

The Kaspersky logo is displayed in a bold, lowercase, sans-serif font. It is positioned within a white, rounded rectangular area that is part of a larger graphic design featuring green and white abstract shapes.

kaspersky

MDM básico no Kaspersky Next Expert View (cloud)

© 2026 AO Kaspersky Lab

Índice

[Ajuda do MDM básico no Kaspersky Next Expert View \(cloud\)](#)

[O que há de novo](#)

[Comparação dos recursos da solução pela ferramenta de gerenciamento](#)

[Operação do Kaspersky Next Expert View \(cloud\)](#)

[Sobre o MDM básico no Kaspersky Next Expert View \(cloud\)](#)

[Sobre o aplicativo Kaspersky Endpoint Security for Android](#)

[Sobre o aplicativo Kaspersky Protection for iOS](#)

[Sobre o plug-in do Kaspersky Mobile Devices Protection and Management](#)

[Requisitos de hardware e software](#)

[Compatibilidade com outros sistemas operacionais](#)

[Problemas conhecidos e considerações](#)

[Guia de Introdução](#)

[A arquitetura da solução](#)

[Definir as configurações do Servidor de Administração para conectar dispositivos móveis](#)

[Cenário: configurar um gateway de conexão para conectar dispositivos móveis ao Kaspersky Next Expert View \(cloud\)](#)

[Adição de uma chave de licença ao repositório do Servidor de Administração](#)

[Implementar um sistema de gerenciamento de dispositivo iOS](#)

[Sobre os modos de operação de dispositivos iOS](#)

[Sobre perfis de gerenciamento](#)

[Implementar o Kaspersky Protection for iOS](#)

[Sobre o Kaspersky Protection for iOS](#)

[Instalação do Kaspersky Protection for iOS](#)

[Ativar o Kaspersky Protection for iOS](#)

[Atualização do Kaspersky Protection for iOS](#)

[Remoção do Kaspersky Protection for iOS](#)

[Implementar um sistema de gerenciamento usando o protocolo MDM do iOS](#)

[Exibir a lista de Servidores de MDM do iOS instalados e definir as respectivas configurações](#)

[Receber ou renovar um Certificado de APNs](#)

[Instalar um Certificado de APNs no Servidor de MDM do iOS](#)

[Eventos do Servidor de MDM do iOS](#)

[Implementar um sistema de gerenciamento de dispositivos Android](#)

[Sobre os modos de operação de dispositivos Android](#)

[Usar o Firebase Cloud Messaging](#)

[Implementar o Kaspersky Endpoint Security for Android](#)

[Sobre o aplicativo Kaspersky Endpoint Security for Android](#)

[Instalação do Kaspersky Endpoint Security for Android](#)

[Instalação manual do Kaspersky Endpoint Security for Android](#)

[Permissões do Kaspersky Endpoint Security for Android](#)

[Iniciar e parar o Kaspersky Endpoint Security for Android](#)

[Ativar o Kaspersky Endpoint Security for Android](#)

[Atualizar o Kaspersky Endpoint Security for Android](#)

[Remover o Kaspersky Endpoint Security for Android](#)

[Permitir que os usuários removam o Kaspersky Endpoint Security for Android](#)

[Remoção do Kaspersky Endpoint Security for Android pelo usuário](#)

[Remoção remota do Kaspersky Endpoint Security for Android](#)

[Gerenciamento de dispositivos móveis no Kaspersky Next Expert View \(cloud\)](#)

[Criação de grupos de administração](#)

[Configurar políticas](#)

[Criar uma política](#)

[Modificar uma política](#)

[Copiar uma política](#)

[Mover uma política para outro grupo de administração](#)

[Visualizar lista de políticas](#)

[Visualizar resultados da distribuição da política](#)

[Gerenciar as revisões de políticas](#)

[Restringir permissões para configurar políticas](#)

[Configurar o controle de acesso baseado em função](#)

[Configurar perfis de política](#)

[Excluir uma política](#)

[Conexão de dispositivos móveis ao Kaspersky Next Expert View \(cloud\)](#)

[Fazer uma conexão direta de dispositivos Android ao Kaspersky Security Center](#)

[Movimentação de dispositivos móveis não atribuídos para grupos de administração](#)

[Ações em dispositivos móveis para fazer a conexão com o Servidor de Administração](#)

[Definir configurações de sincronização](#)

[Gerenciar certificados de dispositivos móveis](#)

[Configurar as regras de emissão do certificado](#)

[Emitir certificados de dispositivos móveis](#)

[Renovar certificados de dispositivos móveis](#)

[Excluir certificados de dispositivos móveis](#)

[Visualizar lista de certificados de dispositivos móveis](#)

[Configuração e gerenciamento](#)

[Controle](#)

[Configurar restrições](#)

[Configurar restrições de dispositivos iOS MDM](#)

[Configurar o acesso do usuário aos sites](#)

[Configurar o acesso aos sites nos dispositivos Android](#)

[Configurar o acesso a sites nos dispositivos iOS MDM do usuário](#)

[Controle de conformidade](#)

[Controle de conformidade de dispositivos Android](#)

[Controle de aplicativos](#)

[Controle de aplicativos em dispositivos Android](#)

[Níveis de proteção de dispositivos móveis](#)

[Inventário de software em dispositivos Android](#)

[Proteção](#)

[Configuração da proteção antimalware em dispositivos Android](#)

[Proteção de dispositivos Android na Internet](#)

[Proteção de dados em um dispositivo perdido ou roubado](#)

[Enviar comandos para um dispositivo móvel perdido ou roubado](#)

[Desbloquear um dispositivo móvel](#)

[Configurar a força da senha de desbloqueio de dispositivo](#)

[Configurar uma senha forte de desbloqueio para um dispositivo Android](#)

[Configurar uma senha forte de desbloqueio para dispositivos iOS MDM](#)

[Configurar uma Rede Privada Virtual \(VPN\)](#)

[Configurar a VPN em dispositivos Android \(somente Samsung\)](#)

[Configurar a VPN em dispositivos iOS MDM](#)

[Configurar o Firewall em dispositivos Android \(somente Samsung\)](#)

[Proteger o Kaspersky Endpoint Security for Android contra a remoção](#)

[Detectar dispositivos invadidos](#)

[Configurar um proxy HTTP global em dispositivos iOS MDM](#)

[Adicionar certificados de segurança aos dispositivos iOS MDM](#)

[Adicionar um perfil SCEP aos dispositivos iOS MDM](#)

[Gerenciamento de dispositivos móveis](#)

[Gerenciar dispositivos Android](#)

[Criar um pacote de aplicativo móvel para dispositivos Android](#)

[Visualizar informações sobre um dispositivo Android](#)

[Desconectar um dispositivo Android do gerenciamento](#)

[Gerenciar dispositivos iOS MDM](#)

[Assinar perfis de gerenciamento com um certificado](#)

[Adicionar um perfil de configuração](#)

[Instalar um perfil de configuração em um dispositivo](#)

[Remover um perfil de configuração de um dispositivo](#)

[Configurar aplicativos gerenciados](#)

[Instalar um aplicativo em um dispositivo móvel](#)

[Atualizar um aplicativo instalado em um dispositivo](#)

[Remover um aplicativo de um dispositivo](#)

[Configurar o roaming em um dispositivo móvel MDM do iOS](#)

[Visualizar informações sobre um dispositivo iOS MDM](#)

[Desconectar um dispositivo iOS MDM do gerenciamento](#)

[Gerenciar configurações dos dispositivos móveis](#)

[Configurar a conexão à rede Wi-Fi](#)

[Conectar dispositivos Android a uma rede Wi-Fi](#)

[Para conectar dispositivos iOS MDM a uma rede Wi-Fi](#)

[Configurar o e-mail](#)

[Configurar uma caixa de e-mail em dispositivos iOS MDM](#)

[Configurar uma caixa de e-mail do Exchange nos dispositivos iOS MDM](#)

[Configurar uma caixa de e-mail do Exchange em dispositivos Android](#)

[Configurar níveis de proteção no Kaspersky Security Center](#)

[Criar um relatório sobre os aplicativos móveis instalados](#)

[Configurar as notificações para o Kaspersky Endpoint Security for Android](#)

[Conectar dispositivos iOS MDM ao AirPlay](#)

[Conectar dispositivos iOS MDM ao AirPrint](#)

[Configurar o nome do ponto de acesso \(APN\)](#)

[Configurar a APN em dispositivos Android \(somente Samsung\)](#)

[Configurar a APN em dispositivos iOS MDM](#)

[Contêiner corporativo](#)

[Sobre contêineres corporativos](#)

[Configurar um contêiner corporativo](#)

[Desbloquear o contêiner corporativo](#)

[Adicionar uma conta LDAP](#)

[Adicionar uma conta de contatos](#)

[Adicionar uma conta de calendário](#)

[Configurar uma assinatura de calendário](#)

[Configurar o SSO](#)

[Gerenciar Clipes da Web](#)

[Adicionar fontes](#)

[Trabalhar com comandos para dispositivos móveis](#)

[Comandos para dispositivos móveis](#)

[Enviar comandos](#)

[Visualizar status de comandos no histórico de comandos](#)

[Participar na Kaspersky Security Network](#)

[Troca de informações com a Kaspersky Security Network](#)

[Ativar e desativar o uso da Kaspersky Security Network](#)

[Samsung Knox](#)

[Configurar o Knox](#)

[Configurar VPN no Knox](#)

[Configurar uma caixa de e-mail do Exchange no Knox](#)

[Configurar APN no Knox](#)

[Configurar Firewall no Knox](#)

[Uso do aplicativo Kaspersky Endpoint Security for Android](#)

[Recursos do aplicativo](#)

[Introdução à janela principal](#)

[Ícone da barra de status](#)

[Verificação do dispositivo](#)

[Executar uma verificação programada](#)

[Alteração do modo de Proteção do dispositivo](#)

[Atualizações do banco de dados antimalware](#)

[Atualização do banco de dados agendada](#)

[O que fazer em caso de perda ou roubo do dispositivo](#)

[Proteção na Web](#)

[Obter certificado](#)

[Sincronizar com o Kaspersky Security Center](#)

[Ativar o aplicativo Kaspersky Endpoint Security for Android sem o Kaspersky Security Center](#)

[Instalar e usar certificados de e-mail e VPN no dispositivo](#)

[Ativar a acessibilidade no Android 13 ou posterior](#)

[Atualizar o aplicativo](#)

[Remover o aplicativo](#)

[Aplicativos com o ícone de maleta](#)

[Aplicativo Knox](#)

[Usar o aplicativo Kaspersky Protection for iOS](#)

[Recursos do aplicativo](#)

[Instalar o aplicativo](#)

[Ativar o aplicativo](#)

[Ativar o aplicativo com um código de ativação](#)

[Introdução à janela principal](#)

[Atualizar o aplicativo](#)

[Usar o diagnóstico para solucionar problemas](#)

[Remover o aplicativo](#)

[Licenciamento do aplicativo](#)

[Sobre o Contrato de Licença de Usuário Final](#)

[Sobre a licença](#)

[Exibir informações de licença](#)

[Sobre a assinatura](#)

[Sobre a chave de licença](#)

[Sobre o código de ativação](#)

[Sobre o arquivo de chave](#)

[Fornecimento de dados no Kaspersky Endpoint Security for Android](#)

[Fornecimento de dados no Kaspersky Protection for iOS](#)

[Contatar o Suporte Técnico](#)

[Como obter suporte técnico](#)

[Suporte técnico pelo Kaspersky CompanyAccount](#)

[Fontes de informação sobre o aplicativo](#)

[Glossário](#)

[Administrador do dispositivo](#)

[Administrador do Kaspersky Security Center](#)

[Agente de Rede](#)

[Arquivo de chave](#)

[Arquivo de manifesto](#)

[Assinatura](#)

[Ativação do aplicativo](#)

[Bancos de dados antimalware](#)

[Categorias da Kaspersky](#)

[Certificado do serviço Apple Push Notification \(APNs\)](#)

[Código de ativação](#)

[Código de desbloqueio](#)

[Contêiner corporativo](#)

[Contrato de Licença de Usuário Final](#)

[Controle básico](#)

[Controle de conformidade](#)

[Dispositivo corporativo](#)

[Dispositivo iOS MDM](#)

[Dispositivo pessoal](#)

[Dispositivo supervisionado](#)

[Estação de trabalho do administrador](#)

[Grupo de administração](#)

[IMAP](#)

[Kaspersky Private Security Network \(KPSN\)](#)
[Kaspersky Security Network \(KSN\)](#)
[Licença](#)
[Malware](#)
[Pacote de instalação](#)
[Pacote de instalação independente](#)
[Perfil de gerenciamento](#)
[Perfil de trabalho do Android](#)
[Período da licença](#)
[Phishing](#)
[Plug-in de gerenciamento móvel](#)
[Política](#)
[POP3](#)
[Proteção básica](#)
[Quarentena](#)
[Servidor de Administração](#)
[Servidor de Administração virtual](#)
[Servidor de MDM do iOS](#)
[Servidor proxy](#)
[Servidor Web do Kaspersky Security Center](#)
[Servidores de atualização da Kaspersky](#)
[Solicitação de assinatura do certificado](#)
[SSL](#)
[Tarefa de grupo](#)
[Informação sobre código de terceiros](#)
[Avisos de marca registrada](#)

Ajuda do MDM básico no Kaspersky Next Expert View (cloud)

 O que há de novo Descubra o que há de novo na versão mais recente da solução.	 Configurar a proteção do dispositivo Gerencie a proteção de dispositivos móveis remotamente. Os recursos incluem Antimalware, Proteção na Web, Antirroubo e muito mais.
 Implementação Saiba como implementar a solução em sua organização e configurar sistemas de gerenciamento para dispositivos Android e iOS.	 Definir configurações do dispositivo Gerencie dispositivos móveis remotamente: configure Wi-Fi, e-mail, Web Clips e muito mais.
 Comandos Gerencie remotamente dispositivos móveis com comandos para dispositivos móveis. Bloquear dispositivo, Limpar os dados corporativos, Localizar o dispositivo, Tirar fotos, Alarme sonoro e muito mais.	 Configurar o controle de dispositivos Monitore dispositivos móveis remotamente, incluindo a configuração de restrições, acesso do usuário a sites, Controle de conformidade, Controle de aplicativos e muito mais.
 Contêiner corporativo Descubra os benefícios do contêiner corporativo e saiba como configurá-lo para o seu dispositivo.	 Corporate App Catalog Crie um Corporate App Catalog personalizado e use um navegador para baixar aplicativos do catálogo nos dispositivos dos usuários.

O que há de novo

Versão 1.0

Nesta versão, adicionamos novos recursos ao plug-in do Kaspersky Mobile Devices Protection and Management para o Kaspersky Next Expert View (cloud):

- A interface do plug-in do Kaspersky Mobile Devices Protection and Management agora oferece suporte a novos idiomas:
 - Espanhol (México)
 - Português (Brasil)
- Correções de bugs e melhorias gerais.

Comparação dos recursos da solução pela ferramenta de gerenciamento

Disponibilidade de recursos por ferramenta de gerenciamento

Funcionalidade	Kaspersky Security Center Web Console		Kaspersky Security Center Web Console		Kaspersky Security Center Cloud Console	
	MDM avançado no Kaspersky Next Expert View (on-premise)	Kaspersky Secure Mobility Management (on-premise)	MDM básico no Kaspersky Next Expert View (on-premise)	Kaspersky Security para dispositivos móveis (on-premise)	MDM básico no Kaspersky Next Expert View (cloud)	Kaspersky Security para dispositivos móveis (cloud)
Gerenciamento de dispositivos móveis						
Gerenciamento de dispositivos Android	✓		✓		✓	
Gerenciamento de dispositivos iOS	✓		✓		✓	
Proteção de dispositivo Aurora	✓		—		—	
Implementação						
Adicionar dispositivos usando um link da App Store	✓		✓		✓	
Adicionar dispositivos criando um pacote de instalação	✓		✓		—	
Adicionar dispositivos diretamente ao grupo de administração após a conexão dos dispositivos	✓		✓		✓	
Criar políticas divididas por modos de operação	✓		✓		—	
Enviar comandos para dispositivos móveis	✓		✓		✓ Conjunto limitado de comandos	
Remover dispositivos móveis do Kaspersky Security Center	✓		✓		✓	
Gerenciamento de certificados						
Emissão de certificados de e-mail	✓		✓		✓ A definição das configurações de emissão não está disponível	
Emissão de certificados VPN	✓		✓		✓ A definição das configurações de emissão não está disponível	
Emitir certificados de dispositivos móveis	✓		✓		✓	
Emitir certificados de dispositivos móveis por meio das ferramentas do Servidor de Administração	✓		✓		✓	
Especificação de arquivos do certificado	✓		✓		✓	
Integração com a infraestrutura de chaves públicas (PKI)	✓		✓		—	

Gerenciamento de políticas			
Acesso baseado em função para configurar políticas de grupo	✓	✓	✓
Configuração de sincronização do dispositivo móvel com o Kaspersky Security Center	✓	✓	✓
Configuração de verificações de malware em dispositivos móveis	✓	✓	✓
Configuração de atualizações do banco de dados antimalware	✓	✓	✓
Configuração de proteção do dispositivo na Internet	✓	✓	✓
Configuração da proteção de dados de dispositivos perdidos ou roubados	✓	✓	✓
Configuração da força da senha de desbloqueio	✓	✓	✓
Configurar o acesso dos usuários a sites	✓	✓	✓
Configuração do Controle de aplicativos	✓	✓ Somente para Android	✓ Somente para Android
Configuração do Controle de conformidade	✓	✓ Somente para Android	✓ Somente para Android
Configuração de regras de concessão de permissão para aplicativos instalados	✓	—	—
Configuração de contêineres corporativos	✓	✓ Conjunto limitado de configurações	✓
Configuração de restrições de funções do dispositivo	✓	✓ Conjunto limitado de configurações	✓
Configuração de conexão a redes Wi-Fi	✓	✓	✓
Configuração de VPN	✓	✓ Para iOS, não há suporte para Per App VPN nem para o protocolo IKEv2. Para Android, a VPN só pode ser configurada via Knox.	✓ Para iOS, não há suporte para Per App VPN nem para o protocolo IKEv2. Para Android, a VPN só pode ser configurada via Knox.
Gerenciamento de configurações do aplicativo	✓	—	—
Envio de arquivos a dispositivos Android	✓	—	—
Samsung Knox	✓	✓ Conjunto limitado de configurações	✓
Controle remoto para Android	✓	—	—
Recursos do Servidor de MDM do iOS			

Instalar e configurar o Servidor de MDM do iOS	✓	✓	✓ Somente configuração aplicável
Atualização e remoção do Servidor de MDM do iOS	✓	✓	—
Emitir certificados de APNs	✓	✓	✓
Conectar dispositivos iOS MDM	✓	✓	✓
Assinar um perfil de gerenciamento do dispositivo por um certificado	✓	✓	✓
Eventos do Servidor de MDM do iOS	✓	✓	✓
Adicionar um perfil de configuração	✓	✓	✓
Outros recursos			
Aceitação global do EULA no Kaspersky Security Center	✓	✓	✓
Configurar a Kaspersky Private Security Network	✓	✓	—

Operação do Kaspersky Next Expert View (cloud)

Esta seção de ajuda descreve a proteção e o gerenciamento de dispositivos móveis usando o Kaspersky Next Expert View (cloud).

Sobre o MDM básico no Kaspersky Next Expert View (cloud)

O MDM básico no Kaspersky Next Expert View (cloud) é uma solução integrada para proteção e gerenciamento de dispositivos móveis corporativos, além de dispositivos móveis pessoais usados por profissionais da empresa para fins corporativos.

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 Kaspersky Endpoint Security for Android inclui os seguintes recursos:

- **Antimalware.** O componente detecta e neutraliza as ameaças no dispositivo utilizando os bancos de dados antimalware e o serviço da Kaspersky Security Network na nuvem. O Antimalware inclui os seguintes componentes:
 - **Proteção.** Detecta ameaças em arquivos abertos, verifica novos aplicativos e previne a infecção do dispositivo em tempo real.
 - **Verificação.** Iniciada sob demanda para todo o sistema de arquivos, somente para aplicativos instalados ou somente para um arquivo ou pasta selecionado.
 - **Atualização.** Permite baixar novos bancos de dados antimalware para o aplicativo.
- **Antirroubo.** Este componente protege as 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 o dispositivo.** Obtém as coordenadas da localização do dispositivo.
 - **Alarme sonoro.** Faz com que o dispositivo acione o disparo de um alarme sonoro.
 - **Limpar os dados corporativos.** Elimina os dados corporativos para proteger a confidencialidade das informações corporativas.

- **Proteção na Web e Controle da Web.** A Proteção na Web bloqueia sites maliciosos projetados para disseminar códigos maliciosos. A Proteção na Web também bloqueia sites falsos (de phishing) projetados para roubar dados confidenciais do usuário (por exemplo, senhas de bancos on-line ou sistemas de dinheiro eletrônico) e acessar as informações financeiras do usuário. A Proteção na Web usa o serviço na nuvem da Kaspersky Security Network para verificar os sites antes que eles sejam abertos. Após a verificação, a Proteção na Web permite que os sites confiáveis sejam carregados e bloqueia sites maliciosos. O Controle da Web permite filtrar 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, como Jogos de azar, loterias, apostas ou Comunicações via Internet.
- **Controle de aplicativos.** Este componente permite instalar aplicativos recomendados e necessários em um dispositivo Android, bem como remover aplicativos bloqueados que violam os requisitos de 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 Next Expert View (cloud) definindo as [configurações das políticas](#) correspondentes.

Sobre o aplicativo Kaspersky Protection for iOS

O aplicativo Kaspersky Protection for iOS garante a proteção dos dispositivos móveis contra phishing e ameaças da Web.

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

- **Proteção na Web.** Esse componente bloqueia sites maliciosos projetados para disseminar 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. É possível configurar esse componente no Kaspersky Next Expert View (cloud) ao definir as configurações das políticas de grupo.
- **Detecção de jailbreak.** Quando o Kaspersky Protection for iOS detecta um jailbreak, ele exibe uma mensagem crítica e informa o usuário sobre o problema.

Sobre o plug-in do Kaspersky Mobile Devices Protection and Management

O plug-in do Kaspersky Mobile Devices Protection and Management permite gerenciar dispositivos móveis e aplicativos móveis, instalados neles, pelo Kaspersky Next Expert View (nuvem). O plug-in do Kaspersky Mobile Devices Protection and Management pode ser usado para:

- Criar políticas de segurança do grupo para dispositivos móveis.
- Definir remotamente as configurações do aplicativo 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.
- Configurar remotamente dispositivos iOS conectados usando o protocolo MDM do iOS (aqui referidos como "dispositivos iOS MDM") e dispositivos iOS com o aplicativo Kaspersky Protection for iOS.

O plug-in do Kaspersky Mobile Devices Protection and Management pode ser instalado ao configurar o Kaspersky Next Expert View (cloud).

Requisitos de hardware e software

Esta seção lista os requisitos de hardware e software para os sistemas operacionais de dispositivos móveis compatíveis com o MDM básico no Kaspersky Next Expert View (cloud).

Requisitos de hardware e software para o Kaspersky Endpoint Security for Android

Para o Kaspersky Endpoint Security for Android, o dispositivo móvel deve atender aos seguintes requisitos:

- 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
- Sistema operacional (exceto Go Edition):
 - Android 5.x (Lollipop)
 - Android 6.x (Marshmallow)
 - Android 7.x (Nougat)
 - Android 8.x (Oreo)
 - Android 9
 - Android 10
 - Android 11

- Android 12, 12L
- Android 13
- Android 14
- Android 15
- Android 16
- Arquitetura do processador x86, x86-64, Arm5, Arm6, Arm7 ou Arm8
- O aplicativo só pode ser instalado na memória principal do dispositivo

Requisitos de hardware e software para o Kaspersky Protection for iOS

Para o Kaspersky Protection for iOS, o dispositivo móvel deve atender aos seguintes requisitos:

- Sistema operacional:
 - iOS:
 - iOS 15.x
 - iOS 16.x
 - iOS 17.x
 - iOS 18.x
 - iOS 26, 26.1, 26.2, 26.3, 26.4 e 26.5
 - iPadOS:
 - iPadOS 15.x
 - iPadOS 16.x
 - iPadOS 17.x
 - iPadOS 26.2 e 26.4
- Conexão com a Internet

Requisitos de hardware e software para um perfil de gerenciamento

Para um perfil de gerenciamento, o dispositivo móvel deve atender aos seguintes requisitos:

- Sistema operacional:
 - iOS:
 - iOS 10.x
 - iOS 11.x
 - iOS 12.x
 - iOS 13.x
 - iOS 14.x
 - iOS 15.x
 - iOS 16.x
 - iOS 17.x
 - iOS 18.x
 - iOS 26, 26.1, 26.2, 26.3, 26.4 e 26.5
 - iPadOS:
 - iPadOS 13.x
 - iPadOS 14.x
 - iPadOS 15.x
 - iPadOS 16.x
 - iPadOS 17.x
 - iPadOS 26.2 e 26.4
- Conexão com a Internet

Compatibilidade com outros sistemas operacionais

O MDM básico no Kaspersky Next Expert View (cloud) é compatível com a proteção e o gerenciamento de dispositivos móveis que executam outros sistemas operacionais usando o aplicativo Kaspersky Endpoint Security for Android.

A tabela descreve a compatibilidade das versões do aplicativo Kaspersky Endpoint Security for Android com outras versões do sistema operacional.

Versão do Kaspersky Endpoint Security for Android	Operating system version	Limitações:
10.571.37	kvadraOS 1.26 (Enterprise)	Problemas conhecidos e considerações

Problemas conhecidos e considerações

Os seguintes problemas conhecidos não são críticos para a operação da solução.

Problemas conhecidos ao conectar dispositivos móveis ao Kaspersky Security Center

- O link para conectar dispositivos móveis ou o link para baixar o pacote de instalação na porta HTTPS 8061 do Servidor Web pode não abrir no mesmo navegador que o Kaspersky Security Center Web Console devido ao erro `NET::ERR_CERT_AUTHORITY_INVALID`. Isso pode acontecer se o Servidor Web usar um certificado autoassinado. Para abrir o link, copie-o e cole-o em um navegador diferente ou substitua o certificado autoassinado por um certificado personalizado emitido pela autoridade do certificado confiável nas propriedades do Servidor de Administração, na guia **Geral**, na seção **Servidor Web**.

Problemas conhecidos ao gerenciar dispositivos móveis

- Se você editar os campos **Nome** e **Descrição** na guia **Geral** das propriedades do dispositivo, as alterações não serão exibidas na lista de dispositivos móveis conectados ao Kaspersky Security Center devido a limitações técnicas.
- O botão [Forçar a sincronização](#) e a caixa de seleção [Não desconectar do Servidor de Administração](#) na janela de propriedades do dispositivo não são compatíveis com dispositivos móveis. Use o comando [Sincronizar o dispositivo](#) para forçar a sincronização de um dispositivo Android ou um dispositivo iOS MDM.
- Na lista de dispositivos móveis gerenciados, a capacidade total de armazenamento exibida de dispositivos iOS pessoais que operam no modo "Kaspersky Protection for iOS" é arredondada para cima.

Problemas conhecidos do Kaspersky Protection for iOS

- O aplicativo Kaspersky Protection for iOS não opera corretamente quando um cliente da VPN com uma conexão VPN ativa está sendo executado no mesmo dispositivo móvel.
- Para uma operação estável do aplicativo Kaspersky Protection for iOS, o aplicativo desatualizado Kaspersky Security for iOS deve ser desinstalado do dispositivo.
- Em alguns dispositivos iOS, as tarefas em segundo plano como [a sincronização com o Kaspersky Security Center](#) ou [a substituição da chave de ativação](#) podem ser executadas depois do que o esperado se o usuário encerrar o Kaspersky Protection for iOS deslizando para cima no Seletor de Apps. Isso ocorre devido aos [limites de execução em segundo plano do iOS](#). Para forçar a execução, reabra o aplicativo.

Para aumentar as chances de que as tarefas em segundo plano sejam executadas, assegure-se do seguinte:

- O aplicativo Kaspersky Protection for iOS está aberto no Seletor de Apps.
- O Modo de dados reduzidos está desativado e o dispositivo está conectado a uma rede Wi-Fi ou a um ponto de acesso.

- O dispositivo está conectado a uma rede de alta qualidade.
- O dispositivo está carregando.
- O Hotspot pessoal está desativado.

Problemas conhecidos ao instalar o Kaspersky Endpoint Security for Android

- O Kaspersky Endpoint Security for Android somente é instalado na memória principal do dispositivo.
- Em dispositivos que executam Android 7, 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 a 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 sem conectar ao Kaspersky Security Center, somente os componentes Antimalware e Proteção na Web estarão disponíveis. O administrador pode definir as configurações de Antimalware 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).
- Em dispositivos pessoais e dispositivos com contêiner corporativo executando o Android 15, os usuários podem criar seu próprio espaço privado. O Kaspersky Endpoint Security for Android não pode verificar aplicativos, fotos e outros arquivos armazenados em espaços privados. A Proteção na Web, o Controle da Web e o Controle de aplicativos não funcionam para aplicativos instalados em espaços privados. Não há suporte para a instalação do Kaspersky Endpoint Security for Android em um espaço privado.

Problemas conhecidos ao atualizar o Kaspersky Endpoint Security for Android

- 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 ao remover o Kaspersky Endpoint Security for Android

- Antes de remover o Kaspersky Endpoint Security for Android do dispositivo, desmarque a caixa de seleção **Bloquear aplicativos do sistema** nas configurações de [Controle de Aplicativos](#) da política ou desative o Controle de aplicativos.

Problemas conhecidos que afetam o Wi-Fi

- Em dispositivos iOS MDM, se você desativar a conexão automática a uma rede Wi-Fi existente nas configurações de política, não poderá ativar a conexão automática a essa rede novamente. Isso se deve a um problema conhecido pela Apple.
- Em dispositivos iOS MDM executando o iOS 18 e o iOS 26, se o tipo de proteção de **Rede pessoal (qualquer)** for selecionado nas configurações da política de [Wi-Fi](#), o dispositivo talvez não seja conectado automaticamente a uma rede Wi-Fi protegida por protocolo WEP ou WPA, mesmo se a caixa de seleção **Conectar automaticamente** estiver marcada. Para conectar-se automaticamente a uma rede Wi-Fi protegida por um protocolo necessário, especifique esse protocolo como o tipo de segurança da rede.

Problemas conhecidos que afetam o Antimalware

- Devido a 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 esses arquivos sem notificar que eles foram ignorados.
- Para a análise adicional de um dispositivo quanto a novas ameaças cujas informações ainda não foram adicionadas aos bancos de dados antimalware, 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, contendo 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 antimalware do Servidor de Administração em um dispositivo móvel pode falhar. Nesse caso, execute a tarefa de atualização do banco de dados antimalware 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 malware em tais dispositivos.
- Em dispositivos executando Android 11 ou posterior, o aplicativo Kaspersky Endpoint Security for Android não pode verificar as pastas "Android/data" e "Android/obb" para detectar malware [devido a limitações técnicas](#).
- Em dispositivos com Android 11 ou posterior, o usuário deve conceder a permissão "Permitir acesso para gerenciar todos os arquivos".
- Em dispositivos que executam o Android 7 ou posterior, a janela de configuração do agendamento da execução da verificação de malware pode ser exibida incorretamente (os elementos de gerenciamento não aparecem). Esta falha é causada por um [defeito bem conhecido no Android 7](#).
- Em dispositivos que executam Android 7, 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, 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 Antimalware quando o arquivo for executado ou durante uma verificação de malware do dispositivo. Esta falha é causada por um [defeito bem conhecido no Android 6](#). Para assegurar a segurança do dispositivo, recomenda-se configurar verificações de malware programadas.

Problemas conhecidos que afetam a Proteção na Web e o Controle da Web

- O Controle da Web em dispositivos Android é compatível apenas com Google Chrome, HUAWEI Browser, Samsung Internet e Yandex Browser.
- O recurso Guias personalizadas é compatível com Google Chrome, Navegador HUAWEI e Samsung Internet.
- O Controle da Web para os navegadores HUAWEI, Samsung Internet e Yandex não bloqueia sites em um dispositivo móvel se um contêiner corporativo for usado e a Proteção na Web estiver ativada somente para o contêiner corporativo.
- Para que a Proteção na Web e o Controle da Web funcionem, você deve ativar o uso da Kaspersky Security Network. O Controle da Web bloqueia os sites com base nos dados da KSN sobre a reputação e a categoria de sites.
- Os sites proibidos podem permanecer desbloqueados pelo Controle da Web em dispositivos que executam o Android 6 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 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 e do Controle da Web.
- Em alguns dispositivos Xiaomi, as permissões "Exibir janela pop-up" e "Exibir janelas pop-up durante a execução em segundo plano" devem ser concedidas para que a Proteção na Web e o Controle da Web funcionem.
- Os sites permitidos podem ser bloqueados no navegador Samsung Internet no modo de Controle da Web **Permitir apenas os sites listados** quando a página for atualizada. Os sites são bloqueados caso uma expressão regular contenha configurações avançadas (por exemplo, `^https?://example.com/pictures/`). Recomenda-se o uso de expressões regulares sem configurações adicionais (por exemplo, `^https?://example.com`).

- Caso o Controle da Web esteja definido para **Proibir todos os sites**, o Kaspersky Endpoint Security for Android não bloqueia a pesquisa no widget de pesquisa do Google. Em vez disso, ele bloqueia o acesso do usuário aos resultados da pesquisa.
- Em um contêiner corporativo, se o Controle da Web estiver definido para **Proibir todos os sites**, o Kaspersky Endpoint Security for Android recarrega infinitamente a página inicial do Google Chrome, bloqueia o navegador e interfere no dispositivo.
- No Yandex Browser e no Samsung Internet, URLs maliciosas e de phishing podem permanecer sem bloqueio. Isso ocorre porque somente o domínio do site é verificado. Se for um domínio malicioso ou de phishing, a Proteção na Web bloqueará a ameaça. Se o domínio não for classificado como malicioso ou de phishing, a URL específica não será bloqueada.
- A lista de sites permitidos criados no cartão do **Controle da Web** não é exibida no Safari em dispositivos iOS MDM executando iOS 26 ou anterior. No entanto, o Controle da Web ainda estará funcionando e os usuários poderão acessar somente sites permitidos. Para exibir os sites permitidos no Safari, marque a caixa de seleção **Adicionar aos favoritos no dispositivo** no cartão do **Controle da Web** e especifique o nome do marcador para cada site da lista.
- Se a opção **Verificar o URL inteiro ao utilizar Guias personalizadas** estiver ativada na seção de configurações da política do Controle da Web, mudar para a versão completa dos navegadores compatíveis só funcionará para sites de phishing e maliciosos.
- Em dispositivos iOS que operam com o modo "Kaspersky Protection for iOS", ao alterar o idioma ou reiniciar o dispositivo, a Proteção na Web é desativada. Para ativar a Proteção na Web, depois de alterar o idioma ou reiniciar o dispositivo, aguarde cerca de um minuto e abra o Kaspersky Protection for iOS.

Problemas conhecidos que afetam o 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 um administrador do dispositivo.
- Para bloquear dispositivos que executam o Android 7 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 ou posterior, o usuário deve conceder a permissão "Permitir o tempo todo" para a localização do dispositivo.

Problemas conhecidos que afetam o 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 causar problemas na operação do dispositivo.
- Em dispositivos iOS MDM, caso seja especificado que os aplicativos na lista de permissão possam ser instalados, todos os aplicativos exceto os aplicativos do sistema e aqueles adicionados na lista de aplicativos permitidos, ficarão ocultos na tela do dispositivo.
- Em alguns dispositivos pessoais HUAWEI e Honor, aplicativos permitidos podem ser bloqueados, e aplicativos proibidos podem permanecer desbloqueados. Isso ocorre porque a categoria de alguns aplicativos da App Gallery não pode ser definida corretamente.
- Em alguns dispositivos Samsung e Oppo, os ícones de aplicativos podem permanecer ocultos na tela de Início depois de desmarcar a caixa de seleção **Bloquear aplicativos do sistema**. Isso acontece devido a limitações do sistema operacional Android.
- Ao configurar um contêiner corporativo no dispositivo, recomendamos desmarcar a caixa de seleção **Bloquear aplicativos do sistema**. O bloqueio de aplicativos do sistema pode causar problemas para a criação do contêiner corporativo.
- Se a caixa de seleção **Bloquear aplicativos do sistema** estiver marcada, dentre os aplicativos do sistema, o mecanismo do sistema para solicitar permissões do aplicativo pode estar bloqueado. Se você quiser desbloquear esse mecanismo, localize o nome dele (por exemplo, `com.google.android.permissioncontroller`) no log de eventos e adicione-o às exceções.

Problemas conhecidos ao gerenciar certificados

- Um novo certificado de dispositivos móveis, VPN ou e-mail para outro usuário não pode ser instalado em um dispositivo móvel se o respectivo dispositivo já tiver o certificado de dispositivos móveis para um usuário atual instalado. No entanto, novos certificados para o usuário atual podem ser [emitidos](#).

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

- Para dispositivos com Android 10 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 sequências repetidas ou ordenadas (por exemplo, 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 pelo menos 8 dígitos. A senha deve ter pelo menos 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](#). Nesse caso, use apenas o aplicativo do sistema Configurações para alterar a senha de desbloqueio.
- Em alguns dispositivos que executam o Android 6 ou posterior, se os dados do dispositivo estiverem com criptografados, um erro pode ocorrer quando a senha de desbloqueio da tela é inserida. Este problema é relacionado aos recursos específicos do serviço de Acessibilidade com firmware MIUI.
- Em alguns dispositivos iOS MDM, se o valor **Número mínimo de caracteres especiais** for especificado e a caixa de seleção **Permitir senha simples** estiver marcada, o dispositivo exibirá informações sobre como definir uma senha de 6 ou mais caracteres, mesmo que seja possível definir uma senha de 4 ou mais caracteres.

Problemas conhecidos que afetam a proteção contra remoção do Kaspersky Endpoint Security for Android

- O Kaspersky Endpoint Security for Android deve ser definido como um administrador do dispositivo.
- Para proteger o aplicativo da remoção em dispositivos que executam o Android 7 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 for Android 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 que executam o Android 10 ou posterior, a proibição do uso de redes Wi-Fi não é compatível.
- Em dispositivos que executam Android 11 ou posterior, o Kaspersky Endpoint Security for Android deverá ser definido como um recurso de acessibilidade. O Kaspersky Endpoint Security for Android solicita ao usuário definir o aplicativo como um recurso de acessibilidade pelo assistente de configuração inicial. O usuário pode ignorar esta etapa ou desativar esse serviço posteriormente nas configurações do dispositivo. Se este for o caso, não será possível restringir o uso da câmera.
- Em dispositivos iOS MDM, os usuários podem ativar os resultados da pesquisa na Internet do Spotlight em Sugestões da Siri, mesmo se a caixa de seleção **Proibir sugestões do Spotlight** estiver marcada. Isso se deve a um problema conhecido pela Apple.
- Em dispositivos Android, quando o uso da câmera é restrito, alguns aplicativos podem ser fechados automaticamente. Esse problema ocorre porque serviços e recursos, como o Android System Intelligence e o Screen Attention, utilizam a câmera do dispositivo para manter a tela ativada enquanto o usuário está olhando para ela.

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 dentro de 30 minutos. Caso contrário, o comando **Localizar o dispositivo** falhará.
- O comando **Localizar o dispositivo** não funciona em dispositivos Android se a opção Precisão de localização do Google estiver desativada nas configurações. Observe que nem todos os dispositivos Android vêm com essa configuração de localização.
- O comando **Redefinir as configurações padrão** não está disponível para dispositivos pessoais e dispositivos com contêiner corporativo executando o Android 14 ou posterior.

Problemas conhecidos que afetam dispositivos específicos

- Em certos dispositivos (por exemplo, HUAWEI, Meizu e Xiaomi), você deve conceder a 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 de executar todas as suas funções depois que o dispositivo móvel é reiniciado.
 - Se o dispositivo estiver bloqueado, você não poderá usar um comando para desbloqueá-lo. Você somente pode desbloquear o dispositivo ao usar um código de desbloqueio de uso único.
 - Em dispositivos com Xiaomi HyperOS, o Kaspersky Endpoint Security for Android pode não conseguir [verificar notificações de aplicativos de mensagens](#) em busca de URLs maliciosas ou de phishing.
- Em determinados dispositivos (por exemplo, Meizu e Asus), a execução do Android 6 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 que executam o Android 5.X, após o Kaspersky Endpoint Security for Android ser definido como um recurso de Acessibilidade, o dispositivo pode exibir uma mensagem incorreta sobre a falta de direitos suficientes. 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 encerrar manualmente o aplicativo. Nesse caso, o dispositivo do usuário fica desprotegido. 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, o usuário pode ocultar a notificação sobre o 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, 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 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 e o Controle da Web não podem ser ativados 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 desse fornecedor fornecem privilégios elevados para o aplicativo Telas recentes personalizado. 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 Google Pixel que executam Android 11 ou anterior, o aplicativo Kaspersky Endpoint Security for Android trava imediatamente após ser iniciado. Isto é causado por um [problema no Android](#).
- No HUAWEI P60 Pro, um contêiner corporativo não pode ser criado.
- Em alguns dispositivos iOS MDM no modo de operação "Perfil de gerenciamento" que executam o iOS 18.2 a iOS 18.3.1, o uso do Safari talvez seja proibido. Isso se deve a um problema conhecido pela Apple.

- Em determinados dispositivos pessoais (por exemplo, OnePlus, Honor) que executam Android 10 ou posterior, uma senha poderá ser solicitada ao conectar-se a redes Wi-Fi protegidas pelo protocolo WPA2 PSK. Isso ocorre devido a alguns problemas com a forma como a [API de sugestão](#) funciona.
- Em dispositivos iOS MDM que executam o iOS 18.0, uma política com o [AirPlay](#) configurado não pode ser entregue ao dispositivo. Isso se deve a um problema conhecido pela Apple. Para garantir a operação adequada, atualize o iOS no dispositivo.

Problemas conhecidos que afetam o aplicativo no Android 13

- No Android 13, o usuário pode usar o Gerenciador de Tarefas em primeiro plano para impedir que o Kaspersky Endpoint Security seja executado em segundo plano. Isso é causado por um [problema no Android 13](#) bem conhecido.
- No Android 13, a permissão para enviar notificações é solicitada no início da configuração inicial do aplicativo. Isso acontece devido a detalhes do sistema operacional Android 13.

Problemas conhecidos que afetam os perfis da política

- Se você mudar para uma licença com funcionalidade básica, as configurações que estão disponíveis somente com uma licença com funcionalidade estendida não são redefinidas para os padrões nos perfis da política.

Problemas conhecidos no controle de acesso baseado em função

- Se o direito de gerenciamento de Chaves de licença não for concedido, pode ocorrer um erro ao abrir uma política existente. Isso não afeta a operação da política.
- Se o direito de gerenciamento de Chaves de licença não foi concedido, você poderá criar uma política sem escolher a licença no assistente de política móvel. No entanto, você não poderá definir as configurações da política.

Problemas conhecidos ao definir as configurações do Servidor Web no gateway de conexão (Agente de Rede para Linux)

- Ao definir as configurações do Servidor Web em um gateway de conexão, se as portas forem modificadas ou os certificados forem emitidos ou reemitidos, pode levar algum tempo para que as novas configurações sejam sincronizadas com o Kaspersky Security Center. Aguarde até 15 minutos ou clique em **Forçar a sincronização** na guia **Geral** das propriedades do host do gateway de conexão (**Gerenciamento de ativos** → **Ativos (dispositivos)**).
- Ao configurar um certificado de Servidor Web personalizado, se os endereços nos campos **Endereço do servidor Web** e **Endereço do certificado** não corresponderem, um erro será exibido. Nesse caso, para salvar as configurações, você precisa carregar um certificado diferente. No entanto, se você alterar o endereço do Servidor Web nas propriedades do ponto de distribuição do Kaspersky Security Center, e o certificado permanecer o mesmo, ainda poderá salvar essas configurações, mesmo se os endereços não corresponderem.

Problemas conhecidos ao migrar do Kaspersky Security Center Windows para o Kaspersky Security Center Linux

- Ao migrar as configurações do Servidor de MDM do iOS do Kaspersky Security Center Windows 14.2 para o Kaspersky Security Center Linux, as configurações de notificação e armazenamento dos eventos do Servidor de MDM do iOS não são transferidas e assumem os valores padrão. Após a migração, você precisará especificar os valores necessários manualmente.
- Se um usuário tiver sido excluído ou estiver faltando no servidor durante a migração, o certificado de dispositivos móveis será exibido na lista de certificados sem o nome de usuário.

Problemas conhecidos que afetam o Servidor de MDM do iOS

- Pode levar pelo menos seis horas para que o certificado do Servidor de MDM do iOS de reserva seja entregue ao dispositivo.

Problemas conhecidos que afetam eventos

- Depois de atualizar o plug-in do Kaspersky Mobile Devices Protection and Management, novos eventos podem ser exibidos de maneira incorreta em uma política criada anteriormente: na guia **Configuração de eventos**, os eventos aparecem ativados, mas as informações sobre eles não são transmitidas. Para assegurar que o plug-in atualizado forneça uma lista atualizada de eventos para uma política criada anteriormente, você deve salvar novamente a política.

Guia de Introdução

Esta seção é destinada não só aos especialistas que instalam a solução MDM básico no Kaspersky Next Expert View (cloud), mas também aos especialistas que fornecem Suporte Técnico a organizações que usam o MDM básico no Kaspersky Next Expert View (cloud).

A arquitetura da solução

O MDM básico no Kaspersky Next Expert View (cloud) inclui os seguintes componentes:

- Aplicativo móvel Kaspersky Endpoint Security for Android
O aplicativo protege dispositivos Android contra ameaças da Web, vírus e outros aplicativos que representam ameaças.
- Aplicativo móvel Kaspersky Protection for iOS
O aplicativo protege dispositivos iOS contra phishing e ameaças da Web, além de permitir a detecção de jailbreak nos dispositivos.
- Plug-in do Kaspersky Mobile Devices Protection and Management
O plug-in permite gerenciar dispositivos com Android e iOS no Kaspersky Next Expert View (cloud).

- Servidor de MDM do iOS

O Servidor de MDM do iOS permite conectar dispositivos iOS ao Servidor de Administração e gerenciar dispositivos iOS.

- Plug-in de configurações do Servidor de MDM do iOS

O plug-in permite definir as configurações do Servidor de MDM do iOS.

Definir as configurações do Servidor de Administração para conectar dispositivos móveis

Antes de conectar dispositivos móveis ao Kaspersky Next Expert View (cloud), é preciso definir as configurações de conexão nas propriedades do Servidor de Administração.

Para definir as configurações do Servidor de Administração para conectar dispositivos móveis:

1. Na janela principal do Kaspersky Next Expert View (cloud), clique no nome do Servidor de Administração.
2. Na janela de propriedades do Servidor de Administração que se abre, configure a porta do Servidor de Administração que será usada por dispositivos móveis:
 - a. Na guia **Geral**, selecione a seção **Portas adicionais**.
 - b. Mude o botão **Abrir porta para dispositivos móveis** para a posição ativado.

Se esta opção estiver ativada, a porta para dispositivos móveis será aberta no Servidor de Administração.
 - 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.
3. Caso necessário, edite o certificado a ser usado pelos dispositivos móveis para se conectar com o Servidor de Administração.

Por padrão, o Servidor de Administração usa o certificado criado depois que a porta para dispositivos móveis é aberta. É possível reemitir ou substituir o certificado emitido pelo Servidor de Administração por outro certificado.

Para editar o certificado:

a. Na guia **Geral**, selecione a seção **Certificados**.

b. Defina as configurações necessárias.

Para obter mais detalhes sobre como trabalhar com certificados no Kaspersky Security Center Linux, consulte a [Ajuda do Kaspersky Security Center](#).

4. Clique em **Salvar** para salvar as alterações feitas e saia da janela de propriedades do Servidor de Administração.

As configurações de conexão do dispositivo móvel estão definidas.

Cenário: configurar um gateway de conexão para conectar dispositivos móveis ao Kaspersky Next Expert View (cloud)

Um gateway de conexão é o Agente de Rede operando em um modo especial. O Agente de Rede é um componente do Kaspersky Security Center que permite a interação entre o Servidor de Administração e os aplicativos da Kaspersky. Um gateway de conexão recebe conexões de outros Agentes de Rede e as canaliza para o Servidor de Administração por meio de sua própria conexão com o Servidor.

Ao contrário de um Agente de Rede comum, um gateway de conexão pode ser configurado para aguardar por conexões do Servidor de Administração, em vez de estabelecer as conexões com ele. Um gateway de conexão na DMZ recebe conexões do Servidor de Administração por meio da porta TLS 13000. Como um gateway de conexão na DMZ não pode alcançar as portas do Servidor de Administração, o Servidor de Administração cria e mantém uma conexão de sinal permanente com um gateway de conexão. A conexão de sinal não é usada para transferência de dados, mas apenas para enviar um convite para interação de rede. Quando um gateway de conexão precisa se conectar ao Servidor de Administração, ele notifica o Servidor por meio dessa conexão de sinal e, em seguida, o Servidor estabelece a conexão necessária para a transferência de dados.

Um gateway de conexão permite usar os recursos de segurança com mais eficiência para proteger a infraestrutura de rede contra possíveis vulnerabilidades.

- Usar um gateway de conexão facilita o monitoramento de atividades suspeitas em um nó de rede separado fora de uma LAN (área de rede local). Ele ajuda a evitar ataques maliciosos diretos por meio de um protocolo móvel, implementando um protocolo diferente para comunicações entre o gateway de conexão e o Kaspersky Security Center.
- A quantidade de possíveis ataques de rede é menor, pois um gateway de conexão recebe conexões do Servidor de Administração por meio de uma única porta (por padrão, 13000), através da qual todas as solicitações são processadas.
- O uso de um gateway de conexão permite verificar o certificado de dispositivos móveis fora de uma rede local e impede que os dispositivos enviem dados ao Kaspersky Security Center antes de serem autenticados, o que proporciona proteção à infraestrutura de rede contra vulnerabilidades em protocolos de nível baixo, como TLS/SSL.

Requisitos

Para que um gateway de conexão funcione corretamente com dispositivos móveis, os seguintes requisitos devem ser atendidos:

- As portas 13292 ou 13293 devem estar abertas no host com o gateway de conexão.

Essas portas são projetadas para conectar e sincronizar dispositivos móveis.

- Ao usar a porta 13293, o certificado TLS é verificado no gateway de conexão (sem ser enviado ao Servidor de Administração).
- Ao usar a porta 13292, o certificado não é verificado (o sinalizador LP_MobileMustUseTwoWayAuthOnPort13292 é ignorado).
- A porta 13000 deve estar aberta entre o gateway de conexão e o Kaspersky Security Center, por meio do qual o gateway de conexão recebe conexões do Servidor de Administração. Ela não precisa ser aberta fora da DMZ.
- O host deve ter um endereço estático que pode ser acessado pela Internet.

Fases

A configuração segue nas seguintes etapas:

1 Instale o Agente de Rede na função de gateway de conexão em um host

Em primeiro lugar, é necessário instalar o Agente de Rede no dispositivo host selecionado que atua na função de gateway de conexão.

Para obter informações sobre como gerar um pacote de instalação do Agente de Rede, consulte a [Ajuda do Kaspersky Security Center](#).

Você pode [instalar o Agente de Rede no modo interativo](#) especificando os parâmetros de instalação passo a passo. Como alternativa, é possível usar um arquivo de resposta, um arquivo de texto que contém um conjunto personalizado de parâmetros de instalação: variáveis e seus respectivos valores. O uso do arquivo de resposta permite executar a instalação no modo silencioso, ou seja, sem a participação do usuário. Para obter informações sobre como instalar o Agente de Rede no modo silencioso, consulte a [Ajuda do Kaspersky Security Center](#).

2 Configure o gateway de conexão no Servidor de Administração do Kaspersky Security Center

Após instalar o Agente de Rede na função de gateway de conexão, você deve conectá-lo ao Servidor de Administração. O Servidor de Administração ainda não lista o dispositivo com o gateway de conexão entre os dispositivos gerenciados porque o gateway de conexão não tentou se conectar ao Servidor de Administração.

Você deve criar um novo grupo dentro do grupo **Dispositivos gerenciados** e adicionar o dispositivo que atua como um gateway de conexão ao grupo criado. Para obter informações sobre como adicionar dispositivos manualmente a grupos no Kaspersky Next Expert View (cloud), consulte a [ajuda do Kaspersky Security Center](#).

Depois disso, [atribua o dispositivo como um ponto de distribuição](#) e configure o ponto de distribuição para atuar como um gateway de conexão na seção **Gateway de conexão** das propriedades do ponto de distribuição. Em seguida, ative as opções **Abrir porta para dispositivos móveis (apenas autenticação SSL do Servidor de Administração)** e **Abrir porta para dispositivos móveis (autenticação SSL bidirecional)** e especifique as portas e os nomes de domínio DNS do ponto de distribuição para conectar dispositivos móveis.

Se a restrição básica 'CA: true' não estiver definida para um certificado de dispositivos móveis personalizado do Servidor de Administração, o mesmo certificado será usado para o gateway de conexão e para o Servidor de Administração. Se a restrição básica 'CA: true' for definida, um certificado separado emitido pelo certificado do Servidor de Administração móvel personalizado será usado para o gateway de conexão.

3 Como reemitir o certificado de dispositivos móveis

Emita novamente o certificado de dispositivos móveis com um endereço de conexão especificado ao configurar o gateway de conexão (na janela de propriedades do Servidor de Administração, selecione **Geral** → **Certificados**). Para obter informações detalhadas sobre a reemissão de certificados de dispositivos móveis, consulte a seção Reemitir o certificado do Servidor de Administração de dispositivo móvel.

Resultados

O gateway de conexão será configurado. Você poderá adicionar novos dispositivos móveis especificando o endereço do gateway de conexão.

Para garantir que os dispositivos móveis sejam sincronizados com o Kaspersky Security Center no gateway de conexão, o endereço de conexão definido ao configurar o gateway de conexão deve ser especificado nas propriedades dos pacotes de instalação do Kaspersky Endpoint Security for Android (**Operações** → **Repositórios** → **Pacotes de instalação**).

Adição de uma chave de licença ao repositório do Servidor de Administração

Para conectar dispositivos móveis ao Kaspersky Next Expert View (cloud) e gerenciá-los, é necessário especificar uma chave de licença compatível com a solução Gerenciamento de Dispositivos Móveis.

A licença sob a qual a solução é usada determina o escopo de configurações básicas ou avançadas que você pode definir. Com uma licença que não inclui a funcionalidade estendida de MDM básico no Kaspersky Next Expert View (cloud), somente as configurações básicas de proteção do dispositivo estão disponíveis no plug-in do Kaspersky Mobile Devices Protection and Management. Para obter informações detalhadas sobre licenças, consulte a seção [Sobre a licença](#).

Para especificar uma chave de licença nas configurações de licença atuais das propriedades do Servidor de Administração:

- Na janela principal do Kaspersky Next Expert View (cloud), clique no nome do Servidor de Administração. Na janela Propriedades do Servidor de Administração que é exibida:
 - a. Na guia **Geral**, selecione a seção **Chaves de licença**.
 - b. No bloco de configurações **Licença atual**, clique em **Selecionar** e execute uma das seguintes ações:
 - Escolha uma das chaves de licença existentes.
 - Especifique o arquivo KEY que deseja adicionar.

A licença escolhida deve ser compatível com a solução de gerenciamento de dispositivos móveis.

c. Clique em **Salvar**.

A chave de licença é especificada nas configurações de licença atuais das propriedades do Servidor de Administração.

Adição de uma chave de licença ao repositório do Servidor de Administração:

1. Na janela principal do Kaspersky Next Expert View (cloud), selecione **Operações** → **Licenças**.
2. Clique em **Adicionar**.
3. Na janela que se abre, clique em **Adicionar arquivo de chave**.
4. Clique em **Selecionar arquivo de chave** e especifique o arquivo KEY que deseja adicionar.

A licença escolhida deve ser compatível com a solução de gerenciamento de dispositivos móveis.

5. Clique em **Salvar**.

A chave de licença é adicionada ao repositório do Servidor de Administração.

Implementar um sistema de gerenciamento de dispositivo iOS

O MDM básico no Kaspersky Next Expert View (cloud) permite gerenciar dispositivos móveis com iOS. Esta seção descreve a implementação de um sistema de gerenciamento de dispositivos iOS.

Sobre os modos de operação de dispositivos iOS

O modo de operação do dispositivo depende do proprietário do dispositivo móvel (pessoal ou corporativo) e dos requisitos de segurança corporativa. Você pode selecionar o modo de operação que seja o mais conveniente para a sua empresa e usar vários modos ao mesmo tempo.

Os seguintes modos de operação estão disponíveis para dispositivos iOS:

- **Kaspersky Protection for iOS**

Proteção contra ameaças da Web e detecção de jailbreak em dispositivos iOS.

- **Perfil de gerenciamento**

Configurações básicas e avançadas para gerenciar dispositivos iOS. Os dispositivos iOS no modo de operação "Perfil de gerenciamento" só podem ser adicionados ao grupo de administração "Dispositivos gerenciados".

Para conectar dispositivos iOS no modo de operação "Perfil de gerenciamento", instale o [Servidor de MDM do iOS](#).

Um *dispositivo supervisionado* é um dispositivo iOS ou iPadOS cujas configurações são monitoradas pelo Apple Configurator, um programa para a configuração de grupo de dispositivos iOS e iPadOS. 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 redefinirá, caso seja necessário. Um dispositivo supervisionado não pode ser sincronizado com o Apple Configurator instalado em outro computador.

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 não são supervisionados.

Sobre perfis de gerenciamento

Um *perfil de gerenciamento* é um perfil que contém as configurações para conectar dispositivos móveis que executam iOS ao Kaspersky Security Center. Após a instalação do perfil de gerenciamento e a sincronização do dispositivo com o servidor de MDM do iOS, o dispositivo passa a ser um dispositivo gerenciado (dispositivo iOS MDM). Os dispositivos iOS MDM são gerenciados por meio do serviço Apple Push Notification (APNs).

Usando um perfil de gerenciamento, é possível:

- Definir remotamente as configurações dos dispositivos iOS usando [políticas](#).
- [Enviar comandos](#) para dispositivos iOS MDM.
- Instalar remotamente os aplicativos da Kaspersky e de terceiros.

A implementação de um perfil de gerenciamento é executada por meio do Kaspersky Next Expert View (cloud) usando o [assistente de conexão de novos dispositivos móveis](#). O usuário instala o perfil de gerenciamento depois de receber um e-mail com informações para conectar o dispositivo móvel ao Kaspersky Security Center. Nenhuma preparação adicional para o perfil é necessária.

Antes de instalar um perfil de gerenciamento, é necessário [implementar um sistema de gerenciamento de dispositivos iOS](#).

Implementar o Kaspersky Protection for iOS

Os dispositivos iOS [no modo de operação "Kaspersky Protection for iOS"](#) são protegidos pelo aplicativo Kaspersky Protection for iOS instalado nos dispositivos dos usuários.

Esta seção contém informações sobre os [recursos](#) do aplicativo Kaspersky Protection for iOS, além do processo de [instalação](#), [ativação](#), [atualização](#) e [remoção](#).

Sobre o Kaspersky Protection for iOS

O Kaspersky Protection for iOS garante a proteção dos dispositivos móveis contra phishing e ameaças da Web. O Kaspersky Protection for iOS oferece os principais recursos a seguir:

- Proteção na Web
- Detecção de jailbreak

Proteção na Web

A Proteção na Web também bloqueia sites maliciosos projetados para propagar código malicioso e também bloqueia sites de phishing projetados para roubar dados confidenciais do usuário (por exemplo, senhas de bancos on-line ou sistemas de dinheiro eletrônico) e acessar as informações financeiras do usuário. A Proteção na Web também monitora a atividade de rede dos aplicativos e todo o tráfego do sistema no dispositivo do usuário.

A Proteção na Web usa o serviço na nuvem da Kaspersky Security Network para verificar os sites antes que eles sejam abertos. Após a verificação, a Proteção na Web permite que os sites confiáveis sejam carregados e bloqueia sites maliciosos.

Somente o domínio do site é verificado. Se for um domínio malicioso ou de phishing, a Proteção na Web bloqueará a ameaça. Se o domínio não for classificado como malicioso ou de phishing, a URL específica não será bloqueada.

A Proteção na Web requer o seguinte para funcionar em um dispositivo gerenciado:

- [O uso da Kaspersky Security Network](#) está ativado nas configurações de política do Kaspersky Next Expert View (cloud).
- O usuário permitiu que o aplicativo Kaspersky Protection for iOS adicionasse uma configuração de VPN.

É possível configurar esse componente do aplicativo no Kaspersky Next Expert View (cloud) definindo as [configurações de política](#) correspondentes.

Detecção de jailbreak

Quando o aplicativo Kaspersky Protection for iOS detecta um jailbreak, ele exibe uma mensagem crítica e informa o usuário sobre o problema.

Um jailbreak permite ignorar os recursos de segurança do sistema operacional, portanto, a segurança do dispositivo do usuário não pode ser garantida, e vários problemas podem surgir, inclusive:

- 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

Instalação do Kaspersky Protection for iOS

Depois de concluir o [assistente de conexão de dispositivo móvel](#), o aplicativo pode ser instalado das seguintes formas:

- Se tiver escolhido a opção **Enviar uma mensagem aos e-mails dos usuários**, os usuários especificados receberão os e-mails com códigos QR e links para conectar os dispositivos móveis ao Servidor de Administração. O link contém todas as informações sobre as configurações de conexões que serão automaticamente transferidas para o aplicativo durante a instalação.

O link do convite é válido por 24 horas. Se o usuário não conseguir instalar o aplicativo a tempo, crie e envie um novo convite.

Depois que o usuário [instalar](#) o Kaspersky Protection for iOS, o dispositivo iOS no modo operacional de proteção básica se conectará ao Servidor de Administração e aparecerá na guia **Dispositivos** do Kaspersky Next Expert View (cloud).

Se o dispositivo do usuário não estiver conectado ao Kaspersky Security Center, o usuário poderá ativar o aplicativo manualmente usando [o código de ativação](#) enviado.

- Se você escolheu a opção **Mostrar códigos QR e links após a conclusão do assistente**, os detalhes da conexão estarão disponíveis na tela Concluir. Leia o código QR usando a câmera do dispositivo iOS no qual deseja instalar o aplicativo.

Ativar o Kaspersky Protection for iOS

No Kaspersky Security Center, a licença pode abranger diversos grupos de recursos. Para garantir que o Kaspersky Protection for iOS seja totalmente funcional, a licença do Kaspersky Security Center adquirida pela organização deve oferecer suporte para a funcionalidade Gerenciamento de Dispositivos Móveis.

Para obter informações detalhadas sobre as opções de licenças, consulte a seção [Sobre a licença](#).

O aplicativo Kaspersky Protection for iOS é ativado em um dispositivo móvel inserindo as informações da licença válidas no aplicativo. As informações da licença são entregues ao dispositivo junto com as configurações das políticas 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. Quando alternado para o modo de funcionalidade limitada, o aplicativo para de executar a sincronização automática com o Kaspersky Security Center. Sendo assim, 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. Na janela principal do Kaspersky Next Expert View (cloud), selecione **Gerenciamento de ativos** → **Políticas**. Na lista de políticas de grupo aberta, clique no nome da política que deseja configurar.
2. Na janela de propriedades da política, selecione **Configurações do aplicativo**.
3. Clique no botão **Licença**.
4. Na janela que se abre, 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.

Se um arquivo de chave for selecionado no armazenamento de chaves do Kaspersky Security Center e enviado ao dispositivo, o Kaspersky Protection for iOS não poderá processá-lo, porque o Kaspersky Protection for iOS não é compatível com esse método de ativação. Para ativar o Kaspersky Protection for iOS, você deve adicionar um código de ativação ao Kaspersky Security Center.

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 **Substituir pela chave selecionada caso a chave seja diferente nos dispositivos**.

No entanto, em alguns dispositivos iOS, a chave de ativação existente pode ser substituída por uma nova em segundo plano mais tarde do que o esperado se o usuário encerrar o Kaspersky Protection for iOS deslizando para cima no App Switcher. Para forçar uma atualização da licença, o usuário deve reabrir o aplicativo. Para obter mais informações sobre restrições e recomendações relacionadas à otimização da execução de tarefas em segundo plano, consulte a seção [problemas conhecidos do Kaspersky Protection for iOS](#).

5. Clique em **Salvar** para salvar as alterações efetuadas.

O aplicativo é ativado após a próxima sincronização do dispositivo com o Servidor de Administração.

O usuário também pode entrar em contato com o administrador para obter um código de ativação e [inserir-lo manualmente](#).

Atualização do Kaspersky Protection for iOS

O Kaspersky Protection for iOS é atualizado de acordo com o procedimento padrão de atualização do aplicativo na plataforma iOS. Para obter informações detalhadas sobre a atualização, consulte a seção [atualizador de aplicativos](#).

Remoção do Kaspersky Protection for iOS

Um usuário remove o aplicativo Kaspersky Protection for iOS manualmente seguindo o procedimento padrão de remoção do aplicativo na plataforma iOS. Para obter informações detalhadas sobre a remoção, consulte a seção [Remover o aplicativo](#).

Implementar um sistema de gerenciamento usando o protocolo MDM do iOS

Os dispositivos iOS no modo de operação “Perfil de gerenciamento” são gerenciados com o uso do protocolo MDM do iOS. Para implementar um sistema de gerenciamento móvel usando o protocolo iOS MDM e conectar dispositivos iOS ao Kaspersky Security Center, siga estas etapas:

- 1 [Receber um Certificado de APNs](#)
- 2 [Instalar um Certificado de APNs no Servidor de MDM do iOS](#)
- 3 [Conectar dispositivos iOS ao Kaspersky Security Center](#)

Exibir a lista de Servidores de MDM do iOS instalados e definir as respectivas configurações

O Kaspersky Next Expert View (cloud) permite exibir a lista de Servidores de MDM do iOS instalados e acessar as respectivas configurações.

Para exibir os Servidores de MDM do iOS instalados:

1. Na janela principal do Kaspersky Next Expert View (cloud), selecione **Gerenciamento de ativos** → **Móvel** → **Servidores de MDM do iOS**.
2. Na lista de Servidores de MDM do iOS instalados que se abre:
 - a. Para instalar o Servidor de MDM do iOS, clique em **Instalar**.
 - b. Para exibir ou definir as configurações do Servidor de MDM do iOS, execute uma das seguintes ações:
 - Marque a caixa de seleção ao lado do Servidor de MDM do iOS cujas configurações você deseja visualizar ou definir e clique em **Modificar configurações**.
A guia **Configurações do aplicativo** da janela de configurações do Servidor de MDM do iOS é exibida.
 - Clique no nome do Servidor de MDM do iOS cujas configurações você deseja visualizar ou definir.
Na janela de configurações do Servidor de MDM do iOS que se abre, vá até a guia **Configurações do aplicativo**.

Para exibir ou definir as configurações do Servidor de MDM do iOS:

1. Vá até a guia **Configurações do aplicativo** da janela de configurações do Servidor de MDM do iOS usando as instruções acima.
 - a. Na seção **Certificados**, você pode gerenciar os certificados necessários para a operação do Servidor de MDM do iOS.
 - **Certificado Apple Push Notification service (APNs)**. O Certificado de APNs é assinado pela Apple e permite usar o serviço Apple Push Notification. Por meio do Apple Push Notification, um Servidor de MDM do iOS pode gerenciar dispositivos iOS. Para obter informações detalhadas sobre o Certificado de APNs, consulte a seção [Receber ou renovar um Certificado de APNs](#).

b. Na seção **Configurações de conexão**, você pode ver e definir as configurações para a conexão do dispositivo móvel ao Servidor de MDM do iOS.

- No bloco de configurações **Sincronização**, você pode ativar ou desativar a sincronização de dispositivos gerenciados com o Servidor de MDM do iOS e especificar o **Período de sincronização (min)**.
- No bloco de configurações **Perfil de gerenciamento do dispositivo**, você pode configurar as propriedades do perfil de instalação. Você pode especificar o **Nome do perfil** (campo obrigatório), a **Empresa** e a **Descrição do perfil**.

Observe que as configurações nessa seção são aplicadas a dispositivos iOS MDM recém-conectados ou a dispositivos iOS MDM conectados anteriormente quando os seus respectivos certificados de dispositivos móveis são renovados.

- Na seção **Perfis de configuração**, você pode exibir e gerenciar perfis de configuração, que são usados para centralizar a definição das configurações de dispositivos iOS gerenciados e aplicar restrições de funções a esses dispositivos. Para obter informações detalhadas sobre o gerenciamento de perfis de configuração, consulte as seções [Adicionar um perfil de configuração](#), [Instalar um perfil de configuração em um dispositivo](#) e [Remover um perfil de configuração de um dispositivo](#).

Receber ou renovar um Certificado de APNs

Para assegurar o funcionamento apropriado do serviço MDM do iOS e respostas em tempo oportuno dos dispositivos móveis aos comandos do administrador, você deve especificar um certificado do serviço Apple Push Notification (Certificado de APNs) nas configurações do Servidor de MDM do iOS.

Caso já tenha um Certificado de APNs, considere renová-lo em vez de receber um novo. Quando o Certificado de APNs existente é substituído por um recém-criado, o Servidor de Administração perde a capacidade de gerenciar os dispositivos iOS MDM conectados anteriormente.

Para emitir ou renovar um Certificado de APNs:

1. Na janela principal do Kaspersky Next Expert View (cloud), selecione **Gerenciamento de ativos** → **Móvel** → **Servidores de MDM do iOS**. Na lista de Servidores de MDM do iOS exibida, clique no Servidor de MDM do iOS cujas configurações você deseja definir.
2. Na janela de configurações do Servidor de MDM do iOS, selecione **Configurações do aplicativo**.
3. Selecione a guia **Certificados**.
4. No bloco de configurações do **Certificado Apple Push Notification service (APNs)**, clique em **Emitir ou renovar**.

O assistente de Certificado de APNs se abre. Clique em **Iniciar** e prossiga pelo assistente usando os botões **Voltar** e **Avançar**.

Quando a Solicitação de Assinatura do Certificado (CSR) é criada na primeira etapa do assistente, sua chave privada é armazenada na RAM do dispositivo. Da mesma forma, todas as etapas do assistente devem ser concluídas sem interrupção em uma única sessão.

Etapa 1. Criar uma Solicitação de Assinatura de Certificado (CSR)

Para criar uma CSR:

- a. Especifique as informações necessárias para gerar um arquivo de solicitação: **Nome comum (CN), Nome da organização (O), Nome da Unidade organizacional (OU), Cidade (L), Região (S), País (C).**
- b. Clique em **Baixar**.

Depois de salvar as alterações, um arquivo CSR será gerado e a chave privada do certificado será salva na memória do dispositivo.

Etapa 2. Assinar o arquivo CSR

Nesta etapa, envie o arquivo CSR recebido na etapa anterior do assistente para a Kaspersky para assinatura:

- a. Clique em **Ir para o Kaspersky CompanyAccount**.
- b. Envie o arquivo CSR criado para a Kaspersky para ser assinado.

Observe que você poderá assinar o arquivo CSR somente depois de carregar uma chave que permite usar a solução Gerenciamento de Dispositivos Móveis.

- c. Após o processamento de sua solicitação online, você receberá um arquivo de solicitação CSR assinado pela Kaspersky.
- d. Salve o arquivo recebido.

Etapa 3. Receber a chave pública do Certificado de APNs

Nesta etapa, execute uma das seguintes ações se desejar emitir um novo certificado ou renovar um existente:

Para emitir um novo certificado:

- a. Clique em **Ir para o portal da Apple**.
- b. Faça login no portal da Apple com uma Apple ID corporativa.

Recomenda-se que evite usar uma Apple ID pessoal. Crie uma Apple ID dedicada para usar como sua ID corporativa. Após você ter criado uma Apple ID, deve vinculá-la à caixa de e-mail da organização, e não a uma caixa de e-mail de um funcionário.

- c. Carregue um arquivo CSR assinado.
O arquivo será usado para gerar a chave pública do Certificado de APNs.
- d. Após o processamento do seu arquivo CSR pela Apple, você receberá a chave pública do Certificado de APNs.
Salve o arquivo recebido.

Para renovar um certificado:

- a. Clique em **Ir para o portal da Apple**.
- b. Faça login no portal da Apple com uma Apple ID corporativa.

Recomenda-se que evite usar uma Apple ID pessoal. Crie uma Apple ID dedicada para usar como sua ID corporativa. Após você ter criado uma Apple ID, deve vinculá-la à caixa de e-mail da organização, e não a uma caixa de e-mail de um funcionário.

- c. Especifique o certificado que deseja renovar.
- d. Carregue um arquivo CSR assinado.
O arquivo será usado para gerar a chave pública do Certificado de APNs.
- e. Após o processamento do seu arquivo CSR pela Apple, você receberá a chave pública do Certificado de APNs.
Salve o arquivo recebido.

Etapa 4. Especificar a chave pública do certificado de APNs

Nesta etapa, carregue o arquivo de chave pública recebido da Apple na etapa anterior do assistente:

- a. Clique em **Selecionar**.
- b. Na janela do Explorador de Arquivos que se abre, especifique um arquivo de certificado no formato PEM, PFX ou P12 e clique em **Abrir**.

Etapa 5. Especificar a senha da chave privada do certificado de APNs

Nesta etapa, informe o nome do certificado e a senha da chave privada:

- a. No campo **Nome do certificado**, especifique um nome personalizado para o certificado.
- b. No campo **Senha da chave privada**, especifique a senha da chave privada para o certificado.
Essa senha será usada para [instalar o Certificado de APNs](#) no Servidor de MDM do iOS.
- c. Em **Confirmar senha**, insira a senha novamente.

Etapa 6. Concluir o CSR

Nesta etapa, o Certificado de APNs é gerado e está pronto para ser instalado no Servidor de MDM do iOS.

- a. Para concluir o CSR, clique em **Baixar certificado de APNs** para salvar o certificado criado.
- b. Clique em **Concluído** para sair do assistente.

A chave privada e a chave pública do certificado são combinadas e o Certificado de APNs é salvo em formato PEM.

Agora você pode [instalar o Certificado de APNs gerado no Servidor de MDM do iOS](#).

Instalar um Certificado de APNs no Servidor de MDM do iOS

Depois que o Certificado de APNs for recebido, você poderá instalá-lo no Servidor de MDM do iOS.

Para instalar o Certificado de APNs no Servidor de MDM do iOS:

1. Na janela principal do Kaspersky Next Expert View (cloud), selecione **Gerenciamento de ativos** → **Móvel** → **Servidores de MDM do iOS**. Na lista de Servidores de MDM do iOS exibida, clique no Servidor de MDM do iOS cujas configurações você deseja definir.
2. Na janela de configurações do Servidor de MDM do iOS, selecione **Configurações do aplicativo**.
3. Selecione a guia **Certificados**.
4. No bloco de configurações do **Certificado Apple Push Notification service (APNs)**:
 - a. Clique em **Instalar**.
 - b. Na janela do Explorador de Arquivos que se abre, especifique um arquivo de certificado no formato PEM e clique em **Abrir**.

Assegure-se de que o certificado instalado esteja em conformidade com os seguintes requisitos de segurança:

 - O nome comum (CN) está especificado.
 - Um tópico de APNs está especificado.
 - O editor de certificado está especificado.
 - A data de expiração correta do certificado está especificada.
 - c. Na janela **Instalando certificado** que se abre, insira a senha da chave privada especificada no [recebimento do Certificado de APNs](#) e clique em **Instalar**.

O Certificado de APNs será instalado no Servidor de MDM do iOS. Os detalhes do certificado serão exibidos no bloco de configurações do **Certificado Apple Push Notification service (APNs)**.

Eventos do Servidor de MDM do iOS

O Kaspersky Next Expert View (cloud) permite visualizar os eventos relacionados ao Servidor de MDM do iOS. Os eventos têm diferentes níveis de gravidade: *Informações*, *Advertência*, *Crítico* e *Falha funcional*.

Para cada evento que pode ser gerado pelo Servidor de MDM do iOS, você pode especificar as configurações de notificação e armazenamento na guia **Configuração de eventos** das configurações do Servidor de MDM do iOS. Recomendamos que você defina as configurações para cada tipo de evento depois de implementar o Servidor de MDM do iOS para limitar o número de eventos exibidos e reduzir o tempo de carregamento da lista de eventos.

Se você quiser definir as configurações de notificação para todos os eventos de uma vez, defina as configurações gerais de notificação nas propriedades do Servidor de Administração. Para obter informações detalhadas sobre notificações, consulte a [Ajuda do Kaspersky Security Center](#).

Para ver os eventos do Servidor de MDM do iOS:

1. Na janela principal do Kaspersky Next Expert View (cloud), selecione **Gerenciamento de ativos** → **Móvel** → **Servidores de MDM do iOS**. Na lista de Servidores de MDM do iOS exibida, clique no Servidor de MDM do iOS cujos eventos você deseja visualizar.
2. Na janela de configurações do Servidor de MDM do iOS, selecione **Configurações do aplicativo**.
3. Selecione a guia **Eventos**.

Os eventos do Servidor de MDM do iOS são exibidos.

Para obter informações detalhadas sobre a exibição de eventos no Kaspersky Next Expert View (cloud), consulte a [ajuda do Kaspersky Security Center](#).

A tabela abaixo mostra os eventos do Servidor de MDM do iOS com o nível de gravidade *Informações*.

Eventos de informações do Servidor de MDM do iOS

Nome de exibição do tipo de evento	Tipo de evento	Prazo de armazenamento padrão
Informações gerais de dispositivo móvel solicitadas	DEVICEINFORMATION_COMMAND_SUCCESSFUL	30 dias
Informações de segurança solicitadas	SECURITYINFO_COMMAND_SUCCESSFUL	30 dias
Novo dispositivo móvel conectado	NEW_DEVICE_CONNECTED	30 dias
Lista de perfis solicitada	PROFILELIST_COMMAND_SUCCESSFUL	30 dias
Perfil instalado	INSTALLPROFILE_COMMAND_SUCCESSFUL	30 dias
Perfil excluído	REMOVEPROFILE_COMMAND_SUCCESSFUL	30 dias
Lista de certificados instalados solicitada	CERTIFICATELIST_COMMAND_SUCCESSFUL	30 dias
Lista de aplicativos instalados solicitada	INSTALLEDAPPLICATIONLIST_COMMAND_SUCCESSFUL	30 dias
Lista de aplicativos gerenciados solicitada	MANAGEDAPPLICATIONLIST_COMMAND_SUCCESSFUL	30 dias
Solicitada a instalação do aplicativo	INSTALLAPPLICATION_COMMAND_SUCCESSFUL	30 dias
Configuração do aplicativo aplicada	APPCONFIG_APPLIED_SUCCESSFUL	30 dias
Aplicativo gerenciado excluído	REMOVEAPPLICATION_COMMAND_SUCCESSFUL	30 dias
Configurado o código de resgate do aplicativo	APPLYREDEMPTIONCODE_COMMAND_SUCCESSFUL	30 dias

Nome de exibição do tipo de evento	Tipo de evento	Prazo de armazenamento padrão
Dispositivo móvel bloqueado	DEVICELock_COMMAND_SUCCESSFUL	30 dias
Redefinição de senha	CLEARPASSCODE_COMMAND_SUCCESSFULL	30 dias
Dados do dispositivo móvel apagados	ERASEDEVICE_COMMAND_SUCCESSFUL	30 dias
Atualização do sistema operacional agendada	SCHEDULEOSUPDATE_COMMAND_SUCCESSFULL	30 dias
Configurações de roaming aplicadas	SETROAMINGSETTINGS_COMMAND_SUCCESSFUL	30 dias
Recebido o código de desvio do bloqueio de ativação	GET_ACTIVATION_LOCK_BYPASS_CODE_COMMAND_SUCCESSFUL	30 dias
Iniciada a verificação de Controle de conformidade	COMPLIANCE_CONTROL_CHEKING_RULES_STARTED	30 dias
Concluída a verificação de Controle de conformidade	COMPLIANCE_CONTROL_CHEKING_RULES_COMPLETED	30 dias
Iniciada resposta do Controle de conformidade	COMPLIANCE_CONTROL_ACTION_STARTED	30 dias
Resposta do Controle de conformidade concluída	COMPLIANCE_CONTROL_ACTION_COMPLETED	30 dias

A tabela abaixo mostra os eventos do Servidor de MDM do iOS com o nível de gravidade *Advertência*.

Eventos de advertência do Servidor de MDM do iOS

Nome de exibição do tipo de evento	Tipo de evento	Prazo de armazenamento padrão
Detectada tentativa de conexão de dispositivo móvel bloqueado	INACTICE_DEVICE_TRY_CONNECTED	30 dias
Perfil de gerenciamento excluído	MDM_PROFILE_WAS_REMOVED	30 dias
Detectada tentativa de reutilização do certificado do usuário	CLIENT_CERT_ALREADY_IN_USE	30 dias
Detectada não conformidade com critério do Controle de conformidade	COMPLIANCE_CONTROL_CONDITIONS_MATCH_DETECTED	30 dias
Falha ao executar resposta de Controle de conformidade	COMPLIANCE_CONTROL_ACTION_FAILED	30 dias
Detectado dispositivo móvel inativo	FOUND_INACTIVE_DEVICE	30 dias
Um código de resgate é necessário	NEED_REDEMPTION_CODE	30 dias
Perfil de gerenciamento excluído do dispositivo móvel	UMDM_PROFILE_WAS_REMOVED	30 dias

A tabela abaixo mostra os eventos do Servidor de MDM do iOS com o nível de gravidade *Falha funcional*.

Eventos de falha funcional do Servidor de MDM do iOS

Nome de exibição do tipo de evento	Tipo de evento	Prazo de armazenamento padrão
Falha ao solicitar informações gerais de dispositivo móvel	DEVICEINFORMATION_COMMAND_FAILED	30 dias
Falha ao solicitar informações de segurança	SECURITYINFO_COMMAND_FAILED	30 dias
Falha ao solicitar lista de perfis	PROFILELIST_COMMAND_FAILED	30 dias
Falha ao instalar perfil	INSTALLPROFILE_COMMAND_FAILED	30 dias
Falha ao excluir o perfil	REMOVEPROFILE_COMMAND_FAILED	30 dias
Falha ao solicitar lista de certificados instalados	CERTIFICATELIST_COMMAND_FAILED	30 dias
Falha ao solicitar lista de aplicativos instalados	INSTALLEDAPPLICATIONLIST_COMMAND_FAILED	30 dias

Nome de exibição do tipo de evento	Tipo de evento	Prazo de armazenamento padrão
Falha ao solicitar a lista de aplicativos gerenciados	MANAGEDAPPLICATIONLIST_COMMAND_FAILED	30 dias
Falha ao solicitar instalação do aplicativo	INSTALLAPPLICATION_COMMAND_FAILED	30 dias
Falha ao aplicar configuração do aplicativo	APPCONFIG_APPLIED_FAILED	30 dias
Falha ao excluir o aplicativo gerenciado	REMOVEAPPLICATION_COMMAND_FAILED	30 dias
Falha ao configurar o código de resgate do aplicativo	APPLYREDEMPTIONCODE_COMMAND_FAILED	30 dias
Falha ao bloquear dispositivo móvel	DEVICELOCK_COMMAND_FAILED	30 dias
Não foi possível redefinir a senha	CLEARPASSCODE_COMMAND_FAILED	30 dias
Falha ao limpar os dados no dispositivo móvel	ERASEDEVICE_COMMAND_FAILED	30 dias
Falha ao agendar atualização do sistema operacional	SCHEDULEOSUPDATE_COMMAND_FAILED	30 dias
Falha ao aplicar configurações de roaming	SETROAMINGSETTINGS_COMMAND_FAILED	30 dias
Falha ao receber o código de desvio de bloqueio de ativação	GET_ACTIVATION_LOCK_BYPASS_CODE_COMMAND_FAILED	30 dias
Erro na operação do aplicativo	PRODUCT_FAILURE	30 dias
O resultado do comando contém dados incorretos	MALFORMED_COMMAND	30 dias
Falha ao enviar a mensagem	SEND_PUSH_NOTIFICATION_FAILED	30 dias
Falha ao enviar o comando (Controle de conformidade)	SEND_COMMAND_FAILED	30 dias
Dispositivo não encontrado	DEVICE_NOT_FOUND	30 dias

Implementar um sistema de gerenciamento de dispositivos Android

O MDM básico no Kaspersky Next Expert View (cloud) permite gerenciar dispositivos móveis com Android. Esta seção descreve a implementação de um sistema de gerenciamento de dispositivos Android.

Sobre os modos de operação de dispositivos Android

O Kaspersky Endpoint Security for Android está instalado nos dispositivos móveis dos usuários. O aplicativo permite definir remotamente as configurações do dispositivo, gerenciar dispositivos de forma centralizada usando comandos e garantir a proteção dos dispositivos móveis contra ameaças da Web, vírus e outros programas que representem ameaças.

Usar o Firebase Cloud Messaging

Para garantir a entrega oportuna de comandos para dispositivos Android, o Kaspersky Security Center usa o mecanismo de notificações push. As notificações push são trocadas entre os dispositivos Android e o Servidor de Administração por meio do Firebase Cloud Messaging (aqui referido como FCM). No Kaspersky Next Expert View (cloud), é possível especificar as configurações do Firebase Cloud Messaging para conectar dispositivos Android ao serviço.

Para recuperar as configurações do Firebase Cloud Messaging, é necessário ter uma conta do Google.

Para ativar o uso do FCM:

1. Na janela principal do Kaspersky Next Expert View (cloud), selecione **Gerenciamento de ativos** → **Móvel** → **Dispositivos**.
2. Abra o menu de 3 pontos (⋮) e selecione **Sincronização forçada de dispositivos Android**.
3. No campo **Número do projeto do Firebase**, especifique a ID do remetente do FCM.
4. No campo **Chave privada**, selecione o arquivo de chave privada.

Na próxima sincronização com o Servidor de Administração, os dispositivos Android serão conectados com o Firebase Cloud Messaging.

Ao alternar para um projeto diferente do Firebase, é necessário aguardar 10 minutos para que o FCM seja retomado.

O serviço FCM é executado nas seguintes faixas de endereços:

- Do dispositivo Android, o acesso é necessário às portas 443 (HTTPS), 5228 (HTTPS), 5229 (HTTPS) e 5230 (HTTPS) dos seguintes endereços:
 - google.com
 - fcm.googleapis.com
 - oauth2.googleapis.com
 - android.apis.google.com
 - Todos dos endereços IP listados no ASN da Google de 15169
- No Servidor de Administração, o acesso é necessário à porta 443 (HTTPS) dos seguintes endereços:
 - fcm.googleapis.com
 - Todos dos endereços IP listados no ASN da Google de 15169

Caso as configurações do servidor proxy tenham sido especificadas nas propriedades do Servidor de Administração no Kaspersky Next Expert View (cloud), elas serão usadas para a interação com o FCM.

Como configurar o FCM: obter o ID do remetente e o arquivo de chave privada

Para configurar o FCM:

1. Registre-se no [portal do Google](#).
2. Acesse o [Console do Firebase](#).
3. Execute uma das seguintes ações:
 - Para criar um novo projeto, clique em **Criar um projeto** e siga as instruções na tela.
 - Abra um projeto existente.
4. Clique no ícone de engrenagem e escolha **Configurações do projeto**.
A janela **Configurações do projeto** é aberta.
5. Selecione a guia **Mensagens na nuvem**.
6. Obtenha o ID do remetente relevante no campo **ID do remetente** na seção **Firebase Cloud Messaging API (V1)**.
7. Selecione a guia **Contas de serviço** e clique em **Gerar nova chave privada**.
8. Na janela exibida, clique em **Gerar chave** para gerar e baixar um arquivo de chave privada.

O Firebase Cloud Messaging agora está configurado.

Implementar o Kaspersky Endpoint Security for Android

Esta seção contém uma visão geral do Kaspersky Endpoint Security for Android e seus respectivos métodos de instalação, atualização e remoção.

Para obter informações detalhadas sobre o Kaspersky Endpoint Security for Android, consulte a seção [Uso do aplicativo Kaspersky Endpoint Security for 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 Kaspersky Endpoint Security for Android inclui os seguintes recursos:

- **Antimalware.** O componente detecta e neutraliza as ameaças no dispositivo utilizando os bancos de dados antimalware e o serviço da Kaspersky Security Network na nuvem. O Antimalware inclui os seguintes componentes:
 - **Proteção.** Detecta ameaças em arquivos abertos, verifica novos aplicativos e previne a infecção do dispositivo em tempo real.
 - **Verificação.** Iniciada sob demanda para todo o sistema de arquivos, somente para aplicativos instalados ou somente para um arquivo ou pasta selecionado.
 - **Atualização.** Permite baixar novos bancos de dados antimalware para o aplicativo.
- **Antirroubo.** Este componente protege as 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 o dispositivo.** Obtém as coordenadas da localização do dispositivo.
 - **Alarme sonoro.** Faz com que o dispositivo acione o disparo de um alarme sonoro.
 - **Limpar os dados corporativos.** Elimina os dados corporativos para proteger a confidencialidade das informações corporativas.
- **Proteção na Web e Controle da Web.** A Proteção na Web bloqueia sites maliciosos projetados para disseminar códigos maliciosos. A Proteção na Web também bloqueia sites falsos (de phishing) projetados para roubar dados confidenciais do usuário (por exemplo, senhas de bancos on-line ou sistemas de dinheiro eletrônico) e acessar as informações financeiras do usuário. A Proteção na Web usa o serviço na nuvem da Kaspersky Security Network para verificar os sites antes que eles sejam abertos. Após a verificação, a Proteção na Web permite que os sites confiáveis sejam carregados e bloqueia sites maliciosos. O Controle da Web permite filtrar 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, como Jogos de azar, loterias, apostas ou Comunicações via Internet.
- **Controle de aplicativos.** Este componente permite instalar aplicativos recomendados e necessários em um dispositivo Android, bem como remover aplicativos bloqueados que violam os requisitos de 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 Next Expert View (cloud) definindo as [configurações das políticas](#) correspondentes.

Instalação do Kaspersky Endpoint Security for Android

Há vários métodos para implementar o aplicativo Kaspersky Endpoint Security for Android. Você pode usar o cenário de instalação mais adequado para a sua organização ou combinar diversos cenários.

Os métodos de instalação incluem o seguinte:

- [Instalação via Kaspersky Security Center](#) usando o **site da Kaspersky**

Escolha esse método para dispositivos móveis que podem acessar a Internet para baixar o arquivo de instalação APK a partir do site da Kaspersky. O aplicativo será atualizado [a partir do site da Kaspersky](#) ou usando a HUAWEI AppGallery, a Samsung Galaxy Store, a RuStore ou o Xiaomi GetApps.

- [Instalação manual](#)

Instalação manual do Kaspersky Endpoint Security for Android

Você pode instalar manualmente o Kaspersky Endpoint Security for Android a partir do site da Kaspersky, HUAWEI AppGallery, Samsung Galaxy Store, RuStore ou Xiaomi GetApps.

Instalar o aplicativo

Para instalar o aplicativo a partir de uma loja de aplicativos, siga o procedimento de instalação padrão para a plataforma Android.

Para instalar o Kaspersky Endpoint Security for Android a partir do site da Kaspersky:

1. Vá para o [site da Kaspersky](#).
2. Encontre o Kaspersky Security for Mobile no site.
3. Toque em **Mostrar downloads**.
4. Selecione uma versão do aplicativo e toque em **Baixar**.
5. Abra o arquivo APK baixado e siga as instruções na tela.

Pode ser necessário permitir que seu navegador instale aplicativos de fontes diferentes do Google Play na seção **Aplicativos** → **Acesso especial de aplicativos** → **Instalar aplicativos desconhecidos** nas configurações do dispositivo. A localização dessas configurações pode variar em dispositivos de fornecedores diferentes.

O aplicativo será instalado no dispositivo.

Configurar o aplicativo

Depois de instalar o Kaspersky Endpoint Security for Android, você deve configurar o aplicativo manualmente. O procedimento de configuração depende de o administrador enviar a você um endereço de servidor ou um link para baixar o aplicativo.

Para configurar o Kaspersky Endpoint Security for Android usando um link para baixar o aplicativo:

1. Abra o Kaspersky Endpoint Security for Android.
2. Leia o Contrato de Licença de Usuário Final. Se você aceitar o Contrato de Licença de Usuário Final, marque a caixa de seleção correspondente e toque em **Continuar**.
3. Toque em **Continuar** e conceda ao aplicativo as permissões necessárias.

4. No campo **Servidor**, especifique o link recebido do administrador.

5. Toque em **Continuar**.

O Kaspersky Endpoint Security for Android está configurado.

Para configurar o Kaspersky Endpoint Security for Android usando um endereço de servidor:

1. Abra o Kaspersky Endpoint Security for Android.

2. Leia o Contrato de Licença de Usuário Final. Se você aceitar o Contrato de Licença de Usuário Final, marque a caixa de seleção correspondente e toque em **Continuar**.

3. Toque em **Continuar** e conceda ao aplicativo as permissões necessárias.

4. No campo **Servidor**, especifique o endereço do Servidor de Administração fornecido pelo administrador.

5. Toque em **Continuar**.

6. Toque em **Ativar** para ativar o aplicativo como administrador do dispositivo.

7. Toque em **Permitir** e conceda ao aplicativo as permissões necessárias.

O Kaspersky Endpoint Security for Android está configurado.

O acesso à Internet deve ser ativado no dispositivo móvel para a sincronização com o Servidor de Administração.

Permissões do Kaspersky Endpoint Security for Android

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 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 executando o Android 11 ou posterior ou Android 6-10 com Google Play Services, você deve desativar a configuração de 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.

Permissão	Função do aplicativo
Telefone (ler o status e a identidade do telefone)	Identificar o dispositivo com o uso de seu IMEI (para Android 5 a 9; para Android 10 a 11 no modo de operação de dispositivo com contêiner corporativo)
	Controle de conformidade, para verificar se o cartão SIM do dispositivo foi substituído ou removido.
Armazenamento (obrigatório)	Antimalware
Acesse para gerenciar todos os arquivos (para Android 11 ou posterior)	Antimalware
Dispositivos por perto (para Android 12 ou posterior)	Restringir o uso do Bluetooth
	Em alguns dispositivos Xiaomi e HUAWEI executando o Android 12, o Kaspersky Endpoint Security for Android não solicita ao usuário a permissão para o recurso Dispositivos Bluetooth por perto . Esse problema é causado pelos recursos específicos do firmware MIUI no Xiaomi e o firmware EMUI no HUAWEI. Apesar da ausência da solicitação dessa permissão, todos os recursos relacionados ao uso do Bluetooth funcionam corretamente nesses dispositivos.
Ignorar a otimização da bateria (para Android 12 ou posterior)	Controle de aplicativos
	Proteção na Web
	Antirroubo
Notificações (para Android 13)	Notificar o usuário sobre problemas de segurança e eventos do aplicativo
Permitir execução em segundo plano (para Android 12 ou posterior)	Garantir a operação contínua do aplicativo. Se a permissão não for concedida, o aplicativo poderá ser descarregado da memória e não poderá ser reiniciado.
Administrador do dispositivo (obrigatório)	Antirroubo – bloquear o dispositivo (somente para o Android 5–6)
	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 ou posterior, o usuário deve conceder a permissão "Enquanto usa o aplicativo" quando solicitado.
Localização	Antirroubo – localizar o dispositivo
	Em dispositivos executando Android 10 ou posterior, o usuário deve conceder a permissão "Permitir o tempo todo" quando solicitado.
	Comandos – obter o histórico de localização

Permissão	Função do aplicativo
Acessibilidade	Antirroubo – bloquear o dispositivo (somente para o Android 7 ou posterior)
	Proteção na Web
	Controle de aplicativos
	Proteção contra a remoção do aplicativo (somente para Android 7 ou posterior)
	Exibição de advertências do Kaspersky Endpoint Security for Android (apenas para Android 10 ou posterior)
	Restringir o uso da câmera (apenas para Android 11 ou posterior)
Exibir janela pop-up (para alguns dispositivos Xiaomi)	Proteção na Web
Exibir janelas pop-up durante a execução em segundo plano (para alguns dispositivos Xiaomi)	Proteção na Web
Executar em segundo plano (para dispositivos Xiaomi com firmware MIUI no Android 11 ou anterior)	Controle de aplicativos
	Proteção na Web
	Antirroubo

Iniciar e parar o Kaspersky Endpoint Security for Android

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 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, por exemplo, ao executar uma verificação de malware programada ou sincronizar o dispositivo com o Kaspersky Security Center. Esse problema ocorre devido aos recursos específicos do software incorporado desses dispositivos.

Ativar o 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 oferecer suporte à funcionalidade Gerenciamento de Dispositivos Móveis.

Para obter informações detalhadas sobre as opções de licenças, consulte a seção [Sobre a licença](#).

A ativação do aplicativo Kaspersky Endpoint Security for Android em um dispositivo móvel é realizada fornecendo informações de licença válidas para o aplicativo. As informações da licença são entregues ao dispositivo junto com as configurações das políticas 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. Quando alternado para o modo de funcionalidade limitada, o aplicativo para de executar a sincronização automática com o Kaspersky Security Center. Sendo assim, se o aplicativo não for ativado 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. Na janela principal do Kaspersky Next Expert View (cloud), selecione **Gerenciamento de ativos** → **Políticas**. Na lista de políticas de grupo aberta, clique no nome da política que deseja configurar.
2. Na janela de propriedades da política, selecione **Configurações do aplicativo**.
3. Clique no botão **Licença**.
4. Na janela que se abre, 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 **Substituir pela chave selecionada caso a chave seja diferente nos dispositivos**.

5. Clique em **Salvar** para salvar as alterações efetuadas.

O aplicativo é ativado após a próxima sincronização do dispositivo com o Kaspersky Security Center.

Atualizar o Kaspersky Endpoint Security for Android

O Kaspersky Endpoint Security for Android pode ser atualizado nas seguintes formas:

- Utilizando o site da Kaspersky. O dispositivo móvel do usuário baixa a nova versão do aplicativo através do site da Kaspersky e a instala no dispositivo.
- Utilizando a HUAWEI AppGallery, Samsung Galaxy Store, RuStore ou Xiaomi GetApps. O usuário do dispositivo móvel baixa a nova versão do aplicativo de uma loja de aplicativos e a instala no dispositivo seguindo o procedimento de atualização padrão para a plataforma Android.

Para atualizar o aplicativo usando a Samsung Galaxy Store, o usuário do dispositivo deve ter uma conta Samsung.

- Utilizando o Kaspersky Security Center. Você pode atualizar remotamente a versão do aplicativo no dispositivo usando o 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 a partir do site da Kaspersky

Para atualizar o aplicativo a partir do site da Kaspersky:

1. Vá para o [site da Kaspersky](#).
2. Encontre o Kaspersky Security for Mobile no site.
3. Toque em **Mostrar downloads**.
4. Selecione uma versão do aplicativo e toque em **Baixar**.
5. Abra o arquivo APK baixado e siga as instruções na tela.

O Kaspersky Endpoint Security for Android está atualizado.

Após baixar o aplicativo, o Kaspersky Endpoint Security for Android verifica os Termos e Condições do Contrato de Licença de Usuário Final (EULA). Caso os termos do EULA tenham sido atualizados, o aplicativo envia uma solicitação para o Kaspersky Security Center. Caso o administrador aceite o EULA no Kaspersky Next Expert View (cloud), o Kaspersky Endpoint Security for Android ignorará a etapa de aceite durante a instalação do aplicativo.

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, você pode selecionar o pacote de instalação independente da versão do Kaspersky Endpoint Security for Android que atende aos requisitos de segurança corporativa.

Você pode atualizar usando o Kaspersky Security Center se o Kaspersky Endpoint Security for Android foi instalado usando um pacote de instalação no Kaspersky Security Center ou um pacote de instalação independente. 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 a Ajuda do Android.

Para atualizar a versão do aplicativo:

1. Adicione um novo pacote de instalação do Kaspersky Endpoint Security for Android.
2. Na janela principal do Kaspersky Next Expert View (cloud), selecione **Gerenciamento de ativos** → **Políticas**. Na lista de políticas de grupo aberta, clique no nome da política que deseja configurar.
3. Na janela de propriedades da política, selecione **Configurações do aplicativo**.
4. Selecione **Android** e vá até a seção **Configurações do KES for Android**.

5. No cartão **Atualização do aplicativo**, clique em **Configurações**.

A janela **Atualização do aplicativo** é exibida.

6. Ative as configurações usando o botão **Atualização do aplicativo**.

7. Clique em **Selecionar**.

A janela **Selecione o pacote de instalação** se abre.

8. Na lista de pacotes de instalação independente do Kaspersky Endpoint Security for Android, selecione o pacote cuja versão atende os requisitos de segurança corporativa.

O Kaspersky Endpoint Security for Android não pode ser passado para uma versão mais antiga do aplicativo.

9. Clique em **Selecionar**.

10. Clique em **OK**.

11. Clique em **Salvar** para salvar as alterações efetuadas.

As configurações do dispositivo móvel são alteradas após a 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 confirmar a instalação, a nova versão do aplicativo será instalada no dispositivo móvel.

A funcionalidade de atualizações (incluindo o fornecimento de atualizações de assinaturas de antimalware e atualizações de base de código), bem como a funcionalidade KSN, podem não estar disponíveis no software nos EUA.

Remover o 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, ela deve ser permitida no cartão **Configurar o acesso às configurações do aplicativo** da seção **Configurações do KES for Android** nas configurações da política.

2. [Remoção do aplicativo pelo administrador](#) (somente Android 13 ou anterior)

O administrador remove o aplicativo remotamente usando o Kaspersky Next Expert View (cloud). O aplicativo pode ser removido de um único dispositivo ou de diversos dispositivos ao mesmo tempo.

Permitir que os usuários removam o Kaspersky Endpoint Security for Android

Para proteger o aplicativo da remoção em dispositivos que executam o Android 7 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.

Para permitir a remoção do aplicativo em uma política de grupo:

1. Na janela principal do Kaspersky Next Expert View (cloud), selecione **Gerenciamento de ativos** → **Políticas**. Na lista de políticas de grupo aberta, clique no nome da política que deseja configurar.
2. Na janela de propriedades da política, selecione **Configurações do aplicativo**.
3. Selecione **Android** e vá até a seção **Configurações do KES for Android**.
4. No cartão **Configurar o acesso às configurações do aplicativo**, clique em **Configurações**.
A janela **Configurar o acesso às configurações do aplicativo** se abre.
5. Marque a caixa de seleção **Permitir a remoção do aplicativo do dispositivo**.
6. Clique em **OK**.
7. Clique em **Salvar** para salvar as alterações efetuadas.

Como resultado, os usuários poderão remover o aplicativo dos dispositivos móveis 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 remover o aplicativo de um dispositivo:

1. Na janela principal do Kaspersky Endpoint Security for Android, selecione **Configurações** → **Configurações do aplicativo** → **Adicional** → **Remover o aplicativo**.
 2. Confirme a remoção do Kaspersky Endpoint Security for Android.
- O Kaspersky Endpoint Security for Android será removido do dispositivo.

Remoção do Kaspersky Endpoint Security for Android pelo usuário

Para remover de forma independente o Kaspersky Endpoint Security for Android de um dispositivo móvel, o usuário deve fazer o seguinte:

1. Na janela principal do Kaspersky Endpoint Security for Android, selecione **Configurações** → **Configurações do aplicativo** → **Adicional** → **Remover o aplicativo**.

Caso o botão **Remover o aplicativo** esteja ausente, isso 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 Kaspersky Endpoint Security for Android será removido do dispositivo.

Recomendamos remover o Kaspersky Endpoint Security for Android usando somente as configurações do aplicativo, conforme descrito nas instruções acima. Outros métodos de desinstalação podem resultar na remoção incompleta de contêineres corporativos e outros comportamentos imprevisíveis.

Remoção remota do Kaspersky Endpoint Security for Android

É possível remover remotamente o aplicativo Kaspersky Endpoint Security for Android de dispositivos com Android 13 ou anterior ao enviar o comando **Redefinir as configurações padrão**.

A execução do comando **Redefinir as configurações padrão** limpa todos os dados e reverte as configurações do dispositivo para seus valores padrão. Esse método de remoção de aplicativo é recomendado pela Android Enterprise para garantir que os dados sejam removidos de um dispositivo.

Para remover o aplicativo:

1. Na janela principal do Kaspersky Next Expert View (cloud), selecione **Gerenciamento de ativos** → **Móvel** → **Dispositivos**.
2. Na lista de dispositivos exibida, selecione um dispositivo para o qual você deseja enviar um comando.

É possível selecionar vários dispositivos.

3. Clique em **Enviar comando**.
4. Na janela **Enviar comando** que se abre, no campo **Comando**, selecione **Redefinir as configurações padrão**.
5. Clique em **Enviar**.

Você pode visualizar e cancelar comandos no **Histórico de comandos**.

O comando é enviado aos dispositivos selecionados. O Kaspersky Endpoint Security for Android é removido desses dispositivos.

6. Na lista de dispositivos, selecione o dispositivo e clique em **Excluir**.

O dispositivo é removido da lista de dispositivos gerenciados no Kaspersky Next Expert View (cloud).

Caso o dispositivo não seja removido do Kaspersky Next Expert View (cloud), pode haver problemas com a instalação adicional de aplicativos da Kaspersky neste dispositivo.

Gerenciamento de dispositivos móveis no Kaspersky Next Expert View (cloud)

Para executar a configuração centralizada de dispositivos móveis, você deve configurar políticas. Uma política é um conjunto de configurações de segurança para gerenciar dispositivos móveis de sistemas e modos operacionais específicos dentro de um grupo de administração, e para gerenciar os aplicativos móveis instalados nesses dispositivos.

Esta seção descreve como criar grupos de administração, configurar políticas para dispositivos móveis e conectar dispositivos móveis ao Kaspersky Security Center para gerenciá-los posteriormente.

Criação de grupos de administração

Para aplicar a política a um grupo de dispositivos, recomenda-se criar um grupo separado para esses dispositivos antes de instalar aplicativos de gerenciamento neles.

Um *grupo de administração* é um conjunto lógico de dispositivos gerenciados combinados na base de um tratado específico com o propósito de gerenciar os dispositivos agrupados como uma unidade única dentro do Kaspersky Security Center.

Todos os dispositivos gerenciados dentro de um grupo de administração são configurados para fazer o seguinte:

- Use as mesmas configurações, que você pode definir nas [políticas](#).
- Use um modo de operação comum para todos os aplicativos por meio da criação de tarefas de grupo com configurações especificadas. Exemplos de tarefas de grupo incluem criar e instalar um pacote de instalação comum, atualizar os bancos de dados e módulos de aplicativos, verificar dispositivo sob demanda e ativar a proteção em tempo real.

Um dispositivo gerenciado pode pertencer a um somente grupo de administração.

Você pode criar hierarquias que têm qualquer grau de aninhamento para Servidores de Administração e grupos. Um único nível de hierarquia pode incluir Servidores de Administração secundários e virtuais, grupos e dispositivos gerenciados. Você também pode migrar dispositivos de um grupo para outro.

Imediatamente após a instalação do Kaspersky Security Center, a hierarquia dos grupos de administração contém apenas um grupo de administração chamado Dispositivos gerenciados. Ao criar uma hierarquia de grupos de administração, você poderá adicionar dispositivos ao grupo Dispositivos gerenciados, e adicionar grupos aninhados.

Para criar um grupo de administração:

1. Na janela principal do Kaspersky Next Expert View (cloud), selecione **Gerenciamento de ativos > Hierarquia de grupos**.
2. Na estrutura do grupo de administração, selecione o grupo de administração ao qual pertencerá o novo grupo.
3. Clique em **Adicionar**.
4. Na janela **Nome do novo grupo de administração** que se abre, insira um nome para o grupo e clique em **Adicionar**.

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

Para criar automaticamente a estrutura de grupos de administração:

1. Na janela principal do Kaspersky Next Expert View (cloud), selecione **Gerenciamento de ativos > Hierarquia de grupos**.
2. Clique em **Importar**.

O Assistente de nova estrutura de grupos de administração é iniciado. Siga as instruções do assistente.

Após criar um grupo de administração, recomenda-se configurar a opção de [alocar automaticamente os 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 específica.

Configurar políticas

Esta seção descreve como gerenciar políticas no Kaspersky Next Expert View (cloud).

Criar uma política

O Kaspersky Next Expert View (nuvem) permite criar políticas para definir as configurações de segurança de um grupo de dispositivos móveis Android e iOS. Os valores de configurações de segurança definidos na política são salvos no Servidor de Administração, distribuídos aos dispositivos móveis durante a sincronização e salvos nos dispositivos como configurações atuais.

Você pode criar políticas usando o assistente de política móvel.

Para criar uma política:

1. Na janela principal do Kaspersky Next Expert View (cloud), selecione **Gerenciamento de ativos → Políticas**.
2. Na estrutura de grupos de administração, selecione o [grupo de administração](#) para o qual você deseja criar uma política.
Por padrão, a nova política é aplicada ao grupo **Dispositivos móveis**.
3. Clique em **Adicionar** para iniciar o assistente de política móvel.

4. Na janela **Selecione o aplicativo**, selecione a opção **Kaspersky Mobile Devices Protection and Management** e clique em **Avançar**.

O assistente de política móvel é iniciado. Clique em **Iniciar** e prossiga pelo assistente usando os botões **Voltar** e **Avançar**.

Etapa 1. Licença

Nesta etapa, escolha uma licença.

A licença escolhida determina as configurações de segurança que você pode definir em uma política. Por padrão, a licença compatível com a funcionalidade MDM básico no Kaspersky Next Expert View (cloud) é selecionada previamente. Você pode escolher uma licença diferente manualmente.

Etapa 2. Sistemas operacionais especificados e modos de operação dos dispositivos

Nesta etapa, escolha os sistemas operacionais aos quais a política será aplicada e especifique os modos de operação dos dispositivos.

- **Android** (proteção de dispositivos Android e configurações para o contêiner corporativo)
- **iOS**
 - Kaspersky Protection for iOS (proteção contra ameaças da Web e detecção de jailbreak em dispositivos iOS)
 - Perfil de gerenciamento (configurações básicas e avançadas para gerenciar dispositivos iOS)

Para obter informações detalhadas, consulte a seção [Sobre os modos de operação de dispositivos iOS](#).

Para conectar dispositivos iOS no modo de operação "Perfil de gerenciamento", é necessário ter [um Servidor de MDM do iOS](#) instalado.

Para o modo de operação "Kaspersky Protection for iOS", é possível criar um grupo de administração separado sem o Servidor de MDM do iOS e distribuir uma política.

Para o modo de operação "Perfil de gerenciamento", é possível criar grupos de administração com diferentes Servidores de MDM do iOS e distribuir políticas diferentes, respectivamente.

1. No campo **Nome**, insira o nome da nova política. Se você especificar o nome de uma política existente, (1) será adicionado automaticamente no final do nome.
2. No bloco de configurações **Status da política**, selecione o status da política:
 - **Ativo**. O assistente salva a política criada no Servidor de Administração. Na próxima sincronização de dispositivos móveis com o Servidor de Administração, a política será usada nos dispositivos como uma política ativa.
 - **Inativo**. 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.

3. No bloco de configurações **Herança de configurações**, selecione as opções de herança:

- **Herdar configurações da política principal**

Se você ativar essa opção em uma política secundária e um administrador bloquear algumas configurações na política principal, você não poderá alterar essas configurações na política secundária.

Se você desativar essa opção em uma política secundária, você poderá alterar todas as configurações na política secundária, mesmo se algumas configurações estiverem bloqueadas na política principal.

- **Forçar herança de configurações nas políticas secundárias**

Se você ativar essa opção em uma política principal, a opção **Herdar configurações da política principal** é ativada em todas as políticas secundárias. 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.

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

A herança das configurações de políticas funciona somente se modos de operação dos dispositivos iguais forem selecionados para a política principal e secundária, ou se os modos operacionais dos dispositivos selecionados para a política secundária fornecerem mais configurações de segurança. Por exemplo, uma política secundária para dispositivos Android com um contêiner corporativo pode herdar configurações de uma política principal para dispositivos pessoais, mas não pode herdar configurações de uma política principal para dispositivos corporativos.

Se você criar uma política secundária que seja incompatível com a política principal, deverá excluí-la e criar uma nova política secundária para gerenciar os dispositivos.

4. Clique em **Salvar**.

A nova política para dispositivos móveis foi criada.

Modificar uma política

O Kaspersky Next Expert View (cloud) permite modificar políticas.

Para modificar uma política:

1. Abra a janela de propriedades da política da seguinte maneira:

- Na janela principal do Kaspersky Next Expert View (cloud), selecione **Gerenciamento de ativos** → **Políticas**. Na lista de políticas de grupo que se abre, clique no nome da política que deseja modificar.
- Na janela principal do Kaspersky Next Expert View (cloud), selecione **Gerenciamento de ativos** → **Móvel** → **Dispositivos**. Clique no dispositivo móvel que se enquadra na política que deseja modificar e, em seguida, selecione a política na guia **Políticas e perfis de política ativos**.

2. Na janela de propriedades da política, vá até a guia **Configurações do aplicativo** e defina as configurações da política.

Também é possível definir configurações gerais, herança de configurações, notificações e log de eventos e perfis de política, além de visualizar o histórico de revisões. Para obter mais informações, consulte a [Ajuda do Kaspersky Security Center](#) ².

Não é possível configurar por quanto tempo os eventos são armazenados no dispositivo móvel do usuário. O período de retenção do log de eventos no dispositivo é ilimitado. No entanto, o tamanho é limitado: quando o log de eventos atingir 200 entradas, as 50 entradas mais antigas serão automaticamente excluídas do registro.

3. Clique em **Salvar** para salvar as alterações feitas na política e sair da janela de propriedades da política.

A política foi modificada. As configurações do dispositivo móvel são definidas após a próxima sincronização do dispositivo com o Kaspersky Security Center.

Copiar uma política

O Kaspersky Next Expert View (cloud) permite criar uma cópia de uma política.

Para criar uma cópia de uma política:

1. Na janela principal do Kaspersky Next Expert View (cloud), selecione **Gerenciamento de ativos** → **Políticas**.
2. Na lista de políticas que se abre, marque a caixa de seleção ao lado do nome da política que deseja copiar e clique em **Copiar**.
3. Na árvore de grupos de administração que se abre, selecione o grupo de destino em que você deseja que a política seja criada.
É possível criar um novo grupo de administração selecionando um grupo existente e clicando em **Adicionar grupo subordinado**.
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 para o 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 sufixo (<próximo número da sequência>) é adicionado ao nome da política recém-criada ou movida, por exemplo: (1).

Mover uma política para outro grupo de administração

O Kaspersky Next Expert View (cloud) permite mover uma política para outro grupo de administração.

Para mover uma política para outro grupo de administração:

1. Na janela principal do Kaspersky Next Expert View (cloud), selecione **Gerenciamento de ativos** → **Políticas**.
2. Na lista de políticas que se abre, 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 subordinado**.
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 da política será criada no grupo-alvo.

O status de cada política copiada ou movida para o 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 sufixo (<próximo número da sequência>) é adicionado ao nome da política recém-criada ou movida, por exemplo: (1).

Visualização da lista de políticas

O Kaspersky Next Expert View (cloud) permite visualizar a lista de políticas criadas, seus status e as propriedades correspondentes.

Para exibir a lista de políticas:

1. Na janela principal do Kaspersky Next Expert View (cloud), selecione **Gerenciamento de ativos** → **Políticas**.
2. A lista de políticas é exibida com informações breves sobre elas. Nessa página, é possível criar, modificar, copiar, mover e excluir políticas.

Visualizar resultados da distribuição da política

O Kaspersky Next Expert View (cloud) permite visualizar o gráfico de distribuição de uma política e as informações sobre todos os dispositivos que se enquadram nela.

Para visualizar os resultados da distribuição de uma política:

1. Na janela principal do Kaspersky Next Expert View (cloud), selecione **Gerenciamento de ativos** → **Políticas**.
2. Na lista de políticas que se abre, marque a caixa de seleção ao lado do nome da política para a qual deseja ver os resultados de distribuição e clique em **Distribuição**.

A página de resultados da distribuição da política é exibida. Essa página contém o resumo da política, um gráfico de distribuição da política e uma tabela com informações sobre todos os dispositivos que se enquadram nela. Você pode abrir a janela de propriedades da política clicando no botão **Configurar política**.

Gerenciar as revisões de políticas

O Kaspersky Next Expert View (cloud) permite visualizar as modificações feitas em uma política durante um determinado período, além de salvar as informações sobre essas modificações em um arquivo.

Para visualizar uma revisão da política:

1. Na janela principal do Kaspersky Next Expert View (cloud), selecione **Gerenciamento de ativos** → **Políticas**.
2. Na lista de políticas exibida, clique na política cuja revisão você deseja visualizar e, em seguida, vá para a seção **Histórico de revisões**.
3. Na lista de revisões de política, clique no número da revisão que deseja visualizar.

Caso o tamanho da revisão seja superior a 10 MB, não será possível visualizá-la usando o Kaspersky Next Expert View (cloud). Você será solicitado a salvar a revisão selecionada em um arquivo JSON.

Se o tamanho da revisão não exceder 10 MB, um relatório no formato HTML com as configurações da revisão da política selecionada será exibido. O relatório é exibido em uma janela pop-up, então assegure-se de que os pop-ups sejam permitidos em seu navegador.

Para salvar uma revisão de política em um arquivo JSON, na lista de revisões de política, selecione a revisão que deseja salvar e clique em **Salvar no arquivo**.

A revisão é salva em um arquivo JSON.

Para obter informações detalhadas sobre o gerenciamento de revisões de políticas, consulte a [Ajuda do Kaspersky Security Center](#).

Restringir permissões para configurar políticas

Os administradores do Kaspersky Security Center podem configurar as permissões de acesso dos usuários do Kaspersky Next Expert View (cloud) para diferentes funções da solução MDM básico no Kaspersky Next Expert View (cloud), dependendo das atribuições de trabalho dos usuários.

Na interface do Kaspersky Next Expert View (cloud), é possível configurar os direitos de acesso nas guias **Segurança** e **Funções do usuário** da janela de propriedades do Servidor de Administração. 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.

Para cada área funcional, o administrador pode atribuir as seguintes permissões:

- **Permitir editar.** O usuário do Kaspersky Next Expert View (cloud) está autorizado a alterar as configurações da política na janela de propriedades.
- **Bloquear a edição.** O usuário do Kaspersky Next Expert View (cloud) 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.

Configurar o controle de acesso baseado em função

O Kaspersky Next Expert View (cloud) oferece recursos para acesso de acordo com a função dos recursos do MDM básico no Kaspersky Next Expert View (cloud).

É possível configurar os direitos de acesso aos recursos do aplicativo do MDM básico no Kaspersky Next Expert View (cloud) por meio de uma das seguintes maneiras:

- Configurando os direitos para cada usuário ou grupo de usuários individualmente.
- Criando funções de usuário padrão com um conjunto predefinido de direitos e atribuindo tais funções aos usuários dependendo do escopo de obrigações deles.

A aplicação de funções de usuário tem como objetivo simplificar e reduzir os procedimentos de rotina de configuração de direitos de acesso dos usuários aos recursos do aplicativo. Os direitos de acesso com em uma função são configurados de acordo com as tarefas "padrão" e o escopo de deveres do usuário.

As funções de usuários podem ter nomes que correspondem a suas finalidades respectivas. Você pode criar um número ilimitado de funções no aplicativo. É possível usar as funções de usuário predefinidas com um conjunto de direitos já configurado ou criar novas funções e configurar os direitos necessários por conta própria.

Para obter informações detalhadas sobre a configuração de acesso do usuário no Kaspersky Security Center, consulte a [Ajuda do Kaspersky Security Center](#).

Algumas das funções de usuário predefinidas não estão autorizadas a funcionar com dispositivos móveis. As funções do usuário predefinidas e disponíveis para o MDM básico no Kaspersky Next Expert View (cloud) estão listadas na tabela abaixo.

Funções do usuário predefinidas para o MDM básico no Kaspersky Next Expert View (cloud)

Função	Leitura	Gravação	Gerenciamento de chaves de licença: criar políticas e modificar configurações de chave de licença	Gerenciamento de patches e vulnerabilidades: visualizar EULAs não aceitos e aceitar EULAs
Administrador do Kaspersky Endpoint Security	+	+	-	-
Operador do Kaspersky Endpoint Security	+	-	-	-
Administrador Principal	+	+	-	-
Operador Principal	+	-	-	-
Administrador do Gerenciamento de Dispositivos Móveis	+	+	+	+
Operador do Gerenciamento de Dispositivos Móveis	+	-	-	-

Para obter informações detalhadas sobre funções de usuário predefinidas, consulte a [Ajuda do Kaspersky Security Center](#).

Área funcional	Direito
Kaspersky Mobile Devices Protection and Management > Kaspersky Next Expert View (cloud) > Configuração do aplicativo	• Leitura: obter acesso de leitura a todas as configurações na seção de política correspondente. • Gravação: obter acesso de gravação a todas as configurações na seção de política correspondente. Observe que, para definir as configurações de Proteção na Web e Controle da Web, o administrador deve ter direitos de leitura e gravação para as áreas funcionais dos controles de proteção e de segurança.
Kaspersky Mobile Devices Protection and Management > Kaspersky Next Expert View (cloud) > Controles de segurança	
Kaspersky Mobile Devices Protection and Management > Kaspersky Next Expert View (cloud) > Contêiner corporativo	
Kaspersky Mobile Devices Protection and Management > Kaspersky Next Expert View (cloud) > Configuração do dispositivo	
Kaspersky Mobile Devices Protection and Management > Kaspersky Next Expert View (cloud) > Configuração dos aplicativos de gerenciamento de dispositivos da Kaspersky	
Kaspersky Mobile Devices Protection and Management > Kaspersky Next Expert View (cloud) > Proteção	
Kaspersky Mobile Devices Protection and Management > Kaspersky Next Expert View (cloud) > Restrições	
Kaspersky Mobile Devices Protection and Management > Kaspersky Next Expert View (cloud) > Configurações do Samsung Knox	

Direitos de acesso ao Gerenciamento de Dispositivos Móveis

Direito	Ação do usuário: são necessários direitos para executar a ação
Gerenciamento de Dispositivos Móveis > Geral > Leitura	• Exibir a seção Móvel no Kaspersky Next Expert View (cloud)
Gerenciamento de Dispositivos Móveis > Geral > Gravação	• Executar qualquer ação com certificados (exceto exibir certificados) O direito Gerenciar certificados também deve ser concedido. • Definir as configurações do Firebase Cloud Messaging.
Gerenciamento de Dispositivos Móveis > Geral > Conectar novos dispositivos	• Conectar novos dispositivos móveis e Servidores de MDM do iOS • Excluir dispositivos
Gerenciamento de Dispositivos Móveis > Geral > Gerenciar certificados	• Executar qualquer ação com certificados • Configurar as regras de emissão do certificado O direito de Gravação também deve ser concedido.
Gerenciamento de Dispositivos Móveis > Geral > Enviar somente comandos de informação a dispositivos móveis	• Enviar e cancelar o comando Sincronizar o dispositivo
Gerenciamento de Dispositivos Móveis > Geral > Enviar comandos para dispositivos móveis	• Enviar e cancelar qualquer comando

Configurar perfis de política

Às vezes, pode ser necessário criar e modificar centralmente várias instâncias de uma única política para um grupo de administração. Essas instâncias podem diferir por apenas uma ou duas configurações.

Para ajudar a evitar a criação de várias instâncias de uma única política, o Kaspersky Next Expert View (cloud) permite criar perfis de política. Os perfis de política são destinados se você quiser que os dispositivos dentro de um grupo de administração único executem sob configurações de política diferentes.

Um perfil da política é um subconjunto denominado como configurações da política. Este subconjunto é distribuído em dispositivos alvo em conjunto com a política, complementando-a em uma condição específica denominada como condição de ativação do perfil. Os perfis somente contêm configurações que se diferenciam da política "básica", que está ativa no dispositivo gerenciado. A ativação de um perfil modifica as configurações da política "básica" que estavam inicialmente ativas no dispositivo. As configurações modificadas assumem valores que foram especificados no perfil.

Você pode modificar as condições específicas que devem afetar a [ativação do perfil da política](#) que você está criando. Para dispositivos móveis, você pode modificar as seguintes condições:

- **Regras para o proprietário do dispositivo específico**

Ativação do perfil no dispositivo de acordo com seu proprietário.

- Proprietário do dispositivo
- O proprietário do dispositivo está incluído em um grupo de segurança interno

- **Regras para atribuição de funções**

Ativação do perfil no dispositivo, dependendo da função do proprietário.

- Ativar o perfil de política por função específica do proprietário do dispositivo

- **Regras para uso de tag**

Ativação do perfil no dispositivo, dependendo das tags atribuídas ao dispositivo.

- Lista de tags
- Aplicar aos dispositivos sem tags especificadas

- **Regras para uso do Active Directory**

Ativação do perfil da política no dispositivo com base na alocação do dispositivo em uma unidade organizacional do Active Directory ou na associação desse dispositivo (ou do proprietário do dispositivo) a um grupo de segurança do Active Directory. O escopo da configuração depende da política usada atualmente.

- Associação do proprietário do dispositivo em um grupo de segurança do Active Directory
- Associação do dispositivo no grupo de segurança do Active Directory
- A alocação do dispositivo está na unidade organizacional do Active Directory

Para obter informações detalhadas sobre como configurar regras de ativação, criar, excluir ou copiar perfis de política, consulte a [Ajuda do Kaspersky Security Center](#).

Excluir uma política

O Kaspersky Next Expert View (cloud) permite excluir políticas.

É possível excluir apenas as políticas que não sejam herdadas no [grupo de administração](#) atual. Se uma política for herdada, você só poderá excluí-la no grupo de nível superior para o qual ela foi criada.

Para excluir uma política:

1. Na janela principal do Kaspersky Next Expert View (cloud), selecione **Gerenciamento de ativos** → **Políticas**.
2. Na lista de políticas que se abre, marque a caixa de seleção ao lado do nome da política que deseja excluir e clique em **Excluir**.
3. Na janela que se abre, clique em **OK** para confirmar a operação.

A política foi excluída. Antes de aplicar a nova política, os dispositivos móveis que pertencem ao grupo de administração continuam a funcionar de acordo com as configurações especificadas na política que foi excluída.

Conexão de dispositivos móveis ao Kaspersky Next Expert View (cloud)

Para gerenciar dispositivos móveis e os aplicativos de gerenciamento de dispositivos móveis instalados neles, você deve conectá-los ao Kaspersky Security Center.

Antes de conectar, assegure-se de que a licença que oferece suporte à solução de gerenciamento de dispositivos móveis esteja configurada na seção [Chaves de licença](#) das propriedades do Servidor de Administração.

Para conectar um dispositivo móvel ao Kaspersky Security Center:

1. Na janela principal do Kaspersky Next Expert View (cloud), selecione **Gerenciamento de ativos** → **Móvel** → **Dispositivos**.
2. Na lista de dispositivos móveis exibida, clique em **Adicionar**.
O Assistente de conexão de novos dispositivos móveis é iniciado. Clique em **Iniciar** e prossiga pelo assistente usando os botões **Voltar** e **Avançar**.

Boas-vindas

Na tela de boas-vindas, você pode ler um resumo das etapas do Assistente de conexão de dispositivos móveis.

Etapa 1. Política

Nesta etapa, escolha uma política para os dispositivos que vão se conectar. Eles operam conforme as configurações de segurança [especificadas na política](#).

- **Usar uma política existente**

Para essa opção, especifique o grupo de administração da política que você deseja escolher. O nome da política, os sistemas operacionais e os modos operacionais dos dispositivos gerenciados por essa política serão exibidos.

Se necessário, clique em **Ir para a política** para visualizar as propriedades da política selecionada.

- **Criar uma nova política**

Para essa opção, clique no botão **Criar política** que é exibido. Você será redirecionado para o [assistente de política móvel](#). Após a criação de uma política com as propriedades necessárias, você pode retornar ao assistente de conexão de dispositivos móveis.

Etapa 2. Sistemas operacionais

Nesta etapa, escolha os sistemas operacionais dos dispositivos que vão se conectar. As configurações da política determinam os sistemas operacionais disponíveis: Android ou iOS.

- **Android**

- **iOS**

Para conectar dispositivos iOS no modo de operação "Perfil de gerenciamento", é necessário ter [um Servidor de MDM do iOS](#) instalado.

O aplicativo *Kaspersky Protection for iOS* será instalado em dispositivos iOS pessoais no modo de operação "Kaspersky Protection for iOS".

Um [perfil de gerenciamento](#) será instalado nos dispositivos no modo de operação "Perfil de gerenciamento".

Em dispositivos móveis que executam iOS 12.1 ou posterior, é necessário confirmar manualmente a instalação de um perfil de gerenciamento em um dispositivo móvel. Você também deve conceder a permissão de gerenciamento remoto do dispositivo.

Etapa 3. Aceitar os contratos

Nesta etapa, escolha quem deve aceitar o Contrato de Licença de Usuário Final (EULA) e a Política de Privacidade.

- **Administrador**

Os contratos são aceitos pelo administrador na próxima etapa do assistente. Nesse caso, o aplicativo ignora a etapa de aceitação durante a instalação do aplicativo.

- **Usuários**

Os acordos são aceitos nos dispositivos móveis pelos usuários.

Observe que o administrador será solicitado a aceitar o EULA somente depois que a mesma versão do EULA for aceita pelos usuários nos dispositivos pela primeira vez. Após a conexão e a primeira sincronização de dispositivos com o Kaspersky Security Center, o administrador poderá aceitar essa versão do EULA na conexão subsequente dos dispositivos.

A lista de contratos aceitos está disponível na seção **Contratos de Licença de Usuário Final** das propriedades do Servidor de Administração.

Etapa 4. Contrato de Licença de Usuário Final e Política de Privacidade

Nesta etapa, se o **Administrador** for selecionado como o destinatário dos contratos na etapa anterior do assistente, você será solicitado a ler a Política de Privacidade, o EULA e todos os documentos associados a eles. Você deve aceitar os termos e as condições do EULA e da Política de Privacidade antes da instalação dos aplicativos de gerenciamento de dispositivos móveis.

Etapa 5. Usuários

Nesta etapa, escolha um ou mais usuários dos dispositivos que serão conectados. Eles receberão as informações para instalar o aplicativo para conectar seus dispositivos ao Kaspersky Security Center. Se um usuário não estiver na lista, é possível adicionar uma nova conta de usuário sem sair do assistente.

- Para escolher um usuário existente, marque as caixas de seleção ao lado dos nomes de usuário correspondentes.
- Para adicionar um novo usuário, clique em **Adicionar um usuário**.
 - a. Especifique as credenciais do usuário no bloco de configurações **Credenciais**.
 - **Nome de usuário**
 - **Senha**

A senha deve cumprir os seguintes requisitos de complexidade:

 - Conter de 8 a 16 caracteres.
 - Conter os caracteres de pelo menos três destes grupos: letras maiúsculas (AZ), letras minúsculas (az), dígitos (0-9), caracteres especiais (@ # \$ % ^ & * - _ ! + = [] { } | : ' . , ? / \ ` ~ " () ;).
 - b. Se necessário, especifique detalhes opcionais no grupo de configurações **Informações opcionais**.
 - **Nome completo do usuário**
 - **Descrição**
 - **Endereço de e-mail**
 - **Número de telefone**

c. Clique em **OK** para salvar as alterações.

O novo usuário será adicionado e exibido na lista de usuários.

- Para modificar os detalhes do usuário, clique em **Editar usuário**.

Os campos que podem ser modificados dependem do subtipo de usuário: *interno* ou *domínio*.

Depois que o dispositivo for conectado, não será possível definir outro usuário como proprietário nem remover o usuário atribuído. No entanto, se você não tiver atribuído um usuário ao conectar o dispositivo, poderá atribuir o usuário mais tarde enviando [um certificado de dispositivos móveis](#).

Etapa 6. Enviar informações da conexão

Nesta etapa, escolha como enviar os códigos QR e links para a instalação dos aplicativos de gerenciamento de dispositivos móveis ou os perfis de gerenciamento. Você pode escolher uma das seguintes opções:

- **Enviar uma mensagem aos e-mails dos usuários**

Escolha essa opção para enviar o detalhes da conexão por e-mail para os usuários selecionados. Para instalar o aplicativo ou um perfil de gerenciamento, o usuário precisa ler o código QR usando a câmera do dispositivo móvel ou abrir o link para o pacote de instalação.

Esses endereços de e-mail devem ser especificados nas configurações da conta do usuário no Kaspersky Security Center.

Se você quiser enviar os detalhes da conexão para um endereço de e-mail não especificado nas configurações da conta do usuário no Kaspersky Security Center, marque a caixa de seleção **Enviar uma cópia da mensagem para um e-mail alternativo** e especifique o endereço de e-mail necessário.

- **Mostrar códigos QR e links após a conclusão do assistente**

Escolha essa opção para verificar o código QR com a câmera do dispositivo móvel ou siga o link no assistente.

Etapa 7. Confirmar

Nessa etapa, verifique os detalhes da conexão do dispositivo móvel especificados nas etapas anteriores e clique em **Concluir** para confirmar a operação.

Se você selecionar um grande número de usuários ou grupos de usuários, a criação de códigos QR e links de conexão poderá levar vários minutos.

Concluir

Na tela Concluir:

- Se você escolheu a opção **Enviar uma mensagem aos e-mails dos usuários**, os usuários especificados receberão os e-mails com códigos QR e links para conectar os dispositivos móveis ao Servidor de Administração.
- Se você escolheu a opção **Mostrar códigos QR e links após a conclusão do assistente**, os detalhes da conexão estarão disponíveis na tela Concluir. Você pode visualizar os detalhes exibidos ou clicar em **Baixar a lista** para receber um arquivo com as informações resumidas.

Clique em **Fechar** para sair do assistente.

Assim que os usuários instalam os aplicativos de gerenciamento de dispositivos móveis, os seus dispositivos serão conectados ao Servidor de Administração e exibidos na guia **Dispositivos** do Kaspersky Next Expert View (cloud).

Agora você pode definir as configurações para dispositivos e aplicativos de gerenciamento de dispositivos móveis usando políticas. É possível também enviar comandos para dispositivos móveis para proteção de dados, caso os dispositivos sejam perdidos ou roubados.

Fazer uma conexão direta de dispositivos Android ao Kaspersky Security Center

Os dispositivos Android podem conectar-se diretamente à porta 13292 do Servidor de Administração.

Dependendo do método usado para autenticação, duas opções de conexão são possíveis.

Conectar dispositivos com um certificado do usuário

Ao conectar um dispositivo com um certificado do usuário, o dispositivo é associado com a conta de usuário à qual o certificado correspondente foi atribuído através das ferramentas do Servidor de Administração.

Neste caso, a autenticação SSL de duas vias (autenticação mútua) será usada. Tanto o Servidor de Administração quanto o dispositivo serão autenticados com certificados.

Conectar dispositivos sem um certificado do usuário

Ao conectar um dispositivo sem um certificado do usuário, o dispositivo não se associa com nenhuma das contas de usuário no Servidor de Administração. No entanto, quando o dispositivo recebe qualquer certificado, ele é associado ao usuário ao qual o certificado correspondente foi atribuído através das ferramentas do Servidor de Administração.

Ao conectar aquele dispositivo ao Servidor de Administração, a autenticação SSL bilateral será aplicada, o que significa que somente o Servidor de Administração será autenticado com o certificado. Após o dispositivo recuperar o certificado do usuário, o tipo de autenticação mudará para a autenticação SSL bilateral (autenticação bilateral SSL, autenticação mútua).

Movimentação de dispositivos móveis não atribuídos para grupos de administração

Quando os dispositivos móveis estão conectados ao Kaspersky Security Center, eles são exibidos na página **Descoberta e implementação > Dispositivos não atribuídos** do Kaspersky Next Expert View (cloud). Para gerenciar os dispositivos recém-conectados, é possível criar uma regra que os aloca automaticamente aos 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 Next Expert View (cloud), selecione **Descoberta e implementação > Dispositivos não atribuídos**.
2. Selecione o dispositivo que deseja migrar para um grupo de administração e clique em **Migrar para 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 subordinado**.
4. Clique em **Mover**.

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

Ações em dispositivos móveis para fazer a conexão com o Servidor de Administração

Dependendo do modo no qual seu dispositivo irá operar, pode ser necessário executar ações adicionais para garantir a proteção do dispositivo e conectá-lo ao Servidor de Administração.

Instalar um certificado de dispositivos móveis

Se você recebeu uma senha de certificado, deve usá-la para instalar o certificado de dispositivos móveis em seu dispositivo.

Para instalar o certificado de dispositivos móveis:

1. Lembre-se ou anote a senha que você recebeu do administrador por e-mail.
2. Execute uma das seguintes ações:
 - Em um dispositivo Android, insira a senha do certificado quando solicitado pelo Kaspersky Endpoint Security for Android.
 - Em um dispositivo iOS, insira a senha do certificado durante a instalação do perfil de gerenciamento do dispositivo.

O certificado de dispositivos móveis será instalado em seu dispositivo.

Pré-configurar dispositivos Android corporativos

Para conectar um dispositivo Android corporativo ao Servidor de Administração, você deve pré-configurar o dispositivo de acordo com a versão do sistema operacional e da disponibilidade de um leitor de código QR.

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 é executada usando o protocolo HTTPS. A sincronização do dispositivo móvel com o Servidor de Administração pode ser executada nas seguintes formas:

- **Por agendamento.** É possível configurar o agendamento da sincronização nas configurações da política. As modificações nas configurações da política, os comandos e tarefas serão executados quando o dispositivo for sincronizado com o Kaspersky Security Center de acordo com o agendamento, por exemplo, com um atraso.

Devido às [limitações do Doze](#), quando você seleciona um período de sincronização curto, os dispositivos podem sincronizar com o Servidor de Administração com menos frequência do que o esperado.

Usar períodos de sincronização curtos diminui a vida útil da bateria do dispositivo.

- **Forçada.** A sincronização é executada usando notificações push do FCM (Firebase Cloud Messaging). A sincronização forçada é principalmente destinada para a entrega oportuna de [comandos a um dispositivo móvel](#). Isso pode ser útil quando um dispositivo móvel está no modo de economia de bateria, porque nesse caso o aplicativo pode executar tarefas depois do que o especificado. Se você quiser usar a sincronização forçada, assegure-se de que as [definições de FCM estejam configuradas](#) no Kaspersky Security Center.

Use o comando [Sincronizar o dispositivo](#) para forçar a sincronização de um dispositivo Android ou um dispositivo iOS MDM.

O botão [Forçar a sincronização](#) e a caixa de seleção [Não desconectar do Servidor de Administração](#) na janela de propriedades do dispositivo não são compatíveis com dispositivos móveis.

Para definir as configurações de sincronização nos dispositivos Android:

1. Na janela principal do Kaspersky Next Expert View (cloud), selecione **Gerenciamento de ativos** → **Políticas**. Na lista de políticas de grupo aberta, clique no nome da política que deseja configurar.
2. Na janela de propriedades da política, selecione **Configurações do aplicativo**.
3. Selecione **Android** e vá até a seção **Configurações do KES for Android**.
4. No cartão **Sincronização programada**, clique em **Configurações**.
A janela **Sincronização programada** será aberta.
5. Ative a sincronização usando o botão **Sincronização programada**.
6. Na lista suspensa **Período de sincronização**, selecione o tempo entre as sincronizações dos dispositivos com o Kaspersky Security Center. O valor padrão é de 3 horas.
7. Para desativar a sincronização dos dispositivos com o Kaspersky Security Center quando estiver em roaming, marque a caixa de seleção **Não sincronizar enquanto estiver em roaming**.

O usuário ainda pode realizar a sincronização manualmente nas configurações do aplicativo (**Configurações** → **Configurações do aplicativo** → **Sincronização** → **Sincronizar**).

8. Clique em **OK**.

9. Clique em **Salvar** para salvar as alterações efetuadas.

As configurações do dispositivo móvel são alteradas após a próxima sincronização do dispositivo com o Kaspersky Security Center. Você pode sincronizar manualmente o dispositivo móvel [usando um comando especial](#).

Para definir as configurações de sincronização para dispositivos iOS que operam no modo "Kaspersky Protection for iOS":

1. Na janela principal do Kaspersky Next Expert View (cloud), selecione **Gerenciamento de ativos** → **Políticas**. Na lista de políticas de grupo aberta, clique no nome da política que deseja configurar.
2. Na janela de propriedades da política, selecione **Configurações do aplicativo**.
3. Selecione **iOS** e vá para a seção **KP para as configurações do iOS**.
4. No cartão **Sincronização programada**, clique em **Configurações**.
A janela **Sincronização programada** será aberta.
5. Ative a sincronização usando o botão **Sincronização programada**.
6. Na lista suspensa **Período de sincronização**, selecione o tempo entre as sincronizações dos dispositivos com o Kaspersky Security Center. O valor padrão é de 6 horas.
7. Clique em **OK**.
8. Clique em **Salvar** para salvar as alterações efetuadas.

As configurações do dispositivo móvel são alteradas após a próxima sincronização do dispositivo com o Kaspersky Security Center.

Em alguns dispositivos iOS, a sincronização em segundo plano pode ser executada depois do que o esperado se o usuário encerrar o Kaspersky Protection for iOS deslizando para cima no App Switcher. Para forçar uma sincronização, o usuário deve reabrir o aplicativo. Para obter mais informações sobre restrições e recomendações relacionadas à otimização da execução de tarefas em segundo plano, consulte a seção [problemas conhecidos do Kaspersky Protection for iOS](#).

Gerenciar certificados de dispositivos móveis

O Kaspersky Next Expert View (cloud) permite emitir, renovar ou excluir certificados móveis, de e-mail ou VPN de dispositivos móveis.

Esta seção contém informações sobre como gerenciar certificados de dispositivos móveis e configurar suas regras de emissão.

Configurar as regras de emissão do certificado

O Kaspersky Next Expert View (cloud) permite configurar como os certificados de dispositivos móveis são emitidos, renovados e protegidos.

Para configurar as regras de emissão de certificado:

1. Na janela principal do Kaspersky Next Expert View (cloud), selecione **Gerenciamento de ativos** → **Móvel** → **Certificados**.

2. Na lista de certificados exibida, clique em **Regras de emissão**.

- Na seção **Certificados de dispositivos móveis**, você pode:
 - a. No bloco de configurações **Validade**, no campo **Período de validade do certificado (dias)**, especifique a vida útil do certificado em dias. O tempo de vida padrão de um certificado é de 365 dias. Quando este período expirar, o dispositivo móvel não será capaz de conectar-se ao Servidor de Administração.
 - b. No bloco de configurações **Renovação**, no campo **Renove o certificado antes que expire em (dias)**, especifique o número de dias restantes até a expiração do certificado atual, quando o Servidor de Administração deve emitir um novo certificado. Por exemplo, se o valor do campo for 4, o Servidor de Administração emite um novo certificado quatro dias antes que o certificado atual expire. O valor padrão é 30.

Marque a caixa de seleção **Renovar o certificado automaticamente** para renovar certificados automaticamente. Caso essa opção seja desativada, os certificados devem ser renovados manualmente à medida que expiram. Essa caixa de seleção é marcada por padrão.
 - c. No bloco de configurações **Proteção por senha**, marque a caixa de seleção **Solicitar a senha durante a instalação do certificado** para solicitar ao usuário 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 tamanho da senha no campo **Comprimento da senha**.

A Proteção por senha está disponível somente para certificados de tipo móvel.

d. Clique em **Salvar** para aplicar as alterações.

As configurações especificadas serão usadas pelo Kaspersky Security Center para emitir, renovar e proteger os certificados de dispositivos móveis.

Emitir certificados de dispositivos móveis

Você pode emitir certificados de dispositivos móveis, de e-mail ou VPN para dispositivos móveis.

Para emitir um certificado:

1. Na janela principal do Kaspersky Next Expert View (cloud), selecione **Gerenciamento de ativos** → **Móvel** → **Certificados**.
2. Na lista de certificados exibida, clique em **Adicionar**.
O Assistente de instalação de certificado é iniciado. Clique em **Iniciar** e prossiga pelo assistente usando os botões **Voltar** e **Avançar**.

Boas-vindas

Na tela de boas-vindas, você pode ler um resumo das etapas do Assistente de emissão de certificado.

Observe que a numeração e o conjunto de etapas podem variar dependendo do tipo de certificado, do sistema operacional e das configurações de emissão definidas na seção [Regras de emissão](#).

Etapa 1. Tipo de certificado

Nesta etapa, escolha o certificado a ser emitido.

- **Certificado de correio** (para configurar o e-mail corporativo nos dispositivos).
- **Certificado VPN** (para configurar o acesso a redes privadas e recursos da Web corporativos nos dispositivos).
- **Certificado de dispositivos móveis** (para identificar dispositivos móveis no Servidor de Administração).

Etapa 2. Sistema operacional

Nesta etapa, escolha o sistema operacional dos dispositivos para os quais o certificado será emitido.

- **Android**
- **iOS**

Etapa 3. Método de conexão

Esta etapa é exibida somente se você selecionou **Certificado de correio** ou **Certificado VPN** como o tipo de certificado e **Android** como o sistema operacional dos dispositivos para os quais o certificado será emitido.

Nesta etapa, escolha o método para conectar os dispositivos ao Servidor de Administração.

- **Conectar usando a autenticação de certificado de dispositivos móveis**
Selecione essa opção se você quiser que o certificado de dispositivos móveis seja usado para identificar o usuário ao conectar-se ao Servidor de Administração.
- **Conectar sem a autenticação de certificado de dispositivos móveis**

Selecione essa opção se você quiser instalar um certificado em um dispositivo sem usar nenhuma autenticação de certificado.

Se houver um certificado de dispositivos móveis no dispositivo, ele sempre será usado para autenticação.

Etapa 4. Usuários

Nesta etapa, escolha um ou mais usuários que receberão as informações para instalar os certificados. Se um usuário não estiver na lista, é possível adicionar uma nova conta de usuário sem sair do assistente.

- Para escolher um usuário existente, marque as caixas de seleção ao lado dos nomes de usuário correspondentes.
- Para adicionar um novo usuário, clique em **Adicionar um usuário**.
 - a. Especifique as credenciais do usuário no bloco de configurações **Credenciais**.
 - **Nome de usuário**
 - **Senha**
A senha deve cumprir os seguintes requisitos de complexidade:
 - Conter de 8 a 16 caracteres.
 - Conter os caracteres de pelo menos três destes grupos: letras maiúsculas (AZ), letras minúsculas (az), dígitos (0-9), caracteres especiais (@ # \$ % ^ & * - _ ! + = [] { } | : ' , . ? / \ ` ~ " () ;).
 - b. Se necessário, especifique detalhes opcionais no grupo de configurações **Informações opcionais**.
 - **Nome completo do usuário**
 - **Descrição**
 - **Endereço de e-mail**
 - **Número de telefone**
 - c. Clique em **OK** para salvar as alterações.
O novo usuário será adicionado e exibido na lista de usuários.
- Para modificar os detalhes do usuário, clique em **Editar usuário**.

Os campos que podem ser modificados dependem do subtipo de usuário: *interno* ou *domínio*.

Etapa 5. Codinome e origem do certificado

Nesta etapa, escolha o codinome e a origem do certificado para importá-lo.

- **Codinome do certificado**

O *codinome de certificado* é um nome que identifica o certificado. Você pode usar o codinome selecionado posteriormente para definir as configurações das políticas: [Conta de e-mail para dispositivos iOS MDM](#); [Conta do Exchange ActiveSync para dispositivos iOS MDM](#); [Rede VPN para dispositivos iOS MDM](#) e [Rede Wi-Fi para dispositivos iOS MDM](#).

Esta opção é disponível somente se você selecionou **Certificado de correio** ou **Certificado VPN** como o tipo de certificado.

- **Carregar arquivo**

Para esta opção, especifique o **Formato do certificado**:

- Para o formato PKCS #12, no campo **Arquivo do certificado**, clique em **Selecionar** e especifique um arquivo P12 ou PFX.
- Para o formato X.509, no campo **Arquivo da chave privada**, clique em **Selecionar** e especifique um arquivo PRK ou PEM.

No campo **Arquivo do certificado**, clique em **Selecionar** e especifique um arquivo CER, CRT ou CERT.

Depois de especificar os arquivos, você também pode inserir a **Senha do certificado**.

Etapa 6. Método de autenticação

Esta etapa é exibida somente se você selecionou **Certificado de dispositivos móveis** como o tipo de certificado, ou se você selecionou **Certificado de correio** ou **Certificado VPN** para dispositivos Android e especificou a opção **Conectar sem a autenticação de certificado móvel** como o método de conexão.

Nesta etapa, escolha o método de autenticação do usuário para receber o certificado.

- **Credenciais de usuário interno ou de domínio.** Os usuários acessarão o certificado usando as credenciais de domínio ou de usuário interno. Em dispositivos móveis, os usuários terão que especificar o login em um dos seguintes formatos:
 - `userPrincipalName@DNSDomainName`
 - `sAMAccountName`
 - `sAMADomain\sAMAccountName`
- **Senha.** Os usuários acessarão o certificado usando uma senha enviada por e-mail ou exibida após a conclusão do assistente.

No bloco de configurações **Uso do certificado no 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)** se você quiser permitir o uso de um certificado várias vezes no mesmo dispositivo.

Esta opção está disponível somente se o **Android** foi escolhido como o sistema operacional dos dispositivos para os quais o certificado será emitido.

Etapa 7. Enviar informações do certificado

Nesta etapa, escolha como enviar as informações de instalação do certificado. Você pode escolher uma das seguintes opções:

- **Enviar uma mensagem aos e-mails dos usuários**

Escolha essa opção para enviar os detalhes da instalação do certificado por e-mail aos usuários selecionados. Esses endereços de e-mail devem ser especificados nas configurações da conta do usuário no Kaspersky Security Center.

Se você quiser enviar os detalhes da instalação do certificado para um endereço de e-mail não especificado nas configurações da conta do usuário no Kaspersky Security Center, marque a caixa de seleção **Enviar uma cópia da mensagem para um e-mail alternativo** e especifique o endereço de e-mail necessário.

- **Mostrar as informações após a conclusão do assistente**

Escolha esta opção para exibir os detalhes da instalação do certificado na etapa final do Assistente de emissão de certificado.

Etapa 8. Confirmar

Nesta etapa, verifique os detalhes de emissão do certificado especificados nas etapas anteriores e clique em **Confirmar e emitir o certificado** para confirmar a operação.

Concluir

Na tela Concluir:

- Se você escolheu a opção **Enviar uma mensagem aos e-mails dos usuários**, os usuários especificados receberão os e-mails com os detalhes da instalação do certificado.
- Se você escolheu a opção **Mostrar as informações após a conclusão do assistente**, os detalhes da instalação do certificado serão exibidos na tela Concluir. Você pode visualizar os detalhes exibidos ou clicar em **Baixar a lista** para receber um arquivo com as informações resumidas.

Clique em **Fechar** para sair do assistente.

Depois de concluir o Assistente de emissão de certificados, os certificados são criados e adicionados à lista de certificados do usuário. Você pode excluir ou renovar certificados, assim como visualizar suas propriedades.

Renovar certificados de dispositivos móveis

Caso um dos certificados esteja prestes a expirar, será possível renová-lo usando o Kaspersky Next Expert View (cloud). Seguindo as etapas abaixo, é possível renovar um certificado de dispositivos móveis.

Para renovar um certificado móvel:

1. Na janela principal do Kaspersky Next Expert View (cloud), selecione **Gerenciamento de ativos** → **Móvel** → **Certificados**.
2. Na lista de certificados exibida, selecione o certificado que deseja renovar e clique em **Renovar**.

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

Excluir certificados de dispositivos móveis

É possível excluir os certificados de dispositivos móveis usando o Kaspersky Next Expert View (cloud).

Observe que, caso um certificado de dispositivos móveis seja excluído, o dispositivo não poderá mais ser sincronizado com o Servidor de Administração e não poderá ser gerenciado por meio do Kaspersky Security Center.

Quando um certificado é excluído, ele é removido apenas do Kaspersky Next Expert View (cloud) e não é mais renovado, mas permanece no dispositivo. Para excluir um certificado de dispositivos iOS MDM, dispositivos corporativos ou dispositivos com contêiner corporativo, você deve executar o [comando Limpar os dados corporativos](#). Em dispositivos Android pessoais, os usuários devem excluir o certificado manualmente.

Quando um certificado de dispositivos móveis é excluído do dispositivo iOS MDM, o dispositivo não é removido do Kaspersky Next Expert View (cloud), mas perde a capacidade de sincronizar com o Servidor de MDM do iOS, e o status "Inativo" é atribuído a ele. Nesse caso, é necessário excluir o dispositivo da lista de dispositivos gerenciados no Kaspersky Next Expert View (cloud) e reconectá-lo por meio do [assistente de conexão de dispositivos móveis](#).

Para excluir um certificado do Kaspersky Next Expert View (cloud):

1. Na janela principal do Kaspersky Next Expert View (cloud), selecione **Gerenciamento de ativos** → **Móvel** → **Certificados**.
2. Na lista de certificados exibida, selecione o certificado que deseja excluir e clique em **Excluir**.

O certificado é excluído e removido da lista de certificados.

Visualizar lista de certificados de dispositivos móveis

O Kaspersky Next Expert View (cloud) permite visualizar os certificados de dispositivos móveis criados e suas propriedades.

Para ver a lista de todos os certificados e suas propriedades:

1. Na janela principal do Kaspersky Next Expert View (cloud), selecione **Gerenciamento de ativos** → **Móvel** → **Certificados**.
2. Na janela exibida, você pode visualizar a lista de todos os certificados criados e suas propriedades exibidas na tabela.

Para visualizar as propriedades de um certificado individual:

1. Na janela principal do Kaspersky Next Expert View (cloud), selecione **Gerenciamento de ativos** → **Móvel** → **Certificados**.
2. Na lista de certificados aberta, selecione o certificado cujas propriedades você deseja visualizar.

3. Na janela **Detalhes do certificado**, veja as propriedades do certificado:

- Nome de usuário
- Status
- Tipo
- Protocolo
- Origem
- Data de expiração
- Data de emissão
- Última atualização de status
- Codinome
- Renovação automática ativada
- Impressão digital

Para visualizar os certificados instalados em um dispositivo iOS MDM:

1. Na janela principal do Kaspersky Next Expert View (cloud), selecione **Gerenciamento de ativos** → **Móvel** → **Dispositivos**.
2. Na lista de dispositivos móveis exibida, selecione o dispositivo cujos certificados você deseja visualizar.
3. Na janela de propriedades do dispositivo que será aberta, escolha a seção **Certificados**.
A lista de certificados instalados no dispositivo e suas propriedades é exibida.

- Nome do certificado
- Certificado do usuário
- Impressão digital do certificado

Configuração e gerenciamento

Esta seção é destinada não só aos especialistas que administram o MDM básico no Kaspersky Next Expert View (cloud), mas também aos especialistas que fornecem Suporte Técnico a organizações que usam o MDM básico no Kaspersky Next Expert View (cloud).

Controle

Esta seção contém informações sobre como monitorar remotamente dispositivos móveis no Kaspersky Next Expert View (cloud).

Configurar restrições

Esta seção fornece instruções sobre como configurar o acesso do usuário aos recursos dos dispositivos móveis.

Configurar restrições de dispositivos iOS MDM

Para garantir a conformidade com os requisitos de segurança corporativa, configure as restrições na operação dos dispositivos iOS MDM.

Os recursos permitidos na seção **Restrições** da política, mas proibidos nos perfis de configuração instalados nos dispositivos não estão disponíveis nos dispositivos.

Configurar restrições de funções

Para configurar as restrições de funções de dispositivos iOS MDM:

1. Na janela principal do Kaspersky Next Expert View (cloud), selecione **Gerenciamento de ativos** → **Políticas**. Na lista de políticas de grupo aberta, clique no nome da política que deseja configurar.
2. Na janela de propriedades da política, selecione **Configurações do aplicativo**.
3. Selecione **iOS** e vá para a seção **Restrições**.
4. No cartão **Restrições de recursos do dispositivo**, clique em **Configurações**.
A janela **Restrições de recursos do dispositivo** é exibida.
5. Ative as configurações usando o botão **Restrições de recursos do dispositivo**.
6. Ative as restrições de funções do dispositivo iOS MDM usando os botões nas guias correspondentes e selecione as restrições de funções necessárias.

Lista de restrições de funções do dispositivo

- Restrições na guia **Geral**:
 - Na seção **Configurações do dispositivo**:
 - **Proibir a discagem por voz em um dispositivo bloqueado**
Uso da função de discagem por voz em um dispositivo móvel bloqueado.
Se a caixa de seleção estiver desmarcada, o usuário poderá usar comandos de voz para discar números de telefone em um dispositivo móvel bloqueado.
Se a caixa de seleção estiver marcada, o usuário não poderá usar comandos de voz para discar números de telefone em um dispositivo móvel bloqueado.
Essa caixa de seleção é desmarcada por padrão.
 - **Limitar o rastreamento de anúncios**

Uso da tecnologia IFA (Identifier for advertisers) para rastrear sites visitados e aplicativos iniciados no dispositivo iOS MDM. A IFA permite configurar o rastreamento de anúncios no dispositivo móvel de acordo com os interesses do usuário.

Caso a caixa de seleção seja marcada, a tecnologia IFA será desativada no dispositivo móvel do usuário.

Se a caixa de seleção estiver desmarcada, a tecnologia IFA será ativada no dispositivo móvel e monitorará os sites visitados e os aplicativos iniciados para mostrar anúncios segmentados.

Essa caixa de seleção é desmarcada por padrão.

■ Proibir o Handoff

Uso da função Handoff no dispositivo móvel do usuário. O Handoff permite iniciar o trabalho com dados em um dispositivo de Apple e, a seguir, alternar para outro dispositivo Apple e continuar a trabalhar com aqueles dados.

Se a caixa de seleção estiver desmarcada, o Handoff está disponível para o usuário.

Se a caixa de seleção estiver marcada, o Handoff não está disponível.

Essa caixa de seleção é desmarcada por padrão.

■ Proibir a edição do nome do dispositivo

Capacidade de modificar o nome do dispositivo móvel.

Se a caixa de seleção estiver desmarcada, o usuário poderá editar o nome do dispositivo móvel.

Se a caixa de seleção estiver marcada, o nome do dispositivo não pode ser editado.

Essa caixa de seleção é desmarcada por padrão.

■ Proibir a modificação de restrições

Capacidade de definir as configurações para restrições no dispositivo móvel. As restrições podem ser utilizadas pelo usuário para executar funções do Controle para Pais no dispositivo móvel. O usuário pode restringir as funções do dispositivo (por exemplo, bloquear o uso da câmera), acesso ao conteúdo de mídia (por exemplo, definir restrições de idade para assistir filmes), o uso de aplicativos (por exemplo, bloquear o uso do iTunes Store), e configurar outras restrições.

Se a caixa de seleção estiver desmarcada, o usuário poderá definir as configurações de restrições no dispositivo móvel.

Se a caixa de seleção estiver marcada, as restrições não podem ser configuradas no dispositivo móvel.

Essa caixa de seleção é desmarcada por padrão.

■ Proibir sugestões do Spotlight

Uso dos resultados de pesquisa da Internet do Spotlight nas Sugestões da Siri. Ao usar as sugestões do Spotlight, as consultas de pesquisa e os seus dados de usuário associados são enviados para a Apple.

Se a caixa de seleção estiver desmarcada, o usuário poderá permitir a exibição dos resultados de pesquisa na Internet do Spotlight nas Sugestões da Siri.

Se a caixa de seleção estiver marcada, os resultados de pesquisa na Internet do Spotlight não estarão disponíveis nas Sugestões da Siri. Os dados do usuário não são enviados para a Apple.

O usuário pode ser capaz de ativar os resultados de pesquisa na Internet do Spotlight nas Sugestões da Siri mesmo se a caixa de seleção estiver marcada. Isso se deve a um problema conhecido pela Apple.

Essa caixa de seleção é desmarcada por padrão.

- Na seção **Proteção contra perda de dados:**

- **Proibir captura e gravação da tela**

Capacidade de fazer uma captura de tela ou vídeo da tela do dispositivo iOS MDM.

Se a caixa de seleção estiver desmarcada, o usuário poderá fazer e salvar capturas de tela e vídeos da tela do dispositivo móvel.

Se a caixa de seleção estiver marcada, o usuário não poderá fazer e salvar capturas de tela e vídeos da tela do dispositivo móvel.

Essa caixa de seleção é desmarcada por padrão.

- **Proibir que aplicativos não gerenciados usem documentos de aplicativos gerenciados**

Capacidade de usar aplicativos não gerenciados (pessoais) no dispositivo iOS MDM para abrir documentos criados usando contas e aplicativos gerenciados (corporativos). Aplicativos não gerenciados são aplicativos instalados, configurados e gerenciados pelo usuário do dispositivo móvel.

Se a caixa de seleção estiver desmarcada, o usuário poderá usar aplicativos não gerenciados para abrir documentos criados em aplicativos corporativos gerenciados.

Se a caixa de seleção estiver marcada, o usuário não poderá usar aplicativos não gerenciados para abrir documentos criados com aplicativos gerenciados. Por exemplo, esta configuração impede que um anexo de e-mail confidencial de uma conta de e-mail gerenciada seja aberto nos aplicativos pessoais do usuário.

Essa caixa de seleção é desmarcada por padrão.

- **Proibir que aplicativos gerenciados usem documentos de aplicativos não gerenciados**

Capacidade de usar aplicativos gerenciados (corporativos) no dispositivo iOS MDM para abrir documentos criados usando aplicativos não gerenciados (pessoais) e contas do usuário. Aplicativos não gerenciados são aplicativos instalados, configurados e gerenciados pelo usuário do dispositivo móvel.

Se a caixa de seleção estiver desmarcada, o usuário poderá usar aplicativos gerenciados para abrir documentos criados usando aplicativos não gerenciados.

Se a caixa de seleção estiver marcada, o usuário não terá permissão para usar aplicativos gerenciados para abrir documentos criados usando aplicativos não gerenciados. Por exemplo, a configuração impede que um documento de uma conta pessoal do iCloud seja aberto em um aplicativo corporativo.

Essa caixa de seleção é desmarcada por padrão.

- **Restringir copiar e colar entre aplicativos gerenciados e não gerenciados**

Restringir a funcionalidade de copiar e colar quando pelo menos uma das seguintes caixas de seleção estiver marcada:

- **Proibir que aplicativos não gerenciados usem documentos de aplicativos gerenciados**
 - **Proibir que aplicativos gerenciados usem documentos de aplicativos não gerenciados**

Se a caixa de seleção estiver marcada, o usuário do dispositivo não poderá usar a área de transferência.

Se a caixa de seleção estiver desmarcada, o usuário do dispositivo poderá usar a área de transferência.

Essa caixa de seleção é desmarcada por padrão.

Quando esta caixa de seleção está marcada, várias combinações das restrições **Proibir que aplicativos não gerenciados usem documentos de aplicativos gerenciados** e **Proibir que aplicativos gerenciados usem documentos de aplicativos não gerenciados** têm efeitos diferentes em termos da capacidade do usuário de usar a área de transferência.

Proibir que aplicativos não gerenciados usem documentos de aplicativos gerenciados	Proibir que aplicativos gerenciados usem documentos de aplicativos não gerenciados	Restrições de funções
Ativado	Ativado	O usuário não pode copiar e colar dados.
Ativado	Desativado	O usuário pode copiar dados de aplicativos gerenciados e colar dados em aplicativos não gerenciados. O usuário não pode copiar dados de aplicativos não gerenciados e colar dados em aplicativos gerenciados.
Desativado	Ativado	O usuário pode copiar dados de aplicativos não gerenciados e colar dados em aplicativos gerenciados. O usuário não pode copiar dados de aplicativos gerenciados e colar dados em aplicativos não gerenciados.
Desativado	Desativado	O usuário pode copiar dados de aplicativos gerenciados e colar dados em aplicativos não gerenciados. O usuário pode copiar dados de aplicativos não gerenciados e colar dados em aplicativos gerenciados.

■ Desativar a criptografia de cópias backup

Criptografia de cópias backup dos dados do dispositivo iOS MDM no aplicativo iTunes no computador do usuário.

Se a caixa de seleção estiver desmarcada, quando uma cópia backup dos dados do dispositivo móvel for criada no aplicativo iTunes, os dados serão criptografados automaticamente e protegidos com uma senha. Nesse caso, o usuário não pode criptografar cópias backup dos dados do dispositivo no aplicativo iTunes.

Se a caixa de seleção estiver marcada, o usuário poderá escolher se deseja criptografar cópias backup dos dados no aplicativo iTunes.

Essa caixa de seleção é desmarcada por padrão.

■ Proibir a redefinição para as configurações padrão

Capacidade de limpar todos os dados do dispositivo e redefini-lo para as configurações de fábrica.

Se a caixa de seleção estiver desmarcada, o usuário pode limpar todos os dados do dispositivo e redefini-lo para as configurações de fábrica.

Se a caixa de seleção estiver marcada, a redefinição para as configurações padrão não está disponível.

Essa caixa de seleção é desmarcada por padrão.

■ Proibir a modificação das configurações da conta

Opção que permite ao usuário adicionar novas contas (como contas de e-mail) e editar as configurações da conta no dispositivo iOS MDM.

Se a caixa de seleção estiver desmarcada, o usuário do dispositivo móvel poderá adicionar novas contas e editar as configurações das contas existentes.

Se a caixa de seleção estiver marcada, o usuário do dispositivo móvel não poderá adicionar novas contas e editar as configurações de contas existentes.

Essa caixa de seleção é desmarcada por padrão.

- Na seção **Segurança e privacidade**:

- **Proibir o envio de dados pessoais e de diagnóstico para a Apple**

Recebimento automático de dados de diagnóstico e informações sobre o uso do dispositivo iOS MDM e transmissão de um relatório com esses dados para a Apple para análise.

Se a caixa de seleção estiver desmarcada, após receber um aviso, o usuário poderá permitir a transmissão de relatórios com dados de diagnóstico e informações sobre o uso do dispositivo móvel para a Apple.

Se a caixa de seleção estiver marcada, a transmissão de relatórios com dados de diagnóstico e informações sobre o uso do dispositivo móvel para a Apple será bloqueada.

Essa caixa de seleção é desmarcada por padrão.

- **Proibir a alteração da senha**

Capacidade de definir, modificar ou excluir a senha de desbloqueio do dispositivo móvel.

Se a caixa de seleção estiver desmarcada, o usuário pode definir, modificar ou excluir a senha usada para desbloquear o dispositivo móvel.

Se a caixa de seleção estiver marcada, o gerenciamento da senha de desbloqueio não está disponível.

Essa caixa de seleção é desmarcada por padrão.

- **Proibir a modificação de configurações do Touch ID e do Face ID**

Capacidade de adicionar e remover impressões digitais do Touch ID ou dados do Face ID.

Se a caixa de seleção estiver desmarcada, o usuário poderá adicionar e remover impressões digitais do Touch ID ou dados do Face ID.

Se a caixa de seleção estiver marcada, o gerenciamento da identificação digital do Touch ID ou dos dados de Face ID não está disponível.

Essa caixa de seleção é desmarcada por padrão.

- **Proibir o desbloqueio do dispositivo usando Touch ID e Face ID**

O Touch ID e o Face ID possibilitam usar uma impressão digital ou reconhecimento facial como senha para desbloquear o dispositivo iOS MDM. O Touch ID e o Face ID também podem ser usados para autenticação de compras por meio do Apple Pay, iTunes Store, App Store e Book Store, e para iniciar sessão em aplicativos.

Se a caixa de seleção estiver desmarcada, o usuário poderá usar impressão digital ou reconhecimento facial em vez de digitar uma senha para desbloquear o dispositivo móvel.

Se a caixa de seleção estiver marcada, o usuário não poderá usar o Touch ID ou o Face ID para desbloquear o dispositivo móvel.

Essa caixa de seleção é desmarcada por padrão.

- **Solicitar a senha para cada compra na iTunes Store**

Uso da senha de restrição para comprar conteúdo de mídia na iTunes Store.

Se a caixa de seleção estiver marcada, antes de fazer a primeira compra na iTunes Store, o usuário deverá especificar uma senha de restrição nas configurações de restrição de compra e, posteriormente, usá-la para evitar compras acidentais ou não autorizadas. Após a conta ser verificada quando o usuário estiver fazendo compras, a senha de restrição não precisará ser digitada novamente por 15 minutos.

Caso a caixa de seleção esteja desmarcada, o usuário não precisará inserir a senha de restrição antes de fazer compras na iTunes Store.

Essa caixa de seleção é desmarcada por padrão.

- **Solicitar a senha na primeira conexão através do AirPlay**

Uso de uma senha na conexão do dispositivo iOS MDM a dispositivos compatíveis com AirPlay. A senha é usada para fazer a transmissão segura do conteúdo de mídia.

Se a caixa de seleção estiver marcada, antes da primeira conexão do dispositivo móvel a dispositivos compatíveis com AirPlay, o usuário deverá especificar uma senha nas configurações de segurança do AirPlay e, posteriormente, inseri-la.

Se a caixa de seleção estiver desmarcada, o usuário pode decidir se deseja usar uma senha ao conectar o dispositivo móvel a dispositivos compatíveis com AirPlay.

Essa caixa de seleção é desmarcada por padrão.

- **Proibir a instalação de perfis de configuração**

Uso de perfis de configuração adicionais no dispositivo iOS MDM.

Se a caixa de seleção estiver desmarcada, o usuário poderá instalar perfis de configuração adicionais no dispositivo móvel.

Se a caixa de seleção estiver marcada, o usuário não poderá instalar perfis de configuração adicionais no dispositivo móvel.

Essa caixa de seleção é desmarcada por padrão.

- **Proibir host não Configurador**

Proteção do dispositivo iOS MDM contra conexões de terceiros. Uma conexão de terceiros é uma conexão com outros dispositivos ou sincronização com serviços da Apple, como o iTunes.

Se a caixa de seleção estiver desmarcada, o usuário poderá sincronizar o dispositivo iOS MDM com outros dispositivos e serviços Apple.

Se a caixa de seleção estiver marcada, os hosts não configuradores no dispositivo móvel do usuário serão bloqueados.

Essa caixa de seleção é desmarcada por padrão.

- **Proibir a modificação de configurações de envio de dados de diagnóstico**

Recebimento automático de dados de diagnóstico e informações sobre o uso do dispositivo iOS MDM e transmissão de um relatório com esses dados para a Apple para análise.

Se a caixa de seleção estiver desmarcada, o usuário pode configurar o envio de relatórios que contêm informações de diagnósticos e dados da utilização do dispositivo móvel para a Apple.

Se a caixa de seleção estiver marcada, as configurações de envio de relatórios que contêm informações de diagnósticos não estão disponíveis.

Essa caixa de seleção é desmarcada por padrão.

- **Na seção iCloud:**

- **Proibir o backup no iCloud**

Backup automático de dados do dispositivo iOS MDM para o iCloud. As cópias dos dados já armazenados no iCloud não são criadas durante o processo de backup. As cópias de conteúdo de mídia recebidas ao sincronizar o dispositivo com um computador e não compradas na iTunes Store também não são criadas.

Se a caixa de seleção estiver desmarcada, o usuário poderá salvar cópias backup dos dados do dispositivo móvel no iCloud. As cópias backup dos dados são salvas no iCloud diariamente quando o dispositivo é ativado, bloqueado e conectado a uma fonte de alimentação.

Se a caixa de seleção estiver marcada, o usuário não poderá salvar cópias backup dos dados do dispositivo móvel no iCloud.

Essa caixa de seleção é desmarcada por padrão.

■ **Proibir o armazenamento de documentos e dados no iCloud**

Backup automático de documentos no iCloud. Os documentos do iCloud podem ser abertos e editados em outros dispositivos nos quais o serviço do iCloud está configurado.

Se a caixa de seleção estiver desmarcada, o usuário poderá salvar documentos no iCloud, abri-los e editá-los em outros dispositivos em aplicativos compatíveis com o iCloud (como o TextEdit).

Se a caixa de seleção estiver marcada, o usuário não terá permissão para salvar documentos no iCloud.

Essa caixa de seleção é desmarcada por padrão.

■ **Proibir o chaveiro do iCloud**

Sincronização automática das credenciais da conta de um usuário de dispositivo iOS MDM com outros dispositivos Apple do usuário. Os dados sincronizados são armazenados no iCloud Keychain. Os dados na iCloud Keychain são criptografados. A iCloud Keychain permite salvar os seguintes dados no iCloud:

- Contas do site
- Números e datas de validade dos cartões bancários
- Senhas de rede sem fio

Se a caixa de seleção estiver desmarcada, o usuário poderá sincronizar os dados das contas com outros dispositivos Apple.

Se a caixa de seleção estiver marcada, o usuário não poderá usar o iCloud Keychain no dispositivo móvel.

Essa caixa de seleção é desmarcada por padrão.

■ **Proibir que os aplicativos gerenciados armazenem dados no iCloud**

Criação de uma cópia de backup dos dados dos aplicativos gerenciados no iCloud.

Se a caixa de seleção estiver desmarcada, o usuário pode armazenar os dados dos aplicativos gerenciados no iCloud.

Se a caixa de seleção estiver marcada, o usuário não pode armazenar dados corporativos no iCloud.

Essa caixa de seleção é desmarcada por padrão.

■ **Proibir o backup de livros corporativos**

Backup de livros corporativos usando o iCloud ou iTunes. Você pode fornecer o acesso aos livros corporativos colocando-os no servidor Web corporativo.

Se a caixa de seleção estiver desmarcada, a cópia de backup dos livros corporativos usando o iCloud ou iTunes está disponível para o usuário.

Se a caixa de seleção estiver marcada, o backup de livros corporativos não está disponível.

Essa caixa de seleção é desmarcada por padrão.

■ **Proibir a sincronização de notas e realces em livros corporativos**

Capacidade de sincronizar notas, favoritos e textos destacados em livros corporativos usando o iCloud.

Se a caixa de seleção estiver desmarcada, o usuário poderá sincronizar notas, favoritos e destaques em livros corporativos. As alterações estarão disponíveis em todos os dispositivos Apple do usuário usando o iCloud.

Se a caixa de seleção estiver marcada, notas, favoritos e textos destacados estarão disponíveis somente neste dispositivo móvel.

Essa caixa de seleção é desmarcada por padrão.

■ **Proibir o compartilhamento de fotos no iCloud**

Uso do compartilhamento de fotos do iCloud no dispositivo iOS MDM para conceder a outros usuários acesso a fotos e vídeos no servidor iCloud. Os outros usuários precisam ter o recurso de compartilhamento de fotos do iCloud configurado.

Se a caixa de seleção estiver desmarcada, o recurso de compartilhamento de fotos do iCloud estará disponível para o usuário. Os usuários de outros dispositivos podem visualizar as fotos e os vídeos do usuário, além de deixar comentários e adicionar suas próprias fotos e vídeos. O usuário também poderá acessar os dados de outros usuários no servidor do iCloud.

Se a caixa de seleção estiver marcada, o recurso de compartilhamento de fotos do iCloud não estará disponível para o usuário. O usuário não pode conceder a outros usuários acesso às suas fotos e vídeos no servidor iCloud nem acessar os dados de outros usuários no servidor iCloud.

Essa caixa de seleção é desmarcada por padrão.

■ **Proibir a Biblioteca de Música do iCloud**

Uso da função iCloud Media Library para o carregamento automático de fotos e vídeos a partir do dispositivo iOS MDM para outros dispositivos Apple do usuário.

Se a caixa de seleção estiver desmarcada, a função iCloud Media Library está disponível para o usuário ao trabalhar com o aplicativo Fotos.

Se a caixa de seleção estiver marcada, a função iCloud Media Library não está disponível para o usuário. As fotos e vídeos do usuário salvas no iCloud Media Library são removidas do servidor iCloud.

Essa caixa de seleção é desmarcada por padrão.

■ Na seção **Certificados**:

■ **Proibir que os usuários aceitem certificados TLS não confiáveis**

Uso de certificados TLS não confiáveis para fornecer um canal de comunicação criptografado entre aplicativos no dispositivo iOS MDM (Correio, Contatos, Calendário, Safari) e recursos corporativos.

Se a caixa de seleção estiver desmarcada, o usuário poderá permitir o uso de um certificado TLS não confiável após receber um aviso.

Se a caixa de seleção estiver marcada, o uso de certificados TLS não confiáveis será bloqueado.

Essa caixa de seleção é desmarcada por padrão.

■ **Proibir a atualização automática de certificados confiáveis**

Atualizações automáticas de certificados confiáveis no dispositivo iOS MDM.

Se a caixa de seleção estiver desmarcada, as alterações feitas nas configurações de confiança de um certificado serão aplicadas automaticamente.

Se a caixa de seleção estiver marcada, as alterações nas configurações de confiança de um certificado não serão aplicadas automaticamente. Depois de receber um aviso, o usuário poderá optar por aplicar as alterações nas configurações de confiança do certificado.

Essa caixa de seleção é desmarcada por padrão.

- Restrições na guia **Aplicativos**:

- Na seção **Geral**:

- **Proibir o uso da câmera**

Uso da câmera no dispositivo móvel do usuário.

Se a caixa de seleção estiver desmarcada, o usuário poderá usar a câmera do dispositivo.

Se a caixa de seleção estiver marcada, o uso da câmera do dispositivo será desativado. O usuário não pode tirar fotos, gravar vídeos ou usar o aplicativo FaceTime. O ícone da câmera na tela inicial do dispositivo doméstico está oculto.

Essa caixa de seleção é desmarcada por padrão.

- **Proibir FaceTime**

- **Proibir iMessage**

Uso do serviço iMessage no dispositivo móvel do usuário.

Se a caixa de seleção estiver desmarcada, o usuário poderá enviar e receber mensagens usando o iMessage.

Se a caixa de seleção estiver marcada, o iMessage não estará disponível no dispositivo móvel. O usuário não pode enviar ou receber mensagens via iMessage.

Essa caixa de seleção é desmarcada por padrão.

- **Proibir Book Store**

Acesso à Livraria no aplicativo Livros da Apple no dispositivo móvel do usuário.

Se a caixa de seleção estiver desmarcada, o usuário poderá visitar a Livraria no aplicativo Livros da Apple instalado no dispositivo.

Se a caixa de seleção estiver marcada, o usuário não poderá acessar a Livraria no aplicativo Livros.

Essa caixa de seleção é desmarcada por padrão.

- **Proibir a instalação de aplicativos do Apple Configurator e iTunes**

O usuário pode instalar aplicativos de forma independente em um dispositivo iOS MDM.

Se a caixa de seleção estiver desmarcada, o usuário poderá instalar ou atualizar aplicativos de forma independente em um dispositivo móvel pela App Store usando o iTunes ou o Apple Configurator.

Se a caixa de seleção estiver marcada, o usuário não poderá instalar ou atualizar aplicativos da App Store usando o iTunes ou o Apple Configurator em um dispositivo móvel. A instalação e as atualizações estão disponíveis apenas para aplicativos corporativos. O ícone da App Store fica oculto na tela inicial do dispositivo iOS MDM.

Essa caixa de seleção é desmarcada por padrão.

- **Proibir a instalação de aplicativos da App Store**

Capacidade de instalar independentemente aplicativos em um dispositivo móvel a partir da App Store. A opção está disponível se a caixa de seleção **Proibir a instalação de aplicativos do Apple Configurator e iTunes** estiver desmarcada.

Se a caixa de seleção estiver desmarcada, o usuário pode instalar ou atualizar aplicativos de forma independente a partir da App Store.

Se a caixa de seleção estiver marcada, o usuário não pode instalar ou atualizar aplicativos de forma independente a partir da App Store no dispositivo móvel. O ícone da App Store fica oculto na tela inicial do dispositivo iOS MDM.

Essa caixa de seleção é desmarcada por padrão.

■ **Proibir o download automático de aplicativos**

Uso de downloads automáticos de aplicativos no dispositivo móvel do usuário. A opção está disponível se a caixa de seleção **Proibir a instalação de aplicativos do Apple Configurator e iTunes** estiver desmarcada.

Se esta caixa de seleção estiver desmarcada, os downloads automáticos de aplicativos estão disponíveis para o usuário. Após essa função ser ativada, os aplicativos que o usuário baixou por meio da App Store são automaticamente baixados nos outros dispositivos Apple do usuário.

Se a caixa de seleção estiver marcada, os downloads automáticos de aplicativos estão desativados e indisponíveis.

Essa caixa de seleção é desmarcada por padrão.

■ **Proibir compras em aplicativos**

Uso do sistema de compras no aplicativo no dispositivo móvel.

Se a caixa de seleção estiver desmarcada, o usuário poderá fazer compras em aplicativos instalados no dispositivo móvel.

Se a caixa de seleção estiver marcada, o usuário não poderá fazer compras em aplicativos instalados no dispositivo móvel.

Essa caixa de seleção é desmarcada por padrão.

■ **Proibir confiar em novos desenvolvedores corporativos**

Capacidade de configurar a confiança de aplicativos corporativos em um dispositivo móvel. Você pode desenvolver aplicativos corporativos e distribuí-los entre os funcionários para uso interno. Para trabalhar com um aplicativo corporativo, o usuário de dispositivo móvel deve torná-lo um aplicativo confiável.

Se a caixa de seleção estiver desmarcada, o usuário poderá configurar a confiança de aplicativos corporativos.

Se a caixa de seleção estiver marcada, o usuário não pode definir o nível de confiança para aplicativos corporativos ao instalar um aplicativo manualmente.

Essa caixa de seleção é desmarcada por padrão.

■ **Proibir a remoção de aplicativos**

A opção permite remover aplicativos do dispositivo móvel.

Se a caixa de seleção estiver desmarcada, o usuário poderá remover aplicativos instalados via App Store ou iTunes do dispositivo.

Se a caixa de seleção estiver marcada, o usuário não poderá remover aplicativos instalados via App Store ou iTunes do dispositivo móvel.

Essa caixa de seleção é desmarcada por padrão.

■ Na seção **AirDrop**:

■ **Proibir AirDrop**

Uso do recurso AirDrop para transmitir dados do usuário do dispositivo iOS MDM para outros dispositivos Apple.

Se a caixa de seleção estiver desmarcada, o usuário poderá usar o AirDrop para transmitir dados para outros dispositivos Apple.

Se a caixa de seleção estiver marcada, o usuário não poderá transmitir dados para outros dispositivos Apple usando o AirDrop.

Essa caixa de seleção é desmarcada por padrão.

- **Tratar o AirDrop como um aplicativo gerenciado**

O uso do AirDrop como um aplicativo gerenciado para transferir dados do dispositivo móvel para outros dispositivos da Apple. Essa restrição requer a marcação da caixa de seleção **Proibir que aplicativos não gerenciados usem documentos de aplicativos gerenciados**. Aplicativos não gerenciados são aplicativos instalados, configurados e gerenciados pelo usuário do dispositivo móvel.

Se a caixa de seleção estiver desmarcada, o AirDrop é tratado como um aplicativo não gerenciado.

Se a caixa de seleção estiver marcada, o AirDrop é tratado como um aplicativo gerenciado.

Essa caixa de seleção é desmarcada por padrão.

- Na seção **Apple Music**:

- **Proibir Apple Music**

Escutar música no dispositivo móvel do usuário usando o serviço Apple Music.

Se a caixa de seleção estiver desmarcada, o usuário pode escutar música no dispositivo móvel no aplicativo Music.

Se a caixa de seleção estiver marcada, o serviço Apple Music não está disponível para o usuário.

Essa caixa de seleção é desmarcada por padrão.

- **Proibir rádio no Apple Music**

Escutar o rádio usando o serviço Apple Music no dispositivo móvel do usuário.

Se a caixa de seleção estiver desmarcada, o usuário pode escutar o rádio no dispositivo móvel no aplicativo Music.

Se a caixa de seleção estiver marcada, o usuário não pode escutar o rádio.

Essa caixa de seleção é desmarcada por padrão.

- Na seção **Apple Watch**:

- **Desativar a detecção do Apple Watch no pulso**

Bloqueio automático do Apple Watch quando o usuário removê-lo de seu pulso.

Se a caixa de seleção estiver desmarcada, o Apple Watch é bloqueado quando o usuário o remove de seu pulso. Para desbloqueá-lo, o usuário deve inserir uma senha no dispositivo móvel.

Se a caixa de seleção estiver marcada, o Apple Watch não pode ser bloqueado após o relógio ser removido.

Essa caixa de seleção é desmarcada por padrão.

- **Proibir o pareamento com o Apple Watch**

Parear o Apple Watch com um dispositivo móvel supervisionado.

Se a caixa de seleção estiver desmarcada, o usuário do dispositivo móvel supervisionado pode pareá-lo com o Apple Watch.

Se a caixa de seleção estiver marcada, o pareamento com o Apple Watch não está disponível.

Essa caixa de seleção é desmarcada por padrão.

- Na seção **Siri**:

- **Proibir Siri**

Descontinuado no iOS 26.4 e posterior.

Uso do aplicativo Siri no dispositivo móvel do usuário.

Se a caixa de seleção estiver desmarcada, o usuário poderá usar comandos de voz da Siri no dispositivo móvel.

Se a caixa de seleção estiver marcada, o usuário não poderá usar comandos de voz da Siri no dispositivo móvel.

Essa caixa de seleção é desmarcada por padrão.

- **Proibir quando o dispositivo estiver bloqueado**

Descontinuado no iOS 26.4 e posterior.

Uso de comandos de voz da Siri quando o dispositivo móvel do usuário estiver bloqueado. O dispositivo móvel do usuário deve ser protegido por senha.

Se a caixa de seleção estiver desmarcada, o usuário poderá usar comandos de voz da Siri em um dispositivo móvel bloqueado.

Se a caixa de seleção estiver marcada, o usuário não poderá usar comandos de voz da Siri em um dispositivo bloqueado.

Essa caixa de seleção é desmarcada por padrão.

- **Proibir o uso de filtros de obscenidades**

Descontinuado no iOS 26.4 e posterior.

Esta opção desativa a filtragem de palavrões durante o uso do aplicativo Siri no dispositivo móvel.

Se a caixa de seleção estiver desmarcada, os palavrões serão filtrados enquanto o usuário usar o aplicativo Siri.

Se a caixa de seleção estiver marcada, palavrões não serão filtrados durante o uso do aplicativo Siri pelo usuário.

Essa caixa de seleção é desmarcada por padrão.

- **Proibir que a Siri use a busca na Internet**

Descontinuado no iOS 26.4 e posterior.

Esta opção proíbe a Siri de usar a pesquisa na Internet para comandos de voz no dispositivo iOS MDM.

Se a caixa de seleção estiver desmarcada, a Siri poderá pesquisar na Internet respostas para as perguntas do usuário.

Se a caixa de seleção estiver marcada, a Siri não poderá pesquisar informações na Internet.

Essa caixa de seleção é desmarcada por padrão.

- Na seção **Find My**:

- **Proibir a localização de dispositivos pelo Find My**

Marcar ou desmarcar a caixa de seleção define se o usuário do dispositivo pode localizar dispositivos no aplicativo Find My.

A restrição é compatível com dispositivos com iOS 13 e posteriores.

Esta caixa de seleção é desmarcada por padrão.

- **Proibir a localização de amigos pelo Find My**

Marcar ou desmarcar a caixa de seleção define se o usuário do dispositivo pode localizar amigos no aplicativo Find My.

A restrição é compatível com dispositivos com iOS 13 e posteriores.

Esta caixa de seleção é desmarcada por padrão.

- Na seção **Classroom**:

- **Proibir a visualização de telas com o Classroom**

Capacidade de um instrutor exibir telas do iPad dos alunos usando o aplicativo Sala de aula.

Se a caixa for estiver desmarcada, o instrutor pode exibir telas do iPad dos alunos no aplicativo Sala de aula.

Se a caixa for estiver marcada, o instrutor não pode exibir telas do iPad dos alunos no aplicativo Sala de aula.

Essa caixa de seleção é desmarcada por padrão.

- Restrições na guia **Rede**:

- Na seção **Celular**:

- **Proibir a sincronização automática quando em roaming**

Proibir a sincronização automática de dados do usuário quando o dispositivo iOS MDM estiver em roaming.

Se a caixa de seleção estiver desmarcada, o usuário poderá ativar a sincronização automática de dados quando o dispositivo estiver em roaming. A ativação da sincronização automática em roaming pode resultar em custos inesperados do serviço móvel.

Se a caixa de seleção estiver marcada, o usuário não poderá usar a sincronização automática de dados quando o dispositivo estiver em roaming.

Essa caixa de seleção é desmarcada por padrão.

- **Proibir a modificação das configurações de celular**

Capacidade de configurar a transferência de dados da rede celular por aplicativos instalados em um dispositivo móvel.

Se a caixa de seleção estiver desmarcada, o usuário poderá definir as configurações para a transferência de dados através de uma rede celular.

Se a caixa de seleção estiver marcada, as configurações para a transferência de dados da rede celular por aplicativos não podem ser modificadas.

Essa caixa de seleção é desmarcada por padrão.

- Restrições na guia **Configurações adicionais**:

- Na seção **Display**:

- **Proibir a alteração do papel de parede**

Capacidade de selecionar a imagem que será exibida na tela de bloqueio ou tela inicial.

Se a caixa de seleção estiver desmarcada, o usuário pode selecionar o papel de parede para o dispositivo móvel.

Se a caixa de seleção estiver marcada, a seleção de papel de parede não está disponível.

Essa caixa de seleção é desmarcada por padrão.

- Na seção **Texto**:

- **Bluetooth a correção ortográfica**

Descontinuado no iOS 26.4 e posterior.

Uso do corretor ortográfico ao inserir texto em um dispositivo móvel. A função de corretor ortográfico sublinha as palavras incorretamente soletradas e sugere correções.

Se a caixa de seleção estiver desmarcada, o usuário pode ativar e usar a função de corretor ortográfico.

Se a caixa de seleção estiver marcada, o corretor ortográfico não está disponível ao inserir texto.

Essa caixa de seleção é desmarcada por padrão.

- **Proibir a correção automática**

Descontinuado no iOS 26.4 e posterior.

Uso da função de correção automática ao inserir texto.

Se a caixa de seleção estiver desmarcada, o usuário poderá ativar e usar a função de correção automática.

Se a caixa de seleção estiver marcada, a correção automática não estará disponível ao inserir texto.

Essa caixa de seleção é desmarcada por padrão.

- **Proibir a busca no dicionário**

Descontinuado no iOS 26.4 e posterior.

Uso de um dicionário para obter definições de palavras no dispositivo móvel. Somente um software de teclado tem a função de dicionário.

Se a caixa de seleção estiver desmarcada, o usuário pode realçar qualquer palavra na tela do dispositivo móvel e obter a definição dela.

Se a caixa de seleção estiver marcada, a pesquisa no dicionário não está disponível.

Essa caixa de seleção é desmarcada por padrão.

- Na seção **Teclado**:

- **Proibir textos preditivos**

Descontinuado no iOS 26.4 e posterior.

Uso da função de entrada de texto previsível. A função de entrada de texto previsível mostra opções para completar palavras e sugestões com base nos dicionários disponíveis.

Se a caixa de seleção estiver desmarcada, o usuário pode ativar e usar a função de entrada de texto previsível.

Se a caixa de seleção estiver marcada, a função de texto previsível não está disponível. Neste caso, as sugestões não são exibidas ao inserir texto.

Essa caixa de seleção é desmarcada por padrão.

- **Proibir atalhos do teclado**

Descontinuado no iOS 26.4 e posterior.

Uso de atalhos de teclado para o acesso rápido às funções do dispositivo móvel.

Se a caixa de seleção estiver desmarcada, o usuário pode ativar a função de atalho de teclado e usá-la ao trabalhar com o dispositivo móvel.

Se a caixa de seleção estiver marcada, a função de atalho de teclado não está disponível.

Essa caixa de seleção é desmarcada por padrão.

- Na seção **Notificações**:

- **Proibir notificações na tela do Wallet quando a tela estiver bloqueada**

Uso de notificações da Carteira na tela de bloqueio do dispositivo iOS MDM.

Se a caixa de seleção estiver desmarcada, as notificações da Carteira serão exibidas na tela de bloqueio do dispositivo móvel.

Se a caixa de seleção estiver marcada, as notificações da Carteira não serão exibidas na tela de bloqueio do dispositivo móvel. Para trabalhar com o Wallet, o usuário deve desbloquear o dispositivo.

Essa caixa de seleção é desmarcada por padrão.

- **Ocultar o Centro de Controle quando a tela estiver bloqueada**

Capacidade de acessar a Central de Controle do dispositivo iOS MDM quando o dispositivo estiver bloqueado.

Se a caixa de seleção estiver desmarcada, o usuário poderá acessar a Central de Controle quando o dispositivo estiver bloqueado.

Se a caixa de seleção estiver marcada, o usuário não poderá acessar a Central de Controle quando o dispositivo estiver bloqueado.

Essa caixa de seleção é desmarcada por padrão.

■ **Ocultar o Centro de Notificação quando a tela estiver bloqueada**

Capacidade de acessar a Central de Notificações do dispositivo iOS MDM quando o dispositivo estiver bloqueado.

Se a caixa de seleção estiver desmarcada, o usuário poderá acessar a Central de Notificações deslizando a tela de bloqueio para baixo.

Se a caixa de seleção estiver marcada, o usuário não poderá acessar a Central de Notificações quando o dispositivo estiver bloqueado.

Essa caixa de seleção é desmarcada por padrão.

■ **Ocultar a visualização Hoje quando a tela estiver bloqueada**

Exibição de informações da Visualização do dia na tela de um dispositivo iOS MDM bloqueado. A seção Hoje da Visualização de notificações mostra as seguintes informações:

- Eventos de calendário
- Lembretes
- Preços das ações
- Clima

Se a caixa de seleção estiver desmarcada, o usuário poderá visualizar as notificações da Visualização do dia em um dispositivo móvel bloqueado.

Se a caixa de seleção estiver marcada, a Visualização do dia não será exibida no dispositivo móvel bloqueado.

Essa caixa de seleção é desmarcada por padrão.

■ **Proibir a modificação das configurações de notificação**

Capacidade de configurar a exibição de notificações no dispositivo móvel.

Se a caixa de seleção estiver desmarcada, o usuário pode definir as configurações para exibir notificações no dispositivo móvel.

Se a caixa de seleção estiver marcada, a exibição de notificações não pode ser configurada.

Essa caixa de seleção é desmarcada por padrão.

7. Clique em **OK**.

8. Clique em **Salvar** para salvar as alterações efetuadas.

Como resultado, as restrições de funções serão configuradas no dispositivo móvel do usuário depois que a política for aplicada.

Configurar as restrições de aplicativos

1. Na janela principal do Kaspersky Next Expert View (cloud), selecione **Gerenciamento de ativos** → **Políticas**. Na lista de políticas de grupo aberta, clique no nome da política que deseja configurar.

2. Na janela de propriedades da política, selecione **Configurações do aplicativo**.

3. Selecione **iOS** e vá para a seção **Restrições**.
4. No cartão **Restrições dos aplicativos**, clique em **Configurações**.
A janela **Restrições dos aplicativos** se abre.
5. Ative as configurações usando o botão **Restrições dos aplicativos**.
6. Configure as restrições de aplicativos de dispositivos iOS MDM.

Lista de restrições de aplicativos

Restrições na seção **Safari**:

- **Permitir o uso do Safari**

Utilização do navegador Safari no dispositivo iOS MDM.

Se a caixa de seleção for marcada, o usuário tem permissão para utilizar o navegador Safari.

Se a caixa de seleção estiver desmarcada, o usuário não tem permissão para utilizar o navegador Safari. O ícone do Safari é ocultado na tela inicial do dispositivo iOS MDM.

Essa caixa de seleção é marcada por padrão.

- **Permitir o AutoFill**

Salvar e preencher automaticamente dados inseridos pelo usuário em formulários da Web no navegador Safari.

Se a caixa de seleção estiver marcada, os dados do usuário inseridos nos formulários da Web serão salvos. Posteriormente, eles são inseridos automaticamente nos formulários da Web.

Se a caixa de seleção estiver desmarcada, os dados do usuário não serão inseridos nos formulários da Web.

Essa caixa de seleção é marcada por padrão.

- **Avisar o usuário quando ele visitar um site perigoso**

Opção que ativa um alerta ao usuário antes de visitar um site que o Kaspersky Mobile Devices Protection and Management avaliou como perigoso.

Se a caixa de seleção estiver marcada, o Kaspersky Mobile Devices Protection and Management avisa o usuário que está tentando visitar um site perigoso.

Se a caixa de seleção estiver desmarcada, o Kaspersky Mobile Devices Protection and Management não avisa o usuário que está tentando visitar um site perigoso.

Essa caixa de seleção é desmarcada por padrão.

- **Permitir o JavaScript**

Utilização do JavaScript pelo navegador Safari.

Se a caixa de seleção estiver marcada, o navegador Safari utiliza JavaScript ao abrir páginas da Web.

Se a caixa de seleção estiver desmarcada, o navegador Safari não utiliza JavaScript ao abrir páginas da Web.

Essa caixa de seleção é marcada por padrão.

- **Bloquear janelas de pop-up**

Bloqueio de janelas pop-up no navegador Safari.

Se a caixa de seleção estiver marcada, o Kaspersky Mobile Devices Protection and Management não bloqueia janelas pop-up no navegador Safari.

Se a caixa de seleção estiver desmarcada, o Kaspersky Mobile Devices Protection and Management não bloqueia janelas pop-up no navegador Safari.

Essa caixa de seleção é desmarcada por padrão.

- **Configurações de cookies**

Selecione a condição para aceitar cookies:

- **Permitir cookies e o rastreamento de sites.** O navegador Safari aceita cookies e permite rastrear a atividade do usuário.
- **Permitir cookies e bloquear o rastreamento de sites.** O navegador Safari aceita cookies e bloqueia o rastreamento da atividade do usuário.
- **Bloquear o rastreamento de cookies e sites.** O navegador Safari bloqueia cookies e o rastreamento da atividade do usuário.

O valor padrão é **Permitir cookies e o rastreamento de sites**.

Restrições na seção **Game Center**:

- **Permitir o uso do Game Center**

Acesso ao serviço de jogos do Game Center a partir do aplicativo Game Center em um dispositivo iOS MDM.

Se a caixa de seleção estiver marcada, o usuário pode visitar o serviço de jogos do Game Center a partir do aplicativo Game Center no dispositivo móvel.

Se a caixa de seleção estiver desmarcada, o usuário não pode visitar o serviço de jogos do Game Center a partir do aplicativo Game Center no dispositivo móvel. O ícone do Game Center é ocultado na tela inicial do dispositivo iOS MDM.

Essa caixa de seleção é marcada por padrão.

- **Permitir adicionar amigos no Game Center**

Uma opção que permite adicionar usuários ao serviço de jogos do Game Center no dispositivo iOS MDM.

Se a caixa de seleção estiver marcada, o usuário pode adicionar outros usuários ao serviço de jogos do Game Center no dispositivo móvel.

Se a caixa de seleção estiver desmarcada, o usuário não tem permissão para adicionar outros usuários ao serviço de jogos do Game Center no dispositivo móvel.

Essa caixa de seleção é marcada por padrão.

- **Permitir jogos multiplayer no Game Center**

Utilização do serviço de jogos do Game Center no modo multijogador no dispositivo iOS MDM.

Se a caixa de seleção estiver marcada, o usuário pode participar de jogos multijogador no serviço de jogos do Game Center no dispositivo móvel.

Se a caixa de seleção estiver desmarcada, o usuário não tem permissão para participar de jogos multijogador no serviço de jogos do Game Center no dispositivo móvel.

Se a caixa de seleção estiver desmarcada, os usuários ainda poderão jogar juntos via SharePlay ou um serviço de terceiros.

Essa caixa de seleção é marcada por padrão.

Restrições na seção **Configurações adicionais**:

- **Permitir o uso da iTunes Store**

Acesso ao serviço de mídia da iTunes Store a partir do aplicativo iTunes em um dispositivo iOS MDM.

Se a caixa de seleção estiver marcada, o usuário pode visualizar, comprar e efetuar o download de conteúdo de mídia da iTunes Store utilizando o aplicativo iTunes no dispositivo móvel.

Se a caixa de seleção estiver desmarcada, o usuário não pode visualizar, comprar e efetuar o download de conteúdo da iTunes Store utilizando o aplicativo iTunes no dispositivo móvel. O ícone do iTunes é ocultado na tela inicial do dispositivo iOS MDM.

Essa caixa de seleção é marcada por padrão.

- **Permitir o uso do News**

Visualizar notícias no dispositivo móvel do usuário usando o aplicativo News.

Se a caixa de seleção estiver marcada, o usuário pode visualizar notícias usando o aplicativo News.

Se a caixa de seleção estiver desmarcada, o aplicativo News não está disponível para o usuário.

Essa caixa de seleção é marcada por padrão.

- **Permitir o uso do Podcasts**

Ouvir podcasts no dispositivo móvel do usuário usando o aplicativo Podcasts.

Se a caixa de seleção estiver marcada, o usuário pode pesquisar, reproduzir e baixar podcasts utilizando o aplicativo Podcasts.

Se a caixa de seleção estiver desmarcada, os podcasts não podem ser baixados no dispositivo móvel.

Essa caixa de seleção é marcada por padrão.

7. Clique em **OK**.

8. Clique em **Salvar** para salvar as alterações efetuadas.

Como resultado, as restrições do aplicativo serão configuradas no dispositivo móvel do usuário depois que a política for aplicada.

Configurar restrições de conteúdo

As categorias usadas para restrições de conteúdo são determinadas pela Apple. Em alguns casos, quando as restrições de conteúdo são configuradas, os resultados reais podem diferir dos resultados esperados.

1. Na janela principal do Kaspersky Next Expert View (cloud), selecione **Gerenciamento de ativos** → **Políticas**. Na lista de políticas de grupo aberta, clique no nome da política que deseja configurar.
2. Na janela de propriedades da política, selecione **Configurações do aplicativo**.
3. Selecione **iOS** e vá para a seção **Restrições**.
4. No cartão **Restrições de conteúdo**, clique em **Configurações**.
A janela **Restrições de conteúdo** se abre.
5. Ative as configurações usando o botão **Restrições de conteúdo**.
6. Configure as restrições de conteúdo do dispositivos iOS MDM.

Lista de restrições

Região

Seleção do país cujo sistema de classificação é automaticamente aplicado ao conteúdo de mídia no dispositivo iOS MDM.

O valor padrão é **Estados Unidos**.

Configurações na seção **Classificação por idade**:

- **Vídeos**

Seleção da classificação de restrição para acesso a filmes no dispositivo iOS MDM.

A lista de classificações depende da região selecionada.

Se a opção **Permitir tudo** estiver marcada, o usuário pode ver qualquer filme no dispositivo móvel.

Por padrão, a opção **Permitir tudo** é selecionada.

- **Programas de TV**

Seleção da classificação de restrição para acesso a programas de televisão no dispositivo iOS MDM.

A lista de classificações depende da região selecionada.

Se a opção **Permitir tudo** estiver marcada, o usuário pode ver qualquer programa de televisão no dispositivo móvel.

Por padrão, a opção **Permitir tudo** é selecionada.

- **Aplicativos**

Seleção da classificação de restrição para acesso a aplicativos terceiros no dispositivo iOS MDM.

A lista de classificações depende do sistema de classificação selecionado.

Se a opção **Permitir tudo** estiver marcada, o usuário pode usar qualquer aplicativo de terceiros no dispositivo móvel.

Por padrão, a opção **Permitir tudo** é selecionada.

As restrições de aplicativos podem ser aplicadas mesmo se a opção **Permitir tudo** estiver selecionada. Isso se deve a um problema conhecido pela Apple.

- **Permitir o download de conteúdos eróticos no Apple Books**

Acesso a conteúdo para adultos na Book Store no dispositivo móvel do usuário.

Se a caixa de seleção estiver marcada, o usuário pode efetuar o download de conteúdo para adultos a partir do aplicativo Apple Books para o dispositivo iOS MDM.

Se a caixa de seleção estiver desmarcada, o usuário não pode efetuar o download de conteúdo para adultos a partir do aplicativo Apple Books para o dispositivo iOS MDM.

Essa caixa de seleção é marcada por padrão.

- **Permitir conteúdo explícito**

Acesso a conteúdo de mídia explícito da iTunes Store no dispositivo iOS MDM. As restrições são aplicadas pelos provedores da iTunes Store.

Se a caixa de seleção estiver marcada, o conteúdo de mídia explícito comprado na iTunes Store está disponível para o usuário do dispositivo móvel.

Se a caixa de seleção estiver desmarcada, o conteúdo de mídia explícito comprado na iTunes Store é ocultado do usuário do dispositivo móvel.

Essa caixa de seleção é marcada por padrão.

7. Clique em **OK**.

8. Clique em **Salvar** para salvar as alterações efetuadas.

Como resultado, as restrições de conteúdo serão configuradas no dispositivo móvel do usuário depois que a política for aplicada.

Configurar o acesso do usuário aos sites

Esta seção contém instruções sobre como configurar o acesso aos sites em dispositivos Android e iOS.

Configurar o acesso aos sites nos dispositivos Android

Você pode usar o Controle da Web para configurar o acesso de usuários de dispositivos Android a sites. O Controle da Web oferece suporte à filtragem de sites por categorias definidas no serviço na nuvem Kaspersky Security Network. A filtragem permite restringir o acesso do usuário a determinados sites ou categorias de sites (por exemplo, "Jogos de azar, loterias, apostas" ou "Comunicações via Internet"). O Controle da Web está ativado por padrão.

No Yandex Browser e no Samsung Internet, URLs maliciosas e de phishing podem permanecer sem bloqueio. Isso ocorre porque somente o domínio do site é verificado. Se for um domínio malicioso ou de phishing, a Proteção na Web bloqueará a ameaça. Se o domínio não for classificado como malicioso ou de phishing, a URL específica não será bloqueada.

O Controle da Web em dispositivos Android é compatível apenas com Google Chrome, HUAWEI Browser, Samsung Internet e Yandex Browser.

O Controle da Web requer o seguinte para funcionar em um dispositivo gerenciado:

- O Kaspersky Endpoint Security for Android deve ser configurado como um serviço de acessibilidade.

Se o Kaspersky Endpoint Security for Android não for ativado como um recurso de acessibilidade e um proxy estiver ativado no cartão **Configurações do Google Chrome**, o Controle da Web não funcionará.

- A Declaração sobre processamento de dados para uso da Proteção na Web (Declaração da Proteção na Web) deve ser aceita. 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.
- Em alguns dispositivos, o usuário deve conceder manualmente as seguintes [permissões](#):
 - **Executar em segundo plano**
 - **Exibir janelas pop-up durante a execução em segundo plano**

- Exibir janela pop-up
- Ignorar otimização de bateria

Para especificar as configurações do acesso do usuário do dispositivo a sites:

1. Na janela principal do Kaspersky Next Expert View (cloud), selecione **Gerenciamento de ativos** → **Políticas**. Na lista de políticas de grupo aberta, clique no nome da política que deseja configurar.
2. Na janela de propriedades da política, selecione **Configurações do aplicativo**.
3. Selecione **Android** e vá para a seção **Controles de segurança**.
4. No cartão **Controle da Web**, clique em **Configurações**.

A janela **Controle da Web** se abre.

5. Selecione uma das seguintes opções:

- Se você desejar que o aplicativo restrinja o acesso do usuário a sites dependendo do seu conteúdo, faça o seguinte:

a. Na lista suspensa **Modo de operação**, selecione **Proibir sites de categorias selecionadas**.

b. Na seção **Categorias**, crie uma lista de categorias proibidas marcando as caixas de seleção ao lado das categorias de sites aos quais o aplicativo bloqueará o acesso.

- Se você quiser que o aplicativo permita ou bloqueie o acesso do usuário somente a sites especificados, faça o seguinte:

a. Na lista suspensa **Modo de operação**, selecione **Permitir apenas os sites listados** ou **Permitir todos os sites, exceto os listados**.

b. Clique em **Adicionar**.

c. Na janela exibida, crie uma lista de sites aos quais o aplicativo permitirá ou bloqueará o acesso, dependendo do valor selecionado na lista suspensa. Você pode adicionar sites por link (URL completa, incluindo o protocolo, por exemplo, `https://example.com`).

Para garantir que o aplicativo permita ou bloqueie o acesso ao site especificado em todas as versões compatíveis do Google Chrome, HUAWEI Browser, Samsung Internet e Yandex Browser, inclua a mesma URL duas vezes, uma vez com o protocolo HTTP (por exemplo, `http://example.com`) e uma vez com o protocolo HTTPS (por exemplo, `https://example.com`).

Por exemplo:

- `https://example.com` – A página principal do site é permitida ou bloqueada. Essa URL só pode ser acessada usando o protocolo HTTP.
- `https://example.com` – A página principal do site é permitida ou bloqueada, mas somente quando acessada por meio do protocolo HTTP. Outros protocolos como HTTPS não são afetados.
- `https://example.com/page/index.html` – Somente a página `index.html` do site será permitida ou bloqueada. O resto do site não é afetado por esta entrada.

O aplicativo também é compatível com expressões regulares. Ao inserir o endereço de um site permitido ou proibido, use os seguintes modelos:

- `https://example\com/.*` - Esse modelo permite ou bloqueia todas as páginas secundárias do site acessadas por meio do protocolo HTTPS (por exemplo, `https://example.com/about`).
- `https?://example\com/.*` - Esse modelo permite ou bloqueia todas as páginas secundárias do site sejam acessadas via protocolos HTTP e HTTPS.
- `https?://.*\example\com` - Esse modelo permite ou bloqueia todas as páginas de subdomínio do site (por exemplo, `https://pictures.example.com`).
- `https?://example\com/[abc]/.*` - Esse modelo permite ou bloqueia todas as páginas secundárias do site onde o caminho da URL começa com 'a', 'b' ou 'c' como o primeiro diretório (por exemplo, `https://example.com/b/about`).
- `https?://\w{3,5}\example\com/.*` - Esse modelo permite ou bloqueia todas as páginas secundárias do site onde o subdomínio consiste em uma palavra com 3 a 5 caracteres (por exemplo, `http://abde.example.com/about`).

Use a expressão `https?` para selecionar os protocolos HTTP e HTTPS. Para obter mais detalhes sobre expressões regulares, consulte o [site de Suporte Técnico da Oracle](#).

d. Clique em **Adicionar**.

- Se quiser que o aplicativo bloqueie o acesso do usuário a todos os sites, na seção **Modo de operação**, selecione **Proibir todos os sites** na lista suspensa.
6. Se você quiser que o aplicativo verifique a URL completa ao abrir um site em Guias personalizadas, marque a caixa de seleção **Verificar o URL inteiro ao utilizar Guias personalizadas**.

As Guias personalizadas são um navegador no aplicativo que permite ao usuário visualizar páginas da Web sem precisar sair do aplicativo e alternar para uma versão completa do navegador da Web. Essa opção fornece um melhor reconhecimento das URLs e verifica as regras do Controle da Web configuradas. Se a caixa de seleção estiver marcada, o Kaspersky Endpoint Security for Android abre o site em uma versão completa do navegador e verifica o endereço da Web completo do site. Se a caixa de seleção estiver desmarcada, o Kaspersky Endpoint Security for Android verificará apenas o domínio do site nas Guias personalizadas.

O recurso Guias personalizadas é compatível com o Google Chrome, HUAWEI Browser e Samsung Internet.

7. Se você quiser eliminar as restrições baseadas em conteúdo no acesso de usuários a sites, desative as configurações usando o botão **Controle da Web** e clique em **Desativar**.

8. Clique em **OK**.

9. Clique em **Salvar** para salvar as alterações efetuadas.

As configurações do dispositivo móvel são alteradas após a próxima sincronização do dispositivo com o Kaspersky Security Center.

Gerenciar a lista de sites

Você pode gerenciar a lista de sites com os seguintes botões:

- **Adicionar:** clique para adicionar um site à lista inserindo uma URL ou uma expressão regular.
- **Carregar:** clique para adicionar vários sites à lista, especificando um arquivo TXT que contenha as URLs ou expressões regulares necessárias. O arquivo deve ser codificado em UTF-8. As URLs ou expressões regulares no arquivo devem ser separadas por ponto e vírgula ou quebras de linha.
- **Editar:** clique para alterar o endereço de um site.
- **Excluir:** clique para remover um ou mais sites da lista.

Configurar o acesso a sites nos dispositivos iOS MDM do usuário

Essas configurações se aplicam aos dispositivos no modo de operação "Perfil de gerenciamento".

Configure o Controle da Web para controlar acesso a sites para usuários de dispositivo iOS MDM. O Controle da Web gerencia o acesso do usuário aos sites com base em listas de sites permitidos e proibidos. O Controle da Web também permite adicionar sites favoritos no painel de favoritos do Safari.

Por padrão, o acesso a sites não é restrito.

Se uma URL for redirecionada para um site diferente, o Controle da Web verificará apenas o destino do redirecionamento.

Para definir as configurações de acesso dos usuários do dispositivo a sites:

1. Na janela principal do Kaspersky Next Expert View (cloud), selecione **Gerenciamento de ativos** → **Políticas**. Na lista de políticas de grupo aberta, clique no nome da política que deseja configurar.
2. Na janela de propriedades da política, selecione **Configurações do aplicativo**.
3. Selecione **iOS** e vá para a seção **Controles de segurança**.
4. No cartão **Controle da Web**, clique em **Configurações**.
A janela **Controle da Web** se abre.
5. Ative as configurações usando o botão **Controle da Web**.
6. Na lista suspensa **Modo de operação**, execute uma das seguintes ações:
 - Se quiser criar uma lista de sites permitidos, selecione **Permitir apenas os sites listados**.
 - Se quiser criar uma lista de sites proibidos, selecione **Permitir todos os sites, exceto os listados**.

7. Faça o seguinte:

a. Clique em **Adicionar**.

b. Adicione os sites que terão acesso permitido ou bloqueado pelo aplicativo, de acordo com a opção selecionada na lista suspensa.

O endereço do site deve começar com `http://` ou `https://`. O Kaspersky Mobile Devices Protection and Management permite ou bloqueia o acesso a todos os sites no domínio. Por exemplo, se você adicionar `http://www.example.com` à lista de sites permitidos, o acesso será permitido a `http://pictures.example.com` e `http://example.com/movies`.

Se você quiser adicionar um site permitido aos favoritos do Safari nos dispositivos móveis, marque a caixa de seleção **Adicionar aos favoritos no dispositivo** abaixo do endereço do site.

c. Clique em **Adicionar**.

8. Clique em **OK**.

9. Clique em **Salvar** para salvar as alterações efetuadas.

Como resultado, depois que a política é aplicada, o Controle da Web será configurado nos dispositivos móveis.

Controle de conformidade

Esta seção contém instruções sobre como monitorar a conformidade de dispositivos com os requisitos corporativos e configurar regras de controle de conformidade.

Controle de conformidade de dispositivos Android

Você pode ter o Controle de conformidade de dispositivos Android com os requisitos de segurança corporativos. Os requisitos de segurança corporativa regulam como o usuário poderá trabalhar com o dispositivo. Por exemplo, a proteção em tempo real deve estar ativada no dispositivo, os bancos de dados antimalware devem estar atualizados e a senha do dispositivo deve ser suficientemente forte. O Controle de conformidade é baseado 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 de tempo alocado para o usuário corrigir a não conformidade (por exemplo, 24 horas).
- Respostas executadas no dispositivo se o usuário não corrigir o problema de não conformidade dentro do período de tempo definido (por exemplo, bloquear o dispositivo).

Se o dispositivo estiver no modo de economia de bateria, o Kaspersky Endpoint Security for Android poderá executar essa tarefa mais tarde do que o especificado.

Para criar uma regra para verificar dispositivos quanto à conformidade com uma política:

1. Na janela principal do Kaspersky Next Expert View (cloud), selecione **Gerenciamento de ativos** → **Políticas**. Na lista de políticas de grupo aberta, clique no nome da política que deseja configurar.
2. Na janela de propriedades da política, selecione **Configurações do aplicativo**.

3. Selecione **Android** e vá para a seção **Controles de segurança**.

4. No cartão **Controle de conformidade**, clique em **Configurações**.

A janela **Controle de conformidade** se abre.

5. Ative as configurações usando o botão **Controle de conformidade**.

6. Na seção **Quando uma não conformidade é detectada**:

- Marque a caixa de seleção **Notificar o usuário** para informar ao usuário que o dispositivo não está em conformidade com a política.
Se a caixa de seleção estiver desmarcada, o usuário não será notificado sobre o problema de não conformidade e a resposta será executada no dispositivo assim que o tempo alocado para corrigir a não conformidade expirar.
- Marque a caixa de seleção **Notificar o administrador por meio da seção "Eventos"** para informar ao administrador que o dispositivo não está em conformidade com a política.

7. Clique em **Adicionar**.

O Adicionar assistente de regra é iniciado. Ele ajudará você a criar um conjunto de regras para verificar a conformidade do dispositivo com a política. Navegue pelo assistente usando os botões **Avançar** e **Voltar**.

Etapa 1. Critério de não conformidade

Clique em **Adicionar critério** para especificar o critério de não conformidade para acionar a regra.

Os seguintes critérios estão disponíveis:

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

O Kaspersky Endpoint Security for Android não está instalado ou em execução no dispositivo.

- **Os bancos de dados antimalware no dispositivo estão desatualizados**

Os bancos de dados antimalware foram atualizados pela última vez há 3 ou mais dias.

- **Aplicativos proibidos estão instalados**

A lista de aplicativos no dispositivo contém aplicativos que estão definidos como proibidos nas configurações de **Controle de Aplicativos** da política.

- **Aplicativos de categorias proibidas estão instalados**

A lista de aplicativos no dispositivo contém aplicativos das categorias definidas como proibidas nas configurações de **Controle de Aplicativos** da política.

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

A lista de aplicativos no dispositivo não contém um aplicativo definido como necessário nas configurações de **Controle de Aplicativos** da política.

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

A versão do Android no dispositivo está fora do intervalo permitido.

Para este critério, especifique as versões mínima e máxima permitidas do Android nos campos **Versão mínima** e **Versão máxima**. Se a versão máxima permitida for definida como **Qualquer**, versões futuras do Android compatíveis com o Kaspersky Endpoint Security for Android também serão permitidas.

- **O dispositivo não é sincronizado há muito tempo**

A última sincronização do dispositivo com o Servidor de Administração é verificada.

Para esse critério, especifique o período máximo após a última sincronização no campo **Período sem sincronização**.

- **O dispositivo foi roteado**

O dispositivo é hackeado (acesso root é obtido no dispositivo).

- **A senha de desbloqueio não está em conformidade com as configurações de segurança especificadas na política**

A senha de desbloqueio no dispositivo não é compatível com as configurações definidas no cartão **Configurações de desbloqueio de tela**.

Etapa 2. Respostas para a não conformidade com os requisitos de segurança

Adicione as respostas a serem executadas no dispositivo se o critério de não conformidade especificado for detectado.

Escolha uma das seguintes opções:

- **Adicionar resposta instantânea.** A resposta é aplicada instantaneamente depois que o critério de não conformidade é detectado.
- **Adicionar resposta adiada.** A resposta é aplicada após um período de adiamento que você pode especificar no campo **Período de adiamento**.

As seguintes respostas estão disponíveis:

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

Todos os aplicativos no dispositivo, exceto os aplicativos do sistema, são bloqueados para inicialização.

Assim que o critério de não conformidade selecionado para a regra não for mais detectado no dispositivo, os aplicativos serão desbloqueados automaticamente.

- **Bloquear dispositivo**

O dispositivo móvel é bloqueado. Para obter acessibilidade aos dados, você deve desbloquear o dispositivo inserindo o código de uso único ou usando o comando **Desbloquear dispositivo**.

- **Limpar os dados corporativos**

Os dados corporativos são limpos no dispositivo. A lista de dados apagados depende do modo em que o dispositivo opera:

- Em um dispositivo pessoal, o perfil Knox e o certificado de e-mail são apagados.
- Em um dispositivo com contêiner corporativo, o contêiner (seu conteúdo, configurações e restrições) e os certificados instalados nele (certificados de perfil de e-mail, VPN e SCEP, exceto os certificados de dispositivos móveis) são apagados.

- **Redefinir as configurações padrão**

Todos os dados são limpos no dispositivo e as configurações são revertidas para os valores de fábrica. Após essa resposta ser executada, o dispositivo não será mais gerenciado. Para conectar o dispositivo ao Kaspersky Security Center, você deve reinstalar o Kaspersky Endpoint Security for Android.

Em dispositivos com Android 14 ou posterior, esta resposta não é aplicável.

Clique em **Adicionar regra** para concluir o Adicionar assistente de regra. A nova regra e seus detalhes aparecerão na lista de regras do Controle de conformidade. Para desativar temporariamente uma regra, use o botão de alternância ao lado da regra selecionada.

Clique em **Salvar** para salvar as alterações efetuadas.

As configurações do dispositivo móvel são alteradas após a próxima sincronização do dispositivo com o Kaspersky Security Center.

Controle de aplicativos

Esta seção contém instruções sobre como configurar o acesso do usuário aos aplicativos em um dispositivo móvel.

Controle de aplicativos em dispositivos Android

O componente Controle de aplicativos permite gerenciar aplicativos em dispositivos Android e configurar o uso deles para manter os dispositivos seguros.

Você restringir a atividade do usuário em um dispositivo no qual os aplicativos proibidos estão instalados ou os aplicativos necessários não estão instalados (por exemplo, bloqueando o dispositivo). Você pode impor restrições usando o componente [Controle de conformidade](#). Para isso, nas configurações da regra, é necessário 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 por meio do Assistente de configuração inicial. O usuário pode ignorar esta etapa ou desativar esse serviço posteriormente nas configurações do dispositivo. Se o usuário fizer isso, o Controle de aplicativos não será executado.

Para definir as configurações de inicialização do aplicativo no dispositivo móvel:

1. Na janela principal do Kaspersky Next Expert View (cloud), selecione **Gerenciamento de ativos** → **Políticas**. Na lista de políticas de grupo aberta, clique no nome da política que deseja configurar.
2. Na janela de propriedades da política, selecione **Configurações do aplicativo**.
3. Selecione **Android** e vá para a seção **Controles de segurança**.
4. No cartão **Controle de Aplicativos**, clique em **Configurações**.
A janela **Controle de Aplicativos** se abre.
5. Ative as configurações usando o botão **Controle de Aplicativos**.

6. Defina as configurações nas seguintes guias:

- Se você quiser configurar regras gerais de gerenciamento de aplicativos, **vá para a guia Uso do aplicativo.**

1. Na lista suspensa **Modo de operação**, selecione o modo Controle de aplicativos:

- Para permitir que o usuário inicie todos os aplicativos, exceto aqueles especificados como bloqueados na lista de categorias e aplicativos, selecione **Usar todos os aplicativos, exceto os proibidos**. O Kaspersky Endpoint Security for Android ocultará ícones dos aplicativos proibidos. Esta opção está marcada por padrão.
- Para permitir que o usuário somente inicie aplicativos especificados na lista de categorias e aplicativos como permitidos, recomendados ou necessários, selecione **Usar apenas os aplicativos permitidos**. O Kaspersky Endpoint Security for Android ocultará os ícones de todos os aplicativos, exceto aqueles especificados na lista de aplicativos permitidos, recomendados ou necessários e aplicativos do sistema.

2. Se você quiser que o Kaspersky Endpoint Security for Android envie dados sobre aplicativos proibidos ao log de eventos sem bloqueá-los, marque a caixa de seleção **Não bloquear aplicativos proibidos, somente adicionar um registro ao log de eventos**.

3. Se você quiser que o Kaspersky Endpoint Security for Android bloqueie a inicialização de aplicativos do sistema (como Calendário, Câmera e Configurações) no dispositivo móvel do usuário, marque a caixa de seleção **Bloquear aplicativos do sistema**. Essa caixa de seleção é exibida no modo **Usar apenas os aplicativos permitidos**.

Recomendamos não bloquear aplicativos do sistema, pois isso pode causar mau funcionamento do dispositivo.

Entre os aplicativos do sistema, o mecanismo do sistema para solicitar permissões do aplicativo pode estar bloqueado. Se você quiser desbloquear esse mecanismo, localize o nome dele (por exemplo, `com.google.android.permissioncontroller`) no log de eventos e adicione-o às exceções.

Antes de remover o Kaspersky Endpoint Security for Android do dispositivo, desmarque essa caixa de seleção ou desative o Controle de aplicativos.

4. Clique em **Adicionar** para adicionar aplicativos e categorias para os quais você deseja definir regras.

A janela **Adicionar app ou categoria** é exibida.

5. No campo **Objeto**, selecione **Aplicativo** ou **Categoria do aplicativo** e faça o seguinte:

- Se você selecionou **Aplicativo**, selecione um pacote de instalação ou especifique o nome do pacote e o nome do aplicativo nos campos correspondentes.
- Se você selecionou **Categoria do aplicativo**, selecione uma categoria e insira uma descrição nos campos correspondentes.
- Clique em **Adicionar**.

O aplicativo ou a categorias é adicionado à lista.

6. Se você quiser receber relatórios sobre os aplicativos instalados, na seção **Relatório sobre aplicativos instalados**, marque a caixa de seleção **Enviar dados sobre aplicativos instalados**.

Se um aplicativo do sistema ou um aplicativo de serviço estiver definido nas configurações do Controle de aplicativos, os dados dele serão enviados independentemente da marcação nas caixas de seleção.

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

- Se você quiser definir ações a serem executadas para aplicativos selecionados, vá para a guia **Gerenciamento do aplicativo**.

1. Na tabela **Ações para aplicativos**, clique em **Adicionar**.

2. Na janela que se abre, execute as seguintes ações:

a. No campo **Ação**, selecione uma das seguintes ações:

- **Instalar**. O usuário será solicitado a instalar o aplicativo.
- **Remover**. O aplicativo será excluído do dispositivo do usuário.
- **Recomendar a instalação**. O usuário receberá uma recomendação para instalar o aplicativo.

b. Preencha os campos a seguir:

Use somente fontes legítimas e confiáveis. Ao definir as configurações nessa seção, você é o único responsável por todos os riscos e as consequências associados ao uso de fontes não confiáveis.

- **Nome do pacote**
- **Nome do aplicativo**
- **Link**

Links para pacotes de aplicativos devem começar com http:// ou https://.

Para a instalação silenciosa, especifique um link de download direto para um arquivo APK que inicia o download sem a interação do usuário. Os links para as páginas da loja de aplicativos não são compatíveis com a instalação silenciosa. É possível colocar arquivos APK no servidor Web ou em outra fonte.

- **Versão**

Esse campo é um parâmetro de string especificado no formato de expressões regulares do Oracle. Para obter mais detalhes sobre expressões regulares, consulte o [site de Suporte Técnico da Oracle](#).

Os campos **Link** e **Versão** não são exibidos se você selecionar **Remover** no campo **Ação**.

c. Clique em **Adicionar**.

A ação configurada é adicionada à lista.

7. Clique em **OK**.

8. Clique em **Salvar** para salvar as alterações efetuadas.

As configurações do dispositivo móvel são alteradas após a próxima sincronização do dispositivo com o Kaspersky Security Center.

Níveis de proteção de dispositivos móveis

Níveis de proteção de dispositivos móveis definidos pelo Kaspersky Security Center

O Kaspersky Next Expert View (cloud) permite avaliar rapidamente o nível de proteção atual dos dispositivos móveis gerenciados na seção **Gerenciamento de ativos** → **Móvel** → **Dispositivos**.

Um dispositivo pode ter um dos seguintes níveis de proteção: **OK**, **Advertência** ou **Crítico**.

Os níveis de proteção são atribuídos e enviados ao Kaspersky Security Center, de acordo com os seguintes requisitos:

- Um motivo para atribuir um nível de proteção é detectado no dispositivo: o dispositivo recebe o status exibido na lista de dispositivos gerenciados.
- Vários motivos para atribuir níveis de proteção são detectados no dispositivo: o Kaspersky Mobile Devices Protection and Management atribui o status mais crítico.
- Nenhum motivo para atribuir um nível de proteção é detectado no dispositivo: o Kaspersky Mobile Devices Protection and Management não envia um status ao Kaspersky Security Center, e o status é definido como **OK**.

Níveis de proteção e seus significados

Nível de proteção	Significado
 OK	A intervenção do administrador não é necessária.
 Advertência	Foram registrados eventos relacionados com ameaças possíveis ou reais à segurança dos dispositivos gerenciados.
 Crítico	Problemas sérios foram encontrados. A intervenção de um administrador é necessária para solucioná-los.

O objetivo do administrador é assegurar que o nível de proteção **OK** exista em todos os dispositivos.

Níveis de proteção de dispositivos móveis definidos pelo Kaspersky Mobile Devices Protection and Management

O Kaspersky Mobile Devices Protection and Management define o nível de proteção de dispositivos móveis com base nas configurações da política e envia os níveis de proteção para o Kaspersky Security Center durante a sincronização. O administrador pode [alterar o nível de proteção na política](#), dependendo do nível de gravidade da condição (consulte a tabela *Valores padrão, motivos e condições para atribuir níveis de proteção a dispositivos Android*). Nesse caso, o valor definido pelo administrador substitui o valor padrão definido pelo Kaspersky Mobile Devices Protection and Management.

Condição	Motivo do nível de proteção	Valor padrão
A proteção em tempo real não está em execução	Um dos seguintes motivos: - A permissão Permitir acesso para gerenciar todos os arquivos não foi concedida. - A Kaspersky Security Network está desativada.	<i>Crítico</i>
A Proteção na Web e o Controle da Web não estão em execução	Um dos seguintes motivos: - A permissão Acessibilidade não foi concedida. - A Proteção na Web foi desativada pelo usuário nas Configurações do Kaspersky Endpoint Security. - A permissão Ignorar otimização da bateria não foi concedida. - A Declaração da Proteção na Web não foi aceita.	<i>Advertência</i>
O Controle de aplicativos não está em execução	A permissão Acessibilidade não foi concedida.	<i>Advertência</i>
O bloqueio do dispositivo não está disponível	Um dos seguintes motivos: - A permissão Administrador do dispositivo não foi concedida. - A permissão Acessibilidade não foi concedida. - O aplicativo não está habilitado para sobrepor outras janelas.	<i>Advertência</i>
A localização do dispositivo não está disponível	Um dos seguintes motivos: - A permissão Localização não foi concedida. - A localização do dispositivo não pode ser determinada (quando a permissão é concedida).	<i>Advertência</i>
As versões da Declaração da Kaspersky Security Network não correspondem	A versão da Declaração da Kaspersky Security Network que o usuário aceitou na política e a versão da Declaração da Kaspersky Security Network no dispositivo não coincidem.	<i>Advertência</i>
As versões da Declaração de marketing não correspondem	A versão da Declaração sobre o processamento de dados para fins de marketing que o usuário aceitou na política e a versão da Declaração sobre o processamento de dados para fins de marketing no dispositivo não coincidem.	<i>OK</i>

Inventário de software em dispositivos Android

Você pode fazer um inventário de aplicativos em dispositivos Android conectados ao Servidor de Administração. O Kaspersky Endpoint Security for Android recebe [informações sobre todos os aplicativos instalados nos dispositivos móveis](#). As informações obtidas durante o inventário são exibidas nas propriedades do dispositivo, na seção **Eventos**. Nesta seção, você pode visualizar informações detalhadas sobre cada aplicativo instalado.

Para ativar o inventário de software:

1. Na janela principal do Kaspersky Next Expert View (cloud), selecione **Gerenciamento de ativos** → **Políticas**. Na lista de políticas de grupo aberta, clique no nome da política que deseja configurar.
2. Na janela de propriedades da política, selecione **Configurações do aplicativo**.
3. Selecione **Android** e vá para a seção **Controles de segurança**.
4. No cartão **Controle de Aplicativos**, clique em **Configurações**.
A janela **Controle de Aplicativos** se abre.
5. Na seção **Relatório sobre aplicativos instalados**, marque a caixa de seleção **Enviar dados sobre aplicativos instalados**.
6. Se você quiser receber dados sobre aplicativos do sistema, marque a caixa de seleção **Enviar dados sobre aplicativos incorporados**.
7. Se você quiser receber dados sobre aplicativos de serviço que não têm uma interface e não podem ser abertos pelo usuário, marque a caixa de seleção **Enviar dados sobre aplicativos de serviço**.

8. Clique em **OK**.

9. Clique em **Salvar** para salvar as alterações efetuadas.

As configurações do dispositivo móvel são alteradas após a 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.

Proteção

Esta seção contém informações sobre como gerenciar remotamente a proteção de dispositivos móveis no Kaspersky Next Expert View (cloud).

Configuração da proteção antimalware em dispositivos Android

Para a detecção oportuna de ameaças, vírus e outros aplicativos maliciosos, você pode definir as configurações de proteção em tempo real e verificação de malware automática.

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

- Vírus, worms, cavalos de troia e ferramentas maliciosas
- Adware
- Aplicativos legítimos que invasores podem usar para comprometer os dispositivos ou dados dos usuários

O Antimalware tem várias limitações:

- Devido a 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 esses arquivos sem notificar que eles foram ignorados.
- Em dispositivos executando Android 11 ou posterior, o Kaspersky Endpoint Security for Android não pode verificar as pastas "Android/data" e "Android/obb" para detectar malware devido a limitações técnicas.

Configurar a proteção em tempo real

Para definir as configurações de proteção em tempo real para dispositivos móveis:

1. Na janela principal do Kaspersky Next Expert View (cloud), selecione **Gerenciamento de ativos** → **Políticas**. Na lista de políticas de grupo aberta, clique no nome da política que deseja configurar.
2. Na janela de propriedades da política, selecione **Configurações do aplicativo**.
3. Selecione **Android** e vá para a seção **Proteção**.
4. No cartão **Proteção em tempo real**, clique em **Configurações**.
A janela **Proteção em tempo real** é exibida.
5. Ative as configurações usando o botão **Proteção em tempo real**.

Se esse botão de alternância estiver ativado, a proteção do dispositivo móvel será ativada e o usuário não poderá desativá-la.

Se esse botão de alternância estiver desativado, a proteção do dispositivo móvel será ativada, mas poderá ser desativada manualmente pelo usuário.

6. Na lista suspensa **Verificação de aplicativos**, selecione o modo de verificação dos aplicativos:

- **Não verificar aplicativos**
- **Verificar apenas novos aplicativos e arquivos da pasta Downloads**
- **Verificar todos os aplicativos e monitorar ações com arquivos**

7. Na lista suspensa **Ação ao detectar ameaça**, selecione uma das seguintes opções:

- **Excluir**

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

- **Ignorar**

Se objetos detectados forem ignorados, o Kaspersky Endpoint Security for Android avisará o usuário sobre problemas na proteção do dispositivo. Para cada ameaça ignorada, o aplicativo oferece ações que o usuário pode executar para eliminar a ameaça. A lista de objetos ignorados pode mudar, por exemplo, se um arquivo malicioso for excluído ou movido. Para receber uma lista atualizada de ameaças, execute uma verificação completa no dispositivo. Para assegurar a proteção confiável dos dados, elimine todos os objetos detectados.

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

8. Para ativar a verificação adicional de novos aplicativos antes da primeira inicialização deles no dispositivo do usuário com ajuda do serviço na nuvem da Kaspersky Security Network, marque a caixa de seleção **Proteção adicional da Kaspersky Security Network**.

9. 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 legítimos que intrusos podem usar para comprometer o dispositivo e os dados do usuário**.

10. Clique em **OK**.

11. Clique em **Salvar** para salvar as alterações efetuadas.

As configurações do dispositivo móvel são alteradas após a próxima sincronização do dispositivo com o Kaspersky Security Center.

Configurar verificações de malware automáticas

Para configurar a execução automática da verificação de malware no dispositivo móvel:

1. Na janela principal do Kaspersky Next Expert View (cloud), selecione **Gerenciamento de ativos** → **Políticas**. Na lista de políticas de grupo aberta, clique no nome da política que deseja configurar.
2. Na janela de propriedades da política, selecione **Configurações do aplicativo**.
3. Selecione **Android** e vá para a seção **Proteção**.
4. No cartão **Verificar**, clique em **Configurações**.
A janela **Verificar** é exibida.
5. Ative as configurações usando o botão **Verificar**.
6. Na lista **Ação ao detectar ameaça**, selecione uma das seguintes opções:

- **Excluir**

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

- **Ignorar**

Se objetos detectados forem ignorados, o Kaspersky Endpoint Security for Android avisará o usuário sobre problemas na proteção do dispositivo. Para cada ameaça ignorada, o aplicativo oferece ações que o usuário pode executar para eliminar a ameaça. A lista de objetos ignorados pode mudar, por exemplo, se um arquivo malicioso for excluído ou movido. Para receber uma lista atualizada de ameaças, execute uma verificação completa no dispositivo. Para assegurar a proteção confiável dos dados, elimine todos os objetos detectados.

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

- **Perguntar ao usuário**

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

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 ou posterior. O Kaspersky Endpoint Security for Android solicita que o usuário defina o aplicativo como um recurso de Acessibilidade por meio do 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.

Se durante uma verificação o Kaspersky Endpoint Security for Android detectar aplicativos maliciosos nos dispositivos dos usuários, as ações serão diferentes dependendo do **modo de gerenciamento do dispositivo**.

Em dispositivos corporativos, os aplicativos maliciosos instalados detectados pelo Kaspersky Endpoint Security for Android são excluídos do dispositivo automaticamente se a opção **Excluir** estiver selecionada. Se o Kaspersky Endpoint Security for Android detectar aplicativos maliciosos do sistema, eles serão proibidos de serem exibidos e iniciados nos dispositivos dos usuários.

Em um contêiner corporativo, os aplicativos maliciosos instalados detectados pelo Kaspersky Endpoint Security for Android não são excluídos, mas proibidos de serem exibidos e iniciados nos dispositivos dos usuários sem notificar os usuários do dispositivo.

Se a opção **Perguntar ao usuário** estiver selecionada, o Kaspersky Endpoint Security for Android solicita que os usuários selecionem uma ação para cada aplicativo detectado, tanto em dispositivos corporativos quanto em dispositivos com um contêiner corporativo.

Os aplicativos maliciosos instalados não podem ser colocados em quarentena. Da mesma forma, se a opção **Excluir e salvar uma cópia de backup do arquivo na Quarentena** estiver selecionada, um aplicativo malicioso detectado será excluído.

Em dispositivos pessoais, os aplicativos maliciosos detectados não podem ser excluídos automaticamente. Nesse caso, o Kaspersky Endpoint Security for Android solicita que o usuário exclua ou ignore o aplicativo detectado.

7. No campo **Verificação programada**, é possível configurar a inicialização de uma verificação completa automática do sistema de arquivos do dispositivo.

8. Se você selecionou uma verificação semanal ou diária, especifique o dia da semana (para verificações semanais) e a hora de início nos campos **Dia** e **Hora**.

Se o dispositivo estiver no modo de economia de bateria, o aplicativo poderá executar essa tarefa mais tarde do que o especificado.

9. Clique em **OK**.

10. Clique em **Salvar** para salvar as alterações efetuadas.

As configurações do dispositivo móvel são alteradas após a 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 antimalware.

Por padrão, as atualizações do bancos de dados antimalware são desativadas quando o dispositivo estiver em modo de roaming. As atualizações agendadas dos bancos de dados antimalware não são executadas.

Configurar atualizações do banco de dados

Para definir as configurações para as atualizações do banco de dados antimalware:

1. Na janela principal do Kaspersky Next Expert View (cloud), selecione **Gerenciamento de ativos** → **Políticas**. Na lista de políticas de grupo aberta, clique no nome da política que deseja configurar.
2. Na janela de propriedades da política, selecione **Configurações do aplicativo**.

3. Selecione **Android** e vá para a seção **Proteção**.

4. No cartão **Atualização do banco de dados**, clique em **Configurações**.

A janela **Atualização do banco de dados** é exibida.

5. Ative as configurações usando o botão **Atualização do banco de dados**.

6. No campo **Atualização do banco de dados agendada**, defina as configurações para atualização automática do banco de dados antimalware no dispositivo do usuário.

7. Se você selecionou uma atualização semanal ou diária do banco de dados, especifique o dia da semana (para atualizações semanais do banco de dados) e a hora de início nos campos **Dia** e **Hora**.

Se o dispositivo estiver no modo de economia de bateria, o aplicativo poderá executar essa tarefa mais tarde do que o especificado.

8. Se você quiser 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 em roaming, marque a caixa de seleção **Permitir a atualização do banco de dados durante o roaming** na seção **Atualização do banco de dados durante o roaming**.

Mesmo que a caixa de seleção esteja desmarcada, o usuário pode manualmente iniciar uma atualização do bancos de dados antimalware quando o dispositivo está em roaming.

9. Clique em **OK**.

10. Clique em **Salvar** para salvar as alterações efetuadas.

As configurações do dispositivo móvel são alteradas após a próxima sincronização do dispositivo com o Kaspersky Security Center.

Proteção de dispositivos Android na Internet

Você pode usar a Proteção na Web para proteger dados pessoais de usuários de dispositivos móveis na Internet. A Proteção na Web bloqueia sites maliciosos que distribuem código malicioso e sites de phishing criados para roubar seus dados confidenciais e obter acesso às 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 está ativada por padrão.

No Yandex Browser e no Samsung Internet, URLs maliciosas e de phishing podem permanecer sem bloqueio. Isso ocorre porque somente o domínio do site é verificado. Se for um domínio malicioso ou de phishing, a Proteção na Web bloqueará a ameaça. Se o domínio não for classificado como malicioso ou de phishing, a URL específica não será bloqueada.

A Proteção na Web em dispositivos Android é compatível apenas com Google Chrome, HUAWEI Browser, Samsung Internet e Yandex Browser.

A Proteção na Web requer o seguinte para funcionar em um dispositivo gerenciado:

- O Kaspersky Endpoint Security for Android deve ser configurado como um serviço de acessibilidade.
- A Declaração sobre processamento de dados para uso da Proteção na Web (Declaração da Proteção na Web) deve ser aceita. 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.
- Em alguns dispositivos, o usuário deve conceder manualmente as seguintes [permissões](#):
 - Executar em segundo plano
 - Exibir janelas pop-up durante a execução em segundo plano
 - Exibir janela pop-up
 - Ignorar otimização de bateria

A Proteção na Web para o HUAWEI Browser, Samsung Internet e Yandex Browser não bloqueia sites em um dispositivo móvel se um contêiner corporativo for usado e a [Proteção na Web estiver ativada somente para o contêiner corporativo](#).

Para ativar a Proteção na Web:

1. Na janela principal do Kaspersky Next Expert View (cloud), selecione **Gerenciamento de ativos** → **Políticas**. Na lista de políticas de grupo aberta, clique no nome da política que deseja configurar.
2. Na janela de propriedades da política, selecione **Configurações do aplicativo**.
3. Selecione **Android** e vá para a seção **Proteção**.
4. No cartão **Proteção na Web**, ative as configurações usando o botão **Proteção na Web**.
5. Clique em **Ativar**.

Se você desativar a Proteção na Web, o [Controle da Web](#) também será desativado.

As configurações do dispositivo móvel são alteradas após a próxima sincronização do dispositivo com o Kaspersky Security Center.

Verificação de notificações de aplicativos de mensagens

O Kaspersky Endpoint Security for Android pode detectar phishing e URLs maliciosas em notificações do Telegram, WhatsApp, do aplicativo de SMS padrão e de outros aplicativos de mensagens comuns. Somente URLs expressas como texto diretamente no texto de notificação podem ser verificadas. URLs incorporadas na marcação não são verificadas.

As seguintes condições devem ser atendidas para ativar a verificação de notificações:

- A Proteção na Web deve estar ativada.
- A exibição de notificações deve ser permitida para os aplicativos de mensagens desejados. O Kaspersky Endpoint Security for Android verifica apenas notificações que podem ser exibidas na tela do dispositivo.
- Nos dispositivos Google Pixel e Vivo, a permissão "Conversas" deve ser concedida ao Kaspersky Endpoint Security nas configurações de acesso às notificações.

Para ativar a verificação de notificações:

1. Na janela principal do Kaspersky Next Expert View (cloud), selecione **Gerenciamento de ativos** → **Políticas**. Na lista de políticas de grupo aberta, clique no nome da política que deseja configurar.
2. Na janela de propriedades da política, selecione **Configurações do aplicativo**.
3. Selecione **Android** e vá para a seção **Proteção**.
4. No cartão **Proteção na Web**, marque a caixa de seleção **Bloquear notificações que contenham phishing e URLs maliciosas**.
5. Para permitir o acesso às notificações em um dispositivo móvel, consulte a seção [Proteção na Web](#).

O aplicativo agora verifica notificações para detectar phishing e URLs maliciosas. Se uma URL perigosa for encontrada, a notificação será bloqueada e uma tela de bloqueio com informações sobre a notificação bloqueada será exibida.

Se o Kaspersky Endpoint Security for Android não estiver ativado como um recurso de Acessibilidade, o aplicativo enviará uma notificação por push sobre as URLs perigosas detectadas em vez de exibir uma tela de bloqueio. Após tocar na notificação push, uma tela com informações sobre a notificação bloqueada é exibida.

Proteção de dados em um dispositivo perdido ou roubado

Essa seção descreve como você pode definir as configurações de acesso não autorizado no dispositivo caso ele seja perdido ou roubado.

Enviar comandos para um dispositivo móvel perdido ou roubado

Para proteger dados em um dispositivo móvel perdido ou roubado, você pode enviar comandos especiais.

É possível enviar comandos para os seguintes tipos de dispositivos móveis gerenciados:

- Dispositivos Android gerenciados pelo aplicativo Kaspersky Endpoint Security for Android
- Dispositivos iOS MDM

Cada tipo de dispositivo é compatível com um conjunto específico de comandos (consulte as tabelas abaixo).

Comandos para dispositivos Android

Comandos para proteger dados em um dispositivo Android perdido ou roubado

Comando	Resultado
Bloquear dispositivo	O dispositivo móvel é bloqueado. Para obter acesso aos dados, você deve desbloquear o dispositivo usando o comando Desbloquear dispositivo ou um código de uso único.
Desbloquear dispositivo	O dispositivo móvel está desbloqueado. Depois de desbloquear um dispositivo executando o Android 5 – 6, a senha de desbloqueio da tela é redefinida para "1234". Após desbloquear um dispositivo com Android 7 ou posterior, a senha de desbloqueio da tela não é alterada.
Redefinir as configurações padrão	Todos os dados são excluídos do dispositivo móvel e as suas configurações são redefinidas para seus valores de fábrica. Após este comando ter sido executado, o dispositivo não será capaz de receber ou executar comandos subsequentes. Esse comando não está disponível para dispositivos pessoais e dispositivos com contêiner corporativo executando o Android 14 ou posterior.
Limpar os dados corporativos	Dados corporativos são limpos no dispositivo. A lista de dados apagados depende do modo em que o dispositivo está operando: - Em um dispositivo pessoal, o contêiner Knox, os arquivos corporativos enviados ao dispositivo e o certificado de e-mail são apagados. - Além disso, se um contêiner corporativo foi criado, o contêiner corporativo (seu conteúdo, arquivos corporativos enviados ao dispositivo, configurações e restrições) e os certificados instalados no contêiner corporativo (certificados de perfil de e-mail, VPN e SCEP, exceto os certificados de dispositivos móveis) são apagados.
Localizar o dispositivo	As coordenadas de localização do dispositivo móvel são obtidas. Para visualizar a localização do dispositivo no Yandex.Maps, vá para a seção Gerenciamento de ativos → Móvel → Dispositivos. Em seguida, escolha um dispositivo e selecione Histórico de comandos → Localizar o dispositivo → Coordenadas do dispositivo → Visualização no mapa. Depois de clicar em Visualização no mapa, as coordenadas do dispositivo são transferidas para o Yandex.Maps e o dispositivo é exibido em um mapa. 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 nos últimos 30 minutos. Caso contrário, o comando falhará. Esse comando não funciona em dispositivos Android se a opção Precisão de localização do Google estiver desativada nas configurações. Observe que nem todos os dispositivos Android vêm com essa configuração de localização.
Alarme sonoro	O dispositivo móvel emite um alarme sonoro por 5 minutos (por 1 minuto se a bateria do dispositivo estiver fraca) ou até que o usuário desbloqueie o dispositivo.

Comandos para dispositivos iOS MDM

Comandos para proteger dados em um dispositivo iOS MDM perdido ou roubado

Comando	Resultado
Bloquear dispositivo	O dispositivo móvel é bloqueado. Para acessar os dados, é necessário desbloquear o dispositivo.
Redefinir a senha de desbloqueio	A senha de desbloqueio de tela do dispositivo móvel é redefinida, e o usuário recebe uma solicitação para definir uma nova senha de acordo com os requisitos da política.

Comando	Resultado
Redefinir as configurações padrão	Todos os dados são excluídos do dispositivo móvel e as suas configurações são redefinidas para seus valores de fábrica. Após este comando ter sido executado, o dispositivo não será capaz de receber ou executar comandos subsequentes.
Limpar os dados corporativos	Todos os perfis de configuração instalados, perfis de provisionamento, o perfil de gerenciamento e os aplicativos para os quais a caixa de seleção Remover quando o perfil de gerenciamento for excluído estiver marcada serão removidos do dispositivo.

Permissões para execução de comandos

São necessários direitos e permissões especiais para executar 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 essa etapa ou desativar esse serviço posteriormente nas configurações do dispositivo. Se este for o caso, será impossível executar os comandos.

Em dispositivos executando Android 10 ou posterior o usuário deve conceder permissão "Permitir o tempo todo" para acessar a localização. Em dispositivos executando Android 11 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. Recomendamos contatar o usuário diretamente, caso a permissão da câmera seja solicitada novamente.

Para obter a lista completa de comandos disponíveis, consulte a seção [Comandos para dispositivos móveis](#). Para saber mais sobre o envio de comandos a partir do Console de Administração, consulte a seção [Enviar comandos](#).

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 uso único 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 tiver sido adicionado à lista, você só pode desbloquear o dispositivo usando um código de uso único. Você não pode usar comandos para desbloquear o dispositivo.

Para saber mais sobre o envio de comandos da lista de dispositivos móveis no Kaspersky Next Expert View (cloud), consulte a seção [Enviar comandos](#).

Um *código de uso único do dispositivo* é um código secreto para desbloquear o dispositivo móvel. O código é gerado pelo Kaspersky Security Center e é exclusivo para cada dispositivo móvel. Você pode alterar o comprimento do código de uso único (4, 8, 12 ou 16 dígitos) nas configurações **Antirroubo** da política.

Para desbloquear um dispositivo móvel usando um código de uso único:

1. Na janela principal do Kaspersky Next Expert View (cloud), selecione **Gerenciamento de ativos** → **Móvel** → **Dispositivos**.
 2. Clique no dispositivo móvel para o qual você deseja obter um código de uso único.
 3. Selecione **Aplicativos** → **Kaspersky Mobile Devices Protection and Management**.
A janela de propriedades do Kaspersky Mobile Devices Protection and Management é exibida.
 4. Selecione a guia **Configurações do aplicativo**.
O código de uso único para o dispositivo selecionado será exibido no campo **Código de uso único** da seção **Código de uso único do dispositivo**.
 5. Use qualquer método disponível (como e-mail) para comunicar o código de uso único ao usuário do dispositivo bloqueado.
O usuário deve inserir o código de uso único na tela do dispositivo que está bloqueado pelo Kaspersky Endpoint Security for Android.
- O dispositivo móvel do usuário é desbloqueado.

Depois de desbloquear um dispositivo executando o Android 5 – 6, a senha de desbloqueio da tela é redefinida para "1234". Após desbloquear um dispositivo com Android 7 ou posterior, a senha de desbloqueio da tela não é alterada.

Para alterar o comprimento do código de uso único do dispositivo:

1. Na janela principal do Kaspersky Next Expert View (cloud), selecione **Gerenciamento de ativos** → **Políticas**. Na lista de políticas de grupo aberta, clique no nome da política que deseja configurar.
2. Na janela de propriedades da política, selecione **Configurações do aplicativo**.
3. Selecione **Android** e vá para a seção **Proteção**.
4. No cartão **Antirroubo**, clique em **Configurações**.
A janela **Antirroubo** é exibida.
5. Selecione o comprimento do código de uso único do dispositivo na lista suspensa correspondente. Por padrão, o código tem 4 dígitos.
6. Se você quiser entrar em contato com a pessoa que encontra o dispositivo móvel, no campo **Texto exibido no dispositivo bloqueado**, insira o texto da mensagem que será exibida na tela de bloqueio.
7. Clique em **OK**.
8. Clique em **Salvar** para salvar as alterações efetuadas.

O comprimento do código de uso único é definido para o valor selecionado.

As configurações do dispositivo móvel são alteradas após a próxima sincronização do dispositivo com o Kaspersky Security Center.

Configurar a força da senha de desbloqueio de dispositivo

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, você precisa configurar o uso de uma senha que o usuário é solicitado a inserir ao desbloquear o dispositivo.

Você pode impor restrições na atividade do usuário no dispositivo se a senha de desbloqueio do dispositivo for fraca (por exemplo, bloqueando 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 atende aos requisitos de segurança**.

Em determinados dispositivos Samsung que executam o Android 7 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 da proteção está ativada para o Kaspersky Endpoint Security for Android](#), e [requisitos de força estão definidos para a senha de desbloqueio da tela](#). Para desbloquear o dispositivo, é necessário [enviar um comando especial ao dispositivo](#).

Definir as configurações da senha de desbloqueio

Para configurar o uso de uma senha de desbloqueio:

1. Na janela principal do Kaspersky Next Expert View (cloud), selecione **Gerenciamento de ativos** → **Políticas**. Na lista de políticas de grupo aberta, clique no nome da política que deseja configurar.
2. Na janela de propriedades da política, selecione **Configurações do aplicativo**.
3. Selecione **Android** e vá para a seção **Controles de segurança**.
4. No cartão **Configurações de desbloqueio de tela**, clique em **Configurações**.
A janela **Configurações de desbloqueio de tela** é exibida.
5. Ative as configurações usando o botão **Configurações de desbloqueio de tela** se você quiser que o aplicativo verifique se uma senha de desbloqueio foi definida.

O botão neste cartão não ativa nem desativa a funcionalidade correspondente nos dispositivos. Ativar o botão permite definir configurações personalizadas. Desativar o botão permite usar as configurações padrão.

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 as seguintes opções, caso seja necessário:

- **Comprimento mínimo da senha**

Número mínimo de caracteres na senha de usuário. Valores possíveis: 4 a 16 caracteres.

A senha do usuário tem 4 caracteres por padrão.

O seguinte se aplica somente ao espaço pessoal do usuário e ao contêiner corporativo:

- No espaço pessoal do usuário, o Kaspersky Endpoint Security converte os requisitos de força da senha em um dos valores disponíveis no sistema: médio ou alto em dispositivos executando Android 10 ou posterior.
- No contêiner corporativo, o Kaspersky Endpoint Security converte os requisitos de força da senha em um dos valores disponíveis no sistema: médio ou alto em dispositivos executando Android 12 ou posterior.

Os valores são determinados usando as seguintes regras:

- Se o comprimento necessário da senha for de 1 a 4 caracteres, o aplicativo solicitará que o usuário defina uma senha de força média. Ela deve ser numérica (PIN), sem sequências repetidas ou ordenadas (por exemplo, 1234), ou alfabética/alfanumérica. O PIN ou a senha deve ter no mínimo 4 caracteres.
- Se o comprimento da senha for de 5 ou mais caracteres, o aplicativo solicitará que o usuário defina uma senha de alta segurança. Ela pode ser tanto numérica (PIN), sem números repetidos ou sequenciais, ou alfabética/alfanumérica (senha). Um PIN deve ter pelo menos 8 dígitos. Uma senha deve ter pelo menos 6 caracteres.

- **Permitir desbloqueio com identificação digital**

Especifica se impressões digitais podem ser usadas para desbloquear a tela.

A caixa de seleção não restringe o uso de um scanner de identificação digital ao fazer login em aplicativos ou ao confirmar compras.

Caso a caixa de seleção esteja marcada, o uso de impressões digitais no dispositivo móvel será permitido.

Caso a caixa de seleção esteja desmarcada, o Kaspersky Endpoint Security for Android bloqueará o uso de impressões digitais para desbloquear a tela. O usuário poderá desbloquear a tela somente com uma senha. Nas configurações do dispositivo, a opção de usar impressões digitais não estará disponível.

Esta caixa de seleção estará disponível apenas se a caixa de seleção **Permitir métodos de desbloqueio biométrico** estiver marcada.

Essa caixa de seleção é marcada por padrão.

Em alguns dispositivos Xiaomi com um contêiner corporativo, o contêiner corporativo pode ser desbloqueado por uma identificação digital somente se você definir o valor **Período de inatividade antes do contêiner corporativo ser bloqueado (s)** depois de definir uma identificação digital como o método de desbloqueio de tela.

7. Clique em **OK**.

8. Clique em **Salvar** para salvar as alterações efetuadas.

As configurações do dispositivo móvel são alteradas após a próxima sincronização do dispositivo com o Kaspersky Security Center.

Definir um código PIN em dispositivos HUAWEI

Alguns dispositivos HUAWEI exibem uma mensagem sobre o método de desbloqueio da tela ser muito simples.

Para definir um código PIN aceitável em um dispositivo HUAWEI, o usuário deve fazer o seguinte:

1. Na mensagem sobre o problema, toque no botão **Editar**.
2. Insira o código PIN atual.
3. Na janela **Definir nova senha**, toque no botão **Alterar método de desbloqueio**.
4. Selecione o método de desbloqueio **PIN personalizado**.
5. Defina o novo código PIN.

O código PIN deve estar em conformidade com os requisitos da política.

Um código PIN aceitável está configurado no dispositivo.

Configurar uma senha forte de desbloqueio para dispositivos iOS MDM

Essas configurações se aplicam aos dispositivos no modo de operação "Perfil de gerenciamento".

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 sequenciais 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 definir as configurações da força para uma senha de desbloqueio em um dispositivo iOS MDM:

1. Na janela principal do Kaspersky Next Expert View (cloud), selecione **Gerenciamento de ativos** → **Políticas**. Na lista de políticas de grupo aberta, clique no nome da política que deseja configurar.
2. Na janela de propriedades da política, selecione **Configurações do aplicativo**.
3. Selecione **iOS** e vá para a seção **Controles de segurança**.
4. No cartão **Configurações de desbloqueio de tela**, clique em **Configurações**.
A janela **Configurações de desbloqueio de tela** é exibida.
5. Ative as configurações usando o botão **Configurações de desbloqueio de tela**.

O botão neste cartão não ativa nem desativa a funcionalidade correspondente nos dispositivos. Ativar o botão permite definir configurações personalizadas. Desativar o botão permite usar as configurações padrão.

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**. Mesmo se a caixa de seleção estiver desmarcada, o usuário poderá definir uma senha com menos de 6 caracteres.
- 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 "\$", "&", "!").

Em alguns dispositivos iOS MDM, se o valor **Número mínimo de caracteres especiais** for especificado e a caixa de seleção **Permitir senha simples** estiver marcada, o dispositivo exibirá informações sobre como definir uma senha de 6 ou mais caracteres, mesmo que seja possível definir uma senha de 4 ou mais caracteres.

- No campo **Tempo de vida máximo da senha (dias)**, especifique o período de tempo em dias durante o qual a senha permanecerá atual. Quando este período expira, o Servidor de MDM do iOS solicita que o usuário troque a senha.
- Na lista **Bloqueio automático**, selecione o período de tempo depois do qual o bloqueio automático deve ser ativado no dispositivo iOS MDM. Se o dispositivo móvel permanecer inativo por esse período, ele entrará no modo de espera.

Em diferentes dispositivos iOS MDM, o tempo real de bloqueio automático do dispositivo pode ser diferente do valor que você especificou:

Em dispositivos iPhone: se você definir o Bloqueio automático em 10 ou 15 minutos, o dispositivo será bloqueado em 5 minutos.

Em dispositivos iPad: se você definir o Bloqueio automático em 1 a 4 minutos, o dispositivo será bloqueado em 2 minutos.

Para outros valores, o tempo real do bloqueio automático do dispositivo coincide com o tempo especificado.

- No campo **Reutilização de senhas anteriores**, especifique o número de senhas usadas (incluindo a senha atual) que o Servidor de MDM do iOS comparará com a nova senha quando o usuário alterar a senha atual. A nova senha será rejeitada se corresponder à senha atual.
- Na lista **Tempo máximo para desbloqueio 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 incorretas da senha**, selecione o número de tentativas de senha com falha que o sistema permite ao usuário antes de apagar o dispositivo.

Se o valor for 6 ou menos, o sistema não aplica atraso e apaga todos os dados e configurações do dispositivo iOS assim que o usuário excede o limite definido.

Se o valor for maior que 7, após 6 tentativas sem sucesso, o dispositivo impõe um atraso antes que o usuário possa inserir novamente a senha de desbloqueio. O atraso começa após a sexta tentativa e aumenta a cada tentativa malsucedida. Após a tentativa final com falha, o sistema apaga todos os dados e configurações de um dispositivo iOS.

Por padrão, o número de tentativas de inserção de senha não é limitado.

Se o usuário exceder o número máximo de tentativas malsucedidas de senha, o dispositivo será redefinido para as configurações padrão.

7. Clique em **Salvar** para salvar as alterações efetuadas.

As configurações do dispositivo móvel são alteradas após a próxima sincronização do dispositivo com o Servidor de MDM do iOS.

Como resultado, depois que a política é aplicada, o Servidor de MDM do 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 será solicitado a alterar 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 um dispositivo Android à Internet de forma segura e proteger a transferência de dados, você pode definir as configurações da VPN (Rede Virtual Privada).

A configuração da VPN é possível apenas para os dispositivos Samsung que executam a versão 11 ou anterior do Android.

Os seguintes requisitos devem ser considerados ao usar uma rede privada virtual:

- O aplicativo que usa a conexão VPN deve ser permitido nas configurações do [Firewall](#).
- As configurações da VPN 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. Na janela principal do Kaspersky Next Expert View (cloud), selecione **Gerenciamento de ativos** → **Políticas**. Na lista de políticas de grupo aberta, clique no nome da política que deseja configurar.
2. Na janela de propriedades da política, selecione **Configurações do aplicativo**.
3. Selecione **Android** e vá para a seção **Configurações do Samsung Knox**.
4. No cartão **VPN**, clique em **Configurações**.
A janela **VPN** se abre.

5. Ative as configurações usando o botão **VPN**.

6. Especificar as seguintes configurações da VPN:

- Configurações na seção **Rede**:
 - No campo **Nome da rede**, insira o nome do túnel VPN.
 - Na lista suspensa **Protocolo**, selecione o tipo de conexão VPN:
 - **IPSec Xauth PSK**. Um protocolo de túnel do tipo "gateway-to-gateway" que permite ao usuário do dispositivo móvel estabelecer uma conexão segura com o servidor VPN utilizando o utilitário de autenticação Xauth.
 - **L2TP IPSec PSK**. Um protocolo de túnel do tipo "gateway-to-gateway" que permite ao usuário do dispositivo móvel estabelecer uma conexão segura com o servidor VPN por meio do protocolo IKE utilizando uma chave predefinida. Esse protocolo é marcado por padrão.
 - **PPTP**. Um protocolo de túnel "point-to-point" que permite ao usuário do dispositivo móvel estabelecer uma conexão segura com o servidor VPN criando um túnel especial em uma rede padrão desprotegida.
 - No campo **Endereço do servidor**, insira o nome de rede ou endereço IP do servidor da VPN.
- Configurações na seção **Configurações do protocolo**:
 - Na lista **Domínio(s) de procura 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.
 - No campo **Servidor(es) 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.
 - 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.

7. Ainda, defina as seguintes configurações:

- Para os protocolos **IPSec Xauth PSK** e **L2TP IPSec PSK**:
 - No campo **Chave compartilhada IPSec**, insira a senha para a chave de segurança IPSec predefinida.
 - No campo **ID IPSec**, insira o nome do usuário do dispositivo móvel.
- Para o protocolo **L2TP IPSec PSK**, especifique a senha para a chave L2TP que no campo **Chave L2TP**.
- Para a rede **PPTP**, selecione a caixa de seleção **Usar 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.

8. Clique em **Salvar** para salvar as alterações efetuadas.

As configurações do dispositivo móvel são alteradas após a próxima sincronização do dispositivo com o Kaspersky Security Center.

Configurar a VPN em dispositivos iOS MDM

Essas configurações se aplicam aos dispositivos no modo de operação “Perfil de gerenciamento”.

Para conectar um dispositivo iOS MDM à uma rede virtual privada (VPN) e proteger os dados enquanto conectado a ela, defina as configurações de conexão da VPN.

Para configurar a conexão da VPN no dispositivo iOS MDM de um usuário:

1. Na janela principal do Kaspersky Next Expert View (cloud), selecione **Gerenciamento de ativos** → **Políticas**. Na lista de políticas de grupo aberta, clique no nome da política que deseja configurar.
2. Na janela de propriedades da política, selecione **Configurações do aplicativo**.
3. Selecione **iOS** e vá para a seção **Configuração do dispositivo**.
4. No cartão **VPN**, clique em **Configurações**.
A janela **VPN** se abre.
5. Ative as configurações usando o botão **VPN**.
6. Clique em **Adicionar**.
A janela **Adicionar configuração de VPN** é exibida.
7. Na guia **Geral**, na seção **Rede**, defina as seguintes configurações:
 - a. No campo **Nome da rede**, insira o nome do túnel VPN.
 - b. Na lista suspensa **Protocolo**, selecione o **tipo de conexão VPN**.
 - **L2TP** (Layer 2 Tunneling Protocol). A conexão é compatível com a autenticação do usuário do dispositivo iOS MDM utilizando senhas MS-CHAP v2, autenticação de dois fatores e autenticação automática utilizando uma chave pública.
 - **IPSec**. A conexão é compatível com a autenticação de usuário baseada em senha, autenticação de dois fatores e autenticação automática utilizando uma chave pública e certificados.
 - **Cisco AnyConnect**. A conexão é compatível com o firewall Cisco Adaptive Security Appliance (ASA) versão 8.0(3).1 ou posterior. Para configurar uma conexão VPN, instale o aplicativo Cisco AnyConnect a partir da App Store no dispositivo iOS MDM.
 - **Juniper SSL**. A conexão é compatível com 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 uma conexão VPN, instale o aplicativo JUNOS a partir da App Store no dispositivo iOS MDM.
 - **F5 SSL**. A conexão é compatível com as soluções F5 BIG-IP Edge Gateway, Access Policy Manager e Fire SSL VPN. Para configurar uma conexão VPN, instale o aplicativo F5 BIG-IP Edge Client a partir da App Store no dispositivo iOS MDM.

- **SonicWALL Mobile Connect.** A conexão é compatível com 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 E-Class NSA com SonicOS versão 5.8.1.0 ou posterior. Para configurar uma conexão VPN, instale o aplicativo SonicWALL Mobile Connect a partir da App Store no dispositivo iOS MDM.
- **Aruba VIA.** A conexão é compatível com controladores de acesso móvel Aruba Networks. Para configurá-los, instale o aplicativo Aruba Networks VIA a partir da App Store no dispositivo iOS MDM.
- **SSL personalizado.** A conexão suporta a autenticação do usuário do dispositivo iOS MDM utilizando senhas e certificados e autenticação de dois fatores.

c. No campo **Endereço do servidor**, insira o nome de rede ou endereço IP do servidor da VPN.

8. Especifique as **configurações para a conexão VPN** de acordo com o tipo selecionado de rede privada virtual.

- **L2TP**

- Configurações na seção **Autenticação**:

- **Tipo de autenticação**

Autenticação de dois fatores de um usuário de dispositivo iOS MDM usando um token RSA SecurID ou autenticação baseada em senha.

- **Nome da conta**

O nome da conta para autorização no servidor VPN.

- **Senha**

A senha da conta para autenticação na rede particular virtual.

- **Método de autenticação**

O método de autenticação de usuários do dispositivo iOS MDM na rede privada virtual.

- **Segredo compartilhado**

Senha para uma chave IPsec predefinida para os protocolos L2TP e IPsec (Cisco).

- **Certificado de autenticação**

O certificado usado para autenticação do usuário.

- Configurações na seção **Outro**:

- **Enviar todo o tráfego pela VPN**

Transmissão de todo o tráfego de saída por meio de uma conexão VPN se um serviço de rede diferente for utilizado (por exemplo: AirPort ou Ethernet).

Se a caixa de seleção estiver marcada, todo o tráfego é enviado por meio de uma conexão VPN.

Se a caixa de seleção estiver desmarcada, o tráfego de saída é transmitido sem o uso obrigatório da conexão VPN.

Essa caixa de seleção é desmarcada por padrão.

- **IPSec**

- Configurações na seção **Autenticação**:

- **Método de autenticação**

- O método de autenticação de usuários do dispositivo iOS MDM na rede privada virtual.

- **Nome da conta**

- O nome da conta para autorização no servidor VPN.

- **Senha**

- A senha da conta para autenticação na rede particular virtual.

- **Segredo compartilhado**

- Senha para uma chave IPSec predefinida para os protocolos L2TP e IPSec (Cisco).

- **Nome do grupo**

- Nome do grupo de dispositivos iOS MDM que se conectam à VPN por meio de protocolos L2TP e IPSec (Cisco). Se a caixa de seleção **Usar autenticação híbrida** for marcada, o nome do grupo deve terminar com "[hybrid]" (por exemplo: "mycompany [hybrid]").

- **Usar autenticação híbrida**

- Utilização de autenticação híbrida quando o usuário se conecta a uma VPN. O servidor VPN utiliza um certificado para autenticação, e o usuário do dispositivo iOS MDM insere uma chave pública para autenticação por meio do protocolo IPSec (Cisco).

- Se a caixa de seleção for marcada, a autenticação híbrida é utilizada quando o usuário conecta-se a uma VPN.

- Se a caixa de seleção for desmarcada, a autenticação híbrida não é utilizada.

- Essa caixa de seleção é desmarcada por padrão.

- **Certificado de autenticação**

- O certificado usado para autenticação do usuário.

- Configurações na seção **Domínios**:

- **Ativar a VPN ao se conectar a domínios especificados**

- Os domínios para os quais a conexão VPN será ativada.

- Configurações na seção **Outro**:

- **Solicitar PIN**

- O aplicativo verifica se a senha do sistema está definida quando o dispositivo móvel é ligado.

- Se a caixa de seleção estiver marcada, o Kaspersky Mobile Devices Protection and Management verifica se a senha do sistema foi definida no dispositivo. Se nenhuma senha do sistema estiver definida no dispositivo, o usuário precisará defini-la. A senha deve ser definida de acordo com as definições configuradas pelo administrador.

- Se a caixa de seleção estiver desmarcada, o Kaspersky Mobile Devices Protection and Management não requer uma senha do sistema.

Essa caixa de seleção é desmarcada por padrão.

- **Cisco AnyConnect**

- Configurações na seção **Rede**:

- **Tempo ocioso antes da desconexão (min)**

- O tempo de espera antes de desconectar uma conexão sob demanda.

- Configurações na seção **Autenticação**:

- **Método de autenticação**

- O método de autenticação de usuários do dispositivo iOS MDM na rede privada virtual.

- **Nome da conta**

- O nome da conta para autorização no servidor VPN.

- **Senha**

- A senha da conta para autenticação na rede particular virtual.

- **Grupo**

- Codinome do grupo de túnel para clientes Cisco AnyConnect conectando-se à VPN.

- **Certificado de autenticação**

- O certificado usado para autenticação do usuário.

- Configurações na seção **Domínios**:

- **Ativar a VPN ao se conectar a domínios especificados**

- Os domínios para os quais a conexão VPN será ativada.

- Configurações na seção **Outro**:

- **Enviar todo o tráfego pela VPN**

- Roteia todo o tráfego pela VPN.

- **Excluir tráfego local**

- Exclui o tráfego local do tráfego roteado através da conexão VPN.

- Essa caixa de seleção estará disponível se a caixa de seleção **Enviar todo o tráfego pela VPN** estiver marcada.

- **Juniper SSL**

- Configurações na seção **Rede**:

- **Tempo ocioso antes da desconexão (min)**

- O tempo de espera antes de desconectar uma conexão sob demanda.

- Configurações na seção **Autenticação**:

- **Método de autenticação**

- O método de autenticação de usuários do dispositivo iOS MDM na rede privada virtual.

- **Nome da conta**

- O nome da conta para autorização no servidor VPN.

- **Senha**

- A senha da conta para autenticação na rede particular virtual.

- **Escopo**

- Nome da rede que inclui servidores VPN e dispositivos iOS MDM para a conexão VPN estabelecida utilizando Juniper SSL.

- **Função**

- Nome da função do usuário que concede o acesso de usuário a recursos utilizando Juniper SSL. Uma função pode combinar vários usuários executando funções similares.

- **Certificado de autenticação**

- O certificado usado para autenticação do usuário.

- Configurações na seção **Domínios**:

- **Ativar a VPN ao se conectar a domínios especificados**

- Os domínios para os quais a conexão VPN será ativada.

- Configurações na seção **Outro**:

- **Enviar todo o tráfego pela VPN**

- Roteia todo o tráfego pela VPN.

- **Excluir tráfego local**

- Exclui o tráfego local do tráfego roteado através da conexão VPN.

- Essa caixa de seleção estará disponível se a caixa de seleção **Enviar todo o tráfego pela VPN** estiver marcada.

- **F5 SSL**

- Configurações na seção **Rede**:

- **Tempo ocioso antes da desconexão (min)**

- O tempo de espera antes de desconectar uma conexão sob demanda.

- Configurações na seção **Autenticação**:

- **Método de autenticação**

O método de autenticação de usuários do dispositivo iOS MDM na rede privada virtual.

- **Nome da conta**

O nome da conta para autorização no servidor VPN.

- **Senha**

A senha da conta para autenticação na rede particular virtual.

- **Certificado de autenticação**

O certificado usado para autenticação do usuário.

- Configurações na seção **Domínios**:

- **Ativar a VPN ao se conectar a domínios especificados**

Os domínios para os quais a conexão VPN será ativada.

- Configurações na seção **Outro**:

- **Enviar todo o tráfego pela VPN**

Roteia todo o tráfego pela VPN.

- **Excluir tráfego local**

Exclui o tráfego local do tráfego roteado através da conexão VPN.

Essa caixa de seleção estará disponível se a caixa de seleção **Enviar todo o tráfego pela VPN** estiver marcada.

- **SonicWALL Mobile Connect**

- Configurações na seção **Rede**:

- **Tempo ocioso antes da desconexão (min)**

O tempo de espera antes de desconectar uma conexão sob demanda.

- Configurações na seção **Autenticação**:

- **Método de autenticação**

O método de autenticação de usuários do dispositivo iOS MDM na rede privada virtual.

- **Nome da conta**

O nome da conta para autorização no servidor VPN.

- **Senha**

A senha da conta para autenticação na rede particular virtual.

- **Domínio ou grupo**

Nome do domínio no servidor SSL VPN (exemplo: vpn.company.com) ou o nome de um grupo de usuário SonicWALL Mobile Connect.

- **Certificado de autenticação**

O certificado usado para autenticação do usuário.

- Configurações na seção **Domínios**:

- **Ativar a VPN ao se conectar a domínios especificados**

Os domínios para os quais a conexão VPN será ativada.

- Configurações na seção **Outro**:

- **Enviar todo o tráfego pela VPN**

Roteia todo o tráfego pela VPN.

- **Excluir tráfego local**

Exclui o tráfego local do tráfego roteado através da conexão VPN.

Essa caixa de seleção estará disponível se a caixa de seleção **Enviar todo o tráfego pela VPN** estiver marcada.

- **Aruba VIA**

- Configurações na seção **Rede**:

- **Tempo ocioso antes da desconexão (min)**

O tempo de espera antes de desconectar uma conexão sob demanda.

- Configurações na seção **Autenticação**:

- **Método de autenticação**

O método de autenticação de usuários do dispositivo iOS MDM na rede privada virtual.

- **Nome da conta**

O nome da conta para autorização no servidor VPN.

- **Senha**

A senha da conta para autenticação na rede particular virtual.

- **Certificado de autenticação**

O certificado usado para autenticação do usuário.

- Configurações na seção **Domínios**:

- **Ativar a VPN ao se conectar a domínios especificados**

Os domínios para os quais a conexão VPN será ativada.

- Configurações na seção **Outro**:

- **Enviar todo o tráfego pela VPN**

Roteia todo o tráfego pela VPN.

- **Excluir tráfego local**

Exclui o tráfego local do tráfego roteado através da conexão VPN.

Essa caixa de seleção estará disponível se a caixa de seleção **Enviar todo o tráfego pela VPN** estiver marcada.

- **SSL personalizado**

- Configurações na seção **Rede**:

- **Tempo ocioso antes da desconexão (min)**

O tempo de espera antes de desconectar uma conexão sob demanda.

- Configurações na seção **Dados da configuração**:

- **Chave**

Contém uma chave com configurações adicionais para a conexão SSL personalizada.

- **Valor**

Contém um valor com configurações adicionais para a conexão SSL personalizada.

- Configurações na seção **Autenticação**:

- **Método de autenticação**

O método de autenticação de usuários do dispositivo iOS MDM na rede privada virtual.

- **Nome da conta**

O nome da conta para autorização no servidor VPN.

- **Senha**

A senha da conta para autenticação na rede particular virtual.

- **Certificado de autenticação**

O certificado usado para autenticação do usuário.

- **ID do pacote**

Se a configuração de VPN personalizada tiver como alvo uma solução de VPN que usa um provedor de extensão de rede, esse campo conterá o identificador de pacote do aplicativo que contém o contêiner do provedor. Entre em contato com o fornecedor da solução VPN para obter o valor do identificador.

- Configurações na seção **Domínios**:

- **Ativar a VPN ao se conectar a domínios especificados**

Os domínios para os quais a conexão VPN será ativada.

9. Se necessário, na guia **Avançado**, na seção **Servidor proxy**, defina as configurações da conexão VPN por meio de um servidor proxy:

a. Marque a caixa de seleção **Usar um servidor proxy**.

b. Configure uma conexão com um servidor proxy:

a. Se você quiser configurar a conexão automaticamente:

- Selecione **Automático**.
- No campo **URL do arquivo PAC**, especifique a URL do arquivo proxy PAC.
- 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 conexão direta se não for possível acessar o arquivo PAC**.

b. Se você quiser configurar a conexão manualmente:

- Selecione **Manual**.
- Nos campos **Endereço do servidor proxy** e **Porta do servidor proxy**, insira o endereço IP ou nome DNS do servidor proxy e número da porta.
- No campo **Nome de usuário**, selecione uma macro que será usada como um nome de usuário para a conexão com o servidor proxy.

c. No campo **Senha**, especifique a senha para a conexão com o servidor proxy.

10. Clique em **Adicionar**.

A nova VPN é exibida na lista.

Você pode modificar ou excluir a VPN da lista usando os botões **Editar** e **Excluir** na parte superior da lista.

11. Clique em **Salvar** para salvar as alterações efetuadas.

As configurações do dispositivo móvel são alteradas após a próxima sincronização do dispositivo com o Servidor de MDM do iOS.

Como resultado, depois que a política é aplicada, a conexão VPN será configurada no dispositivo iOS MDM do usuário.

Configurar o Firewall em dispositivos Android (somente Samsung)

Especifique as configurações do Firewall para monitorar conexões de rede no dispositivo móvel do usuário.

O Firewall pode ser configurado apenas em dispositivos Samsung que executam Android 15 ou versões anteriores.

Para configurar o Firewall em um dispositivo móvel de um usuário:

1. Na janela principal do Kaspersky Next Expert View (cloud), selecione **Gerenciamento de ativos** → **Políticas**. Na lista de políticas de grupo aberta, clique no nome da política que deseja configurar.
2. Na janela de propriedades da política, selecione **Configurações do aplicativo**.
3. Selecione **Android** e vá para a seção **Configurações do Samsung Knox**.
4. Na placa **Firewall**, clique em **Configurações**.
A janela **Firewall** é exibida.
5. Ative as configurações usando o botão **Firewall**.
6. Na lista suspensa **Acesso à Internet**, selecione o modo do Firewall. Dependendo do modo de operação, o Firewall monitora conexões estabelecidas pelo dispositivo móvel do usuário:
 - Se você quiser permitir conexões de entrada e saída de todos os aplicativos instalados, selecione **Permitir para todos os aplicativos**. Este modo é selecionado por padrão.
 - Se você quiser bloquear todas as atividades de rede, exceto para vários aplicativos específicos, selecione **Permitir para aplicativos listados**.
7. Se você selecionou **Permitir para aplicativos listados** como o modo Firewall, crie uma lista de aplicativos para os quais todas as atividades de rede são permitidas:
 - a. Na seção **Aplicativos com acesso à Internet**, clique em **Adicionar**.
A janela **Adicionar aplicativo** é exibida.
 - 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 **Adicionar**.

O novo aplicativo para o qual o Firewall está desativado aparece na lista.

Você pode modificar ou excluir aplicativos de dispositivos móveis da lista usando os botões **Editar** e **Excluir** na parte superior da lista.

8. Clique em **OK**.
9. Clique em **Salvar** para salvar as alterações efetuadas.

As configurações do dispositivo móvel são alteradas após a próxima sincronização do dispositivo com o Kaspersky Security Center.

Proteger o Kaspersky Endpoint Security for Android contra a remoção

Para a proteção de dispositivos móveis 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 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 da proteção está ativada para o Kaspersky Endpoint Security for Android](#), e [requisitos de força estão definidos para a senha de desbloqueio da tela](#). Para desbloquear o dispositivo, é necessário [enviar um comando especial ao dispositivo](#).

Para proteger o aplicativo da remoção em dispositivos que executam o Android 7 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 essa etapa ou desativar esse serviço posteriormente nas configurações do dispositivo. Se este for o caso, o aplicativo não é protegido contra a remoção.

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

1. Na janela principal do Kaspersky Next Expert View (cloud), selecione **Gerenciamento de ativos** → **Políticas**. Na lista de políticas de grupo aberta, clique no nome da política que deseja configurar.
2. Na janela de propriedades da política, selecione **Configurações do aplicativo**.
3. Selecione **Android** e vá até a seção **Configurações do KES for Android**.
4. No cartão **Configurar o acesso às configurações do aplicativo**, clique em **Configurações**.
A janela **Configurar o acesso às configurações do aplicativo** se abre.
5. Ative as configurações usando o botão **Configurar o acesso às configurações do aplicativo**.

O botão neste cartão não ativa nem desativa a funcionalidade correspondente nos dispositivos. Ativar o botão permite definir configurações personalizadas. Desativar o botão permite usar as configurações padrão.

6. Desmarque a caixa de seleção **Permitir a remoção do aplicativo do dispositivo**.
7. Clique em **OK**.
8. Clique em **Salvar** para salvar as alterações efetuadas.

As configurações do dispositivo móvel são alteradas após a próxima sincronização do dispositivo com o Kaspersky Security Center. Se uma tentativa for feita para remover o aplicativo, o dispositivo móvel será bloqueado.

Detectar dispositivos invadidos

O Kaspersky Next Expert View (cloud) permite detectar dispositivos Android invadidos (com root) e jailbreaks em dispositivos iOS. Os arquivos do sistema ficam desprotegidos em dispositivos hackeados, podendo, portanto, ser modificados. Se uma tentativa de invasão for detectada, recomendamos restaurar imediatamente a operação normal do dispositivo.

Em caso de invasão do dispositivo, uma notificação será enviada ao usuário. É possível visualizar as notificações de invasão no Kaspersky Next Expert View (cloud) na seção **Monitoramento** → **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). Você pode impor restrições usando o componente Controle de conformidade. Para isso, [crie uma regra de conformidade](#) com o critério **O dispositivo foi roteado**.

Configurar um proxy HTTP global em dispositivos iOS MDM

Essas configurações se aplicam aos dispositivos no modo de operação “Perfil de gerenciamento”.

Para fazer o roteamento do tráfego da Internet do usuário, configure a conexão do dispositivo iOS MDM com a Internet por meio de um servidor proxy.

Tenha cuidado ao definir essas configurações. Se as configurações estiverem incorretas, os dispositivos poderão perder a conexão com a Internet e não serão sincronizados com o servidor iOS MDM. Se isso acontecer, será necessário adicionar os dispositivos novamente.

Para especificar as configurações do servidor proxy HTTP global no dispositivo iOS MDM do usuário:

1. Na janela principal do Kaspersky Next Expert View (cloud), selecione **Gerenciamento de ativos** → **Políticas**. Na lista de políticas de grupo aberta, clique no nome da política que deseja configurar.
2. Na janela de propriedades da política, selecione **Configurações do aplicativo**.
3. Selecione **iOS** e vá para a seção **Configuração do dispositivo**.
4. No cartão **Proxy HTTP global**, clique em **Configurações**.
A janela **Proxy HTTP global** é exibida.
5. Ative as configurações usando o botão **Proxy HTTP global**.
6. Selecione o tipo de configuração de proxy HTTP global:
 - Para especificar as configurações de conexão com o servidor proxy manualmente:
 - a. Na seção **Tipo de configuração**, selecione **Manual**.
 - b. Nos campos **Endereço do servidor proxy** e **Porta do servidor proxy**, insira o nome de um host ou do endereço IP de um servidor proxy e o número da porta do servidor proxy.

- c. No campo **Nome de usuário**, defina o nome da conta de usuário para autorização no servidor proxy.
- d. No campo **Senha**, defina a senha para a 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 cativas sem conectar o proxy**.
- Para especificar as configurações da conexão ao servidor proxy usando um arquivo PAC (Proxy Auto Configuration) predefinido:
 - a. Na seção **Tipo de configuração**, 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 conexão direta se não for possível acessar o arquivo PAC**.
 - d. Para permitir que o usuário acesse redes cativas, selecione a caixa **Permitir o acesso às redes cativas sem conectar o proxy**.

7. Clique em **OK**.

8. Clique em **Salvar** para salvar as alterações efetuadas.

Como resultado, o usuário do dispositivo móvel se conectará à Internet por meio de um servidor proxy depois que a política for aplicada.

Adicionar certificados de segurança aos dispositivos iOS MDM

Essas configurações se aplicam aos dispositivos no modo de operação "Perfil de gerenciamento".

Você pode adicionar certificados aos dispositivos iOS MDM para simplificar a autenticação do usuário e garantir a segurança dos dados. Os dados assinados com um certificado são protegidos contra modificação enquanto são transferidos pela rede. A criptografia de dados usando um certificado fornece um nível adicional de segurança para os dados. O certificado também pode ser usado para verificar a identidade do usuário.

O Kaspersky Mobile Devices Protection and Management é compatível com 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 privada.

Para adicionar um certificado de segurança a dispositivos iOS MDM:

1. Na janela principal do Kaspersky Next Expert View (cloud), selecione **Gerenciamento de ativos** → **Políticas**. Na lista de políticas de grupo aberta, clique no nome da política que deseja configurar.
2. Na janela de propriedades da política, selecione **Configurações do aplicativo**.
3. Selecione **iOS** e vá para a seção **Configuração do dispositivo**.

4. No cartão **Gerenciamento de certificados**, clique em **Configurações**.

A janela **Gerenciamento de certificados** é exibida.

5. Ative as configurações usando o botão **Gerenciamento de certificados**.

6. Clique em **Carregar** e especifique o caminho para o certificado.

Os arquivos de certificados PKCS#1 têm as extensões CER, DER ou PEM. Os arquivos de certificados PKCS#12 têm as extensões P12 ou PFX. A senha para um certificado PKCS#12 não deve estar em branco.

7. Clique em **Abrir**.

Se o certificado for protegido por senha, insira-a. O novo certificado é exibido na lista.

8. Clique em **OK**.

9. Clique em **Salvar** para salvar as alterações efetuadas.

As configurações do dispositivo móvel são alteradas após a próxima sincronização do dispositivo com o Servidor de MDM do iOS.

Como resultado, depois que a política é aplicada, os certificados são instalados automaticamente nos dispositivos.

Adicionar um perfil SCEP aos dispositivos iOS MDM

Essas configurações se aplicam aos dispositivos no modo de operação "Perfil de gerenciamento".

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 feitas três tentativas de sondagem do servidor SCEP em intervalos de 10 segundos. Se todas as tentativas de assinar o certificado falharem, você precisará gerar uma nova solicitação de assinatura do certificado.
- O certificado 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. Na janela principal do Kaspersky Next Expert View (cloud), selecione **Gerenciamento de ativos** → **Políticas**. Na lista de políticas de grupo aberta, clique no nome da política que deseja configurar.
2. Na janela de propriedades da política, selecione **Configurações do aplicativo**.
3. Selecione **iOS** e vá para a seção **Configuração do dispositivo**.

4. No cartão **SCEP**, clique em **Configurações**.

A janela **SCEP** é exibida.

5. Ative as configurações usando o botão **SCEP**.

6. Clique em **Adicionar**.

A janela **Adicionar perfil SCEP** é exibida.

7. Na seção **Servidor SCEP**, especifique as seguintes configurações do servidor SCEP:

- No campo **Nome da configuração**, especifique o nome do Centro de Certificação implementado no servidor SCEP. O centro de certificação fornece ao usuário de um dispositivo iOS MDM certificados utilizando o Simple Certificate Enrollment Protocol (SCEP).
- No campo **URL do servidor**, insira o endereço da Web do servidor SCEP onde o Centro de Certificação será implementado.
A URL pode conter o endereço IP ou o nome de domínio completo (FQDN). Por exemplo:
`http://10.10.10.10/certserver/companyscep`.
- No campo **Número máximo de tentativas de verificação periódica**, especifique o número máximo de tentativas de sondagem do servidor SCEP para obter o certificado assinado. Por padrão, o máximo são 3 tentativas.
Se todas as tentativas de assinar o certificado falharem, você precisará gerar uma nova solicitação de assinatura do certificado.
- No campo **Intervalo da verificação periódica (seg.)**, especifique o número de segundos entre as tentativas de sondagem do servidor SCEP para obter o certificado assinado. Por padrão, o valor é 10 segundos.
- No campo **Frase-desafio estática**, insira uma chave de registro pré-publicada.
Antes de assinar um certificado, o servidor SCEP solicita que o usuário do dispositivo móvel insira a chave. Se este campo estiver em branco, o SCEP não solicitará a chave.
- Na lista suspensa **Método de carregamento de impressão digital do certificado**, selecione como adicionar uma impressão digital do certificado. Você pode utilizar impressões digitais de certificado baseadas no algoritmo de hash SHA-1 ou MD5.
 - Se você selecionou a opção **Manualmente**, no campo **Impressão digital do certificado** exibido, insira uma impressão digital exclusiva do certificado para verificar a autenticidade da resposta do Centro de Certificação.
 - Se você selecionou a opção **Do arquivo**, carregue um arquivo CER, KEY ou PEM. A impressão digital será gerada e adicionada 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.

8. Na seção **Assunto**, especifique as seguintes configurações:

- No campo **Nome do assunto**, insira uma cadeia com os atributos do usuário do dispositivo iOS MDM que estão incluídos no certificado X.500.

Os atributos podem conter detalhes do país (C), localidade (L), estado (ST), organização (O), unidade organizacional (OU), nome de usuário comum (CN) e contêiner. Por exemplo:
`/C=RU/O=MyCompany/CN=User/`.

Você também pode utilizar outros atributos especificados no RFC 5280.

Atributos são utilizados por serviços DNS para validar o certificado emitido pela Autoridade de Autenticação a pedido do usuário.

- Clique no botão **Adicionar assunto do nome alternativo** para adicionar um campo para especificar o nome alternativo do assunto:

- Na lista suspensa **Tipo do assunto do nome alternativo** exibida, selecione o tipo de nome alternativo do assunto para o servidor SCEP. Você pode adicionar apenas um nome alternativo de cada tipo.

Você pode usar um nome alternativo de assunto para identificar o usuário do dispositivo iOS MDM. Por padrão, a identificação com base no nome alternativo não é usada.

- **Nome DNS.** Identificação utilizando o nome de domínio.
- **Nome principal NT.** Nome DNS do usuário do dispositivo iOS MDM na rede Windows NT. O nome do assunto NT está contido na solicitação do certificado enviada ao servidor SCEP. Você também pode utilizar o nome do sujeito NT para identificar o usuário do dispositivo iOS MDM.
- **Endereço de e-mail.** Identificação usando o endereço de e-mail. O endereço de e-mail deve ser especificado de acordo com o RFC 822.
- **Identificador de Recursos Uniforme (URI).** Identificação utilizando o endereço IP ou endereço no formato FQDN.
- No campo **Assunto do nome alternativo**, insira o nome alternativo do sujeito do certificado X.500. O valor do nome alternativo do sujeito depende do tipo de sujeito selecionado: o endereço de e-mail do usuário, domínio ou endereço da Web.

9. Na seção **Chave**, defina as configurações da chave de criptografia:

- Na lista suspensa **Tamanho da chave (bit)**, selecione o tamanho da chave de registro em bits: 1024, 2048 ou 4096. O valor padrão é 1024 bits.

- Se quiser permitir que o usuário use um certificado recebido do servidor SCEP como assinar o certificado, marque a caixa de seleção **Usar como assinatura digital**.

A assinatura de dados protege os dados contra modificação. Por exemplo, o Safari pode validar a autenticidade do certificado e estabelecer uma sessão de troca de dados segura.

- Se você deseja permitir que o usuário use um certificado recebido do servidor SCEP para criptografia de dados, selecione a caixa **Usar para criptografia**.

A criptografia de dados também oferece proteção a dados confidenciais durante a troca de dados em uma rede. Por exemplo, o Safari pode estabelecer uma sessão de troca de dados segura utilizando criptografia. Isto garante a autenticidade do site e confirma que a conexão ao site foi criptografada para impedir a interceptação de dados pessoais e confidenciais.

Você não pode usar simultaneamente o certificado do servidor SCEP como um certificado de assinatura de dados e um certificado de criptografia de dados.

- Se você quiser permitir que todos os Aplicativos permitidos instalados acessem a chave privada a partir do certificado do servidor SCEP, marque a caixa de seleção **Permitir que todos os aplicativos acessem a chave privada**.
- Se você não quiser que a chave privada seja exportada do chaveiro, marque a caixa de seleção **Proibir a exportação da chave privada tendo como origem o armazenamento portátil**.

10. Clique em **Adicionar**.

O novo perfil SCEP é exibido na lista.

Você pode modificar ou excluir perfis do SCEP da lista usando os botões **Editar** e **Excluir** na parte superior da lista.

11. Clique em **OK**.

12. Clique em **Salvar** para salvar as alterações efetuadas.

As configurações do dispositivo móvel são alteradas após a próxima sincronização do dispositivo com o Servidor de MDM do iOS.

Como resultado, depois que a política é aplicada, o dispositivo móvel do usuário é configurado automaticamente para receber um certificado a partir do centro de certificação por meio da Internet.

Gerenciamento de dispositivos móveis

Esta seção contém informações sobre como gerenciar remotamente dispositivos móveis no Kaspersky Next Expert View (cloud).

Gerenciar dispositivos Android

O Kaspersky Next Expert View (cloud) permite gerenciar dispositivos Android das seguintes formas:

- Gerenciar centralmente dispositivos usando comandos.
- Visualizar informações sobre as configurações para gerenciamento de dispositivos Android.
- Instalar aplicativos usando pacotes de aplicativos móveis.
- Conectar-se a dispositivos e controlá-los remotamente.
- Desconectar dispositivos Android do gerenciamento.

Criar um pacote de aplicativo móvel para dispositivos Android

Para criar um pacote de aplicativos móveis:

1. Na janela principal do Kaspersky Security Center Web Console, selecione **Gerenciamento de ativos** → **Móvel** → **Aplicativos e arquivos**.

2. Clique em **Android**.

3. Clique em **Aplicativos** e, em seguida, clique em **Adicionar**.

A janela **Adicionar aplicativo** é exibida.

4. Especifique o nome do aplicativo no campo **Nome do aplicativo**. Esse nome será usado para identificar o aplicativo nas configurações da política.
5. Clique em **Selecionar** e selecione um arquivo APK em seu computador.
6. Clique em **Salvar** para salvar as alterações efetuadas.

O pacote de aplicativos recém-criado é exibido na lista de aplicativos na guia **Aplicativos**.

Se você selecionar um arquivo APK grande, o carregamento do aplicativo poderá levar algum tempo. Não feche a seção **Aplicativos e arquivos** até que o aplicativo seja carregado.

Na seção **Aplicativos e arquivos**, você também pode [adicionar aplicativos iOS](#).

Visualizar informações sobre um dispositivo Android

Para visualizar informações sobre um dispositivo Android:

1. Na janela principal do Kaspersky Next Expert View (cloud), selecione **Gerenciamento de ativos** → **Móvel** → **Dispositivos**.

A lista de dispositivos móveis gerenciados é exibida.

2. Para filtrar dispositivos Android, clique no cabeçalho da coluna **SO** e selecione **Android**.

A lista de dispositivos Android é exibida.

Dependendo do banco de dados usado, as pesquisas podem diferenciar maiúsculas de minúsculas.

3. Selecione o dispositivo móvel sobre o qual você deseja visualizar as informações.

Uma janela com as propriedades do dispositivo Android é exibida.

A janela de propriedades do dispositivo móvel exibe informações sobre o dispositivo Android conectado.

Os números IMEI são exibidos para todos os dispositivos que executam o Android 5 a 9 e dispositivos com um contêiner corporativo que executam o Android 10 a 11.

Se uma versão antiga do Kaspersky Endpoint Security for Android (10.52.1.3 ou anterior) estiver instalada nos dispositivos, o valor do **Modo de operação** será definido como **Desconhecido**.

Desconectar um dispositivo Android do gerenciamento

Para desconectar um dispositivo Android do gerenciamento, o usuário deve remover o Kaspersky Endpoint Security for Android do dispositivo móvel. Depois que o usuário tiver removido o Kaspersky Endpoint Security for Android, o administrador poderá remover o dispositivo móvel da lista de dispositivos gerenciados no Kaspersky Next Expert View (cloud).

Se o Kaspersky Endpoint Security for Android não tiver sido removido do dispositivo móvel, o aquele dispositivo reaparece na lista de dispositivos gerenciados após a sincronização com o Servidor de Administração.

Para remover um dispositivo Android da lista de dispositivos gerenciados:

1. Na janela principal do Kaspersky Next Expert View (cloud), selecione **Gerenciamento de ativos** → **Móvel** → **Dispositivos**.

A lista de dispositivos móveis gerenciados é exibida.

2. Para filtrar dispositivos Android, clique no cabeçalho da coluna **SO** e selecione **Android**.

A lista de dispositivos Android é exibida.

3. Selecione o dispositivo móvel que você deseja desconectar.

4. Clique em **Excluir**.

O dispositivo será removido da lista de dispositivos gerenciados.

Gerenciar dispositivos iOS MDM

Esta seção descreve recursos avançados para o gerenciamento de dispositivos iOS MDM no Kaspersky Next Expert View (cloud).

Assinar perfis de gerenciamento com um certificado

Essa funcionalidade está disponível com o Kaspersky Security Center Linux 15.2 ou posterior.

É possível assinar perfis de gerenciamento com um certificado recebido de uma autoridade do certificado confiável.

Não é necessário um certificado para que o perfil de gerenciamento funcione corretamente. Caso o perfil de gerenciamento não esteja assinado com um certificado, ao instalar o perfil de gerenciamento, uma advertência será exibida e os usuários serão solicitados a confirmar que confiam na organização que enviou o certificado.

Para assinar perfis de gerenciamento com um certificado:

1. Na janela principal do Kaspersky Next Expert View (cloud), selecione **Gerenciamento de ativos** → **Móvel** → **Servidores de MDM do iOS**.

A lista de Servidores de MDM do iOS é exibida.

2. Clique em **Assinando o certificado**.

A janela **Assinando o certificado** é exibida.

3. No campo **Formato do certificado**, especifique o tipo de certificado público ou privado:

- Se o valor **PKCS #12** for selecionado, especifique o arquivo de certificado e a senha.
- Se o valor **X.509** for selecionado:
 - a. Especifique o arquivo de chave privada.
 - b. Especifique o arquivo de chave pública.
 - c. Especifique a senha da chave privada.

4. Clique em **Salvar**.

Os perfis de gerenciamento criados que agora serão assinados com o certificado especificado.

Adicionar um perfil de configuração

Para criar um perfil de configuração, você pode usar o Apple Configurator 2, disponível no site da Apple. O Apple Configurator 2 funciona somente em dispositivos que executam o macOS. Se você não tiver esses dispositivos à sua disposição, poderá usar o Utilitário de Configuração do iPhone. No entanto, a Apple não oferece mais suporte para o Utilitário de Configuração do iPhone.

Para adicionar um perfil de configuração para um Servidor de MDM do iOS:

1. Na janela principal do Kaspersky Next Expert View (cloud), selecione **Gerenciamento de ativos** → **Móvel** → **Servidores de MDM do iOS**. Na lista de Servidores de MDM do iOS exibida, clique no Servidor de MDM do iOS cujas configurações você deseja definir.
2. Na janela de configurações do Servidor de MDM do iOS, selecione **Configurações do aplicativo**.
3. Selecione a guia **Perfis de configuração**.
4. Para adicionar um novo perfil de configuração, clique em **Adicionar**.
5. Na janela exibida, selecione o perfil de configuração que você quer adicionar.

O nome do perfil de configuração não deve ter mais de 100 caracteres. Se você inserir um nome mais longo, somente parte dele será exibida.

O novo perfil de configuração será exibido na lista de perfis de configuração.

Você pode [instalar o perfil de configuração que você criou nos dispositivos iOS MDM](#).

Instalar um perfil de configuração em um dispositivo

Você pode instalar um perfil de configuração em um dispositivo iOS MDM na janela **Enviar comando** ou na guia **Perfis de configuração** na janela de propriedades do dispositivo.

Na janela **Enviar comando**, você pode instalar perfis de configuração em vários dispositivos.

Para instalar um perfil de configuração na janela Enviar comando:

1. Na janela principal do Kaspersky Next Expert View (cloud), selecione **Gerenciamento de ativos** → **Móvel** → **Dispositivos**.
2. Na lista de dispositivos exibida, selecione os dispositivos nos quais você deseja instalar os perfis de configuração.
3. Clique em **Enviar comando**.
4. Na janela **Enviar comando** exibida, no campo **Comando**, selecione o comando **Instalar o perfil de configuração**.
5. Na seção **Perfis de configuração**, selecione os [perfis de configuração que deseja instalar](#) nos dispositivos.
6. Clique em **Enviar**.

O comando é enviado aos dispositivos selecionados.

Para instalar um perfil de configuração na janela de propriedades do dispositivo:

1. Na janela principal do Kaspersky Next Expert View (cloud), selecione **Gerenciamento de ativos** → **Móvel** → **Dispositivos**.
2. Na lista de dispositivos exibida, clique no nome do dispositivo no qual você deseja instalar os perfis de configuração.
A janela de propriedades de dispositivo é exibida.
3. Selecione a guia **Perfis de configuração**.
4. Na parte superior da lista de perfis de configuração, clique em **Instalar**.
5. Na janela exibida, selecione os perfis de configuração que deseja instalar no dispositivo e clique em **Instalar**.

O comando é enviado para o dispositivo.

A instalação de perfis pode levar alguns minutos. O comando é executado somente se o dispositivo estiver conectado à Internet. Para verificar se um perfil foi instalado, clique em **Atualizar a lista**.

Remover um perfil de configuração de um dispositivo

Você pode remover um perfil de configuração de um dispositivo iOS MDM na janela **Enviar comando** ou na guia **Perfis de configuração** na janela de propriedades do dispositivo.

Na janela **Enviar comando**, você pode remover perfis de configuração de vários dispositivos.

*Para remover um perfil de configuração na janela **Enviar comando**:*

1. Na janela principal do Kaspersky Next Expert View (cloud), selecione **Gerenciamento de ativos** → **Móvel** → **Dispositivos**.
2. Na lista de dispositivos exibida, selecione os dispositivos dos quais você deseja remover os perfis de configuração.
3. Clique em **Enviar comando**.
4. Na janela **Enviar comando** exibida, no campo **Comando**, selecione o comando **Excluir perfil de configuração**.
5. Na seção **Perfis de configuração**, selecione os perfis de configuração que deseja remover dos dispositivos.
6. Clique em **Enviar**.

O comando é enviado aos dispositivos selecionados.

O perfil pode ser exibido na lista de perfis de configuração instalados no dispositivo por vários minutos após ter sido excluído.

Para remover um perfil de configuração na janela de propriedades do dispositivo:

1. Na janela principal do Kaspersky Next Expert View (cloud), selecione **Gerenciamento de ativos** → **Móvel** → **Dispositivos**.
2. Na lista de dispositivos exibida, clique no nome do dispositivo do qual você deseja remover os perfis de configuração.
A janela de propriedades de dispositivo é exibida.
3. Selecione a guia **Perfis de configuração**.
4. Na lista de perfis de configuração, selecione os perfis de configuração que deseja remover do dispositivo e clique em **Excluir**.

O comando é enviado para o dispositivo.

A remoção de perfis pode levar alguns minutos. O comando é executado somente se o dispositivo estiver conectado à Internet. Para verificar se um perfil foi removido, clique em **Atualizar a lista**.

Não é possível impedir que os usuários removam o perfil de configuração por meio das configurações do dispositivo.

Configurar aplicativos gerenciados

Antes de instalar um aplicativo em um dispositivo iOS MDM, você deve adicionar o aplicativo no Servidor de Administração. Um aplicativo é considerado gerenciado se tiver sido instalado em um dispositivo através do Kaspersky Mobile Devices Protection and Management. Um aplicativo gerenciado pode ser gerenciado remotamente por meio do Kaspersky Mobile Devices Protection and Management.

Para adicionar um aplicativo gerenciado a um Servidor de MDM do iOS:

1. Na janela principal do Kaspersky Next Expert View (cloud), selecione **Gerenciamento de ativos** → **Móvel** → **Aplicativos e arquivos**.
2. Clique em **iOS** e, em seguida, clique em **Adicionar**.
A janela **Adicionar aplicativo** é exibida.
3. Especifique o nome do aplicativo no campo **Nome do aplicativo**. Esse nome será usado para identificar o aplicativo nas configurações da política.
4. No campo **Método de instalação**, selecione um dos seguintes métodos para adicionar o aplicativo:
 - **App Store**
5. Execute uma das seguintes ações:

Use somente fontes legítimas e confiáveis. Ao definir as configurações nessa seção, você é o único responsável por todos os riscos e as consequências associados ao uso de fontes não confiáveis.

- Se você selecionou **Pacote de instalação**, clique em **Selecionar** e carregue um arquivo IPA do computador.
 - Se você selecionou **Link para o arquivo de manifesto**, especifique um link para um arquivo de manifesto que pode ser usado para baixar o aplicativo.
 - Se você selecionou **App Store**, especifique um link ou ID do aplicativo a ser adicionado da App Store.
6. Se necessário, defina as seguintes configurações:
 - Marque a caixa de seleção **Remover quando o perfil de gerenciamento for excluído** se desejar que o aplicativo seja removido do dispositivo móvel do usuário juntamente com o perfil de gerenciamento. Essa caixa de seleção é marcada por padrão.
 - Marque a caixa de seleção **Bloquear o backup dos dados do aplicativo no iCloud** se quiser bloquear o backup dos dados do aplicativo no iCloud.
 7. Clique em **Salvar** para salvar as alterações efetuadas.

O aplicativo recém-criado é exibido na tabela de aplicativos na guia **iOS**.

Se você selecionar um arquivo IPA grande, o carregamento do aplicativo poderá levar algum tempo. Não feche a seção **Aplicativos e arquivos** até que o aplicativo seja carregado.

Você pode visualizar e editar as propriedades do aplicativo clicando no aplicativo na lista ou remover o aplicativo usando o botão **Excluir**.

Instalar um aplicativo em um dispositivo móvel

Para instalar um aplicativo em um dispositivo móvel:

1. Na janela principal do Kaspersky Next Expert View (cloud), selecione **Gerenciamento de ativos** → **Móvel** → **Dispositivos**.
2. Na lista de dispositivos exibida, selecione os dispositivos nos quais você deseja instalar os aplicativos.
3. Clique em **Enviar comando**.
4. Na janela **Enviar comando** exibida, no campo **Comando**, selecione o comando **Instalar o aplicativo**.
5. No campo **Aplicativos**, selecione [os aplicativos que deseja instalar nos dispositivos](#).
6. Clique em **Enviar**.

O comando é enviado aos dispositivos selecionados.

Atualizar um aplicativo instalado em um dispositivo

Você pode atualizar um aplicativo em um dispositivo iOS MDM na janela **Enviar comando** ou na guia **Aplicativos** na janela de propriedades do dispositivo.

Na janela **Enviar comando**, você pode atualizar aplicativos em vários dispositivos.

*Para atualizar um aplicativo em um dispositivo iOS MDM na janela **Enviar comando**:*

1. Na janela principal do Kaspersky Next Expert View (cloud), selecione **Gerenciamento de ativos** → **Móvel** → **Dispositivos**.
2. Na lista de dispositivos exibida, selecione os dispositivos nos quais você deseja atualizar os aplicativos.
3. Clique em **Enviar comando**.
4. Na janela **Enviar comando** exibida, no campo **Comando**, selecione o comando **Atualizar o aplicativo**.
5. Na seção **Aplicativos**, selecione os aplicativos que deseja atualizar nos dispositivos.
6. Clique em **Enviar**.

O comando é enviado aos dispositivos selecionados.

Para atualizar um aplicativo em um dispositivo iOS MDM na janela de propriedades do dispositivo:

1. Na janela principal do Kaspersky Next Expert View (cloud), selecione **Gerenciamento de ativos** → **Móvel** → **Dispositivos**.
2. Na lista de dispositivos exibida, clique no nome do dispositivo no qual você deseja atualizar os aplicativos.
A janela de propriedades de dispositivo é exibida.

3. Selecione a guia **Aplicativos**.

4. Na parte superior da lista de aplicativos, clique em **Atualização**.

5. Na janela exibida, selecione os aplicativos que deseja atualizar no dispositivo e clique em **Atualização**.

O comando é enviado para o dispositivo.

A atualização dos aplicativos pode levar alguns minutos. O comando é executado somente se o dispositivo estiver conectado à Internet. Para verificar se um aplicativo foi atualizado, clique em **Atualizar a lista**.

Remover um aplicativo de um dispositivo

Você pode remover um aplicativo de um dispositivo iOS MDM na janela **Enviar comando** ou na guia **Aplicativos** na janela de propriedades do dispositivo.

Na janela **Enviar comando**, você pode remover aplicativos de vários dispositivos.

Para remover um aplicativo de um dispositivo iOS MDM na janela Enviar comando:

1. Na janela principal do Kaspersky Next Expert View (cloud), selecione **Gerenciamento de ativos** → **Móvel** → **Dispositivos**.
2. Na lista de dispositivos exibida, selecione os dispositivos dos quais você deseja remover os aplicativos.
3. Clique em **Enviar comando**.
4. Na janela **Enviar comando** exibida, no campo **Comando**, selecione o comando **Excluir aplicativo**.
5. Na seção **Aplicativos**, selecione os aplicativos que deseja remover dos dispositivos.
6. Clique em **Enviar**.

O comando é enviado aos dispositivos selecionados.

Para remover um aplicativo de um dispositivo iOS MDM na janela de propriedades do dispositivo:

1. Na janela principal do Kaspersky Next Expert View (cloud), selecione **Gerenciamento de ativos** → **Móvel** → **Dispositivos**.
2. Na lista de dispositivos exibida, clique no nome do dispositivo do qual você deseja remover os aplicativos.
A janela de propriedades de dispositivo é exibida.
3. Selecione a guia **Aplicativos**.
4. Na lista de aplicativos, selecione os aplicativos que deseja remover do dispositivo e clique em **Excluir**.

O comando é enviado para o dispositivo.

A remoção de aplicativos pode levar alguns minutos. O comando é executado somente se o dispositivo estiver conectado à Internet. Para verificar se um aplicativo foi removido, clique em **Atualizar a lista**.

Configurar o roaming em um dispositivo móvel iOS MDM

Para configurar o roaming:

1. Na janela principal do Kaspersky Next Expert View (cloud), selecione **Gerenciamento de ativos** → **Móvel** → **Dispositivos**.
2. Na lista de dispositivos exibida, selecione os dispositivos para os quais você deseja definir as configurações de roaming.
3. Clique em **Enviar comando**.
4. Na janela **Enviar comando** que é exibida, no campo **Comando**, selecione o comando **Alterar configurações de roaming**.
5. Na seção **Ação**, realize uma das seguintes ações:
 - Se você quiser ativar o roaming de dados, selecione **Ativar roaming de dados**.
 - Se você quiser desativar o roaming de dados, selecione **Desativar o roaming de dados**.
6. Clique em **Enviar**.

O comando é enviado aos dispositivos selecionados.

Visualizar informações sobre um dispositivo iOS MDM

Para visualizar informações sobre um dispositivo MDM do iOS:

1. Na janela principal do Kaspersky Next Expert View (cloud), selecione **Gerenciamento de ativos** → **Móvel** → **Dispositivos**.

A lista de dispositivos móveis gerenciados é exibida.

2. Para filtrar dispositivos iOS MDM, clique no cabeçalho da coluna **Modo de operação** e selecione o modo de operação do dispositivo iOS MDM sobre o qual você deseja visualizar as informações.

A lista de dispositivos iOS MDM é exibida.

Dependendo do banco de dados usado, as pesquisas podem diferenciar maiúsculas de minúsculas.

3. Selecione o dispositivo móvel sobre o qual você deseja visualizar as informações.

Uma janela com as propriedades do dispositivo iOS MDM é exibida.

Ao exibir valores numéricos, pode ocorrer um erro de vários centésimos.

A guia **Geral** da janela de propriedades exibe informações sobre o dispositivo iOS MDM conectado.

As seguintes propriedades de dispositivos iOS MDM executando o iOS 26 ou posterior podem não ser exibidas: **IMEI**, **Número de telefone**, **MEID**, **ICCID**, **Nome da rede móvel atual**, **Nome da rede móvel local**, **Versão das configurações da operadora**, **Roaming de voz ativado**, **Em roaming**, **Código do país da rede local**, **Código da rede doméstica**, **Código do país do host** e **Código da rede atual**.

A guia **Certificados** da janela de propriedades exibe as informações sobre os certificados instalados no dispositivo iOS MDM selecionado.

A guia **Aplicativos** da janela de propriedades exibe as informações sobre os aplicativos instalados no dispositivo iOS MDM selecionado.

A guia **Perfis de configuração** da janela de propriedades exibe as informações sobre os perfis de configuração instalados no dispositivo iOS MDM selecionado.

Desconectar um dispositivo iOS MDM do gerenciamento

Se quiser parar de gerenciar um dispositivo iOS MDM, você pode desconectá-lo do gerenciamento no Kaspersky Security Center.

Não recomendamos desconectar o dispositivo do gerenciamento com a remoção do perfil de gerenciamento, pois esse dispositivo talvez não funcione corretamente quando reconectado. Para parar de gerenciar um dispositivo iOS MDM, desconecte-o do Servidor de MDM do iOS, conforme descrito nesta seção.

Para desconectar um dispositivo iOS MDM do Servidor de MDM do iOS:

1. Na janela principal do Kaspersky Next Expert View (cloud), selecione **Gerenciamento de ativos** → **Móvel** → **Dispositivos**.

A lista de dispositivos móveis gerenciados é exibida.

2. Para filtrar dispositivos iOS MDM, clique no cabeçalho da coluna **Modo de operação** e selecione o modo de operação do dispositivo iOS MDM que você deseja desconectar.

A lista de dispositivos iOS MDM que operam no modo selecionado é exibida.

3. Selecione o dispositivo móvel que você deseja desconectar.

4. Clique em **Excluir**.

Na lista, o dispositivo iOS MDM é marcado para remoção. Em um minuto, o dispositivo é removido do banco de dados do Servidor de MDM do iOS e, em seguida, é removido automaticamente da lista de dispositivos gerenciados.

Depois que o dispositivo iOS MDM for desconectado do gerenciamento, todos os perfis de configuração instalados, o perfil de gerenciamento e os aplicativos para os quais a opção **Remover quando o perfil de gerenciamento for excluído** tiver sido ativada nas configurações do Servidor de MDM do iOS serão removidos do dispositivo. A política de MDM do iOS também será excluída.

Não é possível impedir que os usuários removam um perfil de gerenciamento pelas configurações do dispositivo.

Gerenciar configurações do dispositivos móveis

Esta seção contém informações sobre como gerenciar remotamente as configurações de dispositivos móveis no Kaspersky Next Expert View (cloud).

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 que um dispositivo Android se conecte a uma rede Wi-Fi disponível e proteja os dados durante a conexão, é necessário definir as configurações da conexão.

Para conectar um dispositivo móvel a uma rede Wi-Fi:

1. Na janela principal do Kaspersky Next Expert View (cloud), selecione **Gerenciamento de ativos** → **Políticas**. Na lista de políticas de grupo aberta, clique no nome da política que deseja configurar.
2. Na janela de propriedades da política, selecione **Configurações do aplicativo**.
3. Selecione **Android** e vá para a seção **Configuração do dispositivo**.
4. No cartão **Wi-Fi**, clique em **Configurações**.
A janela **Wi-Fi** é exibida.
5. Ative as configurações usando o botão **Wi-Fi**.
6. Clique em **Adicionar**.
A janela **Adicionar rede Wi-Fi** é exibida.
7. No campo **Identificador do conjunto de serviços (SSID)**, insira o nome da rede Wi-Fi que inclua o ponto de acesso (SSID).
8. Marque a caixa de seleção **Rede oculta** caso deseje que a rede Wi-Fi fique oculta na lista de redes disponíveis no dispositivo.
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.
9. Na seção **Proteção**, selecione o tipo de segurança da rede Wi-Fi (rede aberta ou rede segura protegida com o protocolo WEP ou WPA2 PSK).

O protocolo WEP é compatível apenas no Android 9 ou anterior.

10. No campo **Senha**, defina uma senha de acesso a rede caso tenha selecionado uma rede segura na etapa 8.
11. Na guia **Adicional**, marque a caixa de seleção **Usar um servidor proxy** se quiser usar um servidor proxy para se conectar à rede Wi-Fi.
12. Caso tenha selecionado **Usar um servidor proxy**, nos campos **Endereço do servidor proxy** e **Porta do servidor proxy**, insira o endereço IP ou nome DNS do servidor proxy e o número da porta, caso seja necessário.

Em dispositivos com Android 8 ou posterior, as configurações do servidor proxy para Wi-Fi não podem ser redefinidas com uma política. No entanto, é possível definir manualmente as configurações do servidor proxy para uma rede Wi-Fi no dispositivo móvel.

Caso não esteja usando um servidor proxy para se conectar a uma rede Wi-Fi, não haverá limitações no uso de políticas para gerenciar uma conexão de rede Wi-Fi.

13. No campo **Não usar o servidor proxy para os endereços especificados**, adicione os 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 o Android 8 ou posterior, a exclusão de endereços da Web do servidor proxy não funciona.

14. Clique em **Adicionar**.

A rede Wi-Fi adicionada é exibida na lista de Redes Wi-Fi.

Essa lista contém os nomes das redes sem fio sugeridas.

Em dispositivos pessoais executando o Android 10 ou posterior, o sistema operacional solicita que o usuário se conecte a essas redes. As redes sugeridas não aparecem na lista de redes salvas nesses dispositivos.

Em dispositivos pessoais que executam o Android 9 ou anterior, depois de sincronizar o dispositivo com o Servidor de Administração, o usuário do dispositivo pode selecionar uma rede sem fio sugerida na lista de redes salvas e conectar-se a ela sem precisar especificar nenhuma configuração de rede.

Você pode modificar ou excluir redes Wi-Fi da lista de redes usando os botões **Editar** e **Excluir** na parte superior da lista.

15. Clique em **OK**.

16. Clique em **Salvar** para salvar as alterações efetuadas.

As configurações do dispositivo móvel são alteradas após a próxima sincronização do dispositivo com o Kaspersky Security Center.

Em dispositivos com Android 10 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. Na janela principal do Kaspersky Next Expert View (cloud), selecione **Gerenciamento de ativos** → **Políticas**. Na lista de políticas de grupo aberta, clique no nome da política que deseja configurar.
2. Na janela de propriedades da política, selecione **Configurações do aplicativo**.
3. Selecione **iOS** e vá para a seção **Configuração do dispositivo**.
4. No cartão **Wi-Fi**, clique em **Configurações**.
A janela **Wi-Fi** é exibida.
5. Ative as configurações usando o botão **Wi-Fi**.
6. Clique em **Adicionar**.
A janela **Adicionar rede Wi-Fi** é exibida.
7. No campo **Identificador do conjunto de serviços (SSID)**, insira o nome da rede Wi-Fi que inclua o ponto de acesso (SSID).
8. Se você quiser que o dispositivo iOS MDM se conecte automaticamente com a rede Wi-Fi, marque a caixa de seleção **Conectar automaticamente**.

Se você desativar a conexão automática a uma rede Wi-Fi existente nas configurações de política, não poderá ativar a conexão automática a essa rede novamente. Isso se deve a um problema conhecido pela Apple.

9. Se você não quiser que os dispositivos iOS MDM se conectem a redes Wi-Fi que exigem autenticação preliminar (redes cativas), marque a caixa de seleção **Desativar a detecção de rede cativa**.
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.
10. Se você quiser que a rede Wi-Fi fique oculta na lista de redes disponíveis no dispositivo iOS MDM, marque 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.
11. Na seção **Proteção**, selecione o tipo de segurança da rede Wi-Fi (rede aberta ou rede segura protegida com o protocolo WEP, WPA, WPA2 ou WPA3).

Em dispositivos com iOS 15 ou anterior, selecionar WPA, WPA2 ou WPA3 é idêntico e permite conectar-se a qualquer rede protegida usando WPA.

- **Rede aberta.** A autenticação do usuário não é necessária.
- **WEP.** A rede é protegida utilizando Wireless Encryption Protocol (WEP).

A proteção WEP está disponível em dispositivos com iOS 5 ou posterior.

- **WPA.** A rede é protegida usando o protocolo WPA (Wi-Fi Protected Access) ou WPA2.
- **WPA2.** A rede é protegida utilizando o protocolo de segurança WPA2 ou WPA3.
- **WPA3.** A rede é protegida utilizando o protocolo de segurança WPA3.
- **Rede pessoal (qualquer).** A rede é protegida usando o protocolo de criptografia WEP, WPA, WPA2 ou WPA3, dependendo do tipo de roteador Wi-Fi. Uma chave de criptografia exclusiva para cada usuário é usada para autenticação.
- **WEP (rede corporativa).** A rede é protegida utilizando o protocolo WEP com o uso de uma chave dinâmica.
- **WPA (rede corporativa).** A rede é protegida usando o protocolo de criptografia WPA ou WPA2 com o uso do protocolo 802.1X.
- **WPA2 (rede corporativa).** A rede é protegida utilizando o protocolo de criptografia WPA2 ou WPA3 com o uso de uma chave compartilhada por todos os usuários (802.1X).
- **WPA3 (rede corporativa).** A rede é protegida utilizando o protocolo de criptografia WPA3 com o uso de uma chave compartilhada por todos os usuários (802.1X).
- **Rede corporativa (qualquer).** A rede é protegida usando o protocolo WEP, WPA, WPA2 ou WPA3, dependendo do tipo de roteador Wi-Fi. A autenticação é realizada usando uma única chave de criptografia compartilhada por todos os usuários.

Se você tiver selecionado alguma das opções de rede corporativa, na seção **Protocolo EAP** poderá selecionar os tipos de protocolos EAP (Extensible Authentication Protocol) para 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.

12. Na seção **Autenticação**, defina as configurações da conta para a autenticação do usuário após a conexão do dispositivo iOS MDM com uma rede Wi-Fi:
 - a. No campo **Nome de usuário**, insira o nome da conta para autenticação do usuário após conexão com a rede Wi-Fi.
 - b. 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.

O ID do usuário foi projetado para tornar o processo de autenticação mais seguro, já que o nome de usuário não é exibido abertamente, mas sim transmitido por meio de um túnel TLS criptografado.
 - c. No campo **Senha**, insira a senha da conta para autenticação em uma rede Wi-Fi.

- d. Se você quiser que o usuário insira a senha manualmente em cada conexão com uma rede sem fio, marque a caixa de seleção **Solicitar senha a cada conexão**.
 - e. Na lista suspensa **Certificado de autenticação**, selecione um certificado para autenticação do usuário na rede Wi-Fi.
 - f. Na lista suspensa **Versão mínima do TLS**, selecione a versão mínima do TLS permitida.
 - g. Na lista suspensa **Versão máxima do TLS**, selecione a versão máxima de TLS permitida.
13. Se necessário, na guia **Adicional**, defina as configurações para conectar-se à rede Wi-Fi através de um servidor proxy:
- a. Marque a caixa de seleção **Usar um servidor proxy**.
 - b. Configure uma conexão com um servidor proxy:
 - a. Se você quiser configurar a conexão automaticamente:
 - Selecione **Automático**.
 - No campo **URL do arquivo PAC**, especifique a URL do arquivo proxy PAC.
 - 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 conexão direta se não for possível acessar o arquivo PAC**.
 - b. Se você quiser configurar a conexão manualmente:
 - Selecione **Manual**.
 - Nos campos **Endereço do servidor proxy** e **Porta do servidor proxy**, insira o endereço IP ou nome DNS do servidor proxy e número da porta.
 - No campo **Nome de usuário**, selecione uma macro que será usada como um nome de usuário para a conexão com o servidor proxy.
 - No campo **Senha**, especifique a senha para a conexão com o servidor proxy.

14. Clique em **Adicionar**.

A nova rede Wi-Fi é exibida na lista.

15. Clique em **OK**.

16. Clique em **Salvar** 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 pelo método de autenticação selecionado.

Configurar o e-mail

Esta seção contém informações sobre a configuração de caixas de e-mail em dispositivos móveis.

Configurar uma caixa de e-mail em dispositivos iOS MDM

Essas configurações se aplicam aos dispositivos no modo de operação "Perfil de gerenciamento".

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 qualquer cliente de e-mail (que não seja o E-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 uma conta.

Para adicionar uma conta de e-mail do usuário do dispositivo iOS MDM:

1. Na janela principal do Kaspersky Next Expert View (cloud), selecione **Gerenciamento de ativos** → **Políticas**. Na lista de políticas de grupo aberta, clique no nome da política que deseja configurar.

2. Na janela de propriedades da política, selecione **Configurações do aplicativo**.

3. Selecione **iOS** e vá para a seção **Configuração do dispositivo**.

4. No cartão **E-mail**, clique em **Configurações**.

A janela **E-mail** é exibida.

5. Ative as configurações usando o botão **E-mail**.

6. Clique em **Adicionar**.

A janela **Adicionar conta de e-mail** é exibida.

7. Especifique as configurações da conta de e-mail:

- Na guia **Geral**, defina as seguintes configurações:
 - a. No campo **Nome de usuário**, especifique o nome de usuário do dispositivo iOS MDM.
 - b. No campo **Endereço de e-mail**, especifique o endereço de e-mail do usuário do dispositivo iOS MDM.
 - c. No campo **Descrição da conta**, insira uma descrição da conta de e-mail do usuário.
 - d. No campo **Protocolo de e-mail**, selecione um dos seguintes protocolos:
 - **POP**
 - **IMAP**

e. Se você selecionou **IMAP**, 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 Google Mail).

f. Nas seções **Configurações do servidor de correio de entrada** e **Configurações do servidor de correio de saída**, defina as configurações de conexão do servidor:

- No campo **Endereço do servidor**, especifique os nomes dos hosts ou endereços IP dos servidores de e-mail de entrada e saída.
- Nos campos **Porta do servidor**, especifique os números de porta dos servidores de e-mail de entrada e de saída.

Para definir configurações opcionais para os servidores de e-mail de entrada e de saída, clique em **Mais configurações** e faça o seguinte:

- No campo **Nome de usuário**, especifique o nome da conta do usuário para autorização nos servidores de e-mail de entrada e de saída.
 - No campo **Tipo de autenticação**, selecione o tipo de autenticação da conta de e-mail do usuário nos servidores de e-mail de entrada e saída.
 - No campo **Senha**, especifique a senha da conta para autenticação em servidores de e-mail de entrada e saída protegidos usando o método de autenticação selecionado.
 - Se você quiser usar o protocolo de transporte de dados SSL (Secure Sockets Layer), marque a caixa de seleção **Usar conexão SSL**.
- Na guia **Avançado**, defina as configurações adicionais da conta de e-mail:
 - a. Na seção **Restrições**, marque ou desmarque as seguintes caixas de seleção, se necessário:

- **Permitir a sincronização de endereços recentes**

Movimentação de mensagens de e-mail entre contas.

Caso a caixa de seleção esteja marcada, o usuário poderá mover mensagens de e-mail de uma conta para outra.

Caso a caixa de seleção esteja desmarcada, o usuário estará proibido de mover mensagens de e-mail de uma conta para outra.

Essa caixa de seleção é marcada por padrão.

Se você quiser proibir o salvamento, a movimentação e o compartilhamento de anexos de uma caixa de e-mail corporativa, desmarque a caixa de seleção **Permitir a movimentação de mensagens entre contas (inclusive contas pessoais e profissionais)** e marque as caixas de seleção **Proibir que aplicativos não gerenciados usem documentos de aplicativos gerenciados** e **Proibir que aplicativos gerenciados usem documentos de aplicativos não gerenciados**.

- **Permitir a movimentação de mensagens entre contas (inclusive contas pessoais e profissionais)**

Sincronização de endereços de e-mail entre contas.

Se a caixa de seleção estiver marcada, ao criar mensagens o usuário poderá usar o histórico de endereços de outra conta de e-mail.

Se essa caixa de seleção estiver desmarcada, os endereços de e-mail usados não serão sincronizados. Ao criar uma mensagem, o usuário de um dispositivo iOS MDM não pode usar o histórico de endereços de outra conta de e-mail.

Essa caixa de seleção é marcada por padrão.

- **Permitir o Mail Drop**

Uso do serviço Mail Drop para encaminhar anexos grandes.

Se a caixa de seleção estiver marcada, o usuário pode utilizar o Mail Drop.

Se a caixa de seleção estiver desmarcada, o usuário não poderá utilizar o Mail Drop.

Essa caixa de seleção é desmarcada por padrão.

- **Permitir o uso apenas do aplicativo E-mail**

Uso apenas do cliente de e-mail padrão do iOS para processar mensagens.

Caso a caixa de seleção esteja marcada, o usuário poderá usar apenas o e-mail no cliente de e-mail padrão do iOS.

Se a caixa de seleção estiver desmarcada, o usuário poderá usar o e-mail no cliente de e-mail padrão do iOS e em outros aplicativos.

Essa caixa de seleção é desmarcada por padrão.

- b. Nas seções **Assinatura** e **Criptografia**, defina as configurações para assinar e criptografar e-mails enviados usando o protocolo S/MIME no aplicativo E-mail.

S/MIME é um protocolo para transmitir mensagens criptografadas assinadas digitalmente. O S/MIME fornece as capacidades de segurança criptografada, tal como a autenticação, controle de integridade da mensagem e não repudição da origem (usando assinaturas digitais). O protocolo também ajuda a melhorar a confidencialidade e a segurança dos dados em mensagens de e-mail usando criptografia.

- **Assinar mensagens**

Assinatura digital de mensagens de saída no aplicativo E-mail.

Se a caixa de seleção estiver marcada, as mensagens enviadas serão assinadas com uma assinatura digital usando o protocolo S/MIME. Uma assinatura digital confirma a autenticidade do remetente e indica que o conteúdo da mensagem não foi modificado durante a transmissão ao destinatário. Um certificado de destinatário (chave pública) deve ser selecionada para uma assinatura de mensagem.

Essa caixa de seleção é desmarcada por padrão.

- **Certificado de assinatura para mensagens enviadas**

Certificado para assinar mensagens de saída com uma assinatura digital utilizando o protocolo S/MIME. A assinatura digital garante que a mensagem foi enviada pelo usuário do dispositivo iOS MDM. É possível adicionar certificados nas configurações de **Gerenciamento de certificados** da política ou na seção **Certificados** do Kaspersky Next Expert View (cloud).

A lista suspensa estará disponível somente se a caixa de seleção **Assinar mensagens** estiver marcada.

- **Criptografar mensagens por padrão**

Criptografia das mensagens de saída no aplicativo E-mail.

Se a caixa de seleção estiver marcada, as mensagens de saída são criptografadas por padrão usando o protocolo S/MIME. Um certificado de destinatário (chave pública) deve ser selecionada para enviar mensagens criptografadas. Se o certificado do destinatário não estiver instalado, as mensagens não podem ser criptografadas. As mensagens criptografadas somente podem ser visualizadas pelos usuários cujos dispositivos tenham um certificado instalado.

Essa caixa de seleção é desmarcada por padrão.

- **Certificado de criptografia**

Certificado de criptografia para criptografar mensagens de saída utilizando o protocolo S/MIME. A criptografia mantém as mensagens confidenciais durante a transmissão e armazenamento. É possível adicionar certificados nas configurações de **Gerenciamento de certificados** da política ou na seção **Certificados** do Kaspersky Next Expert View (cloud).

A lista suspensa estará disponível somente se a caixa de seleção **Criptografar mensagens por padrão** estiver marcada.

- **Mostrar botão de alternância para criptografar mensagens selecionadas**

Exibição do ícone  no aplicativo E-mail no campo **Para** para enviar mensagens criptografadas.

Se a caixa de seleção estiver marcada, o usuário do dispositivo móvel poderá criptografar mensagens individuais clicando no ícone.

Se a caixa de seleção estiver desmarcada, o ícone para a criptografia de mensagens não será exibido. Neste caso, a caixa de seleção **Criptografar mensagens por padrão** determina se o e-mail de saída será criptografado.

8. Clique em **Salvar**.

A nova conta de e-mail é exibida na lista.

Você pode modificar ou excluir contas de e-mail da lista usando os botões **Editar** e **Excluir** na parte superior da lista.

9. Clique em **OK**.

10. Clique em **Salvar** para salvar as alterações efetuadas.

As configurações do dispositivo móvel são alteradas após a próxima sincronização do dispositivo com o Servidor de MDM do iOS.

Como resultado, depois que a política é aplicada, as contas de e-mail da lista são adicionadas no dispositivo móvel do usuário.

Recomendamos fechar e abrir o aplicativo Configurações no dispositivo iOS MDM depois de configurar uma caixa de e-mail.

Configurar uma caixa de e-mail do Exchange nos dispositivos iOS MDM

Essas configurações se aplicam aos dispositivos no modo de operação "Perfil de gerenciamento".

Para permitir que o usuário do dispositivo iOS MDM use e-mail corporativo, calendários, contatos, notas e tarefas, adicione a conta do 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 do Exchange ActiveSync de um usuário do dispositivo iOS MDM:

1. Na janela principal do Kaspersky Next Expert View (cloud), selecione **Gerenciamento de ativos** → **Políticas**. Na lista de políticas de grupo aberta, clique no nome da política que deseja configurar.

2. Na janela de propriedades da política, selecione **Configurações do aplicativo**.

3. Selecione **iOS** e vá para a seção **Configuração do dispositivo**.

4. No cartão **Exchange ActiveSync**, clique em **Configurações**.

A janela **Exchange ActiveSync** é exibida.

5. Ative as configurações usando o botão **Exchange ActiveSync**.

6. Clique em **Adicionar**.

A janela **Adicionar conta do Exchange ActiveSync** é exibida.

7. Especifique as configurações do Exchange ActiveSync:

- Na guia **Geral**, especifique os dados do usuário:
 - No campo **Nome da conta**, insira o nome da conta para autorização no servidor Microsoft Exchange.
 - No campo **Endereço do servidor do Exchange ActiveSync**, insira o nome do DNS ou endereço IP do servidor do Microsoft Exchange.
- Configurações na seção **Credenciais de usuário**:
 - No campo **Domínio do usuário**, insira o nome do domínio do usuário do dispositivo iOS MDM.
 - No campo **Nome de usuário**, insira o nome do usuário do dispositivo iOS MDM.
Se você deixar esse campo em branco, o Kaspersky Mobile Devices Protection and Management solicita que o usuário insira o nome de usuário ao aplicar a política no dispositivo iOS MDM.
 - No campo **Endereço de e-mail**, especifique o endereço de e-mail do usuário do dispositivo iOS MDM.

- Configurações na seção **Autenticação**:

- No campo **Senha**, insira a senha da conta do Exchange ActiveSync para autorização no servidor do Microsoft Exchange.
- Na lista suspensa **Certificado de autenticação**, selecione o certificado usado para autenticar o usuário do dispositivo iOS MDM no servidor do Microsoft Exchange. É possível adicionar certificados nas configurações de **Gerenciamento de certificados** da política ou na seção **Certificados** do Kaspersky Next Expert View (cloud).

- Na guia **Adicional**, defina as configurações adicionais da conta do Exchange ActiveSync:

- Na seção **Sincronização de e-mail**, na lista suspensa **Período de sincronização**, selecione o intervalo de tempo durante o qual o e-mail é automaticamente sincronizado e armazenado no dispositivo iOS MDM. Quanto mais longo for o período de sincronização de e-mail, mais espaço livre será necessário na memória do dispositivo móvel. Mensagens que não foram sincronizadas não estão disponíveis sem uma conexão de Internet. O valor padrão é **1 semana**.

- Na seção **Restrições**, marque ou desmarque as seguintes caixas de seleção, se necessário:

- **Permitir a movimentação de mensagens entre contas (inclusive contas pessoais e profissionais)**

Movimentação de mensagens de e-mail entre contas.

Caso a caixa de seleção esteja marcada, o usuário poderá mover mensagens de e-mail de uma conta para outra.

Caso a caixa de seleção esteja desmarcada, o usuário estará proibido de mover mensagens de e-mail de uma conta para outra.

Essa caixa de seleção é marcada por padrão.

Se você quiser proibir o salvamento, a movimentação e o compartilhamento de anexos de uma caixa de e-mail corporativa, desmarque a caixa de seleção **Permitir a movimentação de mensagens entre contas (inclusive contas pessoais e profissionais)** e marque as caixas de seleção **Proibir que aplicativos não gerenciados usem documentos de aplicativos gerenciados** e **Proibir que aplicativos gerenciados usem documentos de aplicativos não gerenciados**.

- **Permitir a sincronização de endereços recentes**

Sincronização de endereços de e-mail entre contas.

Se a caixa de seleção estiver marcada, ao criar mensagens o usuário poderá usar o histórico de endereços de outra conta de e-mail.

Se essa caixa de seleção estiver desmarcada, os endereços de e-mail usados não serão sincronizados. Ao criar uma mensagem, o usuário de um dispositivo iOS MDM não pode usar o histórico de endereços de outra conta de e-mail.

Essa caixa de seleção é marcada por padrão.

- **Permitir o uso apenas do aplicativo E-mail**

Uso apenas do cliente de e-mail padrão do iOS para processar mensagens.

Caso a caixa de seleção esteja marcada, o usuário poderá usar apenas o e-mail no cliente de e-mail padrão do iOS.

Se a caixa de seleção estiver desmarcada, o usuário poderá usar o e-mail no cliente de e-mail padrão do iOS e em outros aplicativos.

Essa caixa de seleção é desmarcada por padrão.

- **Usar conexão SSL**

Marque essa caixa de seleção para usar o protocolo de transporte de dados SSL (Secure Sockets Layer) para proteger a transmissão de dados.

Essa caixa de seleção é marcada por padrão.

- Na seção **Assinatura e criptografia**, defina as configurações para assinar e criptografar e-mails enviados usando o protocolo S/MIME no aplicativo E-mail. *S/MIME* é um protocolo para transmitir mensagens criptografadas assinadas digitalmente. O S/MIME fornece as capacidades de segurança criptografada, tal como a autenticação, controle de integridade da mensagem e não repudição da origem (usando assinaturas digitais). O protocolo também usa a criptografia para ajudar a aprimorar o nível de confidencialidade e segurança dos dados nas mensagens de e-mail.

- **Assinar mensagens**

Assinatura digital de mensagens de saída no aplicativo E-mail.

Se a caixa de seleção estiver marcada, as mensagens enviadas serão assinadas com uma assinatura digital usando o protocolo S/MIME. Uma assinatura digital confirma a autenticidade do remetente e indica que o conteúdo da mensagem não foi modificado durante a transmissão ao destinatário. Um certificado de destinatário (chave pública) deve ser selecionada para uma assinatura de mensagem.

Essa caixa de seleção é desmarcada por padrão.

- **Certificado de assinatura para mensagens enviadas**

Certificado para assinar mensagens de saída com uma assinatura digital utilizando o protocolo S/MIME. A assinatura digital garante que a mensagem foi enviada pelo usuário do dispositivo iOS MDM. É possível adicionar certificados nas configurações de **Gerenciamento de certificados** da política ou na seção **Certificados** do Kaspersky Next Expert View (cloud).

A lista suspensa estará disponível somente se a caixa de seleção **Assinar mensagens** estiver marcada.

- **Criptografar mensagens por padrão**

Criptografia das mensagens de saída no aplicativo E-mail.

Se a caixa de seleção estiver marcada, as mensagens de saída são criptografadas por padrão usando o protocolo S/MIME. Um certificado de destinatário (chave pública) deve ser selecionada para enviar mensagens criptografadas. Se o certificado do destinatário não estiver instalado, as mensagens não podem ser criptografadas. As mensagens criptografadas somente podem ser visualizadas pelos usuários cujos dispositivos tenham um certificado instalado.

Essa caixa de seleção é desmarcada por padrão.

- **Certificado de criptografia**

Certificado de criptografia para criptografar mensagens de saída utilizando o protocolo S/MIME. A criptografia mantém as mensagens confidenciais durante a transmissão e armazenamento. É possível adicionar certificados nas configurações de **Gerenciamento de certificados** da política ou na seção **Certificados** do Kaspersky Next Expert View (cloud).

A lista suspensa estará disponível somente se a caixa de seleção **Criptografar mensagens por padrão** estiver marcada.

- **Mostrar botão de alternância para criptografar mensagens selecionadas**

Exibição do ícone  no aplicativo E-mail no campo **Para** para enviar mensagens criptografadas.

Se a caixa de seleção estiver marcada, o usuário do dispositivo móvel poderá criptografar mensagens individuais clicando no ícone.

Se a caixa de seleção estiver desmarcada, o ícone para a criptografia de mensagens não será exibido. Neste caso, a caixa de seleção **Criptografar mensagens por padrão** determina se o e-mail de saída será criptografado.

8. Clique em **Adicionar**.

A nova conta Exchange ActiveSync é exibida na lista.

Você pode modificar ou excluir contas do Exchange ActiveSync da lista usando os botões **Editar** e **Excluir** na parte superior da lista.

9. Clique em **OK**.

10. Clique em **Salvar** para salvar as alterações efetuadas.

As configurações do dispositivo móvel são alteradas após a próxima sincronização do dispositivo com o Servidor de MDM do iOS.

Como resultado, depois que a política é aplicada, as contas do Exchange ActiveSync da lista compilada são adicionadas no dispositivo móvel do usuário.

Configurar uma caixa de e-mail do Exchange em dispositivos Android

Para trabalhar com e-mail corporativo, contatos e o calendário no dispositivo móvel, você pode definir as configurações de caixa de e-mail do Exchange para o aplicativo padrão Samsung Email.

Uma caixa de e-mail do Exchange pode ser configurada apenas em dispositivos Samsung que executam Android 9 ou versões anteriores.

Para configurar uma caixa de e-mail do Exchange no dispositivo móvel de um usuário:

1. Na janela principal do Kaspersky Next Expert View (cloud), selecione **Gerenciamento de ativos** → **Políticas**. Na lista de políticas de grupo aberta, clique no nome da política que deseja configurar.
2. Na janela de propriedades da política, selecione **Configurações do aplicativo**.
3. Selecione **Android** e vá para a seção **Configurações do Samsung Knox**.
4. No cartão **Exchange ActiveSync**, clique em **Configurações**.
A janela **Exchange ActiveSync** é exibida.
5. Ative as configurações usando o botão **Exchange ActiveSync**.
6. No campo **Endereço do servidor**, insira o endereço IP ou nome DNS do servidor que hospeda o servidor de e-mail.
7. No campo **Nome do domínio**, insira o nome do domínio do usuário do dispositivo móvel na rede corporativa.

8. Na lista suspensa **Intervalo de sincronização**, selecione o intervalo de sincronização de dispositivos móveis com o servidor do Microsoft Exchange.
9. Para usar o protocolo de transporte de dados SSL (Secure Sockets Layer), selecione a caixa de seleção **Usar conexão SSL**. O protocolo SSL usa criptografia e autenticação baseada em certificado para a transferência segura de dados. Essa caixa de seleção é marcada por padrão.
10. Para usar certificados digitais para proteger a transferência de dados entre o dispositivo móvel do usuário e o servidor Microsoft Exchange, selecione a caixa de seleção **Verificar o certificado do servidor**. É feita a verificação da emissão do certificado do servidor a partir do certificado raiz confiável. Essa caixa de seleção é marcada por padrão.
11. Clique em **Salvar** para salvar as alterações efetuadas.

As configurações do dispositivo móvel são alteradas após a próxima sincronização do dispositivo com o Kaspersky Security Center.

Configurar níveis de proteção no Kaspersky Security Center

Essas configurações se aplicam a dispositivos Android.

Para configurar regras para atribuir níveis de proteção no Kaspersky Security Center:

1. Na janela principal do Kaspersky Next Expert View (cloud), selecione **Gerenciamento de ativos** → **Políticas**. Na lista de políticas de grupo aberta, clique no nome da política que deseja configurar.
2. Na janela de propriedades da política, selecione **Configurações do aplicativo**.
3. Selecione **Android** e vá até a seção **Configurações do KES for Android**.
4. No cartão **Configurações de gravidade para o nível de proteção do dispositivo**, clique em **Configurações**. A janela **Configurações de gravidade para o nível de proteção do dispositivo** é exibida.
5. Ative as configurações usando o botão **Configurações de gravidade para o nível de proteção do dispositivo**.
6. Selecione o nível de proteção **OK**, **Advertência** ou **Crítico** para cada uma das seguintes condições:

- **A proteção em tempo real não está em execução**

A lista suspensa na qual você pode selecionar o nível de proteção de um dispositivo móvel no qual a proteção em tempo real não está em execução.

A proteção em tempo real permite detectar ameaças em arquivos que estão sendo abertos, assim como verificar novos aplicativos e interromper infecções de dispositivos em tempo real.

A execução da proteção em tempo real pode falhar pelos seguintes motivos:

- O usuário recusou usar a Kaspersky Security Network no dispositivo móvel nas configurações de antimalware do Kaspersky Endpoint Security for Android.
- O usuário não concedeu ao aplicativo o acesso para gerenciar todos os arquivos.

Se a proteção em tempo real não estiver em execução, você também poderá configurar restrições à operação do dispositivo móvel nas configurações **Controle de conformidade** da política.

- **A Proteção na Web e o Controle da Web não estão em execução**

Lista suspensa onde você pode selecionar o nível de proteção de um dispositivo móvel no qual a Proteção na Web e o Controle da Web não estão em execução.

A Proteção na Web permite verificar sites e bloquear sites de phishing e maliciosos.

O Controle da Web permite configurar o acesso do usuário a sites específicos e categorias de sites.

A Proteção na Web e o Controle da Web podem não funcionar pelos seguintes motivos:

- O usuário desativou a Proteção na Web no dispositivo móvel na configurações do Kaspersky Endpoint Security for Android.
- O usuário não ativou o Kaspersky Endpoint Security for Android como um recurso de Acessibilidade.
- A permissão [Ignorar otimização da bateria](#) não foi concedida.
- A Declaração da Proteção na Web não foi aceita.

Se a Proteção na Web e o Controle da Web não estiverem em execução, você também poderá configurar restrições à operação do dispositivo móvel nas configurações **Controle de conformidade** da política.

- **O Controle de aplicativos não está em execução**

A lista suspensa onde você pode selecionar o nível de proteção de um dispositivo móvel no qual o Controle de aplicativos não está em execução.

O Controle de aplicativos permite bloquear a execução de aplicativos em dispositivos móveis se estes aplicativos não atendem os requisitos de segurança corporativos.

O Controle de aplicativos pode não ser executado se o usuário não ativou o aplicativo como um recurso de Acessibilidade em dispositivos que executam o Android 5 ou posterior.

Se o Controle de aplicativos não estiver em execução, você também poderá configurar restrições à operação do dispositivo móvel nas configurações **Controle de conformidade** da política.

- **O bloqueio do dispositivo não está disponível**

A lista suspensa onde você pode selecionar o nível de proteção de um dispositivo móvel no qual o bloqueio do dispositivo não está disponível.

O dispositivo pode ser bloqueado nos seguintes casos:

- O comando Antirroubo é recebido.
- O Cartão SIM é substituído ou o dispositivo está ligado sem um Cartão SIM.
- Uma tentativa é feita para remover o Kaspersky Endpoint Security for Android enquanto a proteção contra a remoção do aplicativo estiver ativada.

O bloqueio do dispositivo pode estar indisponível devido aos seguintes motivos:

- O usuário não definiu o aplicativo como um administrador de dispositivo.
- O usuário não ativou o aplicativo como um serviço de Acessibilidade em dispositivos que executam o Android 7 ou posterior.
- O usuário não ativou o aplicativo para sobrepor outras janelas em dispositivos que executam o Android 7 ou posterior.

- **A localização do dispositivo não está disponível**

Lista suspensa onde você pode selecionar o nível de proteção de um dispositivo móvel cuja localização não pode ser determinada.

A localização é determinada depois que o comando **Localizar o dispositivo** é recebido.

A localização do dispositivo pode estar indisponível pelos seguintes motivos:

- O usuário não concedeu a permissão de localizar o dispositivo no aplicativo.
- O usuário desativou o módulo GPS nas configurações do dispositivo.
- **As versões da Declaração da Kaspersky Security Network não correspondem**

Lista suspensa onde é possível selecionar o nível de proteção de um dispositivo móvel se a versão da Declaração da Kaspersky Security Network aceita pelo administrador não corresponder à versão aceita pelo usuário do dispositivo. As estatísticas não listadas na versão da declaração aceita pelo usuário não são enviadas à Kaspersky Security Network.

- **As versões da Declaração de marketing não correspondem**

Lista suspensa na qual é possível selecionar o nível de proteção de um dispositivo móvel se a versão da Declaração sobre o processamento de dados para fins de marketing aceita pelo administrador não corresponder à versão aceita pelo usuário do dispositivo. Os dados não são transferidos para serviços de terceiros.

A lista de serviços de terceiros pode ser encontrada na Declaração sobre o processamento de dados para fins de marketing.

7. Clique em **OK**.

8. Clique em **Salvar** para salvar as alterações efetuadas.

As configurações do dispositivo móvel são alteradas após a próxima sincronização do dispositivo com o Kaspersky Security Center.

Para obter mais informações sobre valores padrão, motivos e condições para atribuir níveis de proteção, consulte a seção [Níveis de proteção de dispositivos móveis](#).

Criar um relatório sobre os aplicativos móveis instalados

O **Relatório sobre os aplicativos móveis instalados** permite obter informações detalhadas sobre os aplicativos instalados nos dispositivos Android dos usuários.

Para permitir que o relatório exiba informações, a caixa de seleção **Enviar dados sobre aplicativos instalados** deve ser marcada nas configurações **Controle de Aplicativos** e o tipo de evento de informações **Um aplicativo foi instalado ou removido (Lista de aplicativos instalados)** deve ser armazenado no banco de dados do Servidor de Administração.

Para ativar o envio de dados:

1. Na janela principal do Kaspersky Next Expert View (cloud), selecione **Gerenciamento de ativos** → **Políticas**. Na lista de políticas de grupo aberta, clique no nome da política que deseja configurar.
2. Na janela de propriedades da política, selecione **Configurações do aplicativo**.
3. Selecione **Android** e vá para a seção **Controles de segurança**.

4. No cartão **Controle de Aplicativos**, clique em **Configurações**.
A janela **Controle de Aplicativos** se abre.
5. Na seção **Relatório sobre aplicativos instalados**, marque a caixa de seleção **Enviar dados sobre aplicativos instalados**.
6. Se você quiser receber dados sobre aplicativos do sistema, marque a caixa de seleção **Enviar dados sobre aplicativos incorporados**.
7. Se você quiser receber dados sobre aplicativos de serviço que não têm uma interface e não podem ser abertos pelo usuário, marque a caixa de seleção **Enviar dados sobre aplicativos de serviço**.
8. Clique em **OK**.
9. Clique em **Salvar** para salvar as alterações efetuadas.
10. Clique no nome da política e selecione **Configuração de eventos**.
11. Siga para a seção **Informações**.
12. Clique no evento **Um aplicativo foi instalado ou removido (Lista de aplicativos instalados)** para abrir suas propriedades.
13. Na janela de propriedades do evento, ative o botão **Armazenar no banco de dados do Servidor de Administração por (dias)** e defina o período de armazenamento. Por padrão, o período de armazenamento é de 30 dias.

Após o período de armazenamento expirar, o Servidor de Administração exclui as informações desatualizadas do banco de dados. Para obter mais informações sobre eventos, consulte a [Ajuda do Kaspersky Security Center](#) ².

14. Clique em **OK**.
 15. Clique em **Salvar** para salvar as alterações efetuadas.
- O envio de dados está ativado.

Para configurar um relatório sobre aplicativos móveis instalados:

1. Na janela principal do Kaspersky Next Expert View (cloud), selecione **Monitoramento** → **Relatórios**.
2. Clique no modelo de relatório **Relatório sobre os aplicativos móveis instalados** para abrir suas propriedades.
3. Na janela que se abre, clique em **Editar**.

4. Edite as propriedades do modelo de relatório:

- Na guia **Geral**, especifique os seguintes parâmetros:

- Nome do modelo de relatório

- **Número máximo de entradas a exibir**

Se esta opção estiver ativada, o número de entradas exibidas na tabela com dados de relatório detalhados não será maior que o valor especificado.

As entradas de relatório são primeiro classificadas segundo as regras especificadas na seção **Campos > Campos de detalhes** das propriedades do modelo de relatório e, em seguida, apenas a primeira das entradas resultantes é mantida. O cabeçalho da tabela com dados de relatório detalhados mostra o número de entradas exibidas e o número total de entradas disponíveis que combinam com outras configurações do modelo de relatório.

Se esta opção estiver desativada, a tabela com dados de relatório detalhados exibe todas as entradas disponíveis. Não recomendamos que você desative essa opção. Limitar o número de entradas de relatório exibidas reduz a carga do sistema de gerenciamento de banco de dados (DBMS) e reduz o tempo necessário para gerar e exportar o relatório. Alguns relatórios contêm um número excessivo de entradas. Se este for o caso, você pode ter dificuldade para ler e analisar todas elas. Além disso, seu dispositivo pode ficar sem memória ao gerar esse relatório. Consequentemente, você não poderá visualizar o relatório.

Por padrão, esta opção está ativada. O valor padrão é 1.000.

- **Grupo**

O conjunto de dispositivos cliente para o qual o relatório é criado.

- **Incluir dados dos Servidores de Administração secundários e virtuais**

Se esta opção estiver ativada, o relatório inclui as informações dos Servidores de Administração secundário e virtual subordinados ao Servidor de Administração para o qual o modelo de relatório é criado.

Desative esta opção se você quiser visualizar dados somente do Servidor de Administração atual.

Por padrão, esta opção está ativada.

- **Até o nível de aninhamento**

O relatório inclui dados de servidores de administração secundários e virtuais localizados sob o Servidor de administração atual a um nível de agrupamento menor ou igual ao valor especificado.

O valor padrão é 1. Convém alterar esse valor caso necessite obter as informações dos Servidores de Administração secundários localizados em níveis mais baixos na árvore.

- **Intervalo de espera dos dados (min)**

Antes de gerar o relatório, o Servidor de administração para o qual o modelo de relatório é criado aguarda pelos dados de Servidores de administração secundários durante o número de minutos especificado. Se nenhum dado for recebido de um Servidor de Administração secundário ao fim desse período, o relatório é executado mesmo assim. Em vez de dados atualizados, o relatório exibe os dados retirados do cache (caso a opção **Dados em cache dos Servidores de Administração secundários** esteja ativada) ou, caso contrário, **N/A** (não acessível).

O valor padrão é 5 (minutos).

- **Dados em cache dos Servidores de Administração secundários**

Os Servidores de Administração secundários regularmente transferem dados para o Servidor de Administração para o qual o modelo de relatório é criado. Os dados transferidos são armazenados no cache naquele Servidor de Administração.

Se o Servidor de Administração atual não puder receber dados de um Servidor de Administração secundário enquanto o relatório estiver sendo gerado, o relatório exibirá dados retirados do cache. A data em que os dados foram transferidos para o cache também é exibida.

Ativar essa opção permite a visualização das informações dos Servidores de Administração secundários, mesmo se os dados atualizados não puderem ser recuperados. Entretanto, os dados exibidos podem ser obsoletos.

Por padrão, esta opção está desativada.

- **Transferir informações detalhadas dos Servidores de Administração secundários**

No relatório gerado, a tabela contendo dados de relatório detalhados inclui dados dos Servidores de Administração secundários do Servidor de Administração para o qual o modelo de relatório é criado.

Ativar esta opção reduz a velocidade de geração de relatórios e aumenta o tráfego entre Servidores de Administração. Entretanto, permite visualizar todos os dados em um relatório.

Em vez de ativar a opção, convém analisar dados de relatório detalhados para detectar um Servidor de Administração secundário defeituoso e, em seguida, gerar o mesmo relatório apenas para o Servidor de Administração defeituoso.

Por padrão, esta opção está desativada.

- Na guia **Campos**, selecione os campos que serão exibidos no relatório e a ordem desses campos, e configure se o relatório deve ser classificados e filtrado segundo cada um dos campos.

5. Clique em **Salvar** para salvar as alterações efetuadas.

O modelo de relatório atualizado aparece na lista de modelos de relatório.

Para criar e exibir um relatório sobre aplicativos móveis instalados:

1. Na janela principal do Kaspersky Next Expert View (cloud), selecione **Monitoramento** → **Relatórios**.
2. Clique em um relatório com o tipo **Relatório sobre os aplicativos móveis instalados**.

Um relatório usando o modelo selecionado é gerado e exibido.

Para obter mais informações sobre como usar relatórios, gerenciar modelos de relatórios personalizados, usar modelos de relatórios para gerar novos relatórios e criar tarefas de entrega de relatórios, consulte a [Ajuda do Kaspersky Security Center](#) ².

Configurar as 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 for Android 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. Você pode tocar no status da proteção do dispositivo e ver os problemas de segurança no aplicativo.
- **Notificações do aplicativo.** Estas notificações informam o usuário do dispositivo sobre o aplicativo (por exemplo, a detecção de uma ameaça).
- **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.

No Android 13, o usuário do dispositivo deve conceder permissão para envio de notificações durante ou depois do Assistente de configuração inicial.

O usuário 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. Na janela principal do Kaspersky Next Expert View (cloud), selecione **Gerenciamento de ativos** → **Políticas**. Na lista de políticas de grupo aberta, clique no nome da política que deseja configurar.
2. Na janela de propriedades da política, selecione **Configurações do aplicativo**.
3. Selecione **Android** e vá até a seção **Configurações do KES for Android**.
4. No cartão **Configurar notificações**, clique em **Configurações**.
A janela **Configurar notificações** se abre.
5. Ative as configurações usando o botão **Configurar notificações**.
6. Se quiser ocultar todas as notificações e mensagens pop-up, na seção **Notificações do Kaspersky Endpoint Security**, marque a caixa de seleção **Desativar as 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.

As notificações no aplicativo (por exemplo, quando o usuário atualiza bancos de dados antimalware manualmente) ainda serão exibidas.

Recomendamos que você ative as notificações e as 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. Nesse caso, os usuários de dispositivos móveis não verão o status de proteção do dispositivo, a menos que abram o aplicativo.

7. Na seção **Notificações internas do aplicativo Kaspersky Endpoint Security**, selecione os problemas do Kaspersky Endpoint Security for Android que você deseja exibir no dispositivo móvel do usuário.

Por padrão, o usuário pode ignorar a notificação **O dispositivo não foi sincronizado com o Servidor de Administração fez tempo**. Se quiser ter mais controle sobre a frequência de sincronização, [ao configurar regras para verificar a conformidade com a política](#), selecione o critério **O dispositivo não foi sincronizado fez tempo** para chamar a atenção do usuário para o problema.

A exibição de determinados problemas do Kaspersky Endpoint Security for Android é obrigatória. Esses problemas são sempre exibidos no dispositivo (por exemplo, problemas sobre a expiração da licença).

8. Clique em **OK**.

9. Clique em **Salvar** para salvar as alterações efetuadas.

As configurações do dispositivo móvel são alteradas após a próxima sincronização do dispositivo com o Kaspersky Security Center. As notificações que você desativar não serão exibidas no dispositivo móvel do usuário.

Conectar dispositivos iOS MDM ao AirPlay

Configure a conexão com dispositivos AirPlay para transmitir músicas, fotos e vídeos a partir do dispositivo iOS MDM para dispositivos AirPlay. Para poder usar o AirPlay, o dispositivo móvel e os dispositivos AirPlay devem estar conectados com a mesma rede sem fio. Os dispositivos AirPlay incluem dispositivos Apple TV (segunda geração ou posterior), dispositivos AirPort Express, alto-falantes, TVs e rádios compatíveis com AirPlay.

A conexão automática com dispositivos AirPlay está disponível para dispositivos no modo de operação "Perfil de gerenciamento".

Para configurar a conexão de um dispositivo iOS MDM com dispositivos AirPlay:

1. Na janela principal do Kaspersky Next Expert View (cloud), selecione **Gerenciamento de ativos** → **Políticas**. Na lista de políticas de grupo aberta, clique no nome da política que deseja configurar.
2. Na janela de propriedades da política, selecione **Configurações do aplicativo**.
3. Selecione **iOS** e vá para a seção **Configuração do dispositivo**.
4. No cartão **AirPlay**, clique em **Configurações**.
A janela **AirPlay** é exibida.
5. Ative as configurações usando o botão **AirPlay**.
6. Na seção **Senhas**, clique em **Adicionar senha**.
7. No campo **Dispositivo**, insira o nome do dispositivo AirPlay na rede sem fio.
8. No campo **Senha**, insira a senha para o dispositivo AirPlay.

9. Se você quiser que os dispositivos iOS MDM se conectem somente a dispositivos AirPlay específicos, crie uma lista de dispositivos permitidos na seção **Dispositivos permitidos**. Para fazer isso, clique em **Adicionar dispositivo** e especifique os endereços MAC dos dispositivos AirPlay.

Para conectar dispositivos iOS MDM executando o iOS 18 ou posterior a qualquer dispositivo AirPlay, você deve especificar o **Nome do dispositivo**.

Para conectar dispositivos iOS MDM executando o iOS 17 ou anterior a qualquer dispositivo AirPlay, você deve especificar o endereço Ethernet e o Wi-Fi para cada dispositivo.

O acesso a dispositivos AirPlay que não estão na lista de dispositivos permitidos é bloqueado. Se a lista de dispositivos permitidos estiver vazia, o Kaspersky Mobile Devices Protection and Management permite o acesso a todos os dispositivos AirPlay.

10. Clique em **OK**.

11. Clique em **Salvar** para salvar as alterações efetuadas.

Como resultado, depois que a política é aplicada, o dispositivo móvel do usuário se conecta automaticamente com dispositivos AirPlay para transmitir conteúdo de mídia.

Conectar dispositivos iOS MDM ao AirPrint

Para ativar a impressão de documentos a partir de um dispositivo iOS MDM sem fio usando a AirPrint, configure a conexão automática a impressoras AirPrint. O dispositivo móvel e a impressora devem estar conectados na mesma rede sem fio. O acesso compartilhado para todos os usuários deve ser configurado na impressora AirPrint.

Para configurar a conexão de um dispositivo iOS MDM a uma impressora AirPrint:

1. Na janela principal do Kaspersky Next Expert View (cloud), selecione **Gerenciamento de ativos** → **Políticas**. Na lista de políticas de grupo aberta, clique no nome da política que deseja configurar.
2. Na janela de propriedades da política, selecione **Configurações do aplicativo**.
3. Selecione **iOS** e vá para a seção **Configuração do dispositivo**.
4. No cartão **AirPrint**, clique em **Configurações**.
A janela **AirPrint** é exibida.
5. Ative as configurações usando o botão **AirPrint**.
6. Clique em **Adicionar**.
A janela **Adicionar impressora** é exibida.
7. No campo **Endereço IP ou FQDN**, insira o endereço IP ou um nome de domínio totalmente qualificado (FQDN) da impressora AirPrint.
8. No campo **Porta**, insira a porta de escuta do destino do AirPrint.
9. 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

10. Clique em **Adicionar**.

A nova impressora AirPrint adicionada é exibida na lista.

11. Clique em **OK**.

12. Clique em **Salvar** para salvar as alterações efetuadas.

Como resultado, depois que a política é aplicada, o usuário do dispositivo móvel pode imprimir documentos sem fio na impressora AirPrint.

Configurar o nome do ponto de acesso (APN)

Esta seção fornece instruções sobre como conectar um dispositivo móvel aos serviços de dados de celular em uma rede móvel.

Configurar a APN em dispositivos Android (somente Samsung)

O APN pode ser configurado somente para 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 móvel. Configurações de ponto de acesso incorretas podem resultar em cobranças adicionais.

Para definir as configurações do Nome do ponto de acesso (APN) no dispositivo móvel de um usuário:

1. Na janela principal do Kaspersky Next Expert View (cloud), selecione **Gerenciamento de ativos** → **Políticas**. Na lista de políticas de grupo aberta, clique no nome da política que deseja configurar.
2. Na janela de propriedades da política, selecione **Configurações do aplicativo**.
3. Selecione **Android** e vá para a seção **Configurações do Samsung Knox**.
4. No cartão **Configurações de APN**, clique em **Configurações**.
A janela **Configurações de APN** é exibida.

5. Ative as configurações usando o botão **Configurações de APN**.

O botão neste cartão não ativa nem desativa a funcionalidade correspondente nos dispositivos. Ativar o botão permite definir configurações personalizadas. Desativar o botão permite usar as configurações padrão.

6. Especifique as seguintes configurações de ponto de acesso para conectar o usuário ao serviço de dados:

- Na lista suspensa **Tipo de APN**, selecione o tipo de ponto de acesso (APN) para transmissão de dados em uma rede móvel GPRS/3G/4G:
 - **Internet**. Conexão do dispositivo móvel do usuário à Internet.
 - **MMS**. Troca de mensagens multimídia MMS.
 - **Internet e MMS**. Conexão à Internet e troca de mensagens multimídia. Esse é o valor padrão.
- No campo **Nome de APN**, especifique o nome do ponto de acesso.
- No campo **MCC**, insira o código de país da rede celular (MCC).
- No campo **MNC**, insira o código de rede celular (MNC).

7. Caso você tenha selecionado **MMS** ou **Internet e MMS** como tipo de ponto de acesso, especifique as configurações MMS adicionais na seção **Servidor MMS**:

- No campo **Nome do servidor MMS**, especifique o nome completo do domínio do servidor do operador de telefonia móvel usado para troca de MMS (por exemplo, `mms.mobile.com`).
- No campo **Endereço do servidor proxy MMS**, insira o nome de rede ou endereço IP do servidor proxy.
- No campo **Porta do servidor proxy MMS**, especifique o número da porta do servidor do operador de telefonia usado para troca de MMS.

8. Na seção **Autenticação**, especifique as seguintes configurações de autenticação:

- Na lista suspensa **Tipo de autenticação**, selecione o tipo de autenticação do usuário do dispositivo móvel que será utilizado no servidor do operador de telefonia móvel para acesso à rede. Por padrão, a autenticação de usuário não é necessária. Os seguintes tipos estão disponíveis:
 - **Nenhum**. A autenticação não é necessária para acessar a rede móvel.
 - **PAP** (Protocolo de Autenticação de Senha). Um protocolo de autenticação que usa senhas como texto simples não criptografado.
 - **CHAP** (Protocolo de Autenticação por Desafio Handshake). Um protocolo de autenticação de solicitação-resposta que usa hash MD5 padrão para criptografar a resposta.
 - **Simultaneamente**. Uso combinado dos protocolos CHAP e PAP.
- No campo **Nome de usuário**, insira o nome de usuário para autorização na rede móvel.
- No campo **Senha**, insira a senha para autorização do usuário na rede móvel.

9. Na seção **Rede**, especifique as seguintes configurações de rede:

- No campo **Nome da rede**, insira o nome da rede.
- 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.

10. Na seção **Servidor proxy**, especifique as seguintes configurações de servidor proxy:

- Marque a caixa de seleção **Usar um servidor proxy** para ativar o uso de um servidor proxy. Essa caixa de seleção é desmarcada por padrão.
- No campo **Endereço do servidor proxy**, especifique o nome de rede ou endereço IP do servidor proxy do operador para acesso de rede. Este campo está disponível somente se a caixa de seleção **Usar um servidor proxy** estiver marcada.
- No campo **Porta do servidor proxy**, especifique o número da porta do servidor proxy do operador para acesso de rede. Este campo está disponível somente se a caixa de seleção **Usar um servidor proxy** estiver marcada.

11. Clique em **OK**.

12. Clique em **Salvar** para salvar as alterações efetuadas.

As configurações do dispositivo móvel são alteradas após a 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.

Para configurar um ponto de acesso num dispositivo iOS MDM do usuário:

1. Na janela principal do Kaspersky Next Expert View (cloud), selecione **Gerenciamento de ativos** → **Políticas**. Na lista de políticas de grupo aberta, clique no nome da política que deseja configurar.
2. Na janela de propriedades da política, selecione **Configurações do aplicativo**.
3. Selecione **iOS** e vá para a seção **Configuração do dispositivo**.
4. No cartão **Configurações de APN**, clique em **Configurações**.
A janela **Configurações de APN** é exibida.
5. Ative as configurações usando o botão **Configurações de APN**.

O botão neste cartão não ativa nem desativa a funcionalidade correspondente nos dispositivos. Ativar o botão permite definir configurações personalizadas. Desativar o botão permite usar as configurações padrão.

6. Na lista suspensa **Tipo de APN**, selecione o tipo de ponto de acesso para transferência de dados em uma rede móvel GPRS/3G/4G:

- **APN incorporado.** Configure as configurações de comunicação celular para transferência de dados por meio de uma operadora de rede móvel compatível com um SIM Apple integrado. Para obter mais detalhes sobre dispositivos com o SIM Apple integrado, visite o [site de Suporte da Apple](#).
- **APN.** Defina as configurações de comunicação celular para transferência de dados por meio da operadora de rede móvel do cartão SIM inserido.
- **APN incorporado e APN.** Defina as configurações de comunicação celular para transferência de dados por meio das operadoras de rede móvel do cartão SIM inserido e do SIM Apple integrado. Para obter mais detalhes sobre dispositivos com um SIM Apple integrado e um slot para cartão SIM, visite o [site de Suporte da Apple](#).

7. Se você selecionou **APN**, na seção **APN**, clique em **Adicionar**.

A janela **Adicionar APN** é exibida.

8. Defina as seguintes configurações:

- a. No campo **Nome de APN**, especifique o nome do ponto de acesso.
- b. Na lista suspensa **Tipo de autenticação**, selecione o tipo de autenticação do usuário no servidor da operadora de telefonia móvel para o acesso à rede (Internet e MMS).
- c. No campo **Nome de usuário**, insira o nome de usuário para autorização na rede móvel.
- d. No campo **Senha**, insira a senha para autorização do usuário na rede móvel.
- e. No campo **Endereço do servidor proxy**, insira o nome do host ou o endereço IP do servidor proxy.
- f. No campo **Porta do servidor proxy**, insira o número da porta do servidor proxy.
- g. Na lista suspensa **Protocolo permitido**, selecione o protocolo da Internet.
- h. Na lista suspensa **Protocolo permitido para roaming**, selecione o protocolo da Internet que será usado durante o roaming internacional.
- i. Na lista suspensa **Protocolo permitido para roaming doméstico**, selecione o protocolo da Internet que será usado durante o roaming doméstico.
- j. Se você quiser que os dispositivos em redes somente IPv6 possam ter acessibilidade a serviços de Internet somente IPv4, marque a caixa de seleção **Usar a tecnologia 4G4XLAT**.
- k. Clique em **OK**.

9. Se você selecionou **APN incorporado**, defina as seguintes configurações:

- a. No campo **Nome de APN incorporado**, especifique o nome do ponto de acesso.
- b. Na lista suspensa **Tipo de autenticação**, selecione o tipo de autenticação do usuário no servidor da operadora de telefonia móvel para o acesso à rede (Internet e MMS).
- c. No campo **Nome de usuário**, insira o nome de usuário para autorização na rede móvel.

d. No campo **Senha**, insira a senha para autorização do usuário na rede móvel.

e. Na lista suspensa **Protocolo permitido**, selecione o protocolo da Internet.

10. Clique em **OK**.

11. Clique em **Salvar** 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.

Contêiner corporativo

Esta seção contém informações como trabalhar com um contêiner corporativo.

Sobre contêineres corporativos

O Android Enterprise é uma plataforma para gerenciar a infraestrutura corporativa de dispositivos móveis e fornece aos funcionários da empresa um ambiente de trabalho seguro no qual eles podem usar seus dispositivos móveis. Para obter detalhes sobre como usar o Android Enterprise, consulte o [site de suporte da Google](#).

Você pode criar um contêiner corporativo que usa um perfil de trabalho do Android em um dispositivo móvel pessoal de um usuário. Um contêiner corporativo é um ambiente seguro no qual o administrador pode gerenciar aplicativos e contas de usuário sem restringir o uso de seus próprios dados pelo usuário. Quando um contêiner corporativo é criado no dispositivo móvel do usuário, os seguintes aplicativos corporativos são automaticamente instalados: Google Play, Google Chrome, Downloads, Kaspersky Endpoint Security for Android e outros. Os aplicativos instalados no contêiner corporativo, bem como as notificações desses aplicativos, são marcados com um ícone de pasta. Você deve criar uma conta corporativa do Google separada para o aplicativo Google Play. Os aplicativos instalados no contêiner corporativo aparecem na lista de aplicativos comuns.

Configurar um contêiner corporativo

Para definir as configurações de um contêiner corporativo:

1. Na janela principal do Kaspersky Next Expert View (cloud), selecione **Gerenciamento de ativos** → **Políticas**. Na lista de políticas de grupo aberta, clique no nome da política que deseja configurar.
2. Na janela de propriedades da política, selecione **Configurações do aplicativo**.
3. Selecione **Android** e vá para a seção **Contêiner corporativo**.
4. No cartão **Contêiner corporativo nos dispositivos**, clique em **Configurações**.
A janela **Contêiner corporativo nos dispositivos** é exibida.
5. Ative as configurações usando o botão **Contêiner corporativo nos dispositivos**.

6. Especifique as configurações do contêiner corporativo:

- Na guia **Geral**, você pode especificar as configurações para compartilhamento de dados, contatos e muito mais.
- Configurações na seção **Acesso e compartilhamento de dados**:

- **Proibir o uso da área de transferência entre aplicativos pessoais e contêiner corporativo**

Marcar ou desmarcar essa caixa de seleção especifica se o usuário do dispositivo tem permissão para copiar dados através da área de transferência entre aplicativos pessoais e o contêiner corporativo.

Essa caixa de seleção é marcada por padrão.

- **Proibir a ativação da depuração em USB**

Restringe o uso de depuração USB no dispositivo móvel do usuário no contêiner corporativo. No modo de depuração USB, o usuário poderá efetuar o download de um aplicativo através de uma estação de trabalho, por exemplo.

Se a caixa de seleção estiver marcada, o modo de depuração USB não estará disponível para o usuário. O usuário é incapaz de configurar o dispositivo móvel através do USB após conectar o dispositivo com uma estação de trabalho.

Se a caixa de seleção estiver desmarcada, o usuário poderá ativar o modo de depuração USB, conectar o dispositivo móvel a uma estação de trabalho através do USB e configurar o dispositivo.

Essa caixa de seleção é marcada por padrão.

- Na guia **Aplicativos**, especifique as seguintes configurações:

- Configurações na seção **Geral**:

- **Ativar o Controle de Aplicativos apenas no contêiner corporativo**

Controla a inicialização dos aplicativos no contêiner corporativo no dispositivo móvel do usuário. Você pode criar listas de aplicativos permitidos, proibidos e recomendados, assim como categorias de aplicativos permitidos e proibidos na seção **Controle de Aplicativos**.

Se a caixa de seleção estiver marcada, dependendo das configurações do Controle de aplicativos, o Kaspersky Endpoint Security bloqueia ou permite a inicialização dos aplicativos somente no contêiner corporativo. O Controle de aplicativos não funciona no espaço pessoal do usuário.

Essa caixa de seleção é marcada por padrão.

- **Ativar a Proteção na Web e Controle da Web apenas no contêiner corporativo**

Restringe o acesso do usuário a sites no contêiner corporativo do dispositivo. Você pode especificar as configurações de acesso ao site nas configurações do **Controle da Web**.

Se essa caixa de seleção estiver marcada, a Proteção na Web e o Controle da Web bloqueiam ou permitem o acesso a sites somente no contêiner corporativo. Além disso, a Proteção na Web e o Controle da Web não funcionam no espaço pessoal do usuário.

Se a caixa de seleção estiver desmarcada, dependendo das configurações da Proteção na Web e do Controle da Web, o Kaspersky Endpoint Security bloqueia ou permite o acesso a sites no espaço pessoal do usuário e no contêiner corporativo.

Essa caixa de seleção é marcada por padrão.

- **Proibir a instalação de aplicativos de fontes desconhecidas no contêiner corporativo**

Restringe a instalação dos aplicativos no contêiner corporativo de todas as origens que não seja do Google Play Enterprise.

Se a caixa de seleção estiver marcada, o usuário somente poderá instalar aplicativos a partir do Google Play. Os usuários utilizam suas próprias contas corporativas do Google para instalar aplicativos.

Se a caixa de seleção estiver desmarcada, o usuário poderá instalar os aplicativos de qualquer forma possível. Somente aplicativos proibidos nas configurações do **Controle de Aplicativos** não podem ser instalados.

Essa caixa de seleção é desmarcada por padrão.

- **Proibir a remoção de aplicativos do contêiner corporativo**

Marcar ou desmarcar esta caixa de seleção especifica se o usuário está proibido de remover aplicativos do contêiner corporativo.

Essa caixa de seleção é desmarcada por padrão.

- Na guia **Certificados**, é possível definir as seguintes configurações:

- **Duplicar a instalação de certificados VPN no espaço pessoal do usuário**

Marcar ou desmarcar a caixa de seleção especifica se o certificado VPN adicionado na seção **Móvel** → **Certificados** do Kaspersky Next Expert View (cloud) e instalado no contêiner corporativo também será instalado no espaço pessoal do usuário.

Por padrão, os certificados VPN recebidos do Kaspersky Security Center são instalados no contêiner corporativo. Essa configuração é aplicada quando um novo certificado VPN é emitido.

Essa caixa de seleção é desmarcada por padrão.

7. Clique em **OK**.

8. Clique em **Salvar** para salvar as alterações efetuadas.

As configurações do dispositivo móvel são alteradas após a próxima sincronização do dispositivo com o Kaspersky Security Center. O dispositivo móvel do usuário é dividido em um contêiner corporativo e um espaço pessoal.

Desbloquear o contêiner corporativo

O contêiner corporativo pode ser bloqueado se o dispositivo não atender aos requisitos de segurança do Controle de conformidade.

Para desbloquear o contêiner corporativo, o usuário do dispositivo móvel deve inserir um código de uso único do contêiner corporativo na tela bloqueada. O código é gerado pelo Kaspersky Security Center e é exclusivo para cada dispositivo móvel. Quando o contêiner corporativo é desbloqueado, a senha do contêiner corporativo é definida com o valor padrão (1234).

Como administrador, você pode exibir o código nas configurações de política aplicadas ao dispositivo móvel. O comprimento do código pode ser alterado (4, 8, 12 ou 16 dígitos) nas configurações **Contêiner corporativo nos dispositivos** da política.

Para desbloquear um contêiner corporativo usando um código de uso único:

1. Na janela principal do Kaspersky Next Expert View (cloud), selecione **Gerenciamento de ativos** → **Móvel** → **Dispositivos**.
2. Clique no dispositivo móvel para o qual você deseja obter um código de uso único.

3. Selecione **Aplicativos** → **Kaspersky Mobile Devices Protection and Management**.

A janela de propriedades do Kaspersky Mobile Devices Protection and Management é exibida.

4. Selecione a guia **Configurações do aplicativo**.

O código de uso único para o dispositivo selecionado será exibido no campo **Código de uso único** da seção **Código de uso único do contêiner corporativo**.

5. Use qualquer método disponível (como e-mail) para comunicar o código de uso único ao usuário.

O usuário deve inserir o código de uso único recebido no seu dispositivo.

O contêiner corporativo do dispositivo móvel do usuário está desbloqueado.

Depois que o contêiner corporativo em um dispositivo é bloqueado, o histórico de senhas do contêiner corporativo é limpo. Isso significa que o usuário pode especificar uma senha recente, independentemente das configurações de senha do contêiner corporativo.

Adicionar uma conta LDAP

Essas configurações se aplicam aos dispositivos no modo de operação "Perfil de gerenciamento".

Para permitir que um usuário do dispositivo iOS MDM acesse contatos corporativos no servidor LDAP, adicione uma conta LDAP.

Para adicionar uma conta LDAP de um usuário do dispositivo iOS MDM:

1. Na janela principal do Kaspersky Next Expert View (cloud), selecione **Gerenciamento de ativos** → **Políticas**. Na lista de políticas de grupo aberta, clique no nome da política que deseja configurar.

2. Na janela de propriedades da política, selecione **Configurações do aplicativo**.

3. Selecione **iOS** e vá para a seção **Configuração do dispositivo**.

4. No cartão **LDAP**, clique em **Configurações**.

A janela **LDAP** é exibida.

5. Ative as configurações usando o botão **LDAP**.

6. Clique em **Adicionar**.

A janela **Adicionar conta LDAP** é exibida.

7. Na guia **Geral**, especifique as seguintes configurações de LDAP:

- Na seção **Servidor**, especifique as seguintes configurações do servidor:
 - No campo **Descrição**, insira uma descrição da conta LDAP do usuário.
 - No campo **Endereço do servidor**, insira o nome do domínio do servidor LDAP.

- Na seção **Autenticação**, especifique as credenciais do usuário:
 - No campo **Nome da conta**, insira o nome da conta para autorização no servidor da LDAP.
 - No campo **Senha**, insira a senha da conta LDAP para autorização no servidor LDAP.
 - Para usar o protocolo de transporte de dados SSL (Secure Sockets Layer) para proteger a transmissão de mensagens, selecione a caixa **Usar conexão SSL**.

8. A guia **Pesquisar**, faça a compilação de uma lista de consultas de pesquisa para o usuário do dispositivo iOS MDM acessar os dados corporativos no servidor LDAP:

- Clique no botão **Adicionar configurações** para adicionar um bloco das configurações da consulta de pesquisa.
- No campo **Nome**, insira o nome de uma consulta de pesquisa.
- Na lista suspensa **Escopo de pesquisa**, selecione o nível de aninhamento da pasta para a pesquisa de dados corporativos no servidor LDAP:
 - **Pasta raiz do servidor LDAP**. Pesquisar na pasta base do servidor LDAP.
 - **Subpastas do primeiro nível**. Pesquisar nas pastas no primeiro nível de aninhamento contando a partir da pasta base.
 - **Todas as subpastas**. Pesquisar nas pastas em todos os níveis de aninhamento a partir da pasta base.
- No campo **Pesquisar base**, insira o caminho da pasta no servidor LDAP na qual a pesquisa inicia-se (por exemplo: "ou=people", "o=example corp").
- Repita as etapas A a D para todas as consultas de pesquisa que você deseja adicionar ao dispositivo iOS MDM.

9. Clique em **Adicionar**.

A nova conta LDAP é exibida na lista.

Você pode modificar ou excluir contas LDAP da lista usando os botões **Editar** e **Excluir** na parte superior da lista.

10. Clique em **OK**.

11. Clique em **Salvar** para salvar as alterações efetuadas.

As configurações do dispositivo móvel são alteradas após a próxima sincronização do dispositivo com o Servidor de MDM do iOS.

Como resultado, depois que a política é aplicada, as contas LDAP da lista compilada são 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 contatos

Essas configurações se aplicam aos dispositivos no modo de operação "Perfil de gerenciamento".

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 contato por meio de qualquer dispositivo.

Para adicionar uma conta CardDAV de um usuário do dispositivo iOS MDM:

1. Na janela principal do Kaspersky Next Expert View (cloud), selecione **Gerenciamento de ativos** → **Políticas**. Na lista de políticas de grupo aberta, clique no nome da política que deseja configurar.
2. Na janela de propriedades da política, selecione **Configurações do aplicativo**.
3. Selecione **iOS** e vá para a seção **Configuração do dispositivo**.
4. No cartão **Contatos**, clique em **Configurações**.
A janela **Contatos** é exibida.
5. Ative as configurações usando o botão **Contatos**.
6. Clique em **Adicionar**.
A janela **Adicionar conta CardDAV** é exibida.
7. Na seção **Servidor**, no campo **Descrição**, insira uma descrição da conta CardDAV do usuário.
8. Nos campos **Endereço do servidor** e **Porta do servidor**, insira o nome do host ou o endereço IP do servidor CardDAV e o número da porta do servidor CardDAV.
9. No campo **Contatar URL**, especifique a URL da conta CardDAV do usuário do dispositivo iOS MDM no servidor CardDAV (por exemplo: `http://example.com/carddav/users/mycompany/user`).
A URL deve começar com `http://` ou `https://`.
10. Na seção **Autenticação**, no campo **Nome da conta**, insira o nome da conta para autorização no servidor CardDAV.
11. No campo **Senha**, insira a senha da conta CardDAV para autorização no servidor CardDAV.
12. Se quiser usar o protocolo de transporte de dados SSL (Secure Sockets Layer) para proteger a transmissão de dados entre o servidor CardDAV e o dispositivo móvel, selecione a caixa **Usar conexão SSL**.
13. Clique em **Adicionar**.
A nova conta CardDAV é exibida na lista.

Você pode modificar ou excluir contas CardDAV da lista usando os botões **Editar** e **Excluir** na parte superior da lista.

14. Clique em **OK**.

15. Clique em **Salvar** para salvar as alterações efetuadas.

As configurações do dispositivo móvel são alteradas após a próxima sincronização do dispositivo com o Servidor de MDM do iOS.

Como resultado, depois que a política é aplicada, as contas CardDAV da lista compilada são adicionadas no dispositivo móvel do usuário.

Se você tiver problemas ao adicionar ou atualizar contas, verifique se as configurações definidas estão corretas.

Adicionar uma conta de calendário

Para permitir que um usuário do dispositivo iOS MDM acesse seus eventos de calendário em um servidor CalDAV, adicione uma 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 de um usuário do dispositivo iOS MDM:

1. Na janela principal do Kaspersky Next Expert View (cloud), selecione **Gerenciamento de ativos** → **Políticas**. Na lista de políticas de grupo aberta, clique no nome da política que deseja configurar.
2. Na janela de propriedades da política, selecione **Configurações do aplicativo**.
3. Selecione **iOS** e vá para a seção **Configuração do dispositivo**.
4. No cartão **Calendário**, clique em **Configurações**.
A janela **Calendário** é exibida.
5. Ative as configurações usando o botão **Calendário**.
6. Clique em **Adicionar**.
A janela **Adicionar conta CalDAV** é exibida.
7. Na seção **Servidor**, no campo **Descrição**, insira uma descrição da conta CalDAV do usuário.
8. Nos campos **Endereço do servidor** e **Porta do servidor**, insira o nome do host ou o endereço IP do servidor CalDAV e o número da porta do servidor CalDAV.
9. No campo **URL do calendário**, especifique a URL da conta CalDAV do usuário do dispositivo iOS MDM no servidor CalDAV (por exemplo: `http://example.com/caldav/users/mycompany/user`).
A URL deve começar com `http://` ou `https://`.
10. Na seção **Autenticação**, no campo **Nome da conta**, insira o nome da conta para autorização no servidor CalDAV.
11. No campo **Senha**, defina a senha para a conta CalDAV para a autorização no servidor CalDAV.

12. Se quiser usar o protocolo de transporte de dados SSL (Secure Sockets Layer) para proteger a transmissão de dados de eventos entre o servidor CalDAV e o dispositivo móvel, selecione a caixa **Usar conexão SSL**.

13. Clique em **Adicionar**.

A nova conta de CalDAV aparece na lista.

Você pode modificar ou excluir contas CalDAV da lista usando os botões **Editar** e **Excluir** na parte superior da lista.

14. Clique em **OK**.

15. Clique em **Salvar** para salvar as alterações efetuadas.

As configurações do dispositivo móvel são alteradas após a próxima sincronização do dispositivo com o Servidor de MDM do iOS.

Como resultado, depois que a política é aplicada, as contas CalDAV da lista compilada são adicionadas no dispositivo móvel do usuário.

Se você tiver problemas ao adicionar ou atualizar contas, verifique se as configurações definidas estão corretas.

Configurar uma assinatura de calendário

Essas configurações se aplicam aos dispositivos no modo de operação "Perfil de gerenciamento".

Para permitir que o usuário do dispositivo iOS MDM adicione eventos de calendários compartilhados (como um calendário corporativo) ao calendário, adicione uma assinatura desses calendários. *Calendários compartilhados* são calendários de outros usuários que têm uma conta CalDAV, calendários iCal e outros calendários publicados.

Para adicionar uma assinatura do calendário:

1. Na janela principal do Kaspersky Next Expert View (cloud), selecione **Gerenciamento de ativos** → **Políticas**. Na lista de políticas de grupo aberta, clique no nome da política que deseja configurar.

2. Na janela de propriedades da política, selecione **Configurações do aplicativo**.

3. Selecione **iOS** e vá para a seção **Configuração do dispositivo**.

4. No cartão **Assinaturas do calendário**, clique em **Configurações**.

A janela **Assinaturas do calendário** é exibida.

5. Ative as configurações usando o botão **Assinaturas do calendário**.

6. Clique em **Adicionar**.

A janela **Adicionar assinatura do calendário** é exibida.

7. No campo **Descrição**, insira uma descrição da assinatura do calendário.

8. No campo **Endereço do servidor**, especifique a URL do calendário de terceiros.

Neste campo, é possível inserir a URL principal da conta CalDAV de um usuário cujo calendário está sendo assinado. Você também pode especificar a URL de um calendário iCal ou de um calendário publicado diferente.

9. No campo **Nome de usuário**, insira o nome da conta para a autenticação no servidor de calendário de terceiros.

10. No campo **Senha**, insira a senha da assinatura do calendário para a autenticação no servidor de calendário de terceiros.

11. Se quiser usar o protocolo de transporte de dados SSL (Secure Sockets Layer) para proteger a transmissão de dados de eventos entre o servidor CalDAV e o dispositivo móvel, selecione a caixa **Usar conexão SSL**.

12. Clique em **Adicionar**.

A nova assinatura do calendário aparece na lista.

Você pode modificar ou excluir assinaturas de calendário da lista usando os botões **Editar** e **Excluir** na parte superior da lista.

13. Clique em **OK**.

14. Clique em **Salvar** para salvar as alterações efetuadas.

As configurações do dispositivo móvel são alteradas após a próxima sincronização do dispositivo com o Servidor de MDM do iOS.

Como resultado, depois que a política é aplicada, os eventos do calendário compartilhado na lista são adicionados ao calendário no dispositivo móvel do usuário.

Configurar o SSO

Essas configurações se aplicam aos dispositivos no modo de operação "Perfil de gerenciamento".

As configurações **SSO** permitem definir as configurações para utilizar a tecnologia Single Sign On. *Single Sign-On (SSO)* é um método de autenticação que permite que um usuário faça login em vários serviços com um único ID. O protocolo Kerberos é utilizado para autenticação de usuário.

Para configurar o uso do SSO em dispositivos iOS MDM:

1. Na janela principal do Kaspersky Next Expert View (cloud), selecione **Gerenciamento de ativos** → **Políticas**. Na lista de políticas de grupo aberta, clique no nome da política que deseja configurar.

2. Na janela de propriedades da política, selecione **Configurações do aplicativo**.

3. Selecione **iOS** e vá para a seção **Configuração do dispositivo**.

4. No cartão **SSO**, clique em **Configurações**.

A janela **SSO** é exibida.

5. Ative as configurações usando o botão **SSO**.

6. Especificar as seguintes configurações:

- No campo **Nome da conta**, especifique o nome da conta de login único do usuário para a autorização do servidor Kerberos.
- Na seção **Autenticação**, especifique as seguintes configurações de autenticação:

- **Nome de usuário do Kerberos**

Nome principal da conta de um usuário de dispositivo iOS MDM no servidor Kerberos. O nome de usuário do Kerberos diferencia maiúsculas e minúsculas e deve ser especificado no formato <principal>/<instância>, onde:

1. <principal> é o nome de usuário.

2. <instância> é a descrição do nome principal, por exemplo, "admin". A instância pode ser ignorada.

Exemplo: se o nome de usuário Kerberos for `mycompany/admin@EXAMPLE.COM` ou `mycompany@EXAMPLE.COM`, será necessário inserir `mycompany/admin` ou `mycompany` respectivamente.

Não use o sinal de arroba (@) nesse campo. Caso contrário, o perfil SSO não será aplicado no dispositivo.

- **Escopo do Kerberos**

O nome da rede à qual os servidores Kerberos e os dispositivos móveis iOS MDM pertencem. O escopo deve ser inserido usando letras maiúsculas.

O nome da rede deve coincidir com o nome do domínio. Por exemplo, se os nomes coincidem, o nome do escopo para o domínio `example.com` é `EXAMPLE.COM`.

Exemplo: se o nome de usuário do Kerberos for `mycompany/admin@EXAMPLE.COM`, você deve inserir `EXAMPLE.COM`.

- **Certificado de autenticação**

O certificado usado para autenticação do usuário.

- Na seção **Prefixos de URL**, especifique os endereços de sites nos quais o Kaspersky Mobile Devices Protection and Management permite o uso de SSO:

- **Limitar a conta para as URLs listadas**

Uso do Single Sign-On para o login automático somente em sites adicionados à lista de endereços da Web permitidos. Você pode criar uma lista de endereços da Web permitidos clicando no botão **Adicionar URL** próximo à caixa de seleção.

Se a caixa de seleção estiver marcada, o usuário pode utilizar o Single Sign-On para autorização em sites que foram adicionados à lista de endereços da Web permitidos.

Se a caixa de seleção estiver desmarcada ou a lista estiver em branco, o usuário poderá utilizar o Single Sign-On para todos os sites no **escopo Kerberos**.

O nome da rede à qual os servidores Kerberos e os dispositivos móveis iOS MDM pertencem. O escopo deve ser inserido usando letras maiúsculas.

O nome da rede deve coincidir com o nome do domínio. Por exemplo, se os nomes coincidem, o nome do escopo para o domínio `example.com` é `EXAMPLE.COM`.

Exemplo: se o nome de usuário do Kerberos for `mycompany/admin@EXAMPLE.COM`, você deve inserir `EXAMPLE.COM`.

Essa caixa de seleção é desmarcada por padrão.

- **Adicionar URL**

Clicar no botão adiciona o campo **Prefixo de URL** para especificar um novo site na lista de endereços da Web para os quais o login único automático é permitido.

O botão está disponível se a caixa de seleção **Limitar a conta para as URLs listadas** for marcada.

O endereço da Web deve começar com `http://` ou `https://`. O Login único automático somente é executado quando o URL totalmente coincide com o modelo URL. Por exemplo, o endereço da Web `https://example.com/` não coincide com o endereço da Web `https://example.com:443/`.

Para permitir o acesso com o Single Sign-On usando o protocolo HTTP, insira o valor `http://`. Para permitir o acesso apenas a sites que utilizam o protocolo HTTPS seguro, insira `https://`.

Se o endereço da Web não terminar com o símbolo "/", o Kaspersky Mobile Devices Protection and Management adiciona esse símbolo automaticamente.

Se a lista de endereços da Web permitidos estiver vazia, o usuário pode usar o Single Sign-On para efetuar o login automático todos os sites no **escopo Kerberos**.

O nome da rede à qual os servidores Kerberos e os dispositivos móveis iOS MDM pertencem. O escopo deve ser inserido usando letras maiúsculas.

O nome da rede deve coincidir com o nome do domínio. Por exemplo, se os nomes coincidem, o nome do escopo para o domínio `example.com` é `EXAMPLE.COM`.

Exemplo: se o nome de usuário do Kerberos for `mycompany/admin@EXAMPLE.COM`, você deve inserir `EXAMPLE.COM`.

- Na seção **IDs dos pacotes**, especifique os IDs de aplicativos nos quais o Kaspersky Mobile Devices Protection and Management permite o uso de SSO:

- **Limitar a conta aos aplicativos listados**

Usar o Single Sign-On para login automático em aplicativos adicionados à lista de identificadores de pacote. Você pode criar uma lista de IDs de pacotes clicando no botão **Adicionar aplicativo** ao lado da caixa de seleção.

Se a caixa de seleção estiver marcada, o usuário pode utilizar o Single Sign-On para acessar aplicativos que foram adicionados à lista de IDs de pacotes.

Se a caixa de seleção estiver desmarcada ou a lista estiver em branco, o usuário poderá usar o Single Sign-On para acessar todos os aplicativos no **escopo Kerberos**.

O nome da rede à qual os servidores Kerberos e os dispositivos móveis iOS MDM pertencem. O escopo deve ser inserido usando letras maiúsculas.

O nome da rede deve coincidir com o nome do domínio. Por exemplo, se os nomes coincidem, o nome do escopo para o domínio `example.com` é `EXAMPLE.COM`.

Exemplo: se o nome de usuário do Kerberos for `mycompany/admin@EXAMPLE.COM`, você deve inserir `EXAMPLE.COM`.

Essa caixa de seleção é desmarcada por padrão.

- **Adicionar aplicativo**

Clicar no botão adiciona o campo **ID do pacote** para especificar um novo ID do pacote na lista de aplicativos para os quais o login único automático é permitido.

O botão está disponível se a caixa de seleção **Limitar a conta aos aplicativos listados** for marcada.

O login único automático é executado somente quando a ID adicionada coincide totalmente com o ID do pacote. Por exemplo: `com.mycompany.myapp`.

Para conceder acesso a diversos aplicativos utilizando o Login único, utilize o símbolo "*" após o caractere ".". Por exemplo: `com.mycompany.*`. O acesso será permitido para todos os aplicativos cujo ID de pacote comece com o prefixo especificado.

Se a lista de IDs do pacote estiver vazia, o usuário pode usar o Single Sign-On para efetuar o login automático em todos os aplicativos no **escopo Kerberos**.

O nome da rede à qual os servidores Kerberos e os dispositivos móveis iOS MDM pertencem. O escopo deve ser inserido usando letras maiúsculas.

O nome da rede deve coincidir com o nome do domínio. Por exemplo, se os nomes coincidem, o nome do escopo para o domínio `example.com` é `EXAMPLE.COM`.

Exemplo: se o nome de usuário do Kerberos for `mycompany/admin@EXAMPLE.COM`, você deve inserir `EXAMPLE.COM`.

7. Clique em **OK**.

8. Clique em **Salvar** para salvar as alterações efetuadas.

As configurações do dispositivo móvel são alteradas após a próxima sincronização do dispositivo com o Servidor de MDM do iOS.

Como resultado, depois que a política é aplicada, o SSO é configurado no dispositivo iOS MDM.

Gerenciar 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 do Clipe da Web na tela inicial do dispositivo, o usuário pode rapidamente abrir sites (como o site corporativo).

Você pode adicionar ou excluir os Clipes da Web em dispositivos de usuário e especificar os ícones exibidos na tela.

Gerenciar Clipes da Web em dispositivos iOS MDM

Por padrão, as seguintes restrições se aplicam aos Clipes da Web:

- O usuário não pode remover manualmente os Clipes da Web do dispositivo móvel.
- Os efeitos visuais de canto arredondado, sombra e brilho são aplicados ao ícone do Clipe da Web na tela.
- Os sites que são exibidos quando o usuário toca em um ícone de um Clipe da Web não são exibidos no modo de tela completa.

Para gerenciar um Clipe da Web no dispositivo iOS MDM de um usuário:

1. Na janela principal do Kaspersky Next Expert View (cloud), selecione **Gerenciamento de ativos** → **Políticas**. Na lista de políticas de grupo aberta, clique no nome da política que deseja configurar.
2. Na janela de propriedades da política, selecione **Configurações do aplicativo**.
3. Selecione **iOS** e vá para a seção **Configuração do dispositivo**.
4. No cartão **Web Clips**, clique em **Configurações**.

A janela **Web Clips** é exibida.

5. Ative as configurações usando o botão **Web Clips**.

6. Clique em **Adicionar**.

A janela **Adicionar Web Clip** é exibida.

7. No campo **Nome do Web Clip**, insira o nome do Clipe da Web a ser exibido na tela inicial do dispositivo iOS MDM.

8. No campo **URL do site**, insira o endereço da Web do site que será exibido ao tocar no ícone do Clipe da Web. O endereço deve começar com `http://` ou `https://`.

Use somente fontes legítimas e confiáveis. Ao definir as configurações nesse campo, você é o único responsável por todos os riscos e as consequências associados ao uso de fontes não confiáveis.

Se o site inserido for proibido ou não estiver na lista de sites permitidos nas configurações do **Controle da Web** da política, os usuários não poderão acessar esse site através do Clipe da Web.

9. Clique em **Selecionar** para especificar a imagem para o ícone do Clipe da Web.

A imagem deve atender os seguintes requisitos:

- Tamanho de imagem não superior a 400 x 400 pixels.
- Formato do arquivo: PNG, JPEG ou ICO.
- Tamanho do arquivo não superior a 1 MB.

Se você não selecionar uma imagem para o Clipe da Web, um quadrado branco é exibido como o ícone.

Se a imagem selecionada tiver um fundo transparente, o fundo será preto no dispositivo.

10. Na seção **Opções**, especifique as seguintes configurações adicionais:

- a. Se você quiser permitir que o usuário remova o Clipe da Web do dispositivo iOS MDM, marque a caixa de seleção **Permitir a remoção do Web Clip**.
- b. Se você quiser 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 predefinido**.
- c. Se você quiser que o site seja exibido no modo de tela cheia no dispositivo iOS MDM quando o usuário toca no ícone, marque a caixa de seleção **Web Clip em tela cheia**.

No modo de tela cheia, a barra de ferramentas do Safari fica oculta e somente o site é exibido na tela do dispositivo.

11. Clique em **Adicionar**.

O novo Clipe da Web é exibido na lista.

Você pode modificar ou excluir Clipes da Web da lista usando os botões **Editar** e **Excluir** na parte superior da lista.

12. Clique em **OK**.

13. Clique em **Salvar** para salvar as alterações efetuadas.

Após a aplicação da política, os ícones do Clipe da Web na lista que você criou são adicionados à tela inicial do dispositivo móvel do usuário.

Os Web Clips excluídos são removidos da tela inicial do dispositivo iOS MDM.

Adicionar fontes

Essas configurações se aplicam aos dispositivos no modo de operação "Perfil de gerenciamento".

Para adicionar uma fonte ao dispositivo iOS MDM de um usuário:

1. Na janela principal do Kaspersky Next Expert View (cloud), selecione **Gerenciamento de ativos** → **Políticas**. Na lista de políticas de grupo aberta, clique no nome da política que deseja configurar.
2. Na janela de propriedades da política, selecione **Configurações do aplicativo**.
3. Selecione **iOS** e vá para a seção **Configuração do dispositivo**.
4. No cartão **Fontes personalizadas**, clique em **Configurações**.
A janela **Fontes personalizadas** é exibida.
5. Ative as configurações usando o botão **Fontes personalizadas**.
6. Clique em **Adicionar**.
7. Selecione o arquivo de fonte salvo em seu computador. O arquivo deve ter a extensão .TTF ou .OTF.

Fontes com a extensão .TTC ou .OTC não são compatíveis.

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.

8. Clique em **Abrir**.

A nova fonte é exibida na lista.

Você pode excluir fontes na lista usando o botão **Excluir** na parte superior da lista.

9. Clique em **OK**.

10. Clique em **Salvar** para salvar as alterações efetuadas.

As configurações do dispositivo móvel são alteradas após a próxima sincronização do dispositivo com o Servidor de MDM do iOS.

Como resultado, depois que a política é aplicada, será solicitado ao usuário que instale as fontes da lista criada.

Trabalhar com comandos para dispositivos móveis

Esta seção contém informações sobre os comandos para o gerenciamento de dispositivos móveis compatíveis com o Kaspersky Security Center. Ela fornece instruções sobre como enviar comandos para dispositivos móveis, assim como visualizar o status de execução de comandos no histórico de comandos.

Comandos para dispositivos móveis

O Kaspersky Security Center é compatível com comandos para o gerenciamento remoto de dispositivos móveis. Por exemplo, caso um dispositivo móvel seja perdido ou roubado, é possível enviar comandos para localizá-lo ou limpar todos os seus corporativos.

É possível enviar comandos para os seguintes tipos de dispositivos móveis gerenciados:

- Dispositivos Android gerenciados pelo aplicativo Kaspersky Endpoint Security for Android
- Dispositivos iOS MDM

Cada tipo de dispositivo é compatível com um conjunto dedicado de comandos.

Você pode cancelar comandos no [Histórico de comandos](#).

Os comandos podem ser entregues quase imediatamente aos dispositivos conectados à Internet. Como resultado, eles podem falhar ao cancelar apesar de serem exibidos como cancelados.

Comandos para dispositivos Android

Comando	Resultado
Bloquear dispositivo	O dispositivo móvel é bloqueado. Para obter acesso aos dados, você deve desbloquear o dispositivo usando o comando Desbloquear dispositivo ou um código de uso único.
Desbloquear dispositivo	O dispositivo móvel está desbloqueado. Depois de desbloquear um dispositivo executando o Android 5 – 6, a senha de desbloqueio da tela é redefinida para "1234". Após desbloquear um dispositivo com Android 7 ou posterior, a senha de desbloqueio da tela não é alterada.

Comando	Resultado
Redefinir as configurações padrão	Todos os dados são excluídos do dispositivo móvel e as suas configurações são redefinidas para seus valores de fábrica. Após este comando ter sido executado, o dispositivo não será capaz de receber ou executar comandos subsequentes. Esse comando não está disponível para dispositivos pessoais e dispositivos com contêiner corporativo executando o Android 14 ou posterior.
Limpar os dados corporativos	Dados corporativos são limpos no dispositivo. A lista de dados apagados depende do modo em que o dispositivo está operando: - Em um dispositivo pessoal, o contêiner Knox, os arquivos corporativos enviados ao dispositivo e o certificado de e-mail são apagados. - Além disso, se um contêiner corporativo foi criado, o contêiner corporativo (seu conteúdo, arquivos corporativos enviados ao dispositivo, configurações e restrições) e os certificados instalados no contêiner corporativo (certificados de perfil de e-mail, VPN e SCEP, exceto os certificados de dispositivos móveis) são apagados.
Sincronizar o dispositivo	Os dados dos dispositivo móvel são sincronizados com o Servidor de Administração. O status <i>Executado</i> pode ser exibido quando o comando foi enviado com êxito, mas ainda não foi recebido pelo dispositivo.
Localizar o dispositivo	As coordenadas de localização do dispositivo móvel são obtidas. Para visualizar a localização do dispositivo no Yandex.Maps, vá para a seção Gerenciamento de ativos → Móvel → Dispositivos. Em seguida, escolha um dispositivo e selecione Histórico de comandos → Localizar o dispositivo → Coordenadas do dispositivo → Visualização no mapa. Depois de clicar em Visualização no mapa, as coordenadas do dispositivo são transferidas para o Yandex.Maps e o dispositivo é exibido em um mapa. 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 nos últimos 30 minutos. Caso contrário, o comando falhará. Esse comando não funciona em dispositivos Android se a opção Precisão de localização do Google estiver desativada nas configurações. Observe que nem todos os dispositivos Android vêm com essa configuração de localização.
Alarme sonoro	O dispositivo móvel emite um alarme sonoro por 5 minutos (por 1 minuto se a bateria do dispositivo estiver fraca) ou até que o usuário desbloqueie o dispositivo.

Comandos para dispositivos iOS MDM

Comando	Resultado
Bloquear dispositivo	O dispositivo móvel é bloqueado. Para acessar os dados, é necessário desbloquear o dispositivo.
Redefinir a senha de desbloqueio	A senha de desbloqueio de tela do dispositivo móvel é redefinida, e o usuário recebe uma solicitação para definir uma nova senha de acordo com os requisitos da política.
Redefinir as configurações padrão	Todos os dados são excluídos do dispositivo móvel e as suas configurações são redefinidas para seus valores de fábrica. Após este comando ter sido executado, o dispositivo não será capaz de receber ou executar comandos subsequentes.
Limpar os dados corporativos	Todos os perfis de configuração instalados, o perfil de gerenciamento e os aplicativos para os quais a caixa de seleção Remover quando o perfil de gerenciamento for excluído estiver marcada serão removidos do dispositivo.
Sincronizar o dispositivo	Os dados dos dispositivo móvel são sincronizados com o Servidor de Administração.

Comando	Resultado
Instalar o perfil de configuração	Um perfil de configuração é instalado no dispositivo móvel. Você não pode instalar um perfil de configuração com configurações para um dispositivo supervisionado em um dispositivo no modo de controle básico.
Excluir perfil de configuração	O perfil de configuração é excluído do dispositivo móvel. O perfil pode ser exibido na lista de perfis de configuração instalados no dispositivo por vários minutos após ter sido excluído.
Instalar o aplicativo	O aplicativo especificado é instalado no dispositivo móvel.
Atualizar o aplicativo	O aplicativo especificado é atualizado no dispositivo móvel.
Excluir aplicativo	O aplicativo especificado é removido do dispositivo móvel.
Alterar configurações de roaming	O roaming de dados e o roaming de voz podem ser ativados ou desativados.

Permissões para execução de comandos

São necessários direitos e permissões especiais para executar 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 essa etapa ou desativar esse serviço posteriormente nas configurações do dispositivo. Se este for o caso, será impossível executar os comandos.

Em dispositivos executando Android 10 ou posterior o usuário deve conceder permissão "Permitir o tempo todo" para acessar a localização. Em dispositivos executando Android 11 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. Recomendamos contatar o usuário diretamente, caso a permissão da câmera seja solicitada novamente.

Enviar comandos

Para enviar um comando para o dispositivo móvel do usuário:

1. Na janela principal do Kaspersky Next Expert View (cloud), selecione **Gerenciamento de ativos** → **Móvel** → **Dispositivos**.
2. Na lista de dispositivos exibida, selecione um dispositivo para o qual você deseja enviar um comando.

É possível selecionar vários dispositivos.

3. Clique em **Enviar comando**.
4. Na janela **Enviar comando** exibida, no campo **Comando**, selecione um comando.

5. Especifique os comandos que você quer enviar.

6. Clique em **Enviar**.

Você pode visualizar e cancelar comandos no **Histórico de comandos**.

O comando é enviado aos dispositivos selecionados.

Visualizar status de comandos no histórico de comandos

O aplicativo salva informações sobre todos os comandos que foram enviados para dispositivos móveis no histórico de comandos. O histórico de comandos contém informações sobre a hora e a data em que cada comando foi enviado para o dispositivo móvel, seus respectivos status e descrições dos resultados. Por exemplo, quando um comando falha, o histórico exibe a causa do erro.

Os comandos enviados para dispositivos móveis podem ter os seguintes status:

- *Enviado*

O comando foi enviado para o dispositivo móvel.

- *Executado*

A execução do comando foi bem-sucedida.

- *Erro*

A execução do comando falhou.

- *Cancelando*

O comando está sendo removido da fila de comandos enviados para o dispositivo móvel.

- *Cancelado*

O comando foi removido com êxito da fila de comandos enviados para o dispositivo móvel.

O aplicativo mantém um histórico de comandos para cada dispositivo móvel.

Para visualizar o histórico de comandos:

1. Na janela principal do Kaspersky Next Expert View (cloud), selecione **Gerenciamento de ativos** → **Móvel** → **Dispositivos**.

2. Na lista de dispositivos móveis, selecione o dispositivo para o qual você deseja visualizar o histórico de comandos.

3. Clique em **Histórico de comandos**.

A janela **Histórico de comandos** é exibida. As seções da janela **Histórico de comandos** correspondem aos comandos que podem ser enviados para o dispositivo móvel.

4. Selecione as seções que contêm os comandos necessários e visualize as informações sobre como os comandos são enviados e executados.

Participar na Kaspersky Security Network

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

A *Kaspersky Security Network (KSN)* é uma infraestrutura de serviços na nuvem que fornece o acesso à base de dados de conhecimento 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 coletar informações em tempo real sobre os tipos e origens de novas ameaças, desenvolver métodos de neutralização delas e reduzir o número de alarmes falsos do Kaspersky Endpoint Security for Android e do Kaspersky Protection for iOS. 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 e o Kaspersky Protection for iOS estiverem em execução e [são automaticamente enviadas à Kaspersky](#). Estas informações permitem manter o acompanhamento das ameaças em tempo real. Os arquivos ou partes de arquivos que podem ser explorados por invasores para danificar o computador ou o conteúdo do usuário também podem ser enviados à Kaspersky para exame complementar.

O uso da Kaspersky Security Network é necessário para a operação do Kaspersky Endpoint Security for Android e do Kaspersky Protection for iOS.

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

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

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 de Usuário Final ao instalar o aplicativo. O Contrato de Licença de Usuário Final define quais dados são transmitidos à Kaspersky Security Network pelo Kaspersky Endpoint Security for Android e pelo Kaspersky Protection for iOS.

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 e o Kaspersky Protection for iOS transmitem para a Kaspersky Security Network. Você pode usar os serviços da Kaspersky Security Network se o período de licença da solução integrada não tiver expirado e a chave não tiver sido excluída da lista de proibições.

A funcionalidade de atualizações (incluindo o fornecimento de atualizações de assinaturas de antimalware e atualizações de base de código), bem como a funcionalidade KSN, podem não estar disponíveis no software nos EUA.

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 os seguintes componentes:

- **[Antimalware](#)**. O aplicativo obtém o acesso à Base de Conhecimento da Kaspersky quanto à reputação de arquivos e aplicativos. O aplicativo verifica ameaças cujas informações ainda não foram adicionadas aos bancos de dados antimalware, mas já estão disponíveis na KSN. O serviço em nuvem da Kaspersky Security Network facilita a funcionalidade completa do Antimalware e reduz a probabilidade de alarmes falsos.
- **[Proteção na Web](#) e [Controle da 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 que restringe a inicialização de aplicativos que não atendam os requisitos de segurança corporativos de acordo com as listas de categorias permitidas e bloqueadas (por exemplo, a categoria "Jogos").

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

As informações sobre os tipos de dados enviados à Kaspersky, ao usar a KSN durante a operação da Proteção na Web e do Controle da 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 a seção [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 Protection for iOS

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

- **Proteção na Web.** O aplicativo usa os dados recebidos da KSN para executar uma verificação de sites antes que eles sejam abertos.

As informações sobre os tipos de dados enviados à Kaspersky ao usar a KSN durante a operação da Proteção na Web estão disponíveis no Contrato de Licença de 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 a seção [Fornecimento de dados no Kaspersky Protection 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 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 aprimorar 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 ou do Kaspersky Protection for iOS.
- 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 os tipos de dados estatísticos enviados à Kaspersky ao usar a KSN durante a operação dos aplicativos móveis estão disponíveis na Declaração da Kaspersky Security Network.

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 e do Kaspersky Protection for iOS que usam a Kaspersky Security Network](#), o aplicativo envia solicitações aos serviços na nuvem. As solicitações contêm os dados descritos nas seções [Fornecimento de dados no Kaspersky Endpoint Security for Android](#) e [Fornecimento de dados no Kaspersky Protection for iOS](#), respectivamente.

Se o uso da Kaspersky Security Network estiver desativado no dispositivo, os recursos do Antimalware, da Proteção na Web, do Controle da Web e do Controle de aplicativos serão desativados automaticamente.

Para ativar ou desativar o uso da Kaspersky Security Network em dispositivos Android:

1. Na janela principal do Kaspersky Next Expert View (cloud), selecione **Gerenciamento de ativos** → **Políticas**. Na lista de políticas de grupo aberta, clique no nome da política que deseja configurar.
2. Na janela de propriedades da política, selecione **Configurações do aplicativo**.
3. Selecione **Android** e vá até a seção **Configurações do KES for Android**.
4. No cartão da **Kaspersky Security Network**, clique em **Configurações**.
A janela **Kaspersky Security Network** é exibida.
5. Ative o botão da **Kaspersky Security Network** para os seguintes componentes: Antimalware, Proteção na Web, Controle da Web e Controle de aplicativos.
6. Clique em **OK**.
7. No cartão **Enviando dados adicionais**, clique em **Configurações**.
8. Na seção **Envio de dados para a Kaspersky Security Network**, marque a caixa de seleção **Permitir o envio de estatísticas para a Kaspersky Security Network** 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.
9. Na seção **Envio de dados para fins de marketing**, marque a caixa de seleção **Permitir o processamento de dados para ajudar a melhorar a qualidade, a aparência e o desempenho do aplicativo** para melhorar a qualidade, a aparência e o desempenho de softwares, produtos, serviços e infraestrutura do titular dos direitos ao analisar a experiência dos usuários, os recursos que eles usam e o status e as configurações do dispositivo.
10. Selecione quem deve aceitar as declarações:
 - Se você selecionar **As Declarações foram aceitas pelo administrador**, será solicitado que você aceite as declarações na janela exibida.
 - Se você selecionar **As Declarações foram aceitas pelos usuários**, o usuário do dispositivo será solicitado a aceitar as declarações.
11. Clique em **OK**.
12. Clique em **Salvar** para salvar as alterações efetuadas.

As configurações do dispositivo móvel são alteradas após a próxima sincronização do dispositivo com o Kaspersky Security Center.

Para ativar ou desativar o uso da Kaspersky Security Network para dispositivos iOS:

1. Na janela principal do Kaspersky Next Expert View (cloud), selecione **Gerenciamento de ativos** → **Políticas**. Na lista de políticas de grupo aberta, clique no nome da política que deseja configurar.
2. Na janela de propriedades da política, selecione **Configurações do aplicativo**.
3. Selecione **iOS** e vá para a seção **KP para as configurações do iOS**.
4. Ative o botão no cartão da **Kaspersky Security Network** para o componente Proteção na Web.

5. No cartão **Enviando dados adicionais**, clique em **Configurações**.

6. Na seção **Envio de dados para a Kaspersky Security Network**, marque a caixa de seleção **Permitir o envio de estatísticas para a Kaspersky Security Network** para enviar dados à Kaspersky.

Estes dados ajudarão o aplicativo Kaspersky Protection for iOS a responder mais rapidamente às ameaças, aprimorar o desempenho dos componentes de proteção e diminuir a probabilidade de falsos alarmes.

7. Selecione quem deve aceitar as declarações:

- Se você selecionar **As Declarações foram aceitas pelo administrador**, será solicitado que você aceite as declarações na janela exibida.
- Se você selecionar **As Declarações foram aceitas pelos usuários**, o usuário do dispositivo será solicitado a aceitar as declarações.

8. Clique em **OK**.

9. Clique em **Salvar** para salvar as alterações efetuadas.

As configurações do dispositivo móvel são alteradas após a próxima sincronização do dispositivo com o Kaspersky Security Center.

Samsung Knox

O *Samsung Knox* é uma solução móvel para configurar e implementar 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](#) .

Configurar o Knox

Esta seção contém informações sobre o trabalho com o Knox em dispositivos da Samsung.

O Knox está somente disponível em dispositivos Samsung que executam o Android 6 ou posterior.

Configurar VPN no Knox

Para conectar um dispositivo Android à Internet de forma segura e proteger a transferência de dados, você pode definir as configurações da VPN (Rede Virtual Privada).

A configuração da VPN é possível apenas para os dispositivos Samsung que executam a versão 11 ou anterior do Android.

Os seguintes requisitos devem ser considerados ao usar uma rede privada virtual:

- O aplicativo que usa a conexão VPN deve ser permitido nas configurações do [Firewall](#).
- As configurações da VPN 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. Na janela principal do Kaspersky Next Expert View (cloud), selecione **Gerenciamento de ativos** → **Políticas**. Na lista de políticas de grupo aberta, clique no nome da política que deseja configurar.

2. Na janela de propriedades da política, selecione **Configurações do aplicativo**.

3. Selecione **Android** e vá para a seção **Configurações do Samsung Knox**.

4. No cartão **VPN**, clique em **Configurações**.

A janela **VPN** se abre.

5. Ative as configurações usando o botão **VPN**.

6. Especificar as seguintes configurações da VPN:

- Configurações na seção **Rede**:
 - No campo **Nome da rede**, insira o nome do túnel VPN.
 - Na lista suspensa **Protocolo**, selecione o tipo de conexão VPN:
 - **IPSec Xauth PSK**. Um protocolo de túnel do tipo "gateway-to-gateway" que permite ao usuário do dispositivo móvel estabelecer uma conexão segura com o servidor VPN utilizando o utilitário de autenticação Xauth.
 - **L2TP IPSec PSK**. Um protocolo de túnel do tipo "gateway-to-gateway" que permite ao usuário do dispositivo móvel estabelecer uma conexão segura com o servidor VPN por meio do protocolo IKE utilizando uma chave predefinida. Esse protocolo é marcado por padrão.
 - **PPTP**. Um protocolo de túnel "point-to-point" que permite ao usuário do dispositivo móvel estabelecer uma conexão segura com o servidor VPN criando um túnel especial em uma rede padrão desprotegida.
 - No campo **Endereço do servidor**, insira o nome de rede ou endereço IP do servidor da VPN.
- Configurações na seção **Configurações do protocolo**:
 - Na lista **Domínio(s) de procura 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.
 - No campo **Servidor(es) 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.

- 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.

7. Ainda, defina as seguintes configurações:

- Para os protocolos **IPSec Xauth PSK** e **L2TP IPSec PSK**:
 - No campo **Chave compartilhada IPSec**, insira a senha para a chave de segurança IPSec predefinida.
 - No campo **ID IPSec**, insira o nome do usuário do dispositivo móvel.
- Para o protocolo **L2TP IPSec PSK**, especifique a senha para a chave L2TP que no campo **Chave L2TP**.
- Para a rede **PPTP**, selecione a caixa de seleção **Usar 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.

8. Clique em **Salvar** para salvar as alterações efetuadas.

As configurações do dispositivo móvel são alteradas após a próxima sincronização do dispositivo com o Kaspersky Security Center.

Configurar uma caixa de e-mail do Exchange no Knox

Para trabalhar com e-mail corporativo, contatos e o calendário no dispositivo móvel, você pode definir as configurações de caixa de e-mail do Exchange para o aplicativo padrão Samsung Email.

Uma caixa de e-mail do Exchange pode ser configurada apenas em dispositivos Samsung que executam Android 9 ou versões anteriores.

Para configurar uma caixa de e-mail do Exchange no dispositivo móvel de um usuário:

1. Na janela principal do Kaspersky Next Expert View (cloud), selecione **Gerenciamento de ativos** → **Políticas**. Na lista de políticas de grupo aberta, clique no nome da política que deseja configurar.
2. Na janela de propriedades da política, selecione **Configurações do aplicativo**.
3. Selecione **Android** e vá para a seção **Configurações do Samsung Knox**.
4. No cartão **Exchange ActiveSync**, clique em **Configurações**.
A janela **Exchange ActiveSync** é exibida.
5. Ative as configurações usando o botão **Exchange ActiveSync**.
6. No campo **Endereço do servidor**, insira o endereço IP ou nome DNS do servidor que hospeda o servidor de e-mail.
7. No campo **Nome do domínio**, insira o nome do domínio do usuário do dispositivo móvel na rede corporativa.

8. Na lista suspensa **Intervalo de sincronização**, selecione o intervalo de sincronização de dispositivos móveis com o servidor do Microsoft Exchange.
9. Para usar o protocolo de transporte de dados SSL (Secure Sockets Layer), selecione a caixa de seleção **Usar conexão SSL**. O protocolo SSL usa criptografia e autenticação baseada em certificado para a transferência segura de dados. Essa caixa de seleção é marcada por padrão.
10. Para usar certificados digitais para proteger a transferência de dados entre o dispositivo móvel do usuário e o servidor Microsoft Exchange, selecione a caixa de seleção **Verificar o certificado do servidor**. É feita a verificação da emissão do certificado do servidor a partir do certificado raiz confiável. Essa caixa de seleção é marcada por padrão.
11. Clique em **Salvar** para salvar as alterações efetuadas.

As configurações do dispositivo móvel são alteradas após a próxima sincronização do dispositivo com o Kaspersky Security Center.

Configurar APN no Knox

O APN pode ser configurado somente para 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 móvel. Configurações de ponto de acesso incorretas podem resultar em cobranças adicionais.

Para definir as configurações do Nome do ponto de acesso (APN) no dispositivo móvel de um usuário:

1. Na janela principal do Kaspersky Next Expert View (cloud), selecione **Gerenciamento de ativos** → **Políticas**. Na lista de políticas de grupo aberta, clique no nome da política que deseja configurar.
2. Na janela de propriedades da política, selecione **Configurações do aplicativo**.
3. Selecione **Android** e vá para a seção **Configurações do Samsung Knox**.
4. No cartão **Configurações de APN**, clique em **Configurações**.
A janela **Configurações de APN** é exibida.
5. Ative as configurações usando o botão **Configurações de APN**.

O botão neste cartão não ativa nem desativa a funcionalidade correspondente nos dispositivos. Ativar o botão permite definir configurações personalizadas. Desativar o botão permite usar as configurações padrão.

6. Especifique as seguintes configurações de ponto de acesso para conectar o usuário ao serviço de dados:

- Na lista suspensa **Tipo de APN**, selecione o tipo de ponto de acesso (APN) para transmissão de dados em uma rede móvel GPRS/3G/4G:
 - **Internet**. Conexão do dispositivo móvel do usuário à Internet.
 - **MMS**. Troca de mensagens multimídia MMS.
 - **Internet e MMS**. Conexão à Internet e troca de mensagens multimídia. Esse é o valor padrão.
- No campo **Nome de APN**, especifique o nome do ponto de acesso.
- No campo **MCC**, insira o código de país da rede celular (MCC).
- No campo **MNC**, insira o código de rede celular (MNC).

7. Caso você tenha selecionado **MMS** ou **Internet e MMS** como tipo de ponto de acesso, especifique as configurações MMS adicionais na seção **Servidor MMS**:

- No campo **Nome do servidor MMS**, especifique o nome completo do domínio do servidor do operador de telefonia móvel usado para troca de MMS (por exemplo, `mms.mobile.com`).
- No campo **Endereço do servidor proxy MMS**, insira o nome de rede ou endereço IP do servidor proxy.
- No campo **Porta do servidor proxy MMS**, especifique o número da porta do servidor do operador de telefonia usado para troca de MMS.

8. Na seção **Autenticação**, especifique as seguintes configurações de autenticação:

- Na lista suspensa **Tipo de autenticação**, selecione o tipo de autenticação do usuário do dispositivo móvel que será utilizado no servidor do operador de telefonia móvel para acesso à rede. Por padrão, a autenticação de usuário não é necessária. Os seguintes tipos estão disponíveis:
 - **Nenhum**. A autenticação não é necessária para acessar a rede móvel.
 - **PAP** (Protocolo de Autenticação de Senha). Um protocolo de autenticação que usa senhas como texto simples não criptografado.
 - **CHAP** (Protocolo de Autenticação por Desafio Handshake). Um protocolo de autenticação de solicitação-resposta que usa hash MD5 padrão para criptografar a resposta.
 - **Simultaneamente**. Uso combinado dos protocolos CHAP e PAP.
- No campo **Nome de usuário**, insira o nome de usuário para autorização na rede móvel.
- No campo **Senha**, insira a senha para autorização do usuário na rede móvel.

9. Na seção **Rede**, especifique as seguintes configurações de rede:

- No campo **Nome da rede**, insira o nome da rede.
- 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.

10. Na seção **Servidor proxy**, especifique as seguintes configurações de servidor proxy:

- Marque a caixa de seleção **Usar um servidor proxy** para ativar o uso de um servidor proxy. Essa caixa de seleção é desmarcada por padrão.
- No campo **Endereço do servidor proxy**, especifique o nome de rede ou endereço IP do servidor proxy do operador para acesso de rede. Este campo está disponível somente se a caixa de seleção **Usar um servidor proxy** estiver marcada.
- No campo **Porta do servidor proxy**, especifique o número da porta do servidor proxy do operador para acesso de rede. Este campo está disponível somente se a caixa de seleção **Usar um servidor proxy** estiver marcada.

11. Clique em **OK**.

12. Clique em **Salvar** para salvar as alterações efetuadas.

As configurações do dispositivo móvel são alteradas após a próxima sincronização do dispositivo com o Kaspersky Security Center.

Configurar Firewall no Knox

Especifique as configurações do Firewall para monitorar conexões de rede no dispositivo móvel do usuário.

O Firewall pode ser configurado apenas em dispositivos Samsung que executam Android 15 ou versões anteriores.

Para configurar o Firewall em um dispositivo móvel de um usuário:

1. Na janela principal do Kaspersky Next Expert View (cloud), selecione **Gerenciamento de ativos** → **Políticas**. Na lista de políticas de grupo aberta, clique no nome da política que deseja configurar.
2. Na janela de propriedades da política, selecione **Configurações do aplicativo**.
3. Selecione **Android** e vá para a seção **Configurações do Samsung Knox**.
4. Na placa **Firewall**, clique em **Configurações**.
A janela **Firewall** é exibida.
5. Ative as configurações usando o botão **Firewall**.
6. Na lista suspensa **Acesso à Internet**, selecione o modo do Firewall. Dependendo do modo de operação, o Firewall monitora conexões estabelecidas pelo dispositivo móvel do usuário:
 - Se você quiser permitir conexões de entrada e saída de todos os aplicativos instalados, selecione **Permitir para todos os aplicativos**. Este modo é selecionado por padrão.
 - Se você quiser bloquear todas as atividades de rede, exceto para vários aplicativos específicos, selecione **Permitir para aplicativos listados**.
7. Se você selecionou **Permitir para aplicativos listados** como o modo Firewall, crie uma lista de aplicativos para os quais todas as atividades de rede são permitidas:
 - a. Na seção **Aplicativos com acesso à Internet**, clique em **Adicionar**.
A janela **Adicionar aplicativo** é exibida.

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 **Adicionar**.

O novo aplicativo para o qual o Firewall está desativado aparece na lista.

Você pode modificar ou excluir aplicativos de dispositivos móveis da lista usando os botões **Editar** e **Excluir** na parte superior da lista.

8. Clique em **OK**.

9. Clique em **Salvar** para salvar as alterações efetuadas.

As configurações do dispositivo móvel são alteradas após a próxima sincronização do dispositivo com o Kaspersky Security Center.

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 Antimalware para proteger o dispositivo contra vírus e outro malware.

O Antimalware 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
- Atualizações do bancos de dados antimalware

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.

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 ou posterior.

- Ative um alarme alto no dispositivo mesmo se o som do dispositivo estiver desativado.
- Adquira as coordenadas da localização do dispositivo.
- Limpe os dados armazenados no dispositivo.
- Redefinir as configurações padrão.
- 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 usando a notificação apropriada ou nas configurações do 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. [Saiba mais.](#)

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, proibidos e necessários. O componente Controle de aplicativos é usado para instalar aplicativos recomendados e requeridos, atualizá-los e remover os aplicativos proibidos.

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 proibidos 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 aplicativos. Se você não ativou este serviço durante o Assistente de Configuração Inicial para o aplicativo, poderá ativar o Kaspersky Endpoint Security como um serviço de Recursos de Acessibilidade usando a notificação apropriada ou nas configurações do dispositivo (**Configurações Android** → **Acessibilidade** → **Serviços**).

Controle de conformidade

O componente Controle de conformidade verifica automaticamente se o dispositivo está em conformidade com os requisitos de segurança corporativa. Se o dispositivo não atender os requisitos de segurança corporativa, o aplicativo mostrará uma notificação com as seguintes informações:

- Motivo da não conformidade (por exemplo, aplicativos proibidos foram detectados no dispositivo ou os bancos de dados antimalware estão desatualizados).
- 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.

Introdução à janela principal

A exibição da janela principal é ligeiramente diferente em diferentes resoluções de tela.

A janela principal exibe o status geral de proteção do dispositivo. Esse status determina a cor da janela:

- Verde indica que a proteção do dispositivo está em um nível ideal.
- Vermelho indica problemas críticos com a segurança do dispositivo.

Na janela principal do aplicativo, você também pode fazer o seguinte:

- Visualizar notificações clicando no botão no canto superior direito. Elas informam sobre problemas de segurança, problemas na operação do aplicativo, conformidade com os requisitos de segurança corporativa e a sua licença.
- Navegue entre a janela principal e as configurações do aplicativo usando os botões na parte inferior.

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 antimalware estão desatualizados ou um aplicativo recém-instalado não foi verificado).

Verificação do dispositivo

O antimalware tem um número de limitações:

- Quando o Antimalware executa, uma ameaça detectada na memória externa do dispositivo (tal como um cartão SD) não pode ser neutralizada automaticamente no [contêiner corporativo](#). O Kaspersky Endpoint Security for Android não tem acesso à memória externa no contêiner corporativo. As informações sobre os objetos detectados são exibidas em notificações 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 a 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 esses arquivos sem notificar que eles foram ignorados.
- Em dispositivos executando Android 11 ou posterior, o aplicativo Kaspersky Endpoint Security for Android não pode verificar as pastas "Android/data" e "Android/obb" para detectar malware [devido a limitações técnicas](#).

Para iniciar uma verificação do dispositivo:

1. Na janela principal do Kaspersky Endpoint Security, toque em **Configurações** → **Configurações do aplicativo** → **Antimalware** → **Iniciar a verificação**.

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 malware pode ser restringido pelo administrador.

Para configurar a verificação de malware:

1. Na janela principal do Kaspersky Endpoint Security, toque em **Configurações** → **Configurações do aplicativo** → **Antimalware** → **Configurações de verificação**.

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. Toque 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. Ela permite excluir ou restaurar os arquivos que foram movidos para o armazenamento isolado dedicado.

- **Perguntar ao usuário**

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. 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 no 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 Antimalware.

Executar uma verificação programada

O antimalware tem um número de limitações:

- Quando o Antimalware executa, uma ameaça detectada na memória externa do dispositivo (tal como um cartão SD) não pode ser neutralizada automaticamente no [contêiner corporativo](#). O Kaspersky Endpoint Security for Android não tem acesso à memória externa no contêiner corporativo. As informações sobre os objetos detectados são exibidas em notificações 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 a 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 esses arquivos sem notificar que eles foram ignorados.
- Em dispositivos executando Android 11 ou posterior, o aplicativo Kaspersky Endpoint Security for Android não pode verificar as pastas "Android/data" e "Android/obb" para detectar malware [devido a limitações técnicas](#).

Para configurar o agendamento de Verificação Completa de um dispositivo:

1. Na janela principal do Kaspersky Endpoint Security, toque em **Configurações** → **Configurações do aplicativo** → **Antimalware** → **Configurações de verificação**.
2. Clique em **Agendamento** e selecione a frequência da verificação completa:
 - **Semanalmente**
 - **Diariamente**
 - **Desativado**
 - **Após a atualização do banco de dados**
3. Toque em **Dia de início** e selecione o dia da semana no qual deseja iniciar a verificação completa.
4. Toque 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.

Se o dispositivo estiver no modo de economia de bateria, o aplicativo poderá executar essa tarefa mais tarde do que o especificado. Para garantir respostas oportunas dos dispositivos Android aos comandos do administrador, ative o [uso do Firebase Cloud Messaging](#).

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 antimalware e o serviço na nuvem da Kaspersky Security Network (Proteção na Nuvem) são usados para garantir a segurança automaticamente.

Para alterar o modo de proteção do dispositivo:

1. Na janela principal do Kaspersky Endpoint Security, toque em **Configurações** → **Configurações do aplicativo** → **Antimalware** → **Modo de proteção em tempo real**.
2. Selecione o modo de Proteção do dispositivo:

- **Desativado.** A Proteção está desativada.
- **Recomendado.** O Antimalware verifica somente os aplicativos instalados a pasta Downloads. O Antimalware verifica os novos aplicativos logo depois de serem instalados.
- **Expandido.** O Antimalware verifica objetos maliciosos em todos os arquivos do dispositivo quando qualquer operação é realizada neles (por exemplo, quando são salvos, movidos ou modificados). O Antimalware 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** → **Configurações do aplicativo** → **Antimalware** na janela principal do Kaspersky Endpoint Security.
2. Ative o botão **Proteção na Nuvem (KSN)**.

O botão **Proteção na Nuvem (KSN)** gerencia o uso da 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 antimalware, mas já estão disponíveis na KSN. O serviço na nuvem da Kaspersky Security Network fornece a operação completa do Antimalware 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. Na janela principal do Kaspersky Endpoint Security, toque em **Configurações** → **Configurações do aplicativo** → **Antimalware** → **Configurações de verificação**.
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. Toque 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.

- **Perguntar ao usuário**

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. 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 no dispositivo. Para assegurar a proteção confiável dos dados, elimine todos os objetos detectados.

As informações sobre ameaças detectadas e as ações tomadas sobre elas são registradas nos relatórios do aplicativo (**Configurações** → **Relatórios**). Você pode optar por exibir relatórios sobre as operações do Antimalware.

Atualizações do banco de dados antimalware

Para atualizar os bancos de dados antimalware do aplicativo:

Na janela principal do Kaspersky Endpoint Security, toque em **Configurações** → **Configurações do aplicativo** → **Antimalware** → **Iniciar a atualização do banco de dados**.

Ao utilizar o Kaspersky Endpoint Security for Android, pode ocorrer um problema de **Nome de domínio do serviço Kaspersky bloqueado**, indicando que questões de rede estão impedindo o aplicativo de acessar os serviços da Kaspersky. Isso pode afetar os recursos de Proteção antimalware e colocar seus dados em risco. Alterar as configurações de conexão pode corrigir o problema.

Esta seção fornece apenas instruções gerais. Consulte o guia do usuário fornecido pelo fabricante do dispositivo para obter instruções específicas.

Para alterar suas configurações de conexão:

1. Vá para **Configurações** no dispositivo.
2. Abra as configurações de conexão.
3. Vá para a seção **DNS privado**.
4. Selecione o **Nome do host do provedor DNS privado** e digite um nome DNS. Por exemplo, você pode digitar "dns.google" para usar o servidor DNS público do Google.
5. Salve as alterações.

As configurações de conexão são alteradas.

Atualização do banco de dados agendada

O aplicativo pode atualizar automaticamente os bancos de dados antimalware de acordo com o agendamento especificado.

Para configurar o agendamento de atualização:

1. Na janela principal do Kaspersky Endpoint Security, toque em **Configurações** → **Configurações do aplicativo** → **Antimalware** → **Configurações de atualização do banco de dados**.
2. Toque em **Agendamento** e selecione a frequência de atualização:
 - **Semanalmente**
 - **Diariamente**
 - **Desativado**
3. Toque em **Dia de início** e selecione o dia da semana no qual deseja executar a atualização.
4. Toque em **Hora de início** e selecione a hora para iniciar a atualização.

As atualizações de banco de dados antimalware são iniciadas de acordo com o agendamento.

Se o dispositivo estiver no modo de economia de bateria, o aplicativo poderá executar essa tarefa mais tarde do que o especificado. Para garantir respostas oportunas dos dispositivos Android aos comandos do administrador, ative o [uso do Firebase Cloud Messaging](#).

A funcionalidade de atualizações (incluindo o fornecimento de atualizações de assinaturas de antimalware e atualizações de base de código), bem como a funcionalidade KSN, podem não estar disponíveis no software nos EUA.

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 Redefinir as configurações padrão for enviado ao dispositivo, o controle sobre o dispositivo será perdido, e os comandos Antirroubo restantes não funcionarão.

Proteção na Web

As seguintes condições devem ser atendidas para habilitar a Proteção na Web:

- O Kaspersky Endpoint Security for Android deve ser configurado como um serviço de acessibilidade.
- A Declaração sobre processamento de dados para uso da Proteção na Web (Declaração da Proteção na Web) deve ser aceita. 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.

- Em alguns dispositivos, as seguintes [permissões](#) devem ser concedidas:
 - Executar em segundo plano
 - Exibir janelas pop-up durante a execução em segundo plano
 - Exibir janela pop-up
 - Ignorar otimização de bateria

No Yandex Browser e no Samsung Internet, URLs maliciosas e de phishing podem permanecer sem bloqueio. Isso ocorre porque somente o domínio do site é verificado. Se for um domínio malicioso ou de phishing, a Proteção na Web bloqueará a ameaça. Se o domínio não for classificado como malicioso ou de phishing, a URL específica não será bloqueada.

A Proteção na Web em dispositivos Android é compatível apenas com Google Chrome, HUAWEI Browser, Samsung Internet e Yandex Browser.

O recurso Guias personalizadas é compatível com Google Chrome, Navegador HUAWEI e Samsung Internet.

Para usar a Proteção na Web no Telegram, desative a abertura de links no navegador do Telegram nas configurações do Telegram.

A Proteção na Web para o HUAWEI Browser, Samsung Internet e Yandex Browser não bloqueia sites em um dispositivo móvel se um contêiner corporativo for usado e a [Proteção na Web estiver ativada somente para o contêiner corporativo](#).

Para usar a Proteção na Web a todo momento enquanto você navega na Web, defina o Google Chrome, o HUAWEI Browse, o Samsung Internet ou o Yandex Browser como o navegador padrão.

Para definir um navegador compatível como o navegador padrão e usar a Proteção na Web para verificar os sites a todo momento:

1. Na janela principal do Kaspersky Endpoint Security, toque em **Configurações** → **Configurações do aplicativo** → **Proteção na Web**.

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 HUAWEI Browser ou o Samsung Internet como navegador padrão. A Proteção na Web verifica os sites constantemente quando você navega na Web.

Verificação de notificações de aplicativos de mensagens

O Kaspersky Endpoint Security for Android pode detectar phishing e URLs maliciosas em notificações do Telegram, WhatsApp, do aplicativo de SMS padrão e de outros aplicativos de mensagens comuns. Somente URLs expressas como texto diretamente no texto de notificação podem ser verificadas. URLs incorporadas na marcação não são verificadas.

As seguintes condições devem ser atendidas para ativar a verificação de notificações:

- A Proteção na Web deve estar ativada.
- A exibição de notificações deve ser permitida para os aplicativos de mensagens desejados. O Kaspersky Endpoint Security for Android verifica apenas notificações que podem ser exibidas na tela do dispositivo.
- Nos dispositivos Google Pixel e Vivo, a permissão "Conversas" deve ser concedida ao Kaspersky Endpoint Security nas configurações de acesso às notificações.

Para permitir acesso às notificações para que o aplicativo possa verificá-las:

1. Na janela principal do Kaspersky Endpoint Security, toque em **Configurações** → **Configurações do aplicativo** → **Proteção na Web**.

2. Ative o botão de alternância **Bloquear notificações que contenham phishing e URLs maliciosas**.

A janela **Acesso à notificação necessário** é exibida.

3. Toque em **Continuar**.

A seção de configurações correspondente é exibida.

4. Ative o botão de alternância do Kaspersky Endpoint Security.

5. Na caixa de diálogo que é aberta, permita que o aplicativo leia todas as suas notificações.

6. Voltar ao Kaspersky Endpoint Security.

O aplicativo agora verifica notificações para detectar phishing e URLs maliciosas. Se uma URL perigosa for encontrada, a notificação será bloqueada e uma tela de bloqueio com informações sobre a notificação bloqueada será exibida.

Se o Kaspersky Endpoint Security for Android não estiver ativado como um recurso de Acessibilidade, o aplicativo enviará uma notificação por push sobre as URLs perigosas detectadas em vez de exibir uma tela de bloqueio. Após tocar na notificação push, uma tela com informações sobre a notificação bloqueada é exibida.

Obter certificado

Para obter um certificado para acessar os recursos da rede corporativa:

1. Na janela principal do Kaspersky Endpoint Security, toque em **Configurações** → **Configurações do aplicativo** → **Adicional** → **Obter o certificado**.
2. Especifique as credenciais de sua conta da rede corporativa. O login deve ser especificado em um dos seguintes formatos:

- userPrincipalName@DNSDomainName
- sAMAccountName
- sAMADomain\sAMAccountName

Para obter mais informações sobre esses atributos, visite o [site de documentação técnica da Microsoft](#). Para obter detalhes, você pode entrar em contato com o administrador.

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.

Sincronizar 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. 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. Na janela principal do Kaspersky Endpoint Security, toque em **Configurações** → **Configurações do aplicativo** → **Sincronização**.
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 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.

Instalar e usar certificados de e-mail e VPN no dispositivo

O administrador pode especificar certificados de e-mail e VPN a serem instalados no dispositivo. Em dispositivos com um contêiner corporativo, esses certificados serão instalados automaticamente.

Um certificado de e-mail é instalado no dispositivo somente se o administrador definir as configurações do Exchange ActiveSync primeiro.

Um certificado VPN também pode ser instalado em um armazenamento de certificados confiável em um espaço pessoal, além do contêiner corporativo, e usado por qualquer aplicativo. Você receberá uma notificação e precisará instalar um certificado VPN manualmente seguindo as instruções abaixo.

Para instalar manualmente um certificado VPN no dispositivo:

1. Abra o Kaspersky Endpoint Security for Android.
2. Toque em **Notificações**.
3. Na notificação sobre o certificado, toque em **Instalar**.
Uma janela com a senha do certificado é exibida.
4. Lembre-se ou anote a senha e toque em **OK**.
5. Quando solicitado, insira a senha do certificado e toque em **OK**.
6. Toque em **OK** para confirmar a instalação do certificado.

O certificado VPN será instalado no dispositivo.

Ativar a acessibilidade no Android 13 ou posterior

No Android 13 ou posterior, os serviços de acessibilidade são restritos a aplicativos que não foram baixados do Google Play ou do HUAWEI AppGallery. Será necessário permitir a Acessibilidade manualmente se o Kaspersky Endpoint Security for Android foi baixado do servidor do Kaspersky Security Center ou do site da Kaspersky.

Se você atualizar o aplicativo Kaspersky Endpoint Security for Android usando um pacote de instalação do Kaspersky Security Center ou um arquivo APK do site da Kaspersky, os serviços de acessibilidade serão desativados. Você deve ativar manualmente os serviços de acessibilidade novamente.

A Acessibilidade é usada para os seguintes propósitos:

- Verificar sites e aplicativos na Kaspersky Security Network
- Bloquear o dispositivo em caso de roubo

- Exibir advertências
- Bloquear a câmera quando restringida pelo administrador

Para ativar a Acessibilidade para o Kaspersky Endpoint Security:

1. Abra a página **Acessibilidade** nas configurações do dispositivo e localize o Kaspersky Endpoint Security.
2. Ative o botão do Kaspersky Endpoint Security. Na caixa de diálogo que diz que os serviços de Acessibilidade estão restritos, toque em **OK**.
Agora é possível conceder ao Kaspersky Endpoint Security acesso às configurações restritas.
3. Abra a página de informações do Kaspersky Endpoint Security nas configurações do dispositivo. Por exemplo, acesse **Configurações > Aplicativos** e localize o aplicativo na lista.
4. Na página de informações do Kaspersky Endpoint Security, toque em **⋮** no canto superior direito e selecione **Permitir configurações restritas**.
O Kaspersky Endpoint Security agora tem acesso às configurações restritas.
5. Volte para a página **Acessibilidade** nas configurações do dispositivo e localize o Kaspersky Endpoint Security.
6. Ative o botão do **Kaspersky Endpoint Security**. Na caixa de diálogo que se abre, permita que o aplicativo tenha controle total do dispositivo.

Os serviços de Acessibilidade agora estão ativados para o Kaspersky Endpoint Security.

Ativar a acessibilidade do aplicativo no Android 13 ou posterior

Para ativar a Acessibilidade para o Kaspersky Endpoint Security:

1. Na caixa de diálogo que solicita a ativação dos serviços de Acessibilidade, toque em **Ativar**.
A página **Acessibilidade** nas configurações do dispositivo se abre.
2. Ative o botão do Kaspersky Endpoint Security. Na caixa de diálogo que diz que os serviços de Acessibilidade estão restritos, toque em **OK**.
Agora é possível conceder ao Kaspersky Endpoint Security acesso às configurações restritas.
3. Abra a página de informações do Kaspersky Endpoint Security nas configurações do dispositivo. Por exemplo, acesse **Configurações > Aplicativos** e localize o aplicativo na lista.
4. Na página de informações do Kaspersky Endpoint Security, toque em **⋮** no canto superior direito e selecione **Permitir configurações restritas**.
O Kaspersky Endpoint Security agora tem acesso às configurações restritas.

5. Volte para o aplicativo e na caixa de diálogo que solicita a ativação dos serviços de Acessibilidade, toque em **Ativar**.

A página **Acessibilidade** nas configurações do dispositivo se abre.

6. Ative o botão do **Kaspersky Endpoint Security**. Na caixa de diálogo que se abre, permita que o aplicativo tenha controle total do dispositivo.

Os serviços de Acessibilidade agora estão ativados para o Kaspersky Endpoint Security.

Atualizar o aplicativo

O Kaspersky Endpoint Security pode ser atualizado nas seguintes formas:

- Usando manualmente o site da Kaspersky. Baixe a nova versão do aplicativo através do site da Kaspersky e a instala no 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 a partir do site da Kaspersky

Para atualizar o aplicativo a partir do site da Kaspersky:

1. Vá para o [site da Kaspersky](#).
2. Encontre o Kaspersky Security for Mobile no site.
3. Toque em **Mostrar downloads**.
4. Selecione uma versão do aplicativo e toque em **Baixar**.
5. Abra o arquivo APK baixado e siga as instruções na tela.

O Kaspersky Endpoint Security for Android está atualizado.

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.

A funcionalidade de atualizações (incluindo o fornecimento de atualizações de assinaturas de antimalware e atualizações de base de código), bem como a funcionalidade KSN, podem não estar disponíveis no software nos EUA.

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 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 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 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

Os aplicativos marcados com um ícone de pasta (aplicativos corporativos) são armazenados em seu dispositivo no contêiner corporativo. O *contêiner corporativo* 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 contêiner corporativo permite armazenar os dados corporativos separadamente dos dados pessoais. Isso mantém os dados corporativos confidenciais e os protege contra malwares. Quando um contêiner corporativo é criado em seu dispositivos, os seguintes aplicativos corporativos são automaticamente instalados no contêiner corporativo: 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 e-mail 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](#) ¹.

Usar o aplicativo Kaspersky Protection for iOS

Esta seção de Ajuda descreve recursos e operações que estão disponíveis para usuários do aplicativo Kaspersky Protection 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 Protection for iOS oferece os principais recursos 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.

Somente o domínio do site é verificado. Se for um domínio malicioso ou de phishing, a Proteção na Web bloqueará a ameaça. Se o domínio não for classificado como malicioso ou de phishing, a URL específica não será bloqueada.

A Proteção na Web também monitora a atividade de rede dos aplicativos e todo o tráfego do sistema em 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 Protection for iOS detecta um jailbreak, ele exibe uma mensagem crítica e informa o administrador sobre o problema.

Um jailbreak permite ignorar os recursos de segurança do sistema operacional. Portanto, a segurança do dispositivo não pode ser garantida, e vários problemas podem surgir, como:

- 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

É possível instalar o aplicativo Kaspersky Protection for iOS usando um link ou um código QR gerado para você pelo administrador no console de gerenciamento. Você receberá essas informações em um e-mail.

Para instalar o aplicativo do Kaspersky Protection for iOS:

1. Encontre a mensagem de e-mail com o convite do administrador para conectar seu dispositivo ao sistema de administração remota do Kaspersky Security Center.
2. Acesse a App Store em uma das seguintes formas:
 - Toque em **Conectar dispositivo** na mensagem se estiver lendo-a no dispositivo iOS no qual deseja instalar o aplicativo.
 - Leia 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. Na página da Web exibida, toque em **Baixar na App Store**.
4. Baixe e instale o aplicativo por meio da App Store seguindo o procedimento de instalação padrão do aplicativo na plataforma do iOS.

O aplicativo Kaspersky Protection for iOS está instalado no seu dispositivo. Para proteger o dispositivo, [ative o aplicativo](#). Caso o dispositivo não esteja conectado ao Kaspersky Security Center, é possível [inserir o código de ativação](#) manualmente.

Ativar o aplicativo

Para ativar o aplicativo do Kaspersky Protection 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 ameaças da Web.
5. Permita que o aplicativo envie notificações push. O aplicativo usa as notificações push para informar você sobre problemas de segurança e com a sua licença.

O aplicativo Kaspersky Protection for iOS em seu dispositivo está ativado.

Ativar o aplicativo com um código de ativação

Ao instalar o Kaspersky Protection 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 Protection 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 Protection 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](#).

A funcionalidade de atualizações (incluindo o fornecimento de atualizações de assinaturas de antimalware e atualizações de base de código), bem como a funcionalidade KSN, podem não estar disponíveis no software nos EUA.

Usar o diagnóstico para solucionar problemas

Se você tiver problemas com o Kaspersky Protection for iOS, os especialistas do suporte técnico da Kaspersky podem solicitar que você envie um *arquivo com informações de diagnóstico*. Esse arquivo permite que os especialistas do suporte técnico rastreiem as causas dos problemas na operação do aplicativo.

Para compartilhar um arquivo com informações de diagnóstico, o diagnóstico deve estar ativado no Kaspersky Protection for iOS.

Recomendamos que você ative o diagnóstico somente se solicitado por um especialista do suporte técnico da Kaspersky.

O salvamento de informações de diagnóstico pode afetar a velocidade da sua conexão com a Internet e o desempenho do seu dispositivo, do Kaspersky Protection for iOS e de outros aplicativos.

Você pode excluir o arquivo com informações de diagnóstico manualmente no aplicativo Arquivos.

Para ativar os diagnósticos:

1. Na janela principal, toque em ⓘ.
2. Na janela **Sobre o aplicativo** exibida, toque em **Diagnóstico**.
3. Na janela **Diagnóstico** que se abre, ative o diagnóstico usando o botão **Diagnóstico**.
4. Aceite a Declaração de Suporte. A Declaração de Suporte descreve [quais dados são salvos no arquivo com informações de diagnóstico](#).
5. Toque em **OK**.

O diagnóstico será ativado em seu dispositivo. Os dados sobre a operação do Kaspersky Protection for iOS agora serão salvos em um arquivo com informações de diagnóstico. Se você tiver um problema, poderá compartilhar esse arquivo com um especialista do suporte técnico da Kaspersky.

Remover o aplicativo

Para remover o aplicativo Kaspersky Protection 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 Protection for iOS foi removido do seu dispositivo.

Licenciamento do aplicativo

Esta seção fornece informações sobre os termos gerais relacionados ao licenciamento do MDM básico no Kaspersky Next Expert View (cloud).

Sobre o Contrato de Licença de Usuário Final

O *Contrato de Licença de Usuário Final* (EULA) é um acordo vinculativo entre você e a AO Kaspersky Lab que estipula os Termos e Condições sob os quais será possível usar o MDM básico no Kaspersky Next Expert View (cloud).

Recomendamos a leitura cuidadosa dos Termos e Condições do EULA antes de usar o MDM básico no Kaspersky Next Expert View (cloud).

É possível visualizar os Termos e Condições do EULA das seguintes maneiras:

- Durante a instalação dos componentes do MDM básico no Kaspersky Next Expert View (cloud).
- 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 Protection 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.
- Na seção **Geral** → **Contratos de Licença do Usuário Final** nas propriedades do Servidor de Administração do Kaspersky Security Center Web Console.
- Na etapa 4 do processo de [conexão de dispositivos móveis ao Kaspersky Security Center Web Console](#), se o **Administrador** tiver sido selecionado na etapa 3. O administrador será solicitado a aceitar o EULA.
- Durante a instalação do aplicativo, se a opção **Usuários** tiver sido selecionada na etapa 3 do processo de [conexão de dispositivos móveis ao Kaspersky Security Center Web Console](#). O usuário do dispositivo móvel será solicitado a aceitar o EULA.

Ao confirmar que concorda com o Contrato de Licença de Usuário Final (EULA) durante a instalação dos componentes do MDM básico no Kaspersky Next Expert View (cloud), você indica seu aceite dos Termos e Condições do Contrato de Licença de Usuário Final. Caso não aceite os termos do Contrato de Licença de Usuário Final, será necessário cancelar a instalação dos componentes do MDM básico no Kaspersky Next Expert View (cloud) e deixar de usá-los.

Sobre a licença

Uma *licença* é um direito com período de validade limitado para uso do MDM básico no Kaspersky Next Expert View (cloud), concedido nos termos do Contrato de Licença (Contrato de Licença de Usuário Final).

O escopo de serviços e o período de validade dependem da licença sob a qual a solução é usada.

São fornecidos os seguintes tipos de licença:

- *Avaliação*

Uma licença gratuita destinada a testar o MDM básico no Kaspersky Next Expert View (cloud).

Uma licença de avaliação é válida por 30 dias. Quando uma licença de avaliação expira, o aplicativo móvel Kaspersky Endpoint Security for Android e o aplicativo móvel Kaspersky Protection for iOS param de executar a maioria das funções, exceto a sincronização com o Servidor de Administração. Para continuar usando os aplicativos, é necessário comprar a licença comercial.

- *Comercial*

Uma licença paga.

Quando uma licença comercial expira, os aplicativos móveis continuam 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:
 - Antimalware. A Proteção em Tempo Real e a verificação de malware do dispositivo estão disponíveis, mas as atualizações do banco de dados antimalware 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, 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).

- Aplicativo Kaspersky Protection for iOS:
 - Sincronização com o Servidor de Administração.

O Kaspersky Protection 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).

Os componentes restantes dos aplicativos móveis não estão disponíveis para o usuário do dispositivo e você não pode definir as configurações de política.

Para continuar usando a funcionalidade completa dos aplicativos e definir as configurações da política, você deve renovar sua licença comercial. Para garantir a proteção ininterrupta dos dispositivos de seus usuários contra todas as ameaças de segurança, recomendamos renovar o período da licença ou comprar uma nova licença antes que a atual expire.

Com uma licença que não inclui a funcionalidade estendida de MDM básico no Kaspersky Next Expert View (cloud), somente as configurações básicas de proteção do dispositivo estão disponíveis no plug-in do Kaspersky Mobile Devices Protection and Management.

Exibir informações de licença

O plug-in do Kaspersky Mobile Devices Protection and Management permite exibir as seguintes informações sobre a licença atual:

- Chave de licença
- O número de dispositivos nos quais a chave de licença pode ser usada
- Tipo de licença
- Data e hora de expiração da licença
- Número de dias antes da expiração da licença
- O tipo de funcionalidade disponível sob a licença atual

Para exibir informações sobre a licença atual:

1. Na janela principal do Kaspersky Next Expert View (cloud), selecione **Gerenciamento de ativos** → **Políticas**. Na lista de políticas de grupo aberta, clique no nome da política que deseja configurar.
2. Na janela de propriedades da política, selecione **Configurações do aplicativo**.
3. Clique em **Licença**.

A janela **Licença** que contém informações sobre a licença é exibida.

Sobre a assinatura

A assinatura do MDM básico no Kaspersky Next Expert View (cloud) é um pedido para usar o aplicativo móvel com os parâmetros selecionados (data de validade da assinatura, número de dispositivos móveis protegidos). Será possível efetuar um pedido de assinatura do MDM básico no Kaspersky Next Expert View (cloud) 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 MDM básico no Kaspersky Next Expert View (cloud) continue funcionando após a expiração do prazo limitado da assinatura, será necessário renovar a 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 MDM básico no Kaspersky Next Expert View (cloud) sob uma assinatura, é necessário 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 MDM básico no Kaspersky Next Expert View (cloud).

Sobre a chave de licença

Uma *chave de licença* é uma sequência de bits que pode ser aplicada para ativar e, em seguida, usar a solução integrada MDM básico no Kaspersky Next Expert View (cloud), de acordo com os termos do Contrato de Licença de Usuário Final. As chaves de licença são geradas pelos especialistas da Kaspersky.

Você pode adicionar uma chave de licença para o aplicativo móvel usando um arquivo de chave ou um 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 aplicativos móveis Android](#). A chave de licença é exibida na interface do Kaspersky Security Center e na interface do aplicativo móvel Android como uma sequência alfanumérica exclusiva.

Após adicionar chaves de licença, você poderá substituí-las por outras chaves de licença.

Não é possível ativar o aplicativo Kaspersky Protection 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 de licença é exibida na interface do aplicativo móvel como uma sequência alfanumérica exclusiva.

A chave de licença poderá ser bloqueada pela Kaspersky, por exemplo, no caso de violação dos termos do Contrato de Licença de Usuário Final. Se a chave de licença estiver bloqueada, os aplicativos móveis interrompem a execução de todas as suas funções, exceto a sincronização com o Servidor de Administração. Para continuar usando os aplicativos, você tem de adicionar uma chave de licença 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 Protection for iOS. O código de ativação é enviado ao endereço de e-mail especificado após a compra da solução integrada MDM básico no Kaspersky Next Expert View (cloud) ou ao efetuar o pedido da versão de avaliação do MDM básico no Kaspersky Next Expert View (cloud).

Para ativar o aplicativo móvel usando 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 o 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 Protection for iOS com um arquivo de chave.

Um arquivo de chave é enviado ao endereço de e-mail fornecido quando a solução integrada MDM básico no Kaspersky Next Expert View (cloud) foi comprada ou quando a versão de avaliação do MDM básico no Kaspersky Next Expert View (cloud) foi solicitada.

Você não precisa se conectar aos servidores de ativação da Kaspersky para ativar o aplicativo com um arquivo de chave.

Você pode recuperar um arquivo de chave se ele tiver sido acidentalmente excluído. Você poderá precisar de um arquivo de chave para se registrar no Kaspersky CompanyAccount, por exemplo.

Para restaurar seu arquivo de chave, realize uma das seguintes ações:

- Entre em contato com o vendedor da licença.
- Receba um arquivo de chave através do [site da Kaspersky](#) usando o código de ativação.

Fornecimento de dados no Kaspersky Endpoint Security for Android

O MDM básico no Kaspersky Next Expert View (cloud) está em conformidade com o Regulamento Geral sobre a Proteção de Dados (GDPR).

Para instalar o aplicativo, você ou um usuário do dispositivo devem ler e aceitar os termos do Contrato de Licença de 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 relativa ao processamento de 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 Mobile Devices Protection and Management também mudará para *Advertência*.

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:

- **Antimalware.** 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 antimalware, mas já estão disponíveis na KSN. O serviço na nuvem da Kaspersky Security Network fornece a operação completa do Antimalware e reduz a probabilidade de falsos alarmes.
- **Proteção na Web e Controle da 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 corporativos de acordo com as listas de categorias permitidas e bloqueadas (por exemplo, a categoria "Jogos").

As informações sobre os tipos de dados enviados à Kaspersky ao usar a KSN durante a operação do antimalware e Controle de aplicativos estão disponíveis no Contrato de Licença de 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 de Usuário Final

Quando o código de ativação for usado para ativar o software a fim de verificar o uso legítimo do Software, o usuário final concorda em fornecer periodicamente ao titular dos direitos as seguintes informações:

- formato dos dados na solicitação à infraestrutura do titular dos direitos; endereço IPv4 acessado do serviço da Web; tamanho do conteúdo da solicitação à infraestrutura do titular dos direitos; ID do protocolo; código de ativação do software; tipo de compactação de dados; ID do software; conjunto de IDs de software que podem ser ativados no dispositivo do usuário; localização de 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 de sistemas operacionais; formato dos dados na solicitação à infraestrutura do titular dos direitos; tipo de soma de verificação para o objeto sendo processado; cabeçalho da licença de software; ID de um centro de ativação regional; data e hora de criação da chave de licença de software; ID da licença de software; ID do modelo de informações usado para fornecer a licença do software; data e hora de expiração da licença de software; status atual da chave de licença do software; tipo de licença de software usada; tipo da licença usada para ativar o software; ID do software derivada 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 para o objeto sendo processado; soma de verificação do objeto sendo processado; o ID do componente de Software;
- ID do registro acionado nos bancos de dados de antimalware do software; carimbo de data/hora do registro acionado nos bancos de dados antimalware do software; tipo do registro acionado nos bancos de dados de antimalware do software; nome do malware detectado ou software legítimo que pode ser usado para danificar o dispositivo ou os dados do usuário;
- nome da loja a partir da qual o aplicativo foi instalado; nome do 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/hora do certificado digital;
- versão completa do software; ID de atualização de software; tipo de software instalado; o identificador de configuração; o resultado da ação do software; código de erro;
- números 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 de arquivos, caminhos de arquivos, endereços, números de telefone ou outras informações pessoais de usuários.

Se você usar os servidores de atualização do titular dos direitos para baixar as atualizações, o usuário final, para aumentar a eficiência do procedimento de atualização, concorda em fornecer periodicamente ao titular dos direitos as seguintes informações:

- ID do software derivada da licença; versão completa do software; ID da licença de software; tipo de licença de software usada; ID de instalação do software (PCID); ID do início da atualização do software; endereço da Web 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 ativado nos bancos de dados antimalware do software; carimbo de data/hora do registro ativado nos bancos de dados antimalware do software; tipo do registro ativado nos bancos de dados antimalware do software; data e hora de lançamento dos bancos de dados do software; versão do SO, número de compilação do SO, número de atualização do SO, edição do SO, informações estendidas sobre a edição do SO; versão do Service Pack do SO; características de detecção; soma de verificação (MD5) do objeto em processamento; nome do objeto em processamento; sinalizador indicando se o objeto em processamento é um arquivo PE; soma de verificação (MD5) da máscara que bloqueou o serviço da Web; soma de verificação (SHA256) do objeto em processamento; tamanho do objeto em processamento; código do tipo de objeto; decisão do software sobre o objeto em processamento; caminho para o objeto em processamento; código do diretório; versão do componente do software; versão das estatísticas enviadas; endereço acessado do serviço da Web (URL, IP); tipo de cliente usado para acessar o serviço da Web; endereço IPv4 acessado do serviço da Web; endereço IPv6 acessado do serviço da Web; endereço Web da fonte da solicitação do serviço da Web (referente); endereço Web em processamento;
- informações sobre os objetos verificados (versão do aplicativo do AndroidManifest.xml; decisão do software sobre o aplicativo; método usado para obter a decisão do software sobre o aplicativo; nome do pacote do instalador de armazenamento; nome do pacote (ou nome do conjunto de pacotes) do AndroidManifest.xml; categoria Google SafetyNet; sinalizador indicando se o SafetyNet está ativado no dispositivo; valor SHA256 da resposta do Google SafetyNet; esquema de assinatura APK para o certificado 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 de expiração do certificado; data e hora de emissão do certificado; versão das estatísticas enviadas; algoritmo para o cálculo da impressão digital do certificado; hash MD5 do arquivo APK instalado; hash MD5 do arquivo DEX localizado dentro do arquivo APK; permissões concedidas dinamicamente ao aplicativo; versão do software de terceiros; sinalizador indicando se o aplicativo é o aplicativo de mensagens SMS padrão; sinalizador indicando se o aplicativo tem direitos de administrador de dispositivos; sinalizador indicando se o aplicativo está no catálogo do sistema; sinalizador indicando se o aplicativo usa serviços de acessibilidade);
- informações sobre todos os objetos e atividades potencialmente maliciosos (conteúdo do fragmento do objeto em processamento; data e hora de expiração do certificado; data e hora de emissão do certificado; identificação da chave da loja de chaves usada para criptografia; protocolo usado para troca de dados com a KSN; ordem do fragmento no objeto em processamento; dados do registro interno, gerados pelo módulo de software antimalware para um objeto em processamento; 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 e configurações do proprietário do certificado; impressão digital do certificado do objeto verificado e do algoritmo de hashing; data e hora da última modificação do objeto em processamento; data e hora da criação de um objeto em processamento; objetos ou suas partes em processamento; descrição de um objeto em processamento conforme definido nas propriedades do objeto; formato do objeto em processamento; tipo de soma de verificação para o objeto em processamento; soma de verificação (MD5) do objeto em processamento; nome do objeto em processamento; soma de verificação (SHA256) do objeto em processamento; tamanho do objeto em processamento; nome do fornecedor do software; a decisão do software sobre o objeto em processamento; versão do objeto em processamento; fonte da decisão tomada para o objeto em processamento; soma de verificação do objeto em processamento; nome do aplicativo de origem; caminho para o objeto em processamento; informações sobre os resultados da verificação da assinatura do arquivo; chave de sessão de logon; algoritmo de criptografia para a chave de sessão de logon; tempo de armazenamento para o objeto em processamento; algoritmo para o cálculo da impressão digital do certificado);

- tipo de compilação, por exemplo, "user" ou "eng"; nome completo do produto; fabricante do produto/hardware; se os aplicativos podem ser instalados fora do Google Play; status do serviço na nuvem para verificação dos aplicativos Google; status do serviço na nuvem para verificação dos aplicativos Google que estão sendo instalados através do ADB; nome de código de desenvolvimento atual ou "REL" para compilações de produção; número de compilação incremental; string de versão visível pelo usuário; nome do dispositivo do usuário; ID de compilação do software visível pelo usuário; identificação digital do firmware; ID do firmware; sinalizador indicando se o dispositivo está enraizado; sistema operacional; nome do software; tipo de licença do software utilizado;
- informações sobre a qualidade dos serviços da KSN (protocolo usado para trocar dados com a KSN; ID do serviço da KSN acessado pelo software; data e hora em que as estatísticas deixaram de ser recebidas; número de conexões com a KSN retiradas do cache; número de solicitações para as quais foi encontrada uma resposta no banco de dados de solicitações local; número de conexões malsucedidas com a KSN; número de transações malsucedidas com a KSN; distribuição temporal de solicitações canceladas para a KSN; distribuição temporal de conexões malsucedidas com a KSN; distribuição temporal de transações malsucedidas com a KSN; distribuição temporal de conexões bem-sucedidas com a KSN; distribuição temporal de transações bem-sucedidas com a KSN; distribuição temporal de solicitações bem-sucedidas para a KSN; distribuição temporal de solicitações para a KSN que foram interrompidas; número de novas conexões com a KSN; número de solicitações malsucedidas para a KSN provocadas por erros de roteamento; número de solicitações malsucedidas provocadas pela desativação da KSN nas configurações do software; número de solicitações malsucedidas para a KSN provocadas por problemas de rede; número de conexões bem-sucedidas com a KSN; número de transações bem-sucedidas com a KSN; número total de solicitações para a 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 da instalação do software (PCID); tipo de software instalado;
- 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 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; informações sobre o aplicativo sobreposto: nome do pacote do aplicativo (para o aplicativo sobreposto: se o anúncio for exibido em uma área de trabalho vazia, o valor deve ser "launcher"); data e hora da sobreposição; informações sobre o aplicativo sobreposto: nome do pacote do aplicativo; largura da sobreposição;

- configurações do ponto de acesso Wi-Fi em uso (tipo de dispositivo detectado; configurações do DHCP (somas de verificação do gateway local IPv6, DHCP IPv6, DNS1 IPv6, DNS2 IPv6; soma de verificação do comprimento do prefixo de rede; soma de verificação do endereço local IPv6); configurações do DHCP (somas de verificação do endereço IP local do gateway, DHCP IP, DNS1 IP, DNS2 IP e máscara de sub-rede); sinalizador indicando 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 conectado; tipo de autenticação de rede Wi-Fi; lista de redes Wi-Fi disponíveis e suas configurações; soma de verificação (MD5 com salto) do endereço MAC do ponto de acesso; soma de verificação (SHA256 com salto) do endereço MAC do ponto de acesso; tipos de conexão com suporte do ponto de acesso Wi-Fi; tipo de criptografia de rede Wi-Fi; hora local do início e fim da conexão da rede Wi-Fi; ID da rede Wi-Fi conforme o endereço MAC do ponto de acesso; ID da rede Wi-Fi conforme o nome da rede Wi-Fi; ID da rede Wi-Fi conforme o nome da rede Wi-Fi e o endereço MAC do ponto de acesso; força do sinal Wi-Fi; nome da rede Wi-Fi; conjunto de protocolos de autenticação com suporte na configuração; protocolo de autenticação usado para conexão WPA-EAP; protocolo de autenticação interna; conjunto de cifras de grupo com suporte nesta configuração; conjunto de protocolos de gerenciamento de chaves com suporte nesta configuração; categoria final de privacidade da rede no software; categoria final de segurança da rede no software; conjunto de cifras de bloco para WPA com suporte nesta configuração; conjunto de protocolos de segurança com suporte nesta configuração);
- data e hora de instalação do software; data de ativação do software; identificador da organização parceira através da qual o pedido de licença de software foi feito; ID do software derivada da licença; número de série da chave de licença do software; localização de software; sinalizador que indica se a participação na KSN está ativada; ID do software licenciado; ID da licença de 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.

Se a versão mais recente da Declaração da Kaspersky Security Network não for aceita, somente as estatísticas listadas na versão aceita anteriormente da declaração serão enviadas à Kaspersky Security Network.

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 a 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 sobre configuração do Kaspersky Endpoint Security for Android como recurso de Acessibilidade
- informações sobre transições entre telas do aplicativo, duração da sessão, início e fim 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 antimalware 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 no qual 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 nos últimos 7 dias e o aplicativo aberto 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 no Firebase são publicadas em: <https://firebase.google.com/support/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 do aplicativo
- 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 que indica se o dispositivo tem jailbreak ou raiz
- força do sinal
- duração dos rastreios automáticos
- rede e as seguintes informações correspondentes: código de resposta; tamanho da carga útil 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 no 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
- nome e versão do SO
- RAM total e quantidade atualmente utilizada

- sinalizador indicando se o dispositivo está roteado
- 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
- informações sobre o sinal que causou o encerramento inesperado do software: 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
- informações sobre eventos que ocorreram antes o software foi encerrado inesperadamente: identificador do evento, data e hora do evento, tipo e valor do evento
- valores de registro da CPU
- tipo de evento e valor

Os dados são encaminhados para a Crashlytics por meio de um canal seguro. As informações sobre como os dados são processados no 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 Protection for iOS

O MDM básico no Kaspersky Next Expert View (cloud) está em conformidade com o Regulamento Geral sobre a Proteção de 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 de 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
- Declaração de Suporte

O usuário pode visualizar os termos desses documentos a qualquer momento na seção **Sobre o aplicativo** → **Contratos e declarações** nas configurações do Kaspersky Protection 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 Protection 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 de 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 Protection 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 de Usuário Final

Quando o código de ativação for usado para ativar o software a fim de verificar o uso legítimo do Software, o usuário final concorda em fornecer periodicamente ao titular dos direitos as seguintes informações:

- Formato dos dados na solicitação à infraestrutura do Titular dos direitos; endereço IPv4 acessado do serviço da Web; tamanho do conteúdo da solicitação à infraestrutura do Titular dos direitos; ID do protocolo; Código de ativação do software; tipo de compactação de dados; ID do software; conjunto de IDs de Software que podem ser ativados no dispositivo do usuário; Localização de 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 usado 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 de celular; família de sistemas operacionais; ID do software derivada da licença; lista de contratos apresentados ao usuário pelo Software; tipo de contrato legal aceito pelo usuário ao usar o Software; versão do contrato legal aceita pelo usuário ao usar o Software; sinalizador que indica se o usuário aceitou os termos do contrato legal ao usar o Software; tipo de soma de verificação para o objeto sendo processado; Cabeçalho da licença de software; ID de um centro de ativação regional; Data e hora de criação da chave de licença de software; ID da licença de software; ID do modelo de informações usado para fornecer a licença do Software; Data e hora de expiração da licença de software; status atual da chave de licença do Software; tipo de licença de Software usada; tipo da licença usada para ativar o Software; ID do software derivada da licença.

O Detentor dos Direitos pode usar essas informações também para obter 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 à infraestrutura do titular dos direitos; endereço acessado do serviço da Web (URL, IP); número da porta; endereço da Web da origem da solicitação de serviço da Web (referenciador).
- Versão completa do software; ID de atualização de software; tipo do software instalado; ID do software; o identificador de configuração; o resultado da ação do software; código de erro.
- Endereço da Web sendo processado; endereço IPv4 acessado do serviço da Web; impressão digital do certificado digital do objeto verificado e algoritmo de hash; tipo de certificado; conteúdo do certificado digital que está 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 da KSN (protocolo usado para trocar dados com a KSN; ID do serviço da KSN acessado pelo software; data e hora em que as estatísticas deixaram de ser recebidas; número de conexões com a KSN retiradas do cache; número de solicitações para as quais foi encontrada uma resposta no banco de dados de solicitações local; número de conexões malsucedidas com a KSN; número de transações malsucedidas com a KSN; distribuição temporal de solicitações canceladas para a KSN; distribuição temporal de conexões malsucedidas com a KSN; distribuição temporal de transações malsucedidas com a KSN; distribuição temporal de conexões bem-sucedidas com a KSN; distribuição temporal de transações bem-sucedidas com a KSN; distribuição temporal de solicitações bem-sucedidas para a KSN; distribuição temporal de solicitações para a KSN que foram interrompidas; número de novas conexões com a KSN; número de solicitações malsucedidas para a KSN provocadas por erros de roteamento; número de solicitações malsucedidas provocadas pela desativação da KSN nas configurações do software; número de solicitações malsucedidas para a KSN provocadas por problemas de rede; número de conexões bem-sucedidas com a KSN; número de transações bem-sucedidas com a KSN; número total de solicitações para a 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 da instalação do software (PCID); tipo de 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 de software; ID do SO; versão do sistema operacional instalado 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.

Fornecimento de dados sob a Declaração de Suporte

Quando [o diagnóstico é ativado no Kaspersky Protection for iOS](#), o aplicativo processa e armazena os seguintes dados pessoais para análise adicional pelo Suporte Técnico:

- Data e hora do evento.
- Códigos HTTP e dados para solicitações do servidor aos sistemas do titular dos direitos: corpo da solicitação; URL de solicitação; respostas do servidor; erros.

- Dados em todas as solicitações de rede: URL de solicitação; status de verificação de tráfego.
- Informações da licença: ID da licença e código de ativação; período de validade do pacote de dados de licença atual; status atual da chave de software; modo de operação após a expiração da licença; data de ativação do software; data de expiração da licença; número do pedido ao comprar a licença.
- Informações sobre a conexão com o Servidor de Administração: senha do certificado; endereço de conexão do Servidor de Administração; ID exclusivo do dispositivo; dados de certificados dos usuários; dados de certificados do Servidor de Administração; configurações de software recebidas do Servidor de Administração.
- Eventos do sistema: abertura e fechamento do software; notificações push do Software.
- Informações sobre a operação do software e seus módulos.
- Versão do SO; tipo de SO.
- ID do dispositivo; tipo de dispositivo.
- ID do software; ID do idioma do software; versão do software; ID de instalação do software.
- Informações sobre erros do software.

O fornecimento das informações mencionadas acima ao suporte técnico é voluntário.

Contatar o Suporte Técnico

Esta seção descreve como adquirir o suporte técnico e os termos com os quais está disponível.

Com obter suporte técnico

Caso não consiga encontrar uma solução para seu problema na documentação do MDM básico no Kaspersky Next Expert View (cloud) ou em nenhuma das fontes de informação sobre o MDM básico no Kaspersky Next Expert View (cloud), contate o Suporte Técnico. Os especialistas do Suporte Técnico responderão a todas as suas dúvidas sobre a instalação e o uso do MDM básico no Kaspersky Next Expert View (cloud).

A Kaspersky fornece suporte para o MDM básico no Kaspersky Next Expert View (cloud) durante o ciclo de vida útil (consulte a [página de ciclo de vida de suporte do produto](#)). Antes de entrar em contato com o Serviço de Suporte Técnico, leia as [regras de suporte](#).

Você pode entrar em contato com o Suporte Técnico de uma das seguintes maneiras:

- [Visitando o site de Suporte Técnico](#)
- Enviando uma solicitação para o Suporte Técnico a partir do [portal Kaspersky CompanyAccount](#)

Suporte técnico pelo Kaspersky CompanyAccount

O [Kaspersky CompanyAccount](#) é um portal para empresas que usam aplicativos Kaspersky. O portal Kaspersky CompanyAccount foi projetado para facilitar a interação entre os usuários e os especialistas da Kaspersky através de solicitações online. Você pode usar o Kaspersky CompanyAccount para monitorar o status e também armazenar um histórico das suas solicitações online.

Você pode registrar todos os funcionários da sua empresa com uma única conta no Kaspersky CompanyAccount. Uma única conta permite gerenciar centralmente solicitações de funcionários registrados enviadas para a Kaspersky, além de gerenciar os privilégios desses funcionários 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 do Suporte Técnico](#).

Fontes de informação sobre o aplicativo

Página da Web do MDM básico no Kaspersky Next Expert View (cloud) no site da Kaspersky

Na [página do MDM básico no Kaspersky Next Expert View \(cloud\)](#), é possível encontrar informações gerais sobre o aplicativo, seus recursos e parâmetros de operação.

A página da Web do MDM básico no Kaspersky Next Expert View (cloud) fornece um link para a eStore. Nela, você pode comprar ou renovar o aplicativo.

Página da Web do MDM básico no Kaspersky Next Expert View (cloud) na Base de Dados de Conhecimento

A *Base de Dados de Conhecimento* é uma seção do site de Serviço ao Cliente da Kaspersky.

Na [página do MDM básico no Kaspersky Next Expert View \(cloud\) na Base de Dados de Conhecimento](#), é possível encontrar artigos que contêm informações úteis, recomendações e respostas a perguntas frequentes sobre a compra, a instalação e o uso do aplicativo.

Os artigos da Base de Dados de Conhecimento podem responder a perguntas relacionadas não apenas ao MDM básico no Kaspersky Next Expert View (cloud), mas também a outros aplicativos da Kaspersky. Os artigos da Base de Dados de Conhecimento podem também incluir notícias do Suporte Técnico.

Ajuda

A ajuda do aplicativo contém arquivos de ajuda.

A ajuda de contexto dos plug-ins de administração para o MDM básico no Kaspersky Next Expert View (cloud) fornece informações sobre as janelas do Kaspersky Security Center: uma descrição das configurações do MDM básico no Kaspersky Next Expert View (cloud) e links para descrições das tarefas que usam essas configurações.

A ajuda completa dos aplicativos do Kaspersky Endpoint Security for Android e do Kaspersky Protection 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.

Agente de Rede

Um componente do Kaspersky Security Center que permite a interação entre o Servidor de Administração e os aplicativos da Kaspersky instalados em um nó específico da rede (estação de trabalho ou servidor).

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 antimalware

Bancos de dados que contêm informações sobre ameaças de segurança ao computador conhecidas pela Kaspersky no momento da liberação dos bancos de dados antimalware. As entradas nos bancos de dados antimalware permitem que o código malicioso seja detectado nos objetos verificados. Os bancos de dados antimalware são criados por especialistas da Kaspersky e atualizados de hora em 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 do serviço Apple Push Notification (APNs)

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 e iPadOS.

Código de ativação

Um código que você recebe ao comprar uma licença do Kaspersky Endpoint Security. Este código é necessário para ativar o aplicativo.

O código de ativação é uma sequência única de vinte letras e números no formato xxxxx-xxxxx-xxxxx-xxxxx.

Código de desbloqueio

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.

Contêiner corporativo

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 contêiner corporativo é criado no dispositivo móvel do usuário, os seguintes aplicativos corporativos são automaticamente instalados no contêiner corporativo: Google Play, Google Chrome, Downloads, Kaspersky Endpoint Security for Android e outros. Os aplicativos corporativos instalados no contêiner corporativo e as notificações sobre esses 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. Os aplicativos instalados no contêiner corporativo aparecem na lista de aplicativos comuns.

Contrato de Licença de 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 básico

Um modo de operação do dispositivo para dispositivos iOS pessoais. Esse modo de operação permite executar a proteção e o gerenciamento básico de dispositivos.

Controle de conformidade

Verificação de que as configurações de um dispositivo móvel e do Kaspersky Endpoint Security for Android cumprem com requisitos de segurança corporativos. Os requisitos de segurança corporativos regulam a utilização do dispositivo. Por exemplo, a proteção em tempo real deve estar ativada no dispositivo, os bancos de dados antimalware devem estar atualizados e a senha do dispositivo deve ser forte o suficiente. O Controle de conformidade é baseado em uma lista de regras. Uma regra de conformidade inclui os seguintes componentes:

- Critério de verificação de dispositivo (por exemplo, ausência de aplicativos proibidos no dispositivo)
- Intervalo de tempo alocado para o usuário 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 tempo definido (por exemplo, bloqueio do dispositivo)

Dispositivo corporativo

Um modo de operação do dispositivo para dispositivos Android de propriedade da empresa. Esse modo permite que você tenha controle total sobre todo o dispositivo e defina um conjunto estendido de configurações e recursos de segurança.

Dispositivo iOS MDM

Um dispositivo móvel iOS controlado pelo [iOS MDM Server](#).

Dispositivo pessoal

Um modo de operação para dispositivos Android pessoais. Esse modo de operação permite executar a proteção e o gerenciamento básico de dispositivos.

Dispositivo supervisionado

Dispositivo iOS ou iPadOS cujas configurações são monitoradas pelo Apple Configurator, um programa para a configuração de grupo de dispositivos iOS e iPadOS. 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 redefinirá, caso seja necessário. Um dispositivo supervisionado não pode ser sincronizado com o Apple Configurator instalado em outro computador.

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 não são supervisionados.

Estação de trabalho do administrador

O computador no qual o Kaspersky Next Expert View (cloud) foi implementado. Usando a estação de trabalho do administrador, com os plug-ins de gerenciamento de dispositivos móveis instalados, o administrador executa o gerenciamento centralizado de dispositivos móveis.

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 (KPSN)

A Kaspersky Private Security Network é uma solução que dá a usuários de dispositivos com aplicativos da Kaspersky instalados acesso a bancos de dados de reputação da Kaspersky Security Network e outros dados estatísticos sem enviar dados dos dispositivos à Kaspersky Security Network. O Kaspersky Private Security Network foi projetado para clientes corporativos que não podem participar do Kaspersky Security Network por algum dos seguintes motivos:

- Os dispositivos não estão conectados à Internet.
- A transmissão de quaisquer dados fora do país ou da LAN corporativa é proibida pela lei ou por políticas de segurança corporativas.

Kaspersky Security Network (KSN)

Uma infraestrutura de serviços online que fornece o acesso aos banco de dados da Kaspersky, que contém informações sobre a reputação de arquivos, recursos da Web e software constantemente atualizadas. A Kaspersky Security Network garante respostas mais rápidas dos aplicativos da Kaspersky quanto a ameaças, aprimora o desempenho de alguns componentes de proteção e reduz a probabilidade de ocorrência de falsos positivos.

Licença

Um direito por tempo limitado para usar o aplicativo, concedido de acordo com o Contrato de Licença de Usuário Final.

Malware

Um programa que infeta outros programas adicionando o seu código para obter controle dos arquivos infectados quando estes são executados. Esta definição simples permite identificar a ação principal executada por qualquer malware: infecção.

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 gerenciamento

Um perfil com um conjunto de configurações para conectar dispositivos móveis iOS ao Servidor de Administração. Um perfil de gerenciamento torna possível distribuir perfis de configuração iOS em modo de segundo plano usando o Servidor de MDM do iOS, além de receber informações de diagnóstico expandidas sobre dispositivos móveis. Um link para o perfil de gerenciamento precisa ser enviado a um usuário com a finalidade de permitir que o Servidor de MDM do iOS descubra e conecte o dispositivo móvel do usuário iOS.

Perfil de trabalho do Android

Um perfil independente que pode ser configurado em um dispositivo Android para assegurar a separação de dados relacionados ao trabalho de dados pessoais. O perfil de trabalho do Android permite que as organizações tenham controle total dos aplicativos e dados de trabalho em um dispositivo, enquanto os aplicativos e dados pessoais do usuário permanecem privados.

Período da licença

Um período durante o qual você tem acesso aos recursos do aplicativo e possui 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 móvel

Um componente dedicado que fornece a interface para gerenciar dispositivos móveis por meio do Kaspersky Next Expert View (cloud).

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.

Proteção básica

Um modo de operação do dispositivo para dispositivos iOS pessoais. Esse modo de operação permite executar a proteção contra ameaças e a detecção de jailbreak em dispositivos usando o Kaspersky Protection for iOS.

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 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 Administração virtual

Um componente do Kaspersky Security Center designado para gerenciamento do sistema de proteção de uma rede corporativa cliente.

O Servidor de Administração virtual é um caso particular de um Servidor de Administração secundário com as seguintes restrições em comparação com o Servidor de Administração físico:

- O Servidor de Administração virtual só pode ser criado no Servidor de Administração principal.
- O Servidor de Administração virtual usa o banco de dados do Servidor de Administração principal. Tarefas de backup e restauração de dados, bem como tarefas de verificação de atualização e download, não são compatíveis com um Servidor de Administração virtual.
- O Servidor virtual não é compatível com a criação de Servidores de Administração secundários (incluindo Servidores virtuais).

Servidor de MDM do iOS

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 da seu próprio cache (se o servidor proxy tiver o seu próprio cache). Em alguns casos, uma solicitação do usuário ou a resposta do servidor pode ser modificada pelo servidor proxy para determinado propósito.

Servidor Web do Kaspersky Security Center

Um componente do Kaspersky Security Center que é instalado em conjunto com o Servidor de Administração. O servidor Web foi projetado para a transmissão, por meio de uma rede, de pacotes de instalação independentes, perfis de gerenciamento do dispositivo e arquivos de uma pasta compartilhada.

Servidores de atualização da Kaspersky

Servidores HTTP(S) na Kaspersky a partir dos quais os aplicativos da Kaspersky baixam atualizações dos bancos de dados e módulos do aplicativo.

Solicitação de assinatura do certificado

Arquivo com as configurações de um Servidor de Administração, que é aprovado pela Kaspersky e enviado à Apple para obter um Certificado de APNs.

SSL

Um protocolo de criptografia de dados usado na Internet e em redes locais. O protocolo Secure Sockets Layer (SSL) é usado em aplicativos da Web para criar uma conexão segura entre o 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.

Informação sobre 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 Protection for iOS)
- [legal_notices_KMDPM.txt](#) [↗] (para o plug-in do Kaspersky Mobile Devices Protection and Management)
- [legal_notices_iOS_MDM.txt](#) [↗] (para o Servidor de MDM do iOS e o plug-in de configurações do Servidor de MDM do iOS)

Em dispositivos móveis, as informações sobre códigos de terceiros estão disponíveis na seção **Sobre o aplicativo** dos aplicativos móveis.

Avisos de marca registrada

As marcas comerciais e as marcas de serviço registradas são de propriedade de seus respectivos proprietários.

Adobe, Flash e PostScript são marcas comerciais registradas ou marcas comerciais da Adobe nos Estados Unidos e/ou outros países.

AMD64 é uma marca comercial ou marca registrada da Advanced Micro Devices, Inc.

Amazon, Amazon EC2, Amazon Web Services, AWS e AWS Marketplace são marcas comerciais da Amazon.com, Inc. ou de suas afiliadas.

Apache é uma marca registrada ou marca comercial da Apache Software Foundation nos Estados Unidos e/ou em outros países.

Apple, Apple Configurator, AirDrop, AirPlay, AirPort, AirPort Express, AirPrint, Aperture, App Store, Apple Music, Apple TV, Apple Watch, AppleScript, Bonjour, Face ID, FaceTime, FileVault, Find My, Find My Friends, Handoff, iBeacon, iBooks, iBooks Store, iCal, iCloud, iCloud Keychain, iMessage, iPad, iPadOS, iPhone, iPhoto, iTunes, iTunes Store, iTunes U, Keychain, macOS, OS X, Safari, Siri, Spotlight e Touch ID são marcas comerciais registradas da Apple Inc.

A palavra, marca e os logótipos Bluetooth são propriedade da Bluetooth SIG, Inc.

Aironet, 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.

Debian é uma marca registrada da Software in the Public Interest, Inc.

Dell Technologies, Dell, SecuriID e outras marcas comerciais são marcas comerciais registradas da Dell Inc. ou de suas subsidiárias.

F5 é uma marca registrada da F5 Networks, Inc. nos Estados Unidos e em outros países específicos.

Google, Android, Chrome, Chromebook, Chromium, Crashlytics, Firebase, Gmail, Google Analytics, Google Assistant, Google Chrome, Google Mail, Google Maps, Google Mobile, Google Play, Google Safe Browsing, Google SafeSearch, Google Translate, Nexus, SPDY e YouTube são marcas comerciais registradas da Google LLC.

HTC é uma marca comercial ou marca registrada nos EUA e/ou em outros países da HTC Corporation e suas afiliadas.

HUAWEI e EMUI são marcas comerciais registradas da Huawei Technologies Co., Ltd.

Juniper Networks, Juniper e JUNOS são marcas comerciais ou marcas registradas da Juniper Networks, Inc. nos Estados Unidos e em outros países.

Linux é a marca registrada de Linus Torvalds nos Estados Unidos e em outros países.

Mail.ru é uma marca comercial da Mail.ru LLC.

Microsoft, Active Directory, ActiveSync, Bing, Forefront, Microsoft Edge, Outlook, SQL Server, Tahoma, Windows, Windows Mobile, Windows Phone e Windows Server são marcas comerciais do grupo de empresas Microsoft.

MOTOROLA e o logotipo M estilizado são marcas comerciais ou marcas registradas da Motorola Trademark Holdings, LLC.

Mozilla e Firefox são marcas comerciais da Mozilla Foundation nos Estados Unidos e em outros países.

OPPO é uma marca comercial ou marca registrada da Guangdong OPPO Mobile Telecommunications Co., Ltd.

Oracle e JavaScript são marcas registradas da Oracle e/ou de suas afiliadas.

Red Hat e Red Hat Enterprise Linux são marcas comerciais da Red Hat Inc. ou de suas subsidiárias registradas nos Estados Unidos e em outros países.

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.

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 propriedade da Symbian Foundation Ltd.