárias e pagamentos na lista de aplicativos protegidos.

### Adicionar um novo aplicativo à lista de aplicativos protegidos

1. Abra a Proteção de pagamento no menu Aplicativos ou no ESET Mobile Security.
2. Toque em **Gerenciar**.
3. Selecione os aplicativos que deseja proteger com a Proteção de pagamento.
4. Toque em **OK** para confirmar sua seleção.

### Abrir um aplicativo de atividade bancária e pagamento usando a Proteção de pagamento

Para garantir a maior proteção de seus aplicativos bancários e de pagamento, abra esses aplicativos no Iniciador Seguro. O Iniciador seguro fornece uma camada adicional de proteção em comparação com a proteção padrão do recurso de Proteção de pagamento ao abrir o aplicativo fora do Iniciador seguro.

O Iniciador seguro é criado automaticamente quando a Proteção de pagamento é ativada. O Iniciador seguro contém todos os aplicativos que estão protegidos pela Proteção de pagamento.

### O que é o Iniciador seguro e como posso acessá-lo?

Você pode encontrar o Iniciador seguro na sua lista de aplicativos  ou em ESET Mobile Security > Proteção de pagamento .

#### Acessar o Iniciador seguro

- i** Para um acesso mais rápido e fácil aos seus aplicativos bancários e de pagamento, você pode adicionar o Iniciador Seguro à sua tela inicial. Para adicionar um Iniciador seguro na sua tela inicial, pressione o ícone do Iniciador seguro e arraste-o para sua tela inicial.

# Filtro de Chamadas

O **Filtro de Chamadas** bloqueia chamadas enviadas ou recebidas com base nas regras definidas.

Notificações de chamada não serão exibidas quando uma chamada recebida é bloqueada. Veja o **Relatório de chamada** para verificar chamadas que possam ter sido bloqueadas por engano.

**Bloquear o Último que Liguei** - toque para bloquear chamadas recebidas do último número de telefone recebido. Isto irá criar uma nova regra.

## Regras

Para criar uma nova regra, toque no ícone +. Consulte [o próximo capítulo](#) para mais informações.

Para modificar uma regra existente, toque na entrada da regra na lista de regras. Para remover uma entrada da lista de **Regras**, selecione a entrada e toque em **Remover**.

## Relatório de chamada

A seção **Relatório de chamada** exibe o relatório de todas as chamadas bloqueadas pelo Filtro de Chamadas. Cada relatório contém o nome da chamada, o número de telefone correspondente e a data e a hora do evento.

### Dispositivos sem cartão SIM

O **Filtro de Chamadas** não funciona em dispositivos que não suportam chamadas e mensagens.

### Chamadas enviadas

O Filtro de chamadas não está bloqueando chamadas enviadas no ESET Mobile Security obtido por meio do Google Play.

### Suporte para Android

O Filtro de chamadas está disponível apenas em dispositivos com Android 6 ou versões posteriores.

## Bloquear números de telefone usando caracteres curinga

Você pode bloquear um intervalo de números usando caracteres curinga como descrito na tabela abaixo:

Caractere curinga	Descrição
*	representa vários caracteres
?	representa um único caractere

### Exemplo

 Se você não quiser receber chamadas de um país específico, digite o código do país e o caractere curinga \* no campo **Número de celular** e todas as chamadas recebidas do país que comecem com esse padrão de número são bloqueadas. Quando você decidir excluir algum número de telefone desse país, [adicione uma nova regra](#) com a ação **Permitir**. A imagem abaixo mostra como bloquear todas as chamadas da Eslováquia.

O Que

Bloquear ▼

---

Quem

Pessoa ▼

Nome

Nome (opcional) + 

Número de telefone

+421\* 

---

Quando

Sempre ▼

**SALVAR**

## Adicionar uma nova regra

Para criar uma nova regra, toque no ícone +.

1. Na seção **O que**, selecione ou **Bloquear** ou **Permitir** para especificar o tipo de regra para chamadas e mensagens. Selecione a direção das chamadas a serem bloqueadas (Recebidas está selecionado por padrão).

2. Na seção **Quem**, selecione uma opção para especificar os números de telefone que serão afetados pela regra.

- **Pessoa** - Selecione uma pessoa da sua lista de contatos, ou adicione o nome e os números manualmente. Você pode atribuir mais números de telefone a um nome clicando no botão + na seção **Número de telefone**.
- **Grupo** - O ESET Mobile Security reconhecerá os grupos de contato salvo em seus Contatos (por exemplo Família, Amigos ou Trabalho).

- **Todos os números desconhecidos** incluirá todos os números de telefone não salvos na sua lista de contatos. Use essa opção para bloquear chamadas indesejadas (por exemplo, ligações de telemarketing) ou para evitar que crianças disquem números desconhecidos.
- **Todos os números conhecidos** incluirá todos os números de telefone salvos na sua lista de contatos.
- **Todos os números** vai bloquear todas as chamadas recebidas.
- **Números restritos** serão aplicados para ligações de pessoas que ocultaram seu número de telefone deliberadamente pelo recurso de restrição de identificação da linha chamadora.

3. Na seção **Quando**, selecione **Sempre** ou **Personalizado** para especificar o intervalo de tempo e os dias da semana em que a regra terá efeito. Por padrão, sábado e domingo estão selecionados.

Visite esse [artigo da Base de conhecimento](#) para instruções ilustradas.

### Filtro de chamada no exterior

- i** Se você estiver no exterior, insira todos os números de telefone na lista com o código de discagem internacional seguido pelo número propriamente dito (por exemplo, +1610100100).

## Inspetor de rede

O Inspetor de rede permite que você escaneie sua rede em busca de dispositivos conectados ao seu roteador e busque vulnerabilidades. O Casa conectada escaneia sua rede em duas etapas.

Primeiro o Inspetor de rede escaneia sua rede em busca de dispositivos conectados. Se um novo dispositivo for descoberto, você verá uma notificação e o dispositivo será marcado com um símbolo de estrela. Descubra dispositivos manualmente na sua rede tocando em **Escanear rede**. Também é possível descobrir dispositivos automaticamente. Para usar essa opção, toque no ícone de menu  > **Configurações** e ative a opção **Descobrir dispositivos automaticamente**.

Na segunda etapa do escaneamento, o Inspetor de rede testa os dispositivos conectados em busca de vulnerabilidades, conectando-se a eles e verificando a existência de vulnerabilidades como portas abertas, nome de usuário e senha de roteador fracos, problemas no firmware do roteador, etc. Essas vulnerabilidades podem ser usadas por atacantes para obter controle do seu roteador e de outros dispositivos conectados a ele. Roteadores e dispositivos controlados por atacantes podem ser usados para coletar informações sobre você, ou para participar de ataques de negação de serviço distribuídos (DDoS), etc.

O Inspetor de rede também oferece a você uma lista abrangente de dispositivos conectados à sua rede para mantê-lo informado sobre quem está conectado à sua rede. Com base nessas informações você pode gerenciar ou negar o acesso desses dispositivos à sua rede da interface web do roteador. A interface web do seu roteador pode ser acessada diretamente do Inspetor de rede, selecionando o roteador e tocando na opção **Abrir interface da web**.

Você pode ver os dispositivos conectados como uma lista ou de forma visual:

- Exibição em lista  - Os dispositivos conectados são exibidos em uma exibição em lista padrão com o Roteador em cima seguido pelos dispositivos on-line, terminando com o histórico de dispositivos conectados anteriormente.
- Exibição sonar  - Os dispositivos são exibidos de forma visual em um meio-círculo com o roteador no

centro. Na segunda camada do centro são exibidos os dispositivos que estão on-line no momento. A terceira camada exibe um histórico dos dispositivos conectados anteriormente. Você pode alternar entre os dispositivos tocando nos botões de setas ou rolando para dentro do círculo.

Para um gerenciamento mais fácil, atribua uma categoria aos dispositivos (como Smartphone, TV, Console de jogo, Computador, etc.), renomeie o dispositivo de forma diferente do nome ou endereço IP padrão do fabricante para nomes mais fáceis de identificar (por exemplo: SM-G955F para o telefone de Sam, 192.168.1.52 para o computador de João, etc.).

Para renomear os dispositivos no Inspetor de rede, toque no ícone do dispositivo no Casa conectada > toque no ícone de lápis no canto superior direito, selecione a categoria do dispositivo, digite o nome do dispositivo e toque em **OK**.

## Auditoria de segurança

A Auditoria de segurança ajuda você a monitorar e alterar configurações importantes do dispositivo. Revise as permissões dadas para cada aplicativo instalado em seu dispositivo para impedir riscos de segurança.

Para ativar ou desativar a Auditoria de segurança e seus componentes específicos, toque no botão do menu  e toque em **Desativar monitoramento do dispositivo** ou **Desativar auditoria do aplicativo**.

- [Monitoramento do dispositivo](#)
- [Auditoria do Aplicativo](#)

## Monitoramento do dispositivo

Na seção **Monitoramento do dispositivo**, defina quais componentes do dispositivo serão monitorados pelo ESET Mobile Security.

Toque em cada opção para ver sua descrição detalhada e status atual. Nas opções **Fontes desconhecidas** e **Modo de depuração**, toque em **Abrir configurações** para alterar as configurações nas **Configurações do sistema operacional Android**.

Você pode desativar cada componente.

1. Toque no componente que deseja desativar.
2. Toque no ícone do menu .
3. Toque em **Desativar**.

## Auditoria do Aplicativo

A Auditoria de aplicativo realiza uma auditoria de aplicativos instalados no seu dispositivo que podem ter acesso a serviços que cobram, rastreiam sua localização ou leem suas informações de identidade, contatos ou mensagens de texto. O ESET Mobile Security fornece uma lista desses aplicativos separados em categorias. Toque em cada

categoria para ver sua descrição detalhada. Toque em um aplicativo para ver seus detalhes de permissão.

## Códigos de indicação

### Importante



Este recurso está disponível apenas para usuários que fizeram o download do ESET Mobile Security do Google Play e não têm a licença na versão premium ativada.

Seu código de indicação é um número único que é atribuído ao seu dispositivo. Compartilhe e receba códigos de indicação para obter uma licença versão premium gratuita do ESET Mobile Security por até um ano.

Compartilhe seu código de indicação com um amigo e ambos receberão uma licença premium gratuita por 30 dias. Se o seu amigo não tiver o ESET Mobile Security, ele receberá um link de download único para o ESET Mobile Security incluindo uma licença premium gratuita de 30 dias.

Cada vez que você compartilhar um código de indicação você receberá uma licença premium gratuita de 30 dias e um troféu virtual para ajudá-lo a acompanhar quantos códigos você compartilhou e recebeu. Cada troféu virtual representa uma licença premium gratuita de 30 dias. Você pode compartilhar até 12 códigos de indicação para receber licenças gratuitas. Depois de receber todos os 12 troféus virtuais, você ainda pode compartilhar seu código com seus amigos que continuarão a receber licenças premium gratuitas de 30 dias, mas você não receberá licenças gratuitas adicionais.



## Indique um amigo

Você pode compartilhar o ESET Mobile Security e ajudar a proteger seus amigos tocando no ícone  **Menu principal** e selecionando **Indicar um amigo**.

Toque no botão **Compartilhar**.

Selecione seu método de compartilhamento preferido e compartilhe seu código de indicação com seus amigos.

## Resgatar código

Na primeira vez que você receber um código de indicação de um amigo, você pode resgatá-lo para receber uma licença versão premium gratuita por 30 dias para você e seu amigo. Você só pode resgatar um código de indicação por vez para receber uma licença premium gratuita por 30.

Para usar o código recebido:

1. navegue para o **Menu principal** .
2. Selecione **Resgatar código**.

Digite o código de indicação que você receber de seu amigo no campo de texto e toque em **Enter**.

Você e o amigo que compartilhou o código vão receber uma confirmação em seus respectivos dispositivos.

Se você tiver mais códigos (além de Códigos de indicação) toque em **Desbloquear outro mês**.

## Configurações

Para acessar as configurações do programa, toque no Menu  na tela principal ESET Mobile Security (ou pressione o botão Menu no seu dispositivo) e toque em **Configurações**.

### Backup e restauração

O ESET Mobile Security permite a você criar um arquivo de backup contendo suas configurações do ESET Mobile Security. Você pode fazer download desse arquivo para um dispositivo externo e usá-lo para restaurar suas configurações do ESET Mobile Security.

### Idioma

Por padrão, o ESET Mobile Security é instalado no idioma definido como padrão do sistema no seu dispositivo (nas configurações de idioma e teclado do sistema operacional Android). Para alterar o idioma da interface de usuário do aplicativo, toque em **Idioma** e selecione o idioma desejado.

### Notificação permanente

(Esta opção está disponível apenas para Android 7 e versões posteriores)

O ESET Mobile Security exibirá uma notificação na parte de baixo da barra de notificação do Android. Se não quiser que a notificação seja exibida, desmarque Notificação permanente e toque em Desativar.

### Consentimento do usuário

- **Permitir ESET LiveGrid®** – para ler mais sobre o sistema de feedback **ESET LiveGrid®**, [visite a seção Configurações avançadas](#).
- **Permitir análise para ajudar a tornar nossos produtos melhores** – o ESET Mobile Security enviará informações anônimas do aplicativo (desempenho, estatísticas operacionais) que vão nos ajudar a melhorar nossos aplicativos e serviços. Para ler mais sobre as informações que coletamos, visite o capítulo [Política de privacidade](#).
- **Permitir o uso de dados para fins de marketing**
- **Permitir o envio de descontos promocionais e novidades sobre produtos da ESET** – você receberá novidades no produto e as ofertas mais recentes da ESET.

## Atualização

Para ter o máximo de proteção, é importante usar a versão mais recente do ESET Mobile Security. Toque em **Atualizar** para ver se há uma nova versão disponível para download no site da ESET. Esta opção não está disponível se você fez o download do ESET Mobile Security a partir do Google Play - neste caso, o produto é atualizado a partir do Google Play.

## Desinstalar

Executar o assistente de desinstalação vai remover o ESET Mobile Security permanentemente do dispositivo. Se a proteção Anti-Theft estiver ativada, você precisará inserir sua senha/padrão de segurança do ESET Mobile Security ou impressão digital. Para desinstalar o produto manualmente, siga [as etapas descritas nesta seção](#).

### Proteção contra desinstalação

A Proteção contra desinstalação não está ativa no Android versões 7.0 e versões posteriores.

## Atendimento ao cliente

Os especialistas de atendimento ao cliente ESET estão disponíveis para ajudar caso você precise de assistência administrativa ou suporte técnico relacionado ao ESET Mobile Security ou a qualquer outro produto ESET.

 [Entre em contato com o Atendimento ao Cliente da ESET.](#)

Para enviar uma solicitação de atendimento diretamente de seu dispositivo:

1. Toque no Menu  na tela principal ESET Mobile Security (ou pressione o botão Menu no seu dispositivo).
2. Toque em **Atendimento ao cliente**.
3. Toque em **Atendimento ao cliente** para criar uma solicitação de suporte técnico.
4. Preencha todos os campos obrigatórios. O ESET Mobile Security inclui a funcionalidade de registro em relatório avançado para ajudar a diagnosticar possíveis problemas técnicos.
5. Para fornecer para a ESET um relatório detalhado do aplicativo, certifique-se de que **Enviar relatório do aplicativo** está selecionado (padrão).
6. Toque em **Enviar** para enviar sua solicitação.
7. Um especialista de Atendimento ao cliente ESET vai entrar em contato no endereço de email fornecido.

### Não foi possível abrir o aplicativo ou ele não está respondendo



Para enviar uma solicitação de suporte para a ESET se o ESET Mobile Security não estiver respondendo ou abrindo, vá para **Configurações > Aplicativos > ESET Mobile Security > Armazenamento > Gerenciar armazenamento**. Clique em **Atendimento ao cliente** e preencha todos os campos obrigatórios.

# 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 dos 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.

**Códigos.** Provisões adicionais são aplicáveis ao Código da seguinte forma:

A ESET pode criar e fornecer códigos de indicação e/ou outros códigos para fins promocionais ou de marketing (doravante os "Códigos") a seu critério. É possível resgatar o Código para prolongar o prazo da licença de acordo com este Contrato. A ESET reserva o direito de desativar o Código a qualquer momento quando o Código for obtido ou usado de uma forma que não esteja de acordo com este Contrato e/ou em caso de crença razoável do envolvimento de erro, fraude ou atividade ilegal. Você é obrigado a cumprir as seguintes restrições:

- i. Você não pode resgatar o Código mais de uma vez.
- ii. Você não pode vender, arrendar ou alugar o Código ou usar o Código para a prestação de serviços comerciais.
- iii. Você concorda que a ESET pode desativar o fornecimento e/ou uso do Código a qualquer momento sem

qualquer responsabilidade para a ESET.

iv. Você concorda que o Código não é válido para troca por dinheiro ou qualquer outra compensação.

v. Você concorda que o Código e/ou o uso do Código pode ser sujeito a termos especiais fornecidos pela ESET para a campanha específica de indicação, promoção e/ou marketing.

EULAID: EULA-PRODUCT-LG-EMS; 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 incluímos 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 você criar a Conta ESET HOME no <https://home.eset.com> e marcar seu dispositivo como perdido através da função Anti-Theft, as informações a seguir serão coletadas e processadas: os dados de localização, capturas de tela, dados sobre a configuração de um computador e dados registrados pela câmera de um computador. Os dados coletados são armazenados em nossos servidores ou nos servidores de nossos prestadores de serviço, com um período de retenção de 3 meses.

**Análise de uso e de travamento.** Com base em seu consentimento ao entrar, coletaremos e analisaremos dados relacionados ao uso de nossos produtos para testar seu desempenho e aprimorá-los para nossos usuários. Os dados coletados podem incluir várias ações e eventos de usuários acontecendo no produto (por exemplo, lançamento do aplicativo, atualização de aplicativo, duração da sessão, compra no aplicativo), informações sobre um dispositivo, plataforma ou sistema operacional usado, bem como dados relacionados à sua idade, sexo, localização e interesses, que podem estar associados a vários identificadores (por exemplo, IDs de instalação). Além disso, processaremos dados técnicos relacionados a falhas do aplicativo (como informações do dispositivo, identificador de instalação, traços da falha, minidespejo de falha) para obter uma visão das falhas, aprender sobre suas causas e garantir que nosso produto está totalmente operacional. Para coletar e analisar esses dados, usamos nosso Programa de melhoria da experiência do cliente (onde apenas dados de telemetria anônimos são

processados) e os serviços Google para obter uma visão mais aprofundada. Para mais informações sobre o tratamento de seus dados pelo Google, consulte a [Política de Privacidade do Google](#) relevante.

**Tratamento para fins de marketing.** Se você escolher nos conceder seu consentimento para fins de marketing, Nós e nossos parceiros de marketing vamos usar os dados sobre seu uso de nosso produto para avaliar o desempenho de nossas atividades de marketing on-line, entender melhor seus interesses e mostrar a Você anúncios on-line que devem ser mais relevantes para você. Os dados coletados podem incluir várias ações e eventos de usuários acontecendo no produto (por exemplo, lançamento do aplicativo, atualização de aplicativo, duração da sessão, compra no aplicativo), informações sobre um dispositivo, plataforma ou sistema operacional usado, bem como dados relacionados à sua idade, sexo, localização e interesses, que podem estar associados a vários identificadores (por exemplo, IDs de instalação, ID de anúncio móvel). Usamos o Google para coletar e analisar esses dados para nós. Para mais informações sobre o tratamento de seus dados pelo Google, consulte a [Política de Privacidade do Google](#) relevante.

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