

The Kaspersky logo is displayed in a bold, black, lowercase sans-serif font. It is positioned in the upper left quadrant of the page, which features a white, rounded rectangular shape against a teal background with a green-to-teal gradient.

# Kaspersky Security für mobile Endgeräte

© 2022 AO Kaspersky Lab

# Inhalt

[Hilfe zu Kaspersky Security für mobile Endgeräte](#)

[Neuerungen](#)

[Vergleich der Programmfunktionen in Abhängigkeit von Verwaltungstools](#)

[Lieferumfang](#)

[Arbeiten in Kaspersky Security Center Web Console und Kaspersky Security Center Cloud Console](#)

[Über die Funktionalität "Mobile Geräte verwalten" in Kaspersky Security Center Web Console und Cloud Console](#)

[Hauptfunktionen zur Verwaltung mobiler Geräte in Kaspersky Security Center Web Console und Cloud Console](#)

[Über die App "Kaspersky Endpoint Security für Android"](#)

[Über die App "Kaspersky Security für iOS"](#)

[Über das Plug-in für Kaspersky Security for Mobile \(Devices\)](#)

[Über das Plug-in für Kaspersky Security for Mobile \(Policies\)](#)

[Hardware- und Softwarevoraussetzungen](#)

[Bekannte Probleme und Besonderheiten](#)

[Bereitstellung einer Lösung zur Verwaltung mobiler Geräte in der Kaspersky Security Center Web Console oder Cloud Console](#)

[Bereitstellungsszenarien](#)

[Vorbereitung der Kaspersky Security Center Web Console und Cloud Console für die Bereitstellung](#)

[Administrationsserver für die Anbindung von mobilen Endgeräten anpassen](#)

[Administrationsgruppe erstellen](#)

[Regel für das automatische Verschieben von Geräten in eine Administrationsgruppe erstellen](#)

[Bereitstellung der Verwaltungs-Plug-ins](#)

[Verwaltungs-Plug-ins aus der Liste der verfügbaren Programmpakete installieren](#)

[Verwaltungs-Plug-ins aus dem Paket des Lieferumfangs installieren](#)

[Mobile App bereitstellen](#)

[Bereitstellung der mobilen App über Kaspersky Security Center Web Console oder Cloud Console](#)

[Mobile App aktivieren](#)

[Bereitstellung der erforderlichen Berechtigungen für die App Kaspersky Endpoint Security für Android](#)

[Zertifikate verwalten](#)

[Zertifikatsliste anzeigen](#)

[Zertifikatseinstellungen festlegen](#)

[Zertifikat erstellen](#)

[Zertifikat erneuern](#)

[Zertifikat löschen](#)

[Informationsaustausch mit Firebase Cloud Messaging](#)

[Mobile Geräte in Kaspersky Security Center Web Console und Cloud Console verwalten](#)

[Mobile Geräte mit Kaspersky Security Center verbinden](#)

[Nicht zugeordnete mobile Geräte in Administrationsgruppen verschieben](#)

[Befehle an mobile Geräte senden](#)

[Mobile Geräte aus Kaspersky Security Center entfernen](#)

[Gruppenrichtlinien verwalten](#)

[Gruppenrichtlinien für die Verwaltung von mobilen Geräten](#)

[Liste der Gruppenrichtlinien anzeigen](#)

[Ergebnisse der Richtlinienverteilung anzeigen](#)

[Gruppenrichtlinie erstellen](#)

[Gruppenrichtlinie bearbeiten](#)

[Gruppenrichtlinie kopieren](#)

[Richtlinie zu einer anderen Administrationsgruppe verschieben](#)

[Gruppenrichtlinie löschen](#)

[Richtlinieneinstellungen definieren](#)

[Antivirenschutz konfigurieren](#)

[Echtzeitschutz konfigurieren](#)

[Die automatische Untersuchung auf Viren auf mobilen Geräten konfigurieren](#)

[Updates der Antiviren-Datenbanken konfigurieren](#)

[Einstellungen zum Entsperren des Geräts konfigurieren](#)

[Datenschutz bei Verlust oder Diebstahl des Geräts konfigurieren](#)

[Anwendungskontrolle konfigurieren](#)

[Übereinstimmungsüberprüfung für mobile Geräte hinsichtlich der korporativen Sicherheit konfigurieren](#)

[Übereinstimmungsregeln aktivieren und deaktivieren](#)

[Übereinstimmungsregeln anpassen](#)

[Übereinstimmungsregeln hinzufügen](#)

[Übereinstimmungsregeln löschen](#)

[Liste mit Kriterien für fehlende Übereinstimmung](#)

[Liste der Maßnahmen bei fehlender Übereinstimmung](#)

[Benutzerzugriff auf Websites anpassen](#)

[Einschränkungen für Funktionen konfigurieren](#)

[Schutz von Kaspersky Endpoint Security für Android vor Deinstallation](#)

[Synchronisierung mobiler Geräte mit Kaspersky Security Center konfigurieren](#)

[Kaspersky Security Network](#)

[Informationsaustausch mit dem Kaspersky Security Network](#)

[Kaspersky Security Network aktivieren und deaktivieren](#)

[Informationsaustausch mit Google Analytics for Firebase, SafetyNet Attestation, Firebase Performance Monitoring und Crashlytics](#)

[Benachrichtigungen auf mobilen Geräten konfigurieren](#)

[Gehackte Geräte erkennen](#)

[Lizenzeinstellungen festlegen](#)

[Ereignisse konfigurieren](#)

[Ereignisse zum Installieren, Aktualisieren und Entfernen von Apps auf den Geräten der Benutzer konfigurieren](#)

[Netzwerkbelastung](#)

[Arbeiten in der MMC-basierten Verwaltungskonsole](#)

[Wichtige Anwendungsfälle](#)

[Über Kaspersky Security für mobile Endgeräte](#)

[Hauptfunktionen zur Verwaltung mobiler Geräte in der Verwaltungskonsole auf MMC-Basis](#)

[Über Kaspersky Endpoint Security für Android](#)

[Über Kaspersky Device Management für iOS](#)

[Über das Exchange-E-Mail-Postfach](#)

[Über das Verwaltungs-Plug-in von Kaspersky Endpoint Security für Android](#)

[Über das Verwaltungs-Plug-in für Kaspersky Device Management für iOS](#)

[Hardware- und Softwarevoraussetzungen](#)

[Bekannte Probleme und Besonderheiten](#)

[Verteilung](#)

[Lösungsarchitektur](#)

[Typische Vorgehensweisen bei der Verteilung der Komplexlösung](#)

[Verteilungsschemata für Kaspersky Endpoint Security für Android](#)

[Verteilungsschemata für das iOS MDM-Profil](#)

[Verwaltungskonsolle für die Verteilung der Komplexlösung vorbereiten](#)

[Einstellungen des Administrationsservers für die Anbindung von mobilen Endgeräten anpassen](#)

[Ordner Mobile Geräte verwalten in der Verwaltungskonsolle anzeigen](#)

[Administrationsgruppe erstellen](#)

[Erstellen einer Regel für das automatische Verschieben von Geräten in eine Administrationsgruppe](#)

[Allgemeines Zertifikat erstellen](#)

[Kaspersky Endpoint Security für Android installieren](#)

[Berechtigungen](#)

[Installation von Kaspersky Endpoint Security für Android über einen Google Play-Link](#)

[Andere Methoden zur Installation von Kaspersky Endpoint Security für Android](#)

[Manuelle Installation über Google Play oder Huawei AppGallery](#)

[Erstellen und Konfigurieren eines Installationspakets](#)

[Erstellen eines eigenständigen Installationspakets](#)

[Synchronisierungseinstellungen anpassen](#)

[Aktivierung der App Kaspersky Endpoint Security für Android](#)

[iOS MDM-Profil installieren](#)

[Über die Verwaltungsmodi für iOS-Geräte](#)

[Installation über Kaspersky Security Center](#)

[Installation des Verwaltungs-Plug-ins](#)

[Upgrade einer Vorgängerversion des Programms](#)

[Update der vorherigen Version von Kaspersky Endpoint Security für Android](#)

[Installation einer vorherigen Version von Kaspersky Endpoint Security für Android](#)

[Update vorheriger Versionen der Verwaltungs-Plug-Ins](#)

[Kaspersky Endpoint Security für Android deinstallieren](#)

[Ferngesteuerte Deinstallation der Anwendung](#)

[Erlaubnis zur Deinstallation der Anwendung die Benutzer](#)

[Deinstallieren der Anwendung durch den Benutzer](#)

[Konfiguration und Verwaltung](#)

[Erste Schritte](#)

[Programm starten und anhalten](#)

[Administrationsgruppe erstellen](#)

[Gruppenrichtlinien für die Verwaltung von mobilen Geräten](#)

[Gruppenrichtlinie erstellen](#)

[Synchronisierungseinstellungen anpassen](#)

[Verwendung der Revisionen von Gruppenrichtlinien](#)

[Gruppenrichtlinie löschen](#)

[Rechte zur Konfiguration von Gruppenrichtlinien einschränken](#)

[Schutz](#)

[Antiviren-Schutz für Android-Geräte anpassen](#)

[Schutz von Android-Geräten im Internet](#)

[Datenschutz bei Verlust oder Diebstahl des Geräts](#)

[Befehle an mobiles Gerät senden](#)

[Entsperren des mobilen Geräts](#)

[Datenverschlüsselung](#)

[Sicherheit des Kennworts für das Entsperren des Geräts anpassen](#)

[Sicherheit des Kennworts für das Entsperren des Android-Geräts anpassen](#)

[Sicherheit des Kennworts für das Entsperren des iOS MDM-Geräts anpassen](#)

[Sicherheit des Kennworts für das Entsperren des EAS-Geräts anpassen](#)

[Konfiguration des virtuellen privaten Netzwerks \(VPN\)](#)  
[VPN-Einstellungen auf Android-Geräten \(nur Samsung\)](#)  
[VPN-Einstellungen auf iOS MDM-Geräten](#)  
[Firewall-Einstellungen auf Android-Geräten \(nur Samsung\)](#)  
[Schutz von Kaspersky Endpoint Security für Android vor Deinstallation](#)  
[Gehackte Geräte erkennen \(root\)](#)  
[Globalen HTTP-Proxy auf iOS MDM-Geräten anpassen](#)  
[Sicherheitszertifikate auf iOS MDM-Geräten hinzufügen](#)  
[SCEP-Profil auf iOS MDM-Geräten hinzufügen](#)

## Kontrolle

[Beschränkungen konfigurieren](#)  
[Besonderheiten für Geräte unter Android Version 10 und später](#)  
[Beschränkungen für Android-Geräte anpassen](#)  
[Beschränkungen für iOS MDM-Geräte anpassen](#)  
[Funktionsbeschränkungen für EAS-Geräte konfigurieren](#)  
[Benutzerzugriff auf Websites anpassen](#)  
[Zugriff auf Websites auf Android-Geräten konfigurieren](#)  
[Zugriff auf Websites auf iOS MDM-Geräten konfigurieren](#)  
[Übereinstimmungsüberprüfung für Android-Geräte hinsichtlich der korporativen Sicherheit](#)  
[Kontrolle des App-Starts](#)  
[Kontrolle des Starts von Apps auf Android-Geräten](#)  
[Einschränkungen der Apps für EAS-Geräte konfigurieren](#)  
[Inventarisierung der Software auf Android-Geräten](#)  
[Einstellungen für die Anzeige von Android-Geräten in Kaspersky Security Center](#)

## Verwaltung

[Verbindungseinstellungen für das WLAN-Netzwerk anpassen](#)  
[Android-Geräte mit einem WLAN-Netzwerk verbinden](#)  
[iOS MDM-Geräte mit einem WLAN-Netzwerk verbinden](#)  
[E-Mail anpassen](#)  
[E-Mail-Postfach auf iOS MDM-Geräten konfigurieren](#)  
[Exchange-E-Mail-Postfach auf iOS MDM-Geräten konfigurieren](#)  
[Einstellungen des Exchange-E-Mail-Postfachs auf dem Android-Gerät \(nur Samsung\)](#)  
[Verwaltung mobiler Anwendungen von Drittherstellern](#)  
[Benachrichtigungen für Kaspersky Endpoint Security für Android anpassen](#)  
[Verbindung von iOS MDM-Geräten mit AirPlay](#)  
[Verbindung von iOS MDM-Geräten mit AirPrint](#)  
[Zugriffspunkt \(APN\) anpassen](#)  
[APN-Einstellungen auf Android-Geräten \(nur Samsung\)](#)  
[APN-Einstellungen auf iOS MDM-Geräten](#)  
[Einstellungen des Arbeitsprofils Android anpassen](#)  
[Über das Arbeitsprofil Android](#)  
[Einstellungen des Arbeitsprofils anpassen](#)  
[LDAP-Account hinzufügen](#)  
[Kalender-Account hinzufügen](#)  
[Kontakte-Account hinzufügen](#)  
[Kalenderabonnement anpassen](#)  
[Webclips hinzufügen](#)  
[Schriftarten hinzufügen](#)

[App über EMM-Systeme von Drittanbietern verwalten \(nur Android\)](#)

[Erste Schritte](#)

[So installieren Sie die App](#)

[So aktivieren Sie die App](#)

[So verbinden Sie Ihr Gerät mit Kaspersky Security Center](#)

[Datei AppConfig](#)

[Netzwerkbelastung](#)

[Teilnahme am Kaspersky Security Network](#)

[Informationsaustausch mit dem Kaspersky Security Network](#)

[Verwendung von Kaspersky Security Network aktivieren und deaktivieren](#)

[Kaspersky Private Security Network verwenden](#)

[Datenbereitstellung an Drittanbieter-Dienste](#)

[Informationsaustausch mit Firebase Cloud Messaging](#)

[Informationsaustausch mit Google Analytics for Firebase, SafetyNet Attestation, Firebase Performance Monitoring und Crashlytics](#)

[Globale Annahme der zusätzlichen Erklärungen](#)

[Samsung KNOX](#)

[Installation der App Kaspersky Endpoint Security für Android über KNOX Mobile Enrollment](#)

[KNOX MDM-Profil erstellen](#)

[Geräte zu KNOX Mobile Enrollment hinzufügen](#)

[App installieren](#)

[KNOX-Container konfigurieren](#)

[Über den KNOX-Container](#)

[Samsung KNOX aktivieren](#)

[Einstellungen der Firewall in KNOX](#)

[Einstellungen des Exchange-E-Mail-Postfachs in KNOX](#)

[Anhang](#)

[Rechte zur Konfiguration von Gruppenrichtlinien](#)

[Kategorien für Apps](#)

[Verwendung der App Kaspersky Endpoint Security für Android](#)

[Funktionen der Anwendung](#)

[Hauptfenster im Überblick](#)

[Untersuchung des Geräts](#)

[Untersuchung nach Zeitplan ausführen](#)

[Schutzmodus ändern](#)

[Update der Antiviren-Datenbanken](#)

[Datenbanken-Update nach Zeitplan](#)

[Aktion bei Diebstahl oder Verlust des Geräts](#)

[Web-Filter](#)

[Anwendungskontrolle](#)

[Zertifikat anfordern](#)

[Synchronisierung mit Kaspersky Security Center](#)

[Die App "Kaspersky Endpoint Security für Android" ohne Kaspersky Security Center aktivieren](#)

[App aktualisieren](#)

[Anwendung deinstallieren](#)

[Apps mit einer "Aktentasche"](#)

[Die Anwendung KNOX](#)

[Verwendung der App Kaspersky Security für iOS](#)

[Funktionen der Anwendung](#)

[App installieren](#)

[App aktivieren](#)

[Die App mit einem Aktivierungscode aktivieren](#)

[Hauptfenster im Überblick](#)

[App aktualisieren](#)

[Anwendung deinstallieren](#)

[Lizenzverwaltung für das Programm](#)

[Über den Lizenzvertrag](#)

[Lizenz-Info](#)

[Über das Abonnement](#)

[Über den Schlüssel](#)

[Über den Aktivierungscode](#)

[Über die Schlüsseldatei](#)

[Bereitstellung von Daten in Kaspersky Endpoint Security für Android](#)

[Bereitstellung von Daten in Kaspersky Security für iOS](#)

[Kontaktaufnahme mit dem Technischen Support](#)

[Kontakt zum Technischen Support](#)

[Technischer Support über das Kaspersky CompanyAccount](#)

[Informationsquellen zur App](#)

[Glossar](#)

[Abonnement](#)

[Administrationsgruppe](#)

[Administrationsserver](#)

[Administrator von Kaspersky Security Center](#)

[Administrator-Arbeitsplatz](#)

[Aktivierungscode](#)

[Antiviren-Datenbanken](#)

[Arbeitsprofil Android](#)

[Betreutes Gerät](#)

[CSR-Anfrage \(Certificate Signing Request\)](#)

[EAS-Gerät](#)

[Eigenständiges Installationspaket](#)

[Endbenutzer-Lizenzvertrag](#)

[Entsperrungscode](#)

[Exchange Server für mobile Geräte](#)

[Geräteadministrator](#)

[Gruppenaufgabe](#)

[Gültigkeitsdauer der Lizenz](#)

[IMAP](#)

[Installationspaket](#)

[iOS MDM-Gerät](#)

[iOS MDM-Profil](#)

[iOS MDM-Server für Mobilgeräte](#)

[Kaspersky Private Security Network \(Private KSN\)](#)

[Kaspersky Security Network \(KSN\)](#)

[Kaspersky-Kategorien](#)

[Kaspersky-Update-Server](#)

[Lizenz](#)  
[Manifest-Datei](#)  
[Phishing](#)  
[POP3](#)  
[Programm aktivieren](#)  
[Provisioning-Profil](#)  
[Proxy-Server](#)  
[Quarantäne](#)  
[Richtlinie](#)  
[Schlüsseldatei](#)  
[SSL](#)  
[Übereinstimmungsüberprüfung](#)  
[Verwaltungs-Plug-in für Programme](#)  
[Virus](#)  
[Webserver für Kaspersky Security Center](#)  
[Zertifikat für den Apple Push Notification Service \(APNs\)](#)  
[Informationen über den Code von Drittherstellern](#)  
[Markenrechtliche Hinweise](#)



# Hilfe zu Kaspersky Security für mobile Endgeräte

Kaspersky Security für mobile Endgeräte dient dem Schutz und der Verwaltung von mobilen Unternehmensgeräten und persönlichen mobilen Geräten, welche die Mitarbeiter einer Organisation für Unternehmenszwecke verwenden.

Die Komponenten und Funktionen von Kaspersky Security für mobile Endgeräte sind auf die Konsole von Kaspersky Security Center angewiesen, die Sie als Schnittstelle zum Schutz und zur Verwaltung mobiler Geräte verwenden.

Wählen Sie je nach Art Ihrer Konsole von Kaspersky Security Center den relevanten Hilfeabschnitt aus:

- [Verwaltungskonsole auf Basis der Microsoft Management Console](#)
- [Kaspersky Security Center Web Console oder Kaspersky Security Center Cloud Console](#)

Die Funktionen und Vorgänge, die für Benutzer der Apps [Kaspersky Endpoint Security für Android](#) und [Kaspersky Security für iOS](#) verfügbar sind, werden in speziellen Hilfeabschnitten beschrieben.

# Neuerungen

## Kaspersky Security für iOS Technisches Release 1

Die neue App von Kaspersky Security für iOS wurde zum Schutz und für die Verwaltung von Unternehmensgeräten mit iOS und iPadOS entwickelt. Die wichtigsten Funktionen der App sind:

- Schutz vor Bedrohungen aus dem Internet.
- Erkennung von Jailbreaks.
- Verwaltung von Unternehmensgeräten mittels Kaspersky Security Center Web Console oder Cloud Console.

## Kaspersky Endpoint Security für Android Technisches Release 42

- Verbesserungen für die Benutzeroberfläche der in App Kaspersky Endpoint Security für Android.
- Kaspersky Endpoint Security für Android benötigt jetzt unter Android 12 oder höher die Berechtigung "Bluetooth-Geräte in der Nähe", damit der Administrator die Bluetooth-Funktion einschränken darf.
- Allgemeine Fehlerbehebungen und Verbesserungen.

## Kaspersky Endpoint Security für Android Technisches Release 41

- Verbesserungen für die Benutzeroberfläche der in App Kaspersky Endpoint Security für Android.
- Verbesserungen für die Benutzeroberfläche in den Richtlinieneinstellungen des Plug-ins von Kaspersky Security for Mobile (Policies) für Kaspersky Security Center Web Console und Cloud Console.
- Allgemeine Fehlerbehebungen und Verbesserungen.

## Kaspersky Endpoint Security für Android Technisches Release 40

- Allgemeine Fehlerbehebungen und Verbesserungen.

## Kaspersky Endpoint Security für Android Technisches Release 39

- Android 12L wird jetzt unterstützt.
- Die folgenden Verträge und Erklärungen wurden aktualisiert:
  - Endbenutzer-Lizenzvertrag
  - Vereinbarung zu Kaspersky Security Network
  - Bestimmungen für die Datenverarbeitung zu Marketingzwecken

Hinweis: Der Administrator kann die neuen Bedingungen der Verträge und Erklärungen in der Verwaltungskonsolle akzeptieren. Dies ermöglicht, diesen Schritt für die Benutzer der App Kaspersky Endpoint Security für Android auf den Geräten zu überspringen.

- Allgemeine Fehlerbehebungen und Verbesserungen.

## Kaspersky Endpoint Security für Android Technisches Release 33

- Wenn Sie die App Kaspersky Endpoint Security für Android [mithilfe von EMM-Systemen von Drittanbietern](#) verwalten, können Sie jetzt mehrere Endbenutzer-Lizenzverträge mit einem einzigen Befehl akzeptieren.
- Sie benötigen keinen Schlüssel mehr, [um Samsung KNOX zu aktivieren](#).
- Die Struktur der Komponentenversionen von Kaspersky Security für mobile Endgeräte wurde geändert, um die Versionsnummer aufzunehmen.

## Kaspersky Endpoint Security für Android Technisches Release 32

- Die App von Kaspersky Endpoint Security für Android wurde angepasst, um aktualisierte Android-Anforderungen zu unterstützen.

## Kaspersky Endpoint Security für Android Technisches Release 31

- Wenn Kaspersky Security Center in Ihrem Unternehmen nicht bereitgestellt wird oder für mobile Geräte nicht zugänglich ist, können Benutzer [die App von Kaspersky Endpoint Security für Android manuell auf ihren Geräten aktivieren](#).
- Kaspersky Security für mobile Endgeräte unterstützt jetzt die Custom Tabs-Funktion von Google Chrome.

## Kaspersky Endpoint Security für Android Technisches Release 30

- Mit Kaspersky Security für mobile Endgeräte können Sie jetzt [mobile Geräte via Kaspersky Security Center Cloud Console schützen und verwalten](#).
- Kaspersky Security für mobile Endgeräte unterstützt jetzt iOS 15 und iPadOS 15.

## Kaspersky Endpoint Security für Android Technisches Release 29

- Die App "Kaspersky Endpoint Security für Android" unterstützt nun Android 12.

## Kaspersky Endpoint Security für Android Technisches Release 27

- Mit Kaspersky Security für mobile Endgeräte können Sie jetzt [mobile Geräte via Kaspersky Security Center Web Console schützen und verwalten](#).

## Kaspersky Endpoint Security für Android Technisches Release 26

- Kaspersky Endpoint Security unterstützt jetzt Lizenzen und Abonnements mit automatischer Verlängerung.

## Kaspersky Endpoint Security für Android Technisches Release 22

- Kaspersky Endpoint Security [unterstützt jetzt Kaspersky Private Security Network](#), eine Lösung, die den Zugriff auf die Reputationsdatenbanken von Kaspersky Security Network ermöglicht, ohne dass Daten außerhalb des Unternehmensnetzwerks gesendet werden müssen.
- Die Installation von Kaspersky Endpoint Security für Android auf Geräten mit Android-Versionen 4.2–4.4.4 wird nicht mehr unterstützt.

## Kaspersky Endpoint Security für Android Technisches Release 20

- Die Benutzer werden nicht aufgefordert, die rechtlichen Erklärungen zu akzeptieren, wenn der Administrator die [Aussagen global akzeptiert](#) hat.
- Die App-Leistung wurde optimiert.

## Kaspersky Endpoint Security für Android Technisches Release 19

- Der Administrator kann jetzt die Erklärung zu Kaspersky Security Network und andere Erklärungen im Namen der Endbenutzer über Kaspersky Security Center akzeptieren.
- Eine Reihe von Fehlern wurde behoben, die Stabilität der Programmausführung wurde verbessert.

## Kaspersky Endpoint Security für Android Technisches Release 18

- Kaspersky Security für mobile Endgeräte unterstützt jetzt Huawei Mobile Services.
- Kaspersky Endpoint Security für Android kann jetzt über die [Huawei App Gallery installiert](#) werden.

## Kaspersky Endpoint Security für Android Technisches Release 17

- Da Kaspersky Endpoint Security API-Level 29 und höher erreichen soll, haben wir einige Änderungen am Verhalten der App auf Geräten mit Android 10 und höher implementiert.
- Neue Einstellungen für die Kennwortstärke mit denen der Benutzer Kennwörter mit der erforderlichen Komplexität festlegen kann.
- Das Verwenden des Fingerabdrucks zum Entsperren des Bildschirms ist jetzt nur für das Android-Arbeitsprofil verfügbar.
- Eine Reihe von Fehlern wurde behoben, die Stabilität der Programmausführung wurde verbessert.

## Kaspersky Endpoint Security für Android Technisches Release 16

- Kaspersky Endpoint Security für Android unterstützt nun Android 11.

- Neue Anforderungen an die Erteilung der Zugriffsrechte für Standort und Kamera in Android 11. Weitere Informationen zu den neuen Regeln für Kamera- und Standortzugriffsberechtigungen finden Sie in diesem [Abschnitt](#).
- Die Unternehmens-E-Mail-Adressen des Benutzers können jetzt über die EMM-Konsole eines Drittanbieters angegeben werden. Diese E-Mail-Adressen werden in Kaspersky Security Center angezeigt, sofern KscCorporateEmail konfiguriert wurde.

## Kaspersky Endpoint Security für Android Technisches Release 14

- Immer, wenn ein Benutzer die Rechte des Geräteadministrators der App gewährt oder entzieht, wird ein Ereignis an die Management-Konsole gesendet.
- Die Einstellung "KscGroup" kann nun in der EMM-Konsole eines Drittanbieters konfiguriert werden. Sobald ein Gerät mit Kaspersky Security Center verbunden wird, wird es automatisch zu einem Unterordner des Ordners "Nicht zugeordnete Geräte" hinzugefügt; der Unterordner trägt den Namen der in der EMM-Konsole festgelegten Gruppe.

## Kaspersky Endpoint Security für Android Technisches Release 13

- Neues Design der Benutzeroberfläche von Kaspersky Endpoint Security für Android.
- Alle Abschnitte der Hilfe sind jetzt online zu finden.
- Die IP-Adressen der verwalteten Geräte werden nun an Kaspersky Security Center gesendet und können in den Abschnitten mit Geräteinformationen angesehen werden.

## Kaspersky Endpoint Security für Android Technisches Release 12

- Es ist nun möglich, den Endbenutzer-Lizenzvertrag (EULA) in Kaspersky Security Center 12.1 per Remote-Zugriff zu akzeptieren. Wenn der Administrator die Bedingungen des Lizenzvertrags und die Datenschutzrichtlinie in der Verwaltungskonsole akzeptiert, überspringt die App diese Schritte während der Installation.
- Benutzer von VMware AirWatch können nun den Gerätenamen in Kaspersky Security Center bearbeiten. Wir haben eine neue Einstellung zur config-Datei hinzugefügt, mit deren Hilfe die App konfiguriert wird. Zum Gerätenamen können noch weitere Informationen hinzugefügt werden (zum Beispiel die Seriennummer des Geräts). Das erleichtert die Suche und das Filtern von Geräten in Kaspersky Security Center.

## Kaspersky Endpoint Security für Android Technisches Release 11

Eine Reihe von Fehlern wurde behoben, die Stabilität der Programmausführung wurde verbessert.

## Kaspersky Endpoint Security für Android Technisches Release 10

- Kaspersky Security für mobile Endgeräte unterstützt jetzt Kaspersky Security Center 12.
- Die Unterstützung für Kaspersky Safe Browser wurde in Kaspersky Security Center 12 beendet. Die Funktionen von Kaspersky Safe Browser können weiterhin in der Version Kaspersky Security Center 11 oder früher verwendet werden.
- Eine Reihe von Fehlern wurde behoben, die Stabilität der Programmausführung wurde verbessert.

## Kaspersky Endpoint Security für Android Service Pack 4 Maintenance Release 3

- Überprüfte Unterstützung für Kaspersky Endpoint Security für Android in Microsoft Intune (eine Enterprise Mobility Management (EMM)-Lösung). Damit die App zusammen mit EMM-Lösungen von Drittherstellern funktioniert, nimmt Kaspersky an der AppConfig Community teil.
- Es ist nun möglich, [Benachrichtigungen und Pop-up-Meldungen zu deaktivieren, wenn die App im Hintergrund ausgeführt wird](#). Bitte beachten Sie, dass es nicht sicher ist, diese Aktionen im Hintergrundmodus auszuführen. Wenn Sie Benachrichtigungen und Pop-up-Meldungen für die Ausführung der App im Hintergrund deaktivieren, werden Benutzer nicht in Echtzeit vor Bedrohungen gewarnt. Die Benutzer der mobilen Geräte müssen dann die App öffnen, um den Schutzstatus des Geräts zu sehen.
- Es ist nun möglich, den Endbenutzer-Lizenzvertrag (EULA) und die Datenschutzrichtlinie in VMware AirWatch zu akzeptieren. Wenn der Administrator den Lizenzvertrag und die Datenschutzrichtlinie in AirWatch-Konsole akzeptiert hat, überspringt Kaspersky Endpoint Security für Android den Schritt zur Annahme des Lizenzvertrags im Assistenten für Erstkonfiguration.
- Die Erklärung zur Verarbeitung von Daten für die Verwendung von Web-Filter (Erklärung für Web-Filter) wurde hinzugefügt. Sie müssen diese Erklärung akzeptieren, um Web-Filter verwenden zu können. Kaspersky Endpoint Security für Android nutzt Kaspersky Security Network (KSN) zur Untersuchung von Websites. Die Erklärung für Web-Filter enthält die Nutzungsbedingungen für den Datenaustausch mit KSN. Sie können die Erklärung für Web-Filter in der Richtlinie annehmen oder einen Gerätebenutzer zur Annahme auffordern.
- Eine Reihe von Fehlern wurde behoben, die Stabilität der Programmausführung wurde verbessert.

# Vergleich der Programmfunktionen in Abhängigkeit von Verwaltungstools

Mobile Geräte können mithilfe der folgenden Verwaltungstools via Kaspersky Security Center verwaltet werden:

- Verwaltungskonsole von Kaspersky Security Center auf der Grundlage der Microsoft Management Console (im Folgenden als "MMC-basiert" bezeichnet)
- Kaspersky Security Center Web Console
- Kaspersky Security Center Cloud Console

Die folgende Tabelle vergleicht die Funktionen, die in diesen Tools zur Verfügung stehen.

Verfügbarkeit von Funktionen in Abhängigkeit von Verwaltungstools

	MMC-basierte Konsole	Web Console	Cloud Console
<b>Allgemein</b>			
Verwaltung von Android-Geräten	<a href="#">Verfügbar</a>	<a href="#">Verfügbar</a>	<a href="#">Verfügbar</a>
Verwaltung von iOS-Geräten	<a href="#">Verfügbar</a> (über ein APNs-Zertifikat)	<a href="#">Verfügbar</a> (über die App "Kaspersky Security für iOS")	<a href="#">Verfügbar</a> (über die App "Kaspersky Security für iOS")
<b>Komponente "Mobile Geräte verwalten"</b>			
Geräte hinzufügen über einen Link auf Google Play	<a href="#">Verfügbar</a>	<a href="#">Verfügbar</a>	<a href="#">Verfügbar</a>
Geräte über einen App Store-Link hinzufügen	Nicht verfügbar	<a href="#">Verfügbar</a>	<a href="#">Verfügbar</a>
iOS-Geräte über ein iOS MDM-Profil hinzufügen	<a href="#">Verfügbar</a>	Nicht verfügbar	Nicht verfügbar
Geräte hinzufügen durch Erstellen eines Installationspakets	<a href="#">Verfügbar</a>	Nicht verfügbar	Nicht verfügbar
Befehle an mobile Geräte senden	<a href="#">Verfügbar</a>	<a href="#">Verfügbar</a> (außer dem Befehl "Foto aufnehmen")	<a href="#">Verfügbar</a> (außer dem Befehl "Foto aufnehmen")
Mobile Geräte aus Kaspersky Security Center entfernen	<a href="#">Verfügbar</a>	<a href="#">Verfügbar</a> (Wird nur aus der Geräteliste entfernt. Die App muss manuell vom Gerät entfernt werden.)	<a href="#">Verfügbar</a> (Wird nur aus der Geräteliste entfernt. Die App muss manuell vom Gerät entfernt werden.)
<b>Zertifikatsverwaltung</b>			
Ausstellen von E-Mail-Zertifikaten	Verfügbar	Nicht verfügbar	Nicht verfügbar
Ausstellen von VPN-Zertifikaten	Verfügbar	Nicht verfügbar	Nicht verfügbar
Ausstellen von mobilen Zertifikaten	Verfügbar	Verfügbar	Verfügbar

Ausstellen von mobilen Zertifikaten mithilfe der Tools des Administrationsservers	<a href="#">Verfügbar</a>	<a href="#">Verfügbar</a>	<a href="#">Verfügbar</a>
Angabe von Zertifikatsdateien	<a href="#">Verfügbar</a>	Nicht verfügbar	Nicht verfügbar
Integration mit einer Public-Key-Infrastruktur	Verfügbar	Nicht verfügbar	Nicht verfügbar
<b>Richtlinienverwaltung</b>			
Rollenbasierter Zugriff auf die Konfiguration von Gruppenrichtlinien	Verfügbar	Nicht verfügbar	Nicht verfügbar
Konfiguration der Synchronisierung von mobilen Geräten mit Kaspersky Security Center	<a href="#">Verfügbar</a>	<a href="#">Verfügbar</a>	<a href="#">Verfügbar</a>
Konfiguration der Untersuchung auf Viren auf mobilen Geräten	<a href="#">Verfügbar</a>	<a href="#">Verfügbar</a>	<a href="#">Verfügbar</a>
Konfiguration des Schutzes mobiler Geräte	<a href="#">Verfügbar</a>	<a href="#">Verfügbar</a>	<a href="#">Verfügbar</a>
Updates der Antiviren-Datenbanken konfigurieren	<a href="#">Verfügbar</a>	<a href="#">Verfügbar</a>	<a href="#">Verfügbar</a>
Datenschutz bei Verlust oder Diebstahl des Geräts konfigurieren	<a href="#">Verfügbar</a>	<a href="#">Verfügbar</a>	<a href="#">Verfügbar</a>
Benutzerzugriff auf Websites anpassen	<a href="#">Verfügbar</a>	<a href="#">Verfügbar</a>	<a href="#">Verfügbar</a>
Anwendungskontrolle konfigurieren	<a href="#">Verfügbar</a>	<a href="#">Verfügbar</a>	<a href="#">Verfügbar</a>
Konfiguration der Übereinstimmungsüberprüfung	<a href="#">Verfügbar</a>	<a href="#">Verfügbar</a>	<a href="#">Verfügbar</a>
Konfiguration der Arbeitsprofile Android	<a href="#">Verfügbar</a>	Nicht verfügbar	Nicht verfügbar
Verbindungseinstellungen für das WLAN-Netzwerk anpassen	<a href="#">Verfügbar</a>	Nicht verfügbar	Nicht verfügbar
Samsung KNOX	<a href="#">Verfügbar</a>	Nicht verfügbar	Nicht verfügbar
<b>Andere Funktionen</b>			
Globale Akzeptanz der EULA in Kaspersky Security Center	<a href="#">Verfügbar</a>	Nicht verfügbar	Nicht verfügbar
Konfiguration von Kaspersky Private Security Network	<a href="#">Verfügbar</a>	Nicht verfügbar	Nicht verfügbar



# Lieferumfang

Der Lieferumfang von Kaspersky Security für mobile Endgeräte kann je nach gewählter Programmversion verschiedene Komponenten enthalten.

## Funktionalität "Mobile Geräte verwalten" in Kaspersky Security Center Web Console

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

Archiv mit den Dateien, die für die Installation des Plug-ins für Kaspersky Security for Mobile (Devices) erforderlich sind:

- `plugin.zip`

Archiv mit dem Plug-in für Kaspersky Security for Mobile (Devices).

- `signature.txt`

Datei mit der Signatur für das Plug-in für Kaspersky Security for Mobile (Devices).

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

Archiv mit den Dateien, die für die Installation des Plug-ins für Kaspersky Security for Mobile (Policies) erforderlich sind:

- `plugin.zip`

Archiv mit dem Plug-in für Kaspersky Security for Mobile (Policies).

- `signature.txt`

Datei mit der Signatur für das Plug-in für Kaspersky Security for Mobile (Policies).

## Funktionalität "Mobile Geräte verwalten" in Kaspersky Security Center Cloud Console

Um mobile Geräte via Kaspersky Security Center Cloud Console zu verwalten, müssen Sie kein Programmpaket herunterladen. Sie müssen lediglich ein Konto in Kaspersky Security Center Cloud Console erstellen. Nähere Informationen zur Erstellung eines Kontos finden Sie in der [Hilfe zu Kaspersky Security Center Cloud Console](#).

## Funktionalität "Mobile Geräte verwalten" in der Verwaltungskonsole auf MMC-Basis

- `Klcfginst_en.exe`

Installationsdatei des Verwaltungs-Plug-ins für Kaspersky Endpoint Security für Android für die Verwaltung der App mithilfe des Remote-Verwaltungssystems Kaspersky Security Center.

- `Klmdminst.exe`

Installationsdatei des Verwaltungs-Plug-ins für Kaspersky Device Management für iOS zur Verwaltung der App mithilfe des Remote-Verwaltungssystems Kaspersky Security Center.

## Datei der App "Kaspersky Endpoint Security für Android"

`KES10_xx_xx_xxx.apk` – Android-Paket der App "Kaspersky Endpoint Security für Android".

## Hilfsdateien

- `sc_package_xx.exe`

Selbstextrahierendes Archiv mit den Dateien, die erforderlich sind, um Installationspakete zur Installation der App "Kaspersky Endpoint Security für Android" zu erstellen:

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

Dateien, die zum Erstellen von Installationspaketen erforderlich sind.

- `installer.ini`

Konfigurationsdatei mit Einstellungen für die Verbindung zum Administrationsserver.

- `KES10_xx_xx_xxx.apk`

Android-Paket der App "Kaspersky Endpoint Security für Android".

- `kmlisten.exe`

Tool zum Bereitstellen von Installationspaketen über den Computer des Administrators.

- `kmlisten.ini`

Konfigurationsdatei mit den Einstellungen für das Tool `kmlisten.exe`.

- `kmlisten.kpd`

Datei mit einer Beschreibung der App.

- `SigningUtility.zip`

Archiv mit dem Tool zum Signieren der Programmpakete der App "Kaspersky Endpoint Security für Android" und der Container für iOS-Geräte.

## Dokumentation

- Hilfe zu Kaspersky Security für mobile Endgeräte.

# Arbeiten in Kaspersky Security Center Web Console und Kaspersky Security Center Cloud Console

Dieser Hilfeabschnitt beschreibt den Schutz und die Verwaltung mobiler Geräte mittels Kaspersky Security Center Web Console (im Folgenden auch als Web Console bezeichnet) oder mittels Kaspersky Security Center Cloud Console (im Folgenden auch als Cloud Console bezeichnet).

## Über die Funktionalität "Mobile Geräte verwalten" in Kaspersky Security Center Web Console und Cloud Console

Mobile Geräte können mithilfe der folgenden Komponenten via Kaspersky Security Center Web Console und Cloud Console verwaltet werden:

- **App "Kaspersky Endpoint Security für Android"**

Die App "Kaspersky Endpoint Security für Android" gewährleistet den Schutz mobiler Geräte vor Webbedrohungen, Viren und anderen gefährlichen Programmen.

- **App von Kaspersky Security für iOS**

Die App "Kaspersky Security für iOS" schützt mobile Geräte vor Phishing und Schadsoftware.

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

Das Plug-in für Kaspersky Security for Mobile (Devices) bietet eine Schnittstelle zur Verwaltung von mobilen Geräten und den darauf installierten mobilen Apps via Kaspersky Security Center Web Console und Cloud Console.

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

Mit dem Plug-in für Kaspersky Security for Mobile (Policies) können Sie mithilfe von Gruppenrichtlinien die Konfigurationseinstellungen für Geräte festlegen, die mit Kaspersky Security Center verbunden sind.

Die Plug-ins sind in das *Remote-Verwaltungssystem von Kaspersky Security Center* integriert. Via Kaspersky Security Center Web Console oder Cloud Console können Sie mobile Geräte sowie Client-Computer und virtuelle Systeme verwalten. Nach dem Verbinden der mobilen Endgeräte mit dem Administrationsserver können die Geräte verwaltet werden. Die verwalteten Geräte können ferngesteuert überwacht werden.

## Hauptfunktionen zur Verwaltung mobiler Geräte in Kaspersky Security Center Web Console und Cloud Console

Kaspersky Security für mobile Endgeräte bietet die folgenden Funktionen:

- Versand von E-Mail-Nachrichten zum Verbinden mobiler Android-Geräte mit Kaspersky Security Center mithilfe von Download-Links für die App "Kaspersky Endpoint Security für Android" aus Google Play.
- Versand von E-Mail-Nachrichten zum Verbinden mobiler iOS-Geräte mit Kaspersky Security Center mithilfe von Download-Links für die App "Kaspersky Security für iOS" aus App Store.
- Remote-Verbindung der mobilen Geräte der Benutzer mit Kaspersky Security Center und anderen externen EMM-Systemen (z. B. VMWare AirWatch, MobileIron, IBM Maas360, SOTI MobiControl).

- Remote-Konfigurieren der mobilen App sowie der Dienste, Apps und Funktionen von mobilen Geräten.
- Ferngesteuerte Konfiguration der Mobilgeräte entsprechend der korporativen Sicherheit.
- Verhinderung des Verlustes der auf mobilen Geräten gespeicherten Unternehmensdaten im Fall von Diebstahl und Verlust (Diebstahlschutz). Wird nur für Android-Geräte unterstützt.
- Kontrolle der Einhaltung der Anforderungen an die Unternehmenssicherheit (Übereinstimmungsüberprüfung). Wird nur für Android-Geräte unterstützt.
- Steuerung des Schutzes vor Online-Bedrohungen und Verwaltung der Internetnutzung auf Mobilgeräten (Web-Filter).
- Konfiguration der Benachrichtigungen, die dem Benutzer in den Apps "Kaspersky Endpoint Security für Android" und "Kaspersky Security für iOS" angezeigt werden.
- An den Administrator gerichtete Benachrichtigungen über den Status und die Ereignisse der Apps "Kaspersky Endpoint Security für Android" und "Kaspersky Security für iOS" können über Kaspersky Security Center oder per E-Mail gesendet werden.
- Kontrolle der Änderungen der RichtlinienEinstellungen (Revisionsverlauf).

Kaspersky Security für mobile Endgeräte besteht aus den folgenden Schutz- und Verwaltungskomponenten:

- Anti-Virus (für Android-Geräte)
- Diebstahlschutz (für Android-Geräte)
- Web-Filter (für Android- und iOS-Geräte)
- Anwendungskontrolle (für Android-Geräte)
- Übereinstimmungsüberprüfung (für Android-Geräte)
- Erkennung von Root-Rechten auf Android-Geräten und Jailbreak-Erkennung auf iOS-Geräten

## Über die App "Kaspersky Endpoint Security für Android"

Die App "Kaspersky Endpoint Security für Android" gewährleistet den Schutz mobiler Geräte vor Webbedrohungen, Viren und anderen gefährlichen Programmen.

Die App "Kaspersky Endpoint Security für Android" enthält folgende Komponenten:

- **Anti-Virus.** Diese Komponente kann Bedrohungen auf Ihrem Gerät erkennen und beseitigen. Dazu werden die Antiviren-Datenbanken der App und der Cloud-Dienst Kaspersky Security Network eingesetzt. Im Lieferumfang von Anti-Virus sind folgende Komponenten enthalten:
  - **Schutz.** Der Schutz erkennt Bedrohungen in geöffneten Dateien, untersucht neue Apps und verhindert im Echtzeitmodus einen Virenbefall des Geräts.
  - **Untersuchung.** Wird bei Bedarf für das gesamte Dateisystem, nur für die installierten Anwendungen, die ausgewählte Datei oder den Ordner ausgeführt.
  - **Update.** Mit dieser Funktion können Sie neue Antiviren-Datenbanken für die App herunterladen.

- **Diebstahlschutz.** Schützt die Informationen auf einem Gerät vor unberechtigt Zugriff, falls das Gerät verloren geht oder gestohlen wird. Mit dieser Komponente können Sie die folgenden Befehle an das Gerät senden:
  - **Gerät orten.** Diese Funktion ermittelt die Koordinaten des Geräts.
  - **Alarmsignal erzeugen.** Das Gerät erzeugt einen lauten Alarmton.
  - **Löschen.** Diese Funktion löscht Unternehmensdaten, um vertrauliche Informationen des Unternehmens zu schützen.
- **Web-Filter.** Ermöglicht das Blockieren schädlicher Websites, die der Verbreitung von Schadcode dienen. Der Web-Filter blockiert außerdem gefälschte (Phishing-)Websites, die dazu dienen, vertrauliche Daten des Benutzers (beispielsweise Kennwörter für Online-Banking oder Zahlungssysteme) zu stehlen und auf die Finanzkonten des Benutzers zuzugreifen. Der Web-Filter untersucht Websites, bevor sie geöffnet werden. Dazu wird der Cloud-Dienst Kaspersky Security Network genutzt. Anhand der Ergebnisse der Untersuchung erlaubt der Web-Filter den Download von als sicher eingestuften Websites und blockiert als gefährliche eingestufte Websites. Der Web-Filter unterstützt ferner die Filterung von Websites nach Kategorien, die im Cloud-Dienst Kaspersky Security Network festgelegt sind. Dadurch kann der Administrator den Zugriff der Benutzer auf bestimmte Kategorien einschränken (beispielsweise auf Webseiten aus der Kategorie "Glücksspiel, Lotterien, Wetten" oder "Kommunikation im Internet").
- **Anwendungskontrolle.** Diese Komponente ermöglicht die Installation von empfohlenen und obligatorischen Anwendungen auf Ihrem Gerät über einen direkten Link zum Programmpaket oder einen Link zu Google Play. Mithilfe der Anwendungskontrolle können Sie verbotene Anwendungen deinstallieren, die der korporativen Sicherheit nicht entsprechen.
- **Übereinstimmungsüberprüfung.** Mit dieser Komponente können verwaltete Geräte auf die Einhaltung der Anforderungen an die Unternehmenssicherheit überprüft werden. Bestimmte Funktionen von Geräten, die dagegen verstoßen, können eingeschränkt werden.

Die Komponenten der App "Kaspersky Endpoint Security für Android" können Sie in Kaspersky Security Center Web Console und Cloud Console konfigurieren, indem Sie [die Einstellungen der Gruppenrichtlinien festlegen](#).

## Über die App "Kaspersky Security für iOS"

Die App "Kaspersky Security für iOS" schützt mobile Geräte vor Phishing und Schadsoftware.

Kaspersky Security für iOS bietet folgende Schlüsselfunktionen:

- **Web-Filter.** Ermöglicht das Blockieren schädlicher Websites, die der Verbreitung von Schadcode dienen. Der Web-Filter blockiert außerdem gefälschte (Phishing-)Websites, die dazu dienen, vertrauliche Daten des Benutzers (beispielsweise Kennwörter für Online-Banking oder Zahlungssysteme) zu stehlen und auf die Finanzkonten des Benutzers zuzugreifen. Der Web-Filter untersucht Websites, bevor sie geöffnet werden. Dazu wird der Cloud-Dienst Kaspersky Security Network genutzt. Anhand der Ergebnisse der Untersuchung erlaubt der Web-Filter den Download von als sicher eingestuften Websites und blockiert als gefährliche eingestufte Websites. Diese Komponente können Sie in Kaspersky Security Center Web Console [über die Einstellungen von Gruppenrichtlinien](#) konfigurieren.
- **Erkennung von Jailbreaks.** Wenn Kaspersky Security für iOS einen Jailbreak erkennt, wird eine kritische Nachricht angezeigt und Sie erhalten eine Problemmeldung.

## Über das Plug-in für Kaspersky Security for Mobile (Devices)

Das Plug-in für Kaspersky Security for Mobile (Devices) bietet eine Schnittstelle zur Verwaltung von mobilen Geräten und den darauf installierten mobilen Apps via Kaspersky Security Center Web Console und Cloud Console. Mithilfe des Plug-ins für Kaspersky Security for Mobile (Devices) können Sie folgende Aktionen ausführen:

- [Mobile Geräte mit Kaspersky Security Center verbinden](#).
- [Zertifikate von mobilen Geräten verwalten](#).
- [Konfiguration von Firebase Cloud Messaging](#) (nur für Android-Geräte).
- [Senden von Befehlen an Mobilgeräte](#) (nur für Android-Geräte).

Das Plug-in für Kaspersky Security for Mobile (Devices) kann bei der Konfiguration von Kaspersky Security Center Web Console installiert werden. Wenn Sie Kaspersky Security Center Cloud Console verwenden, müssen Sie dieses Plug-in nicht installieren. Weitere Informationen zu Bereitstellungsszenarien in verschiedenen Konsolentypen finden Sie im Abschnitt "[Bereitstellungsszenarien](#)".

## Über das Plug-in für Kaspersky Security for Mobile (Policies)

Mit dem Plug-in für Kaspersky Security for Mobile (Policies) können Sie mithilfe von Gruppenrichtlinien die Konfigurationseinstellungen für Geräte festlegen, die mit Kaspersky Security Center verbunden sind. Mithilfe des Plug-ins für Kaspersky Security for Mobile (Policies) können Sie folgende Aktionen ausführen:

- [Gruppenrichtlinien für den Schutz der mobilen Endgeräte erstellen](#).
- [Remote-Konfiguration der Einstellungen für die mobile App auf mobilen Benutzergeräten](#).
- Abrufen von Berichten und Statistiken über die Ausführung der mobilen App auf den mobilen Benutzergeräten.

Das Plug-in für Kaspersky Security for Mobile (Policies) kann bei der Konfiguration von Kaspersky Security Center Web Console installiert werden. Wenn Sie Kaspersky Security Center Cloud Console verwenden, müssen Sie dieses Plug-in nicht installieren. Weitere Informationen zu Bereitstellungsszenarien in verschiedenen Konsolentypen finden Sie im Abschnitt "[Bereitstellungsszenarien](#)".

## Hardware- und Softwarevoraussetzungen

Dieser Abschnitt nennt die Hardware- und Softwareanforderungen für den Computer des Administrators, der für die Installation des Plug-ins "Kaspersky Security for Mobile (Devices)" und des Plug-ins "Kaspersky Security for Mobile (Policies)" in Kaspersky Security Center Web Console und Cloud Console verwendet wird, sowie die Hardware- und Softwareanforderungen für die mobilen Apps.

### Hardware- und Softwareanforderungen für den Computer des Administrators

Um das Plug-in für Kaspersky Security for Mobile (Devices) und das Plug-in für Kaspersky Security for Mobile (Policies) zu installieren, muss der Computer des Administrators die Hardwarevoraussetzungen von Kaspersky Security Center erfüllen. Weitere Informationen zu den Hardware- und Softwarevoraussetzungen von Kaspersky Security Center finden Sie hier:

- Wenn Sie Kaspersky Security Center Web Console verwenden, lesen Sie bitte die [Hilfe zu Kaspersky Security Center](#).
- Wenn Sie Kaspersky Security Center Cloud Console verwenden, lesen Sie bitte die [Hilfe zu Kaspersky Security Center Cloud Console](#).

Um das Plug-in für Kaspersky Security for Mobile (Devices) und das Plug-in für Kaspersky Security for Mobile (Policies) in Kaspersky Security Center Web Console verwenden zu können, muss Kaspersky Security Center Web Console auf dem Computer des Administrators installiert sein.

Um das Plug-in für Kaspersky Security for Mobile (Devices) und das Plug-in für Kaspersky Security for Mobile (Policies) in Kaspersky Security Center Cloud Console verwenden zu können, müssen Sie ein Konto in Kaspersky Security Center Cloud Console erstellen. Nähere Informationen zur Erstellung eines Kontos finden Sie in der [Hilfe zu Kaspersky Security Center Cloud Console](#).

Die App "Kaspersky Endpoint Security für Android" kann auch als Bestandteil der folgenden [externen EMM-Lösungen](#) verwendet werden:

- VMware AirWatch 9.3 und höher
- MobileIron 10.0 und höher
- IBM MaaS360 10.68 und höher
- Microsoft Intune 1908 und höher
- SOTI MobiControl 14.1.4 (1693) und höher

## Hardware und Softwareanforderungen an das mobile Gerät des Benutzers für die Installation der App "Kaspersky Endpoint Security für Android"

Für die App "Kaspersky Endpoint Security für Android" müssen folgende Hardware- und Softwarevoraussetzungen erfüllt sein:

- Smartphone oder Tablet mit einer Bildschirmgröße ab 320 x 480 Pixel
- 65 MB freier Speicherplatz im Geräte Hauptspeicher
- Android 5.0–12 (einschließlich Android 12L, mit Ausnahme der Go Edition)
- Prozessorarchitektur x86, x86-64, Arm5, Arm6, Arm7, Arm8

Die App kann nur im Geräte Hauptspeicher installiert werden.

## Hardware und Softwareanforderungen an das mobile Gerät des Benutzers für die Installation der App "Kaspersky Security für iOS"

Die App von Kaspersky Security besitzt folgende Hardwarevoraussetzungen:

- iPhone 6S und höher
- iPad Air 2 und höher

Die App von Kaspersky Security besitzt folgende Softwarevoraussetzungen:

- iOS 14.1 und höher
- iPadOS 14.1 und höher

Kaspersky Security für iOS funktioniert nicht ordnungsgemäß, wenn auf demselben Mobilgerät ein VPN-Client mit aktiver VPN-Verbindung ausgeführt wird.

## Bekannte Probleme und Besonderheiten

Kaspersky Endpoint Security für Android und Kaspersky Security für iOS haben einige bekannte Probleme, die für den Betrieb dieser Apps nicht kritisch sind.

### Bekannte Probleme von Kaspersky Security für iOS

- Kaspersky Security für iOS funktioniert nicht ordnungsgemäß, wenn auf demselben Mobilgerät ein VPN-Client mit aktiver VPN-Verbindung ausgeführt wird.

### Bekannte Probleme von Kaspersky Endpoint Security für Android

#### Bekannte Probleme beim Starten der Verwaltung für mobile Geräte in der Kaspersky Security Center Web Console

- Sie können die Komponente "Mobile Geräte verwalten" entweder während der Erstkonfiguration der Verwaltungskonsole auf MMC-Basis von Kaspersky Security Center (während der Ausführung des Schnellstartassistenten) oder später starten, [indem Sie den Ordner "Mobile Geräte verwalten"](#) in der Verwaltungskonsole anzeigen.

#### Bekannte Probleme bei der Installation von Apps

- Kaspersky Endpoint Security für Android kann nur in den Hauptspeicher des Geräts installiert werden.
- Auf Geräten mit Android 7.0 kann es beim Versuch, die Rechte des Administrators für Kaspersky Endpoint Security für Android in den Geräteeinstellungen zu deaktivieren, zu einem Absturz kommen, wenn für Kaspersky Endpoint Security für Android das Overlay über anderen Fenstern verboten ist. Das Problem hängt mit dem bekannten [Fehler in Android 7](#) zusammen.
- Die App Kaspersky Endpoint Security für Android auf Geräten mit Android 7.0 und höher unterstützt den Mehrfenster-Modus nicht.
- Kaspersky Endpoint Security für Android läuft nicht auf Chromebook-Geräten mit dem Betriebssystem Chrome.
- Kaspersky Endpoint Security für Android funktioniert nicht auf Geräten mit Android (Go Edition) als Betriebssystem.
- Bei der Verwendung von Kaspersky Endpoint Security für Android mit externen EMM-Systemen (z. B. VMWare AirWatch) sind nur die Komponenten "Anti-Virus" und "Web-Filter" verfügbar. Der Administrator kann die Einstellungen von Anti-Virus und Web-Filter in der Konsole des EMM-Systems anpassen. Dabei werden die



Benachrichtigungen über die App-Ausführung nur in der Benutzeroberfläche der App von Kaspersky Endpoint Security für Android angezeigt (Berichte).

## Bekannte Probleme beim Upgrade der App-Version

- Sie können Kaspersky Endpoint Security für Android nur auf eine neuere Version der App upgraden. Ein Downgrade zu einer älteren Version von Kaspersky Endpoint Security für Android ist nicht möglich.

## Bekannte Probleme bei der Ausführung von Anti-Virus

- Aufgrund von technischen Beschränkungen kann Kaspersky Endpoint Security für Android Dateien mit einer Größe von mehr als 2 GB nicht untersuchen. Während der Untersuchung überspringt die App solche Dateien, und Sie werden nicht benachrichtigt, wenn solche Dateien übersprungen werden.
- Um das Gerät zusätzlich auf neue Bedrohungen untersuchen zu können, über die noch keine Informationen in den Antiviren-Datenbanken vorhanden sind, muss die Nutzung von Kaspersky Security Network aktiviert werden. *Kaspersky Security Network (KSN)* ist eine Infrastruktur von Cloud-Diensten, die Zugriff auf eine aktuelle Wissensdatenbank von Kaspersky bietet. Diese Datenbank enthält Informationen zur Reputation von Dateien, Webressourcen und Programmen. Für die Nutzung von KSN benötigt das mobile Gerät Internetzugang.
- In einigen Fällen kann auf mobilen Geräten die Aktualisierung der Antiviren-Datenbanken vom Administrationsserver fehlschlagen. Führen Sie in diesem Fall die Update-Aufgabe für die Antiviren-Datenbanken auf dem Administrationsserver aus.
- Auf einigen Geräten findet Kaspersky Endpoint Security für Android keine Geräte, die über USB OTG angeschlossen sind. Auf solchen Geräten kann keine Untersuchung auf Viren durchgeführt werden.
- Auf Geräten mit Android 11.0 oder höher muss der Nutzer die Berechtigung "Zugriff auf alle Dateien" erteilen.
- Auf Geräten mit Android 7.0 und höher wird das Fenster der Zeitplan-Einstellungen für den Start der Untersuchung auf Viren möglicherweise nicht korrekt angezeigt (Steuerelemente werden nicht angezeigt). Das Problem hängt mit dem bekannten [Fehler in Android 7](#) zusammen.
- Auf Geräten mit Android 7.0 erkennt der Echtzeitschutz im erweiterten Modus keine Bedrohungen in Dateien, die auf einer externen SD-Karte gespeichert sind.
- Auf Geräten unter Android 6.0 erkennt Kaspersky Endpoint Security für Android nicht, wenn eine schädliche Datei in den Gerätespeicher geladen wird. Die schädliche Datei kann vom Anti-Virus beim Start der Datei oder während der Untersuchung des Geräts auf Viren erkannt werden. Das Problem hängt mit dem bekannten [Fehler in Android 6.0](#) zusammen. Um die Sicherheit des Geräts zu gewährleisten, wird empfohlen, den Start der Untersuchung auf Viren nach Zeitplan einzurichten.

## Bekannte Probleme bei der Ausführung von Web-Filter

- Der Web-Filter funktioniert auf Android-Geräten nur mit den Browsern Google Chrome (einschließlich der Funktion Custom Tabs), Huawei Browser und Samsung Internet Browser.
- Damit der Web-Filter ausgeführt werden kann, muss die Nutzung von Kaspersky Security Network aktiviert werden. Der Web-Filter blockiert Websites unter Berücksichtigung der KSN-Daten zur Reputation und Kategorie von Websites.
- Auf Geräten mit dem Betriebssystem Android 6.0 mit dem installierten Browser Google Chrome Version 51 oder früher kann der Web-Filter verbotene Websites nicht blockieren, wenn sie auf eine der folgenden Arten geöffnet wurden (das Problem ist mit einem bekannten Defekt in Google Chrome verbunden):

- Über die Ergebnisse einer Suchanfrage.
- Aus einer Liste mit Registerkarten.
- Aus dem Verlauf von Suchanfragen.
- Bei Verwendung der Funktion der Autovervollständigung von Webadressen.
- Beim Öffnen der Website in einer neuen Registerkarte in Google Chrome.
- Blockierte Websites können im Browser Google Chrome Version 50 oder früheren Versionen nicht gesperrt werden, wenn die Website aus den Ergebnissen einer Google-Suchanfrage geöffnet wird und die Funktion **"Registerkarten und Apps zusammenführen"** in der Browser-Konfiguration aktiviert ist. Problem im Zusammenhang mit bekannten [Fehlern in Google Chrome](#).
- Websites aus verbotenen Kategorien werden in Google Chrome eventuell nicht blockiert, wenn der Benutzer sie aus der App eines Drittanbieters heraus öffnet (z. B. aus einem IM-Client). Das Problem ist verbunden mit den Besonderheiten des Dienstes für erleichterte Bedienung mit der Funktion Chrome Custom Tabs.
- Die verbotenen Websites werden im Samsung Internet Browser eventuell nicht blockiert, wenn der Benutzer sie im Hintergrundmodus aus dem Kontextmenü oder aus der App eines Drittanbieters heraus öffnet (z. B. aus einem IM-Client).
- Für die Ausführung des Web-Filters muss Kaspersky Endpoint Security für Android als Dienst für erleichterte Bedienung installiert sein.
- Im Samsung Internet Browser können im Modus des Web-Filters **Nur aufgezählte Websites sind erlaubt** beim Neuladen der Seite eventuell erlaubte Websites blockiert werden. Die Websites werden blockiert, wenn der reguläre Ausdruck zusätzliche Parameter enthält (z. B. `^https?:\\\/example\.com\/pictures\/`). Es wird empfohlen, reguläre Ausdrücke ohne zusätzliche Parameter zu verwenden (z. B. beispielsweise `^https?:\\\/example\.com`).

## Bekannte Probleme bei der Ausführung von Diebstahlschutz

- Zur schnellen Übermittlung von Befehlen an Android-Geräte verwendet die App den Dienst Firebase Cloud Messaging (FCM). Werden die Einstellungen von FCM nicht angepasst, so werden die Befehle nur während der Synchronisierung des Geräts mit Kaspersky Security Center nach dem Zeitplan übermittelt, der in der Richtlinie festgelegt wurde (z. B. alle 24 Stunden).
- Um das Gerät sperren zu können, muss Kaspersky Endpoint Security für Android als Geräteadministrator installiert sein.
- Auf Geräten mit dem Betriebssystem Android 7.0 und höher muss Kaspersky Endpoint Security für Android als Dienst für erleichterte Bedienung installiert sein, um das Gerät sperren zu können.
- Auf einigen Geräten können die Befehle von Diebstahlschutz nicht ausgeführt werden, wenn das Gerät sich im Stromsparmodus befindet. Dieser Defekt wurde für Alcatel 5080X bestätigt.
- Um Geräte mit Android 10.0 und höher zu orten, muss der Benutzer die Berechtigung "Immer" für die Verwendung des Standorts erteilen.

## Bekannte Probleme bei der Ausführung von Anwendungskontrolle

- Für die Ausführung der Anwendungskontrolle muss Kaspersky Endpoint Security für Android als Dienst für erleichterte Bedienung installiert sein.

- Damit die Anwendungskontrolle (Kontrolle von App-Kategorien) ausgeführt werden kann, muss die Nutzung von Kaspersky Security Network aktiviert werden. Die Anwendungskontrolle ermittelt die App-Kategorie anhand der Daten, die in KSN verfügbar sind. Für die Nutzung von KSN benötigt das mobile Gerät Internetzugang. Um die Anwendungskontrolle zu verwenden, können Sie einzelne Apps zu Listen verbotener und erlaubter Anwendungen hinzufügen. In diesem Fall ist der Zugriff auf KSN nicht erforderlich.
- Es wird empfohlen, bei der Konfiguration der Anwendungskontrolle das Kontrollkästchen **System-Apps sperren** zu deaktivieren. Das Sperren von System-Apps kann zu Störungen im Betrieb des Geräts führen.

## Bekannte Probleme beim Anpassen der Zuverlässigkeit des Kennworts zum Entsperren des Geräts.

- Auf Geräten mit Android 10.0 oder später löst Kaspersky Endpoint Security die Anforderungen an die Zuverlässigkeit des Kennworts in einen der Systemwerte auf: Mittel oder Hoch.  
Wenn eine Kennwortlänge von 1 bis 4 Zeichen erforderlich ist, fordert die App den Benutzer auf, ein Kennwort mittlerer Stärke festzulegen. Dieses muss entweder numerisch (PIN) ohne wiederholte oder aufeinanderfolgende (z. B. 1234) Sequenzen oder alphanumerisch sein. PIN oder Kennwort müssen mindestens 4 Zeichen lang sein.  
Wenn eine Kennwortlänge von 5 oder mehr Zeichen erforderlich ist, fordert die App den Benutzer auf, ein Kennwort hoher Stärke festzulegen. Dieses muss entweder numerisch (PIN) ohne wiederholte oder aufeinanderfolgende Sequenzen oder alphanumerisch (Kennwort) sein. Die PIN muss mindestens 8 Zeichen lang sein, das Kennwort muss mindestens 6 Zeichen lang sein.
- Wenn auf Geräten mit Android 7.1.1 das Passwort zum Entsperren nicht den Anforderungen an die Unternehmenssicherheit entspricht (Übereinstimmungsüberprüfung), wird die System-App "Einstellungen" beim Versuch, das Passwort zum Entsperren in Kaspersky Endpoint Security für Android zu ändern, möglicherweise nicht ordnungsgemäß ausgeführt. Problem im Zusammenhang mit bekannten [Fehlern in Android 7.1.1](#). Verwenden Sie in diesem Fall nur die Systemanwendung "Einstellungen", um das Passwort zu ändern.
- Auf einigen Geräten mit Android 6.0 und höher kann bei der Eingabe des Passworts zum Entsperren ein Fehler auftreten, wenn die Daten auf dem Gerät verschlüsselt sind. Das Problem ist verbunden mit den Besonderheiten des Dienstes für erleichterte Bedienung in MIUI-Firmware.

## Bekannte Probleme mit dem Schutz der App vor der Deinstallation

- Kaspersky Endpoint Security für Android muss als Geräteadministrator installiert werden.
- Auf den Geräten unter Verwaltung des Betriebssystems Android 7.0 und höher muss zum Schutz der App vor dem Löschen Kaspersky Endpoint Security für Android als Dienst für erleichterte Bedienung installiert sein.
- Auf einigen Geräten von Xiaomi und Huawei funktioniert der Schutz von Kaspersky Endpoint Security für Android gegen die Deinstallation nicht. Das Problem wird durch Besonderheiten der Firmware für MIUI 7 und 8 auf Xiaomi und der EMUI-Firmware auf Huawei verursacht.

## Bekannte Probleme bei der Konfiguration von Gerätebeschränkungen

- Auf Geräten mit Android 10.0 oder höher wird das Verbot der Verwendung von WLAN-Netzwerken nicht unterstützt.
- Auf Geräten mit Android 10.0 oder höher kann die Nutzung der Kamera nicht vollständig verboten werden.
- Auf Geräten mit dem Betriebssystem Android 11 und höher muss Kaspersky Endpoint Security für Android als Dienst für erleichterte Bedienung installiert sein. Der Assistent für die Erstkonfiguration von Kaspersky

Endpoint Security für Android ermöglicht dem Benutzer, die App als Bedienungshilfe zu installieren. Der Benutzer kann diesen Schritt überspringen oder den Dienst in den Einstellungen des Geräts später deaktivieren. In einem solchen Fall können Sie die Verwendung der Kamera nicht einschränken.

## Bekannte Probleme beim Senden von Befehlen an mobile Geräte

- Wenn der Benutzer auf Geräten mit Android 12 oder höher die Berechtigung "Ungefährer Standort verwenden" erteilt hat, versucht die App "Kaspersky Endpoint Security für Android" zunächst, den genauen Standort des Geräts zu ermitteln. Gelingt dies nicht, wird der ungefähre Gerätestandort nur zurückgegeben, wenn er frühestens 30 Minuten zuvor empfangen wurde. Andernfalls schlägt der Befehl **Gerät orten** fehl.

## Bekannte Probleme mit bestimmten Geräten

- Auf bestimmten Geräten (zum Beispiel Huawei, Meizu und Xiaomi) müssen Sie Kaspersky Endpoint Security für Android die Berechtigung für Autostart erteilen oder das Programm manuell zur Liste der Apps hinzufügen, die beim Hochfahren des Betriebssystems gestartet werden. Wenn die App nicht zur Liste hinzugefügt wird, stellt Kaspersky Endpoint Security für Android nach dem Neustart des mobilen Geräts sämtliche Funktionen ein. Außerdem kann das Gerät nicht mit einem Befehl entsperrt werden, wenn es gesperrt wurde. Sie können das Gerät nur mithilfe des einmaligen Codes für die Freischaltung entsperren.
- Nach der Datenverschlüsselung und dem Neustart des Geräts verlangt Android auf einigen Geräten (z. B. Meizu, Asus) unter Android 6.0 und höher die Eingabe des Zahlencodes. Wenn der Benutzer ein Sperrmuster für das Entsperren verwendet, muss das Sperrmuster in einen Zifferncode übersetzt werden. Weitere Informationen zur Eingabe des Sperrmusters als Zahlencode finden Sie auf der Website des technischen Supports des Herstellers ihres mobilen Geräts. Das Problem ist verbunden mit den Besonderheiten des Dienstes für erleichterte Bedienung.
- Auf einigen Huawei-Geräten mit Android 5.X wird nach dem Festlegen von Kaspersky Endpoint Security für Android als Dienst für erleichterte Bedienung eine fehlerhafte Benachrichtigung über das Fehlen der entsprechenden Berechtigungen angezeigt. Um diese Benachrichtigung auszublenden, aktivieren Sie die App in den Geräteeinstellungen als geschützt.
- Auf einigen Huawei-Geräten mit Android 5.X und 6.X kann der Benutzer bei aktiviertem Stromsparmodus für Kaspersky Endpoint Security für Android die Ausführung der App selbständig beenden. Das Gerät des Benutzers ist dabei nicht geschützt. Das Problem ist verbunden mit den Besonderheiten der Software von Huawei. Um den Schutz des Geräts wiederherzustellen, starten Sie Kaspersky Endpoint Security für Android manuell. Es wird empfohlen den Stromsparmodus für Kaspersky Endpoint Security für Android in den Geräteeinstellungen zu deaktivieren.
- Auf Huawei-Geräten mit der Firmware EMUI unter Android 7.0 kann der Benutzer die Benachrichtigung über den Schutzstatus von Kaspersky Endpoint Security für Android ausblenden. Das Problem ist verbunden mit den Besonderheiten der Software von Huawei.
- Auf einigen Xiaomi-Geräten wird der Benutzer aufgefordert, nicht den PIN-Code, sondern das Passwort zum Entsperren des Bildschirms zu ändern, wenn die Kennwortlänge in der Richtlinie auf länger als 5 Zeichen festgelegt wurde. Es ist nicht möglich, einen PIN-Code mit mehr als 5 Zeichen festzulegen. Das Problem ist verbunden mit den Besonderheiten der Software von Xiaomi.
- Auf Xiaomi-Geräten mit der Firmware MIUI unter Android 6.0 ist das Symbol von Kaspersky Endpoint Security für Android in der Statuszeile evtl. ausgeblendet. Das Problem ist verbunden mit den Besonderheiten der Software von Xiaomi. Es wird empfohlen, die Anzeige von Benachrichtigungssymbolen in den Benachrichtigungseinstellungen zu erlauben.
- Auf einigen Nexus-Geräten unter Android 6.0.1 ist es während der Ausführung des Schnellstartassistenten für Kaspersky Endpoint Security für Android nicht möglich, die erforderlichen Rechte für eine ordnungsgemäße App-Funktion zu erteilen. Das Problem ist mit einem bekannten Defekt im Security Patch für Android von

Google verbunden. Für die ordnungsgemäße App-Funktion müssen die erforderlichen Rechte in den Einstellungen des Geräts manuell erteilt werden.

- Auf einigen Samsung-Geräten mit dem Betriebssystem Android 7.0 und höher kann das Gerät gesperrt werden, wenn der Benutzer versucht, das Gerät mit einer nicht unterstützten Methode zu entsperren (z. B. mit Sperrmuster), und folgende Bedingungen erfüllt sind: Der Schutz vor Deinstallation für Kaspersky Endpoint Security für Android ist aktiviert und die Anforderungen an die Stärke des Kennworts zum Entsperren des Geräts sind festgelegt. Zum Entsperren muss ein bestimmter Befehl an das Gerät gesendet werden.
- Auf einigen Samsung-Geräten ist es nicht möglich, die Verwendung von Fingerabdrücken zum Entsperren des Bildschirms zu verbieten.
- Auf einigen Samsung-Geräten funktioniert Web-Filter nicht, wenn das Gerät mit einem 3G/4G-Netzwerk verbunden ist, auf dem Gerät der Stromsparmodus aktiviert ist und die Hintergrunddaten eingeschränkt sind. Es wird empfohlen, die Funktion zur Einschränkung von Hintergrundprozessen in den Stromspareinstellungen zu deaktivieren.
- Außerdem verbietet Kaspersky Endpoint Security für Android auf einigen Samsung-Geräten, auf denen das Kennwort zum Entsperren nicht den Anforderungen an die Unternehmenssicherheit entspricht, die Nutzung der Fingerabdrücke für das Entsperren des Bildschirms nicht.
- Bei einigen Geräten der Marken Honor und Huawei können Sie die Verwendung von Bluetooth nicht einschränken. Wenn Kaspersky Endpoint Security für Android versucht, die Verwendung von Bluetooth einzuschränken, zeigt das Betriebssystem eine Benachrichtigung mit den folgenden Optionen an: Ablehnen oder Zulassen. Auf diese Weise kann der Benutzer die Einschränkung ablehnen und weiterhin Bluetooth verwenden.
- Auf Blackview-Geräten kann der Benutzer den Speicher der App "Kaspersky Endpoint Security für Android" löschen. Als Folge werden der Geräteschutz und die Geräteverwaltung deaktiviert, alle festgelegten Einstellungen werden wirkungslos und die App von Kaspersky Endpoint Security für Android wird aus den Diensten für erleichterte Bedienung entfernt. Dies liegt daran, dass die Geräte dieses Anbieters die angepasste App "Letzte Anwendungen" enthalten, die mit erhöhten Rechten ausgestattet ist. Diese App kann die Einstellungen von Kaspersky Endpoint Security für Android außer Kraft setzen und kann nicht ersetzt werden, da sie Teil des Android-Betriebssystems ist.
- Auf einigen Geräten mit Android 11 stürzt die App von Kaspersky Endpoint Security für Android sofort nach dem Start ab. Das Problem hängt mit dem bekannten [Fehler in Android 11](#) zusammen.

## Bereitstellung einer Lösung zur Verwaltung mobiler Geräte in der Kaspersky Security Center Web Console oder Cloud Console

Um mobile Geräte mithilfe von Kaspersky Security Center Web Console oder Cloud Console zu verwalten, müssen Sie eine Lösung für die Verwaltung mobiler Geräte bereitstellen.

### Bereitstellungsszenarien

#### Bereitstellung in der Kaspersky Security Center Web Console

Die Bereitstellung der Verwaltungslösung für mobile Geräte in der Kaspersky Security Center Web Console umfasst die folgenden Schritte:

- 1 [Vorbereitung der Kaspersky Security Center Web Console für die Bereitstellung](#)
- 2 [Bereitstellung der Verwaltungs-Plug-ins](#)
- 3 [Mobile App bereitstellen](#)
- 4 [\(Optional, nur für Android\) Konfigurierung des Informationsaustauschs mit Firebase Cloud Messaging](#)

Es wird empfohlen, diesen Schritt auszuführen, um die rechtzeitige Zustellung von Befehlen an mobile Geräte und die erzwungene Synchronisierung im Falle einer Änderung von Richtlinieneinstellungen sicherzustellen.

## Bereitstellung in der Kaspersky Security Center Cloud Console

Die Bereitstellung der Lösung zur Verwaltung mobiler Geräte in der Kaspersky Security Center Cloud Console umfasst die folgenden Schritte:

- 1 [Vorbereitung der Kaspersky Security Center Cloud Console für die Bereitstellung](#)
- 2 [Mobile App bereitstellen](#)
- 3 [\(Optional, nur für Android\) Konfigurierung des Informationsaustauschs mit Firebase Cloud Messaging](#)

Es wird empfohlen, diesen Schritt auszuführen, um die rechtzeitige Zustellung von Befehlen an mobile Geräte und die erzwungene Synchronisierung im Falle einer Änderung von Richtlinieneinstellungen sicherzustellen.

## Vorbereitung der Kaspersky Security Center Web Console und Cloud Console für die Bereitstellung

Dieser Abschnitt enthält Anweisungen zur Vorbereitung der Kaspersky Security Center Web Console und der Cloud Console für die Bereitstellung.

## Administrationsserver für die Anbindung von mobilen Endgeräten anpassen

Damit die mobilen Geräte eine Verbindung zum Administrationsserver herstellen können, müssen vor der Installation der App "Kaspersky Endpoint Security für Android" oder "Kaspersky Security für iOS" auf mobilen Geräten die Verbindungseinstellungen der mobilen Geräte in den Administrationsserver-Eigenschaften festgelegt werden.

*So legen Sie die Einstellungen des Administrationsservers für die Verbindung mit mobilen Geräten fest:*

1. Starten Sie die Komponente "Mobile Geräte verwalten" im Administrationsserver.

Sie können die Komponente "Mobile Geräte verwalten" entweder während der Erstkonfiguration der Verwaltungskonsole auf MMC-Basis von Kaspersky Security Center (während der Ausführung des Schnellstartassistenten) oder später starten, [indem Sie den Ordner "Mobile Geräte verwalten"](#) in der Verwaltungskonsole anzeigen.

2. Klicken Sie im Hauptfenster von Kaspersky Security Center Web Console oder Cloud Console auf **Einstellungen** (⚙️).

Das Eigenschaftfenster des Administrationsservers wird geöffnet.

3. Konfigurieren Sie die Ports des Administrationsservers, die von den mobilen Geräten verwendet werden sollen:

a. Wählen Sie den Ports Abschnitt **Zusätzliche Ports**.

b. Aktivieren Sie den Schalter **Port für mobile Endgeräte öffnen**.

c. Geben Sie im Feld **Port zur Synchronisierung mobiler Geräte** den Port an, über den mobile Geräte mit dem Administrationsserver verbunden werden sollen.

Als Standard wird Port 13292 verwendet.

Wenn der Schalter **Port für mobile Endgeräte öffnen** deaktiviert ist oder ein ungültiger Verbindungsport angegeben wurde, können mobile Geräte keine Verbindung mit dem Administrationsserver herstellen.

d. Geben Sie im Feld **Port zur Aktivierung von mobilen Geräten** den Port an, über den sich mobile Geräte mit dem Administrationsserver verbinden sollen, um die mobile App zu aktivieren.

Als Standard wird Port 17100 verwendet.

Wenn Sie einen falschen Verbindungsport angeben, können die Benutzer von mobilen Geräten die mobile App nicht über den Administrationsserver aktivieren.

4. Bearbeiten Sie bei Bedarf das Zertifikat, das von Mobilgeräten für die Verbindung mit dem Administrationsserver verwendet werden soll.

Standardmäßig verwendet der Administrationsserver das Zertifikat, welches bei der Installation des Administrationsservers erstellt wurde. Wenn Sie möchten, ersetzen Sie das über den Administrationsserver ausgestellte Zertifikat durch ein anderes Zertifikat oder stellen Sie das über den Administrationsserver ausgestellte Zertifikat erneut aus.

So bearbeiten Sie das Zertifikat:

a. Wählen Sie den Abschnitt **Zertifikate**.

b. Legen Sie die gewünschten Einstellungen fest.

Nähere Informationen über Zertifikate finden Sie in der [Hilfe zu Kaspersky Security Center](#).

5. Klicken Sie auf die Schaltfläche **Speichern**, um die vorgenommenen Änderungen zu speichern und das Eigenschaftfenster des Administrationsservers zu verlassen.

Nach der Konfiguration der Verbindungseinstellungen für mobile Geräte können Sie die App "Kaspersky Endpoint Security für Android" oder "Kaspersky Security für iOS" auf den mobilen Geräten installieren und diese unter Verwendung der festgelegten Einstellungen mit dem Administrationsserver verbinden.

## Administrationsgruppe erstellen

[Gruppenrichtlinien](#) dienen der zentralen Konfiguration der Apps "Kaspersky Endpoint Security für Android" und "Kaspersky Security für iOS", die auf den mobilen Geräten der Benutzer installiert sind.

Um eine Richtlinie auf eine Gerätegruppe anzuwenden, sollte vor der Installation von mobilen Anwendungen auf den Geräten der Benutzer für die entsprechenden Geräte im Ordner **Verwaltete Geräte** eine separate Administrationsgruppe erstellt werden.



Es wird empfohlen, nach dem Erstellen der Administrationsgruppe die [automatische Verschiebung von Geräten in diese Gruppe anzupassen](#), auf denen Sie die Apps installieren wollen. Danach müssen mithilfe der Gruppenrichtlinie gemeinsame Einstellungen für alle Geräte festgelegt werden.

*So erstellen Sie eine Administrationsgruppe:*

1. Wählen Sie im Hauptfenster von Kaspersky Security Center Web Console oder Cloud Console **GERÄTE > GRUPPENHIERARCHIE**.
2. Wählen Sie in der Administrationsgruppenstruktur die Administrationsgruppe aus, die die neue Administrationsgruppe aufnehmen soll.
3. Klicken Sie auf die Schaltfläche **Hinzufügen**.
4. Geben Sie im nächsten Fenster **Name der neuen Administrationsgruppe** einen Namen für die Gruppe ein und klicken Sie dann auf die Schaltfläche **Hinzufügen**.

Eine neue Administrationsgruppe mit dem angegebenen Namen wird in der Hierarchie der Administrationsgruppen angezeigt.

## Regel für das automatische Verschieben von Geräten in eine Administrationsgruppe erstellen

Wenn die App "Kaspersky Endpoint Security für Android" oder "Kaspersky Security für iOS" auf mobilen Geräten installiert ist, wird sie auf der Seite **ENTDECKUNG UND SOFTWAREVERTEILUNG > NICHT ZUGEORDNETE GERÄTE** in Kaspersky Security Center Web Console oder Cloud Console angezeigt. Um neu angeschlossene Geräte zu verwalten, können Sie diese [manuell in eine Administrationsgruppe verschieben](#) oder eine Regel für das automatische Verschieben von Geräten in Administrationsgruppen erstellen.

*So erstellen Sie eine Regel für das automatische Verschieben von mobilen Geräten in Administrationsgruppen:*

1. Wählen Sie im Hauptfenster von Kaspersky Security Center Web Console oder Cloud Console die Option **ENTDECKUNG UND SOFTWAREVERTEILUNG > SOFTWAREVERTEILUNG UND ZUWEISUNG > VERSCHIEBUNGSREGELN**.
2. Klicken Sie im sich öffnenden Fenster **Neue Regel** auf die Schaltfläche **Hinzufügen**.
3. Geben Sie im Feld **Regelname** den Regelnamen an.
4. Geben Sie im Feld **Administrationsgruppe** an, welcher Administrationsgruppe die Geräte nach der Installation der App zugeordnet werden sollen.
5. Wählen Sie im Abschnitt **Regel anwenden** die Variante **Wird einmal pro Gerät ausgeführt** aus.
6. Aktivieren Sie das Kontrollkästchen **Nur Geräte verschieben, die sich nicht in einer Administrationsgruppe befinden**, damit durch die Anwendung dieser Regel mobile Geräte, die bereits anderen Administrationsgruppen zugeordnet wurden, nicht verschoben werden.
7. Aktivieren Sie das **Kontrollkästchen Regel** aktivieren, um die Regel sofort nach der Erstellung anzuwenden. Sie können die Regel später jederzeit mit dem Schalter auf der Seite **VERSCHIEBUNGSREGELN** aktivieren.
8. Wählen Sie **REGELBEDINGUNGEN > Anwendung** und gehen Sie wie folgt vor:
  - a. Aktivieren Sie den Schalter **Version des Betriebssystems**.



b. Wählen Sie in der angezeigten Liste der Betriebssysteme den Punkt **Android** oder **iOS** aus.

Die Regel wird auf die entsprechenden Geräte angewendet. Sie müssen mindestens eine Bedingung angeben, um eine Regel zu erstellen.

9. Klicken Sie auf **Speichern**, um die Regel zu erstellen.

Die neu erstellte Regel wird auf der Seite **VERSCHIEBUNGSREGELN** angezeigt. Kaspersky Security Center ordnet alle neu verbundenen Geräte gemäß dieser Regel der ausgewählten Administrationsgruppe zu.

Nähere Informationen über die Verwaltung von Administrationsgruppen und über den Umgang mit nicht zugeordneten Geräten finden Sie hier:

- Wenn Sie Kaspersky Security Center Web Console verwenden, lesen Sie bitte die [Hilfe zu Kaspersky Security Center](#).
- Wenn Sie Kaspersky Security Center Cloud Console verwenden, lesen Sie bitte die [Hilfe zu Kaspersky Security Center Cloud Console](#).

## Bereitstellung der Verwaltungs-Plug-ins

Um mobile Geräte via Kaspersky Security Center Web Console zu verwalten, müssen die folgenden Verwaltungs-Plug-ins installiert sein:

- [Plug-in für Kaspersky Security for Mobile \(Devices\)](#)
- [Plug-in für Kaspersky Security for Mobile \(Policies\)](#)

Wenn Sie Kaspersky Security Center Cloud Console verwenden, müssen Sie die Verwaltungs-Plug-ins nicht installieren. Sie müssen lediglich ein Konto in Kaspersky Security Center Cloud Console erstellen. Nähere Informationen zur Erstellung eines Kontos finden Sie in der [Hilfe zu Kaspersky Security Center Cloud Console](#).

Sie können die Verwaltungs-Plug-ins auf folgende Arten installieren:

- Mithilfe des Schnellstartassistenten von Kaspersky Security Center Web Console.  
Kaspersky Security Center Web Console fordert Sie nach der Installation des Administrationsservers bei der ersten Verbindung automatisch auf, den Schnellstartassistenten auszuführen. Sie können den Schnellstartassistenten aber auch jederzeit manuell starten.  
Nähere Informationen zum Schnellstartassistenten für Kaspersky Security Center finden Sie in der [Hilfe zu Kaspersky Security Center](#).
- [Mithilfe der Liste mit verfügbaren Programmpaketen in Kaspersky Security Center Web Console](#).  
Die Liste der verfügbaren Pakete des Lieferumfangs wird automatisch aktualisiert, wenn neue Versionen von Kaspersky-Programmen veröffentlicht werden.
- Laden Sie die Programmpakete von einer externen Quelle herunter und [fügen Sie Verwaltungs-Plug-ins zu Kaspersky Security Center Web Console hinzu](#).  
Die Programmpakete der Verwaltungs-Plug-ins können z. B. von der Kaspersky-Website heruntergeladen werden.

## Verwaltungs-Plug-ins aus der Liste der verfügbaren Programmpakete installieren

*So installieren Sie die Verwaltungs-Plug-ins:*

1. Wählen Sie im Hauptfenster von Kaspersky Security Center Web Console die Option **KONSOLENEINSTELLUNGEN > WEB-PLUG-INS** aus.

2. Klicken Sie auf die Schaltfläche **Hinzufügen**.

Eine Liste der aktuellen Versionen von Kaspersky-Programmen wird angezeigt.

3. Installieren Sie die Verwaltungs-Plug-ins:

a. Klicken Sie in der Liste der verfügbaren Apps auf den Abschnitt **Mobile Geräte**, um ihn zu erweitern.

b. Wählen Sie **Kaspersky Security for Mobile (Devices)** aus und klicken Sie dann auf **Plug-in installieren**.

c. Wählen Sie **Kaspersky Security for Mobile (Policies)** aus und klicken Sie dann auf **Plug-in installieren**.

Die Programmpakete werden heruntergeladen und die Plug-ins werden installiert. Sobald alle Plug-ins installiert und zu Kaspersky Security Center Web Console hinzugefügt wurden, wird ein Bestätigungsfenster angezeigt.

## Verwaltungs-Plug-ins aus dem Paket des Lieferumfangs installieren

Sie können das Programmpaket von der Kaspersky-Website herunterladen.

*So installieren Sie das Plug-in für Kaspersky Security for Mobile (Devices) aus dem Programmpaket:*

1. Kopieren Sie die Dateien `plugin.zip` und `signature.txt` aus dem Archiv `on_prem_ksm_devices_xx.x.x.x.zip` des Programmpakets in die Administrator-Workstation.

2. Wählen Sie im Hauptfenster von Kaspersky Security Center Web Console die Option **KONSOLENEINSTELLUNGEN > WEB-PLUG-INS** aus.

3. Klicken Sie auf **Aus Datei hinzufügen**.

4. Klicken Sie im sich öffnenden Fenster **Aus Datei hinzufügen** auf **ZIP-Datei hochladen** und finden Sie `plugin.zip`.

5. Klicken Sie auf **Signatur hochladen** und finden Sie `signature.txt`.

6. Klicken Sie auf die Schaltfläche **Hinzufügen**.

Das Plug-in für Kaspersky Security for Mobile (Devices) wird installiert und zu Kaspersky Security Center Web Console hinzugefügt.

*So installieren Sie das Plug-in für Kaspersky Security for Mobile (Policies) aus dem Programmpaket:*

1. Kopieren Sie die Dateien `plugin.zip` und `signature.txt` aus dem Archiv `on_prem_ksm_policies_xx.x.x.x.zip` des Programmpakets in die Administrator-Workstation.

2. Wählen Sie im Hauptfenster von Kaspersky Security Center Web Console die Option **KONSOLEN-EINSTELLUNGEN > WEB-PLUG-INS** aus.

3. Klicken Sie auf **Aus Datei hinzufügen**.

4. Klicken Sie im sich öffnenden Fenster **Aus Datei hinzufügen** auf **ZIP-Datei hochladen** und finden Sie `plugin.zip`.

5. Klicken Sie auf **Signatur hochladen** und finden Sie `signature.txt`.

6. Klicken Sie auf die Schaltfläche **Hinzufügen**.

Das Plug-in für Kaspersky Security for Mobile (Policies) wird installiert und zu Kaspersky Security Center Web Console hinzugefügt.

Sie können sich davon überzeugen, dass die Verwaltungs-Plug-ins installiert wurden, indem Sie sich die Liste der installierten Plug-ins auf der Seite **KONSOLEN-EINSTELLUNGEN > WEB-PLUG-INS** ansehen.

## Mobile App bereitstellen

Um mobile Geräte in Kaspersky Security Center Web Console oder Cloud Console zu verwalten, müssen Sie die App "Kaspersky Endpoint Security für Android" oder "Kaspersky Security für iOS" auf den mobilen Geräten bereitstellen. Die Apps können über Kaspersky Security Center Web Console oder Cloud Console auf mobilen Geräten bereitgestellt werden.

## Bereitstellung der mobilen App über Kaspersky Security Center Web Console oder Cloud Console

Die mobile App wird auf den mobilen Geräten der Benutzer bereitgestellt, deren Benutzerkonten zu Kaspersky Security Center hinzugefügt wurden. Weitere Informationen zu Benutzerkonten im Kaspersky Security Center:

- Wenn Sie Kaspersky Security Center Web Console verwenden, lesen Sie bitte die [Hilfe zu Kaspersky Security Center](#).
- Wenn Sie Kaspersky Security Center Cloud Console verwenden, lesen Sie bitte die [Hilfe zu Kaspersky Security Center Cloud Console](#).

Sie können das Plug-in "Kaspersky Security for Mobile (Devices)" verwenden, um die App über Kaspersky Security Center Web Console und Cloud Console zu installieren, indem Sie einen Installationslink an ein mobiles Gerät senden.

- Auf einem Android-Gerät erhält der Benutzer einen Google Play-Link für den Download der App "Kaspersky Endpoint Security für Android". Die Installation wird mit der für die Android-Plattform typischen Methode ausgeführt. Nach der App-Installation muss der Benutzer [die erforderlichen Berechtigungen erteilen](#).

Einige Huawei- und Honor-Geräte nutzen keine Google-Dienste und haben deshalb keinen Zugriff auf Apps in Google Play. Wenn Benutzer von Huawei- und Honor-Geräten die App nicht über Google Play installieren können, weisen Sie sie an, die App über die Huawei App Gallery zu installieren.

- Auf einem iOS-Gerät erhält der Benutzer einen App Store-Link für den Download der App "Kaspersky Security für iOS". Die Installation wird mit der für die iOS-Plattform typischen Methode ausgeführt.

Bevor Sie ein iOS-Gerät verbinden, müssen Sie die Adresse von Kaspersky Security Center an den Gerätebenutzer senden. Dies dient der Überprüfung der Verbindungssicherheit. Der Benutzer sieht diese Adresse während der App-Installation und kann die Verbindung trennen, falls die angezeigte Adresse nicht mit der von Ihnen gesendeten Adresse übereinstimmt.

Der Link enthält die folgenden Daten:

- Synchronisierungseinstellungen für Kaspersky Security Center
- Allgemeines Zertifikat

*Um die App auf einem mobilen Gerät bereitzustellen:*

1. Starten Sie den Assistenten für die Verbindung eines mobilen Gerätes:

- Wählen Sie im Hauptfenster von Kaspersky Security Center Web Console oder Cloud Console **GERÄTE > MOBIL > GERÄTE** aus und klicken Sie dann auf **Hinzufügen**.
- Wählen Sie im Hauptfenster der Kaspersky Security Center Web Console oder Cloud Console **BENUTZER & ROLLEN > BENUTZER** aus. Klicken Sie auf den Namen des Benutzers oder der Benutzergruppe, an den bzw. die Sie den Link zum Verbinden eines mobilen Gerätes senden möchten, und wählen Sie dann **GERÄTE**. Klicken Sie auf **Mobiles Gerät hinzufügen**. Wiederholen Sie in diesem Fall den Schritt 3.

Folgen Sie dem Assistenten, indem Sie auf die Schaltfläche **Weiter** klicken.

2. Auswahl des Betriebssystems der Geräte, die Sie hinzufügen möchten:

- **Android**
- **iOS und iPadOS**

3. Wählen Sie die Benutzer und Benutzergruppen aus, an die Sie den Link zum Verbinden eines mobilen Gerätes senden möchten.

4. Auswahl der E-Mail-Adressen, an die der Link gesendet wird:

- **Alle E-Mail-Adressen**
- **Primäre E-Mail-Adresse**
- **Alternative E-Mail-Adresse**
- **Andere E-Mail-Adresse**

Wenn Sie diese Option auswählen, geben Sie unten die E-Mail-Adresse an.

5. Die Linkzusammenfassung wird angezeigt.

Stellen Sie sicher, dass alle Parameter des Links korrekt sind, und klicken Sie dann auf **Senden**.

6. Es öffnet sich ein Fenster mit der Bestätigung, dass der Link zum Hinzufügen eines mobilen Gerätes gesendet wurde.

Klicken Sie auf **OK**, um den Assistenten abzuschließen.

Wenn der Benutzer die App "Kaspersky Endpoint Security für Android" oder "Kaspersky Security für iOS" installiert, wird das Benutzergerät auf der Registerkarte **GERÄTE > MOBIL > GERÄTE** in Web Console oder Cloud Console angezeigt. Nachdem die App auf den Benutzergeräten installiert ist, können Sie die Einstellungen für Geräte und Apps über [Gruppenrichtlinien](#) konfigurieren. Sie können ferner [Befehle an mobile Geräte senden](#) (nur für Android), um die Daten bei Verlust oder Diebstahl der Geräte zu schützen.

## Mobile App aktivieren

Eine Lizenz für Kaspersky Security Center kann sich auf unterschiedliche Funktionalitätsgruppen beziehen. Damit alle Funktionen der App "Kaspersky Endpoint Security für Android" und "Kaspersky Security für iOS" wie vorgesehen funktionieren, muss die von Ihrem Unternehmen für Kaspersky Security Center erworbene Lizenz auch für die Funktionalität **Mobile Geräte verwalten** gelten. Die Funktionalität **Mobile Geräte verwalten** ist für die Verbindung der mobilen Geräte mit Kaspersky Security Center sowie ihre Verwaltungen vorgesehen.

Ausführliche Informationen zur Lizenzverwaltung von Kaspersky Security Center und zu den Lizenzverwaltungsoptionen:

- Wenn Sie Kaspersky Security Center Web Console verwenden, lesen Sie bitte die [Hilfe zu Kaspersky Security Center](#).
- Wenn Sie Kaspersky Security Center Cloud Console verwenden, lesen Sie bitte die [Hilfe zu Kaspersky Security Center Cloud Console](#).

Die Aktivierung der App "Kaspersky Endpoint Security für Android" oder "Kaspersky Security für iOS" auf einem mobilen Gerät erfolgt durch die Bereitstellung von Informationen über eine gültige Lizenz für die App. Die Lizenzinformationen werden zusammen mit der Richtlinie bei der Synchronisierung Ihres Geräts mit Kaspersky Security Center an das mobile Gerät übermittelt.

Wenn die mobile App nicht innerhalb von 30 Tagen nach der Installation auf dem mobilen Gerät aktiviert wird, wechselt die App automatisch in den eingeschränkten Funktionsmodus. In diesem Modus haben die meisten Komponenten keine Funktion. Beim Wechsel in den eingeschränkten Funktionsmodus stellt die App die automatische Synchronisierung mit Kaspersky Security Center ein. Sollte die App nach der Installation nicht innerhalb von 30 Tagen aktiviert worden sein, so muss das Gerät manuell mit Kaspersky Security Center synchronisiert werden.

Wenn Kaspersky Security Center in Ihrem Unternehmen nicht bereitgestellt wird oder für mobile Geräte nicht verfügbar ist, können Benutzer die mobile App manuell auf ihren Geräten aktivieren.

*Um die mobile App zu aktivieren:*

1. Öffnen Sie das Fenster mit den Richtlinieneigenschaften:

- Wählen Sie im Hauptfenster der Kaspersky Security Center Web Console oder Cloud Console **GERÄTE > RICHTLINIEN & PROFILE** aus. Klicken Sie in der sich öffnenden Liste der Gruppenrichtlinien auf den Namen der Richtlinie, die Sie konfigurieren möchten.
- Wählen Sie im Hauptfenster der Kaspersky Security Center Web Console oder Cloud Console **GERÄTE > MOBIL > GERÄTE** aus. Klicken Sie auf das mobile Gerät, das unter die Richtlinie fällt, die Sie konfigurieren möchten, und wählen Sie anschließend die Richtlinie auf der Registerkarte **AKTIVE RICHTLINIEN UND RICHTLINIENPROFILE** aus.

2. Wählen Sie auf der Seite mit den Richtlinieneigenschaften **PROGRAMMEINSTELLUNGEN > Lizenzen** aus.

3. Wählen Sie über die Dropdown-Liste den erforderlichen Lizenzschlüssel aus dem Schlüsselspeicher des Administrationsservers aus.

Die Details des Lizenzschlüssels werden in den Feldern darunter angezeigt.

Sie können den vorhandenen Aktivierungsschlüssel auf dem Mobilgerät ersetzen, wenn er sich von dem in der Dropdown-Liste oben ausgewählten unterscheidet. Aktivieren Sie dazu das Kontrollkästchen **Mit diesem Schlüssel ersetzen, falls sich der Schlüssel auf dem Gerät unterscheidet**.

4. Klicken Sie auf die Schaltfläche **Speichern**, um die an der Richtlinie vorgenommenen Änderungen zu speichern und das Fenster mit den Richtlinieneigenschaften zu verlassen.

Die Einstellungen werden nach der nächsten planmäßigen Synchronisierung des Geräts mit Kaspersky Security Center auf dem mobilen Gerät konfiguriert.

## Bereitstellung der erforderlichen Berechtigungen für die App Kaspersky Endpoint Security für Android

Für bestimmte Funktionen der App Kaspersky Endpoint Security für Android sind Berechtigungen erforderlich. Kaspersky Endpoint Security für Android fragt während der Installation sowie nach der Installation und vor der Nutzung einzelner Funktionen der App nach obligatorischen Berechtigungen. Kaspersky Endpoint Security für Android kann nicht installiert werden, ohne dass die obligatorischen Berechtigungen erteilt werden.

Auf einigen Geräten (z. B. Huawei, Meizu, Xiaomi) muss Kaspersky Endpoint Security für Android in den Geräteeinstellungen manuell zur Liste der Apps hinzugefügt werden, die beim Start des Betriebssystems gestartet werden. Wenn die App nicht zur Liste hinzugefügt wird, stellt Kaspersky Endpoint Security für Android nach dem Neustart des mobilen Geräts sämtliche Funktionen ein.

Auf Geräten mit Android 11 oder höher müssen Sie die Systemeinstellung **Berechtigungen entfernen, wenn die App nicht verwendet wird** deaktivieren. Andernfalls setzt das System die vom Benutzer an die App erteilten Berechtigungen automatisch zurück, nachdem die App einige Monate lang nicht verwendet wurde.

Berechtigungen, welche die App "Kaspersky Endpoint Security für Android" anfragt

Berechtigung	App-Funktion
<b>Telefon</b> (nur für Android 5.0–9.X erforderlich)	Verbindung mit Kaspersky Security Center (Geräte-ID)
<b>Speicher</b> (obligatorisch)	Anti-Virus
<b>Zugriff auf alle Dateien</b>	Anti-Virus (nur für Android 11 und höher)
<b>Bluetooth-Geräte in der Nähe</b> (für Android 12 und höher)	Bluetooth-Verwendung beschränken
<b>Geräteadministrator</b> (obligatorisch)	Diebstahlschutz – Gerät sperren (nur für Android 5.0–6.X)
	Diebstahlschutz – Foto mit der Frontkamera aufnehmen

	<p>Obwohl die Funktion "Foto aufnehmen" in der Kaspersky Security Center Web Console und der Cloud Console nicht unterstützt wird, benötigt die App Kaspersky Endpoint Security für Android diese Berechtigung, damit sie von allen Kaspersky Security Center-Konsolen verwaltet werden kann.</p>
	Diebstahlschutz – Alarmsignal erzeugen
	Diebstahlschutz – auf Werkseinstellungen zurücksetzen
	Kennwortschutz
	Schutz der App vor der Deinstallation
	Installation von Sicherheitszertifikaten
	Anwendungskontrolle
	Beschränkung der Verwendung von Kamera, Bluetooth, WLAN
<b>Kamera</b>	<p>Diebstahlschutz – Foto mit der Frontkamera aufnehmen</p> <p>Obwohl die Funktion "Foto aufnehmen" in der Kaspersky Security Center Web Console und der Cloud Console nicht unterstützt wird, benötigt die App Kaspersky Endpoint Security für Android diese Berechtigung, damit sie von allen Kaspersky Security Center-Konsolen verwaltet werden kann.</p> <p>Auf Geräten mit Android 11.0 und höher muss der Benutzer bei entsprechender Aufforderung die Berechtigung "Nur während Nutzung der App" erteilen.</p>
<b>Standort</b>	<p>Diebstahlschutz – Gerät orten</p> <p>Auf Geräten mit Android 10.0 und höher muss der Benutzer bei entsprechender Aufforderung die Berechtigung "Immer" erteilen.</p>
<b>Erleichterte Bedienung</b>	<p>Diebstahlschutz – Gerät sperren (nur für Android 7.0 und höher)</p> <p>Web-Filter</p> <p>Anwendungskontrolle</p> <p>Schutz der App vor der Deinstallation (nur für Android 7.0 und höher)</p> <p>Anzeige von Warnungen von Kaspersky Endpoint Security für Android (nur für Android 10.0 und höher)</p> <p>Verwendung der Kamera beschränken (nur für Android 11 und höher)</p>

## Zertifikate verwalten

Mobile Zertifikate werden verwendet, um die Benutzer von mobilen Geräten auf dem Administrationsserver zu identifizieren.

Mit der Kaspersky Security Center Web Console und der Cloud Console können Sie die folgenden Aktionen mit Benutzerzertifikaten ausführen:

- Zertifikate und ihren Status anzeigen.
- Neue Zertifikate erstellen.
- Auslaufende Zertifikate erneuern.
- Zertifikate löschen.

Weitere Informationen zu Kaspersky Security Center-Zertifikaten:

- Wenn Sie Kaspersky Security Center Web Console verwenden, lesen Sie bitte die [Hilfe zu Kaspersky Security Center](#).
- Wenn Sie Kaspersky Security Center Cloud Console verwenden, lesen Sie bitte die [Hilfe zu Kaspersky Security Center Cloud Console](#).

## Zertifikatsliste anzeigen

Mit der Kaspersky Security Center Web Console und der Cloud Console können Sie die angewendeten mobilen Benutzerzertifikate, ihren Status und ihre Eigenschaften anzeigen.

*So zeigen Sie die Liste der angewendeten Mobilfunkzertifikate für Benutzer an:*

1. Wählen Sie im Hauptfenster von Kaspersky Security Center Web Console oder Cloud Console die Option **GERÄTE > MOBIL > GERÄTE** aus.
2. Wählen Sie **Zertifikate verwalten** aus.

Die Seite **Mobile Zertifikate** mit Informationen zu den angewendeten Mobilfunkzertifikaten des Benutzers wird geöffnet. Sie können Details zu einem Zertifikat anzeigen, indem Sie in der Spalte **Benutzername** darauf klicken.

## Zertifikatseinstellungen festlegen

Via Kaspersky Security Center Web Console oder Cloud Console können Sie Gültigkeitsdauer, automatische Updates und Kennwortschutz für mobile Zertifikate anpassen.

*So legen Sie die Einstellungen mobiler Zertifikate fest:*

1. Wählen Sie im Hauptfenster von Kaspersky Security Center Web Console oder Cloud Console die Option **GERÄTE > MOBIL > GERÄTE** aus.
2. Wählen Sie **Zertifikate verwalten** aus.
3. Wählen Sie **Zertifikatseinstellungen** aus.
4. Im sich öffnenden Fenster **Mobile Zertifikate erstellen** können Sie Folgendes konfigurieren:

- **Gültigkeitsdauer des Zertifikats (Tage)**



Gültigkeitsdauer des Zertifikats in Tagen. Standardmäßig beträgt die Gültigkeitsdauer des Zertifikats 365 Tage. Nach Ablauf dieser Frist kann sich das mobile Gerät nicht mehr mit dem Administrationsserver verbinden.

- **Neuausstellung bei Ablauf des Zertifikats in (Tagen)**

Anzahl der Tage bis zum Ablauf der Gültigkeitsdauer des aktuellen Zertifikats, während der vom Administrationsserver ein neues Zertifikat ausgestellt werden muss. Wenn in diesem Feld beispielsweise der Wert 4 angegeben ist, stellt der Administrationsserver innerhalb von vier Tagen vor Ablauf der Gültigkeitsdauer des aktuellen Zertifikats ein neues Zertifikat aus. Der Standardwert ist 1.

- **Zertifikat automatisch neu ausstellen, wenn möglich**

Die Zertifikate werden nach Möglichkeit automatisch neu ausgestellt. Wenn diese Option deaktiviert ist, müssen Zertifikate nach Ablauf manuell neu ausgestellt werden. Diese Option ist standardmäßig deaktiviert.

- **Kennwort während der Installation des Zertifikats anfordern**

Der Benutzer wird bei der Installation des Zertifikats auf dem mobilen Gerät aufgefordert, ein Kennwort einzugeben. Das Kennwort wird nur einmal bei der Installation des Zertifikats auf dem mobilen Gerät verwendet. Das Kennwort wird automatisch mithilfe des Administrationsservers erstellt und per E-Mail an die Benutzer gesendet. Die Kennwortlänge können Sie im Feld **Kennwortlänge** angeben.

5. Klicken Sie auf **Speichern**, um die Änderungen zu übernehmen und das Fenster zu schließen.

Die festgelegten Einstellungen werden von Kaspersky Security Center verwendet, um mobile Zertifikate zu erstellen, zu aktualisieren und zu schützen.

## Zertifikat erstellen

Sie können in Kaspersky Security Center Web Console und Cloud Console mobile Zertifikate erstellen, um die Benutzer von mobilen Geräten zu identifizieren.

*So erstellen Sie ein mobiles Zertifikat:*

1. Wählen Sie im Hauptfenster von Kaspersky Security Center Web Console oder Cloud Console die Option **GERÄTE > MOBIL > GERÄTE** aus.
2. Wählen Sie **Zertifikate verwalten** aus.
3. Klicken Sie im sich öffnenden Fenster **Mobile Zertifikate** auf **Hinzufügen**, um den **Assistent zum Erstellen eines mobilen Zertifikats** zu starten. Folgen Sie den Anweisungen des Assistenten mithilfe der Schaltfläche **Weiter**.
4. Wählen Sie die Benutzer oder Benutzergruppen aus, deren mobilen Geräte Sie mit einem neuen Zertifikat verwalten möchten.
5. Legen Sie die **Einstellungen zur Veröffentlichung** fest:
  - Wenn Sie die Benutzer über das neue Zertifikat benachrichtigen möchten, aktivieren Sie das Kontrollkästchen **Benutzer über das neue Zertifikat informieren**.
  - Wenn Sie die mehrfache Verwendung eines Zertifikats auf demselben Gerät zulassen möchten, aktivieren Sie das Kontrollkästchen **Mehrmaliges Verwenden eines Zertifikats auf dem gleichen Gerät zulassen (gilt nur für Geräte, auf denen Kaspersky Endpoint Security für Android installiert ist)**.
6. Wählen Sie den **Authentifizierungstyp** aus:

- Wählen Sie **Anmeldedaten (Domain-Login oder Benutzername)**, wenn Benutzer mit ihren Anmeldedaten auf das Zertifikat zugreifen sollen.
- Wählen Sie **Einmalkennwort** aus, wenn Benutzer mit einem Einmalkennwort auf das Zertifikat zugreifen sollen.

Diese Option ist verfügbar, wenn Sie im vorherigen Schritt nicht das Kontrollkästchen **Mehrmaliges Verwenden eines Zertifikats auf dem gleichen Gerät zulassen (gilt nur für Geräte, auf denen Kaspersky Endpoint Security für Android installiert ist)** aktiviert haben.

- Wählen Sie **Kennwort** aus, wenn Benutzer mit einem Kennwort auf das Zertifikat zugreifen sollen.

Diese Option ist verfügbar, wenn Sie im vorherigen Schritt das Kontrollkästchen **Mehrmaliges Verwenden eines Zertifikats auf dem gleichen Gerät zulassen (gilt nur für Geräte, auf denen Kaspersky Endpoint Security für Android installiert ist)** aktiviert haben.

7. Geben Sie die Methode der Auslieferung des Zertifikats im Feld **Auslieferung des Zertifikats** an:

- Wenn Sie im vorherigen Schritt **Einmalkennwort** ausgewählt haben, wählen Sie eine der folgenden Optionen:
  - Wenn Sie das Kennwort per E-Mail senden möchten, wählen Sie **Benutzer mittels E-Mail informieren**. Wählen Sie dann die zu verwendende E-Mail-Adresse aus oder wählen Sie **Andere E-Mail-Adresse**, um eine andere E-Mail-Adresse anzugeben.
  - Wenn Sie die Benutzer auf eine andere Weise über das Kennwort informieren möchten, wählen Sie **Kennwort nach Abschließen des Assistenten anzeigen**.
- Wenn Sie im vorherigen Schritt **Anmeldedaten (Domain-Login oder Benutzername)** ausgewählt haben, wählen Sie die zu verwendende E-Mail-Adresse oder wählen Sie **Andere E-Mail-Adresse**, um eine andere E-Mail-Adresse anzugeben.

8. Die Zusammenfassung zum Zertifikat wird angezeigt.

Stellen Sie sicher, dass alle Einstellungen korrekt sind, und klicken Sie dann auf **Erstellen**.

Daraufhin erstellt der **Assistent zum Erstellen eines mobilen Zertifikats** ein Zertifikat, das Benutzer auf ihren mobilen Geräten installieren können. Das Zertifikat wird nach der nächsten Synchronisierung der mobilen Geräte mit Kaspersky Security Center verfügbar.

Weitere Informationen über die Erstellung der Zertifikate und die Anpassung der Regeln für ihre Ausstellung finden Sie hier:

- Wenn Sie Kaspersky Security Center Web Console verwenden, lesen Sie bitte die [Hilfe zu Kaspersky Security Center](#).
- Wenn Sie Kaspersky Security Center Cloud Console verwenden, lesen Sie bitte die [Hilfe zu Kaspersky Security Center Cloud Console](#).

## Zertifikat erneuern

Wenn eines der angewendeten Mobilfunkzertifikate demnächst abläuft, können Sie es mithilfe der Kaspersky Security Center Web Console oder Cloud Console erneuern.

*So erneuern Sie ein Mobilfunkzertifikat:*

1. Wählen Sie im Hauptfenster von Kaspersky Security Center Web Console oder Cloud Console die Option **GERÄTE > MOBIL > GERÄTE** aus.
2. Wählen Sie **Zertifikate verwalten** aus.
3. Wählen Sie das Zertifikat aus, das Sie erneuern möchten, und klicken Sie dann auf **Neu ausstellen**.

Der Status des Zertifikats ändert sich in **Das Zertifikat wurde neu ausgestellt**.

## Zertifikat löschen

Sie können mobile Zertifikate mithilfe der Kaspersky Security Center Web Console oder der Cloud Console löschen.

Wenn Sie ein mobiles Zertifikat löschen, kann das Gerät nicht mehr mit dem Administrationsserver synchronisiert und nicht über das Kaspersky Security Center verwaltet werden. Um das mobile Gerät wieder verwalten zu können, müssen Sie die [App Kaspersky Endpoint Security für Android](#) darauf neu installieren.

*So löschen Sie ein Mobilfunkzertifikat:*

1. Wählen Sie im Hauptfenster von Kaspersky Security Center Web Console oder Cloud Console die Option **GERÄTE > MOBIL > GERÄTE** aus.
2. Wählen Sie **Zertifikate verwalten** aus.
3. Wählen Sie das Zertifikat aus, das Sie löschen möchten, und klicken Sie dann auf **Löschen**.

Das Zertifikat wird gelöscht und aus der Liste der Zertifikate entfernt.

## Informationsaustausch mit Firebase Cloud Messaging

Kaspersky Endpoint Security für Android verwendet den Dienst Firebase Cloud Messaging (FCM) zur rechtzeitigen Zustellung von Befehlen an mobile Geräte und zur erzwungenen Synchronisierung im Falle einer Änderung von Richtlinieneinstellungen.

Für die Nutzung des Dienstes Firebase Cloud Messaging müssen die Einstellungen des Dienstes in Kaspersky Security Center Web Console oder Cloud Console definiert werden.

*So aktivieren Sie Firebase Cloud Messaging in der Kaspersky Security Center Web Console oder Cloud Console:*

1. Wählen Sie im Hauptfenster von Kaspersky Security Center Web Console oder Cloud Console die Option **GERÄTE > MOBIL > SYNCHRONISIEREN VON ANDROID-GERÄTEN** aus.

Das Fenster **Synchronisieren von Android-Geräten** wird geöffnet.

2. Geben Sie in den Feldern **Sender-ID** und **Server-Schlüssel** die Firebase Cloud Messaging-Einstellungen an: SENDER\_ID und API Key.

Firebase Cloud Messaging ist aktiviert.

*So erhalten Sie eine Sender-ID und den Server-Schlüssel:*

1. Registrieren Sie sich im [Google-Portal](#).
2. Wechseln Sie zur [Google Cloud Platform](#).
3. Erstellen Sie ein neues Projekt.  
Warten Sie, bis das Projekt erstellt wurde.
4. Suchen Sie die entsprechende SENDER\_ID des Projekts.
5. Aktivieren Sie Google Firebase Cloud Messaging für Android.
6. Befolgen Sie die Anweisungen auf dem Bildschirm, um Anmeldedaten zu erstellen.
7. Rufen Sie aus den Eigenschaften der neu erstellten Anmeldedaten den API-Schlüssel ab.

Ausführliche Informationen zu den Vorgängen in der Google Cloud Platform finden Sie [in der entsprechenden Dokumentation](#).

Sie verfügen nun über eine **Sender-ID** und einen **Server-Schlüssel**, um die Firebase Cloud Messaging-Einstellungen zu konfigurieren.

Wenn die Einstellungen von Firebase Cloud Messaging nicht definiert sind, dann werden die Befehle auf dem mobilen Gerät und die Richtlinieneinstellungen während der Synchronisierung des Geräts mit Kaspersky Security Center nach dem Zeitplan, der in der Richtlinie festgelegt wurde (z. B. alle 24 Stunden), an das Gerät zugestellt. Das bedeutet, dass die Befehle und Richtlinieneinstellungen mit Verzögerung zugestellt werden.

Um die Kernfunktionen der Software nutzen zu können, stimmen Sie zu, dem Dienst Firebase Cloud Messaging die eindeutige ID der App-Installation (Instance ID) sowie die folgenden Informationen automatisch zu übermitteln:

- Informationen über die installierte Software: Version der App, App-ID, Build-Version der App, Name des App-Pakets.
- Informationen über den Computer, auf dem die Software installiert ist: Version des Betriebssystems, Geräte-ID, Version der Google-Dienste.
- Informationen über FCM: ID der App in FCM, Benutzer-ID in FCM, Protokollversion.

Die Übermittlung der Daten an Firebase erfolgt über einen geschützten Kanal. Der Zugang zu und der Schutz von Informationen wird durch die entsprechenden Nutzungsbedingungen der Firebase-Dienste geregelt: [Firebase Bedingungen für Datenverarbeitung und Sicherheit](#), [Datenschutz und Sicherheit in Firebase](#).

*Um den Datenaustausch mit dem Dienst Firebase Cloud Messaging zu verbieten, gehen Sie wie folgt vor:*

1. Wählen Sie im Hauptfenster von Kaspersky Security Center Web Console oder Cloud Console die Option **GERÄTE > MOBIL > SYNCHRONISIEREN VON ANDROID-GERÄTEN** aus.  
Das Fenster **Synchronisieren von Android-Geräten** wird geöffnet.
2. Klicken Sie auf **Zurücksetzen**.
3. Klicken Sie im nächsten Fenster auf die Schaltfläche **OK**, um das Zurücksetzen zu bestätigen.

Die Firebase Cloud Messaging-Einstellungen werden gelöscht.

# Mobile Geräte in Kaspersky Security Center Web Console und Cloud Console verwalten

Mobile Geräte können via Kaspersky Security Center Web Console und Cloud Console mithilfe von [Gruppenrichtlinien](#) und mittels [Versand von Befehlen an mobile Geräte](#) verwaltet werden (nur für Android).

Um mobile Geräte via Kaspersky Security Center Web Console zu verwalten, müssen Sie [Verwaltungs-Plugins installieren](#).

## Mobile Geräte mit Kaspersky Security Center verbinden

Damit ein mobiles Gerät über die Kaspersky Security Center Web Console oder Cloud Console verwaltet werden kann, muss es mit Kaspersky Security Center verbunden sein. Die Liste der mit Kaspersky Security Center verbundenen mobilen Geräte finden Sie auf der Registerkarte **GERÄTE > MOBIL > GERÄTE** in Web Console oder Cloud Console.

Bevor Sie ein iOS-Gerät verbinden, müssen Sie die Adresse von Kaspersky Security Center an den Gerätebenutzer senden. Dies dient der Überprüfung der Verbindungssicherheit. Der Benutzer sieht diese Adresse während der App-Installation und kann die Verbindung trennen, falls die angezeigte Adresse nicht mit der von Ihnen gesendeten Adresse übereinstimmt.

*So verbinden Sie ein mobiles Gerät mit Kaspersky Security Center:*

1. Starten Sie den Assistenten für die Verbindung eines mobilen Gerätes:

- Wählen Sie im Hauptfenster von Kaspersky Security Center Web Console oder Cloud Console **GERÄTE > MOBIL > GERÄTE** aus und klicken Sie dann auf **Hinzufügen**.
- Wählen Sie im Hauptfenster der Kaspersky Security Center Web Console oder Cloud Console **BENUTZER & ROLLEN > BENUTZER** aus. Klicken Sie auf den Namen des Benutzers oder der Benutzergruppe, an den bzw. die Sie den Link zum Verbinden eines mobilen Gerätes senden möchten, und wählen Sie dann **GERÄTE**. Klicken Sie auf **Mobiles Gerät hinzufügen**. Wiederholen Sie in diesem Fall den Schritt 3.

Folgen Sie dem Assistenten, indem Sie auf die Schaltfläche **Weiter** klicken.

2. Auswahl des Betriebssystems der Geräte, die Sie hinzufügen möchten:

- **Android**
- **iOS und iPadOS**

3. Wählen Sie die Benutzer und Benutzergruppen aus, an die Sie den Link zum Verbinden eines mobilen Gerätes senden möchten.

4. Auswahl der E-Mail-Adressen, an die der Link gesendet wird:

- **Alle E-Mail-Adressen**

- **Primäre E-Mail-Adresse**
- **Alternative E-Mail-Adresse**
- **Andere E-Mail-Adresse**

Wenn Sie diese Option auswählen, geben Sie unten die E-Mail-Adresse an.

5. Die Linkzusammenfassung wird angezeigt.

Stellen Sie sicher, dass alle Parameter des Links korrekt sind, und klicken Sie dann auf **Senden**.

6. Es öffnet sich ein Fenster mit der Bestätigung, dass der Link zum Hinzufügen eines mobilen Gerätes gesendet wurde.

Klicken Sie auf **OK**, um den Assistenten abzuschließen.

Wenn der Benutzer die App "Kaspersky Endpoint Security für Android" oder "Kaspersky Security für iOS" installiert, wird das Benutzergerät auf der Registerkarte **GERÄTE > MOBIL > GERÄTE** von Web Console oder Cloud Console angezeigt.

## Nicht zugeordnete mobile Geräte in Administrationsgruppen verschieben

Wenn die App "Kaspersky Endpoint Security für Android" oder "Kaspersky Security für iOS" auf mobilen Geräten installiert ist, wird sie auf der Seite **ENTDECKUNG UND SOFTWAREVERTEILUNG > NICHT ZUGEORDNETE GERÄTE** in Kaspersky Security Center Web Console oder Cloud Console angezeigt. Um neu verbundene Geräte zu verwalten, können Sie [eine Regel für das automatische Verschieben der Geräte in eine Administrationsgruppe erstellen](#) oder diese manuell in eine [Administrationsgruppe](#) verschieben.

*So verschieben Sie ein nicht zugewiesenes mobiles Gerät in eine Administrationsgruppe:*

1. Wählen Sie im Hauptfenster von Kaspersky Security Center Web Console oder Cloud Console die Option **ENTDECKUNG UND SOFTWAREVERTEILUNG > NICHT ZUGEORDNETE GERÄTE** aus.
2. Wählen Sie das Gerät aus, das Sie in eine Administrationsgruppe verschieben möchten, und klicken Sie dann auf **In Gruppe verschieben**.
3. Wählen Sie in der sich öffnenden Strukturansicht der Administrationsgruppen die Zielgruppe aus, in die Sie das Gerät verschieben möchten.  
Sie können eine neue Administrationsgruppe erstellen, indem Sie eine vorhandene Gruppe auswählen und dann auf **Untergeordnete Gruppe hinzufügen** klicken.
4. Klicken Sie auf **Verschieben**.

Das Gerät wird in die angegebene Administrationsgruppe verschoben und die [Gruppenrichtlinie](#) wird darauf angewendet.

## Befehle an mobile Geräte senden

Mit Kaspersky Security Center können Sie Befehle an mobile Android-Geräte senden, um Daten auf einem verlorenen oder gestohlenen Mobilgerät zu schützen oder um die erzwungene Synchronisierung eines mobilen Geräts durchzuführen.

An iOS-Geräte können keine Befehle gesendet werden.

Die folgenden Befehle werden unterstützt:

- **Gerät sperren**

Das mobile Gerät wird gesperrt.

- **Gerät entsperren**

Das mobile Gerät wird entsperrt. Auf den Geräten unter Verwaltung des Betriebssystems Android 5.0 – 6.X wird nach der Freischaltung des Mobilgeräts das Kennwort zur Freischaltung des Bildschirm (PIN-Code) mit "1234" ersetzt. Auf den Geräten unter Verwaltung des Betriebssystems Android 7.0 und höher bleibt nach dem Entsperren des Mobilgeräts das Kennwort zur Freischaltung des Bildschirms unverändert.

- **Auf Werkseinstellungen zurücksetzen**

Sämtliche Daten werden vom mobilen Gerät gelöscht, die Einstellungen des mobilen Geräts werden auf die Werkseinstellung zurückgesetzt.

- **Unternehmensdaten löschen**

Die Daten in Containern und das E-Mail-Konto des Unternehmens werden vom mobilen Gerät gelöscht.

- **Gerät orten**

Der Standort des Geräts wurde bestimmt und wird auf Google Maps angezeigt. Der Mobilfunkanbieter kann für den Internetzugang eine Gebühr erheben.

Wenn der Benutzer auf Geräten mit Android 12 oder höher die Berechtigung "Ungefähren Standort verwenden" erteilt hat, versucht die App "Kaspersky Endpoint Security für Android" zunächst, den genauen Standort des Geräts zu ermitteln. Gelingt dies nicht, wird der ungefähre Gerätestandort nur zurückgegeben, wenn er frühestens 30 Minuten zuvor empfangen wurde. Andernfalls schlägt der Befehl **Gerät orten** fehl.

- **Alarmton abspielen**

Das mobile Gerät erzeugt ein Alarmsignal. Das Alarmsignal wird 5 Minuten (bei niedrigem Akkuladestand 1 Minute) lang wiedergegeben.

- **Gerät synchronisieren**

Die Synchronisierung des mobilen Geräts mit Kaspersky Security Center wird ausgeführt.

Die App "Kaspersky Endpoint Security für Android" erfordert bestimmte [Berechtigungen](#) für die Ausführung von Befehlen. Während der Ausführung des Schnellstartassistenten bietet Kaspersky Endpoint Security für Android an, dem Benutzer der App die erforderlichen Berechtigungen bereitzustellen. Der Benutzer kann diese Schritte überspringen oder die Berechtigungen in den Einstellungen des Geräts später deaktivieren. In diesem Fall ist die Ausführung von Befehlen nicht möglich.

Auf Geräten mit Android 10.0 und höher muss der Benutzer für den Zugriff auf den Standort die Berechtigung "Immer" erteilen. Auf Geräten unter Android 11.0 und später muss der Benutzer auch die Berechtigung "Nur während der Nutzung der App" erteilen, um Zugriff auf die Kamera zu erhalten. Andernfalls werden die Befehle der Funktion "Diebstahlschutz" nicht ausgeführt. Der Benutzer wird über diese Einschränkung in Kenntnis gesetzt und erneut aufgefordert, die Berechtigung der erforderlichen Ebene zu erteilen. Falls der Benutzer für den Kamerazugriff die Option "Nur dieses Mal" auswählt, gilt der Zugriff für die App als erteilt. Es wird empfohlen, den Benutzer direkt zu kontaktieren, falls die Berechtigung auf den Kamerazugriff erneut angefordert wird.

*So senden Sie einen Befehl an ein mobiles Gerät:*

1. Wählen Sie im Hauptfenster der Kaspersky Security Center Web Console oder Cloud Console **GERÄTE > MOBIL > GERÄTE** aus.
2. Wählen Sie das Gerät aus, an das Sie den Befehl senden möchten, und klicken Sie dann entweder auf **Kontrolle** oder **Verwalten**.
3. Wählen Sie den gewünschten Befehl in der Liste **Verfügbare Befehle** aus und klicken Sie auf **OK**.
4. Klicken Sie auf **OK**, falls Sie aufgefordert werden, den Vorgang zu bestätigen.

Der angegebene Befehl wird an das mobile Gerät gesendet und das Bestätigungsfenster wird angezeigt.

## Mobile Geräte aus Kaspersky Security Center entfernen

Wenn Sie ein mobiles Gerät nicht mehr verwalten müssen, können Sie es via Web Console oder Cloud Console aus Kaspersky Security Center entfernen.

*So entfernen Sie ein mobiles Gerät aus Kaspersky Security Center:*

1. Entfernen Sie die mobile App vom Gerät oder stellen Sie sicher, dass der Benutzer die App vom entsprechenden Gerät entfernt hat.
2. Wählen Sie im Hauptfenster der Kaspersky Security Center Web Console oder Cloud Console **GERÄTE > MOBIL > GERÄTE** aus.
3. Wählen Sie das mobile Gerät aus, das Sie löschen möchten, und klicken Sie auf **Löschen**.
4. Klicken Sie auf **OK**, um den Vorgang zu bestätigen.

Das Gerät wird aus Kaspersky Security Center gelöscht.

## Gruppenrichtlinien verwalten

Dieser Abschnitt beschreibt die Verwaltung von Gruppenrichtlinien via Kaspersky Security Center Web Console und Cloud Console.

### Gruppenrichtlinien für die Verwaltung von mobilen Geräten

Eine *Gruppenrichtlinie* ist eine eindeutige Auswahl von Einstellungen zur Verwaltung von mobilen Geräten, die zur Administrationsgruppe gehören und von mobilen Apps auf den Geräten installiert werden.

Mithilfe der Richtlinie können Sie Einstellungen sowohl für einzelne Geräte als auch Gruppen konfigurieren. Verwaltungseinstellungen für eine Gerätegruppe können im Eigenschaftenfenster der Gruppenrichtlinie.

Jede Einstellung in einer Richtlinie besitzt das Attribut "Schloss", mit dem gekennzeichnet wird, ob der Parameter in den Richtlinien einer untergeordneten Hierarchieebene (für Untergruppen und untergeordnete Administrationsserver) und in den lokalen Programmeinstellungen verändert werden darf.



Einstellungswerte, die in der Richtlinie und in den lokalen Programmeinstellungen festgelegt wurden, werden auf dem Administrationsserver gespeichert, während der Synchronisierung auf mobile Geräte verteilt und auf den Geräten als gültige Anwendungseinstellungen gespeichert. Wenn der Benutzer auf seinem Gerät andere Einstellungswerte festlegt, die nicht mit einem "Schloss" fixiert wurden, werden bei der nächsten Synchronisierung des Geräts mit dem Administrationsserver die neuen Einstellungswerte an den Administrationsserver übertragen und anstelle der Werte, die früher vom Administrator eingestellt worden sind, in den lokalen Programmeinstellungen gespeichert.

Um die Unternehmenssicherheit mobiler Android-Geräte zu gewährleisten, können Sie überwachen, ob die [Anforderungen an die Unternehmenssicherheit](#) auf Benutzergeräten eingehalten werden.

Nähere Informationen zur Verwaltung von Richtlinien und Administrationsgruppen via Kaspersky Security Center Web Console und Cloud Console finden Sie hier:

- Wenn Sie Kaspersky Security Center Web Console verwenden, lesen Sie bitte die [Hilfe zu Kaspersky Security Center](#).
- Wenn Sie Kaspersky Security Center Cloud Console verwenden, lesen Sie bitte die [Hilfe zu Kaspersky Security Center Cloud Console](#).

## Liste der Gruppenrichtlinien anzeigen

Mithilfe von Kaspersky Security Center Web Console und Cloud Console können Sie Gruppenrichtlinien sowie deren Status und Eigenschaften anzeigen.

*So zeigen Sie die Liste der Gruppenrichtlinien an,*

Wählen Sie im Hauptfenster der Kaspersky Security Center Web Console oder Cloud Console **GERÄTE > RICHTLINIEN & PROFILE** aus.

Die Liste mit Gruppenrichtlinien und Kurzinformationen zu den Gruppenrichtlinien wird geöffnet. Auf dieser Seite können Sie Gruppenrichtlinien [erstellen](#), [ändern](#), [kopieren](#), [verschieben](#) und [löschen](#).

## Ergebnisse der Richtlinienverteilung anzeigen

Mithilfe von Kaspersky Security Center Web Console und Cloud Console können Sie das Verteilungsdiagramm einer Gruppenrichtlinie sowie die Informationen zu allen Geräten anzeigen, die unter diese Richtlinie fallen.

*So zeigen Sie die Verteilungsergebnisse einer Gruppenrichtlinie an:*

1. Wählen Sie im Hauptfenster der Kaspersky Security Center Web Console oder Cloud Console **GERÄTE > RICHTLINIEN & PROFILE** aus.
2. Aktivieren Sie in der sich öffnenden Liste der Gruppenrichtlinien das Kontrollkästchen neben dem Namen der Richtlinie, für die Sie die Verteilungsergebnisse anzeigen möchten, und klicken Sie dann auf **Verteilung**.

Die Seite mit den Ergebnissen der Richtlinienverteilung wird geöffnet. Diese Seite enthält die Zusammenfassung der Richtlinie, das Verteilungsdiagramm der Richtlinie und die Tabelle mit Informationen zu allen Geräten, die unter diese Richtlinie fallen. Das Fenster mit den Richtlinieneigenschaften kann über die Schaltfläche **Richtlinie konfigurieren** geöffnet werden.

# Gruppenrichtlinie erstellen

Mithilfe von Kaspersky Security Center Web Console und Cloud Console können Sie Gruppenrichtlinien für die Verwaltung mobiler Geräte erstellen.

*So erstellen Sie eine Gruppenrichtlinie:*

1. Wählen Sie im Hauptfenster der Kaspersky Security Center Web Console oder Cloud Console **GERÄTE > RICHTLINIEN & PROFILE** aus.

2. Klicken Sie in der sich öffnenden Liste der Gruppenrichtlinien von Kaspersky Security Center auf **Aktueller Pfad**, um die [Administrationsgruppe](#) auszuwählen, für die Sie eine Richtlinie erstellen möchten.

Standardmäßig wird die neue Gruppenrichtlinie auf die Gruppe **Verwaltete Geräte angewendet**.

3. Klicken Sie auf **Hinzufügen**, um den Assistenten zum Erstellen von Richtlinien zu starten. Folgen Sie dem Assistenten, indem Sie auf die Schaltfläche **Weiter** klicken.

4. Wählen Sie eine App aus, die der Plattform entspricht:

- **Kaspersky Endpoint Security für Android**
- **Kaspersky Security für iOS**

5. Geben Sie im Feld **Name** einen Namen für die neue Richtlinie an. Wenn Sie den Namen einer bereits vorhandenen Richtlinie verwenden, erhält er automatisch den Zusatz (1).

6. Wählen Sie den Richtlinienstatus:

- **Aktiv**

Der Assistent speichert die erstellte Richtlinie auf dem Administrationsserver. Bei der nächsten Synchronisierung des mobilen Geräts mit dem Administrationsserver wird die Richtlinie auf dem Gerät als aktive Richtlinie verwendet.

- **Inaktiv**

Der Assistent speichert die erstellte Richtlinie als Reserve-Richtlinie auf dem Administrationsserver. Die Richtlinie kann später bei einem bestimmten Ereignis aktiviert werden. Bei Bedarf kann eine inaktive Richtlinie aktiviert werden.

In einer Gruppe können mehrere Richtlinien für ein Programm erstellt werden. Es gibt aber immer nur eine aktive Richtlinie. Nach dem Erstellen einer neuen aktiven Richtlinie wird die zuvor aktive Richtlinie automatisch inaktiv.

7. Sie können zwei Erboptionen aktivieren oder deaktivieren: **Einstellungen aus übergeordneter Richtlinie erben** und **Vererben der Einstellungen für untergeordnete Richtlinien erzwingen**:

- Wenn Sie die Option **Einstellungen aus übergeordneter Richtlinie erben** für eine untergeordnete [Administrationsgruppe](#) aktivieren und einige Einstellungen in der übergeordneten Richtlinie sperren, können Sie diese Einstellungen nicht in der Richtlinie für die untergeordnete Gruppe bearbeiten. Sie können jedoch Einstellungen ändern, die in der übergeordneten Richtlinie nicht gesperrt sind.
- Wenn Sie die Option **Einstellungen aus übergeordneter Richtlinie erben** für eine untergeordnete [Administrationsgruppe](#) deaktivieren, können Sie alle Einstellungen in der untergeordneten Gruppe

bearbeiten, selbst wenn einige Einstellungen in der übergeordneten Richtlinie gesperrt sind.

- Wenn Sie die Option **Vererben der Einstellungen für untergeordnete Richtlinien erzwingen** in der übergeordneten [Administrationsgruppe](#) aktivieren, wird dadurch die Option **Einstellungen aus übergeordneter Richtlinie erben** für alle untergeordneten Richtlinien aktiviert. In diesem Fall kann diese Option nicht für untergeordnete Richtlinien deaktiviert werden. Alle Einstellungen, die in der übergeordneten Richtlinie gesperrt sind, werden zwangsweise an untergeordnete Gruppen vererbt und können in den untergeordneten Gruppen nicht bearbeitet werden.
- In den Richtlinien für die Gruppe **Verwaltete Geräte** beeinflusst die Option **Einstellungen aus übergeordneter Richtlinie erben** keine anderen Einstellungen, da die Gruppe **Verwaltete Geräte** keine Gruppen höherer Ebene besitzt und somit keine Richtlinien erbt.

Standardmäßig ist die Option **Einstellungen aus übergeordneter Richtlinie erben** aktiviert und die Option **Vererben der Einstellungen für untergeordnete Richtlinien erzwingen** deaktiviert.

8. Bei Bedarf können Sie die Einstellungen der neu erstellten Richtlinie anpassen. Wählen Sie dazu die Registerkarte **PROGRAMMEINSTELLUNGEN** aus und befolgen Sie die Anweisungen im Abschnitt "[Richtlinieneinstellungen definieren](#)".

Alternativ können Sie dies auch später tun.

9. Klicken Sie auf **Speichern**, um die Richtlinie zu erstellen.

Eine neue Gruppenrichtlinie zum Verwalten von mobilen Geräten wird erstellt.

## Gruppenrichtlinie bearbeiten

Mithilfe von Kaspersky Security Center Web Console und Cloud Console können Sie die Einstellungen von Gruppenrichtlinien bearbeiten.

*So bearbeiten Sie eine Gruppenrichtlinie:*

1. Öffnen Sie das Fenster mit den Richtlinieneigenschaften:

- Wählen Sie im Hauptfenster der Kaspersky Security Center Web Console oder Cloud Console **GERÄTE > RICHTLINIEN & PROFILE** aus. Klicken Sie in der sich öffnenden Liste der Gruppenrichtlinien auf den Namen der Richtlinie, die Sie konfigurieren möchten.
- Wählen Sie im Hauptfenster der Kaspersky Security Center Web Console oder Cloud Console **GERÄTE > MOBIL > GERÄTE** aus. Klicken Sie auf das mobile Gerät, das unter die Richtlinie fällt, die Sie konfigurieren möchten, und wählen Sie anschließend die Richtlinie auf der Registerkarte **AKTIVE RICHTLINIEN UND RICHTLINIENPROFILE** aus.

2. Wählen Sie im Fenster mit den Richtlinieneigenschaften die Option **PROGRAMMEINSTELLUNGEN** aus und passen Sie dann die Richtlinieneinstellungen wie im Abschnitt "[Richtlinieneinstellungen definieren](#)" beschrieben an.

Sie können außerdem allgemeine Einstellungen, die Vererbung von Einstellungen, Ereignisprotokollierung und Benachrichtigungen sowie Richtlinienprofile konfigurieren und den Revisionsverlauf ansehen. Weitere Informationen finden Sie in der [Hilfe zu Kaspersky Security Center](#).

3. Klicken Sie auf die Schaltfläche **Speichern**, um die an der Richtlinie vorgenommenen Änderungen zu speichern und das Fenster mit den Richtlinieneigenschaften zu verlassen.

Die Einstellungen werden nach der nächsten planmäßigen Synchronisierung des Geräts mit Kaspersky Security Center auf dem mobilen Gerät konfiguriert.

## Gruppenrichtlinie kopieren

Mithilfe von Kaspersky Security Center Web Console und Cloud Console können Sie eine Kopie einer Gruppenrichtlinie erstellen.

*So erstellen Sie eine Kopie einer Gruppenrichtlinie:*

1. Wählen Sie im Hauptfenster der Kaspersky Security Center Web Console oder Cloud Console **GERÄTE > RICHTLINIEN & PROFILE** aus.
2. Aktivieren Sie in der sich öffnenden Liste der Gruppenrichtlinien das Kontrollkästchen neben dem Namen der Richtlinie, für die Sie eine Kopie erstellen möchten, und klicken Sie auf **Kopieren**.
3. Wählen Sie in der sich öffnenden Strukturansicht der [Administrationsgruppen](#) die Zielgruppe aus, in der Sie eine Kopie der Richtlinie erstellen möchten.  
Sie können eine neue Administrationsgruppe erstellen, indem Sie eine vorhandene Gruppe auswählen und dann auf **Untergeordnete Gruppe hinzufügen** klicken.
4. Klicken Sie auf **Kopieren**.
5. Klicken Sie auf **OK**, um den Vorgang zu bestätigen.

In der Zielgruppe wird unter demselben Namen eine Kopie der Richtlinie erstellt. Der Status jeder kopierten oder verschobenen Richtlinie in der Zielgruppe ist **Inaktiv**. Sie können den Status jederzeit zu **Aktiv** ändern.

Existiert in der Zielgruppe bereits eine Richtlinie mit einem identischen Namen wie die neu erstellte oder verschobene Richtlinie, so wird der Index (<nächste laufende Nummer>) an den Namen der neu erstellten oder verschobenen Richtlinie angehängt, zum Beispiel: (1).

## Richtlinie zu einer anderen Administrationsgruppe verschieben

Mithilfe von Kaspersky Security Center Web Console und Cloud Console können Sie eine Richtlinie in eine andere [Administrationsgruppe](#) verschieben.

*So verschieben Sie eine Richtlinie in eine andere Administrationsgruppe:*

1. Wählen Sie im Hauptfenster der Kaspersky Security Center Web Console oder Cloud Console **GERÄTE > RICHTLINIEN & PROFILE** aus.
2. Aktivieren Sie in der sich öffnenden Liste der Gruppenrichtlinien das Kontrollkästchen neben dem Namen der Richtlinie, die Sie in eine andere Administrationsgruppe verschieben möchten, und klicken Sie auf **Verschieben**.
3. Wählen Sie in der sich öffnenden Strukturansicht der Administrationsgruppen die Zielgruppe aus, in die Sie die Richtlinie verschieben möchten.  
Sie können eine neue Administrationsgruppe erstellen, indem Sie eine vorhandene Gruppe auswählen und dann auf **Untergeordnete Gruppe hinzufügen** klicken.

4. Klicken Sie auf **Verschieben**.

5. Klicken Sie auf **OK**, um den Vorgang zu bestätigen.

Das Ergebnis hängt von den Eigenschaften der Richtlinienvererbung ab:

- Wenn die Richtlinie in der Quellgruppe keine geerbte Richtlinie ist, wird sie zur Zielgruppe verschoben.
- Wenn die Richtlinie in der Quellgruppe eine geerbte Richtlinie ist, wird sie nicht verschoben. Stattdessen wird eine Kopie dieser Richtlinie in der Zielgruppe erstellt.

Der Status jeder kopierten oder verschobenen Richtlinie in der Zielgruppe ist **Inaktiv**. Sie können den Status jederzeit zu **Aktiv** ändern.

Existiert in der Zielgruppe bereits eine Richtlinie mit einem identischen Namen wie die neu erstellte oder verschobene Richtlinie, so wird der Index (<nächste laufende Nummer>) an den Namen der neu erstellten oder verschobenen Richtlinie angehängt, zum Beispiel: (1).

## Gruppenrichtlinie löschen

Mithilfe von Kaspersky Security Center Web Console und Cloud Console können Sie Gruppenrichtlinien löschen.

Sie können nur Richtlinien löschen, die in der aktuellen Administrationsgruppe nicht geerbt sind. Eine geerbte Richtlinie kann nur in der Gruppe der höheren Ebene gelöscht werden, für die sie erstellt wurde.

*So löschen Sie eine Gruppenrichtlinie:*

1. Wählen Sie im Hauptfenster der Kaspersky Security Center Web Console oder Cloud Console **GERÄTE > RICHTLINIEN & PROFILE** aus.
2. Aktivieren Sie in der sich öffnenden Liste der Gruppenrichtlinien das Kontrollkästchen neben dem Namen der Richtlinie, die Sie löschen möchten, und klicken Sie auf **Löschen**.
3. Klicken Sie auf **OK**, um den Vorgang zu bestätigen.

Die Gruppenrichtlinie wird gelöscht.

## Richtlinieneinstellungen definieren

In diesem Abschnitt wird beschrieben, wie Sie die Richtlinieneinstellungen von Kaspersky Security Center für die Verwaltung mobiler Geräte festlegen.

Sie können die Richtlinieneinstellungen entweder beim [Erstellen](#) oder beim [Bearbeiten](#) einer Richtlinie festlegen.

## Antivirenschutz konfigurieren

Diese Richtlinieneinstellungen können nur für Android-Geräte festgelegt werden.

Für das frühzeitige Erkennen von Bedrohungen, Viren und anderer schädlicher Apps ist es erforderlich, die Einstellungen für den Echtzeitschutz sowie den Autostart der Untersuchung auf Viren anzupassen.

Kaspersky Endpoint Security für Android entdeckt folgende Objekttypen:

- Viren, Würmer, Trojaner und schädliche Programme.
- Adware.
- Apps, die von Angreifern verwendet werden können, um ein Gerät oder Benutzerdaten zu beschädigen.

Aufgrund von technischen Beschränkungen kann Kaspersky Endpoint Security für Android Dateien mit einer Größe von mehr als 2 GB nicht untersuchen. Während der Untersuchung überspringt die App große Dateien, und benachrichtigt Sie nicht, wenn derartige Dateien übersprungen werden.

## Echtzeitschutz konfigurieren

Diese Richtlinieneinstellungen können nur für Android-Geräte festgelegt werden.

*So konfigurieren Sie den Echtzeitschutz:*

1. Öffnen Sie das Fenster mit den Richtlinieneigenschaften:

- Wählen Sie im Hauptfenster der Kaspersky Security Center Web Console oder Cloud Console **GERÄTE > RICHTLINIEN & PROFILE** aus. Klicken Sie in der sich öffnenden Liste der Gruppenrichtlinien auf den Namen der Richtlinie, die Sie konfigurieren möchten.
- Wählen Sie im Hauptfenster der Kaspersky Security Center Web Console oder Cloud Console **GERÄTE > MOBIL > GERÄTE** aus. Klicken Sie auf das mobile Gerät, das unter die Richtlinie fällt, die Sie konfigurieren möchten, und wählen Sie anschließend die Richtlinie auf der Registerkarte **AKTIVE RICHTLINIEN UND RICHTLINIENPROFILE** aus.

2. Wählen Sie im Fenster mit den Richtlinieneigenschaften die Option **PROGRAMMEINSTELLUNGEN > Basisschutz** aus.

3. Passen Sie im Abschnitt **Anti-Virus** die Schutzeinstellungen für das Dateisystem des mobilen Endgeräts an:

- Zur Aktivierung des Echtzeitschutzes vor Bedrohungen für das Mobilgerät, aktivieren Sie das Kontrollkästchen **Antiviren-Schutz in Echtzeit aktivieren**.
- Geben Sie die Sicherheitsstufe an:
  - Wenn Kaspersky Endpoint Security für Android nur neue Apps und Dateien aus dem Ordner "Downloads" untersuchen soll, wählen Sie **Nur neue Apps untersuchen**.
  - Um den erweiterten Schutz des Mobilgeräts vor Bedrohungen zu aktivieren, wählen Sie **Alle Apps untersuchen und Aktionen mit Dateien überwachen**.

Kaspersky Endpoint Security für Android untersucht dann alle Dateien, die vom Benutzer auf dem Gerät geöffnet, verändert, verschoben, kopiert, installiert und gespeichert werden. Außerdem werden mobile Apps sofort nach ihrer Installation untersucht.

Auf Geräten mit dem Betriebssystem Android 8.0 und höher untersucht Kaspersky Endpoint Security für Android Dateien, die der Benutzer ändert, verschiebt, installiert und speichert, sowie die Kopien von Dateien. Kaspersky Endpoint Security für Android untersucht Dateien nicht bei ihrem Öffnen und untersucht keine Quelldateien beim Kopieren.

- Um die erweiterte Untersuchung neuer Apps vor deren ersten Start auf dem Benutzergerät mithilfe des Cloud-Dienstes von Kaspersky Security Network zu aktivieren, müssen Sie das Kontrollkästchen **Zusätzlicher Schutz durch Kaspersky Security Network** aktivieren.
  - Um Adware und Apps zu blockieren, die von Angreifern verwendet werden können, um das Gerät oder Benutzerdaten zu schädigen, aktivieren Sie das Kontrollkästchen **Adware, Autodialer und Apps erkennen, die von Cyberkriminellen verwendet werden können, um das Gerät und die Daten des Benutzers zu beschädigen**.
4. Wählen Sie im Abschnitt **Einstellungen von Anti-Virus** die Aktion aus, die bei der Erkennung einer Bedrohung ausgeführt werden soll:

- **Datei löschen und eine Backup-Kopie in der Quarantäne speichern**

Die gefundenen Objekte werden automatisch gelöscht. Der Benutzer muss keine weiteren Aktionen vornehmen. Vor dem Löschen eines Objekts erstellt Kaspersky Endpoint Security für Android eine Sicherungskopie der Datei und speichert sie in Quarantäne.

- **Löschen**

Die gefundenen Objekte werden automatisch gelöscht. Der Benutzer muss keine weiteren Aktionen vornehmen. Vor dem Löschen zeigt Kaspersky Endpoint Security für Android eine kurze Benachrichtigung über den Fund des Objekts an.

- **Überspringen**

Wenn gefundene Objekte übersprungen wurden, warnt Kaspersky Endpoint Security für Android den Benutzer vor Problemen beim Schutz des Geräts. Die Informationen über die übersprungenen Objekte werden im Abschnitt **Status** der App angezeigt. Für jede übersprungene Bedrohung werden die Aktionen angeführt, die der Benutzer ausführen kann, um die Bedrohung zu beseitigen. Die Liste der übersprungenen Objekte kann sich ändern, beispielsweise wenn die schädliche Datei gelöscht oder verschoben wurde. Um die aktuelle Liste der Bedrohungen zu erhalten, starten Sie die vollständige Untersuchung des Geräts. Für einen zuverlässigen Schutz Ihrer Daten entfernen Sie alle gefundenen Objekte.

5. Klicken Sie auf die Schaltfläche **Speichern**, um die an der Richtlinie vorgenommenen Änderungen zu speichern und das Fenster mit den Richtlinieneigenschaften zu verlassen.

Die Einstellungen werden nach der nächsten planmäßigen Synchronisierung des Geräts mit Kaspersky Security Center auf dem mobilen Gerät konfiguriert.

## Die automatische Untersuchung auf Viren auf mobilen Geräten konfigurieren



Diese Richtlinieneinstellungen können nur für Android-Geräte festgelegt werden.

*So starten Sie die Untersuchung auf Viren auf dem mobilen Gerät des Benutzers automatisch:*

1. Öffnen Sie das Fenster mit den Richtlinieneigenschaften:

- Wählen Sie im Hauptfenster der Kaspersky Security Center Web Console oder Cloud Console **GERÄTE > RICHTLINIEN & PROFILE** aus. Klicken Sie in der sich öffnenden Liste der Gruppenrichtlinien auf den Namen der Richtlinie, die Sie konfigurieren möchten.
- Wählen Sie im Hauptfenster der Kaspersky Security Center Web Console oder Cloud Console **GERÄTE > MOBIL > GERÄTE** aus. Klicken Sie auf das mobile Gerät, das unter die Richtlinie fällt, die Sie konfigurieren möchten, und wählen Sie anschließend die Richtlinie auf der Registerkarte **AKTIVE RICHTLINIEN UND RICHTLINIENPROFILE** aus.

2. Wählen Sie im Fenster mit den Richtlinieneigenschaften die Option **PROGRAMMEINSTELLUNGEN > Basisschutz** aus.

3. Um Adware und Apps zu blockieren, die von Angreifern verwendet werden können, um das Gerät oder Benutzerdaten zu schädigen, aktivieren Sie das Kontrollkästchen **Adware, Autodialer und Apps erkennen, die von Cyberkriminellen verwendet werden können, um das Gerät und die Daten des Benutzers zu beschädigen** im Abschnitt **Untersuchung des Geräts**.

4. Wählen Sie aus der Liste **Aktion beim Fund einer Bedrohung** eine der folgenden Optionen:

- **Datei löschen und eine Backup-Kopie in der Quarantäne speichern**

Die gefundenen Objekte werden automatisch gelöscht. Der Benutzer muss keine weiteren Aktionen vornehmen. Vor dem Löschen eines Objekts erstellt Kaspersky Endpoint Security für Android eine Sicherungskopie der Datei und speichert sie in Quarantäne.

- **Löschen**

Die gefundenen Objekte werden automatisch gelöscht. Der Benutzer muss keine weiteren Aktionen vornehmen. Vor dem Löschen zeigt Kaspersky Endpoint Security für Android eine kurze Benachrichtigung über den Fund des Objekts an.

- **Überspringen**

Wenn gefundene Objekte übersprungen wurden, warnt Kaspersky Endpoint Security für Android den Benutzer vor Problemen beim Schutz des Geräts. Die Informationen über die übersprungenen Objekte werden im Abschnitt **Status** der App angezeigt. Für jede übersprungene Bedrohung werden die Aktionen angeführt, die der Benutzer ausführen kann, um die Bedrohung zu beseitigen. Die Liste der übersprungenen Objekte kann sich ändern, beispielsweise wenn die schädliche Datei gelöscht oder verschoben wurde. Um die aktuelle Liste der Bedrohungen zu erhalten, starten Sie die vollständige Untersuchung des Geräts. Für einen zuverlässigen Schutz Ihrer Daten entfernen Sie alle gefundenen Objekte.

- **Aktion erfragen**

Kaspersky Endpoint Security für Android gibt eine Benachrichtigung aus, in welcher der Benutzer aufgefordert wird, eine Aktion für das gefundene Objekt auszuwählen: **Überspringen** oder **Löschen**.

Die Option **Aktion erfragen** erlaubt dem Benutzer des Geräts, beim Fund mehrerer Objekte die ausgewählte Aktion mithilfe des Kontrollkästchens **Auf alle Bedrohungen anwenden** für jede Datei auszuführen.



Zur Anzeige der Benachrichtigung auf mobilen Geräten mit Android 10.0 und höher muss Kaspersky Endpoint Security für Android als Bedienungshilfe installiert sein. Der Assistent für die Erstkonfiguration von Kaspersky Endpoint Security für Android ermöglicht dem Benutzer, die App als Bedienungshilfe zu installieren. Der Benutzer kann diesen Schritt überspringen oder den Dienst in den Einstellungen des Geräts später deaktivieren. In diesem Fall zeigt Kaspersky Endpoint Security für Android ein Android-Systemfenster an, in welchem der Benutzer aufgefordert wird, für das gefundene Objekt die Aktion Überspringen oder Löschen auszuwählen. Um die Aktion auf mehrere Objekte anzuwenden, öffnen Sie Kaspersky Endpoint Security.

5. Im Abschnitt **Untersuchung nach Zeitplan** können Sie die automatische vollständige Untersuchung des Gerätedateisystems konfigurieren.

Wählen Sie eine der folgenden Optionen:

- **Deaktiviert**

Der Untersuchung des Gerätedateisystems wird nicht automatisch gestartet.

- **Nach dem Datenbanken-Update**

Das Gerätedateisystem wird nach jedem Update der Antiviren-Datenbank automatisch untersucht.

- **1x täglich**

Das Gerätedateisystem wird jeden Tag automatisch untersucht.

Wenn Sie diese Option auswählen, können Sie auch den Zeitpunkt der Untersuchung im Feld **Startzeit** angeben.

- **jede Woche am**

Das Gerätedateisystem wird einmal pro Woche automatisch untersucht.

Wenn Sie diese Option auswählen, können Sie auch den Wochentag auswählen, an dem die Untersuchung ausgeführt werden soll, indem Sie die Dropdown-Liste verwenden und die Uhrzeit der Untersuchung im Feld **Startzeit** angeben.

Unter Android 12 oder höher führt die App diese Aufgabe möglicherweise später aus, wenn sich das Gerät im Stromsparmodus befindet.

6. Klicken Sie auf die Schaltfläche **Speichern**, um die an der Richtlinie vorgenommenen Änderungen zu speichern und das Fenster mit den Richtlinieneigenschaften zu verlassen.

Die Einstellungen werden nach der nächsten planmäßigen Synchronisierung des Geräts mit Kaspersky Security Center auf dem mobilen Gerät konfiguriert.

## Updates der Antiviren-Datenbanken konfigurieren

Diese Richtlinieneinstellungen können nur für Android-Geräte festgelegt werden.

*So konfigurieren Sie Updates der Antiviren-Datenbanken:*

1. Öffnen Sie das Fenster mit den Richtlinieneigenschaften:

- Wählen Sie im Hauptfenster der Kaspersky Security Center Web Console oder Cloud Console **GERÄTE > RICHTLINIEN & PROFILE** aus. Klicken Sie in der sich öffnenden Liste der Gruppenrichtlinien auf den Namen der Richtlinie, die Sie konfigurieren möchten.
  - Wählen Sie im Hauptfenster der Kaspersky Security Center Web Console oder Cloud Console **GERÄTE > MOBIL > GERÄTE** aus. Klicken Sie auf das mobile Gerät, das unter die Richtlinie fällt, die Sie konfigurieren möchten, und wählen Sie anschließend die Richtlinie auf der Registerkarte **AKTIVE RICHTLINIEN UND RICHTLINIENPROFILE** aus.
2. Wählen Sie im Fenster mit den Richtlinieneigenschaften die Option **PROGRAMMEINSTELLUNGEN > Datenbanken-Update** aus.
3. Passen Sie im Abschnitt **Datenbanken-Update** den Zeitplan für das automatische Update der Datenbanken auf dem Gerät des Benutzers an.

Wählen Sie eine der folgenden Optionen:

- **Deaktiviert**

Die automatischen Updates der Antiviren-Datenbanken werden deaktiviert.

- **1x täglich**

Die Antiviren-Datenbanken werden täglich aktualisiert.

Wenn Sie diese Option wählen, können Sie auch den Zeitpunkt der Aktualisierung in dem Feld **Zeitpunkt des Updates** angeben.

- **1x wöchentlich**

Die Antiviren-Datenbanken werden einmal pro Woche aktualisiert.

Wenn Sie diese Option auswählen, können Sie auch den Zeitpunkt der Aktualisierung im Feld **Zeitpunkt des Updates** und den Wochentag, an dem die Aktualisierung ausgeführt werden soll, in der Dropdown-Liste **Wochentag** angeben.

Unter Android 12 oder höher führt die App diese Aufgabe möglicherweise später aus, wenn sich das Gerät im Stromsparmodus befindet.

4. Legen Sie im Abschnitt **Quelle für das Datenbanken-Update** eine Update-Quelle fest, von der Kaspersky Endpoint Security für Android die Updates für die Antiviren-Datenbanken der App kopieren und installieren soll:

- **Kaspersky-Server**

Kaspersky Endpoint Security für Android verwendet einen Kaspersky-Update-Server als Update-Quelle, um Antiviren-Datenbanken auf das Gerät des Benutzers herunterzuladen.

- **Administrationsserver**

Nur verfügbar, wenn Sie Kaspersky Security Center Web Console verwenden.

Kaspersky Endpoint Security für Android verwendet die Datenverwaltung des Kaspersky Security Center Administrationsservers als Update-Quelle, um Antiviren-Datenbanken auf das Gerät des Benutzers herunterzuladen.

- **Andere Quelle**

Kaspersky Endpoint Security für Android verwendet einen Drittanbieter-Server als Update-Quelle, um Antiviren-Datenbanken auf das Gerät des Benutzers herunterzuladen.

Wenn Sie diese Option auswählen, müssen Sie im Feld **Anderen Server als Update-Quelle für den Download der Antiviren-Datenbanken verwenden** die Adresse eines HTTP-Servers angeben.

5. Damit Kaspersky Endpoint Security für Android das Datenbanken-Update nach dem festgelegten Zeitplan auch dann herunterlädt, wenn sich das Benutzergerät in einer Roaming-Zone befindet, aktivieren Sie im Abschnitt **Antiviren-Datenbanken beim Roaming aktualisieren** das Kontrollkästchen **Datenbanken-Update beim Roaming erlauben**.
6. Klicken Sie auf die Schaltfläche **Speichern**, um die an der Richtlinie vorgenommenen Änderungen zu speichern und das Fenster mit den Richtlinieneigenschaften zu verlassen.

Die Einstellungen werden nach der nächsten planmäßigen Synchronisierung des Geräts mit Kaspersky Security Center auf dem mobilen Gerät konfiguriert.

## Einstellungen zum Entsperren des Geräts konfigurieren

Diese Richtlinieneinstellungen können nur für Android-Geräte festgelegt werden.

Zur Gewährleistung der Sicherheit des mobilen Geräts muss die Verwendung des Kennwortes, das beim Einschalten des Geräts aus dem Schlafmodus abgefragt wird, angepasst werden.

Sie können eine Beschränkung der Benutzertätigkeit auf einem Gerät festlegen, für das ein zu einfaches Kennwort zum Entsperren festgelegt wurde (z. B. Gerät sperren). Diese Beschränkung können Sie mithilfe der Komponente zur [Übereinstimmungsüberprüfung](#) definieren.

Auf einigen Samsung-Geräten mit dem Betriebssystem Android 7.0 und höher kann das Gerät gesperrt werden, wenn der Benutzer versucht, das Gerät mit einer nicht unterstützten Methode zu entsperren (z. B. mit Sperrmuster), und folgende Bedingungen erfüllt sind: [Der Schutz vor Deinstallation für Kaspersky Endpoint Security für Android ist aktiviert](#) und [die Anforderungen an die Stärke des Kennworts zum Entsperren des Geräts sind festgelegt](#). Zum Entsperren muss ein bestimmter Befehl an das Gerät gesendet werden.

*So passen Sie Stärke für das Passwort zum Entsperren an:*

1. Öffnen Sie das Fenster mit den Richtlinieneigenschaften:
  - Wählen Sie im Hauptfenster der Kaspersky Security Center Web Console oder Cloud Console **GERÄTE > RICHTLINIEN & PROFILE** aus. Klicken Sie in der sich öffnenden Liste der Gruppenrichtlinien auf den Namen der Richtlinie, die Sie konfigurieren möchten.
  - Wählen Sie im Hauptfenster der Kaspersky Security Center Web Console oder Cloud Console **GERÄTE > MOBIL > GERÄTE** aus. Klicken Sie auf das mobile Gerät, das unter die Richtlinie fällt, die Sie konfigurieren möchten, und wählen Sie anschließend die Richtlinie auf der Registerkarte **AKTIVE RICHTLINIEN UND RICHTLINIENPROFILE** aus.
2. Wählen Sie im Fenster mit den Richtlinieneigenschaften die Option **PROGRAMMEINSTELLUNGEN > Basisschutz** aus.
3. Wenn Sie möchten, dass die App prüft, ob ein Kennwort für das Entsperren des Geräts vorhanden ist, aktivieren Sie im Abschnitt **Zum Festlegen eines Passworts für das Entsperren des Bildschirms auffordern** die Option **Passwortschutz**.

Wenn die Anwendung feststellt, dass auf dem Gerät kein Kennwort vorhanden ist, wird der Benutzer aufgefordert, ein Kennwort festzulegen. Das Kennwort wird unter Berücksichtigung der vom Administrator angegebenen Einstellungen festgelegt.

4. Geben Sie die Mindestanzahl von Zeichen im Kennwort des Benutzers an.

Mögliche Werte: 4 bis 16 Zeichen.

Standardmäßig enthält das Benutzerkennwort 4 Zeichen.

Auf Geräten mit Android 10.0 oder später löst Kaspersky Endpoint Security die Anforderungen an die Zuverlässigkeit des Kennworts in einen der Systemwerte auf: Mittel oder Hoch.

Die Werte für Geräte mit Android 10.0 oder höher werden mithilfe der folgenden Regeln bestimmt:

- Wenn eine Kennwortlänge von 1 bis 4 Zeichen erforderlich ist, fordert die App den Benutzer auf, ein Kennwort mittlerer Stärke festzulegen. Dieses muss entweder numerisch (PIN) ohne wiederholte oder aufeinanderfolgende (z. B. 1234) Sequenzen oder alphanumerisch sein. PIN oder Kennwort müssen mindestens 4 Zeichen lang sein.
- Wenn eine Kennwortlänge von 5 oder mehr Zeichen erforderlich ist, fordert die App den Benutzer auf, ein Kennwort hoher Stärke festzulegen. Dieses muss entweder numerisch (PIN) ohne wiederholte oder aufeinanderfolgende Sequenzen oder alphanumerisch (Kennwort) sein. Die PIN muss mindestens 8 Zeichen lang sein, das Kennwort muss mindestens 6 Zeichen lang sein.

5. Wenn Sie möchten, dass der Benutzer Fingerabdrücke zum Entsperren des Bildschirms verwenden kann, aktivieren Sie das Kontrollkästchen **Verwendung von Fingerabdruck erlauben (für Geräte mit Android 9 oder niedriger)**. Wenn das Kennwort zum Entsperren nicht den Anforderungen an die Unternehmenssicherheit entspricht, ist es nicht möglich, den Fingerabdruckscanner zum Entsperren des Bildschirms zu verwenden.

Auf Geräten mit Android 10.0 oder höher wird die Verwendung eines Fingerabdrucks zum Entsperren des Bildschirms nicht unterstützt.

Kaspersky Endpoint Security für Android beschränkt nicht die Nutzung des Fingerabdruckscanners für die Anmeldung in Apps oder die Bestätigung von Käufen.

Auf einigen Samsung-Geräten ist es nicht möglich, die Verwendung von Fingerabdrücken zum Entsperren des Bildschirms zu verbieten.

Außerdem verbietet Kaspersky Endpoint Security für Android auf einigen Samsung-Geräten, auf denen das Kennwort zum Entsperren nicht den Anforderungen an die Unternehmenssicherheit entspricht, die Nutzung der Fingerabdrücke für das Entsperren des Bildschirms nicht.

Nach dem Hinzufügen eines Fingerabdrucks in den Einstellungen des Geräts kann der Benutzer den Bildschirm auf eine der folgenden Arten entsperren:

- Finger auf den Fingerabdruckscanner legen – Standardmethode.
- Kennwort für das Entsperren eingeben – alternative Methode.

6. Klicken Sie auf die Schaltfläche **Speichern**, um die an der Richtlinie vorgenommenen Änderungen zu speichern und das Fenster mit den Richtlinieneigenschaften zu verlassen.

Die Einstellungen werden nach der nächsten planmäßigen Synchronisierung des Geräts mit Kaspersky Security Center auf dem mobilen Gerät konfiguriert.

## Datenschutz bei Verlust oder Diebstahl des Geräts konfigurieren

Diese Richtlinieneinstellungen können nur für Android-Geräte festgelegt werden.

Um Unternehmensdaten bei Verlust oder Diebstahl eines Mobilgeräts zu schützen, müssen Sie den Schutz vor unbefugtem Zugriff konfigurieren.

Um den Schutz vor gestohlenen oder verlorenen Gerätedaten zu gewährleisten, muss Kaspersky Endpoint Security für Android als Bedienungshilfe eingerichtet sein. Der Assistent für die Erstkonfiguration von Kaspersky Endpoint Security für Android ermöglicht dem Benutzer, die App als Bedienungshilfe zu installieren. Der Benutzer kann diesen Schritt überspringen oder den Dienst in den Einstellungen des Geräts später deaktivieren.

*So konfigurieren Sie den Datenschutz bei Verlust oder Diebstahl des Geräts:*

1. Öffnen Sie das Fenster mit den Richtlinieneigenschaften:

- Wählen Sie im Hauptfenster der Kaspersky Security Center Web Console oder Cloud Console **GERÄTE > RICHTLINIEN & PROFILE** aus. Klicken Sie in der sich öffnenden Liste der Gruppenrichtlinien auf den Namen der Richtlinie, die Sie konfigurieren möchten.
- Wählen Sie im Hauptfenster der Kaspersky Security Center Web Console oder Cloud Console **GERÄTE > MOBIL > GERÄTE** aus. Klicken Sie auf das mobile Gerät, das unter die Richtlinie fällt, die Sie konfigurieren möchten, und wählen Sie anschließend die Richtlinie auf der Registerkarte **AKTIVE RICHTLINIEN UND RICHTLINIENPROFILE** aus.

2. Wählen Sie im Fenster mit den Richtlinieneigenschaften die Option **PROGRAMMEINSTELLUNGEN > Basisschutz** aus.

3. Konfigurieren Sie die Gerätesperre im Abschnitt **Diebstahlschutz**:

- Geben Sie die Anzahl der Zeichen im Entsperrcode an.
- Geben Sie den Text an, der angezeigt werden soll, wenn das Gerät gesperrt ist.

4. Klicken Sie auf die Schaltfläche **Speichern**, um die an der Richtlinie vorgenommenen Änderungen zu speichern und das Fenster mit den Richtlinieneigenschaften zu verlassen.

Die Einstellungen werden nach der nächsten planmäßigen Synchronisierung des Geräts mit Kaspersky Security Center auf dem mobilen Gerät konfiguriert.

## Anwendungskontrolle konfigurieren

Diese Richtlinieneinstellungen können nur für Android-Geräte festgelegt werden.

Die *Anwendungskontrolle* führt eine Untersuchung der auf dem mobilen Gerät installierten Apps auf Übereinstimmung mit den Anforderungen an die Unternehmenssicherheit durch. Der Administrator erstellt in Kaspersky Security Center entsprechend den Anforderungen an die Unternehmenssicherheit Listen von erlaubten, verbotenen, obligatorischen und empfohlenen Apps. Nach der Ausführung der Anwendungskontrolle bietet Kaspersky Endpoint Security dem Benutzer an, obligatorische und empfohlene Apps zu installieren sowie verbotene zu löschen. Verbotene Apps können nicht auf dem mobilen Gerät des Benutzers gestartet werden.

In der Kaspersky Security Center Web Console und Cloud Console können Sie Apps auf den Geräten der Benutzer verwalten, indem Sie vordefinierte Regeln anwenden. Sie können zwei Arten der **Anwendungskontrolle** konfigurieren: App-Regeln und Kategorieregeln.

Eine **App-Regel** wird auf eine bestimmte App angewendet, während eine **Kategorieregel** auf jede App angewendet wird, die zu einer vordefinierten Kategorie gehört. App-Kategorien werden von Kaspersky-Experten festgelegt.

*So konfigurieren Sie die **Anwendungskontrolle**:*

1. Öffnen Sie das Fenster mit den Richtlinieneigenschaften:

- Wählen Sie im Hauptfenster der Kaspersky Security Center Web Console oder Cloud Console **GERÄTE > RICHTLINIEN & PROFILE** aus. Klicken Sie in der sich öffnenden Liste der Gruppenrichtlinien auf den Namen der Richtlinie, die Sie konfigurieren möchten.
- Wählen Sie im Hauptfenster der Kaspersky Security Center Web Console oder Cloud Console **GERÄTE > MOBIL > GERÄTE** aus. Klicken Sie auf das mobile Gerät, das unter die Richtlinie fällt, die Sie konfigurieren möchten, und wählen Sie anschließend die Richtlinie auf der Registerkarte **AKTIVE RICHTLINIEN UND RICHTLINIENPROFILE** aus.

2. Wählen Sie auf der Seite mit den Richtlinieneigenschaften die Option **PROGRAMMEINSTELLUNGEN > Sicherheitskontrolle** aus.

3. Fügen Sie in der Tabelle unter dem Abschnitt **Anwendungskontrolle** Regeln hinzu, die definieren, welche Apps kontrolliert werden.

- So fügen Sie eine Regel für eine bestimmte App hinzu:
  - a. Klicken Sie in der Tabelle auf **App-Regel**.
  - b. Wählen Sie im sich öffnenden Fenster **App-Regel** die anzuwendende Aktion für die Apps aus, die von der erstellten Regel abgedeckt werden.
  - c. Geben Sie die App an, die der Regel unterliegt, indem Sie den **Link zum Installationspaket** (z. B. <https://play.google.com/store/apps/details?id=com.kaspersky.kes>), den **Paketname** (z. B. **katana.facebook.com**) und **App-Name** ausfüllen.
  - d. Klicken Sie auf **Speichern**.

Die Regel wird der Liste mit Regeln der **Anwendungskontrolle** hinzugefügt.

- So fügen Sie eine Regel für eine App-Kategorie hinzu:
  - a. Klicken Sie in der Tabelle im Abschnitt **Anwendungskontrolle** auf **Kategorieregel**.
  - b. Wählen Sie im sich öffnenden Fenster **Kategorieregel** die App-Kategorie aus der Dropdown-Liste aus.

Apps innerhalb der ausgewählten Kategorie unterliegen der erstellten Regel.

- c. Wählen Sie im Abschnitt **Betriebsmodus** die auszuführende Aktion für startende Apps der ausgewählten Kategorie aus: **Verbotene Apps** oder **Erlaubte Apps**.
- d. Füllen Sie, falls erforderlich, folgendes Feld aus: **Zusätzlicher Kommentar, der beim Fund einer App aus einer bestimmten Kategorie auf dem Benutzergerät angezeigt wird**.
- e. Klicken Sie auf **Speichern**.

Die Regel wird der Liste mit Regeln der **Anwendungskontrolle** hinzugefügt.

4. Wählen Sie im Abschnitt **Aktionen für verbotene Apps** aus, welche Aktion für verbotene Anwendungen ausgeführt wird:
- Wenn Kaspersky Endpoint Security für Android den Start verbotener Anwendungen auf dem Mobilgerät des Benutzers blockieren soll, wählen Sie **App-Start blockieren**.
  - Damit Kaspersky Endpoint Security für Android Daten über verbotene Anwendungen ins Ereignisprotokoll sendet, ohne sie zu blockieren, aktivieren Sie **Verbotene Apps nicht blockieren, nur benachrichtigen**.
5. Wählen Sie im Abschnitt **Betriebsmodus** aus, ob die von Ihnen hinzugefügten Regeln erlaubte oder verbotene Apps definieren:
- Wenn die Regeln festlegen sollen, welche Apps zulässig sind, wählen Sie **Verbotene Apps** aus.  
Damit Kaspersky Endpoint Security für Android den Start von Systemanwendungen auf dem mobilen Gerät im Modus **Verbotene Apps** blockiert (z. B. Kalender, Kamera, Einstellungen), aktivieren Sie das Kontrollkästchen **System-Apps sperren**.

Die Experten Kaspersky empfehlen nicht, die Systemanwendungen zu sperren, da es zu den Störungen in der Arbeit des Geräts bringen kann.

- Wenn die Regeln festlegen sollen, welche Apps verboten sind, wählen Sie **Erlaubte Apps** aus.
6. Um Informationen über alle auf Mobilgeräten installierten Apps zu erhalten, aktivieren Sie im Abschnitt **App-Bericht** das Kontrollkästchen **Eine Liste der installierten Apps auf allen mobilen Geräten senden**.  
Kaspersky Endpoint Security für Android sendet jedes Mal nach der Installation oder dem Löschen einer Anwendung vom Gerät die Daten ins Ereignisprotokoll.
7. Klicken Sie auf die Schaltfläche **Speichern**, um die an der Richtlinie vorgenommenen Änderungen zu speichern und das Fenster mit den Richtlinieneigenschaften zu verlassen.

Die Einstellungen werden nach der nächsten planmäßigen Synchronisierung des Geräts mit Kaspersky Security Center auf dem mobilen Gerät konfiguriert.

## Übereinstimmungsüberprüfung für mobile Geräte hinsichtlich der korporativen Sicherheit konfigurieren

Diese Richtlinieneinstellungen können nur für Android-Geräte festgelegt werden.



Mit der Übereinstimmungsüberprüfung können Sie Android-Geräte auf Einhaltung der Anforderungen an die Unternehmenssicherheit überwachen und bei fehlender Übereinstimmung Maßnahmen ergreifen. Die Anforderungen der korporativen Sicherheit regeln die Arbeit der Benutzer mit den Geräten. Auf dem Gerät muss beispielsweise der Echtzeitschutz aktiviert sein, die Antiviren-Datenbanken müssen aktuell sein und das Kennwort des Geräts muss hinreichend komplex sein. Die Übereinstimmungsüberprüfung funktioniert auf der Grundlage einer Liste von Regeln. Eine Übereinstimmungsregel besteht aus folgenden Komponenten:

- [Kriterium für fehlende Übereinstimmung des Geräts](#).
- [Aktion, die für das Gerät ausgeführt wird](#), wenn der Benutzer die fehlende Übereinstimmung nicht im Laufe der angegebenen Zeitspanne behebt (z. B. Sperre des Geräts).
- Zeitspanne, die dem Benutzer des Geräts zur Beseitigung von Abweichungen zur Verfügung steht (z. B. 24 Stunden).

Nach Ablauf des angegebenen Zeitraums wird die ausgewählte Aktion auf dem Gerät des Benutzers ausgeführt.

Unter Android 12 oder höher führt die App diese Aufgabe möglicherweise später aus, wenn sich das Gerät im Stromsparmodus befindet.

Um die Übereinstimmungsüberprüfung zu konfigurieren, können Sie die folgenden Aktionen ausführen:

- [Vorhandene Übereinstimmungsregeln aktivieren oder deaktivieren](#).
- [Eine vorhandene Übereinstimmungsregel anpassen](#).
- [Eine neue Regel hinzufügen](#).
- [Eine Regel löschen](#).

## Übereinstimmungsregeln aktivieren und deaktivieren

Diese Richtlinieneinstellungen können nur für Android-Geräte festgelegt werden.

*So aktivieren oder deaktivieren Sie auf mobilen Geräten vorhandene Regeln zur Übereinstimmungsüberprüfung für die Anforderungen an die Unternehmenssicherheit:*

1. Öffnen Sie das Fenster mit den Richtlinieneigenschaften:

- Wählen Sie im Hauptfenster der Kaspersky Security Center Web Console oder Cloud Console **GERÄTE > RICHTLINIEN & PROFILE** aus. Klicken Sie in der sich öffnenden Liste der Gruppenrichtlinien auf den Namen der Richtlinie, die Sie konfigurieren möchten.
- Wählen Sie im Hauptfenster der Kaspersky Security Center Web Console oder Cloud Console **GERÄTE > MOBIL > GERÄTE** aus. Klicken Sie auf das mobile Gerät, das unter die Richtlinie fällt, die Sie konfigurieren möchten, und wählen Sie anschließend die Richtlinie auf der Registerkarte **AKTIVE RICHTLINIEN UND RICHTLINIENPROFILE** aus.

2. Wählen Sie auf der Seite mit den Richtlinieneigenschaften die Option **PROGRAMMEINSTELLUNGEN > Sicherheitskontrolle** aus.



3. Aktivieren oder deaktivieren Sie im Abschnitt **Übereinstimmungsüberprüfung** die vorhandenen Übereinstimmungsregeln, indem Sie die Umschalter in der Spalte **Status** verwenden.
4. Klicken Sie auf die Schaltfläche **Speichern**, um die an der Richtlinie vorgenommenen Änderungen zu speichern und das Fenster mit den Richtlinieneigenschaften zu verlassen.

Die Einstellungen werden nach der nächsten planmäßigen Synchronisierung des Geräts mit Kaspersky Security Center auf dem mobilen Gerät konfiguriert.

## Übereinstimmungsregeln anpassen

Diese Richtlinieneinstellungen können nur für Android-Geräte festgelegt werden.

*So passen Sie eine Regel zur Prüfung der Übereinstimmung von Mobilgeräten mit den Anforderungen an die Unternehmenssicherheit an:*

1. Öffnen Sie das Fenster mit den Richtlinieneigenschaften:
  - Wählen Sie im Hauptfenster der Kaspersky Security Center Web Console oder Cloud Console **GERÄTE > RICHTLINIEN & PROFILE** aus. Klicken Sie in der sich öffnenden Liste der Gruppenrichtlinien auf den Namen der Richtlinie, die Sie konfigurieren möchten.
  - Wählen Sie im Hauptfenster der Kaspersky Security Center Web Console oder Cloud Console **GERÄTE > MOBIL > GERÄTE** aus. Klicken Sie auf das mobile Gerät, das unter die Richtlinie fällt, die Sie konfigurieren möchten, und wählen Sie anschließend die Richtlinie auf der Registerkarte **AKTIVE RICHTLINIEN UND RICHTLINIENPROFILE** aus.
2. Wählen Sie auf der Seite mit den Richtlinieneigenschaften die Option **PROGRAMMEINSTELLUNGEN > Sicherheitskontrolle** aus.
3. Wählen Sie im Abschnitt **Übereinstimmungsüberprüfung** die Regel aus, die Sie anpassen möchten, und klicken Sie dann auf **Ändern**.
4. Passen Sie im folgenden Fenster **Regel** die Regel folgendermaßen an:
  - a. Konfigurieren Sie für die Regel in der Spalte **Aktion** die Liste der [Aktionen, die bei fehlender Übereinstimmung ausgeführt werden](#), indem Sie neue Aktionen hinzufügen, die vorhandenen Aktionen bearbeiten oder löschen.
  - b. Geben Sie optional den Zeitraum an, in dem ein Benutzer die fehlende Übereinstimmung beheben kann, indem Sie für jede Aktion die Spalte **Zeit für die Beseitigung** verwenden.
  - c. Klicken Sie auf die Schaltfläche **Speichern**, um die Regel zu speichern.
5. Klicken Sie auf die Schaltfläche **Speichern**, um die an der Richtlinie vorgenommenen Änderungen zu speichern und das Fenster mit den Richtlinieneigenschaften zu verlassen.

Die Einstellungen werden nach der nächsten planmäßigen Synchronisierung des Geräts mit Kaspersky Security Center auf dem mobilen Gerät konfiguriert.

## Übereinstimmungsregeln hinzufügen

Diese Richtlinieneinstellungen können nur für Android-Geräte festgelegt werden.

*So fügen Sie eine Regel zur Prüfung der Übereinstimmung von Mobilgeräten mit den Anforderungen an die Unternehmenssicherheit hinzu:*

1. Öffnen Sie das Fenster mit den Richtlinieneigenschaften:
  - Wählen Sie im Hauptfenster der Kaspersky Security Center Web Console oder Cloud Console **GERÄTE > RICHTLINIEN & PROFILE** aus. Klicken Sie in der sich öffnenden Liste der Gruppenrichtlinien auf den Namen der Richtlinie, die Sie konfigurieren möchten.
  - Wählen Sie im Hauptfenster der Kaspersky Security Center Web Console oder Cloud Console **GERÄTE > MOBIL > GERÄTE** aus. Klicken Sie auf das mobile Gerät, das unter die Richtlinie fällt, die Sie konfigurieren möchten, und wählen Sie anschließend die Richtlinie auf der Registerkarte **AKTIVE RICHTLINIEN UND RICHTLINIENPROFILE** aus.
2. Wählen Sie auf der Seite mit den Richtlinieneigenschaften die Option **PROGRAMMEINSTELLUNGEN > Sicherheitskontrolle** aus.
3. Klicken Sie im Abschnitt **Übereinstimmungsüberprüfung** auf **Regel**.
4. Definieren Sie im folgenden Fenster **Regel** die Regel wie folgt:
  - a. Wählen Sie das [Kriterium für fehlende Übereinstimmung](#) für die Regel aus.
  - b. Klicken Sie auf **Hinzufügen** und wählen Sie für die Regel in der Spalte **Aktion** die [Aktion, die bei fehlender Übereinstimmung ausgeführt wird](#) aus.  
Sie können mehrere Aktionen hinzufügen.
  - c. Geben Sie den Zeitraum an, in dem ein Benutzer die Nichteinhaltung beheben kann, indem Sie für jede Aktion die Spalte **Zeit für die Beseitigung** verwenden.
  - d. Klicken Sie auf die Schaltfläche **Speichern**, um die Regel zu speichern.
5. Klicken Sie auf die Schaltfläche **Speichern**, um die an der Richtlinie vorgenommenen Änderungen zu speichern und das Fenster mit den Richtlinieneigenschaften zu verlassen.

Die Einstellungen werden nach der nächsten planmäßigen Synchronisierung des Geräts mit Kaspersky Security Center auf dem mobilen Gerät konfiguriert.

## Übereinstimmungsregeln löschen

Diese Richtlinieneinstellungen können nur für Android-Geräte festgelegt werden.

So löschen Sie eine Regel zur Prüfung der Übereinstimmung von Mobilgeräten mit den Anforderungen an die Unternehmenssicherheit:

1. Öffnen Sie das Fenster mit den Richtlinieneigenschaften:

- Wählen Sie im Hauptfenster der Kaspersky Security Center Web Console oder Cloud Console **GERÄTE > RICHTLINIEN & PROFILE** aus. Klicken Sie in der sich öffnenden Liste der Gruppenrichtlinien auf den Namen der Richtlinie, die Sie konfigurieren möchten.
- Wählen Sie im Hauptfenster der Kaspersky Security Center Web Console oder Cloud Console **GERÄTE > MOBIL > GERÄTE** aus. Klicken Sie auf das mobile Gerät, das unter die Richtlinie fällt, die Sie konfigurieren möchten, und wählen Sie anschließend die Richtlinie auf der Registerkarte **AKTIVE RICHTLINIEN UND RICHTLINIENPROFILE** aus.

2. Wählen Sie auf der Seite mit den Richtlinieneigenschaften die Option **PROGRAMMEINSTELLUNGEN > Sicherheitskontrolle** aus.

3. Wählen Sie im Abschnitt **Übereinstimmungsüberprüfung** die Regel aus, die Sie löschen möchten, und klicken Sie anschließend auf **Löschen**.

4. Klicken Sie auf die Schaltfläche **Speichern**, um die an der Richtlinie vorgenommenen Änderungen zu speichern und das Fenster mit den Richtlinieneigenschaften zu verlassen.

Die Einstellungen werden nach der nächsten planmäßigen Synchronisierung des Geräts mit Kaspersky Security Center auf dem mobilen Gerät konfiguriert.

## Liste mit Kriterien für fehlende Übereinstimmung

Diese Richtlinieneinstellungen können nur für Android-Geräte festgelegt werden.

Um sicherzustellen, dass ein Android-Gerät die Anforderungen an die Unternehmenssicherheit erfüllt, kann Kaspersky Endpoint Security für Android das Gerät anhand der folgenden Kriterien überprüfen:

- **Der Echtzeitschutz ist deaktiviert.**

Der Echtzeitschutz muss aktiviert sein.

Weitere Informationen zur Konfiguration des Echtzeitschutzes finden Sie im Abschnitt "[Echtzeitschutz konfigurieren](#)".

- **Antiviren-Datenbanken sind veraltet.**

Die Antiviren-Datenbank von Kaspersky Endpoint Security für Android muss regelmäßig aktualisiert werden.

Weitere Informationen zur Konfiguration der Einstellungen für die Updates der Antiviren-Datenbank finden Sie im Abschnitt "[Antivirenschutz konfigurieren](#)".

- **Verbotene Apps wurden installiert.**

Auf dem Gerät dürfen keine Apps installiert sein, die entsprechend des Abschnitts **Anwendungskontrolle** die Klassifikation **Start blockieren** erhalten haben.

Weitere Informationen zum Erstellen von Regeln für Apps finden Sie im Abschnitt "[Anwendungskontrolle konfigurieren](#)".

- **Apps aus verbotenen Kategorien sind installiert.**

Auf dem Gerät dürfen keine Apps installiert sein, die unter eine Kategorie fallen, die entsprechend des Abschnitts **Anwendungskontrolle** die Klassifikation **Start blockieren** erhalten hat.

Weitere Informationen zum Erstellen von Regeln für Programmkategorien finden Sie im Abschnitt "[Anwendungskontrolle konfigurieren](#)".

- **Nicht alle benötigten Apps sind installiert.**

Auf dem Gerät müssen bestimmte Apps installiert sein, die entsprechend des Abschnitts **Anwendungskontrolle** die Klassifikation **Installation erzwingen** erhalten haben.

Weitere Informationen zum Erstellen von Regeln für Apps finden Sie im Abschnitt "[Anwendungskontrolle konfigurieren](#)".

- **Die Version des Betriebssystems ist veraltet.**

Das Gerät muss über eine zulässige Version des Betriebssystems verfügen.

Um dieses Kriterium fehlender Übereinstimmung zu verwenden, müssen Sie die Spanne der zulässigen Betriebssystemversionen in den Dropdown-Listen **Niedrigste Betriebssystemversion** und **Höchste Betriebssystemversion** angeben.

- **Das Gerät wurde lange nicht mehr synchronisiert.**

Das Gerät muss regelmäßig mit dem Administrationsserver synchronisiert werden.

Um dieses Kriterium fehlender Übereinstimmung zu verwenden, müssen Sie in der Dropdown-Liste **Synchronisierungsintervall** das maximale Zeitintervall zwischen den Gerätesynchronisierungen angeben.

- **Auf dem Gerät wurden root-Rechte empfangen.**

Das Gerät darf nicht gerootet werden.

Weitere Informationen finden Sie im Abschnitt "[Gehackte Geräte erkennen \(root\)](#)".

- **Das Passwort zum Entsperren entspricht nicht den Anforderungen des Unternehmens.**

Das Gerät muss mit einem Passwort zum Entsperren geschützt werden, das den [Anforderungen an die Stärke des Passworts zum Entsperren](#) entspricht.

## Liste der Maßnahmen bei fehlender Übereinstimmung

Diese Richtlinieneinstellungen können nur für Android-Geräte festgelegt werden.

Die folgende Aktionen sind verfügbar, wenn der Benutzer die fehlende Übereinstimmung nicht innerhalb des angegebenen Zeitraums behebt:

- **Alle Apps blockieren, außer System-Apps.**

Der Start aller Apps auf dem mobilen Gerät des Benutzers wird verboten, mit Ausnahme von System-Apps.

- **Gerät sperren.**

Das mobile Gerät ist blockiert. Um Zugriff auf die Daten zu erhalten, muss [das Gerät entsperrt werden](#). Wenn der Grund für die Sperrung nach der Entsperrung des Geräts nicht beseitigt wurde, wird das Gerät nach einem festgelegten Zeitraum wieder gesperrt.

- **Unternehmensdaten löschen.**

Löschen Sie containerisierte Daten, E-Mail-Konten des Unternehmens, Verbindungseinstellungen von WLAN und VPN des Unternehmens sowie die Zugangspunktnamen (APN).

- **Gerät auf Werkseinstellungen zurücksetzen.**

Alle Daten wurden vom mobilen Gerät gelöscht, die Einstellungen des mobilen Geräts wurden auf Werkseinstellungen zurückgesetzt.

## Benutzerzugriff auf Websites anpassen

Diese Richtlinieneinstellungen können für Android- und iOS-Geräte festgelegt werden.

Um persönliche Daten und Unternehmensdaten zu schützen, die beim Surfen im Internet auf Mobilgeräten gespeichert werden, können Sie den Website-Zugriff der Benutzer mithilfe des Web-Filters konfigurieren. Der Web-Filter untersucht Websites, bevor ein Benutzer sie öffnet, und blockiert anschließend Websites, die bösartigen Code verbreiten, und Phishing-Websites, die vertrauliche Daten stehlen und Zugriff auf Finanzkonten erlangen wollen.

Für Android-Geräte unterstützt diese Funktion auch die Filterung von Websites nach den Kategorien, die im Cloud-Dienst [Kaspersky Security Network](#) festgelegt sind. Die Filterung ermöglicht Ihnen, den Zugriff auf einzelne Websites oder bestimmte Website-Kategorien einzuschränken (z. B. auf Websites aus der Kategorie "**Glücksspiel, Lotterien, Wetten**" oder "**Kommunikation im Internet**").

Auf Android-Geräten funktioniert der Web-Filter nur in den Browsern Google Chrome, Huawei Browser und Samsung Internet Browser.

Um einen ordnungsgemäßen Betrieb des Web-Filters zu gewährleisten, muss Kaspersky Endpoint Security für Android als Bedienungshilfe installiert sein. Der Assistent für die Erstkonfiguration von Kaspersky Endpoint Security für Android ermöglicht dem Benutzer, die App als Bedienungshilfe zu installieren. Der Benutzer kann diesen Schritt überspringen oder den Dienst in den Einstellungen des Geräts später deaktivieren.

Auf iOS-Geräten muss der Benutzer der App "Kaspersky Security für iOS" erlauben, eine VPN-Konfiguration für den Web-Filter hinzuzufügen.

*So konfigurieren Sie den Benutzerzugriff auf Web-Sites:*

1. Öffnen Sie das Fenster mit den Richtlinieneigenschaften:
  - Wählen Sie im Hauptfenster der Kaspersky Security Center Web Console oder Cloud Console **GERÄTE > RICHTLINIEN & PROFILE** aus. Klicken Sie in der sich öffnenden Liste der Gruppenrichtlinien auf den Namen der Richtlinie, die Sie konfigurieren möchten.
  - Wählen Sie im Hauptfenster der Kaspersky Security Center Web Console oder Cloud Console **GERÄTE > MOBIL > GERÄTE** aus. Klicken Sie auf das mobile Gerät, das unter die Richtlinie fällt, die Sie konfigurieren möchten, und wählen Sie anschließend die Richtlinie auf der Registerkarte **AKTIVE RICHTLINIEN UND RICHTLINIENPROFILE** aus.
2. Wählen Sie auf der Seite mit den Richtlinieneigenschaften die Option **PROGRAMMEINSTELLUNGEN > Sicherheitskontrolle** aus.
3. Aktivieren Sie im Abschnitt **Web-Filter** das Kontrollkästchen **Web-Filter aktivieren**, um die Funktion einzuschalten.
4. Für Android-Geräte können Sie eine der folgenden Optionen auswählen:

- So beschränken Sie den Benutzerzugriff auf Websites basierend auf deren Inhalten:
  - a. Wählen Sie **Websites der angegebenen Kategorien blockieren** aus.
  - b. Aktivieren Sie die Kontrollkästchen neben den Kategorien von Websites, auf die Kaspersky Endpoint Security für Android den Zugriff blockieren soll.

Wenn der Web-Filter eingeschaltet ist, wird der Benutzerzugriff auf Websites der Kategorien **Phishing** und **Websites mit Schadsoftware** immer blockiert.

- So geben Sie die Liste der erlaubten Websites an:
    - a. Wählen Sie **Nur die angegebenen Websites erlauben** aus.
    - b. Erstellen Sie eine Liste der Websites, indem Sie Adressen von Websites hinzufügen, auf welche die App den Zugriff nicht beschränken soll. Kaspersky Endpoint Security für Android unterstützt nur reguläre Ausdrücke. Geben Sie die Adresse der erlaubten Website nach einem der folgenden Muster ein:
      - `http:\\\\www\\.example\\.com.*` – alle untergeordneten Seiten der Website (beispielsweise `http://www.example.com/about`) sind erlaubt.
      - `https:\\\\.*example\\.com` – alle Subdomains der Website (beispielsweise `https://pictures.example.com`) sind erlaubt.
    - c. Sie können auch den Ausdruck `https?` verwenden, um HTTP und HTTPS auszuwählen. Weitere Informationen über reguläre Ausdrücke finden Sie auf der Seite [des technischen Supports von Oracle](#).
  - Um den Benutzerzugriff auf alle Websites zu blockieren, wählen Sie **Alle Websites blockieren** aus.
5. Klicken Sie auf die Schaltfläche **Speichern**, um die an der Richtlinie vorgenommenen Änderungen zu speichern und das Fenster mit den Richtlinieneigenschaften zu verlassen.

Die Einstellungen werden nach der nächsten planmäßigen Synchronisierung des Geräts mit Kaspersky Security Center auf dem mobilen Gerät konfiguriert.

## Einschränkungen für Funktionen konfigurieren

Diese Richtlinieneinstellungen können nur für Android-Geräte festgelegt werden.

Mit der Kaspersky Security Center Web Console können Sie den Benutzerzugriff auf die folgenden Funktionen mobiler Geräte konfigurieren:

- WLAN
- Kamera
- Bluetooth

Standardmäßig darf der Benutzer auf dem Geräte die Kamera, WLAN und Bluetooth ohne Beschränkungen verwenden.

Um die Beschränkung der Verwendung der Funktionen Kamera, WLAN und Bluetooth auf dem Gerät anzupassen, gehen Sie wie folgt vor:

1. Öffnen Sie das Fenster mit den Richtlinieneigenschaften:

- Wählen Sie im Hauptfenster der Kaspersky Security Center Web Console oder Cloud Console **GERÄTE > RICHTLINIEN & PROFILE** aus. Klicken Sie in der sich öffnenden Liste der Gruppenrichtlinien auf den Namen der Richtlinie, die Sie konfigurieren möchten.
- Wählen Sie im Hauptfenster der Kaspersky Security Center Web Console oder Cloud Console **GERÄTE > MOBIL > GERÄTE** aus. Klicken Sie auf das mobile Gerät, das unter die Richtlinie fällt, die Sie konfigurieren möchten, und wählen Sie anschließend die Richtlinie auf der Registerkarte **AKTIVE RICHTLINIEN UND RICHTLINIENPROFILE** aus.

2. Wählen Sie auf der Seite mit den Richtlinieneigenschaften die Option **PROGRAMMEINSTELLUNGEN > Sicherheitskontrolle** aus.

3. Passen Sie im Block **Funktionsverwaltung** die Verwendung von WLAN, Kamera und Bluetooth an:

- Um das WLAN-Modul auf dem mobilen Gerät des Benutzers auszuschalten, aktivieren Sie das Kontrollkästchen **Verwendung von WLAN verbieten**.

Auf Geräten mit Android 10.0 oder höher wird das Verbot der Verwendung von WLAN-Netzwerken nicht unterstützt.

- Um die Kamera auf dem mobilen Gerät des Benutzers auszuschalten, aktivieren Sie das Kontrollkästchen **Kameraverwendung verbieten**.

Auf Geräten mit Android 10.0 oder höher kann die Nutzung der Kamera nicht vollständig verboten werden.

Auf Geräten mit dem Betriebssystem Android 11 und höher muss Kaspersky Endpoint Security für Android als Dienst für erleichterte Bedienung installiert sein. Der Assistent für die Erstkonfiguration von Kaspersky Endpoint Security für Android ermöglicht dem Benutzer, die App als Bedienungshilfe zu installieren. Der Benutzer kann diesen Schritt überspringen oder den Dienst in den Einstellungen des Geräts später deaktivieren. In einem solchen Fall können Sie die Verwendung der Kamera nicht einschränken.

- Um Bluetooth auf dem mobilen Gerät des Benutzers auszuschalten, aktivieren Sie das Kontrollkästchen **Bluetooth verbieten**.

Auf Android 12 oder höher kann die Verwendung von Bluetooth nur deaktiviert werden, wenn der Gerätebenutzer die Berechtigung **Bluetooth-Geräte in der Nähe** gewährt hat. Der Benutzer kann diese Berechtigung beim Ausführen des Schnellstartassistenten oder später gewähren.

4. Klicken Sie auf die Schaltfläche **Speichern**, um die an der Richtlinie vorgenommenen Änderungen zu speichern und das Fenster mit den Richtlinieneigenschaften zu verlassen.

Die Einstellungen werden nach der nächsten planmäßigen Synchronisierung des Geräts mit Kaspersky Security Center auf dem mobilen Gerät konfiguriert.

# Schutz von Kaspersky Endpoint Security für Android vor Deinstallation

Für den Schutz des mobilen Geräts und die Erfüllung der Anforderungen an die Unternehmenssicherheit können Sie für Kaspersky Endpoint Security für Android den Schutz vor Deinstallation aktivieren. In diesem Fall kann der Benutzer die App unter Verwendung der Oberfläche von Kaspersky Endpoint Security für Android nicht deinstallieren. Beim Deinstallieren der App mithilfe der Tools des Android-Betriebssystems wird dem Benutzer eine Anfrage zum Deaktivieren der Administratorrechte für Kaspersky Endpoint Security für Android angezeigt. Nach dem Deaktivieren der Rechte wird das mobile Gerät gesperrt.

*So aktivieren Sie den Schutz von Kaspersky Endpoint Security für Android vor Deinstallation:*

1. Öffnen Sie das Fenster mit den Richtlinieneigenschaften:

- Wählen Sie im Hauptfenster der Kaspersky Security Center Web Console oder Cloud Console **GERÄTE > RICHTLINIEN & PROFILE** aus. Klicken Sie in der sich öffnenden Liste der Gruppenrichtlinien auf den Namen der Richtlinie, die Sie konfigurieren möchten.
- Wählen Sie im Hauptfenster der Kaspersky Security Center Web Console oder Cloud Console **GERÄTE > MOBIL > GERÄTE** aus. Klicken Sie auf das mobile Gerät, das unter die Richtlinie fällt, die Sie konfigurieren möchten, und wählen Sie anschließend die Richtlinie auf der Registerkarte **AKTIVE RICHTLINIEN UND RICHTLINIENPROFILE** aus.

2. Wählen Sie auf der Seite mit den Richtlinieneigenschaften die Option **PROGRAMMEINSTELLUNGEN > Sicherheitskontrolle** aus.

3. Deaktivieren Sie im Abschnitt **App auf dem mobilen Gerät verwalten** das Kontrollkästchen **Entfernen der App Kaspersky Endpoint Security für Android vom Gerät erlauben**.

Auf den Geräten unter Verwaltung des Betriebssystems Android 7.0 und höher muss zum Schutz der App vor dem Löschen Kaspersky Endpoint Security für Android als Dienst für erleichterte Bedienung installiert sein. Während der Ausführung des Schnellstartassistenten bietet Kaspersky Endpoint Security für Android an, dem Benutzer der App die erforderlichen Berechtigungen bereitzustellen. Der Benutzer kann diese Schritte überspringen oder die Berechtigungen in den Einstellungen des Geräts später deaktivieren. In diesem Fall ist der Schutz der Anwendung vor dem Löschen nicht aktiviert.

4. Klicken Sie auf die Schaltfläche **Speichern**, um die an der Richtlinie vorgenommenen Änderungen zu speichern und das Fenster mit den Richtlinieneigenschaften zu verlassen.

Die Einstellungen werden nach der nächsten planmäßigen Synchronisierung des Geräts mit Kaspersky Security Center auf dem mobilen Gerät konfiguriert.

Beim Versuch, die App zu löschen, wird das mobile Gerät gesperrt.

## Synchronisierung mobiler Geräte mit Kaspersky Security Center konfigurieren

Diese Richtlinieneinstellungen können für Android- und iOS-Geräte festgelegt werden.



Um mobile Geräte verwalten und Berichte oder Statistiken von mobilen Geräten empfangen zu können, müssen die Synchronisierungseinstellungen festgelegt werden. Die Synchronisierung eines mobilen Geräts mit Kaspersky Security Center kann auf folgende Arten erfolgen:

- **Nach Zeitplan.** Die Synchronisierung nach Zeitplan wird mittels HTTP durchgeführt. In den Richtlinieneinstellungen können Sie einen Zeitplan für die Synchronisierung konfigurieren. Änderungen an Richtlinieneinstellungen sowie Befehle und Aufgaben werden erst ausgeführt, wenn mobile Geräte mit Kaspersky Security Center entsprechend dem Zeitplan synchronisiert sind – also mit einer gewissen Verzögerung. Standardmäßig werden die mobilen Endgeräte alle 6 Stunden automatisch mit Kaspersky Security Center synchronisiert.

Unter Android 12 oder höher führt die App diese Aufgabe möglicherweise später aus, wenn sich das Gerät im Stromsparmodus befindet.

- **Erzwungen** (nur für Android-Geräte). Die erzwungene Synchronisierung erfolgt mithilfe von Push-Benachrichtigungen des [FCM-Dienstes \(Firebase Cloud Messaging\)](#). Die erzwungene Synchronisierung ist in erster Linie dafür gedacht, eine rechtzeitige [Übermittlung von Befehlen an das mobile Gerät](#) zu gewährleisten. Wenn Sie die erzwungene Synchronisierung verwenden möchten, stellen Sie sicher, dass die FCM-Einstellungen in Kaspersky Security Center konfiguriert sind.

*So konfigurieren Sie die Synchronisierung von Mobilgeräten mit Kaspersky Security Center:*

1. Öffnen Sie das Fenster mit den Richtlinieneigenschaften:

- Wählen Sie im Hauptfenster der Kaspersky Security Center Web Console oder Cloud Console **GERÄTE > RICHTLINIEN & PROFILE** aus. Klicken Sie in der sich öffnenden Liste der Gruppenrichtlinien auf den Namen der Richtlinie, die Sie konfigurieren möchten.
- Wählen Sie im Hauptfenster der Kaspersky Security Center Web Console oder Cloud Console **GERÄTE > MOBIL > GERÄTE** aus. Klicken Sie auf das mobile Gerät, das unter die Richtlinie fällt, die Sie konfigurieren möchten, und wählen Sie anschließend die Richtlinie auf der Registerkarte **AKTIVE RICHTLINIEN UND RICHTLINIENPROFILE** aus.

2. Wählen Sie auf der Seite mit den Richtlinieneigenschaften **PROGRAMMEINSTELLUNGEN > Synchronisierung** aus.

3. Verwenden Sie im Abschnitt **Synchronisierung mit dem Administrationsserver** die Dropdown-Liste **Synchronisierungsintervall**, um die Synchronisierungszeit zu wählen.

Standardmäßig wird die Synchronisierung alle sechs Stunden ausgeführt.

4. Für Android-Geräte können Sie die Synchronisierung deaktivieren, wenn sich das Gerät im Roaming befindet. Aktivieren Sie dazu das Kontrollkästchen **Synchronisierung im Roaming deaktivieren**.

Standardmäßig ist die Synchronisierung bei Roaming aktiviert.

5. Klicken Sie auf die Schaltfläche **Speichern**, um die an der Richtlinie vorgenommenen Änderungen zu speichern und das Fenster mit den Richtlinieneigenschaften zu verlassen.

Die Einstellungen werden nach der nächsten planmäßigen Synchronisierung des Geräts mit Kaspersky Security Center auf dem mobilen Gerät konfiguriert.

Um mobile Geräte noch effektiver zu schützen, verwenden Kaspersky Endpoint Security für Android und Kaspersky Security für iOS die von Benutzern aus aller Welt erfassten Daten. Zur Verarbeitung dieser Daten dient das Netzwerk *Kaspersky Security Network*.

*Kaspersky Security Network (KSN)* ist eine Infrastruktur von Cloud-Diensten, die Zugriff auf eine aktuelle Wissensdatenbank von Kaspersky bietet. Diese Datenbank enthält Informationen zur Reputation von Dateien, Webressourcen und Programmen. Die Nutzung der Daten aus dem Kaspersky Security Network gewährleistet eine höhere Reaktionsschnelligkeit der Kaspersky-Programme auf Bedrohungen, erhöht die Effektivität vieler Schutzkomponenten und verringert die Wahrscheinlichkeit von Fehlalarmen.

Ihre Teilnahme an Kaspersky Security Network hilft Kaspersky, in Echtzeit Informationen über die Arten und Quellen neuer Bedrohungen zu erfassen, passende Neutralisierungsmethoden zu entwickeln und die Anzahl der Fehlalarme zu reduzieren. Darüber hinaus erhalten Sie durch die Teilnahme am Kaspersky Security Network Zugriff auf die Reputationsdatenbanken für Programme und Websites.

Wenn Sie an Kaspersky Security Network teilnehmen, werden während der Ausführung der mobilen App bestimmte Statistikdaten erfasst und automatisch an Kaspersky übermittelt. Mithilfe dieser Informationen können Bedrohungen in Echtzeit verfolgt werden. Für eine zusätzliche Untersuchung können außerdem Dateien (oder Dateiteile) an Kaspersky geschickt werden, die von Angreifern zur Beschädigung des Computers oder der Benutzerdaten verwendet werden können.

Der Cloud-Dienst Kaspersky Security Network wird von den folgenden App-Komponenten verwendet:

- In der App "Kaspersky Endpoint Security für Android" von den Komponenten Anti-Virus, Web-Filter und Anwendungskontrolle.
- In der App "Kaspersky Security für iOS" von der Komponente Web-Filter.

Um KSN zu verwenden, müssen Sie den Bedingungen des Endbenutzer-Lizenzvertrags zustimmen. Weitere Informationen über die Daten, die an KSN gesendet werden, finden Sie im Abschnitt [Informationsaustausch mit Kaspersky Security Network](#).

Die Ablehnung der Teilnahme an KSN reduziert das Schutzniveau des Geräts, was zur Infektion des Geräts und dem Verlust der Informationen führen kann.

Um die Leistung der mobilen App zu optimieren, können Sie auch statistische Daten an Kaspersky Security Network bereitstellen.

Die Bereitstellung von Informationen an Kaspersky Security Network ist freiwillig.

## Informationsaustausch mit dem Kaspersky Security Network

### Informationsaustausch in Kaspersky Endpoint Security für Android

Zur Erhöhung des Niveaus des Echtzeitschutzes verwendet Kaspersky Endpoint Security für Android den Cloud-Dienst Kaspersky Security Network für die Ausführung folgender Komponenten:

- **Anti-Virus.** Die App erhält Zugriff auf die operative Wissensdatenbank von Kaspersky, welche die Reputationen von Dateien und Apps enthält. Bei der Untersuchung werden Bedrohungen gesucht, die schon in KSN eingetragen sind, auch wenn über sie noch keine Informationen in den Antiviren-Datenbanken vorhanden sind. Der Cloud-Dienst Kaspersky Security Network gewährleistet die uneingeschränkte Funktion von Anti-Virus und reduziert die Wahrscheinlichkeit von Fehlalarmen.

- **Web-Filter.** Die App führt eine Untersuchung von Websites vor ihrem Öffnen durch und berücksichtigt dabei Daten, die von KSN übermittelt werden. Außerdem bestimmt die App auf Grundlage von Listen mit erlaubten und verbotenen Kategorien die Kategorie von Websites, um den Internetzugriff der Benutzer zu kontrollieren (z. B. Kategorie "Kommunikation im Internet").
- **Anwendungskontrolle.** Die App bestimmt auf Grundlage von Listen mit erlaubten und verbotenen Kategorien (z. B. Kategorie "Spiele") die App-Kategorie, um den Start von Apps zu beschränken, die nicht den Anforderungen an die Unternehmenssicherheit genügen.

Informationen zu den Daten, die bei der Nutzung von KSN während der Ausführung von Anti-Virus und Anwendungskontrolle an Kaspersky übertragen werden, finden Sie im Endbenutzer-Lizenzvertrag. Indem Sie die Lizenzvereinbarung akzeptieren, stimmen Sie zu, dass diese Informationen übertragen werden.

Informationen zu den Daten, die bei der Nutzung von KSN während der Ausführung von Web-Filter an Kaspersky übertragen werden, finden Sie in der Erklärung für die Datenverarbeitung für Web-Filter. Indem Sie die Erklärung akzeptieren, stimmen Sie zu, dass diese Informationen übertragen werden.

Weitere Informationen über die Bereitstellung von Daten an KSN finden Sie im Abschnitt [Bereitstellung von Daten in Kaspersky Endpoint Security für Android](#).

Die Bereitstellung von Daten an KSN ist freiwillig. Wenn Sie möchten, können Sie [den Datenaustausch mit KSN deaktivieren](#).

## Informationsaustausch in Kaspersky Security für iOS

Zur Verbesserung des Echtzeitschutzes verwendet Kaspersky Security für iOS den Cloud-Dienst Kaspersky Security Network für die Funktion der Komponente **Web-Filter**. Die App verwendet Daten aus KSN, um Webressourcen vor dem Öffnen zu untersuchen.

Informationen zu den Arten der Daten, die bei der KSN-Nutzung während der Ausführung des Web-Filters an Kaspersky übertragen werden, finden Sie im Endbenutzer-Lizenzvertrag. Indem Sie die Lizenzvereinbarung akzeptieren, stimmen Sie zu, dass diese Informationen übertragen werden.

Weitere Informationen über die Bereitstellung von Daten an KSN finden Sie im Abschnitt [Bereitstellung von Daten in Kaspersky Security für iOS](#).

Die Bereitstellung von Daten an KSN ist freiwillig. Wenn Sie möchten, können Sie [den Datenaustausch mit KSN deaktivieren](#).

## Statistiken von Android- und iOS-Apps an KSN senden

Zum Austausch von Daten mit KSN, um die Qualität der App zu verbessern, müssen die folgenden Bedingungen erfüllt sein:

- Der Benutzer des Geräts muss die Bedingungen der Erklärung zu Kaspersky Security Network lesen und akzeptieren.
- Sie müssen die Übermittlung [statistischer Daten an KSN in den Einstellungen der Gruppenrichtlinie erlauben](#) (siehe unten).

Sie können den Versand von statistischen Daten an KSN jederzeit ablehnen. Informationen zu den Arten der statistischen Daten, die bei der KSN-Nutzung während der Ausführung der mobilen App an Kaspersky übertragen werden, finden Sie in der Erklärung zu Kaspersky Security Network.

# Kaspersky Security Network aktivieren und deaktivieren

Die Verwendung von Kaspersky Security Network ist standardmäßig aktiviert.

Wenn die Verwendung von Kaspersky Security Network deaktiviert ist, werden Web-Filter, Anwendungskontrolle und der zusätzliche Schutz in Kaspersky Security Network automatisch deaktiviert und die entsprechenden Einstellungen sind nicht mehr verfügbar.

*Gehen Sie folgendermaßen vor, um die Nutzung von Kaspersky Security Network zu aktivieren oder zu deaktivieren:*

1. Öffnen Sie das Fenster mit den Richtlinieneigenschaften:

- Wählen Sie im Hauptfenster der Kaspersky Security Center Web Console oder Cloud Console **GERÄTE > RICHTLINIEN & PROFILE** aus. Klicken Sie in der sich öffnenden Liste der Gruppenrichtlinien auf den Namen der Richtlinie, die Sie konfigurieren möchten.
- Wählen Sie im Hauptfenster der Kaspersky Security Center Web Console oder Cloud Console **GERÄTE > MOBIL > GERÄTE** aus. Klicken Sie auf das mobile Gerät, das unter die Richtlinie fällt, die Sie konfigurieren möchten, und wählen Sie anschließend die Richtlinie auf der Registerkarte **AKTIVE RICHTLINIEN UND RICHTLINIENPROFILE** aus.

2. Wählen Sie auf der Seite mit den Richtlinieneigenschaften **ANWENDUNGSEINSTELLUNGEN > KSN und Statistik** aus.

3. Um die Verwendung von Kaspersky Security Network ein- oder auszuschalten, aktivieren oder deaktivieren Sie das Kontrollkästchen **Kaspersky Security Network verwenden**.

4. Wenn die Nutzung von Kaspersky Security Network aktiviert ist und Sie der Übermittlung von Daten an Kaspersky zustimmen, aktivieren Sie das Kontrollkästchen **Übermittlung von Statistikdaten an Kaspersky Security Network erlauben**. Mithilfe dieser Daten kann die mobile App schneller auf Bedrohungen reagieren, die Leistung der Schutzkomponenten verbessern und die Wahrscheinlichkeit von Fehlalarmen reduzieren.

5. Klicken Sie auf die Schaltfläche **Speichern**, um die an der Richtlinie vorgenommenen Änderungen zu speichern und das Fenster mit den Richtlinieneigenschaften zu verlassen.

Die Einstellungen werden nach der nächsten planmäßigen Synchronisierung des Geräts mit Kaspersky Security Center auf dem mobilen Gerät konfiguriert.

## Informationsaustausch mit Google Analytics for Firebase, SafetyNet Attestation, Firebase Performance Monitoring und Crashlytics

Diese Richtlinieneinstellungen können nur für Android-Geräte festgelegt werden.

Kaspersky Endpoint Security für Android tauscht Daten mit den Diensten Google Analytics for Firebase, SafetyNet Attestation, Firebase Performance Monitoring und Crashlytics aus, um die Qualität, das Erscheinungsbild, und die Leistung der Software, der Produkte, der Dienste und der Infrastruktur von Kaspersky durch die Analyse von Benutzererfahrung, Funktionen, Statuswerten und verwendeten Geräteeinstellungen zu verbessern.

Informationsaustausch mit den Diensten Google Analytics for Firebase, SafetyNet Attestation, Firebase Performance Monitoring und Crashlytics ist standardmäßig deaktiviert.

*Um den Datenaustausch zu aktivieren:*

1. Öffnen Sie das Fenster mit den Richtlinieneigenschaften:

- Wählen Sie im Hauptfenster der Kaspersky Security Center Web Console oder Cloud Console **GERÄTE > RICHTLINIEN & PROFILE** aus. Klicken Sie in der sich öffnenden Liste der Gruppenrichtlinien auf den Namen der Richtlinie, die Sie konfigurieren möchten.
- Wählen Sie im Hauptfenster der Kaspersky Security Center Web Console oder Cloud Console **GERÄTE > MOBIL > GERÄTE** aus. Klicken Sie auf das mobile Gerät, das unter die Richtlinie fällt, die Sie konfigurieren möchten, und wählen Sie anschließend die Richtlinie auf der Registerkarte **AKTIVE RICHTLINIEN UND RICHTLINIENPROFILE** aus.

2. Wählen Sie auf der Seite mit den Richtlinieneigenschaften **ANWENDUNGSEINSTELLUNGEN > KSN und Statistik** aus.

3. Aktivieren Sie im Abschnitt **Versand von Statistikdaten** das Kontrollkästchen **Datenübertragung zulassen, um zu helfen, die Qualität, das Design und die Leistung der App zu verbessern**.

4. Klicken Sie auf die Schaltfläche **Speichern**, um die an der Richtlinie vorgenommenen Änderungen zu speichern und das Fenster mit den Richtlinieneigenschaften zu verlassen.


Die Einstellungen werden nach der nächsten planmäßigen Synchronisierung des Geräts mit Kaspersky Security Center auf dem mobilen Gerät konfiguriert.

## Benachrichtigungen auf mobilen Geräten konfigurieren

Diese Richtlinieneinstellungen können nur für Android-Geräte festgelegt werden.

Wenn Sie möchten, dass der Benutzer des Mobilgeräts von den Benachrichtigungen von Kaspersky Security für Android nicht abgelenkt wird, können Sie einige Benachrichtigungen deaktivieren.

Kaspersky Endpoint Security verwendet die folgenden Tools, um den Schutzstatus des Geräts anzuzeigen:

- **Benachrichtigung über den Schutzstatus.** Diese Benachrichtigung ist an die Benachrichtigungsleiste angeheftet. Eine Benachrichtigung über den Schutzstatus kann nicht entfernt werden. Die Benachrichtigung zeigt den Schutzstatus des Geräts (z. B. ) und die Anzahl etwaiger Probleme an. Der Gerätebenutzer kann auf den Schutzstatus des Geräts tippen, um die Liste mit Problemen in der App anzuzeigen.
- **App-Benachrichtigungen.** Diese Benachrichtigungen informieren den Gerätebenutzer über die App (z. B. über das Erkennen von Bedrohungen).
- **Pop-up-Meldungen.** Pop-up-Meldungen erfordern eine Aktion seitens des Gerätebenutzers (z. B. eine Aktion beim Fund einer Bedrohung).

Standardmäßig sind alle Benachrichtigungen von Kaspersky Endpoint Security für Android aktiviert.

Der Benutzer des Android-Geräts kann alle Benachrichtigungen von Kaspersky Endpoint Security für Android in den Einstellungen in der Benachrichtigungsleiste deaktivieren. Wenn die Benachrichtigungen deaktiviert sind, überwacht der Benutzer die Ausführung des App nicht und könnte wichtige Informationen übersehen (z. B. Hinweise auf eine Störung bei der Synchronisierung des Geräts mit Kaspersky Security Center). Um den Status der App-Ausführung zu sehen, muss der Benutzer Kaspersky Endpoint Security für Android öffnen.


*So konfigurieren Sie die Anzeige der Benachrichtigungen über die Ausführung von Kaspersky Endpoint Security für Android auf einem mobilen Gerät:*

1. Öffnen Sie das Fenster mit den Richtlinieneigenschaften:

- Wählen Sie im Hauptfenster der Kaspersky Security Center Web Console oder Cloud Console **GERÄTE > RICHTLINIEN & PROFILE** aus. Klicken Sie in der sich öffnenden Liste der Gruppenrichtlinien auf den Namen der Richtlinie, die Sie konfigurieren möchten.
- Wählen Sie im Hauptfenster der Kaspersky Security Center Web Console oder Cloud Console **GERÄTE > MOBIL > GERÄTE** aus. Klicken Sie auf das mobile Gerät, das unter die Richtlinie fällt, die Sie konfigurieren möchten, und wählen Sie anschließend die Richtlinie auf der Registerkarte **AKTIVE RICHTLINIEN UND RICHTLINIENPROFILE** aus.

2. Wählen Sie auf der Seite mit den Richtlinieneigenschaften **ANWENDUNGSEINSTELLUNGEN > Benachrichtigungen und Berichte** aus.

3. Konfigurieren Sie im Abschnitt **Benachrichtigungen** die Anzeige von Benachrichtigungen:

- Um alle Benachrichtigungen und Pop-up-Meldungen auszublenden, deaktivieren Sie den Umschalter **Benachrichtigungen anzeigen, wenn Kaspersky Endpoint Security im Hintergrund ausgeführt wird**. Kaspersky Endpoint Security für Android zeigt dann nur Benachrichtigungen zum Schutzstatus an. Die Benachrichtigung zeigt den Schutzstatus des Geräts (z. B. ) und die Anzahl der Probleme an. Die App zeigt auch Benachrichtigungen an, wenn der Benutzer mit der App arbeitet (z. B. wenn der Benutzer die Antiviren-Datenbanken manuell aktualisiert).

Die Experten bei Kaspersky empfehlen, Benachrichtigungen und Pop-up-Meldungen zu aktivieren. Wenn Sie Benachrichtigungen und Pop-up-Meldungen für die Ausführung der App im Hintergrund deaktivieren, werden Benutzer nicht in Echtzeit vor Bedrohungen gewarnt. Die Benutzer der mobilen Geräte müssen dann die App öffnen, um den Schutzstatus des Geräts zu sehen.

- Wählen Sie unter **Liste mit den auf den Benutzergeräten angezeigten Sicherheitsproblemen** die Probleme von Kaspersky Endpoint Security für Android aus, die auf dem Mobilgerät des Benutzers angezeigt werden sollen.

4. Klicken Sie auf die Schaltfläche **Speichern**, um die an der Richtlinie vorgenommenen Änderungen zu speichern und das Fenster mit den Richtlinieneigenschaften zu verlassen.

Die Einstellungen werden nach der nächsten planmäßigen Synchronisierung des Geräts mit Kaspersky Security Center auf dem mobilen Gerät konfiguriert.

## Gehackte Geräte erkennen



Mit Kaspersky Security Center Web Console können Sie Geräte-Hacks (Root-Rechte) auf Android-Geräten und Jailbreaks auf iOS-Geräten erkennen. Auf gehackten Geräten sind die Systemdateien nicht geschützt und können daher verändert werden. Ferner können auf gehackten Geräte Apps von Drittherstellern aus unbekannten Quellen installiert werden. Nachdem Sie festgestellt haben, dass ein Gerät gehackt wurde, wird es empfohlen, den normalen Gerätebetrieb wiederherzustellen.

Kaspersky Endpoint Security für Android verwendet die folgenden Dienste, um zu erkennen, wenn ein Benutzer Root-Rechte erhält:

- *Embedded Service von Kaspersky Endpoint Security für Android.* Ein Kaspersky-Dienst, der überprüft, ob der Benutzer eines Mobilgeräts Root-Rechte erhalten hat (Kaspersky Mobile Security SDK).
- *SafetyNet Attestation.* Ein Google-Dienst, der die Integrität des Betriebssystems prüft, die Hardware und Software des Geräts analysiert und sonstige Sicherheitsprobleme ermittelt. Weitere Informationen über die Funktion von SafetyNet Attestation finden Sie auf der Website des technischen Supports von Android.

Kaspersky Security für iOS verwendet die folgenden Dienste, um Jailbreaks zu erkennen:

- *Embedded Service von Kaspersky Security für iOS.* Ein Kaspersky-Dienst, der überprüft, ob ein mobiles Gerät modifiziert wurde (Jailbreak) (Kaspersky Mobile Security SDK).

Sollte ein Gerät gehackt werden, erhalten Sie eine Benachrichtigung. Sie können die Benachrichtigungen über Hacks in Kaspersky Security Center Web Console auf der Registerkarte **ÜBERWACHUNG & BERICHTERSTATTUNG > DASHBOARD** anzeigen. Außerdem können Sie die Benachrichtigungen über gehackte Geräte in den Benachrichtigungseinstellungen über Ereignisse deaktivieren.

Auf Geräten mit Android-Betriebssystem können Sie im Fall eines gehackten Geräts eine Beschränkung der Benutzeraktivitäten festlegen (beispielsweise das Gerät sperren). Diese Beschränkungen können Sie mithilfe der Komponente zur Übereinstimmungsüberprüfung festlegen. [Erstellen Sie dazu eine Übereinstimmungsregel](#) mit dem Kriterium **Auf dem Gerät wurden root-Rechte empfangen**.

## Lizenzeinstellungen festlegen

Diese Richtlinieneinstellungen können für Android- und iOS-Geräte festgelegt werden.

Um mobile Geräte in Kaspersky Security Center Web Console oder Cloud Console zu verwalten, müssen Sie [die mobile App auf den mobilen Geräten aktivieren](#). Die Aktivierung der App "Kaspersky Endpoint Security für Android" oder "Kaspersky Security für iOS" auf einem mobilen Gerät erfolgt durch die Bereitstellung von Informationen über eine gültige Lizenz für die App. Die Lizenzinformationen werden zusammen mit der Richtlinie bei der Synchronisierung Ihres Geräts mit Kaspersky Security Center an das mobile Gerät übermittelt.

Wenn die mobile App nicht innerhalb von 30 Tagen nach der Installation auf dem mobilen Gerät aktiviert wird, wechselt die App automatisch in den eingeschränkten Funktionsmodus. In diesem Modus haben die meisten Komponenten keine Funktion. Beim Wechsel in den eingeschränkten Funktionsmodus stellt die App die automatische Synchronisierung mit Kaspersky Security Center ein. Sollte die App nach der Installation nicht innerhalb von 30 Tagen aktiviert worden sein, so muss das Gerät manuell mit Kaspersky Security Center synchronisiert werden.

*So legen Sie die Lizenzeinstellungen einer Gruppenrichtlinie fest:*

1. Öffnen Sie das Fenster mit den Richtlinieneigenschaften:

- Wählen Sie im Hauptfenster der Kaspersky Security Center Web Console oder Cloud Console **GERÄTE > RICHTLINIEN & PROFILE** aus. Klicken Sie in der sich öffnenden Liste der Gruppenrichtlinien auf den Namen

der Richtlinie, die Sie konfigurieren möchten.

- Wählen Sie im Hauptfenster der Kaspersky Security Center Web Console oder Cloud Console **GERÄTE > MOBIL > GERÄTE** aus. Klicken Sie auf das mobile Gerät, das unter die Richtlinie fällt, die Sie konfigurieren möchten, und wählen Sie anschließend die Richtlinie auf der Registerkarte **AKTIVE RICHTLINIEN UND RICHTLINIENPROFILE** aus.

2. Wählen Sie auf der Seite mit den Richtlinieneigenschaften **PROGRAMMEINSTELLUNGEN > Lizenzen** aus.

3. Wählen Sie über die Dropdown-Liste den erforderlichen Lizenzschlüssel aus dem Schlüsselspeicher des Administrationsservers aus.

Die Details des Lizenzschlüssels werden in den Feldern darunter angezeigt.

Sie können den vorhandenen Aktivierungsschlüssel auf dem Mobilgerät ersetzen, wenn er sich von dem in der Dropdown-Liste oben ausgewählten unterscheidet. Aktivieren Sie dazu das Kontrollkästchen **Mit diesem Schlüssel ersetzen, falls sich der Schlüssel auf dem Gerät unterscheidet**.

4. Klicken Sie auf die Schaltfläche **Speichern**, um die an der Richtlinie vorgenommenen Änderungen zu speichern und das Fenster mit den Richtlinieneigenschaften zu verlassen.

Die Einstellungen werden nach der nächsten planmäßigen Synchronisierung des Geräts mit Kaspersky Security Center auf dem mobilen Gerät konfiguriert.

## Ereignisse konfigurieren

Diese Richtlinieneinstellungen können für Android- und iOS-Geräte festgelegt werden.

Sie können die Speicher- und Benachrichtigungseinstellungen für Ereignisse festlegen, die auf den Geräten Ihrer Benutzer auftreten und an das Kaspersky Security Center gesendet werden.

Sie können Ereignisse nur konfigurieren, wenn Sie eine Richtlinie [ändern](#).

Ereignisse werden auf den folgenden Registerkarten nach Ereigniskategorien verteilt:

- **Kritische Meldung**

Ein kritisches Ereignis weist auf ein Problem hin, das zu Datenverlust, einer Betriebsstörung oder einem kritischen Fehler führen kann.

- **Fehlfunktion**

Eine Fehlfunktion weist auf ein schwerwiegendes Problem, einen Fehler oder eine Störung hin, die während des Betriebs der App aufgetreten ist.

- **Warnung**

Eine Warnung muss nicht zwingend schwerwiegend sein, weist aber auf einen Umstand hin, der später zu einem Problem führen könnte.

- **Information**



Informationseignisse informieren über den erfolgreichen Abschluss von Vorgängen oder Prozeduren sowie über die ordnungsgemäße Ausführung der App.

In jedem Abschnitt zeigt die Liste die Ereignistypen und die standardmäßige Speicherdauer von Ereignissen im Kaspersky Security Center (in Tagen) an.

In der Ereignisliste der können Sie Folgendes tun:

- Hinzufügen oder Entfernen eines Ereignistyps aus der Liste der Ereignistypen, die an Kaspersky Security Center gesendet werden.
- Festlegen der Speicher- und Benachrichtigungseinstellungen für jeden Ereignistyp, z. B. wie lange Ereignisse dieses Typs in der Datenbank des Administrationsservers gespeichert werden sollen oder ob Sie über Ereignisse dieses Typs per E-Mail benachrichtigt werden.

Nähere Informationen zur Konfiguration von Ereignissen via Kaspersky Security Center Web Console und Cloud Console finden Sie hier:

- Wenn Sie Kaspersky Security Center Web Console verwenden, lesen Sie bitte die [Hilfe zu Kaspersky Security Center](#).
- Wenn Sie Kaspersky Security Center Cloud Console verwenden, lesen Sie bitte die [Hilfe zu Kaspersky Security Center Cloud Console](#).

## Ereignisse zum Installieren, Aktualisieren und Entfernen von Apps auf den Geräten der Benutzer konfigurieren

Diese Richtlinieneinstellungen können für Android- und iOS-Geräte festgelegt werden.

Wenn Sie die Kaspersky Security Center Cloud Console verwenden, enthält die Liste der [Ereignistypen, die auf den Geräten Ihrer Benutzer auftreten](#) und die an das Kaspersky Security Center gesendet werden, nicht die Installation, Aktualisierung und Löschung von Apps auf den Geräten. Dies liegt daran, dass solche Ereignisse sehr häufig auftreten und diese Ereignisse andere wichtige Ereignisse in der Datenbank von Kaspersky Security Center ersetzen können, wenn die maximale Anzahl an Ereignissen erreicht ist. Sie können außerdem die Leistung des Administrationsservers, des DBMS und die Bandbreite der Internetverbindung mit der Kaspersky Security Center Cloud Console beeinträchtigen.

Wenn Sie dennoch Ereignisse dieser Art speichern und darüber benachrichtigt werden möchten, gehen Sie wie in diesem Abschnitt beschrieben vor.

*So konfigurieren Sie Ereignisse zum Installieren, Aktualisieren und Entfernen von Apps auf den Geräten der Benutzer:*

1. Fügen Sie in den Einstellungen einer Richtlinie auf der Registerkarte **EREIGNISKONFIGURATION** den informativen Ereignistyp **App installiert oder gelöscht (Liste der installierten Apps)** zur Liste der in der Datenbank des Administrationsservers gespeicherten Ereignisse hinzu.

Weitere Informationen zur Konfiguration von Ereignissen finden Sie in der [Hilfe zur Kaspersky Security Center Cloud Console](#).

2. Aktivieren Sie die Option [Eine Liste der installierten Apps auf allen mobilen Geräten senden](#).

Ereignisse zum Installieren, Aktualisieren und Entfernen von Apps auf den Geräten der Benutzer werden in der Datenbank von Kaspersky Security Center gespeichert. Sie werden über diese Ereignisse benachrichtigt.

## Netzwerkbelastung

Dieser Abschnitt enthält Informationen über den Umfang des Netzwerkverkehrs, der zwischen den mobilen Geräten und Kaspersky Security Center während der Programmausführung aufkommt.






Datenverkehr

Aufgabe	Ausgehender Datenverkehr	Eingehender Datenverkehr	Gesamter Datenverkehr
Ursprüngliche Verteilung der App, MB	0,08	17,76	17,84
Ursprüngliches Update der Antiviren-Datenbanken (der Umfang des Datenverkehrs kann sich aufgrund der Größe der Antiviren-Datenbanken unterscheiden), MB	0,04	2,21	2,25
Synchronisierung des mobilen Geräts mit Kaspersky Security Center, MB	0,03	0,02	0,05
Regelmäßiges Update der Antiviren-Datenbanken (der Umfang des Datenverkehrs kann sich aufgrund der Größe der Antiviren-Datenbanken unterscheiden), MB	0,08	3,06	3,14
Ausführung der Diebstahlschutz-Befehle. Gerät orten (der Umfang des Datenverkehrs kann sich aufgrund der Merkmale der integrierten Kamera und der Bildqualität unterscheiden), MB	0,09	0,8	0,17
Ausführung der Diebstahlschutz-Befehle. Foto aufnehmen, MB	1,0	0,02	1,02
Ausführung der Diebstahlschutz-Befehle. Gerät sperren, MB	0,06	0,05	0,11
Mittlerer Verbrauch in 24 Stunden, MB	0,22	6,96	7,18

# Arbeiten in der MMC-basierten Verwaltungskonsole

Dieser Hilfeabschnitt beschreibt den Schutz und die Verwaltung von mobilen Geräten mithilfe der Verwaltungskonsole auf MMC-Basis von Kaspersky Security Center.

## Wichtige Anwendungsfälle

 INSTALLATION	 KONTROLLE
<a href="#">Wie wird Kaspersky Endpoint Security für Android ferngesteuert installiert?</a>	<a href="#">Wie verbietet man dem Benutzer, auf dem Gerät zu spielen?</a>
<a href="#">Wie verbietet man dem Benutzer, Kaspersky Endpoint Security für Android zu löschen?</a>	<a href="#">Wie wird der Zugriff auf Websites auf dem Gerät angepasst?</a>
<a href="#">Wie wird Kaspersky Endpoint Security für Android aktiviert?</a>	<a href="#">Wie erkennt man root?</a>
 SCHUTZ	 VERWALTUNG
<a href="#">Wie blockiert man ein Gerät, das verloren oder gestohlen wurde?</a>	<a href="#">Wie konfiguriert man das E-Mail-Postfach auf dem Gerät?</a>
<a href="#">Wie schützt man sich vor Bedrohungen im Internet?</a>	<a href="#">Wie schließt das mobile Gerät an das WLAN an?</a>
<a href="#">Wie verhindert man die Verwendung eines leeren Kennworts?</a>	<a href="#">Wie installiert man korporative Apps?</a>
 VERWENDUNG VON DRITTANBIETERSOFTWARE	
<a href="#">Android Enterprise (<a href="#">Apps mit einer "Aktentasche"</a>, <a href="#">Einstellungen des Arbeitsprofils Android anpassen</a>)</a>	
<a href="#">VMware AirWatch, MobileIron, IBM Maas360, SOTI MobiControl</a>	

## Über Kaspersky Security für mobile Endgeräte

Die integrierte Lösung *Kaspersky Security für mobile Endgeräte* dient dem Schutz und der Verwaltung von mobilen Unternehmensgeräten und persönlichen mobilen Geräten, welche die Mitarbeiter einer Organisation für Unternehmenszwecke verwenden.

Kaspersky Security für mobile Endgeräte besteht aus folgenden Komponenten:

- Mobile Anwendung Kaspersky Endpoint Security für Android.  
Die App "Kaspersky Endpoint Security für Android" gewährleistet den Schutz mobiler Geräte vor Webbedrohungen, Viren und anderen gefährlichen Programmen.
- Verwaltungs-Plug-in von Kaspersky Endpoint Security für Android

Das Verwaltungs-Plug-in für Kaspersky Endpoint Security für Android bietet eine Verwaltungsschnittstelle für mobile Endgeräte und darauf installierte mobile Anwendungen über die Administrationskonsole von Kaspersky Security Center.

- Verwaltungs-Plug-in für Kaspersky Device Management für iOS

Das Verwaltungs-Plug-in von Kaspersky Device Management für iOS ermöglicht, die Konfigurationseinstellungen der Geräte, die über das iOS MDM-Protokoll (im Weiteren "iOS MDM-Geräte") und Exchange ActiveSync (im Weiteren "EAS-Geräte") an Kaspersky Security Center angeschlossen sind, ohne Nutzung der iPhone Configuration Utility und der Management-Konsole von Exchange anzupassen.

Die Verwaltungs-Plug-ins werden in das *Remote-Management-System von Kaspersky Security Center integriert*. Mithilfe der einheitlichen Verwaltungskonsole für Kaspersky Security Center verwaltet der Administrator alle mobilen Endgeräte eines Unternehmens sowie Client-Computer und virtuelle Systeme. Nach dem Verbinden der mobilen Endgeräte mit dem Administrationsserver können die Geräte verwaltet werden. Der Administrator kann die verwalteten Geräte ferngesteuert kontrollieren.

Die mobile App Kaspersky Endpoint Security für Android kann auch im Rahmen des *Remote-Verwaltungssystems für Kaspersky Endpoint Security Cloud* ausgeführt werden. Details zur Arbeit mit den Apps über Kaspersky Endpoint Security zu Cloud finden Sie in der [Online-Hilfe zu Kaspersky Endpoint Security Cloud](#)<sup>2</sup>.

Die mobile App Kaspersky Endpoint Security für Android kann auch als [Bestandteil der externen EMM-Lösungen der Mitglieder der AppConfig Community](#) verwendet werden.

## Hauptfunktionen zur Verwaltung mobiler Geräte in der Verwaltungskonsole auf MMC-Basis

Kaspersky Security für mobile Endgeräte bietet die folgenden Funktionen:

- Versand von E-Mail-Nachrichten für die Verbindung von Android-Geräten mit Kaspersky Security Center mithilfe von Google-Play-Links.
- Remote-Verbindung der mobilen Geräte der Benutzer mit Kaspersky Security Center und anderen externen EMM-Systemen (z. B. VMWare AirWatch, MobileIron, IBM Maas360, SOTI MobiControl).
- Remote-Konfiguration der App "Kaspersky Endpoint Security für Android" und der Dienste, Apps und Funktionen von Android-Geräten.
- Ferngesteuerte Konfiguration der Mobilgeräte entsprechend der korporativen Sicherheit.
- Verhinderung des Verlustes der auf mobilen Geräten gespeicherten Unternehmensdaten im Fall von Diebstahl und Verlust (Diebstahlschutz).
- Kontrolle der Einhaltung der Anforderungen an die Unternehmenssicherheit (Übereinstimmungsüberprüfung).
- Kontrolle der Internetnutzung auf mobilen Geräten (Web-Filter).
- Anpassen eines Unternehmenspostfachs auf mobilen Geräten, insbesondere, wenn im Unternehmen der Microsoft Exchange-Mail-Server bereitgestellt wurde (nur für iOS- und Samsung-Geräte).
- Anpassen der Berechtigung zur Nutzung von VPN auf mobilen Geräten im Unternehmensnetzwerk (WLAN, VPN). VPN kann nur auf iOS- und Samsung-Geräten konfiguriert werden.
- Anpassen der Anzeige des Status des mobilen Geräts in Kaspersky Security Center bei einem Verstoß gegen die Richtlinienregeln: Kritisch, Warnung, OK.

- Konfiguration der Benachrichtigungen, die dem Benutzer in der App "Kaspersky Endpoint Security für Android" angezeigt werden.
- Anpassen der Einstellungen auf Geräten mit Unterstützung von Samsung KNOX 2.6 und höher.
- Konfiguration der Einstellungen auf Geräten, die Arbeitsprofile Android unterstützen.
- Verteilung von Kaspersky Endpoint Security für Android über die Konsole Samsung KNOX Mobile Enrollment. Samsung KNOX Mobile Enrollment ist für die Masseninstallation und die Erstkonfiguration von Apps auf neuen Samsung-Geräten vorgesehen, die bei offiziellen Anbietern erworben wurden.
- Das Upgrade von Kaspersky Endpoint Security für Android auf die festgelegte Version kann mithilfe der Richtlinien von Kaspersky Security Center vorgenommen werden.
- Benachrichtigung des Administrators über den Status und die Ereignisse in der Ausführung der Kaspersky Endpoint Security für Android-App in Kaspersky Security Center oder per E-Mail.
- Kontrolle der Änderungen der Richtlinienereinstellungen (Revisionsverlauf).

Kaspersky Security für mobile Endgeräte besteht aus den folgenden Schutz- und Verwaltungskomponenten:

- Anti-Virus (für Android-Geräte)
- Diebstahlschutz (für Android-Geräte)
- Web-Filter (für Android- und iOS-Geräte)
- Anwendungskontrolle (für Android-Geräte)
- Übereinstimmungsüberprüfung (für Android-Geräte)
- Erkennung von Root-Berechtigungen auf Geräten (für Android-Geräte)

## Über Kaspersky Endpoint Security für Android

Die App "Kaspersky Endpoint Security für Android" gewährleistet den Schutz mobiler Geräte vor Webbedrohungen, Viren und anderen gefährlichen Programmen.

Die App von Kaspersky Endpoint Security für Android enthält folgende Komponenten:

- **Anti-Virus.** Kann Bedrohungen auf einem mobilen Gerät erkennen und beseitigen. Dazu werden die Antiviren-Datenbanken der App und der Cloud-Dienst [Kaspersky Security Network](#) eingesetzt. Im Lieferumfang von Anti-Virus sind folgende Komponenten enthalten:
  - Schutz. Der Schutz kann Bedrohungen in geöffneten Dateien erkennen, untersucht neue Anwendungen und verhindert im Echtzeitmodus einen Virenbefall des Geräts.
  - Untersuchung. Wird bei Bedarf für das gesamte Dateisystem, nur für die installierten Anwendungen, die ausgewählte Datei oder den Ordner ausgeführt.
  - Update. Über die Funktion Update können Sie neue Antiviren-Datenbanken für die App herunterladen.
- **Diebstahlschutz.** Schützt die Informationen auf einem Gerät vor unberechtigt Zugriff, falls das Gerät verloren geht oder gestohlen wird. Mit dieser Komponente können Sie die folgenden Befehle an das Gerät

senden:

- **Gerät orten**, um die Koordinaten des Gerätestandorts zu ermitteln.
- **Alarmsignal erzeugen**, damit das Gerät einen lauten Alarmton erzeugt.
- **Foto aufnehmen**, damit das Gerät Bilder mit der Frontkamera aufnimmt, sobald jemand versucht, dieses zu entsperren.
- Unternehmensdaten **löschen**, um vertrauliche Informationen des Unternehmens zu schützen.
- **Web-Filter**. Ermöglicht das Blockieren schädlicher Websites, die der Verbreitung von Schadcode dienen. Der Web-Filter blockiert ebenfalls gefälschte (Phishing) Websites, die dazu dienen, vertrauliche Daten des Benutzers (beispielsweise Kennwörter für Online-Banking oder Zahlungssysteme) zu stehlen und auf die Finanzkonten des Benutzers zuzugreifen. Der Web-Filter untersucht Webseiten, bevor sie geöffnet werden. Dazu wird der Cloud-Dienst Kaspersky Security Network genutzt. Anhand der Ergebnisse der Untersuchung erlaubt der Web-Filter den Download von als sicher eingestuften Websites und blockiert als gefährliche eingestufte Websites. Der Web-Filter unterstützt ferner die Filterung von Websites nach Kategorien, die im Cloud-Dienst Kaspersky Security Network festgelegt sind. Dadurch kann der Administrator den Zugriff der Benutzer auf bestimmte Kategorien einschränken (beispielsweise auf Webseiten aus der Kategorie "Glücksspiel, Lotterien, Wetten" oder "Kommunikation im Internet").
- **Anwendungskontrolle**. Diese Komponente ermöglicht die Installation von empfohlenen und obligatorischen Anwendungen auf Ihrem Gerät über einen direkten Link zum Programmpaket oder einen Link zu Google Play. Mithilfe der Anwendungskontrolle können Sie verbotene Anwendungen deinstallieren, die der korporativen Sicherheit nicht entsprechen.
- **Übereinstimmungsüberprüfung**. Mit dieser Komponente können verwaltete Geräte auf die Einhaltung der Anforderungen an die Unternehmenssicherheit überprüft werden. Bestimmte Funktionen von Geräten, die dagegen verstoßen, können eingeschränkt werden.

## Über Kaspersky Device Management für iOS

Kaspersky Device Management für iOS gewährleistet den Schutz und die Steuerung mobiler Geräte, die mit Kaspersky Security Center verbunden sind, und bietet Funktionen zur Geräteverwaltung wie:

- **Kennwortschutz**. Mit dieser Funktion können Sie Anforderungen an die Kennwortstärke festlegen, damit Benutzer komplexe Kennwörter verwenden, die den Anforderungen an die Kennwortrichtlinien des Unternehmens entsprechen.
- **Netzwerkverwaltung**. Mit dieser Funktion können Sie zulässige VPNs und WLAN-Netzwerke hinzufügen und den Zugriff auf andere Netzwerke beschränken.
- **Unternehmensdaten löschen**. Sollte das Gerät verloren gehen oder gestohlen werden, können Sie einen Befehl zum Löschen von Daten an das Gerät senden, um vertrauliche Informationen des Unternehmens zu schützen.
- **Web-Filter**. Ermöglicht das Blockieren schädlicher Websites, die der Verbreitung von Schadcode dienen. Der Web-Filter blockiert ebenfalls gefälschte (Phishing) Websites, die dazu dienen, vertrauliche Daten des Benutzers (beispielsweise Kennwörter für Online-Banking oder Zahlungssysteme) zu stehlen und auf die Finanzkonten des Benutzers zuzugreifen. Der Web-Filter untersucht Webseiten, bevor sie geöffnet werden. Dazu wird der Cloud-Dienst Kaspersky Security Network genutzt. Anhand der Ergebnisse der Untersuchung erlaubt der Web-Filter den Download von als sicher eingestuften Websites und blockiert als gefährliche eingestufte Websites. Der Web-Filter unterstützt ferner die Filterung von Websites nach Kategorien, die im Cloud-Dienst Kaspersky Security Network festgelegt sind. Dadurch kann der Administrator den Zugriff der

Benutzer auf bestimmte Kategorien einschränken (beispielsweise auf Webseiten aus der Kategorie "Glücksspiel, Lotterien, Wetten" oder "Kommunikation im Internet").

- **Programmbeschränkungen.** Mit dieser Komponente können Sie steuern, welche nativen Apps des Geräts (z. B. iTunes, Safari, Game Center) auf einem kontrollierten Gerät verwendet werden dürfen.
- **Funktionsbeschränkungen.** Mit dieser Komponente können verwaltete Geräte auf die Einhaltung der Anforderungen an die Unternehmenssicherheit überprüft werden. Bestimmte Funktionen von Geräten, die dagegen verstoßen, können eingeschränkt werden.

## Über das Exchange-E-Mail-Postfach

Das *Exchange-E-Mail-Postfach* ist die Client-App des Dienstes Exchange ActiveSync. Diese App ist dafür vorgesehen, Unternehmensbenutzer bei der Arbeit mit E-Mail, Kalender, Kontakten und Aufgaben zu unterstützen. Das Exchange-E-Mail-Postfach ermöglicht eine Verbindung des mobilen Geräts mit dem Microsoft Exchange-Server. Details über den Dienst Exchange ActiveSync finden Sie auf der [Website des technischen Supports von Microsoft](#).

Für die Verwaltung von mobilen Geräten über das Exchange ActiveSync-Protokoll muss der Exchange-Server bereitgestellt sein. Weitere Informationen über die Installation eines Exchange-Servers finden Sie in der [Hilfe zu Kaspersky Security Center](#). Auf mobilen Geräten sind keine erweiterten Einstellungen erforderlich.

Mithilfe des Exchange-Postfachs können Sie die EAS-Geräte mithilfe von Gruppenrichtlinien ferngesteuert konfigurieren sowie einen Befehl zur Datenlöschung absenden. Das Exchange ActiveSync-Protokoll unterstützt folgende Betriebssysteme:

- Windows Mobile
- Windows CE
- Windows Phone
- Android
- Bada
- BlackBerry 10
- iOS
- Symbian

Die Auswahl der Einstellungen für die Geräteverwaltung mithilfe von Exchange ActiveSync ist vom Betriebssystem abhängig, das auf dem mobilen Gerät installiert ist. Einzelheiten zur Unterstützung des Exchange ActiveSync-Protokolls für ein konkretes Betriebssystem erhalten Sie in der Dokumentation des Betriebssystems.

## Über das Verwaltungs-Plug-in von Kaspersky Endpoint Security für Android

Das Verwaltungs-Plug-in für Kaspersky Endpoint Security für Android bietet eine Verwaltungsschnittstelle für mobile Endgeräte und darauf installierte mobile Anwendungen über die Administrationskonsole von Kaspersky Security Center. Mithilfe des Verwaltungs-Plug-ins für Kaspersky Endpoint Security für Android können Sie folgende Aktionen ausführen:

- Gruppenrichtlinien für den Schutz der mobilen Endgeräte erstellen.
- Einstellungen für die Ausführung der App Kaspersky Endpoint Security für Android auf den mobilen Geräten der Benutzer ferngesteuert anpassen.
- Berichte und Statistiken über die Ausführung der mobilen App Kaspersky Endpoint Security für Android auf den Geräten der Benutzer erhalten.

Das Verwaltungs-Plug-in für Kaspersky Endpoint Security für Android wird standardmäßig bei der Softwareverteilung von Kaspersky Security Center installiert. Für das Plug-in ist keine separate Installation erforderlich.

## Über das Verwaltungs-Plug-in für Kaspersky Device Management für iOS

Das Verwaltungs-Plug-in für Kaspersky Device Management für iOS ist eine Schnittstelle, mit deren Hilfe mobile Geräte, die über das Protokoll iOS MDM bzw. Exchange ActiveSync verbunden sind, über die Verwaltungskonsolle von Kaspersky Security Center verwaltet werden können. Mithilfe des Verwaltungs-Plug-ins für Kaspersky Device Management für iOS können Sie folgende Aktionen ausführen:

- Gruppenrichtlinien für den Schutz der mobilen Endgeräte erstellen.
- per Remote-Zugriff die Geräte konfigurieren, die über das Exchange ActiveSync-Protokoll verbunden sind (im Folgenden "EAS-Geräte").
- per Remote-Zugriff die Geräte konfigurieren, die über das iOS MDM-Protokoll verbunden sind (im Folgenden "iOS MDM-Geräte").
- Berichte und Statistikdaten zum Betrieb der Benutzergeräte abrufen.

Weitere Informationen zur Verbindung von mobilen Geräten mit Kaspersky Security Center über das iOS MDM-Protokoll bzw. das Exchange ActiveSync-Protokoll finden Sie in der [Hilfe zu Kaspersky Security Center](#).

Das Verwaltungs-Plug-in für Kaspersky Device Management für iOS wird standardmäßig bei der Softwareverteilung von Kaspersky Security Center installiert. Für das Plug-in ist keine separate Installation erforderlich.

## Hardware- und Softwarevoraussetzungen

Dieser Abschnitt enthält die Hardware und Softwarevoraussetzungen für den Computer des Administrators, der für die Implementierung der Anwendung auf den mobilen Geräten verwendet wird, sowie eine Aufzählung der Betriebssysteme für mobile Geräte, die von Kaspersky Security für mobile Endgeräte unterstützt werden.

### Hardware- und Softwareanforderungen für den Computer des Administrators

Für die Verteilung der Komplettlösung Kaspersky Security für mobile Endgeräte muss der Computer des Administrators die Hardwarevoraussetzungen von Kaspersky Security Center erfüllen. Weitere Informationen über die Hardwarevoraussetzungen von Kaspersky Security Center finden Sie in der [Hilfe zu Kaspersky Security Center](#).

Für die Ausführung des Verwaltungs-Plug-ins von Kaspersky Endpoint Security für Android muss auf dem Computer des Administrators die Verwaltungskonsolle von Kaspersky Security Center 12 oder höher installiert sein.



Für die Ausführung des Verwaltungs-Plug-ins Kaspersky Device Management für iOS muss der Computer des Administrators folgende Softwarevoraussetzungen erfüllen:

- Verwaltungskonsole von Kaspersky Security Center 12 oder höher
- Komponente Exchange-Server
- Komponente iOS MDM-Server für Mobilgeräte
- SSE2-Befehlssatz oder neuerer Version

Für die Verteilung der mobilen Anwendung Kaspersky Endpoint Security für Android über den Administrationsserver muss der Computer des Administrators folgende Softwarevoraussetzungen erfüllen:

- Kaspersky Security Center 12 oder höher
- Verwaltungs-Plug-in von Kaspersky Endpoint Security für Android

Für die Verteilung der mobilen Anwendung Kaspersky Endpoint Security für Android aus den entsprechenden Online-Shops liegen für den Computer des Administrators keine Softwareanforderungen vor.

Die mobile App Kaspersky Endpoint Security für Android kann auch im Rahmen des Remote-Verwaltungssystems für Kaspersky Endpoint Security Cloud 6.0 und höher ausgeführt werden. Weitere Informationen zur Arbeit mit Apps über Kaspersky Endpoint Security Cloud finden Sie in der [Hilfe zu Kaspersky Endpoint Security Cloud](#)<sup>12</sup>.

Die mobile App Kaspersky Endpoint Security für Android kann auch als Bestandteil von [externen EMM-Lösungen](#) verwendet werden:

- VMware AirWatch 9.3 und höher
- MobileIron 10.0 und höher
- IBM MaaS360 10.68 und höher
- Microsoft Intune 1908 und höher
- SOTI MobiControl 14.1.4 (1693) und höher

Hardware und Softwareanforderungen an das mobile Gerät des Benutzers für die Installation der App "Kaspersky Endpoint Security für Android"

Für die App "Kaspersky Endpoint Security für Android" müssen folgende Hardware- und Softwarevoraussetzungen erfüllt sein:

- Smartphone oder Tablet mit einer Bildschirmgröße ab 320 x 480 Pixel
- 65 MB freier Speicherplatz im Geräte Hauptspeicher
- Android 5.0–12 (einschließlich Android 12L, mit Ausnahme der Go Edition)
- Prozessorarchitektur x86, x86-64, Arm5, Arm6, Arm7, Arm8

Die App kann nur im Geräte Hauptspeicher installiert werden.

# Hard- und Softwareanforderungen an das mobile Gerät des Benutzers für das iOS MDM-Profil

Das iOS MDM-Profil hat folgende Hard- und Softwareanforderungen:

- iOS 10.0–15.0 oder iPadOS 13–15
- Internetverbindung

## Bekannte Probleme und Besonderheiten

Kaspersky Endpoint Security für Android hat eine Reihe von bekannten Problemen mit geringfügiger Bedeutung für die Ausführung der App.

### Bekannte Probleme bei der Installation von Apps

- Kaspersky Endpoint Security für Android kann nur in den Hauptspeicher des Geräts installiert werden.
- Auf Geräten mit Android 7.0 kann es beim Versuch, die Rechte des Administrators für Kaspersky Endpoint Security für Android in den Geräteeinstellungen zu deaktivieren, zu einem Absturz kommen, wenn für Kaspersky Endpoint Security für Android das Overlay über anderen Fenstern verboten ist. Das Problem hängt mit dem bekannten [Fehler in Android 7](#) zusammen.
- Die App Kaspersky Endpoint Security für Android auf Geräten mit Android 7.0 und höher unterstützt den Mehrfenster-Modus nicht.
- Kaspersky Endpoint Security für Android läuft nicht auf Chromebook-Geräten mit dem Betriebssystem Chrome.
- Kaspersky Endpoint Security für Android funktioniert nicht auf Geräten mit Android (Go Edition) als Betriebssystem.
- Bei der Verwendung von Kaspersky Endpoint Security für Android mit externen EMM-Systemen (z. B. VMWare AirWatch) sind nur die Komponenten "Anti-Virus" und "Web-Filter" verfügbar. Der Administrator kann die Einstellungen von Anti-Virus und Web-Filter in der Konsole des EMM-Systems anpassen. Dabei werden die Benachrichtigungen über die App-Ausführung nur in der Benutzeroberfläche der App von Kaspersky Endpoint Security für Android angezeigt (Berichte).

### Bekannte Probleme beim Upgrade der App-Version

- Sie können Kaspersky Endpoint Security für Android nur auf eine neuere Version der App upgraden. Ein Downgrade zu einer älteren Version von Kaspersky Endpoint Security für Android ist nicht möglich.
- Für das Upgrade von Kaspersky Endpoint Security für Android mithilfe eines eigenständigen Installationspakets muss auf dem mobilen Gerät des Benutzers die Installation von Apps aus unbekannten Quellen erlaubt sein.
- Das Update über Google Play ist verfügbar, wenn Kaspersky Endpoint Security für Android über Google Play installiert wurde. Wenn die App auf andere Weise installiert wurde, ist ein Update über Google Play nicht möglich.
- Das Update über Kaspersky Security Center ist verfügbar, wenn Kaspersky Endpoint Security für Android über Kaspersky Security Center installiert wurde. Wenn die App über Google Play installiert wurde, ist ein Update

über Kaspersky Security Center nicht möglich.

- Nach der Aktualisierung der Verwaltungs-Plug-ins auf Technical Release 33 muss auch die App von Kaspersky Endpoint Security für Android auf Technical Release 33 aktualisiert werden. Andernfalls können Sie Samsung KNOX auf einigen Geräten Ihrer Benutzer nicht aktivieren.

## Bekannte Probleme bei der Ausführung von Anti-Virus

- Aufgrund von technischen Beschränkungen kann Kaspersky Endpoint Security für Android Dateien mit einer Größe von mehr als 2 GB nicht untersuchen. Während der Untersuchung überspringt die App solche Dateien, und Sie werden nicht benachrichtigt, wenn solche Dateien übersprungen werden.
- Um das Gerät zusätzlich auf neue Bedrohungen untersuchen zu können, über die noch keine Informationen in den Antiviren-Datenbanken vorhanden sind, muss die Nutzung von Kaspersky Security Network aktiviert werden. *Kaspersky Security Network (KSN)* ist eine Infrastruktur von Cloud-Diensten, die Zugriff auf eine aktuelle Wissensdatenbank von Kaspersky bietet. Diese Datenbank enthält Informationen zur Reputation von Dateien, Webressourcen und Programmen. Für die Nutzung von KSN benötigt das mobile Gerät Internetzugang.
- In einigen Fällen kann auf mobilen Geräten die Aktualisierung der Antiviren-Datenbanken vom Administrationsserver fehlschlagen. Führen Sie in diesem Fall die Update-Aufgabe für die Antiviren-Datenbanken auf dem Administrationsserver aus.
- Auf einigen Geräten findet Kaspersky Endpoint Security für Android keine Geräte, die über USB OTG angeschlossen sind. Auf solchen Geräten kann keine Untersuchung auf Viren durchgeführt werden.
- Auf Geräten mit Android 11.0 oder höher muss der Nutzer die Berechtigung "Zugriff auf alle Dateien" erteilen.
- Auf Geräten mit Android 7.0 und höher wird das Fenster der Zeitplan-Einstellungen für den Start der Untersuchung auf Viren möglicherweise nicht korrekt angezeigt (Steuerelemente werden nicht angezeigt). Das Problem hängt mit dem bekannten [Fehler in Android 7](#) zusammen.
- Auf Geräten mit Android 7.0 erkennt der Echtzeitschutz im erweiterten Modus keine Bedrohungen in Dateien, die auf einer externen SD-Karte gespeichert sind.
- Auf Geräten unter Android 6.0 erkennt Kaspersky Endpoint Security für Android nicht, wenn eine schädliche Datei in den Gerätespeicher geladen wird. Die schädliche Datei kann vom Anti-Virus beim Start der Datei oder während der Untersuchung des Geräts auf Viren erkannt werden. Das Problem hängt mit dem bekannten [Fehler in Android 6.0](#) zusammen. Um die Sicherheit des Geräts zu gewährleisten, wird empfohlen, den Start der Untersuchung auf Viren nach Zeitplan einzurichten.

## Bekannte Probleme bei der Ausführung von Web-Filter

- Der Web-Filter funktioniert auf Android-Geräten nur mit den Browsern Google Chrome (einschließlich der Funktion Custom Tabs), Huawei Browser und Samsung Internet Browser. Web-Filter für Samsung Internet Browser blockiert keine Websites auf mobilen Geräten, wenn ein Arbeitsprofil verwendet wird und [Web-Filter nur für das Arbeitsprofil aktiviert ist](#).
- Im Arbeitsprofil untersucht Kaspersky Endpoint Security nur die Website-Domain im HTTPS-Datenverkehr. Bösartige Websites und Phishing-Websites werden eventuell nicht blockiert, wenn die App im Arbeitsprofil installiert ist. Wenn die Domain vertrauenswürdig ist, kann Web-Filter eine Bedrohung überspringen (z. B. <https://trusted.domain.com/phishing/>). Wenn die Domain nicht vertrauenswürdig ist, blockiert Web-Filter bösartige Websites und Phishing-Websites.
- Damit der Web-Filter ausgeführt werden kann, muss die Nutzung von Kaspersky Security Network aktiviert werden. Der Web-Filter blockiert Websites unter Berücksichtigung der KSN-Daten zur Reputation und

## Kategorie von Websites.

- Auf Geräten mit dem Betriebssystem Android 6.0 mit dem installierten Browser Google Chrome Version 51 oder früher kann der Web-Filter verbotene Websites nicht blockieren, wenn sie auf eine der folgenden Arten geöffnet wurden (das Problem ist mit einem bekannten Defekt in Google Chrome verbunden):
  - Über die Ergebnisse einer Suchanfrage.
  - Aus einer Liste mit Registerkarten.
  - Aus dem Verlauf von Suchanfragen.
  - Bei Verwendung der Funktion der Autovervollständigung von Webadressen.
  - Beim Öffnen der Website in einer neuen Registerkarte in Google Chrome.
- Blockierte Websites können im Browser Google Chrome Version 50 oder früheren Versionen nicht gesperrt werden, wenn die Website aus den Ergebnissen einer Google-Suchanfrage geöffnet wird und die Funktion **"Registerkarten und Apps zusammenführen"** in der Browser-Konfiguration aktiviert ist. Problem im Zusammenhang mit bekannten [Fehlern in Google Chrome](#).
- Websites aus verbotenen Kategorien werden in Google Chrome eventuell nicht blockiert, wenn der Benutzer sie aus der App eines Drittanbieters heraus öffnet (z. B. aus einem IM-Client). Das Problem ist verbunden mit den Besonderheiten des Dienstes für erleichterte Bedienung mit der Funktion Chrome Custom Tabs.
- Die verbotenen Websites werden im Samsung Internet Browser eventuell nicht blockiert, wenn der Benutzer sie im Hintergrundmodus aus dem Kontextmenü oder aus der App eines Drittanbieters heraus öffnet (z. B. aus einem IM-Client).
- Für die Ausführung des Web-Filters muss Kaspersky Endpoint Security für Android als Dienst für erleichterte Bedienung installiert sein.
- Beachten Sie bei der Eingabe der Adresse einer Website in den Einstellungen von Web-Filter die folgenden Regeln:
  - Geben Sie für Android-Geräte die Adresse im Format eines regulären Ausdrucks an (z. B. `http://www.example.com.*`).
  - Geben Sie für iOS MDM-Geräte das Datenübertragungsprotokoll HTTP oder HTTPS an (beispielsweise `http://www.example.com`) an.
- Im Samsung Internet Browser können im Modus des Web-Filters **Nur aufgezählte Websites sind erlaubt** beim Neuladen der Seite eventuell erlaubte Websites blockiert werden. Die Websites werden blockiert, wenn der reguläre Ausdruck zusätzliche Parameter enthält (z. B. `^https?:\\example\\.com\\/pictures\\/`). Es wird empfohlen, reguläre Ausdrücke ohne zusätzliche Parameter zu verwenden (z. B. beispielsweise `^https?:\\example\\.com`).

## Bekannte Probleme bei der Ausführung von Diebstahlschutz

- Zur schnellen Übermittlung von Befehlen an Android-Geräte verwendet die App den Dienst Firebase Cloud Messaging (FCM). Werden die Einstellungen von FCM nicht angepasst, so werden die Befehle nur während der Synchronisierung des Geräts mit Kaspersky Security Center nach dem Zeitplan übermittelt, der in der Richtlinie festgelegt wurde (z. B. alle 24 Stunden).
- Um das Gerät sperren zu können, muss Kaspersky Endpoint Security für Android als Geräteadministrator installiert sein.

- Auf Geräten mit dem Betriebssystem Android 7.0 und höher muss Kaspersky Endpoint Security für Android als Dienst für erleichterte Bedienung installiert sein, um das Gerät sperren zu können.
- Auf einigen Geräten können die Befehle von Diebstahlschutz nicht ausgeführt werden, wenn das Gerät sich im Stromsparmodus befindet. Dieser Defekt wurde für Alcatel 5080X bestätigt.
- Um Geräte mit Android 10.0 und höher zu orten, muss der Benutzer die Berechtigung "Immer" für die Verwendung des Standorts erteilen.
- Um ein Foto auf einem Gerät mit Android 11.0 und höher aufzunehmen, muss der Benutzer die Berechtigung "Nur während Nutzung der App" für den Kamerazugriff erteilen.

## Bekannte Probleme bei der Ausführung von Anwendungskontrolle

- Für die Ausführung der Anwendungskontrolle muss Kaspersky Endpoint Security für Android als Dienst für erleichterte Bedienung installiert sein.
- Damit die Anwendungskontrolle (Kontrolle von App-Kategorien) ausgeführt werden kann, muss die Nutzung von Kaspersky Security Network aktiviert werden. Die Anwendungskontrolle ermittelt die App-Kategorie anhand der Daten, die in KSN verfügbar sind. Für die Nutzung von KSN benötigt das mobile Gerät Internetzugang. Um die Anwendungskontrolle zu verwenden, können Sie einzelne Apps zu Listen verbotener und erlaubter Anwendungen hinzufügen. In diesem Fall ist der Zugriff auf KSN nicht erforderlich.
- Es wird empfohlen, bei der Konfiguration der Anwendungskontrolle das Kontrollkästchen **System-Apps sperren** zu deaktivieren. Das Sperren von System-Apps kann zu Störungen im Betrieb des Geräts führen.

## Bekannte Probleme bei der E-Mail-Konfiguration

- Das E-Mail-Postfach kann nur auf folgenden Geräten per Remote-Zugriff konfiguriert werden:
  - iOS MDM-Geräte.
  - Samsung-Geräte (Exchange ActiveSync).
  - Android-Geräte mit dem installierten Mail-Client TouchDown.

In älteren Versionen von Kaspersky Endpoint Security für Android können Sie die Einstellungen des TouchDown-Profiles auf dem Gerät des Benutzers per Fernzugriff mithilfe von Kaspersky Security Center anpassen. In Kaspersky Endpoint Security für Android Service Pack 4 wird TouchDown nicht mehr unterstützt. Weitere Informationen finden Sie auf der [Website des technischen Supports von Symantec](#).

Nach dem Update des Verwaltungs-Plug-ins für Kaspersky Endpoint Security für Android werden die TouchDown-Einstellungen in der Richtlinie ausgeblendet, bleiben aber gespeichert. Bei der Verbindung neuer Geräte werden die TouchDown-Einstellungen nach der Übernahme der Richtlinie eingerichtet.

Nach der Änderung und Speicherung der Richtlinie werden die TouchDown-Einstellungen gelöscht. Die TouchDown-Einstellungen auf den Geräten der Benutzer werden nach der Anwendung der Richtlinie zurückgesetzt.

## Bekannte Probleme beim Anpassen der Zuverlässigkeit des Kennworts zum Entsperren des Geräts.

- Auf Geräten mit Android 10.0 oder später löst Kaspersky Endpoint Security die Anforderungen an die Zuverlässigkeit des Kennworts in einen der Systemwerte auf: Mittel oder Hoch.

Wenn einen Kennwortlänge von 1 bis 4 Zeichen erforderlich ist, fordert die App den Benutzer auf, ein Kennwort mittlerer Stärke festzulegen. Dieses muss entweder numerisch (PIN) ohne wiederholte oder aufeinanderfolgende (z. B. 1234) Sequenzen oder alphanumerisch sein. PIN oder Kennwort müssen mindestens 4 Zeichen lang sein.

Wenn einen Kennwortlänge von 5 oder mehr Zeichen erforderlich ist, fordert die App den Benutzer auf, ein Kennwort hoher Stärke festzulegen. Dieses muss entweder numerisch (PIN) ohne wiederholte oder aufeinanderfolgende Sequenzen oder alphanumerisch (Kennwort) sein. Die PIN muss mindestens 8 Zeichen lang sein, das Kennwort muss mindestens 6 Zeichen lang sein.

- Auf Geräten unter Android 10.0 oder später kann die Verwendung des Fingerabdrucks zum Entsperren des Bildschirms nur für das Arbeitsprofil verwaltet werden.
- Wenn auf Geräten mit Android 7.1.1 das Passwort zum Entsperren nicht den Anforderungen an die Unternehmenssicherheit entspricht (Übereinstimmungsüberprüfung), wird die System-App "Einstellungen" beim Versuch, das Passwort zum Entsperren in Kaspersky Endpoint Security für Android zu ändern, möglicherweise nicht ordnungsgemäß ausgeführt. Problem im Zusammenhang mit bekannten [Fehlern in Android 7.1.1](#). Verwenden Sie in diesem Fall nur die Systemanwendung "Einstellungen", um das Passwort zu ändern.
- Auf einigen Geräten mit Android 6.0 und höher kann bei der Eingabe des Passworts zum Entsperren ein Fehler auftreten, wenn die Daten auf dem Gerät verschlüsselt sind. Das Problem ist verbunden mit den Besonderheiten des Dienstes für erleichterte Bedienung in MIUI-Firmware.

## Bekannte Probleme bei der WLAN-Konfiguration

- Auf Geräten mit dem Betriebssystem Android Version 8.0 und höher können die Einstellungen des Proxyservers ein WLAN-Netzwerk nicht mithilfe der Richtlinie angepasst werden. Sie können die Proxyserver-Einstellungen für das WLAN-Netzwerk auf dem mobilen Gerät manuell anpassen.

## Bekannte Probleme bei der APN-Konfiguration

- Die APN-Konfiguration per Remote-Zugriff ist nur auf iOS MDM-Geräten oder Samsung-Geräten verfügbar.
- Sie können die APN-Einstellungen für iOS MDM-Geräte im Abschnitt **Mobilfunk** anpassen. Der Abschnitt **APN** ist veraltet. Bevor Sie die APN-Einstellungen anpassen, stellen Sie sicher, dass das Kontrollkästchen **Auf dem Gerät anwenden** im Abschnitt **APN** deaktiviert ist.

## Bekannte Probleme mit der Firewall

- Die Nutzung der Firewall ist nur auf Samsung-Geräten verfügbar.

## Bekannte Probleme bei der VPN-Konfiguration

- Die VPN-Einstellungen können nur auf folgenden Geräten per Remote-Zugriff konfiguriert werden:
  - iOS MDM-Geräte.

- Samsung-Geräte.

## Bekannte Probleme beim Arbeiten mit Containern

- In Kaspersky Security für mobile Endgeräte Service Pack 3 Maintenance Release 2 wird das Erstellen von Containern für mobile Apps nicht mehr unterstützt. Sie können jedoch Container auf Android-Geräten hinzufügen, die in früheren Programmversionen erstellt wurden.
- Um die App-Installation in Containern zu ermöglichen, muss auf dem mobilen Gerät des Benutzers die Installation von Apps aus unbekannten Quellen erlaubt sein. Nähere Informationen über die Installation von Apps ohne Google Play finden Sie in der [Android-Hilfe](#).
- Die Containerisierung von Anwendungen für Android-Geräte, die mehr als 65.536 Methoden unterstützen (multidex configuration) wird nicht unterstützt.

## Bekannte Probleme mit dem Schutz der App vor der Deinstallation

- Kaspersky Endpoint Security für Android muss als Geräteadministrator installiert werden.
- Auf den Geräten unter Verwaltung des Betriebssystems Android 7.0 und höher muss zum Schutz der App vor dem Löschen Kaspersky Endpoint Security für Android als Dienst für erleichterte Bedienung installiert sein.
- Auf einigen Geräten von Xiaomi und Huawei funktioniert der Schutz von Kaspersky Endpoint Security für Android gegen die Deinstallation nicht. Das Problem wird durch Besonderheiten der Firmware für MIUI 7 und 8 auf Xiaomi und der EMUI-Firmware auf Huawei verursacht.

## Bekannte Probleme bei der Konfiguration von Gerätebeschränkungen

- Auf Geräten mit Android 10.0 oder höher wird das Verbot der Verwendung von WLAN-Netzwerken nicht unterstützt.
- Auf Geräten mit Android 10.0 oder höher kann die Nutzung der Kamera nicht vollständig verboten werden.
- Auf Geräten mit dem Betriebssystem Android 11 und höher muss Kaspersky Endpoint Security für Android als Dienst für erleichterte Bedienung installiert sein. Der Assistent für die Erstkonfiguration von Kaspersky Endpoint Security für Android ermöglicht dem Benutzer, die App als Bedienungshilfe zu installieren. Der Benutzer kann diesen Schritt überspringen oder den Dienst in den Einstellungen des Geräts später deaktivieren. In einem solchen Fall können Sie die Verwendung der Kamera nicht einschränken.

## Bekannte Probleme beim Senden von Befehlen an mobile Geräte

- Wenn der Benutzer auf Geräten mit Android 12 oder höher die Berechtigung "Ungefährer Standort verwenden" erteilt hat, versucht die App "Kaspersky Endpoint Security für Android" zunächst, den genauen Standort des Geräts zu ermitteln. Gelingt dies nicht, wird der ungefähre Gerätestandort nur zurückgegeben, wenn er frühestens 30 Minuten zuvor empfangen wurde. Andernfalls schlägt der Befehl **Gerät orten** fehl.

## Bekannte Probleme mit dem Arbeitsprofil Android

- Wenn Sie ein Android-Arbeitsprofil mithilfe einer Richtlinie erstellen, muss der Benutzer die Berechtigung "Zugriff auf alle Dateien" den Instanzen von Kaspersky Endpoint Security für Android erteilen, die auf Geräten mit Android 11 oder höher installiert sind und die sich auf das Arbeitsprofil beziehen.



## Bekannte Probleme mit bestimmten Geräten

- Auf bestimmten Geräten (zum Beispiel Huawei, Meizu und Xiaomi) müssen Sie Kaspersky Endpoint Security für Android die Berechtigung für Autostart erteilen oder das Programm manuell zur Liste der Apps hinzufügen, die beim Hochfahren des Betriebssystems gestartet werden. Wenn die App nicht zur Liste hinzugefügt wird, stellt Kaspersky Endpoint Security für Android nach dem Neustart des mobilen Geräts sämtliche Funktionen ein. Außerdem kann das Gerät nicht mit einem Befehl entsperrt werden, wenn es gesperrt wurde. Sie können das Gerät nur mithilfe des einmaligen Codes für die Freischaltung entsperren.
- Nach der Datenverschlüsselung und dem Neustart des Geräts verlangt Android auf einigen Geräten (z. B. Meizu, Asus) unter Android 6.0 und höher die Eingabe des Zahlencodes. Wenn der Benutzer ein Sperrmuster für das Entsperren verwendet, muss das Sperrmuster in einen Zifferncode übersetzt werden. Weitere Informationen zur Eingabe des Sperrmusters als Zahlencode finden Sie auf der Website des technischen Supports des Herstellers ihres mobilen Geräts. Das Problem ist verbunden mit den Besonderheiten des Dienstes für erleichterte Bedienung.
- Auf einigen Huawei-Geräten mit Android 5.X wird nach dem Festlegen von Kaspersky Endpoint Security für Android als Dienst für erleichterte Bedienung eine fehlerhafte Benachrichtigung über das Fehlen der entsprechenden Berechtigungen angezeigt. Um diese Benachrichtigung auszublenden, aktivieren Sie die App in den Geräteeinstellungen als geschützt.
- Auf einigen Huawei-Geräten mit Android 5.X und 6.X kann der Benutzer bei aktiviertem Stromsparmodus für Kaspersky Endpoint Security für Android die Ausführung der App selbständig beenden. Das Gerät des Benutzers ist dabei nicht geschützt. Das Problem ist verbunden mit den Besonderheiten der Software von Huawei. Um den Schutz des Geräts wiederherzustellen, starten Sie Kaspersky Endpoint Security für Android manuell. Es wird empfohlen den Stromsparmodus für Kaspersky Endpoint Security für Android in den Geräteeinstellungen zu deaktivieren.
- Auf Huawei-Geräten mit der Firmware EMUI unter Android 7.0 kann der Benutzer die Benachrichtigung über den Schutzstatus von Kaspersky Endpoint Security für Android ausblenden. Das Problem ist verbunden mit den Besonderheiten der Software von Huawei.
- Auf einigen Xiaomi-Geräten wird der Benutzer aufgefordert, nicht den PIN-Code, sondern das Passwort zum Entsperren des Bildschirms zu ändern, wenn die Kennwortlänge in der Richtlinie auf länger als 5 Zeichen festgelegt wurde. Es ist nicht möglich, einen PIN-Code mit mehr als 5 Zeichen festzulegen. Das Problem ist verbunden mit den Besonderheiten der Software von Xiaomi.
- Auf Xiaomi-Geräten mit der Firmware MIUI unter Android 6.0 ist das Symbol von Kaspersky Endpoint Security für Android in der Statuszeile evtl. ausgeblendet. Das Problem ist verbunden mit den Besonderheiten der Software von Xiaomi. Es wird empfohlen, die Anzeige von Benachrichtigungssymbolen in den Benachrichtigungseinstellungen zu erlauben.
- Auf einigen Nexus-Geräten unter Android 6.0.1 ist es während der Ausführung des Schnellstartassistenten für Kaspersky Endpoint Security für Android nicht möglich, die erforderlichen Rechte für eine ordnungsgemäße App-Funktion zu erteilen. Das Problem ist mit einem bekannten Defekt im Security Patch für Android von Google verbunden. Für die ordnungsgemäße App-Funktion müssen die erforderlichen Rechte in den Einstellungen des Geräts manuell erteilt werden.
- Auf einigen Samsung-Geräten mit dem Betriebssystem Android 7.0 und höher kann das Gerät gesperrt werden, wenn der Benutzer versucht, das Gerät mit einer nicht unterstützten Methode zu entsperren (z. B. mit Sperrmuster), und folgende Bedingungen erfüllt sind: Der Schutz vor Deinstallation für Kaspersky Endpoint Security für Android ist aktiviert und die Anforderungen an die Stärke des Kennworts zum Entsperren des Geräts sind festgelegt. Zum Entsperren muss ein bestimmter Befehl an das Gerät gesendet werden.
- Auf einigen Samsung-Geräten ist es nicht möglich, die Verwendung von Fingerabdrücken zum Entsperren des Bildschirms zu verbieten.



- Auf einigen Samsung-Geräten funktioniert Web-Filter nicht, wenn das Gerät mit einem 3G/4G-Netzwerk verbunden ist, auf dem Gerät der Stromsparmodus aktiviert ist und die Hintergrunddaten eingeschränkt sind. Es wird empfohlen, die Funktion zur Einschränkung von Hintergrundprozessen in den Stromspareinstellungen zu deaktivieren.
- Außerdem verbietet Kaspersky Endpoint Security für Android auf einigen Samsung-Geräten, auf denen das Kennwort zum Entsperren nicht den Anforderungen an die Unternehmenssicherheit entspricht, die Nutzung der Fingerabdrücke für das Entsperren des Bildschirms nicht.
- Auf einigen Samsung-Geräten werden das allgemeine Zertifikat und das VPN-Zertifikat manchmal nach der Ausführung eines Befehls von Diebstahlschutz (Suche, Gerätesperre, Entsperren und Fotografieren) gelöscht. Für die weitere Ausführung müssen die Zertifikate erneut installiert werden. Das Problem ist mit dem Sicherheitsstandard "Mobile Device Fundamentals Protection Profile" (MDFPP) verbunden.
- Bei einigen Geräten der Marken Honor und Huawei können Sie die Verwendung von Bluetooth nicht einschränken. Wenn Kaspersky Endpoint Security für Android versucht, die Verwendung von Bluetooth einzuschränken, zeigt das Betriebssystem eine Benachrichtigung mit den folgenden Optionen an: Ablehnen oder Zulassen. Auf diese Weise kann der Benutzer die Einschränkung ablehnen und weiterhin Bluetooth verwenden.
- Auf einigen Samsung-Geräten ist die Aktivierung des KNOX MDM-Profiles nach der Installation oder Aktualisierung von Kaspersky Endpoint Security aus einem eigenständigen Installationspaket nicht verfügbar.
- Auf Blackview-Geräten kann der Benutzer den Speicher der App "Kaspersky Endpoint Security für Android" löschen. Als Folge werden der Geräteschutz und die Geräteverwaltung deaktiviert, alle festgelegten Einstellungen werden wirkungslos und die App von Kaspersky Endpoint Security für Android wird aus den Diensten für erleichterte Bedienung entfernt. Dies liegt daran, dass die Geräte dieses Anbieters die angepasste App "Letzte Anwendungen" enthalten, die mit erhöhten Rechten ausgestattet ist. Diese App kann die Einstellungen von Kaspersky Endpoint Security für Android außer Kraft setzen und kann nicht ersetzt werden, da sie Teil des Android-Betriebssystems ist.
- Auf einigen Geräten mit Android 11 stürzt die App von Kaspersky Endpoint Security für Android sofort nach dem Start ab. Das Problem hängt mit dem bekannten [Fehler in Android 11](#) zusammen.

## Verteilung

Dieser Abschnitt der Hilfe richtet sich an Experten, die für die Installation von Kaspersky Security für mobile Endgeräte zuständig sind, sowie an Experten, die für die technische Unterstützung von Unternehmen verantwortlich sind, die Kaspersky Security für mobile Endgeräte einsetzen.

## Lösungsarchitektur

Kaspersky Security für mobile Endgeräte besteht aus folgenden Komponenten:

- Mobile Anwendung Kaspersky Endpoint Security für Android.

Die App "Kaspersky Endpoint Security für Android" gewährleistet den Schutz mobiler Geräte vor Webbedrohungen, Viren und anderen gefährlichen Programmen. Gewährleistet die Interaktion zwischen dem mobilen Gerät und dem Kaspersky Security Center Administrationsserver mithilfe von Firebase Cloud Messaging.

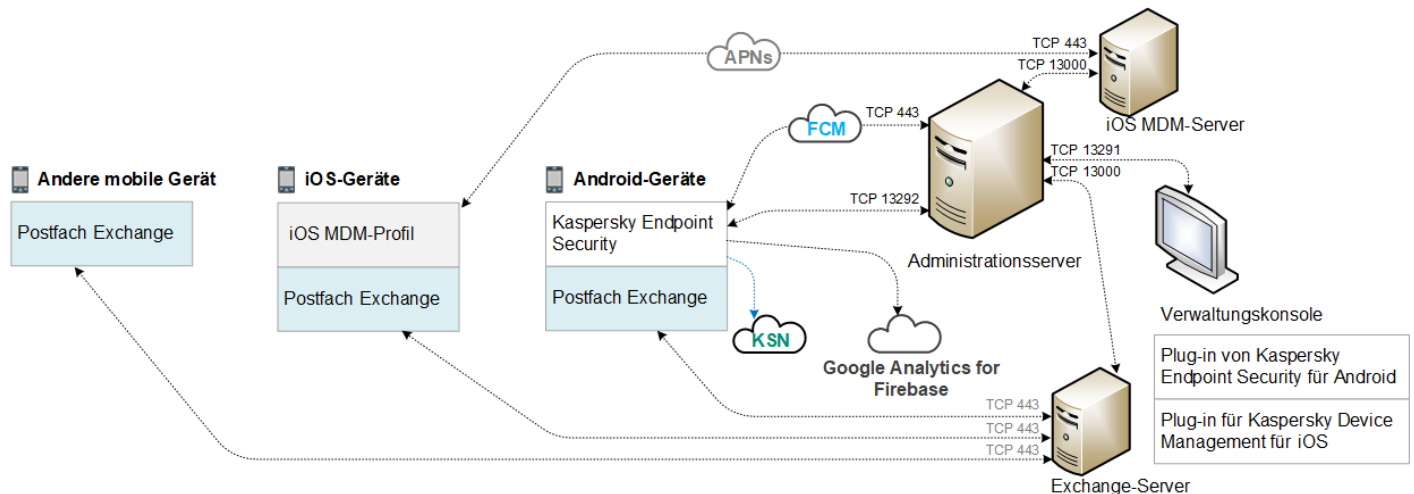
- Verwaltungs-Plug-in von Kaspersky Endpoint Security für Android

Das Verwaltungs-Plug-in für Kaspersky Endpoint Security für Android bietet eine Verwaltungsschnittstelle für mobile Endgeräte und darauf installierte mobile Anwendungen über die Administrationskonsole von Kaspersky Security Center.

- Verwaltungs-Plug-in für Kaspersky Device Management für iOS

Das Verwaltungs-Plug-in für Kaspersky Device Management für iOS ist eine Schnittstelle, mit deren Hilfe mobile Geräte, die über das Protokoll iOS MDM bzw. Exchange ActiveSync verbunden sind, über die Verwaltungskonsole von Kaspersky Security Center verwaltet werden können.

Die Architektur von Kaspersky Security für mobile Endgeräte ist in der nachfolgenden Abbildung dargestellt.



Architektur von Kaspersky Security für mobile Endgeräte

Weitere Informationen über die Verwaltungskonsole, den Administrationsserver, den Exchange-Server und den iOS MDM-Server finden Sie in der [Hilfe zu Kaspersky Security Center](#).

## Typische Vorgehensweisen bei der Verteilung der Komplexlösung

Dieser Abschnitt informiert über die typischen Verteilungsschemata von Kaspersky Endpoint Security für mobile Endgeräte.

Die Verteilung der Komplexlösung auf Android-Geräten und iOS-Geräten erfolgt gemäß unterschiedlichen Schemata. Wenn im Unternehmen mobilen Geräte unter verschiedenen Betriebssystemen verwendet werden, muss die Installation der Anwendung für jedes Betriebssystem separat gemäß dem entsprechenden Verteilungsschema durchgeführt werden.

## Verteilungsschemata für Kaspersky Endpoint Security für Android

Kaspersky Endpoint Security für Android kann im Unternehmensnetzwerk mithilfe verschiedener Methoden auf die mobilen Geräte verteilt werden. Sie können die für Ihr Unternehmen geeignetste Methode zur Verteilung auswählen oder auch mehrere Verteilungsmethoden gleichzeitig verwenden.

Weitere Informationen zur Verteilung von Kaspersky Endpoint Security für Android über Kaspersky Endpoint Security Cloud finden Sie in der [Hilfe zu Kaspersky Endpoint Security Cloud](#).

## Verteilungsschemata für Kaspersky Endpoint Security für Android über Kaspersky Security Center

Die Verteilung von Kaspersky Endpoint Security für Android über Kaspersky Security Center kann auf folgende Arten durchgeführt werden:

- Mithilfe des Versands von Nachrichten mit einem Link auf Google Play (empfohlen)
- Mithilfe des Versands von Nachrichten mit einem Link zum eigenständigen Paket der App

Die [Verteilung von Kaspersky Endpoint Security für Android mithilfe von Google Play](#) besteht aus dem Versand von Nachrichten aus der Verwaltungskonsolle mit einem Link auf Google Play an die Benutzer der Geräte.

Die Verteilung von Kaspersky Endpoint Security für Android mithilfe des Versandes des autonomen Paketes besteht aus den folgenden Aktionen des Administrators:

1. [Erstellen eines Installationspakets für die Anwendung.](#)
2. [Anpassen des Installationspakets.](#)
3. [Erstellen eines eigenständigen Installationspakets.](#)
4. [Versand einer Nachricht mit einem Link zum Herunterladen des eigenständigen Installationspakets an die Benutzer von Android-Geräten. Ein Massenversand ist möglich.](#)

Die Installation von Kaspersky Endpoint Security für Android auf dem mobilen Gerät wird vom Benutzer durchgeführt, nachdem dieser die Nachricht mit dem Link auf Google Play oder zum Herunterladen der Programmdistribution vom Webserver für Kaspersky Security Center erhalten hat. Zusätzliche Vorbereitungen für die Ausführung der App sind nicht erforderlich.

## Verteilungsschema für Kaspersky Endpoint Security für Android aus Google Play

Es ist empfehlenswert, das Verteilungsschema aus Google Play zu verwenden, wenn keine Remote-Installation durchgeführt werden kann.

Die Installation von Kaspersky Endpoint Security für Android aus Google Play wird vom Benutzer des Geräts selbstständig durchgeführt. Der Benutzer lädt die Distribution der mobilen Anwendung aus Google Play herunter und installiert sie auf dem Gerät. Nach der Installation der Anwendung auf dem mobilen Gerät sind zusätzliche Vorbereitungsarbeiten erforderlich: Konfiguration der Verbindungseinstellungen zum Administrationsserver und Installation eines [allgemeinen Zertifikats](#).

## Verteilungsschema für Kaspersky Endpoint Security für Android über KNOX Mobile Enrollment

Kaspersky Endpoint Security für Android wird verteilt, indem das KNOX MDM-Profil auf mobilen Geräten hinzugefügt wird. Das KNOX MDM-Profil enthält den Link zur App, die sich auf dem Webserver für Kaspersky Security Center oder auf einem anderen Server befindet. Nach der Installation der App auf dem mobilen Gerät muss zusätzlich ein [allgemeines Zertifikat](#) installiert werden.

Weitere Informationen zur Installation über KNOX Mobile Enrollment finden Sie im Abschnitt [Samsung KNOX](#).

## Verteilungsschemata für das iOS MDM-Profil

Das *iOS MDM-Profil* ist ein Profil, das die Verbindungseinstellungen für mobile Geräte unter Verwaltung des Betriebssystems iOS zu Kaspersky Security Center enthält. Nach der Installation des iOS MDM-Profiles und der Synchronisierung mit Kaspersky Security Center wird das Gerät zu einem verwalteten Gerät. Die Verwaltung der mobilen Geräte wird mithilfe von Apple Push Notification Service (APNs) realisiert. Weitere Informationen über die Installation des iOS MDM-Profiles und die Arbeit mit APNs finden Sie in der [Hilfe zu Kaspersky Security Center](#).

Mithilfe des iOS MDM-Profiles können Sie folgende Aktionen ausführen:

- Die Einstellungen der iOS MDM-Geräte mithilfe der Gruppenrichtlinien ferngesteuert anpassen.
- Befehle zum Sperren des Geräts und Löschen der Daten absenden.
- Apps von Kaspersky sowie andere Dritthersteller-Apps ferngesteuert installieren.

Das iOS MDM-Profil kann auf den mobilen Geräten im Netzwerk des Unternehmens auf verschiedene Weise geöffnet werden. Sie können die für Ihr Unternehmen geeignetste Methode zur Verteilung auswählen oder auch mehrere Verteilungsmethoden gleichzeitig verwenden.

Vor der Verteilung des iOS MDM-Profiles muss der Administrator wie folgt vorgehen:

1. Den iOS MDM-Server für Mobilgeräte installieren.
2. Das Zertifikat Apple Push Notification Service (APNs-Zertifikat) abrufen.
3. Das APNs-Zertifikat auf dem iOS MDM-Server für Mobilgeräte installieren.

Weitere Informationen über die Installation des iOS MDM-Servers für Mobilgeräte und die Arbeit mit dem APNs-Zertifikat finden Sie in der [Hilfe zu Kaspersky Security Center](#).

Weitere Informationen über die Verteilung des iOS MDM-Profiles in Kaspersky Endpoint Security Cloud finden Sie in der [Hilfe zu Kaspersky Endpoint Security Cloud](#).

## Verteilungsschemata für das iOS MDM-Profil über Kaspersky Security Center

Die Verteilung des iOS MDM-Profiles über Kaspersky Security Center kann mithilfe des Versands von Nachrichten mit einem Link zum Download des iOS MDM-Profiles durchgeführt werden. Ein Massenversand ist möglich.

Die Installation des iOS MDM-Profiles auf dem mobilen Gerät wird vom Benutzer durchgeführt, nachdem dieser die Nachricht mit dem Link auf den Webserver für Kaspersky Security Center erhalten hat. Eine weitere Vorbereitung des iOS MDM-Profiles ist nicht erforderlich.

Nähere Informationen über die Erstellung eines iOS MDM-Profiles finden Sie in der [Hilfe zu Kaspersky Security Center](#).

## Verwaltungskonsole für die Verteilung der Komplexlösung vorbereiten

Dieser Abschnitt enthält Anweisungen zur Vorbereitung der Verwaltungskonsole für die Verteilung der Komplexlösung.

## Einstellungen des Administrationsservers für die Anbindung von mobilen Endgeräten anpassen

Damit die mobilen Geräte eine Verbindung zum Administrationsserver herstellen können, müssen vor der Installation der mobilen App Kaspersky Endpoint Security die Verbindungseinstellungen der mobilen Geräte in den Eigenschaften des Administrationsservers konfiguriert werden.

*Um die Einstellungen des Administrationsservers für die Verbindung von mobilen Geräten anzupassen, gehen Sie wie folgt vor:*

1. Wählen Sie im Kontextmenü des Administrationsservers den Punkt **Eigenschaften** aus.  
Das Eigenschaftsfenster des Administrationsservers wird geöffnet.
2. Wählen Sie den Abschnitt **Verbindungseinstellungen des Servers** → **Zusätzliche Ports** aus.
3. Aktivieren Sie das Kontrollkästchen **Port für mobile Endgeräte öffnen**.
4. Geben Sie im Feld **Port für mobile Geräte** den Port an, über den mit dem Administrationsserver mobile Geräte verbunden werden sollen.  
Als Standard wird Port 13292 verwendet. Wenn das Kontrollkästchen **Port für mobile Endgeräte öffnen** deaktiviert ist oder ein ungültiger Port für die Verbindung angegeben wurde, können mobile Geräte keine Verbindung mit dem Administrationsserver herstellen.
5. Geben Sie im Feld **Port zur Aktivierung von mobilen Clients** den Port an, über den sich die mobilen Geräte mit dem Administrationsserver verbinden sollen, um die App Kaspersky Endpoint Security für Android zu aktivieren.  
Als Standard wird Port 17100 verwendet.
6. Klicken Sie auf **OK**.

## Ordner Mobile Geräte verwalten in der Verwaltungskonsole anzeigen

Das Verzeichnis der mobilen Endgeräte, die vom Administrationsserver verwaltet werden, kann in der Verwaltungskonsole in der Ansicht des Ordners **Mobile Geräte verwalten** angezeigt werden. Des Weiteren können hier Verwaltungseinstellungen für mobile Endgeräte angepasst werden.

*Um die Ansicht des Ordners **Mobile Geräte verwalten** in der Verwaltungskonsole zu aktivieren, gehen Sie wie folgt vor:*

1. Wählen Sie im Kontextmenü des Administrationsservers den Punkt **Ansicht** → **Benutzeroberfläche anpassen** aus.
2. Aktivieren Sie im folgenden Fenster das Kontrollkästchen **Mobile Geräte verwalten anzeigen**.
3. Klicken Sie auf **OK**.

Der Ordner **Mobile Geräte verwalten** wird nach dem Neustart der Verwaltungskonsole in der Struktur der Verwaltungskonsole angezeigt.

## Administrationsgruppe erstellen

Zur zentralen Konfiguration der App Kaspersky Endpoint Security für Android, die auf den mobilen Geräten der Benutzer installiert ist, müssen [Gruppenrichtlinien](#) auf diese Geräte angewendet werden.

Um eine Richtlinie auf eine Gerätegruppe anzuwenden, sollte vor der Installation von mobilen Anwendungen auf den Geräten der Benutzer für die entsprechenden Geräte im Ordner **Verwaltete Geräte** eine separate Administrationsgruppe erstellt werden.

Nach dem Erstellen der Administrationsgruppe ist es empfehlenswert, die [automatische Verschiebung von Geräten in diese Gruppe anzupassen](#), auf denen Sie die Apps installieren wollen. Danach müssen mithilfe der Gruppenrichtlinie gemeinsame Einstellungen für alle Geräte festgelegt werden.

*Um eine Administrationsgruppe zu erstellen, gehen Sie wie folgt vor:*

1. Wählen Sie in der Konsolenstruktur den Ordner **Verwaltete Geräte**.
2. Wählen Sie im Arbeitsbereich des Ordners **Verwaltete Geräte** oder eines Unterordners die Registerkarte **Geräte**.
3. Klicken Sie auf **Gruppe erstellen**.

Das Fenster zum Erstellen einer der neuen Gruppe wird geöffnet.

4. Geben Sie im folgenden Fenster **Gruppenname** einen Namen für die Gruppe an und klicken Sie auf **OK**.

In der Konsolenstruktur erscheint ein neuer Ordner für die Administrationsgruppe mit dem festgelegten Namen. Weitere Informationen über Administrationsgruppen finden Sie in der [Hilfe zu Kaspersky Security Center](#).

## Erstellen einer Regel für das automatische Verschieben von Geräten in eine Administrationsgruppe

Eine zentrale Verwaltung der Einstellungen für die App Kaspersky Endpoint Security für Android, die auf mobilen Geräten der Benutzer installiert ist, ist nur dann möglich, wenn diese Geräte sich in einer zuvor erstellten Administrationsgruppe befinden, [für die eine Gruppenrichtlinie vorhanden ist](#).

Wenn keine Regel für das automatische Verschieben von in Netzwerken gefundenen mobilen Geräten in die Administrationsgruppe angegeben ist, wird ein Gerät nach der ersten Synchronisierung des Geräts mit dem Administrationsserver automatisch in die Verwaltungskonsolle, in den Ordner **Erweitert** → **Netzwerkabfrage** → **Domänen** → **KES10** verschoben. Die Gruppenrichtlinie wird auf dieses Gerät nicht angewendet.

*Um eine Regel für das automatische Verschieben von mobilen Endgeräten in eine Administrationsgruppe zu erstellen, gehen Sie wie folgt vor:*

1. Wählen Sie in der Konsolenstruktur den Ordner **Nicht zugeordnete Computer und Geräte anzeigen**.
2. Wählen Sie im Kontextmenü des Ordners **Nicht zugeordnete Computer und Geräte anzeigen** den Punkt **Eigenschaften** aus.  
Daraufhin wird das Fenster **Eigenschaften: Nicht zugeordnete Geräte** geöffnet.
3. Klicken Sie im Abschnitt **Verschieben von Geräten** auf **Hinzufügen**, um den Vorgang zum Erstellen einer Regel für das automatische Verschieben von Geräten in eine Administrationsgruppe zu starten.  
Das Fenster **Neue Regel** wird geöffnet.
4. Geben Sie einen Namen für die Regel ein.
5. Geben Sie an, in welche Administrationsgruppe die Geräte nach der Installation der mobilen App Kaspersky Endpoint Security für Android verschoben werden sollen. Klicken Sie dazu rechts vom Feld **Gruppe, in die die Geräte verschoben werden sollen** auf **Durchsuchen** und wählen Sie im folgenden Fenster eine Gruppe aus.

6. Wählen Sie im Abschnitt **Regelausführung** die Variante **Wird einmal pro Gerät ausgeführt** aus.
7. Aktivieren Sie das Kontrollkästchen **Nur Geräte verschieben, die sich nicht in Administrationsgruppen befinden**, damit durch die Anwendung dieser Regel mobile Geräte, die bereits anderen Administrationsgruppen zugeordnet wurden, nicht in die ausgewählte Gruppe verschoben werden.
8. Aktivieren Sie das Kontrollkästchen **Regel aktivieren**, damit die Regel auf neu gefundene Geräte angewendet wird.
9. Öffnen Sie den Abschnitt **Programme** und gehen Sie wie folgt vor:
  - a. Aktivieren Sie das Kontrollkästchen **Version des Betriebssystems**.
  - b. Wählen Sie eines oder mehrere Betriebssysteme für die Geräte aus, die in die angegebene Gruppe verschoben werden sollen: Android oder iOS.
10. Klicken Sie auf **OK**.

Die erstellte Regel steht auf der Liste für Regeln für das Verschieben von Geräten im Abschnitt **Verschieben von Geräten** im Eigenschaftsfenster des Ordners **Nicht zugeordnete Geräte anzeigen**.

Wenn die Regel ausgeführt wird, verschiebt Kaspersky Security Center alle Geräte, die den Bedingungen entsprechen, aus dem Ordner **Nicht zugeordnete Geräte** in die von Ihnen angegebene Administrationsgruppe. Mobile Endgeräte, die zuvor in den Ordner **Nicht zugeordnete Geräte anzeigen** verschoben wurden, können auch manuell in eine gewünschte Administrationsgruppe des Ordners **Verwaltete Geräte** verschoben werden. Weitere Informationen über die Verwaltung von Administrationsgruppen und über den Umgang mit nicht zugeordneten Geräten finden Sie in der [Hilfe zu Kaspersky Security Center](#).

## Allgemeines Zertifikat erstellen

Zur Identifizierung des Mobilgerätenutzers muss in der Verwaltungskonsole ein allgemeines Zertifikat erstellt werden.

*Um ein allgemeines Zertifikat zu erstellen, gehen Sie wie folgt vor:*

1. Wählen Sie in der Konsolenstruktur den Ordner **Mobile Geräte verwalten** → **Zertifikate**.
2. Starten Sie im Arbeitsplatz des Ordners **Zertifikate** mithilfe des Links **Zertifikat hinzufügen** den Assistenten zur Zertifikatinstallation.
3. Wählen Sie im Fenster **Zertifikatstyp** des Assistenten die Option **Allgemeines Zertifikat**.
4. Geben Sie im Fenster **Benutzer auswählen** des Assistenten den Benutzer an, für den Sie ein allgemeines Zertifikat erstellen möchten.
5. Wählen Sie im Fenster **Ursprung des Zertifikats** des Assistenten die Methode zur Erstellung des allgemeinen Zertifikats.
  - Um das allgemeine Zertifikat mithilfe der Tools des Administrationsservers zu erstellen, wählen Sie die Option **Zertifikat mithilfe der Tools des Administrationsservers erstellen**.
  - Um einem Benutzer ein zuvor erstelltes Zertifikat zuzuweisen, wählen Sie die Option **Zertifikatsdatei angeben**. Öffnen Sie mithilfe der Schaltfläche **Angeben** das Fenster **Zertifikat** und geben Sie darin die Datei des Zertifikats an.

Deaktivieren Sie das Kontrollkästchen **Zertifikat veröffentlichen**, wenn Sie den Typ des mobilen Geräts und die Methode zur Benachrichtigung des Benutzers über die Erstellung des Zertifikats nicht angeben möchten.



6. Konfigurieren Sie im Fenster **Benachrichtigungsmethode** des Assistenten die Benachrichtigungseinstellungen für den Benutzer des mobilen Geräts für die Benachrichtigung über die Erstellung eines Zertifikats per SMS-Nachricht oder E-Mail.
7. Klicken Sie im Fenster **Zertifikat erstellen** auf die Schaltfläche **Fertig**, um den Assistenten zur Zertifikatsinstallation zu beenden.

Daraufhin wird ein allgemeines Zertifikat erstellt, das vom Benutzer auf dem mobilen Gerät installiert werden kann. Zum Abrufen des Zertifikats muss das mobile Gerät mit dem Administrationsserver synchronisiert werden. Weitere Informationen über die Erstellung der Zertifikate und die Anpassung der Regeln für ihre Ausstellung finden Sie in der [Hilfe zu Kaspersky Security Center](#).

## Kaspersky Endpoint Security für Android installieren

In diesem Abschnitt werden die Methoden zur Verteilung von Kaspersky Endpoint Security für Android im Unternehmensnetzwerk beschrieben.

### Berechtigungen

Kaspersky Endpoint Security für Android fragt den Benutzer nach erforderlichen Berechtigungen, damit alle App-Funktionen ordnungsgemäß ausgeführt werden können. Kaspersky Endpoint Security für Android fragt nach obligatorischen Berechtigungen während der Ausführung des Installationsassistenten sowie nach der Installation vor der Nutzung bestimmter App-Funktionen. Kaspersky Endpoint Security für Android kann nicht installiert werden, ohne dass die obligatorischen Berechtigungen erteilt werden.

Auf einigen Geräten (z. B. Huawei, Meizu, Xiaomi) muss Kaspersky Endpoint Security für Android in den Geräteeinstellungen manuell zur Liste der Apps hinzugefügt werden, die beim Start des Betriebssystems gestartet werden. Wenn die App nicht zur Liste hinzugefügt wird, stellt Kaspersky Endpoint Security für Android nach dem Neustart des mobilen Geräts sämtliche Funktionen ein.

Auf Geräten mit Android 11 oder höher müssen Sie die Systemeinstellung **Berechtigungen entfernen, wenn die App nicht verwendet wird** deaktivieren. Andernfalls setzt das System die vom Benutzer an die App erteilten Berechtigungen automatisch zurück, nachdem die App einige Monate lang nicht verwendet wurde.

In Kaspersky Endpoint Security für Android Service Pack 4 Update 4 (Version 10.8.0.103) werden der Anruf- und SMS-Filter und die SIM-Kontrolle nicht mehr unterstützt. In diesem Fall fragt Kaspersky Endpoint Security für Android den Benutzer nicht um Erlaubnis für die SMS-Verwaltung. Um den Anruf- und SMS-Filter sowie alle Funktionen der SIM-Kontrolle nutzen zu können, verwenden Sie ältere Versionen von Kaspersky Endpoint Security für Android.

Berechtigungen, die Kaspersky Endpoint Security für Android anfragt

Berechtigung	App-Funktion
<b>Telefon</b> (nur für Android 5.0 – 9.X erforderlich)	Verbindung mit Kaspersky Security Center (Geräte-ID)
<b>Speicher</b> (obligatorisch)	Anti-Virus
<b>Zugriff auf alle Dateien</b>	Anti-Virus (nur für Android 11 und höher)



<b>Bluetooth-Geräte in der Nähe</b> (für Android 12 und höher)	Bluetooth-Verwendung beschränken
<b>Geräteadministrator</b> (obligatorisch)	Diebstahlschutz – Gerät sperren (nur für Android 5.0 – 6.X)
	Diebstahlschutz – Foto mit der Frontkamera aufnehmen
	Diebstahlschutz – Alarmsignal erzeugen
	Diebstahlschutz – auf Werkseinstellungen zurücksetzen
	Kennwortschutz
	Schutz der App vor der Deinstallation
	Installation von Sicherheitszertifikaten
	Anwendungskontrolle
	KNOX-Verwaltung (nur für Samsung-Geräte)
	WLAN-Konfiguration
	Konfiguration von Exchange ActiveSync
	Beschränkung der Verwendung von Kamera, Bluetooth, WLAN
<b>Kamera</b>	Diebstahlschutz – Foto mit der Frontkamera aufnehmen  <div> Auf Geräten mit Android 11.0 und höher muss der Benutzer bei entsprechender Aufforderung die Berechtigung "Nur während Nutzung der App" erteilen. </div>
<b>Standort</b>	Diebstahlschutz – Gerät orten  <div> Auf Geräten mit Android 10.0 und höher muss der Benutzer bei entsprechender Aufforderung die Berechtigung "Immer" erteilen. </div>
<b>Erleichterte Bedienung</b>	Diebstahlschutz – Gerät sperren (nur für Android 7.0 und höher)
	Web-Filter
	Anwendungskontrolle
	Schutz der App vor der Deinstallation (nur für Android 7.0 und höher)
	Anzeige von Warnungen von Kaspersky Endpoint Security für Android (nur für Android 10.0 und höher)
	Verwendung der Kamera beschränken (nur für Android 11 und höher)

Installation von Kaspersky Endpoint Security für Android über einen Google Play-Link

Die Installation von Kaspersky Endpoint Security für Android wird auf den mobilen Geräten der Benutzer ausgeführt, deren Benutzerkonten zu Kaspersky Security Center hinzugefügt wurden. Weitere Informationen zu Benutzerkonten in Kaspersky Security Center finden Sie in der [Hilfe zu Kaspersky Security Center](#).

Kaspersky Security für mobile Endgeräte erlaubt, die App mithilfe eines Google Play-Links über Kaspersky Security Center zu installieren (empfohlene Methode).

Der Benutzer erhält einen Link auf Google Play. Die Installation wird mit der für die Android-Plattform typischen Methode ausgeführt. Nach der Installation sind keine zusätzlichen Einstellungen von Kaspersky Endpoint Security für Android erforderlich.

Einige Huawei- und Honor-Geräte nutzen keine Google-Dienste und haben deshalb keinen Zugriff auf Apps in Google Play. Wenn Benutzer von Huawei- und Honor-Geräten die App nicht über Google Play installieren können, weisen Sie sie an, die App über die Huawei App Gallery zu installieren.

Der Link enthält die folgenden Daten:

- Synchronisierungseinstellungen für Kaspersky Security Center.
- Allgemeines Zertifikat.
- Hinweis auf die Annahme der Bedingungen des Endbenutzer-Lizenzvertrags für Kaspersky Endpoint Security für Android und der zusätzlichen Erklärungen. Wenn der Administrator die Bedingungen der Lizenzvertrags und der zusätzlichen Erklärungen in der Verwaltungskonsole akzeptiert, überspringt Kaspersky Endpoint Security für Android den Annahmeschritt während der Installation der App.

*So installieren Sie Kaspersky Endpoint Security für Android über Kaspersky Security Center mithilfe eines Google Play-Links:*

1. Wählen Sie in der Konsolenstruktur den Ordner **Mobile Geräte verwalten** → **Mobile Geräte** aus.

2. Klicken Sie im Arbeitsplatz des Ordners **Mobile Geräte** auf die Schaltfläche **Mobiles Gerät hinzufügen**.

Der Assistent zur Verbindung eines neuen mobilen Geräts wird gestartet. Folgen Sie den Anweisungen.

3. Wählen Sie im Fenster **Betriebssystem** des Assistenten **Android** aus.

Kaspersky Security Center sucht nach Updates für das Verwaltungs-Plug-in. Wenn Kaspersky Security Center Updates findet, können Sie die neue Version des Verwaltungs-Plug-ins installieren. Beim Update des Verwaltungs-Plug-ins können Sie die Bedingungen des Endbenutzer-Lizenzvertrags (EULA) und der zusätzlichen Erklärungen für Kaspersky Endpoint Security für Android akzeptieren. Wurden der Lizenzvertrag und die zusätzlichen Erklärungen vom Administrator bereits in der Verwaltungskonsole akzeptiert, überspringt Kaspersky Endpoint Security für Android den Annahmeschritt während der Installation der App. Diese Funktion ist in Kaspersky Security Center 12 verfügbar.

4. Wählen Sie auf der Seite **Installationsmethode von Kaspersky Endpoint Security für Android** die App-Installationsmethode **Mithilfe eines Google Play-Links** aus.

5. Wählen Sie auf der Seite **Auswahl der Benutzer** des Assistenten einen oder mehrere Benutzer für die Installation von Kaspersky Endpoint Security für Android auf deren mobilen Geräten aus.

Wenn der Benutzer nicht in der Liste enthalten ist, können Sie ein neues Benutzerkonto hinzufügen, ohne den Assistenten zur Verbindung eines neuen mobilen Geräts verlassen zu müssen.

6. Wählen Sie auf der Seite **Ursprung des Zertifikates** des Assistenten die Quelle des Zertifikates für den Schutz des Datenaustausches zwischen Kaspersky Endpoint Security für Android und Kaspersky Security Center aus:

- **Zertifikat mithilfe des Administrationsservers ausstellen.** In diesem Fall wird das Zertifikat automatisch erstellt.
- **Zertifikatsdatei angeben.** In diesem Fall ist es erforderlich, vorläufig ein eigenes Zertifikat vorzubereiten und es im Fenster des Assistenten auszuwählen. Diese Variante kann nicht verwendet werden, wenn Sie Kaspersky Endpoint Security für Android auf mehreren mobilen Geräten installieren wollen. Für jeden Benutzer muss ein separates Zertifikat erstellt werden.

7. Wählen Sie auf der Seite **Benachrichtigungsmethode für Benutzer** des Assistenten den Übertragungskanal für den Link für die Installation der App aus:

- Um den Link per E-Mail zu versenden, wählen Sie **Link zu Kaspersky Endpoint Security versenden** aus und passen Sie die Einstellungen im Block **Per E-Mail** an. Überzeugen Sie sich, dass in den Einstellungen der Benutzerkonten die E-Mail-Adresse angegeben ist.
- Um den Link per SMS-Nachricht zu versenden, wählen Sie **Link an Kaspersky Endpoint Security versenden** aus und passen Sie die Einstellungen im Block **Mit SMS** an. Überzeugen Sie sich, dass in den Einstellungen der Benutzerkonten die Telefonnummer angegeben ist.
- Wählen Sie für die Installation von Kaspersky Endpoint Security für Android mithilfe eines QR-Codes **Link auf das Installationspaket anzeigen** aus und scannen Sie den QR-Code mithilfe der Kamera des mobilen Geräts.
- Wenn Ihnen keine der aufgezählten Methoden zusagt, wählen Sie **Link auf das Installationspaket anzeigen** → **Kopieren** aus, um den Link für die Installation von Kaspersky Endpoint Security für Android in der Zwischenablage zu speichern. Übergeben Sie den Link für die Installation der App auf eine beliebige verfügbare Weise. Sie können auch [andere Installationsmethoden für Kaspersky Endpoint Security für Android](#) verwenden.

8. Klicken Sie auf **Fertig stellen**, um den Assistenten zur Verbindung eines neuen mobilen Geräts zu beenden.

Nach der Installation von Kaspersky Endpoint Security für Android auf den mobilen Geräten der Benutzer können Sie die Einstellungen der Geräte und Apps mithilfe der [Gruppenrichtlinien](#) anpassen. Sie können ferner [Befehle an die mobilen Geräte senden](#), um die Daten im Falle eines Verlustes oder Diebstahls der Geräte zu schützen.

## Andere Methoden zur Installation von Kaspersky Endpoint Security für Android

Sie können Kaspersky Endpoint Security für Android mithilfe eines Links zu Ihrem eigenen Webserver installieren oder die Benutzer anweisen, die App manuell zu installieren.

### Manuelle Installation über Google Play oder Huawei AppGallery

Benutzer können Kaspersky Endpoint Security für Android manuell über Google Play oder Huawei AppGallery installieren. Die Installation wird mit der für die Android-Plattform typischen Methode ausgeführt. Zur Installation der App verwendet der Benutzer seinen persönlichen Google-Account.

Details über den Ablauf der Installation von Kaspersky Endpoint Security für Android aus Google Play finden Sie auf der [Seite des technischen Supports von Google](#).

Details über den Ablauf der Installation von Kaspersky Endpoint Security für Android aus der Huawei AppGallery finden Sie auf der [Support-Website von HUAWEI](#).

Einige Huawei- und Honor-Geräte nutzen keine Google-Dienste und haben deshalb keinen Zugriff auf Apps in Google Play. Wenn Benutzer von Huawei- und Honor-Geräten die App nicht über Google Play installieren können, weisen Sie sie an, die App über die Huawei App Gallery zu installieren.

Nach der Installation von Kaspersky Endpoint Security für Android aus Google Play oder Huawei AppGallery muss die App auf die Ausführung vorbereitet werden. Die Vorbereitung der Anwendung für die Verwendung umfasst folgende Schritte:

1. Der Administrator übermittelt dem Benutzer die Einstellungen für die Synchronisierung des mobilen Geräts mit dem Administrationsserver (Serveradresse und Port) mithilfe einer beliebigen Methode (beispielsweise in einer E-Mail-Nachricht).
2. Der Benutzer passt die Einstellungen für die Synchronisierung des mobilen Geräts mit dem Administrationsserver während der Ausführung des Schnellstartassistenten oder in den Einstellungen von Kaspersky Endpoint Security für Android an.
3. Der Administrator [erstellt ein allgemeines Zertifikat](#) für den Benutzer des mobilen Geräts.
4. Der Benutzer erhält eine automatische Benachrichtigung mit der Aufforderung, das allgemeine Zertifikat zu installieren. Nach seiner Zustimmung wird das allgemeine Zertifikat auf dem mobilen Gerät installiert.

Für die Synchronisierung mit dem Administrationsserver muss auf dem mobilen Gerät der Internetzugang aktiviert sein.

Detaillierte Informationen über die Konfiguration der Einstellungen für die Synchronisierung des mobilen Geräts mit dem Administrationsserver und den Empfang eines allgemeinen Zertifikats finden Sie in der [Hilfe zu Kaspersky Security](#).

Bei der nächsten Synchronisierung des mobilen Geräts mit dem Administrationsserver wird das mobile Gerät des Benutzers, auf dem Kaspersky Endpoint Security für Android installiert ist, in den Ordner **Erweitert** → **Netzwerkabfrage** → **Domänen** der Administrationsgruppe verschoben, die bei der Installation der App festgelegt wurde (standardmäßig ist das die Gruppe **KES10**). Sie können das mobile Gerät entweder manuell oder mithilfe der Regeln für die automatische Verschiebung in die erstellte Administrationsgruppe in den Ordner "Verwaltete Geräte" verschieben.

Diese Installationsart ist praktisch, wenn Sie eine bestimmte Version von Kaspersky Endpoint Security für Android installieren möchten.

*Bei der Installation von Kaspersky Endpoint Security für Android über einen Link auf den eigenen Web-Server muss folgendermaßen vorgegangen werden:*

1. [Erstellen Sie ein Installationspaket und konfigurieren Sie seine Einstellungen](#).

Ein *Installationspaket* ist eine Zusammenstellung von Dateien, die für die ferngesteuerte Installation von Kaspersky-Anwendungen mithilfe von Kaspersky Security Center erstellt wurden.

2. [Eigenständiges Installationspaket erstellen](#).

Ein *eigenständiges Installationspaket* ist eine Installationsdatei für eine mobile Anwendung, in der die Verbindungseinstellungen der Anwendung zum Administrationsserver und ein Hinweis auf die Annahme der Bedingungen des Endbenutzer-Lizenzvertrags (EULA) für Kaspersky Endpoint Security für Android enthalten sind. Dieses Paket wird auf der Grundlage des Installationspakets für Kaspersky Endpoint Security für Android erstellt. Ein eigenständiges Paket ist ein spezieller Fall eines Pakets für mobile Anwendungen.

Der Benutzer erhält einen Link auf den Web-Server, auf dem sich das eigenständige Installationspaket von Kaspersky Endpoint Security für Android befindet. Bei der Installation der App muss der Benutzer die apk-Datei ausführen. Nach der Installation sind keine zusätzlichen Einstellungen von Kaspersky Endpoint Security für Android erforderlich.

Bei der Installation von Kaspersky Endpoint Security für Android mithilfe eines Links auf einen eigenen Webserver muss auf dem mobilen Gerät des Benutzers die Installation von Apps aus unbekannten Quellen erlaubt sein.

## Erstellen und Konfigurieren eines Installationspakets

Das Installationspaket von Kaspersky Endpoint Security für Android ist ein selbstentpackendes Archiv `sc_package.exe`. Das Archiv enthält die Dateien, die für die Installation der mobilen App auf den Geräten erforderlich sind:

- `adb.exe`, `AdbWinApi.dll`, `AdbWinUsbApi.dll` – Auswahl von Dateien, die für eine Installation von Kaspersky Endpoint Security für Android erforderlich ist.
- `installer.ini` – Konfigurationsdatei mit Einstellungen für die Verbindung zum Administrationsserver.
- `KES10_xx_xx_xxx.apk` – Installationsdatei der mobilen Anwendung von Kaspersky Endpoint Security für Android.
- `kmlisten.exe` – Tool zur Bereitstellung des Installationspakets der App über eine Workstation.
- `kmlisten.ini` – Konfigurationsdatei mit Einstellungen für das Tool zur Bereitstellung des Installationspakets.
- `kmlisten.kpd` – Datei mit einer Beschreibung des Apps.

*Um ein Installationspaket für Kaspersky Endpoint Security für Android zu erstellen, gehen Sie wie folgt vor:*

1. Wählen Sie in der Konsolenstruktur den Ordner **Erweitert** → **Remote-Installation** → **Installationspakete** aus.
2. Klicken Sie im Arbeitsplatz des Ordners **Installationspakete** auf die Schaltfläche **Installationspaket erstellen**. Der Assistent für das Erstellen des Installationspakets wird gestartet. Folgen Sie den Anweisungen.
3. Klicken Sie im Fenster **Typ des Installationspakets auswählen** des Assistenten auf **Installationspaket für das Kaspersky-Programm erstellen**.
4. Geben Sie im Fenster des Assistenten **Name des Installationspakets festlegen** den Namen des Installationspakets ein, der im Arbeitsbereich des Ordners **Installationspakete** angezeigt werden soll.
5. Wählen Sie im Fenster **Programmdistribution zur Installation auswählen** des Assistenten das selbstentpackende Archiv `sc_package.exe`, welches Teil des Lieferumfangs ist.  
Wenn das Archiv bereits entpackt wurde, wählen Sie die Datei `kmlisten.kpd` aus, die eine Programmbeschreibung enthält. Im Eingabefeld werden Name und Versionsnummer des Programms angezeigt.
6. Lesen Sie sich im Fenster **Endbenutzer-Lizenzvertrag akzeptieren** des Assistenten die Bedingungen des Endbenutzer-Lizenzvertrags aufmerksam durch und akzeptieren Sie sie.

Sie müssen die Bedingungen des Endbenutzer-Lizenzvertrags akzeptieren, um das Installationspaket erstellen zu können. Wenn Sie die Bedingungen der Lizenzvertrags in der Verwaltungskonsolle akzeptieren, überspringt Kaspersky Endpoint Security für Android während der Installation der App den Schritt mit der Aufforderung zur Annahme der Bedingungen.

Wenn Sie den Schutz der mobilen Geräte beenden möchten, können Sie die App "Kaspersky Endpoint Security für Android" deinstallieren und Ihren Endbenutzer-Lizenzvertrag (EULA) für die App widerrufen. Mehr Informationen zum Widerruf des EULA finden Sie in der *Hilfe zu Kaspersky Security Center*.

Nach dem Abschluss des Assistenten erscheint das Installationspaket im Arbeitsbereich des Ordners **Installationspakete**. Installationspakete werden im Administrationsserver im angegebenen gemeinsamen Ordner im Serviceordner Packages gespeichert.

*Um ein Installationspaket anzupassen, gehen Sie wie folgt vor:*

1. Wählen Sie in der Konsolenstruktur den Ordner **Erweitert** → **Remote-Installation** → **Installationspakete** aus.
2. Wählen Sie im Kontextmenü des Installationspakets für Kaspersky Endpoint Security für Android den Punkt **Eigenschaften** aus.
3. Geben Sie auf der Registerkarte **Einstellungen** die Einstellungen für die Verbindung der mobilen Endgeräte mit dem Administrationsserver und den Namen der Administrationsgruppe an, zu der die mobilen Endgeräte nach der ersten Synchronisierung mit dem Administrationsserver automatisch hinzugefügt werden sollen. Gehen Sie dazu folgendermaßen vor:
  - Geben Sie im Abschnitt **Verbindung zum Administrationsserver** im Feld **Serveradresse** den Namen des Administrationsservers für die Verbindung von mobilen Endgeräten an. Verwenden Sie dazu das Format, in dem der Name bei der Installation der Komponente **Unterstützung von mobilen Endgeräten** bei der Verteilung des Administrationsservers angegeben wurde.

Geben Sie abhängig vom Namensformat des Administrationsservers für die Komponente **Unterstützung von mobilen Endgeräten** entweder den DNS-Namen oder die IP-Adresse des Administrationsservers an. Geben Sie im Feld **Nummer des SSL-Ports** die Nummer des Ports an, der auf dem Administrationsserver für eine Verbindung mit mobilen Geräten reserviert ist. Als Standard wird Port 13292 verwendet.
  - Geben Sie im Abschnitt **Verteilung von Computern auf Gruppen** im Feld **Gruppenname** den Namen der Gruppe ein, zu der mobile Endgeräte nach der ersten Synchronisierung mit dem Administrationsserver hinzugefügt werden sollen (als Standard gilt **KES10**).

Die angegebene Gruppe wird automatisch im Ordner **Erweitert** → **Netzwerkabfrage** → **Domänen** erstellt.
  - Aktivieren Sie im Abschnitt **Aktionen bei Installation** das Kontrollkästchen **E-Mail-Adresse erfragen**, damit die App den Benutzer beim ersten Start nach seiner Unternehmens-E-Mail-Adresse fragt.

Die E-Mail-Adresse des Benutzers wird verwendet, um einen Namen für mobile Endgeräte zu erstellen, wenn diese Geräte einer Administrationsgruppe hinzugefügt werden.
4. Klicken Sie auf Übernehmen, um die angegebenen **Anwenden** zu übernehmen.

## Erstellen eines eigenständigen Installationspakets

*Um ein eigenständiges Installationspaket zu erstellen, gehen Sie wie folgt vor:*

1. Wählen Sie in der Konsolenstruktur den Ordner **Erweitert** → **Remote-Installation** → **Installationspakete** aus.
2. Wählen Sie das Installationspaket für die App Kaspersky Endpoint Security für Android aus.

3. Wählen Sie im Kontextmenü des Installationspakets Liste für Installationspakete den Punkt **Autonomes Installationspaket erstellen** aus.

Dadurch wird der Assistent für das Erstellen von autonomen Installationspaketen gestartet. Folgen Sie den Anweisungen.

4. Konfigurieren Sie die Methoden zur Verteilung des eigenständigen Installationspakets:

- Um den Pfad zu einem erstellten eigenständigen Installationspaket über E-Mail unter den Benutzern zu verteilen, klicken Sie im Block **Weitere Aktionen** auf den Link **zum eigenständigen Installationspaket über E-Mail verteilen**.

Daraufhin öffnet sich das Fenster zum Erstellen einer Nachricht, deren Text einen Pfad zum freigegebenen Ordner mit dem autonomen Installationspaket enthält.

- Um einen Link zu einem erstellten eigenständigen Installationspaket auf der Website Ihres Unternehmens hinzuzufügen, klicken Sie auf den Link **Beispiel für HTML-Code zum Hinzufügen eines Links auf der Website**.

Die Datei tmp-Datei mit dem HTML\_RJL des Links wird geöffnet.

5. Um ein erstelltes eigenständiges Installationspaket auf dem Web-Server von Kaspersky Security Center zu veröffentlichen sowie die gesamte Liste der eigenständigen Pakete für das ausgewählte Installationspaket anzuzeigen, aktivieren Sie im Fenster des Assistenten **Assistent für das Erstellen von eigenständigen Installationspaketen wurde erfolgreich ausgeführt** das Kontrollkästchen **Liste der autonomen Pakete öffnen**.

Nach Abschluss des Assistenten öffnet sich das Fenster **Liste der eigenständigen Pakete für das Installationspaket <Name des Installationspakets>**.

Das Fenster **Liste der eigenständigen Pakete für das Installationspaket <Name des Installationspakets>** enthält folgende Informationen:

- Liste der autonomen Installationspakete.
- Netzwerkpfad zum öffentlichen Ordner im Feld **Pfad**.
- Adresse des autonomen Pakets auf dem Webserver von Kaspersky Security Center im Feld **Webadresse**.

Bei Versand über E-Mail können Sie als Ressource für den Download der Installationsdatei der Anwendung sowohl die Adresse im Feld **Webadresse** als auch die Adresse im Feld **Pfad** angeben. Beim Versand von SMS-Nachrichten an Benutzer müssen Sie den Link für den Download angeben, der im Feld **Webadresse** angegeben ist.

Es wird empfohlen, die Adresse des autonomen Pakets in die Zwischenablage zu kopieren und anschließend als Link für den Download der entsprechenden Installationsdatei in die E-Mail-Nachricht oder die SMS-Nachricht an die Benutzer einzufügen.

## Synchronisierungseinstellungen anpassen

Um mobile Geräte verwalten und Berichte oder Statistiken von mobilen Geräten der Benutzer empfangen zu können, müssen die Synchronisierungseinstellungen konfiguriert werden. Die Synchronisierung eines mobilen Geräts mit Kaspersky Security Center kann auf folgende Arten erfolgen:

- **Nach Zeitplan.** Die Synchronisierung nach Zeitplan wird mit Hilfe des HTTP-Protokolls durchgeführt. Sie können in den Einstellungen der Gruppenrichtlinie einen Zeitplan für die Synchronisierung konfigurieren. Änderungen an den Einstellungen der Gruppenrichtlinie, Befehle und Aufgaben werden während der Synchronisierung des




Geräts mit Kaspersky Security Center nach Zeitplan ausgeführt, also mit einer gewissen Verzögerung. Standardmäßig werden die mobilen Endgeräte alle 6 Stunden automatisch mit Kaspersky Security Center synchronisiert.

Unter Android 12 oder höher führt die App diese Aufgabe möglicherweise später aus, wenn sich das Gerät im Stromsparmodus befindet.

- **Erzwungen.** Die erzwungene Synchronisierung erfolgt mithilfe von Push-Benachrichtigungen [des FCM-Dienstes \(Firebase Cloud Messaging\)](#). Die erzwungene Synchronisierung ist in erster Linie dafür gedacht, eine rechtzeitige [Übermittlung von Befehlen an das mobile Gerät](#) zu gewährleisten. Wenn Sie die erzwungene Synchronisierung verwenden möchten, stellen Sie sicher, dass die GSM-Einstellungen in Kaspersky Security Center konfiguriert sind. Weitere Informationen finden Sie in der [Hilfe zu Kaspersky Security Center](#).

*Um die Einstellungen für die Synchronisierung der mobilen Endgeräte mit Kaspersky Security Center anzupassen, gehen Sie wie folgt vor:*

1. Wählen Sie in der Konsolenstruktur im Ordner **Verwaltete Geräte** die Administrationsgruppe, zu der die Android-Geräte gehören.
2. Gehen Sie Im Arbeitsbereich der Gruppe auf die Registerkarte **Richtlinien**.
3. Öffnen Sie über Doppelklick auf eine beliebige Spalte das Eigenschaftenfenster der Richtlinie.
4. Wählen Sie im Fenster **Eigenschaften <Name der Richtlinie>** den Abschnitt **Synchronisierung**.
5. Wählen Sie die Regelmäßigkeit des Synchronisierungsstarts in der Dropdown-Liste **Synchronisierung starten**.
6. Um die Synchronisierung des Geräts mit Kaspersky Security Center beim Roaming zu verbieten, aktivieren Sie das Kontrollkästchen **Synchronisierung beim Roaming deaktivieren**.  
Der Benutzer des Geräts kann die Synchronisierung manuell in den Einstellungen der App ( → **Einstellungen** → **Synchronisierung** → **Synchronisieren**) ausführen.
7. Um die Synchronisierungseinstellungen (Serveradresse, Port und Administrationsgruppe) vor dem Benutzer zu verbergen, deaktivieren Sie in den Einstellungen der App das Kontrollkästchen **Synchronisierungseinstellungen auf dem Gerät anzeigen**. Verborgene Einstellungen können nicht geändert werden.
8. Klicken Sie auf **Anwenden**, um die vorgenommenen Änderungen zu speichern.

Die Einstellungen werden nach der nächsten planmäßigen Synchronisierung des Geräts mit Kaspersky Security Center auf dem mobilen Gerät konfiguriert. Sie können die Synchronisierung des mobilen Geräts mit einem [speziellen Befehl](#) erzwingen. Weitere Informationen zur Arbeit mit den Befehlen für die Mobilgeräte finden Sie in der [Hilfe zu Kaspersky Security Center](#).

## Aktivierung der App Kaspersky Endpoint Security für Android

Eine Lizenz für Kaspersky Security Center kann sich auf unterschiedliche Funktionalitätsgruppen beziehen. Für die ordnungsgemäße Funktion von Kaspersky Endpoint Security für Android muss die vom Unternehmen erworbene Lizenz für Kaspersky Security Center auch für die Funktionalität **Mobile Geräte verwalten** gelten. Die Funktionalität **Mobile Geräte verwalten** ist für die Verbindung der mobilen Geräte mit Kaspersky Security Center sowie ihre Verwaltungen vorgesehen.

Weitere Informationen über die Lizenzierung von Kaspersky Security Center und die Lizenzierungsvarianten finden Sie in der [Hilfe zu Kaspersky Security Center](#).



Die Aktivierung der App Kaspersky Endpoint Security für Android auf einem mobilen Gerät erfolgt durch die Bereitstellung gültiger Lizenzinformationen für die App. Die Lizenzinformationen werden zusammen mit der Richtlinie bei der Synchronisierung Ihres Geräts mit Kaspersky Security Center an das mobile Gerät übermittelt.

Falls die App Kaspersky Endpoint Security für Android nicht innerhalb von 30 Tagen nach der Installation auf dem mobilen Gerät aktiviert wird, wechselt die Anwendung automatisch in den Eingeschränkten Funktionsmodus. In diesem Modus haben die meisten Komponenten keine Funktion. Beim Wechsel in den eingeschränkten Funktionsmodus stellt die App die automatische Synchronisierung mit Kaspersky Security Center ein. Sollte die App nach der Installation nicht innerhalb von 30 Tagen aktiviert worden sein, so muss das Gerät manuell mit Kaspersky Security Center synchronisiert werden.

Wenn Kaspersky Security Center in Ihrem Unternehmen nicht bereitgestellt wird oder für mobile Geräte nicht zugänglich ist, können Benutzer [die App von Kaspersky Endpoint Security für Android manuell auf ihren Geräten aktivieren](#).

*Um die App Kaspersky Endpoint Security für Android zu aktivieren, gehen Sie wie folgt vor:*

1. Wählen Sie in der Konsolenstruktur im Ordner **Verwaltete Geräte** die Administrationsgruppe, zu der die Android-Geräte gehören.
2. Gehen Sie im Arbeitsbereich der Gruppe auf die Registerkarte **Richtlinien**.
3. Öffnen Sie über Doppelklick auf eine beliebige Spalte das Eigenschaftenfenster der Richtlinie.
4. Wählen Sie im Fenster **Eigenschaften <Name der Richtlinie>** den Abschnitt **Lizenzverwaltung**.
5. Wählen Sie im Block **Lizenzverwaltung** in der Dropdown-Liste **Schlüssel** den Schlüssel für die Aktivierung der App, der im Schlüsselspeicher des Kaspersky Security Center Administrationsservers abgelegt wurde.  
Im Feld darunter werden Informationen über die App, für deren Benutzung die Lizenz erworben wurde, die Gültigkeitsdauer der Lizenz und ihr Typ angezeigt.
6. Aktivieren Sie das Kontrollkästchen **Mit dem Schlüssel aus dem Speicher des Kaspersky Security Center aktivieren**.  
Wenn die App ohne den Schlüssel aus der Schlüsselablage von Kaspersky Security Center aktiviert wurde, ersetzt Kaspersky Security für mobile Endgeräte diesen Schlüssel durch den aus der Dropdown-Liste **Schlüssel** ausgewählten Schlüssel.
7. Um die Anwendung auf dem Mobilgerät des Nutzers zu aktivieren, blockieren Sie die Änderung von Einstellungen.
8. Klicken Sie auf **Anwenden**, um die vorgenommenen Änderungen zu speichern.  
Die Einstellungen werden nach der nächsten planmäßigen Synchronisierung des Geräts mit Kaspersky Security Center auf dem mobilen Gerät konfiguriert.

## iOS MDM-Profil installieren

In diesem Abschnitt werden die Methoden zur Verteilung der iOS MDM-Profile im Netzwerk des Unternehmens beschrieben.

Vor der Verteilung des iOS MDM-Profils muss der Administrator wie folgt vorgehen:

1. Den iOS MDM-Server für Mobilgeräte installieren.

2. Das Zertifikat Apple Push Notification Service (APNs-Zertifikat) abrufen.
3. Das APNs-Zertifikat auf dem iOS MDM-Server für Mobilgeräte installieren.

Weitere Informationen über die Installation des iOS MDM-Servers für Mobilgeräte und die Arbeit mit dem APNs-Zertifikat finden Sie in der [Hilfe zu Kaspersky Security Center](#).

Weitere Informationen über die Verteilung des iOS MDM-Profiles in Kaspersky Endpoint Security Cloud finden Sie in der [Hilfe zu Kaspersky Endpoint Security Cloud](#).

## Über die Verwaltungsmodi für iOS-Geräte

Das Verwaltungssystem für iOS-Geräte kann auf mehrere Arten implementiert werden. Der Verwaltungsmodus ist vom Besitzer des mobilen Geräts (Privat- oder Firmengerät) und von den Anforderungen an die Unternehmenssicherheit abhängig. Sie können den für das Unternehmen geeignetsten Verwaltungsmodus auswählen oder mehrere Verwaltungsmodi gleichzeitig verwenden.

### Nicht kontrollierte Geräte

*Nicht kontrollierte Geräte* sind private Geräte der Mitarbeiter, die mit Kaspersky Security Center verbunden sind. In diesem Modus darf der Benutzer eine persönliche Apple ID verwenden, beliebige Apps nutzen und persönliche Daten auf dem Gerät speichern. Sie können den Zugriff auf Unternehmensressourcen, die Sicherheitseinstellungen sowie andere Einstellungen mithilfe der [Gruppenrichtlinie von Kaspersky Device Management für iOS](#) anpassen. Standardmäßig sind alle iOS-Geräte nicht kontrollierte Geräte.

### Kontrollierte Geräte

*Kontrollierte iOS-Geräte* sind Unternehmensgeräte, die mit Kaspersky Security Center verbunden sind. Die Erstkonfiguration des mobilen Geräts wird im Apple Configurator vorgenommen. *Apple Configurator* ist ein Programm zur Vorbereitung und Konfiguration von iOS-Geräten. Apple Configurator wird auf einem Computer unter OS X installiert. Näheres zur Verwendung von Apple Configurator finden Sie auf [der Website des technischen Supports von Apple](#). Zusätzliche Änderungen der Einstellungen können mithilfe der [Gruppenrichtlinie von Kaspersky Device Management für iOS](#) vorgenommen werden. Auf den kontrollierten Geräten ist eine weitere Auswahl an Einstellungen verfügbar. Globaler HTTP-Proxy, erweiterte Beschränkungen (z. B. Verbot der Nutzung von iMessage, Game Center) oder Verbot der Änderung des Benutzerkontos.

Um mit kontrollierten und nicht kontrollierten iOS-Geräten arbeiten zu können, muss auf dem iOS MDM-Server ein APNs-Zertifikat und auf den mobilen Geräten der Benutzer ein iOS MDM-Profil installiert sein.

## Installation über Kaspersky Security Center

Die Installation des iOS MDM-Profiles wird auf den mobilen Geräten der Benutzer ausgeführt, deren Benutzerkonten zu Kaspersky Security Center hinzugefügt wurden. Weitere Informationen zu Benutzerkonten in Kaspersky Security Center finden Sie in der [Hilfe zu Kaspersky Security Center](#).

*Um das iOS MDM-Profil zu installieren, gehen Sie wie folgt vor:*

1. Wählen Sie in der Konsolenstruktur den Ordner **Mobile Geräte verwalten** → **Mobile Geräte** aus.
2. Klicken Sie im Arbeitsplatz des Ordners **Mobile Geräte** auf die Schaltfläche **Mobiles Gerät hinzufügen**.

Der Assistent zur Verbindung eines neuen mobilen Geräts wird gestartet. Folgen Sie den Anweisungen.

3. Wählen Sie im Fenster **Betriebssystem** des Assistenten **iOS** aus.
4. Wählen Sie im Fenster **Schutzmethode von iOS MDM-Geräten** des Assistenten **iOS MDM-Profil des iOS MDM-Server für Mobilgeräte verwenden** aus und geben Sie ein iOS MDM-Profil aus der Liste an.
5. Wählen Sie im Fenster **Auswahl der Benutzer** des Assistenten einen oder mehrere Benutzer für die Installation des iOS MDM-Profils auf deren mobilen Geräten aus.  
  
Wenn es keinen Benutzer in der Liste gibt, können Sie ein neues Benutzerkonto hinzufügen, ohne den Assistenten zur Verbindung eines neuen mobilen Geräts verlassen zu müssen.
6. Wählen Sie im Fenster **Ursprung des Zertifikates** des Assistenten die Quelle des Zertifikates für den Schutz des Datenaustausches zwischen dem mobilen Gerät und Kaspersky Security Center aus:
  - **Zertifikat mithilfe des Administrationsservers ausstellen.** In diesem Fall wird das Zertifikat automatisch erstellt.
  - **Zertifikatsdatei angeben.** In diesem Fall ist es erforderlich, vorläufig ein eigenes Zertifikat vorzubereiten und es im Fenster des Assistenten auszuwählen. Diese Variante kann nicht verwendet werden, wenn Sie das iOS MDM-Profil auf mehreren mobilen Geräten installieren wollen. Für jeden Benutzer muss ein separates Zertifikat erstellt werden.
7. Wählen Sie im Fenster **Benachrichtigungsmethode für Benutzer** des Assistenten den Übertragungskanal für den Link für die Installation der App aus:
  - Um den Link per E-Mail zu versenden, wählen Sie **Link zum iOS MDM-Profil versenden** aus und passen Sie die Einstellungen im Block **Per E-Mail** an. Überzeugen Sie sich, dass in den Einstellungen der Benutzerkonten die E-Mail-Adresse angegeben ist.
  - Um den Link per SMS-Nachricht zu versenden, wählen Sie **Link zum iOS MDM-Profil versenden** aus und passen Sie die Einstellungen im Block **Mit SMS** an. Überzeugen Sie sich, dass in den Einstellungen der Benutzerkonten die Telefonnummer angegeben ist.
  - Wählen Sie für die Installation des iOS MDM-Profils mithilfe eines QR-Codes **Link auf das Installationspaket anzeigen** aus und scannen Sie den QR-Code mithilfe der Kamera des mobilen Geräts.
  - Wenn Ihnen keine der aufgezählten Methoden zusagt, wählen Sie **Link auf das Installationspaket anzeigen** → **Kopieren** aus, um den Link für die Installation des iOS MDM-Profils in der Zwischenablage zu speichern. Übergeben Sie den Link für die Installation der App auf eine beliebige verfügbare Weise.

8. Beenden Sie den Assistenten zur Verbindung eines neuen mobilen Geräts.

Nach der Installation des iOS MDM-Profils auf den mobilen Geräten der Benutzer können Sie die Einstellungen der Apps mithilfe der [Gruppenrichtlinien](#) anpassen. Sie können ferner [Befehle an die mobilen Geräte senden](#), um die Daten im Falle eines Verlustes oder Diebstahls der Geräte zu schützen.

Auf mobilen Geräten mit iOS 12.1 und höher muss die Installation des iOS MDM-Profils auf dem mobilen Gerät manuell bestätigt werden. Außerdem muss die Erlaubnis zur Remote-Verwaltung des Geräts gewährt werden.

## Installation des Verwaltungs-Plug-ins

Für die Verwaltung von mobilen Geräten auf dem Administrator-Arbeitsplatz müssen die folgenden Verwaltungs-Plug-ins installiert werden:

- Das Verwaltungs-Plug-in für Kaspersky Endpoint Security für Android bietet eine Verwaltungsschnittstelle für mobile Endgeräte und darauf installierte mobile Anwendungen über die Administrationskonsole von Kaspersky Security Center.
- Das Verwaltungs-Plug-in für Kaspersky Device Management für iOS ist eine Schnittstelle, mit deren Hilfe mobile Geräte, die über das Protokoll iOS MDM bzw. Exchange ActiveSync verbunden sind, über die Verwaltungskonsole von Kaspersky Security Center verwaltet werden können.

Sie können Verwaltungs-Plug-ins auf folgende Arten installieren:

- Installieren Sie ein Verwaltungs-Plug-in mithilfe des Schnellstartassistenten von Kaspersky Security Center.  
Das Programm fordert Sie nach der Installation des Administrationsservers bei der ersten Verbindung automatisch auf, den Schnellstartassistenten auszuführen. Sie können den Schnellstartassistenten aber auch jederzeit manuell starten.

Mithilfe des Schnellstartassistenten können Sie die Bedingungen des Endbenutzer-Lizenzvertrags (EULA) für die App Kaspersky Endpoint Security für Android in der Verwaltungskonsole akzeptieren. Wurden die Bedingungen des Lizenzvertrags vom Administrator bereits in der Verwaltungskonsole akzeptiert, überspringt Kaspersky Endpoint Security für Android während der Installation der App den Annahmeschritt. Nähere Informationen zum Schnellstartassistenten für Kaspersky Security Center finden Sie in der [Hilfe zu Kaspersky Security Center](#).

- Installieren Sie das Verwaltungs-Plug-in mithilfe der Liste der verfügbaren Installationspakete in der Verwaltungskonsole von Kaspersky Security Center.  
Die Liste der verfügbaren Pakete des Lieferumfangs wird automatisch aktualisiert, wenn neue Versionen von Kaspersky-Programmen veröffentlicht werden.
- Laden Sie das Installationspaket von einer externen Quelle herunter und installieren Sie das Verwaltungs-Plug-in mithilfe der exe-Datei.  
Das Installationspaket für das Verwaltungs-Plug-in kann beispielsweise von der Kaspersky-Website heruntergeladen werden.

## Verwaltungs-Plug-ins aus der Liste in der Verwaltungskonsole installieren

*So installieren Sie die Verwaltungs-Plug-ins:*

1. Wählen Sie in der Konsolenstruktur **Erweitert** → **Remote-Installation** → **Installationspakete** aus.
2. Wählen Sie im Arbeitsbereich **Weitere Aktionen** → **Aktuelle Versionen von Kaspersky-Programmen anzeigen**.  
Eine Liste der aktuellen Versionen von Kaspersky-Programmen wird angezeigt.
3. Wählen Sie im Abschnitt **Mobile Geräte** das Plug-in **Kaspersky Endpoint Security für Android** oder **Kaspersky Device Management für iOS** aus.
4. Klicken Sie auf die Schaltfläche **Installationspakete herunterladen**.  
Ein Plug-in-Lieferumfang wird in den Computerspeicher heruntergeladen (exe-Datei).
5. Führen Sie die exe-Datei aus und folgen Sie den Anweisungen des Installationsassistenten.

## Verwaltungs-Plug-ins aus dem Paket des Lieferumfangs installieren

*Um das Verwaltungs-Plug-in von Kaspersky Endpoint Security für Android zu installieren,*

Kopieren Sie die Installationsdatei `klcfinst.exe` für das Plug-in aus dem Paket des Lieferumfangs der Komplexlösung und starten Sie die Datei am Administrator-Arbeitsplatz.

Die Installation wird von einem Assistenten durchgeführt und erfordert keine Einstellungen.

*Um das Verwaltungs-Plug-In für Kaspersky Device Management für iOS zu installieren,*

Kopieren Sie die Installationsdatei `klmdminst.exe` für das Plug-in aus dem Paket des Lieferumfangs der Komplexlösung und starten Sie die Datei am Administrator-Arbeitsplatz.

Die Installation wird von einem Assistenten durchgeführt und erfordert keine Einstellungen.

Sie können sich davon überzeugen, dass die Verwaltungs-Plug-ins installiert sind, indem Sie sich die Liste der installierten Verwaltungs-Plug-ins für Programme im Eigenschaftenfenster des Administrationsservers im Abschnitt **Erweitert** → **Informationen über installierte Verwaltungs-Plug-ins für Programme** ansehen.

## Upgrade einer Vorgängerversion des Programms

Das Programmupgrade muss unter Berücksichtigung folgender Anforderungen durchgeführt werden:

- Beachten Sie die Version des Verwaltungs-Plug-ins von Kaspersky Endpoint Security und der mobilen App Kaspersky Endpoint Security für Android.  
Die Build-Nummern der Versionen des Verwaltungs-Plug-ins und der mobilen App können Sie in den Release Notes zu Kaspersky Security für mobile Endgeräte einsehen.
- Vergewissern Sie sich, dass Kaspersky Security Center [den Softwarevoraussetzungen von Kaspersky Security für mobile Endgeräte](#) entspricht.
- Die Verwaltungs-Plug-ins von Kaspersky Endpoint Security 10.0 Service Pack 2 (Build 10.6.0.1801) und Kaspersky Device Management für iOS 10.0 Service Pack 2 (Build 10.6.0.1767) und spätere Versionen können automatisch bis zur aktuellen Version aktualisiert werden. Ein Update des Verwaltungs-Plug-ins von früheren Versionen wird nicht unterstützt.  
Für das Update der Verwaltungs-Plug-ins von früheren Versionen müssen die installierten Verwaltungs-Plug-ins und die mit ihrer Hilfe erstellten Gruppenrichtlinien gelöscht werden. Installieren Sie danach die neuen Versionen der Verwaltungs-Plug-ins. Details zum Löschen der Verwaltungs-Plug-ins finden Sie auf der [Website des technischen Supports von AO Kaspersky](#).<sup>2</sup>
- Verwenden Sie auf allen mobilen Geräten des Unternehmens eine Version von Kaspersky Endpoint Security für Android.

Die Fristen und die Bedingungen für den technischen Supports der Versionen von Kaspersky Security für mobile Endgeräte finden Sie auf der [Website des technischen Supports von AO Kaspersky](#).<sup>2</sup>


*Gehen Sie folgendermaßen vor, um die Version des Builds der Verwaltungs-Plug-ins anzuzeigen:*

1. Wählen Sie in der Konsolenstruktur im Kontextmenü des Administrationsservers den Punkt **Eigenschaften** aus.

## 2. Wählen Sie im Eigenschaftfenster des Administrationsservers **Erweitert** → **Informationen über installierte Verwaltungs-Plug-ins für Programme**.

Im Arbeitsplatz werden Informationen über die installierten Verwaltungs-Plug-ins im Format <Name des Plug-Ins> <Version> <Build> angezeigt.

Sie können die Version und die Nummer des Builds der App Kaspersky Endpoint Security für Android auf folgende Weise anzeigen:

- Wenn Kaspersky Endpoint Security für Android [mithilfe eines eigenständigen Installationspakets installiert wurde](#), können Sie die Version und die Nummer des Builds der App in den Eigenschaften des Pakets einsehen.
- Wenn Kaspersky Endpoint Security für Android [über Google Play installiert wurde](#), können Sie die Nummer des Builds in den Einstellungen der App einsehen ( → **Über die App**).

## Update der vorherigen Version von Kaspersky Endpoint Security für Android

Kaspersky Endpoint Security für Android kann folgendermaßen aktualisiert werden:

- Mithilfe von Google Play. Der Benutzer des mobilen Geräts lädt von Google Play eine neue Version der App herunter und installiert sie auf seinem Gerät.
- Mithilfe von Kaspersky Security Center. Sie aktualisieren die Version der App auf dem Gerät ferngesteuert mithilfe des Remote-Management-Systems für Kaspersky Security Center.

Sie können die für Ihr Unternehmen am geeignetste Update-Methode für die App auswählen. Sie können nur eine einzige Update-Methode verwenden.

### Update mithilfe von Google Play

Das Update mithilfe von Google Play wird mit der für die Android-Plattform typischen Methode ausgeführt. Für das Update der App müssen folgende Bedingungen erfüllt sein:

- Der Benutzer des mobilen Geräts muss ein Google-Konto haben.
- Das Gerät muss dem Google-Konto zugeordnet sein.
- Das Gerät muss mit dem Internet verbunden sein.

Nach dem Download der App aus Google Play, überprüft Kaspersky Endpoint Security für Android die Bedingungen des Endbenutzer-Lizenzvertrags (EULA). Wenn die Bedingungen des EULA aktualisiert werden, sendet die App eine Anfrage an das Kaspersky Security Center. Wurde der EULA vom Administrator bereits in der Verwaltungskonsole akzeptiert, überspringt Kaspersky Endpoint Security für Android während der Installation der App den Annahmeschritt. Sollte der Administrator eine veraltete Version des Verwaltungs-Plug-ins verwenden, fordert Kaspersky Security Center Sie auf, das Verwaltungs-Plug-in zu aktualisieren. Beim Update des Verwaltungs-Plug-ins kann der Administrator die Bedingungen des EULA in der Verwaltungskonsole für Kaspersky Endpoint Security für Android akzeptieren.

Das Update der App über Google Play ist verfügbar, wenn Kaspersky Endpoint Security für Android über Google Play installiert wurde. Wenn die App auf andere Weise installiert wurde, ist ein Update über Google Play nicht möglich.



## Update mithilfe von Kaspersky Security Center

Das Update von Kaspersky Endpoint Security für Android mithilfe von Kaspersky Security Center erfolgt als Ergebnis der Anwendung einer Gruppenrichtlinie. In den Einstellungen der Gruppenrichtlinie können Sie ein eigenständiges Installationspaket für Kaspersky Endpoint Security für Android auswählen, dessen Version den Anforderungen an die Unternehmenssicherheit entspricht.

Das Update über Kaspersky Security Center ist verfügbar, wenn Kaspersky Endpoint Security für Android über Kaspersky Security Center installiert wurde. Wenn die App über Google Play installiert wurde, ist ein Update über Kaspersky Security Center nicht möglich.

Für das Upgrade von Kaspersky Endpoint Security für Android mithilfe eines eigenständigen Installationspakets muss auf dem mobilen Gerät des Benutzers die Installation von Apps aus unbekannten Quellen erlaubt sein. Nähere Informationen über die Installation von Apps ohne Google Play finden Sie in der [Android-Hilfe](#).

*Gehen Sie folgendermaßen vor, um die App auf die neue Version zu aktualisieren:*

1. Wählen Sie in der Konsolenstruktur im Ordner **Verwaltete Geräte** die Administrationsgruppe, zu der die Android-Geräte gehören.
2. Gehen Sie im Arbeitsbereich der Gruppe auf die Registerkarte **Richtlinien**.
3. Öffnen Sie über Doppelklick auf eine beliebige Spalte das Eigenschaftenfenster der Richtlinie.
4. Wählen Sie im folgenden Fenster **Eigenschaften <Name der Richtlinie>** den Abschnitt **Erweitert** aus.
5. Klicken Sie im Block **Update von Kaspersky Endpoint Security für Android** auf die Schaltfläche **Auswählen**.  
Das Fenster **Update von Kaspersky Endpoint Security für Android** wird geöffnet.
6. Wählen Sie aus der Liste der eigenständigen Installationspakete für Kaspersky Endpoint Security das Paket, dessen Version den Anforderungen an die Unternehmenssicherheit entspricht.

Sie können Kaspersky Endpoint Security nur auf die neueste Version der App aktualisieren. Ein Update auf eine ältere Version von Kaspersky Endpoint Security ist nicht möglich.

7. Klicken Sie auf die Schaltfläche **Auswählen**.

Im Block **Update von Kaspersky Endpoint Security für Android** wird die Beschreibung des ausgewählten eigenständigen Installationspakets angezeigt.

8. Klicken Sie auf **Anwenden**, um die vorgenommenen Änderungen zu speichern.

Die Einstellungen werden nach der nächsten planmäßigen Synchronisierung des Geräts mit Kaspersky Security Center auf dem mobilen Gerät konfiguriert. Der Benutzer des mobilen Geräts wird aufgefordert, die neue Version der App zu installieren. Nach Erhalt der Zustimmung wird die neue Version der App auf dem mobilen Gerät installiert.

## Installation einer vorherigen Version von Kaspersky Endpoint Security für Android

Wenn Sie das automatische Update der App umgehen und eine bestimmte Version von Kaspersky Endpoint Security für Android verwenden möchten, deaktivieren Sie das automatische Update der App in den Einstellungen von Google Play. Weitere Informationen finden Sie auf der [Website des technischen Supports von Google](#) <sup>2</sup>.

Das automatische Update von Kaspersky Endpoint Security für Android ist nur bei der Installation der App [über Google Play](#) oder [über Kaspersky Security Center mit dem Link zu Google Play](#) verfügbar. Wenn die App [über Kaspersky Security Center mit einem Link auf einen eigenen Webserver \(mittels autonomem Installationspaket\)](#) installiert wird, ist das automatische Update nicht verfügbar. In diesem Fall müssen Sie [Kaspersky Endpoint Security für Android manuell mithilfe einer Gruppenrichtlinie aktualisieren](#).

Gehen Sie wie folgt vor, um eine ältere Version von Kaspersky Endpoint Security für Android zu installieren:

1. [Löschen Sie Kaspersky Endpoint Security für Android von den mobilen Geräten der Benutzer](#).
2. [Installieren Sie Kaspersky Endpoint Security für Android über Kaspersky Security Center mit dem Link auf einen eigenen Webserver](#). Dazu benötigen Sie das Installationspaket einer bestimmten Version. Sie können das Programmpaket einer älteren Version von Kaspersky Endpoint Security für Android auf der [Website des Technischen Supports von Kaspersky](#) herunterladen.

Weitere Informationen über die Verwendung älterer Versionen von Kaspersky Endpoint Security für Android finden Sie in der *Hilfe zur entsprechenden Version von Kaspersky Security für mobile Endgeräte*.

## Update vorheriger Versionen der Verwaltungs-Plug-Ins

Sie können Verwaltungs-Plug-ins mithilfe der folgenden Verfahren aktualisieren:

- Installieren Sie die neue Version des Verwaltungs-Plug-ins mithilfe der Liste der verfügbaren Programmpakete in der Verwaltungskonsole von Kaspersky Security Center.  
Die Liste der verfügbaren Pakete des Lieferumfangs wird automatisch aktualisiert, wenn neue Versionen von Kaspersky-Programmen veröffentlicht werden.
- Laden Sie das Programmpaket von einer externen Quelle herunter und installieren Sie die neue Version des Verwaltungs-Plug-ins mithilfe der exe-Datei.

Für das Update der Verwaltungs-Plug-ins von Kaspersky Endpoint Security für Android und Kaspersky Device Management für iOS muss die aktuelle Programmversion von der [Seite von Kaspersky Security für mobile Endgeräte](#) <sup>2</sup> heruntergeladen und der [Installationsassistent für jedes der Verwaltungs-Plug-ins](#) gestartet werden. Vorgängerversionen der Plug-ins werden während der Ausführung des Installationsassistenten automatisch deinstalliert.

Die Kaspersky-Experten empfehlen, die App und das Verwaltungs-Plug-in derselben Version zu verwenden. Wenn ein Benutzer die App über Google Play aktualisiert, zeigt das Kaspersky Security Center eine Benachrichtigung mit einer Aufforderung zum Aktualisieren des Verwaltungs-Plug-ins an.

Beim Update der Verwaltungs-Plug-ins bleiben bereits vorhandene Administrationsgruppen im Ordner **Verwaltete Geräte** und Regeln für das automatische Verschieben von Geräten aus dem Ordner **Nicht zugeordnete Geräte** in diese Gruppen erhalten. Bestehende Gruppenrichtlinien für mobile Geräte bleiben ebenfalls erhalten. Neue Richtlinieneinstellungen, die einer neuen Funktion von Kaspersky Security für mobile Endgeräte dienen, werden in vorhandene Richtlinien integriert und erhalten Standardwerte.



Wenn in der neuen Version des Verwaltungs-Plug-ins neue Einstellungen hinzugefügt oder Standardwerte geändert wurden, werden die Änderungen erst übernommen, sobald die Gruppenrichtlinie geöffnet wird. Solange der Administrator die Gruppenrichtlinie nicht öffnet, gelten auf den mobilen Geräten auch nach dem Update der Version des Plug-ins weiterhin die Einstellungen der früheren Version.

## Aus der Liste in der Verwaltungskonsolle aktualisieren

*So aktualisieren Sie die Verwaltungs-Plug-ins:*

1. Wählen Sie in der Konsolenstruktur **Erweitert** → **Remote-Installation** → **Installationspakete** aus.
2. Wählen Sie im Arbeitsbereich **Weitere Aktionen** → **Aktuelle Versionen von Kaspersky-Programmen anzeigen**.

Eine Liste der aktuellen Versionen von Kaspersky-Programmen wird angezeigt.

3. Wählen Sie im Abschnitt **Mobile Geräte** das Plug-in **Kaspersky Endpoint Security für Android** oder **Kaspersky Device Management für iOS** aus.

4. Klicken Sie auf die Schaltfläche **Installationspakete herunterladen**.

Ein Plug-in-Paket des Lieferumfangs wird in den Computerspeicher heruntergeladen (exe-Datei). Starten Sie die exe-Datei. Folgen Sie den Anweisungen des Installationsassistenten.

## Aktualisieren aus dem Paket des Lieferumfangs

*Um das Verwaltungs-Plug-in von Kaspersky Endpoint Security für Android zu aktualisieren,*

Kopieren Sie die Installationsdatei `klcfinst.exe` für das Plug-in aus dem Paket des Lieferumfangs der Komplexlösung und starten Sie die Datei am Administrator-Arbeitsplatz.

Die Installation wird von einem Assistenten begleitet und erfordert keine Einstellungen.

*Um das Verwaltungs-Plug-In für Kaspersky Device Management für iOS zu aktualisieren,*

Kopieren Sie die Installationsdatei `klmdminst.exe` für das Plug-in aus dem Paket des Lieferumfangs der Komplexlösung und starten Sie die Datei am Administrator-Arbeitsplatz.

Die Installation des Plug-ins wird von einem Assistenten begleitet und erfordert keine Einstellungen.

Sie können sich davon überzeugen, dass die Verwaltungs-Plug-ins aktualisiert sind, indem Sie sich die Liste der installierten Verwaltungs-Plug-ins für Programme im Eigenschaftenfenster des Administrationsservers im Abschnitt **Erweitert** → **Informationen über installierte Verwaltungs-Plug-ins für Programme** ansehen.

## Kaspersky Endpoint Security für Android deinstallieren

Kaspersky Endpoint Security für Android kann auf folgende Arten deinstalliert werden:

1. Deinstallieren der Anwendung durch den Benutzer

Der Benutzer deinstalliert Kaspersky Endpoint Security für Android selbstständig über die Benutzeroberfläche der Anwendung. Damit der Benutzer die Anwendung deinstallieren kann, muss in der Gruppenrichtlinie, die für das Gerät angewendet wird, die Deinstallation der Anwendung erlaubt sein.

## 2. Deinstallieren der Anwendung durch den Administrator.

Der Administrator deinstalliert die Anwendung ferngesteuert mithilfe der Administrationskonsole von Kaspersky Security Center. Die Anwendung kann von einem einzelnen Gerät oder von mehreren Geräten gleichzeitig deinstalliert werden.

# Ferngesteuerte Deinstallation der Anwendung

Sie können Kaspersky Endpoint Security für Android auf folgende Arten ferngesteuert von den mobilen Geräten der Benutzer deinstallieren:

- Mithilfe einer Gruppenrichtlinie. Diese Methode eignet sich besonders, wenn Sie die Anwendung von mehreren Geräten gleichzeitig deinstallieren möchten.
- Mithilfe der Konfiguration der lokalen Einstellungen der Anwendung. Diese Methode eignet sich besonders, wenn Sie die Anwendung von einem einzelnen Gerät deinstallieren möchten.

*Um die Anwendung mithilfe der Anwendung einer Gruppenrichtlinie zu deinstallieren, gehen Sie wie folgt vor:*

1. Wählen Sie in der Konsolenstruktur im Ordner **Verwaltete Geräte** die Administrationsgruppe, zu der die Android-Geräte gehören.
2. Gehen Sie im Arbeitsbereich der Gruppe auf die Registerkarte **Richtlinien**.
3. Öffnen Sie über Doppelklick auf eine beliebige Spalte das Eigenschaftensfenster der Richtlinie.
4. Wählen Sie im folgenden Fenster **Eigenschaften <Name der Richtlinie>** den Abschnitt **Erweitert** aus.
5. Aktivieren Sie im Block **Kaspersky Endpoint Security für Android deinstallieren** das Kontrollkästchen **App Kaspersky Endpoint Security für Android vom Gerät deinstallieren**.
6. Klicken Sie auf **Anwenden**, um die vorgenommenen Änderungen zu speichern.

Daraufhin wird die Anwendung Kaspersky Endpoint Security für Android nach der nächsten Synchronisierung mit dem Administrationsserver von den mobilen Geräten entfernt. Die Benutzer der mobilen Geräte erhalten eine Benachrichtigung über die Deinstallation der Anwendung.

*Um die Anwendung mithilfe der Konfiguration der lokalen Einstellungen zu deinstallieren, gehen Sie wie folgt vor:*

1. Wählen Sie in der Konsolenstruktur **Mobile Geräte verwalten** → **Mobile Geräte** aus.
2. Wählen Sie in der Geräteliste das Gerät, von dem Sie die App deinstallieren möchten.
3. Öffnen Sie über Doppelklick das Eigenschaftensfenster des Geräts.
4. Wählen Sie den Abschnitt **Programme** → **Kaspersky Endpoint Security für Android** aus.
5. Öffnen Sie über Doppelklick das Eigenschaftensfenster der Anwendung Kaspersky Endpoint Security.
6. Wählen Sie den Abschnitt **Erweitert**.

7. Aktivieren Sie im Block **App Kaspersky Endpoint Security für Android löschen** das Kontrollkästchen **App Kaspersky Endpoint Security für Android vom Gerät deinstallieren**.

8. Klicken Sie auf **Anwenden**, um die vorgenommenen Änderungen zu speichern.

Daraufhin wird die Anwendung Kaspersky Endpoint Security für Android nach der nächsten Synchronisierung mit dem Administrationsserver von den mobilen Geräten entfernt. Der Benutzer des Geräts erhält eine Benachrichtigung über die Deinstallation der Anwendung.

## Erlaubnis zur Deinstallation der Anwendung die Benutzer

Auf den Geräten unter Verwaltung des Betriebssystems Android 7.0 und höher muss zum Schutz der App vor dem Löschen Kaspersky Endpoint Security für Android als Dienst für erleichterte Bedienung installiert sein. Während der Ausführung des Schnellstartassistenten bietet Kaspersky Endpoint Security für Android an, dem Benutzer der App die erforderlichen Berechtigungen bereitzustellen. Der Benutzer kann diese Schritte überspringen oder die Berechtigungen in den Einstellungen des Geräts später deaktivieren. In diesem Fall ist der Schutz der Anwendung vor dem Löschen nicht aktiviert.

Sie können den Benutzern auf folgende Arten erlauben, Kaspersky Endpoint Security für Android von ihren mobilen Geräten zu deinstallieren:

- Mithilfe einer Gruppenrichtlinie. Diese Methode eignet sich besonders, wenn Sie Benutzern mehrerer Geräten gleichzeitig die Deinstallation der Anwendung erlauben möchten.
- Mithilfe der lokalen Einstellungen der Anwendung. Diese Methode eignet sich besonders, wenn Sie dem Benutzer eines einzelnen Geräts die Deinstallation der Anwendung erlauben möchten.

*Um die Deinstallation der Anwendung in der Gruppenrichtlinie zu erlauben, gehen Sie wie folgt vor:*

1. Wählen Sie in der Konsolenstruktur im Ordner **Verwaltete Geräte** die Administrationsgruppe, zu der die Android-Geräte gehören.
2. Gehen Sie Im Arbeitsbereich der Gruppe auf die Registerkarte **Richtlinien**.
3. Öffnen Sie über Doppelklick auf eine beliebige Spalte das Eigenschaftensfenster der Richtlinie.
4. Wählen Sie im folgenden Fenster **Eigenschaften <Name der Richtlinie>** den Abschnitt **Erweitert** aus.
5. Aktivieren Sie im Block **App Kaspersky Endpoint Security für Android löschen** das Kontrollkästchen **Löschen der App Kaspersky Endpoint Security für Android erlauben**.
6. Klicken Sie auf **Anwenden**, um die vorgenommenen Änderungen zu speichern.

Daraufhin wird nach der nächsten Synchronisierung mit dem Administrationsserver die Deinstallation der Anwendung durch den Benutzer auf dem mobilen Gerät erlaubt. In den Einstellungen von Kaspersky Endpoint Security für Android wird die Schaltfläche zur Deinstallation der Anwendung verfügbar.

*Um die Deinstallation der Anwendung in den lokalen Einstellungen der Anwendung zu erlauben, gehen Sie wie folgt vor:*


1. Wählen Sie in der Konsolenstruktur **Erweitert** → **Mobile Geräte verwalten** → **Mobile Geräte** aus.

2. Wählen Sie in der Geräteliste das Gerät, für das Sie die Deinstallation der Anwendung durch den Benutzer erlauben möchten.
3. Öffnen Sie über Doppelklick das Eigenschaftenfenster des Geräts.
4. Wählen Sie den Abschnitt **Programme** → **Kaspersky Endpoint Security für mobile Endgeräte**.
5. Öffnen Sie über Doppelklick das Eigenschaftenfenster der Anwendung Kaspersky Endpoint Security.
6. Wählen Sie den Block **Erweitert**.
7. Aktivieren Sie im Block **App Kaspersky Endpoint Security für Android löschen** das Kontrollkästchen **Löschen der App Kaspersky Endpoint Security für Android erlauben**.
8. Klicken Sie auf **Anwenden**, um die vorgenommenen Änderungen zu speichern.

Daraufhin wird nach der nächsten Synchronisierung mit dem Administrationsserver die Deinstallation der Anwendung durch den Benutzer auf dem mobilen Gerät erlaubt. In den Einstellungen von Kaspersky Endpoint Security für Android wird die Schaltfläche zur Deinstallation der Anwendung verfügbar.

## Deinstallieren der Anwendung durch den Benutzer

*Um Kaspersky Endpoint Security für Android selbstständig von seinem mobilen Gerät zu deinstallieren, muss der Benutzer folgendermaßen vorgehen:*

1. Im Hauptfenster von Kaspersky Endpoint Security für Android auf  → App **löschen klicken**.  
Auf dem Bildschirm erscheint eine Bestätigungsanfrage.  
Wenn die Schaltfläche **App löschen** fehlt, hat der Administrator den [Schutz von Kaspersky Endpoint Security für Android vor der Deinstallation](#) aktiviert.

2. Entfernen von Kaspersky Endpoint Security für Android bestätigen.

Die App Kaspersky Endpoint Security für Android wird vom mobilen Gerät des Benutzers entfernt.

## Konfiguration und Verwaltung

Dieser Abschnitt der Hilfe richtet sich an Experten, die für die Administration von Kaspersky Security für mobile Endgeräte zuständig sind, sowie an Experten, die für die technische Unterstützung von Unternehmen verantwortlich sind, die Kaspersky Security für mobile Endgeräte einsetzen.

## Erste Schritte

In diesem Abschnitt werden die Aktionen beschrieben, die während der ersten Schritte mit Kaspersky Security für mobile Endgeräte ausgeführt werden sollten.

## Programm starten und anhalten

Kaspersky Security Center startet und installiert die Verwaltungs-Plug-ins für Kaspersky Endpoint Security und Kaspersky Device Management für iOS automatisch.

Kaspersky Endpoint Security für Android wird beim Start des Betriebssystems gestartet und schützt während seiner Sitzung das mobile Gerät des Benutzers. Der Benutzer kann die App beenden, indem er die Verbindung aller Komponenten von Kaspersky Endpoint Security für Android trennt. Sie können den Zugriff des Benutzers auf die Verwaltung der Komponenten der App mithilfe von [Gruppenrichtlinien](#) anpassen.

Auf einigen Geräten (z. B. Huawei, Meizu, Xiaomi) muss Kaspersky Endpoint Security für Android manuell zur Liste der Apps hinzugefügt werden, die beim Start des Betriebssystems gestartet werden (**Sicherheit** → **Berechtigungen** → **Autostart**). Wenn die App nicht zur Liste hinzugefügt wird, stellt Kaspersky Endpoint Security für Android nach dem Neustart des mobilen Geräts sämtliche Funktionen ein.

Außerdem muss der Stromsparmodus für Kaspersky Endpoint Security für Android deaktiviert werden. Dies wird benötigt, damit die App im Hintergrund arbeiten kann, um z. B. die Untersuchung auf Viren nach Zeitplan zu starten oder das Gerät mit Kaspersky Security Center zu synchronisieren. Das Problem ist verbunden mit den Besonderheiten der integrierten Software dieser Geräte.

## Administrationsgruppe erstellen

Zur zentralen Konfiguration der App Kaspersky Endpoint Security für Android, die auf den mobilen Geräten der Benutzer installiert ist, müssen [Gruppenrichtlinien](#) auf diese Geräte angewendet werden.

Um eine Richtlinie auf eine Gerätegruppe anzuwenden, sollte vor der Installation von mobilen Anwendungen auf den Geräten der Benutzer für die entsprechenden Geräte im Ordner **Verwaltete Geräte** eine separate Administrationsgruppe erstellt werden.

Nach dem Erstellen der Administrationsgruppe ist es empfehlenswert, die [automatische Verschiebung von Geräten in diese Gruppe anzupassen](#), auf denen Sie die Apps installieren wollen. Danach müssen mithilfe der Gruppenrichtlinie gemeinsame Einstellungen für alle Geräte festgelegt werden.

*Um eine Administrationsgruppe zu erstellen, gehen Sie wie folgt vor:*

1. Wählen Sie in der Konsolenstruktur den Ordner **Verwaltete Geräte**.
2. Wählen Sie im Arbeitsbereich des Ordners **Verwaltete Geräte** oder eines Unterordners die Registerkarte **Geräte**.
3. Klicken Sie auf **Gruppe erstellen**.

Das Fenster zum Erstellen einer der neuen Gruppe wird geöffnet.

4. Geben Sie im folgenden Fenster **Gruppenname** einen Namen für die Gruppe an und klicken Sie auf **OK**.

In der Konsolenstruktur erscheint ein neuer Ordner für die Administrationsgruppe mit dem festgelegten Namen. Weitere Informationen über Administrationsgruppen finden Sie in der [Hilfe zu Kaspersky Security Center](#).

## Gruppenrichtlinien für die Verwaltung von mobilen Geräten

Eine *Gruppenrichtlinie* ist eine eindeutige Auswahl von Einstellungen zur Verwaltung von mobilen Geräten, die zur Administrationsgruppe gehören und von mobilen Apps auf den Geräten installiert werden. Sie können eine Gruppenrichtlinie mithilfe des Assistenten für das Erstellen einer Richtlinie erstellen.






Mithilfe der Richtlinie können Sie Einstellungen sowohl für einzelne Geräte als auch Gruppen konfigurieren. Verwaltungseinstellungen für eine Gerätegruppe können im Eigenschaftfenster der Gruppenrichtlinie. Und für ein Gerät im Fenster der lokalen Programmeinstellungen angepasst werden. Verwaltungseinstellungen, die für ein Gerät individuell festgelegt wurden, können sich von den Einstellungswerten unterscheiden, die in der Richtlinie für eine Gruppe, zu der dieses Gerät gehört, festgelegt wurden.

Jede Einstellung in einer Richtlinie besitzt das Attribut "Schloss", mit dem gekennzeichnet wird, ob der Parameter in den Richtlinien einer untergeordneten Hierarchieebene (für Untergruppen und untergeordnete Administrationsserver) und in den lokalen Programmeinstellungen verändert werden darf.

Einstellungswerte, die in der Richtlinie und in den lokalen Programmeinstellungen festgelegt wurden, werden auf dem Administrationsserver gespeichert, während der Synchronisierung auf mobile Geräte verteilt und auf den Geräten als gültige Anwendungseinstellungen gespeichert. Wenn der Benutzer auf seinem Gerät andere Einstellungswerte festlegt, die nicht mit einem "Schloss" fixiert wurden, werden bei der nächsten Synchronisierung des Geräts mit dem Administrationsserver die neuen Einstellungswerte an den Administrationsserver übertragen und anstelle der Werte, die früher vom Administrator eingestellt worden sind, in den lokalen Programmeinstellungen gespeichert.

Um den aktuellen Status der korporativen Sicherheit der mobilen Geräte zu gewährleisten, können Sie die [Geräte der Benutzer auf Einhaltung der Gruppenrichtlinie zur Verwaltung kontrollieren](#).

Im oberen Bereich des Fensters der Gruppenrichtlinie wird der Indikator für die Sicherheitsstufe angezeigt. Der Indikator der Sicherheitsstufe hilft Ihnen dabei, die Richtlinie so anzupassen, dass eine hohe Sicherheitsstufe für die Geräte gewährleistet wird. Der Indikator für die Sicherheitsstufe ändert den Status abhängig von den Einstellungen der Richtlinie:

-  **Hohe Sicherheitsstufe** – der Schutz der Geräte auf dem entsprechenden Niveau ist gewährleistet. Alle Schutzkomponenten sind aktiviert und arbeiten mit den von Kaspersky empfohlenen Einstellungen.
-  **Mittlere Sicherheitsstufe** – die Sicherheitsstufe ist herabgesetzt. Einige wichtige Schutzkomponenten (beispielsweise der Web-Filter) sind deaktiviert. Wichtige Probleme sind durch das Zeichen  gekennzeichnet.
-  **Niedrige Sicherheitsstufe** – es liegen Probleme vor, die zur Infektion des Geräts und zu Datenverlust führen können. Einige kritische Schutzkomponenten sind deaktiviert (beispielsweise ist der Echtzeitschutz für Geräte deaktiviert). Kritische Probleme sind durch das Zeichen  gekennzeichnet.

Weitere Informationen zur Verwaltung von Richtlinien und Administrationsgruppen in der Verwaltungskonsolle für Kaspersky Security Center finden Sie in der [Hilfe zu Kaspersky Security Center](#).

## Gruppenrichtlinie erstellen

In diesem Abschnitt wird die Erstellung von Gruppenrichtlinien für Geräte, auf denen die App Kaspersky Endpoint Security für Android verwendet wird, sowie der Richtlinie für EAS-Geräte und iOS MDM-Geräte beschrieben.

Richtlinien, die für die Administrationsgruppe angelegt wurden, werden im Arbeitsplatz der Gruppe in der Verwaltungskonsolle für Kaspersky Security Center auf der Registerkarte **Richtlinien** angezeigt. Neben dem Namen einer Richtlinie wird ein Symbol für den Status der Richtlinie angezeigt (aktiv bzw. nicht aktiv). In einer Gruppe können mehrere Richtlinien für verschiedene Programme erstellt werden. Für jedes Programm kann nur eine Richtlinie aktiv sein. Nach dem Erstellen einer neuen aktiven Richtlinie wird die zuvor aktive Richtlinie inaktiv.

Sie können die Richtlinie nach dem Erstellen ändern.

Um eine Gruppenrichtlinie zur Verwaltung von mobilen Geräten zu erstellen, gehen Sie folgendermaßen vor:

1. Wählen Sie in der Konsolenstruktur eine Administrationsgruppe, für die eine Richtlinie erstellt werden soll.
2. Gehen Sie Im Arbeitsbereich der Gruppe auf die Registerkarte **Richtlinien**.
3. Starten Sie den Assistenten für eine neue Richtlinie über den Link **Richtlinie erstellen**.

Dadurch wird der Assistent für das Erstellen einer Richtlinie gestartet.

## Schritt 1. Programm für das Erstellen einer Gruppenrichtlinie auswählen

Wählen Sie in diesem Schritt das Programm zur Erstellung der Gruppenrichtlinie aus der Liste aus:

- **Kaspersky Endpoint Security für Android** – für Geräte, auf denen die mobile App Kaspersky Endpoint Security für Android verwendet wird.

Es wird empfohlen, eine separate Richtlinie für Huawei- und Honor-Geräte zu erstellen, die keinen Zugriff auf Google-Play-Dienste haben. Auf diese Weise können Sie an die Benutzer solcher Geräte Links zur Huawei AppGallery senden.

- **Kaspersky Device Management für iOS** – für EAS-Geräte und iOS MDM-Geräte.

Eine Richtlinie für mobile Geräte kann erstellt werden, wenn auf dem Administrator-Arbeitsplatz das Verwaltungs-Plug-in von Kaspersky Endpoint Security für Android und das Verwaltungs-Plug-in von Kaspersky Device Management für iOS installiert sind. Wenn die Plug-ins nicht installiert sind, steht der Programmname des entsprechenden Programms nicht auf der Programmliste.

Gehen Sie zum nächsten Schritt des Richtlinien-Assistenten.

## Schritt 2. Name einer Gruppenrichtlinie eingeben

Geben Sie bei diesem Schritt im Feld **Name** einen Namen für die neue Richtlinie an. Wenn Sie den Namen einer bereits vorhandenen Richtlinie verwenden, erhält er automatisch den Zusatz (1).

Gehen Sie zum nächsten Schritt des Richtlinien-Assistenten.

## Schritt 3. Gruppenrichtlinie für das Programm erstellen

Bei diesem Schritt schlägt der Assistent vor, einen Status für die Richtlinie festzulegen:

- **Aktive Richtlinie.** Der Assistent speichert die erstellte Richtlinie auf dem Administrationsserver. Bei der nächsten Synchronisierung des mobilen Geräts mit dem Administrationsserver wird die Richtlinie auf dem Gerät als aktive Richtlinie verwendet.
- **Inaktive Richtlinie.** Der Assistent speichert die erstellte Richtlinie als Reserve-Richtlinie auf dem Administrationsserver. Die Richtlinie kann später bei einem bestimmten Ereignis aktiviert werden. Bei Bedarf kann eine inaktive Richtlinie aktiviert werden.



In einer Gruppe können mehrere Richtlinien für ein Programm erstellt werden. Es gibt aber immer nur eine aktive Richtlinie. Nach dem Erstellen einer neuen aktiven Richtlinie wird die zuvor aktive Richtlinie automatisch inaktiv.

Beenden Sie den Assistenten.

## Synchronisierungseinstellungen anpassen


Um mobile Geräte verwalten und Berichte oder Statistiken von mobilen Geräten der Benutzer empfangen zu können, müssen die Synchronisierungseinstellungen konfiguriert werden. Die Synchronisierung eines mobilen Geräts mit Kaspersky Security Center kann auf folgende Arten erfolgen:

- **Nach Zeitplan.** Die Synchronisierung nach Zeitplan wird mit Hilfe des HTTP-Protokolls durchgeführt. Sie können in den Einstellungen der Gruppenrichtlinie einen Zeitplan für die Synchronisierung konfigurieren. Änderungen an den Einstellungen der Gruppenrichtlinie, Befehle und Aufgaben werden während der Synchronisierung des Geräts mit Kaspersky Security Center nach Zeitplan ausgeführt, also mit einer gewissen Verzögerung. Standardmäßig werden die mobilen Endgeräte alle 6 Stunden automatisch mit Kaspersky Security Center synchronisiert.

Unter Android 12 oder höher führt die App diese Aufgabe möglicherweise später aus, wenn sich das Gerät im Stromsparmodus befindet.

- **Erzwungen.** Die erzwungene Synchronisierung erfolgt mithilfe von Push-Benachrichtigungen [des FCM-Dienstes \(Firebase Cloud Messaging\)](#). Die erzwungene Synchronisierung ist in erster Linie dafür gedacht, eine rechtzeitige [Übermittlung von Befehlen an das mobile Gerät](#) zu gewährleisten. Wenn Sie die erzwungene Synchronisierung verwenden möchten, stellen Sie sicher, dass die GSM-Einstellungen in Kaspersky Security Center konfiguriert sind. Weitere Informationen finden Sie in der [Hilfe zu Kaspersky Security Center](#).

*Um die Einstellungen für die Synchronisierung der mobilen Endgeräte mit Kaspersky Security Center anzupassen, gehen Sie wie folgt vor:*

1. Wählen Sie in der Konsolenstruktur im Ordner **Verwaltete Geräte** die Administrationsgruppe, zu der die Android-Geräte gehören.
2. Gehen Sie im Arbeitsbereich der Gruppe auf die Registerkarte **Richtlinien**.
3. Öffnen Sie über Doppelklick auf eine beliebige Spalte das Eigenschaftenfenster der Richtlinie.
4. Wählen Sie im Fenster **Eigenschaften <Name der Richtlinie>** den Abschnitt **Synchronisierung**.
5. Wählen Sie die Regelmäßigkeit des Synchronisierungsstarts in der Dropdown-Liste **Synchronisierung starten**.
6. Um die Synchronisierung des Geräts mit Kaspersky Security Center beim Roaming zu verbieten, aktivieren Sie das Kontrollkästchen **Synchronisierung beim Roaming deaktivieren**.  
Der Benutzer des Geräts kann die Synchronisierung manuell in den Einstellungen der App ( → **Einstellungen** → **Synchronisierung** → **Synchronisieren**) ausführen.
7. Um die Synchronisierungseinstellungen (Serveradresse, Port und Administrationsgruppe) vor dem Benutzer zu verbergen, deaktivieren Sie in den Einstellungen der App das Kontrollkästchen **Synchronisierungseinstellungen auf dem Gerät anzeigen**. Verborgene Einstellungen können nicht geändert werden.
8. Klicken Sie auf **Anwenden**, um die vorgenommenen Änderungen zu speichern.



Die Einstellungen werden nach der nächsten planmäßigen Synchronisierung des Geräts mit Kaspersky Security Center auf dem mobilen Gerät konfiguriert. Sie können die Synchronisierung des mobilen Geräts mit einem [speziellen Befehl](#) erzwingen. Weitere Informationen zur Arbeit mit den Befehlen für die Mobilgeräte finden Sie in der [Hilfe zu Kaspersky Security Center](#).

## Verwendung der Revisionen von Gruppenrichtlinien

Kaspersky Security Center ermöglicht die Nachverfolgung von Änderungen an den Gruppenrichtlinien. Bei jedem Speichern der Änderungen einer Gruppenrichtlinie wird eine *Revision* erstellt. Jede Revision trägt eine Nummer.

Die Verwendung von Revisionen ist nur für die Richtlinien von Kaspersky Endpoint Security für Android verfügbar. Für die Richtlinie von Kaspersky Device Management für iOS sind keine Revisionen verfügbar.

Sie können folgende Aktionen mit den Revisionen der Gruppenrichtlinien ausführen:

- Eine ausgewählte Revision mit der aktuellen Revision vergleichen
- Ausgewählte Revisionen miteinander vergleichen
- Eine Richtlinie mit der ausgewählten Revision einer anderen Richtlinie vergleichen
- Die ausgewählte Revision anzeigen
- Ein Rollback der Änderungen an einer Richtlinie zur ausgewählten Revision vornehmen
- Revisionen in einer txt-Datei speichern

Weitere Informationen über die Verwendung der Revisionen von Gruppenrichtlinien und anderen Objekten (z. B. Benutzerkonten) finden Sie in der [Hilfe zu Kaspersky Security Center](#).

*Um den Verlauf der Revisionen einer Gruppenrichtlinie anzuzeigen, gehen Sie wie folgt vor:*

1. Wählen Sie in der Konsolenstruktur im Ordner **Verwaltete Geräte** die Administrationsgruppe, zu der die Android-Geräte gehören.
2. Gehen Sie Im Arbeitsbereich der Gruppe auf die Registerkarte **Richtlinien**.
3. Öffnen Sie über Doppelklick auf eine beliebige Spalte das Eigenschaftenfenster der Richtlinie.
4. Wählen Sie im Fenster **Eigenschaften** der Richtlinie den Abschnitt **Revisionsverlauf**.

Eine Liste mit den Revisionen der Richtlinie wird angezeigt. Sie enthält folgende Informationen:

- Nummer der Revision der Richtlinie.
- Datum und Uhrzeit Richtlinienänderung.
- Name des Benutzers, der die Richtlinie geändert hat.
- Ausgeführte Aktion mit der Richtlinie.
- Beschreibung der Revision der Änderung an den Richtlinieneinstellungen.

## Gruppenrichtlinie löschen

Um eine Gruppenrichtlinie zu löschen, gehen Sie wie folgt vor:

1. Wählen Sie in der Konsolenstruktur die Administrationsgruppe aus, für die die Richtlinie gelöscht werden soll.
2. Wählen Sie im Arbeitsbereich der Administrationsgruppe auf der Registerkarte **Richtlinien** die Richtlinie aus, die Sie löschen möchten.
3. Klicken Sie mit der rechten Maustaste auf die Richtlinie und wählen **Löschen** aus.

Daraufhin wird die Gruppenrichtlinie gelöscht. Bis zur Anwendung einer neuen Gruppenrichtlinie arbeiten die mobilen Geräte, die zur Administrationsgruppe gehören, mit den Einstellungen der gelöschten Richtlinie weiter.

## Rechte zur Konfiguration von Gruppenrichtlinien einschränken

Die Administratoren für Kaspersky Security Center können die Zugriffsrechte der Benutzer der Verwaltungskonsole auf verschiedene Funktionen der Komplettlösung Kaspersky Security für mobile Endgeräte abhängig von den dienstlichen Verpflichtungen der Benutzer konfigurieren.

In der Benutzeroberfläche der Verwaltungskonsole erfolgt die Konfiguration der Zugriffsrechte im Eigenschaftfenster des Administrationsservers auf den Registerkarten **Sicherheit** und **Benutzerrollen**. Auf der Registerkarte **Benutzerrollen** können typische Benutzerrollen mit einer festgelegten Konfiguration von Rechten hinzugefügt werden. Im Abschnitt **Sicherheit** können Sie die Rechte eines einzelnen Benutzers oder einer Benutzergruppe anpassen sowie einem Benutzer oder einer Benutzergruppe eine Rolle zuweisen. Die Benutzerrechte werden für jedes Programm nach *Funktionsbereichen* konfiguriert.

Sie können die Benutzerrechte ferner nach Funktionsbereichen konfigurieren. Informationen über die Entsprechung der Funktionsbereiche mit den Registerkarten der Richtlinien finden Sie im [Anhang](#).

Für jeden Funktionsbereich kann der Administrator folgende Zugriffsrechte zuweisen:

- **Ändern von Einstellungen erlauben.** Der Benutzer der Verwaltungskonsole darf die Richtlinieneinstellungen im Eigenschaftfenster der Richtlinie ändern.
- **Ändern von Einstellungen verbieten.** Dem Benutzer der Administrationskonsole ist es verboten, die Richtlinieneinstellungen im Eigenschaftfenster der Richtlinie zu ändern. Die den Funktionsbereichen entsprechenden Registerkarten der Richtlinie, für die diese Berechtigung zugewiesen wurde, werden nicht in der Schnittstelle angezeigt.

Weitere Informationen über die Rechte und Benutzerrollen in der Verwaltungskonsole von Kaspersky Security Center finden Sie in der [Hilfe zu Kaspersky Security Center](#).

## Schutz

Dieser Abschnitt enthält Informationen darüber, wie der Schutz der mobilen Geräte in der Administrationskonsole von Kaspersky Security Center ferngesteuert verwaltet wird.

## Antiviren-Schutz für Android-Geräte anpassen

Für das rechtzeitige Entdecken von Bedrohungen, Viren sowie anderer schädlicher Apps ist es erforderlich, die Einstellungen des Echtzeitschutzes und des automatischen Starts der Untersuchung auf Viren anzupassen.

Kaspersky Endpoint Security für Android entdeckt folgende Objekttypen:

- Viren, Würmer, Trojaner und schädliche Programme.
- Adware.
- Apps, die von Angreifern verwendet werden können, um ein Gerät oder Benutzerdaten zu beschädigen.

Anti-Virus hat eine Reihe von Beschränkungen:

- Bei der Ausführung von Anti-Virus im Arbeitsprofil ist es nicht möglich, eine Bedrohung, die im externen Gerätespeicher gefunden wurde (beispielsweise auf der SD-Karte) automatisch zu entfernen ([Apps mit einer "Aktentasche"](#), [Einstellungen des Arbeitsprofils Android anpassen](#)). Bei Kaspersky Endpoint Security für Android gibt es im Arbeitsprofil keinen Zugriff auf den externen Speicher. Die Informationen über die gefundenen Bedrohungen werden im [Abschnitt Status](#) der App angezeigt. Zur Beseitigung der im externen Speicher gefundenen Objekte muss die Datei manuell gelöscht und die Untersuchung des Geräts erneut gestartet werden.
- Aufgrund von technischen Beschränkungen kann Kaspersky Endpoint Security für Android Dateien mit einer Größe von mehr als 2 GB nicht untersuchen. Während der Untersuchung überspringt die App solche Dateien, und Sie werden nicht benachrichtigt, wenn solche Dateien übersprungen werden.

*Gehen Sie folgendermaßen vor, um die Einstellungen des Echtzeitschutzes für das mobile Gerät anzupassen:*

1. Wählen Sie in der Konsolenstruktur im Ordner **Verwaltete Geräte** die Administrationsgruppe, zu der die Android-Geräte gehören.
2. Gehen Sie Im Arbeitsbereich der Gruppe auf die Registerkarte **Richtlinien**.
3. Öffnen Sie über Doppelklick auf eine beliebige Spalte das Eigenschaftenfenster der Richtlinie.
4. Wählen Sie im folgenden Fenster **Eigenschaften <Name der Richtlinie>** den Abschnitt **Schutz** aus.
5. Passen Sie im Block **Schutz** die Schutzeinstellungen des Dateisystems des mobilen Endgeräts an:
  - Um den Echtzeitschutz des Mobilgeräts vor Bedrohungen zu aktivieren, aktivieren Sie das Kontrollkästchen **Schutz aktivieren**.  
Kaspersky Endpoint Security für Android untersucht dann nur neue Apps und Dateien aus dem Download-Ordner.
  - Um den erweiterten Schutz des Mobilgeräts vor Bedrohungen zu aktivieren, aktivieren Sie das Kontrollkästchen **Erweiterter Schutzmodus**.  
Kaspersky Endpoint Security für Android untersucht dann alle Dateien, die vom Benutzer auf dem Gerät geöffnet, verändert, verschoben, kopiert, installiert und gespeichert werden. Außerdem werden mobile Apps sofort nach ihrer Installation untersucht.

Auf Geräten mit dem Betriebssystem Android 8.0 und höher untersucht Kaspersky Endpoint Security für Android Dateien, die der Benutzer ändert, verschiebt, installiert und speichert, sowie die Kopien von Dateien. Kaspersky Endpoint Security für Android untersucht Dateien nicht bei ihrem Öffnen und untersucht keine Quelldateien beim Kopieren.

- Um die erweiterte Untersuchung neuer Apps vor deren ersten Start auf dem Benutzergerät mithilfe des Cloud-Dienstes von Kaspersky Security Network zu aktivieren, aktivieren Sie das Kontrollkästchen **Cloud-Sicherheit (KSN)**.
- Um Adware und Apps zu blockieren, die von Angreifern verwendet werden können, um das Gerät oder Benutzerdaten zu schädigen, aktivieren Sie das Kontrollkästchen **Adware, Autodialer und andere Apps erkennen, mit denen Angreifer das Gerät und die Daten des Benutzers beschädigen können**.

6. Wählen Sie aus der Liste **Aktion beim Fund einer Bedrohung** eine der folgenden Varianten aus:

- **Löschen**

Die gefundenen Objekte werden automatisch gelöscht. Der Benutzer muss keine weiteren Aktionen vornehmen. Vor dem Löschen zeigt Kaspersky Endpoint Security für Android eine kurze Benachrichtigung über den Fund des Objekts an.

- **Überspringen**

Wenn gefundene Objekte übersprungen wurden, warnt Kaspersky Endpoint Security für Android den Benutzer vor Problemen beim Schutz des Geräts. Die Informationen über die übersprungenen Objekte werden im Abschnitt **Status** der App angezeigt. Für jede übersprungene Bedrohung werden die Aktionen angeführt, die der Benutzer ausführen kann, um die Bedrohung zu beseitigen. Die Liste der übersprungenen Objekte kann sich ändern, beispielsweise wenn die schädliche Datei gelöscht oder verschoben wurde. Um die aktuelle Liste der Bedrohungen zu erhalten, [starten Sie die vollständige Untersuchung des Geräts](#). Für einen zuverlässigen Schutz Ihrer Daten entfernen Sie alle gefundenen Objekte.

- **Quarantäne**

7. Klicken Sie auf **Anwenden**, um die vorgenommenen Änderungen zu speichern.

Die Einstellungen werden nach der nächsten planmäßigen Synchronisierung des Geräts mit Kaspersky Security Center auf dem mobilen Gerät konfiguriert.

*Gehen Sie folgendermaßen vor, um Untersuchung auf Viren auf dem mobilen Gerät des Benutzers automatisch zu starten:*

1. Wählen Sie in der Konsolenstruktur im Ordner **Verwaltete Geräte** die Administrationsgruppe, zu der die Android-Geräte gehören.
2. Gehen Sie im Arbeitsbereich der Gruppe auf die Registerkarte **Richtlinien**.
3. Öffnen Sie über Doppelklick auf eine beliebige Spalte das Eigenschaftenfenster der Richtlinie.
4. Wählen Sie im Fenster **Eigenschaften <Name der Richtlinie>** den Abschnitt **Untersuchung**.
5. Um Adware und Apps zu blockieren, die von Angreifern verwendet werden können, um das Gerät oder Benutzerdaten zu schädigen, aktivieren Sie das Kontrollkästchen **Adware, Autodialer und andere Apps erkennen, mit denen Angreifer das Gerät und die Daten des Benutzers beschädigen können**.

6. Wählen Sie aus der Liste **Aktion beim Fund einer Bedrohung** eine der folgenden Varianten aus:

- **Löschen**

Die gefundenen Objekte werden automatisch gelöscht. Der Benutzer muss keine weiteren Aktionen vornehmen. Vor dem Löschen zeigt Kaspersky Endpoint Security für Android eine kurze Benachrichtigung über den Fund des Objekts an.

- **Überspringen**

Wenn gefundene Objekte übersprungen wurden, warnt Kaspersky Endpoint Security für Android den Benutzer vor Problemen beim Schutz des Geräts. Die Informationen über die übersprungenen Objekte werden im Abschnitt **Status** der App angezeigt. Für jede übersprungene Bedrohung werden die Aktionen angeführt, die der Benutzer ausführen kann, um die Bedrohung zu beseitigen. Die Liste der übersprungenen Objekte kann sich ändern, beispielsweise wenn die schädliche Datei gelöscht oder verschoben wurde. Um die aktuelle Liste der Bedrohungen zu erhalten, [starten Sie die vollständige Untersuchung des Geräts](#). Für einen zuverlässigen Schutz Ihrer Daten entfernen Sie alle gefundenen Objekte.

- **Quarantäne**

- **Aktion erfragen**

Kaspersky Endpoint Security für Android gibt eine Benachrichtigung aus, in welcher der Benutzer aufgefordert wird, eine Aktion für das gefundene Objekt auszuwählen: **Überspringen** oder **Löschen**.

Die Option **Aktion erfragen** erlaubt dem Benutzer des Geräts, beim Fund mehrerer Objekte die ausgewählte Aktion mithilfe des Kontrollkästchens **Auf alle Bedrohungen anwenden** für jede Datei auszuführen.

Zur Anzeige der Benachrichtigung auf mobilen Geräten mit Android 10.0 und höher muss Kaspersky Endpoint Security für Android als Bedienungshilfe installiert sein. Der Assistent für die Erstkonfiguration von Kaspersky Endpoint Security für Android ermöglicht dem Benutzer, die App als Bedienungshilfe zu installieren. Der Benutzer kann diesen Schritt überspringen oder den Dienst in den Einstellungen des Geräts später deaktivieren. In diesem Fall zeigt Kaspersky Endpoint Security für Android ein Android-Systemfenster an, in welchem der Benutzer aufgefordert wird, für das gefundene Objekt die Aktion Überspringen oder Löschen auszuwählen. Um die Aktion auf mehrere Objekte anzuwenden, öffnen Sie Kaspersky Endpoint Security.

7. Passen Sie im Block **Untersuchung nach Zeitplan** die Einstellungen für den automatischen Start der vollständigen Untersuchung des Gerätedateisystems an. Klicken Sie dazu auf die Schaltfläche **Zeitplan** und legen Sie im folgenden Fenster **Zeitplan** eine Frequenz und den Startzeitpunkt für die vollständige Untersuchung fest.

Unter Android 12 oder höher führt die App diese Aufgabe möglicherweise später aus, wenn sich das Gerät im Stromsparmodus befindet.

8. Klicken Sie auf **Anwenden**, um die vorgenommenen Änderungen zu speichern.

Die Einstellungen werden nach der nächsten planmäßigen Synchronisierung des Geräts mit Kaspersky Security Center auf dem mobilen Gerät konfiguriert. Kaspersky Endpoint Security für Android untersucht alle Dateien, einschließlich der Archive.

Damit der Schutz des mobilen Geräts immer auf dem aktuellen Stand bleibt, müssen die Einstellungen für das Update der Antiviren-Datenbanken konfiguriert werden.

Standardmäßig ist das Update der Antiviren-Datenbanken der App in Roaming-Zonen deaktiviert. Das Update der Antiviren-Datenbanken der App nach Zeitplan wird nicht ausgeführt.

*Gehen Sie folgendermaßen vor, um die Einstellungen für das Update der Antiviren-Datenbanken der App anzupassen:*

1. Wählen Sie in der Konsolenstruktur im Ordner **Verwaltete Geräte** die Administrationsgruppe, zu der die Android-Geräte gehören.
2. Gehen Sie Im Arbeitsbereich der Gruppe auf die Registerkarte **Richtlinien**.
3. Öffnen Sie über Doppelklick auf eine beliebige Spalte das Eigenschaftenfenster der Richtlinie.
4. Wählen Sie im Fenster **Eigenschaften <Name der Richtlinie>** den Abschnitt **Datenbanken-Update**.
5. Damit Kaspersky Endpoint Security für Android das Datenbanken-Update nach dem festgelegten Zeitplan herunterlädt, falls sich das Gerät in einer Roaming-Zone befindet, aktivieren Sie im Block **Datenbanken-Update beim Roaming** das Kontrollkästchen **Datenbanken-Update beim Roaming erlauben**.  
Auch wenn das Kontrollkästchen deaktiviert ist, kann der Benutzer das Update der Antiviren-Datenbanken im Roaming manuell starten.
6. Legen Sie im Abschnitt **Quelle für das Datenbanken-Update** eine Updatequelle fest, von der Kaspersky Endpoint Security für Android die Updates für die Antiviren-Datenbanken der App kopieren und installieren soll:

- **Kaspersky-Server**

Die Kaspersky-Update-Server werden als Update-Quelle für den Download der Datenbanken von Kaspersky Endpoint Security für Android auf die mobilen Geräte der Benutzer verwendet. Um die Datenbanken über die Server von Kaspersky zu aktualisieren, übermittelt Kaspersky Endpoint Security für Android Daten an Kaspersky (z. B. die ID des Starts der Update-Aufgabe). Eine Liste mit den beim Datenbanken-Update übermittelten Daten finde Sie im [Endbenutzer-Lizenzvertrag](#).

- **Administrationsserver**

Der Speicher des Administrationsservers von Kaspersky Security Center wird als Update-Quelle für den Download der Datenbanken von Kaspersky Endpoint Security für Android auf die mobilen Geräte der Benutzer verwendet.

- **Andere Quelle**

Ein Dritthersteller-Server wird als Update-Quelle für den Download der Datenbanken von Kaspersky Endpoint Security für Android auf die mobilen Geräte der Benutzer verwendet. Für das Update muss die Adresse des HTTP-Servers im Feld unten (beispielsweise, <http://domain.com/>) eingegeben werden.

7. Passen Sie im Block **Datenbanken-Update nach Zeitplan** die Einstellungen für den automatischen Start des Updates der Antiviren-Datenbanken auf dem Gerät des Benutzers an. Klicken Sie dazu auf die Schaltfläche **Zeitplan** und legen Sie im folgenden Fenster **Zeitplan** eine Frequenz und den Startzeitpunkt für den Start des Updates fest.

Unter Android 12 oder höher führt die App diese Aufgabe möglicherweise später aus, wenn sich das Gerät im Stromsparmodus befindet.

8. Klicken Sie auf **Anwenden**, um die vorgenommenen Änderungen zu speichern.

Die Einstellungen werden nach der nächsten planmäßigen Synchronisierung des Geräts mit Kaspersky Security Center auf dem mobilen Gerät konfiguriert.

## Schutz von Android-Geräten im Internet

Aktivieren Sie Web-Filter, um die persönlichen Daten des Benutzers des mobilen Geräts im Internet zu schützen. Der Web-Filter blockiert bösartige Websites, deren Zweck darin besteht, einen schädlichen Code zu verbreiten, sowie Phishing-Websites, die Ihre vertraulichen Daten erschleichen und sich Zugang zu Ihren Finanzkonten verschaffen. Der Web-Filter untersucht Webseiten, bevor sie geöffnet werden. Dazu wird der Cloud-Dienst [Kaspersky Security Network](#) genutzt. Web-Filter ermöglicht außerdem, [den Zugriff des Benutzers auf Websites](#) auf Grundlage der erstellten Listen mit erlaubten und verbotenen Websites anzupassen.


Kaspersky Endpoint Security für Android muss als Dienst für erleichterte Bedienung installiert werden. Der Assistent für die Erstkonfiguration von Kaspersky Endpoint Security für Android ermöglicht dem Benutzer, die App als Bedienungshilfe zu installieren. Der Benutzer kann diesen Schritt überspringen oder den Dienst in den Einstellungen des Geräts später deaktivieren.

Der Web-Filter funktioniert auf Android-Geräten nur mit den Browsern Google Chrome (einschließlich der Funktion Custom Tabs), Huawei Browser und Samsung Internet Browser. Web-Filter für Samsung Internet Browser blockiert keine Websites auf mobilen Geräten, wenn ein Arbeitsprofil verwendet wird und [Web-Filter nur für das Arbeitsprofil aktiviert ist](#).

*Um Web-Filter in Google Chrome, Huawei Browser und Samsung Internet Browser zu aktivieren, gehen Sie wie folgt vor:*

1. Wählen Sie in der Konsolenstruktur im Ordner **Verwaltete Geräte** die Administrationsgruppe, zu der die Android-Geräte gehören.
2. Gehen Sie im Arbeitsbereich der Gruppe auf die Registerkarte **Richtlinien**.
3. Öffnen Sie über Doppelklick auf eine beliebige Spalte das Eigenschaftenfenster der Richtlinie.
4. Wählen Sie im Fenster **Eigenschaften** der Richtlinie die Option **Web-Filter**.
5. Um Web-Filter zu verwenden, müssen Sie oder der Gerätebenutzer die Erklärung zur Verarbeitung von Daten für die Verwendung von Web-Filter (Erklärung für Web-Filter) akzeptieren:
  - a. Klicken Sie auf den Link **Erklärung für Web-Filter**.

Die **Erklärung zur Verarbeitung von Daten für die Verwendung von Web-Filter** wird geöffnet. Um die Erklärung für Web-Filter zu akzeptieren, müssen Sie die Datenschutzrichtlinie lesen und akzeptieren.
  - b. Klicken Sie auf den Link "Datenschutzrichtlinie". Lesen und akzeptieren Sie die Datenschutzrichtlinie.

Wenn Sie die Datenschutzrichtlinie nicht akzeptieren, kann der Benutzer des mobilen Geräts die Datenschutzrichtlinie im Assistenten für die Erstkonfiguration oder in der App akzeptieren ( → **Über die App** → **Nutzungsbedingungen** → **Datenschutzrichtlinie**).
  - c. Wählen Sie den Modus für die Annahme der Erklärung für Web-Filter:
    - **Ich habe die Erklärung für Web-Filter gelesen und akzeptiere sie**
    - **Gerätebenutzer zur Annahme der Erklärung für Web-Filter auffordern**
    - **Ich lehne die Erklärung für Web-Filter ab**
6. Wenn Sie die Option **Ich lehne die Erklärung für Web-Filter ab** auswählen, blockiert der Web-Filter keine Websites auf mobilen Geräten. Die Benutzer von mobilen Geräten können den Web-Filter nicht in Kaspersky Endpoint Security aktivieren.



7. Aktivieren Sie das Kontrollkästchen **Web-Filter aktivieren**.

8. Klicken Sie auf **Anwenden**, um die vorgenommenen Änderungen zu speichern.

Die Einstellungen werden nach der nächsten planmäßigen Synchronisierung des Geräts mit Kaspersky Security Center auf dem mobilen Gerät konfiguriert.

## Datenschutz bei Verlust oder Diebstahl des Geräts

Dieser Abschnitt enthält Informationen über die Konfiguration der Schutzes des mobilen Geräts vor unerwünschten Zugriffen im Fall von Verlust oder Diebstahl.

### Befehle an mobiles Gerät senden

Zum Datenschutz auf dem mobilen Gerät können Sie bei Verlust oder Diebstahls die folgenden Befehle versenden.

Befehle zum Datenschutz bei Verlust oder Diebstahl des Geräts

Verbindungsmethode für Kaspersky Security Center	Befehl	Ergebnis der Befehlsausführung
Kaspersky Endpoint Security für Android	Schloss	Das mobile Gerät ist blockiert.
	Entsperren	Auf den Geräten unter Verwaltung des Betriebssystems Android 5.0 – 6.X wird nach der Freischaltung des Mobilgeräts das Kennwort zur Freischaltung des Bildschirm (PIN-Code) mit "1234" ersetzt. Auf den Geräten unter Verwaltung des Betriebssystems Android 7.0 und höher bleibt nach dem Entsperren des Mobilgeräts das Kennwort zur Freischaltung des Bildschirms unverändert.
	Standort des Geräts bestimmen	<p>Der Standort des Geräts wurde bestimmt und wird auf Google Maps angezeigt. Der Mobilfunkanbieter erhebt für den SMS-Versand und den Internetzugang Gebühren.</p> <div><p>Wenn der Benutzer auf Geräten mit Android 12 oder höher die Berechtigung "Ungefährer Standort verwenden" erteilt hat, versucht die App "Kaspersky Endpoint Security für Android" zunächst, den genauen Standort des Geräts zu ermitteln. Gelingt dies nicht, wird der ungefähre Gerätestandort nur zurückgegeben, wenn er frühestens 30 Minuten zuvor empfangen wurde. Andernfalls schlägt der Befehl <b>Gerät orten</b> fehl.</p></div>
	Fotoaufnahme	Das mobile Gerät ist blockiert. Das Foto wird mit der Frontkamera des Geräts aufgenommen, wenn jemand versucht, das Gerät zu entsperren. Der Mobilfunkanbieter erhebt für den SMS-Versand und den Internetzugang Gebühren.



		<p>Beim Versuch, das Gerät zu entsperren, stimmt der Benutzer automatisch der Aufnahme von Fotos zu.</p> <p>Wenn die Berechtigung zur Verwendung der Kamera widerrufen wurde, zeigt das mobile Gerät eine Benachrichtigung an und fordert Sie auf, die Berechtigung zu erteilen. Wenn auf einem mobilen Gerät mit Android 12 oder höher die Berechtigung zur Verwendung der Kamera über die Schnelleinstellungen widerrufen wurde, wird die Benachrichtigung nicht angezeigt, aber das aufgenommene Foto ist schwarz.</p>
	Alarmsignal erzeugen	Das mobile Gerät erzeugt ein Alarmsignal. Das Alarmsignal wird 5 Minuten (bei niedrigem Akkuladestand 1 Minute) lang wiedergegeben.
	Unternehmensdaten löschen	Die Daten in Containern, das Benutzerkonto der Unternehmens-E-Mail, die Verbindungseinstellungen für das WLAN-Netzwerk, das VPN-Netz und den Zugriffspunkt (APN) des Unternehmens, das Arbeitsprofil Android, der KNOX-Container sowie der KNOX License Manager-Schlüssel werden gelöscht.
	Einstellungen auf die Werkseinstellungen zurücksetzen	Alle Daten wurden vom mobilen Gerät gelöscht, die Einstellungen des mobilen Geräts wurden auf Werkseinstellungen zurückgesetzt. Nach dem Ausführen dieses Befehls kann das Gerät die nachfolgenden Befehle nicht erhalten und ausführen.
iOS MDM-Profil	Schloss	Das mobile Gerät ist blockiert.
	Entsperren	Die Sperre des mobilen Geräts mithilfe eines PIN-Codes ist deaktiviert. Der früher festgelegte PIN-Code wurde zurückgesetzt.
	Unternehmensdaten löschen	Alle installierten Konfigurationsprofile, Provisioning-Profile, iOS MDM-Profile und Apps, für die das Kontrollkästchen <b>Zusammen mit dem iOS MDM-Profil deinstallieren</b> aktiviert ist, wurden gelöscht.
	Einstellungen auf die Werkseinstellungen zurücksetzen	Alle Daten wurden vom mobilen Gerät gelöscht, die Einstellungen des mobilen Geräts wurden auf Werkseinstellungen zurückgesetzt. Nach dem Ausführen dieses Befehls kann das Gerät die nachfolgenden Befehle nicht erhalten und ausführen.
Exchange-E-Mail-Postfach	Einstellungen auf die Werkseinstellungen zurücksetzen	Alle Daten wurden vom mobilen Gerät gelöscht, die Einstellungen des mobilen Geräts wurden auf Werkseinstellungen zurückgesetzt. Nach dem Ausführen dieses Befehls kann das Gerät die nachfolgenden Befehle nicht erhalten und ausführen.

Für die Befehlsausführung benötigt Kaspersky Endpoint Security für Android spezielle Rechte und die [Berechtigungen](#). Während der Ausführung des Schnellstartassistenten bietet Kaspersky Endpoint Security für Android an, dem Benutzer der App die erforderlichen Rechte und Berechtigungen bereitzustellen. Der Benutzer kann diese Schritte überspringen oder die Berechtigungen in den Einstellungen des Geräts später deaktivieren. In diesem Fall ist die Ausführung von Befehlen nicht möglich.

Auf Geräten mit Android 10.0 und höher muss der Benutzer für den Zugriff auf den Standort die Berechtigung "Immer" erteilen. Auf Geräten unter Android 11.0 und später muss der Benutzer auch die Berechtigung "Beim Verwenden der App" erteilen, um Zugriff auf die Kamera zu erhalten. Andernfalls werden die Befehle der Funktion "Diebstahlschutz" nicht ausgeführt. Der Benutzer wird über diese Einschränkung in Kenntnis gesetzt und erneut aufgefordert, die Berechtigungen der erforderlichen Ebene zu erteilen. Falls der Benutzer für den Kamerazugriff die Option "Nur dieses Mal" auswählt, gilt der Zugriff für die App als erteilt. Es wird empfohlen, den Benutzer direkt zu kontaktieren, falls die Berechtigung auf den Kamerazugriff erneut angefordert wird.

Weitere Informationen zum Versand der Befehle aus der Liste der mobilen Geräte in der Verwaltungskonsolle finden Sie in der Hilfe zu [Kaspersky Security Center](#).

## Entsperren des mobilen Geräts

Sie können das mobile Gerät auf folgende Weisen entsperren:

- [einen Befehl zum Entsperren an das mobile Gerät senden](#).
- auf dem mobilen Gerät einen einmaligen Code zum Entsperren eingeben (nur für Android-Geräte).

Auf einigen Geräten (z. B. Huawei, Meizu, Xiaomi) muss Kaspersky Endpoint Security für Android manuell zur Liste der Apps hinzugefügt werden, die beim Start des Betriebssystems gestartet werden. Wenn die App nicht zur Liste hinzugefügt wurde, können Sie das Gerät nur mithilfe des einmaligen Codes für die Freischaltung entsperren. Es ist nicht möglich, das Gerät mit Befehlen zu entsperren.

Weitere Informationen zum Versand der Befehle aus der Liste der mobilen Geräte in der Verwaltungskonsolle finden Sie in der Hilfe zu [Kaspersky Security Center](#).

Der *einmaliger Code für die Freischaltung* ist ein Geheimcode des Programms für das Entsperren des mobilen Geräts. Der Einmalige Code wird vom Programm generiert und ist für jedes Mobilgerät einzigartig. Sie können die Länge des einmaligen Codes (4, 8 oder 16 Ziffern) in den Einstellungen der Gruppenrichtlinie im Abschnitt **Diebstahlschutz** ändern.

*Um das Mobilgerät mithilfe des Einmalcodes zu entsperren, gehen Sie wie folgt vor:*

1. Wählen Sie in der Konsolenstruktur **Mobile Geräte verwalten** → **Mobile Geräte** aus.
2. Wählen Sie das mobile Gerät aus, für das Sie einen Einmalcode zum Entsperren erhalten möchten.
3. Öffnen Sie über Doppelklick das Eigenschaftenfenster des mobilen Geräts.
4. Wählen Sie den Abschnitt **Programme** → **Kaspersky Endpoint Security für Android** aus.
5. Öffnen Sie über Doppelklick das Eigenschaftenfenster der Anwendung Kaspersky Endpoint Security.
6. Wählen Sie den Abschnitt **Diebstahlschutz**.
7. Im Block **Einmaliger Code für die Freischaltung des Gerätes** im Feld **Einmalcode** wird der für das ausgewählte Gerät einheitliche Code angegeben.
8. Teilen Sie dem Benutzer des gesperrten Mobilgeräts den Einmalcode auf eine beliebige verfügbare Weise (beispielsweise per E-Mail-Nachricht) mit.

9. Der Benutzer gibt den Einmalcode am Bildschirm des von Kaspersky Endpoint Security für Android gesperrten Geräts ein.

Das Mobilgerät wird entsperrt. Auf den Geräten unter Verwaltung des Betriebssystems Android 5.0 – 6.X wird nach der Freischaltung des Mobilgeräts das Kennwort zur Freischaltung des Bildschirms (PIN-Code) mit "1234" ersetzt. Auf den Geräten unter Verwaltung des Betriebssystems Android 7.0 und höher bleibt nach dem Entsperren des Mobilgeräts das Kennwort zur Freischaltung des Bildschirms unverändert.

## Datenverschlüsselung

Zum Schutz der Daten vor unbefugtem Zugriff muss die Verschlüsselung aller Daten auf dem Gerät aktiviert werden (z. B. Anmeldedaten, Daten zu externen Geräten und Apps sowie E-Mail-Nachrichten, SMS-Nachrichten, Kontakten, Fotos und andere Dateien). Für den Zugriff auf die verschlüsselten Daten muss ein spezieller Schlüssel – [das Kennwort zum Entsperren des Geräts](#) – eingegeben werden. Auf diese Weise wird der Zugriff auf Daten, die verschlüsselt sind, nur gewährt, wenn das Gerät entsperrt wurde.

Auf iOS-Geräten ist die Datenverschlüsselung standardmäßig aktiviert, wenn ein Kennwort zum Entsperren des Geräts festgelegt wurde (**Einstellungen → Touch ID und Kennwort / Face ID und Kennwort → Code aktivieren**).

*Um alle Daten auf einem Android-Gerät zu verschlüsseln, gehen Sie wie folgt vor:*

1. Aktivieren Sie die Bildschirmsperre auf dem Android-Gerät (**Einstellungen → Sicherheit → Bildschirmsperre**).
2. Legen Sie ein Kennwort zum Entsperren des Geräts fest, das den Anforderungen an die Unternehmenssicherheit entspricht.

Es wird empfohlen, nicht das Sperrmuster zum Entsperren des Geräts zu verwenden. Nach der Datenverschlüsselung und dem Neustart des Geräts verlangt Android auf einigen Android-Geräten unter Android 6.0 und höher die Eingabe des Zahlencodes anstelle des Sperrmusters. Das Problem ist verbunden mit den Besonderheiten des Dienstes für erleichterte Bedienung. In diesem Fall müssen Sie zum Entsperren des Bildschirms das Sperrmuster als Zahlencode eingeben. Weitere Informationen zur Eingabe des Sperrmusters als Zahlencode finden Sie auf der Website des technischen Supports des Herstellers ihres mobilen Geräts.

3. Aktivieren Sie die Verschlüsselung aller Daten des Geräts (**Einstellungen → Sicherheit → Telefon verschlüsseln**).

## Sicherheit des Kennworts für das Entsperren des Geräts anpassen

Zum Schutz des Zugriffs auf das mobile Gerät des Benutzers muss für das Gerät ein Entsperrungskennwort festgelegt werden.

Dieser Abschnitt enthält Informationen über die Konfiguration des Kennwortschutzes für Android-Geräte und iOS-Geräte.

### Sicherheit des Kennworts für das Entsperren des Android-Geräts anpassen

Zur Gewährleistung der Sicherheit des Android-Geräts muss die Verwendung des Kennwortes, das beim Einschalten des Geräts aus dem Schlafmodus abgefragt wird, angepasst werden.

Sie können eine Beschränkung der Benutzertätigkeit auf einem Gerät festlegen, für das ein zu einfaches Kennwort zum Entsperren festgelegt wurde (z. B. Gerät sperren). Diese Beschränkung können Sie mithilfe der Komponente [Übereinstimmungsüberprüfung](#) definieren. Wählen Sie dazu in den Einstellungen der Untersuchungsregel die Option **Das Kennwort zum Entsperren entspricht nicht den Anforderungen des Unternehmens** aus.

Auf einigen Samsung-Geräten mit dem Betriebssystem Android 7.0 und höher kann das Gerät gesperrt werden, wenn der Benutzer versucht, das Gerät mit einer nicht unterstützten Methode zu entsperren (z. B. mit Sperrmuster), und folgende Bedingungen erfüllt sind: [Der Schutz vor Deinstallation für Kaspersky Endpoint Security für Android ist aktiviert](#) und [die Anforderungen an die Stärke des Kennworts zum Entsperren des Geräts sind festgelegt](#). Zum Entsperren muss ein bestimmter [Befehl an das Gerät gesendet](#) werden.

*Gehen Sie folgendermaßen vor, um die Verwendung des Kennworts für das Entsperren des Geräts anzupassen:*

1. Wählen Sie in der Konsolenstruktur im Ordner **Verwaltete Geräte** die Administrationsgruppe, zu der die Android-Geräte gehören.
2. Gehen Sie im Arbeitsbereich der Gruppe auf die Registerkarte **Richtlinien**.
3. Öffnen Sie über Doppelklick auf eine beliebige Spalte das Eigenschaftenfenster der Richtlinie.
4. Wählen Sie im Fenster **Eigenschaften <Name der Richtlinie>** den Abschnitt **Geräteverwaltung**.
5. Wenn Sie möchten, dass die App prüft, ob ein Kennwort für das Entsperren des Geräts vorhanden ist, aktivieren Sie im Block **Bildschirmsperre** das Kontrollkästchen **Zum Festlegen eines Kennworts für das Entsperren des Bildschirms auffordern**.

Wenn die Anwendung feststellt, dass auf dem Gerät kein Kennwort vorhanden ist, wird der Benutzer aufgefordert, ein Kennwort festzulegen. Das Kennwort wird unter Berücksichtigung der vom Administrator angegebenen Einstellungen festgelegt.

6. Geben Sie die Mindestanzahl von Zeichen im Kennwort an.

Mindestanzahl von Zeichen im Kennwort des Benutzers. Mögliche Werte: 4 bis 16 Zeichen.

Standardmäßig enthält das Benutzerkennwort 4 Zeichen.

Auf Geräten mit Android 10.0 oder später löst Kaspersky Endpoint Security die Anforderungen an die Zuverlässigkeit des Kennworts in einen der Systemwerte auf: Mittel oder Hoch.

Die Werte für Geräte mit Android 10.0 oder höher werden mithilfe der folgenden Regeln bestimmt:

- Wenn eine Kennwortlänge von 1 bis 4 Zeichen erforderlich ist, fordert die App den Benutzer auf, ein Kennwort mittlerer Stärke festzulegen. Dieses muss entweder numerisch (PIN) ohne wiederholte oder aufeinanderfolgende (z. B. 1234) Sequenzen oder alphabetisch/alphanumerisch sein. PIN oder Kennwort müssen mindestens 4 Zeichen lang sein.
  - Wenn eine Kennwortlänge von 5 oder mehr Zeichen erforderlich ist, fordert die App den Benutzer auf, ein Kennwort hoher Stärke festzulegen. Dieses muss entweder numerisch (PIN) ohne wiederholte oder aufeinanderfolgende Sequenzen oder alphabetisch/alphanumerisch (Kennwort) sein. Die PIN muss mindestens 8 Zeichen lang sein, das Kennwort muss mindestens 6 Zeichen lang sein.
7. Wenn Sie möchten, dass der Benutzer die Möglichkeit hat, Fingerabdrücke zum Entsperren des Bildschirms zu verwenden, aktivieren Sie das Kontrollkästchen **Verwendung von Fingerabdrücken erlauben**. Wenn das Kennwort zum Entsperren nicht den Anforderungen an die Unternehmenssicherheit entspricht, ist es nicht möglich, den Fingerabdruckscanner zum Entsperren des Bildschirms zu verwenden.

Auf Geräten unter Android 10.0 oder später kann die Verwendung des Fingerabdrucks zum Entsperren des Bildschirms nur für das Arbeitsprofil verwaltet werden.

Kaspersky Endpoint Security für Android beschränkt nicht die Nutzung des Fingerabdruckscanners für die Anmeldung in Apps oder die Bestätigung von Käufen.

Auf einigen Samsung-Geräten ist es nicht möglich, die Verwendung von Fingerabdrücken zum Entsperren des Bildschirms zu verbieten. Außerdem verbietet Kaspersky Endpoint Security für Android auf einigen Samsung-Geräten, auf denen das Kennwort zum Entsperren nicht den Anforderungen an die Unternehmenssicherheit entspricht, die Nutzung der Fingerabdrücke für das Entsperren des Bildschirms nicht.

Nach dem Hinzufügen eines Fingerabdrucks in den Einstellungen des Geräts kann der Benutzer den Bildschirm auf eine der folgenden Arten entsperren:

- Finger auf den Fingerabdruckscanner legen – Standardmethode.
- Kennwort für das Entsperren eingeben – alternative Methode.

8. Klicken Sie auf **Anwenden**, um die vorgenommenen Änderungen zu speichern.

Die Einstellungen werden nach der nächsten planmäßigen Synchronisierung des Geräts mit Kaspersky Security Center auf dem mobilen Gerät konfiguriert.

## Sicherheit des Kennworts für das Entsperren des iOS MDM-Geräts anpassen

Für den Schutz der Daten des iOS MDM-Geräts müssen die Anforderungen an die Sicherheit des Entsperrungskennworts angepasst werden.

Standardmäßig darf der Benutzer ein einfaches Kennwort verwenden. Ein *einfaches Kennwort* ist ein Kennwort, das eine Abfolge von Zeichen oder sich wiederholenden Zeichen enthält, beispielsweise, "abcd" oder "2222". Die Eingabe eines alphanumerischen Kennworts mit Sonderzeichen ist nicht obligatorisch. Die Gültigkeitsdauer und die Anzahl der Versuche zur Eingabe des Kennworts sind standardmäßig nicht begrenzt.

*Um die Sicherheitseinstellungen des Entsperrungskennworts für das iOS MDM-Gerät anzupassen, gehen Sie wie folgt vor:*

1. Wählen Sie in der Konsolenstruktur im Ordner **Verwaltete Geräte** die Administrationsgruppe, zu der die iOS MDM-Geräte gehören.
2. Gehen Sie Im Arbeitsbereich der Gruppe auf die Registerkarte **Richtlinien**.
3. Öffnen Sie über Doppelklick das Eigenschaftfenster der Richtlinie.
4. Wählen Sie im Fenster **Eigenschaften <Name der Richtlinie>** den Abschnitt **Kennwort**.
5. Aktivieren Sie im Block **Kennwordeinstellungen** das Kontrollkästchen **Einstellungen auf dem Gerät anwenden**.
6. Passen Sie die Sicherheitseinstellungen des Entsperrungskennworts an:

- Um dem Benutzer die Verwendung eines einfachen Kennworts zu erlauben, aktivieren Sie das Kontrollkästchen **Einfaches Passwort erlauben**.
- Um die Verwendung eines alphanumerischen Kennwortes zu fordern, aktivieren Sie das Kontrollkästchen **Alphanumerische Wertangabe verlangen**.
- Wählen Sie in der Liste **Mindestanzahl von Zeichen** die Mindestlänge des Kennworts in Zeichen aus.
- Wählen Sie in der Liste **Mindestanzahl von Sonderzeichen** die Mindestanzahl der Sonderzeichen im Kennwort aus (beispielsweise, "\$", "&", "!").
- Legen Sie im Feld **Maximale Verwendungsdauer** den Zeitraum in Tagen fest, während dessen das Kennwort gültig ist. Nach Ablauf der festgelegten Gültigkeitsdauer fordert Kaspersky Device Management für iOS den Benutzer auf, das Kennwort zu ändern.
- Wählen Sie in der Liste **Automatische Sperre aktivieren nach** die Zeit für die Aktivierung der Autosperre des iOS MDM-Mobilgeräts.
- Legen Sie im Feld **Kennwortchronik** die Anzahl der verwendeten Kennwörter (einschließlich das aktuelle) fest, die Kaspersky Device Management für iOS beim Ändern des Kennworts mit dem neuen Kennwort vergleichen soll. Wenn die Kennwörter übereinstimmen, wird das neue Kennwort nicht akzeptiert.
- Wählen Sie in der Liste **Maximale Dauer, um ohne Kennwort zu entsperren** den Zeitraum, während dessen der Benutzer das iOS MDM-Mobilgerät ohne die Eingabe eines Kennworts entsperren kann.
- Wählen Sie in der Liste **Maximale Anzahl der Eingabeversuche** Anzahl der verfügbaren Eingabeversuche für die Entsperrung des iOS MDM-Geräts aus.

7. Klicken Sie auf **Anwenden**, um die vorgenommenen Änderungen zu speichern.

Nach dem Anwenden der Richtlinie auf dem Mobilgerät überprüft Kaspersky Device Management für iOS die Kennwortsicherheit. Wenn die Sicherheit des Entsperrungskennworts auf dem Gerät nicht den Anforderungen der Richtlinie entspricht, wird der Benutzer dazu aufgefordert, das Kennwort zu ändern.

## Sicherheit des Kennworts für das Entsperrn des EAS-Geräts anpassen

Für den Schutz von Daten des EAS-Geräts muss ein sicheres Entsperrungskennwort eingerichtet werden.

Standardmäßig fordert Kaspersky Device Management für iOS den Benutzer nach dem Einschalten des mobilen Endgeräts nicht dazu auf, ein Entsperrungskennwort einzugeben oder festzulegen.

*Um die Sicherheitseinstellungen des Entsperrungskennworts für das EAS-Gerät anzupassen, gehen Sie wie folgt vor:*

1. Wählen Sie in der Konsolenstruktur im Ordner **Verwaltete Geräte** die Administrationsgruppe, zu der die EAS-Geräte gehören.
2. Gehen Sie Im Arbeitsbereich der Gruppe auf die Registerkarte **Richtlinien**.
3. Öffnen Sie über Doppelklick das Eigenschaftfenster der Richtlinie.
4. Wählen Sie im Fenster Eigenschaften <Name der Richtlinie> den Abschnitt **Kennwort**.
5. Aktivieren Sie im Block **Kennwordeinstellungen** das Kontrollkästchen **Kennwort erforderlich**.
6. Passen Sie die Sicherheitseinstellungen des Entsperrungskennworts an:

- Damit der Benutzer im Kennwort verpflichtend Buchstaben und Ziffern verwenden muss, aktivieren Sie das Kontrollkästchen **Alphanumerische Wertangabe verlangen**. Legen Sie im Feld **Minimale Anzahl von Zeichensätzen** die Schwierigkeitsstufe des alphanumerischen Kennworts fest. Mögliche Werte: von 1 bis 4. Der Wert 1 entspricht der minimalen Sicherheitsstufe.
- Um dem Benutzer die Verwendung der Funktion für die Kennwortwiederherstellung zu erlauben, aktivieren Sie das Kontrollkästchen **Kennwortwiederherstellung aktivieren**.
- Um die Dateien im Gerätespeicher zu verschlüsseln, aktivieren Sie das Kontrollkästchen **Verschlüsselung auf dem Gerät verlangen**.
- Um die Dateien auf der Speicherkarte zu verschlüsseln, aktivieren Sie das Kontrollkästchen **Verschlüsselung auf der Speicherkarte verlangen**.
- Um dem Benutzer die Verwendung eines einfachen, nur aus Zahlen bestehen Kennworts zu erlauben, aktivieren Sie das Kontrollkästchen **Einfaches Passwort erlauben**.
- Um die Anzahl der Eingabeversuche für den Zugriff auf das Gerät zu beschränken, aktivieren Sie das Kontrollkästchen **Maximale Anzahl der Eingabeversuche**. Geben Sie im Feld rechts vom Kontrollkästchen die Anzahl der verfügbaren Eingabeversuche für die Entsperrung des Geräts ein. Wenn der Benutzer die festgelegte Anzahl der Fehlversuche überschreitet, löscht Kaspersky Device Management für iOS alle Daten von dem Gerät.
- Um die Mindestanzahl von Zeichen im Kennwort des Benutzers festzulegen, aktivieren Sie das Kontrollkästchen **Mindestanzahl von Zeichen**. Geben Sie im Feld rechts vom Kontrollkästchen die minimale Anzahl der Zeichen im Kennwort ein. Mögliche Werte: 4 bis 16 Zeichen.
- Um nach einer bestimmten Zeit der Inaktivität des Benutzers (der Benutzer hat auf dem Gerät keine Aktionen durchgeführt) die Eingabe des Kennworts zu fordern, aktivieren Sie das Kontrollkästchen **Inaktivitätsdauer bis zur erneuten Kennworteingabe (Minuten)**. Geben Sie im Feld rechts neben dem Kontrollkästchen die Inaktivitätsdauer in Minuten an. Nach Ablauf dieser Zeitspanne fordert das Programm den Benutzer auf, das Kennwort einzugeben.
- Um die Gültigkeitsdauer des Kennworts zu beschränken, aktivieren Sie das Kontrollkästchen **Kennwortalter (Tage)**. Geben Sie im Feld rechts vom Kontrollkästchen die Gültigkeitsdauer des Kennworts ein. Nach Ablauf dieser Frist fordert das Programm den Benutzer auf, ein neues Kennwort einzugeben.
- Geben Sie im Feld **Kennwortchronik** die Anzahl der vorherigen Kennwörter an, die vom Benutzer nicht verwendet werden können.

7. Klicken Sie auf **Anwenden**, um die vorgenommenen Änderungen zu speichern.

Die Einstellungen werden nach der nächsten planmäßigen Synchronisierung des Geräts mit Kaspersky Security Center auf dem mobilen Gerät konfiguriert. Nach dem Anwenden der Richtlinie auf dem mobilen Gerät des Benutzers überprüft Kaspersky Device Management für iOS, ob ein Kennwort festgelegt wurde. Wenn kein Entsperrungskennwort auf dem Gerät angegeben wurde, wird der Benutzer zu seiner Eingabe aufgefordert. Das Kennwort wird unter Berücksichtigung der in der Richtlinie festgelegten Einstellungen angegeben. Wenn ein Entsperrungskennwort auf dem Gerät angegeben wurde, jedoch nicht den Anforderungen der Richtlinie entspricht, wird der Benutzer dazu aufgefordert, das Kennwort zu ändern.

## Konfiguration des virtuellen privaten Netzwerks (VPN)

Dieser Abschnitt enthält Informationen über das Anpassen der Einstellungen des virtuellen privaten Netzwerkes (VPN) zur sicheren Verbindung mit WLAN-Netzwerken.

## VPN-Einstellungen auf Android-Geräten (nur Samsung)

Für die sichere Verbindung des Android-Gerätes mit WLAN-Netzwerken und den Schutz der Datenübertragung ist es nötig, die VPN-Einstellungen (Virtual Private Network) anzupassen.

Die VPN-Konfiguration ist nur für Samsung-Geräte möglich.

Bei der Verwendung eines virtuellen privaten Netzwerks müssen folgende Anforderungen berücksichtigt werden:

- Die App, die die VPN-Verbindung verwendet, muss in den [Einstellungen der Firewall erlaubt sein](#).
- Die in der Richtlinie konfigurierten Einstellungen des virtuellen privaten Netzwerks können nicht für System-Apps verwendet werden. Für System-Apps muss die VPN-Verbindung manuell konfiguriert werden.
- Für einige Apps, die eine VPN-Verbindung verwenden, ist beim ersten Start eine zusätzliche Konfiguration erforderlich. Um die Konfiguration durchführen zu können, muss die VPN-Verbindung in den Einstellungen der App freigegeben werden.

*Um das VPN auf dem mobilen Gerät des Benutzers anzupassen, gehen Sie wie folgt vor:*

1. Wählen Sie in der Konsolenstruktur im Ordner **Verwaltete Geräte** die Administrationsgruppe, zu der die Android-Geräte gehören.
2. Gehen Sie Im Arbeitsbereich der Gruppe auf die Registerkarte **Richtlinien**.
3. Öffnen Sie über Doppelklick auf eine beliebige Spalte das Eigenschaftenfenster der Richtlinie.
4. Wählen Sie im Fenster **Eigenschaften** der Richtlinie den Abschnitt **Verwaltung von Samsung KNOX** → **Verwaltung von Samsung-Geräten** aus.
5. Klicken Sie im Block **VPN** auf **Anpassen**.  
Das Fenster **VPN-Netzwerk** wird geöffnet.
6. Wählen Sie in der Dropdown-Liste **Verbindungstyp** den Typ der VPN-Verbindung.
7. Geben Sie im Feld **Netzwerkname** den Namen des VPN-Tunnels ein.
8. Geben Sie im Feld **Serveradresse** den Netzwerknamen oder die IP-Adresse des VPN-Servers ein.
9. Geben Sie im Feld **DNS-Suchdomain(s)** die Domain für die DNS-Suche ein, die automatisch zum Namen des DNS-Servers hinzugefügt wird.  
Sie können mehrere Domains der DNS-Suche mit Leerzeichen getrennt eingeben.
10. Geben Sie im Feld **DNS-Server** den vollständigen Domain-Namen oder die IP-Adresse des DNS-Servers ein.  
Sie können mehrere DNS-Server mit Leerzeichen getrennt angeben.
11. Geben Sie im Feld **Re-Routing** den IP-Adressbereich des Netzwerks an, mit dem Daten über die VPN-Verbindung ausgetauscht werden.



Wenn im Feld **Re-Routing** kein Bereich von IP-Adressen angegeben ist, wird der gesamte Internet-Datenverkehr über die VPN-Verbindung geleitet.

12. Passen Sie für die Netzwerktypen **IPSec Xauth PSK** und **L2TP IPSec PSK** zusätzlich folgende Einstellungen an:

- a. Geben Sie im Feld **IPSec-Schlüssel (Shared Secret)** das Kennwort des vorher im Vorfeld installierten Sicherheitsschlüssels IPSec ein.
- b. Geben Sie im Feld **IPSec-Kennung** den Benutzernamen des Mobilgerätnutzers ein.

13. Geben Sie für den Netzwerktyp **L2TP IPSec PSK** im Feld **L2TP-Schlüssel** zusätzlich das Kennwort für den L2TP-Schlüssel ein.

14. Aktivieren Sie für den Netzwerktyp **PPTP** das Kontrollkästchen **SSL-Verbindung verwenden**, damit die App für die Gewährleistung der Datensicherheit beim Verbinden des Mobilgeräts mit dem VPN-Server die Verschlüsselungsmethode MPPE (Microsoft Point-to-Point Encryption) verwendet.

15. Klicken Sie auf **Anwenden**, um die vorgenommenen Änderungen zu speichern.

Die Einstellungen werden nach der nächsten planmäßigen Synchronisierung des Geräts mit Kaspersky Security Center auf dem mobilen Gerät konfiguriert.

## VPN-Einstellungen auf iOS MDM-Geräten

Für die Verbindung des iOS MDM-Geräts mit dem virtuellen privaten Netzwerk (VPN) und Sicherstellung der Datensicherheit beim Verbinden mit dem VPN-Netzwerk müssen die Einstellungen für die Verbindung mit dem VPN-Netzwerk angepasst werden.

*Um die VPN-Verbindung auf dem iOS MDM-Gerät anzupassen, gehen Sie wie folgt vor:*

1. Wählen Sie in der Konsolenstruktur im Ordner **Verwaltete Geräte** die Administrationsgruppe, zu der die iOS MDM-Geräte gehören.
2. Gehen Sie Im Arbeitsbereich der Gruppe auf die Registerkarte **Richtlinien**.
3. Öffnen Sie über Doppelklick das Eigenschaftfenster der Richtlinie.
4. Wählen Sie im Fenster **Eigenschaften <Name der Richtlinie>** den Abschnitt **VPN**.
5. Klicken Sie im Abschnitt **VPN-Netzwerke** auf **Hinzufügen**.

Das Fenster **VPN-Netzwerk** wird geöffnet.

6. Geben Sie im Feld **Netzwerkname** den Namen des VPN-Tunnels ein.

7. Wählen Sie in der Dropdown-Liste **Verbindungstyp** den Typ der VPN-Verbindung:

- **L2TP** (Layer 2 Tunneling Protocol). Die Verbindung unterstützt die Authentifizierung des Nutzers eines iOS MDM-Mobilgeräts mithilfe der MS-CHAP v2-Kennwörter, die 2-Faktor-Authentifizierung und die automatische Authentifizierung mithilfe eines Schlüssel (Shared Secrets).
- **PPTP** (Point-to-Point Tunneling Protocol). Die Verbindung unterstützt die Authentifizierung des Nutzers eines iOS MDM-Mobilgeräts mithilfe der MS-CHAP v2-Kennwörter und die 2-Faktor-Authentifizierung.

- **IPSec (Cisco).** Die Verbindung unterstützt die Authentifizierung des Nutzers mithilfe von Kennwörtern, die 2-Faktor-Authentifizierung und die automatische Authentifizierung mithilfe eines Schlüssels (Shared Secret)s und der Zertifikate.
- **Cisco AnyConnect.** Die Verbindung unterstützt die Netzwerk-Firewall Cisco Adaptive Security Appliance (ASA) der Version 8.0(3)1 und höher. Für die Konfiguration der VPN-Verbindung muss auf dem iOS MDM-Mobilgerät die App Cisco AnyConnect aus dem App Store installiert werden.
- **Juniper SSL.** Die Verbindung unterstützt das Gateway Juniper Networks SSL VPN Serie SA Version 6.4 und höher mit dem Paket Juniper Networks IVE Version 7.0 und höher. Für die Konfiguration der VPN-Verbindung muss auf dem iOS MDM-Gerät die Anwendung JUNOS aus dem App Store installiert werden.
- **F5 SSL.** Die Verbindung unterstützt die Lösungen F5 BIG-IP Edge Gateway, Access Policy Manager und Fire SSL VPN. Für die Konfiguration der VPN-Verbindung muss auf dem iOS MDM-Gerät die App F5 BIG-IP Edge Client aus dem App Store installiert werden.
- **SonicWALL Mobile Connect.** Die Verbindung unterstützt Geräte SonicWALL Aventail E-Class Secure Remote Access der Version 10.5.4 und höher, Geräte SonicWALL SRA der Version 5.5 und höher und Geräte SonicWALL Next-Generation Firewall, einschließlich TZ, NSA, E-Class NSA mit SonicOS der Version 5.8.1.0 und höher. Für die Konfiguration der VPN-Verbindung muss auf dem iOS MDM-Gerät die App SonicWALL Mobile Connect aus dem App Store installiert werden.
- **Aruba VIA.** Die Verbindung unterstützt Controller für den Mobilzugriff Aruba Networks. Für ihre Konfiguration muss auf dem iOS MDM-Gerät die Anwendung Aruba Networks VIA aus dem App Store installiert werden.
- **Custom SSL.** Die Verbindung unterstützt die Authentifizierung des Benutzers eines iOS MDM-Mobilgeräts mithilfe von Kennwörtern und Zertifikaten sowie die 2-Faktor-Authentifizierung.

8. Geben Sie im Feld **Serveradresse** den Netzwerknamen oder die IP-Adresse des VPN-Servers ein.

9. Geben Sie im Feld **Accountname** den Kontonamen des Benutzerkontos für die Autorisierung auf dem VPN-Server. Sie können Makros aus der Dropdown-Liste **Makro hinzufügen**.

10. Passen Sie die Sicherheitsparameter für die VPN-Verbindung gemäß dem ausgewählten Typen des virtuellen privaten Netzwerks an.

11. Bei Bedarf können Sie die Einstellungen für die Verbindung mit einem VPN-Netzwerk über einen Proxyserver anpassen:

- Wählen Sie die Registerkarte **Einstellungen für Proxy-Server**.
- Wählen Sie den Konfigurationsmodus für den Proxy-Server aus und geben die Verbindungseinstellungen an.
- Klicken Sie auf **OK**.

Auf dem iOS MDM-Gerät werden die Einstellungen für die Verbindung des Geräts mit einem VPN-Netzwerk über den Proxy-Server angepasst werden.

12. Klicken Sie auf **OK**.

Das neue VPN-Netzwerk wird in der Liste angezeigt.

13. Klicken Sie auf **Anwenden**, um die vorgenommenen Änderungen zu speichern.

Nach dem Anwenden der Richtlinie wird auf dem iOS MDM-Gerät die Verbindung mit dem VPN-Netzwerk angepasst werden.

## Firewall-Einstellungen auf Android-Geräten (nur Samsung)

Für die Kontrolle der Netzwerkverbindungen müssen auf dem Mobilgerät des Nutzers die Firewall-Einstellungen angepasst werden.

*Um die Firewall auf dem mobilen Gerät anzupassen, gehen Sie wie folgt vor:*

1. Wählen Sie in der Konsolenstruktur im Ordner **Verwaltete Geräte** die Administrationsgruppe, zu der die Android-Geräte gehören.
2. Gehen Sie Im Arbeitsbereich der Gruppe auf die Registerkarte **Richtlinien**.
3. Öffnen Sie über Doppelklick auf eine beliebige Spalte das Eigenschaftenfenster der Richtlinie.
4. Wählen Sie im Fenster **Eigenschaften** der Richtlinie den Abschnitt **Verwaltung von Samsung KNOX** → **Verwaltung von Samsung-Geräten** aus.
5. Klicken Sie unter **Firewall** auf **Anpassen**.  
Das Fenster **Firewall** wird geöffnet.
6. Wählen Sie den Firewall-Modus:
  - Um alle eingehenden und ausgehenden Verbindungen zu erlauben, verschieben Sie den Schieberegler in die Position **Alle erlauben**.
  - Um jede Netzwerkaktivität mit Ausnahme von Apps aus der Ausnahmenliste zu blockieren, verschieben Sie den Schieberegler in die Position **Alle blockieren, Ausnahmen ausgenommen**.
7. Wenn Sie den Firewall-Modus **Alle blockieren, Ausnahmen ausgenommen** gewählt haben, erstellen Sie eine Ausnahmenliste:
  - a. Klicken Sie auf **Hinzufügen**.  
Das Fenster **Ausnahme für Firewall** wird geöffnet.
  - b. Geben Sie im Feld **App-Name** den Namen der mobilen App ein.
  - c. Geben Sie im Feld **Paketname** den Systemnamen der mobilen App (zum Beispiel `com.mobileapp.example`) ein.
  - d. Klicken Sie auf **OK**.
8. Klicken Sie auf **Anwenden**, um die vorgenommenen Änderungen zu speichern.

Die Einstellungen werden nach der nächsten planmäßigen Synchronisierung des Geräts mit Kaspersky Security Center auf dem mobilen Gerät konfiguriert.

## Schutz von Kaspersky Endpoint Security für Android vor Deinstallation

Für den Schutz des mobilen Geräts und die Erfüllung der Anforderungen an die Unternehmenssicherheit können Sie den Schutz von Kaspersky Endpoint Security für Android vor dem Deinstallieren aktivieren. In diesem Fall ist dem Benutzer das Deinstallieren der App mithilfe der Benutzeroberfläche von Kaspersky Endpoint Security für Android nicht möglich. Beim Deinstallieren der App mithilfe der Tools des Betriebssystems Android wird eine Anfrage zum Deaktivieren der Administratorrechte für Kaspersky Endpoint Security für Android angezeigt. Nach dem Deaktivieren der Rechte wird das mobile Gerät gesperrt.

Auf einigen Samsung-Geräten mit dem Betriebssystem Android 7.0 und höher kann das Gerät gesperrt werden, wenn der Benutzer versucht, das Gerät mit einer nicht unterstützten Methode zu entsperren (z. B. mit Sperrmuster), und folgende Bedingungen erfüllt sind: [Der Schutz vor Deinstallation für Kaspersky Endpoint Security für Android ist aktiviert](#) und [die Anforderungen an die Stärke des Kennworts zum Entsperren des Geräts sind festgelegt](#). Zum Entsperren muss ein bestimmter [Befehl an das Gerät gesendet](#) werden.

*Um den Schutz von Kaspersky Endpoint Security für Android vor dem Deinstallieren zu aktivieren, gehen Sie wie folgt vor:*

1. Wählen Sie in der Konsolenstruktur im Ordner **Verwaltete Geräte** die Administrationsgruppe, zu der die Android-Geräte gehören.
2. Gehen Sie im Arbeitsbereich der Gruppe auf die Registerkarte **Richtlinien**.
3. Öffnen Sie über Doppelklick auf eine beliebige Spalte das Eigenschaftenfenster der Richtlinie.
4. Wählen Sie im folgenden Fenster **Eigenschaften <Name der Richtlinie>** den Abschnitt **Erweitert** aus.
5. Deaktivieren Sie im Block **App Kaspersky Endpoint Security für Android löschen** das Kontrollkästchen **Löschen der App Kaspersky Endpoint Security für Android erlauben**.

Auf den Geräten unter Verwaltung des Betriebssystems Android 7.0 und höher muss zum Schutz der App vor dem Löschen Kaspersky Endpoint Security für Android als Dienst für erleichterte Bedienung installiert sein. Während der Ausführung des Schnellstartassistenten bietet Kaspersky Endpoint Security für Android an, dem Benutzer der App die erforderlichen Berechtigungen bereitzustellen. Der Benutzer kann diese Schritte überspringen oder die Berechtigungen in den Einstellungen des Geräts später deaktivieren. In diesem Fall ist der Schutz der Anwendung vor dem Löschen nicht aktiviert.

6. Klicken Sie auf **Anwenden**, um die vorgenommenen Änderungen zu speichern.

Die Einstellungen werden nach der nächsten planmäßigen Synchronisierung des Geräts mit Kaspersky Security Center auf dem mobilen Gerät konfiguriert. Beim Versuch, die App zu löschen, wird das mobile Gerät gesperrt.

## Gehackte Geräte erkennen (root)

Kaspersky Security für mobile Endgeräte ermöglicht das Erkennen einer Manipulation des Geräts (root). Auf gehackten Geräten sind die Systemdateien nicht geschützt und können verändert werden. Ferner können auf gehackten Geräte Apps von Drittherstellern aus unbekannten Quellen installiert werden. Nachdem Sie festgestellt haben, dass ein Gerät gehackt wurde, wird es empfohlen, den normalen Gerätebetrieb wiederherzustellen.

Um das Erlangen von root-Rechten durch den Benutzer zu entdecken, verwendet Kaspersky Endpoint Security für Android folgende Dienste:

- *Integrierter Dienst Kaspersky Endpoint Security für Android*: ein Dienst von Kaspersky, der das Erlangen von root-Rechten durch den Benutzer des mobilen Geräts prüft (Kaspersky Mobile Security SDK).

- **SafetyNet Attestation:** ein Google-Dienst, der die Integrität des Betriebssystems prüft, die Hardware und Software des Geräts analysiert und sonstige Sicherheitsprobleme ermittelt. Weitere Informationen über die Funktion von SafetyNet Attestation finden Sie auf der [Website des technischen Supports von Android](#).

Sollte ein Gerät gehackt werden, erhalten Sie eine Benachrichtigung. Sie können Benachrichtigungen über gehackte Geräte im Arbeitsplatz des Administrationsservers auf der Registerkarte **Monitoring** einsehen. Außerdem können Sie die Benachrichtigungen über gehackte Geräte in den Benachrichtigungseinstellungen über Ereignisse deaktivieren.

Auf Geräten unter dem Betriebssystem Android können Sie im Fall eines gehackten Geräts eine Beschränkung der Benutzertätigkeit auf dem Gerät festlegen (beispielsweise das Gerät blockieren). Diese Beschränkung können Sie mithilfe der Komponente [Übereinstimmungsüberprüfung](#) (s. Abb. unten) anpassen. Dazu muss in den Einstellungen der Überprüfungsregeln das Kriterium **Auf dem Gerät wurden root-Rechte empfangen** ausgewählt werden.

## Globalen HTTP-Proxy auf iOS MDM-Geräten anpassen

Für den Schutz des Datenverkehrs muss die Verbindung des iOS MDM-Geräts mit dem Internet über einen Proxy-Server angepasst werden.

Die automatische Verbindung mit dem Internet über einen Proxy-Server ist nur für kontrollierte Geräte möglich.

*Um Global HTTP Proxy auf dem iOS MDM-Gerät anzupassen, gehen Sie wie folgt vor:*

1. Wählen Sie in der Konsolenstruktur im Ordner **Verwaltete Geräte** die Administrationsgruppe, zu der die iOS MDM-Geräte gehören.
2. Gehen Sie Im Arbeitsbereich der Gruppe auf die Registerkarte **Richtlinien**.
3. Öffnen Sie über Doppelklick das Eigenschaftfenster der Richtlinie.
4. Wählen Sie im Fenster **Eigenschaften <Name der Richtlinie>** den Abschnitt **Globaler HTTP-Proxy**.
5. Aktivieren Sie im Block **Einstellungen für Globaler HTTP-Proxy** das Kontrollkästchen **Einstellungen auf dem Gerät anwenden**.
6. Wählen Sie den Konfigurationstyp für Global HTTP Proxy aus.

Standardmäßig ist der manuelle Installationstyp für Global HTTP Proxy festgelegt und der Benutzer darf keine Verbindung mit den abonnierten Netzwerken ohne eine Proxy-Server-Verbindung herstellen. *Captive-Netzwerke* sind drahtlose Netzwerke, die eine vorherige Authentifizierung auf dem Mobilgerät ohne eine Proxy-Server-Verbindung erfordern.

- Wenn Sie die Einstellungen für die Verbindung mit dem Proxy-Server manuell eingeben möchten, gehen Sie wie folgt vor:
  - a. Wählen Sie in der Dropdown-Liste **Einstellungstyp Manuell** aus.
  - b. Geben Sie im Feld **Proxyserveradresse und Port** den Namen des Hosts, der Domain oder die IP-Adresse des Proxy-Servers und die Portnummer des Proxy-Servers ein.

- c. Geben Sie im Feld **Benutzername** den Kontonamen des Benutzers für die Autorisierung auf dem Proxyserver an. Sie können Makros aus der Dropdown-Liste **Makro hinzufügen**.
- d. Geben Sie im Feld **Kennwort** den Namen des Accounts für die Autorisierung auf dem Proxy-Server.
- e. Um dem Benutzer den Zugriff auf Abonetzwerke zu erlauben, aktivieren Sie das Kontrollkästchen **Zugriff auf abonnierte Netzwerke ohne Verbindung zum Proxy-Server erlauben**.
- Um die Einstellungen der Verbindung mit dem Proxyserver mithilfe der vorbereiteten PAC-Datei (Proxy Auto Configuration) anzupassen, gehen Sie wie folgt vor:
  - a. Wählen Sie in der Dropdown-Liste **Einstellungstyp Automatisch** aus.
  - b. Geben Sie im Feld **Webadresse der PAC-Datei** die Webadresse der PAC-Datei ein (beispielsweise, <http://www.example.com/filename.pac>).
  - c. Um dem Benutzer die Verbindung des mobilen Geräts mit dem kabellosen Netzwerk ohne die Verwendung eines Proxyservers zu erlauben, falls die PAC-Datei nicht verfügbar ist, aktivieren Sie das Kontrollkästchen **Direktverbindung zulassen, wenn PAC-Datei nicht verfügbar**.
  - d. Um dem Benutzer den Zugriff auf Abonetzwerke zu erlauben, aktivieren Sie das Kontrollkästchen **Zugriff auf abonnierte Netzwerke ohne Verbindung zum Proxy-Server erlauben**.
- 7. Klicken Sie auf **Anwenden**, um die vorgenommenen Änderungen zu speichern.

Nach dem Anwenden der Richtlinie kann der Benutzer des mobilen Geräts eine Verbindung mit dem Internet über einen Proxyserver herstellen.

## Sicherheitszertifikate auf iOS MDM-Geräten hinzufügen

Für die Vereinfachung der Benutzer-Authentifizierung und die Datensicherheit müssen auf dem iOS MDM-Gerät des Nutzers Zertifikate hinzugefügt werden. Die Signatur von Daten mithilfe eines Zertifikats ermöglicht den Schutz der Daten vor Änderungen während des Transfers im Netzwerk. Die Datenverschlüsselung mithilfe eines Zertifikats ermöglicht einen zusätzlichen Schutz von Informationen. Das Zertifikat kann auch für den Identitätsnachweis des Nutzers verwendet werden.

Kaspersky Device Management für iOS unterstützt folgende Zertifikatstandards:

- **PKCS#1** – Verschlüsselung mit offenem Schlüssel auf der Basis der RSA-Algorithmen.
- **PKCS#12** – Speicherung und Transfers des Zertifikats und des geschlossenen Schlüssels.

*Um ein Sicherheitszertifikat auf dem iOS MDM-Gerät hinzuzufügen, gehen Sie wie folgt vor:*

1. Wählen Sie in der Konsolenstruktur im Ordner **Verwaltete Geräte** die Administrationsgruppe, zu der die iOS MDM-Geräte gehören.
2. Gehen Sie Im Arbeitsbereich der Gruppe auf die Registerkarte **Richtlinien**.
3. Öffnen Sie über Doppelklick das Eigenschaftfenster der Richtlinie.
4. Wählen Sie im Fenster **Eigenschaften <Name der Richtlinie>** den Abschnitt **Zertifikate**.
5. Klicken Sie im Block **Zertifikate** auf **Hinzufügen**.

Das Fenster **Zertifikat** wird geöffnet.

6. Geben Sie im Feld **Dateiname** den Pfad zum Zertifikat an:

Dateien der PKCS#1-Zertifikate haben die Erweiterungen cer, crt oder der. Dateien der PKCS#12-Zertifikate haben die Erweiterungen p12 oder pfx.

7. Klicken Sie auf **Öffnen**.

Wenn das Zertifikat durch ein Kennwort geschützt ist, muss das Kennwort eingegeben werden. Daraufhin wird das neue Zertifikat in der Liste angezeigt.

8. Klicken Sie auf **Anwenden**, um die vorgenommenen Änderungen zu speichern.

Nach dem Anwenden der Richtlinie wird dem Benutzer von der Anwendung vorgeschlagen, Zertifikate aus der erstellten Liste hinzuzufügen.

## SCEP-Profil auf iOS MDM-Geräten hinzufügen

Damit der Benutzer eines iOS MDM-Geräts automatisch Zertifikate aus dem Zertifizierungszentrum über das Internet erhalten kann, muss ein SCEP-Profil hinzugefügt werden. Das SCEP-Profil unterstützt das Protokoll für die einfache Registrierung von Zertifikaten.

Standardmäßig wird das SCEP-Profil mit den folgenden Parametern hinzugefügt:

- Für die Registrierung der Zertifikate wird kein alternativer Inhabername verwendet.
- Es werden drei Versuche für SCEP-Serverabfragen mit einem Intervall von 10 Sekunden unternommen. Wenn alle Versuche der Zertifikatsignatur fehlgeschlagen sind, muss eine neue Anfrage für die Signatur des Zertifikats erstellt werden.
- Das erhaltene Zertifikat darf nicht für die Signatur oder Verschlüsselung von Daten verwendet werden.

Sie können die angegebenen Parameter beim Hinzufügen des SCEP-Profiles ändern.

*Gehen Sie folgendermaßen vor, um ein SCEP-Profil hinzuzufügen:*

1. Wählen Sie in der Konsolenstruktur im Ordner **Verwaltete Geräte** die Administrationsgruppe, zu der die iOS MDM-Geräte gehören.
2. Gehen Sie Im Arbeitsbereich der Gruppe auf die Registerkarte **Richtlinien**.
3. Öffnen Sie über Doppelklick das Eigenschaftfenster der Richtlinie.
4. Wählen Sie im Fenster **Eigenschaften <Name der Richtlinie>** den Abschnitt **SCEP**.
5. Klicken Sie im Abschnitt **SCEP-Profil** auf **Hinzufügen**.

Es öffnet sich das Fenster **SCEP-Profil**.

6. Geben Sie im Feld **Webadresse des Servers** die Webadresse des SCEP-Servers ein, auf dem das Zertifizierungszentrum verteilt wurde.

Die Webadresse kann eine IP-Adresse oder den vollständigen Domainnamen (FQDN) enthalten. Beispielsweise, <http://10.10.10.10/certserver/companyscep>.

7. Geben Sie im Feld **Name** den Namen des Zertifizierungszentrums ein, das sich auf dem SCEP-Server befindet.

8. Geben Sie im Feld **Schlüsselkennung des Antragstellers** die Zeile mit den Attributen des Nutzers eines iOS MDM-Geräts aus dem X.500-Zertifikat ein.

Die Attribute können Angaben zum Land (C), Unternehmen (O) und dem allgemeinen Benutzernamen (CN) enthalten. Beispielsweise, /C=RU/O=MyCompany/CN=User/. Sie können auch andere Attribute, die in RFC 5280 verzeichnet sind, verwenden.

9. Wählen Sie in der Dropdown-Liste **Typ des alternativen Namens des Antragstellers** den Typ des alternativen Namens des SCEP-Serverinhabers:

- **Nein** – die Identifizierung mithilfe des alternativen Namens wird nicht verwendet.
- **RFC 822-Name** – Identifizierung mithilfe der E-Mail-Adresse. Die E-Mail-Adresse muss gemäß RFC 822 angegeben werden.
- **DNS-Name** – Identifizierung mithilfe des Domain-Namens.
- **URI** – Identifizierung mithilfe der IP-Adresse oder Adresse im FQDN-Format.

Sie können den alternativen Namen des Inhabers für die Identifizierung des Nutzers des iOS MDM-Mobilgeräts verwenden.

10. Geben Sie im Feld **Alternativer Name des Antragstellers** den alternativen Namen des X.500-Zertifikatinhabers ein. Der Wert des alternativen Namens des Inhabers hängt von seinem Typ ab: E-Mail-Adresse des Benutzers, Domain oder Webadresse.

11. Geben Sie im Feld **Name des NT-Antragstellers** den DNS-Benutzernamen des Nutzers des iOS MDM-Mobilgeräts im Windows NT-Netzwerk ein.

Der Name des NT-Antragstellers ist in der Anfrage für das Zertifikat an den SCEP-Server enthalten.

12. Geben Sie im Feld **Anzahl der Versuche für SCEP-Serverabfragen** die maximale Anzahl der Versuche für SCEP-Serverabfragen für die Signatur des Zertifikats ein.

13. Legen Sie im Feld **Intervall für Versuche (Sekunden)** den Zeitraum und die Uhrzeit in Sekunden zwischen den Versuchen für SCEP-Serverabfragen für die Signatur des Zertifikats fest.

14. Geben Sie im Feld **Registrierungsanfrage** den im Voraus veröffentlichten Registrierungsschlüssel ein.

Vor der Signatur des Zertifikats fragt der SCEP-Server den Mobilgerätenutzer nach dem Schlüssel. Wenn das Eingabefeld leer gelassen wird, fragt der SCEP-Server nicht nach dem Schlüssel.

15. Wählen Sie in der Dropdown-Liste **Schlüssellänge** die Länge des Registrierungsschlüssels in Bit aus: 1024 oder 2048.

16. Wenn Sie dem Benutzer die Verwendung eines vom SCEP-Server erhaltenen Schlüssels als Signaturzertifikat erlauben möchten, aktivieren Sie das Kontrollkästchen **Als digitale Signatur verwenden**.

17. Wenn Sie dem Benutzer die Verwendung eines vom SCEP-Server erhaltenen Schlüssels für die Datenverschlüsselung erlauben möchten, aktivieren Sie das Kontrollkästchen **Zur Verschlüsselung verwenden**.

Es ist verboten, das Zertifikat des SCEP-Servers als Signaturzertifikat und Verschlüsselungszertifikat gleichzeitig zu verwenden.

18. Geben Sie im Feld **Zertifikatfingerabdruck** den einzigartigen Fingerabdruck des Zertifikats für die Authentifizierung der Antwort vom Zertifizierungszentrum ein. Sie können Zertifikatfingerabdrücke mit dem Hashalgorithmus SHA-1 oder MD5 verwenden. Sie können den Zertifikatfingerabdruck manuell kopieren oder ein



Zertifikat mithilfe der Schaltfläche **Aus Zertifikat erstellen** wählen. Beim Erstellen des Fingerabdrucks mithilfe der Schaltfläche **Aus Zertifikat erstellen** wird der Fingerabdruck automatisch in das Feld eingefügt.

Der Zertifikatfingerabdruck muss angegeben werden, wenn die Datenübertragung zwischen dem Mobilgerät und dem Zertifizierungszentrum über das HTTP-Protokoll erfolgt.

19. Klicken Sie auf **OK**.

Das neue SCEP-Profil wird in der Liste angezeigt.

20. Klicken Sie auf **Anwenden**, um die vorgenommenen Änderungen zu speichern.

Nach dem Anwenden der Richtlinie wird das mobile Gerät so konfiguriert, dass es automatisch über das Internet ein Zertifikat aus dem Zertifizierungszentrum abrufen.

## Kontrolle

Dieser Abschnitt enthält Informationen darüber, wie mobile Geräte ferngesteuert in der Administrationskonsole von Kaspersky Security Center kontrolliert werden.

## Beschränkungen konfigurieren

Dieser Abschnitt enthält Anweisungen zur Konfiguration des Benutzerzugriffs auf die Funktionen der mobilen Geräte.

### Besonderheiten für Geräte unter Android Version 10 und später

In Android 10 wurden viele Änderungen und Einschränkungen im Hinblick auf API 29 oder höher eingeführt. Einige dieser Änderungen betreffen die Verfügbarkeit und Funktion einiger Funktionen dieser App. Diese Besonderheiten gelten nur für Geräte, die unter Android 10 oder später laufen.

### Fähigkeit zur Aktivierung, Deaktivierung und Konfiguration von WLAN

- WLAN-Netzwerke können in der Verwaltungskonsolle von Kaspersky Security Center hinzugefügt, gelöscht und konfiguriert werden. Wenn ein WLAN-Netzwerk zu einer Richtlinie hinzugefügt wird, empfängt Kaspersky Endpoint Security diese Netzwerkkonfiguration bei der ersten Verbindung mit Kaspersky Security Center.
- Wenn ein Gerät ein Netzwerk erkennt, das durch Kaspersky Security Center konfiguriert wurde, fordert Kaspersky Endpoint Security den Benutzer auf, eine Verbindung mit diesem Netzwerk herzustellen. Wenn sich der Benutzer entscheidet, eine Verbindung zum Netzwerk herzustellen, werden alle über Kaspersky Security Center konfigurierten Einstellungen automatisch übernommen. Das Gerät stellt sodann eine Verbindung mit diesem Netzwerk her, wenn es in dessen Empfangsbereich ist, ohne den Benutzer weiter zu benachrichtigen.
- Falls ein Benutzergerät bereits mit einem anderen WLAN-Netzwerk verbunden ist, wird der Benutzer manchmal möglicherweise nicht aufgefordert, eine Netzwerkerweiterung zu genehmigen. In solchen Fällen muss der Benutzer das WLAN aus- und wieder einschalten, um den Vorschlag zu erhalten.

- Wenn Kaspersky Endpoint Security einem Benutzer vorschlägt, eine Verbindung mit einem WLAN-Netzwerk herzustellen und der Benutzer dies ablehnt, wird die Berechtigung der App zum Ändern des WLAN-Status widerrufen. Kaspersky Endpoint Security kann dann nicht vorschlagen, eine Verbindung mit WLAN-Netzwerken herzustellen, solange der Benutzer nicht wieder die Berechtigung dazu erteilt, indem er auf **Einstellungen** → **Apps & Benachrichtigungen** → **Spezieller App-Zugriff** → **WLAN-Steuerung** → **Kaspersky Endpoint Security** wechselt.
- Nur offene Netzwerke und mittels WPA2-PSK verschlüsselte Netzwerke werden unterstützt. WEP- und WPA-Verschlüsselung wird nicht unterstützt.
- Wenn das Kennwort für ein zuvor von der App vorgeschlagenes Netzwerk geändert wird, muss der Benutzer dieses Netzwerk händisch aus der Liste der bekannten Netzwerke löschen. Das Gerät ist dann in der Lage, einen Netzwerkvorschlag von Kaspersky Endpoint Security zu empfangen und eine Verbindung herzustellen.
- Wenn ein Gerätebetriebssystem von Android Version 9 oder früher auf Android Version 10 oder später aktualisiert wird und/oder Kaspersky Endpoint Security auf einem unter Android Version 10 oder später laufenden Gerät aktualisiert wird, können die zuvor über Kaspersky Security Center hinzugefügten Netzwerke nicht über Richtlinien von Kaspersky Security Center modifiziert oder gelöscht werden. Der Benutzer kann jedoch solche Netzwerke in den Geräteeinstellungen manuell modifizieren oder löschen.
- Auf Geräten unter Android 10 wird ein Benutzer zur Eingabe des Kennworts aufgefordert, wenn er versucht, manuell eine Verbindung zu einem geschützten vorgeschlagenen Netzwerk herzustellen. Bei einer automatischen Verbindung muss kein Kennwort eingegeben werden. Falls ein Benutzergerät mit einem anderen WLAN-Netzwerk verbunden ist, muss der Benutzer zuerst die Verbindung zu diesem Netzwerk trennen, um sich automatisch mit einem der vorgeschlagenen Netzwerke verbinden zu können.
- Auf Geräten unter Android 11 kann ein Benutzer ohne Eingabe des Kennworts manuell eine Verbindung mit einem geschützten Netzwerk herstellen, das von der App vorgeschlagen wurde.
- Wenn Kaspersky Endpoint Security von einem Gerät deinstalliert wird, werden die zuvor von der App vorgeschlagenen Netzwerke ignoriert.
- Das Verbot der Verwendung von WLAN-Netzwerken wird nicht unterstützt.

## Kamerazugriff

- Auf Geräten unter Android 10 kann die Nutzung der Kamera nicht vollständig verboten werden. Das Verbot der Kameranutzung für das Arbeitsprofil ist nach wie vor möglich.
- Wenn eine Drittanbieter-App versucht, auf die Kamera des Geräts zuzugreifen, wird diese App blockiert und der Benutzer wird über das Problem benachrichtigt. Apps, die die Kamera verwenden, während sie im Hintergrund ausgeführt werden, können jedoch nicht blockiert werden.
- Wenn eine externe Kamera von einem Gerät getrennt wird, wird in einigen Fällen möglicherweise eine Benachrichtigung angezeigt, dass die Kamera nicht verfügbar ist.

## Bildschirmensperrverfahren verwalten

- Kaspersky Endpoint Security löst die Anforderungen an die Zuverlässigkeit des Kennworts jetzt in einen der Systemwerte auf: Mittel oder Hoch.
  - Wenn eine Kennwortlänge von 1 bis 4 Zeichen erforderlich ist, fordert die App den Benutzer auf, ein Kennwort mittlerer Stärke festzulegen. Dieses muss entweder numerisch (PIN) ohne wiederholte oder aufeinanderfolgende (z. B. 1234) Sequenzen oder alphanumerisch sein. PIN oder Kennwort müssen mindestens 4 Zeichen lang sein.

- Wenn eine Kennwortlänge von 5 oder mehr Zeichen erforderlich ist, fordert die App den Benutzer auf, ein Kennwort hoher Stärke festzulegen. Dieses muss entweder numerisch (PIN) ohne wiederholte oder aufeinanderfolgende Sequenzen oder alphanumerisch (Kennwort) sein. Die PIN muss mindestens 8 Zeichen lang sein, das Kennwort muss mindestens 6 Zeichen lang sein.
- Die Verwendung des Fingerabdrucks zum Entsperren des Bildschirms kann nur für das Arbeitsprofil verwaltet werden.

## Beschränkungen für Android-Geräte anpassen

Zur Gewährleistung der Sicherheit des Android-Geräts müssen die Einstellungen für die Verwendung der Funktionen Kamera, WLAN und Bluetooth auf dem Gerät angepasst werden.

Standardmäßig darf der Benutzer auf dem Geräte die Kamera, WLAN und Bluetooth ohne Beschränkungen verwenden.

*Um die Beschränkung der Verwendung der Funktionen Kamera, WLAN und Bluetooth auf dem Gerät anzupassen, gehen Sie wie folgt vor:*

1. Wählen Sie in der Konsolenstruktur im Ordner **Verwaltete Geräte** die Administrationsgruppe, zu der die Android-Geräte gehören.
2. Gehen Sie im Arbeitsbereich der Gruppe auf die Registerkarte **Richtlinien**.
3. Öffnen Sie über Doppelklick auf eine beliebige Spalte das Eigenschaftfenster der Richtlinie.
4. Wählen Sie im Fenster **Eigenschaften <Name der Richtlinie>** den Abschnitt **Geräteverwaltung**.
5. Passen Sie im Block **Beschränkungen** die Verwendung von WLAN, Kamera und Bluetooth an:
  - Um das WLAN-Modul auf dem mobilen Gerät des Benutzers auszuschalten, aktivieren Sie das Kontrollkästchen **Verwendung von WLAN verbieten**.

Auf Geräten mit Android 10.0 oder höher wird das Verbot der Verwendung von WLAN-Netzwerken nicht unterstützt.

- Um die Kamera auf dem mobilen Gerät des Benutzers auszuschalten, aktivieren Sie das Kontrollkästchen **Kameraverwendung verbieten**.

Auf Geräten mit Android 10.0 oder höher kann die Nutzung der Kamera nicht vollständig verboten werden.

Auf Geräten mit dem Betriebssystem Android 11 und höher muss Kaspersky Endpoint Security für Android als Dienst für erleichterte Bedienung installiert sein. Der Assistent für die Erstkonfiguration von Kaspersky Endpoint Security für Android ermöglicht dem Benutzer, die App als Bedienungshilfe zu installieren. Der Benutzer kann diesen Schritt überspringen oder den Dienst in den Einstellungen des Geräts später deaktivieren. In einem solchen Fall können Sie die Verwendung der Kamera nicht einschränken.

- Um Bluetooth auf dem mobilen Gerät des Benutzers auszuschalten, aktivieren Sie das Kontrollkästchen **Bluetooth verbieten**.

Auf Android 12 oder höher kann die Verwendung von Bluetooth nur deaktiviert werden, wenn der Gerätebenutzer die Berechtigung **Bluetooth-Geräte in der Nähe** gewährt hat. Der Benutzer kann diese Berechtigung beim Ausführen des Schnellstartassistenten oder später gewähren.

6. Klicken Sie auf **Anwenden**, um die vorgenommenen Änderungen zu speichern.

Die Einstellungen werden nach der nächsten planmäßigen Synchronisierung des Geräts mit Kaspersky Security Center auf dem mobilen Gerät konfiguriert.

## Beschränkungen für iOS MDM-Geräte anpassen

Für die Einhaltung der Sicherheitsbestimmungen des Unternehmens müssen Beschränkungen für das iOS MDM-Gerät festgelegt werden.

*Um die Beschränkungen für das iOS MDM-Gerät anzupassen, gehen Sie wie folgt vor:*

1. Wählen Sie in der Konsolenstruktur im Ordner **Verwaltete Geräte** die Administrationsgruppe, zu der die iOS MDM-Geräte gehören.
2. Gehen Sie Im Arbeitsbereich der Gruppe auf die Registerkarte **Richtlinien**.
3. Öffnen Sie über Doppelklick das Eigenschaftfenster der Richtlinie.
4. Wählen Sie im Fenster **Eigenschaften <Name der Richtlinie>** den Abschnitt **Funktionsbeschränkungen**.
5. Aktivieren Sie im Block **Einstellungen für Funktionsbeschränkungen** das Kontrollkästchen **Einstellungen auf dem Gerät anwenden**.
6. Passen Sie die Beschränkungen für iOS MDM-Geräte an.
7. Klicken Sie auf **Anwenden**, um die vorgenommenen Änderungen zu speichern.
8. Wählen Sie den Abschnitt **App-Beschränkungen**.
9. Aktivieren Sie im Block **Einstellungen für App-Beschränkungen** das Kontrollkästchen **Einstellungen auf dem Gerät anwenden**.
10. Passen Sie die App-Beschränkungen für iOS MDM-Geräte an.
11. Klicken Sie auf **Anwenden**, um die vorgenommenen Änderungen zu speichern.
12. Wählen Sie den Abschnitt **Beschränkungen für Medieninhalte**.
13. Aktivieren Sie im Block **Einstellungen für Beschränkungen für Medieninhalte** das Kontrollkästchen **Einstellungen auf dem Gerät anwenden**.
14. Passen Sie die Beschränkungen für Medieninhalte für iOS MDM-Geräte an.
15. Klicken Sie auf **Anwenden**, um die vorgenommenen Änderungen zu speichern.

Nach dem Anwenden der Richtlinie werden auf dem Mobilgerät die Beschränkungen für Funktionen, Anwendungen und Medieninhalte angepasst werden.

## Funktionsbeschränkungen für EAS-Geräte konfigurieren

Zur Sicherstellung der Sicherheit des EAS-Geräts müssen die Funktionsbeschränkungen des Geräts angepasst werden.

Standardmäßig darf der Benutzer die Funktionen des EAS-Geräts unbeschränkt nutzen.

*Um die Funktionsbeschränkungen auf den EAS-Geräten anzupassen, gehen Sie wie folgt vor:*

1. Wählen Sie in der Konsolenstruktur im Ordner **Verwaltete Geräte** die Administrationsgruppe, zu der die EAS-Geräte gehören.
2. Gehen Sie Im Arbeitsbereich der Gruppe auf die Registerkarte **Richtlinien**.
3. Öffnen Sie über Doppelklick das Eigenschaftfenster der Richtlinie.
4. Wählen Sie im Fenster Eigenschaften <Name der Richtlinie> den Abschnitt **Funktionsbeschränkungen**.
5. Erlauben oder verbieten Sie im Block **Einstellungen für Funktionsbeschränkungen** die Nutzung der Funktionen des EAS-Geräts:
  - Um den Anschluss von Speicherkarten und anderen Wechseldatenträger an das Gerät zu erlauben, aktivieren Sie das Kontrollkästchen **Wechselmedien erlauben**.
  - Um die Verwendung der Kamera zu erlauben, aktivieren Sie das Kontrollkästchen **Kameraverwendung erlauben**.
  - Um WLAN-Verbindungen zu erlauben, aktivieren Sie das Kontrollkästchen **WLAN-Verwendung erlauben**.
  - Um die Verwendung des Infrarotanschlusses zu erlauben, aktivieren Sie das Kontrollkästchen **Infrarotverbindung erlauben**.
  - Um die Verwendung des Geräts als WLAN-Zugriffspunkt für die Herstellung eines kabellosen Netzwerks zu erlauben, aktivieren Sie das Kontrollkästchen **Verwendung des Geräts als Wi-Fi-Zugriffspunkt erlauben**.
  - Um eine Verbindung vom Gerät zu einem Remotedesktop zu erlauben, aktivieren Sie das Kontrollkästchen **Verbindung des Geräts mit Remote Desktop erlauben**.
  - Um auf dem Gerät einen ActiveSync Client-Desktop zu verwenden, aktivieren Sie das Kontrollkästchen **Synchronisierung des Schreibtischs erlauben**.
  - Erlauben oder verbieten Sie **Bluetooth verwenden** die Verwendung von Bluetooth auf dem EAS-Gerät:
    - **Erlauben**. Die Verwendung von Bluetooth auf dem Mobilgerät des Nutzers ist erlaubt.
    - **Bei drahtloser Verbindung**. Die Verwendung von Bluetooth ist erlaubt, wenn das Mobilgerät an ein kabelloses Netzwerk angeschlossen ist.
    - **Verbieten**. Die Verwendung von Bluetooth auf dem Mobilgerät des Nutzers ist verboten.
6. Klicken Sie auf **Anwenden**, um die vorgenommenen Änderungen zu speichern.

Die Einstellungen werden nach der nächsten planmäßigen Synchronisierung des Geräts mit Kaspersky Security Center auf dem mobilen Gerät konfiguriert.

## Benutzerzugriff auf Websites anpassen

Dieser Abschnitt enthält Anweisungen zur Konfiguration des Zugriffs auf Websites auf Android- und iOS-Geräten.

### Zugriff auf Websites auf Android-Geräten konfigurieren

Der Zugriff der Benutzer von Android-Geräten auf Websites kann mithilfe von Web-Filter konfiguriert werden. Der Web-Filter unterstützt die Filterung von Websites nach Kategorien, die im Cloud-Dienst [Kaspersky Security Network](#) festgelegt sind. Die Filterung ermöglicht Ihnen, den Zugriff der Benutzer auf einzelne Websites oder bestimmte Website-Kategorien einzuschränken (z. B. auf Websites aus der Kategorie "Glücksspiel, Lotterien, Wetten" oder "Kommunikation im Internet"). Web-Filter schützt außerdem die persönlichen Daten der Benutzer im Internet.

Kaspersky Endpoint Security für Android muss als Dienst für erleichterte Bedienung installiert werden. Der Assistent für die Erstkonfiguration von Kaspersky Endpoint Security für Android ermöglicht dem Benutzer, die App als Bedienungshilfe zu installieren. Der Benutzer kann diesen Schritt überspringen oder den Dienst in den Einstellungen des Geräts später deaktivieren. In diesem Fall wird der Web-Filter nicht ausgeführt.


Der Web-Filter funktioniert auf Android-Geräten nur mit den Browsern Google Chrome (einschließlich der Funktion Custom Tabs), Huawei Browser und Samsung Internet Browser. Web-Filter für Samsung Internet Browser blockiert keine Websites auf mobilen Geräten, wenn ein Arbeitsprofil verwendet wird und [Web-Filter nur für das Arbeitsprofil aktiviert ist](#).

Standardmäßig ist der Web-Filter eingeschaltet: der Zugriff auf Websites der Kategorien **Phishing** und **Schadsoftware** ist eingeschränkt.

*Um den Zugriff des Benutzers auf Websites anzupassen, gehen Sie wie folgt vor:*

1. Wählen Sie in der Konsolenstruktur im Ordner **Verwaltete Geräte** die Administrationsgruppe, zu der die Android-Geräte gehören.
2. Gehen Sie im Arbeitsbereich der Gruppe auf die Registerkarte **Richtlinien**.
3. Öffnen Sie über Doppelklick auf eine beliebige Spalte das Eigenschaftenfenster der Richtlinie.
4. Wählen Sie im Fenster **Eigenschaften** der Richtlinie die Option **Web-Filter**.
5. Aktivieren Sie das Kontrollkästchen **Web-Filter aktivieren**.
6. Um Web-Filter zu verwenden, müssen Sie oder der Gerätebenutzer die Erklärung zur Verarbeitung von Daten für die Verwendung von Web-Filter (Erklärung für Web-Filter) akzeptieren:
  - a. Klicken Sie auf den Link **Erklärung für Web-Filter**.

Die **Erklärung zur Verarbeitung von Daten für die Verwendung von Web-Filter** wird geöffnet. Um die Erklärung für Web-Filter zu akzeptieren, müssen Sie die Datenschutzrichtlinie lesen und akzeptieren.
  - b. Klicken Sie auf den Link "Datenschutzrichtlinie". Lesen und akzeptieren Sie die Datenschutzrichtlinie.

Wenn Sie die Datenschutzrichtlinie nicht akzeptieren, kann der Benutzer des mobilen Geräts die Datenschutzrichtlinie im Assistenten für die Erstkonfiguration oder in der App akzeptieren ( → **Über die App** → **Nutzungsbedingungen** → **Datenschutzrichtlinie**).

c. Wählen Sie den Modus für die Annahme der Erklärung für Web-Filter:

- **Ich habe die Erklärung für Web-Filter gelesen und akzeptiere sie**
- **Gerätebenutzer zur Annahme der Erklärung für Web-Filter auffordern**
- **Ich lehne die Erklärung für Web-Filter ab**

Wenn Sie die Option **Ich lehne die Erklärung für Web-Filter ab** auswählen, blockiert der Web-Filter keine Websites auf mobilen Geräten. Die Benutzer von mobilen Geräten können den Web-Filter nicht in Kaspersky Endpoint Security aktivieren.

7. Wenn Sie möchten, dass die Anwendung den Zugriff des Benutzers auf Websites abhängig von deren Inhalten blockiert, gehen Sie folgendermaßen vor:

- Wählen Sie im Block **Web-Filter** in der Dropdown-Liste den Punkt **Websites der ausgewählten Kategorien sind verboten**.
- Erstellen Sie eine Liste mit verbotenen Kategorien, indem Sie die Kontrollkästchen der Kategorien von Websites aktivieren, auf die die App den Zugriff blockieren soll.

8. Wenn Sie möchten, dass die Anwendung den Zugriff des Benutzers nur auf Websites freigibt, die vom Administrator festgelegt wurden, gehen Sie folgendermaßen vor:

- Wählen Sie im Block **Web-Filter** in der Dropdown-Liste den Punkt **Nur aufgezählte Websites sind erlaubt**.
- Erstellen Sie eine Liste der Websites, indem Sie Adressen von Websites hinzufügen, auf die die App den Zugriff nicht beschränken soll. Kaspersky Endpoint Security für Android unterstützt nur reguläre Ausdrücke. Geben Sie die Adresse der erlaubten Website nach einem der folgenden Muster ein:

- `http://www.example.com.*` – alle untergeordneten Seiten der Website (beispielsweise `http://www.example.com/about`) sind erlaubt.
- `https://.*example.com` – alle Subdomains der Website (beispielsweise `https://pictures.example.com`) sind erlaubt.

Sie können auch den Ausdruck `https?` verwenden, um die Protokolle HTTP und HTTPS auszuwählen. Weitere Informationen über reguläre Ausdrücke finden Sie auf der Seite [des technischen Supports von Oracle](#).

9. Wenn Sie möchten, dass die App den Zugriff des Benutzers auf alle Websites blockiert, wählen Sie im Block **Web-Filter** in der Dropdown-Liste das Element **Alle Websites sind verboten**.

10. Wenn der Zugriff auf Webseiten nicht in Abhängigkeit der Inhalte beschränkt werden soll, deaktivieren Sie das Kontrollkästchen **Web-Filter aktivieren**.

11. Klicken Sie auf **Anwenden**, um die vorgenommenen Änderungen zu speichern.

Die Einstellungen werden nach der nächsten planmäßigen Synchronisierung des Geräts mit Kaspersky Security Center auf dem mobilen Gerät konfiguriert.

## Zugriff auf Websites auf iOS MDM-Geräten konfigurieren

Damit der Zugriff eines Benutzers auf Websites über ein iOS MDM-Gerät kontrolliert werden kann, müssen die Einstellungen von Web-Filter angepasst werden. Der Web-Filter kontrolliert den Zugriff des Benutzers auf Websites auf der Grundlage der Listen von erlaubten und verbotenen Websites. Ferner ermöglicht der Web-Filter das Hinzufügen von Lesezeichen für Websites in die Lesezeichenleiste von Safari.

Standardmäßig ist der Zugriff auf Websites nicht beschränkt.

Die Einstellungen für Web-Filter können nur auf kontrollierten Geräten angepasst werden.

*Um den Zugriff auf Websites auf dem iOS MDM-Gerät anzupassen, gehen Sie wie folgt vor:*

1. Wählen Sie in der Konsolenstruktur im Ordner **Verwaltete Geräte** die Administrationsgruppe, zu der die iOS MDM-Geräte gehören.
2. Gehen Sie Im Arbeitsbereich der Gruppe auf die Registerkarte **Richtlinien**.
3. Öffnen Sie über Doppelklick das Eigenschaftfenster der Richtlinie.
4. Wählen Sie im Fenster **Eigenschaften <Name der Richtlinie>** den Abschnitt **Web-Filter**.
5. Aktivieren Sie im Block **Web-Filter-Einstellungen** das Kontrollkästchen **Einstellungen auf dem Gerät anwenden**.
6. Um den Zugriff auf verbotene Websites zu blockieren und den Zugriff auf erlaubte Websites zu erlauben, gehen Sie wie folgt vor:
  - a. Wählen Sie in der Dropdown-Liste **Filtermodus für Websites** den Modus **Inhalte für Erwachsene beschränken**.
  - b. Erstellen Sie im Block **Erlaubte Websites** die Liste der erlaubten Websites.

Die Adresse der Website muss mit "http://" oder "https://" beginnen. Kaspersky Device Management für iOS stellt den Zugriff auf alle Websites der Domain bereit. Wenn Sie zur Liste der erlaubten Websites beispielsweise http://www.example.com hinzugefügt haben, ist der Zugriff auf http://pictures.example.com und http://example.com/movies erlaubt. Wenn die Liste der zugelassenen Websites leer ist, erlaubt die Anwendung den Zugriff auf alle Websites, außer denen in der Liste der verbotenen Websites.
  - c. Erstellen Sie im Block **Verbotene Websites** die Liste der verbotenen Websites.

Die Adresse der Website muss mit "http://" oder "https://" beginnen. Kaspersky Device Management für iOS verbietet den Zugriff auf alle Websites der Domain.
7. Um den Zugriff auf alle Websites außer den erlaubten aus der Lesezeichenliste zu blockieren, gehen Sie wie folgt vor:
  - a. Wählen Sie in der Dropdown-Liste **Filtermodus für Websites** den Modus **Nur Websites aus der Lesezeichenliste erlauben**.
  - b. Erstellen Sie im Block **Registerkarten** die Liste mit den Lesezeichen der erlaubten Websites.



Die Adresse der Website muss mit "http://" oder "https://" beginnen. Kaspersky Device Management für iOS stellt den Zugriff auf alle Websites der Domain bereit. Wenn die Lesezeichenliste leer ist, erlaubt die Anwendung den Zugriff auf alle Websites. Kaspersky Device Management für iOS fügt Websites aus der Lesezeichenliste in die Lesezeichenleiste von Safari auf dem mobilen Gerät des Nutzers hinzu.

8. Klicken Sie auf **Anwenden**, um die vorgenommenen Änderungen zu speichern.

Nach dem Anwenden der Richtlinie wird auf dem Mobilgerät des Nutzers die Filterung der Websites gemäß dem ausgewählten Modus und den erstellten Listen angepasst.

## Übereinstimmungsüberprüfung für Android-Geräte hinsichtlich der korporativen Sicherheit

Sie können Android-Geräte auf die Einhaltung der Anforderungen der korporativen Sicherheit überwachen. Die Anforderungen der korporativen Sicherheit regeln die Arbeit der Benutzer mit den Geräten. Auf dem Gerät muss beispielsweise der Echtzeitschutz, aktiviert sein, die Antiviren-Datenbanken müssen aktuell sein und das Kennwort des Geräts muss hinreichend komplex sein. Die Übereinstimmungsüberprüfung funktioniert auf der Grundlage einer Liste von Regeln. Eine Übereinstimmungsregel besteht aus folgenden Komponenten:

- Kriterien zur Untersuchung des Geräts (beispielsweise das Fehlen von verbotenen Apps auf dem Gerät).
- Zeitspanne, die dem Benutzer des Geräts zur Beseitigung von Abweichungen zur Verfügung steht (z. B 24 Stunden).
- Aktion, die für das Gerät ausgeführt wird, wenn der Benutzer Abweichungen nicht im Laufe der angegebenen Zeitspanne beseitigt (beispielsweise Sperre des Geräts).

Unter Android 12 oder höher führt die App diese Aufgabe möglicherweise später aus, wenn sich das Gerät im Stromsparmodus befindet.

Die folgenden Aktionen sind verfügbar, wenn der Benutzer die Abweichung innerhalb der angegebenen Zeit nicht beseitigt:

- **Sperre aller Apps mit Ausnahme der System-Apps.** Der Start aller Apps auf dem mobilen Gerät des Benutzers wird verboten, mit Ausnahme von System-Apps.
- **Gerät blockieren.** Das mobile Gerät ist blockiert. Um Zugriff auf die Daten zu erhalten, muss [das Gerät entsperrt werden](#). Wenn der Grund für die Sperrung nach der Entsperrung des Geräts nicht beseitigt wurde, wird das Gerät nach einem festgelegten Zeitraum wieder gesperrt.
- **Unternehmensdaten löschen.** Die Daten in Containern, das Benutzerkonto der Unternehmens-E-Mail, die Verbindungseinstellungen für das WLAN-Netzwerk, das VPN-Netz und den Zugriffspunkt (APN) des Unternehmens, das Arbeitsprofil Android, der KNOX-Container sowie der KNOX License Manager-Schlüssel werden gelöscht.
- **Auf Werkseinstellungen zurücksetzen.** Alle Daten wurden vom mobilen Gerät gelöscht, die Einstellungen des mobilen Geräts wurden auf Werkseinstellungen zurückgesetzt. Nach der Ausführung dieser Aktion wird das Gerät nicht länger verwaltet. Um das Gerät mit Kaspersky Security Center zu verbinden, muss [Kaspersky Endpoint Security für Android](#) erneut installiert werden.

*Um eine Untersuchungsregel zur Prüfung von Geräten auf Übereinstimmung mit der Gruppenrichtlinie zu erstellen, gehen Sie folgendermaßen vor:*

1. Wählen Sie in der Konsolenstruktur im Ordner **Verwaltete Geräte** die Administrationsgruppe, zu der die Android-Geräte gehören.
2. Gehen Sie Im Arbeitsbereich der Gruppe auf die Registerkarte **Richtlinien**.
3. Öffnen Sie über Doppelklick auf eine beliebige Spalte das Eigenschaftenfenster der Richtlinie.
4. Wählen Sie im Fenster **Eigenschaften** der Richtlinie den Abschnitt **Übereinstimmungsüberprüfung**.
5. Um Benachrichtigungen über Geräte zu erhalten, die nicht der Richtlinie entsprechen, aktivieren Sie im Block **Benachrichtigung bei Richtlinienverstoß** das Kontrollkästchen **Administrator benachrichtigen**.  
 Wenn ein Gerät nicht der Richtlinie entspricht, erstellt Kaspersky Endpoint Security für Android bei der Synchronisierung des Geräts mit dem Administrationsserver im Ereignisprotokoll den Eintrag **Ein Konflikt wurde erkannt: <Name des Überprüfungskriteriums>**. Das Ereignisprotokoll kann auf der Registerkarte **Ereignisse** in den Eigenschaften des Administrationsservers oder in den lokalen Eigenschaften des Programms angezeigt werden.
6. Um den Benutzer des Geräts davon zu benachrichtigen, dass Geräte erkannt wurden, die nicht der Richtlinie entsprechen, aktivieren Sie im Block **Benachrichtigung bei Richtlinienverstoß** das Kontrollkästchen **Benutzer benachrichtigen**.  
 Wenn ein Gerät nicht der Richtlinie entspricht, benachrichtigt Kaspersky Endpoint Security für Android bei der Synchronisierung des Geräts mit dem Administrationsserver den Benutzer darüber im Abschnitt **Status**.
7. Erstellen Sie im Block **Übereinstimmungsregeln** eine Liste der Überprüfungsregeln bzgl. der Einhaltung der Richtlinie. Gehen Sie dazu folgendermaßen vor:
  - a. Klicken Sie auf **Hinzufügen**.  
 Der Assistent für eine neue Überprüfungsregel wird gestartet.
  - b. Befolgen Sie die Anweisungen des Assistenten für eine neue Überprüfungsregel.  
 Nach Abschluss des Assistenten wird die neue Regel im Block **Übereinstimmungsregeln** in der Liste der Untersuchungsregeln angezeigt.
8. Um die Untersuchungsregel zeitweilig zu deaktivieren, benutzen Sie die Optionsschaltfläche neben der ausgewählten Regel.
9. Klicken Sie auf **Anwenden**, um die vorgenommenen Änderungen zu speichern.  
 Die Einstellungen werden nach der nächsten planmäßigen Synchronisierung des Geräts mit Kaspersky Security Center auf dem mobilen Gerät konfiguriert. Wenn das Gerät des Benutzers nicht den Regeln entspricht, werden die von Ihnen in der Liste der Untersuchungsregeln festgelegten Beschränkungen auf das Gerät angewendet.

## Kontrolle des App-Starts

Dieser Abschnitt enthält Anweisungen zur Konfiguration des Benutzerzugriffs auf die Apps auf den mobilen Geräten.

### Kontrolle des Starts von Apps auf Android-Geräten

Um die Sicherheit des mobilen Geräts des Benutzers sicherzustellen, müssen Sie die Einstellungen für den Start von Apps auf dem Gerät konfigurieren.

Sie können eine Beschränkung der Benutzertätigkeit auf einem Gerät festlegen, auf dem verbotene Anwendungen installiert sind oder benötigte Apps fehlen (z. B. Gerät sperren). Diese Beschränkung können Sie mithilfe der Komponente [Übereinstimmungsüberprüfung](#) definieren. Dazu muss in den Einstellungen der Untersuchungsregel die Option **Verbotene Apps wurden installiert, Apps aus verbotenen Kategorien sind installiert** oder **Nicht alle benötigten Apps sind installiert** ausgewählt werden.

Für die Ausführung der Anwendungskontrolle muss Kaspersky Endpoint Security für Android als Dienst für erleichterte Bedienung installiert sein. Der Assistent für die Erstkonfiguration von Kaspersky Endpoint Security für Android ermöglicht dem Benutzer, die App als Bedienungshilfe zu installieren. Der Benutzer kann diesen Schritt überspringen oder den Dienst in den Einstellungen des Geräts später deaktivieren. In diesem Fall wird die Anwendungskontrolle nicht ausgeführt.

*Gehen Sie folgendermaßen vor, um die Einstellungen für den Start von Anwendungen auf dem Mobilgerät anzupassen:*

1. Wählen Sie in der Konsolenstruktur im Ordner **Verwaltete Geräte** die Administrationsgruppe, zu der die Android-Geräte gehören.
2. Gehen Sie im Arbeitsbereich der Gruppe auf die Registerkarte **Richtlinien**.
3. Öffnen Sie über Doppelklick auf eine beliebige Spalte das Eigenschaftenfenster der Richtlinie.
4. Wählen Sie im Fenster **Eigenschaften <Name der Richtlinie>** den Abschnitt **Anwendungskontrolle**.
5. Wählen Sie im Block **Modus** den Modus für den Start von Anwendungen auf dem Mobilgerät:
  - Damit der Benutzer alle Apps mit Ausnahme der in der Liste der Kategorien und Apps als verboten festgelegten starten kann, wählen Sie den Modus **Verbotene Apps**.
  - Um dem Benutzer nur den Start der in der Liste der Kategorien und Apps als erlaubt, empfohlen oder obligatorisch festgelegten Apps zu erlauben, wählen Sie den Modus **Erlaubte Apps**.
6. Damit Kaspersky Endpoint Security für Android Daten über verbotene Anwendungen ins Ereignisprotokoll sendet, ohne sie zu blockieren, aktivieren Sie das Kontrollkästchen **Verbotene Apps nicht blockieren, nur im Ereignisprotokoll erfassen**.

Bei der nächsten Synchronisierung des mobilen Geräts mit dem Administrationsserver erstellt Kaspersky Endpoint Security für Android im Ereignisprotokoll den Eintrag **Verbotene App wurde installiert**. Das Ereignisprotokoll kann auf der Registerkarte **Ereignisse** in den Eigenschaften des Administrationsservers oder in den lokalen Eigenschaften des Programms angezeigt werden.
7. Damit Kaspersky Endpoint Security für Android den Start von Systemanwendungen auf dem mobilen Gerät im Modus **Erlaubte Apps** blockiert (z. B. Kalender, Kamera, Einstellungen), aktivieren Sie das Kontrollkästchen **System-Apps sperren**.

Die Experten Kaspersky empfehlen nicht, die Systemanwendungen zu sperren, da es zu den Störungen in der Arbeit des Geräts bringen kann.

8. Erstellen Sie eine Liste von Kategorien und Apps zur Konfiguration des Starts der Apps.

Ausführliche Informationen über die App-Kategorien finden Sie im [Anhang](#).

Eine Liste der Apps, die zur jeweiligen Kategorie gehören, finden Sie auf der [Website von Kaspersky](#).<sup>1</sup>
9. Klicken Sie auf **Anwenden**, um die vorgenommenen Änderungen zu speichern.

Die Einstellungen werden nach der nächsten planmäßigen Synchronisierung des Geräts mit Kaspersky Security Center auf dem mobilen Gerät konfiguriert.

## Einschränkungen der Apps für EAS-Geräte konfigurieren

Zur Gewährleistung der Sicherheit des EAS-Geräts müssen die Beschränkungen für Apps (Browser, nicht signierte Apps) angepasst werden.

Standardmäßig darf der Benutzer die Anwendungen des EAS-Geräts uneingeschränkt nutzen.

*Um die Beschränkungen für Anwendungen auf dem EAS-Gerät anzupassen, gehen Sie wie folgt vor:*

1. Wählen Sie in der Konsolenstruktur im Ordner **Verwaltete Geräte** die Administrationsgruppe, zu der die EAS-Geräte gehören.
2. Gehen Sie Im Arbeitsbereich der Gruppe auf die Registerkarte **Richtlinien**.
3. Öffnen Sie über Doppelklick das Eigenschaftfenster der Richtlinie.
4. Wählen Sie im Fenster Eigenschaften <Name der Richtlinie> den Abschnitt **App-Beschränkungen**.
5. Passen Sie im Block **Einstellungen für App-Beschränkungen** die Beschränkungen für Anwendungen an:
  - Um dem Benutzer die Verwendung eines Browsers zu erlauben, aktivieren Sie das Kontrollkästchen **Browserverwendung erlauben**.
  - Um dem Benutzer das Erstellen von persönlichen E-Mail-Konten (POP3 oder IMAP4) zu erlauben, aktivieren Sie das Kontrollkästchen **Eigene Mail erlauben**.
  - Um dem Benutzer den Start von nicht mit einem Echtheitszertifikat signierten Apps zu erlauben, aktivieren Sie das Kontrollkästchen **Unsignierte Apps erlauben**.
  - Um dem Benutzer die Installation von nicht mit einem Echtheitszertifikat signierten Apps zu erlauben, aktivieren Sie das Kontrollkästchen **Unsignierte Installationspakete erlauben**.
6. Klicken Sie auf **Anwenden**, um die vorgenommenen Änderungen zu speichern.

Die Einstellungen werden nach der nächsten planmäßigen Synchronisierung des Geräts mit Kaspersky Security Center auf dem mobilen Gerät konfiguriert.

## Inventarisierung der Software auf Android-Geräten

Sie können auf Android-Geräten, die mit Kaspersky Security Center verbunden sind, eine Inventarisierung der Apps vornehmen. Kaspersky Endpoint Security für Android erhält Informationen über alle Apps, die auf den mobilen Geräten installiert sind. Die bei der Inventarisierung erhobenen Informationen werden in den Eigenschaften des Geräts im Block **Ereignisse** angezeigt. Sie können ausführliche Informationen über jede installierte App einsehen, einschließlich Version und Hersteller.

*Um die Inventarisierung von Apps zu aktivieren, gehen Sie wie folgt vor:*

1. Wählen Sie in der Konsolenstruktur im Ordner **Verwaltete Geräte** die Administrationsgruppe, zu der die Android-Geräte gehören.
2. Gehen Sie Im Arbeitsbereich der Gruppe auf die Registerkarte **Richtlinien**.

3. Öffnen Sie über Doppelklick auf eine beliebige Spalte das Eigenschaftenfenster der Richtlinie.
4. Wählen Sie im Fenster **Eigenschaften <Name der Richtlinie>** den Abschnitt **Anwendungskontrolle**.
5. Aktivieren Sie im Block **Software-Inventur** das Kontrollkästchen **Daten über installierte Apps senden**.
6. Klicken Sie auf **Anwenden**, um die vorgenommenen Änderungen zu speichern.

Die Einstellungen werden nach der nächsten planmäßigen Synchronisierung des Geräts mit Kaspersky Security Center auf dem mobilen Gerät konfiguriert. Kaspersky Endpoint Security für Android sendet jedes Mal nach der Installation oder dem Löschen einer Anwendung vom Gerät die Daten ins Ereignisprotokoll.

## Einstellungen für die Anzeige von Android-Geräten in Kaspersky Security Center

Zur Erleichterung der Arbeit mit der Liste der mobilen Geräte ist es nötig, die Einstellungen zur Anzeige des Geräts in Kaspersky Security Center anzupassen. Standardmäßig wird die Liste der mobilen Geräte im Konsolenbaum **Erweitert** → **Mobile Geräte verwalten** → **Mobile Geräte** angezeigt. Die Informationen über das Gerät werden automatisch aktualisiert. Sie können die Liste der mobilen Geräte auch manuell über die Schaltfläche **Aktualisieren** in der rechten oberen Ecke aktualisieren.

Nach der Verbindung des Geräts mit Kaspersky Security Center werden Geräte automatisch zur Liste mit mobilen Geräten hinzugefügt. Die Liste mit mobilen Geräten kann ausführliche Informationen über dieses Gerät enthalten: Modell, Betriebssystem, IP-Adresse und andere.

Sie können das Format des Gerätenamens anpassen sowie den Status des Geräts auswählen. Der Gerätestatus informiert Sie über die Ausführung der Komponenten von Kaspersky Endpoint Security für Android auf dem mobilen Gerät des Benutzers.

Die Komponenten von Kaspersky Endpoint Security für Android können aus folgenden Gründen nicht ausgeführt werden:

- Der Benutzer hat die Komponente in den Geräteeinstellungen deaktiviert.
- Der Benutzer hat der App nicht die notwendigen Rechte für die Ausführung der Komponente gewährt (beispielsweise fehlt die Erlaubnis zur Standortbestimmung des Geräts für die Ausführung des entsprechenden Befehls des Diebstahlschutzes).

Für die Anzeige des Gerätestatus muss die Bedingung **Vom Programm bestimmt** in den Eigenschaften der Administrationsgruppe (**Eigenschaften** → **Gerätestatus** → **Bedingungen für den Gerätestatus "Kritisch"** und **Bedingungen für den Gerätestatus "Warnung"**) aktiviert werden. In den Eigenschaften der Administrationsgruppe können Sie auch andere Kriterien für das Festlegen des Status des mobilen Geräts auswählen.

*Um die Anzeige von Android-Geräten in Kaspersky Security Center anzupassen, gehen Sie wie folgt vor:*

1. Wählen Sie in der Konsolenstruktur im Ordner **Verwaltete Geräte** die Administrationsgruppe, zu der die Android-Geräte gehören.
2. Gehen Sie Im Arbeitsbereich der Gruppe auf die Registerkarte **Richtlinien**.
3. Öffnen Sie über Doppelklick auf eine beliebige Spalte das Eigenschaftenfenster der Richtlinie.

4. Wählen Sie im Fenster **Eigenschaften <Name der Richtlinie>** den Abschnitt **Geräteinformationen**.

5. Wählen Sie im Block **Geräte name in Kaspersky Security Center** das Format des Gerätenamens in der Verwaltungskonsole aus:

- Gerätemodell [E-Mail, Geräte-ID]
- Gerätemodell [E-Mail (falls vorhanden) oder Geräte-ID]

*Geräte-ID* ist eine eindeutige ID, die Kaspersky Endpoint Security für Android aus den vom Gerät empfangenen Daten generiert. Für mobile Geräte mit Android 10 und höher verwendet Kaspersky Endpoint Security für Android die SSAID (Android-ID) oder die Prüfsumme anderer vom Gerät empfangenen Daten. In früheren Android-Versionen verwendet die App die IMEI.

6. Bringen Sie das Attribut Schloss in die geschlossene Stellung (🔒).

7. Wählen Sie im Block **Gerätestatus in Kaspersky Security Center** den Status des Geräts aus, wenn die Komponente von Kaspersky Endpoint Security für Android nicht funktioniert: 🔴 (**Kritisch**), 🟡 (**Warnung**) oder 🟢 (**OK**).

In der Liste der mobilen Geräte wird der Status des Geräts entsprechend dem ausgewählten Status geändert.

8. Bringen Sie das Attribut Schloss in die geschlossene Stellung.

9. Klicken Sie auf **Anwenden**, um die vorgenommenen Änderungen zu speichern.

Die Einstellungen werden nach der nächsten planmäßigen Synchronisierung des Geräts mit Kaspersky Security Center auf dem mobilen Gerät konfiguriert.

## Verwaltung

Dieser Abschnitt enthält Informationen darüber, wie die Einstellungen der mobilen Geräte in der Administrationskonsole von Kaspersky Security Center ferngesteuert verwaltet werden.

## Verbindungseinstellungen für das WLAN-Netzwerk anpassen

Dieser Abschnitt enthält Anweisungen zur Einstellung der automatischen Verbindung mit dem WLAN-Unternehmensnetzwerk auf Android- und iOS MDM-Geräten.

### Android-Geräte mit einem WLAN-Netzwerk verbinden

*Gehen Sie folgendermaßen vor, um ein mobiles Gerät mit einem WLAN-Netzwerk zu verbinden:*

1. Wählen Sie in der Konsolenstruktur im Ordner **Verwaltete Geräte** die Administrationsgruppe, zu der die Android-Geräte gehören.
2. Gehen Sie im Arbeitsbereich der Gruppe auf die Registerkarte **Richtlinien**.
3. Öffnen Sie über Doppelklick auf eine beliebige Spalte das Eigenschaftenfenster der Richtlinie.
4. Wählen Sie im Fenster **Eigenschaften <Name der Richtlinie>** den Abschnitt **WLAN** aus.

5. Im Block **WLAN-Netzwerke** klicken Sie auf **Hinzufügen**.

Das Fenster **WLAN-Netzwerk** wird geöffnet.

6. Geben Sie im Feld **Netzwerk-SSID** den Namen des WLAN-Netzwerks mit dem Zugriffspunkt (SSID) an.

7. Wählen Sie im Block **Netzwerkschutz** den Sicherheitstyp des WLAN-Netzwerks (offenes oder über das WEP oder WPA/WPA2 PSK-Protokoll geschütztes Netzwerk).

8. Geben Sie im Feld **Kennwort** das Kennwort für den Zugang zum Netzwerk an, falls Sie im vorhergehenden Schritt ein geschütztes Netzwerk ausgewählt haben.

9. Geben Sie im Feld **Proxyserveradresse und Port** die IP-Adresse oder den DNS-Namen des Proxyservers und die Portnummer an (falls erforderlich).

Auf Geräten mit dem Betriebssystem Android Version 8.0 und höher können die Einstellungen des Proxyservers ein WLAN-Netzwerk nicht mithilfe der Richtlinie angepasst werden. Sie können die Proxyserver-Einstellungen für das WLAN-Netzwerk auf dem mobilen Gerät manuell anpassen.

Wenn Sie den Proxyserver für die Verbindung mit dem WLAN-Netzwerk verwenden, können Sie die Verbindungseinstellungen des Netzwerks mit Hilfe der Richtlinie anpassen. Die Proxyserver-Einstellungen auf Geräten mit Android 8.0 und höher müssen manuell angepasst werden. Die Verbindungseinstellungen des WLAN-Netzwerks können auf Geräten mit 8.0 und höher mit Ausnahme des Kennworts für den Netzwerkzugriff nicht mithilfe der Richtlinie geändert werden.

Wenn Sie keinen Proxyserver für die Verbindung mit dem WLAN-Netzwerk verwenden, ist Verwaltung der Verbindung mit dem WLAN-Netzwerk mithilfe der Richtlinien nicht beschränkt.

10. Erstellen Sie im Feld **Proxyserver für folgende Adressen nicht verwenden** eine Liste mit Webadressen, für die bei einer Verbindung kein Proxyserver verwendet werden soll.

Sie können beispielsweise die Adresse `example.com` angeben. In diesem Fall wird der Proxyserver nicht für die Adressen `pictures.example.com`, `example.com/movies` usw. verwendet. Das Protokoll (beispielsweise `http://`) kann weggelassen werden.

Auf Geräten mit dem Betriebssystem Android Version 8.0 und höher funktioniert die Ausnahme des Proxyservers für Webadressen nicht.

11. Klicken Sie auf **OK**.

Das hinzugefügte WLAN-Netzwerk wird in der Liste **WLAN-Netzwerke** angezeigt.

Sie können WLAN-Netzwerke in der Liste mithilfe der Schaltflächen **Ändern** und **Löschen** im oberen Bereich der Liste ändern und löschen.

12. Klicken Sie auf **Anwenden**, um die vorgenommenen Änderungen zu speichern.

Die Einstellungen werden nach der nächsten planmäßigen Synchronisierung des Geräts mit Kaspersky Security Center auf dem mobilen Gerät konfiguriert. Nach der Anwendung der Richtlinie auf dem mobilen Gerät kann sich der Benutzer beim hinzugefügten WLAN-Netzwerk anmelden, ohne die Netzwerkeinstellungen angeben zu müssen.

Auf Geräten unter Android Version 10.0 oder später wird die Berechtigung der App zum Ändern der WLAN-Status widerrufen, wenn der Benutzer sich weigert, eine Verbindung zum vorgeschlagenen WLAN-Netzwerk herzustellen. Der Benutzer muss diese Berechtigung händisch erteilen.

## iOS MDM-Geräte mit einem WLAN-Netzwerk verbinden

Für die automatische Verbindung des iOS MDM-Geräts mit einem verfügbaren WLAN-Netzwerk und zur Gewährleistung der Datensicherheit müssen die Verbindungseinstellungen angepasst werden.

*Um die Verbindung des iOS MDM-Geräts mit dem WLAN-Netzwerk anzupassen, gehen Sie wie folgt vor:*

1. Wählen Sie in der Konsolenstruktur im Ordner **Verwaltete Geräte** die Administrationsgruppe, zu der die iOS MDM-Geräte gehören.
2. Gehen Sie Im Arbeitsbereich der Gruppe auf die Registerkarte **Richtlinien**.
3. Öffnen Sie über Doppelklick das Eigenschaftfenster der Richtlinie.
4. Wählen Sie im Fenster **Eigenschaften <Name der Richtlinie>** den Abschnitt **WLAN** aus.

5. Klicken Sie im Block **WLAN-Netzwerke** auf **Hinzufügen**.

Das Fenster **WLAN-Netzwerk** wird geöffnet.

6. Geben Sie im Feld **Netzwerk-SSID** den Namen des WLAN-Netzwerks mit dem Zugriffspunkt (SSID) an.
7. Damit sich das iOS MDM-Gerät automatisch mit dem WLAN-Netzwerk verbindet, aktivieren Sie das Kontrollkästchen **Automatisches Verbinden**.
8. Damit keine Verbindung des iOS MDM-Geräts mit einem WLAN-Netzwerk möglich ist, das eine vorläufige Authentifizierung fordert (firmeneigenes Netzwerk), aktivieren Sie das Kontrollkästchen **Erkennen von Netzwerken mit Authentifizierung verbieten**.

Für die Nutzung des firmeneigenen Netzwerks muss ein Abonnement abgeschlossen, eine Vereinbarung übernommen oder ein Beitrag bezahlt werden. Firmeneigene Netzwerke sind beispielsweise in Cafés oder Hotels installiert.

9. Damit das WLAN-Netzwerk nicht in der Liste der verfügbaren Netzwerke auf dem iOS MDM-Gerät angezeigt wird, aktivieren Sie das Kontrollkästchen **Unsichtbares Netzwerk**.

Für die Verbindung mit dem Netzwerk muss in diesem Fall der Benutzer die in den Einstellungen des WLAN-Routers angegebene SSID-Netzwerk-ID auf dem Mobilgerät manuell eingeben.

10. Wählen Sie in der Dropdown-Liste **Netzwerkschutz** den Typ der Verbindung mit einem WLAN-Netzwerk:

- **Deaktiviert**. Die Authentifizierung des Benutzers ist nicht erforderlich.
- **WEP**. Das Netzwerk ist über das Verschlüsselungsprotokoll WEP (Wireless Encryption Protocol) geschützt.
- **WPA/WPA2 (persönlich)**. Das Netzwerk ist über das Verschlüsselungsprotokoll WPA / WPA2 (Wi-Fi Protected Access) geschützt.
- **WPA2 (persönlich)**. Das Netzwerk ist über das Verschlüsselungsprotokoll WPA / WPA2 (Wi-Fi Protected Access 2.0) geschützt. Der Schutztyp WPA2 ist auf Geräten mit dem Betriebssystem iOS Version 8 und höher verfügbar. WPA2 ist auf Apple TV-Geräten nicht verfügbar.



- **Beliebig (persönlich).** Das Netzwerk ist über das Verschlüsselungsprotokoll WEP, WPA oder WPA2 je nach Typ des WLAN-Routers geschützt. Für die Authentifizierung wird ein für jeden Benutzer individueller Verschlüsselungsschlüssel verwendet.
- **WEP (dynamisch).** Das Netzwerk ist über das Verschlüsselungsprotokoll WEP unter Verwendung eines dynamischen Schlüssels geschützt.
- **WPA/WPA2 (Unternehmen).** Das Netzwerk ist über das Verschlüsselungsprotokoll WPA/WPA2 unter Verwendung des Protokolls 802.1X geschützt.
- **WPA2 (Unternehmen).** Das Netzwerk ist über das Verschlüsselungsprotokoll WPA2 unter Verwendung eines Verschlüsselungsschlüssels für alle Benutzer geschützt (802.1X). Der Schutztyp WPA2 ist auf Geräten mit dem Betriebssystem iOS Version 8 und höher verfügbar. WPA2 ist auf Apple TV-Geräten nicht verfügbar.
- **Beliebig (Unternehmen).** Das Netzwerk ist über das Verschlüsselungsprotokoll WEP oder WPA / WPA2 je nach Typ des WLAN-Routers geschützt. Für die Authentifizierung wird ein Verschlüsselungsschlüssel für alle Benutzer verwendet.

Wenn Sie in der Liste **Netzwerkschutz** die Variante **WEP (dynamisch)**, **WPA/WPA2 (Unternehmen)**, **WPA/WPA2 (Unternehmen)** oder **Beliebig (Unternehmen)** ausgewählt haben, können Sie im Block **Protokolle** die Typen der EAP (Extensible Authentication Protocol) Protokolle für die Benutzeridentifizierung in einem WLAN-Netzwerk auswählen.

Weiterhin können Sie im Block **Vertrauenswürdige Zertifikate** die Liste der vertrauenswürdigen Zertifikate für die Authentifizierung des iOS MDM-Gerätbenutzers auf den vertrauenswürdigen Servern erstellen.

11. Passen Sie die Kontoeinstellungen für die Authentifizierung des Nutzers eines iOS MDM-Geräts beim Verbinden mit dem WLAN-Netzwerk an:

a. Klicken Sie im Block **Authentifizierung** auf **Anpassen**.

Das Fenster **Authentifizierung** wird geöffnet.

b. Geben Sie im Feld **Benutzername** den Kontonamen für die Authentifizierung beim Verbinden mit dem WLAN-Netzwerk ein.

c. Damit der Benutzer bei jeder Verbindung mit dem WLAN-Netzwerk das Kennwort manuell eingeben muss, aktivieren Sie das Kontrollkästchen **Kennwort erforderlich bei jeder Verbindung**.

d. Geben Sie im Feld **Kennwort** das Kennwort des Kontos für die Authentifizierung im WLAN-Netzwerk ein.

e. Wählen Sie in der Dropdown-Liste **Authentifizierungszertifikat** ein Zertifikat für die Authentifizierung des Benutzers im WLAN-Netzwerk. Wenn in der Liste die Zertifikate fehlen, können Sie diese **im Abschnitt [Zertifikate](#)** hinzufügen.

f. Geben Sie im Feld **Benutzer-ID** die Benutzer-ID ein, die während des Datentransfers bei der Authentifizierung statt des realen Benutzernamen angezeigt wird.

Die Benutzer-ID ist zum Erhöhen des Sicherheitsniveaus bei der Authentifizierung vorgesehen, da der Benutzername nicht offen, sondern in einem verschlüsselten TLS-Tunnel angezeigt wird.

g. Klicken Sie auf **OK**.

Auf dem iOS MDM-Gerät werden die Kontoeinstellungen für die Benutzer-Authentifizierung beim Verbinden mit einem WLAN-Netzwerk angepasst.

12. Bei Bedarf können Sie die Einstellungen für die Verbindung mit einem WLAN-Netzwerk über einen Proxyserver anpassen:

a. Klicken Sie unter **Proxy-Server** auf **Anpassen**.

b. Wählen Sie im Fenster **Proxy-Server** den Konfigurationsmodus für den und geben Sie die Verbindungseinstellungen ein.

c. Klicken Sie auf **OK**.

Auf dem iOS MDM-Gerät werden die Einstellungen für die Verbindung des Geräts mit einem WLAN-Netzwerk über den Proxyserver angepasst werden.

13. Klicken Sie auf **OK**.

Das neue WLAN-Netzwerk wird in der Liste angezeigt.

14. Klicken Sie auf **Anwenden**, um die vorgenommenen Änderungen zu speichern.

Nach dem Anwenden der Richtlinie wird auf dem iOS MDM-Gerät die Verbindung mit dem WLAN-Netzwerk angepasst werden. Das Mobilgerät des Nutzers wird sich automatisch mit dem verfügbaren WLAN-Netzwerk verbinden. Die Datensicherheit beim Verbinden mit einem WLAN-Netzwerk wird durch die Authentifizierungstechnologie gewährleistet.

## E-Mail anpassen

Dieser Abschnitt enthält Informationen über die Konfiguration der E-Mail-Postfächer auf mobilen Geräten.

### E-Mail-Postfach auf iOS MDM-Geräten konfigurieren

Damit der Nutzer eines iOS MDM-Geräts mit E-Mails arbeiten kann, muss der Benutzerkontenliste auf iOS MDM-Geräten ein E-Mail-Account hinzugefügt werden.

Standardmäßig wird ein E-Mail-Konto mit folgenden Parametern hinzugefügt:

- E-Mail-Protokoll – IMAP.
- Benutzer darf E-Mail-Nachrichten zwischen seinen Accounts verschieben und Adressen der Accounts synchronisieren.
- Für die Arbeit mit den E-Mails darf der Benutzer beliebige E-Mail-Clients (nicht nur Mail) verwenden.
- Bei der Übermittlung von E-Mails wird keine SSL-Verbindung verwendet.

Sie können die angegebenen Parameter beim Hinzufügen des Accounts ändern.

*Um einen E-Mail-Account des iOS MDM-Gerätnutzers hinzuzufügen, gehen Sie wie folgt vor:*

1. Wählen Sie in der Konsolenstruktur im Ordner **Verwaltete Geräte** die Administrationsgruppe, zu der die iOS MDM-Geräte gehören.
2. Gehen Sie Im Arbeitsbereich der Gruppe auf die Registerkarte **Richtlinien**.
3. Öffnen Sie über Doppelklick das Eigenschaftfenster der Richtlinie.
4. Wählen Sie im Fenster **Eigenschaften** der Richtlinie den Block **E-Mail**.

5. Klicken Sie im Block **E-Mail-Accounts** auf die Schaltfläche **Hinzufügen**.

Es öffnet sich das Fenster **E-Mail-Account**.

6. Geben Sie im Feld **Beschreibung** die Beschreibung des E-Mail-Kontos des Nutzers ein.

7. Wählen Sie ein E-Mail-Protokoll aus:

- **POP**
- **IMAP**

8. Geben Sie bei Bedarf den Präfix für den IMAP-Pfad im Feld **IMAP-Pfad-Präfix**.

Das IMAP-Pfad-Präfix muss groß geschrieben werden (beispielsweise, GMAIL für Google Mail). Dieses Feld ist verfügbar, wenn das Account-Protokoll IMAP ausgewählt wurde.


9. Geben Sie im Feld **Benutzername, der in Nachrichten angezeigt wird** den Benutzernamen ein, der im Feld **Von:** für alle ausgehenden E-Mails angezeigt wird.

10. Geben Sie im Feld **E-Mail-Adresse** die E Mail Adresse des Nutzers eines iOS MDM-Geräts.

11. Passen Sie die erweiterten E-Mail-Kontoeinstellungen an:

- Um dem Benutzer das Verschieben von E-Mail-Nachrichten zwischen den Konten zu erlauben, aktivieren Sie das Kontrollkästchen **Verschieben von Nachrichten zwischen Accounts erlauben**.
- Um die Synchronisierung der verwendeten E-Mail-Adressen zwischen Konten des Benutzers zu erlauben, aktivieren Sie das Kontrollkästchen **Synchronisierung der zuletzt verwendeten Adressen erlauben**.
- Um dem Benutzer zu erlauben, den Dienst Mail Drop für die Sendung von großen Anhängen zu verwenden, aktivieren Sie das Kontrollkästchen **Mail Drop erlauben**.
- Um dem Benutzer die Verwendung nur eines Standard-iOS-Mail-Clients zu erlauben, aktivieren Sie das Kontrollkästchen **Nur für Mail-App erlauben**.

12. Konfigurieren Sie die Einstellungen für die Verwendung des S/MIME-Protokolls in der Mail-App. Bei *S/MIME* handelt es sich um ein Protokoll für die Übertragung von verschlüsselten Nachrichten mit einer digitalen Signatur.

- Um das S/MIME-Protokoll zum Signieren ausgehender E-Mails zu verwenden, aktivieren Sie das Kontrollkästchen **Nachrichten unterschreiben** und wählen Sie das Zertifikat für die Signatur aus. Die digitale Signatur bestätigt die Authentizität des Absenders und zeigt dem Empfänger an, dass sich der Inhalt der Nachricht während der Übertragung nicht geändert hat. Die Signatur von Nachrichten ist auf mobilen Geräten mit dem Betriebssystem iOS Version 10.3 und höher verfügbar.
- Um das S/MIME-Protokoll zum Signieren ausgehender E-Mails zu verwenden, aktivieren Sie das Kontrollkästchen **Nachrichten standardmäßig verschlüsseln** und wählen Sie das Zertifikat für die Verschlüsselung (öffentlicher Schlüssel) aus. Die Verschlüsselung von Nachrichten ist auf mobilen Geräten mit dem Betriebssystem iOS Version 10.3 und höher verfügbar.
- Um dem Benutzer zu ermöglichen, Nachrichten einzeln zu verschlüsseln, aktivieren Sie das Kontrollkästchen **Toggle für Nachrichtenverschlüsselung anzeigen**. Um verschlüsselte Nachrichten zu versenden, muss der Benutzer in der Mail-App auf das Symbol  im Feld **An** klicken.

13. Passen Sie in den Abschnitten **Posteingangsserver** und **Postausgangsserver** über die Schaltfläche **Konfigurieren** die Einstellungen der Verbindung mit den Servern an:

- **Serveradresse und Port:** Hostnamen oder IP-Adressen des Posteingangs- und des Postausgangsservers sowie Portnummern der Server.
- **Accountname:** Kontoname des Benutzers für die Authentifizierung auf dem Posteingangs- und Postausgangsserver.
- **Authentifizierungstyp:** Authentifizierungstyp des E-Mail-Accounts des Nutzers auf den Posteingangs- und Postausgangsservern.
- **Kennwort:** Kennwort des Kontos für die Authentifizierung auf dem Posteingangs- und Postausgangsserver, geschützt durch die ausgewählte Authentifizierungsmethode.
- **Ein Kennwort für die Server der eingehenden und ausgehenden Nachrichten verwenden:** Nutzung eines Kennworts zur Benutzerauthentifizierung auf den Posteingangs- und Postausgangsservern.
- **SSL-Verbindung verwenden:** Transportprotokoll für den E-Mail-Transfer SSL (Secure Sockets Layer), das die Methoden der Verschlüsselung und Authentifizierung auf der Grundlage von Zertifikaten für den Schutz des E-Mail-Transfers verwendet.

14. Klicken Sie auf **OK**.

Das neue E-Mail-Konto wird in der Liste angezeigt.

15. Klicken Sie auf **Anwenden**, um die vorgenommenen Änderungen zu speichern.

Nach dem Anwenden der Richtlinie werden auf dem Mobilgerät des Nutzers E-Mail-Accounts aus der erstellten Liste hinzugefügt.

## Exchange-E-Mail-Postfach auf iOS MDM-Geräten konfigurieren

Damit der Nutzer eines iOS MDM-Geräts mit geschäftlichen E-Mails, dem Kalender, den Kontakten, Notizen und Aufgaben arbeiten kann, muss auf dem Microsoft Exchange Server ein Exchange ActiveSync-Account hinzugefügt werden.

Standardmäßig wird auf dem Microsoft Exchange-Server ein Benutzerkonto mit folgenden Parametern hinzugefügt:


- E-Mails werden einmal wöchentlich synchronisiert.
- Benutzer darf E-Mails zwischen seinen Accounts verschieben und Adressen der Accounts synchronisieren.
- Für die Arbeit mit den E-Mails darf der Benutzer beliebige E-Mail-Clients (nicht nur Mail) verwenden.
- Bei der Übermittlung von E-Mails wird keine SSL-Verbindung verwendet.

Sie können die festgelegten Parameter beim Hinzufügen eines Exchange ActiveSync-Konten ändern.

*Um einen Exchange ActiveSync-Account des Nutzers eines iOS MDM-Geräts hinzuzufügen, gehen Sie wie folgt vor:*

1. Wählen Sie in der Konsolenstruktur im Ordner **Verwaltete Geräte** die Administrationsgruppe, zu der die iOS MDM-Geräte gehören.
2. Gehen Sie Im Arbeitsbereich der Gruppe auf die Registerkarte **Richtlinien**.
3. Öffnen Sie über Doppelklick das Eigenschaftenfenster der Richtlinie.

4. Wählen Sie im Fenster **Eigenschaften <Name der Richtlinie>** den Abschnitt **Exchange ActiveSync**.
5. Klicken Sie im Block **Exchange ActiveSync-Konto** auf die Schaltfläche **Hinzufügen**.  
Das Fenster **Exchange ActiveSync-Konto** auf der Registerkarte **Allgemein** öffnet sich.
6. Geben Sie im Feld **Accountname** den Kontonamen für die Autorisierung auf dem Microsoft Exchange Server ein. Sie können Makros aus der Dropdown-Liste **Makro hinzufügen**.
7. Geben Sie im Feld **Serveradresse** den Netzwerknamen oder die IP-Adresse des Microsoft Exchange Servers ein.
8. Wenn Sie das Transportprotokoll für den E-Mail-Transfer SSL verwenden möchten, aktivieren Sie das Kontrollkästchen **SSL-Verbindung verwenden**.
9. Geben Sie im Feld **Domain** den Domain-Namen des Nutzers eines iOS MDM-Geräts ein. Sie können Makros aus der Dropdown-Liste **Makro hinzufügen**.
10. Geben Sie im Feld **Accountbenutzer** den Benutzernamen des Nutzers eines iOS MDM-Geräts ein.  
Wenn dieses Feld leer bleibt, wird Kaspersky Device Management für iOS nach dem Anwenden der Richtlinie auf dem iOS MDM-Gerät den Benutzer nach dem Namen fragen. Sie können Makros aus der Dropdown-Liste **Makro hinzufügen**.
11. Geben Sie im Feld **E-Mail-Adresse** die E-Mail-Adresse des Nutzers eines iOS MDM-Geräts ein. Sie können Makros aus der Dropdown-Liste **Makro hinzufügen**.
12. Geben Sie im Feld **Kennwort** das Kennwort für den Exchange ActiveSync-Account für die Autorisierung auf dem Microsoft Exchange Server ein.
13. Wählen Sie die Registerkarte **Erweitert** und passen Sie die erweiterten Exchange ActiveSync-Kontoeinstellungen an:
  - **E-Mail synchronisieren <Zeitraum>**.
  - **Authentifizierungstyp**.
  - **Verschieben von Nachrichten zwischen Accounts erlauben**.
  - **Synchronisierung der zuletzt verwendeten Adressen erlauben**.
  - **Nur für Mail-App erlauben**.
14. Konfigurieren Sie die Einstellungen für die Verwendung des S/MIME-Protokolls in der Mail-App. Bei *S/MIME* handelt es sich um ein Protokoll für die Übertragung von verschlüsselten Nachrichten mit einer digitalen Signatur.
  - Um das S/MIME-Protokoll zum Signieren ausgehender E-Mails zu verwenden, aktivieren Sie das Kontrollkästchen **Nachrichten unterschreiben** und wählen Sie das Zertifikat für die Signatur aus. Die digitale Signatur bestätigt die Authentizität des Absenders und zeigt dem Empfänger an, dass sich der Inhalt der Nachricht während der Übertragung nicht geändert hat. Die Signatur von Nachrichten ist auf mobilen Geräten mit dem Betriebssystem iOS Version 10.3 und höher verfügbar.
  - Um das S/MIME-Protokoll zum Signieren ausgehender E-Mails zu verwenden, aktivieren Sie das Kontrollkästchen **Nachrichten standardmäßig verschlüsseln** und wählen Sie das Zertifikat für die Verschlüsselung (öffentlicher Schlüssel) aus. Die Verschlüsselung von Nachrichten ist auf mobilen Geräten mit dem Betriebssystem iOS Version 10.3 und höher verfügbar.

- Um dem Benutzer zu ermöglichen, Nachrichten einzeln zu verschlüsseln, aktivieren Sie das Kontrollkästchen **Toggle für Nachrichtenverschlüsselung anzeigen**. Um verschlüsselte Nachrichten zu versenden, muss der Benutzer in der Mail-App auf das Symbol  im Feld **An** klicken.

15. Klicken Sie auf **OK**.

Das neue Exchange ActiveSync-Konto wird in der Liste angezeigt.

16. Klicken Sie auf **Anwenden**, um die vorgenommenen Änderungen zu speichern.

Nach dem Anwenden der Richtlinie werden auf dem Mobilgerät des Nutzers Exchange ActiveSync-Konten aus der erstellten Liste hinzugefügt.

## Einstellungen des Exchange-E-Mail-Postfachs auf dem Android-Gerät (nur Samsung)

Für die Arbeit mit E-Mail, Kontakten und Kalender des Unternehmens auf dem mobilen Gerät müssen die Einstellungen des Exchange-E-Mail-Postfachs angepasst werden.

Die Konfiguration einer Exchange-Mailbox ist nur für Samsung-Geräte möglich.

*Um das Exchange-E-Mail-Postfach auf dem mobilen Gerät anzupassen, gehen Sie wie folgt vor:*

1. Wählen Sie in der Konsolenstruktur im Ordner **Verwaltete Geräte** die Administrationsgruppe, zu der die Android-Geräte gehören.
2. Gehen Sie Im Arbeitsbereich der Gruppe auf die Registerkarte **Richtlinien**.
3. Öffnen Sie über Doppelklick auf eine beliebige Spalte das Eigenschaftenfenster der Richtlinie.
4. Wählen Sie im Fenster **Eigenschaften** der Richtlinie den Abschnitt **Verwaltung von Samsung KNOX** → **Verwaltung von Samsung-Geräten** aus.
5. Klicken Sie unter **Exchange ActiveSync** auf **Anpassen**.  
Es öffnet sich das Fenster **Einstellungen des Exchange-Mailservers**.
6. Geben Sie im Feld **Serveradresse** die IP-Adresse oder den DNS-Namen des Servers, auf der der Mail-Server installiert ist.
7. Geben Sie im Feld **Domain** den Namen der Domäne des Benutzers im Unternehmensnetzwerk ein.
8. Wählen Sie in der Dropdown-Liste **Regelmäßigkeit der Synchronisierung** den gewünschten Zeitraum für die Synchronisierung des mobilen Geräts mit dem Microsoft Exchange-Server.
9. Um das Transportprotokoll für den E-Mail-Transfer SSL zu verwenden, aktivieren Sie das Kontrollkästchen **SSL-Verbindung verwenden**.
10. Um digitale Zertifikate für den Schutz des Datentransfers zwischen dem mobilen Gerät und dem Microsoft Exchange-Server zu verwenden, aktivieren Sie das Kontrollkästchen **Serverzertifikat prüfen**.
11. Klicken Sie auf **Anwenden**, um die vorgenommenen Änderungen zu speichern.

Die Einstellungen werden nach der nächsten planmäßigen Synchronisierung des Geräts mit Kaspersky Security Center auf dem mobilen Gerät konfiguriert.

## Verwaltung mobiler Anwendungen von Drittherstellern

Zur Aktivitätsüberwachung von mobilen Anwendungen, die auf einem mobilen Endgerät, können Sie Container verwenden. Ein *Container* ist eine spezielle Schnittstelle für mobile Anwendungen, mit der sich die Aktionen der im Container befindlichen Anwendungen überwachen lassen. Dadurch sind persönliche und Unternehmensdaten des Benutzers auf dem Gerät sicher.

In Kaspersky Security für mobile Endgeräte Service Pack 3 Maintenance Release 2 wird das Erstellen von Containern für mobile Apps nicht mehr unterstützt. Sie können jedoch Container auf Android-Geräten hinzufügen, die in früheren Programmversionen erstellt wurden.

Sie können eine der folgenden Methoden verwenden, um eine Anwendung in einem Container auf dem mobilen Endgerät zu installieren:


- Senden einer E-Mail-Nachricht an den Benutzer. Die Nachricht enthält einen Link zur Distribution der App im Container.
- Anwendung im Container in den Richtlinienereigenschaften im Abschnitt **Anwendungskontrolle** als obligatorisch oder zur Installation erlaubt festlegen. Nach der Synchronisierung des Geräts mit Kaspersky Security Center wird die Distribution der Anwendung im Container automatisch auf das Gerät des Benutzers kopiert.

Um die App-Installation in Containern zu ermöglichen, muss auf dem mobilen Gerät des Benutzers die Installation von Apps aus unbekannten Quellen erlaubt sein. Zur Gewährleistung der Sicherheit des Geräts und dem Schutz von Daten nach der Installation von Apps in Containern wird empfohlen, die Installation von Apps aus unbekannten Quellen zu verbieten. Nähere Informationen über die Installation von Apps ohne Google Play finden Sie in der [Android-Hilfe](#).

## Benachrichtigungen für Kaspersky Endpoint Security für Android anpassen

Wenn Sie möchten, dass der Benutzer des Mobilgeräts von den Benachrichtigungen von Kaspersky Security für Android nicht abgelenkt wird, können Sie einige Benachrichtigungen deaktivieren.

Kaspersky Endpoint Security verwendet die folgenden Tools, um den Schutzstatus des Geräts anzuzeigen:

- **Benachrichtigung über den Schutzstatus.** Diese Benachrichtigung ist an die Benachrichtigungsleiste angeheftet. Die Benachrichtigung über den Schutzstatus kann nicht entfernt werden. Die Benachrichtigung zeigt den Schutzstatus des Geräts (z. B. ) und die Anzahl etwaiger Probleme an. Tippen Sie auf den Schutzstatus des Geräts, um die Liste mit Problemen in der App anzuzeigen.
- **App-Benachrichtigungen.** Diese Benachrichtigungen informieren den Gerätebenutzer über die App (z. B. über das Erkennen von Bedrohungen).
- **Pop-up-Meldungen.** Pop-up-Meldungen erfordern eine Aktion seitens des Gerätebenutzers (z. B. eine Aktion beim Fund einer Bedrohung).

Standardmäßig sind alle Benachrichtigungen von Kaspersky Endpoint Security für Android aktiviert.

Der Benutzer des Android-Geräts kann alle Benachrichtigungen von Kaspersky Endpoint Security für Android in den Einstellungen in der Benachrichtigungsleiste deaktivieren. Wenn die Benachrichtigungen deaktiviert sind, überwacht der Benutzer die Ausführung des App nicht und könnte wichtige Informationen übersehen (z. B. Hinweise auf eine Störung bei der Synchronisierung des Geräts mit Kaspersky Security Center). Um den Status der App-Ausführung zu sehen, muss der Benutzer Kaspersky Endpoint Security für Android öffnen.

*Um die Anzeige der Benachrichtigungen über die Ausführung von Kaspersky Endpoint für Android anzupassen, gehen Sie wie folgt vor:*

1. Wählen Sie in der Konsolenstruktur im Ordner **Verwaltete Geräte** die Administrationsgruppe, zu der die Android-Geräte gehören.
2. Gehen Sie im Arbeitsbereich der Gruppe auf die Registerkarte **Richtlinien**.
3. Öffnen Sie über Doppelklick auf eine beliebige Spalte das Eigenschaftenfenster der Richtlinie.
4. Wählen Sie im folgenden Fenster **Eigenschaften <Name der Richtlinie>** den Abschnitt **Erweitert** aus.
5. Klicken Sie im Block **App-Benachrichtigungen** auf **Anpassen**.

Das Fenster **Benachrichtigungseinstellungen auf dem Gerät** wird geöffnet.

6. Wählen Sie die Probleme von Kaspersky Endpoint Security für Android aus, die Sie auf dem mobilen Gerät des Benutzers ausblenden möchten, und klicken Sie auf **OK**.

Kaspersky Endpoint Security für Android zeigt weder Probleme in der Benachrichtigung zum Schutzstatus noch Probleme im Block **Status** in der App an. Kaspersky Endpoint Security für Android zeigt die Benachrichtigung zum Schutzstatus sowie die App-Benachrichtigungen weiterhin an.

Die Anzeige einiger Probleme von Kaspersky Endpoint Security für Android ist obligatorisch und kann nicht deaktiviert werden (z. B. Probleme mit der Gültigkeitsdauer der Lizenz).

7. Um alle Benachrichtigungen und Pop-up-Meldungen auszublenden, wählen Sie den Modus **Benachrichtigungen und Pop-ups deaktivieren, wenn die App im Hintergrund läuft**.

Kaspersky Endpoint Security für Android zeigt dann nur Benachrichtigungen zum Schutzstatus an. Die Benachrichtigung zeigt den Schutzstatus des Geräts (z. B. ⓘ) und die Anzahl der Probleme an. Außerdem zeigt die App Benachrichtigungen an, wenn Benutzer die App selbst verwenden (wenn Benutzer z. B. manuelle Updates der Antiviren-Datenbanken vornehmen).

Die Experten bei Kaspersky empfehlen, Benachrichtigungen und Pop-up-Meldungen zu aktivieren. Wenn Sie Benachrichtigungen und Pop-up-Meldungen für die Ausführung der App im Hintergrund deaktivieren, werden Benutzer nicht in Echtzeit vor Bedrohungen gewarnt. Die Benutzer der mobilen Geräte müssen dann die App öffnen, um den Schutzstatus des Geräts zu sehen.

8. Klicken Sie auf **Anwenden**, um die vorgenommenen Änderungen zu speichern.

Die Einstellungen werden nach der nächsten planmäßigen Synchronisierung des Geräts mit Kaspersky Security Center auf dem mobilen Gerät konfiguriert. Auf dem mobilen Gerät des Benutzers werden die Benachrichtigungen von Kaspersky Endpoint Security für Android, die Sie deaktiviert haben, nicht angezeigt.

## Verbindung von iOS MDM-Geräten mit AirPlay



Um die Musik, Fotos und Videos vom iOS MDM-Gerät auf die AirPlay-Geräte zu streamen, muss die automatische Verbindung zu den AirPlay-Geräten angepasst werden. Für die Verwendung der AirPlay-Technologie müssen das Mobilgerät und die AirPlay-Geräte mit einem kabellosen Netzwerk verbunden sein. Zu den AirPlay-Geräten zählen Apple TV-Geräte (zweite und dritte Generation), AirPort Express-Geräte, Lautsprecher oder Anlagen, die AirPlay unterstützen.

Die automatische Verbindung mit den AirPlay-Geräten ist nur für kontrollierte Geräte möglich.

*Um die Verbindung des iOS MDM-Geräts mit den AirPlay-Geräten anzupassen, gehen Sie wie folgt vor:*

1. Wählen Sie in der Konsolenstruktur im Ordner **Verwaltete Geräte** die Administrationsgruppe, zu der die iOS MDM-Geräte gehören.
2. Gehen Sie Im Arbeitsbereich der Gruppe auf die Registerkarte **Richtlinien**.
3. Öffnen Sie über Doppelklick das Eigenschaftsfenster der Richtlinie.
4. Wählen Sie im Fenster **Eigenschaften <Name der Richtlinie>** den Abschnitt **AirPlay**.
5. Aktivieren Sie im Block **AirPlay-Geräte** das Kontrollkästchen **Einstellungen auf dem Gerät anwenden**.
6. Klicken Sie im Block **Kennwörter** auf **Hinzufügen**.  
In die Kennworttabelle wird eine leere Zeile hinzugefügt.
7. Geben Sie in der Spalte **Gerätename** den Namen des AirPlay-Geräts im kabellosen Netzwerk ein.
8. Geben Sie in der Spalte **Kennwort** das Kennwort des AirPlay-Geräts ein.
9. Um die Verbindung des iOS MDM-Geräts mit den AirPlay-Geräten zu beschränken, erstellen Sie im Block **Erlaubte Geräte** eine Liste mit erlaubten Geräten. Fügen Sie dazu in die Liste der erlaubten Geräte die MAC-Adressen der AirPlay-Geräte hinzu.  
Auf die AirPlay-Geräte, die nicht in der Liste der erlaubten Geräte enthalten sind, ist der Zugriff verboten. Wenn Sie die Liste der erlaubten Geräte leer lassen, wird Kaspersky Device Management für iOS den Zugriff auf alle AirPlay-Geräte erlauben.
10. Klicken Sie auf **Anwenden**, um die vorgenommenen Änderungen zu speichern.  
  
Nach dem Anwenden der Richtlinie wird sich das Mobilgerät des Nutzers automatisch mit den AirPlay-Geräten für den Transfer von Medieninhalten verbinden.

## Verbindung von iOS MDM-Geräten mit AirPrint

Für den Druck von Dokumenten von dem iOS MDM-Gerät mithilfe der drahtlosen Technologie AirPrint muss die automatische Verbindung zu den AirPrint-Druckern angepasst werden. Das mobile Gerät und der Drucker müssen mit einem kabellosen Netzwerk verbunden sein. Auf dem AirPrint-Drucker muss ein allgemeiner Zugriff für alle Benutzer eingerichtet werden.

*Um die Verbindung des iOS MDM-Geräts mit dem AirPrint-Drucker anzupassen, gehen Sie wie folgt vor:*

1. Wählen Sie in der Konsolenstruktur im Ordner **Verwaltete Geräte** die Administrationsgruppe, zu der die iOS MDM-Geräte gehören.
2. Gehen Sie Im Arbeitsbereich der Gruppe auf die Registerkarte **Richtlinien**.

3. Öffnen Sie über Doppelklick das Eigenschaftfenster der Richtlinie.

4. Wählen Sie im Fenster **Eigenschaften <Name der Richtlinie>** den Abschnitt **AirPrint**.

5. Klicken Sie im Block **AirPrint-Drucker** auf **Hinzufügen**.

Das Fenster **Drucker** wird geöffnet.

6. Geben Sie im Feld **IP-Adresse** die IP-Adresse des AirPrint-Druckers ein.

7. Geben Sie im Feld **Ressourcenpfad** den Pfad zum AirPrint-Drucker ein.

Der Druckerpfad entspricht dem rp-Schlüssel (Ressourcenpfad) des Bonjour-Protokolls. Beispielsweise:

- printers/Canon\_MG5300\_series.
- ipp/print.
- Epson\_IPP\_Printer.

8. Klicken Sie auf **OK**.

Der hinzugefügte AirPrint-Drucker wird in der Liste angezeigt.

9. Klicken Sie auf **Anwenden**, um die vorgenommenen Änderungen zu speichern.

Nach dem Anwenden der Richtlinie kann der Nutzer des Mobilgeräts Dokumente auf dem AirPrint-Drucker über eine kabellose Verbindung drucken.

## Zugriffspunkt (APN) anpassen

Für die Verbindung des mobilen Geräts mit den Diensten zur Datenübertragung im mobilen Netzwerk ist nötig, die APN-Einstellungen (Access Point Name) anzupassen.

### APN-Einstellungen auf Android-Geräten (nur Samsung)

Die Konfiguration von APN ist nur für Samsung-Geräte möglich.

Für die Verwendung des Access Points muss auf dem mobilen Gerät des Benutzers eine SIM-Karte eingerichtet sein. Die Parameter des Access Points werden vom Mobilfunkanbieter bereitgestellt. Eine inkorrekte Konfiguration des Access Points kann zu zusätzlichen Ausgaben für die mobile Nachrichtenübertragung führen.

*Um die Einstellungen des Zugriffspunkts (APN) anzupassen, gehen Sie wie folgt vor:*

1. Wählen Sie in der Konsolenstruktur im Ordner **Verwaltete Geräte** die Administrationsgruppe, zu der die Android-Geräte gehören.
2. Gehen Sie Im Arbeitsbereich der Gruppe auf die Registerkarte **Richtlinien**.
3. Öffnen Sie über Doppelklick auf eine beliebige Spalte das Eigenschaftfenster der Richtlinie.

4. Wählen Sie im Fenster **Eigenschaften** der Richtlinie den Abschnitt **Verwaltung von Samsung KNOX** → **APN**.

5. Klicken Sie im Block **APN** auf **Anpassen**.

Das Fenster **Einstellungen für APN** wird geöffnet.

6. Geben Sie auf der Registerkarte **Allgemein** folgende Einstellungen des Zugriffspunkts an:

- a. Wählen Sie in der Dropdown-Liste **Typ des Zugriffspunkts** den Typ des Zugriffspunkts aus.
- b. Geben Sie im Feld **Name des Zugriffspunkts** den Namen des Zugriffspunkts an.
- c. Geben Sie im Feld **MCC** den mobilen Ländercode (MCC) an.
- d. Geben Sie im Feld **MNC** den Funknetzcode (MNC) an.
- e. Wenn Sie als Zugriffspunkt **MMS** oder **Internet und MMS** gewählt haben, geben Sie die erweiterten Einstellungen für MMS an:
  - Geben Sie im Feld **Server für MMS** den vollständigen Domain-Namen des Servers des Mobilfunkanbieters für den MMS-Tausch an.
  - Geben Sie im Feld **Proxy-Server für MMS** den Netzwerknamen oder die IP-Adresse des Proxy-Servers und die Portnummer des Proxy-Servers des Mobilfunkanbieters für den MMS-Tausch an.

7. Passen Sie auf der Registerkarte **Erweitert** die erweiterten Einstellungen des Zugriffspunkts (APN) an:

- a. Wählen Sie in der Dropdown-Liste **Authentifizierungstyp** den Typ der Autorisierung des Mobilgerätenutzers auf dem Server des Mobilfunkanbieters für den Zugriff auf das Netzwerk.
- b. Geben Sie im Feld **Serveradresse** den Netzwerknamen des Servers des Mobilfunkanbieters, über den der Zugriff auf die Datenübermittlungsdienste erfolgt.
- c. Geben Sie im Feld **Proxy-Server-Adresse** den Netzwerknamen oder die IP-Adresse des Proxy-Servers und die Portnummer des Proxy-Servers des Mobilfunkanbieters für den Zugriff auf das Netzwerk ein.
- d. Geben Sie im Feld **Benutzername** den Namen des Benutzers für die Autorisierung im mobilen Netzwerk an.
- e. Geben Sie im Feld **Kennwort** das Kennwort für die Autorisierung im mobilen Netzwerk an.

8. Klicken Sie auf **Anwenden**, um die vorgenommenen Änderungen zu speichern.

Die Einstellungen werden nach der nächsten planmäßigen Synchronisierung des Geräts mit Kaspersky Security Center auf dem mobilen Gerät konfiguriert.

## APN-Einstellungen auf iOS MDM-Geräten

Für die Verbindung des Nutzers eines iOS MDM-Geräts mit den Diensten für den Datentransfer in einem Mobilnetz muss der Zugriffspunkt (APN) angepasst werden.

Der Abschnitt **APN** ist veraltet. Es wird empfohlen, die APN-Einstellungen im Abschnitt **Mobilfunk** anzupassen. Vor dem Anpassen der Mobilfunkeinstellungen überzeugen Sie sich, dass die Einstellungen des Abschnitts **APN** auf dem Gerät nicht verwendet werden (das Kontrollkästchen **Einstellungen auf dem Gerät anwenden** deaktiviert ist). Die Einstellungen der Abschnitte **APN** und **Mobilfunk** können nicht gleichzeitig verwendet werden.

Um den Zugriffspunkt auf dem iOS MDM-Gerät anzupassen, gehen Sie wie folgt vor:

1. Wählen Sie in der Konsolenstruktur im Ordner **Verwaltete Geräte** die Administrationsgruppe, zu der die iOS MDM-Geräte gehören.
2. Gehen Sie Im Arbeitsbereich der Gruppe auf die Registerkarte **Richtlinien**.
3. Öffnen Sie über Doppelklick das Eigenschaftfenster der Richtlinie.
4. Wählen Sie im Fenster **Eigenschaften <Name der Richtlinie>** den Abschnitt **Mobilfunk** aus.
5. Aktivieren Sie im Block **Mobilfunkeinstellungen** das Kontrollkästchen **Einstellungen auf dem Gerät anwenden**.
6. Wählen Sie in der Liste "**APN-Typ**" den Typ des Zugriffspunkts für die Datenübertragung im mobilen Netzwerk GPRS/3G/4G aus:
  - **Integrierter APN** – Anpassen der Mobilfunkeinstellungen für die Datenübertragung über einen Mobilfunk-Provider, der die Arbeit mit der integrierten Apple-SIM unterstützt. Nähere Informationen über Geräte mit integrierter Apple-SIM finden Sie auf der [Seite des technischen Supports von Apple](#).
  - **APN** – Anpassen der Mobilfunkeinstellungen für die Datenübertragung über den Mobilfunk-Provider der eingesetzten SIM-Karte.
  - **Integrierter APN und APN** – Anpassen der Mobilfunkeinstellungen für die Datenübertragung durch die Mobilfunk-Provider der eingesetzten SIM-Karte und der integrierten Apple-SIM. Nähere Informationen über Geräte mit integrierter Apple-SIM und einem Steckplatz für SIM-Karten finden Sie auf der [Seite des technischen Supports von Apple](#).
7. Geben Sie im Feld **Name des Zugriffspunkts** den Namen des Zugriffspunkts an.
8. Wählen Sie in der Dropdown-Liste **Authentifizierungstyp** einen Authentifizierungstyp des Benutzers des mobilen Geräts auf dem Server des Mobilfunkanbieter für den Zugriff auf das Netzwerk (Internet und MMS):
9. Geben Sie im Feld **Benutzername** den Namen des Benutzers für die Autorisierung im mobilen Netzwerk an.
10. Geben Sie im Feld **Kennwort** das Kennwort für die Autorisierung im mobilen Netzwerk an.
11. Geben Sie im Feld **Proxyserveradresse und Port** den Namen des Hosts, der Domain oder die IP-Adresse des Proxy-Servers und die Portnummer des Proxy-Servers ein.
12. Klicken Sie auf **Anwenden**, um die vorgenommenen Änderungen zu speichern.

Nach dem Anwenden der Richtlinie wird auf dem Mobilgerät der Zugriffspunkt (APN) angepasst werden.

## Einstellungen des Arbeitsprofils Android anpassen

Dieser Abschnitt enthält Informationen über die Arbeit mit dem Arbeitsprofil Android.

### Über das Arbeitsprofil Android

*Android Enterprise* ist eine Plattform für die Verwaltung der mobilen Infrastruktur des Unternehmens, die den Mitarbeitern eine Arbeitsumgebung für die Arbeit auf mobilen Endgeräten bietet. Ausführliche Informationen zur Arbeit mit Android Enterprise, s. [Website des technischen Supports von Google](#).

Sie können auf dem mobilen Gerät des Benutzers ein Arbeitsprofil Android (im Weiteren auch "Arbeitsprofil") erstellen. Das *Arbeitsprofil Android* ist eine sichere Umgebung auf dem Benutzergerät, in der der Administrator die Verwaltung von Apps und Kontos ausführen kann, ohne den Benutzer in den Möglichkeiten bei der Arbeit mit seinen eigenen Daten einzuschränken. Bei der Erstellung des Arbeitsprofils auf dem mobilen Gerät des Benutzers werden darin automatisch folgende korporative Apps installiert: Google Play, Google Chrome, Downloads, Kaspersky Endpoint Security für Android und andere. Die im Arbeitsprofil installierten korporativen Apps sowie die Benachrichtigungen dieser Apps sind mit dem Symbol  markiert. Für die App Google Play muss ein separates geschäftliches Google-Konto angelegt werden. Apps, die sich im Arbeitsprofil befinden, werden in der allgemeinen App-Liste angezeigt.

## Einstellungen des Arbeitsprofils anpassen

*Um die Einstellungen des Arbeitsprofils Android zu konfigurieren, gehen Sie folgendermaßen vor:*

1. Wählen Sie in der Konsolenstruktur im Ordner **Verwaltete Geräte** die Administrationsgruppe, zu der die Android-Geräte gehören.
2. Gehen Sie Im Arbeitsbereich der Gruppe auf die Registerkarte **Richtlinien**.
3. Öffnen Sie über Doppelklick auf eine beliebige Spalte das Eigenschaftfenster der Richtlinie.
4. Wählen Sie im Fenster **Eigenschaften** der Richtlinie die Option **Arbeitsprofil Android** aus.
5. Aktivieren Sie im Arbeitsbereich **Arbeitsprofil Android** das Kontrollkästchen **Arbeitsprofil erstellen**.
6. Geben Sie die Einstellungen des Arbeitsprofils an:
  - Um die Anwendungskontrolle im Arbeitsprofil Android zu aktivieren und im persönlichen Profil zu deaktivieren, aktivieren Sie das Kontrollkästchen **Anwendungskontrolle nur im Arbeitsprofil aktivieren**.  
Im Block **Benutzer** können Sie **App-Kontrolle** auswählen und im Arbeitsbereich dieses Abschnittes Listen für erlaubte, verbotene, empfohlene und obligatorische Apps sowie erlaubte und verbotene App-Kategorien erstellen.
  - Um für Google Chrome den Web-Filter im Arbeitsprofil zu aktivieren und im persönlichen Profil zu deaktivieren, aktivieren Sie im Arbeitsbereich des Abschnittes **Arbeitsprofil Android** das Kontrollkästchen **Web-Filter nur im Arbeitsprofil aktivieren**.

Web-Filter für Samsung Internet Browser blockiert Websites sowohl im persönlichen Profil als auch im Arbeitsprofil. Es ist nicht möglich, Web-Filter für Samsung Internet Browser nur im Arbeitsprofil zu aktivieren. Um für Samsung Internet Browser den Web-Filter im Arbeitsprofil zu verwenden, deaktivieren Sie die Option **Web-Filter nur im Arbeitsprofil aktivieren**. Wenn diese Option aktiviert ist, wird Web-Filter für Samsung Internet Browser nicht ausgeführt. Der Web-Filter im Arbeitsprofil ist standardmäßig deaktiviert.

Der Web-Filter funktioniert auf Android-Geräten nur mit den Browsern Google Chrome und Samsung Internet Browser.

Sie können im **Block Web-Filter** die Einstellungen für den Zugriff auf Websites anpassen, indem Sie eine Liste mit Kategorien für blockierte Websites oder mit erlaubten Websites erstellen.

- Um dem Benutzer das Kopieren von Daten aus Apps des Arbeitsprofils in persönliche Apps mithilfe der Zwischenablage zu verbieten, aktivieren Sie das Kontrollkästchen **Übertragung von Daten aus dem Arbeitsprofil in das private Profil verbieten**.
  - Um dem Benutzer die Verwendung des Debug-Modus über USB auf dem mobilen Gerät im Arbeitsprofil zu verbieten, aktivieren Sie das Kontrollkästchen **Aktivierung des Debug-Modus über USB verbieten**.  
Im Debug-Modus über USB kann der Benutzer z. B. eine App über die Workstation herunterladen.
  - Um dem Benutzer die Installation von Apps im Arbeitsprofil für Android aus allen Quellen mit Ausnahme von Google Play zu verbieten, aktivieren Sie das Kontrollkästchen **Installation von Anwendungen aus unbekannten Quellen in das Arbeitsprofil verbieten**.
  - Um dem Benutzer die Deinstallation von Apps aus dem Arbeitsprofil für Android zu verbieten, aktivieren Sie das Kontrollkästchen **Deinstallation von Anwendungen aus dem Arbeitsprofil verbieten**.
7. Um die Einstellungen des Arbeitsprofils auf dem mobilen Gerät des Benutzers anzupassen, sperren Sie die Änderung der Einstellungen.
8. Klicken Sie auf **Anwenden**, um die vorgenommenen Änderungen zu speichern.

Die Einstellungen werden nach der nächsten planmäßigen Synchronisierung des Geräts mit Kaspersky Security Center auf dem mobilen Gerät konfiguriert. Der Speicherplatz des mobilen Geräts des Benutzers wird auf das Arbeitsprofil und das persönliche Profil aufgeteilt.

## LDAP-Account hinzufügen

Damit der Nutzer eines iOS MDM-Geräts den Zugriff auf Geschäftskontakte auf dem LDAP-Server erhält, muss ein LDAP-Account hinzugefügt werden.

*Um einen LDAP-Account des Nutzers eines iOS MDM-Geräts hinzuzufügen, gehen Sie wie folgt vor:*

1. Wählen Sie in der Konsolenstruktur im Ordner **Verwaltete Geräte** die Administrationsgruppe, zu der die iOS MDM-Geräte gehören.
2. Gehen Sie im Arbeitsbereich der Gruppe auf die Registerkarte **Richtlinien**.
3. Öffnen Sie über Doppelklick das Eigenschaftfenster der Richtlinie.
4. Wählen Sie im Fenster **Eigenschaften <Name der Richtlinie>** den Abschnitt **LDAP**.
5. Klicken Sie im Block **LDAP-Benutzerkonten** auf die Schaltfläche **Hinzufügen**.  
Das Fenster **LDAP-Account** wird geöffnet.
6. Geben Sie im Feld **Beschreibung** die Beschreibung des LDAP-Accounts des Nutzers ein. Sie können Makros aus der Dropdown-Liste **Makro hinzufügen**.
7. Geben Sie im Feld **Accountname** den Kontonamen für die Autorisierung auf dem LDAP-Server ein. Sie können Makros aus der Dropdown-Liste **Makro hinzufügen**.
8. Geben Sie im Feld **Kennwort** das Kennwort des LDAP-Accounts für die Authentifizierung auf dem LDAP-Server.
9. Geben Sie im Feld **Serveradresse** den Domain-Namen des LDAP-Servers ein. Sie können Makros aus der Dropdown-Liste **Makro hinzufügen**.

10. Um für den Schutz der übertragenen Nachrichten das Transportprotokoll für den Datentransfer SSL zu verwenden, aktivieren Sie das Kontrollkästchen **SSL-Verbindung verwenden**.
11. Erstellen Sie eine Liste mit den Suchanfragen für den Zugriff des Nutzers eines iOS MDM-Geräts auf die Ordner mit den Unternehmensdaten auf dem LDAP-Server:
- Klicken Sie im Block **Sucheinstellungen** auf **Hinzufügen**.  
In der Tabelle mit den Suchanfragen wird eine leere Zeile angezeigt.
  - Geben Sie in der Spalte **Name** den Namen der Suchanfrage ein.
  - Geben Sie in der Spalte **Suchtiefe** die Verschachtelungsebene des Ordners für die Suche nach Unternehmensdaten auf dem LDAP-Server ein:
    - **Strukturstamm** – Suche im Basisordner des LDAP-Servers.
    - **Eine Ebene** – Suche in den Ordnern auf der ersten Verschachtelungsebene des Basisordners.
    - **Teilbaum** – Suche in den Ordnern auf allen Verschachtelungsebenen des Basisordners.
  - Geben Sie im Feld **Suchbereich** den Pfad zum Ordner auf dem LDAP-Server, von dem aus die Suche beginnt (beispielsweise, "ou=people", "o=example corp") ein.
  - Wiederholen Sie die Schritte a-d für alle Suchanfragen, die Sie auf dem iOS MDM-Gerät hinzufügen möchten.
12. Klicken Sie auf **OK**.  
Das neue LDAP-Konto wird in der Liste angezeigt.
13. Klicken Sie auf **Anwenden**, um die vorgenommenen Änderungen zu speichern.
- Nach dem Anwenden der Richtlinie werden auf dem Mobilgerät des Nutzers LDAP-Accounts aus der erstellten Liste hinzugefügt. Der Benutzer kann Zugriff auf Unternehmenskontakte in den iOS-Standardanwendungen Kontakte, Nachrichten und Mail erhalten.

## Kalender-Account hinzufügen

Damit der Nutzer eines iOS MDM-Geräts mit den Kalenderereignissen auf dem CalDAV-Server arbeiten kann, muss ein CalDAV-Account hinzugefügt werden. Die Synchronisierung mit dem CalDAV-Server ermöglicht es dem Benutzer, Einladungen zu erstellen und anzunehmen, Updates der Ereignisse zu erhalten und Aufgaben mit der Anwendung Erinnerungen zu synchronisieren.

*Um einen CalDAV-Account des iOS MDM-Gerätbenutzers hinzuzufügen, gehen Sie wie folgt vor:*

- Wählen Sie in der Konsolenstruktur im Ordner **Verwaltete Geräte** die Administrationsgruppe, zu der die iOS MDM-Geräte gehören.
- Gehen Sie im Arbeitsbereich der Gruppe auf die Registerkarte **Richtlinien**.
- Öffnen Sie über Doppelklick das Eigenschaftsfenster der Richtlinie.
- Wählen Sie im Fenster **Eigenschaften <Name der Richtlinie>** den Abschnitt **Kalender**.
- Klicken Sie im Block **CalDAV-Accounts** auf die Schaltfläche **Hinzufügen**.

Es öffnet sich das Fenster **CalDAV-Account**.

6. Geben Sie im Feld **Beschreibung** die Beschreibung des CalDAV-Kontos des Nutzers ein.
7. Geben Sie im Feld **Serveradresse und Port** den Namen des Hosts oder die IP-Adresse des Proxy-Servers und die Portnummer des CalDAV-Servers ein.
8. Geben Sie im Feld **Primäre Webadresse** die Webadresse des CalDAV-Accounts des Nutzers eines iOS MDM-Geräts auf dem CalDAV-Server ein (beispielsweise, <http://example.com/caldav/users/mycompany/user>).  
Die Webadresse muss mit "http://" beginnen oder "https://" beginnen.
9. Geben Sie im Feld **Accountname** den Kontonamen des Benutzers für die Autorisierung auf dem CalDAV-Server ein.
10. Geben Sie im Feld **Kennwort** das Kennwort des Kontos für die Autorisierung auf dem CalDAV-Server ein.
11. Um zum Schutz der Übertragung von Ereignisdaten zwischen dem CalDAV-Server und dem mobilen Gerät das Transportprotokoll für den Datentransfer SSL zu verwenden, aktivieren Sie das Kontrollkästchen **SSL-Verbindung verwenden**.
12. Klicken Sie auf **OK**.  
Das neue CalDAV-Konto wird in der Liste angezeigt.
13. Klicken Sie auf **Anwenden**, um die vorgenommenen Änderungen zu speichern.

Nach dem Anwenden der Richtlinie werden auf dem Mobilgerät des Nutzers CalDAV-Accounts aus der erstellten Liste hinzugefügt.

## Kontakte-Account hinzufügen

Damit der Nutzer eines iOS MDM-Geräts seine Kontakte mit dem CardDAV-Server synchronisieren kann, muss ein CardDAV-Account hinzugefügt werden. Die Synchronisierung mit dem CardDAV-Server ermöglicht es dem Benutzer, Zugriff auf Kontaktdaten von jedem Gerät aus zu erhalten.

*Um einen CardDAV-Account des iOS MDM-Gerätbenutzers hinzuzufügen, gehen Sie wie folgt vor:*

1. Wählen Sie in der Konsolenstruktur im Ordner **Verwaltete Geräte** die Administrationsgruppe, zu der die iOS MDM-Geräte gehören.
2. Gehen Sie Im Arbeitsbereich der Gruppe auf die Registerkarte **Richtlinien**.
3. Öffnen Sie über Doppelklick das Eigenschaftfenster der Richtlinie.
4. Wählen Sie im Fenster **Eigenschaften <Name der Richtlinie>** den Abschnitt **Kontakte**.
5. Klicken Sie im Block **CardDAV-Accounts** auf die Schaltfläche **Hinzufügen**.  
Es öffnet sich das Fenster **CardDAV-Account**.
6. Geben Sie im Feld **Beschreibung** die Beschreibung des CardDAV-Kontos des Nutzers ein. Sie können Makros aus der Dropdown-Liste **Makro hinzufügen**.
7. Geben Sie im Feld **Serveradresse und Port** den Namen des Hosts oder die IP-Adresse des Proxy-Servers und die Portnummer des CardDAV-Servers ein.



8. Geben Sie im Feld **Primäre Webadresse** die Webadresse des CardDAV-Accounts des Nutzers eines iOS MDM-Geräts auf dem CardDAV-Server ein (beispielsweise, <http://example.com/carddav/users/mycompany/user>).  
Die Webadresse muss mit "http://" beginnen oder "https://" beginnen.
9. Geben Sie im Feld **Accountname** den Kontonamen des Benutzers für die Autorisierung auf dem CardDAV-Server ein. Sie können Makros aus der Dropdown-Liste **Makro hinzufügen**.
10. Geben Sie im Feld **Kennwort** das Kennwort des Kontos für die Autorisierung auf dem CardDAV-Server ein.
11. Um zum Schutz der Übertragung von Kontakten zwischen dem CardDAV-Server und dem mobilen Gerät das Transportprotokoll für den Datentransfer SSL zu verwenden, aktivieren Sie das Kontrollkästchen **SSL-Verbindung verwenden**.
12. Klicken Sie auf **OK**.  
Das neue CardDAV-Konto wird in der Liste angezeigt.
13. Klicken Sie auf **Anwenden**, um die vorgenommenen Änderungen zu speichern.

Nach dem Anwenden der Richtlinie werden auf dem Mobilgerät des Nutzers CardDAV-Accounts aus der erstellten Liste hinzugefügt.

## Kalenderabonnement anpassen

Damit der Benutzer eines iOS MDM-Geräts Ereignisse aus den externen Kalendern (beispielsweise, aus dem Unternehmenskalender) in seinen Kalender hinzufügen kann, muss ein Abonnement zum Kalender hinzugefügt werden. *Externe Kalender* sind Kalender anderer Hersteller, die über ein CalDAV-Konto verfügen, iCal-Kalender sowie andere öffentliche Kalender.

*Gehen Sie folgendermaßen vor, um ein Kalenderabonnement hinzuzufügen:*

1. Wählen Sie in der Konsolenstruktur im Ordner **Verwaltete Geräte** die Administrationsgruppe, zu der die iOS MDM-Geräte gehören.
2. Gehen Sie Im Arbeitsbereich der Gruppe auf die Registerkarte **Richtlinien**.
3. Öffnen Sie über Doppelklick das Eigenschaftfenster der Richtlinie.
4. Wählen Sie im Fenster **Eigenschaften <Name der Richtlinie>** den Abschnitt **Kalenderabonnement**.
5. Klicken Sie im Block **Kalenderabonnements** auf die Schaltfläche **Hinzufügen**.  
Es öffnet sich das Fenster **Kalenderabonnement**.
6. Geben Sie im Feld **Beschreibung** die Beschreibung des Kalenderabonnements ein.
7. Geben Sie im Feld **Webadresse des Servers** die Webadresse des Dritthersteller-Kalenders ein.  
Sie können in diesem Feld die primäre Webadresse des CalDAV-Accounts des Benutzers angeben, dessen Kalender abonniert werden soll. Auch können Sie die Webadresse des iCal-Kalenders oder eines anderen veröffentlichten Kalenders angeben.
8. Geben Sie im Feld **Benutzername** den Kontonamen des Benutzers für die Authentifizierung auf dem Server des Dritthersteller-Kalenders ein.
9. Geben Sie im Feld **Kennwort** das Kennwort für das Kalenderabonnement für die Authentifizierung auf dem Server des Dritthersteller-Kalenders ein.

10. Um zum Schutz der Übertragung von Ereignisdaten zwischen dem CalDAV-Server und dem mobilen Gerät das Transportprotokoll für den Datentransfer SSL zu verwenden, aktivieren Sie das Kontrollkästchen **SSL-Verbindung verwenden**.
11. Klicken Sie auf **OK**.
12. Das neue Kalenderabonnement wird in der Liste angezeigt.
13. Klicken Sie auf **Anwenden**, um die vorgenommenen Änderungen zu speichern.

Nach dem Anwenden der Richtlinie werden auf dem Mobilgerät des Nutzers Ereignisse aus den externen Kalendern aus der erstellten Liste hinzugefügt.

## Webclips hinzufügen

*Webclip* ist eine Anwendung, die eine Website vom Hauptbildschirm des iOS MDM-Mobilgeräts öffnet. Über die Symbole der Webclips auf dem Hauptbildschirm des Geräts kann der Benutzer schnell Websites öffnen (beispielsweise, die Unternehmenswebsite). Sie können Webclips auf die Nutzergeräte hinzufügen und das Aussehen des Webclipsymbols auf dem Bildschirm anpassen.

Standardmäßig werden folgende Beschränkungen bei der Verwendung von Webclips angewendet:

- Der Benutzer darf die Webclips nicht selbständig vom Mobilgerät entfernen.
- Websites, die beim Antippen des Webclipsymbols geöffnet werden, werden nicht auf gesamten Bildschirm angezeigt.
- Auf das Webclipsymbol werden die visuellen Effekte Abgerundete Ecken, Schatten und Glanz angewendet.

*Um auf dem iOS MDM-Gerät des Benutzers einen Webclip hinzuzufügen, gehen Sie wie folgt vor:*

1. Wählen Sie in der Konsolenstruktur im Ordner **Verwaltete Geräte** die Administrationsgruppe, zu der die iOS MDM-Geräte gehören.
2. Gehen Sie Im Arbeitsbereich der Gruppe auf die Registerkarte **Richtlinien**.
3. Öffnen Sie über Doppelklick das Eigenschaftfenster der Richtlinie.
4. Wählen Sie im Fenster **Eigenschaften <Name der Richtlinie>** den Abschnitt **Webclips**.
5. Klicken Sie im Abschnitt **Webclips** auf **Hinzufügen**.  
Das Fenster **Webclips** wird geöffnet.
6. Geben Sie im Feld **Name** den Namen des Webclips ein, der auf dem Hauptbildschirm des iOS MDM-Geräts angezeigt wird.
7. Geben Sie im Feld **Webadresse** die Adresse der Website ein, die beim Antippen des Webclips geöffnet wird. Die Adresse muss mit "http://" beginnen oder "https://" beginnen.
8. Um dem Benutzer das Löschen von Webclips vom iOS MDM-Gerät zu erlauben, aktivieren Sie das Kontrollkästchen **Löschen erlauben**.
9. Klicken Sie auf die Schaltfläche **Auswählen** und geben Sie die Datei mit dem Icon für das Webclipsymbol an.

Das Symbol wird auf dem Hauptbildschirm des iOS MDM-Geräts angezeigt. Das Icon muss folgende Anforderungen erfüllen:

- Icongröße beträgt maximal 400 x 400 Pixel.
- Datei im Format GIF, JPEG oder PNG.
- Dateigröße maximal 1 MB.

Das Webclipsymbol ist für die Vorschau im Feld **Symbol** verfügbar. Wenn Sie kein Bild für den Webclip auswählen, wird ein weißes Quadrat als Symbol angezeigt.

Wenn Sie möchten, dass das Webclipsymbol ohne spezielle visuelle Effekte (abgerundete Ecken und Glanz) angezeigt wird, aktivieren Sie das Kontrollkästchen **Webclip ohne visuelle Effekte**.

10. Wenn Sie möchten, dass beim Antippen des Websitesymbols die Website in der Vollbildansicht auf dem Bildschirm des iOS MDM-Geräts angezeigt wird, aktivieren Sie das Kontrollkästchen **Vollbild-Webclip**.

11. Klicken Sie auf **OK**.

Der neue Webclip wird in der Liste angezeigt.

12. Klicken Sie auf **Anwenden**, um die vorgenommenen Änderungen zu speichern.

Nach dem Anwenden der Richtlinie werden auf dem Mobilgerät des Nutzers Webclipsymbole aus der erstellten Liste hinzugefügt.

## Schriftarten hinzufügen

*Um eine Schriftart auf dem iOS MDM-Gerät hinzuzufügen, gehen Sie wie folgt vor:*

1. Wählen Sie in der Konsolenstruktur im Ordner **Verwaltete Geräte** die Administrationsgruppe, zu der die iOS MDM-Geräte gehören.
2. Gehen Sie Im Arbeitsbereich der Gruppe auf die Registerkarte **Richtlinien**.
3. Öffnen Sie über Doppelklick das Eigenschaftfenster der Richtlinie.
4. Wählen Sie im Fenster **Eigenschaften <Name der Richtlinie>** den Abschnitt **Schriften**.
5. Klicken Sie im Block **Schriften** auf **Hinzufügen**.  
Das Fenster **Schrift** wird geöffnet.
6. Geben Sie im Feld **Dateiname** den Pfad zur Schriftendatei (Datei mit der Erweiterung ttf oder otf).

Die Schriftarten mit der Erweiterung ttc oder otc werden nicht unterstützt.

Die Schriftarten werden über den Namen PostScript identifiziert. Installieren Sie keine Schriftarten mit dem gleichen PostScript-Namen, auch wenn sich ihr Inhalt unterscheidet. Die Installation von Schriftarten mit demselben PostScript-Namen führt zu einem unbekannten Fehler.

7. Klicken Sie auf **Öffnen**.

Die neue Schrift wird in der Liste angezeigt.

8. Klicken Sie auf **Anwenden**, um die vorgenommenen Änderungen zu speichern.

Nach dem Anwenden der Richtlinie wird dem Benutzer von der Anwendung vorgeschlagen, Schriften aus der erstellten Liste hinzuzufügen.

## App über EMM-Systeme von Drittanbietern verwalten (nur Android)

Die App Kaspersky Endpoint Security für Android kann ohne Kaspersky Administration Systems verwendet werden. Verwenden Sie Lösungen anderer EMM-Dienstanbieter (Enterprise Mobility Management), um Kaspersky Endpoint Security für Android bereitzustellen und zu verwalten. Damit die Anwendung zusammen mit EMM-Lösungen von Drittherstellern funktioniert, nimmt Kaspersky an der [AppConfig Community](#) teil.

Die Verwaltung der App Kaspersky Endpoint Security für Android mithilfe von externen EMM-Lösungen ist nur auf Geräten mit Android verfügbar.

Sie können EMM-Lösungen von Drittanbietern verwenden, um nur die App Kaspersky Endpoint Security für Android bereitzustellen. Verbinden Sie das Gerät mit Kaspersky Security Center und verwalten Sie die App über die Verwaltungskonsole. In diesem Fall ist die Verwaltung von Kaspersky Endpoint Security für Android über die EMM-Konsole nicht verfügbar.

Wenn Sie Kaspersky Endpoint Security für Android mithilfe des EMM-Systems eines Drittanbieters bereitgestellt haben, ist es nicht möglich, die App über Kaspersky Endpoint Security Cloud zu verwalten. Sie können Kaspersky Endpoint Security für Android über die EMM-Konsole verwalten.

Die folgenden EMM-Lösungen unterstützen die Verwendung von Kaspersky Endpoint Security für Android:

- VMware AirWatch
- MobileIron
- IBM Maas360
- Microsoft Intune
- SOTI MobiControl

In der EMM-Konsole können Sie folgende Aktionen ausführen:

- App im [Arbeitsprofil Android](#) auf den Geräten der Benutzer verteilen.
- App aktivieren.
- App-Einstellungen anpassen:
  - Den Schutz vor schädlichen Websites und Phishing-Websites im Internet aktivieren.
  - Die Einstellungen der Verbindung des Geräts mit Kaspersky Security Center anpassen.
  - Die Einstellungen von Anti-Virus anpassen.

- Den Zeitplan des Starts der Untersuchung des Geräts auf Viren anpassen.
- Adware sowie anderen Apps erkennen, die von Angreifern verwendet werden können, um ein Gerät oder Benutzerdaten zu beschädigen.
- Den Zeitplan des Updates der App-Datenbanken anpassen.

## Erste Schritte

Um die App auf den mobilen Geräten der Benutzer zu verteilen, muss Kaspersky Endpoint Security für Android zum EMM-App-Store hinzugefügt werden. Sie können Kaspersky Endpoint Security für Android mithilfe eines [Links zu Google Play](#) zum EMM-App-Store hinzufügen. Weitere Informationen zur Verwendung von App in der EMM-Konsole finden Sie auf der *Seite des technischen Supports des EMM-Diensteanbieters*.

Kaspersky Endpoint Security für Android wird im [Arbeitsprofil Android](#) verteilt. Die App ist von den persönlichen Daten des Benutzers isoliert und schützt nur die Unternehmensdaten im Arbeitsprofil. Es wird empfohlen, den Schutz von Kaspersky Endpoint Security für Android vor einer Deinstallation über die EMM-Konsole zu gewährleisten.

## So installieren Sie die App

Wählen Sie unter Berücksichtigung der EMM-Konsole eine Installationsmethode der App auf den Geräten aus: automatische Installation, Versand einer E-Mail-Nachricht mit einem Link zur App in Google Play, oder eine andere verfügbare Methode.

Die folgenden Berechtigungen sind für den Betrieb der App erforderlich:

- Berechtigung "Speicher" für den Zugriff auf Dateien während der Ausführung von Anti-Virus (nur für Android 6.0 und höher).
- Berechtigungen "Telefon" zur Identifizierung des Geräts, z.B. bei der Aktivierung der App.
- Anfrage auf das Hinzufügen von Kaspersky Endpoint Security für Android zur Liste mit Apps, die beim Hochfahren des Betriebssystems gestartet werden (auf einigen Geräten, z. B. Huawei, Meizu, Xiaomi). Wenn keine Anfrage auf das Hinzufügen angezeigt wird, fügen Sie Kaspersky Endpoint Security für Android manuell zur Autostart-Liste mit Apps hinzu. Die Anfrage wird eventuell nicht angezeigt, wenn im Arbeitsprofil die App "Sicherheit" nicht installiert ist.

Sie können die erforderlichen Berechtigungen in der EMM-Konsole erteilen, bevor Sie die App Kaspersky Endpoint Security für Android bereitstellen. Weitere Informationen zur Erteilung von Berechtigungen in der EMM-Konsole finden Sie auf der *Website des technischen Supports des EMM-Diensteanbieters*. Die Berechtigungen können auch während der Ausführung des Assistenten für die Erstkonfiguration von Kaspersky Endpoint Security für Android auf dem Gerät erteilt werden.

Die App Kaspersky Endpoint Security für Android wird im [Arbeitsprofil Android](#) installiert.

Für die Funktion von Web-Filter muss in den Einstellungen von Google Chrome ein Proxyserver eingerichtet werden:

- Modus der Einrichtung des Proxyservers: manuell.
- Adresse und Port des Proxyservers: 127.0.0.1:3128.

- Unterstützung des SPDY-Protokolls: deaktiviert.
- Datenkomprimierung durch den Proxyserver: deaktiviert.

## So aktivieren Sie die App

Die Informationen über die [Lizenz](#) werden zusammen mit den anderen Einstellungen in der [Konfigurationsdatei](#) an das mobile Gerät übermittelt.

Wenn die App nicht innerhalb von 30 Tagen ab dem Datum der Installation auf dem Mobilgerät aktiviert wird, läuft die Gültigkeitsdauer der Testlizenz ab. Nach Ablauf der Gültigkeitsdauer der Testlizenz stellt die mobile App Kaspersky Endpoint Security für Android die Funktion ein.

Nach Ablauf der Gültigkeitsdauer der kommerziellen Lizenz setzt die mobile App ihre Arbeit mit eingeschränkter Funktionalität fort (z. B. ist kein Datenbanken-Update und keine Nutzung des Dienstes Kaspersky Endpoint Security für Android möglich). Zur weiteren Nutzung der App mit allen Funktionen ist eine Verlängerung der kommerziellen Lizenz erforderlich.

*Um die Anwendung Kaspersky Endpoint Security für Android zu aktivieren, gehen Sie wie folgt vor:*

1. Öffnen Sie in der EMM-Konsole die Einstellungen von Kaspersky Endpoint Security für Android.
2. Geben Sie im Feld der Einstellung LicenseActivationCode [den Aktivierungscode der App](#) ein.

Zur Aktivierung der App auf dem Gerät wird Zugriff auf die Aktivierungsserver von Kaspersky benötigt.

## So verbinden Sie Ihr Gerät mit Kaspersky Security Center

Nach der Installation von Kaspersky Endpoint Security für Android auf Ihrem mobilen Gerät können Sie das Gerät mit Kaspersky Security Center verbinden. Die Informationen zur Verbindung des Geräts mit Kaspersky Security Center werden zusammen mit anderen Einstellungen, die in der [Konfigurationsdatei](#) angegeben sind, an das mobile Gerät übermittelt. Nachdem Sie das Gerät mit Kaspersky Security Center verbunden haben, können Sie die App-Einstellungen mithilfe von Gruppenrichtlinien zentral anpassen. Außerdem können Sie Berichte und Statistiken über die Ausführung von Kaspersky Endpoint Security für Android abrufen.

Bevor Sie Geräte mit Kaspersky Security Center verbinden, stellen Sie sicher, dass die folgenden Bedingungen erfüllt sind:

- Am Administrator-Arbeitsplatz [wurde das Verwaltungs-Plug-in für Kaspersky Endpoint Security für Android](#) installiert.
- In den Eigenschaften des Administrationsservers [wurde ein Port für die Verbindung von mobilen Geräten geöffnet](#).
- In der Verwaltungskontrolle wurde die [Anzeige des Ordners Mobile Geräte verwalten](#) aktiviert.
- Im Zertifikatsspeicher von Kaspersky Security Center [wurde ein allgemeines Zertifikat erstellt, mit dem der Benutzer des mobilen Geräts identifiziert werden kann](#).

Es wird empfohlen, die folgenden Aktionen auszuführen, bevor Sie Geräte mit Kaspersky Security Center verbinden:

- Wenn Sie Aufgaben und Richtlinien für mobile Geräte erstellen möchten, [erstellen Sie eine separate Administrationsgruppe](#) für mobile Geräte.
- Wenn Sie mobile Geräte automatisch in eine separate Administrationsgruppe verschieben möchten, [erstellen Sie eine Regel für das automatische Verschieben von Geräten](#) aus dem Ordner **Nicht zugeordnete Geräte**.
- Wenn Sie die Einstellungen von Kaspersky Endpoint Security für Android zentral konfigurieren möchten, [erstellen Sie eine Gruppenrichtlinie](#).

Um das Gerät mit Kaspersky Security Center zu verbinden, gehen Sie wie folgt vor:

1. Öffnen Sie in der EMM-Konsole die Einstellungen von Kaspersky Endpoint Security für Android.
2. Geben Sie im Feld KscServer den DNS-Namen oder die IP-Adresse des Kaspersky Security Center Administrationsservers ein. Der Standardport ist 13292.
3. Wenn Sie möchten, dass die Benutzer von mobilen Geräten nicht durch Benachrichtigungen von Kaspersky Endpoint Security für Android gestört werden, deaktivieren Sie die Benachrichtigungen der App. Setzen Sie dazu den Parameter `DisableNotification = True`.

Nach dem Herstellen der Verbindung zeigt die App alle Benachrichtigungen an. Sie können [einige Benachrichtigungen der App in den Richtlinieneinstellungen deaktivieren](#).

Deaktivieren Sie die Benachrichtigungen über die App-Ausführung nicht, wenn Sie Kaspersky Security Center nicht verwenden. Andernfalls können die Benutzer z. B. nicht über den Ablauf der Lizenz benachrichtigt werden. Als Ergebnis stellt die App sämtliche Funktionen ein.

Nach der Konfiguration der Verbindungseinstellungen zeigt Kaspersky Endpoint Security für Android eine Benachrichtigung an, in der sie die Erteilung der folgenden zusätzlichen Berechtigungen anfordert:

- Berechtigung "Kamera" für den Betrieb von Diebstahlschutz (Befehl **Foto aufnehmen**).
- Berechtigung "Standort" für den Betrieb von Diebstahlschutz (Befehl **Gerät orten**).
- Administratorrechte (Rechte des Besitzers des Android-Arbeitsprofils) für das Gerät zur Ausführung der folgenden App-Funktionen:
  - Installation von Sicherheitszertifikaten.
  - WLAN-Konfiguration.
  - Konfiguration von Exchange ActiveSync.
  - Beschränkung der Verwendung von Kamera, Bluetooth, WLAN.

Aufgrund der Besonderheiten des Android-Arbeitsprofils (da kein Dienst für erleichterte Bedienung vorhanden ist) sind die Anwendungskontrolle und der Diebstahlschutz nicht in der App verfügbar.

Sobald die Benutzer die erforderlichen Berechtigungen erteilen, werden ihre Geräte mit Kaspersky Security Center verbunden. Wenn keine Regel für das automatische Verschieben von Geräten in die Administrationsgruppe erstellt wurde, wird das Gerät automatisch zum Ordner **Nicht zugeordnete Geräte** hinzugefügt. Wenn eine Regel für das automatische Verschieben von Geräten in die Administrationsgruppe erstellt wurde, wird das Gerät automatisch zum angegebenen Ordner hinzugefügt.

Kaspersky Endpoint Security verwendet das folgende Format für Gerätenamen:

- Gerätemodell [E-Mail, Geräte-ID]
- Gerätemodell [E-Mail (falls vorhanden) oder Geräte-ID]

Die Geräte-ID ist eine eindeutige ID, die Kaspersky Endpoint Security für Android aus den vom Gerät empfangenen Daten generiert. Für mobile Geräte mit Android 10 und höher verwendet Kaspersky Endpoint Security für Android die SSAID (Android-ID) oder die Prüfsumme anderer vom Gerät empfangenen Daten. In früheren Android-Versionen verwendet die App die IMEI. Das [Format des Gerätenamens kann in der Gruppenrichtlinie angepasst werden](#). Außerdem kann dem Gerätenamen ein Tag hinzugefügt werden. Das erleichtert die Suche und das Filtern von Geräten in Kaspersky Security Center. Das Tag ist nur für VMware AirWatch verfügbar.

*So fügen Sie einem Gerätenamen ein Tag hinzu:*

1. Öffnen Sie in der EMM-Konsole die Einstellungen von Kaspersky Endpoint Security für Android.

2. Wählen Sie im Feld KscDeviceNameTag die folgenden Werte:

- {DeviceSerialNumber} – Seriennummer des Geräts.
- {DeviceUid} – eindeutige Geräteerkennung (UDID).
- {DeviceAssetNumber} – Anlagennummer des Geräts. Diese Nummer wird intern in Ihrem Unternehmen erzeugt.

Es wird empfohlen, nur diese Werte zu verwenden. VMware AirWatch unterstützt zwar auch andere Werte, aber wir können nicht garantieren, dass Kaspersky Endpoint Security mit diesen Werten funktioniert.

Sie können mehrere Werte hinzufügen (z. B. {DeviceSerialNumber} {DeviceUid}). Das Tag wird zum Gerätenamen in Kaspersky Security Center hinzugefügt. Ein Leerzeichen trennt Tag und Geräteiname. Zum Beispiel: Lautet der Geräteiname Google Pixel 2 a10c6b75f7b31de9 22:7D:78:9E:C5:1E, dann ist 22:7D:78:9E:C5:1E das UDID-Tag. Wenn Sie Kaspersky Security Center und VMware AirWatch verwenden, können Sie in beiden Konsolen Geräte anhand des Tags identifizieren. Um das Gerät abzugleichen, wählen Sie die gleichen Werte für den Gerätenamen (z. B. die Seriennummer des Geräts).

Sobald das Gerät mit Kaspersky Security Center verbunden ist, werden die App-Einstellungen gemäß der Gruppenrichtlinie geändert. Kaspersky Endpoint Security für Android ignoriert die App-Einstellungen in der Konfigurationsdatei, die über die EMM-Konsole angepasst wurden. Es können alle Bereiche der Richtlinie mit Ausnahme der folgenden konfiguriert werden:

- **Diebstahlschutz** (Gerätesperre)
- **Container**
- **Geräteverwaltung** (Bildschirmsperre)
- **Anwendungskontrolle** (Sperren von verbotenen Apps)
- **Arbeitsprofil Android**
- **Samsung KNOX verwalten**



Aufgrund der Besonderheiten bei der Bereitstellung des Arbeitsprofils können die Einstellungen der Gruppenrichtlinie aus dem Abschnitt **Arbeitsprofil Android** nicht angewendet werden. Diese Einstellungen können nur angewendet werden, wenn das Arbeitsprofil mithilfe von Kaspersky Security Center erstellt wurde.

## Datei AppConfig

In einer EMM-Konsole wird eine Konfigurationsdatei erstellt, mit deren Hilfe die App konfiguriert wird. Die in der Konfigurationsdatei enthaltenen App-Einstellungen finden Sie in der nachfolgenden Tabelle.

Einstellungen der Konfigurationsdatei

Konfigurationsschlüssel	Beschreibung	Typ	Wert
LicenseActivationCode	Aktivierungscode der App	String	<p>Aktivierungscode aus zwanzig lateinischen Buchstaben und Ziffern. Die Aktivierung der App mithilfe eines Aktivierungscodes ist ein Internet-Verbindungsprozess, der erforderlich ist, um eine Verbindung mit den Aktivierungsservern von Kaspersky herzustellen.</p> <p>Bleibt das Feld leer, so wird die App eine Testlizenz aktiviert. Die Testlizenz ist 30 Tage gültig. Nach Ablauf der Gültigkeitsdauer der Testlizenz stoppt die mobile App Kaspersky Endpoint Security für Android die Funktion ein. Um die App weiter nutzen zu können, müssen Sie eine kommerzielle Lizenz erwerben.</p>
EulaAcceptanceConfirmationV1	<Link für die Annahme des Lizenzvertrags>	Choice	<div> <p>Diese Einstellung ist nur für VM AirWatch verfügbar.</p> <p>Accepted – Ich bestätige, dass ich die Bedingungen und Bestimmungen des Endbenutzer-Lizenzvertrags vollständig gelesen habe, sie verstehe und akzeptiere.</p> <p>Declined – Ich lehne die Bedingungen und Bestimmungen dieses Endbenutzer-Lizenzvertrags (EULA) ab.</p> <p>Internetzugang ist erforderlich, um eine Verbindung zu den Kaspersky-Servern herzustellen und die Bedingungen und Bestimmungen des EULA für alle Geräte zu akzeptieren.</p> <p>Wenn Sie Declined gewählt haben, fordert die App den Benutzer auf, die Bedingungen des EULA zu akzeptieren. Die Benutzer des mobilen Geräts müssen die Bedingungen im Assistenten für die Erstkonfiguration akzeptieren.</p> </div>

EulaAcceptanceCodeV1	Code des Lizenzvertrags	String	<p>Diese Einstellungen sind nur für VMware AirWatch verfügbar.</p>
EulaAcceptanceCodesV2	Codes für den Endbenutzer-Lizenzvertrag	String	
			<p>Verwenden Sie <code>EulaAcceptanceCodeV1</code>, wenn einen einzelnen Endbenutzer-Lizenzvertrag (EULA) akzeptieren möchten. Verwenden Sie <code>EulaAcceptanceCodesV2</code>, wenn mehrere EULAs gleichzeitig akzeptieren möchten. Das Feld <code>EulaAcceptanceCodesV2</code> muss durch Semikolons getrennte Liste EULA-Codes enthalten: "<code>&lt;EULAid1&gt;;&lt;EULAid2&gt;;&lt;EULAid3&gt;;...</code>".</p> <p>Der Code des Endbenutzer-Lizenzvertrags befindet sich im Endbenutzer-Lizenzvertrag.</p> <p><i>So zeigen Sie den Code des Lizenzvertrags an:</i></p> <ol style="list-style-type: none"> <li>1. Kopieren Sie den Link des Lizenzvertrags (<code>EulaAcceptanceConfirmation</code>) in der EMM-Konsole.</li> <li>2. Fügen Sie den Link im Browser. Der Endbenutzer-Lizenzvertrag (EULA) wird geöffnet.</li> <li>3. Lesen Sie sich die Bedingungen und Bestimmungen des EULA durch. Finden Sie den Code des Lizenzvertrags. Internetzugang ist erforderlich, um eine Verbindung zu den Kaspersky Servern herzustellen und die Bedingungen und Bestimmungen der EULAs für alle mobilen Geräte akzeptieren.</li> </ol> <p>Wenn Sie diese Felder leer lassen, fordert die App den Benutzer auf, die Bedingungen der EULAs zu akzeptieren. Der Benutzer des mobilen Geräts akzeptiert die Bedingungen im Assistenten für die Erstkonfiguration.</p> <p>Wenn Sie die Werte beider Felder angeben, werden die Bedingungen der EULAs, die in den Feldern angegeben sind, akzeptiert.</p>
KscServer	Adresse und Port des Administrationsservers von Kaspersky Security Center	String	<p>DNS-Name oder IP-Adresse des Administrationsservers für Kaspersky Security Center und Portnummer. Geben Sie die Adresse wie folgt an:</p>

			<Serveradresse>: <port>. Wenn keine Serveradresse ohne Port angegeben wird, wird der Standardport 13292 verwendet.
DisableNotification	Benachrichtigungen der App deaktivieren, solange keine Verbindung zu Kaspersky Security Center besteht	Boolean	<p>True – Kaspersky Endpoint Security für Android blendet alle Benachrichtigungen über die App-Ausführung aus. Kaspersky Endpoint Security für Android blendet Benachrichtigungen aus, solange das Gerät nicht mit Kaspersky Security Center verbunden ist. Nach dem Herstellen der Verbindung zeigt das Gerät alle Benachrichtigungen an. Sie können <a href="#">einige Benachrichtigungen der App deaktivieren</a> und die Richtlinieneinstellungen deaktivieren.</p> <p>False – Kaspersky Endpoint Security für Android zeigt alle Benachrichtigungen über die App-Ausführung an.</p>
ScanScheduleType	Startmodus für die Untersuchung	Choice	<p>AfterUpdate – Start der Untersuchung auf Viren nach dem Datenbank-Update. Die App aktualisiert die Antiviren-Datenbanken gemäß dem festgelegten Zeitplan (UpdateScheduleType).</p> <p>Daily – Start der Untersuchung Viren einmal täglich. Passen Sie die Uhrzeit für den Untersuchungsstart (ScanScheduleTime) an.</p> <p>Weekly – Start der Untersuchung Viren einmal wöchentlich. Wählen Sie den Wochentag für den Start der Untersuchung auf Viren (ScanScheduleDay) und passen Sie die Uhrzeit an (ScanScheduleTime).</p> <p>Off – der automatische Start der Untersuchung auf Viren ist deaktiviert. Der Benutzer des Geräts kann unabhängig vom festgelegten Wochentag eine manuelle Untersuchung auf Viren starten.</p>
ScanScheduleDay	Tag für den Untersuchungsstart	Choice	Monday / Tuesday / Wednesday / Thursday / Friday / Saturday / Sunday

			<p>Sunday</p> <p>Sie können nur einen Wert auswä</p>
ScanScheduleTime	Uhrzeit für den Untersuchungsstart	String	<p>Uhrzeit im 24-Stunden-Format (z. B. 13:00) oder im 12-Stunden-Format (z. B. 10.30 pm).</p>
ScanScheduleLock	Die Anpassung des Startmodus der Untersuchung verbieten	Boolean	<p>True – der Benutzer kann nicht die Einstellungen des Startmodus der Untersuchung auf Viren in den App-Einstellungen zugreifen.</p> <p>False – der Benutzer kann den Startmodus der Untersuchung anpassen und z. B. den automatisierten Start der Untersuchung auf Viren deaktivieren.</p>
ScanOnlyExecutableFiles	Typen der Dateien für die Untersuchung (Untersuchung auf Viren)	Choice	<p>AllFiles – Untersuchung aller Dateien</p> <p>OnlyExecutables – Untersuchung nur ausführbarer Dateien. Zu den ausführbaren Dateien gehören Dateien mit den Erweiterungen apk (zip), etc.</p> <p>In Kaspersky Endpoint Security für Android Service Pack 4 Maintenance Release 1 ist es unmöglich, die Untersuchung nur von ausführbaren Dateien zu aktivieren.</p>
ScanArchives	Archive mit Entpackern untersuchen	Boolean	<p>True – die App entpackt Archive und untersucht ihre Inhalte.</p> <p>False – die App untersucht nur Archivdateien.</p> <p>Die App untersucht nur Archive mit der Erweiterung zip (apk).</p> <p>In Kaspersky Endpoint Security für Android Service Pack 4 Maintenance Release 1 ist es nicht möglich, die Untersuchung von Archiven zu deaktivieren.</p>
ScanActionOnThreatFound	Aktion beim Fund einer Bedrohung (Untersuchung auf Viren)	Choice	<p>Quarantine – die App verschiebt gefundene Objekte in die Quarantäne. Die Quarantäne speichert diese Objekte in komprimierter Form, um eine Beschädigung des Geräts auszuschließen. Die Quarantäne ermöglicht das Löschen oder Wiederherstellen von Dateien in einem speziellen isolierten Speicher.</p> <p>Delete – die App löscht gefundene Objekte.</p>

			<p>Skip – die App verändert die gefundenen Objekte nicht. Wenn gefundene Objekte übersprungen wurden, warnt Kaspersky Endpoir Security für Android den Benutzer. Problemen beim Schutz des Geräts. Beim Versuch, auf dem Gerät auf ein Objekt zuzugreifen (z. B. Kopieren, Öffnen), blockiert die Anwendung den Zugriff darauf.</p> <p>AskUser – die App fordert den Benutzer auf, für jedes gefundene Objekt eine Aktion auszuwählen: überspringen, in die Quarantäne verschieben oder löschen. Beim Fund mehrerer Objekte kann der Benutzer die ausgewählte Aktion auf alle Objekte anwenden.</p> <p>Die App speichert die Informationen über die gefundenen Bedrohungen und die ausgeführten Aktionen in den Berichten der App.</p>
ScanLock	Anpassung der Einstellungen der Untersuchung verbieten	Boolean	<p>True – der Benutzer kann nicht auf die Einstellungen der Untersuchung zugreifen: Typ der zu untersuchenden Dateien, Untersuchung von Archivdateien, Aktion beim Fund einer Bedrohung.</p> <p>False – der Benutzer kann die Einstellungen der Untersuchung anpassen und z. B. die Aktion Skip beim Fund der Bedrohung auswählen.</p>
ScanAndProtectionAdwareRiskware	Adware, Autodialer und Apps blockieren, die Angreifer verwenden können, um das Gerät und die Daten des Benutzers zu beschädigen	Boolean	<p>True – die App erkennt Adware und andere Apps, die Angreifer verwenden können, um das Gerät und die Daten des Benutzers zu beschädigen.</p> <p>False – die App überspringt Adware und andere Apps, die Angreifer verwenden können, um das Gerät und die Daten des Benutzers zu beschädigen.</p>
ProtectionMode	Echtzeitschutz-Modus	Choice	<p>Recommended – die App untersucht neue Apps einmal sofort nach ihrer Installation sowie Dateien aus dem Download-Ordner.</p> <p>Extended – die App untersucht Dateien, die der Benutzer auf dem Gerät öffnet, bearbeitet, kopiert, ausführt oder speichert. Außerdem untersucht sie neue Apps und Dateien im Download-Ordner.</p> <p>Disabled – der Echtzeitschutz ist deaktiviert.</p>
UseKsnMode	Modus Kaspersky Security Network	Choice	<p>Recommended – die App tauscht Informationen mit <a href="#">Kaspersky Security Network</a> (KSN).</p>

			<p>aus. Kaspersky Endpoint Security Android verwendet KSN für den Echtzeitschutz des Geräts vor Bedrohungen (Cloud-Sicherheit) die Funktion von Web-Filter im In</p> <p>Extended – die App tauscht Dat <a href="#">Kaspersky Security Network</a> aus sendet zusätzlich bestimmte Sta über die Ausführung von Kaspers Endpoint Security für Android an Virenlabor. Mithilfe dieser Informa können Bedrohungen in Echtzeit werden. Durch die Dienste von KS erfolgt keinerlei Erfassung, Verark oder Speicherung von persönlich Daten des Benutzers.</p> <p>Disabled – die App verwendet l Daten von <a href="#">Kaspersky Security Ne</a> Es ist nicht möglich, Web-Filter (EnableWebFilter) zu aktiviere Komponente "Cloud-Sicherheit" i Anti-Virus nicht verfügbar.</p>
ProtectScanOnlyExecutableFiles	Typen der Dateien für die Untersuchung (Echtzeitschutz)	Boolean	<p>AllFiles – Untersuchung aller [</p> <p>OnlyExecutables – Untersucht nur ausführbaren Dateien. Zu den ausführbaren Dateien gehören De mit den Erweiterungen apk (zip), c</p> <p>In Kaspersky Endpoint Security fi Android Service Pack 4 Maintena Release 1 ist es unmöglich, die Untersuchung nur von ausführbar Dateien zu aktivieren.</p>
ProtectionActionOnThreatFound	Aktion beim Fund einer Bedrohung (Echtzeitschutz)	Choice	<p>Quarantine – die App verschiebt gefundene Objekte in die Quarantäne. Die Quarantäne speichert diese [ in komprimierter Form, um eine Beschädigung des Geräts auszuschließen. Die Quarantäne ermöglicht das Löschen oder Wiederherstellen von Dateien in e speziellen isolierten Speicher.</p> <p>Delete – die App löscht gefundene Objekte.</p> <p>Skip – die App verändert die gefundenen Objekte nicht. Wenn gefundene Objekte übersprungen wurden, warnt Kaspersky Endpoint Security für Android den Benutzer Problemen beim Schutz des Geräts. Beim Versuch, auf dem Gerät auf Objekt zuzugreifen (z. B. Kopieren, Öffnen), blockiert die App den Zugriff darauf.</p>

			Die App speichert die Information über die gefundenen Bedrohungen, die ausgeführten Aktionen in den Berichten der App.
ProtectionLock	Anpassung der Einstellungen des Echtzeitschutzes verbieten	Boolean	<p>True – der Benutzer kann nicht auf die folgenden Einstellungen des Echtzeitschutzes zugreifen: Echtzeitschutz-Modus, Typ der zu untersuchenden Dateien, Aktion Fund einer Bedrohung.</p> <p>False – der Benutzer kann die Einstellungen des Echtzeitschutz anpassen und z. B. die Aktion Skifund der Bedrohung auswählen.</p>
UpdateScheduleType	Startmodus für das Datenbanken-Update	Choice	<p>Daily – das Vorhandensein von Antiviren-Datenbanken wird einmal täglich geprüft, ihr Download auf Geräte erfolgt einmal täglich. Passen Sie die Startzeit des Datenbanken-Updates (UpdateScheduleTime) an.</p> <p>Weekly – das Vorhandensein von Antiviren-Datenbanken wird einmal wöchentlich geprüft, ihr Download auf die Geräte erfolgt einmal wöchentlich. Wählen Sie den Wochentag für den Start des Datenbanken-Updates (UpdateScheduleDay) und passen Sie die Uhrzeit an (UpdateScheduleTime).</p> <p>Off – das automatische Update der Antiviren-Datenbanken ist deaktiviert.</p> <p>Der Benutzer des Geräts kann unabhängig vom festgelegten Wochentag ein manuelles Update der Antiviren-Datenbanken starten.</p>
UpdateScheduleDay	Starttag für das Datenbanken-Update	Choice	<p>Monday / Tuesday / Wednesday / Thursday / Friday / Saturday / Sunday</p> <p>Sie können nur einen Wert auswählen.</p>
UpdateScheduleTime	Startzeit für das Datenbanken-Update	String	Uhrzeit im 24-Stunden-Format (z. B. 13:00) oder im 12-Stunden-Format (z. B. 10.30 pm).
UpdateScheduleLock	Die Anpassung des Startmodus des Datenbanken-Updates verbieten	Boolean	<p>True – der Benutzer kann nicht auf die Einstellungen des Startmodus des Datenbanken-Updates in den App-Einstellungen zugreifen.</p> <p>False – der Benutzer kann den Startmodus des Datenbanken-Updates anpassen und z. B. den automatisierten Start des Updates der Antiviren-Datenbanken deaktivieren.</p>
AllowUpdateInRoaming	Datenbanken-Update beim Roaming erlauben	Boolean	True – die App lädt Antiviren-Datenbanken herunter, wenn das Gerät sich in einer Roaming-Zone befindet.

			<p>App lädt die Antiviren-Datenbank gemäß dem festgelegten Zeitplan (UpdateScheduleType) herunter.</p> <p>False – die App lädt Antiviren-Datenbanken nur dann herunter, wenn das Gerät sich im Heimnetz befindet.</p>
EnableWebFilter	Web-Filter	Boolean	<p>True – die App blockiert böartige Websites und Phishing-Websites Internet mithilfe der Komponente Filter. Der Web-Filter funktioniert Google Chrome.</p> <div style="background-color: #f8d7da; padding: 10px; margin: 10px 0;"> <p>Bösartige Websites und Phishing-Websites, die das HTTPS-Protokoll nutzen, bleiben von der Blockierung ausgeschlossen, wenn die Domain vertrauenswürdig ist. Wenn die Domain nicht vertrauenswürdig ist, blockiert Web-Filter böartige Websites und Phishing-Websites.</p> </div> <p>False – der Schutz vor schädlichen Websites und Phishing-Websites deaktiviert.</p> <p>Für die Funktion von Web-Filter müssen folgende Bedingungen erfüllt sein:</p> <ul style="list-style-type: none"> <li>• Gerätebenutzer akzeptieren die Datenschutzrichtlinie und die Erklärung für Web-Filter im Assistenten für die Erstkonfiguration oder in den App-Einstellungen</li> <li>• In den Einstellungen des Browsers ein Proxyserver eingerichtet:  ProxyMode = "fixed_service" ProxyServer = "127.0.0.1:3128" DisableSpdy = true DataCompressionProxyEnabled = false Die Konfiguration des Proxyserver kann je nach Google Chrome variieren. Weitere Informationen zu den Einstellungen von Google Chrome finden Sie auf <a href="#">der Website des Projekts Chromium</a>.  Setzen Sie nach dem Löschen der App Kaspersky Endpoint Security für Android vom mobilen Gerät die Einstellungen des Proxyserver zurück.</li> <li>• In den Einstellungen der App ist die Nutzung von KSN aktiviert:</li> </ul>



			<p>UseKsnMode = Recommend UseKsnMode = Extended.</p> <ul style="list-style-type: none"> <li>Es wird empfohlen, in den Einstellungen des Betriebssystems Google Chrome als Standardbrowser auszuwählen.</li> </ul>
EnableWebFilterLock	Anpassung von Web-Filter verbieten	Boolean	<p>True – der Benutzer kann nicht die Einstellungen von Web-Filter in den Einstellungen zugreifen.</p> <p>False – der Benutzer kann die Einstellungen von Web-Filter anpassen und z. B. den Schutz vor schädlichen Websites und Phishing-Websites im Internet deaktivieren.</p>
UpdateServer	Adresse des Servers, der als Quelle für das Datenbanken-Update dient	String	<p>Die Adresse des Servers, der als Quelle für das Datenbanken-Update dient: <code>http://update.server.com</code>.</p> <p>Bleibt das Feld leer, so verwendet Kaspersky Endpoint Security für die Kaspersky-Update-Server.</p>
AllowGoogleAnalytics	Daten übermitteln an die Dienste Google Analytics for Firebase, SafetyNet Attestation, Firebase Performance Monitoring und Crashlytics	Boolean	<p>True – Die App übermittelt automatisch Betriebsdaten von Kaspersky Endpoint Security für Android an die Dienste Google Analytics for Firebase, SafetyNet Attestation, Firebase Performance Monitoring und Crashlytics. Die Daten sind für die Verbesserung der App-Ausführung und die Analyse der Benutzerzufriedenheit erforderlich. Die Übermittlung von Daten an Google Analytics für Firebase, SafetyNet Attestation, Firebase Performance Monitoring und Crashlytics erfolgt über eine sichere Verbindung. Der Zugriff auf die Daten und ihr Schutz sind gemäß den entsprechenden Nutzungsbedingungen von Google Analytics für Firebase, SafetyNet Attestation, Firebase Performance Monitoring und Crashlytics geschützt.</p> <p>False – Die Übermittlung von Daten an die Dienste Google Analytics for Firebase, SafetyNet Attestation, Firebase Performance Monitoring und Crashlytics ist deaktiviert.</p>
KscDeviceNameTag	Tag des Gerätenamens für Kaspersky Security Center	String	<div>Diese Einstellung ist nur für VMs mit AirWatch verfügbar.</div>



Der String muss eine gültige E-Mail-Adresse sein. Andere Werte werden ignoriert.

## Netzwerkbelastung

Dieser Abschnitt enthält Informationen über den Umfang des Netzwerkverkehrs, der zwischen den mobilen Geräten und Kaspersky Security Center während der Programmausführung aufkommt.

### Datenverkehr

Aufgabe	Ausgehender Datenverkehr	Eingehender Datenverkehr	Gesamter Datenverkehr
Ursprüngliche Verteilung der App, MB	0,08	17,76	17,84
Ursprüngliches Update der Antiviren-Datenbanken (der Umfang des Datenverkehrs kann sich aufgrund der Größe der Antiviren-Datenbanken unterscheiden), MB	0,04	2,21	2,25
Synchronisierung des mobilen Geräts mit Kaspersky Security Center, MB	0,03	0,02	0,05
Regelmäßiges Update der Antiviren-Datenbanken (der Umfang des Datenverkehrs kann sich aufgrund der Größe der Antiviren-Datenbanken unterscheiden), MB	0,08	3,06	3,14
Ausführung der Diebstahlschutz-Befehle. Gerät orten (der Umfang des Datenverkehrs kann sich aufgrund der Merkmale der integrierten Kamera und der Bildqualität unterscheiden), MB	0,09	0,8	0,17
Ausführung der Diebstahlschutz-Befehle. Foto aufnehmen, MB	1,0	0,02	1,02
Ausführung der Diebstahlschutz-Befehle. Gerät sperren, MB	0,06	0,05	0,11
Mittlerer Verbrauch in 24 Stunden, MB	0,22	6,96	7,18

## Teilnahme am Kaspersky Security Network

Um die Effektivität des Schutzes von mobilen Geräten zu erhöhen, verwendet Kaspersky Endpoint Security für Android die von Benutzern aus aller Welt übermittelten Daten. Zur Verarbeitung dieser Daten dient das Netzwerk *Kaspersky Security Network*.

*Kaspersky Security Network (KSN)* ist eine Infrastruktur von Cloud-Diensten, die Zugriff auf eine aktuelle Wissensdatenbank von Kaspersky bietet. Diese Datenbank enthält Informationen zur Reputation von Dateien, Webressourcen und Programmen. Die Nutzung der Daten aus dem Kaspersky Security Network gewährleistet eine höhere Reaktionsschnelligkeit der Kaspersky-Programme auf Bedrohungen, erhöht die Effektivität vieler Schutzkomponenten und verringert die Wahrscheinlichkeit von Fehlalarmen.

Ihre Teilnahme am Kaspersky Security Network ermöglicht Kaspersky, schnell Informationen über Typen und Quellen neuer Bedrohungen zu erhalten, Neutralisierungsmethoden zu entwickeln und die Anzahl an Fehlalarmen von Kaspersky Endpoint Security für Android zu reduzieren. Darüber hinaus erhalten Sie durch die Teilnahme am Kaspersky Security Network Zugriff auf die Reputationsdatenbanken für Programme und Websites.

Wenn Sie an Kaspersky Security Network teilnehmen, werden bestimmte Statistikdaten, die während der Ausführung von Kaspersky Endpoint Security für Android auf dem Computer des Benutzers gesammelt werden, [automatisch an Kaspersky übermittelt](#). Mithilfe dieser Informationen können Bedrohungen in Echtzeit verfolgt werden. Für eine zusätzliche Untersuchung können außerdem Dateien (oder Dateiteile) an Kaspersky geschickt werden, die von Angreifern zur Beschädigung des Computers oder der Benutzerdaten verwendet werden können.

Die Verwendung von Kaspersky Security Network ist eine Voraussetzung für die Ausführung von Kaspersky Endpoint Security für Android. KSN wird für die Funktion der Hauptkomponenten der Anwendung verwendet: Anti-Virus, Web-Filter und Programmkontrolle. Die Ablehnung der Teilnahme an KSN reduziert das Schutzniveau des Geräts, was zur Infektion des Geräts und dem Verlust der Informationen führen kann. Um mit der Nutzung von Kaspersky Security Network beginnen zu können, müssen Sie während der Installation der Anwendung die Bedingungen des Endbenutzer-Lizenzvertrags akzeptieren. Im Endbenutzer-Lizenzvertrag finden Sie Informationen darüber, welche Daten Kaspersky Endpoint Security für Android an Kaspersky Security Network übermittelt.

Um die Funktion der Anwendung zu optimieren, können Sie zusätzlich statistische Daten an Kaspersky Security Network übermitteln. Die Teilnahme an Kaspersky Security Network zur Verarbeitung von statistischen Daten ist freiwillig. Um mit der Nutzung von Kaspersky Security Network beginnen zu können, müssen Sie die Bedingungen einer speziellen Vereinbarung, der *Vereinbarung zum Kaspersky Security Network* akzeptieren. Sie können jederzeit die [Teilnahme am Kaspersky Security Network beenden](#). In der KSN-Vereinbarung finden Sie Informationen darüber, welche Daten Kaspersky Endpoint Security für Android an Kaspersky Security Network übermittelt.

## Informationsaustausch mit dem Kaspersky Security Network

Zur Erhöhung des Niveaus des operativen Schutzes verwendet Kaspersky Security für mobile Endgeräte den Cloud-Dienst Kaspersky Security Network für die Ausführung folgender Komponenten:

- [Anti-Virus](#). Die App erhält Zugriff auf die operative Wissensdatenbank von Kaspersky, welche die Reputationen von Dateien und Apps enthält. Bei der Untersuchung werden Bedrohungen gesucht, die schon in KSN eingetragen sind, auch wenn über sie noch keine Informationen in den Antiviren-Datenbanken vorhanden sind. Der Cloud-Dienst Kaspersky Security Network gewährleistet die uneingeschränkte Funktion von Anti-Virus und reduziert die Wahrscheinlichkeit von Fehlalarmen.
- [Web-Filter](#). Die App führt eine Untersuchung von Websites vor ihrem Öffnen durch und berücksichtigt dabei Daten, die von KSN übermittelt werden. Außerdem bestimmt die App auf Grundlage von Listen mit erlaubten und verbotenen Kategorien die Kategorie von Websites, um den Internetzugriff der Benutzer zu kontrollieren (z. B. Kategorie "Kommunikation im Internet").
- [Anwendungskontrolle](#). Die App bestimmt auf Grundlage von Listen mit erlaubten und verbotenen Kategorien (z. B. Kategorie "Spiele") die App-Kategorie, um den Start von Apps zu beschränken, die nicht den Anforderungen an die Unternehmenssicherheit genügen.

Informationen zu den Daten, die bei der Nutzung von KSN während der Ausführung von Anti-Virus und Anwendungskontrolle an Kaspersky übertragen werden, finden Sie im Endbenutzer-Lizenzvertrag. Indem Sie die Lizenzvereinbarung akzeptieren, stimmen Sie zu, dass diese Informationen übertragen werden.

Informationen zu den Daten, die bei der Nutzung von KSN während der Ausführung von Web-Filter an Kaspersky übertragen werden, finden Sie in der Erklärung für die Datenverarbeitung für Web-Filter. Indem Sie die Erklärung akzeptieren, stimmen Sie zu, dass diese Informationen übertragen werden.

Sie können die Teilnahme an Kaspersky Security Network zwecks Aufspürung neuer und schwer erkennbarer Bedrohungen und ihrer Quellen sowie Bedrohungen durch Angriffe und zwecks Erhöhung des Schutzniveaus für Daten, die auf dem Gerät gespeichert und verarbeitet werden, erweitern.

Zum Austausch von Daten mit KSN, um die Qualität der App zu verbessern, müssen die folgenden Bedingungen erfüllt sein:

- Sie oder der Benutzer des Geräts müssen die Bedingungen der Erklärung zu Kaspersky Security Network lesen und akzeptieren. Wenn Sie bestimmen, dass die Erklärung von den Benutzern akzeptiert werden soll, werden diese in Form einer Mitteilung im Hauptfenster der App aufgefordert, die Bedingungen der Erklärung zu akzeptieren. Benutzer können die Erklärungen auch im Block **Über die App** in den Einstellungen von Kaspersky Endpoint Security für Android akzeptieren.

Wenn Sie die Erklärungen global akzeptieren, müssen die Versionen der über Kaspersky Security Center akzeptierten Erklärungen mit den bereits von den Benutzern akzeptierten Versionen übereinstimmen. Andernfalls werden die Benutzer über das Problem informiert und aufgefordert, die Version einer Erklärung zu akzeptieren, die der vom Administrator global akzeptierten Version entspricht. Außerdem ändert sich der Gerätestatus im Plug-in "Kaspersky Security for Mobile (Devices)" in *Warnung*.

- Sie müssen die Übermittlung [statistischer Daten an KSN in den Einstellungen der Gruppenrichtlinie erlauben](#) (siehe unten).

Sie können den Versand von statistischen Daten an KSN jederzeit ablehnen. Informationen zu den statistischen Daten, die bei der Nutzung von KSN während der Ausführung der mobilen App Kaspersky Endpoint Security für Android auf den mobilen Geräten an Kaspersky übertragen werden, finden Sie in der Erklärung zu Kaspersky Security Network.

Weitere Informationen über die Bereitstellung von Daten an KSN finden Sie im Abschnitt [Datenbereitstellung](#).

Die Bereitstellung von Daten an KSN ist freiwillig. Wenn Sie möchten, können Sie [den Datenaustausch mit KSN deaktivieren](#).

## Verwendung von Kaspersky Security Network aktivieren und deaktivieren

Damit [Komponenten von Kaspersky Endpoint Security für Android, die Kaspersky Security Network verwenden](#), ausgeführt werden können, sendet die App Anfragen an den Cloud-Dienst. Die Anfragen enthalten die im Abschnitt [Datenbereitstellung](#) beschriebenen Daten.

Wenn die Verwendung von Kaspersky Security Network auf dem Gerät deaktiviert ist, werden die Komponenten "Cloud-Sicherheit", "Web-Filter" und "Anwendungskontrolle" automatisch deaktiviert.

*Gehen Sie folgendermaßen vor, um die Nutzung von Kaspersky Security Network zu aktivieren oder zu deaktivieren:*

1. Öffnen Sie das Fenster zur Konfiguration der Einstellungen der Richtlinie zur Verwaltung von mobilen Geräte, auf denen Kaspersky Endpoint Security für Android installiert ist.
2. Wählen Sie im folgenden Fenster **Eigenschaften <Name der Richtlinie>** den Abschnitt **Erweitert** aus.
3. Passen Sie im Block **Einstellungen für Kaspersky Security Network (KSN)** die Nutzung von Kaspersky Security Network an:
  - Aktivieren Sie das Kontrollkästchen **Kaspersky Security Network verwenden**, damit folgende Komponenten ausgeführt werden können: Anti-Virus (Cloud-Sicherheit), Web-Filter, Anwendungskontrolle (App-Kategorien).

- Aktivieren Sie das Kontrollkästchen **Übermittlung von Statistikdaten an KSN erlauben**, um Daten an Kaspersky zu übermitteln. Mithilfe dieser Daten kann Kaspersky Endpoint Security für Android schneller auf Bedrohungen reagieren, die Leistung der Schutzkomponenten verbessern und die Wahrscheinlichkeit von Fehlalarmen reduzieren.

4. Klicken Sie auf **Anwenden**, um die vorgenommenen Änderungen zu speichern.

Die Einstellungen werden nach der nächsten planmäßigen Synchronisierung des Geräts mit Kaspersky Security Center auf dem mobilen Gerät konfiguriert. Nach der Annahme der Richtlinie werden die Komponenten, in denen Kaspersky Security Network verwendet wird, deaktiviert und eine Konfiguration dieser Komponenten ist nicht mehr möglich.

## Kaspersky Private Security Network verwenden

*Kaspersky Private Security Network* (im Folgenden auch als *Private KSN* oder *KPSN* bezeichnet) ist eine Lösung, die den Zugriff auf die Reputationsdatenbanken von Kaspersky Security Network gewährt, ohne Daten von den Geräten der Benutzer an Kaspersky Security Network zu senden.

Eine Datenbank mit der Reputation von Objekten (Dateien oder URLs) wird auf dem Server von Kaspersky Private Security Network gespeichert, nicht jedoch auf den Servern von Kaspersky Security Network. Die KPSN-Reputationsdatenbanken werden im Unternehmensnetzwerk gespeichert und vom Unternehmensadministrator verwaltet.

Wenn KPSN aktiviert ist, sendet Kaspersky Endpoint Security keine statistischen Daten von den Geräten der Benutzer an KSN.

*So aktivieren Sie die Verwendung von Private KSN über Kaspersky Security Center:*

1. Klicken Sie im Hauptfenster von Kaspersky Security Center Web Console oder Cloud Console auf **Einstellungen** (⚙️).

Das Eigenschaftfenster des Administrationsservers wird geöffnet.

2. Wählen Sie auf der Registerkarte **Allgemein** den Abschnitt **KSN-Proxy-Einstellungen** aus.
3. Setzen Sie den Schalter in die Position **Kaspersky Private Security Network verwenden AKTIVIERT**.
4. Klicken Sie auf die Schaltfläche **Datei mit KSN-Proxy-Einstellungen auswählen** und suchen Sie nach der Konfigurationsdatei mit der Erweiterung pkcs7 oder pem (von Kaspersky bereitgestellt).
5. Klicken Sie auf **Öffnen**.
6. Wenn Sie die Proxyserver-Einstellungen in den Eigenschaften des Administrationsservers angepasst haben, aber Ihre Netzwerkarchitektur eine direkte Verwendung von Private KSN erfordert, aktivieren Sie die Option **KSC-Proxyserver-Einstellungen beim Verbinden zu Private KSN ignorieren**. Andernfalls können Anfragen von den verwalteten Apps Private KSN nicht erreichen.
7. Klicken Sie auf **Speichern**.

Nach dem Download der Einstellungen werden in der Benutzeroberfläche der Name des Providers, die Kontaktdaten des Providers und das Erstellungsdatum der Datei mit den Einstellungen von Private KSN angezeigt. Die KPSN-Einstellungen werden auf mobile Geräte angewendet.

Wenn Sie zu Private KSN wechseln, unterstützt die Anwendungskontrolle die bei der Verwendung von Global KSN verfügbaren App-Kategorien nicht. Die App-Kategorisierung ist verfügbar, wenn Sie wieder zu KSN wechseln.

## Datenbereitstellung an Drittanbieter-Dienste

Kaspersky Endpoint Security für Android verwendet die Google™-Dienste Firebase Cloud Messaging, Google Analytics for Firebase™, SafetyNet Attestation, Firebase Performance Monitoring und Crashlytics. Kaspersky Endpoint Security für Android verwendet den Dienst Firebase Cloud Messaging (FCM) zur rechtzeitigen Zustellung von Befehlen an mobile Geräte und zur erzwungenen Synchronisierung im Falle einer Änderung von Richtlinienereinstellungen. Kaspersky Endpoint Security für Android verwendet die Dienste Google Analytics for Firebase, SafetyNet Attestation, Firebase Performance Monitoring und Crashlytics zur Erhöhung der Qualität der App und zur effektiven Erstellung von Marketingmaterialien von Kaspersky.

## Informationsaustausch mit Firebase Cloud Messaging

Kaspersky Endpoint Security für Android verwendet den Dienst Firebase Cloud Messaging (FCM) zur rechtzeitigen Zustellung von Befehlen an mobile Geräte und zur erzwungenen Synchronisierung im Falle einer Änderung von Richtlinienereinstellungen. Dabei verwendet die App den Mechanismus der Push-Benachrichtigungen.

Für die Nutzung des Dienstes Firebase Cloud Messaging müssen die Einstellungen des Dienstes in Kaspersky Security Center angepasst werden. Weitere Informationen zur Konfiguration von Firebase Cloud Messaging in Kaspersky Security Center finden Sie in der [Hilfe zu Kaspersky Security Center](#). Wenn die Einstellungen von Firebase Cloud Messaging nicht angepasst werden, dann werden die Befehle auf dem mobilen Gerät und die Richtlinienereinstellungen während der Synchronisierung des Geräts mit Kaspersky Security Center nach dem Zeitplan, der in der Richtlinie festgelegt wurde (z. B. alle 24 Stunden), an das Gerät zugestellt. Das bedeutet, dass die Befehle und Richtlinienereinstellungen mit Verzögerung zugestellt werden.

Um die Kernfunktionen der Software nutzen zu können, stimmen Sie zu, dem Dienst Firebase Cloud Messaging die eindeutige ID der App-Installation (Instance ID) sowie die folgenden Informationen automatisch zu übermitteln:

- Informationen über die installierte Software: Version der App, App-ID, Build-Version der App, Name des App-Pakets.
- Informationen über den Computer, auf dem die Software installiert ist: Version des Betriebssystems, Geräte-ID, Version der Google-Dienste.
- Informationen über FCM: ID der App in FCM, Benutzer-ID in FCM, Protokollversion.

Die Übermittlung der Daten an Firebase erfolgt über einen geschützten Kanal. Der Zugriff auf diese Informationen und ihr Schutz sind durch die entsprechenden Nutzungsbedingungen von Firebase geregelt: <https://firebase.google.com/terms/data-processing-terms/>, <https://firebase.google.com/support/privacy/>.

*Um den Datenaustausch mit dem Dienst Firebase Cloud Messaging zu verbieten, gehen Sie wie folgt vor:*

1. Wählen Sie in der Konsolenstruktur **Mobile Geräte verwalten** → **Mobile Geräte** aus.
2. Wählen Sie im Kontextmenü des Ordners **Mobile Geräte** den Punkt **Eigenschaften** aus.



3. Wählen Sie im Eigenschaftfenster des Ordners **Mobile Geräte** den Abschnitt **Einstellungen von Google Firebase Cloud Messaging** aus.

4. Klicken Sie auf die Schaltfläche **Einstellungen zurücksetzen**.

## Informationsaustausch mit Google Analytics for Firebase, SafetyNet Attestation, Firebase Performance Monitoring und Crashlytics

Wenn Sie eine frühere Version des Verwaltungs-Plug-ins verwenden und den Informationsaustausch mit dem Google Analytics-Dienst aktiviert haben, lässt Kaspersky Endpoint Security für Android Service Pack 4 Maintenance Release 3 den Informationsaustausch mit dem Google Analytics-Dienst erfolgen. Die Unterstützung für Google Analytics wurde beendet.

Kaspersky Security für mobile Endgeräte tauscht zu folgenden Zwecken Daten mit den Diensten Google Analytics for Firebase, SafetyNet Attestation, Firebase Performance Monitoring und Crashlytics aus:

- Um die Qualität der App zu verbessern.

Für den Datenaustausch mit den Diensten Google Analytics for Firebase, SafetyNet Attestation, Firebase Performance Monitoring und Crashlytics zum Zweck der Leistungsverbesserung der App, müssen die folgenden Bedingungen erfüllt sein:

- Der Administrator oder der Benutzer des Geräts muss die Bedingungen der Erklärung zu Kaspersky Security Network akzeptieren. Wenn Sie bestimmen, dass die Erklärung von den Benutzern akzeptiert werden soll, werden diese in Form einer Mitteilung im Hauptfenster der App aufgefordert, die Bedingungen der Erklärung zu akzeptieren. Benutzer können die Erklärungen auch im Block **Über die App** in den Einstellungen von Kaspersky Endpoint Security für Android akzeptieren.

Wenn Sie die Erklärungen global akzeptieren, müssen die Versionen der über Kaspersky Security Center akzeptierten Erklärungen mit den bereits von den Benutzern akzeptierten Versionen übereinstimmen. Andernfalls werden die Benutzer über das Problem informiert und aufgefordert, die Version einer Erklärung zu akzeptieren, die der vom Administrator global akzeptierten Version entspricht. Außerdem ändert sich der Gerätestatus im Plug-in "Kaspersky Security for Mobile (Devices)" in *Warnung*.

- Der Administrator muss die Übermittlung statistischer Daten an KSN in den Einstellungen der Gruppenrichtlinie erlauben (siehe unten).
- Zur effektiven Erstellung von Marketingmaterialien durch Kaspersky.

Für den Datenaustausch mit den Diensten Google Analytics for Firebase, SafetyNet Attestation, Firebase Performance Monitoring und Crashlytics zum Zweck effektiver Erstellung von Marketingmaterialien durch Kaspersky, müssen die folgenden Bedingungen erfüllt sein:

- Der Administrator oder Benutzer des Geräts muss die Erklärung zur Datenverarbeitung für Marketingzwecke lesen und akzeptieren. Wenn Sie bestimmen, dass Benutzer die Erklärung akzeptieren sollen, können diese die Erklärung bei der Installation der App oder im Block **Über die App** in den Einstellungen von Kaspersky Endpoint Security für Android akzeptieren.
- Der Administrator muss die Datenübermittlung an Google Analytics for Firebase, SafetyNet Attestation, Firebase Performance Monitoring und Crashlytics in den Einstellungen der Gruppenrichtlinie erlauben (siehe unten).





Der Rechteinhaber verwendet Informationssysteme von Drittanbietern zur Datenverarbeitung. Deren Datenverarbeitung unterliegt den Datenschutzrichtlinien solcher Informationssysteme von Drittanbietern. Der Rechteinhaber verwendet die folgenden Dienste zur Verarbeitung der aufgezählten Daten:

### Google Analytics für Firebase

Während der Benutzung der Software werden die folgenden Daten automatisch und regelmäßig an Google Analytics für Firebase übertragen, um den erklärten Zweck zu erreichen:

- App-Informationen (App-Version, App-ID und die ID der App im Firebase-Dienst, Instanz-ID im Firebase-Dienst, Name des Shops, in dem die Anwendung erworben wurde, Zeitstempel des ersten Starts der Software)
- Installations-ID der App auf dem Gerät und Installationsmethode auf dem Gerät
- Informationen über die Region und die Sprachlokalisierung
- Informationen über die Auflösung des Gerätebildschirms
- Informationen über den Nutzer, der Root erhält
- Diagnoseinformationen zum Gerät aus dem SafetyNet-Attestation-Dienst
- Informationen zur Einstellung von Kaspersky Endpoint Security für Android als Zugangsfunktion
- Informationen über Übergänge zwischen Anwendungsbildschirmen, Sitzungsdauer, Beginn und Ende einer Bildschirmsitzung, Bildschirmname
- Informationen über das verwendete Protokoll, mit welchem Daten an den Firebase-Dienst gesendet werden, die Version und die ID der verwendeten Datenübertragungsmethode
- Informationen zum Typ und zu den Parametern des Ereignisses, auf das sich der Versand der Daten bezieht
- Informationen über die App-Lizenz, ihre Verfügbarkeit und die Anzahl der Geräte
- Informationen darüber, wie oft die Antiviren-Datenbanken aktualisiert und die Geräte mit dem Administrationsserver synchronisiert werden
- Informationen über die Verwaltungskonsole (Kaspersky Security Center oder EMM-Systeme von Drittanbietern)
- Android-ID
- Werbe-ID
- Informationen über den Benutzer: Altersgruppe und Geschlecht, Land des Wohnsitzes, Liste der Interessen
- Informationen über den Computer des Benutzers, auf dem die Software installiert ist: Name des Herstellers des Computers, Typ des Computers, Modell, Version und Sprachversion (Gebietsschema) des Betriebssystems, Informationen darüber, ob die Anwendung innerhalb der letzten 7 Tage zum ersten Mal geöffnet wurde oder ob das erste Öffnen mehr als 7 Tage zurückliegt

Die Daten werden an Firebase über einen sicheren Kanal übertragen. Informationen über die Verarbeitung von Daten in Firebase werden hier veröffentlicht: <https://firebase.google.com/support/privacy>.

### SafetyNet Attestation

Während der Benutzung der Software werden die folgenden Daten automatisch und regelmäßig an SafetyNet Attestation übertragen, um den erklärten Zweck zu erreichen:

- Zeitpunkt der Geräteprüfung
- Informationen über die Software, Name und Daten zu den Softwarezertifikaten
- Ergebnisse der Geräteprüfung
- willkürliche ID-Prüfungen, um die Ergebnisse des zu prüfenden Geräts zu ermitteln

Die Daten werden an SafetyNet Attestation über einen sicheren Kanal übertragen. Informationen darüber, wie SafetyNet Attestation Daten verarbeitet, wurden hier veröffentlicht:

<https://policies.google.com/privacy>.

### **Firestore-Leistungsüberwachung**

Während der Benutzung der Software werden die folgenden Daten automatisch und regelmäßig an SafetyNet Attestation übertragen, um den erklärten Zweck zu erreichen:

- einmalige Installations-ID
- Name des Anwendungspakets
- Version der installierten Software
- Akkustand und Ladestatus des Akkus
- Mobilfunkanbieter
- App-Ausführungsstatus (Vordergrund oder Hintergrund)
- Geografie
- IP-Adresse
- Sprachcode des Gerätes
- Informationen über die Funk-/Netzwerkverbindung
- pseudonyme ID der Software-Instanz
- RAM- und Datenträgergröße
- Kennzeichen, das angibt, ob es ein Gerät mit Jailbreak ist oder ob das Gerät gerootet ist
- Signalstärke
- Dauer von automatisierten Ablaufverfolgungen
- Netzwerk und die folgenden entsprechenden Informationen: Antwortcode, Payload-Größe in Byte, Antwortzeit
- Gerätebeschreibung

Die Daten werden an Firestore- Performance-Monitoring über einen sicheren Kanal übertragen. Informationen darüber, wie Daten in Firestore-Performance-Monitoring verarbeitet werden, sind hier veröffentlicht: <https://firebase.google.com/support/privacy>.

## Crashlytics

Während der Benutzung der Software werden die folgenden Daten automatisch und regelmäßig an Crashlytics übertragen, um den erklärten Zweck zu erreichen:

- Software-ID
- Version der installierten Software
- Kennzeichen, das angibt, ob die Software im Hintergrund ausgeführt wurde
- CPU-Architektur
- einmalige Ereignis-ID
- Datum und Uhrzeit des Ereignisses
- Gerätemodell
- gesamter Speicherplatz und derzeit genutzter Platz
- Name und Version des Betriebssystems
- gesamter RAM und derzeit genutzter Anteil
- Kennzeichen, das angibt, ob das Gerät gerootet ist
- Bildschirmausrichtung zum Ereigniszeitpunkt
- Produkt-/Hardware-Hersteller
- einmalige Installations-ID
- Version der gesendeten Statistiken
- Ausnahmetyp der Software
- Text der Fehlermeldung
- Kennzeichen, das angibt, dass die Software-Ausnahme durch eine verschachtelte Ausnahme verursacht wurde
- Thread-ID
- Kennzeichen, das angibt, ob der Frame die Ursache des Software-Fehlers war
- Kennzeichen, das angibt, dass der Thread dazu führte, dass die Software unerwartet beendet wurde
- Informationen über das Signal, das dazu führte, dass die Software unerwartet beendet wurde: Signalname, Signalcode, Signaladresse
- für jeden Frame, der einem Thread zugeordnet ist, Ausnahme oder Fehler: Name der Framedatei, Zeilennummer der Framedatei, Debug-Symbole, Adresse und Offset im Binärabbild, Anzeigenname der Bibliothek mit dem Frame, Typ des Frames, Kennzeichen, das angibt, ob der Frame den Fehler verursacht hat

- Betriebssystem-ID
- ID des Problems, das dem Ereignis zugeordnet ist
- Informationen über Ereignisse, die eingetreten sind, bevor die Software unerwartet beendet wurde: Ereignis-ID, Ereignisdatum und -uhrzeit, Ereignistyp und -wert
- CPU-Registrierungswerte
- Ereignistyp und -wert

Die Daten werden an Facebook über einen sicheren Kanal übertragen. Informationen über die Verarbeitung von Daten in Crashlytics werden hier veröffentlicht: <https://firebase.google.com/terms/crashlytics-app-distribution-data-processing-terms>.

Die Angabe obenstehender Informationen für die Datenverarbeitung zu Marketing-Zwecken ist freiwillig.

*Um den Datenaustausch mit den Diensten Google Analytics for Firebase, SafetyNet Attestation, Firebase Performance Monitoring und Crashlytics zu deaktivieren:*

1. Öffnen Sie das Fenster zur Konfiguration der Einstellungen der Richtlinie zur Verwaltung der mobilen Geräte, auf denen die App Kaspersky Endpoint Security für Android installiert ist.
2. Wählen Sie im folgenden Fenster **Eigenschaften <Name der Richtlinie>** den Abschnitt **Erweitert** aus.
3. Deaktivieren Sie im Abschnitt **Datenübertragung** das Kontrollkästchen **Datenübertragung zulassen, um bei der Verbesserung der Qualität, Erscheinung und Leistung der App zu helfen**.
4. Klicken Sie auf **Anwenden**, um die vorgenommenen Änderungen zu speichern.

Die Einstellungen werden nach der nächsten planmäßigen Synchronisierung des Geräts mit Kaspersky Security Center auf dem mobilen Gerät konfiguriert.

## Globale Annahme der zusätzlichen Erklärungen

Um den von Kaspersky Endpoint Security für Android bereitgestellten Schutz zu aktivieren, müssen die Bestimmungen des Endbenutzer-Lizenzvertrags sowie zusätzliche Erklärungen (siehe unten) akzeptiert werden. Eine Richtlinie kann so konfiguriert werden, dass die nachfolgenden Erklärungen für alle Benutzer global akzeptiert werden. Die Benutzer werden nicht aufgefordert, die Bedingungen der folgenden Lizenzverträge und Erklärungen, die bereits global akzeptiert wurden, zu lesen und zu akzeptieren:

- Vereinbarung zu Kaspersky Security Network
- Erklärung für die Datenverarbeitung für Web-Filter
- Bestimmungen für die Datenverarbeitung zu Marketingzwecken

Wenn Sie die Erklärungen global akzeptieren, müssen die Versionen der über Kaspersky Security Center akzeptierten Erklärungen mit den bereits von den Benutzern akzeptierten Versionen übereinstimmen. Andernfalls werden die Benutzer über das Problem informiert und aufgefordert, die Version einer Erklärung zu akzeptieren, die der vom Administrator global akzeptierten Version entspricht. Außerdem ändert sich der Gerätestatus im Plug-in "Kaspersky Security for Mobile (Devices)" in **Warnung**.

So bestimmen Sie mithilfe einer Gruppenrichtlinie, ob die Bedingungen global oder von Benutzern akzeptiert werden sollen:

1. Wählen Sie in der Konsolenstruktur im Ordner **Verwaltete Geräte** die Administrationsgruppe, zu der die Android-Geräte gehören.
2. Gehen Sie im Arbeitsbereich der Gruppe auf die Registerkarte **Richtlinien**.
3. Öffnen Sie über Doppelklick auf eine beliebige Spalte das Eigenschaftfenster der Richtlinie.
4. Wählen Sie im folgenden Fenster **Eigenschaften <Name der Richtlinie>** den Abschnitt **Erweitert** aus.
5. Wählen Sie im Block **Datenweiterleitung** aus, ob die Erklärung zur Datenverarbeitung für Marketingzwecke global oder von den einzelnen Benutzern akzeptiert werden soll.
6. Wählen Sie im Block **Einstellungen für Kaspersky Security Network (KSN)** aus, ob die Erklärung zu Kaspersky Security Network global oder von Benutzern akzeptiert werden soll.
7. Klicken Sie auf **Anwenden**, um die vorgenommenen Änderungen zu speichern.

Der Benutzer kann die Bedingungen für die App jederzeit in den Einstellungen von Kaspersky Endpoint Security für Android im Abschnitt **Über die App** akzeptieren oder ablehnen.

## Samsung KNOX

*Samsung KNOX* ist eine mobile Lösung zur Konfiguration sowie zum Schutz von mobilen Samsung-Geräten unter dem Betriebssystem Android. Nähere Informationen über Samsung KNOX finden Sie auf der [Seite des technischen Supports von Samsung](#).

## Installation der App Kaspersky Endpoint Security für Android über KNOX Mobile Enrollment

KNOX Mobile Enrollment (KME) ist ein Bestandteil der mobilen Lösung Samsung KNOX. Die Komponente wird für die Masseninstallation und die Erstkonfiguration von Apps auf neuen Samsung-Geräten verwendet, die bei offiziellen Anbietern erworben wurden.

Die Installation der App Kaspersky Endpoint Security für Android über KNOX Mobile Enrollment besteht aus den folgenden Schritten:

1. [Erstellen eines KNOX MDM-Profiles mit der App Kaspersky Endpoint Security für Android.](#)
2. [Geräte zu KNOX Mobile Enrollment hinzufügen.](#)
3. [Installation der App Kaspersky Endpoint Security für Android auf den mobilen Geräten des Benutzers.](#)

Weitere Informationen zur Verwendung von KNOX Mobile Enrollment finden Sie im [Benutzerhandbuch für KNOX Mobile Enrollment](#).

Die Verteilung über KNOX Mobile Enrollment ist nur für Samsung-Geräte möglich. Eine Liste mit unterstützten Geräten finden Sie auf der [Seite des technischen Supports von Samsung](#).

## KNOX MDM-Profil erstellen

Das KNOX MDM-Profil ist ein Profil, das Links zu Apps enthält, über die sie schnell auf den mobilen Geräten verteilt und konfiguriert werden können.

Um ein KNOX MDM-Profil zu erstellen, gehen Sie wie folgt vor:

1. Melden Sie sich in der [Konsole für Samsung KNOX](#) → **KNOX Mobile Enrollment** an.

2. Wählen Sie den Abschnitt **MDM-Profile** aus.

3. Klicken Sie auf **Hinzufügen**.

Der Assistent zur Erstellung eines KNOX MDM-Profiles wird ausgeführt.

4. Wählen Sie im Schritt **Verbindung des MDM-Servers** **Mein MDM-Dienst erfordert keine Server-URI** und klicken Sie auf **Weiter**.

5. Gehen Sie im Schritt **Angaben zum MDM-Profil** wie folgt vor:

a. Geben Sie allgemeine Informationen über das KNOX MDM-Profil ein: **Name des Profils** und **Beschreibung**.

b. Geben Sie über die Schaltfläche **MDM-Apps hinzufügen** den Pfad zur APK-Installationsdatei ein.

Die Installationsdatei von Kaspersky Endpoint Security für Android gehört zum [Lieferumfang von Kaspersky Security für mobile Endgeräte](#). Speichern Sie die APK-Installationsdatei vorübergehend auf dem Webserver für Kaspersky Security Center oder auf einem anderem Server, auf den das Gerät für Downloads zugreifen kann.

c. Geben Sie die Einstellungen für die Verbindung des Geräts mit Kaspersky Security Center im Feld **Benutzerdefinierte JSON-Daten** im folgenden Format ein:

```
{"serverAddress": "ksc.server.com", "serverPort": "12345", "groupName": "MOBILE GROUP"}
```

Die Verbindung des Geräts mit Kaspersky Security Center ist für die [Aktivierung der App](#), die Konfiguration des Geräts und [den Versand von Befehlen](#) erforderlich.

d. Aktivieren Sie das Kontrollkästchen **Hinzufügen von Vereinbarungen im Zusammenhang mit Knox**.

Für die Installation von Kaspersky Endpoint Security für Android über KNOX Mobile Enrollment muss der Benutzer des mobilen Geräts die Bedingungen des Lizenzvertrags von Samsung annehmen. Sie können sich im Block **Endbenutzer-Lizenzverträge, Nutzungsbedingungen und Benutzervereinbarungen** mit den Bedingungen des Lizenzvertrags von Samsung vertraut machen. Darüber hinaus können Sie über die Schaltfläche **Benutzervereinbarung hinzufügen** weitere juristische Dokumente Ihres Unternehmens hinzufügen, die für die Implementierung des KNOX MDM-Profiles erforderlich sind.

e. Deaktivieren Sie das Kontrollkästchen **Knox-Lizenz diesem Profil zuordnen**.

Die Informationen über die Lizenz für Samsung KNOX werden zusammen mit der [Richtlinie bei der Synchronisierung Ihres Geräts mit Kaspersky Security Center](#) an das mobile Gerät übermittelt.

6. Klicken Sie auf **Speichern**.

Daraufhin wird das neue KNOX MDM-Profil mit der App Kaspersky Endpoint Security für Android in der KME-Konsole zur Liste hinzugefügt.

## Geräte zu KNOX Mobile Enrollment hinzufügen

Geräte können auf folgende Arten zur Konsole KNOX Mobile Enrollment (KME) hinzugefügt werden:

- Der Anbieter fügt die Geräte nach dem Kauf des Geräts automatisch zur KME-Konsole hinzu.  
Wählen Sie diese Option, wenn Ihr Unternehmen mit einem offiziellen Anbieter von Samsung-Geräten zusammenarbeitet.
- Der Administrator installiert die App KNOX Deployment über Google Play auf seinem mobilen Gerät und überträgt das KNOX MDM-Profil mithilfe von Bluetooth oder NFC (Near Field Communication) auf die Geräte der Benutzer. Nach der Verteilung des KNOX MDM-Profiles wird das Gerät automatisch zur KME-Konsole hinzugefügt.  
Wählen Sie diese Option, wenn die Samsung-Geräte nicht bei einem offiziellen Anbieter erworben wurden.

## Gerät über den Anbieter hinzufügen

Ein offizieller Anbieter von Samsung-Geräten ist in Samsung KNOX registriert. Eine Liste mit offiziellen Anbietern finden Sie auf der [Seite des technischen Supports von Samsung](#)<sup>2</sup>. Der Anbieter fügt die Geräte nach dem Kauf des Geräts automatisch zur KME-Konsole für Ihr Samsung-Konto hinzu. Damit der Anbieter Geräte hinzufügen kann, muss er in der KME-Konsole für Ihr Samsung-Konto registriert werden. Um den Anbieter von Samsung-Geräten zur KME-Konsole hinzufügen zu können, benötigen Sie die Verkäufer-ID. Wenden Sie sich an den Anbieter, um die Verkäufer-ID zu erhalten. Geben Sie in der Anfrage Ihre KNOX Kunden-ID an.

*Um Ihre KNOX Kunden-ID zu finden, gehen Sie wie folgt vor:*

1. Melden Sie sich in der [Konsole für Samsung KNOX](#)<sup>2</sup> → **KNOX Mobile Enrollment** an.
2. Wählen Sie den Abschnitt **Verkäufer**.
3. Im Feld **KNOX Kunden-ID** wird Ihre ID angezeigt.

Sobald der Anbieter Ihnen eine Antwort mit der Verkäufer-ID gesendet hat, registrieren Sie ihn in der MME-Konsole. Vor der Registrierung des Anbieters können Sie ein KNOX MDM-Profil erstellen, um das Profil beim Hinzufügen von neuen Geräten automatisch zu verteilen.

*Um einen offiziellen Anbieter in der KME-Konsole zu registrieren, gehen Sie wie folgt vor:*

1. Melden Sie sich in der [Konsole für Samsung KNOX](#)<sup>2</sup> → **KNOX Mobile Enrollment** an.
2. Wählen Sie den Abschnitt **Verkäufer**.
3. Klicken Sie auf die Schaltfläche **Verkäufer registrieren**.  
Das Fenster zur Registrierung eines Geräteanbieters wird geöffnet.
4. Geben Sie im Feld **Verkäufer-ID** die ID ein, die Sie vom offiziellen Anbieter von Samsung-Geräten erhalten haben.
5. Wenn Sie ein [KNOX MDM-Profil erstellt haben](#), wählen Sie im Fenster der Registrierung des Anbieters das KNOX MDM-Profil aus.  
Beim Hinzufügen von neuen Geräten wird das KNOX MDM-Profil automatisch installiert.
6. Wählen Sie in der Liste **Bevorzugte Bestätigungsmethode für Downloads** eine Bestätigungsmethode für das Hinzufügen eines Geräts für den Anbieter aus.
  - **Alle Downloads müssen bestätigt werden.** Beim Hinzufügen des Geräts durch den Anbieter müssen Sie den Vorgang bestätigen.



- **Alle Downloads dieses Anbieters automatisch bestätigen.** Die Geräte des Anbieters werden automatisch zur KME-Konsole hinzugefügt.

7. Klicken Sie auf **OK**.

Der Anbieter von Samsung-Geräten wird zur Liste der Anbieter in der KME-Konsole hinzugefügt.

Nach dem Kauf von neuen Geräten bei einem offiziellen Anbieter wird die App "Kaspersky Endpoint Security für Android" automatisch auf dem Gerät installiert, sobald dieses sich mit dem Internet verbindet. Weitere Informationen zur Verwendung von KNOX Mobile Enrollment finden Sie im [Benutzerhandbuch für KNOX Mobile Enrollment](#). Wenn Sie bereits eine Liste mit Geräten in der KME-Konsole erstellt haben, fügen Sie das KNOX MDM-Profil mit der KNOX MDM-App auf dem Gerät hinzu.

*Um ein KNOX MDM-Profil an Geräte zu übermitteln, gehen Sie wie folgt vor:*

1. Melden Sie sich in der [Konsole für Samsung KNOX](#) → **KNOX Mobile Enrollment** an.
2. Wählen Sie den Abschnitt **Geräte** → **Alle Geräte** aus.
3. Wählen Sie die Geräte aus, auf denen Sie das KNOX MDM-Profil installieren möchten.
4. Klicken Sie auf **Anpassen**.  
Das Fenster **Geräteinformationen** wird geöffnet.
5. Wählen Sie in der Liste **MDM-Profil** das KNOX MDM-Profil mit der App Kaspersky Endpoint Security für Android aus.
6. Geben Sie im Feld **Tags** die Tags für die Gruppierung und Kennzeichnung der Geräte sowie für die Suchoptimierung in der KME-Konsole ein.
7. Geben Sie die Anmeldedaten des Gerätebenutzers in den Feldern **Benutzer-ID** und **Kennwort** ein.  
Die Anmeldedaten werden zum Abrufen des allgemeinen Zertifikates benötigt. Die Benutzer-ID und das Kennwort müssen mit den Anmeldedaten des Benutzers in Kaspersky Security Center übereinstimmen (vollständiger Name und Kennwort in den Eigenschaften des Benutzerkontos).
8. Wählen Sie das KNOX MDM-Profil für die übrigen Geräte aus.
9. Klicken Sie auf **Speichern**.

Daraufhin wird der Benutzer bei der Verbindung des Geräts mit dem Internet aufgefordert, das KNOX MDM-Profil zu installieren.

## Gerät mithilfe der App KNOX Deployment hinzufügen

Wenn Sie das Samsung-Gerät nicht bei einem offiziellen Anbieter erworben haben, können Sie es mithilfe von Bluetooth oder NFC zu KNOX Mobile Enrollment hinzufügen. Dazu wird das mobile Gerät eines Administrators benötigt, mit dessen Hilfe die KNOX MDM-Profile an die mobilen Geräte der Benutzer übermittelt werden.

Um Geräte mithilfe der App KNOX Deployment hinzufügen zu können, müssen folgende Bedingungen erfüllt sein:

- Auf den mobilen Geräten müssen je nach der ausgewählten Übermittlungsmethode die Module Bluetooth oder NFC aktiviert sein.
- Die mobilen Geräte müssen mit dem Internet verbunden sein.

Um ein KNOX MDM-Profil mithilfe der App KNOX Deployment zu übermitteln, gehen Sie wie folgt vor:

1. Installieren Sie auf dem mobilen Gerät des Administrators die [App KNOX Deployment aus Google Play](#).
2. Starten Sie die App KNOX Deployment.
3. Geben Sie die Anmeldedaten Ihres Samsung-Benutzerkontos ein.
4. Passen Sie im Fenster **KNOX Deployment** die Einstellungen der Verteilung des KNOX MDM-Profils an:
  - Wählen Sie das [KNOX MDM-Profil](#) aus.
  - Wählen Sie eine Verteilungsmethode aus: **Bluetooth** oder **NFC**.  
Wenn Sie Bluetooth verwenden, können Sie das KNOX MDM-Profil auf mehreren Geräten gleichzeitig hinzufügen.
5. Klicken Sie auf **Verteilung starten**:
  - **Bluetooth.** Öffnen Sie auf dem mobilen Gerät des Benutzers die Website <https://configure.samsungknox.com>.  
Der Assistent zur Registrierung des Geräts in Samsung KNOX wird gestartet. Folgen Sie den Anweisungen auf dem Bildschirm.  
Nach der Installation des KNOX MDM-Profils wird das neue Gerät mit dem Tag **Bluetooth** zur KME-Konsole hinzugefügt.
  - **NFC.** Halten Sie das mobile Gerät des Administrators an das mobile Gerät des Benutzers und übermitteln Sie das KNOX MDM-Profil.  
Daraufhin wird der Benutzer auf seinem Gerät aufgefordert, das KNOX MDM-Profil zu installieren. Das neue Gerät mit dem Tag **NFC** wird zur KME-Konsole hinzugefügt.

## App installieren

Stellen Sie vor der Installation von Kaspersky Endpoint Security für Android [in der Verwaltungskonsole von Kaspersky Security Center ein allgemeines Zertifikat für die Benutzer von mobilen Geräten aus](#). Das allgemeine Zertifikat ist für die Identifizierung des Benutzers des mobilen Geräts in der Verwaltungskonsole für Kaspersky Security Center erforderlich.

Sobald die Verteilung des KNOX MDM-Profils auf dem mobilen Gerät beginnt, wird die APK-Installationsdatei automatisch heruntergeladen. Die Installation der App Kaspersky Endpoint Security für Android wird automatisch gestartet. Der Benutzer muss den Endbenutzer-Lizenzvertrag für Samsung KNOX und den Endbenutzer-Lizenzvertrag für Kaspersky Endpoint Security für Android annehmen. Eine zusätzliche Konfiguration der App ist nicht erforderlich. Nach der Installation der App erfolgt eine automatische Synchronisierung mit Kaspersky Security Center. Daraufhin wird das mobile Gerät in der Verwaltungskonsole für Kaspersky Security Center zur Administrationsgruppe hinzugefügt, die in den Einstellungen des [KNOX MDM-Profils](#) (groupName) angegeben ist.

## KNOX-Container konfigurieren

Dieser Abschnitt enthält Informationen über die Arbeit mit KNOX-Containern auf Samsung-Geräten unter Verwaltung des Betriebssystems Android.

Die Nutzung der KNOX-Container ist nur auf Samsung-Geräten unter Verwaltung des Betriebssystems Android Version 5.0 oder höher verfügbar.

## Über den KNOX-Container

Der *KNOX-Container* ist eine sichere Umgebung auf dem Gerät des Benutzers mit einem separaten Desktop, einer Startleiste, Apps und Widgets. Der KNOX-Container ermöglicht eine Isolierung von korporativen Apps und Daten von den persönlichen. Der KNOX-Container ist eine Komponente der mobilen Lösung Samsung KNOX.

*Samsung KNOX* ist eine mobile Lösung zur Konfiguration sowie zum Schutz von mobilen Samsung-Geräten unter dem Betriebssystem Android. Nähere Informationen über Samsung KNOX finden Sie auf der [Seite des technischen Supports von Samsung](#).

Die KNOX-Container ermöglichen die Trennung von persönlichen und Unternehmensdaten auf dem mobilen Gerät. Es ist beispielsweise unmöglich, eine Datei, die sich im KNOX-Container befindet, mithilfe des persönlichen E-Mail-Postfachs abzusenden. Es ist empfehlenswert, den KNOX-Container zu verteilen, wenn für die Arbeit mit den Unternehmensdaten die persönlichen mobilen Geräte der Mitarbeiter verwendet werden.

Für die Nutzung von KNOX-Containern muss [Samsung KNOX aktiviert](#) werden. Nach der Synchronisierung des Geräts mit Kaspersky Security Center wird dem Benutzer des mobilen Geräts vorgeschlagen, einen KNOX-Container zu installieren. Vor der Installation des KNOX-Containers muss der Benutzer die Bedingungen des Endbenutzer-Lizenzvertrags des Unternehmens Samsung akzeptieren.

Nach der Installation des KNOX-Containers auf dem Desktop des mobilen Geräts wird das KNOX-Symbol



hinzugefügt. Alternativ wird der Arbeitsbereich zur App-Liste auf dem mobilen Gerät hinzugefügt. Für die Arbeit mit den Unternehmensdaten muss der Benutzer die App im KNOX-Container ausführen.

Kaspersky Endpoint Security für Android ist nicht im KNOX-Container installiert und schützt die Unternehmensdaten nicht. Kaspersky Endpoint Security für Android erkennt nicht den Download schädlicher Dateien und blockiert keine schädlichen Websites im KNOX-Container. Die Ausführung von Apps und die Verwendung der Kamera können im KNOX-Container nicht kontrolliert werden. Kaspersky Endpoint Security für Android schützt nur persönliche Daten. Unternehmensdaten können mit den Tools von Samsung KNOX geschützt werden. Nähere Informationen über Samsung KNOX finden Sie auf der [Seite des technischen Supports von Samsung](#).

## Samsung KNOX aktivieren

Um einen KNOX-Container auf dem mobilen Gerät des Benutzers verwenden zu können, müssen Sie Samsung KNOX aktivieren. Das Verfahren zur Aktivierung von Samsung KNOX hängt von der Version von Kaspersky Endpoint Security für Android ab, die auf den Geräten Ihrer Benutzer installiert ist:

- Wenn auf den Geräten die aktuelle Version von Kaspersky Endpoint Security für Android installiert ist, benötigen Sie keine Schlüssel, um Samsung KNOX zu aktivieren.
- Wenn auf den Geräten eine alte Version von Kaspersky Endpoint Security für Android (10.8.3.174 oder früher) installiert ist, müssen Sie von Samsung einen KNOX License Manager-Schlüssel (im Folgenden KLM-Schlüssel genannt) beziehen. Der *KNOX License Manager-Schlüssel* ist ein eindeutiger Code, der vom System zur

Lizenzverwaltung von Samsung KNOX verwendet wird. Ausführliche Informationen zum KLM-Schlüssel finden Sie auf der [Website für den Technischen Support von Samsung KNOX](#).

Die Verwendung von KNOX-Containern ist nur auf Samsung-Geräten möglich.

*Um Samsung KNOX zu aktivieren, gehen Sie wie folgt vor:*

1. Wählen Sie in der Konsolenstruktur im Ordner **Verwaltete Geräte** die Administrationsgruppe, zu der die Android-Geräte gehören.
2. Gehen Sie Im Arbeitsbereich der Gruppe auf die Registerkarte **Richtlinien**.
3. Öffnen Sie über Doppelklick auf eine beliebige Spalte das Eigenschaftfenster der Richtlinie.
4. Wählen Sie im Fenster **Eigenschaften** der Richtlinie den Abschnitt **Verwaltung von Samsung KNOX → KNOX-Container**.
5. Geben Sie im Feld **KNOX License Manager-Schlüssel** Folgendes an:
  - Wenn auf den Geräten die aktuelle Version von Kaspersky Endpoint Security für Android installiert ist, geben Sie ein beliebiges Zeichen ein.
  - Wenn auf den Geräten eine alte Version von Kaspersky Endpoint Security für Android (10.8.3.174 oder früher) installiert ist, geben Sie den von Samsung erhaltenen KLM-Schlüssel ein.
6. Bringen Sie das Attribut Schloss in die geschlossene Stellung .
7. Klicken Sie auf **Anwenden**, um die vorgenommenen Änderungen zu speichern.

Samsung KNOX wird nach der nächsten Synchronisierung des Geräts mit Kaspersky Security Center aktiviert. Der Benutzer wird aufgefordert, die Bedingungen des Endbenutzer-Lizenzvertrags des Unternehmens Samsung zu akzeptieren und den KNOX-Container zu installieren.

*Um Samsung KNOX zu deaktivieren, gehen Sie wie folgt vor:*

1. Wählen Sie in der Konsolenstruktur im Ordner **Verwaltete Geräte** die Administrationsgruppe, zu der die Android-Geräte gehören.
2. Gehen Sie Im Arbeitsbereich der Gruppe auf die Registerkarte **Richtlinien**.
3. Öffnen Sie über Doppelklick auf eine beliebige Spalte das Eigenschaftfenster der Richtlinie.
4. Wählen Sie im Fenster **Eigenschaften** der Richtlinie den Abschnitt **Verwaltung von Samsung KNOX → KNOX-Container**.
5. Löschen Sie den Wert des Feldes **KNOX License Manager-Schlüssel**.
6. Klicken Sie auf **Anwenden**, um die vorgenommenen Änderungen zu speichern.

Samsung KNOX wird nach der nächsten Synchronisierung des Geräts mit Kaspersky Security Center deaktiviert. Der Zugriff auf den KNOX-Container wird blockiert.

## Beschränkungen von Samsung KNOX

- Die Verwendung von KNOX-Containern ist nur auf Samsung-Geräten verfügbar.
- Auf Samsung-Geräten, die KNOX 2.6, 2.7 und 2.7.1 unterstützen, funktionieren der Web-Filter und die Programmkontrolle nicht innerhalb eines KNOX-Containers. Das Problem ist mit dem Fehlen der erforderlichen Rechte im KNOX-Container verbunden (Dienst für erleichterte Bedienung). Auf Geräten mit Unterstützung für KNOX 2.8 und höher funktionieren alle Komponenten der App ohne Beschränkungen.
- Die Ausführung von Versionen von Kaspersky Endpoint Security für Android, die älter sind als Service Pack 4 Maintenance Release 3 Update 2, ist auf Samsung-Geräten mit Android 10 aufgrund von Samsung KNOX-Updates möglicherweise instabil. Es wird empfohlen, Kaspersky Endpoint Security für Android auf die Version Service Pack 4 Maintenance Release 3 Update 2 zu aktualisieren.

## Einstellungen der Firewall in KNOX

Für die Kontrolle der Netzwerkverbindungen müssen im KNOX-Container die Firewall-Einstellungen angepasst werden.

*Um die Firewall im KNOX-Container anzupassen, gehen Sie wie folgt vor:*

1. Wählen Sie in der Konsolenstruktur im Ordner **Verwaltete Geräte** die Administrationsgruppe, zu der die Android-Geräte gehören.
2. Gehen Sie Im Arbeitsbereich der Gruppe auf die Registerkarte **Richtlinien**.
3. Öffnen Sie über Doppelklick auf eine beliebige Spalte das Eigenschaftenfenster der Richtlinie.
4. Wählen Sie im Fenster **Eigenschaften** der Richtlinie den Abschnitt **Verwaltung von Samsung KNOX → KNOX-Container**.
5. Klicken Sie unter **Firewall** auf **Anpassen**.  
Das Fenster **Firewall** wird geöffnet.
6. Wählen Sie den Firewall-Modus:
  - Um alle eingehenden und ausgehenden Verbindungen zu erlauben, verschieben Sie den Schieberegler in die Position **Alle erlauben**.
  - Um jede Netzwerkaktivität mit Ausnahme von Apps aus der Ausnahmenliste zu blockieren, verschieben Sie den Schieberegler in die Position **Alle blockieren, Ausnahmen ausgenommen**.
7. Wenn Sie den Firewall-Modus **Alle blockieren, Ausnahmen ausgenommen** gewählt haben, erstellen Sie eine Ausnahmenliste:
  - a. Klicken Sie auf **Hinzufügen**.  
Das Fenster **Ausnahme für Firewall** wird geöffnet.
  - b. Geben Sie im Feld **App-Name** den Namen der mobilen App ein.
  - c. Geben Sie im Feld **Paketname** den Systemnamen der mobilen App (zum Beispiel `com.mobileapp.example`) ein.
  - d. Klicken Sie auf **OK**.

8. Klicken Sie auf **Anwenden**, um die vorgenommenen Änderungen zu speichern.

Die Einstellungen werden nach der nächsten planmäßigen Synchronisierung des Geräts mit Kaspersky Security Center auf dem mobilen Gerät konfiguriert.

## Einstellungen des Exchange-E-Mail-Postfachs in KNOX

Für die Arbeit mit E-Mail, Kontakten und Kalender des Unternehmens im KNOX-Container müssen die Einstellungen des Exchange-E-Mail-Postfachs angepasst werden.

*Um das Exchange-E-Mail-Postfach im KNOX-Container anzupassen, gehen Sie wie folgt vor:*

1. Wählen Sie in der Konsolenstruktur im Ordner **Verwaltete Geräte** die Administrationsgruppe, zu der die Android-Geräte gehören.
2. Gehen Sie Im Arbeitsbereich der Gruppe auf die Registerkarte **Richtlinien**.
3. Öffnen Sie über Doppelklick auf eine beliebige Spalte das Eigenschaftenfenster der Richtlinie.
4. Wählen Sie im Fenster **Eigenschaften** der Richtlinie den Abschnitt **Verwaltung von Samsung KNOX → KNOX-Container**.
5. Klicken Sie unter **Exchange ActiveSync** auf **Anpassen**.  
Es öffnet sich das Fenster **Einstellungen des Exchange-Mailservers**.
6. Geben Sie im Feld **Serveradresse** die IP-Adresse oder den DNS-Namen des Servers, auf der der Mail-Server installiert ist.
7. Geben Sie im Feld **Domain** den Namen der Domäne des Benutzers im Unternehmensnetzwerk ein.
8. Wählen Sie in der Dropdown-Liste **Regelmäßigkeit der Synchronisierung** den gewünschten Zeitraum für die Synchronisierung des mobilen Geräts mit dem Microsoft Exchange-Server.
9. Um das Transportprotokoll für den E-Mail-Transfer SSL zu verwenden, aktivieren Sie das Kontrollkästchen **SSL-Verbindung verwenden**.
10. Um digitale Zertifikate für den Schutz des Datentransfers zwischen dem mobilen Gerät und dem Microsoft Exchange-Server zu verwenden, aktivieren Sie das Kontrollkästchen **Serverzertifikat prüfen**.
11. Klicken Sie auf **Anwenden**, um die vorgenommenen Änderungen zu speichern.

Die Einstellungen werden nach der nächsten planmäßigen Synchronisierung des Geräts mit Kaspersky Security Center auf dem mobilen Gerät konfiguriert.

## Anhang

Dieser Abschnitt enthält Informationen, die den Haupttext des Dokuments ergänzen.

## Rechte zur Konfiguration von Gruppenrichtlinien

Die Administratoren für Kaspersky Security Center können die Zugriffsrechte der Benutzer der Administrationskonsole auf verschiedene Programmfunktionen abhängig von den dienstlichen Verpflichtungen der Benutzer konfigurieren.

Für jeden Funktionsbereich kann der Administrator folgende Zugriffsrechte zuweisen:

- **Ändern von Einstellungen erlauben.** Der Benutzer der Verwaltungskonsole darf die Richtlinieneinstellungen im Eigenschaftenfenster der Richtlinie ändern.
- **Ändern von Einstellungen verbieten.** Dem Benutzer der Administrationskonsole ist es verboten, die Richtlinieneinstellungen im Eigenschaftenfenster der Richtlinie zu ändern. Die den Funktionsbereichen entsprechenden Registerkarten der Richtlinie, für die diese Berechtigung zugewiesen wurde, werden nicht in der Schnittstelle angezeigt.

Zugriffsrechte auf die Abschnitte des Verwaltungs-Plug-ins von Kaspersky Endpoint Security

Funktionsbereich	Abschnitt Richtlinien
Android Enterprise	Arbeitsprofil Android
Diebstahlschutz	Diebstahlschutz
Anwendungskontrolle	Anwendungskontrolle
Schutz	Schutz, Untersuchung, Update
Übereinstimmungsüberprüfung	Übereinstimmungsüberprüfung
Container	Container
Geräteeinstellungen	Geräteverwaltung, Synchronisierung
Verwaltung von Samsung-Geräten	APN, Verwaltung von Samsung-Geräten, KNOX-Container
Systemverwaltung	Erweitert, WLAN
Web-Filter	Web-Filter

Zugriffsrechte auf die Abschnitte des Verwaltungs-Plug-ins von Kaspersky Device Management für iOS

Funktionsbereich	Abschnitt Richtlinien
Erweitert	Webclips, Schriftarten, AirPlay, AirPrint
Exchange ActiveSync	Allgemein, Kennwort, Synchronisierung, Funktionsbeschränkungen, App-Beschränkungen
Allgemein	Allgemein, Einmalanmeldung, Web-Filter, WLAN, Zugriffspunkt (APN), Exchange ActiveSync, E-Mail, Konfigurationseinstellungen
LDAP (Kalender/Kontakte)	LDAP, Kalender, Kontakte, Signaturen und Kalender
Einschränkungen und Sicherheit	Funktionsbeschränkungen, App-Beschränkungen, Beschränkungen für Medieninhalte, Kennwort, VPN, Globaler HTTP-Proxy, Zertifikate, SCEP

## Kategorien für Apps

Die Anwendungskontrolle unterstützt die Kategorisierung von Apps. Der Modus, der für die App-Kategorie festgelegt ist, wird für alle Apps aus dieser Kategorie angewendet. Die Kategorie wird für jede App mit dem Cloud-Dienst Kaspersky Security Network ermittelt.

Kategorie	Beschreibung
Unterhaltung	Apps für interaktive Unterhaltung.
IM-Clients, Apps zum Telefonieren	Apps für Instant Messaging, Sprach- und Videokommunikation über IP-Telefonie.
Soziale Netzwerke	Apps für soziale Netzwerke, Blogs.
Business-Software	Apps für Steuerabrechnungen, Verwaltung von Bankentransaktionen, Arbeit mit Tabellen, Buchhaltung sowie andere geschäftliche Apps. Texteditoren.
Haus, Familie, Hobby, Gesundheit	Apps für Rezepte, Stilempfehlungen. Apps für Fitness, Trainingspläne, Diätempfehlungen, Tipps für gesunde Ernährung, Sicherheitstechnik, Arbeitsschutz.
Medizin	Apps mit Verzeichnissen von Symptomen und Arzneimitteln, Apps für Angestellte in der Gesundheitssphäre, medizinische Zeitschriften und Neuigkeiten.
Multimedia	Abonnementdienste für Filme, Multimedia- und Videoplayer. Musikdienste, Player, Radiosendungen.
Software für Grafikdesign.	Kamera-Apps, Bildbearbeitungstools, Apps für die Fotoverwaltung und -veröffentlichung.
Plug-ins für Nachrichten und RSS-Feeds.	Apps für Zeitungen, Zeitschriften, Blogs, Nachrichtenfeeds.
Wetter.	Apps für die Wettervorhersage.
Apps für die Bildung.	Anwendungen zum Lesen von Büchern, Katalogen, Lernbüchern, Wörterbüchern, Thesauren, Nachschlagewerke. Apps für die Prüfungsvorbereitung, Lehrmaterialien, Wörterbücher, Förderspiele, Sprachlerntools.
Online-Shopping	Apps für Online-Einkäufe und Teilnahme an Auktionen, Geschenkgutscheine, Preisvergleichsportale und Tools für Einkaufslisten, Lesen von Produktbewertungen.
Personalisierungs-Apps	Apps für die benutzerdefinierte Personalisierung des Desktops, der Widgets, der Verknüpfungen.
Betriebssysteme und Hilfsprogramme	Systemanwendungen für die Verwaltung des Betriebssystems, Benutzerinteraktion, Arbeitsspeicherverwaltung.
Apps für die Kartenansicht	Reiseführer für Städte, Informationen zu lokalen Firmen, Tools für die Reiseplanung.
Sonstige Apps	Software-Bibliotheken, technische Demoverversionen der Apps. Apps, die in keine der Kategorien passen.
Verkehrswesen	Apps für öffentliche Transportmittel, Navigationsapps, Apps zum Autofahren.
Spiele	Arcade, Quizspiele, Rennspiele, Sonstige, Kasino, Karten, Musik, Brettspiele, Lernspiele, Puzzle, Abenteuer, Rollenspiele, Simulation, Wortspiele, Sportspiele, Strategie, Action.
Browser	Apps für die Anzeige von Websites, Webdokumenten, Dateien. Apps für die Verwaltung von Webanwendungen.
Entwickler-Tools	Apps für die Software-Entwicklung. Debugger, Linker, Quellcode-Editoren, GUI-Editoren.
Betriebssystem-Apps	Apps, die gemeinsam mit dem Betriebssystem geliefert werden und für die Ausführung des Betriebssystems erforderlich sind.
Software für die Arbeit im Internet	Download-Manager, Mail-Clients, Apps für die Suche im Internet sowie andere Apps für die Arbeit mit dem Internet.



Software für die Netzwerkinfrastruktur	Apps für die Verwaltung von Servern, Geräten für die Datenspeicherung, Netzwerkgeräten, Software innerhalb eines Unternehmensnetzwerks, Automatisierung und Integration der Infrastruktur.
Netzwerk-Software	Apps für die Teamarbeit von Benutzergruppen auf mehreren Geräten, Kommunikation zwischen den Geräten in einem Unternehmen.
Systemtools	Apps, die gemeinsam mit dem Betriebssystem geliefert werden: Dateimanager, Archivierungsprogramme, Diagnosetools für Hardware und Software, Speicheroptimierungstools, Deinstallationstools, Prozessorverwaltungstools.
Schutzsoftware	Apps für den Datenschutz auf dem Gerät. Apps für die Erkennung und Behebung von Bedrohungen auf dem Gerät. Firewalls. Apps für die Datenverschlüsselung.
Downloadmanager	Apps für den Download von Dateien aus externen Quellen.
Apps zum Speichern von Dateien im Internet.	Apps für die Arbeit mit Online-Speichern für Dateien, Notizen, Multimedia.
Hilfe-Apps	Programme zum Lesen von Büchern, Katalogen, Lernbüchern, Wörterbüchern, Thesauren, Nachschlagewerke.
E-Mail-Programme	Apps für den Versand und den Empfang von E-Mails.

# Verwendung der App Kaspersky Endpoint Security für Android

In diesem Hilfeabschnitt werden Funktionen und Vorgänge beschrieben, die den Benutzern der App Kaspersky Endpoint Security für Android zur Verfügung stehen.

Die Artikel in diesem Abschnitt besprechen alle Optionen, die auf einem mobilen Gerät verfügbar oder sichtbar sind. Das eigentliche Layout und Verhalten der App hängt davon ab, welches Remote-Verwaltungssystem implementiert ist und auf welche Weise der Administrator die Einstellungen Ihres Geräts mit Rücksicht auf die Anforderungen an die Unternehmenssicherheit anpasst. Einige der in diesem Abschnitt beschriebenen Funktionen und Optionen spiegeln womöglich nicht Ihre Erfahrung mit der App wider. Bei Fragen zur App auf Ihrem konkreten Gerät wenden Sie sich bitte an Ihren Administrator.

## Funktionen der Anwendung

Kaspersky Endpoint Security bietet folgende Funktionen.

### Schutz vor Viren und anderen schädlichen Anwendungen.

Die Komponente Anti-Virus bietet Schutz vor Viren und anderen schädlichen Anwendungen.

Anti-Virus führt folgende Funktionen aus:

- Alle Geräte, installierte Anwendungen oder ausgewählte Ordner auf Bedrohungen untersuchen
- Gerät im Echtzeitmodus schützen
- Neu installierte Anwendungen vor dem ersten Start untersuchen
- Antiviren-Datenbanken aktualisieren

Wenn auf dem Mobilgerät eine App installiert ist, die das Sammeln und den Versand von Daten zur Verarbeitung ausführt, kann Kaspersky Security für Android eine solche App als schädlich einstufen.

## Anwendungskontrolle

Gemäß der korporativen Sicherheit erstellt der *Administrator für das Remote-Verwaltungssystem* (im Folgenden auch "Administrator") Listen empfohlener, verbotener und obligatorischer Anwendungen. Installationen und Updates empfohlener und verpflichtender Anwendungen sowie das Löschen verbotener Anwendungen werden über die Komponente Anwendungskontrolle ausgeführt.

Die Anwendungskontrolle ermöglicht die Installation von empfohlenen und obligatorischen Anwendungen auf Ihrem Gerät über einen direkten Link zur Distribution oder einen Link zu Google Play. Mithilfe der Anwendungskontrolle können Sie verbotene Anwendungen deinstallieren, die der korporativen Sicherheit nicht entsprechen.

Für die Ausführung der Anwendungskontrolle muss Kaspersky Endpoint Security als Dienst für erleichterte Bedienung installiert sein. Sie konnten den Dienst während der Ausführung des Schnellstartassistenten der Anwendung aktivieren. Wenn Sie diesen Schritt übersprungen haben, aktivieren Sie Kaspersky Endpoint Security als Dienst für erleichterte Bedienung im Abschnitt **Status**, indem Sie die entsprechende Benachrichtigung auswählen, oder in den Einstellungen des Geräts (**Android-Einstellungen** → **Erleichterte Bedienung** → **Dienste ausgewählt**).

## Datenschutz bei Verlust oder Diebstahl des Geräts

Damit Ihre Informationen nicht in fremde Hände gelangen, oder um das Gerät bei Verlust oder Diebstahl zu suchen, wird die Komponente Diebstahlschutz verwendet.

Der Diebstahlschutz erlaubt die ferngesteuerte Ausführung folgender Aktionen:

- Gerät sperren.

Damit ein Betrüger das Gerät nicht entsperren kann, muss auf mobilen Geräten unter dem Betriebssystem Android 7.0 und höher Kaspersky Endpoint Security als Dienst für erleichterte Bedienung installiert sein.

- Auf dem Geräte einen lauten Alarm aktivieren, selbst wenn das Gerät auf lautlos geschaltet ist.
- Gerätekoordinaten auf der Karte erhalten.
- Auf dem Gerät gespeicherte Daten löschen.
- Einstellungen auf die Werkseinstellungen zurücksetzen.
- Unbemerkt ein Foto der Person aufnehmen, die Ihr Gerät verwendet.

Für die Ausführung des Diebstahlschutzes muss Kaspersky Endpoint Security als Geräteadministrator installiert sein. Sie können die Administratorrechte für das Gerät während der Erstkonfiguration der Anwendungen zuweisen. Wenn Sie diesen Schritt übersprungen haben, weisen Sie Kaspersky Endpoint Security die Administratorrechte im Abschnitt **Status** zu, indem Sie die entsprechende Benachrichtigung auswählen, oder in den Einstellungen des Geräts (**Android-Einstellungen** → **Sicherheit** → **Geräteadministratoren**).

## Schutz vor Bedrohungen aus dem Internet

Die Komponente Web-Filter bietet Schutz vor Bedrohungen aus dem Internet.

Der Web-Filter blockiert bösartige Websites, deren Zweck darin besteht, einen schädlichen Code zu verbreiten, sowie Phishing-Websites, die Ihre vertraulichen Daten erschleichen und sich Zugang zu Ihren Finanzkonten verschaffen. Der Web-Filter untersucht Websites, bevor sie geöffnet werden. Dazu wird der Cloud-Dienst "Kaspersky Security Network" genutzt.

So aktivieren Sie Web-Filter:

- Kaspersky Endpoint Security muss als Dienst für erleichterte Bedienung installiert sein.

- Sie müssen die Erklärung zur Verarbeitung von Daten für die Verwendung von Web-Filter (Erklärung für Web-Filter) akzeptieren. Kaspersky Endpoint Security nutzt Kaspersky Security Network (KSN) zur Untersuchung von Websites. Die Erklärung für Web-Filter enthält die Nutzungsbedingungen für den Datenaustausch mit KSN.

Ihr Administrator kann die Erklärung für Web-Filter in Kaspersky Security Center für Sie akzeptieren. In einem solchen Fall werden von Ihnen keine weiteren Schritte benötigt.

Wenn Ihr Administrator die Erklärung für Web-Filter nicht akzeptiert hat und stattdessen Ihnen eine entsprechende Aufforderung zugesandt hat, müssen Sie die Erklärung für Web-Filter in den App-Einstellungen lesen und akzeptieren.

Wenn Ihr Administrator die Erklärung für Web-Filter nicht akzeptiert hat, ist Web-Filter nicht verfügbar.

Der Web-Filter funktioniert auf Android-Geräten nur mit den Browsern Google Chrome (einschließlich der Funktion Custom Tabs), Huawei Browser und Samsung Internet Browser. Web-Filter für Samsung Internet Browser blockiert keine Websites auf mobilen Geräten, wenn ein Arbeitsprofil verwendet wird und [Web-Filter nur für das Arbeitsprofil aktiviert ist](#).

## Hauptfenster im Überblick

Das Hauptfenster sieht je nach Bildschirmauflösung unterschiedlich aus.

Beim Auftreten von Problemen, die zur Senkung des Schutzniveaus, einer Infektion des Geräts oder dem Verlust von Informationen führen können, ändert sich das Aussehen des Hauptbildschirmes.

Im Abschnitt **Status** werden die folgenden Informationen angezeigt:

- Probleme beim Schutz Ihres Geräts
- Informationen über die Einhaltung der Anforderungen an die Unternehmenssicherheit auf Ihrem Gerät
- Informationen über den Schutzzustand Ihres Geräts

Sie können den Abschnitt **Status** öffnen, indem Sie in den oberen Teil des Hauptfensters von Kaspersky Endpoint Security klicken.

### Probleme beim Schutz des Geräts

Schutzprobleme werden nach Kategorien gruppiert. Für jedes Problem werden Aktionen genannt, die Sie zur Problemlösung ausführen können.

Im Abschnitt **Status** wird ferner eine Liste der übersprungenen Objekte angezeigt, die von der App gefunden wurden. Die Liste der übersprungenen Objekte kann sich ändern, beispielsweise wenn die schädliche Datei gelöscht oder verschoben wurde. Um die aktuelle Liste der Bedrohungen zu erhalten, [starten Sie die vollständige Untersuchung des Geräts](#). Für einen zuverlässigen Schutz Ihrer Daten entfernen Sie alle gefundenen Objekte.

Es gibt zwei Typen von Schutzproblemen:

- *Benachrichtigungen*. Gelb hervorgehoben. Benachrichtigungen informieren Sie über Ereignisse, die wichtig für die Sicherheit des Geräts sind (beispielsweise, dass die letzte Untersuchung länger als 14 Tage zurück liegt oder

dass eine neue Anwendung ohne Untersuchung installiert wurde). Das benachrichtigende Problem kann ausgeblendet werden. Danach ist die Information im Menü **Ausgeblendete Probleme** verfügbar.

- *Kritische Meldungen.* Rot hervorgehoben. Kritische Meldungen informieren Sie über Ereignisse, die vorrangige Priorität für die Sicherheit Ihres Geräts besitzen (z. B. dass das letzte Update der Antiviren-Datenbanken lange zurückliegt oder eine verbotene Anwendung installiert ist). Sie können kritische Meldungen nicht ausblenden.

## Übereinstimmungsüberprüfung

Die Anwendung überprüft automatisch, ob das Gerät der korporativen Sicherheit entspricht. Im Abschnitt **Status** werden folgende Informationen über die Einhaltung der Anforderungen an die Unternehmenssicherheit durch Ihr Gerät angezeigt.

- Grund der Nichtübereinstimmung des Geräts mit den Anforderungen an die Unternehmenssicherheit (beispielsweise wurden auf dem Gerät verbotene Apps gefunden).
- Zeitspanne, innerhalb der Sie die Nichtübereinstimmung beseitigen müssen (beispielsweise 24 Stunden).
- Aktion, die auf dem Gerät ausgeführt wird, wenn Sie die Abweichungen nicht im Laufe der angegebenen Zeitspanne beseitigen (z. B. Sperre des Geräts).
- Variante der Aktion zur Beseitigung der Nichtübereinstimmung des Geräts mit den Anforderungen der Unternehmensrichtlinie.

## Symbol in der Statuszeile

Nach dem Abschluss des Assistenten für die Erstkonfiguration wird das Symbol von Kaspersky Endpoint Security in der Statusleiste angezeigt.

Das Symbol dient als Aktivitätsanzeige für Anwendung und ermöglicht den Zugriff auf das Hauptfenster von Kaspersky Endpoint Security.

Das Symbol dient als Anzeige für die Ausführung von Kaspersky Endpoint Security und weist auf den Schutzstatus Ihres Geräts hin:

- ✓ – Das Gerät ist geschützt.
- ⚠ – Es gibt Probleme beim Schutz (z. B. sind die Antiviren-Datenbanken veraltet oder es wurde eine neue, nicht untersuchte Anwendung installiert).

## Untersuchung des Geräts

Anti-Virus hat eine Reihe von Beschränkungen:

- Bei der Ausführung von Anti-Virus im Arbeitsprofil ist es nicht möglich, eine Bedrohung, die im externen Gerätespeicher gefunden wurde (beispielsweise auf der SD-Karte) automatisch zu entfernen ([Apps mit einer „Aktentasche“](#), [Einstellungen des Arbeitsprofils Android anpassen](#)). Bei Kaspersky Endpoint Security für Android gibt es im Arbeitsprofil keinen Zugriff auf den externen Speicher. Die Informationen über die gefundenen Bedrohungen werden im [Abschnitt Status](#) der App angezeigt. Zur Beseitigung der im externen Speicher gefundenen Objekte muss die Datei manuell gelöscht und die Untersuchung des Geräts erneut gestartet werden.


- Aufgrund von technischen Beschränkungen kann Kaspersky Endpoint Security für Android Dateien mit einer Größe von mehr als 2 GB nicht untersuchen. Während der Untersuchung überspringt die App solche Dateien, und Sie werden nicht benachrichtigt, wenn solche Dateien übersprungen werden.

*Gehen Sie folgendermaßen vor, um eine Untersuchung des Geräts zu starten:*

1. Klicken Sie im Hauptfenster von Kaspersky Endpoint Security in der Schnellstart-Leiste auf **Scan**.
2. Wählen Sie den Untersuchungsbereich des Geräts aus:
  - **Gesamtes Gerät untersuchen.** Die Anwendung untersucht das gesamte Dateisystem des Geräts.
  - **Installierte Apps untersuchen.** Die Anwendung untersucht nur installierte Anwendungen.
  - **Benutzerdefinierte Untersuchung.** Die App überprüft den ausgewählten Ordner oder eine einzelne Datei. Sie können ein einzelnes Objekt (einen Ordner oder eine Datei) bzw. einen der folgenden Abschnitte des Gerätespeichers auswählen:
    - **Gerätespeicher.** Speicher des ganzen Geräts, der für den Lesezugriff verfügbar ist. Diesem Bereich gehört auch der Systemabschnitt des Speichers, auf dem die Dateien des Betriebssystems gespeichert werden, an.
    - **Interner Speicher.** Gerätespeicherabschnitt, der für die Installation von Apps und die Speicherung von Medieninhalten, Dokumenten und anderen Dateien vorgesehen ist.
    - **Externer Speicher.** Speicher der externen SD-Karte. Wenn keine externe SD-Karte installiert wurde, ist diese Variante verborgen.

Der Zugriff auf die Einstellungen der Untersuchung auf Viren kann durch Ihren Administrator beschränkt werden.


*Um die Untersuchung auf Viren anzupassen, gehen Sie wie folgt vor:*

1. Tippen Sie im Hauptfenster von Kaspersky Endpoint Security in der Schnellstart-Leiste auf  → **Einstellungen** → **Anti-Virus** → **Untersuchung**.
2. Wenn Sie möchten, dass die App während der Untersuchung Adware und Anwendungen erkennt, die von Angreifern verwendet werden können, um das Gerät oder Ihre Daten zu schädigen, aktivieren Sie den Schalter **Adware, Autodialer u. a.**
3. Klicken Sie auf **Aktion beim Fund einer Bedrohung** und wählen Sie die Standardaktion der App:
  - **Quarantäne**  
Die Quarantäne speichert diese Dateien in komprimierter Form, um eine Beschädigung des Geräts auszuschließen. Die Quarantäne ermöglicht das Löschen oder Wiederherstellen von Dateien in einen speziellen isolierten Speicher.
  - **Aktion erfragen**  
Die App fordert Sie auf, für jedes gefundene Objekt eine Aktion auszuwählen: überspringen, in die Quarantäne verschieben oder löschen. Beim Fund mehrerer Objekte können Sie die ausgewählte Aktion auf alle Objekte anwenden.
  - **Löschen**

Die gefundenen Objekte werden automatisch gelöscht. Es sind keine weiteren Aktionen erforderlich. Vor dem Löschen zeigt Kaspersky Endpoint Security eine kurze Benachrichtigung über den Fund des Objekts an.

- **Überspringen**

Wenn gefundene Objekte übersprungen wurden, warnt Kaspersky Endpoint Security Sie vor Problemen beim Schutz des Geräts. Die Informationen über die übersprungenen Objekte werden im Abschnitt **Status** der App angezeigt. Für jede übersprungene Bedrohung werden Aktionen angezeigt, die Sie ausführen können, um diese zu beseitigen. Die Liste der übersprungenen Objekte kann sich ändern, beispielsweise wenn die schädliche Datei gelöscht oder verschoben wurde. Um die aktuelle Liste der Bedrohungen zu erhalten, starten Sie die vollständige Untersuchung des Geräts. Für einen zuverlässigen Schutz Ihrer Daten entfernen Sie alle gefundenen Objekte.


Die App speichert die Informationen über die gefundenen Bedrohungen und die ausgeführten Aktionen in den Berichten der App ( → **Berichte**). Sie können die Berichte über die Ausführung des Anti-Virus anzeigen lassen.

## Untersuchung nach Zeitplan ausführen

Anti-Virus hat eine Reihe von Beschränkungen:

- Bei der Ausführung von Anti-Virus im Arbeitsprofil ist es nicht möglich, eine Bedrohung, die im externen Gerätespeicher gefunden wurde (beispielsweise auf der SD-Karte) automatisch zu entfernen ([Apps mit einer „Aktentasche“](#), [Einstellungen des Arbeitsprofils Android anpassen](#)). Bei Kaspersky Endpoint Security für Android gibt es im Arbeitsprofil keinen Zugriff auf den externen Speicher. Die Informationen über die gefundenen Bedrohungen werden im [Abschnitt Status](#) der App angezeigt. Zur Beseitigung der im externen Speicher gefundenen Objekte muss die Datei manuell gelöscht und die Untersuchung des Geräts erneut gestartet werden.
- Aufgrund von technischen Beschränkungen kann Kaspersky Endpoint Security für Android Dateien mit einer Größe von mehr als 2 GB nicht untersuchen. Während der Untersuchung überspringt die App solche Dateien, und Sie werden nicht benachrichtigt, wenn solche Dateien übersprungen werden.

*Gehen Sie folgendermaßen vor, um Zeitplan für die vollständige Untersuchung des Geräts anzupassen:*

1. Tippen Sie im Hauptfenster von Kaspersky Endpoint Security in der Schnellstart-Leiste auf  → **Einstellungen** → **Anti-Virus** → **Untersuchung**.

2. Klicken Sie auf **Zeitplan** und wählen Sie die Häufigkeit der vollständigen Untersuchung aus:

- **Wöchentlich**
- **Daily**
- **Deaktiviert**
- **Nach dem Datenbanken-Update**

3. Klicken Sie auf **Starttag** und wählen Sie den Wochentag, an dem die vollständige Untersuchung gestartet werden soll.

4. Klicken Sie auf **Startzeit** und geben Sie die Uhrzeit für den Start der vollständigen Untersuchung an.

Die vollständige Untersuchung des Geräts wird gemäß dem Zeitplan gestartet.

Unter Android 12 oder höher führt die App diese Aufgabe möglicherweise später aus, wenn sich das Gerät im Stromsparmodus befindet.

## Schutzmodus ändern

Der Echtzeitschutz kann Bedrohungen in geöffneten Dateien erkennen und Apps während ihrer Installation auf dem Gerät in Echtzeit untersuchen. Zur Gewährleistung des Schutzes werden automatisch die Antiviren-Datenbanken und der Cloud-Dienst Kaspersky Security Network (Cloud-Sicherheit) verwendet.

*Gehen Sie folgendermaßen vor, um den Schutzmodus des Geräts zu ändern:*

1. Tippen Sie im Hauptfenster von Kaspersky Endpoint Security in der Schnellstart-Leiste auf  → **Einstellungen** → **Anti-Virus** → **Echtzeitschutz**.

2. Bestimmen Sie den Schutzmodus für das Gerät:

- **Deaktiviert.** Der Schutz wurde deaktiviert.
- **Empfohlen.** Anti-Virus prüft nur die installierten Anwendungen und die Dateien aus dem Ordner "Downloads". Neue Anwendungen werden von Anti-Virus nur einmal untersucht, und zwar sofort nach der Installation.
- **Erweitert.** Anti-Virus untersucht alle Dateien auf schädliche Objekte. Eine Untersuchung erfolgt bei jeder Aktion, die mit Dateien auf dem Gerät ausgeführt wird (beispielsweise Speichern, Verschieben oder Ändern). Außerdem untersucht Anti-Virus neue Anwendungen sofort nach ihrer Installation.

Die Informationen über den geltenden Schutzmodus werden unter der Beschreibung der Komponente angezeigt.

Der Zugriff auf die Einstellungen des Echtzeitschutzes kann durch Ihren Administrator beschränkt werden.

*Um die Cloud-Sicherheit (KSN) zu aktivieren, gehen Sie wie folgt vor:*

1. Tippen Sie im Hauptfenster von Kaspersky Endpoint Security in der Schnellstart-Leiste auf  → **Einstellungen** → **Anti-Virus**.


2. Aktivieren Sie den Schalter **Cloud-Sicherheit (KSN)**.

Der Schalter **Cloud-Sicherheit (KSN)** verwaltet die Verwendung von Kaspersky Security Network nur für den Echtzeitschutz des Geräts. Wenn das Kontrollkästchen deaktiviert ist, verwendet Kaspersky Endpoint Security KSN weiterhin im Betrieb anderer App-Komponenten.

Die App erhält nun Zugriff auf die operative Wissensdatenbank von Kaspersky, welche die Reputationen von Dateien und Apps enthält. Bei der Untersuchung werden Bedrohungen gesucht, die schon in KSN eingetragen sind, auch wenn über sie noch keine Informationen in den Antiviren-Datenbanken vorhanden sind. Der Cloud-Dienst Kaspersky Security Network gewährleistet die uneingeschränkte Funktion von Anti-Virus und reduziert die Wahrscheinlichkeit von Fehlalarmen. Nur Ihr Administrator kann die Verwendung von Kaspersky Security Network vollständig deaktivieren.

*So konfigurieren Sie den Echtzeitschutz:*



1. Klicken Sie im Hauptfenster von Kaspersky Endpoint Security in der Schnellstart-Leiste auf  → **Einstellungen** → **Anti-Virus** → **Echtzeitschutz**.
2. Wenn Sie möchten, dass die App während der Untersuchung Adware und Anwendungen erkennt, die von Angreifern verwendet werden können, um das Gerät oder Ihre Daten zu schädigen, aktivieren Sie den Schalter **Adware, Autodialer u. a.**
3. Klicken Sie auf **Aktion beim Fund einer Bedrohung** und wählen Sie die Standardaktion der App:

- **Quarantäne**


Die Quarantäne speichert diese Dateien in komprimierter Form, um eine Beschädigung des Geräts auszuschließen. Die Quarantäne ermöglicht das Löschen oder Wiederherstellen von Dateien in einen speziellen isolierten Speicher.

- **Löschen**

Die gefundenen Objekte werden automatisch gelöscht. Es sind keine weiteren Aktionen erforderlich. Vor dem Löschen zeigt Kaspersky Endpoint Security eine kurze Benachrichtigung über den Fund des Objekts an.

- **Überspringen**

Wenn gefundene Objekte übersprungen wurden, warnt Kaspersky Endpoint Security Sie vor Problemen beim Schutz des Geräts. Die Informationen über die übersprungenen Objekte werden im Abschnitt **Status** der App angezeigt. Für jede übersprungene Bedrohung werden Aktionen angezeigt, die Sie ausführen können, um diese zu beseitigen. Die Liste der übersprungenen Objekte kann sich ändern, beispielsweise wenn die schädliche Datei gelöscht oder verschoben wurde. Um die aktuelle Liste der Bedrohungen zu erhalten, starten Sie die vollständige Untersuchung des Geräts. Für einen zuverlässigen Schutz Ihrer Daten entfernen Sie alle gefundenen Objekte.

Die App speichert die Informationen über die gefundenen Bedrohungen und die ausgeführten Aktionen in den Berichten der App ( → **Einstellungen** → **Berichte**). Sie können die Berichte über die Ausführung des Anti-Virus anzeigen lassen.

## Update der Antiviren-Datenbanken

*Um die Antiviren-Datenbanken der Anwendung zu aktualisieren:*

Tippen Sie im Hauptfenster von Kaspersky Endpoint Security in der Schnellstart-Leiste auf **Datenbanken-Update**.

## Datenbanken-Update nach Zeitplan

Die Anwendung kann die Antiviren-Datenbanken automatisch gemäß dem festgelegten Zeitplan aktualisieren.

*Gehen Sie folgendermaßen vor, um den Update-Zeitplan anzupassen:*

1. Tippen Sie im Hauptfenster von Kaspersky Endpoint Security in der Schnellstart-Leiste auf  → **Einstellungen** → **Anti-Virus** → **Datenbanken-Update**.

2. Klicken Sie auf **Zeitplan** und wählen Sie die Häufigkeit der Updates aus:

- **Wöchentlich**

- **Daily**

- **Deaktiviert**

3. Klicken Sie auf **Starttag** und wählen Sie den Wochentag, an dem das Update gestartet werden soll.

4. Klicken Sie auf **Startzeit** und geben Sie die Uhrzeit für den Start des Updates an.

Das Update der Antiviren-Datenbanken wird nach Zeitplan gestartet.

Unter Android 12 oder höher führt die App diese Aufgabe möglicherweise später aus, wenn sich das Gerät im Stromsparmodus befindet.

## Aktion bei Diebstahl oder Verlust des Geräts

Kontaktieren Sie Ihren Systemadministrator, falls Ihr Gerät gestohlen wird oder verloren geht. Der Administrator startet auf dem Gerät ferngesteuert die Funktionen des Diebstahlschutzes in Übereinstimmung mit den Anforderungen der Unternehmenssicherheit.

Sobald ein Befehl zum vollständigen Zurücksetzen an das Gerät gesendet wird, kann das Gerät nicht mehr gesteuert werden und die anderen Befehle des Diebstahlschutzes werden unwirksam.

## Web-Filter

So aktivieren Sie Web-Filter:

- Kaspersky Endpoint Security muss als Dienst für erleichterte Bedienung installiert sein.
- Sie müssen die Erklärung zur Verarbeitung von Daten für die Verwendung von Web-Filter (Erklärung für Web-Filter) akzeptieren. Kaspersky Endpoint Security nutzt Kaspersky Security Network (KSN) zur Untersuchung von Websites. Die Erklärung für Web-Filter enthält die Nutzungsbedingungen für den Datenaustausch mit KSN.

Ihr Administrator kann die Erklärung für Web-Filter in Kaspersky Security Center für Sie akzeptieren. In einem solchen Fall werden von Ihnen keine weiteren Schritte benötigt.

Wenn Ihr Administrator die Erklärung für Web-Filter nicht akzeptiert hat und stattdessen Ihnen eine entsprechende Aufforderung zugesandt hat, müssen Sie die Erklärung für Web-Filter in den App-Einstellungen lesen und akzeptieren.

Wenn Ihr Administrator die Erklärung für Web-Filter nicht akzeptiert hat, ist Web-Filter nicht verfügbar.

Der Web-Filter funktioniert auf Android-Geräten nur mit den Browsern Google Chrome (einschließlich der Funktion Custom Tabs), Huawei Browser und Samsung Internet Browser. Web-Filter für Samsung Internet Browser blockiert keine Websites auf mobilen Geräten, wenn ein Arbeitsprofil verwendet wird und [Web-Filter nur für das Arbeitsprofil aktiviert ist](#).

Wenn Sie möchten, dass Web-Filter die Websites während der Arbeit im Internet im Echtzeitmodus überprüft, legen Sie Google Chrome oder Samsung Internet Browser als Standardbrowser fest.

*Gehen Sie folgendermaßen vor, um den unterstützten Browser als Standardbrowser festzulegen und den Web-Filter für die permanente Untersuchung von Websites zu verwenden:*

1. Tippen Sie im Hauptfenster von Kaspersky Endpoint Security in der Schnellstart-Leiste auf  → **Einstellungen** → **Web-Filter**.

2. Stellen Sie den Umschalter **Web-Filter** auf An.

3. Tippen Sie auf **Standardbrowser festlegen**.

Diese Schaltfläche wird angezeigt, wenn der Web-Filter aktiviert ist, aber kein unterstützter Browser als Standardbrowser festgelegt ist.

Es wird ein Assistent zum Festlegen des Standardbrowsers gestartet.

4. Folgen Sie den Anweisungen des Assistenten.

Nach Abschluss des Assistenten wird Google Chrome, Huawei Browser oder Samsung Internet Browser als Standardbrowser festgelegt. Web-Filter wird die Websites während der Arbeit im Internet im Echtzeitmodus überprüfen.

## Anwendungskontrolle

Die *Anwendungskontrolle* führt eine Untersuchung der auf dem mobilen Gerät installierten Apps auf Übereinstimmung mit den Anforderungen an die Unternehmenssicherheit durch. Der Administrator erstellt in Kaspersky Security Center entsprechend den Anforderungen an die Unternehmenssicherheit Listen von erlaubten, verbotenen, obligatorischen und empfohlenen Apps. Nach der Ausführung der Anwendungskontrolle bietet Kaspersky Endpoint Security an, obligatorische und empfohlene Apps zu installieren sowie verbotene Apps zu löschen. Verbotene Apps können nicht auf dem mobilen Gerät gestartet werden.

*Um obligatorische und empfohlene Apps zu installieren bzw. verbotene Apps zu löschen, gehen Sie wie folgt vor:*


1. Wechseln Sie zum Abschnitt **Status** von Kaspersky Endpoint Security.

2. Wählen Sie die Aufgabe "Anwendungskontrolle" aus.

3. Führen Sie die angebotenen Aktionsvarianten aus.

## Zertifikat anfordern

*Gehen Sie folgendermaßen vor, um ein Zertifikat für den Zugriff auf Ressourcen aus dem Unternehmensnetzwerk anzufordern:*

1. Tippen Sie im Hauptfenster von Kaspersky Endpoint Security in der Schnellstart-Leiste auf  → **Einstellungen** → **Erweitert** → **Anfordern eines Zertifikats**.

2. Geben Sie Ihre Anmeldedaten für das Unternehmensnetzwerk an.

3. Falls Sie vom Administrator ein einmaliges Kennwort erhalten haben, aktivieren Sie das Kontrollkästchen **Einmalkennwort** und geben Sie dieses Kennwort ein.

Der Assistent zur Zertifikatinstallation wird gestartet.

4. Folgen Sie den Anweisungen des Assistenten.

## Synchronisierung mit Kaspersky Security Center

Die Synchronisierung des mobilen Geräts mit dem Remote-Verwaltungssystem für Kaspersky Security Center ist für den Schutz und die Konfiguration Ihres Geräts in Übereinstimmung mit den Anforderungen an die Unternehmenssicherheit erforderlich. Die Synchronisierung des Geräts mit Kaspersky Security Center wird automatisch ausgeführt. Sie können die Synchronisierung auch manuell ausführen. Nach der ersten Synchronisierung wird Ihr Gerät in die Liste der mobilen Geräte aufgenommen, die durch Kaspersky Security Center verwaltet werden. Danach kann der Administrator die Einstellungen Ihres Geräts gemäß der korporativen Sicherheit festlegen.

Sie können die Einstellungen für die Synchronisierung während der Ausführung des Assistenten für die Erstkonfiguration bzw. in den Einstellungen von Kaspersky Endpoint Security anpassen. Die Synchronisierungseinstellungen müssen separat angepasst werden, wenn Sie Kaspersky Endpoint Security mithilfe von Google Play installiert haben. Für den Erhalt von Einstellungswerten für die Synchronisierung wenden Sie sich an den Administrator.

Ändern Sie die Einstellungen für die Synchronisierung des Geräts mit dem Remote-Management-System von Kaspersky Security Center nur nach Aufforderung des Administrators.

*Um das Gerät mit Kaspersky Security Center zu synchronisieren, gehen Sie wie folgt vor:*

1. Tippen Sie im Hauptfenster von Kaspersky Endpoint Security in der Schnellstart-Leiste auf  → **Einstellungen** → **Synchronisierung**.

2. Legen Sie im Abschnitt **Synchronisierungseinstellungen** Werte für folgende Einstellungen fest:

- **Server**
- **Port**
- **Gruppe**
- **Geschäftliche E-Mail-Adresse**

Die Synchronisierungseinstellungen können vom Administrator ausgeblendet werden.

3. Klicken Sie auf **Synchronisieren**.

## Die App "Kaspersky Endpoint Security für Android" ohne Kaspersky Security Center aktivieren

In den meisten Fällen wird die auf Ihrem Gerät installierte App "Kaspersky Endpoint Security für Android" vom Administrator zentral im Remote-Verwaltungssystem Kaspersky Security Center aktiviert. Wenn Ihr Gerät nicht mit Kaspersky Security Center verbunden ist, können Sie den Aktivierungscode manuell eingeben. Wenden Sie sich an den Administrator, um den Aktivierungscode zu erhalten.

Aktivieren Sie die App nur dann manuell, wenn Sie vom Administrator dazu aufgefordert werden.

*So geben Sie den Aktivierungscode ein:*

1. Tippen Sie in der Fehlermeldung, die Sie darüber informiert, dass Ihre Lizenz bald abläuft oder abgelaufen ist und dass Ihr Gerät nicht mit dem Administrationsserver verbunden ist, auf **Aktivieren**.
2. Geben Sie im Aktivierungsfenster den Aktivierungscode ein, den Sie vom Administrator erhalten haben, und tippen Sie dann auf **Aktivieren**.
3. Wenn der Aktivierungscode korrekt ist, wird eine Benachrichtigung über die erfolgte Aktivierung der App zusammen mit dem Ablaufdatum der Lizenz angezeigt.

Die App "Kaspersky Endpoint Security für Android" auf Ihrem Gerät ist nun aktiviert.

## App aktualisieren

Kaspersky Endpoint Security kann folgendermaßen aktualisiert werden:

- Manuell mithilfe von Google Play. Sie laden von Google Play eine neue Version der App herunter und installieren sie auf Ihrem Gerät.
- Mithilfe des Administrators. Der Administrator aktualisiert die Version der App auf Ihrem Gerät ferngesteuert mithilfe des Remote-Management-Systems Kaspersky Security Center.

### Update mithilfe von Google Play

Der Administrator kann Ihnen verbieten, die App mithilfe von Google Play zu aktualisieren.

Das Update mithilfe von Google Play wird mit der für die Android-Plattform typischen Methode ausgeführt. Für das Update der App müssen folgende Bedingungen erfüllt sein:

- Sie müssen über ein Google-Konto verfügen.
- Das Gerät muss dem Google-Konto zugeordnet sein.
- Das Gerät muss mit dem Internet verbunden sein.

Detaillierte Informationen über das Anlegen eines Google-Kontos, die Zuordnung des Geräts zum Google-Konto und die Nutzung von Google Play erfahren Sie auf der [Seite des technischen Supports von Google](#).

### Update mithilfe von Kaspersky Security Center

Das Update der App mithilfe von Kaspersky Security Center besteht aus den folgenden Schritten:

1. Der Administrator sendet an Ihr mobiles Gerät eine Distribution der App, deren Version den Anforderungen an die Unternehmenssicherheit entspricht.

Auf Ihrem Gerät wird eine Aufforderung zur Installation von Kaspersky Endpoint Security angezeigt.

## 2. Akzeptieren Sie die Bedingungen des Updates.

Die neue Version der App wird auf Ihrem Gerät installiert. Eine zusätzliche Konfiguration der App nach dem Update ist nicht erforderlich.

## Anwendung deinstallieren


Der Administrator kann Ihnen verbieten, die Anwendung selbständig zu löschen. In diesem Fall ist das Löschen Kaspersky Endpoint Security unmöglich.

Kaspersky Endpoint Security kann folgendermaßen gelöscht werden:

- Selbständig in den Einstellungen der Anwendung.
- Selbständig in den Einstellungen des Geräts.
- Mithilfe des Administrators. Der Administrator kann die Anwendung ferngesteuert mithilfe des Remote-Management-Systems Kaspersky Security Center von Ihrem Gerät löschen.

### Löschen in den Einstellungen der Anwendung

*Um Kaspersky Endpoint Security von Ihrem Gerät zu entfernen, gehen Sie wie folgt vor:*

1. Tippen Sie im Hauptfenster von Kaspersky Endpoint Security in der Schnellstart-Leiste auf  → **App löschen**.

Der Deinstallationsassistent der Anwendung wird gestartet.

2. Folgen Sie den Anweisungen des Assistenten.

### Löschen in den Einstellungen des Geräts

Die Deinstallation der Anwendung wird mit der für die Android-Plattform typischen Methode ausgeführt. Für das Löschen der Anwendung ist es erforderlich, die Administratorrechte für Kaspersky Endpoint Security in den Sicherheitseinstellungen des Geräts zu deaktivieren.

Auf Geräten unter dem Betriebssystem Android Version 7.0 und höher wird beim Versuch die Anwendung in den Android-Einstellungen zu löschen, das Gerät blockiert, wenn der Administrator das Löschen verboten hat. Für die Entsperrung des Geräts wenden sich an Ihrem Administrator.

### Löschen mithilfe von Kaspersky Security Center

Das Löschen der Anwendung mithilfe von Kaspersky Security Center besteht aus den folgenden Schritten:

1. Der Administrator sendet den Befehl zum Löschen der Anwendung auf Ihr mobiles Gerät.  
Ihr mobiles Gerät zeigt eine Aufforderung an, die Deinstallation von Kaspersky Endpoint Security zu bestätigen.

2. Bestätigen Sie die Deinstallation der Anwendung.

Die Anwendung wird von Ihrem Gerät gelöscht.

## Apps mit einer "Aktentasche"



Das Symbol der App im Arbeitsprofil Android

Apps, die mit einem Aktentasche-Symbol markiert sind (korporative Apps), befinden sich auf Ihrem Gerät im Arbeitsprofil Android (im Folgenden auch "Arbeitsprofil"). Das *Arbeitsprofil Android* ist eine sichere Umgebung auf Ihrem Gerät, in der der Administrator die Verwaltung von Apps und Konten ausführen kann, ohne Sie in Ihren Möglichkeiten bei der Arbeit mit persönlichen Daten einzuschränken.

Das Arbeitsprofil ermöglicht ein Speichern der Unternehmensdaten getrennt von den persönlichen Daten. Dies gewährleistet die Vertraulichkeit der Unternehmensdaten und ihren Schutz vor Schadsoftware. Bei der Erstellung des Arbeitsprofils auf Ihrem mobilen Gerät werden im Arbeitsprofil automatisch folgende korporativen Apps installiert: Google Play, Google Chrome, Downloads, Kaspersky Endpoint Security für Android und sonstige.

## Die Anwendung KNOX



Das KNOX-Symbol

Die KNOX-App öffnet den KNOX-Container auf Ihrem Gerät. Der *KNOX-Container* ist eine sichere Umgebung auf Ihrem Gerät mit einem separaten Desktop, einer Startleiste, Apps und Widgets. Der Administrator kann die App und die Benutzerkonten im KNOX-Container verwalten, ohne Sie in Ihren Möglichkeiten bei der Arbeit mit persönlichen Daten einzuschränken.

Der KNOX-Container ermöglicht ein Speichern der Unternehmensdaten getrennt von den persönlichen Daten. Dies gewährleistet die Vertraulichkeit der Unternehmensdaten und ihren Schutz vor Schadsoftware.

Im KNOX-Container stehen Ihnen das E-Mail-Postfach des Unternehmens, die Kontaktdaten der Mitarbeiter des Unternehmens, der Dateispeicher und andere Apps zur Verfügung.

Details über die Arbeit mit KNOX finden Sie auf der [Seite des technischen Supports von Samsung](#).<sup>12</sup>

# Verwendung der App Kaspersky Security für iOS

In diesem Hilfeabschnitt werden Funktionen und Vorgänge beschrieben, die den Benutzern der App Kaspersky Security für iOS zur Verfügung stehen.

Die Artikel in diesem Abschnitt besprechen alle Optionen, die auf einem mobilen Gerät verfügbar oder sichtbar sind. Das eigentliche Layout und Verhalten der App hängt davon ab, welches Remote-Verwaltungssystem implementiert ist und auf welche Weise der Administrator die Einstellungen Ihres Geräts mit Rücksicht auf die Anforderungen an die Unternehmenssicherheit anpasst. Einige der in diesem Abschnitt beschriebenen Funktionen und Optionen spiegeln womöglich nicht Ihre Erfahrung mit der App wider. Bei Fragen zur App auf Ihrem konkreten Gerät wenden Sie sich bitte an Ihren Administrator.

## Funktionen der Anwendung

Kaspersky Security für iOS bietet folgende Funktionen.

### Schutz vor Bedrohungen aus dem Internet

Die Komponente Web-Filter bietet Schutz vor Bedrohungen aus dem Internet.

Der Web-Filter blockiert bösartige Websites, deren Zweck darin besteht, einen schädlichen Code zu verbreiten, sowie Phishing-Websites, die Ihre vertraulichen Daten erschleichen und sich Zugang zu Ihren Finanzkonten verschaffen. Der Web-Filter untersucht Websites, bevor sie geöffnet werden. Dazu wird der Cloud-Dienst "Kaspersky Security Network" genutzt. Der Web-Filter untersucht auch die Online-Aktivitäten der Apps auf Ihrem Gerät.

Damit der Web-Filter funktioniert, müssen Sie der App erlauben, eine VPN-Konfiguration hinzuzufügen.

### Erkennung von Jailbreaks

Wenn Kaspersky Security für iOS einen Jailbreak erkennt, wird eine Warnung angezeigt und Ihr Administrator erhält eine Problemmeldung.

Die App kann nicht für die Sicherheit Ihres Gerätes garantieren, da ein Jailbreak bestimmte Sicherheitsfunktionen umgeht und zahlreiche Probleme verursachen kann wie beispielsweise:

- Sicherheitslücken
- Stabilitätsprobleme
- Störung von Apple-Diensten
- Mögliche Abstürze und Einfrieren des Gerätes
- Verkürzte Akkulaufzeit
- Fehler beim Anwenden von iOS-Updates



# App installieren

*Um die App Kaspersky Security für iOS zu installieren:*

1. Suchen Sie nach der E-Mail-Nachricht, mit der Ihr Administrator Sie einlädt, Kaspersky Security für iOS aus dem App Store zu installieren.
2. Gehen Sie zum App Store. Dafür gibt es die folgenden Möglichkeiten:
  - Tippen Sie auf den Link, wenn Sie die Nachricht auf dem iOS-Gerät lesen, auf dem Sie die App installieren möchten.
  - Scannen Sie den QR-Code mit dem iOS-Gerät, auf dem Sie die App installieren möchten, wenn Sie die Nachricht auf einem Computer lesen.

Der Einladungslink ist für 24 Stunden gültig. Sollte der Link ablaufen, bevor Sie die App installiert haben, fordern Sie bei Ihrem Administrator eine neue Einladung an.

3. Laden Sie die App aus dem App Store herunter und installieren Sie sie. Folgen Sie dazu dem standardmäßigen Installationsverfahren auf der iOS-Plattform.

Die App Kaspersky Security für iOS ist jetzt auf Ihrem Gerät installiert. Um das Gerät zu schützen, aktivieren Sie die App.

# App aktivieren

*Um die App Kaspersky Security für iOS zu aktivieren, gehen Sie wie folgt vor:*

1. Starten Sie die App auf Ihrem Gerät.
2. Akzeptieren Sie die Vereinbarungen und Erklärungen, indem Sie die Kontrollkästchen **Endbenutzer-Lizenzvertrag** und **Datenschutzrichtlinie für Produkte und Dienste** aktivieren.

Akzeptieren Sie optional die **Erklärung zu Kaspersky Security Network**, um zuzustimmen, dass Statistiken an Kaspersky Security Network gesendet werden. Dadurch wird die Leistung der App verbessert und für einen unterbrechungsfreien Betrieb gesorgt.
3. Tippen Sie auf **Weiter**. Die App stellt eine Verbindung zu dem Fernverwaltungssystem Kaspersky Security Center her und fordert Lizenzinformationen an.
4. Erlauben Sie der App, eine VPN-Konfiguration hinzuzufügen. Die App verwendet die VPN-Konfiguration, um Websites auf Phishing zu untersuchen und Ihr Gerät vor Schadsoftware zu schützen.
5. Erlauben Sie der App, Push-Benachrichtigungen zu senden. Die App verwendet Benachrichtigungen, um Sie über Sicherheitsprobleme und den Status Ihrer Lizenz zu informieren.

Die App "Kaspersky Security für iOS" auf Ihrem Gerät ist nun aktiviert.

# Die App mit einem Aktivierungscode aktivieren

Wenn Sie Kaspersky Security für iOS auf Ihrem Gerät installieren, stellt die App automatisch eine Verbindung zum Fernverwaltungssystem Kaspersky Security Center her und ruft Lizenzinformationen ab. Wenn Ihr Gerät nicht mit Kaspersky Security Center verbunden ist, können Sie den Aktivierungscode manuell eingeben. Wenden Sie sich an den Administrator, um den Aktivierungscode zu erhalten.

Aktivieren Sie die App nur dann manuell, wenn Sie vom Administrator dazu aufgefordert werden.

*So geben Sie den Aktivierungscode ein:*

1. Tippen Sie in der Nachricht, die über die fehlende Aktivierung der App informiert, auf **App aktivieren**.
2. Geben Sie im Aktivierungsfenster den Aktivierungscode ein, den Sie vom Administrator erhalten haben, und tippen Sie dann auf **Aktivieren**.

Wenn der Aktivierungscode korrekt ist, wird eine Benachrichtigung über die erfolgte Aktivierung der App zusammen mit dem Ablaufdatum der Lizenz angezeigt.

Die App "Kaspersky Security für iOS" auf Ihrem Gerät ist nun aktiviert.

## Hauptfenster im Überblick

Das Hauptfenster sieht je nach Bildschirmauflösung unterschiedlich aus.

Das Hauptfenster enthält:

- Allgemeiner Schutzstatus Ihres Gerätes.
- Nachrichten, die sich auf den Status von App-Komponenten und Schutzproblemen beziehen.

Es gibt drei Arten von Nachrichten:

- Grün hervorgehoben. Statusnachrichten, die darüber informieren, dass der Schutz in bestimmten Bereichen aktiv ist.
- Gelb hervorgehoben. Informative Nachrichten, die über Ereignisse informieren, die die Gerätesicherheit beeinflussen können.
- Rot hervorgehoben. Kritische Nachrichten, die über Ereignisse informieren, die für die Gerätesicherheit kritisch sind.

Sie können auf eine Nachricht tippen, um Details zu erhalten.

## App aktualisieren

Sie können die neueste Version von Kaspersky Security für iOS aus dem App Store herunterladen und wie auf der iOS-Plattform üblich auf Ihrem Gerät installieren. Außerdem können Sie die automatischen Updates aktivieren. Die App muss nach dem Update nicht zusätzlich konfiguriert werden.

Für das Update der App müssen folgende Bedingungen erfüllt sein:

- Sie benötigen eine Apple-ID.

- Das Gerät muss Ihrem Apple-Konto verknüpft sein.
- Das Gerät muss mit dem Internet verbunden sein.

Auf der [Apple-Support-Website](#) erfahren Sie, wie Sie eine Apple-ID erstellen, Ihr Gerät mit Ihrer Apple-ID verknüpfen und den App Store verwenden können.

## Anwendung deinstallieren

*Um die App Kaspersky Security für iOS zu entfernen, folgen Sie dem standardmäßigen Verfahren auf der iOS-Plattform:*

1. Halten Sie auf dem Startbildschirm das App-Symbol gedrückt.
2. Entfernen Sie die App.

Die App Kaspersky Security für iOS wurde jetzt von Ihrem Gerät entfernt.

# Lizenzverwaltung für das Programm

Dieser Abschnitt informiert über die wichtigsten Begriffe, die mit der Lizenzierung von Kaspersky Security für mobile Endgeräte zusammenhängen.

## Über den Lizenzvertrag

Der *Endbenutzer-Lizenzvertrag* (EULA) ist ein rechtsgültiger Vertrag zwischen Ihnen und AO Kaspersky Lab. Er bestimmt die Bedingungen für Kaspersky Security für mobile Endgeräte.

Lesen Sie die Bedingungen des EULA sorgfältig durch, bevor Sie beginnen, mit Kaspersky Security für mobile Endgeräte zu arbeiten.

Sie können sich die Bedingungen des EULA auf folgende Arten ansehen:

- Während der Installation der Komponenten von Kaspersky Security für mobile Endgeräte.
- Lesen Sie die Datei `license.txt`, die im selbstextrahierenden Archiv des Programmpakets für die Installation der App "Kaspersky Endpoint Security für Android" enthalten ist.
- In Kaspersky Endpoint Security für Android unter **Über die App**.
- Im Abschnitt **Über die App** → **Verträge und Erklärungen** in Kaspersky Security für iOS.
- Im Abschnitt **Erweitert** → **Akzeptierte Lizenzverträge** in den Eigenschaften des Administrationsservers. Diese Funktion ist in Kaspersky Security Center 12.1 und höher verfügbar.

Wenn Sie bei der Installation der Komponenten von Kaspersky Security für mobile Endgeräte dem Text des Endbenutzer-Lizenzvertrags (EULA) zustimmen, gelten die Bedingungen des Endbenutzer-Lizenzvertrags als akzeptiert. Falls Sie die Bedingungen des Endbenutzer-Lizenzvertrags ablehnen, müssen Sie die Installation der Komponenten von Kaspersky Security für mobile Endgeräte abbrechen und dürfen diese nicht verwenden.

## Lizenz-Info

Die *Lizenz* begründet ein zeitlich begrenztes Nutzungsrecht für die integrierte Lösung "Kaspersky Security für mobile Endgeräte", die Ihnen auf Basis eines Endbenutzer-Lizenzvertrags überlassen wird.

Die Lizenz berechtigt Sie zur Nutzung folgender Leistungen:

- Nutzung der Anwendungen auf mobilen Endgeräten gemäß den Bestimmungen des Endbenutzer-Lizenzvertrags.
- Technischer Support.

Der Umfang der verfügbaren Leistungen und die Nutzungsdauer der mobilen Anwendungen sind vom Typ der Lizenz abhängig, mit der die Anwendung aktiviert wurde.

Es sind folgende Lizenztypen vorgesehen:

- *Test*.

Eine kostenlose Lizenz, die dazu dient, sich mit Kaspersky Security für mobile Endgeräte vertraut zu machen.

Die Testlizenz ist 30 Tage gültig. Nach Ablauf der Testlizenz stellt die mobile App "Kaspersky Endpoint Security für Android" und "Kaspersky Security für iOS" die Ausführung der meisten Funktionen ein. Eine Ausnahme ist die Synchronisierung mit dem Administrationsserver. Um die App weiter nutzen zu können, müssen Sie eine kommerzielle Lizenz erwerben.

- *Kommerziell.*

Eine Lizenz, die beim Kauf von Kaspersky Security für mobile Endgeräte zur Verfügung gestellt wird.

Nach Ablauf der Gültigkeitsdauer der kommerziellen Lizenz wird die mobile App weiterhin mit begrenzter Funktionalität ausgeführt.

Im eingeschränkten Funktionsmodus sind je nach App die folgenden Komponenten verfügbar.

- App "Kaspersky Endpoint Security für Android":
  - **Anti-Virus.** Echtzeitschutz und die Untersuchung des Geräts auf Viren sind verfügbar; das Update der Antiviren-Datenbanken ist nicht verfügbar.
  - **Diebstahlschutz.** Nur der Versand von Befehlen an das mobile Gerät ist verfügbar.
  - **Synchronisierung mit dem Administrationsserver.**

Kaspersky Endpoint Security für Android beendet den Austausch von Informationen mit [Kaspersky Security Network](#), [Google Analytics for Firebase](#), [SafetyNet Attestation](#), [Firebase Performance Monitoring und Crashlytics](#) im Falle einer Sperrung des [Kaspersky-Schlüssels](#) nach Ablauf der Testlizenz und beim Fehlen einer Lizenz (wenn der Aktivierungscode aus der Gruppenrichtlinie entfernt wurde).

- App von Kaspersky Security für iOS:
  - **Synchronisierung mit dem Administrationsserver.**

Wenn die Testlizenz abläuft oder keine Lizenz vorhanden ist (der Aktivierungscode aus der Gruppenrichtlinie entfernt wurde), tauscht Kaspersky Security für iOS keine Informationen mehr mit [Kaspersky Security Network](#) aus.

Die übrigen Komponenten der mobilen App stehen dem Gerätebenutzer nicht zur Verfügung. Der Administrator kann diese Komponenten im eingeschränkten Funktionsmodus mithilfe von Gruppenrichtlinien verwalten. Die übrigen Komponenten der App können nicht mithilfe von Gruppenrichtlinien angepasst werden.

Zur weiteren Nutzung der App mit allen Funktionen ist eine Verlängerung der kommerziellen Lizenz erforderlich. Es wird empfohlen, die Gültigkeitsdauer der Lizenz rechtzeitig vor dem Ablaufdatum zu verlängern oder eine neue Lizenz zu kaufen. Nur so lässt sich ein optimaler Schutz vor allen Computerbedrohungen gewährleisten.

## Über das Abonnement

Ein Abonnement für Kaspersky Security für mobile Endgeräte ist ein Auftrag, nach dem die mobile Anwendung mit bestimmten Einstellungen (Abonnement-Laufzeit, Anzahl der geschützten mobilen Geräte) genutzt werden kann. Ein Abonnement für Kaspersky Security für mobile Endgeräte kann bei einem Provider registriert werden (z. B. bei einem Internet-Provider). Das Abonnement kann manuell oder automatisch verlängert oder auch gekündigt werden. Das Abonnement wird auf der Provider-Webseite verwaltet.

Ein Abonnement kann beschränkt (z. B. auf ein Jahr) oder unbeschränkt sein (ohne Ablaufdatum). Um Kaspersky Security für mobile Endgeräte weiterhin zu nutzen, muss ein beschränktes Abonnement rechtzeitig verlängert werden. Ein unbeschränktes Abonnement wird automatisch verlängert, falls der vereinbarte Betrag rechtzeitig an den Dienstleister überwiesen wird.

Nach Ablauf eines befristeten Abonnements wird möglicherweise eine Übergangsfrist zur Abonnement-Verlängerung gewährt, während der die Funktionalität der App erhalten bleibt. Verfügbarkeit und Dauer der Nachfrist werden vom Lieferanten der Dienstleistungen bestimmt.

Um Kaspersky Security für mobile Endgeräte mit einem Abonnement zu nutzen, muss der Aktivierungscode übernommen werden, den Sie von Ihrem Provider erhalten. Nach Übernahme des Aktivierungscode wird der Schlüssel für die Lizenz zur Nutzung des Programms gemäß dem Abonnement installiert.

Für die Abonnement-Verwaltung stehen je nach Provider unterschiedliche Optionen zur Verfügung. Der Provider stellt möglicherweise keine Übergangsfrist für die Verlängerung des Abonnements zur Verfügung, innerhalb der die Funktionen der App erhalten bleiben.

Die für ein Abonnement erhaltenen Aktivierungscodes können nicht für die Aktivierung vorheriger Versionen von Kaspersky Security für mobile Endgeräte verwendet werden.

## Über den Schlüssel

Ein *Schlüssel* ist eine Bitsequenz, mit deren Hilfe Sie die komplexe Lösung Kaspersky Security für mobile Endgeräte aktivieren können, um sie dann in Übereinstimmung mit dem Endbenutzer-Lizenzvertrag zu nutzen. Der Schlüssel wird von den Kaspersky-Experten generiert.

Einen Schlüssel für die mobile App können Sie mithilfe einer Schlüsseldatei oder eines Aktivierungscodes hinzufügen:

- Wenn Ihr Unternehmen das Programmpaket Kaspersky Security Center bereitstellt, müssen Sie die [Schlüsseldatei](#) verwenden und diese [an die mobilen Android-Apps verteilen](#). Der Schlüssel wird auf der Programmoberfläche von Kaspersky Security Center und auf der Programmoberfläche der mobilen Android-App als eine einmalige alphanumerische Zeichenfolge angezeigt.

Hinzugefügte Schlüssel können später durch andere Schlüssel ersetzt werden.

Die App "Kaspersky Security für iOS" kann nicht mit einer Schlüsseldatei aktiviert werden.

- Wenn Ihr Unternehmen Kaspersky Security Center nicht verwendet, müssen Sie den [Aktivierungscode](#) mit dem Benutzer teilen. Der Benutzer gibt diesen Aktivierungscode in der mobilen Android- oder iOS-App ein. Der Schlüssel wird auf der Programmoberfläche der mobilen App als eine einmalige alphanumerische Zeichenfolge angezeigt.

Ein Schlüssel kann von Kaspersky gesperrt werden, wenn beispielsweise die Bedingungen des Lizenzvertrags verletzt werden. Ist der Schlüssel gesperrt, stellt die mobile App die Ausführung der aller Funktionen ein. Eine Ausnahme ist die Synchronisierung mit dem Administrationsserver. Um die App weiter nutzen zu können, müssen Sie einen anderen Schlüssel hinzufügen.

## Über den Aktivierungscode

Der *Aktivierungscode* ist eine eindeutige Zeichenfolge aus zwanzig Buchstaben und Ziffern. Wenn Sie den Aktivierungscode eingeben, wird ein Schlüssel hinzugefügt, mit dem die mobile App "Kaspersky Endpoint Security für Android" oder "Kaspersky Security für iOS" aktiviert wird. Sie erhalten den Aktivierungscode an die von Ihnen angegebene E-Mail-Adresse, nachdem Sie die komplexe Lösung Kaspersky Security für mobile Endgeräte erworben haben oder eine Testversion von Kaspersky Security für mobile Endgeräte bestellt haben.

Zur Aktivierung der mobilen App mithilfe eines Aktivierungscodes ist ein Internetzugang erforderlich, um eine Verbindung mit den Aktivierungsservern von Kaspersky herzustellen.

Wenn der Aktivierungscode nach der Aktivierung der mobilen Anwendung verloren geht, können Sie ihn wiederherstellen. Der Aktivierungscode kann beispielsweise für die Registrierung im Kaspersky CompanyAccount erforderlich sein. Wenden Sie sich an den [Technischen Support von Kaspersky](#), um den Aktivierungscode wiederherzustellen.

## Über die Schlüsseldatei

Eine *Schlüsseldatei* ist eine Datei mit der Erweiterung key, die Sie von Kaspersky erhalten. Die Schlüsseldatei dient dazu, einen Schlüssel für die Aktivierung der mobilen App "Kaspersky Endpoint Security für Android" hinzuzufügen.

Die App "Kaspersky Security für iOS" kann nicht mit einer Schlüsseldatei aktiviert werden.

Sie erhalten die Schlüsseldatei an die von Ihnen angegebene E-Mail-Adresse, nachdem Sie die komplexe Lösung "Kaspersky Security für mobile Endgeräte" erworben haben oder eine Testversion von Kaspersky Security für mobile Endgeräte bestellt haben.

Um die Anwendung mit einer Schlüsseldatei zu aktivieren, ist keine Verbindung mit den Aktivierungsservern von Kaspersky erforderlich.

Eine versehentlich gelöschte Schlüsseldatei kann wiederhergestellt werden. Die Schlüsseldatei kann unter anderem auch für die Registrierung bei Kaspersky CompanyAccount erforderlich sein.

Zur Wiederherstellung der Schlüsseldatei müssen Sie eine der folgenden Aktionen ausführen:

- Kontaktieren Sie den Lizenzverkäufer.
- Rufen Sie die Schlüsseldatei anhand Ihres verfügbaren Aktivierungscodes auf der [Website von Kaspersky](#) ab.

## Bereitstellung von Daten in Kaspersky Endpoint Security für Android

Kaspersky Security für mobile Endgeräte entspricht der Datenschutz-Grundverordnung (DSGVO).

Um die App zu installieren, müssen entweder Sie selbst oder der Benutzer des Geräts die Bedingungen des Endbenutzer-Lizenzvertrags lesen und akzeptieren. Darüber hinaus können Sie eine Richtlinie so konfigurieren, dass die nachfolgenden Erklärungen für alle Benutzer global akzeptiert werden. Andernfalls werden die Benutzer in einer Mitteilung im Hauptfenster der App aufgefordert, die folgenden Erklärungen zur Verarbeitung persönlicher Benutzerdaten zu akzeptieren:

- Vereinbarung zu Kaspersky Security Network
- Erklärung für die Datenverarbeitung für Web-Filter

- Bestimmungen für die Datenverarbeitung zu Marketingzwecken

Wenn Sie die Erklärungen global akzeptieren, müssen die Versionen der über Kaspersky Security Center akzeptierten Erklärungen mit den bereits von den Benutzern akzeptierten Versionen übereinstimmen. Andernfalls werden die Benutzer über das Problem informiert und aufgefordert, die Version einer Erklärung zu akzeptieren, die der vom Administrator global akzeptierten Version entspricht. Außerdem ändert sich der Gerätestatus im Plug-in "Kaspersky Security for Mobile (Devices)" in *Warnung*.

Der Benutzer kann die Bedingungen für die App jederzeit in den Einstellungen von Kaspersky Endpoint Security für Android im Abschnitt **Über die App** akzeptieren oder ablehnen.

## Informationsaustausch mit dem Kaspersky Security Network

Zur Erhöhung des Niveaus des Echtzeitschutzes verwendet Kaspersky Endpoint Security für Android den Cloud-Dienst Kaspersky Security Network für die Ausführung folgender Komponenten:

- **Anti-Virus.** Die App erhält Zugriff auf die operative Wissensdatenbank von Kaspersky, welche die Reputationen von Dateien und Apps enthält. Bei der Untersuchung werden Bedrohungen gesucht, die schon in KSN eingetragen sind, auch wenn über sie noch keine Informationen in den Antiviren-Datenbanken vorhanden sind. Der Cloud-Dienst Kaspersky Security Network gewährleistet die uneingeschränkte Funktion von Anti-Virus und reduziert die Wahrscheinlichkeit von Fehlalarmen.
- **Web-Filter.** Die App führt eine Untersuchung von Websites vor ihrem Öffnen durch und berücksichtigt dabei Daten, die von KSN übermittelt werden. Außerdem bestimmt die App auf Grundlage von Listen mit erlaubten und verbotenen Kategorien die Kategorie von Websites, um den Internetzugriff der Benutzer zu kontrollieren (z. B. Kategorie "Kommunikation im Internet").
- **Anwendungskontrolle.** Die App bestimmt auf Grundlage von Listen mit erlaubten und verbotenen Kategorien (z. B. Kategorie "Spiele") die App-Kategorie, um den Start von Apps zu beschränken, die nicht den Anforderungen an die Unternehmenssicherheit genügen.

Informationen zu den Daten, die bei der Nutzung von KSN während der Ausführung von Anti-Virus und Anwendungskontrolle an Kaspersky übertragen werden, finden Sie im Endbenutzer-Lizenzvertrag. Indem Sie die Lizenzvereinbarung akzeptieren, stimmen Sie zu, dass diese Informationen übertragen werden.

Informationen zu den Daten, die bei der Nutzung von KSN während der Ausführung von Web-Filter an Kaspersky übertragen werden, finden Sie in der Erklärung für die Datenverarbeitung für Web-Filter. Indem Sie die Erklärung akzeptieren, stimmen Sie zu, dass diese Informationen übertragen werden.

Informationen zu den statistischen Daten, die bei der Nutzung von KSN während der Ausführung der mobilen App Kaspersky Endpoint Security für Android auf den mobilen Geräten an Kaspersky übertragen werden, finden Sie in der Erklärung zu Kaspersky Security Network. Indem Sie die Erklärung akzeptieren, stimmen Sie zu, dass diese Informationen übertragen werden.

## Bereitstellung von Daten im Rahmen des Endbenutzer-Lizenzvertrags

Wenn die Software mit einem Aktivierungscode aktiviert wird, verpflichtet sich der Endbenutzer, zur Verifizierung der legitimen Nutzung der Software dem Rechtsinhaber regelmäßig die folgenden Informationen zur Verfügung zu stellen:

- Format der Daten in der Anfrage an die Infrastruktur des Rechteinhabers; aufgerufene IPv4-Adresse des Webdienstes; Größe des Inhalts der Anfrage an die Infrastruktur des Rechteinhabers; Protokoll-ID; Software-Aktivierungscode; Typ der Datenkomprimierung; Software-ID; Satz von IDs der Software, die auf dem Benutzergerät aktiviert werden kann; Software-Lokalisierung; Vollversion der Software; einmalige Geräte-ID;



Datum und Uhrzeit auf dem Benutzergerät; ID der Software-Installation (PCID); Version des Betriebssystems, Build-Nummer des Betriebssystems, Update-Nummer des Betriebssystems, Edition des Betriebssystems, erweiterte Informationen über die Edition des Betriebssystems; Gerätemodell; Betriebssystemfamilie; Format der Daten in der Anfrage an die Infrastruktur des Rechteinhabers; Prüfsummentyp des verarbeiteten Objekts; Kopfzeile der Softwarelizenz; ID eines regionalen Aktivierungscenters; Datum und Uhrzeit der Erstellung des Software-Lizenzschlüssels; Softwarelizenz-ID; ID des Informationsmodells, das zur Bereitstellung der Softwarelizenz verwendet wird; Ablaufdatum und -uhrzeit der Softwarelizenz; aktueller Status des Software-Lizenzschlüssels; Typ der verwendeten Softwarelizenz; Typ der Lizenz, mit der die Software aktiviert wurde; Aus der Lizenz abgeleitete Software-ID.

Um den Computer vor Sicherheitsbedrohungen zu schützen, erklärt sich der Endbenutzer damit einverstanden, dem Rechtsinhaber regelmäßig folgende Informationen zur Verfügung zu stellen:

- Prüfsummentyp des verarbeiteten Objekts; Prüfsumme des verarbeiteten Objekts; ID der Softwarekomponente
- ID des ausgelösten Eintrags in den Antiviren-Datenbanken der Software; Zeitstempel des ausgelösten Eintrags in den Antiviren-Datenbanken der Software; Typ des ausgelösten Eintrags in den Antiviren-Datenbanken der Software; Name der erkannten Schadsoftware oder legitimen Software, mit der das Gerät oder die Daten des Benutzers beschädigt werden können
- Name des Shops, aus dem die Anwendung installiert wurde; Name des Anwendungspakets; öffentlicher Schlüssel, mit dem die APK-Datei signiert wurde; Prüfsumme des Zertifikats, mit dem die APK-Datei signiert wurde; Zeitstempel des digitalen Zertifikats
- Vollversion der Software; ID des Software-Updates; Typ der installierten Software; Konfigurations-ID; Ergebnis der Software-Aktion; Fehlercode
- Zahlen, die nach bestimmten mathematischen Regeln von der APK-Datei der Android-App abgeleitet werden und die es nicht erlauben, den ursprünglichen Dateiinhalt wiederherzustellen; Diese Daten enthalten keine Dateinamen, Dateipfade, Adressen, Telefonnummern oder sonstige Informationen des Benutzers

Wenn Sie zum Herunterladen der Updates die Update-Server des Rechtsinhabers verwenden, verpflichtet sich der Endbenutzer zur Erhöhung der Effizienz des Update-Vorgangs, dem Rechtsinhaber regelmäßig die folgenden Informationen zur Verfügung zu stellen:

- Aus der Lizenz abgeleitete Software-ID; Vollversion der Software; Softwarelizenz-ID; Typ der verwendeten Softwarelizenz; ID der Software-Installation (PCID); Start-ID des Software-Updates; Webadresse, die verarbeitet wird.

Der Rechteinhaber kann diese Informationen auch zum Sammeln statistischer Daten über die Verbreitung und Verwendung der Software nutzen.

Diese Informationen werden von Kaspersky in Übereinstimmung mit den gesetzlichen Anforderungen geschützt. Die gesammelten Quellinformationen werden in verschlüsselter Form gespeichert und regelmäßig (2 Mal jährlich) oder auf Anforderung des Benutzers gelöscht. Die Daten der allgemeinen Statistik werden unbegrenzt gespeichert.

## Bereitstellung von Daten im Rahmen der Erklärung zu Kaspersky Security Network

Die Verwendung des KSN kann zu einer höheren Wirksamkeit des von der Software gebotenen Schutzes gegen Bedrohungen für die Informations- und Netzsicherheit führen.

Wenn Sie eine Lizenz für 5 oder mehr Knoten verwenden, erhält und verarbeitet der Rechteinhaber automatisch die folgenden Daten während der Nutzung von KSN:

- ID des ausgelösten Eintrags in den Antiviren-Datenbanken der Software; Zeitstempel des ausgelösten Eintrags in den Antiviren-Datenbanken der Software; Typ des ausgelösten Eintrags in den Antiviren-Datenbanken der Software; Veröffentlichungsdatum und -uhrzeit der Software-Datenbanken; Version des Betriebssystems, Build-Nummer des Betriebssystems, Update-Nummer des Betriebssystems, Edition des Betriebssystems, erweiterte Informationen über die Edition des Betriebssystems; Version des Betriebssystem Service Packs; Erkennungseigenschaften; Prüfsumme (MD5) des verarbeiteten Objekts; Name des verarbeiteten Objekts; Kennzeichen, das angibt, ob das verarbeitete Objekt eine PE-Datei ist; Prüfsumme (MD5) der Maske, die den Webdienst blockiert hat; Prüfsumme (SHA256) des verarbeiteten Objekts; Größe des verarbeiteten Objekts; Objekttypcode; Entscheidung der Software für das verarbeitete Objekt; Speicherpfad des verarbeiteten Objekts; Verzeichniscode; Version der Software-Komponente; Version der gesendeten Statistiken; aufgerufene Adresse des Webdienstes (URL, IP); Typ des Clients, mit dem auf den Webdienst zugegriffen wird; aufgerufene IPv4-Adresse des Webdienstes; aufgerufene IPv6-Adresse des Webdienstes; Webadresse der Quelle der Webdienst-Anfrage (Referenz); webadresse, die verarbeitet wird
- Informationen über untersuchte Objekte (App-Version aus AndroidManifest.xml; Entscheidung der Software im Hinblick auf die Anwendung; Methode, mit welcher die Entscheidung der Software im Hinblick auf die Anwendung abgerufen wird; Name des Installationsprogramm-Pakets im Shop; Paketname (oder Bundle-Name) von AndroidManifest.xml; Google SafetyNet-Kategorie; Kennzeichen, das angibt, ob SafetyNet auf dem Gerät aktiviert ist; SHA256-Wert aus der Google SafetyNet-Antwort; APK Signature Scheme für das APK-Zertifikat; Versionscode der installierten Software; Seriennummer des Zertifikats, mit dem die APK-Datei signiert wurde; Name der APK-Datei, die installiert wird; Pfad der APK-Datei, die installiert wird; Aussteller des Zertifikats, mit dem die APK-Datei signiert wurde; öffentlicher Schlüssel, mit dem die APK-Datei signiert wurde; Prüfsumme des Zertifikats, mit dem die APK-Datei signiert wurde; Datum und Uhrzeit des Ablaufs des Zertifikats; Datum und Uhrzeit der Ausstellung des Zertifikats; Version der gesendeten Statistiken; Algorithmus zur Berechnung eines Fingerabdrucks des digitalen Zertifikats; MD5-Hash der installierten APK-Datei; MD5-Hash der DEX-Datei, die sich in der APK-Datei befindet; Berechtigungen, die der Anwendung dynamisch gewährt werden; Version der Drittanbieter-Software; Kennzeichen, das angibt, ob die Anwendung der Standard-SMS-Messenger ist; Kennzeichen, das angibt, ob das Programm über Geräteadministrator-Rechte verfügt; Kennzeichen, das angibt, ob die Anwendung im Systemkatalog ist; Kennzeichen, das angibt, ob die Anwendung Bedienungshilfen-Dienste verwendet)
- Informationen über alle potenziell böartigen Objekte und Aktivitäten (Fragment-Inhalt des bearbeiteten Objekts; Datum und Uhrzeit des Ablaufs des Zertifikats; Datum und Uhrzeit der Ausstellung des Zertifikats; ID des Schlüssels aus dem für die Verschlüsselung verwendeten Keystore; Protokoll, das für den Datenaustausch mit dem KSN verwendet wird; Fragmentreihenfolge im verarbeiteten Objekt; Daten des internen Protokolls, das vom Antiviren-Software-Modul für ein verarbeitetes Objekt generiert wird; Name des Zertifikatausstellers; öffentlicher Schlüssel des Zertifikats; Berechnungsalgorithmus für den öffentlichen Schlüssel des Zertifikats; Seriennummer des Zertifikats; Datum und Uhrzeit der Signierung des Objekts; Name des Zertifikatinhabers und Einstellungen; digitaler Zertifikatfingerabdruck des untersuchten Objekts und Hash-Algorithmus; Datum und Uhrzeit der letzten Änderung des verarbeiteten Objekts; Datum und Uhrzeit der Erstellung eines verarbeiteten Objekts; verarbeitete Objekte oder Teile davon; Beschreibung eines verarbeiteten Objekts gemäß der Definition in den Objekteigenschaften; Format des verarbeiteten Objekts; Prüfsummentyp des verarbeiteten Objekts; Prüfsumme (MD5) des verarbeiteten Objekts; Name des verarbeiteten Objekts; Prüfsumme (SHA256) des verarbeiteten Objekts; Größe des verarbeiteten Objekts; Name des Softwareherstellers; Entscheidung der Software für das verarbeitete Objekt; Version des verarbeiteten Objekts; Quelle der für das verarbeitete Objekt getroffenen Entscheidung; Prüfsumme des verarbeiteten Objekts; Name der übergeordneten Anwendung; Speicherpfad des verarbeiteten Objekts; Informationen über die Ergebnisse der Dateisignaturprüfung; Schlüssel für Anmeldesitzung; Verschlüsselungsalgorithmus für den Schlüssel der Anmeldesitzung; Speicherzeit für das verarbeitete Objekt; Algorithmus zur Berechnung eines Fingerabdrucks des digitalen Zertifikats)
- Build-Typ, z. B. "Benutzer" oder "eng"; vollständiger Produktname; Produkt-/Hardware-Hersteller; ob Apps außerhalb von Google Play installiert werden können; Status des Cloud-Dienstes zur Überprüfung von Google-Apps; Status des Cloud-Dienstes zur Überprüfung von Google-Apps, die über ADB installiert werden; aktueller Entwicklungs-Codename oder "REL" für Produktions-Builds; inkrementelle Versionsnummer; für den Benutzer sichtbare Versionszeichenfolge; Name des Benutzergerätes; für den Benutzer sichtbare Build-ID der Software; Firmware-Fingerabdruck; Firmware-ID; Kennzeichen, das angibt, ob das Gerät gerootet ist; Betriebssystem; Name der Software; Typ der verwendeten Softwarelizenz

- Informationen über die Qualität von KSN-Diensten (Protokoll, das für den Datenaustausch mit dem KSN verwendet wird; ID des KSN-Dienstes, auf den die Software zugegriffen hat; Datum und Uhrzeit, ab der keine Statistiken mehr empfangen wurden; Anzahl der KSN-Verbindungen, die aus dem Cache entnommen wurden; Anzahl der Anfragen, für die in der lokalen Anfragedatenbank eine Antwort gefunden wurde; Anzahl der fehlgeschlagenen KSN-Verbindungen; Anzahl der fehlgeschlagenen KSN-Transaktionen; zeitliche Verteilung stornierter Anfragen an das KSN; zeitliche Verteilung erfolgloser KSN-Verbindungen; zeitliche Verteilung erfolgloser KSN-Transaktionen; zeitliche Verteilung erfolgreicher KSN-Verbindungen; zeitliche Verteilung erfolgreicher KSN-Transaktionen; zeitliche Verteilung erfolgreicher Anfragen an das KSN; zeitliche Verteilung von Anfragen an das KSN mit Zeitüberschreitung; Anzahl neuer KSN-Verbindungen; Anzahl erfolgloser Anfragen an das KSN aufgrund von Routing-Fehlern; Anzahl erfolgloser Anfragen aufgrund der Deaktivierung des KSN in den Softwareeinstellungen; Anzahl erfolgloser Anfragen an das KSN aufgrund von Netzwerkproblemen; Anzahl erfolgreicher KSN-Verbindungen; Anzahl erfolgreicher KSN-Transaktionen; Gesamtzahl der Anfragen an das KSN; Datum und Uhrzeit, ab der Statistiken empfangen wurden)
- Gerätekennung; Vollversion der Software; ID des Software-Updates; ID der Software-Installation (PCID); Typ der installierten Software
- Bildschirmhöhe des Gerätes; Bildschirmbreite des Gerätes; Informationen über die überlappende Anwendung: MD5-Hash der APK-Datei; Informationen über die überlappende Anwendung: MD5-Hash der Datei "classes.dex"; Informationen über die überlappende Anwendung: Name der APK-Datei; Informationen über die überlappende Anwendung: Pfad der APK-Datei ohne den Dateinamen; Höhe der Überlappung; Informationen über die überlappende Software: MD5-Hash der APK-Datei; überlappende Programminformationen: MD5-Hash der Datei "classes.dex"; überlappende Programminformationen: Name der APK-Datei; überlappende Programminformationen: Pfad der APK-Datei ohne den Dateinamen; überlappende Programminformationen: Name des Programmpakets (für das überlappende Programm: Wenn die Werbung auf einem leeren Desktop angezeigt wird, muss der Wert "Launcher" lauten); Datum und Uhrzeit der Überlappung; Informationen über die überlappende Anwendung: Name des Anwendungspakets; Breite der Überlappung
- Einstellungen der verwendeten Wi-Fi-Access-Points (erkannter Gerätetyp; DHCP-Einstellungen (Prüfsummen der lokalen IPv6, DHCP IPv6, DNS1 IPv6, DNS2 IPv6 des Gateways; Prüfsumme der Netzwerkpräfixlänge; Prüfsumme der lokalen Adresse IPv6); DHCP-Einstellungen (Prüfsummen der lokalen IP-Adresse des Gateways, DHCP IP, DNS1 IP, DNS2 IP und Subnetzmaske); Kennzeichen, das angibt, ob die DNS-Domäne existiert; Prüfsumme der zugewiesenen lokalen IPv6-Adresse; Prüfsumme der zugewiesenen lokalen IPv4-Adresse; Kennzeichen, das angibt, ob das Gerät angeschlossen ist; Authentifizierungstyp des WLAN-Netzwerks; Liste der verfügbaren WLAN-Netzwerke und ihrer Einstellungen; Prüfsumme (MD5 mit Salt) der MAC-Adresse des Zugriffspunktes; Prüfsumme (SHA256 mit Salt) der MAC-Adresse des Zugriffspunktes; Verbindungstypen, die der WLAN-Zugriffspunkt unterstützt; Verschlüsselungstyp des WLAN-Netzwerks; lokale Zeit für den Beginn und das Ende der WLAN-Netzwerkverbindung; ID des WLAN-Netzwerks, basierend auf der MAC-Adresse des Zugriffspunktes; ID des WLAN-Netzwerks, basierend auf dem Namen des WLAN-Netzwerks; ID des WLAN-Netzwerks, basierend auf dem Namen des WLAN-Netzwerks und der MAC-Adresse des Zugriffspunktes; WLAN-Signalstärke; Name des WLAN-Netzwerks; Satz der Authentifizierungsprotokolle, die von dieser Konfiguration unterstützt werden; Authentifizierungsprotokoll, das für eine WPA-EAP-Verbindung verwendet wird; internes Authentifizierungsprotokoll; Satz der Gruppenverschlüsselungen, die von dieser Konfiguration unterstützt werden; Satz der Schlüsselverwaltungsprotokolle, die von dieser Konfiguration unterstützt werden; endgültige Privatsphären-Kategorie des Netzwerks in der Software; endgültige Sicherheitskategorie des Netzwerks in der Software; Satz der Blockverschlüsselungen für WPA, die von dieser Konfiguration unterstützt werden; Satz der Sicherheitsprotokolle, die von dieser Konfiguration unterstützt werden)
- Installationsdatum und -uhrzeit der Software; Datum der Softwareaktivierung; ID der Partnerorganisation, über die die Softwarelizenz bestellt wurde; Aus der Lizenz abgeleitete Software-ID; Seriennummer des Softwarelizenzschlüssels; Software-Lokalisierung; Kennzeichen, das angibt, ob die Teilnahme am KSN aktiviert ist; ID der lizenzierten Software; Softwarelizenz-ID; Betriebssystem-ID; Bit-Version des Betriebssystems

Um den erklärten Zweck eines besseren Schutzes durch die Software zu erreichen, kann der Rechteinhaber darüber hinaus Objekte (Datei oder Teil einer Datei, Dienstinformationen) erhalten, die von Angreifern dazu missbraucht werden könnten, dem Computer und der Informationssicherheit zu schaden.

Die Teilnahme an Kaspersky Security Network zur Verarbeitung von statistischen Daten ist freiwillig. Sie können jederzeit die [Teilnahme am Kaspersky Security Network beenden](#).

## Bereitstellung von Daten im Rahmen der Bestimmungen für die Datenverarbeitung für Web-Filter.

Gemäß der Erklärung für Web-Filter verarbeitet der Rechteinhaber Daten, die für die Ausführung von Web-Filter benötigt werden. Der angegebene Zweck umfasst das Erkennen von Bedrohungen und das Ermitteln der Kategorien besuchter Websites mithilfe des Cloud-Dienstes Kaspersky Security Network (KSN).

Mit Ihrer Einwilligung werden folgende Daten gemäß der Erklärung für Web-Filter in regelmäßigen Abständen automatisch an den Rechteinhaber gesendet:

- Produktversion; Eindeutige Geräte-ID; Installations-ID; Produkttyp.
- URL-Adresse der Seite, Portnummer, URL-Protokoll, URL, die auf die angeforderte Information verweist.

## Bereitstellung von Daten im Rahmen der Bestimmungen für die Datenverarbeitung zu Marketingzwecken

Der Rechteinhaber verwendet Informationssysteme von Drittanbietern zur Datenverarbeitung. Deren Datenverarbeitung unterliegt den Datenschutzrichtlinien solcher Informationssysteme von Drittanbietern. Der Rechteinhaber verwendet die folgenden Dienste zur Verarbeitung der aufgezählten Daten:

### Google Analytics für Firebase

Während der Benutzung der Software werden die folgenden Daten automatisch und regelmäßig an Google Analytics für Firebase übertragen, um den erklärten Zweck zu erreichen:

- App-Informationen (App-Version, App-ID und die ID der App im Firebase-Dienst, Instanz-ID im Firebase-Dienst, Name des Shops, in dem die Anwendung erworben wurde, Zeitstempel des ersten Starts der Software)
- Installations-ID der App auf dem Gerät und Installationsmethode auf dem Gerät
- Informationen über die Region und die Sprachlokalisierung
- Informationen über die Auflösung des Gerätebildschirms
- Informationen über den Nutzer, der Root erhält
- Diagnoseinformationen zum Gerät aus dem SafetyNet-Attestation-Dienst
- Informationen zur Einstellung von Kaspersky Endpoint Security für Android als Zugangsfunktion
- Informationen über Übergänge zwischen Anwendungsbildschirmen, Sitzungsdauer, Beginn und Ende einer Bildschirmsitzung, Bildschirmname
- Informationen über das verwendete Protokoll, mit welchem Daten an den Firebase-Dienst gesendet werden, die Version und die ID der verwendeten Datenübertragungsmethode
- Informationen zum Typ und zu den Parametern des Ereignisses, auf das sich der Versand der Daten bezieht
- Informationen über die App-Lizenz, ihre Verfügbarkeit und die Anzahl der Geräte

- Informationen darüber, wie oft die Antiviren-Datenbanken aktualisiert und die Geräte mit dem Administrationsserver synchronisiert werden
- Informationen über die Verwaltungskonsole (Kaspersky Security Center oder EMM-Systeme von Drittanbietern)
- Android-ID
- Werbe-ID
- Informationen über den Benutzer: Altersgruppe und Geschlecht, Land des Wohnsitzes, Liste der Interessen
- Informationen über den Computer des Benutzers, auf dem die Software installiert ist: Name des Herstellers des Computers, Typ des Computers, Modell, Version und Sprachversion (Gebietsschema) des Betriebssystems, Informationen darüber, ob die Anwendung innerhalb der letzten 7 Tage zum ersten Mal geöffnet wurde oder ob das erste Öffnen mehr als 7 Tage zurückliegt

Die Daten werden an Firebase über einen sicheren Kanal übertragen. Informationen über die Verarbeitung von Daten in Firebase werden hier veröffentlicht: <https://firebase.google.com/support/privacy>.

### **SafetyNet Attestation**

Während der Benutzung der Software werden die folgenden Daten automatisch und regelmäßig an SafetyNet Attestation übertragen, um den erklärten Zweck zu erreichen:

- Zeitpunkt der Geräteprüfung
- Informationen über die Software, Name und Daten zu den Softwarezertifikaten
- Ergebnisse der Geräteprüfung
- willkürliche ID-Prüfungen, um die Ergebnisse des zu prüfenden Geräts zu ermitteln

Die Daten werden an SafetyNet Attestation über einen sicheren Kanal übertragen. Informationen darüber, wie SafetyNet Attestation Daten verarbeitet, wurden hier veröffentlicht: <https://policies.google.com/privacy>.

### **Firebase-Leistungsüberwachung**

Während der Benutzung der Software werden die folgenden Daten automatisch und regelmäßig an SafetyNet Attestation übertragen, um den erklärten Zweck zu erreichen:

- einmalige Installations-ID
- Name des Anwendungspakets
- Version der installierten Software
- Akkustand und Ladestatus des Akkus
- Mobilfunkanbieter
- App-Ausführungsstatus (Vordergrund oder Hintergrund)
- Geografie
- IP-Adresse
- Sprachcode des Gerätes

- Informationen über die Funk-/Netzwerkverbindung
- pseudonyme ID der Software-Instanz
- RAM- und Datenträgergröße
- Kennzeichen, das angibt, ob es ein Gerät mit Jailbreak ist oder ob das Gerät gerootet ist
- Signalstärke
- Dauer von automatisierten Ablaufverfolgungen
- Netzwerk und die folgenden entsprechenden Informationen: Antwortcode, Payload-Größe in Byte, Antwortzeit
- Gerätebeschreibung

Die Daten werden an Firebase- Performance-Monitoring über einen sicheren Kanal übertragen. Informationen darüber, wie Daten in Firebase-Performance-Monitoring verarbeitet werden, sind hier veröffentlicht:

<https://firebase.google.com/support/privacy>.

## Crashlytics

Während der Benutzung der Software werden die folgenden Daten automatisch und regelmäßig an Crashlytics übertragen, um den erklärten Zweck zu erreichen:

- Software-ID
- Version der installierten Software
- Kennzeichen, das angibt, ob die Software im Hintergrund ausgeführt wurde
- CPU-Architektur
- einmalige Ereignis-ID
- Datum und Uhrzeit des Ereignisses
- Gerätemodell
- gesamter Speicherplatz und derzeit genutzter Platz
- Name und Version des Betriebssystems
- gesamter RAM und derzeit genutzter Anteil
- Kennzeichen, das angibt, ob das Gerät gerootet ist
- Bildschirmausrichtung zum Ereigniszeitpunkt
- Produkt-/Hardware-Hersteller
- einmalige Installations-ID
- Version der gesendeten Statistiken
- Ausnahmetyp der Software

- Text der Fehlermeldung
- Kennzeichen, das angibt, dass die Software-Ausnahme durch eine verschachtelte Ausnahme verursacht wurde
- Thread-ID
- Kennzeichen, das angibt, ob der Frame die Ursache des Software-Fehlers war
- Kennzeichen, das angibt, dass der Thread dazu führte, dass die Software unerwartet beendet wurde
- Informationen über das Signal, das dazu führte, dass die Software unerwartet beendet wurde: Signalname, Signalcode, Signaladresse
- für jeden Frame, der einem Thread zugeordnet ist, Ausnahme oder Fehler: Name der Framedatei, Zeilennummer der Framedatei, Debug-Symbole, Adresse und Offset im Binärbild, Anzeigename der Bibliothek mit dem Frame, Typ des Frames, Kennzeichen, das angibt, ob der Frame den Fehler verursacht hat
- Betriebssystem-ID
- ID des Problems, das dem Ereignis zugeordnet ist
- Informationen über Ereignisse, die eingetreten sind, bevor die Software unerwartet beendet wurde: Ereignis-ID, Ereignisdatum und -uhrzeit, Ereignistyp und -wert
- CPU-Registrierungswerte
- Ereignistyp und -wert

Die Daten werden an Facebook über einen sicheren Kanal übertragen. Informationen über die Verarbeitung von Daten in Crashlytics werden hier veröffentlicht: <https://firebase.google.com/terms/crashlytics-app-distribution-data-processing-terms>.

Die Angabe obenstehender Informationen für die Datenverarbeitung zu Marketing-Zwecken ist freiwillig.

## Bereitstellung von Daten in Kaspersky Security für iOS

Kaspersky Security für mobile Endgeräte entspricht der Datenschutz-Grundverordnung (DSGVO).

Um die App zu installieren, muss der Benutzer die Bedingungen der folgenden Vereinbarungen zur Verarbeitung persönlicher Benutzerdaten lesen und akzeptieren:

- Endbenutzer-Lizenzvertrag
- Datenschutzrichtlinie für Produkte und Dienste

Optional kann der Benutzer die Bedingungen der folgenden Vereinbarung lesen und akzeptieren:

- Vereinbarung zu Kaspersky Security Network

Der Benutzer kann die Bedingungen dieser Dokumente jederzeit im Abschnitt **Über die App → Verträge und Erklärungen** in den Einstellungen von Kaspersky Security für iOS einsehen. In diesem Abschnitt kann der Benutzer auch die Bedingungen der KSN-Erklärung akzeptieren oder ablehnen.

## Informationsaustausch mit dem Kaspersky Security Network

Zur Verbesserung des Echtzeitschutzes verwendet Kaspersky Security für iOS den Cloud-Dienst Kaspersky Security Network für die Funktion der Komponente [Web-Filter](#). Die App verwendet Daten aus KSN, um Webressourcen vor dem Öffnen zu untersuchen.

Informationen zu den Arten der Daten, die bei der KSN-Nutzung während der Ausführung des Web-Filters an Kaspersky übertragen werden, finden Sie im Endbenutzer-Lizenzvertrag. Indem Sie die Lizenzvereinbarung akzeptieren, stimmen Sie zu, dass diese Informationen übertragen werden.

Informationen zu den statistischen Daten, die bei der Nutzung von KSN während der Ausführung der mobilen App Kaspersky Security für iOS auf den mobilen Geräten an Kaspersky übertragen werden, finden Sie in der Erklärung zu Kaspersky Security Network. Indem Sie die Erklärung akzeptieren, stimmen Sie zu, dass diese Informationen übertragen werden.

## Bereitstellung von Daten im Rahmen des Endbenutzer-Lizenzvertrags

Wenn die Software mit einem Aktivierungscode aktiviert wird, verpflichtet sich der Endbenutzer, zur Verifizierung der legitimen Nutzung der Software dem Rechtsinhaber regelmäßig die folgenden Informationen zur Verfügung zu stellen:

- Format der Daten in der Anfrage an die Infrastruktur des Rechteinhabers; aufgerufene IPv4-Adresse des Webdienstes; Größe des Inhalts der Anfrage an die Infrastruktur des Rechteinhabers; Protokoll-ID; Software-Aktivierungscode; Typ der Datenkomprimierung; Software-ID; Satz von IDs der Software, die auf dem Benutzergerät aktiviert werden kann; Software-Lokalisierung; Vollversion der Software; einmalige Geräte-ID; Datum und Uhrzeit auf dem Benutzergerät; ID der Software-Installation (PCID); derzeit verwendeter Software-Aktivierungscode; Version des Betriebssystems, Build-Nummer des Betriebssystems, Update-Nummer des Betriebssystems, Edition des Betriebssystems, erweiterte Informationen über die Edition des Betriebssystems; Gerätemodell; Code des Mobilfunkanbieters; Betriebssystemfamilie; Aus der Lizenz abgeleitete Software-ID; Liste der Vereinbarungen, die dem Benutzer von der Software angezeigt werden; Typ des rechtsgültigen Vertrages, den der Benutzer während der Nutzung der Software akzeptiert hat; Version des rechtsgültigen Vertrages, den der Benutzer während der Nutzung der Software akzeptiert hat; Kennzeichen, das angibt, ob der Benutzer die Bedingungen des rechtsgültigen Vertrages während der Nutzung der Software akzeptiert hat; Prüfsummentyp des verarbeiteten Objekts; Kopfzeile der Softwarelizenz; ID eines regionalen Aktivierungscentrums; Datum und Uhrzeit der Erstellung des Software-Lizenzschlüssels; Softwarelizenz-ID; ID des Informationsmodells, das zur Bereitstellung der Softwarelizenz verwendet wird; Ablaufdatum und -uhrzeit der Softwarelizenz; aktueller Status des Software-Lizenzschlüssels; Typ der verwendeten Softwarelizenz; Typ der Lizenz, mit der die Software aktiviert wurde; Aus der Lizenz abgeleitete Software-ID.

Der Rechtsinhaber kann diese Informationen auch zum Sammeln statistischer Daten zur Verbreitung und Verwendung der Software des Rechtsinhabers nutzen.

Um den Computer vor Sicherheitsbedrohungen zu schützen, erklärt sich der Endbenutzer damit einverstanden, dem Rechtsinhaber regelmäßig folgende Informationen zur Verfügung zu stellen:

- Format der Daten in der Anfrage an die Infrastruktur des Rechteinhabers; aufgerufene Adresse des Webdienstes (URL, IP); Portnummer; Webadresse der Quelle der Webdienst-Anfrage (Referenz).
- Vollversion der Software; ID des Software-Updates; Typ der installierten Software; Software-ID; Konfigurationsbezeichnung; Ergebnis der Software-Aktion; Fehlercode.
- Webadresse, die verarbeitet wird aufgerufene IPv4-Adresse des Webdienstes; digitaler Zertifikatfingerabdruck des untersuchten Objekts und Hash-Algorithmus; Zertifikatstyp; Inhalte des verarbeiteten digitalen Zertifikats.

## Bereitstellung von Daten im Rahmen der Erklärung zu Kaspersky Security Network



Wenn KSN-Erklärung akzeptiert wird, erhält und verarbeitet der Rechteinhaber automatisch die folgenden Daten:

- Informationen über die Qualität von KSN-Diensten (Protokoll, das für den Datenaustausch mit dem KSN verwendet wird; ID des KSN-Dienstes, auf den die Software zugegriffen hat; Datum und Uhrzeit, ab der keine Statistiken mehr empfangen wurden; Anzahl der KSN-Verbindungen, die aus dem Cache entnommen wurden; Anzahl der Anfragen, für die in der lokalen Anfragedatenbank eine Antwort gefunden wurde; Anzahl der fehlgeschlagenen KSN-Verbindungen; Anzahl der fehlgeschlagenen KSN-Transaktionen; zeitliche Verteilung stornierter Anfragen an das KSN; zeitliche Verteilung erfolgloser KSN-Verbindungen; zeitliche Verteilung erfolgloser KSN-Transaktionen; zeitliche Verteilung erfolgreicher KSN-Verbindungen; zeitliche Verteilung erfolgreicher KSN-Transaktionen; zeitliche Verteilung erfolgreicher Anfragen an das KSN; zeitliche Verteilung von Anfragen an das KSN mit Zeitüberschreitung; Anzahl neuer KSN-Verbindungen; Anzahl erfolgloser Anfragen an das KSN aufgrund von Routing-Fehlern; Anzahl erfolgloser Anfragen aufgrund der Deaktivierung des KSN in den Softwareeinstellungen; Anzahl erfolgloser Anfragen an das KSN aufgrund von Netzwerkproblemen; Anzahl erfolgreicher KSN-Verbindungen; Anzahl erfolgreicher KSN-Transaktionen; Gesamtzahl der Anfragen an das KSN; Datum und Uhrzeit, ab der Statistiken empfangen wurden)
- Geräteerkennung; Vollversion der Software; ID des Software-Updates; ID der Software-Installation (PCID); Typ der installierten Software
- Installationsdatum und -uhrzeit der Software; Datum der Softwareaktivierung; Software-Lokalisierung; Kennzeichen, das angibt, ob die Teilnahme am KSN aktiviert ist; ID der lizenzierten Software; Softwarelizenz-ID; Betriebssystem-ID; Version des auf dem Computer des Benutzers installierten Betriebssystems; Bit-Version des Betriebssystems

Die Teilnahme an Kaspersky Security Network zur Verarbeitung von statistischen Daten ist freiwillig. Sie können jederzeit die Teilnahme am Kaspersky Security Network beenden.

# Kontaktaufnahme mit dem Technischen Support

Dieser Abschnitt beschreibt, wie und unter welchen Bedingungen Sie technischen Support erhalten.

## Kontakt zum Technischen Support

Wenn Sie in der Dokumentation von Kaspersky Security für mobile Endgeräte und in den anderen Informationsquellen zu Kaspersky Security für mobile Endgeräte keine Lösung für Ihr Problem finden können, wenden Sie sich an den Technischen Support. Die Support-Mitarbeiter beantworten all Ihre Fragen zur Installation und Verwendung von Kaspersky Security für mobile Endgeräte.

Kaspersky bietet Unterstützung für Kaspersky Security für mobile Endgeräte während seines Lebenszyklus (siehe [Seite Produktsupportlebenszyklus](#)). Bitte lesen Sie die [Support-Regeln](#), bevor Sie sich an den Technischen Support wenden.

Eine Kontaktaufnahme mit den Support-Experten ist auf folgende Weise möglich:

- [Rufen Sie die Website des Technischen Supports auf](#)
- Senden Sie eine Anfrage an den Technischen Support über das [Portal Kaspersky CompanyAccount](#)

## Technischer Support über das Kaspersky CompanyAccount

[Kaspersky CompanyAccount](#) ist ein Portal für Unternehmen, die Kaspersky-Programme verwenden. Das Portal Kaspersky CompanyAccount vereinfacht die Interaktion zwischen Benutzern und Experten von Kaspersky mittels Online-Anfragen. Mithilfe von Kaspersky CompanyAccount können Sie den Status Ihrer Online-Anfragen verfolgen und eine Chronik mit allen Anfragen speichern.

Sie können alle Mitarbeiter Ihrer Firma unter einem Benutzerkonto für Kaspersky CompanyAccount registrieren. Mithilfe eines einheitlichen Kontos können Sie die Online-Anfragen der bei Kaspersky registrierten Mitarbeiter zentral verwalten und die Berechtigungen dieser Mitarbeiter für Kaspersky CompanyAccount verwalten.

Das Portal Kaspersky CompanyAccount ist in den folgenden Sprachen verfügbar:

- Englisch
- Spanisch
- Italienisch
- Deutsch
- Polnisch
- Portugiesisch
- Russisch
- Französisch

- Japanisch

Weitere Informationen über Kaspersky CompanyAccount finden Sie auf der [Support-Webseite](#) .

# Informationsquellen zur App

## Seite von Kaspersky Security für mobile Endgeräte auf der Kaspersky-Website

Auf der [Seite von Kaspersky Security für mobile Endgeräte](#) finden Sie allgemeine Informationen über das Programm, seine Funktionen und Besonderheiten.

Die Seite von Kaspersky Security für mobile Endgeräte enthält einen Link zum Online-Shop. Dort können Sie ein Programm kaufen oder die Nutzungsrechte für das Programm verlängern.

## Webseite für Kaspersky Security für mobile Endgeräte in der Wissensdatenbank

Die *Wissensdatenbank* ist ein Abschnitt auf der Webseite des Technischen Supports.

Auf der [Seite von Kaspersky Security für mobile Endgeräte in der Wissensdatenbank](#) finden Sie nützliche Informationen, Tipps und Antworten auf häufige Fragen. Dabei werden Fragen wie Kauf, Installation und Verwendung des Programms behandelt.

Artikel der Wissensdatenbank beantworten nicht nur Fragen in Bezug auf Kaspersky Security für mobile Endgeräte, sondern auch auf andere Programme von Kaspersky. In den Artikeln der Wissensdatenbank können auch Neuigkeiten über den Technischen Support enthalten sein.

## Online-Hilfe

Das elektronische Hilfesystem des Programms umfasst verschiedene Hilfedateien.

Die Kontexthilfe für das Verwaltungs-Plug-in von Kaspersky Security für mobile Endgeräte bietet Informationen über die einzelnen Fenster von Kaspersky Security Center. Dazu gehören eine Beschreibung der Einstellungen von Kaspersky Security für mobile Endgeräte und Links zur Beschreibung der Aufgaben, in denen diese Einstellungen verwendet werden.

In der vollständigen Hilfe für die Anwendungen Kaspersky Endpoint Security für Android und Kaspersky Security für iOS finden Sie Informationen zur Konfiguration und Nutzung der mobilen Anwendungen.

## Diskussion über die Kaspersky-Programme im Kaspersky Support Forum

Wenn Ihre Frage nicht dringend ist, können Sie mit den Experten von Kaspersky und mit anderen Anwendern in [unserem Forum](#) darüber diskutieren.

Im Forum können Sie Diskussionsthemen nachlesen, Kommentare abgeben und neue Themen zur Diskussion stellen.

# Glossar

## Abonnement

Ermöglicht die Verwendung des Programms unter Berücksichtigung der ausgewählten Optionen (Ablaufdatum und Anzahl der Geräte). Sie können Ihr Abonnement anhalten und fortsetzen, automatisch verlängern oder beenden.

## Administrationsgruppe

Gruppe von verwalteten Geräten, beispielsweise von mobilen Geräten, die aufgrund ihrer Funktionen und der darauf installierten Programme zusammengefasst wurden. Verwaltete Geräte werden zur einfachen Verwaltung der Computer als geschlossene Einheit gruppiert. Beispielsweise, können mobile Geräte unter einem Betriebssystem in eine Administrationsgruppe gruppiert werden. Eine Gruppe kann andere Administrationsgruppe enthalten. Für Geräte, die in Gruppen zusammengefasst sind, können Gruppenrichtlinien und Gruppenaufgaben erstellt werden.

## Administrationsserver

Komponente des Programms Kaspersky Security Center, das der zentralen Speicherung von Informationen über im Unternehmensnetzwerk installierte Kaspersky-Programme. Und der Verwaltung dieser Programme dient.

## Administrator von Kaspersky Security Center

Die Person, die den Programmbetrieb über das zentralisierte Remote-Verwaltungssystem Kaspersky Security Center verwaltet.

## Administrator-Arbeitsplatz

Der Computer, auf dem die Kaspersky Security Center Verwaltungskonsole bereitgestellt wurde. Wenn auf dem Administrator-Arbeitsplatz ein Verwaltungs-Plug-in für das Programm installiert ist, kann der Administrator mobile Anwendungen von Kaspersky Endpoint Security, die auf den Nutzergeräten verteilt sind, verwalten.

## Aktivierungscode

Diesen Code erhalten Sie beim Kauf einer Lizenz für Kaspersky Endpoint Security. Der Code wird zur Aktivierung des Programms benötigt.

Der Aktivierungscode besteht aus einer eindeutigen Folge von zwanzig lateinischen Zeichen und Ziffern im Format xxxxx-xxxxx-xxxxx-xxxxx.

## Antiviren-Datenbanken

Datenbanken, die Informationen über Bedrohungen der Computersicherheit enthalten, die Kaspersky zum Zeitpunkt der Veröffentlichung der Antiviren-Datenbank bekannt waren. Die Einträge in den Antiviren-Datenbanken ermöglichen das Erkennen von böartigem Code in den untersuchten Objekten. Die Antiviren-Datenbanken werden von den Kaspersky-Experten erstellt und stündlich aktualisiert.

## Arbeitsprofil Android

Sichere Umgebung auf dem Benutzergerät, in der der Administrator die Apps und Konten des Benutzers verwalten kann, ohne diesen in seinen Möglichkeiten bei der Arbeit mit persönlichen Daten einzuschränken. Bei der Erstellung des Arbeitsprofils auf dem mobilen Benutzergerät werden im Arbeitsprofil automatisch folgende korporativen Apps installiert: Google Play, Google Chrome, Downloads, Kaspersky Endpoint Security für Android und sonstige. Die im Arbeitsprofil installierten korporativen Apps sowie die Benachrichtigungen dieser Apps sind mit dem Symbol einer roten Aktentasche markiert. Für die App Google Play muss ein separates geschäftliches Google-Konto angelegt werden. Apps, die sich im Arbeitsprofil befinden, werden in der allgemeinen App-Liste angezeigt.

## Betreutes Gerät

iOS-Gerät, dessen Einstellungen vom Apple Configurator überwacht werden, einem Programm zur Gruppenkonfiguration von iOS-Geräten. Ein betreutes Gerät hat in Apple Configurator den Status *supervised*. Bei jeder Verbindung eines betreuten Geräts mit dem Computer überprüft Apple Configurator, ob die Konfiguration des Geräts mit den festgelegten Einstellungen übereinstimmt, und passt diese anschließend bei Bedarf an. Das betreute Gerät kann nicht mit einem auf einem anderen Computer installierten Apple Configurator synchronisiert werden.

Für betreute Geräte können mehr Einstellungen mittels der Richtlinie Kaspersky Device Management für iOS angepasst werden als für nicht betreute Geräte. So können Sie z. B. einen HTTP-Proxyserver konfigurieren, der den Internet-Datenverkehr auf dem Gerät innerhalb des Unternehmensnetzwerks überwacht. Standardmäßig sind alle mobilen Geräte unbetreut.

## CSR-Anfrage (Certificate Signing Request)

Datei mit Einstellungen für den Administrationsserver, die nach der Bestätigung durch Kaspersky an Apple übermittelt wird, um ein APNs-Zertifikat zu erhalten.

## EAS-Gerät

Mobiles Endgerät, das über das Protokoll Exchange ActiveSync mit dem Administrationsserver verbunden wird.

## Eigenständiges Installationspaket

Installationsdatei für die Anwendung Kaspersky Endpoint Security für das Betriebssystem Android, das Einstellungen für die Verbindung der Anwendung mit dem Administrationsserver enthält. Es wird auf Basis eines Installationspakets für dieses Programm erstellt und ist ein Sonderfall des Pakets für mobile Anwendungen.

## Endbenutzer-Lizenzvertrag

Rechtsgültiger Vertrag zwischen Ihnen und AO Kaspersky Lab. Er legt die Nutzungsbedingungen für das Programm fest.

## Entsperrungscode

Ein Code, den Sie in Kaspersky Security Center abrufen können. Er wird benötigt, um das Gerät nach der Ausführung der Befehle **Sperren und Gerät orten**, **Alarmsignal erzeugen** oder **Foto aufnehmen** sowie beim Auslösen des Selbstschutzes zu entsperren.

## Exchange Server für mobile Geräte

Eine Komponente von Kaspersky Endpoint Security, die eine Verbindung von mobilen Exchange ActiveSync-Endgeräten mit dem Administrationsserver ermöglicht.

## Geräteadministrator

Kombination von Berechtigungen für eine Anwendung auf dem Android-Gerät, die es der Anwendung erlaubt, Richtlinien für die Geräteverwaltung zu nutzen. Er ist notwendig, um alle Funktionen von Kaspersky Endpoint Security auf dem Android-Gerät zu verwenden.

## Gruppenaufgabe

Aufgabe für die Administrationsgruppe. Wird auf allen verwalteten Geräten der Gruppe ausgeführt.

## Gültigkeitsdauer der Lizenz

Der Zeitraum, in dem Sie Zugriff auf die Funktionen des Programms und die zusätzlichen Dienste haben. Die Dienste, die Sie verwenden können, sind vom Lizenztyp abhängig.

## IMAP

Das Protokoll für den Zugriff auf die E-Mail. Im Unterschied zum Protokoll POP3, gewährt IMAP erweiterte Möglichkeiten der Arbeit mit den Postfächern, wie die Verwaltung von Ordnern, die Manipulation von Nachrichten ohne Kopieren ihres Inhalts vom Mail-Server. Das IMAP-Protokoll verwendet den Port 134.

## Installationspaket

Zusammenstellung von Dateien, die zur Remote-Installation einer Kaspersky-Anwendung mithilfe eines Remote-Management-Systems dient. Ein Installationspaket wird auf der Grundlage von speziellen Dateien erstellt, die im Programmpaket enthalten sind. Das Installationspaket enthält eine Auswahl von Einstellungen, die für die Installation des Programms und die Gewährleistung seiner problemlosen Ausführung sofort nach der Installation erforderlich sind. Die Einstellungswerte im Installationspaket entsprechen der Standardkonfiguration der Anwendung.

## iOS MDM-Gerät

Mobiles Endgerät für die iOS-Plattform, das von einem [iOS MDM-Server](#) für Mobilgeräte verwaltet wird.

## iOS MDM-Profil

Profil mit Einstellungen für die Verbindung von mobilen iOS-Geräten mit dem Administrationsserver. Das iOS MDM-Profil erlaubt das Senden von iOS-Konfigurationsprofilen im Hintergrundmodus mithilfe des iOS MDM-Servers für Mobilgeräte sowie das Erhalten erweiterter Diagnoseinformationen über mobile Geräte. Der Link für ein iOS MDM-Profil muss an den Benutzer gesendet werden, damit der iOS MDM-Server für Mobilgeräte das mobile Gerät erkennen und in die iOS-Verwaltung einbinden kann.

## iOS MDM-Server für Mobilgeräte

Eine Komponente von Kaspersky Endpoint Security, die auf einem Client-Gerät installiert wird. Sie ermöglicht die Verbindung von mobilen iOS-Geräten mit dem Administrationsserver und deren Verwaltung mithilfe des Dienstes Apple Push Notifications (APNs).

## Kaspersky Private Security Network (Private KSN)

Kaspersky Private Security Network ist eine Lösung, dank der Benutzer von Geräten mit installierten Kaspersky-Anwendungen auf die Reputationsdatenbanken von Kaspersky Security Network und andere statistische Daten zugreifen können, ohne dass Daten von ihren Geräten an Kaspersky Security Network gesendet werden müssen. Kaspersky Private Security Network wurde für Unternehmenskunden entwickelt, die aus einem der folgenden Gründe nicht an Kaspersky Security Network teilnehmen können:

- Die Benutzergeräte haben keine Internetverbindung.
- Die Übertragung von Daten außerhalb des Landes oder des lokalen Unternehmensnetzwerks ist gesetzlich oder durch die Sicherheitsrichtlinien des Unternehmens verboten.

## Kaspersky Security Network (KSN)

Eine Infrastruktur aus Cloud-Diensten, die Zugriff auf die Kaspersky-Datenbank bietet. Diese Datenbank enthält laufend aktualisierte Informationen über die Reputation von Dateien, Webressourcen und Software. Kaspersky Security Network gewährleistet eine schnellere Reaktion der Programme von Kaspersky auf neue Bedrohungen, erhöht die Leistung einiger Schutzkomponenten und verringert die Wahrscheinlichkeit von Fehlalarmen.



## Kaspersky-Kategorien

Durch die Mitarbeiter von Kaspersky ausgearbeitete, fertige Datenkategorien. Diese Kategorien können beim Datenbanken-Update des Programms aktualisiert werden. Der Experte für Informationssicherheit kann diese fertigen Kategorien weder ändern noch löschen.

## Kaspersky-Update-Server

HTTP(S)-Server bei Kaspersky, von denen Programme von Kaspersky Updates für Datenbanken und Programm-Module herunterladen.

## Lizenz

Ein zeitlich begrenztes Nutzungsrecht für eine App, das Ihnen auf Basis eines Endbenutzer-Lizenzvertrags überlassen wird.

## Manifest-Datei

Eine Datei im Format PLIST. Diese Datei enthält einen Link zur Anwendungsdatei (ipa-Datei), die auf dem Webserver abgelegt ist. Sie wird vom iOS-Gerät für die Suche, den Download und die Installation von Anwendungen vom Webserver verwendet.

## Phishing

Eine Art des Internet-Betrugs mit dem Ziel, unberechtigten Zugriff auf die vertraulichen Daten der Benutzer zu erlangen.

## POP3

Das Netzwerkprotokoll für den Abruf von Nachrichten vom Mail-Server durch den Mail-Client.

## Programm aktivieren

Alle Programmfunktionen freischalten. Das Programm wird vom Benutzer während oder nach der Installation aktiviert. Für die Aktivierung des Programms benötigt der Benutzer einen Aktivierungscode oder eine Schlüsseldatei.

## Provisioning-Profil

Eine Sammlung an Einstellungen für den Betrieb der Anwendungen auf mobilen iOS-Geräten. Ein Provisioning-Profil enthält Informationen über die Lizenz und ist mit einer konkreten Anwendung verknüpft.

## Proxy-Server

Ein Computernetzwerkdienst, der Benutzern ermöglicht, indirekte Abfragen anderer Netzwerkdienste durchzuführen. Zunächst stellt der Benutzer eine Verbindung zu einem Proxyserver her und fordert eine Ressource an (z. B. eine Datei), die sich auf einem anderen Server befindet. Danach stellt der Proxyserver entweder eine Verbindung zum angegebenen Server her und ruft die Ressource von dort ab oder gibt die Ressource aus einem eigenständigen Cache zurück (vorausgesetzt, dass der Proxyserver über einen Cache verfügt). In einigen Fällen kann die Anfrage des Kunden oder die Antwort des Servers zu bestimmten Zwecken verändert werden.

## Quarantäne

Ordner, in den Kaspersky gefundene, möglicherweise infizierte Objekte verschiebt. Objekte werden verschlüsselt in der Quarantäne gespeichert, was ihre Beeinflussung des Computersystems unterbindet.

## Richtlinie

Programm- und Anwendungseinstellungen für Kaspersky Endpoint Security, die auf Geräte in den Administrationsgruppen oder auf einzelne Geräte angewandt werden. Für verschiedene Administrationsgruppen können verschiedene Richtlinien gelten. Die Richtlinie beinhaltet festgelegte Parameter für alle Funktionen der mobilen Anwendungen von Kaspersky Endpoint Security.

## Schlüsseldatei

Datei im Format xxxxxxxx.key, die es ermöglicht, Programme von Kaspersky mit einer Testlizenz oder mit einer kommerziellen Lizenz zu nutzen. Das Programm erzeugt eine Schlüsseldatei auf Basis des Aktivierungscodes. Das Programm darf nur verwendet werden, wenn eine Schlüsseldatei vorliegt.

## SSL

Datenverschlüsselungsprotokoll, das im Internet und in lokalen Netzwerken verwendet wird. Das Secure Sockets Layer-Protokoll (SSL) wird in Web-Apps zum Herstellen von geschützten Verbindungen zwischen Client und Server verwendet.

## Übereinstimmungsüberprüfung

Untersuchung der Übereinstimmung der Einstellungen des mobilen Geräts und Kaspersky Endpoint Security für Android mit den Anforderungen an die Unternehmenssicherheit. Die Anforderungen an die Unternehmenssicherheit regeln die Gerätenutzung. Auf dem Gerät muss beispielsweise der Echtzeitschutz aktiviert sein, die Antiviren-Datenbanken müssen aktuell sein und das Kennwort des Geräts muss hinreichend komplex sein. Die Übereinstimmungsüberprüfung funktioniert auf der Grundlage einer Liste von Regeln. Eine Übereinstimmungsregel besteht aus folgenden Komponenten:

- Kriterien zur Untersuchung des Geräts (beispielsweise das Fehlen von verbotenen Apps auf dem Gerät)
- Zeitspanne, die dem Benutzer des Geräts zur Beseitigung von Abweichungen zur Verfügung steht (z. B. 24 Stunden)
- Aktion, die für das Gerät ausgeführt wird, wenn der Benutzer die Abweichungen nicht im Laufe der angegebenen Zeitspanne beseitigt (beispielsweise Sperrung des Geräts)

## Verwaltungs-Plug-in für Programme

Spezielle Komponente, die eine Schnittstelle zur Verwaltung eines Kaspersky-Programms über die Verwaltungskonsole bereitstellt. Jede Anwendung, die durch Kaspersky Security Center SPE verwaltet werden kann, verfügt über ihr eigenes Verwaltungs-Plug-in. Das Verwaltungs-Plug-in ist Teil aller Kaspersky-Anwendungen, die über Kaspersky Security Center verwaltet werden können.

## Virus

Ein Programm, das seinen eigenen Code in andere Programme schreibt und sie damit infiziert, um dann beim Start infizierter Dateien die Kontrolle zu erlangen. Diese einfache Definition fasst die wichtigste Funktion von Viren zusammen: die Infektion.

## Webserver für Kaspersky Security Center



Komponente von Kaspersky Security Center, die zusammen mit dem Administrationsserver installiert wird. Der Webserver ist für die Übermittlung von autonomen Installationspaketen, iOS MDM-Profilen und Dateien aus dem Ordner für den allgemeinen Zugriff über das Netzwerk vorgesehen.

## Zertifikat für den Apple Push Notification Service (APNs)

Zertifikat, das von Apple signiert wird und Ihnen ermöglicht, den Dienst Apple Push Notification zu nutzen. Mithilfe des Dienstes Apple Push Notification kann der iOS MDM-Server iOS-Geräte verwalten.

## Informationen über den Code von Drittherstellern

Informationen über den Code von Drittherstellern finden Sie in den folgenden Dateien, die Sie herunterladen und lesen können:

- [legal\\_notices\\_Android.txt](#)  (für die App "Kaspersky Endpoint Security für Android")
- [legal\\_notices\\_iOS.txt](#)  (für die App "Kaspersky Security für iOS")

Auf mobilen Geräten sind Informationen über den Code von Drittherstellern im Abschnitt **Über die App** der mobilen Apps verfügbar.

# Markenrechtliche Hinweise

Eingetragene Markenzeichen und Handelsmarken sind das Eigentum ihrer Besitzer.

PostScript ist ein Markenzeichen oder eingetragenes Markenzeichen von Adobe in den USA und/oder in anderen Ländern.

AirDrop und AirPrint sind Markenzeichen von Apple Inc.

Apple, Apple Configurator, AirPlay, Airport Express, App Store, Apple TV, Bonjour, Face ID, FaceTime, FileVault, iBooks, iCal, iCloud, iPad, iPadOS, iPhone, iTunes, OS X, Safari, Spotlight und Touch ID sind in den USA und in anderen Ländern und Regionen eingetragene Markenzeichen von Apple Inc.

Aruba Networks ist ein in den USA und einigen anderen Ländern eingetragenes Markenzeichen von Aruba Networks, Inc.

Die Bluetooth-Wortmarke, das Markenzeichen und die Bluetooth-Logos sind Eigentum von Bluetooth SIG, Inc.

Cisco, Cisco AnyConnect und IOS sind Markenzeichen oder eingetragene Markenzeichen von Cisco Systems, Inc. und/oder von verbundenen Unternehmen in den USA und in einigen anderen Ländern.

SecurID ist ein Markenzeichen oder eingetragenes Markenzeichen von EMC Corporation in den USA und/oder in anderen Ländern.

Google, Android, Chrome, Chromebook, Chromium, Crashlytics, Firebase, Google Analytics, Google Chrome, Google Mail, Google Maps, Google Play, Nexus und SPDY sind Markenzeichen von Google LLC.

HTC ist eine Marke der HTC Corporation.

Huawei, HUAWEI und EMUI sind in China und in anderen Ländern eingetragene Markenzeichen von Huawei Technologies Co., Ltd.

IBM und Maas360 sind Markenzeichen der International Business Machines Corporation, die in vielen Ländern der Welt eingetragen sind.

Juniper Networks, Juniper und JUNOS sind Markenzeichen oder eingetragene Markenzeichen von Juniper Networks, Inc. in den USA und in anderen Ländern.

Microsoft, ActiveSync, Microsoft Intune, Tahoma, Windows, Windows Mobile und Windows Phone sind Markenzeichen der Microsoft-Unternehmensgruppe.

MOTOROLA und das Stylized M Logo sind Markenzeichen oder eingetragene Markenzeichen der Motorola Trademark Holdings, LLC.

Oracle und JavaScript sind eingetragene Markenzeichen von Oracle und/oder von verbundenen Unternehmen.

BlackBerry ist eine in den Vereinigten Staaten von Amerika eingetragene Marke von Research In Motion Limited und kann auch in anderen Ländern angemeldet oder registriert sein.

Samsung ist ein in den USA oder in anderen Ländern eingetragenes Markenzeichen des Unternehmens SAMSUNG.

SonicWALL, Aventail, und SonicWALL Mobile Connect sind Marken von SonicWALL, Inc.

SOTI und MobiControl sind in den USA und in anderen Ländern eingetragene Markenzeichen von SOTI Inc.

Symantec ist ein Markenzeichen oder eingetragenes Markenzeichen der Symantec Corporation und/oder ihrer verbundenen Unternehmen in den USA und anderen Ländern.

Das Markenzeichen Symbian ist Eigentum von Symbian Foundation Ltd.

AirWatch, VMware und VMware Workspace ONE sind Markenzeichen oder eingetragene Markenzeichen von VMware, Inc. oder in den USA und/oder in anderen Ländern eingetragene Markenzeichen von VMware, Inc.

F5 ist ein Markenzeichen von F5 Networks, Inc. in den USA und bestimmten anderen Ländern.