ESET MOBILE SECURITY para Android

Guia do Usuário

(destinado ao produto versão 3.5 e posterior)

Clique aqui para fazer download da versão mais recente deste documento

ESET MOBILE SECURITY

O ESET Mobile Security foi desenvolvido pela ESET, spol. s r.o. Para obter mais informações, visite www.eset.com.br.

Atendimento ao Cliente: http://support.eset.com/

REV. 30. 1. 2017

Índice

1. Introdução 4
   - 1.1 Novidades da versão 3.5 4
   - 1.2 Requisitos mínimos do sistema 4
2. Instalação 4
   - 2.1 Download do Google Play 5
   - 2.2 Download do site da ESET 5
   - 2.3 Assistente inicial 6
3. Desinstalação 9
4. Ativação do produto 9
5. Antivírus 10
   - 5.1 Rastreamentos automáticos 12
   - 5.2 Logs de rastreamento 13
   - 5.3 Configurações avançadas 14
6. Antifurto 15
   - 6.1 Portal da Web 16
     - 6.1.1 Otimização 17
     - 6.1.2 Proteção proativa 17
   - 6.2 Proteção SIM 17
     - 6.2.1 Cartões SIM confiáveis 18
     - 6.2.2 Contatos confiáveis 18
   - 6.3 Comandos de Texto por SMS 19
   - 6.4 Configurações 20
     - 6.4.1 Senha de segurança 20
     - 6.4.2 Detalhes de contato 20
7. Antiphishing 21
8. SMS & Filtro de Chamadas 22
   - 8.1 Permissões 22
     - 8.1.1 Adicionar uma nova regra 23
   - 8.2 Histórico 23
9. Auditoria de segurança 23
   - 9.1 Monitoramento do Dispositivo 24
   - 9.2 Auditoria de Aplicativo 25
10. Relatório de segurança 26
11. Configurações 27
12. Atendimento ao cliente 28

1. Introdução

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

Os recursos principais incluem:

- Antivírus
- Antifurto
- Antiphishing
- Integração com o portal My Eset
- SMS & filtro de chamada
- Auditoria de segurança
- Relatório de segurança

1.1 Novidades da versão 3.5

As atualizações e melhorias a seguir foram introduzidas no ESET Mobile Security versão 3.5:

- Proteção proativa
- Antiphishing aprimorado
- Relatório de segurança
- As permissões do sistema podem ser acessadas com facilidade a partir de ESET Mobile Security
- Localização mais recente do dispositivo salva no ESET Antifurto antes do dispositivo ficar sem bateria

1.2 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 4 (Ice Cream Sandwich) ou posterior
- Resolução da tela de toque: mínimo 480x800 px
- CPU: ARM com conjunto de instrução ARMv7+, x86 Intel Atom
- RAM: 128 MB
- Espaço livre de armazenamento interno: 20 MB
- Conexão com a Internet

OBSERVAÇÃO: Dispositivos com SIM duplo e root não são compatíveis. O Antifurto e Filtro de Chamadas e SMS não estão disponíveis em tablets que não suportam chamadas e mensagens.

2. Instalação

O ESET Mobile Security está disponível para download nesses canais de distribuição:

Google Play - este aplicativo recebe atualizações regulares através do Google Play

Site ESET - este aplicativo recebe atualizações do sistema de verificação de atualizações versão ESET

Amazon Appstore

Para proteger suas informações pessoais e os recursos do seu dispositivo Android, o ESET Mobile Security precisará acessar as funções do seu dispositivo e, em alguns casos, tomar controle delas. Para explicações detalhadas sobre

cada tipo de permissão e como elas são usadas, veja a tabela neste artigo da Base de conhecimento:
http://support.eset.com/kb2711/#PrivacyPolicy
(O artigo não está disponível em todos os idiomas.)

2.1 Download do Google Play

Abra o aplicativo do Google Play Store no seu dispositivo Android e faça uma busca por ESET Mobile Security (ou apenas ESET).

Alternativamente, siga o link ou leia o código QR abaixo usando seu dispositivo móvel e um aplicativo de leitura de QR:

Google play https://play.google.com/store/apps/details?id=com.eset.ems2.gp

2.2 Download do site da ESET

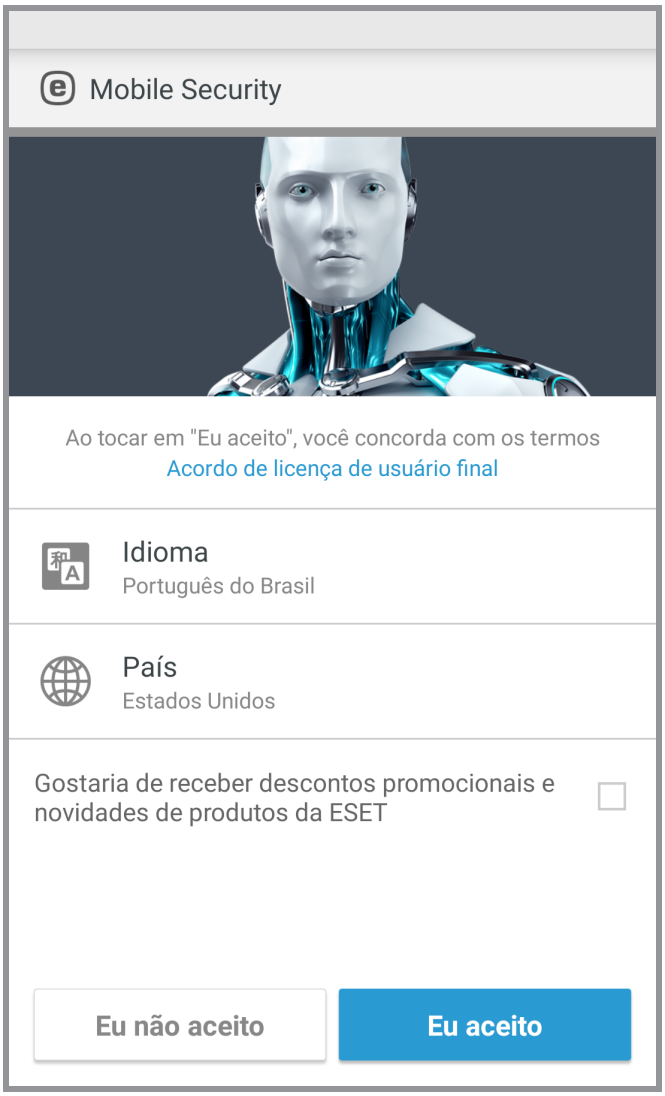
A disponibilidade da versão da web varia dependendo de sua região.

1. Download do arquivo de instalação APK do site ESET.
2. Certifique-se de que os aplicativos de fontes desconhecidas são permitidos no seu dispositivo. Para isso, toque no ícone do Iniciador na tela inicial do Android (ou vá para Início > Menu). Toque em **Configurações** > **Segurança**. A caixa de seleção ao lado de **Recursos desconhecidos** deve ser selecionada.
3. Abra o arquivo a partir da área de notificação do Android ou localize-o usando um navegador de arquivos. O arquivo normalmente é guardado na pasta Download.
4. Toque em **Instalar** e depois em **Abrir**.

2.3 Assistente inicial

Quando o aplicativo estiver instalado, siga os avisos na tela do assistente inicial:

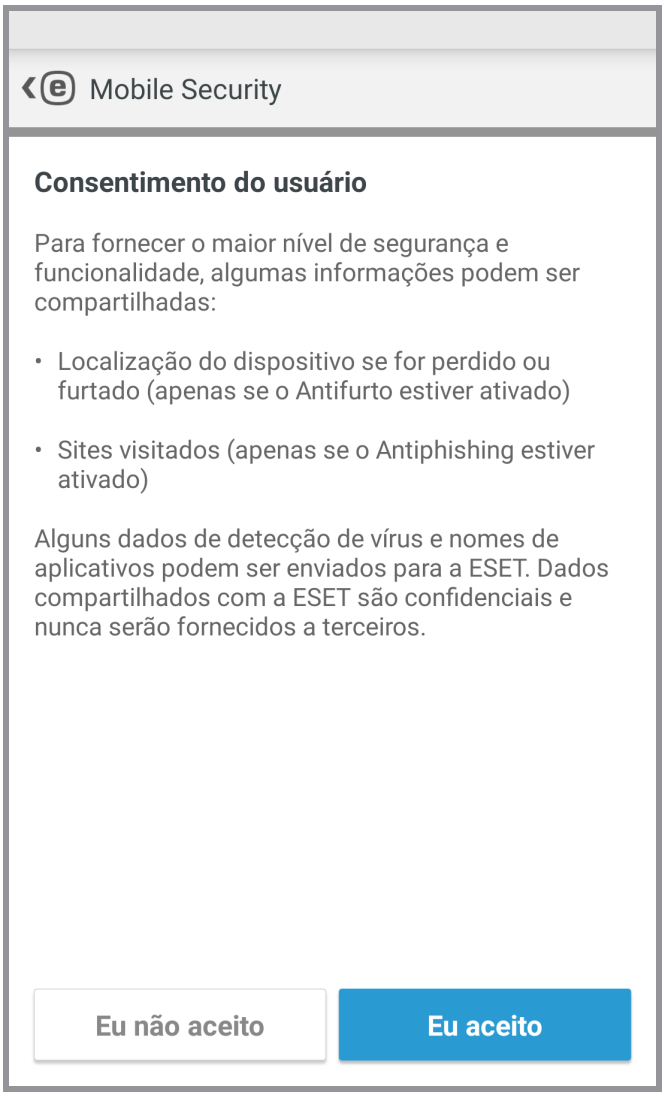
1. Toque em **Idioma** para selecionar o idioma que você quer usar no ESET Mobile Security. Isto pode ser alterado posteriormente nas configurações do programa.



2. Toque em **País** para selecionar o país onde você vive atualmente.

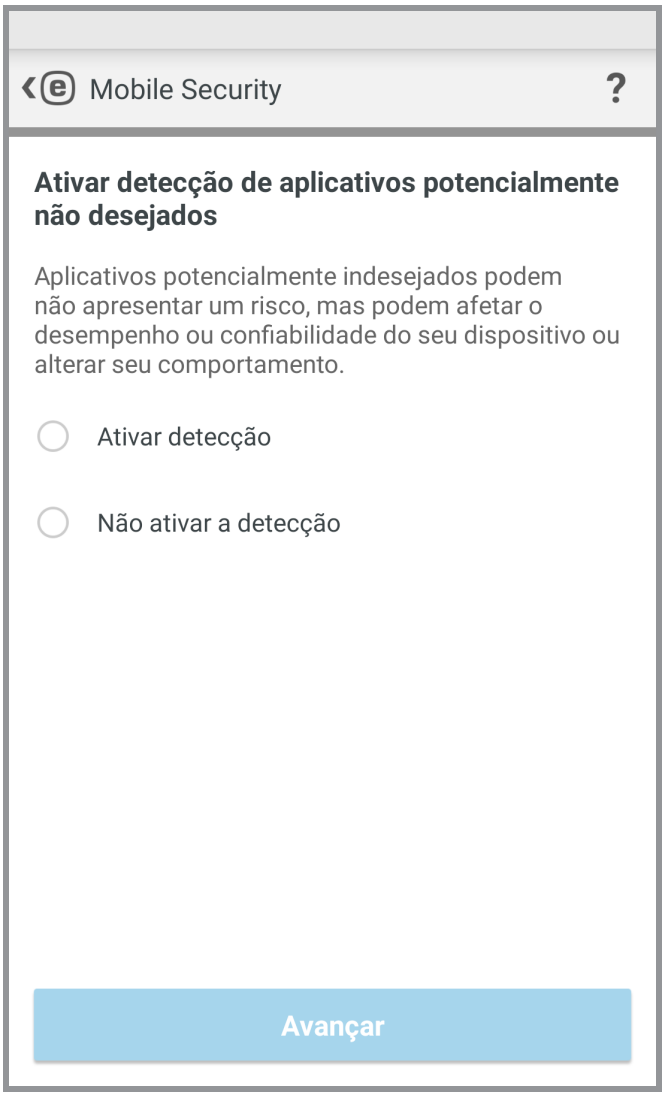
3. Toque em **Aceitar** para concordar com o Contrato de Licença de Usuário Final.

4. Toque em **Aceitar** na tela de **Consentimento do usuário**. Algumas informações como localização do dispositivo e sites visitados podem ser compartilhadas com a ESET.



5. Toque em **Avançar**se quiser participar do **ESET Live Grid**. Isto pode ser alterado posteriormente nas configurações do programa. Para ler mais, veja esta seção.

6. Selecione **Ativar detecção** ou **Não ativar detecção** para determinar se o ESET Mobile Security vai detectar Aplicativos potencialmente indesejados (PUAs), em seguida toque em **Avançar**. Isto pode ser alterado posteriormente nas configurações do programa. Para mais detalhes sobre PUAs, consulte esta seção.



7. Na próxima etapa, você verá uma lista de todas as contas de email disponíveis no seu dispositivo. Selecione a conta que você quer que a ESET use para comunicação sobre o registro da licença do produto, informações de redefinição de senha de segurança e comunicações do Atendimento ao cliente ESET. Se não houver conta de email listada, toque em **Adicionar Conta** > **OK** > **Existente** para entrar na sua conta de email existente ou toque em **Nova** para criar uma nova.

8. Toque em **Ativar** para ativar os recursos premium do produto ou toque em **Ignorar** para começar a usar a versão gratuita.

3. Desinstalação

O ESET Mobile Security pode ser desinstalado usando o assistente de Desinstalação disponível no menu principal do programa. Toque em Menu  > **Configurações** > **Desinstalar**. Será solicitado que você insira sua Senha de segurança.

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

1. Toque no ícone do Iniciador  na tela inicial do Android (ou vá para Início > Menu) e toque em **Configurações** > **Segurança** > **Administradores do dispositivo**. Selecione ESET Mobile Security e toque em **Desativar**. Digite **Desbloquear** e insira sua Senha de segurança. Você pode ignorar esta etapa se o aplicativo não estiver mais definido como o administrador do Dispositivo.
2. Volte para **Configurações** e toque em **Gerenciar apps** > ESET Mobile Security > **Desinstalar**.

4. Ativação do produto

O ESET Mobile Security tem três versões disponíveis:

- Gratuito - recursos básicos de uso gratuito por tempo ilimitado
- Avaliação - recursos premium ativados por um tempo limitado (30 dias por padrão)
- Premium - recursos premium são ativados até sua licença expirar

Esta tabela indica quais recursos estão disponíveis nas versões Gratuito, Avaliação e Premium:

	Gratuito	Avaliação e Premium
Antivírus	✔	
Antivírus - rastreamentos automáticos		✔
Atualizações automáticas de banco de dados de vírus		✔
Antifurto - comandos SMS (exceto Apagar)	✔	
Antifurto - portal da web		✔
Antifurto - Proteção SIM		✔
Antiphishing		✔
SMS & filtro de chamada		✔
Auditoria de segurança		✔
Relatório de segurança	✔	

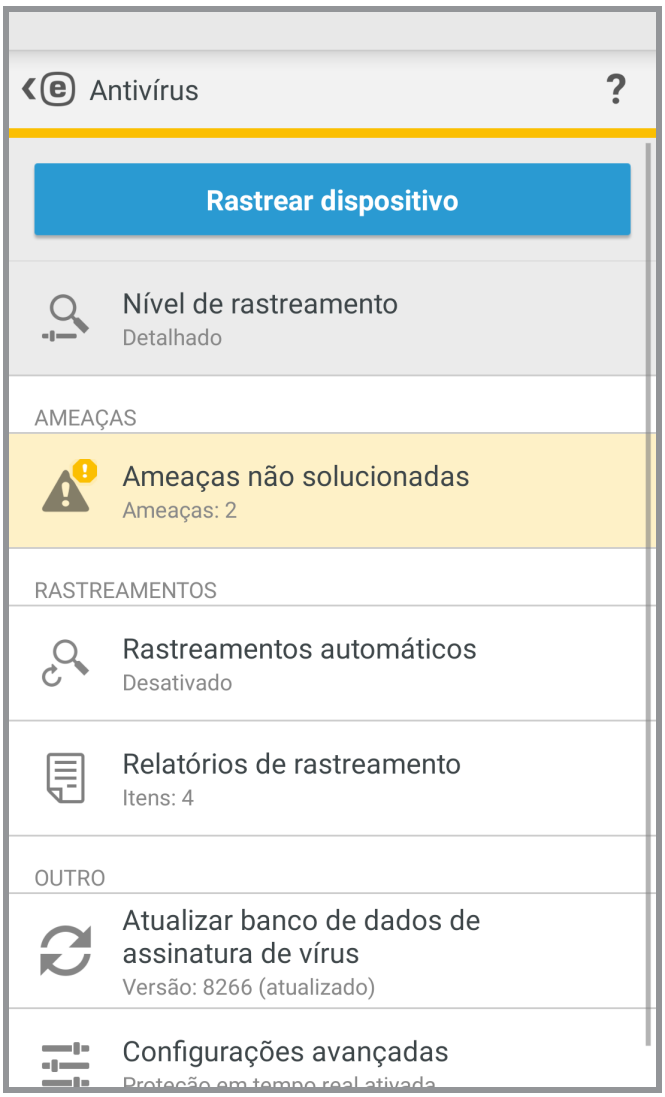
Para ativar o ESET Mobile Security diretamente no seu dispositivo Android, toque em Menu  na tela principal ESET Mobile Security (ou pressione o botão **MENU** no seu dispositivo) e toque em **Licença**.

Há várias maneiras de ativar o ESET Mobile Security. A disponibilidade de um método específico de ativação pode variar conforme sei país, assim como os meios de distribuição (página da web da ESET, Google Play, Amazon Appstore).

- **Comprar premium** - selecione esta opção se você não tem uma licença e deseja adquirir uma através do Google Play.
- **Digite uma Chave de licença** - selecione esta opção se você já tem uma chave de licença. Uma chave de licença é uma string única formatada: XXXX-XXXX-XXXX-XXXX-XXXX que é usado para identificar o proprietário da licença. Ela pode ser encontrada no email que você recebeu da ESET ou no cartão de licença incluído na caixa de compra.
- **Ativar Avaliação Gratuita**- selecione esta opção se quiser avaliar o ESET Mobile Security antes de realizar uma compra. Isso só pode ser feito uma vez por conta do Google.
- **Eu tenho um Usuário e Senha, o que faço?** - selecione esta opção para converter seu Nome de usuário e Senha para uma Chave de licença em https://my.eset.com/convert

5. Antivírus

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



Rastrear dispositivo

Alguns tipos de arquivo predefinidos são rastreados por padrão. Um rastreamento do dispositivo verifica a memória, os processos em execução e as bibliotecas de links dependentes, assim como os arquivos que fazem parte dos armazenamentos interno e removível. Um breve resumo do rastreamento será salvo em um arquivo de relatório disponível na seção Relatórios de rastreamento. Se quiser anular o rastreamento já em andamento, toque em  .

Nível de rastreamento

Há dois níveis de rastreamento para escolher:

- **Inteligente** - O rastreamento Inteligente vai rastrear aplicativos instalados, arquivos DEX (arquivos executáveis para o sistema operacional Android), arquivos SO (bibliotecas), arquivos com uma profundidade máxima de rastreamento de 3 arquivos compactados e o conteúdo do cartão SD.
- **Detalhado** - O rastreamento detalhado vai rastrear todos os tipos de arquivo independentemente de sua extensão na memória interna e no cartão SD.

Atualizar banco de dados de assinatura de vírus

Por padrão, o ESET Mobile Security inclui uma tarefa de atualização a fim de garantir que o programa seja atualizado regularmente. Para executar a atualização manualmente, toque em **Atualizar banco de dados de assinatura de vírus**.

OBSERVAÇÃO: Para evitar a utilização desnecessária da largura de banda, as atualizações são lançadas apenas quando necessário, ou seja, quando surge uma nova ameaça. As atualizações são fornecidas gratuitamente, mas a operadora poderá cobrar pela transferência de dados.

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

- Rastreamentos automáticos
- Logs de rastreamento
- Configurações avançadas

5.1 Rastreamentos automáticos

Além do rastreamento de Dispositivo acionado manualmente, o ESET Mobile Security também oferece rastreamentos automáticos.

Nível de rastreamento

Há dois níveis de rastreamento para escolher. Esta configuração é aplicável ao Rastreamento no carregador e Rastreamento Programado:

- **Inteligente** - O rastreamento Inteligente vai rastrear aplicativos instalados, arquivos DEX (arquivos executáveis para o sistema operacional Android), arquivos SO (bibliotecas), arquivos com uma profundidade máxima de rastreamento de 3 arquivos compactados e o conteúdo do cartão SD.
- **Detalhado** - O rastreamento detalhado vai rastrear todos os tipos de arquivo independentemente de sua extensão na memória interna e no cartão SD.

Rastreamento no carregador

Quando isto estiver selecionado, um rastreamento 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.

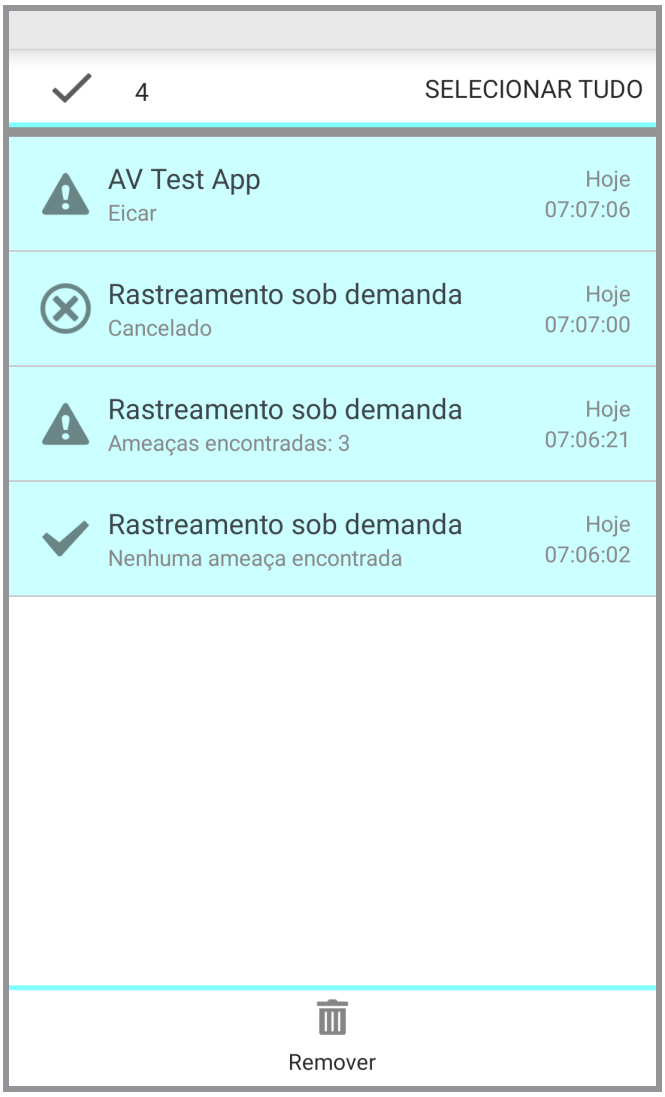
5.2 Logs de rastreamento

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

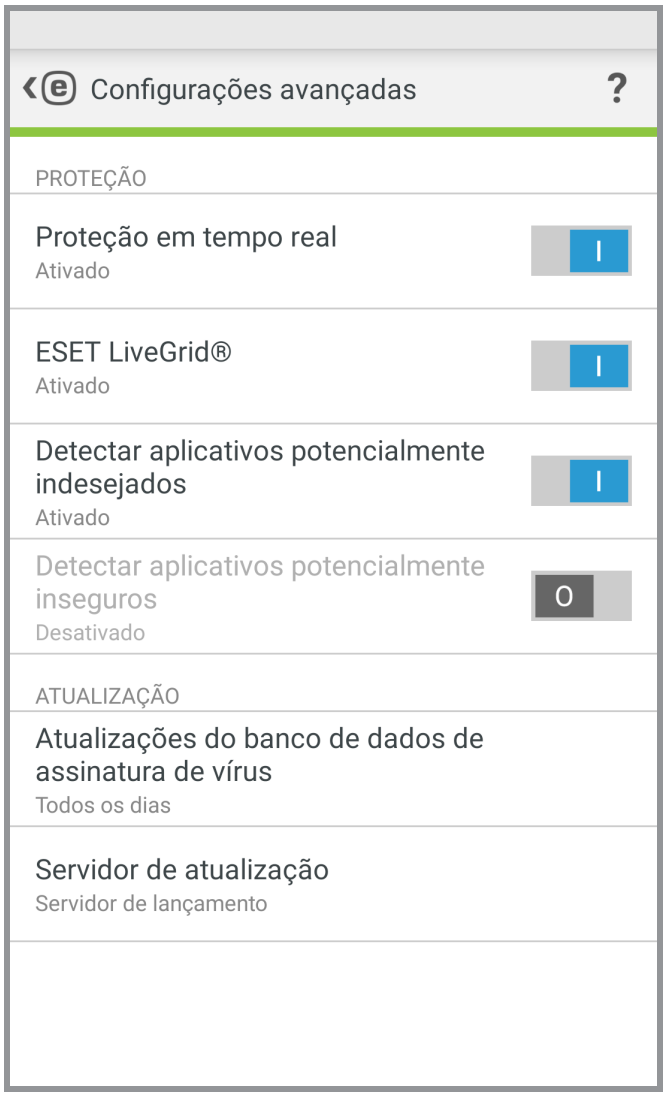
Cada relatório contém:

- 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

Para remover um relatório da lista, toque e segure para selecioná-lo e toque em Remover .



5.3 Configurações avançadas



Proteção em tempo real

O rastreamento em tempo real é iniciado automaticamente na inicialização do sistema e rastreia os arquivos com os quais você interage. Rastreia automaticamente a pasta *Download* e os aplicativos instalados ou atualizados.

ESET Live Grid

Criado a partir do sistema de alerta antecipado avançado *ThreatSense.Net*, o ESET Live Grid é projetado para fornecer ao seu dispositivo níveis adicionais de segurança. Ele monitora constantemente os programas em execução no sistema e processa com relação à inteligência mais recente coletada de milhões de usuários do ESET em todo o mundo. Além disso, os rastreamentos são processados com mais rapidez e precisão conforme o banco de dados do ESET Live Grid cresce ao longo do tempo. Isso nos permite oferecer proteção proativa e velocidade de rastreamento melhores para todos os usuários ESET. Recomendamos que você ative este recurso. Obrigado pelo seu apoio.

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. Existem algumas situações em que você pode sentir que os benefícios do aplicativo potencialmente indesejado superam os riscos. Por isso a ESET atribui a estes aplicativos uma categoria de risco menor em comparação com outros tipos de software malicioso.

Detectar aplicativos potencialmente inseguros

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

Atualizações do banco de dados de assinatura de vírus

Esta opção permite definir o intervalo de tempo para o download automático do banco de dados de ameaças. Essas atualizações são lançadas apenas quando necessário, ou seja, quando surge uma nova ameaça ao banco de dados. Recomendamos que você deixe essa configuração no valor padrão (diariamente).

Servidor de atualização

Esta opção permite a você escolher atualizar seu dispositivo a partir do **servidor de pré-lançamento**. Atualizações em modo de teste são atualizações que passaram por testes internos e estarão disponíveis ao público geral em breve. Você pode se beneficiar do acesso aos métodos de detecção e correções mais recentes. No entanto, o modo de teste pode não ser sempre estável. Para verificar as versões dos módulos de programa atuais, toque no Menu  na tela principal ESET Mobile Security e toque em **Sobre** > **ESET Mobile Security**. Se o usuário tiver apenas conhecimentos básicos, é recomendando deixar a opção **Servidor de lançamento** selecionada por padrão.

6. Antifurto

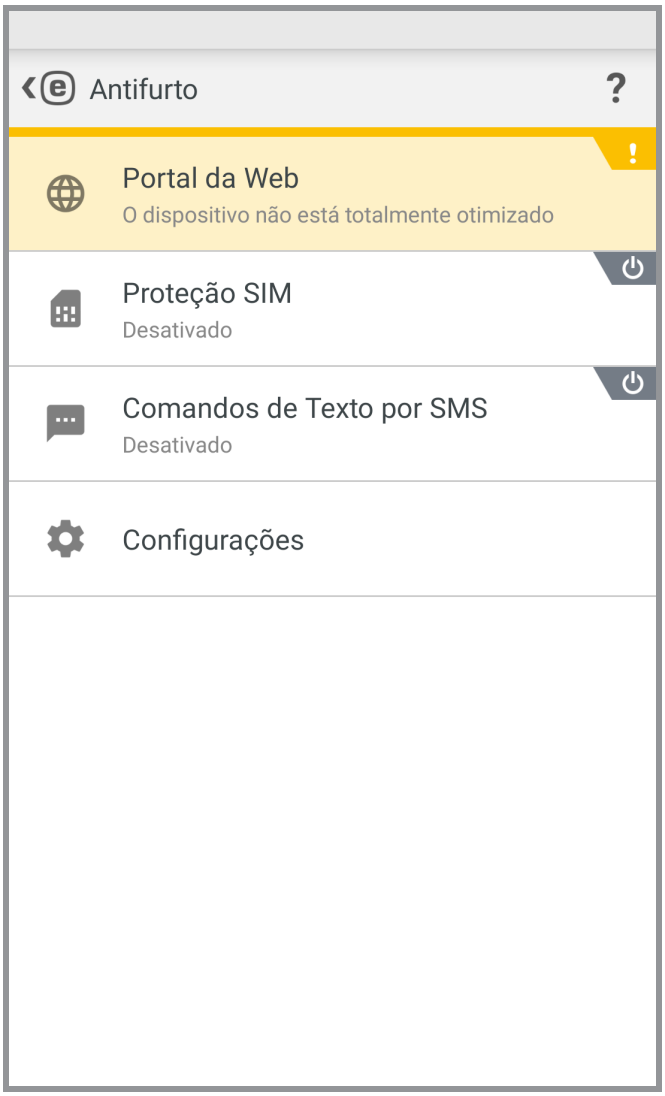
A funcionalidade **Antifurto** protege seu dispositivo móvel contra o acesso não autorizado.

Se você perder seu aparelho ou alguém roubá-lo e substituir seu cartão SIM por um cartão novo (não confiável), o dispositivo será bloqueado automaticamente pelo ESET Mobile Security e um SMS de alerta será enviado para o(s) número(s) de telefone definido(s) pelo usuário. Essa mensagem incluirá o número de telefone do cartão SIM inserido no momento, o número IMSI (International Mobile Subscriber Identity, identidade internacional de assinante móvel) e o número IMEI (International Mobile Equipment Identity, identidade internacional de equipamento móvel) do telefone. O usuário não autorizado não terá conhecimento do envio desta mensagem porque ela será automaticamente excluída das sequências de mensagens do seu aparelho. Você também pode solicitar coordenadas de GPS do dispositivo móvel perdido ou apagar remotamente todos os dados armazenados no dispositivo.

OBSERVAÇÃO: Certos recursos do Antifurto (Cartões SIM confiáveis e Comandos de Texto por SMS) não estão disponíveis em dispositivos que não tem suporte para mensagens de texto.

6.1 Portal da Web

A Versão 3 do ESET Mobile Security é integrada completamente com a proteção Antifurto ESET através do portal My Eset. Do portal 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 My ESET, 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. Agora você pode aproveitar gerenciar os recursos de segurança do Antifurto do my.eset.com. Se você já tem uma conta My ESET, toque em **Entrar** e digite seu email e senha. Assim que essas etapas estiverem completas, você pode associar o dispositivo com sua conta My ESET.

Para mais orientações sobre como usar os recursos do Antifurto no portal My ESET, consulte a ajuda on-line Antifurto ou toque em **Ajuda** no canto superior direito da tela.

Localização mais recente - este recurso salva a localização do dispositivo no ESET Antifurto antes do dispositivo ficar sem bateria.

6.1.1 Otimização

A otimização do ESET Antifurto é uma avaliação técnica mensurável do estado de segurança de seu dispositivo. A proteção Antifurto examinará seu sistema quanto aos 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 este 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 são usados** - acesse essa configuração nas configurações Android > **Localização** > **Modo** > **Alta precisão**
- **Bloqueio de tela desprotegido** - para proteger o seu dispositivo com um código de bloqueio de tela, senha, PIN ou padrão, vá para as Configurações Android > **Bloquear tela** > **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 Antifurto irá notificá-lo sobre a atividade suspeita no portal My Eset.
- **Dados móveis não ativados** - acesse essa configuração nas configurações Android > **Sem fio e Redes** > **Redes móveis** > **Dados**.
- **Serviços Google Play não estão presentes** - O ESET Antifurto usa os serviços do Google Play para fornecer comandos ao seu dispositivo em tempo real e exibir notificações de push. Se esses serviços estiverem desativados ou faltando em seu dispositivo, as funções do ESET Antifurto gerenciadas a partir do My Eset serão limitadas. Neste caso recomendamos usar os Comandos por SMS no lugar do portal My Eset.

6.1.2 Proteção proativa

Este recurso permite a você ajustar os alertas e atividades acionados pelo modo Suspeito, onde o ESET Mobile Security salva regularmente a localização do dispositivo, fotos da câmera e endereços IP do WiFi. Você pode definir o seguinte:

- **Ativado quando a tentativa de desbloqueio falha** - ativado por padrão, bloqueia o dispositivo quando um código incorreto de desbloqueio de tela é inserido
- **Número máximo de tentativas falhas de desbloquear** - número de tentativas de desbloquear permitidas
- **Tempo para correção** - por padrão, você tem 15 segundos para inserir o código de desbloqueio correto
- **Salvar fotos no dispositivo** - salva as fotos da câmera traseira e dianteira na sua Galeria do dispositivo e no portal Antifurto no caso de uma tentativa falha de desbloqueio ou remoção do cartão SIM

6.2 Proteção SIM

Para começar a usar a Proteção SIM, toque em **Antifurto** > **Proteção SIM** no menu principal do programa e depois toque na chave  para ativar o recurso. Um assistente simples vai orientá-lo pela configuração. Essas etapas também podem ser acessadas através do assistente de configuração dos comandos de mensagens de texto SMS:

- Digitar uma Senha de segurança
- Adicionar Detalhes de contato
- Habilitar proteção contra desinstalação
- Salve um cartão SIM atual como um cartão SIM confiável
- Adicionar um Contato confiável

6.2.1 Cartões SIM confiáveis

A seção **SIM Confiável** mostra a lista de cartões SIM que serão aceitos pelo ESET Mobile Security. Se você inserir um cartão SIM não definido nesta lista, a tela será bloqueada e um SMS de alerta será enviado para os Contatos confiáveis.

Para adicionar um novo cartão SIM, toque em  . Digite um **NOME PARA O CARTÃO SIM** (por exemplo, casa, trabalho) e seu número IMSI (International Mobile Subscriber Identity). O IMSI (International Mobile Subscriber Identity) normalmente é apresentado como um número de 15 dígitos impresso no seu cartão SIM. Em alguns casos, ele pode ser mais curto.

Para remover um cartão SIM da lista, selecione o cartão SIM e toque em  .

OBSERVAÇÃO: O recurso de cartão SIM Confiável não está disponível em dispositivos CDMA, WCDMA e somente Wi-Fi.

6.2.2 Contatos confiáveis

Na seção Contatos confiáveis você pode adicionar ou remover números de telefone de seus amigos ou familiares que serão capazes de:

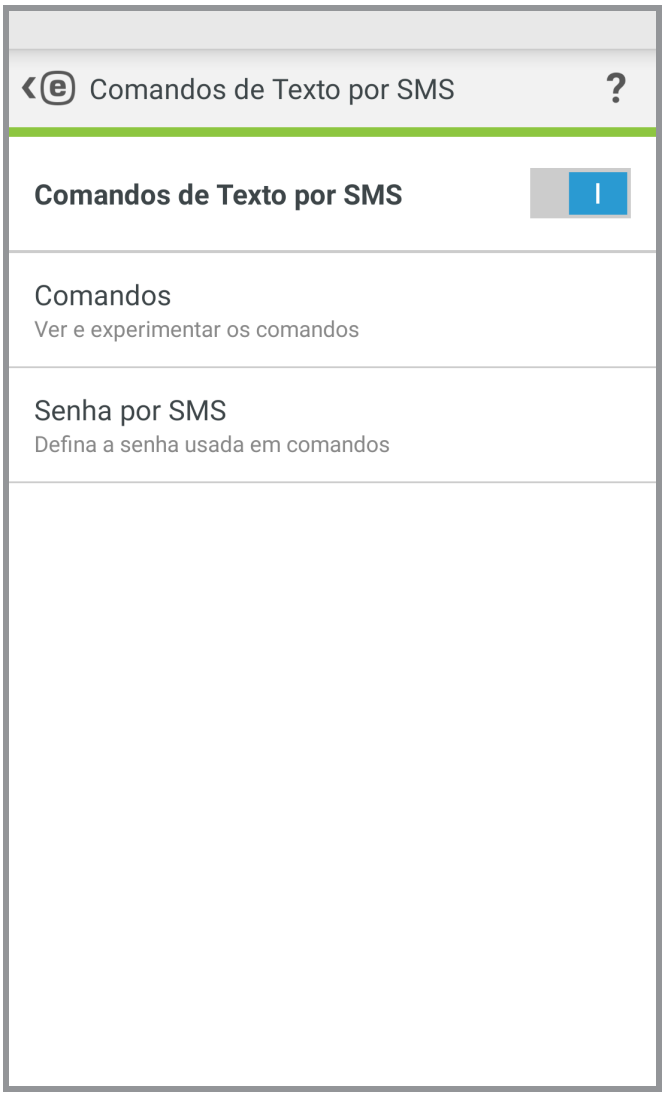
- Receber um SMS de alerta depois de detectar um cartão SIM não autorizado no seu dispositivo
- Redefinir sua Senha de segurança (desde que a opção **Permitir redefinição remota da Senha de segurança** esteja ativada para este contato)

Para adicionar um novo Contato confiável, toque em  e digite o nome do amigo e número do celular, ou toque em para selecionar um contato da lista de Contatos do seu telefone. Para remover um Contato confiável, selecione a entrada e toque em Remover  .

Se uma entrada de Contato confiável tiver mais de um número de telefone, o SMS de alerta e redefinição de senha vão funcionar com todos os números associados.

OBSERVAÇÃO: 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).

6.3 Comandos de Texto por SMS



Para começar a usar comandos por mensagens de texto SMS, toque em **Antifurto** > **Comandos de Texto por SMS** no menu principal do programa e depois toque na chave para ativar o recurso. Se você já concluiu o assistente Proteção SIM, esta configuração só vai solicitar que você adicione um parâmetro adicional - a senha SMS. A Senha de segurança pode ser usada para isso, mas não é recomendado que isso seja feito já que a senha SMS será visível na tela do dispositivo em mensagens que chegam.

Os comandos SMS a seguir podem ser enviados:

Desbloquear
`eset remote reset`
Envie este comando do dispositivo de um amigo confiável para desbloquear a tela do seu dispositivo.

Bloquear
`eset lock senha`
Isto vai bloquear o dispositivo - será possível desbloquear usando a senha de segurança.

Tocar alarme
`eset siren senha`
Um alarme alto vai começar a tocar mesmo se o dispositivo estiver configurado como silencioso.

Localizar
`eset find senha`
Você receberá uma mensagem de texto com as coordenadas de GPS do dispositivo de destino, incluindo um link para esse local no Google Maps. O dispositivo enviará uma nova SMS se um local mais preciso estiver disponível depois de um determinado tempo.

Apagar
`eset wipe senha`
Todos os contatos, mensagens, emails, contas, conteúdo do cartão SD, imagens, músicas e vídeos armazenados nas pastas padrão serão permanentemente apagados do dispositivo. O ESET Mobile Security continuará instalado.

OBSERVAÇÃO: Apesar dos comandos de SMS não serem sensíveis a maiúsculas e minúsculas, a senha precisa ser digitada exatamente como foi definida no assistente de configuração do Antifurto.

6.4 Configurações

Na seção de Configurações do Antifurto, acesse o seguinte:

- Senha de segurança
- Detalhes de contato

6.4.1 Senha de segurança

Sua **Senha de segurança** é necessária para desbloquear seu dispositivo, acessar o Antifurto, desinstalar o ESET Mobile Security ou enviar comandos de texto SMS (desde que essa opção tenha sido ativada ao criar uma senha SMS).

Se você esquecer a Senha de segurança, tente as opções a seguir:

- Enviar uma mensagem de texto de um número de celular de um Contato confiável para o seu número. A mensagem deve estar na forma: eset remote reset
- Se o seu dispositivo estiver conectado na Internet, solicite um código de redefinição de senha tocando em **Email** no seu dispositivo bloqueado. Um email contendo o código de verificação será entregue para a conta de email do Google definida durante a instalação. Digite o código de verificação e a nova senha na tela bloqueada.
- Redefina a senha no portal My Eset. Depois de entrar, selecione seu dispositivo, clique em **Configurações** e digite uma nova senha.
- Se o seu dispositivo não estiver conectado na Internet, preencha o formulário neste artigo da Base de conhecimento.
- Entre em contato com o Atendimento ao Cliente da ESET se você não conseguir enviar os dados supracitados.

IMPORTANTE: Para criar uma senha segura que será mais difícil de adivinhar, use uma combinação de letras minúsculas, letras maiúsculas e números.

6.4.2 Detalhes de contato

Se um dispositivo for marcado como perdido no my.eset.com, as informações dos **Detalhes de contato** serão exibidas na tela do seu dispositivo bloqueado para ajudar o localizador a entrar em contato com você.

Estas informações podem incluir:

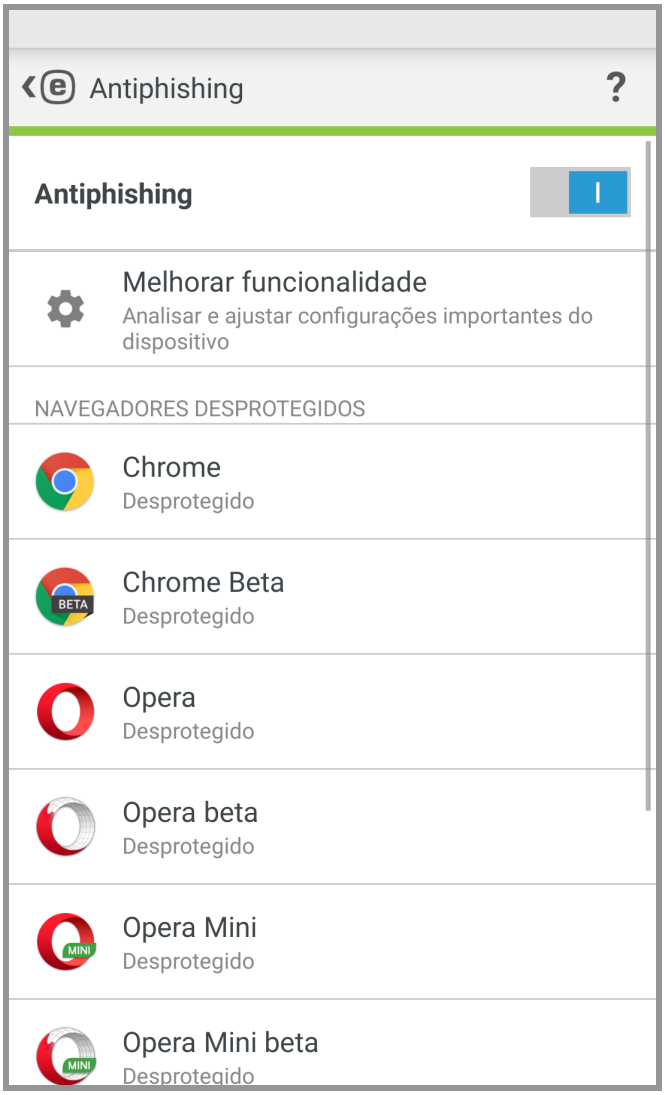
- Seu nome (opcional)
- Número de celular de backup de um membro da família ou amigo
- Descrição do dispositivo (opcional)
- Endereço de e-mail (opcional)

7. Antiphishing

O termo *phishing* define uma atividade criminal que usa engenharia social (a manipulação de usuários a fim de obter informações confidenciais). O roubo de identidade é utilizado frequentemente para obter acesso a dados confidenciais como números de contas bancárias, números de cartões de crédito, números de PIN ou nomes de usuários e senhas.

Recomendamos manter o **Antiphishing** 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 mais comuns disponíveis no sistema operacional Android - Chrome e navegadores padrão que vêm pré-instalados em dispositivos Android (normalmente chamados de *Internet* ou *Navegador*). Outros navegadores podem estar listados como Desprotegidos, já que eles não fornecer integração suficiente para o Antiphishing. Para aproveitar ao máximo a funcionalidade do Antiphishing, recomendamos que você não use os navegadores não compatíveis.



Melhorar funcionalidade - O ESET Mobile Security avisa se a sua Proteção Antiphishing precisar de mais permissões concedidas pelo sistema operacional Android. Toque em **Permitir** para abrir as configurações de Acessibilidade do sistema e considere as opções disponíveis para fornecer suporte a mais navegadores e ativar a proteção quando o navegador estiver no modo privado (incógnito). Se não quiser que esse problema seja reportado como um problema, toque em **Ignorar este problema (não recomendado)**.

8. SMS & Filtro de Chamadas

O **SMS e Filtro de Chamadas** bloqueia mensagens SMS/MMS recebidas e chamadas recebidas/realizadas de acordo com as regras definidas pelo usuário.

Mensagens indesejadas geralmente incluem anúncios de operadoras ou mensagens de usuários desconhecidos ou indeterminados. Notificações não serão exibidas quando uma mensagem ou chamada recebida é bloqueada. Veja a seção Histórico para verificar chamadas ou mensagens que possam ter sido bloqueadas por engano.

OBSERVAÇÃO: O SMS e Filtro de Chamadas não funciona em tablets que não suportam chamadas e mensagens. Filtros SMS/MMS não estão disponíveis em dispositivos Android OS 4.4 e versões posteriores e serão desativados em dispositivos onde o Google Hangouts é definido como o principal aplicativo de SMS.

8.1 Permissões

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

Para criar uma nova regra, toque em **Regras** > **Adicionar regra**. Consulte o próximo capítulo para mais informações.

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

8.1.1 Adicionar uma nova regra

1. Na seção **Ação**, selecione ou **Bloquear** ou **Permitir** para especificar o tipo de regra para chamadas e mensagens.
2. Na seção **Quem**, selecione uma opção para especificar os números de telefone que serão afetados pela regra.
   - **Pessoa**
   - **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.
   - **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 **O que**, selecione o tipo de chamada ou mensagem de texto que deve ser bloqueado ou permitido:
    chamadas enviadas
    chamadas recebidas
    mensagens de texto (SMS) recebidas ou
    mensagens multimídia (MMS) recebidas
4. 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.

OBSERVAÇÃO: 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).

8.2 Histórico

A seção **Histórico** exibe o registro em relatório de chamadas e mensagens bloqueadas pelo Filtro de Chamadas e SMS. Cada relatório contém o nome do evento, o número de telefone correspondente e a data e a hora do evento. Os registros de mensagens SMS e MMS também preservam o corpo da mensagem.

Para remover uma entrada da lista, selecione a entrada e toque em Remover  .

9. Auditoria de segurança

A Auditoria de segurança ajuda você a monitorar e alterar configurações importantes do dispositivo e revisar permissões de aplicativos instalados para impedir riscos de segurança.

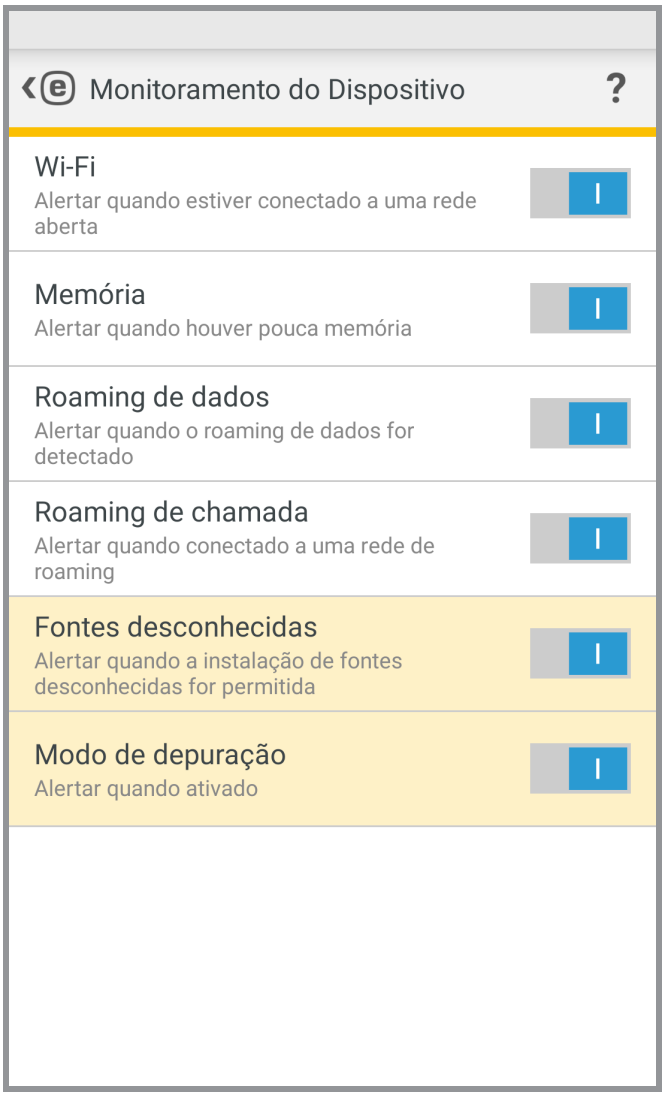
Para ativar ou desativar a Auditoria de segurança e seus componentes específicos, toque em  .

- Monitoramento do dispositivo
- Auditoria do Aplicativo

9.1 Monitoramento do Dispositivo

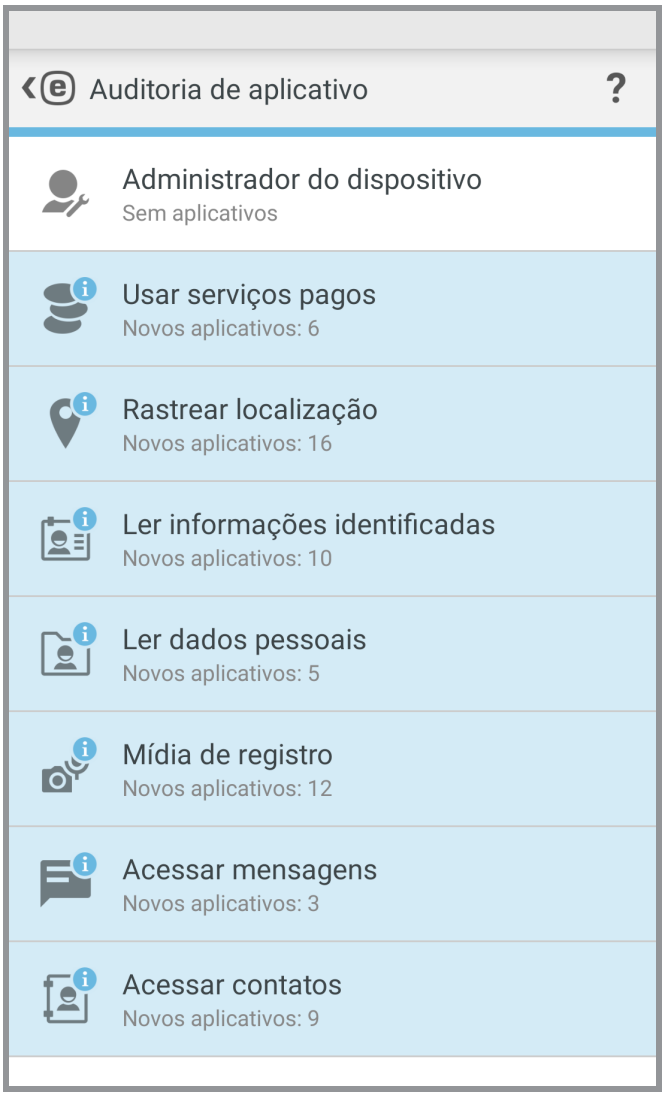
Na seção **Monitoramento do dispositivo**, defina quais componentes do dispositivo serão monitorados pelo ESET Mobile Security.

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.



9.2 Auditoria de 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.



10. 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 sendo usados na tela do Relatório de segurança. Cada seção de módulo do programa contém as informações a seguir.

Antivírus:

- Aplicativos instalados
- Atualizar aplicativo
- Aplicativos rastreados
- Ameaças detectadas
- Atualizações do banco de dados de assinatura de vírus

Antifurto

Antiphishing:

- Sites rastreados
- Ameaças detectadas

Filtro de Chamadas e SMS:

- Chamadas enviadas
- Chamadas recebidas
- Chamadas bloqueadas

Auditoria de segurança:

- Alertas de roaming
- Avisos de WiFi aberta

Ative a opção **Notificação de relatório mensal** para exibir uma mensagem breve na barra de notificação Android. Toque na notificação para abrir a janela do **Relatório de segurança**.

11. 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**.

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

O ícone ESET Mobile Security será exibido no canto superior esquerdo da tela (barra de status do Android). Se você não deseja que esse ícone seja exibido, desmarque **Notificação permanente** e toque em **Desativar**.

Ofertas especiais

Você receberá notícias no produto e as ofertas mais recentes da ESET.

Atualização

Para 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 remove permanentemente o ESET Mobile Security do dispositivo. Se a Proteção contra desinstalar foi ativada, você precisará digitar a Senha de segurança. Para desinstalar o produto manualmente, siga as etapas descritas nesta seção.

12. 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.

Para entrar em contato com o Atendimento ao Cliente da ESET, siga este link.

Para enviar uma solicitação de atendimento diretamente de seu dispositivo, toque no Menu na tela principal do ESET Mobile Security (ou pressionando o botão Menu no seu dispositivo), toque em **Atendimento ao cliente** > **Atendimento ao Cliente** e preencha todos os campos obrigatórios. O ESET Mobile Security inclui funcionalidades de registro em relatório avançado para ajudar a diagnosticar problemas técnicos em potencial. Para fornecer para a ESET um relatório detalhado do aplicativo, certifique-se de que **Enviar relatório do aplicativo** está selecionado (padrão). Toque em **Enviar** para enviar sua solicitação. Um Especialista de Atendimento ao Cliente ESET vai entrar em contato com você no endereço de email fornecido.