kaspersky

Kaspersky Security for Mobile

Índice

Ajuda do Kaspersky Security for Mobile

O Kaspersky Security for Mobile se destina à proteção e gerenciamento de dispositivos móveis corporativos, assim como dispositivos móveis pessoais usados pelos funcionários da empresa para fins corporativos.

Os componentes e recursos do Kaspersky Security for Mobile dependem do console do Kaspersky Security Center usado como uma interface para proteger e gerenciar os dispositivos móveis.

Selecione a seção de ajuda necessária, dependendo do console do Kaspersky Security Center:

- Console de administração baseado em console de gerenciamento Microsoft
- Kaspersky Security Center Web Console ou Kaspersky Security Center Cloud Console

Seções de Ajuda separadas descrevem recursos e operações que estão disponíveis para usuários do aplicativo Kaspersky Endpoint Security for Android e do aplicativo Kaspersky Security for iOS.

O que há de novo

Kaspersky Security for iOS Technical Release 1

The new Kaspersky Security for iOS app is intended for protecting and managing corporate iOS and iPadOS devices. The app offers the following key features:

- Proteção contra ameaças on-line.
- Detecção de jailbreak.
- Gerenciamento de dispositivos corporativos usando o Kaspersky Security Center Web Console e o Cloud Console.

Kaspersky Endpoint Security for Android Technical Release 42

- Melhorias na interface do usuário do aplicativo do Kaspersky Endpoint Security for Android.
- O aplicativo Kaspersky Endpoint Security for Android agora requer a permissão "Dispositivos Bluetooth por perto" no Android 12 ou posterior para permitir que o administrador restrinja o uso do Bluetooth.
- Correções de bugs e melhorias gerais.

Kaspersky Endpoint Security for Android Technical Release 41

- Melhorias na interface do usuário do aplicativo do Kaspersky Endpoint Security for Android.
- Melhorias na interface do usuário nas configurações de política do plug-in do Kaspersky Security for Mobile (Policies) para o Kaspersky Security Center Web Console e Cloud Console.
- Correções de bugs e melhorias gerais.

Kaspersky Endpoint Security for Android Technical Release 40

- Correções de bugs e melhorias gerais.

Kaspersky Endpoint Security for Android Technical Release 39

- O Android 12L agora é compatível.
- Os seguintes acordos e declarações foram atualizados:
  - Contrato de Licença do Usuário Final
  - Declaração da Kaspersky Security Network
  - Declaração quanto ao processamento dos dados para propósitos de marketing

Observe que o administrador pode aceitar os novos termos dos contratos e instruções no Console de Administração. Isso permite ignorar esta etapa para os usuários do aplicativo Kaspersky Endpoint Security for Android nos dispositivos.

- Correções de bugs e melhorias gerais.

Kaspersky Endpoint Security for Android Technical Release 33

- Ao gerenciar o aplicativo Kaspersky Endpoint Security for Android usando sistemas EMM de terceiros, é possível agora aceitar múltiplos Contratos de Licença de Usuário Final usando um único comando.
- Não é mais preciso usar uma chave para ativar o Samsung KNOX.
- A estrutura das versões dos componentes do Kaspersky Security for Mobile foi modificada para incluir o número da versão.

Kaspersky Endpoint Security for Android Technical Release 32

- O aplicativo Kaspersky Endpoint Security for Android foi modificado para ser compatível com os requisitos atualizados do Android.

Kaspersky Endpoint Security for Android Technical Release 31

- Se o Kaspersky Security Center não estiver implementado em sua organização ou não estiver acessível para dispositivos móveis, os usuários poderão ativar manualmente o aplicativo Kaspersky Endpoint Security for Android em seus dispositivos.
- O Kaspersky Security for Mobile agora oferece suporte ao recurso Guias personalizadas do Google Chrome.

Kaspersky Endpoint Security for Android Technical Release 30

- O Kaspersky Security for Mobile agora permite a proteção e o gerenciamento de dispositivos móveis no Kaspersky Security Center Cloud Console.
- O Kaspersky Security for Mobile agora é compatível com o iOS 15 e o iPadOS 15.

Kaspersky Endpoint Security for Android Technical Release 29

- O aplicativo Kaspersky Endpoint Security for Android agora é compatível com Android 12.

Kaspersky Endpoint Security for Android Technical Release 27

- O Kaspersky Security for Mobile permite agora a proteção e o gerenciamento de dispositivos móveis no Kaspersky Security Center Web Console.

Kaspersky Endpoint Security for Android Technical Release 26

- O Kaspersky Endpoint Security agora é compatível com licenças e assinaturas com renovação automática.

Kaspersky Endpoint Security for Android Technical Release 22

- O Kaspersky Endpoint Security agora oferece suporte à Kaspersky Private Security Network, uma solução que permite acesso aos bancos de dados de reputação da Kaspersky Security Network sem enviar dados para fora da rede corporativa.
- O Kaspersky Endpoint Security for Android não oferece mais suporte à instalação em dispositivos que executam as versões 4.2 a 4.4.4 do Android.

Kaspersky Endpoint Security for Android Technical Release 20

- Os usuários não são convidados a aceitar as Declarações Legais caso o administrador opte por aceitá-las globalmente.
- O desempenho do aplicativo foi otimizado.

Kaspersky Endpoint Security for Android Technical Release 19

- O administrador agora pode aceitar o Kaspersky Security Network e outras declarações em nome dos usuários finais por meio do Kaspersky Security Center.
- Foram corrigidos diversos erros e a estabilidade operacional foi aprimorada.

Kaspersky Endpoint Security for Android Technical Release 18

- O Kaspersky Security for Mobile agora tem suporte para os Serviços Móveis Huawei.
- O Kaspersky Endpoint Security for Android agora pode ser instalado pela Huawei AppGallery.

Kaspersky Endpoint Security for Android Technical Release 17

- O Kaspersky Endpoint Security for Android agora é direcionado para API nível 29 e superior, trazendo algumas mudanças no comportamento do aplicativo em dispositivos que executam Android 10 ou superior.
- Novas configurações de força da senha para que o usuário escolha senhas com a complexidade exigida.
- A definição do uso de impressão digital como um método de desbloqueio da tela está agora disponível somente para o perfil de trabalho do Android.
- Foram corrigidos diversos erros e a estabilidade operacional foi aprimorada.

Kaspersky Endpoint Security for Android Technical Release 16

- O Kaspersky Endpoint Security for Android agora é compatível com Android 11.
- Novos requisitos de permissões de geolocalização e câmera disponíveis no Android 11. É possível ler mais sobre as novas regras de permissões para acessar a câmera e a localização nesta seção.

- Agora é possível especificar endereços de e-mail corporativos de usuários em um console EMM de terceiros. Estes e-mails serão exibidos no Kaspersky Security Center contanto que o novo KscCorporateEmail tenha sido configurado.

Kaspersky Endpoint Security for Android Technical Release 14

- Sempre que um usuário permite ou revoga os privilégios de Administrador de Dispositivo do aplicativo, um evento é enviado para o Console de gerenciamento.
- O parâmetro "KscGroup" agora pode ser configurado em consoles EMM de terceiros. Quando um dispositivo é conectado ao Kaspersky Security Center, ele é adicionado automaticamente a uma subpasta da pasta Dispositivos não atribuídos, com o mesmo nome que o grupo configurado no console EMM.

Kaspersky Endpoint Security for Android Technical Release 13

- Novo design da interface de usuário para o Kaspersky Endpoint Security for Android.
- Todas as seções de ajuda agora estão on-line.
- Os endereços IP dos dispositivos gerenciados agora são enviados para o Kaspersky Security Center e podem ser visualizados nas seções de informações sobre o dispositivo.

Kaspersky Endpoint Security for Android Technical Release 12

- Foi adicionada a capacidade de aceitar o Contrato de Licença do Usuário Final (EULA) no Kaspersky Security Center 12.1 remotamente. Se o administrador aceitar os termos do Contrato de Licença e da Política de Privacidade no Console de Administração, o aplicativo ignorará estas etapas durante o processo de instalação.
- Foi adicionada a capacidade de editar o nome do dispositivo no Kaspersky Security Center, para usuários do VMware AirWatch. Adicionamos uma nova configuração ao arquivo config, usado para configurar o aplicativo. É possível adicionar mais informações ao nome do dispositivo (por exemplo, o número de série do dispositivo). Dessa maneira, é mais fácil encontrar e classificar dispositivos no Kaspersky Security Center.

Kaspersky Endpoint Security for Android Technical Release 11

Foram corrigidos diversos erros e a estabilidade operacional foi aprimorada.

Kaspersky Endpoint Security for Android Technical Release 10

- O Kaspersky Security for Mobile agora oferece suporte ao Kaspersky Security Center 12.
- O suporte ao Kaspersky Safe Browser foi descontinuado no Kaspersky Security Center 12. É possível usar as funções do Kaspersky Safe Browser ao usar o Kaspersky Security Center 11 ou anterior.
- Foram corrigidos diversos erros e a estabilidade operacional foi aprimorada.

Kaspersky Endpoint Security for Android Service Pack 4 Maintenance Release 3

- Suporte verificado do Kaspersky Endpoint Security for Android no Microsoft Intune (uma solução de Enterprise Mobility Management (EMM)). A Kaspersky participa da Comunidade AppConfig para assegurar que o aplicativo funcione com soluções EMM de terceiros.

- Foi adicionada a capacidade de desativar notificações e mensagens pop-up quando o aplicativo estiver em segundo plano. Lembre-se de que não é seguro executar essas ações no modo de segundo plano. Se você desativar as notificações e mensagens pop-up quando o aplicativo estiver em segundo plano, o aplicativo não alertará os usuários sobre ameaças em tempo real. Os usuários de dispositivos móveis podem saber o status da proteção do dispositivo apenas quando abrem o aplicativo.

- Foi adicionada a capacidade de aceitar o Contrato de Licença do Usuário Final (EULA) e a Política de Privacidade no VMware AirWatch. Se o administrador aceitou o Contrato de Licença e a Política de Privacidade em um console AirWatch, o Kaspersky Endpoint Security for Android ignorará a etapa de aceitação no Assistente de Configuração Inicial.

- Foi adicionada a Declaração relativa ao processamento de dados com o propósito de usar a Proteção na Web (Declaração de Proteção na Web). É necessário aceitar a declaração para usar a Proteção na Web. O Kaspersky Endpoint Security for Android usa a Kaspersky Security Network (KSN) para verificar sites. A Declaração da Proteção na Web contém os Termos e Condições de troca de dados com a KSN. É possível aceitar a Declaração da Proteção na Web na política ou solicitar a aceitação do usuário do dispositivo.

- Foram corrigidos diversos erros e a estabilidade operacional foi aprimorada.

Comparação de recursos do aplicativo, dependendo das ferramentas de gerenciamento

É possível gerenciar dispositivos móveis no Kaspersky Security Center usando as seguintes ferramentas de gerenciamento:

- Console de Administração do Kaspersky Security Center com base no Console de Gerenciamento Microsoft (daqui em diante mencionado como "baseado no MMC")
- Kaspersky Security Center Web Console
- Kaspersky Security Center Cloud Console

A tabela a seguir compara os recursos disponíveis nessas ferramentas.

Disponibilidade de recursos dependendo das ferramentas de gerenciamento

	Console baseado em MMC	Web Console	Cloud Console
Geral			
Gerenciamento de dispositivos Android	Disponível	Disponível	Disponível
Gerenciamento de dispositivos iOS	Disponível (por meio de um certificado de APNs)	Disponível (por meio do aplicativo Kaspersky Security for iOS)	Disponível (por meio do aplicativo Kaspersky Security for iOS)
Gerenciamento de dispositivos móveis			
Adicionar dispositivos usando um link do Google Play	Disponível	Disponível	Disponível
Adicionar dispositivos usando um link da App Store	Não disponível	Disponível	Disponível
Adicionar dispositivos iOS usando um perfil MDM do iOS	Disponível	Não disponível	Não disponível
Adicionar dispositivos criando um pacote de instalação	Disponível	Não disponível	Não disponível
Envio de comandos para dispositivos móveis	Disponível	Disponível (exceto o comando Mugshot)	Disponível (exceto o comando Mugshot)
Remoção de dispositivos móveis do Kaspersky Security Center	Disponível	Disponível (Remover somente da lista de dispositivos. O aplicativo deve ser removido manualmente do dispositivo).	Disponível (Remover somente da lista de dispositivos. O aplicativo deve ser removido manualmente do dispositivo).
Gerenciamento de certificados			
Emissão de certificados	Disponível	Não disponível	Não disponível

de e-mail			
Emissão de certificados VPN	Disponível	Não disponível	Não disponível
Emissão de certificados móveis	Disponível	Disponível	Disponível
Emissão de certificados móveis através das ferramentas do Servidor de Administração	Disponível	Disponível	Disponível
Especificar arquivos do certificado	Disponível	Não disponível	Não disponível
Integração com infraestrutura de chave pública	Disponível	Não disponível	Não disponível
Gerenciamento de políticas			
Acesso baseado em função para configurar políticas de grupo	Disponível	Não disponível	Não disponível
Configurar a sincronização do dispositivo móvel com o Kaspersky Security Center	Disponível	Disponível	Disponível
Configuração de verificações de vírus em dispositivos móveis	Disponível	Disponível	Disponível
Configuração da proteção do dispositivo móvel	Disponível	Disponível	Disponível
Configurar atualizações do banco de dados antivírus	Disponível	Disponível	Disponível
Configurar a proteção de dados de dispositivos perdidos ou roubados	Disponível	Disponível	Disponível
Configurar o acesso do usuário aos sites	Disponível	Disponível	Disponível
Configurar o controle de aplicativos	Disponível	Disponível	Disponível
Configuração do controle de conformidade	Disponível	Disponível	Disponível
Configurar perfis de trabalho do Android	Disponível	Não disponível	Não disponível
Configurar a conexão à rede Wi-Fi	Disponível	Não disponível	Não disponível
Samsung KNOX	Disponível	Não disponível	Não disponível
Outros recursos			

Aceitação global do EULA no Kaspersky Security Center	Disponível	Não disponível	Não disponível
Configurar a Kaspersky Private Security Network	Disponível	Não disponível	Não disponível

Kit de distribuição

O kit de distribuição do Kaspersky Security for Mobile pode incluir vários componentes, dependendo da versão escolhida do aplicativo.

Gerenciamento de dispositivos móveis no Kaspersky Security Center Web Console

- `on_prem_ksm_devices_xx.x.x.x.zip`

  Arquivo comprimido que contém os arquivos necessários para a instalação do plug-in do Kaspersky Security for Mobile (Devices)

  - `plugin.zip`

    Arquivo comprimido que contém o plug-in do Kaspersky Security for Mobile (Devices).

  - `signature.txt`

    Arquivo que contém a assinatura do plug-in do Kaspersky Security for Mobile (Devices).

- `on_prem_ksm_policies_xx.x.x.x.zip`

  Arquivo comprimido que contém os arquivos necessários para a instalação do plug-in do Kaspersky Security for Mobile (Policies):

  - `plugin.zip`

    Arquivo comprimido que contém o plug-in do Kaspersky Security for Mobile (Policies).

  - `signature.txt`

    Arquivo que contém a assinatura do plug-in do Kaspersky Security for Mobile (Policies).

Gerenciamento de dispositivos móveis no Kaspersky Security Center Cloud Console

Para gerenciar o dispositivo móvel no Kaspersky Security Center Cloud Console, não é necessário baixar um pacote de distribuição. Basta criar uma conta no Kaspersky Security Center Cloud Console. Para obter mais informações sobre como criar uma conta, consulte a *Ajuda do Kaspersky Security Center Cloud Console*.

Gerenciamento de dispositivos móveis no console de administração baseado em MMC

- `Klcfginst_en.exe`

  Instalador do plug-in de administração do Kaspersky Endpoint Security for Android para administrar o aplicativo por meio do sistema de administração remota do Kaspersky Security Center.

- `Klmdminst.exe`

  Instalador do plug-in de administração do Kaspersky Device Management for iOS para gerenciar o aplicativo por meio do sistema de administração remota do Kaspersky Security Center.

Arquivo do aplicativo Kaspersky Endpoint Security for Android

`KES10_xx_xx_xxx.apk` — arquivo do pacote Android do aplicativo Kaspersky Endpoint Security for Android.

Arquivos auxiliares

- `sc_package_xx.exe`

  Arquivo comprimido de extração automática contendo os arquivos necessários para instalar o aplicativo Kaspersky Endpoint Security for Android ao criar os pacotes de instalação:

  - `adb.exe, AdbWinApi.dll, AdbWinUsbApi.dll`

    Arquivos necessários para criar os pacotes de instalação.

  - `installer.ini`

    Arquivo de configuração contendo as configurações de conexão do servidor de administração.

  - `KES10_xx_xx_xxx.apk`

    Arquivo do pacote Android do aplicativo Kaspersky Endpoint Security for Android.

  - `kmlisten.exe`

    Utilitário para entrega de pacotes de instalação por meio do computador do administrador.

  - `kmlisten.ini`

    Arquivo de configuração contendo as configurações do utilitário `kmlisten.exe`.

  - `kmlisten.kpd`

    Arquivo de descrição do aplicativo.

- `SigningUtility.zip`

  Arquivo comprimido contendo o utilitário para assinar os pacotes de distribuição do aplicativo Kaspersky Endpoint Security for Android e contêineres para dispositivos iOS.

Documentação

- Ajuda do Kaspersky Security for Mobile.

Trabalhando no Kaspersky Security Center Web Console e no Kaspersky Security Center Cloud Console

Esta seção de Ajuda descreve a proteção e o gerenciamento de dispositivos móveis usando o Kaspersky Security Center Web Console (doravante também denominado como Web Console) ou o Kaspersky Security Center Cloud Console (doravante também denominado como Cloud Console).

Sobre o gerenciamento de dispositivos móveis no Kaspersky Security Center Web Console e Cloud Console

É possível gerenciar os dispositivos móveis no Kaspersky Security Center Web Console e no Cloud Console usando os seguintes componentes:

- **Aplicativo Kaspersky Endpoint Security for Android**

  O aplicativo Kaspersky Endpoint Security for Android garante a proteção de dispositivos móveis contra ameaças da web, vírus e outros programas que representam ameaças.

- **Aplicativo do Kaspersky Security for iOS**

  O aplicativo Kaspersky Security for iOS garante a proteção de dispositivos móveis contra phishing e malwares.

- **Plug-in do Kaspersky Security for Mobile (Devices)**

  O plug-in do Kaspersky Security for Mobile (Devices) fornece a interface para gerenciar dispositivos móveis e os aplicativos móveis neles instalados por meio do Kaspersky Security Center Web Console e Cloud Console.

- **Plug-in do Kaspersky Security for Mobile (Policies)**

  O plug-in do Kaspersky Security for Mobile (Policies) permite definir as configurações dos dispositivos conectados ao Kaspersky Security Center, usando políticas de grupo.

Os plug-ins são integrados ao *sistema de administração remota do Kaspersky Security Center*. É possível usar o Kaspersky Security Center Web Console ou Cloud Console para gerenciar os dispositivos móveis, assim como os computadores clientes e sistemas virtuais. Após você conectar dispositivos móveis ao Servidor de Administração, eles ficam a ser gerenciados. É possível monitorar remotamente os dispositivos gerenciados.

Principais recursos de gerenciamento de dispositivos móveis no Kaspersky Security Center Web Console e Cloud Console

O Kaspersky Security for Mobile oferece os seguintes recursos:

- Distribuição de mensagens de e-mail para conectar dispositivos móveis Android ao Kaspersky Security Center usando links para baixar o aplicativo Kaspersky Endpoint Security for Android do Google Play.

- Distribuição de mensagens de e-mail para conectar dispositivos móveis iOS ao Kaspersky Security Center usando links para baixar o aplicativo Kaspersky Security for iOS da App Store.

- Conexão remota de dispositivos móveis com o Kaspersky Security Center e sistemas EMM de terceiros (por exemplo, VMWare AirWatch, MobileIron, IBM Maas360, SOTI MobiControl).

- Configuração remota do aplicativo móvel, assim como a configuração remota de serviços, aplicativos e funções de dispositivos móveis.
- Configuração remota de dispositivos móveis de acordo com os requisitos de segurança corporativa.
- Prevenção de vazamento de informações corporativas armazenadas em dispositivos móveis, no caso de perda ou roubo (Antirroubo). Compatível apenas com dispositivos Android.
- Controle de conformidade com requisitos de segurança corporativa (Controle de Conformidade). Compatível apenas com dispositivos Android.
- Controle de proteção contra ameaças on-line e controle de uso da Internet em dispositivos móveis (Proteção na Web).
- Configuração de notificações mostradas ao usuário nos aplicativos Kaspersky Endpoint Security for Android e Kaspersky Security for iOS.
- As notificações do administrador sobre o status e os eventos dos aplicativos Kaspersky Endpoint Security for Android e Kaspersky Security for iOS podem ser comunicadas no Kaspersky Security Center ou por e-mail.
- Controle de alterações das configurações da política (histórico de revisão).

O Kaspersky Security for Mobile inclui os seguintes componentes de proteção e gerenciamento:

- Antivírus (para dispositivos Android)
- Antirroubo (para dispositivos Android)
- Proteção na Web (para dispositivos Android e iOS)
- Controle de aplicativos (para dispositivos Android)
- Controle de conformidade (para dispositivos Android)
- Detecção de privilégios de root em dispositivos Android e detecção de jailbreak em dispositivos iOS

Sobre o aplicativo Kaspersky Endpoint Security for Android

O aplicativo Kaspersky Endpoint Security for Android garante a proteção de dispositivos móveis contra ameaças da web, vírus e outros programas que representam ameaças.

O aplicativo Kaspersky Endpoint Security for Android inclui os seguintes componentes:

- **Antivírus**. O componente detecta e neutraliza as ameaças em seu dispositivo utilizando os bancos de dados antivírus do aplicativo e o serviço da Kaspersky Security Network na nuvem. O Antivírus inclui os seguintes componentes:
  - **Proteção**. Detecta ameaças em arquivos abertos, verifica novos aplicativos e previne a infecção do dispositivo em tempo real.
  - **Verificação**. Ela é iniciada sob demanda para todo o sistema de arquivos, somente para aplicativos instalados ou um arquivo ou pasta selecionado.
  - **Atualização**. Permite o download de novos bancos de dados antivírus para o aplicativo.

- **Antirroubo**. Este componente protege informações no dispositivo contra acesso não autorizado, em caso de perda ou roubo do dispositivo. Esse componente permite enviar os seguintes comandos ao dispositivo:
  - **Localização**. Obtém as coordenadas da localização do dispositivo.
  - **Alarme**. Faz com que o dispositivo acione o disparo de um alarme sonoro.
  - **Limpeza**. Elimina os dados corporativos para proteger a confidencialidade das informações corporativas.
- **Proteção na Web**. Este componente bloqueia sites maliciosos projetados para espalhar códigos maliciosos. A Proteção na Web também bloqueia os sites falsos (phishing) projetados para roubar os dados confidenciais do usuário (por exemplo, senhas de serviços bancários on-line ou sistemas de transferência de dinheiro) e acessar as informações financeiras do usuário. A Proteção na Web verifica os sites antes de abri-los utilizando o serviço na nuvem Kaspersky Security Network. Após a verificação, a Proteção na Web permite que os sites confiáveis sejam carregados e bloqueia sites maliciosos. A Proteção na Web também é compatível com a filtragem de sites por categorias definidas no serviço da nuvem da Kaspersky Security Network. Isso permite ao administrador restringir o acesso do usuário a determinadas categorias de páginas da Web (por exemplo, páginas da Web das categorias de "Jogos de azar, loterias, apostas" ou "Comunicações via Internet").
- **Controle de aplicativos.** Esse componente permite instalar os aplicativos recomendados e requeridos no seu dispositivo por meio de um link direto para o pacote de distribuição ou um link para o Google Play. O Controle de Aplicativos permite remover os aplicativos bloqueados que violam os requisitos da segurança corporativa.
- **Controle de conformidade.** O componente permite verificar a conformidade dos dispositivos gerenciados com os requisitos de segurança corporativa e impõe restrições a certas funções de dispositivos que não estão em conformidade.

É possível configurar os componentes do aplicativo Kaspersky Endpoint Security for Android no Kaspersky Security Center Web Console e Cloud Console definindo as configurações das políticas de grupo.

Sobre o aplicativo Kaspersky Security for iOS

O aplicativo Kaspersky Security for iOS garante a proteção de dispositivos móveis contra phishing e malwares.

O aplicativo Kaspersky Security for iOS oferece os seguintes recursos principais:

- **Proteção na Web**. Este componente bloqueia sites maliciosos projetados para espalhar códigos maliciosos. A Proteção na Web também bloqueia os sites falsos (phishing) projetados para roubar os dados confidenciais do usuário (por exemplo, senhas de serviços bancários on-line ou sistemas de transferência de dinheiro) e acessar as informações financeiras do usuário. A Proteção na Web verifica os sites antes de abri-los utilizando o serviço na nuvem Kaspersky Security Network. Após a verificação, a Proteção na Web permite que os sites confiáveis sejam carregados e bloqueia sites maliciosos. Você pode configurar esse componente no Kaspersky Security Center Web Console definindo as configurações das políticas de grupo.
- **Detecção de jailbreak**. Quando o Kaspersky Security for iOS detecta um jailbreak, ele exibe uma mensagem crítica e informa sobre o problema.

Sobre o plug-in do Kaspersky Security for Mobile (Devices)

O plug-in do Kaspersky Security for Mobile (Devices) fornece a interface para gerenciar dispositivos móveis e os aplicativos móveis neles instalados por meio do Kaspersky Security Center Web Console e Cloud Console. O plug-in do Kaspersky Security for Mobile (Devices) permite que você faça o seguinte:

- Conexão de dispositivos móveis ao Kaspersky Security Center.
- Gerenciamento dos certificados de dispositivos móveis.
- Configurar o Firebase Cloud Messaging (somente para dispositivos Android).
- Enviar comandos para dispositivos móveis (somente para dispositivos Android).

O plug-in do Kaspersky Security for Mobile (Devices) pode ser instalado ao configurar o Kaspersky Security Center Web Console. Caso esteja usando o Kaspersky Security Center Cloud Console, não é necessário instalar o plug-in. Para obter mais informações sobre os cenários de implantação em diferentes tipos de consoles, consulte a seção "Cenários de implantação".

Sobre o plug-in do Kaspersky Security for Mobile (Policies)

O plug-in do Kaspersky Security for Mobile (Policies) permite definir as configurações dos dispositivos conectados ao Kaspersky Security Center, usando políticas de grupo. O plug-in do Kaspersky Security for Mobile (Policies) pode ser usado para realizar o seguinte:

- Criar políticas de segurança do grupo para dispositivos móveis.
- Definir remotamente as configurações operacionais do aplicativo móvel nos dispositivos móveis dos usuários.
- Receber relatórios e estatísticas sobre a operação do aplicativo móvel nos dispositivos móveis dos usuários.

O plug-in do Kaspersky Security for Mobile (Policies) pode ser instalado ao configurar o Kaspersky Security Center Web Console. Caso esteja usando o Kaspersky Security Center Cloud Console, não é necessário instalar o plug-in. Para obter mais informações sobre os cenários de implantação em diferentes tipos de consoles, consulte a seção "Cenários de implantação".

Requisitos de hardware e software

Esta seção lista os requisitos de hardware e software para o computador do administrador que é usado para instalar o plug-in do Kaspersky Security for Mobile (Devices) e o plug-in do Kaspersky Security for Mobile (Policies) no Kaspersky Security Center Web Console e Cloud Console, bem como os requisitos de hardware e software dos aplicativos móveis.

Requisitos de hardware e software para o computador do administrador

Para instalar o plug-in do Kaspersky Security for Mobile (Devices) e o plug-in do Kaspersky Security for Mobile (Policies), o computador do administrador deve atender aos requisitos de hardware do Kaspersky Security Center. Para obter mais informações sobre os requisitos de hardware e software do Kaspersky Security Center:

- Caso use o Kaspersky Security Center Web Console, consulte a *Ajuda do Kaspersky Security Center*.
- Caso use o Kaspersky Security Center Cloud Console, consulte a *Ajuda do Kaspersky Security Center Cloud Console*.

Para usar o plug-in do Kaspersky Security for Mobile (Devices) e o plug-in do Kaspersky Security for Mobile (Policies) no Kaspersky Security Center Web Console, o Kaspersky Security Center Web Console deve ser instalado no computador do administrador.

Para usar o plug-in do Kaspersky Security for Mobile (Devices) e o plug-in do Kaspersky Security for Mobile (Policies) no Kaspersky Security Center Cloud Console, você deve criar uma conta no Kaspersky Security Center Cloud Console. Para obter mais informações sobre como criar uma conta, consulte a *Ajuda do Kaspersky Security Center Cloud Console*.

O aplicativo Kaspersky Endpoint Security for Android pode funcionar dentro dos seguintes sistemas EMM de terceiros:

- VMWare AirWatch 9.3 ou posterior
- MobileIron 10.0 ou posterior
- IBM MaaS360 10.68 ou posterior
- Microsoft Intune 1908 ou posterior
- SOTI MobiControl 14.1.4 (1693) ou posterior

Requisitos de hardware e software para o dispositivo móvel do usuário para compatibilidade com a instalação do aplicativo Kaspersky Endpoint Security for Android

O aplicativo Kaspersky Endpoint Security for Android possui os seguintes requisitos de hardware e software:

- Smartphone ou tablet com uma resolução de tela de 320 x 480 pixels ou superior
- 65 MB de espaço disponível livre na memória principal do dispositivo
- Android 5.0–12 (incluindo Android 12L, excluindo Go Edition)
- arquitetura do processador x86, x86-64, Arm5, Arm6, Arm7 ou Arm8

O aplicativo é instalado somente na memória principal do dispositivo.

Requisitos de hardware e software para o dispositivo móvel do usuário para compatibilidade com a instalação do aplicativo Kaspersky Security for iOS

The Kaspersky Security for iOS app has the following hardware requirements:

- iPhone 6S ou posterior
- iPad Air 2 ou posterior

The Kaspersky Security for iOS app has the following software requirements:

- iOS 14.1 ou posterior
- iPadOS 14.1 ou posterior

O aplicativo Kaspersky Security for iOS não pode operar corretamente quando um cliente da VPN com uma conexão VPN ativa está sendo executado no mesmo dispositivo móvel.

Problemas conhecidos e considerações

O Kaspersky Endpoint Security for Android e o Kaspersky Security for iOS têm vários problemas conhecidos que não são críticos para a operação desses aplicativos.

Problemas conhecidos do Kaspersky Security for iOS

- O aplicativo Kaspersky Security for iOS não pode operar corretamente quando um cliente da VPN com uma conexão VPN ativa está sendo executado no mesmo dispositivo móvel.

Problemas conhecidos do Kaspersky Endpoint Security for Android

Problemas conhecidos ao iniciar o gerenciamento de dispositivos móveis no Kaspersky Security Center Web Console

- É possível iniciar o gerenciamento de dispositivos móveis durante a configuração inicial do Console de Administração baseado no MMC do Kaspersky Security Center (enquanto o assistente de início rápido é executado) ou posteriormente exibindo a pasta gerenciamento de dispositivos móveis no Console de Administração.

Problemas conhecidos ao instalar aplicativos

- O Kaspersky Endpoint Security for Android somente é instalado na memória principal do dispositivo.
- Em dispositivos que executam Android 7.0, um erro pode ocorrer durante tentativas de desativar os direitos de administrador para o Kaspersky Endpoint Security for Android nas configurações do dispositivo se o Kaspersky Endpoint Security for Android for proibido de se sobrepor em outras janelas. Esta falha é causada por um defeito bem conhecido no Android 7.
- O Kaspersky Endpoint Security for Android em dispositivos que executam o Android 7.0 ou posterior não tem suporte para o modo de múltiplas janelas.
- O Kaspersky Endpoint Security for Android não funciona em dispositivos Chromebook executando o sistema operacional Chrome.
- O Kaspersky Endpoint Security for Android não funciona em dispositivos executando o sistema operacional Android (Go edition).
- Ao usar o aplicativo Kaspersky Endpoint Security for Android com sistemas EMM de terceiros (por exemplo, VMWare AirWatch), somente os componentes Antivírus e Proteção na Web estarão disponíveis. O administrador pode definir as configurações de Antivírus e Proteção na Web no console do sistema EMM. Neste caso, as notificações sobre a operação do aplicativo somente estão disponíveis na interface do aplicativo Kaspersky Endpoint Security for Android (Relatórios).

Problemas conhecidos ao atualizar a versão do aplicativo

- Somente é possível fazer uma atualização do Kaspersky Endpoint Security for Android para uma versão mais recente do aplicativo. O Kaspersky Endpoint Security for Android não pode ser passado para uma versão mais

antiga.

Problemas conhecidos na operação Antivírus

- Devido às limitações técnicas, o Kaspersky Endpoint Security for Android não pode verificar arquivos com um tamanho de 2 GB ou mais. Durante uma verificação, o aplicativo ignora tais arquivos sem notificá-lo que tais arquivos foram ignorados.
- Para a análise adicional de um dispositivo quanto a novas ameaças cujas informações ainda não foram adicionadas aos bancos de dados antivírus, você deve ativar o uso da Kaspersky Security Network. A *Kaspersky Security Network (KSN)* é uma infraestrutura de serviços na nuvem que fornece o acesso à Base de Dados de Conhecimento on-line da Kaspersky, que contém informações sobre a reputação de arquivos, recursos da Web e softwares. Para usar a KSN, o dispositivo móvel deve estar conectado à Internet.
- Em alguns casos, a atualização dos bancos de dados antivírus do Servidor de Administração em um dispositivo móvel pode falhar. Nesse caso, execute a tarefa de atualização do banco de dados de antivírus no Servidor de Administração.
- Em alguns dispositivos, o Kaspersky Endpoint Security for Android não detecta dispositivos conectados através do USB OTG. Não é possível executar uma verificação de vírus em tais dispositivos.
- Em dispositivos com Android 11.0 ou posterior, o usuário deve conceder a permissão "Permitir acesso para gerenciar todos os arquivos".
- Em dispositivos que executam o Android 7.0 ou posterior, a janela de configuração do agendamento da execução da verificação de vírus pode ser incorretamente exibida (os elementos de gerenciamento não são mostrados). Esta falha é causada por um defeito bem conhecido no Android 7.
- Em dispositivos que executam Android 7.0, a proteção em tempo real no modo estendido não detecta ameaças em arquivos armazenados em um cartão SD externo.
- Em dispositivos que executam o Android 6.0, o Kaspersky Endpoint Security for Android não detecta o download de um arquivo malicioso para a memória do dispositivo. Um arquivo malicioso pode ser detectado pelo Antivírus quando o arquivo for executado ou durante uma verificação de vírus do dispositivo. Esta falha é causada por um defeito bem conhecido no Android 6.0. Para assegurar a segurança do dispositivo, recomenda-se configurar verificações de vírus agendadas.

Problemas conhecidos na operação de Proteção na Web

- · A Proteção na Web nos dispositivos Android funciona apenas nos navegadores Google Chrome (incluindo o recurso Guias personalizadas), Huawei Browser e Samsung Internet.
- Para que a Proteção na Web funcione, você deve ativar o uso da Kaspersky Security Network. A Proteção na Web bloqueia os sites com base nos dados da KSN sobre a reputação e a categoria de sites.
- Os sites proibidos podem permanecer desbloqueados pela Proteção na Web em dispositivos que executam o Android 6.0 com a versão 51 de Google Chrome (ou qualquer versão anterior) instalado se o site for aberto nas seguintes formas (este problema é causado por um defeito bem conhecido no Google Chrome):
  - Dos resultados da pesquisa
  - Da lista de favoritos
  - Do histórico de pesquisa

- Usar a função de preenchimento automático do endereço da Web
- Abrir o site em uma nova aba no Google Chrome

- Os sites proibidos podem permanecer desbloqueados no Google Chrome versão 50 (ou qualquer versão anterior) se o site tiver sido aberto da página de resultados de uma solicitação de pesquisa do Google enquanto o recurso de **Mesclar abas e aplicativos** estiver ativado nas configurações do navegador. Esta falha é causada por um defeito bem conhecido no Google Chrome.
- Os sites de categorias bloqueadas podem permanecer desbloqueados no Google Chrome se o usuário os abrir a partir de aplicativos de terceiros, por exemplo, de um aplicativo cliente de MI. Este problema é relacionado à forma como o serviço de Acessibilidade trabalha com o recurso de Abas Personalizados do Chrome.
- Os sites proibidos podem permanecer desbloqueados no Samsung Internet Browser se o usuário os abrir no modo de segundo plano a partir do menu de contexto ou de aplicativos de terceiros; por exemplo, de um aplicativo cliente de MI.
- O Kaspersky Endpoint Security for Android deve ser definido como um recurso de Acessibilidade para assegurar o funcionamento apropriado da Proteção na Web.
- Os sites permitidos podem ser bloqueados no Navegador de Internet da Samsung em **Apenas sites listados são permitidos** pelo modo Proteção na Web quando a página for atualizada. Os sites são bloqueados se uma expressão regular contiver configurações avançadas (por exemplo, `^https?:\/\/example\.com\/pictures\/`). Recomenda-se usar expressões regulares sem configurações adicionais (por exemplo, `^https?:\/\/example\.com`).

Problemas conhecidos na operação Antirroubo

- Para a entrega oportuna de comandos aos dispositivos Android, o aplicativo usa o serviço Firebase Cloud Messaging (FCM). Se FCM não for configurado, os comandos serão entregues ao dispositivo somente durante a sincronização com o Kaspersky Security Center, de acordo com o agendamento definido na política, por exemplo, a cada 24 horas.
- Para bloquear um dispositivo, o Kaspersky Endpoint Security for Android deve ser definido como o administrador do dispositivo.
- Para bloquear dispositivos que executam o Android 7.0 ou posterior, o Kaspersky Endpoint Security for Android deve ser definido como um recurso de Acessibilidade.
- Em alguns dispositivos, os comandos Antirroubo podem falhar se o modo de Economia de bateria estiver ativado no dispositivo. Esse defeito foi confirmado no Alcatel 5080X.
- Para localizar dispositivos executando Android 10.0 ou posterior, o usuário deve conceder a permissão "Permitir o tempo todo" à localização do dispositivo.

Problemas conhecidos na operação de Controle de aplicativos

- O Kaspersky Endpoint Security for Android deve ser definido como um recurso de acessibilidade para assegurar o funcionamento apropriado do Controle de aplicativos.
- Para que o Controle de Aplicativos (categorias de aplicativos) funcione, você deve ativar o uso da Kaspersky Security Network. O Controle de Aplicativos determina a categoria de um aplicativo com base nos dados que estão disponíveis na KSN. Para usar a KSN, o dispositivo móvel deve estar conectado à Internet. Para o Controle de Aplicativos, você pode adicionar aplicativos individuais às listas de aplicativos bloqueados e permitidos. Neste caso, a KSN não é necessária.

- Ao configurar o Controle de Aplicativos, recomenda-se desmarcar a caixa de seleção **Bloquear aplicativos do sistema**. O bloqueio de aplicativos do sistema pode levar a problemas na operação do dispositivo.

Problemas conhecidos ao configurar a força da senha para desbloqueio do dispositivo

- Para dispositivos com Android 10.0 ou posterior, o Kaspersky Endpoint Security divide os requisitos da força de segurança da senha em um dos valores do sistema: médio ou alto.

  Se a quantidade de símbolos exigida for de 1 a 4, então o aplicativo solicita ao usuário que defina uma senha de força média. Ela deve ser numérica (PIN), sem números repetidos ou sequenciais (ex. 1234), ou alfanumérica. O PIN ou a senha deve ter no mínimo 4 caracteres.

  Se o número de símbolos exigidos for 5 ou mais, então o aplicativo solicita ao usuário que defina uma senha de segurança alta. Ela deve ser numérica (PIN), sem números repetidos ou sequenciais, ou alfanumérica (senha). O PIN deve ter no mínimo 8 dígitos; a senha deve ter no mínimo 6 caracteres.

- Nos dispositivos que executam o Android 7.1.1, se a senha de desbloqueio não atender os requisitos de segurança corporativa (Controle de conformidade), o aplicativo do sistema Configurações pode não funcionar corretamente quando houver uma tentativa de desbloquear a senha através do Kaspersky Endpoint Security for Android. Esta falha é causada por um defeito bem conhecido no Android 7.1.1. Neste caso, para alterar a senha desbloqueada, use somente as Configurações do sistema do aplicativo.

- Em alguns dispositivos que executam o Android 6.0 ou posterior, um erro pode ocorrer quando a senha de desbloqueio da tela é inserida caso os dados do dispositivo estiverem criptografados. Este problema é relacionado aos recursos específicos do serviço de Acessibilidade com firmware MIUI.

Problemas conhecidos com a proteção contra a remoção do aplicativo

- O Kaspersky Endpoint Security for Android deve ser definido como o administrador do dispositivo.

- Para proteger o aplicativo da remoção em dispositivos que executam o Android 7.0 ou posterior, o Kaspersky Endpoint Security for Android deve ser definido como um recurso de Acessibilidade.

- Em alguns dispositivos de Huawei e Xiaomi, a proteção contra remoção do Kaspersky Endpoint Security não funciona. Este problema é causado pelos recursos específicos do firmware MIUI 7 e 8 em dispositivos Xiaomi e do firmware EMUI em dispositivos Huawei.

Problemas conhecidos ao configurar restrições de dispositivo

- Em dispositivos Android 10.0 ou posteriores, a proibição do uso de redes Wi-Fi não é compatível.

- Em dispositivos Android 10.0 ou posteriores, o uso da câmera não pode ser totalmente proibido.

- Nos dispositivos que executam o Android 11 ou posterior, o Kaspersky Endpoint Security for Android deve ser definido como um recurso de Acessibilidade. O Kaspersky Endpoint Security for Android solicita que o usuário defina o aplicativo como um recurso de Acessibilidade pelo Assistente de Configuração Inicial. O usuário pode ignorar esta etapa ou desativar este serviço nas configurações de dispositivo em um momento posterior. Nesse caso, não será possível restringir o uso da câmera.

Problemas conhecidos ao enviar comandos para dispositivos móveis

- Em dispositivos executando Android 12 ou posterior, se o usuário tiver concedido a permissão "Usar local aproximado", o aplicativo Kaspersky Endpoint Security for Android tentará primeiro obter a localização precisa

do dispositivo. Se isso não for bem-sucedido, a localização aproximada do dispositivo será retornada apenas se tiver sido recebida não mais de 30 minutos antes. Caso contrário, o comando **Localizar o dispositivo** falhará.

Problemas conhecidos com dispositivos específicos

- Em certos dispositivos (por exemplo, Huawei, Meizu e Xiaomi), você deve conceder uma permissão de inicialização automática ao Kaspersky Endpoint Security for Android ou adicioná-lo manualmente à lista de aplicativos iniciados quando o sistema operacional for inicializado. Se o aplicativo não for adicionado à lista, o Kaspersky Endpoint Security for Android para a execução de todas as suas funções após a reinicialização do dispositivo móvel. Além disso, se o dispositivo foi bloqueado, você não pode usar um comando para desbloquear o dispositivo. Você somente pode desbloquear o dispositivo ao usar um código de desbloqueio de uma só utilização.

- Em determinados dispositivos (por exemplo, Meizu e Asus), a execução do Android 6.0 ou posterior, após a criptografia dos dados e o reinício do dispositivo Android, você deve inserir uma senha numérica para desbloquear o dispositivo. Se o usuário usar uma senha gráfica para desbloquear o dispositivo, você deve converter a senha gráfica em uma senha numérica. Para obter mais detalhes sobre a conversão de uma senha gráfica em uma senha numérica, consulte o site de Suporte Técnico do fabricante de dispositivo móvel. Este problema é relacionado à operação do serviço Recursos de Acessibilidade.

- Em alguns dispositivos Huawei executando o Android 5.X, após o Kaspersky Endpoint Security for Android ser definido como um recursos de acessibilidade, uma mensagem incorreta sobre a falta de direitos apropriados será exibida. Para ocultar esta mensagem, ative o aplicativo como aplicativo protegido nas configurações do dispositivo.

- Em alguns dispositivos Huawei que executam o Android 5. X ou 6. X, quando o modo de Economia de bateria estiver ativado para o Kaspersky Endpoint Security for Android, o usuário pode terminar manualmente o aplicativo. O dispositivo do usuário se torna desprotegido após isso. Esse problema é devido a alguns recursos do software da Huawei. Para restaurar a proteção do dispositivo, execute manualmente o Kaspersky Endpoint Security for Android. Recomenda-se desativar o modo de Economia de bateria para o Kaspersky Endpoint Security for Android nas configurações do dispositivo.

- Em dispositivos Huawei com o firmware EMUI executando o Android 7.0, o usuário pode ocultar a notificação quanto ao status da proteção do Kaspersky Endpoint Security for Android. Esse problema é devido a alguns recursos do software da Huawei.

- Em alguns dispositivos Xiaomi, ao definir o comprimento de senha em mais de 5 caracteres em uma política, o usuário será solicitado a modificar a senha de desbloqueio da tela em vez do código PIN. Você não pode definir um código PIN que tenha mais de 5 caracteres. Este problema é devido a alguns recursos do software da Xiaomi.

- Em dispositivos Xiaomi com o firmware MIUI executando o Android 6.0, o ícone do Kaspersky Endpoint Security for Android na barra de status pode estar oculto. Este problema é devido a alguns recursos do software da Xiaomi. Recomenda-se permitir a exibição de ícones de notificação nas configurações de Notificações.

- Em alguns dispositivos Nexus que executam o Android 6.0.1, os privilégios necessários para o funcionamento apropriado não podem ser concedidos através do Assistente de Início Rápido do Kaspersky Endpoint Security for Android. Esta falha é causada por um defeito bem conhecido na Correção de Segurança para o Android pelo Google. Para assegurar a operação apropriada, os privilégios necessários devem ser manualmente concedidos nas configurações do dispositivo.

- Em determinados dispositivos Samsung que executam o Android 7.0 ou posterior, quando o usuário tenta configurar métodos não compatíveis para desbloquear o dispositivo (por exemplo, uma senha gráfica), o dispositivo pode ser bloqueado se as seguintes condições forem atendidas: A remoção do Kaspersky Endpoint Security for Android está ativada e os requisitos de força da senha de desbloqueio da tela estão definidos. Para desbloquear o dispositivo, é necessário enviar um comando especial ao dispositivo.

- Em determinados dispositivos Samsung é impossível bloquear o uso de impressões digitais para desbloquear a tela.
- A Proteção na Web não pode ser ativada em alguns dispositivos Samsung, caso o dispositivo esteja conectado a uma rede 3G/4G e tenha o modo de Economia de bateria ativado para restringir os dados de segundo plano. Recomenda-se desativar a função que restringe os processos em segundo plano nas configurações de Economia de bateria.
- Em determinados dispositivos Samsung, se a senha de desbloqueio não estiver em conformidade com requisitos de segurança corporativa, o Kaspersky Endpoint Security for Android não bloqueia o uso de impressões digitais para desbloquear a tela.
- Em alguns dispositivos Honor e Huawei, não é possível restringir o uso de Bluetooth. Quando o Kaspersky Endpoint Security for Android tenta restringir o uso de Bluetooth, o sistema operacional exibe uma notificação com a opção de rejeitar ou permitir essa restrição. O usuário pode rejeitar essa restrição e continuar usando o Bluetooth.
- Em dispositivos Blackview, o usuário pode limpar a memória do aplicativo Kaspersky Endpoint Security for Android. Como resultado, a proteção e o gerenciamento do dispositivo são desativados, todas as configurações definidas tornam-se ineficazes e o aplicativo Kaspersky Endpoint Security for Android é removido dos recursos de Acessibilidade. Isso ocorre porque os dispositivos deste fornecedor fornecem o aplicativo de Telas recentes personalizado com privilégios elevados. Este aplicativo pode substituir as configurações do Kaspersky Endpoint Security for Android e não pode ser substituído porque ele faz parte do sistema operacional Android.
- Em alguns dispositivos que executam o Android 11, o aplicativo Kaspersky Endpoint Security for Android trava imediatamente após ser iniciado. Essa falha é causada por um familiar defeito no Android 11.

Implementação de uma solução de gerenciamento de dispositivos móveis no Kaspersky Security Center Web Console ou Cloud Console

Para gerenciar dispositivos móveis usando o Kaspersky Security Center Web Console ou Cloud Console, é necessário implementar uma solução de gerenciamento de dispositivos móveis.

Cenários de implementação

Implementação no Kaspersky Security Center Web Console

A implementação da solução de gerenciamento de dispositivos móveis no Kaspersky Security Center Web Console consiste nas seguintes etapas:

1. Preparação do Kaspersky Security Center Web Console para implementação
2. Implementação dos plug-ins de administração
3. Implementar o aplicativo móvel
4. (Opcional, somente para Android) Configuração da troca de informações com o Firebase Cloud Messaging

Recomenda-se executar esta etapa para garantir a entrega oportuna de comandos para dispositivos móveis e sincronização forçada quando as configurações de política forem alteradas.

Implementação no Kaspersky Security Center Cloud Console

A implementação da solução de gerenciamento de dispositivos móveis no Kaspersky Security Center Cloud Console consiste nas seguintes etapas:

1. Preparação do Kaspersky Security Center Cloud Console para implementação
2. Implementar o aplicativo móvel
3. (Opcional, somente para Android) Configuração da troca de informações com o Firebase Cloud Messaging

Recomenda-se executar esta etapa para garantir a entrega oportuna de comandos para dispositivos móveis e sincronização forçada quando as configurações de política forem alteradas.

Preparação do Kaspersky Security Center Web Console e Cloud Console para implementação

Esta seção fornece instruções sobre como preparar o Kaspersky Security Center Web Console e Cloud Console para implementação.

Configuração do servidor de administração para conexão de dispositivos móveis

Para que os dispositivos móveis possam se conectar ao Servidor de Administração, você deve definir as configurações de conexão do dispositivo móvel nas propriedades do Servidor de Administração antes de instalar o aplicativo Kaspersky Endpoint Security for Android ou o aplicativo Kaspersky Security for iOS em dispositivos móveis.

Para definir as configurações do servidor de administração para a conexão do dispositivo móvel:

1. Inicie o gerenciamento do dispositivo móvel no servidor de administração.

   É possível iniciar o gerenciamento de dispositivos móveis durante a configuração inicial do Console de Administração baseado no MMC do Kaspersky Security Center (enquanto o assistente de início rápido é executado) ou posteriormente exibindo a pasta gerenciamento de dispositivos móveis no Console de Administração.

2. Na janela principal do Kaspersky Security Center Web Console ou Cloud Console, clique em **Configurações** ( ).

   A janela de propriedades do servidor de administração é aberta.

3. Configure as portas do servidor de administração usadas pelos dispositivos móveis:

   a. Selecione a seção **Portas adicionais**.

b. Mude o botão **Abrir a porta para os dispositivos móveis** para a posição ativado.

c. No campo **Porta para sincronização de dispositivos móveis**, especifique a porta à qual os dispositivos móveis serão conectados ao servidor de administração.

A porta 13292 é utilizada por padrão.

Caso o botão **Abrir porta para dispositivos móveis** esteja na posição desativado ou se uma porta de conexão for especificada incorretamente, os dispositivos móveis não poderão se conectar com o servidor de administração.

d. No campo **Porta para ativar dispositivos móveis**, especifique a porta a ser usada pelos dispositivos móveis para conexão com o Servidor de Administração para a ativação do aplicativo móvel.

A porta 17100 é utilizada por padrão.

Se você especificar uma porta de conexão incorreta, os usuários de dispositivos móveis não poderão ativar o aplicativo móvel usando o Servidor de Administração.

4. Caso necessário, edite o certificado que será usado pelos dispositivos móveis para conexão ao servidor de administração.

Por padrão, o servidor de administração usa o certificado que foi criado durante a instalação do servidor de administração. Caso queira, substitua o certificado emitido por meio do servidor de administração por outro certificado ou reemita o certificado emitido por meio do servidor de administração.

Para editar o certificado*:*

a. Selecione a seção **Certificados**.

b. Defina as configurações necessárias.

Para obter informações detalhadas sobre os certificados, consulte a *Ajuda do Kaspersky Security Center*.

5. Clique no botão **Salvar** para salvar as alterações feitas nas configurações e sair da janela de propriedades do servidor de administração.

Após definir as configurações de conexão do dispositivo móvel, você pode instalar o aplicativo Kaspersky Endpoint Security for Android ou o aplicativo Kaspersky Security for iOS em dispositivos móveis e conectá-los ao Servidor de Administração usando as configurações especificadas.

Criação de um grupo de administração

As Políticas de grupo são usados para realizar a configuração centralizada dos aplicativos Kaspersky Endpoint Security for Android e Kaspersky Security for iOS instalados nos dispositivos móveis dos usuários.

Para aplicar a política a um grupo de dispositivos, recomenda-se criar um grupo separado para esses dispositivos em **Dispositivos gerenciados** antes de instalar aplicativos móveis nos dispositivos dos usuários.

Após criar um grupo de administração, recomenda-se configurar a opção de alocar automaticamente dispositivos nos quais deseja instalar os aplicativos para esse grupo. Em seguida, defina as configurações que são comuns a todos os dispositivos usando uma política do grupo.

Para criar um grupo de administração:

1. Na janela principal do Kaspersky Security Center Web Console ou Cloud Console, selecione **DISPOSITIVOS** > **HIERARQUIA DE GRUPOS**.

2. Na estrutura do grupo de administração, selecione o grupo de administração que deve incluir o novo grupo de administração.

3. Clique no botão **Adicionar**.

4. Na janela aberta **Nome do novo grupo de administração**, insira um nome para o grupo e clique no botão **Adicionar**.

Um novo grupo de administração com o nome especificado aparece na hierarquia de grupos de administração.

Criação de uma regra para alocação automática de um dispositivo para grupos de administração

Quando o aplicativo Kaspersky Endpoint Security for Android ou o aplicativo Kaspersky Security for iOS é instalado em dispositivos móveis, eles são exibidos na página **DESCOBERTA E IMPLEMENTAÇÃO** > **DISPOSITIVOS NÃO ATRIBUÍDOS** do Kaspersky Security Center Web Console ou Cloud Console. Para gerenciar os dispositivos recém-conectados, é possível movê-los manualmente para um grupo de administração ou criar uma regra para alocá-los automaticamente a grupos de administração.

Para criar uma regra para alocação automática de dispositivos móveis para grupos de administração:

1. Na janela principal do Kaspersky Security Center Web Console ou Cloud Console, selecione **DESCOBERTA E IMPLEMENTAÇÃO** > **IMPLEMENTAÇÃO E ATRIBUIÇÃO** > **REGRAS MÓVEIS**.

2. Na janela **Nova regra** aberta, clique no botão **Adicionar**.

3. No **Nome da regra**, especifique o nome da regra.

4. No campo **Grupo de administração**, selecione o grupo de administração ao qual os dispositivos móveis serão alocados após a instalação do aplicativo neles.

5. Na seção **Aplicação da regra**, selecione **Executar uma vez para cada dispositivo**.

6. Marque a caixa de seleção **Mover somente os dispositivos não adicionados ao grupo de administração** para evitar a movimentação de dispositivos móveis alocados a outros grupos de administração ao aplicar a regra.

7. Marque a caixa de seleção **Ativar regra** para aplicar imediatamente a regra após criá-la.

   É possível ativar a regra a qualquer momento mudando a seleção com o botão na página **REGRAS DE MOVIMENTO**.

8. Selecione **CONDIÇÕES DA REGRA** > **Aplicativos** e faça o seguinte:

   a. Ative o botão de seleção **Versão do sistema operacional**.

   b. Na lista de sistemas operacionais que se abre, selecione **Android** ou **iOS**.

   A regra será aplicada aos dispositivos correspondentes. É possível especificar pelo menos uma condição para criar uma regra.

9. Clique em **Salvar** para criar a regra.

A regra recém-criada é exibida na página **REGRAS DE MOVIMENTO**. De acordo com a regra, o Kaspersky Security Center alocará todos os dispositivos recém-conectados ao grupo de administração selecionado.

Para obter informações detalhadas sobre o gerenciamento de grupos de administração e ações com dispositivos não atribuídos:

- Caso use o Kaspersky Security Center Web Console, consulte a *Ajuda do Kaspersky Security Center*.
- Caso use o Kaspersky Security Center Cloud Console, consulte a *Ajuda do Kaspersky Security Center Cloud Console*.

Implementação dos plug-ins de administração

Para gerenciar dispositivos móveis no Kaspersky Security Center Web Console, os seguintes plug-ins de administração devem ser instalados:

- Plug-in do Kaspersky Security for Mobile (Devices)
- Plug-in do Kaspersky Security for Mobile (Policies)

> Caso esteja usando o Kaspersky Security Center Cloud Console, não é necessário instalar os plug-ins de administração. Basta criar uma conta no Kaspersky Security Center Cloud Console. Para obter mais informações sobre como criar uma conta, consulte a *Ajuda do Kaspersky Security Center Cloud Console*.

É possível usar os seguintes métodos para instalar os plug-ins de administração:

- Por meio do uso do assistente de início rápido do Kaspersky Security Center Web Console.

  O Kaspersky Security Center Web Console solicita a execução do assistente de início rápido, automaticamente após a instalação do servidor de administração, durante a sua primeira conexão. Também é possível iniciar o Assistente de Início Rápido manualmente a qualquer momento.

  Para obter mais informações sobre o Assistente de Início Rápido do Kaspersky Security Center, consulte a *Ajuda do Kaspersky Security Center*.

- Usando a lista de pacotes de distribuição disponíveis no Kaspersky Security Center Web Console.

  A lista de pacotes de distribuição disponíveis é atualizada automaticamente depois que novas versões dos aplicativos da Kaspersky são lançadas.

- Baixe os pacotes de distribuição de uma fonte externa e adicione os plug-ins de administração ao Kaspersky Security Center Web Console.

  Por exemplo, os pacotes de distribuição do plug-in de administração podem ser baixados no site da Kaspersky.

Instalação de plug-ins de administração a partir da lista de pacotes de distribuição disponíveis

Para instalar os plug-ins de administração:

1. Na janela principal do Kaspersky Security Center Web Console, selecione **CONFIGURAÇÕES DO CONSOLE** > **PLUG-INS DA WEB**.
2. Clique no botão **Adicionar**.

   Isso abrirá a lista de versões atualizadas dos aplicativos da Kaspersky.
3. Instalar os plug-ins de administração:

a. Na lista de aplicativos disponíveis, clique na seção **Dispositivos móveis** para expandi-la.

b. Selecione Kaspersky Security for Mobile (Devices) e clique em **Instalar plug-in**.

c. Selecione **Kaspersky Security for Mobile (Policies)** e clique em **Instalar plug-in**.

Os pacotes de distribuição são baixados e os plug-ins são instalados. Quando cada plug-in for instalado e adicionado ao Kaspersky Security Center Web Console, uma janela de confirmação será exibida.

Instalação do plug-in de administração a partir do pacote de distribuição

É possível baixar o pacote de distribuição no site da Kaspersky.

Para instalar o plug-in do Kaspersky Security for Mobile (Devices) do pacote de distribuição:

1. Copie os arquivos `plugin.zip` e `signature.txt` do arquivo comprimido `on_prem_ksm_devices_xx.x.x.x.zip` do pacote de distribuição para a estação de trabalho do administrador.
2. Na janela principal do Kaspersky Security Center Web Console, selecione **CONFIGURAÇÕES DO CONSOLE** > **PLUG-INS DA WEB**.
3. Clique em **Adicionar a partir do arquivo**.
4. Na janela **Adicionar do arquivo** que se abre, clique em **Carregar arquivo ZIP** e procure `plugin.zip`.
5. Clique em **Carregar assinatura** e navegue até `assinatura.txt`.
6. Clique no botão **Adicionar**.

O plug-in do Kaspersky Security for Mobile (Devices) é instalado e adicionado ao Kaspersky Security Center Web Console.

Para instalar o plug-in do Kaspersky Security for Mobile (Policies) do pacote de distribuição:

1. Copie os arquivos `plugin.zip` e `signature.txt` do arquivo comprimido `on_prem_ksm_policies_xx.x.x.x.zip` do pacote de distribuição para a estação de trabalho do administrador.
2. Na janela principal do Kaspersky Security Center Web Console, selecione **CONFIGURAÇÕES DO CONSOLE** > **PLUG-INS DA WEB**.
3. Clique em **Adicionar a partir do arquivo**.
4. Na janela **Adicionar do arquivo** que se abre, clique em **Carregar arquivo ZIP** e procure `plugin.zip`.
5. Clique em **Carregar assinatura** e navegue até `assinatura.txt`.
6. Clique no botão **Adicionar**.

O plug-in do Kaspersky Security for Mobile (Policies) é instalado e adicionado ao Kaspersky Security Center Web Console.

É possível verificar se os plug-ins de administração foram instalados visualizando a lista de plug-ins na página **CONFIGURAÇÕES DO CONSOLE** > **PLUG-INS DA WEB**.

Implementar o aplicativo móvel

Para gerenciar dispositivos móveis no Kaspersky Security Center Web Console ou Cloud Console, você deve implementar o aplicativo Kaspersky Endpoint Security for Android ou o aplicativo Kaspersky Security for iOS em dispositivos móveis. É possível implementar aplicativos em dispositivos móveis usando o Kaspersky Security Center Web Console ou Cloud Console.

Implementar o aplicativo móvel usando o Kaspersky Security Center Web Console ou Cloud Console

O aplicativo móvel é implementado nos dispositivos móveis dos usuários cujas contas de usuário foram adicionadas ao Kaspersky Security Center. Para obter mais informações sobre contas de usuário no Kaspersky Security Center:

- Caso use o Kaspersky Security Center Web Console, consulte a *Ajuda do Kaspersky Security Center*.
- Caso use o Kaspersky Security Center Cloud Console, consulte a *Ajuda do Kaspersky Security Center Cloud Console*.

É possível usar o plug-in do Kaspersky Security for Mobile (Devices) para instalar o aplicativo do Kaspersky Security Center Web Console e Cloud Console enviando um link de instalação para um dispositivo móvel.

- Em um dispositivo Android, o usuário recebe um link do Google Play para baixar o aplicativo Kaspersky Endpoint Security for Android. O aplicativo pode ser instalado seguindo o procedimento padrão de instalação na plataforma Android. Após a instalação do aplicativo, o usuário deve fornecer as permissões necessárias.

  Alguns dispositivos Huawei e Honor não têm serviços do Google e, portanto, não têm acesso aos aplicativos do Google Play. Se alguns usuários de aparelhos Huawei e Honor não puderem instalar o aplicativo do Google Play, é recomendável que sejam instruídos a instalar o aplicativo da Huawei App Gallery.

- Em um dispositivo iOS, o usuário recebe um link da App Store para baixar o aplicativo Kaspersky Security for iOS. O aplicativo pode ser instalado seguindo o procedimento padrão de instalação na plataforma iOS.

  Antes de conectar um dispositivo iOS, envie o endereço do Kaspersky Security Center ao usuário do dispositivo para melhorar a segurança da conexão. O usuário verá esse endereço durante a instalação do aplicativo e poderá cancelar a conexão se o endereço exibido não corresponder ao endereço enviado.

O link contém os seguintes dados:

- Configurações de sincronização do Kaspersky Security Center
- Certificado geral

Para implementar o aplicativo em um dispositivo móvel:

1. Inicie o Assistente de Conexão de Novos Dispositivos Móveis:

   - Na janela principal do Kaspersky Security Center Web Console ou Cloud Console, selecione **DISPOSITIVOS** > **MÓVEIS** > **DISPOSITIVOS** e clique em **Adicionar**.

   - Na janela principal do Kaspersky Security Center Web Console ou Cloud Console, selecione **USUÁRIOS E FUNÇÕES** > **USUÁRIOS**. Clique no nome do usuário ou do grupo de usuários para o qual deseja enviar o link para conectar um dispositivo móvel e selecione **DISPOSITIVOS.** Clique em **Adicionar dispositivo móvel**. Neste caso, pule a etapa 3.

   Prossiga com o Assistente usando o botão **Avançar**.

2. Selecione o sistema operacional dos dispositivos que você deseja adicionar:

   - **Android**

   - **iOS e iPadOS**

3. Selecione usuários e grupos de usuários para os quais você deseja enviar o link para conectar um dispositivo móvel.

4. Selecione os endereços de e-mail para os quais enviar o link:

   - **Todos os endereços de e-mail**

   - **Endereço de e-mail principal**

   - **Endereço de e-mail alternativo**

   - **Outro endereço de e-mail**

     Ao selecionar esta opção, especifique o endereço de e-mail abaixo.

5. O resumo do link é exibido.

   Certifique-se de que todos os parâmetros do link estejam corretos e clique em **Enviar**.

6. Uma janela é aberta com a confirmação de que o link para adicionar um dispositivo móvel foi enviado.

   Clique em **OK** para concluir o Assistente.

Quando o usuário instalar o aplicativo Kaspersky Endpoint Security for Android ou o aplicativo Kaspersky Security for iOS, o dispositivo do usuário será exibido na guia **DISPOSITIVOS** > **MÓVEIS** > **DISPOSITIVOS** do Web Console ou Cloud Console. Depois de instalar o aplicativo nos dispositivos móveis dos usuários, será possível definir as configurações para dispositivos e aplicativos usando as políticas de grupo. Também será possível enviar comandos para dispositivos móveis (somente para Android) para proteção de dados caso os dispositivos sejam perdidos ou roubados.

Ativar o aplicativo móvel

No Kaspersky Security Center, a licença pode abranger diversos grupos de recursos. Para garantir que o aplicativo Kaspersky Endpoint Security for Android e o aplicativo Kaspersky Security for iOS estejam totalmente funcionais, a licença do Kaspersky Security Center adquirida pela organização deve fornecer a funcionalidade **Gerenciamento de dispositivos móveis**. A funcionalidade **Gerenciamento de dispositivo móvel** é destinada a conectar dispositivos móveis ao Kaspersky Security Center e gerenciá-los.

Para obter informações detalhadas sobre o licenciamento do Kaspersky Security Center e sobre as opções de licenciamento:

- Caso use o Kaspersky Security Center Web Console, consulte a *Ajuda do Kaspersky Security Center*.
- Caso use o Kaspersky Security Center Cloud Console, consulte a *Ajuda do Kaspersky Security Center Cloud Console*.

A ativação do aplicativo Kaspersky Endpoint Security for Android ou do aplicativo Kaspersky Security for iOS em um dispositivo móvel é feita fornecendo informações de licença válidas ao aplicativo. As informações da licença são entregues ao dispositivo móvel, junto com a política, quando o dispositivo é sincronizado com o Kaspersky Security Center.

Caso a ativação do aplicativo móvel não seja concluída em 30 dias a partir do momento da instalação no dispositivo móvel, o aplicativo será automaticamente alterado para o modo de funcionalidade limitada. Nesse modo, a maioria dos componentes do aplicativo são desativados. Ao mudar para o modo de funcionalidade limitada, o aplicativo para de executar a sincronização automática com o Kaspersky Security Center. Portanto, se a ativação do aplicativo não tiver sido concluída em 30 dias após a instalação, o usuário deverá sincronizar manualmente o dispositivo com o Kaspersky Security Center.

Se o Kaspersky Security Center não estiver implementado em sua organização ou não estiver acessível para dispositivos móveis, os usuários poderão ativar manualmente o aplicativo móvel nos dispositivos.

Para ativar o aplicativo móvel:

1. Abra a janela de propriedades da política:
   - Na janela principal do Kaspersky Security Center Web Console ou Cloud Console, selecione **DISPOSITIVOS** > **POLÍTICAS E PERFIS**. Na lista de políticas de grupo aberta, clique no nome da política que deseja configurar.
   - Na janela principal do Kaspersky Security Center Web Console ou Cloud Console, selecione **DISPOSITIVOS** > **MÓVEIS** > **DISPOSITIVOS**. Clique no dispositivo móvel que se enquadra na política que desejar configurar e, em seguida, selecione a política na guia **POLÍTICAS ATIVAS E PERFIS DE POLÍTICAS.**
2. Na página de propriedades da política, selecione **CONFIGURAÇÕES DO APLICATIVO** > **Licenças**.
3. Use a lista suspensa para selecionar a chave de licença necessária do armazenamento de chaves do Servidor de Administração.

   Os detalhes da chave de licença são exibidos nos campos abaixo.

   > É possível substituir a chave de ativação existente no dispositivo móvel se ela for diferente da selecionada na lista suspensa acima. Para fazer isso, marque a caixa de seleção **Se a chave no dispositivo for diferente, substitua por esta chave** caixa de seleção.
4. Clique no botão **Salvar** para salvar as alterações feitas na política e sair da janela de propriedades da política.

As configurações do dispositivo móvel são definidas depois da próxima sincronização do dispositivo com o Kaspersky Security Center.

Fornecimento de permissões necessárias para o aplicativo Kaspersky Endpoint Security for Android

Certos recursos do aplicativo Kaspersky Endpoint Security for Android requerem permissões. O Kaspersky Endpoint Security for Android solicita permissões obrigatórias durante a instalação, bem como após a instalação e antes de usar recursos individuais do aplicativo. É impossível instalar o Kaspersky Endpoint Security for Android sem fornecer as permissões obrigatórias.

Em determinados dispositivos (por exemplo, Huawei, Meizu e Xiaomi), o Kaspersky Endpoint Security for Android deve ser adicionado manualmente na lista de aplicativos que serão iniciados quando o sistema operacional inicializar nas configurações do dispositivo. Se o aplicativo não for adicionado à lista, o Kaspersky Endpoint Security for Android para a execução de todas as suas funções após a reinicialização do dispositivo móvel.

Em dispositivos com Android 11 ou posterior, é necessário desabilitar a configuração do sistema **Remover permissões se o aplicativo não for usado**. Caso contrário, depois que o aplicativo não for usado por alguns meses, o sistema redefinirá automaticamente as permissões que o usuário concedeu ao aplicativo.

Permissões solicitadas pelo aplicativo Kaspersky Endpoint Security for Android

Permissão	Função do aplicativo
Telefone (necessário apenas para o Android 5.0–9.X)	Conectar-se ao Kaspersky Security Center (ID do dispositivo)
Armazenamento (obrigatório)	Antivírus
Acesso para gerenciar todos os arquivos	Antivírus (somente para Android 11 ou posterior)
Dispositivos Bluetooth por perto (para Android 12 ou posterior)	Restringir o uso do Bluetooth
Administrador do dispositivo (obrigatório)	Antirroubo – bloqueia o dispositivo (somente para o Android 5.0–6.X)
	Antirroubo – tirar um retrato com a câmera frontal Embora a função de tirar retratos não seja compatível com o Kaspersky Security Center Web Console e Cloud Console, o aplicativo Kaspersky Endpoint Security for Android requer essa permissão para que possa ser gerenciado por todos os consoles do Kaspersky Security Center.
	Antirroubo – soar um alarme
	Antirroubo – redefinição completa
	Proteção por senha
	Proteção contra a remoção do aplicativo
	Instalar o certificado de segurança
	Controle de aplicativos
	Restringir o uso da câmera, Bluetooth e Wi-Fi

Câmera	Antirroubo – tirar um retrato com a câmera frontal Embora a função de tirar retratos não seja compatível com o Kaspersky Security Center Web Console e Cloud Console, o aplicativo Kaspersky Endpoint Security for Android requer essa permissão para que possa ser gerenciado por todos os consoles do Kaspersky Security Center. Em dispositivos executando Android 11.0 ou posterior, o usuário deve conceder a permissão "Enquanto usa o aplicativo" quando solicitado
Localização	Antirroubo – localizar o dispositivo Em dispositivos executando Android 10.0 ou posterior, o usuário deve conceder a permissão "Permitir o tempo todo" quando solicitado.
Acessibilidade	Antirroubo – bloquear o dispositivo (somente para o Android 7.0 ou posterior)
	Proteção na Web
	Controle de aplicativos
	Proteção contra a remoção do aplicativo (somente para Android 7.0 ou posterior)
	Exibição de avisos do Kaspersky Endpoint Security for Android (apenas para Android 10.0 ou posterior)
	Restringir o uso da câmera (apenas para Android 11 ou posterior)

Gerenciamento de certificados

Os certificados móveis são usados com o propósito de identificar os usuários de dispositivos móveis no Servidor de Administração.

O Kaspersky Security Center Web Console e Cloud Console permite executar as seguintes ações com certificados móveis de usuário:

- Visualize os certificados e seus status.
- Crie novos certificados.
- Renove os certificados expirados.
- Exclua certificados.

Para obter mais informações sobre os certificados do Kaspersky Security Center:

- Caso use o Kaspersky Security Center Web Console, consulte a *Ajuda do Kaspersky Security Center*.
- Caso use o Kaspersky Security Center Cloud Console, consulte a *Ajuda do Kaspersky Security Center Cloud Console*.

Visualização da lista de certificados

O Kaspersky Security Center Web Console e Cloud Console permite visualizar os certificados móveis do usuário aplicados, com status e propriedades.

Para visualizar a lista de certificados móveis de usuário aplicados:

1. Na janela principal do Kaspersky Security Center Web Console ou Cloud Console, selecione **DISPOSITIVOS** > **CELULAR** > **DISPOSITIVOS**.

2. Selecione **Gerenciar certificados**.

A página **Certificados móveis** é aberta com informações sobre os certificados móveis do usuário aplicados. É possível ver os detalhes de um certificado clicando nele na coluna **Nome do usuário**.

Definição das configurações do certificado

É possível usar o Kaspersky Security Center Web Console ou Cloud Console para configurar o tempo de vida, as atualizações automáticas e a proteção por senha dos certificados móveis.

Para definir as configurações do certificado móvel:

1. Na janela principal do Kaspersky Security Center Web Console ou Cloud Console, selecione **DISPOSITIVOS** > **CELULAR** > **DISPOSITIVOS**.

2. Selecione **Gerenciar certificados**.

3. Selecione **Configurações do certificado**.

4. Na janela aberta **Gerar certificados móveis**, é possível configurar o seguinte:

   - **Período de validade do certificado (dias)**

     Período de vida do certificado em dias. O tempo de vida padrão de um certificado é de 365 dias. Quando o período expirar, o dispositivo móvel não será capaz de se conectar ao servidor de administração.

   - **Renovar quando o certificado estiver para expirar em (dias)**

     O número de dias restantes até a expiração do certificado atual durante os quais o servidor de administração deveria emitir um novo certificado. Por exemplo, se o valor do campo for 4, o servidor de administração emitirá um novo certificado quatro dias antes da expiração do certificado atual. O valor padrão é 1 semana.

   - **Renovar o certificado automaticamente, se possível**

     Caso seja possível, os certificados serão reemitidos automaticamente. Caso esta opção seja desativada, os certificados devem ser reemitidos manualmente à medida que expiram. Por padrão, a opção está desabilitada.

   - **Solicitar senha durante a instalação do certificado**

     Será solicitado ao usuário fornecer uma senha quando o certificado for instalado em um dispositivo móvel. A senha é usada apenas uma vez — durante a instalação do certificado no dispositivo móvel. A senha será gerada automaticamente pelo servidor de administração e enviada ao usuário por e-mail. É possível especificar o **Comprimento da senha** no campo.

5. Clique em **Salvar** para aplicar as alterações e fechar a janela.

As configurações especificadas serão usadas pelo Kaspersky Security Center para criar, atualizar e proteger certificados móveis.

Criação de um certificado

É possível criar os certificados móveis no Kaspersky Security Center Web Console e Cloud Console com o objetivo de identificar os usuários de dispositivos móveis.

Para criar um certificado móvel:

1. Na janela principal do Kaspersky Security Center Web Console ou Cloud Console, selecione **DISPOSITIVOS** > **CELULAR** > **DISPOSITIVOS**.

2. Selecione **Gerenciar certificados**.

3. Na janela aberta **Certificados móveis**, clique em **Adicionar** para iniciar o **Assistente de criação de certificado móvel**. Prossiga com o assistente usando o botão **Avançar**.

4. Selecione os usuários ou grupos de usuários cujos dispositivos móveis deseja gerenciar com um novo certificado.

5. Especifique os **Parâmetros de publicação**:

   - Caso deseje notificar os usuários sobre o novo certificado, marque a caixa de seleção **Notificar o usuário sobre o novo certificado**.

   - Caso queira permitir o uso de um certificado várias vezes no mesmo dispositivo, marque a caixa de seleção **Permitir o uso de um certificado várias vezes no mesmo dispositivo (apenas para dispositivos com o Kaspersky Endpoint Security for Android instalado)**.

6. Selecione o **Tipo de autenticação**:

   - Selecione **Credenciais (login ou nome de usuário de domínio)**, caso deseje que os usuários acessem o certificado usando as suas credenciais.

   - Selecione **Senha temporária**, caso deseje que os usuários acessem o certificado usando uma senha descartável.

     A opção está disponível caso não tenha marcado a caixa de seleção **Permitir o uso de um certificado várias vezes no mesmo dispositivo (apenas para dispositivos com o Kaspersky Endpoint Security for Android instalado)** na etapa anterior.

   - Selecione **Senha**, caso deseje que os usuários acessem o certificado usando uma senha.

     A opção está disponível caso marque a caixa de seleção **Permitir o uso de um certificado várias vezes no mesmo dispositivo (apenas para dispositivos com o Kaspersky Endpoint Security for Android instalado)** na etapa anterior.

7. Especifique o método de entrega do certificado no campo **Entrega de certificado**:

   - Caso tenha selecionado **Senha temporária** na etapa anterior, selecione uma das seguintes opções:

     - Caso deseje enviar a senha por e-mail, selecione **Notificar o usuário por e-mail**.

Em seguida, selecione o endereço de e-mail a ser usado ou selecione **Outro endereço de e-mail** para especificar outro endereço de e-mail.

- Caso deseje notificar os usuários sobre a senha por outros meios, selecione **Mostrar a senha depois de concluir o Assistente**.

- Caso tenha selecionado **Credenciais (login ou nome de usuário de domínio)** na etapa anterior, selecione o endereço de e-mail a ser usado ou selecione **Outro endereço de e-mail** para especificar outro endereço de e-mail.

8. O resumo do certificado é exibido.

   Certifique-se de que todos os parâmetros do link estejam corretos e clique em **Criar**.

Como resultado, o **Assistente de criação de certificado móvel** cria um certificado geral que os usuários podem instalar no dispositivo móvel. O certificado fica disponível após a próxima sincronização de dispositivos móveis com o Kaspersky Security Center.

Para obter mais informações sobre como criar certificados e configurar regras para emiti-los:

- Caso use o Kaspersky Security Center Web Console, consulte a *Ajuda do Kaspersky Security Center*.
- Caso use o Kaspersky Security Center Cloud Console, consulte a *Ajuda do Kaspersky Security Center Cloud Console*.

Renovação de um certificado

Se algum dos certificados móveis aplicados estiver prestes a expirar, será possível renová-lo usando o Kaspersky Security Center Web Console ou Cloud Console.

Para renovar um certificado móvel:

1. Na janela principal do Kaspersky Security Center Web Console ou Cloud Console, selecione **DISPOSITIVOS** > **CELULAR** > **DISPOSITIVOS**.
2. Selecione **Gerenciar certificados**.
3. Selecione o certificado que deseja renovar e clique em **Renovar**.

   O status do certificado muda para **O certificado foi renovado**.

Exclusão de um certificado

É possível excluir certificados móveis usando o Kaspersky Security Center Web Console ou Cloud Console.

Se um certificado móvel for excluído, o dispositivo não poderá mais sincronizar com o Servidor de Administração e não será possível gerenciá-lo por meio do Kaspersky Security Center. Para começar a gerenciar o dispositivo móvel novamente, será necessário reinstalar nele o aplicativo Kaspersky Endpoint Security for Android.

Para excluir um certificado móvel:

1. Na janela principal do Kaspersky Security Center Web Console ou Cloud Console, selecione **DISPOSITIVOS** > **CELULAR** > **DISPOSITIVOS**.
2. Selecione **Gerenciar certificados**.
3. Selecione o certificado que deseja excluir e clique em **Excluir**.

O certificado é excluído e removido da lista de certificados.

Trocar informações com o Firebase Cloud Messaging

O Kaspersky Endpoint Security for Android usa o serviço Firebase Cloud Messaging (FCM) para assegurar a entrega em tempo hábil de comandos a dispositivos móveis e a sincronização forçada quando as configurações de política são modificadas.

Para usar o serviço Firebase Cloud Messaging, é necessário definir as configurações do serviço no Kaspersky Security Center Web Console ou Cloud Console.

Para ativar o Firebase Cloud Messaging no Kaspersky Security Center Web Console ou Cloud Console:

1. Na janela principal do Kaspersky Security Center Web Console ou Cloud Console, selecione **DISPOSITIVOS** > **MÓVEIS** > **SINCRONIZAÇÃO DE DISPOSITIVOS ANDROID**.

   A janela **Sincronização de dispositivos Android** é aberta.
2. Nos campos **ID do remetente** e **Chave do servidor**, especifique as configurações do Firebase Cloud Messaging: SENDER_ID e Chave de API.

O Firebase Cloud Messaging está ativado.

Para obter um ID do remetente e a chave do servidor:

1. Registre-se no portal do Google.
2. Acesse Google Cloud Platform.
3. Crie um novo projeto.

   Aguarde a criação do projeto.
4. Encontre o SENDER_ID correspondente ao projeto.
5. Ative o Google Firebase Cloud Messaging for Android.
6. Siga as instruções na tela para criar as credenciais.
7. Recupere a chave de API nas propriedades das credenciais recém-criadas.

Para obter informações detalhadas sobre as operações no Google Cloud Platform, consulte a documentação.

Agora é possível usar um **ID do remetente** e uma **Chave do servidor** para definir as configurações do Firebase Cloud Messaging.

Se as configurações do Firebase Cloud Messaging não estiverem definidas, os comandos no dispositivo móvel e as configurações de política serão entregues quando o dispositivo for sincronizado com o Kaspersky Security Center de acordo com o agendamento definido na política (por exemplo, a cada 24 horas). Em outras palavras, os comandos e configurações de política serão entregues com um atraso.

Para os propósitos de apoiar a funcionalidade principal do produto, você aceita fornecer automaticamente a ID exclusiva da instalação do aplicativo (ID da Instância) ao serviço Firebase Cloud Messaging, bem como os seguintes dados:

- Informações sobre o software instalado: versão do aplicativo, ID do aplicativo, versão da compilação do aplicativo, nome do pacote do aplicativo.
- Informações sobre o computador no qual o software está instalado: versão do SO, ID do dispositivo, versão dos serviços Google.
- Informações sobre o FCM: ID do aplicativo no FCM, ID do usuário do FCM, versão do protocolo.

Os dados são transmitidos aos serviços Firebase por meio de uma conexão segura. O acesso e a proteção das informações são regulados pelos termos de uso relevantes dos serviços do Firebase: Termos de segurança e processamento de dados do Firebase, Privacidade e segurança no Firebase.

Para prevenir a troca de informações com o serviço Firebase Cloud Messaging:

1. Na janela principal do Kaspersky Security Center Web Console ou Cloud Console, selecione **DISPOSITIVOS** > **MÓVEIS** > **SINCRONIZAÇÃO DE DISPOSITIVOS ANDROID**.

   A janela **Sincronização de dispositivos Android** é aberta.

2. Clique em **Redefinir**.

3. Na janela que é aberta, clique no botão **OK** para confirmar a redefinição.

As configurações do Firebase Cloud Messaging são apagadas.

Gerenciamento de dispositivos móveis no Kaspersky Security Center Web Console e Cloud Console

É possível gerenciar dispositivos móveis no Kaspersky Security Center Web Console e Cloud Console usando políticas de grupo e enviando comandos para dispositivos móveis (somente para Android).

Para gerenciar os dispositivos móveis no Kaspersky Security Center Web Console, é preciso instalar os plug-ins de administração.

Conexão de dispositivos móveis ao Kaspersky Security Center

Para gerenciar um dispositivo móvel usando o Kaspersky Security Center Web Console ou Cloud Console, o dispositivo deve estar conectado ao Kaspersky Security Center. É possível visualizar a lista de dispositivos móveis conectados ao Kaspersky Security Center na guia **DISPOSITIVOS** > **CELULAR** > **DISPOSITIVOS** do Web Console ou Cloud Console.

Antes de conectar um dispositivo iOS, envie o endereço do Kaspersky Security Center ao usuário do dispositivo para melhorar a segurança da conexão. O usuário verá esse endereço durante a instalação do aplicativo e poderá cancelar a conexão se o endereço exibido não corresponder ao endereço enviado.

Para conectar um dispositivo móvel ao Kaspersky Security Center:

1. Inicie o Assistente de Conexão de Novos Dispositivos Móveis:

   - Na janela principal do Kaspersky Security Center Web Console ou Cloud Console, selecione **DISPOSITIVOS** > **MÓVEIS** > **DISPOSITIVOS** e clique em **Adicionar**.

   - Na janela principal do Kaspersky Security Center Web Console ou Cloud Console, selecione **USUÁRIOS E FUNÇÕES** > **USUÁRIOS**. Clique no nome do usuário ou do grupo de usuários para o qual deseja enviar o link para conectar um dispositivo móvel e selecione **DISPOSITIVOS.** Clique em **Adicionar dispositivo móvel**. Neste caso, pule a etapa 3.

   Prossiga com o Assistente usando o botão **Avançar**.

2. Selecione o sistema operacional dos dispositivos que você deseja adicionar:

   - **Android**

   - **iOS e iPadOS**

3. Selecione usuários e grupos de usuários para os quais você deseja enviar o link para conectar um dispositivo móvel.

4. Selecione os endereços de e-mail para os quais enviar o link:

   - **Todos os endereços de e-mail**

   - **Endereço de e-mail principal**

   - **Endereço de e-mail alternativo**

   - **Outro endereço de e-mail**

     Ao selecionar esta opção, especifique o endereço de e-mail abaixo.

5. O resumo do link é exibido.

   Certifique-se de que todos os parâmetros do link estejam corretos e clique em **Enviar**.

6. Uma janela é aberta com a confirmação de que o link para adicionar um dispositivo móvel foi enviado.

   Clique em **OK** para concluir o Assistente.

Quando o usuário instala o aplicativo Kaspersky Endpoint Security for Android ou o aplicativo Kaspersky Security for iOS, o dispositivo do usuário será exibido na guia **DISPOSITIVOS** > **MÓVEL** > **DISPOSITIVOS** do Web Console ou Cloud Console.

Movimentação de dispositivos móveis não atribuídos para grupos de administração

Quando o aplicativo Kaspersky Endpoint Security for Android ou o aplicativo Kaspersky Security for iOS é instalado em dispositivos móveis, eles são exibidos na página **DESCOBERTA E IMPLEMENTAÇÃO** > **DISPOSITIVOS NÃO ATRIBUÍDOS** do Kaspersky Security Center Web Console ou Cloud Console. Para gerenciar os dispositivos recém-conectados, é possível criar uma regra para a sua alocação automática a grupos de administração ou movê-los para um grupo de administração manualmente.

Para mover um dispositivo móvel não atribuído a um grupo de administração:

1. Na janela principal do Kaspersky Security Center Web Console ou Cloud Console, selecione **DESCOBERTA E IMPLEMENTAÇÃO** > **DISPOSITIVOS NÃO ATRIBUÍDOS**.
2. Selecione o dispositivo que deseja mover para um grupo de administração e clique em **Mover para o grupo**.
3. Na árvore de grupos de administração aberta, selecione o grupo de destino para o qual deseja mover o dispositivo.

   É possível criar um novo grupo de administração selecionando um grupo existente e clicando em **Adicionar grupo secundário**.
4. Clique em **Mover**.

O dispositivo é movido para o grupo de administração especificado e a política de grupo é aplicada a ele.

Envio de comandos para dispositivos móveis

É possível enviar comandos para dispositivos móveis Android para proteger dados em um dispositivo móvel perdido ou roubado ou para executar a sincronização forçada de um dispositivo móvel com o Kaspersky Security Center.

Não é possível enviar comandos para dispositivos iOS.

Os seguintes comandos são compatíveis:

- **Bloquear dispositivo**

  O dispositivo móvel é bloqueado.
- **Desbloquear dispositivo**

  O dispositivo móvel está desbloqueado. Após desbloquear um dispositivo com o Android 5.0 – 6.X em execução, a senha de desbloqueio da tela (código PIN) é reinicializada para "1234". Após desbloquear um dispositivo com o Android em execução 7.0 ou posterior, a senha de desbloqueio da tela não é modificada.
- **Redefinir para as configurações de fábrica**

  Todos os dados são excluídos do dispositivo móvel e as configurações são revertidas aos valores padrão.
- **Limpar os dados corporativos**

  Os dados em contêineres e a conta de e-mail corporativa são apagados do dispositivo móvel.
- **Localizar o dispositivo**

  O dispositivo é localizado e exibido no Google Maps. O provedor de serviços móveis pode cobrar uma taxa pelo acesso à Internet.

Em dispositivos executando Android 12 ou posterior, se o usuário tiver concedido a permissão "Usar local aproximado", o aplicativo Kaspersky Endpoint Security for Android tentará primeiro obter a localização precisa do dispositivo. Se isso não for bem-sucedido, a localização aproximada do dispositivo será retornada apenas se tiver sido recebida não mais de 30 minutos antes. Caso contrário, o comando **Localizar o dispositivo** falhará.

- **Alarme sonoro**

  O dispositivo móvel soa um alarme. O alarme soa por 5 minutos (ou durante 1 minuto se a bateria de dispositivo estiver baixa).

- **Sincronizar o dispositivo**

  O dispositivo móvel é sincronizado com o Kaspersky Security Center.

O aplicativo Kaspersky Endpoint Security for Android requer permissões específicas para a execução de comandos. Quando o assistente Configuração inicial estiver sendo executado, o Kaspersky Endpoint Security for Android solicita ao usuário conceder ao aplicativo todas as permissões necessárias. O usuário pode ignorar estas etapas ou desativar estas permissões nas configurações de dispositivo em um momento posterior. Se este for o caso, será impossível executar os comandos.

Em dispositivos executando Android 10.0 ou posterior o usuário deve conceder permissão "Permitir o tempo todo" para acessar a localização. Em dispositivos executando Android 11.0 ou posterior, o usuário também deve conceder a permissão "Enquanto usa o aplicativo" para acessar a câmera. Caso contrário, os comandos antirroubo não funcionarão. O usuário será notificado desta limitação e novamente será solicitado que conceda as permissões do nível necessário. Se o usuário selecionar a opção "Somente desta vez" para a permissão da câmera, o acesso será considerado concedido pelo aplicativo. Recomenda-se contatar o usuário diretamente, caso a permissão da câmera seja solicitada novamente.

Para enviar um comando a um dispositivo móvel:

1. Na janela principal do Kaspersky Security Center Web Console ou Cloud Console, selecione **DISPOSITIVOS** > **MÓVEIS** > **DISPOSITIVOS**.
2. Selecione o dispositivo para o qual deseja enviar o comando e clique em **Controlar** ou **Gerenciar**.
3. Selecione o comando necessário na lista **Comandos disponíveis** e clique em **OK**.
4. Clique em **OK**, caso seja solicitado confirmar a operação.

O comando especificado é enviado ao dispositivo móvel e a janela de confirmação é exibida.

Remoção de dispositivos móveis do Kaspersky Security Center

Caso não precise mais gerenciar um dispositivo móvel, o usuário pode removê-lo do Kaspersky Security Center usando o Web Console ou Cloud Console.

Para remover um dispositivo móvel do Kaspersky Security Center:

1. Remova o aplicativo móvel do dispositivo ou certifique-se de que o usuário tenha removido o aplicativo do dispositivo necessário.
2. Na janela principal do Kaspersky Security Center Web Console ou Cloud Console, selecione **DISPOSITIVOS** > **MÓVEIS** > **DISPOSITIVOS**.

3. Selecione o certificado que deseja remover e clique em **Excluir**.

4. Clique em **OK** para confirmar a operação.

O dispositivo é removido do Kaspersky Security Center.

Gerenciamento de políticas de grupo

Esta seção descreve como gerenciar políticas de grupo no Kaspersky Security Center Web Console e Cloud Console.

Políticas de grupo para gerenciar dispositivos móveis

Uma *política do grupo* é um pacote de configurações para gerenciar dispositivos móveis que pertencem a um grupo de administração e para gerenciar aplicativos móveis instalados nos dispositivos.

Você pode usar uma política para definir as configurações de dispositivos individuais como de um grupo de dispositivos. Para um grupo de dispositivos, as configurações de administração podem ser especificadas na janela de propriedades de política do grupo.

Cada parâmetro representado em uma política tem um atributo de "bloqueio", que mostra se a configuração pode ser modificada nas políticas de níveis de hierarquia inclusos (para grupos inclusos e Servidores de Administração escravos), nas configurações locais do aplicativo.

Os valores de configurações definidos na política e nas configurações locais do aplicativo são salvos no Servidor de Administração, distribuídos para dispositivos móveis durante a sincronização e salvos em dispositivos como configurações atuais. Se o usuário tiver especificado outros valores de configurações que não foram "bloqueadas", durante a próxima sincronização do dispositivo com o Servidor de Administração os novos valores de configurações são enviados para o Servidor de Administração e salvos nas configurações locais do aplicativo em vez dos valores que foram anteriormente especificados pelo administrador.

Para manter a segurança corporativa dos dispositivos móveis Android atualizada, é possível monitorar os dispositivos dos usuários quanto à conformidade com os requisitos de segurança corporativa.

Para obter mais detalhes sobre o gerenciamento de políticas e grupos de administração no Kaspersky Security Center Web Console e Cloud Console:

- Caso use o Kaspersky Security Center Web Console, consulte a *Ajuda do Kaspersky Security Center*.
- Caso use o Kaspersky Security Center Cloud Console, consulte a *Ajuda do Kaspersky Security Center Cloud Console*.

Visualização da lista de políticas de grupo

O Kaspersky Security Center Web Console e Cloud Console permite visualizar as políticas de grupo, com status e propriedades.

Para exibir a lista de políticas de grupo:

Na janela principal do Kaspersky Security Center Web Console ou Cloud Console, selecione **DISPOSITIVOS** > **POLÍTICAS E PERFIS**.

A lista de políticas de grupo é aberta com informações breves sobre as políticas de grupo. Na página, é possível criar, modificar, copiar, mover e excluir políticas de grupo.

Visualização dos resultados da distribuição da política

O Kaspersky Security Center Web Console e Cloud Console permite visualizar o gráfico de distribuição de uma política de grupo e obter informações sobre todos os dispositivos que se enquadram nessa política.

Para visualizar os resultados da distribuição de uma política de grupo:

1. Na janela principal do Kaspersky Security Center Web Console ou Cloud Console, selecione **DISPOSITIVOS** > **POLÍTICAS E PERFIS**.
2. Na lista de políticas de grupo aberta, marque a caixa de seleção ao lado do nome da política para a qual deseja ver os resultados da distribuição e clique em **Distribuição**.

A página de resultados da distribuição da política é aberta. A página contém o resumo da política, o gráfico de distribuição da política e a tabela com as informações sobre todos os dispositivos que se enquadram nessa política. É possível abrir a janela de propriedades da política clicando no botão **Configurar política**.

Criar uma política do grupo

O Kaspersky Security Center Web Console e Cloud Console permite a criação de políticas de grupo com a finalidade de gerenciar dispositivos móveis.

Para criar uma política de grupo:

1. Na janela principal do Kaspersky Security Center Web Console ou Cloud Console, selecione **DISPOSITIVOS** > **POLÍTICAS E PERFIS**.
2. Na lista de políticas de grupo do Kaspersky Security Center aberta, clique em **Caminho atual** para selecionar o Grupo de administração para o qual deseja criar uma política.

   Por padrão, a nova política de grupo é aplicada ao grupo de **Dispositivos gerenciados**.
3. Clique em **Adicionar** para iniciar o assistente de criação de política. Prossiga com o Assistente usando o botão **Avançar**.
4. Selecione um aplicativo dependendo da plataforma:
   - **Kaspersky Endpoint Security for Android**
   - **Kaspersky Security for iOS**
5. Digite o nome da nova política no campo **Nome**. Se você especificar o nome de uma política existente, será adicionado (1) automaticamente no final.
6. Selecione o status da política:
   - **Ativa**

O Assistente salva a política criada no Servidor de Administração. Na próxima sincronização do dispositivo móvel com o Servidor de Administração, a política será usada no dispositivo como a política ativa.

- **Inativa**

  O Assistente salva a política criada no Servidor de Administração como política de backup. Essa política pode ser ativada no futuro após um evento específico. Se necessário, uma política inativa pode ser mudada para o estado ativo.

  Diversas políticas podem ser criadas para um aplicativo no grupo, mas somente uma pode estar ativa. Quando uma nova política ativa é criada, a política ativa anterior torna-se automaticamente inativa.

7. É possível ativar ou desativar duas opções de herança, **Herdar configurações da política principal** e **Forçar a herança de configurações nas políticas secundárias**:

   - Caso ative a opção **Herdar as configurações da política principal** para um grupo de administração secundário e bloquear algumas configurações na política principal, não será possível alterar essas configurações na política para o grupo secundário. É possível, entretanto, alterar as configurações que não estão bloqueadas na política principal.

   - Caso desabilite a opção **Herdar as configurações da política principal** para um grupo de administração secundário, será possível alterar todas as configurações desse grupo, mesmo se algumas configurações estiverem bloqueadas na política principal.

   - Caso ative a opção **Forçar a herança de configurações em políticas secundárias** no grupo de administração principal, isso ativa a opção **Herdar as configurações da política principal** para cada política secundária. Nesse caso, não é possível desabilitar essa opção para nenhuma política secundária. Todas as configurações bloqueadas na política principal são herdadas obrigatoriamente pelos grupos secundários e não é possível alterar essas configurações nesses grupos.

   - Nas políticas para o grupo **Dispositivos gerenciados**, a opção **Herdar configurações da política principal** não afeta nenhuma configuração, porque o grupo **Dispositivos gerenciados** não possui grupos ascendentes, portanto, não herda nenhuma política.

   Por padrão, a opção **Herdar configurações da política principal** está ativada e a opção **Forçar herança de configurações nas políticas secundárias** está desativada.

8. Caso queira, é possível definir as configurações da política recém-criada. Para fazer isso, selecione a guia **CONFIGURAÇÕES DO APLICATIVO** e prossiga conforme descrito na seção "Definição das configurações de política".

   Alternativamente, é possível fazer isso mais tarde.

9. Clique em **Salvar** para criar a política.

Uma nova política de grupo para gerenciar os dispositivos móveis é criada.

Modificação de uma política de grupo

O Kaspersky Security Center Web Console e Cloud Console permite a modificação das configurações das políticas de grupo.

Para modificar uma política de grupo:

1. Abra a janela de propriedades da política:

- Na janela principal do Kaspersky Security Center Web Console ou Cloud Console, selecione **DISPOSITIVOS** > **POLÍTICAS E PERFIS**. Na lista de políticas de grupo aberta, clique no nome da política que deseja configurar.

- Na janela principal do Kaspersky Security Center Web Console ou Cloud Console, selecione **DISPOSITIVOS** > **MÓVEIS** > **DISPOSITIVOS**. Clique no dispositivo móvel que se enquadra na política que desejar configurar e, em seguida, selecione a política na guia **POLÍTICAS ATIVAS E PERFIS DE POLÍTICAS.**

2. Na janela de propriedades da política, selecione **CONFIGURAÇÕES DE APLICATIVO** e defina as configurações de política conforme descrito na seção "Definição das configurações de política".

   Também é possível definir as configurações gerais, a herança de configurações, o registro de eventos e notificações, os perfis de política e visualizar o histórico de revisão. Para obter mais informações, consulte a *Ajuda do Kaspersky Security Center*.

3. Clique no botão **Salvar** para salvar as alterações feitas na política e sair da janela de propriedades da política.

As configurações do dispositivo móvel são definidas depois da próxima sincronização do dispositivo com o Kaspersky Security Center.

Cópia de uma política de grupo

O Kaspersky Security Center Web Console e Cloud Console permite a criação de uma cópia de uma política de grupo.

Para criar uma cópia de uma política de grupo:

1. Na janela principal do Kaspersky Security Center Web Console ou Cloud Console, selecione **DISPOSITIVOS** > **POLÍTICAS E PERFIS**.

2. Na lista aberta de políticas de grupo, marque a caixa de seleção ao lado do nome da política para a qual deseja criar uma cópia e clique em **Copiar**.

3. Na árvore aberta de grupos de administração, selecione o grupo de destino no qual deseja criar uma cópia da política.

   É possível criar um novo grupo de administração selecionando um grupo existente e clicando em **Adicionar grupo secundário**.

4. Clique em **Copiar**.

5. Clique em **OK** para confirmar a operação.

Uma cópia da política será criada no grupo-alvo com o mesmo nome. O status de cada política copiada ou movida no grupo-alvo será **Inativo**. É possível alterar o status para **Ativo** a qualquer momento.

Caso uma política com um nome idêntico ao da política recém-criada ou movida já exista no grupo alvo, o índice (<next sequence number>) é adicionado ao nome da política recém-criada ou movida, por exemplo: (1).

Movimentação de uma política para outro grupo de administração

O Kaspersky Security Center Web Console e Cloud Console permite a movimentação de uma política para outro grupo de administração.

Para mover uma política para outro grupo de administração:

1. Na janela principal do Kaspersky Security Center Web Console ou Cloud Console, selecione **DISPOSITIVOS** > **POLÍTICAS E PERFIS**.
2. Na lista de políticas de grupo aberta, marque a caixa de seleção ao lado do nome da política que deseja mover para outro grupo de administração e clique em **Mover**.
3. Na árvore de grupos de administração aberta, selecione o grupo de destino para o qual deseja mover a política.

   É possível criar um novo grupo de administração selecionando um grupo existente e clicando em **Adicionar grupo secundário**.
4. Clique em **Mover**.
5. Clique em **OK** para confirmar a operação.

O resultado depende das propriedades de herança da política:

- Caso a política não tenha sido herdada no grupo de origem, ela será movida para o grupo de destino.
- Caso a política tenha sido herdada no grupo de origem, ela não será movida. Em vez disso, uma cópia desta política será criada no grupo-alvo.

O status de cada política copiada ou movida no grupo-alvo será **Inativo**. É possível alterar o status para **Ativo** a qualquer momento.

Caso uma política com um nome idêntico ao da política recém-criada ou movida já exista no grupo alvo, o índice (<next sequence number>) é adicionado ao nome da política recém-criada ou movida, por exemplo: (1).

Exclusão de uma política de grupo

O Kaspersky Security Center Web Console e Cloud Console permite a exclusão de políticas de grupo.

É possível excluir apenas uma política que não seja herdada no grupo de administração atual. Caso uma política tenha sido herdada, só será possível exclui-la do grupo de nível superior para o qual ela foi criada.

Para excluir uma política do grupo:

1. Na janela principal do Kaspersky Security Center Web Console ou Cloud Console, selecione **DISPOSITIVOS** > **POLÍTICAS E PERFIS**.
2. Na lista de políticas de grupo aberta, marque a caixa de seleção ao lado do nome da política que deseja excluir e clique em **Excluir**.

3. Clique em **OK** para confirmar a operação.

A política de grupo será excluída.

Definir as configurações de políticas

Esta seção descreve como definir as configurações das políticas do Kaspersky Security Center para o gerenciamento de dispositivos móveis.

É possível definir as configurações de política ao criar ou modificar uma política.

Configurar a proteção antivírus

É possível definir essas configurações de política apenas para dispositivos Android.

Para a detecção oportuna de ameaças, vírus e outros aplicativos maliciosos, é necessário configurar a proteção em tempo real e a execução automática da verificação de vírus.

O Kaspersky Endpoint Security for Android detecta os seguintes tipos de objetos:

- Vírus, worms, Cavalos de Troia e ferramentas maliciosas
- Adware
- Aplicativo que pode ser explorado por criminosos para danificar o dispositivo ou os dados pessoais

Devido às limitações técnicas, o Kaspersky Endpoint Security for Android não pode verificar arquivos com um tamanho de 2 GB ou mais. Durante uma verificação, o aplicativo ignora arquivos grandes e não avisa que esses arquivos foram ignorados.

Configurar a proteção em tempo real

É possível definir essas configurações de política apenas para dispositivos Android.

Para configurar a proteção em tempo real:

1. Abra a janela de propriedades da política:
   - Na janela principal do Kaspersky Security Center Web Console ou Cloud Console, selecione **DISPOSITIVOS** > **POLÍTICAS E PERFIS**. Na lista de políticas de grupo aberta, clique no nome da política que deseja configurar.
   - Na janela principal do Kaspersky Security Center Web Console ou Cloud Console, selecione **DISPOSITIVOS** > **MÓVEIS** > **DISPOSITIVOS**. Clique no dispositivo móvel que se enquadra na política que desejar configurar e, em seguida, selecione a política na guia **POLÍTICAS ATIVAS E PERFIS DE POLÍTICAS.**

2. Na janela de propriedades da política, selecione **CONFIGURAÇÕES DO APLICATIVO** > **Proteção essencial**.

3. Na seção **Antivírus**, configure a proteção do sistema de arquivos do dispositivo móvel:

   - Para ativar a proteção em tempo real do dispositivo móvel contra ameaças, selecione a caixa **Ativar a proteção antivírus em tempo real**.

   - Especifique o nível de proteção:

     - Caso queira que o Kaspersky Endpoint Security for Android verifique apenas novos aplicativos e arquivos da pasta Downloads, selecione **Verificar apenas novos aplicativos**.

     - Para ativar a proteção expandida do dispositivo móvel contra ameaças, selecione **Verificar todos os aplicativos e monitorar ações com arquivos**.

       O Kaspersky Endpoint Security for Android verificará todos os arquivos que o usuário abrir, modificar, mover, copiar, instalar ou salvar no dispositivo, assim como os novos aplicativos móveis instalados.

       Em dispositivos que executam Android 8.0 ou posterior, o Kaspersky Endpoint Security for Android verifica os arquivos que o usuário modifica, move, instala e salva, assim como as cópias dos arquivos. O Kaspersky Endpoint Security for Android não verifica os arquivos quando são abertos, ou arquivos de origem quando copiados.

   - Para ativar a verificação adicional de novos aplicativos de iniciar o dispositivo do usuário pela primeira vez por meio do serviço na nuvem da Kaspersky Security Network, marque a caixa de seleção **Proteção adicional da Kaspersky Security Network**.

   - Para bloquear adwares e aplicativos que podem ser explorados por criminosos para danificar o dispositivo ou os dados do usuário, marque a caixa de seleção **Detectar adwares, discadores automáticos e aplicativos que podem ser usados por cibercriminosos para causar danos ao dispositivo e aos dados do usuário**.

4. Na seção de **Configurações do antivírus**, selecione a ação a ser executada na detecção de ameaças:

   - **Excluir e salvar uma cópia de backup do arquivo na Quarentena**

     Os objetos detectados serão automaticamente excluídos. O usuário não deve executar qualquer ação adicional. Antes de excluir um objeto, o Kaspersky Endpoint Security for Android criará uma cópia backup do arquivo e a salvará em quarentena.

   - **Excluir**

     Os objetos detectados serão automaticamente excluídos. O usuário não deve executar qualquer ação adicional. Antes de excluir um objeto, o Kaspersky Endpoint Security for Android exibirá uma notificação temporária sobre a detecção do objeto.

   - **Ignorar**

     Se os objetos detectados foram ignorados, o Kaspersky Endpoint Security for Android avisa o usuário sobre os problemas na proteção do dispositivo. As informações sobre os objetos ignorados são exibidas na seção **Status** do aplicativo. Para cada ameaça ignorada, o aplicativo fornece ações que o usuário pode executar para eliminar a ameaça. A lista de objetos ignorados pode modificar-se, por exemplo, se um arquivo malicioso foi excluído ou movido. Para receber uma lista atualizada de ameaças, execute uma verificação completa do dispositivo. Para assegurar a proteção confiável dos dados, elimine todos os objetos detectados.

5. Clique no botão **Salvar** para salvar as alterações feitas na política e sair da janela de propriedades da política.

As configurações do dispositivo móvel são definidas depois da próxima sincronização do dispositivo com o Kaspersky Security Center.

Configurar a execução automática da verificação de vírus em um dispositivo móvel

É possível definir essas configurações de política apenas para dispositivos Android.

Para configurar a execução automática da verificação de vírus em um dispositivo móvel:

1. Abra a janela de propriedades da política:

   - Na janela principal do Kaspersky Security Center Web Console ou Cloud Console, selecione **DISPOSITIVOS** > **POLÍTICAS E PERFIS**. Na lista de políticas de grupo aberta, clique no nome da política que deseja configurar.

   - Na janela principal do Kaspersky Security Center Web Console ou Cloud Console, selecione **DISPOSITIVOS** > **MÓVEIS** > **DISPOSITIVOS**. Clique no dispositivo móvel que se enquadra na política que desejar configurar e, em seguida, selecione a política na guia **POLÍTICAS ATIVAS E PERFIS DE POLÍTICAS.**

2. Na janela de propriedades da política, selecione **CONFIGURAÇÕES DO APLICATIVO** > **Proteção essencial**.

3. Para bloquear adwares e aplicativos que podem ser explorados por criminosos para danificar o dispositivo ou os dados do usuário, marque a caixa de seleção **Detectar adwares, discadores automáticos e aplicativos que podem ser usados por cibercriminosos para causar danos ao dispositivo e aos dados do usuário** na seção **Verificação do dispositivo**.

4. Na lista **Ação na detecção de ameaças**, selecione uma das seguintes opções:

   - **Excluir e salvar uma cópia de backup do arquivo na Quarentena**

     Os objetos detectados serão automaticamente excluídos. O usuário não deve executar qualquer ação adicional. Antes de excluir um objeto, o Kaspersky Endpoint Security for Android criará uma cópia backup do arquivo e a salvará em quarentena.

   - **Excluir**

     Os objetos detectados serão automaticamente excluídos. O usuário não deve executar qualquer ação adicional. Antes de excluir um objeto, o Kaspersky Endpoint Security for Android exibirá uma notificação temporária sobre a detecção do objeto.

   - **Ignorar**

     Se os objetos detectados foram ignorados, o Kaspersky Endpoint Security for Android avisa o usuário sobre os problemas na proteção do dispositivo. As informações sobre os objetos ignorados são exibidas na seção **Status** do aplicativo. Para cada ameaça ignorada, o aplicativo fornece ações que o usuário pode executar para eliminar a ameaça. A lista de objetos ignorados pode modificar-se, por exemplo, se um arquivo malicioso foi excluído ou movido. Para receber uma lista atualizada de ameaças, execute uma verificação completa do dispositivo. Para assegurar a proteção confiável dos dados, elimine todos os objetos detectados.

- **Perguntar ao usuário**

  O aplicativo Kaspersky Endpoint Security for Android exibe uma notificação solicitando que o usuário escolha a ação a ser executada no objeto detectado: **Ignorar** ou **Excluir**.

  Quando o aplicativo detectar diversos objetos, a opção **Perguntar ao usuário** permite que o usuário do dispositivo aplique a ação selecionada a cada arquivo usando a caixa de seleção **Aplicar a todas as ameaças**.

  O Kaspersky Endpoint Security for Android deve ser definido como um recurso de Acessibilidade para assegurar a exibição de notificações em dispositivos móveis com Android 10.0 ou posterior. O Kaspersky Endpoint Security for Android solicita que o usuário defina o aplicativo como um recurso de Acessibilidade pelo Assistente de Configuração Inicial. O usuário pode ignorar esta etapa ou desativar este serviço nas configurações de dispositivo em um momento posterior. Nesse caso, o Kaspersky Endpoint Security for Android exibe uma janela de sistema do Android solicitando que o usuário escolha a ação a ser executada no objeto detectado: Ignorar ou Excluir. Para aplicar a ação a múltiplos objetos, é preciso abrir o Kaspersky Endpoint Security.

5. Na seção **Verificação agendada**, é possível configurar a verificação completa automática do sistema de arquivos do dispositivo.

   Selecione uma das seguintes opções:

   - **Desativado**

     A verificação do sistema de arquivos do dispositivo não será iniciada automaticamente.

   - **Após a atualização do banco de dados**

     O sistema de arquivos do dispositivo será verificado automaticamente a cada atualização do banco de dados antivírus.

   - **Diariamente**

     O sistema de arquivos do dispositivo será verificado automaticamente todos os dias.

     Se selecionar essa opção, também poderá especificar a hora da verificação no campo **Hora de início**.

   - **Semanalmente às(aos)**

     O sistema de arquivos do dispositivo será verificado automaticamente uma vez por semana.

     Se selecionar essa opção, também poderá selecionar o dia da semana em que deseja executar a verificação, usando a lista suspensa, bem como especificar a hora da varredura no campo **Hora de início**.

   No Android 12 ou posterior, o aplicativo pode realizar essa tarefa após o especificado se o dispositivo estiver no modo de economia de bateria.

6. Clique no botão **Salvar** para salvar as alterações feitas na política e sair da janela de propriedades da política.

As configurações do dispositivo móvel são definidas depois da próxima sincronização do dispositivo com o Kaspersky Security Center.

Configurar atualizações do banco de dados antivírus

É possível definir essas configurações de política apenas para dispositivos Android.

Para configurar as atualizações do banco de dados antivírus:

1. Abra a janela de propriedades da política:

   - Na janela principal do Kaspersky Security Center Web Console ou Cloud Console, selecione **DISPOSITIVOS** > **POLÍTICAS E PERFIS**. Na lista de políticas de grupo aberta, clique no nome da política que deseja configurar.

   - Na janela principal do Kaspersky Security Center Web Console ou Cloud Console, selecione **DISPOSITIVOS** > **MÓVEIS** > **DISPOSITIVOS**. Clique no dispositivo móvel que se enquadra na política que desejar configurar e, em seguida, selecione a política na guia **POLÍTICAS ATIVAS E PERFIS DE POLÍTICAS.**

2. Na janela de propriedades da política, selecione **CONFIGURAÇÕES DO APLICATIVO** > **Atualização do banco de dados**.

3. Na seção **Atualização do banco de dados**, configure o agendamento das atualizações automáticas do banco de dados no dispositivo do usuário.

   Selecione uma das seguintes opções:

   - **Desativado**

     As atualizações automáticas dos bancos de dados antivírus serão desativadas.

   - **Diariamente**

     Os bancos de dados antivírus serão atualizados todos os dias.

     Se selecionar essa opção, também poderá especificar a hora da atualização no campo **Hora da atualização**.

   - **Semanalmente**

     Os bancos de dados antivírus serão atualizados uma vez por semana.

     Se selecionar essa opção, também poderá especificar a hora da atualização no campo **Hora da atualização**, bem como o dia da semana em que deseja executar a atualização na lista suspensa **Dia da semana**.

   No Android 12 ou posterior, o aplicativo pode realizar essa tarefa após o especificado se o dispositivo estiver no modo de economia de bateria.

4. Na seção **Origem de atualização do banco de dados**, especifique a origem de atualização a partir da qual o Kaspersky Endpoint Security for Android recebe e instala as atualizações do banco de dados antivírus:

   - **Servidores da Kaspersky**

     O Kaspersky Endpoint Security for Android usará um servidor de atualizações da Kaspersky como fonte de atualização para baixar os bancos de dados antivírus para o dispositivo do usuário.

   - **Servidor de administração**

     Disponível apenas se você usar o Kaspersky Security Center Web Console.

     O Kaspersky Endpoint Security for Android usará o repositório do servidor de administração do Kaspersky Security Center como fonte de atualização a fim de baixar bancos de dados antivírus para o dispositivo do usuário.

- **Outra origem**

  O Kaspersky Endpoint Security for Android usará um servidor de terceiros como fonte de atualização a fim de baixar bancos de dados antivírus para o dispositivo do usuário.

  Se selecionar essa opção, será necessário especificar o endereço HTTP do servidor no campo **Use outro servidor como fonte de atualização para bancos de dados antivírus**.

5. Caso queira que o Kaspersky Endpoint Security for Android baixe as atualizações do banco de dados antivírus de acordo com a agenda de atualizações com o dispositivo do usuário em roaming, marque a caixa de seleção **Permitir a atualização do banco de dados quando em roaming** na seção **Atualizar os bancos de dados antivírus quando em roaming** em roaming.

6. Clique no botão **Salvar** para salvar as alterações feitas na política e sair da janela de propriedades da política.

As configurações do dispositivo móvel são definidas depois da próxima sincronização do dispositivo com o Kaspersky Security Center.

Definir as configurações de desbloqueio do dispositivo

É possível definir essas configurações de política apenas para dispositivos Android.

Para manter o dispositivo móvel seguro, é necessário definir uma senha que será solicitada ao usuário quando o dispositivo sair do modo ocioso.

É possível impor restrições à atividade do usuário no dispositivo se a senha de desbloqueio do dispositivo for fraca (por exemplo, bloquear o dispositivo). É possível impor restrições por meio do componente Controle de conformidade.

Em determinados dispositivos Samsung que executam o Android 7.0 ou posterior, quando o usuário tenta configurar métodos não compatíveis para desbloquear o dispositivo (por exemplo, uma senha gráfica), o dispositivo pode ser bloqueado se as seguintes condições forem atendidas: A remoção do Kaspersky Endpoint Security for Android está ativada e os requisitos de força da senha de desbloqueio da tela estão definidos. Para desbloquear o dispositivo, é necessário enviar um comando especial ao dispositivo.

Para configurar a força da senha de desbloqueio:

1. Abra a janela de propriedades da política:

   - Na janela principal do Kaspersky Security Center Web Console ou Cloud Console, selecione **DISPOSITIVOS** > **POLÍTICAS E PERFIS**. Na lista de políticas de grupo aberta, clique no nome da política que deseja configurar.

   - Na janela principal do Kaspersky Security Center Web Console ou Cloud Console, selecione **DISPOSITIVOS** > **MÓVEIS** > **DISPOSITIVOS**. Clique no dispositivo móvel que se enquadra na política que desejar configurar e, em seguida, selecione a política na guia **POLÍTICAS ATIVAS E PERFIS DE POLÍTICAS.**

2. Na janela de propriedades da política, selecione **CONFIGURAÇÕES DO APLICATIVO** > **Proteção essencial**.

3. Caso queira que o aplicativo verifique se uma senha de desbloqueio foi definida, selecione **Exigir a definição da senha de desbloqueio da tela** na seção **Proteção por senha**.

   Se o aplicativo detectar que nenhuma senha do sistema foi definida no dispositivo, o usuário será solicitado a defini-la. A senha é definida de acordo com os parâmetros definidos pelo administrador.

4. Especifique o número mínimo de caracteres da senha do usuário.

   Valores possíveis: 4 a 16 caracteres.

   A senha do usuário tem 4 caracteres por padrão.

   Para dispositivos com Android 10.0 ou posterior, o Kaspersky Endpoint Security divide os requisitos da força de segurança da senha em um dos valores do sistema: médio ou alto.

   Os valores para dispositivos com Android 10.0 ou posterior são determinados pelas seguintes regras:

   - Se a quantidade de símbolos exigida for de 1 a 4, então o aplicativo solicita ao usuário que defina uma senha de força média. Ela deve ser numérica (PIN), sem números repetidos ou sequenciais (ex. 1234), ou alfanumérica. O PIN ou a senha deve ter no mínimo 4 caracteres.

   - Se o número de símbolos exigidos for 5 ou mais, então o aplicativo solicita ao usuário que defina uma senha de segurança alta. Ela deve ser numérica (PIN), sem números repetidos ou sequenciais, ou alfanumérica (senha). O PIN deve ter no mínimo 8 dígitos; a senha deve ter no mínimo 6 caracteres.

5. Caso queira usar impressões digitais para desbloquear a tela, marque a caixa de seleção **Permitir o uso de impressões digitais (para dispositivos com Android 9 ou anterior)**. Se a senha de desbloqueio não estiver em conformidade com os requisitos de segurança corporativa, não será possível usar um digitalizador de impressão digital para desbloquear a tela.

   O uso da impressão digital para desbloquear a tela não é compatível com dispositivos Android 10.0 ou posteriores.

   O Kaspersky Endpoint Security for Android não restringe o uso de um digitalizador de impressão digital para efetuar o login em aplicativos ou para confirmar compras.

   Em determinados dispositivos Samsung é impossível bloquear o uso de impressões digitais para desbloquear a tela.

   Em determinados dispositivos Samsung, se a senha de desbloqueio não estiver em conformidade com requisitos de segurança corporativa, o Kaspersky Endpoint Security for Android não bloqueia o uso de impressões digitais para desbloquear a tela.

   Após adicionar uma impressão digital nas configurações do dispositivo, o usuário pode desbloquear a tela por meio dos seguintes métodos:

   - Passe o dedo no digitalizador de impressão digital (método principal).

   - Insira a senha de desbloqueio (método de backup).

6. Clique no botão **Salvar** para salvar as alterações feitas na política e sair da janela de propriedades da política.

As configurações do dispositivo móvel são definidas depois da próxima sincronização do dispositivo com o Kaspersky Security Center.

Configurar a proteção de dados de dispositivos perdidos ou roubados

É possível definir essas configurações de política apenas para dispositivos Android.

Para proteger os dados corporativos no caso de o dispositivo móvel ser perdido ou roubado, é necessário configurar a proteção contra acesso não autorizado.

Para garantir a proteção de dados de dispositivos roubados ou perdidos, o Kaspersky Endpoint Security for Android deve ser definido como um recurso de acessibilidade. O Kaspersky Endpoint Security for Android solicita que o usuário defina o aplicativo como um recurso de Acessibilidade pelo Assistente de Configuração Inicial. O usuário pode ignorar esta etapa ou desativar este serviço nas configurações de dispositivo em um momento posterior.

Para configurar a proteção de dados de dispositivos perdidos ou roubados:

1. Abra a janela de propriedades da política:

   - Na janela principal do Kaspersky Security Center Web Console ou Cloud Console, selecione **DISPOSITIVOS** > **POLÍTICAS E PERFIS**. Na lista de políticas de grupo aberta, clique no nome da política que deseja configurar.

   - Na janela principal do Kaspersky Security Center Web Console ou Cloud Console, selecione **DISPOSITIVOS** > **MÓVEIS** > **DISPOSITIVOS**. Clique no dispositivo móvel que se enquadra na política que desejar configurar e, em seguida, selecione a política na guia **POLÍTICAS ATIVAS E PERFIS DE POLÍTICAS.**

2. Na janela de propriedades da política, selecione **CONFIGURAÇÕES DO APLICATIVO** > **Proteção essencial**.

3. Na seção **Antirroubo**, configure o bloqueio do dispositivo:

   - Especifique o número de caracteres do código de desbloqueio.

   - Especifique o texto a ser exibido quando o dispositivo for bloqueado.

4. Clique no botão **Salvar** para salvar as alterações feitas na política e sair da janela de propriedades da política.

   As configurações do dispositivo móvel são definidas depois da próxima sincronização do dispositivo com o Kaspersky Security Center.

Configurar o controle de aplicativos

É possível definir essas configurações de política apenas para dispositivos Android.

O *Controle de Aplicativos* verifica que se os aplicativos instalados em um dispositivo móvel estejam em conformidade com os requisitos da segurança corporativa. No Kaspersky Security Center, o administrador cria listas de aplicativos permitidos, bloqueados, obrigatórios e recomendados segundo os requisitos da segurança corporativa. Como resultado do Controle de aplicativos, o Kaspersky Endpoint Security solicita que o usuário instale aplicativos obrigatórios e recomendados e que remova os aplicativos bloqueados. É impossível iniciar aplicativos bloqueados no dispositivo móvel do usuário.

No Web Console e no Cloud Console do Kaspersky Security Center, é possível gerenciar aplicativos nos dispositivos dos usuários usando regras predefinidas. É possível configurar dois tipos de regras do **Controle de aplicativos**: regras de aplicativos e regras de categoria.

A **Regra do aplicativo** se aplica a um aplicativo específico, enquanto a **Regra da categoria** se aplica a qualquer aplicativo que pertença a uma categoria predefinida. As categorias de aplicativos são especificadas pelos especialistas da Kaspersky.

*Para configurar o **Controle de aplicativos**:*

1. Abra a janela de propriedades da política:

   - Na janela principal do Kaspersky Security Center Web Console ou Cloud Console, selecione **DISPOSITIVOS** > **POLÍTICAS E PERFIS**. Na lista de políticas de grupo aberta, clique no nome da política que deseja configurar.

   - Na janela principal do Kaspersky Security Center Web Console ou Cloud Console, selecione **DISPOSITIVOS** > **MÓVEIS** > **DISPOSITIVOS**. Clique no dispositivo móvel que se enquadra na política que desejar configurar e, em seguida, selecione a política na guia **POLÍTICAS ATIVAS E PERFIS DE POLÍTICAS.**

2. Na página de propriedades da política, selecione **CONFIGURAÇÕES DO APLICATIVO** > **Controles de segurança**.

3. Na tabela da seção **Controle de aplicativos**, adicione regras que definirão quais aplicativos serão controlados.

   - Para adicionar uma regra a um aplicativo específico:

     a. Na tabela, clique em **Regra do aplicativo**.

     b. Na janela **Regra do aplicativo** que é aberta, escolha a ação que será executada com os aplicativos cobertos pela regra criada.

     c. Especifique o aplicativo que estará sujeito à regra preenchendo **Link para o pacote de instalação (por exemplo, https://play.google.com/store/apps/details?id=com.kaspersky.kes)**, **Nome do pacote (por exemplo, katana.facebook.com)** e **Nome do aplicativo**.

     d. Clique em **Salvar**.

     A regra será adicionada à lista de regras do **Controle de aplicativos**.

   - Para adicionar uma regra a uma categoria de aplicativos:

     a. Na tabela da seção **Controle de aplicativos**, clique em **Regra da categoria**.

     b. Na janela **Regra da categoria** que será aberta, selecione a categoria de aplicativos na lista suspensa.

     Os aplicativos da categoria selecionada estarão sujeitos à regra criada.

     c. Na seção **Modo de operação**, selecione a ação que será realizada quando for tentada a execução de algum aplicativo da categoria selecionada **Aplicativos proibidos** ou **Aplicativos permitidos**.

d. Preencha o **Comentários adicionais mostrados no dispositivo do usuário quando um aplicativo de uma categoria especificada é detectado**, se necessário.

e. Clique em **Salvar**.

A regra será adicionada à lista de regras do **Controle de aplicativos**.

4. Na seção **Ações com aplicativos proibidos**, escolha qual ação será executada para aplicativos proibidos:

   - Caso queira que o Kaspersky Endpoint Security for Android bloqueie a abertura de aplicativos proibidos no dispositivo móvel do usuário, selecione **Bloquear a inicialização de aplicativos**.
   - Caso queira que o Kaspersky Endpoint Security for Android envie dados de aplicativos proibidos ao registro de eventos sem bloqueá-los, selecione **Não bloquear aplicativos proibidos, apenas informar**.

5. Na seção **Modo de operação**, escolha se as regras adicionadas definirão os aplicativos permitidos ou proibidos:

   - Caso queira que as regras definam quais aplicativos são permitidos, selecione **Aplicativos proibidos**.

     Caso queira que o Kaspersky Endpoint Security for Android bloqueie a abertura de aplicativos do sistema no dispositivo móvel do usuário (tal como Calendário, Câmera e Configurações), no modo **Aplicativos proibidos**, marque a caixa de seleção **Bloquear aplicativos do sistema**.

     > Os especialistas da Kaspersky recomendam não bloquear os aplicativos do sistema porque isso pode levar a falhas na operação do dispositivo.

   - Caso queira que as regras definam quais aplicativos são proibidos, selecione **Aplicativos permitidos**.

6. Para receber informações de todos os aplicativos instalados em dispositivos móveis, na seção **Relatório do aplicativo**, marque a caixa de seleção **Enviar uma lista de aplicativos instalados em todos os dispositivos móveis**.

   O Kaspersky Endpoint Security for Android envia dados ao log de eventos cada vez que um aplicativo é instalado ou removido do dispositivo.

7. Clique no botão **Salvar** para salvar as alterações feitas na política e sair da janela de propriedades da política.

As configurações do dispositivo móvel são definidas depois da próxima sincronização do dispositivo com o Kaspersky Security Center.

Configurar o controle de conformidade de dispositivos móveis com requisitos de segurança corporativa

> É possível definir essas configurações de política apenas para dispositivos Android.

O controle de conformidade permite monitorar a conformidade dos dispositivos Android com os requisitos de segurança corporativa e tomar medidas em caso de não conformidade. Os requisitos de segurança corporativa regulam como o usuário pode trabalhar com o dispositivo. Por exemplo, a proteção em tempo real deve ser ativada no dispositivo, os bancos de dados antivírus devem estar atualizados e a senha do dispositivo deve ser suficientemente forte. O controle de conformidade tem base em uma lista de regras. Uma regra de conformidade inclui os seguintes componentes:

- Critério de não conformidade do dispositivo.
- A ação que será executada no dispositivo se o usuário não corrigir a não conformidade dentro do prazo definido.
- Período do tempo alocado para o usuário para corrigir a não conformidade (por exemplo, 24 horas).

  Quando o prazo especificado terminar, a ação selecionada será executada no dispositivo do usuário.

  > No Android 12 ou posterior, o aplicativo pode realizar essa tarefa após o especificado se o dispositivo estiver no modo de economia de bateria.

Para configurar o controle de conformidade, é possível executar as seguintes ações:

- Ativar ou desativar as regras de conformidade existentes.
- Editar uma regra de conformidade existente.
- Adicionar uma nova regra.
- Excluir uma regra.

Ativar e desativar as regras de conformidade

> É possível definir essas configurações de política apenas para dispositivos Android.

Para ativar ou desativar as regras existentes de controle de conformidade de dispositivos móveis com requisitos de segurança corporativa:

1. Abra a janela de propriedades da política:
   - Na janela principal do Kaspersky Security Center Web Console ou Cloud Console, selecione **DISPOSITIVOS** > **POLÍTICAS E PERFIS**. Na lista de políticas de grupo aberta, clique no nome da política que deseja configurar.
   - Na janela principal do Kaspersky Security Center Web Console ou Cloud Console, selecione **DISPOSITIVOS** > **MÓVEIS** > **DISPOSITIVOS**. Clique no dispositivo móvel que se enquadra na política que desejar configurar e, em seguida, selecione a política na guia **POLÍTICAS ATIVAS E PERFIS DE POLÍTICAS.**
2. Na página de propriedades da política, selecione **CONFIGURAÇÕES DO APLICATIVO** > **Controles de segurança**.
3. Na seção **Controle de conformidade**, ative ou desative as regras de conformidade existentes usando os botões de seleção na coluna **Status**.
4. Clique no botão **Salvar** para salvar as alterações feitas na política e sair da janela de propriedades da política.

As configurações do dispositivo móvel são definidas depois da próxima sincronização do dispositivo com o Kaspersky Security Center.

Editar as regras de conformidade

É possível definir essas configurações de política apenas para dispositivos Android.

Para editar uma regra a fim de controlar a conformidade dos dispositivos móveis com os requisitos de segurança corporativa:

1. Abra a janela de propriedades da política:

   - Na janela principal do Kaspersky Security Center Web Console ou Cloud Console, selecione **DISPOSITIVOS** > **POLÍTICAS E PERFIS**. Na lista de políticas de grupo aberta, clique no nome da política que deseja configurar.

   - Na janela principal do Kaspersky Security Center Web Console ou Cloud Console, selecione **DISPOSITIVOS** > **MÓVEIS** > **DISPOSITIVOS**. Clique no dispositivo móvel que se enquadra na política que desejar configurar e, em seguida, selecione a política na guia **POLÍTICAS ATIVAS E PERFIS DE POLÍTICAS.**

2. Na página de propriedades da política, selecione **CONFIGURAÇÕES DO APLICATIVO** > **Controles de segurança**.

3. Na seção **Controle de conformidade**, selecione a regra que deseja editar e clique em **Editar**.

4. Na janela **Regra** que se abre, edite a regra da seguinte maneira:

   a. Na coluna **Ação**, configure a lista de ações a serem realizadas em caso de não conformidade com a regra, adicionando novas ações, editando as ações existentes ou as excluindo.

   b. Opcionalmente, especifique o prazo para o usuário corrigir a não conformidade usando a coluna **Tempo para a correção** para cada ação.

   c. Clique no botão **Salvar** para salvar a regra.

5. Clique no botão **Salvar** para salvar as alterações feitas na política e sair da janela de propriedades da política.

As configurações do dispositivo móvel são definidas depois da próxima sincronização do dispositivo com o Kaspersky Security Center.

Adicionar regras de conformidade

É possível definir essas configurações de política apenas para dispositivos Android.

Para adicionar uma regra a fim de controlar a conformidade dos dispositivos móveis com os requisitos de segurança corporativa:

1. Abra a janela de propriedades da política:

   - Na janela principal do Kaspersky Security Center Web Console ou Cloud Console, selecione **DISPOSITIVOS** > **POLÍTICAS E PERFIS**. Na lista de políticas de grupo aberta, clique no nome da política que deseja

configurar.

- Na janela principal do Kaspersky Security Center Web Console ou Cloud Console, selecione **DISPOSITIVOS** > **MÓVEIS** > **DISPOSITIVOS**. Clique no dispositivo móvel que se enquadra na política que desejar configurar e, em seguida, selecione a política na guia **POLÍTICAS ATIVAS E PERFIS DE POLÍTICAS.**

2. Na página de propriedades da política, selecione **CONFIGURAÇÕES DO APLICATIVO** > **Controles de segurança**.

3. Na seção **Controle de conformidade**, clique em **Regra**.

4. Na janela **Regra** que se abre, defina a regra da seguinte maneira:

   a. Selecione o critério de não conformidade para a regra.

   b. Clique em **Adicionar** e selecione a ação a ser realizada em caso de não conformidade com a regra na coluna **Ação**.

   É possível adicionar várias ações.

   c. Especifique o prazo para o usuário corrigir a não conformidade usando a coluna **Tempo para a correção** para cada ação.

   d. Clique no botão **Salvar** para salvar a regra.

5. Clique no botão **Salvar** para salvar as alterações feitas na política e sair da janela de propriedades da política.

As configurações do dispositivo móvel são definidas depois da próxima sincronização do dispositivo com o Kaspersky Security Center.

Excluir regras de conformidade

É possível definir essas configurações de política apenas para dispositivos Android.

Para excluir uma regra a fim de controlar a conformidade dos dispositivos móveis com os requisitos de segurança corporativa:

1. Abra a janela de propriedades da política:

   - Na janela principal do Kaspersky Security Center Web Console ou Cloud Console, selecione **DISPOSITIVOS** > **POLÍTICAS E PERFIS**. Na lista de políticas de grupo aberta, clique no nome da política que deseja configurar.

   - Na janela principal do Kaspersky Security Center Web Console ou Cloud Console, selecione **DISPOSITIVOS** > **MÓVEIS** > **DISPOSITIVOS**. Clique no dispositivo móvel que se enquadra na política que desejar configurar e, em seguida, selecione a política na guia **POLÍTICAS ATIVAS E PERFIS DE POLÍTICAS.**

2. Na página de propriedades da política, selecione **CONFIGURAÇÕES DO APLICATIVO** > **Controles de segurança**.

3. Na seção **Controle de conformidade**, selecione a regra que deseja excluir e clique em **Excluir**.

4. Clique no botão **Salvar** para salvar as alterações feitas na política e sair da janela de propriedades da política.

As configurações do dispositivo móvel são definidas depois da próxima sincronização do dispositivo com o Kaspersky Security Center.

Lista de critérios de não conformidade

É possível definir essas configurações de política apenas para dispositivos Android.

Para garantir que o dispositivo Android esteja em conformidade com os requisitos de segurança corporativa, o Kaspersky Endpoint Security for Android pode verificar o dispositivo de acordo com os seguintes critérios:

- **A proteção em tempo real está desativada**.

  A proteção em tempo real deve ser ativada.

  Para obter mais informações sobre como configurar a proteção em tempo real, consulte a seção "Configurar a proteção em tempo real".

- **Os bancos de dados do antivírus estão desatualizados**.

  O banco de dados antivírus do Kaspersky Endpoint Security for Android deve ser atualizado regularmente.

  Para obter mais informações sobre como definir as configurações de atualizações do banco de dados antivírus, consulte a seção "Configurar a proteção antivírus".

- **Aplicativos proibidos estão instalados**.

  O dispositivo não deve ter instalados aqueles aplicativos classificados como **Bloquear a inicialização**, conforme previsto na seção **Controle de aplicativos**.

  Para obter mais informações sobre a criação de regras para aplicativos, consulte a seção "Configurar o controle de aplicativos".

- **Aplicativos de categorias proibidas estão instalados**.

  O dispositivo não deve ter instalados aqueles aplicativos que se enquadram na categoria classificada como **Bloquear a inicialização**, conforme previsto na seção **Controle de aplicativos**.

  Para obter mais informações sobre a criação de regras para categorias de aplicativos, consulte a seção "Configurar o controle de aplicativos".

- **Nem todos os aplicativos obrigatórios estão instalados**.

  O dispositivo deve ter instalados aqueles aplicativos específicos classificados como **Instalação forçada**, conforme previsto na seção **Controle de aplicativos**.

  Para obter mais informações sobre a criação de regras para aplicativos, consulte a seção "Configurar o controle de aplicativos".

- **A versão do sistema operacional está desatualizada**.

  O dispositivo deve ter uma versão permitida do sistema operacional.

  Para usar esse critério de não conformidade, é preciso especificar o intervalo de versões permitidas do sistema operacional nas listas suspensas **Versão mínima do sistema operacional** e **Versão máxima do sistema operacional**.

- **O dispositivo não foi sincronizado faz tempo**.

  O dispositivo deve ser sincronizado regularmente com o Servidor de administração.

  Para usar esse critério de não conformidade, é necessário especificar o intervalo máximo entre as sincronizações do dispositivo na lista suspensa **Período de sincronização**.

- **O dispositivo foi roteado**.

  O dispositivo não deve ser modificado.

  Para obter mais informações, consulte a seção "Detectar invasões do dispositivo (raiz)".

- **A senha de desbloqueio não está em conformidade com os requisitos de segurança**.

  O dispositivo deve ser protegido com uma senha de desbloqueio que esteja em conformidade com os requisitos de força da senha de desbloqueio.

Lista de ações em caso de não conformidade

É possível definir essas configurações de política apenas para dispositivos Android.

Se o usuário não corrigir o problema de não conformidade dentro do tempo especificado, as seguintes ações estarão disponíveis:

- **Bloquear todos os aplicativos, exceto os aplicativos do sistema**.

  Todos os aplicativos no dispositivo móvel do usuário são bloqueados contra inicialização, com exceção dos aplicativos do sistema.

- **Bloquear dispositivo**.

  O dispositivo móvel é bloqueado. Para obter o acesso aos dados, você deve desbloquear o dispositivo. Se o motivo para bloquear o dispositivo não for corrigido depois que o dispositivo for desbloqueado, o dispositivo será novamente bloqueado após o período especificado.

- **Limpar os dados corporativos**.

  Limpam-se os dados em contêineres, a conta de e-mail corporativa, a configurações para conexão com a rede Wi-Fi e VPN corporativos, bem como o nome de ponto do acesso (APN).

- **Redefinir por completo o dispositivo para as configurações de fábrica**.

  Todos os dados são excluídos do dispositivo móvel e as configurações são revertidas aos valores de fábrica.

Configurar o acesso do usuários aos sites

É possível definir essas configurações de política para dispositivos Android e iOS.

Para proteger dados pessoais e corporativos armazenados em dispositivos móveis durante a navegação na Internet, você pode configurar o acesso do usuário a sites usando a Proteção na Web. A Proteção na Web verifica os sites antes que o usuário os abra e, em seguida, bloqueia sites que distribuem códigos maliciosos e sites de phishing projetados para roubar dados confidenciais e obter acesso a contas financeiras.

Para dispositivos Android, esse recurso também é compatível com a filtragem de sites por categorias definidas no serviço de nuvem da Kaspersky Security Network. A filtragem permite restringir o acesso a determinados sites ou categorias de sites (por exemplo, categorias de "**Jogos de azar, loterias, apostas**" ou "**Comunicações via Internet**").

Em dispositivos Android, a Proteção na Web funciona apenas nos navegadores Google Chrome, Huawei Browser e Samsung Internet Browser.

Para garantir a operação adequada da Proteção na Web, o Kaspersky Endpoint Security for Android deve ser definido como um recurso de acessibilidade. O Kaspersky Endpoint Security for Android solicita que o usuário defina o aplicativo como um recurso de Acessibilidade pelo Assistente de Configuração Inicial. O usuário pode ignorar esta etapa ou desativar este serviço nas configurações de dispositivo em um momento posterior.

Em dispositivos iOS, o usuário deve permitir que o aplicativo Kaspersky Security for iOS adicione uma configuração de VPN para que a Proteção na Web funcione.

Para configurar o acesso do usuário aos sites:

1. Abra a janela de propriedades da política:
   - Na janela principal do Kaspersky Security Center Web Console ou Cloud Console, selecione **DISPOSITIVOS** > **POLÍTICAS E PERFIS**. Na lista de políticas de grupo aberta, clique no nome da política que deseja configurar.
   - Na janela principal do Kaspersky Security Center Web Console ou Cloud Console, selecione **DISPOSITIVOS** > **MÓVEIS** > **DISPOSITIVOS**. Clique no dispositivo móvel que se enquadra na política que desejar configurar e, em seguida, selecione a política na guia **POLÍTICAS ATIVAS E PERFIS DE POLÍTICAS.**
2. Na página de propriedades da política, selecione **CONFIGURAÇÕES DO APLICATIVO** > **Controles de segurança**.
3. Na seção **Proteção na Web**, marque a caixa de seleção **Ativar a Proteção na Web** para ativar o recurso.
4. Para dispositivos Android, você pode selecionar uma das seguintes opções:
   - Para restringir o acesso do usuário a sites com base no conteúdo:
     a. Selecione **Bloquear sites de categorias especificadas**.
     b. Marque as caixas de seleção ao lado das categorias de sites aos quais o Kaspersky Endpoint Security for Android bloqueará o acesso.

     Se a Proteção na Web estiver ativada, o acesso do usuário a sites das categorias **Phishing** e **Sites de malwares** permanecerá sempre bloqueado.
   - Para especificar a lista de sites permitidos:
     a. Selecione **Permitir apenas sites especificados**.
     b. Crie uma lista de sites adicionando os endereços aos quais o aplicativo não bloqueará o acesso. O Kaspersky Endpoint Security for Android é compatível somente com expressões regulares. Ao inserir o endereço de um site permitido, use os seguintes modelos:
        - `http:\/\/www\.example\.com.*`—Todas as páginas secundárias do site são permitidas (por exemplo, `http://www.example.com/about`).

- `https:\/\/.*example\.com`—Todas as páginas de subdomínio do site são permitidas (por exemplo, `https://pictures.example.com`).

c. É possível também usar a expressão `https?` para selecionar HTTP e HTTPS. Para obter mais detalhes sobre expressões regulares, consulte o site de Suporte Técnico da Oracle.

- Para bloquear o acesso do usuário a todos os sites, selecione **Bloquear todos os sites**.

5. Clique no botão **Salvar** para salvar as alterações feitas na política e sair da janela de propriedades da política.

As configurações do dispositivo móvel são definidas depois da próxima sincronização do dispositivo com o Kaspersky Security Center.

Configurar restrições de funções

É possível definir essas configurações de política apenas para dispositivos Android.

O Kaspersky Security Center Web Console permite configurar o acesso do usuário aos seguintes recursos dos dispositivos móveis:

- Wi-Fi
- Câmera
- Bluetooth

Por padrão, o usuário pode usar o Wi-Fi, a câmera e o Bluetooth no dispositivo sem restrições.

Para configurar as restrições de uso do Wi-Fi, da câmera e do Bluetooth no dispositivo:

1. Abra a janela de propriedades da política:

   - Na janela principal do Kaspersky Security Center Web Console ou Cloud Console, selecione **DISPOSITIVOS** > **POLÍTICAS E PERFIS**. Na lista de políticas de grupo aberta, clique no nome da política que deseja configurar.
   - Na janela principal do Kaspersky Security Center Web Console ou Cloud Console, selecione **DISPOSITIVOS** > **MÓVEIS** > **DISPOSITIVOS**. Clique no dispositivo móvel que se enquadra na política que desejar configurar e, em seguida, selecione a política na guia **POLÍTICAS ATIVAS E PERFIS DE POLÍTICAS.**

2. Na página de propriedades da política, selecione **CONFIGURAÇÕES DO APLICATIVO** > **Controles de segurança**.

3. Na seção **Gerenciamento de recursos**, configure o uso de Wi-Fi, da câmera e do Bluetooth:

   - Para desativar o módulo Wi-Fi no dispositivo móvel do usuário, selecione a caixa de seleção **Proibir o uso do Wi-Fi**.

     Em dispositivos Android 10.0 ou posteriores, a proibição do uso de redes Wi-Fi não é compatível.

- Para desativar a câmera no dispositivo móvel do usuário, selecione a caixa de seleção **Proibir o uso da câmera**.

  Em dispositivos Android 10.0 ou posteriores, o uso da câmera não pode ser totalmente proibido.

  Nos dispositivos que executam o Android 11 ou posterior, o Kaspersky Endpoint Security for Android deve ser definido como um recurso de Acessibilidade. O Kaspersky Endpoint Security for Android solicita que o usuário defina o aplicativo como um recurso de Acessibilidade pelo Assistente de Configuração Inicial. O usuário pode ignorar esta etapa ou desativar este serviço nas configurações de dispositivo em um momento posterior. Nesse caso, não será possível restringir o uso da câmera.

- Para desativar o Bluetooth no dispositivo móvel do usuário, marque a caixa de seleção **Proibir o uso do Bluetooth**.

  No Android 12 ou posterior, o uso do Bluetooth pode ser desabilitado somente se o usuário do dispositivo tiver concedido a permissão **Dispositivos Bluetooth por perto**. O usuário pode conceder essa permissão durante o Assistente de Configuração Inicial ou posteriormente.

4. Clique no botão **Salvar** para salvar as alterações feitas na política e sair da janela de propriedades da política.

As configurações do dispositivo móvel são definidas depois da próxima sincronização do dispositivo com o Kaspersky Security Center.

Proteger o Kaspersky Endpoint Security for Android contra a remoção

Para a proteção do dispositivo móvel e a conformidade com requisitos de segurança corporativa, é possível ativar a proteção contra a remoção do Kaspersky Endpoint Security for Android. Nesse caso, o usuário não pode remover o aplicativo por meio da interface do Kaspersky Endpoint Security for Android. Ao remover o aplicativo por meio das ferramentas do sistema operacional Android, o usuário precisa desativar os direitos de administrador para o Kaspersky Endpoint Security for Android. Após desativar os direitos, o dispositivo móvel será bloqueado.

Para ativar a proteção contra a remoção do Kaspersky Endpoint Security for Android:

1. Abra a janela de propriedades da política:

   - Na janela principal do Kaspersky Security Center Web Console ou Cloud Console, selecione **DISPOSITIVOS** > **POLÍTICAS E PERFIS**. Na lista de políticas de grupo aberta, clique no nome da política que deseja configurar.

   - Na janela principal do Kaspersky Security Center Web Console ou Cloud Console, selecione **DISPOSITIVOS** > **MÓVEIS** > **DISPOSITIVOS**. Clique no dispositivo móvel que se enquadra na política que desejar configurar e, em seguida, selecione a política na guia **POLÍTICAS ATIVAS E PERFIS DE POLÍTICAS.**

2. Na página de propriedades da política, selecione **CONFIGURAÇÕES DO APLICATIVO** > **Controles de segurança**.

3. Na seção **Gerenciar aplicativo no dispositivo móvel**, desmarque a caixa de seleção **Permitir a remoção do Kaspersky Endpoint Security for Android**

Para proteger o aplicativo da remoção em dispositivos que executam o Android 7.0 ou posterior, o Kaspersky Endpoint Security for Android deve ser definido como um recurso de Acessibilidade. Quando o assistente Configuração inicial estiver sendo executado, o Kaspersky Endpoint Security for Android solicita ao usuário conceder ao aplicativo todas as permissões necessárias. O usuário pode ignorar estas etapas ou desativar estas permissões nas configurações de dispositivo em um momento posterior. Se este for o caso, o aplicativo não é protegido contra a remoção.

4. Clique no botão **Salvar** para salvar as alterações feitas na política e sair da janela de propriedades da política.

As configurações do dispositivo móvel são definidas depois da próxima sincronização do dispositivo com o Kaspersky Security Center.

Se uma tentativa for feita para remover o aplicativo, o dispositivo móvel será bloqueado.

Configurar a sincronização de dispositivos móveis com o Kaspersky Security Center

É possível definir essas configurações de política para dispositivos Android e iOS.

Para gerenciar dispositivos móveis e receber relatórios ou estatísticas de dispositivos móveis, é necessário definir as configurações de sincronização. A sincronização de dispositivos móveis com o Kaspersky Security Center pode ser executada nas seguintes formas:

- **Por agendamento**. A sincronização de acordo com o agendamento é executada usando-se o HTTP. É possível configurar o agendamento da sincronização nas propriedades da política. As modificações nas configurações, nos comandos e nas tarefas da política são executadas quando os dispositivos móveis são sincronizados com o Kaspersky Security Center de acordo com o agendamento, ou seja, com um atraso. Por padrão, os dispositivos móveis são sincronizados com o Kaspersky Security Center automaticamente a cada 6 horas.

  No Android 12 ou posterior, o aplicativo pode realizar essa tarefa após o especificado se o dispositivo estiver no modo de economia de bateria.

- **Forçada** (para dispositivos Android). A sincronização forçada é executada por meio de notificações push do serviço FCM (Firebase Cloud Messaging). A sincronização forçada é principalmente destinada para a entrega oportuna de comandos à um dispositivo móvel. Caso queira usar a sincronização forçada, certifique-se de que as definições de FCM estejam configuradas no Kaspersky Security Center.

Para configurar a sincronização do dispositivo móvel com o Kaspersky Security Center:

1. Abra a janela de propriedades da política:

   - Na janela principal do Kaspersky Security Center Web Console ou Cloud Console, selecione **DISPOSITIVOS** > **POLÍTICAS E PERFIS**. Na lista de políticas de grupo aberta, clique no nome da política que deseja configurar.

   - Na janela principal do Kaspersky Security Center Web Console ou Cloud Console, selecione **DISPOSITIVOS** > **MÓVEIS** > **DISPOSITIVOS**. Clique no dispositivo móvel que se enquadra na política que desejar configurar e, em seguida, selecione a política na guia **POLÍTICAS ATIVAS E PERFIS DE POLÍTICAS.**

2. Na página de propriedades da política, selecione **CONFIGURAÇÕES DO APLICATIVO** > **Sincronização**.

3. Na seção **Sincronização com o Servidor de Administração**, use a lista suspensa **Período de sincronização** para selecionar o período de sincronização.

   Por padrão, a sincronização é realizada a cada 6 horas.

4. Para dispositivos Android, é possível desativar a sincronização quando o dispositivo está em roaming. Para isso, marque a caixa de seleção **Não sincronizar quando em roaming**.

   Por padrão, a sincronização durante o roaming está ativada.

5. Clique no botão **Salvar** para salvar as alterações feitas na política e sair da janela de propriedades da política.

As configurações do dispositivo móvel são definidas depois da próxima sincronização do dispositivo com o Kaspersky Security Center.

Kaspersky Security Network

Para proteger os dispositivos móveis com mais eficiência, o Kaspersky Endpoint Security for Android e o Kaspersky Security for iOS usam dados adquiridos de usuários em todo o mundo. *A Kaspersky Security Network* é projetada para processar tais dados.

Kaspersky Security Network (KSN) é uma infraestrutura de serviços na nuvem que fornece o acesso à base de dados de conhecimento on-line da Kaspersky, contendo informações sobre a reputação de arquivos, recursos da Web e softwares. A utilização dos dados da Kaspersky Security Network garante respostas mais rápidas dos aplicativos da Kaspersky a novas ameaças, aprimora o desempenho de alguns componentes de proteção e reduz a possibilidade de falsos positivos.

Sua participação na Kaspersky Security Network ajuda a Kaspersky a adquirir informações em tempo real sobre os tipos e fontes de novas ameaças, desenvolver métodos para neutralizá-las e reduzir o número de alarmes falsos. A participação na Kaspersky Security Network também permite acessar estatísticas de reputação para aplicativos e sites.

Quando você participa da Kaspersky Security Network, algumas estatísticas são adquiridas enquanto o aplicativo móvel está em execução e são enviadas automaticamente para a Kaspersky. Estas informações permitem manter o acompanhamento das ameaças em tempo real. Os arquivos ou partes deles que podem ser explorados por invasores para danificar o computador ou o conteúdo do usuário também podem ser enviados à Kaspersky para exame complementar.

Os seguintes componentes do aplicativo usam o serviço de nuvem da Kaspersky Security Network:

- Os componentes Antivírus, Proteção na Web e Controle de aplicativos no aplicativo Kaspersky Endpoint Security for Android.
- O componente Proteção na Web no aplicativo Kaspersky Security for iOS.

Para começar a usar a KSN, você deve aceitar os termos e condições do Contrato de Licença do Usuário Final. Para obter mais informações sobre o envio de dados para a KSN, consulte Troca de informações com a Kaspersky Security Network.

A recusa em participar da KSN reduz o nível da proteção de dispositivo, que pode levar a infecção do dispositivo e perda dos dados.

Para aprimorar o desempenho do aplicativo móvel, também é possível fornecer dados estatísticos à Kaspersky Security Network.

O fornecimento de informações à Kaspersky Security Network é voluntário.

Troca de informações com a Kaspersky Security Network

Troca de informações no Kaspersky Endpoint Security for Android

Para aprimorar a proteção em tempo real, o Kaspersky Endpoint Security for Android usa o serviço na nuvem da Kaspersky Security Network para a operação dos seguintes componentes:

- **Antivírus.** O aplicativo obtém o acesso à Base de Conhecimento on-line da Kaspersky quanto à reputação de arquivos e aplicativos. A verificação é executada para as ameaças cujas informações ainda não foram adicionadas ao banco de dados antivírus, mas já estão disponíveis na KSN. O serviço na nuvem da Kaspersky Security Network fornece a operação completa do antivírus e reduz a probabilidade de falsos alarmes.

- **Proteção na Web.** O aplicativo usa os dados recebidos da KSN para executar uma verificação de sites antes que eles sejam abertos. O aplicativo também determina a categoria de site que controla o acesso à Internet para os usuários de acordo com as listas de categorias permitidas e bloqueadas (por exemplo, a categoria "Comunicações via Internet").

- **Controle de aplicativos.** O aplicativo determina a categoria de aplicativo que restringe a inicialização de aplicativos que não atendam os requisitos de segurança corporativa de acordo com as listas de categorias permitidas e bloqueadas (por exemplo, a categoria "Jogos").

As informações sobre o tipo de dados enviados à Kaspersky ao usar a KSN durante a operação do antivírus e controle de aplicativos estão disponíveis no Contrato de Licença do Usuário Final. Ao aceitar os termos e condições do Contrato de Licença, o usuário concorda em transferir as seguintes informações.

As informações sobre o tipo de dados enviados à Kaspersky, ao usar a KSN durante a operação da proteção na web, estão disponíveis na Declaração sobre o processamento de dados para a proteção na web. Ao aceitar os termos e condições da Declaração, o usuário concorda em transferir as seguintes informações.

Para obter mais informações sobre a coleta de dados para a KSN, consulte Fornecimento de dados no Kaspersky Endpoint Security for Android.

A provisão de dados para a KSN é voluntária. Caso queira, é possível desativar a troca de dados com a KSN.

Troca de informações no Kaspersky Security for iOS

Para melhorar a proteção em tempo real, o Kaspersky Security for iOS usa o serviço de nuvem da Kaspersky Security Network para operar o componente **Proteção na Web**. O aplicativo usa os dados recebidos da KSN para verificar os recursos da Web antes de serem abertos.

As informações sobre o tipo de dados enviados à Kaspersky ao usar a KSN durante a operação da Proteção na Web estão disponíveis no Contrato de Licença do Usuário Final. Ao aceitar os termos e condições do Contrato de Licença, o usuário concorda em transferir as seguintes informações.

Para obter mais informações sobre a coleta de dados para a KSN, consulte Fornecimento de dados no Kaspersky Security for iOS.

A provisão de dados para a KSN é voluntária. Caso queira, é possível desativar a troca de dados com a KSN.

Envio de estatísticas para a KSN de aplicativos Android e iOS

Para trocar dados com a KSN com os propósitos de aprimora o desempenho do aplicativo, as seguintes condições devem ser cumpridas:

- O usuário do dispositivo deve ler e aceitar os termos da Declaração da Kaspersky Security Network.
- É preciso definir as configurações de política de grupo para permitir que as estatísticas sejam enviadas à KSN.

Você pode optar por não enviar dados estatísticos par a Kaspersky Security Network a qualquer momento. As informações sobre o tipo de dados estatísticos enviados à Kaspersky ao usar a KSN durante a operação do aplicativo móvel estão disponíveis na Declaração da Kaspersky Security Network.

Ativar e desativar a Kaspersky Security Network

Por padrão, o uso da Kaspersky Security Network está ativado.

Se o uso do Kaspersky Security Network estiver desabilitado, a Proteção na Web, o Controle de aplicativos e a proteção adicional na Kaspersky Security Network serão desabilitados automaticamente e suas configurações ficarão indisponíveis.

Para ativar ou desativar o uso da Kaspersky Security Network:

1. Abra a janela de propriedades da política:
   - Na janela principal do Kaspersky Security Center Web Console ou Cloud Console, selecione **DISPOSITIVOS** > **POLÍTICAS E PERFIS**. Na lista de políticas de grupo aberta, clique no nome da política que deseja configurar.
   - Na janela principal do Kaspersky Security Center Web Console ou Cloud Console, selecione **DISPOSITIVOS** > **MÓVEIS** > **DISPOSITIVOS**. Clique no dispositivo móvel que se enquadra na política que desejar configurar e, em seguida, selecione a política na guia **POLÍTICAS ATIVAS E PERFIS DE POLÍTICAS.**
2. Na página de propriedades da política, selecione **CONFIGURAÇÕES DO APLICATIVO** > **KSN e estatísticas**.
3. Para ativar ou desativar o uso da Kaspersky Security Network, marque ou desmarque a caixa de seleção **Usar a Kaspersky Security Network**.
4. Se o uso da Kaspersky Security Network estiver ativado e concordar em enviar dados à Kaspersky, marque a caixa de seleção **Permitir que as estatísticas sejam enviadas para a Kaspersky Security Network**. Esses dados ajudarão o aplicativo móvel a responder mais rapidamente às ameaças, melhorar o desempenho dos componentes de proteção e diminuir a probabilidade de alarmes falsos.
5. Clique no botão **Salvar** para salvar as alterações feitas na política e sair da janela de propriedades da política.

As configurações do dispositivo móvel são definidas depois da próxima sincronização do dispositivo com o Kaspersky Security Center.

Trocar informações com o Google Analytics for Firebase, SafetyNet Attestation, Firebase Performance Monitoring e Crashlytics

É possível definir essas configurações de política apenas para dispositivos Android.

O Kaspersky Endpoint Security for Android troca dados com os serviços Google Analytics for Firebase, SafetyNet Attestation, Firebase Performance Monitoring e Crashlytics para melhorar a qualidade, a aparência e o desempenho do software, produtos, serviços e infraestrutura da Kaspersky analisando a experiência dos usuários, recursos, status e configurações utilizadas no dispositivo.

A troca de informações com os serviços Google Analytics for Firebase, SafetyNet Attestation, Firebase Performance Monitoring e Crashlytics está desativada por padrão.

Para ativar a troca de dados:

1. Abra a janela de propriedades da política:

   - Na janela principal do Kaspersky Security Center Web Console ou Cloud Console, selecione **DISPOSITIVOS** > **POLÍTICAS E PERFIS**. Na lista de políticas de grupo aberta, clique no nome da política que deseja configurar.

   - Na janela principal do Kaspersky Security Center Web Console ou Cloud Console, selecione **DISPOSITIVOS** > **MÓVEIS** > **DISPOSITIVOS**. Clique no dispositivo móvel que se enquadra na política que desejar configurar e, em seguida, selecione a política na guia **POLÍTICAS ATIVAS E PERFIS DE POLÍTICAS.**

2. Na página de propriedades da política, selecione **CONFIGURAÇÕES DO APLICATIVO** > **KSN e estatísticas**.

3. Na seção **Envio de estatísticas**, marque a caixa de seleção **Permitir a transferência de dados para ajudar a aprimorar a qualidade, a aparência e o desempenho do aplicativo**.

4. Clique no botão **Salvar** para salvar as alterações feitas na política e sair da janela de propriedades da política.

As configurações do dispositivo móvel são definidas depois da próxima sincronização do dispositivo com o Kaspersky Security Center.

Configurar notificações em dispositivos móveis

É possível definir essas configurações de política apenas para dispositivos Android.

Caso não queira que o usuário do dispositivo móvel receba notificações do Kaspersky Endpoint Security for Android, é possível desativar certas notificações.

Kaspersky Endpoint Security usa as seguintes ferramentas para exibir o status da proteção do dispositivo:

- **Notificação de status da proteção**. Esta notificação é afixada à barra de notificação. Uma notificação de status da proteção não pode ser removida. A notificação exibe o status da proteção do dispositivo (por exemplo,) e o número de problemas, se houver. O usuário do dispositivo pode tocar no status da proteção do dispositivo e ver a lista de problemas no aplicativo.

- **Notificações do aplicativo**. Estas notificações informam o usuário do dispositivo sobre o aplicativo (por exemplo, detecção de ameaças).

- **Mensagens pop-up**. As mensagens pop-up requerem determinada ação do usuário do dispositivo (por exemplo, a ação a ser executada quando detectada uma ameaça).

Todas as notificações do Kaspersky Endpoint Security for Android são ativadas por padrão.

Um usuário de dispositivo Android pode desativar todas as notificações do Kaspersky Endpoint Security for Android nas configurações na barra de notificação. Se as notificações forem desativadas, o usuário não monitora a operação do aplicativo e pode ignorar informações importantes (por exemplo, informações sobre falhas durante a sincronização do dispositivo com o Kaspersky Security Center). Neste caso, para conhecer o status da operação do aplicativo, o usuário deve abrir o Kaspersky Endpoint Security for Android.

Para configurar a exibição de notificações sobre a operação do Kaspersky Endpoint Security for Android em um dispositivo móvel:

1. Abra a janela de propriedades da política:

   - Na janela principal do Kaspersky Security Center Web Console ou Cloud Console, selecione **DISPOSITIVOS** > **POLÍTICAS E PERFIS**. Na lista de políticas de grupo aberta, clique no nome da política que deseja configurar.

   - Na janela principal do Kaspersky Security Center Web Console ou Cloud Console, selecione **DISPOSITIVOS** > **MÓVEIS** > **DISPOSITIVOS**. Clique no dispositivo móvel que se enquadra na política que desejar configurar e, em seguida, selecione a política na guia **POLÍTICAS ATIVAS E PERFIS DE POLÍTICAS.**

2. Na página de propriedades da política, selecione **CONFIGURAÇÕES DO APLICATIVO** > **Notificações e relatórios**.

3. Na seção **Notificações**, configure a exibição de notificações:

   - Para ocultar todas as notificações e mensagens pop-up, desative o botão de seleção **Exibir notificações quando o Kaspersky Endpoint Security estiver em segundo plano**.

     O Kaspersky Endpoint Security for Android exibirá apenas a notificação de status da proteção. A notificação exibe o status da proteção do dispositivo (por exemplo,) e o número de problemas. O aplicativo também exibe notificações quando o usuário está trabalhando com o aplicativo (por exemplo, o usuário atualiza os bancos de dados antivírus manualmente).

     Os especialistas da Kaspersky recomendam ativar notificações e mensagens pop-up. Se você desativar as notificações e mensagens pop-up quando o aplicativo estiver em segundo plano, o aplicativo não alertará os usuários sobre ameaças em tempo real. Usuários de dispositivos móveis podem saber o status da proteção do dispositivo apenas ao abrirem o aplicativo.

   - Em **Lista de problemas de segurança exibidos nos dispositivos dos usuários** selecione os problemas do Kaspersky Endpoint Security for Android que devem ser exibidos no dispositivo móvel do usuário.

4. Clique no botão **Salvar** para salvar as alterações feitas na política e sair da janela de propriedades da política.

As configurações do dispositivo móvel são definidas depois da próxima sincronização do dispositivo com o Kaspersky Security Center.

Detectar invasões do dispositivo

O Kaspersky Security Center Web Console permite detectar hacks de dispositivos (root) em dispositivos Android e jailbreaks em dispositivos iOS. Os arquivos do sistema ficam desprotegidos em dispositivos hackeados, podendo, portanto, ser modificados. Além disso, aplicativos de terceiros de origens desconhecidas podem ser instalados em dispositivos hackeados. Após a detecção de uma tentativa de invasão, recomendamos restaurar imediatamente a operação normal do dispositivo.

O Kaspersky Endpoint Security for Android usa os seguintes serviços para detectar quando um usuário obtém privilégios de root:

- *Serviço incorporado do Kaspersky Endpoint Security for Android.* Um serviço Kaspersky que verifica se o usuário de dispositivo móvel obteve privilégios root (Kaspersky Mobile Security SDK).

- *SafetyNet Attestation.* Um serviço Google que verifica a integridade do sistema operacional, analisa o hardware e o software do dispositivo e identifica outros problemas de segurança. Para obter mais detalhes sobre o SafetyNet Attestation, visite o site de Suporte Técnico do Android.

O Kaspersky Security for iOS usa o seguinte serviço para detectar um jailbreak:

- *Serviço incorporado do Kaspersky Security for iOS* Um serviço da Kaspersky que verifica se o dispositivo está bloqueado por jailbreak (Kaspersky Mobile Security SDK).

Em caso de invasão do dispositivo, uma notificação será enviada ao usuário. É possível ver as notificações de invasão no Kaspersky Security Center Web Console na guia **MONITORAMENTO E RELATÓRIO** > **PAINEL**. É possível também desativar as notificações sobre invasões nas configurações de notificação de evento.

Em dispositivos Android, é possível impor restrições à atividade do usuário em caso de invasão do dispositivo (por exemplo, bloquear o dispositivo). É possível impor restrições por meio do componente Controle de conformidade. Para isso, crie uma regra de conformidade com o critério **O dispositivo foi roteado**.

Definição de configurações de licenciamento

É possível definir essas configurações de política para dispositivos Android e iOS.

Para gerenciar dispositivos móveis no Kaspersky Security Center Web Console ou Cloud Console, você deve ativar o aplicativo móvel nos dispositivos móveis. A ativação do aplicativo Kaspersky Endpoint Security for Android ou do aplicativo Kaspersky Security for iOS em um dispositivo móvel é feita fornecendo informações de licença válidas ao aplicativo. As informações da licença são entregues ao dispositivo móvel, junto com a política, quando o dispositivo é sincronizado com o Kaspersky Security Center.

Caso a ativação do aplicativo móvel não seja concluída em 30 dias a partir do momento da instalação no dispositivo móvel, o aplicativo será automaticamente alterado para o modo de funcionalidade limitada. Nesse modo, a maioria dos componentes do aplicativo são desativados. Ao mudar para o modo de funcionalidade limitada, o aplicativo para de executar a sincronização automática com o Kaspersky Security Center. Portanto, se a ativação do aplicativo não tiver sido concluída em 30 dias após a instalação, o usuário deverá sincronizar manualmente o dispositivo com o Kaspersky Security Center.

Para definir as configurações de licenciamento de uma política de grupo:

1. Abra a janela de propriedades da política:

   - Na janela principal do Kaspersky Security Center Web Console ou Cloud Console, selecione **DISPOSITIVOS** > **POLÍTICAS E PERFIS**. Na lista de políticas de grupo aberta, clique no nome da política que deseja configurar.

- Na janela principal do Kaspersky Security Center Web Console ou Cloud Console, selecione **DISPOSITIVOS** > **MÓVEIS** > **DISPOSITIVOS**. Clique no dispositivo móvel que se enquadra na política que desejar configurar e, em seguida, selecione a política na guia **POLÍTICAS ATIVAS E PERFIS DE POLÍTICAS.**

2. Na página de propriedades da política, selecione **CONFIGURAÇÕES DO APLICATIVO** > **Licenças**.

3. Use a lista suspensa para selecionar a chave de licença necessária do armazenamento de chaves do Servidor de Administração.

   Os detalhes da chave de licença são exibidos nos campos abaixo.

   > É possível substituir a chave de ativação existente no dispositivo móvel se ela for diferente da selecionada na lista suspensa acima. Para fazer isso, marque a caixa de seleção **Se a chave no dispositivo for diferente, substitua por esta chave** caixa de seleção.

4. Clique no botão **Salvar** para salvar as alterações feitas na política e sair da janela de propriedades da política.

   As configurações do dispositivo móvel são definidas depois da próxima sincronização do dispositivo com o Kaspersky Security Center.

Configuração de eventos

> É possível definir essas configurações de política para dispositivos Android e iOS.

É possível definir as configurações de armazenamento e notificação de eventos dos dispositivos de seus usuários que são enviados ao Kaspersky Security Center.

> É possível configurar eventos apenas ao modificar uma política.

Os eventos são distribuídos por nível de importância nas seguintes guias:

- **Crítico**

  Um evento crítico indica um problema que pode levar à perda de dados, a um mau funcionamento operacional ou a um erro crítico.

- **Falha funcional**

  Uma falha funcional indica um problema sério, erro ou mau funcionamento que ocorreu durante a operação do aplicativo.

- **Aviso**

  Um aviso não é necessariamente grave, mas indica um potencial problema futuro.

- **Informações**

  Um evento informativo notifica sobre a conclusão bem-sucedida de uma operação ou procedimento, ou sobre o funcionamento adequado do aplicativo.

Em cada seção, a lista mostra os tipos de eventos e o prazo de armazenamento de eventos padrão no Kaspersky Security Center (em dias).

Na lista de eventos, é possível fazer o seguinte:

- Adicione ou remova um tipo de evento da lista de tipos de eventos enviados ao Kaspersky Security Center.
- Defina as configurações de armazenamento e notificação para cada tipo de evento, por exemplo: por quanto tempo eventos desse tipo devem ser armazenados no banco de dados do Servidor de Administração ou se você será notificado por e-mail sobre eventos desse tipo.

Para obter mais detalhes sobre a configuração de eventos no Kaspersky Security Center Web Console e Cloud Console:

- Caso use o Kaspersky Security Center Web Console, consulte a *Ajuda do Kaspersky Security Center*.
- Caso use o Kaspersky Security Center Cloud Console, consulte a *Ajuda do Kaspersky Security Center Cloud Console*.

Configuração de eventos de instalação, atualização e remoção de aplicativos nos dispositivos dos usuários

É possível definir essas configurações de política para dispositivos Android e iOS.

Caso o Kaspersky Security Center Cloud Console seja usado, a lista de tipos de eventos que ocorrem nos dispositivos dos seus usuários e que são enviados para o Kaspersky Security Center não incluem a instalação, atualização e remoção de aplicativos nos dispositivos. Isso acontece porque os eventos ocorrem com muita frequência e podem substituir outros eventos importantes no banco de dados do Kaspersky Security Center quando o limite de contagem de eventos é atingido. Eles também podem afetar o desempenho do Servidor de administração ou do DBMS e a largura da banda da conexão com a Internet com o Kaspersky Security Center Cloud Console.

Se, no entanto, você desejar armazenar eventos deste tipo e ser notificado sobre eles, proceda conforme descrito nesta seção.

Para configurar os eventos de instalação, a atualização e a remoção de aplicativos nos dispositivos dos usuários:

1. Nas configurações de uma política, na guia **CONFIGURAÇÃO DO EVENTO**, adicione o tipo de evento informativo **Um aplicativo foi instalado ou removido (Lista de aplicativos instalados)** à lista de eventos armazenados no banco de dados do Servidor de Administração.

   Para obter mais detalhes sobre a configuração de eventos, consulte a *Ajuda do Kaspersky Security Center Cloud Console*.

2. Ative a opção **Enviar uma lista de aplicativos instalados em todos os dispositivos móveis**.

Os eventos de instalação, atualização e remoção de aplicativos nos dispositivos dos usuários são armazenados no banco de dados do Kaspersky Security Center. Você é notificado sobre esses eventos.

Carga da rede

Esta seção contém informações sobre o volume do tráfego de rede que é trocado entre dispositivos móveis e o Kaspersky Security Center.

Volume de tráfego

Tarefa	Tráfego de saída	Tráfego de entrada	Tráfego total
Implementação inicial do aplicativo, MB	0,08	17,76	17,84
A atualização inicial dos bancos de dados antivírus (o volume de tráfego pode ser diferente devido ao tamanho dos bancos de dados antivírus), MB	0,04	2,21	2,25
Sincronização do dispositivo móvel com o Kaspersky Security Center, MB	0,03	0,02	0,05
A atualização regular dos bancos de dados antivírus (o volume de tráfego pode ser diferente devido ao tamanho dos bancos de dados antivírus), MB	0,08	3,06	3,14
Execução de comandos Antirroubo Localizar o dispositivo (o volume de tráfego pode ser diferente devido às especificações da câmera incorporada e a qualidade das imagens), MB	0,09	0,8	0,17
Execução de comandos Antirroubo Retrato, MB	1,0	0,02	1,02
Execução de comandos Antirroubo Bloqueio do dispositivo, MB	0,06	0,05	0,11
Volume diário médio, MB	0,22	6,96	7,18

Trabalhando no console de administração baseado em MMC

Esta seção de ajuda descreve a proteção e o gerenciamento de dispositivos móveis usando o console de administração baseado no MMC do Kaspersky Security Center.

Principais casos de uso

INSTALAÇÃO

Como instalar o Kaspersky Endpoint Security for Android remotamente?

Como bloquear um usuário para que não remova o Kaspersky Endpoint Security for Android?

Como ativar o Kaspersky Endpoint Security for Android?

PROTEÇÃO

Como bloquear um dispositivo que foi perdido ou roubado?

Como me proteger contra ameaças na Internet?

Como proibir o uso de uma senha vazia?

UTILIZAÇÃO DE SOLUÇÕES DE TERCEIROS

Android Enterprise (Aplicativos com o ícone de maleta, Configurar o perfil de trabalho do Android)

VMware AirWatch, MobileIron, IBM Maas360, SOTI MobiControl

CONTROLE

Como bloquear um usuário de jogar jogos em um dispositivo?

Como configurar o acesso a sites em um dispositivo?

Como detectar a raiz?

GERENCIAMENTO

Como configurar uma caixa de correio em um dispositivo?

Como conectar um dispositivo móvel à rede Wi-Fi?

Como instalar um aplicativo corporativo?

Sobre o Kaspersky Security for Mobile

O *Kaspersky Security for Mobile* é uma solução integrada para proteção e gerenciamento de dispositivos móveis corporativos assim como dispositivos móveis pessoais usados por funcionários de empresas para finalidades corporativas.

O Kaspersky Security for Mobile inclui os seguintes componentes:

- Aplicativo móvel Kaspersky Endpoint Security for Android

  O aplicativo Kaspersky Endpoint Security for Android garante a proteção de dispositivos móveis contra ameaças da web, vírus e outros programas que representam ameaças.

- Plug-in de administração do Kaspersky Endpoint Security for Android

O Plug-in de administração do Kaspersky Endpoint Security for Android oferece a interface para gerenciar dispositivos móveis e aplicativos móveis instalados neles através do Console de administração do Kaspersky Security Center.

- Plug-in de Administração para o Kaspersky Device Management for iOS

  O Plug-in de Administração do Kaspersky Device Management for iOS permite que você defina as configurações de dispositivos conectados ao Kaspersky Security Center através do protocolo iOS MDM (aqui referido como "dispositivos iOS MDM") e o protocolo Exchange ActiveSync (aqui referido como "dispositivos EAS"), sem usar o iPhone Configuration Utility ou o Console de gerenciamento do Exchange.

Os Plug-ins de Administração são integrados no sistema de administração remota do *Kaspersky Security Center*. O administrador pode usar um único Console de Administração do Kaspersky Security Center para gerenciar qualquer dispositivo móvel na rede corporativa bem como computadores cliente e sistemas virtuais. Após você conectar dispositivos móveis ao Servidor de Administração, eles ficam a ser gerenciados. O administrador pode monitorar remotamente dispositivos gerenciados.

O aplicativo móvel do Kaspersky Endpoint Security for Android também pode operar como parte do *sistema de administração remota do Kaspersky Endpoint Security Cloud*. Para obter mais detalhes sobre o trabalho com aplicativos via Kaspersky Endpoint Security Cloud, consulte a *Ajuda on-line do Kaspersky Endpoint Security Cloud*.

O aplicativo móvel Kaspersky Endpoint Security for Android também pode operar como parte das soluções EMM de terceiros dos participantes da Comunidade do AppConfig.

Principais recursos de gerenciamento de dispositivos móveis no Console de Administração baseado em MMC

O Kaspersky Security for Mobile oferece os seguintes recursos:

- Distribuição de mensagens de e-mail para conectar os dispositivos Android ao Kaspersky Security Center usando links do Google Play.
- Conexão remota de dispositivos móveis com o Kaspersky Security Center e sistemas EMM de terceiros (por exemplo, VMWare AirWatch, MobileIron, IBM Maas360, SOTI MobiControl).
- Configuração remota do aplicativo Kaspersky Endpoint Security for Android, assim como configuração remota de serviços, aplicativos e funções de dispositivos Android.
- Configuração remota de dispositivos móveis de acordo com os requisitos de segurança corporativa.
- Prevenção de vazamento de informações corporativas armazenadas em dispositivos móveis, no caso de perda ou roubo (Antirroubo).
- Controle de conformidade com requisitos de segurança corporativa (Controle de Conformidade).
- Controle do uso da Internet em dispositivos móveis (Proteção na Web).
- Configuração do e-mail corporativo em dispositivos móveis, incluindo as organizações com um servidor de e-mail do Microsoft Exchange implementado na empresa (apenas para dispositivos iOS e Samsung).
- Configuração da rede corporativa (Wi-Fi, VPN), permitindo que a VPN seja utilizada em dispositivos móveis. A VPN pode ser configurada unicamente em dispositivos iOS e Samsung.

- Configuração da exibição do status do dispositivo móvel no Kaspersky Security Center quando as regras de política são violadas: Crítico, Aviso ou OK.
- Configuração de notificações exibidas ao usuário no aplicativo Kaspersky Endpoint Security for Android.
- A definição das configurações em dispositivos com suporte para Samsung KNOX 2.6 ou posterior.
- Definição das configurações em dispositivos compatíveis com perfis de trabalho do Android.
- Implementação do Kaspersky Endpoint Security for Android por meio do console do Samsung KNOX Mobile Enrollment. O Samsung KNOX Mobile Enrollment é para a instalação em lote e a configuração inicial dos aplicativos nos dispositivos Samsung comprados de fornecedores oficiais.
- Um upgrade do Kaspersky Endpoint Security for Android para a versão especificada pode ser executada usando as políticas do Kaspersky Security Center.
- As notificações do administrador sobre o status e os eventos do aplicativo Kaspersky Endpoint Security for Android podem ser comunicadas no Kaspersky Security Center ou por e-mail.
- Controle de alterações das configurações da política (histórico de revisão).

O Kaspersky Security for Mobile inclui os seguintes componentes de proteção e gerenciamento:

- Antivírus (para dispositivos Android)
- Antirroubo (para dispositivos Android)
- Proteção na Web (para dispositivos Android e iOS)
- Controle de aplicativos (para dispositivos Android)
- Controle de conformidade (para dispositivos Android)
- Detecção de privilégios raiz em dispositivos (para dispositivos Android)

Sobre o aplicativo Kaspersky Endpoint Security for Android

O aplicativo Kaspersky Endpoint Security for Android garante a proteção de dispositivos móveis contra ameaças da web, vírus e outros programas que representam ameaças.

O aplicativo Kaspersky Endpoint Security for Android inclui os seguintes componentes:

- **Antivírus**. Permite detectar e neutralizar ameaças em seu dispositivo utilizando os bancos de dados antivírus do aplicativo e o serviço da Kaspersky Security Network na nuvem. O Antivírus inclui os seguintes componentes:
  - Proteção. Detecta ameaças em arquivos abertos, verifica novos aplicativos e previne a infecção do dispositivo em tempo real.
  - Verificação. Ela é iniciada sob demanda para todo o sistema de arquivos, somente para aplicativos instalados ou um arquivo ou pasta selecionado.
  - Atualização. A Atualização permite o download de novos bancos de dados antivírus para o aplicativo.

- **Antirroubo.** Este componente protege informações no dispositivo contra acesso não autorizado, em caso de perda ou roubo do dispositivo. Esse componente permite enviar os seguintes comandos ao dispositivo:
  - **Localizar** para obter as coordenadas da localização do dispositivo.
  - **Alarme** para acionar o disparo de um alarme sonoro.
  - **Retrato** para fazer o dispositivo tirar fotos com a câmera frontal se alguém tentar desbloqueá-lo.
  - **Limpar** os dados corporativos para proteger a confidencialidade das informações empresariais.
- **Proteção na Web.** Este componente bloqueia sites maliciosos criados para espalhar código malicioso. A Proteção na Web também bloqueia sites falsos (phishing) criados para roubar dados confidenciais do usuário (por exemplo, senhas de serviços bancários on-line ou sistemas de transferência de dinheiro) e acessar as informações financeiras do usuário. A Proteção na Web verifica os sites antes de abri-los utilizando o serviço Kaspersky Security Network na nuvem. Após a verificação, a Proteção na Web permite que os sites confiáveis sejam carregados e bloqueia sites maliciosos. A Proteção na Web também é compatível com a filtragem de sites por categorias definidas no serviço na nuvem da Kaspersky Security Network. Isso permite ao administrador restringir o acesso do usuário a determinadas categorias de páginas da Web (por exemplo, páginas da Web das categorias de "Jogos de azar, loterias, apostas" ou "Comunicações via Internet").
- **Controle de aplicativos.** Esse componente permite instalar os aplicativos recomendados e requeridos no seu dispositivo por meio de um link direto para o pacote de distribuição ou um link para o Google Play. O Controle de Aplicativos permite remover os aplicativos bloqueados que violam os requisitos da segurança corporativa.
- **Controle de conformidade.** Esse componente permite verificar a conformidade dos dispositivos gerenciados com os requisitos de segurança corporativa e impor restrições a certas funções de dispositivos não compatíveis.

Sobre o Kaspersky Device Management for iOS

O Kaspersky Device Management for iOS garante a proteção e o controle de dispositivos móveis que estão conectados ao Kaspersky Security Center e fornece recursos de gerenciamento de dispositivo, como:

- **Proteção por senha**. Esse recurso permite a definição de requisitos de complexidade de senha para que os usuários utilizem senhas complexas em conformidade com a política de senhas corporativas.
- **Gerenciamento de rede**. Esse recurso permite adicionar redes VPN e Wi-Fi aprovadas ou restringir o acesso a outras.
- **Limpar os dados corporativos**. Caso o dispositivo seja perdido ou roubado, é possível enviar o comando Wipe para proteger informações sensíveis da empresa.
- **Proteção na Web**. Este componente bloqueia sites maliciosos criados para espalhar código malicioso. A Proteção na Web também bloqueia sites falsos (phishing) criados para roubar dados confidenciais do usuário (por exemplo, senhas de serviços bancários on-line ou sistemas de transferência de dinheiro) e acessar as informações financeiras do usuário. A Proteção na Web verifica os sites antes de abri-los utilizando o serviço Kaspersky Security Network na nuvem. Após a verificação, a Proteção na Web permite que os sites confiáveis sejam carregados e bloqueia sites maliciosos. A Proteção na Web também é compatível com a filtragem de sites por categorias definidas no serviço na nuvem da Kaspersky Security Network. Isso permite ao administrador restringir o acesso do usuário a determinadas categorias de páginas da Web (por exemplo, páginas da Web das categorias de "Jogos de azar, loterias, apostas" ou "Comunicações via Internet").
- **Restrições de aplicativo.** Esse componente permite controlar se os aplicativos locais, tais como iTunes, Safari ou Game Center podem ser usados em um dispositivo supervisionado.

- **Restrições de funções.** Esse componente permite verificar a conformidade dos dispositivos gerenciados com os requisitos de segurança corporativa e impor restrições a certas funções de dispositivos não compatíveis.

Sobre uma caixa de correio do Exchange

Uma *caixa de correio Exchange* é um aplicativo cliente do serviço Exchange ActiveSync. O aplicativo foi concebido para ajudar usuários corporativos a trabalhar com e-mail, calendário, contatos e tarefas. Uma caixa de correio Exchange permite que você conecte um dispositivo móvel a um servidor Microsoft Exchange. Para obter mais detalhes sobre o serviço Exchange ActiveSync, visite o *site de Suporte Técnico da Microsoft*.

Para gerenciar dispositivos móveis usando o protocolo Exchange ActiveSync, o Servidor do Exchange deve ser implementado no servidor Microsoft Exchange. Para mais detalhes sobre a instalação de um Servidor do Exchange, consulte a *Ajuda Kaspersky Security Center*. Nenhuma configuração adicional é necessária nos dispositivos móveis.

Usando uma caixa de correio do Exchange, é possível configurar remotamente dispositivos EAS usando políticas de grupo e enviar o comando de limpeza de dados. Os seguintes sistemas operacionais suportam o protocolo Exchange ActiveSync:

- Windows Mobile
- Windows CE
- Windows Phone
- Android
- Bada
- BlackBerry 10
- iOS
- Symbian

O conjunto de configurações de gerenciamento para um dispositivo Exchange ActiveSync depende do sistema operacional executado pelo dispositivo móvel. Para obter detalhes sobre os recursos de suporte do protocolo Exchange ActiveSync para um sistema operacional específico, consulte a documentação do sistema operacional específico.

Sobre o plug-in de administração do Kaspersky Endpoint Security for Android

O Plug-in de administração do Kaspersky Endpoint Security for Android oferece a interface para gerenciar dispositivos móveis e aplicativos móveis instalados neles através do Console de administração do Kaspersky Security Center. O Plug-in de administração do Kaspersky Endpoint Security for Android pode ser usado para:

- Criar políticas de segurança do grupo para dispositivos móveis.
- Definir remotamente as configurações operacionais do aplicativo móvel do Kaspersky Endpoint Security for Android nos dispositivos móveis de usuários.

- Receber relatórios e estatísticas sobre a operação do aplicativo móvel do Kaspersky Endpoint Security for Android nos dispositivos dos usuários.

O plug-in de administração do Kaspersky Endpoint Security for Android é instalado por padrão a implementar o Kaspersky Security Center. O plug-in não necessita de instalação individual.

Sobre o plug-in de administração do Kaspersky Device Management for iOS

O plug-in de administração do Kaspersky Device Management for iOS oferece uma interface para gerenciar dispositivos móveis conectados através dos protocolos iOS MDM e Exchange ActiveSync através do Console de Administração do Kaspersky Security Center. O Plug-in de administração do Kaspersky Device Management for iOS pode ser usado para:

- Criar políticas de segurança do grupo para dispositivos móveis.
- Configurar remotamente os dispositivos conectados através do protocolo Exchange ActiveSync (doravante referido como "Dispositivos EAS").
- Configurar remotamente os dispositivos conectados através do protocolo iOS MDM (doravante referido como "Dispositivos iOS MDM").
- Receber relatórios e estatísticas sobre a operação dos dispositivos móveis dos usuários.

Para obter mais detalhes sobre como conectar dispositivos móveis ao Kaspersky Security Center usando os protocolos iOS MDM e Exchange ActiveSync, consulte a *Ajuda do Kaspersky Security Center*.

O plug-in de administração do Kaspersky Device Management for iOS é instalado por padrão ao implementar o Kaspersky Security Center. O plug-in não precisa de uma instalação separada.

Requisitos de hardware e software

Esta seção lista os requisitos de hardware e software para o computador do administrador que é usado para implementar os aplicativos nos dispositivos móveis, assim como os sistemas operacionais do dispositivo móvel suportados pelo Kaspersky Security for Mobile.

Requisitos de hardware e software para o computador do administrador

Para implementar a solução abrangente Kaspersky Security for Mobile, o computador do administrador tem de atender aos requisitos de hardware do Kaspersky Security Center. Para obter mais detalhes sobre os requisitos de hardware do Kaspersky Security Center, consulte a *Ajuda do Kaspersky Security Center*.

Para trabalhar com o Plug-in de Administração do Kaspersky Endpoint Security for Android, o Console de Administração do Kaspersky Security Center versão 12 ou posterior deve ser instalado no computador do administrador.

Para trabalhar com o Plug-in de administração do Kaspersky Device Management for iOS, o computador do administrador deve atender os seguintes requisitos de software:

- Console de Administração do Kaspersky Security Center 12 ou posterior
- Componente do servidor do Exchange

- Componente do servidor de MDM do iOS
- Conjunto de instruções da versão SSE2 ou da versão mais recente

Para implementar aplicativos móveis do Kaspersky Endpoint Security for Android através do Servidor de Administração, o computador do administrador deve cumprir os seguintes requisitos de software:

- Kaspersky Security Center 12 ou posterior
- Plug-in de Administração para o Kaspersky Endpoint Security for Android

Não há requisitos de software para o computador do administrador quando o aplicativo móvel do Kaspersky Endpoint Security for Android for implementado a partir das lojas on-line relevantes.

O aplicativo móvel do Kaspersky Endpoint Security for Android também pode ser usado como parte do sistema de administração remota do Kaspersky Endpoint Security Cloud (versão 6.0 ou posterior). Para obter mais detalhes sobre o trabalho com aplicativos via Kaspersky Endpoint Security Cloud, consulte a *Ajuda do Kaspersky Endpoint Security Cloud*.

O aplicativo móvel Kaspersky Endpoint Security for Android pode funcionar dentro de sistemas EMM de terceiros:

- VMWare AirWatch 9.3 ou posterior
- MobileIron 10.0 ou posterior
- IBM MaaS360 10.68 ou posterior
- Microsoft Intune 1908 ou posterior
- SOTI MobiControl 14.1.4 (1693) ou posterior

Requisitos de hardware e software para o dispositivo móvel do usuário para compatibilidade com a instalação do aplicativo Kaspersky Endpoint Security for Android

O aplicativo Kaspersky Endpoint Security for Android possui os seguintes requisitos de hardware e software:

- Smartphone ou tablet com uma resolução de tela de 320 x 480 pixels ou superior
- 65 MB de espaço disponível livre na memória principal do dispositivo
- Android 5.0–12 (incluindo Android 12L, excluindo Go Edition)
- arquitetura do processador x86, x86-64, Arm5, Arm6, Arm7 ou Arm8

O aplicativo é instalado somente na memória principal do dispositivo.

Requisitos de hardware e software para um Perfil de iOS MDM

Para um perfil de iOS MDM, o dispositivo deve atender os seguintes requisitos de hardware e software:

- iOS 10.0-15.0 ou iPadOS 13-15
- Conexão com a internet

Problemas conhecidos e considerações

O Kaspersky Endpoint Security for Android possui alguns problemas conhecidos que não são críticos para o funcionamento do aplicativo.

Problemas conhecidos ao instalar aplicativos

- O Kaspersky Endpoint Security for Android somente é instalado na memória principal do dispositivo.
- Em dispositivos que executam Android 7.0, um erro pode ocorrer durante tentativas de desativar os direitos de administrador para o Kaspersky Endpoint Security for Android nas configurações do dispositivo se o Kaspersky Endpoint Security for Android for proibido de se sobrepor em outras janelas. Esta falha é causada por um defeito bem conhecido no Android 7.
- O Kaspersky Endpoint Security for Android em dispositivos que executam o Android 7.0 ou posterior não tem suporte para o modo de múltiplas janelas.
- O Kaspersky Endpoint Security for Android não funciona em dispositivos Chromebook executando o sistema operacional Chrome.
- O Kaspersky Endpoint Security for Android não funciona em dispositivos executando o sistema operacional Android (Go edition).
- Ao usar o aplicativo Kaspersky Endpoint Security for Android com sistemas EMM de terceiros (por exemplo, VMWare AirWatch), somente os componentes Antivírus e Proteção na Web estarão disponíveis. O administrador pode definir as configurações de Antivírus e Proteção na Web no console do sistema EMM. Neste caso, as notificações sobre a operação do aplicativo somente estão disponíveis na interface do aplicativo Kaspersky Endpoint Security for Android (Relatórios).

Problemas conhecidos ao atualizar a versão do aplicativo

- Somente é possível fazer uma atualização do Kaspersky Endpoint Security for Android para uma versão mais recente do aplicativo. O Kaspersky Endpoint Security for Android não pode ser passado para uma versão mais antiga.
- Para atualizar o Kaspersky Endpoint Security for Android usando um pacote de instalação independente, a instalação de aplicativos de origens desconhecidas deve ser permitida no dispositivo móvel do usuário.
- Você pode atualizar através do Google Play se o Kaspersky Endpoint Security for Android tiver sido instalado a partir do Google Play. Se o aplicativo foi instalado usando outro método, você não pode atualizar através do Google Play.
- Você pode atualizar por meio do Kaspersky Security Center se o Kaspersky Endpoint Security for Android tiver sido instalado via Kaspersky Security Center. Se o aplicativo foi instalado a partir do Google Play, você não pode atualizar o aplicativo através do Kaspersky Security Center.
- Depois de atualizar os plug-ins de administração para o Technical Release 33, o aplicativo Kaspersky Endpoint Security for Android também deve ser atualizado para o Technical Release 33. Caso contrário, não será possível ativar o Samsung KNOX em alguns dos dispositivos de seus usuários.

Problemas conhecidos na operação Antivírus

- Devido às limitações técnicas, o Kaspersky Endpoint Security for Android não pode verificar arquivos com um tamanho de 2 GB ou mais. Durante uma verificação, o aplicativo ignora tais arquivos sem notificá-lo que tais arquivos foram ignorados.

- Para a análise adicional de um dispositivo quanto a novas ameaças cujas informações ainda não foram adicionadas aos bancos de dados antivírus, você deve ativar o uso da Kaspersky Security Network. A *Kaspersky Security Network (KSN)* é uma infraestrutura de serviços na nuvem que fornece o acesso à Base de Dados de Conhecimento on-line da Kaspersky, que contém informações sobre a reputação de arquivos, recursos da Web e softwares. Para usar a KSN, o dispositivo móvel deve estar conectado à Internet.

- Em alguns casos, a atualização dos bancos de dados antivírus do Servidor de Administração em um dispositivo móvel pode falhar. Nesse caso, execute a tarefa de atualização do banco de dados de antivírus no Servidor de Administração.

- Em alguns dispositivos, o Kaspersky Endpoint Security for Android não detecta dispositivos conectados através do USB OTG. Não é possível executar uma verificação de vírus em tais dispositivos.

- Em dispositivos com Android 11.0 ou posterior, o usuário deve conceder a permissão "Permitir acesso para gerenciar todos os arquivos".

- Em dispositivos que executam o Android 7.0 ou posterior, a janela de configuração do agendamento da execução da verificação de vírus pode ser incorretamente exibida (os elementos de gerenciamento não são mostrados). Esta falha é causada por um defeito bem conhecido no Android 7.

- Em dispositivos que executam Android 7.0, a proteção em tempo real no modo estendido não detecta ameaças em arquivos armazenados em um cartão SD externo.

- Em dispositivos que executam o Android 6.0, o Kaspersky Endpoint Security for Android não detecta o download de um arquivo malicioso para a memória do dispositivo. Um arquivo malicioso pode ser detectado pelo Antivírus quando o arquivo for executado ou durante uma verificação de vírus do dispositivo. Esta falha é causada por um defeito bem conhecido no Android 6.0. Para assegurar a segurança do dispositivo, recomenda-se configurar verificações de vírus agendadas.

Problemas conhecidos na operação de Proteção na Web

- · A Proteção na Web nos dispositivos Android funciona apenas nos navegadores Google Chrome (incluindo o recurso Guias personalizadas), Huawei Browser e Samsung Internet. A Proteção na Web para Samsung Internet Browser não bloqueia sites em um dispositivo móvel se um perfil de trabalho for usado e a Proteção na Web estiver ativada apenas para o perfil de trabalho.

- O Kaspersky Endpoint Security no perfil de trabalho verifica apenas o domínio do site no tráfego HTTPS. Sites maliciosos e de phishing podem permanecer desbloqueados se o aplicativo estiver instalado no perfil de trabalho. Se o domínio for confiável, a Proteção na Web poderá ignorar uma ameaça (por exemplo, `https://trusted.domain.com/phishing/`). Se o domínio não for confiável, a Proteção na Web bloqueará sites maliciosos e de phishing.

- Para que a Proteção na Web funcione, você deve ativar o uso da Kaspersky Security Network. A Proteção na Web bloqueia os sites com base nos dados da KSN sobre a reputação e a categoria de sites.

- Os sites proibidos podem permanecer desbloqueados pela Proteção na Web em dispositivos que executam o Android 6.0 com a versão 51 de Google Chrome (ou qualquer versão anterior) instalado se o site for aberto nas seguintes formas (este problema é causado por um defeito bem conhecido no Google Chrome):

  - Dos resultados da pesquisa

  - Da lista de favoritos

- Do histórico de pesquisa
- Usar a função de preenchimento automático do endereço da Web
- Abrir o site em uma nova aba no Google Chrome

- Os sites proibidos podem permanecer desbloqueados no Google Chrome versão 50 (ou qualquer versão anterior) se o site tiver sido aberto da página de resultados de uma solicitação de pesquisa do Google enquanto o recurso de **Mesclar abas e aplicativos** estiver ativado nas configurações do navegador. Esta falha é causada por um defeito bem conhecido no Google Chrome.
- Os sites de categorias bloqueadas podem permanecer desbloqueados no Google Chrome se o usuário os abrir a partir de aplicativos de terceiros, por exemplo, de um aplicativo cliente de MI. Este problema é relacionado à forma como o serviço de Acessibilidade trabalha com o recurso de Abas Personalizados do Chrome.
- Os sites proibidos podem permanecer desbloqueados no Samsung Internet Browser se o usuário os abrir no modo de segundo plano a partir do menu de contexto ou de aplicativos de terceiros; por exemplo, de um aplicativo cliente de MI.
- O Kaspersky Endpoint Security for Android deve ser definido como um recurso de Acessibilidade para assegurar o funcionamento apropriado da Proteção na Web.
- Ao inserir um endereço de site nas configurações de Proteção na Web, faça a adesão às seguintes regras:
  - Para dispositivos Android, especifique o endereço no formato de expressões regular (por exemplo, `http:\/\/www\.example\.com.*`).
  - Para dispositivos iOS MDM, especifique o protocolo de transporte de dados HTTP ou HTTPS (por exemplo, `http://www.example.com`).
- Os sites permitidos podem ser bloqueados no Navegador de Internet da Samsung em **Apenas sites listados são permitidos** pelo modo Proteção na Web quando a página for atualizada. Os sites são bloqueados se uma expressão regular contiver configurações avançadas (por exemplo, `^https?:\/\/example\.com\/pictures\/`). Recomenda-se usar expressões regulares sem configurações adicionais (por exemplo, `^https?:\/\/example\.com`).

Problemas conhecidos na operação Antirroubo

- Para a entrega oportuna de comandos aos dispositivos Android, o aplicativo usa o serviço Firebase Cloud Messaging (FCM). Se FCM não for configurado, os comandos serão entregues ao dispositivo somente durante a sincronização com o Kaspersky Security Center, de acordo com o agendamento definido na política, por exemplo, a cada 24 horas.
- Para bloquear um dispositivo, o Kaspersky Endpoint Security for Android deve ser definido como o administrador do dispositivo.
- Para bloquear dispositivos que executam o Android 7.0 ou posterior, o Kaspersky Endpoint Security for Android deve ser definido como um recurso de Acessibilidade.
- Em alguns dispositivos, os comandos Antirroubo podem falhar se o modo de Economia de bateria estiver ativado no dispositivo. Esse defeito foi confirmado no Alcatel 5080X.
- Para localizar dispositivos executando Android 10.0 ou posterior, o usuário deve conceder a permissão "Permitir o tempo todo" à localização do dispositivo.

- Para tirar um retrato com dispositivos executando Android 11.0 ou posterior, o usuário deve conceder a permissão "Enquanto usa o aplicativo" para acessar a câmera.

Problemas conhecidos na operação de Controle de aplicativos

- O Kaspersky Endpoint Security for Android deve ser definido como um recurso de acessibilidade para assegurar o funcionamento apropriado do Controle de aplicativos.
- Para que o Controle de Aplicativos (categorias de aplicativos) funcione, você deve ativar o uso da Kaspersky Security Network. O Controle de Aplicativos determina a categoria de um aplicativo com base nos dados que estão disponíveis na KSN. Para usar a KSN, o dispositivo móvel deve estar conectado à Internet. Para o Controle de Aplicativos, você pode adicionar aplicativos individuais às listas de aplicativos bloqueados e permitidos. Neste caso, a KSN não é necessária.
- Ao configurar o Controle de Aplicativos, recomenda-se desmarcar a caixa de seleção **Bloquear aplicativos do sistema**. O bloqueio de aplicativos do sistema pode levar a problemas na operação do dispositivo.

Problemas conhecidos ao configurar e-mail

- A configuração remota de uma caixa de correio somente está disponível nos seguintes dispositivos:
  - Dispositivos iOS MDM.
  - Dispositivos Samsung (Exchange ActiveSync).
  - Dispositivos Android com o programa de e-mail de TouchDown instalado.

    Em versões anteriores do Kaspersky Endpoint Security for Android, você podia usar o Kaspersky Security Center para configurar remotamente as configurações do perfil TouchDown em um dispositivo de um usuário. O suporte para o TouchDown foi descontinuado no Kaspersky Endpoint Security for Android Service Pack 4. Para obter mais detalhes, consulte o *site de suporte técnico da Symantec*.

    Após atualizar o plug-in Kaspersky Endpoint Security for Android, as configurações do TouchDown na política estarão ocultas, mas salvas. Quando os novos dispositivos são conectados, as configurações do TouchDown serão definidas após a aplicação da política.

    Após a política ter sido modificada e salva, as configurações do TouchDown serão excluídas. As configurações do TouchDown no dispositivo de um usuário serão apagadas após a aplicação de uma política.

Problemas conhecidos ao configurar a força da senha para desbloqueio do dispositivo

- Para dispositivos com Android 10.0 ou posterior, o Kaspersky Endpoint Security divide os requisitos da força de segurança da senha em um dos valores do sistema: médio ou alto.

  Se a quantidade de símbolos exigida for de 1 a 4, então o aplicativo solicita ao usuário que defina uma senha de força média. Ela deve ser numérica (PIN), sem números repetidos ou sequenciais (ex. 1234), ou alfanumérica. O PIN ou a senha deve ter no mínimo 4 caracteres.

Se o número de símbolos exigidos for 5 ou mais, então o aplicativo solicita ao usuário que defina uma senha de segurança alta. Ela deve ser numérica (PIN), sem números repetidos ou sequenciais, ou alfanumérica (senha). O PIN deve ter no mínimo 8 dígitos; a senha deve ter no mínimo 6 caracteres.

- Em dispositivos com Android 10.0 ou posterior, o uso das digitais para desbloquear a tela pode ser disponibilizado somente para o perfil de trabalho.

- Nos dispositivos que executam o Android 7.1.1, se a senha de desbloqueio não atender os requisitos de segurança corporativa (Controle de conformidade), o aplicativo do sistema Configurações pode não funcionar corretamente quando houver uma tentativa de desbloquear a senha através do Kaspersky Endpoint Security for Android. Esta falha é causada por um defeito bem conhecido no Android 7.1.1. Neste caso, para alterar a senha desbloqueada, use somente as Configurações do sistema do aplicativo.

- Em alguns dispositivos que executam o Android 6.0 ou posterior, um erro pode ocorrer quando a senha de desbloqueio da tela é inserida caso os dados do dispositivo estiverem criptografados. Este problema é relacionado aos recursos específicos do serviço de Acessibilidade com firmware MIUI.

Problemas conhecidos ao configurar a Wi-Fi

- Em dispositivos que executam o Android versão 8.0 ou posterior, as configurações do servidor proxy para a Wi-Fi não podem ser redefinidas com a política. No entanto, você pode definir manualmente as configurações de servidor proxy para uma rede Wi-Fi no dispositivo móvel.

Problemas conhecidos ao configurar o APN

- A configuração remota da APN está disponível apenas para os dispositivos iOS MDM ou Samsung.

- Configurar APN para dispositivos iOS MDM na seção **Comunicação celular**. A seção **APN** está desatualizada. Antes de definir as configurações APN, assegure-se que a caixa de seleção **Aplicar no dispositivo** seção **APN** esteja desmarcada.

Problemas conhecidos com o Firewall

- O uso do Firewall está disponível apenas em dispositivos Samsung.

Problemas conhecidos com a configuração da VPN

- A configuração remota da VPN somente está disponível nos seguintes dispositivos:
  - Dispositivos iOS MDM.
  - Dispositivos Samsung.

Problemas conhecidos ao trabalhar com contêineres

- No Kaspersky Security for Mobile Service Pack 3 Maintenance Release 2, não mais há suporte para criar contêineres para aplicativos móveis. Contudo, os contêineres que foram criados em versões mais antigas do aplicativo podem ser adicionados aos dispositivos Android.

- Para instalar aplicativos em contêineres, a instalação de aplicativos de origens desconhecidas deve ser permitida no dispositivo móvel do usuário. Para obter detalhes sobre a instalação de aplicativos sem o Google

Play, consulte o *Guia de Ajuda do Android*.

- A conteinerização do aplicativo não é suportada em dispositivos Android de aplicações que contêm mais de 65.536 métodos (configuração multidex).

Problemas conhecidos com a proteção contra a remoção do aplicativo

- O Kaspersky Endpoint Security for Android deve ser definido como o administrador do dispositivo.
- Para proteger o aplicativo da remoção em dispositivos que executam o Android 7.0 ou posterior, o Kaspersky Endpoint Security for Android deve ser definido como um recurso de Acessibilidade.
- Em alguns dispositivos de Huawei e Xiaomi, a proteção contra remoção do Kaspersky Endpoint Security não funciona. Este problema é causado pelos recursos específicos do firmware MIUI 7 e 8 em dispositivos Xiaomi e do firmware EMUI em dispositivos Huawei.

Problemas conhecidos ao configurar restrições de dispositivo

- Em dispositivos Android 10.0 ou posteriores, a proibição do uso de redes Wi-Fi não é compatível.
- Em dispositivos Android 10.0 ou posteriores, o uso da câmera não pode ser totalmente proibido.
- Nos dispositivos que executam o Android 11 ou posterior, o Kaspersky Endpoint Security for Android deve ser definido como um recurso de Acessibilidade. O Kaspersky Endpoint Security for Android solicita que o usuário defina o aplicativo como um recurso de Acessibilidade pelo Assistente de Configuração Inicial. O usuário pode ignorar esta etapa ou desativar este serviço nas configurações de dispositivo em um momento posterior. Nesse caso, não será possível restringir o uso da câmera.

Problemas conhecidos ao enviar comandos para dispositivos móveis

- Em dispositivos executando Android 12 ou posterior, se o usuário tiver concedido a permissão "Usar local aproximado", o aplicativo Kaspersky Endpoint Security for Android tentará primeiro obter a localização precisa do dispositivo. Se isso não for bem-sucedido, a localização aproximada do dispositivo será retornada apenas se tiver sido recebida não mais de 30 minutos antes. Caso contrário, o comando **Localizar o dispositivo** falhará.

Problemas conhecidos com o perfil de trabalho do Android

- Caso um perfil de trabalho do Android seja criado usando uma política, o usuário deverá conceder a permissão "Permitir acesso para gerenciar todos os arquivos" ao Kaspersky Endpoint Security for Android que está instalado nos dispositivos que executam o Android 11 ou posterior e que está relacionado ao perfil de trabalho.

Problemas conhecidos com dispositivos específicos

- Em certos dispositivos (por exemplo, Huawei, Meizu e Xiaomi), você deve conceder uma permissão de inicialização automática ao Kaspersky Endpoint Security for Android ou adicioná-lo manualmente à lista de aplicativos iniciados quando o sistema operacional for inicializado. Se o aplicativo não for adicionado à lista, o Kaspersky Endpoint Security for Android para a execução de todas as suas funções após a reinicialização do dispositivo móvel. Além disso, se o dispositivo foi bloqueado, você não pode usar um comando para desbloquear o dispositivo. Você somente pode desbloquear o dispositivo ao usar um código de desbloqueio de uma só utilização.

- Em determinados dispositivos (por exemplo, Meizu e Asus), a execução do Android 6.0 ou posterior, após a criptografia dos dados e o reinício do dispositivo Android, você deve inserir uma senha numérica para desbloquear o dispositivo. Se o usuário usar uma senha gráfica para desbloquear o dispositivo, você deve converter a senha gráfica em uma senha numérica. Para obter mais detalhes sobre a conversão de uma senha gráfica em uma senha numérica, consulte o site de Suporte Técnico do fabricante de dispositivo móvel. Este problema é relacionado à operação do serviço Recursos de Acessibilidade.

- Em alguns dispositivos Huawei executando o Android 5.X, após o Kaspersky Endpoint Security for Android ser definido como um recursos de acessibilidade, uma mensagem incorreta sobre a falta de direitos apropriados será exibida. Para ocultar esta mensagem, ative o aplicativo como aplicativo protegido nas configurações do dispositivo.

- Em alguns dispositivos Huawei que executam o Android 5. X ou 6. X, quando o modo de Economia de bateria estiver ativado para o Kaspersky Endpoint Security for Android, o usuário pode terminar manualmente o aplicativo. O dispositivo do usuário se torna desprotegido após isso. Esse problema é devido a alguns recursos do software da Huawei. Para restaurar a proteção do dispositivo, execute manualmente o Kaspersky Endpoint Security for Android. Recomenda-se desativar o modo de Economia de bateria para o Kaspersky Endpoint Security for Android nas configurações do dispositivo.

- Em dispositivos Huawei com o firmware EMUI executando o Android 7.0, o usuário pode ocultar a notificação quanto ao status da proteção do Kaspersky Endpoint Security for Android. Esse problema é devido a alguns recursos do software da Huawei.

- Em alguns dispositivos Xiaomi, ao definir o comprimento de senha em mais de 5 caracteres em uma política, o usuário será solicitado a modificar a senha de desbloqueio da tela em vez do código PIN. Você não pode definir um código PIN que tenha mais de 5 caracteres. Este problema é devido a alguns recursos do software da Xiaomi.

- Em dispositivos Xiaomi com o firmware MIUI executando o Android 6.0, o ícone do Kaspersky Endpoint Security for Android na barra de status pode estar oculto. Este problema é devido a alguns recursos do software da Xiaomi. Recomenda-se permitir a exibição de ícones de notificação nas configurações de Notificações.

- Em alguns dispositivos Nexus que executam o Android 6.0.1, os privilégios necessários para o funcionamento apropriado não podem ser concedidos através do Assistente de Início Rápido do Kaspersky Endpoint Security for Android. Esta falha é causada por um defeito bem conhecido na Correção de Segurança para o Android pelo Google. Para assegurar a operação apropriada, os privilégios necessários devem ser manualmente concedidos nas configurações do dispositivo.

- Em determinados dispositivos Samsung que executam o Android 7.0 ou posterior, quando o usuário tenta configurar métodos não compatíveis para desbloquear o dispositivo (por exemplo, uma senha gráfica), o dispositivo pode ser bloqueado se as seguintes condições forem atendidas: A remoção do Kaspersky Endpoint Security for Android está ativada e os requisitos de força da senha de desbloqueio da tela estão definidos. Para desbloquear o dispositivo, é necessário enviar um comando especial ao dispositivo.

- Em determinados dispositivos Samsung é impossível bloquear o uso de impressões digitais para desbloquear a tela.

- A Proteção na Web não pode ser ativada em alguns dispositivos Samsung, caso o dispositivo esteja conectado a uma rede 3G/4G e tenha o modo de Economia de bateria ativado para restringir os dados de segundo plano. Recomenda-se desativar a função que restringe os processos em segundo plano nas configurações de Economia de bateria.

- Em determinados dispositivos Samsung, se a senha de desbloqueio não estiver em conformidade com requisitos de segurança corporativa, o Kaspersky Endpoint Security for Android não bloqueia o uso de impressões digitais para desbloquear a tela.

- Após executar os comandos de Antirroubo (tal como, Localizar, Bloquear dispositivo, Desbloquear e Retrato), o certificado geral e o certificado VPN podem ser excluídos de alguns dispositivos Samsung. Os certificados

precisam ser reinstalados para continuar. Esse problema ocorre devido ao padrão de segurança Fundamentos do Perfil de Proteção para Dispositivos Móveis (MDFPP).

- Em alguns dispositivos Honor e Huawei, não é possível restringir o uso de Bluetooth. Quando o Kaspersky Endpoint Security for Android tenta restringir o uso de Bluetooth, o sistema operacional exibe uma notificação com a opção de rejeitar ou permitir essa restrição. O usuário pode rejeitar essa restrição e continuar usando o Bluetooth.

- Em alguns dispositivos Samsung, após a instalação ou atualização do Kaspersky Endpoint Security de um pacote de instalação autônomo, a ativação do perfil KNOX MDM fica indisponível.

- Em dispositivos Blackview, o usuário pode limpar a memória do aplicativo Kaspersky Endpoint Security for Android. Como resultado, a proteção e o gerenciamento do dispositivo são desativados, todas as configurações definidas tornam-se ineficazes e o aplicativo Kaspersky Endpoint Security for Android é removido dos recursos de Acessibilidade. Isso ocorre porque os dispositivos deste fornecedor fornecem o aplicativo de Telas recentes personalizado com privilégios elevados. Este aplicativo pode substituir as configurações do Kaspersky Endpoint Security for Android e não pode ser substituído porque ele faz parte do sistema operacional Android.

- Em alguns dispositivos que executam o Android 11, o aplicativo Kaspersky Endpoint Security for Android trava imediatamente após ser iniciado. Essa falha é causada por um familiar defeito no Android 11.

Implementação

Esta seção da Ajuda é destinada para especialistas que administram e administram o Kaspersky Security for Mobile, assim como para especialistas que fornecem o Suporte Técnico às organizações que usam o Kaspersky Security for Mobile.

A arquitetura da solução

O Kaspersky Security for Mobile inclui os seguintes componentes:

- Aplicativo móvel Kaspersky Endpoint Security for Android

  O aplicativo Kaspersky Endpoint Security for Android garante a proteção de dispositivos móveis contra ameaças da web, vírus e outros programas que representam ameaças. Ele suporta a interação entre o dispositivo móvel e o Servidor de Administração do Kaspersky Security Center usando o Firebase Cloud Messaging.

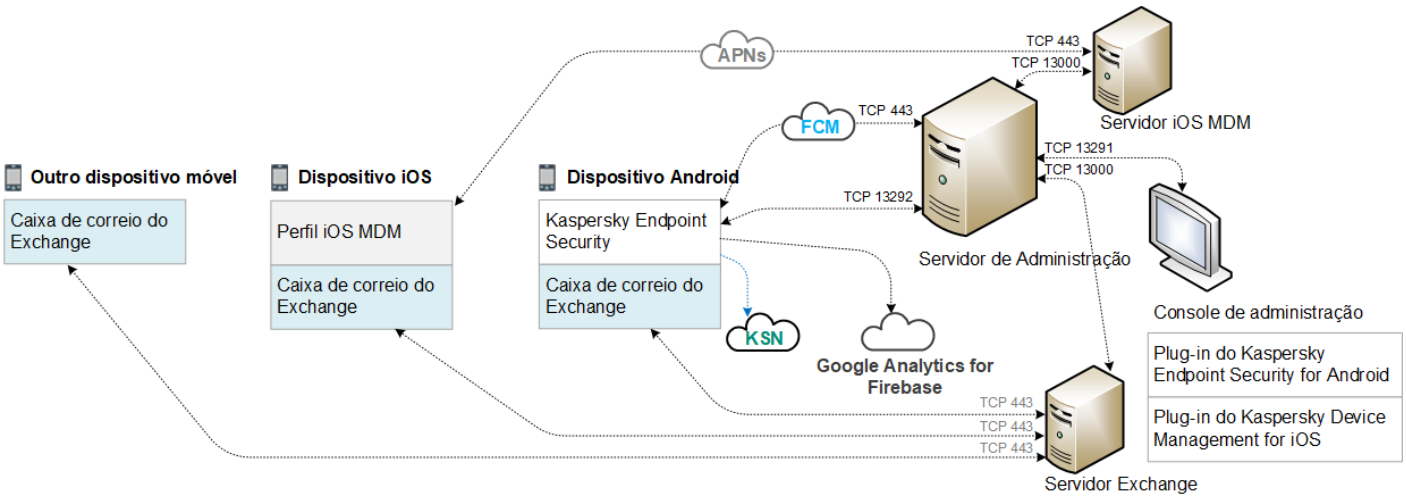
- Plug-in de administração do Kaspersky Endpoint Security for Android

  O Plug-in de administração do Kaspersky Endpoint Security for Android oferece a interface para gerenciar dispositivos móveis e aplicativos móveis instalados neles através do Console de administração do Kaspersky Security Center.

- Plug-in de Administração para o Kaspersky Device Management for iOS

  O plug-in de administração do Kaspersky Device Management for iOS oferece uma interface para gerenciar dispositivos móveis conectados através dos protocolos iOS MDM e Exchange ActiveSync através do Console de Administração do Kaspersky Security Center.

A arquitetura da solução integrada Kaspersky Security for Mobile é mostrada na figura abaixo.



Arquitetura do Kaspersky Security for Mobile

Para obter detalhes sobre o Console de Administração, Servidor de Administração, Servidor do Exchange e Servidor de MDM do iOS, consulte a *Ajuda do Kaspersky Security Center*.

Cenários comuns de implementação da solução integrada

Esta seção cobre os cenários comuns de implementação da solução integrada Kaspersky Security for Mobile.

Diferentes cenários de implementação podem ser usados para implementar a solução integrada em dispositivos Android e dispositivos iOS. Se a organização usar dispositivos móveis que executam diversos sistemas operacionais, os aplicativos devem ser instalados para cada sistema operacional separadamente ao seguir o cenário de implementação apropriado.

Cenários de implementação para o Kaspersky Endpoint Security for Android

O Kaspersky Endpoint Security for Android pode ser implementado em dispositivos móveis dentro da rede corporativa de diversas maneiras. Você pode usar o cenário de implementação mais adequado para a sua organização ou combinar diversos cenários de implementação.

Para obter detalhes sobre a implementação do Kaspersky Endpoint Security for Android no Kaspersky Endpoint Security Cloud, consulte a *Ajuda do Kaspersky Endpoint Security Cloud*.

Implementar o Kaspersky Endpoint Security for Android através do Kaspersky Security Center

Você pode implementar o Kaspersky Endpoint Security for Android através do Kaspersky Security Center usando os seguintes métodos:

- Entregue mensagens com o link do Google Play (recomendado)
- Entregue mensagens com um link ao pacote de aplicativo independente

A implementação do Kaspersky Endpoint Security for Android usando Google Play consiste no envio de mensagens que contêm o link para o Google Play para usuários de dispositivos a partir do Console de Administração.

A implementação do Kaspersky Endpoint Security for Android através do pacote de entrega independente consiste nas seguintes etapas a serem executadas pelo administrador:

1. Criar um pacote de instalação do aplicativo.
2. Definição das configurações do pacote de instalação.
3. Criar um pacote de instalação independente.
4. Enviar mensagens com um link para baixar de um pacote de instalação independente para usuários de dispositivos Android. O correio em massa está disponível.

O usuário instala o Kaspersky Endpoint Security for Android em um dispositivo móvel após receber uma mensagem com um link ao Google Reproduzem ou um link para baixar o pacote de instalação do Servidor da Web do Kaspersky Security Center. Nenhuma preparação adicional é necessária para começar a usar o aplicativo.

Implementar o Kaspersky Endpoint Security for Android a partir do Google Play

Recomenda-se empregar o cenário de implementação do Google Play se a instalação remota não for possível.

O Kaspersky Endpoint Security for Android é instalado a partir do Google Play de forma independente pelos usuários de dispositivos. Os usuários efetuam o download do pacote de distribuição do aplicativo móvel a partir do Google Play e instalam o aplicativo nos dispositivos. Depois que o aplicativo tiver sido instalado no dispositivo, você deve fazer preparações adicionais antes que possa começar a usá-lo: definir as configurações da conexão ao Servidor de Administração e instalar um certificado geral.

Implementar o Kaspersky Endpoint Security for Android através do KNOX Mobile Enrollment

A implementação do Kaspersky Endpoint Security for Android consiste em adicionar um perfil KNOX MDM aos dispositivos móveis. O perfil MDM de KNOX contém um link para um aplicativo implementado no Servidor da Web do Kaspersky Security Center ou em outro servidor. Após a instalação do aplicativo no dispositivo móvel, você também deve instalar um certificado geral.

É possível ler sobre a instalação por meio do KNOX Mobile Enrollment na seção Samsung KNOX.

Cenários de implementação para o perfil de iOS MDM

Um *perfil de iOS MDM* é um perfil que contém as configurações para conectar dispositivos móveis que executam iOS ao Kaspersky Security Center. Após a instalação de um perfil de iOS MDM e sincronização com o Kaspersky Security Center, o dispositivo se torna um dispositivo gerenciado. Os dispositivos móveis são gerenciados através do serviço Apple Push Notification (APNs). Para obter mais detalhes sobre como instalar um perfil de iOS MDM e trabalhar com APNs, consulte a *Ajuda do Kaspersky Security Center*.

Usando um perfil de iOS MDM, é possível:

- Definir remotamente as configurações dos dispositivos iOS MDM usando políticas de grupo.
- Enviar comandos de bloqueio e de limpeza de dados do dispositivo.
- Instale remotamente os aplicativos da Kaspersky e outras aplicativos de terceiros.

Um perfil de iOS MDM pode ser implementado em dispositivos móveis dentro da rede corporativa de diversas maneiras. Você pode usar o cenário de implementação mais adequado para a sua organização ou combinar diversos cenários de implementação.

Antes de implementar um perfil de iOS MDM, o administrador deve fazer o seguinte:

1. Instale um servidor de MDM do iOS.
2. Obtenha um certificado do Apple Push Notification Service da Apple (certificado de APNs).
3. Instale um certificado de APNs no servidor de MDM do iOS.

Para obter mais detalhes sobre como instalar um Servidor de MDM do iOS e trabalhar com um certificado de APNs, consulte a *Ajuda do Kaspersky Security Center*.

Para obter detalhes sobre a implementação de um perfil de iOS MDM no Kaspersky Endpoint Security Cloud, consulte a *Ajuda do Kaspersky Endpoint Security Cloud*.

Implementar um perfil de iOS MDM através do Kaspersky Security Center

A implementação de um perfil de iOS MDM através do Kaspersky Security Center pode ser executada enviando mensagens que contêm um link para baixar o perfil de iOS MDM. O correio em massa está disponível.

O usuário instala o perfil de iOS MDM em um dispositivo móvel depois de receber a mensagem com um link ao Servidor da Web do Kaspersky Security Center. Nenhuma preparação adicional para o perfil de iOS MDM é necessária.

Para obter mais detalhes sobre como criar um perfil de iOS MDM, consulte a *Ajuda do Kaspersky Security Center*.

Preparar o Console de administração para a implementação de uma solução integrada

Esta seção fornece instruções sobre a preparação do Console de Administração para a implementação da solução integrada.

Configurações do Servidor de Administração para conexão de dispositivos móveis

Para que os dispositivos móveis possam se conectar ao Servidor de Administração, antes de instalar o aplicativo móvel do Kaspersky Endpoint Security, defina as configurações de conexão do dispositivo móvel nas propriedades do Servidor de Administração.

Para definir as configurações do Servidor de Administração para conexão de dispositivos móveis:

1. No menu de contexto do Servidor de Administração, selecione **Propriedades**.

   A janela Configurações do Servidor de Administração é aberta.

2. Selecione **Configurações de conexão do servidor** → **Portas adicionais**.

3. Selecione a caixa de seleção **Abrir a porta para dispositivos móveis**.

4. No campo **Porta para dispositivos móveis**, especifique a porta através da qual os dispositivos móveis serão conectados ao Servidor de Administração.

   A porta 13292 é utilizada por padrão. Se a caixa **Abrir porta para dispositivos móveis** for desmarcada ou a porta de conexão incorreta for especificada, os dispositivos móveis não poderão se conectar com o Servidor de Administração.

5. No campo **Porta para ativar dispositivos móveis clientes**, especifique a porta a ser usada por dispositivos móveis para conectar-se ao Servidor de Administração para a ativação do aplicativo do Kaspersky Endpoint Security for Android. A porta 17100 é utilizada por padrão.

6. Clique em **OK**.

Exibir a pasta Gerenciamento de dispositivo móvel no Console de Administração

Ao exibir a pasta **Gerenciamento de dispositivo móvel** no Console de Administração, você pode visualizar a lista de dispositivos móveis gerenciados pelo Servidor de Administração, definir as configurações de gerenciamento dos dispositivos móveis e instalar certificados nos dispositivos móveis dos usuários.

*Para ativar a exibição da pasta **Gerenciamento de dispositivo móvel** no Console de Administração:*

1. No menu de contexto do Servidor de Administração, selecione **Exibir → Configurar a interface**.

2. Na janela que for aberta, selecione a caixa de seleção **Exibir o Gerenciamento de dispositivos móveis**.

3. Clique em **OK**.

A pasta **Gerenciamento de dispositivo móvel** é exibida na árvore do Console de administração após este ter sido reiniciado.

Criação de um grupo de administração

Para executar a configuração centralizada do aplicativo do Kaspersky Endpoint Security for Android instalado nos dispositivos móveis dos usuários, as políticas de grupo devem ser aplicadas aos dispositivos.

Para aplicar a política a um grupo de dispositivos, recomenda-se criar um grupo separado para esses dispositivos na pasta **Dispositivos gerenciados** antes de instalar os aplicativos móveis nos dispositivos dos usuários.

Após criar um grupo de administração, recomenda-se configurar a opção de alocar automaticamente dispositivos nos quais deseja instalar os aplicativos para esse grupo. Em seguida, defina as configurações que são comuns a todos os dispositivos usando uma política do grupo.

Para criar um grupo de administração, siga as etapas abaixo:

1. Na árvore do console, selecione a pasta **Dispositivos gerenciados**.

2. Na área de trabalho da pasta **Dispositivos gerenciados** ou de sua subpasta, selecione a guia **Dispositivos**.

3. Clique no botão **Novo grupo**.

Isto abre a janela na qual você pode criar um novo grupo.

4. Na janela **Nome do grupo** digite o nome do grupo e clique em **OK**.

Uma nova pasta de grupo de administração com o nome especificado é exibida na árvore de console. Para obter informações mais detalhadas sobre a utilização de grupos de administração, consulte a *Ajuda do Kaspersky Security Center*.

Criação de uma regra para alocação automática do dispositivo para grupos de administração

É possível administrar centralmente as configurações do aplicativo do Kaspersky Endpoint Security for Android em dispositivos móveis de usuários apenas se os dispositivos pertencerem a um grupo de administração criado anteriormente para o qual uma política de grupo tiver sido configurada.

Se a regra para alocar automaticamente os dispositivos móveis detectados na rede ao grupo de administração não estiver configurada, durante a primeira sincronização do dispositivo com o Servidor de Administração, o dispositivo é enviado automaticamente para o Console de Administração na pasta **Adicional** → **Conjunto de rede** → **Domínios** → **KES10**. Uma política do grupo não se aplica a esse dispositivo.

Para criar a regra para a alocação automática de dispositivos móveis para grupos de administração, siga as etapas abaixo:

1. Na árvore do console, selecione a pasta **Dispositivos não atribuídos**.
2. No menu de contexto da pasta **Dispositivos não atribuídos**, selecione **Propriedades**.

   A janela **Propriedades: Dispositivos não atribuídos** é exibida.
3. Na seção **Mover dispositivos**, clique em **Adicionar** para iniciar o processo de criar uma regra para a alocação automática de dispositivos em um grupo de administração.

   A janela **Nova regra** é exibida.
4. Digite o nome da regra.
5. Especifique o grupo de administração ao qual os dispositivos móveis devem ser alocados depois que o aplicativo móvel do Kaspersky Endpoint Security for Android tiver sido instalado neles. Para fazer isso, clique em **Procurar** à direita do campo **Grupo para mover os dispositivos para** e selecione o grupo na janela que for exibida.
6. Na seção **Aplicação da regra**, selecione **Executar uma vez para cada dispositivo**.
7. Marque a caixa de seleção **Mover somente dispositivos não adicionados aos grupos de administração** para evitar a alocação de dispositivos móveis ao grupo selecionado que são alocados a outros grupos de administração ao aplicar a regra.
8. Selecione a caixa de verificação **Ativar regra**, para que a regra possa ser aplicada a dispositivos detectados recentemente.
9. Abra a seção **Aplicativos** e faça o seguinte:

   a. Selecione a caixa de seleção **Versão do sistema operacional**.

   b. Selecione um ou diversos tipos de sistemas operacionais dos dispositivos a serem alocados ao grupo especificado: Android ou iOS.

10. Clique em **OK**.

    A regra recém-criada é exibida na lista de regras de alocação de dispositivo na seção **Mover dispositivos** na janela Propriedades da pasta **Dispositivos não atribuídos**.

De acordo com a regra, o Kaspersky Security Center aloca todos os dispositivos que atendam aos requisitos especificados na pasta **Dispositivos não atribuídos** para o grupo selecionado. Os dispositivos móveis anteriormente alocados na pasta **Dispositivos não atribuídos** também podem ser alocados manualmente ao grupo de administração exigido da pasta **Dispositivos gerenciados**. Para obter informações mais detalhadas sobre o gerenciamento de grupos de administração e ações com dispositivos não distribuídos, consulte a *Ajuda do Kaspersky Security Center*.

Criar um certificado geral

Você deve criar um certificado geral no Console de Administração para efeitos de identificar o usuário de um dispositivo móvel.

Para criar um certificado geral:

1. Na árvore do console, selecione a pasta **Gerenciamento de Dispositivos Móveis → Certificados**.
2. Na área de trabalho da pasta **Certificados**, clique no botão **Adicionar certificado** para iniciar o Assistente de Instalação do Certificado.
3. Na janela **Tipo de certificado** do Assistente, selecione a opção **Certificado geral**.
4. Na janela **Seleção do usuário** do Assistente, especifique os usuários para quem deseja criar um certificado geral.
5. Na janela **Origem de certificado** do Assistente, selecione o método pelo qual você deseja criar o certificado geral.
   - Para criar um certificado geral automaticamente usando as ferramentas do Servidor de Administração, selecione **Emitir o certificado através das ferramentas do Servidor de Administração**.
   - Para atribuir um certificado criado anteriormente a um usuário, selecione a opção **Especificar arquivo de certificado**. Clique no botão **Especificar** para abrir a janela **Certificado** e especificar o certificado na mesma.

     Desmarque a caixa de seleção **Publicar o certificado** se você não desejar especificar o tipo de dispositivo móvel e o método de notificar o usuário sobre a criação do certificado.
6. Na janela **Método de notificação ao usuário** do assistente, defina as configurações de notificação do usuário do dispositivo móvel sobre a criação do certificado utilizando uma mensagem de texto ao através de e-mail.
7. Na janela **Gerar do certificado** do Assistente, clique **Concluído** para concluir o Assistente de Instalação do Certificado.

Como resultado, o Assistente de Criação do Certificado cria um certificado geral que o usuário pode instalar no dispositivo móvel. Para obter o certificado, inicie a sincronização do dispositivo móvel com o Servidor de Administração. Para obter mais informações sobre a criação de certificados e a configuração de regras para emiti-los, consulte a *Ajuda do Kaspersky Security Center*.

Instalação do Kaspersky Endpoint Security for Android

Esta seção descreve os métodos para implementar o Kaspersky Security for Android em uma rede corporativa.

Permissões

Para todos os recursos dos aplicativos, o Kaspersky Endpoint Security for Android solicita ao usuário as permissões necessárias. O Kaspersky Endpoint Security for Android solicita as permissões obrigatórias ao concluir o Assistente de Instalação, assim como após a instalação antes da utilização dos recursos individuais dos aplicativos. É impossível instalar o Kaspersky Endpoint Security for Android sem fornecer as permissões obrigatórias.

Em certos dispositivos (por exemplo, Huawei, Meizu e Xiaomi), o Kaspersky Endpoint Security for Android deve ser adicionado manualmente à lista de aplicativos que serão iniciados ao inicializar o sistema operacional nas configurações do dispositivo. Se o aplicativo não for adicionado à lista, o Kaspersky Endpoint Security for Android para a execução de todas as suas funções após a reinicialização do dispositivo móvel.

Em dispositivos com Android 11 ou posterior, é necessário desabilitar a configuração do sistema **Remover permissões se o aplicativo não for usado**. Caso contrário, depois que o aplicativo não for usado por alguns meses, o sistema redefinirá automaticamente as permissões que o usuário concedeu ao aplicativo.

Não há mais suporte para o Filtro de Chamadas e Mensagens de texto e para o SIM Watch no Kaspersky Endpoint Security for Android Service Pack 4 Atualização 4 (Compilação 10.8.0.103). Neste caso, o Kaspersky Endpoint Security for Android não solicita ao usuário a permissão de gerenciamento de SMS. Para ativar o Filtro de Chamadas e Mensagens de texto e todos os recursos do SIM Watch, você deve usar uma versão anterior do Kaspersky Endpoint Security for Android.

Permissões solicitadas pelo Kaspersky Endpoint Security for Android

Permissão	Função do aplicativo
Telefone (necessário apenas para o Android 5.0 – 9.X)	Conectar-se ao Kaspersky Security Center (ID do dispositivo)
Armazenamento (obrigatório)	Antivírus
Acesso para gerenciar todos os arquivos	Antivírus (somente para Android 11 ou posterior)
Dispositivos Bluetooth por perto (para Android 12 ou posterior)	Restringir o uso do Bluetooth
Administrador do dispositivo (obrigatório)	Antirroubo – bloqueia o dispositivo (somente para o Android 5.0 – 6.X)
	Antirroubo – tirar um retrato com a câmera frontal
	Antirroubo – soar um alarme
	Antirroubo – redefinição completa
	Proteção por senha
	Proteção contra a remoção do aplicativo
	Instalar o certificado de segurança
	Controle de aplicativos

	Gerenciar KNOX (somente para dispositivos Samsung)
	Configurar o Wi-Fi
	Configurar o Exchange ActiveSync
	Restringir o uso da câmera, Bluetooth e Wi-Fi
Câmera	Antirroubo – tirar um retrato com a câmera frontal Em dispositivos executando Android 11.0 ou posterior, o usuário deve conceder a permissão "Enquanto usa o aplicativo" quando solicitado
Localização	Antirroubo – localizar o dispositivo Em dispositivos executando Android 10.0 ou posterior, o usuário deve conceder a permissão "Permitir o tempo todo" quando solicitado.
Acessibilidade	Antirroubo – bloquear o dispositivo (somente para o Android 7.0 ou posterior)
	Proteção na Web
	Controle de aplicativos
	Proteção contra a remoção do aplicativo (somente para Android 7.0 ou posterior)
	Exibição de avisos do Kaspersky Endpoint Security for Android (apenas para Android 10.0 ou posterior)
	Restringir o uso da câmera (apenas para Android 11 ou posterior)

Instalação do Kaspersky Endpoint Security for Android usando um link do Google Play

O Kaspersky Endpoint Security for Android é instalado nos dispositivos móveis de usuários cujas contas de usuário foram adicionadas no Kaspersky Security Center. Para obter mais detalhes sobre as contas de usuário no Kaspersky Security Center, consulte a Ajuda do Kaspersky Security Center.

O Kaspersky Security for Mobile permite instalar o aplicativo através do Kaspersky Security Center usando um link do Google Play (método recomendado).

O usuário receberá um link ao Google Play. O aplicativo pode ser instalado seguindo o procedimento padrão de instalação na plataforma Android. A configuração adicional do Kaspersky Endpoint Security for Android após a instalação não é necessária.

Alguns dispositivos Huawei e Honor não possuem serviços Google e, consequentemente, acesso a aplicativos no Google Play. Se alguns usuários de aparelhos Huawei e Honor não puderem instalar o aplicativo do Google Play, é recomendável que sejam instruídos a instalar o aplicativo da Huawei App Gallery.

O link contém os seguintes dados:

- Configurações de sincronização do Kaspersky Security Center.
- Certificado geral.
- Indicador de aceite dos Termos e Condições do Contrato de Licença do Usuário Final para o Kaspersky Endpoint Security for Android e Declarações adicionais. Caso o administrador aceite os termos do Contrato de Licença e as Declarações adicionais no Console de Administração, o Kaspersky Endpoint Security for Android ignorará a etapa de aceite durante a instalação do aplicativo.

Para instalar o Kaspersky Endpoint Security for Android por meio do Kaspersky Security Center usando um link do Google Play:

1. Na árvore do console, selecione a pasta **Gerenciamento de Dispositivos Móveis → Dispositivos móveis**.
2. Na área de trabalho da pasta **Dispositivos móveis**, clique no botão **Adicionar dispositivo móvel**.

   Isto inicia o assistente Nova conexão de dispositivo móvel. Siga as instruções do Assistente.
3. Na janela **Sistema operacional** do Assistente, selecione **Android**.

   O Kaspersky Security Center verifica a existência de atualizações do plug-in de administração. Se o Kaspersky Security Center detectar atualizações, você poderá instalar a nova versão do plug-in de administração. Quando o plug-in de administração for atualizado, será possível aceitar os Termos e Condições do Contrato de Licença do Usuário Final e as Declarações adicionais para o Kaspersky Endpoint Security for Android. Caso o administrador aceite o Contrato de Licença e as Declarações adicionais no Console de Administração, o Kaspersky Endpoint Security for Android ignorará a etapa de aceite durante a instalação do aplicativo. Esse recurso está disponível no Kaspersky Security Center versão 12.
4. Na página **Método de instalação do Kaspersky Endpoint Security for Android**, selecione o método de instalação do aplicativo **Usando um link do Google Play**.
5. Na página **Selecionar usuários** do Assistente, selecione um ou mais usuários para instalar o Kaspersky Endpoint Security for Android em seus dispositivos móveis.

   Se um usuário não estiver na lista, é possível adicionar uma nova conta de usuário sem sair do Assistente de Conexão de Novos Dispositivos Móveis.
6. Na página **Origem do certificado** do Assistente, selecione a origem do certificado para a proteção da transferência de dados entre o Kaspersky Endpoint Security for Android e o Kaspersky Security Center:

   - **Emitir o certificado através das ferramentas do Servidor de Administração.** Neste caso, o certificado será criado automaticamente.
   - **Especifique o arquivo do certificado**. Neste caso, o seu próprio certificado deve ser preparado antes do tempo e então selecionado na janela do Assistente. Esta opção não pode ser usada se você quiser instalar o Kaspersky Endpoint Security for Android em vários dispositivos móveis. Um certificado separado deve ser criado para cada usuário.
7. Na página **Método de notificação ao usuário** do Assistente, selecione o canal usado para enviar o link de instalação do aplicativo:

   - Para enviar o link por e-mail, selecione **Enviar o link ao Kaspersky Endpoint Security** e defina as configurações na seção **Por e-mail**. Assegure-se de que o endereço de e-mail esteja especificado nas configurações de contas de usuário.
   - Para enviar o link por mensagem SMS, selecione **Enviar o link ao a Kaspersky Endpoint Security** e defina as configurações na seção **Por SMS**. Assegure-se de que o número de telefone esteja especificado nas configurações de contas de usuário.

- Para instalar o Kaspersky Endpoint Security for Android usando um código QR, selecione **Mostrar link para o pacote de instalação** e digitalize o código QR usando a câmera do dispositivo móvel.

- Se nenhum dos métodos listados for conveniente para você, selecione **Mostrar o link para o pacote de instalação** → **Copiar** para copiar o link para instalar o Kaspersky Endpoint Security for Android na área de transferência. Usar qualquer método disponível para entregar o link de instalação do aplicativo. Também é possível usar outros métodos de instalação do Kaspersky Endpoint Security for Android.

8. Clique em **Concluir** para fechar o Assistente de Conexão de Novos Dispositivos Móveis.

Após instalar o Kaspersky Endpoint Security for Android nos dispositivos móveis de usuários, será possível definir as configurações dos dispositivos e aplicativos usando políticas de grupo. Você também será capaz de enviar comandos aos dispositivos móveis para a proteção dos dados em caso de perda ou roubo dos dispositivos.

Outros métodos de instalação do Kaspersky Endpoint Security for Android

É possível instalar o Kaspersky Endpoint Security for Android usando um link para seu próprio servidor da Web ou instruir os usuários a instalar o aplicativo manualmente.

Instalação manual a partir do Google Play ou da Huawei AppGallery

Os usuários podem instalar manualmente o Kaspersky Endpoint Security for Android do Google Play ou Huawei AppGallery. O aplicativo pode ser instalado ao seguir o procedimento padrão de instalação da plataforma Android. Os usuários usam suas próprias contas do Google para instalar o aplicativo.

Para obter detalhes sobre o procedimento de instalação do Kaspersky Endpoint Security for Android a partir do Google Play, consulte o site de suporte técnico da Google.

Para obter detalhes sobre o procedimento de instalação do Kaspersky Endpoint Security for Android a partir da Huawei AppGallery, consulte o site de suporte HUAWEI.

Alguns dispositivos Huawei e Honor não possuem serviços Google e, consequentemente, acesso a aplicativos no Google Play. Se alguns usuários de aparelhos Huawei e Honor não puderem instalar o aplicativo do Google Play, é recomendável que sejam instruídos a instalar o aplicativo da Huawei App Gallery.

Após instalar o Kaspersky Endpoint Security for Android a partir do Google Play ou Huawei AppGallery, você deve preparar o aplicativo para uso. O processo de preparar o aplicativo para utilização inclui as seguintes etapas:

1. O administrador envia as configurações da sincronização do dispositivo móvel com o Servidor de Administração (endereço do servidor e número da porta) usando qualquer método disponível (por exemplo, enviando uma mensagem de e-mail).

2. O usuário pode definir as configurações da sincronização do dispositivo móvel com o Servidor de Administração durante a operação do Assistente de Configuração Inicial ou nas configurações do Kaspersky Endpoint Security for Android.

3. O administrador cria um certificado geral para o dispositivo móvel do usuário.

4. O usuário recebe uma notificação automática com uma mensagem para instalar o certificado geral. Quando a instalação for confirmada, o certificado geral é instalado no dispositivo móvel.

O acesso à Internet deve ser ativado no dispositivo móvel para a sincronização com o Servidor de Administração.

Consulte a Ajuda do Kaspersky Security Center para obter detalhes sobre como definir as configurações da sincronização do dispositivo móvel com o Servidor de Administração e receber um certificado geral.

Durante a próxima sincronização do dispositivo móvel com o Servidor de Administração, o dispositivo móvel do usuário no qual o Kaspersky Endpoint Security for Android estiver instalado é movido para a pasta **Adicional** → **Conjunto de redes** → **Domínios** no grupo de administração que foi especificado durante a instalação do aplicativo (o grupo padrão é **KES10**). É possível mover um dispositivo móvel para o grupo de administração criado na pasta Dispositivos gerenciados manualmente ou utilizando as regras de alocação automática.

Este método de instalação é conveniente se você quiser instalar uma versão específica do Kaspersky Endpoint Security for Android.

Para instalar o Kaspersky Endpoint Security for Android usando um link ao seu próprio servidor da Web:

1. Crie um pacote de instalação e defina suas configurações.

   O *pacote de instalação* é um conjunto de arquivos criado para a instalação remota do aplicativo da Kaspersky através do Kaspersky Security Center.

2. Crie um pacote de instalação independente.

   Um *pacote de instalação independente* é o arquivo de instalação de um aplicativo móvel que contém as configurações da conexão do aplicativo ao Servidor de Administração e um indicador de aceite dos Termos e Condições do Contrato de Licença do Usuário Final (EULA) para o Kaspersky Endpoint Security for Android. É criado com base no pacote de instalação do Kaspersky Endpoint Security for Android. O pacote de instalação independente é um caso especial de um pacote de instalação.

O usuário receberá um link ao servidor da Web que hospeda o pacote de instalação independente do Kaspersky Endpoint Security for Android. Para instalar o aplicativo, o usuário deve executar o arquivo APK. A configuração adicional do Kaspersky Endpoint Security for Android após a instalação não é necessária.

Para instalar o Kaspersky Endpoint Security for Android usando um link ao seu próprio servidor da Web, a instalação de aplicativos de origens desconhecidas deve ser permitida no dispositivo móvel do usuário.

Criar e configurar um pacote de instalação

O pacote de instalação do Kaspersky Endpoint Security for Android é o arquivo comprimido de extração automática `sc_package.exe`. O arquivo comprimido inclui os arquivos necessários para instalar o aplicativo móvel nos dispositivos:

- `adb.exe`, `AdbWinApi.dll`, `AdbWinUsbApi.dll` – Conjunto de arquivos necessários para a instalação do Kaspersky Endpoint Security for Android.
- `installer.ini` – Arquivo de configuração que contém as configurações de conexão do Servidor de Administração.
- `KES10_xx_xx_xxx.apk` – Arquivo de instalação para o Kaspersky Endpoint Security for Android.
- `kmlisten.exe` – Utilitário para entrega do pacote de instalação do aplicativo através da estação de trabalho.

- `kmlisten.ini` – Arquivo de configuração que contém as configurações do utilitário de fornecimento do pacote de instalação.
- `kmlisten.kpd` – Arquivo de descrição do aplicativo.

Para criar o pacote de instalação do Kaspersky Endpoint Security for Android:

1. Na árvore do console, selecione a pasta **Adicional** → **Instalação remota** → **Pacotes de instalação**.
2. Na área de trabalho da pasta **Pacotes de Instalação**, clique no botão **Criar pacote de instalação**.

   O assistente de criação do pacote de instalação é iniciado. Siga as instruções do Assistente.
3. Na janela **Selecionar o tipo de pacote de instalação** do Assistente, clique em **Criar o pacote de instalação para o aplicativo da Kaspersky**.
4. Na janela **Definir o nome do pacote de instalação** do Assistente, insira o nome do pacote de instalação que será exibido na área de trabalho da pasta **Pacotes de instalação**.
5. Na janela **Selecionar o pacote de instalação para a instalação** do Assistente, selecione o arquivo comprimido de extração automática `sc_package.exe` incluído no kit de distribuição.

   Caso já tenha descompactado o arquivo comprimido, selecione o arquivo de descrição do aplicativo, `kmlisten.kpd`. No campo de entrada, serão exibidos o nome do aplicativo e o número da versão.
6. Na janela **Aceitar o EULA** do Assistente, leia, compreenda e aceite os termos e condições do Contrato de Licença do Usuário Final.

   É necessário aceitar os termos e condições do Contrato de Licença do Usuário Final para criar o pacote de instalação. Se você aceitar os termos do Contrato de Licença no Console de Administração, o Kaspersky Endpoint Security for Android ignorará a etapa de aceite durante a instalação do aplicativo.

   Se você decidir parar a proteção dos dispositivos móveis, é possível desinstalar o Kaspersky Endpoint Security for Android e revogar o seu Contrato de Licença do Usuário Final (EULA) do aplicativo. Para saber mais sobre a revogação do EULA, consulte a *Ajuda do Kaspersky Security Center*.

Após a conclusão do Assistente, o pacote de instalação criado aparecerá na área de trabalho da pasta **Pacotes de instalação**. Os pacotes de instalação são armazenados na pasta Pacotes, na pasta pública compartilhada no Servidor de Administração.

Para definir as configurações do pacote de instalação:

1. Na árvore do console, selecione a pasta **Adicional** → **Instalação remota** → **Pacotes de instalação**.
2. No menu de contexto do pacote de instalação do Kaspersky Endpoint Security for Android, selecione **Propriedades**.
3. Na guia **Configurações**, especifique as configurações de conexão do Servidor de Administração para dispositivos móveis e o nome do grupo de administração ao qual os dispositivos móveis serão adicionados automaticamente após a primeira sincronização com o Servidor de Administração. Siga as etapas abaixo:

   - Na seção **Conexão com o Servidor de Administração**, no campo **Endereço do servidor**, digite o nome do Servidor de Administração para dispositivos móveis no formato utilizado para instalar o **Suporte de dispositivos móveis** durante a implementação do Servidor de Administração.

     Dependendo do formato do nome do Servidor de Administração para o componente **Suporte de dispositivos móveis**, especifique o nome DNS ou o endereço IP do Servidor de Administração. No campo **Número da porta SSL**, especifique o número de abertura de porta no Servidor de Administração para conexão de dispositivos móveis. A porta 13292 é utilizada por padrão.

- Na seção **Alocação de computadores para grupos**, no campo **Nome do grupo**, digite o nome do grupo ao qual os dispositivos móveis serão adicionados após a primeira sincronização com o Servidor de Administração (**KES10** é utilizado por padrão).

  O grupo especificado será automaticamente criado na pasta **Adicional** → **Conjunto de rede** → **Domínios**.

- Na seção **Ações durante a instalação**, selecione a caixa de seleção **Solicitar endereço de e-mail**, se você deseja que o aplicativo solicite que os usuários forneçam seu endereço de e-mail corporativo quando o aplicativo for iniciado pela primeira vez.

  O endereço de e-mail do usuário é utilizado para formar o nome do dispositivo móvel quando ele é adicionado ao grupo de administração.

4. Para aplicar as configurações especificadas, clique em **Aplicar**.

Criar um pacote de instalação independente

Para criar um pacote de instalação independente, siga as etapas abaixo:

1. Na árvore do console, selecione a pasta **Adicional** → **Instalação remota** → **Pacotes de instalação**.

2. Escolha o pacote de instalação do Kaspersky Endpoint Security for Android.

3. No menu de contexto do pacote de instalação, selecione **Criar** um **pacote de instalação independente**.

   O assistente que cria o pacote de instalação independente será iniciado. Siga as instruções do Assistente.

4. Configurar as formas nas quais o pacote de instalação independente é distribuído:

   - Para distribuir o caminho para o pacote de instalação independente criado para os usuários através de e-mail, na seção **Ações adicionais** clique no link **Enviar o link para o pacote de instalação independente por e-mail**.

     A janela do editor de mensagem é aberta e o texto na janela contém o caminho para a pasta compartilhada com o pacote de instalação independente.

   - Para publicar o link no pacote de instalação independente no site corporativo, clique no link **Código HTML de exemplo para publicar link no site**.

     Isso abre um arquivo tmp com links HTML_RJL.

5. Para publicar o pacote de instalação independente criado no servidor da Web do Kaspersky Security Center e visualizar a totalidade da lista de pacotes independentes para o pacote de instalação selecionado, na janela **Assistente do pacote de instalação independente concluído com êxito** selecione a caixa **Abrir a lista de pacotes independentes**.

Após o assistente fechar, a janela **Lista de pacotes independentes para o pacote de instalação <Installation package name>** é aberta.

A janela **Lista de pacotes independentes para o pacote de instalação <Installation package name>** contém as seguintes informações:

- Uma lista de pacotes de instalação independentes;

- O caminho de rede para a pasta compartilhada no campo **Caminho**;

- O endereço do pacote independente no servidor da Web do Kaspersky Security Center no campo **URL**.

Ao enviar notificações por e-mail, é possível especificar o endereço no campo **URL** ou o caminho no campo **Caminho** como um recurso a partir do qual os usuários podem baixar o arquivo de configuração do aplicativo. Ao enviar notificações de mensagens de texto aos usuários, você deve especificar o link de download no campo **URL**.

É recomendável copiar o endereço do pacote independente criado para a área de transferência e colar o link para o pacote de instalação requerido na notificação de e-mail ou mensagem de texto para os usuários.

Definir configurações de sincronização

Para gerenciar dispositivos móveis e receber relatórios ou estatísticas de dispositivos móveis de usuários, você deve definir as configurações de sincronização. A sincronização do dispositivo móvel com o Kaspersky Security Center pode ser executada nas seguintes formas:

- **Por agendamento**. A sincronização de acordo com o agendamento é executada usando o protocolo HTTP. Você pode configurar o agendamento da sincronização nas configurações de política de grupo. As modificações nas configurações de política de grupo, os comandos e tarefas serão executadas quando o dispositivo sincronizar com o Kaspersky Security Center de acordo com o agendamento, por exemplo, com um atraso. Por padrão, os dispositivos móveis são sincronizados com o Kaspersky Security Center automaticamente a cada 6 horas.

  No Android 12 ou posterior, o aplicativo pode realizar essa tarefa após o especificado se o dispositivo estiver no modo de economia de bateria.

- **Forçada**. A sincronização forçada é executada usando as notificações push do serviço FCM (Firebase Cloud Messaging). A sincronização forçada é principalmente destinada para a entrega oportuna de comandos à um dispositivo móvel. Caso queira usar a sincronização forçada, certifique-se de que as definições de GSM estejam configuradas no Kaspersky Security Center. Para obter mais informações, consulte a Ajuda do Kaspersky Security Center.

Para definir as configurações de sincronização do dispositivo móvel com o Kaspersky Security Center:

1. No árvore do console, na pasta **Dispositivos gerenciados**, selecione o grupo de administração ao qual os dispositivos Android pertencem.
2. Na área de trabalho do grupo, selecione a guia **Políticas**.
3. Clique duas vezes em qualquer coluna para abrir a janela de propriedades da política.
4. Na janela **Propriedades** da política, selecione a seção **Sincronização**.
5. Selecione a frequência de sincronização na lista suspensa **Sincronizar**.
6. Para desativar a sincronização de um dispositivo com o Kaspersky Security Center ao estar em roaming, selecione a caixa de seleção **Não sincronizar em roaming**.

   O usuário de dispositivo pode executar manualmente a sincronização nas configurações do aplicativo (→ **Configurações** → **Sincronização** → **Sincronizar**).
7. Para ocultar as configurações de sincronização (endereço do servidor, porta e grupo de administração) do usuário nas configurações do aplicativo, desmarque a caixa de seleção **Mostrar as configurações de sincronização no dispositivo**. É impossível modificar as configurações ocultas.

8. Clique no botão **Aplicar** para salvar as alterações efetuadas.

As configurações do dispositivo móvel são definidas depois da próxima sincronização do dispositivo com o Kaspersky Security Center. Você pode sincronizar manualmente o dispositivo móvel usando um comando especial. Para saber mais sobre o trabalho com comandos de dispositivos móveis, consulte a *Ajuda do Kaspersky Security Center*.

Ativação do aplicativo Kaspersky Endpoint Security for Android

No Kaspersky Security Center, a licença pode abranger diversos grupos de recursos. Para garantir que o Kaspersky Endpoint Security for Android seja totalmente funcional, a licença do Kaspersky Security Center adquirida pela organização deve fornecer a funcionalidade de **Gerenciamento de Dispositivos Móveis**. A funcionalidade **Gerenciamento de dispositivo móvel** é destinada a conectar dispositivos móveis ao Kaspersky Security Center e gerenciá-los.

Para obter informações detalhadas sobre o licenciamento do Kaspersky Security Center e as opções de licenciamento, consulte a *Ajuda do Kaspersky Security Center*.

A ativação do aplicativo Kaspersky Endpoint Security for Android em um dispositivo móvel é feita fornecendo informações de licença válidas para o aplicativo. As informações da licença são entregues ao dispositivo móvel, junto com a política, quando o dispositivo é sincronizado com o Kaspersky Security Center.

Se a ativação do aplicativo Kaspersky Endpoint Security for Android não for concluída em 30 dias a partir do momento da instalação no dispositivo móvel, o aplicativo mudará automaticamente para o modo de funcionalidade limitada. Nesse modo, a maioria dos componentes do aplicativo são desativados. Ao mudar para o modo de funcionalidade limitada, o aplicativo para de executar a sincronização automática com o Kaspersky Security Center. Portanto, se a ativação do aplicativo não tiver sido concluída em 30 dias após a instalação, o usuário deverá sincronizar manualmente o dispositivo com o Kaspersky Security Center.

Se o Kaspersky Security Center não estiver implementado em sua organização ou não estiver acessível para dispositivos móveis, os usuários poderão ativar manualmente o aplicativo Kaspersky Endpoint Security for Android em seus dispositivos.

Para ativar o aplicativo do Kaspersky Endpoint Security for Android:

1. No árvore do console, na pasta **Dispositivos gerenciados**, selecione o grupo de administração ao qual os dispositivos Android pertencem.

2. Na área de trabalho do grupo, selecione a guia **Políticas**.

3. Clique duas vezes em qualquer coluna para abrir a janela de propriedades da política.

4. Na janela **Propriedades** da política, selecione a seção **Licenciamento**.

5. Na seção **Licenciamento**, abra a lista suspensa **Chave** e selecione a chave de ativação do aplicativo requerida no armazenamento de chave do Servidor de Administração do Kaspersky Security Center.

   Os detalhes do aplicativo para o qual a licença foi comprada são exibidos no campo abaixo.

6. Selecione a caixa de seleção **Ativar com uma chave a partir do armazenamento do Kaspersky Security Center**.

   Se o aplicativo tiver sido ativado sem uma chave armazenada no armazenamento do Kaspersky Security Center, o Kaspersky Security for Mobile substitui essa chave pela chave de ativação selecionada na lista suspensa **Chave**.

7. Para ativar o aplicativo no dispositivo móvel do usuário, bloqueie alterações às configurações.

8. Clique no botão **Aplicar** para salvar as alterações efetuadas.

   As configurações do dispositivo móvel são definidas depois da próxima sincronização do dispositivo com o Kaspersky Security Center.

Instalar um perfil de iOS MDM

Esta seção descreve os métodos para implementar perfis iOS MDM em uma rede corporativa.

Antes de implementar um perfil de iOS MDM, o administrador deve fazer o seguinte:

1. Instale um servidor de MDM do iOS.

2. Obtenha um certificado do Apple Push Notification Service da Apple (certificado de APNs).

3. Instale um certificado de APNs no servidor de MDM do iOS.

Para obter mais detalhes sobre como instalar um Servidor de MDM do iOS e trabalhar com um certificado de APNs, consulte a *Ajuda do Kaspersky Security Center*.

Para obter detalhes sobre a implementação de um perfil de iOS MDM no Kaspersky Endpoint Security Cloud, consulte a *Ajuda do Kaspersky Endpoint Security Cloud*.

Sobre os modos de gerenciamento de dispositivo iOS

Você pode implementar um sistema de gerenciamento de dispositivo iOS de vários modos diferentes. O modo de gerenciamento depende do proprietário do dispositivo móvel (pessoal ou corporativo) e dos requisitos de segurança corporativa. Você pode selecionar o modo de gerenciamento que seja o mais conveniente para a empresa, e use vários modos ao mesmo tempo.

Dispositivos não supervisionados.

Os dispositivos iOS não supervisionados são dispositivos pessoais de funcionários que são conectados ao Kaspersky Security Center. Neste modo, permite-se que o usuário use uma ID da Apple pessoal, trabalhar com qualquer aplicativo e armazenar dados pessoais no dispositivo. Você pode usar uma política de grupo do Kaspersky Device Management for iOS para configurar o acesso aos recursos corporativos, configurações de segurança e outras configurações. Por padrão, todos os dispositivos iOS são não supervisionados.

Dispositivos supervisionados

Os dispositivos iOS supervisionados são dispositivos corporativos que estão conectados ao Kaspersky Security Center. A configuração inicial do dispositivo móvel é executada no Apple Configurator. O *Apple Configurator* é um aplicativo para preparar e configurar dispositivos iOS. O Apple Configurator é instalado em um computador executando o OS X. Para obter mais detalhes sobre como trabalhar com o Apple Configurator, consulte o site de Suporte Técnico da Apple. Você pode usar uma política de grupo do Kaspersky Device Management for iOS para configuração adicional. Em dispositivos supervisionados, você pode acessar uma seleção extensa de configurações. Por exemplo, você pode configurar o Proxy HTTP Global e restrições adicionais (por exemplo, o uso bloqueado de iMessage e Centro de Jogo), e você pode bloquear modificações da conta de usuário.

Para trabalhar com dispositivos iOS supervisionados e não supervisionados, o servidor de MDM do iOS deve ter um certificado de APNs instalado, e um perfil de iOS MDM deve ser instalado nos dispositivos móveis dos usuários.

Instalar através do Kaspersky Security Center

O perfil de iOS MDM é instalado nos dispositivos móveis de usuários cujas contas de usuário foram adicionadas no Kaspersky Security Center. Para obter mais detalhes sobre as contas de usuário no Kaspersky Security Center, consulte a *Ajuda do Kaspersky Security Center*.

Para instalar um perfil de iOS MDM:

1. Na árvore do console, selecione a pasta **Gerenciamento de Dispositivos Móveis → Dispositivos móveis**.
2. Na área de trabalho da pasta **Dispositivos móveis**, clique no botão **Adicionar dispositivo móvel**.

   Isto inicia o assistente Nova conexão de dispositivo móvel. Siga as instruções do Assistente.
3. Na janela **Sistema operacional** do Assistente, selecione **iOS**.
4. Na janela **Método de proteção de dispositivo iOS MDM** do Assistente, selecione **Usar o perfil de iOS MDM do Servidor de MDM do iOS** e especifique o perfil de iOS MDM da lista.
5. Na janela **Usuários selecionados** do Assistente, selecione um ou vários usuários para a instalação do perfil de iOS MDM em seus dispositivos móveis.

   Se o usuário não estiver na lista, você pode adicionar uma nova conta de usuário sem sair do Assistente Nova conexão de dispositivo móvel.
6. Na janela **Origem do certificado** do Assistente, selecione a origem do certificado para a proteção da transferência de dados entre o dispositivo móvel e o Kaspersky Security Center:

   - **Emitir o certificado através das ferramentas do Servidor de Administração**. Neste caso, o certificado será criado automaticamente.
   - **Especifique o arquivo do certificado**. Neste caso, o seu próprio certificado deve ser preparado antes do tempo e então selecionado na janela do Assistente. Esta opção não pode ser usada se você quiser instalar o perfil MDM iOS em vários dispositivos móveis. Um certificado separado deve ser criado para cada usuário.
7. Na janela **Método de notificação ao usuário** do Assistente, selecione o canal usado para enviar o link de instalação do aplicativo:

   - Para enviar o link por e-mail, selecione **Enviar o link ao perfil de iOS MDM** e defina as configurações na seção **Por e-mail**. Assegure-se de que o endereço de e-mail esteja especificado nas configurações de contas de usuário.
   - Para enviar o link por mensagem SMS, selecione **Enviar o link ao perfil de iOS MDM** e defina as configurações na seção **Por SMS**. Assegure-se de que o número de telefone esteja especificado nas configurações de contas de usuário.
   - Para instalar o perfil de iOS MDM usando um código QR, selecione **Mostrar link para o pacote de instalação** e digitalize o código QR usando a câmera do dispositivo móvel.
   - Se nenhum dos métodos listados for conveniente para você, selecione **Mostra o link para o pacote de instalação → Copiar** para copiar o link de instalação do perfil de iOS MDM na área de transferência. Usar qualquer método disponível para entregar o link de instalação do aplicativo.
8. Conclua a utilização do novo assistente Conectar dispositivo móvel.

Após instalar o perfil de iOS MDM nos dispositivos móveis de usuários, você será capaz de definir as configurações do aplicativo usando políticas de grupo. Você também será capaz de enviar comandos aos dispositivos móveis para a proteção dos dados em caso de perda ou roubo dos dispositivos.

Em dispositivos móveis que executam iOS 12.1 ou posterior, você deve confirmar manualmente a instalação de um perfil de iOS MDM no dispositivo móvel. Você também deve conceder a permissão de gerenciamento remoto do dispositivo.

Instalar os plug-ins de administração

Para gerenciar dispositivos móveis, os seguintes plug-ins de administração devem ser instalados na estação de trabalho do administrador:

- O Plug-in de administração do Kaspersky Endpoint Security for Android oferece a interface para gerenciar dispositivos móveis e aplicativos móveis instalados neles através do Console de administração do Kaspersky Security Center.
- O plug-in de administração do Kaspersky Device Management for iOS oferece uma interface para gerenciar dispositivos móveis conectados através dos protocolos iOS MDM e Exchange ActiveSync através do Console de Administração do Kaspersky Security Center.

É possível instalar os plug-ins de administração usando os seguintes métodos:

- Instalar um plug-in de administração usando o Assistente de Início Rápido do Kaspersky Security Center.

  O aplicativo solicita que você execute o Assistente de Início Rápido automaticamente após a instalação do Servidor de Administração, na primeira conexão a ele. Também é possível iniciar o Assistente de Início Rápido manualmente a qualquer momento.

  O Assistente de Início Rápido permite aceitar os Termos e Condições do Contrato de Licença do Usuário Final (EULA) para o aplicativo do Kaspersky Endpoint Security for Android no Console de Administração. Se o administrador aceitar os termos do Contrato de Licença no Console de Administração, o Kaspersky Endpoint Security for Android ignorará a etapa de aceite durante a instalação do aplicativo. Para obter mais detalhes sobre o Assistente de Início Rápido do Kaspersky Security Center, consulte a *Ajuda do Kaspersky Security Center*.

- Instalar o plug-in de administração usando a lista de pacotes de distribuição disponíveis no Console de Administração do Kaspersky Security Center.

  A lista de pacotes de distribuição disponíveis é atualizada automaticamente depois que novas versões dos aplicativos da Kaspersky são lançadas.

- Baixar o pacote de distribuição de uma fonte externa e instalar o plug-in de administração usando o arquivo EXE.

  Por exemplo, o pacote de distribuição do plug-in de administração pode ser baixado no site da Kaspersky.

Instalar plug-ins de administração da lista no Console de Administração

Para instalar os plug-ins de administração:

1. Na árvore do console, selecione **Avançado** → **Instalação remota** → **Pacotes de instalação**.

2. Na área de trabalho, selecione **Ações adicionais → Exibir versões atuais dos aplicativos da Kaspersky**.

   Isso abrirá a lista de versões atualizadas dos aplicativos da Kaspersky.

3. Na seção **Dispositivos Móveis**, selecione o plug-in do **Kaspersky Endpoint Security for Android** ou do **Kaspersky Device Management for iOS**.

4. Clique no botão **Baixar pacotes de distribuição**.

   Um pacote de distribuição de plug-in será baixado para a memória do computador (arquivo EXE).

5. Execute o arquivo EXE e siga as instruções do Assistente de Instalação.

Instalação do plug-in de administração a partir do pacote de distribuição

Para instalar o Plug-in de administração do Kaspersky Endpoint Security for Android,

Copie o arquivo de instalação do plug-in `klcfinst.exe` do pacote de distribuição da solução integrada e execute-o na estação de trabalho do administrador.

A instalação é executada pelo Assistente e não será necessário definir as configurações.

Para instalar o plug-in de administração do Kaspersky Device Management for iOS,

Copie o arquivo de instalação do plug-in `klmdminst.exe` do pacote de distribuição da solução integrada e execute-o na estação de trabalho do administrador.

A instalação é executada pelo Assistente e não será necessário definir as configurações.

É possível certificar-se de que o plug-in de administração esteja instalado visualizando a lista de plug-ins de administração do aplicativo instalado na janela Propriedades do Servidor de Administração na seção **Avançado → Detalhes sobre os plug-ins de gerenciamento instalados**.

Atualizar uma versão anterior do aplicativo

A atualização do aplicativo deve atender os seguintes requisitos:

- A versão do plug-in de administração do Kaspersky Endpoint Security e a versão do aplicativo móvel Kaspersky Endpoint Security for Android deve coincidir.

  Você pode exibir os números de compilação das versões do plug-in de administração e do aplicativo móvel nas Notas de Versão do Kaspersky Security for Mobile.

- Assegure-se de que o Kaspersky Security Center satisfaz os requisitos de software do Kaspersky Security for Mobile.

- Os plug-ins de administração do Kaspersky Endpoint Security 10.0 Service Pack 2 (Compilação 10.6.0.1801) e do Kaspersky Device Management for iOS 10.0 Service Pack 2 (Compilação 10.6.0.1767) e versões posteriores podem ser automaticamente ser atualizados para a versão atual. As atualizações de versões anteriores de plug-ins de administração não são suportadas.

  Para atualizar os plug-ins de administração de versões anteriores, você deve remover os plug-ins de administração instalados e as políticas de grupo que foram criadas com eles. Então, instale as novas versões dos plug-ins de administração. Para obter detalhes sobre a remoção de plug-ins de administração, visite o *site de Suporte Técnico da Kaspersky*.

- Use a mesma versão do Kaspersky Endpoint Security for Android em todos os dispositivos móveis da organização.

Os termos e condições de Suporte Técnico para versões do Kaspersky Security for Mobile estão disponíveis no *site de Suporte Técnico da Kaspersky*.

Para exibir a versão e o número da compilação de plug-ins de administração:

1. Na árvore do console no menu de contexto do Servidor de Administração, selecione **Propriedades**.
2. Na janela de propriedades do Servidor de Administração, selecione **Avançado** → **Detalhes sobre os plug-ins de gerenciamento instalados**.

   A área de trabalho exibe as informações sobre plug-ins de administração instalados no formato `<Plug-in name> <Version> <Build>`.

Você pode exibir a versão e o número da compilação do aplicativo Kaspersky Endpoint Security for Android usando os seguintes métodos:

- Se o Kaspersky Endpoint Security for Android foi instalado com um pacote de instalação independente, você pode exibir a versão e o número da compilação do aplicativo nas propriedades do pacote.
- Se Kaspersky Endpoint Security for Android foi instalado através do Google Play, você pode exibir o número da compilação nas configurações do aplicativo (→ **Sobre o aplicativo**).

Atualizar a versão anterior do Kaspersky Endpoint Security for Android

O Kaspersky Endpoint Security for Android pode ser atualizado nas seguintes formas:

- Usando o Google Play. O dispositivo móvel do usuário efetua o download da nova versão do aplicativos através do Google Play e a instala no dispositivo.
- Utilizando o Kaspersky Security Center. Você pode atualizar remotamente a versão do aplicativo em seu dispositivo usando o sistema de administração remota do Kaspersky Security Center.

Você pode selecionar o método de atualização do aplicativo que for o mais conveniente para a sua organização. Você pode usar somente um método de atualização.

Atualizar o aplicativo através do Google Play

O aplicativo pode ser atualizado a partir do Google Play seguindo o procedimento de atualização padrão para a plataforma Android. As seguintes condições devem ser atendidas para que o aplicativo seja atualizado:

- O usuário do dispositivo deve ter uma conta do Google.
- O dispositivo deve estar vinculado com a conta do Google.
- O dispositivo deve estar conectado à Internet.

Após baixar o aplicativo no Google Play, o Kaspersky Endpoint Security for Android verifica os Termos e Condições do Contrato de Licença do Usuário Final (EULA). Caso os termos do EULA tenham sido atualizados, o aplicativo envia uma solicitação para o Kaspersky Security Center. Se o administrador aceitar o EULA no Console de Administração, o Kaspersky Endpoint Security for Android ignorará a etapa de aceite durante a instalação do aplicativo. Caso o administrador use uma versão desatualizada do plug-in de administração, o Kaspersky Security Center solicita que você o atualize. Ao atualizar o plug-in de administração, o administrador pode aceitar os termos do EULA para o Kaspersky Endpoint Security for Android no Console de Administração.

É possível atualizar o aplicativo através do Google Play se o Kaspersky Endpoint Security for Android tiver sido instalado a partir dele. Se o aplicativo tiver sido instalado usando outro método, não será possível pode atualizá-lo através do Google Play.

Atualização do aplicativo através do Kaspersky Security Center

O Kaspersky Endpoint Security for Android pode ser atualizado usando o Kaspersky Security Center após a aplicação de uma política de grupo. Nas configurações da política de grupo, é possível selecionar o pacote de instalação independente do Kaspersky Endpoint Security for Android da versão que atenda a seus requisitos de segurança corporativa.

Você pode atualizar por meio do Kaspersky Security Center se o Kaspersky Endpoint Security for Android tiver sido instalado via Kaspersky Security Center. Se o aplicativo foi instalado a partir do Google Play, você não pode atualizar o aplicativo através do Kaspersky Security Center.

Para atualizar o Kaspersky Endpoint Security for Android usando um pacote de instalação independente, a instalação de aplicativos de origens desconhecidas deve ser permitida no dispositivo móvel do usuário. Para obter detalhes sobre a instalação de aplicativos sem o Google Play, consulte o *Guia de Ajuda do Android*.

Para atualizar a versão do aplicativo:

1. No árvore do console, na pasta **Dispositivos gerenciados**, selecione o grupo de administração ao qual os dispositivos Android pertencem.
2. Na área de trabalho do grupo, selecione a guia **Políticas**.
3. Clique duas vezes em qualquer coluna para abrir a janela de propriedades da política.
4. Na janela **Propriedades** da política, selecione a seção **Adicional**.
5. Na seção **Atualizando o Kaspersky Endpoint Security for Android**, clique no botão **Selecionar...**.

   Isto abre a janela **Atualizando o Kaspersky Endpoint Security for Android**.
6. Na lista de pacotes de instalação independente do Kaspersky Endpoint Security, selecione o pacote cuja versão atende os requisitos de segurança corporativa.

   Você pode efetuar uma atualização do Kaspersky Endpoint Security somente para uma versão mais recente do aplicativo. O Kaspersky Endpoint Security não pode ser atualizado para versão mais antiga do aplicativo.
7. Clique no botão **Selecionar**.

Uma descrição do pacote de instalação selecionado é exibida na seção **Atualizando o Kaspersky Endpoint Security for Android**.

8. Clique no botão **Aplicar** para salvar as alterações efetuadas.

As configurações do dispositivo móvel são definidas depois da próxima sincronização do dispositivo com o Kaspersky Security Center. O usuário do dispositivo móvel é solicitado a instalar a nova versão do aplicativo. Depois que o usuário der o consentimento, a nova versão do aplicativo será instalada no dispositivo móvel.

Instalar uma versão anterior do Kaspersky Endpoint Security for Android

Se desejar prevenir a atualização automática do aplicativo e usar uma versão específica do Kaspersky Endpoint Security for Android, desative a atualização automática do aplicativo nas configurações do Google Play. Para obter mais detalhes, consulte o site de suporte técnico da Google.

A atualização automática do Kaspersky Endpoint Security for Android só está disponível se o aplicativo foi instalado a partir do Google Play ou do Kaspersky Security Center usando o link do Google Play. Se o aplicativo foi instalado pelo Kaspersky Security Center usando um link para seu próprio servidor Web (usando o pacote de instalação independente), a atualização automática não está disponível. Neste caso, você pode usar uma política de grupo para atualizar manualmente o Kaspersky Endpoint Security for Android.

Para instalar uma versão anterior do Kaspersky Endpoint Security for Android:

1. Remover o Kaspersky Endpoint Security for Android dos dispositivos móveis dos usuários.

2. Instalar o Kaspersky Endpoint Security for Android pelo Kaspersky Security Center usando um link para seu próprio servidor Web. Para isso, você precisará do pacote de instalação da versão específica. Você pode baixar o pacote de distribuição de versões anteriores do Kaspersky Endpoint Security for Android no site de Suporte técnico da Kaspersky.

Para mais informações sobre versões anteriores do Kaspersky Endpoint Security for Android, consulte a *Ajuda da versão apropriada do Kaspersky Security for Mobile*.

Atualizar das versões anteriores de plug-ins de administração

É possível atualizar plug-ins de administração usando os seguintes métodos:

- Instalar a nova versão do plug-in de administração a partir da lista de pacotes de distribuição disponíveis no Console de Administração do Kaspersky Security Center.

  A lista de pacotes de distribuição disponíveis é atualizada automaticamente depois que novas versões dos aplicativos da Kaspersky são lançadas.

- Baixar o pacote de distribuição de uma fonte externa e instalar a nova versão do plug-in de administração usando o arquivo EXE.

  Para atualizar os plug-ins de administração do Kaspersky Endpoint Security for Android e do Kaspersky Device Management for iOS, você deve baixar a versão mais recente do aplicativo a partir da página da Web do Kaspersky Security for Mobile e executar o Assistente de configuração para cada um dos dois plug-ins. As versões anteriores dos plug-ins são removidas automaticamente durante a operação do Assistente de Instalação.

Os especialistas da Kaspersky recomendam usar a mesma versão do aplicativo e dos plug-ins de administração. Se o usuário atualizar o aplicativo a partir do Google Play, o Kaspersky Security Center mostrará uma notificação solicitando a atualização do plug-in de administração.

Os plug-ins de administração são atualizados, os grupos de administração existentes na pasta **Dispositivos gerenciados** e as regras para a atribuição automática de dispositivos da pasta **Dispositivos não atribuídos** para esses grupos são salvos. As políticas de grupo existentes para dispositivos móveis são também salvas. Novas configurações de política que implementam as novas funções da solução integrada Kaspersky Security for Mobile serão adicionadas às políticas existentes e assumirão os valores padrão.

Se as novas configurações foram adicionadas ou os valores padrões foram modificados na nova versão do plug-in de administração, as modificações somente serão aplicadas após que uma política de grupo for aberta. Até que o administrador abra uma política de grupo, as configurações da versão anterior do plug-in serão aplicadas nos dispositivos móveis mesmo se a versão do plug-in tiver sido atualizada.

Atualização a partir da lista no Console de Administração

Para atualizar os plug-ins de administração:

1. Na árvore do console, selecione **Avançado → Instalação remota → Pacotes de instalação**.
2. Na área de trabalho, selecione **Ações adicionais → Exibir versões atuais dos aplicativos da Kaspersky**.

   Isso abrirá a lista de versões atualizadas dos aplicativos da Kaspersky.
3. Na seção **Dispositivos Móveis**, selecione o plug-in do **Kaspersky Endpoint Security for Android** ou do **Kaspersky Device Management for iOS**.
4. Clique no botão **Baixar pacotes de distribuição**.

   Um pacote de distribuição de plug-in será baixado para a memória do computador (arquivo EXE). Execute o arquivo EXE. Siga as instruções do Assistente de Instalação.

Atualização a partir do pacote de distribuição

Para atualizar o Plug-in de administração do Kaspersky Endpoint Security for Android,

Copie o arquivo de instalação do plug-in `klcfinst.exe` do pacote de distribuição da solução integrada e execute-o na estação de trabalho do administrador.

A instalação é executada pelo Assistente e não será necessário definir as configurações.

Para atualizar o Plug-in de administração do Kaspersky Device Management for iOS,

Copie o arquivo de instalação do plug-in `klmdminst.exe` do pacote de distribuição da solução integrada e execute-o na estação de trabalho do administrador.

A instalação do plug-in é executada pelo Assistente e não será necessário definir as configurações.

É possível certificar-se de que os plug-ins de administração estejam atualizados visualizando a lista de plug-ins de administração do aplicativo instalados na janela de propriedades do Servidor de Administração, na seção **Avançado → Detalhes sobre os plug-ins de gerenciamento de aplicativos instalados**.

Remoção do Kaspersky Endpoint Security for Android

O Kaspersky Endpoint Security for Android pode ser removido das seguintes formas:

1. Remoção do aplicativo pelo usuário

   O usuário remove manualmente o Kaspersky Endpoint Security for Android usando a interface do aplicativo. Para que os usuários possam remover o aplicativo, a remoção do aplicativo deve ser permitida na política aplicada ao dispositivo.

2. Remoção do aplicativo pelo administrador

   O administrador remove o aplicativo remotamente usando o Console de administração do Kaspersky Security Center. O aplicativo pode ser removido de um determinado dispositivo ou de diversos dispositivos ao mesmo tempo.

Remoção remota do aplicativo

Você pode remover o Kaspersky Endpoint Security for Android dos dispositivos móveis de usuários remotamente nas seguintes maneiras:

- Usar uma política de grupo. Este método é conveniente se você desejar remover o aplicativos de diversos dispositivos de uma só vez.
- Ao definir as configurações do aplicativo local. Este método é conveniente se você desejar remover o aplicativo de uma determinado dispositivo.

Para remover o aplicativo ao aplicar uma política de grupo:

1. No árvore do console, na pasta **Dispositivos gerenciados**, selecione o grupo de administração ao qual os dispositivos Android pertencem.
2. Na área de trabalho do grupo, selecione a guia **Políticas**.
3. Clique duas vezes em qualquer coluna para abrir a janela de propriedades da política.
4. Na janela **Propriedades** da política, selecione a seção **Adicional**.
5. Na seção **Desinstalar o Kaspersky Endpoint Security for Android**, selecione a caixa de seleção **Desinstalar o Kaspersky Endpoint Security for Android do dispositivo**.
6. Clique no botão **Aplicar** para salvar as alterações efetuadas.

Como resultado, o Kaspersky Endpoint Security for Android é removido dos dispositivos móveis depois da sincronização com o Servidor de Administração. Os usuários de dispositivos móveis recebem uma notificação de que o aplicativo foi removido.

Para remover o aplicativo ao definir as configurações locais:

1. Na árvore do console, selecione **Gerenciamento de dispositivo móvel → Dispositivos móveis**.
2. Na lista de dispositivos, selecione o dispositivo do qual você desejar remover o aplicativo.
3. Clique duas vezes para abrir a janela Propriedades do dispositivo.
4. Selecione **Aplicativos → Kaspersky Endpoint Security for Android**.
5. Abra a janela Propriedades do Kaspersky Endpoint Security ao clicar duas vezes.
6. Selecione a seção **Adicional**.
7. Na seção **Remoção do Kaspersky Endpoint Security for Android**, selecione a caixa de seleção **Desinstalar o Kaspersky Endpoint Security for Android do dispositivo**.
8. Clique no botão **Aplicar** para salvar as alterações efetuadas.

Como resultado, o Kaspersky Endpoint Security for Android é removido do dispositivo móvel após a sincronização com o Servidor de Administração. O usuário do dispositivo móvel recebe uma notificação de que o aplicativo foi removido.

Permissão para os usuários removerem o aplicativo

Para proteger o aplicativo da remoção em dispositivos que executam o Android 7.0 ou posterior, o Kaspersky Endpoint Security for Android deve ser definido como um recurso de Acessibilidade. Quando o assistente Configuração inicial estiver sendo executado, o Kaspersky Endpoint Security for Android solicita ao usuário conceder ao aplicativo todas as permissões necessárias. O usuário pode ignorar estas etapas ou desativar estas permissões nas configurações de dispositivo em um momento posterior. Se este for o caso, o aplicativo não é protegido contra a remoção.

Você pode permitir que os usuários removam o Kaspersky Endpoint Security for Android dos seus dispositivos móveis nas seguintes maneiras:

- Usar uma política de grupo. Este método é conveniente se você desejar permitir que os usuários possam remover o aplicativo de diversos dispositivos de uma só vez.
- Usar configurações do aplicativo local. Este método é conveniente se você desejar permitir que o usuário de um determinado dispositivo possa remover o aplicativo.

Para permitir a remoção do aplicativo em uma política de grupo:

1. No árvore do console, na pasta **Dispositivos gerenciados**, selecione o grupo de administração ao qual os dispositivos Android pertencem.
2. Na área de trabalho do grupo, selecione a guia **Políticas**.
3. Clique duas vezes em qualquer coluna para abrir a janela de propriedades da política.
4. Na janela **Propriedades** da política, selecione a seção **Adicional**.
5. Na seção **Remoção do Kaspersky Endpoint Security for Android**, defina a caixa de seleção **Permitir a remoção do Kaspersky Endpoint Security for Android**.
6. Clique no botão **Aplicar** para salvar as alterações efetuadas.

Como resultado, a remoção do aplicativo pelo usuário do dispositivo móvel é permitida após a sincronização com o Servidor de Administração. O botão de remoção do aplicativo se torna disponível nas configurações do Kaspersky Endpoint Security for Android.

Para permitir a remoção do aplicativo nas configurações do aplicativo local:

1. Na árvore do console, selecione **Adicional** → **Gerenciamento de dispositivo móvel** → **Dispositivos móveis**.
2. Na lista de dispositivos, selecione o dispositivo do qual você deseja permitir a remoção do aplicativo pelo usuário.
3. Clique duas vezes para abrir a janela Propriedades do dispositivo.
4. Selecione **Aplicativos** → **Kaspersky Endpoint Security for Mobile**.
5. Abra a janela Propriedades do Kaspersky Endpoint Security ao clicar duas vezes.
6. Selecione a seção **Adicional**.
7. Na seção **Remoção do Kaspersky Endpoint Security for Android**, defina a caixa de seleção **Permitir a remoção do Kaspersky Endpoint Security for Android**.
8. Clique no botão **Aplicar** para salvar as alterações efetuadas.

Como resultado, a remoção do aplicativo pelo usuário do dispositivo móvel é permitida após a sincronização com o Servidor de Administração. O botão de remoção do aplicativo se torna disponível nas configurações do Kaspersky Endpoint Security for Android.

Remoção do aplicativo pelo usuário

Para remover de forma independente o Kaspersky Endpoint Security for Android de um dispositivo móvel, o usuário deve de fazer o seguinte:

1. Na janela principal do Kaspersky Endpoint Security for Android, toque em ☰ → **Desinstalar o aplicativo**.

   É exibido uma solicitação de confirmação na tela.

   Se o botão **Desinstalar o aplicativo** estiver ausente, isto significa que o administrador ativou a proteção contra a remoção do Kaspersky Endpoint Security for Android.
2. Confirme a remoção do Kaspersky Endpoint Security for Android.

O aplicativo Kaspersky Endpoint Security for Android será removido do dispositivo móvel do usuário.

Configuração e Gerenciamento

Esta seção da Ajuda é destinada para especialistas que administram o Kaspersky Security for Mobile, assim como para especialistas que fornecem o Suporte Técnico às organizações que usam o Kaspersky Security for Mobile.

Guia de Introdução

Esta seção descreve as ações recomendadas ao começar a usar o Kaspersky Security for Mobile.

Iniciar e parar o aplicativo

O Kaspersky Security Center é automaticamente iniciado e para os plug-ins de administração do Kaspersky Endpoint Security e do Kaspersky Device Management for iOS.

O Kaspersky Endpoint Security for Android será iniciado quando o sistema operacional inicia e protege o dispositivo móvel durante toda a sessão. O usuário pode parar o aplicativo desativando todos os componentes do Kaspersky Endpoint Security for Android. Você pode usar as políticas de grupo para configurar as permissões do usuário para gerenciar componentes do aplicativo.

Em determinados dispositivos (por exemplo, Huawei, Meizu e Xiaomi), você deve adicionar manualmente o Kaspersky Endpoint Security for Android na lista de aplicativos que são iniciados quando o sistema operacional inicia (**Segurança** → **Permissões** → **Execução automática**). Se o aplicativo não for adicionado à lista, o Kaspersky Endpoint Security for Android para a execução de todas as suas funções após a reinicialização do dispositivo móvel.

Você também deve desativar o modo de Economia de bateria para o Kaspersky Endpoint Security for Android. Isto é necessário para que o aplicativo seja executado em segundo plano, tal como executar uma verificação de vírus agendada ou sincronizar o dispositivo com o Kaspersky Security Center. Este problema é atribuível aos recursos específicos do software incorporado destes dispositivos.

Criação de um grupo de administração

Para executar a configuração centralizada do aplicativo do Kaspersky Endpoint Security for Android instalado nos dispositivos móveis dos usuários, as políticas de grupo devem ser aplicadas aos dispositivos.

Para aplicar a política a um grupo de dispositivos, recomenda-se criar um grupo separado para esses dispositivos na pasta **Dispositivos gerenciados** antes de instalar os aplicativos móveis nos dispositivos dos usuários.

Após criar um grupo de administração, recomenda-se configurar a opção de alocar automaticamente dispositivos nos quais deseja instalar os aplicativos para esse grupo. Em seguida, defina as configurações que são comuns a todos os dispositivos usando uma política do grupo.

Para criar um grupo de administração, siga as etapas abaixo:

1. Na árvore do console, selecione a pasta **Dispositivos gerenciados**.
2. Na área de trabalho da pasta **Dispositivos gerenciados** ou de sua subpasta, selecione a guia **Dispositivos**.
3. Clique no botão **Novo grupo**.
   Isto abre a janela na qual você pode criar um novo grupo.
4. Na janela **Nome do grupo** digite o nome do grupo e clique em **OK**.

Uma nova pasta de grupo de administração com o nome especificado é exibida na árvore de console. Para obter informações mais detalhadas sobre a utilização de grupos de administração, consulte a *Ajuda do Kaspersky Security Center*.

Políticas de grupo para gerenciar dispositivos móveis

Uma *política do grupo* é um pacote de configurações para gerenciar dispositivos móveis que pertencem a um grupo de administração e para gerenciar aplicativos móveis instalados nos dispositivos. Você pode criar uma política do grupo usando o Assistente de Políticas.

Você pode usar uma política para definir as configurações de dispositivos individuais como de um grupo de dispositivos. Para um grupo de dispositivos, as configurações de administração podem ser especificadas na janela de propriedades de política do grupo. Para um único dispositivo, elas podem ser especificadas na janela de configurações locais do aplicativo. As configurações individuais de gerenciamento especificadas para um dispositivo podem ser diferentes dos valores de configurações especificadas na política para um grupo ao qual esse dispositivo pertence.

Cada parâmetro representado em uma política tem um atributo de "bloqueio", que mostra se a configuração pode ser modificada nas políticas de níveis de hierarquia inclusos (para grupos inclusos e Servidores de Administração escravos), nas configurações locais do aplicativo.

Os valores de configurações definidos na política e nas configurações locais do aplicativo são salvos no Servidor de Administração, distribuídos para dispositivos móveis durante a sincronização e salvos em dispositivos como configurações atuais. Se o usuário tiver especificado outros valores de configurações que não foram "bloqueadas", durante a próxima sincronização do dispositivo com o Servidor de Administração os novos valores de configurações são enviados para o Servidor de Administração e salvos nas configurações locais do aplicativo em vez dos valores que foram anteriormente especificados pelo administrador.

Para manter a segurança corporativa de dispositivos móveis atualizada, você pode monitorar os dispositivos de usuários quanto à conformidade com a política de gerenciamento de grupo.

O indicador de nível de proteção é exibido na parte superior da janela de política de grupo. O indicador do nível de proteção irá ajudá-lo a configurar a política para assegurar um alto nível de proteção do dispositivo. O status do indicador do nível de proteção modifica-se dependendo das configurações da política:

- **Alto nível de proteção** – um nível apropriado da proteção do dispositivo é fornecido. Todos os componentes de proteção funcionam de acordo com as configurações recomendadas pela Kaspersky.
- **Nível médio de proteção** – o nível de proteção é menor do que o recomendado. Alguns componentes de proteção críticos são desativados (por exemplo, Proteção na Web). Os problemas importantes são marcados com o ícone .
- **Baixo nível de proteção** – existem problemas que podem levar à infecção do dispositivo e à perda de dados. Alguns componentes de proteção críticos são desativados (por exemplo, a proteção em tempo real de dispositivos é desativada). Os problemas Críticos são marcados com o ícone .

Para obter mais detalhes sobre o gerenciamento de políticas e grupos de administração no Console de Administração do Kaspersky Security Center, consulte a *Ajuda do Kaspersky Security Center*.

Criar uma política do grupo

Esta seção descreve o processo de criação de políticas de grupo para dispositivos nos quais o aplicativo móvel do Kaspersky Endpoint Security for Android estiver instalado e as políticas para dispositivos EAS e iOS MDM.

As políticas criadas para um grupo de administração são mostradas na área de trabalho de grupo no Console de administração do Kaspersky Security Center na guia **Políticas**. O ícone que indica o status de política (ativa/inativa) aparece antes do nome da política. É possível criar várias políticas para diferentes aplicativos em um grupo. Somente uma política para cada aplicativo pode estar ativa. Quando uma nova política ativa é criada, a política ativa anterior torna-se inativa.

É possível modificar uma política após sua criação.

Para criar uma política para gerenciar dispositivos móveis:

1. Na árvore do console, selecione um grupo de administração para o qual você deseja criar uma política.
2. Na área de trabalho do grupo, selecione a guia **Políticas**.
3. Clique no link **Criar política** para iniciar o Assistente de Política.

   Isso inicia o Assistente de política.

Etapa 1. Escolher um aplicativo para criar uma política de grupo

Nessa etapa, selecione o aplicativo para o qual você deseja criar uma política do grupo na lista de aplicativos:

- **Kaspersky Endpoint Security for Android** – para dispositivos que usam o aplicativo móvel do Kaspersky Endpoint Security for Android.

Recomenda-se a criação de uma política separada para os dispositivos Huawei e Honor que não tenham os serviços Google play. Assim, é possível enviar links para os usuários do Huawei AppGallery que usam esses dispositivos.

- **Kaspersky Device Management for iOS** – para dispositivos EAS e dispositivos iOS MDM.

Uma política para dispositivos móveis pode ser criada se o plug-in de administração do Kaspersky Endpoint Security for Android e o plug-in de administração do Kaspersky Device Management for iOS estiverem instalados no desktop do administrador. Se os plug-ins não estiverem instalados, o nome do aplicativo relevante não é exibido na lista de aplicativos.

Prossiga para a próxima etapa do Assistente de política.

Etapa 2. Inserir um nome para a política de grupo

Nessa etapa, digite o nome da nova política no campo **Nome**. Se você especificar o nome de uma política existente, será adicionado (1) automaticamente no final.

Prossiga para a próxima etapa do Assistente de política.

Etapa 3. Criar uma política de grupo par ao aplicativo

Nesta etapa, o Assistente solicita a seleção do status da política:

- **Ativar política**. O Assistente salva a política criada no Servidor de Administração. Na próxima sincronização do dispositivo móvel com o Servidor de Administração, a política será usada no dispositivo como a política ativa.

- **Política inativa.** O Assistente salva a política criada no Servidor de Administração como política de backup. Essa política pode ser ativada no futuro após um evento específico. Se necessário, uma política inativa pode ser mudada para o estado ativo.

  Diversas políticas podem ser criadas para um aplicativo no grupo, mas somente uma pode estar ativa. Quando uma nova política ativa é criada, a política ativa anterior torna-se automaticamente inativa.

Saia do Assistente.

Definir configurações de sincronização

Para gerenciar dispositivos móveis e receber relatórios ou estatísticas de dispositivos móveis de usuários, você deve definir as configurações de sincronização. A sincronização do dispositivo móvel com o Kaspersky Security Center pode ser executada nas seguintes formas:

- **Por agendamento**. A sincronização de acordo com o agendamento é executada usando o protocolo HTTP. Você pode configurar o agendamento da sincronização nas configurações de política de grupo. As modificações nas configurações de política de grupo, os comandos e tarefas serão executadas quando o dispositivo sincronizar com o Kaspersky Security Center de acordo com o agendamento, por exemplo, com um atraso. Por padrão, os dispositivos móveis são sincronizados com o Kaspersky Security Center automaticamente a cada 6 horas.

  No Android 12 ou posterior, o aplicativo pode realizar essa tarefa após o especificado se o dispositivo estiver no modo de economia de bateria.

- **Forçada**. A sincronização forçada é executada usando as notificações push do serviço FCM (Firebase Cloud Messaging). A sincronização forçada é principalmente destinada para a entrega oportuna de comandos à um dispositivo móvel. Caso queira usar a sincronização forçada, certifique-se de que as definições de GSM estejam configuradas no Kaspersky Security Center. Para obter mais informações, consulte a Ajuda do Kaspersky Security Center.

Para definir as configurações de sincronização do dispositivo móvel com o Kaspersky Security Center:

1. No árvore do console, na pasta **Dispositivos gerenciados**, selecione o grupo de administração ao qual os dispositivos Android pertencem.

2. Na área de trabalho do grupo, selecione a guia **Políticas**.

3. Clique duas vezes em qualquer coluna para abrir a janela de propriedades da política.

4. Na janela **Propriedades** da política, selecione a seção **Sincronização**.

5. Selecione a frequência de sincronização na lista suspensa **Sincronizar**.

6. Para desativar a sincronização de um dispositivo com o Kaspersky Security Center ao estar em roaming, selecione a caixa de seleção **Não sincronizar em roaming**.

   O usuário de dispositivo pode executar manualmente a sincronização nas configurações do aplicativo (→ **Configurações** → **Sincronização** → **Sincronizar**).

7. Para ocultar as configurações de sincronização (endereço do servidor, porta e grupo de administração) do usuário nas configurações do aplicativo, desmarque a caixa de seleção **Mostrar as configurações de sincronização no dispositivo**. É impossível modificar as configurações ocultas.

8. Clique no botão **Aplicar** para salvar as alterações efetuadas.

As configurações do dispositivo móvel são definidas depois da próxima sincronização do dispositivo com o Kaspersky Security Center. Você pode sincronizar manualmente o dispositivo móvel usando um comando especial. Para saber mais sobre o trabalho com comandos de dispositivos móveis, consulte a *Ajuda do Kaspersky Security Center*.

Gerenciar as revisões em políticas de grupo

O Kaspersky Security Center lhe permite acompanhar as modificações da política de grupo. Cada vez que você salva as modificações feitas em uma política de grupo, uma *revisão* é criada. Cada revisão tem um número.

Você pode gerenciar as revisões somente para as políticas do Kaspersky Endpoint Security for Android. Você não pode gerenciar as revisões para uma política do Kaspersky Device Management for iOS.

Você pode executar as seguintes ações nas revisões da política de grupo:

- Comparar uma revisão selecionada à atual
- Comparar as revisões selecionadas
- Comparar uma política com uma revisão selecionada de outra política
- Exibir uma revisão selecionada
- Reverter as mudanças da política para uma revisão selecionada
- Salvar as revisões como um arquivo .txt

Para obter mais detalhes sobre o gerenciamento de revisões de políticas de grupo e outros objetos (por exemplo, contas de usuário), consulte a *Ajuda do Kaspersky Security Center*.

Para exibir o histórico das revisões de política de grupo:

1. No árvore do console, na pasta **Dispositivos gerenciados**, selecione o grupo de administração ao qual os dispositivos Android pertencem.

2. Na área de trabalho do grupo, selecione a guia **Políticas**.

3. Clique duas vezes em qualquer coluna para abrir a janela de propriedades da política.

4. Na janela **Propriedades** da política, selecione a seção **Histórico de revisões**.

   Uma lista de revisões de política é exibida. Ela contém as seguintes informações:

   - Número da revisão da política
   - Data e hora em que política foi modificada
   - O nome do usuário que modificou a política

- A ação executada na política
- Descrição da revisão feita nas configurações da política

Remover um política do grupo

Para remover uma política do grupo:

1. Na árvore do console, selecione um grupo de administração para o qual você deseja remover uma política.
2. Na área de trabalho do grupo de administração da guia **Políticas**, selecione a política que você deseja remover.
3. No menu de contexto da política, selecione **Excluir**.

   Como resultado, a política do grupo é excluída. Antes de aplicar a nova política do grupo, os dispositivos móveis que pertencem ao grupo de administração continuam a funcionar com as configurações especificadas na política que foi excluída.

Restringir permissões para configurar políticas de grupo

Os administradores do Kaspersky Security Center podem configurar as permissões de acesso de usuários ao Console de Administração para diferentes funções da solução integrada Kaspersky Security for Mobile, dependendo das obrigações de trabalho dos usuários.

Na interface do Console de Administração, você pode configurar direitos de acesso na janela de propriedades do Servidor de Administração nas guias **Segurança** e **Funções do usuário**. A guia **Funções do usuário** permite que você adicione funções de usuário padrão com um conjunto predefinido de direitos. A seção **Segurança** permite que você configure direitos para um usuário ou grupo de usuários ou que atribua funções a um usuário ou a um grupo de usuários. Os direitos do usuário para cada aplicativo são configurados de acordo com *escopos funcionais*.

Você também pode configurar permissões de usuário específicas para as áreas funcionais. As informações sobre a correspondência entre áreas funcionais e as guias de política são fornecidas no Anexo.

Para cada área funcional, o administrador pode atribuir as seguintes permissões:

- **Permitir editar**. O usuário do Console de Administração está autorizado a alterar as configurações da política na janela de propriedades.
- **Bloquear a edição**. O usuário do Console de Administração está proibido de alterar as configurações da política na janela de propriedades. As guias de política que pertencem ao escopo funcional para o qual esse direito foi atribuído não são exibidas na interface.

Para obter mais detalhes sobre o gerenciamento de direitos do usuário e funções no Console de Administração do Kaspersky Security Center, consulte a *Ajuda do Kaspersky Security Center*.

Proteção

Esta seção contém informações sobre como gerenciar remotamente a proteção de dispositivos móveis no Console de Administração do Kaspersky Security Center.

Configurar a proteção antivírus em dispositivos Android

Para a detecção oportuna de ameaças, vírus e outros aplicativos maliciosos, você deve definir as configurações de proteção em tempo real e execução automática de verificações de vírus.

O Kaspersky Endpoint Security for Android detecta os seguintes tipos de objetos:

- Vírus, worms, Cavalos de Troia e ferramentas maliciosas
- Adware
- Aplicativo que pode ser explorado por criminosos para danificar o dispositivo ou os dados pessoais

O antivírus tem um número de limitações:

- Quando o Antivírus está sendo executado, uma ameaça detectada na memória externa do dispositivo (tal como um cartão SD) não pode ser neutralizada automaticamente no perfil para Trabalho (Aplicativos com o ícone de maleta, Configurar o perfil Android para o trabalho). O Kaspersky Endpoint Security for Android não tem acesso à memória externa no perfil para Trabalho. As informações sobre os objetos detectados são exibidas na seção **Status** do aplicativo. Para neutralizar objetos detectados na memória externa, os arquivos do objeto têm de ser excluídos manualmente e a verificação do dispositivo reiniciada.
- Devido às limitações técnicas, o Kaspersky Endpoint Security for Android não pode verificar arquivos com um tamanho de 2 GB ou mais. Durante uma verificação, o aplicativo ignora tais arquivos sem notificá-lo que tais arquivos foram ignorados.

Para definir as configurações de proteção em tempo real de dispositivo móveis:

1. No árvore do console, na pasta **Dispositivos gerenciados**, selecione o grupo de administração ao qual os dispositivos Android pertencem.
2. Na área de trabalho do grupo, selecione a guia **Políticas**.
3. Clique duas vezes em qualquer coluna para abrir a janela de propriedades da política.
4. Na janela **Propriedades** da política, selecione a seção **Proteção**.
5. Na seção **Proteção**, especifique as configurações da proteção do sistema de arquivos do dispositivo móvel:
   - Para ativar a proteção em tempo real do dispositivo móvel contra ameaças, selecione a caixa **Ativar proteção**.

     O Kaspersky Endpoint Security for Android somente verifica novos aplicativos e arquivos da pasta Downloads.
   - Para ativar a proteção expandida do dispositivo móvel contra ameaças, selecione a caixa **Modo de proteção estendida**.

     O Kaspersky Endpoint Security for Android verificará todos os arquivos que o usuário abrir, modificar, mover, copiar, instalar ou salvar no dispositivo, assim como os novos aplicativos móveis instalados.

Em dispositivos que executam Android 8.0 ou posterior, o Kaspersky Endpoint Security for Android verifica os arquivos que o usuário modifica, move, instala e salva, assim como as cópias dos arquivos. O Kaspersky Endpoint Security for Android não verifica os arquivos quando são abertos, ou arquivos de origem quando copiados.

- Para ativar a verificação adicional de novos aplicativos antes de sua primeira inicialização no dispositivo do usuário com ajuda do serviço na nuvem da Kaspersky Security Network, marque a caixa de seleção **Proteção na nuvem (KSN)**.
- Para bloquear adwares e aplicativos que podem ser explorados por criminosos para danificar o dispositivo ou os dados do usuário, marque a caixa de seleção **Detectar adwares, discadores automáticos e aplicativos que podem ser usados por criminosos para danificar o dispositivo e os dados do usuário**.

6. Na lista **Ação na detecção de ameaças**, selecione uma das seguintes opções:
   - **Excluir**

     Os objetos detectados serão automaticamente excluídos. O usuário não deve executar qualquer ação adicional. Antes de excluir um objeto, o Kaspersky Endpoint Security for Android exibirá uma notificação temporária sobre a detecção do objeto.
   - **Ignorar**

     Se os objetos detectados foram ignorados, o Kaspersky Endpoint Security for Android avisa o usuário sobre os problemas na proteção do dispositivo. As informações sobre os objetos ignorados são exibidas na seção **Status** do aplicativo. Para cada ameaça ignorada, o aplicativo fornece ações que o usuário pode executar para eliminar a ameaça. A lista de objetos ignorados pode modificar-se, por exemplo, se um arquivo malicioso foi excluído ou movido. Para receber uma lista atualizada de ameaças, execute uma verificação completa do dispositivo. Para assegurar a proteção confiável dos dados, elimine todos os objetos detectados.
   - **Quarentena**
7. Clique no botão **Aplicar** para salvar as alterações efetuadas.

As configurações do dispositivo móvel são definidas depois da próxima sincronização do dispositivo com o Kaspersky Security Center.

Para configurar a execução automática da verificação de vírus no dispositivo móvel:

1. No árvore do console, na pasta **Dispositivos gerenciados**, selecione o grupo de administração ao qual os dispositivos Android pertencem.
2. Na área de trabalho do grupo, selecione a guia **Políticas**.
3. Clique duas vezes em qualquer coluna para abrir a janela de propriedades da política.
4. Na janela **Propriedades** da política, selecione a seção **Verificar**.
5. Para bloquear adwares e aplicativos que podem ser explorados por criminosos para danificar o dispositivo ou os dados do usuário, marque a caixa de seleção **Detectar adwares, discadores automáticos e aplicativos que podem ser usados por criminosos para danificar o dispositivo e os dados do usuário**.
6. Na lista **Ação na detecção de ameaças**, selecione uma das seguintes opções:

- **Excluir**

  Os objetos detectados serão automaticamente excluídos. O usuário não deve executar qualquer ação adicional. Antes de excluir um objeto, o Kaspersky Endpoint Security for Android exibirá uma notificação temporária sobre a detecção do objeto.

- **Ignorar**

  Se os objetos detectados foram ignorados, o Kaspersky Endpoint Security for Android avisa o usuário sobre os problemas na proteção do dispositivo. As informações sobre os objetos ignorados são exibidas na seção **Status** do aplicativo. Para cada ameaça ignorada, o aplicativo fornece ações que o usuário pode executar para eliminar a ameaça. A lista de objetos ignorados pode modificar-se, por exemplo, se um arquivo malicioso foi excluído ou movido. Para receber uma lista atualizada de ameaças, execute uma verificação completa do dispositivo. Para assegurar a proteção confiável dos dados, elimine todos os objetos detectados.

- **Quarentena**

- **Perguntar ao usuário**

  O aplicativo Kaspersky Endpoint Security for Android exibe uma notificação solicitando que o usuário escolha a ação a ser executada no objeto detectado: **Ignorar** ou **Excluir**.

  Quando o aplicativo detectar diversos objetos, a opção **Perguntar ao usuário** permite que o usuário do dispositivo aplique a ação selecionada a cada arquivo usando a caixa de seleção **Aplicar a todas as ameaças**.

  O Kaspersky Endpoint Security for Android deve ser definido como um recurso de Acessibilidade para assegurar a exibição de notificações em dispositivos móveis com Android 10.0 ou posterior. O Kaspersky Endpoint Security for Android solicita que o usuário defina o aplicativo como um recurso de Acessibilidade pelo Assistente de Configuração Inicial. O usuário pode ignorar esta etapa ou desativar este serviço nas configurações de dispositivo em um momento posterior. Nesse caso, o Kaspersky Endpoint Security for Android exibe uma janela de sistema do Android solicitando que o usuário escolha a ação a ser executada no objeto detectado: Ignorar ou Excluir. Para aplicar a ação a múltiplos objetos, é preciso abrir o Kaspersky Endpoint Security.

7. A seção **Verificação agendada** permite definir as configurações de início automático da verificação completa do sistema de arquivos do dispositivo. Para fazer isso, clique no botão **Agendamento** e especifique a frequência e a hora inicial da verificação completa na janela **Agendamento**.

   No Android 12 ou posterior, o aplicativo pode realizar essa tarefa após o especificado se o dispositivo estiver no modo de economia de bateria.

8. Clique no botão **Aplicar** para salvar as alterações efetuadas.

As configurações do dispositivo móvel são definidas depois da próxima sincronização do dispositivo com o Kaspersky Security Center. O Kaspersky Endpoint Security for Android verifica todos os arquivos, inclusive o conteúdo dos arquivos comprimidos.

Para manter atualizada a proteção do dispositivo móvel, defina as configurações da atualização do banco de dados de antivírus.

Por padrão, as atualizações do banco de dados de antivírus são desativadas quando o dispositivo estiver em modo de roaming. As atualizações agendadas dos bancos de dados antivírus não são executadas.

Para definir as configurações de atualizações do banco de dados de antivírus:

1. No árvore do console, na pasta **Dispositivos gerenciados**, selecione o grupo de administração ao qual os dispositivos Android pertencem.

2. Na área de trabalho do grupo, selecione a guia **Políticas**.

3. Clique duas vezes em qualquer coluna para abrir a janela de propriedades da política.

4. Na janela **Propriedades** da política, selecione a seção **Atualização do banco de dados**.

5. Se você desejar que o Kaspersky Endpoint Security for Android faça o download das atualizações do banco de dados de acordo com o agendamento de atualização quando o dispositivo estiver na zona de roaming, selecione a caixa de seleção **Permitir a atualização do banco de dados quando em roaming** na seção **Atualizar o banco de dados quando em roaming**.

   Mesmo que a caixa de seleção esteja desmarcada, o usuário pode iniciar uma atualização do banco de dados de antivírus manualmente quando o dispositivo estiver em roaming.

6. Na seção **Fonte de atualização do banco de dados**, especifique a origem de atualização a partir da qual o Kaspersky Endpoint Security for Android recebe e instala as atualizações do banco de dados antivírus:

   - **Servidores da Kaspersky**

     Utiliza o servidor de atualização da Kaspersky como origem de atualização para efetuar o download dos bancos de dados do Kaspersky Endpoint Security for Android nos dispositivos móveis dos usuários. Para atualizar os bancos de dados de servidores da Kaspersky, o Kaspersky Endpoint Security for Android transmite dados à Kaspersky (por exemplo, a ID da tarefa de atualização executada). A lista de dados transmitidos durante as atualizações do banco de dados é fornecida no Contrato de Licença do Usuário Final.

   - **Servidor de Administração**

     Utiliza o repositório do Servidor de Administração do Kaspersky Security Center como a origem de atualização para efetuar o download dos bancos de dados do Kaspersky Endpoint Security for Android nos dispositivos móveis dos usuários.

   - **Outra fonte**

     Utiliza um servidor de terceiros como origem de atualização para efetuar o download dos bancos de dados do Kaspersky Endpoint Security for Android nos dispositivos móveis dos usuários. Para iniciar uma atualização, você deve inserir o endereço de um servidor HTTP no campo abaixo (por exemplo, http://domain.com/).

7. Na seção **Atualização do banco de dados agendada**, defina as configurações para atualização automática do banco de dados de antivírus no dispositivo do usuário. Para fazer isso, clique no botão **Agendamento** e especifique a frequência e a hora inicial das atualizações na janela **Agendamento**.

   No Android 12 ou posterior, o aplicativo pode realizar essa tarefa após o especificado se o dispositivo estiver no modo de economia de bateria.

8. Clique no botão **Aplicar** para salvar as alterações efetuadas.

As configurações do dispositivo móvel são definidas depois da próxima sincronização do dispositivo com o Kaspersky Security Center.

Proteção de dispositivos Android na Internet

Para proteger os dados pessoais de um usuário de dispositivo móvel na Internet, ative a proteção na web. A Proteção na Web bloqueia sites maliciosos que distribuem códigos maliciosos e sites de phishing criados para roubar seus dados confidenciais e obter acesso a suas contas financeiras. A Proteção na Web verifica os sites antes de abri-los utilizando o serviço Kaspersky Security Network na nuvem. A Proteção na Web também permite configurar o acesso de um usuário a sites com base em listas predefinidas de sites permitidos e bloqueados.

O Kaspersky Endpoint Security for Android deve ser definido como um Recursos de Acessibilidade. O Kaspersky Endpoint Security for Android solicita que o usuário defina o aplicativo como um recurso de Acessibilidade pelo Assistente de Configuração Inicial. O usuário pode ignorar esta etapa ou desativar este serviço nas configurações de dispositivo em um momento posterior.

- A Proteção na Web nos dispositivos Android funciona apenas nos navegadores Google Chrome (incluindo o recurso Guias personalizadas), Huawei Browser e Samsung Internet. A Proteção na Web para Samsung Internet Browser não bloqueia sites em um dispositivo móvel se um perfil de trabalho for usado e a Proteção na Web estiver ativada apenas para o perfil de trabalho.

Para ativar a Proteção na Web no Google Chrome e no Navegador da Internet da Samsung:

1. No árvore do console, na pasta **Dispositivos gerenciados**, selecione o grupo de administração ao qual os dispositivos Android pertencem.
2. Na área de trabalho do grupo, selecione a guia **Políticas**.
3. Clique duas vezes em qualquer coluna para abrir a janela de propriedades da política.
4. Na janela **Propriedades** da política, selecione **Proteção na Web**.
5. Para usar a Proteção na Web, você ou o usuário do dispositivo deve ler e aceitar a Declaração relativa ao processamento de dados com o propósito de usar a Proteção na Web (Declaração de Proteção na Web):
   a. Clique no link **Declaração da Proteção na Web**.
      Isso abre a janela **Declaração relativa ao processamento de dados com o propósito de usar a Proteção na Web**. Para aceitar a Declaração da Proteção na Web, você deve ler e aceitar a Política de Privacidade.
   b. Clique no link Política de Privacidade. Leia e aceite a Política de Privacidade.
      Se você não aceitar a Política de Privacidade, o usuário do dispositivo móvel poderá aceitar a Política de Privacidade no Assistente de Configuração Inicial ou no aplicativo (→ **Sobre o aplicativo** → **Termos e condições** → **Política de Privacidade**).
   c. Selecione o modo de aceitação da Declaração da Proteção na Web:
      - **Li e aceito a Declaração de Proteção na Web**
      - **Solicitar a aceitação da Declaração de Proteção na Web do usuário do dispositivo**
      - **Não aceito a Declaração da Proteção na Web**
6. Se você selecionar **Eu não aceito a Declaração de Proteção na Web**, a Proteção na Web não bloqueará sites em um dispositivo móvel. O usuário do dispositivo móvel não pode ativar a Proteção na Web no Kaspersky Endpoint Security.
7. Selecione a caixa de seleção **Ativar a Proteção na Web**.

8. Clique no botão **Aplicar** para salvar as alterações efetuadas.

As configurações do dispositivo móvel são definidas depois da próxima sincronização do dispositivo com o Kaspersky Security Center.

Proteção de dados perdidos ou roubados

Essa seção descreve como você pode definir as configurações de acesso não autorizado no dispositivo caso ele seja perdido ou roubado.

Enviar comandos Antirroubo para um dispositivo móvel

Para proteger dados em um dispositivo móvel perdido ou roubado, você pode enviar comandos especiais (consulte a tabela abaixo).

Comandos para proteger dados em um dispositivo perdido ou roubado

Método de conexão ao Kaspersky Security Center	Comando	Resultado da execução do comando
Kaspersky Endpoint Security for Android	Bloquear	O dispositivo móvel é bloqueado.
	Desbloquear	Após desbloquear um dispositivo com o Android 5.0 – 6.X em execução, a senha de desbloqueio da tela (código PIN) é reinicializada para "1234". Após desbloquear um dispositivo com o Android em execução 7.0 ou posterior, a senha de desbloqueio da tela não é modificada.
	Localizar o dispositivo	O dispositivo é localizado e exibido no Google Maps. O provedor de serviços móvel cobra uma taxa para enviar o SMS e para o acesso à Internet. Em dispositivos executando Android 12 ou posterior, se o usuário tiver concedido a permissão "Usar local aproximado", o aplicativo Kaspersky Endpoint Security for Android tentará primeiro obter a localização precisa do dispositivo. Se isso não for bem-sucedido, a localização aproximada do dispositivo será retornada apenas se tiver sido recebida não mais de 30 minutos antes. Caso contrário, o comando **Localizar o dispositivo** falhará.
	Retrato	O dispositivo móvel é bloqueado. O retrato é tirado pela câmera frontal do dispositivo quando alguém tenta desbloqueá-lo. O provedor de serviços móvel cobra uma taxa para enviar o SMS e para o acesso à Internet. Ao tentar desbloquear o dispositivo, o usuário automaticamente consente no retrato.

		Se a permissão para usar a câmera tiver sido revogada, o dispositivo móvel exibirá uma notificação e solicitará a permissão. Em um dispositivo móvel executando Android 12 ou posterior, se a permissão para usar a câmera tiver sido revogada por meio das Configurações rápidas, a notificação não será exibida, mas a foto tirada será preta.
	Alarme	O dispositivo móvel soa um alarme. O alarme soa por 5 minutos (ou durante 1 minuto se a bateria do dispositivo estiver fraca).
	Limpar os dados corporativos	Limpar os dados em contêiner, conta de e-mail corporativo, configurações para conectar à rede Wi-Fi corporativa e VPN, nome do ponto de acesso (APN), perfil de trabalho do Android, contêiner KNOX e a chave do Gerenciador de licença KNOX.
	Redefinir para as configurações de fábrica	Todos os dados são excluídos do dispositivo móvel e as configurações são revertidas aos valores de fábrica. Após este comando ter sido executado, o dispositivo não será capaz de receber ou executar comandos subsequentes.
Perfil de iOS MDM	Bloquear	O dispositivo móvel é bloqueado.
	Desbloquear	O bloqueio do dispositivo móvel com um código PIN é desativado. O código PIN anteriormente especificado foi redefinido.
	Limpar os dados corporativos	Todos os perfis de configuração instalados, perfis de provisionamento, perfil de iOS MDM e aplicativos para os quais a caixa de seleção **Remover junto com o perfil de iOS MDM** tiver sido selecionada são removidos do dispositivo.
	Redefinir para as configurações de fábrica	Todos os dados são excluídos do dispositivo móvel e as configurações são revertidas aos valores de fábrica. Após este comando ter sido executado, o dispositivo não será capaz de receber ou executar comandos subsequentes.
Caixa de correio do Exchange	Redefinir para as configurações de fábrica	Todos os dados são excluídos do dispositivo móvel e as configurações são revertidas aos valores de fábrica. Após este comando ter sido executado, o dispositivo não será capaz de receber ou executar comandos subsequentes.

Os direitos e permissões especiais são necessários para a execução de comandos do Kaspersky Endpoint Security for Android. Quando o Assistente de Configuração Inicial estiver em execução, o Kaspersky Endpoint Security for Android solicita que o usuário conceda ao aplicativo todos os direitos e permissões necessários. O usuário pode ignorar estas etapas ou desativar estas permissões nas configurações de dispositivo em um momento posterior. Se este for o caso, será impossível executar os comandos.

Em dispositivos executando Android 10.0 ou posterior o usuário deve conceder permissão "Permitir o tempo todo" para acessar a localização. Em dispositivos executando Android 11.0 ou posterior, o usuário também deve conceder a permissão "Enquanto usa o aplicativo" para acessar a câmera. Caso contrário, os comandos antirroubo não funcionarão. O usuário será notificado desta limitação e novamente será solicitado que conceda permissões do nível necessário. Se o usuário selecionar a opção "Somente desta vez" para a permissão da câmera, o acesso será considerado concedido pelo aplicativo. Recomenda-se contatar o usuário diretamente, caso a permissão da câmera seja solicitada novamente.

Para saber mais sobre o envio de comandos da lista de dispositivos móveis no Console de Administração, consulte a *Ajuda do Kaspersky Security Center*.

Desbloquear um dispositivo móvel

Você pode desbloquear um dispositivo móvel usando os seguintes métodos:

- Enviar o comando de bloqueio do dispositivo móvel.
- Insira o código de desbloqueio para uma só utilização no dispositivo móvel (somente para dispositivos Android).

Em determinados dispositivos (por exemplo, Huawei, Meizu e Xiaomi), é preciso adicionar manualmente o Kaspersky Endpoint Security for Android na lista de aplicativos que são iniciados quando o sistema operacional inicia. Se o aplicativo não for adicionado à lista, você somente pode desbloquear o dispositivo usando código de desbloqueio de uma só utilização. Você não pode usar comandos para desbloquear o dispositivo.

Para saber mais sobre o envio de comandos da lista de dispositivos móveis no Console de Administração, consulte a *Ajuda do Kaspersky Security Center*.

Um *código de desbloqueio para uma só utilização* é um código de acesso secreto do aplicativo para desbloquear o dispositivo móvel. O código para uma só utilização é gerado pelo aplicativo e é exclusivo para cada dispositivo móvel. Você pode modificar o comprimento do código para uma só utilização (4, 8 ou 16 dígitos) nas configurações de política de grupo na seção **Antirroubo**.

Para desbloquear o dispositivo móvel usando um código para uma só utilização:

1. Na árvore do console, selecione **Gerenciamento de dispositivo móvel** → **Dispositivos móveis**.
2. Selecione um dispositivo móvel para o qual você deseja obter um código de desbloqueio temporário.
3. Clique duas vezes para abrir a janela Propriedades do dispositivo móvel.
4. Selecione **Aplicativos** → **Kaspersky Endpoint Security for Android**.
5. Abra a janela Propriedades do Kaspersky Endpoint Security ao clicar duas vezes.
6. Selecione a seção **Antirroubo**.
7. Um código único para o dispositivo selecionado será exibido no campo **Código para uma só utilização** da seção **Código para uma só utilização para o desbloqueio do dispositivo**.
8. Use qualquer método disponível (como e-mail) para comunicar o código para uma só utilização ao usuário do dispositivo bloqueado.
9. O usuário insere o código para uma só utilização na tela do dispositivo que é bloqueado pelo Kaspersky Endpoint Security for Android.

O dispositivo móvel será desbloqueado. Após desbloquear um dispositivo com o Android 5.0 – 6.X em execução, a senha de desbloqueio da tela (código PIN) é reinicializada para "1234". Após desbloquear um dispositivo com o Android em execução 7.0 ou posterior, a senha de desbloqueio da tela não é modificada.

Criptografia de dados

Para proteger os dados contra o acesso não autorizado, você deve ativar a criptografia de todos os dados no dispositivo (por exemplo, credenciais de conta, dispositivos e aplicativos externos, assim como mensagens de e-mail, mensagens SMS, contatos, fotos e outros arquivos). Para o acesso aos dados criptografados, você deve especificar uma chave especial – senha de desbloqueio do dispositivo. Se os dados estiverem criptografados, o acesso a eles somente pode ser obtido quando o dispositivo for desbloqueado.

A criptografia de dados é ativada por padrão em dispositivos iOS bloqueados por senha (**Configurações** → **Touch ID / Face ID e Senha** → **Ativara senha)**.

Para criptografar todos os dados em um dispositivo Android:

1. Ative o bloqueio da tela no dispositivo Android (**Configurações** → **Segurança** → **Bloquear a tela**).
2. Defina uma senha de desbloqueio do dispositivo que esteja em conformidade com os requisitos de segurança corporativa.

   Não se recomenda usar uma senha de padrão para desbloquear o dispositivo. Em determinados dispositivos Android que executam o Android 6.0 ou posterior, após criptografar os dados e reiniciar o dispositivo Android, é necessário inserir uma senha numérica para desbloquear o dispositivo em vez de uma senha de padrão. Este problema é relacionado à operação do serviço Recursos de Acessibilidade. Para desbloquear a tela do dispositivo neste caso, converta a senha de padrão em uma senha numérica. Para obter mais detalhes sobre a conversão de uma senha de padrão em uma senha numérica, consulte o site de Suporte Técnico do fabricante do dispositivo móvel.

3. Ative a criptografia de todos os dados no dispositivo (**Configurações** → **Segurança** → **Criptografas dados**).

Configurar a força da senha de desbloqueio

Para proteger o acesso ao dispositivo móvel de um usuário, você deve definir uma senha de desbloqueio do dispositivo.

Esta seção contém informações sobre como configurar a proteção por senha em dispositivos Android e iOS.

Configurar uma senha forte de desbloqueio para um dispositivo Android

Para manter um dispositivo Android seguro, é necessário configurar uma senha que será solicitada quando o dispositivo sair do modo ocioso.

É possível impor restrições à atividade do usuário no dispositivo se a senha de desbloqueio do dispositivo for fraca (por exemplo, bloquear o dispositivo). Você pode impor restrições usando o componente Controle de conformidade. Para fazer isso, nas configurações da regra de verificação, você deve selecionar o critério **A senha de desbloqueio não está em conformidade com os requisitos de segurança**.

Em determinados dispositivos Samsung que executam o Android 7.0 ou posterior, quando o usuário tenta configurar métodos não compatíveis para desbloquear o dispositivo (por exemplo, uma senha gráfica), o dispositivo pode ser bloqueado se as seguintes condições forem atendidas: A remoção do Kaspersky Endpoint Security for Android está ativada e os requisitos de força da senha de desbloqueio da tela estão definidos. Para desbloquear o dispositivo, é necessário enviar um comando especial ao dispositivo.

Para configurar o uso de uma senha de desbloqueio:

1. No árvore do console, na pasta **Dispositivos gerenciados**, selecione o grupo de administração ao qual os dispositivos Android pertencem.

2. Na área de trabalho do grupo, selecione a guia **Políticas**.

3. Clique duas vezes em qualquer coluna para abrir a janela de propriedades da política.

4. Na janela **Propriedades** da política, selecione a seção **Gerenciamento do dispositivo**.

5. Se você desejar que o aplicativo verifique se uma senha de desbloqueio foi definida, selecione a caixa de seleção **Exigir a definição da senha de desbloqueio da tela** na seção **Bloquear a tela**.

   Se o aplicativo detectar que nenhuma senha do sistema foi definida no dispositivo, o usuário será solicitado a defini-la. A senha é definida de acordo com os parâmetros definidos pelo administrador.

6. Especifique o número mínimo de caracteres.

   O número mínimo de caracteres da senha do usuário. Valores possíveis: 4 a 16 caracteres.

   A senha do usuário tem 4 caracteres por padrão.

   > Para dispositivos com Android 10.0 ou posterior, o Kaspersky Endpoint Security divide os requisitos da força de segurança da senha em um dos valores do sistema: médio ou alto.

   Os valores para dispositivos com Android 10.0 ou posterior são determinados pelas seguintes regras:

   - Se a quantidade de símbolos exigida for de 1 a 4, então o aplicativo solicita ao usuário que defina uma senha de força média. Ela pode ser tanto numérica (PIN), sem números repetidos ou sequenciais (ex. 1234), ou alfabética/alfanumérica. O PIN ou a senha deve ter no mínimo 4 caracteres.

   - Se o número de símbolos exigidos for 5 ou mais, então o aplicativo solicita ao usuário que defina uma senha de segurança alta. Ela pode ser tanto numérica (PIN), sem números repetidos ou sequenciais, ou alfabética/alfanumérica (senha). O PIN deve ter no mínimo 8 dígitos; a senha deve ter no mínimo 6 caracteres.

7. Se você quiser que o usuário tenha a capacidade de usar impressões digitais para desbloquear a tela, selecione a caixa de seleção **Permitir o uso da impressão digital**. Se a senha de desbloqueio não estiver em conformidade com os requisitos de segurança corporativa, não será possível usar um digitalizador de impressão digital para desbloquear a tela.

   > Em dispositivos com Android 10.0 ou posterior, o uso das digitais para desbloquear a tela pode ser disponibilizado somente para o perfil de trabalho.

   > o Kaspersky Endpoint Security for Android não restringe o uso de um digitalizador de impressão digital para efetuar o login em aplicativos ou para confirmar compras

   > Em determinados dispositivos Samsung é impossível bloquear o uso de impressões digitais para desbloquear a tela. Em determinados dispositivos Samsung, se a senha de desbloqueio não estiver em conformidade com requisitos de segurança corporativa, o Kaspersky Endpoint Security for Android não bloqueia o uso de impressões digitais para desbloquear a tela.

   Após adicionar uma impressão digital nas configurações do dispositivo, o usuário pode desbloquear a tela usando os seguintes métodos:

- Passe o dedo no digitalizador de impressão digital (método principal).
- Insira a senha de desbloqueio (método de backup).

8. Clique no botão **Aplicar** para salvar as alterações efetuadas.

As configurações do dispositivo móvel são definidas depois da próxima sincronização do dispositivo com o Kaspersky Security Center.

Configurar uma senha forte de desbloqueio para dispositivos iOS MDM

Para proteger os dados do seu dispositivo iOS MDM, especifique as configurações da força de senha de desbloqueio.

Por padrão, o usuário pode usar uma senha simples. Uma *senha simples* é uma senha que contém caracteres sucessivos ou repetidos, como "abcd" ou "2222". Não é requerido que o usuário insira uma senha alfanumérica que inclua símbolos especiais. Por padrão, o período de validade da senha e o número de tentativas de inserção da senha não são limitados.

Para especificar as configurações da força para uma senha de desbloqueio num dispositivo iOS MDM:

1. No árvore do console, na pasta **Dispositivos gerenciados**, selecione o grupo de administração ao qual os dispositivos iOS MDM pertencem.
2. Na área de trabalho do grupo, selecione a guia **Políticas**.
3. Clique duas vezes para abrir a janela de propriedades da política.
4. Na janela **Propriedades** da política, selecione a seção **Senha**.
5. Na seção **Configurações de senha**, selecione a caixa **Aplicar as configurações no dispositivo**.
6. Especifique as configurações de força da senha de desbloqueio:
   - Para permitir que o usuário use uma senha simples, selecione a caixa **Permitir senha simples**.
   - Para requerer o uso de letras e números na senha, selecione a caixa de seleção **Solicitar valor alfanumérico**.
   - Na lista **Comprimento mínimo da senha**, selecione o número mínimo de caracteres da senha.
   - Na lista **Número mínimo de caracteres especiais**, selecione o número mínimo de caracteres especiais na senha (como "$", "&", "!").
   - No campo **Tempo de vida máximo da senha**, especifique o período de tempo em dias durante o qual a senha permanecerá atual. Quando o período expira, o Kaspersky Device Management for iOS solicita que o usuário troque a senha.
   - Na lista **Ativar o bloqueio automático em**, selecione o período de tempo após o qual o bloqueio automático do dispositivo iOS MDM será ativado.
   - No campo **Histórico de senha**, especifique o número de senhas usadas (incluindo a senha atual) que o Kaspersky Mobile Device Management for iOS compara com a nova senha quando o usuário altera a senha antiga. Se as senhas coincidem, a nova senha é rejeitada.
   - Na lista **Tempo máximo para desbloquear sem senha**, selecione o período de tempo durante o qual o usuário pode desbloquear o dispositivo iOS MDM sem inserir a senha.

- Em **Número máximo de tentativas de acesso**, selecione o número de tentativas de acesso que o usuário pode efetuar para inserir a senha de desbloqueio do dispositivo iOS MDM.

7. Clique no botão **Aplicar** para salvar as alterações efetuadas.

Como resultado, após a política ser aplicada, o Kaspersky Device Management for iOS verifica a força da senha configurada no dispositivo móvel do usuário. Se a força da senha de desbloqueio do dispositivo não estiver conforme a política, o usuário deve alterar a senha.

Configurar uma senha forte de desbloqueio para dispositivos EAS

Configure uma senha de desbloqueio forte para proteger dados no dispositivo EAS.

Por padrão, quando um dispositivo móvel é ligado, o Kaspersky Device Management for iOS não solicita que o usuário insira ou configure uma senha de desbloqueio.

Para especificar as configurações da força para uma senha de desbloqueio num dispositivo EAS:

1. No árvore do console, na pasta **Dispositivos gerenciados**, selecione o grupo de administração ao qual os dispositivos EAS pertencem.

2. Na área de trabalho do grupo, selecione a guia **Políticas**.

3. Clique duas vezes para abrir a janela de propriedades da política.

4. Na janela Propriedades da política, selecione a seção **Senha**.

5. Na seção **Configurações de senha**, selecione a caixa **Solicitar a senha**.

6. Especifique as configurações de força da senha de desbloqueio:

   - Para requerer que o usuário use letras e números na senha, selecione a caixa de seleção **Solicitar valor alfanumérico**. No campo **Número mínimo do conjunto de caracteres**, especifique o nível de força da senha alfanumérica. Os valores possíveis são: 1 a 4 caracteres. O valor "1" corresponde ao nível de força mais baixo.

   - Para permitir que o usuário use a função de recuperação de senha, selecione a caixa **Ativar a recuperação da senha**.

   - Se você desejar que os arquivos sejam criptografados na memória do dispositivo, selecione a caixa de seleção **Requerer a criptografia no dispositivo**.

   - Se você desejar que os arquivos sejam criptografados no cartão de memória do dispositivo, selecione a caixa de seleção **Requerer a criptografia no cartão de memória**.

   - Para permitir que um usuário use uma senha simples que consiste somente em números, selecione a caixa **Permitir senha simples**.

   - Para limitar o número de tentativas para inserir a senha para acessar o dispositivo, selecione a caixa de seleção **Número máximo de tentativas de acesso**. No campo à direita da caixa de seleção, especifique o número de tentativas de inserção da senha que o usuário pode fazer para desbloquear o dispositivo. Se o usuário não inserir a senha correta após o número especificado de tentativas seguidas, o Kaspersky Device Management for iOS limpa todos os dados.

   - Para especificar o comprimento mínimo da senha do usuário, selecione a caixa **Comprimento mínimo da senha**. Especifique o número mínimo de caracteres da senha no campo à direita da caixa de seleção. Valores possíveis: 4 a 16 caracteres.

- Para solicitar que o usuário insira a senha após o dispositivo ficar ocioso por algum tempo, selecione a caixa de seleção **Tempo de ociosidade até a nova tentativa de inserção da senha (min)**. No campo à direita na caixa de seleção, especifique o período de ociosidade em minutos. Quando este período decorre, o aplicativo solicita que o usuário insira a senha.

- Para limitar o período de validade da senha, selecione a caixa **Período de validade da senha (dias)**. No campo à direita da caixa de seleção, especifique o período de validade da senha. Quando este período expira, o aplicativo solicita que o usuário troque a senha.

- No campo **Histórico de senha**, especifique o número das senhas antigas mais recentes que não podem ser novamente usadas.

7. Clique no botão **Aplicar** para salvar as alterações efetuadas.

As configurações do dispositivo móvel são definidas depois da próxima sincronização do dispositivo com o Kaspersky Security Center. Depois que a política é aplicada, o Kaspersky Device Management for iOS verifica se há uma senha configurada no dispositivo móvel do usuário. Se a senha de desbloqueio não for configurada no dispositivo, é solicitado ao usuário que a configure. A senha deve ser configurada tendo em conta as configurações da política. Se a senha de desbloqueio do dispositivo for configurada, mas não estiver conforme a política, é solicitado que o usuário altere a senha.

Configurar uma Rede Privada Virtual (VPN)

Esta seção contém informações sobre a definição de configurações da Rede Privada Virtual (VPN) para a conexão segura às redes Wi-Fi.

Configurar a VPN em dispositivos Android (somente Samsung)

Para conectar com segurança um dispositivo Android a redes Wi-Fi e proteger a transferência de dados, você deve definir as configurações da VPN (Rede Privada Virtual).

A configuração da VPN é possível somente para os dispositivos Samsung.

Os requisitos seguintes devem ser considerados ao usar uma rede privada virtual:

- O aplicativo que usa a conexão VPN deve ser permitida nas configurações do Firewall.

- As configurações da rede privada virtual especificadas na política não podem ser aplicadas nos aplicativos do sistema. A conexão com a VPN para aplicativos do sistema deve ser configurada manualmente.

- Alguns aplicativos que usam a conexão com a VPN devem ter configurações adicionais especificadas ao inicializar pela primeira vez. Para especificar as configurações, a conexão com a VPN deve ser permitida nas configurações do aplicativo.

Para configurar a VPN em um dispositivo móvel de um usuário:

1. No árvore do console, na pasta **Dispositivos gerenciados**, selecione o grupo de administração ao qual os dispositivos Android pertencem.

2. Na área de trabalho do grupo, selecione a guia **Políticas**.

3. Clique duas vezes em qualquer coluna para abrir a janela de propriedades da política.

4. Na janela **Propriedades** da política, selecione a seção **Gerenciar o Samsung KNOX → Gerenciar dispositivos Samsung**.

5. Na seção **VPN**, clique no botão **Configurar**.

   Isto abre a janela **Rede VPN**.

6. Na lista suspensa **Tipo de conexão**, selecione o tipo de conexão VPN.

7. No campo **Nome da rede**, insira o nome do túnel VPN.

8. No campo **Endereço do servidor**, insira o nome de rede ou endereço IP do servidor da VPN.

9. Na lista **Domínio(s) de pesquisa DNS**, insira o domínio de pesquisa DNS a adicionar automaticamente ao nome do servidor DNS.

   Você pode especificar vários domínios de pesquisa DNS, separando-os com espaços em branco.

10. No campo **Servidore(s) DNS**, insira o nome completo do domínio ou endereço IP do servidor DNS.

    Você pode especificar vários servidores DNS, separando-os com espaços em branco.

11. No campo **Roteamento**, insira a faixa de endereços IP da rede cujos dados são trocados através da conexão com a VPN.

    Caso a faixa de endereços IP não seja especificada no campo **Roteamento**, todo o tráfego da Internet passará pela conexão da VPN.

12. Adicionalmente defina as seguintes configurações para redes dos tipos **IPSec Xauth PSK** e **L2TP IPSec PSK**:

    a. No campo **Chave compartilhada IPSec**, insira a senha para a chave de segurança IPSec predefinida.

    b. No campo **ID IpSec**, Insira o nome do usuário do dispositivo móvel.

13. Para uma rede **L2TP IPSec PSK**, especifique adicionalmente a senha para a chave L2TP que no campo **Chave L2TP**.

14. Para uma rede **PPTP**, selecione a caixa de seleção **Usar a conexão SSL** para que o aplicativo use o método MPPE (Microsoft Point-to-Point Encryption) de criptografia de dados para tornar segura a transmissão de dados quando o dispositivo móvel se conectar ao servidor VPN.

15. Clique no botão **Aplicar** para salvar as alterações efetuadas.

As configurações do dispositivo móvel são definidas depois da próxima sincronização do dispositivo com o Kaspersky Security Center.

Configurar a VPN em dispositivos iOS MDM

Para conectar um dispositivo iOS MDM à uma Rede Virtual Privada (VPN) e proteger os dados durante a conexão com a VPN, defina as configurações de conexão da VPN.

Para configurar a conexão da VPN no dispositivo iOS MDM de um usuário:

1. No árvore do console, na pasta **Dispositivos gerenciados**, selecione o grupo de administração ao qual os dispositivos iOS MDM pertencem.

2. Na área de trabalho do grupo, selecione a guia **Políticas**.

3. Clique duas vezes para abrir a janela de propriedades da política.

4. Na janela **Propriedades** da política, selecione a seção **VPN**.

5. Clique no botão **Adicionar** na seção **Redes VPN**.

   Isto abre a janela **Rede VPN**.

6. No campo **Nome da rede**, insira o nome do túnel VPN.

7. Na lista suspensa **Tipo de conexão**, selecione o tipo de conexão VPN:

   - **L2TP** (Layer 2 Tunneling Protocol). A conexão suporta a autenticação do usuário do dispositivo móvel iOS MDM utilizando senhas MS-CHAP v2, autenticação de dois fatores e autenticação automática utilizando uma chave pública.

   - **PPTP** (Point-to-Point Tunneling Protocol). A conexão suporta a autenticação do usuário do dispositivo móvel iOS MDM utilizando senhas MS-CHAP v2 e autenticação de dois fatores.

   - **IPSec (Cisco)**. A conexão suporta autenticação de usuário baseada em senha, autenticação de dois fatores e autenticação automática utilizando uma chave pública e certificados.

   - **Cisco AnyConnect**. A conexão suporta o firewall Cisco Adaptive Security Appliance (ASA) versão 8.0(3).1 ou posterior. Para configurar a conexão VPN, instale o aplicativo Cisco AnyConnect a partir da App Store no dispositivo móvel iOS MDM.

   - **Juniper SSL**. A conexão suporta o gateway Juniper Networks SSL VPN, Série SA, versão 6.4 ou posterior com o pacote Juniper Networks IVE versão 7.0 ou posterior. Para configurar a conexão VPN, instale o aplicativo JUNOS a partir da App Store no dispositivo móvel iOS MDM.

   - **F5 SSL**. A conexão suporta as soluções F5 BIG-IP Edge Gateway, Access Policy Manager e Fire SSL VPN. Para configurar a conexão VPN, instale o aplicativo F5 BIG-IP Edge Client a partir da App Store no dispositivo móvel iOS MDM.

   - **SonicWALL Mobile Connect**. A conexão suporte dispositivos SonicWALL Aventail E-Class Secure Remote Access versão 10.5.4 ou posterior, dispositivos SonicWALL SRA versão 5.5 ou posterior, bem como dispositivos SonicWALL Next-Generation Firewall, incluindo TZ, NSA, E-Class NSA com SonicOS versão 5.8.1.0 ou posterior. Para configurar a conexão VPN, instale o aplicativo SonicWALL Mobile Connect a partir da App Store no dispositivo móvel iOS MDM.

   - **Aruba VIA**. A conexão suporta controladores de acesso móvel Aruba Networks. Para configurá-los, instale o aplicativo Aruba Networks VIA a partir da App Store no dispositivo móvel iOS MDM.

   - **SSL personalizado**. A conexão suporte a autenticação do usuário do dispositivo móvel iOS MDM utilizando senhas e certificados e autenticação de dois fatores.

8. No campo **Endereço do servidor**, insira o nome de rede ou endereço IP do servidor da VPN.

9. No campo **Nome da conta**, insira o nome da conta para autorização no servidor da VPN. Você pode usar macros a partir da lista suspensa **Macros disponíveis**.

10. Especifique as configurações de segurança para a conexão VPN de acordo com o tipo selecionado de rede privada virtual.

11. Se necessário, especifique as configurações da conexão VPN através de um servidor proxy:

a. Selecione a guia **Configurações do servidor proxy**.

b. Selecione o modo de configuração do servidor proxy e especifique as configurações da conexão.

c. Clique em **OK**.

Como resultado, as configurações da conexão do dispositivo com uma VPN através de um servidor proxy serão configuradas no dispositivo iOS MDM.

12. Clique em **OK**.

    A nova VPN é exibida na lista.

13. Clique no botão **Aplicar** para salvar as alterações efetuadas.

Como resultado, uma conexão com a VPN será configurada no dispositivo iOS MDM do usuário onde a política foi aplicada.

Configurar o Firewall em dispositivos Android (somente Samsung)

Especifique as configurações do Firewall para monitorar conexões de rede no dispositivo móvel do usuário.

Para configurar o Firewall em um dispositivo móvel:

1. No árvore do console, na pasta **Dispositivos gerenciados**, selecione o grupo de administração ao qual os dispositivos Android pertencem.

2. Na área de trabalho do grupo, selecione a guia **Políticas**.

3. Clique duas vezes em qualquer coluna para abrir a janela de propriedades da política.

4. Na janela **Propriedades** da política, selecione a seção **Gerenciar o Samsung KNOX → Gerenciar dispositivos Samsung**.

5. Na janela **Firewall**, clique em **Configurar**.

   A janela **Firewall** é aberta.

6. Selecione o modo do Firewall:

   - Para permitir todas as conexões de entrada e saída no dispositivo móvel, mova o seletor deslizante para **Permitir tudo**.

   - Para bloquear toda a atividade da rede exceto dos aplicativos na lista de exclusões, mova o controle deslizante para cima, para **Bloquear todos exceto exceções**.

7. Se você configurar o modo do Firewall para **Bloquear todos exceto exceções**, crie uma lista de exclusões:

   a. Clique em **Adicionar**.

      Isto abre a janela **Exclusão para o firewall**.

   b. No campo **Nome do aplicativo**, insira o nome de um aplicativo móvel.

   c. No campo **Nome do pacote**, insira o nome do sistema do pacote do aplicativo móvel (por exemplo, `com.mobileapp.example`).

d. Clique em **OK**.

8. Clique no botão **Aplicar** para salvar as alterações efetuadas.

As configurações do dispositivo móvel são definidas depois da próxima sincronização do dispositivo com o Kaspersky Security Center.

Proteger o Kaspersky Endpoint Security for Android contra a remoção

Para a proteção do dispositivo móvel e a conformidade com requisitos de segurança corporativa, você pode ativar a proteção contra a remoção do Kaspersky Endpoint Security for Android. Neste caso, o usuário não pode remover o aplicativo usando a interface do Kaspersky Endpoint Security for Android. Ao remover o aplicativo usando as ferramentas do sistema operacional Android, você é solicitado a desativar os direitos de administrador para o Kaspersky Endpoint Security for Android. Após desativar os direitos, o dispositivo móvel será bloqueado.

Em determinados dispositivos Samsung que executam o Android 7.0 ou posterior, quando o usuário tenta configurar métodos não compatíveis para desbloquear o dispositivo (por exemplo, uma senha gráfica), o dispositivo pode ser bloqueado se as seguintes condições forem atendidas: A remoção do Kaspersky Endpoint Security for Android está ativada e os requisitos de força da senha de desbloqueio da tela estão definidos. Para desbloquear o dispositivo, é necessário enviar um comando especial ao dispositivo.

Para ativar a proteção contra a remoção do Kaspersky Endpoint Security for Android:

1. No árvore do console, na pasta **Dispositivos gerenciados**, selecione o grupo de administração ao qual os dispositivos Android pertencem.

2. Na área de trabalho do grupo, selecione a guia **Políticas**.

3. Clique duas vezes em qualquer coluna para abrir a janela de propriedades da política.

4. Na janela **Propriedades** da política, selecione a seção **Adicional**.

5. Na seção **Remoção do Kaspersky Endpoint Security for Android**, limpe a caixa de seleção **Permitir a remoção do Kaspersky Endpoint Security for Android**.

   Para proteger o aplicativo da remoção em dispositivos que executam o Android 7.0 ou posterior, o Kaspersky Endpoint Security for Android deve ser definido como um recurso de Acessibilidade. Quando o assistente Configuração inicial estiver sendo executado, o Kaspersky Endpoint Security for Android solicita ao usuário conceder ao aplicativo todas as permissões necessárias. O usuário pode ignorar estas etapas ou desativar estas permissões nas configurações de dispositivo em um momento posterior. Se este for o caso, o aplicativo não é protegido contra a remoção.

6. Clique no botão **Aplicar** para salvar as alterações efetuadas.

As configurações do dispositivo móvel são definidas depois da próxima sincronização do dispositivo com o Kaspersky Security Center. Se uma tentativa for feita para remover o aplicativo, o dispositivo móvel será bloqueado.

Detectar hackers do dispositivo (raiz)

O Kaspersky Security for Mobile permite detectar hackers do dispositivo (raiz). Os arquivos do sistema estão desprotegidos em um dispositivo hackeado, e por isso podem ser modificados. Além disso, aplicativos de terceiros de origens desconhecidas podem ser instalados em dispositivos hackeados. Após a detecção de uma tentativa de invasão, recomendamos restaurar imediatamente a operação normal do dispositivo.

Para detectar quando um usuário obtém privilégios de root, o Kaspersky Endpoint Security for Android usa os seguintes serviços:

- *O serviço incorporado do Kaspersky Endpoint Security for Android* é um serviço da Kaspersky que verifica se um usuário de dispositivo móvel obteve privilégios raiz (Kaspersky Mobile Security SDK).

- O *SafetyNet Attestation* é um serviço da Google que verifica a integridade do sistema operacional, analisa o hardware e software do dispositivo e identifica outros problemas de segurança. Para obter mais detalhes sobre o SafetyNet Attestation, visite o site de Suporte Técnico do Android.

Em caso de invasão do dispositivo, uma notificação será enviada ao usuário. Você pode visualizar notificações de hacking na área de trabalho do Servidor de Administração na guia **Monitorar**. É possível também desativar as notificações sobre invasões nas configurações de notificação de evento.

Em dispositivos que executam o Android, você pode impor restrições na atividade do usuário no dispositivo se o dispositivo for hackeado (por exemplo, bloquear o dispositivo). Você pode impor restrições usando o componente Controle de conformidade (veja a figura abaixo). Para fazer isso, nas configurações da regra de verificação, selecione o critério **O dispositivo foi roteado**.

Configurar um proxy HTTP global em dispositivos iOS MDM

Para proteger o tráfego da Internet do usuário, configure a conexão do dispositivo iOS MDM com a Internet por meio de um servidor proxy.

A conexão automática com a Internet por meio de um servidor proxy está disponível somente para os dispositivos controlados.

Para especificar as configurações do servidor proxy HTTP global no dispositivo iOS MDM do usuário:

1. No árvore do console, na pasta **Dispositivos gerenciados**, selecione o grupo de administração ao qual os dispositivos iOS MDM pertencem.

2. Na área de trabalho do grupo, selecione a guia **Políticas**.

3. Clique duas vezes para abrir a janela de propriedades da política.

4. Na janela **Propriedades** da política, selecione a seção **Proxy HTTP global**.

5. Na seção **Configurações do proxy HTTP global**, selecione a caixa **Aplicar as configurações no dispositivo**.

6. Selecione o tipo de configuração de proxy HTTP global.

   Por padrão, o tipo manual de configuração de proxy HTTP global é selecionado e o usuário está proibido de se conectar com redes cativas sem se conectar com um servidor proxy. *Redes cativas* são redes sem fio que requerem autenticação preliminar no dispositivo móvel sem conectar com o servidor proxy.

   - Para especificar as configurações de conexão com o servidor proxy manualmente:

a. Na lista suspensa **Tipo de configurações proxy**, selecione **Manual**.

b. No campo **Endereço e porta do servidor proxy**, insira o nome de um anfitrião ou do endereço IP de um servidor proxy e o número da porta do servidor proxy.

c. No campo **Nome de usuário**, configure o nome da conta do usuário para autorização do servidor proxy. Você pode usar macros a partir da lista suspensa **Macros disponíveis**.

d. No campo **Senha**, configure a senha da conta do usuário para autorização no servidor proxy.

e. Para permitir que o usuário acesse redes cativas, selecione a caixa **Permitir o acesso às redes captivas sem conectar o proxy**.

- Para especificar as configurações da conexão ao servidor proxy usando um arquivo PAC (Proxy Auto Configuration) predefinido:

a. Na lista suspensa **Tipo de configurações proxy**, selecione **Automático**.

b. No campo **URL do arquivo PAC**, insira o endereço da Web do arquivo PAC (por exemplo: http://www.example.com/filename.pac).

c. Para permitir que o usuário conecte o dispositivo móvel a uma rede sem fio se usar um servidor proxy quando o arquivo PAC não pode ser acessado, selecione a caixa **Permitir a conexão direta de o arquivo PAC não puder ser acessado**.

d. Para permitir que o usuário acesse redes cativas, selecione a caixa **Permitir o acesso às redes captivas sem conectar o proxy**.

7. Clique no botão **Aplicar** para salvar as alterações efetuadas.

Como resultado, após a aplicação da política, o usuário do dispositivo móvel pode estabelecer conexão com a Internet por meio de um servidor proxy.

Adicionar certificados de segurança aos dispositivos iOS MDM

Para simplificar a autenticação do usuário e garantir a segurança dos dados, adicione certificados ao dispositivo iOS MDM do usuário. Os dados assinados com um certificado são protegidos contra modificação durante a troca de rede. A criptografia de dados usando um certificado fornece um nível adicional de segurança para os dados. O certificado pode também ser usado para verificar a identidade do usuário.

O Kaspersky Mobile Device Management for iOS suporta os seguintes padrões de certificado:

- **PKCS#1** – criptografia com uma chave pública baseada em algoritmos RSA.
- **PKCS#12** – armazenamento e transmissão de um certificado e uma chave particular.

Para adicionar um certificado de segurança no dispositivo iOS MDM de um usuário:

1. No árvore do console, na pasta **Dispositivos gerenciados**, selecione o grupo de administração ao qual os dispositivos iOS MDM pertencem.
2. Na área de trabalho do grupo, selecione a guia **Políticas**.
3. Clique duas vezes para abrir a janela de propriedades da política.

4. Na janela **Propriedades** da política, selecione a seção **Certificados**.

5. Clique no botão **Adicionar** na seção **Certificados**.

   A janela **Certificado** abre.

6. No campo **Nome do arquivo**, especifique o caminho para o certificado:

   > Os arquivos de certificados PKCS#1 têm as extensões cer, crt ou der. Os arquivos de certificados PKCS#12 têm as extensões p12 ou pfx.

7. Clique em **Abrir**.

   Se o certificado for protegido por senha, especifique a senha. O novo certificado é exibido na lista.

8. Clique no botão **Aplicar** para salvar as alterações efetuadas.

Como resultado, após a aplicação da política, será solicitado ao usuário que instale certificados da lista que foi criada.

Adicionar um perfil SCEP aos dispositivos iOS MDM

É preciso adicionar um perfil SCEP para permitir que o usuário do dispositivo iOS MDM receba automaticamente os certificados do centro de certificação por meio da Internet. O perfil SCEP permite suporte do Simple Certificate Enrollment Protocol.

Um perfil SCEP com as configurações seguintes é adicionado por padrão:

- O nome de sujeito alternativo não é usado para registrar certificados.
- São efetuadas três tentativas com uma diferença de 10 segundos entre si para checar o servidor SCEP. Se todas as tentativas de assinar o certificado falharem, você precisa gerar uma nova solicitação de assinatura do certificado.
- O certificado que foi recebido não pode ser usado para assinatura ou criptografia de dados.

Você pode editar as configurações especificadas ao adicionar o perfil SCEP.

Para adicionar um perfil SCEP:

1. No árvore do console, na pasta **Dispositivos gerenciados**, selecione o grupo de administração ao qual os dispositivos iOS MDM pertencem.

2. Na área de trabalho do grupo, selecione a guia **Políticas**.

3. Clique duas vezes para abrir a janela de propriedades da política.

4. Na janela **Propriedades** da política, selecione a seção **SCEP**.

5. Clique no botão **Adicionar** na seção **Perfis SCEP**.

   A janela **Perfil SCEP** é exibida.

6. No campo **Endereço do servidor da Web**, insira o endereço da Web do servidor SCEP onde o Centro de Certificação será implementado.

O URL pode conter o endereço IP ou o nome de domínio completo (FQDN). Por exemplo: http://10.10.10.10/certserver/companyscep.

7. No campo **Nome**, insira o nome do Centro de Certificação implementado no servidor SCEP.

8. No campo **Assunto**, insira uma cadeia com os atributos do usuário do dispositivo iOS MDM que estão incluídos no certificado X.500.

   Atributos contêm informações sobre o país (C), organização (O) e nome comum do usuário (CN). Por exemplo: /C=RU/O=MyCompany/CN=User/. Você também pode utilizar outros atributos especificados no RFC 5280.

9. Na lista suspensa **Tipo de nome alternativo do sujeito**, selecione o tipo de nome alternativo do sujeito no servidor SCEP:

   - **Não** – a identificação de nome alternativo não é utilizada.
   - **Nome RFC 822** – identificação utilizando o endereço de e-mail. O endereço de e-mail deve ser especificado de acordo com o RFC 822.
   - **Nome DNS** – identificação utilizando o nome de domínio.
   - **URI** – identificação utilizando o endereço IP ou endereço no formato FQDN.

   Você pode utilizar um nome alternativo para o sujeito para identificar o usuário do dispositivo móvel iOS MDM.

10. No campo **Nome alternativo do sujeito**, insira o nome alternativo do sujeito do certificado X.500. O valor do nome alternativo do sujeito depende do tipo de sujeito: o endereço de e-mail do usuário, domínio ou endereço da Web.

11. No campo **Nome do assunto NT**, insira o nome DNS do usuário do dispositivo móvel iOS MDM na rede Windows NT.

    O nome do assunto NT está contido na solicitação do certificado enviada ao servidor SCEP.

12. No campo **Número de tentativas de amostragem no servidor SCEP**, especifique o número máximo de tentativas para checar o servidor SCEP para obter o certificado assinado.

13. No campo **Frequência de tentativas (seg)**, especifique o período em segundos entre as tentativas para checar o servidor SCEP para obter o certificado assinado.

14. No campo **Solicitação de registro**, insira uma chave de registro pré-publicada.

    Antes de assinar um certificado, o servidor SCEP solicita que o usuário do dispositivo móvel forneça uma chave. Se este campo estiver em branco, o SCEP não solicita a chave.

15. Na lista suspensa **Tamanho da chave**, selecione o tamanho da chave de registro em bits: 1024 ou 2048.

16. Se você desejar permitir que o usuário use um certificado recebido do servidor SCEP como assinar o certificado, selecione a caixa **Usar para assinar**.

17. Se você desejar permitir que o usuário use um certificado recebido do servidor SCEP para criptografia de dados, selecione a caixa **Usar para descriptografar**.

    É proibido utilizar o certificador do servidor SCEP como um certificado de assinatura de dados e um certificado de criptografia de dados ao mesmo tempo.

18. No campo **Impressão digital do certificado**, insira uma impressão digital de certificado para verificar a autenticidade da resposta do Centro de Certificação. Você pode utilizar impressões digitais de certificado com o algoritmo de hash SHA-1 ou MD5. Você pode copiar a impressão digital do certificado manualmente ou selecionar um certificado utilizando o botão **Criar a partir do certificado...**. Quando a impressão digital é criada utilizando o botão **Criar a partir do certificado...**, a impressão digital é adicionada ao campo automaticamente.

    A impressão digital do certificado precisa ser especificada se a troca de dados entre o dispositivo móvel e o Centro de certificação ocorre por meio de um protocolo HTTP.

19. Clique em **OK**.

    O novo perfil SCEP é exibido na lista.

20. Clique no botão **Aplicar** para salvar as alterações efetuadas.

Como resultado, após a política ser aplicada, o dispositivo móvel do usuário é configurado automaticamente para receber um certificado a partir do centro de certificação por meio da Internet.

Controle

Esta seção contém informações sobre como monitorar remotamente dispositivos móveis no Console de Administração do Kaspersky Security Center.

Configurar restrições

Esta seção fornece instruções sobre como configurar o acesso do usuário aos recursos dos dispositivos móveis.

Considerações especiais para dispositivos com Android versões 10 e posteriores

O Android 10 introduziu diversas mudanças e restrições em relação ao API 29 ou superior. Algumas destas mudanças afetam a disponibilidade ou funcionalidade de determinados recursos do aplicativo. Estas considerações se aplicam somente a dispositivos com Android 10 ou posterior.

Capacidade de ativar, desativar e configurar a Wi-Fi

- Redes Wi-Fi podem ser adicionadas, excluídas e configuradas no Console de Administração do Kaspersky Security Center. Quando uma rede Wi-Fi é adicionada a uma política, o Kaspersky Endpoint Security recebe a configuração dessa rede assim que se ela conecta pela primeira vez com o Kaspersky Security Center.

- Quando um dispositivo detecta uma rede configurada por meio do Kaspersky Security Center, o Kaspersky Endpoint Security solicita ao usuário que se conecte a essa rede. Caso o usuário escolha conectar-se à rede, todas as configurações definidas por meio do Kaspersky Security Center serão automaticamente aplicadas. O dispositivo então passa a se conectar automaticamente à rede quando estiver em seu raio de alcance, sem exibir nenhuma notificação ao usuário.

- Se o dispositivo do usuário já estiver conectado a outra rede Wi-Fi, às vezes o usuário pode não receber a mensagem de solicitação para aprovar a adição de uma rede. Nesse caso, o usuário deve desligar a Wi-Fi e ligá-la novamente para receber a sugestão.

- Quando o Kaspersky Endpoint Security sugere que o usuário se conecte a uma rede Wi-Fi e o usuário se recusa, a permissão do aplicativo para mudar o estado da Wi-Fi é revogada. Assim, o Kaspersky Endpoint Security não pode mais sugerir a conexão com redes Wi-Fi até que o usuário conceda a permissão novamente acessando **Configurações → Aplicativos e notificações → Acesso especial de aplicativos → Controle de Wi-Fi → Kaspersky Endpoint Security**.

- Somente redes abertas e redes criptografadas com WPA2-PSK possuem suporte. Criptografias WEP e WPA não possuem suporte.

- Se a senha para uma rede sugerida anteriormente pelo aplicativo for alterada, o usuário deve excluir manualmente essa rede da lista de redes conhecidas. Desta forma, o dispositivo poderá receber uma nova sugestão de rede do Kaspersky Endpoint Security e conectar-se a ela.

- Quando o SO de um dispositivo é atualizado do Android versão 9 ou anterior para o Android 10 ou posterior, e/ou o Kaspersky Endpoint Security instalado em um dispositivo com Android versão 10 ou posterior é atualizado, as redes adicionadas anteriormente via Kaspersky Security Center não podem ser modificadas ou excluídas por meio das políticas do Kaspersky Security Center. Porém, o usuário pode modificar ou excluir essas redes manualmente nas configurações do dispositivo.

- Em dispositivos com Android 10, o usuário recebe uma solicitação de senha ao tentar se conectar manualmente a uma rede protegida sugerida. A conexão automática não requer inserção da senha. Se o dispositivo de um usuário estiver conectado a outra rede Wi-Fi, o usuário deve primeiro se desconectar dessa rede para se conectar automaticamente a uma das redes sugeridas.

- Em dispositivos com Android 11, o usuário pode se conectar manualmente a uma rede protegida sugerida pelo aplicativo sem inserir a senha.

- Quando o Kaspersky Endpoint Security é removido do dispositivo, as redes anteriormente sugeridas pelo aplicativo são ignoradas.

- Não há suporte para a proibição do uso de redes Wi-Fi.

Acesso à câmera

- Em dispositivos com Android 10, o uso da câmera não pode ser totalmente proibido. Contudo, é possível proibir o uso da câmera para o perfil de trabalho.

- Se um aplicativo de terceiros tentar acessar a câmera do dispositivo, o aplicativo será bloqueado e o usuário será notificado. No entanto, os aplicativos que usam a câmera enquanto estão em execução em segundo plano não podem ser bloqueados.

- Quando uma câmera externa for desconectada de um dispositivo, uma notificação sobre a indisponibilidade da câmera pode ser exibida em alguns casos.

Gerenciamento de métodos de desbloqueio de tela

- O Kaspersky Endpoint Security agora divide os requisitos da força de segurança da senha em um dos valores do sistema: médio ou alto.

    - Se a quantidade de símbolos exigida for de 1 a 4, então o aplicativo solicita ao usuário que defina uma senha de força média. Ela deve ser numérica (PIN), sem números repetidos ou sequenciais (ex. 1234), ou alfanumérica. O PIN ou a senha deve ter no mínimo 4 caracteres.

    - Se o número de símbolos exigidos for 5 ou mais, então o aplicativo solicita ao usuário que defina uma senha de segurança alta. Ela deve ser numérica (PIN), sem números repetidos ou sequenciais, ou alfanumérica

(senha). O PIN deve ter no mínimo 8 dígitos; a senha deve ter no mínimo 6 caracteres.

- O uso das digitais para desbloquear a tela pode ser disponibilizado somente para o perfil de trabalho.

Configurar as restrições para dispositivos Android

Para manter um dispositivo Android seguro, defina as configurações de uso do Wi-Fi, da câmera e do Bluetooth no dispositivo.

Por padrão, o usuário pode usar o Wi-Fi, a câmera e o Bluetooth no dispositivo sem restrições.

Para configurar as restrições de uso do Wi-Fi, da câmera e do Bluetooth no dispositivo:

1. No árvore do console, na pasta **Dispositivos gerenciados**, selecione o grupo de administração ao qual os dispositivos Android pertencem.
2. Na área de trabalho do grupo, selecione a guia **Políticas**.
3. Clique duas vezes em qualquer coluna para abrir a janela de propriedades da política.
4. Na janela **Propriedades** da política, selecione a seção **Gerenciamento do dispositivo**.
5. Na seção **Restrições**, configure o uso de Wi-Fi, da câmera e do Bluetooth:
   - Para desativar o módulo Wi-Fi no dispositivo móvel do usuário, selecione a caixa de seleção **Proibir o uso do Wi-Fi**.

     Em dispositivos Android 10.0 ou posteriores, a proibição do uso de redes Wi-Fi não é compatível.

   - Para desativar a câmera no dispositivo móvel do usuário, selecione a caixa de seleção **Proibir o uso da câmera**.

     Em dispositivos Android 10.0 ou posteriores, o uso da câmera não pode ser totalmente proibido.

     Nos dispositivos que executam o Android 11 ou posterior, o Kaspersky Endpoint Security for Android deve ser definido como um recurso de Acessibilidade. O Kaspersky Endpoint Security for Android solicita que o usuário defina o aplicativo como um recurso de Acessibilidade pelo Assistente de Configuração Inicial. O usuário pode ignorar esta etapa ou desativar este serviço nas configurações de dispositivo em um momento posterior. Nesse caso, não será possível restringir o uso da câmera.

   - Para desativar o Bluetooth no dispositivo móvel do usuário, marque a caixa de seleção **Proibir o uso do Bluetooth**.

     No Android 12 ou posterior, o uso do Bluetooth pode ser desabilitado somente se o usuário do dispositivo tiver concedido a permissão **Dispositivos Bluetooth por perto**. O usuário pode conceder essa permissão durante o Assistente de Configuração Inicial ou posteriormente.

6. Clique no botão **Aplicar** para salvar as alterações efetuadas.

As configurações do dispositivo móvel são definidas depois da próxima sincronização do dispositivo com o Kaspersky Security Center.

Configurar restrições da funcionalidade de dispositivos iOS MDM

Para garantir a conformidade com os requisitos de segurança corporativa, configure as restrições na operação do dispositivo iOS MDM.

Para configurar as restrições da funcionalidade de dispositivos iOS MDM:

1. No árvore do console, na pasta **Dispositivos gerenciados**, selecione o grupo de administração ao qual os dispositivos iOS MDM pertencem.
2. Na área de trabalho do grupo, selecione a guia **Políticas**.
3. Clique duas vezes para abrir a janela de propriedades da política.
4. Na janela **Propriedades** da política, selecione a seção **Restrições de funções**.
5. Na seção **Configurações de restrições de funções**, selecione a caixa **Aplicar as configurações no dispositivo**.
6. Configure restrições da funcionalidade de dispositivos iOS MDM.
7. Clique no botão **Aplicar** para salvar as alterações efetuadas.
8. Selecione a seção **Restrições para aplicativos**.
9. Na seção **Configurações de restrição dos aplicativos**, selecione a caixa **Aplicar as configurações no dispositivo**.
10. Configure as restrições para aplicativos do dispositivo iOS MDM.
11. Clique no botão **Aplicar** para salvar as alterações efetuadas.
12. Selecione a seção **Restrições para conteúdo da mídia**.
13. Na seção **Configurações de restrição de conteúdo da mídia**, selecione a caixa **Aplicar as configurações no dispositivo**.
14. Configure as restrições para conteúdo de mídia no dispositivo iOS MDM.
15. Clique no botão **Aplicar** para salvar as alterações efetuadas.

Como resultado, após a aplicação da política, as restrições de funcionalidades, aplicativos e conteúdo de mídia serão configuradas no dispositivo móvel do usuário.

Configurar restrições da funcionalidade de dispositivos EAS

Configure as restrições na funcionalidade de dispositivos para manter um dispositivo EAS seguro.

Por padrão, o usuário pode usar funcionalidades de um dispositivo EAS sem restrições.

Para configurar restrições na funcionalidade de dispositivos EAS:

1. No árvore do console, na pasta **Dispositivos gerenciados**, selecione o grupo de administração ao qual os dispositivos EAS pertencem.

2. Na área de trabalho do grupo, selecione a guia **Políticas**.

3. Clique duas vezes para abrir a janela de propriedades da política.

4. Na janela Propriedades da política, selecione a seção **Restrições de funções**.

5. Na seção **Configurações de restrições de funções**, permita ou bloqueie o uso das funcionalidades do dispositivo EAS:

   - Para permitir conectar cartões de memória e outras unidades removíveis com um dispositivo selecione a caixa de seleção **Permitir discos removíveis**.

   - Para permitir o uso da câmera, selecione a caixa de seleção **Permitir o uso da câmera**.

   - Para permitir conexões Wi-Fi, selecione a caixa de seleção **Permitir o uso do Wi-Fi**.

   - Para permitir o uso da porta de conexão infravermelho, selecione a caixa de seleção **Permitir a conexão infravermelho**.

   - Para permitir que o usuário use um dispositivo como um ponto de acesso Wi-Fi para criar uma rede sem fio, selecione a caixa de seleção **Permitir o uso do dispositivo como ponto de acesso Wi-Fi**.

   - Para permitir que o dispositivo se conecte com um desktop remoto, selecione a caixa de seleção **Permitir a conexão de área de trabalho remota**.

   - Para permitir que o usuário use o cliente Desktop ActiveSync no dispositivo, selecione a caixa de seleção **Permitir a sincronização com o desktop**.

   - Na lista suspensa **Uso do Bluetooth**, permita ou bloqueie o uso de Bluetooth no dispositivo EAS:

     - **Permitir**. A utilização de Bluetooth no dispositivo móvel é permitida.

     - **Ao usar mãos livres**. O uso de Bluetooth é permitido quando auscultadores sem fio são conectados com o dispositivo móvel.

     - **Negar**. A utilização de Bluetooth no dispositivo móvel está bloqueada.

6. Clique no botão **Aplicar** para salvar as alterações efetuadas.

As configurações do dispositivo móvel são definidas depois da próxima sincronização do dispositivo com o Kaspersky Security Center.

Configurar o acesso do usuários aos sites

Esta seção contém instruções sobre como configurar o acesso aos sites em dispositivos Android e iOS.

Configurar o acesso a sites no dispositivos Android

Você pode usar a Proteção na Web para configurar o acesso de usuários de dispositivo Android a sites. A Proteção na Web é compatível com a filtragem de sites por categorias definidas no serviço na nuvem da Kaspersky Security Network. A filtragem permite restringir o acesso do usuário a determinadas categorias de sites (por exemplo, os das categorias de "Jogos de azar, loterias, apostas" ou "Comunicações via Internet"). A Proteção na Web também protege os dados pessoais de usuários na Internet.

O Kaspersky Endpoint Security for Android deve ser definido como um Recursos de Acessibilidade. O Kaspersky Endpoint Security for Android solicita que o usuário defina o aplicativo como um recurso de Acessibilidade pelo Assistente de Configuração Inicial. O usuário pode ignorar esta etapa ou desativar este serviço nas configurações de dispositivo em um momento posterior. Se este for o caso, a Proteção na Web não será executada.

· A Proteção na Web nos dispositivos Android funciona apenas nos navegadores Google Chrome (incluindo o recurso Guias personalizadas), Huawei Browser e Samsung Internet. A Proteção na Web para Samsung Internet Browser não bloqueia sites em um dispositivo móvel se um perfil de trabalho for usado e a Proteção na Web estiver ativada apenas para o perfil de trabalho.

A Proteção na Web está ativada por padrão: o acesso do usuário a sites nas categorias **Phishing** e **Malware** está bloqueado.

Para especificar as configurações do acesso do usuário do dispositivo a sites:

1. No árvore do console, na pasta **Dispositivos gerenciados**, selecione o grupo de administração ao qual os dispositivos Android pertencem.
2. Na área de trabalho do grupo, selecione a guia **Políticas**.
3. Clique duas vezes em qualquer coluna para abrir a janela de propriedades da política.
4. Na janela **Propriedades** da política, selecione **Proteção na Web**.
5. Selecione a caixa de seleção **Ativar a Proteção na Web**.
6. Para usar a Proteção na Web, você ou o usuário do dispositivo deve ler e aceitar a Declaração relativa ao processamento de dados com o propósito de usar a Proteção na Web (Declaração de Proteção na Web):
   a. Clique no link **Declaração da Proteção na Web**.

      Isso abre a janela **Declaração relativa ao processamento de dados com o propósito de usar a Proteção na Web**. Para aceitar a Declaração da Proteção na Web, você deve ler e aceitar a Política de Privacidade.

   b. Clique no link Política de Privacidade. Leia e aceite a Política de Privacidade.

      Se você não aceitar a Política de Privacidade, o usuário do dispositivo móvel poderá aceitar a Política de Privacidade no Assistente de Configuração Inicial ou no aplicativo (→ **Sobre o aplicativo** → **Termos e condições** → **Política de Privacidade**).

   c. Selecione o modo de aceitação da Declaração da Proteção na Web:

      - **Li e aceito a Declaração de Proteção na Web**
      - **Solicitar a aceitação da Declaração de Proteção na Web do usuário do dispositivo**
      - **Não aceito a Declaração da Proteção na Web**

Se você selecionar **Eu não aceito a Declaração de Proteção na Web**, a Proteção na Web não bloqueará sites em um dispositivo móvel. O usuário do dispositivo móvel não pode ativar a Proteção na Web no Kaspersky Endpoint Security.

7. Se você desejar que o aplicativo restrinja o acesso do usuário a sites dependendo do seu conteúdo, faça o seguinte:

   a. Na seção **Proteção na Web**, selecione na lista suspensa **Os sites das categorias selecionadas são proibidos**.

   b. Crie uma lista de categorias bloqueadas marcando as caixas de seleção ao lado das categorias de sites cujo acesso ao aplicativo será bloqueado.

8. Se você desejar que o aplicativo permita o acesso do usuário apenas aos sites especificados pelo administrador, faça o seguinte:

   a. Na seção **Proteção na Web**, selecione **Apenas sites listados são permitidos** na lista suspensa.

   b. Crie uma lista de sites adicionando endereços cujo acesso ao aplicativo não será bloqueado. O Kaspersky Endpoint Security for Android é compatível somente com expressões regulares. Ao inserir o endereço de um site permitido, use os seguintes modelos:

      - `http:\/\/www\.example\.com.*`—Todas as páginas secundárias do site são permitidas (por exemplo, `http://www.example.com/about`).

      - `https:\/\/.*example\.com`—Todas as páginas de subdomínio do site são permitidas (por exemplo, `https://pictures.example.com`).

      Você também pode usar a expressão `https?` para selecionar protocolos HTTP e HTTPS. Para obter mais detalhes sobre expressões regulares, consulte o site de Suporte Técnico da Oracle.

9. Se desejar que o aplicativo bloqueie o acesso do usuário a todos os sites, na seção **Proteção na Web**, selecione **Todos os sites estão bloqueados** na lista suspensa.

10. Para suspender as restrições baseadas em conteúdo sobre o acesso do usuário a sites, desmarque a caixa de seleção **Ativar a Proteção na Web**.

11. Clique no botão **Aplicar** para salvar as alterações efetuadas.

As configurações do dispositivo móvel são definidas depois da próxima sincronização do dispositivo com o Kaspersky Security Center.

Configurar o acesso a sites no dispositivos iOS MDM do usuário:

Configure a Proteção na Web para controlar acesso a sites para usuários de dispositivo iOS MDM. A Proteção na Web controla o acesso de um usuário a sites com base em listas de sites permitidos e bloqueados. A Proteção na Web também permite adicionar marcadores de sites no painel de marcadores no Safari.

Por padrão, o acesso a sites não é restrito.

A Proteção na Web pode ser configurada somente para dispositivos supervisionados.

Para configurar o acesso a sites no dispositivo iOS MDM do usuário:

1. No árvore do console, na pasta **Dispositivos gerenciados**, selecione o grupo de administração ao qual os dispositivos iOS MDM pertencem.

2. Na área de trabalho do grupo, selecione a guia **Políticas**.

3. Clique duas vezes para abrir a janela de propriedades da política.

4. Na janela **Propriedades** da política, selecione a seção **Proteção na Web**.

5. Na seção **Configurações da Proteção na Web**, selecione a caixa **Aplicar as configurações no dispositivo**.

6. Para bloquear o acesso a sites bloqueados e permitir o acesso a sites permitidos:

   a. Na lista suspensa **Modo de filtro da Web**, selecione o modo **Limitar conteúdo adulto**.

   b. Na seção **Sites permitidos**, crie uma lista de sites permitidos.

      O endereço do site deve começar com `"http://"` ou `"https://"`. O Kaspersky Device Management for iOS permite acessar todos os sites no domínio. Por exemplo, se você adicionou http://www.example.com à lista de sites permitidos, acesso é permitido para http://pictures.example.com e http://example.com/movies. Se a lista de sites permitidos estiver vazia, o aplicativo permite o acesso a todos os sites, exceto aqueles incluídos na lista de sites bloqueados.

   c. Na seção **Sites proibidos**, crie uma lista de sites bloqueados.

      O endereço do site deve começar com `"http://"` ou `"https://"`. O Kaspersky Device Management for iOS bloqueia o acesso a todos os sites no domínio.

7. Para bloquear o acesso a todos os sites exceto os sites permitidos na lista:

   a. Na lista suspensa **Modo de filtro da Web**, selecione o modo **Permitir somente os sites favoritos**.

   b. Na seção **Favoritos**, crie uma lista de marcadores de sites permitidos.

      O endereço do site deve começar com `"http://"` ou `"https://"`. O Kaspersky Device Management for iOS permite acessar todos os sites no domínio. Se a lista de favoritos estiver vazia, o aplicativo permite o acesso a todos os sites. O Kaspersky Device Management for iOS adiciona sites da lista de favoritos na guia de marcadores do Safari no dispositivo móvel do usuário.

8. Clique no botão **Aplicar** para salvar as alterações efetuadas.

Como resultado, após a aplicação da política, a Proteção na Web será configurada no dispositivo móvel do usuário de acordo com o modo selecionado e as listas criadas.

Controle de conformidade de dispositivos Android com requisitos de segurança corporativa

Você pode controlar os dispositivos Android quanto à conformidade com os requisitos de segurança corporativa. Os requisitos de segurança corporativa regulam como o usuário pode trabalhar com o dispositivo. Por exemplo, a proteção em tempo real deve ser ativada no dispositivo, os bancos de dados antivírus devem estar atualizados, e a senha do dispositivo deve ser suficientemente forte. O controle de conformidade tem base em uma lista de regras. Uma regra de conformidade inclui os seguintes componentes:

- Critério de verificação do dispositivo (por exemplo, ausência de aplicativos bloqueados no dispositivo).

- Período do tempo alocado para o usuário para corrigir a não conformidade (por exemplo, 24 horas).

- A ação que será executada no dispositivo se o usuário não corrigir a não conformidade dentro do período do tempo definido (por exemplo, bloqueio do dispositivo).

  No Android 12 ou posterior, o aplicativo pode realizar essa tarefa após o especificado se o dispositivo estiver no modo de economia de bateria.

Se o usuário não corrigir a não conformidade dentro do tempo especificado, as seguintes ações estão disponíveis:

- **Bloquear todos os aplicativos com exceção dos do sistema**. Todos os aplicativos no dispositivo móvel do usuário são bloqueados contra inicialização, com exceção dos aplicativos do sistema.
- **Bloquear dispositivo**. O dispositivo móvel é bloqueado. Para obter o acesso aos dados, você deve desbloquear o dispositivo. Se o motivo para bloquear o dispositivo não for corrigido depois que o dispositivo for desbloqueado, o dispositivo será novamente bloqueado após o período especificado.
- **Limpar os dados corporativos**. Limpar os dados em contêiner, conta de e-mail corporativo, configurações para conectar à rede Wi-Fi corporativa e VPN, nome do ponto de acesso (APN), perfil de trabalho do Android, contêiner KNOX e a chave do Gerenciador de licença KNOX.
- **Redefinição completa**. Todos os dados são excluídos do dispositivo móvel e as configurações são revertidas aos valores de fábrica. Após esta ação ter sido concluída, o dispositivo não mais será um dispositivo gerenciado. Para conectar o dispositivo ao Kaspersky Security Center, você deve reinstalar o Kaspersky Endpoint Security for Android.

Para criar uma regra de verificação para verificar dispositivos quanto à conformidade com uma política do grupo:

1. No árvore do console, na pasta **Dispositivos gerenciados**, selecione o grupo de administração ao qual os dispositivos Android pertencem.
2. Na área de trabalho do grupo, selecione a guia **Políticas**.
3. Clique duas vezes em qualquer coluna para abrir a janela de propriedades da política.
4. Na janela **Propriedades** da política, selecione a seção **Controle de conformidade**.
5. Para receber notificações sobre os dispositivos que não estão em conformidade com a política, na seção **Notificação de não conformidade**, selecione a caixa de seleção **Notificar o administrador**.

   Se o dispositivo não estiver em conformidade com uma política, durante a sincronização do dispositivo com o Servidor de Administração, o Kaspersky Endpoint Security for Android gera uma entrada para **Violação detectada: <name of the criterion checked>** no registro de eventos. Você pode exibir o Registro de eventos na guia **Eventos** nas propriedades do Servidor de Administração ou nas propriedades locais do aplicativo.
6. Para notificar o usuário do dispositivo que o dispositivo móvel do usuário não está em conformidade com a política, na seção **Notificação de não conformidade**, selecione a caixa de seleção **Notificar o usuário**.

   Quando o dispositivo não estiver em conformidade com a política durante a sincronização do dispositivo com o Servidor de Administração, o Kaspersky Endpoint Security for Android notifica o usuário sobre isso na seção **Status**.
7. Na seção **Regras de conformidade**, compile uma lista de regras para verificar o dispositivo quanto à conformidade com a política. Siga as etapas abaixo:

   a. Clique em **Adicionar**.

      O assistente Regras de verificação é iniciado.

   b. Siga as instruções no assistente Regras de verificação.

Quando o assistente terminar, a nova regra é exibida na seção **Regras de conformidade** na lista de regras de verificação.

8. Para desativar temporariamente uma regra de verificação que você tiver criado, use o botão de seleção junto de cada regra selecionada.

9. Clique no botão **Aplicar** para salvar as alterações efetuadas.

As configurações do dispositivo móvel são definidas depois da próxima sincronização do dispositivo com o Kaspersky Security Center. Se o dispositivo do usuário não estiver em conformidade com as regras, as restrições que você especificou na lista de regras de verificação são aplicadas ao dispositivo.

Controle de Inicialização de Aplicativo

Esta seção contém instruções sobre como configurar o acesso do usuário aos aplicativos em um dispositivo móvel.

Controle de Inicialização de Aplicativos em dispositivos Android

Para manter o dispositivo móvel do usuário seguro, você deve definir as configurações de inicialização de aplicativos no dispositivo.

Você pode impor restrições na atividade do usuário em um dispositivo no qual os aplicativos bloqueados estão instalados ou os aplicativos necessários não estão instalados (por exemplo, bloquear o dispositivo). Você pode impor restrições usando o componente Controle de conformidade. Para fazer isso, nas configurações da regra de verificação, você deve selecionar o critério **Aplicativos proibidos estão instalados**, **Aplicativos de categorias proibidas estão instalados** ou **Nem todos os aplicativos obrigatórios estão instalados**.

O Kaspersky Endpoint Security for Android deve ser definido como um recurso de acessibilidade para assegurar o funcionamento apropriado do Controle de aplicativos. O Kaspersky Endpoint Security for Android solicita que o usuário defina o aplicativo como um recurso de Acessibilidade pelo Assistente de Configuração Inicial. O usuário pode ignorar esta etapa ou desativar este serviço nas configurações de dispositivo em um momento posterior. Se esse for o caso, o Controle do Aplicativo não será executado.

Para especificar as configurações de inicialização do aplicativo no dispositivo móvel:

1. No árvore do console, na pasta **Dispositivos gerenciados**, selecione o grupo de administração ao qual os dispositivos Android pertencem.

2. Na área de trabalho do grupo, selecione a guia **Políticas**.

3. Clique duas vezes em qualquer coluna para abrir a janela de propriedades da política.

4. Na janela **Propriedades** da política, selecione a seção **Controle de aplicativos**.

5. Na seção **Modo de operação**, selecione o modo de inicialização do aplicativo no dispositivo móvel do usuário:

   - Para permitir que o usuário inicie todos os aplicativos, exceto os aplicativos especificados na lista de categorias e aplicativos como aplicativos bloqueados, selecione o modo **Aplicativos bloqueados**.

   - Para permitir que o usuário somente inicie aplicativos especificados na Lista de categorias e aplicativos, como aplicativos permitidos, recomendados ou requeridos, selecione o modo **Aplicativos permitidos**.

6. Se você quiser que o Kaspersky Endpoint Security for Android envie dados sobre aplicativos proibidos ao registro de eventos sem bloqueá-los, selecione a caixa de seleção **Não bloquear aplicativos proibidos, somente escreva no registro de eventos**.

   Durante a sincronização do dispositivo móvel do usuário com o Servidor de Administração, o Kaspersky Endpoint Security for Android gera uma entrada para **Um aplicativo proibido foi instalado** no registro de eventos. Você pode exibir o Registro de eventos na guia **Eventos** nas propriedades do Servidor de Administração ou nas propriedades locais do aplicativo.

7. Se você desejar que o Kaspersky Endpoint Security for Android bloqueie a inicialização de aplicativos do sistema no dispositivo móvel do usuário (tal como Calendário, Câmera e Configurações), no modo **Aplicativos permitidos**, selecione a caixa de seleção **Bloquear aplicativos do sistema**.

   Os especialistas da Kaspersky recomendam não bloquear os aplicativos do sistema porque isso pode levar a falhas na operação do dispositivo.

8. Crie uma lista de categorias e aplicativos para configurar a inicialização de aplicativos.

   Para obter detalhes sobre as categorias de aplicativos, consulte os Apêndices.

   Para obter uma lista dos aplicativos que pertencem a cada categoria, visite o site da Kaspersky.

9. Clique no botão **Aplicar** para salvar as alterações efetuadas.

As configurações do dispositivo móvel são definidas depois da próxima sincronização do dispositivo com o Kaspersky Security Center.

Configurar as restrições de dispositivo EAS para aplicativos

Para manter o dispositivo EAS protegido, configure restrições de atividade do aplicativo (navegador, aplicativos não atribuídos).

Por padrão, o usuário pode usar aplicativos no dispositivo EAS sem restrições.

Para configurar restrições na atividade de aplicativos no dispositivo EAS:

1. No árvore do console, na pasta **Dispositivos gerenciados**, selecione o grupo de administração ao qual os dispositivos EAS pertencem.

2. Na área de trabalho do grupo, selecione a guia **Políticas**.

3. Clique duas vezes para abrir a janela de propriedades da política.

4. Na janela Propriedades da política, selecione a seção **Restrições para aplicativos**.

5. Na seção **Configurações de restrição dos aplicativos**, configure as restrições de atividade do aplicativo:

   - Para permitir que o usuário use o navegador, selecione a caixa de seleção **Permitir o uso do navegador**.

   - Para permitir que o usuário crie contas de e-mail pessoais (POP3 ou IMAP4), selecione a caixa **Permitir o correio pessoal**.

   - Para permitir que o usuário inicie aplicativos que não foram assinados com um certificado de autenticação, selecione a caixa **Permitir aplicativos não assinados**.

- Para permitir que o usuário instale aplicativos que não foram assinados com um certificado de autenticação, selecione a caixa **Permitir a instalação de pacotes não assinados**.

6. Clique no botão **Aplicar** para salvar as alterações efetuadas.

As configurações do dispositivo móvel são definidas depois da próxima sincronização do dispositivo com o Kaspersky Security Center.

Inventário de software em dispositivos Android

Você pode inventariar os aplicativos nos dispositivos Android conectados ao Kaspersky Security Center. O Kaspersky Endpoint Security for Android recebe informações sobre todas os aplicativos instalados nos dispositivos móveis. As informações coletadas durante o inventário são exibidas nas propriedades do dispositivo, na seção **Eventos**. Você pode exibir a informação detalhada sobre cada aplicativo instalado, inclusive a sua versão e publicador.

Para ativar o inventário de software:

1. No árvore do console, na pasta **Dispositivos gerenciados**, selecione o grupo de administração ao qual os dispositivos Android pertencem.

2. Na área de trabalho do grupo, selecione a guia **Políticas**.

3. Clique duas vezes em qualquer coluna para abrir a janela de propriedades da política.

4. Na janela **Propriedades** da política, selecione a seção **Controle de aplicativos**.

5. Na seção **Inventário de software**, selecione a caixa de seleção **Enviar dados sobre os aplicativos instalados**.

6. Clique no botão **Aplicar** para salvar as alterações efetuadas.

As configurações do dispositivo móvel são definidas depois da próxima sincronização do dispositivo com o Kaspersky Security Center. O Kaspersky Endpoint Security for Android envia dados ao log de eventos cada vez que um aplicativo é instalado ou removido do dispositivo.

Configurar a exibição de dispositivos Android no Kaspersky Security Center

Para operações convenientes com a lista de dispositivos móveis, você deve definir as configurações para exibir dispositivos no Kaspersky Security Center. Por padrão, a lista de dispositivos móveis é exibida na árvore do console **Adicional → Gerenciamento de dispositivo móvel → Dispositivos móveis**. As informações do dispositivo são atualizadas automaticamente. Você também pode atualizar manualmente a lista de dispositivos móveis ao clicar no botão **Atualizar** no canto superior direito.

Depois de conectar o dispositivo ao Kaspersky Security Center, os dispositivos são automaticamente adicionados à lista de dispositivos móveis. A lista de dispositivos móveis pode conter informações detalhadas sobre o dispositivo: modelo, sistema operacional, endereço IP e outros.

Você pode configurar o formato do nome do dispositivo e selecionar o status do dispositivo. O status do dispositivo informa você sobre como os componentes do Kaspersky Endpoint Security for Android estão operando no dispositivo móvel do usuário.

Os componentes do Kaspersky Endpoint Security for Android podem não estar operacionais pelos seguintes motivos:

- O usuário desativou o componente nas configurações do dispositivo.
- O usuário não concedeu ao aplicativo as permissões necessárias para o componente para operar (por exemplo, não há permissão para determinar a localização do dispositivo para o comando Antirroubo correspondente).

Para exibir o status do dispositivo, você deve ativar a condição **Determinado pelo aplicativo** nas propriedades do grupo de administração (**Propriedades** → **Status do dispositivo** → **Definir o status para Crítico se** e **Definir o status do dispositivo para Aviso se**). Nas propriedades do grupo de administração, você também pode selecionar outros critérios para formar o status do dispositivo móvel.

Para configurar a exibição de dispositivos Android no Kaspersky Security Center:

1. No árvore do console, na pasta **Dispositivos gerenciados**, selecione o grupo de administração ao qual os dispositivos Android pertencem.
2. Na área de trabalho do grupo, selecione a guia **Políticas**.
3. Clique duas vezes em qualquer coluna para abrir a janela de propriedades da política.
4. Na janela **Propriedades** da política, selecione a seção **Informações do dispositivo**.
5. Na seção **Nome do dispositivo no Kaspersky Security Center**, selecione o formato do nome do dispositivo no Console de Administração:
   - Modelo do dispositivo [e-mail, ID do dispositivo]
   - Modelo do dispositivo [e-mail (se houver) ou ID do dispositivo]

   Um *ID do dispositivo* é um ID exclusivo que o Kaspersky Endpoint Security for Android gera a partir dos dados recebidos de um dispositivo. Para dispositivos móveis com Android 10 ou posterior, o Kaspersky Endpoint Security for Android usa o SSAID (ID do Android) ou checksum de outros dados recebidos do dispositivo. Para versões anteriores do Android, o aplicativo usa o IMEI.
6. Definir o atributo Bloqueio na posição de bloqueado ( ).
7. Na seção **Status do dispositivo no Kaspersky Security Center**, selecione o status apropriado do dispositivo se um componente do Kaspersky Endpoint Security for Android não estiver funcionando: (**Crítico**), (**Aviso**) ou (**OK**).

   Na lista de dispositivos móveis, o status do dispositivo será modificado de acordo com o status selecionado.
8. Definir o atributo Bloqueio na posição de bloqueado.
9. Clique no botão **Aplicar** para salvar as alterações efetuadas.

As configurações do dispositivo móvel são definidas depois da próxima sincronização do dispositivo com o Kaspersky Security Center.

Gerenciamento

Esta seção contém informações sobre como gerenciar remotamente as configurações de dispositivos móveis no Console de Administração do Kaspersky Security Center.

Configurar a conexão à rede Wi-Fi

Esta seção fornece instruções sobre como configurar a conexão automática à uma rede Wi-Fi corporativa em dispositivos Android e iOS MDM.

Conectar dispositivos Android a uma rede Wi-Fi

Para conectar o dispositivo móvel a uma rede Wi-Fi:

1. No árvore do console, na pasta **Dispositivos gerenciados**, selecione o grupo de administração ao qual os dispositivos Android pertencem.
2. Na área de trabalho do grupo, selecione a guia **Políticas**.
3. Clique duas vezes em qualquer coluna para abrir a janela de propriedades da política.
4. Na janela **Propriedades** da política, selecione a seção **Wi-Fi**.
5. Na seção **Redes Wi-Fi**, clique em **Adicionar**.

   Isto abre a janela **Rede Wi-Fi**.
6. No campo **Identificador do conjunto de serviços (SSID)**, insira o nome da rede Wi-Fi que inclua o ponto de acesso (SSID).
7. Na seção **Proteção da rede**, selecione o tipo de segurança da rede Wi-Fi (rede pública ou rede segura protegida por protocolo WEP ou WPA/WPA2 PSK).
8. No campo **Senha**, defina uma senha de acesso a rede se você selecionou uma rede segura na etapa anterior.
9. No campo **Endereço e porta do servidor proxy**, insira o endereço IP ou nome DNS do servidor proxy e número da porta, se necessário.

   Em dispositivos que executam o Android versão 8.0 ou posterior, as configurações do servidor proxy para a Wi-Fi não podem ser redefinidas com a política. No entanto, você pode definir manualmente as configurações de servidor proxy para uma rede Wi-Fi no dispositivo móvel.

   Se você estiver usando um servidor proxy para conectar-se à uma rede Wi-Fi, poderá usar uma política para definir as configurações para conectar-se à rede. Em dispositivos que executam Android 8.0 ou posterior, você deve definir manualmente as configurações de servidor proxy. Em dispositivos que executam Android 8.0 ou posterior, você não pode usar uma política para modificar as configurações de conexão de rede Wi-Fi, exceto a senha de acesso à rede.

   Se você não estiver usando um servidor proxy para conectar-se à uma rede Wi-Fi, não há nenhuma limitação sobre o uso de políticas para gerenciar a conexão à rede Wi-Fi.
10. No campo **Não usar o servidor proxy para os endereços**, gere a lista de endereços da Web que podem ser acessados sem o uso do servidor proxy.

    Por exemplo, você pode inserir o endereço `example.com`. Nesse caso, o servidor proxy não será usado para os endereços `pictures.example.com`, `example.com/movies`, etc. O protocolo (por exemplo, `http://`) pode ser omitido.

Em dispositivos que executam a versão 8.0 Android ou posterior, a exclusão do servidor proxy para endereços da Web não funciona.

11. Clique em **OK**.

    A rede Wi-Fi adicionada é exibida na lista de **Redes Wi-Fi**.

    Você pode modificar ou excluir redes Wi-Fi da lista de redes usando os botões **Editar** e **Excluir** na parte superior da lista.

12. Clique no botão **Aplicar** para salvar as alterações efetuadas.

As configurações do dispositivo móvel são definidas depois da próxima sincronização do dispositivo com o Kaspersky Security Center. Após a política ter sido aplicada no dispositivo móvel, o usuário poderá conectar-se com a rede Wi-Fi que foi adicionada, sem precisar especificar as configurações da rede.

Em dispositivos com Android 10.0 ou posterior, se um usuário se recusar a se conectar à rede Wi-Fi sugerida, a permissão do aplicativo de mudar o estado da Wi-Fi é revogada. O usuário precisa conceder essa permissão manualmente.

Para conectar dispositivos iOS MDM a uma rede Wi-Fi

Para que um dispositivo iOS MDM se conecte automaticamente a uma rede Wi-Fi disponível e proteja os dados durante a conexão, você deve definir as configurações da conexão.

Para configurar a conexão de um dispositivo iOS MDM com uma rede Wi-Fi:

1. No árvore do console, na pasta **Dispositivos gerenciados**, selecione o grupo de administração ao qual os dispositivos iOS MDM pertencem.
2. Na área de trabalho do grupo, selecione a guia **Políticas**.
3. Clique duas vezes para abrir a janela de propriedades da política.
4. Na janela **Propriedades** da política, selecione a seção **Wi-Fi**.
5. Clique no botão **Adicionar** na seção **Redes Wi-Fi**.

   Isto abre a janela **Rede Wi-Fi**.
6. No campo **Identificador do conjunto de serviços (SSID)**, insira o nome da rede Wi-Fi que inclua o ponto de acesso (SSID).
7. Se você desejar que o dispositivo iOS MDM se conecte automaticamente com a rede Wi-Fi, selecione a caixa de seleção **Conexão automática**.
8. Para tornar impossível conectar dispositivos iOS MDM à uma rede Wi-Fi que necessita de autenticação preliminar (rede cativa), selecione a caixa de seleção **Desativar a detecção de redes cativas**.

   Para usar uma rede cativa, você deve assinar, aceitar um contrato ou fazer um pagamento. As redes cativas podem ser implementadas em cafés e hotéis, por exemplo.

9. Se você desejar que a rede Wi-Fi fique oculta na lista de redes disponíveis no dispositivo iOS MDM, selecione a caixa de seleção **Rede oculta**.

   Nesse caso, para conectar-se com a rede, o usuário deve conectar-se manualmente, inserir o SSID da rede especificado nas configurações do roteador Wi-Fi no dispositivo móvel.

10. Na lista suspensa **Proteção da rede**, selecione o tipo de proteção da conexão da rede Wi-Fi:

    - **Desativado**. A autenticação de usuário não é necessária.
    - **WEP**. A rede é protegida utilizando Wireless Encryption Protocol (WEP).
    - **WPA/WPA2 (Pessoal)**. A rede é protegida utilizando protocolo WPA / WPA2 (Wi-Fi Protected Access).
    - **WPA2 (Pessoal)**. A rede é protegida utilizando protocolo WPA2 (Wi-Fi Protected Access 2.0). A proteção WPA2 está disponível para dispositivos móveis executando o iOS versão 8 ou posterior. O WPA2 não está disponível nos dispositivos Apple TV.
    - **Qualquer (Pessoal)**. A rede é protegida utilizando protocolo de criptografia WEP, WPA ou WPA2 dependendo do tipo de roteador de Wi-Fi. Uma chave de criptografia exclusiva para cada usuário é usada para autenticação.
    - **WEP (Dinâmico)**. A rede é protegida utilizando o protocolo WEP com o uso de uma chave dinâmica.
    - **WPA/WPA2 (Corporativo)**. A rede está protegida usando o protocolo de criptografia WPA/WPA2 com o uso do protocolo 802.1X.
    - **WPA2 (Corporativo)**. A rede é protegida utilizando o protocolo de criptografia WPA2 com o uso de uma chave compartilhada por todos os usuários (802.1X). A proteção WPA2 está disponível para dispositivos móveis executando o iOS versão 8 ou posterior. O WPA2 não está disponível nos dispositivos Apple TV.
    - **Qualquer (Corporativo)**. A rede é protegida utilizando protocolo WEP ou WPA/WPA2 dependendo do tipo de roteador Wi-Fi. Uma chave de criptografia compartilhada por todos os usuários é usada para autenticação.

    Se você tiver selecionado **WEP (Dinâmico)**, **WPA/WPA2 (Corporativo)**, **WPA2 (Corporativo)** ou **Qualquer (Corporativo)** na lista **Proteção da rede**, na seção **Protocolos** você pode selecionar os tipos de protocolos EAP (Protocolo de Autenticação Extensível) para a identificação do usuário na rede Wi-Fi.

    Na seção **Certificados confiáveis**, você pode também criar uma lista de certificados confiáveis para autenticação do usuário do dispositivo iOS MDM em servidores confiáveis.

11. Defina as configurações da conta para a autenticação do usuário após a conexão do dispositivo iOS MDM com uma rede Wi-Fi.

    a. Na seção **Autenticação**, clique no botão **Configurar**.

       A janela **Autenticação** abre.

    b. No campo **Nome de usuário**, insira o nome da conta para autenticação do usuário após conexão com a rede Wi-Fi.

    c. Para requerer que o usuário insira a senha manualmente em cada conexão com uma rede sem fio, selecione a caixa de seleção **Solicitar a senha em cada conexão**.

    d. No campo **Senha**, insira a senha da conta para autenticação em uma rede Wi-Fi.

    e. Na lista suspensa **Certificado de autenticação**, selecione um certificado para autenticação do usuário na rede Wi-Fi. Se a lista não contiver nenhum certificado, **você pode adicioná-los na seção** Certificados.

f. No campo **ID do usuário**, insira o ID do usuário exibido durante a transmissão de dados após a autenticação em alternativa ao nome real do usuário.

A ID do usuário é projetada para tornar o processo de autenticação mais seguro, já que o nome de usuário não é exibido abertamente, mas transmitido por meio de um túnel TLS criptografado.

g. Clique em **OK**.

Como resultado, as configurações da conta para a autenticação do usuário ao conectar-se com a rede Wi-Fi serão configuradas no dispositivo iOS MDM.

12. Se necessário, defina as configurações de conexão com a rede Wi-Fi através de um servidor proxy:

a. Na seção **Servidor proxy**, clique no botão **Configurar**.

b. Na janela **Servidor proxy** que é exibida, selecione o modo de configuração do servidor proxy e especifique as configurações de conexão.

c. Clique em **OK**.

Como resultado, as configurações da conexão do dispositivo com uma rede Wi-Fi através de um servidor proxy serão configuradas no dispositivo iOS MDM.

13. Clique em **OK**.

A nova rede Wi-Fi é exibida na lista.

14. Clique no botão **Aplicar** para salvar as alterações efetuadas.

Como resultado, uma conexão com a rede Wi-Fi será configurada no dispositivo iOS MDM do usuário onde a política foi aplicada. O dispositivo móvel do usuário irá automaticamente conectar-se com as redes Wi-Fi disponíveis. A segurança de dados durante uma conexão com a rede Wi-Fi é assegurada pela tecnologia de autenticação.

Configurar o e-mail

Esta seção contém informações sobe a configuração de caixas de correio em dispositivos móveis.

Configurar uma caixa de correio em dispositivos iOS MDM

Para permitir que um usuário de dispositivo iOS MDM trabalhe com o e-mail, adicione a conta de e-mail do usuário à lista de contas no dispositivo iOS MDM.

Por padrão, a conta de e-mail é adicionada com as seguintes configurações:

- Protocolo de e-mail – IMAP.
- O usuário pode mover mensagens de e-mail entre as contas do usuário e sincronizar endereços da conta.
- O usuário pode usar quaisquer clientes de e-mail (que não o Mail) para usar o e-mail.
- A conexão SSL não é usada durante a transmissão de mensagens.

Você pode editar as configurações especificadas ao adicionar a conta.

Para adicionar uma conta de e-mail do usuário do dispositivo iOS MDM:

1. No árvore do console, na pasta **Dispositivos gerenciados**, selecione o grupo de administração ao qual os dispositivos iOS MDM pertencem.
2. Na área de trabalho do grupo, selecione a guia **Políticas**.
3. Clique duas vezes para abrir a janela de propriedades da política.
4. Na janela **Propriedades** da política, selecione **E-mail**.
5. Clique no botão **Adicionar** na seção **Conta de e-mail**.

   A janela **Conta de e-mail** é exibida.
6. No campo **Descrição**, insira uma descrição da conta de e-mail do usuário.
7. Selecione o protocolo de e-mail:

   - **POP**
   - **IMAP**
8. Se necessário, especifique o prefixo do caminho IMAP no campo **Prefixo do caminho IMAP**.

   O prefixo do caminho IMAP deve ser inserido usando letras maiúsculas (por exemplo: GMAIL para o Google Mail). Este campo fica disponível se o protocolo de conta IMAP for selecionado.
9. No campo **Nome de usuário como exibido nas mensagens**, insira o nome de usuário para que seja exibido no campo **De:**. para todas as mensagens enviadas.
10. No campo **Endereço de e-mail**, especifique o endereço de e-mail do usuário do dispositivo iOS MDM.
11. Configurar as Configurações adicionais da conta de e-mail:

    - Para permitir que o usuário mova mensagens de e-mail entre as contas do usuário, selecione a caixa **Permitir o movimento de mensagens entre contas**.
    - Para permitir que os endereços de e-mail sejam sincronizados entre as contas do usuário, selecione a caixa de seleção **Permitir a sincronização de endereços recentes**.
    - Para permitir que um usuário use o serviço Mail Drop para enviar anexos de grande tamanho, selecione a caixa de seleção **Permitir o Mail Drop**.
    - Para permitir que o usuário somente use o cliente de e-mail iOS padrão, selecione a caixa de seleção **Permitir somente o uso do aplicativo Mail**.
12. Definir as configurações para usar o protocolo S/MIME no aplicativo de correio. O *S/MIME* é um protocolo para transmitir mensagens criptografadas digitalmente assinadas.

    - Para usar o protocolo S/MIME para assinar o correio de saída, selecione a caixa de seleção **Assine as mensagens** e selecione um certificado para a assinatura. Uma assinatura digital confirma a autenticidade do remetente e indica que o conteúdo da mensagem não foi modificado durante a transmissão ao destinatário. Uma assinatura da mensagem está disponível nos dispositivos que executam a verão 10.3 ou posterior do iOS.
    - Para usar o protocolo S/MIME para criptografar o correio de saída, selecione a caixa de seleção **Criptografar as mensagens por padrão** e selecione um certificado para a criptografia (chave pública). A

criptografia de mensagens está disponível para dispositivos móveis executando o iOS versão 10.3 ou posterior.

- Para ativar a um usuário para criptografar mensagens individuais, selecione a caixa de seleção **Mostrar o botão de seleção para criptografar as mensagens**. Para enviar mensagens criptografadas, o usuário deve clicar no ícone na aplicativo de correio no campo **Para**.

13. Nas seções **Servidor de correio de entrada** e **Servidor de correio de saída**, clique no botão **Configurações** para especificar as configurações de conexão com o servidor:

    - **Endereço e porta do servidor**: Nomes de anfitriões ou endereços IP de servidores de correio de entrada e de saída e números de porta do servidor.
    - **Nome da conta**: Nome da conta do usuário para autorização do servidor de correio de entrada e saída.
    - **Tipo de autenticação**: Tipo de autenticação da conta de e-mail do usuário em servidores de correio de entrada e de saída.
    - **Senha**: Senha da conta para autenticação no servidor de e-mail de saída e entrada protegido por meio do método de autenticação selecionado.
    - **Use uma senha para servidores de correio de entrada e de saída**: use uma senha para a autenticação de usuário em servidores de correio de entrada e de saída.
    - **Usar a conexão SSL**: o uso do protocolo de transporte de dados SSL (Secure Sockets Layer) que usa criptografia e autenticação baseada em certificados para proteger a transmissão de dados.

14. Clique em **OK**.

    A nova conta de e-mail é exibida na lista.

15. Clique no botão **Aplicar** para salvar as alterações efetuadas.

Como resultado, após a política ser aplicada, as contas de e-mail da lista compilada serão adicionadas no dispositivo móvel do usuário.

Configurar uma caixa de correio Exchange nos dispositivos iOS MDM

Para permitir que o usuário do dispositivo iOS MDM use e-mail corporativo, calendários, contatos, notas e tarefas, adicione a conta Exchange ActiveSync do usuário no servidor Microsoft Exchange.

Por padrão, uma conta com as configurações que se seguem é adicionada no servidor Microsoft Exchange:

- O e-mail é sincronizado uma vez por semana.
- O usuário pode mover mensagens entre as contas do usuário e sincronizar endereços da conta.
- O usuário pode usar quaisquer clientes de e-mail (que não o Mail) para usar o e-mail.
- A conexão SSL não é usada durante a transmissão de mensagens.

Você pode editar as configurações especificadas ao adicionar a conta Exchange ActiveSync.

Para adicionar a conta Exchange ActiveSync do usuário do dispositivo iOS MDM:

1. No árvore do console, na pasta **Dispositivos gerenciados**, selecione o grupo de administração ao qual os dispositivos iOS MDM pertencem.

2. Na área de trabalho do grupo, selecione a guia **Políticas**.

3. Clique duas vezes para abrir a janela de propriedades da política.

4. Na janela **Propriedades** da política, selecione a seção **Exchange ActiveSync**.

5. Clique no botão **Adicionar** na seção **Contas do Exchange ActiveSync**.

   A janela **Conta do Exchange ActiveSync** é exibida na guia **Geral**.

6. No campo **Nome da conta**, insira o nome da conta para autorização no servidor Microsoft Exchange. Você pode usar macros a partir da lista suspensa **Macros disponíveis**.

7. No campo **Endereço do servidor**, insira o nome da rede ou endereço IP do servidor Microsoft Exchange.

8. Para usar o protocolo de transporte de dados SSL (Secure Sockets Layer) para proteger a transmissão de dados, selecione a caixa **Usar a conexão SSL**.

9. No campo **Domínio**, insira o nome do domínio do usuário do dispositivo iOS MDM. Você pode usar macros a partir da lista suspensa **Macros disponíveis**.

10. No campo **Nome de usuário da conta**, insira o nome de usuário do dispositivo iOS MDM.

    Se você deixar esse campo em branco, o Kaspersky Device Management for iOS solicita que o usuário insira o nome de usuário ao aplicar a política no dispositivo iOS MDM. Você pode usar macros a partir da lista suspensa **Macros disponíveis**.

11. No campo **Endereço de e-mail**, especifique o endereço de e-mail do usuário do dispositivo iOS MDM. Você pode usar macros a partir da lista suspensa **Macros disponíveis**.

12. No campo **Senha**, insira a senha da conta Exchange ActiveSync para autorização no servidor Microsoft Exchange.

13. Selecione a guia **Adicional** e defina as configurações adicionais da conta do Exchange ActiveSync:

    - **Número de dias para sincronizar o correio <time period>**.
    - **Tipo de autenticação**.
    - **Permitir o movimento de mensagens entre contas**.
    - **Permitir a sincronização de endereços recentes**.
    - **Permitir somente o uso do aplicativo Mail**.

14. Definir as configurações para usar o protocolo S/MIME no aplicativo de correio. O *S/MIME* é um protocolo para transmitir mensagens criptografadas digitalmente assinadas.

    - Para usar o protocolo S/MIME para assinar o correio de saída, selecione a caixa de seleção **Assine as mensagens** e selecione um certificado para a assinatura. Uma assinatura digital confirma a autenticidade do remetente e indica que o conteúdo da mensagem não foi modificado durante a transmissão ao destinatário. Uma assinatura da mensagem está disponível nos dispositivos que executam a verão 10.3 ou posterior do iOS.

- Para usar o protocolo S/MIME para criptografar o correio de saída, selecione a caixa de seleção **Criptografar as mensagens por padrão** e selecione um certificado para a criptografia (chave pública). A criptografia de mensagens está disponível para dispositivos móveis executando o iOS versão 10.3 ou posterior.

- Para ativar a um usuário para criptografar mensagens individuais, selecione a caixa de seleção **Mostrar o botão de seleção para criptografar as mensagens**. Para enviar mensagens criptografadas, o usuário deve clicar no ícone na aplicativo de correio no campo **Para**.

15. Clique em **OK**.

    A nova conta Exchange ActiveSync é exibida na lista.

16. Clique no botão **Aplicar** para salvar as alterações efetuadas.

Como resultado, após a aplicação da política, as contas Exchange ActiveSync da lista compilada serão adicionadas no dispositivo móvel do usuário.

Configurar uma caixa de correio Exchange em dispositivos Android (somente Samsung)

Para trabalhar com correio corporativo, contatos e o calendário no dispositivo móvel, você deve definir as configurações de caixa de correio Exchange.

A configuração de uma caixa de correio do Exchange só é possível para os dispositivos Samsung.

Para configurar uma caixa de correio Exchange em um dispositivo móvel:

1. No árvore do console, na pasta **Dispositivos gerenciados**, selecione o grupo de administração ao qual os dispositivos Android pertencem.

2. Na área de trabalho do grupo, selecione a guia **Políticas**.

3. Clique duas vezes em qualquer coluna para abrir a janela de propriedades da política.

4. Na janela **Propriedades** da política, selecione a seção **Gerenciar o Samsung KNOX → Gerenciar dispositivos Samsung**.

5. Na janela **Exchange ActiveSync**, clique no botão **Configurar**.

   A janela **Configurações do servidor Exchange de correio** é exibida.

6. No campo **Endereço do servidor**, insira o endereço IP ou nome DNS do servidor que hospeda o servidor de correio.

7. No campo **Domínio**, insira o nome do domínio do usuário do dispositivo móvel na rede corporativa.

8. Na lista suspensa **Intervalo de sincronização**, selecione o intervalo desejado de sincronização de dispositivos móveis com o servidor Microsoft Exchange.

9. Para usar o protocolo de transporte de dados SSL (Secure Sockets Layer), selecione a caixa de seleção **Usar a conexão SSL**.

10. Para usar certificados digitais para proteger a transferência de dados entre o dispositivo móvel e o servidor Microsoft Exchange, selecione a caixa de seleção **Verificar o certificado do servidor**.

11. Clique no botão **Aplicar** para salvar as alterações efetuadas.

As configurações do dispositivo móvel são definidas depois da próxima sincronização do dispositivo com o Kaspersky Security Center.

Gerenciamento de aplicativos móveis de terceiros

Você pode usar contêineres para monitorar a atividade de aplicativos móveis iniciados no dispositivo do usuário. *Um contêiner* é um armazenamento especial para aplicativos móveis que possibilita controlar a atividade do aplicativo em contêiner, protegendo os dados pessoais e corporativos do usuário no dispositivo.

No Kaspersky Security for Mobile Service Pack 3 Maintenance Release 2, não mais há suporte para criar contêineres para aplicativos móveis. Contudo, os contêineres que foram criados em versões mais antigas do aplicativo podem ser adicionados aos dispositivos Android.

Você pode instalar um aplicativo em contêiner no dispositivo do usuário em uma das seguintes formas:

- Ao enviar uma mensagem por e-mail ao usuário com um link para pacote de instalação do aplicativo em contêiner.
- Ao especificar um aplicativo em contêiner conforme exigido ou permitido na seção **Controle de aplicativos** da janela de propriedades da política. Após o dispositivo móvel ser sincronizado com o Kaspersky Security Center, o pacote de distribuição do aplicativo no contêiner é automaticamente copiado para o dispositivo do usuário.

Para instalar aplicativos em contêineres, a instalação de aplicativos de origens desconhecidas deve ser permitida no dispositivo móvel do usuário. Para proteger o seu dispositivo e os seus dados depois de instalar aplicativos em contêineres, recomenda-se proibir a instalação de aplicativos de origens desconhecidas. Para obter detalhes sobre a instalação de aplicativos sem o Google Play, consulte o *Guia de Ajuda do Android*.

Configurar notificações para o Kaspersky Endpoint Security for Android

Caso não queira que o usuário do dispositivo móvel receba notificações do Kaspersky Endpoint Security for Android, é possível desativar certas notificações.

O Kaspersky Endpoint Security usa as seguintes ferramentas para exibir o status da proteção do dispositivo:

- **Notificação de status da proteção**. Esta notificação é afixada à barra de notificação. A notificação do status da proteção não pode ser removida. A notificação exibe o status da proteção do dispositivo (por exemplo,) e o número de problemas, se houver. Você pode tocar no status da proteção do dispositivo e ver a lista de problemas no aplicativo.
- **Notificações do aplicativo**. Estas notificações informam o usuário do dispositivo sobre o aplicativo (por exemplo, detecção de ameaças).
- **Mensagens pop-up**. As mensagens pop-up requerem ação do usuário do dispositivo (por exemplo, ação a ser executada quando uma ameaça é detectada).

Todas as notificações do Kaspersky Endpoint Security for Android são ativadas por padrão.

Um usuário de dispositivo Android pode desativar todas as notificações do Kaspersky Endpoint Security for Android nas configurações na barra de notificação. Se as notificações forem desativadas, o usuário não monitora a operação do aplicativo e pode ignorar informações importantes (por exemplo, informações sobre falhas durante a sincronização do dispositivo com o Kaspersky Security Center). Neste caso, para conhecer o status da operação do aplicativo, o usuário deve abrir o Kaspersky Endpoint Security for Android.

Para configurar a exibição de notificações sobre a operação do Kaspersky Endpoint Security for Android:

1. No árvore do console, na pasta **Dispositivos gerenciados**, selecione o grupo de administração ao qual os dispositivos Android pertencem.
2. Na área de trabalho do grupo, selecione a guia **Políticas**.
3. Clique duas vezes em qualquer coluna para abrir a janela de propriedades da política.
4. Na janela **Propriedades** da política, selecione a seção **Adicional**.
5. Na seção **Notificações do aplicativo**, clique no botão **Configurar**.

   A janela **Configurações de notificação do dispositivo** é aberta.
6. Selecione os problemas do Kaspersky Endpoint Security for Android que deseja ocultar no dispositivo móvel do usuário e clique no botão **OK**.

   O Kaspersky Endpoint Security for Android não exibirá problemas na notificação de status da proteção e na seção **Status** do aplicativo. O Kaspersky Endpoint Security for Android continuará exibindo notificações de status da proteção e notificações do aplicativo.

   Certos problemas do Kaspersky Endpoint Security for Android são obrigatórios e impossíveis de desativar (como problemas relativos à expiração da licença).
7. Para ocultar todas as notificações e mensagens pop-up, selecione **Desativar notificações e pop-ups quando o aplicativo estiver em segundo plano**.

   O Kaspersky Endpoint Security for Android exibirá apenas a notificação de status da proteção. A notificação exibe o status da proteção do dispositivo (por exemplo,) e o número de problemas. Além disso, o aplicativo exibe notificações quando o usuário está trabalhando com o aplicativo (o usuário atualiza os bancos de dados antivírus manualmente, por exemplo).

   Os especialistas da Kaspersky recomendam ativar notificações e mensagens pop-up. Se você desativar as notificações e mensagens pop-up quando o aplicativo estiver em segundo plano, o aplicativo não alertará os usuários sobre ameaças em tempo real. Usuários de dispositivos móveis podem saber o status da proteção do dispositivo apenas ao abrirem o aplicativo.
8. Clique no botão **Aplicar** para salvar as alterações efetuadas.

As configurações do dispositivo móvel são definidas depois da próxima sincronização do dispositivo com o Kaspersky Security Center. As notificações do Kaspersky Endpoint Security for Android que você desativa não serão exibidas no dispositivo móvel do usuário.

Conectar dispositivos iOS MDM ao AirPlay

Configure a conexão com dispositivos AirPlay para ativar a transmissão de música, fotos e vídeos a partir do dispositivo iOS MDM para dispositivos AirPlay. Para poder usar tecnologia AirPlay, o dispositivo móvel e os dispositivos AirPlay devem estar conectados com a mesma rede sem fio. Dispositivos AirPlay incluem dispositivos Apple TV (da segunda e terceira geração), dispositivos AirPort Express, alto-falantes ou rádios compatíveis com o AirPlay.

A conexão automática com dispositivos AirPlay está disponível somente para dispositivos controlados.

Para configurar a conexão de um dispositivo iOS MDM com dispositivos AirPlay:

1. No árvore do console, na pasta **Dispositivos gerenciados**, selecione o grupo de administração ao qual os dispositivos iOS MDM pertencem.
2. Na área de trabalho do grupo, selecione a guia **Políticas**.
3. Clique duas vezes para abrir a janela de propriedades da política.
4. Na janela **Propriedades** da política, selecione a seção **AirPlay**.
5. Na seção **Dispositivos AirPlay**, selecione a caixa de seleção **Aplicar as configurações no dispositivo**.
6. Clique no botão **Adicionar** na seção **Senhas**.

   Uma linha vazia é adicionada à tabela de senhas.
7. Na coluna **Nome do dispositivo**, insira o nome do dispositivo AirPlay na rede sem fio.
8. Na coluna **Senha**, insira a senha para o dispositivo AirPlay.
9. Para restringir o acesso de dispositivos iOS MDM a dispositivos AirPlay, crie uma lista de dispositivos na seção **Dispositivos permitidos**. Para isso, adicione os endereços MAC de dispositivos AirPlay à lista de dispositivos permitidos.

   O Acesso a dispositivos AirPlay que não estão na lista de dispositivos permitidos é bloqueado. Se a lista de dispositivos permitidos for deixada em branco, o Kaspersky Mobile Device Management for iOS permite acessar todos os dispositivos AirPlay.
10. Clique no botão **Aplicar** para salvar as alterações efetuadas.

Como resultado, após a aplicação da política, o dispositivo móvel do usuário irá automaticamente se conectar com dispositivos AirPlay para transmitir conteúdo de mídia.

Conectar dispositivos iOS MDM ao AirPrint

Para ativar a impressão de documentos a partir do dispositivo iOS MDM sem fio usando a tecnologia AirPrint, configure a conexão automática a impressoras AirPrint. O dispositivo móvel e a impressora devem estar conectados à mesma rede sem fio. Acesso compartilhado para todos os usuários tem que ser configurado na impressora AirPrint.

Para configurar a conexão de um dispositivo iOS MDM a uma impressora AirPrint:

1. No árvore do console, na pasta **Dispositivos gerenciados**, selecione o grupo de administração ao qual os dispositivos iOS MDM pertencem.
2. Na área de trabalho do grupo, selecione a guia **Políticas**.

3. Clique duas vezes para abrir a janela de propriedades da política.

4. Na janela **Propriedades** da política, selecione a seção **AirPrint**.

5. Clique no botão **Adicionar** na seção **Impressoras AirPrint**.

   A janela **Impressora** é aberta.

6. No campo **Endereço IP**, insira o endereço IP da impressora AirPrint.

7. No campo **Caminho do recurso**, insira o caminho para a impressora AirPrint.

   O caminho para a impressora corresponde à chave rp (resource path) do protocolo Bonjour. Por exemplo:

   - printers/Canon_MG5300_series
   - ipp/print
   - Epson_IPP_Printer

8. Clique em **OK**.

   A nova impressora AirPrint adicionada é exibida na lista.

9. Clique no botão **Aplicar** para salvar as alterações efetuadas.

Como resultado, após a política ser aplicada, o usuário do dispositivo móvel pode imprimir documentos sem fio na impressora AirPrint.

Configurar o nome do ponto de acesso (APN)

Para conectar um dispositivo móvel aos serviços de transferência de dados em uma rede móvel, você deve definir as configurações de APN (Nome de Ponto de Acesso).

Configurar a APN em dispositivos Android (somente Samsung)

A configuração da APN só é possível para os dispositivos Samsung.

Um cartão SIM deve ser inserido para ser possível usar um ponto de acesso no dispositivo móvel do usuário. As configurações de ponto de acesso são fornecidas pela operadora de telefonia móvel. Configurações de ponto de acesso incorretas podem resultar em cobranças de telefonia móvel adicionais.

Para definir as configurações do Nome do Ponto de Acesso (APN):

1. No árvore do console, na pasta **Dispositivos gerenciados**, selecione o grupo de administração ao qual os dispositivos Android pertencem.

2. Na área de trabalho do grupo, selecione a guia **Políticas**.

3. Clique duas vezes em qualquer coluna para abrir a janela de propriedades da política.

4. Na janela **Propriedades** da política, selecione a seção **Gerenciar o Samsung KNOX → APN**.

5. Na seção **APN**, clique no botão **Configurar**.

   A janela **Configurações de APN** é aberta.

6. Na guia **Geral**, especifique as seguintes configurações do ponto de acesso:

   a. Na lista suspensa **Tipo de APN**, selecione o tipo de ponto de acesso.

   b. No campo **Nome de APN**, especifique o nome do ponto de acesso.

   c. No campo **MCC**, insira o código de país da rede celular (MCC).

   d. No campo **MNC**, insira o código de rede celular (MNC).

   e. Caso você tenha selecionado **MMS** ou **Internet e MMS** como tipo de ponto de acesso, especifique as configurações MMS adicionais seguintes:

      - No campo **Servidor de MMS**, especifique o nome completo do domínio do servidor do operador celular usado para troca de MMS.

      - No campo **Servidor proxy de MMS**, especifique o nome da rede ou endereço IP do servidor proxy e o número da porta do servidor do operador celular usado para troca de MMS.

7. Na guia **Adicional**, configure as configurações adicionais no nome do ponto de acesso (APN):

   a. Na lista suspensa **Tipo de autenticação**, selecione o tipo de autenticação do usuário do dispositivo móvel no servidor da operadora de telefonia móvel para o acesso à rede.

   b. No campo **Endereço do servidor**, especifique o nome de rede do servidor do operador móvel através do qual os serviços de transmissão de dados são acessados.

   c. No campo **Endereço do servidor proxy**, especifique o nome de rede ou endereço de IP e número da porta do servidor proxy do operador para acesso de rede.

   d. No campo **Nome de usuário**, insira o nome de usuário para autorização na rede móvel.

   e. No campo **Senha**, insira a senha para autorização do usuário na rede móvel.

8. Clique no botão **Aplicar** para salvar as alterações efetuadas.

As configurações do dispositivo móvel são definidas depois da próxima sincronização do dispositivo com o Kaspersky Security Center.

Configurar a APN em dispositivos iOS MDM

O Nome do Ponto de Acesso (APN) deve ser configurado para permitir o serviço de transmissão de dados da rede móvel no dispositivo iOS MDM do usuário.

A seção **APN** está desatualizada. Recomenda-se definir as configurações APN na seção **Comunicação celular**. Antes de definir as configurações de comunicação de celular, assegure-se de que as configurações da seção **APN** não foram aplicadas no dispositivo (a caixa de seleção **Aplicar as configurações no dispositivo** esteja desmarcada). As configurações das seções **APN** e de **Comunicação celular** não podem ser usadas concorrentemente.

Para configurar um ponto de acesso num dispositivo iOS MDM do usuário:

1. No árvore do console, na pasta **Dispositivos gerenciados**, selecione o grupo de administração ao qual os dispositivos iOS MDM pertencem.
2. Na área de trabalho do grupo, selecione a guia **Políticas**.
3. Clique duas vezes para abrir a janela de propriedades da política.
4. Na janela **Propriedades** da política, selecione a seção **Comunicação celular**.
5. Na seção **Configurações de comunicação celular**, selecione a caixa **Aplicar as configurações no dispositivo**.
6. Na lista de **Tipo de APN**, selecione o tipo do ponto de acesso para a transferência de dados em uma rede móvel GPRS/3G/4G:
   - **APN incorporado** – definição das configurações de comunicação por celular para a transferência de dados por meio de um operador de rede móvel compatível com operação com Apple SIM incorporado. Para obter mais detalhes sobre dispositivos com Apple SIM incorporado, visite o site de Suporte Técnico da Apple.
   - **APN** – definição de configurações de comunicação de celular para a transferência de dados através do operador de rede móvel do Cartão SIM inserido.
   - **APN incorporado e APN** – definição das configurações de comunicação por celular para a transferência de dados por meio de operadores da rede móvel do Cartão SIM inserido e do Apple SIM incorporado. Para obter mais detalhes sobre dispositivos com um Apple SIM incorporado e um slot de Cartão SIM, visite o site de Suporte Técnico da Apple.
7. No campo **Nome de APN**, especifique o nome do ponto de acesso.
8. Na lista suspensa **Tipo de autenticação**, selecione o tipo de autenticação do usuário do dispositivo no servidor da operadora de telefonia móvel para o acesso à rede (Internet e MMS):
9. No campo **Nome de usuário**, insira o nome de usuário para autorização na rede móvel.
10. No campo **Senha**, insira a senha para autorização do usuário na rede móvel.
11. No campo **Endereço e porta do servidor proxy**, insira o nome de um anfitrião ou do endereço IP de um servidor proxy e o número da porta do servidor proxy.
12. Clique no botão **Aplicar** para salvar as alterações efetuadas.

Como resultado, o nome do ponto de acesso (APN) é configurado no dispositivo móvel do usuário após a aplicação da política.

Configurar o perfil de trabalho do Android

Esta seção contém informações sobre como trabalhar com um perfil de trabalho do Android.

Sobre o perfil de trabalho do Android

O *Android Enterprise* é uma plataforma para gerenciar a infraestrutura corporativa de dispositivos móveis, que fornece aos funcionários da empresa um ambiente de trabalho no qual eles podem usar seus dispositivos móveis. Para obter detalhes sobe como usar o Android Enterprise, consulte o site de suporte da Google.

Você pode criar o perfil de trabalho do Android (aqui também denominado "perfil de trabalho") no dispositivo móvel do usuário. O *perfil de trabalho do Android* é um ambiente seguro no dispositivo do usuário no qual o administrador pode gerenciar os aplicativos e as contas de usuário sem restringir o uso dos dados pessoais pelo usuário. Quando um perfil de trabalho for criado no dispositivo móvel do usuário, os seguintes aplicativos corporativos são automaticamente instalados no perfil de trabalho: Google Play Market, Google Chrome, Downloads, Kaspersky Endpoint Security for Android e outros. Os aplicativos corporativos instalados no perfil de trabalho e as notificações sobre estes aplicativos são marcados com um ícone . Você deve criar uma conta corporativa do Google separada para o aplicativo Google Play Market. Os aplicativos instalados no perfil do trabalho aparecem na lista de aplicativos comuns.

Configurar o perfil do trabalho

Para definir as configurações do perfil de trabalho do Android:

1. No árvore do console, na pasta **Dispositivos gerenciados**, selecione o grupo de administração ao qual os dispositivos Android pertencem.
2. Na área de trabalho do grupo, selecione a guia **Políticas**.
3. Clique duas vezes em qualquer coluna para abrir a janela de propriedades da política.
4. Na janela **Propriedades** da política, selecione **Perfil do Android para o trabalho**.
5. Na área de trabalho do **Perfil de trabalho do Android**, selecione a caixa de seleção **Criar o perfil de trabalho**.
6. Especifique as configurações do perfil de trabalho:

   - Para ativar o Controle de aplicativos no perfil de trabalho do Android e desativá-lo no perfil pessoal, selecione a caixa de seleção **Ativar o Controle de aplicativos somente no perfil do trabalho**.

     Na seção **Usuários**, é possível selecionar **Controle de aplicativos** e usar a área de trabalho para criar listas de aplicativos permitidos, bloqueados, recomendados e necessários, bem como categorias de aplicativos permitidos e bloqueados na seção.

   - Para ativar a Proteção na Web para Google Chrome no perfil de trabalho e desativá-la no perfil pessoal, na área de trabalho da seção de **Perfil de trabalho do Android**, marque a caixa de seleção **Ativar a Proteção na Web somente no perfil do trabalho**.

     A Proteção na Web para Samsung Internet Browser bloqueia sites nos perfis pessoal e de trabalho. Não é possível ativar a Proteção na Web para Samsung Internet Browser apenas no perfil de trabalho. Para usar a Proteção na Web para o Samsung Internet Browser no perfil de trabalho, desative a opção **Ativar a Proteção na Web somente no perfil do trabalho**. Se essa opção estiver ativada, a Proteção na Web para o Samsung Internet Browser não será executada. A Proteção na Web no perfil de trabalho é desativada por padrão.

     A Proteção na Web em dispositivos Android funciona somente no navegador Google Chrome e no Samsung Internet Browser.

     É possível especificar as configurações de acesso a sites (criar uma lista de categorias de sites bloqueadas ou uma lista de sites permitidos) na seção **Proteção na Web**.

- Para proibir o usuário de copiar dados dos aplicativos do perfil de trabalho para aplicativos pessoais por meio da Área de transferência, marque a caixa de seleção **Proibir a transferência de dados do perfil do trabalho para o perfil pessoal**.

- Para bloquear o usuário de usar o modo de depuração de USB no dispositivo móvel no perfil de trabalho, selecione a caixa de seleção **Proibir a ativação do modo de depuração USB**.

  No modo de depuração de USB, o usuário poderá baixar um aplicativo usando uma área de trabalho, por exemplo.

- Para proibir que o usuário instale aplicativos no perfil de trabalho do Android de todas as origens exceto do Google Play, selecione a caixa de seleção **Proibir a instalação de aplicativos no perfil do trabalho de origens desconhecidas**.

- Para proibir que o usuário remova aplicativos do perfil de trabalho do Android, selecione a caixa de seleção **Proibir a remoção de aplicativos do perfil do trabalho**.

7. Para definir as configurações do perfil de trabalho no dispositivo móvel do usuário, bloqueie alterações às configurações.

8. Clique no botão **Aplicar** para salvar as alterações efetuadas.

As configurações do dispositivo móvel são definidas depois da próxima sincronização do dispositivo com o Kaspersky Security Center. O espaço do dispositivo móvel do usuário é dividido em um perfil de trabalho e um perfil pessoal.

Adicionar uma conta LDAP

Para permitir que o usuário do dispositivo iOS MDM acesse contatos corporativos no servidor LDAP, adicione a conta LDAP.

Para adicionar a conta LDAP do usuário do dispositivo iOS MDM:

1. No árvore do console, na pasta **Dispositivos gerenciados**, selecione o grupo de administração ao qual os dispositivos iOS MDM pertencem.

2. Na área de trabalho do grupo, selecione a guia **Políticas**.

3. Clique duas vezes para abrir a janela de propriedades da política.

4. Na janela **Propriedades** da política, selecione a seção **LDAP**.

5. Clique no botão **Adicionar** na seção **Contas LDAP**.

   A janela **Conta LDAP** é exibida.

6. No campo **Descrição**, insira uma descrição da conta LDAP do usuário. Você pode usar macros a partir da lista suspensa **Macros disponíveis**.

7. No campo **Nome da conta**, insira o nome da conta para autorização no servidor da LDAP. Você pode usar macros a partir da lista suspensa **Macros disponíveis**.

8. No campo **Senha**, insira a senha da conta LDAP para autorização no servidor LDAP.

9. No campo **Endereço do servidor**, insira o nome do domínio do servidor LDAP. Você pode usar macros a partir da lista suspensa **Macros disponíveis**.

10. Para usar o protocolo de transporte de dados SSL (Secure Sockets Layer) para proteger a transmissão de mensagens, selecione a caixa **Usar a conexão SSL**.

11. Compile uma lista de consultas de pesquisa para o acesso do usuário do dispositivo móvel iOS MDM a dados corporativos no servidor LDAP:

    a. Clique no botão **Adicionar** na seção **Configurações da pesquisa**.

    Uma linha em branco é exibida na tabela com consultas de pesquisa.

    b. Na coluna **Nome**, insira o nome de uma consulta de pesquisa.

    c. Na coluna **Escopo da pesquisa**, selecione o nível de aninhamento da pasta para a pesquisa de dados corporativos no servidor LDAP:

    - **Base** – pesquisar na pasta base do servidor LDAP.
    - **Um nível** – pesquisar nas pastas no primeiro nível de aninhamento contando a partir da pasta base.
    - **Subárvore** – pesquisar nas pastas em todos os níveis de aninhamento a partir da pasta base.

    d. Na coluna **Base da pesquisa**, insira o caminho da pasta no servidor LDAP na qual a pesquisa inicia-se (por exemplo: "ou=people", "o=example corp").

    e. Repita as etapas A a D para todas as consultas de pesquisa que você deseja adicionar ao dispositivo iOS MDM.

12. Clique em **OK**.

    A nova conta LDAP é exibida na lista.

13. Clique no botão **Aplicar** para salvar as alterações efetuadas.

Como resultado, após a política ser aplicada, as contas LDAP da lista compilada serão adicionadas no dispositivo móvel do usuário. O usuário pode acessar contatos corporativos nos aplicativos padrão do iOS: Contatos, mensagens e e-mail.

Adicionar uma conta de calendário

Para permitir que o usuário do dispositivo iOS MDM acesse eventos do calendário do usuário no servidor CalDAV, adicione a conta CalDAV. A sincronização com o servidor CalDAV permite que o usuário crie e receba convites, receba atualizações de eventos e sincronize tarefas com o aplicativo Lembretes.

Para adicionar a conta CalDAV do usuário do dispositivo iOS MDM:

1. No árvore do console, na pasta **Dispositivos gerenciados**, selecione o grupo de administração ao qual os dispositivos iOS MDM pertencem.

2. Na área de trabalho do grupo, selecione a guia **Políticas**.

3. Clique duas vezes para abrir a janela de propriedades da política.

4. Na janela **Propriedades** da política, selecione a seção **Calendário**.

5. Clique no botão **Adicionar** na seção **Contas CalDAV**.

   A janela **Conta CalDAV** é exibida.

6. No campo **Descrição**, insira uma descrição da conta CalDAV do usuário.

7. No campo **Endereço e porta do servidor**, insira o nome de um anfitrião ou do endereço IP de um servidor CalDAV e o número da porta do servidor CalDAV.

8. No campo **URL principal**, especifique o URL da conta CalDAV do usuário do dispositivo iOS MDM no servidor CalDAV (por exemplo: http://example.com/caldav/users/mycompany/user).

   O URL deve começar com `"http://"` ou `"https://"`.

9. No campo **Nome da conta**, insira o nome da conta para autorização no servidor CalDAV.

10. No campo **Senha**, configure a senha da conta CalDAV para autorização no servidor CalDAV.

11. Para usar o protocolo de transporte de dados SSL (Secure Sockets Layer) para proteger a transmissão de dados do evento entre o servidor CalDAV e o dispositivo móvel, selecione a caixa **Usar a conexão SSL**.

12. Clique em **OK**.

    A nova conta CalDAV é exibida na lista.

13. Clique no botão **Aplicar** para salvar as alterações efetuadas.

Como resultado, após a política ser aplicada, as contas CalDAV da lista compilada serão adicionadas no dispositivo móvel do usuário.

Adicionar uma conta de contatos

Para permitir que o usuário do dispositivo iOS MDM sincronize dados com o servidor CardDAV, adicione a conta CardDAV. A sincronização com o servidor CardDAV permite que o usuário acesse os detalhes de conta a partir de qualquer dispositivo.

Para adicionar a conta CardDAV do usuário do dispositivo iOS MDM:

1. No árvore do console, na pasta **Dispositivos gerenciados**, selecione o grupo de administração ao qual os dispositivos iOS MDM pertencem.

2. Na área de trabalho do grupo, selecione a guia **Políticas**.

3. Clique duas vezes para abrir a janela de propriedades da política.

4. Na janela **Propriedades** da política, selecione a seção **Contatos**.

5. Clique no botão **Adicionar** na seção **Contas CardDAV**.

   A janela **Conta CardDAV** é exibida.

6. No campo **Descrição**, insira uma descrição da conta CardDAV do usuário. Você pode usar macros a partir da lista suspensa **Macros disponíveis**.

7. No campo **Endereço e porta do servidor**, insira o nome de um anfitrião ou do endereço IP de um servidor CardDAV e o número da porta do servidor CardDAV.

8. No campo **URL principal**, especifique o URL da conta CardDAV do usuário do dispositivo iOS MDM no servidor CardDAV (por exemplo: http://example.com/carddav/users/mycompany/user).

   O URL deve começar com `"http://"` ou `"https://"`.

9. No campo **Nome da conta**, insira o nome da conta para autorização no servidor CardDAV. Você pode usar macros a partir da lista suspensa **Macros disponíveis**.

10. No campo **Senha**, configure a senha da conta CardDAV para autorização no servidor CardDAV.

11. Para usar o protocolo de transporte de dados SSL (Secure Sockets Layer) para proteger a transmissão de contatos entre o servidor CardDAV e o dispositivo móvel, selecione a caixa **Usar a conexão SSL**.

12. Clique em **OK**.

    A nova conta CardDAV é exibida na lista.

13. Clique no botão **Aplicar** para salvar as alterações efetuadas.

Como resultado, após a política ser aplicada, as contas CardDAV da lista compilada serão adicionadas no dispositivo móvel do usuário.

Configurar uma assinatura de calendário

Para permitir que o usuário do dispositivo iOS MDM adicione eventos de calendários compartilhados (como o calendário corporativo) ao calendário do usuário, adicione a assinatura para esse calendário. *Calendários compartilhados* são calendários de outros usuários que possuem uma conta CalDAV, calendários iCal e outros calendários publicados abertamente.

Para adicionar a assinatura do calendário:

1. No árvore do console, na pasta **Dispositivos gerenciados**, selecione o grupo de administração ao qual os dispositivos iOS MDM pertencem.

2. Na área de trabalho do grupo, selecione a guia **Políticas**.

3. Clique duas vezes para abrir a janela de propriedades da política.

4. Na janela **Propriedades** da política, selecione a seção **Assinatura do calendário**.

5. Clique no botão **Adicionar** na seção **Assinaturas do calendário**.

   A janela **Assinatura do calendário** é aberta.

6. No campo **Descrição**, insira uma descrição de uma assinatura do calendário.

7. No campo **Endereço do servidor da Web**, especifique o URL de um calendário de terceiros.

   Neste campo, você pode inserir o URL de e-mail da conta CalDAV do usuário cujo calendário você está assinando. Você também pode especificar o URL de um calendário iCal ou um calendário publicado abertamente diferente.

8. No campo **Nome de usuário**, insira o nome da conta do usuário para a autenticação no servidor do calendário de terceiros.

9. No campo **Senha**, insira a senha da assinatura do calendário para a autenticação no servidor do calendário de terceiros.

10. Para usar o protocolo de transporte de dados SSL (Secure Sockets Layer) para proteger a transmissão de dados do evento entre o servidor CalDAV e o dispositivo móvel, selecione a caixa **Usar a conexão SSL**.

11. Clique em **OK**.

12. A nova assinatura de calendário é exibida na lista.

13. Clique no botão **Aplicar** para salvar as alterações efetuadas.

Como resultado, após a aplicação da política, os eventos do calendário compartilhado na lista serão adicionados ao calendário no dispositivo móvel do usuário.

Adicionar clipes da Web

Um *clipe da Web* é um aplicativo que abre um site a partir da tela inicial do dispositivo móvel. Ao clicar nos ícones de Clipes da Web na tela inicial do dispositivo, o usuário pode rapidamente abrir sites (como o site corporativo). Você pode adicionar Clipes da Web a dispositivos de usuários e configurar o aspeto do ícone do Clipe da Web exibido na tela.

Por padrão, aplicam-se as seguintes restrições seguintes no uso de Clipes da Web:

- O usuário não pode remover manualmente Clipes da Web do dispositivo móvel.
- Os sites que são exibidos quando o usuário clica em um ícone de um Clipe da Web não são exibidos no modo de tela completa.
- Os efeitos visuais de canto arredondado, sombra e brilho são aplicados ao ícone do Clipe da Web na tela.

Para adicionar um Clipe da Web no dispositivo iOS MDM de um usuário:

1. No árvore do console, na pasta **Dispositivos gerenciados**, selecione o grupo de administração ao qual os dispositivos iOS MDM pertencem.
2. Na área de trabalho do grupo, selecione a guia **Políticas**.
3. Clique duas vezes para abrir a janela de propriedades da política.
4. Na janela **Propriedades** da política, selecione a seção **Clipes da Web**.
5. Clique no botão **Adicionar** na seção **Clipes da Web**.

   A janela **Clipe da Web** é aberta.
6. No campo **Nome**, insira o nome do Clipe da Web a exibir na tela inicial do dispositivo iOS MDM.
7. No campo **URL**, insira o endereço da Web do site que será exibido ao clicar no ícone do Clipe da Web. O endereço deve começar com `"http://"` ou `"https://"`.
8. Para permitir que o usuário remova um Clipe da Web do dispositivo iOS MDM, selecione a caixa **Permitir a remoção**.
9. Clique no botão **Selecionar...** e especifique o arquivo com a imagem para o ícone do Clipe da Web.

   O ícone é exibido na tela inicial do dispositivo iOS MDM. A imagem deve atender os seguintes requisitos:

   - Tamanho de imagem não superior a 400 x 400 pixels
   - Formato de arquivo: GIF, JPEG ou PNG
   - Tamanho do arquivo não superior a 1 MB

O ícone do Clipe da Web está disponível para pré-visualização no campo **Ícone**. Se você não selecionar uma imagem para o Clipe da Web, um quadrado branco é exibido como o ícone.

Se você desejar que o ícone do Clipe da Web seja exibido sem efeitos visuais especiais (cantos do ícone arredondados e efeito de brilho), selecione a caixa **Ícone pré-composto**.

10. Se você desejar que o site seja exibido no modo de tela completa no dispositivo iOS MDM quando clicar no ícone, selecione a caixa **Clipe da Web em tela cheia**.

11. Clique em **OK**.

    O novo Clipe da Web é exibido na lista.

12. Clique no botão **Aplicar** para salvar as alterações efetuadas.

Como resultado, após a aplicação da política, os ícones de Clipes da Web da lista que você criou são adicionados à tela inicial do dispositivo móvel do usuário.

Adicionar fontes

Para adicionar uma fonte ao dispositivo iOS MDM de um usuário:

1. No árvore do console, na pasta **Dispositivos gerenciados**, selecione o grupo de administração ao qual os dispositivos iOS MDM pertencem.

2. Na área de trabalho do grupo, selecione a guia **Políticas**.

3. Clique duas vezes para abrir a janela de propriedades da política.

4. Na janela **Propriedades** da política, selecione a seção **Fontes**.

5. Clique no botão **Adicionar** na seção **Fontes**.

   A janela **Fonte** abre.

6. No campo **Nome do arquivo**, especifique o caminho para o arquivo da fonte (um arquivo com a extensão .ttf ou .otf).

   Fontes com a extensão ttc ou otc não são suportadas.

   As fontes são identificadas usando o nome PostScript. Não instale fontes com o mesmo nome PostScript mesmo que o seu conteúdo seja diferente. Instalar fontes com o mesmo nome PostScript resultará em um erro indefinido.

7. Clique em **Abrir**.

   A nova fonte é exibida na lista.

8. Clique no botão **Aplicar** para salvar as alterações efetuadas.

Como resultado, após a aplicação da política, será solicitado ao usuário que instale fontes da lista que foi criada.

Gerenciando o aplicativo usando sistemas EMM de terceiros (somente Android)

É possível usar o aplicativo Kaspersky Endpoint Security for Android sem os sistemas de administração da Kaspersky. Use soluções de outros provedores de serviços EMM (Enterprise Mobility Management) para implementar e gerenciar o aplicativo Kaspersky Endpoint Security for Android. A Kaspersky participa da Comunidade AppConfig para assegurar que o aplicativo funcione com soluções EMM de terceiros.

É possível gerenciar o aplicativo Kaspersky Endpoint Security for Android por meio de soluções EMM de terceiros somente em dispositivos Android.

Você pode usar as soluções EMM de terceiros para implementar apenas o aplicativo Kaspersky Endpoint Security for Android. Conecte o dispositivo ao Kaspersky Security Center e gerencie o aplicativo no Console de administração. Nesse caso, o gerenciamento do aplicativo Kaspersky Endpoint Security for Android no console EMM estará indisponível.

Se você implementou o aplicativo Kaspersky Endpoint Security for Android usando o sistema EMM de terceiros, é impossível gerenciar o aplicativo no Kaspersky Endpoint Security Cloud. É possível gerenciar o aplicativo Kaspersky Endpoint Security for Android no Console EMM.

As seguintes soluções EMM dão suporte ao uso do aplicativo Kaspersky Endpoint Security for Android:

- VMware AirWatch
- MobileIron
- IBM Maas360
- Microsoft Intune
- SOTI MobiControl

Você pode executar as seguintes ações no Console EMM:

- Implemente o aplicativo em um perfil de trabalho do Android nos dispositivos de usuários.
- Ative o aplicativo.
- Definir as configurações do aplicativo:
  - Ative a proteção contra sites de phishing e maliciosos na Internet.
  - Definir as configurações para conectar o dispositivo ao Kaspersky Security Center.
  - Definir as configurações do Antivírus.
  - Configurar o agendamento para executar uma verificação de vírus no dispositivo.
  - Ative a detecção de adware e aplicativos que podem ser explorados por criminosos para danificar o dispositivo do usuário ou seus dados pessoais.

- Configurar o agendamento para as atualizações do banco de dados do aplicativo.

Guia de Introdução

Para implementar o aplicativo nos dispositivos móveis de usuários, você deve adicionar o Kaspersky Endpoint Security for Android à loja do aplicativo EMM. Você pode adicionar o Kaspersky Endpoint Security for Android à loja de aplicativo EMM usando um link do Google Play. Para obter mais detalhes sobre como trabalhar com aplicativos no Console EMM, visite o *site de suporte técnico do provedor de serviços EMM*.

O aplicativo Kaspersky Endpoint Security for Android é implementado em um perfil de trabalho do Android. O aplicativo é isolado dos dados pessoais do usuário e somente protege os dados corporativos no perfil de trabalho. Recomenda-se assegurar que o Kaspersky Endpoint Security for Android esteja protegido contra a remoção por ferramentas do Console EMM.

Como instalar o aplicativo

Dependendo do Console EMM, selecione o método para instalar o aplicativo nos dispositivos: instalação silenciosa, enviar um e-mail que contém um link ao aplicativo no Google Play, ou outro método disponível.

As seguintes permissões são necessárias para o funcionamento do aplicativo:

- Permissão de armazenamento para acessar arquivos quando o Antivírus estiver em execução (apenas para Android 6.0 ou posterior).
- Permissão de telefone para identificar o dispositivo, por exemplo, ao ativar o aplicativo.
- A solicitação de adicionar o Kaspersky Endpoint Security for Android na lista de aplicativos que são iniciados no momento da inicialização do sistema operacional (em determinados dispositivos, como Huawei, Meizu e Xiaomi). Se a solicitação para adicionar não for exibida, manualmente adicione o Kaspersky Endpoint Security for Android à lista de aplicativos de inicialização. A solicitação não pode ser exibida se o aplicativo de segurança não for instalado no perfil de trabalho.

É possível conceder as permissões necessárias no Console EMM antes de implementar o aplicativo Kaspersky Endpoint Security for Android. Para obter mais detalhes sobre como conceder as permissões no Console EMM, visite o *site de suporte técnico do provedor de serviços EMM*. Também é possível conceder as permissões ao concluir o Assistente de configuração inicial do Kaspersky Endpoint Security for Android no dispositivo.

O aplicativo Kaspersky Endpoint Security for Android será instalado no perfil de trabalho do Android.

Para a operação da Proteção na Web, você também deve configurar um servidor proxy nas configurações do Google Chrome:

- Modo de configuração do servidor proxy: manual.
- Endereço do servidor proxy e porta: 127.0.0.1:3128.
- Suporte para o protocolo SPDY: desativado.
- Compactação dos dados através do servidor proxy: desativado.

Como ativar o aplicativo

As informações sobre a licença são transmitidas ao dispositivo móvel em conjunto com outras configurações no arquivo de configuração.

Se o aplicativo não for ativado dentro de 30 dias após a sua instalação no dispositivo móvel, a licença de avaliação irá expirar. Quando da Licença de avaliação expirar, todos os recursos do aplicativo móvel Kaspersky Endpoint Security for Android serão desativados.

Quando a Licença comercial expirar, o aplicativo móvel continua a funcionar com funcionalidade limitada (por exemplo, as atualizações do banco de dados do Kaspersky Endpoint Security for Android não estarão disponíveis). Para continuar usando o aplicativo no modo de funcionalidade completa, é necessário renovar a Licença comercial.

Para ativar o Kaspersky Endpoint Security for Android:

1. No Console EMM, abra as configurações do aplicativo Kaspersky Endpoint Security for Android.
2. No campo `LicenseActivationCode`, insira o código de ativação do aplicativo.

   Para ativar o aplicativo em um dispositivo, você deve ter acesso aos servidores de ativação da Kaspersky.

Como conectar um dispositivo ao Kaspersky Security Center

Depois que o Kaspersky Endpoint Security for Android estiver instalado em um dispositivo móvel, você poderá conectar o dispositivo ao Kaspersky Security Center. Os dados necessários para conectar o dispositivo ao Kaspersky Security Center são transmitidos para o dispositivo móvel juntamente com as outras configurações listadas no arquivo de configuração. Depois de conectar o dispositivo ao Kaspersky Security Center, é possível usar políticas de grupo para configurar centralmente as configurações do aplicativo. Também é possível receber relatórios e estatísticas sobre o desempenho do Kaspersky Endpoint Security for Android.

Antes de conectar dispositivos ao Kaspersky Security Center, certifique-se de que as seguintes condições sejam atendidas:

- O plug-in de administração do Kaspersky Endpoint Security for Android está instalado na estação de trabalho do administrador.
- A porta para conectar dispositivos móveis está aberta nas propriedades do Servidor de Administração.
- A exibição da pasta **Gerenciamento de dispositivo móvel** está ativada no Console de Administração.
- Um certificado geral para identificar o usuário do dispositivo móvel foi criado no armazenamento de certificados do Kaspersky Security Center.

Antes de conectar dispositivos ao Kaspersky Security Center, recomenda-se o seguinte:

- Caso deseje criar tarefas e políticas para dispositivos móveis, crie um grupo de administração separado para dispositivos móveis.
- Caso deseje mover automaticamente os dispositivos móveis para um grupo de administração separado, crie uma regra para mover dispositivos automaticamente da pasta **dispositivos não atribuídos**.
- Caso deseje configurar o Kaspersky Endpoint Security for Android centralmente, crie uma política de grupo.

Para conectar um dispositivo ao Kaspersky Security Center:

1. No Console EMM, abra as configurações do aplicativo Kaspersky Endpoint Security for Android.
2. No campo `KscServer`, digite o nome DNS ou o endereço IP do servidor de administração do Kaspersky Security Center. A porta padrão é 13292.
3. Se você não quiser que o usuário seja distraído por notificações do Kaspersky Endpoint Security for Android, desative as notificações do aplicativo. Para isso, defina a configuração `DisableNotification = True`.

   Após a conexão, o aplicativo exibe todas as notificações. Você pode desativar determinadas notificações do aplicativo nas configurações da política.

   Não desative as notificações do aplicativo caso não use o Kaspersky Security Center. Isso pode fazer com que um usuário não receba notificações sobre a expiração da licença. Como resultado, o aplicativo deixará de executar suas funções.

Após a configuração da conexão, o Kaspersky Endpoint Security for Android exibe uma notificação solicitando que você conceda os seguintes direitos e permissões adicionais:

- Permissão para usar a câmera para a operação do antirroubo (comando **Retrato**).
- Permissão para usar a localização para a operação do antirroubo (comando **Localizar dispositivo**).
- Direitos de administrador do dispositivo (proprietário do perfil de trabalho do Android) para a operação das seguintes funções do aplicativo:
  - Instalar o certificado de segurança.
  - Configurar o Wi-Fi.
  - Configurar o Exchange ActiveSync.
  - Restringir o uso da câmera, Bluetooth e Wi-Fi.

Devido às características específicas de um perfil de trabalho do Android (ausência do serviço de Acessibilidade), os recursos Controle de aplicativos e Antirroubo não estão disponíveis no aplicativo.

Quando o usuário conceder os direitos e permissões necessários, o dispositivo será conectado ao Kaspersky Security Center. Caso uma regra para mover automaticamente os dispositivos para um grupo de administração não tenha sido criada, o dispositivo será automaticamente adicionado à pasta **dispositivos não atribuídos**. Se uma regra para mover dispositivos automaticamente para um grupo de administração tiver sido criada, o dispositivo será automaticamente adicionado ao grupo definido.

O Kaspersky Endpoint Security oferece os seguintes formatos de nomes de dispositivos:

- Modelo do dispositivo [e-mail, ID do dispositivo]
- Modelo do dispositivo [e-mail (se houver) ou ID do dispositivo]

Um ID do dispositivo é um ID exclusivo que o Kaspersky Endpoint Security for Android gera a partir dos dados recebidos de um dispositivo. Para dispositivos móveis com Android 10 ou posterior, o Kaspersky Endpoint Security for Android usa o SSAID (ID do Android) ou checksum de outros dados recebidos do dispositivo. Para versões anteriores do Android, o aplicativo usa o IMEI. É possível configurar o formato do nome do dispositivo na política de grupo. Também é possível adicionar uma tag ao nome do dispositivo. Dessa maneira, é mais fácil encontrar e classificar dispositivos no Kaspersky Security Center. Essa tag está disponível apenas para o VMware AirWatch.

Para adicionar uma tag ao nome do dispositivo:

1. No Console EMM, abra as configurações do aplicativo Kaspersky Endpoint Security for Android.
2. No campo `KscDeviceNameTag`, selecione os valores:
   - `{DeviceSerialNumber}` – Número de série do dispositivo.
   - `{DeviceUid}` – Identificador exclusivo do dispositivo (UDID).
   - `{DeviceAssetNumber}` – Número do ativo do dispositivo. Esse número é criado internamente em sua organização.

   Recomendamos utilizar apenas esses valores. O VMware AirWatch tem suporte para outros valores, mas o Kaspersky Endpoint Security não pode garantir que esses valores funcionem.

É possível adicionar valores (por exemplo, `{DeviceSerialNumber} {DeviceUid}`). A tag será adicionada ao nome do dispositivo no Kaspersky Security Center. Um espaço separa a tag do nome do dispositivo. Por exemplo, caso o nome do dispositivo seja `Google Pixel 2 a10c6b75f7b31de9 22:7D:78:9E:C5:1E`, então `22:7D:78:9E:C5:1E` é a tag UDID. Se você usa o Kaspersky Security Center e o VMwareAirWatch, a tag permite que você identifique dispositivos nos dois consoles. Para fazer a correspondência do dispositivo, selecione os mesmos valores para o nome do dispositivo (por exemplo, o número de série do dispositivo).

Depois que o dispositivo for conectado ao Kaspersky Security Center, as configurações do aplicativo serão alteradas de acordo com a política de grupo. O Kaspersky Endpoint Security for Android ignora as configurações do aplicativo do arquivo de configuração configurado no Console EMM. É possível configurar todas as seções da política, exceto as seguintes:

- **Antirroubo** (bloqueio do dispositivo)
- **Contêineres**
- **Gerenciamento do dispositivo** (bloqueio da tela)
- **Controle de aplicativos** (bloqueio de aplicativos proibidos)
- **Perfil de trabalho do Android**
- **Gerenciar o Samsung KNOX**

Devido ao método usado para implementar um perfil de trabalho, não é possível aplicar as configurações de política de grupo a partir da seção **Perfil de trabalho do Android**. Essas configurações só podem ser aplicadas se o perfil de trabalho tiver sido criado usando o Kaspersky Security Center.

Arquivo AppConfig

Um arquivo de configuração é gerado para configurar o aplicativo em um Console EMM. As configurações do aplicativo no arquivo de configuração são apresentadas na tabela abaixo.

Configurações do arquivo de configuração

Chave de configuração	Descrição	Tipo	Valor
`LicenseActivationCode`	Código de ativação do aplicativo	String	Código de ativação do aplicativo composto de 20 letras latinas e numerais. Para ativar o aplicativo com um código de ativação, é preciso ter acesso à Internet para se conectar com os servidores de ativação da Kaspersky. Se você deixar o campo branco, o aplicativo será ativado com uma licença de avaliação. A licença de avaliação é válida por 30 dias. Quando da Licença de avaliação expirar, todos os recursos do aplicativo móvel Kaspersky Endpoint Security for Android serão desativados. Para continuar usando o aplicativo, você precisa comprar a licença comercial.
`EulaAcceptanceConfirmationV1`	<License Agreement link>	Choice	Essa configuração está disponível apenas para o VMware AirWatch. `Accepted` – Confirmo que li, compreendi e aceito por completo os termos e condições deste Contrato de Licença do Usuário Final. `Declined` – Não aceito os termos e condições deste Contrato de Licença do Usuário Final (EULA). Para aceitar os termos e condições do EULA para todos os dispositivos móveis, é preciso ter acesso à Internet para se conectar aos servidores da Kaspersky. Se você escolher `Recusado`, o aplicativo solicitará que o usuário aceite os termos e condições do EULA. Os usuários de dispositivos móveis podem aceitar as condições no Assistente de Configuração Inicial.
`EulaAcceptanceCodeV1`	Código do Contrato de Licença	String	As configurações estão disponíveis somente para o VMware AirWatch.
`EulaAcceptanceCodesV2`	Códigos do Contrato de Licença	String	

			Utilize a `EulaAcceptanceCodeV1` caso queira aceitar um único Contrato de Licença do Usuário Final (EULA). Utilize a `EulaAcceptanceCodesV2` caso queira aceitar vários EULAs ao mesmo tempo. O campo `EulaAcceptanceCodesV2` deve conter uma lista separada por ponto e vírgula de códigos EULA: `"<EULAid1>;<EULAid2>;<EULAid3>;..."`. O código do Contrato de licença está contido no Contrato de Licença do Usuário Final. *Para saber o código do Contrato de Licença:* 1. Copie o link do Contrato de Licença (`EulaAcceptanceConfirmationV1`) do Console EMM. 2. Cole o link no navegador. O Contrato de Licença do Usuário Final (EULA) é aberto. 3. Leia os termos e condições deste EULA e encontre o código do Contrato de Licença. Para aceitar os termos e condições do EULA para todos os dispositivos móveis, é preciso ter acesso à Internet para se conectar aos servidores da Kaspersky. Caso o campo seja deixado em branco, o aplicativo solicitará que o usuário aceite os termos e condições do EULA. O usuário do dispositivo móvel pode aceitar as condições no Assistente de Configuração Inicial. Caso os valores de ambos os campos sejam especificados, os termos e condições de todos os EULAs especificados neles serão aceitos.
`KscServer`	Endereço e porta do Servidor de Administração do Kaspersky Security Center	String	Nome DNS ou endereço IP do Servidor de Administração do Kaspersky Security Center e número da porta. Insira o endereço da seguinte forma: `<server address>:<port>`. Se você inserir o endereço do servidor sem especificar a porta, o aplicativo usará a porta padrão 13292.
`DisableNotification`	Desativar notificações do aplicativo antes de	Boolean	`True` – O Kaspersky Endpoint Security for Android oculta todas as notificações do aplicativo. O Kaspersky Endpoint Security for Android oculta notificações

	conectar ao Kaspersky Security Center		até que o dispositivo conecte ao Kaspersky Security Center. Após a conexão, o aplicativo exibe todas as notificações. Você pode desativar determinadas notificações do aplicativo nas configurações da política. Não desative as notificações do aplicativo caso não use o Kaspersky Security Center. Isso pode fazer com que um usuário não receba notificações sobre a expiração da licença. Neste caso, o aplicativo pararia de funcionar. `False` – O Kaspersky Endpoint Security for Android exibe todas as notificações do aplicativo.
`ScanScheduleType`	Modo de execução da verificação	Choice	`AfterUpdate` – Inicia uma verificação de vírus após uma atualização do banco de dados. O aplicativo atualiza os bancos de dados antivírus de acordo com o agendamento definido `(UpdateScheduleType)`. `Daily` – Inicia uma verificação de vírus uma vez por dia. Configurar a hora de início da verificação `(ScanScheduleTime)`. `Weekly` – Inicia uma verificação de vírus uma vez por semana. Selecione o dia da semana para iniciar uma verificação de vírus `(ScanScheduleDay)` e configure o horário `(ScanScheduleTime)`. `Off` – O início automático de uma verificação de vírus é desativado. Independente de qual o valor estiver definido, o usuário do dispositivo pode iniciar manualmente uma verificação de vírus.
`ScanScheduleDay`	Dia da verificação	Choice	`Monday / Tuesday / Wednesday / Thursday / Friday / Saturday / Sunday` Você somente pode selecionar um valor para esta configuração.
`ScanScheduleTime`	Hora da verificação	String	O horário pode ser indicado em formato de 24 horas (por exemplo, 13:00) ou no formato de 12 horas (por exemplo, 10:30 P.M.).
`ScanScheduleLock`	Configuração do bloqueio do modo de execução da verificação	Boolean	`True` – O usuário não pode acessar as configurações do modo de execução da verificação de vírus dentro das configurações do aplicativo.

			`False` – O usuário pode configurar o modo de execução de verificação de vírus e, por exemplo, desativar o início automático de uma verificação de vírus.
`ScanOnlyExecutableFiles`	Tipos de arquivos para verificar (Verificação de vírus)	Choice	`AllFiles` – Verificar todos os arquivos. `OnlyExecutables` – Somente verificar arquivos executáveis. Os arquivos executáveis são arquivos com as extensões .apk (.zip), .dex ou .so. No Kaspersky Endpoint Security for Android Service Pack 4 Maintenance Release 1, não é possível ativar a verificação apenas de arquivos executáveis.
`ScanArchives`	Verificar os arquivos comprimidos ao descompactar	Boolean	`True` – O aplicativo descompacta os arquivos comprimidos e verifica o seu conteúdo. `False` – O aplicativo somente verifica os arquivos comprimidos. O aplicativo somente verifica arquivos comprimidos com a extensão .zip (.apk). No Kaspersky Endpoint Security for Android Service Pack 4 Maintenance Release 1, não é possível desativar a verificação do conteúdo de arquivos comprimidos.
`ScanActionOnThreatFound`	Ação na detecção de ameaça (Verificação de vírus)	Choice	`Quarantine` – O aplicativo coloca os objetos detectados na Quarentena. A quarentena armazena os arquivos comprimidos como arquivos comprimidos, para que não danifiquem o dispositivo. Esse Quarentena permite excluir ou restaurar os arquivos que foram movidos para isolado dedicado. `Delete` – O aplicativo exclui os objetos detectados. `Skip` – O aplicativo deixa os objetos detectados inalterados. Se os objetos detectados foram ignorados, o Kaspersky Endpoint Security for Android avisa o usuário sobre os problemas na proteção do dispositivo. Quando houver uma tentativa de acessar um objeto no dispositivo (tal como uma tentativa de copiá-lo ou abri-lo), o aplicativo bloqueia o acesso ao objeto. `AskUser` – O aplicativo solicita que o usuário selecione uma ação para cada objeto detectado: ignorar, colocar na quarentena ou excluir. Quando múltiplos objetos são detectados, o usuário pode aplicar uma ação selecionada a todos os objetos.

			As informações sobre as ameaças detectadas e as ações empreendidas neles são registradas nos relatórios do aplicativo.
`ScanLock`	Configuração do bloqueio nas configurações da verificação	Boolean	`True` – As seguintes configurações da verificação não podem ser acessadas pelo usuário nas configurações do aplicativo: os tipos de arquivos para verificar, a verificação de arquivos comprimidos e a ação para empreender em uma ameaça detectada. `False` – O usuário pode definir as configurações da verificação e, por exemplo, selecionar a ação `Skip` para as ameaças detectadas.
`ScanAndProtectionAdwareRiskware`	Bloqueie adware, discadores automáticos e aplicativos que podem ser usados por criminosos para danificar o dispositivo e os dados do usuário	Boolean	`True` – O aplicativo detecta adwares e outros aplicativos que podem ser explorados por criminosos para danificar o dispositivo do usuário ou seus dados pessoais. `False` – O aplicativo ignora adwares e outros aplicativos que podem ser explorados por criminosos para danificar o dispositivo do usuário ou seus dados pessoais.
`ProtectionMode`	Modo de Proteção em tempo real	Choice	`Recommended` – O aplicativo verifica novos aplicativos somente uma vez, imediatamente após serem instalados, assim como os arquivos na pasta Downloads. `Extended` – O aplicativo verifica todos os arquivos que o usuário abre, modifica, copia, executa e salva no dispositivo. O aplicativo também verifica novos aplicativos e arquivos da pasta Downloads. `Disabled` – A proteção em tempo real está desativada.
`UseKsnMode`	Modo da Kaspersky Security Network	Choice	`Recommended` – O aplicativo troca dados com a Kaspersky Security Network (KSN). O Kaspersky Endpoint Security for Android usa a KSN para a proteção em tempo real do dispositivo contra as ameaças (proteção na nuvem) e a operação da proteção na web na Internet.

			`Extended` – O aplicativo troca dados com a Kaspersky Security Network e envia ao Laboratório de Vírus determinadas estatísticas de desempenho do Kaspersky Endpoint Security for Android. Estas informações permitem manter o acompanhamento das ameaças em tempo real. Nenhum dado pessoal é coletado, processado ou armazenado por serviços KSN. `Disabled` – O aplicativo não usa os dados da Kaspersky Security Network. Você não pode ativar a Proteção na Web (`EnableWebFilter`). O componente Proteção na nuvem não está disponível para o Antivírus.
`ProtectScanOnlyExecutableFiles`	Tipos de arquivos para verificar (Proteção em Tempo real)	Boolean	`AllFiles` – Verificar todos os arquivos. `OnlyExecutables` – Somente verificar arquivos executáveis. Os arquivos executáveis são arquivos com as extensões .apk (.zip), .dex ou .so. No Kaspersky Endpoint Security for Android Service Pack 4 Maintenance Release 1, não é possível ativar a verificação apenas de arquivos executáveis.
`ProtectionActionOnThreatFound`	Ação na detecção de ameaça (Proteção em Tempo real)	Choice	`Quarantine` – O aplicativo coloca os objetos detectados na Quarentena. A quarentena armazena os arquivos comprimidos como arquivos comprimidos, para que não danifiquem o dispositivo. A quarentena permite excluir ou restaurar os arquivos que foram movidos para o armazenamento isolado. `Delete` – O aplicativo exclui objetos detectados. `Skip` – O aplicativo deixa os objetos detectados inalterados. Se os objetos detectados foram ignorados, o Kaspersky Endpoint Security for Android avisa o usuário sobre os problemas na proteção do dispositivo. Quando for feita uma tentativa de acessar um objeto no dispositivo (como uma tentativa de copiá-lo ou abri-lo), o aplicativo bloqueia o acesso ao objeto. As informações sobre as ameaças detectadas e as ações empreendidas neles são registradas nos relatórios do aplicativo.
`ProtectionLock`	Configuração do bloqueio nas configurações	Boolean	`True` – As seguintes configurações de proteção em tempo real não podem ser acessadas pelo usuário nas configurações do aplicativo: modo de

	de proteção em tempo real		proteção em tempo real, tipos de arquivos para verificar e a ação para empreender quando uma ameaça for detectada. `False` – O usuário pode definir as configurações de proteção em tempo real e, por exemplo, selecionar a ação `Skip` para as ameaças detectadas.
`UpdateScheduleType`	Modo de execução da atualização dos bancos de dados	Choice	`Daily` – Verificar novos bancos de dados antivírus e baixá-los nos dispositivos uma vez por dia. Configurar a hora de início da atualização do banco de dados `(UpdateScheduleTime)`. `Weekly` – Verificar novos bancos de dados antivírus e baixá-los nos dispositivos uma vez por semana. Selecione o dia da semana para iniciar uma atualização do banco de dados `(UpdateScheduleDay)` e configure o horário `(UpdateScheduleTime)`. `Off` – A atualização automática dos bancos de dados antivírus é desativada. Qualquer que seja o valor definido, o usuário pode iniciar manualmente uma atualização do banco de dados antivírus.
`UpdateScheduleDay`	Dia para iniciar uma atualização do banco de dados	Choice	`Monday / Tuesday / Wednesday / Thursday / Friday / Saturday / Sunday` Você somente pode selecionar um valor para esta configuração.
`UpdateScheduleTime`	Hora de início da atualização do banco de dados	String	O horário pode ser indicado em formato de 24 horas (por exemplo, 13:00) ou no formato de 12 horas (por exemplo, 10:30 P.M.).
`UpdateScheduleLock`	Configuração do bloqueio do modo de execução da atualização do banco de dados	Boolean	`True` – O usuário não pode acessar as configurações do modo de execução da atualização dos banco de dados dentro das configurações do aplicativo. `False` – O usuário pode configurar o modo de execução da atualização do banco de dados e, por exemplo, desativar a função de início automático das atualizações do banco de dados antivírus.
`AllowUpdateInRoaming`	Atualizar os bancos de dados quando em roaming	Boolean	`True` – O aplicativo baixa os bancos de dados antivírus se o dispositivo estiver na zona de roaming. O aplicativo baixa os bancos de dados antivírus de acordo com o agendamento definido `(UpdateScheduleType)`. `False` – O aplicativo baixa os bancos de dados antivírus somente se o dispositivo estiver na rede doméstica.

`EnableWebFilter`	Proteção na Web	Boolean	`True` – O aplicativo usa o componente proteção na web para bloquear sites maliciosos e de phishing na Internet. A Proteção na Web somente suporta o Google Chrome. Sites maliciosos e de phishing que usam o protocolo HTTPS conseguem permanecer desbloqueados se o domínio for confiável. Se o domínio não for confiável, a Proteção na Web bloqueará sites maliciosos e de phishing. `False` – A proteção contra sites maliciosos e de phishing é desativada. Para que o componente Proteção na Web funcione, as seguintes condições devem ser atendidas: • Os usuários dos dispositivos aceitam a Política de Privacidade e a Declaração da Proteção na Web no Assistente de Configuração Inicial ou nas configurações do aplicativo. • Um servidor proxy é configurado nas configurações do navegador: `ProxyMode = "fixed_servers"` `ProxyServer = "127.0.0.1:3128"` `DisableSpdy = true` `DataCompressionProxyEnabled = false` A configuração do servidor proxy pode variar dependendo da versão do Google Chrome. Para obter mais detalhes sobre a configuração do Google Chrome, visite o site do projeto Chromium. Após o aplicativo Kaspersky Endpoint Security for Android for removido do dispositivo móvel, redefina as configurações do servidor proxy. • O Uso da KSN está ativado nas configurações do aplicativo: `UseKsnMode = Recommended` ou `UseKsnMode = Extended`. • Recomenda-se selecionar o Google Chrome como o navegador padrão nas configurações do sistema operacional.

`EnableWebFilterLock`	Configuração do bloqueio da Proteção na Web	Boolean	`True` – O usuário não pode acessar as configurações da Proteção na Web dentro das configurações do aplicativo. `False` – O usuário pode definir as configurações da proteção na web e, por exemplo, desativar a proteção contra sites maliciosos e de phishing na Internet.
`UpdateServer`	Endereço do servidor de fonte de atualização do banco de dados	String	Endereço do servidor que hospeda as atualizações do banco de dados, por exemplo, `http://update.server.com`. Se você deixar o campo em branco, o Kaspersky Endpoint Security for Android usa os servidores de atualização da Kaspersky.
`AllowGoogleAnalytics`	Enviar dados para os serviços Google Analytics for Firebase, SafetyNet Attestation, Firebase Performance Monitoring e Crashlytics	Boolean	`Verdadeiro`: o aplicativo envia automaticamente os dados de operação do Kaspersky Endpoint Security for Android aos serviços Google Analytics for Firebase, SafetyNet Attestation, Firebase Performance Monitoring e Crashlytics. Esses dados são necessários para aprimorar o desempenho do aplicativo e para analisar a satisfação do usuário. Os dados são transmitidos para os serviços Google Analytics for Firebase, SafetyNet Attestation, Firebase Performance Monitoring e Crashlytics por meio de uma conexão segura. O acesso e a proteção de dados são regulados pelos termos de uso relevantes dos serviços Google Analytics for Firebase, SafetyNet Attestation, Firebase Performance Monitoring e Crashlytics. `Falso`: o envio de dados para os serviços Google Analytics for Firebase, SafetyNet Attestation, Firebase Performance Monitoring e Crashlytics está desativado.
`KscDeviceNameTag`	Tag do nome do dispositivo do Kaspersky Security Center	String	Essa configuração está disponível apenas para o VMware AirWatch. A tag será adicionada ao nome do dispositivo no Kaspersky Security Center. Um espaço separa a tag do nome do dispositivo. Dessa maneira, é mais fácil encontrar e classificar dispositivos no Kaspersky Security Center.

			• `{DeviceSerialNumber}` – Número de série do dispositivo. • `{DeviceUid}` – Identificador exclusivo do dispositivo (UDID). • `{DeviceAssetNumber}` – Número do ativo do dispositivo. Esse número é criado internamente em sua organização. É possível adicionar valores (por exemplo, `{DeviceSerialNumber}` `{DeviceUid}`). Recomendamos utilizar apenas esses valores. O VMware AirWatch tem suporte para outros valores, mas o Kaspersky Endpoint Security não pode garantir que esses valores funcionem.
`KscGroup`	Nome do grupo de dispositivos	String	É possível especificar grupos de dispositivos em um console EMM. Quando um dispositivo for conectado ao Kaspersky Security Center, ele será adicionado automaticamente a uma subpasta da pasta Dispositivos não atribuídos. O nome da subpasta coincidirá com o nome do grupo especificado nesse parâmetro. É possível criar regras para mover dispositivos automaticamente para subpastas da pasta Dispositivos não atribuídos para grupos de administração na pasta Dispositivos gerenciados. Se esse campo for deixado em branco, o dispositivo será adicionado automaticamente à raiz da pasta Dispositivos não atribuídos.
`KscCorporateEmail`	E-mail corporativo do usuário	String	Você pode especificar os endereços de e-mail corporativo dos usuários em um console EMM. Estes e-mails serão exibidos no Kaspersky Security Center. A string deve ser um endereço de e-mail válido. Outros valores são ignorados.

Carga da rede

Esta seção contém informações sobre o volume do tráfego de rede que é trocado entre dispositivos móveis e o Kaspersky Security Center.

Volume de tráfego

Tarefa	Tráfego de saída	Tráfego de entrada	Tráfego total
Implementação inicial do aplicativo, Mb	0,08	17,76	17,84
A atualização inicial dos bancos de dados antivírus (o volume de tráfego pode ser diferente devido ao tamanho dos bancos de dados antivírus), MB	0,04	2,21	2,25
Sincronização do dispositivo móvel com o Kaspersky Security Center, MB	0,03	0,02	0,05
A atualização regular dos bancos de dados antivírus (o volume de tráfego pode ser diferente devido ao tamanho dos bancos de dados antivírus), MB	0,08	3,06	3,14
Execução de comandos Antirroubo Localizar o dispositivo (o volume de tráfego pode ser diferente devido às especificações da câmera incorporada e a qualidade das imagens), MB	0,09	0,8	0,17
Execução de comandos Antirroubo Retrato, MB	1,0	0,02	1,02
Execução de comandos Antirroubo Bloqueio do dispositivo, MB	0,06	0,05	0,11
Volume diário médio, MB	0,22	6,96	7,18

Participar na Kaspersky Security Network

Para proteger os dispositivos móveis de forma mais eficaz, o Kaspersky Endpoint Security for Android usa os dados coletados de usuários ao redor do mundo. *A Kaspersky Security Network* é projetada para processar tais dados.

A *Kaspersky Security Network (KSN)* é uma infraestrutura de serviços na nuvem que fornece o acesso à Base de Dados de Conhecimento on-line da Kaspersky, que contém informações sobre a reputação de arquivos, recursos da Web e softwares. A utilização dos dados da Kaspersky Security Network garante respostas mais rápidas dos aplicativos da Kaspersky a novas ameaças, aprimora o desempenho de alguns componentes de proteção e reduz a possibilidade de falsos positivos.

A participação na Kaspersky Security Network ajuda a Kaspersky a coletar informações sobre tipos e origens de novas ameaças em tempo real, desenvolver métodos para neutralizá-las e reduzir o número de alarmes falsos do Kaspersky Endpoint Security for Android. A participação na Kaspersky Security Network também permite acessar estatísticas de reputação para aplicativos e sites.

Quando você participa da Kaspersky Security Network, determinadas estatísticas são coletadas enquanto o Kaspersky Endpoint Security for Android estiver em execução e são automaticamente enviadas à Kaspersky. Estas informações permitem manter o acompanhamento das ameaças em tempo real. Os arquivos ou as suas partes que podem ser explorados por intrusos para danificar o computador ou o conteúdo do usuário também podem ser enviados à Kaspersky para um exame adicional.

O uso da Kaspersky Security Network é necessário para a operação do Kaspersky Endpoint Security for Android. A KSN é usada pelos componentes principais do aplicativo: Antivírus, Proteção na Web e Controle de aplicativos. A recusa em participar da KSN reduz o nível da proteção de dispositivo, que pode levar a infecção do dispositivo e perda dos dados. Para iniciar o uso da Kaspersky Security Network, é necessário aceitar os termos do Contrato de Licença do Usuário Final ao instalar o aplicativo. Ao ler o Contrato de Licença do Usuário Final, você poderá saber quais dados são transmitidos à Kaspersky Security Network pelo Kaspersky Endpoint Security for Android.

Para aprimorar o desempenho do aplicativo, você pode, adicionalmente, fornecer dados estatísticos à Kaspersky Security Network. O fornecimento das informações mencionadas acima à KSN é voluntário. Para iniciar o uso da Kaspersky Security Network, é necessário aceitar os termos de um acordo especial – a *Declaração da Kaspersky Security Network*. Você pode optar por não participação na Kaspersky Security Network a qualquer momento. A Declaração da Kaspersky Security Network descreve os tipos de dados que o Kaspersky Endpoint Security for Android transmite para a Kaspersky Security Network.

Troca de informações com a Kaspersky Security Network

Para aprimorar a proteção em tempo real, o Kaspersky Security for Mobile usa o serviço na nuvem da Kaspersky Security Network para a operação dos seguintes componentes:

- **Antivírus.** O aplicativo obtém o acesso à Base de Conhecimento on-line da Kaspersky quanto à reputação de arquivos e aplicativos. A verificação é executada para as ameaças cujas informações ainda não foram adicionadas ao banco de dados antivírus, mas já estão disponíveis na KSN. O serviço na nuvem da Kaspersky Security Network fornece a operação completa do Antivírus e reduz a probabilidade de falsos alarmes.

- **Proteção na Web.** O aplicativo usa os dados recebidos da KSN para executar uma verificação de sites antes que eles sejam abertos. O aplicativo também determina a categoria de site para controlar o acesso à Internet para os usuários de acordo com as listas de categorias permitidas e bloqueadas (por exemplo, a categoria "Comunicações via Internet").

- **Controle de aplicativos.** O aplicativo determina a categoria de aplicativo para restringir a inicialização de aplicativos que não atendam aos requisitos de segurança corporativa com base em listas de categorias permitidas e bloqueadas (por exemplo, a categoria "Jogos").

As informações sobre o tipo de dados enviados à Kaspersky ao usar a KSN durante a operação do antivírus e controle de aplicativos estão disponíveis no Contrato de Licença do Usuário Final. Ao aceitar os termos e condições do Contrato de Licença, o usuário concorda em transferir as seguintes informações.

As informações sobre o tipo de dados enviados à Kaspersky, ao usar a KSN durante a operação da proteção na web, estão disponíveis na Declaração sobre o processamento de dados para a proteção na web. Ao aceitar os termos e condições da Declaração, o usuário concorda em transferir as seguintes informações.

Para os propósitos de identificar as ameaças de segurança de informações emergentes, ameaças de intrusão e ameaças que são difíceis de detectar (junto com as suas respectivas origens) e para aprimorar a proteção das informações armazenadas e processadas em um dispositivo, você pode estender sua participação na Kaspersky Security Network.

Para trocar dados com a KSN com os propósitos de aprimora o desempenho do aplicativo, as seguintes condições devem ser cumpridas:

- Você ou o usuário do dispositivo devem ler e aceitar os termos da Declaração da Kaspersky Security Network. Caso opte pelo aceite da Declaração pelos usuários, eles receberão uma notificação na tela principal do aplicativo para aceitar os termos da Declaração. Os usuários também podem aceitar as Declarações na seção **Sobre o aplicativo**, nas configurações do Kaspersky Endpoint Security for Android.

  Caso opte por aceitar as Declarações globalmente, as versões das Declarações aceitas por meio do Kaspersky Security Center devem corresponder às versões já aceitas pelos usuários. Caso contrário, os usuários serão informados sobre o problema e convidados a aceitar a versão de uma Declaração que corresponda à versão aceita globalmente pelo administrador. O status do dispositivo no plug-in do Kaspersky Security for Mobile (Devices) também mudará para *Aviso*.

- É preciso definir as configurações de política de grupo para permitir que as estatísticas sejam enviadas à KSN.

Você pode optar por não enviar dados estatísticos par a Kaspersky Security Network a qualquer momento. As informações sobre o tipo de dados estatísticos enviados à Kaspersky ao usar a KSN durante a operação do aplicativo móvel do Kaspersky Endpoint Security for Android estão disponíveis na Declaração da Kaspersky Security Network.

Para obter mais informações sobre a coleta de dados para a KSN, consulte a seção "Provisão de dados".

A provisão de dados para a KSN é voluntária. Caso queira, é possível desativar a troca de dados com a KSN.

Ativar e desativar o uso da Kaspersky Security Network

Para a operação de componentes do Kaspersky Endpoint Security for Android que usam a Kaspersky Security Network, o aplicativo envia solicitações aos serviços na nuvem. As solicitações contêm os dados conforme descrito na seção "Provisão de dados".

Se o uso da Kaspersky Security Network estiver desativado no dispositivo, os componentes de Proteção na Nuvem, a Proteção na Web e Controle de aplicativos serão desativados automaticamente.

Para ativar ou desativar o uso da Kaspersky Security Network:

1. Abra a janela com as configurações da política de gerenciamento para dispositivos móveis nos quais o Kaspersky Endpoint Security for Android estiver instalado.
2. Na janela **Propriedades** da política, selecione a seção **Adicional**.
3. Na seção **Configurações da Kaspersky Security Network (KSN)**, defina as configurações para usar a Kaspersky Security Network:
   - Selecione a caixa de seleção **Usar a Kaspersky Security Network** para a operação dos seguintes componentes: Antivírus (Proteção na Nuvem), Proteção na Web e Controle de aplicativos (categorias de aplicativos).
   - Selecione caixa de seleção **Permitir que as estatísticas sejam enviadas para a KSN** para enviar dados à Kaspersky. Estes dados ajudarão o aplicativo Kaspersky Endpoint Security for Android a mais rapidamente responder às ameaças, aprimorar o desempenho dos componentes de proteção e diminuir a probabilidade de falsos alarmes.
4. Clique no botão **Aplicar** para salvar as alterações efetuadas.

As configurações do dispositivo móvel são definidas depois da próxima sincronização do dispositivo com o Kaspersky Security Center. Após a política ter sido aplicada, os componentes que usam a Kaspersky Security Network são desativados e as configurações do componente ficam indisponíveis.

Usar a Kaspersky Private Security Network

A Kaspersky Private Security Network (*KSN privada* ou *KPSN)* é uma solução que concede acesso aos bancos de dados de reputação da Kaspersky Security Network, sem enviar dados dos dispositivos dos usuários para a Kaspersky Security Network.

Um banco de dados de reputação de objetos (arquivos ou URLs) é armazenado no servidor da Kaspersky Private Security Network, mas não nos servidores da Kaspersky Security Network. Os bancos de dados de reputação da KPSN são armazenados na rede corporativa e gerenciados pelo administrador da empresa.

Quando a KPSN é ativada, o Kaspersky Endpoint Security não envia nenhum dado estatístico dos dispositivos para a KSN.

Para ativar o uso da KSN Privada por meio do Kaspersky Security Center:

1. Na janela principal do Kaspersky Security Center Web Console ou Cloud Console, clique em **Configurações** ( ).

   A janela de propriedades do servidor de administração é aberta.

2. Na guia **Geral**, selecione a seção de **configurações de proxy KSN.**

3. Mude o botão de alternância para a posição **Usar Kaspersky Private Security Network ATIVADO**.

4. Clique no botão **Selecionar arquivo com configurações de Proxy da KSN** e procure o arquivo de configuração que possui a extensão pkcs7 ou pem (fornecido pela Kaspersky).

5. Clique em **Abrir**.

6. Caso as configurações do servidor proxy tenham sido definidas nas propriedades do servidor de administração, mas a sua arquitetura de rede requeira o uso da KSN Privada diretamente, ative a opção **Ignorar as configurações do servidor proxy KSC ao conectar na KSN Privada**. Caso contrário, as solicitações dos aplicativos gerenciados não podem alcançar a KSN Privada.

7. Clique no botão **Salvar**.

Após baixar as configurações, a interface exibe o nome e os contatos do provedor, assim como a data de criação do arquivo com as configurações da KSN Privada. As configurações KPSN são aplicadas aos dispositivos móveis.

Quando você muda para a KSN privada, o Controle de aplicativos não fornece suporte às mesmas categorias de aplicativos da KSN Global. A categorização de aplicativos estará disponível se você escolher voltar para a KSN.

Provisão de dados para serviços de terceiros

O Kaspersky Endpoint Security for Android usa os serviços Google™ conhecidos como Firebase Cloud Messaging, Google Analytics for Firebase™, SafetyNet Attestation, Firebase Performance Monitoring e Crashlytics. O Kaspersky Endpoint Security for Android usa o serviço Firebase Cloud Messaging (FCM) para assegurar a entrega em tempo hábil de comandos a dispositivos móveis e a sincronização forçada quando as configurações de política são modificadas. O Kaspersky Endpoint Security for Android usa os serviços Google Analytics for Firebase, SafetyNet Attestation, Firebase Performance Monitoring e Crashlytics para melhorar o desempenho do aplicativo e ajudar a Kaspersky a criar materiais de marketing mais eficazes.

Trocar informações com o Firebase Cloud Messaging

O Kaspersky Endpoint Security for Android usa o serviço Firebase Cloud Messaging (FCM) para assegurar a entrega em tempo hábil de comandos a dispositivos móveis e a sincronização forçada quando as configurações de política são modificadas. O aplicativo também usa notificações push.

Para usar o Firebase Cloud Messaging, você deve definir as configurações do serviço no Kaspersky Security Center. Para obter mais detalhes sobre como configurar o Firebase Cloud Messaging no Kaspersky Security Center, consulte a *Ajuda do Kaspersky Security Center*. Se as configurações do Firebase Cloud Messaging não estiverem definidas, os comandos no dispositivo móvel e as configurações de política serão entregues quando o dispositivo for sincronizado com o Kaspersky Security Center de acordo com a programação definida na política (por exemplo, a cada 24 horas). Em outras palavras, os comandos e configurações de política serão entregues com um atraso.

Para os propósitos de apoiar a funcionalidade principal do produto, você aceita fornecer automaticamente a ID exclusiva da instalação do aplicativo (ID da Instância) ao serviço Firebase Cloud Messaging, bem como os seguintes dados:

- Informações sobre o software instalado: versão do aplicativo, ID do aplicativo, versão da compilação do aplicativo, nome do pacote do aplicativo.
- Informações sobre o computador no qual o software está instalado: versão do SO, ID do dispositivo, versão dos serviços Google.
- Informações sobre o FCM: ID do aplicativo no FCM, ID do usuário do FCM, versão do protocolo.

Os dados são transmitidos aos serviços Firebase por meio de uma conexão segura. O acesso a e a proteção das informações são governadas pelos termos relevantes dos serviços do Firebase: https://firebase.google.com/terms/data-processing-terms/, https://firebase.google.com/support/privacy/.

Para prevenir a troca de informações com o serviço Firebase Cloud Messaging:

1. Na árvore do console, selecione **Gerenciamento de dispositivo móvel → Dispositivos móveis**.
2. No menu de contexto da pasta **Dispositivos móveis**, selecione **Propriedades**.
3. Na janela Propriedades da pasta **Dispositivos móveis**, selecione a seção **de configurações do Google Firebase Cloud Messaging**.
4. Clique no botão **Redefinir as configurações**.

Trocar informações com o Google Analytics for Firebase, SafetyNet Attestation, Firebase Performance Monitoring e Crashlytics

Caso você use o Plug-in de administração de uma versão anterior e tenha ativado a troca de dados com o serviço do Google Analytics, o Kaspersky Endpoint Security for Android Service Pack 4 Maintenance Release 3 executará a troca de dados com o serviço Google Analytics para Firebase. O suporte para Google Analytics foi descontinuado.

O Kaspersky Security for Mobile troca dados com os serviços Google Analytics for Firebase, SafetyNet Attestation, Firebase Performance Monitoring e Crashlytics com os seguintes objetivos:

- Para aprimorar o desempenho do aplicativo:

  Para trocar dados com os serviços Google Analytics for Firebase, SafetyNet Attestation, Firebase Performance Monitoring e Crashlytics com o objetivo de aprimorar o desempenho do aplicativo, as seguintes condições devem ser atendidas:

- O administrador ou o usuário do dispositivo devem ler e aceitar os termos da Declaração da Kaspersky Security Network. Caso opte pelo aceite da Declaração pelos usuários, eles receberão uma notificação na tela principal do aplicativo para aceitar os termos da Declaração. Os usuários também podem aceitar as Declarações na seção **Sobre o aplicativo**, nas configurações do Kaspersky Endpoint Security for Android.

  Caso opte por aceitar as Declarações globalmente, as versões das Declarações aceitas por meio do Kaspersky Security Center devem corresponder às versões já aceitas pelos usuários. Caso contrário, os usuários serão informados sobre o problema e convidados a aceitar a versão de uma Declaração que corresponda à versão aceita globalmente pelo administrador. O status do dispositivo no plug-in do Kaspersky Security for Mobile (Devices) também mudará para *Aviso*.

- O administrador deve definir as configurações de política de grupo para permitir que as estatísticas sejam enviadas à KSN (veja abaixo).

- Para ajudar a Kaspersky a criar materiais de marketing mais eficazes.

  Para trocar dados com os serviços Google Analytics for Firebase, SafetyNet Attestation, Firebase Performance Monitoring e Crashlytics com o objetivo de ajudar a Kaspersky a criar materiais de marketing eficazes, as seguintes condições devem ser atendidas:

  - O administrador ou o usuário do dispositivo devem ler e aceitar os termos da Declaração relativos ao processamento de dados para fins de marketing. Caso opte pelo aceite da Declaração pelos usuários, eles podem aceitar os termos da Declaração ao instalar o aplicativo ou na seção **Sobre o aplicativo**, nas configurações do Kaspersky Endpoint Security for Android.

  - O administrador deve definir as configurações de política de grupo para permitir que as estatísticas sejam enviadas ao Google Analytics for Firebase, SafetyNet Attestation, Firebase Performance Monitoring e Crashlytics (consulte abaixo).

A provisão de dados para o Google Analytics for Firebase, SafetyNet Attestation, Firebase Performance Monitoring e Crashlytics de acordo com a Declaração relativa ao processamento de dados para fins de marketing

O Titular usa sistemas de informação de terceiros para processar dados. O processamento de dados feito por esses terceiros é regido pelas declarações de privacidade de tais sistemas de informação de terceiros. A seguir, os serviços que o Titular usa e os dados processados por eles:

Google Analytics para Firebase

Durante o uso do Software, os seguintes dados serão enviados para o Google Analytics para Firebase automaticamente e de forma regular, a fim de atingir a finalidade declarada:

- Informações do aplicativo (versão do aplicativo, ID do aplicativo e a ID do aplicativo no serviço Firebase, ID da instância no serviço Firebase, nome da loja onde o aplicativo foi obtido, carimbo de data/hora do primeiro lançamento do Software)
- ID da instalação do aplicativo no dispositivo e o método de instalação no dispositivo
- informações sobre a região e a localização do idioma
- informações sobre a resolução de tela do dispositivo
- informações sobre a obtenção de root pelo usuário
- informações de diagnóstico sobre o dispositivo do serviço SafetyNet Attestation
- informações sobre configuração do Kaspersky Endpoint Security for Android como recurso de Acessibilidade
- informações sobre transições entre as telas do aplicativo, duração da sessão, início e término de uma sessão de tela, nome da tela
- informações sobre o protocolo usado para enviar dados para o serviço Firebase, sua versão e ID do método de envio de dados utilizado
- detalhes sobre o tipo e os parâmetros do evento para o qual os dados são enviados
- informações sobre a licença do aplicativo, sua disponibilidade e o número de dispositivos
- informações sobre a frequência de atualizações do banco de dados de antivírus e sincronização com o Servidor de Administração
- informações sobre o Console de Administração (Kaspersky Security Center ou sistemas EMM de terceiros)
- ID do Android
- ID de publicidade
- informações sobre o Usuário: categoria de idade e sexo, identificador do país de residência e lista de interesses
- informações sobre o computador do Usuário onde o Software está instalado: nome do fabricante do computador, tipo de computador, modelo, versão e idioma (localidade) do sistema operacional, informações sobre o aplicativo aberto pela primeira vez nos últimos 7 dias e o aplicativo aberto pela primeira vez há mais de 7 dias

  Os dados são encaminhados para o Firebase por meio de um canal seguro. Informações sobre como os dados são processados in Firebase são publicadas em: https://firebase.google.com/support/privacy.

SafetyNet Attestation

Durante o uso do Software, os seguintes dados serão enviados para o SafetyNet Attestation automaticamente e de forma regular a fim de atingir a finalidade declarada:

- momento de verificação do dispositivo
- informações sobre software, nome e dados sobre os certificados do software
- resultados da verificação do dispositivo
- verificações de ID aleatórias para verificar os resultados do dispositivo de verificação

  Os dados são encaminhados para o SafetyNet Attestation por meio de um canal seguro. Informações sobre como os dados são processados in SafetyNet Attestation são publicadas em: https://policies.google.com/privacy.

Firebase Performance Monitoring

Durante o uso do Software, os seguintes dados serão enviados automaticamente e de forma regular para o Firebase Performance Monitoring a fim de alcançar a finalidade declarada:

- ID exclusiva de instalação
- nome de pacote do aplicativo
- versão do software instalado
- nível da bateria e estado de carregamento da bateria
- operadora
- estado de primeiro ou segundo plano da aplicação
- geografia
- Endereço IP
- código de idioma do dispositivo
- informações sobre a conexão de rádio/rede
- ID pseudônimo da instância do Software;
- tamanho da RAM e do disco
- sinalizador indicando se o dispositivo está rooteado;
- força do sinal
- duração dos rastreios automáticos
- rede e as seguintes informações correspondentes: código de resposta, tamanho da carga em bytes, tempo de resposta
- descrição do dispositivo

Os dados são encaminhados para o Firebase Performance Monitoring por meio de um canal seguro. Informações sobre como os dados são processados in Firebase Performance Monitoring são publicadas em: https://firebase.google.com/support/privacy.

Crashlytics

Durante o uso do Software, os seguintes dados serão enviados automaticamente e de forma regular para o Crashlytics a fim de alcançar a finalidade declarada:

- ID do software
- versão do software instalado
- sinalizador que indica se o Software estava sendo executado em segundo plano
- arquitetura da CPU
- ID único do evento
- data e hora do evento
- modelo do dispositivo
- espaço em disco total e quantidade atualmente utilizada
- o nome e versão do aplicativo
- RAM total e quantidade atualmente utilizada
- sinalizador indicando se o dispositivo está rooteado;
- orientação da tela no momento do evento
- fabricante de produto/hardware;
- ID exclusiva de instalação
- versão das estatísticas que estão sendo enviadas;
- o tipo de exceção do Software
- texto da mensagem de erro
- sinalizador que indica que a exceção do Software foi causada por uma exceção inserida
- ID da thread
- um sinalizador indicando se o quadro foi a causa do erro do software
- sinalizador que indica que a thread causou o encerramento inesperado do Software
- informação sobre o sinal que fez com que o software encerrasse inesperadamente: nome do sinal, código do sinal, endereço do sinal
- para cada quadro associado a uma thread, exceção ou erro: o nome do arquivo de quadro, número da linha do arquivo de quadro, símbolos de depuração, endereço e deslocamento na imagem binária, nome de

exibição da biblioteca com o quadro, tipo de quadro, sinalizador indicando se o quadro foi a causa do erro

- ID do SO;
- ID da emissão associada ao evento
- informação sobre eventos que aconteceram antes de o Software encerrar inesperadamente: identificador do evento, data e hora do evento, tipo de evento e valor
- valores de registro da CPU
- tipo de evento e valor

  Os dados são encaminhados para a Crashlytics por meio de um canal seguro. Informações sobre como os dados são processados in Crashlytics são publicadas em: https://firebase.google.com/terms/crashlytics-app-distribution-data-processing-terms.

O fornecimento das informações acima para processamento para fins de marketing é voluntário.

Para desativar a troca de dados com os serviços Google Analytics for Firebase, SafetyNet Attestation, Firebase Performance Monitoring e Crashlytics:

1. Abra a janela de configuração do gerenciamento da política para dispositivos móveis nos quais o aplicativo Kaspersky Endpoint Security for Android está instalado.
2. Na janela **Propriedades** da política, selecione a seção **Adicional**.
3. Na seção **Transferência de dados**, desmarque a caixa de seleção **Permitir a transferência de dados para ajudar a melhorar a qualidade, a aparência e o desempenho do aplicativo**.
4. Clique no botão **Aplicar** para salvar as alterações efetuadas.

As configurações do dispositivo móvel são definidas depois da próxima sincronização do dispositivo com o Kaspersky Security Center.

Aceitação global de Declarações adicionais

Para ativar a proteção fornecida pelo Kaspersky Endpoint Security for Android, os termos do Contrato de Licença do Usuário Final, bem como as Declarações adicionais (veja abaixo), devem ser aceitos. Uma política para a aceitação das Declarações listadas abaixo globalmente é configurada, para todos os usuários. Os usuários não serão convidados a ler e aceitar os termos dos seguintes Contratos e Declarações que já foram aceitos globalmente:

- Declaração da Kaspersky Security Network
- Declaração relativa ao processamento dos dados para a Proteção na Web
- Declaração quanto ao processamento dos dados para propósitos de marketing

Caso opte por aceitar as Declarações globalmente, as versões das Declarações aceitas por meio do Kaspersky Security Center devem corresponder às versões já aceitas pelos usuários. Caso contrário, os usuários serão informados sobre o problema e convidados a aceitar a versão de uma Declaração que corresponda à versão aceita globalmente pelo administrador. O status do dispositivo no plug-in do Kaspersky Security for Mobile (Devices) também mudará para *Aviso*.

Para escolher se os termos devem ser aceitos globalmente ou pelos usuários por meio da aplicação de uma política de grupo:

1. No árvore do console, na pasta **Dispositivos gerenciados**, selecione o grupo de administração ao qual os dispositivos Android pertencem.
2. Na área de trabalho do grupo, selecione a guia **Políticas**.
3. Clique duas vezes em qualquer coluna para abrir a janela de propriedades da política.
4. Na janela **Propriedades** da política, selecione a seção **Adicional**.
5. Na seção **Transferência de dados**, escolha se a Declaração sobre o processamento de dados para fins de marketing será aceita globalmente ou pelos usuários.
6. Na seção de **configurações do Kaspersky Security Network (KSN)**, escolha se a Declaração do Kaspersky Security Network será aceita globalmente ou pelos usuários.
7. Clique no botão **Aplicar** para salvar as alterações efetuadas.

O usuário pode aceitar os termos de uma Declaração ou recusá-los a qualquer momento na seção **Sobre o aplicativo** nas configurações do Kaspersky Endpoint Security for Android.

Samsung KNOX

O *Samsung KNOX* é uma solução móvel para configurar e proteger dispositivos móveis da Samsung que executam o sistema operacional Android. Para obter mais detalhes sobre o Samsung KNOX, visite o *site de Suporte Técnico da Samsung*.

Instalação do aplicativo Kaspersky Endpoint Security for Android por meio do KNOX Mobile Enrollment

O KNOX Mobile Enrollment (KME) faz parte da solução móvel Samsung KNOX. Ele é usado para instalação em lotes e configuração inicial de aplicativos em novos dispositivos Samsung adquiridos de fornecedores oficiais.

A instalação do Kaspersky Endpoint Security for Android através do KNOX Mobile Enrollment consiste nas seguintes etapas:

1. Crie um perfil KNOX MDM com o aplicativo Kaspersky Endpoint Security for Android.
2. Adicionar dispositivos no KNOX Mobile Enrollment.
3. Instalar o aplicativo Kaspersky Endpoint Security for Android no dispositivo móvel do usuário.

Para obter mais detalhes sobre como trabalhar com o KNOX Mobile Enrollment, consulte o *Guia do Usuário do KNOX Mobile Enrollment*.

A implantação via KNOX Mobile Enrollment é possível somente para os dispositivos Samsung. Para obter a lista de dispositivos compatíveis, visite *o site de suporte técnico da Samsung*.

Criar um perfil KNOX MDM

Um perfil *KNOX MDM* é um perfil que contém links para os aplicativos para a sua rápida implementação e para a configuração inicial nos dispositivos móveis.

Para criar um perfil KNOX MDM:

1. Efetue o login no console Samsung KNOX → **KNOX Mobile Enrollment**.
2. Selecione a seção **Perfis MDM**.
3. Clique em **Adicionar**.

   O Assistente de Novo Perfil KNOX MDM é iniciado.
4. Na etapa **Conexão ao servidor MDM**, selecione **O URI do servidor não é necessário para o meu serviço MDM** e clique em **Avançar**.
5. Na etapa **Informações do perfil MDM**:
   a. Insira as informações gerais sobre o perfil KNOX MDM: **Nome** e **Descrição** do perfil.
   b. Clique no botão **Adicionar aplicativos MDM** e insira o caminho para o arquivo de instalação APK.

      O arquivo de instalação para o Kaspersky Endpoint Security for Android está incluído no kit de distribuição do Kaspersky Security for Mobile. Primeiro, coloque o arquivo de instalação APK no Servidor da Web do Kaspersky Security Center ou em outro servidor que esteja acessível para baixar do dispositivo.
   c. Insira as configurações para conectar o dispositivo ao Kaspersky Security Center no campo **Dados de usuário JSON** no seguinte formato:
      `{"serverAddress":"ksc.server.com","serverPort":"12345","groupName":"MOBILE GROUP"}`.

      O dispositivo deve estar conectado ao Kaspersky Security Center para ativar o aplicativo, configure o dispositivo e envie os comandos.
   d. Selecione a caixa de seleção **Adicionar os Contratos Knox**.

      Para instalar o Kaspersky Endpoint Security for Android através do KNOX Mobile Enrollment, o usuário do dispositivo móvel deve aceitar os termos do Contrato de Licença da Samsung. Você pode exibir os termos do Contrato de Licença da Samsung na seção denominada **Contratos de Licença do Usuário Final, Termos do Serviço e Contratos de Usuário**. Você também pode adicionar outros documentos legais da sua empresa que são necessários para implementar um perfil KNOX MDM ao clicar no botão **Adicionar o Contrato de Licença do Usuário Final**.
   e. Limpe a caixa de seleção **Vincular a licença do Knox com este perfil**.

      As informações da licença Samsung KNOX são entregues ao dispositivo móvel junto com a política quando o dispositivo for sincronizado com o Kaspersky Security Center.
6. Clique no botão **Salvar**.

Como resultado, o novo perfil KNOX MDM com o aplicativo Kaspersky Endpoint Security for Android será adicionado à lista no console KME.

Adicionar dispositivos no KNOX Mobile Enrollment

Os dispositivos podem ser adicionados no console do KNOX Mobile Enrollment (KME) das seguintes formas:

- O fornecedor adiciona automaticamente os dispositivos no console KME após a compra dos dispositivos.

  Selecione este método se a sua organização estiver trabalhando com um fornecedor oficial de dispositivos Samsung.

- O administrador instala o aplicativo KNOX Deployment a partir do Google Play no seu dispositivo móvel e migra o perfil KNOX MDM para os dispositivos dos usuários por Bluetooth ou NFC (Near Field Communication). Após a implementação do perfil KNOX MDM, o dispositivo será adicionado automaticamente no console KME.

  Selecione este método se os dispositivos Samsung não foram comprados de um fornecedor oficial.

Adicionar um dispositivo pelo fornecedor

Um fornecedor oficial de dispositivos Samsung está registrado no Samsung KNOX. Para obter uma lista de fornecedores oficiais, visite o *site de suporte técnico da Samsung*. O fornecedor adiciona automaticamente os dispositivos no console KME da sua conta Samsung imediatamente após a compra dos dispositivos. Para que os dispositivos sejam adicionados pelo fornecedor, você deve registrar o fornecedor no console KME para a sua conta da Samsung. Você precisará de uma ID de revendedor para adicionar o fornecedor de dispositivos Samsung no console KME. Para receber a ID de revendedor, envie uma solicitação ao fornecedor. Na solicitação, especifique sua ID de cliente KNOX.

Para exibir sua ID de cliente KNOX:

1. Efetue o login no console Samsung KNOX → **KNOX Mobile Enrollment**.
2. Selecione a seção **Revendedores**.
3. Sua ID será exibida no campo **ID de cliente KNOX**.

Após receber uma resposta do fornecedor com a ID do revendedor, registre o fornecedor no console KME. Antes de registrar o fornecedor, você pode criar um perfil KNOX MDM para que ele possa ser automaticamente implementado ao adicionar novos dispositivos.

Para registrar um fornecedor oficial no console KME:

1. Efetue o login no console Samsung KNOX → **KNOX Mobile Enrollment**.
2. Selecione a seção **Revendedores**.
3. Clique no botão **Registrar o revendedor**.

   Uma janela para registrar o fornecedor do dispositivo será aberta.
4. No campo **ID do revendedor**, insira a ID recebida do fornecedor oficial de dispositivos Samsung.
5. Se você criou um perfil KNOX MDM, selecione o perfil KNOX MDM na janela de registro do fornecedor.

   Ao adicionar novos dispositivos, o perfil KNOX MDM será automaticamente instalado.

6. Na lista **Método preferido de confirmação de download**, selecione um método para confirmar a adição de um dispositivo para um fornecedor.

   - **Todos os downloads devem ser confirmados**. Quando um dispositivo for adicionado pelo fornecedor, você precisará confirmar a operação.

   - **Confirmar automaticamente todos os downloads deste revendedor**. Os dispositivos do fornecedor serão automaticamente adicionados no console KME.

7. Clique em **OK**.

O fornecedor de dispositivos Samsung será adicionado à lista de fornecedores no console KME.

Após a compra de novos dispositivos no fornecedor oficial, o aplicativo Kaspersky Endpoint Security for Android será automaticamente instalado nos dispositivos após os dispositivos estarem conectados na Internet. Para obter mais detalhes sobre como trabalhar com o KNOX Mobile Enrollment, consulte o *Guia do Usuário do KNOX Mobile Enrollment*. Se você já tiver uma lista de dispositivos no console KME, adicione o perfil KNOX MDM com o aplicativo KNOX MDM ao dispositivo.

Para entregar um perfil KNOX MDM aos dispositivos:

1. Efetue o login no console Samsung KNOX → **KNOX Mobile Enrollment**.

2. Selecione **Dispositivos** → **Todos os dispositivos**.

3. Selecione os dispositivos nos quais você quer instalar o perfil KNOX MDM.

4. Clique no botão **Configurar**.

   A janela **Informações do dispositivo** será aberta.

5. Na lista **Perfil MDM**, selecione o perfil KNOX MDM com o aplicativo Kaspersky Endpoint Security for Android.

6. No campo **Identificadores**, insira os identificadores para agrupar e legendar dispositivos, e para a otimização de pesquisa no console KME.

7. Insira as credenciais da conta do usuário do dispositivo nos campos **ID do usuário** e **Senha**.

   As credenciais da conta são necessárias para receber um certificado geral. A ID do usuário e a senha devem coincidir com as credenciais da conta do usuário no Kaspersky Security Center (Nome completo e Senha nas propriedades da conta do usuário).

8. Selecione o perfil KNOX MDM para os dispositivos restantes.

9. Clique no botão **Salvar**.

Após o dispositivo estar conectado na Internet, será solicitado ao usuário a instalação do perfil KNOX MDM.

Adicionar um dispositivo por meio do aplicativo KNOX Deployment

Se você não comprou o seu dispositivo Samsung de um fornecedor oficial, poderá adicionar o dispositivo ao KNOX Mobile Enrollment por Bluetooth ou NFC. Isto irá requerer o dispositivo móvel do administrador que será usado para entregar perfis KNOX MDM aos dispositivos móveis dos usuários.

Para adicionar dispositivos usando o aplicativo KNOX Deployment, as seguintes condições precisam ser atendidas:

- Dependendo do modo de entrega selecionado, os módulos Bluetooth ou NFC devem ser ativados nos dispositivos móveis.
- Os dispositivos móveis devem estar conectados à Internet.

Para entregar um perfil KNOX MDM usando o aplicativo KNOX Deployment:

1. Instale o aplicativo KNOX Deployment a partir do Google Play no dispositivo móvel do administrador.
2. Inicie o aplicativo KNOX Deployment.
3. Insira suas credenciais da conta da Samsung.
4. Na janela **KNOX Deployment**, defina as configurações para implementar um perfil KNOX MDM:
   - Selecione o perfil KNOX MDM.
   - Selecione o modo de implementação: **Bluetooth** ou **NFC**.

     Usando Bluetooth, você pode adicionar um perfil KNOX MDM em diversos dispositivos ao mesmo tempo.
5. Clique em **Iniciar a implementação**:
   - **Bluetooth**. No dispositivo móvel do usuário, abra o site https://configure.samsungknox.com.

     Isto inicia o Assistente de Registro de Dispositivo KNOX da Samsung. Siga as instruções na tela.

     Após o perfil KNOX MDM ter sido instalado, o novo dispositivo com o identificador **Bluetooth** será adicionado ao console KME.
   - **NFC**. Traga o dispositivo móvel do administrador para perto do dispositivo móvel do usuário e transfira o perfil KNOX MDM.

     No dispositivo móvel do usuário, haverá um prompt para instalar o perfil KNOX MDM. O novo dispositivo com o identificador **NFC** será adicionado no console KME.

Instalar o aplicativo

Antes de instalar o aplicativo Kaspersky Endpoint Security for Android, emita um certificado geral para os usuários de dispositivo móvel no Console de Administração do Kaspersky Security Center. Um certificado geral é necessário para identificar o usuário do dispositivo móvel no Console de Administração do Kaspersky Security Center.

Após o início da implementação do perfil KNOX MDM, o arquivo de instalação APK será automaticamente baixado no dispositivo móvel. A instalação do aplicativo Kaspersky Endpoint Security for Android é iniciada automaticamente. O usuário deve aceitar o Contrato de Licença do Samsung KNOX e o Contrato de Licença do Kaspersky Endpoint Security for Android. Nenhuma configuração adicional do aplicativo é necessária. Após o aplicativo estar instalado, a sincronização com o Kaspersky Security Center será automaticamente executada. O dispositivo móvel será adicionado ao Console de Administração do Kaspersky Security Center para o grupo de administração especificado nas configurações do perfil KNOX MDM (`groupName`).

Configuração de contêineres KNOX

Esta seção contém informações sobre o trabalho com contêineres KNOX em dispositivos da Samsung que executam o Android.

O uso de contêineres KNOX somente está disponível em dispositivos Samsung que executam a versão 6.0 ou posterior do Android.

Sobre contêineres KNOX

Um *contêiner KNOX* é um ambiente seguro no dispositivo de usuário que tem a sua própria área de trabalho, painel de inicialização, aplicativos e widgets. Um contêiner KNOX permite que você isole aplicativos corporativos e dados de aplicativos pessoais e dados. Um contêiner KNOX é um componente da solução móvel Samsung KNOX.

O *Samsung KNOX* é uma solução móvel para configurar e proteger dispositivos móveis da Samsung que executam o sistema operacional Android. Para obter mais detalhes sobre o Samsung KNOX, visite o *site de Suporte Técnico da Samsung*.

Os contêineres KNOX permitem separar dados pessoais e dados corporativos em um dispositivo móvel. Por exemplo, é impossível usar uma caixa de correio pessoal para enviar um arquivo que está localizado em um contêiner KNOX. Recomenda-se implementar um contêiner KNOX se os dispositivos móveis pessoais de funcionários forem usados para trabalhar com dados corporativos.

Para usar contêineres KNOX, você deve ativar o Samsung KNOX. Após sincronizar um dispositivo com o Kaspersky Security Center, será solicitado que o usuário do dispositivo instale o contêiner KNOX. Antes de instalar o contêiner KNOX, o usuário deve aceitar os termos do Contrato de Licença do Usuário Final da Samsung.

Após instalar o contêiner KNOX, o ícone KNOX será adicionado à área de trabalho do dispositivo móvel. Ou o espaço de trabalho será adicionado à lista de aplicativos no dispositivo móvel. Para trabalhar com dados corporativos, o usuário precisa iniciar o aplicativo do contêiner KNOX.

O Kaspersky Endpoint Security for Android não está instalado no contêiner KNOX e não protege os dados corporativos. O Kaspersky Endpoint Security for Android não detecta o download de arquivos maliciosos e bloqueia sites maliciosos no contêiner KNOX. Não é possível controlar a inicialização de aplicativos ou proibir o uso da câmera no contêiner KNOX. O Kaspersky Endpoint Security for Android protege apenas dados particulares. É possível proteger dados corporativos com as ferramentas do Samsung KNOX. Para obter mais detalhes sobre o Samsung KNOX, visite o *site de Suporte Técnico da Samsung*.

Ativar o Samsung KNOX

Para usar um contêiner KNOX no dispositivo móvel do usuário, você deve ativar o Samsung KNOX. O procedimento de ativação do Samsung KNOX depende da versão do Kaspersky Endpoint Security for Android instalada nos dispositivos dos usuários:

- Caso a versão atual do Kaspersky Endpoint Security for Android esteja instalada nos dispositivos, não é preciso de nenhuma chave para ativar o Samsung KNOX.

- Caso uma versão antiga do Kaspersky Endpoint Security for Android (10.8.3.174 ou anterior) esteja instalada nos dispositivos, será necessário obter uma chave do gerenciador de licença KNOX (doravante denominada chave KLM) da Samsung. Uma *chave do KNOX License Manager* é um código único que é usado pelo sistema de

licenciamento da Samsung KNOX. Para obter informações detalhadas sobre a chave KLM, consulte o site de Suporte Técnico para o KNOX da Samsung.

A utilização de contêineres KNOX é possível somente em dispositivos Samsung.

Para ativar o Samsung KNOX:

1. No árvore do console, na pasta **Dispositivos gerenciados**, selecione o grupo de administração ao qual os dispositivos Android pertencem.
2. Na área de trabalho do grupo, selecione a guia **Políticas**.
3. Clique duas vezes em qualquer coluna para abrir a janela de propriedades da política.
4. Na janela **Propriedades** da política, selecione a seção **Gerenciar o Samsung KNOX → Contêineres KNOX**.
5. No campo **chave do gerenciador de licença KNOX**, especifique o seguinte:
   - Caso a versão atual do Kaspersky Endpoint Security for Android esteja instalada nos dispositivos, digite qualquer caractere.
   - Caso uma versão antiga do Kaspersky Endpoint Security for Android (10.8.3.174 ou anterior) esteja instalada nos dispositivos, insira a chave KLM recebida da Samsung.
6. Definir o atributo Bloqueio na posição de bloqueado.
7. Clique no botão **Aplicar** para salvar as alterações efetuadas.

O Samsung KNOX será ativado após a próxima sincronização do dispositivo com o Kaspersky Security Center. O usuário será solicitado a aceitar os termos do Contrato de Licença do Usuário Final da Samsung e instalar o contêiner KNOX.

Para desativar o Samsung KNOX:

1. No árvore do console, na pasta **Dispositivos gerenciados**, selecione o grupo de administração ao qual os dispositivos Android pertencem.
2. Na área de trabalho do grupo, selecione a guia **Políticas**.
3. Clique duas vezes em qualquer coluna para abrir a janela de propriedades da política.
4. Na janela **Propriedades** da política, selecione a seção **Gerenciar o Samsung KNOX → Contêineres KNOX**.
5. Limpe o valor do campo **chave do gerenciador de licença KNOX**.
6. Clique no botão **Aplicar** para salvar as alterações efetuadas.

O Samsung KNOX será desativado após a próxima sincronização do dispositivo com o Kaspersky Security Center. O acesso ao contêiner KNOX será bloqueado.

Limitações do Samsung KNOX

- A utilização dos contêineres KNOX está disponível somente em dispositivos Samsung.

- Em dispositivos Samsung compatíveis com KNOX 2.6, 2.7 e 2.7.1, a Proteção na Web e o Controle de aplicativos não funcionam em um contêiner KNOX. Este problema é devido à falta de permissões necessárias no contêiner KNOX (Serviço de Acessibilidade). Nos dispositivos compatíveis com KNOX 2.8 e posterior, todos os componentes do aplicativo operam sem limitações.

- As versões do Kaspersky Endpoint Security for Android anteriores ao Service Pack 4 Maintenance Release 3 Atualização 2 podem funcionar de forma instável nos dispositivos Samsung Android 10 devido às atualizações do Samsung KNOX. Recomenda-se atualizar o Kaspersky Endpoint Security for Android para a versão Service Pack 4 Maintenance Release 3 Atualização 2.

Configurar o Firewall no KNOX

Você deve definir as configurações de Firewall para monitorar as conexões da rede em um contêiner KNOX.

Para configurar o Firewall em um contêiner KNOX:

1. No árvore do console, na pasta **Dispositivos gerenciados**, selecione o grupo de administração ao qual os dispositivos Android pertencem.

2. Na área de trabalho do grupo, selecione a guia **Políticas**.

3. Clique duas vezes em qualquer coluna para abrir a janela de propriedades da política.

4. Na janela **Propriedades** da política, selecione a seção **Gerenciar o Samsung KNOX → Contêineres KNOX**.

5. Na janela **Firewall**, clique em **Configurar**.

   A janela **Firewall** é aberta.

6. Selecione o modo do Firewall:

   - Para permitir todas as conexões de entrada e saída no dispositivo móvel, mova o seletor deslizante para **Permitir tudo**.

   - Para bloquear toda a atividade da rede exceto dos aplicativos na lista de exclusões, mova o controle deslizante para cima, para **Bloquear todos exceto exceções**.

7. Se você configurar o modo do Firewall para **Bloquear todos exceto exceções**, crie uma lista de exclusões:

   a. Clique em **Adicionar**.

      Isto abre a janela **Exclusão para o firewall**.

   b. No campo **Nome do aplicativo**, insira o nome de um aplicativo móvel.

   c. No campo **Nome do pacote**, insira o nome do sistema do pacote do aplicativo móvel (por exemplo, `com.mobileapp.example`).

   d. Clique em **OK**.

8. Clique no botão **Aplicar** para salvar as alterações efetuadas.

As configurações do dispositivo móvel são definidas depois da próxima sincronização do dispositivo com o Kaspersky Security Center.

Configurar uma caixa de correio do Exchange no KNOX

Para trabalhar com correio corporativo, contatos e o calendário em um contêiner KNOX, você deve definir as configurações da caixa de correio do Exchange.

Para configurar uma caixa de correio do Exchange em um contêiner KNOX:

1. No árvore do console, na pasta **Dispositivos gerenciados**, selecione o grupo de administração ao qual os dispositivos Android pertencem.
2. Na área de trabalho do grupo, selecione a guia **Políticas**.
3. Clique duas vezes em qualquer coluna para abrir a janela de propriedades da política.
4. Na janela **Propriedades** da política, selecione a seção **Gerenciar o Samsung KNOX → Contêineres KNOX**.
5. Na janela **Exchange ActiveSync**, clique no botão **Configurar**.

   A janela **Configurações do servidor Exchange de correio** é exibida.
6. No campo **Endereço do servidor**, insira o endereço IP ou nome DNS do servidor que hospeda o servidor de correio.
7. No campo **Domínio**, insira o nome do domínio do usuário do dispositivo móvel na rede corporativa.
8. Na lista suspensa **Intervalo de sincronização**, selecione o intervalo desejado de sincronização de dispositivos móveis com o servidor Microsoft Exchange.
9. Para usar o protocolo de transporte de dados SSL (Secure Sockets Layer), selecione a caixa de seleção **Usar a conexão SSL**.
10. Para usar certificados digitais para proteger a transferência de dados entre o dispositivo móvel e o servidor Microsoft Exchange, selecione a caixa de seleção **Verificar o certificado do servidor**.
11. Clique no botão **Aplicar** para salvar as alterações efetuadas.

As configurações do dispositivo móvel são definidas depois da próxima sincronização do dispositivo com o Kaspersky Security Center.

Apêndices

Esta seção fornece informações que complementam o texto do documento.

Permissões para configurar políticas de grupo

Os administradores do Kaspersky Security Center podem configurar os direitos de acesso de usuários do Console de Administração para diferentes funções, dependendo dos cargos dos usuários.

Para cada área funcional, o administrador pode atribuir as seguintes permissões:

- **Permitir editar**. O usuário do Console de Administração está autorizado a alterar as configurações da política na janela de propriedades.

- **Bloquear a edição**. O usuário do Console de Administração está proibido de alterar as configurações da política na janela de propriedades. As guias de política que pertencem ao escopo funcional para o qual esse direito foi atribuído não são exibidas na interface.

Permissões para acessar seções do plug-in de administração do Kaspersky Endpoint Security

Escopo funcional	Seção de políticas
Android Enterprise	Perfil de trabalho do Android
Antirroubo	Antirroubo
Controle de aplicativos	Controle de aplicativos
Proteção	Proteção, Verificação, Atualização
Controle de conformidade	Controle de conformidade
Contêineres	Contêineres
Configurações do dispositivo	Controle de dispositivos, Sincronização
Gerenciar dispositivos Samsung	APN, Gerenciando dispositivos da Samsung, contêineres KNOX
Gerenciamento do sistema	Avançado, Wi-Fi
Proteção na Web	Proteção na Web

Permissões de acessar seções do plug-in de administração do Kaspersky Device Management for iOS

Escopo funcional	Seção de políticas
Adicional	Clipes da Web, Fontes, AirPlay, AirPrint
Exchange ActiveSync	Geral, senha, sincronização, restrições de funcionalidades, restrições de aplicativos
Geral	Geral, Login único, Proteção na Web, Wi-Fi, nome do ponto de acesso (APN), Exchange ActiveSync, e-mail, cargas personalizadas
LDAP (calendário/contatos)	LDAP, Calendário, Contatos, Assinaturas do calendário
Limitações e segurança	Restrições de funções, Restrições para aplicativos, Restrições para conteúdo de mídia, Senha, VPN, Proxy HTTP Global, Certificados, SCEP

Categorias de aplicativos

O Controle de aplicativos suporta a categorização de aplicativos. O modo de operação configurado para a categoria do aplicativo é aplicado a todos os aplicativos nesta categoria. A categoria de cada aplicativo é determinada pelo serviço na nuvem do Kaspersky Security Network.

Categorias de aplicativos

Categoria	Descrição
Entretenimento	Aplicativos de entretenimento interativo.
Clientes de MI, aplicativos de	Aplicativos de mensagem momentânea, voz e comunicação de vídeo sobre IP.

mensagem móveis	
Redes sociais	Aplicativos para usar redes sociais e blogs.
Software administrativos	Aplicativos para o cálculo impostos, gerenciamento de operações bancárias, tratamento de planilhas, contabilidade e outros aplicativos orientados ao negócio. Editores de texto.
Residência, família, hobbies, saúde	Aplicativos com receitas, dicas de estilo. Aplicativos para se exercitar, mantendo uma programação de exercícios físicos, recebendo dicas sobre dieta, nutrição saudável, segurança e prevenção de acidente.
Médico	Os aplicativos que contêm catálogos de sintomas e medicações, aplicativos para profissionais de saúde, revistas de serviço de saúde e notícias.
Multimídia	Serviços de assinatura de filmes, reprodutores de mídia e reprodutores de vídeo. Serviços musicais, reprodutores, rádio transmissões.
Software de design gráfico	Aplicativos para uso com uma câmera, editores gráficos, aplicativos para gerenciar e publicar fotos.
Plug-ins para ler notícias e alimentações RSS	Aplicativos para ler jornais, revistas, blogs, e agregadores de notícias.
Clima	Aplicativos que exibem a previsão do tempo.
Aplicativos de educação	Leitores de livros, manuais, livros, dicionários, thesaurus, enciclopédias. Aplicativos que ajudam a estudar para exames, materiais de treinamento, dicionários, jogos desenvolventes, ferramentas de estudo de idioma.
Compras on-line	Aplicativos para fazer compras on-line e licitar em leilões, cupons de presente, ferramentas de comparação de preços, aplicativos de lista de compras, aplicativos para ler o comentário sobre produtos.
Utilitários de inicialização	Os aplicativos cujo objetivo é o de redesenhar a área de trabalho, widgets, atalhos.
Sistemas operacionais e utilitários	Aplicativos do sistema que fornecem o gerenciamento do sistema operacional, interação de usuário e gerenciamento da RAM.
Visualizadores de mapa	Guias de cidade, informações sobre negócios locais, ferramentas de planejamento de viagem.
Outros aplicativos	Bibliotecas de software, versões de demonstrações técnicas de aplicativos. Aplicativos não incluídos em nenhuma categoria.
Transporte	Aplicativos para usar o transporte público, ferramentas de navegação, aplicativos para condutores.
Jogos	Arcadas, apostas, corrida, outro, cassino, jogos de cartão, música, jogos de tabuleiro, tutoriais, quebra-cabeças, aventuras, RPG, simuladores, jogos de palavras, jogos de esportes, estratégias, ação.
Navegadores	Aplicativos para exibir sites, os conteúdos de documentos e arquivos da Web. Aplicativos para gerenciar aplicativos da Web.
Ferramentas de desenvolvimento	Aplicativos destinados para desenvolver softwares. Programas de depuração, compiladores, editores de código, editores da interface gráfico de usuário.
Aplicativos de SO	Aplicativos fornecidos junto com o sistema operacional e necessários para o funcionamento apropriado do sistema operacional.
Aplicativos de Internet	Gerenciadores de download, clientes de correio, aplicativos de pesquisa na web e outros aplicativos para a navegação tranquila na Internet.

Software de infraestrutura de rede	Aplicativos para gerenciar servidores, dispositivos de armazenamento de dados, equipamento de rede, software dentro de uma rede corporativa, automação e integração da infraestrutura completa.
Software de conexão em rede	Aplicativos para organizar a colaboração de um grupo de usuários em múltiplos dispositivos, e a comunicação entre dispositivos.
Utilitários do sistema	Aplicativos fornecidos em conjunto com o sistema operacional: gerenciadores de arquivos, ferramentas de arquivamento, utilitários para o diagnóstico de hardware e software, ferramentas de otimização da memória, programas de desinstalação, utilitários de gerenciamento do processador.
Software de segurança	Aplicativos de proteção dos dados de dispositivo. Aplicativos que detectam e neutralizam as ameaças no dispositivo. Firewalls. Aplicativos de criptografia de dados.
Gerenciadores de download	Aplicativos para baixar de arquivos de origens externas.
Aplicativos para armazenar arquivos na Internet	Aplicativos para gerenciar os armazenamentos on-line de arquivos, notas e multimídia.
Sistemas de referência	Leitores de livros, manuais, livros, dicionários, thesaurus, wiki-enciclopédias.
Aplicativos de e-mail	Aplicativos usados para enviar e receber mensagens de e-mail.

Uso do aplicativo Kaspersky Endpoint Security for Android

Esta seção de Ajuda descreve recursos e operações que estão disponíveis para usuários do aplicativo Kaspersky Endpoint Security for Android.

Os artigos nesta seção englobam todas as opções que podem estar disponíveis ou visíveis em um dispositivo móvel. O layout e o comportamento reais do aplicativo dependem de qual sistema de administração remota é implementado e como o administrador configura o seu dispositivo de acordo com os requisitos de segurança corporativa. Algumas funções e opções descritas nesta seção podem não se aplicar à sua experiência real com o aplicativo. Caso tenha alguma dúvida sobre o aplicativo em seu dispositivo específico, entre em contato com o administrador.

Recursos do aplicativo

O Kaspersky Endpoint Security oferece os seguintes recursos chave.

Proteção contra vírus e outro malware

O aplicativo usa o componente Antivírus para proteger o dispositivo contra vírus e outro malware.

O Antivírus executa as seguintes funções:

- Verifica todo o dispositivo, os aplicativos instalados ou as pastas selecionadas quanto à existência de ameaças
- Protege o dispositivo em tempo real
- Verifica os novos aplicativos instalados antes de eles serem inicializados pela primeira vez
- Atualiza bancos de dados antivírus

Se um aplicativo que coleta informações e as envia para ser processadas estiver instalado em um dispositivo móvel, o Kaspersky Endpoint Security for Android pode classificar este aplicativo como malware.

Controle de aplicativos

De acordo com os requisitos de segurança corporativa, *o administrador do sistema de administração remoto* (aqui referido como "administrador") cria listas de aplicativos recomendados, bloqueados e requeridos. O componente Controle de aplicativos é usado para instalar aplicativos recomendados e requeridos, atualizá-los e remover os aplicativos bloqueados.

O Controle de Aplicativos permite instalar aplicativos recomendados e requeridos no seu dispositivo por meio de um link direto para o pacote de distribuição ou um link ao Google Play. O Controle de Aplicativos permite remover os aplicativos bloqueados que violam os requisitos da segurança corporativa.

O Kaspersky Endpoint Security deve ser ativado como um serviço de recurso de acessibilidade para garantir o funcionamento apropriado do controle de aplicativo. Se você não ativou este serviço durante o Assistente de Configuração Inicial para o aplicativo, poderá ativar o Kaspersky Endpoint Security como um serviço Recursos de Acessibilidade na seção **Status** selecionando a notificação apropriada, ou nas configurações do dispositivo (**Configurações Android** → **Acessibilidade** → **Serviços**).

Proteção de dados perdidos ou roubados

O componente Antirroubo protege seus dados contra o acesso não autorizado e ajuda você a localizar o dispositivo caso ele seja roubado ou perdido.

O Antirroubo permite executar as seguintes operações remotamente:

- Bloquear o dispositivo.

  Para impedir que um criminoso tenha a capacidade de desbloquear o dispositivo, o Kaspersky Endpoint Security deve ser ativado como um serviço Recursos de Acessibilidade em dispositivos móveis que executam Android 7.0 ou posterior.

- Ative um alarme alto no dispositivo mesmo se o som do dispositivo estiver desativado.
- Adquira as coordenadas do mapa da localização do dispositivo.
- Limpe os dados armazenados no dispositivo.
- Redefinir para as configurações de fábrica.
- Tirar secretamente uma foto da pessoa que está usando o seu dispositivo.

Para ativar operações Antirroubo, o Kaspersky Endpoint Security deve ser ativado como um administrador de dispositivo. Se você não concedeu direitos de administrador do dispositivo durante a configuração inicial dos aplicativos, poderá conceder direitos de administrador ao Kaspersky Endpoint Security na seção **Status** selecionando a notificação apropriada, ou nas configurações de dispositivo (**Configurações Android** → **Segurança** → **Administradores de dispositivo**).

Proteção contra ameaças on-line

O componente Proteção na Web fornece proteção contra ameaças on-line.

A Proteção na Web bloqueia sites maliciosos que distribuem códigos maliciosos e sites de phishing criados para roubar seus dados confidenciais e obter acesso a suas contas financeiras. A Proteção na Web verifica os sites antes de abri-los utilizando o serviço na nuvem da Kaspersky Security Network.

Para ativar a Proteção na Web:

- O Kaspersky Endpoint Security deve ser ativado como um serviço Recursos de Acessibilidade.
- É necessário aceitar a Declaração relativa ao processamento de dados com o propósito de usar a Proteção na Web (Declaração da Proteção na Web). O Kaspersky Endpoint Security usa a Kaspersky Security Network (KSN) para verificar sites. A Declaração da Proteção na Web contém os termos de troca de dados com a KSN.

Seu administrador pode aceitar a Declaração da Proteção na Web para você no Kaspersky Security Center. Nesse caso, não é necessária nenhuma ação da sua parte.

Se o seu administrador não aceitou a Declaração de Proteção na Web e enviou a você a solicitação para fazer isso, você deve ler e aceitar a Declaração de Proteção na Web nas configurações do aplicativo.

Se seu administrador não aceitou a Declaração da Proteção na Web, a Proteção na Web não estará disponível.

- A Proteção na Web nos dispositivos Android funciona apenas nos navegadores Google Chrome (incluindo o recurso Guias personalizadas), Huawei Browser e Samsung Internet. A Proteção na Web para Samsung Internet Browser não bloqueia sites em um dispositivo móvel se um perfil de trabalho for usado e a Proteção na Web estiver ativada apenas para o perfil de trabalho.

Introdução à janela principal

A exibição da janela principal é ligeiramente diferente em diferentes resoluções de tela.

A aparência da tela principal modifica-se no caso de problemas que possam levar a uma redução do nível de proteção, infecção do dispositivo ou perda de informações.

A seção **Status** exibe as seguintes informações:

- Problemas na proteção do seu dispositivo
- Informações sobre se o seu dispositivo estar ou não em conformidade com os requisitos de segurança corporativa
- Informações sobre o status da proteção do seu dispositivo

Você pode abrir a seção **Status** tocando no topo da janela principal do Kaspersky Endpoint Security.

Problemas com a proteção do dispositivo

Os problemas de proteção são agrupados por categorias. Para cada problema são listadas ações que você pode usar para solucionar o problema.

A seção **Status** também exibe uma lista de objetos ignorados detectados pelo aplicativo. A lista de objetos ignorados pode modificar-se, por exemplo, se um arquivo malicioso foi excluído ou movido. Para receber uma lista atualizada de ameaças, execute uma verificação completa do dispositivo. Para assegurar a proteção confiável dos dados, elimine todos os objetos detectados.

Existem dois tipos de problemas de proteção:

- *Problemas de notificação*. Realçados a amarelo. Os problemas de notificação informam o usuário sobre eventos que afetam a segurança do dispositivo (por exemplo, o fato da última verificação ter sido realizada há mais de 14 dias ou de que um novo aplicativo instalado não foi verificado). Você também pode ocultar um problema de notificação. As informações sobre o problema podem posteriormente ser acessadas através do menu **Problemas ocultados**.
- *Críticos*. Realçados a vermelho. Problemas críticos notificam o usuário sobre eventos de importância crítica para a segurança do dispositivo (como o fato de que os bancos de dados antivírus não foram atualizados por

um longo tempo ou um aplicativo bloqueado foi instalado no dispositivo). Um problema crítico não pode ser ocultado.

Controle de conformidade

O aplicativo verifica automaticamente se o dispositivo está em conformidade com os requisitos de segurança corporativa. Informações sobre se o seu dispositivo atende ou não os requisitos de segurança corporativa são mostradas na seção **Status**.

- O motivo de o dispositivo não estar em conformidade com os requisitos da segurança corporativa (por exemplo, aplicativos bloqueados foram detectados no dispositivo).
- O período do tempo dentro do qual você deve eliminar a não conformidade (por exemplo, 24 horas).
- Ação que será executada no dispositivo se você não eliminar a não conformidade dentro do período de tempo especificado (por exemplo, o dispositivo será bloqueado).
- A ação executada para corrigir a não conformidade do dispositivo com os requisitos da segurança corporativa.

Ícone da barra de status

Após a conclusão do primeiro início do assistente, o ícone do Kaspersky Endpoint Security é exibido na barra de status.

O ícone reflete a operação do aplicativo e fornece acesso à janela principal do Kaspersky Endpoint Security.

O ícone indica a operação do Kaspersky Endpoint Security e reflete o status da proteção do seu dispositivo:

– o dispositivo está protegido.

– há problemas com a proteção (por exemplo, os bancos de dados antivírus estão desatualizados ou um aplicativo recém-instalado não foi verificado).

Verificação do dispositivo

O antivírus tem um número de limitações:

- Quando o Antivírus está sendo executado, uma ameaça detectada na memória externa do dispositivo (tal como um cartão SD) não pode ser neutralizada automaticamente no perfil para Trabalho (Aplicativos com o ícone de maleta, Configurar o perfil Android para o trabalho). O Kaspersky Endpoint Security for Android não tem acesso à memória externa no perfil para Trabalho. As informações sobre os objetos detectados são exibidas na seção **Status** do aplicativo. Para neutralizar objetos detectados na memória externa, os arquivos do objeto têm de ser excluídos manualmente e a verificação do dispositivo reiniciada.
- Devido às limitações técnicas, o Kaspersky Endpoint Security for Android não pode verificar arquivos com um tamanho de 2 GB ou mais. Durante uma verificação, o aplicativo ignora tais arquivos sem notificá-lo que tais arquivos foram ignorados.

Para iniciar uma verificação do dispositivo:

1. Toque em **Verificar** no painel de início rápido na janela principal do Kaspersky Endpoint Security.
2. Selecione o escopo de verificação do dispositivo:

- **Verificar todo o dispositivo**. O aplicativo verifica todo o sistema de arquivos do dispositivo.
- **Verificar os aplicativos instalados**. O aplicativo verifica somente os aplicativos instalados.
- **Verificação personalizada**. O aplicativo verifica a pasta ou arquivo individual selecionada. Você pode selecionar um objeto individual (pasta ou arquivo) ou uma das seguintes partições da memória do dispositivo:
  - **Memória do dispositivo**. Memória acessível para leitura de todo o dispositivo. Isto também inclui a partição de memória do sistema que armazena os arquivos do sistema operacional.
  - **Memória interna**. Partição de memória do dispositivo destinada à instalação de aplicativos e armazenamento de conteúdo de mídia, documentos e outros arquivos.
  - **Memória externa**. Memória do cartão SD externo. Se nenhum cartão SD externo estiver instalado, esta opção é oculta.

O acesso às configurações da verificação de vírus pode ser restringido pelo administrador.

Para configurar a verificação de vírus:

1. No painel de início rápido na janela principal do Kaspersky Endpoint Security, toque em ☰ → **Configurações** → **Antivírus** → **Verificar**.
2. Caso deseje que o aplicativo detecte adwares e aplicativos que possam ser usados por hackers para causar danos ao dispositivo ou aos dados quando o aplicativo realizar uma verificação, ative o botão **Adware, discadores e outros**.
3. Clique em **Ação na detecção de ameaças** e selecione a ação a ser tomada pelo aplicativo por padrão:
   - **Quarentena**

     A quarentena armazena os arquivos comprimidos como arquivos comprimidos, para que não danifiquem o dispositivo. Esse Quarentena permite excluir ou restaurar os arquivos que foram movidos para isolado dedicado.
   - **Solicitar ação**

     O aplicativo solicita que você selecione uma ação para cada objeto detectado: ignorar, colocar em quarentena ou excluir. Quando múltiplos objetos são detectados, você pode aplicar uma ação selecionada a todos os objetos.
   - **Excluir**

     Os objetos detectados serão automaticamente excluídos. Não é necessária nenhuma ação adicional. Antes de excluir um objeto, o Kaspersky Endpoint Security exibirá uma notificação temporária sobre a detecção do objeto.
   - **Ignorar**

     Se os objetos detectados foram ignorados, o Kaspersky Endpoint Security avisa você sobre os problemas na proteção do dispositivo. As informações sobre os objetos ignorados são exibidas na seção **Status** do aplicativo. Para cada ameaça ignorada, o aplicativo fornece ações que você pode executar para eliminar a ameaça. A lista de objetos ignorados pode modificar-se, por exemplo, se um arquivo malicioso foi excluído ou movido. Para receber uma lista atualizada de ameaças, execute uma verificação completa do dispositivo. Para assegurar a proteção confiável dos dados, elimine todos os objetos detectados.

As informações sobre as ameaças detectadas e as ações executadas são registradas nos relatórios do aplicativo (→ **Relatórios**). Você pode optar por exibir relatórios sobre as operações do Antivírus.

Executar uma Verificação agendada

O antivírus tem um número de limitações:

- Quando o Antivírus está sendo executado, uma ameaça detectada na memória externa do dispositivo (tal como um cartão SD) não pode ser neutralizada automaticamente no perfil para Trabalho (Aplicativos com o ícone de maleta, Configurar o perfil Android para o trabalho). O Kaspersky Endpoint Security for Android não tem acesso à memória externa no perfil para Trabalho. As informações sobre os objetos detectados são exibidas na seção **Status** do aplicativo. Para neutralizar objetos detectados na memória externa, os arquivos do objeto têm de ser excluídos manualmente e a verificação do dispositivo reiniciada.

- Devido às limitações técnicas, o Kaspersky Endpoint Security for Android não pode verificar arquivos com um tamanho de 2 GB ou mais. Durante uma verificação, o aplicativo ignora tais arquivos sem notificá-lo que tais arquivos foram ignorados.

Para configurar a programação de Verificação Completa de um dispositivo:

1. No painel de início rápido na janela principal do Kaspersky Endpoint Security, toque em → **Configurações** → **Antivírus** → **Verificar**.
2. Clique em **Agendamento** e selecione a frequência da verificação completa:
   - **Semanalmente**
   - **Diariamente**
   - **Desativado**
   - **Após a atualização do banco de dados**
3. Clique em **Dia de início** e selecione o dia da semana no qual deseja iniciar a verificação completa.
4. Clique em **Hora de início** e especifique a hora para iniciar a verificação completa.

Uma verificação completa do dispositivo é iniciada de acordo com o agendamento.

No Android 12 ou posterior, o aplicativo pode realizar essa tarefa após o especificado se o dispositivo estiver no modo de economia de bateria.

Alteração do modo de Proteção do dispositivo

A Proteção em tempo real permite detectar ameaças nos arquivos abertos e verificar aplicativos enquanto eles estão sendo instalados no dispositivo em tempo real. Os bancos de dados antivírus e o serviço na nuvem do Kaspersky Security Network (Proteção na Nuvem) são usados para garantir a segurança automaticamente.

Para alterar o modo de proteção do dispositivo:

1. No painel de início rápido na janela principal do Kaspersky Endpoint Security, toque em → **Configurações** → **Antivírus** → **Modo de proteção em tempo real**.

2. Selecione o modo de Proteção do dispositivo:

   - **Desativado**. A Proteção está desativada.

   - **Recomendado**. O antivírus verifica somente os aplicativos instalados a pasta Downloads. O antivírus verifica os novos aplicativos logo depois de serem instalados.

   - **Expandido**. O antivírus verifica objetos maliciosos em todos os arquivos do dispositivo quando qualquer operação é realiza neles (por exemplo, quando são salvos, movidos ou modificados). O antivírus também verifica os novos aplicativos assim que são instalados.

Informações sobre o modo de Proteção atual são exibidas na sob a descrição do componente.

O acesso às configurações da Proteção em tempo real pode ser restringido pelo administrador.

Para ativar a Proteção na Nuvem (KSN):

1. Toque em → **Configurações** → **Antivírus** no painel de início rápido na janela principal do Kaspersky Endpoint Security.

2. Ative o botão **Proteção na Nuvem (KSN)**.

   O botão **Proteção na Nuvem (KSN)** gerencia o uso do Kaspersky Security Network apenas para a proteção em tempo real de um dispositivo. Se a caixa de seleção estiver desmarcada, o Kaspersky Endpoint Security continuará a usar a KSN para a operação de outros componentes do aplicativo.

Como resultado, o aplicativo obtém acesso à base de conhecimento on-line da Kaspersky quanto à reputação de arquivos e aplicativos. A verificação é executada para as ameaças cujas informações ainda não foram adicionadas ao banco de dados antivírus, mas já estão disponíveis na KSN. O serviço na nuvem da Kaspersky Security Network fornece a operação completa do Antivírus e reduz a probabilidade de falsos alarmes. Apenas o administrador pode desativar totalmente o uso da Kaspersky Security Network.

Para configurar a Proteção em tempo real:

1. No painel de início rápido na janela principal do Kaspersky Endpoint Security, toque em → **Configurações** → **Antivírus** → **Modo de proteção em tempo real**.

2. Caso deseje que o aplicativo detecte adwares e aplicativos que possam ser usados por hackers para causar danos ao dispositivo ou aos dados quando o aplicativo realizar uma verificação, ative o botão **Adware, discadores e outros**.

3. Clique em **Ação na detecção de ameaças** e selecione a ação a ser tomada pelo aplicativo por padrão:

   - **Quarentena**

     A quarentena armazena os arquivos comprimidos como arquivos comprimidos, para que não danifiquem o dispositivo. A quarentena permite excluir ou restaurar os arquivos que foram movidos para o armazenamento isolado.

   - **Excluir**

Os objetos detectados serão automaticamente excluídos. Não é necessária nenhuma ação adicional. Antes de excluir um objeto, o Kaspersky Endpoint Security exibirá uma notificação temporária sobre a detecção do objeto.

- **Ignorar**

  Se os objetos detectados foram ignorados, o Kaspersky Endpoint Security avisa você sobre os problemas na proteção do dispositivo. As informações sobre os objetos ignorados são exibidas na seção **Status** do aplicativo. Para cada ameaça ignorada, o aplicativo fornece ações que você pode executar para eliminar a ameaça. A lista de objetos ignorados pode modificar-se, por exemplo, se um arquivo malicioso foi excluído ou movido. Para receber uma lista atualizada de ameaças, execute uma verificação completa do dispositivo. Para assegurar a proteção confiável dos dados, elimine todos os objetos detectados.

As informações sobre as ameaças detectadas e as ações executadas são registradas nos relatórios do aplicativo (→ **Configurações** → **Relatórios**). Você pode optar por exibir relatórios sobre as operações do Antivírus.

Atualizações do banco de dados de antivírus

Para atualizar os bancos de dados antivírus do aplicativo:

Toque em **Atualização do banco de dados** no painel de início rápido na janela principal do Kaspersky Endpoint Security.

Atualização do banco de dados agendada

O aplicativo pode atualizar automaticamente os bancos de dados antivírus de acordo com o agendamento especificado.

Para configurar o agendamento de atualização:

1. No painel de início rápido na janela principal do Kaspersky Endpoint Security, toque em → **Configurações** → **Antivírus** → **Atualização do banco de dados**.
2. Clique em **Agendamento** e selecione a frequência de atualização:
   - **Semanalmente**
   - **Diariamente**
   - **Desativado**
3. Clique em **Dia de início** e selecione o dia da semana no qual deseja executar a atualização.
4. Clique em **Hora de início** e selecione a hora para iniciar a atualização.

As atualizações de banco de dados de antivírus são iniciadas de acordo com o agendamento.

No Android 12 ou posterior, o aplicativo pode realizar essa tarefa após o especificado se o dispositivo estiver no modo de economia de bateria.

O que fazer em caso de perda ou roubo do dispositivo

Caso o dispositivo seja perdido ou roubado, entre em contato com o administrador do sistema. O administrador pode executar remotamente os comandos de Antirroubo em seu dispositivo de acordo com os requisitos da política de segurança corporativa.

Se um comando de reset completo for enviado ao dispositivo, o controle sobre o dispositivo será perdido, e os comandos antirroubo restantes não funcionarão.

Proteção na Web

Para ativar a Proteção na Web:

- O Kaspersky Endpoint Security deve ser ativado como um serviço Recursos de Acessibilidade.
- É necessário aceitar a Declaração relativa ao processamento de dados com o propósito de usar a Proteção na Web (Declaração da Proteção na Web). O Kaspersky Endpoint Security usa a Kaspersky Security Network (KSN) para verificar sites. A Declaração da Proteção na Web contém os termos de troca de dados com a KSN.

  Seu administrador pode aceitar a Declaração da Proteção na Web para você no Kaspersky Security Center. Nesse caso, não é necessária nenhuma ação da sua parte.

  Se o seu administrador não aceitou a Declaração de Proteção na Web e enviou a você a solicitação para fazer isso, você deve ler e aceitar a Declaração de Proteção na Web nas configurações do aplicativo.

  Se seu administrador não aceitou a Declaração da Proteção na Web, a Proteção na Web não estará disponível.

· A Proteção na Web nos dispositivos Android funciona apenas nos navegadores Google Chrome (incluindo o recurso Guias personalizadas), Huawei Browser e Samsung Internet. A Proteção na Web para Samsung Internet Browser não bloqueia sites em um dispositivo móvel se um perfil de trabalho for usado e a Proteção na Web estiver ativada apenas para o perfil de trabalho.

Para usar a Proteção na Web a todo momento enquanto você navega na Web, defina o Google Chrome ou o navegador Samsung Internet como o navegador padrão.

Para definir um navegador suportado como o navegador padrão e usar a Proteção na Web para verificar os sites a todo momento:

1. Toque em ☰ → **Configurações** → **Proteção na Web** no painel de início rápido da janela principal do Kaspersky Endpoint Security.
2. Mude o botão **Proteção na web** para a posição ativado.
3. Toque em **Definir navegador padrão**.

   Este botão é exibido quando a Proteção na Web está ativado e um navegador compatível não foi definido como o navegador padrão.

   O assistente de seleção do navegador padrão é iniciado.
4. Siga as instruções do assistente.

O assistente define o Google Chrome, o navegador Huawei ou o navegador Samsung Internet como navegador padrão. A Proteção na Web verifica os sites constantemente quando você navega na Web.

Controle de aplicativos

O *Controle de Aplicativos* verifica que se os aplicativos instalados em um dispositivo móvel estejam em conformidade com os requisitos da segurança corporativa. No Kaspersky Security Center, o administrador cria listas de aplicativos permitidos, bloqueados, obrigatórios e recomendados segundo os requisitos da segurança corporativa. Como resultado do Controle de aplicativos, o Kaspersky Endpoint Security solicita que você instale aplicativos obrigatórios e recomendados e que remova os aplicativos bloqueados. É impossível iniciar aplicativos bloqueados no seu dispositivo móvel.

Para instalar aplicativos obrigatórios e recomendados ou para remover aplicativos bloqueados:

1. Siga para a seção **Status** do Kaspersky Endpoint Security.
2. Selecione as tarefas de Controle de Aplicativos.
3. Execute as ações recomendadas.

Obter certificado

Para obter um certificado para acessar os recursos da rede corporativa:

1. Toque em → **Configurações** → **Adicionais** → **Obter o certificado** no painel de início rápido na janela principal do Kaspersky Endpoint Security.
2. Especifique as credenciais de sua conta da rede corporativa.
3. Se você recebeu uma senha temporária do administrador, selecione a caixa de seleção **Senha temporária** e digite a senha recebida.

   O Assistente de Instalação do Certificado é iniciado.
4. Siga as instruções do assistente.

Sincronizando com o Kaspersky Security Center

A sincronização do dispositivo móvel com o sistema de administração remota do Kaspersky Security Center é necessária para proteger e configurar seu dispositivo de acordo com os requisitos de segurança corporativa. O dispositivo é automaticamente sincronizado com o Kaspersky Security Center, e você também pode iniciar a sincronização manualmente. Depois da primeira sincronização, o seu dispositivo é adicionado à lista de dispositivos móveis gerenciados através do Kaspersky Security Center. O administrador então pode configurar o seu dispositivo de acordo com os requisitos de segurança corporativa.

Você pode definir as configurações de sincronização ao executar o assistente de configuração inicial ou nas configurações do Kaspersky Endpoint Security. As configurações de sincronização devem ser configuradas se você tiver instalado o Kaspersky Endpoint Security usando o Google Play. Solicite ao seu administrador do sistema os valores das configurações de sincronização.

Modifique as configurações de sincronização do dispositivo com o sistema de administração remota do Kaspersky Security Center somente quando for instruído a fazê-lo pelo administrador.

Para sincronizar seu dispositivo com o Kaspersky Security Center:

1. Toque em ☰ → **Configurações** → **Sincronização** no painel de início rápido na janela principal do Kaspersky Endpoint Security.
2. Na seção **Configurações de sincronização**, especifique os valores das seguintes configurações:
   - **Servidor**
   - **Porta**
   - **Grupo**
   - **Endereço de e-mail corporativo**

   As configurações de sincronização podem ser ocultas pelo administrador.
3. Toque em **Sincronizar**.

Ativar o aplicativo Kaspersky Endpoint Security for Android sem o Kaspersky Security Center

Na maioria dos casos, o aplicativo Kaspersky Endpoint Security for Android instalado em seu dispositivo é ativado pelo administrador centralmente no sistema de administração remota do Kaspersky Security Center. Caso o dispositivo não esteja conectado ao Kaspersky Security Center, é possível inserir o código de ativação manualmente. Para obter o código de ativação, entre em contato com o administrador.

Ative o aplicativo manualmente apenas quando instruído a fazê-lo pelo administrador.

Para inserir o código de ativação:

1. Na mensagem de erro que informa que sua licença expirará em breve ou expirou e que seu dispositivo não está conectado ao Servidor de Administração, toque em **Ativar**.
2. Na janela de ativação, digite o código de ativação fornecido pelo administrador e toque em **Ativar**.
3. Caso o código de ativação esteja correto, uma notificação será exibida, informando que o aplicativo foi ativado juntamente com a data de expiração da licença.

O aplicativo Kaspersky Endpoint Security for Android em seu dispositivo está ativado.

Atualizar o aplicativo

O Kaspersky Endpoint Security pode ser atualizado nas seguintes formas:

- Manualmente, usando o Google Play. Você pode efetuar o download da nova versão do aplicativos através do Google Play e a instalar em seu dispositivo.
- Com a ajuda do administrador. O administrador pode atualizar remotamente a versão do aplicativo em seu dispositivo usando o sistema de administração remota do Kaspersky Security Center.

Atualizar o aplicativo através do Google Play

O administrador poderá bloqueá-lo de atualizar o aplicativo a partir do Google Play.

O aplicativo pode ser atualizado a partir do Google Play seguindo o procedimento de atualização padrão para a plataforma Android. As seguintes condições devem ser atendidas para que o aplicativo seja atualizado:

- Você deve ter uma conta do Google.
- O dispositivo deve estar vinculado com a conta do Google.
- O dispositivo deve estar conectado à Internet.

Para saber mais sobre como criar uma conta do Google, vincular seu dispositivo com sua conta ou trabalhar com a Google Play Store, consulte o site de suporte da Google.

Atualizar o aplicativo através do Kaspersky Security Center

A atualização do aplicativo usando o Kaspersky Security Center consiste nas seguintes etapas:

1. O administrador envia ao seu dispositivo móvel o pacote de distribuição do aplicativo cuja versão atende os requisitos da segurança corporativa.

   Uma solicitação para instalar o Kaspersky Endpoint Security em seu dispositivo é exibida.

2. Aceite os termos e condições da atualização.

   A nova versão do aplicativo será instalada no seu dispositivo. O aplicativo não necessita de nenhuma configuração adicional após a atualização.

Remover o aplicativo

O administrador poderá bloqueá-lo de remover o aplicativo por si só. Se este for o caso, você não poderá remover o Kaspersky Endpoint Security.

O Kaspersky Endpoint Security poderá removido com os seguintes métodos:

- Manualmente nas configurações do aplicativo.
- Manualmente nas configurações do dispositivo.

- Com a ajuda do administrador. O administrador pode remover remotamente o aplicativo do seu dispositivo usando o sistema de administração remota do Kaspersky Security Center.

Remoção nas configurações do aplicativo

Para remover o Kaspersky Endpoint Security do seu dispositivo:

1. No painel de início rápido da janela principal do Kaspersky Endpoint Security, toque em → **Desinstalar o aplicativo**.

   Isto inicia o assistente Remoção do aplicativo.

2. Siga as instruções do assistente.

Remoção nas configurações do dispositivo

O aplicativo poderá ser removido ao seguir o procedimento padrão para a plataforma Android. Para remover o aplicativo, os direitos de administrador para o Kaspersky Endpoint Security devem ser desativados nas configurações de segurança do dispositivo.

Em dispositivos que executam o Android 7.0 ou posterior, se o administrador tiver bloqueado a remoção, o dispositivo será bloqueado se for feita uma tentativa de remover o aplicativo nas configurações Android. Para desbloquear o dispositivo, contate com o seu administrador.

Remoção através do Kaspersky Security Center

A remoção do aplicativo usando o Kaspersky Security Center consiste nas seguintes etapas:

1. O administrador envia o comando de remoção do aplicativo ao seu dispositivo móvel.

   O seu dispositivo móvel exibe um prompt para confirmar a remoção do Kaspersky Endpoint Security.

2. Confirme a remoção do aplicativo.

   O aplicativo será removido do seu dispositivo.

Aplicativos com o ícone de maleta

Ícone Aplicativo no perfil de trabalho do Android

Os aplicativos marcados com um ícone de maleta (aplicativos corporativos) são armazenados em seu dispositivo no perfil de trabalho do Android (aqui também "perfil do trabalho"). *O perfil do Android para o trabalho* é um ambiente seguro em seu dispositivo, no qual o administrador pode gerenciar aplicativos e contas sem restringir sua capacidade de trabalhar com dados pessoais.

O perfil do trabalho lhe permite armazenar os dados corporativos separadamente dos dados pessoais. Isso mantém os dados corporativos confidenciais e os protege contra malwares. Quando um perfil de trabalho for criado em seu dispositivos, o seguintes aplicativos corporativos são automaticamente instalados no perfil de trabalho: Google Play Market, Google Chrome, Downloads, Kaspersky Endpoint Security for Android e outros.

Aplicativo KNOX

Ícone do KNOX

O aplicativo KNOX abre um contêiner KNOX no seu dispositivo. Um *contêiner KNOX* é um ambiente seguro no seu dispositivo que tem a sua própria área de trabalho, painel de inicialização, aplicativos e widgets. O administrador pode gerenciar aplicativos e contas em um contêiner KNOX sem restringir as suas capacidades de trabalhar com dados pessoais.

O contêiner KNOX lhe permite armazenar os dados corporativos separadamente dos dados pessoais. Isso mantém os dados corporativos confidenciais e os protege contra malwares.

Em um contêiner KNOX, você pode acessar a sua caixa de correio da empresa, as informações de contato de funcionários da empresa, armazenamento de arquivo e outros aplicativos.

Para obter mais detalhes sobre como trabalhar com o KNOX, visite o *site de Suporte Técnico da Samsung*.

Uso do aplicativo Kaspersky Security for iOS

Esta seção de Ajuda descreve recursos e operações que estão disponíveis para usuários do aplicativo Kaspersky Security for iOS.

Os artigos nesta seção englobam todas as opções que podem estar disponíveis ou visíveis em um dispositivo móvel. O layout e o comportamento reais do aplicativo dependem de qual sistema de administração remota é implementado e como o administrador configura o seu dispositivo de acordo com os requisitos de segurança corporativa. Algumas funções e opções descritas nesta seção podem não se aplicar à sua experiência real com o aplicativo. Caso tenha alguma dúvida sobre o aplicativo em seu dispositivo específico, entre em contato com o administrador.

Recursos do aplicativo

O Kaspersky Security for iOS oferece os recursos chave a seguir.

Proteção contra ameaças on-line

O componente Proteção na Web fornece proteção contra ameaças on-line.

A Proteção na Web bloqueia sites maliciosos que distribuem códigos maliciosos e sites de phishing criados para roubar seus dados confidenciais e obter acesso a suas contas financeiras. A Proteção na Web verifica os sites antes de abri-los utilizando o serviço na nuvem da Kaspersky Security Network. A Proteção na Web também verifica a atividade online dos aplicativos no seu dispositivo.

Para que a Proteção na Web funcione, é necessário permitir que o aplicativo adicione uma configuração de VPN.

Detecção de jailbreak

Quando o Kaspersky Security for iOS detecta um jailbreak, ele exibe uma mensagem crítica e informa o administrador sobre o problema.

O aplicativo não pode garantir a segurança do dispositivo porque o jailbreak contorna os recursos de segurança e pode causar muitos problemas, incluindo:

- Vulnerabilidades de segurança
- Problemas de estabilidade
- Interrupção de serviços da Apple
- Possíveis falhas e travamentos
- Encurtamento da vida da bateria
- Incapacidade de aplicar atualizações do iOS

Instalar o aplicativo

Para instalar o aplicativo do Kaspersky Security for iOS:

1. Encontre a mensagem de e-mail com o convite do administrador para instalar o Kaspersky Security for iOS na App Store.
2. Acesse a App Store em uma das seguintes formas:
   - Toque no link na mensagem se estiver lendo-a no dispositivo iOS no qual deseja instalar o aplicativo.
   - Digitalize o código QR usando o dispositivo iOS no qual deseja instalar o aplicativo, se estiver lendo a mensagem em um computador.

   O link do convite é válido por 24 horas. Se não for possível instalar o aplicativo dentro do prazo, entre em contato com o administrador para obter um novo convite.
3. Baixe e instale o aplicativo por meio da App Store seguindo o procedimento de instalação padrão na plataforma do iOS.

O aplicativo Kaspersky Security for iOS está instalado no seu dispositivo. Para proteger o dispositivo, ative o aplicativo.

Ativar o aplicativo

Para ativar o aplicativo do Kaspersky Security for iOS:

1. Inicie o aplicativo no dispositivo.
2. Aceite os contratos e declarações marcando as caixas de seleção **Contrato de Licença do Usuário Final** e **Política de Privacidade de Produtos e Serviços**.

   É possível também aceitar a **Declaração da Kaspersky Security Network** para permitir o envio de estatísticas para a Kaspersky Security Network. Isso melhora o desempenho do aplicativo e garante sua operação ininterrupta.
3. Toque em **Avançar**. O aplicativo se conecta ao sistema de administração remota do Kaspersky Security Center e obtém a informação de licença.
4. Permita que o aplicativo adicione uma configuração de VPN. O aplicativo usa a configuração da VPN para verificar sites em busca de phishing e proteger o dispositivo contra malware.
5. Permita que o aplicativo envie notificações push. O aplicativo usa as notificações push para informar você sobre problemas de segurança e o status da licença.

O aplicativo Kaspersky Security for iOS em seu dispositivo está ativado.

Ativar o aplicativo com um código de ativação

Ao instalar o Kaspersky Security for iOS app no dispositivo, o aplicativo se conecta ao sistema de administração remota do Kaspersky Security Center e obtém a informação de licença automaticamente. Caso o dispositivo não esteja conectado ao Kaspersky Security Center, é possível inserir o código de ativação manualmente. Para obter o código de ativação, entre em contato com o administrador.

Ative o aplicativo manualmente apenas quando instruído a fazê-lo pelo administrador.

Para inserir o código de ativação:

1. Na mensagem que informa que o aplicativo não está ativado, toque em **Ativar o aplicativo**.
2. Na janela de ativação, digite o código de ativação fornecido pelo administrador e toque em **Ativar**.

   Caso o código de ativação esteja correto, uma notificação será exibida, informando que o aplicativo foi ativado juntamente com a data de expiração da licença.

O aplicativo Kaspersky Security for iOS em seu dispositivo está ativado.

Introdução à janela principal

A exibição da janela principal é ligeiramente diferente em diferentes resoluções de tela.

A janela principal exibe:

- Status da proteção geral do dispositivo.
- Mensagens que indicam o status dos componentes do aplicativo e os problemas de proteção.

Há três tipos de mensagens:

- Realçadas em verde. Mensagens de status que informam que a proteção está ativa na área especificada.
- Realçados a amarelo. Mensagens de informações que informam sobre eventos que podem afetar a segurança do dispositivo.
- Realçados a vermelho. Mensagens críticas que informam sobre eventos de importância crítica para a segurança do dispositivo.

Toque na mensagem para obter mais detalhes.

Atualizar o aplicativo

É possível baixar o a última versão do aplicativo do Kaspersky Security for iOS na App Store e instalá-lo no dispositivo seguindo o procedimento de atualização padrão na plataforma iOS. Também é possível ativar as atualizações automáticas. O aplicativo não necessita de nenhuma configuração adicional após a atualização.

As seguintes condições devem ser atendidas para que o aplicativo seja atualizado:

- É necessário ter um ID Apple.
- O dispositivo deve estar vinculado com seu ID Apple.

- O dispositivo deve estar conectado à Internet.

Para saber mais sobre como criar um ID Apple, vincular seu dispositivo ao ID Apple ou trabalhar com a App Store, consulte o site de suporte da Apple.

Remover o aplicativo

Para remover o aplicativo Kaspersky Security for iOS, siga o procedimento padrão na plataforma iOS:

1. Na tela Inicial, toque e segure o ícone do aplicativo.
2. Remova o aplicativo.

O aplicativo Kaspersky Security for iOS foi removido do seu dispositivo.

Licenciamento do aplicativo

Esta seção fornece informações sobre os termos gerais relativos ao licenciamento do Kaspersky Security for Mobile.

Sobre o Contrato de Licença do Usuário Final

O *Contrato de Licença do Usuário Final* (EULA) é um acordo vinculativo entre você e a AO Kaspersky Lab, que determina os Termos e Condições sob os quais você poderá usar o Kaspersky Security for Mobile.

Recomendamos a leitura cuidadosa dos Termos e Condições do EULA antes de usar o Kaspersky Security for Mobile.

É possível visualizar os Termos e Condições do EULA das seguintes maneiras:

- Durante a instalação de componentes do Kaspersky Security for Mobile.
- Ao ler o arquivo license.txt incluído no arquivo comprimido de extração automática do kit de distribuição para instalar o aplicativo Kaspersky Endpoint Security for Android.
- Na seção **Sobre o aplicativo** no Kaspersky Endpoint Security for Android.
- Na seção **Sobre o aplicativo** → **Contratos e declarações** no Kaspersky Security for iOS.
- Na seção **Avançado** → **Contratos de Licença aceitos** nas propriedades do Servidor de Administração. Esse recurso está disponível no Kaspersky Security Center versão 12.1 e posterior.

Ao confirmar que concorda com o Contrato de Licença do Usuário Final (EULA) durante a instalação dos componentes do Kaspersky Security for Mobile, você indica seu aceite dos Termos e Condições do Contrato de Licença do Usuário Final. Caso não aceite os termos do Contrato de Licença do Usuário Final, você deverá cancelar a instalação dos componentes do Kaspersky Security for Mobile e abster-se de utilizá-los.

Sobre a licença

A licença é um direito com tempo limitado de uso da solução integrada Kaspersky Security for Mobile, que é fornecida sob os termos do Contrato de Licença do Usuário Final.

A Licença atual lhe dá o direito para os seguintes tipos de serviços:

- Use os aplicativos em dispositivos móveis de acordo com os termos do Contrato de Licença do Usuário Final.
- Receber Suporte técnico.

O escopo dos serviços disponíveis e os termos de uso do aplicativo dependem do tipo de Licença sob o qual o aplicativo foi ativado.

Os seguintes tipos de Licença estão disponíveis:

- *Licença de avaliação*.

  Uma licença gratuita para avaliar o Kaspersky Security for Mobile.

A licença de avaliação é válida por 30 dias. Quando a licença de avaliação expira, o aplicativo móvel Kaspersky Endpoint Security for Android e o aplicativo móvel Kaspersky Security for iOS param de executar a maioria das funções, exceto a sincronização com o Servidor de Administração. Para continuar usando o aplicativo, você precisa comprar a licença comercial.

- *Comercial*.

  Uma licença fornecida quando você compra o Kaspersky Security for Mobile.

  Quando a licença comercial expirar, o aplicativo móvel continua funcionando, mas com a funcionalidade limitada.

  No modo de funcionalidade limitada, os seguintes componentes estão disponíveis dependendo do aplicativo.

  - Aplicativo Kaspersky Endpoint Security for Android:

    - **Antivírus**. A proteção em tempo real e a verificação de vírus do dispositivo estão disponíveis, mas as atualizações do banco de dados antivírus não estão.
    - **Antirroubo**. Apenas o envio de comandos para o dispositivo móvel está disponível.
    - **Sincronização com o Servidor de Administração**.

    O Kaspersky Endpoint Security for Android deixará de trocar informações com a Kaspersky Security Network e o Google Analytics for Firebase, SafetyNet Attestation, Firebase Performance Monitoring e Crashlytics se a chave da Kaspersky estiver bloqueada, se a licença de avaliação expirar ou se uma licença estiver ausente (o código de ativação é removido da política de grupo).

  - Aplicativo do Kaspersky Security for iOS:

    - **Sincronização com o Servidor de Administração**.

    O Kaspersky Security for iOS para de trocar informações com a Kaspersky Security Network se a licença de avaliação expirar ou se faltar uma licença (o código de ativação é removido da política de grupo).

  Os componentes restantes do aplicativo móvel não estão disponíveis para o usuário do dispositivo. O administrador pode usar políticas de grupo de gerenciar estes componentes no modo de funcionalidade limitada. Você não pode usar políticas de grupo para configurar outros componentes do aplicativo.

  Para continuar usando o aplicativo no modo de funcionalidade completa, é necessário renovar a Licença comercial. Recomendamos a renovação da Licença ou a compra uma nova antes que a atual expire a fim de assegurar a proteção máxima de seu computador contra todas as ameaças de segurança.

Sobre a assinatura

A *Assinatura para o Kaspersky Security for Mobile* é um pedido para usar o aplicativo móvel com os parâmetros selecionados (data de validade da assinatura, número de dispositivos móveis protegidos). Você poderá efetuar um pedido de assinatura do Kaspersky Security for Mobile com seu provedor de serviços (como o seu ISP). A assinatura poderá ser renovada manual ou automaticamente ou você poderá cancelar sua assinatura. Você poderá gerenciar sua assinatura no site do provedor de serviços.

A assinatura poderá ser limitada (por exemplo, um ano) ou ilimitada (sem data de validade). Para que o Kaspersky Security for Mobile continue a funcionar após a expiração do prazo limitado da assinatura, você deverá renovar sua assinatura. A assinatura ilimitada é renovada automaticamente se um pré-pagamento foi efetuado em tempo ao provedor de serviços.

No caso de uma assinatura limitada, quando ela expira, um período de carência poderá ser fornecido para a renovação da assinatura, e durante este período os aplicativos irão reter sua funcionalidade. A disponibilidade e a duração de tal período de carência são à discrição do provedor de serviços.

Para usar o Kaspersky Security for Mobile sob uma assinatura, você deve aplicar o código de ativação recebido do provedor de serviços. Após o código de ativação tiver sido aplicado, a chave será instalada para a Licença para usar o aplicativo sob assinatura.

As possíveis opções de gerenciamento da assinatura podem variar com cada provedor de serviços. O provedor de serviços pode não oferecer um período de carência para a renovação da assinatura durante o qual os aplicativos retêm sua funcionalidade.

Os códigos de ativação comprados sob a assinatura não podem ser usados para ativar versões anteriores do Kaspersky Security for Mobile.

Sobre a chave

Uma *chave* é uma sequência de bits que pode ser aplicada para ativar e usar a solução integrada do Kaspersky Security for Mobile, de acordo com os termos do Contrato de Licença do Usuário Final. As chaves são geradas pelos especialistas da Kaspersky.

Você pode adicionar uma chave para o aplicativo móvel usando um arquivo de chave ou código de ativação:

- Se a sua organização implementou o pacote de software do Kaspersky Security Center, você deve aplicar o arquivo de chave e distribuí-lo para os aplicativo móveis Android. A chave é exibida na interface do Kaspersky Security Center e na interface do aplicativo móvel Android como uma sequência alfanumérica exclusiva.

  Após adicionar chaves, você poderá substitui-las por outras chaves.

  Não é possível ativar o aplicativo Kaspersky Security for iOS com um arquivo de chave.

- Se a sua organização não usar o Kaspersky Security Center, será necessário compartilhar o código de ativação com o usuário. O usuário insere esse código de ativação no aplicativo móvel Android ou iOS. A chave é exibida na interface do aplicativo móvel como uma sequência alfanumérica exclusiva.

A chave poderá ser bloqueada pela Kaspersky, por exemplo, no caso de violação dos termos do Contrato de Licença do Usuário Final. Se a chave estiver bloqueada, o aplicativo móvel interrompe a execução de todas as suas funções, exceto a sincronização com o Servidor de Administração. Para continuar usando o aplicativo, você tem de adicionar uma chave diferente.

Sobre o código de ativação

O *código de ativação* é uma sequência única de 20 caracteres alfanuméricos. Você insere um código de ativação para adicionar uma chave que ativa o aplicativo móvel Kaspersky Endpoint Security for Android ou o aplicativo móvel Kaspersky Security for iOS. Você recebe o código de ativação no endereço de e-mail que especificou após comprar a solução integrada do Kaspersky Security for Mobile ou ao efetuar o pedido da versão de avaliação do Kaspersky Security for Mobile.

Para ativar o aplicativo móvel com um código de ativação, é preciso ter acesso à Internet para se conectar com os servidores de ativação da Kaspersky.

Se você perdeu seu código de ativação após ter ativado o aplicativo, ele pode ser restaurado. Você poderá precisar de seu código de ativação, por exemplo, para registrar com a Kaspersky CompanyAccount. Para restaurar o código de ativação, entre em contato com o Suporte Técnico da Kaspersky.

Sobre o arquivo de chave

Um *arquivo de chave* é um arquivo com a extensão .key que você recebe da Kaspersky. A finalidade de um arquivo de chave é adicionar uma chave que ative o aplicativo Kaspersky Endpoint Security for Android.

Não é possível ativar o aplicativo Kaspersky Security for iOS com um arquivo de chave.

O usuário recebe o arquivo de chave no endereço de e-mail especificado após a compra da solução integrada do Kaspersky Security for Mobile ou ao efetuar o pedido da versão de avaliação do Kaspersky Security for Mobile.

Você não precisa se conectar aos servidores de ativação da Kaspersky para poder ativar o aplicativo com um arquivo de chave.

Você poderá recuperar o arquivo de chave se este for acidentalmente excluído. Por exemplo, você poderá precisar de um arquivo de chave para se registrar com a Kaspersky CompanyAccount.

Para recuperar um arquivo de chave, execute uma das seguintes ações:

- Entre em contato com o vendedor da licença.
- Receba um arquivo de chave através do site da Kaspersky ao usar seu código de ativação disponível.

Fornecimento de dados no Kaspersky Endpoint Security for Android

O Kaspersky Security for Mobile está em conformidade com os Regulamentos Gerais de Proteção dos Dados (GDPR).

Para instalar o aplicativo, você ou um usuário do dispositivo devem ler e aceitar os termos do Contrato de Licença do Usuário Final. Além disso, é possível configurar uma política para aceitar as Declarações listadas abaixo globalmente, para todos os usuários. Caso contrário, os usuários serão avisados por uma notificação na tela principal do aplicativo para que aceitem as seguintes Declarações sobre o processamento dos dados pessoais do usuário:

- Declaração da Kaspersky Security Network
- Declaração relativa ao processamento dos dados para a Proteção na Web
- Declaração quanto ao processamento dos dados para propósitos de marketing

Caso opte por aceitar as Declarações globalmente, as versões das Declarações aceitas por meio do Kaspersky Security Center devem corresponder às versões já aceitas pelos usuários. Caso contrário, os usuários serão informados sobre o problema e convidados a aceitar a versão de uma Declaração que corresponda à versão aceita globalmente pelo administrador. O status do dispositivo no plug-in do Kaspersky Security for Mobile (Devices) também mudará para *Aviso*.

O usuário pode aceitar os termos de uma Declaração ou recusá-los a qualquer momento na seção **Sobre o aplicativo** nas configurações do Kaspersky Endpoint Security for Android.

Troca de informações com a Kaspersky Security Network

Para aprimorar a proteção em tempo real, o Kaspersky Endpoint Security for Android usa o serviço na nuvem da Kaspersky Security Network para a operação dos seguintes componentes:

- **Antivírus.** O aplicativo obtém o acesso à Base de Conhecimento on-line da Kaspersky quanto à reputação de arquivos e aplicativos. A verificação é executada para as ameaças cujas informações ainda não foram adicionadas ao banco de dados antivírus, mas já estão disponíveis na KSN. O serviço na nuvem da Kaspersky Security Network fornece a operação completa do antivírus e reduz a probabilidade de falsos alarmes.

- **Proteção na Web.** O aplicativo usa os dados recebidos da KSN para executar uma verificação de sites antes que eles sejam abertos. O aplicativo também determina a categoria de site que controla o acesso à Internet para os usuários de acordo com as listas de categorias permitidas e bloqueadas (por exemplo, a categoria "Comunicações via Internet").

- **Controle de aplicativos.** O aplicativo determina a categoria de aplicativo que restringe a inicialização de aplicativos que não atendam os requisitos de segurança corporativa de acordo com as listas de categorias permitidas e bloqueadas (por exemplo, a categoria "Jogos").

As informações sobre o tipo de dados enviados à Kaspersky ao usar a KSN durante a operação do antivírus e controle de aplicativos estão disponíveis no Contrato de Licença do Usuário Final. Ao aceitar os termos e condições do Contrato de Licença, o usuário concorda em transferir as seguintes informações.

As informações sobre o tipo de dados enviados à Kaspersky, ao usar a KSN durante a operação da proteção na web, estão disponíveis na Declaração sobre o processamento de dados para a proteção na web. Ao aceitar os termos e condições da Declaração, o usuário concorda em transferir as seguintes informações.

As informações sobre o tipo de dados estatísticos enviados à Kaspersky ao usar a KSN durante a operação do aplicativo móvel do Kaspersky Endpoint Security for Android estão disponíveis na Declaração da Kaspersky Security Network. Ao aceitar os termos e condições da Declaração, o usuário concorda em transferir as seguintes informações.

Provisão de Dados de acordo com o Contrato de Licença do Usuário Final

Nas situações em que o Código de Ativação é usado para ativar o Software, para verificar o uso legítimo do Software, o Usuário Final concorda em fornecer ao Titular dos Direitos periodicamente as seguintes informações:

- formato dos dados na solicitação para a infraestrutura do Titular dos direitos; endereço IPv4 do serviço Web acessado; tamanho do conteúdo do pedido para a infraestrutura do titular dos direitos; ID do protocolo; código de ativação do Software; tipo de compactação de dados; ID do Software; conjunto de IDs do Software que podem ser ativados no dispositivo do usuário; localização do Software; versão completa do Software; ID exclusivo do dispositivo; data e hora no dispositivo do usuário; ID de instalação do Software (PCID); Versão do SO, número da compilação do SO, número da atualização do SO, edição do SO, informações estendidas sobre a edição do SO; modelo do dispositivo; família do sistema operacional; formato dos dados na solicitação para a infraestrutura do Titular dos direitos; tipo de soma de verificação do objeto que está sendo processado;

cabeçalho da licença do Software; ID de um centro de ativação regional; data e hora de criação da chave de licença do Software; ID da licença do Software; ID do modelo de informações usado para fornecer a licença do Software; data e hora de expiração da licença do Software; status atual da chave de licença do Software; tipo de licença do Software usada; tipo da licença utilizada para ativar o Software; ID do Software derivado da licença.

A fim de proteger o Computador contra ameaças à informação, o Usuário Final concorda em fornecer periodicamente ao Titular as seguintes informações:

- tipo de soma de verificação do objeto que está sendo processado; soma de verificação do objeto que está sendo processado; o ID de componente do Software;
- ID do registro acionado nos bancos de dados antivírus do Software; carimbo de data e hora do registro acionado nos bancos de dados antivírus do Software; tipo de registro acionado nos bancos de dados antivírus do Software; Nome do malware detectado ou do software legítimo que pode ser usado para causar danos ao dispositivo ou aos dados do usuário;
- nome da loja através da qual o aplicativo foi instalado; nome de pacote do aplicativo; chave pública usada para assinar o arquivo APK; soma de verificação do certificado usado para assinar o arquivo APK; carimbo de data e hora do certificado digital;
- versão completa do Software; ID de atualização do Software; tipo de instalação de Software; o identificador de configuração; o resultado da ação do Software; código de erro;
- números que são derivados do arquivo APK do aplicativo Android de acordo com certas regras matemáticas e que não permitem a restauração do conteúdo do arquivo original; esses dados não contêm nomes e caminhos de arquivos, endereços, números de telefone ou outras informações pessoais dos usuários.

Se Você usar os servidores de atualização do Titular dos Direitos para baixar as Atualizações, o Usuário Final, a fim de aumentar a eficiência do procedimento de atualização, concordará em fornecer periodicamente ao Titular dos Direitos as seguintes informações:

- ID do Software derivado da licença; versão completa do Software; ID da licença do Software; tipo de licença do Software usada; ID de instalação do Software (PCID); ID do início da atualização do Software; endereço da Web que está sendo processado.

O Detentor dos Direitos pode usar tais informações também para receber informações estatísticas sobre a distribuição e do uso do Software.

As informações recebidas são protegidas pela Kaspersky de acordo com os requisitos estabelecidos por lei. As informações originais recebidas são armazenadas no formato criptografado e são destruídas na medida que sejam acumuladas (duas vezes por ano) ou por solicitação do usuário. As estatísticas gerais são armazenadas indefinidamente.

Provisão de dados sob a Declaração da Kaspersky Security Network

A utilização da KSN pode aumentar a eficácia da proteção fornecida pelo Software contra ameaças à segurança das informações e da rede.

Caso o usuário use uma licença para 5 ou mais nós, o Titular receberá e processará automaticamente os seguintes dados durante o uso da KSN:

- ID do registro acionado nos bancos de dados antivírus do Software; carimbo de data e hora do registro acionado nos bancos de dados antivírus do Software; tipo de registro acionado nos bancos de dados antivírus do Software; data e hora do lançamento dos bancos de dados do Software; Versão do SO, número da compilação do SO, número da atualização do SO, edição do SO, informações estendidas sobre a edição do SO;

versão do Service Pack do SO; detectar características; soma de verificação (MD5) do objeto que está sendo processado; nome do objeto sendo processado; sinalizador que indica se o objeto que está sendo processado é um arquivo PE; soma de verificação (MD5) da máscara que bloqueou o serviço Web; soma de verificação (SHA256) do objeto sendo processado; tamanho do objeto sendo processado; código do tipo de objeto; a decisão do Software sobre o objeto que está sendo processado; caminho para o objeto sendo processado; código do diretório; versão do componente do Software; versão das estatísticas que estão sendo enviadas; endereço acessado do serviço da web (URL, IP); tipo de cliente utilizado para aceder ao serviço Web; endereço IPv4 do serviço Web acessado; endereço IPv6 do serviço Web acessado; endereço da Web da origem da solicitação de serviço da web (referenciador). endereço da Web que está sendo processado;

- informações sobre objetos verificados (versão do aplicativo do AndroidManifest.xml; a decisão do Software sobre o aplicativo; método utilizado para obter a decisão do Software sobre o aplicativo; nome do pacote de instalação da loja; nome do pacote (ou nome do pacote de software) do AndroidManifest.xml; Categoria do Google SafetyNet; sinalizador que indica se o SafetyNet está ativado no dispositivo; valor SHA256 da resposta do Google SafetyNet; Esquema de assinatura do APK para o certificado do APK; código de versão do Software instalado; número de série do certificado que foi usado para assinar o arquivo APK; nome do arquivo APK que está sendo instalado; caminho para o arquivo APK que está sendo instalado; emissor do certificado que foi usado para assinar o arquivo APK; chave pública usada para assinar o arquivo APK; soma de verificação do certificado usado para assinar o arquivo APK; data e hora em que certificado expira; data e hora em que o certificado foi emitido; versão das estatísticas que estão sendo enviadas; algoritmo para calcular o thumbprint do certificado digital; hash MD5 do arquivo APK instalado; hash MD5 do arquivo DEX localizado no arquivo APK; autorizações concedidas dinamicamente ao aplicativo; versão do software de terceiros; sinalizador que indica se o aplicativo é o serviço de mensagens SMS predefinido; sinalizador que indica se o aplicativo tem Direitos de Administrador do dispositivo; sinalizador que indica se o aplicativo está no catálogo do sistema; sinalizador que indica se o aplicativo usa serviços de acessibilidade);

- informações sobre todos os objetos e atividades potencialmente maliciosos (conteúdo de fragmento do objeto sendo processado; data e hora em que certificado expira; data e hora em que o certificado foi emitido; ID da chave do keystore usado para criptografia; protocolo utilizado para trocar dados com a KSN; ordem de fragmento no objeto que está sendo processado; dados do log interno, gerados pelo módulo do Software antivírus para um objeto que está sendo processado; nome do emissor do certificado; chave pública do certificado; algoritmo de cálculo da chave pública do certificado; número de série do certificado; data e hora da assinatura do objeto; nome do proprietário do certificado e definições; impressão digital do certificado digital do objeto digitalizado e algoritmo de hash; data e hora da última modificação do objeto que está sendo processado; data e hora de criação de um objeto que está sendo processado; objetos ou partes dos mesmos que estão sendo processados; descrição de um objeto que está sendo processado de acordo com a definição nas propriedades do objeto; formato do objeto sendo processado; tipo de soma de verificação do objeto que está sendo processado; soma de verificação (MD5) do objeto que está sendo processado; nome do objeto sendo processado; soma de verificação (SHA256) do objeto sendo processado; tamanho do objeto sendo processado; nome do fornecedor do Software; a decisão do Software sobre o objeto que está sendo processado; versão do objeto sendo processado; origem da decisão tomada para o objeto que está sendo processado; soma de verificação do objeto que está sendo processado; nome do aplicativo principal; caminho para o objeto sendo processado; informações sobre os resultados de verificação da assinatura do arquivo; chave da sessão de início de sessão; algoritmo de criptografia para a chave da sessão de login; tempo de armazenamento do objeto que está sendo processado; algoritmo para calcular o thumbprint do certificado digital);

- tipo de compilação, por exemplo, "user" ou "ing"; nome completo do produto; fabricante de produto/hardware; se os aplicativos podem ser instalados fora do Google Play; status do serviço na nuvem para verificação de aplicativos Google; estado do serviço na nuvem para verificação de aplicativos do Google instalados através de ADB; codinome de desenvolvimento atual ou "REL" para compilações de produção; número da compilação incremental; string da versão visível para o usuário; nome do dispositivo do usuário; ID da compilação do Software visível para o usuário; impressão digital do firmware; ID do firmware; sinalizador indicando se o dispositivo está rooteado; sistema operacional; nome do Software; tipo de licença do Software usada;

- informações sobre a qualidade dos serviços KSN (protocolo utilizado para trocar dados com a KSN; ID do serviço da KSN acedido pelo Software; data e hora em que as estatísticas deixaram de ser recebidas; número de ligações da KSN extraídas da cache; número de pedidos para os quais foi encontrada uma resposta na base de dados de pedidos local; número de ligações da KSN malsucedidas; número de transações da KSN

malsucedidas; distribuição temporal das solicitações à KSN canceladas; distribuição temporal de conexões à KSN malsucedidas; distribuição temporal de transações da KSN malsucedidas; distribuição temporal de ligações da KSN bem-sucedidas; distribuição temporal de transações da KSN bem-sucedidas; distribuição temporal de solicitações à KSN bem-sucedidas; distribuição de tempo das solicitações à KSN que atingiram o limite de tempo; número de novas ligações da KSN; número de solicitações à KSN malsucedidas causadas por erros de roteamento; número de pedidos malsucedidos causados pela desativação da KSN nas definições do Software; número de pedidos malsucedidos para a KSN causados por problemas de rede; número de conexões à KSN bem-sucedidas; número de transações da KSN bem-sucedidas; número total de solicitações à KSN; data e hora em que as estatísticas começaram a ser recebidas);

- ID do dispositivo; versão completa do Software; ID de atualização do Software; ID de instalação do Software (PCID); tipo de instalação de Software;

- altura da tela do dispositivo; largura da tela do dispositivo; informações sobre o aplicativo sobreposto: hash MD5 do arquivo APK; informações sobre o aplicativo sobreposto: hash MD5 do arquivo classes.dex; informações sobre o aplicativo sobreposto: nome do arquivo APK; informações sobre o aplicativo sobreposto: caminho para o arquivo APK sem o nome do arquivo; altura da sobreposição; informações sobre o Software sobreposto: hash MD5 do arquivo APK; informações do aplicativo sobreposto: hash MD5 do arquivo classes.dex; informações do aplicativo sobreposto: nome do arquivo APK; informações do aplicativo sobreposto: caminho para o arquivo APK sem o nome do arquivo; informações do aplicativo sobreposto: nome do pacote do aplicativo (para o aplicativo sobreposto: se o anúncio for exibido em um desktop vazio, o valor deve ser "iniciador"); data e hora da sobreposição; informações sobre o aplicativo sobreposto: nome de pacote do aplicativo; largura da sobreposição;

- configurações do ponto de acesso de Wi-Fi em uso (tipo de dispositivo detectado; Configurações DHCP (somas de verificação de IPv6, DHCP IPv6, DNS1 IPv6, DNS2 IPv6 locais do gateway; soma de verificação do comprimento do prefixo da rede; soma de verificação do endereço IPv6 local); configurações DHCP (somas de verificação do endereço IP local do gateway, IP DHCP, IP DNS1, IP DNS2 e máscara de sub-rede); sinalizador que indica se o domínio DNS existe; soma de verificação do endereço IPv6 local atribuído; soma de verificação do endereço IPv4 local atribuído; sinalizador indicando se o dispositivo está ligado; tipo de autenticação da rede Wi-Fi; lista de redes Wi-Fi disponíveis e as suas definições; soma de verificação (MD5 com salt) do endereço MAC do ponto de acesso; soma de verificação (SHA256 com salt) do endereço MAC do ponto de acesso; tipos de conexão com suporte do ponto de acesso Wi-Fi; tipo de criptografia da rede Wi-Fi; hora local de início e término da conexão da rede Wi-Fi; ID da rede Wi-Fi com base no endereço MAC do ponto de acesso; ID da rede Wi-Fi com base no nome da rede Wi-Fi; ID da rede Wi-Fi com base no nome da rede Wi-Fi e no endereço MAC do ponto de acesso; intensidade do sinal Wi-Fi; nome da rede Wi-Fi; conjunto de protocolos de autenticação suportados por esta configuração; protocolo de autenticação utilizado para uma conexão WPA-EAP; protocolo de autenticação interna; o conjunto de cifras do grupo suportado por esta configuração; o conjunto de protocolos de gerenciamento de chaves suportados por esta configuração; a categoria final de privacidade da rede no Software; a categoria de segurança final da rede no Software; conjunto de cifras em bloco para WPA suportadas por esta configuração; o conjunto de protocolos de segurança suportados por esta configuração);

- Data e hora da instalação do Software; data de ativação do Software; identificador da organização parceira pela qual o pedido da licença do Software foi feito; ID do Software derivado da licença; número de série da chave de licença do Software; localização do Software; sinalizador que indica se a participação na KSN está ativada; ID do Software licenciado; ID da licença do Software; ID do SO; versão de bits do sistema operacional.

Além disso, para cumprir o objetivo declarado de aumentar a eficácia de proteção fornecida pelo Software, o Titular dos Direitos poderá receber objetos que podem ser explorados por invasores para danificar o Computador e criar ameaças à segurança das informações.

O fornecimento das informações mencionadas acima à KSN é voluntário. Você pode optar por não participação na Kaspersky Security Network a qualquer momento.

Fornecimento de dados de acordo com a Declaração relativa ao processamento dos dados para a Proteção na Web

De acordo com a Declaração da proteção na web, o Detentor dos Direitos processa os dados para obter a funcionalidade de proteção na web. O objetivo declarado inclui detectar ameaças da Web e determinar as categorias de sites visitados usando o serviço na nuvem Kaspersky Security Network (KSN).

Com seu consentimento, os seguintes dados serão automaticamente enviados regularmente para o Detentor dos Direitos de acordo com a Declaração da Proteção na Web:

- Versão do produto; Identificador exclusivo do dispositivo; ID de instalação; Tipo de Produto.
- Endereço de URL da página, número da porta, protocolo de URL, URL que se refere à informação solicitada.

Provisão de Dados de acordo com a Declaração quanto ao processamento de dados para propósitos de marketing

O Titular usa sistemas de informação de terceiros para processar dados. O processamento de dados feito por esses terceiros é regido pelas declarações de privacidade de tais sistemas de informação de terceiros. A seguir, os serviços que o Titular usa e os dados processados por eles:

Google Analytics para Firebase

Durante o uso do Software, os seguintes dados serão enviados para o Google Analytics para Firebase automaticamente e de forma regular, a fim de atingir a finalidade declarada:

- Informações do aplicativo (versão do aplicativo, ID do aplicativo e a ID do aplicativo no serviço Firebase, ID da instância no serviço Firebase, nome da loja onde o aplicativo foi obtido, carimbo de data/hora do primeiro lançamento do Software)
- ID da instalação do aplicativo no dispositivo e o método de instalação no dispositivo
- informações sobre a região e a localização do idioma
- informações sobre a resolução de tela do dispositivo
- informações sobre a obtenção de root pelo usuário
- informações de diagnóstico sobre o dispositivo do serviço SafetyNet Attestation
- informações sobre configuração do Kaspersky Endpoint Security for Android como recurso de Acessibilidade
- informações sobre transições entre as telas do aplicativo, duração da sessão, início e término de uma sessão de tela, nome da tela
- informações sobre o protocolo usado para enviar dados para o serviço Firebase, sua versão e ID do método de envio de dados utilizado
- detalhes sobre o tipo e os parâmetros do evento para o qual os dados são enviados
- informações sobre a licença do aplicativo, sua disponibilidade e o número de dispositivos
- informações sobre a frequência de atualizações do banco de dados de antivírus e sincronização com o Servidor de Administração

- informações sobre o Console de Administração (Kaspersky Security Center ou sistemas EMM de terceiros)
- ID do Android
- ID de publicidade
- informações sobre o Usuário: categoria de idade e sexo, identificador do país de residência e lista de interesses
- informações sobre o computador do Usuário onde o Software está instalado: nome do fabricante do computador, tipo de computador, modelo, versão e idioma (localidade) do sistema operacional, informações sobre o aplicativo aberto pela primeira vez nos últimos 7 dias e o aplicativo aberto pela primeira vez há mais de 7 dias

  Os dados são encaminhados para o Firebase por meio de um canal seguro. Informações sobre como os dados são processados in Firebase são publicadas em: https://firebase.google.com/support/privacy.

SafetyNet Attestation

Durante o uso do Software, os seguintes dados serão enviados para o SafetyNet Attestation automaticamente e de forma regular a fim de atingir a finalidade declarada:

- momento de verificação do dispositivo
- informações sobre software, nome e dados sobre os certificados do software
- resultados da verificação do dispositivo
- verificações de ID aleatórias para verificar os resultados do dispositivo de verificação

  Os dados são encaminhados para o SafetyNet Attestation por meio de um canal seguro. Informações sobre como os dados são processados in SafetyNet Attestation são publicadas em: https://policies.google.com/privacy.

Firebase Performance Monitoring

Durante o uso do Software, os seguintes dados serão enviados automaticamente e de forma regular para o Firebase Performance Monitoring a fim de alcançar a finalidade declarada:

- ID exclusiva de instalação
- nome de pacote do aplicativo
- versão do software instalado
- nível da bateria e estado de carregamento da bateria
- operadora
- estado de primeiro ou segundo plano da aplicação
- geografia
- Endereço IP
- código de idioma do dispositivo
- informações sobre a conexão de rádio/rede
- ID pseudônimo da instância do Software;

- tamanho da RAM e do disco
- sinalizador indicando se o dispositivo está rooteado;
- força do sinal
- duração dos rastreios automáticos
- rede e as seguintes informações correspondentes: código de resposta, tamanho da carga em bytes, tempo de resposta
- descrição do dispositivo

  Os dados são encaminhados para o Firebase Performance Monitoring por meio de um canal seguro. Informações sobre como os dados são processados in Firebase Performance Monitoring são publicadas em: https://firebase.google.com/support/privacy.

Crashlytics

Durante o uso do Software, os seguintes dados serão enviados automaticamente e de forma regular para o Crashlytics a fim de alcançar a finalidade declarada:

- ID do software
- versão do software instalado
- sinalizador que indica se o Software estava sendo executado em segundo plano
- arquitetura da CPU
- ID único do evento
- data e hora do evento
- modelo do dispositivo
- espaço em disco total e quantidade atualmente utilizada
- o nome e versão do aplicativo
- RAM total e quantidade atualmente utilizada
- sinalizador indicando se o dispositivo está rooteado;
- orientação da tela no momento do evento
- fabricante de produto/hardware;
- ID exclusiva de instalação
- versão das estatísticas que estão sendo enviadas;
- o tipo de exceção do Software
- texto da mensagem de erro
- sinalizador que indica que a exceção do Software foi causada por uma exceção inserida

- ID da thread
- um sinalizador indicando se o quadro foi a causa do erro do software
- sinalizador que indica que a thread causou o encerramento inesperado do Software
- informação sobre o sinal que fez com que o software encerrasse inesperadamente: nome do sinal, código do sinal, endereço do sinal
- para cada quadro associado a uma thread, exceção ou erro: o nome do arquivo de quadro, número da linha do arquivo de quadro, símbolos de depuração, endereço e deslocamento na imagem binária, nome de exibição da biblioteca com o quadro, tipo de quadro, sinalizador indicando se o quadro foi a causa do erro
- ID do SO;
- ID da emissão associada ao evento
- informação sobre eventos que aconteceram antes de o Software encerrar inesperadamente: identificador do evento, data e hora do evento, tipo de evento e valor
- valores de registro da CPU
- tipo de evento e valor

  Os dados são encaminhados para a Crashlytics por meio de um canal seguro. Informações sobre como os dados são processados in Crashlytics são publicadas em: https://firebase.google.com/terms/crashlytics-app-distribution-data-processing-terms.

O fornecimento das informações acima para processamento para fins de marketing é voluntário.

Fornecimento de dados no Kaspersky Security for iOS

O Kaspersky Security for Mobile está em conformidade com os Regulamentos Gerais de Proteção dos Dados (GDPR).

Para instalar o aplicativo, um usuário do dispositivo deve ler e aceitar os termos das seguintes declarações sobre o processamento dos dados pessoais do usuário:

- Contrato de Licença do Usuário Final
- Política de Privacidade de Produtos e Serviços

Opcionalmente, o usuário pode ler e aceitar os termos da seguinte declaração:

- Declaração da Kaspersky Security Network

O usuário pode visualizar os termos desses documentos a qualquer momento na seção **Sobre o aplicativo** → **Contratos e declarações** nas configurações do Kaspersky Security for iOS. Nesta seção, o usuário também pode aceitar ou recusar os termos da Declaração da KSN.

Troca de informações com a Kaspersky Security Network

Para melhorar a proteção em tempo real, o Kaspersky Security for iOS usa o serviço de nuvem da Kaspersky Security Network para operar o componente **Proteção na Web**. O aplicativo usa os dados recebidos da KSN para verificar os recursos da Web antes de serem abertos.

As informações sobre o tipo de dados enviados à Kaspersky ao usar a KSN durante a operação da Proteção na Web estão disponíveis no Contrato de Licença do Usuário Final. Ao aceitar os termos e condições do Contrato de Licença, o usuário concorda em transferir as seguintes informações.

As informações sobre o tipo de dados estatísticos enviados à Kaspersky ao usar a KSN durante a operação do aplicativo móvel Kaspersky Security for iOS estão disponíveis na Declaração da Kaspersky Security Network. Ao aceitar os termos e condições da Declaração, o usuário concorda em transferir as seguintes informações.

Provisão de Dados de acordo com o Contrato de Licença do Usuário Final

Nas situações em que o Código de Ativação é usado para ativar o Software, para verificar o uso legítimo do Software, o Usuário Final concorda em fornecer ao Titular dos Direitos periodicamente as seguintes informações:

- formato dos dados na solicitação para a infraestrutura do Titular dos Direitos; endereço IPv4 do serviço Web acessado; tamanho do conteúdo do pedido para a infraestrutura do titular dos direitos; ID do protocolo; código de ativação do Software; tipo de compactação de dados; ID do Software; conjunto de IDs do Software que podem ser ativados no dispositivo do usuário; localização do Software; versão completa do Software; ID exclusivo do dispositivo; data e hora no dispositivo do usuário; ID de instalação do Software (PCID); código de ativação do Software utilizado atualmente; Versão do SO, número da compilação do SO, número da atualização do SO, edição do SO, informações estendidas sobre a edição do SO; modelo do dispositivo; código da operadora móvel; família do sistema operacional; ID do Software derivado da licença; lista de acordos apresentados ao usuário pelo software; tipo de contrato jurídico aceito pelo usuário ao usar o Software; versão do acordo legal aceito pelo usuário durante o uso do Software; sinalizador indicando se o usuário aceitou os termos do acordo legal ao usar o Software; tipo de soma de verificação do objeto que está sendo processado; cabeçalho da licença do Software; ID de um centro de ativação regional; data e hora de criação da chave de licença do Software; ID da licença do Software; ID do modelo de informações usado para fornecer a licença do Software; data e hora de expiração da licença do Software; status atual da chave de licença do Software; tipo de licença do Software usada; tipo da licença utilizada para ativar o Software; ID do Software derivado da licença.

O Detentor dos Direitos pode usar essas informações também para coletar informações estatísticas sobre a distribuição e o uso do Software do Detentor dos Direitos.

A fim de proteger o Computador contra ameaças à informação, o Usuário Final concorda em fornecer periodicamente ao Titular as seguintes informações:

- formato dos dados na solicitação para a infraestrutura do Titular dos Direitos; endereço acessado do serviço da web (URL, IP); número da porta; endereço da Web da fonte da solicitação de serviço da Web (referenciador).
- versão completa do Software; ID de atualização do Software; tipo do Software instalado; ID do Software; o identificador da configuração; o resultado da ação do Software; código de erro.
- Endereço da web que está sendo processado; endereço IPv4 do serviço Web acessado; impressão digital do certificado digital do objeto digitalizado e algoritmo de hash; tipo de certificado; conteúdo do certificado digital sendo processado.

Provisão de dados sob a Declaração da Kaspersky Security Network

Quando a Declaração da KSN é aceita, o Detentor de Direitos recebe e processa automaticamente os seguintes dados:

- informações sobre a qualidade dos serviços KSN (protocolo utilizado para trocar dados com a KSN; ID do serviço da KSN acedido pelo Software; data e hora em que as estatísticas deixaram de ser recebidas; número de ligações da KSN extraídas da cache; número de pedidos para os quais foi encontrada uma resposta na base de dados de pedidos local; número de ligações da KSN malsucedidas; número de transações da KSN malsucedidas; distribuição temporal das solicitações à KSN canceladas; distribuição temporal de conexões à KSN malsucedidas; distribuição temporal de transações da KSN malsucedidas; distribuição temporal de ligações da KSN bem-sucedidas; distribuição temporal de transações da KSN bem-sucedidas; distribuição temporal de solicitações à KSN bem-sucedidas; distribuição de tempo das solicitações à KSN que atingiram o limite de tempo; número de novas ligações da KSN; número de solicitações à KSN malsucedidas causadas por erros de roteamento; número de pedidos malsucedidos causados pela desativação da KSN nas definições do Software; número de pedidos malsucedidos para a KSN causados por problemas de rede; número de conexões à KSN bem-sucedidas; número de transações da KSN bem-sucedidas; número total de solicitações à KSN; data e hora em que as estatísticas começaram a ser recebidas).

- ID do dispositivo; versão completa do Software; ID de atualização do Software; ID de instalação do Software (PCID); tipo do Software instalado.

- Data e hora da instalação do Software; data de ativação do Software; localização do Software; sinalizador que indica se a participação na KSN está ativada; ID do Software licenciado; ID da licença do Software; ID do SO; versão do sistema operacional instalada no computador do usuário; versão de bits do sistema operacional.

O fornecimento das informações mencionadas acima à KSN é voluntário. Você pode optar por não participação na Kaspersky Security Network a qualquer momento.

Entre em contato com o Suporte técnico

Essa seção descreve como obter suporte técnico e os termos em que está disponível.

Como obter Suporte Técnico

Caso não consiga encontrar uma solução para o seu problema na documentação do Kaspersky Security for Mobile ou em qualquer uma das fontes de informação sobre o Kaspersky Security for Mobile, entre em contato com o Suporte Técnico. Os especialistas do Suporte Técnico responderão a todas as suas perguntas sobre a instalação e o uso do Kaspersky Security for Mobile.

A Kaspersky fornece suporte ao Kaspersky Security for Mobile durante o ciclo de vida do produto (consulte a página do ciclo de vida de suporte do produto). Antes de entrar em contato com o Suporte Técnico, leia as regras de suporte.

Você pode entrar em contato com o Suporte Técnico das seguintes formas:

- Ao visitar o site de Suporte Técnico
- Enviando uma solicitação ao Suporte Técnico através do portal Kaspersky CompanyAccount

Suporte técnico através do Kaspersky CompanyAccount

O Kaspersky CompanyAccount é um portal para empresas que usam aplicativos da Kaspersky. O portal Kaspersky CompanyAccount foi concebido para facilitar a interação entre usuários e especialistas da Kaspersky através de solicitações on-line. É possível usar o Kaspersky CompanyAccount para rastrear o status de suas solicitações on-line além de armazenar um histórico delas.

Você pode registrar todos os funcionários de sua empresa em uma única conta do Kaspersky CompanyAccount. Uma única conta permite que você gerencie centralmente as solicitações de funcionários registrados para a Kaspersky, bem como gerenciar os privilégios que esses funcionários têm através do Kaspersky CompanyAccount.

O portal Kaspersky CompanyAccount está disponível nos seguintes idiomas:

- Inglês
- Espanhol
- Italiano
- Alemão
- Polonês
- Português
- Russo
- Francês

- Japonês

Para saber mais sobre o Kaspersky CompanyAccount, visite o site de Suporte Técnico.

Fontes de informações sobre o aplicativo

Página da Web do Kaspersky Security for Mobile no site da Kaspersky

Na página do Kaspersky Security for Mobile é possível encontrar informações gerais sobre o aplicativo, seus recursos e parâmetros de operação.

A página da Web do Kaspersky Security for Mobile fornece um link para a eStore. Nela, você pode comprar ou renovar o aplicativo.

Página web do Kaspersky Security for Mobile na Base de dados de conhecimento

Base de Dados de Conhecimento é uma seção do site de Suporte Técnico.

Na página do Kaspersky Security for Mobile na Base de Dados de Conhecimento, é possível encontrar artigos com informações úteis, recomendações e respostas para perguntas frequentes sobre a compra, instalação e uso do aplicativo.

Os artigos da Base de Dados de Conhecimento podem responder perguntas relacionadas não apenas ao Kaspersky Security for Mobile mas também a outros aplicativos da Kaspersky. Os artigos da Base de Dados de Conhecimento podem também incluir notícias do Suporte Técnico.

Ajuda on-line

A ajuda on-line do aplicativo contém arquivos de ajuda.

A Ajuda de contexto para os plug-ins de administração para o Kaspersky Security for Mobile fornece informações sobre as janelas do Kaspersky Security Center: uma descrição das configurações para o Kaspersky Security for Mobile e links para descrições das tarefas que usam estas configurações.

A ajuda completa dos aplicativos Kaspersky Endpoint Security for Android e Kaspersky Security for iOS fornece informações sobre como configurar e usar aplicativos móveis.

Discutir os aplicativos da Kaspersky no Fórum de Suporte da Kaspersky

Se a sua pergunta não precisar de uma resposta urgente, você poderá discuti-la com os especialistas da Kaspersky e outros usuários no nosso Fórum.

No Fórum, é possível visualizar os tópicos de discussão, postar comentários e criar novos tópicos de discussão.

Glossário

Administrador do dispositivo

Um conjunto de direitos do aplicativo em um dispositivo Android que permite ao aplicativo utilizar as políticas de gerenciamento do dispositivo. É necessário implementar a funcionalidade completa do Kaspersky Endpoint Security em dispositivos Android.

Administrador do Kaspersky Security Center

A pessoa que gerencia as operações do aplicativo por meio do sistema de administração centralizada remota do Kaspersky Security Center.

Arquivo de chave

Um arquivo no formato xxxxxxxx.key que possibilita o uso de um aplicativo da Kaspersky sob uma licença de avaliação ou licença comercial. O aplicativo gera o arquivo de chave com base no código de ativação. Você só pode usar o aplicativo quando tiver um arquivo de chave.

Arquivo de manifesto

Um arquivo em formato PLIST que contém um link para o arquivo do aplicativo (arquivo ipa) localizado em um servidor Web. É utilizado por dispositivos iOS para localizar, baixar e instalar aplicativos de um servidor Web.

Assinatura

Permite o uso do aplicativo dentro dos parâmetros selecionados (data de expiração e número de dispositivos). Você pode pausar ou retomar sua assinatura, renová-la automaticamente ou cancelá-la.

Ativação do aplicativo

Alternando o aplicativo para o modo de totalmente funcional. A ativação do aplicativo é executada pelo usuário durante ou após a instalação do aplicativo. Você deve ter um código de ativação ou arquivo de chave para ativar o aplicativo.

Bancos de dados antivírus

Os bancos de dados que contêm informações sobre as ameaças de segurança do computador conhecidas pela Kaspersky a partir da data de lançamento dos bancos de dados antivírus. As entradas nos bancos de dados antivírus permitem que códigos maliciosos sejam detectados nos objetos verificados. Os bancos de dados antivírus são criados pelos especialistas da Kaspersky e atualizados a cada hora.

Categorias da Kaspersky

Categorias de dados predefinidas desenvolvidas por especialistas da Kaspersky. As categorias podem ser atualizadas durante as atualizações do banco de dados do aplicativo. Um Diretor de segurança não pode modificar ou excluir categorias predefinidas.

Certificado (APNs) de serviço de Notificação Apple Push

Certificado assinado pela Apple, que permite que você use o Apple Push Notification. Por meio do Apple Push Notification, um Servidor de MDM do iOS pode gerenciar dispositivos iOS.

Código de ativação

Um código que você recebe ao comprar uma licença do Kaspersky Endpoint Security. Esse código é necessário para a ativação do aplicativo.

O código de ativação é uma sequência única de vinte letras e números no formato xxxxx-xxxxx-xxxxx-xxxxx.

Código para desbloquear

Um código que você pode obter no Kaspersky Security Center. É necessário desbloquear um dispositivo após a execução dos comandos **Bloquear e Localizar**, **Alarme** ou **Retrato** terem sido executados e quando a Autodefesa for acionada.

Contrato de Licença do Usuário Final

O contrato que vincula Você e a AO Kaspersky Lab que estipula os termos com os quais Você pode usar o aplicativo.

Controle de conformidade

A verificação das configurações de um dispositivo móvel e do Kaspersky Endpoint Security for Android para atestar que estejam em conformidade com os requisitos de segurança corporativa. Os requisitos de segurança corporativa regulam o uso do dispositivo. Por exemplo, a proteção em tempo real deve estar ativada no dispositivo, os bancos de dados antivírus devem estar atualizados e a senha do dispositivo deve ser forte o suficiente. O controle de conformidade tem base em uma lista de regras. Uma regra de conformidade inclui os seguintes componentes:

- Critério de verificação do dispositivo (por exemplo, ausência de aplicativos proibidos no dispositivo)
- Intervalo de tempo alocado para que o usuário corrija a não conformidade (por exemplo, 24 horas)
- A ação que será executada no dispositivo se o usuário não corrigir a não conformidade dentro do tempo definido (por exemplo, bloqueio do dispositivo)

Dispositivo EAS

Um dispositivo móvel conectado ao Servidor de Administração por meio do protocolo Exchange ActiveSync.

Dispositivo iOS MDM

Um dispositivo móvel iOS controlado pelo Servidor de iOS MDM.

Dispositivo supervisionado

Dispositivo iOS cujas configurações são monitoradas pelo Apple Configurator, um programa para a configuração de grupo de dispositivos iOS. Um dispositivo supervisionado tem o status *supervisionado* no Apple Configurator. Sempre que um dispositivo supervisionado se conectar ao computador, o Apple Configurator verificará a configuração do dispositivo em relação às configurações de referência especificadas e as redefinirá, caso seja necessário. Um dispositivo supervisionado não pode ser sincronizado com o Apple Configurator instalado em um computador diferente.

Todo dispositivo supervisionado fornece mais configurações para serem redefinidas através da política do Kaspersky Device Management for iOS do que um dispositivo não supervisionado. Por exemplo, é possível configurar um servidor proxy HTTP para monitorar o tráfego da Internet em um dispositivo na rede corporativa. Por padrão, todos os dispositivos móveis são não supervisionados.

Estação de trabalho do administrador

O computador no qual o Console de Administração do Kaspersky Security Center foi implementado. Se o plug-in de administração de aplicativos estiver instalado na estação de trabalho do administrador, ele pode gerenciar os aplicativos móveis do Kaspersky Endpoint Security implementados em dispositivos do usuário.

Grupo de administração

Um conjunto de dispositivos gerenciados, como dispositivos móveis, agrupados de acordo com as funções que realizam e o conjunto de aplicativos instalados neles. Os dispositivos gerenciados são agrupados para que possam ser gerenciados como um todo. Por exemplo, os dispositivos móveis com o mesmo sistema operacional podem ser combinados em um grupo de administração. Um grupo pode incluir outros grupos de administração. É possível criar políticas de grupo e tarefas de grupo para dispositivos de grupo.

IMAP

Protocolo para acessar o e-mail. Em contraste com o protocolo POP3, o IMAP fornece capacidades estendidas para trabalhar com caixas de correio, tal como gerenciar pastas e manusear mensagens sem copiar o seu conteúdo do servidor de e-mail. O protocolo IMAP usa a porta 134.

Kaspersky Private Security Network (KSN Privada)

A Kaspersky Private Security Network é uma solução que fornece acesso por meio do aplicativo aos bancos de dados de reputação da Kaspersky Security Network, além de outros dados estatísticos, sem enviar dados de seus dispositivos para a Kaspersky Security Network. A Kaspersky Private Security Network foi desenvolvida para clientes corporativos que não têm acesso à Kaspersky Security Network por qualquer um dos seguintes motivos:

- Os dispositivos do usuário não estão conectados à Internet.
- A transmissão de quaisquer dados para fora do país ou da LAN corporativa é proibida por lei ou por políticas de segurança corporativa.

Kaspersky Security Network (KSN)

Uma infraestrutura de serviços na nuvem que oferece acesso ao banco de dados da Kaspersky, com informações constantemente atualizadas sobre a reputação de arquivos, recursos da web e softwares. O Kaspersky Security Network garante respostas mais rápidas dos aplicativos da Kaspersky a novas ameaças, aprimora o desempenho de alguns componentes de proteção e reduz a possibilidade de falsos positivos.

Licença

Um direito por tempo limitado para usar o aplicativo, concedido de acordo com o Contrato de Licença do Usuário Final.

Pacote de instalação

Um conjunto de arquivos criado para instalação remota de um aplicativo da Kaspersky, utilizando o sistema de administração remota. Um pacote de instalação é criado com base nos arquivos dedicados incluídos no pacote de distribuição do aplicativo. O pacote de instalação contém uma gama de configurações necessárias para instalar o aplicativo e colocá-lo em execução imediatamente após a instalação. Os valores de configurações no kit de distribuição correspondem aos valores padrão das configurações do aplicativo.

Pacote de instalação independente

Um arquivo de instalação do Kaspersky Endpoint Security para o sistema operacional Android, que contém as configurações de conexão do aplicativo no Servidor de Administração. Ele é criado com base no pacote de instalação do aplicativo e é um caso específico do pacote de aplicativos móveis.

Perfil de iOS MDM

Um perfil com um conjunto de configurações para conectar dispositivos móveis iOS ao Servidor de Administração. Um perfil de iOS MDM torna possível distribuir perfis de configuração iOS em modo de segundo plano usando o Servidor de MDM do iOS, bem como receber informações de diagnóstico expandidas sobre dispositivos móveis. Um link para o perfil de iOS MDM precisa ser enviado a um usuário com a finalidade de permitir que o Servidor de iOS MDM descubra e conecte o dispositivo móvel do usuário iOS.

Perfil de provisionamento

Coleção de configurações para a operação de aplicativos em dispositivos móveis iOS. Um perfil de provisionamento contém informações sobre a licença; ele está vinculado a um aplicativo específico.

Perfil de trabalho do Android

Um ambiente seguro no dispositivo do usuário, no qual o administrador pode gerenciar os aplicativos e as contas de usuário sem restringir o uso dos dados pessoais pelo usuário. Quando um perfil de trabalho for criado no dispositivo móvel do usuário, o seguintes aplicativos corporativos são automaticamente instalados no perfil de trabalho: Google Play Market, Google Chrome, Downloads, Kaspersky Endpoint Security for Android e outros. Os aplicativos corporativos instalados no perfil do trabalho e as notificações sobre estes aplicativos são marcados com um ícone de maleta na cor vermelha. Você deve criar uma conta corporativa do Google separada para o aplicativo Google Play Market. Os aplicativos instalados no perfil do trabalho aparecem na lista de aplicativos comuns.

Período da licença

Um período do tempo durante o qual você tem acesso aos recursos do aplicativo e aos direitos de usar serviços adicionais. Os serviços que você pode usar dependem do tipo de licença.

Phishing

Um tipo de fraude na Internet que visa obter acesso não autorizado aos dados confidenciais dos usuários.

Plug-in de gerenciamento do aplicativo

Um componente dedicado que fornece a interface para gerenciar os aplicativos da Kaspersky por meio do Console de Administração. Cada aplicativo que possa ser gerenciado por meio do Kaspersky Security Center SPE tem seu próprio plug-in de gerenciamento. O plug-in de gerenciamento está incluído em todos os aplicativos da Kaspersky que possam ser gerenciados através do Kaspersky Security Center.

Política

Um conjunto de configurações do aplicativo e aplicativos móveis do Kaspersky Endpoint Security aplicadas a grupos de administração e dispositivos individuais. É possível aplicar diferentes políticas a diferentes grupos de administração. Uma política inclui configurações especificadas para todos os aplicativos móveis do Kaspersky Endpoint Security.

POP3

Protocolo da rede usado por um programa de e-mail cliente para receber mensagens de um servidor de e-mail.

Quarentena

A pasta para a qual o aplicativo da Kaspersky move os aplicativos provavelmente infectados que foram detectados. Os objetos são armazenados na Quarentena em formato criptografado para evitar qualquer impacto no computador.

Servidor da Web do Kaspersky Security Center

Um componente do Kaspersky Security Center instalado junto com o Servidor de Administração. O Servidor da Web foi projetado para a transmissão, através de uma rede, de pacotes de instalação independentes, perfis do iOS MDM e arquivos de uma pasta compartilhada.

Servidor de Administração

Um componente do Kaspersky Security Center que armazena centralmente informações sobre todos os aplicativos da Kaspersky instalados dentro da rede corporativa. Ele pode ser utilizado para gerenciar esses aplicativos.

Servidor de dispositivos móveis

Um componente do Kaspersky Endpoint Security que permite conectar dispositivos móveis do Exchange ActiveSync ao Servidor de Administração.

Servidor de iOS MDM

Um componente do Kaspersky Endpoint Security que é instalado em dispositivo cliente e que permite a conexão de dispositivos móveis iOS ao Servidor de Administração, além do gerenciamento dos dispositivos móveis iOS através do serviço Apple Push Notifications (APNs).

Servidor proxy

Um serviço de rede de computador que permite que os usuários façam solicitações indiretas a outros serviços de rede. Primeiro, um usuário se conecta a um servidor proxy e solicita um recurso (por exemplo, um arquivo) localizado em outro servidor. Então o servidor proxy conecta-se ao servidor especificado e obtém o recurso dele ou devolve o recurso do seu próprio cache (se o proxy tiver seu próprio cache). Em alguns casos, a solicitação de um usuário ou a resposta de um servidor pode ser modificada pelo servidor proxy para determinados propósitos.

Servidores de atualização da Kaspersky

Os servidores HTTP(S) na Kaspersky dos quais os aplicativos da Kaspersky baixam o banco de dados e os módulos de atualizações do aplicativo.

Solicitação de Assinatura do Certificado

Arquivo com as configurações de um Servidor de Administração, aprovado pela Kaspersky e enviado à Apple para a obtenção de um certificado de APNs.

SSL

Um protocolo de criptografia de dados usados na Internet e em redes locais. O protocolo de Camada de Soquete Seguro (SSL, Secure Socket Layer) é usado em aplicativos da Web para criar uma conexão segura entre um cliente e o servidor.

Tarefa de grupo

Uma tarefa que se destina a um grupo de administração e é executada em dispositivos gerenciados incluídos no grupo.

Vírus

Um programa que infecta outros adicionando-lhes seu próprio código para obter o controle quando os arquivos infectados forem executados. Essa definição simples permite identificar a principal ação executada por qualquer vírus: infecção.

Informações sobre o código de terceiros

É possível baixar e ler informações sobre códigos de terceiros nos seguintes arquivos:

- legal_notices_Android.txt (para o aplicativo Kaspersky Endpoint Security for Android)
- legal_notices_iOS.txt (para o aplicativo Kaspersky Security for iOS)

Em dispositivos móveis, as informações sobre códigos de terceiros estão disponíveis na seção **Sobre o aplicativo** dos aplicativos móveis.

Avisos de marcas registradas

As marcas comerciais e as marcas de serviço registradas são de propriedade de seus respectivos proprietários.

PostScript é marca registrada ou comercial da Adobe nos Estados Unidos e/ou em outros países.

AirDrop e AirPrint são marcas comerciais da Apple Inc.

Apple, Apple Configurator, AirPlay, AirPort Express, App Store, Apple TV, Bonjour, Face ID, FaceTime, FileVault, iBooks, iCal, iCloud, iPad, iPadOS, iPhone, iTunes, OS X, Safari, Spotlight e Touch ID são marcas comerciais da Apple Inc., registradas nos EUA e em outros países e regiões.

Aruba Networks é uma marca comercial da Aruba Networks, Inc. nos Estados Unidos e em alguns outros países.

A palavra, marca e logotipos Bluetooth são de propriedade da Bluetooth SIG, Inc.

Cisco, Cisco AnyConnect e IOS são marcas registradas ou marcas comerciais da Cisco Systems, Inc. e/ou de suas afiliadas nos Estados Unidos e em alguns outros países.

SecurID é marca registrada ou comercial da EMC Corporation nos Estados Unidos e/ou em outros países.

Google, Android, Chrome, Chromebook, Chromium, Crashlytics, Firebase, Google Analytics, Google Chrome, Google Mail, Google Maps, Google Play, Nexus e SPDY são marcas comerciais da Google LLC.

HTC é uma marca comercial da HTC Corporation.

Huawei, HUAWEI e EMUI são marcas comerciais da Huawei Technologies Co., Ltd registradas na China e em outros países.

IBM e Maas360 são marcas comerciais da International Business Machines Corporation, registradas em muitas jurisdições em todo o mundo.

Juniper Networks, Juniper e JUNOS são marcas comerciais ou marcas registradas da Juniper Networks, Inc. nos Estados Unidos e em outros países.

Microsoft, ActiveSync, Microsoft Intune, Tahoma, Windows, Windows Mobile e Windows Phone são marcas registradas comerciais do grupo de empresas Microsoft.

MOTOROLA e o logotipo M estilizado são marcas comerciais ou marcas registradas da Motorola Trademark Holdings, LLC.

Oracle e JavaScript são marcas registradas da Oracle e/ou de suas afiliadas.

A marca registrada BlackBerry é de propriedade da Research In Motion Limited e registrada no Estados Unidos e pode estar pendente ou registrada em outros países.

Samsung é uma marca comercial da SAMSUNG nos Estados Unidos e em outros países.

SonicWALL, Aventail e SonicWALL Mobile Connect são marcas are marcas registradas da SonicWall, Inc.

SOTI e MobiControl são marcas registradas da SOTI Inc. nos Estados Unidos e em outras jurisdições.

Symantec é uma marca comercial ou uma marca registrada da Symantec Corporation ou de suas afiliadas nos Estados Unidos e em outros países.

A marca comercial Symbian é de propriedade da Symbian Foundation Ltd.