kaspersky

Advanced MDM in Kaspersky Next Expert View (on-premise)

© 2026 AO Kaspersky Lab

Contents

Advanced MDM in Kaspersky Next Expert View (on-premise) help

What's new

Fixed issues

Comparison of solution features by management tool

Working in Kaspersky Next Expert View (on-premise)

- About Advanced MDM in Kaspersky Next Expert View (on-premise)
  - Distribution kit
  - About the Kaspersky Endpoint Security for Android app
  - About the Kaspersky Protection for iOS app
  - About Kaspersky Mobile Devices Protection and Management plug-in
  - Hardware and software requirements
    - Compatibility with other operating systems
  - Known issues and considerations
- Getting started
  - Solution architecture
  - Deployment scenarios
  - Deploying a mobile device management solution
    - Deploying Kaspersky Security Center Linux and Kaspersky Next Expert View (on-premise)
    - Deploying mobile management plug-ins
    - Configuring Administration Server settings for connecting mobile devices
      - Scenario: Configuring a connection gateway to connect mobile devices to Kaspersky Next Expert View (on-premise)
      - Adding installation packages to Administration Server repository
      - Adding a license key to the Administration Server repository
      - Installing Network Agent Linux
      - Configuring Kaspersky Security Center Linux Web Server settings
        - Configuring Web Server settings on a connection gateway (Network Agent for Linux)
        - Transferring the Web Server certificate to devices on the connection gateway
    - Migrating from Kaspersky Security Center Windows to Kaspersky Security Center Linux
      - Backing up and restoring Administration Server data using the klbackup utility
        - Backing up Administration Server data on a Windows device
        - Restoring Administration Server data on a Linux device
      - Backing up and restoring the iOS MDM Server data using the kliosbackup utility
  - Deploying an iOS device management system
    - About iOS device operating modes
    - About management profiles
    - Deploying Kaspersky Protection for iOS
      - About Kaspersky Protection for iOS
      - Installing Kaspersky Protection for iOS
      - Activating Kaspersky Protection for iOS
      - Updating Kaspersky Protection for iOS
      - Removing Kaspersky Protection for iOS

- Deploying a management system using the iOS MDM protocol
  - Deploying iOS MDM Server
    - Comparison of iOS MDM Server features depending on the management tools
    - Configuring an iOS MDM Server installation package
    - Installing iOS MDM Server using a remote installation task
    - Local installation of iOS MDM Server on a device via an installation package
    - Updating iOS MDM Server using a remote installation task or locally
    - Deleting iOS MDM Server using a remote uninstallation task
  - Viewing the list of installed iOS MDM Servers and configuring their settings
  - Configuring an iOS MDM Server certificate
  - Configuring a reserve iOS MDM Server certificate
  - Receiving or renewing an APNs certificate
  - Installing an APNs certificate on iOS MDM Server
  - Configuring access to Apple Push Notification service
  - iOS MDM Server events
  - Obtaining iOS MDM Server diagnostic data
- Deploying an Android device management system
  - About Android device operating modes
  - Using Firebase Cloud Messaging
  - Deploying Kaspersky Endpoint Security for Android
    - About the Kaspersky Endpoint Security for Android app
    - Installing Kaspersky Endpoint Security for Android
      - Creating the Kaspersky Endpoint Security for Android installation package
      - Manual installation of Kaspersky Endpoint Security for Android
      - Installing Kaspersky Endpoint Security for Android on corporate devices in a closed network
  - Permissions for Kaspersky Endpoint Security for Android
  - Starting and stopping Kaspersky Endpoint Security for Android
  - Activating Kaspersky Endpoint Security for Android
  - Updating Kaspersky Endpoint Security for Android
  - Removing Kaspersky Endpoint Security for Android
    - Permitting users to remove Kaspersky Endpoint Security for Android
    - Removal of Kaspersky Endpoint Security for Android by the user
    - Remote removal of Kaspersky Endpoint Security for Android on corporate devices
- Managing mobile devices in Kaspersky Next Expert View (on-premise)
  - Creating administration groups
  - Configuring policies
    - Creating a policy
    - Modifying a policy
    - Copying a policy
    - Moving a policy to another administration group
    - Viewing the list of policies
    - Viewing the policy distribution results
    - Managing revisions to policies
    - Restricting permissions to configure policies
    - Configuring role-based access control
    - Configuring policy profiles
    - Deleting a policy

- Connecting mobile devices to Kaspersky Next Expert View (on-premise)
  - Direct connection of Android devices to Kaspersky Security Center
  - Moving unassigned mobile devices to administration groups
  - Actions on mobile devices to connect to Administration Server
- Configuring synchronization settings
- Managing certificates of mobile devices
  - Reissuing the mobile Administration Server certificate
  - Configuring certificate issuance rules
  - Issuing mobile device certificates
  - Renewing mobile device certificates
  - Deleting mobile device certificates
  - Integration with Public Key Infrastructure
  - Viewing the list of mobile device certificates

Configuration and management

- Control
  - Configuring restrictions
    - Configuring restrictions for personal Android devices
    - Configuring iOS MDM device restrictions
  - Configuring user access to websites
    - Configuring access to websites on Android devices
    - Configuring access to websites on iOS MDM devices
  - Compliance Control
    - Compliance Control of Android devices
    - Compliance Control of iOS MDM devices
  - App Control
    - App Control on Android devices
    - App Control on iOS MDM devices
  - Call Control on Android devices
  - Mobile device protection levels
  - Software inventory on Android devices
- Protection
  - Configuring anti-malware protection on Android devices
  - Protecting Android devices on the internet
  - Protection of data on a stolen or lost device
    - Sending commands to a lost or stolen mobile device
    - Unlocking a mobile device
  - Configuring the device unlock password strength
    - Configuring a strong unlock password for an Android device
    - Configuring a strong unlock password for an iOS MDM device
  - Configuring a virtual private network (VPN)
    - Configuring VPN on Android devices (only Samsung)
    - Configuring VPN on iOS MDM devices
    - Configuring Per App VPN for iOS system apps
    - Configuring Per App VPN for third-party iOS apps
  - Configuring Firewall on Android devices (only Samsung)
  - Protecting Kaspersky Endpoint Security for Android against removal
  - Detecting hacked devices

- Configuring a global HTTP proxy on iOS MDM devices
- Adding security certificates to iOS MDM devices
- Adding a SCEP profile to iOS MDM devices
- Restricting SD card usage (only Samsung)

Management of mobile devices

- Remote access to Android devices
  - Installing and configuring a TURN server
  - Specifying remote control server settings in Kaspersky Security Center
  - Starting a remote control session
- Managing Android devices
  - Corporate devices
    - Restricting Android features on devices
    - Configuring kiosk mode for Android devices
    - Connecting to a NDES/SCEP server
  - Enabling certificate-based authentication of devices
  - Creating a mobile application package for Android devices
  - Sending files to Android devices
  - Viewing information about an Android device
  - Disconnecting an Android device from management
- Managing iOS MDM devices
  - Signing management profiles with a certificate
  - Adding a configuration profile
  - Installing a configuration profile on a device
  - Removing a configuration profile from a device
  - Configuring managed apps
  - Installing an app on a mobile device
  - Updating an app installed on a device
  - Removing an app from a device
  - Configuring roaming on an iOS MDM mobile device
  - Viewing information about an iOS MDM device
  - Configuring kiosk mode for iOS MDM devices
  - Disconnecting an iOS MDM device from management

Management of mobile device settings

- Configuring connection to a Wi-Fi network
  - Connecting Android devices to a Wi-Fi network
  - Connecting iOS MDM devices to a Wi-Fi network
- Configuring email
  - Configuring a mailbox on iOS MDM devices
  - Configuring an Exchange mailbox on iOS MDM devices
  - Configuring an Exchange mailbox on Android devices
- Configuring protection levels in Kaspersky Security Center
- Managing app configurations
  - Managing Google Chrome settings
  - Managing Exchange ActiveSync for Gmail
  - Configuring other apps
- Managing app permissions
- Creating a report on installed mobile apps

Installing root certificates on Android devices
Configuring notifications for Kaspersky Endpoint Security for Android
Selecting the download manager for Android devices
Connecting iOS MDM devices to AirPlay
Connecting iOS MDM devices to AirPrint
Configuring the Access Point Name (APN)
Configuring APN on Android devices (only Samsung)
Configuring APN on iOS MDM devices
Corporate container
About corporate containers
Configuring a corporate container
Unlocking the corporate container
Adding an LDAP account
Adding a contacts account
Adding a calendar account
Configuring a calendar subscription
Configuring SSO
Managing Web Clips
Setting a wallpaper
Adding fonts
Working with commands for mobile devices
Commands for mobile devices
Sending commands
Viewing the statuses of commands in the command history
Managing the app by using third-party EMM solutions (Android only)
Getting started
How to install the app
Protecting devices on the internet
How to activate the app
How to connect a device to Kaspersky Security Center
Silent mode
AppConfig file
Participating in Kaspersky Security Network
Information exchange with Kaspersky Security Network
Enabling and disabling the use of Kaspersky Security Network
Using Kaspersky Private Security Network
Samsung Knox
Installation of Kaspersky Endpoint Security for Android via Knox Mobile Enrollment
Creating a Knox profile
Adding devices in Knox Mobile Enrollment
Installing the app
Configuring Knox
Restricting SD card usage in Knox
Configuring VPN in Knox
Configuring an Exchange mailbox in Knox
Configuring APN in Knox
Configuring Firewall in Knox

Using the Kaspersky Endpoint Security for Android app
App features
Main window at a glance
Status bar icon
Device scan
Running a scheduled scan
Changing the Protection mode
Anti-malware database updates
Scheduled database update
Things to do if your device gets lost or stolen
Web Protection
Protection against unwanted calls
Get Certificate
Synchronizing with Kaspersky Security Center
Allowing remote access to your device
Activating the Kaspersky Endpoint Security for Android app without Kaspersky Security Center
Installing the app on corporate devices
Configuring the app on corporate devices running Android 7 and later
Configuring the app on corporate devices running Android 5-6
Installing root certificates on the device
Installing and using mail and VPN certificates on the device
Enabling accessibility on Android 13 or later
Updating the app
Removing the app
Applications with a briefcase icon
Knox app
Using the Kaspersky Protection for iOS app
App features
Installing the app
Activating the app
Activating the app with an activation code
Main window at a glance
Updating the app
Using diagnostics to troubleshoot issues
Removing the app
Application licensing
About the End User License Agreement
About the license
Viewing license information
About the subscription
About the license key
About the activation code
About the key file
Data provision in Kaspersky Endpoint Security for Android
Data provision in Kaspersky Protection for iOS

Contact Technical Support
- How to get technical support
- Technical support via Kaspersky CompanyAccount

Sources of information about the application

Glossary
- Activating the application
- Activation code
- Administration group
- Administration Server
- Administrator's workstation
- Android Work Profile
- Anti-malware databases
- Apple Push Notification service (APNs) certificate
- Basic control
- Basic protection
- Certificate Signing Request
- Compliance Control
- Corporate container
- Corporate device
- Device administrator
- End User License Agreement
- Group task
- IMAP
- Installation package
- iOS MDM device
- iOS MDM Server
- Kaspersky categories
- Kaspersky Private Security Network (KPSN)
- Kaspersky Security Center Administrator
- Kaspersky Security Center Web Server
- Kaspersky Security Network (KSN)
- Kaspersky update servers
- Key file
- License
- License term
- Malware
- Management profile
- Manifest file
- Mobile management plug-in
- Network Agent
- Personal device
- Phishing
- Policy
- POP3
- Proxy server
- Quarantine
- SSL

Standalone installation package
Subscription
Supervised device
Unlock code
Virtual Administration Server
Information about third-party code
Trademark notices

Advanced MDM in Kaspersky Next Expert View (on-premise) help

	**What's new** Find out what's new in the latest solution release.		**Set up device protection** Manage mobile device protection remotely. Features include Anti-Malware, Web Protection, Anti-Theft, and more.
	**Distribution kit** Learn about various components, depending on the chosen solution version.		**Set up device settings** Manage mobile devices remotely: configure Wi-Fi, VPN, email, root certificates on Android devices, Web Clips, and more.
	**Deployment** Learn how to deploy the solution in your organization and configure management systems for Android devices and iOS devices.		**Set up device control** Monitor mobile devices remotely, including configuring restrictions, user access to websites, Compliance Control, App Control, and more.
	**Commands** Remotely manage mobile devices with mobile commands. Lock device, Wipe corporate data, Locate device, Take photos, Sound alarm, and more.		**Set up corporate devices** Manage Android operating system restrictions, Google Chrome settings, Kiosk mode, and more.
	**Corporate container** Discover the benefits of corporate container and learn how to configure it for your device.		**Other** Manage the security of your Android devices using a third-party EMM solution, or install our solution via Knox for enhanced security on Samsung devices.
	**Corporate App Catalog** Create a customized corporate app catalog and use a browser to download apps from the catalog to users' devices.		

What's new

Version 10.0

In this release, we added new features to the Kaspersky Mobile Devices Protection and Management plug-in for Kaspersky Next Expert View (on-premise):

- Android 17 is now supported.
- You can now use the Call Control feature to configure Kaspersky Endpoint Security for Android to protect users against fraudulent, spam, and other unwanted calls.

Fixed issues

The table below lists all the issues found in previous versions of Advanced MDM in Kaspersky Next Expert View (on-premise) that are fixed in the current version.

List of issues fixed in Advanced MDM in Kaspersky Next Expert View (on-premise) 10.0

Issue ID	Issue description
10216978	If the server connection step was skipped during the installation of Kaspersky Endpoint Security for Android, and the link for connecting the mobile device to the virtual Administration Server was entered later in the synchronization settings, then the first synchronization was performed with the virtual Administration Server, but subsequent synchronizations were performed with the primary Administration Server.
10079161	On personal Android devices, the system statistics on use of location services were updated after changing the cellular data type even if the location was not requested.
9984204	On some Google Pixel devices, Kaspersky Endpoint Security for Android had stability issues if the app was deployed in an Android work profile created by a third-party EMM (Enterprise Mobility Management) solution.
9595795	An issue about detected legitimate software cannot be hidden from the list of issues, even if this software was not classified as malicious and the **Detect adware, autodialers, and legitimate apps that intruders can use to compromise the user's device and data** check box was cleared in both the **Scan** and **Real-time protection** settings of the policy.
9715410	Corporate Android devices disconnected from a configured Wi-Fi network after receiving a command from Kaspersky Security Center and automatically reconnected after a few seconds.
9978463	Only three QR codes could be displayed at a time after completing the Mobile device connection wizard, which made it impossible to connect devices with all supported operating systems at once within a single session.
9821628	The error description about an out-of-range Web Server port value was unclear (`Assertion "nTmpPort && nTmpPort <= 65535" failed`).
9978844	Some Android app packages could not be uploaded to the Kaspersky Security Center server because reading the resource file header from the APK file finished with an error.
9844707	Kaspersky Security Center and FCM (Firebase Cloud Messaging) interacted directly, even if a proxy server was configured.
9669181	When issuing a mail or VPN certificate for Android devices, the option to specify a certificate alias was mentioned, but this option is not available.
10142672	When configuring VPN for iOS MDM devices, specifying the HTTP or HTTPS protocol in the **Domain** field was mandatory.

Comparison of solution features by management tool

Availability of features by management tool

Functionality	Advanced MDM in Kaspersky Next Expert View (on-premise)	Basic MDM in Kaspersky Next Expert View (on-premise)	Basic MDM in Kaspersky Next Expert View (cloud)
	Kaspersky Next Expert View	Kaspersky Next Expert View	Kaspersky Next Expert View
Mobile device management			
Android device management	✓	✓	✓
iOS device management	✓	✓	✓
Aurora device protection	✓	—	—
Deployment			
Add devices using an App Store link	✓	✓	✓
Add devices by creating an installation package	✓	✓	—
Add devices directly to the administration group after devices connect	✓	✓	✓
Create policies divided by operating modes	✓	✓	✓
Send commands to mobile devices	✓	✓	✓ Limited set of commands
Remove mobile devices from Kaspersky Security Center	✓	✓	✓
Certificate management			
Issue mail certificates	✓	✓	✓ Configuring settings for issuing is not available
Issue VPN certificates	✓	✓	✓ Configuring settings for issuing is not available
Issue mobile certificates	✓	✓	✓
Issue mobile certificates through Administration Server tools	✓	✓	✓
Specify certificate files	✓	✓	✓
Integrate with Public Key Infrastructure (PKI)	✓	✓	—
Policy management			
Role-based access to configuring group policies	✓	✓	✓
Configure mobile device synchronization with Kaspersky Security Center	✓	✓	✓
Configure malware scans on mobile devices	✓	✓	✓
Configure anti-malware database updates	✓	✓	✓
Configure device protection on the internet	✓	✓	✓

Configure protection of stolen or lost device data	✓	✓	✓
Configure the device unlock password strength	✓	✓	✓ Limited set of settings
Configure user access to websites	✓	✓	✓
Configure App Control	✓	✓ Only for Android	✓ Only for Android
Configure Compliance Control	✓	✓ Only for Android	✓ Only for Android
Configure Call Control	✓ Only for Android	—	—
Configure permission granting rules for installed apps	✓	—	—
Configure corporate containers	✓	✓ Limited set of settings	✓ Limited set of settings
Configure device feature restrictions	✓	✓ Limited set of settings	✓
Configure connections to Wi-Fi networks	✓	✓	✓
Configure VPN	✓	✓ For iOS, Per App VPN and IKEv2 protocol are not supported. For Android, VPN can be configured via Knox only.	✓ For iOS, Per App VPN and IKEv2 protocol are not supported. For Android, VPN can be configured via Knox only.
Manage app configurations	✓	—	—
Send files to Android devices	✓	—	—
Samsung Knox	✓	✓ Limited set of settings	✓
Remote control for Android	✓	—	—
iOS MDM Server features			
Install and configure iOS MDM Server	✓	✓	✓ Only applicable settings
Update and remove iOS MDM Server	✓	✓	—
Issue APNs certificates	✓	✓	✓
Connect iOS MDM devices	✓	✓	✓
Sign a management profile by a certificate	✓	✓	—
iOS MDM Server events	✓	✓	✓
Add a configuration profile	✓	✓	✓
Other features			
Global acceptance of EULA in Kaspersky Security Center	✓	✓	✓
Configure Kaspersky Private Security Network	✓	✓	—

Working in Kaspersky Next Expert View (on-premise)

This Help section describes protection and management of mobile devices by using Kaspersky Next Expert View (on-premise).

About Advanced MDM in Kaspersky Next Expert View (on-premise)

Advanced MDM in Kaspersky Next Expert View (on-premise) is an integrated solution for protecting and managing corporate mobile devices as well as personal mobile devices used by company employees for corporate purposes.

Distribution kit

The Advanced MDM in Kaspersky Next Expert View (on-premise) distribution kit may include different components, depending on the chosen solution version. For information about the compatibility of the plug-in version and Kaspersky Security Center versions, see the hardware and software requirements.

Mobile device management in Kaspersky Next Expert View (on-premise)

> This component is compatible with Kaspersky Security Center Linux 15.1. For information on the version compatible with Kaspersky Security Center Windows, see the Kaspersky Secure Mobility Management 4.1 Help.

- `on_prem_ksm_policies_<version>.zip`

  Archive that contains the files required for installation of the Kaspersky Mobile Devices Protection and Management plug-in:

  - `plugin.zip`

    Archive that contains the Kaspersky Mobile Devices Protection and Management plug-in.

  - `signature.txt`

    File that contains the signature for the Kaspersky Mobile Devices Protection and Management plug-in.

iOS MDM Server settings plug-in

This component is compatible with Kaspersky Security Center Linux 15.1. For information on the version compatible with Kaspersky Security Center Windows, see the Kaspersky Secure Mobility Management 4.1 Help.

- `on_prem_iosmdm_<version>.zip`

  Archive that contains the files required for installation of the iOS MDM Server settings plug-in:

  - `plugin.zip`

    Archive that contains the iOS MDM Server settings plug-in.

  - `signature.txt`

    File that contains the signature for the iOS MDM Server settings plug-in.

iOS MDM Server

This component is compatible with Kaspersky Security Center Linux 15.1. For information on the version compatible with Kaspersky Security Center Windows, see the Kaspersky Secure Mobility Management 4.1 Help.

- `kliosmdm-<architecture>-<version>-<package manager>_<language>.tar.gz`

  Archive that contains the files required for installation of iOS MDM Server, depending on the package manager and architecture:

  - `kliosmdm.kpd`

    iOS MDM Server description file.

  - `akinstall.sh`

    Script that lets you automate installation of iOS MDM Server.

  - `kliosmdm-<version>.<architecture>.rpm` or `kliosmdm_<version>_<architecture>.deb`

    iOS MDM Server installation package.

  - `kpd.loc/`

    Folder with CFG files specifying paths to End User License Agreements.

  - `license/`

    Folder with End User License Agreements and Privacy Policy in different languages in TXT format.

Kaspersky Endpoint Security for Android app

- `<version>_sc_package.zip`

  Archive that contains the files required for installing the Kaspersky Endpoint Security for Android app by creating installation packages:

  - `installer.ini`

    Configuration file that contains Administration Server connection settings.

  - `kesandroid<version>_<languages>_Prod_Release.apk`

    Android package file of the Kaspersky Endpoint Security for Android app.

  - `eula/`

    Folder with End User License Agreements in different languages in TXT format.

  - `kpd.loc/`

    INI files specifying paths to End User License Agreements.

  - `ksm.kpd`

    Application description file.

File with Corporate App Catalog

`Install_<version>.exe`—Distribution package of Corporate App Catalog. The package includes the following components:

- Corporate App Catalog
- Corporate App Catalog Management Console
- Apache server

For more information about installing Corporate App Catalog, please refer to the *Corporate App Catalog Help*.

Documentation

- Help for Advanced MDM in Kaspersky Next Expert View (on-premise).

About the Kaspersky Endpoint Security for Android app

The Kaspersky Endpoint Security for Android app ensures the protection of mobile devices against web threats, viruses, and other programs that pose threats.

The Kaspersky Endpoint Security for Android includes the following features:

- **Anti-Malware**. This component detects and neutralizes threats on the device by using the anti-malware databases and the Kaspersky Security Network cloud service. Anti-Malware includes the following components:
  - **Protection**. It detects threats in open files, scans new apps, and prevents device infection in real time.
  - **Scan**. It is started on demand for the entire file system, only for installed apps, or only for a selected file or folder.
  - **Update**. It lets you download new anti-malware databases for the app.
- **Anti-Theft**. This component protects the information on the device against unauthorized access in case the device is lost or stolen. This component lets you send the following commands to the device:
  - **Locate device**. Get the coordinates of the device's location.
  - **Sound alarm**. Make the device sound a loud alarm.
  - **Wipe corporate data**. Erase corporate data to protect sensitive company information.
- **Web Protection** and **Web Control**. Web Protection blocks malicious websites designed to spread malicious code. Web Protection also blocks fake (phishing) websites designed to steal the user's confidential data (for example, passwords for online banking or e-money systems) and access the user's financial info. Web Protection uses the Kaspersky Security Network cloud service to scan websites before they open. After scanning, Web Protection allows trustworthy websites to load and blocks malicious websites. Web Control allows website filtering by categories defined in the Kaspersky Security Network cloud service. This lets the administrator restrict user access to certain categories of web pages (for example, Gambling, lotteries, sweepstakes or Internet communication).
- **App Control**. This component lets you install recommended and required apps to an Android device as well as remove blocked apps that violate corporate security requirements.
- **Compliance Control**. This component lets you check managed devices for compliance with corporate security requirements and impose restrictions on certain functions of non-compliant devices.
- **Call Control**. This component lets you protect managed devices against fraudulent, spam, and other unwanted calls.

You can configure the components of the Kaspersky Endpoint Security for Android app in Kaspersky Next Expert View (on-premise) by defining the corresponding policy settings.

About the Kaspersky Protection for iOS app

The Kaspersky Protection for iOS app ensures protection of mobile devices against phishing and web threats.

The Kaspersky Protection for iOS app offers the following key features:

- **Web Protection**. This component blocks malicious websites designed to spread malicious code. Web Protection also blocks fake (phishing) websites designed to steal confidential data of the user (for example, passwords for online banking or e-money systems) and access the user's financial info. Web Protection scans websites before you open them, by using the Kaspersky Security Network cloud service. After scanning, Web Protection allows trustworthy websites to load and blocks malicious websites. You can configure this component in Kaspersky Next Expert View (on-premise) by defining the settings of group policies.

- **Jailbreak detection**. When Kaspersky Protection for iOS detects a jailbreak, it displays a critical message and informs you about the issue.

About Kaspersky Mobile Devices Protection and Management plug-in

The Kaspersky Mobile Devices Protection and Management plug-in lets you manage mobile devices and mobile apps installed on them in Kaspersky Next Expert View (on-premise). The Kaspersky Mobile Devices Protection and Management plug-in can be used to:

- Create group security policies for mobile devices.

- Remotely configure the settings of the Kaspersky Endpoint Security for Android app on users' mobile devices.

- Receive reports and statistics on the operation of the Kaspersky Endpoint Security for Android mobile app on users' devices.

- Remotely configure iOS devices connected using the iOS MDM protocol (hereinafter referred to as "iOS MDM devices") and iOS devices with the Kaspersky Protection for iOS app.

- Remotely configure Aurora devices with the Kaspersky Endpoint Security for Aurora app.

The Kaspersky Mobile Devices Protection and Management plug-in can be installed when configuring Kaspersky Next Expert View (on-premise). For more information about deployment scenarios, see Deploying mobile management plug-ins.

Hardware and software requirements

This section lists the hardware and software requirements for the administrator's computer that is used to deploy apps on mobile devices, as well as the mobile device operating systems supported by Advanced MDM in Kaspersky Next Expert View (on-premise).

This article lists the software versions on which the application has been tested and for which it is guaranteed to work correctly. The application may also work with other software versions, but those configurations have not undergone a full testing cycle and are not included in the list of guaranteed-supported versions.

Hardware and software requirements for the administrator's computer

The Kaspersky Security Center Linux server host must meet the following requirements:

- Software requirements:
  - Administration Server of Kaspersky Security Center Linux 15.2 or later
  - Web Console of Kaspersky Security Center Linux 15.2 or later
  - Kaspersky Mobile Devices Protection and Management Plug-in 10.53 or later
  - iOS MDM Server for Linux 15.2 or later
  - iOS MDM Server settings Plug-in 15.2 or later
- Hardware requirements:
  - To deploy Advanced MDM in Kaspersky Next Expert View (on-premise), the hardware requirements for Kaspersky Security Center must be met.
  - For iOS MDM Server:
    - CPU with an operating frequency of 1 GHz or higher. For a 64-bit operating system, the minimum CPU frequency is 1.4 GHz
    - RAM: 4 GB
    - Available disk space: 4 GB

Version compatibility

The following version combinations are supported:

- Kaspersky Mobile Devices Protection and Management Plug-in version 10.53 supports only Kaspersky Security Center Linux 15.1 or later.
- Kaspersky Mobile Devices Protection and Management Plug-in versions 10.54 or later support only Kaspersky Security Center Linux 15.2 or later.

The following versions are fully compatible:

- Kaspersky Mobile Devices Protection and Management Plug-in 10.53 and Kaspersky Security Center Linux 15.1 or later.
- Kaspersky Mobile Devices Protection and Management Plug-in 10.54 and Kaspersky Security Center Linux 15.2 or later.
- Kaspersky Mobile Devices Protection and Management Plug-in 10.55 and Kaspersky Security Center Linux 15.3 or later.

- Kaspersky Mobile Devices Protection and Management Plug-in 10.56 and Kaspersky Security Center Linux 16.1 or later.
- Kaspersky Mobile Devices Protection and Management Plug-in 10.57 and Kaspersky Security Center Linux 16.2 or later.
- Kaspersky Mobile Devices Protection and Management Plug-in 10.58 and Kaspersky Security Center Linux 16.3 or later.

Hardware and software requirements for Kaspersky Endpoint Security for Android

For Kaspersky Endpoint Security for Android, the mobile device must meet the following requirements:

- Smartphone or tablet with a screen resolution of 320x480 pixels or higher
- 65 MB of free disk space in the main memory of the device
- Operating system (excluding 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
  - Android 17
- x86, x86-64, Arm5, Arm6, Arm7, or Arm8 processor architecture
- The app can be installed only in the main memory of the device

Hardware and software requirements for Kaspersky Protection for iOS

For Kaspersky Protection for iOS, the mobile device must meet the following requirements:

- Operating system:
  - iOS:
    - iOS 15.x
    - iOS 16.x
    - iOS 17.x
    - iOS 18.x
    - iOS 26.2, 26.3, 26.5
  - iPadOS:
    - iPadOS 15.x
    - iPadOS 16.x
    - iPadOS 17.x
    - iPadOS 26.2, 26.5
- Internet connection

Hardware and software requirements for a management profile

For a management profile, the mobile device must meet the following requirements:

- Operating system:
  - 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, 26.5
  - iPadOS:
    - iPadOS 13.x
    - iPadOS 14.x
    - iPadOS 15.x
    - iPadOS 16.x
    - iPadOS 17.x
    - iPadOS 26.2, 26.4, 26.5
- Internet connection

Compatibility with other operating systems

Advanced MDM in Kaspersky Next Expert View (on-premise) supports protection and management of mobile devices running other operating systems using the Kaspersky Endpoint Security for Android app.

The table describes the compatibility of the Kaspersky Endpoint Security for Android app versions with other operating system versions.

Compatibility of Kaspersky Endpoint Security for Android with other operating systems

Kaspersky Endpoint Security for Android version	Operating system version	Limitations
10.57.1.37	kvadraOS 1.26 (Enterprise)	Known issues and considerations

Known issues and considerations

The following known issues are non-critical for the operation of the solution.

Known issues when connecting mobile devices to Kaspersky Security Center

- The link for connecting mobile devices or the link to download the installation package on Web Server HTTPS port 8061 may fail to open in the same browser as Kaspersky Next Expert View (on-premise) due to the `NET::ERR_CERT_AUTHORITY_INVALID` error. This may happen if Web Server uses a self-signed certificate. To open the link, copy and paste it in a different browser or replace the self-signed certificate with a custom certificate issued by the trusted certification authority in the Administration Server properties, on the **General** tab, in the **Web Server** section.

Known issues when managing mobile devices

- If you edit the **Name** and **Description** fields on the **General** tab of the device properties, the changes will not be displayed in the list of mobile devices connected to Kaspersky Security Center due to technical limitations.
- The **Force synchronization** button and the **Do not disconnect from the Administration Server** check box in the device properties window are not supported by mobile devices. Use the **Synchronize device** command to force synchronization of an Android device or an iOS MDM device.
- In the list of managed mobile devices, the displayed total storage capacity of personal iOS devices operating in basic protection mode is rounded up.

Known issues of Kaspersky Protection for iOS

- The Kaspersky Protection for iOS app does not operate properly when a VPN client with an active VPN connection is running on the same mobile device.
- For stable operation of the Kaspersky Protection for iOS app, the outdated Kaspersky Security for iOS app must be uninstalled from the device.
- On some iOS devices, background tasks (for example, synchronization with Kaspersky Security Center or replacement of the activation key) may be executed later than expected if the user quit Kaspersky Protection for iOS by swiping up in the App Switcher. This is due to iOS background execution limits. To force execution, reopen the app.

  To increase the chances that background tasks will run, ensure the following:

  - The Kaspersky Protection for iOS app is opened in the App Switcher.
  - Low data mode is turned off and the device is connected to a Wi-Fi network or a hotspot.
  - The device is connected to a high-quality network.
  - The device is charging.
  - The Personal Hotspot is turned off.

Known issues when installing Kaspersky Endpoint Security for Android

- Kaspersky Endpoint Security for Android is installed only in the main memory of the device.
- On devices running Android 7, an error may occur during attempts to disable administrator rights for Kaspersky Endpoint Security for Android in the device settings if Kaspersky Endpoint Security for Android is prohibited from overlaying other windows. This issue is caused by a well-known defect in Android 7.
- Kaspersky Endpoint Security for Android on devices running Android 7.0 or later does not support multi-window mode.

- Kaspersky Endpoint Security for Android does not work on Chromebook devices running the Chrome operating system.
- Kaspersky Endpoint Security for Android does not work on devices running Android (Go edition) operating systems.
- When using the Kaspersky Endpoint Security for Android app with third-party EMM systems without connecting to Kaspersky Security Center, only the Anti-Malware and Web Protection components are available. The administrator can configure the settings of Anti-Malware and Web Protection in the EMM system console. In this case, notifications about app operation are available only in the interface of the Kaspersky Endpoint Security for Android app (Reports).
- When installing Kaspersky Endpoint Security for Android on a corporate device using ADB, if you set a screen unlock password on the device after you reset it to factory settings, you must reset the device to factory settings again before installing the app.
- On personal devices and devices with a corporate container running Android 15, users can create their own private space. Kaspersky Endpoint Security for Android cannot scan apps, photos, and other files stored in a private space. Web Protection, Web Control, and App Control do not work for apps installed in a private space. Installation of Kaspersky Endpoint Security for Android in a private space is not supported.

Known issues when updating Kaspersky Endpoint Security for Android

- You can upgrade Kaspersky Endpoint Security for Android only to a more recent version of the app. Kaspersky Endpoint Security for Android cannot be downgraded to an older version.

Known issues when removing Kaspersky Endpoint Security for Android

- Before removing Kaspersky Endpoint Security for Android from the device, clear the **Block system apps** check box in the **App Control** settings of the policy or disable App Control.

Known issues affecting Wi-Fi

- On iOS MDM devices, if you disable automatic connection to an existing Wi-Fi network in the policy settings, you will not be able to enable automatic connection to this network again. This is due to an issue known to Apple.
- On iOS MDM devices running iOS 18 and iOS 26, if the **Personal network (any)** network protection type is selected in the Wi-Fi policy settings, the device may not be automatically connected to a Wi-Fi network secured by WEP, WPA, or WPA3 protocol, even if the **Connect automatically** check box is selected. To automatically connect to a Wi-Fi network secured by a required protocol, specify that protocol as the network security type.

Known issues when configuring VPN

- If you install an app with configured Per App VPN on an iOS MDM device and then disable VPN in the policy and synchronize this device, the "App will use a VPN for network access" message may still appear in the configuration profile information. For up-to-date information about the app, reinstall or update it.

Known issues affecting Anti-Malware

- Due to technical limitations, Kaspersky Endpoint Security for Android cannot scan files with a size of 2 GB or more. During a scan, the app skips such files without notifying you that such files were skipped.
- To further analyze a device for new threats for which information has not yet been added to anti-malware databases, you must enable the use of Kaspersky Security Network. *Kaspersky Security Network (KSN)* is an infrastructure of cloud services providing access to the Kaspersky online knowledge base with information about the reputation of files, web resources, and software. To use KSN, the mobile device must be connected to the internet.
- In some cases, updating anti-malware databases from the Administration Server on a mobile device may fail. In this case, run the anti-malware database update task on the Administration Server.
- On some devices, Kaspersky Endpoint Security for Android does not detect devices connected over USB OTG. It is not possible to run a malware scan on such devices.
- On devices running Android 11 or later, the Kaspersky Endpoint Security for Android app can't scan the "Android/data" and "Android/obb" folders and detect malware in them due to technical limitations.
- On devices running Android 11 or later, the user must grant the "Allow access to manage all files" permission.
- On devices running Android 7 or later, the configuration window for the malware scan run schedule might display incorrectly (management elements are not shown). This issue is caused by a well-known defect in Android 7.
- On devices running Android 7, real-time protection in extended mode does not detect threats in files stored on an external SD card.
- On devices running Android 6, Kaspersky Endpoint Security for Android does not detect the downloading of a malicious file to the device memory. A malicious file may be detected by Anti-Malware when the file is run or during a malware scan of the device. This issue is caused by a well-known defect in Android 6. To ensure device security, it is recommended to configure scheduled malware scans.

Known issues affecting Web Protection and Web Control

- Web Control on Android devices is supported only by Google Chrome, HUAWEI Browser, Samsung Internet, and Yandex Browser.
- The Custom Tabs feature is supported by Google Chrome, HUAWEI Browser, and Samsung Internet.

- Web Control for HUAWEI Browser, Samsung Internet Browser, and Yandex Browser does not block sites on a mobile device if a corporate container is used and Web Protection is enabled only for the corporate container.
- For Web Protection and Web Control to work, you must enable the use of Kaspersky Security Network. Web Control blocks websites based on KSN data on the reputation and category of websites.
- Forbidden websites may remain unblocked by Web Control on devices running Android 6 with Google Chrome version 51 (or any earlier version) installed if the website is opened in the following ways (this issue is caused by a well-known defect in Google Chrome):
  - From search results.
  - From the bookmarks list.
  - From the search history.
  - Using the web address autocomplete function.
  - Opening the website in a new tab in Google Chrome.
- Forbidden websites may remain unblocked in Google Chrome version 50 (or any earlier version) if the website is opened from Google search results while the **Merge Tabs and Apps** feature is enabled in the browser settings. This issue is caused by a well-known defect in Google Chrome.
- Websites from blocked categories may remain unblocked in Google Chrome if the user opens them from third-party apps, for example, from an IM client app. This issue is related to how the Accessibility service works with the Chrome Custom Tabs feature.
- Forbidden websites may remain unblocked in Samsung Internet if the user opens them in background mode from the context menu or from third-party apps, for example, from an IM client app.
- Kaspersky Endpoint Security for Android must be set as an Accessibility feature to ensure proper functioning of Web Protection and Web Control.
- On some Xiaomi devices, the "Display pop-up window" and "Display pop-up windows while running in the background" permissions should be granted for Web Protection and Web Control to work.
- Allowed websites may be blocked in Samsung Internet in the **Allow only listed websites** Web Control mode when the page is refreshed. Websites are blocked if a regular expression contains advanced settings (for example, `^https?://example.com/pictures/`). It is recommended to use regular expressions without additional settings (for example, `^https?://example.com`).
- If Web Control is set to **Prohibit all websites**, Kaspersky Endpoint Security for Android does not block search in the Google Search widget. Instead, it blocks user access to the search results.
- In a corporate container, if Web Control is set to **Prohibit all websites**, Kaspersky Endpoint Security for Android endlessly reloads the Google Chrome home page, blocks the browser, and interferes with the device.
- In Yandex Browser and Samsung Internet, malicious and phishing URLs may remain unblocked. This is because only the website domain is scanned. If it is a malicious or phishing domain, Web Protection blocks the threat. If the domain is not classified as malicious or phishing, the specific URL is not blocked.
- The list of allowed websites created in the **Web Control** card does not display in Safari on iOS MDM devices running iOS 26 or earlier. However, Web Control still works and users can access only allowed websites. To display allowed websites in Safari, select the **Add to bookmarks on device** check box in the **Web Control** card and specify the bookmark name for each website from the list.

- If the **Check full URL when using Custom Tabs** option is enabled in the Web Control section of the policy settings, switching to the full version of supported browsers only works for phishing and malicious websites.
- On iOS devices operating in basic protection mode, when you change the language on the device or restart the device, Web Protection is disabled. To enable Web Protection, after you change the language or the device restarts, wait about a minute and then open Kaspersky Protection for iOS.

Known issues affecting Anti-Theft

- For timely delivery of commands to Android devices, the app uses the Firebase Cloud Messaging (FCM) service. If FCM is not configured, commands will be delivered to the device only during synchronization with Kaspersky Security Center according to the schedule defined in the policy, for example, every 24 hours.
- To lock a device, Kaspersky Endpoint Security for Android must be set as a device administrator.
- To lock devices running Android 7 or later, Kaspersky Endpoint Security for Android must be set as an Accessibility feature.
- On some devices, Anti-Theft commands may fail to execute if Battery Saver mode is enabled on the device. This defect has been confirmed on Alcatel 5080X.
- To locate devices running Android 10 or later, the user must grant the "All the time" permission for device location.

Known issues affecting App Control

- Kaspersky Endpoint Security for Android must be set as an Accessibility feature to ensure proper functioning of App Control. This does not apply to corporate devices.
- For App Control (app categories) to work, you must enable the use of Kaspersky Security Network. App Control determines the category of an app based on data that is available in KSN. To use KSN, the mobile device must be connected to the internet. For App Control, you can add individual apps to the lists of blocked and allowed apps. In this case, KSN is not required.
- When configuring App Control, it is recommended to clear the **Block system apps** check box. Blocking system apps may lead to problems in the operation of the device.
- On iOS MDM devices, if you specify allowed apps in the list of apps allowed to be installed, all apps except system apps and those added to the list of allowed apps will be hidden on the device screen.
- On some HUAWEI and Honor personal devices, apps from allowed categories may be blocked and apps from forbidden categories may remain unblocked. This is because the category for some apps from the App Gallery cannot be correctly defined.
- On some Samsung and Oppo devices, app icons may remain hidden on the home screen after clearing the **Block system apps** check box. This is due to limitations of the Android operating system.
- When configuring a corporate container on the device, we recommend clearing the **Block system apps** check box. Blocking system apps may lead to problems with creating the corporate container.

- If **Block system apps** check box is selected, among system apps, the system mechanism for requesting app permissions may be blocked. If you want to unblock this mechanism, find its name (for example, `com.google.android.permissioncontroller`) in the event log and add it to the exceptions.

- On some Android devices, required apps will not be downloaded until the user unlocks the device screen.

Known issues affecting Compliance Control

- If a non-existent iOS version is specified for the **Update operating system** response, the device will upgrade to the latest downloaded operating system.

- On non-supervised iOS MDM devices running iOS 26 or later, compliance rules for which the **Roaming** criterion is selected may not work correctly.

Known issues when managing certificates

- When the **Integrate issuance of certificates with Microsoft Certification Authority (CA) via PKI** option is enabled in the **Issuance rules**, the settings of mail and VPN certificates may remain inactive for a certain time while waiting for the PKI response.

- You cannot automatically renew a mail or VPN certificate uploaded from a file (with the **Integrate issuance of certificates with Microsoft Certification Authority (CA) via PKI** option disabled in the **PKI settings** section of the **Issuance rules**), since there is no access to the Certificate Authority (CA) of such a certificate. To renew the certificate, you need to upload a new certificate file manually.

- A new mobile, VPN, or mail certificate for another user cannot be installed on a mobile device if the device already has the mobile certificate for a current user installed. However, new certificates for the current user can be issued.

Known issues when configuring the device unlock password strength

- On devices running Android 10 or later, Kaspersky Endpoint Security resolves the password strength requirements into one of the system values: medium or high.

  If the password length required is 1 to 4 symbols, then the app prompts the user to set a medium-strength password. It must be either numeric (PIN), with no repeating or ordered sequences (e.g. 1234), or alphanumeric. The PIN or password must be at least 4 characters long.

  If the password length required is 5 or more symbols, then the app prompts the user to set a high-strength password. It must be either numeric (PIN), with no repeating or ordered sequences, or alphanumeric (password). The PIN must be at least 8 digits long. The password must be at least 6 characters long.

- On devices running Android 7.1.1, if the unlock password does not meet the corporate security requirements (Compliance Control), the Settings system app may function improperly when an attempt is made to change the unlock password through Kaspersky Endpoint Security for Android. The issue is caused by a well-known defect in Android 7.1.1. In this case, only use the Settings system app to change the unlock password.

- On some devices running Android 6 or later, if device data is encrypted, an error may occur when the screen unlock password is entered. This issue is related to specific features of the Accessibility service with MIUI firmware.

- On some iOS MDM devices, if the **Minimum number of special characters** value is specified and the **Allow simple password** check box is selected, the device displays information about setting a password of 6 or more characters even though it is possible to set a password of 4 or more characters.

Known issues affecting Kaspersky Endpoint Security for Android removal protection

- Kaspersky Endpoint Security for Android must be set as a device administrator.

- To protect the app from removal on devices running Android 7 or later, Kaspersky Endpoint Security for Android must be set as an Accessibility feature.

- On some Xiaomi and HUAWEI devices, Kaspersky Endpoint Security for Android removal protection does not work. This issue is caused by the specific features of MIUI 7 and 8 firmware on Xiaomi and EMUI firmware on HUAWEI.

Known issues when configuring device restrictions

- On personal devices and devices with a work profile running Android 10 or later, prohibiting the use of Wi-Fi networks is not supported.

- On devices running Android 11 or later, Kaspersky Endpoint Security for Android must be set as an Accessibility feature. Kaspersky Endpoint Security for Android prompts the user to set the app as an Accessibility feature through the Initial Configuration Wizard. The user can skip this step or later disable this service in the device settings. If this is the case, you will not be able to restrict use of the camera.

- On iOS MDM devices, users may be able to enable Spotlight internet search results in Siri Suggestions even if the **Prohibit Spotlight suggestions** check box is selected. This is due to an issue known to Apple.

- On Android devices, when use of the camera is prohibited, some apps may close automatically. This issue is due to how services and features such as Android System Intelligence and Screen Attention use the device camera to keep the screen on while the user is looking at it.

Known issues when sending commands to mobile devices

- On devices running Android 12 or later, if the user granted the "Use approximate location" permission, the Kaspersky Endpoint Security for Android app first tries to get the precise device location. If this is not successful, the approximate device location is returned only if it was received within the last 30 minutes. Otherwise, the **Locate device** command fails.

- The **Locate device** command does not work on Android devices if Google Location Accuracy is disabled in the settings. Please be aware that not all Android devices come with this location setting.

- If you send the **Enable Lost Mode** command to a supervised iOS MDM device without a SIM card and the device is restarted, the device won't be able to connect to Wi-Fi and receive the **Disable Lost Mode** command. This is a specific feature of iOS devices. To avoid this issue, you can either send the command only to devices with a SIM card, or insert a SIM card into the locked device to allow it to receive the **Disable Lost Mode** command over the mobile network.

- The **Reset to factory settings** command is unavailable for personal devices and devices with a corporate container running Android 14 or later.

- Before executing the **Reset password** command, the device screen must be locked and unlocked at least once.

- The **Reset password** command cannot be executed on a corporate device if you set a screen unlock password before installing Kaspersky Endpoint Security for Android. To avoid this, the device must be reset to factory settings right before installing the app.

- On supervised devices that have a passcode set and are running iOS 26.3, 26.4, and 26.5, when the **OS update (supervised only)** command is sent to the device, the downloaded update may not be displayed or may be displayed without a specific version, and the installation attempt may fail with an error. As a result, the update cannot be installed.

- On Android devices, if the device time is ahead of the Kaspersky Security Center server time, location history data returned by the **Get location history** command with timestamps later than the server time are not displayed in the location history by default.

Known issues affecting specific devices

- On certain devices (for example, HUAWEI, Meizu, and Xiaomi), you must grant Kaspersky Endpoint Security for Android the autostart permission or manually add it to the list of apps that are started when the operating system starts. If the app is not added to the list:

  - Kaspersky Endpoint Security for Android stops performing all of its functions after the mobile device is restarted.

  - If the device has been locked, you cannot use a command to unlock the device. You can unlock the device only by using a one-time unlock code.

  - On devices running Xiaomi HyperOS, Kaspersky Endpoint Security for Android may not scan notifications from messengers in order to detect malicious and phishing URLs.

- On certain devices (for example, Meizu and Asus) running Android 6 or later, after encrypting data and restarting the Android device, you must enter a numeric password to unlock the device. If the user uses a graphic password to unlock the device, you must convert the graphic password to a numeric password. For more details about converting a graphic password into a numeric password, please refer to the Technical Support website of the mobile device manufacturer. This issue is related to the operation of the Accessibility Features service.

- On some HUAWEI devices running Android 5.X, after Kaspersky Endpoint Security for Android is set as an Accessibility feature, the device may incorrectly display a message about a lack of sufficient rights. To hide this message, enable the app as a protected app in the device settings.

- On some HUAWEI devices running Android 5.X or 6.X, when Battery Saver mode is enabled for Kaspersky Endpoint Security for Android, the user can manually terminate the app. The user device then becomes unprotected. This issue is due to some features of HUAWEI software. To restore device protection, run Kaspersky Endpoint Security for Android manually. It is recommended to disable Battery Saver mode for Kaspersky Endpoint Security for Android in the device settings.

- On HUAWEI devices with EMUI firmware running Android 7, the user can hide the notification regarding the protection status of Kaspersky Endpoint Security for Android. This issue is due to some features of HUAWEI software.

- On some Xiaomi devices, when setting the password length to more than 5 characters in a policy, the user will be prompted to change the screen unlock password instead of the PIN code. You cannot set a PIN code that has more than 5 characters. This issue is due to some features of Xiaomi software.

- On Xiaomi devices with MIUI firmware running Android 6, the Kaspersky Endpoint Security for Android icon may be hidden in the status bar. This issue is due to some features of Xiaomi software. It is recommended to allow the display of notification icons in the Notifications settings.

- On some Nexus devices running Android 6.0.1, the privileges required for proper operation cannot be granted through the Quick Start Wizard of Kaspersky Endpoint Security for Android. This issue is caused by a well-known defect in Security Patch for Android by Google. To ensure proper operation, the required privileges must be manually granted in the device settings.

- On certain Samsung devices running Android 7 or later, when the user attempts to configure unsupported methods for unlocking the device (for example, a graphical password), the device may be locked if the following conditions are met: Kaspersky Endpoint Security for Android removal protection is enabled and screen unlock password strength requirements are set. To unlock the device, you must send a special command to the device.

- On certain Samsung devices, it is impossible to block the use of fingerprints for unlocking the screen.

- Web Protection and Web Control cannot be enabled on some Samsung devices, if the device is connected to a 3G/4G network, has Battery Saver mode enabled and restricts background data. It is recommended to disable the function that restricts background processes in Battery Saver settings.

- On certain Samsung devices, if the unlock password does not comply with corporate security requirements, Kaspersky Endpoint Security for Android does not block the use of fingerprints for unlocking the screen.

- On some Honor and HUAWEI devices, you cannot restrict the use of Bluetooth. When Kaspersky Endpoint Security for Android attempts to restrict the use of Bluetooth, the operating system shows a notification with options to reject or allow this restriction. The user can reject this restriction and continue to use Bluetooth.

- On Blackview devices, the user can clear the memory for the Kaspersky Endpoint Security for Android app. As a result, device protection and management are disabled, all defined settings become ineffective, and the Kaspersky Endpoint Security for Android app is removed from the Accessibility features. This is because this vendor's devices provide elevated privileges to the customized Recent screens app. This app can override Kaspersky Endpoint Security for Android settings and cannot be replaced because it is part of the Android operating system.

- On some Google Pixel devices running Android 11 or earlier, the Kaspersky Endpoint Security for Android app crashes immediately after starting. This is caused by an issue in Android.

- On HUAWEI P60 Pro, a corporate container cannot be created.

- On some iOS MDM devices with basic control operating mode running iOS 18.2 - iOS 18.3.1, the use of Safari can be prohibited. This is due to an issue known to Apple.

- On certain personal devices (for example, OnePlus, Honor) running Android 10 or later, a password can be requested when connecting to Wi-Fi networks secured by the WPA2 PSK or WPA3 PSK protocol. This is due to some issues with how the Suggestion API works.

- On iOS MDM devices running iOS 18.0, a policy with AirPlay configured cannot be delivered to the device. This is due to an issue known to Apple. To ensure proper operation, update iOS on the device.

- On some devices, during a remote connection session, the administrator cannot grant system permissions to apps (except for Kaspersky Endpoint Security for Android) due to the operating system restrictions when accessibility features are enabled.

- On some HUAWEI devices and devices running kvadraOS 1.26 (Enterprise) in the corporate device operating mode, the unlock password specified in the **Screen unlock settings** policy section is not applied on the device if the user has previously set a PIN code on this device.

- On supervised devices running iOS 26.3.1 (a), iOS 26.5, and iPadOS 26.5, when the **Prohibit modifying Personal Hotspot settings** check box is selected in the **Device feature restrictions** settings of the policy, some Personal Hotspot settings can still be modified by the user. This is due to an issue known to Apple.

Known issues affecting the app on Android 13

- On Android 13, the user can use the Foreground Services Task Manager to stop Kaspersky Endpoint Security from running in the background. This is caused by a well-known issue in Android 13.

- On Android 13, the permission to send notifications is requested when the initial app configuration begins. This is due to specifics of the Android 13 operating system.

Known issues affecting policy profiles

- If you switch to a license with basic functionality, settings that are available only with a license with extended functionality do not reset to defaults in policy profiles.

Known issues in role-based access control

- If the License key management right is not granted, when opening an existing policy, an error may occur. This does not affect the operation of the policy.

- If the License key management right is not granted, you can create a policy without choosing the license in the Mobile policy wizard. However, in this case, you cannot configure the policy settings.

Known issues when configuring Web Server settings on connection gateway (Network Agent Linux)

- When configuring Web Server settings on a connection gateway, if ports are modified or certificates are issued or reissued, it may take some time for the new settings to synchronize with Kaspersky Security Center. Please wait up to 15 minutes or click **Force synchronization** on the **General** tab of the connection gateway host properties (**Asset management** → **Assets (Devices)**).

- When configuring a custom Web Server certificate, if the addresses in the **Web Server address** and **Certificate address** fields do not match, an error will be displayed. In this case, to save the settings, you need to upload a different certificate. However, if you change the Web Server address in the distribution point properties of Kaspersky Security Center and the certificate remains the same, you can still save these settings, even if the addresses do not match.

Known issues when migrating from Kaspersky Security Center Windows to Kaspersky Security Center Linux

- When migrating iOS MDM Server settings from Kaspersky Security Center Windows 14.2 to Kaspersky Security Center Linux, the notification and storage settings of the iOS MDM Server events are not transferred and instead take default values. After the migration, you will need to specify the required values manually.

- If a user was deleted or is missing from the server during migration, the mobile certificate is displayed in the list of certificates without the user name.

Known issues affecting iOS MDM Server

- It may take at least 6 hours for the issued reserve iOS MDM Server certificate to be delivered to the device.

Known issues affecting KSN Proxy

- If mobile devices are connected to Kaspersky Security Center through the connection gateway, KSN Proxy does not work. In this case, disable the **Enable KSN Proxy on Administration Server Enabled** toggle switch in the **KSN Proxy** section of the Administration Server properties window. For detailed information on enabling and disabling the usage of KSN Proxy, refer to the Kaspersky Security Center Help.

Known issues in corporate device mode

- On corporate devices with Android 10, location permissions are automatically set to **Allow only while using the app** instead of **Allow all the time** and can't be changed by the administrator or users. This issue is caused by a well-known bug in Android 10.
- Managing update settings on mobile devices is vendor-specific. On some Android and kvadraOS 1.26 (Enterprise) devices, the restriction on manual installation of operating system updates may work incorrectly.
- On corporate devices running Android 10 or later, Knox settings may not be applied if Kaspersky Endpoint Security for Android is deployed via an installation package.

Known issues in kiosk mode

- On iOS MDM devices running iOS 17 and iPadOS 17, if the **Auto-Rotate Screen** check box is cleared in the **Kiosk mode** settings, screen orientation still changes automatically when the device is rotated.
- On iOS MDM devices running iOS 26 or later and iPadOS 26 or later, app icons may appear blocked on the home screen after disabling kiosk mode, but apps still can be opened. To update their state, try swiping the screen.
- On iPhone 15 and later, if the **Ring/Silent Switch** check box is cleared in the kiosk mode settings, the user can still switch between Ring and Silent modes using the Action button.
- On some corporate Android devices in kiosk mode, the incoming call screen may not be displayed while the device is unlocked and the app is running. In this case, the call cannot be answered, and only a missed call notification will be shown afterwards. Due to this limitation, we do not recommend enabling Call Control, as it may not work correctly in this mode.

Known issues affecting remote control of Android devices

- On some devices, screen sharing may be interrupted when the device screen is locked.
- Remote control sessions fail to establish when started from Yandex Browser. The problem is caused by an issue in Yandex Browser and may occur during the first launch or after restarting the browser or the administrator's computer. We recommend using other browsers supported by the Kaspersky Mobile Devices Protection and Management plug-in to start remote sessions, such as Google Chrome, Microsoft Edge, Mozilla Firefox, and Safari.
- Attempts to manage the Kaspersky Endpoint Security for Android app using third-party mobile device remote management solutions may result in errors.
- Remote connection to mobile devices running kvadraOS 1.26 (Enterprise) may not be established when the device screen is in horizontal orientation.
- On devices running Android 16, buttons in system dialogs may not respond during remote control sessions. This is due to specifics of the Android 16 operating system and the apps the administrator interacts with during the session.

Known issues affecting events

- After updating the Kaspersky Mobile Devices Protection and Management plug-in, new events may display incorrectly in a previously created policy: on the **Event configuration** tab, the events appear enabled, but information about them is not transmitted. To ensure the updated plug-in provides an up-to-date list of events for a previously created policy, you must re-save this policy.

Getting started

This section is intended for specialists who install the Advanced MDM in Kaspersky Next Expert View (on-premise) solution, as well as for specialists who provide technical support to organizations that use Advanced MDM in Kaspersky Next Expert View (on-premise).

Solution architecture

Advanced MDM in Kaspersky Next Expert View (on-premise) includes the following components:

- Kaspersky Endpoint Security for Android mobile app

  The app protects Android devices against web threats, viruses, and other apps that pose threats.

- Kaspersky Protection for iOS mobile app

  The app protects iOS devices against phishing and web threats and lets you detect jailbreaking on devices.

- Kaspersky Endpoint Security for Aurora mobile app

  The app protects Aurora devices against malware and other files that pose threats.

- Kaspersky Mobile Devices Protection and Management plug-in

  The plug-in lets you manage devices running Android, iOS, and Aurora in Kaspersky Next Expert View (on-premise).

- iOS MDM Server

  iOS MDM Server lets you connect iOS devices to the Administration Server and manage iOS devices.

- iOS MDM Server settings plug-in

  The plug-in lets you configure iOS MDM Server settings.

Deployment scenarios

The deployment of Advanced MDM in Kaspersky Next Expert View (on-premise) in Kaspersky Next Expert View (on-premise) consists of the following steps:

1. Deploying Kaspersky Security Center Linux and Kaspersky Next Expert View (on-premise)
2. Deploying mobile management plug-ins
3. Configuring Administration Server settings for connecting mobile devices
4. Deploying an iOS device management system
5. Deploying an Android device management system
6. Managing mobile devices in Kaspersky Next Expert View (on-premise)

Deploying a mobile device management solution

To connect and manage mobile devices using Kaspersky Next Expert View (on-premise), you must deploy a mobile device management solution. This section describes the recommended actions when getting started with Advanced MDM in Kaspersky Next Expert View (on-premise).

Deploying Kaspersky Security Center Linux and Kaspersky Next Expert View (on-premise)

Select a Linux device that you intend to use as the administrator's workstation, ensure that the device meets the software and hardware requirements, and then install Kaspersky Security Center and Kaspersky Next Expert View (on-premise) on the device.

For instructions on installing Kaspersky Security Center Linux, refer to the Kaspersky Security Center Help.

For instructions on installing Kaspersky Next Expert View (on-premise), refer to the Kaspersky Security Center Help.

Deploying mobile management plug-ins

To use the Advanced MDM in Kaspersky Next Expert View (on-premise) solution and connect mobile devices, you must add and install the following mobile management plug-ins:

- Kaspersky Mobile Devices Protection and Management
  - `on_prem_ksm_policies_<version>.zip`

Archive that contains the files required for the installation of the Kaspersky Mobile Devices Protection and Management plug-in:

- `plugin.zip`

  Archive that contains the Kaspersky Mobile Devices Protection and Management plug-in.

- `signature.txt`

  File that contains the signature for the Kaspersky Mobile Devices Protection and Management plug-in.

- iOS MDM Server settings

  - `on_prem_iosmdm_<version>.zip`

    Archive that contains the files required for the installation of the iOS MDM Server settings plug-in:

    - `plugin.zip`

      Archive that contains the iOS MDM Server settings plug-in.

    - `signature.txt`

      File that contains the signature for the iOS MDM Server settings plug-in.

To install a management plug-in:

1. In the main window of Kaspersky Next Expert View (on-premise), select **Settings** → **Web plug-ins**.
2. In the window that opens, click **Add**.

   The list of available plug-ins is displayed.
3. In the list of available plug-ins, select the plug-in you want to install by clicking on its name.

   A plug-in description page is displayed.
4. On the plug-in description page, click **Install plug-in**.
5. When the installation is complete, click **OK**.

The management plug-in is downloaded with the default configuration and displayed in the list of management plug-ins.

You can add plug-ins and update downloaded plug-ins from a file. You can download management plug-ins and web management plug-ins from the Kaspersky Customer Service webpage.

To load or update a plug-in from a file:

1. In the main window of Kaspersky Next Expert View (on-premise), select **Settings** > **Web plug-ins**.
2. In the window that opens:

   - Click **Add from file** to load a plug-in from a file.
   - Click **Update from file** to load an update of a plug-in from a file.

3. Specify the file and signature of the file.

4. Load the specified files.

   The management plug-in is loaded from the file and displayed in the list of management plug-ins.

> Updates functionality (including providing anti-malware signature updates and codebase updates), as well as KSN functionality may not be available in the software in the U.S.

For information about the compatibility of the plug-in version and Kaspersky Security Center versions, see the hardware and software requirements.

Configuring Administration Server settings for connecting mobile devices

Before connecting mobile devices to Kaspersky Next Expert View (on-premise), you must define the connection settings in the Administration Server properties.

To configure Administration Server settings for connecting mobile devices:

1. In the main window of Kaspersky Next Expert View (on-premise), click the Administration Server name.

2. In the Administration Server properties window that opens, configure the Administration Server port that will be used by mobile devices:

   a. In the **General** tab, select the **Additional ports** section.

   b. Enable the **Open port for mobile devices** toggle button.

      If this option is enabled, the port for mobile devices will be open on the Administration Server.

   c. In the **Port for mobile device synchronization** field, specify the port through which mobile devices will connect to the Administration Server.

      Port 13292 is used by default.

      If the **Open port for mobile devices** toggle button is off or an incorrect connection port is specified, mobile devices will not be able to connect to the Administration Server.

3. If necessary, edit the certificate that will be used by mobile devices to connect to the Administration Server.

> By default, Administration Server uses the certificate created after the port for mobile devices is opened. You can reissue or replace the certificate issued through the Administration Server with another certificate.

To edit the certificate:

a. In the **General** tab, select the **Certificates** section.

b. Define the required settings.

For more details on working with certificates in Kaspersky Security Center Linux, refer to the Kaspersky Security Center Help.

4. Click **Save** to save the changes you have made and exit the Administration Server properties window.

The mobile device connection settings are configured.

Scenario: Configuring a connection gateway to connect mobile devices to Kaspersky Next Expert View (on-premise)

A connection gateway is Network Agent operating in a special mode. Network Agent is a Kaspersky Security Center component that enables interaction between the Administration Server and Kaspersky applications. A connection gateway receives connections from other Network Agents and tunnels them to the Administration Server through its own connection with the Server.

Unlike an ordinary Network Agent, a connection gateway may be configured to wait for connections from the Administration Server rather than establishing connections to it. A connection gateway in DMZ receives connections from the Administration Server through the 13000 TLS port. Since a connection gateway in DMZ cannot reach the Administration Server ports, the Administration Server creates and maintains a permanent signal connection with a connection gateway. The signal connection is not used for data transfer, it is only aimed at sending an invitation for network interaction. When a connection gateway needs to connect to the Administration Server, it notifies the Server through this signal connection, and then the Server establishes the required connection for data transfer.

A connection gateway lets you more efficiently use the security features to protect network infrastructure against potential vulnerabilities.

- Using a connection gateway makes it easier to monitor suspicious activity on a separate network node outside a LAN (local network area). It helps to avoid direct malicious attacks via a mobile protocol by implementing a different protocol for communications between the connection gateway and Kaspersky Security Center.
- The surface of potential network attacks is smaller, since a connection gateway receives connections from the Administration Server through a single port (by default, 13000) through which all requests are processed.
- Using a connection gateway makes it possible to verify the mobile certificate outside a LAN and prevent devices from sending data to Kaspersky Security Center before they are authenticated, which protects network infrastructure against vulnerabilities in low-level protocols such as TLS/SSL.

Requirements

For a connection gateway to work correctly with mobile devices, the following requirements must be met:

- Port 13293 or port 13292 must be open on the host with the connection gateway.

These ports are designed to connect and synchronize mobile devices.

- When using port 13293, the TLS certificate is verified on the connection gateway (without being sent to the Administration Server).
- When using port 13292, the certificate is not verified (the LP_MobileMustUseTwoWayAuthOnPort13292 flag is ignored).

- Port 13000 must be open between the connection gateway and Kaspersky Security Center, through which the connection gateway receives connections from the Administration Server. It does not need to be open outside the DMZ.
- The host must have a static address accessible from the internet.

Stages

The configuration proceeds in the following steps:

1. **Installing Network Agent in the connection gateway role on a host**

   First, you need to install Network Agent on the selected host device acting in the gateway connection role.

   For information about generating a Network Agent installation package, refer to the Kaspersky Security Center Help.

   You can install Network Agent in interactive mode by specifying installation parameters step by step. Alternatively, you can use an answer file—a text file that contains a custom set of installation parameters: variables and their respective values. Using this answer file allows you to run an installation in silent mode, that is, without user participation. For information on installing Network Agent in silent mode, refer to the Kaspersky Security Center Help.

2. **Configuring the connection gateway on Kaspersky Security Center Administration Server**

   Once you have installed Network Agent in the connection gateway role, you must connect it to Administration Server. Administration Server does not yet list the device with the connection gateway among the managed devices because the connection gateway has not tried to connect to Administration Server.

   You must create a new group under the **Managed Devices** group and add the device acting as a connection gateway to the group that you have created. For information on manually adding devices to groups in Kaspersky Next Expert View (on-premise), refer to the Kaspersky Security Center Help.

   After that, assign the device as a distribution point and configure the distribution point to act as a connection gateway in the **Connection gateway** section of the distribution point properties. Then enable the **Open port for mobile devices (SSL authentication of the Administration Server only)** and **Open port for mobile devices (two-way SSL authentication)** options and specify ports and DNS domain names of the distribution point to connect mobile devices.

   If the 'CA: true' basic constraint is not set for a custom mobile Administration Server certificate, the same certificate will be used for the connection gateway as for the Administration Server. If the 'CA: true' basic constraint is set, a separate certificate issued from the custom mobile Administration Server certificate will be used for the connection gateway.

3. **Reissue the mobile certificate**

   Reissue the mobile certificate with a connection address specified when configuring the connection gateway (in the Administration Server properties window, select **General** → **Certificates**). For detailed information on reissuing mobile certificates, refer to the Reissuing the mobile Administration Server certificate section.

Results

The connection gateway will be configured. You will be able to add new mobile devices by specifying the connection gateway address.

To make sure mobile devices are synchronized with Kaspersky Security Center on the connection gateway, the connection address you have set when configuring the connection gateway must be specified in the properties of Kaspersky Endpoint Security for Android installation packages (**Operations** → **Repositories** → **Installation packages**).

Adding installation packages to Administration Server repository

For further deployment of mobile management systems, you need to add the following installation packages to the Administration Server repository:

- Network Agent Linux installation package (for later installation of Network Agent on a workstation).
- iOS MDM Server installation package (for later installation of iOS MDM Server to connect and manage iOS devices).
- Kaspersky Endpoint Security for Android installation package (for later installation of Kaspersky Endpoint Security for Android on devices).

For instructions on adding installation packages to the Administration Server repository, refer to the Kaspersky Security Center Help.

Adding a license key to the Administration Server repository

To connect mobile devices to Kaspersky Next Expert View (on-premise) and manage them, you must specify a license key that supports the Mobile Device Management solution.

The license under which the solution is used determines a scope of basic or advanced settings you can configure. With a license that does not provide the extended Advanced MDM in Kaspersky Next Expert View (on-premise) functionality, only basic device protection settings are available in the Kaspersky Mobile Devices Protection and Management plug-in. For detailed information on licenses, refer to the About the license section.

To specify a license key in the current license settings of the Administration Server properties:

- In the main window of Kaspersky Next Expert View (on-premise), click the Administration Server name.

  In the Administration Server properties window that opens:

  a. On the **General** tab, select the **License keys** section.

  b. In the **Current license** block of settings, click **Select** and do one of the following:

  - Choose one of the existing license keys.
  - Specify the KEY file you want to add.

The license you choose must support the Mobile Management solution.

c. Click **Save**.

The license key is specified in the current license settings of the Administration Server properties.

To add a license key to the Administration Server repository:

1. In the main window of Kaspersky Next Expert View (on-premise), select **Operations** → **Licenses**.
2. Click **Add**.
3. In the window that opens, click **Add key file**.
4. Click **Select key file**, and then specify the KEY file you want to add.

   The license you choose must support the Mobile Management solution.

5. Click **Save**.

The license key is added to the Administration Server repository.

Installing Network Agent Linux

Network Agent Linux is a Kaspersky Security Center component that enables interaction between the Administration Server and Kaspersky applications that are installed on a workstation or server.

To deploy an iOS device management system, you must install Network Agent on a workstation on which iOS MDM Server will later be deployed. After Network Agent is installed, you will be able to configure and install iOS MDM Server on it to subsequently connect and manage iOS devices.

For the instructions on installing Network Agent Linux, refer to the Kaspersky Security Center Help.

Configuring Kaspersky Security Center Linux Web Server settings

Kaspersky Security Center Linux Web Server (Web Server) is a component of Kaspersky Security Center Linux installed together with the Administration Server. Web Server is designed for network transmission of stand-alone installation packages, management profiles, and files from a shared folder.

Installation packages that have been created are published on Web Server automatically and then removed after the first download. The administrator can send a new link to the user in any convenient way, such as by email.

For detailed information, refer to the Kaspersky Security Center Help.

To connect mobile devices, make sure the Web Server FQDN is specified correctly in the Administration Server properties:

1. In the main window of Kaspersky Next Expert View (on-premise), click the Administration Server name.
2. In the Administration Server properties window that opens, on the **General** tab, select the **Web Server** section.
3. In the **Web Server FQDN** field, check if the specified FQDN (a fully qualified domain name) is publicly resolvable by DNS servers.

Configuring Web Server settings on a connection gateway (Network Agent for Linux)

A separate Web Server service is implemented on a distribution point in a connection gateway mode, which allows working with mobile devices connected to Kaspersky Security Center. This service is responsible for transferring app installation packages and management profiles to devices without directly connecting them to the Administration Server. Files are transferred as the service processes HTTP/HTTPS file requests on a connection gateway.

Web Server on a connection gateway only works for downloading the following types of files to mobile devices:

- Kaspersky mobile apps

  Installation packages of Kaspersky mobile apps added to policies by the administrator via Kaspersky Next Expert View (on-premise).

- Third-party mobile apps

  Installation packages of third-party mobile apps created by the administrator for their subsequent installation on devices from a local file.

- Management profiles for iOS MDM devices

To connect new devices to Kaspersky Security Center, installation packages and management profiles are published on the Web Server connection gateway if it has been deployed.

Links to installation packages are located in the policy settings and the "Apps & files" and "Installation packages" sections of Kaspersky Security Center.

This functionality is available with Kaspersky Security Center Linux 15.2 or later.

The Web Server service on a connection gateway is installed together with Network Agent Linux. To use this functionality, you must assign a device that will act as a distribution point in a connection gateway mode to be used as Web Server, and then specify the corresponding settings.

Assign a device that will act as a distribution point in a connection gateway mode

To assign a device that will act as a distribution point in a connection gateway mode:

1. In the main window of Kaspersky Next Expert View (on-premise), click the Administration Server name.
2. In the Administration Server properties window that opens, on the **General** tab, select the **Distribution points** section.
3. Click **Assign**.
4. In the window that opens, select the device that you want to act as a distribution point.

5. Click **OK**.

   The selected device appears in the list of distribution points.

6. Click the name of the device.

7. In the properties window of the distribution points that opens, select the **Connection gateway** section.

8. Enable the **Connection gateway** toggle switch.

9. Specify the DNS domain name of the distribution point under which it will be available to mobile devices.

10. Click **OK**.

A device that will act as a distribution point in a connection gateway mode is assigned.

Configure Web Server settings on a connection gateway

To configure Web Server settings on a connection gateway:

1. In the main window of Kaspersky Next Expert View (on-premise), click the Administration Server name.

2. In the Administration Server properties window that opens, on the **General** tab, select the **Web Server** section.

3. In the **Web Server settings on connection gateway (Network Agent for Linux)** block of settings, select the **Launch an additional Web Server on connection gateway** check box.

   This Web Server will be used to transfer files to devices.

4. In the **Connection gateway** field that appears, specify the host on which Web Server will be deployed to act as a connection gateway. Only hosts that support this functionality are displayed in the drop-down list.

5. In the **Web Server settings for selected connection gateway** block of settings that opens, configure the Web Server ports:

   a. Select **Open Web Server HTTPS port** if you want Web Server to be accessible on the HTTPS port and handle HTTPS requests. You will also need to configure a corresponding certificate to secure this port.

      a. Specify the **HTTPS port**.

      b. Specify the **Certificate source** for the Web Server HTTPS port.

         By default, the certificate issued by the Administration Server is used – it is valid for 397 days and is renewed automatically after it expires. If necessary, you can renew this certificate manually by clicking the **Reissue** button.

         To continue using this certificate, select **Issue certificate through Administration Server**. To upload a custom certificate manually, select **Upload certificate from file**.

         To upload a certificate from a file:

         - Click **Upload from file**.

         - In the window that opens, choose the **Certificate format**.

- For a **PKCS #12** certificate, specify the path to the certificate file (P12 or PFX) and enter the certificate password.

  For an **X.509** certificate, specify the path to the public and private key files and enter the private key password.

- Click **Save**.

c. Make sure the addresses in the **Web Server address** (the address of Web Server whose requests will be processed by Kaspersky Security Center) and **Certificate address** (the address of the issued certificate) fields match. Otherwise, you need to reissue the certificate issued by the Administration Server or upload a different custom certificate.

In order for devices to securely download files from Web Server on a connection gateway via HTTPS, the Web Server certificate must be installed on these devices.

b. Select **Open Web Server HTTP port** if you want Web Server to be accessible on the HTTP port and handle HTTP requests.

a. Specify the **HTTP port**.

c. Click **Save**.

Web Server settings on a connection gateway are configured.

If HTTP or HTTPS port settings are changed, you need to update the links to previously published installation packages for mobile devices connected to Web Server on the connection gateway. Please republish the links in the policy settings and the "Apps & files" and "Installation packages" sections of Kaspersky Security Center.

To update the links to installation packages:

- In the "Apps & files" section:

  a. In the main window of Kaspersky Next Expert View (on-premise), select **Asset management** → **Mobile** → **Apps & files**.

  b. Click **Android** or **iOS** depending on the required operating system.

  c. In the list of apps that opens, do one of the following:

  - Select the check boxes next to the names of the apps whose installation package links you want to update, and then click **Republish**.
  - Click the names of the apps whose installation package links you want to update, and then click **Republish** in the window that opens.

- In the "Installation packages" section:

  a. In the main window of Kaspersky Next Expert View (on-premise), select **Operations** → **Repositories** → **Installation packages**.

  b. In the window that opens, click **View the list of stand-alone packages**.

c. Select the app whose installation package link you want to update, and then click **Unpublish**.

d. Click **Publish**.

The links to installation packages are updated.

Transferring the Web Server certificate to devices on the connection gateway

In order for devices to securely download files from Web Server on a connection gateway via HTTPS, the Web Server certificate must be installed on these devices.

Transferring the Web Server certificate to iOS MDM devices

When connecting new iOS MDM devices, Kaspersky Security Center automatically adds the certificate public key of Web Server on a connection gateway to the management profiles.

This allows devices to verify the HTTPS connection and safely download third-party apps from Web Server on the connection gateway.

If the certificate changes, it is updated on iOS MDM devices during synchronization with iOS MDM Server.

Transferring the Web Server certificate to Android devices

If you use Web Server with a self-signed certificate instead of a certificate signed by a certification authority (CA), the standard Android download manager lets you download apps and installation packages from Web Server on a connection gateway only via HTTP.

To securely download apps and installation packages from Web Server with a self-signed certificate to devices, you can use the built-in Kaspersky Endpoint Security for Android download manager that always uses HTTPS. For detailed information, refer to the Selecting the download manager for Android devices section.

Migrating from Kaspersky Security Center Windows to Kaspersky Security Center Linux

You can migrate mobile device data from Kaspersky Security Center Windows to Kaspersky Security Center Linux by transferring the mobile device management infrastructure from Windows to Linux servers. Following migration, mobile devices are automatically connected to Kaspersky Security Center Linux without the need for manual reconnection and are managed by the same policy as on Windows servers.

Prerequisites

Before you start:

- Make sure that the necessary features of Kaspersky Security Center Windows are supported in Kaspersky Security Center Linux. For detailed information on the main features of Kaspersky Security Center as a Windows-based solution or Linux-based solution, refer to the Kaspersky Security Center Help.
- Get acquainted with the **DBMSes and Kaspersky Security Center and iOS MDM Server versions** between which migration is possible.
  - Mobile device data can be migrated between the following DBMSes:
    - Kaspersky Security Center Windows + Microsoft SQL Server → Kaspersky Security Center Linux + PostgreSQL, Postgres Pro
    - Kaspersky Security Center Windows + MariaDB → Kaspersky Security Center Linux + PostgreSQL, Postgres Pro
    - Kaspersky Security Center Windows + MySQL → Kaspersky Security Center Linux + PostgreSQL, Postgres Pro
    - Kaspersky Security Center Windows + PostgreSQL, Postgres Pro → Kaspersky Security Center Linux + PostgreSQL, Postgres Pro
    - Kaspersky Security Center Windows + MariaDB → Kaspersky Security Center Linux + MariaDB
    - Kaspersky Security Center Windows + MySQL → Kaspersky Security Center Linux + MySQL

To enable migration to PostgreSQL or Postgres Pro, you must install a patch for the corresponding version of Kaspersky Security Center Windows Administration Server. Contact Kaspersky Technical Support to get the required patch.

For Kaspersky Secure Mobility Management based on Kaspersky Security Center Windows 14.2: 14.2.0.26967-pf5

For Kaspersky Security Center Windows 14.2: 14.2.0.48079-pf5

For Kaspersky Security Center Windows 15.1: 15.1.0.20748-pf2

The above patches are mandatory. To avoid possible errors during migration, we recommend installing not only the mandatory patch versions, but also all previous ones (starting with pf1) that correspond to the version of Kaspersky Security Center you are migrating from.

If you use MySQL or MariaDB as a DBMS for Kaspersky Security Center Windows and Kaspersky Security Center Linux, before creating a data backup, make sure that the `lower_case_table_names` parameter matches for the current and new DBMSes.

When installing MySQL or MariaDB for Kaspersky Security Center Linux, you must set this parameter to the same value as specified for Windows. For detailed information about backing up and restoring Administration Server data when using MySQL or MariaDB, refer to the Kaspersky Security Center Help.

- Migration between the following versions of Kaspersky Security Center is possible:
  - Kaspersky Security Center Windows 14.2 MMC-based Administration Console (on-premises) → Kaspersky Security Center Linux 15.4 Web Console (on-premises)
  - Kaspersky Security Center Windows 14.2.0.48079 MMC-based Administration Console (on-premises) (for Kaspersky Secure Mobility Management) → Kaspersky Security Center Linux 15.4 Web Console (on-premises)
  - Kaspersky Security Center Windows 15.1 MMC-based Administration Console (on-premises) → Kaspersky Security Center Linux 15.4 Web Console (on-premises)
  - Kaspersky Security Center Windows 14.2 Web Console and Cloud Console (on-premises) → Kaspersky Security Center Linux 15.4 Web Console (on-premises)
  - Kaspersky Security Center Windows 15.1 Web Console and Cloud Console (on-premises) → Kaspersky Security Center Linux 15.4 Web Console (on-premises)
- Migration between the following versions of iOS MDM Servers is possible:
  - iOS MDM Server Windows 14.2 (for Kaspersky Secure Mobility Management) → iOS MDM Server Linux 15.4
  - iOS MDM Server Windows 14.2 → iOS MDM Server Linux 15.4
  - iOS MDM Server Windows 15.1 → iOS MDM Server Linux 15.4

- Learn about the **data that is transferred during migration**.

  The following data is transferred:

  - Kaspersky Security Center settings
    - FQDN for connecting mobile devices to Kaspersky Security Center
    - Mobile-specific settings: licenses, Firebase Cloud Messaging (FCM) integration settings, certificates for signing management profiles, settings for issuing mobile certificates, information on accepted End User License Agreements, Kaspersky Security Network (KSN) proxy settings, Kaspersky Private Security Network (KPSN) configuration files

      If you are using Kaspersky Security Center build 14.2.0.26967, to migrate FCM settings to Postgres correctly, you must install the 14.2.0.26967-pf4 patch. If the patch is not installed, migration will fail due to a database error. In this case, to avoid errors, delete all FCM settings before the migration.

      PKI integration settings for issuing mobile certificates are not migrated.

    - Role-based access control configuration files
    - Kaspersky Endpoint Security for Android database update settings
    - Signing keys for Kaspersky Endpoint Security for Android APK files

- Mobile devices
  - Information on mobile devices managed by Kaspersky Endpoint Security for Android and Kaspersky Protection for iOS
  - Event logs of mobile devices managed by Kaspersky Endpoint Security for Android and Kaspersky Protection for iOS
  - History of previously executed and pending commands on Android devices and their results
  - Information on links, installation packages, and management profiles created for mobile devices waiting to be connected
  - Kaspersky Endpoint Security for Android settings and installation packages
  - iOS MDM Server settings and installation packages

    Information on Android devices awaiting connection is not migrated.

- Policies
  - Policies for mobile device management in MMC-based Administration Console of Kaspersky Security Center (Android and iOS devices)
  - Policies for mobile device management in Kaspersky Security Center Web Console and Cloud Console (Android and iOS devices)
- Certificates
  - Mobile Administration Server certificates (main and reserve certificates, Web Server certificates)
  - Information on user certificates (mobile, mail, and VPN certificates) and their statuses
- iOS MDM Servers
  - Installed iOS MDM Servers
  - iOS MDM Server event logs
- iOS MDM Server settings, certificates (iOS MDM Server certificate, APNs certificate), and configuration profiles

  iOS MDM Server apps are not migrated.

  Host-specific data such as information on profiles created for mobile devices awaiting connection and commands awaiting execution is not migrated.

When migrating iOS MDM Server settings from Kaspersky Security Center Windows 14.2 to Kaspersky Security Center Linux, the notification and storage settings of the iOS MDM Server events are not transferred and instead take default values. After the migration, you will need to specify the required values manually.

- Web Server
  - Kaspersky Endpoint Security for Android settings and installation packages
  - iOS MDM Server settings and installation packages

Apps for mobile devices stored on Kaspersky Security Center Web Server are not migrated using the klbackup utility and must be transferred manually.

- Connection gateway (Network Agent) settings

The installed mobile management plug-ins are not migrated. After you restore the Administration Server and iOS MDM Server data from a backup copy, you need to download and install the Kaspersky Mobile Devices Protection and Management plug-in and iOS MDM Server plug-in.

Stages

The migration process entails creating a data backup using the *klbackup* utility to transfer the Administration Server data and using the *kliosbackup* utility to transfer the iOS MDM Server data.

For the transferred mobile devices to be displayed correctly in Kaspersky Next Expert View (on-premise), both Administration Server and iOS MDM Server must be migrated. First you need to migrate Administration Server and then iOS MDM Server as described in the scenario below.

Migration proceeds in stages:

1 Prepare for migration

1. Make sure that you have the administrator's internal user account under which you can log in to Administration Server.

   The administrator's account will be used to log in to Kaspersky Security Center Linux Administration Server. If you do not have this account and you are logged in only under a local Windows account or a domain account, you will not be able to log in to Kaspersky Security Center Linux Administration Server after restoring data from the backup. Kaspersky Security Center Linux Administration Server does not support logging in using the local Windows account. Logging in under the domain account is possible, but may require additional configuration of Administration Server.

   If you do not have the administrator's account, you will have to create this account after restoring data from the backup copy using the kladduser utility.

2. In Kaspersky Security Center Windows, enable the **Inherit settings from Administration Server or parent group** option in the **Security** section of the **Managed devices** group properties window to ensure the inheritance of rights and access to policy settings.

   The **Security** section is available if the **Display security settings sections** check box is selected in the interface settings window.

3. Create a task for downloading updates to the Kaspersky Security Center repository.

   This task is required to download the latest role-based access control configuration file from Kaspersky servers to the repository of Administration Server. For detailed information on creating this task, refer to the Kaspersky Security Center Help.

4. If you need to migrate policies created in the Kaspersky Security for Mobile (Policies) plug-in of Kaspersky Security Center Web Console and Cloud Console, delete all its policy profiles. The policies of this plug-in that contain policy profiles will not be migrated.

2 Create an up-to-date backup copy of the Kaspersky Security Center Windows Administration Server data

Depending on the DBMS type used for Kaspersky Security Center Windows and Kaspersky Security Center Linux, do one of the following:

- To migrate MySQL or MariaDB to MySQL or MariaDB: create a backup copy using the klbackup utility on the device that has Administration Server installed.
- To migrate Microsoft SQL Server to MySQL or MariaDB: create a backup copy using the klbackup utility, with the **Migrate to MySQL/MariaDB format** option enabled.
- To migrate Microsoft SQL Server to PostgreSQL or Postgres Pro:

  a. Install a patch for the corresponding version of Kaspersky Security Center Windows Administration Server:

     - For Kaspersky Secure Mobility Management based on Kaspersky Security Center Windows 14.2: 14.2.0.26967-pf5
     - For Kaspersky Security Center Windows 14.2: 14.2.0.48079-pf5
     - For Kaspersky Security Center Windows 15.1: 15.1.0.20748-pf2

     Contact Kaspersky Technical Support to get these patches.

  b. Create a backup copy using the klbackup utility.

     - If you run klbackup from the command line, use the `-migrate postgres` flag.
     - If you use the klbackup interface, enable the **Migrate to Postgres format** option.

  c. Disconnect Kaspersky Security Center Windows Administration Server from the network.

3 Prepare a new device for the installation of Kaspersky Security Center Linux

1. Choose a new device on which to install Administration Server. This device must meet hardware and software requirements.
2. Make sure that the ports used on Administration Server are available.
3. Assign to the new device the same Host Name and FQDN as on the Windows server.

4. Set the environment variable `KLCS_FF_UMDM_POLICIES_MIGRATION` to 1:

   ```
   export KLCS_FF_UMDM_POLICIES_MIGRATION=1
   ```

   As an alternative, immediately after the installation of Kaspersky Security Center Linux, use the klscflag utility to configure the corresponding server flag using the command:

   ```
   klscflag -fset -pv .core/.independent -s klcsff -n KLCS_FF_UMDM_POLICIES_MIGRATION -t d -v 1
   ```

4 Install and configure the DBMS

1. Choose the DBMS type that provides optimum performance taking into account the number of networked devices, network topology, and load on the network. You can choose from one of the supported DBMSes.

2. Install the DBMS that corresponds to the DBMS type selected when creating a backup. For detailed information on installing the selected DBMS, refer to its documentation.

   > The new database version must not be lower than the current one.

3. Configure the DBMS to work with Kaspersky Security Center Linux.

5 Install Kaspersky Security Center Linux and complete the migration of Administration Server

1. Install Kaspersky Security Center Linux on the new device.

   The administrator's internal user account created during the installation, as well as other objects (groups, policies, tasks, users) created before the restoration of Administration Server data from the backup, will be lost after the restoration. These objects will be replaced by objects that are contained in the backup.

2. After the installation is complete, restore the Administration Server data on the new device using the klbackup utility.

   > Due to limitations of PostgreSQL, you need to temporarily grant PostgreSQL superuser privileges to the account that Administration Server uses to connect to the DBMS.

   > We recommend that you start the data restoration process immediately after the Kaspersky Security Center Linux installation without any intermediate reboots.

3. If you did not have the administrator's internal user account under which you were logged in to Kaspersky Security Center Windows Administration Server and you used a local Windows account or a domain account, create an administrator's account using the kladduser utility:

   ```
   /opt/kaspersky/ksc64/sbin/kladduser -n ksc -p <password>
   ```

   where the `<password>` parameter meets the following requirements:

   - The user password cannot have less than 8 or more than 256 characters
   - The password must contain characters from at least three of the groups listed below:
     - Uppercase letters (A-Z)
     - Lowercase letters (a-z)

- Numbers (0-9)
- Special characters (@ # $ % ^ & * - _ ! + = [ ] { } | : ' , . ? / \ ` ~ " ( ) ;)

4. Check the restoration status (for example, using the `journalctl -u kladminserver_srv.service -b` command) to ensure that mobile policies migrate successfully.
5. Install Kaspersky Security Center Web Console.
6. Log in to Kaspersky Security Center Web Console under the administrator's internal user account.

   The data initialization process usually takes up to 15 minutes after the Administration Server data is restored. The exact time depends on hardware performance and the volume of Administration Server data. During this time, Kaspersky Security Center Web Console may fail to connect and may display errors.
7. Deploy the mobile management plug-ins.
8. Install Network Agent Linux.
9. Check the functionality of the main Administration Server features when the data initialization in the database is complete. Verify that Administration Server synchronizes with managed devices and the Administration Server data is restored.

   Forced synchronization with mobile devices is performed to check their connection after migration.
10. Poll domain controllers to restore information on the domain structure, user accounts, groups, and DNS names of devices that are included in the domains.
11. If necessary, uninstall Administration Server and the database server from the previous device.

    There must not be multiple Administration Servers on the same network with the same connection address and Administration Server certificate.

    The administrator now has access to the Administration Server data and devices previously managed by Kaspersky Security Center Windows, taking into account the functionality supported in Kaspersky Security Center Linux.

    For the **Saving location history** option of the **Location tracking** policy settings to work correctly, add the **Device location history** event type on the **Event settings** tab and enable its storage in the Administration Server database in the event properties. This action must be performed for all migrated policies.

6 Migrate the iOS MDM Server Windows data

If you have multiple iOS MDM Servers installed, you need to perform the migration procedure for each of them.

1. Make sure that the FQDN of iOS MDM Server Linux is the same as the FQDN of iOS MDM Server Windows.
2. If you have reserve iOS MDM Server certificates, make sure that the kliosmdm.ini file located in the iOS MDM working directory contains the SrvResCertPwd password.

   If there is no password in the kliosmdm.ini file, reissue or delete the reserve iOS MDM Server certificate (kliosmdmserver2_cert.pem), the password for which is missing from the file.
3. Create a backup copy of iOS MDM Server using the kliosbackup utility.
4. Deploy iOS MDM Server on the new device with Kaspersky Security Center Linux installed.
5. Transfer the files with iOS MDM Server backup data to the new device.
6. Restore iOS MDM Server data using the kliosbackup utility.

   If any setting value fails to migrate, it will be replaced with the default value.

Once the migration process is complete, all connected devices are automatically synchronized with iOS MDM Server Linux without the need for reconnection.

Backing up and restoring Administration Server data using the klbackup utility

Migration from Kaspersky Security Center Windows to Kaspersky Security Center Linux is performed using the klbackup utility, which is included in the Kaspersky Security Center distribution kit. After the installation of Administration Server, the utility is located in the root of the destination folder specified during installation.

To migrate Administration Server Windows data using the klbackup utility:

1. Create a backup copy of Administration Server data on a Windows device that has Administration Server installed
2. Restore Administration Server data from the created backup copy on a Linux device

Backing up Administration Server data on a Windows device

You can backup Administration Server Windows data using the klbackup utility, which runs in two modes:

- Interactive
- Silent

Backing up Administration Server Windows data in interactive mode

To create a backup copy of Administration Server Windows data in interactive mode:

1. On a Windows device, run the klbackup utility located in the Kaspersky Security Center installation folder (by default, `C:\Program Files (x86)\Kaspersky Lab\Kaspersky Security Center\klbackup.exe`).

2. In the first window of the wizard, select **Perform backup of Administration Server data**.

   Click **Next**.

3. In the next window of the wizard:

   a. Specify the **Backup destination folder**.

   b. Enable the **Migrate database** option.

   c. Select one of the following options:

      a. **Migrate to MySQL/MariaDB format**

      Enable this option if you currently use SQL Server as the DBMS for Administration Server and you want to migrate the data from SQL Server to MySQL or MariaDB DBMS. Kaspersky Security Center will create a backup compatible with MySQL and MariaDB. After that, you can restore the data from the backup into MySQL or MariaDB.

      b. **Migrate to Postgres format**

      Enable this option if you currently use SQL Server as the DBMS for Administration Server and you want to migrate the data from SQL Server to PostgreSQL or Postgres Pro DBMS. Kaspersky Security Center will create a backup compatible with PostgreSQL and Postgres Pro. After that, you can restore the data from the backup into PostgreSQL or Postgres Pro.

      This option becomes available only if you install a patch for the corresponding version of Kaspersky Security Center Windows Administration Server. Contact Kaspersky Technical Support to get the required patch.

      For Kaspersky Secure Mobility Management based on Kaspersky Security Center Windows 14.2: 14.2.0.26967-pf5

      For Kaspersky Security Center Windows 14.2: 14.2.0.48079-pf5

      For Kaspersky Security Center Windows 15.1: use the 15.1.0.20748-pf2

   d. Enable the **Include current date and time in the name of the backup destination folder** option.

e. Set a password to protect sensitive data.

Click **Next** to start the backup process.

A backup copy of the Administration Server data is created.

An error may occur when restoring Administration Server data from a backup copy created using the klbackup utility in interactive mode. If you create a backup copy using the klbackup utility with the 15.1.0.20748-pf2 patch installed and the **Migrate database** option disabled, an error occurs when restoring this copy (for all DBMSes, except MySQL and MariaDB). If you want to create a backup copy with the 15.1.0.20748-pf2 patch installed without migrating to another DBMS, run the klbackup utility from the command line.

Backing up Administration Server Windows data in silent mode

To create a backup copy of Administration Server Windows data in silent mode, run the klbackup utility with the required set of keys from the command line of the device that has Administration Server installed.

Example:

```
cd 'C:\Program Files (x86)\Kaspersky Lab\Kaspersky Security Center\'
klbackup.exe -migrate postgres -path BACKUP_PATH -use_ts -password PASSWORD
```

If no password is specified in the command line of klbackup, the utility prompts you to enter the password interactively.

Descriptions of the keys:

- `-path BACKUP_PATH` — Save information in the `BACKUP_PATH` folder (mandatory parameter).

  The database server account and the klbackup utility need to be granted permissions to change data in the `BACKUP_PATH` folder.

- `-migrate mysql` — Create a backup of Administration Server data stored in an SQL Server database that is compatible with MySQL (including MariaDB). You can restore the data from the backup into MySQL.

- `-migrate postgres` — Create a backup of Administration Server data stored in an SQL Server database that is compatible with PostgreSQL and Postgres Pro. You can restore the data from the backup into PostgreSQL or Postgres Pro.

  This option becomes available only if you install a patch for the corresponding version of Kaspersky Security Center Windows Administration Server. Contact Kaspersky Technical Support to get the required patch.

  For Kaspersky Secure Mobility Management based on Kaspersky Security Center Windows 14.2: 14.2.0.26967-pf5

  For Kaspersky Security Center Windows 14.2: 14.2.0.48079-pf5

  For Kaspersky Security Center Windows 15.1: 15.1.0.20748-pf2

- `-use_ts` — When saving the data, copy the information to the `BACKUP_PATH` folder, to a subfolder with a name formatted as `klbackup YYYY-MM-DD # HH-MM-SS`, which includes the backup operation's current date and time in UTC. If no key is specified, the information is saved in the root of the `BACKUP_PATH` folder.

An error message appears during any attempt to save information in a folder that already stores a backup copy. In this case, no information is updated.

The `-use_ts` key lets you maintain an archive of Administration Server data. For example, if the `-path` key indicates the `C:\KLBackups` folder, the `klbackup 2025/6/19 # 11-30-18` folder then stores information about the status of Administration Server as of June 19, 2025, at 11:30:18 AM.

- `-password PASSWORD` — Password to protect sensitive data.

A forgotten password cannot be recovered. There are no password requirements. The password length is unlimited and zero length (no password) is also acceptable.

To view a full list of the utility keys, refer to the Kaspersky Security Center Help.

Restoring Administration Server data on a Linux device

You can restore Administration Server Windows data from a backup copy on a Linux device in silent mode by running the klbackup utility with the required set of keys from the command line.

When you use the klbackup utility, Network Agent flags are not restored and must be configured manually.

Example:
```
/opt/kaspersky/ksc64/sbin/klbackup -path BACKUP_PATH -restore -password PASSWORD
```

Descriptions of the keys:

- `-path BACKUP_PATH` — Use data from the `BACKUP_PATH` folder for restoration (mandatory parameter).

  The database server account and the klbackup utility need to be granted permissions to change data in the `BACKUP_PATH` folder.

- `-restore` — Restore the Administration Server data. Data is restored using the information contained in the `BACKUP_PATH` folder. If no key is specified, data is backed up in the `BACKUP_PATH` folder.

- `-password PASSWORD` — Password to protect sensitive data.

When restoring data, you must enter the password specified during the backup.

To view a full list of the utility keys, refer to the Kaspersky Security Center Help.

Backing up and restoring the iOS MDM Server data using the kliosbackup utility

Migration from iOS MDM Server Windows to iOS MDM Server Linux is performed using the kliosbackup utility, which lets you backup and restore information on all connected iOS MDM devices and their properties. The utility runs in silent mode.

For the transferred mobile devices to be displayed correctly in Kaspersky Next Expert View (on-premise), both Administration Server and iOS MDM Server must be migrated. For detailed information on the migration scenario, refer to the Migrating from Kaspersky Security Center Windows to Kaspersky Security Center Linux section.

By default, the kliosbackup utility is located in the following installation folder:

- For Windows: `C:\Program Files (x86)\Kaspersky Lab\Mobile Device Management for IOS`
- For Linux: `/opt/kaspersky/iosmdm/bin/`

To migrate iOS MDM Server Windows data using the kliosbackup utility:

1. Create a backup copy of iOS MDM Server data on a Windows device that has iOS MDM Server installed.

   Run kliosbackup with the required set of keys from the command line.

   Example:
   ```
   kliosbackup -backup -path BACKUP_PATH [-pwd PASSWORD]
   ```

2. Restore iOS MDM Server data from the created backup copy on a Linux device.

   Transfer the files with iOS MDM Server backup data to a Linux device, and then run kliosbackup with the required set of keys from the command line.

   Example:
   ```
   kliosbackup -restore -path BACKUP_PATH [-pwd PASSWORD]
   ```

Descriptions of the keys:

- `-backup` — Create a backup the iOS MDM Server data.
- `-restore` — Restore the iOS MDM Server data. Data is restored using the information contained in the `BACKUP_PATH` folder.
- `-path BACKUP_PATH` — Specify a local path to the folder with backup data.
- `-pwd PASSWORD` — Set a backup password.

Deploying an iOS device management system

Advanced MDM in Kaspersky Next Expert View (on-premise) lets you manage mobile devices running iOS. This section describes the deployment of an iOS device management system.

About iOS device operating modes

The device operating mode depends on the owner of the mobile device (personal or corporate) and corporate security requirements. You can choose the operating mode that is most suitable for your company and use several modes at the same time.

The following device operating modes are available for iOS devices:

- Basic protection
- Basic control
- Supervised

Basic protection

Basic protection is the device operating mode for personal or corporate iOS devices. This operating mode lets you protect against web threats and detect jailbreaking on devices using the Kaspersky Protection for iOS app.

Basic control

Basic control is the device operating mode for personal iOS devices. This operating mode lets you protect and perform basic management of devices.

The user is allowed to use a personal Apple ID, work with any apps, and store personal data on the device. You can configure policy settings to control user's access to corporate resources and manage other security requirements.

To manage iOS devices in the basic control operating mode, you must have an installed and configured iOS MDM Server.

Supervised

Supervised is the device operating mode for corporate iOS devices. This operating mode provides a wider range of settings to define through the policy than devices in other operating modes, for example:

- Send additional commands to manage Bluetooth settings, update operating system, locate device or sound alarm in Lost Mode.
- Manage advanced restrictions:
  - Network restrictions (prohibit modifying Personal Hotspot settings, prohibit creating VPN configurations, force Wi-Fi on and allow connection to specified Wi-Fi networks on, prohibit modifying Bluetooth settings).
  - App restrictions (for example, prohibit installation of apps from Apple Configurator and iTunes).
  - Prohibit access to USB devices in Files and disable access to USB devices when the device is locked.
- Configure advanced App Control settings (for example, create custom lists of allowed and forbidden apps).
- Configure Web Control settings.
- Configure an HTTP proxy server to monitor internet traffic on a device within the corporate network.

To manage iOS devices in the supervised operating mode, you must have an installed and configured iOS MDM Server and devices switched to the supervised status in Apple Configurator. For detailed information on working with Apple Configurator, refer to the Apple Technical Support website.

About management profiles

A *management profile* is a profile that contains the settings for connecting mobile devices running iOS to Kaspersky Security Center. After installation of management profile and device synchronization with iOS MDM Server, the device becomes a managed device (iOS MDM device). iOS MDM devices are managed through the Apple Push Notification service (APNs).

Using a management profile, you can do the following:

- Remotely configure the settings of iOS devices using policies.
- Send commands to iOS MDM devices.
- Remotely install Kaspersky apps and third-party apps.

The deployment of a management profile is carried out via Kaspersky Next Expert View (on-premise) using the Mobile device connection wizard. The user installs the management profile after receiving an email with the details for connecting the mobile device to Kaspersky Security Center. No additional preparations for the profile are required.

Before installing a management profile, you must deploy an iOS device management system.

Deploying Kaspersky Protection for iOS

iOS devices in basic protection operating mode are protected by the Kaspersky Protection for iOS app installed on users' devices.

This section contains information about the Kaspersky Protection for iOS app's features as well as the process for installation, activation, updating, and removal.

About Kaspersky Protection for iOS

Kaspersky Protection for iOS ensures protection of mobile devices against phishing and web threats. Kaspersky Protection for iOS offers the following key features:

- Web Protection
- Jailbreak detection

Web Protection

Web Protection blocks malicious websites designed to spread malicious code and also blocks phishing websites designed to steal the user's confidential data (for example, passwords for online banking or e-money systems) and access the user's financial info. Web Protection also monitors the network activity of apps and all system traffic on the user's device.

Web Protection uses the Kaspersky Security Network cloud service to scan websites before they are opened. After scanning, Web Protection allows trustworthy websites to load and blocks malicious websites.

Only the website domain is scanned. If it is a malicious or phishing domain, Web Protection blocks the threat. If the domain is not classified as malicious or phishing, the specific URL is not blocked.

Web Protection requires the following to operate on a managed device:

- The use of Kaspersky Security Network is enabled in the policy settings of Kaspersky Next Expert View (on-premise).
- The user allowed the Kaspersky Protection for iOS app to add a VPN configuration.

You can configure this app component in Kaspersky Next Expert View (on-premise) by specifying the corresponding policy settings.

Jailbreak detection

When the Kaspersky Protection for iOS app detects a jailbreak, it displays a critical message and informs you about the issue.

A jailbreak allows bypassing the operating system's security features, so the security of the user's device cannot be guaranteed, and various problems may arise, including:

- Security vulnerabilities
- Stability issues
- Disruption of Apple services
- Potential crashes and freezes
- Shortened battery life
- Inability to apply iOS updates

Installing Kaspersky Protection for iOS

After completing the Mobile device connection wizard, the app can be installed in the following ways:

- If you chose the **Send a message to users' email addresses** option, the specified users will receive emails with QR codes and links for connecting mobile devices to the Administration Server. The link contains all the information about the connection settings that will be automatically transferred to the app during installation.

  The invitation link is valid for 24 hours. If the user doesn't manage to install the app in time, create and send a new invitation.

  Once the user installs Kaspersky Protection for iOS, the iOS device in basic protection operating mode will connect to the Administration Server and appear on the **Devices** tab of Kaspersky Next Expert View (on-premise).

If the user's device is not connected to Kaspersky Security Center, the user can activate the app manually using the activation code you send.

- If you chose the **Show the details after completing the wizard** option, the connection details will be available on the Finish screen. Scan the QR code using the camera of the iOS device that you want to install the app on.

Activating Kaspersky Protection for iOS

In Kaspersky Security Center, the license can cover various groups of features. To ensure that the Kaspersky Protection for iOS app is fully functional, the Kaspersky Security Center license purchased by the organization must support the Mobile Device Management functionality.

For detailed information about licensing options, refer to the About the license section.

The Kaspersky Protection for iOS app is activated on a mobile device by providing valid license information to the app. License information is delivered to the device together with the policy settings as soon as the device is synchronized with Kaspersky Security Center.

If activation of the mobile app is not completed within 30 days from the time of installation on the mobile device, the app is automatically switched to limited functionality mode. In this mode, most of the app components are not operational. When switched to limited functionality mode, the app stops performing automatic synchronization with Kaspersky Security Center. Accordingly, if activation of the app has not been completed within 30 days after the installation, the user must synchronize the device with Kaspersky Security Center manually.

If Kaspersky Security Center is not deployed in your organization or is not accessible to mobile devices, users can activate the mobile app on their devices manually.

To activate the mobile app:

1. In the main window of Kaspersky Next Expert View (on-premise), select **Asset management** → **Policies**. In the list of group policies that opens, click the name of the policy that you want to configure.

2. In the policy properties window, select **Application settings**.

3. Click the **License** button.

4. In the window that opens, use the drop-down list to select the required license key from the key storage of the Administration Server.

   The details of the license key are displayed in the fields below.

If a key file is selected from the Kaspersky Security Center key storage and sent to the device, Kaspersky Protection for iOS will be not able to process it, because Kaspersky Protection for iOS does not support this activation method. To activate Kaspersky Protection for iOS, you must add an activation code to Kaspersky Security Center.

You can replace the existing activation key on the mobile device if it is different from the one selected in the drop-down list above. To do so, select the **Replace with selected key if the key on devices is different** check box.

However, on some iOS devices, the existing activation key may be replaced by a new one in the background later than expected if the user quit Kaspersky Protection for iOS by swiping up in the App Switcher. To force a license update, the user must reopen the app. For more information about restrictions and recommendations related to optimizing background task execution, see the Known issues of Kaspersky Protection for iOS section.

5. Click **Save** to save the changes you have made.

The app is activated after the next device synchronization with the Administration Server.

The user can also contact the administrator for an activation code and enter it manually.

Updating Kaspersky Protection for iOS

Kaspersky Protection for iOS is updated by following the standard app update procedure on the iOS platform. For detailed information about updating, refer to the Update the app section.

Removing Kaspersky Protection for iOS

A user removes the Kaspersky Protection for iOS app manually by following the standard app removal procedure on the iOS platform. For detailed information about removal, refer to the Remove the app section.

Deploying a management system using the iOS MDM protocol

iOS devices with basic control and supervised operating modes are managed using the iOS MDM protocol. To deploy a mobile management system using the iOS MDM protocol and connect iOS devices to Kaspersky Security Center, follow these steps:

1. **Deploy iOS MDM Server**
2. **Receive an APNs certificate**
3. **Install the APNs certificate on iOS MDM Server**
4. **Connect iOS devices to Kaspersky Security Center**

Deploying iOS MDM Server

iOS MDM Server is a component of Advanced MDM in Kaspersky Next Expert View (on-premise) which allows iOS MDM devices to connect to Kaspersky Security Center and facilitates management of these devices through Apple Push Notifications (APNs) by installing dedicated management profiles on them.

iOS MDM Server receives inbound connections from mobile devices through its TLS port (by default, port 443), which is managed by Kaspersky Security Center using Network Agent. Network Agent is installed locally on a device with an iOS MDM Server deployed.

The number of copies of iOS MDM Server to be installed can be selected either based on available hardware or on the total number of mobile devices covered.

Please keep in mind that the recommended maximum number of mobile devices to be managed through iOS MDM Server is 50,000. In order to reduce the load, the entire pool of devices can be distributed among several servers that have iOS MDM Server installed.

Comparison of iOS MDM Server features depending on the management tools

The available features of iOS MDM Server depend on the management tools.

You can manage iOS MDM Server settings using the following consoles of Kaspersky Security Center:

- Kaspersky Security Center Web Console
- Kaspersky Security Center Cloud Console

The table below compares the features that are available in these tools.

Availability of features by management tool

	Web Console	Cloud Console
General		
Install iOS MDM Server	Available	Available
Update iOS MDM Server	Available	Not available
Delete iOS MDM Server	Available	Not available
View the list of installed iOS MDM Servers	Available	Available
View and modify the settings of installed iOS MDM Servers	Available	Available
Select a certificate to sign a management profile	Available	Not available
View the list of iOS MDM Server events	Available	Available
Configure iOS MDM Server events	Available	Available
APNs proxy server		
Configure a proxy to access APNs	Available	Not available
Certificates		
Receive, renew, and install an APNs certificate	Available	Available
Manage an iOS MDM Server certificate	Available	Not available
Manage a reserve iOS MDM Server certificate	Available	Not available
Manage an iOS MDM Server root certificate	Available	Not available
Connection settings		
Configure a synchronization period	Available	Available
Configure a local access point	Available	Not available
Configure an external access point	Available	Not available
Configure a management profile	Available	Available

	Web Console	Cloud Console
Configuration profiles		
Manage configuration profiles	Available	Available

Configuring an iOS MDM Server installation package

Before you install iOS MDM Server, you need to configure the iOS MDM Server installation package properties.

The iOS MDM Server installation package is an archive that contains the files required for the installation of the iOS MDM Server depending on the package manager and architecture: `kliosmdm-<architecture>-<version>-<package manager>_<language>.tar.gz`

To configure an iOS MDM Server installation package:

1. In the main window of Kaspersky Next Expert View (on-premise), select **Operations** → **Repositories** → **Installation packages**.
2. In the window that opens, click the iOS MDM Server installation package you want to configure.

   The installation package properties window opens.
3. In the **Settings** tab, specify the iOS MDM Server properties.

   a. In the **Connection settings** group of settings, configure the following properties:

   > It is recommended to use the default values.

   - **iOS MDM external connection port**. In this field, specify an external port for connecting mobile devices to the iOS MDM service.

     External port 5223 is used by mobile devices for communication with the APNs server. Make sure that port 5223 is open in the Firewall for connecting with the address range 17.0.0.0/8.

     Port 443 is used for connecting to iOS MDM Server by default. If port 443 is already in use by another service or application, it can be replaced with, for example, port 9443.

     Port 2197 is used by iOS MDM Server to send notifications to the APNs server. APNs servers run in load-balancing mode. Mobile devices do not always connect to the same IP addresses to receive notifications. The 17.0.0.0/8 address range is reserved for Apple, and it is therefore recommended to specify this entire range as an allowed range in Firewall settings.

   - **Network Agent connection port**. In this field, specify a port for connecting the iOS MDM service to Network Agent. The default port number is 9799.

   - **iOS MDM local connection port**. In this field, specify a local port for connecting Network Agent to the iOS MDM service. The default port number is 9899.

   b. In the **iOS MDM Server address** group of settings, specify the address of the workstation on which iOS MDM Server is to be installed. This address will be used for connecting managed mobile devices to the iOS MDM service. The workstation must be available for connection of iOS MDM devices.

Choose one of the following options:

- **Use FQDN device name**. The fully qualified domain name (FQDN) of the device will be used.
- **Use specified address**. Specify the specific address of the device manually.

  Do not add the URL scheme and the port number in the address string. These values will be added automatically.

4. Click **Save**.

The iOS MDM Server installation package properties are configured. Now you can install iOS MDM Server with the specified settings.

Installing iOS MDM Server using a remote installation task

Kaspersky Next Expert View (on-premise) lets you install iOS MDM Server remotely using a remote installation task. This task is created and assigned to up to 1000 devices through a corresponding wizard. The wizard will help install iOS MDM Server in an administration group, on devices with specific IP addresses, or on a selection of managed devices.

Please note that you will not be able to specify the iOS MDM Server settings during the installation. The settings are configured in the iOS MDM Server installation package properties.

Before installing iOS MDM Server on a device, make sure the Kaspersky Mobile Devices Protection and Management and iOS MDM Server settings plug-ins are installed.

To install iOS MDM Server using a remote installation task:

1. Install Network Agent on a workstation on which iOS MDM Server will be deployed.
2. In the main window of Kaspersky Next Expert View (on-premise), select **Asset management → Mobile → iOS MDM Servers**.
3. Click **Install**.

   The New task wizard starts. Proceed through the wizard using the **Next** button.
4. In the **New task settings** window that opens:
   a. In the **Task name** field, specify a custom name for the task, if necessary (The default name is "Install iOS MDM Server").
   b. In the **Devices to which the task will be assigned** group of settings, choose **Specify device addresses manually or import addresses from a list**. You can specify DNS names, IP addresses, and IP subnets of devices to which you want to assign the task.
5. At the **Task scope** step:
   a. Click **Add devices**.
   b. In the window that opens, in the drop-down list, choose the **Select networked devices detected by Administration Server** option.

c. Select devices or a device selection.

d. Click **Add**.

After you add the devices, they are displayed in the table.

6. At the **Installation packages** step, specify the following settings:

   a. In the **Select installation package** field, select the configured iOS MDM Server installation package.

   b. In the **Select Network Agent** field, select the installed Network Agent.

   c. In the **Force installation package download** group of settings, select the **Using Network Agent** check box to distribute the files that are required for iOS MDM Server installation via Network Agent.

   d. In the **Maximum number of concurrent downloads** field, specify the maximum allowed number of devices to which Administration Server can simultaneously transmit the files.

   e. In the **Maximum number of installation attempts** field, specify the maximum number of times the installer will be allowed to run.

   f. Specify the additional settings:

   - Click the **Do not re-install application if it is already installed** check box. The application will not be re-installed if it has already been installed on the device.

   - Click the **Verify operating system type before downloading** check box. Before transmitting the files to devices, Kaspersky Security Center checks if the installation utility settings are applicable to the operating system of the device. If the settings are not applicable, Kaspersky Security Center does not transmit the files and does not attempt to install the application. For example, to install some application to devices of an administration group that includes devices running various operating systems, you can assign the installation task to the administration group, and then enable this option to skip devices that run an operating system other than the required one.

7. At the next step of the wizard, you will be prompted to select the action that will be performed if installation process prompts to restart the operating system. Select the **Do not restart the device** option or skip this step, as it does not apply to Linux operating system.

8. At the **Select accounts to access devices** step, choose the **No account required (Network Agent installed)** option. If this option is selected, you do not have to specify the account under which the application installer will be run. The task will run under the account under which the Administration Server service is running. If Network Agent has not been installed on devices, this option is unavailable.

9. At the **Finish task creation** step, click the **Finish** button to create the task and close the wizard.

iOS MDM Server is installed using a remote installation task.

When reinstalling iOS MDM Server from scratch, you must delete the /var/opt/kaspersky/iosmdm folder on the host with the installed iOS MDM Server. If the folder has not been deleted, the certificate of the old iOS MDM Server will be automatically used during the installation, and a reserve certificate will be issued to the newly installed iOS MDM Server address, if it has been changed.

If you only need to update iOS MDM Server without reinstalling it from scratch, you do not need to delete the specified folder.

For more information about additional settings, file distribution methods, and the assigning the task to a device section, refer to Kaspersky Security Center help.

Local installation of iOS MDM Server on a device via an installation package

Kaspersky Next Expert View (on-premise) lets you install iOS MDM Server on a local device using an installation package, that is, without interactively inputting the installation settings.

Before installing iOS MDM Server on a device, make sure the Kaspersky Mobile Devices Protection and Management and iOS MDM Server settings plug-ins are installed.

To install and configure iOS MDM Server on a local device manually:

1. Install iOS MDM Server:

   a. Read the End User License Agreement. Use the command below only if you understand and accept the terms of the End User License Agreement.

   b. Depending on your operating system, run one of the following commands to launch the installation file:

      a. For Debian:

         ```
         apt install /<path>/kliosmdm_<version_number>_amd64.deb
         ```

      b. For Red Hat Enterprise Linux:

         ```
         yum install /<path>/kliosmdm_<version_number>.x86_64.rpm -y
         ```

      iOS MDM Server is installed. The installer offers to start the setup procedure by executing the postinstall.pl script.

2. Configure iOS MDM Server using one of the methods:

   a. Configuration with the *postinstall* settings specified by the interactive step-by-step wizard:

      a. Run the following command:

         ```
         /opt/kaspersky/iosmdm/lib/bin/setup/postinstall.pl
         ```

   b. Configuration with the key arguments specified as *postinstall* settings:

      a. Run the following command:

         ```
         opt/kaspersky/bin/postinstall.pl -- <params>
         ```

      where `<params>` is one of the settings specified in the *iOS MDM Server installation settings* table below.

The names and possible values for the settings that can be configured when installing iOS MDM Server are listed in the table. You can specify these settings in any convenient order.

Setting name	Setting description	Values
EULA_ACCEPTED	Acceptance of the terms of the End User License Agreement. This setting is mandatory.	• *1* - I have fully read, understand and accept the terms of the End User License Agreement • *Other value or no value* - I do not accept the terms of the License Agreement (installation is not performed)
DONT_USE_ANSWER_FILE	Whether or not to use a TXT answer file with iOS MDM Server installation settings. The file is included in the installation package or stored on the Administration Server. You do not have to specify an additional path to the file. This setting is mandatory.	• *1* - Do not use an answer with settings • *Other value or no value* - Use an answer file with settings
CONNECTORPORT	Local port for connecting the iOS MDM service to Network Agent. The default port number is 9799. This setting is optional.	Numerical value - *9799*
LOCALSERVERPORT	Local port for connecting Network Agent to the iOS MDM service. The default port number is 9899. This setting is optional.	Numerical value - *9899*
EXTERNALSERVERPORT	Port for connecting a device to iOS MDM Server. The default port number is 443. This setting is optional.	Numerical value - *443*
EXTERNAL_SERVER_URL	External address of the device on which iOS MDM Server is to be installed. This address will be used for connecting managed mobile devices to the iOS MDM service. The device must be available for connection through iOS MDM. The address must not include the URL scheme and number of the port because these values will be added automatically. This setting is optional.	Device FQDN - *example.fqdn.com*

Example:
```
/opt/kaspersky/bin/postinstall.pl --EULA 1 --DONT_USE_ANSWER_FILE 1 --EXTERNALSERVERPORT 9443 --CONNECTORPORT 9799
```

To install and configure iOS MDM Server in silent mode automatically using an answer file:

An *answer file* is a text file that contains a custom set of installation settings (variables and their corresponding values).

1. Create an answer file (in TXT format) in the directory where the installation will be performed: `/tmp/answers.txt`.

2. Specify the required values in the answer file:

   - EULA_ACCEPTED=1

     Acceptance of the terms of the End User License Agreement.

   - KLIOSMDM_AUTOINSTALL=1

     Using a TXT answer file with iOS MDM Server installation settings.

   - EXTERNALSERVERPORT=443

     Port for connecting a device to iOS MDM Server.

- CONNECTORPORT=9799

  Local port for connecting the iOS MDM service to Network Agent.

- LOCALSERVERPORT=9899

  Local port for connecting Network Agent to the iOS MDM service.

- EXTERNAL_SERVER_URL=example.fqdn.com

  External address of the device on which iOS MDM Server is to be installed.

3. Set the value of the KLAUTOANSWERS environment variable by entering the full name of the answer file (including the path), for example: `export KLAUTOANSWERS=/tmp/answers.txt`.

4. Launch the iOS MDM Server installation.

iOS MDM Server is installed and configured in silent mode automatically using an answer file.

When reinstalling iOS MDM Server from scratch, you must delete the /var/opt/kaspersky/iosmdm folder on the host with the installed iOS MDM Server. If the folder has not been deleted, the certificate of the old iOS MDM Server will be automatically used during the installation, and a reserve certificate will be issued to the newly installed iOS MDM Server address, if it has been changed.

If you only need to update iOS MDM Server without reinstalling it from scratch, you do not need to delete the specified folder.

Updating iOS MDM Server using a remote installation task or locally

Kaspersky Next Expert View (on-premise) lets you update iOS MDM Server using a remote installation task or locally on a device.

Please note that you will not be able to specify the iOS MDM Server settings during the update. The settings are configured in the iOS MDM Server installation package properties.

To update iOS MDM Server using a remote installation task:

1. In the main window of Kaspersky Next Expert View (on-premise), select **Asset management** → **Mobile** → **iOS MDM Servers**.

2. Click **Update**.

   The New task wizard starts. Proceed through the wizard using the **Next** button.

3. In the **New task settings** window that opens:

   a. In the **Task name** field, specify a custom name for the task, if necessary (The default name is Update iOS MDM Server).

   b. In the **Devices to which the task will be assigned** group of settings, the device on which iOS MDM Server is installed will be displayed.

4. At the **Installation packages** step, specify the following settings:

    a. In the **Select installation package** field, select the configured iOS MDM Server installation package.

    b. In the **Force installation package download** group of settings, select the **Using Network Agent** check box to distribute the files that are required to update iOS MDM Server via Network Agent.

    c. In the **Maximum number of concurrent downloads** field, specify the maximum allowed number of client devices to which Administration Server can simultaneously transmit the files.

    d. In the **Maximum number of installation attempts** field, specify the maximum number of times the installer will be allowed to run.

    e. Specify the additional settings:

    - Click the **Do not re-install application if it is already installed** check box. The application will not be re-installed if it has already been installed on this device.

    - Click the **Verify operating system type before downloading** check box. Before transmitting the files to devices, Kaspersky Security Center checks if the installation utility settings are applicable to the operating system of the device. If the settings are not applicable, Kaspersky Security Center does not transmit the files and does not attempt to install the application. For example, to install some application on devices of an administration group that includes devices running various operating systems, you can assign the installation task to the administration group, and then enable this option to skip devices that run an operating system other than the required one.

5. At the next step of the wizard, you will be asked to select the action that will be performed if the application installation prompts you to restart the operating system. Select the **Do not restart the device** option or skip this step, as it does not apply to the Linux operating system.

6. At the **Select accounts to access devices** step, choose the **No account required (Network Agent installed)** option. If this option is selected, you do not have to specify the account under which the application installer will be run. The task will run under the account under which the Administration Server service is running. If Network Agent has not been installed on devices, this option is unavailable.

7. At the **Finish task creation** step, click the **Finish** button to create the task and close the wizard.

iOS MDM Server is updated using the remote installation task.

To update iOS MDM Server locally, follow the steps described for Local installation of iOS MDM Server on a device via installation package using the newer version of the installation package.

Deleting iOS MDM Server using a remote uninstallation task

Kaspersky Next Expert View (on-premise) lets you delete iOS MDM Server remotely using a remote uninstallation task.

Before deleting iOS MDM Server, make sure the iOS MDM Server installation package has been created and added to the Administration Server repository (**Operations** > **Repositories** > **Installation packages**).

To delete iOS MDM Server:

1. In the main window of Kaspersky Next Expert View (on-premise), select **Asset management** → **Mobile** → **iOS MDM Servers**.

2. Select the iOS MDM Server that you want to uninstall, and then click **Delete**.

   The New task wizard starts. Follow the wizard steps as described in the Kaspersky Security Center Help.

Viewing the list of installed iOS MDM Servers and configuring their settings

Kaspersky Next Expert View (on-premise) lets you view the list of installed iOS MDM Servers and access their settings.

To view the installed iOS MDM Servers:

1. In the main window of Kaspersky Next Expert View (on-premise), select **Asset management** → **Mobile** → **iOS MDM Servers**.

2. In the list of installed iOS MDM Servers that opens:

   a. To install iOS MDM Server, click **Install**.

   b. To update iOS MDM Server, click **Update**.

   c. To delete iOS MDM Server, click **Delete**.

   d. To view or configure the iOS MDM Server settings, do one of the following:

   - Select the check box next to the iOS MDM Server whose settings you want view or configure, and then click **Modify settings**.

     The **Application settings** tab of the iOS MDM Server settings window opens.

   - Click the name of the iOS MDM Server whose settings you want view or configure.

     In the iOS MDM Server settings window that opens, navigate to the **Application settings** tab.

To view or configure the iOS MDM Server settings:

1. Navigate to the **Application settings** tab of the iOS MDM Server settings window using the instructions above.

   a. In the **General** section, you can view the general iOS MDM Server properties.

   - **Name**. The iOS MDM Server custom name.
   - **Version**. The version of the installed iOS MDM Server.
   - **Modified**. The date and time of the latest iOS MDM Server update or modification.
   - **Host name**. The name of the device on which iOS MDM Server is installed.
   - **Host path**. The path to iOS MDM Server on the device on which it is installed.

   > You cannot modify the settings in this section.

b. In the **APNs proxy server** section, you can specify the following settings for Apple Push Notification Service (APNs):

- **Address**. APNs proxy server address.
- **Port**. APNs proxy server port.
- **User name**. APNs proxy user name.
- **Password**. APNs proxy password.

> If you intend to access APNs from the iOS MDM service through a proxy server, the **Use proxy server to connect to APNs** option must be enabled.

> For detailed information on APNs proxy server, refer to the Configuring access to Apple Push Notification service section.

c. In the **Certificates** section, you can manage the certificates required for the operation of iOS MDM Server.

- **Apple Push Notification service (APNs) certificate**. The APNs certificate is signed by Apple and lets you use Apple Push Notification. Through Apple Push Notification, an iOS MDM Server can manage iOS devices. For detailed information on the APNs certificate, refer to the Receiving or renewing an APNs certificate section.
- **iOS MDM Server certificate**. The iOS MDM Server certificate is used to establish the connection and verify trust between iOS devices and iOS MDM Server.
- **iOS MDM Server reserve certificate**. The iOS MDM Server reserve certificate ensures seamless switching of iOS devices after the main iOS MDM Server certificate expires. For detailed information on the iOS MDM Server reserve certificate, refer to the Configuring a reserve iOS MDM Server certificate section.
- **iOS MDM Server root certificate**. The iOS MDM Server root certificate is stored and managed by Kaspersky Security Center. It is sent to iOS MDM Server during the connection to Kaspersky Security Center and is used to issue mobile certificates by Kaspersky Security Center to authenticate iOS MDM devices via the mTLS protocol.

d. In the **Connection settings** section, you can view and configure the settings for mobile device connection to iOS MDM Server.

- In the **Synchronization** block of settings, you can enable or disable the synchronization of managed devices with iOS MDM Server and specify the **Synchronization period (min)**.
- In the **Local access point** block of settings, you can specify the **Network Agent connection port** (a port for connecting iOS devices to Network Agent) and **iOS MDM local connection port** (a local port for connecting Network Agent to the iOS MDM service). For detailed information on these values, refer to the Configuring an iOS MDM Server installation package section.
- In the **External access point** block of settings, you can specify the **iOS MDM external connection port** (external port for connecting mobile devices to the iOS MDM service).

- In the **Management profile** block of settings, you can configure the installation profile properties. You can specify **Profile name** (a mandatory field), **Company**, and **Profile description**.

  Please note that the settings in this section are applied to newly connected iOS MDM devices or to previously connected iOS MDM devices when their mobile certificates are renewed.

- In the **Configuration profiles** section, you can view and manage configuration profiles, which are used to centrally define the settings of managed iOS devices and restrict the features of these devices. For detailed information on managing configuration profiles, refer to the Adding a configuration profile, Installing a configuration profile on a device, and Removing a configuration profile from a device sections.

Configuring an iOS MDM Server certificate

The iOS MDM server certificate is used to establish a connection and verify trust between the iOS MDM device and iOS MDM Server.

The iOS MDM Server certificate is issued by Kaspersky Security Center automatically upon the initial deployment of iOS MDM Server and installed on a device where iOS MDM Server is deployed. If you want to use a certificate issued by your certification authority, you need to specify a custom certificate file that will be used as an iOS MDM Server certificate.

If you specify a custom iOS MDM Server certificate, the **Issue** button for the iOS MDM Server reserve certificate will become unavailable. You need to specify the reserve certificate manually by clicking **Install**.

To specify a custom iOS MDM Server certificate:

1. In the main window of Kaspersky Next Expert View (on-premise), select **Asset management → Mobile → iOS MDM Servers**. In the list of iOS MDM Servers that opens, click the iOS MDM Server whose settings you want to configure.

2. In the iOS MDM Server settings window, select **Application settings**.

3. Select the **Certificates** tab.

   a. In the **iOS MDM Server certificate** block of settings, click **Install**.

   b. In the File Explorer window that opens, specify a certificate file in PEM, PFX, or P12 format, and then click **Open**.

   Make sure the certificate you install complies with the following security requirements:

   - Common Name (CN) is specified;
   - a Subject Alternative Name (SAN) of DNS is specified;
   - a certificate publisher is specified;
   - a correct certificate expiration date is specified;
   - the certificate chain is complete;
   - Extended Key Usage (EKU) is XKU_SSL_SERVER (1.3.6.1.5.5.7.3.1 serverAuth);

- the RSA key size in the certificate chain is at least 2048 bits;
- the RSA key size of the root certificate is at least 4096 bits;
- the hash algorithm in the certificate chain is from the SHA-2 family.

c. In the **Installing certificate** window that opens, enter the certificate password, and then click **Install**.

d. Click **Save**.

Your custom certificate is specified as the iOS MDM Server certificate. The certificate details are displayed in the **iOS MDM Server certificate** block of settings.

If you need to renew the iOS MDM Server certificate, we recommend using the reserve iOS MDM Server certificate without reissuing the main certificate.

If you still want to renew the iOS MDM Server certificate, first stop Kaspersky Security Center, Network Agent, and iOS MDM Server applications, delete the kliosmdmserver_cert.pem certificate and its password (string SrvCertPwd= in the kliosmdm.ini file), and then restart Kaspersky Security Center, Network Agent, and iOS MDM Server. Please note that these actions will result in the loss of the iOS MDM Server connection with devices.

Configuring a reserve iOS MDM Server certificate

The iOS MDM Server functionality lets you issue a reserve certificate. This certificate is intended for use in management profiles to ensure seamless switching of managed iOS devices after the iOS MDM Server certificate expires.

If your iOS MDM Server uses a default certificate issued by Kaspersky, you can issue a reserve certificate (or specify your own custom certificate as a reserve one) before the iOS MDM Server certificate expires. By default, the reserve certificate is automatically issued 60 days before the iOS MDM Server certificate expires. The reserve iOS MDM Server certificate becomes the main certificate immediately after the iOS MDM Server certificate expires. The public key is distributed to all managed devices through configuration profiles, so you do not have to transmit it manually.

Please note that the reserve iOS MDM Server certificate is not issued automatically if you use an iOS MDM Server custom certificate. If you use a custom certificate, we recommend that you specify a reserve certificate when installing iOS MDM Server or no later than 30 days before the expiration of the existing iOS MDM Server certificate.

If the certificate expires and no reserve has been specified, the connection between iOS MDM Server and iOS MDM devices will be lost. In this case, to reconnect devices, you must specify a new certificate and reinstall management profiles on each of the managed devices.

To issue a reserve iOS MDM Server certificate or specify a custom reserve certificate:

1. In the main window of Kaspersky Next Expert View (on-premise), select **Asset management → Mobile → iOS MDM Servers**. In the list of iOS MDM Servers that opens, click the iOS MDM Server whose settings you want to configure.
2. In the iOS MDM Server settings window, select **Application settings**.

3. Select the **Certificates** tab.

4. In the **iOS MDM Server reserve certificate** block of settings, do one of the following:

- If you plan to continue using a self-signed certificate (the one issued by Kaspersky):

  a. Click **Issue**.

  > If you have a custom iOS MDM Server certificate specified, the **Issue** button for the iOS MDM Server reserve certificate will be unavailable. You need to specify the reserve certificate manually by clicking **Install**.

  b. In the **Apply iOS MDM Server reserve certificate** window that opens, select one of the two options for the date when the reserve certificate should be applied:

  - If you want to apply the reserve certificate when the current certificate expires, select the **After the current certificate expires** option.
  - If you want to apply the reserve certificate before the current certificate expires, select the **After specified period (days)** option. In the entry field next to this option, specify the duration of the period after which the reserve certificate must replace the current certificate.

  > The validity period of the reserve certificate that you specify cannot exceed the validity period of the current iOS MDM Server certificate.

  c. Click **OK**.

  The self-signed reserve iOS MDM Server certificate is issued and specified as the reserve iOS MDM Server certificate.

  > Please note that when you specify the date when the reserve certificate should be applied, the certificate will be issued before you save the changes in the **Certificates** section. If you want to issue a new reserve certificate, open the iOS MDM Server settings again, remove the previously issued reserve certificate by clicking **Delete**, and issue a new reserve certificate by following the instructions above.

- If you plan to use a custom certificate issued by your certification authority:

  a. Click **Install**.

  b. In the File Explorer window that opens, specify a certificate file in PEM, PFX, or P12 format, and then click **Open**.

  Make sure the certificate you install complies with the following security requirements:

  - a correct Subject Alternative Name (SAN) of DNS is specified;
  - a correct certificate publisher is specified;
  - a correct certificate expiration date is specified;
  - the certificate chain is complete;

- Extended Key Usage (EKU) is XKU_SSL_SERVER (1.3.6.1.5.5.7.3.1 serverAuth);
- the RSA key size in the certificate chain is at least 2048 bits;
- the RSA key size of the root certificate is at least 4096 bits;
- the hash algorithm in the certificate chain is from the SHA-2 family.

c. In the **Installing certificate** window that opens, enter the certificate password, and then click **Install**.

d. Click **Save**.

Your custom certificate is specified as the reserve iOS MDM Server certificate.

Please note that when you specify the date when the reserve certificate should be applied, the certificate will be issued before you save the changes in the **Certificates** section. If you want to issue a new reserve certificate, open the iOS MDM Server settings again, remove the previously issued reserve certificate by clicking **Delete**, and issue a new reserve certificate by following the instructions above.

You have a specified reserve iOS MDM Server certificate. The reserve certificate details are displayed in the **iOS MDM Server reserve certificate** block of settings.

Receiving or renewing an APNs certificate

To ensure proper functioning of the iOS MDM service and timely responses of mobile devices to the administrator's commands, you need to specify an Apple Push Notification service certificate (APNs certificate) in the iOS MDM Server settings.

If you already have an APNs certificate, please consider renewing it instead of receiving a new one. When you replace the existing APNs certificate with a newly created one, Administration Server can no longer manage the previously connected iOS MDM devices.

To issue or renew an APNs certificate:

1. In the main window of Kaspersky Next Expert View (on-premise), select **Asset management → Mobile → iOS MDM Servers**. In the list of iOS MDM Servers that opens, click the iOS MDM Server whose settings you want to configure.
2. In the iOS MDM Server settings window, select **Application settings**.
3. Select the **Certificates** tab.
4. In the **Apple Push Notification service (APNs) certificate** block of settings, click **Issue or renew**.

   The APNs certificate wizard opens. Click **Start** and then proceed through the wizard using the **Back** and **Next** buttons.

   When the Certificate Signing Request (CSR) is created at the first step of the wizard, its private key is stored in the RAM of your device. Accordingly, all the steps of the wizard must be completed without interruption within a single session.

Step 1. Create a Certificate Signing Request (CSR)

To create a CSR:

a. Specify the required information for generating a request file: **Common Name (CN)**, **Organization Name (O)**, **Organization Unit Name (OU)**, **City (L)**, **Region (S)**, **Country (C)**.

b. Click **Download**.

After you save the changes, a CSR file will be generated, and the private key of the certificate will be saved in the device memory.

Step 2. Sign the CSR file

At this step, send the CSR file that you received in the previous step of the wizard to Kaspersky for signing:

a. Click **Go to Kaspersky CompanyAccount**.

b. Send the created CSR file to Kaspersky to be signed.

> Please note that you will be able to sign the CSR file only after you upload a key that lets you use the Mobile Device Management solution.

c. After your request is successfully processed, you will receive a CSR file signed by Kaspersky.

d. Save the received file.

Step 3. Receive the APNs certificate public key

At this step, do one of the following if you want to issue a new certificate or renew an existing one:

To issue a new certificate:

a. Click **Go to Apple portal**.

b. Log in to the Apple portal with a corporate Apple ID.

> We recommend that you avoid using a personal Apple ID. Create a dedicated Apple ID to make it your corporate ID. After you have created an Apple ID, link it with the organization's mailbox, not a mailbox of an employee.

c. Upload a signed CSR file.

The file will be used to generate the public key of the APNs certificate.

d. After your CSR is processed by Apple, you will receive the public key of the APNs certificate.

Save the received file.

To renew a certificate:

a. Click **Go to Apple portal**.

b. Log in to the Apple portal with a corporate Apple ID.

> We recommend that you avoid using a personal Apple ID. Create a dedicated Apple ID to make it your corporate ID. After you have created an Apple ID, link it with the organization's mailbox, not a mailbox of an employee.

c. Specify the certificate you want to renew.

d. Upload a signed CSR file.

The file will be used to generate the public key of the APNs certificate.

e. After your CSR is processed by Apple, you will receive the public key of the APNs certificate.

Save the received file.

Step 4. Specify the APNs certificate public key

At this step, upload the public key file received from Apple in the previous step of the wizard:

a. Click **Select**.

b. In the File Explorer window that opens, specify a certificate file in PEM, PFX, or P12 format, and then click **Open**.

Step 5. Specify the APNs certificate private key password

At this step, enter the certificate name and private key password:

a. In the **Certificate name** field, specify a custom name for the certificate.

b. In the **Private key password** field, specify the private key password for the certificate.

This password will be used to install the APNs certificate on iOS MDM Server.

c. In the **Confirm password**, enter the password again.

Step 6. Complete the CSR

At this step, the APNs certificate is generated and ready to be installed on iOS MDM Server.

a. To complete the CSR, click **Download APNs certificate** to save the created certificate.

b. Click **Done** to exit the wizard.

The private and public keys of the certificate are combined, and the APNs certificate is saved in PEM format.

Now you can install the generated APNs certificate on iOS MDM Server.

Installing an APNs certificate on iOS MDM Server

After the APNs certificate is received, you can install it on iOS MDM Server.

To install the APNs certificate on iOS MDM Server:

1. In the main window of Kaspersky Next Expert View (on-premise), select **Asset management → Mobile → iOS MDM Servers**. In the list of iOS MDM Servers that opens, click the iOS MDM Server whose settings you want to configure.
2. In the iOS MDM Server settings window, select **Application settings**.
3. Select the **Certificates** tab.
4. In the **Apple Push Notification service (APNs) certificate** block of settings:
   a. Click **Install**.
   b. In the File Explorer window that opens, specify a certificate file in PEM format, and then click **Open**.
   Make sure the certificate you install complies with the following security requirements:
   - Common Name (CN) is specified;
   - an APNs topic is specified;
   - a certificate publisher is specified;
   - a correct certificate expiration date is specified.
   c. In the **Installing certificate** window that opens, enter the private key password specified when receiving the APNs certificate, and then click **Install**.

The APNs certificate will be installed on iOS MDM Server. The certificate details will be displayed in the **Apple Push Notification service (APNs) certificate** block of settings.

Configuring access to Apple Push Notification service

To ensure proper functioning of the iOS MDM service and timely responses from mobile devices to the administrator's commands, you need to specify an Apple Push Notification Service certificate (APNs certificate) in the iOS MDM Server settings.

When interacting with Apple Push Notification service (APNs), the iOS MDM service connects to the external address api.push.apple.com through port 2197 (outbound). Therefore, the iOS MDM service requires access to port TCP 2197 for the range of addresses 17.0.0.0/8. From the iOS device, this interaction requires access to port TCP 5223 for the range of addresses 17.0.0.0/8.

If you intend to access APNs from the iOS MDM service through a proxy server, you must enable the use of a proxy server for connecting to APNs.

To enable the use of a proxy server to connect to APNs:

1. In the main window of Kaspersky Next Expert View (on-premise), select **Asset management → Mobile → iOS MDM Servers**. In the list of iOS MDM Servers that opens, click the iOS MDM Server whose settings you want to configure.
2. In the iOS MDM Server settings window, select **Application settings**.
3. Select the **APNs proxy server** tab.
4. In the window that opens, enable the **Use proxy server to connect to APNs** toggle switch.
5. Configure the following settings:
    a. In the **Address** field, specify the APNs proxy server address.
    b. In the **Port** field, specify the APNs proxy server port.
    c. In the **User name** field, specify the APNs proxy user name.
    d. In the **Password** field, specify the APNs proxy password.
6. Click **Save**.

Proxy server is now used to connect to APNs.

iOS MDM Server events

Kaspersky Next Expert View (on-premise) lets you view the events related to iOS MDM Server. The events have different severity levels: *Information*, *Warning*, *Critical*, *Functional failure*.

For each event that can be generated by iOS MDM Server, you can specify notification and storage settings on the **Event configuration** tab of the iOS MDM Server settings. We recommend that you configure the settings for each event type after deploying iOS MDM Server to limit the displayed number of events and reduce the event list loading time.

If you want to configure notification settings for all events at once, configure general notification settings in the Administration Server properties. For detailed information on notifications, refer to the Kaspersky Security Center Help.

To view iOS MDM Server events:

1. In the main window of Kaspersky Next Expert View (on-premise), select **Asset management → Mobile → iOS MDM Servers**. In the list of iOS MDM Servers that opens, click the iOS MDM Server whose events you want to view.
2. In the iOS MDM Server settings window, select **Application settings**.
3. Select the **Events** tab.

The iOS MDM Server events are displayed.

For detailed information on viewing events in Kaspersky Next Expert View (on-premise), refer to the Kaspersky Security Center Help.

The table below shows the events of iOS MDM Server that have the *Information* severity level.

iOS MDM Server information events

Event type display name	Event type	Default storage term
General information about mobile device requested	DEVICEINFORMATION_COMMAND_SUCCESSFUL	30 days
Security information requested	SECURITYINFO_COMMAND_SUCCESSFUL	30 days
New mobile device connected	NEW_DEVICE_CONNECTED	30 days
List of profiles requested	PROFILELIST_COMMAND_SUCCESSFUL	30 days
Profile installed	INSTALLPROFILE_COMMAND_SUCCESSFUL	30 days
Profile deleted	REMOVEPROFILE_COMMAND_SUCCESSFUL	30 days
List of provisioning profiles requested	PROVISIONINGPROFILELIST_COMMAND_SUCCESSFUL	30 days
Provisioning profile installed	INSTALLPROVISIONINGPROFILE_COMMAND_SUCCESSFUL	30 days
Provisioning profile deleted	REMOVEPROVISIONINGPROFILE_COMMAND_SUCCESSFUL	30 days
List of installed certificates requested	CERTIFICATELIST_COMMAND_SUCCESSFUL	30 days
List of installed apps requested	INSTALLEDAPPLICATIONLIST_COMMAND_SUCCESSFUL	30 days
List of managed apps requested	MANAGEDAPPLICATIONLIST_COMMAND_SUCCESSFUL	30 days
App installation requested	INSTALLAPPLICATION_COMMAND_SUCCESSFUL	30 days
App configuration applied	APPCONFIG_APPLIED_SUCCESSFUL	30 days
Managed app deleted	REMOVEAPPLICATION_COMMAND_SUCCESSFUL	30 days
App redemption code set	APPLYREDEMPTIONCODE_COMMAND_SUCCESSFUL	30 days
Mobile device locked	DEVICELOCK_COMMAND_SUCCESSFUL	30 days
Password reset	CLEARPASSCODE_COMMAND_SUCCESSFULL	30 days
Data from mobile device wiped	ERASEDEVICE_COMMAND_SUCCESSFUL	30 days
Operating system update scheduled	SCHEDULEOSUPDATE_COMMAND_SUCCESSFULL	30 days
Roaming settings applied	SETROAMINGSETTINGS_COMMAND_SUCCESSFUL	30 days
Bluetooth settings applied	SETBLUETOOTHSETTINGS_COMMAND_SUCCESSFUL	30 days
Lost Mode enabled	ENABLE_LOST_MODE_COMMAND_SUCCESSFUL	30 days
Sound played in Lost Mode	PLAY_LOST_MODE_SOUND_COMMAND_SUCCESSFUL	30 days
Mobile device location received	GET_DEVICE_LOCATION_COMMAND_SUCCESSFUL	30 days
Lost Mode disabled	DISABLE_LOST_MODE_COMMAND_SUCCESFUL	30 days
Activation lock bypass code received	GET_ACTIVATION_LOCK_BYPASS_CODE_COMMAND_SUCCESSFUL	30 days
Compliance Control check started	COMPLIANCE_CONTROL_CHEKING_RULES_STARTED	30 days
Compliance Control check completed	COMPLIANCE_CONTROL_CHEKING_RULES_COMPLETED	30 days
Compliance Control response started	COMPLIANCE_CONTROL_ACTION_STARTED	30 days
Compliance Control response completed	COMPLIANCE_CONTROL_ACTION_COMPLETED	30 days

The table below shows the events of iOS MDM Server that have the *Warning* severity level.

iOS MDM Server warning events

Event type display name	Event type	Default storage term
Attempt to connect locked mobile device detected	INACTICE_DEVICE_TRY_CONNECTED	30 days
Management profile deleted	MDM_PROFILE_WAS_REMOVED	30 days
Attempt to reuse user certificate detected	CLIENT_CERT_ALREADY_IN_USE	30 days
Non-compliance with Compliance Control criterion detected	COMPLIANCE_CONTROL_CONDITIONS_MATCH_DETECTED	30 days
Failed to perform Compliance Control response	COMPLIANCE_CONTROL_ACTION_FAILED	30 days
Inactive mobile device detected	FOUND_INACTIVE_DEVICE	30 days
Redemption code is required	NEED_REDEMPTION_CODE	30 days
Management profile deleted from mobile device	UMDM_PROFILE_WAS_REMOVED	30 days

The table below shows the events of iOS MDM Server that have the *Functional failure* severity level.

iOS MDM Server functional failure events

Event type display name	Event type	Default storage term
Failed to request general information about mobile device	DEVICEINFORMATION_COMMAND_FAILED	30 days
Failed to request security information	SECURITYINFO_COMMAND_FAILED	30 days
Failed to request list of profiles	PROFILELIST_COMMAND_FAILED	30 days
Failed to install profile	INSTALLPROFILE_COMMAND_FAILED	30 days
Failed to delete profile	REMOVEPROFILE_COMMAND_FAILED	30 days
Failed to request list of provisioning profiles	PROVISIONINGPROFILELIST_COMMAND_FAILED	30 days
Failed to install provisioning profile	INSTALLPROVISIONINGPROFILE_COMMAND_FAILED	30 days
Failed to delete provisioning profile	REMOVEPROVISIONINGPROFILE_COMMAND_FAILED	30 days
Failed to request list of installed certificates	CERTIFICATELIST_COMMAND_FAILED	30 days
Failed to request list of installed apps	INSTALLEDAPPLICATIONLIST_COMMAND_FAILED	30 days
Failed to request list of managed apps	MANAGEDAPPLICATIONLIST_COMMAND_FAILED	30 days
Failed to request app installation	INSTALLAPPLICATION_COMMAND_FAILED	30 days
Failed to apply app configuration	APPCONFIG_APPLIED_FAILED	30 days
Failed to delete managed app	REMOVEAPPLICATION_COMMAND_FAILED	30 days
Failed to set app redemption code	APPLYREDEMPTIONCODE_COMMAND_FAILED	30 days
Failed to lock mobile device	DEVICELOCK_COMMAND_FAILED	30 days
Failed to reset password	CLEARPASSCODE_COMMAND_FAILED	30 days
Failed to wipe data from mobile device	ERASEDEVICE_COMMAND_FAILED	30 days
Failed to schedule operating system update	SCHEDULEOSUPDATE_COMMAND_FAILED	30 days
Failed to apply roaming settings	SETROAMINGSETTINGS_COMMAND_FAILED	30 days
Failed to apply Bluetooth settings	SETBLUETOOTHSETTINGS_COMMAND_FAILED	30 days
Failed to enable Lost Mode	ENABLE_LOST_MODE_COMMAND_FAILED	30 days
Failed to play sound in Lost Mode	PLAY_LOST_MODE_SOUND_COMMAND_FAILED	30 days
Failed to receive mobile device location	GET_DEVICE_LOCATION_COMMAND_FAILED	30 days
Failed to disable Lost Mode	DISABLE_LOST_MODE_COMMAND_FAILED	30 days
Failed to receive activation lock bypass code	GET_ACTIVATION_LOCK_BYPASS_CODE_COMMAND_FAILED	30 days
Error in app operation	PRODUCT_FAILURE	30 days

Event type display name	Event type	Default storage term
Command result contains incorrect data	MALFORMED_COMMAND	30 days
Failed to send message	SEND_PUSH_NOTIFICATION_FAILED	30 days
Failed to send command (Compliance Control)	SEND_COMMAND_FAILED	30 days
Failed to find device	DEVICE_NOT_FOUND	30 days
Failed to configure Per App VPN for app	PERAPP_VPN_SETUP_FAILED	30 days

Obtaining iOS MDM Server diagnostic data

When creating a request to Kaspersky Technical Support, you may be asked to create and attach a trace file. Trace files are used by Technical Support for diagnostic purposes. They contain all steps of application command execution written in the file, which allows to detect the step on which an error occurs.

We recommend that you obtain the traces of iOS MDM Server together with the traces of Network Agent, as they contain the iOS MDM Server connector details.

There are several tracing levels for iOS MDM Server:

- 0 - CRITICAL
- 1 - ERROR
- 2 - MESSAGE
- 3 - DEBUG

Ask a support engineer which tracing level to set. If the Technical Support engineer has not specified the trace level, we recommend obtaining level 2 traces.

To enable the iOS MDM Server tracing and create trace files:

1. Open the iOS MSM Server settings file `/var/opt/kaspersky/iosmdm/settings.ini`.
2. Specify the values required to enable tracing. We recommend that you specify the following default values:
   - *LogCommEnabled*=1
     Enabling or disabling the tracing of the iOS MDM Server and connector communication library.
   - *LogSettingsEnabled*=1
     Enabling or disabling the tracing of the iOS MDM Server and connector settings library.
   - *LogCommVerboseLevel*=2
     The tracing level of the iOS MDM Server and connector communication library.
   - *LogSettingsVerboseLevel*=2
     The tracing level of the iOS MDM Server and connector settings library.

- *LogVerboseLevel*=2

  The tracing level of iOS MDM Server.

- *LogFolder*=/var/opt/kaspersky/iosmdm

  The directory for writing trace files.

3. Restart the iOS MDM Server and Network Agent services by running the following commands:

   ```
   systemctl restart klnagent
   systemctl restart kliosmdm
   ```

   The iOS MDM Server tracing is enabled. Trace files are created in the directory that you specified as the *LogFolder* value: *klcon_comm.log*, *klcon_settings.log*, *klsrv.log*, *klsrv_comm.log*, *klsrv_settings.log*.

To disable the iOS MDM Server tracing:

1. Open the iOS MSM Server settings file `/var/opt/kaspersky/iosmdm/settings.ini`.
2. Modify the file by deleting the strings that have been created to enable tracing:

   - *LogCommEnabled*=1
   - *LogSettingsEnabled*=1
   - *LogCommVerboseLevel*=2
   - *LogSettingsVerboseLevel*=2
   - *LogVerboseLevel*=2
   - *LogFolder*=/var/opt/kaspersky/iosmdm

3. Restart the iOS MDM Server and Network Agent services by running the following commands:

   ```
   systemctl restart klnagent
   systemctl restart kliosmdm
   ```

   The iOS MDM Server tracing is disabled.

Deploying an Android device management system

Advanced MDM in Kaspersky Next Expert View (on-premise) lets you manage mobile devices running Android. This section describes the deployment of an Android device management system.

About Android device operating modes

The device operating mode depends on the owner of mobile device (personal or corporate) and corporate security requirements. You can choose the operating mode that is most suitable for your company and use several modes at the same time.

The following device operating modes are available for Android devices:

- Personal device
- Device with corporate container
- Corporate device

Personal device

Personal device is the device operating mode for personal Android devices. This operating mode lets you protect and perform basic management of devices.

Device with corporate container

Device with corporate container is the device operating mode for personal Android devices with an Android Work Profile, which provides an isolated corporate environment on a device.

This operating mode lets you manage apps and user accounts in a safe environment on a device without restricting the use of personal data by the user. When a Work Profile is created on the user's mobile device, the following corporate apps are automatically installed in the container (if applicable): Google Play Market, Google Chrome, Downloads, Kaspersky Endpoint Security for Android, and others. Corporate apps installed in the Work Profile and their notifications are marked with a blue briefcase icon. Apps installed in the work profile appear in the common list of apps.

Corporate device

Corporate device is the device operating mode for company-owned Android devices. This operating mode lets you have full control over the entire device and configure an extended set of security settings and features:

- Restrictions on Android features
- Management of Google Chrome settings
- Silent installation of required apps and removal of blocked apps in App Control
- Kiosk mode
- Management of Exchange ActiveSync
- NDES and SCEP integration

Using Firebase Cloud Messaging

To ensure timely delivery of commands to Android devices, Kaspersky Security Center uses the mechanism of push notifications. Push notifications are exchanged between Android devices and Administration Server through Firebase Cloud Messaging (hereinafter referred to as FCM). In Kaspersky Next Expert View (on-premise), you can specify the Firebase Cloud Messaging settings to connect Android devices to the service.

To retrieve the settings of Firebase Cloud Messaging, you must have a Google account.

To enable the use of FCM:

1. In the main window of Kaspersky Next Expert View (on-premise), select **Asset management** → **Mobile** → **Devices**.
2. Open the 3-dot menu (⋮) and select **Forced Android device synchronization**.
3. In the **Firebase project number** field, specify the FCM Sender ID.
4. In the **Private key** field, select the private key file.

   At the next synchronization with Administration Server, Android devices will be connected to Firebase Cloud Messaging.

When you switch to a different Firebase project, you need to wait 10 minutes for FCM to resume.

FCM service runs in the following address ranges:

- From the Android device's side, access is required to ports 443 (HTTPS), 5228 (HTTPS), 5229 (HTTPS), and 5230 (HTTPS) of the following addresses:
  - google.com
  - fcm.googleapis.com
  - oauth2.googleapis.com
  - android.apis.google.com
  - All of the IP addresses listed in Google's ASN of 15169
- From the Administration Server side, access is required to port 443 (HTTPS) of the following addresses:
  - fcm.googleapis.com
  - All of the IP addresses listed in Google's ASN of 15169

If the proxy server settings have been specified in the Administration Server properties in Kaspersky Next Expert View (on-premise), they will be used for interaction with FCM.

Configuring FCM: getting the Sender ID and private key file

To configure FCM:

1. Register on the Google portal.
2. Go to the Firebase console.
3. Do one of the following:
   - To create a new project, click **Create a project** and follow the instructions on the screen.
   - Open an existing project.
4. Click the gear icon and choose **Project settings**.
   The **Project settings** window opens.
5. Select the **Cloud Messaging** tab.
6. Retrieve the relevant Sender ID from the **Sender ID** field in the **Firebase Cloud Messaging API (V1)** section.
7. Select the **Service accounts** tab and click **Generate new private key**.
8. In the window that opens, click **Generate key** to generate and download a private key file.

Firebase Cloud Messaging is now configured.

Deploying Kaspersky Endpoint Security for Android

This section contains a general overview of Kaspersky Endpoint Security for Android and the methods of installing, updating, and removing the app.

For detailed information on Kaspersky Endpoint Security for Android, refer to the Using the Kaspersky Endpoint Security for Android app section.

About the Kaspersky Endpoint Security for Android app

The Kaspersky Endpoint Security for Android app ensures the protection of mobile devices against web threats, viruses, and other programs that pose threats.

The Kaspersky Endpoint Security for Android includes the following features:

- **Anti-Malware**. This component detects and neutralizes threats on the device by using the anti-malware databases and the Kaspersky Security Network cloud service. Anti-Malware includes the following components:
  - **Protection**. It detects threats in open files, scans new apps, and prevents device infection in real time.
  - **Scan**. It is started on demand for the entire file system, only for installed apps, or only for a selected file or folder.
  - **Update**. It lets you download new anti-malware databases for the app.
- **Anti-Theft**. This component protects the information on the device against unauthorized access in case the device is lost or stolen. This component lets you send the following commands to the device:
  - **Locate device**. Get the coordinates of the device's location.
  - **Sound alarm**. Make the device sound a loud alarm.
  - **Wipe corporate data**. Erase corporate data to protect sensitive company information.
- **Web Protection** and **Web Control**. Web Protection blocks malicious websites designed to spread malicious code. Web Protection also blocks fake (phishing) websites designed to steal the user's confidential data (for example, passwords for online banking or e-money systems) and access the user's financial info. Web Protection uses the Kaspersky Security Network cloud service to scan websites before they open. After scanning, Web Protection allows trustworthy websites to load and blocks malicious websites. Web Control allows website filtering by categories defined in the Kaspersky Security Network cloud service. This lets the administrator restrict user access to certain categories of web pages (for example, Gambling, lotteries, sweepstakes or Internet communication).
- **App Control**. This component lets you install recommended and required apps to an Android device as well as remove blocked apps that violate corporate security requirements.
- **Compliance Control**. This component lets you check managed devices for compliance with corporate security requirements and impose restrictions on certain functions of non-compliant devices.
- **Call Control**. This component lets you protect managed devices against fraudulent, spam, and other unwanted calls.

You can configure the components of the Kaspersky Endpoint Security for Android app in Kaspersky Next Expert View (on-premise) by defining the corresponding policy settings.

Installing Kaspersky Endpoint Security for Android

There are several methods to deploy the Kaspersky Endpoint Security for Android app. You can use the most suitable installation scenario for your company or combine several installation scenarios.

The installation methods include the following:

- Installation via Kaspersky Security Center using one of the installation sources:
  - **Kaspersky website** (for all operating modes)

    Choose this method for mobile devices that can access the internet to download the APK installation file from the Kaspersky website. The app will then be updated from the Kaspersky website or using HUAWEI AppGallery, Samsung Galaxy Store, RuStore, or Xiaomi GetApps.

  - **Installation package** (for all operating modes)

    The Kaspersky Endpoint Security for Android installation package will be downloaded from the Kaspersky Security Center server and updated via Kaspersky Security Center using policy settings. You can choose this method if mobile devices in your company have no access to the internet.

    For this installation source, before connecting mobile devices, create the Kaspersky Endpoint Security for Android installation package.
- Manual installation

Creating the Kaspersky Endpoint Security for Android installation package

The Kaspersky Endpoint Security for Android app can be deployed using the installation package.

You can use this installation method if mobile devices in your company have no access to the internet.

For this installation method, you need to create a Kaspersky Endpoint Security for Android installation package before connecting Android devices to Kaspersky Security Center. The installation package will be downloaded from Kaspersky Security Center and updated via Kaspersky Security Center using policy settings.

The Kaspersky Endpoint Security for Android installation package is an archive that contains the files required for installing the Kaspersky Endpoint Security for Android app:

- `installer.ini`

  Configuration file that contains Administration Server connection settings.

- `kesandroid<version>_<languages>_Prod_Release.apk`

  Android package file of the Kaspersky Endpoint Security for Android app.

- `ksm.kpd`

  Application description file.

- `eula/`

  Folder with End User License Agreements in different languages in TXT format.

- `kpd.loc/`

  INI files specifying paths to End User License Agreements.

To create the Kaspersky Endpoint Security for Android installation package:

1. In the main window of Kaspersky Next Expert View (on-premise), select **Operations** → **Repositories** → **Installation packages**.

2. In the list of installation packages that opens, click **Add**. The New package wizard starts. Follow the instructions of the wizard as described in the Kaspersky Security Center Help to create an installation package from a file or create a stand-alone installation package.

To configure the Kaspersky Endpoint Security for Android installation package:

1. In the main window of Kaspersky Next Expert View (on-premise), select **Operations** → **Repositories** → **Installation packages**.

2. In the list of installation packages that opens, click the Kaspersky Endpoint Security for Android installation package you want to configure.

3. In the installation package properties window, select the **Settings** tab.

   a. In the **Connection to the Administration Server** group of settings, configure the following values:

      - **Server address**. Specify the address of the server to which the Android devices will connect.

      - **SSL port for devices synchronization**. Specify the number of the port opened on the Administration Server for connecting mobile devices. Port 13292 is used by default.

   b. For stand-alone installation packages, in the **Subgroup name** field of the **Subgroup in Unassigned devices** group of settings, specify the name of the group to which Android devices will be added after the first synchronization with the Administration Server. KES10 is used by default.

   c. In the **Actions during installation on device** group of settings, click the **Prompt user for email address** check box if you want Kaspersky Endpoint Security for Android to ask users to provide their corporate email address when the app is started for the first time.

      User email address is used to form the name of the mobile device when it is added to the administration group.

4. Click **Save**.

The Kaspersky Endpoint Security for Android installation package is configured.

Manual installation of Kaspersky Endpoint Security for Android

You can manually install Kaspersky Endpoint Security for Android from the Kaspersky website, HUAWEI AppGallery, Samsung Galaxy Store, RuStore, or Xiaomi GetApps.

Installing the app

To install the app from an app store, follow the standard installation procedure for the Android platform.

To install Kaspersky Endpoint Security for Android from the Kaspersky website:

1. Go to the Kaspersky website.

2. Find Kaspersky Security for Mobile on the website.

3. Tap **Show Downloads**.
4. Select a version of the app and tap **Download**.
5. Open the downloaded APK file and follow the instructions on the screen.

> You may need to allow your browser to install apps from sources other than Google Play in the **Apps** → **Special app access** → **Install unknown apps** section in device settings. The location of these settings may differ on devices from different vendors.

The app will be installed on the device.

Configuring the app

After installing Kaspersky Endpoint Security for Android, you must manually configure the app. The configuration procedure depends on whether the administrator sent you a server address or a link for downloading the app.

To configure Kaspersky Endpoint Security for Android using a link for downloading the app:

1. Open Kaspersky Endpoint Security for Android.
2. Read the End User License Agreement. If you accept the End User License agreement, select the corresponding check box and tap **Continue**.
3. Tap **Continue** and grant the app the required permissions.
4. In the **Server** field, specify the link that you received from the administrator.
5. Tap **Continue**.

Kaspersky Endpoint Security for Android is configured.

To configure Kaspersky Endpoint Security for Android using a server address:

1. Open Kaspersky Endpoint Security for Android.
2. Read the End User License Agreement. If you accept the End User License agreement, select the corresponding check box and tap **Continue**.
3. Tap **Continue** and grant the app the required permissions.
4. In the **Server** field, specify the Administration Server address provided by the administrator.
5. Tap **Continue**.
6. Tap **Enable** to enable the app as the device administrator.
7. Tap **Allow** and grant the app the required permissions.

Kaspersky Endpoint Security for Android is configured.

Internet access must be enabled on the mobile device for synchronization with the Administration Server.

Installing Kaspersky Endpoint Security for Android on corporate devices in a closed network

When deploying Kaspersky Endpoint Security for Android in corporate device operating mode via QR code on devices with pre-installed Google Mobile Services (GMS), their Wi-Fi connectivity to certain Google endpoints is checked. If a Wi-Fi network has no access to the internet, the connectivity check fails and the deployment finishes with an error.

To avoid the connectivity check, you can deploy the Kaspersky Endpoint Security for Android app on corporate devices in a closed network by using a Proxy Auto-Configuration (PAC) file.

To use a PAC file to deploy the Kaspersky Endpoint Security for Android app:

1. Create a PAC file (for example, proxy.pac) with the following contents:
   ```
   function FindProxyForURL(url, host) {
   return "DIRECT";
   }
   ```

2. Publish the created PAC file on a resource that will be available in the closed network (for example, on an IIS Web server).

   Save a link to the PAC file (for example, https://intranet.mycompany.com/files/proxy.pac).

3. Make sure the APK file of the Kaspersky Endpoint Security for Android app being deployed is available within the closed network. To do this, use one of the methods below:

   - Download the app installation package from the Kaspersky Security Center server. If the server is accessible, the installation packages will be available there.

   - Download the APK installation file from the Kaspersky website and upload it to the closed network.

     Choose the general version of the app as the source.

4. Send the app installation link and QR code to the user by following the instructions of Mobile device connection wizard.

   On the **Operating systems** step of the wizard, in the **Installation settings** section, you will be asked to specify the network for downloading the Kaspersky Endpoint Security for Android app. At this step, configure the use of the previously created PAC file for network connection by linking it to the Wi-Fi network settings on a device. To do this, use one of the methods below:

   - In the **Installation network** settings section, choose **Prompt the user to select a Wi-Fi network on device**. While deploying the app, the user will need to specify the link to the PAC file (step 2) in the network settings when choosing a Wi-Fi network on the device. After the connection is established, the user will be able to continue the device setup and activate the app by following the instructions of the app's Initial Configuration Wizard.

   - In the **Installation network** settings section, choose **Only use the specified Wi-Fi network** (Android 9 or later), click the **Select network** button, and then insert the link to the previously created PAC file (step 2) in the **PAC file URL** field.

   If the APK installation file has been downloaded from the Kaspersky website (step 3), you need to replace the link in the QR code with the address of the closed network link.

When deploying the app via an installation package downloaded from Kaspersky Security Center, after the device is reset to factory settings and the QR code is scanned, a **Blocked by Play Protect** message may appear on the device. The issue is caused by the installation package's signing certificate being different from the one specified in Google Play. The user should continue the installation by choosing **Install anyway**. If **OK** is selected, the installation process will be interrupted and the device will be reset to factory settings.

The Kaspersky Endpoint Security for Android app is installed on a device in corporate device operating mode in a closed network.

Permissions for Kaspersky Endpoint Security for Android

For all features of apps, Kaspersky Endpoint Security for Android prompts the user for the required permissions. Kaspersky Endpoint Security for Android prompts for the mandatory permissions while the Setup Wizard is completed, as well as after installation and prior to using individual features of apps. It is impossible to install Kaspersky Endpoint Security for Android without providing the mandatory permissions.

On certain devices (for example, HUAWEI, Meizu, and Xiaomi), you must manually add Kaspersky Endpoint Security for Android to the list of apps that are started when the operating system starts in the device settings. If the app is not added to the list, Kaspersky Endpoint Security for Android stops performing all of its functions after the mobile device is restarted.

On devices running Android 11 or later or Android 6-10 with Google Play services, you must disable the **Remove permissions if app isn't used** system setting. Otherwise, after the app is not used for a few months, the system automatically resets the permissions that the user granted to the app.

Permissions requested by Kaspersky Endpoint Security for Android

Permission	App function
Phone (read phone status and identity)	Identify the device using its IMEI (for Android 5–9; for Android 10 or later in the corporate device operating mode; for Android 10–11 for the device with corporate container operating mode)
	Compliance Control – check whether the device SIM card has been replaced or removed
Storage (mandatory)	Anti-Malware
Access to manage all files (for Android 11 or later)	Anti-Malware
Nearby devices (for Android 12 or later)	Restrict use of Bluetooth On some Xiaomi and HUAWEI devices running Android 12, Kaspersky Endpoint Security for Android does not prompt the user for the **Nearby Bluetooth devices** permission. This issue is caused by the specific features of MIUI firmware on Xiaomi and EMUI firmware on HUAWEI. Despite the absence of the request for this permission, all features related to using Bluetooth work correctly on these devices.
Ignore battery optimization (for Android 12 or later)	App Control
	Web Protection
	Anti-Theft
Notifications (for Android 13)	Notify the user about security issues and app events
Allow running in the background (for Android 12 or later)	Ensure continuous operation of the app. If permission is not granted, the app may be unloaded from memory and unable to restart.

Permission	App function
Device administrator (mandatory)	Anti-Theft – lock the device (only for Android 5–6)
	Anti-Theft – take a mugshot with frontal camera
	Anti-Theft – sound an alarm
	Anti-Theft – full reset
	Password protection
	App removal protection
	Install security certificate
	App Control
	Manage Knox (only for Samsung devices)
	Configure Wi-Fi
	Configure Exchange ActiveSync
	Restrict use of the camera, Bluetooth, and Wi-Fi
Camera	Anti-Theft – take a mugshot with frontal camera On devices running Android 11 or later, the user must grant the "While using the app" permission when prompted.
Location	Anti-Theft – locate device On devices running Android 10 or later, the user must grant the "All the time" permission when prompted.
	Commands – Get location history
Accessibility	Anti-Theft – lock the device (only for Android 7 or later)
	Web Protection
	App Control
	Call Control
	App removal protection (only for Android 7 or later)
	Display of warnings of Kaspersky Endpoint Security for Android (only for Android 10 or later)
	Restrict use of the camera (only for Android 11 or later)
Display pop-up window (for some Xiaomi devices)	Web Protection
Display pop-up windows while running in the background (for some Xiaomi devices)	Web Protection
Run in the background (for Xiaomi devices with MIUI firmware on Android 11 or earlier)	App Control
	Web Protection
	Anti-Theft
Access to call log	Call Control – check calls and get information about callers
Access to contacts	Call Control – identify who is calling
Permission to manage calls	Call Control – block spam and other unwanted calls

Permission	App function
Allow Kaspersky Endpoint Security for Android to be the default app to identify numbers and spam	Call Control – identify numbers and spam On devices running Android 8-9, allow Kaspersky Endpoint Security for Android to be the default calling app. On devices running Android 10 or later, allow Kaspersky Endpoint Security for Android to be the default Caller ID app.

Starting and stopping Kaspersky Endpoint Security for Android

Kaspersky Endpoint Security for Android launches when the operating system starts up and protects the mobile device during the entire session. The user can stop the app by disabling all Kaspersky Endpoint Security for Android components. You can use policies to configure user permissions to manage app components.

On certain devices (for example, HUAWEI, Meizu, and Xiaomi), you must manually add Kaspersky Endpoint Security for Android to the list of apps that are started when the operating system starts (**Security** → **Permissions** → **Autorun**). If the app is not added to the list, Kaspersky Endpoint Security for Android stops performing all of its functions after the mobile device is restarted.

You must also disable Battery Saver mode for Kaspersky Endpoint Security for Android. This is necessary for the app to run in the background, for example, when running a scheduled malware scan or synchronizing the device with Kaspersky Security Center. This issue is due to the specific features of the embedded software of these devices.

Activating Kaspersky Endpoint Security for Android

In Kaspersky Security Center, the license can cover various groups of features. To ensure that the Kaspersky Endpoint Security for Android app is fully functional, the Kaspersky Security Center license purchased by the organization must support the Mobile Device Management functionality.

For detailed information about licensing options, refer to the About the license section.

Activating the Kaspersky Endpoint Security for Android app on a mobile device is performed by providing valid license information to the app. License information is delivered to the device together with the policy settings as soon as the device is synchronized with Kaspersky Security Center.

If activation of the mobile app is not completed within 30 days from the time of installation on the mobile device, the app is automatically switched to limited functionality mode. In this mode, most of the app components are not operational. When switched to limited functionality mode, the app stops performing automatic synchronization with Kaspersky Security Center. Accordingly, if the app is not activated within 30 days after the installation, the user must synchronize the device with Kaspersky Security Center manually.

If Kaspersky Security Center is not deployed in your organization or is not accessible to mobile devices, users can activate the mobile app on their devices manually.

To activate the mobile app:

1. In the main window of Kaspersky Next Expert View (on-premise), select **Asset management** → **Policies**. In the list of group policies that opens, click the name of the policy that you want to configure.
2. In the policy properties window, select **Application settings**.
3. Click the **License** button.
4. In the window that opens, use the drop-down list to select the required license key from the key storage of the Administration Server.

   The details of the license key are displayed in the fields below.

   > You can replace the existing activation key on the mobile device if it is different from the one selected in the drop-down list above. To do so, select the **Replace with selected key if the key on devices is different** check box.

5. Click **Save** to save the changes you have made.

The app is activated after the next device synchronization with Kaspersky Security Center.

Updating Kaspersky Endpoint Security for Android

Kaspersky Endpoint Security for Android can be updated in the following ways:

- Using the Kaspersky website. The mobile device user downloads the new version of the app from the Kaspersky website and installs it on the device.
- Using HUAWEI AppGallery, Samsung Galaxy Store, RuStore, or Xiaomi GetApps. The mobile device user downloads the new version of the app from an app store and installs it on the device following the standard update procedure for the Android platform.

  > To update the app using the Samsung Galaxy Store, the device user must have a Samsung account.

- Using Kaspersky Security Center. You can remotely update the version of the app on the device using Kaspersky Security Center.

You can select the app update method that is most suitable for your organization. You can use only one update method.

Updating the app from the Kaspersky website

To update the app from the Kaspersky website:

1. Go to the Kaspersky website.
2. Find Kaspersky Security for Mobile on the website.

3. Tap **Show Downloads**.

4. Select a version of the app and tap **Download**.

5. Open the downloaded APK file and follow the instructions on the screen.

   Kaspersky Endpoint Security for Android is updated.

After downloading the app, Kaspersky Endpoint Security for Android checks the Terms and Conditions of the End User License Agreement (EULA). If the terms of the EULA have been updated, the app sends a request to the Kaspersky Security Center. If the administrator accepts the EULA in Kaspersky Next Expert View (on-premise), Kaspersky Endpoint Security for Android skips the acceptance step during installation of the app.

Updating the app through Kaspersky Security Center

Kaspersky Endpoint Security for Android can be updated using Kaspersky Security Center after a group policy is applied. In the group policy settings, you can select the standalone installation package of the version of Kaspersky Endpoint Security for Android that meets the corporate security requirements.

You can update through Kaspersky Security Center if Kaspersky Endpoint Security for Android was installed using an installation package in Kaspersky Security Center or using a standalone installation package. If the app was installed from Google Play, you cannot update the app through Kaspersky Security Center.

To update Kaspersky Endpoint Security for Android using a standalone installation package, installation of apps from unknown sources must be allowed on the user's mobile device. For details about installing apps without Google Play, please refer to the Android Help.

To update the version of the app:

1. Add a new Kaspersky Endpoint Security for Android installation package.

2. In the main window of Kaspersky Next Expert View (on-premise), select **Asset management** → **Policies**. In the list of group policies that opens, click the name of the policy that you want to configure.

3. In the policy properties window, select **Application settings**.

4. Select **Android** and go to the **KES for Android settings** section.

5. On the **App update** card, click **Settings**.

   The **App update** window opens.

6. Enable the settings using the **App update** toggle switch.

7. Click **Select**.

   The **Select installation package** window opens.

8. In the list of Kaspersky Endpoint Security for Android standalone installation packages, select the package whose version meets the corporate security requirements.

   Kaspersky Endpoint Security for Android cannot be downgraded to an older version of the application.

9. Click **Select**.

10. Click **OK**.

11. Click **Save** to save the changes you have made.

    Mobile device settings are changed after the next device synchronization with Kaspersky Security Center. The mobile device user is prompted to install the new version of the app. After the user confirms installation, the new app version is installed on the mobile device.

Updates functionality (including providing anti-malware signature updates and codebase updates), as well as KSN functionality may not be available in the software in the U.S.

Removing Kaspersky Endpoint Security for Android

Kaspersky Endpoint Security for Android can be removed in the following ways:

1. App removal by the user

   The user removes Kaspersky Endpoint Security for Android manually using the app interface. In order for users to be able to remove the app, the app removal should be allowed in the **Configure access to app settings** card of the **KES for Android settings** section in the policy settings.

2. App removal by the administrator (corporate devices only)

   The administrator removes the app remotely using the Kaspersky Next Expert View (on-premise). The app can be removed from an individual device or from several devices at once.

Permitting users to remove Kaspersky Endpoint Security for Android

To protect the app from removal on devices running Android 7 or later, Kaspersky Endpoint Security for Android must be set as an Accessibility feature. When the Initial Configuration Wizard is running, Kaspersky Endpoint Security for Android prompts the user to grant the application all required permissions. The user can skip these steps or disable these permissions in the device settings at a later time. If this is the case, the app is not protected from removal.

To allow removal of the app in a group policy:

1. In the main window of Kaspersky Next Expert View (on-premise), select **Asset management** → **Policies**. In the list of group policies that opens, click the name of the policy that you want to configure.

2. In the policy properties window, select **Application settings**.

3. Select **Android** and go to the **KES for Android settings** section.

4. On the **Configure access to app settings** card, click **Settings**.

   The **Configure access to app settings** window opens.

5. Select the **Allow removing the app from device** check box.

6. Click **OK**.

7. Click **Save** to save the changes you have made.

As a result, users will be allowed to remove the app from mobile devices after synchronization with the Administration Server. The app removal button becomes available in the Kaspersky Endpoint Security for Android settings.

To remove the app from a device:

1. In the main window of Kaspersky Endpoint Security for Android, select **Settings** → **App settings** → **Additional** → **Remove app**.

   On corporate devices, Kaspersky Endpoint Security for Android can be removed only by the administrator.

2. Confirm removal of Kaspersky Endpoint Security for Android.

Kaspersky Endpoint Security for Android will be removed from the device.

Removal of Kaspersky Endpoint Security for Android by the user

On corporate devices, Kaspersky Endpoint Security for Android can be removed only by the administrator.

To independently remove Kaspersky Endpoint Security for Android from a mobile device, the user must do the following:

1. In the main window of Kaspersky Endpoint Security for Android, select **Settings** → **App settings** → **Additional** → **Remove app**.

   If the **Remove app** button is missing, this means that the administrator enabled protection against removal of Kaspersky Endpoint Security for Android or the device operates in corporate device mode.

2. Confirm the removal of Kaspersky Endpoint Security for Android.

Kaspersky Endpoint Security for Android will be removed from the device.

We recommend that you remove Kaspersky Endpoint Security for Android only using the app settings, as described in the instructions above. Other uninstallation methods may result in incomplete removal of corporate containers and cause other unpredictable behavior.

Remote removal of Kaspersky Endpoint Security for Android on corporate devices

You can remove the Kaspersky Endpoint Security for Android app from corporate devices remotely by sending a **Reset to factory settings** command.

Executing the **Reset to factory settings** command wipes all data from the device and rolls back device settings to their factory values. This app removal method is recommended by Android Enterprise to guarantee that data is removed from a corporate device.

To remove the app:

1. In the main window of Kaspersky Next Expert View (on-premise), select **Asset management** → **Mobile** → **Devices**.
2. In the list of devices that opens, select a device that you want to send a command to.

   You can select multiple devices.
3. Click **Send command**.
4. In the **Send command** window that opens, in the **Command** field, select the **Reset to factory settings** command.
5. Click **Send**.

   You can view and cancel commands in the **Command history**.

   The command is sent to the devices you selected. Kaspersky Endpoint Security for Android is removed from these devices.
6. In the list of devices, select the device, and then click **Delete**.

   The device is removed from the list of managed devices in Kaspersky Next Expert View (on-premise).

   If the device is not removed from Kaspersky Next Expert View (on-premise), there can be problems with further installation of Kaspersky apps on this device.

Managing mobile devices in Kaspersky Next Expert View (on-premise)

To perform centralized configuration of mobile devices, you must configure policies. A policy is a set of security settings for managing mobile devices of specified operating systems and device operating modes within an administration group and for managing the mobile apps installed on devices.

This section describes how to create administration groups, configure policies for mobile devices, and connect mobile devices to Kaspersky Security Center in order to subsequently manage them.

Creating administration groups

To apply a policy to a group of devices, you are advised to create a separate group for these devices prior to installing mobile management apps.

An *administration group* is a logical set of managed devices combined on the basis of a specific trait for the purpose of managing the grouped devices as a single unit within Kaspersky Security Center.

All managed devices within an administration group are configured to do the following:

- Use the same settings, which you can specify in policies.
- Use a common operating mode for all applications through the creation of group tasks with specified settings. Examples of group tasks include creating and installing a common installation package, updating the application databases and modules, scanning the device on demand, and enabling real-time protection.

A managed device can belong to only one administration group.

You can create hierarchies that have any degree of nesting for Administration Servers and groups. A single hierarchy level can include secondary and virtual Administration Servers, groups, and managed devices. You can also move devices from one group to another.

Immediately after Kaspersky Security Center is installed, the hierarchy of administration groups contains only one administration group called Managed devices. When creating a hierarchy of administration groups, you can add devices to the Managed devices group, and add nested groups.

To create an administration group:

1. In the main window of Kaspersky Next Expert View (on-premise), select **Asset management** > **Hierarchy of groups**.
2. In the administration group structure, select the administration group that the new administration group will belong to.
3. Click **Add**.
4. In the **Name of the new administration group** window that opens, enter a name for the group, and then click **Add**.

A new administration group with the specified name appears in the hierarchy of administration groups.

To automatically create a structure of administration groups:

1. In the main window of Kaspersky Next Expert View (on-premise), select **Asset management** > **Hierarchy of groups**.
2. Click **Import**.

The New administration group structure wizard starts. Follow the instructions of the wizard.

After creating an administration group, we recommend configuring the option to automatically assign devices on which you want to install apps to this group. Then configure the settings that are common to all devices using a specific policy.

Configuring policies

This section describes how to manage policies in Kaspersky Next Expert View (on-premise).

Creating a policy

Kaspersky Next Expert View (on-premise) lets you create policies to configure the security settings of a group of Android, iOS, and Aurora mobile devices. The values of security settings configured in policies are saved on the Administration Server, distributed to mobile devices during synchronization, and saved to devices as current settings.

You can create policies using the Mobile policy wizard.

To create a policy:

1. In the main window of Kaspersky Next Expert View (on-premise), select **Asset management** → **Policies**.
2. In the administration group structure, select the administration group you want to create a policy for.

   By default, the new policy is applied to the **Mobile devices** group.
3. Click **Add** to start the Mobile policy wizard.
4. In the **Select application** window, select the **Kaspersky Mobile Devices Protection and Management** option, and then click **Next**.

   The Mobile policy wizard starts. Click **Start**, and then proceed through the wizard using the **Back** and **Next** buttons.

Step 1. License

At this step, choose a license.

The license you choose determines the security settings that you can configure in a policy. By default, the license that supports the Advanced MDM in Kaspersky Next Expert View (on-premise) functionality is pre-selected. You can choose a different license manually.

After the license is updated in the parent policy, the child policy must be re-saved to apply the changes.

Step 2. Operating systems and device operating modes

At this step, choose the operating systems the policy will apply to and specify the device operating modes.

- **Android**
  - **Personal device** (basic protection and management of a personal Android device).
  - **Device with corporate container** (isolated corporate environment on an Android device).
  - **Corporate device** (an extended set of settings for managing a corporate Android device).
    For detailed information, refer to the About Android device operating modes section.
- **iOS**
  - **Basic protection** (protection against web threats and jailbreak detection on iOS devices).
  - **Basic control** (basic management of a personal iOS device).
  - **Supervised** (an extended set of settings for managing an iOS device).
    For detailed information, refer to the About iOS device operating modes section.

    To connect and manage iOS devices in basic control and supervised operating modes, you must have an iOS MDM Server installed in the selected administration group. For detailed information on installing iOS MDM Server, refer to the Deploying iOS MDM Server section.

    For the basic protection operating mode, you can create a separate administration group without iOS MDM Server and distribute a policy.

    For the basic control or supervised operating modes, you can create administration groups with different iOS MDM Servers and distribute different policies respectively.

    Also, you can combine devices in basic control and supervised operating modes into one administration group and distribute a policy for supervised operating mode. In this case, settings supported by the corresponding operating mode will be applied on devices.
- **Aurora**
  - **Protection** (protection of Aurora devices against threats).

    To connect Aurora devices, you need to have Kaspersky Endpoint Security for Aurora pre-installed on the devices that will connect.

*On the **General** tab of the New policy window:*

1. In the **Name** field, type the name of the new policy. If you specify the name of an existing policy, it will have (1) added at the end automatically.

2. In the **Policy status** block of settings, select the status of the policy:

   - **Active**. The wizard saves the created policy on the Administration Server. At the next synchronization of mobile devices with the Administration Server, the policy will be used on devices as an active policy.

   - **Inactive**. The wizard saves the created policy on the Administration Server as a backup policy. This policy can be activated in the future after a specific event. If necessary, an inactive policy can be switched to an active state.

     Several policies can be created for one application in the group, but only one of them can be active. When a new active policy is created, the previous active policy automatically becomes inactive.

3. In the **Settings inheritance** block of settings, select the inheritance options:

   - **Inherit settings from parent policy**

     If you enable this option in a child policy and an administrator locks some settings in the parent policy, then you cannot change these settings in the child policy.

     If you disable this option in a child policy, then you can change all the settings in the child policy, even if some settings are locked in the parent policy.

   - **Force inheritance of settings in child policies**

     If you enable this option in a parent policy, this enables the **Inherit settings from parent policy** option for each child policy. In this case, you cannot disable this option for any child policy. All the settings that are locked in the parent policy are forcibly inherited in the child groups and you cannot change these settings in the child groups.

   By default, the **Inherit settings from parent policy** option is enabled and the **Force inheritance of settings in child policies** option is disabled.

   For more information about inheritance of policies, refer to the Kaspersky Security Center help.

   Inheritance of policy settings works only if either identical device operating modes are selected for the parent and child policy or device operating modes selected for the child policy provide more security settings. For example, a child policy for Android devices with a corporate container can inherit settings from a parent policy for personal devices but cannot inherit settings from a parent policy for corporate devices.
   If you create a child policy that is incompatible with the parent policy, you must delete it and create a new child policy to manage devices.

4. Click **Save**.

The new policy for mobile devices is created. For more information about configuring policy settings, refer to the Configuration and management section.

Modifying a policy

Kaspersky Next Expert View (on-premise) lets you modify policies.

To modify a policy:

1. Open the policy properties window by doing one of the following:

   - In the main window of Kaspersky Next Expert View (on-premise), select **Asset management** → **Policies**. In the list of policies that opens, click the name of the policy that you want to modify.

   - In the main window of Kaspersky Next Expert View (on-premise), select **Asset management** → **Mobile** → **Devices**. Click the mobile device that falls under the policy that you want to modify, and then select the policy on the **Active policies and policy profiles** tab.

2. In the policy properties window, navigate to the **Application settings** tab, and then define the policy settings.

   You can also configure general settings, settings inheritance, event logging and notifications, and policy profiles, and also view the revision history. For more information, please refer to the Kaspersky Security Center Help.

3. Click **Save** to save the changes you have made to the policy and exit the policy properties window.

The policy is modified. Mobile device settings are configured after the next device synchronization with Kaspersky Security Center.

Copying a policy

Kaspersky Next Expert View (on-premise) lets you create a copy of a policy.

To create a copy of a policy:

1. In the main window of Kaspersky Next Expert View (on-premise), select **Asset management** → **Policies**.

2. In the list of policies that opens, select the check box next to the name of the policy you want to copy, and then click **Copy**.

3. In the tree of administration groups that opens, select the target group where you want the policy to be created.

   You can create a new administration group by selecting an existing group, and then clicking **Add child group**.

4. Click **Copy**.

5. Click **OK** to confirm the operation.

A copy of the policy will be created in the target group under the same name. The status of each copied or moved policy in the target group will be *Inactive*. You can change the status to *Active* at any time.

If a policy with a name identical to that of the newly created or moved policy already exists in the target group, the (<next sequence number>) suffix is added to the name of the newly created or moved policy, for example: (1).

Moving a policy to another administration group

Kaspersky Next Expert View (on-premise) lets you move a policy to another administration group.

To move a policy to another administration group:

1. In the main window of Kaspersky Next Expert View (on-premise), select **Asset management** → **Policies**.
2. In the list of policies that opens, select the check box next to the name of the policy that you want to move to another administration group, and then click **Move**.
3. In the tree of administration groups that opens, select the target group to which you want to move the policy.

   You can create a new administration group by selecting an existing group, and then clicking **Add child group**.
4. Click **Move**.
5. Click **OK** to confirm the operation.

The result depends on the policy inheritance properties:

- If the policy is not inherited in the source group, it will be moved to the target group.
- If the policy is inherited in the source group, it will not be moved. Instead, a copy of the policy will be created in the target group.

The status of each copied or moved policy in the target group will be *Inactive*. You can change the status to *Active* at any time.

If a policy with a name identical to that of the newly created or moved policy already exists in the target group, the (<next sequence number>) suffix is added to the name of the newly created or moved policy, for example: (1).

Viewing the list of policies

Kaspersky Next Expert View (on-premise) lets you view the list of created policies, their statuses, and properties.

To view the list of policies:

1. In the main window of Kaspersky Next Expert View (on-premise), select **Asset management** → **Policies**.
2. The list of policies opens with brief information about the policies. On this page, you can create, modify, copy, move, and delete policies.

Viewing the policy distribution results

Kaspersky Next Expert View (on-premise) lets you view the distribution chart of a policy and the information about all devices that fall under that policy.

To view the results of distributing a policy:

1. In the main window of Kaspersky Next Expert View (on-premise), select **Asset management** → **Policies**.
2. In the list of policies that opens, select the check box next to the name of the policy whose distribution results you want to view, and then click **Distribution**.

The policy distribution results page opens. This page contains the policy summary, a policy distribution chart, and a table with information about all devices that fall under that policy. You can open the policy properties window by clicking the **Configure policy** button.

Managing revisions to policies

Kaspersky Next Expert View (on-premise) lets you view modifications made to a policy over a certain period, as well as save information about these modifications in a file.

To view a policy revision:

1. In the main window of Kaspersky Next Expert View (on-premise), select **Asset management** → **Policies**.
2. In the list of policies that opens, click the policy whose revision you want to view, and then go to the **Revision history** section.
3. In the list of policy revisions, click the number of the revision that you want to view.

> If the size of the revision is more than 10 MB, you will not be able to view it using Kaspersky Next Expert View (on-premise). You will be prompted to save the selected revision to a JSON file.
>
> If the size of the revision does not exceed 10 MB, a report in HTML format with the settings of the selected policy revision is displayed. The report is displayed in a pop-up window, so make sure pop-ups are allowed in your browser.

To save a policy revision to a JSON file, in the list of policy revisions, select the revision that you want to save, and then click **Save to file**.

The revision is saved to a JSON file.

For detailed information on managing revisions to policies, refer to the Kaspersky Security Center Help.

Restricting permissions to configure policies

Kaspersky Security Center administrators can configure the access permissions of Kaspersky Next Expert View (on-premise) users for different functions of the Advanced MDM in Kaspersky Next Expert View (on-premise) solution depending on the job duties of users.

In the Kaspersky Next Expert View (on-premise) interface, you can configure access rights on the **Security** and **User roles** tabs of the Administration Server properties window. The **User roles** tab lets you add standard user roles with a predefined set of rights. The **Security** section lets you configure rights for one user or a group of users or assign roles to one user or a group of users. User rights for each application are configured according to functional scopes.

For each functional area, the administrator can assign the following permissions:

- **Allow editing**. The Kaspersky Next Expert View (on-premise) user is allowed to change the policy settings in the properties window.
- **Block editing**. The Kaspersky Next Expert View (on-premise) user is prohibited from changing the policy settings in the properties window. Policy tabs belonging to the functional scope for which this right has been assigned are not displayed in the interface.

For more details on managing user rights and roles in Kaspersky Next Expert View (on-premise), see the Kaspersky Security Center help.

Configuring role-based access control

Kaspersky Next Expert View (on-premise) provides facilities for role-based access to the features of Advanced MDM in Kaspersky Next Expert View (on-premise).

You can configure access rights to application features for Advanced MDM in Kaspersky Next Expert View (on-premise) in one of the following ways:

- By configuring the rights for each user or group of users individually.
- By creating standard user roles with a predefined set of rights and assigning those roles to users depending on their scope of duties.

Application of user roles is intended to simplify and shorten routine procedures of configuring users' access rights to application features. Access rights within a role are configured in accordance with the standard tasks and the users' scope of duties.

User roles can be assigned names that correspond to their respective purposes. You can create an unlimited number of roles in the application. You can use the predefined user roles with already configured set of rights, or create new roles and configure the required rights yourself.

For detailed information on configuring user access in Kaspersky Security Center, refer to the Kaspersky Security Center Help.

Some of the predefined user roles are not authorized to work with mobile devices. The predefined user roles which are available for the Advanced MDM in Kaspersky Next Expert View (on-premise) features are listed in the table below.

Predefined user roles for Advanced MDM in Kaspersky Next Expert View (on-premise)

Role	Read	Write	License key management: create policies and modify license key settings	Vulnerability and patch management: view unaccepted EULAs and accept EULAs
Kaspersky Endpoint Security Administrator	+	+	-	-
Kaspersky Endpoint Security Operator	+	-	-	-
Main Administrator	+	+	-	-
Main Operator	+	-	-	-
Mobile Device Management Administrator	+	+	+	+
Mobile Device Management Operator	+	-	-	-

For detailed information on predefined user roles, refer to the Kaspersky Security Center Help.

Access rights to Advanced MDM in Kaspersky Next Expert View (on-premise) features

Functional area	Right
Kaspersky Mobile Devices Protection and Management > Kaspersky Next Expert View (on-premise) > App configuration	• **Read:** Get read access to all settings in the corresponding policy section • **Write:** Get write access to all settings in the corresponding policy section Please note, to configure the Web Protection and Web Control settings, the administrator must have the **Read** and **Write** rights for both the **Protection** and **Security controls** functional areas.
Kaspersky Mobile Devices Protection and Management > Kaspersky Next Expert View (on-premise) > Security controls	
Kaspersky Mobile Devices Protection and Management > Kaspersky Next Expert View (on-premise) > Corporate container	
Kaspersky Mobile Devices Protection and Management > Kaspersky Next Expert View (on-premise) > Device configuration	
Kaspersky Mobile Devices Protection and Management > Kaspersky Next Expert View (on-premise) > Configuration of Kaspersky device management apps	
Kaspersky Mobile Devices Protection and Management > Kaspersky Next Expert View (on-premise) > Protection	
Kaspersky Mobile Devices Protection and Management > Kaspersky Next Expert View (on-premise) > Restrictions	
Kaspersky Mobile Devices Protection and Management > Kaspersky Next Expert View (on-premise) > Samsung Knox settings	

Mobile Device Management access rights

Right	User action: right required to perform the action
Mobile Device Management > **General** > **Read**	• View the **Mobile** section in Kaspersky Next Expert View (on-premise)
Mobile Device Management > **General** > **Write**	• Perform any action with certificates (except viewing certificates) The **Manage certificates** right must also be granted. • Configure Firebase Cloud Messaging settings
Mobile Device Management > **General** > **Connect new devices**	• Connect new mobile devices and iOS MDM Servers • Delete devices
Mobile Device Management > **General** > **Manage certificates**	• Perform any action with certificates • Configure certificate issuance rules The **Write** right must also be granted.
Mobile Device Management > **General** > **Send only information commands to mobile devices**	• Send and cancel the **Synchronize device** command
Mobile Device Management > **General** > **Send commands to mobile devices**	• Send and cancel any command
Mobile Device Management > General > Start RDP sessions	• Establish remote connections to devices

Configuring policy profiles

Policy profiles make it easier to manage multiple versions of the same policy within an administration group. You can create a single policy and add profiles that contain only the settings you want to customize, eliminating the need to create several similar policies from scratch.

Each profile is a specific subset of policy settings. The policy provides the main settings for managed devices, while each profile contains only the settings that differ from the main policy settings.

Profiles are distributed to managed devices together with the policy and are applied when their activation conditions are met. When a profile is activated, its settings override the corresponding settings of the main policy. For example, a policy may prevent users from installing apps on managed devices in general, while a profile under that policy allows users to install apps from a specific group of devices or users.

Using policy profiles allows you to manage different device configurations while maintaining a single policy.

You can modify the specific conditions that must affect activation of the policy profile that you are creating. For mobile devices, you can modify the following conditions:

- **Rules for specific device owner**

  Profile activation on the device according to its owner.

  - **Device owner**
  - **Device owner is included in an internal security group**

- **Rules for role assignment**

  Profile activation on the device depending on the owner's role.

  - **Activate policy profile by specific role of device owner**

- **Rules for tag usage**

  Profile activation on the device depending on the tags assigned to the device.

  - **Tag list**
  - **Apply to devices without the specified tags**

- **Rules for Active Directory usage**

  Policy profile activation on the device based on the device allocation in an Active Directory organizational unit or the membership of that device (or the device owner) in an Active Directory security group. The configuration scope depends on the currently used policy.

  - **Device owner's membership in an Active Directory security group**
  - **Device membership in Active Directory security group**
  - **Device allocation in Active Directory organizational unit**

For detailed information on configuring activation rules, creating, deleting, or copying policy profiles, refer to the Kaspersky Security Center Help.

Deleting a policy

Kaspersky Next Expert View (on-premise) lets you delete policies.

You can delete only policies that are not inherited in the current administration group. If a policy is inherited, you can only delete it in the higher-level group for which it was created.

If you delete a parent policy, its child policies will remain and become available for editing.

To delete a policy:

1. In the main window of Kaspersky Next Expert View (on-premise), select **Asset management** → **Policies**.
2. In the list of policies that opens, select the check box next to the name of the policy that you want to delete, and then click **Delete**.
3. In the window that opens, click **OK** to confirm the operation.

The policy is deleted. Before the new policy is applied, mobile devices belonging to the administration group continue to work according to the settings specified in the policy that has been deleted.

Connecting mobile devices to Kaspersky Next Expert View (on-premise)

To manage mobile devices and the mobile management apps installed on them, you must connect these devices to Kaspersky Security Center.

Before connecting, make sure the license that supports the Mobile Management solution is configured in the **License keys** section of the Administration Server properties.

To connect a mobile device to Kaspersky Security Center:

1. In the main window of Kaspersky Next Expert View (on-premise), select **Asset management** → **Mobile** → **Devices**.
2. In the list of mobile devices that opens, click **Add**.

   The Mobile device connection wizard starts. Click **Start**, and then proceed through the wizard using the **Back** and **Next** buttons.

Welcome

On the welcome screen, you can read a summary of the Mobile device connection wizard steps.

Step 1. Policy

At this step, choose a policy for devices that will connect. Devices operate according to the security settings specified in the policy.

- **Use an existing policy**

  For this option, specify the administration group of the policy you want to choose. The policy name, operating systems and operating modes of the devices managed by this policy will be displayed.

  If necessary, click **Go to policy** to view the properties of the policy you have selected.

- **Create a new policy**

  For this option, click the **Create policy** button that appears. You will be redirected to the Mobile policy wizard. After a policy with the required properties is created, you can return to the Mobile device connection wizard.

Step 2. Operating systems

At this step, choose the operating systems of the devices that will connect. The policy settings determine the available operating systems: Android, iOS, or Aurora.

- **Android**

  After you select this operating system, the Kaspersky Endpoint Security for Android **Installation settings** will be displayed. To modify them, click **Edit settings**.

  a. Choose the **Installation source** for Kaspersky Endpoint Security for Android:

  - **Kaspersky website**

    Choose this method for mobile devices that can access the internet to download the APK installation file from the Kaspersky website. The app will then be updated from the Kaspersky website or using HUAWEI AppGallery, Samsung Galaxy Store, RuStore, or Xiaomi GetApps.

    This installation source works for all operating modes.

  - **RuStore**

    The user will receive a link to RuStore. The app can be installed from RuStore by following the standard installation procedure on the Android platform.

    The link contains the following data:

    - Kaspersky Security Center synchronization settings.
    - Details for automatic receiving of the mobile certificate upon the first synchronization.
    - Indication of whether the End User License Agreement for Kaspersky Endpoint Security for Android and additional Statements were accepted. If the administrator accepts the agreements in the Kaspersky Next Expert View (on-premise), Kaspersky Endpoint Security for Android skips the acceptance step during the app installation.

    This installation source works only for personal devices and devices with a corporate container.

- **Installation package**

  The Kaspersky Endpoint Security for Android installation package will be downloaded from the Kaspersky Security Center server and updated via Kaspersky Security Center using policy settings. You can choose this method if mobile devices in your company have no access to the internet.

  For this installation source, before connecting mobile devices, create the Kaspersky Endpoint Security for Android installation package.

  This installation source works for all operating modes.

  - To choose an installation package, click **Select installation package**, and then select the installation package from the list that opens.
  - If there are no available installation packages, you will be offered to create one. Click **Create installation package**, and then follow the steps of the New package wizard as described in the Kaspersky Security Center Help to create an installation package from a file or create a stand-alone installation package. After the installation package is created, you can return to the Mobile device connection wizard.

  > Automatic app updates through the store are not available with this installation method. You can update the app manually in the **App update** section of the policy settings.
  > The latest installation package uploaded to Kaspersky Security Center is used to install the app on devices.

  > For corporate devices, make sure the **Allow using HTTP to download the app** check box is selected to ensure Kaspersky Endpoint Security for Android is downloaded. Otherwise, the app will be downloaded via HTTPS only if the Kaspersky Security Center Web Server certificate was issued by a trusted certificate authority.

  For more information on the installation methods, refer to the Installing Kaspersky Endpoint Security for Android section.

b. Choose **Installation network** for Kaspersky Endpoint Security for Android (corporate devices only):

- **Prompt the user to select a Wi-Fi network on device**

  If you choose this option, the user will be prompted to connect to any available Wi-Fi network for downloading the app.

- **Only use the specified Wi-Fi network** (Android 9 or later)

  To choose an installation network, click **Select network**.

  In the window that opens, specify the following settings:

  - **Service set identifier (SSID)**

    Specifies the name of a wireless network with an access point (SSID). The wireless network name should not be longer than 32 characters.

  - **Hidden network**

    Specifies whether the selected network broadcasts its SSID.

  - **Network protection**

Specifies a wireless network security type. Possible values:

- **NONE**

  If selected, the network is not protected.

- **WPA**

  If selected, the network is protected using the WPA security protocol. This option requires entering a password to access the network.

- **WEP**

  If selected, the network is protected using the WEP protocol. This option requires entering a password to access the network and applies only to devices running Android 9 or earlier.

- **Password**

  Specifies the password for accessing a wireless network protected using a WPA or WEP protocol. The password will be sent to the user in a QR code.

  Do not send a password for a confidential Wi-Fi network that must not be publicly accessible. The password is sent to the user in unencrypted form along with other device configuration data.

- **Use proxy server**

  Specifies the use of a proxy server. If this check box is selected, you need to provide the proxy server address and port. You can also specify a list of addresses for which the proxy will be bypassed.

- **Proxy server address**

  Specifies the IP address or the symbol name (web address) of the proxy server. The maximum number of characters is 256.

- **Proxy server port**

  Specifies the port number of the proxy server. The value should be in the interval between 0 and 65536.

- **PAC file URL**

  A URL to a proxy auto-configuration (PAC) file for the Wi-Fi network.

- **Do not use proxy server for the following addresses**

  Specifies the addresses for which the proxy server should not be used.

  You can enter the address in `example.com` format. If you enter `example.com`, the proxy server will not be used for the addresses `pictures.example.com`, `example.com/movies`, etc. The protocol (for example, `http://`) can be omitted.

Do not use a password for a confidential Wi-Fi network that must not be publicly accessible. The unencrypted password is sent to the user in a QR code along with other device configuration data.

- **Try to use mobile network** (Android 8 or later)

  If you choose this option, the device will try to use mobile data to download the app. If the device does not have a SIM card or the mobile network is not available, the user will be prompted to select any available Wi-Fi network.

c. Click the **Enable all system apps** check box (corporate devices only) if you want system apps to remain active on the device. If necessary, they can be disabled later in the App Control section.

- **iOS**

  To connect and manage iOS devices in basic control and supervised operating modes, you must have an iOS MDM Server installed in the selected administration group. For detailed information on installing iOS MDM Server, refer to the Deploying iOS MDM Server section.

  The *Kaspersky Protection for iOS app* will be installed on personal iOS devices in the basic protection operating mode.

  A *management profile* will be installed on the devices operating in basic control and supervised operating modes.

  On devices running iOS 12.1 or later, you must manually confirm the installation of a management profile on a mobile device. You must also grant the permission for remote management of the device.

- **Aurora**

  To connect Aurora devices, you need to have Kaspersky Endpoint Security for Aurora pre-installed on the devices that will connect.

Step 3. Accept agreements

At this step, choose who must accept the End User License Agreement (EULA) and Privacy Policy.

- **Administrator**

  The agreements are accepted by the administrator in the next step of the wizard. In this case, the app skips the acceptance step during the app installation.

- **Users**

  The agreements are accepted on mobile devices by users.

This step only applies to Android and iOS operating systems. If you are connecting Aurora devices, the agreements are only accepted by users on their mobile devices.

Please note that the administrator will be offered to accept the EULA only after the same version of the EULA is accepted by users on devices for the first time. After the connection and first synchronization of devices with Kaspersky Security Center, the administrator will be able to accept this version of EULA upon subsequent connection of devices.

The list of accepted agreements is available in the **End User License Agreements** section of the Administration Server properties.

Step 4. End User License Agreement and Privacy Policy

At this step, if **Administrator** is selected as the recipient of the agreements in the previous step of the wizard, you will be offered to read the Privacy Policy, EULA, and all the documents associated with it. You must accept the terms and conditions of the EULA and Privacy Policy before installation of the mobile device management apps.

Step 5. Users

At this step, choose one or more users of the devices that will connect. These users will receive the details for installing the app to connect their devices to Kaspersky Security Center. If a user is not in the list, you can add a new user account without exiting the wizard.

- To choose an existing user, select check boxes next to the corresponding user names.
- To add a new user, click **Add user**.

  a. Specify user credentials in the **Credentials** block of settings.

  - **User name**
  - **Password**

    The password must meet the following complexity requirements:

    - It must contain between 8 and 16 characters.
    - It must contain the characters from at least three of these groups: uppercase letters (A-Z), lowercase letters (a-z), digits (0-9), special characters (@ # $ % ^ & * - _ ! + = [ ] { } | : ' , . ? / \ ` ~ " ( ) ;).

  b. If necessary, specify the optional details in the **Optional information** group of settings.

  - **Full user name**
  - **Description**
  - **Email address**
  - **Phone number**

  c. Click **OK** to save the changes.

  The new user will be added and displayed in the list of users.

- To modify user details, click **Edit user**.

  The fields you can modify depend on the user subtype - *internal* or *domain*.

You cannot specify another user as a device owner or remove the assigned user after the device has been connected. However if you have not assigned any user when connecting the device, you can assign the user later by delivering a mobile certificate.

Step 6. Send connection details

At this step, choose how to send the QR codes and links for installing the mobile management apps or management profiles. You can choose one of the following options:

- **Send a message to users' email addresses**

  Choose this option to send the connection details by email to the selected users. To install the app or a management profile, the user needs to scan the QR code using the camera of the mobile device or open the link to the installation package.

  These email addresses must be specified in the user account settings in Kaspersky Security Center.

  If you want to send the connection details to an email address that is not specified in the user account settings in Kaspersky Security Center, select the **Send a copy of the message to an alternate email address** check box, and then specify the required email address.

- **Show the details after completing the wizard**

  Choose this option to scan the QR code with the camera of the mobile device or follow the link in the wizard.

Step 7. Confirm

At this step, check the mobile device connection details specified in the earlier steps, and then click **Finish** to confirm the operation.

If you select a large number of users or user groups, creating QR codes and connection links may take several minutes.

Finish

On the **Finish** screen:

- If you chose the **Send a message to users' email addresses** option, the specified users will receive the emails with QR codes and links for connecting mobile devices to the Administration Server.

- If you chose the **Show the details after completing the wizard** option, the connection details will be available on the **Finish** screen. You can view the displayed details or click **Download list** to receive a file with summarized information. The connection details are shown only once and cannot be accessed again after the **Finish** screen is closed.

Click **Close** to exit the wizard.

As soon as users install the mobile management apps, their devices are connected to the Administration Server and displayed on the **Devices** tab of Kaspersky Next Expert View (on-premise).

You can now configure the settings for devices and mobile management apps using policies. You will also be able to send commands to mobile devices for data protection in case devices are lost or stolen.

Direct connection of Android devices to Kaspersky Security Center

Android devices can connect directly to port 13292 of the Administration Server.

Depending on the method used for authentication, two connection options are possible.

Connecting devices with a user certificate

When connecting a device with a user certificate, the device is associated with the user account to which the corresponding certificate has been assigned through the Administration Server tools.

In this case, two-way SSL authentication (mutual authentication) will be used. Both the Administration Server and the device will be authenticated with certificates.

Connecting devices without a user certificate

When connecting a device without a user certificate, the device is associated with none of the user's accounts on Administration Server. However, when the device receives any certificate, the device will be associated with the user to which the corresponding certificate has been assigned through the Administration Server tools.

When connecting that device to the Administration Server, one-way SSL authentication will be applied, which means that only Administration Server is authenticated with the certificate. After the device retrieves the user certificate, the type of authentication will change to two-way SSL authentication (2-way SSL authentication, mutual authentication).

Moving unassigned mobile devices to administration groups

When the mobile devices are connected to Kaspersky Security Center, they are displayed on the **Asset management → Unassigned devices** page of Kaspersky Next Expert View (on-premise). To manage newly connected devices, you can create a rule that automatically assigns them to administration groups or you can move them to an administration group manually.

To move an unassigned mobile device to an administration group:

1. In the main window of Kaspersky Next Expert View (on-premise), select **Asset management → Unassigned devices**.

2. Select the device that you want to move to an administration group, and then click **Move to group**.

3. In the tree of administration groups that opens, select the target group to which you want to move the device.

   You can create a new administration group by selecting an existing group, and then clicking **Add child group**.

4. Click **Move**.

The device is moved to the specified administration group and the corresponding policy is applied to it.

Actions on mobile devices to connect to Administration Server

Depending on the mode in which your device will operate, you may have to perform additional actions to protect your device and connect it to the Administration Server.

Install a mobile certificate

If you received a certificate password, you must use it to install the mobile certificate on your device.

To install the mobile certificate:

1. Remember or write down the password you received from your administrator by email.
2. Do one of the following:

   - On an Android device, enter the certificate password when prompted by Kaspersky Endpoint Security for Android.
   - On an iOS device, enter the certificate password during installation of the management profile.

The mobile certificate will be installed on your device.

Pre-configure corporate Android devices

To connect a corporate Android device to the Administration Server, you must pre-configure the device depending on the operating system version and availability of a QR code scanner.

Install Kaspersky Endpoint Security for Aurora

The QR code that you received from your administrator contains the settings used to connect your device to the Administration Server. Before you connect the device, you must install Kaspersky Endpoint Security for Aurora. For more information on installing Kaspersky Endpoint Security on Aurora devices, see the Kaspersky Endpoint Security for Aurora Help.

Configuring synchronization settings

To manage mobile devices and receive reports or statistics from mobile devices of users, you must configure the synchronization settings. Synchronization is performed using the HTTPS protocol. Mobile device synchronization with the Administration Server may be performed in the following ways:

- **By schedule**. You can configure the synchronization schedule in the policy settings. Modifications to policy settings, commands and tasks will be performed when the device synchronizes with Kaspersky Security Center according to the schedule, i.e. with a delay.

Due to Doze limitations, when you select a short synchronization period, devices may synchronize with the Administration Server less frequently than expected.

Using short synchronization periods decreases device battery life.

- **Forced**. Synchronization is performed using FCM (Firebase Cloud Messaging) push notifications. Forced synchronization is primarily intended for timely delivery of commands to a mobile device. This may be useful when a mobile device is in battery-saver mode, because in this case the app may perform tasks later than specified. If you want to use forced synchronization, make sure that the FCM settings are configured in Kaspersky Security Center.

  Use the **Synchronize device** command to force synchronization of an Android device or an iOS MDM device.

> The **Force synchronization** button and the **Do not disconnect from the Administration Server** check box in the device properties window are not supported by mobile devices.

To configure synchronization settings for Android devices:

1. In the main window of Kaspersky Next Expert View (on-premise), select **Asset management** → **Policies**. In the list of group policies that opens, click the name of the policy that you want to configure.
2. In the policy properties window, select **Application settings**.
3. Select **Android** and go to the **KES for Android settings** section.
4. On the **Scheduled synchronization** card, click **Settings**.

   The **Scheduled synchronization** window opens.
5. Enable synchronization using the **Scheduled synchronization** toggle switch.
6. In the **Synchronization period** drop-down list, select the period of time between synchronizations of devices with Kaspersky Security Center. The default value is 3 hours.
7. To disable synchronization of devices with Kaspersky Security Center while roaming, select the **Do not synchronize while roaming** check box.

   The device user can manually perform synchronization in the app settings (**Settings** → **App settings** → **Synchronization** → **Synchronize**).
8. Click **OK**.
9. Click **Save** to save the changes you have made.

Mobile device settings are changed after the next device synchronization with Kaspersky Security Center. You can manually synchronize the mobile device using a special command.

To configure synchronization settings for iOS devices operating in basic protection mode:

1. In the main window of Kaspersky Next Expert View (on-premise), select **Asset management** → **Policies**. In the list of group policies that opens, click the name of the policy that you want to configure.
2. In the policy properties window, select **Application settings**.
3. Select **iOS** and go to the **KP for iOS settings** section.

4. On the **Scheduled synchronization** card, click **Settings**.

   The **Scheduled synchronization** window opens.

5. Enable synchronization using the **Scheduled synchronization** toggle switch.

6. In the **Synchronization period** drop-down list, select the period of time between synchronizations of devices with Kaspersky Security Center. The default value is 6 hours.

7. Click **OK**.

8. Click **Save** to save the changes you have made.

Mobile device settings are changed after the next device synchronization with Kaspersky Security Center.

On some iOS devices, the background synchronization may be performed later than expected if the user quit Kaspersky Protection for iOS by swiping up in the App Switcher. To force synchronization, the user must reopen the app. For more information about restrictions and recommendations related to optimizing background task execution, see the Known issues of Kaspersky Protection for iOS section.

For more information about configuring synchronization settings for iOS devices in basic control and supervised operating modes, refer to the Viewing the list of installed iOS MDM Servers and configuring their settings section.

Managing certificates of mobile devices

Kaspersky Next Expert View (on-premise) lets you issue, renew, or delete mobile, mail, or VPN certificates of mobile devices.

This section contains information about how to manage mobile device certificates and configure their issuance rules.

Reissuing the mobile Administration Server certificate

You need to specify a reserve mobile Administration Server certificate to meet the security requirements of your organization and maintain a continuous connection between managed devices and the Administration Server. A mobile certificate issued by Kaspersky Security Center is reissued by default.

We recommend that you specify a reserve certificate when installing the Administration Server or no later than 30 days before the expiration of the existing certificate. The exact expiration time is available in the **Expires** field of the certificate settings (in the main menu, select → **General** → **Certificates**).

The maximum validity period of any Administration Server certificate is 397 days.

The reserve certificate is delivered to the device during synchronization and becomes the main certificate immediately after the existing certificate expires. If the certificate expires and no reserve certificate has been specified, the connection between the Administration Server and Kaspersky Endpoint Security on managed devices will be lost. In this case, to reconnect devices, you must specify a new certificate and reinstall Kaspersky Endpoint Security on each of the managed devices.

To reissue the Administration Server certificate with delayed activation (to use a certificate as a reserve certificate):

1. In the main window of Kaspersky Next Expert View (on-premise), click the Administration Server name.
2. In the Administration Server properties window that opens, select **General** → **Certificates**.
3. If you plan to continue using the certificate issued by Kaspersky Security Center:
    a. Click **Reissue**.
    b. In the window that opens:
        1. In the **Connection address** section, select **Use old connection address** or **Change connection address to**, if a new connection address will be used.
        2. In the **Activate new certificate** section, select **After this period expires, days** and specify the number of days before the certificate becomes active.

            We recommend to specify a certificate activation period of at least 30 days so that all devices have time to receive the certificate. Please note that the specified period must be greater than the period for synchronizing devices with the Administration Server. For more information about configuring settings for device synchronization with the Administration Server, see the Configuring synchronization settings section.

        3. Click **OK**.

    Alternatively, if you plan to use your own custom certificate:

    a. Check whether your certificate meets the requirements of Kaspersky Security Center. If necessary, modify the certificate.
    b. Select the **Other certificate** option and click **Manage certificate**.
    c. In the window that opens, click **Browse**.
    d. In the window that opens, select the type of your certificate and then specify the certificate location and settings:
        - If you select **PKCS #12**, click the **Browse** button next to the **Certificate** field and specify the certificate file on your hard drive. If the certificate file is password-protected, enter the password in the **Password** field.
        - If you select **X.509**, click the **Browse** button next to the **Private key** field and specify the private key on your hard drive. If the private key is password-protected, enter the password in the **Password** field. Then click the **Browse** button next to the **Certificate** field and specify the public key on your hard drive.
    e. In the **Activate new certificate** section, select **After this period expires, days** and specify the number of days before the certificate becomes active.
    f. Click **Save**.

g. Click **OK**.

h. Click **Save** to save the changes you have made.

The certificate is reissued as a reserve certificate.

To immediately reissue the Administration Server certificate (not recommended if you have any managed mobile devices):

Do not select **Immediately** if you have any managed mobile devices. If you select this option, the connection with all managed devices will be lost, since the new certificate will not be delivered to devices, and the previous certificate will no longer be valid.

1. In the main window of Kaspersky Next Expert View (on-premise), click the Administration Server name.
2. In the Administration Server properties window that opens, select **General** → **Certificates**.
3. If you plan to continue using the certificate issued by Kaspersky Security Center:

   a. Click **Reissue**.

   b. In the window that opens:

      1. In the **Connection address** section, select **Use old connection address** or **Change connection address to**, if a new connection address will be used.
      2. In the **Activate new certificate** section, select **Immediately**.
      3. Click **OK**.

   Alternatively, if you plan to use your own custom certificate:

   a. Check whether your certificate meets the requirements of Kaspersky Security Center. If necessary, modify the certificate.

   b. Select the **Other certificate** option and click **Manage certificate**.

   c. In the window that opens, click **Browse**.

   d. In the window that opens, select the type of your certificate and then specify the certificate location and settings:

      - If you select **PKCS #12**, click the **Browse** button next to the **Certificate** field and specify the certificate file on your hard drive. If the certificate file is password-protected, enter the password in the **Password** field.
      - If you select **X.509**, click the **Browse** button next to the **Private key** field and specify the private key on your hard drive. If the private key is password-protected, enter the password in the **Password** field. Then click the **Browse** button next to the **Certificate** field and specify the public key on your hard drive.

   e. In the **Activate new certificate** section, select **Immediately**.

   f. Click **Save**.

g. Click **OK**.

h. Click **Save** to save the changes you have made.

The certificate is reissued as the main Administration Server certificate.

For more information about certificates, please refer to the Kaspersky Security Center Help.

Configuring certificate issuance rules

Kaspersky Next Expert View (on-premise) lets you configure how the certificates for mobile devices are issued, renewed, and protected.

To configure certificate issuance rules:

1. In the main window of Kaspersky Next Expert View (on-premise), select **Asset management** → **Mobile** → **Certificates**.

2. In the list of certificates that opens, click **Issuance rules**.

   - In the **PKI settings** section:

     a. In the **Integration with PKI** block of settings, enable the **Integrate issuance of certificates with Microsoft Certification Authority (CA) via PKI** toggle switch to issue certificates automatically following integration.

     Click **Select device**, and then specify a device with Network Agent installed that will connect to Microsoft CA.

     For detailed information on PKI, refer to the Integration with Public Key Infrastructure section.

     b. In the **Domain account for transmitting requests to issue certificates** block of settings, specify the **PKI account name** (the name of the user account to be used for PKI integration in the `userPrincipalName@DNSDomainName` format) and **Password** (the domain password for the account).

     c. Click **Save** to apply the changes.

   - In the **Mobile certificates** section, you can do the following:

     a. In the **Validity** block of settings, in the **Certificate validity period (days)** field, specify the certificate lifetime in days. The default lifetime of a certificate is 365 days. When this period expires, the mobile device will not be able to connect to the Administration Server.

     b. In the **Renewal** block of settings, in the **Renew certificate before it expires in (days)** field, specify the number of days remaining until the current certificate's expiration when Administration Server should issue a new certificate. For example, if the value of the field is 4, Administration Server issues a new certificate four days before the current certificate expires. The default value is 30.

     Select the **Renew certificate automatically** check box to renew certificates automatically. If this option is disabled, certificates must be renewed manually as they expire. This check box is selected by default.

c. In the **Password protection** block of settings, select the **Prompt for password during certificate installation** check box to prompt the user for a password when the certificate is installed on a mobile device. The password is used only once during the installation of the certificate on the mobile device. The password will be automatically generated by Administration Server and sent to the user by email. You can specify the password length in the **Password length** field.

> Password protection is only available for mobile certificates.

d. Click **Save** to apply the changes.

- In the **Mail certificates** and **VPN certificates** sections, if PKI integration is configured:

a. In the **Renewal** block of settings, in the **Renew certificate before it expires in (days)** field, specify the number of days remaining until the current certificate's expiration when Administration Server should issue a new certificate. For example, if the value of the field is 4, Administration Server issues a new certificate four days before the current certificate expires.

Select the **Renew certificate automatically** check box to renew certificates automatically. If this option is disabled, certificates must be renewed manually as they expire. This check box is selected by default.

b. In the **PKI settings** block of settings, specify the **Certificate template name in PKI** (the certificate template that will be used to issue certificates to domain users).

The Network Agent for Windows service installed on a device which connects to CA is run under the specified user account. This service is responsible for issuing users' domain certificates. The service is run when the list of certificate templates is loaded by clicking the **Refresh list** button or when a certificate is generated.

> When connecting a non-domain user's mobile device (running either Android or iOS) to Kaspersky Security Center, the attempt to issue a certificate may fail.

c. In the **Automatic issuance of mail certificate on device connection** and **Automatic issuance of VPN certificate on device connection** blocks of settings, select the **Issue for devices managed by Kaspersky Endpoint Security for Android** or **Issue for iOS MDM devices** check boxes to enable automatic issuance of a mail or VPN certificate when devices connect to Kaspersky Security Center.

If you selected the **Issue for iOS MDM devices** check box, choose the certificate alias from the drop-down list. The certificate alias is a name that identifies the certificate. You can configure the subsequent use of the selected alias for the certificate issuance in the following policy sections:

- For mail certificates: in the properties of the Email account for iOS MDM devices and in the properties of the Exchange ActiveSync account for iOS MDM devices.
- For VPN certificates: in the properties of the VPN network for iOS MDM devices and in the properties of the Wi-Fi network for iOS MDM devices.

You can also change the alias for individual or multiple mail and VPN certificates by clicking **Modify alias** in the list of certificates (**Asset management** → **Mobile** → **Certificates**).

d. Click **Save** to apply the changes.

The specified settings will be used by Kaspersky Security Center to issue, renew, and protect the certificates of mobile devices.

Issuing mobile device certificates

You can issue mobile, mail, or VPN certificates for mobile devices.

To issue a certificate:

1. In the main window of Kaspersky Next Expert View (on-premise), select **Asset management** → **Mobile** → **Certificates**.
2. In the list of certificates that opens, click **Add**.

   The Certificate issuance wizard starts. Click **Start**, and then proceed through the wizard using the **Back** and **Next** buttons.

Welcome

On the welcome screen, you can read a summary of the Certificate issuance wizard steps.

> Please note that the numbering and set of steps may vary depending on the certificate type, operating system, and the issuance settings defined in the **Issuance rules** section.

Step 1. Certificate type

At this step, choose the certificate to be issued.

- **Mail certificate** (to configure corporate email on devices).
- **VPN certificate** (to configure access to private networks and corporate web resources on devices).
- **Mobile certificate** (to identify mobile devices on the Administration Server).

Step 2. Operating system

At this step, choose the operating system of the devices for which the certificate will be issued.

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

Step 3. Connection method

> This step is displayed only if you selected **Mail certificate** or **VPN certificate** as the certificate type and **Android** as the operating system of the devices for which the certificate will be issued.

At this step, choose the method for connecting devices to Administration Server.

- **Connect using mobile certificate authentication**

  Select this option if you want the mobile certificate to be used for user identification upon connecting to Administration Server.

- **Connect without mobile certificate authentication**

  Select this option if you want to install a certificate on a device using no certificate authentication.

  > If there is a mobile certificate on the device, it will always be used for authentication.

Step 4. Users

At this step, choose one or more users that will receive the details for installing certificates. If a user is not in the list, you can add a new user account without exiting the wizard.

- To choose an existing user, select check boxes next to the corresponding user names.
- To add a new user, click **Add user**.

  a. Specify user credentials in the **Credentials** block of settings.

  - **User name**
  - **Password**

    The password must meet the following complexity requirements:

    - It must contain between 8 and 16 characters.
    - It must contain the characters from at least three of these groups: uppercase letters (A-Z), lowercase letters (a-z), digits (0-9), special characters (@ # $ % ^ & * - _ ! + = [ ] { } | : ' , . ? / \ ` ~ " ( ) ;).

  b. If necessary, specify the optional details in the **Optional information** group of settings.

  - **Full user name**
  - **Description**
  - **Email address**
  - **Phone number**

  c. Click **OK** to save the changes.

  The new user will be added and displayed in the list of users.

- To modify user details, click **Edit user**.

The fields you can modify depend on the user subtype - *internal* or *domain*.

Step 5. Certificate alias and source

At this step, choose the certificate alias and source for importing the certificate.

- **Certificate alias**

  A *certificate alias* is a name that identifies the certificate. You can use the selected alias later to configure policy settings: Email account for iOS MDM devices; Exchange ActiveSync account for iOS MDM devices; VPN network for iOS MDM devices; Wi-Fi network for iOS MDM devices.

  > This option is available only if you selected **Mail certificate** or **VPN certificate** as the certificate type.

- **Integrate issuance with Microsoft CA via PKI**

  For this option, specify one of the available templates imported from Microsoft CA in the **PKI template** field.

  > This option is available only if the integration with PKI is enabled in the Issuance rules.

- **Upload file**

  For this option, specify the **Certificate format**:

  - For the PKCS #12 format, in the **Certificate file** field, click **Select**, and then specify a P12 or PFX file.
  - For the X.509 format, in the **Private key file** field, click **Select**, and then specify a PRK or PEM file.

    In the **Certificate file** field, click **Select**, and then specify a CER, CRT, or CERT file.

    After you specify the files, you can also enter the **Certificate password**.

Step 6. Authentication method

> This step is displayed only if you selected **Mobile certificate** as the certificate type, or if you selected **Mail certificate** or **VPN certificate** for Android devices and specified the **Connect without mobile certificate authentication** option as the connection method.

At this step, choose the user authentication method for receiving the certificate.

- **Domain or internal user credentials**. Users will access the certificate using the domain or internal user credentials. On mobile devices, users will have to specify the login in one of the following formats:
  - `userPrincipalName@DNSDomainName`
  - `sAMAccountName`
  - `sAMADomain\sAMAccountName`
- **Password**. Users will access the certificate using a password sent by email or displayed after completing the wizard.

In the **Certificate use on device** block of settings, click the **Allow using one certificate multiple times on the same device (only for devices with Kaspersky Endpoint Security for Android installed)** check box if you want to allow using one mobile certificate multiple times on the same device.

This option is available only if **Android** is chosen as the operating system of the devices for which the certificate will be issued.

Step 7. Send certificate details

At this step, choose how to send the certificate installation details. You can choose one of the following options:

- **Send a message to users' email addresses**

  Choose this option to send the certificate installation details by email to the selected users. These email addresses must be specified in the user account settings in Kaspersky Security Center.

  If you want to send the certificate installation details to an email address that is not specified in the user account settings in Kaspersky Security Center, select the **Send a copy of the message to an alternate email address** check box, and then specify the required email address.

- **Show the details after completing the wizard**

  Choose this option to display the certificate installation details at the final step of the Certificate issuance wizard.

Step 8. Confirm

At this step, check the certificate issuance details specified in the earlier steps, and then click **Confirm and issue certificate** to confirm the operation.

Finish

On the Finish screen:

- If you chose the **Send a message to users' email addresses** option, the specified users will receive the emails with certificate installation details.

- If you chose the **Show the details after completing the wizard** option, certificate installation details are displayed on the Finish screen. You can view the displayed details or click **Download list** to receive a file with summarized information.

Click **Close** to exit the wizard.

After completing the Certificate issuance wizard, certificates are created and added to the list of user certificates. You can delete or renew certificates, as well as view their properties.

Renewing mobile device certificates

If one of the certificates is about to expire, you can renew it using Kaspersky Next Expert View (on-premise).

By following the steps below, you can renew a mobile certificate or a mail or VPN certificate issued via PKI.

To renew a certificate:

1. In the main window of Kaspersky Next Expert View (on-premise), select **Asset management** → **Mobile** → **Certificates**.
2. In the list of certificates that opens, select the certificate you want to renew, and then click **Renew**.

The status of the certificate changes to **Certificate renewed**.

Deleting mobile device certificates

You can delete the certificates of mobile devices using Kaspersky Next Expert View (on-premise).

Please note that if you delete a mobile certificate, the device can no longer synchronize with Administration Server and cannot be managed by means of Kaspersky Security Center.

When you delete a certificate, it is only removed from Kaspersky Next Expert View (on-premise) and is no longer renewed, but remains on the device. To delete a certificate from iOS MDM devices, corporate devices, or devices with corporate container, you must execute the Wipe corporate data command. On personal Android devices, users should delete the certificate manually.

When you delete a mobile certificate of the iOS MDM device, the device is not removed from Kaspersky Next Expert View (on-premise), but it loses the ability to synchronize with iOS MDM Server and the "Inactive" status is assigned to it. In this case, you have to delete this device from the list of managed devices in Kaspersky Next Expert View (on-premise), and then reconnect it using Mobile device connection wizard.

To delete a certificate from Kaspersky Next Expert View (on-premise):

1. In the main window of Kaspersky Next Expert View (on-premise), select **Asset management** → **Mobile** → **Certificates**.
2. In the list of certificates that opens, select the certificate you want to delete, and then click **Delete**.

The certificate is deleted and removed from the list of certificates.

Integration with Public Key Infrastructure

You can integrate the issuance of certificates with Microsoft Certification Authority (CA) via Public Key Infrastructure (PKI). Integration with PKI is primarily intended for simplifying the issuance of domain user certificates by Administration Server. Following integration, certificates are issued automatically.

You can perform the PKI integration with specified settings and assign PKI to act as the source of certificates for specific types of certificates. The PKI integration settings specified in the **Issuance rules** let you set the individual default template for all types of certificates.

The specifics of using PKI integration to issue certificates:

- The PKI integration is disabled by default. You can enable it using the **Integrate issuance of certificates with Microsoft Certification Authority (CA) via PKI** toggle switch. For detailed information on enabling PKI and configuring its settings, refer to the Configuring certificate issuance rules section.

- The certificate issuance is carried out using Network Agent Windows, which enables the integration between Administration Server and Microsoft CA. Since there can be multiple devices with Network Agent installed, you can specify the device that will connect to Microsoft CA in the **Issuance rules**. This device must have an Enrollment Agent (EA) certificate installed in the certificates repository of the account under which the integration with PKI is performed. The certificate is issued by the administrator of the domain's CA.

- The account under which integration with PKI is performed must be a domain user and have the right to *Log On As Service*.

- Kaspersky Security Center can only work with one PKI (Microsoft CA) integration at a time.

For detailed information on configuring integration with PKI to issue certificates, refer to the Configuring certificate issuance rules section.

Configuring integration with PKI through Network Agent Windows

Linux-based domain workstations do not support native integration with PKI. Therefore, to enable integration between Administration Server and Microsoft CA, you need to configure an intermediate Windows host with Network Agent installed that will address domain requests to the CA.

To configure Microsoft Active Directory and CA for PKI integration:

1. Create a domain account under which the integration with PKI will be performed. This account will be used for transmitting requests to Microsoft CA to issue certificates.

   a. Run secpol.msc.

   b. In the window that opens, click **Local Policies** → **User Rights Assignment** → **Allow log as a service** to provide the *Log on as Service* permission to the domain account.

2. Grant the domain account the permission to work with CA.

   a. On the server side with the CA, open the certsrv.msc CA snap-in.

   b. Choose the CA, and then click **Properties**.

   c. On the **Security** tab, click **Add**, and then specify the previously created domain account.

   d. Provide the **Issue and Manage certificates** permission to the domain account.

   e. Apply the changes.

3. Add the **Enrollment Agent** certificate template to the list of certificates to be issued:

   a. In the CA snap-in, right-click **Certificate Templates** → **New** → **Certificate Template to Issue**.

   b. Select the **Enrollment Agent** template, and then click **OK**.

c. Make sure the domain user has an access to the certificate template:

a. In the certsrv.msc snap-in, click **Certificate Templates** → **Manage**.

b. In the window that opens, click **Properties** → **Security**.

c. In the window that opens, check if the user has a *Read & Enroll* right.

To configure PKI integration using an intermediate Windows host with Network Agent installed:

1. Prepare a server that will act as an intermediary between Kaspersky Security Center Linux and CA.

   It must be a Windows server in the same domain as the CA.

2. Grant the previously created domain account the permission to access an intermediate Windows server.

3. Log in to the server under the domain account to create a permanent user profile and install the Enrollment Agent certificate:

   a. Log in to the Windows host where Network Agent will be deployed.

   b. Run certmgr.msc as an administrator.

   c. Click **Personal** → **All Tasks** → **Request New Certificate...** to launch the Certificate Enrollment wizard.

   Follow the steps of the wizard with the default settings.

   d. At the **Request Certificates** step, select the **Enrollment Agent** certificate type, and then click **Enroll**.

   After the enrollment status is set to "Succeeded", click **Finish**.

   > If errors occur, wait for policies to be applied on the host or check that the user rights in the Permissions for Domain Controllers settings are configured correctly.

4. Provide the *Log on as Service* permission to the domain account on the Windows host.

   a. Run secpol.msc.

   b. In the window that opens, click **Local Policies** → **User Rights Assignment** → **Allow log as a service**.

5. Install Network Agent Windows. For detailed information on the installation, refer to the Kaspersky Security Center Help.

   - Install Network Agent with the default values, except for the Administration Server address. Make sure that port 13000 is open on the host with Kaspersky Security Center installed.
   - Make sure that the connection with the Windows host is established (in Kaspersky Next Expert View (on-premise), click **Asset management** → **Unassigned devices**).
   - Wait for 15 minutes until the first scheduled synchronization of Network Agent with Kaspersky Security Center is established.

Viewing the list of mobile device certificates

Kaspersky Next Expert View (on-premise) lets you view the created mobile device certificates and their properties.

To view the list of all certificates and their properties:

1. In the main window of Kaspersky Next Expert View (on-premise), select **Asset management** → **Mobile** → **Certificates**.

2. In the window that opens, you can view the list of all created certificates and their properties displayed in the table.

To view the properties of an individual certificate:

1. In the main window of Kaspersky Next Expert View (on-premise), select **Asset management** → **Mobile** → **Certificates**.

2. In the list of certificates that opens, select the certificate whose properties you want to view.

3. In the **Certificate details** window, view the certificate properties:

   - **User name**
   - **Status**
   - **Type**
   - **Protocol**
   - **Source**
   - **Expiration date**
   - **Issue date**
   - **Latest status update**
   - **Alias**
   - **Automatic renewal enabled**
   - **Thumbprint**

To view the certificates installed on an iOS MDM device:

1. In the main window of Kaspersky Next Expert View (on-premise), select **Asset management** → **Mobile** → **Devices**.

2. In the list of mobile devices that opens, choose the device whose certificates you want to view.

3. In the device properties window that opens, choose the **Certificates** section.

   The list of certificates installed on the device and their properties are displayed.

   - **Certificate name**
   - **User certificate**
   - **Certificate thumbprint**

Configuration and management

This section is intended for specialists who administer Advanced MDM in Kaspersky Next Expert View (on-premise), as well as for specialists who provide technical support to organizations that use Advanced MDM in Kaspersky Next Expert View (on-premise).

Control

This section contains information about how to remotely monitor mobile devices in the Kaspersky Next Expert View (on-premise).

Configuring restrictions

This section provides instructions on how to configure user access to the features of mobile devices.

Configuring restrictions for personal Android devices

These settings apply to personal devices and devices with a corporate container.

To keep an Android device secure, Kaspersky Mobile Devices Protection and Management lets you configure user access to the following features of mobile devices:

- Wi-Fi
- Camera
- Bluetooth

By default, the user can use Wi-Fi, camera, and Bluetooth on the device without restrictions.

To configure the Wi-Fi, camera, and Bluetooth usage restrictions on the device:

1. In the main window of Kaspersky Next Expert View (on-premise), select **Asset management** → **Policies**. In the list of group policies that opens, click the name of the policy that you want to configure.
2. In the policy properties window, select **Application settings**.
3. Select **Android** and go to the **Restrictions** section.
4. On the **Device feature restrictions** card, click **Settings**.

   The **Device feature restrictions** window opens.
5. Enable the settings using the **Device feature restrictions** toggle switch.

6. Configure usage of Wi-Fi, camera, and Bluetooth:

   - To disable the Wi-Fi module on the user's mobile device, select the **Prohibit use of Wi-Fi** check box.

     On personal devices and devices with a corporate container running Android 10 or later, prohibiting the use of Wi-Fi networks is not supported.

   - To disable the camera on the user's mobile device, select the **Prohibit use of camera** check box.

     When camera usage is prohibited, the app displays a notification upon opening and then closes shortly after. On Asus and OnePlus devices, the notification is shown in full screen. The device user can tap the **Close** button to exit the app.

     On devices running Android 11 or later, Kaspersky Endpoint Security for Android must be set as an Accessibility feature. Kaspersky Endpoint Security for Android prompts the user to set the app as an Accessibility feature through the Initial Configuration Wizard. The user can skip this step or later disable this service in the device settings. If this is the case, you will not be able to restrict use of the camera.

   - To disable Bluetooth on the user's mobile device, select the **Prohibit use of Bluetooth** check box.

     On Android 12 or later, the use of Bluetooth can be disabled only if the device user granted the **Nearby devices** permission. The user can grant this permission during the Initial Configuration Wizard or later.

     On personal devices running Android 13 or later, the use of Bluetooth cannot be disabled.

7. Click **OK**.

8. Click **Save** to save the changes you have made.

Mobile device settings are changed after the next device synchronization with Kaspersky Security Center.

You can also restrict additional operating system features on corporate devices.

Configuring iOS MDM device restrictions

To ensure compliance with corporate security requirements, configure restrictions on the operation of iOS MDM devices.

Features that are allowed in the **Restrictions** section of the policy but prohibited in configuration profiles installed on devices are unavailable on devices.

Configuring feature restrictions

To configure iOS MDM device feature restrictions:

1. In the main window of Kaspersky Next Expert View (on-premise), select **Asset management** → **Policies**. In the list of group policies that opens, click the name of the policy that you want to configure.
2. In the policy properties window, select **Application settings**.
3. Select **iOS** and go to the **Restrictions** section.
4. On the **Device feature restrictions** card, click **Settings**.

   The **Device feature restrictions** window opens.
5. Enable the settings using the **Device feature restrictions** toggle switch.
6. Enable iOS MDM device feature restrictions using toggle switches on corresponding tabs and select the required restrictions.

   List of device feature restrictions

   - Restrictions on the **General** tab:
     - In the **Device settings** section:
       - **Prohibit voice dial on a locked device**

         Use of the voice dialing function on a locked mobile device.

         If the check box is cleared, the user can use voice commands to dial phone numbers on a locked mobile device.

         If the check box is selected, the user cannot use voice commands to dial phone numbers on a locked mobile device.

         This check box is cleared by default.

       - **Limit ad tracking**

         Use of IFA (Identifier for advertisers) technology for keeping track of websites visited and apps launched on the iOS MDM device. IFA makes it possible to configure ad tracking on the mobile device according to the user's interests.

         If the check box is selected, IFA technology is disabled on the user's mobile device.

         If the check box is cleared, IFA technology is enabled on the mobile device and keeps track of visited websites and started apps in order to show targeted ads.

         This check box is cleared by default.

       - **Prohibit Handoff**

         Use of the Handoff function on the user's mobile device. Handoff enables you to start working with data on one Apple device and then switch to another Apple device and continue working with that data.

         If the check box is cleared, Handoff is available to the user.

         If the check box is selected, Handoff is not available.

         This check box is cleared by default.

       - **Prohibit editing device name**

Ability to modify the name of the mobile device.

If the check box is cleared, the user can edit the mobile device name.

If the check box is selected, the device name cannot be edited.

This check box is cleared by default.

- **Prohibit modifying restrictions**

  Ability to configure the settings for restrictions on the mobile device. Restrictions may be utilized by the user to perform parental control functions on the mobile device. The user can restrict device functions (for example, block use of the camera), access to media content (for example, set age restrictions on viewing films), use of apps (for example, block the use of iTunes Store), and configure other restrictions.

  If the check box is cleared, the user can configure the settings for restrictions on the mobile device.

  If the check box is selected, restrictions cannot be configured on the mobile device.

  This check box is cleared by default.

- **Prohibit Spotlight suggestions**

  Use of Spotlight internet search results in Siri Suggestions. When using Spotlight suggestions, search queries and their associated user data are sent to Apple.

  If the check box is cleared, the user can allow displaying Spotlight internet search results in Siri Suggestions.

  If the check box is selected, Spotlight internet search results are not available in Siri Suggestions. User data is not sent to Apple.

  > The user may be able to enable Spotlight internet search results in Siri Suggestions even if the check box is selected. This is due to an issue known to Apple.

  This check box is cleared by default.

- In the **Data loss protection** section:

  - **Prohibit screenshots and screen recording**

    Ability to take a screenshot or video from the screen of the iOS MDM device.

    If the check box is cleared, the user can take and save screenshots and videos from the screen of the mobile device.

    If the check box is selected, the user cannot take and save screenshots and videos from the screen of the mobile device.

    This check box is cleared by default.

  - **Prohibit non-managed apps from using documents from managed apps**

    Ability to use non-managed (personal) apps on the iOS MDM device to open documents created using managed (corporate) apps and accounts. Non-managed apps are apps installed, configured, and managed by the mobile device user.

    If the check box is cleared, the user can use non-managed apps to open documents created in managed corporate apps.

    If the check box is selected, the user is not allowed to use non-managed apps to open documents created using managed apps. For example, this setting prevents a confidential email attachment from a managed email account from being opened in the user's personal apps.

This check box is cleared by default.

- **Prohibit managed apps from using documents from non-managed apps**

  Ability to use managed (corporate) apps on the iOS MDM device to open documents created using non-managed (personal) apps and accounts of the user. Non-managed apps are apps installed, configured, and managed by the mobile device user.

  If the check box is cleared, the user can use managed apps to open documents created using non-managed apps.

  If the check box is selected, the user is not allowed to use managed apps to open documents created using non-managed apps. For example, this setting prevents a document from a personal iCloud account from being opened in a corporate app.

  This check box is cleared by default.

- **Restrict copy and paste between managed and non-managed apps**

  Restricts copy and paste functionality when at least one of the following check boxes is selected:

  - **Prohibit non-managed apps from using documents from managed apps**
  - **Prohibit managed apps from using documents from non-managed apps**

  If the check box is selected, the device user cannot use clipboard.

  If the check box is cleared, the device user can use clipboard.

  This check box is cleared by default.

  When this check box is selected, various combinations of the **Prohibit non-managed apps from using documents from managed apps** and the **Prohibit managed apps from using documents from non-managed apps** restrictions have different effects in terms of the user's ability to use clipboard.

Prohibit non-managed apps from using documents from managed apps	Prohibit managed apps from using documents from non-managed apps	Feature restriction
Enabled	Enabled	The user cannot copy and paste data.
Enabled	Disabled	The user can copy data from managed apps and paste data to non-managed apps. The user cannot copy data from non-managed apps and paste data to managed apps.
Disabled	Enabled	The user can copy data from non-managed apps and paste data to managed apps. The user cannot copy data from managed apps and paste data to non-managed apps.
Disabled	Disabled	The user can copy data from managed apps and paste data to non-managed apps. The user can copy data from non-managed apps and paste data to managed apps.

- **Disable encryption of backup copies**

  Encryption of backup copies of iOS MDM device data in the iTunes app on the user's computer.

  If the check box is cleared, when a backup copy of mobile device data is created in the iTunes app, data is encrypted automatically and protected with a password. In this case, the user cannot encrypt backup copies of device data in the iTunes app.

  If the check box is selected, the user can choose whether to encrypt backup copies of data in the iTunes app.

  This check box is cleared by default.

- **Prohibit reset to factory settings**

Ability to wipe all data from the device and reset the device to its factory settings.

If the check box is cleared, the user can wipe all data from the device and reset it to factory settings.

If the check box is selected, full reset to factory settings is not available.

This check box is cleared by default.

- **Prohibit modifying account settings**

  Option that lets the user add new accounts (such as email accounts) and edit account settings on the iOS MDM device.

  If the check box is cleared, the mobile device user can add new accounts and edit the settings of existing accounts.

  If the check box is selected, the mobile device user is not allowed to add new accounts and edit the settings of existing accounts.

  This check box is cleared by default.

- In the **Security and privacy** section:

  - **Prohibit sending diagnostic and personal data to Apple**

    Automatic receiving of diagnostic data and information on iOS MDM device usage and transmission of a report with this data to Apple for analysis.

    If the check box is cleared, after being shown a warning the user may allow transmission of reports with diagnostic data and information on mobile device usage to Apple.

    If the check box is selected, transmission of reports with diagnostic data and information on mobile device usage to Apple is blocked.

    This check box is cleared by default.

  - **Prohibit changing password**

    Ability to set, change, or delete the mobile device unlock password.

    If the check box is cleared, the user can set, change, or delete the password used for unlocking the mobile device.

    If the check box is selected, management of the device unlock password is not available.

    This check box is cleared by default.

  - **Prohibit modifying Touch ID and Face ID settings**

    Ability to add and remove Touch ID fingerprints or Face ID data.

    If the check box is cleared, the user can add and remove Touch ID fingerprints or Face ID data.

    If the check box is selected, management of Touch ID fingerprint or Face ID data is not available.

    This check box is cleared by default.

  - **Prohibit device unlock using Touch ID and Face ID**

    Touch ID and Face ID make it possible to use a fingerprint or facial recognition as a password for unlocking the iOS MDM device. Touch ID and Face ID can also be used for authentication of purchases by means of Apple Pay, iTunes Store, App Store, and Book Store, and to sign in to apps.

    If the check box is cleared, the user can use a fingerprint or facial recognition instead of entering a password to unlock the mobile device.

    If the check box is selected, the user cannot use Touch ID or Face ID for unlocking the mobile device.

    This check box is cleared by default.

- **Prompt for password for each purchase on iTunes Store**

  Use of the restriction password for purchasing media content in iTunes Store.

  If the check box is selected, prior to making the first purchase via iTunes Store the user has to specify a restriction password in the purchase restriction settings and subsequently use it for preventing accidental or unauthorized purchases. After the account has been verified when the user is making purchases, the restriction password does not have to be re-entered for 15 minutes.

  If the check box is cleared, the user is not required to enter the restriction password before making purchases in iTunes Store.

  This check box is cleared by default.

- **Prompt for password on first connection via AirPlay**

  Use of a password upon connection of the iOS MDM device to devices compatible with AirPlay. The password is used for safe transmission of media content.

  If the check box is selected, before the first connection of the mobile device to devices compatible with AirPlay, the user must specify a password in the AirPlay security settings and subsequently enter it.

  If the check box is cleared, the user can decide whether to use a password when connecting the mobile device to devices compatible with AirPlay.

  This check box is cleared by default.

- **Prohibit installing configuration profiles**

  Use of additional configuration profiles on the iOS MDM device.

  If the check box is cleared, the user can install additional configuration profiles on the mobile device.

  If the check box is selected, the user cannot install additional configuration profiles on the mobile device.

  This check box is cleared by default.

- **Prohibit non-Configurator hosts**

  Protection of the iOS MDM device against third-party connections. A third-party connection is a connection to other devices or synchronization with Apple services, such as iTunes.

  If the check box is cleared, the user can synchronize the iOS MDM device with other devices and Apple services.

  If the check box is selected, non-Configurator hosts on the user's mobile device are blocked.

  This check box is cleared by default.

- **Prohibit modifying settings for sending diagnostic data**

  Automatic receiving of diagnostic data and information on iOS MDM device usage and transmission of a report with this data to Apple for analysis.

  If the check box is cleared, the user can configure the submission of reports containing diagnostic information and mobile device usage data to Apple.

  If the check box is selected, the settings for submission of reports containing diagnostic information are not available.

  This check box is cleared by default.

- In the **iCloud** section:

  - **Prohibit backup in iCloud**

Automatic backup of data from the iOS MDM device to iCloud. Copies of data already stored in iCloud are not created during the backup process. Copies of media content that was received by synchronizing the device with a computer and not purchased from iTunes Store are not created either.

If the check box is cleared, the user can save backup copies of mobile device data in iCloud. Backup copies of data are saved in iCloud on a daily basis when the device is enabled, locked, and connected to a power source.

If the check box is selected, the user cannot save backup copies of mobile device data in iCloud.

This check box is cleared by default.

- **Prohibit storing documents and data in iCloud**

  Automatic backup of documents in iCloud. iCloud documents can be opened and edited on other devices on which the iCloud service is configured.

  If the check box is cleared, the user can save documents in iCloud, open and edit them on other devices in applications that support iCloud (such as TextEdit).

  If the check box is selected, the user is not allowed to save documents in iCloud.

  This check box is cleared by default.

- **Prohibit iCloud Keychain**

  Automatic synchronization of the account credentials of an iOS MDM device user with the user's other Apple devices. The synchronized data is stored in iCloud Keychain. Data in iCloud Keychain is encrypted. iCloud Keychain makes it possible to save the following data in iCloud:

  - Website accounts
  - Bank card numbers and expiration dates
  - Wireless network passwords

  If the check box is cleared, the user can synchronize data of accounts with the user's other Apple devices.

  If the check box is selected, the user is not allowed to use iCloud Keychain on the mobile device.

  This check box is cleared by default.

- **Prohibit managed apps from storing data in iCloud**

  Creation of a backup copy of the data of managed apps in iCloud.

  If the check box is cleared, the user can store the data of managed apps in iCloud.

  If the check box is selected, the user cannot store corporate data in iCloud.

  This check box is cleared by default.

- **Prohibit backup of enterprise books**

  Backup of enterprise books using iCloud or iTunes. You can provide access to enterprise books by placing them on the corporate web server.

  If the check box is cleared, backup of enterprise books using iCloud or iTunes is available to the user.

  If the check box is selected, backup of enterprise books is not available.

  This check box is cleared by default.

- **Prohibit synchronizing notes and highlights in enterprise books**

  Ability to synchronize notes, bookmarks, and highlighted text in enterprise books using iCloud.

If the check box is cleared, the user can synchronize notes, bookmarks, and highlights in enterprise books. Changes will be available on all the user's Apple devices using iCloud.

If the check box is selected, notes, bookmarks and highlighted text will be available only on this mobile device.

This check box is cleared by default.

- **Prohibit iCloud photo sharing**

  Use of iCloud photo sharing on the iOS MDM device to grant other users access to photos and videos on the iCloud server. The other users need to have the iCloud photo sharing feature configured.

  If the check box is cleared, the iCloud photo sharing feature is available to the user. Users of other devices can view the user's photos and videos, leave comments, and add their own photos and videos. The user can also access the data of other users on the iCloud server.

  If the check box is selected, the iCloud photo sharing feature is not available to the user. The user cannot grant other users access to the user's photos and videos on the iCloud server or access the data of other users on the iCloud server.

  This check box is cleared by default.

- **Prohibit iCloud Media Library**

  Use of the iCloud Media Library function for automatic uploading of photos and videos from the iOS MDM device to the user's other Apple devices.

  If the check box is cleared, the iCloud Media Library function is available to the user when working with the Photos app.

  If the check box is selected, the iCloud Media Library function is not available to the user. The user's photos and videos saved in the iCloud Media Library are removed from the iCloud server.

  This check box is cleared by default.

- In the **Certificates** section:

  - **Prohibit users from accepting untrusted TLS certificates**

    Use of untrusted TLS certificates for providing an encrypted communication channel between apps on the iOS MDM device (Mail, Contacts, Calendar, Safari) and corporate resources.

    If the check box is cleared, the user may allow the use of an untrusted TLS certificate after being shown a warning.

    If the check box is selected, the use of untrusted TLS certificates is blocked.

    This check box is cleared by default.

  - **Prohibit automatic updates of trusted certificates**

    Automatic updates of trusted certificates on the iOS MDM device.

    If the check box is cleared, changes made to the trust settings of a certificate are applied automatically.

    If the check box is selected, changes to trust settings of a certificate are not applied automatically. After being shown a warning, the user may choose to apply changes to trust settings of the certificate.

    This check box is cleared by default.

- Restrictions on the **Apps** tab:

  - In the **General** section:

- **Prohibit use of camera**

  Use of the camera on the user's mobile device.

  If the check box is cleared, the user is allowed to use the device camera.

  If the check box is selected, use of the device camera is disabled. The user cannot take photos, record videos, or use the FaceTime app. The camera icon on the device home screen is hidden.

  This check box is cleared by default.

- **Prohibit FaceTime**

  Use of the FaceTime app on the user's mobile device. This check box is available if the use of the device camera is allowed. This setting is available if the **Prohibit use of camera** check box is cleared.

  If the check box is cleared, the user can make and receive calls using FaceTime.

  If the check box is selected, the FaceTime app is disabled on the user device. The user cannot make or receive video calls.

  This check box is cleared by default.

- **Prohibit iMessage**

  Use of the iMessage service on the user's mobile device.

  If the check box is cleared, the user can send and receive messages using iMessage.

  If the check box is selected, iMessage is not available on the mobile device. The user cannot send or receive messages via iMessage.

  This check box is cleared by default.

- **Prohibit Book Store**

  Access to Book Store from the Apple Books app on the user's mobile device.

  If the check box is cleared, the user can visit Book Store from the Apple Books app installed on the device.

  If the check box is selected, the user cannot visit Book Store from the Apple Books app.

  This check box is cleared by default.

- **Prohibit installation of apps from Apple Configurator and iTunes**

  The user can independently install apps on an iOS MDM device.

  If the check box is cleared, the user can independently install or update apps on a mobile device from App Store using iTunes or Apple Configurator.

  If the check box is selected, the user cannot install or update apps from App Store using iTunes or Apple Configurator on a mobile device. Installation and updates are available only for corporate apps. The App Store icon is hidden on the home screen of the iOS MDM device.

  This check box is cleared by default.

- **Prohibit installation of apps from the App Store**

  Ability to independently install apps on a mobile device from the App Store. The check box is available if the **Prohibit installation of apps from Apple Configurator and iTunes** check box is cleared.

  If the check box is cleared, the user can independently install or update apps from the App Store.

If the check box is selected, the user cannot install or update apps from the App Store on the mobile device. The App Store icon is hidden on the home screen of the iOS MDM device.

This check box is cleared by default.

- **Prohibit automatic app downloads**

  Use of automatic app downloads on the user's mobile device. The check box is available if the **Prohibit installation of apps from Apple Configurator and iTunes** check box is cleared.

  If the check box is cleared, automatic app downloads are available to the user. After this function is enabled, the apps that the user downloaded from the App Store are automatically downloaded to the user's other Apple devices.

  If the check box is selected, automatic app downloads are disabled and unavailable.

  This check box is cleared by default.

- **Prohibit in-app purchases**

  Use of the in-app purchase system on the mobile device.

  If the check box is cleared, the user can make purchases in apps installed on the mobile device.

  If the check box is selected, the user cannot make purchases in apps installed on the mobile device.

  This check box is cleared by default.

- **Prohibit trusting new enterprise developers**

  Ability to configure trusting of corporate apps on a mobile device. You can develop corporate apps and distribute them among employees for internal use. To work with a corporate app, the mobile device user must make it a trusted app.

  If the check box is cleared, the user can configure trusting of corporate apps.

  If the check box is selected, the user cannot set the trust level for corporate apps when installing an app manually.

  This check box is cleared by default.

- **Prohibit removing apps**

  This option allows removing apps from the mobile device.

  If the check box is cleared, the user can remove apps installed via the App Store or iTunes from the device.

  If the check box is selected, the user cannot remove apps installed via the App Store or iTunes from the mobile device.

  This check box is cleared by default.

- In the **AirPrint** section:

  - **Prohibit AirPrint**

    Selecting or clearing this check box specifies whether the device user can use AirPrint.

    The check box is cleared by default.

  - **Prohibit storing AirPrint credentials**

    Selecting or clearing this check box specifies whether the device user can store a keychain of user name and password for AirPrint.

    The restriction is supported on devices with iOS 11 and later.

The check box is cleared by default.

- **Prohibit iBeacon discovery of AirPrint printers**

  Selecting or clearing this check box specifies whether iBeacon discovery of AirPrint printers is enabled. Disabling iBeacon discovery of AirPrint printers prevents spurious AirPrint Bluetooth beacons from getting information about network traffic.

  The restriction is supported on devices with iOS 11 and later.

  The check box is cleared by default.

- **Force AirPrint to use a trusted TLS certificate**

  Selecting or clearing this check box specifies whether a trusted certificate is required for TLS printing communication.

  The restriction is supported on devices with iOS 11 and later.

  The check box is cleared by default.

- In the **AirDrop** section:

  - **Prohibit AirDrop**

    Use of the AirDrop feature for transmitting user data from the iOS MDM device to other Apple devices.

    If the check box is cleared, the user can use AirDrop to transmit data to other Apple devices.

    If the check box is selected, the user cannot transmit data to other Apple devices using AirDrop.

    This check box is cleared by default.

  - **Treat AirDrop as a managed app**

    Use of AirDrop as a managed app for transferring data from the mobile device to other Apple devices. This restriction requires that you select the **Prohibit non-managed apps from using documents from managed apps** check box. Non-managed apps are apps installed, configured, and managed by the mobile device user.

    If the check box is cleared, AirDrop is treated as a non-managed app.

    If the check box is selected, AirDrop is treated as a managed app.

    This check box is cleared by default.

- In the **Apple Music** section:

  - **Prohibit Apple Music**

    Listening to music on the user's mobile device using the Apple Music service.

    If the check box is cleared, the user can listen to music on the mobile device in the Music app.

    If the check box is selected, the Apple Music service is not available to the user.

    This check box is cleared by default.

  - **Prohibit Radio in Apple Music**

    Listening to the radio using the Apple Music service on the user's mobile device.

    If the check box is cleared, the user can listen to the radio in the Music app on the mobile device.

    If the check box is selected, the user cannot listen to the radio.

    This check box is cleared by default.

- In the **Apple Watch** section:
  - **Disable Apple Watch wrist detection**

    Automatic locking of Apple Watch when the user removes the watch from their hand.

    If the check box is cleared, Apple Watch is locked when the user removes a watch from their hand. To unlock it, the user must enter a password on the mobile device.

    If the check box is selected, Apple Watch cannot be locked after a watch is removed.

    This check box is cleared by default.

  - **Prohibit pairing with Apple Watch**

    Pairing of Apple Watch with a supervised mobile device.

    If the check box is cleared, the user of the supervised mobile device can pair it with Apple Watch.

    If the check box is selected, pairing with Apple Watch is not available.

    This check box is cleared by default.

- In the **Siri** section:
  - **Prohibit Siri**

    > Deprecated in iOS 26.4 and later.

    Usage of the Siri app on the user's mobile device.

    If the check box is cleared, the user can use Siri voice commands on the mobile device.

    If the check box is selected, the user cannot use Siri voice commands on the mobile device.

    This check box is cleared by default.

  - **Prohibit when device is locked**

    > Deprecated in iOS 26.4 and later.

    Use of Siri voice commands when the user's mobile device is locked. The user's mobile device has to be password-protected.

    If the check box is cleared, the user can use Siri voice commands on a locked mobile device.

    If the check box is selected, the user cannot use Siri voice commands on a locked device.

    This check box is cleared by default.

  - **Prohibit use of profanity filter**

    > Deprecated in iOS 26.4 and later.

    This option disables the filtering of profanity while using the Siri app on the mobile device.

    If the check box is cleared, profanity is filtered while the user uses the Siri app.

    If the check box is selected, profanity is not filtered while the user uses the Siri app.

    This check box is cleared by default.

- **Prohibit Siri from using internet search**

  > Deprecated in iOS 26.4 and later.

  This option prohibits Siri from using internet search for voice commands on the iOS MDM device.

  If the check box is cleared, Siri can search the internet for answers to the user's questions.

  If the check box is selected, Siri cannot search the internet for information.

  This check box is cleared by default.

- In the **Find My** section:

  - **Prohibit locating devices in Find My**

    Selecting or clearing this check box specifies whether the device user can find devices in the Find My app.

    The restriction is supported on devices with iOS 13 and later.

    The check box is cleared by default.

  - **Prohibit locating friends in Find My**

    Selecting or clearing this check box specifies whether the device user can find friends in the Find My app.

    The restriction is supported on devices with iOS 13 and later.

    The check box is cleared by default.

- In the **Classroom** section:

  - **Prohibit screen viewing via Classroom**

    Ability for an instructor to view students' iPad screens using the Classroom application.

    If the check box is cleared, the instructor can view students' iPad screens in the Classroom application.

    If the check box is selected, the instructor cannot view students' iPad screens in the Classroom application.

    This check box is cleared by default.

- Restrictions on the **Storage** tab:

  - In the **General** section:

    - **Prohibit access to USB devices in Files**

      If the check box is cleared, the user can access connected USB devices in the Files app.

      If the check box is selected, access to connected USB devices in the Files app is blocked.

      The setting is available for mobile devices running iOS 13.1 or later.

      This check box is cleared by default.

    - **Disable access to USB devices when the device is locked**

      Specifies whether USB Restricted Mode is enabled when the device is locked.

If the check box is selected, then when the device is locked, connections to USB drives are limited by USB Restricted Mode.

If the check box is cleared, the device is allowed to connect to USB drives when locked.

The setting is available for mobile devices running iOS 11.4.1 or later.

This check box is cleared by default.

- Restrictions on the **Network** tab:
  - In the **General** section:
    - **Prohibit use of NFC**

      If the check box is cleared, the use of NFC is allowed.

      If the check box is selected, the use of NFC is disabled.

      The setting is available for mobile devices running iOS version 14.2 or later.

      This check box is cleared by default.

    - **Prohibit creating VPN configurations**

      If the check box is cleared, the user can create a VPN configuration on the managed device.

      If the check box is selected, the user can't create a VPN configuration on the managed device.

      The setting is available for mobile devices running iOS version 11 or later.

      This check box is cleared by default.

    - **Prohibit modifying eSIM settings**

      Selecting or clearing this check box specifies whether the device user can change settings related to the carrier plan.

      The restriction is supported on devices with iOS 11 and later.

      The check box is cleared by default.

  - In the **Wi-Fi** section:
    - **Force Wi-Fi on**

      Specifies whether Wi-Fi on the managed device should be always on. The device can connect to any Wi-Fi network.

      If the check box is selected, Wi-Fi on the device is always on, even in flight mode. The user cannot disable Wi-Fi in the device settings.

      If the check box is cleared, the user can disable Wi-Fi in the device settings.

      The setting is available for mobile devices running iOS version 13 or later.

      This check box is cleared by default.

    - **Force connection to allowed Wi-Fi networks only**

      Specifies whether the device can connect to allowed Wi-Fi networks only. This option is available if you add at least one Wi-Fi network to the list of Wi-Fi networks in the Wi-Fi section.

      If the check box is selected, the device connects to allowed Wi-Fi networks only. The user cannot disable Wi-Fi in the device settings.

      If the check box is cleared, the user can connect to any Wi-Fi network.

      The setting is available for mobile devices running iOS version 14.5 or later.

This check box is cleared by default.

- **Prohibit modifying Personal Hotspot settings**

  If the check box is cleared, the device user can modify Personal Hotspot settings.

  If the check box is selected, the device user cannot modify Personal Hotspot settings.

  The setting is available for mobile devices running iOS 12.2 or later.

  This check box is cleared by default.

- In the **Bluetooth** section:

  - **Prohibit modifying Bluetooth settings**

    If the check box is cleared, the user can modify Bluetooth settings on the mobile device.

    If the check box is selected, Bluetooth settings cannot be modified on the mobile device.

    The setting is available for mobile devices running iOS 11 or later.

    This check box is cleared by default.

- In the **Cellular** section:

  - **Prohibit automatic sync while roaming**

    Prohibit automatic synchronization of user data when the iOS MDM device is roaming.

    If the check box is cleared, the user can enable automatic data synchronization when the device is roaming. Enabling automatic synchronization in roaming can result in unexpected mobile service costs.

    If the check box is selected, the user is not allowed to use automatic data synchronization when the device is roaming.

    This check box is cleared by default.

  - **Prohibit modifying cellular settings**

    Ability to configure cellular network data transfer by apps installed on a mobile device.

    If the check box is cleared, the user can configure the settings for data transfer over a cellular network.

    If the check box is selected, the settings for cellular network data transfer by apps cannot be modified.

    This check box is cleared by default.

- Restrictions on the **Additional settings** tab:

  - In the **Display** section:

    - **Prohibit changing wallpaper**

      Ability to select the image that will be displayed on the lock screen or Home screen.

      If the check box is cleared, the user can select the wallpaper for the mobile device.

      If the check box is selected, wallpaper selection is not available.

      This check box is cleared by default.

- In the **Text** section:
  - **Prohibit spellcheck**

    Deprecated in iOS 26.4 and later.

    Use of spellcheck when entering text on a mobile device. The spellcheck function underlines incorrectly spelled words and suggests corrections.

    If the check box is cleared, the user can enable and use the spellcheck function.

    If the check box is selected, spellcheck is not available when entering text.

    This check box is cleared by default.

  - **Prohibit auto-correction**

    Deprecated in iOS 26.4 and later.

    Use of the auto-correct function when entering text.

    If the check box is cleared, the user can enable and use the auto-correct function.

    If the check box is selected, auto-correct is not available when entering text.

    This check box is cleared by default.

  - **Prohibit dictionary search**

    Deprecated in iOS 26.4 and later.

    Use of a dictionary to get the definitions of words on the mobile device. Only a software keyboard has a dictionary function.

    If the check box is cleared, the user can highlight any word on the screen of the mobile device and get the definition of that word.

    If the check box is selected, dictionary search is not available.

    This check box is cleared by default.

- In the **Keyboard** section:
  - **Prohibit predictive text**

    Deprecated in iOS 26.4 and later.

    Use of the predictive text input function. The predictive text input function shows options for completing words and suggestions based on available dictionaries.

    If the check box is cleared, the user can enable and use the predictive text input function.

    If the check box is selected, the predictive text function is not available. In this case, suggestions are not displayed when entering text.

    This check box is cleared by default.

- **Prohibit keyboard shortcuts**

  > Deprecated in iOS 26.4 and later.

  Use of keyboard shortcuts for quick access to mobile device functions.

  If the check box is cleared, the user can enable the keyboard shortcut function and use it when working with the mobile device.

  If the check box is selected, the keyboard shortcut function is not available.

  This check box is cleared by default.

- In the **Notifications** section:

  - **Prohibit Wallet on-screen notifications when screen is locked**

    Use of Wallet notifications on the lock screen of the iOS MDM device.

    If the check box is cleared, Wallet notifications are displayed on the lock screen of the mobile device.

    If the check box is selected, Wallet notifications are not displayed on the lock screen of the mobile device. To work with Wallet, the user must unlock the device.

    This check box is cleared by default.

  - **Hide Control Center when screen is locked**

    Ability to go to the Control Center of the iOS MDM device when the device is locked.

    If the check box is cleared, the user can go to the Control Center when the device is locked.

    If the check box is selected, the user cannot go to the Control Center when the device is locked.

    This check box is cleared by default.

  - **Hide Notification Center when screen is locked**

    Ability to go to the Notification Center of the iOS MDM device when the device is locked.

    If the check box is cleared, the user can go to the Notification Center by swiping the lock screen down.

    If the check box is selected, the user cannot go to the Notification Center when the device is locked.

    This check box is cleared by default.

  - **Hide Today View when screen is locked**

    Display of information from the Today View on the screen of a locked iOS MDM device. The Today section of the Notification View shows the following information:

    - Calendar events
    - Reminders
    - Stock prices
    - Weather

    If the check box is cleared, the user can view notifications from the Today View on a locked mobile device.

If the check box is selected, the Today View is not displayed on the locked mobile device.

This check box is cleared by default.

- **Prohibit modifying notification settings**

  Ability to configure the display of notifications on the mobile device.

  If the check box is cleared, the user can configure the settings for displaying notifications on the mobile device.

  If the check box is selected, the display of notifications cannot be configured.

  This check box is cleared by default.

- Restrictions on the **OS update** tab:
  - In the **General** section:
    - **Delay software updates (days)**

      Allows delaying operating system updates on the device.

      If the check box is selected, the user cannot access updates for the specified period. The default delay is 30 days. You can specify another period in the **Number of days from 1 to 90** field.

      If the check box is cleared, the user can update the software as soon as updates are available.

      The setting is available for mobile devices running iOS version 11.3 or later.

      This check box is cleared by default.

7. Click **OK**.
8. Click **Save** to save the changes you have made.

As a result, feature restrictions will be configured on the user's mobile device after the policy is applied.

Configuring app restrictions

1. In the main window of Kaspersky Next Expert View (on-premise), select **Asset management** → **Policies**. In the list of group policies that opens, click the name of the policy that you want to configure.
2. In the policy properties window, select **Application settings**.
3. Select **iOS** and go to the **Restrictions** section.
4. On the **App restrictions** card, click **Settings**.

   The **App restrictions** window opens.
5. Enable the settings using the **App restrictions** toggle switch.
6. Configure iOS MDM device app restrictions.

   List of app restrictions

   Restrictions in the **Safari** section:

   - **Allow use of Safari**

     Use of the Safari browser on the iOS MDM device.

     If the check box is selected, the user is allowed to use the Safari browser.

If the check box is cleared, the user is not allowed to use the Safari browser. The Safari icon is hidden on the home screen of the iOS MDM device.

This check box is selected by default.

- **Allow AutoFill**

  Saving and autofilling of data entered by the user in web forms in the Safari browser.

  If this check box is selected, user data entered in web forms is saved. Later it is automatically inserted in web forms.

  If this check box is cleared, user data is not inserted in web forms.

  This check box is selected by default.

- **Warn the user when visiting a dangerous website**

  Option that enables a user warning prior to a visit to a website that Kaspersky Mobile Devices Protection and Management has found to be dangerous.

  If the check box is selected, Kaspersky Mobile Devices Protection and Management warns a user attempting to visit a dangerous website.

  If the check box is cleared, Kaspersky Mobile Devices Protection and Management does not warn a user attempting to visit a dangerous website.

  This check box is cleared by default.

- **Allow JavaScript**

  Use of JavaScript by the Safari browser.

  If the check box is selected, the Safari browser uses JavaScript when opening web pages.

  If the check box is cleared, the Safari browser does not use JavaScript when opening web pages.

  This check box is selected by default.

- **Block pop-up windows**

  Blocking of pop-up windows in the Safari browser.

  If this check box is selected, Kaspersky Mobile Devices Protection and Management blocks pop-up windows in the Safari browser.

  If this check box is cleared, Kaspersky Mobile Devices Protection and Management does not block pop-up windows in the Safari browser.

  This check box is cleared by default.

- **Cookie settings**

  Select the condition for accepting cookies:

  - **Allow cookies and website tracking**. The Safari browser accepts cookies and allows tracking user activity.
  - **Allow cookies and block website tracking**. The Safari browser accepts cookies and blocks tracking user activity.
  - **Block cookies and website tracking**. The Safari browser blocks cookies and tracking user activity.

  The default value is **Allow cookies and website tracking**.

Restrictions in the **Game Center** section:

- **Allow use of Game Center**

Access to the Game Center gaming service from the Game Center app on an iOS MDM device.

If the check box is selected, the user can visit the Game Center gaming service from the Game Center app on the mobile device.

If the check box is cleared, the user cannot visit the Game Center gaming service from the Game Center app on the mobile device. The Game Center icon is hidden on the home screen of the iOS MDM device.

This check box is selected by default.

- **Allow adding friends in Game Center**

  An option that allows adding users in the Game Center gaming service on the iOS MDM device.

  If the check box is selected, the user can add other users in the Game Center gaming service on the mobile device.

  If the check box is cleared, the user is not allowed to add other users in the Game Center gaming service on the mobile device.

  This check box is selected by default.

- **Allow multiplayer games in Game Center**

  Use of the Game Center gaming service in multiplayer mode on the iOS MDM device.

  If the check box is selected, the user can participate in multiplayer games in the Game Center gaming service on the mobile device.

  If the check box is cleared, the user is not allowed to participate in multiplayer games in the Game Center gaming service on the mobile device.

  > If the check box is cleared, users can still play games together via SharePlay or a third-party service.

  This check box is selected by default.

Restrictions in the **Additional settings** section:

- **Allow use of iTunes Store**

  Access to the iTunes Store media service from the iTunes app on an iOS MDM device.

  If the check box is selected, the user can view, buy, and download media content from the iTunes Store using the iTunes app on the mobile device.

  If the check box is cleared, the user cannot view, buy, and download media content from the iTunes Store using the iTunes app on the mobile device. The iTunes icon is hidden on the home screen of the iOS MDM device.

  This check box is selected by default.

- **Allow use of News**

  Viewing of news on the user's mobile device using the News app.

  If the check box is selected, the user can view news using the News app.

  If the check box is cleared, the News app is not available to the user.

  This check box is selected by default.

- **Allow use of Podcasts**

  Listening to podcasts on the user's mobile device using the Podcasts app.

  If the check box is selected, the user can search, play, and download podcasts using the Podcasts app.

  If the check box is cleared, podcasts cannot be downloaded to the mobile device.

This check box is selected by default.

7. Click **OK**.

8. Click **Save** to save the changes you have made.

As a result, app restrictions will be configured on the user's mobile device after the policy is applied.

Configuring content restrictions

Categories used for content restrictions are determined by Apple. In some cases, when content restrictions are configured, actual results may differ from expected results.

1. In the main window of Kaspersky Next Expert View (on-premise), select **Asset management** → **Policies**. In the list of group policies that opens, click the name of the policy that you want to configure.

2. In the policy properties window, select **Application settings**.

3. Select **iOS** and go to the **Restrictions** section.

4. On the **Content restrictions** card, click **Settings**.

   The **Content restrictions** window opens.

5. Enable the settings using the **Content restrictions** toggle switch.

6. Configure iOS MDM device content restrictions.

   List of content restrictions

   Region

   Selection of the country whose rating system is automatically applied to media content on the iOS MDM device.

   The default value is **United States**.

   Settings in the **Age rating** section:

   - **Videos**

     Selection of the restriction rating for access to movies on the iOS MDM device.

     The list of ratings depends on the region selected.

     If the **Allow all** option is selected, the user can view any movies on the mobile device.

     The **Allow all** option is selected by default.

   - **TV shows**

     Selection of the restriction rating for access to TV shows on the iOS MDM device.

     The list of ratings depends on the region selected.

     If the **Allow all** option is selected, the user can view any TV shows on the mobile device.

     The **Allow all** option is selected by default.

   - **Apps**

     Selection of the restriction rating for access to third-party apps on the iOS MDM device.

The list of ratings depends on the rating system selected.

If the **Allow all** option is selected, the user can use any third-party apps on the mobile device.

The **Allow all** option is selected by default.

> App restrictions may be enforced even if the **Allow all** option is selected. This is due to an issue known to Apple.

- **Allow downloading erotica in Apple Books**

  Access to adult content in Book Store on the user's mobile device.

  If the check box is selected, the user can download adult content from the Apple Books app to the iOS MDM device.

  If the check box is cleared, the user cannot download adult content from the Apple Books app to the iOS MDM device.

  This check box is selected by default.

- **Allow explicit content**

  Access to explicit media content from the iTunes Store on the iOS MDM device. Restrictions are applied by iTunes Store providers.

  If the check box is selected, explicit media content purchased via iTunes Store is available to the mobile device user.

  If the check box is cleared, explicit media content purchased via iTunes Store is hidden from the mobile device user.

  This check box is selected by default.

7. Click **OK**.
8. Click **Save** to save the changes you have made.

As a result, content restrictions will be configured on the user's mobile device after the policy is applied.

Configuring user access to websites

This section contains instructions on how to configure access to websites on Android and iOS devices.

Configuring access to websites on Android devices

You can use Web Control to configure Android device users' access to websites. Web Control supports website filtering by categories defined in the Kaspersky Security Network cloud service. Filtering allows you to restrict user access to certain websites or categories of websites (for example, "Gambling, lotteries, sweepstakes" or "Internet communication"). Web Control is enabled by default.

In Yandex Browser and Samsung Internet, malicious and phishing URLs may remain unblocked. This is because only the website domain is scanned. If it is a malicious or phishing domain, Web Protection blocks the threat. If the domain is not classified as malicious or phishing, the specific URL is not blocked.

Web Control on Android devices is supported only in Google Chrome, HUAWEI Browser, Samsung Internet, and Yandex Browser.

Web Control requires the following to operate on a managed device:

- Kaspersky Endpoint Security for Android must be configured as an Accessibility service.

  On corporate devices, if Kaspersky Endpoint Security for Android is not enabled as an Accessibility feature, Web Control is supported only in Google Chrome and checks only the domain of a website. To allow other browsers (Samsung Internet, Yandex Browser, and HUAWEI Browser) to support Web Control, enable Kaspersky Endpoint Security as an Accessibility feature. This will also let you use the Custom Tabs feature.

  If Kaspersky Endpoint Security for Android is not enabled as an Accessibility feature and a proxy is enabled in the **Google Chrome settings** card, Web Control will not work.

- The Statement regarding data processing for the purpose of using Web Protection (Web Protection Statement) must be accepted. Kaspersky Endpoint Security uses Kaspersky Security Network (KSN) to scan websites. The Web Protection Statement contains the terms of data exchange with KSN.

- On some devices, the user must manually grant the following permissions:

  - **Run in the background**
  - **Display pop-up windows while running in the background**
  - **Display pop-up window**
  - **Ignore battery optimization**

To configure the settings for device users' access to websites:

1. In the main window of Kaspersky Next Expert View (on-premise), select **Asset management** → **Policies**. In the list of group policies that opens, click the name of the policy that you want to configure.
2. In the policy properties window, select **Application settings**.
3. Select **Android** and go to the **Security controls** section.
4. On the **Web Control** card, click **Settings**.

   The **Web Control** window opens.

5. Select one of the following options:

- If you want the app to restrict user access to websites depending on their content, do the following:

  a. In the **Operating mode** drop-down list, in the drop-down list select **Prohibit websites in selected categories**.

  b. In the **Categories** section, create a list of prohibited categories by selecting the check boxes next to the categories of websites to which the app will block access.

- If you want the app to allow or block user access only to specified websites, do the following:

  a. In the **Operating mode** drop-down list, select **Allow only listed websites** or **Allow all websites except listed ones**.

  b. Click **Add**.

  c. In the window that opens, create a list of websites to which the app will allow or block access, depending on the value selected in the drop-down list. You can add websites by link (full URL, including the protocol, for example, `https://example.com`).

  To make sure that the app allows or blocks access to the specified website in all supported versions of Google Chrome, HUAWEI Browser, Samsung Internet, and Yandex Browser include the same URL twice — once with the HTTP protocol (for example, `http://example.com`) and once with the HTTPS protocol (for example, `https://example.com`).

  For example:

  - `https://example.com` — The main page of the website is either allowed or blocked. This URL can only be accessed through the HTTP protocol.
  - `http://example.com` — The main page of the website is either allowed or blocked, but only when accessed through the HTTP protocol. Other protocols like HTTPS are not affected.
  - `https://example.com/page/index.html` — Only the index.html page of the website will be allowed or blocked. The rest of the website is not affected by this entry.

  The app also supports regular expressions. When entering the address of an allowed or forbidden website, use the following templates:

  - `https://example\.com/.*` — This template blocks or allows all child pages of the website, accessed via the HTTPS protocol (for example, `https://example.com/about`).
  - `https?://example\.com/.*` — This template blocks or allows all child pages of the website, accessed via both the HTTP and HTTPS protocols.
  - `https?://.*\.example\.com` — This template blocks or allows all subdomain pages of the website (for example, `https://pictures.example.com`).
  - `https?://example\.com/[abc]/.*` — This template blocks or allows all child pages of the website where the URL path begins with 'a', 'b', or 'c' as the first directory (for example, `https://example.com/b/about`).
  - `https?://\w{3,5}.example\.com/.*` — This template blocks or allows all child pages of the website where the subdomain consists of a word with 3 to 5 characters (for example, `http://abde.example.com/about`).

Use the `https?` expression to select both the HTTP and HTTPS protocols. For more details on regular expressions, please refer to the Oracle Technical Support website.

d. Click **Add**.

- If you want the app to block user access to all websites, in the **Operating mode** section, in the drop-down list, select **Prohibit all websites**.

6. If you want the app to check the full URL when opening a website in Custom Tabs, select the **Check full URL when using Custom Tabs** check box.

   Custom Tabs is an in-app browser that allows the user to view web pages without having to leave the app and switch to a full web browser version. This option provides better URL recognition and checks URLs against the configured Web Control rules. If the check box is selected, Kaspersky Endpoint Security for Android opens the website in a full version of the browser and checks the whole web address of the website. If the check box is cleared, Kaspersky Endpoint Security for Android checks only the domain of the website in Custom Tabs.

   The Custom Tabs feature is supported in Google Chrome, HUAWEI Browser, and Samsung Internet.

7. If you want to lift content-based restrictions on user access to websites, disable the settings using the **Web Control** toggle switch and click **Disable**.

8. Click **OK**.

9. Click **Save** to save the changes you have made.

Mobile device settings are changed after the next device synchronization with Kaspersky Security Center.

Managing the website list

You can manage the list of websites with the following buttons:

- **Add** — Click to add a website to the list by entering a URL or regular expression.
- **Upload** — Click to add multiple websites to the list by specifying a TXT file that contains the required URLs or regular expressions. The file must be encoded in UTF-8. URLs or regular expressions in the file must be separated by semicolons or line breaks.
- **Edit** — Click to change the address of a website.
- **Delete** — Click to remove one or more websites from the list.

Configuring access to websites on iOS MDM devices

These settings apply to supervised devices.

Configure Web Control settings to control access to websites for iOS MDM device users. Web Control manages users' access to websites based on lists of allowed and forbidden websites. Web Control also lets you add website bookmarks on the bookmark panel in Safari.

By default, access to websites is not restricted.

If a URL is redirected to a different website, Web Control checks only the redirect target.

To configure settings for device users' access to websites:

1. In the main window of Kaspersky Next Expert View (on-premise), select **Asset management** → **Policies**. In the list of group policies that opens, click the name of the policy that you want to configure.
2. In the policy properties window, select **Application settings**.
3. Select **iOS** and go to the **Security controls** section.
4. On the **Web Control** card, click **Settings**.

   The **Web Control** window opens.
5. Enable the settings using the **Web Control** toggle switch.
6. In the **Operating mode** drop-down list do one of the following:
   - If you want to create a list of allowed websites, select **Allow only listed websites**.
   - If you want to create a list of forbidden websites, select **Allow all websites except listed ones**.
7. Do one of the following:
   - If you want to add websites manually:
     a. Click **Add**.
     b. Add websites to which the app will allow or block access, depending on the value selected in the drop-down list.

        The website address should begin with `http://` or `https://`. Kaspersky Mobile Devices Protection and Management allows or blocks access to all websites in the domain. For example, if you add `http://www.example.com` to the list of allowed websites, access is allowed `http://pictures.example.com` and `http://example.com/movies`.

        If you want to add an allowed website to bookmarks in Safari on mobile devices, select the **Add to bookmarks on device** check box below the website address.
     c. Click **Add**.
   - If you want to upload a TXT file with a list of websites, click **Upload**.

     The TXT file must be saved with the UTF-8 encoding and LF or CR+RF line breaks.
8. Click **OK**.
9. Click **Save** to save the changes you have made.

As a result, once the policy is applied, Web Control will be configured on the mobile devices.

Compliance Control

This section contains instructions on how to monitor the compliance of devices with corporate requirements and configure compliance control rules.

Compliance Control of Android devices

You can control Android devices for compliance with corporate security requirements. Corporate security requirements regulate how the user can work with the device. For example, the real-time protection must be enabled on the device, the anti-malware databases must be up-to-date, and the device password must be sufficiently strong. Compliance Control is based on a list of rules. A compliance rule includes the following components:

- Device check criterion (for example, absence of blocked apps on the device).
- Time period allocated for the user to fix the non-compliance (for example, 24 hours).
- Responses performed on the device if the user does not correct the non-compliance issue within the set time period (for example, lock the device).

  If the device is in battery saver mode, Kaspersky Endpoint Security for Android may perform this task later than specified.

To create a rule for checking devices for compliance with a policy:

1. In the main window of Kaspersky Next Expert View (on-premise), select **Asset management** → **Policies**. In the list of group policies that opens, click the name of the policy that you want to configure.
2. In the policy properties window, select **Application settings**.
3. Select **Android** and go to the **Security controls** section.
4. On the **Compliance Control** card, click **Settings**.

   The **Compliance Control** window opens.
5. Enable the settings using the **Compliance Control** toggle switch.
6. In the **When non-compliance is detected** section:
   - Select the **Notify user** check box to inform the user that the device does not comply with the policy.

     If the check box is cleared, the user is not notified of the non-compliance issue, and the response is performed on the device as soon as the time allocated for fixing the non-compliance expires.
   - Select the **Notify the administrator through the "Events" section** check box to inform the administrator that the device does not comply with the policy.
7. Click **Add**.

   The Add rule wizard starts. This wizard will help you create a set of rules for checking the device compliance with the policy. Navigate through the wizard using the **Next** and **Back** buttons.

Step 1. Criterion for non-compliance

Click **Add criterion** to specify the non-compliance criterion to trigger the rule.

The following criteria are available:

- **Real-time protection is disabled**

  Kaspersky Endpoint Security for Android is not installed or running on the device.

- **Anti-malware databases on device are out of date**

  Anti-malware databases were last updated 3 or more days ago.

- **Forbidden apps are installed**

  The list of apps on the device contains apps that are set as forbidden in the **App Control** settings of the policy.

- **Apps from forbidden categories are installed**

  The list of apps on the device contains apps from the categories that are set as forbidden in the **App Control** settings of the policy.

- **Not all required apps are installed**

  The list of apps on the device does not contain an app that is set as required in the **App Control** settings of the policy.

- **Operating system version is outdated**

  The Android version on the device is outside the allowed range.

  For this criterion, specify the minimum and maximum allowed versions of Android in the **Minimum version** and **Maximum version** fields. If the maximum allowed version is set to **Any**, future Android versions supported by Kaspersky Endpoint Security for Android will also be allowed.

- **Device has not been synchronized for a long time**

  The last synchronization of the device with the Administration Server is checked.

  For this criterion, specify the maximum period after the last synchronization in the **Period without synchronization** field.

- **Device has been rooted**

  The device is hacked (root access is gained on the device).

- **Unlock password is not compliant with security settings specified in policy**

  The unlock password on the device is not compliant with the settings defined in the **Screen unlock settings** card.

- **Installed version of Kaspersky Endpoint Security for Android is outdated**

  Kaspersky Endpoint Security for Android installed on the device is obsolete.

  This criterion applies only to an app installed using a Kaspersky Endpoint Security for Android installation package and if the minimum allowed version of Kaspersky Endpoint Security for Android is specified in the **App update** settings of the policy.

- **SIM card usage is not compliant with security requirements**

  The device SIM card has been replaced or removed compared to the previous check state, or an additional SIM card has been inserted.

For this criterion, select the specific condition that must be monitored:

- **The SIM card must not be replaced or removed**
- **The SIM card must not be replaced or removed; additional SIM cards must not be inserted**

- **Device location**

  The device is outside the specified geofence areas.

  > Specifying the geofence area will result in increased device power consumption.

  For this criterion, select the specific condition that must be monitored:

  - **The device is within a specified geofence** (the geofence areas are combined using the OR logical operator).
  - **The device is outside specified geofences** (the geofence areas are combined using the AND logical operator).

  To add a geofence area:

  1. Click **Add geofences**.

     The **Add geofences** window opens.

  2. Specify the **Geofence name**.

  3. Specify the geofence perimeter by entering a latitude and a longitude for each point.

     > For each geofence area, you can manually enter from 3 to 100 coordinate pairs (latitude, longitude) as decimal numbers.
     >
     > A geofence perimeter must not contain intersecting lines.

     If needed, you can specify more than 3 points by clicking the **Add point** button.

     To delete a point, click the **X** button.

     You can view the specified geofence area in the Yandex.Maps program by clicking **View on map**.

  4. Click **OK** to add the specified geofences.

- **Kaspersky Endpoint Security for Android has no access to precise or background location**

  Kaspersky Endpoint Security for Android is not allowed to access the precise location of the device or use the device location in the background.

- **Required permissions are missing**

  Kaspersky Endpoint Security for Android is not granted the permissions required for the app to function properly under the current policy settings.

Step 2. Responses for non-compliance with security requirements

Add the responses to be performed on the device if the specified non-compliance criterion is detected.

Choose one of the following options:

- **Add instant response**. The response is applied instantly after the non-compliance criterion is detected.
- **Add deferred response**. The response is applied after a deferral period that you can specify in the **Deferral period** field.

  The following responses are available:

  - **Block all apps except system apps**

    All apps on the device, except system apps, are blocked from starting.

    As soon as the non-compliance criterion selected for the rule is no longer detected on the device, the apps are automatically unblocked.

  - **Lock device**

    The mobile device is locked. To obtain access to data, you must unlock the device by entering the one-time passcode or using the **Unlock device** command.

  - **Wipe corporate data**

    The corporate data is wiped from the device. The list of wiped data depends on the mode in which the device operates:

    - On a personal device, Knox profile and mail certificate are wiped.
    - On a corporate device, Knox profile and the certificates installed by Kaspersky Endpoint Security for Android (mail, VPN, and SCEP profile certificates, except the mobile certificates) are wiped.
    - Additionally, on a device with corporate container, the container (its content, configurations, and restrictions) and the certificates installed in it (mail, VPN, and SCEP profile certificates, except the mobile certificates) are wiped.

  - **Reset to factory settings**

    All data is wiped from the device and settings are rolled back to their factory values. After this response is performed, the device will no longer be managed. To connect the device to Kaspersky Security Center, you must reinstall Kaspersky Endpoint Security for Android.

    On devices running Android 14 or later, this response is only applicable if the device is operating in corporate device mode.

  - **Lock corporate container**

    Corporate container on the device is locked. To obtain access to corporate container, you must unlock it.

    > The response is only applicable to devices running Android 6 or later.

    > After the corporate container on a device is locked, the history of the container passwords is cleared. It means that the user can specify one of the recent passwords, regardless of the corporate container password settings.

  - **Wipe data of all apps**

    On a corporate device, data of all apps on the device is wiped.

    On a device with corporate container, data of all apps in the container is wiped.

As a result, apps are rolled back to their default state.

> The response is only applicable to devices running Android 9 or later in corporate device or device with corporate container operating modes.

- **Wipe data of a specified app**

  For this response, you need to specify the package name for the app whose data is to be wiped. **How to get the package name of an app**

  To get the name of an app package:

  1. Open Google Play.
  2. Find the app and open its page.

     The app's URL ends with its package name (for example, https://play.google.com/store/apps/details?id=**com.android.chrome**).

  To get the name of an app package that has been added to Kaspersky Security Center:

  1. In the main window of Kaspersky Next Expert View (on-premise), select **Asset management** → **Mobile** → **Apps & files**.
  2. Select **Android** → **Apps**.

     In the list of apps that opens, app identifiers are displayed in the **Package name** column.

  As a result, the app is rolled back to its default state.

  > The response is only applicable to devices running Android 9 or later in corporate device or device with corporate container operating modes.

- **Prohibit safe boot**

  The user is not allowed to boot the device in safe mode.

  > The response is only applicable to corporate devices running Android 6 or later.

- **Prohibit use of camera**

  The user is not allowed to use any cameras on the device.

- **Prohibit use of Bluetooth**

  The user is not allowed to turn on and configure Bluetooth settings.

  > The response is only applicable to personal devices running Android 12 or earlier, corporate devices, or devices with corporate container.

- **Prohibit use of Wi-Fi**

  The user is not allowed to use and configure Wi-Fi settings.

The response is only applicable to personal devices running Android 9 or earlier or corporate devices.

- **Prohibit USB debugging features**

  The user is not allowed to use USB debugging features and developer mode on the device.

  The response is only applicable to corporate devices or devices with corporate container.

- **Prohibit airplane mode**

  The user is not allowed to enable airplane mode on the device.

  The response is only applicable to corporate devices running Android 9 or later.

Click **Add rule** to finish the Add rule wizard. The new rule and its details appear in the list of the Compliance Control rules. To temporarily disable a rule, use the toggle switch next to the selected rule.

To enable the automatic wiping of data from devices associated with disabled accounts of Active Directory users, select the **Wipe data from devices with disabled Active Directory user accounts** check box and select one of the following actions:

- **Wipe corporate data**
- **Reset to factory settings**

  On devices running Android 14 or later, this action is only applicable if the device is operating in corporate device mode.

These settings require integration with Microsoft Active Directory.

If you use policy profiles, be sure to enable the wipe data option for the entire policy. When a user account is disabled in Active Directory, it is first removed from the Active Directory user group. As a result, the policy profile is no longer applied to this user account, so the data is not wiped from the device.

Click **Save** to save the changes you have made.

Mobile device settings are changed after the next device synchronization with Kaspersky Security Center.

Compliance Control of iOS MDM devices

Compliance Control lets you monitor iOS MDM devices for compliance with corporate security requirements and take actions if non-compliance is found. Compliance Control is based on a list of rules. Each rule includes the following components:

- Status (whether the rule is enabled or disabled).
- Non-compliance criteria (for example, absence of the specified apps or the operating system version).
- Responses performed on the device if the user does not correct the non-compliance issue within the set time period (for example, wipe corporate data or send an email message to the user).

To create a rule for checking devices for compliance with a policy:

1. In the main window of Kaspersky Next Expert View (on-premise), select **Asset management** → **Policies**. In the list of group policies that opens, click the name of the policy that you want to configure.
2. In the policy properties window, select **Application settings**.
3. Select **iOS** and go to the **Security controls** section.
4. On the **Compliance Control** card, click **Settings**.

   The **Compliance Control** window opens.
5. Enable the settings using the **Compliance Control** toggle switch.
6. Click **Add**.

   The Add rule wizard starts. This wizard will help you create a set of rules for checking the device compliance with the policy. Navigate through the wizard using the **Next** and **Back** buttons.

Step 1. Criterion for non-compliance

Click **Add criterion** to specify the non-compliance criterion to trigger the rule.

The following criteria are available:

- **List of installed apps**

  The list of apps on the device contains forbidden apps or does not contain required apps.

  For this criterion, select a condition (**Contains** or **Does not contain**) and specify the **Bundle ID** of the app. **How to get the bundle ID of an app**

  To get the bundle ID of a built-in iPhone or iPad app,

  Follow the instructions in the Apple documentation.

  To get the bundle ID of any iPhone or iPad app:

  1. Open the App Store.
  2. Find the required app and open its page.

     The app's URL ends with its numerical identifier (for example, https://apps.apple.com/us/app/google-chrome/id**535886823**).
  3. Copy this identifier (without the letters "id").

4. Open the web page `https://itunes.apple.com/lookup?id=<copied identifier>`.

   This downloads a text file.

5. Open the downloaded file and find the "bundleId" fragment in it.

The text that directly follows this fragment is the bundle ID of the required app.

To get the bundle ID of an app that has been added to Kaspersky Security Center:

1. In the main window of Kaspersky Next Expert View (on-premise), select **Asset management** → **Mobile** → **Apps & files**.
2. Click **iOS**.

   In the list of apps that opens, app identifiers are displayed in the **Bundle ID** column.

- **Operating system version**

  The version of the operating system on the device is outside the allowed range.

  For this criterion, select a condition (**Equal to**, **Not equal to**, **Earlier than**, **Earlier than or equal to, Later than**, or **Later than or equal to**) and specify the iOS version.

  Note that the **Equal to** and **Not equal to** operators check for a full match of the operating system version with the specified value. For instance, if you specify iOS 15 in the rule, but the device is running iOS 15.2, the **Equal to** criterion is not met. If you need to specify a range of versions, you can create two criteria and use the **Earlier than** and **Later than** operators.

- **Supervision status**

  The supervision status of the device is not the one required.

  For this criterion, select the device operating mode (**Supervised** or **Basic control**).

- **Device type**

  The device type is not the one required.

  For this criterion, select a device type (**iPhone** or **iPad**).

- **Device model**

  The device model is not the one required.

  For this criterion, select a condition (**Equal to** or **Not equal to**) and specify models that will be checked or excluded from the check, respectively.

  To specify a model, in the **Model identifier** field, select the required model from the list or enter a value manually. The list contains mobile device codes and their matching product names. For example, if you want to add all iPhone 14 models, type "iPhone 14". In this case, you can select any of the available models: "iPhone 14", "iPhone 14 Plus", "iPhone 14 Pro", "iPhone 14 Pro Max".

  In some cases, the same product name may correspond to several mobile device codes (for example, the "iPhone 7" product name corresponds to two mobile device codes, "iPhone 9.1" and "iPhone 9.3"). Be sure that you select all of the mobile device codes that correspond to the required models.

  If you enter a value that is not on the list, nothing will be found. However, you can click **Add: "<value>"** under the field to add the entered value to the criterion.

If you specify the criteria that contradict each other (for example, **Device type** is set to **iPhone** but the list of values of **Device model**, with the **Equal to** operator selected, contains an iPad model), an error message is displayed. You cannot save a rule with such criteria.

- **Roaming**

  The device roaming status is not the one required.

  For this criterion, select a condition (**Device is roaming** or **Device is not roaming**).

- **Password on device**

  A password is not set or not compliant with the settings specified in the **Screen unlock settings** card.

  For this criterion, select a condition (**Not set**, **Set but not compliant**, or **Set and compliant)**.

- **Free storage on device**

  The amount of free space on the device is less than the specified threshold.

  For this criterion, specify the threshold amount of free space (**Less than**), and then select the measurement unit (**MB** or **GB**).

- **Device is not encrypted**

  The device is not encrypted.

  Data encryption is enabled by default on password-locked iOS devices (**Settings** > **Touch ID** / **Face ID and Password** > **Enable Password**). Also, the hardware encryption on a device must be set to **At block and file level** (you can check this setting in the device properties: go to **Asset management** → **Mobile** → **Devices**, and then select the required device).

- **Actions with SIM card**

  The device SIM card has been replaced or removed compared to the previous check state, or an additional SIM card has been inserted.

  For this criterion, select a condition (**The SIM card must not be replaced or removed** or **The SIM card must not be replaced or removed; additional SIM cards must not be inserted**).

  On eSIM compatible devices, the non-compliance detection cannot be removed by inserting the previously removed eSIM. This is because the device operating system recognizes each added eSIM as a new one. In this case, delete the compliance control rule from the policy.

- **Device has not been synchronized for a long time**

  The last synchronization of the device with iOS MDM Server is checked.

  For this criterion, specify the maximum time after the last sync in the **Period without synchronization** field, and then select the measurement unit (**Hours** or **Days**).

  We do not recommend that you specify a value less than the value of the **Synchronization period (min)** setting specified in the iOS MDM Server settings.

Step 2. Responses for non-compliance with security requirements

Add the responses to be performed on the device if the specified non-compliance criterion is detected.

Choose one of the following options:

- **Add instant response**. The response is applied instantly after the non-compliance criterion is detected.
- **Add deferred response**. The response is applied after a deferral period that you can specify in the **Deferral period** field.

  Responses are performed during the compliance rule check, which happens every 40 minutes, and persist until the next synchronization with the iOS MDM Server. To prevent repeating responses from a single non-compliance instance, set the **Synchronization period (min)** value to 30 minutes in the iOS MDM Server settings.

  If you specify responses that contradict each other, an error message is displayed. You cannot save such a rule.

  When the non-compliance criteria selected for the rule are no longer detected on the device, you can revert the response by sending the respective command to the device.

  The following responses are available:

  - **Send a message to the user**

    The user is informed about the non-compliance by email.

    For this response, specify user email addresses in the **Email** and **Alternate email address** fields. If necessary, you can also edit the email subject and default text.

    Make sure the **Email** notifications are configured in the Administration Server properties. For detailed information on configuring notifications delivery, refer to the Kaspersky Security Center Help.

  - **Wipe corporate data**

    All installed configuration profiles, provisioning profiles, the management profile, and apps for which the **Remove when management profile is deleted** check box has been selected are removed from the device. This response is performed by sending the **Wipe corporate data** command.

  - **Modify profile**

    For this response, specify one of the actions:

    - **Install profile**. The configuration profile is installed on device. This action is performed by sending the **Install configuration profile** command. For this response, you also need to specify the ID of the profile to be installed.

      Before the profile is installed, it must be added to the list of configuration profiles in the **Configuration profiles** section of the iOS MDM Server settings.

    - **Delete specified profile**. The configuration profile is deleted from the device. This response is performed by sending the **Delete configuration profile** command. For this action, you also need to specify the ID of the profile to be deleted.

- **Delete all profiles**. All previously installed configuration profiles are deleted from the device.

  When the non-compliance criteria selected for the rule are no longer detected on the device, you can install the deleted configuration profiles one by one, by sending the respective command to the device.

- **Update operating system**

  For this response, specify the **OS version** and one of the actions:

  - **Download and install**. The device operating system is downloaded and installed.

    If a non-existent operating system version is specified in the **Operating system version** criterion, the device will upgrade to the latest downloaded operating system.

  - **Download only**. The device operating system is downloaded.
  - **Install only**. The previously downloaded operating system is installed.

  This response is only applicable to supervised devices.

- **Modify Bluetooth settings**

  For this response, specify whether you want to enable or disable Bluetooth on the device.

  This response is only applicable to supervised devices.

- **Reset to factory settings**

  All data is deleted from the device and the settings are rolled back to their default values. After this response is performed, the device will no longer be managed. To connect the device to Kaspersky Security Center, you must reinstall the management profile on it.

- **Modify apps**

  For this response, specify one of the actions:

  - **Delete specified app**. The specified app is removed from the device.

    You can delete only a managed app. An app is considered managed if it has been installed through Kaspersky Security Center by executing the **Install app** command.

    When the non-compliance criteria selected for the rule are no longer detected on the device, you can revert the response by sending the respective command to the device.

    For this action, specify the **Bundle ID** of the app to be deleted. **How to get the bundle ID of an app**

    To get the bundle ID of a built-in iPhone or iPad app,

    Follow the instructions in the Apple documentation.

To get the bundle ID of any iPhone or iPad app:

1. Open the App Store.
2. Find the required app and open its page.

   The app's URL ends with its numerical identifier (for example, https://apps.apple.com/us/app/google-chrome/id**535886823**).
3. Copy this identifier (without the letters "id").
4. Open the web page `https://itunes.apple.com/lookup?id=<copied identifier>`.

   This downloads a text file.
5. Open the downloaded file and find the "bundleId" fragment in it.

   The text that directly follows this fragment is the bundle ID of the required app.

To get the bundle ID of an app that has been added to Kaspersky Security Center:

1. In the main window of Kaspersky Next Expert View (on-premise), select **Asset management** → **Mobile** → **Apps & files**.
2. Click **iOS**.

   In the list of apps that opens, app identifiers are displayed in the **Bundle ID** column.

- **Delete all apps**. All managed apps are deleted from the device.

  You can delete only managed apps. An app is considered managed if it has been installed through Kaspersky Security Center by executing the **Install app** command.

  When the non-compliance criteria selected for the rule are no longer detected on the device, you can install the deleted apps one by one, by sending the respective command to the device.

  For this action, specify the **Bundle ID** of the apps to be deleted. **How to get the bundle ID of an app**

  To get the bundle ID of a built-in iPhone or iPad app,

  Follow the instructions in the Apple documentation.

  To get the bundle ID of any iPhone or iPad app:

  1. Open the App Store.
  2. Find the required app and open its page.

     The app's URL ends with its numerical identifier (for example, https://apps.apple.com/us/app/google-chrome/id**535886823**).
  3. Copy this identifier (without the letters "id").

4. Open the web page `https://itunes.apple.com/lookup?id=<copied identifier>`.

   This downloads a text file.

5. Open the downloaded file and find the "bundleId" fragment in it.

The text that directly follows this fragment is the bundle ID of the required app.

To get the bundle ID of an app that has been added to Kaspersky Security Center:

1. In the main window of Kaspersky Next Expert View (on-premise), select **Asset management** → **Mobile** → **Apps & files**.
2. Click **iOS**.

   In the list of apps that opens, app identifiers are displayed in the **Bundle ID** column.

- **Delete profile of specified type**

  For this response, specify the **Profile type** to be deleted from the device (for example, **Web Clips** or **Calendar subscriptions**).

  As soon as the non-compliance criteria selected for the rule are no longer detected on the device, the deleted profiles are automatically restored.

- **Modify roaming settings**

  For this response, specify whether you want to enable or disable data roaming on the device.

Click **Add rule** to finish the Add rule wizard. The new rule and its details appear in the list of Compliance Control rules. To temporarily disable a rule, use the toggle switch next to the selected rule.

To enable the automatic wiping of data from devices associated with disabled accounts of Active Directory users, select the **Wipe data from devices with disabled Active Directory user accounts** check box and choose one of the following actions:

- **Wipe corporate data**
- **Reset to factory settings**

> These settings require integration with Microsoft Active Directory.

> If you use policy profiles, be sure to enable the wipe data option for the entire policy. When a user account is disabled in Active Directory, it is first removed from the Active Directory user group. As a result, the policy profile is no longer applied to this user account, so the data is not wiped from the device.

Click **Save** to save the changes you have made.

App Control

This section contains instructions on how to configure user access to apps on a mobile device.

App Control on Android devices

The App Control component lets you manage apps on Android devices and configure use of these apps to keep the devices secure.

You can restrict user activity on a device on which forbidden apps are installed or required apps are not installed (for example, by locking the device). You can impose restrictions using the Compliance Control component. To do so, in the rule settings, you must select the **Forbidden apps are installed**, **Apps from forbidden categories are installed**, or **Not all required apps are installed** criterion.

Kaspersky Endpoint Security for Android must be set as an Accessibility feature to ensure proper functioning of App Control. Kaspersky Endpoint Security for Android prompts the user to set the app as an Accessibility feature through the Initial Configuration Wizard. The user can skip this step or later disable this service in the device settings. If the user does this, App Control will not run. On corporate devices, App Control will run but may not work correctly if the Accessibility permission is not granted. It is still necessary to grant the Accessibility permission to the app for it to operate properly.

On corporate devices, you have extended control over the device. App Control operates without notifying the device user:

- Required apps are installed automatically in the background. To install apps silently, you need to specify a link to the APK file of the required app in the policy settings.
- Forbidden apps can be deleted from the device automatically. To delete apps silently, you need to select the **Remove forbidden apps automatically** check box in the policy settings.

To configure app startup settings on the mobile device:

1. In the main window of Kaspersky Next Expert View (on-premise), select **Asset management** → **Policies**. In the list of group policies that opens, click the name of the policy that you want to configure.
2. In the policy properties window, select **Application settings**.
3. Select **Android** and go to the **Security controls** section.
4. On the **App Control** card, click **Settings**.

   The **App Control** window opens.
5. Enable the settings using the **App Control** toggle switch.

6. Configure the settings on the following tabs:

- If you want to configure general rules of app management, **go to the App use tab**.

  1. In the **Operating mode** drop-down list, select the App Control mode:

     - To allow the user to start all apps except those specified as blocked in the list of categories and apps, select **Use all apps except forbidden ones**. Kaspersky Endpoint Security for Android will hide icons of forbidden apps. This option is selected by default.

     - To allow the user to start only apps specified in the list of categories and apps as allowed, recommended, or required apps, select **Use only allowed apps**. Kaspersky Endpoint Security for Android will hide icons of all apps except those specified in the list of allowed, recommended, or required apps and system apps.

  2. If you want Kaspersky Endpoint Security for Android to send data on forbidden apps to the event log without blocking them, select the **Do not block forbidden apps, only add a record to the event log** check box.

  3. If you want Kaspersky Endpoint Security for Android to block startup of system apps (such as Calendar, Camera, and Settings) on the user's mobile device, select the **Block system apps** check box. This check box is displayed in the **Use only allowed apps** mode.

     We recommend that you do not block system apps because doing so could cause the device to malfunction.

     Among system apps, the system mechanism for requesting app permissions may be blocked. If you want to unblock this mechanism, find its name (for example, `com.google.android.permissioncontroller`) in the event log and add it to the exceptions.

     Before removing Kaspersky Endpoint Security for Android from the device, clear this check box or disable App Control.

  4. If you want Kaspersky Endpoint Security for Android to remove forbidden apps from the device in the background without notifying the user, select the **Remove forbidden apps automatically** check box. This check box is displayed in policies for managing corporate devices.

  5. Click **Add** to add apps and categories for which you want to set rules.

     The **Add app or category** window opens.

  6. In the **Object** field, select either **App** or **App category** and do the following:

     - If you selected **App**, select an installation package or specify the package name and the app name in the corresponding fields.

     - If you selected **App category**, select a category and enter a description in the corresponding fields.

     - Click **Add**.

     The app or category is added to the list.

7. If you want to configure exceptions from listed forbidden or allowed apps, click **Exceptions**, specify package names in the window that opens, and click **OK**.

8. If you want to receive reports on installed apps, in the **Report on installed apps** section, select the **Send data on installed apps** check box. Then you can select the following check boxes:

   - **Send data on built-in apps** to send data on system apps.
   - **Send data on service apps** to send data on service apps that have no user interface and cannot be started manually.

   If a system app or service app is configured in the App Control settings, app data is sent regardless of the state of the check boxes.

   Kaspersky Endpoint Security for Android sends data to the event log each time an app is installed on a device or removed from it.

- If you want to set actions to be performed for selected apps, **go to the App management tab**.

  1. In the **Actions for apps** table, click **Add**.
  2. In the window that opens, do the following:

     a. In the **Action** field select one of the following actions:

     - **Install**. The user will be prompted to install the app.
     - **Remove**. The app will be deleted from the user's device.
     - **Recommend installation**. The user will receive a recommendation to install the app.

     b. Fill in the following fields:

     Use only legitimate and trusted sources. By configuring the settings in this section, you are solely responsible for any potential risks and consequences associated with using unreliable sources.

     - **Package name**
     - **App name**
     - **Link**

       Links to app packages must start with http:// or https://.

       For silent installation, specify a direct download link to an APK file that initiates a download without user interaction. Links to app store pages are not supported for silent installation. You can place APK files on Web Server or another source.

     - **Version**

       This field is a string parameter specified in the format of Oracle regular expressions. For more details on regular expressions, please refer to the Oracle Technical Support website.

The **Link** and **Version** fields are not displayed if you select **Remove** in the **Action** field.

c. Click **Add**.

The configured action is added to the list.

7. Click **OK.**
8. Click **Save** to save the changes you have made.

Mobile device settings are changed after the next device synchronization with Kaspersky Security Center.

App Control on iOS MDM devices

These settings apply to supervised devices.

Kaspersky Security Center lets you manage apps on iOS MDM devices to keep these devices secure. You can create a list of apps allowed to be installed on devices and a list of apps prohibited from being displayed and launched on devices.

To configure the list of apps allowed or prohibited to be installed on devices:

1. In the main window of Kaspersky Next Expert View (on-premise), select **Asset management** → **Policies**. In the list of group policies that opens, click the name of the policy that you want to configure.
2. In the policy properties window, select **Application settings**.
3. Select **iOS** and go to the **Security controls** section.
4. On the **App Control** card, click **Settings**.

   The **App Control** window opens.
5. Enable the settings using the **App Control** toggle switch.
6. In the **Operating mode** field, select one of the following options:

   - **Use all apps except forbidden ones**

     All apps will be displayed and available to run on the device except the ones from the list.

     Do not add the Settings and Phone apps to the list of forbidden apps, otherwise the management profile cannot be updated on the device.

   - **Use only allowed apps**

     This option is selected by default. If you select this option, the user will be able to open only the following apps on the device:

     - Apps from the list of allowed apps
     - System apps: Settings (for iOS and iPadOS) and Phone (for iOS)

All other apps will be hidden.

7. Click **Add** to add apps to the list.
8. In the window that opens, specify the app's bundle ID in the corresponding field. Specify the `com.apple.webapp` value to allow or restrict all Web Clips. **How to get the bundle ID of an app**

   To get the bundle ID of a built-in iPhone or iPad app,

   Follow the instructions in the Apple documentation.

   To get the bundle ID of any iPhone or iPad app:

   1. Open the App Store.
   2. Find the required app and open its page.

      The app's URL ends with its numerical identifier (for example, https://apps.apple.com/us/app/google-chrome/id**535886823**).
   3. Copy this identifier (without the letters "id").
   4. Open the web page `https://itunes.apple.com/lookup?id=<copied identifier>`.

      This downloads a text file.
   5. Open the downloaded file and find the "bundleId" fragment in it.

   The text that directly follows this fragment is the bundle ID of the required app.

   To get the bundle ID of an app that has been added to Kaspersky Security Center:

   1. In the main window of Kaspersky Next Expert View (on-premise), select **Asset management** → **Mobile** → **Apps & files**.
   2. Click **iOS**.

      In the list of apps that opens, app identifiers are displayed in the **Bundle ID** column.

   If necessary, you can specify several bundle IDs by clicking the **Add bundle ID** button.
9. Click **Save**.
10. Click **OK**.
11. Click **Save** to save the changes you have made.

Mobile device settings are changed after the next device synchronization with the iOS MDM Server.

As a result, once the policy is applied, the specified settings for apps are configured on devices.

Call Control on Android devices

The Call Control component lets you manage incoming and outgoing calls on Android devices and configure protection of devices against spam, fraudulent, and other unwanted calls.

Kaspersky Endpoint Security for Android handles and blocks unwanted calls on devices according to the specified Call Control policy settings. Phone numbers are checked against offline databases stored locally on devices and against global online databases. Based on the check results, the app either allows or blocks calls and, if configured, notifies the user about the number and its reputation.

Phone number databases are downloaded and updated according to the schedule configured in the **Database update** policy settings.

Prerequisites

If the Kaspersky Who Calls app is active on a device with Call Control enabled, call blocking behavior may be unpredictable due to a potential settings conflict. Pop-ups from Kaspersky Endpoint Security for Android with number information may also work incorrectly.

To avoid unpredictable behavior, before enabling Call Control, make sure that the Kaspersky Who Calls app is not installed on devices. For example, you can specify the **Remove** action for Kaspersky Who Calls in the App Control policy settings.

Before you start, we recommend that you ensure the following conditions are met:

- A license that provides the extended functionality of Kaspersky Secure Mobility Management with Call Control is installed in the Administration Server repository.
- Call Control Statement is accepted by the administrator. Otherwise, the user will be prompted to accept the agreement upon enabling call protection on their device.
- The version of Kaspersky Endpoint Security for Android installed on devices is 10.58.1.38 or later.
- The **Prohibit outgoing phone calls** restriction is disabled in the **Device feature restrictions** policy settings for corporate devices.

Configure Call Control

To set up protection of devices against unwanted calls:

1. In the main window of Kaspersky Next Expert View (on-premise), select **Asset management** → **Policies**. In the list of group policies that opens, click the name of the policy that you want to configure.
2. In the policy properties window, select **Application settings**.
3. Select **Android** and go to the **Security controls** section.
4. On the **Call Control** card, click **Settings**.

   The **Call Control** window opens.
5. Enable the settings using the **Call Control** toggle switch.

6. On the **General** tab:

- In the **Region of offline databases for number checking** field, select a region that will be considered the local region of all devices managed by the current policy. Offline databases for the selected region will be downloaded to devices for faster phone number checks.

  The Call Control feature is not intended for use within the territory of the European Union, the United Kingdom, State of California (USA), Brazil, Vietnam, and Indonesia and must not be activated within those territories. By enabling this feature, you confirm that you assume full responsibility for its use in your region and that, by using it, you comply with all provisions of applicable law.

  If your region is not listed, choose **Other**, but note that Kaspersky Endpoint Security for Android will not be able to download offline number databases and check call categories and number reputation while offline.

- In the **Operating mode** field, choose how call protection will work:

  - **Notify user about number reputation**. During calls, users will receive pop-ups from Kaspersky Endpoint Security for Android with information about the number and its reputation. Unwanted calls will not be blocked.

  - **Block fraudulent and spam calls or calls from specific categories**. During calls, users will receive pop-ups from Kaspersky Endpoint Security for Android with information about the number and its reputation, if configured in the policy. Fraudulent and spam calls, as well as calls from categories specified in the policy, will be automatically blocked.

  - **Advanced mode**. During calls, users will receive pop-ups from Kaspersky Endpoint Security for Android with information about the number and its reputation, if configured in the policy. Calls will be allowed or blocked based on the advanced settings specified in the policy.

    Depending on the selected operating mode, additional settings are available:

    - In the **Number lists** block of settings, specify the list of allowed or forbidden numbers.

      You can configure number lists to specify allowed and forbidden numbers.

      - Allowed numbers will be considered trusted, regardless of their reputation. Calls from and to numbers on this list will not be blocked.

      - Forbidden numbers will be considered unwanted, regardless of their reputation. All calls from and to numbers on this list will be blocked.

      To add allowed numbers:

      1. Click **Allowed numbers**.

      2. In the window that opens, if you want to enable blocking of all numbers that are not on the allowed list, select the **Block all numbers not on the allowed list** check box.

         Enabling this option will disable all settings specified in the **Block calls by category** and **Forbidden numbers** sections.

      3. Click **Add**.

         The **Add allowed numbers** window opens.

4. In the **Add number** field, specify the number that you want to allow.

   - Click **Add number** to add another allowed number.
   - Click **Add range of numbers** to add a range of numbers.

     Specify the lower and upper limits of the number range in the corresponding fields.

5. Click **Add**.

   The specified allowed numbers appear in the list.

   You can modify or delete allowed numbers or number ranges using the **Edit** and **Delete** buttons at the top of the list.

6. If you want to upload a file with a list of numbers from the administrator's computer, click **Upload**.

   The TXT file must not be larger than 5 MB and must be saved with the UTF-8 encoding. Numbers must be separated by line breaks, and number ranges must be separated by semicolons.

   If you upload an allowed or forbidden list that contains a number that is already on the opposite list, all calls from and to that number will be blocked.

7. Click **OK**.

To add forbidden numbers:

1. Click **Forbidden numbers**.
2. In the window that opens, click **Add**.

   The **Add forbidden numbers** window opens.

3. In the **Number** field, specify the number that you want to forbid.

   - Click **Add number** to add another forbidden number.
   - Click **Add range of numbers** to add a range of numbers.

4. Click **Add**.

   The specified forbidden numbers appear in the list.

   You can modify or delete forbidden numbers or number ranges using the **Edit** and **Delete** buttons at the top of the list.

5. If you want to upload a file with a list of numbers from the administrator's computer, click **Upload**.

   The TXT file must not be larger than 5 MB and must be saved with the UTF-8 encoding. Numbers must be separated by line breaks, and number ranges must be separated by semicolons.

If you upload an allowed or forbidden list that contains a number that is already on the opposite list, all calls from and to that number will be blocked.

6. Click **OK**.

- In the **Block calls by category** block of settings, set call restrictions for specific categories.

  Select one of the following options:

  - **Block all fraudulent and spam calls**

    All fraudulent and spam calls will be blocked on devices.

  - **Block calls from selected categories**

    Calls from the call categories specified in the policy will be blocked on devices.

    Specify at least one call category from the list. You can select all categories at once.

    If Kaspersky Endpoint Security for Android is not granted access to the user's contacts, the app will not be able to check calls from the **Not in contacts** category until this access is granted.

  - **Do not block calls by category**

    Calls will not be blocked by categories.

7. On the **Additional** tab:

- Select the **Trust user contacts** check box to allow all numbers from the user's contacts, except those specified in the forbidden list.

  If this option is enabled, Kaspersky Endpoint Security for Android will consider all numbers from the user's address book as trusted. These numbers will not be checked against the number databases and will not be blocked unless they are added to the list of forbidden numbers in the policy.

  If Kaspersky Endpoint Security for Android is not granted access to the user's contacts, the app will check all calls regardless of whether the number is in the contact list.

  On devices with a corporate container, if the **Prohibit personal apps from accessing corporate container contacts** option is enabled in the **Corporate container on devices** policy settings, Kaspersky Endpoint Security for Android will only be able to check if the number is in the user's contact list in the user's personal profile. If this option is disabled, the app will also check contacts in the work profile.

- In the **Incoming calls** and **Outgoing calls** blocks of settings, select **Show pop-ups from Kaspersky Endpoint Security for Android** to notify the user about number reputation.

If you choose this option, the user will be prompted to enable accessibility and allow displaying notifications from Kaspersky Endpoint Security for Android.

- **For any numbers**

  Users will receive pop-up notifications with information on number reputation for all numbers.

- **Only for numbers that are not in the user's contact list**

  Users will receive pop-up notifications with information on number reputation only for those numbers that are not in their contact list.

  If Kaspersky Endpoint Security for Android is not granted access to the user's contacts, the app will show pop-ups for all numbers until this access is granted.

8. Click **OK** to save the changes you have made.

Mobile device settings are changed after the next device synchronization with Kaspersky Security Center.

Call Control is not supported on devices with DSFA (Dual Sim Full Active).

Interaction of Call Control with Kaspersky Security Network

If Kaspersky Security Network is disabled or Kaspersky Private Security Network is enabled, global online databases will be unavailable. Still, Kaspersky Endpoint Security for Android will be able to check phone numbers. Call checking features will depend on the region selected in the **Region of offline databases for number checking** field:

- If a specific region is chosen, numbers will be checked against offline databases. Numbers from allowed or forbidden lists and from the categories *Not in contacts*, *Foreign numbers*, *Hidden numbers* will also be checked.
- If **Other** is chosen, only numbers from allowed or forbidden lists and from the categories *Not in contacts, Foreign numbers*, *Hidden numbers* will be checked.

To enable Kaspersky Security Network, Kaspersky Security Network Statement must be accepted by the administrator or by user on their device.

Call Control events

Kaspersky Next Expert View (on-premise) lets you monitor the operation of Call Control on devices by viewing corresponding events. These events reflect:

- Enabling and disabling of call protection functionality on devices
- Acceptance status of the Call Control Statement

- Detection of fraudulent and spam calls
- Blocking of calls
- Failed attempts to check numbers

> The **Failed to check number** event may be displayed in the Kaspersky Security Center event list either due to a technical error in the operation of the Kaspersky Endpoint Security for Android app or due to the absence of a specific phone number in the number databases.

For detailed information on viewing events in Kaspersky Next Expert View (on-premise), refer to the Kaspersky Security Center Help.

Mobile device protection levels

Mobile device protection levels defined by Kaspersky Security Center

Kaspersky Next Expert View (on-premise) lets you quickly assess the current protection level of managed mobile devices in the **Asset management** → **Mobile** → **Devices** section.

A device can have one of the following protection levels: **OK**, **Warning**, or **Critical**.

The protection levels are assigned and sent to Kaspersky Security Center, in accordance with the following requirements:

- One reason for assigning a protection level is detected on the device — the device gets the status displayed in the list of managed devices.
- Multiple reasons for assigning protection levels are detected on the device — Kaspersky Mobile Devices Protection and Management assigns the most critical status.
- No reasons for assigning a protection level are detected on the device — Kaspersky Mobile Devices Protection and Management does not send a status to Kaspersky Security Center, and the status is set as *OK*.

Protection levels and their meanings

Protection level	Meaning
OK	An administrator's intervention is not required.
Warning	Events have been logged that are related to potential or actual threats to the security of managed devices.
Critical	Serious problems have been encountered. An administrator's intervention is required to solve them.

The administrator's goal is to ensure that the *OK* protection level exists on all devices.

Mobile device protection levels defined by Kaspersky Mobile Devices Protection and Management

Kaspersky Mobile Devices Protection and Management defines the protection level of mobile devices based on policy settings and then sends the protection levels to Kaspersky Security Center during synchronization. The administrator can change the protection level in the policy, depending on the severity level of the condition (see the *Default values, reasons, and conditions for assigning a protection level on Android devices table*). In this case, the value set by the administrator overrides the default value defined by Kaspersky Mobile Devices Protection and Management.

Default values, reasons, and conditions for assigning a protection level on Android devices

Condition	Reason for protection level	Default value
Real-time protection is not running	One of the following reasons: • The Access to manage all files permission has not been granted. • Kaspersky Security Network is switched off.	*Critical*
Web Protection and Web Control are not running	One of the following reasons: • The Accessibility permission has not been granted. • Web Protection was switched off by the user in Kaspersky Endpoint Security settings. • The Ignore battery optimization permission has not been granted. • The Web Protection Statement has not been accepted.	*Warning*
App Control is not running	The Accessibility permission has not been granted.	*Warning*
Device lock is not available	One of the following reasons: • The Device administrator permission has not been granted. • The Accessibility permission has not been granted. • The app is not enabled to overlay other windows.	*Warning*
Device location is not available	One of the following reasons: • The Location permission has not been granted. • The device location cannot be determined (when permission is granted).	*Warning*
Versions of the Kaspersky Security Network Statement do not match	The version of the Kaspersky Security Network Statement that the user accepted in the policy and the version of the Kaspersky Security Network Statement on the device do not match.	*Warning*
Versions of the Marketing Statement do not match	The version of the Statement regarding data processing for marketing purposes that the user accepted in the policy and the version of the Statement regarding data processing for marketing purposes on the device do not match.	*OK*

Software inventory on Android devices

You can take an inventory of apps on Android devices connected to the Administration Server. Kaspersky Endpoint Security for Android receives information about all apps installed on mobile devices. Information obtained while taking inventory is displayed in the device properties in the **Events** section. In this section, you can view detailed information on each installed app.

To enable software inventory:

1. In the main window of Kaspersky Next Expert View (on-premise), select **Asset management** → **Policies**. In the list of group policies that opens, click the name of the policy that you want to configure.
2. In the policy properties window, select **Application settings**.
3. Select **Android** and go to the **Security controls** section.
4. On the **App Control** card, click **Settings**.

   The **App Control** window opens.

5. In the **Report on installed apps** section, select the **Send data on installed apps** check box.
6. If you want to receive data about system apps, select the **Send data on built-in apps** check box.
7. If you want to receive data about service apps, which do not have an interface and cannot be opened by the user, select the **Send data on service apps** check box.
8. Click **OK**.
9. Click **Save** to save the changes you have made.

Mobile device settings are changed after the next device synchronization with Kaspersky Security Center. Kaspersky Endpoint Security for Android sends data to the event log each time an app is installed or removed from the device.

Protection

This section contains information about how to remotely manage protection of mobile devices in the Kaspersky Next Expert View (on-premise).

Configuring anti-malware protection on Android devices

For timely detection of threats, viruses, and other malicious applications, you can configure the settings for real-time protection and automatic malware scans.

Kaspersky Endpoint Security for Android detects the following types of objects:

- Viruses, worms, Trojans, and malicious tools
- Adware
- Legitimate apps that intruders can use to compromise users' devices or data

Anti-Malware has several limitations:

- Due to technical limitations, Kaspersky Endpoint Security for Android cannot scan files with a size of 2 GB or more. During a scan, the app skips such files without notifying you that such files were skipped.
- On devices running Android 11 or later, Kaspersky Endpoint Security for Android can't scan the "Android/data" and "Android/obb" folders and detect malware in them due to technical limitations.

Configuring real-time protection

To configure real-time protection settings for mobile devices:

1. In the main window of Kaspersky Next Expert View (on-premise), select **Asset management** → **Policies**. In the list of group policies that opens, click the name of the policy that you want to configure.
2. In the policy properties window, select **Application settings**.

3. Select **Android** and go to the **Protection** section.

4. On the **Real-time protection** card, click **Settings**.

   The **Real-time protection** window opens.

5. Enable the settings using the **Real-time protection** toggle switch.

   If this toggle switch is turned on, mobile device protection is enabled and the user cannot disable it.

   If this toggle switch is turned off, mobile device protection is enabled but can be manually disabled by the user.

6. In the **App scan** drop-down list, select the app scan mode:

   - **Do not scan apps**
   - **Scan only new apps and files from the Downloads folder**
   - **Scan all apps and monitor actions with files**

7. In the **Action on threat detection** drop-down list, select one of the following options:

   - **Delete**

     Detected objects will be automatically deleted. The user is not required to take any additional actions. Prior to deleting an object, Kaspersky Endpoint Security for Android will display a temporary notification about the detection of the object.

   - **Skip**

     If detected objects have been skipped, Kaspersky Endpoint Security for Android warns the user about problems in device protection. For each skipped threat, the app provides actions that the user can perform to eliminate the threat. The list of skipped objects may change, for example, if a malicious file is deleted or moved. To receive an up-to-date list of threats, run a full device scan. To ensure reliable protection of your data, eliminate all detected objects.

   - **Delete and save a backup copy of file in quarantine**

8. To enable additional scanning of new apps before they are started for the first time on the user's device with the help of the Kaspersky Security Network cloud service, select the **Additional protection by Kaspersky Security Network** check box.

9. To block adware and apps that can be exploited by criminals to harm the device or user data, select the **Detect adware, autodialers, and legitimate apps that intruders can use to compromise the user's device and data** check box.

10. Click **OK**.

11. Click **Save** to save the changes you have made.

Mobile device settings are changed after the next device synchronization with Kaspersky Security Center.

Configuring automatic malware scans

To configure autorun of malware scans on the mobile device:

1. In the main window of Kaspersky Next Expert View (on-premise), select **Asset management** → **Policies**. In the list of group policies that opens, click the name of the policy that you want to configure.
2. In the policy properties window, select **Application settings**.
3. Select **Android** and go to the **Protection** section.
4. On the **Scan** card, click **Settings**.

   The **Scan** window opens.
5. Enable the settings using the **Scan** toggle switch.
6. In the **Action on threat detection** list, select one of the following options:

   - **Delete**

     Detected objects will be automatically deleted. The user is not required to take any additional actions. Prior to deleting an object, Kaspersky Endpoint Security for Android will display a temporary notification about the detection of the object.

   - **Skip**

     If detected objects have been skipped, Kaspersky Endpoint Security for Android warns the user about problems in device protection. For each skipped threat, the app provides actions that the user can perform to eliminate the threat. The list of skipped objects may change, for example, if a malicious file is deleted or moved. To receive an up-to-date list of threats, run a full device scan. To ensure reliable protection of your data, eliminate all detected objects.

   - **Delete and save a backup copy of file in quarantine**

   - **Ask user**

     Kaspersky Endpoint Security for Android displays a notification prompting the user to choose the action to take on the detected object: **Skip** or **Delete**.

     Kaspersky Endpoint Security for Android must be set as an Accessibility feature to ensure the display of notifications on mobile devices running Android 10 or later. Kaspersky Endpoint Security for Android prompts the user to set the app as an Accessibility feature through the Initial Configuration Wizard. The user can skip this step or disable this service in the device settings at a later time. In this case, Kaspersky Endpoint Security for Android displays an Android system window prompting the user to choose the action to take on the detected object: Skip or Delete. To apply an action to multiple objects, you need to open Kaspersky Endpoint Security.

If during a scan Kaspersky Endpoint Security for Android detects malicious apps on users' devices, the actions differ depending on the **device management mode**.

On corporate devices, installed malicious apps detected by Kaspersky Endpoint Security for Android are deleted from the device automatically if the **Delete** option is selected. If Kaspersky Endpoint Security for Android detects malicious system apps, they are prohibited from being displayed and launched on users' devices.

In a corporate container, installed malicious apps detected by Kaspersky Endpoint Security for Android are not deleted but prohibited from being displayed and launched on users' devices without notifying device users.

If the **Ask user** option is selected, Kaspersky Endpoint Security for Android prompts users to select an action for each detected app, both on corporate devices and devices with a corporate container.

> Installed malicious apps cannot be quarantined. Accordingly, if the **Delete and save a backup copy of file in quarantine** option is selected, a detected malicious app is deleted.

On personal devices, detected malicious apps cannot be deleted automatically. In this case, Kaspersky Endpoint Security for Android prompts the user to delete or skip the detected app.

7. In the **Scheduled scan** field, you can configure the settings for automatic launching a full scan of the device file system.
8. If you selected a weekly or daily scan, specify the day of the week (for weekly scans) and start time in the **Day** and **Time** fields.

   > If the device is in battery saver mode, the app may perform this task later than specified.

9. Click **OK**.
10. Click **Save** to save the changes you have made.

    Mobile device settings are changed after the next device synchronization with Kaspersky Security Center. Kaspersky Endpoint Security for Android scans all files, including the contents of archives.

To keep mobile device protection up to date, configure the anti-malware database update settings.

By default, anti-malware database updates are disabled when the device is roaming. Scheduled updates of anti-malware databases are not performed.

Configuring database updates

To configure settings for anti-malware database updates:

1. In the main window of Kaspersky Next Expert View (on-premise), select **Asset management** → **Policies**. In the list of group policies that opens, click the name of the policy that you want to configure.
2. In the policy properties window, select **Application settings**.
3. Select **Android** and go to the **Protection** section.
4. On the **Database update** card, click **Settings**.

   The **Database update** window opens.

5. Enable the settings using the **Database update** toggle switch.

6. In the **Scheduled database update** field, you can configure the settings for automatic anti-malware database updates on the user's device.

7. If you selected a weekly or daily database update, specify the day of the week (for weekly database updates) and start time in the **Day** and **Time** fields.

   If the device is in battery saver mode, the app may perform this task later than specified.

8. In the **Database update source** section, specify the update source from which Kaspersky Endpoint Security for Android receives and installs anti-malware database updates:

   - **Kaspersky servers**

     Using a Kaspersky update server as an update source for downloading the databases of Kaspersky Endpoint Security for Android on users' mobile devices. To update databases using Kaspersky servers, Kaspersky Endpoint Security for Android transmits data to Kaspersky (for example, the update task run ID). The list of data that is transmitted during database updates is provided in the End User License Agreement.

   - **Administration Server**

     Using the repository of Kaspersky Security Center Administration Server as an update source for downloading the databases of Kaspersky Endpoint Security for Android on users' mobile devices.

   - **Other source**

     Using a third-party server as an update source for downloading the databases of Kaspersky Endpoint Security for Android on users' mobile devices. To start an update, you must enter the address of an HTTP server in the field below (for example, `http://domain.com/`).

9. If you want Kaspersky Endpoint Security for Android to download database updates according to the update schedule when the device is roaming, select the **Allow database update while roaming** check box in the **Database update while roaming** section.

   Even if the check box is cleared, the user can manually start an anti-malware database update when the device is roaming.

10. Click **OK**.

11. Click **Save** to save the changes you have made.

Mobile device settings are changed after the next device synchronization with Kaspersky Security Center.

Protecting Android devices on the internet

You can use Web Protection to protect personal data of mobile device users on the internet. Web Protection blocks malicious websites that distribute malicious code, and phishing websites designed to steal your confidential data and gain access to your financial accounts. Web Protection scans websites before you open them using the Kaspersky Security Network cloud service. Web Protection is enabled by default.

In Yandex Browser and Samsung Internet, malicious and phishing URLs may remain unblocked. This is because only the website domain is scanned. If it is a malicious or phishing domain, Web Protection blocks the threat. If the domain is not classified as malicious or phishing, the specific URL is not blocked.

Web Protection on Android devices is supported only in Google Chrome, HUAWEI Browser, Samsung Internet, and Yandex Browser.

Web Protection requires the following to operate on a managed device:

- Kaspersky Endpoint Security for Android must be configured as an Accessibility service.

  On corporate devices, if Kaspersky Endpoint Security for Android is not enabled as an Accessibility feature, Web Protection is supported only in Google Chrome and checks only the domain of a website. To allow other browsers (Samsung Internet, Yandex Browser, and HUAWEI Browser) to support Web Protection, enable Kaspersky Endpoint Security as an Accessibility feature.

- The Statement regarding data processing for the purpose of using Web Protection (Web Protection Statement) must be accepted. Kaspersky Endpoint Security uses Kaspersky Security Network (KSN) to scan websites. The Web Protection Statement contains the terms of data exchange with KSN.

- On some devices, the user must manually grant the following permissions:

  - **Run in the background**
  - **Display pop-up windows while running in the background**
  - **Display pop-up window**
  - **Ignore battery optimization**

Web Protection for HUAWEI Browser, Samsung Internet, and Yandex Browser does not block sites on a mobile device if a corporate container is used and Web Protection is enabled only for the corporate container.

To enable Web Protection:

1. In the main window of Kaspersky Next Expert View (on-premise), select **Asset management** → **Policies**. In the list of group policies that opens, click the name of the policy that you want to configure.
2. In the policy properties window, select **Application settings**.
3. Select **Android** and go to the **Protection** section.
4. On the **Web Protection** card, enable the settings using the **Web Protection** toggle switch.

5. Click **Enable**.

> If you disable Web Protection, Web Control will also be disabled.

Mobile device settings are changed after the next device synchronization with Kaspersky Security Center.

Scanning notifications from messengers

Kaspersky Endpoint Security for Android can detect malicious and phishing URLs in notifications from Telegram, WhatsApp, the default SMS app, and other common messengers. Only URLs expressed as text directly in the notification text can be scanned. URLs embedded in markup are not scanned.

The following conditions must be met to enable notification scanning:

- Web Protection must be enabled.
- Displaying notifications must be allowed for the desired messengers. Kaspersky Endpoint Security for Android scans only notifications that can be displayed on the device screen.
- On Google Pixel and Vivo devices, the "Conversations" permission must be granted to Kaspersky Endpoint Security in the notification access settings.

To enable scan of notifications:

1. In the main window of Kaspersky Next Expert View (on-premise), select **Asset management** → **Policies**. In the list of group policies that opens, click the name of the policy that you want to configure.
2. In the policy properties window, select **Application settings**.
3. Select **Android** and go to the **Protection** section.
4. On the **Web Protection** card, select the **Block notifications that contain malicious and phishing URLs** check box.
5. To allow access to notifications on a mobile device, refer to the Web Protection section.

The app now scans notifications to detect malicious and phishing URLs. If a dangerous URL is found, the notification is blocked and a blocking screen with information about the blocked notification appears.

> If Kaspersky Endpoint Security for Android is not enabled as an Accessibility feature, the app sends a push notification about the detected dangerous URLs instead of displaying a blocking screen. After tapping the push notification, a screen with information about the blocked notification appears.

Protection of data on a stolen or lost device

This section describes how you can configure the unauthorized access protection settings on the device in case it gets lost or stolen.

Sending commands to a lost or stolen mobile device

To protect data on a mobile device that is lost or stolen, you can send special commands.

You can send commands to the following types of managed mobile devices:

- Android devices managed via the Kaspersky Endpoint Security for Android app
- iOS MDM devices

Each device type supports a specific set of commands (see the tables below).

Commands for Android devices

Commands for protecting data on a lost or stolen Android device

Command	Result
Lock device	The mobile device is locked. To obtain access to data, you must unlock the device using the **Unlock device** command or a one-time passcode.
Unlock device	The mobile device is unlocked. After unlocking a device running Android 5 – 6, the screen unlock password is reset to "1234". After unlocking a device running Android 7 or later, the screen unlock password is not changed.
Reset to factory settings	All data is deleted from the mobile device and the settings are rolled back to their factory values. After this command is executed, the device will not be able to receive or execute subsequent commands. This command is unavailable for personal devices and devices with a corporate container running Android 14 or later.
Wipe corporate data	Corporate data is wiped from the device. The list of wiped data depends on the mode the device is operating in: • On a personal device, the Knox container, corporate files sent to the device, and mail certificate are wiped. • On a corporate device, the Knox container, corporate files sent to the device, and the certificates installed by Kaspersky Endpoint Security for Android (mail, VPN, and SCEP profile certificates, except the mobile certificates) are wiped. • Additionally, if a corporate container was created, the corporate container (its contents, corporate files sent to the device, configurations, and restrictions) and the certificates installed in the corporate container (mail, VPN, and SCEP profile certificates, except the mobile certificates) are wiped.
Locate device	The mobile device's location coordinates are obtained. To view the device location in Yandex.Maps, go to the **Asset management** → **Mobile** → **Devices** section. Then choose a device and select **Command history** → **Locate device** → **Device coordinates** → **View on map**. After you click **View on map**, the device coordinates are transferred to Yandex.Maps and the device is shown on a map. On devices running Android 12 or later, if the user granted the "Use approximate location" permission, the Kaspersky Endpoint Security for Android app first tries to get the precise device location. If this is not successful, the approximate device location is returned only if it was received within the past 30 minutes. Otherwise, the command fails. This command does not work on Android devices if Google Location Accuracy is disabled in the settings. Please be aware that not all Android devices come with this location setting.

Command	Result
Take photos	The mobile device is locked. Photos are taken using the front camera of the device when somebody attempts to unlock the device. On devices with a pop-up front camera, the photo will be black if the camera is stowed. When attempting to unlock the device, the user automatically consents to having their photo taken on the device. If the permission to use the camera has been revoked, the mobile device displays a notification and prompts to provide the permission. On a mobile device running Android 12 or later, if the permission to use the camera has been revoked via Quick Settings, the notification is not displayed but the taken photo is black.
Sound alarm	The mobile device sounds an alarm for 5 minutes (for 1 minute if the device battery is low) or until the user unlocks the device.
Wipe app data	The data of a specified app is wiped from the mobile device. For this action, you need to specify the package name for the app whose data is to be deleted. As a result, the app is rolled back to its default state. The data of system and administrative apps is not wiped.
Wipe data of all apps	The data of all apps is wiped from the mobile device. On a corporate device, the data of all apps on the device is wiped. On a device with a corporate container, the data of all apps in the corporate container is wiped. As a result, apps are rolled back to their default state. The data of system and administrative apps is not wiped.
Get location history	The mobile device's location history for the last 14 days is displayed. To view the device location in Yandex.Maps, go to the **Asset management** → **Mobile** → **Devices** section. Then choose a device and select **Command history** → **Get location history** → **View on map**. After you click **View on map**, the device coordinates are transferred to Yandex.Maps and the device is shown on a map. Due to technical limitations on Android devices, the device location may be retrieved less often than specified in the **Location tracking** settings.

Commands for iOS MDM devices

Commands for protecting data on a lost or stolen iOS MDM device

Command	Result
Lock device	The mobile device is locked. To access data, you must unlock the device.
Reset unlock password	The mobile device's screen unlock password is reset, and the user is prompted to set a new password in accordance with policy requirements.
Reset to factory settings	All data is deleted from the mobile device and the settings are rolled back to their factory values. After this command is executed, the device will not be able to receive or execute subsequent commands.
Wipe corporate data	All installed configuration profiles, provisioning profiles, the management profile, and apps for which the **Remove when management profile is deleted** check box has been selected are removed from the device.

Command	Result
Enable Lost Mode (supervised only)	Lost Mode is enabled on the supervised mobile device, and the device is locked. The device screen shows a message and phone number that you can edit. If you send the **Enable Lost Mode** command to a supervised iOS MDM device without a SIM card and this device is restarted, the device won't be able to connect to Wi-Fi and receive the **Disable Lost Mode** command. This is a specific feature of iOS devices. To avoid this issue, you can either send the command only to devices with a SIM card, or insert a SIM card into the locked device to allow it to receive the **Disable Lost Mode** command over the mobile network.
Locate device (Lost Mode only)	The location of the mobile device is obtained. To view the device location in Yandex.Maps, go to the **Asset management** → **Mobile** → **Devices** section. Then choose a device and select **Command history** → **Locate device** → **Device coordinates** → **View on map**. After you click **View on map**, the device coordinates are transferred to Yandex.Maps and the device is shown on a map.
Sound alarm (Lost Mode only)	A sound is played on the lost mobile device.
Disable Lost Mode (supervised only)	Lost Mode is disabled on the mobile device, and the device is unlocked.

Permissions for executing commands

Special rights and permissions are required for executing Kaspersky Endpoint Security for Android commands. When the Initial Configuration Wizard is running, Kaspersky Endpoint Security for Android prompts the user to grant the application all required rights and permissions. The user can skip these steps or later disable these permissions in the device settings. If this is the case, it will be impossible to execute commands.

On devices running Android 10 or later, the user must grant the "All the time" permission to access the location. On devices running Android 11 or later, the user must also grant the "While using the app" permission to access the camera. Otherwise, Anti-Theft commands will not function. The user will be notified of this limitation and will again be prompted to grant the required level of permissions. If the user selects the "Only this time" option for the camera permission, access is considered granted by the app. We recommend contacting the user directly if the Camera permission is requested again.

For the complete list of available commands, please refer to the Commands for mobile devices section. To learn more about sending commands from Administration Console, please refer to the Sending commands section.

Unlocking a mobile device

You can unlock a mobile device using the following methods:

- Send the mobile device unlock command
- Enter the one-time passcode on the mobile device (only for Android devices)

On certain devices (for example, HUAWEI, Meizu, and Xiaomi), you must manually add Kaspersky Endpoint Security for Android to the list of apps that are started when the operating system starts. If the app is not added to the list, you can unlock the device only by using a one-time passcode. You cannot use commands to unlock the device.

To learn more about sending commands from the list of mobile devices in Kaspersky Next Expert View (on-premise), please refer to the Sending commands section.

A one-time device passcode is a secret code for unlocking the mobile device. The passcode is generated by Kaspersky Security Center and is unique for each mobile device. You can change the length of the one-time passcode (4, 8, 12, or 16 digits) in the **Anti-Theft** settings of the policy.

To unlock a mobile device using a one-time passcode:

1. In the main window of Kaspersky Next Expert View (on-premise), select **Asset management** → **Mobile** → **Devices**.
2. Click the mobile device for which you want to get a one-time passcode.
3. Select **Applications** → **Kaspersky Mobile Devices Protection and Management**.

   The Kaspersky Mobile Devices Protection and Management properties window opens.
4. Select the **Application settings** tab.

   The unique passcode for the selected device is shown in the **One-time code** field of the **One-time device passcode** section.
5. Use any available method (such as email) to communicate the one-time passcode to the user of the locked device.

   The user then must enter the received one-time passcode on the screen of the device that is locked by Kaspersky Endpoint Security for Android.

The user's mobile device is unlocked.

After unlocking a device running Android 5 – 6, the screen unlock password is reset to "1234". After unlocking a device running Android 7 or later, the screen unlock password is not changed.

To change the length of the one-time device passcode:

1. In the main window of Kaspersky Next Expert View (on-premise), select **Asset management** → **Policies**. In the list of group policies that opens, click the name of the policy that you want to configure.
2. In the policy properties window, select **Application settings**.
3. Select **Android** and go to the **Protection** section.
4. On the **Anti-Theft** card, click **Settings**.

   The **Anti-Theft** window opens.
5. Select the length of the one-time device passcode in the corresponding drop-down list. By default, the passcode is 4 digits long.
6. If you want to contact the person who finds the mobile device, in the **Text displayed on locked device** field, enter the text of the message that will be shown on the lock screen.
7. Click **OK**.
8. Click **Save** to save the changes you have made.

The length of the one-time passcode is set to the selected value.

Mobile device settings are changed after the next device synchronization with Kaspersky Security Center.

Configuring the device unlock password strength

To protect access to a user's mobile device, you should set a device unlock password.

This section contains information about how to configure password protection on Android and iOS devices.

Configuring a strong unlock password for an Android device

To keep an Android device secure, you need to configure the use of a password that the user is prompted to enter when unlocking the device.

You can impose restrictions on the user's activity on the device if the unlock password is weak (for example, by locking the device). You can impose restrictions using the Compliance Control component. To do this, in the scan rule settings, you must select the **Unlock password doesn't comply with security requirements** criterion.

On certain Samsung devices running Android 7 or later, when the user attempts to configure unsupported methods for unlocking the device (for example, a graphical password), the device may be locked if the following conditions are met: removal protection is enabled for Kaspersky Endpoint Security for Android and strength requirements are set for the screen unlock password. To unlock the device, you must send a special command to the device.

Configuring unlock password settings

To configure the use of an unlock password:

1. In the main window of Kaspersky Next Expert View (on-premise), select **Asset management** → **Policies**. In the list of group policies that opens, click the name of the policy that you want to configure.
2. In the policy properties window, select **Application settings**.
3. Select **Android** and go to the **Security controls** section.
4. On the **Screen unlock settings** card, click **Settings**.

   The **Screen unlock settings** window opens.
5. Enable the settings using the **Screen unlock settings** toggle switch, if you want the app to check whether an unlock password has been set.

   The toggle switch in this card does not enable or disable the corresponding functionality on devices. Enabling the toggle switch lets you configure custom settings. Disabling the toggle switch lets you use default settings.

   If the app detects that no system password has been set on the device, it prompts the user to set one. The password is set according to the parameters defined by the administrator.

6. Specify the following options, if required:

- **Minimum password length**

  The minimum number of characters in the user password. Possible values: 4 to 16 characters.

  The user's password is 4 characters long by default.

  The following applies only to the user's personal space and the corporate container:

  - In the user's personal space, Kaspersky Endpoint Security converts the password strength requirements into one of values available in the system: medium or high on devices running Android 10 or later.

  - In the corporate container, Kaspersky Endpoint Security converts the password strength requirements into one of the values available in the system: medium or high on devices running Android 12 or later.

  The values are determined using the following rules:

  - If the required password length is 1 to 4 characters, then the app prompts the user to set a medium-strength password. It must be either numeric (PIN) with no repeating or ordered sequences (e.g. 1234), or alphabetic/alphanumeric. The PIN or password must be at least 4 characters long.

  - If the required password length is 5 or more characters, then the app prompts the user to set a high-strength password. It must be either numeric (PIN) with no repeating or ordered sequences, or alphabetic/ alphanumeric (password). A PIN must be at least 8 digits long. A password must be at least 6 characters long.

- **Minimum password complexity requirements**

  Specifies the minimum unlock password requirements. These requirements apply only to new user passwords. The following values are available:

  - **Numeric**

    The user can set a password that includes numbers or set any stronger password (for instance, an alphabetic or alphanumeric password).

    This option is selected by default.

  - **Alphabetic**

    The user can set a password that includes letters (or other non-number symbols) or set any stronger password (for instance, an alphanumeric password).

  - **Alphanumeric**

    The user can set a password that includes both numbers and letters (or other non-number symbols) or set any stronger complex password.

  - **No requirements**

    The user can set any password.

  - **Complex**

    The user must set a complex password according to the specified password properties:

    - **Minimum number of letters**

    - **Minimum number of digits**

    - **Minimum number of special characters**

- **Minimum number of lowercase letters**
- **Minimum number of uppercase letters**
- **Minimum number of non-alphabetic characters**

- **Complex numeric**

  The user can set a password that includes numbers with no repetitions (e.g. 4444) and no ordered sequences (e.g. 1234, 4321, 2468) or set any stronger complex password.

- **Maximum password lifetime (days)**

  Specifies the number of days before the password expires. Applying a new value will set the current password lifetime to the new value.

  The default value is 0. This means that the password won't expire.

- **Number of days to send a notification before a required password change**

  Specifies the number of days to notify the user before the password expires.

  The default value is 0. This means that the user won't be notified about an expiring password.

- **Number of recent passwords that cannot be set as a new password**

  Specifies the maximum number of previous user passwords that can't be used as a new password. This setting applies only when the user sets a new password on the device.

  The default value is 0. This means that the new user password can match any previous password except the current one.

- **Period of inactivity before the screen locks (sec)**

  Specifies the period of inactivity before the device locks.

  The default value is 0. This means that the device won't lock after a certain period.

- **Period after biometric unlock before password must be entered (min)**

  Specifies the period for unlocking the device without a password. During this period, the user can use biometric methods to unlock the screen. After this period, the user can unlock the screen only with a password.

  The default value is 0. This means that the user won't be forced to unlock the device with a password after a certain period.

- **Allow biometric unlock methods**

  If the check box is selected, the use of biometric unlock methods on the mobile device is allowed.

  If the check box is cleared, Kaspersky Endpoint Security for Android blocks the use of biometric methods to unlock the screen. The user can unlock the screen only with a password.

  This check box is selected by default.

- **Allow fingerprint unlock**

  Specifies whether fingerprints can be used to unlock the screen.

  This check box does not restrict the use of a fingerprint scanner when signing in to apps or confirming purchases.

If the check box is selected, the use of fingerprints on the mobile device is allowed.

If the check box is cleared, Kaspersky Endpoint Security for Android blocks the use of fingerprints to unlock the screen. The user can unlock the screen only with a password. In the device settings, the option to use fingerprints will be unavailable.

This check box is available only if the **Allow biometric unlock methods** check box is selected.

This check box is selected by default.

On some Xiaomi devices with a corporate container, the corporate container may be unlocked by a fingerprint only if you set the **Period of inactivity before corporate container is locked (sec)** value after setting a fingerprint as the screen unlock method.

- **Allow face unlock**

  If the check box is selected, the use of face scanning is allowed on the mobile device.

  If the check box is cleared, Kaspersky Endpoint Security for Android blocks the use of face scanning to unlock the screen.

  This check box is available only if the **Allow biometric unlock methods** check box is selected.

  This check box is selected by default.

- **Allow iris scanning**

  If the check box is selected, the use of iris scanning is allowed on the mobile device.

  If the check box is cleared, Kaspersky Endpoint Security for Android blocks the use of iris scanning to unlock the screen.

  This check box is available only if the **Allow biometric unlock methods** check box is selected.

  This check box is selected by default.

- **Reset to factory settings after failed attempts to enter password**

  Allows limiting the number of attempts to enter the screen unlock password.

  If the check box is selected, the app wipes all device data if the user fails to enter the correct password after the specified number of attempts.

  If the check box is cleared, the number of attempts is not limited.

  The check box is cleared by default.

- **Maximum number of failed password attempts**

  Specifies the number of password entry attempts that the user can make to unlock the device. The default value is 8. The maximum available value is 20.

  The field is available if the **Reset to factory settings after failed attempts to enter password** check box is selected.

- **Set new password**

  This option lets you set the password on the user corporate device.

  Click this button to open the **New screen unlock password** window and enter a new password.

  The complexity of the entered password must comply with requirements configured earlier in the **Screen unlock settings** card of the policy.

Once you save the policy, this option applies to the device by sending a command with the specified password. The input is cleared and the specified password is not saved in Administration Console.

- If the device is not protected with the password or is running Android 10 or earlier, Kaspersky Endpoint Security for Android sets the password immediately.
- If the device is protected with the password or is running Android 11 or later, Kaspersky Endpoint Security for Android prompts the user to apply the new password.

If you leave this option empty, no changes are applied to the device.

7. Click **OK**.
8. Click **Save** to save the changes you have made.

Mobile device settings are changed after the next device synchronization with Kaspersky Security Center.

Setting a new unlock password

To set a new password on a user's corporate device:

1. In the main window of Kaspersky Next Expert View (on-premise), select **Asset management** → **Policies**. In the list of group policies that opens, click the name of the policy that you want to configure.
2. In the policy properties window, select **Application settings**.
3. Select **Android** and go to the **Restrictions** section.
4. On the **New screen unlock password** card, click **Settings**.

   The **New screen unlock password** window opens.
5. Enable the settings using the **New screen unlock password** toggle switch.
6. Enter a new password that will be used to unlock the user's mobile device. This password must comply with current screen unlock password settings.
7. If you want to edit the current unlock password settings, click the **Configure screen unlock settings** button.

   In the **Screen unlock settings** window that opens, configure screen unlock password settings, if required.
8. Click **OK**.

   If the device is not protected with a password or is running Android 10 or earlier, Kaspersky Endpoint Security for Android sets the password immediately. If the device is protected with the password or is running Android 11 or later, Kaspersky Endpoint Security for Android prompts the user to apply the new password.
9. Click **Save** to save the changes you have made.

The new password is set on user's mobile device. Mobile device settings are changed after the next device synchronization with Kaspersky Security Center.

Setting a PIN code on HUAWEI devices

Some HUAWEI devices display a message about screen unlocking method being too simple.

To set an acceptable PIN code on a HUAWEI device, the user must do the following:

1. In the message about the issue, tap the **Edit** button.
2. Enter the current PIN code.
3. In the **Set new password** window, tap the **Change unlock method** button.
4. Select the **Custom PIN** unlock method.
5. Set the new PIN code.

   The PIN code must be compliant with policy requirements.

An acceptable PIN code is set on the device.

Configuring a strong unlock password for an iOS MDM device

These settings apply to supervised devices and devices operating in basic control mode.

To protect iOS MDM device data, configure the unlock password strength settings.

By default, the user can use a simple password. A *simple password* is a password that contains sequential or repeated characters such as "abcd" or "2222". The user is not required to enter an alphanumeric password that includes special symbols. By default, the password validity period and the number of password entry attempts are not limited.

To configure the unlock password strength settings for an iOS MDM device:

1. In the main window of Kaspersky Next Expert View (on-premise), select **Asset management** → **Policies**. In the list of group policies that opens, click the name of the policy that you want to configure.
2. In the policy properties window, select **Application settings**.
3. Select **iOS** and go to the **Security controls** section.
4. On the **Screen unlock settings** card, click **Settings**.

   The **Screen unlock settings** window opens.
5. Enable the settings using the **Screen unlock settings** toggle switch.

   The toggle switch in this card does not enable or disable the corresponding functionality on devices. Enabling the toggle switch lets you configure custom settings. Disabling the toggle switch lets you use default settings.

6. Configure the unlock password strength settings:

- To allow the user to use a simple password, select the **Allow simple password** check box. Even if this check box is cleared, the user can set a password with less than 6 characters.

  If only the **Allow simple password** check box is selected, no password will be requested. To prompt the user to set a password, select both the **Allow simple password** check box and the **Force use of password** check box.

- To require use of both letters and numbers in the password, select the **Prompt for alphanumeric value** check box.

- To require use of a password, select the **Force use of password** check box. If the check box is cleared, the mobile device can be used without a password.

  If the **Prompt for alphanumeric value**, **Minimum password length**, or **Minimum number of special characters** options are enabled, a password is requested even if the **Force use of password** check box is cleared.

- In the **Minimum password length** list, select the minimum password length in characters.

- In the **Minimum number of special characters** list, select the minimum number of special characters in the password (such as "$", "&", "!").

  On some iOS MDM devices, if the **Minimum number of special characters** value is specified and the **Allow simple password** check box is selected, the device displays information about setting a password of 6 or more characters even though it is possible to set a password of 4 or more characters.

- In the **Maximum password lifetime (days)** field, specify the period of time in days during which the password will stay current. When this period expires, the iOS MDM Server prompts the user to change the password.

- In the **Auto-Lock** list, select the amount of time after which Auto-Lock should be enabled on the iOS MDM device. If the mobile device remains idle for this time period, it switches to sleep mode.

  On different iOS MDM devices, the actual time of the device's automatic locking may differ from the value that you have specified:

  On iPhone devices: if you set Auto-Lock in 10 or 15 minutes, the device will be locked in 5 minutes.

  On iPad devices: if you set Auto-Lock in 1 – 4 minutes, the device will be locked in 2 minutes.

  For other values the actual time of the device's automatic locking matches the specified time.

- In the **Reuse of previous passwords** field, specify the number of used passwords (including the current password) that the iOS MDM Server will compare with the new password when the user changes the current password. If the passwords match, the new password is rejected.

- In the **Maximum time for unlock without password** list, select the amount of time during which the user can unlock the iOS MDM device without entering the password.

- In the **Maximum number of failed password attempts** list, select the number of failed password attempts that the system allows the user before it erases the device.

If the value is equal to 6 or lower, the system has no time delay and triggers the erase of all data and settings from an iOS device as soon as the user exceeds the set limit.

If the value is more than 7, then after 6 failed attempts, the device imposes a time delay before the user can enter the unlock password again. The time delay begins after the sixth attempt and increases with each failed attempt. After the final failed attempt, the system erase all data and settings from an iOS device.

By default, the number of password entry attempts is not limited.

If the user exceeds the maximum number of failed password attempts, the device is reset to factory settings.

7. Click **Save** to save the changes you have made.

Mobile device settings are changed after the next device synchronization with the iOS MDM Server.

As a result, once the policy is applied, the iOS MDM Server checks the strength of the password set on the user's mobile device. If the strength of the device unlock password does not comply with the policy, the user is prompted to change the password.

Configuring a virtual private network (VPN)

This section contains information on configuring virtual private network (VPN) settings for secure connection to Wi-Fi networks.

Configuring VPN on Android devices (only Samsung)

To securely connect an Android device to the internet and protect data transfer, you can configure VPN (Virtual Private Network) settings.

Configuration of VPN is possible only for Samsung devices running Android 11 or earlier.

The following requirements must be considered when using a virtual private network:

- The app that uses the VPN connection must be allowed in the **Firewall** settings.
- VPN settings configured in the policy cannot be applied to system apps. The VPN connection for system apps has to be configured manually.
- Some apps that use a VPN connection need to have additional settings configured at first startup. To configure settings, a VPN connection has to be allowed in app settings.

To configure VPN on a user's mobile device:

1. In the main window of Kaspersky Next Expert View (on-premise), select **Asset management** → **Policies**. In the list of group policies that opens, click the name of the policy that you want to configure.
2. In the policy properties window, select **Application settings**.
3. Select **Android** and go to the **Samsung Knox settings** section.
4. On the **VPN** card, click **Settings**.

   The **VPN** window opens.
5. Enable the settings using the **VPN** toggle switch.
6. Specify the following VPN settings:

   - Settings in the **Network** section:
     - In the **Network name** field, enter the name of the VPN tunnel.
     - In the **Protocol** drop-down list, select the VPN connection type:
       - **IPSec Xauth PSK**. A tunneling protocol of the "gateway-to-gateway" type that lets the mobile device user establish a secure connection with the VPN server using the Xauth authentication utility.
       - **L2TP IPSec PSK**. A tunneling protocol of the "gateway-to-gateway" type that lets the mobile device user establish a secure connection with the VPN server via the IKE protocol using a preset key. This protocol is selected by default.
       - **PPTP**. A "point-to-point" tunneling protocol that lets the mobile device user establish a secure connection to the VPN server by creating a special tunnel on a standard unsecured network.
     - In the **Server address** field, enter the network name or IP address of the VPN server.
   - Settings in the **Protocol settings** section:
     - In the **DNS search domain(s)** list, enter the DNS search domain to be automatically added to the DNS server name.

       You can specify several DNS search domains, separating them with blank spaces.
     - In the **DNS server(s)** field, enter the full domain name or IP address of the DNS server.

       You can specify several DNS servers, separating them with blank spaces.
     - In the **Routing** field, enter the range of network IP addresses with which data is exchanged via the VPN connection.

       If a range of IP addresses is not specified in the **Routing** field, all internet traffic will pass through the VPN connection.

7. Additionally, configure the following settings:

   - For the **IPSec Xauth PSK** and **L2TP IPSec PSK** protocols:

     - In the **IPSec shared key** field, enter the password for the preset IPSec security key.

     - In the **IPSec ID** field, enter the name of the mobile device user.

   - For the **L2TP IPSec PSK** protocol, specify the password for the L2TP key in the **L2TP key** field.

   - For the **PPTP** network, select the **Use SSL connection** check box so that the app will use the MPPE (Microsoft Point-to-Point Encryption) method of data encryption to secure data transmission when the mobile device connects to the VPN server.

8. Click **Save** to save the changes you have made.

Mobile device settings are changed after the next device synchronization with Kaspersky Security Center.

Configuring VPN on iOS MDM devices

These settings apply to supervised devices and devices operating in basic control mode.

To connect an iOS MDM device to a virtual private network (VPN) and protect data while connected to the VPN, configure the VPN connection settings. The IKEv2 and IPSec VPN protocols also let you set up a Per App VPN connection.

To configure a VPN connection on a user's iOS MDM device:

1. In the main window of Kaspersky Next Expert View (on-premise), select **Asset management** → **Policies**. In the list of group policies that opens, click the name of the policy that you want to configure.

2. In the policy properties window, select **Application settings**.

3. Select **iOS** and go to the **Device configuration** section.

4. On the **VPN** card, click **Settings**.

   The **VPN** window opens.

5. Enable the settings using the **VPN** toggle switch.

6. Click **Add**.

   The **Add VPN configuration** window opens.

7. On the **General** tab, in the **Network** section, configure the following settings:

   a. In the **Network name** field, enter the name of the VPN tunnel.

   b. In the **Protocol** drop-down list, select the **type of the VPN connection**.

   - **L2TP** (Layer 2 Tunneling Protocol). The connection supports authentication of the iOS MDM device user using MS-CHAP v2 passwords, two-factor authentication, and automatic authentication using a public key.
   - **IKEv2** (Internet Key Exchange version 2). The connection establishes the Security Association (SA) attribute between two network entities and supports authentication using EAP (Extensible Authentication Protocols), shared secrets, and certificates.
   - **IPSec**. The connection supports password-based user authentication, two-factor authentication, and automatic authentication using a public key and certificates.
   - **Cisco AnyConnect**. The connection supports the Cisco Adaptive Security Appliance (ASA) firewall version 8.0(3).1 or later. To configure a VPN connection, install the Cisco AnyConnect app from the App Store on the iOS MDM device.
   - **Juniper SSL**. The connection supports the Juniper Networks SSL VPN gateway, Series SA, version 6.4 or later with the Juniper Networks IVE package version 7.0 or later. To configure a VPN connection, install the JUNOS app from the App Store on the iOS MDM device.
   - **F5 SSL**. The connection supports the F5 BIG-IP Edge Gateway, Access Policy Manager, and Fire SSL VPN solutions. To configure a VPN connection, install the F5 BIG-IP Edge Client app from the App Store on the iOS MDM device.
   - **SonicWALL Mobile Connect**. The connection supports SonicWALL Aventail E-Class Secure Remote Access devices version 10.5.4 or later, SonicWALL SRA devices version 5.5 or later, as well as SonicWALL Next-Generation Firewall devices, including TZ, NSA, and E-Class NSA with SonicOS version 5.8.1.0 or later. To configure a VPN connection, install the SonicWALL Mobile Connect app from the App Store on the iOS MDM device.
   - **Aruba VIA**. The connection supports Aruba Networks mobile access controllers. To configure them, install the Aruba Networks VIA app from the App Store on the iOS MDM device.
   - **Custom SSL**. The connection supports authentication of the iOS MDM device user using passwords and certificates and two-factor authentication.

   c. In the **Server address** field, enter the network name or IP address of the VPN server.

8. Configure the **settings for the VPN connection** according to the selected type of virtual private network.

   - L2TP
     - Settings in the **Authentication** section:
       - **Authentication type**

         Two-factor authentication of an iOS MDM device user using an RSA SecurID token or password-based authentication.

       - **Account name**

         The account name for authorization on the VPN server.

- **Password**

  The password of the account for authentication on the virtual private network.

- **Authentication method**

  The method of authenticating iOS MDM device users on the virtual private network.

- **Shared secret**

  Password for a preset IPSec security key for the L2TP and IPSec (Cisco) protocols.

- **Authentication certificate**

  The certificate used for user authentication.

- Settings in the **Other** section:

  - **Send all traffic via VPN**

    Transmission of all outbound traffic via the VPN connection if a different network service is used (example: AirPort or Ethernet).

    If the check box is selected, all traffic is sent via the VPN connection.

    If the check box is cleared, outbound traffic is transmitted without requiring the use of the VPN connection.

    This check box is cleared by default.

- **IPSec**

  - Settings in the **Authentication** section:

    - **Authentication method**

      The method of authenticating iOS MDM device users on the virtual private network.

    - **Account name**

      The account name for authorization on the VPN server.

    - **Password**

      The password of the account for authentication on the virtual private network.

    - **Shared secret**

      Password for a preset IPSec security key for the L2TP and IPSec (Cisco) protocols.

    - **Group name**

      Name of the group of iOS MDM devices that connect to the VPN via L2TP and IPSec (Cisco) protocols. If the **Use hybrid authentication** check box is selected, the group name must end with " [hybrid]" (for example: "mycompany [hybrid]").

    - **Use hybrid authentication**

      Use of hybrid authentication when the user connects to a VPN. The VPN server uses a certificate for authentication, and the iOS MDM device user enters a public key for authentication via the IPSec (Cisco) protocol.

If the check box is selected, hybrid authentication is used when the user connects to a VPN.

If the check box is cleared, the hybrid authentication is not used.

This check box is cleared by default.

- **Authentication certificate**

  The certificate used for user authentication.

- Settings in the **Domains** section:

  - **Enable VPN when connecting to specified domains**

    The domains for which the VPN connection will be enabled.

- Settings in the **Other** section:

  - **Prompt for PIN**

    The application checks whether the system password is set when the mobile device is turned on.

    If the check box is selected, Kaspersky Mobile Devices Protection and Management checks if the system password is set on the device. If no system password is set on the device, the user has to set it. The password should be set in accordance with the settings configured by the administrator.

    If the check box is cleared, Kaspersky Mobile Devices Protection and Management does not require a system password.

    This check box is cleared by default.

- **IKEv2**

  - Settings in the **Network** section:

    - **Dead peer detection interval**

      The frequency at which the IKEv2 VPN client should run the Dead Peer Detection (DPD) algorithm. The following values are available:

      - **Not selected**. Do not run DPD.
      - **Low**. Run DPD every 30 minutes.
      - **Medium**. Run DPD every 10 minutes.
      - **High**. Run DPD every 1 minute.

      The default value is set to **Medium**.

  - Settings in the **Authentication** section:

    - **Authentication method**

      The method of authenticating iOS MDM device users on the virtual private network.

    - **Local identifier**

      The identifier of the IKEv2 VPN client (iOS MDM device).

    - **Remote identifier**

The identifier of the IKEv2 VPN server.

- **Shared secret**

  The shared secret used for IKEv2 VPN authentication.

- **Common Name (CN) of server certificate**

  This name is used to validate the certificate sent by the IKEv2 VPN server. If this option is not set, the certificate is validated using the remote identifier.

- **Common Name (CN) of server certificate publisher**

  If this option is set, IKEv2 sends a certificate request based on this certificate issuer to the server.

- **Authentication certificate**

  The certificate used for user authentication.

- **EAP authentication**

  The type of EAP authentication used for the VPN IKEv2 connection. The following values are available:

  - **Credentials**
  - **Certificate**

  The default value is **Credentials**.

- **Account name**

  The account name for authorization on the VPN server.

- **Password**

  The password of the account for authentication on the virtual private network.

- **Minimum TLS version**

  The minimum TLS version used for EAP authentication. The following values are available:

  - **TLS 1.0**
  - **TLS 1.1**
  - **TLS 1.2**

  The default value is **TLS 1.0**.

- **Maximum TLS version**

  The maximum TLS version used for EAP authentication. The following values are available:

  - **TLS 1.0**
  - **TLS 1.1**
  - **TLS 1.2**

  The default value is **TLS 1.2**.

- Settings in the **Security association** section:
  - **SA parameters**

    Determines the object in which the parameters are sent. Possible values:
    - **IKEv2**
    - **Child**

    The default value is **IKEv2**.
  - **Encryption algorithm**

    Determines the encryption algorithm used for the connection. Possible values:
    - **DES**
    - **3DES**
    - **AES-128**
    - **AES-256**
    - **AES-128-GCM**
    - **AES-256-GCM**
    - **ChaCha20Poly1305**

    The default value is **AES-256**.
  - **Integrity algorithm**

    Determines the integrity algorithm used for the connection. Possible values:
    - **SHA1-96**
    - **SHA1-160**
    - **SHA2-256**
    - **SHA2-384**
    - **SHA2-512**

    The default value is **SHA2-256**.
  - **Diffie-Hellman group**

    Determines the Diffie-Hellman group used when setting up the VPN tunnel.
    The default value is 14.
  - **SA Lifetime (min)**

    The rekey interval in minutes.
- Settings in the **Other** section:
  - **Disable redirect**

Specifies whether IKEv2 VPN server redirects are disabled.

If the check box is selected, the IKEv2 VPN connection is not redirected.

If the check box is cleared, the IKEv2 VPN connection is redirected if a redirect request is received from the server.

This check box is cleared by default.

- **Disable Mobility and Multi-homing Protocol**

  Specifies whether Mobility and Multi-homing Protocol (MOBIKE) is disabled for the IKEv2 VPN connection.

  If the check box is selected, MOBIKE is disabled

  If the check box is cleared, MOBIKE is enabled.

  This check box is cleared by default.

- **Use internal IPv4 and IPv6 subnet attributes**

  Specifies whether the IKEv2 VPN client should use the INTERNAL_IP4_SUBNET and INTERNAL_IP6_SUBNET configuration attributes sent by the IKEv2 VPN server.

  If the check box is selected, INTERNAL_IP4_SUBNET and INTERNAL_IP6_SUBNET attributes are used.

  If the check box is cleared, INTERNAL_IP4_SUBNET and INTERNAL_IP6_SUBNET attributes are not used.

  This check box is cleared by default.

- **Enable a tunnel over cellular data**

  Specifies whether fallback is enabled.

  If the check box is selected, the device enables a tunnel over cellular data to carry traffic that is eligible for Wi-Fi Assist and also requires a VPN.

  If the check box is cleared, fallback is disabled.

  This check box is cleared by default.

- **Enable Perfect Forward Secrecy**

  Specifies whether Perfect Forward Secrecy (PFS) is enabled for the IKEv2 VPN connection.

  If the check box is selected, PFS is enabled.

  If the check box is cleared, PFS is disabled.

  This check box is cleared by default.

- **Cisco AnyConnect**

  - Settings in the **Network** section:

    - **Idle time before disconnection (min)**

      The time to wait before disconnecting an on-demand connection.

  - Settings in the **Authentication** section:

    - **Authentication method**

      The method of authenticating iOS MDM device users on the virtual private network.

- **Account name**

  The account name for authorization on the VPN server.

- **Password**

  The password of the account for authentication on the virtual private network.

- **Group**

  Alias of the tunneling group for Cisco AnyConnect clients connecting to the VPN.

- **Authentication certificate**

  The certificate used for user authentication.

- Settings in the **Domains** section:

  - **Enable VPN when connecting to specified domains**

    The domains for which the VPN connection will be enabled.

- Settings in the **Other** section:

  - **Send all traffic via VPN**

    Routes all traffic via the VPN.

  - **Exclude local traffic**

    Excludes local traffic from traffic routed via the VPN connection.
    This check box is available if the **Send all traffic via VPN** check box is selected.

- **Juniper SSL**

  - Settings in the **Network** section:

    - **Idle time before disconnection (min)**

      The time to wait before disconnecting an on-demand connection.

  - Settings in the **Authentication** section:

    - **Authentication method**

      The method of authenticating iOS MDM device users on the virtual private network.

    - **Account name**

      The account name for authorization on the VPN server.

    - **Password**

      The password of the account for authentication on the virtual private network.

    - **Scope**

      Name of the network that includes VPN servers and iOS MDM devices for the VPN connection established using Juniper SSL.

- **Role**

  Name of the user role that grants the user access to resources using Juniper SSL. A role can combine several users performing similar functions.

- **Authentication certificate**

  The certificate used for user authentication.

- Settings in the **Domains** section:

  - **Enable VPN when connecting to specified domains**

    The domains for which the VPN connection will be enabled.

- Settings in the **Other** section:

  - **Send all traffic via VPN**

    Routes all traffic via the VPN.

  - **Exclude local traffic**

    Excludes local traffic from traffic routed via the VPN connection.
    This check box is available if the **Send all traffic via VPN** check box is selected.

- **F5 SSL**

  - Settings in the **Network** section:

    - **Idle time before disconnection (min)**

      The time to wait before disconnecting an on-demand connection.

  - Settings in the **Authentication** section:

    - **Authentication method**

      The method of authenticating iOS MDM device users on the virtual private network.

    - **Account name**

      The account name for authorization on the VPN server.

    - **Password**

      The password of the account for authentication on the virtual private network.

    - **Authentication certificate**

      The certificate used for user authentication.

  - Settings in the **Domains** section:

    - **Enable VPN when connecting to specified domains**

      The domains for which the VPN connection will be enabled.

- Settings in the **Other** section:
  - **Send all traffic via VPN**

    Routes all traffic via the VPN.
  - **Exclude local traffic**

    Excludes local traffic from traffic routed via the VPN connection.
    This check box is available if the **Send all traffic via VPN** check box is selected.

- **SonicWALL Mobile Connect**
  - Settings in the **Network** section:
    - **Idle time before disconnection (min)**

      The time to wait before disconnecting an on-demand connection.
  - Settings in the **Authentication** section:
    - **Authentication method**

      The method of authenticating iOS MDM device users on the virtual private network.
    - **Account name**

      The account name for authorization on the VPN server.
    - **Password**

      The password of the account for authentication on the virtual private network.
    - **Domain or group**

      Domain name of the SSL VPN server (example: vpn.company.com) or the name of a group of SonicWALL Mobile Connect users.
    - **Authentication certificate**

      The certificate used for user authentication.
  - Settings in the **Domains** section:
    - **Enable VPN when connecting to specified domains**

      The domains for which the VPN connection will be enabled.
  - Settings in the **Other** section:
    - **Send all traffic via VPN**

      Routes all traffic via the VPN.
    - **Exclude local traffic**

      Excludes local traffic from traffic routed via the VPN connection.
      This check box is available if the **Send all traffic via VPN** check box is selected.

- **Aruba VIA**
  - Settings in the **Network** section:
    - **Idle time before disconnection (min)**

      The time to wait before disconnecting an on-demand connection.
  - Settings in the **Authentication** section:
    - **Authentication method**

      The method of authenticating iOS MDM device users on the virtual private network.
    - **Account name**

      The account name for authorization on the VPN server.
    - **Password**

      The password of the account for authentication on the virtual private network.
    - **Authentication certificate**

      The certificate used for user authentication.
  - Settings in the **Domains** section:
    - **Enable VPN when connecting to specified domains**

      The domains for which the VPN connection will be enabled.
  - Settings in the **Other** section:
    - **Send all traffic via VPN**

      Routes all traffic via the VPN.
    - **Exclude local traffic**

      Excludes local traffic from traffic routed via the VPN connection.
      This check box is available if the **Send all traffic via VPN** check box is selected.
- **Custom SSL**
  - Settings in the **Network** section:
    - **Idle time before disconnection (min)**

      The time to wait before disconnecting an on-demand connection.
  - Settings in the **Configuration data** section:
    - **Key**

      Contains a key with additional settings for the Custom SSL connection.
    - **Value**

Contains a value with additional settings for the Custom SSL connection.

- Settings in the **Authentication** section:
  - **Authentication method**

    The method of authenticating iOS MDM device users on the virtual private network.

  - **Account name**

    The account name for authorization on the VPN server.

  - **Password**

    The password of the account for authentication on the virtual private network.

  - **Authentication certificate**

    The certificate used for user authentication.

  - **Bundle ID**

    If the custom VPN configuration targets a VPN solution that uses a network extension provider, then this field contains the bundle identifier of the app that contains the provider. Contact the VPN solution vendor for the value of the identifier.

- Settings in the **Domains** section:
  - **Enable VPN when connecting to specified domains**

    The domains for which the VPN connection will be enabled.

9. If necessary, on the **Additional** tab, in the **Proxy server** section, configure the settings of the VPN connection via a proxy server:

   a. Select the **Use a proxy server** check box.

   b. Configure a connection to a proxy server:

      a. If you want to configure the connection automatically:

      - Select **Automatic**.
      - In the **PAC file URL** field, specify the URL of the proxy PAC file.
      - To allow the user to connect the mobile device to a wireless network without using a proxy server when the PAC file cannot be accessed, select the **Allow direct connection if PAC file cannot be accessed** check box.

b. If you want to configure the connection manually:

- Select **Manual**.
- In the **Proxy server address** and **Proxy server port** fields, enter the IP address or DNS name of the proxy server and port number.
- In the **User name** field, select a macro that will be used as a user name for the connection to the proxy server.

c. In the **Password** field, specify the password for the connection to the proxy server.

10. For **IKEv2** and **IPSec** connections, if necessary, set up Per App VPN functionality for supported system apps (Mail, Calendar, Contacts, and Safari) or for third-party apps.

11. Click **Add**.

    The new VPN is displayed in the list.

    You can modify or delete VPN in the list using the **Edit** and **Delete** buttons at the top of the list.

12. Click **Save** to save the changes you have made.

Mobile device settings are changed after the next device synchronization with the iOS MDM Server.

As a result, once the policy is applied, the VPN connection will be configured on the user's iOS MDM device.

Configuring Per App VPN for iOS system apps

These settings apply to supervised devices and devices operating in basic control mode.

The Per App VPN functionality lets a device establish a VPN connection when supported system apps or third-party apps are launched. This functionality is available for IKEv2 and IPSec connections.

The following system apps support Per App VPN connections:

- Mail
- Calendar
- Contacts
- Safari
- Messages

For the Per App VPN functionality to work correctly, the iOS MDM Server version must not be earlier than 15.4.0.2019.

To enable the Per App VPN functionality for supported system apps:

1. Perform the initial setup of the VPN connection.
2. On the **Additional** tab, in the **Per App VPN** section, select the **Enable Per App VPN** check box.
3. Set up Per App VPN for supported system apps in the corresponding settings of the policy.

Mail

To specify the Per App VPN configuration for the Mail app:

1. In the main window of Kaspersky Next Expert View (on-premise), select **Asset management** → **Policies**. In the list of group policies that opens, click the name of the policy that you want to configure.
2. In the policy properties window, select **Application settings**.
3. Select **iOS** and go to the **Device configuration** section.
4. On the **Email** card, click **Settings**.

   The **Email** window opens.
5. Enable the settings using the **Email** toggle switch.
6. Add a new email account or edit an existing account.
7. On the **Additional** tab, in the **Per App VPN** section, select the **Enable Per App VPN** check box.
8. Select a configuration from the **Per App VPN configuration** drop-down list.
9. Click **Save**.
10. Click **OK**.
11. Click **Save** to save the changes you have made.

Mobile device settings are changed after the next device synchronization with the iOS MDM Server.

As a result, once the policy is applied, Per App VPN is configured for the Mail app.

Calendar

To specify the Per App VPN configuration for the Calendar app:

1. In the main window of Kaspersky Next Expert View (on-premise), select **Asset management** → **Policies**. In the list of group policies that opens, click the name of the policy that you want to configure.
2. In the policy properties window, select **Application settings**.
3. Select **iOS** and go to the **Device configuration** section.
4. On the **Calendar** card, click **Settings**.

   The **Calendar** window opens.

5. Enable the settings using the **Calendar** toggle switch.
6. Add a new calendar account or edit an existing account.
7. In the **Per App VPN** section, select the **Enable Per App VPN** check box.
8. Select a configuration from the **Per App VPN configuration** drop-down list.
9. Click **Add**.
10. Click **OK**.
11. Click **Save** to save the changes you have made.

Mobile device settings are changed after the next device synchronization with the iOS MDM Server.

As a result, once the policy is applied, Per App VPN is configured for the Calendar app.

Calendar subscriptions

A list of subscriptions to calendars of other CalDAV users, iCal calendars, and other published calendars.

To specify the Per App VPN configuration for calendar subscriptions:

1. In the main window of Kaspersky Next Expert View (on-premise), select **Asset management** → **Policies**. In the list of group policies that opens, click the name of the policy that you want to configure.
2. In the policy properties window, select **Application settings**.
3. Select **iOS** and go to the **Device configuration** section.
4. On the **Calendar subscriptions** card, click **Settings**.

   The **Calendar subscriptions** window opens.
5. Enable the settings using the **Calendar subscriptions** toggle switch.
6. Add a new calendar subscription or edit an existing subscription.
7. In the **Per App VPN** section, select the **Enable Per App VPN** check box.
8. Select a configuration from the **Per App VPN configuration** drop-down list.
9. Click **Add**.
10. Click **OK**.
11. Click **Save** to save the changes you have made.

Mobile device settings are changed after the next device synchronization with the iOS MDM Server.

As a result, once the policy is applied, Per App VPN is configured for calendar subscriptions.

Contacts

To specify the Per App VPN configuration for the Contacts app:

1. In the main window of Kaspersky Next Expert View (on-premise), select **Asset management** → **Policies**. In the list of group policies that opens, click the name of the policy that you want to configure.
2. In the policy properties window, select **Application settings**.
3. Select **iOS** and go to the **Device configuration** section.
4. On the **Contacts** card, click **Settings**.

   The **Contacts** window opens.
5. Enable the settings using the **Contacts** toggle switch.
6. Add a new contacts account or edit an existing account.
7. In the **Per App VPN** section, select the **Enable Per App VPN** check box.
8. Select a configuration from the **Per App VPN configuration** drop-down list.
9. Click **Add**.
10. Click **OK**.
11. Click **Save** to save the changes you have made.

Mobile device settings are changed after the next device synchronization with the iOS MDM Server.

As a result, once the policy is applied, Per App VPN is configured for the Contacts app.

Safari

To specify the Per App VPN configuration for Safari:

1. In the main window of Kaspersky Next Expert View (on-premise), select **Asset management** → **Policies**. In the list of group policies that opens, click the name of the policy that you want to configure.
2. In the policy properties window, select **Application settings**.
3. Select **iOS** and go to the **Device configuration** section.
4. On the **Per App VPN for Safari** card, click **Settings**.

   The **Per App VPN for Safari** window opens.
5. Enable the settings using the **Per App VPN for Safari** toggle switch.
6. Click **Add**.

   The **Add a website domain** window opens.
7. Select a configuration from the **Per App VPN configuration** drop-down list.

8. In the **Domain name** field, specify the website domain that will trigger the VPN connection in Safari. The domain must be in the `www.example.com` format.

9. Click **Add**.

   The new domain appears in the **Safari website domains** list.

   > You can modify or delete Safari website domains in the list using the **Edit** and **Delete** buttons at the top of the list.

10. Click **OK**.

11. Click **Save** to save the changes you have made.

Mobile device settings are changed after the next device synchronization with the iOS MDM Server.

As a result, once the policy is applied, Per App VPN is configured for Safari website domains.

LDAP

An LDAP account provides access to corporate data and contacts in the standard iOS apps: Contacts, Messages, and Mail.

To specify the Per App VPN configuration for an LDAP account:

1. In the main window of Kaspersky Next Expert View (on-premise), select **Asset management** → **Policies**. In the list of group policies that opens, click the name of the policy that you want to configure.

2. In the policy properties window, select **Application settings**.

3. Select **iOS** and go to the **Device configuration** section.

4. On the **LDAP** card, click **Settings**.

   The **LDAP** window opens.

5. Enable the settings using the **LDAP** toggle switch.

6. Add a new LDAP account or edit an existing account.

7. In the **Per App VPN** section, select the **Enable Per App VPN** check box.

8. Select a configuration from the **Per App VPN configuration** drop-down list.

9. Click **Add**.

10. Click **OK**.

11. Click **Save** to save the changes you have made.

Mobile device settings are changed after the next device synchronization with the iOS MDM Server.

As a result, once the policy is applied, Per App VPN is configured for the LDAP account.

Exchange ActiveSync

An Exchange ActiveSync account lets you synchronize corporate email, calendar, contacts, notes, and tasks from the Microsoft Exchange server.

To specify the Per App VPN configuration for an Exchange ActiveSync account:

1. In the main window of Kaspersky Next Expert View (on-premise), select **Asset management** → **Policies**. In the list of group policies that opens, click the name of the policy that you want to configure.
2. In the policy properties window, select **Application settings**.
3. Select **iOS** and go to the **Device configuration** section.
4. On the **Exchange ActiveSync** card, click **Settings**.
   The **Exchange ActiveSync** window opens.
5. Enable the settings using the **Exchange ActiveSync** toggle switch.
6. Add a new Exchange ActiveSync account or edit an existing account.
7. On the **Additional** tab, in the **Per App VPN** section, select the **Enable Per App VPN** check box.
8. Select a configuration from the **Per App VPN configuration** drop-down list.
9. Click **Add**.
10. Click **OK**.
11. Click **Save** to save the changes you have made.

Mobile device settings are changed after the next device synchronization with the iOS MDM Server.

As a result, once the policy is applied, Per App VPN is configured for the Exchange ActiveSync account.

Configuring Per App VPN for third-party iOS apps

These settings apply to supervised devices and devices operating in basic control mode.

The Per App VPN functionality lets a device establish a VPN connection when supported system apps or third-party apps are launched. This functionality is available for IKEv2 and IPSec connections.

For the Per App VPN functionality to work correctly, the iOS MDM Server version must not be earlier than 15.4.0.2019.

To configure Per App VPN for a third-party app:

1. In the main window of Kaspersky Next Expert View (on-premise), select **Asset management** → **Policies**. In the list of group policies that opens, click the name of the policy that you want to configure.
2. In the policy properties window, select **Application settings**.
3. Select **iOS** and go to the **Device configuration** section.
4. On the **VPN** card, click **Settings**.

   The **VPN** window opens.
5. Set up a VPN connection with the **IKEv2** or **IPSec** protocol.
6. On the **Additional** tab, in the **Per App VPN** section, select the **Enable Per App VPN** check box.
7. Select the Per App VPN configuration alias that you want to apply to this VPN configuration.

   The alias lets you use the corresponding VPN configuration for an installation package of a third-party app.

   > If a Per App VPN configuration alias is not selected, Per App VPN is still available for system apps.

   > If you change the previously selected Per App VPN configuration alias, VPN will be disabled for all third-party apps using this configuration after they are reinstalled or updated.
8. Click **Add**.

   The new VPN configuration that supports Per App VPN functionality is displayed in the list.
9. Click **Save** to save the changes you have made.
10. To set up Per App VPN for the required third-party app, do one of the following:

    - **Specify a Per App VPN configuration alias for a new third-party app**

      1. In the main window of Kaspersky Next Expert View (on-premise), select **Asset management** → **Mobile** → **Apps & files** → **iOS**.
      2. Click **Add**.

         The **Add app** window opens.
      3. Configure an app.
      4. In the **Per App VPN** section, click **Enable Per App VPN** and select the alias of the VPN configuration that you want to enable while using this app.

         The configured settings will be applied after the app is installed.
      5. Click **Add**.

      The new managed app for which Per App VPN has been configured appears in the list.

- **Specify a Per App VPN configuration alias for an already installed third-party app**

  1. In the main window of Kaspersky Next Expert View (on-premise), select **Asset management** → **Mobile** → **Apps & files** → **iOS**.

  2. Click the name of the app in the list for which you want to configure Per App VPN.

     The **App details** window opens.

  3. In the **Per App VPN** section, click **Enable Per App VPN** and select the alias of the VPN configuration that you want to enable while using this app.

     The configured settings will be applied after the app is reinstalled or updated.

  4. Click **OK**.

  The specified Per App VPN configuration alias for this managed app appears in the corresponding table column.

Mobile device settings are changed after the next device synchronization with the iOS MDM Server.

After the required third-party app is installed, the Per App VPN will be configured for this app.

Configuring Firewall on Android devices (only Samsung)

Configure Firewall settings to monitor network connections on the user's mobile device.

Firewall can be configured only for Samsung devices operating in the following modes:

- corporate device
- personal device running Android 15 or earlier
- device with corporate container running Android 15 or earlier

To configure Firewall on a user's mobile device:

1. In the main window of Kaspersky Next Expert View (on-premise), select **Asset management** → **Policies**. In the list of group policies that opens, click the name of the policy that you want to configure.
2. In the policy properties window, select **Application settings**.
3. Select **Android** and go to the **Samsung Knox settings** section.
4. On the **Firewall** card, click **Settings**.

   The **Firewall** window opens.
5. Enable the settings using the **Firewall** toggle switch.

6. In the **Internet access** drop-down list, select the Firewall mode. Depending on its operating mode, Firewall monitors connections established by the user's mobile device:

   - If you want to allow inbound and outbound connections of all installed apps, select **Allow for all apps**. This mode is selected by default.
   - If you want to block all network activity except for several specified apps, select **Allow for listed apps**.

7. If you selected **Allow for listed apps** as the Firewall mode, create a list of apps for which all network activity is allowed:

   a. In the **Apps with internet access** section, click **Add**.

   The **Add app** window opens.

   b. In the **App name** field, enter the name of the mobile app.

   c. In the **Package name** field, enter the system name of the mobile app package (for example, `com.mobileapp.example`).

   d. Click **Add**.

   The new app for which Firewall is disabled appears in the list.

   > You can modify or delete mobile apps in the list using the **Edit** and **Delete** buttons at the top of the list.

8. Click **OK**.

9. Click **Save** to save the changes you have made.

Mobile device settings are changed after the next device synchronization with Kaspersky Security Center.

Protecting Kaspersky Endpoint Security for Android against removal

To protect mobile devices and comply with corporate security requirements, you can enable protection against removal of Kaspersky Endpoint Security for Android. In this case, the user cannot remove the app using the Kaspersky Endpoint Security for Android interface. When removing the app using Android operating system tools, you are prompted to disable administrator rights for Kaspersky Endpoint Security for Android. After disabling the rights, the mobile device will be locked.

> On certain Samsung devices running Android 7 or later, when the user attempts to configure unsupported methods for unlocking the device (for example, a graphical password), the device may be locked if the following conditions are met: removal protection is enabled for Kaspersky Endpoint Security for Android and strength requirements are set for the screen unlock password. To unlock the device, you must send a special command to the device.

To protect the app from removal on devices running Android 7 or later, Kaspersky Endpoint Security for Android must be set as an Accessibility feature. When the Initial Configuration Wizard is running, Kaspersky Endpoint Security for Android prompts the user to grant the application all required permissions. The user can skip these steps or later disable these permissions in the device settings. If this is the case, the app is not protected from removal.

To enable protection against removal of Kaspersky Endpoint Security for Android:

1. In the main window of Kaspersky Next Expert View (on-premise), select **Asset management** → **Policies**. In the list of group policies that opens, click the name of the policy that you want to configure.
2. In the policy properties window, select **Application settings**.
3. Select **Android** and go to the **KES for Android settings** section.
4. On the **Configure access to app settings** card, click **Settings**.

   The **Configure access to app settings** window opens.
5. Enable the settings using the **Configure access to app settings** toggle switch.

   > The toggle switch in this card does not enable or disable the corresponding functionality on devices. Enabling the toggle switch lets you configure custom settings. Disabling the toggle switch lets you use default settings.
6. Clear the **Allow removing the app from device** check box.
7. Click **OK**.
8. Click **Save** to save the changes you have made.

Mobile device settings are changed after the next device synchronization with Kaspersky Security Center. If an attempt is made to remove the app, the mobile device will be locked.

Detecting hacked devices

Kaspersky Next Expert View (on-premise) lets you detect hacked (rooted) Android devices and jailbreaking on iOS devices. System files are unprotected on a hacked device and can therefore be modified. If a hack attempt is detected, we recommend that you immediately restore normal operation of the device.

If a device is hacked, you receive a notification. You can view hacking notifications in Kaspersky Next Expert View (on-premise) in the **Monitoring** → **Dashboard** section. You can also disable notifications about hacks in the event notification settings.

On Android devices, you can impose restrictions on the user's activity if the device is hacked (for example, lock the device). You can impose restrictions using the Compliance Control component. To do this, create a compliance rule with the **Device has been rooted** criterion.

Configuring a global HTTP proxy on iOS MDM devices

> These settings apply to supervised devices.

To route the user's internet traffic, configure the iOS MDM device connect to the internet through a proxy server.

Be careful when configuring these settings. If the settings are incorrect, devices may lose their internet connection and will not synchronize with the iOS MDM Server. If this happens, you will have to add the devices again.

To configure global HTTP proxy settings on the user's iOS MDM device:

1. In the main window of Kaspersky Next Expert View (on-premise), select **Asset management** → **Policies**. In the list of group policies that opens, click the name of the policy that you want to configure.
2. In the policy properties window, select **Application settings**.
3. Select **iOS** and go to the **Device configuration** section.
4. On the **Global HTTP proxy** card, click **Settings**.
   The **Global HTTP proxy** window opens.
5. Enable the settings using the **Global HTTP proxy** toggle switch.
6. Select the type of global HTTP proxy configuration:
   - To specify the proxy server connection settings manually:
     a. In the **Setting type** section, select **Manual**.
     b. In the **Proxy server address** and **Proxy server port** fields, enter the name of a host or the IP address of a proxy server and the number of the proxy server port.
     c. In the **User name** field, set the user account name for authorization on the proxy server.
     d. In the **Password** field, set the user account password for authorization on the proxy server.
     e. To allow the user to access captive networks, select the **Allow access to captive networks without connecting to proxy** check box.
   - To configure the proxy server connection settings using a predefined PAC (Proxy Auto Configuration) file:
     a. In the **Setting type** section, select **Automatic**.
     b. In the **PAC file URL** field, enter the web address of the PAC file (for example: `http://www.example.com/filename.pac`).
     c. To allow the user to connect the mobile device to a wireless network without using a proxy server when the PAC file cannot be accessed, select the **Allow direct connection if PAC file cannot be accessed** check box.
     d. To allow the user to access captive networks, select the **Allow access to captive networks without connecting to proxy** check box.

7. Click **OK**.

8. Click **Save** to save the changes you have made.

As a result, the mobile device user will connect to the internet via a proxy server after the policy is applied.

Adding security certificates to iOS MDM devices

These settings apply to supervised devices and devices operating in basic control mode.

You can add certificates to iOS MDM devices to simplify user authentication and ensure data security. The data signed with a certificate is protected against modification while it is transferred over the network. Data encryption using a certificate provides an added level of security for the data. The certificate can also be used to verify user identity.

Kaspersky Mobile Devices Protection and Management supports the following certificate standards:

- **PKCS#1**. Encryption with a public key based on RSA algorithms.
- **PKCS#12**. Storage and transmission of a certificate and a private key.

To add a security certificate to iOS MDM devices:

1. In the main window of Kaspersky Next Expert View (on-premise), select **Asset management** → **Policies**. In the list of group policies that opens, click the name of the policy that you want to configure.

2. In the policy properties window, select **Application settings**.

3. Select **iOS** and go to the **Device configuration** section.

4. On the **Certificate management** card, click **Settings**.
   The **Certificate management** window opens.

5. Enable the settings using the **Certificate management** toggle switch.

6. Click **Upload** and specify the path to the certificate.

   Files of PKCS#1 certificates have the CER, DER, or PEM extension. Files of PKCS#12 certificates have the P12 or PFX extension. The password for a PKCS#12 certificate must not me empty.

7. Click **Open**.
   If the certificate is password-protected, enter the password. The new certificate appears in the list.

8. Click **OK**.

9. Click **Save** to save the changes you have made.

Mobile device settings are changed after the next device synchronization with the iOS MDM Server.

As a result, once the policy is applied, certificates are automatically installed on devices.

Adding a SCEP profile to iOS MDM devices

These settings apply to supervised devices and devices operating in basic control mode.

You have to add a SCEP profile to enable the iOS MDM device user to automatically receive certificates from the Certification Center via the internet. The SCEP profile enables support of the Simple Certificate Enrollment Protocol.

A SCEP profile with the following settings is added by default:

- The alternative subject name is not used for registering certificates.
- Three attempts are made at 10-second intervals to poll the SCEP server. If all attempts to sign the certificate fail, you have to generate a new certificate signing request.
- The received certificate cannot be used for data signing or encryption.

You can edit the specified settings when adding the SCEP profile.

To add a SCEP profile:

1. In the main window of Kaspersky Next Expert View (on-premise), select **Asset management** → **Policies**. In the list of group policies that opens, click the name of the policy that you want to configure.
2. In the policy properties window, select **Application settings**.
3. Select **iOS** and go to the **Device configuration** section.
4. On the **SCEP** card, click **Settings**.

   The **SCEP** window opens.
5. Enable the settings using the **SCEP** toggle switch.
6. Click **Add**.

   The **Add SCEP profile** window opens.
7. In the **SCEP Server** section, specify the following SCEP server settings:

   - In the **Configuration name** field, specify the name of the Certification Center deployed on the SCEP server. The Certification Center supplies the user of an iOS MDM device with certificates using the Simple Certificate Enrollment Protocol (SCEP).
   - In the **Server URL** field, enter the web address of the SCEP server on which the Certification Center is deployed.

     The URL can contain the IP address or the full domain name (FQDN). For example, `http://10.10.10.10/certserver/companyscep`.
   - In the **Maximum number of polling attempts** field, specify the maximum number of attempts to poll the SCEP server to get the certificate signed. By default, the value is 3 attempts.

     If all attempts to sign the certificate fail, you have to generate a new certificate signing request.

- In the **Polling interval (sec)** field, specify the number of seconds between attempts to poll the SCEP server to get the certificate signed. By default, the value is 10 seconds.

- In the **Static challenge phrase** field, enter a pre-published registration key.

  Before signing a certificate, the SCEP server prompts the mobile device user to enter the key. If this field is left blank, the SCEP does not request the key.

- In the **Method for uploading certificate thumbprint** drop-down list, select how to add a certificate thumbprint. You can use certificate thumbprints based on the SHA-1 or MD5 hashing algorithm.

  - If you selected the **Manually** option, in the **Certificate thumbprint** field that appears, enter a unique certificate thumbprint for verifying the authenticity of the response from the Certification Center.

  - If you selected the **From file** option, upload a CER, KEY, or PEM file. The thumbprint will be generated and added automatically.

  The certificate thumbprint has to be specified if data exchange between the mobile device and the Certification Center takes place via the HTTP protocol.

8. In the **Subject** section, specify the following settings:

- In the **Subject Name** field, enter a string with the attributes of the iOS MDM device user that are contained in the X.500 certificate.

  Attributes can contain details of the country (C), locality (L), state (ST), organization (O), organization unit (OU), and common user name (CN). For example, `/C=RU/O=MyCompany/CN=User/`.

  You can also use other attributes specified in RFC 5280.

  Attributes are used by DNS services to validate the certificate issued by the Authentication Authority at the user's request.

- Click the **Add Subject Alternative Name** button to add a field for specifying the subject alternative name:

  - In the **Type of Subject Alternative Name** drop-down list that appears, select the type of subject alternative name for the SCEP server. You can add only one alternative name of each type.

    You can use a subject alternative name to identify the user of the iOS MDM device. By default, identification based on the alternative name is not used.

    - **DNS name**. Identification using the domain name.

    - **NT Principal Name**. DNS name of the iOS MDM device user on the Windows NT network. The NT subject name is contained in the certificate request sent to the SCEP server. You can also use the name of the NT subject to identify the user of the iOS MDM device.

    - **Email address**. Identification using the email address. The email address must be specified according to RFC 822.

    - **Uniform Resource Identifier (URI)**. Identification using the IP address or address in FQDN format.

  - In the **Subject Alternative Name** field, enter the alternative name of the subject of the X.500 certificate. The value of the subject alternative name depends on the selected subject type: the user's email address, domain, or web address.

9. In the **Key** section, configure the encryption key settings:

   - In the **Key size (bit)** drop-down list, select the size of the registration key in bits: 1024, 2048, or 4096. The default value is 1024 bits.
   - If you want to allow the user to use a certificate received from the SCEP server as a signing certificate, select the **Use as digital signature** check box.

     Data signing protects data against modification. For example, Safari can validate the authenticity of the certificate and establish a safe data exchange session.
   - If you want to allow the user to use a certificate received from the SCEP server for data encryption, select the **Use for encryption** check box.

     Data encryption also protects confidential data during data exchange over a network. For example, Safari can establish a secure data exchange session using encryption. This guarantees website authenticity and confirms that the connection to the website is encrypted to prevent interception of personal and confidential data.

     You cannot simultaneously use the SCEP server certificate as a data signing certificate and a data encryption certificate.
   - If you want to allow all installed apps to access the private key from the SCEP server certificate, select the **Allow all apps to access private key** check box.
   - If you do not want the private key to be exported from the keychain, select the **Prohibit exporting private key from the Keychain** check box.

10. Click **Add**.

    The new SCEP profile appears in the list.

    You can modify or delete SCEP profiles in the list using the **Edit** and **Delete** buttons at the top of the list.

11. Click **OK**.

12. Click **Save** to save the changes you have made.

Mobile device settings are changed after the next device synchronization with the iOS MDM Server.

As a result, once the policy is applied, the user's mobile device is configured to automatically receive a certificate from the Certification Center via the internet.

Restricting SD card usage (only Samsung)

Configure SD card restrictions to control usage of SD cards on the user's Samsung device that supports Knox.

To restrict SD card usage on a mobile device:

1. In the main window of Kaspersky Next Expert View (on-premise), select **Asset management** → **Policies**. In the list of group policies that opens, click the name of the policy that you want to configure.
2. In the policy properties window, select **Application settings**.

3. Select **Android** and go to the **Samsung Knox settings** section.

4. On the **Device feature restrictions** card, click **Settings**.

   The **Device feature restrictions** window opens.

5. Enable the settings using the **Device feature restrictions** toggle switch.

6. In the **SD card settings** section, specify the required restrictions:

   - **Prohibit access to SD card**

     This setting applies to devices with Android 5-12.

     Selecting or clearing this check box specifies whether access to the SD card is disabled or enabled on the device.

     This check box is cleared by default.

   - **Prohibit writing to SD card**

     Selecting or clearing this check box specifies whether writing to the SD card is disabled or enabled on the device.

     This check box is cleared by default.

   - **Prohibit moving apps to SD card**

     Selecting or clearing this check box specifies whether the device user is allowed to move apps to the SD card.

     This check box is cleared by default.

7. In the **Additional settings** section, you can specify any additional restrictions:

   - **Prohibit sending crash reports to Google**

     This setting applies to devices running Android 11 or earlier.

     If the check box is selected, Kaspersky Endpoint Security for Android blocks sending crash reports to Google.

     If the check box is cleared, sending reports is allowed.

     This check box is cleared by default.

   - **Prohibit developer mode**

     This setting applies to devices running Android 11 or earlier.

     If the check box is selected, the device user is not allowed to enable developer mode on the device.

     If the check box is cleared, the user is allowed to enable developer mode on the device.

     This check box is cleared by default.

8. Click **OK**.

9. Click **Save** to save the changes you have made.

Mobile device settings are changed after the next device synchronization with Kaspersky Security Center. SD card settings are now configured.

Management of mobile devices

This section contains information about how to remotely manage mobile devices in Kaspersky Next Expert View (on-premise).

Remote access to Android devices

Kaspersky Next Expert View (on-premise) lets you establish a remote connection to Android devices through the Kaspersky Endpoint Security for Android app installed on the device. Once you start a remote control session, you can view the device screen, take screenshots, and perform actions on the device.

Establishing a remote connection proceeds in stages:

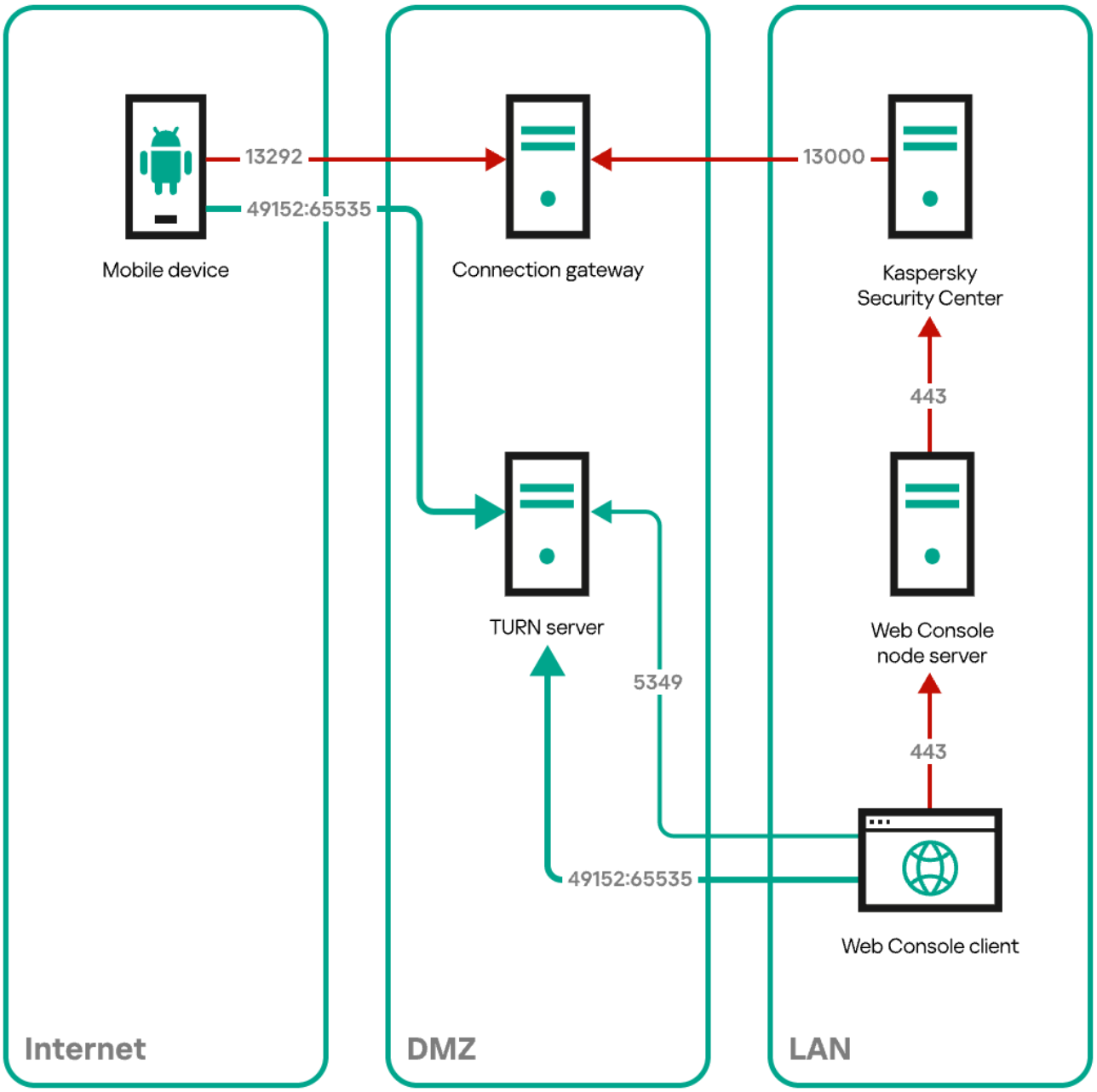
1. Install and configure a TURN server
2. Specify remote control server settings in Kaspersky Security Center
3. Start a remote control session

Installing and configuring a TURN server

Remote connection overview

Remote access to an Android device entails establishing a connection using *WebRTC (Web Real-Time Communication)*, a data streaming technology that enables peer-to-peer connections between two browsers or mobile apps. Data transmission using WebRTC is carried out through a *TURN (Traversal Using Relays around NAT) server*, which acts as an intermediary and relays traffic between connection participants.

The remote connection process is shown in the figure below.



The TURN server must be accessible for both the browser from which you connect to the device and the mobile device itself. If the browser is in the local network and the mobile device is in the internet, the TURN server can be placed in the DMZ. The information for establishing the connection is transmitted to the device via the mobile protocol. To establish a connection, you need to configure a port range on the TURN server. Two ports are used per connection.

A TURN server performs the following functions:

- Establish a connection

  A TURN server enables the ICE (Interactive Connectivity Establishment) candidate exchange process for defining the optimal connection path between Kaspersky Next Expert View (on-premise) and the mobile device. Upon request from the device, the TURN server returns an ICE candidate, a potential network route (port 5349 in the figure above) that can be used for establishing a connection.

- Transmit video data

  A TURN server acts as a tunnel that accepts connections from Kaspersky Security Center and the mobile device. Both peers send their media streams to the TURN server, which then relays the data to the other peer and ensures media transfer.

Install and configure a TURN Server

1 Install a TURN server

System requirements for the TURN server:

- 2 CPU or vCPU
- 4 GB RAM
- 15 GB HDD
- 512 KB/s per active connection

We recommend using the *coturn* server, which is one of the TURN server implementations. It can be installed from the GitHub repository or your operating system's package manager. The example below applies to coturn version 4.5.2.

The instructions below describe how to install coturn using Ubuntu as an example:

1. Install the coturn package on the DMZ server using the following commands:
   ```
   sudo apt-get update
   sudo apt install coturn
   ```
2. After the installation is successfully completed, check the status of the running coturn service:
   ```
   systemctl status coturn.service
   ```
3. Add the coturn service to startup:
   ```
   sudo systemctl enable coturn
   ```

2 Configure the TURN server

1. Specify the required parameters in the TURN server configuration file using a text editor, for example, *Vim* or *nano*. The file is located at `/etc/turnserver.conf`.

   Use the **example TURN server parameters**. Unused parameters should be commented out.

Example TURN server parameters for coturn 4.5.2

Parameter	Type	Description
`tls-listening-port=5349`	Required	Listening port for TLS connections
`server-name=<example.abc.com>`	Required	FQDN name or IP address of the server
`realm=<abc.com>`	Required	Domain name of the server
`min-port=50010`	Required	Lower value of the port range for the UDP (User Datagram Protocol) relay Two UDP ports are used for one remote control session.
`max-port=50120`	Required	Upper value of the port range for the UDP relay
`verbose`	Optional	Use detailed logging

Parameter	Type	Description
`fingerprint`	Required	Use a digital fingerprint to identify the server and enhance its security
`use-auth-secret`	Required	Authentication method
`static-auth-secret=<secret>`	Required	Static value of the authentication secret for the TURN server REST API The value is a string that the server uses to validate the initial ICE request. Afterwards the connection secret is generated dynamically. The static secret value should be changed periodically, taking into account security requirements and the organization's password policy.
`no-udp`	Optional	Restrict unencrypted UDP listening
`no-tcp`	Optional	Restrict unencrypted TCP (Transmission Control Protocol) listening
`stale-nonce=300`	Optional	Timeout for providing credentials from an unauthorized user (sec)
`cert=/AFMH/SSL/cert.pem`	Required	Path to the certificate in PEM format
`pkey=/AFMH/SSL/key.pem`	Required	Path to the certificate key in PEM format
`log-file=/var/tmp/turn.log`	Required	Path for storing log files
`new-log-timestamp`	Optional	Enable including time in log files
`log-binding`	Optional	Enable UDP endpoint detailed logging
`no-stun`	Optional	Disable STUN (Session Traversal Utilities for NAT) functionality so that the server only operates in TURN mode
`no-multicast-peers`	Optional	Disable multicast peers support to prevent sending data to multiple recipients at once as an additional security measure
`no-tlsv1`	Optional	Disable insecure versions of TLS v1
`no-tlsv1_1`	Optional	Disable insecure versions of TLS v1_1
`cipher-list=ECDHE-RSA-AES256-GCM-SHA384:ECDHE-RSA-AES128-GCM-SHA256:ECDHE-ECDSA-AES128-GCM-SHA256:ECDHE-ECDSA-AES256-GCM-SHA384:ECDHE-RSA-CHACHA20-POLY1305`	Optional	Enable use of permitted ciphers for TLS 1.2

`denied-peer-ip=10.0.0.0-10.255.255.255`
`denied-peer-ip=192.168.0.0-192.168.255.255`
`denied-peer-ip=172.16.0.0-172.31.255.255`
	Optional	Deny TURN server client access to local network segments

`allowed-peer-ip=ipv4, ipv4-ipv4`	Optional	Allow an address or range of addresses of the local subnet by excluding it from the prohibited list
`max-bps=200000`	Optional	Maximum throughput of a single TURN server session (bps)
`bps-capacity`	Optional	Maximum total throughput that the TURN server is allowed to allocate (bps)

2. Configure Firewall on the server by opening the ports specified in the TURN server configuration file:

```
sudo ufw allow 5349/tcp
sudo ufw allow 50010:50120/udp
```

3 Get and configure the TURN server certificate

You can get a certificate from a CA or generate a self-signed certificate.

- A certificate obtained from CA must be in PEM format and issued to the server FQDN specified in the TURN server configuration file.

- To generate a self-signed certificate (for example, using the OpenSSL utility):

  1. Generate a CA key:
     ```
     openssl genrsa -out ca_key.key 2048
     ```

  2. Generate a self-signed CA certificate using your organization's specific parameters or your custom parameters:
     ```
     openssl req -x509 -new -nodes -key ca_key.key -sha256 -days 365 -subj "/C=<Country>/ST=<State or Province>/L=<Locality>/O=<Organization>/CN=<Common Name>" -out root_cert.pem
     ```

  3. Generate a server private key:
     ```
     openssl genrsa -out cert_key.key 2048
     ```

  4. Create Certificate Signing Request (CSR) for the server using your organization's specific parameters or your custom parameters:
     ```
     openssl req -new -key cert_key.key -subj "/C=<Country>/ST=<State or Province>/L=<Locality>/O=<Organization>" -out server_cert.csr
     ```

  5. Create a configuration for the SAN, EKU, and KeyUsage extensions - an `ext.cnf` file with the following contents:
     ```
     [ v3_req ]
     subjectAltName = @alt_names
     extendedKeyUsage = serverAuth
     keyUsage = digitalSignature, keyCertSign, cRLSign
     [ alt_names ]
     DNS.1 = <TURN server FQDN>
     ```

  6. Sign the server CA certificate:
     ```
     openssl x509 -req -in server_cert.csr -CA root_cert.pem -CAkey ca_key.key -CAcreateserial -out server_cert.crt -days 365 -sha256 -extfile ext.cnf -extensions v3_req
     ```

  7. Convert the server private key to PEM format for use in the TURN server configuration file:
     ```
     openssl rsa -in cert_key.key -out cert_key.pem -outform PEM
     ```

  8. Convert the CA-signed server certificate to PEM format for use in the TURN server configuration file:
     ```
     openssl x509 -in server_cert.crt -out server_cert.pem
     ```

  9. Convert the self-signed root certificate to CRT format for installation in the Trusted Certification Authority certificate store on the administrator's computer:
     ```
     openssl x509 -in root_cert.pem -out root_cert.crt
     ```

  10. Specify the path to the previously obtained `server_cert.pem` and `cert_key.pem` files in the TURN server configuration file. This path must be accessible by TURN server, for example, `/var/opt/turn`.

      Make sure that the `turnserver` user has the read permission.

  11. Install the `root_cert.crt` file in the Trusted Certification Authority certificate store on the administrator's computer, and then restart the browser.

4 Complete the setup

1. Restart coturn:
   ```
   systemctl restart coturn.service
   ```
2. Restart UFW:
   ```
   systemctl restart ufw
   ```

Specifying remote control server settings in Kaspersky Security Center

After installing and configuring the TURN server, you need to specify remote control settings in Kaspersky Security Center so it can access this TURN server. The settings are not passed to the TURN server automatically. They must be specified separately and must match the values specified in the TURN server configuration file.

As soon as the required settings are specified, Kaspersky Security Center will be able to generate the remote control session data and send it to an Android device via the mobile protocol.

To specify the remote control server settings in Kaspersky Security Center:

1. In the main window of Kaspersky Next Expert View (on-premise), click the Administration Server name.
2. In the Administration Server properties window that opens, on the **General** tab, select the **Connection ports** section.
3. In the **Remote control server settings for Android** block of settings, enable the **Use Remote control server for Android devices** toggle switch.

   This toggle determines whether Kaspersky Security Center uses a TURN server to remotely access Android devices.
4. Specify the **TURN server FQDN**.

   This setting specifies the FQDN (DNS name) that Kaspersky Security Center will use to get the ICE candidate's public address and port for remote control of the device.

   > This field cannot contain an IP address.
5. Specify the **TURN server port for ICE candidate request**.

   The port is required for Kaspersky Endpoint Security for Android and Kaspersky Security Center to request their ICE candidate from the TURN server. The TURN server will respond to the request with the address and port from which the request was received.

   > ICE candidates are requested in unencrypted form.

   > The TURN server port must match the `tls-listening-port` value specified in the TURN server configuration file.
6. Set the **TURN server static secret**.

   This setting is required for Kaspersky Security Center to generate session secrets for connecting to the TURN server. The static secret is a random string in the form of a password.

The specified TURN server static secret is not displayed in the settings field and remains invisible.

Make sure the secret matches the `static-auth-secret` value specified in the TURN server configuration file.

7. Upload the **TURN server certificate**.

   Upload the public key `root_cert.crt` of the TURN server certificate that you received at stage 3 step 9 of configuring TURN server by clicking **Upload**. This public key will be used by the administrator's browser and Kaspersky Endpoint Security for Android to verify the authenticity of the TURN server that will return ICE candidates.

   The certificate can be uploaded in PEM, CER, or CRT format and must be identical to the one installed on the TURN server, including the server address format (FQDN or DNS name).

8. Click **Save**.

The remote control server settings are specified. You can now start a remote control session for the device.

Starting a remote control session

To start and manage a remote control session:

1. Make sure the required **conditions for remote connection** are met.
   - The installed version of Kaspersky Next Expert View (on-premise) is 16.1 or later.
   - The installed version of Kaspersky Mobile Devices Protection and Management plug-in is 10.56 or later.
   - A TURN server is installed and configured.
   - The remote control server settings are specified in Kaspersky Security Center.
   - A license that provides the extended functionality of Advanced MDM in Kaspersky Next Expert View (on-premise) is installed in the Administration Server repository.
   - The administrator has the **Start RDP sessions** and **Send commands to mobile devices** rights to establish remote connections.
   - The mobile device to be accessed remotely is running Android 8 or later.
   - The installed version of Kaspersky Endpoint Security for Android on the device is 10.56.1.11 or later.
   - The device user has accepted the End User License Agreement (EULA) that includes the remote control functionality.
2. In the main window of Kaspersky Next Expert View (on-premise), select **Asset management** → **Mobile** → **Devices**.
3. In the list of mobile devices that opens, select the check box next to the device that you want to access remotely.

4. Open the 3-dot menu (⋮) and select **Remote control for Android** to start a remote control session.

   You cannot start a remote control session for a device that is currently being remotely controlled by another administrator.

   The remote control window opens and the remote control session is initiated. As soon as the mobile device synchronizes with Kaspersky Security Center, the user will receive the remote connection request. If Firebase Cloud messaging (FCM) integration is configured, synchronization occurs automatically. Otherwise, wait for scheduled synchronization or ask the user to synchronize their device manually.

   The user connection timeout does not exceed one hour. After this time, the session must be restarted.

   If the mobile device is running in corporate device mode, you can try to connect to the device without requesting user consent.

   You can configure whether user consent is requested when starting a remote control session in the **Configure notifications** settings of the **KES for Android settings** section (corporate device mode only).

5. As soon as the user accepts the request and the remote control session starts, the device screen is displayed. The image is displayed in the orientation of the mobile device screen.

   While the session is active, you can do the following:

   - View the device screen and check the connection speed.

     You cannot view the contents of the screen if it is protected from screenshot capturing and video recording (for example, incognito browser mode or the device lock screen).

   - Perform actions on the device:

     - By clicking the **Home**, **Back**, and **Overview** buttons below the displayed device screen.
     - By navigating the device using gestures. Gestures are applied by clicking on the display area. You can imitate tapping or long-tapping by pressing or long-pressing the device image, or you can drag and release the cursor.

   - Take screenshots by clicking **Take screenshot**.

     A screenshot is saved in the browser's Downloads folder, and its title contains the device name, date, and exact time of the screenshot.

   - Stop the session by clicking **Stop** or start it again for the same device without exiting the window.

     Once the remote control session starts, you can continue working in Kaspersky Next Expert View (on-premise) in a new browser tab without interrupting your active session. You can also open Kaspersky Security Center in another tab or window and start another remote control session for another device.

Switching away from the remote connection window interrupts the remote control session. To work with other Kaspersky Security Center sections while maintaining an active session, open Kaspersky Security Center in another browser window or tab.

The user can stop the remote control session at any moment on their device.

Managing Android devices

Kaspersky Next Expert View (on-premise) lets you manage Android devices in the following ways:

- Centrally manage devices by using commands.
- View information about the settings for management of Android devices.
- Install apps by using mobile app packages.
- Connect to devices and control them remotely.
- Disconnect Android devices from management.

Corporate devices

This section contains information about managing the settings of corporate Android devices. For information about installing Kaspersky Endpoint Security for Android on corporate devices, see here.

Restricting Android features on devices

These settings apply to corporate devices.

You can restrict Android operating system features on corporate devices. For example, you can restrict factory reset, changing credentials, use of Google Play and Google Chrome, file transfer over USB, changing location settings, and management of system updates. You can also restrict operating system features on personal devices and devices with a corporate container.

To restrict Android features:

1. In the main window of Kaspersky Next Expert View (on-premise), select **Asset management** → **Policies**. In the list of group policies that opens, click the name of the policy that you want to configure.
2. In the policy properties window, select **Application settings**.
3. Select **Android** and go to the **Restrictions** section.
4. On the **Device feature restrictions** card, click **Settings**.
   The **Device feature restrictions** window opens.
5. Enable the settings using the **Device feature restrictions** toggle switch.

6. Enable device feature restrictions using toggle switches on the corresponding tabs and select the required restrictions.

7. Click **OK**.

8. Click **Save** to save the changes you have made.

Mobile device settings are changed after the next device synchronization with Kaspersky Security Center.

Restrict device features

On the **General** tab, you can enable or disable the following features.

- Features in the **Data loss protection** section:

  - **Prohibit reset to factory settings**

    Selecting or clearing this check box specifies whether the device user is allowed to perform a factory reset from device settings.

    This check box is cleared by default.

  - **Prohibit screen capture**

    Selecting or clearing this check box specifies whether the device user is allowed to take screenshots and record and share the device screen. It also specifies whether the contents of the device screen are allowed to be captured for artificial intelligence purposes.

    This check box is cleared by default.

  - **Prohibit safe boot**

    Selecting or clearing this check box specifies whether the device user is allowed to boot the device in safe mode.

    The restriction is supported on devices with Android 6 or later.

    This check box is cleared by default.

- Features in the **Calls and SMS** section:

  - **Prohibit outgoing phone calls**

    Selecting or clearing this check box specifies whether the device user is allowed to make outgoing phone calls on this device.

    This check box is cleared by default.

  - **Prohibit sending and receiving SMS messages**

    Selecting or clearing this check box specifies whether the device user is allowed to send and receive SMS messages on this device.

    This check box is cleared by default.

- Features in the **Location services** section:

  - **Prohibit use of location**

    Prevents turning location services on and off.

If the check box is selected, the device user cannot turn location services on or off. Search in Anti-Theft mode becomes unavailable.

If the check box is cleared, the device user can turn location services on or off.

This check box is cleared by default.

Various combinations of values for **Prohibit use of location** and **Prohibit modifying location settings** produce different results for the location services feature and configuration.

Prohibit use of location	Prohibit modifying location settings	Feature restriction result
Enabled	Enabled	Location services are disabled and cannot be enabled by the device user.
Enabled	Disabled	Location services are disabled and can be enabled by the device user. Disabling the **Prohibit modifying location settings** restriction makes it possible for the user to disable location services on the device, which may make some features unavailable.
Disabled	Enabled	Location services are enabled and cannot be disabled by the device user.
Disabled	Disabled	Location services are enabled and can be disabled by the device user. Disabling the **Prohibit modifying location settings** restriction makes it possible for the user to disable location services on the device, which may make some features unavailable.

- **Prohibit sharing location**

  If this option is enabled, the user cannot share the device location via apps that provide a location-sharing feature.

  By default, the option is disabled.

- **Prohibit modifying location settings**

  Prevents changing location settings.

  If the check box is selected, the device user cannot change location settings or disable location services.

  If the check box is cleared, the device user can change location settings.

  The restriction is supported on devices with Android 9 or later.

  This check box is cleared by default.

  Various combinations of values for **Prohibit use of location** and **Prohibit modifying location settings** produce different results for the location services feature and configuration.

Prohibit use of location	Prohibit modifying location settings	Feature restriction result
Enabled	Enabled	Location services are disabled and cannot be enabled by the device user.
Enabled	Disabled	Location services are disabled and can be enabled by the device user. Disabling the **Prohibit modifying location settings** restriction makes it possible for the user to disable location services on the device, which may make some features unavailable.

Disabled	Enabled	Location services are enabled and cannot be disabled by the device user.
Disabled	Disabled	Location services are enabled and can be disabled by the device user. Disabling the **Prohibit modifying location settings** restriction makes it possible for the user to disable location services on the device, which may make some features unavailable.

- Features in the **Keyguard** section:
  - **Prohibit keyguard features**

    Selecting or clearing the check box specifies whether a user's device can be unlocked with a swipe.

    This setting has no effect if a password, PIN code, or pattern is currently set as an unlock method on the device.

    This check box is cleared by default.

  - **Prohibit disabling keyguard notifications**

    Selecting or clearing the check box specifies whether notifications are prohibited when the device screen is locked.

    This check box is cleared by default.

  - **Prohibit using keyguard camera**

    Selecting or clearing the check box specifies whether the device user is prohibited to use the camera when the device is locked.

    This check box is cleared by default.

  - **Prohibit using keyguard trust agents**

    Selecting or clearing this check box specifies whether trusted apps are prohibited when the device screen is locked. *Trusted apps* are apps that allow the device user to unlock the device without a password, PIN code, or fingerprint.

    This check box is cleared by default.

- Features in the **Users and accounts** section:
  - **Prohibit adding Google accounts**

    Selecting or clearing the check box specifies whether the device user is allowed to add and remove Google accounts.

    This check box is cleared by default.

  - **Prohibit adding users**

    Selecting or clearing the check box specifies whether the device user is allowed to add new users.

    This check box is selected by default. If a corporate device was connected to Kaspersky Security Center via a QR code, the restriction is enabled and can't be disabled.

    The restriction can be disabled only on devices that meet the following requirements:
    - The corporate device was connected to Kaspersky Security Center via the `adb.exe` installation package.
    - The device must support multiple users.

- **Prohibit switching user**

  If this option is enabled, the user cannot switch the current user of the device.

  By default, the option is disabled.

- **Prohibit removing users**

  Selecting or clearing the check box specifies whether the device user is allowed to remove users.

  This check box is selected by default. If a corporate device was connected to Kaspersky Security Center via a QR code, the restriction can't be disabled.

  The restriction can be disabled only on devices that meet the following requirements:

  - The corporate device was connected to Kaspersky Security Center via the `adb.exe` installation package.
  - The device must support multiple users.

- **Prohibit changing credentials**

  Selecting or clearing this check box specifies whether the device user is allowed to change user credentials in the operating system.

  This check box is cleared by default.

Restrict app features

On the **Apps** tab, you can enable or disable the following features.

- Features in the **General** section:

  - **Prohibit installation of apps**

    Selecting or clearing the check box specifies whether the device user is allowed to install apps on the device.

    This check box is cleared by default.

  - **Prohibit installation of apps from unknown sources**

    Selecting or clearing the check box specifies whether the device user is allowed to install apps from unknown sources.

    This check box is cleared by default.

  - **Prohibit modification of apps in Settings**

    Prevents modifying apps in Settings.

    If the check box is selected, the device user is not allowed to perform the following actions:

    - Uninstall apps
    - Disable apps
    - Clear app caches
    - Clear app data

- Force stop apps
- Clear app defaults

If the check box is cleared, the device user is allowed to modify apps in Settings.

This check box is cleared by default.

- **Prohibit disabling app verification**

  Selecting or clearing the check box specifies whether the device user is allowed to disable app verification.

  This check box is cleared by default.

- **Prohibit uninstallation of apps**

  Selecting or clearing the check box specifies whether a device user is allowed to uninstall apps from this device.

  This check box is cleared by default.

- Features in the **Google apps** section:

  - **Prohibit Google Play**

    Selecting or clearing the check box specifies whether the device user is allowed to use Google Play.

    This check box is cleared by default.

  - **Prohibit Google Chrome**

    Prevents use of Google Chrome.

    If the check box is selected, the device user cannot start Google Chrome or configure it in system settings.

    If the check box is cleared, the device user is allowed to use Google Chrome on the device.

    The check box is cleared by default.

  - **Prohibit Google Assistant**

    Selecting or clearing the check box specifies whether the device user is allowed to use Google Assistant on the device.

    This check box is cleared by default.

- Features in the **Camera** section:

  - **Prohibit use of camera**

    Selecting or clearing the check box specifies whether the device user is allowed to use all cameras on the device.

    If the check box is selected, the solution usually blocks the camera from being opened. However, for Asus, Honor, and OnePlus devices, the icon for the camera app is completely hidden when the check box is selected.

    This check box is cleared by default.

  - **Prohibit camera toggle**

    Prevents the device user from toggling the camera.

    If the check box is selected, the device user cannot block the camera access via the system toggle.

    If the check box is cleared, the device user is allowed to use the camera toggle.

The restriction is supported on devices with Android 12 or later.

This check box is cleared by default.

> On some Xiaomi and HUAWEI devices running Android 12, this restriction does not work. This issue is caused by the specific features of MIUI firmware on Xiaomi devices and EMUI firmware on HUAWEI devices.

- **Granting runtime permissions for apps**

  This setting allows you to select an action to be performed when apps installed on corporate devices are running and request additional permissions. This does not apply to permissions granted in Settings (e.g. Access All Files) on the device.

  - **Allow users to configure permissions**

    When a permission is requested, the user decides whether to grant the specified permission to the app.

    This option is selected by default.

  - **Grant permissions automatically**

    All apps installed on corporate devices are granted permissions without user interaction.

  - **Deny permissions automatically**

    All apps installed on corporate devices are denied permissions without user interaction.

    Users can adjust app permissions in device settings before these permissions are denied automatically.

  On Android 12 or later, the following permissions can't be granted automatically but can be denied automatically. If you select **Grant permissions automatically**, the app will prompt the user for these permissions:

  - Location permissions
  - Permissions for camera
  - Permissions to record audio
  - Permission for activity recognition
  - Permissions to monitor SMS and MMS incoming messages
  - Permissions to access body sensor data

Restrict storage features

On the **Storage** tab, in the **General** section, you can enable or disable the following features.

- **Prohibit debugging features**

  Prevents use of debugging features.

  If the check box is selected, the device user cannot use USB debugging features and developer mode.

  If the check box is cleared, the device user is allowed to enable and access debugging features and developer mode.

  This check box is cleared by default.

- **Prohibit mounting physical external media**

  Selecting or clearing the check box specifies whether the device user is allowed to mount physical external media, such as SD cards and OTG adapters.

  This check box is cleared by default.

- **Prohibit file transfer over USB**

  Selecting or clearing this check box specifies whether the device user is allowed to transfer files over USB.

  This check box is cleared by default.

- **Prohibit backup service**

  Selecting or clearing the check box specifies whether the device user is allowed to enable or disable the backup service.

  The restriction is supported on devices with Android 8 or later.

  This check box is cleared by default.

Restrict network features

On the **Network** tab, you can enable or disable the following features.

- Features in the **General** section:

  - **Prohibit airplane mode**

    Selecting or clearing the check box specifies whether the device user is allowed to enable airplane mode on the device.

    This restriction is supported on devices with Android 9 or later.

    This check box is cleared by default.

  - **Prohibit use of Android Beam via NFC**

    Selecting or clearing the check box specifies whether beaming out data from apps via NFC is allowed on the device. However, the device user can enable or disable NFC.

    This check box is cleared by default.

  - **Prohibit use of tethering**

    Selecting or clearing the check box specifies whether the device user is allowed to configure tethering and hotspots.

    This check box is cleared by default.

  - **Prohibit modifying VPN settings**

    Prevents changing VPN settings.

    If the check box is selected, the device user cannot configure a VPN in Settings and VPNs are prohibited from starting.

    If the check box is cleared, the device user is allowed to modify a VPN in Settings.

    This check box is cleared by default.

- **Prohibit resetting network settings**

  Selecting or clearing the check box specifies whether the device user is allowed to reset network settings in Settings.

  This restriction is supported on devices with Android 6 or later.

  This check box is cleared by default.

- Features in the **Wi-Fi** section:

  - **Prohibit use of Wi-Fi**

    Selecting or clearing the check box specifies whether the device user is allowed to use Wi-Fi and configure it in Settings.

    This check box is cleared by default.

  - **Prohibit enabling/disabling Wi-Fi**

    If this option is enabled, the user cannot enable or disable Wi-Fi on the device. Also, Wi-Fi cannot be disabled via airplane mode.

    By default, the option is disabled.

  - **Prohibit modifying Wi-Fi settings**

    Selecting or clearing the check box specifies whether the device user is allowed to configure Wi-Fi access points via Settings. The restriction does not affect Wi-Fi tethering settings.

    This check box is cleared by default.

  - **Prohibit Wi-Fi Direct**

    If this option is enabled, the user cannot use the Wi-Fi Direct feature on the device.

    By default, the option is disabled.

  - **Prohibit sharing pre-configured Wi-Fi networks**

    If this option is enabled, the user cannot share Wi-Fi networks that are configured in the policy settings. Other Wi-Fi networks on the device are not affected.

    By default, the option is disabled.

  - **Prohibit adding Wi-Fi networks**

    If this option is enabled, the user cannot manually add new Wi-Fi networks on the device.

    By default, the option is disabled.

  - **Prohibit changing pre-configured Wi-Fi networks**

    Selecting or clearing the check box specifies whether the device user is allowed to change Wi-Fi configurations added by the administrator in the Wi-Fi section.

    This check box is cleared by default.

- Features in the **Bluetooth** section:

  - **Prohibit use of Bluetooth**

    Prevents use of Bluetooth.

    If the check box is selected, the device user cannot turn on and configure Bluetooth via Settings.

If the check box is cleared, the device user is allowed to use Bluetooth.

The restriction is supported on devices with Android 8 or later.

This check box is cleared by default.

- **Prohibit modifying Bluetooth settings**

  Selecting or clearing the check box specifies whether the device user is allowed to configure Bluetooth via Settings.

  This check box is cleared by default.

- **Prohibit outgoing data sharing over Bluetooth**

  Selecting or clearing the check box specifies whether outgoing Bluetooth data sharing is allowed on the device.

  The restriction is supported on devices with Android 8.0 or later.

  This check box is cleared by default.

- Features in the **Mobile networks** section:

  - **Prohibit modifying mobile network settings**

    Selecting or clearing the check box specifies whether the device user is allowed to change mobile network settings.

    This check box is cleared by default.

  - **Prohibit use of cellular data while roaming**

    Selecting or clearing the check box specifies whether the device user is allowed to use cellular data while roaming.

    If the check box is selected, the device can't update anti-malware databases and synchronize with the Administration Server while roaming.

    To allow anti-malware database updates while roaming, this check box must be cleared and the **Allow database update while roaming** check box in the **Database update** settings of the policy must be selected.

    To allow device synchronization with the Administration Server while roaming, both this check box and the **Do not synchronize while roaming** check box in the **Scheduled synchronization** settings of the policy must be cleared.

    This restriction is supported on devices with Android 7 or later.

    This check box is cleared by default.

Additional restrictions

On the **Additional settings** tab, you can enable or disable the following features.

- Features in the **Language, date, and time** section:

  - **Prohibit changing language**

    Selecting or clearing the check box specifies whether the device user is allowed to change the device language.

    This restriction is supported on devices with Android 9 or later.

This check box is cleared by default.

> On some corporate devices (for example, Xiaomi, TECNO, and Realme) running Android 9 or later, when you select the **Prohibit changing language** check box, the user still can change the language, and no warning message appears.

- **Prohibit changing date, time, and time zone**

  Selecting or clearing the check box specifies whether the device user is allowed to change date, time, and time zone in Settings.

  This restriction is supported on devices with Android 9 or later.

  This check box is cleared by default.

- Features in the **Display** section:

  - **Prohibit changing wallpaper**

    Selecting or clearing the check box specifies whether the device user is allowed to change the wallpaper on the mobile device.

    This restriction is supported on devices with Android 7 or later.

    This check box is cleared by default.

  - **Prohibit adjusting brightness**

    Selecting or clearing the check box specifies whether the device user is allowed to adjust the brightness on the mobile device.

    This restriction is supported on devices with Android 9 or later.

    This check box is cleared by default.

  - **Prohibit status bar**

    Prevents the status bar from being displayed.

    If the check box is selected, the status bar is not displayed on the device. Notifications and quick settings accessible via the status bar are also blocked.

    If the check box is cleared, the status bar can be displayed on the device.

    The restriction is supported on devices with Android 6 or later.

    This check box is cleared by default.

  - **Prohibit ambient display**

    If this option is enabled, the user cannot use the Ambient Display feature on the device.

    By default, the option is disabled.

- Features in the **Screen on** section:

  - **Force screen on when plugged in to AC charger**

    Selecting or clearing the check box specifies whether the device screen will be on while the device is charging using an AC charger.

    The restriction is supported on devices with Android 6 or later.

    This check box is cleared by default.

- **Force screen on when plugged in to USB charger**

  Selecting or clearing the check box specifies whether the device screen will be on while the device is charging using a USB charger.

  The restriction is supported on devices with Android 6 or later.

  This check box is cleared by default.

- **Force screen on when charging wirelessly**

  Selecting or clearing this check box specifies whether the device screen will be on while the device is charging using a wireless charger.

  The restriction is supported on devices with Android 6 or later.

  This check box is cleared by default.

- Features in the **Microphone** section:

  - **Prohibit unmuting microphone**

    If this option is enabled, the device microphone is muted.

    If this option is disabled, the user can unmute the microphone and adjust its volume.

    By default, the option is disabled.

  - **Prohibit microphone toggle**

    If this option is enabled, the user cannot disable access to the microphone via the system toggle on the device. If access to the microphone on the device is disabled when this option is enabled, it is automatically re-enabled.

    By default, the option is disabled.

    > On some Xiaomi and HUAWEI devices running Android 12, this restriction does not work. This issue is caused by the specific features of MIUI firmware on Xiaomi devices and EMUI firmware on HUAWEI devices.

- Features in the **Volume** section:

  - **Prohibit adjusting volume**

    Restricts volume adjustment and muting the device.

    If the check box is selected, the device user can't adjust the volume and the device is muted.

    If the check box is cleared, the device user can adjust the volume and the device is unmuted.

    > Anti-Theft can disregard this restriction to play a sound on the device. The restriction is disabled to allow the sound to play, and then it is re-enabled.

    This check box is cleared by default.

Restrict system updates

Management of update settings on mobile devices is vendor-specific. On some Android devices, the restriction on manual installation of operating system updates may not work correct.

On the **OS update** tab, you can configure the following settings.

- In the **Update mode** section:
  - **Set system update policy**

    Type of system update policy.

    If the check box is selected, one of the following system update policies is set:

    - **Install updates automatically**. Installs system updates immediately without user interaction. This option is selected by default.
    - **Install updates during daily window**. Installs system updates during a daily maintenance window without user interaction.

      You also need to set the start and end of the daily maintenance window in the **Start time** and **End time** fields respectively.
    - **Postpone updates for 30 days**. Postpones the installation of system updates for 30 days.

      After the specified period, the operating system prompts the device user to install the updates. The period is reset and starts again if a new system update is available.

    If the check box is cleared, a system update policy is not set.

    This check box is selected by default.

    Management of update settings on mobile devices is vendor-specific. On some Android devices, the restriction on manual installation of operating system updates may not work correct.

- In the **Freeze periods** section:
  - **System update freeze periods**

    This block lets you set one or more freeze periods of up to 90 days during which system updates will not be installed on the device. When the device is in a freeze period, it behaves as follows:

    - The device does not receive any notifications about pending system updates.
    - System updates are not installed.
    - The device user cannot check for system updates manually.

      To add a freeze period, click **Add period** and enter the start and end of the freeze period in the **Start date** and **End date** fields respectively.

    > Each freeze period can be at most 90 days long, and the interval between consecutive freeze periods must be at least 60 days.

    The restriction is supported on devices with Android 9 or later.

    Management of update settings on mobile devices is vendor-specific. On some Android devices, the restriction on manual installation of operating system updates may not work correct.

Configuring kiosk mode for Android devices

> These settings apply to corporate devices.

Kiosk mode is a Kaspersky Endpoint Security for Android feature that lets you limit the apps available to a device user to a single app or a set of multiple apps. You can also efficiently manage some device settings.

Kiosk mode does not affect the work of the Kaspersky Endpoint Security for Android app. It runs in the background, shows notifications, and can be updated.

Types of kiosk modes

The following types of kiosk mode are available in Kaspersky Endpoint Security:

- Single-app mode

  Kiosk mode with only a single app. In this mode, a device user can open only the one app that is allowed on the device and specified in the kiosk mode settings. If the app that you want to add to kiosk mode is not installed on the device, kiosk mode activates after the app is installed.

  On Android 9 or later, the app launches directly in kiosk mode.
  On Android 8 or earlier, the specified app must support kiosk mode functionality and call the `startLockTask()` method itself to launch the app.

- Multi-app mode

  Kiosk mode with multiple apps. In this mode, a device user can open only the set of apps that are allowed on the device and specified in the kiosk mode settings.

Before you configure kiosk mode

Before you configure kiosk mode, do the following:

- Before specifying the apps that are allowed to be run on the device in kiosk mode, go to **Asset management** → **Policies** → **Application settings** → **Android** → **Security controls** → **App Control** → **App management**. Click **Add** and select the **Install** action for these apps.

  Then, the specified apps will appear in the **App package** list of the **Kiosk mode** policy settings.

- If you want to specify trusted apps that users can navigate to from the ones allowed in kiosk mode, first add these apps as allowed in the **App Control** policy settings. Do one of the following:

  - On the **App use** tab, add the app to the **Allowed apps** list.
  - On the **App management** tab, select the **Install** or **Recommend installation** action for the app.

  Then, the specified apps will appear in the **Trusted apps** section of the **Kiosk mode** policy settings.

- Before activating kiosk mode, we recommend that you prohibit starting Google Assistant by enabling the corresponding restriction in **Asset management** → **Policies** → **Application settings** → **Android** → **Restrictions** → **Device feature restrictions** → **Apps** → **Prohibit Google Assistant**. Otherwise, Google Assistant starts in kiosk mode and allows non-trusted apps to be opened.

Open the kiosk mode settings

To open the kiosk mode settings:

1. In the main window of Kaspersky Next Expert View (on-premise), select **Asset management** → **Policies**. In the list of group policies that opens, click the name of the policy that you want to configure.
2. In the policy properties window, select **Application settings**.
3. Select **Android** and go to the **Restrictions** section.
4. On the **Kiosk mode** card, click **Settings**.

The **Kiosk mode** window opens.

Configure single-app mode

To configure single-app mode:

1. Enable the settings using the **Kiosk mode** toggle switch.
2. In the **Operating mode** drop-down list, select **Single-app mode**.
3. In the **App package** drop-down list, select an app package with the app that is allowed to be run on the device.
4. Specify any required restrictions. For available restrictions, see the "Kiosk mode restrictions" section below.
5. Select the **Allow navigation to trusted apps** check box if you want to add other apps that a device user can navigate to. For more details, see the "Add additional apps" section below.
6. Click **OK**.
7. Click **Save** to save the changes you have made.

Mobile device settings are changed after the next device synchronization with Kaspersky Security Center.

Configure multi-app mode

To configure multi-app mode:

1. Enable the settings using the **Kiosk mode** toggle switch.
2. In the **Operating mode** drop-down list, select **Multi-app mode**.
3. Click **Add package** and select the apps that are allowed to be run on the device.
4. Specify any required restrictions. For available restrictions, see the "Kiosk mode restrictions" section below.
5. Select the **Allow navigation to trusted apps** check box if you want to add other apps that a device user can navigate to. For more details, see the "Add additional apps" section below.

6. Click **OK**.

7. Click **Save** to save the changes you have made.

Mobile device settings are changed after the next device synchronization with Kaspersky Security Center.

Kiosk mode restrictions

You can set the following restrictions in kiosk mode:

- **Prohibit Overview button**

  Selecting or clearing this check box specifies whether the Overview button is hidden. This restriction is supported on devices with Android 9 or later.

  The check box is selected by default.

- **Prohibit Home button**

  Selecting or clearing this check box specifies whether the Home button is hidden. This restriction is supported on devices with Android 9 or later.

  The check box is selected by default.

- **Prohibit status bar**

  Selecting or clearing this check box specifies whether the status bar displays notifications, indicators such as connectivity and battery, and the sound and vibrate options. This restriction is supported on devices with Android 9 or later.

  The check box is selected by default.

- **Prohibit system notifications**

  Selecting or clearing this check box specifies whether system notifications are hidden. This restriction is supported on devices with Android 9 or later.

  The check box is selected by default.

- **Prohibit enabling kiosk mode if not all selected apps are updated or installed**

  Selecting or clearing this check box specifies whether kiosk mode can be enabled if one or more kiosk-mode apps are not updated or installed on the device.

  If this check box is selected, kiosk mode cannot be enabled until all required apps are installed and up to date. If kiosk mode is already enabled and apps cannot be updated, Kaspersky Endpoint Security for Android displays a blocking screen to restrict use of the device. To continue using kiosk mode with older versions of apps, the user must tap **Back to kiosk mode** on the blocking screen. This blocking screen will reappear if kiosk-mode apps are not updated within 24 hours or if the App Control policy settings for kiosk-mode apps are modified and required apps are still not up to date.

  If this check box is cleared, kiosk mode can be enabled even if not all required apps are updated or installed.

  This check box is available only if kiosk mode is running in multi-app mode.

  The check box is selected by default.

Disabling kiosk mode using a one-time code

A one-time code is a secret code for disabling kiosk mode. The code is generated by Kaspersky Security Center and is unique for each mobile device. You can change the length of the one-time code (4, 8, 12, or 16 digits) in the **Kiosk mode** settings of the policy.

To configure disabling kiosk mode:

1. In the **Disable using one-time code** section, select the **Allow disabling kiosk mode using one-time code** check box.
2. If necessary, change the length of the one-time code in the corresponding drop-down list. By default, the code is 4 digits long.
3. Click **OK**.
4. Click **Save** to save the changes you have made.

Kiosk mode can now be disabled using a one-time code. The length of the one-time code is set to the selected value.

Mobile device settings are changed after the next device synchronization with Kaspersky Security Center.

To disable kiosk mode on a user's mobile device using one-time code:

1. In the main window of Kaspersky Next Expert View (on-premise), select **Asset management** → **Mobile** → **Devices**.
2. Click the mobile device for which you want to get a one-time code.
3. Select **Applications** → **Kaspersky Mobile Devices Protection and Management**.

   The **Kaspersky Mobile Devices Protection and Management** properties window opens.
4. Select the **Application settings** tab.

   The unique code for the selected device is displayed in the **One-time code** field of the **One-time code to disable kiosk mode** section.
5. Use any available method (such as email) to communicate the one-time code to the user of the device.
6. After receiving a one-time code, the user must do the following:

   a. To open a window with a field for entering the one-time code, do one of the following:

   - Tap the back button 3 or more times.
   - Tap the Home button 3 or more times, if the **Prohibit Home button** check box is cleared in the **Restrictions** section of the **Kiosk mode** card.
   - Tap and hold the shield image on the Kaspersky Endpoint Security for Android home screen.

   b. Enter the one-time code.

Kiosk mode is disabled on the user's mobile device.

To enable kiosk mode again after disabling it using one-time code, you must configure kiosk mode settings and synchronize the user's mobile device with Kaspersky Security Center. The user must then confirm enabling kiosk mode in the message that appears on the device.

Add additional apps

Besides locking the device to a single app or set of apps, you can also specify additional apps, that the main app can use. These additional apps allow the apps added to kiosk mode to provide their full functionality. For example, the user can view a document or access a website opened from the main app. By default, these additional apps are hidden on a device and a user cannot launch them manually. Additional apps are not required for the kiosk mode to launch.

To add additional apps:

1. In the **Trusted apps** section, select the **Allow navigation to trusted apps** check box.
2. To specify a trusted app, do one of the following:
   - Click **Add from App Control** and select the app from the list of the apps previously added in the **App Control** policy settings.

     Only apps for which the **Install** or **Recommend installation** action is selected or apps that are in the **Allowed apps** list will be available.

   - Click **Add by package name** and specify the desired app package name.

     How to get the package name of an app

     To get the name of an app package:

     1. Open Google Play.
     2. Find the app and open its page.

        The app's URL ends with its package name (for example, https://play.google.com/store/apps/details?id=**com.android.chrome**).

     To get the name of an app package that has been added to Kaspersky Security Center:

     1. In the main window of Kaspersky Next Expert View (on-premise), select **Asset management** → **Mobile** → **Apps & files**.
     2. Select **Android** → **Apps**.

        In the list of apps that opens, app identifiers are displayed in the **Package name** column.
3. Click **OK**.
4. Click **Save** to save the changes you have made.

Additional apps are added.

Mobile device settings are changed after the next device synchronization with Kaspersky Security Center.

Connecting to a NDES/SCEP server

These settings apply to corporate devices.

You can connect to an NDES/SCEP server to obtain a certificate from a certificate authority (CA) using the Simple Certificate Enrollment Protocol (SCEP). To do this, you need to add a connection to the certificate authority and a certificate profile.

To add a connection to the certificate authority and a certificate profile:

1. In the main window of Kaspersky Next Expert View (on-premise), select **Asset management** → **Policies**. In the list of group policies that opens, click the name of the policy that you want to configure.
2. In the policy properties window, select **Application settings**.
3. Select **Android** and go to the **Device configuration** section.
4. On the **SCEP and NDES** card, click **Settings**.

   The **SCEP and NDES** window opens.
5. Enable the settings using the **SCEP and NDES** toggle switch.

   The **Add connection to certificate authority** window opens.
6. Add a connection to the certificate authority:

   a. In the **Connection name** field, enter the name of the connection to the certificate authority.

   b. In the **Protocol type** drop-down list, select the protocol version.

   c. In the **Server URL** field, enter the URL of a NDES or SCEP server.

   > The format of the NDES server URL is `http://<ServerName>/certsrv/mscep/mscep.dll`.

   d. In the **Challenge phrase type** drop-down list, select one of the following options to configure the authentication challenge:

   - **None**

     Challenge response is disabled. No authentication data is required.

   - **Static**

     Challenge response is enabled. You must enter the authentication phrase in the **Static challenge phrase** field.

   e. If you selected the **Static** option, in the **Static challenge phrase** field, enter the authentication phrase.

   f. Click **Add**.

   The connection to the certificate authority is added. You can add multiple connections to certificate authorities.
7. Select the **Certificate profile** tab and click **Add**.

   The **Add profile** window opens.

8. Add a certificate profile:

    a. In the **General settings** section, in the **Profile name** field, enter the unique certificate profile name.

    b. In the **Certificate authority (CA)** drop-down list select the certificate authority that you added on the **Certificate authority** tab.

    c. In the **Subject Name** field specify the subject of the certificate. *Subject name* is a unique identifier that includes information about what is being certified, such as common name, organization, organizational unit, and country code. You can either enter a value or select a macro by clicking the + button.

    d. If you want to add an alternative name that represents the certificate subject name, click **Add Subject Alternative Name** and configure the following settings:

        1. In the **Type of Subject Alternative Name** drop-down list select the subject alternative name type.

        2. In the **Subject Alternative Name** field enter the alternative name. You can either enter a value or select a macro by clicking the + button.

    You can add multiple subject alternative names.

    e. In the **Key** section, in the **Key size (bit)** drop-down list, select the certificate's private key length.

    f. In the **Private key type** drop-down list select the certificate's private key type:

    g. If you want the certificate to be automatically reissued to the device before it expires, in the **Certificate** section, select the **Renew certificate automatically** check box. This check box is cleared by default.

    h. If you selected the **Renew certificate automatically** check box, enter the number of days before the expiration date when the certificate is reissued in the **Renew certificate before it expires in (days)** field.

    i. Click **Add**.

    The certificate profile is added. You can add multiple certificate profiles.

9. Click **OK**.

10. Click **Save** to save the changes you have made.

    Mobile device settings are changed after the next device synchronization with Kaspersky Security Center.

You can edit or remove the added connections to certificate authorities and certificate profiles by clicking **Edit** and **Delete** at the top of the list.

If you delete a connection to a certificate authority, all certificate profiles that use it are also removed.

Enabling certificate-based authentication of devices

To enable certificate-based authentication of a device:

1. Open the command line on a device where the Administration Server is installed.
2. Go to the directory containing the klscflag utility.

   By default, the utility is located in `/opt/kaspersky/ksc64/sbin`.

3. Run the following command under an account with root privileges to configure certificate-based authentication of devices on the Administration Server:

   ```
   ./klscflag -fset -pv ".core/.independent" -s KLLIM -n
   LP_MobileMustUseTwoWayAuthOnPort13292 -t d -v 1
   ```

4. Restart the Administration Server service.

   After you start the Administration Server service, certificate-based authentication of the device using a shared certificate will be required.

   The first connection of the device to the Administration Server does not require a certificate.

By default, certificate-based authentication of devices is disabled.

Creating a mobile application package for Android devices

To create a mobile app package:

1. In the main window of Kaspersky Next Expert View (on-premise), select **Asset management** → **Mobile** → **Apps & files**.
2. Click **Android**.
3. Click **Apps** and then click **Add**.

   The **Add app** window opens.

4. Specify the app name in the **App name** field. This name will be used to identify the app in policy settings.
5. Click **Select** and select an APK file on your computer.
6. Click **Save** to save the changes you have made.

   The newly created app package is displayed in the list of apps on the **Apps** tab.

   If you select a large APK file, the app may take some time to upload. Do not close the **Apps & files** section until the app is uploaded.

In the **Apps & files** section, you can also add iOS apps.

Sending files to Android devices

This functionality is available with Kaspersky Security Center Linux 15.2 or later.

Kaspersky Next Expert View (on-premise) lets you send files in any format to Android devices in all operating modes.

Sending files is available with a license that provides the extended functionality of Advanced MDM in Kaspersky Next Expert View (on-premise). For detailed information on licenses, refer to the About the license section.

Before you send files to devices, you must add files to the Administration Server. You can add files in the **Apps & files** section and then select which files to send to devices in the **File sharing** policy settings.

Each file may be no larger than 1.5 GB.

For file sharing to work, Kaspersky Endpoint Security for Android must be granted the "All files access" permission on devices running Android 11 or later or the "Storage" permission on devices running Android 10 or earlier.

On devices with a corporate container, you can copy the files that you send to the corporate container to the user's personal space.

Adding and managing files

To add files to the Administration Server:

1. In the main window of Kaspersky Next Expert View (on-premise), select **Asset management** → **Mobile** → **Apps & files**.
2. Select **Android** → **Files**.

   The list of files opens.
3. Click **Add**.

   The **Add file** window opens.
4. Click **Select** to select the file that you want to add.
5. If necessary, in the **Description** field, enter additional information about the file.
6. Click **Add**.

The file will be added to the Administration Server.

You can delete files or download them to your computer using the corresponding buttons at the top of the list.

If you delete a file in the **Apps & files** section, it is deleted from the Administration Server but remains on devices. To remove the file from devices, delete it in the **File sharing** policy settings.

You can view information about any file in the list by clicking its name.

Sending files to devices

To send files to devices:

1. In the main window of Kaspersky Next Expert View (on-premise), select **Asset management** → **Policies**. In the list of group policies that opens, click the name of the policy that you want to configure.
2. In the policy properties window, select **Application settings**.
3. Select **Android** and go to the **Device configuration** section.
4. On the **File sharing** card, click **Settings**.

   The **File sharing** window opens.
5. Enable the settings using the **File sharing** toggle switch.
6. Click **Add**.

   The **Add file** window opens.
7. In the **File name** drop-down list, select a file that you added in the **Apps & files** section.
8. In the **Root folder** drop-down list, do one of the following:

   - Select a standard root folder on devices.
   - Select **Custom folder** to specify the root folder manually in the **Folder** field.
9. In the **Folder** field, do one of the following:

   - If you selected a standard root folder, specify the rest of the path of the folder to which the file will be sent.
   - If you selected **Custom folder**, specify the full path of the folder to which the file will be sent.

   The path must use slashes (/) as separators and may include letters, digits, underscore characters (_), and dashes (-).

   If the folder you specify does not exist on devices, Kaspersky Endpoint Security for Android creates it automatically.
10. If you want to send several files to devices, click **Add file** and repeat steps 7-9.
11. Click **Add**.

    The new file appears in the list.

12. Click **OK**.

13. Click **Save** to save the changes you have made.

    Files are sent to devices after the next device synchronization with Kaspersky Security Center. Due to technical limitations, delivering large files to devices may take some time.

You can delete files from devices using the corresponding button at the top of the list.

If you delete a file in the **File sharing** policy settings, it is deleted from devices but remains on the Administration Server.

Viewing information about an Android device

To view information about an Android device:

1. In the main window of Kaspersky Next Expert View (on-premise), select **Asset management** → **Mobile** → **Devices**.

   The list of managed mobile devices opens.

2. To filter Android devices, click the **OS** column heading and select **Android**.

   The list of Android devices is displayed.

   Depending on the database you use, searches may be case-sensitive.

3. Select the mobile device you want to view information about.

   A window with the properties of the Android device opens.

The mobile device properties window displays information about the connected Android device.

IMEI numbers are displayed for all devices running Android 5–9, corporate devices running Android 10 or later, and devices with a corporate container running Android 10–11.

If an old version of Kaspersky Endpoint Security for Android (10.52.1.3 or earlier) is installed on the devices the **Operating mode** value is set to **Unknown**.

Disconnecting an Android device from management

To disconnect an Android device from management, the user has to remove Kaspersky Endpoint Security for Android from the mobile device. After the user has removed Kaspersky Endpoint Security for Android, the administrator can remove the mobile device from the list of managed devices in Kaspersky Next Expert View (on-premise).

If Kaspersky Endpoint Security for Android has not been removed from the mobile device, that mobile device reappears in the list of managed devices after synchronization with the Administration Server.

To remove an Android device from the list of managed devices:

1. In the main window of Kaspersky Next Expert View (on-premise), select **Asset management** → **Mobile** → **Devices**.

   The list of managed mobile devices opens.

2. To filter Android devices, click the **OS** column heading and select **Android**.

   The list of Android devices is displayed.

3. Select the mobile device you want to disconnect.

4. Click **Delete**.

The mobile device is removed from the list of managed devices.

Managing iOS MDM devices

This section describes advanced features for management of iOS MDM devices in Kaspersky Next Expert View (on-premise).

Signing management profiles with a certificate

This functionality is available with Kaspersky Security Center Linux 15.2 or later.

You can sign management profiles with a certificate received from a trusted certification authority.

A certificate is not required for the management profile to operate correctly. If the management profile is not signed with a certificate, then when installing the management profile, a warning appears and users are prompted to confirm that they trust the organization that sent the certificate.

To sign management profiles with a certificate:

1. In the main window of Kaspersky Next Expert View (on-premise), select **Asset management** → **Mobile** → **iOS MDM Servers**.

   The list of iOS MDM Servers opens.

2. Click **Signing certificate**.

   The **Signing certificate** window opens.

3. In the **Certificate format** field, specify the public or private certificate type:
   - If the **PKCS #12** value is selected, specify the certificate file and the password.
   - If the **X.509** value is selected:
     a. Specify the private key file.
     b. Specify the public key file.
     c. Specify the private key password.
4. Click **Save**.

Management profiles that you create will now be signed with the specified certificate.

Adding a configuration profile

To create a configuration profile, you can use Apple Configurator 2, which is available on the Apple website. Apple Configurator 2 works only on devices running macOS. If you do not have such devices at your disposal, you can use iPhone Configuration Utility. However, Apple no longer supports iPhone Configuration Utility.

To add a configuration profile to an iOS MDM Server:

1. In the main window of Kaspersky Next Expert View (on-premise), select **Asset management → Mobile → iOS MDM Servers**. In the list of iOS MDM Servers that opens, click the iOS MDM Server whose settings you want to configure.
2. In the iOS MDM Server settings window, select **Application settings**.
3. Select the **Configuration profiles** tab.
4. To add a new configuration profile, click **Add**.
5. In the window that opens, select the configuration profile that you want to add.

   The configuration profile name should not be longer than 100 characters. If you enter a longer name, only part of it will be displayed.

The new configuration profile will be displayed in the list of configuration profiles.

You can install the profile that you have created on iOS MDM devices.

Installing a configuration profile on a device

You can install a configuration profile on an iOS MDM device in the **Send command** window or on the **Configuration profiles** tab in the device properties window.

In the **Send command** window, you can install configuration profiles on multiple devices.

To install a configuration profile in the Send command window:

1. In the main window of Kaspersky Next Expert View (on-premise), select **Asset management** → **Mobile** → **Devices**.
2. In the list of devices that opens, select the devices that you want to install configuration profiles on.
3. Click **Send command**.
4. In the **Send command** window that opens, in the **Command** field, select the **Install configuration profile** command.
5. In the **Configuration profiles** section, select the configuration profiles that you want to install on the devices.
6. Click **Send**.

The command is sent to the devices you selected.

To install a configuration profile in the device properties window:

1. In the main window of Kaspersky Next Expert View (on-premise), select **Asset management** → **Mobile** → **Devices**.
2. In the list of devices that opens, click the name of the device that you want to install configuration profiles on.

   The device properties window opens.
3. Select the **Configuration profiles** tab.
4. At the top of the configuration profiles list, click **Install**.
5. In the window that opens, select the configuration profiles that you want to install on the device and click **Install**.

The command is sent to the device.

Installing profiles may take a few minutes. The command is executed only if a device is connected to the internet. To check whether a profile has been installed, click **Refresh list**.

Removing a configuration profile from a device

You can remove a configuration profile from an iOS MDM device in the **Send command** window or on the **Configuration profiles** tab in the device properties window.

In the **Send command** window, you can remove configuration profiles from multiple devices.

To remove a configuration profile in the Send command window:

1. In the main window of Kaspersky Next Expert View (on-premise), select **Asset management** → **Mobile** → **Devices**.
2. In the list of devices that opens, select the devices that you want to remove configuration profiles from.
3. Click **Send command**.
4. In the **Send command** window that opens, in the **Command** field, select the **Delete configuration profile** command.
5. In the **Configuration profiles** section, select the configuration profiles that you want to remove from the devices.
6. Click **Send**.

The command is sent to the devices you selected.

The profile may be displayed in the list of configuration profiles installed on the device for several minutes after it has been deleted.

To remove a configuration profile in the device properties window:

1. In the main window of Kaspersky Next Expert View (on-premise), select **Asset management** → **Mobile** → **Devices**.
2. In the list of devices that opens, click the name of the device that you want to remove configuration profiles from.

   The device properties window opens.
3. Select the **Configuration profiles** tab.
4. In the configuration profiles list, select the configuration profiles that you want to remove from the device and click **Delete**.

The command is sent to the device.

Removing profiles may take a few minutes. The command is executed only if a device is connected to the internet. To check whether a profile has been removed, click **Refresh list**.

You cannot prevent users from removing the configuration profile through the device settings.

Configuring managed apps

Before installing an app on an iOS MDM device, you must add that app to the Administration Server. An app is considered managed if it has been installed on a device through Kaspersky Mobile Devices Protection and Management. A managed app can be managed remotely by means of Kaspersky Mobile Devices Protection and Management.

To add a managed app to an iOS MDM Server:

1. In the main window of Kaspersky Next Expert View (on-premise), select **Asset management** → **Mobile** → **Apps & files**.
2. Click **iOS**, and then click **Add**.

   The **Add app** window opens.
3. Specify the app name in the **App name** field. This name will be used to identify the app in policy settings.
4. In the **Installation method** field, select one of the following methods to add the app:

   - **Installation package**
   - **Link to manifest file**

     A manifest file is a PLIST file, which is required to install an app on an iOS device. These files are dictionaries containing app installation settings (for example, the location of the installation package). When you use a manifest file to add an app, you have to fill in these settings manually. When you add an app from the App Store or an IPA file, the manifest file is generated automatically.

     To get a manifest file for an app, we recommend first adding the app to the iOS MDM Server using an IPA file. In this case, the iOS MDM Server automatically generates a manifest file, which you can download and modify later.
   - **App Store**
5. Do one of the following:

   Use only legitimate and trusted sources. By configuring the settings in this section, you are solely responsible for any potential risks and consequences associated with using unreliable sources.

   - If you selected **Installation package**, click **Select**, and upload an IPA file from your computer.
   - If you selected **Link to manifest file**, specify a link to a manifest file that can be used to download the app.
   - If you selected **App Store**, specify a link or ID of the app to be added from the App Store.
6. If necessary, in the **Per App VPN** section, configure Per App VPN.
7. If necessary, configure the following settings:

   - Select the **Remove when management profile is deleted** check box if you want the app to be removed from the user's mobile device along with the management profile. This check box is selected by default.
   - Select the **Block backup of app data to iCloud** check box if you want to block backup of the app data to iCloud.
8. If you want to add a custom configuration for the app, in the **App configuration** section, click **Select** and select a configuration file in PLIST format on your computer.

To generate a configuration file, you can use a configuration generator (for example, https://appconfig.jamfresearch.com/generator) or refer to the official documentation on the app to be configured.

Example of a basic configuration for the Microsoft Outlook app

Microsoft Outlook app configuration

Configuration key	Description	Type	Value	Defau value
`com.microsoft.outlook.EmailProfile.EmailAccountName`	Username	String	The username that will be used to pull the username from Microsoft Active Directory. It might be different from the user's email address. For example, `User`.	
`com.microsoft.outlook.EmailProfile.EmailAddress`	Email address	String	The email address that will be used to pull the user's email address from Microsoft Active Directory. For example, `user@companyname.com`.	
`com.microsoft.outlook.EmailProfile.EmailUPN`	User Principal Name or username for the email profile that is used to authenticate the account	String	The name of the user in email address format. For example, `userupn@companyname.com`.	
`com.microsoft.outlook.EmailProfile.ServerAuthentication`	Authentication method	String	`Username and Password` – Prompts the device user for their password. `Certificates` – Certificate-based authentication.	`Userna and Passwo`
`com.microsoft.outlook.EmailProfile.ServerHostName`	ActiveSync FQDN	String	The Exchange ActiveSync email server URL. You don't need to use HTTP:// or HTTPS:// in front of the URL. For example, `mail.companyname.com`.	
`com.microsoft.outlook.EmailProfile.AccountDomain`	Email domain	String	The account domain of the user. For example, `companyname`.	
`com.microsoft.outlook.EmailProfile.AccountType`	Authentication type	String	`ModernAuth` – Uses a token-based identity management method. Specify ModernAuth as the Account Type for Exchange Online. `BasicAuth` – Prompts the device user for their password. Specify BasicAuth as the Account Type for Exchange On-Premises.	`BasicA`

Configuration key	Description	Type	Value	Defau value
`IntuneMAMRequireAccounts`	Is sign-in required	String	Specifies whether account sign-in is required. You can select one of the following values: `Enabled` - The app requires the user to sign-in to the managed user account defined by the `IntuneMAMUPN` key to receive Org data. `Disabled` - No account sign-in is required	
`IntuneMAMUPN`	UPN Address	String	The User Principal Name of the account allowed to sign into the app. For example, `userupn@companyname.com`.	

Example of a configuration file for the Microsoft Outlook app

```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE plist PUBLIC "-//Apple//DTD PLIST 1.0//EN"
"http://www.apple.com/DTDs/PropertyList-1.0.dtd">
<plist version="1.0">
<dict>
  <key>com.microsoft.outlook.EmailProfile.AccountType</key>
  <string>BasicAuth</string>
  <key>com.microsoft.outlook.EmailProfile.EmailAccountName</key>
  <string>My Work Email</string>
  <key>com.microsoft.outlook.EmailProfile.ServerHostName</key>
  <string>exchange.server.com</string>
  <key>com.microsoft.outlook.EmailProfile.EmailAddress</key>
  <string>%email%</string>
  <key>com.microsoft.outlook.EmailProfile.EmailUPN</key>
  <string>%full_name%</string>
  <key>com.microsoft.outlook.EmailProfile.AccountDomain</key>
  <string>my-domain</string>
  <key>com.microsoft.outlook.EmailProfile.ServerAuthentication</key>
  <string>Username and Password</string>
  <key>IntuneMAMAllowedAccountsOnly</key>
  <string>Enabled</string>
  <key>IntuneMAMUPN</key>
  <string>%full_name%</string>
</dict>
</plist>
```

You can use macros in the corresponding fields of the configuration file to replace values. **Available macros**

Macros which can be used in configuration files

Macro	Description
`%full_name%`	Full user name
`%email%`	User's main email address
`%email1%`	User's first backup email address
`%email2%`	User's second backup email address
`%mobile_phone%`	User's mobile phone number
`%phone_number%`	User's main phone number
`%phone_number1%`	User's first backup phone number

Macro	Description
%phone_number2%	User's second backup phone number
%short_name%	User name
%domain_name%	Name of user's domain
%job_title%	User's job title
%department%	Department name
%company%	Company name

9. Click **Save** to save the changes you have made.

The newly created app is displayed in the table of apps on the **iOS** tab.

If you select a large IPA file, the app may take some time to upload. Do not close the **Apps & files** section until the app is uploaded.

You can view and edit app properties by clicking the app in the list or remove the app using the **Delete** button.

Installing an app on a mobile device

To install an app on a mobile device:

1. In the main window of Kaspersky Next Expert View (on-premise), select **Asset management** → **Mobile** → **Devices**.
2. In the list of devices that opens, select the devices that you want to install apps on.
3. Click **Send command**.
4. In the **Send command** window that opens, in the **Command** field, select the **Install app** command.
5. In the **Apps** field, select the apps that you want to install on the devices.
6. Click **Send**.

   The command is sent to the devices you selected.

Updating an app installed on a device

You can update an app on an iOS MDM device in the **Send command** window or on the **Apps** tab in the device properties window.

In the **Send command** window, you can update apps on multiple devices.

To update an app on an iOS MDM device in the Send command window:

1. In the main window of Kaspersky Next Expert View (on-premise), select **Asset management** → **Mobile** → **Devices**.
2. In the list of devices that opens, select the devices that you want to update apps on.
3. Click **Send command**.
4. In the **Send command** window that opens, in the **Command** field, select the **Update app** command.
5. In the **Apps** section, select the apps that you want to update on the devices.
6. Click **Send**.

The command is sent to the devices you selected.

To update an app on an iOS MDM device in the device properties window:

1. In the main window of Kaspersky Next Expert View (on-premise), select **Asset management** → **Mobile** → **Devices**.
2. In the list of devices that opens, click the name of the device that you want to update apps on.

   The device properties window opens.
3. Select the **Apps** tab.
4. At the top of the apps list, click **Update**.
5. In the window that opens, select the apps that you want to update on the device and click **Update**.

The command is sent to the device.

Updating apps may take a few minutes. The command is executed only if a device is connected to the internet. To check whether an app has been updated, click **Refresh list**.

Removing an app from a device

You can remove an app from an iOS MDM device in the **Send command** window or on the **Apps** tab in the device properties window.

In the **Send command** window, you can remove apps from multiple devices.

To remove an app from an iOS MDM device in the Send command window:

1. In the main window of Kaspersky Next Expert View (on-premise), select **Asset management** → **Mobile** → **Devices**.
2. In the list of devices that opens, select the devices that you want to remove apps from.

3. Click **Send command**.
4. In the **Send command** window that opens, in the **Command** field, select the **Delete app** command.
5. In the **Apps** section, select the apps that you want to remove from the devices.
6. Click **Send**.

The command is sent to the devices you selected.

To remove an app from an iOS MDM device in the device properties window:

1. In the main window of Kaspersky Next Expert View (on-premise), select **Asset management** → **Mobile** → **Devices**.
2. In the list of devices that opens, click the name of the device that you want to remove apps from.

   The device properties window opens.
3. Select the **Apps** tab.
4. In the apps list, select the apps that you want to remove from the device and click **Delete**.

The command is sent to the device.

Removing apps may take a few minutes. The command is executed only if a device is connected to the internet. To check whether an app has been removed, click **Refresh list**.

Configuring roaming on an iOS MDM mobile device

To configure roaming:

1. In the main window of Kaspersky Next Expert View (on-premise), select **Asset management** → **Mobile** → **Devices**.
2. In the list of devices that opens, select the devices that you want to configure roaming settings for.
3. Click **Send command**.
4. In the **Send command** window that opens, in the **Command** field, select the **Change roaming settings** command.
5. In the **Action** section, do one of the following:
   - If you want to enable data roaming, select **Enable data roaming**.
   - If you want to disable data roaming, select **Disable data roaming**.
6. Click **Send**.

The command is sent to the devices you selected.

Viewing information about an iOS MDM device

To view information about an iOS MDM device:

1. In the main window of Kaspersky Next Expert View (on-premise), select **Asset management** → **Mobile** → **Devices**.

   The list of managed mobile devices opens.

2. To filter iOS MDM devices, click the **Operating mode** column heading and select the operating mode of the iOS MDM device you want to view information about.

   The list of iOS MDM devices is displayed.

   Depending on the database you use, searches may be case-sensitive.

3. Select the mobile device you want to view information about.

   A window with the properties of the iOS MDM device opens.

   When displaying numeric values, an error of several hundredths is possible.

The **General** tab of the properties window displays information about the connected iOS MDM device.

The following properties of iOS MDM devices running iOS 26 or later may not be displayed: **IMEI**, **Phone number**, **MEID**, **ICCID**, **Current mobile network name**, **Home mobile network name**, **Carrier settings version**, **Voice roaming enabled**, **In roaming**, **Home network country code**, **Home network code**, **Host country code**, **Current network code**.

The **Certificates** tab of the properties window displays information about the certificates installed on the selected iOS MDM device.

The **Apps** tab of the properties window displays information about the apps installed on the selected iOS MDM device.

The **Configuration profiles** tab of the properties window displays information about the configuration profiles installed on the selected iOS MDM device.

Configuring kiosk mode for iOS MDM devices

These settings apply to supervised devices.

Kiosk mode is an iOS feature that lets you limit the apps available to a device user to a single app. In this mode, a device user can open only the one app that is allowed on the device and specified in the kiosk mode settings.

Open the kiosk mode settings

To open the kiosk mode settings:

1. In the main window of Kaspersky Next Expert View (on-premise), select **Asset management** → **Policies**. In the list of group policies that opens, click the name of the policy that you want to configure.
2. In the policy properties window, select **Application settings**.
3. Select **iOS** and go to the **Restrictions** section.
4. On the **Kiosk mode** card, click **Settings**.

The **Kiosk mode** window opens.

Configure kiosk mode

To enable kiosk mode:

1. Enable the settings using the **Kiosk mode** toggle switch to activate kiosk mode on a supervised device.
2. In the **Bundle ID** field, enter the unique identifier of an app selected for kiosk mode (for example, com.apple.calculator).

   How to get the bundle ID of an app

   To get the bundle ID of a built-in iPhone or iPad app,

   Follow the instructions in the Apple documentation.

   To get the bundle ID of any iPhone or iPad app:

   1. Open the App Store.
   2. Find the required app and open its page.

      The app's URL ends with its numerical identifier (for example, https://apps.apple.com/us/app/google-chrome/id**535886823**).
   3. Copy this identifier (without the letters "id").
   4. Open the web page `https://itunes.apple.com/lookup?id=<copied identifier>`.

      This downloads a text file.
   5. Open the downloaded file and find the "bundleId" fragment in it.

   The text that directly follows this fragment is the bundle ID of the required app.

   To get the bundle ID of an app that has been added to Kaspersky Security Center:

   1. In the main window of Kaspersky Next Expert View (on-premise), select **Asset management** → **Mobile** → **Apps & files**.
   2. Click **iOS**.

      In the list of apps that opens, app identifiers are displayed in the **Bundle ID** column.

> To select a different app, you need to disable kiosk mode, save the changes to the policy, and enable kiosk mode for a new app.

The app that is selected for kiosk mode must be installed on the device. Otherwise, the device will be locked until kiosk mode is disabled.

The use of the selected app must also be allowed in the policy settings. If the use of the app is prohibited, kiosk mode will not be enabled until the selected app is removed from the list of forbidden apps.

> In some cases, kiosk mode can still be enabled even when the use of the selected app is prohibited in the policy settings.

3. Specify the settings that will be enabled on the device in kiosk mode in the corresponding section. For available settings, see the "Kiosk mode settings" section below.
4. Specify the settings that the user can edit on the device in kiosk mode in the corresponding section.
5. Click **OK**.
6. Click **Save** to save the changes you have made.

Mobile device settings are changed after the next device synchronization with the iOS MDM Server.

As a result, once the policy is applied, kiosk mode is enabled. The selected app is forced to open on a supervised device, and the use of other apps is prohibited. The selected app reopens immediately after the device is restarted.

To edit the kiosk mode settings, you need to disable kiosk mode, save changes to the policy, and then enable kiosk mode again with the new settings.

To disable kiosk mode:

1. Disable the settings using the **Kiosk mode** toggle switch to deactivate kiosk mode on a supervised device.
2. Click **OK**.
3. Click **Save** to save the changes you have made.

Mobile device settings are changed after the next device synchronization with the iOS MDM Server.

As a result, once the policy is applied, kiosk mode is disabled and the use of all apps is allowed on the supervised device.

Now, you can enable kiosk mode again with the new settings.

Kiosk mode settings

- **Auto-Lock**

  If the check box is selected, Auto-Lock is enabled. The screen is automatically locked on the device.

  If the check box is cleared, Auto-Lock is disabled.

This check box is selected by default.

- **Touch (not recommended to disable)**

  If the check box is selected, all touch input capabilities are enabled.

  If the check box is cleared, all touch input capabilities are disabled.

  This check box is selected by default.

- **AssistiveTouch**

  If the check box is selected, AssistiveTouch is enabled. The device screen is adapted to the user's unique physical needs.

  If the check box is cleared, AssistiveTouch is disabled.

  This check box is cleared by default.

- **Voice Control**

  If the check box is selected, Voice Control is enabled. The user can navigate and interact with the device using voice commands.

  If the check box is cleared, Voice Control is disabled.

  This check box is cleared by default.

- **VoiceOver**

  If the check box is selected, VoiceOver is enabled. Audible descriptions of what appears on the screen are given.

  If the check box is cleared, VoiceOver is disabled.

  This check box is cleared by default.

- **Speak Selection**

  If the check box is selected, Speak Selection is enabled. The text selected on the screen is spoken.

  If the check box is cleared, Speak Selection is disabled.

  This check box is cleared by default.

- **Volume Buttons**

  If the check box is selected, the volume buttons are enabled. The user can adjust the volume on the device.

  If the check box is cleared, the volume buttons are disabled.

  This check box is selected by default.

- **Mono Audio**

  If the check box is selected, Mono Audio is enabled. The left and right headphone channels are combined to play the same content.

  If the check box is cleared, Mono Audio is disabled.

  This check box is cleared by default.

- **Zoom**

  If the check box is selected, Zoom is enabled. The user can zoom in and out on the content on the screen.

  If the check box is cleared, Zoom is disabled.

This check box is selected by default.

- **Auto-Rotate Screen**

  If the check box is selected, Auto-Rotate Screen is enabled. Screen orientation automatically changes when the device is rotated.

  If the check box is cleared, Auto-Rotate Screen is disabled.

  This check box is selected by default.

- **Invert Colors**

  If the check box is selected, inverting colors on the screen is enabled. The displayed colors are changed to their opposite colors.

  If the check box is cleared, inverting colors on the screen is disabled.

  This check box is cleared by default.

- **Ring/Silent Switch**

  If the check box is selected, Ring/Silent Switch is enabled. The user can switch between Ring and Silent modes to mute or unmute sounds and alerts.

  If the check box is cleared, Ring/Silent Switch is disabled.

  This check box is selected by default.

- **Sleep/Wake Button**

  If the check box is selected, the Sleep/Wake button is enabled. The user can put the device to sleep or wake the device.

  If the check box is cleared, the Sleep/Wake button is disabled.

  This check box is selected by default.

Disconnecting an iOS MDM device from management

If you want to stop managing an iOS MDM device, you can disconnect it from management in Kaspersky Security Center.

> We do not recommend disconnecting the device from management by removing the management profile on an iOS MDM device, since such device may not work correctly when reconnected. To stop managing an iOS MDM device, disconnect it from the iOS MDM Server as described in this section.

To disconnect an iOS MDM device from the iOS MDM Server:

1. In the main window of Kaspersky Next Expert View (on-premise), select **Asset management → Mobile → Devices**.

   The list of managed mobile devices opens.

2. To filter iOS MDM devices, click the **Operating mode** column heading and select the operating mode of the iOS MDM device you want to disconnect.

   The list of iOS MDM devices operating in the selected mode is displayed.

3. Select the mobile device you want to disconnect.

4. Click **Delete**.

   In the list, the iOS MDM device is marked for removal. Within one minute, the device is removed from the database of the iOS MDM Server, after which it is automatically removed from the list of managed devices.

After the iOS MDM device is disconnected from management, all installed configuration profiles, the management profile, and apps for which the **Remove when management profile is deleted** option has been enabled in the iOS MDM Server settings, will be removed from the device. The iOS MDM policy will also be deleted.

You cannot prevent users from removing a management profile through the device settings.

Management of mobile device settings

This section contains information about how to remotely manage the settings of mobile devices in Kaspersky Next Expert View (on-premise).

Configuring connection to a Wi-Fi network

This section provides instructions on how to configure automatic connection to a corporate Wi-Fi network on Android and iOS MDM devices.

Connecting Android devices to a Wi-Fi network

For an Android device to automatically connect to an available Wi-Fi network and protect data during the connection, you must configure the connection settings.

To connect a mobile device to a Wi-Fi network:

1. In the main window of Kaspersky Next Expert View (on-premise), select **Asset management** → **Policies**. In the list of group policies that opens, click the name of the policy that you want to configure.

2. In the policy properties window, select **Application settings**.

3. Select **Android** and go to the **Device configuration** section.

4. On the **Wi-Fi** card, click **Settings**.

   The **Wi-Fi** window opens.

5. Enable the settings using the **Wi-Fi** toggle switch.

6. Click **Add**.

   The **Add Wi-Fi network** window opens.

7. In the **Service set identifier (SSID)** field, enter the name of the Wi-Fi network that includes the access point (SSID).

8. Select the **Connect automatically** check box if you want Android devices to automatically connect to the Wi-Fi network.

9. Select the **Hidden network** check box if you want the Wi-Fi network to be hidden in the list of available networks on the device.

   In this case, to connect to the network the user needs to manually enter the service set identifier (SSID) specified in the settings of the Wi-Fi router on the mobile device.

10. In the **Protection** section, select the type of Wi-Fi network security (open network or secure network protected with the WEP, WPA2 PSK, WPA3 PSK, WPA3-Enterprise, WPA3-Enterprise 192-bit, or 802.1.x EAP protocol).

    The 802.1.x EAP security protocol is supported only in Kaspersky Endpoint Security for Android 10.48.1.1 or later. The WEP protocol is supported only on Android 9 or earlier. The WPA3 PSK, WPA3-Enterprise, and WPA3-Enterprise 192-bit protocols are supported only on Android 10 or later.

11. If you selected the 802.1.x EAP, WPA3-Enterprise, or WPA3-Enterprise 192-bit security protocol, specify the following network protection settings:

    - **EAP method**

      Specifies an Extensible Authentication Protocol (EAP) method for network authentication. Possible values:

      - **TLS** (default)
      - **PEAP**
      - **TTLS**

    - **Method for uploading root certificate**

      Specifies the way you want to upload a root certificate. Possible values:

      - **From the list of root certificates** – Lets you select any available certificate from the drop-down list.
      - **From file** – Lets you upload a certificate file from your computer.

    - **Root certificate**

      Specifies the root certificate to be used by the Wi-Fi network.

    - **User certificate**

      Specifies the user certificate to be used by the Wi-Fi network if the TLS EAP method is selected.

The following values are available in the drop-down list:

- **Not selected** – The user certificate is not specified.
- **User certificates** – The VPN certificates that were added in the **Certificates** section and installed on the user device. If you choose this option, but no VPN certificate is installed on the device, the user certificate is not used for this Wi-Fi network.
- **SCEP profiles** – SCEP certificate profiles configured in the **SCEP and NDES** settings and used to obtain certificates.

- **Domain name**

  Specifies the constraint for the server domain name.

  If set, this Fully Qualified Domain Name (FQDN) is used as a suffix match requirement for the root certificate in SubjectAltName dNSName element(s). If a matching dNSName is found, this constraint is met.

  You can specify multiple match strings using semicolons to separate the strings. A match with any of the values is considered a sufficient match for the certificate (i.e., the OR operator is used).

  If you specify *, any root certificate is considered valid. This value is specified by default.

- **Two-factor authentication type**

  Specifies a two-factor authentication type. Possible values:

  - **Not selected** (default)
  - **MSCHAP**
  - **MSCHAPV2**
  - **GTC**

- **User ID**

  Specifies a user ID to be used to connect to the Wi-Fi network.

- **Anonymous ID**

  Specifies an anonymous identity that is different from the user identity and is used if the PEAP or TTLS method of network authentication is selected.

- **Password**

  Specifies a password for accessing the wireless network. The password will be sent in a QR code.

  Do not send a password for a confidential Wi-Fi network that should not be publicly available. The password is transmitted unencrypted along with other data to configure the device.

12. In the **Password** field, set a network access password if you selected a secure network at step 9.
13. On the **Additional** tab, select the **Use a proxy server** check box if you want to use a proxy server to connect to the Wi-Fi network.
14. If you selected **Use a proxy server**, in the **Proxy server address** and **Proxy server port** fields, enter the IP address or DNS name of the proxy server and port number, if necessary.

On devices running Android 8 or later, proxy server settings for Wi-Fi cannot be redefined with a policy. However, you can manually configure the proxy server settings for a Wi-Fi network on the mobile device.

If you are not using a proxy server to connect to a Wi-Fi network, there are no limitations on using policies to manage a Wi-Fi network connection.

15. In the **Do not use proxy server for the specified addresses** field, add web addresses that can be accessed without the use of the proxy server.

    For example, you can enter the address `example.com`. In this case, the proxy server will not be used for the addresses `pictures.example.com`, `example.com/movies`, etc. The protocol (for example, `http://`) can be omitted.

    On devices running Android 8 or later, excluding web addresses from the proxy server does not work.

16. Click **Add**.

    The added Wi-Fi network is displayed in the list of Wi-Fi networks.

    This list contains the names of suggested wireless networks.

    On personal devices running Android 10 or later, the operating system prompts the user to connect to such networks. Suggested networks don't appear in the saved networks list on these devices.

    On corporate devices and personal devices running Android 9 or earlier, after synchronizing the device with the Administration Server, the device user can select a suggested wireless network in the saved networks list and connect to it without having to specify any network settings.

    You can modify or delete Wi-Fi networks in the list of networks using the **Edit** and **Delete** buttons at the top of the list.

17. Click **OK**.

18. Click **Save** to save the changes you have made.

Mobile device settings are changed after the next device synchronization with Kaspersky Security Center.

On devices running Android 10 or later, if a user refuses to connect to the suggested Wi-Fi network, the app's permission to change Wi-Fi state is revoked. The user must grant this permission manually.

Connecting iOS MDM devices to a Wi-Fi network

For an iOS MDM device to automatically connect to an available Wi-Fi network and protect data during the connection, you must configure the connection settings.

To configure the connection of an iOS MDM device to a Wi-Fi network:

1. In the main window of Kaspersky Next Expert View (on-premise), select **Asset management** → **Policies**. In the list of group policies that opens, click the name of the policy that you want to configure.

2. In the policy properties window, select **Application settings**.

3. Select **iOS** and go to the **Device configuration** section.

4. On the **Wi-Fi** card, click **Settings**.

   The **Wi-Fi** window opens.

5. Enable the settings using the **Wi-Fi** toggle switch.

6. Click **Add**.

   The **Add Wi-Fi network** window opens.

7. In the **Service set identifier (SSID)** field, enter the name of the Wi-Fi network that includes the access point (SSID).

8. If you want iOS MDM devices to automatically connect to the Wi-Fi network, select the **Connect automatically** check box.

   > If you disable automatic connection to an existing Wi-Fi network in the policy settings, you will not be able to enable automatic connection to this network again. This is due to an issue known to Apple.

9. If you don't want iOS MDM devices to connect to Wi-Fi networks requiring preliminary authentication (captive networks), select the **Disable captive network detection** check box.

   To use a captive network, you must subscribe, accept an agreement, or make a payment. Captive networks may be deployed in cafes and hotels, for example.

10. If you want the Wi-Fi network to be hidden in the list of available networks on the iOS MDM device, select the **Hidden network** check box.

    In this case, to connect to the network the user needs to manually enter the service set identifier (SSID) specified in the settings of the Wi-Fi router on the mobile device.

11. If you want iOS MDM devices to use static MAC addresses when they connect to the Wi-Fi network, select the **Disable MAC address randomization** check box.

12. In the **Protection** section, select the type of Wi-Fi network security (open network or secure network protected with the WEP, WPA, WPA2, or WPA3 protocol).

    > On devices running iOS 15 or earlier, selecting WPA, WPA2, or WPA3 is identical and lets you connect to any network protected using WPA.

    - **Open network**. User authentication is not required.
    - **WEP**. The network is protected using Wireless Encryption Protocol (WEP).

      > WEP protection is available on devices running iOS 5 or later.

    - **WPA**. The network is protected using the WPA (Wi-Fi Protected Access) or WPA2 protocol.
    - **WPA2**. The network is protected using the WPA2 or WPA3 protocol.
    - **WPA3**. The network is protected using the WPA3 protocol.

- **Personal network (any)**. The network is protected using the WEP, WPA, WPA2, or WPA3 encryption protocol depending on the type of Wi-Fi router. An encryption key unique to each user is used for authentication.

- **WEP (corporate network)**. The network is protected using the WEP protocol with the use of a dynamic key.

- **WPA (corporate network)**. The network is protected using the WPA or WPA2 encryption protocol with the use of the 802.1X protocol.

- **WPA2 (corporate network)**. The network is protected using the WPA2 or WPA3 encryption protocol with the use of one key shared by all users (802.1X).

- **WPA3 (corporate network)**. The network is protected using the WPA3 encryption protocol with the use of one key shared by all users (802.1X).

- **Corporate network (any)**. The network is protected using the WEP, WPA, WPA2, or WPA3 protocol depending on the type of Wi-Fi router. Authentication is performed using a single encryption key shared by all users.

If you have selected any of the corporate network options, in the **EAP protocol** section you can select the types of EAP protocols (Extensible Authentication Protocol) for user identification on the Wi-Fi network.

In the **Trusted certificates** section, you can also create a list of trusted certificates for authentication of the iOS MDM device user on trusted servers.

13. In the **Authentication** section, configure the settings of the account for user authentication upon connection of the iOS MDM device to the Wi-Fi network:

    a. In the **User name** field, enter the account name for user authentication upon connection to the Wi-Fi network.

    b. In the **User ID** field, enter the user ID displayed during data transmission upon authentication instead of the user's real name.

    The user ID is designed to make the authentication process more secure, since the user name is not displayed openly, but rather transmitted via an encrypted TLS tunnel.

    c. In the **Password** field, enter the password of the account for authentication on the Wi-Fi network.

    d. If you want the user to enter the password manually upon every connection to the Wi-Fi network, select the **Prompt for password at each connection** check box.

    e. In the **Authentication certificate** drop-down list, select a certificate for user authentication on the Wi-Fi network.

    f. In the **Minimum TLS version** drop-down list, select the minimum allowed TLS version.

    g. In the **Maximum TLS version** drop-down list, select the maximum allowed TLS version.

14. If necessary, on the **Additional** tab, configure the settings for connecting to the Wi-Fi network via a proxy server:

    a. Select the **Use a proxy server** check box.

    b. Configure a connection to a proxy server:

        a. If you want to configure the connection automatically:

            - Select **Automatic**.
            - In the **PAC file URL** field, specify the URL of the proxy PAC file.
            - To allow the user to connect the mobile device to a wireless network without using a proxy server when the PAC file cannot be accessed, select the **Allow direct connection if PAC file cannot be accessed** check box.

        b. If you want to configure the connection manually:

            - Select **Manual**.
            - In the **Proxy server address** and **Proxy server port** fields, enter the IP address or DNS name of the proxy server and port number.
            - In the **User name** field, select a macro that will be used as a user name for the connection to the proxy server.
            - In the **Password** field, specify the password for the connection to the proxy server.

15. Click **Add**.

    The new Wi-Fi network is displayed in the list.

16. Click **OK**.

17. Click **Save** to save the changes you have made.

As a result, a Wi-Fi network connection will be configured on the user's iOS MDM device once the policy is applied. The user's mobile device will automatically connect to available Wi-Fi networks. Data security during a Wi-Fi network connection is ensured by the selected authentication method.

Configuring email

This section contains information on configuring mailboxes on mobile devices.

Configuring a mailbox on iOS MDM devices

These settings apply to supervised devices and devices operating in basic control mode.

To enable an iOS MDM device user to work with email, add the user's email account to the list of accounts on the iOS MDM device.

By default, the email account is added with the following settings:

- Email protocol – IMAP.
- The user can move email messages between the user's accounts and synchronize account addresses.
- The user can use any email client (other than Mail) to use email.
- The SSL connection is not used during transmission of messages.

You can edit the specified settings when adding an account.

To add an email account of the iOS MDM device user:

1. In the main window of Kaspersky Next Expert View (on-premise), select **Asset management** → **Policies**. In the list of group policies that opens, click the name of the policy that you want to configure.
2. In the policy properties window, select **Application settings**.
3. Select **iOS** and go to the **Device configuration** section.
4. On the **Email** card, click **Settings**.

   The **Email** window opens.
5. Enable the settings using the **Email** toggle switch.
6. Click **Add**.

   The **Add email account** window opens.
7. Specify the email account settings:

   - On the **General** tab, configure the following settings:

     a. In the **User name** field, specify the name of the iOS MDM device user. You can either enter a value or select a macro by clicking the + button.

     b. In the **Email address** field, specify the email address of the iOS MDM device user. You can either enter a value or select a macro by clicking the + button.

     c. In the **Account description** field, enter a description of the user's email account.

     d. In the **Email protocol** field, select one of the following protocols:

     - **POP**
     - **IMAP**

     e. If you selected **IMAP**, specify the IMAP path prefix in the **IMAP path prefix** field.

     The IMAP path prefix must be entered using uppercase letters (for example: GMAIL for Google Mail).

f. In the **Incoming mail server settings** and **Outgoing mail server settings** sections, configure the server connection settings:

- In the **Server address** field, specify names of hosts or IP addresses of incoming and outgoing mail servers.
- In the **Server port** fields, specify the port numbers of incoming and outgoing mail servers.

To configure optional settings for the incoming and outgoing mail servers, click **More settings** and do the following:

- In the **User name** field, specify the name of the user's account for authorization on the incoming and outgoing mail servers. You can either enter a value or select a macro by clicking the + button.
- In the **Authentication type** field, select the type of authentication of the user's email account on the incoming and outgoing mail servers.
- In the **Password** field, specify the account password for authenticating on incoming and outgoing mail servers protected using the selected authentication method.
- If you want to use the SSL (Secure Sockets Layer) data transport protocol, select the **Use SSL connection** check box.
- If you want to use the same password for user authentication on the incoming and outgoing mail servers, select the **Use the same password for incoming and outgoing mail servers** check box.

- On the **Additional** tab, configure the additional settings of the email account:

a. In the **Permissions** section, select or clear the following check boxes, if necessary:

- **Allow syncing recent addresses**

  Moving email messages between accounts.

  If the check box is selected, the user can move email messages from one account to another.

  If the check box is cleared, the user is prohibited from moving email messages from one account to another.

  This check box is selected by default.

  > If you want to prohibit saving, moving, and sharing attachments from a corporate mailbox, clear the **Allow movement of messages between accounts (including work and personal accounts)** check box and select the Prohibit non-managed apps from using documents from managed apps and Prohibit managed apps from using documents from non-managed apps check boxes.

- **Allow movement of messages between accounts (including work and personal accounts)**

  Synchronization of email addresses between accounts.

  If the check box is selected, when creating messages the user can use another email account's address history.

  If this check box is cleared, used email addresses are not synchronized. When creating a message, the user of an iOS MDM device cannot use another email account's address history.

  This check box is selected by default.

- **Allow Mail Drop**

  Use of the Mail Drop service to forward large attachments.

  If the check box is selected, the user can use Mail Drop.

  If the check box is cleared, the user cannot use Mail Drop.

  This check box is cleared by default.

- **Allow using only the Mail app**

  Use of only the standard iOS mail client for processing messages.

  If the check box is selected, the user can use email only in the standard iOS email client.

  If the check box is cleared, the user can use email both in the standard iOS email client and in other apps.

  This check box is cleared by default.

b. In the **Signature** and **Encryption** sections, configure the settings for signing and encrypting outgoing mail using the S/MIME protocol in the Mail app.

   S/MIME is a protocol for transmitting digitally signed encrypted messages. S/MIME provides cryptographic security capabilities such as authentication, message integrity control, and non-repudiation of origin (using digital signatures). The protocol also helps improve the confidentiality and security of data in email messages by using encryption.

   - **Sign messages**

     Digital signature of outgoing messages in the Mail app.

     If the check box is selected, outgoing messages are signed with a digital signature using the S/MIME protocol. A digital signature confirms the authenticity of the sender and indicates that the contents of the message have not been modified during transmission to the recipient. A recipient certificate (public key) must be selected for a message signature.

     This check box is cleared by default.

   - **Signing certificate for outgoing messages**

     Certificate for signing outgoing messages with a digital signature using the S/MIME protocol. The digital signature guarantees that the message was sent by the iOS MDM device user. You can add certificates in the **Certificate management** settings of the policy or in the **Certificates** section of Kaspersky Next Expert View (on-premise).

     This drop-down list is available only if the **Sign messages** check box is selected.

   - **Encrypt messages by default**

     Encryption of outgoing messages in the Mail app.

     If the check box is selected, outgoing messages are encrypted by default using the S/MIME protocol. A recipient certificate (public key) must be selected for sending encrypted messages. If a recipient certificate is not installed, messages cannot be encrypted. Encrypted messages can be viewed only by users whose devices have a certificate installed.

     This check box is cleared by default.

   - **Encryption certificate**

     Encryption certificate for encrypting outgoing messages using the S/MIME protocol. Encryption keeps messages confidential during transmission and storage. You can add certificates in the **Certificate management** settings of the policy or in the **Certificates** section of Kaspersky Next Expert View (on-premise).

This drop-down list is available only if the **Encrypt messages by default** check box is selected.

- **Show toggle button for encrypting selected messages**

  Display of the icon in the Mail app in the **To** field for sending encrypted messages.

  If this check box is selected, the mobile device user can encrypt individual messages by clicking the icon.

  If the check box is cleared, the icon for encrypting messages is not displayed. In this case, the **Encrypt messages by default** check box determines whether outgoing mail is encrypted.

- If necessary, in the **Per App VPN** section, configure Per App VPN.

8. Click **Save**.

   The new email account appears in the list.

   You can modify or delete email accounts in the list using the **Edit** and **Delete** buttons at the top of the list.

9. Click **OK**.

10. Click **Save** to save the changes you have made.

Mobile device settings are changed after the next device synchronization with the iOS MDM Server.

As a result, once the policy is applied, email accounts from the list are added on the user's mobile device.

We recommend closing and opening the Settings app on the iOS MDM device after you configure a mailbox.

Configuring an Exchange mailbox on iOS MDM devices

These settings apply to supervised devices and devices operating in basic control mode.

To allow an iOS MDM device user to use corporate email, calendar, contacts, notes, and tasks, add the user's Exchange ActiveSync account on the Microsoft Exchange server.

By default, an account with the following settings is added on the Microsoft Exchange server:

- Email is synchronized once per week.
- The user can move messages between the user's accounts and synchronize account addresses.
- The user can use any email clients (other than Mail) to use email.
- The SSL connection is not used during transmission of messages.

You can edit the specified settings when adding the Exchange ActiveSync account.

To add an Exchange ActiveSync account of an iOS MDM device user:

1. In the main window of Kaspersky Next Expert View (on-premise), select **Asset management** → **Policies**. In the list of group policies that opens, click the name of the policy that you want to configure.

2. In the policy properties window, select **Application settings**.

3. Select **iOS** and go to the **Device configuration** section.

4. On the **Exchange ActiveSync** card, click **Settings**.

   The **Exchange ActiveSync** window opens.

5. Enable the settings using the **Exchange ActiveSync** toggle switch.

6. Click **Add**.

   The **Add Exchange ActiveSync account** window opens.

7. Specify the Exchange ActiveSync settings:

   - On the **General** tab, specify the user's data:

     - In the **Account name** field, enter the account name for authorization on the Microsoft Exchange server. You can either enter a value or select a macro by clicking the + button.

     - In the **Exchange ActiveSync server address** field, enter the DNS name or IP address of the Microsoft Exchange server.

     - Settings in the **User credentials** section:

       - In the **User domain** field, enter the name of the iOS MDM device user's domain. You can either enter a value or select a macro by clicking the + button.

       - In the **User name** field, enter the name of the iOS MDM device user. You can either enter a value or select a macro by clicking the + button.

         If you leave this field blank, Kaspersky Mobile Devices Protection and Management prompts the user to enter the user name when applying the policy on the iOS MDM device.

       - In the **Email address** field, specify the email address of the iOS MDM device user. You can either enter a value or select a macro by clicking the + button.

     - Settings in the **Authentication** section:

       - In the **Password** field, enter the password of the Exchange ActiveSync account for authorization on the Microsoft Exchange server.

       - In the **Authentication certificate** drop-down list, select the certificate used for authenticating the iOS MDM device user on the Microsoft Exchange server. You can add certificates in the **Certificate management** settings of the policy or in the **Certificates** section of Kaspersky Next Expert View (on-premise).

- On the **Additional** tab, configure the additional settings of the Exchange ActiveSync account:
  - In the **Email synchronization** section, in the **Synchronization period** drop-down list, select the time interval for which email is automatically synchronized and stored on the iOS MDM device. The longer the email synchronization period, the more free space required in the memory of the mobile device. Messages that have not been synchronized are not available without an internet connection. The default value is **1 week**.
  - In the **Restrictions** section, select or clear the following check boxes, if necessary:
    - **Allow movement of messages between accounts (including work and personal accounts)**

      Moving email messages between accounts.

      If the check box is selected, the user can move email messages from one account to another.

      If the check box is cleared, the user is prohibited from moving email messages from one account to another.

      This check box is selected by default.

      > If you want to prohibit saving, moving, and sharing attachments from a corporate mailbox, clear the **Allow movement of messages between accounts (including work and personal accounts)** check box and select the Prohibit non-managed apps from using documents from managed apps and Prohibit managed apps from using documents from non-managed apps check boxes.

    - **Allow syncing recent addresses**

      Synchronization of email addresses between accounts.

      If the check box is selected, when creating messages the user can use another email account's address history.

      If this check box is cleared, used email addresses are not synchronized. When creating a message, the user of an iOS MDM device cannot use another email account's address history.

      This check box is selected by default.

    - **Allow using only the Mail app**

      Use of only the standard iOS mail client for processing messages.

      If the check box is selected, the user can use email only in the standard iOS email client.

      If the check box is cleared, the user can use email both in the standard iOS email client and in other apps.

      This check box is cleared by default.

    - **Use SSL connection**

      Select this check box to use the SSL (Secure Sockets Layer) data transport protocol to secure the transmission of data.

      This check box is selected by default.

- In the **Signature and encryption** section, configure the settings for signing and encrypting outgoing mail using the S/MIME protocol in the Mail app. *S/MIME* is a protocol for transmitting digitally signed encrypted messages. S/MIME provides cryptographic security capabilities such as authentication, message integrity control, and non-repudiation of origin (using digital signatures). The protocol also uses encryption to help improve the level of confidentiality and security of data in email messages.

  - **Sign messages**

    Digital signature of outgoing messages in the Mail app.

    If the check box is selected, outgoing messages are signed with a digital signature using the S/MIME protocol. A digital signature confirms the authenticity of the sender and indicates that the contents of the message have not been modified during transmission to the recipient. A recipient certificate (public key) must be selected for a message signature.

    This check box is cleared by default.

  - **Signing certificate for outgoing messages**

    Certificate for signing outgoing messages with a digital signature using the S/MIME protocol. The digital signature guarantees that the message was sent by the iOS MDM device user. You can add certificates in the **Certificate management** settings of the policy or in the **Certificates** section of Kaspersky Next Expert View (on-premise).

    This drop-down list is available only if the **Sign messages** check box is selected.

  - **Encrypt messages by default**

    Encryption of outgoing messages in the Mail app.

    If the check box is selected, outgoing messages are encrypted by default using the S/MIME protocol. A recipient certificate (public key) must be selected for sending encrypted messages. If a recipient certificate is not installed, messages cannot be encrypted. Encrypted messages can be viewed only by users whose devices have a certificate installed.

    This check box is cleared by default.

  - **Encryption certificate**

    Encryption certificate for encrypting outgoing messages using the S/MIME protocol. Encryption keeps messages confidential during transmission and storage. You can add certificates in the **Certificate management** settings of the policy or in the **Certificates** section of Kaspersky Next Expert View (on-premise).

    This drop-down list is available only if the **Encrypt messages by default** check box is selected.

  - **Show toggle button for encrypting selected messages**

    Display of the icon in the Mail app in the **To** field for sending encrypted messages.

    If this check box is selected, the mobile device user can encrypt individual messages by clicking the icon.

    If the check box is cleared, the icon for encrypting messages is not displayed. In this case, the **Encrypt messages by default** check box determines whether outgoing mail is encrypted.

- If necessary, in the **Per App VPN** section, configure Per App VPN.

8. Click **Add**.

The new Exchange ActiveSync account appears in the list.

You can modify or delete Exchange ActiveSync accounts in the list using the **Edit** and **Delete** buttons at the top of the list.

9. Click **OK**.
10. Click **Save** to save the changes you have made.

Mobile device settings are changed after the next device synchronization with the iOS MDM Server.

As a result, once the policy is applied, Exchange ActiveSync accounts from the compiled list are added on the user's mobile device.

Configuring an Exchange mailbox on Android devices

To work with corporate mail, contacts, and the calendar on the mobile device, you can configure the Exchange mailbox settings for the standard Samsung Email app.

An Exchange mailbox can be configured only for Samsung devices running Android 9 or earlier.

To configure an Exchange mailbox on a user's mobile device:

1. In the main window of Kaspersky Next Expert View (on-premise), select **Asset management** → **Policies**. In the list of group policies that opens, click the name of the policy that you want to configure.
2. In the policy properties window, select **Application settings**.
3. Select **Android** and go to the **Samsung Knox settings** section.
4. On the **Exchange ActiveSync** card, click **Settings**.

   The **Exchange ActiveSync** window opens.
5. Enable the settings using the **Exchange ActiveSync** toggle switch.
6. In the **Server address** field, enter the IP address or DNS name of the server hosting the mail server.
7. In the **Domain name** field, enter the name of the mobile device user's domain on the corporate network.
8. In the **Synchronization interval** drop-down list, select the interval for mobile device synchronization with the Microsoft Exchange server.
9. To use the SSL (Secure Sockets Layer) data transport protocol, select the **Use SSL connection** check box. The SSL protocol uses encryption and certificate-based authentication for secure data transfer. This check box is selected by default.
10. To use digital certificates to protect data transfer between the user's mobile device and the Microsoft Exchange server, select the **Verify server certificate** check box. The server certificate is verified to have been issued from the trusted root certificate. This check box is selected by default.
11. Click **Save** to save the changes you have made.

Mobile device settings are changed after the next device synchronization with Kaspersky Security Center.

Configuring protection levels in Kaspersky Security Center

These settings apply to Android devices.

To configure rules for assigning protection levels in Kaspersky Security Center:

1. In the main window of Kaspersky Next Expert View (on-premise), select **Asset management** → **Policies**. In the list of group policies that opens, click the name of the policy that you want to configure.
2. In the policy properties window, select **Application settings**.
3. Select **Android** and go to the **KES for Android settings** section.
4. On the **Severity settings for device protection level** card, click **Settings**.

   The **Severity settings for device protection level** window opens.
5. Enable the settings using the **Severity settings for device protection level** toggle switch.
6. Select the **OK**, **Warning**, or **Critical** protection level for each of the following conditions:

   - **Real-time protection is not running**

     Drop-down list where you can select the protection level of a mobile device on which real-time protection is not running.

     Real-time protection lets you detect threats in files being opened, as well as scan new apps and stop device infections in real time.

     Real-time protection may fail to run for the following reasons:

     - The user declined to use Kaspersky Security Network on the mobile device in the Anti-Malware settings of Kaspersky Endpoint Security for Android.
     - The user did not grant the app access to manage all files.

     If real-time protection is not running, you can also configure restrictions on operation of the mobile device in the **Compliance Control** settings of the policy.

   - **Web Protection and Web Control are not running**

     Drop-down list where you can select the protection level of a mobile device on which Web Protection and Web Control are not running.

     Web Protection lets you scan websites and block malicious and phishing websites.

     Web Control lets you configure user access to specific websites and categories of websites.

     Web Protection and Web Control may fail to run for the following reasons:

     - The user disabled Web Protection on the mobile device in the Kaspersky Endpoint Security for Android settings.
     - The user did not enable Kaspersky Endpoint Security for Android as an Accessibility feature.
     - The Ignore battery optimization permission has not been granted.
     - The Web Protection Statement has not been accepted.

If Web Protection and Web Control are not running, you can also configure restrictions on the operation of the mobile device in the **Compliance Control** settings of the policy.

- **App Control is not running**

  Drop-down list where you can select the protection level of a mobile device on which App Control is not running.

  App Control lets you block apps from running on mobile devices if those apps do not meet the corporate security requirements.

  App Control may not run if the user did not enable the app as an Accessibility feature on devices running Android 5 or later.

  If App Control is not running, you can also configure restrictions on the operation of the mobile device in the **Compliance Control** settings of the policy.

- **Device lock is not available**

  Drop-down list where you can select the protection level of a mobile device on which device lock is not available.

  The device may be locked in the following cases:

  - The Anti-Theft command is received.
  - The SIM card is replaced or the device is turned on without a SIM card.
  - An attempt is made to remove Kaspersky Endpoint Security for Android while app removal protection is enabled.

  Device lock may be unavailable for the following reasons:

  - The user did not set the app as a device administrator.
  - The user did not enable the app as an Accessibility service on devices running Android 7 or later.
  - The user did not enable the app to overlay other windows on devices running Android 7 or later.

- **Device location is not available**

  Drop-down list where you can select the protection level of a mobile device whose location cannot be determined.

  The location is determined after the **Locate device** command is received.

  Locating the device may be unavailable for the following reasons:

  - The user did not grant the device locate permission to the app.
  - The user turned off the GPS module in the device settings.

- **Versions of the Kaspersky Security Network Statement do not match**

  Drop-down list where you can select the protection level of a mobile device if the version of the Kaspersky Security Network Statement accepted by the administrator does not match the version accepted by the device user. Statistics not listed in the version of the Statement accepted by the user are not sent to Kaspersky Security Network.

- **Versions of the Marketing Statement do not match**

  Drop-down list where you can select the protection level of a mobile device if the version of the Statement regarding data processing for marketing purposes accepted by the administrator does not match the version accepted by the device user. Data is not transferred to third-party services.

  > The list of third-party services can be found in the Statement regarding data processing for marketing purposes.

7. Click **OK**.
8. Click **Save** to save the changes you have made.

Mobile device settings are changed after the next device synchronization with Kaspersky Security Center.

For more information about default values, reasons, and conditions for assigning protection levels, please refer to the Mobile device protection levels section.

Managing app configurations

This section provides instructions on how to manage settings and edit configurations of the apps installed on your users' devices.

Managing Google Chrome settings

> These settings apply to corporate devices and devices with a corporate container.

To configure Google Chrome settings:

1. In the main window of Kaspersky Next Expert View (on-premise), select **Asset management** → **Policies**. In the list of group policies that opens, click the name of the policy that you want to configure.
2. In the policy properties window, select **Application settings**.
3. Select **Android** and go to the **App configuration** section.
4. On the **Google Chrome settings** card, click **Settings**.

   The **Google Chrome settings** window opens.
5. Enable the settings using the **Google Chrome settings** toggle switch.

   > The toggle switch in this card does not enable or disable the corresponding functionality on devices. Enabling the toggle switch lets you configure custom settings. Disabling the toggle switch lets you use default settings.

6. Configure the required settings.

7. Click **OK**.

8. Click **Save** to save the changes you have made.

Mobile device settings are changed after the next device synchronization with Kaspersky Security Center.

Manage content settings

On the **Content** tab, you can manage the following settings:

- In the **Cookies** section:
  - **Default mode**

    Default cookie settings.

    Available options:
    - **Allow all websites to save local data** (default)
    - **Prohibit all websites from saving local data**
    - **Configure settings for selected websites**
    - **Do not configure cookie settings**
  - **Exceptions**

    Exceptions from the websites that are prohibited from or allowed to save local data.

    For more information on URL patterns, see the Chrome enterprise documentation.
  - **Websites**

    The websites that are prohibited from or allowed to save local data.

    For more information on URL patterns, see the Chrome enterprise documentation.
- In the **JavaScript** section:
  - **Default mode**

    Default JavaScript settings.

    Available options:
    - **Allow JavaScript on all websites** (default)
    - **Prohibit JavaScript on all websites**
  - **Exceptions**

    Exceptions from the websites that are prohibited from or allowed to use JavaScript.

    For more information on URL patterns, see the Chrome enterprise documentation.
- In the **Pop-ups** section:
  - **Default mode**

    Default pop-up setting.

Available options:

- **Allow pop-ups on all websites**. Lets all sites open pop-up windows. This value is selected by default.
- **Prohibit pop-ups on all websites**. Prohibits all sites from opening pop-up windows.

> Only pop-ups included into the Google abusive pop-ups database will be blocked.

- **Exceptions**

  Exceptions from the websites that are prohibited from or allowed to display pop-up windows.

- In the **Location tracking** section:
  - **Default mode**

    The default geographic location settings.
    Available options:
    - **Allow all websites to track user's location**
    - **Prohibit all websites from tracking user's location**
    - **Ask whenever website wants to track user's location** (default)

Manage proxy settings

On the **Proxy** tab, you can manage the following settings:

- **Default mode**

  Proxy settings for Google Chrome and ARC-apps.
  Available options:
  - **Never use proxy**. Prohibits use of proxies and all other proxy settings are ignored.
  - **Detect proxy settings automatically**. Detects proxy settings automatically and all other options are ignored.
  - **Use PAC file**. Uses the proxy PAC file specified in the **PAC file URL** field.
  - **Use fixed proxy servers**. Uses the data specified in the **Proxy server URL** field and **Exceptions** list.
  - **Use system proxy settings**. Uses the system proxy settings. This option is selected by default.
- **PAC file URL**

  A URL to a proxy PAC file.
- **Proxy server URL**

  A URL of the proxy server.
- **Exceptions**

  A list of hosts for which the proxy will be bypassed.

Manage search settings

On the **Search** tab, you can manage the following settings:

- In the **Touch to Search** section:
  - **Enable Touch to Search**

    Selecting or clearing this check box specifies whether the device user is allowed to use Touch to Search and turn the feature on or off.

    This check box is selected by default.

- In the **Search provider** section:
  - **Operating mode**

    This option lets you determine whether to configure a search provider that will be used on user devices.

    If you select **Enable default search provider**, you can specify search provider settings.

  - **Search provider name**

    The default search provider name.

    Examples:

    ```
    Google
    Yandex
    Mail.ru
    Bing
    ```

  - **Search URL**

    The URL of the search engine used during default searches.

    Examples:

    ```
    https://www.google.com/search?q={searchTerms}
    https://ya.ru/search/?text={searchTerms}
    https://go.mail.ru/search?q={searchTerms}
    https://www.bing.com/search?q={searchTerms}
    ```

  - **Suggest URL**

    The URL of the search engine to provide search suggestions.

    Examples:

    ```
    https://www.google.com/complete/search?client=chrome&hl=ru&q={searchTerms}
    https://suggest.yandex.net/suggest-ff.cgi?part={searchTerms}
    https://go.mail.ru/suggest?q={searchTerms}
    https://api.bing.com/osjson.aspx?query={searchTerms}
    ```

  - **Icon URL**

    > Use only legitimate and trusted sources. By configuring the settings in this field, you are solely responsible for any potential risks and consequences associated with using unreliable sources.

    The URL of the default search provider's favicon.

    Examples:

```
https://www.google.com/favicon.ico
https://ya.ru/favicon.ico
https://go.mail.ru/favicon.ico
https://www.bing.com/sa/simg/bing_p_rr_teal_min.ico
```

- **Encodings**

  Character encodings supported by the search provider. The supported encodings are:

  - UTF-8
  - UTF-16
  - GB2312
  - ISO-8859-1

- **Alternate URLs**

  A list of alternate URLs to retrieve search terms from the search engine.

- **Image search URL**

  The URL of the search engine used for image search.

- **New tab URL**

  The URL of the search engine used to provide a New Tab page.

  Examples:

  ```
  https://www.google.com
  https://ya.ru
  https://go.mail.ru
  https://www.bing.com
  ```

- **Parameters for search URL that uses POST**

  URL parameters when searching a URL with the POST method. The parameters are comma-separated key-value pairs. If a value is a template parameter, for example, '{searchTerms}', it is replaced with real search terms. For example:

  ```
  q={searchTerms},ie=utf-8,oe=utf-8
  ```

- **Parameters for suggest URL that uses POST**

  URL parameters for search suggestions using the POST method. The parameters are comma-separated key-value pairs. If a value is a template parameter, for example, '{searchTerms}', it is replaced with real search terms. For example:

  ```
  q={searchTerms},ie=utf-8,oe=utf-8
  ```

- **Parameters for image URL that uses POST**

  URL parameters for image search using the POST method. The parameters are comma-separated key-value pairs. If a value is a template parameter, for example, '{imageThumbnail}', it is replaced with the real image thumbnail. For example:

  ```
  content={imageThumbnail},url={imageURL},sbisrc={SearchSource}
  ```

Manage security settings

On the **Security** tab, you can manage the following settings:

- In the **Google Safe Browsing and SafeSearch** section:
  - **Safe Browsing operating mode**

    Google Safe Browsing protection level.

    Available options:
    - **No protection**. Disables Google Safe Browsing completely.
    - **Standard protection.** Makes Google Safe Browsing always enabled in standard protection mode. This option is selected by default.
    - **Enhanced protection**. Makes Google Safe Browsing always enabled in enhanced protection mode, but device user browsing experience data will be sent to Google.
  - **Force SafeSearch**

    Selecting or clearing this check box specifies whether Google Search queries will be performed via Google SafeSearch.

    This check box is cleared by default.
  - **Disable proceeding from the Safe Browsing warning page**

    Selecting or clearing this check box specifies whether the device user is allowed to proceed to the flagged site on Google Safe Browsing warnings, such as malware and phishing. The restriction does not apply to issues related to an SSL certificate, such as invalid or expired certificates.

    This check box is cleared by default.
- In the **Blocked websites** section:
  - **Block access to these websites**

    A list of forbidden URLs. You can also set URL patterns, for example: `[*.]example.com`.
  - **Exceptions**

    A list of URLs that are exceptions to the list specified in **Block access to these websites**. You can also set URL patterns, for example: `[*.]example.com`.
- In the **Passwords and autofill** section:
  - **Enable saving passwords**

    Selecting or clearing the check box specifies whether Google Chrome will remember the passwords the device user enters and also offer them the next time the device user signs in.

    This check box is selected by default.
  - **Enable autofill for addresses**

    Autofill settings for addresses.

    If the check box is selected, the device user is allowed to manage autofill for addresses in the user interface.

If the check box is cleared, autofill never suggests or fills in address information, nor does it save additional address information that the device user submits while browsing the web.

This check box is selected by default.

- **Enable autofill for bank cards**

  Autofill settings for bank cards.

  If the check box is selected, the device user is allowed to manage autofill suggestions for bank cards in the user interface.

  If the check box is cleared, autofill never suggests or fills in bank card information, nor does it save additional bank card information that the device user submits while browsing the web.

  This check box is selected by default.

- In the **Network** section:

  - **Minimum TLS version**

    Minimum allowed TLS version.

    Available options:

    - **TLS 1.0** (default)
    - **TLS 1.1**
    - **TLS 1.2**

  - **Enable network prediction**

    Selecting or clearing this check box specifies whether Google Chrome will predict such network actions as DNS prefetching, TCP and SSL preconnection and prerendering of webpages.

    If the check box is cleared, network prediction is disabled, but the device user can enable it.

    This check box is selected by default.

Manage additional settings

On the **Additional settings** tab, you can manage the following settings:

- In the **Bookmarks** section:

  - **Managed bookmarks**

    An admin-managed list of bookmarks. The list is a dictionary with `name` and `url` keys. In other words, the key holds a bookmark's name and target. You can also set up a subfolder with a `children` key, which also has a list of bookmarks.

    By default, the folder name for managed bookmarks is "Managed bookmarks". You can change it by adding a new sub-dictionary. To do this, specify the `toplevel_name` key with the required folder name as its value.

    If you enter an incomplete URL as a bookmark's target, Google Chrome will substitute it with a URL as if it was submitted through the address bar. For example, `kaspersky.com` becomes `https://www.kaspersky.com`.

    For example:

    With no "children" key:

    ```
    "Managed bookmarks":
    [
    ```

```
  {
    //Changes the default folder name
    "toplevel_name": "Advanced MDM in Kaspersky Next Expert View (on-premise)"
  },
  {
    //Adds a bookmark to the managed bookmarks folder
    "name": "Help",
    "url": "https://support.kaspersky.com/help/KSMM/7.0/en-US/254248.htm"
  },
  {
    "name": "Official website",
    "url": "https://www.kaspersky.ru/enterprise-security/mobile"
  }
]
```

With "children" key:

```
"Managed bookmarks":
[
  {
    "toplevel_name": "Company bookmarks"
  },
  {
    "name": "Homepage",
    "url": "mydomain.com"
  },
  {
    "children": [
      {
        "name": "HR",
        "url": "mydomain.com/hr"
      },
      {
        "name": "Submit a ticket",
        "url": "mydomain.com/it-support"
      }
    ],
    "name": "Internal URLs"
  },
  {
    "name": "Android resources",
    "url": "https://developer.android.com/"
  }
]
```

- **Enable bookmark editing**

  Selecting or clearing this check box specifies whether the device user is allowed to add, remove, or modify bookmarks.

  This check box is selected by default.

- In the **History and Incognito mode** section:

  - **Availability of Incognito mode**

    Specifies whether the device user can enable Incognito mode in Google Chrome.

Available options:

- **Incognito mode is available** (default)
- **Incognito mode is disabled**

- **Disable saving browser history**

  Selecting or clearing this check box specifies whether browsing history is saved and tab syncing is on.

  This check box is cleared by default.

- In the **Other** section:

  - **Restricted Mode for YouTube**

    Minimum required Restricted Mode level for YouTube.

    Available options:

    - **Do not enforce Restricted Mode**. Specifies that Google Chrome does not force Restricted Mode. However, external policies might still enforce Restricted Mode. This option is selected by default.
    - **Enforce at least Moderate Restricted Mode**. Lets a device user enable the Moderate Restricted Mode on YouTube.
    - **Enforce Strict Restricted Mode**. Makes Strict Restricted Mode on YouTube always active.

  - **Google Translate operating mode**

    Translation functionality.

    Available options:

    - **Always offer translation**. Shows the integrated translation notification and a translate option at the top of the screen.
    - **Never offer translation**. Disables all built-in translation functionality.
    - **Prompt the user for action**. Lets the user decide whether to use translation functionality. This option is selected by default.

  - **Enable alternate error pages**

    Selecting the check box specifies whether Google Chrome is allowed to use built-in error pages, such as "Page not found".

    This check box is cleared by default.

  - **Enable printing**

    Selecting or clearing this check box specifies whether the device user is allowed to print in Google Chrome.

    This check box is selected by default.

  - **Enable search suggestions**

    Selecting or clearing this check box specifies whether search suggestions are enabled in Google Chrome's address bar.

    This check box is selected by default.

Managing Exchange ActiveSync for Gmail

These settings apply to corporate devices and devices with a corporate container.

The **Exchange ActiveSync** settings let you manage Exchange ActiveSync for the Gmail app.

To configure Exchange ActiveSync settings:

1. In the main window of Kaspersky Next Expert View (on-premise), select **Asset management** → **Policies**. In the list of group policies that opens, click the name of the policy that you want to configure.
2. In the policy properties window, select **Application settings**.
3. Select **Android** and go to the **App configuration** section.
4. On the **Exchange ActiveSync** card, click **Settings**.
   The **Exchange ActiveSync** window opens.
5. Enable the settings using the **Exchange ActiveSync** toggle switch.
6. Specify the Exchange ActiveSync settings:
   - On the **General** tab, specify the following settings:
     - **Exchange ActiveSync server address**

       The Exchange ActiveSync email server URL. You don't need to use `http://` or `https://` in front of the URL.
     - Settings in the **User credentials** section:
       - **Device ID**

         A string used by a Kaspersky Security Center proxy or a third-party gateway to identify the device and connect it to Exchange ActiveSync. You can either enter a value or select a macro by clicking the + button.
       - **User name**

         The user name that will be used to pull the user name from Microsoft Active Directory. It might be different from the user's email address. You can either enter a value or select a macro by clicking the + button.
       - **Email address**

         The email address that will be used to pull the user's email address from Microsoft Active Directory. You can either enter a value or select a macro by clicking the + button.
     - Settings in the **Authentication** section:
       - **Authentication type**

The authentication type used to verify a device user's email credential. Possible values:

- **Modern token-based authentication**. Uses a token-based identity management method. This value is selected by default.
- **Basic authentication**. Prompts the device user for their password and stores it for future use.

- **Authentication certificate**

  The authentication certificate used to verify user identity, simplify user authentication, and ensure data security.

  The following values are available in the drop-down list:

  - **Not selected**. The authentication certificate is not specified.
  - **User certificates**. The list of Mail certificates configured in the **Asset management** → **Mobile** → **Certificates** section.
  - **SCEP profiles**. The list of SCEP certificate profiles configured in the **SCEP and NDES** card of the **Device configuration** section of the policy and used to obtain certificates.

- On the **Additional** tab, specify the following settings:
  - Settings in the **Email synchronization** section:
    - **Synchronization period**

      The default time interval for synchronization of mail items between Exchange ActiveSync servers and Gmail. Possible values:

      - 1 day
      - 3 days
      - 1 week (default)
      - 2 weeks
      - 1 month

  - Settings in the **Restrictions** section:
    - **Use SSL connection**

      Selecting or clearing this check box specifies whether communication to the server port specified in the **Exchange ActiveSync server address** field will use the SSL protocol.

      This check box is selected by default.

    - **Disable SSL certificate verification**

      Selecting or clearing this check box specifies whether validation checks on SSL certificates used on Exchange ActiveSync servers will be performed. Performing a check is useful if certificates are self-signed.

      This check box is cleared by default.

    - **Allow unmanaged accounts**

Selecting or clearing the check box specifies whether the device user is allowed to add other accounts to the Gmail app.

This check box is selected by default.

- Settings in the **Signature** section:
  - **Default email signature**

    The default email signature that is automatically added at the bottom of emails.

7. Click **OK**.
8. Click **Save** to save the changes you have made.

Mobile device settings are changed after the next device synchronization with Kaspersky Security Center.

Configuring other apps

These settings apply to corporate devices and devices with a corporate container.

The **Configure other apps** settings let you configure installed apps that support configurations.

To add app configurations:

1. In the main window of Kaspersky Next Expert View (on-premise), select **Asset management** → **Policies**. In the list of group policies that opens, click the name of the policy that you want to configure.
2. In the policy properties window, select **Application settings**.
3. Select **Android** and go to the **App configuration** section.
4. On the **Configure other apps** card, click **Settings**.

   The **Configure other apps** window opens.
5. Enable the settings using the **Configure other apps** toggle switch.
6. Click **Add**.

   The **Add app configuration** window opens.
7. In the **Method for adding configuration** drop-down list, select how to add configuration:
   - **App package uploaded by administrator**

     When adding an app configuration by using an APK file from your computer, you must select a file saved on your computer.

     After that, you can view the description for each setting of the configuration. These descriptions are part of the configuration file.

     Configuration keys uploaded from the app package cannot be deleted. If you want to add a new setting to the uploaded configuration, click the **Add setting** button.

- **Kaspersky Security Center installation package**

  When adding an app configuration using an installation package from Kaspersky Security Center, you need to select the app from a list of mobile app packages.

  After that, you can view the description for each setting of the configuration. These descriptions are part of the configuration file.

  Settings of configurations added using installation packages cannot be deleted.

- **Manual configuration**

  When this method is selected, click the **Add setting** button to add a new setting to the configuration.

8. In the **Configuration data** section, specify the following settings:

- **App name**

  Name of the app to which the configuration is to be applied.

  When importing a configuration from an APK file or an installation package, the value is inserted automatically.

- **Package name**

  Name of the package to which the configuration is to be applied.

  How to get the package name of an app

  To get the name of an app package:

  1. Open Google Play.
  2. Find the app and open its page.

     The app's URL ends with its package name (for example, https://play.google.com/store/apps/details?id=**com.android.chrome**).

  To get the name of an app package that has been added to Kaspersky Security Center:

  1. In the main window of Kaspersky Next Expert View (on-premise), select **Asset management** → **Mobile** → **Apps & files**.
  2. Select **Android** → **Apps**.

     In the list of apps that opens, app identifiers are displayed in the **Package name** column.

  When importing a configuration from an APK file or an installation package, the value is inserted automatically.

  You can add only one configuration for each package name.

- **Version**

  Version of the app, that the created configuration will be based on.

  When importing a configuration from an APK file or installation package, the value is inserted automatically.

- **Comment**

  An optional comment.

An example of configured basic parameters for the Microsoft Outlook app.

Microsoft Outlook app configuration

Configuration key	Description	Type	Value	Defau value
`com.microsoft.outlook.EmailProfile.EmailAccountName`	Username	String	The username that will be used to pull the username from Microsoft Active Directory. It might be different from the user's email address. You can either enter a value or select a macro by clicking the + button. For example, `User`.	
`com.microsoft.outlook.EmailProfile.EmailAddress`	Email address	String	The email address that will be used to pull the user's email address from Microsoft Active Directory. You can either enter a value or select a macro by clicking the + button. For example, `user@companyname.com`.	
`com.microsoft.outlook.EmailProfile.EmailUPN`	User Principal Name or username for the email profile that is used to authenticate the account	String	The name of the user in email address format. For example, `userupn@companyname.com`.	
`com.microsoft.outlook.EmailProfile.ServerAuthentication`	Authentication method	String	`Username and Password` – Prompts the device user for their password. `Certificates` – Certificate-based authentication.	`Userna and Passwo`
`com.microsoft.outlook.EmailProfile.ServerHostName`	ActiveSync FQDN	String	The Exchange ActiveSync email server URL. You don't need to use `http://` or `https://` in front of the URL. For example, `mail.companyname.com`.	
`com.microsoft.outlook.EmailProfile.AccountDomain`	Email domain	String	The account domain of the user. You can either enter a value or select a macro by clicking the + button. For example, `companyname`.	
`com.microsoft.outlook.EmailProfile.AccountType`	Authentication type	String	`ModernAuth` – Uses a token-based identity management method. Specify ModernAuth as the Account Type for Exchange Online. `BasicAuth` – Prompts the device user for their password. Specify BasicAuth as the Account Type for Exchange On-Premises.	`BasicA`

9. Click the **Add setting** button to add a block of the app configuration settings. You can add several blocks of settings.

   Specify the following parameters for each block of settings of the configuration:

   - **Key**

     Cannot be left blank. The value of this parameter is filled in manually.

- **Type**

  Cannot be left blank. The value of this parameter is selected from a drop-down list.

  The following types are available:

  - **String**. A sequence of characters, digits, or symbols, always treated as text.
  - **Bool**. True or false.
  - **Integer**. A numeric data type for numbers without fractions.
  - **Bundle**. A set of fields of any type, except for Bundle or BundleArray.
  - **BundleArray**. A set of Bundles.

- **Value**

  An optional parameter, whose value depends on the setting type.

For some types of settings, additional parameters can be configured. For example:

- You can add macros for a **String**.
- You can add a field to a **Bundle**.
- You can add a Bundle to a **BundleArray**.

It is also possible to edit a setting to be added to a BundleArray by clicking the **Configure Bundle** button and configuring the setting's parameters.

For information about configuring rules, please refer to the official documentation for the app to be configured.

10. Click **Add**.

    The configuration appears in the list of app configurations.

    > You can modify or delete app configurations in the list using the **Edit** and **Delete** buttons at the top of the list.

11. Click **OK**.
12. Click **Save** to save the changes you have made.

The app configuration is applied.

> Some apps may not notify Kaspersky Endpoint Security for Android that the app configuration has been applied.

When configuring some apps, certificates installed on devices via Kaspersky Security Center can be used. In this case, you must specify a certificate alias in the app configuration:

- `VpnCert` for VPN certificates.
- `MailCert` for mail certificates.
- `SCEP_profile_name` for certificates received using SCEP.

Managing app permissions

These settings apply to corporate devices and devices with a corporate container.

App permission management settings let you configure rules for granting runtime permissions that are requested from the device user while the app is running.

To add app permissions:

1. In the main window of Kaspersky Next Expert View (on-premise), select **Asset management** → **Policies**. In the list of group policies that opens, click the name of the policy that you want to configure.
2. In the policy properties window, select **Application settings**.
3. Select **Android** and go to the **App configuration** section.
4. On the **App permission management** card, click **Settings**.

   The **App permission management** window opens.
5. Enable the settings using the **App permission management** toggle switch.
6. Click **Add**.

   The **Add app with permission granting rules** window opens.
7. In the **Method for adding configuration** section, select how to add a configuration with permission granting rules:

   - **App package uploaded by administrator**

     When adding a configuration by uploading an app package, you need to select an APK file saved on your computer.

     After that, you can view a list of runtime permissions and select an action to be performed for each permission.

   - **Kaspersky Security Center installation package**

     When adding a configuration using an installation package added to Kaspersky Security Center, you need to select the app from the list of mobile app packages.

     After that, you can view a list of runtime permissions and select the action to be performed for each permission.

- **Manual configuration**

  When adding a configuration manually, you must click the **Add rule** button to select a permission and a corresponding action from the drop-down lists.

8. In the **App data** section, specify the following settings:

   - **App name**

     Name of the app for which permissions are to be configured.

     When importing a configuration from an APK file or an installation package, the value is inserted automatically.

   - **Package name**

     Name of the package for which permissions are to be configured.

     How to get the package name of an app

     To get the name of an app package:

     1. Open Google Play.
     2. Find the app and open its page.

        The app's URL ends with its package name (for example, https://play.google.com/store/apps/details?id=**com.android.chrome**).

     To get the name of an app package that has been added to Kaspersky Security Center:

     1. In the main window of Kaspersky Next Expert View (on-premise), select **Asset management** → **Mobile** → **Apps & files**.
     2. Select **Android** → **Apps**.

        In the list of apps that opens, app identifiers are displayed in the **Package name** column.

     When importing a configuration from an APK file or an installation package, the value is inserted automatically.

   - **Comment**

     An optional comment.

9. Click the **Add rule** button to add and configure a new rule. You can add several permissions.

   Select one of the following **permissions**.

   - Permission for call handover
   - Location permissions
   - Permission to use saved geographic locations
   - Permission for activity recognition
   - Permission for answerphone voice mails
   - Permission to answer phone calls

- Permissions for Bluetooth
- Permissions to access body sensors data
- Permission for phone calls
- Permissions for camera
- Permission to access account list
- Permissions to access nearby devices via Wi-Fi
- Permission to send notifications
- Permission to manage outgoing calls
- Permission to read calendar data
- Permission to read call log
- Permission to read contact list
- Permissions to read external storage

  Denying this permission prevents an app from scanning device data in the background, but the user can still pick files to share.
- Permission to read device's phone numbers
- Permission to read phone state
- Permissions to monitor SMS and MMS incoming messages
- Permission to receive WAP push messages
- Permission to record audio
- Permission to send SMS
- Permission to use SIP telephony
- Permission to access devices that use UWB
- Permission to write data to calendar
- Permission to write and read data of call log
- Permission to write contacts
- Permission to write data to external storage

To configure granting rules for app runtime permissions, you need to select one of the following actions for each permission:

- **Allow users to configure permissions**

  When a permission is requested, the user decides whether to grant the specified permission to the app.

This option is selected by default.

- **Grant permissions automatically**

  The app is granted the permission without user interaction.

  On devices with a corporate container running Android 12 or later, the following permissions can't be granted automatically but can be denied automatically. If you select this option, the app will prompt the user for these permissions:

  - Location permissions
  - Permissions for camera
  - Permissions to record audio
  - Permission for activity recognition
  - Permissions to monitor SMS and MMS incoming messages
  - Permissions to access body sensor data

- **Deny permissions automatically**

  The app is denied the permission without user interaction.

You can save only one granting rule for each app permission.

If a user has previously granted or denied a permission, the **Grant permissions automatically** and **Deny permissions automatically** actions will make further configuration of permissions on the device unavailable. To allow the user to change the settings, set the policy action to **Allow users to configure permissions** and synchronize the device, or ask the user to reinstall the app.

10. Click **Add**.

    The configuration appears in the **Apps with configured permission granting rules** list.

    You can modify or delete configurations in the list using the **Edit** and **Delete** buttons at the top of the list.

11. Click **OK**.

12. Click **Save** to save the changes you have made.

The configuration with permission granting rules is applied. Mobile device settings are changed after the next device synchronization with Kaspersky Security Center.

Permission granting rules configured for specific apps have precedence over the general policy for granting permissions. For example, if you first select the **Deny permissions automatically** option in the Corporate container on devices section, and then select the **Grant permissions automatically** option for a specific app in the **App permission management** section, the permission for this app will be granted automatically.

Creating a report on installed mobile apps

The **Report on installed mobile apps** lets you get detailed information about the apps installed on users' Android devices.

To allow the report to display information, the **Send data on installed apps** check box must be selected in **App Control** settings and the **An app was installed or removed (list of installed apps)** informational event type must be stored in the Administration Server database.

To enable sending data:

1. In the main window of Kaspersky Next Expert View (on-premise), select **Asset management** → **Policies**. In the list of group policies that opens, click the name of the policy that you want to configure.
2. In the policy properties window, select **Application settings**.
3. Select **Android** and go to the **Security controls** section.
4. On the **App Control** card, click **Settings**.

   The **App Control** window opens.
5. In the **Report on installed apps** section, select the **Send data on installed apps** check box.
6. If you want to receive data about system apps, select the **Send data on built-in apps** check box.
7. If you want to receive data about service apps, which do not have an interface and cannot be opened by the user, select the **Send data on service apps** check box.
8. Click **OK**.
9. Click **Save** to save the changes you have made.
10. Click the name of the policy and select **Event configuration**.
11. Go to the **Info** section.
12. Click the **An app was installed or removed (list of installed apps)** event to open its properties.
13. In the event properties window, turn on the **Store in the Administration Server database for (days)** toggle switch and set the storage period. By default, the storage period is 30 days.

    After the storage period expires, the Administration Server deletes outdated information from the database. For more information about events, please refer to the Kaspersky Security Center Help.

    You cannot configure how long events are stored on a user's mobile device. The retention period for the event log on the device is unlimited. However, the size is limited: when the event log reaches 200 entries, the 50 oldest entries are automatically deleted from the log.
14. Click **OK**.
15. Click **Save** to save the changes you have made.

Sending data is enabled.

To configure a report on installed mobile apps:

1. In the main window of Kaspersky Next Expert View (on-premise), select **Monitoring** → **Reports**.
2. Click the **Report on installed mobile apps** report template to open its properties.
3. In the window that opens, click **Edit**.
4. Edit the report template properties:
   - On the **General** tab, specify the following parameters:
     - Report template name
     - **Maximum number of entries to display**

       If this option is enabled, the number of entries displayed in the table with detailed report data does not exceed the specified value.

       Report entries are first sorted according to the rules specified in the **Fields** > **Details fields** section of the report template properties, and then only the first of the resulting entries are kept. The heading of the table with detailed report data shows the displayed number of entries and the total available number of entries that match other report template settings.

       If this option is disabled, the table with detailed report data displays all available entries. We do not recommend that you disable this option. Limiting the number of displayed report entries reduces the load on the database management system (DBMS) and reduces the time required for generating and exporting the report. Some reports contain an excessive number of entries. If this is the case, you may find it difficult to read and analyze them all. Also, your device may run out of memory while generating such a report. Consequently, you will not be able to view the report.

       By default, this option is enabled. The default value is 1000.

     - **Group**

       The set of client devices the report is created for.

     - **Include data from secondary and virtual Administration Servers**

       If this option is enabled, the report includes the information from the secondary and virtual Administration Servers that are subordinate to the Administration Server for which the report template is created.

       Disable this option if you want to view data only from the current Administration Server.

       By default, this option is enabled.

     - **Up to nesting level**

       The report includes data from secondary and virtual Administration Servers that are located under the current Administration Server on a nesting level that is less than or equal to the specified value.

       The default value is 1. You may want to change this value if you have to get information from secondary Administration Servers located at lower levels in the tree.

     - **Data wait interval (min)**

       Before generating the report, the Administration Server for which the report template is created waits for data from secondary Administration Servers during the specified number of minutes. If no data is received from a secondary Administration Server at the end of this period, the report runs anyway. Instead of up-to-date data, the report shows data taken from the cache (if the **Cache data from secondary Administration Servers** option is enabled), or **N/A** (not available) otherwise.

The default value is 5 (minutes).

- **Cache data from secondary Administration Servers**

  Secondary Administration Servers regularly transfer data to the Administration Server for which the report template is created. The transferred data is stored in the cache on that Administration Server.

  If the current Administration Server cannot receive data from a secondary Administration Server while generating the report, the report shows data taken from the cache. The date when the data was transferred to the cache is also displayed.

  Enabling this option lets you view information from secondary Administration Servers even if up-to-date data cannot be retrieved. However, the displayed data may be obsolete.

  By default, this option is disabled.

- **Transfer detailed information from secondary Administration Servers**

  In the generated report, the table with detailed report data includes data from secondary Administration Servers of the Administration Server for which the report template is created.

  Enabling this option slows report generation and increases traffic between Administration Servers. However, it lets you view all data in one report.

  Instead of enabling this option, you may want to analyze detailed report data to detect a faulty secondary Administration Server, and then generate the same report only for that faulty Administration Server.

  By default, this option is disabled.

- On the **Fields** tab, select the fields that will be displayed in the report and the order of these fields, and configure whether the report must be sorted and filtered by each of the fields.

5. Click **Save** to save the changes you have made.

The updated report template appears in the list of report templates.

To create and view a report on installed mobile apps:

1. In the main window of Kaspersky Next Expert View (on-premise), select **Monitoring** → **Reports**.
2. Click a report with the **Report on installed mobile apps** type.

A report using the selected template is generated and displayed.

For more information about using reports, managing custom report templates, using report templates to generate new reports, and creating report delivery tasks, please refer to the Kaspersky Security Center Help.

Installing root certificates on Android devices

A root certificate is a public key certificate issued by a trusted certificate authority (CA). Root certificates are used to verify custom certificates and guarantee their identity.

Kaspersky Next Expert View (on-premise) lets you add root certificates to be installed to a trusted certificate store on Android devices.

These certificates are installed on user devices as follows:

- On corporate devices, the certificates are installed automatically.

  If you delete a root certificate in the policy settings, it will also be automatically deleted on the device during the next synchronization with the Administration Server.

- On personal devices:

  - If a corporate container was not created, the device user is prompted to install each certificate manually in a personal space by following the instructions in the notification.
  - If a corporate container was created, the certificates are installed automatically to the container. If the **Duplicate installation of root certificates in user's personal space** check box is selected in the corporate container settings, the certificates can also be installed in a personal space. The device user is prompted to do this manually by following the instructions in the notification.

    If you delete a root certificate in the policy settings, it will also be automatically deleted on the device during the next synchronization with the Administration Server.

    For instructions on how to install certificates in a personal space, please refer to Installing root certificates on the device.

To add a root certificate:

1. In the main window of Kaspersky Next Expert View (on-premise), select **Asset management** → **Policies**. In the list of group policies that opens, click the name of the policy that you want to configure.
2. In the policy properties window, select **Application settings**.
3. Select **Android** and go to the **Device configuration** section.
4. On the **Root certificates** card, click **Settings**.

   The **Root certificates** window opens.
5. Enable the settings using the **Root certificates** toggle switch.
6. Click **Add**.

   The file explorer opens.
7. Select a certificate file (a CER, PEM, KEY, or CRT file) and click **Open**.

   The certificate file must be no larger than 10 MB.

   The certificate will appear in the list of root certificates.
8. Click **OK**.
9. Click **Save** to save the changes you have made.

Mobile device settings are configured after the next device synchronization with Kaspersky Security Center.

Configuring notifications for Kaspersky Endpoint Security for Android

If you don't want the mobile device user to be distracted by Kaspersky Endpoint Security for Android notifications, you can disable certain notifications.

Kaspersky Endpoint Security for Android uses the following tools to display the status of device protection:

- **Protection status notification**. This notification is pinned to the notification bar. A protection status notification cannot be removed. The notification displays the device protection status (for example,) and the number of issues, if any. You can tap the device protection status and see security issues in the app.
- **App notifications**. These notifications inform the device user about the application (for example, the detection of a threat).
- **Pop-up messages**. Pop-up messages require action from the device user (for example, action to take when a threat is detected).

All Kaspersky Endpoint Security for Android notifications are enabled by default.

On Android 13, the device user must grant the permission to send notifications during or after the Initial Configuration Wizard.

The user can disable all notifications from Kaspersky Endpoint Security for Android in the settings on the notification bar. If notifications are disabled, the user is not monitoring operation of the app and may ignore important information (for example, information about failures during device synchronization with Kaspersky Security Center). In this case, to find out the app operating status, the user must open Kaspersky Endpoint Security for Android.

To configure displaying notifications about the operation of Kaspersky Endpoint Security for Android:

1. In the main window of Kaspersky Next Expert View (on-premise), select **Asset management** → **Policies**. In the list of group policies that opens, click the name of the policy that you want to configure.
2. In the policy properties window, select **Application settings**.
3. Select **Android** and go to the **KES for Android settings** section.
4. On the **Configure notifications** card, click **Settings**.

   The **Configure notifications** window opens.
5. Enable the settings using the **Configure notifications** toggle switch.
6. If you want to hide all notifications and pop-up messages, in the **Notifications from Kaspersky Endpoint Security** section, select the **Disable notifications when Kaspersky Endpoint Security is in the background** check box.

   Kaspersky Endpoint Security for Android will display only the protection status notification. The notification displays the device protection status (for example,) and the number of issues.

   In-app notifications (for example, when the user updates anti-malware databases manually) will still be displayed.

We recommend that you enable notifications and pop-up messages. If you disable notifications and pop-up messages when the app is in the background, the app will not warn users about threats in real time. In this case, mobile device users will not see the device protection status unless they open the app.

7. In the **Kaspersky Endpoint Security in-app notifications** section, select the Kaspersky Endpoint Security for Android issues that you want to display on the user's mobile device.

   By default, the user may ignore the **Device has not been synchronized with the Administration Server for a long time** notification. If you want to have more control over the synchronization frequency, when configuring rules for checking compliance with the policy, select the **Device has not been synchronized for a long time** criterion to draw the user's attention to the issue.

   Displaying certain Kaspersky Endpoint Security for Android issues is mandatory. These issues are always displayed on the device (for example, issues about license expiration).

8. Click **OK**.

9. Click **Save** to save the changes you have made.

Mobile device settings are changed after the next device synchronization with Kaspersky Security Center. The notifications that you disable will not be displayed on the user's mobile device.

Selecting the download manager for Android devices

If you use Web Server with a self-signed certificate instead of a certificate signed by a certification authority (CA), the standard Android download manager lets you download apps and Kaspersky Endpoint Security for Android installation packages from your Web Server to devices only via HTTP.

To securely download apps and installation packages from Web Server with a self-signed certificate to devices, you can use the built-in Kaspersky Endpoint Security for Android download manager that always uses HTTPS.

The built-in Kaspersky Endpoint Security for Android download manager is enabled by default.

To change the download manager used by Kaspersky Endpoint Security for Android:

1. In the main window of Kaspersky Next Expert View (on-premise), select **Asset management** → **Policies**. In the list of group policies that opens, click the name of the policy that you want to configure.

2. In the policy properties window, select **Application settings**.

3. Select **Android** and go to the **KES for Android settings** section.

4. Do one of the following:

   - To use the Kaspersky Endpoint Security for Android download manager, turn on the **Built-in download manager** toggle switch.
   - To use the standard Android download manager, turn off the **Built-in download manager** toggle switch.

The download manager used on devices is configured.

Mobile device settings are changed after the next device synchronization with Kaspersky Security Center.

Connecting iOS MDM devices to AirPlay

Configure the connection to AirPlay devices to stream music, photos, and videos from an iOS MDM device to AirPlay devices. To be able to use AirPlay, the mobile device and AirPlay devices must be connected to the same wireless network. AirPlay devices include Apple TV devices (second generation or later), AirPort Express devices, speakers, TVs, and radios with AirPlay support.

Automatic connection to AirPlay devices is available for devices operating in basic control mode and for supervised devices.

To configure the connection of an iOS MDM device to AirPlay devices:

1. In the main window of Kaspersky Next Expert View (on-premise), select **Asset management** → **Policies**. In the list of group policies that opens, click the name of the policy that you want to configure.
2. In the policy properties window, select **Application settings**.
3. Select **iOS** and go to the **Device configuration** section.
4. On the **AirPlay** card, click **Settings**.

   The **AirPlay** window opens.
5. Enable the settings using the **AirPlay** toggle switch.
6. In the **Passwords** section, click **Add password**.
7. In the **Device** field, enter the name of the AirPlay device on the wireless network.
8. In the **Password** field, enter the password to the AirPlay device.
9. If you want iOS MDM devices to connect only to specific AirPlay devices, create a list of allowed devices in the **Allowed devices** section. To do this, click **Add device** and specify the MAC addresses of AirPlay devices.

   To connect iOS MDM devices running iOS 18 or later to any AirPlay devices, you must specify the **Device name**.

   To connect iOS MDM devices running iOS 17 or earlier to any AirPlay devices, you must specify both the Wi-Fi and Ethernet address for each device.

Access to AirPlay devices that are not in the list of allowed devices is blocked. If the list of allowed devices is empty, Kaspersky Mobile Devices Protection and Management allows access to all AirPlay devices.

10. Click **OK**.

11. Click **Save** to save the changes you have made.

As a result, once the policy is applied, the user's mobile device will automatically connect to AirPlay devices to stream media.

Connecting iOS MDM devices to AirPrint

To enable printing documents from an iOS MDM device wirelessly using AirPrint, configure automatic connection to AirPrint printers. The mobile device and printer must be connected to the same wireless network. Shared access for all users must be configured on the AirPrint printer.

To configure the connection of an iOS MDM device to an AirPrint printer:

1. In the main window of Kaspersky Next Expert View (on-premise), select **Asset management** → **Policies**. In the list of group policies that opens, click the name of the policy that you want to configure.

2. In the policy properties window, select **Application settings**.

3. Select **iOS** and go to the **Device configuration** section.

4. On the **AirPrint** card, click **Settings**.

   The **AirPrint** window opens.

5. Enable the settings using the **AirPrint** toggle switch.

6. Click **Add**.

   The **Add printer** window opens.

7. In the **IP address or FQDN** field, enter the IP address or a fully qualified domain name (FQDN) of the AirPrint printer.

8. In the **Port** field, enter the listening port of the AirPrint destination.

9. In the **Resource path** field, enter the path to the AirPrint printer.

   The path to the printer corresponds to the rp (resource path) key of the Bonjour protocol. For example:

   - printers/Canon_MG5300_series
   - ipp/print
   - Epson_IPP_Printer

10. If you want to protect the connection to the AirPrint printer using the TLS protocol, select the **Use TLS** check box.

11. Click **Add**.

    The newly added AirPrint printer appears in the list.

12. Click **OK**.

13. Click **Save** to save the changes you have made.

    As a result, once the policy is applied, the mobile device user can wirelessly print documents on the AirPrint printer.

Configuring the Access Point Name (APN)

This section provides instructions on how to connect a mobile device to cellular data services on a mobile network.

Configuring APN on Android devices (only Samsung)

APN can be configured only for Samsung devices.

A SIM card must be inserted to be able to use an access point on the user's mobile device. Access point settings are provided by the mobile operator. Incorrect access point settings may result in additional mobile charges.

To configure the Access Point Name (APN) settings on a user's mobile device:

1. In the main window of Kaspersky Next Expert View (on-premise), select **Asset management** → **Policies**. In the list of group policies that opens, click the name of the policy that you want to configure.

2. In the policy properties window, select **Application settings**.

3. Select **Android** and go to the **Samsung Knox settings** section.

4. On the **APN settings** card, click **Settings**.

   The **APN settings** window opens.

5. Enable the settings using the **APN settings** toggle switch.

   The toggle switch in this card does not enable or disable the corresponding functionality on devices. Enabling the toggle switch lets you configure custom settings. Disabling the toggle switch lets you use default settings.

6. Specify the following access point settings for connecting the user to the data service:

   - In the **APN type** drop-down list, select the type of access point (APN) for data transmission on a GPRS/3G/4G mobile network:

     - **Internet**. Connection of the user's mobile device to the internet.
     - **MMS**. Exchange of MMS multimedia messages.
     - **Internet and MMS**. Connection to the internet and exchange of multimedia messages. This is the default value.

   - In the **APN name** field, specify the name of the access point.
   - In the **MCC** field, enter the mobile country code (MCC).
   - In the **MNC** field, enter the mobile network code (MNC).

7. If you have selected **MMS** or **Internet and MMS** as the type of access point, specify the following additional MMS server settings in the **MMS server** section:

   - In the **MMS server name** field, specify the full domain name of the mobile carrier's server used for MMS exchange (for example, `mms.mobile.com`).
   - In the **MMS proxy server address** field, specify the network name or IP address of the proxy server.
   - In the **MMS proxy server port** field, specify the port number of the mobile carrier's server used for MMS exchange.

8. In the **Authentication** section, specify the authentication settings:

   - In the **Authentication type** drop-down list, select the type of authentication of the mobile device user that will be used on the mobile carrier's server for network access. By default, user authentication is not required. The following types are available:

     - **None**. User authentication is not required to access the mobile network.
     - **PAP** (Password Authentication Protocol). An authentication protocol that uses passwords as plain non-encrypted text.
     - **CHAP** (Challenge Handshake Authentication Protocol). A request-response authentication protocol that uses standard MD5 hashing to encrypt the response.
     - **Concurrently**. Combined use of CHAP and PAP protocols.

   - In the **User name** field, enter the user name for authorization on the mobile network.
   - In the **Password** field, enter the password for user authorization on the mobile network.

9. In the **Network** section, specify the following network settings:

   - In the **Network name** field, enter the name of the network.
   - In the **Server address** field, specify the network name of the mobile carrier's server through which data transmission services are accessed.

10. In the **Proxy server** section, specify the following proxy server settings:

    - Select the **Use a proxy server** check box to enable the use of a proxy server. This check box is cleared by default.
    - In the **Proxy server address** field, specify the network name or IP address of the mobile carrier's proxy server for network access. This field is available only if the **Use a proxy server** check box is selected.
    - In the **Proxy server port** field, specify the port number of the mobile carrier's proxy server for network access. This field is available only if the **Use a proxy server** check box is selected.

11. Click **OK**.

12. Click **Save** to save the changes you have made.

    Mobile device settings are changed after the next device synchronization with Kaspersky Security Center.

Configuring APN on iOS MDM devices

The Access Point Name (APN) has to be configured in order to enable the mobile network data transmission service on the user's iOS MDM device.

To configure an access point on a user's iOS MDM device:

1. In the main window of Kaspersky Next Expert View (on-premise), select **Asset management** → **Policies**. In the list of group policies that opens, click the name of the policy that you want to configure.

2. In the policy properties window, select **Application settings**.

3. Select **iOS** and go to the **Device configuration** section.

4. On the **APN settings** card, click **Settings**.

   The **APN settings** window opens.

5. Enable the settings using the **APN settings** toggle switch.

   > The toggle switch in this card does not enable or disable the corresponding functionality on devices. Enabling the toggle switch lets you configure custom settings. Disabling the toggle switch lets you use default settings.

6. In the **APN type** drop-down list, select the type of access point for data transfer on a GPRS/3G/4G mobile network:

    - **Built-in APN**. Configure cellular communication settings for data transfer via a mobile network operator that supports operation with a built-in Apple SIM. For more details about devices with a built-in Apple SIM, visit the Apple Support website.
    - **APN**. Configure cellular communication settings for data transfer via the mobile network operator of the inserted SIM card.
    - **Built-in APN and APN**. Configure cellular communication settings for data transfer via the mobile network operators of the inserted SIM card and the built-in Apple SIM. For more details about devices with a built-in Apple SIM and a SIM card slot, visit the Apple Support website.

7. If you selected **APN**, in the **APN** section click **Add**.

   The **Add APN** window opens.

8. Configure the following settings:

   a. In the **APN name** field, specify the name of the access point.

   b. In the **Authentication type** drop-down list, select the type of user authentication on the mobile operator's server for network access (internet and MMS).

   c. In the **User name** field, enter the user name for authorization on the mobile network.

   d. In the **Password** field, enter the password for user authorization on the mobile network.

   e. In the **Proxy server address** field, enter the name of the host or the IP address of the proxy server.

   f. In the **Proxy server port** field, enter the number of the proxy server port.

   g. In the **Allowed protocol** drop-down list, select the internet protocol.

   h. In the **Allowed protocol for roaming** drop-down list, select the internet protocol that will be used during international roaming.

   i. In the **Allowed protocol for domestic roaming** drop-down list, select the internet protocol that will be used during domestic roaming.

   j. If you want devices on IPv6-only networks to be able to access IPv4-only internet services, select the **Use the 464XLAT technology** check box.

   k. Click **OK**.

9. If you selected **Built-in APN**, configure the following settings:

   a. In the **Built-in APN name** field, specify the name of the access point.

   b. In the **Authentication type** drop-down list, select the type of user authentication on the mobile operator's server for network access (internet and MMS).

   c. In the **User name** field, enter the user name for authorization on the mobile network.

   d. In the **Password** field, enter the password for user authorization on the mobile network.

   e. In the **Allowed protocol** drop-down list, select the internet protocol.

10. Click **OK**.

11. Click **Save** to save the changes you have made.

As a result, the access point name (APN) is configured on the user's mobile device after the policy is applied.

Corporate container

This section contains information about working with a corporate container.

About corporate containers

Android Enterprise is a platform for managing the corporate mobile infrastructure and provides company employees with a safe work environment in which they can use mobile devices. For details on using Android Enterprise, see the Google support website.

You can create a corporate container that uses an Android Work Profile on a user's personal mobile device. A corporate container is a safe environment in which the administrator can manage apps and user accounts without restricting the user's use of their own data. When a corporate container is created on the user's mobile device, the following corporate apps are automatically installed in it: Google Play, Google Chrome, Downloads, Kaspersky Endpoint Security for Android, and others. Apps installed in the corporate container as well as notifications from these apps are marked with a briefcase icon. You have to create a separate Google corporate account for the Google Play app. Apps installed in a corporate container appear in the common list of apps.

Configuring a corporate container

To configure the settings of a corporate container:

1. In the main window of Kaspersky Next Expert View (on-premise), select **Asset management** → **Policies**. In the list of group policies that opens, click the name of the policy that you want to configure.
2. In the policy properties window, select **Application settings**.
3. Select **Android** and go to the **Corporate container** section.
4. On the **Corporate container on devices** card, click **Settings**.
   The **Corporate container on devices** window opens.
5. Enable the settings using the **Corporate container on devices** toggle switch.
6. Specify the corporate container settings:
   - On the **General** tab, you can specify the settings for data sharing, contacts, and more.
     - Settings in the **Data access and sharing** section:
       - **Prohibit personal apps from sharing data with corporate container apps**

         Restricts sharing files, pictures, or other data from personal apps with corporate container apps.
         If the check box is selected, personal apps can't share data with corporate container apps.
         If the check box is cleared, personal apps can share data with corporate container apps.
         This check box is selected by default.

       - **Prohibit corporate container apps from sharing data with personal apps**

         Restricts sharing files, pictures, or other data from corporate container apps with personal apps.
         If the check box is selected, the apps in the corporate container can't share data with personal apps.
         If the check box is cleared, the apps in the corporate container can share data with personal apps.
         This check box is selected by default.

- **Prohibit corporate container apps from accessing personal files**

  Restricts access of corporate container apps to personal files.

  If the check box is selected, the user can't access personal files when using corporate container apps.

  If the check box is cleared, the user can access personal files when using corporate container apps. Note that the access must be also supported by the apps that are being used.

  This check box is selected by default.

- **Prohibit personal apps from accessing files in corporate container**

  Restricts access of personal apps to files in the corporate container.

  If the check box is selected, the user can't access files in the corporate container when using personal apps.

  If the check box is cleared, the user can access files in the corporate container when using personal apps. Note that the access must be supported by the apps that are being used.

  This check box is selected by default.

- **Prohibit use of clipboard between personal apps and corporate container**

  Selecting or clearing this check box specifies whether the device user is allowed to copy data via the clipboard between personal apps and the corporate container.

  This check box is selected by default.

- **Prohibit activation of USB debugging**

  Restricts the use of USB debugging on the user's mobile device in the corporate container. In USB debugging mode, the user can download an app via a workstation, for example.

  If the check box is selected, USB debugging mode is not available to the user. The user is unable to configure the mobile device via USB after connecting the device to a workstation.

  If the check box is cleared, the user can enable USB debugging mode, connect the mobile device to a workstation via USB, and configure the device.

  This check box is selected by default.

- **Prohibit users from adding and removing accounts in corporate container**

  If the check box is selected, the user is prohibited to add and remove accounts in the corporate container via the Settings or Google apps. This includes restricting the ability to sign in to Google apps for the first time. However, the user can sign in, add, and remove accounts via some other third-party apps in the corporate container.

  Accounts that were added before the restriction is set will not be removed and sign in to these accounts is not restricted.

  This check box is selected by default.

- **Prohibit screen sharing, recording, and screenshots in corporate container apps**

  Selecting or clearing this check box specifies whether the device user is allowed to take screenshots of, record and share the device screen in corporate container apps. It also specifies whether the contents of the device screen are allowed to be captured for artificial intelligence purposes.

  This check box is selected by default.

- Settings in the **File sharing** section:

  - **Copy shared files to user's personal space**

Selecting or clearing this check box specifies whether files sent to a user's device with a corporate container are copied to the user's personal space on the device.

This check box applies only to files that have not yet been sent to the device. Files that were sent to the device before the check box is selected are not copied to the user's personal space.

This check box is cleared by default.

- Settings in the **Contacts** section:

  - **Prohibit showing contact name from corporate container for incoming personal calls**

    Selecting or clearing this check box specifies whether a contact name from the corporate container will be shown for personal incoming calls.

    This check box is selected by default.

  - **Prohibit personal apps from accessing corporate container contacts**

    Selecting or clearing this check box specifies whether personal contact management apps are allowed to access corporate container contacts.

    This check box is selected by default.

- On the **Apps** tab, specify the following settings:

  - Settings in the **General** section:

    - **Enable App Control in corporate container only**

      Controls the startup of apps in the corporate container on the user's mobile device. You can create lists of allowed, forbidden, and recommended apps as well as allowed and forbidden app categories in the **App Control** section.

      If this check box is selected, then depending on the App Control settings, Kaspersky Endpoint Security blocks or allows startup of apps only in the corporate container. Moreover, App Control does not work in the user's personal space.

      This check box is selected by default.

    - **Enable Web Protection and Web Control in corporate container only**

      Restricts user access to websites in the corporate container on the device. You can specify website access settings in the **Web Control** settings.

      If this check box is selected, Web Protection and Web Control block or allow access to websites only in the corporate container. Moreover, Web Protection and Web Control do not work in the user's personal space.

      If this check box is cleared, then depending on the Web Protection and Web Control settings, Kaspersky Endpoint Security blocks or allows access to websites in the user's personal space and the corporate container.

      This check box is selected by default.

    - **Prohibit installation of apps from unknown sources in corporate container**

      Restricts installation of apps in the corporate container from all sources other than Google Play Enterprise.

      If the check box is selected, the user can install apps only from Google Play. Users use their own Google corporate accounts to install apps.

      If the check box is cleared, the user can install apps in any available way. Only apps forbidden in the **App Control** settings can't be installed.

This check box is cleared by default.

- **Prohibit removing apps from corporate container**

  Selecting or clearing this check box specifies whether the user is prohibited from removing apps from the corporate container.

  This check box is cleared by default.

- **Prohibit displaying notifications from corporate container apps when screen is locked**

  Restricts displaying the contents of notifications from corporate container apps on the lock screen of the device.

  If the check box is selected, the contents of notifications from corporate container apps can't be viewed on the device lock screen. To view these notifications, the user has to unlock the device or corporate container.

  If the check box is cleared, notifications from corporate container apps are displayed on the device lock screen.

  This check box is selected by default.

- **Prohibit use of camera for corporate container apps**

  Selecting or clearing this check box specifies whether corporate container apps can access the device camera.

  This check box is selected by default.

- In the **Granting runtime permissions for corporate container apps** section you can select an action to be performed when corporate container apps are running and request additional permissions. This does not apply to permissions granted in the device settings (for example, Access All Files).

  - **Allow users to configure permissions**

    When a permission is requested, the user decides whether to grant the specified permission to the app.

    This option is selected by default.

  - **Grant permissions automatically**

    All corporate container apps are granted permissions without user interaction.

    On Android 12 or later, the following permissions can't be granted automatically but can be denied automatically. If you select this option, the app will prompt the user for these permissions:

    - Location permissions
    - Permissions for camera
    - Permissions to record audio
    - Permission for activity recognition
    - Permissions to monitor SMS and MMS incoming messages
    - Permissions to access body sensor data

  - **Deny permissions automatically**

    All corporate container apps are denied permissions without user interaction.

Users can adjust app permissions in the device settings before these permissions are denied automatically.

- In the **Adding widgets of corporate container apps to device home screen** section you can choose whether the device user is allowed to add widgets of corporate container apps to the device home screen.

  - **Prohibit for all apps**

    The device user is prohibited from adding widgets of apps installed in the corporate container.

    This option is selected by default.

  - **Allow for all apps**

    The device user is allowed to add widgets of all apps installed in the corporate container.

  - **Allow only for the listed apps**

    The device user is allowed to add widgets of listed apps installed in the corporate container.

    To add an app to the list, click **Add** and enter an app package name.

    How to get the package name of an app

    To get the name of an app package:

    1. Open Google Play.
    2. Find the app and open its page.

       The app's URL ends with its package name (for example, https://play.google.com/store/apps/details?id=**com.android.chrome**).

    To get the name of an app package that has been added to Kaspersky Security Center:

    1. In the main window of Kaspersky Next Expert View (on-premise), select **Asset management** → **Mobile** → **Apps & files**.
    2. Select **Android** → **Apps**.

       In the list of apps that opens, app identifiers are displayed in the **Package name** column.

- On the **Certificates** tab, you can configure the following settings:

  - **Duplicate installation of VPN certificates in user's personal space**

    Selecting or clearing the check box specifies whether the VPN certificate added in the **Mobile** → **Certificates** section of the Kaspersky Next Expert View (on-premise) and installed in the corporate container will also be installed in the user's personal space.

    By default, VPN certificates received from Kaspersky Security Center are installed in the corporate container. This setting is applied when a new VPN certificate is issued.

    This check box is cleared by default.

  - **Duplicate installation of root certificates in user's personal space**

    Selecting or clearing the check box specifies whether the root certificates added in the **Root certificates** settings and installed in the corporate container will also be installed in the user's personal space.

This check box is cleared by default.

- On the **Password** tab, specify the corporate container password settings:

  - **Require setting a password for corporate container**

    Lets you specify the requirements for the corporate container password according to company security requirements.

    If the check box is selected, password requirements are available for configuration. When the policy is applied, the user receives a notification prompting them to set up a corporate container password according to company requirements.

    If the check box is cleared, password settings cannot be edited.

    This check box is cleared by default.

  - **Minimum password length**

    The minimum number of characters in the user password. Possible values: 4 to 16 characters.

    The user's password is 4 characters long by default.

    The following applies only to the user's personal space and the corporate container:

    - In the user's personal space, Kaspersky Endpoint Security converts the password strength requirements into one of values available in the system: medium or high on devices running Android 10 or later.

    - In the corporate container, Kaspersky Endpoint Security converts the password strength requirements into one of the values available in the system: medium or high on devices running Android 12 or later.

    The values are determined using the following rules:

    - If the required password length is 1 to 4 characters, then the app prompts the user to set a medium-strength password. It must be either numeric (PIN) with no repeating or ordered sequences (e.g. 1234), or alphabetic/alphanumeric. The PIN or password must be at least 4 characters long.

    - If the required password length is 5 or more characters, then the app prompts the user to set a high-strength password. It must be either numeric (PIN) with no repeating or ordered sequences, or alphabetic/ alphanumeric (password). A PIN must be at least 8 digits long. A password must be at least 6 characters long.

  - **Minimum password complexity requirements**

    Specifies the minimum unlock password requirements. These requirements apply only to new user passwords. The following values are available:

    - **Numeric**

      The user can set a password that includes numbers or set any stronger password (for instance, an alphabetic or alphanumeric password).

      This option is selected by default.

    - **Alphabetic**

      The user can set a password that includes letters (or other non-number symbols) or set any stronger password (for instance, an alphanumeric password).

    - **Alphanumeric**

      The user can set a password that includes both numbers and letters (or other non-number symbols) or set any stronger complex password.

- **No requirements**

  The user can set any password.

- **Complex**

  The user must set a complex password according to the specified password properties:

  - **Minimum number of letters**
  - **Minimum number of digits**
  - **Minimum number of special characters (for example, !@#$%)**
  - **Minimum number of uppercase letters**
  - **Minimum number of lowercase letters**
  - **Minimum number of non-alphabetic characters (for example, 1^*9)**

- **Complex numeric**

  The user can set a password that includes numbers with no repetitions (e.g. 4444) and no ordered sequences (e.g. 1234, 4321, 2468) or set any stronger complex password.

- **Maximum number of failed password attempts before corporate container is deleted**

  Specifies the maximum number of user attempts to enter the password to unlock the corporate container. When the policy is applied, the corporate container will be deleted from the device after the maximum number of failed attempts is exceeded.

  Possible values are 4 to 16.

  The default value is not set. This means that the attempts are not limited.

- **Maximum password lifetime (days)**

  Specifies the number of days before the password expires. Applying a new value will set the current password lifetime to the new value.

  The default value is 0. This means that the password won't expire.

- **Number of days to send a notification before a required password change**

  Specifies the number of days to notify the user before the password expires.

  The default value is 0. This means that the user won't be notified about an expiring password.

- **Number of recent passwords that cannot be set as a new password**

  Specifies the maximum number of previous user passwords that can't be used as a new password. This setting applies only when the user sets a new password on the device.

  The default value is 0. This means that the new user password can match any previous password except the current one.

- **Period of inactivity before corporate container is locked (sec)**

  Specifies the period of inactivity before the device locks.

  The default value is 0. This means that the device won't lock after a certain period.

- **Period after biometric unlock before password must be entered (min)**

  Specifies the period for unlocking the device without a password. During this period, the user can use biometric methods to unlock the screen. After this period, the user can unlock the screen only with a password.

  The default value is 0. This means that the user won't be forced to unlock the device with a password after a certain period.

- **Allow biometric unlock methods**

  If the check box is selected, the use of biometric unlock methods on the mobile device is allowed.

  If the check box is cleared, Kaspersky Endpoint Security for Android blocks the use of biometric methods to unlock the screen. The user can unlock the screen only with a password.

  This check box is selected by default.

- **Allow fingerprint unlock**

  Specifies whether fingerprints can be used to unlock the screen.

  > This check box does not restrict the use of a fingerprint scanner when signing in to apps or confirming purchases.

  If the check box is selected, the use of fingerprints on the mobile device is allowed.

  If the check box is cleared, Kaspersky Endpoint Security for Android blocks the use of fingerprints to unlock the screen. The user can unlock the screen only with a password. In the device settings, the option to use fingerprints will be unavailable.

  This check box is available only if the **Allow biometric unlock methods** check box is selected.

  This check box is selected by default.

  > On some Xiaomi devices with a corporate container, the corporate container may be unlocked by a fingerprint only if you set the **Period of inactivity before corporate container is locked (sec)** value after setting a fingerprint as the screen unlock method.

- **Allow face unlock**

  If the check box is selected, the use of face scanning is allowed on the mobile device.

  If the check box is cleared, Kaspersky Endpoint Security for Android blocks the use of face scanning to unlock the screen.

  This check box is available only if the **Allow biometric unlock methods** check box is selected.

  This check box is selected by default.

- **Allow iris scanning**

  If the check box is selected, the use of iris scanning is allowed on the mobile device.

  If the check box is cleared, Kaspersky Endpoint Security for Android blocks the use of iris scanning to unlock the screen.

  This check box is available only if the **Allow biometric unlock methods** check box is selected.

  This check box is selected by default.

- On the **Passcode** tab, specify the one-time passcode settings. The user will be prompted to enter the one-time passcode to unlock their corporate container if it is locked.

  - **Passcode length**

    The number of digits in the passcode. Possible values: 4, 8, 12, or 16 characters.

    The passcode length is 4 characters by default.

7. Click **OK**.

8. Click **Save** to save the changes you have made.

Mobile device settings are changed after the next device synchronization with Kaspersky Security Center. The user's mobile device is divided into a corporate container and a personal space.

Unlocking the corporate container

The corporate container can be locked if the device does not meet the Compliance Control security requirements.

To unlock the corporate container, the user of the mobile device must enter a one-time corporate container passcode on the locked screen. The passcode is generated by Kaspersky Security Center and is unique for each mobile device. When the corporate container is unlocked, the corporate container password is set to the default value (1234).

As an administrator, you can view the passcode in the policy settings that are applied to the mobile device. The length of the passcode can be changed (4, 8, 12, or 16 digits) in the **Corporate container on devices** settings of the policy.

To unlock a corporate container using a one-time passcode:

1. In the main window of Kaspersky Next Expert View (on-premise), select **Asset management** → **Mobile** → **Devices**.

2. Click the mobile device for which you want to get a one-time passcode.

3. Select **Applications** → **Kaspersky Mobile Devices Protection and Management**.

   The Kaspersky Mobile Devices Protection and Management properties window opens.

4. Select the **Application settings** tab.

   The unique passcode for the selected device is shown in the **One-time code** field of the **One-time corporate container passcode** section.

5. Use any available method (such as email) to communicate the one-time passcode to the user.

   The user then must enter the received one-time passcode on their device.

The corporate container of the user's mobile device is unlocked.

After the corporate container on a device is locked, the history of corporate container passwords is cleared. This means that the user can specify a recent password, regardless of the corporate container password settings.

Adding an LDAP account

These settings apply to supervised devices and devices operating in basic control mode.

To enable an iOS MDM device user to access corporate contacts on the LDAP server, add an LDAP account.

To add an LDAP account of an iOS MDM device user:

1. In the main window of Kaspersky Next Expert View (on-premise), select **Asset management** → **Policies**. In the list of group policies that opens, click the name of the policy that you want to configure.
2. In the policy properties window, select **Application settings**.
3. Select **iOS** and go to the **Device configuration** section.
4. On the **LDAP** card, click **Settings**.

   The **LDAP** window opens.
5. Enable the settings using the **LDAP** toggle switch.
6. Click **Add**.

   The **Add LDAP account** window opens.
7. On the **General** tab. specify the following LDAP settings:
   - In the **Server** section, specify the server settings:
     - In the **Description** field, enter a description of the user's LDAP account. You can either enter a value or select a macro by clicking the + button.
     - In the **Server address** field, enter the name of the LDAP server domain.
   - In the **Authentication** section, specify the user's credentials:
     - In the **Account name** field, enter the account name for authorization on the LDAP server. You can either enter a value or select a macro by clicking the + button.
     - In the **Password** field, enter the password of the LDAP account for authorization on the LDAP server.
     - To use the SSL (Secure Sockets Layer) data transport protocol to secure the transmission of messages, select the **Use SSL connection** check box.
   - If necessary, in the **Per App VPN** section, configure Per App VPN.
8. On the **Search** tab, compile a list of search queries for the iOS MDM device user to access corporate data on the LDAP server:
   a. Click the **Add setting** button to add a block of the search query settings.
   b. In the **Name** field, enter the name of a search query.

c. In the **Search scope** drop-down list, select the nesting level of the folder for searching corporate data on the LDAP server:

- **Root folder of the LDAP server**. Search in the base folder of the LDAP server.
- **First level subfolders**. Search in folders in the first nesting level, counting from the base folder.
- **All subfolders**. Search in folders in all nesting levels, counting from the base folder.

d. In the **Search base** field, enter the path to the folder on the LDAP server where the search begins (for example: "ou=people", "o=example corp").

e. Repeat steps a-d for all search queries that you want to add to the iOS MDM device.

9. Click **Add**.

   The new LDAP account appears in the list.

   You can modify or delete LDAP accounts in the list using the **Edit** and **Delete** buttons at the top of the list.

10. Click **OK**.

11. Click **Save** to save the changes you have made.

Mobile device settings are changed after the next device synchronization with the iOS MDM Server.

As a result, once the policy is applied, LDAP accounts from the compiled list is added on the user's mobile device. The user can access corporate contacts in the standard iOS apps: Contacts, Messages, and Mail.

Adding a contacts account

These settings apply to supervised devices and devices operating in basic control mode.

To let the iOS MDM device user synchronize data with the CardDAV server, add a CardDAV account. Synchronization with the CardDAV server lets the user access the contact details from any device.

To add a CardDAV account of an iOS MDM device user:

1. In the main window of Kaspersky Next Expert View (on-premise), select **Asset management** → **Policies**. In the list of group policies that opens, click the name of the policy that you want to configure.
2. In the policy properties window, select **Application settings**.
3. Select **iOS** and go to the **Device configuration** section.
4. On the **Contacts** card, click **Settings**.

   The **Contacts** window opens.

5. Enable the settings using the **Contacts** toggle switch.

6. Click **Add**.

   The **Add CardDAV account** window opens.

7. In the **Server** section, in the **Description** field, enter a description of the user's CardDAV account.

8. In the **Server address** and **Server port** fields, enter the host name or the IP address of the CardDAV server and the number of the CardDAV server port.

9. In the **Contact URL** field, specify the URL of the CardDAV account of the iOS MDM device user on the CardDAV server (for example: `http://example.com/carddav/users/mycompany/user`).

   The URL must begin with `http://` or `https://`.

10. In the **Authentication** section, in the **Account name** field, enter the account name for authorization on the CardDAV server.

11. In the **Password** field, enter the CardDAV account password for authorization on the CardDAV server.

12. If you want to use the SSL (Secure Sockets Layer) data transport protocol to secure the transmission of data between the CardDAV server and the mobile device, select the **Use SSL connection** check box.

13. If necessary, in the **Per App VPN** section, configure Per App VPN.

14. Click **Add**.

    The new CardDAV account appears in the list.

    > You can modify or delete CardDAV accounts in the list using the **Edit** and **Delete** buttons at the top of the list.

15. Click **OK**.

16. Click **Save** to save the changes you have made.

Mobile device settings are changed after the next device synchronization with the iOS MDM Server.

As a result, once the policy is applied, CardDAV accounts from the compiled list will be added on the user's mobile device.

> If you experience problems when adding or updating accounts, check whether the settings you configured are correct.

Adding a calendar account

To let an iOS MDM device user access their calendar events on a CalDAV server, add a CalDAV account. Synchronization with the CalDAV server lets the user create and receive invitations, receive event updates, and synchronize tasks with the Reminders app.

To add an iOS MDM device user's CalDAV account:

1. In the main window of Kaspersky Next Expert View (on-premise), select **Asset management** → **Policies**. In the list of group policies that opens, click the name of the policy that you want to configure.
2. In the policy properties window, select **Application settings**.
3. Select **iOS** and go to the **Device configuration** section.
4. On the **Calendar** card, click **Settings**.

   The **Calendar** window opens.
5. Enable the settings using the **Calendar** toggle switch.
6. Click **Add**.

   The **Add CalDAV account** window opens.
7. In the **Server** section, in the **Description** field, enter a description of the user's CalDAV account.
8. In the **Server address** and **Server port** fields, enter the host name or the IP address of a CalDAV server and the number of the CalDAV server port.
9. In the **Calendar URL** field, specify the URL of the CalDAV account of the iOS MDM device user on the CalDAV server (for example, http://example.com/caldav/users/mycompany/user).

   The URL must begin with `http://` or `https://`.
10. In the **Authentication** section, in the **Account name** field, enter the account name for authorization on the CalDAV server.
11. In the **Password** field, set the CalDAV account password for authorization on the CalDAV server.
12. If you want to use the SSL (Secure Sockets Layer) data transport protocol to secure transmission of event data between the CalDAV server and the mobile device, select the **Use SSL connection** check box.
13. If necessary, in the **Per App VPN** section, configure Per App VPN.
14. Click **Add**.

    The new CalDAV account appears in the list.

    > You can modify or delete CalDAV accounts in the list using the **Edit** and **Delete** buttons at the top of the list.
15. Click **OK**.
16. Click **Save** to save the changes you have made.

Mobile device settings are changed after the next device synchronization with the iOS MDM Server.

As a result, once the policy is applied, CalDAV accounts from the compiled list is added on the user's mobile device.

If you experience problems when adding or updating accounts, check whether the settings you configured are correct.

Configuring a calendar subscription

These settings apply to supervised devices and devices operating in basic control mode.

To let the iOS MDM device user add events of shared calendars (such as a corporate calendar) to the user's calendar, add a subscription to these calendars. *Shared calendars* are calendars of other users who have a CalDAV account, iCal calendars, and other published calendars.

To add a calendar subscription:

1. In the main window of Kaspersky Next Expert View (on-premise), select **Asset management** → **Policies**. In the list of group policies that opens, click the name of the policy that you want to configure.
2. In the policy properties window, select **Application settings**.
3. Select **iOS** and go to the **Device configuration** section.
4. On the **Calendar subscriptions** card, click **Settings**.

   The **Calendar subscriptions** window opens.
5. Enable the settings using the **Calendar subscriptions** toggle switch.
6. Click **Add**.

   The **Add calendar subscription** window opens.
7. In the **Description** field, enter a description of the calendar subscription.
8. In the **Server address** field, specify the URL of a third-party calendar.

   In this field, you can enter the main URL of the CalDAV account of a user whose calendar you are subscribing to. You can also specify the URL of an iCal calendar or a different published calendar.
9. In the **User name** field, enter the user account name for authentication on the server of the third-party calendar.
10. In the **Password** field, enter the calendar subscription password for authentication on the server of the third-party calendar.
11. If you want to use the SSL (Secure Sockets Layer) data transport protocol to secure the transmission of event data between the CalDAV server and the mobile device, select the **Use SSL connection** check box.
12. If necessary, in the **Per App VPN** section, configure Per App VPN.
13. Click **Add**.

The new calendar subscription appears in the list.

> You can modify or delete calendar subscriptions in the list using the **Edit** and **Delete** buttons at the top of the list.

14. Click **OK**.
15. Click **Save** to save the changes you have made.

Mobile device settings are changed after the next device synchronization with the iOS MDM Server.

As a result, once the policy is applied, events from the shared calendar in the list will be added to the calendar on the user's mobile device.

Configuring SSO

> These settings apply to supervised devices and devices operating in basic control mode.

The **SSO** settings let you configure account settings for using Single Sign-On technology. *Single Sign-On (SSO)* is an authentication method that allows a user to sign in to multiple services with a single ID. The Kerberos protocol is used for user authentication.

To configure the use of SSO on iOS MDM devices:

1. In the main window of Kaspersky Next Expert View (on-premise), select **Asset management** → **Policies**. In the list of group policies that opens, click the name of the policy that you want to configure.
2. In the policy properties window, select **Application settings**.
3. Select **iOS** and go to the **Device configuration** section.
4. On the **SSO** card, click **Settings**.
   The **SSO** window opens.
5. Enable the settings using the **SSO** toggle switch.
6. Specify the following settings:
   - In the **Account name** field, specify the name of the user's Single Sign-On account for Kerberos server authorization. You can either enter a value or select a macro by clicking the + button.
   - In the **Authentication** section, specify the authentication settings:
     - **Kerberos user name**

       Main name of the account of an iOS MDM device user on the Kerberos server. The Kerberos user name is case-sensitive and must be specified in the format `<primary>/<instance>`, where:

       1. `<primary>` is the user name.
       2. `<instance>` is a description of the primary name, such as "admin". The instance may be omitted.

Example: if the Kerberos user name is `mycompany/admin@EXAMPLE.COM` or `mycompany@EXAMPLE.COM`, you must enter `mycompany/admin` or `mycompany` respectively.

You can either enter a value or select a macro by clicking the + button.

> Do not use the at sign (@) in this field. Otherwise the SSO profile will not be applied on the device.

- **Kerberos scope**

  Name of the network to which Kerberos servers and iOS MDM devices belong. The scope must be entered using uppercase letters.

  The network name must match the domain name. For example, if the names match, the name of the scope for the example.com domain is `EXAMPLE.COM`.

  Example: if the Kerberos user name is `mycompany/admin@EXAMPLE.COM`, you must enter `EXAMPLE.COM`.

- **Authentication certificate**

  The certificate used for user authentication.

- In the **URL prefixes** section, specify the addresses of websites on which Kaspersky Mobile Devices Protection and Management allows using SSO:

  - **Limit account to the listed URLs**

    Use of Single Sign-On for automatic sign-in only to websites added to the list of allowed web addresses. You can create a list of allowed web addresses by clicking the **Add URL** button next to the check box.

    If the check box is selected, the user can use Single Sign-On for authorization on websites that have been added to the list of allowed web addresses.

    If the check box is cleared or the list is empty, the user can use Single Sign-On for all websites within the **Kerberos scope**.

    Name of the network to which Kerberos servers and iOS MDM devices belong. The scope must be entered using uppercase letters.

    The network name must match the domain name. For example, if the names match, the name of the scope for the example.com domain is `EXAMPLE.COM`.

    Example: if the Kerberos user name is `mycompany/admin@EXAMPLE.COM`, you must enter `EXAMPLE.COM`.

    This check box is cleared by default.

  - **Add URL**

    Clicking the button adds the **URL prefix** field for specifying a new website in the list of web addresses for which automatic Single Sign-On is allowed.

    The button is available if the **Limit account to the listed URLs** check box is selected.

    The web address must begin with `http://` or `https://`. Automatic Single Sign-On is performed only when the URL fully matches the URL template. For example, the web address `https://example.com/` does not match the web address `https://example.com:443/`.

    To allow Single Sign-On access only to websites that use the HTTP protocol, enter the value `http://`. To allow access only to websites that use the secure HTTPS protocol, enter `https://`.

    If the web address does not end with the "/" symbol, Kaspersky Mobile Devices Protection and Management adds this symbol automatically.

    If the list of allowed web addresses is empty, the user can use Single Sign-On to automatically sign in to all websites within the **Kerberos scope**.

Name of the network to which Kerberos servers and iOS MDM devices belong. The scope must be entered using uppercase letters.

The network name must match the domain name. For example, if the names match, the name of the scope for the example.com domain is `EXAMPLE.COM`.

Example: if the Kerberos user name is `mycompany/admin@EXAMPLE.COM`, you must enter `EXAMPLE.COM`.

- In the **Bundle IDs** section, specify the IDs of apps in which Kaspersky Mobile Devices Protection and Management allows using SSO:

  - **Limit account to the listed apps**

    Using Single Sign-On for automatic sign-in to apps added to the list of bundle identifiers. You can create a list of bundle IDs by clicking the **Add app** button next to the check box.

    If the check box is selected, the user can use Single Sign-On only for authorization in apps that have been added to the list of bundle IDs.

    If the check box is cleared or the list is empty, the user can use Single Sign-On for all apps within the **Kerberos scope**.

    Name of the network to which Kerberos servers and iOS MDM devices belong. The scope must be entered using uppercase letters.

    The network name must match the domain name. For example, if the names match, the name of the scope for the example.com domain is `EXAMPLE.COM`.

    Example: if the Kerberos user name is `mycompany/admin@EXAMPLE.COM`, you must enter `EXAMPLE.COM`.

    This check box is cleared by default.

  - **Add app**

    Clicking the button adds the **Bundle ID** field for specifying a new bundle ID in the list of apps for which automatic Single Sign-On is allowed.

    The button is available if the **Limit account to the listed apps** check box is selected.

    Automatic Single Sign-On is performed only when the added ID fully matches the bundle ID. For example: `com.mycompany.myapp`.

    To grant access to several apps using Single Sign-On, use the "*" symbol after the "." character. For example: `com.mycompany.*`. Access will be allowed to all apps whose bundle ID begins with the specified prefix.

    If the list of bundle IDs is empty, the user can use Single Sign-On to automatically sign in to all apps within the **Kerberos scope**.

    Name of the network to which Kerberos servers and iOS MDM devices belong. The scope must be entered using uppercase letters.

    The network name must match the domain name. For example, if the names match, the name of the scope for the example.com domain is `EXAMPLE.COM`.

    Example: if the Kerberos user name is `mycompany/admin@EXAMPLE.COM`, you must enter `EXAMPLE.COM`.

7. Click **OK**.

8. Click **Save** to save the changes you have made.

Mobile device settings are changed after the next device synchronization with the iOS MDM Server.

As a result, once the policy is applied, SSO is configured on the iOS MDM device.

Managing Web Clips

A *Web Clip* is an app that opens a website from the home screen of a mobile device. By clicking Web Clip icons on the home screen of the device, the user can quickly open websites (such as the corporate website). Web Clips may also pop-up if the user taps and holds the Kaspersky Endpoint Security for Android app icon.

You can add or delete Web Clips on user devices and specify icons displayed on the screen. Web Clips can be added on both Android and iOS MDM devices.

Managing Web Clips on Android devices

To manage Web Clips on a user's Android device:

1. In the main window of Kaspersky Next Expert View (on-premise), select **Asset management** → **Policies**. In the list of group policies that opens, click the name of the policy that you want to configure.
2. In the policy properties window, select **Application settings**.
3. Select **Android** and go to the **Device configuration** section.
4. On the **Web Clips** card, click **Settings**.

   The **Web Clips** window opens.
5. Enable the settings using the **Web Clips** toggle switch.
6. Click **Add**.

   The **Add Web Clip** window opens.
7. In the **Web Clip name** field, enter the name of the Web Clip to be displayed on the home screen of the Android device.
8. In the **Website URL** field, enter the web address of the website that will open when the user taps the Web Clip icon. The address should begin with `http://` or `https://`.

   Use only legitimate and trusted sources. By configuring the settings in this field, you are solely responsible for any potential risks and consequences associated with using unreliable sources.

   If the entered website is forbidden or is not on the list of allowed websites in the **Web Control** settings of the policy, users will not be able to access this website via the Web Clip.
9. Click **Select** to specify the image for the Web Clip icon.

   The image must meet the following requirements:

   - File format: PNG, JPEG, or ICO.
   - File size no larger than 1 MB.

If you do not select an image for the Web Clip, a blank square is displayed as the icon.

10. Click **Add**.

    The new Web Clip appears in the list.

    You can modify or delete Web Clips in the list using the **Edit** and **Delete** buttons at the top of the list.

11. Click **OK**.

12. Click **Save** to save the changes you have made.

Once the policy is applied to a device, the Kaspersky Endpoint Security for Android app shows notifications to prompt the user to install the Web Clips you created. After the user installs these Web Clips, the corresponding icons are added on the home screen of the device.

If there is no in-app notifications prompting the user to install Web Clips, make sure the **Device has not been synchronized with the Administration Server for a long time** check box is selected in the **Configure notifications** settings of the **KES for Android settings** section.

The deleted Web Clips are disabled on the home screen of the Android device. If the user taps the corresponding icon, a notification appears that the Web Clip is no longer available. The user should delete the Web Clip from the home screen by following a vendor-specific procedure.

Managing Web Clips on iOS MDM devices

By default, the following restrictions apply to Web Clips:

- The user cannot manually remove Web Clips from the mobile device.
- The corner rounding, shadow, and gloss visual effects are applied to the Web Clip icon on the screen.
- Websites that open when the user taps a Web Clip icon do not open in full-screen mode.

To manage Web Clips on a user's iOS MDM device:

1. In the main window of Kaspersky Next Expert View (on-premise), select **Asset management** → **Policies**. In the list of group policies that opens, click the name of the policy that you want to configure.
2. In the policy properties window, select **Application settings**.
3. Select **iOS** and go to the **Device configuration** section.
4. On the **Web Clips** card, click **Settings**.

   The **Web Clips** window opens.
5. Enable the settings using the **Web Clips** toggle switch.

6. Click **Add**.

   The **Add Web Clip** window opens.

7. In the **Web Clip name** field, enter the name of the Web Clip to be displayed on the home screen of the iOS MDM device.

8. In the **Website URL** field, enter the web address of the website that will open when the user taps the Web Clip icon. The address should begin with `http://` or `https://`.

   Use only legitimate and trusted sources. By configuring the settings in this field, you are solely responsible for any potential risks and consequences associated with using unreliable sources.

   If the entered website is forbidden or is not on the list of allowed websites in the **Web Control** settings of the policy, users will not be able to access this website via the Web Clip.

9. Click **Select** to specify the image for the Web Clip icon.

   The image must meet the following requirements:

   - Image size no greater than 400 x 400 pixels.
   - File format: PNG, JPEG, or ICO.
   - File size no larger than 1 MB.

   If you do not select an image for the Web Clip, a blank square is displayed as the icon.

   If the selected image has a transparent background, the background will be black on the device.

10. In the **Options** section, specify the following additional settings:

    a. If you want to allow the user to remove the Web Clip from the iOS MDM device, select the **Allow removal of Web Clip** check box.

    b. If you want the Web Clip icon to be displayed without special visual effects (rounding of icon corners and gloss effect), select the **Precomposed icon** check box.

    c. If you want the website to open in full-screen mode on the iOS MDM device when the user taps the icon, select the **Full screen Web Clip** check box.

       In full-screen mode, the Safari toolbar is hidden and only the website is shown on the device screen.

11. Click **Add**.

    The new Web Clip appears in the list.

    You can modify or delete Web Clips in the list using the **Edit** and **Delete** buttons at the top of the list.

12. Click **OK**.

13. Click **Save** to save the changes you have made.

Once the policy is applied, the Web Clip icons in the list you have created are added on the home screen of the user's mobile device.

The deleted Web Clips are removed from the home screen of the iOS MDM device.

Setting a wallpaper

You can set an image as the home screen wallpaper and lock screen wallpaper on users' devices that fall under the same policy.

To set a wallpaper on users' Android devices:

1. In the main window of Kaspersky Next Expert View (on-premise), select **Asset management** → **Policies**. In the list of group policies that opens, click the name of the policy that you want to configure.
2. In the policy properties window, select **Application settings**.
3. Select **Android** and go to the **Device configuration** section.
4. On the **Custom wallpapers** card, click **Settings**.

   The **Custom wallpapers** window opens.
5. Enable the settings using the **Custom wallpapers** toggle switch.
6. In the **Home screen wallpaper** section, in the **How to set wallpaper** drop-down list, select the method for specifying the wallpaper:

   - **Upload file**

     For this option, you need to upload a PNG or JPEG image no larger than 1 MB from your computer.

   - **Download image from the internet**

     For this option, you need to specify a URL beginning with `http://` or `https://`. Use only trusted URLs.
7. Add an image to be used as a wallpaper:

   Use only legitimate and trusted sources. By configuring the settings in this section, you are solely responsible for any potential risks and consequences associated with using unreliable sources.

   - If you selected the **Upload file** option, click **Select** to upload an image. When the upload is finished, an image preview will be displayed.
   - If you selected the **Download image from the internet** option, specify the link to the image in the **Link to image** field. You can click **Open preview** to view the image in a new browser tab.
8. If you want to use the same image as the lock screen wallpaper, in the **Lock screen wallpaper** section, select the **Use home screen wallpaper for lock screen** check box.

9. Click **OK**.
10. Click **Save** to save the changes you have made.

The imported image is set as a wallpaper on users' devices.

Adding fonts

These settings apply to supervised devices and devices operating in basic control mode.

To add a font on a user's iOS MDM device:

1. In the main window of Kaspersky Next Expert View (on-premise), select **Asset management** → **Policies**. In the list of group policies that opens, click the name of the policy that you want to configure.
2. In the policy properties window, select **Application settings**.
3. Select **iOS** and go to the **Device configuration** section.
4. On the **Custom fonts** card, click **Settings**.

   The **Custom fonts** window opens.
5. Enable the settings using the **Custom fonts** toggle switch.
6. Click **Add**.
7. Select the font file saved on your computer. The file must have the .TTF or .OTF extension.

   Fonts with the .TTC or .OTC extension are not supported.

   Fonts are identified using the PostScript name. Do not install fonts with the same PostScript name even if their content is different. Installing fonts with the same PostScript name will result in an error.
8. Click **Open**.

   The new font appears in the list.

   You can delete fonts in the list using the **Delete** button at the top of the list.
9. Click **OK**.
10. Click **Save** to save the changes you have made.

Mobile device settings are changed after the next device synchronization with the iOS MDM Server.

As a result, once the policy is applied, the user will be prompted to install fonts from the list that has been created.

Working with commands for mobile devices

This section contains information about commands for managing mobile devices supported by Kaspersky Security Center. It provides instructions on how to send commands to mobile devices, as well as how to view the execution statuses of commands in the command history.

Commands for mobile devices

Kaspersky Security Center supports commands for remote mobile device management. For instance, if a mobile device is lost or stolen, you can send commands to locate the device or wipe all corporate data from the device.

You can send commands to the following types of managed mobile devices:

- Android devices managed via the Kaspersky Endpoint Security for Android app
- iOS MDM devices

Each device type supports a dedicated set of commands.

You can cancel commands in the **Command history**.

Commands may be delivered almost immediately to devices connected to the internet. As a result, they may fail to cancel despite being displayed as canceled.

Commands for Android devices

Command	Result
Lock device	The mobile device is locked. To obtain access to data, you must unlock the device using the **Unlock device** command or a one-time passcode.
Unlock device	The mobile device is unlocked. After unlocking a device running Android 5 – 6, the screen unlock password is reset to "1234". After unlocking a device running Android 7 or later, the screen unlock password is not changed.
Reset to factory settings	All data is deleted from the mobile device and the settings are rolled back to their factory values. After this command is executed, the device will not be able to receive or execute subsequent commands. This command is unavailable for personal devices and devices with a corporate container running Android 14 or later.
Wipe corporate data	Corporate data is wiped from the device. The list of wiped data depends on the mode the device is operating in: • On a personal device, the Knox container, corporate files sent to the device, and mail certificate are wiped. • On a corporate device, the Knox container, corporate files sent to the device, and the certificates installed by Kaspersky Endpoint Security for Android (mail, VPN, and SCEP profile certificates, except the mobile certificates) are wiped. • Additionally, if a corporate container was created, the corporate container (its contents, corporate files sent to the device, configurations, and restrictions) and the certificates installed in the corporate container (mail, VPN, and SCEP profile certificates, except the mobile certificates) are wiped.

Command	Result
Synchronize device	The mobile device data is synchronized with the Administration Server. The *Executed* status may be displayed when the command has been successfully sent but not yet received by the device.
Locate device	The mobile device's location coordinates are obtained. Location timestamps are displayed according to the Kaspersky Security Center server time. To view the device location in Yandex.Maps, go to the **Asset management** → **Mobile** → **Devices** section. Then choose a device and select **Command history** → **Locate device** → **Device coordinates** → **View on map**. After you click **View on map**, the device coordinates are transferred to Yandex.Maps and the device is shown on a map. On devices running Android 12 or later, if the user granted the "Use approximate location" permission, the Kaspersky Endpoint Security for Android app first tries to get the precise device location. If this is not successful, the approximate device location is returned only if it was received within the past 30 minutes. Otherwise, the command fails. This command does not work on Android devices if Google Location Accuracy is disabled in the settings. Please be aware that not all Android devices come with this location setting.
Take photos	The mobile device is locked. Photos are taken using the front camera of the device when somebody attempts to unlock the device. On devices with a pop-up front camera, the photo will be black if the camera is stowed. When attempting to unlock the device, the user automatically consents to having their photo taken on the device. If the permission to use the camera has been revoked, the mobile device displays a notification and prompts to provide the permission. On a mobile device running Android 12 or later, if the permission to use the camera has been revoked via Quick Settings, the notification is not displayed but the taken photo is black.
Sound alarm	The mobile device sounds an alarm for 5 minutes (for 1 minute if the device battery is low) or until the user unlocks the device.
Wipe app data	The data of a specified app is wiped from the mobile device. For this action, you need to specify the package name for the app whose data is to be deleted. As a result, the app is rolled back to its default state. The data of system and administrative apps is not wiped.
Wipe data of all apps	The data of all apps is wiped from the mobile device. On a corporate device, the data of all apps on the device is wiped. On a device with a corporate container, the data of all apps in the corporate container is wiped. As a result, apps are rolled back to their default state. The data of system and administrative apps is not wiped.
Send message	A message with the specified title and text is sent to the user's mobile device. You can send only a push notification or both a push notification and an alert.

Command	Result
Get location history	The mobile device's location history for the last 14 days is displayed. Location timestamps are displayed according to the device time. To view the device location in Yandex.Maps, go to the **Asset management** → **Mobile** → **Devices** section. Then choose a device and select **Command history** → **Get location history** → **View on map**. After you click **View on map**, the device coordinates are transferred to Yandex.Maps and the device is shown on a map. Due to technical limitations on Android devices, the device location may be retrieved less often than specified in the **Location tracking** settings.
Reboot device	The mobile device is rebooted. The command execution result will be sent to Kaspersky Security Center after the user unlocks their device. The device cannot be rebooted during a call. Kaspersky Endpoint Security for Android will attempt to execute the command again after the call ends. This command is available only for corporate devices running Android 7 or later.
Reset password	The unlock password of the corporate device or corporate container is reset. This command is unavailable for personal devices.

Commands for iOS MDM devices

Command	Result
Lock device	The mobile device is locked. To access data, you must unlock the device.
Reset unlock password	The mobile device's screen unlock password is reset, and the user is prompted to set a new password in accordance with policy requirements.
Reset to factory settings	All data is deleted from the mobile device and the settings are rolled back to their factory values. After this command is executed, the device will not be able to receive or execute subsequent commands.
Wipe corporate data	All installed configuration profiles, the management profile, and apps for which the **Remove when management profile is deleted** check box has been selected are removed from the device.
Synchronize device	The mobile device data is synchronized with the Administration Server.
Install configuration profile	A configuration profile is installed on the mobile device. You cannot install a configuration profile with settings for a supervised device on a device in basic control mode.
Delete configuration profile	The configuration profile is deleted from the mobile device. The profile may be displayed in the list of configuration profiles installed on the device for several minutes after it has been deleted.
Install app	The specified app is installed on the mobile device.
Update app	The specified app is updated on the mobile device.
Delete app	The specified app is removed from the mobile device.

Command	Result
OS update (supervised only)	Operating system updates are scheduled on the mobile device according to the specified update settings. This command may fail to be executed when a device does not have enough storage space or the specified OS version is not available for the selected device. We recommend specifying the latest available OS version.
Change roaming settings	Data roaming and voice roaming are enabled or disabled.
Set Bluetooth state (supervised only)	Bluetooth is enabled or disabled on the mobile device. This command is supported only for supervised devices running iOS 11.3 or later.
Enable Lost Mode (supervised only)	Lost Mode is enabled on the supervised mobile device, and the device is locked. The device screen shows a message and phone number that you can edit. If you send the Enable Lost Mode command to a supervised iOS MDM device without a SIM card and this device is restarted, the device won't be able to connect to Wi-Fi and receive the Disable Lost Mode command. This is a specific feature of iOS devices. To avoid this issue, you can either send the command only to devices with a SIM card, or insert a SIM card into the locked device to allow it to receive the Disable Lost Mode command over the mobile network.
Locate device (Lost Mode only)	The location of the mobile device is obtained. To view the device location in Yandex.Maps, go to the **Asset management** → **Mobile** → **Devices** section. Then choose a device and select **Command history** → **Locate device** → **Device coordinates** → **View on map**. After you click **View on map**, the device coordinates are transferred to Yandex.Maps and the device is shown on a map.
Sound alarm (Lost Mode only)	A sound is played on the lost mobile device.
Disable Lost Mode (supervised only)	Lost Mode is disabled on the mobile device, and the device is unlocked.

Permissions for executing commands

Special rights and permissions are required for executing Kaspersky Endpoint Security for Android commands. When the Initial Configuration Wizard is running, Kaspersky Endpoint Security for Android prompts the user to grant the application all required rights and permissions. The user can skip these steps or later disable these permissions in the device settings. If this is the case, it will be impossible to execute commands.

On devices running Android 10 or later, the user must grant the "All the time" permission to access the location. On devices running Android 11 or later, the user must also grant the "While using the app" permission to access the camera. Otherwise, Anti-Theft commands will not function. The user will be notified of this limitation and will again be prompted to grant the required level of permissions. If the user selects the "Only this time" option for the camera permission, access is considered granted by the app. We recommend contacting the user directly if the Camera permission is requested again.

Sending commands

To send a command to the user's mobile device:

1. In the main window of Kaspersky Next Expert View (on-premise), select **Asset management** → **Mobile** → **Devices**.
2. In the list of devices that opens, select a device that you want to send a command to.

   You can select multiple devices.

3. Click **Send command**.
4. In the **Send command** window that opens, in the **Command** field, select a command.
5. Configure the command that you want to send.
6. Click **Send**.

   You can view and cancel commands in the **Command history**.

The command is sent to the devices you selected.

Viewing the statuses of commands in the command history

The application saves information about all commands that have been sent to mobile devices to the command history. The command history contains information about the time and date that each command was sent to the mobile device, their statuses, and descriptions of the results. For example, when a command fails, the history displays the cause of the error.

Commands sent to mobile devices can have the following statuses:

- *Sent*

  The command has been sent to the mobile device.

- *Executed*

  Execution of the command has succeeded.

- *Error*

  Execution of the command failed.

- *Canceling*

  The command is being removed from the queue of commands sent to the mobile device.

- *Canceled*

  The command has been successfully removed from the queue of commands sent to the mobile device.

The application maintains a command history for each mobile device.

To view the command history:

1. In the main window of Kaspersky Next Expert View (on-premise), select **Asset management** → **Mobile** → **Devices**.
2. In the list of mobile devices, select the one for which you want to view the command history.
3. Click **Command history**.

   The **Command history** window opens. The sections of the **Command history** window correspond to the commands that can be sent to the mobile device.
4. Select sections containing the necessary commands and view information about how the commands are sent and executed.

Managing the app by using third-party EMM solutions (Android only)

You can use Kaspersky Endpoint Security for Android without Kaspersky Administration Systems. Use other EMM (Enterprise Mobility Management) service providers' solutions to deploy and manage Kaspersky Endpoint Security for Android. Kaspersky participates in the AppConfig Community to ensure that the app operates with third-party EMM solutions.

Also, you can use a third-party EMM solution only to deploy Kaspersky Endpoint Security for Android and then manage devices in the Kaspersky Next Expert View (on-premise) after deployment.

If Kaspersky Endpoint Security for Android is deployed using a third-party EMM solution, you cannot manage the app in Kaspersky Endpoint Security Cloud but you can manage the app in the EMM Console, Kaspersky Next Expert View (on-premise), or Kaspersky Security Center Cloud Console.

You can perform the following actions in the EMM Console:

- Deploy the app to an Android work profile created by a third-party EMM solution.
- Activate the app.
- Configure app settings:
  - Enable protection against malicious and phishing websites on the internet.
  - Configure settings for connecting the device to Kaspersky Security Center.
  - Configure Anti-Malware settings.
  - Configure the schedule for running a malware scan on the device.
  - Enable detection of adware and apps that could be exploited by criminals to harm the user's device or personal data.
  - Configure the schedule for app database updates.

If Kaspersky Endpoint Security for Android is deployed in an Android work profile created by a third-party EMM solution, the following limitations apply:

- The following features are not available:
  - Remote control for Android
  - Call Control
- The following commands do not affect a work profile:
  - **Lock device**
  - **Take photos**
  - Commands that manage a corporate container (for example, **Wipe corporate data**)
- Settings in the following policy sections cannot be applied:
  - **Wi-Fi**
  - **Custom wallpapers**
  - **Corporate container on devices**
- You cannot protect Kaspersky Endpoint Security for Android against removal.
- When you set password requirements for the device, they are applied to the work profile password.
- In the list of mobile devices, the device is displayed as personal.
- A root certificate cannot be installed to the work profile.
- The **Reset to factory settings** command results in the removal of the work profile.
- To turn off the sound after sending the **Sound alarm** command, you can simply wake the device from sleep mode, regardless of whether the device has a password.

Getting started

Kaspersky Endpoint Security for Android is currently not available in Google Play.

To deploy Kaspersky Endpoint Security for Android on users' devices, you must add the app to the EMM app store using the APK installation file from the Kaspersky website. For more details about working with apps in the EMM Console, visit the *technical support website of the EMM service provider*.

Kaspersky Endpoint Security for Android is deployed in an Android work profile created by a third-party EMM solution. The app is isolated from the user's personal data and protects only corporate data in the work profile.

We recommend protecting the Kaspersky Endpoint Security for Android app from removal by the EMM Console's tools.

How to install the app

If you want to manage devices in a third-party EMM console, you can distribute the app using the APK file from the Kaspersky website.

The following permissions are required for the app to work:

- Storage permission for accessing files when Anti-Malware is running (only for Android 6 or later).
- Phone permission for identifying the device, for example, when activating the app.
- Device administrator permission for the main protection features, such as Anti-Theft and App Control.
- Request to add Kaspersky Endpoint Security for Android to the list of apps that are started at operating system startup (on certain devices, such as HUAWEI, Meizu, and Xiaomi). If the add request is not displayed, manually add Kaspersky Endpoint Security for Android to the list of startup apps. The request may not be displayed if the Security app is not installed in the work profile.

You can grant the required permissions in the EMM Console before deploying the Kaspersky Endpoint Security for Android app. For more details about granting the permissions in the EMM Console, visit the *technical support website of the EMM service provider*. You can also grant the permissions while completing the Initial Configuration Wizard of Kaspersky Endpoint Security for Android on the device.

Kaspersky Endpoint Security for Android will be installed in the Android work profile created by the third-party EMM solution. The app will then be updated from the Kaspersky website or using HUAWEI AppGallery, Samsung Galaxy Store, RuStore, or Xiaomi GetApps.

For operation of Web Protection, you must also configure a proxy server in Google Chrome settings using AppConfig via the third-party EMM system:

- Proxy server configuration mode: manual.
- Proxy server address and port: 127.0.0.1:3128.
- SPDY protocol support: disabled.
- Data compression through proxy server: disabled.

Protecting devices on the internet

To protect the personal data of a mobile device user on the internet, enable Web Protection. Web Protection blocks malicious websites that distribute malicious code, and phishing websites designed to steal your confidential data and gain access to your financial accounts. Web Protection uses the Kaspersky Security Network cloud service to scan websites before you open them.

For the Web Protection component to work, the following conditions must be met:

- The proxy server is configured in the browser settings:

  ```
  ProxyMode = "fixed_servers"
  ```

`ProxyServer = "127.0.0.1:3128"`

`DisableSpdy = true`

`DataCompressionProxyEnabled = false`

The proxy server configuration may depend on the Google Chrome version. For more details about configuring Google Chrome, visit the Chromium project website.

After the Kaspersky Endpoint Security for Android app is removed from the mobile device, reset the proxy server settings.

- Device users accept the Privacy Policy and the Web Protection Statement in the Initial Configuration Wizard or app settings.

  The administrator can accept the Web Protection Statement in the Kaspersky Next Expert View (on-premise).

- Web Protection is enabled in the app settings:

  `EnableWebFilter = True`, `EnableWebFilterLock = True`.

- Use of KSN is enabled in the app settings: `UseKsnMode = Recommended` or `UseKsnMode = Extended`.

If users' devices are connected to the Kaspersky Security Center, enable Web Protection in the group policy. Also, you can accept the Web Protection Statement in the Kaspersky Next Expert View (on-premise).

After enabling Web Protection in the Kaspersky Endpoint Security for Android app and configuring Google Chrome, check protection against web threats. To check protection, you can use the EICAR test file.

How to activate the app

Information about the license is sent to the mobile device together with the other settings in the configuration file.

If the app is not activated within 30 days after its installation on the mobile device, the trial license expires. When the trial license expires, all features of Kaspersky Endpoint Security for Android are disabled.

When a commercial license expires, the app continues running with limited functionality (for example, Kaspersky Endpoint Security for Android database updates are not available). To continue using the full functionality of the app, you must renew your commercial license.

To activate Kaspersky Endpoint Security for Android:

1. In the EMM Console, open the settings of the Kaspersky Endpoint Security for Android app.
2. In the `LicenseActivationCode` field, enter the app activation code.

   To activate the app on a device, you must have access to Kaspersky activation servers.

How to connect a device to Kaspersky Security Center

After Kaspersky Endpoint Security for Android is installed on a mobile device, you can connect the device to Kaspersky Security Center. The data necessary for connecting the device to Kaspersky Security Center is sent to the mobile device together with the other settings listed in the configuration file. After connecting the device to Kaspersky Security Center, you can use group policies to centrally configure the app settings. You can also receive reports and statistics on the performance of Kaspersky Endpoint Security for Android.

Prior to connecting devices to Kaspersky Security Center, make sure that the following conditions are fulfilled:

- Kaspersky Mobile Devices Protection and Management plug-in is installed on the host of the Kaspersky Next Expert View (on-premise).
- The port for connecting mobile devices is opened in the Administration Server properties.
- A mobile certificate for identifying the mobile device user has been created in the Administration Server properties of Kaspersky Security Center.

Prior to connecting devices to Kaspersky Security Center, we recommend doing the following:

- If you want to create policies for mobile devices, create a separate administration group for mobile devices. Only the personal device operating mode is supported by third-party EMM solutions.
- If you want to automatically move mobile devices to a separate administration group, create a rule for automatically moving devices from the **Unassigned devices** folder.
- If you want to centrally configure Kaspersky Endpoint Security for Android, create a group policy.

To connect a device to Kaspersky Security Center:

1. In the EMM Console, open the settings of the Kaspersky Endpoint Security for Android app.
2. In the `KscServer` field, enter the DNS name or IP address of the Kaspersky Security Center Administration Server. The default port is 13292.
3. If you do not want the user to be distracted by Kaspersky Endpoint Security for Android notifications, disable app notifications. To do so, set `DisableNotification = True`.

   After connecting, the app shows all notifications. You can disable certain app notifications in the policy settings.

   Do not disable app notifications if you do not use Kaspersky Security Center. This could cause a user to not receive notifications about the license expiring. As a result, the app will stop performing its functions.

After the connection settings are configured, Kaspersky Endpoint Security for Android displays a notification prompting you to grant the following additional rights and permissions:

- Permission to use the camera for Anti-Theft operation (**Take photos** command).
- Permission to use the location for Anti-Theft operation (**Locate device** command).
- Device administrator rights (Android work profile owner) for operation of the following app functions:
  - Configure Wi-Fi.
  - Restrict use of the camera, Bluetooth, and Wi-Fi.

Due to the specific characteristics of a third-party Android work profile, Anti-Theft features are unavailable in the app and the App Control cannot block apps by their category.

When the user grants the necessary rights and permissions, the device will be connected to Kaspersky Security Center. If a rule for automatically moving devices to an administration group has not been created, the device will be automatically added to the **Unassigned devices** folder. If a rule for automatically moving devices to an administration group has been created, the device will be automatically added to the specified group.

Kaspersky Endpoint Security provides the following device name format: Device model [device ID, email].

You can also add a tag to the device name. This makes it easier to find and sort devices in Kaspersky Security Center.

To add the tag to the device name:

1. In the EMM Console, open the settings of the Kaspersky Endpoint Security for Android app.
2. In the `KscDeviceNameTag` field, select the values:
   - `{DeviceSerialNumber}` – Serial number of the device.
   - `{DeviceUid}` – Unique device identifier (UDID).
   - `{DeviceAssetNumber}` – Device asset number. This number is created internally from within your organization.

   We recommend using only these values.

You can add some values (for example, `{DeviceSerialNumber} {DeviceUid}`). The tag will be added to the device name in Kaspersky Security Center. A space separates the tag and the device name. For example, if the device name is `Google Pixel 2 a10c6b75f7b31de9 22:7D:78:9E:C5:1E`, then the UDID tag is `22:7D:78:9E:C5:1E`.

After the device is connected to Kaspersky Security Center, the app settings will be changed according to the group policy. Kaspersky Endpoint Security for Android ignores the app settings from the configuration file that was configured in the EMM Console. You can configure all sections of the policy except the following sections:

- **Anti-Theft**
- **Screen unlock settings**
- The **App use** tab of the **App Control** section
- **Corporate container on devices**
- **Samsung Knox settings**

Due to the method used to deploy a third-party work profile, you cannot apply group policy settings from the **Corporate container on devices** section. These settings can be applied only if the corporate container was created using Kaspersky Security Center.

Silent mode

An Android device user can disable all notifications from Kaspersky Endpoint Security for Android in the settings on the notification bar. If notifications are disabled, the user does not monitor the operation of the app and may not see important information (for example, real-time information about threats). In this case, to find out the app operating status, the user must open Kaspersky Endpoint Security for Android.

If you do not want the mobile device user to be distracted by Kaspersky Endpoint Security for Android notifications, you can disable certain notifications.

The Kaspersky Endpoint Security uses the following tools to display the device protection status:

- **Protection status notification**. This notification is pinned to the notification bar. The protection status notification cannot be removed. It displays the device protection status (for example,) and number of issues, if any. You can tap the device protection status and see the list of issues in the app.
- **App notifications**. These notifications inform the device user about the application (for example, threat detection).
- **Pop-up messages**. Pop-up messages require action from the device user (for example, what action to take when a threat is detected).

The silent mode settings are sent to the mobile device together with the other settings in the configuration file. Set the `DisableNotification` parameter to `True`.

If the device is connected to Kaspersky Security Center, you can enable silent mode only in the group policy.

AppConfig file

A configuration file is generated to configure the app in an EMM Console. The app settings in the configuration file are presented in the table below.

Configuration key	Description	Type	Value	Default value
`LicenseActivationCode`	App activation code	String	App activation code consisting of 20 Latin letters and numerals. To activate the app by using the activation code, you need internet access to connect to Kaspersky activation servers. If you leave the field blank, the app will be activated with a trial license. The trial license is valid for 30 days. When the trial license expires, all features of the Kaspersky Endpoint Security for Android mobile app are disabled. To continue using the app, you must purchase a commercial license.	
`EulaAcceptanceConfirmationV1`	<License Agreement link>	Choice	`Accepted` – I confirm that I have fully read, understand, and accept the terms and conditions of this End User License Agreement. `Declined` – I do not accept the terms and conditions of this End User License Agreement (EULA). To accept the terms and conditions of the EULA for all mobile devices, you need internet access to connect to Kaspersky servers. If you chose `Declined`, the app will ask the user to accept the terms and conditions of the EULA. Mobile device users can accept the conditions in the Initial Configuration Wizard.	
`EulaAcceptanceCodeV1`	License Agreement code	String	Use `EulaAcceptanceCodeV1` if you want to accept a single End User License Agreement (EULA). Use `EulaAcceptanceCodesV2` if you want to accept several EULAs at the same time. The `EulaAcceptanceCodesV2` field must contain a semicolon-separated list of EULA codes: `"<EULAid1>;<EULAid2>;<EULAid3>;..."`. License Agreement code is contained in the End User License Agreement. *To learn License Agreement code:* 1. Copy the License Agreement link (`EulaAcceptanceConfirmationV1`) from the EMM Console. 2. Paste the link into the browser. The End User License Agreement (EULA) opens. 3. Read the terms and conditions of this EULA and find the License Agreement code. To accept the terms and conditions of the EULAs for all mobile devices, you need internet access to connect to Kaspersky servers. If you leave the fields blank, the app will ask the user to accept the terms and conditions of the EULAs. Mobile device user can accept the conditions in the Initial Configuration Wizard. If you specify the values of both fields, the terms and conditions of all EULAs specified in them will be accepted.	
`EulaAcceptanceCodesV2`	License Agreement codes	String		
`KscServer`	Kaspersky Security Center Administration Server address and port	String	DNS name or IP address of the Kaspersky Security Center Administration Server and port number. Enter the address as follows: `<server address>:<port>`. If you enter the server address without specifying the port, the app will use the default port 13292.	`<server address>:13292`

Configuration key	Description	Type	Value	Default value
`DisableNotification`	Disable app notifications before connecting to Kaspersky Security Center	Boolean	`True` – Kaspersky Endpoint Security for Android hides all app notifications until the device connects to Kaspersky Security Center. After connecting, the app shows all notifications. You can disable certain app notifications in the policy settings. Do not disable app notifications if you do not use Kaspersky Security Center. This could cause a user to miss receiving notifications about a license expiration. In this case, the app would stop performing its functions. `False` – Kaspersky Endpoint Security for Android shows all app notifications.	`False`
`ScanScheduleType`	Scan run mode	Choice	`AfterUpdate` – Start a malware scan after a database update. The app updates anti-malware databases according to the defined schedule (`UpdateScheduleType`). `Daily` – Start a malware scan once a day. Configure the scan start time (`ScanScheduleTime`). `Weekly` – Start a malware scan once a week. Select the day of the week to start a malware scan (`ScanScheduleDay`) and configure the time (`ScanScheduleTime`). `Off` – Autostart of a malware scan is disabled. Irrespective of which value is set, the device user can manually start a malware scan.	`AfterUpdate`
`ScanScheduleDay`	Day of scan	Choice	`Monday / Tuesday / Wednesday / Thursday / Friday / Saturday / Sunday` You can select only one value for this setting.	`Monday`
`ScanScheduleTime`	Time of scan	String	The time can be indicated in 24-hour format (for example, 13:00) or 12-hour format (for example, 10:30 PM).	`8:00`
`ScanScheduleLock`	Block configuration of the scan run mode	Boolean	`True` – The user cannot access the malware scan run mode settings within the app settings. `False` – The user can configure the malware scan run mode and, for example, disable autostart of a malware scan.	`True`
`ScanActionOnThreatFound`	Action on threat detection (malware scan)	Choice	`Quarantine` – The app puts detected objects in Quarantine. Quarantine stores files as archives, so they cannot harm the device. The Quarantine lets you delete or restore the files that were moved to isolated storage. `Delete` – The app deletes the detected objects. `Skip` – The app leaves the detected objects unchanged. If the detected objects have been skipped, Kaspersky Endpoint Security for Android warns the user about problems in device protection. When there is an attempt to access an object on the device (such as an attempt to copy or open it), the app blocks access to the object. `AskUser` – The app prompts the user to select an action for each detected object: skip, quarantine, or delete. When multiple objects are detected, the user can apply a selected action to all objects. Information about detected threats and the actions taken on them is logged in app reports.	`Quarantine`

Configuration key	Description	Type	Value	Default value
`ScanLock`	Block configuration of scan settings	Boolean	`True` – The following scan settings cannot be accessed by the user in the app settings: the type of files to scan, scanning of archives, and the action to take when a threat is detected. `False` – The user can configure scan settings and, for example, select the `Skip` action for detected threats.	`True`
`ScanAndProtectionAdwareRiskware`	Block adware, autodialers, and apps that can be used by criminals to cause harm to the user's device and data	Boolean	`True` – The app detects adware and other apps that can be used by criminals to cause harm to the user's device and data. `False` – The app skips adware and other apps that can be used by criminals to cause harm to the user's device and data.	`True`
`ProtectionMode`	Real-time protection mode	Choice	`Recommended` – The app only scans new apps once, immediately after they have been installed, as well as files from the Downloads folder. `Extended` – The app scans all files that the user opens, modifies, copies, runs and saves on the device. The app also scans new apps and files from the Downloads folder. `Disabled` – Real-time protection is disabled.	`Recommended`
`UseKsnMode`	Kaspersky Security Network mode	Choice	`Recommended` – The app exchanges data with Kaspersky Security Network (KSN). Kaspersky Endpoint Security for Android uses KSN for real-time protection of the device against threats (Cloud Protection) and the operation of Web Protection on the internet. `Extended` – The app exchanges data with Kaspersky Security Network and also sends the Virus Laboratory certain performance statistics from Kaspersky Endpoint Security for Android. This information makes it possible to keep track of threats in real time. No personal data is collected, processed, or stored by KSN services. `Disabled` – The app does not use data from Kaspersky Security Network. You cannot enable Web Protection (`EnableWebFilter`). The Cloud Protection component is not available for Anti-Malware.	`Recommended`
`ProtectionActionOnThreatFound`	Action on threat detection (Real-time Protection)	Choice	`Quarantine` – The app puts detected objects in Quarantine. Quarantine stores files as archives, so they cannot harm the device. Quarantine lets you delete or restore the files that were moved to isolated storage. `Delete` – The app deletes detected objects. `Skip` – The app leaves the detected objects unchanged. If the detected objects have been skipped, Kaspersky Endpoint Security for Android warns the user about problems in device protection. When an attempt is made to access an object on the device (such as an attempt to copy or open it), the app blocks access to the object. Information about detected threats and the actions taken on them is logged in app reports.	`Quarantine`
`ProtectionLock`	Block configuration of real-time protection settings	Boolean	`True` – The following real-time protection settings cannot be accessed by the user in the app settings: real-time protection mode, types of files to scan, and the action to take when a threat is detected. `False` – The user can configure real-time protection settings and, for example, can select the `Skip` action for detected threats.	`True`

Configuration key	Description	Type	Value	Default value
`UpdateScheduleType`	Databases update run mode	Choice	`Daily` – Check for new anti-malware databases and download them to devices once a day. Configure the database update start time (`UpdateScheduleTime`). `Weekly` – Check for new anti-malware databases and download them to devices once a week. Select the day of the week to start a database update (`UpdateScheduleDay`) and configure the time (`UpdateScheduleTime`). `Off` – Automatic update of anti-malware databases is disabled. Irrespective of which value is set, the device user can manually start an update of anti-malware databases.	`Daily`
`UpdateScheduleDay`	Day to start a database update	Choice	`Monday / Tuesday / Wednesday / Thursday / Friday / Saturday / Sunday` You can select only one value for this setting.	`Monday`
`UpdateScheduleTime`	Database update start time	String	The time can be indicated in 24-hour format (for example, 13:00) or 12-hour format (for example, 10:30 PM).	`8:00`
`UpdateScheduleLock`	Block configuration of the database update run mode	Boolean	`True` – The user cannot access the database update run mode settings within the app settings. `False` – The user can configure the database update run mode and, for example, disable autostart of anti-malware database updates.	`True`
`AllowUpdateInRoaming`	Update databases in roaming	Boolean	`True` – The app downloads anti-malware databases if the device is in the roaming zone. The app downloads anti-malware databases according to the defined schedule (`UpdateScheduleType`). `False` – The app downloads anti-malware databases only if the device is in the home network.	`False`

Configuration key	Description	Type	Value	Default value

`EnableWebFilter`	Web Protection	Boolean	`True` – The app uses the Web Protection component to block malicious and phishing websites on the internet.
			Web Protection on Android devices is supported only by Google Chrome, HUAWEI Browser, Samsung Internet, and Yandex Browser.
			Only the website domain is scanned. If it is a malicious or phishing domain, Web Protection blocks the threat. If the domain is not classified as malicious or phishing, the specific URL is not blocked.
			`False` – Protection against malicious and phishing websites is disabled.
			For the Web Protection component to work, the following conditions must be met:
			• Device users accept the Privacy Policy and the Web Protection Statement in the Initial Configuration Wizard or app settings.
			• For corporate devices, Kaspersky Endpoint Security for Android is enabled as an Accessibility feature.
			• For devices with a corporate container, a proxy server is configured in the browser settings:
			`ProxyMode = "fixed_servers"`
			`ProxyServer = "127.0.0.1:3128"`
			`DisableSpdy = true`
			`DataCompressionProxyEnabled = false`
			Proxy server configuration may vary depending on the browser version.
			After the Kaspersky Endpoint Security for Android app is removed from the mobile device, reset the proxy server settings.
			• Use of KSN is enabled in the app settings: `UseKsnMode = Recommended` or `UseKsnMode = Extended`.
			• It is recommended to select Google Chrome, HUAWEI Browser, Samsung Internet Browser, or Yandex Browser as the default browser in the operating system settings.
				`False`

`EnableWebFilterLock`	Block configuration of Web Protection	Boolean	`True` – The user cannot access Web Protection settings within the app settings. `False` – The user can configure Web Protection settings and, for example, disable protection against malicious and phishing websites on the internet.	`True`
`UpdateServer`	Database update source server address	String	Address of the server hosting the database updates, for example, `http://update.server.com`. If you leave the field blank, Kaspersky Endpoint Security for Android uses the Kaspersky database update servers.	

Configuration key	Description	Type	Value	Default value
`AllowGoogleAnalytics`	Submit data to the Google Analytics for Firebase, Firebase Performance Monitoring, and Crashlytics services	Boolean	`True` – The app automatically submits Kaspersky Endpoint Security for Android operating data to the Google Analytics for Firebase, Firebase Performance Monitoring, and Crashlytics services. This data is necessary in order to improve the performance of the app and to analyze user satisfaction. Data is transferred to the Google Analytics for Firebase, Firebase Performance Monitoring, and Crashlytics services over a secure connection. Access to and protection of data is regulated by the relevant terms of use of the Google Analytics for Firebase, Firebase Performance Monitoring, and Crashlytics services. `False` – Submission of data to the Google Analytics for Firebase, Firebase Performance Monitoring, and Crashlytics services is disabled.	`True`
`KscDeviceNameTag`	Device Name Tag for Kaspersky Security Center	String	The tag will be added to the device name in Kaspersky Security Center. A space separates the tag and the device name. This makes it easier to find and sort devices in Kaspersky Security Center. • `{DeviceSerialNumber}` – Serial number of the device. • `{DeviceUid}` – Unique device identifier (UDID). • `{DeviceAssetNumber}` – Device asset number. This number is created internally within your organization. You can add some values (for example, `{DeviceSerialNumber} {DeviceUid}`). We recommend using only these values.	
`KscGroup`	Device group name	String	You can specify device groups in an EMM console. When a device is connected to Kaspersky Security Center, it will be automatically added to a subfolder of the of Unassigned devices folder. The name of the subfolder will match the group name specified in this parameter. You can then create rules for automatically moving devices from subfolders of the Unassigned devices folder to administration groups in the **Discovery & deployment** > **Deployment & assignment** > **Moving rules** section. If you leave the field blank, the device will be automatically added to the root of the **Unassigned devices** folder.	`KES10`
`KscCorporateEmail`	User's corporate email	String	You can specify users' corporate email addresses in an EMM console. These emails will be displayed in Kaspersky Security Center. The string must be a valid email address. Other values are ignored.	
`KscDeviceName`	Device name in Kaspersky Security Center	String	You can specify the device name displayed in Kaspersky Security Center. The specified value will completely replace the device name. The value set in the `KscDeviceNameTag` setting will be ignored. If you leave the field blank, the device name will be generated according to the format specified in the Kaspersky Security Center group policy.	

Participating in Kaspersky Security Network

To protect mobile devices more effectively, Kaspersky Endpoint Security for Android and Kaspersky Protection for iOS use data acquired from users around the globe. Kaspersky Security Network is designed to process this data.

Kaspersky Security Network (KSN) is an infrastructure of cloud services providing access to the Kaspersky knowledge base with information about the reputation of files, web resources, and software. The use of data from Kaspersky Security Network ensures faster responses by Kaspersky applications to threats, improves the performance of some protection components, and reduces the likelihood of false alarms.

Your participation in Kaspersky Security Network helps Kaspersky to acquire real-time information about the types and sources of new threats, develop methods for neutralizing them, and reduce the number of false alarms raised by Kaspersky Endpoint Security for Android and Kaspersky Protection for iOS. Participation in Kaspersky Security Network also lets you access reputation statistics for applications and websites.

When you participate in Kaspersky Security Network, some statistics are acquired while Kaspersky Endpoint Security for Android and Kaspersky Protection for iOS are running and are automatically sent to Kaspersky. This information makes it possible to keep track of threats in real time. Files or parts of files that may be exploited by intruders to harm the computer or user's content can be also sent to Kaspersky for additional examination.

Use of Kaspersky Security Network is required for the operation of Kaspersky Endpoint Security for Android and Kaspersky Protection for iOS.

The following app components use the Kaspersky Security Network cloud service:

- The Anti-Malware, Web Protection, Web Control, App Control, and Call Control components in the Kaspersky Endpoint Security for Android app.
- The Web Protection component in the Kaspersky Protection for iOS app.

Refusal to participate in KSN reduces the level of device protection, which may lead to infection of the device and loss of data. To start using Kaspersky Security Network, you must accept the terms of the End User License Agreement when installing the app. The End User License Agreement outlines which data is transmitted to Kaspersky Security Network by Kaspersky Endpoint Security for Android and Kaspersky Protection for iOS.

To improve the performance of the app, you can additionally provide statistical data to Kaspersky Security Network. Providing the above information to the KSN is voluntary. To start using Kaspersky Security Network, you have to accept the terms of a special agreement – the Kaspersky Security Network Statement. You can opt out of participating in Kaspersky Security Network at any time. The Kaspersky Security Network Statement describes the types of data that Kaspersky Endpoint Security for Android and Kaspersky Protection for iOS transmit to Kaspersky Security Network. You can use Kaspersky Security Network services if the license term for the integrated solution has not expired and the key has not been denylisted.

Updates functionality (including providing anti-malware signature updates and codebase updates), as well as KSN functionality may not be available in the software in the U.S.

Information exchange with Kaspersky Security Network

Information exchange in Kaspersky Endpoint Security for Android

To improve real-time protection, Kaspersky Endpoint Security for Android uses the Kaspersky Security Network cloud service for the following components:

- **Anti-malware**. The app obtains access to the Kaspersky knowledge base regarding the reputation of files and apps. The app scans for threats whose information has not yet been added to anti-malware databases but is already available in KSN. Kaspersky Security Network cloud service facilitates the full Anti-Malware functionality and reduces the likelihood of false alarms.

- **Web Protection** and **Web Control**. The app uses data received from KSN to scan websites before they are opened. The app also determines the website category to control internet users' access based on lists of allowed and blocked categories (for example, the "Internet communication" category).

- **App Control**. The app determines the app category to restrict the startup of apps that do not meet corporate security requirements based on lists of allowed and blocked categories (for example, the "Games" category).

- **Call Control**. The app sends the requests about phone number reputation to KSN and, based on the information received, blocks or allows calls on devices.

Information on the types of data submitted to Kaspersky when using KSN during operation of Anti-Malware and App Control is available in the End User License Agreement. By accepting the terms and conditions of the License Agreement, you agree to transfer this information.

Information on the types of data submitted to Kaspersky when using KSN during operation of Web Protection and Web Control is available in the Statement regarding data processing for Web Protection. By accepting the terms and conditions of the Statement, you agree to transfer this information.

Information on the types of data submitted to Kaspersky when using KSN during operation of Call Control is available in the Statement regarding data processing for Call Control functionality. By accepting the terms and conditions of the Statement, you agree to transfer this information.

For more information about the provision of data to KSN, refer to the Data provision in Kaspersky Endpoint Security for Android section.

Providing data to KSN is voluntary. If you want, you can disable data exchange with KSN.

Information exchange in Kaspersky Protection for iOS

To improve real-time protection, Kaspersky Protection for iOS uses the Kaspersky Security Network cloud service for the following components:

- **Web Protection**. The app uses data received from KSN to scan websites before they are opened.

Information on the types of data submitted to Kaspersky when using KSN during operation of Web Protection is available in the End User License Agreement. By accepting the terms and conditions of the License Agreement, you agree to transfer this information.

For more information about the provision of data to KSN, refer to the Data provision in Kaspersky Protection for iOS section.

Providing data to KSN is voluntary. If you want, you can disable data exchange with KSN.

Sending statistics to KSN from Android and iOS apps

For the purposes of identifying emerging information security threats, intrusion threats, and threats that are hard to detect (along with their respective sources), and to improve the protection of information stored and processed on a device, you can extend your participation in Kaspersky Security Network.

To exchange data with KSN for the purposes of improving the performance of the app, the following conditions must be fulfilled:

- You or the device user must read and accept the terms of the Kaspersky Security Network Statement. If you choose for the Statement to be accepted by users, they will be prompted by a notification on the main app screen to accept the terms of the Statement. Users can also accept the Statements in the **About the app** section in the Kaspersky Endpoint Security for Android or Kaspersky Protection for iOS settings.
- You must configure the group policy settings to allow statistics to be sent to KSN.

You can opt out of sending statistical data to Kaspersky Security Network at any time. Information on the types of statistical data submitted to Kaspersky when using KSN during the operation of mobile apps is available in the Kaspersky Security Network Statement.

Providing data to KSN is voluntary. If you want, you can disable data exchange with KSN.

Enabling and disabling the use of Kaspersky Security Network

For the operation of Kaspersky Endpoint Security for Android and Kaspersky Protection for iOS components that use Kaspersky Security Network, the app sends requests to cloud services. Requests contain the data described in the Data provision in Kaspersky Endpoint Security for Android and Data provision in Kaspersky Protection for iOS sections respectively.

If the use of Kaspersky Security Network is disabled on the device, the Anti-Malware, Web Protection, Web Control, and App Control features are disabled automatically. Call Control will not work or will work with limitations, depending on the selected region.

To enable or disable the use of Kaspersky Security Network for Android devices:

1. In the main window of Kaspersky Next Expert View (on-premise), select **Asset management** → **Policies**. In the list of group policies that opens, click the name of the policy that you want to configure.
2. In the policy properties window, select **Application settings**.
3. Select **Android** and go to the **KES for Android settings** section.
4. On the **Kaspersky Security Network** card, click **Settings**.

   The **Kaspersky Security Network** window opens.
5. Enable the **Kaspersky Security Network** toggle switch for the following components: Anti-Malware, Web Protection, Web Control, and App Control.

6. In the **KSN Proxy** section, select the **Switch to using public Kaspersky Security Network servers if KSN Proxy is not available** check box if needed.

7. Click **OK**.

8. On the **Sending additional data** card, click **Settings**.

9. In the **Sending data to Kaspersky Security Network** section, select the **Allow sending statistics to Kaspersky Security Network** check box to submit data to Kaspersky.

   This data will help the Kaspersky Endpoint Security for Android app more quickly respond to threats, improve the performance of protection components, and decrease the likelihood of false alarms.

10. In the **Sending data for marketing purposes** section, select the **Allow data processing to help improve the quality, appearance, and performance of the app** check box to improve the quality, appearance, and performance of the Rightholder's Software, products, services, and infrastructure by analyzing users' experience, features they use, and device status and settings.

11. Select who must accept the Statements:

    - If you select **Statements are accepted by administrator**, you will be prompted to accept the Statements in the window that opens.

    - If you select **Statements are accepted by users**, the device user will be prompted to accept the Statements.

12. Click **OK**.

13. Click **Save** to save the changes you have made.

Mobile device settings are changed after the next device synchronization with Kaspersky Security Center.

To enable or disable the use of Kaspersky Security Network for iOS devices:

1. In the main window of Kaspersky Next Expert View (on-premise), select **Asset management** → **Policies**. In the list of group policies that opens, click the name of the policy that you want to configure.

2. In the policy properties window, select **Application settings**.

3. Select **iOS** and go to the **KP for iOS settings** section.

4. Enable the toggle switch on the **Kaspersky Security Network** card for the Web Protection component.

5. On the **Sending additional data** card, click **Settings**.

6. In the **Sending data to Kaspersky Security Network** section, select the **Allow sending statistics to Kaspersky Security Network** check box to submit data to Kaspersky.

   This data will help the Kaspersky Protection for iOS app more quickly respond to threats, improve the performance of protection components, and decrease the likelihood of false alarms.

7. Select who must accept the Statements:

   - If you select **Statements are accepted by administrator**, you will be prompted to accept the Statements in the window that opens.

   - If you select **Statements are accepted by users**, the device user will be prompted to accept the Statements.

8. Click **OK**.

9. Click **Save** to save the changes you have made.

Mobile device settings are changed after the next device synchronization with Kaspersky Security Center.

Using Kaspersky Private Security Network

Kaspersky Private Security Network (hereinafter also referred to as *KPSN)* is a solution that grants access to the reputation databases of Kaspersky Security Network (KSN), without sending data from users' devices to Kaspersky Security Network.

A database of the reputations of objects (files or URLs) is stored on the Kaspersky Private Security Network server, but not on Kaspersky Security Network servers. KPSN reputation databases are stored within the corporate network and are managed by the company administrator.

When KPSN is enabled, Kaspersky Endpoint Security for Android does not send any statistical data from users' devices to KSN.

KPSN is applicable only for Android devices managed by Kaspersky Endpoint Security for Android. Kaspersky Protection for iOS continues to send statistical data from users' devices to KSN.

To enable use of KPSN via Kaspersky Security Center:

1. In the main window of Kaspersky Next Expert View (on-premise), click the Administration Server name.

2. In the Administration Server properties window that opens, on the **General** tab, select the **KSN settings** section.

3. Switch the toggle button to the **Use Kaspersky Private Security Network Enabled** position.

4. Click the **Select file with KSN Proxy settings** button, and then browse for the configuration file that with PKCS7 or PEM extension (provided by Kaspersky).

5. Click **Open**.

6. If you have the proxy server settings configured in the Administration Server properties, but your network architecture requires that you use KPSN directly, enable the **Ignore proxy server settings when connecting to KPSN** option. Otherwise, requests from the managed applications cannot reach KPSN.

7. Click **Save** to save the changes you have made.

After the settings are downloaded, the interface displays the provider's name and contacts, as well as the creation date of the file with the settings of KPSN. KPSN settings are applied to mobile devices.

When you switch to KPSN, App Control does not support the app categories available when using KSN. App categorization will be available if you choose to switch back to KSN.

If KPSN is enabled, Call Control will not work or will work with limitations, depending on the selected region.

If mobile devices are connected to Kaspersky Security Center through the connection gateway, KSN Proxy does not work. In this case, disable the **Enable KSN Proxy on Administration Server Enabled** toggle switch in the **KSN Proxy** section of the Administration Server properties window. For detailed information on enabling and disabling the usage of KSN Proxy, refer to the Kaspersky Security Center Help.

Samsung Knox

Samsung Knox is a mobile solution for configuring and deploying Samsung mobile devices running the Android operating system. For more details about Samsung Knox, please visit the Samsung technical support website.

Installation of Kaspersky Endpoint Security for Android via Knox Mobile Enrollment

Knox Mobile Enrollment (KME) is part of the Samsung Knox mobile solution. It is used for batch installation and initial configuration of apps on new Samsung devices.

Installation of Kaspersky Endpoint Security for Android via Knox Mobile Enrollment consists of the following steps:

1. **Creating a Knox profile with the Kaspersky Endpoint Security for Android app**
2. **Adding devices in Knox Mobile Enrollment**
3. **Installing the Kaspersky Endpoint Security for Android app on the user's mobile devices**

For more details about working with Knox Mobile Enrollment, please refer to the Knox Mobile Enrollment User Guide.

Deployment via Knox Mobile Enrollment is possible only for supported Samsung devices.

Creating a Knox profile

A *Knox profile* is a profile that contains links to apps for their quick deployment and initial configuration on mobile devices.

To create a Knox profile:

1. Sign in to the Samsung Knox console → **Knox Mobile Enrollment**.
2. Select the **Profiles** section.
3. Click **Actions** > **Create profile**.

   The Create New Profile wizard starts.
4. Select **Android Enterprise** as the profile type.
5. In the **Android enterprise profile details** window that opens, specify the following settings:

   a. In the **Basic information** section, enter general information about the Knox profile: **Profile name** and **Description**.

   b. In the **EMM information** section, in the **Pick your EMM** field, select **Other**.

   c. In the **EMM agent APK** field, enter the path to the APK installation file.

   The installation file for Kaspersky Endpoint Security for Android is included in the Advanced MDM in Kaspersky Next Expert View (on-premise) distribution kit. First, download the APK installation file. Then place the APK installation file on the Kaspersky Security Center Web Server or on another server that is accessible for downloading from the device.
6. Click **Continue**.
7. In the **Android enterprise profile settings** window that opens, specify the following settings:

   a. In the **EMM configuration** section, enter the settings for connecting the device to Kaspersky Security Center in the **Custom JSON data (as defined by EMM)** field in the following format:

   b. `{"serverAddress":"myServer.domain.com","serverPort":"12345","vsrv":"virtualServerID"`
   `GROUP","eulas":"cmFuZG9tYmFzZTY0c3RyaW5n"}`.

   The following fields of the JSON file are now supported:

   - `serverAddress` - the address of the Kaspersky Security Center.
   - `serverPort` - the number of the port for mobile device synchronization to the Administration Server via the specified address.
   - `vsrv` (optional) - the Virtual Administration Server.
   - `groupName` (optional) - the name of the subgroup in the Unassigned group.
   - `eulas` (optional) - the list of the accepted EULAs (an array of binary identifiers, 16 bytes long).

The `connectionString` parameter is no longer supported for KME (Knox Mobile Enrollment).

c. To install Kaspersky Endpoint Security for Android via Knox Mobile Enrollment, the mobile device user must accept the terms of the Samsung License Agreement. You can view the terms of the Samsung License Agreement in the **Privacy Policy, EULAs and Terms of Service** section. You can also add other legal documents of your company that are necessary for deploying a Knox profile by clicking the **Add legal agreement** button.

8. Click the **Save** button.

As a result, the new Knox profile with the Kaspersky Endpoint Security for Android app will be added to the list in the KME console.

Adding devices in Knox Mobile Enrollment

Devices can be added in the Knox Mobile Enrollment (KME) console in the following ways:

- The vendor automatically adds devices in the KME console after the devices are purchased.
- The administrator installs the Knox Deployment app from Google Play on their mobile device and migrates the Knox profile to users' devices using Bluetooth, Wi-Fi Direct, or a QR code.

After the device is reset to the factory settings, the Knox profile will be installed. After deployment of the Knox profile, the device will be automatically added in the KME console.

Adding a device through the Knox Deployment app

If you did not purchase your Samsung device from an official vendor, you can add the device to Knox Mobile Enrollment using Bluetooth, Wi-Fi Direct, or a QR code. This will require the administrator's mobile device that will be used to deliver Knox profiles to users' mobile devices.

To add devices using the Knox Deployment app, the following conditions must be met:

- Depending on the selected delivery mode, Bluetooth or Wi-Fi must be enabled on the mobile devices.
- The mobile devices must be connected to the internet.

To deliver a Knox profile using the Knox Deployment app:

1. Install the Knox Deployment app from Google Play on the administrator's primary mobile device.
2. Start the Knox Deployment app.
3. Enter your Samsung account credentials to sign in.
4. In the **Knox Deployment** window, configure the settings for deploying a Knox profile:
   a. In the **Knox services** section, select **Knox Mobile Enrollment**.
   b. Select the desired Knox profile from the list.

c. Select the **Deployment mode**:

- **Bluetooth**. Set the duration of Bluetooth connection and specify whether the Bluetooth connection is automatic or manual.

  When using Bluetooth, you can add a Knox profile to several devices at the same time.

- **Wi-Fi Direct**. Specify whether the Wi-Fi Direct connection is automatic or manual. Then follow the instructions on the screen.

d. Tap **Start deployment**.

5. On the receiver device, draw a plus-sign (+) gesture on the **Welcome** window to initiate deployment.

6. In the **Knox Deployment** menu that opens, select whether you want to use Bluetooth or Wi-Fi Direct to enroll a device:

   a. If you selected **Bluetooth**, approve the pairing request that appears on the primary device. Then the receiver device downloads the profile. Follow the instructions on the screen.

   After the Knox profile is installed, the new device will be added with the **Bluetooth** tag to the KME console.

   b. If you selected **Wi-Fi Direct**, follow the instructions on the screen.

   After the Knox profile is installed, the new device will be added with the **Wi-Fi** tag to the KME console.

7. When the receiver device is configured, tap **Finish deployment** on the primary device in order to complete the enrollment.

After the device is reset to the factory settings, the Knox profile will be installed.

To deliver a Knox profile using a QR code:

1. On the receiver device, draw a plus-sign (+) gesture on the **Welcome** window to initiate deployment.

2. In the **Knox Deployment** menu that opens, select **QR-code**.

3. In the KME Console, select the desired profile in the **Profiles** section.

4. If there is no QR code next to the profile name, open the profile settings and click the **Add a QR-code** button on the second page.

5. Follow the instructions on the screen and save the profile.

   The generated QR code appears near the profile name.

6. Scan a QR code from the KME Console with the camera on the user's mobile device running Android 10 or later.

   After the Knox profile is installed, the new device with the **QR-code** tag will be added to the KME console.

After the device is reset to the factory settings, the Knox profile will be installed.

Adding a device through the vendor

Official vendors of Samsung devices can be registered in Samsung Knox. For the list of official vendors, visit the Samsung technical support website. The vendor automatically adds devices in the KME console for your Samsung account immediately after the devices are purchased. To have the devices added by the vendor, you must register the vendor in the KME console for your Samsung account. You will need a reseller ID to add the Samsung device vendor in the KME console. To receive the reseller ID, you must send a request to the vendor. In the request, specify your Knox client ID.

To view your Knox client ID:

1. Sign in to the Samsung Knox console → **Knox Mobile Enrollment**.
2. Select the **Resellers** section.
3. Your ID is displayed in the **Knox Customer ID** field.

After you receive a response from the vendor with the reseller ID, register the vendor in the KME console. Prior to registering the vendor, you can create a Knox profile so that the profile can be automatically deployed when adding new devices.

To register an official vendor in the KME console:

1. Sign in to the Samsung Knox console → **Knox Mobile Enrollment**.
2. Select the **Resellers** section.
3. Click the **Register reseller** button.

   The window for registering the device vendor opens.
4. In the **Reseller ID** field, enter the ID received from the official Samsung device vendor.
5. If you created a Knox profile, select the Knox profile in the vendor registration window.

   When you add new devices, the Knox profile is automatically installed.

   For more information about configuring other settings, please refer to the Samsung technical support website.
6. Click **OK**.

The Samsung device vendor will be added to the list of vendors in the KME console.

After new devices are purchased from the official vendor, Kaspersky Endpoint Security for Android will be automatically installed on the devices after the devices are connected to the internet. For more details about working with Knox Mobile Enrollment, please refer to the Knox Mobile Enrollment User Guide. If you already have a list of devices in the KME console, add the Knox profile with the Knox app to the device.

Installing the app

Prior to installing Kaspersky Endpoint Security for Android, issue a mobile certificate for mobile device users in the Kaspersky Next Expert View (on-premise). A mobile certificate is required for identifying the mobile device user in the Kaspersky Next Expert View (on-premise).

To deliver the Knox profile to devices:

1. Sign in to the Samsung Knox console → **Knox Mobile Enrollment**.
2. Select **Devices** → **All devices**.
3. Select the devices on which you want to install the Knox profile.

   The **Device info** window opens.
4. In the **Profiles** list, select the Knox profile with Kaspersky Endpoint Security for Android.
5. In the **Tags** field, enter tags for grouping and labeling devices, and for search optimization in the KME console.
6. Enter the user account credentials of the device into the **User ID** and **Password** fields.

   Account credentials are required for receiving a mobile certificate. The user ID and password must match the user account credentials in Kaspersky Security Center (**Name** and **Password** in the user account properties).

   To receive a mobile certificate only with a password and without a login, enter the `"DO_NOT_USE_LOGIN"` value in the **User ID** field. Kaspersky Endpoint Security for Android will not use the login to request a certificate.
7. Select the Knox profile for the remaining devices.
8. Click the **Save** button.

After the device is reset to the factory settings, the Knox profile will be installed.

After deployment of the Knox profile is started, the APK installation file will be automatically downloaded on the mobile device. Installation of Kaspersky Endpoint Security for Android starts automatically. No additional configuration of the app is required. After the initial setup of the device is performed and the app is installed, synchronization with Kaspersky Security Center will be performed automatically. The mobile device will be added to the Kaspersky Next Expert View (on-premise).

Configuring Knox

This section contains information about working with Knox on Samsung devices.

Knox is available only on Samsung devices running Android 6 or later.

Restricting SD card usage in Knox

Configure SD card restrictions to control usage of SD cards on the user's Samsung device that supports Knox.

To restrict SD card usage on a mobile device:

1. In the main window of Kaspersky Next Expert View (on-premise), select **Asset management** → **Policies**. In the list of group policies that opens, click the name of the policy that you want to configure.
2. In the policy properties window, select **Application settings**.
3. Select **Android** and go to the **Samsung Knox settings** section.
4. On the **Device feature restrictions** card, click **Settings**.

   The **Device feature restrictions** window opens.
5. Enable the settings using the **Device feature restrictions** toggle switch.
6. In the **SD card settings** section, specify the required restrictions:

   - **Prohibit access to SD card**

     This setting applies to devices with Android 5-12.

     Selecting or clearing this check box specifies whether access to the SD card is disabled or enabled on the device.

     This check box is cleared by default.

   - **Prohibit writing to SD card**

     Selecting or clearing this check box specifies whether writing to the SD card is disabled or enabled on the device.

     This check box is cleared by default.

   - **Prohibit moving apps to SD card**

     Selecting or clearing this check box specifies whether the device user is allowed to move apps to the SD card.

     This check box is cleared by default.
7. In the **Additional settings** section, you can specify any additional restrictions:

   - **Prohibit sending crash reports to Google**

     This setting applies to devices running Android 11 or earlier.

     If the check box is selected, Kaspersky Endpoint Security for Android blocks sending crash reports to Google.

     If the check box is cleared, sending reports is allowed.

This check box is cleared by default.

- **Prohibit developer mode**

  > This setting applies to devices running Android 11 or earlier.

  If the check box is selected, the device user is not allowed to enable developer mode on the device.

  If the check box is cleared, the user is allowed to enable developer mode on the device.

  This check box is cleared by default.

8. Click **OK**.
9. Click **Save** to save the changes you have made.

Mobile device settings are changed after the next device synchronization with Kaspersky Security Center. SD card settings are now configured.

Configuring VPN in Knox

To securely connect an Android device to the internet and protect data transfer, you can configure VPN (Virtual Private Network) settings.

> Configuration of VPN is possible only for Samsung devices running Android 11 or earlier.

The following requirements must be considered when using a virtual private network:

- The app that uses the VPN connection must be allowed in the **Firewall** settings.
- VPN settings configured in the policy cannot be applied to system apps. The VPN connection for system apps has to be configured manually.
- Some apps that use a VPN connection need to have additional settings configured at first startup. To configure settings, a VPN connection has to be allowed in app settings.

To configure VPN on a user's mobile device:

1. In the main window of Kaspersky Next Expert View (on-premise), select **Asset management** → **Policies**. In the list of group policies that opens, click the name of the policy that you want to configure.
2. In the policy properties window, select **Application settings**.
3. Select **Android** and go to the **Samsung Knox settings** section.
4. On the **VPN** card, click **Settings**.

   The **VPN** window opens.
5. Enable the settings using the **VPN** toggle switch.

6. Specify the following VPN settings:

- Settings in the **Network** section:
  - In the **Network name** field, enter the name of the VPN tunnel.
  - In the **Protocol** drop-down list, select the VPN connection type:
    - **IPSec Xauth PSK**. A tunneling protocol of the "gateway-to-gateway" type that lets the mobile device user establish a secure connection with the VPN server using the Xauth authentication utility.
    - **L2TP IPSec PSK**. A tunneling protocol of the "gateway-to-gateway" type that lets the mobile device user establish a secure connection with the VPN server via the IKE protocol using a preset key. This protocol is selected by default.
    - **PPTP**. A "point-to-point" tunneling protocol that lets the mobile device user establish a secure connection to the VPN server by creating a special tunnel on a standard unsecured network.
  - In the **Server address** field, enter the network name or IP address of the VPN server.
- Settings in the **Protocol settings** section:
  - In the **DNS search domain(s)** list, enter the DNS search domain to be automatically added to the DNS server name.

    You can specify several DNS search domains, separating them with blank spaces.
  - In the **DNS server(s)** field, enter the full domain name or IP address of the DNS server.

    You can specify several DNS servers, separating them with blank spaces.
  - In the **Routing** field, enter the range of network IP addresses with which data is exchanged via the VPN connection.

    If a range of IP addresses is not specified in the **Routing** field, all internet traffic will pass through the VPN connection.

7. Additionally, configure the following settings:

- For the **IPSec Xauth PSK** and **L2TP IPSec PSK** protocols:
  - In the **IPSec shared key** field, enter the password for the preset IPSec security key.
  - In the **IPSec ID** field, enter the name of the mobile device user.
- For the **L2TP IPSec PSK** protocol, specify the password for the L2TP key in the **L2TP key** field.
- For the **PPTP** network, select the **Use SSL connection** check box so that the app will use the MPPE (Microsoft Point-to-Point Encryption) method of data encryption to secure data transmission when the mobile device connects to the VPN server.

8. Click **Save** to save the changes you have made.

Mobile device settings are changed after the next device synchronization with Kaspersky Security Center.

Configuring an Exchange mailbox in Knox

To work with corporate mail, contacts, and the calendar on the mobile device, you can configure the Exchange mailbox settings for the standard Samsung Email app.

An Exchange mailbox can be configured only for Samsung devices running Android 9 or earlier.

To configure an Exchange mailbox on a user's mobile device:

1. In the main window of Kaspersky Next Expert View (on-premise), select **Asset management** → **Policies**. In the list of group policies that opens, click the name of the policy that you want to configure.
2. In the policy properties window, select **Application settings**.
3. Select **Android** and go to the **Samsung Knox settings** section.
4. On the **Exchange ActiveSync** card, click **Settings**.

   The **Exchange ActiveSync** window opens.
5. Enable the settings using the **Exchange ActiveSync** toggle switch.
6. In the **Server address** field, enter the IP address or DNS name of the server hosting the mail server.
7. In the **Domain name** field, enter the name of the mobile device user's domain on the corporate network.
8. In the **Synchronization interval** drop-down list, select the interval for mobile device synchronization with the Microsoft Exchange server.
9. To use the SSL (Secure Sockets Layer) data transport protocol, select the **Use SSL connection** check box. The SSL protocol uses encryption and certificate-based authentication for secure data transfer. This check box is selected by default.
10. To use digital certificates to protect data transfer between the user's mobile device and the Microsoft Exchange server, select the **Verify server certificate** check box. The server certificate is verified to have been issued from the trusted root certificate. This check box is selected by default.
11. Click **Save** to save the changes you have made.

Mobile device settings are changed after the next device synchronization with Kaspersky Security Center.

Configuring APN in Knox

APN can be configured only for Samsung devices.

A SIM card must be inserted to be able to use an access point on the user's mobile device. Access point settings are provided by the mobile operator. Incorrect access point settings may result in additional mobile charges.

To configure the Access Point Name (APN) settings on a user's mobile device:

1. In the main window of Kaspersky Next Expert View (on-premise), select **Asset management** → **Policies**. In the list of group policies that opens, click the name of the policy that you want to configure.

2. In the policy properties window, select **Application settings**.

3. Select **Android** and go to the **Samsung Knox settings** section.

4. On the **APN settings** card, click **Settings**.

   The **APN settings** window opens.

5. Enable the settings using the **APN settings** toggle switch.

   > The toggle switch in this card does not enable or disable the corresponding functionality on devices. Enabling the toggle switch lets you configure custom settings. Disabling the toggle switch lets you use default settings.

6. Specify the following access point settings for connecting the user to the data service:

   - In the **APN type** drop-down list, select the type of access point (APN) for data transmission on a GPRS/3G/4G mobile network:

     - **Internet**. Connection of the user's mobile device to the internet.
     - **MMS**. Exchange of MMS multimedia messages.
     - **Internet and MMS**. Connection to the internet and exchange of multimedia messages. This is the default value.

   - In the **APN name** field, specify the name of the access point.
   - In the **MCC** field, enter the mobile country code (MCC).
   - In the **MNC** field, enter the mobile network code (MNC).

7. If you have selected **MMS** or **Internet and MMS** as the type of access point, specify the following additional MMS server settings in the **MMS server** section:

   - In the **MMS server name** field, specify the full domain name of the mobile carrier's server used for MMS exchange (for example, `mms.mobile.com`).
   - In the **MMS proxy server address** field, specify the network name or IP address of the proxy server.
   - In the **MMS proxy server port** field, specify the port number of the mobile carrier's server used for MMS exchange.

8. In the **Authentication** section, specify the authentication settings:

    - In the **Authentication type** drop-down list, select the type of authentication of the mobile device user that will be used on the mobile carrier's server for network access. By default, user authentication is not required. The following types are available:

        - **None**. User authentication is not required to access the mobile network.
        - **PAP** (Password Authentication Protocol). An authentication protocol that uses passwords as plain non-encrypted text.
        - **CHAP** (Challenge Handshake Authentication Protocol). A request-response authentication protocol that uses standard MD5 hashing to encrypt the response.
        - **Concurrently**. Combined use of CHAP and PAP protocols.

    - In the **User name** field, enter the user name for authorization on the mobile network.
    - In the **Password** field, enter the password for user authorization on the mobile network.

9. In the **Network** section, specify the following network settings:

    - In the **Network name** field, enter the name of the network.
    - In the **Server address** field, specify the network name of the mobile carrier's server through which data transmission services are accessed.

10. In the **Proxy server** section, specify the following proxy server settings:

    - Select the **Use a proxy server** check box to enable the use of a proxy server. This check box is cleared by default.
    - In the **Proxy server address** field, specify the network name or IP address of the mobile carrier's proxy server for network access. This field is available only if the **Use a proxy server** check box is selected.
    - In the **Proxy server port** field, specify the port number of the mobile carrier's proxy server for network access. This field is available only if the **Use a proxy server** check box is selected.

11. Click **OK**.

12. Click **Save** to save the changes you have made.

Mobile device settings are changed after the next device synchronization with Kaspersky Security Center.

Configuring Firewall in Knox

Configure Firewall settings to monitor network connections on the user's mobile device.

Firewall can be configured only for Samsung devices operating in the following modes:

- corporate device
- personal device running Android 15 or earlier
- device with corporate container running Android 15 or earlier

To configure Firewall on a user's mobile device:

1. In the main window of Kaspersky Next Expert View (on-premise), select **Asset management** → **Policies**. In the list of group policies that opens, click the name of the policy that you want to configure.
2. In the policy properties window, select **Application settings**.
3. Select **Android** and go to the **Samsung Knox settings** section.
4. On the **Firewall** card, click **Settings**.

   The **Firewall** window opens.
5. Enable the settings using the **Firewall** toggle switch.
6. In the **Internet access** drop-down list, select the Firewall mode. Depending on its operating mode, Firewall monitors connections established by the user's mobile device:
   - If you want to allow inbound and outbound connections of all installed apps, select **Allow for all apps**. This mode is selected by default.
   - If you want to block all network activity except for several specified apps, select **Allow for listed apps**.
7. If you selected **Allow for listed apps** as the Firewall mode, create a list of apps for which all network activity is allowed:
   a. In the **Apps with internet access** section, click **Add**.

      The **Add app** window opens.

   b. In the **App name** field, enter the name of the mobile app.

   c. In the **Package name** field, enter the system name of the mobile app package (for example, `com.mobileapp.example`).

   d. Click **Add**.

   The new app for which Firewall is disabled appears in the list.

   > You can modify or delete mobile apps in the list using the **Edit** and **Delete** buttons at the top of the list.
8. Click **OK**.
9. Click **Save** to save the changes you have made.

Mobile device settings are changed after the next device synchronization with Kaspersky Security Center.

Using the Kaspersky Endpoint Security for Android app

This Help section describes features and operations that are available to users of the Kaspersky Endpoint Security for Android app.

Articles in this section comprise all the options that can be available or visible on a mobile device. The actual layout and behavior of the app depends on the remote administration system that is implemented and how the administrator configures your device in accordance with corporate security requirements. Some functions and options described in this section may not apply to your actual experience with the app. If you have any questions about the app on your specific device, contact your administrator.

App features

Kaspersky Endpoint Security offers the following key features.

Protection against viruses and other malware

The app uses the Anti-Malware component to protect the device against viruses and other malware.

Anti-Malware performs the following functions:

- Scans the entire device, installed apps, or selected folders for threats
- Protects the device in real time
- Scans newly installed apps before they are launched for the first time
- Updates anti-malware databases

If an application that collects information and sends it to be processed is installed on a mobile device, Kaspersky Endpoint Security for Android may classify this application as malware.

Protection of stolen or lost device data

The Anti-Theft component protects your data against unauthorized access and helps you to locate the device if it gets lost or stolen.

Anti-Theft lets you perform the following operations remotely:

- Lock the device.

  To prevent a hacker from having the capability to unlock the device, Kaspersky Endpoint Security must be enabled as an Accessibility Features service on mobile devices running Android 7 or later.

- Turn on a loud alarm on the device even if the device sound is disabled.
- Get the device location coordinates.
- Wipe data stored on the device.
- Reset to factory settings.
- Secretly take a photo of the person using your device.

To enable Anti-Theft operations, Kaspersky Endpoint Security must be enabled as a device administrator. If you did not grant device administrator rights during the initial configuration of apps, you can grant administrator rights to Kaspersky Endpoint Security using the appropriate notification or in the device settings (**Android Settings** → **Security** → **Device administrators**).

Protection against online threats

The Web Protection component provides protection against online threats.

Web Protection blocks malicious websites that distribute malicious code, and phishing websites designed to steal your confidential data and gain access to your financial accounts. Web Protection scans websites before you open them by using the Kaspersky Security Network cloud service. Learn more.

App Control

According to corporate security requirements, the *administrator of the remote administration system* (hereinafter also "administrator") creates lists of recommended, forbidden, and required apps. The App Control component is used to install recommended and required apps, update them, and remove forbidden apps.

App Control lets you install recommended and required apps to your device via a direct link to the distribution package or a link to Google Play. App Control lets you remove forbidden apps that violate corporate security requirements.

Kaspersky Endpoint Security must be enabled as an Accessibility Features service to ensure proper functioning of App Control. If you did not enable this service during the Initial Configuration Wizard for the app, you can enable Kaspersky Endpoint Security as an Accessibility Features service using the appropriate notification or in the device settings (**Android Settings** → **Accessibility** → **Services**).

Compliance Control

The Compliance Control component automatically checks whether the device conforms to corporate security requirements. If your device does not meet corporate security requirements, the app shows a notification with the following information:

- Reason for the non-compliance (for example, forbidden apps were detected on the device or anti-malware databases are out of date).
- Time period within which you must eliminate the non-compliance (for example, 24 hours).
- Action that will be taken on the device if you do not eliminate the non-compliance within the specified time period (for example, device will be locked).
- Action performed to fix the device's non-compliance with corporate security requirements.

Protection against unwanted calls

The Call Control component provides protection against fraudulent, spam, and other unwanted calls.

Main window at a glance

The appearance of the main window slightly differs for different screen resolutions.

The main window displays the overall protection status of your device. This status determines the color of the window:

- Green indicates that device protection is at an optimal level.
- Red indicates critical problems with device security.

In the main app window, you can also do the following:

- View notifications by clicking the button at the top right corner. They inform you about security issues, problems in app operation, compliance with corporate security requirements, and your license.
- Navigate between the main window and app settings using the buttons at the bottom.

Status bar icon

After the first launch wizard finishes, the icon of Kaspersky Endpoint Security appears in the status bar.

The icon reflects the operation of the app and provides access to the main window of Kaspersky Endpoint Security.

The icon signals the operation of Kaspersky Endpoint Security and reflects the protection status of your device:

– Device is protected.

– There are problems with protection (for example, the anti-malware databases are out of date or a newly installed app has not been scanned).

Device scan

Anti-Malware has a number of limitations:

- When Anti-Malware is running, a threat detected in the external memory of the device (such as an SD card) cannot be neutralized automatically in the corporate container. Kaspersky Endpoint Security for Android does not have access to external memory in the corporate container. Information about detected objects is displayed in app notifications. To neutralize objects detected in the external memory, the object files have to be deleted manually and the device scan restarted.
- Due to technical limitations, Kaspersky Endpoint Security for Android cannot scan files with a size of 2 GB or more. During a scan, the app skips such files without notifying you that such files were skipped.
- On devices running Android 11 or later, the Kaspersky Endpoint Security for Android app can't scan the "Android/data" and "Android/obb" folders and detect malware in them due to technical limitations.

To start a device scan:

1. In the main window of Kaspersky Endpoint Security, tap **Settings** → **App settings** → **Anti-Malware** → **Start scan**.
2. Select the device scan scope:
   - **Scan entire device**. The app scans the entire file system of the device.
   - **Scan installed apps**. The app scans only installed apps.
   - **Custom Scan**. The app scans the selected folder or individual file. You can select an individual object (folder or file) or one of the following partitions of device memory:
     - **Device memory**. Read-accessible memory of the entire device. This also includes the system memory partition that stores operating system files.
     - **Internal memory**. Device memory partition intended for installation of apps and storage of media content, documents, and other files.
     - **External memory**. External SD card memory. If no external SD card is installed, this option is hidden.

Access to malware scan settings may be restricted by your administrator.

To configure the malware scan:

1. In the main window of Kaspersky Endpoint Security, tap **Settings** → **App settings** → **Anti-Malware** → **Scan settings**.

2. If you want the app to detect adware and apps that could be used by hackers to cause harm to your device or data when the app performs a scan, switch on the **Adware, dialers, and other** toggle button.

3. Tap **Action on threat detection**, and then select the action taken by the app by default:

   - **Quarantine**

     Quarantine stores files as archives, so they cannot harm the device. The Quarantine lets you delete or restore the files that were moved to isolated storage.

   - **Ask user**

     The app prompts you to select an action for each detected object: skip, quarantine, or delete. When multiple objects are detected, you can apply a selected action to all objects.

   - **Delete**

     Detected objects will be automatically deleted. No additional actions are required. Prior to deleting an object, Kaspersky Endpoint Security will display a temporary notification about the detection of the object.

   - **Skip**

     If the detected objects have been skipped, Kaspersky Endpoint Security warns you about problems in device protection. For each skipped threat, the app provides actions that you can perform to eliminate the threat. The list of skipped objects may change, for example, if a malicious file was deleted or moved. To receive an up-to-date list of threats, run a full device scan. To ensure reliable protection of your data, eliminate all detected objects.

Information about detected threats and the actions taken on them is logged in app reports (**Settings** → **Reports**). You can choose to display reports on Anti-Malware operations.

Running a scheduled scan

Anti-Malware has a number of limitations:

- When Anti-Malware is running, a threat detected in the external memory of the device (such as an SD card) cannot be neutralized automatically in the corporate container. Kaspersky Endpoint Security for Android does not have access to external memory in the corporate container. Information about detected objects is displayed in app notifications. To neutralize objects detected in the external memory, the object files have to be deleted manually and the device scan restarted.

- Due to technical limitations, Kaspersky Endpoint Security for Android cannot scan files with a size of 2 GB or more. During a scan, the app skips such files without notifying you that such files were skipped.

- On devices running Android 11 or later, the Kaspersky Endpoint Security for Android app can't scan the "Android/data" and "Android/obb" folders and detect malware in them due to technical limitations.

To configure the full scan schedule for a device:

1. In the main window of Kaspersky Endpoint Security, tap **Settings** → **App settings** → **Anti-Malware** → **Scan settings**.
2. Tap **Schedule**, and then select the full scan frequency:
   - **Weekly**
   - **Daily**
   - **Disabled**
   - **After database update**
3. Tap **Start day**, and then select the day of the week when you want to start the full scan.
4. Tap **Start time**, and then select the time for starting the full scan.

A full scan of the device is started according to schedule.

If the device is in battery saver mode, the app may perform this task later than specified. To ensure timely responses of Android devices to the administrator's commands, enable the use of Firebase Cloud Messaging.

Changing the Protection mode

Real-Time Protection lets you detect threats in files being opened, and scan apps while they are being installed on the device in real time. The anti-malware databases and the Kaspersky Security Network cloud service (Cloud Protection) are used to ensure security automatically.

To change the device protection mode:

1. In the main window of Kaspersky Endpoint Security, tap **Settings** → **App settings** → **Anti-Malware** → **Real-time protection mode**.
2. Select the device Protection mode:
   - **Disabled**. Protection is disabled.
   - **Recommended**. Anti-Malware scans only installed apps and files from the Downloads folder. Anti-Malware scans new apps as soon as they are installed.
   - **Extended**. Anti-Malware scans all device files for malicious objects when any operation is performed with them (for example, when they are saved, moved, or modified). Anti-Malware also scans new apps as soon as they are installed.

Information about the current Protection mode is displayed under the description of the component.

Access to Real-Time Protection settings may be restricted by your administrator.

To enable Cloud Protection (KSN):

1. Tap **Settings** → **App settings** → **Anti-Malware** in the main window of Kaspersky Endpoint Security.
2. Switch on the **Cloud Protection (KSN)** toggle button.

   The **Cloud Protection (KSN)** toggle button manages the use of Kaspersky Security Network only for real-time protection of a device. If the check box is cleared, Kaspersky Endpoint Security continues to use KSN for the operation of other components of the app.

As a result, the app obtains access to the Kaspersky online knowledge base regarding the reputation of files and apps. The scan is performed for threats whose information has not yet been added to anti-malware databases but is already available in KSN. Kaspersky Security Network cloud service provides full operation of Anti-Malware and reduces the likelihood of false alarms. Only your administrator can fully disable the use of Kaspersky Security Network.

To configure Real-Time Protection:

1. In the main window of Kaspersky Endpoint Security, tap **Settings** → **App settings** → **Anti-Malware** → **Scan settings**.
2. If you want the app to detect adware and apps that could be used by hackers to cause harm to your device or data when the app performs a scan, switch on the **Adware, dialers, and other** toggle button.
3. Tap **Action on threat detection**, and then select the action taken by the app by default:
   - **Quarantine**

     Quarantine stores files as archives, so they cannot harm the device. Quarantine lets you delete or restore the files that were moved to isolated storage.
   - **Ask user**

     The app prompts you to select an action for each detected object: skip, quarantine, or delete. When multiple objects are detected, you can apply a selected action to all objects.

- **Delete**

  Detected objects will be automatically deleted. No additional actions are required. Prior to deleting an object, Kaspersky Endpoint Security will display a temporary notification about the detection of the object.

- **Skip**

  If the detected objects have been skipped, Kaspersky Endpoint Security warns you about problems in device protection. For each skipped threat, the app provides actions that you can perform to eliminate the threat. The list of skipped objects may change, for example, if a malicious file was deleted or moved. To receive an up-to-date list of threats, run a full device scan. To ensure reliable protection of your data, eliminate all detected objects.

Information about detected threats and the actions taken on them is logged in the app reports (**Settings** → **Reports**). You can choose to display reports on Anti-Malware operations.

Anti-malware database updates

To update anti-malware databases of the app:

In the main window of Kaspersky Endpoint Security, tap **Settings** → **App settings** → **Anti-Malware** → **Start database update**.

When you use Kaspersky Endpoint Security for Android, you may encounter a **Kaspersky service domain name blocked** issue, which means network issues are preventing the app from reaching Kaspersky services. This may affect the Anti-Malware protection features and put your data at risk. Changing your connection settings might fix the issue.

This section only gives general instructions. Please refer to the user guide provided by your device manufacturer for specific instructions.

To change your connection settings:

1. Go to **Settings** on the device.
2. Open the connection settings.
3. Go to the **Private DNS** section.
4. Select **Private DNS provider hostname**, and then type a DNS name. For example, you could type "dns.google" to use Google's public DNS server.
5. Save the changes.

The connection settings are changed.

Scheduled database update

The app can automatically update the anti-malware databases according to the schedule you specify.

To configure the update schedule:

1. In the main window of Kaspersky Endpoint Security, tap **Settings** → **App settings** → **Anti-Malware** → **Database update settings**.
2. Tap **Schedule**, and then select the update frequency:
   - **Weekly**
   - **Daily**
   - **Disabled**
3. Tap **Start day**, and then select the day of the week when you want to run the update.
4. Tap **Start time**, and then select the time for starting the update.

Anti-malware database updates are started according to schedule.

If the device is in battery saver mode, the app may perform this task later than specified. To ensure timely responses of Android devices to the administrator's commands, enable the use of Firebase Cloud Messaging.

Updates functionality (including providing anti-malware signature updates and codebase updates), as well as KSN functionality may not be available in the software in the U.S.

Things to do if your device gets lost or stolen

If your device gets lost or stolen, contact your system administrator. The administrator can execute Anti-Theft commands on your device remotely according to corporate security requirements.

If a Reset to factory settings command is sent to the device, control over the device will be lost, and the remaining Anti-Theft commands will not work.

Web Protection

The following conditions must be met to enable Web Protection:

- Kaspersky Endpoint Security for Android must be configured as an Accessibility service.

  If the Kaspersky Endpoint Security for Android app on a corporate device is not enabled as an Accessibility Features service, Web Protection is supported only by the Google Chrome browser and checks only the domain of a website. To allow other browsers (Samsung Internet, Yandex Browser, and HUAWEI Browser) support Web Protection, enable Kaspersky Endpoint Security as an Accessibility Features service. This will also enable the Custom Tabs feature operation.

- The Statement regarding data processing for the purpose of using Web Protection (Web Protection Statement) must be accepted. Kaspersky Endpoint Security uses Kaspersky Security Network (KSN) to scan websites. The Web Protection Statement contains the terms of data exchange with KSN.

  Your administrator can accept the Web Protection Statement for you in Kaspersky Security Center. In this case, you are not required to take any action.

  If your administrator has not accepted the Web Protection Statement and has sent you the request to do this, you must read and accept the Web Protection Statement in the app settings.

  If your administrator has not accepted the Web Protection Statement, Web Protection is not available.

- On some devices, the following permissions must be granted:

  - **Run in the background**
  - **Display pop-up windows while running in the background**
  - **Display pop-up window**
  - **Ignore battery optimization**

In Yandex Browser and Samsung Internet, malicious and phishing URLs may remain unblocked. This is because only the website domain is scanned. If it is a malicious or phishing domain, Web Protection blocks the threat. If the domain is not classified as malicious or phishing, the specific URL is not blocked.

Web Protection on Android devices is supported only by Google Chrome, HUAWEI Browser, Samsung Internet, and Yandex Browser.

The Custom Tabs feature is supported by Google Chrome, HUAWEI Browser, and Samsung Internet.

To use Web Protection in Telegram, disable opening links in the In-App Telegram browser in Telegram settings.

Web Protection for HUAWEI Browser, Samsung Internet, and Yandex Browser does not block sites on a mobile device if a corporate container is used and Web Protection is enabled only for the corporate container.

To use Web Protection at all times when you browse the web, set Google Chrome, HUAWEI Browser, Samsung Internet, or Yandex Browser as the default browser.

To set a supported browser as the default browser and use Web Protection for website scanning at all times:

1. In the main window of Kaspersky Endpoint Security, tap **Settings** → **App settings** → **Web Protection**.
2. Switch the **Web Protection** toggle button to On.
3. Tap **Set default browser**.

   This button is displayed when Web Protection is enabled and a supported browser has not been set as the default browser.

The default browser selection wizard starts.

4. Follow the wizard instructions.

The wizard sets Google Chrome, HUAWEI Browser, or Samsung Internet as the default browser. Web Protection continuously scans websites while you browse the web.

Scanning notifications from messengers

Kaspersky Endpoint Security for Android can detect malicious and phishing URLs in notifications from Telegram, WhatsApp, the default SMS app, and other common messengers. Only URLs expressed as text directly in the notification text can be scanned. URLs embedded in markup are not scanned.

The following conditions must be met to enable notification scanning:

- Web Protection must be enabled.
- Displaying notifications must be allowed for the desired messengers. Kaspersky Endpoint Security for Android scans only notifications that can be displayed on the device screen.
- On Google Pixel and Vivo devices, the "Conversations" permission must be granted to Kaspersky Endpoint Security in the notification access settings.

To allow access to notifications so the app can scan them:

1. In the main window of Kaspersky Endpoint Security, tap **Settings** → **App settings** → **Web Protection**.
2. Turn on the **Block notifications that contain malicious and phishing URLs** toggle switch.

   The **Notification access required** window opens.
3. Tap **Continue**.

   The corresponding settings section opens.
4. Turn on the Kaspersky Endpoint Security toggle switch.
5. In the dialog that opens, allow the app to read all your notifications.
6. Go back to Kaspersky Endpoint Security.

The app now scans notifications to detect malicious and phishing URLs. If a dangerous URL is found, the notification is blocked and a blocking screen with information about the blocked notification appears.

If Kaspersky Endpoint Security for Android is not enabled as an Accessibility feature, the app sends a push notification about the detected dangerous URLs instead of displaying a blocking screen. After tapping the push notification, a screen with information about the blocked notification appears.

Protection against unwanted calls

Your administrator may suggest protecting your device against unwanted calls. In this case, Kaspersky Endpoint Security for Android will monitor your calls and obtain information about numbers to block fraudulent, spam, and other unwanted calls according to corporate security requirements.

Protection rules are set by the administrator. If you do not agree with certain number being blocked, contact your administrator.

Call protection is not supported on devices with DSFA (Dual Sim Full Active).

To enable call protection:

1. Accept the Call Control Statement and Privacy Policy if they have not been accepted before.

   Your administrator can accept the Call Control Statement for you in Kaspersky Security Center. In this case, you are not required to take any action.

   If your administrator has not accepted the Call Control Statement and has sent you the request to do this, you must read and accept the Call Control Statement in the app settings.

2. Grant Kaspersky Endpoint Security for Android the required permissions by following the instructions provided in the app:

   - **Accessibility** and **Notifications** permissions to show you pop-up notifications and inform you who is calling
   - **Access to call log** to check calls and get information about callers
   - **Access to contacts** to identify who is calling you
   - **Permission to manage calls** to block spam and other unwanted calls
   - **Allow Kaspersky Endpoint Security for Android to be your default app to identify numbers and spam**:
     - On devices running Android 8-9, allow Kaspersky Endpoint Security for Android to be your default calling app.

       If Kaspersky Endpoint Security for Android is set as the default calling app on devices running Android 8-9, calls will only be routed to the system calling app, and third-party calling apps will not work.

     - On devices running Android 10 or later, allow Kaspersky Endpoint Security for Android to be your default Caller ID app (**Settings** → **Apps** → **Choose default apps** → **Caller ID & spam app**).

If Kaspersky Endpoint Security for Android is set as the default Caller ID app on devices running Android 8-9, calls will only be routed to the system calling app, and third-party calling apps will not work.

Call protection on your device is enabled.

Depending on the settings specified by your administrator, you may receive pop-up notifications from Kaspersky Endpoint Security for Android with information about numbers and their reputation. You can use these pop-ups to leave feedback on numbers to help Kaspersky Endpoint Security for Android identify calls better.

Get Certificate

To obtain a certificate for accessing corporate network resources:

1. In the main window of Kaspersky Endpoint Security, tap **Settings** → **App settings** → **Additional** → **Get certificate**.
2. Specify your corporate network account credentials. The login must be specified in one of the following formats:
   - `userPrincipalName@DNSDomainName`
   - `sAMAccountName`
   - `sAMADomain\sAMAccountName`

   For more information on these attributes, visit the Microsoft Technical documentation website. For details, you may contact your administrator.
3. If you have received a one-time password from the administrator, select the **One-time password** check box, and then enter the password you received.

   The Certificate Installation Wizard starts.
4. Follow the wizard's instructions.

Synchronizing with Kaspersky Security Center

Synchronization of the mobile device with the Kaspersky Security Center remote administration system is required for protecting and configuring your device in accordance with corporate security requirements. The device is automatically synchronized with Kaspersky Security Center, and you can also start synchronization manually. After the first synchronization, your device is added to the list of mobile devices managed via Kaspersky Security Center. The administrator can then configure your device in accordance with corporate security requirements.

You can configure synchronization settings while running the Initial Configuration Wizard or in the settings of Kaspersky Endpoint Security. Request the values of synchronization settings from your system administrator.

Modify the settings of device synchronization with the Kaspersky Security Center remote administration system only when instructed to do so by the administrator.

To synchronize your device with Kaspersky Security Center:

1. In the main window of Kaspersky Endpoint Security, tap **Settings** → **App settings** → **Synchronization**.
2. In the **Synchronization settings** section, specify the values of the following settings:
   - **Server**
   - **Port**
   - **Group**
   - **Corporate email address**

   Synchronization settings can be hidden by the administrator.
3. Tap **Synchronize**.

Allowing remote access to your device

Your administrator may request remote access to your device. In this case, after the next synchronization of your device with Kaspersky Security Center, you will receive an issue or notification with an offer to connect to the remote control session.

During the session, the administrator will be able to view the device screen, take screenshots, and perform actions on the device. Kaspersky Endpoint Security for Android will inform you about the status of the remote connection. You can stop the session at any time.

Before connecting to a remote control session:

- Accept the agreements offered to you. They contain information on the remote control functionality.
- Enable accessibility for Kaspersky Endpoint Security for Android.
- Allow viewing the device screen. This permission must be granted each time before you start screen sharing.

To start a remote control session:

1. Make sure that the offered agreements are accepted and that accessibility is enabled for Kaspersky Endpoint Security for Android.
2. Tap **Allow** in the received issue or notification requesting your permission to start a remote control session.

   The notification is sent after device synchronization with Kaspersky Security Center. If synchronization does not occur automatically, your administrator may ask you to synchronize the device manually.
3. Grant permission to view the full screen of the device.
4. In the window with instructions for connecting to the session, tap **Allow and start session**.

The remote control session starts.

If you want to end the session, tap **Stop**.

Activating the Kaspersky Endpoint Security for Android app without Kaspersky Security Center

In most cases, the Kaspersky Endpoint Security for Android app that is installed on your device is activated by the administrator centrally in the Kaspersky Security Center remote administration system. If your device is not connected to Kaspersky Security Center, you can enter the activation code manually. To get the activation code, contact the administrator.

Activate the app manually only when instructed to do so by the administrator.

To enter the activation code:

1. In the message that says that your license will soon expire or has expired and that your device is not connected to the Administration Server, tap **Activate**.
2. In the activation window, enter the activation code that the administrator gave you, and then tap **Activate**.
3. If the activation code is correct, a notification is displayed saying that the app has activated, along with the license expiration date.

The Kaspersky Endpoint Security for Android app on your device is activated.

Installing the app on corporate devices

Corporate device is the device operation mode for company-owned Android devices. This mode allows the administrator to have full control over the entire device and configure a wide range of device functions.

Before installing the app on a corporate device, you need to reset the device to factory settings and pre-configure it.

The Kaspersky Endpoint Security for Android app can be installed in one of the following ways:

- Using the QR code generated in Kaspersky Security Center for devices running Android 7 and later.
- Using the app installation package from Kaspersky Security Center and running the command in ADB. This method is suitable for devices running Android 5-6 and devices with later Android versions on which the QR code scanner is not available.

Configuring the app on corporate devices running Android 7 and later

To deploy the app on corporate devices, you need to reset the devices to factory settings and install the app using the QR code generated in Kaspersky Security Center. The QR code contains all the necessary data for app configuration.

To install the Kaspersky Endpoint Security for Android app on the corporate device:

1. Reset the device to factory settings.

   The device reboots, and the welcome screen appears.

2. Tap six times on an empty space of the device's welcome screen.

   The QR code reader appears.

3. Scan the QR code generated in Kaspersky Security Center for app installation.

4. Perform the initial setup of the device. The operating system installs the Kaspersky Endpoint Security for Android app in the background.

   Once the device setup completes, Kaspersky Endpoint Security for Android starts on the device.

   On Xiaomi devices running Android 12, Kaspersky Endpoint Security for Android does not start automatically. In this case, please, start the app manually.

5. Activate the app by following the instructions in the app's Initial Configuration Wizard.

   When deploying the app via the installation package downloaded from Kaspersky Security Center, after the device is reset to factory settings and the QR code is scanned, the **Blocked by Play Protect** message may appear on the device. The issue is caused by the installation package signing certificate being different from the one specified in Google Play. The user should continue the installation by choosing **Install anyway**. If **OK** is selected, the installation process will be interrupted and the device will be reset to factory settings.

The Kaspersky Endpoint Security for Android app is installed and activated on the corporate device.

Configuring the app on corporate devices running Android 5-6

For corporate devices running Android 5-6, the process of configuring the app differs from the standard one. You need to pre-configure the device, install the app, and use Android Debug Bridge (ADB) for additional settings.

This scenario can also be used for other Android versions and for devices on which the QR code scanner is not available.

To deploy the Kaspersky Endpoint Security for Android app on the corporate device with Android 5-6:

1. Reset the device to factory settings. You can skip this step and go to step 2 if the device has not been used before.

   If you set a screen unlock password on the device after you reset it to factory settings, you must reset the device to factory settings again before installing the app using ADB.

2. Enable the developer mode:

   a. Navigate to the **Settings** → **About phone** section.

   b. Tap the **Build Number** option seven times until you see the "**You are now a developer!**" message.

   On some devices, these sections might be located or named differently. For more details, please refer to the Android documentation.

3. Enable the **USB debugging** option in the **Settings** → **Developer options** section.

4. Allow app installation from the sources other than Google Play:

   a. Navigate to the **Settings** → **Security** section.

   b. Enable the **Unknown sources** option.

5. Install the Kaspersky Endpoint Security for Android app on the device via the app installation package from Kaspersky Security Center or using other suitable methods of installation (for example, an APK file).

6. In the window that opens on the device after installation, tap **Done** to exit the Installation Wizard.

   For this scenario to work correctly, do not launch the app before running the ADB command described in step 9.

7. Install ADB on your computer.

8. Connect the device to the computer using a USB cable.

   The system will show a dialog asking whether to allow the device debugging on the computer. Click **OK**.

9. Start ADB and run the following command:

   `adb shell dpm set-device-owner com.kaspersky.kes/com.kms.selfprotection.DeviceAdmin`.

10. Start the Kaspersky Endpoint Security for Android app and activate it by following the instructions in the app's Initial Configuration Wizard.

Some Xiaomi devices cannot be enrolled using ADB if MIUI optimization is turned on. To enroll these devices, turn off MIUI optimization by navigating to **Settings** → **Build number**. Tap on the build number six to eight times to enable **`Developer options`** and disable MIUI optimization. Perform the above mentioned steps again to successfully enroll these devices.

Installing root certificates on the device

A root certificate is a public key certificate issued by a trusted certificate authority (CA). Root certificates are used to verify custom certificates and guarantee their identity.

Your administrator can specify root certificates to be installed on the device. On corporate devices and devices with a corporate container, these certificates are installed automatically. On personal devices, you will get notifications and have to install each certificate manually by following the instructions below.

To manually install a root certificate on the device:

1. Open the device **Settings**.
2. Navigate to the security settings. The path depends on the device model and operating system version. For instance, you may need to tap **Advanced settings** → **Security** or **Security & lock screen** → **Credential storage**.
3. Tap **Install from Phone Storage** / **Install from SD Card** or a similar option.
4. Tap **CA Certificate**.
5. On the confirmation window, tap **Install Anyway**.
6. In the appeared file manager, select the required root certificate.

   On some devices, the downloaded certificates may not be displayed in **Recent files**. Please wait for 3-5 minutes and open the file manager again. The waiting time depends on the device model. If after 3-5 minutes no files have appeared, go to the **Internal storage\Download\kesm_certs** or **SD card\Download\kesm_certs** folder and select the required root certificate.

The root certificate will be installed on the device.

Installing and using mail and VPN certificates on the device

Your administrator can specify mail and VPN certificates to be installed on the device. On corporate devices or devices with a corporate container, such certificates are installed automatically.

A mail certificate is installed on the device only if your administrator first configures Exchange ActiveSync settings.

A VPN certificate can also be installed in a trusted certificate store in a personal space in addition to the corporate container and be used by any app. You will get a notification and have to install a VPN certificate manually by following the instructions below.

To manually install a VPN certificate on the device:

1. Open Kaspersky Endpoint Security for Android.
2. Tap **Notifications**.
3. In the notification about the certificate, tap **Install**.

   A window with the certificate password opens.
4. Remember or write down the password and tap **OK**.
5. When prompted, enter the certificate password and tap **OK**.
6. Tap **OK** to confirm installation of the certificate.

The VPN certificate will be installed on the device.

Enabling accessibility on Android 13 or later

On Android 13 or later, accessibility services are restricted for apps not downloaded from Google Play or HUAWEI AppGallery. You must manually allow accessibility services if you downloaded Kaspersky Endpoint Security for Android from the Kaspersky Security Center server or the Kaspersky website.

If you update the Kaspersky Endpoint Security for Android app using a Kaspersky Security Center installation package or APK file from the Kaspersky website, accessibility services will be disabled. You must manually enable accessibility services again.

Accessibility is used for the following purposes:

- Check websites and apps in Kaspersky Security Network
- Lock the device in case of theft
- Display warnings
- Block the camera when restricted by the administrator

To enable accessibility for Kaspersky Endpoint Security:

1. Open the **Accessibility** page in the device settings and find Kaspersky Endpoint Security.
2. Turn on the Kaspersky Endpoint Security switch. In the dialog that says that accessibility services are restricted, tap **OK**.

   Now you can give Kaspersky Endpoint Security access to the restricted settings.
3. Open the Kaspersky Endpoint Security info page in the device settings. For example, go to **Settings** > **Apps** and then find the app in the list of apps.
4. On the Kaspersky Endpoint Security info page, tap ⋮ in the top right corner and select **Allow restricted settings**.

   Kaspersky Endpoint Security now has access to the restricted settings.

5. Go back to the **Accessibility** page in the device settings and find Kaspersky Endpoint Security.
6. Turn on the **Kaspersky Endpoint Security** switch. In the dialog that opens, allow the app to have full control of your device.

Accessibility services are now enabled for Kaspersky Endpoint Security.

Enabling accessibility for the app on Android 13 or later

To enable accessibility for Kaspersky Endpoint Security:

1. In the dialog that asks you to turn on accessibility services, tap **Turn On**.

   The **Accessibility** page in the device settings opens.
2. Turn on the Kaspersky Endpoint Security switch. In the dialog that says that accessibility services are restricted, tap **OK**.

   Now you can give Kaspersky Endpoint Security access to the restricted settings.
3. Open the Kaspersky Endpoint Security info page in the device settings. For example, go to **Settings** > **Apps** and then find the app in the list of apps.
4. On the Kaspersky Endpoint Security info page, tap ⋮ in the top right corner and select **Allow restricted settings**.

   Kaspersky Endpoint Security now has access to the restricted settings.
5. Go back to the app and in the dialog that asks you to turn on accessibility services, tap **Turn On**.

   The **Accessibility** page in the device settings opens.
6. Turn on the **Kaspersky Endpoint Security** switch. In the dialog that opens, allow the app to have full control of your device.

Accessibility services are now enabled for Kaspersky Endpoint Security.

Updating the app

Kaspersky Endpoint Security can be updated in the following ways:

- Manually using the Kaspersky website. You download the new version of the app from the Kaspersky website and install it on the device.
- With the help of the administrator. The administrator can remotely update the version of the app on your device by using the Kaspersky Security Center remote administration system.

Updating the app from the Kaspersky website

To update the app from the Kaspersky website:

1. Go to the Kaspersky website.
2. Find Kaspersky Security for Mobile on the website.
3. Tap **Show Downloads**.
4. Select a version of the app and tap **Download**.
5. Open the downloaded APK file and follow the instructions on the screen.

Kaspersky Endpoint Security for Android is updated.

Updating the app via Kaspersky Security Center

Updating the app via Kaspersky Security Center consists of the following steps:

1. The administrator sends to your mobile device the distribution package of the app whose version meets the corporate security requirements.

   A prompt to install Kaspersky Endpoint Security on your device is displayed.

2. Accept the update terms and conditions.

   The new version of the app will be installed to your device. The app does not require additional configuration after the update.

Updates functionality (including providing anti-malware signature updates and codebase updates), as well as KSN functionality may not be available in the software in the U.S.

Removing the app

The administrator can block you from removing the app on your own. If this is the case, you cannot remove Kaspersky Endpoint Security.

Kaspersky Endpoint Security can be removed by the following methods:

- Manually in the device settings.
- With the help of the administrator. The administrator can remotely remove the app from your device by using the Kaspersky Security Center remote administration system.

On corporate devices, Kaspersky Endpoint Security for Android can be removed only by the administrator by resetting the device to factory settings.

Removal in the device settings

The app is removed by following the standard procedure for the Android platform. To remove the app, administrator rights for Kaspersky Endpoint Security must be disabled in the device security settings.

On devices running Android 7 or later, if the administrator has blocked removal, the device will be locked if an attempt is made to remove the app in the Android settings. To unlock the device, contact your administrator.

Removal via Kaspersky Security Center

App removal by using Kaspersky Security Center consists of the following steps:

1. The administrator sends the app removal command to your mobile device.

   Your mobile device displays a prompt to confirm removal of Kaspersky Endpoint Security.

2. Confirm app removal.

   The app will be removed from your device.

Applications with a briefcase icon

Apps marked with a briefcase icon (corporate apps) are stored on your device in the corporate container. *Corporate container* is a safe environment on your device in which the administrator can manage apps and accounts without restricting your capabilities to work with personal data.

The corporate container lets you store corporate data separately from personal data. This keeps corporate data confidential and protects it against malware. When a corporate container is created on your device, the following corporate apps are automatically installed in the corporate container: Google Play Market, Google Chrome, Downloads, Kaspersky Endpoint Security for Android, and others.

Knox app



Knox icon

The Knox app opens a Knox container on your device. A *Knox container* is a safe environment on your device that has its own desktop, launch panel, apps, and widgets. The administrator can manage apps and accounts in a Knox container without restricting your capabilities to work with personal data.

A Knox container lets you store corporate data separately from personal data. This keeps corporate data confidential and protects it against malware.

In a Knox container, you can access your company mailbox, the contact information of enterprise employees, file storage, and other applications.

For more details about working with Knox, please visit the Samsung technical support website.

Using the Kaspersky Protection for iOS app

This Help section describes features and operations that are available to users of the Kaspersky Protection for iOS app.

Articles in this section comprise all the options that can be available or visible on a mobile device. The actual layout and behavior of the app depends on the remote administration system that is implemented and how the administrator configures your device in accordance with corporate security requirements. Some functions and options described in this section may not apply to your actual experience with the app. If you have any questions about the app on your specific device, contact your administrator.

App features

Kaspersky Protection for iOS offers the following key features.

Protection against online threats

The Web Protection component provides protection against online threats.

Web Protection blocks malicious websites that distribute malicious code, and phishing websites designed to steal your confidential data and gain access to your financial accounts. Web Protection scans websites before you open them by using the Kaspersky Security Network cloud service.

Only the website domain is scanned. If it is a malicious or phishing domain, Web Protection blocks the threat. If the domain is not classified as malicious or phishing, the specific URL is not blocked.

Web Protection also monitors the network activity of apps and all system traffic on your device.

For Web Protection to work, you must allow the app to add a VPN configuration.

Jailbreak detection

When Kaspersky Protection for iOS detects a jailbreak, it displays a critical message and informs your administrator about the issue.

A jailbreak allows bypassing the operating system's security features, so the security of your device cannot be guaranteed, and various problems may arise, including:

- Security vulnerabilities
- Stability issues

- Disruption of Apple services
- Potential crashes and freezes
- Shortened battery life
- Inability to apply iOS updates

Installing the app

You can install the Kaspersky Protection for iOS app using a link or a QR code generated for you by the administrator in the management console. You will receive this information in an email.

To install the Kaspersky Protection for iOS app:

1. Find the email message with the administrator's invitation to connect your device to the Kaspersky Security Center remote administration system.
2. Go to the App Store in one of the following ways:
   - Tap **Connect device** in the message if you are reading it on the iOS device that you want to install the app on.
   - Scan the QR code using the iOS device that you want to install the app on, if you are reading the message on a computer.

   The invitation link is valid for 24 hours. If you don't manage to install the app in time, contact your administrator for a new invitation.
3. On the web page that opens, tap **Download on the App Store**.
4. Download and install the app from the App Store by following the standard app installation procedure on the iOS platform.

The Kaspersky Protection for iOS app is installed on your device. To protect the device, activate the app. If your device is not connected to Kaspersky Security Center, you can activate the app manually using the activation code provided by your administrator.

Activating the app

To activate the Kaspersky Protection for iOS app:

1. Start the app on your device.
2. Accept the agreements and statements by selecting the **End User License Agreement** and **Products and Services Privacy Policy** checkboxes.

   Optionally, accept the **Kaspersky Security Network Statement** to allow statistics to be sent to Kaspersky Security Network. This improves the performance of the app and ensures its uninterrupted operation.

3. Tap **Next**. The app connects to the Kaspersky Security Center remote administration system and gets license information.

4. Allow the app to add a VPN configuration. The app uses the VPN configuration to check websites for phishing and protect your device from web threats.

5. Allow the app to send push notifications. The app uses notifications to inform you about security issues and your license.

The Kaspersky Protection for iOS app on your device is activated.

Activating the app with an activation code

When you install the Kaspersky Protection for iOS app on your device, the app connects to the Kaspersky Security Center remote administration system and gets license information automatically. If your device is not connected to Kaspersky Security Center, you can enter the activation code manually. To get the activation code, contact the administrator.

Activate the app manually only when instructed to do so by the administrator.

To enter the activation code:

1. In the message that says that the app is not activated, tap **Activate the app**.

2. In the activation window, enter the activation code that the administrator gave you, and then tap **Activate**.

   If the activation code is correct, a notification is displayed saying that the app has activated, along with the license expiration date.

The Kaspersky Protection for iOS app on your device is activated.

Main window at a glance

The appearance of the main window slightly differs for different screen resolutions.

The main window displays:

- Overall protection status of your device.
- Messages that indicate app component statuses and protection issues.

There are three types of messages:

- Highlighted in green. Status messages that inform you that protection is active in the specified area.
- Highlighted in yellow. Information messages that inform you about events that may affect device security.
- Highlighted in red. Critical messages that inform you about events of critical importance to device security.

You can tap a message for details.

Updating the app

You can download the latest version of the Kaspersky Protection for iOS app from the App Store and install it on your device by following the standard update procedure on the iOS platform. You can also turn on automatic updates. The app does not require any additional configuration after the update.

The following conditions must be met in order for the app to be updated:

- You must have an Apple ID.
- The device must be linked to your Apple ID.
- The device must be connected to the internet.

To learn more about creating an Apple ID, linking your device to your Apple ID, or working with the App Store, see the Apple support website.

Updates functionality (including providing anti-malware signature updates and codebase updates), as well as KSN functionality may not be available in the software in the U.S.

Using diagnostics to troubleshoot issues

If you experience issues with Kaspersky Protection for iOS, Kaspersky Technical Support specialists may ask you to send them a *file with diagnostic information*. This file allows Technical Support specialists to track down the causes of problems in the operation of the app.

In order to share a file with diagnostic information, diagnostics must be enabled in Kaspersky Protection for iOS.

We recommend that you enable diagnostics only if asked to do so by a Kaspersky Technical Support specialist.

Saving diagnostic information may affect your internet connection speed and the performance of your device, Kaspersky Protection for iOS, and other apps.

You can delete the file with diagnostic information manually in the Files app.

To enable diagnostics:

1. In the main window, tap ⓘ.
2. In the **About the App** window that opens, tap **Diagnostics**.
3. In the **Diagnostics** window that opens, enable diagnostics using the **Diagnostics** toggle switch.

4. Accept the Support Statement. The Support Statement describes what data is saved in the file with diagnostic information.

5. Tap **OK**.

Diagnostics will be enabled on your device. Data on the operation of Kaspersky Protection for iOS will now be saved in a file with diagnostic information. If you experience an issue, you can share this file with a Kaspersky Technical Support specialist.

Removing the app

To remove the Kaspersky Protection for iOS app, follow the standard procedure on the iOS platform:

1. On the Home screen, touch and hold the app icon.

2. Remove the app.

The Kaspersky Protection for iOS app is removed from your device.

Application licensing

This section provides information about the general terms related to licensing Advanced MDM in Kaspersky Next Expert View (on-premise).

About the End User License Agreement

The *End User License Agreement* (EULA) is a binding agreement between you and AO Kaspersky Lab, stipulating the Terms and Conditions on which you may use Advanced MDM in Kaspersky Next Expert View (on-premise).

We recommend carefully reading the Terms and Conditions of the EULA before using Advanced MDM in Kaspersky Next Expert View (on-premise).

You can view the Terms and Conditions of the EULA in the following ways:

- During installation of components of Advanced MDM in Kaspersky Next Expert View (on-premise).
- By reading the license.txt file included in the self-extracting archive of the distribution kit for installing the Kaspersky Endpoint Security for Android app.
- In the **About the app** section in Kaspersky Endpoint Security for Android.
- In the **About the App** → **Agreements and Statements** section in Kaspersky Protection for iOS.
- In the **Advanced** → **Accepted License Agreements** section in the Administration Server properties. This feature is available in Kaspersky Security Center version 12.1 and later.
- In the **General** → **End User License Agreements** section in the Administration Server properties of Kaspersky Next Expert View (on-premise).
- At step 4 of the process of connecting mobile devices to Kaspersky Next Expert View (on-premise), if **Administrator** was selected at step 3. The administrator will be prompted to accept the EULA.
- During app installation, if **Users** was selected at step 3 of the process of connecting mobile devices to Kaspersky Next Expert View (on-premise). The mobile device user will be prompted to accept the EULA.

By confirming that you agree with the End User License Agreement (EULA) when installing the components of Advanced MDM in Kaspersky Next Expert View (on-premise), you signify your acceptance of the Terms and Conditions of the End User License Agreement. If you do not accept the terms of the End User License Agreement, you must cancel installation of Advanced MDM in Kaspersky Next Expert View (on-premise) components and refrain from using them.

About the license

A *license* is a time-limited right to use Kaspersky Secure Mobility Management, granted under the terms of the signed License Contract (End User License Agreement).

The scope of services and validity period depend on the license under which the solution is used.

The following license types are provided:

- *Trial*

  A free license intended for trying out the Kaspersky Secure Mobility Management.

  A trial license is valid for 30 days. When a trial license expires, the Kaspersky Endpoint Security for Android mobile app and the Kaspersky Protection for iOS mobile app stop performing most functions, except for synchronization with the Administration Server. To continue using the apps, you need to purchase a commercial license.

- *Commercial*

  A paid license.

  When a commercial license expires, the mobile apps continue to work, but with limited functionality.

  In limited functionality mode, the following components are available depending on the app.

  - Kaspersky Endpoint Security for Android app:

    - Anti-Malware. Real-time Protection and malware scan of the device are available, but anti-malware database updates are not available.
    - Anti-Theft. Only sending commands to mobile device is available.
    - Synchronization with the Administration Server.

    Kaspersky Endpoint Security for Android stops exchanging information with Kaspersky Security Network, Google Analytics for Firebase, Firebase Performance Monitoring, and Crashlytics if the Kaspersky key is blocked, if a trial license expires or if a license is missing (the activation code is removed from the policy).

  - Kaspersky Protection for iOS app:

    - Synchronization with the Administration Server.

    Kaspersky Protection for iOS stops exchanging information with Kaspersky Security Network if a trial license expires or if a license is missing (the activation code is removed from the policy).

  The remaining components of the mobile apps are not available to the device user and you cannot configure policy settings.

  To continue using the full functionality of the apps and configure policy settings, you must renew your commercial license. To ensure uninterrupted protection of your users' devices against all security threats, we recommend renewing the license term or buying a new license before the current one expires.

  With a license that does not provide extended Kaspersky Secure Mobility Management functionality, only basic device protection settings are available in the Kaspersky Mobile Devices Protection and Management plug-in.

  The Call Control feature is available only with an extended functionality license with Call Control.

Viewing license information

The Kaspersky Mobile Devices Protection and Management plug-in lets you view the following information about the current license:

- License key
- The number of devices on which the license key can be used
- License type
- License expiration date and time
- Number of days until the license expires
- The type of functionality available under the current license

To view information about the current license:

1. In the main window of Kaspersky Next Expert View (on-premise), select **Asset management** → **Policies**. In the list of group policies that opens, click the name of the policy that you want to configure.
2. In the policy properties window, select **Application settings**.
3. Click **License**.

   The **License** window containing information about the license opens.

About the subscription

Subscription for Advanced MDM in Kaspersky Next Expert View (on-premise) is an order for using the mobile app with the selected parameters (subscription expiry date, number of mobile devices protected). You can order subscription for Advanced MDM in Kaspersky Next Expert View (on-premise) from your service provider (such as your ISP). Subscription can be renewed manually or automatically, or you may cancel your subscription. You can manage your subscription on the website of the service provider.

Subscription can be limited (for example, one-year) or unlimited (with no expiration date). To keep Advanced MDM in Kaspersky Next Expert View (on-premise) working after expiry of the limited subscription term, you have to renew your subscription. Unlimited subscription is renewed automatically provided a prepayment to the service provider was timely.

If the subscription is limited, when it expires you may be offered a grace period for renewing the subscription, during which time the apps will retain their functionality. The availability and duration of such grace period are at the discretion of the service provider.

To use Advanced MDM in Kaspersky Next Expert View (on-premise) under subscription, you have to apply the activation code received from the service provider. After the activation code is applied, the key is installed for the license for using the application under subscription.

The possible subscription management options may vary with each service provider. The service provider may not offer a subscription renewal grace period during which the apps will retain their functionality.

Activation codes purchased under subscription cannot be used for activating earlier versions of Advanced MDM in Kaspersky Next Expert View (on-premise).

About the license key

A *license key* is a sequence of bits that you can apply to activate and then use the integrated solution Advanced MDM in Kaspersky Next Expert View (on-premise) in accordance with the terms of the End User License Agreement. License keys are generated by Kaspersky specialists.

You can add a license key for the mobile app by using a key file or an activation code:

- If your organization has deployed the Kaspersky Security Center software suite, you have to apply the key file and distribute it to Android mobile apps. The license key is displayed in the interface of Kaspersky Security Center and the interface of the Android mobile app as a unique alphanumeric sequence.

  After adding license keys, you can replace them with other license keys.

  You can't activate the Kaspersky Protection for iOS app with a key file.

- If your organization does not use Kaspersky Security Center, you have to share the activation code with the user. The user enters this activation code in the Android or iOS mobile app. The license key is displayed in the mobile app interface as a unique alphanumeric sequence.

The license key may be blocked by Kaspersky if, for example, the terms of the End User License Agreement have been violated. If the license key has been blocked, the mobile apps stop performing all their functions except for synchronization with the Administration Server. To continue using the apps, you need to add a different license key.

About the activation code

Activation code is a unique sequence of 20 alphanumeric characters. You enter an activation code to add a key that activates the Kaspersky Endpoint Security for Android mobile app or the Kaspersky Protection for iOS mobile app. You receive the activation code at the email address that you have specified after purchasing the integrated solution Advanced MDM in Kaspersky Next Expert View (on-premise) or after ordering the trial version of Advanced MDM in Kaspersky Next Expert View (on-premise).

To activate the mobile app by using the activation code, you need internet access to connect to Kaspersky activation servers.

If you have lost your activation code after you activated the app, it can be restored. You may need your activation code, e.g., to register with Kaspersky CompanyAccount. To restore the activation code, contact Kaspersky Technical Support.

About the key file

A *key file* is a file with the .key extension that you receive from Kaspersky. The purpose of a key file is to add a key that activates the Kaspersky Endpoint Security for Android app.

You can't activate the Kaspersky Protection for iOS app with a key file.

You receive a key file at the email address that you provided when you bought the integrated solution Advanced MDM in Kaspersky Next Expert View (on-premise) or ordered the trial version of Advanced MDM in Kaspersky Next Expert View (on-premise).

You do not need to connect to Kaspersky activation servers in order to activate the application with a key file.

You can restore a key file if it has been accidentally deleted. You may need a key file to register a Kaspersky CompanyAccount, for example.

To restore your key file, perform any of the following actions:

- Contact the license seller.
- Receive a key file through Kaspersky website by using your available activation code.

Data provision in Kaspersky Endpoint Security for Android

Advanced MDM in Kaspersky Next Expert View (on-premise) complies with the General Data Protection Regulations (GDPR).

To install the app, either you or a device user must read and accept the terms of the End User License Agreement. In addition, you can configure a policy to accept the Statements listed below globally, for all users. Otherwise, users will be prompted by a notification on the main app screen to accept the following Statements regarding the processing of the user's personal data:

- Kaspersky Security Network Statement
- Statement regarding data processing for Web Protection
- Statement regarding data processing for marketing purposes
- Statement regarding data processing for Call Control functionality

If you choose to accept the statements globally, the versions of the statements accepted via Kaspersky Security Center must match the versions already accepted by users. Otherwise, the users will be informed about the issue and prompted to accept the version of a statement that matches the version accepted globally by the administrator. The device status in the Kaspersky Mobile Devices Protection and Management plug-in will also change to *Warning*.

The user may accept the terms of a Statement or decline them at any time in the **About the app** section in the settings of Kaspersky Endpoint Security for Android.

Information exchange with Kaspersky Security Network

To improve real-time protection, Kaspersky Endpoint Security for Android uses the Kaspersky Security Network cloud service for operating the following components:

- **Anti-Malware**. The app obtains access to the Kaspersky online knowledge base regarding the reputation of files and apps. The scan is performed for threats whose information has not yet been added to anti-malware databases but is already available in KSN. Kaspersky Security Network cloud service provides full operation of Anti-Malware and reduces the likelihood of false alarms.

- **Web Protection** and **Web Control**. The app uses data received from KSN to scan websites before they are opened. The app also determines the website category to control internet access to users, based on lists of allowed and blocked categories (for example, the "Internet communication" category).

- **App Control**. The app determines the app category to restrict the startup of apps that do not meet corporate security requirements, based on lists of allowed and blocked categories (for example, the "Games" category).

- **Call Control**. The app sends the requests about phone number reputation to KSN and, based on the information received, blocks or allows calls on devices.

Information on the type of data submitted to Kaspersky when using KSN during operation of Anti-Malware and App Control is available in the End User License Agreement. By accepting the terms and conditions of the License Agreement, you agree to transfer this information.

Information on the type of data submitted to Kaspersky when using KSN during operation of Web Protection is available in the Statement regarding data processing for Web Protection. By accepting the terms and conditions of the Statement, you agree to transfer this information.

Information on the type of statistic data submitted to Kaspersky when using KSN during operation of the Kaspersky Endpoint Security for Android mobile app is available in the Kaspersky Security Network Statement. By accepting the terms and conditions of the Statement, you agree to transfer this information.

Information on the type of data submitted to Kaspersky when using KSN during operation of Call Control is available in the Statement regarding data processing for Call Control functionality. By accepting the terms and conditions of the Statement, you agree to transfer this information.

Data provision under the End User License Agreement

Where the Activation Code is used to activate the Software, in order to verify legitimate use of the Software, the End User agrees to periodically provide the Rightholder the following information:

- format of the data in the request to Rightholder infrastructure; accessed IPv4 address of the web service; size of the content of the request to Rightholder infrastructure; protocol ID; Software activation code; data compression type; Software ID; set of IDs of Software that can be activated on the user's device; Software localization; full version of the Software; unique device ID; date and time on the user's device; Software installation ID (PCID); OS version, OS build number, OS update number, OS edition, extended information about the OS edition; device model; operating system family; format of the data in the request to Rightholder infrastructure; checksum type for the object being processed; Software license header; ID of a regional activation center; Software license key creation date and time; Software license ID; ID of the information model used to provide the Software license; Software license expiration date and time; current status of the Software license key; type of Software license used; type of the license used to activate the Software; Software ID derived from the license.

In order to protect the Computer against information security threats, the End User agrees to periodically provide the Rightholder the following information:

- checksum type for the object being processed; checksum of the object being processed; the Software component ID;

- ID of the triggered record in the Software's anti-malware databases; timestamp of the triggered record in the Software's anti-malware databases; type of the triggered record in the Software's anti-malware databases; name of the detected malware or legitimate software that can be used to damage the user's device or data;

- name of store from which the application was installed; application package name; public key used to sign the APK file; checksum of the certificate used to sign the APK file; digital certificate timestamp;

- full version of the Software; Software update ID; type of installed Software; the config identifier; the result of the Software action; error code;

- numbers that are derived from the Android application APK file according to certain mathematical rules and that do not allow restoration of the original file content; this data does not contain file names, file paths, addresses, phone numbers, or other personal information of users.

If You use the Rightholder's update servers to download the Updates, the End User, in order to increase the efficiency of the update procedure, agrees to periodically provide the Rightholder the following information:

- Software ID derived from the license; full version of the Software; Software license ID; type of Software license used; Software installation ID (PCID); ID of the Software update start; web address being processed.

The Rightholder can use such information also for receiving statistical information about the distribution and use of the Software.

The received information is protected by Kaspersky in accordance with the requirements established by law. The original received information is stored in encrypted form and is destroyed as it is accumulated (twice per year) or at the request of the User. General statistics are stored indefinitely.

Data provision under the Kaspersky Security Network Statement

Use of the KSN could lead to increase the effectiveness of protection provided by the Software, against information and network security threats.

If you use a license for 5 or more nodes, the Rightholder will automatically receive and process the following data during use of the KSN:

- ID of the triggered record in the Software's anti-malware databases; timestamp of the triggered record in the Software's anti-malware databases; type of the triggered record in the Software's anti-malware databases; release date and time of the Software's databases; OS version, OS build number, OS update number, OS edition, extended information about the OS edition; OS Service Pack version; detect characteristics; checksum (MD5) of the object being processed; name of the object being processed; flag indicating whether the object being processed is a PE file; checksum (MD5) of the mask that blocked the web service; checksum (SHA256) of the object being processed; size of the object being processed; object type code; the Software's decision on the object being processed; path to the object being processed; directory code; version of the Software's component; version of the statistics being sent; accessed address of the web service (URL, IP); type of client used to access the web service; accessed IPv4 address of the web service; accessed IPv6 address of the web service; web address of the source of the web service request (referer); web address being processed;

- information about scanned objects (application version from AndroidManifest.xml; the Software's decision on the application; method used to get the Software's decision on the application; store installer package name; package name (or bundle name) from AndroidManifest.xml; Google SafetyNet category; flag indicating whether the SafetyNet is enabled on the device; SHA256 value from Google SafetyNet response; APK Signature Scheme for the APK certificate; version code of the installed Software; serial number of the certificate that was used to sign the APK file; name of the APK file that is being installed; path to the APK file that is being installed; issuer of the certificate that was used to sign the APK file; public key used to sign the APK file; checksum of the certificate used to sign the APK file; date and time when the certificate expires; date and time when the certificate was issued; version of the statistics being sent; algorithm for calculating the digital certificate thumbprint; MD5 hash of the installed APK file; MD5 hash of the DEX file located within the APK file; permissions granted dynamically to the application; third-party software version; flag indicating whether the application is the default SMS messenger; flag indicating whether the application has Device Administrator rights; flag indicating whether the application is in the system catalog; flag indicating whether the application uses accessibility services);

- information about all potentially malicious objects and activities (fragment content of the object being processed; date and time when the certificate expires; date and time when the certificate was issued; ID of the key from the keystore used for encryption; protocol used to exchange data with KSN; fragment order in the object being processed; data of the internal log, generated by the anti-malware Software module for an object being processed; certificate issuer name; public key of the certificate; calculation algorithm of public key of the certificate; certificate serial number; date and time of signing the object; certificate owner name and settings; digital certificate thumbprint of the scanned object and hashing algorithm; date and time of the last modification of the object being processed; date and time of creating an object being processed; objects or its parts being processed; description of an object being processed as defined in the object properties; format of the object being processed; checksum type for the object being processed; checksum (MD5) of the object being processed; name of the object being processed; checksum (SHA256) of the object being processed; size of the object being processed; Software vendor name; the Software's decision on the object being processed; version of the object being processed; source of the decision made for the object being processed; checksum of the object being processed; parent application name; path to the object being processed; information about file signature check results; logon session key; encryption algorithm for the logon session key; storage time for object being processed; algorithm for calculating the digital certificate thumbprint);

- build type, for example, "user" or "eng"; full product name; product/hardware manufacturer; whether apps can be installed from outside of Google Play; status of the cloud service for verification of Google apps; status of the cloud service for verification of Google apps being installed through ADB; current development codename or "REL" for production builds; incremental build number; user-visible version string; user device name; user-visible Software's build ID; firmware fingerprint; firmware ID; flag indicating whether the device is rooted; operating system; Software name; type of Software license used;

- information about the quality of KSN services (protocol used to exchange data with KSN; ID of the KSN service accessed by the Software; date and time when statistics stopped being received; number of KSN connections taken from the cache; number of requests for which a response was found in the local request database; number of unsuccessful KSN connections; number of unsuccessful KSN transactions; temporal distribution of cancelled requests to KSN; temporal distribution of unsuccessful KSN connections; temporal distribution of unsuccessful KSN transactions; temporal distribution of successful KSN connections; temporal distribution of successful KSN transactions; temporal distribution of successful requests to KSN; temporal distribution of requests to KSN that timed out; number of new KSN connections; number of unsuccessful requests to KSN caused by routing errors; number of unsuccessful requests caused by KSN being disabled in the Software settings; number of unsuccessful requests to KSN caused by network problems; number of successful KSN connections; number of successful KSN transactions; total number of requests to KSN; date and time when statistics started being received);

- device ID; full version of the Software; Software update ID; Software installation ID (PCID); type of installed Software;

- device screen height; device screen width; information about the overlapping application: MD5 hash of the APK file; information about the overlapping application: MD5 hash of the classes.dex file; information about the overlapping application: name of the APK file; information about the overlapping application: path to the APK file without the file name; overlap height; information about the overlapped Software: MD5 hash of the APK file; overlapped application information: classes.dex file MD5 hash; overlapped application information: APK file name; overlapped application information: path to APK file without file name; overlapped application information: application package name (for the overlapped application: if the advertisement is shown on an empty desktop, the value should be "launcher"); overlap date and time; information about the overlapping application: application package name; overlap width;

- settings of the Wi-Fi access point in use (detected device type; DHCP settings (checksums of gateway local IPv6, DHCP IPv6, DNS1 IPv6, DNS2 IPv6; checksum of network prefix length; checksum of local address IPv6); DHCP settings (checksums of the local IP address of the gateway, DHCP IP, DNS1 IP, DNS2 IP, and subnet mask); flag indicating whether the DNS domain exists; checksum of the assigned local IPv6 address; checksum of the assigned local IPv4 address; flag indicating whether the device is plugged in; Wi-Fi network authentication type; list of available Wi-Fi networks and their settings; checksum (MD5 with salt) of the MAC address of the access point; checksum (SHA256 with salt) of the MAC address of the access point; connection types supported by the Wi-Fi access point; Wi-Fi network encryption type; local time of the start and end of the Wi-Fi network connection; Wi-Fi network ID based on the MAC address of the access point; Wi-Fi network ID based on the Wi-Fi network name; Wi-Fi network ID based on the Wi-Fi network name and the MAC address of the access point; Wi-Fi signal strength; Wi-Fi network name; set of authentication protocols supported by this configuration; authentication protocol used for a WPA-EAP connection; internal authentication protocol; set of group ciphers supported by this configuration; set of key management protocols supported by this configuration; the network's final privacy category in the Software; the network's final security category in the Software; set of block ciphers for WPA that are supported by this configuration; set of security protocols supported by this configuration);

- installation date and time for the Software; Software activation date; identifier of the partner organization via which the Software license order was placed; Software ID derived from the license; serial number of the Software license key; Software localization; flag indicating whether participation in KSN is enabled; ID of the licensed Software; Software license ID; OS ID; operating system bit version.

If you have enabled the Call Control functionality in the Software, then when using Kaspersky Security Network, the Rightholder will automatically receive and process the following data in addition to the data listed above:

- product version; unique device identifier; installation ID; product type;
- instance ID of the anti-spam component; telephone number whose reputation is being requested; call type; network metadata: time zone; network metadata: MCC; network metadata: MNC; number of SIM cards; call metadata: date and hour of call; call metadata: length of call; call metadata: whether the phone number is in the contact list; call metadata: whether the number is in the blocked list; name of the region from which the message is sent; call method; release date and time of the Software databases; timestamp of the Software databases; status of getting information about the phone number;
- phone number checked; information about the phone number: comment; phone number type (spam or not spam, organization); name of the region from which the message is sent; device unique ID checksum; not normalized phone number being processed.

Also, in order to achieve the declared purpose of increasing the effectiveness of protection provided by the Software, the Rightholder may receive objects that could be exploited by intruders to harm the Computer and create information security threats.

Providing the above information to the KSN is voluntary. You can opt out of participating in Kaspersky Security Network at any time.

If the latest version of the Kaspersky Security Network Statement is not accepted, only statistics listed in the previously accepted version of the Statement are sent to Kaspersky Security Network.

Data provision under the Statement regarding data processing for Web Protection

According to Web Protection Statement the Rightholder processes data in order for Web Protection functionality. The stated purpose includes detecting web threats and determining the categories of visited websites using Kaspersky Security Network (KSN).

With Your consent, the following data will be automatically sent on a regular basis to the Rightholder under the Web Protection Statement:

- Product version; Unique device identifier; Installation ID; Product type.
- URL address of the page, port number, URL protocol, URL, which refers to the requested information.

Data provision under the Statement regarding data processing for marketing purposes

The Rightholder uses third-party information systems to process data. Their data processing is governed by the privacy statements of such third-party information systems. The following are the services that the Rightholder uses and the data they process:

Google Analytics for Firebase

During use of the Software, the following data will be sent to Google Analytics for Firebase automatically and on a regular basis in order to achieve the declared purpose:

- app info (app version, app ID, and the ID of the app in the Firebase service, instance ID in the Firebase service, name of the store where the application was obtained, timestamp of the first launch of the Software)
- ID of app installation on the device and method of installation on the device
- information about the region and language localization
- information about the device screen resolution
- information about the user obtaining root
- information about setting Kaspersky Endpoint Security for Android as an Accessibility feature
- information about transitions between application screens, session duration, beginning and end of a screen session, screen name
- information about the protocol used to submit data to the Firebase service, its version, and ID of the data submission method used
- details on the type and parameters of the event for which data is submitted
- information about the app license, its availability, the number of devices
- information about the frequency of anti-malware database updates and synchronization with Administration Server
- information about the Administration Console (Kaspersky Security Center or third-party EMM systems)
- Android ID
- advertising ID
- information about the User: age category and gender, identifier of the country of residence, and list of interests
- information about the User's computer where the Software is installed: computer manufacturer name, type of computer, model, version and the language (locale) of the operating system, information about the application first opened in the last 7 days and the application first opened more than 7 days ago

  Data is forwarded to Firebase over a secure channel. Information about how data is processed in Firebase is published at: https://firebase.google.com/support/privacy.

Firebase Performance Monitoring

During the use of the Software, the following data will be sent to Firebase Performance Monitoring automatically and on a regular basis in order to achieve the declared purpose:

- unique installation ID
- application package name
- version of the installed software
- battery level and battery-charging state
- carrier

- app foreground or background state
- geography
- IP address
- device language code
- information about the radio/network connection
- pseudonymous Software instance ID
- RAM and disk size
- flag indicating whether the device is jailbroken or rooted
- signal strength
- duration of automated traces
- network, and the following corresponding information: response code, payload size in bytes, response time
- device description

  Data is forwarded to Firebase Performance Monitoring over a secure channel. Information about how data is processed in Firebase Performance Monitoring is published at: https://firebase.google.com/support/privacy.

Crashlytics

During the use of the Software, the following data will be sent to Crashlytics automatically and on a regular basis in order to achieve the declared purpose:

- Software ID
- version of the installed software
- flag indicating whether the Software was running in the background
- CPU architecture
- unique event ID
- event date and time
- device model
- total disk space and amount currently used
- name and version of the OS
- total RAM and amount currently used
- flag indicating whether the device is rooted
- screen orientation at the time of the event
- product/hardware manufacturer

- unique installation ID
- version of the statistics being sent
- the Software exception type
- text of the error message
- a flag indicating that the Software exception was caused by a nested exception
- thread ID
- a flag indicating whether the frame was the cause of the Software error
- a flag indicating that the thread caused the Software to terminate unexpectedly
- information about the signal that caused the Software to terminate unexpectedly: signal name, signal code, signal address
- for each frame associated with a thread, exception, or error: the name of the frame file, line number of the frame file, debug symbols, address and offset in the binary image, display name of the library with the frame, type of the frame, flag indicating whether the frame was the cause of the error
- OS ID
- ID of the issue associated with the event
- information about events that happened before the Software terminated unexpectedly: event identifier, event date and time, event type and value
- CPU register values
- event type and value

  Data is forwarded to Crashlytics over a secure channel. Information about how data is processed in Crashlytics is published at: https://firebase.google.com/terms/crashlytics-app-distribution-data-processing-terms.

Providing the above information for processing for marketing purposes is voluntary.

Data provision under the Statement regarding data processing for Call Control functionality

Under the laws of some countries, some of the data processed under this Statement may be classified as personal data. With Your consent, the following data will be automatically sent on a regular basis to the Rightholder under the Statement:

- Product version; Unique device identifier; Installation ID; Product type;
- Statistics message type; Telephone number whose reputation is being requested; Statistics submission scenario.

Data provision in Kaspersky Protection for iOS

Advanced MDM in Kaspersky Next Expert View (on-premise) complies with the General Data Protection Regulations (GDPR).

To install the app, a device user must read and accept the terms of the following statements regarding the processing of the user's personal data:

- End User License Agreement
- Products and Services Privacy Policy

Optionally, the user may read and accept the terms of the following statement:

- Kaspersky Security Network Statement
- Support Statement

The user can view the terms of these documents at any time in the **About the App → Agreements and Statements** section in the settings of Kaspersky Protection for iOS. In this section, the user can also accept or decline the terms of the KSN Statement.

Information exchange with Kaspersky Security Network

To improve real-time protection, Kaspersky Protection for iOS uses the Kaspersky Security Network cloud service for operating the **Web Protection** component. The app uses data received from KSN to scan web resources before they are opened.

Information on the type of data submitted to Kaspersky when using KSN during operation of Web Protection is available in the End User License Agreement. By accepting the terms and conditions of the License Agreement, you agree to transfer this information.

Information on the type of statistic data submitted to Kaspersky when using KSN during operation of the Kaspersky Protection for iOS mobile app is available in the Kaspersky Security Network Statement. By accepting the terms and conditions of the Statement, you agree to transfer this information.

Data provision under the End User License Agreement

Where the Activation Code is used to activate the Software, in order to verify legitimate use of the Software, the End User agrees to periodically provide the Rightholder the following information:

- Format of the data in the request to Rightholder's infrastructure; accessed IPv4 address of the web service; size of the content of the request to Rightholder infrastructure; protocol ID; Software activation code; data compression type; Software ID; set of IDs of Software that can be activated on the user's device; Software localization; full version of the Software; unique device ID; date and time on the user's device; Software installation ID (PCID); currently used Software activation code; OS version, OS build number, OS update number, OS edition, extended information about the OS edition; device model; mobile carrier code; operating system family; Software ID derived from the license; list of agreements presented to the user by the Software; type of legal agreement accepted by the user while using the Software; version of the legal agreement accepted by the user while using the Software; flag indicating whether the user has accepted the terms of the legal agreement while using the Software; checksum type for the object being processed; Software license header; ID of a regional activation center; Software license key creation date and time; Software license ID; ID of the information model used to provide the Software license; Software license expiration date and time; current status of the Software license key; type of Software license used; type of the license used to activate the Software; Software ID derived from the license.

The Rightholder can use such information also for obtaining statistical information about the distribution and use of the Rightholder's Software.

In order to protect the Computer against information security threats, the End User agrees to periodically provide the Rightholder the following information:

- Format of the data in the request to Rightholder's infrastructure; accessed address of the web service (URL, IP); port number; web address of the source of the web service request (referrer).

- Full version of the Software; Software update ID; type of the installed Software; Software ID; the configuration identifier; the result of the Software action; error code.

- Web address being processed; accessed IPv4 address of the web service; digital certificate thumbprint of the scanned object and hashing algorithm; certificate type; contents of the digital certificate being processed.

Data provision under the Kaspersky Security Network Statement

When the KSN Statement is accepted, the Rightholder automatically receives and processes the following data:

- Information about the quality of KSN services (protocol used to exchange data with KSN; ID of the KSN service accessed by the Software; date and time when statistics stopped being received; number of KSN connections taken from the cache; number of requests for which a response was found in the local request database; number of unsuccessful KSN connections; number of unsuccessful KSN transactions; temporal distribution of cancelled requests to KSN; temporal distribution of unsuccessful KSN connections; temporal distribution of unsuccessful KSN transactions; temporal distribution of successful KSN connections; temporal distribution of successful KSN transactions; temporal distribution of successful requests to KSN; temporal distribution of requests to KSN that timed out; number of new KSN connections; number of unsuccessful requests to KSN caused by routing errors; number of unsuccessful requests caused by KSN being disabled in the Software settings; number of unsuccessful requests to KSN caused by network problems; number of successful KSN connections; number of successful KSN transactions; total number of requests to KSN; date and time when statistics started being received).

- Device ID; full version of the Software; Software update ID; Software installation ID (PCID); type of the installed Software.

- Installation date and time for the Software; Software activation date; Software localization; flag indicating whether participation in KSN is enabled; ID of the licensed Software; Software license ID; OS ID; version of the operating system installed on the user's computer; operating system bit version.

Providing the above information to the KSN is voluntary. You can opt out of participating in Kaspersky Security Network at any time.

Data provision under the Support Statement

When diagnostics are enabled in Kaspersky Protection for iOS, the app processes and stores the following personal data for further analysis by Technical Support:

- Event date and time.

- HTTP codes and data for server requests to the Rightholder's systems: request body; request URL; server responses; errors.

- Data on all network requests: request URL; traffic check status.

- License information: license ID and activation code; validity period of the current license data package; current Software key status; operating mode after the license expires; Software activation date; license expiration date; order number when purchasing the license.

- Information about the connection with the Administration Server: certificate password; Administration Server connection address; unique device ID; users' certificates data; Administration Server certificates data; Software settings received from the Administration Server.

- System events: opening and closing the Software; push notifications from the Software.

- Information about the operation of the Software and its modules.

- OS version; OS type.
- Device ID; device type.
- Software ID; Software language ID; Software version; Software installation ID.
- Information about Software errors.

Providing the above information to the Technical Support is voluntary.

Contact Technical Support

This section describes how to get technical support and the terms on which it is available.

How to get technical support

If you can't find a solution to your issue in the Advanced MDM in Kaspersky Next Expert View (on-premise) documentation or in any of the sources of information about Advanced MDM in Kaspersky Next Expert View (on-premise), contact Technical Support. Technical Support specialists will answer all your questions about installing and using Advanced MDM in Kaspersky Next Expert View (on-premise).

Kaspersky provides support of Advanced MDM in Kaspersky Next Expert View (on-premise) during its lifecycle (see the product support lifecycle page). Before contacting Technical Support, please read the support rules.

You can contact Technical Support in one of the following ways:

- By visiting the Technical Support website
- By sending a request to Technical Support from the Kaspersky CompanyAccount portal

Technical support via Kaspersky CompanyAccount

Kaspersky CompanyAccount is a portal for companies that use Kaspersky applications. The Kaspersky CompanyAccount portal is designed to facilitate interaction between users and Kaspersky specialists through online requests. You can use Kaspersky CompanyAccount to track the status of your online requests and store a history of them as well.

You can register all of your organization's employees under a single account on Kaspersky CompanyAccount. A single account lets you centrally manage electronic requests from registered employees to Kaspersky and also manage the privileges of these employees via Kaspersky CompanyAccount.

The Kaspersky CompanyAccount portal is available in the following languages:

- English
- Spanish
- Italian
- German
- Polish
- Portuguese

- Russian
- French
- Japanese

To learn more about Kaspersky CompanyAccount, visit the Technical Support website.

Sources of information about the application

Advanced MDM in Kaspersky Next Expert View (on-premise) web page on the Kaspersky website

On the Advanced MDM in Kaspersky Next Expert View (on-premise) page, you can find general information about the application, its features and operation parameters.

The web page of Advanced MDM in Kaspersky Next Expert View (on-premise) provides a link to eStore. There you can purchase or renew the application.

Advanced MDM in Kaspersky Next Expert View (on-premise) web page in the Knowledge Base

Knowledge Base is a section on the Kaspersky Customer Service website.

On the Advanced MDM in Kaspersky Next Expert View (on-premise) page in the Knowledge Base you can find articles that contain useful information, recommendations and answers to frequently asked questions on the application purchasing, installation, and use.

Knowledge Base articles can answer questions relating to not only to Advanced MDM in Kaspersky Next Expert View (on-premise) but also to other Kaspersky applications. Knowledge Base articles can also include Technical Support news.

Help

The Help of the application comprises help files.

Online help of the Kaspersky Endpoint Security for Android and Kaspersky Protection for iOS apps provides information on how to configure and use mobile apps.

Discussing Kaspersky applications on Kaspersky Support Forum

If your question does not require an immediate answer, you can discuss it with Kaspersky experts and other users on our Forum.

On the Forum, you can view discussion topics, post your comments, and create new discussion topics.

Glossary

Activating the application

Switching the application to fully functional mode. Application activation is performed by the user during or after installation of the application. You should have an activation code or key file to activate the application.

Activation code

A code that you receive when purchasing a license for Kaspersky Endpoint Security. This code is required for activating the application.

The activation code is a unique sequence of twenty letters and numbers in the format xxxxx-xxxxx-xxxxx-xxxxx.

Administration group

A set of managed devices, such as mobile devices grouped according to the functions they perform and the set of apps installed on them. Managed devices are grouped so that they can be managed as a single whole. For example, mobile devices running the same operating system can be combined into an administration group. A group may include other administration groups. It is possible to create group policies and send commands for group devices.

Administration Server

A component of Kaspersky Security Center that centrally stores information about all Kaspersky applications that are installed within the corporate network. It can also be used to manage these applications.

Administrator's workstation

The computer on which Kaspersky Next Expert View (on-premise) has been deployed. Using the administrator's workstation, with the mobile management plug-ins installed, the administrator performs the centralized management of mobile devices.

Android Work Profile

A self contained profile that can be set up on an Android device to ensure the separation of work related data from personal data. Android Work Profile lets organizations have full control of the work apps and data on a device while user's personal apps and data remain private.

Anti-malware databases

Databases that contain information about computer security threats known to Kaspersky as of when the anti-malware databases are released. Entries in anti-malware databases allow malicious code to be detected in scanned objects. Anti-malware databases are created by Kaspersky experts and updated hourly.

Apple Push Notification service (APNs) certificate

Certificate signed by Apple, which allows you to use Apple Push Notification. Through Apple Push Notification, an iOS MDM Server can manage iOS and iPadOS devices.

Basic control

A device operating mode for personal iOS devices. This operating mode lets you perform the protection and basic management of devices.

Basic protection

A device operating mode for personal iOS devices. This operating mode lets you perform the protection against web threats and jailbreak detection on devices using the Kaspersky Protection for iOS.

Certificate Signing Request

File with the settings of an Administration Server, which is approved by Kaspersky and then sent to Apple to obtain an APNs certificate.

Compliance Control

Verification that the settings of a mobile device and Kaspersky Endpoint Security for Android comply with corporate security requirements. Corporate security requirements regulate the device usage. For example, real-time protection must be enabled on the device, the anti-malware databases must be up-to-date, and the device password must be strong enough. Compliance control is based on a list of rules. A compliance rule includes the following components:

- Device check criterion (for example, absence of prohibited apps on the device)
- Time interval allocated for the user to fix the noncompliance (for example, 24 hours)
- Action that will be taken on the device if the user does not fix the noncompliance within the time set (for example, locking the device)

Corporate container

A safe environment on the user's device in which the administrator can manage apps and user accounts without restricting the use of personal data by the user. When a corporate container is created on the user's mobile device, the following corporate apps are automatically installed in the corporate container: Google Play, Google Chrome, Downloads, Kaspersky Endpoint Security for Android, and others. Corporate apps installed in the corporate container and notifications of these apps are marked with a briefcase icon. You have to create a separate Google corporate account for the Google Play app. Apps installed in the corporate container appear in the common list of apps.

Corporate device

A device operating mode for company-owned Android devices. This operating mode lets you have full control over the entire device and configure an extended set of security settings and features.

Device administrator

A set of app rights on an Android device that enables the app to use device management policies. It is necessary to implement full functionality of Kaspersky Endpoint Security on Android devices.

End User License Agreement

Binding agreement between you and AO Kaspersky Lab that stipulates the terms on which you may use the application.

Group task

A task intended for an administration group and performed on all managed devices included in the group.

IMAP

Protocol for accessing email. In contrast to the POP3 protocol, IMAP provides extended capabilities for working with mailboxes, such as managing folders and handling messages without copying their contents from the mail server. The IMAP protocol uses port 143.

Installation package

A set of files created for remote installation of a Kaspersky application by using the remote administration system. An installation package is created on the basis of dedicated files included in the application distribution package. The installation package contains a range of settings needed to install the application and get it running immediately after installation. The values of settings in the distribution kit correspond to default values of application settings.

iOS MDM device

An iOS mobile device controlled by the iOS MDM Server.

iOS MDM Server

A component of Kaspersky Endpoint Security that is installed on a client device, allowing connection of iOS mobile devices to the Administration Server and management of iOS mobile devices through Apple Push Notifications (APNs).

Kaspersky categories

Predefined data categories developed by Kaspersky experts. Categories can be updated during application database updates. A security officer cannot modify or delete predefined categories.

Kaspersky Private Security Network (KPSN)

Kaspersky Private Security Network is a solution that gives users of devices with Kaspersky applications installed access to reputation databases of Kaspersky Security Network and other statistical data—without sending data from their devices to Kaspersky Security Network. Kaspersky Private Security Network is designed for corporate customers who are unable to participate in Kaspersky Security Network for any of the following reasons:

- Devices are not connected to the internet.
- Transmission of any data outside the country or the corporate LAN is prohibited by law or corporate security policies.

Kaspersky Security Center Administrator

The person managing application operations through the Kaspersky Security Center remote centralized administration system.

Kaspersky Security Center Web Server

A component of Kaspersky Security Center that is installed together with Administration Server. Web Server is designed for transmission, over a network, of stand-alone installation packages, management profiles, and files from a shared folder.

Kaspersky Security Network (KSN)

An infrastructure of cloud services that provides access to the Kaspersky database with constantly updated information about the reputation of files, web resources, and software. Kaspersky Security Network ensures faster responses by Kaspersky applications to threats, improves the performance of some protection components, and reduces the likelihood of false positives.

Kaspersky update servers

HTTP(S) servers at Kaspersky from which Kaspersky applications download database and application module updates.

Key file

A file in xxxxxxxx.key format that makes it possible to use a Kaspersky application under a trial or commercial license. The application generates the key file based on the activation code. You may use the application only when you have a key file.

License

A time-limited right to use the app, granted under the End User License Agreement.

License term

A time period during which you have access to the application features and rights to use additional services. The services you can use depend on the type of the license.

Malware

A program that infects other ones, by adding its code to them in order to gain control when infected files are run. This simple definition allows identifying the main action performed by any malware: infection.

Management profile

A profile that contains a set of settings for connecting iOS mobile devices to the Administration Server. A management profile makes it possible to distribute iOS configuration profiles in background mode using the iOS MDM Server, and also receive extended diagnostic information about mobile devices. A link to the management profile needs to be sent to a user in order to enable the iOS MDM Server to discover and connect the user's iOS mobile device.

Manifest file

A file in PLIST format containing a link to the app file (IPA file) located on a web server. It is used by iOS devices to locate, download, and install apps from a web server.

Mobile management plug-in

A dedicated component that provides the interface for managing mobile devices through Kaspersky Next Expert View (on-premise).

Network Agent

A Kaspersky Security Center component that enables interaction between the Administration Server and Kaspersky applications that are installed on a specific network node (workstation or server).

Personal device

A device operating mode for personal Android devices. This operating mode lets you perform the protection and basic management of devices.

Phishing

A type of internet fraud aimed at obtaining unauthorized access to users' confidential data.

Policy

A set of settings of the application and Kaspersky Endpoint Security mobile apps applied to devices in administration groups or to individual devices. Different policies can be applied to different administration groups. A policy includes the configured settings of all functions of Kaspersky Endpoint Security mobile apps.

POP3

Network protocol used by a mail client to receive messages from a mail server.

Proxy server

A computer network service which allows users to make indirect requests to other network services. First, a user connects to a proxy server and requests a resource (e.g., a file) located on another server. Then the proxy server either connects to the specified server and obtains the resource from it or returns the resource from its own cache (if the proxy has its own cache). In some cases, a user's request or a server's response can be modified by the proxy server for certain purposes.

Quarantine

The folder to which the Kaspersky application moves probably infected objects that have been detected. Objects are stored in Quarantine in encrypted form in order to avoid any impact on the computer.

SSL

A data encryption protocol used on the internet and local networks. The Secure Sockets Layer (SSL) protocol is used in web applications to create a secure connection between a client and server.

Standalone installation package

An installation file of Kaspersky Endpoint Security for the Android operating system, which contains the settings of application connection to the Administration Server. It is created on the basis of the installation package of this application and is a particular case of mobile app package.

Subscription

Enables use of the application within the selected parameters (expiration date and number of devices). You can pause or resume your subscription, renew it automatically, or cancel it.

Supervised device

iOS or iPadOS device whose settings are monitored by Apple Configurator, a program for group configuration of iOS and iPadOS devices. A supervised device has the *supervised* status in Apple Configurator. Every time a supervised device connects to the computer, Apple Configurator checks the device configuration against the specified reference settings, and then redefines them if necessary. A supervised device cannot be synchronized with Apple Configurator installed on a different computer.

Every supervised device provides more settings to redefine through the Kaspersky Device Management for iOS policy than a non-supervised device. For example, you can configure an HTTP proxy server to monitor internet traffic on a device within the corporate network. By default, all mobile devices are non-supervised.

Unlock code

A code that you can get in Kaspersky Security Center. It is needed to unlock a device after the **Lock & Locate**, **Alarm**, or **Mugshot** commands have been executed, and when Self-Defense is triggered.

Virtual Administration Server

A component of Kaspersky Security Center, designed for management of the protection system of a client organization's network.

Virtual Administration Server is a particular case of a secondary Administration Server and has the following restrictions as compared with a physical Administration Server:

- Virtual Administration Server can be created only on a primary Administration Server.
- Virtual Administration Server uses the primary Administration Server database in its operation. Data backup and restoration tasks, as well as update scan and download tasks, are not supported on a virtual Administration Server.
- Virtual Server does not support creation of secondary Administration Servers (including virtual Servers).

Information about third-party code

You can download and read information about third-party code in the following files:

- legal_notices_Android.txt (for the Kaspersky Endpoint Security for Android app)
- legal_notices_iOS.txt (for the Kaspersky Protection for iOS app)
- legal_notices_KMDPM.txt (for the Kaspersky Mobile Devices Protection and Management plug-in)
- legal_notices_iOS_MDM.txt (for iOS MDM Server and the iOS MDM Server settings plug-in)

On mobile devices, information about third-party code is available in the **About the App** section of the mobile apps.

Trademark notices

Registered trademarks and service marks are the property of their respective owners.

Adobe, Flash, and PostScript are either registered trademarks or trademarks of Adobe in the United States and/or other countries.

AMD64 is a trademark or registered trademark of Advanced Micro Devices, Inc.

Amazon, Amazon EC2, Amazon Web Services, AWS, and AWS Marketplace are trademarks of Amazon.com, Inc. or its affiliates.

Apache is either a registered trademark or a trademark of the Apache Software Foundation in the United States and/or other countries.

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, and Touch ID are trademarks of Apple Inc.

The Bluetooth word, mark and logos are owned by Bluetooth SIG, Inc.

Aironet, Cisco, Cisco AnyConnect, and IOS are registered trademarks or trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

Debian is a registered trademark of Software in the Public Interest, Inc.

Dell Technologies, Dell, SecurID, and other trademarks are trademarks of Dell Inc. or its subsidiaries.

F5 is a trademark of F5 Networks, Inc. in the U.S. and in certain other countries.

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, and YouTube are trademarks of Google LLC.

HTC is a trademark or registered trademark in the U.S. and/or other countries of HTC Corporation and its affiliates.

HUAWEI and EMUI are trademarks of Huawei Technologies Co., Ltd.

Juniper Networks, Juniper, and JUNOS are trademarks or registered trademarks of Juniper Networks, Inc. in the United States and other countries.

Linux is the registered trademark of Linus Torvalds in the U.S. and other countries.

Mail.ru is a Trademark of Mail.ru LLC.

Microsoft, Active Directory, ActiveSync, Bing, Forefront, Microsoft Edge, Outlook, SQL Server, Tahoma, Windows, Windows Mobile, Windows Phone, and Windows Server are trademarks of the Microsoft group of companies.

MOTOROLA and the Stylized M Logo are trademarks or registered trademarks of Motorola Trademark Holdings, LLC.

Mozilla and Firefox are trademarks of the Mozilla Foundation in the U.S. and other countries.

OPPO is a trademark or registered trademark of Guangdong OPPO Mobile Telecommunications Co., Ltd.

Oracle, JavaScript are registered trademarks of Oracle and/or its affiliates.

Red Hat and Red Hat Enterprise Linux are trademarks or registered trademarks of Red Hat, Inc. or its subsidiaries in the United States and other countries.

The BlackBerry trademark is owned by Research In Motion Limited and is registered in the United States and may be pending or registered in other countries.

Samsung is a trademark of SAMSUNG in the United States or other countries.

SonicWALL, Aventail, and SonicWALL Mobile Connect are trademarks of SonicWall, Inc.

Symantec is a trademark or registered trademark of Symantec Corporation or its affiliates in the U.S. and other countries.

Symbian trademark is owned by the Symbian Foundation Ltd.