kaspersky

Kaspersky Security for Mobile

目录

Kaspersky Security for Mobile 帮助

Kaspersky Security for Mobile 旨在保护和管理公司移动设备以及公司员工用于公司用途的个人移动设备。

Kaspersky Security for Mobile 的组件和功能取决于您使用的 Kaspersky Security Center 控制台，该控制台用作保护和管理移动设备的界面。

根据您的 Kaspersky Security Center 控制台，选择必要的帮助部分：

- 基于 Microsoft 管理控制台的管理控制台
- Kaspersky Security Center Web Console 或 Kaspersky Security Center 云控制台

单独的“帮助”部分介绍了 Kaspersky Endpoint Security for Android 应用程序和 Kaspersky Security for iOS 应用程序的用户可以使用的功能和操作。

新增功能

Kaspersky Endpoint Security for Android Technical Release 44

- 现已支持 Android 13。
- 对于 SOTI MobiControl 控制台用户，增加了一个在 Kaspersky Security Center 中指定 SOTI MobiControl 设备名称的选项。
- 常规问题修复和改进。

Kaspersky Endpoint Security for Android Technical Release 43

- 在 Android 12 或更高版本中，Kaspersky Endpoint Security for Android 应用程序需要获得在后台运行的权限。
- 在 Android 13 中，Kaspersky Endpoint Security for Android 应用程序会提示需要发送通知的权限。
- 常规问题修复和改进。

Kaspersky Security for iOS Technical Release 1

新的 Kaspersky Security for iOS 应用旨在保护和管理公司 iOS 和 iPadOS 设备。该应用提供了以下主要功能：

- 防御在线威胁。
- 越狱检测。
- 使用 Kaspersky Security Center Web Console 和云控制台管理公司设备。

Kaspersky Endpoint Security for Android Technical Release 42

- Kaspersky Endpoint Security for Android 应用的用户界面增强。
- Kaspersky Endpoint Security for Android 应用现在需要 Android 12 或以上版本的“附近的蓝牙设备”权限，以允许管理员限制使用蓝牙。
- 常规问题修复和改进。

Kaspersky Endpoint Security for Android Technical Release 41

- Kaspersky Endpoint Security for Android 应用的用户界面增强。
- 增强了适用于 Kaspersky Security Center Web Console 和云控制台的 Kaspersky Security for Mobile (Policies) 插件的策略设置中的用户界面。
- 常规问题修复和改进。

Kaspersky Endpoint Security for Android Technical Release 40

- 常规问题修复和改进。

Kaspersky Endpoint Security for Android Technical Release 39

- 现已支持 Android 12L。
- 如下协议和声明已更新：
  - 最终用户授权许可协议
  - 卡巴斯基安全网络声明
  - 有关将数据处理用于市场营销的声明

  请注意，管理员可以在管理控制台中接受协议和声明的新条款。这允许设备上 Kaspersky Endpoint Security for Android 应用程序的用户跳过此步骤。
- 常规问题修复和改进。

Kaspersky Endpoint Security for Android Technical Release 33

- 使用第三方 EMM 系统管理 Kaspersky Endpoint Security for Android 应用时，现在可以使用单个命令接受多个最终用户授权许可协议。
- 不再需要密钥来激活 Samsung KNOX。
- Kaspersky Security for Mobile 组件版本的结构已修改为包含版本号。

Kaspersky Endpoint Security for Android Technical Release 32

- Kaspersky Endpoint Security for Android 应用程序已修改为支持更新的 Android 要求。

Kaspersky Endpoint Security for Android Technical Release 31

- 如果您的组织中未部署 Kaspersky Security Center 或移动设备无法访问 Kaspersky Security Center，用户可以在其设备上手动激活 Kaspersky Endpoint Security for Android 应用程序。
- Kaspersky Security for Mobile 现在支持 Google Chrome 的自定义标签功能。

Kaspersky Endpoint Security for Android Technical Release 30

- Kaspersky Security for Mobile 现在允许您在 Kaspersky Security Center Cloud Console 中保护和管理移动设备。
- Kaspersky Security for Mobile 现在支持 iOS 15 和 iPadOS 15。

Kaspersky Endpoint Security for Android Technical Release 29

- Kaspersky Endpoint Security for Android 应用程序现在支持 Android 12。

Kaspersky Endpoint Security for Android Technical Release 27

- Kaspersky Security for Mobile 现在允许您在 Kaspersky Security Center Web Console 中保护和管理移动设备。

Kaspersky Endpoint Security for Android Technical Release 26

- Kaspersky Endpoint Security 现在支持自动续订的授权许可和订阅。

Kaspersky Endpoint Security for Android Technical Release 22

- Kaspersky Endpoint Security 现在支持卡巴斯基私有安全网络，该解决方案允许访问卡巴斯基安全网络的信誉数据库，无需在公司网络外部发送数据。
- Kaspersky Endpoint Security for Android 不再支持在运行 Android 4.2 – 4.4.4版本的设备上进行安装。

Kaspersky Endpoint Security for Android Technical Release 20

- 如果管理员选择了全局接受声明，用户不会被提示接受法律声明。
- 应用程序性能已优化。

Kaspersky Endpoint Security for Android Technical Release 19

- 管理员现在可以通过 Kaspersky Security Center 代表最终用户接受卡巴斯基安全网络声明和其他声明。
- 修复了几个错误，且改进了操作稳定性。

Kaspersky Endpoint Security for Android Technical Release 18

- Kaspersky Security for Mobile 现在支持华为移动服务。
- Kaspersky Endpoint Security for Android 现在可以从华为应用市场安装。

Kaspersky Endpoint Security for Android Technical Release 17

- Kaspersky Endpoint Security 现在以 API 级别 29 及更高级别为目标，为运行 Android 10 或更高版本的设备上的应用程序行为带来了一些变化。
- 新的密码强度设置，供用户设置所需复杂度的密码。
- 现在只能在 Android 工作配置文件中将使用指纹配置为屏幕解锁方式。
- 修复了几个错误，且改进了操作稳定性。

Kaspersky Endpoint Security for Android Technical Release 16

- Kaspersky Endpoint Security for Android 现在支持 Android 11。
- Android 11 带来的地理位置和摄像头权限的新要求。您可以在本节进一步了解摄像头和位置访问权限的新规则。
- 您现在可以在第三方 EMM 控制台中指定用户的公司电子邮件地址。如果配置了新的 KscCorporateEmail，这些电子邮件将显示在 Kaspersky Security Center 中。

Kaspersky Endpoint Security for Android Technical Release 14

- 每当用户允许或撤销应用程序的设备管理员权限时，都会向管理控制台发送一个事件。
- 现在可以在第三方 EMM 控制台中配置“KscGroup”参数。当设备连接到 Kaspersky Security Center 后，它将自动被添加到“未分配的设备”文件夹的子文件夹中，该子文件夹的名称与 EMM 控制台中配置的组名称相同。

Kaspersky Endpoint Security for Android Technical Release 13

- 新的 Kaspersky Endpoint Security for Android 用户界面设计。
- 所有帮助章节现在都在线提供。
- 受管理设备的 IP 地址现在会发送到 Kaspersky Security Center 并可以在设备信息区域中查看。

Kaspersky Endpoint Security for Android Technical Release 12

- 增加了在 Kaspersky Security Center 12.1 中远程接受最终用户授权许可协议 (EULA) 的功能。如果管理员在管理控制台中接受授权许可协议和隐私策略的条款，则应用程序在安装过程中将跳过这些步骤。
- 为使用 VMware AirWatch 的用户添加了在 Kaspersky Security Center 中编辑设备名称的功能。我们在配置文件中添加了新的设置，可用于配置应用程序。您可以将更多信息添加到设备名称（例如设备序列号等）中。这样可以更加便于在 Kaspersky Security Center 中查找和排序设备。

Kaspersky Endpoint Security for Android Technical Release 11

修复了几个错误，且改进了操作稳定性。

Kaspersky Endpoint Security for Android Technical Release 10

- Kaspersky Security for Mobile 现在支持 Kaspersky Security Center 12。
- Kaspersky Security Center 12 已停止对 Kaspersky Safe Browser 的支持。在使用 Kaspersky Security Center 11 或更早版本时，可以使用 Kaspersky Safe Browser 功能。
- 修复了几个错误，且改进了操作稳定性。

Kaspersky Endpoint Security for Android Service Pack 4 Maintenance Release 3

- Kaspersky Endpoint Security for Android 支持 Microsoft Intune (一个企业移动管理解决方案(EMM))。Kaspersky 参与 AppConfig Community 以确保应用程序可与第三方 EMM 解决方案一起运行。

- 添加了当应用处于后台模式时禁用通知和弹出消息的功能。请记住在后台模式运行这些操作是不安全的。如果当应用处于后台模式时您禁用通知和弹出消息，应用将不会警告用户实时威胁。移动设备用户仅在打开应用时才可以学习设备的设备保护状态。

- 增加了在 VMware AirWatch 中接受最终用户授权许可协议 (EULA) 和隐私策略的功能。如果管理员在 AirWatch 控制台接受授权许可协议和隐私策略，Kaspersky Endpoint Security for Android 将在初始化配置向导中跳过接受步骤。

- 添加了关于以使用 Web 保护为目的的数据处理声明(Web 保护声明)。您必须接受声明以使用 Web 保护。Kaspersky Endpoint Security for Android 使用卡巴斯基安全网络 (KSN) 扫描网站。Web 保护声明包含与 KSN 交换数据的条款和条件。您可以在策略中接受 Web 保护声明或请求从设备用户处接受。

- 修复了几个错误，且改进了操作稳定性。

取决于管理工具的应用程序功能的比较

您可以在 Kaspersky Security Center 中使用以下管理工具管理移动设备：

- 基于 Microsoft 管理控制台（下称“基于 MMC”）的 Kaspersky Security Center 管理控制台
- Kaspersky Security Center Web Console
- Kaspersky Security Center 云控制台

下表比较了这些工具中可用的功能。

功能的可用性取决于管理工具

	基于 MMC 的控制台	Web Console	云控制台
常规			
Android 设备管理	可用	可用	可用
iOS 设备管理	可用（通过 APNs 证书）	可用（通过 Kaspersky Security for iOS 应用程序）	可用（通过 Kaspersky Security for iOS 应用程序）
移动设备管理			
通过 Google Play 链接添加设备	可用	可用	可用
使用 App Store 链接添加设备	不可用	可用	可用
使用 iOS MDM 配置文件添加 iOS 设备	可用	不可用	不可用
通过创建安装包添加设备	可用	不可用	不可用
向移动设备发送命令	可用	可用（“拍摄面部照片”命令除外）	可用（“拍摄面部照片”命令除外）
从 Kaspersky Security Center 移除移动设备	可用	可用（仅从设备列表中删除。必须手动从设备中删除该应用程序。）	可用（仅从设备列表中删除。必须手动从设备中删除该应用程序。）
证书管理			
颁发邮件证书	可用	不可用	不可用
颁发 VPN 证书	可用	不可用	不可用
颁发移动证书	可用	可用	可用
通过管理服务器工具颁发移动证书	可用	可用	可用
指定证书文件	可用	不可用	不可用
与公钥基础设施集成	可用	不可用	不可用
策略管理			

对配置组策略的基于角色的访问	可用	不可用	不可用
配置移动设备与 Kaspersky Security Center 的同步	可用	可用	可用
配置对移动设备的病毒扫描	可用	可用	可用
配置移动设备保护	可用	可用	可用
配置反病毒数据库更新	可用	可用	可用
配置对被盗或丢失设备的数据的保护	可用	可用	可用
配置用户对网站的访问	可用	可用	可用
配置应用程序控制	可用	可用	可用
配置合规性控制	可用	可用	可用
配置 Android 工作配置文件	可用	不可用	不可用
配置与 Wi-Fi 网络的连接	可用	不可用	不可用
三星 KNOX	可用	不可用	不可用
其他功能			
在 Kaspersky Security Center 中全局接受 EULA	可用	不可用	不可用
配置卡巴斯基私有安全网络	可用	不可用	不可用

分发包

Kaspersky Security for Mobile 分发包可能包含各种组件，具体取决于所选的应用程序版本。

Kaspersky Security Center Web Console 中的移动设备管理

- `on_prem_ksm_devices_xx.x.x.x.zip`
  包含安装 Kaspersky Security for Mobile (Devices) 插件所需文件的压缩包：
  - `plugin.zip`
    包含 Kaspersky Security for Mobile (Devices) 插件的压缩包。
  - `signature.txt`
    包含 Kaspersky Security for Mobile (Devices) 插件签名的文件。
- `on_prem_ksm_policies_xx.x.x.x.zip`
  包含安装 Kaspersky Security for Mobile (Policies) 插件所需文件的压缩包：
  - `plugin.zip`
    包含 Kaspersky Security for Mobile (Policies) 插件的压缩包。
  - `signature.txt`
    包含 Kaspersky Security for Mobile (Policies) 插件签名的文件。

Kaspersky Security Center 云控制台中的移动设备管理

要在 Kaspersky Security Center 云控制台中管理移动设备，您无需下载分发包。您只需要在 Kaspersky Security Center 云控制台中创建一个账户。有关创建账户的更多信息，请参阅 *Kaspersky Security Center 云控制台帮助*。

基于 MMC 的管理控制台中的移动设备管理

- `Klcfginst_en.exe`
  通过 Kaspersky Security Center 远程管理系统管理应用程序所用的 Kaspersky Endpoint Security for Android 插件的安装文件。
- `Klmdminst.exe`
  通过 Kaspersky Security Center 远程管理系统管理应用程序所用的 Kaspersky Device Management for iOS 管理插件的安装文件。

Kaspersky Endpoint Security for Android 应用程序的文件

`KES10_xx_xx_xxx.apk` — Kaspersky Endpoint Security for Android 应用程序的 Android 包文件。

辅助文件

- `sc_package_xx.exe`

  自解压压缩包，其中包含通过创建安装包安装 Kaspersky Endpoint Security for Android 应用程序所需的文件：

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

    创建安装包所需的文件。

  - `installer.ini`

    包含管理服务器连接设置的配置文件。

  - `KES10_xx_xx_xxx.apk`

    Kaspersky Endpoint Security for Android 应用程序的 Android 包文件。

  - `kmlisten.exe`

    通过管理员的计算机传送安装包的实用工具。

  - `kmlisten.ini`

    包含 `kmlisten.exe` 实用工具设置的配置文件。

  - `kmlisten.kpd`

    应用程序说明文件。

- `SigningUtility.zip`

  包含实用工具的压缩包，该实用工具用于对 Kaspersky Endpoint Security for Android 应用程序的分发包和适用于 iOS 设备的容器进行签名。

文档

- Kaspersky Security for Mobile 帮助。

在 Kaspersky Security Center Web Console 和 Kaspersky Security Center 云控制台中工作

本帮助部分介绍了使用 Kaspersky Security Center Web Console（以下简称 Web Console）或 Kaspersky Security Center 云控制台（以下简称云控制台）对移动设备的保护和管理。

关于 Kaspersky Security Center Web Console 和云控制台中的移动设备管理

您可以使用以下组件在 Kaspersky Security Center Web Console 和云控制台中管理移动设备：

- **Kaspersky Endpoint Security for Android 应用程序**

  Kaspersky Endpoint Security for Android 应用可确保移动设备抵御 Web 威胁、病毒和构成威胁的其他程序的侵害。

- **Kaspersky Security for iOS 应用**

  Kaspersky Security for iOS 应用程序可确保保护移动设备免受网络钓鱼和 Web 威胁的侵害。

- **Kaspersky Security for Mobile (Devices) 插件**

  Kaspersky Security for Mobile (Devices) 插件提供了界面，用于通过 Kaspersky Security Center Web Console 和云控制台管理移动设备和这些设备上安装的移动应用程序。

- **Kaspersky Security for Mobile (Policies) 插件**

  Kaspersky Security for Mobile (Policies) 插件允许您使用组策略为连接到 Kaspersky Security Center 的设备定义配置设置。

插件集成到 *Kaspersky Security Center 远程管理系统*中。您可以使用 Kaspersky Security Center Web Console 或云控制台来管理移动设备以及客户端计算机和虚拟系统。将移动设备连接至管理服务器后，移动设备就变成托管设备。您可以远程监控受管理设备。

Kaspersky Security Center Web Console 和云控制台中的移动设备管理的主要功能

Kaspersky Security for Mobile 包括以下功能：

- 通过使用从 Google Play 下载 Kaspersky Endpoint Security for Android 应用程序的链接，分发用于将 Android 移动设备连接到 Kaspersky Security Center 的电子邮件。
- 通过使用从 App Store 下载 Kaspersky Security for iOS 应用程序的链接，分发用于将 iOS 移动设备连接到 Kaspersky Security Center 的电子邮件。
- 远程连接移动设备到 Kaspersky Security Center 和其他第三方 EMM 系统（例如，VMWare AirWatch、MobileIron、IBM Maas360、SOTI MobiControl）。
- 远程配置移动应用，以及远程配置服务、应用和移动设备功能。
- 根据企业安全要求远程配置移动设备。

- 预防移动设备在丢失或被盗时存储的企业信息泄露（反盗窃）。仅 Android 设备支持。
- 企业安全需求合规性控制（合规性控制）。仅 Android 设备支持。
- 控制对在线威胁的防护并控制移动设备的互联网使用（Web 保护）。
- 设置在 Kaspersky Endpoint Security for Android 和 Kaspersky Security for iOS 应用程序中显示给用户的通知。
- 关于 Kaspersky Endpoint Security for Android 和 Kaspersky Security for iOS 应用程序状态和事件的管理员通知可以在 Kaspersky Security Center 中或通过电子邮件进行沟通。
- 策略设置的变更控制（修订历史记录）。

Kaspersky Security for Mobile 包括以下保护和管理组件：

- 反病毒（对于 Android 设备）
- 反盗窃（对于 Android 设备）
- 网页保护（对于 Android 和 iOS 设备）
- 应用程序控制（对于 Android 设备）
- 合规性控制（对于 Android 设备）
- 检测 Android 设备的 root 权限和 iOS 设备的越狱状态

关于 Kaspersky Endpoint Security for Android 应用程序

Kaspersky Endpoint Security for Android 应用可确保移动设备抵御 Web 威胁、病毒和构成威胁的其他程序的侵害。

Kaspersky Endpoint Security for Android 应用包括以下组件：

- **反病毒**。该组件使用反病毒数据库和卡巴斯基安全网络云服务检测并消除设备上的威胁。反病毒功能包含以下组件：
  - **保护**。它会检测打开的文件中的威胁，扫描新应用，并实时防止设备感染。
  - **扫描**。它根据需要针对整个文件系统、仅针对已安装的应用程序或针对选定的文件或文件夹启动。
  - **更新**。允许您为应用程序下载新的反病毒数据库。
- **反盗窃**。该组件在设备丢失或被盗时保护设备上的信息，防御未经授权的访问。通过此组件可以向设备发送以下命令：
  - **定位**。获取设备位置的坐标。
  - **警报**。使设备发出响亮的警报声。
  - **擦除**。擦除公司数据以保护公司敏感信息。

- **Web 保护**。该组件可以阻止用于扩散恶意代码的恶意网站。Web 保护还会阻止旨在盗窃用户机密数据（例如，网上银行或电子货币系统的密码）并访问用户财务信息的虚假（钓鱼）网站。Web 保护将在您打开网站前使用卡巴斯基安全网络云服务扫描网站。扫描之后，Web 防护将允许可信的网站加载并阻止恶意网站。Web 保护还支持按卡巴斯基安全网络云服务中定义的类别进行网站过滤。这允许管理员限制用户对某些类别网页的访问（例如"赌博、彩票、抽奖"或"互联网通信"类别中的网页）。

- **应用程序控制**。使用此组件可以通过指向分发包的直接链接或指向 Google Play 的链接，将推荐和必需的应用程序安装到您的设备上。应用程序控制还允许您卸载那些违反公司安全要求的已阻止应用程序。

- **合规性控制**。此组件允许您检查受管理设备是否符合公司安全要求，并对不符合要求的设备的某些功能施加限制。

您可以在 Kaspersky Security Center Web Console 和云控制台中通过定义组策略的设置来配置 Kaspersky Endpoint Security for Android 应用程序的组件。

关于 Kaspersky Security for iOS 应用程序

Kaspersky Security for iOS 应用程序可确保保护移动设备免受网络钓鱼和 Web 威胁的侵害。

Kaspersky Security for iOS 应用程序提供了下列主要功能：

- **Web 保护**。该组件可以阻止用于扩散恶意代码的恶意网站。Web 保护还会阻止旨在盗窃用户机密数据（例如，网上银行或电子货币系统的密码）并访问用户财务信息的虚假（钓鱼）网站。Web 保护将在您打开网站前使用卡巴斯基安全网络云服务扫描网站。扫描之后，Web 防护将允许可信的网站加载并阻止恶意网站。您可以在 Kaspersky Security Center Web Console 和云控制台中通过定义组策略的设置来配置此组件。

- **越狱检测**。当 Kaspersky Security for iOS 检测到越狱时，会显示一条重要消息并通知您该问题。

关于 Kaspersky Security for Mobile (Devices) 插件

Kaspersky Security for Mobile (Devices) 插件提供了界面，用于通过 Kaspersky Security Center Web Console 和云控制台管理移动设备和这些设备上安装的移动应用程序。Kaspersky Security for Mobile (Devices) 插件允许您执行以下操作：

- 将移动设备连接到 Kaspersky Security Center。

- 管理移动设备的证书。

- 配置 Firebase Cloud Messaging（仅适用于 Android 设备）。

- 向移动设备发送命令（仅适用于 Android 设备）。

可以在配置 Kaspersky Security Center Web Console 时安装 Kaspersky Security for Mobile (Devices) 插件。如果您使用的是 Kaspersky Security Center 云控制台，则无需安装此插件。有关不同类型控制台中的部署方案的更多信息，请参见"部署方案"部分。

关于 Kaspersky Security for Mobile (Policies) 插件

Kaspersky Security for Mobile (Policies) 插件允许您使用组策略为连接到 Kaspersky Security Center 的设备定义配置设置。Kaspersky Security for Mobile (Policies) 插件可用于执行以下操作：

- 为移动设备创建组安全策略。
- 远程配置用户移动设备上的移动应用程序的运行设置。
- 接收有关用户移动设备上的移动应用程序运行情况的报告和统计信息。

可以在配置 Kaspersky Security Center Web Console 时安装 Kaspersky Security for Mobile (Policies) 插件。如果您使用的是 Kaspersky Security Center 云控制台，则无需安装此插件。有关不同类型控制台中的部署方案的更多信息，请参见"部署方案"部分。

硬件和软件要求

本部分列出了用于在 Kaspersky Security Center Web Console 和云控制台中安装 Kaspersky Security for Mobile (Devices) 插件和 Kaspersky Security for Mobile (Policies) 插件的管理员计算机的硬件和软件要求，以及移动应用程序的硬件和软件要求。

管理员计算机的硬件和软件要求

要安装 Kaspersky Security for Mobile (Devices) 插件和 Kaspersky Security for Mobile (Policies) 插件，管理员的计算机必须满足 Kaspersky Security Center 的硬件要求。有关 Kaspersky Security Center 的硬件和软件要求的更多信息：

- 如果您使用 Kaspersky Security Center Web Console，请参阅 *Kaspersky Security Center 帮助*。
- 如果您使用 Kaspersky Security Center 云控制台，请参阅 *Kaspersky Security Center 云控制台帮助*。

要在 Kaspersky Security Center Web Console 中使用 Kaspersky Security for Mobile (Devices) 插件和 Kaspersky Security for Mobile (Policies) 插件，必须在管理员的计算机上安装 Kaspersky Security Center Web Console。

要在 Kaspersky Security Center 云控制台中使用 Kaspersky Security for Mobile (Devices) 插件和 Kaspersky Security for Mobile (Policies) 插件，必须在 Kaspersky Security Center 云控制台中创建一个账户。有关创建账户的更多信息，请参阅 *Kaspersky Security Center 云控制台帮助*。

Kaspersky Endpoint Security for Android 应用程序可以在以下第三方 EMM 系统中工作：

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

支持安装 Kaspersky Endpoint Security for Android 应用程序的用户移动设备的硬件和软件要求

Kaspersky Endpoint Security for Android 应用程序具有以下硬件和软件要求：

- 智能手机或平板电脑的分辨率为 320x480 像素或更高
- 设备的主存储器具有 65 MB 的可用空间

- Android 5.0–13（包括 Android 12L，但不包括 Go Edition）
- x86、x86-64、Arm5、Arm6、Arm7 或 Arm8 处理器架构

应用程序只能安装到设备的主存储器。

支持安装 Kaspersky Security for iOS 应用程序的用户移动设备的硬件和软件要求

Kaspersky Security for iOS 应用的硬件要求如下：

- iPhone 6S 或以上版本
- iPad Air 2 或以上版本

Kaspersky Security for iOS 应用的软件要求如下：

- iOS 14.1 或更新
- iPadOS 14.1 或更新

当具有活跃 VPN 连接的 VPN 客户端在同一台移动设备上运行时，Kaspersky Security for iOS 应用无法正常运行。

已知问题和注意事项

Kaspersky Endpoint Security for Android 和 Kaspersky Security for iOS 有几个已知问题，这些问题对于这两个应用程序的运行是非关键的。

Kaspersky Security for iOS 的已知问题

- 当具有活跃 VPN 连接的 VPN 客户端在同一台移动设备上运行时，Kaspersky Security for iOS 应用无法正常运行。

Kaspersky Endpoint Security for Android 的已知问题

在 Kaspersky Security Center Web Console 中启动移动设备管理时的已知问题

- 您可以在基于 MMC 的 Kaspersky Security Center 管理控制台的初始配置期间（在运行快速启动向导时）或稍后通过在管理控制台中显示“移动设备管理”文件夹来启动移动设备管理。

安装应用程序时的已知问题

- Kaspersky Endpoint Security for Android 仅安装在设备的主内存中。
- 在运行 Android 7.0 的设备上，当 Kaspersky Endpoint Security for Android 被禁止覆盖其他窗口时，当试图禁用 Kaspersky Endpoint Security for Android 的管理员权限时可能发生错误。该问题是因一个众所周知的

Android 7 缺陷 导致。

- 在运行 Android 7.0 或更新版本的设备上，Kaspersky Endpoint Security for Android 不支持多窗口模式。
- Kaspersky Endpoint Security for Android 与运行 Chrome 操作系统的 Chromebook 设备不兼容。
- Kaspersky Endpoint Security for Android 与运行 Android (Go edition) 操作系统的设备不兼容。
- 当将 Kaspersky Endpoint Security for Android 应用程序与第三方 EMM 系统（例如，VMWare AirWatch）一起使用时，仅反病毒和 Web 保护组件可用。管理员可以在 EMM 系统控制台中配置反病毒和 Web 保护的设置。在这种情况下，有关应用程序运行的通知仅在 Kaspersky Endpoint Security for Android 应用程序的界面（报告）中可用。

升级应用程序版本时的已知问题

- 您只能将 Kaspersky Endpoint Security for Android 升级至最近的应用程序版本。Kaspersky Endpoint Security for Android 不能降级至较老版本。

反病毒运行的已知问题

- 由于技术限制，Kaspersky Endpoint Security for Android 无法扫描大小为 2 GB 或更大的文件。在扫描期间，应用程序将跳过此类文件，而不会通知您此类文件被跳过。
- 要对设备进行信息尚未添加到反病毒数据库中的新威胁的附加分析，您必须启用卡巴斯基安全网络。*卡巴斯基安全网络 (KSN)* 是一种云服务基础设施，它提供对 Kaspersky 在线知识库的访问，该知识库包含有关文件、Web 资源和软件的信誉的信息。要使用 KSN，移动设备必须连接到互联网。
- 在某些情况下，在移动设备上从管理服务器更新反病毒数据库可能会失败。在这种情况下，请在管理服务器上运行反病毒数据库更新任务。
- 在某些设备上，Kaspersky Endpoint Security for Android 不会检测通过 USB OTG 连接的设备。无法对此类设备运行病毒扫描。
- 在运行 Android 11.0 或更高版本的设备上，用户必须授予“允许访问以管理所有文件”权限。
- 在运行 Android 7.0 或更新版本的设备上，病毒扫描运行计划的配置窗口可能显示不正确（管理元件未显示）。该问题是因一个众所周知的 Android 7 缺陷 导致。
- 在运行 Android 7.0 的设备上，扩展模式下的实时保护检测不到外部 SD 卡上存储的文件中的威胁。
- 在运行 Android 6.0 的设备上，Kaspersky Endpoint Security for Android 不检测下载恶意文件到设备内存的操作。当恶意文件运行时，或者在设备病毒扫描过程中，恶意软件可以被反病毒检测到。该问题因一个众所周知的 Android 6.0 缺陷 导致。要确保设备安全，建议配置计划病毒扫描。

Web 保护运行的已知问题

- 安卓设备上的 Web 保护仅在 Google Chrome 浏览器（包括自定义标签功能）、Huawei Browser 和 Samsung Internet Browser 中可用。
- 要使 Web 保护工作，您必须启用卡巴斯基安全网络。Web 保护会基于有关网站信誉和类别的 KSN 数据阻止网站。

- 如果通过以下方式打开禁止的网站，在运行 Android 6.0 并安装 Google Chrome 51 版（或任何更早版本）的设备上，Web 保护可能会保持解除阻止这些网站（该问题是因一个众所周知的 Google Chrome 缺陷导致）：
  - 通过搜索结果。
  - 通过书签列表。
  - 通过搜索历史记录。
  - 使用网址自动填写功能。
  - 在 Google Chrome 中的新标签页中打开网站。
- 如果通过 Google 搜索结果打开禁止的网站，当浏览器设置中启用了“**Merge Tabs and Apps**”功能时，这些网站可能在 Google Chrome 50 版（或任何更早版本）中保持解除阻止。该问题是因一个众所周知的 Google Chrome 缺陷导致。
- 如果用户通过第三方应用（例如，通过即时通讯客户端应用）打开受阻止类别中的网站，则这些网站可能在 Google Chrome 中保持解除阻止。该问题关乎可访问功能服务与 Chrome 自定义标签功能如何配合使用。
- 如果用户在后台模式下通过上下文菜单或通过第三方应用（例如，即时通讯客户端应用）打开禁止的网站，这些网站可能会在 Samsung Internet Browser 中保持解除阻止。
- 必须将 Kaspersky Endpoint Security for Android 设置为可访问功能以确保 Web 保护能正常运行。
- 当刷新页面时，Samsung Internet Browser 在“**仅允许列出的网站**”Web 保护模式下可能会阻止允许的网站。如果常规表达式包含高级设置（例如，`^https?:\/\/example\.com\/pictures\/`），则会阻止网站。建议使用不含附加设置的常规表达式（例如，`^https?:\/\/example\.com`）。

反盗窃运行的已知问题

- 为了将命令及时传送到安卓设备，应用会使用 Firebase Cloud Messaging (FCM) 服务。如果未配置 FCM，将仅在与 Kaspersky Security Center 同步期间按照策略中定义的计划（例如，每 24 小时）将命令传送到设备。
- 要锁定设备，必须将 Kaspersky Endpoint Security for Android 设置为设备管理员。
- 要锁定运行 Android 7.0 或更高版本的设备，必须将 Kaspersky Endpoint Security for Android 设置为可访问功能。
- 在某些设备上，如果设备上启用了低电量模式，反盗窃命令可能无法执行。该缺陷在 Alcatel 5080X 上被确认。
- 要定位运行 Android 10.0 或更高版本的设备，用户必须为设备定位授予“始终”权限。

应用程序控制运行的已知问题

- 必须将 Kaspersky Endpoint Security for Android 设置为无障碍功能才能确保“应用程序控制”正常运行。
- 要使应用程序控制（应用程序类别）工作，您必须启用卡巴斯基安全网络。应用程序控制会基于 KSN 中可用的数据确定应用程序的类别。要使用 KSN，移动设备必须连接到互联网。对于应用程序控制，您可以将单个应用程序添加到阻止和允许的应用程序列表。在这种情况下，无需 KSN。
- 当配置应用程序控制时，建议清除“**阻止系统应用程序**”复选框。阻止系统应用程序可能会导致设备运行问题。

配置设备解锁密码强度时的已知问题

- 在运行 Android 10.0 或更高版本的设备上，Kaspersky Endpoint Security 将密码强度要求解析为系统值之一：中或高。

  如果所需的密码长度是 1 到 4 个符号，该应用程序会提示用户设置中强度密码。它必须是没有重复并且没有顺序（例如 1234）的数字（PIN），或者是字母数字。PIN 或密码必须至少有 4 个字符长。

  如果所需的密码长度是 5 个或更多符号，该应用程序会提示用户设置高强度密码。它必须是没有重复并且没有顺序的数字（PIN），或者是字母数字（密码）。PIN 必须至少为 8 位数字；密码必须至少有 6 个字符长。

- 在运行 Android 7.1.1 的设备上，如果解锁密码不符合企业安全需要（合规性控制），当尝试通过 Kaspersky Endpoint Security for Android 更改解锁密码时，“设置”系统应用可能无法正常工作。该问题是因一个众所周知的 Android 7.1.1 缺陷 导致。这种情况下，仅可使用设置系统 app 来更改解锁密码。

- 在一些运行 Android 6.0 或更新版本的设备上，如果设备数据被加密，当输入屏幕解锁密码时可能发生错误。该问题与 MIUI 固件的辅助功能服务的特定功能有关。

应用程序删除保护的已知问题

- 必须将 Kaspersky Endpoint Security for Android 设置为设备管理员。

- 要保护在运行安卓 7.0 或更高版本的设备上的应用程序不会被卸载，必须将 Kaspersky Endpoint Security for Android 设置为可访问功能。

- 在某些小米和华为设备上，Kaspersky Endpoint Security for Android 卸载保护不工作。该问题是由小米的 MIUI 7 和 8 固件以及华为的 EMUI 固件的特定功能导致。

配置设备限制时的已知问题

- 在运行 Android 10.0 或更高版本的设备上，不支持禁止使用 Wi-Fi 网络。

- 在运行 Android 10.0 或更高版本的设备上，不能完全禁止使用摄像头。

- 在运行 Android 11 或更高版本的设备上，必须将 Kaspersky Endpoint Security for Android 设置为无障碍功能。Kaspersky Endpoint Security for Android 会提示用户通过初始配置向导将该应用程序设置为可访问功能。用户可以跳过此步骤或以后在设备设置中禁用此服务。如果是这种情况，您将无法限制使用摄像头。

向移动设备发送命令时的已知问题

- 在运行 Android 12 或更高版本的设备上，如果用户授予了“使用大致位置”权限，Kaspersky Endpoint Security for Android 应用程序首先会尝试获取精确的设备位置。如果获取不成功，则只有在不超过 30 分钟前已收到设备的大致位置时，才会返回该位置。否则，“**定位设备**”命令将失败。

特定设备的已知问题

- 在某些设备（例如，华为、魅族和小米）上，您必须为 Kaspersky Endpoint Security for Android 授予自动启动权限，或手动将其添加到在操作系统启动时启动的应用程序列表中。如果未将该应用程序添加到列表，在移动设备重新启动后，Kaspersky Endpoint Security for Android 会停止执行其所有功能。此外，如果设备已锁定，您无法使用命令解锁设备。您只能通过使用一次性解锁码解锁设备。

- 在运行 Android 6.0 或更高版本的某些设备（例如，魅族和 Asus）上，在加密数据和重启安卓设备之后，您必须输入数字密码才能解锁设备。如果用户使用图形密码解锁设备，您必须将图形密码转换为数字密码。对于

更多转换图形密码到数字密码的详情，请参考移动设备生产商的技术支持网站。该问题关乎可访问功能服务的操作。

- 在某些运行 Android 5.X 的华为设备上，将 Kaspersky Endpoint Security for Android 设置为无障碍功能后，可能会显示一条有关缺少适当权限的错误消息。要隐藏此消息，请在设备设置中将该应用程序设置为受保护应用程序。

- 在某些运行 Android 5.X 或 6.X 的华为设备上，当为 Kaspersky Endpoint Security for Android 启用低电量模式时，用户可以手动终止该应用程序。那样之后，用户设备变成无保护状态。该问题是由于华为软件的一些功能导致的。若要恢复设备保护，请手动运行 Kaspersky Endpoint Security for Android。建议在设备设置中对 Kaspersky Endpoint Security for Android 禁用低电量模式。

- 在运行基于 Android 7.0 的 EMUI 固件的华为设备上，用户可以隐藏关于 Kaspersky Endpoint Security for Android 保护状态的通知。该问题是由于华为软件的一些功能导致的。

- 在某些小米设备上，当在策略中设置超过 5 个字符的密码长度时，用户将被提示更改屏幕解锁密码而不是 PIN 码。您设置的 PIN 码不能超过 5 个字符。该问题是由于小米软件的一些功能导致的。

- 在运行基于 Android 6.0 的 MIUI 固件的小米设备上，Kaspersky Endpoint Security for Android 图标可能在状态栏中隐藏。该问题是由于小米软件的一些功能导致的。建议在“通知”设置中允许显示通知图标。

- 在一些运行 Android 6.0.1 的 Nexus 设备上，正常操作所需的权限无法通过 Kaspersky Endpoint Security for Android 快速启动向导授予。该问题由众所周知的 Google 的安卓安全补丁缺陷导致。为确保正常运行，必须在设备设置中手动授予所需权限。

- 在某些运行 Android 7.0 或更高版本的三星设备上，当用户尝试配置不受支持的方法（例如，图形密码）来解锁设备时，如果满足以下条件，设备可能会锁定：Kaspersky Endpoint Security for Android 卸载保护已启用并且设置了屏幕解锁密码长度要求。要解锁设备，您必须发送特殊命令到设备。

- 在某些三星设备上，无法阻止使用指纹解锁屏幕。

- 在某些三星设备上，如果设备连接到 3G/4G 网络，启用了省电模式并限制后台数据，则无法启用 Web 保护。建议在“低电量模式”设置中禁用限制后台进程的功能。

- 在某些三星设备上，如果解锁密码不符合企业安全要求，Kaspersky Endpoint Security for Android 不会阻止使用指纹解锁屏幕。

- 在某些荣耀和华为设备上，您无法限制蓝牙的使用。当 Kaspersky Endpoint Security for Android 试图限制蓝牙使用时，操作系统显示包含拒绝或允许该限制的选项的通知。用户可以拒绝该限制并继续使用蓝牙。

- 在 Blackview 设备上，用户可以清除 Kaspersky Endpoint Security for Android 应用程序的内存。结果是，设备保护和管理将被禁用，所有已定义的设置都将无效，并且 Kaspersky Endpoint Security for Android 应用程序从无障碍功能中删除。这是因为此供应商的设备为自定义的“最近使用的应用”屏幕应用程序提供了提升的权限。此应用程序可以覆盖 Kaspersky Endpoint Security for Android 设置并且无法替换，因为它是 Android 操作系统的一部分。

- 在某些运行 Android 11 的设备上，Kaspersky Endpoint Security for Android 应用程序在启动后立即崩溃。该问题由一个众所周知的 Android 11 缺陷 导致。

应用程序在 Android 13 中运行的已知问题

- 在 Android 13 中，用户可以使用前台服务任务管理器来阻止 Kaspersky Endpoint Security 在后台运行。这是由 Android 13 中的一个众所周知的问题 导致的。

- 在 Android 13 中，开始初始应用配置时会请求发送通知的权限。这是 Android 13 操作系统的特性所致。

在 Kaspersky Security Center Web Console 或云控制台中部署移动设备管理解决方案

要使用 Kaspersky Security Center Web Console 或云控制台管理移动设备，您必须部署移动设备管理解决方案。

部署方案

在 Kaspersky Security Center Web Console 中部署

在 Kaspersky Security Center Web Console 中部署移动设备管理解决方案包括以下步骤：

1. 准备 Kaspersky Security Center Web Console 以进行部署
2. 部署管理插件
3. 部署移动应用程序
4. （可选，仅适用于 Android）配置与 Firebase Cloud Messaging 的信息交换

   建议执行此步骤以确保在更改策略设置后及时将命令传送到移动设备并进行强制同步。

在 Kaspersky Security Center 云控制台中部署

在 Kaspersky Security Center 云控制台中部署移动设备管理解决方案包括以下步骤：

1. 准备 Kaspersky Security Center 云控制台以进行部署
2. 部署移动应用程序
3. （可选，仅适用于 Android）配置与 Firebase Cloud Messaging 的信息交换

   建议执行此步骤以确保在更改策略设置后及时将命令传送到移动设备并进行强制同步。

准备 Kaspersky Security Center Web Console 和云控制台以进行部署

本节提供有关准备 Kaspersky Security Center Web Console 和云控制台以进行部署的说明。

配置管理服务器以连接移动设备

为了使移动设备能够连接到管理服务器，在移动设备上安装 Kaspersky Endpoint Security for Android 应用程序或 Kaspersky Security for iOS 应用程序之前，必须在管理服务器属性中定义移动设备连接设置。

要为移动设备连接定义管理服务器设置：

1. 在管理服务器中启动移动设备管理。

   您可以在基于 MMC 的 Kaspersky Security Center 管理控制台的初始配置期间（在运行快速启动向导时）或稍后通过在管理控制台中显示“移动设备管理”文件夹来启动移动设备管理。

2. 在 Kaspersky Security Center Web Console 或云控制台的主窗口中，单击“**设置**”()。

   将打开管理服务器属性窗口。

3. 配置移动设备将使用的管理服务器端口：

   a. 选择“**其他端口**”区域。

   b. 启用“**为移动设备开放端口**”切换按钮。

   c. 在“**用于同步移动设备的端口**”字段中，指定移动设备用来连接至管理服务器的端口。

      默认情况下使用 13292。

      如果“**为移动设备开放端口**”切换按钮关闭，或者指定了错误的连接端口，移动设备将无法连接至管理服务器。

   d. 在“**用于激活移动设备的端口**”字段中，指定移动设备用于连接到管理服务器以激活移动应用程序的端口。

      默认情况下使用 13292。

      如果指定错误的连接端口，移动设备的用户将无法使用管理服务器激活移动应用程序。

4. 如有必要，编辑移动设备将用来连接到管理服务器的证书。

   默认情况下，管理服务器使用在安装管理服务器期间创建的证书。如果需要，请将通过管理服务器颁发的证书替换为其他证书或重新颁发通过管理服务器颁发的证书。

   要编辑证书：

   a. 选择“**证书**”区域。

   b. 定义所需的设置。

      有关证书的详细信息，请参阅 *Kaspersky Security Center 帮助*。

5. 单击“**保存**”按钮以保存对设置所做的更改并退出管理服务器属性窗口。

配置移动设备连接设置后，您可以在移动设备上安装 Kaspersky Endpoint Security for Android 应用程序或 Kaspersky Security for iOS 应用程序，并使用指定的设置将它们连接到管理服务器。

创建管理组

组策略用于对用户移动设备上安装的 Kaspersky Endpoint Security for Android 应用程序或 Kaspersky Security for iOS 应用程序执行集中配置。

若要将策略应用于一组设备，建议您在用户设备上安装移动应用程序之前，先在“**受管理设备**”中为这些设备创建单独的组。

创建管理组后，建议配置选项以将要安装应用程序的设备自动分配到此组。然后使用组策略配置所有设备通用的设置。

要创建管理组：

1. 在 Kaspersky Security Center Web Console 或云控制台的主窗口中，选择“**设备 > 组层次结构**”。
2. 在管理组结构中，选择要包括新管理组的管理组。
3. 单击“**添加**”按钮。
4. 在打开的“**新管理组的名称**”窗口中，输入组的名称，然后单击“**添加**”按钮。

具有指定名称的新管理组出现在管理组层次结构中。

创建自动将设备分配至管理组的规则

在移动设备上安装 Kaspersky Endpoint Security for Android 应用程序或 Kaspersky Security for iOS 应用程序后，这些设备会显示在 Kaspersky Security Center Web Console 或云控制台的“**发现和部署 > 未分配的设备**”页面上。要管理新连接的设备，可以手动将它们移动到管理组或创建自动将它们分配到管理组的规则。

要创建自动将移动设备分配到管理组的规则：

1. 在 Kaspersky Security Center Web Console 或云控制台的主窗口中，选择“**发现和部署 > 部署和分配 > 移动规则**”。
2. 在打开的“**新规则**”窗口中，单击“**添加**”按钮。
3. 在“**规则名称**”字段中，指定规则名称。
4. 在“**管理组**”字段中，选择移动设备在安装了应用程序后将分配到的管理组。
5. 在“**应用规则**”区域中，选择“**为每个设备运行一次**”。
6. 选中“**仅移动未添加至管理组的设备**”复选框，以防止在应用规则时将移动设备移至其他管理组。
7. 选中“**启用规则**”复选框，以在创建规则后立即应用该规则。
   您稍后可以随时使用“**移动规则**”页面上的切换按钮启用该规则。
8. 选择“**规则条件 > 应用程序**”，然后执行以下操作：
   a. 启用“**操作系统版本**”切换按钮。
   b. 在打开的操作系统列表中，选择“**Android**”或“**iOS**”。

   该规则将应用于相应设备。您必须至少指定一个条件才能创建规则。
9. 单击“**保存**”以创建规则。

新创建的规则显示在“**移动规则**”页面上。根据规则，Kaspersky Security Center 会将所有新连接的设备分配到选定的管理组。

有关管理组对未分配设备的管理和操作的详细信息：

- 如果您使用 Kaspersky Security Center Web Console，请参阅 *Kaspersky Security Center 帮助*。
- 如果您使用 Kaspersky Security Center 云控制台，请参阅 *Kaspersky Security Center 云控制台帮助*。

部署管理插件

要在 Kaspersky Security Center Web Console 中管理移动设备，必须安装以下管理插件：

- Kaspersky Security for Mobile (Devices) 插件
- Kaspersky Security for Mobile (Policies) 插件

如果您使用的是 Kaspersky Security Center 云控制台，则无需安装管理插件。您只需要在 Kaspersky Security Center 云控制台中创建一个账户。有关创建账户的更多信息，请参阅 *Kaspersky Security Center 云控制台帮助*。

您可以使用以下方法安装管理插件：

- 通过使用 Kaspersky Security Center Web Console 的快速启动向导。

  安装管理服务器后，Kaspersky Security Center Web Console 会在您第一次连接时自动提示您运行快速启动向导。您也可以随时手动启动快速启动向导。

  有关 Kaspersky Security Center 快速启动向导的详细信息，请参阅 *Kaspersky Security Center 帮助*。

- 通过使用 Kaspersky Security Center Web Console 中的可用分发包列表。

  在新版本的 Kaspersky 应用程序发布后，可用分发包列表会自动更新。

- 从外部源下载分发包并将管理插件添加到 Kaspersky Security Center Web Console。

  例如，可以在 Kaspersky 网站上下载管理插件的分发包。

从可用分发包列表安装管理插件

要安装管理插件：

1. 在 Kaspersky Security Center Web Console 的主窗口中，选择“**控制台设置** > **WEB 插件**”。
2. 单击“**添加**”按钮。

   这将打开 Kaspersky 应用程序最新版本的列表。
3. 安装管理插件：

   a. 在可用应用程序列表中，单击“**移动设备**”区域将其展开。

   b. 选择“**Kaspersky Security for Mobile (Devices)**”，然后单击“**安装插件**”。

   c. 选择“**Kaspersky Security for Mobile (Policies)**”，然后单击“**安装插件**”。

将下载分发包并安装插件。安装每个插件并将其添加到 Kaspersky Security Center Web Console 后，将显示一个确认窗口。

从分发包安装管理插件

您可以在 Kaspersky 网站下载分发包。

要从分发包安装 Kaspersky Security for Mobile (Devices) 插件：

1. 将分发包的 `on_prem_ksm_devices_xx.x.x.x.zip` 压缩文件中的 `plugin.zip` 和 `signature.txt` 文件复制到管理员的工作站。
2. 在 Kaspersky Security Center Web Console 的主窗口中，选择“**控制台设置** > **WEB 插件**”。
3. 单击“**从文件添加**”。
4. 在打开的“**从文件添加**”窗口中，单击“**上传 ZIP 文件**”，然后浏览查找 `plugin.zip`。
5. 单击“**上传签名**”，然后浏览查找 `signature.txt`。
6. 单击“**添加**”按钮。

Kaspersky Security for Mobile (Devices) 插件已安装并添加到 Kaspersky Security Center Web Console。

要从分发包安装 Kaspersky Security for Mobile (Policies) 插件：

1. 将分发包的 `on_prem_ksm_policies_xx.x.x.x.zip` 压缩文件中的 `plugin.zip` 和 `signature.txt` 文件复制到管理员的工作站。
2. 在 Kaspersky Security Center Web Console 的主窗口中，选择“**控制台设置** > **WEB 插件**”。
3. 单击“**从文件添加**”。
4. 在打开的“**从文件添加**”窗口中，单击“**上传 ZIP 文件**”，然后浏览查找 `plugin.zip`。
5. 单击“**上传签名**”，然后浏览查找 `signature.txt`。
6. 单击“**添加**”按钮。

Kaspersky Security for Mobile (Policies) 插件已安装并添加到 Kaspersky Security Center Web Console。

您可以通过在“**控制台设置** > **WEB 插件**”页面上查看已安装的插件列表来确保已安装管理插件。

部署移动应用程序

要在 Kaspersky Security Center Web Console 或云控制台中管理移动设备，您必须在移动设备上部署 Kaspersky Endpoint Security for Android 应用程序或 Kaspersky Security for iOS 应用程序。您可以使用 Kaspersky Security Center Web Console 或云控制台在移动设备上部署应用程序。

使用 Kaspersky Security Center Web Console 或云控制台部署移动应用程序

移动应用程序将部署到其用户账户已添加到 Kaspersky Security Center 的用户的移动设备上。有关 Kaspersky Security Center 中用户账户的更多信息：

- 如果您使用 Kaspersky Security Center Web Console，请参阅 *Kaspersky Security Center 帮助*。
- 如果您使用 Kaspersky Security Center 云控制台，请参阅 *Kaspersky Security Center 云控制台帮助*。

您可以使用 Kaspersky Security for Mobile (Devices) 插件从 Kaspersky Security Center Web Console 和云控制台通过向移动设备发送安装链接来安装应用程序。

- 在 Android 设备上，用户会收到用于下载 Kaspersky Endpoint Security for Android 应用程序的 Google Play 链接。可通过执行 Android 平台上的标准安装步骤，安装该应用程序。安装应用程序后，用户必须提供所需的权限。

  某些华为和荣耀设备未安装 Google 服务，因此无法访问 Google Play 中的应用程序。如果某些华为和荣耀设备用户无法从 Google Play 安装应用，应指导他们从华为应用市场安装应用。

- 在 iOS 设备上，用户会收到用于下载 Kaspersky Security for iOS 应用程序的 App Store 链接。可通过执行 iOS 平台上的标准安装步骤，安装该应用程序。

  连接 iOS 设备前，请将 Kaspersky Security Center 的地址发送给设备用户，以提高连接安全性。用户在安装应用程序时将看到该地址，如果显示的地址与您发送的地址不匹配，用户可以取消连接。

链接包含以下数据：

- Kaspersky Security Center 同步设置
- 常规证书

要在移动设备上部署应用程序：

1. 启动移动设备连接向导：

   - 在 Kaspersky Security Center Web Console 或云控制台的主窗口中，选择“**设备 > 移动 > 设备**”，然后单击“**添加**”。
   - 在 Kaspersky Security Center Web Console 或云控制台的主窗口中，选择“**用户和角色 > 用户**”。单击要向其发送连接移动设备链接的用户或用户组的名称，然后选择“**设备**”。单击“**添加移动设备**”。在这种情况下，请跳过步骤 3。

   使用“**下一步**”按钮继续向导。

2. 选择要添加的设备的操作系统：

   - **Android**
   - **iOS 和 iPadOS**

3. 选择要向其发送用于连接移动设备的链接的用户和用户组。

4. 设置要将链接发送到的电子邮件地址：

   - **所有电子邮件地址**
   - **主要电子邮件地址**

- **备用电子邮件地址**
- **其他电子邮件地址**

  如果选择此选项，请在下面指定电子邮件地址。

5. 将显示链接摘要。

   确保链接的所有参数都正确，然后单击“**发送**”。

6. 将打开一个窗口，确认已发送添加移动设备的链接。

   单击“**确定**”完成向导。

当用户安装 Kaspersky Endpoint Security for Android 应用程序或 Kaspersky Security for iOS 应用程序时，用户的设备将显示在 Web Console 或云控制台的“**设备**”>“**移动**”>“**设备**”选项卡上。在用户的移动设备上安装应用程序后，您将能够使用组策略配置设备和应用程序的设置。如果设备丢失或被盗，您还可以向移动设备发送命令（仅适用于 Android）来保护数据。

激活移动应用程序

Kaspersky Security Center 授权许可可应用于不同组的功能。为了确保 Kaspersky Endpoint Security for Android 应用程序和 Kaspersky Security for iOS 应用程序完全正常运行，组织购买的 Kaspersky Security Center 授权许可必须提供**移动设备管理**功能。**移动设备管理**功能旨在将移动设备连接到 Kaspersky Security Center 并管理它们。

有关授权 Kaspersky Security Center 和授权许可选项的详细信息：

- 如果您使用 Kaspersky Security Center Web Console，请参阅 *Kaspersky Security Center 帮助*。
- 如果您使用 Kaspersky Security Center 云控制台，请参阅 *Kaspersky Security Center 云控制台帮助*。

在移动设备上激活 Kaspersky Endpoint Security for Android 应用程序或 Kaspersky Security for iOS 应用程序是通过向该应用程序提供有效的授权许可信息来完成的。当设备与 Kaspersky Security Center 同步时，授权许可信息将与策略一起传递到移动设备。

如果在移动设备上安装移动应用程序后 30 天内未完成激活，该应用程序将自动切换至受限功能模式。在此模式中，大部分应用程序组件都无法运行。切换到受限功能模式后，该应用程序将停止执行与 Kaspersky Security Center 的自动同步。因此，如果在应用程序安装后 30 天内未完成激活，用户必须手动与 Kaspersky Security Center 同步设备。

如果您的组织中未部署 Kaspersky Security Center 或移动设备无法访问 Kaspersky Security Center，用户可以在其设备上手动激活移动应用程序。

要激活移动应用程序：

1. 打开策略属性窗口：
   - 在 Kaspersky Security Center Web Console 或云控制台的主窗口中，选择“**设备 > 策略和配置文件**”。在打开的组策略列表中，单击要配置的策略的名称。
   - 在 Kaspersky Security Center Web Console 或云控制台的主窗口中，选择“**设备 > 移动 > 设备**”。单击受到您要配置的策略影响的移动设备，然后在“**活动策略和策略配置文件**”选项卡上选择该策略。
2. 在策略属性页面中，选择“**应用程序设置 > 授权许可**”。
3. 使用下拉列表从管理服务器的密钥存储中选择所需的授权许可密钥。

   授权许可密钥的详细信息显示在下面的字段中。

如果移动设备上的现有激活密钥与上面下拉列表中选择的密钥不同，则可以将其替换。为此，请选中“**如果设备上的密钥不同，则替换为此密钥**”复选框。

4. 单击“**保存**”按钮以保存对策略所做的更改并退出策略属性窗口。

与 Kaspersky Security Center 的下次设备同步之后可配置移动设备设置。

提供 Kaspersky Endpoint Security for Android 应用程序所需的权限

Kaspersky Endpoint Security for Android 应用程序的某些功能需要权限。Kaspersky Endpoint Security for Android 会在安装期间以及安装之后和使用应用程序的各个功能之前要求必需权限。如果未提供必需权限，将无法安装 Kaspersky Endpoint Security for Android。

在某些设备（例如，华为、魅族和小米）上，您必须手动将 Kaspersky Endpoint Security for Android 添加到在操作系统启动时启动的应用程序列表中。如果未将该应用程序添加到列表，在移动设备重新启动后，Kaspersky Endpoint Security for Android 会停止执行其所有功能。

在运行 Android 11 或更高版本的设备上，必须禁用“**如果不使用应用程序则移除权限**”系统设置。否则，在几个月未使用该应用程序后，系统会自动重置用户授予该应用程序的权限。

Kaspersky Endpoint Security for Android 应用程序请求的权限

权限	应用程序功能
电话（适用于 Android 5.0–9.X）	连接到 Kaspersky Security Center（设备 ID）
存储（必需）	反病毒
管理所有文件的访问权限（适用于 Android 11 或更高版本）	反病毒
附近的蓝牙设备（适用于 Android 12 或更高版本）	限制使用蓝牙
通知（适用于 Android 13）	通知用户安全问题和应用程序事件
允许在后台运行（适用于 Android 12 或更高版本）	确保应用程序持续运行。如果未授予权限，应用程序可能会从内存中卸载并且无法重新启动。
设备管理员（必需）	反盗窃 – 锁定设备（仅适用于安卓 5.0–6.X）
	反盗窃 – 使用前置摄像头拍摄面部照片 虽然 Kaspersky Security Center Web Console 和云控制台不支持拍摄面部照片，但 Kaspersky Endpoint Security for Android 应用程序仍需要此权限，以便所有 Kaspersky Security Center 控制台都可以对其进行管理。

	反盗窃 – 发出警报声
	反盗窃 – 完全重置
	密码保护
	应用程序卸载保护
	安装安全证书
	应用程序控制
	限制使用摄像头、蓝牙和 Wi-Fi
摄像头	反盗窃 – 使用前置摄像头拍摄面部照片 虽然 Kaspersky Security Center Web Console 和云控制台不支持拍摄面部照片，但 Kaspersky Endpoint Security for Android 应用程序仍需要此权限，以便所有 Kaspersky Security Center 控制台都可以对其进行管理。 在运行 Android 11.0 或更高版本的设备上，用户必须在收到提示时授予“使用应用程序时”权限。
定位	反盗窃 – 定位设备 在运行 Android 10.0 或更高版本的设备上，用户必须在收到提示时授予“始终”权限。
可访问功能	反盗窃 – 锁定设备（仅适用于安卓 7.0 或更高版本）
	Web 保护
	应用程序控制
	应用程序卸载保护（仅适用于安卓 7.0 或更高版本）
	显示 Kaspersky Endpoint Security for Android 的警告（仅适用于 Android 10.0 或更高版本）
	限制使用摄像头（仅适用于 Android 11 或更高版本）

管理证书

移动证书用于识别管理服务器上的移动设备用户。

Kaspersky Security Center Web Console 和云控制台允许使用用户移动证书执行以下操作：

- 查看证书及其状态。
- 创建新证书。
- 续订即将到期的证书。

- 删除证书。

有关 Kaspersky Security Center 证书的更多信息：

- 如果您使用 Kaspersky Security Center Web Console，请参阅 *Kaspersky Security Center 帮助*。
- 如果您使用 Kaspersky Security Center 云控制台，请参阅 *Kaspersky Security Center 云控制台帮助*。

查看证书列表

Kaspersky Security Center Web Console 和云控制台允许查看应用的用户移动证书、它们的状态和属性。

要查看应用的用户移动证书列表：

1. 在 Kaspersky Security Center Web Console 或云控制台的主窗口中，选择“**设备 > 移动 > 设备**”。
2. 选择“**管理证书**”。

   将打开“**移动证书**”页面，其中包含有关应用的用户移动证书的信息。您可以通过在“**用户名**”列中单击证书来查看证书的详细信息。

定义证书设置

您可以使用 Kaspersky Security Center Web Console 或云控制台配置移动证书的生命周期、自动更新和密码保护。

要定义移动证书设置：

1. 在 Kaspersky Security Center Web Console 或云控制台的主窗口中，选择“**设备 > 移动 > 设备**”。
2. 选择“**管理证书**”。
3. 选择“**证书设置**”。
4. 在打开的“**生成移动证书**”窗口中，可以配置以下内容：

   - **证书有效期(天)**

     证书生命周期（天）。证书的默认生命周期为 365 天。当此周期到期时，移动设备将无法连接到管理服务器。

   - **离证书过期多少天时重新颁发**

     管理服务器应在当前证书过期前多少天颁发新证书。例如，如果该字段的值为 4，则管理服务器会在当前证书过期前四天颁发新证书。默认值为 1。

   - **如果可能，自动重新颁发证书**

     如果可能，将自动重新颁发证书。如果禁用此选项，则必须在证书到期时手动重新颁发证书。默认情况下，禁用此选项。

   - **证书安装期间提示输入密码**

     在移动设备上安装证书时，用户将被提示输入密码。在移动设备上安装证书期间，仅使用一次密码。密码将由管理服务器自动生成并通过电子邮件发送给用户。您可以在“**密码长度**”字段中指定密码长度。

5. 单击“**保存**”以应用更改并关闭窗口。

Kaspersky Security Center 将使用指定的设置来创建、更新和保护移动证书。

创建证书

您可以在 Kaspersky Security Center Web Console 和云控制台中创建移动证书，以标识移动设备的用户。

要创建移动证书：

1. 在 Kaspersky Security Center Web Console 或云控制台的主窗口中，选择“**设备 > 移动 > 设备**”。
2. 选择“**管理证书**”。
3. 在打开的“**移动证书**”窗口中，单击“**添加**”以启动“**移动证书创建向导**”。使用“**下一步**”按钮继续向导。
4. 选择要使用新证书管理其移动设备的用户或用户组。
5. 指定**发布参数**：
   - 如果要通知用户有新证书，请选中“**通知用户有新证书**”复选框。
   - 如果您希望允许在同一设备上多次使用一个证书，请选中“**允许在同一设备上多次使用一个证书(仅针对安装了 Kaspersky Endpoint Security for Android 的设备)**”复选框。
6. 选择**身份验证类型**：
   - 如果您希望用户使用其凭据访问证书，请选择“**凭据(域登录名或用户名)**”。
   - 如果您希望用户使用一次性密码访问证书，请选择“**一次性密码**”。
     如果您没有在上一步选中“**允许在同一设备上多次使用一个证书(仅针对安装了 Kaspersky Endpoint Security for Android 的设备)**”复选框，则此选项可用。
   - 如果您希望用户使用密码访问证书，请选择“**密码**”。
     如果您在上一步选中了“**允许在同一设备上多次使用一个证书(仅针对安装了 Kaspersky Endpoint Security for Android 的设备)**”复选框，则此选项可用。
7. 在“**证书传送**”字段中指定证书传送方法：
   - 如果您在上一步选择了“**一次性密码**”，请选择以下选项之一：
     - 如果您希望通过电子邮件发送密码，请选择“**通过电子邮件通知用户**”。
       然后选择要使用的电子邮件地址或选择“**其他电子邮件地址**”以指定其他电子邮件地址。
     - 如果您希望通过其他方式通知用户密码，请选择“**完成向导后显示密码**”。
   - 如果您在上一步选择了“**凭据(域登录名或用户名)**，请选择要使用的电子邮件地址或选择”**其他电子邮件地址**“以指定其他电子邮件地址。
8. 将显示证书摘要。
   确保所有参数都正确，然后单击“**创建**”。

这样，**移动证书创建向导**将创建一个证书，用户可以在其移动设备上安装该证书。当下一次移动设备与 Kaspersky Security Center 同步后，该证书可用。

有关创建证书和配置证书颁发规则的更多信息：

- 如果您使用 Kaspersky Security Center Web Console，请参阅 *Kaspersky Security Center 帮助*。
- 如果您使用 Kaspersky Security Center 云控制台，请参阅 *Kaspersky Security Center 云控制台帮助*。

续订证书

如果任何已应用的移动证书即将到期，您可以使用 Kaspersky Security Center Web Console 或云控制台进行续订。

要续订移动证书：

1. 在 Kaspersky Security Center Web Console 或云控制台的主窗口中，选择“**设备** > **移动** > **设备**”。
2. 选择“**管理证书**”。
3. 选择要续订的证书，然后单击“**重新颁发**”。

   证书状态更改为“**证书已重新颁发**”。

删除证书

您可以使用 Kaspersky Security Center Web Console 或云控制台删除移动证书。

如果删除移动证书，设备将无法再与管理服务器同步，并且无法通过 Kaspersky Security Center 进行管理。要再次开始管理移动设备，您需要在其上重新安装 Kaspersky Endpoint Security for Android 应用程序。

要删除移动证书：

1. 在 Kaspersky Security Center Web Console 或云控制台的主窗口中，选择“**设备** > **移动** > **设备**”。
2. 选择“**管理证书**”。
3. 选择要删除的证书，然后单击“**删除**”。

   证书即被删除并从证书列表中移除。

与 Firebase Cloud Messaging 交换信息

Kaspersky Endpoint Security for Android 使用 Firebase Cloud Messaging (FCM) 服务以确保向移动设备的命令传送并在策略设置被更改时强制同步。

要使用 Firebase Cloud Messaging 服务，您必须在 Kaspersky Security Center Web Console 或云控制台中配置服务设置。

要在 Kaspersky Security Center Web Console 或云控制台中启用 Firebase Cloud Messaging：

1. 在 Kaspersky Security Center Web Console 或云控制台的主窗口中，选择“**设备 > 移动 > ANDROID 设备同步**”。

   将打开“**Android 设备同步**”窗口。

2. 在“**发送方 ID**”和“**服务器密钥**”字段中，指定 Firebase Cloud Messaging 设置：SENDER_ID 和 API 密钥。

Firebase Cloud Messaging 即被启用。

要获取发件人 ID 和服务器密钥：

1. 在 Google 门户上注册。
2. 转到 Google Cloud 平台。
3. 创建一个新项目。

   等待项目创建完成。
4. 查找该项目的相关 SENDER_ID。
5. 启用 Google Firebase Cloud Messaging for Android。
6. 按照屏幕上的说明创建凭据。
7. 从新创建的凭据的属性中检索 API 密钥。

有关 Google Cloud 平台中的操作的详细信息，请参阅其文档。

您现在有**发送方 ID** 和**服务器密钥**来配置 Firebase Cloud Messaging 设置。

如果未定义 Firebase Cloud Messaging 设置，当移动设备根据策略中设置的计划（例如，每 24 小时一次）与 Kaspersky Security Center 同步时，设备上的命令和策略设置将被传送。换句话说，命令和策略设置将被延迟传送。

出于支持产品主要功能的目的，您同意自动提供 Firebase Cloud Messaging 服务应用安装的独一 ID（实例 ID）以及以下数据：

- 已安装软件的信息：应用版本、应用 ID、应用版本号、应用包名称。
- 安装了软件的计算机信息：OS 版本、设备 ID、Google 服务版本。
- FCM 信息：FCM 中应用 ID、FCM 用户 ID、协议版本。

数据通过安全连接传输到 Firebase 服务。对信息的访问和保护受 Firebase 服务的相关使用条款监管：Firebase 数据处理和安全条款、Firebase 中的隐私和安全。

阻止与 Firebase Cloud Messaging 服务交换信息：

1. 在 Kaspersky Security Center Web Console 或云控制台的主窗口中，选择“**设备 > 移动 > ANDROID 设备同步**”。

   将打开“**Android 设备同步**”窗口。
2. 单击“**重置**”。

3. 在打开的窗口中，单击“**确定**”按钮以确认重置。

Firebase Cloud Messaging 设置即被清除。

在 Kaspersky Security Center Web Console 和云控制台中管理移动设备

您可以在 Kaspersky Security Center Web Console 和云控制台中通过使用组策略和向移动设备发送命令（仅适用于 Android）来管理移动设备。

要在 Kaspersky Security Center Web Console 中管理移动设备，必须安装管理插件。

将移动设备连接到 Kaspersky Security Center

要使用 Kaspersky Security Center Web Console 或云控制台管理移动设备，设备必须连接到 Kaspersky Security Center。您可以在 Web Console 或云控制台的“**设备 > 移动 > 设备**”选项卡上查看连接到 Kaspersky Security Center 的移动设备列表。

连接 iOS 设备前，请将 Kaspersky Security Center 的地址发送给设备用户，以提高连接安全性。用户在安装应用程序时将看到该地址，如果显示的地址与您发送的地址不匹配，用户可以取消连接。

要将移动设备连接到 Kaspersky Security Center：

1. 启动移动设备连接向导：

   - 在 Kaspersky Security Center Web Console 或云控制台的主窗口中，选择“**设备 > 移动 > 设备**”，然后单击“**添加**”。
   - 在 Kaspersky Security Center Web Console 或云控制台的主窗口中，选择“**用户和角色 > 用户**”。单击要向其发送连接移动设备链接的用户或用户组的名称，然后选择“**设备**”。单击“**添加移动设备**”。在这种情况下，请跳过步骤 3。

   使用“**下一步**”按钮继续向导。

2. 选择要添加的设备的操作系统：

   - **Android**
   - **iOS 和 iPadOS**

3. 选择要向其发送用于连接移动设备的链接的用户和用户组。

4. 设置要将链接发送到的电子邮件地址：

   - **所有电子邮件地址**
   - **主要电子邮件地址**
   - **备用电子邮件地址**

- **其他电子邮件地址**

  如果选择此选项，请在下面指定电子邮件地址。

5. 将显示链接摘要。

   确保链接的所有参数都正确，然后单击“**发送**”。

6. 将打开一个窗口，确认已发送添加移动设备的链接。

   单击“**确定**”完成向导。

当用户安装 Kaspersky Endpoint Security for Android 应用程序或 Kaspersky Security for iOS 应用程序时，用户的设备将显示在 Web Console 或云控制台的“**设备 > 移动 > 设备**”选项卡上。

将未分配的移动设备移至管理组

在移动设备上安装 Kaspersky Endpoint Security for Android 应用程序或 Kaspersky Security for iOS 应用程序后，这些设备会显示在 Kaspersky Security Center Web Console 或云控制台的“**发现和部署 > 未分配的设备**”页面上。要管理新连接的设备，可以创建自动将它们分配到管理组的规则或手动将它们移至管理组。

要将未分配的移动设备移至管理组：

1. 在 Kaspersky Security Center Web Console 或云控制台的主窗口中，选择“**发现和部署 > 未分配的设备**”。

2. 选择要移至管理组的设备，然后单击“**移至组**”。

3. 在打开的管理组树中，选择要将设备移至的目标组。

   您可以通过选择现有组，然后单击“**添加子组**”来创建新的管理组。

4. 单击“**移动**”。

设备将移至指定的管理组并被应用组策略。

向移动设备发送命令

您可以向 Android 移动设备发送命令来保护丢失或被盗的移动设备上的数据，或者执行移动设备与 Kaspersky Security Center 的强制同步。

> 您不能向 iOS 设备发送命令。

支持以下命令：

- **锁定设备**

  移动设备将锁定。

- **解锁设备**

  移动设备将解锁。解锁运行着 Android 5.0 – 6.X 的移动设备后，屏幕解锁密码 (PIN code) 重置为“1234”。解锁运行着 Android 7.0 或更新版本的设备后，屏幕解锁密码不变。

- **重置为出厂设置**

  所有数据都将从移动设备中删除，并且设置将回滚至默认值。

- **擦除企业数据**

  容器化数据和公司电子邮件账户将从移动设备中擦除。

- **定位设备**

  设备将被定位并显示在 Google Maps 中。移动服务提供商可能会收取互联网访问费用。

  > 在运行 Android 12 或更高版本的设备上，如果用户授予了“使用大致位置”权限，Kaspersky Endpoint Security for Android 应用程序首先会尝试获取精确的设备位置。如果获取不成功，则只有在不超过 30 分钟前已收到设备的大致位置时，才会返回该位置。否则，“**定位设备**”命令将失败。

- **发出警报**

  移动设备发出警报。警报响 5 分钟（如果设备的电池电量低，则响 1 分钟）。

- **同步设备**

  移动设备与 Kaspersky Security Center 同步。

Kaspersky Endpoint Security for Android 应用程序需要特定权限才能执行命令。当初始配置向导正在运行时，Kaspersky Endpoint Security for Android 会提示用户授予应用程序所有必需的权限。用户可以跳过这些步骤或以后在设备设置中禁用这些权限。如果是这种情况，将不可能执行命令。

> 在运行 Android 10.0 或更高版本的设备上，用户必须授予“始终”权限才能访问位置。在运行 Android 11.0 或更高版本的设备上，用户必须授予“使用应用程序时”权限才能访问摄像头。否则，反盗窃命令将不起作用。用户将被通知这一限制，并再次被提示授予所需级别的权限。如果用户为摄像头权限选择“仅此一次”选项，则认为应用程序授予了访问权限。如果再次请求摄像头权限，建议直接联系用户。

要向移动设备发送命令：

1. 在 Kaspersky Security Center Web Console 或云控制台的主窗口中，选择“**设备 > 移动 > 设备**”。
2. 选择要向其发送命令的设备，然后单击“**控制**”或“**管理**”。
3. 在“**可用命令**”列表中选择所需命令，然后单击“**确定**”。
4. 如果系统提示您确认操作，请单击“**确定**”。

   指定的命令即发送到移动设备并显示确认窗口。

从 Kaspersky Security Center 移除移动设备

如果您不再需要管理移动设备，可以使用 Web Console 或云控制台将其从 Kaspersky Security Center 中移除。

要从 Kaspersky Security Center 中移除移动设备：

1. 从设备中删除移动应用程序，或确保用户已从所需设备中删除应用程序。
2. 在 Kaspersky Security Center Web Console 或云控制台的主窗口中，选择“**设备 > 移动 > 设备**”。
3. 选择要移除的移动设备，然后单击“**删除**”。
4. 单击“**确定**”确认操作。

该设备即从 Kaspersky Security Center 中移除。

管理组策略

本节介绍如何在 Kaspersky Security Center Web Console 和云控制台中管理组策略。

用于管理移动设备的组策略

组策略 是用于管理属于管理组的移动设备和管理设备上安装的移动应用程序的设置包。

您可以使用策略配置单个设备和设备组的设置。对于一组设备，可在组策略属性窗口中配置管理设置。

策略中的每个参数都有"锁"属性，该"锁定"显示是否允许在嵌套层次结构级别（对嵌套组和辅助管理服务器而言）、任务设置和本地应用程序设置修改策略。

在本地应用程序中和策略中配置的设置值将保存在管理服务器上，在同步期间分发至移动设备并将其作为当前值保存在设备中。如果用户指定了未被"锁定"的其他设置值，在设备与管理服务器下次同步期间，设置新值将被传递给管理服务器，并保存在应用程序本地设置中，而不是先前由管理员指定的值。

为了使 Android 移动设备的公司安全保护保持最新，您可以监控用户的设备是否符合公司安全要求。

有关在 Kaspersky Security Center Web Console 和云控制台中管理策略和管理组的更多详细信息：

- 如果您使用 Kaspersky Security Center Web Console，请参阅 *Kaspersky Security Center 帮助*。
- 如果您使用 Kaspersky Security Center 云控制台，请参阅 *Kaspersky Security Center 云控制台帮助*。

查看组策略列表

Kaspersky Security Center Web Console 和云控制台允许您查看组策略、它们的状态和属性。

要查看组策略列表，

在 Kaspersky Security Center Web Console 或云控制台的主窗口中，选择"**设备 > 策略和配置文件**"。

将打开组策略列表，其中包含有关组策略的简要信息。在此页面上，您可以创建、修改、复制、移动和删除组策略。

查看策略分发结果

Kaspersky Security Center Web Console 和云控制台允许您查看组策略的分布图以及受该策略影响的所有设备的信息。

要查看组策略的分发结果：

1. 在 Kaspersky Security Center Web Console 或云控制台的主窗口中，选择"**设备 > 策略和配置文件**"。

2. 在打开的组策略列表中，选中要查看其分发结果的策略名称旁边的复选框，然后单击“**分发**”。

将打开策略分发结果页面。此页面包含策略摘要、策略分布图表以及包含受该策略影响的所有设备的信息的表格。您可以单击“**配置策略**”按钮来打开策略属性窗口。

创建组策略

Kaspersky Security Center Web Console 和云控制台允许您创建组策略以管理移动设备。

要创建组策略：

1. 在 Kaspersky Security Center Web Console 或云控制台的主窗口中，选择“**设备 > 策略和配置文件**”。
2. 在打开的 Kaspersky Security Center 组策略列表中，单击“**当前路径**”以选择要为其创建策略的管理组。
   默认情况下，新的组策略应用于“**受管理设备**”组。
3. 单击“**添加**”以启动策略创建向导。使用“**下一步**”按钮继续向导。
4. 根据平台选择应用程序：
   - **Kaspersky Endpoint Security for Android**
   - **Kaspersky Security for iOS**
5. 在“**名称**”字段中输入新策略的名称。如果您指定了现有策略的名称，它将在最后自动添加 (1)。
6. 选择策略状态：
   - 活动
     向导将在管理服务器上保存已创建的策略。在移动设备下次与管理服务器同步时，该策略将在设备上用作活动策略。
   - 不活动
     向导将在管理服务器上以备份策略的方式保存已创建的策略。在后续某个特殊事件之后该策略将被激活。如有必要可将不活动的策略切换为活动状态。

     可以为组中一个应用程序创建若干个策略，但是只能激活它们中的一个策略。当创建新的活动策略时，先前的活动策略将自动变为不活动状态。
7. 您可以启用或禁用两个继承选项，“**从父策略继承设置**”和“**强制继承子策略中的设置**”：
   - 如果为子管理组启用“**从父策略继承设置**”并锁定父策略中的某些设置，则无法在子组的策略中更改这些设置。但是，您可以更改父策略中未锁定的设置。
   - 如果为子管理组禁用“**从父策略继承设置**”，则可以更改子组中的所有设置，即使某些设置在父策略中被锁定。
   - 如果在父管理组中启用“**强制继承子策略中的设置**”，这将为每个子策略启用“**从父策略继承设置**”选项。在这种情况下，不能为任何子策略禁用此选项。父策略中锁定的所有设置都在子组中强制继承，并且您不能在子组中更改这些设置。

- 在“**受管理设备**”组的策略中，“**从父策略继承设置**”选项不会影响任何设置，因为“**受管理设备**”组没有任何上游组，因此不会继承任何策略。

默认情况下，启用“**从父策略继承设置**”选项，禁用“**强制继承子策略中的设置**”选项。

8. 如果需要，您可以定义新创建的策略的设置。为此，请选择“**应用程序设置**”选项卡，然后按照“定义策略设置”部分中所述进行操作。

   或者，您可以稍后执行该操作。

9. 单击“**保存**”以创建策略。

一个新的用于管理移动设备的组策略即被创建。

修改组策略

Kaspersky Security Center Web Console 和云控制台允许您修改组策略的设置。

要修改组策略：

1. 打开策略属性窗口：

   - 在 Kaspersky Security Center Web Console 或云控制台的主窗口中，选择“**设备 > 策略和配置文件**”。在打开的组策略列表中，单击要配置的策略的名称。
   - 在 Kaspersky Security Center Web Console 或云控制台的主窗口中，选择“**设备 > 移动 > 设备**”。单击受到您要配置的策略影响的移动设备，然后在“**活动策略和策略配置文件**”选项卡上选择该策略。

2. 在策略属性窗口中，选择“**应用程序设置**”，然后按照“定义策略设置”部分中所述定义策略设置。

   > 您还可以配置常规设置、设置继承、事件记录和通知、策略配置文件以及查看修订历史记录。有关详细信息，请参阅 *Kaspersky Security Center 帮助*。

3. 单击“**保存**”按钮以保存对策略所做的更改并退出策略属性窗口。

与 Kaspersky Security Center 的下次设备同步之后可配置移动设备设置。

复制组策略

Kaspersky Security Center Web Console 和云控制台允许您创建组策略的副本。

要创建组策略的副本：

1. 在 Kaspersky Security Center Web Console 或云控制台的主窗口中，选择“**设备 > 策略和配置文件**”。
2. 在打开的组策略列表中，选中要为其创建副本的策略名称旁边的复选框，然后单击“**复制**”。
3. 在打开的管理组树中，选择要在其中创建策略副本的目标组。

   您可以通过选择现有组，然后单击“**添加子组**”来创建新的管理组。

4. 单击“**复制**”。

5. 单击“**确定**”确认操作。

将在目标组中以相同名称创建策略副本。目标组中每个复制或移动的策略的状态都将为“**不活动**”。您可以随时将状态更改为“**活动**”。

如果目标组中已经存在与新创建或移动的策略具有相同名称的策略，则在新创建或移动的策略的名称中添加 (<下一个序号>) 索引，例如：(1)。

将策略移动到另一个管理组

Kaspersky Security Center Web Console 和云控制台允许您将策略移动到其他管理组。

要将策略移动到另一个管理组：

1. 在 Kaspersky Security Center Web Console 或云控制台的主窗口中，选择“**设备 > 策略和配置文件**”。

2. 在打开的组策略列表中，选中要移动到其他管理组的策略名称旁边的复选框，然后单击“**移动**” 。

3. 在打开的管理组树中，选择要将策略移至的目标组。
   您可以通过选择现有组，然后单击“**添加子组**”来创建新的管理组。

4. 单击“**移动**”。

5. 单击“**确定**”确认操作。

结果取决于策略继承属性：

- 如果源组中未继承该策略，该策略将被移至目标组。
- 如果源组中继承了该策略，则不会移动该策略。而是在目标组中创建该策略的副本。

目标组中每个复制或移动的策略的状态都将为“**不活动**”。您可以随时将状态更改为“**活动**”。

如果目标组中已经存在与新创建或移动的策略具有相同名称的策略，则在新创建或移动的策略的名称中添加 (<下一个序号>) 索引，例如：(1)。

删除组策略

Kaspersky Security Center Web Console 和云控制台允许您删除组策略。

> 您只能删除当前管理组中未继承的策略。如果某个策略被继承，则只能在创建它的上级组中将其删除。

要删除组策略：

1. 在 Kaspersky Security Center Web Console 或云控制台的主窗口中，选择“**设备 > 策略和配置文件**”。

2. 在打开的组策略列表中，选中要删除的策略名称旁边的复选框，然后单击“**删除**”。

3. 单击“**确定**”确认操作。

组策略将被删除。

定义策略设置

本节介绍如何定义 Kaspersky Security Center 策略的设置以管理移动设备。

您可以在创建或修改策略时定义策略设置。

配置反病毒保护

> 您只能为 Android 设备定义这些策略设置。

为了及时检测威胁、病毒和其他恶意应用程序，您应配置实时防护和病毒扫描自动运行。

Kaspersky Endpoint Security for Android 可检测以下类型的对象：

- 病毒、蠕虫、木马和恶意工具。
- 广告软件。
- 检测可被犯罪分子入侵以损害您的设备或个人数据的应用程序。

> 由于技术限制，Kaspersky Endpoint Security for Android 无法扫描大小为 2 GB 或更大的文件。在扫描期间，应用程序将跳过大文件，并且不会通知您此类文件被跳过。

配置实时保护

> 您只能为 Android 设备定义这些策略设置。

要配置实时保护：

1. 打开策略属性窗口：
   - 在 Kaspersky Security Center Web Console 或云控制台的主窗口中，选择“**设备 > 策略和配置文件**”。在打开的组策略列表中，单击要配置的策略的名称。
   - 在 Kaspersky Security Center Web Console 或云控制台的主窗口中，选择“**设备 > 移动 > 设备**”。单击受到您要配置的策略影响的移动设备，然后在“**活动策略和策略配置文件**”选项卡上选择该策略。
2. 在策略属性窗口中，选择“**应用程序设置 > 基本保护**”。

3. 在“**反病毒**”区域中，配置移动设备文件系统保护：

- 要启用对移动设备的实时保护以抵御威胁，请选中“**启用实时反病毒保护**”复选框。
- 指定保护级别：
  - 如果您希望 Kaspersky Endpoint Security for Android 仅扫描“下载”文件夹中的新应用程序和文件，请选择“**仅扫描新应用程序**”。
  - 要启用对移动设备的扩展保护以抵御威胁，请选择“**扫描所有应用程序，监测文件操作**”。

    Kaspersky Endpoint Security for Android 将扫描用户在设备上打开、修改、移动、复制、安装或保存的所有文件，以及新安装的移动应用程序。

    在运行 Android 8.0 或更高版本的设备上，Kaspersky Endpoint Security for Android 将扫描用户修改、移动、安装和保存的文件，以及文件副本。在打开文件或复制源文件时，Kaspersky Endpoint Security for Android 不会进行扫描。
- 要在用户设备上首次启动新应用程序之前使用卡巴斯基安全网络云服务对其进行附加扫描，请选中“**卡巴斯基安全网络提供的其他保护**”复选框。
- 要阻止可被犯罪分子利用来损害设备或用户数据的广告软件和应用程序，请选中“**检测可能被网络犯罪分子利用以对用户的设备和数据造成损害的广告软件、自动拨号软件和应用程序**”复选框。

4. 在“**反病毒设置**”区域中，选择在检测到威胁时执行的操作：

- **删除文件并在隔离区保存文件的备份副本**

  检测到的对象将被自动删除。不要求用户做任何其他操作。在删除对象之前，Kaspersky Endpoint Security for Android 将创建文件的备份副本并将其保存在隔离区中。
- **删除**

  检测到的对象将被自动删除。不要求用户做任何其他操作。删除对象之前，Kaspersky Endpoint Security for Android 将显示检测到对象的临时通知。
- **跳过**

  如果检测到的对象被跳过，Kaspersky Endpoint Security for Android 会警告用户设备保护方面存在问题。有关跳过的对象的信息会显示在应用程序的“**状态**”部分中。对于每个跳过的威胁，应用程序都提供用户可以执行以消除威胁的操作。跳过的威胁列表可能会更改，例如，如果可疑文件被删除或移动。若要接收最新的威胁列表，请运行完整设备扫描。为了确保可靠地保护您的数据，请消除所有检测到的对象。

5. 单击“**保存**”按钮以保存对策略所做的更改并退出策略属性窗口。

与 Kaspersky Security Center 的下次设备同步之后可配置移动设备设置。

配置移动设备上的病毒扫描自动运行

您只能为 Android 设备定义这些策略设置。

要配置移动设备上的病毒扫描自动运行：

1. 打开策略属性窗口：

   - 在 Kaspersky Security Center Web Console 或云控制台的主窗口中，选择“**设备 > 策略和配置文件**”。在打开的组策略列表中，单击要配置的策略的名称。

   - 在 Kaspersky Security Center Web Console 或云控制台的主窗口中，选择“**设备 > 移动 > 设备**”。单击受到您要配置的策略影响的移动设备，然后在“**活动策略和策略配置文件**”选项卡上选择该策略。

2. 在策略属性窗口中，选择“**应用程序设置 > 基本保护**”。

3. 要阻止可被犯罪分子利用来损害设备或用户数据的广告软件和应用程序，请选中“**设备扫描**”区域中的“**检测可能被网络犯罪分子利用以对用户的设备和数据造成损害的广告软件、自动拨号软件和应用程序**”复选框。

4. 在“**检测到威胁时执行的操作**”列表中，选择以下选项之一：

   - **删除文件并在隔离区保存文件的备份副本**

     检测到的对象将被自动删除。不要求用户做任何其他操作。在删除对象之前，Kaspersky Endpoint Security for Android 将创建文件的备份副本并将其保存在隔离区中。

   - **删除**

     检测到的对象将被自动删除。不要求用户做任何其他操作。删除对象之前，Kaspersky Endpoint Security for Android 将显示检测到对象的临时通知。

   - **跳过**

     如果检测到的对象被跳过，Kaspersky Endpoint Security for Android 会警告用户设备保护方面存在问题。有关跳过的对象的信息会显示在应用程序的“**状态**”部分中。对于每个跳过的威胁，应用程序都提供用户可以执行以消除威胁的操作。跳过的威胁列表可能会更改，例如，如果可疑文件被删除或移动。若要接收最新的威胁列表，请运行完整设备扫描。为了确保可靠地保护您的数据，请消除所有检测到的对象。

   - **询问用户**

     Kaspersky Endpoint Security for Android 应用程序将显示一条通知，提示用户选择要对检测到的对象采取的操作：“**跳过**”或“**删除**”。

     当应用程序检测到多个对象时，“**询问用户**”选项允许设备用户通过使用“**应用到所有威胁**”复选框将所选操作应用于每个文件。

     必须将 Kaspersky Endpoint Security for Android 设置为辅助功能，以确保在运行安卓 10.0 或更高版本的移动设备上显示通知。Kaspersky Endpoint Security for Android 会提示用户通过初始配置向导将该应用程序设置为可访问功能。用户可以跳过此步骤或以后在设备设置中禁用此服务。在这种情况下，Kaspersky Endpoint Security for Android 将显示一个 Android 系统窗口，提示用户选择要对检测到的对象采取的操作：“跳过”或“删除”。要对多个对象应用操作，您需要打开 Kaspersky Endpoint Security。

5. 在“**计划扫描**”区域中，可以配置对设备文件系统的自动全盘扫描。

   选择以下选项之一：

   - **已禁用**

     设备文件系统的扫描不会自动启动。

- **数据库更新后**

  每次更新反病毒数据库后自动扫描设备文件系统。

- **每天**

  每天自动扫描设备文件系统。

  如果选择此选项，还可以在“**开始时间**”字段中指定扫描时间。

- **每周**

  每周自动扫描一次设备文件系统。

  如果选择此选项，还可以使用下拉列表选择要在星期几运行扫描，并在“**开始时间**”字段中指定扫描时间。

> 在 Android 12 或更高版本上，如果设备处于省电模式，应用程序可能会晚于指定的时间执行此任务。

6. 单击“**保存**”按钮以保存对策略所做的更改并退出策略属性窗口。

与 Kaspersky Security Center 的下次设备同步之后可配置移动设备设置。

配置反病毒数据库更新

> 您只能为 Android 设备定义这些策略设置。

要配置反病毒数据库更新：

1. 打开策略属性窗口：

   - 在 Kaspersky Security Center Web Console 或云控制台的主窗口中，选择“**设备 > 策略和配置文件**”。在打开的组策略列表中，单击要配置的策略的名称。

   - 在 Kaspersky Security Center Web Console 或云控制台的主窗口中，选择“**设备 > 移动 > 设备**”。单击受到您要配置的策略影响的移动设备，然后在“**活动策略和策略配置文件**”选项卡上选择该策略。

2. 在策略属性窗口中，选择“**应用程序设置 > 数据库更新**”。

3. 在“**数据库更新**”区域中，配置用户设备上的数据库自动更新计划。

   选择以下选项之一：

   - **已禁用**

     反病毒数据库的自动更新将被禁用。

   - **每天**

     反病毒数据库将每天更新。

     如果选择此选项，还可以在“**更新时间**”字段中指定更新时间。

   - **每周**

     反病毒数据库每周更新一次。

如果选择此选项，还可以在“**更新时间**”字段中指定更新时间，并在“**周几**”下拉列表中指定要在星期几运行更新。

在 Android 12 或更高版本上，如果设备处于省电模式，应用程序可能会晚于指定的时间执行此任务。

4. 在“**数据库更新源**”区域中，指定 Kaspersky Endpoint Security for Android 接收并安装反病毒数据库更新所需的更新源：

   - **Kaspersky 服务器**

     Kaspersky Endpoint Security for Android 将使用 Kaspersky 更新服务器作为更新源，以将反病毒数据库下载到用户设备。

   - **管理服务器**

     仅当使用 Kaspersky Security Center Web Console 时可用。

     Kaspersky Endpoint Security for Android 将使用 Kaspersky Security Center 管理服务器的存储库作为更新源，以将反病毒数据库下载到用户设备。

   - **其他更新源**

     Kaspersky Endpoint Security for Android 将使用第三方服务器作为更新源，以将反病毒数据库下载到用户设备。

     如果选择此选项，则必须在“**使用另一台服务器作为反病毒数据库的更新源**”字段中指定 HTTP 服务器的地址。

5. 如果您希望 Kaspersky Endpoint Security for Android 在用户的设备漫游时按照更新计划下载反病毒数据库更新，请在“**漫游时升级反病毒数据库**”区域中选中“**允许漫游时数据库更新**”复选框。

6. 单击“**保存**”按钮以保存对策略所做的更改并退出策略属性窗口。

与 Kaspersky Security Center 的下次设备同步之后可配置移动设备设置。

定义设备解锁设置

您只能为 Android 设备定义这些策略设置。

为确保移动设备安全，您需要配置使用密码，在设备从睡眠模式唤醒时提示用户输入密码。

如果解锁密码太弱，您可以对设备上的用户活动施加限制（例如锁定设备）。您可以使用“合规性控制”组件施加限制。

在某些运行 Android 7.0 或更高版本的三星设备上，当用户尝试配置不受支持的方法（例如，图形密码）来解锁设备时，如果满足以下条件，设备可能会锁定：Kaspersky Endpoint Security for Android 卸载保护已启用并且设置了屏幕解锁密码长度要求。要解锁设备，您必须发送特殊命令到设备。

要配置设备解锁密码强度：

1. 打开策略属性窗口：

- 在 Kaspersky Security Center Web Console 或云控制台的主窗口中，选择“**设备 > 策略和配置文件**”。在打开的组策略列表中，单击要配置的策略的名称。
- 在 Kaspersky Security Center Web Console 或云控制台的主窗口中，选择“**设备 > 移动 > 设备**”。单击受到您要配置的策略影响的移动设备，然后在“**活动策略和策略配置文件**”选项卡上选择该策略。

2. 在策略属性窗口中，选择“**应用程序设置 > 基本保护**”。
3. 如果您希望应用程序检查是否设置了解锁密码，请在“**密码保护**”区域中选中“**需要设置屏幕解锁密码**”。

   如果应用程序检测到设备上未设置任何系统密码，则提示用户进行设置。密码根据管理员定义的参数来设置。
4. 指定用户密码的最小字符数。

   可能值：4 到 16 个字符。

   默认情况下，用户的密码包含 4 个字符。

   在运行 Android 10.0 或更高版本的设备上，Kaspersky Endpoint Security 将密码强度要求解析为系统值之一：中或高。

   运行 Android 10.0 或更高版本的设备的值通过以下规则确定：

   - 如果所需的密码长度是 1 到 4 个符号，该应用程序会提示用户设置中等强度的密码。它必须是没有重复并且没有顺序（例如 1234）的数字 (PIN)，或者是字母数字。PIN 或密码必须至少有 4 个字符长。
   - 如果所需的密码长度是 5 个或更多符号，该应用程序会提示用户设置高强度密码。它必须是没有重复并且没有顺序的数字 (PIN)，或者是字母数字（密码）。PIN 必须至少为 8 位数字；密码必须至少有 6 个字符长。
5. 如果您希望用户能够使用指纹解锁屏幕，请选中“**允许使用指纹(针对运行 Android 9 或更早版本的设备)**”复选框。如果解锁密码不符合公司安全要求，则无法使用指纹扫描器解锁屏幕。

   在运行 Android 10.0 或更高版本的设备上，不支持使用指纹解锁屏幕。

   Kaspersky Endpoint Security for Android 不会限制使用指纹扫描器来登录应用程序或确认购买。

   在某些三星设备上，无法阻止使用指纹解锁屏幕。

   在某些三星设备上，如果解锁密码不符合企业安全要求，Kaspersky Endpoint Security for Android 不会阻止使用指纹解锁屏幕。

   在设备设置中添加指纹后，用户可以使用以下方法解锁屏幕：

   - 将手指按在指纹扫描器上（主要方法）。
   - 输入解锁密码（备用方法）。
6. 单击“**保存**”按钮以保存对策略所做的更改并退出策略属性窗口。

与 Kaspersky Security Center 的下次设备同步之后可配置移动设备设置。

配置对被盗或丢失设备的数据的保护

您只能为 Android 设备定义这些策略设置。

要在移动设备丢失或被盗时保护公司数据，您必须配置非授权访问保护。

为确保对被盗或丢失设备的数据的保护，必须将 Kaspersky Endpoint Security for Android 设置为辅助功能。Kaspersky Endpoint Security for Android 会提示用户通过初始配置向导将该应用程序设置为可访问功能。用户可以跳过此步骤或以后在设备设置中禁用此服务。

要配置对被盗或丢失设备的数据的保护：

1. 打开策略属性窗口：
   - 在 Kaspersky Security Center Web Console 或云控制台的主窗口中，选择“**设备 > 策略和配置文件**”。在打开的组策略列表中，单击要配置的策略的名称。
   - 在 Kaspersky Security Center Web Console 或云控制台的主窗口中，选择“**设备 > 移动 > 设备**”。单击受到您要配置的策略影响的移动设备，然后在“**活动策略和策略配置文件**”选项卡上选择该策略。
2. 在策略属性窗口中，选择“**应用程序设置 > 基本保护**”。
3. 在“**反盗窃**”区域中，配置设备锁定：
   - 指定解锁代码中的字符数。
   - 指定设备锁定时将显示的文本。
4. 单击“**保存**”按钮以保存对策略所做的更改并退出策略属性窗口。

与 Kaspersky Security Center 的下次设备同步之后可配置移动设备设置。

配置应用程序控制

您只能为 Android 设备定义这些策略设置。

*应用程序控制*会检查移动设备上安装的应用程序是否符合公司安全要求。在 Kaspersky Security Center，管理员根据公司安全要求创建允许、阻止、强制和推荐的应用程序的列表。作为应用程序控制的结果，Kaspersky Endpoint Security 会提示用户安装必需和推荐的应用程序以及删除被阻止的应用程序。无法在用户的移动设备上启动被阻止的应用程序。

在 Kaspersky Security Center Web Console 和云控制台中，可以通过应用预定义的规则来管理用户设备上的应用程序。您可以配置两种类型的**应用程序控制**规则：应用程序规则和类别规则。

应用规则适用于特定应用程序，而**类别规则**适用于属于某个预定义类别的任何应用程序。应用程序类别由 Kaspersky 专家指定。

要配置应用程序控制：

1. 打开策略属性窗口：

   - 在 Kaspersky Security Center Web Console 或云控制台的主窗口中，选择“**设备 > 策略和配置文件**”。在打开的组策略列表中，单击要配置的策略的名称。

   - 在 Kaspersky Security Center Web Console 或云控制台的主窗口中，选择“**设备 > 移动 > 设备**”。单击受到您要配置的策略影响的移动设备，然后在“**活动策略和策略配置文件**”选项卡上选择该策略。

2. 在策略属性页面中，选择“**应用程序设置 > 安全控制**”。

3. 在“**应用程序控制**”区域下的表中，添加将定义哪些应用程序将受控制的规则。

   - 要添加适用于为特定应用程序的规则：

     a. 在表中，单击“**应用规则**”。

     b. 在打开的“**应用规则**”窗口中，选择将对所创建的规则覆盖的应用程序执行的操作。

     c. 通过填写“**安装包的链接(比如 https://play.google.com/store/apps/details?id=com.kaspersky.kes)**”、“**安装包名称(比如 katana.facebook.com)**”和“**应用程序名称**”来指定将受规则约束的应用程序。

     d. 单击“**保存**”。

     该规则将添加到**应用程序控制**规则列表中。

   - 要添加适用于应用程序类别的规则：

     a. 在“**应用程序控制**”区域下的表中，单击“**类别规则**”。

     b. 在打开的“**类别规则**”窗口中，从下拉列表中选择应用程序类别。

     所选类别中的应用程序将受所创建的规则约束。

     c. 在“**运行模式**”区域中，选择当所选类别中的任何应用程序试图启动时将执行的操作：“**禁止的应用程序**”或“**允许的应用程序**”。

     d. 如有必要，填写“**检测到指定类别的应用程序时，在用户设备上显示的附加注释**”。

     e. 单击“**保存**”。

     该规则将添加到**应用程序控制**规则列表中。

4. 在“**对已禁止的应用程序执行的操作**”区域中，选择对已禁用的应用程序执行的操作：

   - 如果您希望 Kaspersky Endpoint Security for Android 阻止在用户的移动设备上启动已禁止的应用程序，请选择“**阻止应用程序启动**”。

   - 如果您希望 Kaspersky Endpoint Security for Android 将有关禁止的应用程序的数据发送到事件日志而不进行阻止，则选中“**不阻止已禁止的应用程序，仅报告**”。

5. 在“**运行模式**”区域中，选择您添加的规则将定义允许的应用程序还是禁止的应用程序：

- 如果您希望规则定义允许哪些应用程序，请选择“**禁止的应用程序**”。

  如果您希望 Kaspersky Endpoint Security for Android 在“**禁止的应用程序**”模式下阻止用户移动设备上的系统应用程序（例如日历、相机和设置）启动，请选中“**阻止系统应用程序**”复选框。

  > Kaspersky 专家建议不要阻止系统应用程序，因为这会导致设备操作故障。

- 如果您希望规则定义禁止哪些应用程序，请选择“**允许的应用程序**”。

6. 要接收有关移动设备上安装的所有应用程序的信息，请在“**应用程序报告**”区域中选中“**发送所有移动设备上已安装应用程序的列表**”复选框。

   Kaspersky Endpoint Security for Android 在每次应用被安装或从设备卸载时发送数据到事件日志。

7. 单击“**保存**”按钮以保存对策略所做的更改并退出策略属性窗口。

与 Kaspersky Security Center 的下次设备同步之后可配置移动设备设置。

配置使移动设备符合公司安全要求的合规性控制

> 您只能为 Android 设备定义这些策略设置。

合规性控制允许您监控 Android 设备是否符合公司安全要求，并在不合规的情况下采取措施。公司安全要求规范用户可以如何使用设备。例如，必须在设备上启用实时保护，反病毒数据库必须是最新的，并且设备密码必须足够强。合规性控制基于规则列表。合规性规则包括以下组成部分：

- 设备不合规标准。
- 如果用户未在规定的时间段内解决不合规问题，将对设备采取的措施。
- 分配给用户以解决不合规问题的时间段（例如，24 小时）。

  当指定的时间段结束后，将在用户的设备上执行选定操作。

  > 在 Android 12 或更高版本上，如果设备处于省电模式，应用程序可能会晚于指定的时间执行此任务。

要配置合规性控制，可以执行以下操作：

- 启用或禁用现有合规性规则。
- 编辑现有合规性规则。
- 添加新规则。
- 删除规则。

启用和禁用合规性规则

您只能为 Android 设备定义这些策略设置。

要启用或禁用使移动设备符合公司安全要求的合规性控制的现有规则：

1. 打开策略属性窗口：
   - 在 Kaspersky Security Center Web Console 或云控制台的主窗口中，选择“**设备 > 策略和配置文件**”。在打开的组策略列表中，单击要配置的策略的名称。
   - 在 Kaspersky Security Center Web Console 或云控制台的主窗口中，选择“**设备 > 移动 > 设备**”。单击受到您要配置的策略影响的移动设备，然后在“**活动策略和策略配置文件**”选项卡上选择该策略。
2. 在策略属性页面中，选择“**应用程序设置 > 安全控制**”。
3. 在“**合规性控制**”区域中，使用“**状态**”列中的切换按钮启用或禁用现有的合规性规则。
4. 单击“**保存**”按钮以保存对策略所做的更改并退出策略属性窗口。

与 Kaspersky Security Center 的下次设备同步之后可配置移动设备设置。

编辑合规性规则

您只能为 Android 设备定义这些策略设置。

要编辑用于控制移动设备符合公司安全要求的规则：

1. 打开策略属性窗口：
   - 在 Kaspersky Security Center Web Console 或云控制台的主窗口中，选择“**设备 > 策略和配置文件**”。在打开的组策略列表中，单击要配置的策略的名称。
   - 在 Kaspersky Security Center Web Console 或云控制台的主窗口中，选择“**设备 > 移动 > 设备**”。单击受到您要配置的策略影响的移动设备，然后在“**活动策略和策略配置文件**”选项卡上选择该策略。
2. 在策略属性页面中，选择“**应用程序设置 > 安全控制**”。
3. 在“**合规性控制**”区域中，选择要编辑的规则，然后单击“**编辑**”。
4. 在打开的“**规则**”窗口中，按如下方式编辑规则：
   a. 在“**操作**”列中，通过添加新操作、编辑现有操作或删除操作来配置不合规时执行的操作列表。
   b. （可选）使用每个操作的“**纠正时间**”列指定用户可以解决不合规问题的时间段。
   c. 单击“**保存**”按钮保存规则。
5. 单击“**保存**”按钮以保存对策略所做的更改并退出策略属性窗口。

与 Kaspersky Security Center 的下次设备同步之后可配置移动设备设置。

添加合规性规则

您只能为 Android 设备定义这些策略设置。

要添加用于控制移动设备符合公司安全要求的规则：

1. 打开策略属性窗口：
   - 在 Kaspersky Security Center Web Console 或云控制台的主窗口中，选择“**设备 > 策略和配置文件**”。在打开的组策略列表中，单击要配置的策略的名称。
   - 在 Kaspersky Security Center Web Console 或云控制台的主窗口中，选择“**设备 > 移动 > 设备**”。单击受到您要配置的策略影响的移动设备，然后在“**活动策略和策略配置文件**”选项卡上选择该策略。
2. 在策略属性页面中，选择“**应用程序设置 > 安全控制**”。
3. 在“**合规性控制**”区域中，单击“**规则**”。
4. 在打开的“**规则**”窗口中，按如下方式定义规则：
   a. 选择规则的不合规标准。
   b. 单击“**添加**”，然后在“**操作**”列中选择不合规时执行的操作。
   您可以添加多个操作。
   c. 使用每个操作的“**纠正时间**”列指定用户可以解决不合规问题的时间段。
   d. 单击“**保存**”按钮保存规则。
5. 单击“**保存**”按钮以保存对策略所做的更改并退出策略属性窗口。

与 Kaspersky Security Center 的下次设备同步之后可配置移动设备设置。

删除合规性规则

您只能为 Android 设备定义这些策略设置。

要删除用于控制移动设备符合公司安全要求的规则：

1. 打开策略属性窗口：
   - 在 Kaspersky Security Center Web Console 或云控制台的主窗口中，选择“**设备 > 策略和配置文件**”。在打开的组策略列表中，单击要配置的策略的名称。
   - 在 Kaspersky Security Center Web Console 或云控制台的主窗口中，选择“**设备 > 移动 > 设备**”。单击受到您要配置的策略影响的移动设备，然后在“**活动策略和策略配置文件**”选项卡上选择该策略。

2. 在策略属性页面中，选择“**应用程序设置** > **安全控制**”。

3. 在“**合规性控制**”区域中，选择要删除的规则，然后单击“**删除**”。

4. 单击“**保存**”按钮以保存对策略所做的更改并退出策略属性窗口。

与 Kaspersky Security Center 的下次设备同步之后可配置移动设备设置。

不合规标准列表

您只能为 Android 设备定义这些策略设置。

为确保 Android 设备符合公司安全要求，Kaspersky Endpoint Security for Android 可以根据以下标准检查设备：

- **已禁用实时保护**。
  必须启用实时保护。
  有关配置实时保护的详细信息，请参阅“配置实时保护”部分。

- **反病毒数据库已过期**。
  Kaspersky Endpoint Security for Android 的反病毒数据库必须定期更新。
  有关定义反病毒数据库更新设置的详细信息，请参阅“配置反病毒保护”部分。

- **已安装被禁止的应用程序**。
  设备不得安装被分类为“**阻止启动**”的应用程序，如“**应用程序控制**”区域中所指定。
  有关创建应用程序规则的详细信息，请参阅“配置应用程序控制”部分。

- **已安装被禁止类别中的应用**。
  设备不得安装属于被分类为“**阻止启动**”的类别的应用程序，如“**应用程序控制**”区域中所指定。
  有关创建应用程序类别规则的详细信息，请参阅“配置应用程序控制”部分。

- **并非已安装所有所需的应用程序**。
  设备必须安装被分类为“**强制安装**”的特定应用程序，如“**应用程序控制**”区域中所指定。
  有关创建应用程序规则的详细信息，请参阅“配置应用程序控制”部分。

- **操作系统版本已过时**。
  设备必须安装了允许的操作系统版本。
  要使用此不合规标准，您必须在“**操作系统最低版本**”和“**操作系统最高版本**”下拉列表中指定允许的操作系统版本范围。

- **设备已长时间未同步**。
  设备必须定期与管理服务器同步。
  要使用此不合规标准，您必须在“**同步间隔**”下拉列表中指定设备同步的最大时间间隔。

- **设备已取得根权限**。
  设备不得取得根权限。
  有关详细信息，请参阅“检测设备入侵（根权限）”部分。

- **解锁密码不符合安全要求。**

  必须使用符合解锁密码强度要求的解锁密码来保护设备。

不合规时的操作列表

您只能为 Android 设备定义这些策略设置。

如果用户未在指定时间内修复不合规问题，则以下操作可用：

- **阻止除系统应用程序之外的所有应用程序。**

  阻止用户移动设备上的所有应用程序（系统应用程序除外）启动。

- **锁定设备。**

  移动设备将被锁定。要获取对数据的访问，您必须 解锁设备。如果设备解锁后，解锁设备的原因未更改，设备将在指定时间段后再次被锁定。

- **擦除企业数据。**

  擦除容器化数据、公司电子邮件帐户、连接到公司 Wi-Fi 网络和 VPN 的设置以及接入点名称 (APN)。

- **将设备完全重置为出厂设置。**

  所有数据都将从移动设备中删除，设置将回滚至其出厂值。

配置用户对网站的访问

您可以为 Android 和 iOS 设备定义这些策略设置。

为了在互联网浏览期间保护移动设备上存储的个人和公司数据，可以使用“Web 保护”配置用户对网站的访问权限。“Web 保护”会在用户打开网站之前对其进行扫描，然后阻止会分发恶意代码的网站以及旨在窃取机密数据和获取金融账户访问权限的钓鱼网站。

对于 Android 设备，此功能还支持按卡巴斯基安全网络云服务中定义的类别进行网站过滤。过滤允许您限制对某些网站或某些类别的网站（例如“**赌博、彩票、抽奖**”或“**互联网通信**”类别中的网站）的访问。

在 Android 设备上，Web 保护仅在 Google Chrome 浏览器、Huawei Browser 和 Samsung Internet Browser 中可用。

为确保“Web 保护”正常运行，必须将 Kaspersky Endpoint Security for Android 设置为辅助功能。Kaspersky Endpoint Security for Android 会提示用户通过初始配置向导将该应用程序设置为可访问功能。用户可以跳过此步骤或以后在设备设置中禁用此服务。

在 iOS 设备上，用户必须允许 Kaspersky Security for iOS 应用程序添加 VPN 配置才能使 Web 保护正常工作。

要配置用户对网站的访问权限：

1. 打开策略属性窗口：
   - 在 Kaspersky Security Center Web Console 或云控制台的主窗口中，选择“**设备 > 策略和配置文件**”。在打开的组策略列表中，单击要配置的策略的名称。
   - 在 Kaspersky Security Center Web Console 或云控制台的主窗口中，选择“**设备 > 移动 > 设备**”。单击受到您要配置的策略影响的移动设备，然后在“**活动策略和策略配置文件**”选项卡上选择该策略。
2. 在策略属性页面中，选择“**应用程序设置 > 安全控制**”。
3. 在“**Web 保护**”区域中，选中“**启用 Web 保护**”复选框以启用该功能。
4. 对于 Android 设备，可以选择以下选项之一：
   - 要根据网站内容限制用户访问网站：
     a. 选择“**阻止指定类别的网站**”。
     b. 选中 Kaspersky Endpoint Security for Android 将阻止访问的网站类别旁边的复选框。

     如果启用 Web 保护，用户对“**钓鱼**”和“**恶意软件网站**”类别中的网站的访问始终会被阻止。
   - 要指定允许的网站列表：
     a. 选择“**仅允许指定网站**”。
     b. 通过添加应用程序不会阻止访问的网站地址来创建网站列表。Kaspersky Endpoint Security for Android 仅支持正规表达式。输入允许的网站的地址时，请使用以下模板：
        - `http:\/\/www\.example\.com.*` – 网站的所有子页面都被允许(例如，`http://www.example.com/about`)。
        - `https:\/\/.*example\.com` – 网站的所有子域页面都被允许(例如，`https://pictures.example.com`)。

     c. 您也可以使用表达式 `https?` 来选择 HTTP 和 HTTPS。对于更多正规表达式的详情，请参考 Oracle 技术支持网站。
   - 要阻止用户访问所有网站，请选择“**阻止所有网站**”。
5. 单击“**保存**”按钮以保存对策略所做的更改并退出策略属性窗口。

与 Kaspersky Security Center 的下次设备同步之后可配置移动设备设置。

配置功能限制

您只能为 Android 设备定义这些策略设置。

Kaspersky Security Center Web Console 允许您配置用户对以下移动设备功能的访问权限：

- Wi-Fi
- 摄像头
- 蓝牙

默认情况下，用户可以在设备上无限制地使用 Wi-Fi、摄像头和蓝牙。

若要在设备上配置 Wi-Fi、摄像头和蓝牙的使用限制，请执行以下步骤：

1. 打开策略属性窗口：
   - 在 Kaspersky Security Center Web Console 或云控制台的主窗口中，选择“**设备 > 策略和配置文件**”。在打开的组策略列表中，单击要配置的策略的名称。
   - 在 Kaspersky Security Center Web Console 或云控制台的主窗口中，选择“**设备 > 移动 > 设备**”。单击受到您要配置的策略影响的移动设备，然后在“**活动策略和策略配置文件**”选项卡上选择该策略。
2. 在策略属性页面中，选择“**应用程序设置 > 安全控制**”。
3. 在“**功能管理**”区域中，配置 Wi-Fi、摄像头和蓝牙的使用：
   - 要禁用用户移动设备上的 Wi-Fi 模块，请选中“**禁止使用 Wi-Fi(仅针对 Android 9 或更早版本的设备)**”复选框。

     在运行 Android 10.0 或更高版本的设备上，不支持禁止使用 Wi-Fi 网络。
   - 要禁用用户移动设备上的摄像头，请选中“**禁止使用摄像头**”复选框。

     在运行 Android 10.0 或更高版本的设备上，不能完全禁止使用摄像头。

     在运行 Android 11 或更高版本的设备上，必须将 Kaspersky Endpoint Security for Android 设置为无障碍功能。Kaspersky Endpoint Security for Android 会提示用户通过初始配置向导将该应用程序设置为可访问功能。用户可以跳过此步骤或以后在设备设置中禁用此服务。如果是这种情况，您将无法限制使用摄像头。
   - 要禁用用户移动设备上的蓝牙，请选中“**禁止使用蓝牙**”复选框。

     在 Android 12 或更高版本上，只有设备用户授予了“**附近的蓝牙设备**”权限后，才能禁用蓝牙。用户可以在初始配置向导期间或稍后授予此权限。
4. 单击“**保存**”按钮以保存对策略所做的更改并退出策略属性窗口。

与 Kaspersky Security Center 的下次设备同步之后可配置移动设备设置。

防止 Kaspersky Endpoint Security for Android 被删除

为了保护移动设备和遵守公司安全要求，您可以启用保护以防止删除 Kaspersky Endpoint Security for Android。在这种情况下，用户无法使用 Kaspersky Endpoint Security for Android 界面删除该应用程序。当使用 Android 操作系统的工具删除应用程序时，用户会被提示禁用 Kaspersky Endpoint Security for Android 的管理员权限。禁用权限后，移动设备将被锁定。

要启用保护以防止删除 Kaspersky Endpoint Security for Android：

1. 打开策略属性窗口：

   - 在 Kaspersky Security Center Web Console 或云控制台的主窗口中，选择“**设备 > 策略和配置文件**”。在打开的组策略列表中，单击要配置的策略的名称。
   - 在 Kaspersky Security Center Web Console 或云控制台的主窗口中，选择“**设备 > 移动 > 设备**”。单击受到您要配置的策略影响的移动设备，然后在“**活动策略和策略配置文件**”选项卡上选择该策略。

2. 在策略属性页面中，选择“**应用程序设置 > 安全控制**”。
3. 在“**管理移动设备上的应用程序**”区域中，清除“**允许从设备删除 Kaspersky Endpoint Security for Android**”复选框。

   要保护在运行安卓 7.0 或更高版本的设备上的应用程序不会被卸载，必须将 Kaspersky Endpoint Security for Android 设置为可访问功能。当初始配置向导正在运行时，Kaspersky Endpoint Security for Android 会提示用户授予应用程序所有必需的权限。用户可以跳过这些步骤或以后在设备设置中禁用这些权限。在这种情况下，不保护该应用程序不被卸载。

4. 单击“**保存**”按钮以保存对策略所做的更改并退出策略属性窗口。

与 Kaspersky Security Center 的下次设备同步之后可配置移动设备设置。

如果尝试删除应用程序，移动设备将被锁定。

配置移动设备与 Kaspersky Security Center 的同步

您可以为 Android 和 iOS 设备定义这些策略设置。

要管理移动设备并从移动设备接收报告或统计信息，必须定义同步设置。移动设备与 Kaspersky Security Center 的同步可通过以下方式执行：

- **按计划**。使用 HTTP 按计划执行同步。您可以在策略属性中配置同步计划。当移动设备按照计划与 Kaspersky Security Center 同步时，执行对策略设置、命令和任务的修改 — 即，有一个延迟。默认情况下，移动设备每六小时与 Kaspersky Security Center 自动同步一次。

  在 Android 12 或更高版本上，如果设备处于省电模式，应用程序可能会晚于指定的时间执行此任务。

- **强制**（适用于 Android 设备）。使用 FCM 服务 (Firebase Cloud Messaging) 的推送通知执行强制同步。强制同步主要用于及时传递命令到移动设备。如果要使用强制同步，请确保在 Kaspersky Security Center 中配置 FCM 设置。

要配置移动设备与 Kaspersky Security Center 的同步：

1. 打开策略属性窗口：
   - 在 Kaspersky Security Center Web Console 或云控制台的主窗口中，选择“**设备 > 策略和配置文件**”。在打开的组策略列表中，单击要配置的策略的名称。
   - 在 Kaspersky Security Center Web Console 或云控制台的主窗口中，选择“**设备 > 移动 > 设备**”。单击受到您要配置的策略影响的移动设备，然后在“**活动策略和策略配置文件**”选项卡上选择该策略。
2. 在策略属性页面中，选择“**应用程序设置 > 同步**”。
3. 在“**与管理服务器同步**”区域中，使用“**同步间隔**”下拉列表选择同步周期。
   默认情况下，每六小时执行一次同步。
4. 对于 Android 设备，您可以禁用在设备漫游时同步。要执行此操作，请选中“**漫游时不同步**”复选框。
   默认情况下，启用漫游时同步。
5. 单击“**保存**”按钮以保存对策略所做的更改并退出策略属性窗口。

与 Kaspersky Security Center 的下次设备同步之后可配置移动设备设置。

卡巴斯基安全网络

为有效保护移动设备，Kaspersky Endpoint Security for Android 和 Kaspersky Security for iOS 使用从全球用户收集到的数据。*卡巴斯基安全网络*用户处理此类数据。

卡巴斯基安全网络 (KSN) 是一种云服务基础设施，它提供对 Kaspersky 在线知识库的访问，该知识库包含有关文件、Web 资源和软件的信誉的信息。使用卡巴斯基安全网络中的数据，可确保在遇到威胁时 Kaspersky 程序能够做出更快速的响应，提高某些保护组件的性能，并降低误报的风险。

您加入卡巴斯基安全网络将帮助卡巴斯基获取有关新威胁的类型和来源的实时信息，研究消除威胁的办法并降低误报数量。加入卡巴斯基安全网络也允许您访问应用程序和网站信誉统计数据。

加入卡巴斯基安全网络后，当移动应用程序运行时，会获取一些统计信息并自动发送至卡巴斯基。该信息有助于实时跟踪威胁。可能会被入侵者用来损坏计算机或用户内容的文件或其部分也会被发送至 Kaspersky 以进行额外的检查。

以下应用程序组件使用卡巴斯基安全网络云服务：

- Kaspersky Endpoint Security for Android 应用程序中的反病毒、Web 保护和应用程序控制组件。
- Kaspersky Security for iOS 应用程序中的 Web 保护组件。

要开始使用 KSN，您必须接受最终用户授权许可协议的条款和条件。有关向 KSN 发送数据的更多信息，请参阅与卡巴斯基安全网络的信息交换。

拒绝参与 KSN 会降低设备保护级别，这将引发设备感染和数据丢失。

要改进移动应用程序性能，还可以将统计数据提供给卡巴斯基安全网络。

向卡巴斯基安全网络提供信息是自愿的。

与卡巴斯基安全网络交换信息

Kaspersky Endpoint Security for Android 中的信息交换

为改进实时保护功能，Kaspersky Endpoint Security for Android 将使用卡巴斯基安全网络云服务来运行以下组件：

- 反病毒。应用获得到关于文件和应用信誉的 Kaspersky 在线知识库的访问。此项扫描旨在扫描威胁信息尚未添加到反病毒数据库但已包含在 KSN 中的威胁。卡巴斯基安全网络云服务提供反病毒的完整操作并降低误报的可能性。
- **Web 保护**。在打开网站之前，该应用程序使用从 KSN 接收的数据来扫描网站。该应用程序会根据允许和阻止的类别（例如，“互联网通信”类别）列表来确定网站类别，以控制用户的互联网访问权限。
- 应用程序控制。该应用程序会根据允许和阻止的类别（例如，“游戏”类别）列表来确定应用程序类别，以限制不符合公司安全要求的应用程序启动。

最终用户授权许可协议中提供了有关在运行反病毒和应用程序控制的过程中使用 KSN 时提交到 Kaspersky 的数据类型的信息。接受授权许可协议的条款和条件即表明您同意传输此信息。

关于 Web 保护的数据处理的声明中提供了有关在运行 Web 保护的过程中使用 KSN 时提交到 Kaspersky 的数据类型的信息。接受声明的条款和条件即表明您同意传输此信息。

有关向 KSN 提供数据的更多信息，请参阅 Kaspersky Endpoint Security for Android 中的数据提供。

向 KSN 提供数据是自愿的。如果需要，您可以禁用与 KSN 的数据交换。

Kaspersky Security for iOS 中的信息交换

为改进实时保护，Kaspersky Security for iOS 使用卡巴斯基安全网络云服务来运行 **Web 保护**组件：在打开 Web 资源之前，该应用程序使用从 KSN 接收的数据来扫描 Web 资源。

最终用户授权许可协议中提供了有关在运行 Web 保护的过程中使用 KSN 时提交到卡巴斯基的数据类型的信息。接受授权许可协议的条款和条件即表明您同意传输此信息。

有关向 KSN 提供数据的更多信息，请参阅 Kaspersky Security for iOS 中的数据提供。

向 KSN 提供数据是自愿的。如果需要，您可以禁用与 KSN 的数据交换。

从 Android 和 iOS 应用程序向 KSN 发送统计数据

要与 KSN 交换数据以提高应用程序的性能，必须满足以下条件：

- 设备用户必须阅读并接受卡巴斯基安全网络声明的条款。
- 您必须将组策略设置配置为允许发送统计信息到 KSN。

您可以随时选择退出发送统计数据到卡巴斯基安全网络。如果卡巴斯基安全网络声明中规定了在运行移动应用程序的过程中使用 KSN，则会将有关统计数据类型的信息提交到卡巴斯基。

启用和禁用卡巴斯基安全网络

默认情况下，启用卡巴斯基安全网络。

如果禁用卡巴斯基安全网络，卡巴斯基安全网络中的 Web 保护、应用程序控制和其他保护将自动被禁用，并且它们的设置变为不可用。

若要启用和禁用使用卡巴斯基安全网络，请执行以下操作：

1. 打开策略属性窗口：
   - 在 Kaspersky Security Center Web Console 或云控制台的主窗口中，选择“**设备 > 策略和配置文件**”。在打开的组策略列表中，单击要配置的策略的名称。
   - 在 Kaspersky Security Center Web Console 或云控制台的主窗口中，选择“**设备 > 移动 > 设备**”。单击受到您要配置的策略影响的移动设备，然后在“**活动策略和策略配置文件**”选项卡上选择该策略。
2. 在策略属性页面中，选择“**应用程序设置 > KSN 和统计数据**”。
3. 要启用或禁用卡巴斯基安全网络，请选中或清除“**使用卡巴斯基安全网络**”复选框。
4. 如果启用了卡巴斯基安全网络并且您同意将数据提交到 Kaspersky，请选中“**允许将统计数据发送到卡巴斯基安全网络**”复选框。此数据将帮助移动应用程序在遇到威胁时更快地作出响应，提高保护组件的性能以及降低误报的风险。
5. 单击“**保存**”按钮以保存对策略所做的更改并退出策略属性窗口。

与 Kaspersky Security Center 的下次设备同步之后可配置移动设备设置。

与 Google Analytics for Firebase、SafetyNet Attestation、Firebase Performance Monitoring 和 Crashlytics 交换信息

您只能为 Android 设备定义这些策略设置。

Kaspersky Endpoint Security for Android 与 Google Analytics for Firebase、SafetyNet Attestation、Firebase Performance Monitoring 和 Crashlytics 服务交换数据，以通过分析用户体验、功能、状态和使用的设备设置来改进卡巴斯基软件、产品、服务和基础设施的质量、外观和性能。

默认情况下，禁止与 Google Analytics for Firebase、SafetyNet Attestation、Firebase Performance Monitoring 和 Crashlytics 服务交换信息。

要启用数据交换：

1. 打开策略属性窗口：

- 在 Kaspersky Security Center Web Console 或云控制台的主窗口中，选择“**设备 > 策略和配置文件**”。在打开的组策略列表中，单击要配置的策略的名称。
- 在 Kaspersky Security Center Web Console 或云控制台的主窗口中，选择“**设备 > 移动 > 设备**”。单击受到您要配置的策略影响的移动设备，然后在“**活动策略和策略配置文件**”选项卡上选择该策略。

2. 在策略属性页面中，选择“**应用程序设置 > KSN 和统计数据**”。
3. 在“**发送统计数据**”区域中，选中“**允许数据传输以帮助提高应用程序的质量、外观和性能**”复选框。
4. 单击“**保存**”按钮以保存对策略所做的更改并退出策略属性窗口。

与 Kaspersky Security Center 的下次设备同步之后可配置移动设备设置。

配置移动设备上的通知

您只能为 Android 设备定义这些策略设置。

如果不希望 Kaspersky Endpoint Security for Android 通知分散移动设备用户的注意力，可以禁用某些通知。

Kaspersky Endpoint Security 使用以下工具显示设备保护状态：

- **保护状态通知**。该通知位于通知栏。保护状态通知无法移除。通知显示设备保护状态（例如，）和可能的问题数量。设备用户可以轻触设备保护状态并查看应用问题列表。
- **应用通知**。这些通知提示设备用户应用程序信息（例如，威胁检测）。
- **弹出消息**。弹出消息需要设备用户的操作（例如，当检测到威胁时要采取的操作）。

所有 Kaspersky Endpoint Security for Android 通知均为默认启用。

在 Android 13 中，设备用户应在初始配置向导期间或之后授予发送通知的权限。

Android 设备用户可以在通知栏的设置中禁用来自 Kaspersky Endpoint Security for Android 的所有通知。如果禁用通知，用户不会监控应用程序的运行，并且可能会忽略重要信息（例如，有关设备与 Kaspersky Security Center 同步期间发生的故障的信息）。在这种情况下，要了解应用程序运行状态，用户必须打开 Kaspersky Endpoint Security for Android。

要配置移动设备上 Kaspersky Endpoint Security for Android 操作的通知显示：

1. 打开策略属性窗口：
   - 在 Kaspersky Security Center Web Console 或云控制台的主窗口中，选择“**设备 > 策略和配置文件**”。在打开的组策略列表中，单击要配置的策略的名称。
   - 在 Kaspersky Security Center Web Console 或云控制台的主窗口中，选择“**设备 > 移动 > 设备**”。单击受到您要配置的策略影响的移动设备，然后在“**活动策略和策略配置文件**”选项卡上选择该策略。
2. 在策略属性页面中，选择“**应用程序设置 > 通知和报告**”。

3. 在“**通知**”区域中，配置通知的显示：

- 要隐藏所有通知和弹出消息，请禁用“**Kaspersky Endpoint Security 在后台时显示通知**”切换按钮。

  Kaspersky Endpoint Security for Android 将仅显示保护状态通知。通知显示设备保护状态（例如，）和问题数量。当用户使用应用程序时，应用程序也会显示通知（例如，用户手动更新反病毒数据库）。

  > Kaspersky 专家建议您启用通知和弹出消息。如果当应用处于后台模式时您禁用通知和弹出消息，应用将不会警告用户实时威胁。移动设备用户仅在打开应用时才可以学习设备保护状态。

- 在“**用户设备上显示的安全问题列表**”中，选择要在用户的移动设备上显示的 Kaspersky Endpoint Security for Android 问题。

4. 单击“**保存**”按钮以保存对策略所做的更改并退出策略属性窗口。

与 Kaspersky Security Center 的下次设备同步之后可配置移动设备设置。

检测设备入侵

通过 Kaspersky Security Center Web Console 可检测 Android 设备上的设备入侵 (root) 和 iOS 设备上的越狱。被入侵的设备上的系统文件不受保护，因此可被修改。此外，来自未知来源的第三方应用可能会安装在被黑客入侵的设备上。在检测到黑客尝试后，建议您立即恢复设备的正常操作。

Kaspersky Endpoint Security for Android 使用以下服务来检测用户何时获取 root 权限：

- *Kaspersky Endpoint Security for Android 的嵌入式服务*。一种 Kaspersky 服务，用于检查移动设备用户是否已获得根权限 (Kaspersky Mobile Security SDK)。
- *SafetyNet Attestation*。一种 Google 服务，用于检查操作系统的完整性，分析设备硬件和软件，以及识别其他安全问题。有关 SafetyNet Attestation 的更多详细信息，请访问 Android 技术支持网站。

Kaspersky Security for iOS 使用以下服务来检测越狱：

- *Kaspersky Security for iOS 的嵌入式服务*。一种卡巴斯基服务，用于检查移动设备是否已越狱 (Kaspersky Mobile Security SDK)。

如果设备被黑客入侵，您会收到一条通知。您可以在 Kaspersky Security Center Web Console 的“**监控和报告 > 仪表板**”选项卡上查看入侵通知。还可以在事件通知设置中停用有关黑客的通知。

在 Android 设备上，如果设备被入侵，您可以对用户活动施加限制（例如锁定设备）。您可以使用“合规性控制”组件施加限制。为此，请创建具有“**设备已取得根权限**”标准的合规性规则。

定义授权许可设置

您可以为 Android 和 iOS 设备定义这些策略设置。

要在 Kaspersky Security Center Web Console 或云控制台中管理移动设备，您必须在移动设备上激活移动应用程序。在移动设备上激活 Kaspersky Endpoint Security for Android 应用程序或 Kaspersky Security for iOS 应用程序是通过向该应用程序提供有效的授权许可信息来完成的。当设备与 Kaspersky Security Center 同步时，授权许可信息将与策略一起传递到移动设备。

如果在移动设备上安装移动应用程序后 30 天内未完成激活，该应用程序将自动切换至受限功能模式。在此模式中，大部分应用程序组件都无法运行。切换到受限功能模式后，该应用程序将停止执行与 Kaspersky Security Center 的自动同步。因此，如果在应用程序安装后 30 天内未完成激活，用户必须手动与 Kaspersky Security Center 同步设备。

要定义组策略的授权许可设置：

1. 打开策略属性窗口：
   - 在 Kaspersky Security Center Web Console 或云控制台的主窗口中，选择“**设备 > 策略和配置文件**”。在打开的组策略列表中，单击要配置的策略的名称。
   - 在 Kaspersky Security Center Web Console 或云控制台的主窗口中，选择“**设备 > 移动 > 设备**”。单击受到您要配置的策略影响的移动设备，然后在“**活动策略和策略配置文件**”选项卡上选择该策略。
2. 在策略属性页面中，选择“**应用程序设置 > 授权许可**”。
3. 使用下拉列表从管理服务器的密钥存储中选择所需的授权许可密钥。
   授权许可密钥的详细信息显示在下面的字段中。

   如果移动设备上的现有激活密钥与上面下拉列表中选择的密钥不同， 则可以将其替换。为此，请选中“**如果设备上的密钥不同，则替换为此密钥**”复选框。
4. 单击“**保存**”按钮以保存对策略所做的更改并退出策略属性窗口。

与 Kaspersky Security Center 的下次设备同步之后可配置移动设备设置。

配置事件

您可以为 Android 和 iOS 设备定义这些策略设置。

您可以定义用户设备上发生的事件以及发送到 Kaspersky Security Center 的事件的存储和通知设置。

仅当修改策略时才能配置事件。

事件按重要性级别分布在以下选项卡上：

- **严重**
  严重事件表示可能导致数据丢失、操作故障或严重错误的问题。
- **功能故障**
  功能故障表示应用程序运行期间发生的严重问题、错误或故障。
- **警告**
  警告不一定是严重的，但仍然表示未来可能出现的问题。
- **信息**

信息事件通知的是操作或程序成功完成，或者应用程序正常运行。

在每个部分，列表显示事件类型和 Kaspersky Security Center 中的默认事件存储期限（以天为单位）。

在事件列表中可以执行以下操作：

- 在发送到 Kaspersky Security Center 的事件类型列表中添加或删除事件类型。
- 定义每种事件类型的存储和通知设置，例如：此类型的事件必须在管理服务器数据库中存储多久，或者是否通过电子邮件将此类型的事件通知您。

有关在 Kaspersky Security Center Web Console 和云控制台中配置事件的更多详细信息：

- 如果您使用 Kaspersky Security Center Web Console，请参阅 *Kaspersky Security Center 帮助*。
- 如果您使用 Kaspersky Security Center 云控制台，请参阅 *Kaspersky Security Center 云控制台帮助*。

配置有关在用户设备上安装、更新和删除应用程序的事件

您可以为 Android 和 iOS 设备定义这些策略设置。

如果您使用 Kaspersky Security Center 云控制台，则用户设备上发生的事件和发送到 Kaspersky Security Center 的事件的类型列表不包括设备上的应用程序安装、更新和删除。这是因为此类事件经常发生，当达到事件计数限制时，这些事件可能会替换 Kaspersky Security Center 数据库中的其他重要事件。它们还可能影响管理服务器或 DBMS 的性能以及与 Kaspersky Security Center 云控制台的互联网连接带宽。

如果您仍然希望存储这种类型的事件并收到有关它们的通知，请按照本部分中的说明进行操作。

要配置有关用户设备上安装、更新和删除应用程序的事件：

1. 在策略设置的“**事件配置**”选项卡上，将“**应用程序已被安装或卸载（已安装应用程序的列表）**”信息事件类型添加到管理服务器数据库中存储的事件列表中。

   有关配置事件的更多详细信息，请参阅 *Kaspersky Security Center 云控制台帮助*。

2. 启用“发送所有移动设备上已安装应用程序的列表”选项。

   有关用户设备上安装、更新和删除应用程序的事件存储在 Kaspersky Security Center 数据库中。您会收到有关这些事件的通知。

网络负载

本节包含有关移动设备和 Kaspersky Security Center 之间交换的网络流量的信息。

流量

任务	外出流量	内进流量	总流量
应用程序初始部署，MB	0.08	17.76	17.84
反病毒数据库初始更新（流量可能会因反病毒数据库的大小而不同），MB	0.04	2.21	2.25

移动设备与 Kaspersky Security Center 同步，MB	0.03	0.02	0.05
反病毒数据库定期更新（流量可能会因反病毒数据库的大小而不同），MB	0.08	3.06	3.14
执行反盗窃命令。定位设备（流量可能会因嵌入式摄像头规格和图像质量而不同），MB	0.09	0.8	0.17
执行反盗窃命令。拍摄面部照片，MB	1.0	0.02	1.02
执行反盗窃命令。设备锁定，MB	0.06	0.05	0.11
平均每日流量，MB	0.22	6.96	7.18

在基于 MMC 的管理控制台中工作

本帮助部分介绍使用基于 MMC 的 Kaspersky Security Center 管理控制台保护和管理移动设备。

关键用例

安装

如何远程安装 Kaspersky Endpoint Security for Android?

如何阻止用户删除 Kaspersky Endpoint Security for Android?

如何激活 Kaspersky Endpoint Security for Android?

保护

如何锁定丢失或被盗的设备?

如何保护自己免受互联网威胁?

如何禁止使用空密码?

使用第三方解决方案

安卓企业（带有手提箱图标的应用程序， 配置安卓工作配置文件）

VMware AirWatch, MobileIron, IBM Maas360, SOTI MobiControl

控制

如何阻止用户在设备上玩游戏?

如何在设备上配置访问网站?

如何检测根权限?

管理

如何在设备上配置邮箱?

如何将移动设备连接到 Wi-Fi?

如何安装企业应用程序?

关于 Kaspersky Security for Mobile

Kaspersky Security for Mobile 是一款集成解决方案，用于保护和管理公司移动设备以及公司员工用于公司用途的个人移动设备。

Kaspersky Security for Mobile 包括以下组件：

- Kaspersky Endpoint Security for Android 移动应用程序

  Kaspersky Endpoint Security for Android 应用可确保移动设备抵御 Web 威胁、病毒和构成威胁的其他程序的侵害。

- Kaspersky Endpoint Security for Android 管理插件。

  Kaspersky Endpoint Security for Android 的管理插件提供界面，用于通过 Kaspersky Security Center 管理控制台，管理移动设备以及安装在这些设备上的移动应用程序。

- Kaspersky Device Management for iOS 管理插件

Kaspersky Device Management for iOS 管理插件允许您在不使用 iPhone 配置实用程序或 Exchange 管理控制台的情况下，为通过 iOS MDM 协议连接到 Kaspersky Security Center 的设备（以下简称“iOS MDM 设备”）和通过 Exchange ActiveSync 协议连接到 Kaspersky Security Center 的设备（以下简称“EAS 设备”）定义配置设置。

管理插件集成到 *Kaspersky Security Center 远程管理系统* 中。管理员可以使用单个的 Kaspersky Security Center 管理控制台管理公司网络中所有移动设备，也可以管理客户端计算机和虚拟系统。将移动设备连接至管理服务器后，移动设备就变成托管设备。管理员可以远程监控托管设备。

Kaspersky Endpoint Security for Android 移动应用程序也可能作为 *Kaspersky Endpoint Security Cloud 远程管理系统*的一部分运行。有关通过 Kaspersky Endpoint Security Cloud 使用应用程序的更多详细信息，请参阅 *“Kaspersky Endpoint Security Cloud 在线帮助”*。

Kaspersky Endpoint Security for Android 移动应用程序也可能作为 AppConfig Community 参与者的第三方 EMM 解决方案的一部分运行。

基于 MMC 的管理控制台中的移动设备管理的主要功能

Kaspersky Security for Mobile 包括以下功能：

- 通过使用 Google Play 链接将连接 Android 设备的邮件消息分发到 Kaspersky Security Center。
- 远程连接移动设备到 Kaspersky Security Center 和其他第三方 EMM 系统（例如，VMWare AirWatch、MobileIron、IBM Maas360、SOTI MobiControl）。
- Kaspersky Endpoint Security for Android 应用的远程配置，以及服务、应用和 Android 设备功能的远程配置。
- 根据企业安全要求远程配置移动设备。
- 预防移动设备在丢失或被盗时存储的企业信息泄露（反盗窃）。
- 企业安全需求合规性控制（合规性控制）。
- 移动设备互联网使用控制（Web 保护）。
- 在移动设备上设置企业邮件，包括在公司部署了 Microsoft Exchange 邮件服务器的组织（仅限 iOS 和三星设备）。
- 配置企业网络（Wi-Fi、VPN），以便在移动设备上使用 VPN。VPN 仅支持在 iOS 和三星设备上配置。
- 配置当策略规则被违反时将显示在 Kaspersky Security Center 中的移动设备状态：紧急、警告、正常。
- 设置在 Kaspersky Endpoint Security for Android 应用上显示给用户的通知。
- 支持 Samsung KNOX 2.6 或更新版本的设备的设置配置。
- 配置支持 Android 工作配置文件的设备上的设置。
- 通过 Samsung KNOX Mobile Enrollment 控制台部署 Kaspersky Endpoint Security for Android 应用程序。Samsung KNOX Mobile Enrollment 设计用于在从官方提供商购买的 Samsung 设备上批量安装和初始化应用配置。
- 可以使用 Kaspersky Security Center 策略将 Kaspersky Endpoint Security for Android 应用程序升级到到指定版本。

- 关于 Kaspersky Endpoint Security for Android 应用状态和事件的管理员通知可以在 Kaspersky Security Center 中或通过邮件进行沟通。
- 策略设置的变更控制（修订历史记录）。

Kaspersky Security for Mobile 包括以下保护和管理组件：

- 反病毒（对于 Android 设备）
- 反盗窃（对于 Android 设备）
- 网页保护（对于 Android 和 iOS 设备）
- 应用程序控制（对于 Android 设备）
- 合规性控制（对于 Android 设备）
- 检测设备上的 root 权限（适用于 Android 设备）

关于 Kaspersky Endpoint Security for Android

Kaspersky Endpoint Security for Android 应用可确保移动设备抵御 Web 威胁、病毒和构成威胁的其他程序的侵害。

Kaspersky Endpoint Security for Android 应用包括以下组件：

- **反病毒**。反病毒功能使用反病毒数据库及卡巴斯基安全网络云服务检测并消除威胁。反病毒功能包含以下组件：
  - 保护。功能在打开的文件中检测威胁、扫描新应用、实时保护设备。
  - 扫描。它根据需要针对整个文件系统、仅针对已安装的应用程序或针对选定的文件或文件夹启动。
  - 更新。“更新”功能允许您为应用程序下载新的反病毒数据库。
- **反盗窃**。该组件在设备丢失或被盗时保护设备上的信息，防御未经授权的访问。通过此组件可以向设备发送以下命令：
  - **定位**，以获取设备位置的坐标。
  - **报警**，使设备发出响亮的警报声。
  - **面部照片**，当有人试图解锁设备时，让设备使用正面摄像头拍照。
  - **擦除**公司数据以保护公司敏感信息。
- **Web 保护**。该组件可以阻止用于扩散恶意代码的恶意网站。Web 保护还会阻止旨在盗窃用户机密数据（例如，网上银行或电子货币系统的密码）并访问用户财务信息的虚假（钓鱼）网站。Web 保护将在您打开网站前使用卡巴斯基安全网络云服务扫描网站。扫描之后，Web 防护将允许可信的网站加载并阻止恶意网站。Web 保护也支持按 Kaspersky Security Network 云服务中所定义类别过滤网站。这允许管理员限制用户对某些类别网页的访问（例如“赌博、彩票、抽奖”或“互联网通信”类别中的网页）。
- **应用程序控制**。使用此组件可以通过指向分发包的直接链接或指向 Google Play 的链接，将推荐和必需的应用程序安装到您的设备上。应用程序控制还允许您卸载那些违反公司安全要求的已阻止应用程序。

- **合规性控制**。此组件允许检查受管理设备是否符合公司安全要求，并对不符合要求的设备的某些功能施加限制。

关于 Kaspersky Device Management for iOS

Kaspersky Device Management for iOS 可确保对连接到 Kaspersky Security Center 的移动设备进行保护和控制，并包括如下设备管理功能：

- **密码保护**。此功能允许设置密码复杂性要求，以便用户使用符合公司密码策略的复杂密码。
- **网络管理**。此功能允许添加经过批准的 VPN 和 Wi-Fi 网络，或限制对其他网络的访问。
- **擦除企业数据**。如果设备丢失或被盗，您可以向其发送"擦除"命令以保护公司的敏感信息。
- **Web 保护**。该组件可以阻止用于扩散恶意代码的恶意网站。Web 保护也可以阻止用于盗窃用户机密数据（例如，网上银行或电子货币系统的密码）并访问用户财务信息的虚假（钓鱼）网站。Web 保护将在您打开网站前使用卡巴斯基安全网络云服务扫描网站。扫描之后，Web 防护将允许可信的网站加载并阻止恶意网站。Web 保护也支持按 Kaspersky Security Network 云服务中所定义类别过滤网站。这允许管理员限制用户对某些类别网页的访问（例如"赌博、彩票、抽奖"或"互联网通信"类别中的网页）。
- **应用程序限制**。通过此组件可以控制是否可以在受监控设备上使用 iTunes、Safari 或 Game Center 等设备本机应用。
- **功能限制**。此组件允许检查受管理设备是否符合公司安全要求，并对不符合要求的设备的某些功能施加限制。

关于 Exchange 邮箱

Exchange 邮箱 是 Exchange ActiveSync 服务的客户端应用程序。该应用程序旨在帮助企业用户使用电子邮件、日历、联系人和任务。Exchange 邮箱允许您将移动设备连接到 Microsoft Exchange 服务器。有关 Exchange ActiveSync 服务的更多详细信息，请访问 *Microsoft 技术支持网站*。

要通过 Exchange ActiveSync 协议管理移动设备，Microsoft Exchange 服务器上必须部署 Exchange 服务器。有关安装 Exchange Server 的更多详细信息，请参阅 *Kaspersky Security Center 帮助*。不需要在移动设备上进行其他配置。

使用 Exchange 邮箱，您可以通过使用组策略远程配置 EAS 设备并可以发送数据擦除命令。以下操作系统支持 Exchange ActiveSync 协议：

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

- iOS
- Symbian

Exchange ActiveSync 设备的一组管理设置的内容取决于移动设备上运行的操作系统。有关适用于特定操作系统的 Exchange ActiveSync 协议的支持功能的详细信息，请参阅特定操作系统的文档。

关于 Kaspersky Endpoint Security for Android 管理插件

Kaspersky Endpoint Security for Android 的管理插件提供界面，用于通过 Kaspersky Security Center 管理控制台，管理移动设备以及安装在这些设备上的移动应用程序。Kaspersky Endpoint Security for Android 管理插件可用于：

- 为移动设备创建组安全策略。
- 远程配置用户移动设备上的 Kaspersky Endpoint Security for Android 应用程序的运行设置。
- 接收有关用户设备上的 Kaspersky Endpoint Security for Android 移动应用程序的运行情况的报告和统计信息。

默认情况下，部署 Kaspersky Security Center 时会安装 Kaspersky Endpoint Security for Android 管理插件。该插件不需要单独安装。

关于 Kaspersky Device Management for iOS 管理插件

Kaspersky Device Management for iOS 的管理插件提供了界面，用于通过 Kaspersky Security Center 管理控制台管理通过 iOS MDM 和 Exchange ActiveSync 协议连接的移动设备。Kaspersky Device Management for iOS 管理插件可用于：

- 为移动设备创建组安全策略。
- 远程配置使用 Exchange ActiveSync 协议连接的设备（也叫 “EAS 设备”）。
- 远程配置使用 iOS MDM 协议连接的设备（也叫 “iOS MDM 设备”）。
- 接受用户移动设备操作的报告和统计信息。

有关通过 iOS MDM 和 Exchange ActiveSync 协议将移动设备连接到 Kaspersky Security Center 的更多详细信息，请参阅 *Kaspersky Security Center 帮助*。

默认情况下，部署 Kaspersky Security Center 时会安装 Kaspersky Device Management for iOS 管理插件。该插件不需要单独安装。

硬件和软件要求

本节列出用于在移动设备上部署应用程序的管理员计算机的硬件和软件要求，以及 Kaspersky Security for Mobile 支持的移动设备操作系统。

管理员计算机的硬件和软件要求

若要部署 Kaspersky Security for Mobile 综合解决方案，管理员的计算机必须满足 Kaspersky Security Center 的硬件要求。有关使用 Kaspersky Security Center 的硬件要求的详情，请参阅*"Kaspersky Security Center 帮助"*。

若要使用 Kaspersky Endpoint Security for Android 的管理插件，必须在管理员的计算机上安装 Kaspersky Security Center 12 或更高版本的管理控制台。

若要使用 Kaspersky Device Management for iOS 管理插件，管理员的计算机必须满足以下软件要求：

- Kaspersky Security Center 12 或更高版本的管理控制台
- Exchange 服务器组件
- iOS MDM 服务器组件
- SSE2 版本或最近版本的指南

若要通过管理服务器部署 Kaspersky Endpoint Security for Android 移动应用程序，管理员的计算机必须满足以下软件要求：

- Kaspersky Security Center 12 或更高版本
- Kaspersky Endpoint Security for Android 管理插件

从相关在线商店部署 Kaspersky Endpoint Security for Android 移动应用程序时，对管理员的计算机没有任何软件要求。

Kaspersky Endpoint Security for Android 移动应用也可以作为 Kaspersky Endpoint Security Cloud 远程管理系统（版本 6.0 及以上）的一部分运行。有关通过 Kaspersky Endpoint Security Cloud 使用应用程序的更多详细信息，请参阅*"Kaspersky Endpoint Security Cloud 帮助"*。

Kaspersky Endpoint Security for Android 移动应用可以与第三方 EMM 系统一起工作：

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

支持安装 Kaspersky Endpoint Security for Android 应用程序的用户移动设备的硬件和软件要求

Kaspersky Endpoint Security for Android 应用程序具有以下硬件和软件要求：

- 智能手机或平板电脑的分辨率为 320x480 像素或更高
- 设备的主存储器具有 65 MB 的可用空间
- Android 5.0–13（包括 Android 12L，但不包括 Go Edition）
- x86、x86-64、Arm5、Arm6、Arm7 或 Arm8 处理器架构

应用程序只能安装到设备的主存储器。

iOS MDM 配置文件的硬件和软件需求

对于 iOS MDM 配置文件，设备必须满足以下硬件和软件需求：

- iOS 10.0-15.0 或 iPadOS 13-15
- 因特网连接

已知问题和注意事项

Kaspersky Endpoint Security for Android 有许多对应用程序运行非关键的已知问题。

安装应用程序时的已知问题

- Kaspersky Endpoint Security for Android 仅安装在设备的主内存中。
- 在运行 Android 7.0 的设备上，当 Kaspersky Endpoint Security for Android 被禁止覆盖其他窗口时，当试图禁用 Kaspersky Endpoint Security for Android 的管理员权限时可能发生错误。该问题是因一个众所周知的 Android 7 缺陷 导致。
- 在运行 Android 7.0 或更新版本的设备上，Kaspersky Endpoint Security for Android 不支持多窗口模式。
- Kaspersky Endpoint Security for Android 与运行 Chrome 操作系统的 Chromebook 设备不兼容。
- Kaspersky Endpoint Security for Android 与运行 Android (Go edition) 操作系统的设备不兼容。
- 当将 Kaspersky Endpoint Security for Android 应用程序与第三方 EMM 系统（例如，VMWare AirWatch）一起使用时，仅反病毒和 Web 保护组件可用。管理员可以在 EMM 系统控制台中配置反病毒和 Web 保护的设置。在这种情况下，有关应用程序运行的通知仅在 Kaspersky Endpoint Security for Android 应用程序的界面（报告）中可用。

升级应用程序版本时的已知问题

- 您只能将 Kaspersky Endpoint Security for Android 升级至最近的应用程序版本。Kaspersky Endpoint Security for Android 不能降级至较老版本。
- 若要使用独立安装包升级 Kaspersky Endpoint Security for Android，必须允许在用户的移动设备上安装来自未知来源的应用程序。
- 如果 Kaspersky Endpoint Security for Android 是从 Google Play 安装的，则可以通过 Google Play 更新。如果该应用程序是使用其他方法安装的，则不能通过 Google Play 更新。
- 如果通过 Kaspersky Security Center 安装了 Kaspersky Endpoint Security for Android，则可以通过 Kaspersky Security Center 更新。如果该应用程序是从 Google Play 安装的，则不能通过 Kaspersky Security Center 更新应用程序。
- 将管理插件升级到 Technical Release 33 后，Kaspersky Endpoint Security for Android 应用程序也必须升级到 Technical Release 33。否则，将无法在某些用户设备上激活 Samsung KNOX。

反病毒运行的已知问题

- 由于技术限制，Kaspersky Endpoint Security for Android 无法扫描大小为 2 GB 或更大的文件。在扫描期间，应用程序将跳过此类文件，而不会通知您此类文件被跳过。
- 要对设备进行信息尚未添加到反病毒数据库中的新威胁的附加分析，您必须启用卡巴斯基安全网络。*卡巴斯基安全网络 (KSN)* 是一种云服务基础设施，它提供对 Kaspersky 在线知识库的访问，该知识库包含有关文件、Web 资源和软件的信誉的信息。要使用 KSN，移动设备必须连接到互联网。
- 在某些情况下，在移动设备上从管理服务器更新反病毒数据库可能会失败。在这种情况下，请在管理服务器上运行反病毒数据库更新任务。
- 在某些设备上，Kaspersky Endpoint Security for Android 不会检测通过 USB OTG 连接的设备。无法对此类设备运行病毒扫描。
- 在运行 Android 11.0 或更高版本的设备上，用户必须授予“允许访问以管理所有文件”权限。
- 在运行 Android 7.0 或更新版本的设备上，病毒扫描运行计划的配置窗口可能显示不正确（管理元件未显示）。该问题是因一个众所周知的 Android 7 缺陷 导致。
- 在运行 Android 7.0 的设备上，扩展模式下的实时保护检测不到外部 SD 卡上存储的文件中的威胁。
- 在运行 Android 6.0 的设备上，Kaspersky Endpoint Security for Android 不检测下载恶意文件到设备内存的操作。当恶意文件运行时，或者在设备病毒扫描过程中，恶意软件可以被反病毒检测到。该问题因一个众所周知的 Android 6.0 缺陷 导致。要确保设备安全，建议配置计划病毒扫描。

Web 保护运行的已知问题

- 安卓设备上的 Web 保护仅在 Google Chrome 浏览器（包括自定义标签功能）、Huawei Browser 和 Samsung Internet Browser 中可用。如果工作配置文件被使用且 Web 保护仅为工作配置文件所启用，Samsung Internet Browser 中的 Web 保护不阻止移动设备上的网站。
- 工作配置文件中的 Kaspersky Endpoint Security 仅扫描 HTTPS 流量中的网站域。如果应用在工作配置文件中被安装，恶意和钓鱼网站可能不被阻止。如果域是受信任的，Web 保护可以跳过威胁（例如，`https://trusted.domain.com/phishing/`）。如果域是不受信任的，Web 保护阻止恶意和钓鱼网站。
- 要使 Web 保护工作，您必须启用卡巴斯基安全网络。Web 保护会基于有关网站信誉和类别的 KSN 数据阻止网站。
- 如果通过以下方式打开禁止的网站，在运行 Android 6.0 并安装 Google Chrome 51 版（或任何更早版本）的设备上，Web 保护可能会保持解除阻止这些网站（该问题是因一个众所周知的 Google Chrome 缺陷导致）：
  - 通过搜索结果。
  - 通过书签列表。
  - 通过搜索历史记录。
  - 使用网址自动填写功能。
  - 在 Google Chrome 中的新标签页中打开网站。
- 如果通过 Google 搜索结果打开禁止的网站，当浏览器设置中启用了“**Merge Tabs and Apps**”功能时，这些网站可能在 Google Chrome 50 版（或任何更早版本）中保持解除阻止。该问题是因一个众所周知的 Google Chrome 缺陷导致。
- 如果用户通过第三方应用（例如，通过即时通讯客户端应用）打开受阻止类别中的网站，则这些网站可能在 Google Chrome 中保持解除阻止。该问题关乎可访问功能服务与 Chrome 自定义标签功能如何配合使用。

- 如果用户在后台模式下通过上下文菜单或通过第三方应用（例如，即时通讯客户端应用）打开禁止的网站，这些网站可能会在 Samsung Internet Browser 中保持解除阻止。
- 必须将 Kaspersky Endpoint Security for Android 设置为可访问功能以确保 Web 保护能正常运行。
- 当在 Web 保护设置中输入网址时，请遵守以下规则：
  - 对于安卓设备，采用常规表达式格式指定地址（例如，`http:\/\/www\.example\.com.*`）。
  - 对于 iOS MDM 设备，指定 HTTP 或 HTTPS 数据传输协议（例如，`http://www.example.com`）。
- 当刷新页面时，Samsung Internet Browser 在“**仅允许列出的网站**”Web 保护模式下可能会阻止允许的网站。如果常规表达式包含高级设置（例如，`^https?:\/\/example\.com\/pictures\/`），则会阻止网站。建议使用不含附加设置的常规表达式（例如，`^https?:\/\/example\.com`）。

反盗窃运行的已知问题

- 为了将命令及时传送到安卓设备，应用会使用 Firebase Cloud Messaging (FCM) 服务。如果未配置 FCM，将仅在与 Kaspersky Security Center 同步期间按照策略中定义的计划（例如，每 24 小时）将命令传送到设备。
- 要锁定设备，必须将 Kaspersky Endpoint Security for Android 设置为设备管理员。
- 要锁定运行 Android 7.0 或更高版本的设备，必须将 Kaspersky Endpoint Security for Android 设置为可访问功能。
- 在某些设备上，如果设备上启用了低电量模式，反盗窃命令可能无法执行。该缺陷在 Alcatel 5080X 上被确认。
- 要定位运行 Android 10.0 或更高版本的设备，用户必须为设备定位授予“始终”权限。
- 要使用运行 Android 11.0 或更高版本的设备拍摄面部照片，用户必须授予“使用应用程序时”权限才能访问摄像头。

应用程序控制运行的已知问题

- 必须将 Kaspersky Endpoint Security for Android 设置为无障碍功能才能确保“应用程序控制”正常运行。
- 要使应用程序控制（应用程序类别）工作，您必须启用卡巴斯基安全网络。应用程序控制会基于 KSN 中可用的数据确定应用程序的类别。要使用 KSN，移动设备必须连接到互联网。对于应用程序控制，您可以将单个应用程序添加到阻止和允许的应用程序列表。在这种情况下，无需 KSN。
- 当配置应用程序控制时，建议清除“**阻止系统应用程序**”复选框。阻止系统应用程序可能会导致设备运行问题。

配置电子邮件时的已知问题

- 远程配置邮箱仅在以下设备上可用：
  - iOS MDM 设备。
  - 三星设备 (Exchange ActiveSync)。
  - 安装了 TouchDown 邮件客户端的安卓设备。

在 Kaspersky Endpoint Security for Android 的先前版本中，您可以使用 Kaspersky Security Center 在用户设备上远程配置 TouchDown 配置文件设置。Kaspersky Endpoint Security for Android Service Pack 4 不再支持 TouchDown。对于更多详情，请参考 *Symantec 技术支持网站*。

升级 Kaspersky Endpoint Security for Android 插件后，策略中的 TouchDown 设置被隐藏但被保存。当有新设备被连接时，TouchDown 设置将在应用策略后被配置。

在策略被修改和保存后，TouchDown 设置将被删除。用户设备上的 TouchDown 设置在应用策略后将被清除。

配置设备解锁密码强度时的已知问题

- 在运行 Android 10.0 或更高版本的设备上，Kaspersky Endpoint Security 将密码强度要求解析为系统值之一：中或高。

  如果所需的密码长度是 1 到 4 个符号，该应用程序会提示用户设置中强度密码。它必须是没有重复并且没有顺序（例如 1234）的数字（PIN），或者是字母数字。PIN 或密码必须至少有 4 个字符长。

  如果所需的密码长度是 5 个或更多符号，该应用程序会提示用户设置高强度密码。它必须是没有重复并且没有顺序的数字（PIN），或者是字母数字（密码）。PIN 必须至少为 8 位数字；密码必须至少有 6 个字符长。

- 在运行 Android 10.0 或更高版本的设备上，使用指纹解锁屏幕只能在工作配置文件中管理。

- 在运行 Android 7.1.1 的设备上，如果解锁密码不符合企业安全需要（合规性控制），当尝试通过 Kaspersky Endpoint Security for Android 更改解锁密码时，“设置”系统应用可能无法正常工作。该问题是因一个众所周知的 Android 7.1.1 缺陷 导致。这种情况下，仅可使用设置系统 app 来更改解锁密码。

- 在一些运行 Android 6.0 或更新版本的设备上，如果设备数据被加密，当输入屏幕解锁密码时可能发生错误。该问题与 MIUI 固件的辅助功能服务的特定功能有关。

配置 Wi-Fi 时的已知问题

- 在运行 Android 版本 8.0 或更新版本的设备上，Wi-Fi 代理服务器设置无法由策略重定义。然而，您可以在移动设备上手动为 Wi-Fi 网路配置代理服务器设置。

配置 APN 时的已知问题

- 只有 iOS MDM 设备或三星设备支持远程配置 APN。

- 在“**手机通信**”区域中为 iOS MDM 设备配置 APN。“**APN**”区域已弃用。在配置 APN 设置之前，确保清除“**APN**”区域中的“**将设置应用于设备**”复选框。

防火墙的已知问题

- 防火墙只能在三星设备上使用。

配置 VPN 时的已知问题

- 远程配置 VPN 仅在以下设备上可用：
  - iOS MDM 设备。
  - 三星设备。

使用容器时的已知问题

- 在 Kaspersky Security for Mobile Service Pack 3 Maintenance Release 2 中，不再支持为移动应用程序创建容器。但是，在早期版本的应用程序中创建的容器可以添加到 Android 设备。
- 要安装集装式应用，用户的移动设备上必须允许安装来自未知来源的应用程序。关于不使用 Google Play 安装应用的详情，请参考 *Android 帮助向导*。
- 对于Android 设备上包含多于 65,536 个方法（multidex 配置）的应用，不支持应用程序集装。

应用程序删除保护的已知问题

- 必须将 Kaspersky Endpoint Security for Android 设置为设备管理员。
- 要保护在运行安卓 7.0 或更高版本的设备上的应用程序不会被卸载，必须将 Kaspersky Endpoint Security for Android 设置为可访问功能。
- 在某些小米和华为设备上，Kaspersky Endpoint Security for Android 卸载保护不工作。该问题是由小米的 MIUI 7 和 8 固件以及华为的 EMUI 固件的特定功能导致。

配置设备限制时的已知问题

- 在运行 Android 10.0 或更高版本的设备上，不支持禁止使用 Wi-Fi 网络。
- 在运行 Android 10.0 或更高版本的设备上，不能完全禁止使用摄像头。
- 在运行 Android 11 或更高版本的设备上，必须将 Kaspersky Endpoint Security for Android 设置为无障碍功能。Kaspersky Endpoint Security for Android 会提示用户通过初始配置向导将该应用程序设置为可访问功能。用户可以跳过此步骤或以后在设备设置中禁用此服务。如果是这种情况，您将无法限制使用摄像头。

向移动设备发送命令时的已知问题

- 在运行 Android 12 或更高版本的设备上，如果用户授予了“使用大致位置”权限，Kaspersky Endpoint Security for Android 应用程序首先会尝试获取精确的设备位置。如果获取不成功，则只有在不超过 30 分钟前已收到设备的大致位置时，才会返回该位置。否则，“**定位设备**”命令将失败。

Android 工作配置文件的已知问题

- 如果使用策略创建安卓工作配置文件，用户必须为安装在运行 Android 11 或更高版本的设备上并与工作配置文件相关的 Kaspersky Endpoint Security for Android 授予“允许访问以管理所有文件”权限。

特定设备的已知问题

- 在某些设备（例如，华为、魅族和小米）上，您必须为 Kaspersky Endpoint Security for Android 授予自动启动权限，或手动将其添加到在操作系统启动时启动的应用程序列表中。如果未将该应用程序添加到列表，在移动设备重新启动后，Kaspersky Endpoint Security for Android 会停止执行其所有功能。此外，如果设备已锁定，您无法使用命令解锁设备。您只能通过使用一次性解锁码解锁设备。

- 在运行 Android 6.0 或更高版本的某些设备（例如，魅族和 Asus）上，在加密数据和重启安卓设备之后，您必须输入数字密码才能解锁设备。如果用户使用图形密码解锁设备，您必须将图形密码转换为数字密码。对于更多转换图形密码到数字密码的详情，请参考移动设备生产商的技术支持网站。该问题关乎可访问功能服务的操作。

- 在某些运行 Android 5.X 的华为设备上，将 Kaspersky Endpoint Security for Android 设置为无障碍功能后，可能会显示一条有关缺少适当权限的错误消息。要隐藏此消息，请在设备设置中将该应用程序设置为受保护应用程序。

- 在某些运行 Android 5.X 或 6.X 的华为设备上，当为 Kaspersky Endpoint Security for Android 启用低电量模式时，用户可以手动终止该应用程序。那样之后，用户设备变成无保护状态。该问题是由于华为软件的一些功能导致的。若要恢复设备保护，请手动运行 Kaspersky Endpoint Security for Android。建议在设备设置中对 Kaspersky Endpoint Security for Android 禁用低电量模式。

- 在运行基于 Android 7.0 的 EMUI 固件的华为设备上，用户可以隐藏关于 Kaspersky Endpoint Security for Android 保护状态的通知。该问题是由于华为软件的一些功能导致的。

- 在某些小米设备上，当在策略中设置超过 5 个字符的密码长度时，用户将被提示更改屏幕解锁密码而不是 PIN 码。您设置的 PIN 码不能超过 5 个字符。该问题是由于小米软件的一些功能导致的。

- 在运行基于 Android 6.0 的 MIUI 固件的小米设备上，Kaspersky Endpoint Security for Android 图标可能在状态栏中隐藏。该问题是由于小米软件的一些功能导致的。建议在“通知”设置中允许显示通知图标。

- 在一些运行 Android 6.0.1 的 Nexus 设备上，正常操作所需的权限无法通过 Kaspersky Endpoint Security for Android 快速启动向导授予。该问题由众所周知的 Google 的安卓安全补丁缺陷导致。为确保正常运行，必须在设备设置中手动授予所需权限。

- 在某些运行 Android 7.0 或更高版本的三星设备上，当用户尝试配置不受支持的方法（例如，图形密码）来解锁设备时，如果满足以下条件，设备可能会锁定：Kaspersky Endpoint Security for Android 卸载保护已启用并且设置了屏幕解锁密码长度要求。要解锁设备，您必须发送特殊命令到设备。

- 在某些三星设备上，无法阻止使用指纹解锁屏幕。

- 在某些三星设备上，如果设备连接到 3G/4G 网络，启用了省电模式并限制后台数据，则无法启用 Web 保护。建议在“低电量模式”设置中禁用限制后台进程的功能。

- 在某些三星设备上，如果解锁密码不符合企业安全要求，Kaspersky Endpoint Security for Android 不会阻止使用指纹解锁屏幕。

- 在执行反盗窃命令（如，定位、设备锁定、解锁和拍摄面部照片）后，某些三星设备上可能会删除常规证书和 VPN 证书。必须重新安装证书才能继续。该问题源于 Mobile Device Fundamentals Protection Profile（MDFPP) 安全标准。

- 在某些荣耀和华为设备上，您无法限制蓝牙的使用。当 Kaspersky Endpoint Security for Android 试图限制蓝牙使用时，操作系统显示包含拒绝或允许该限制的选项的通知。用户可以拒绝该限制并继续使用蓝牙。

- 在某些三星设备上，从独立安装包安装或更新 Kaspersky Endpoint Security 后，KNOX MDM 配置文件激活不可用。

- 在 Blackview 设备上，用户可以清除 Kaspersky Endpoint Security for Android 应用程序的内存。结果是，设备保护和管理将被禁用，所有已定义的设置都将无效，并且 Kaspersky Endpoint Security for Android 应用程序从无障碍功能中删除。这是因为此供应商的设备为自定义的“最近使用的应用”屏幕应用程序提供了提升的权

限。此应用程序可以覆盖 Kaspersky Endpoint Security for Android 设置并且无法替换，因为它是 Android 操作系统的一部分。

- 在某些运行 Android 11 的设备上，Kaspersky Endpoint Security for Android 应用程序在启动后立即崩溃。该问题由一个众所周知的 Android 11 缺陷 导致。

应用程序在 Android 13 中运行的已知问题

- 在 Android 13 中，用户可以使用前台服务任务管理器来阻止 Kaspersky Endpoint Security 在后台运行。这是由 Android 13 中的一个众所周知的问题 导致的。
- 在 Android 13 中，开始初始应用配置时会请求发送通知的权限。这是 Android 13 操作系统的特性所致。

部署

本帮助部分面向安装 Kaspersky Security for Mobile 的专家，以及向使用 Kaspersky Security for Mobile 的组织提供技术支持的专家。

解决方案架构

Kaspersky Security for Mobile 包括以下组件：

- Kaspersky Endpoint Security for Android 移动应用程序

  Kaspersky Endpoint Security for Android 应用可确保移动设备抵御 Web 威胁、病毒和构成威胁的其他程序的侵害。它支持移动设备与 Kaspersky Security Center 管理服务器之间使用 Firebase Cloud Messaging 进行交互。

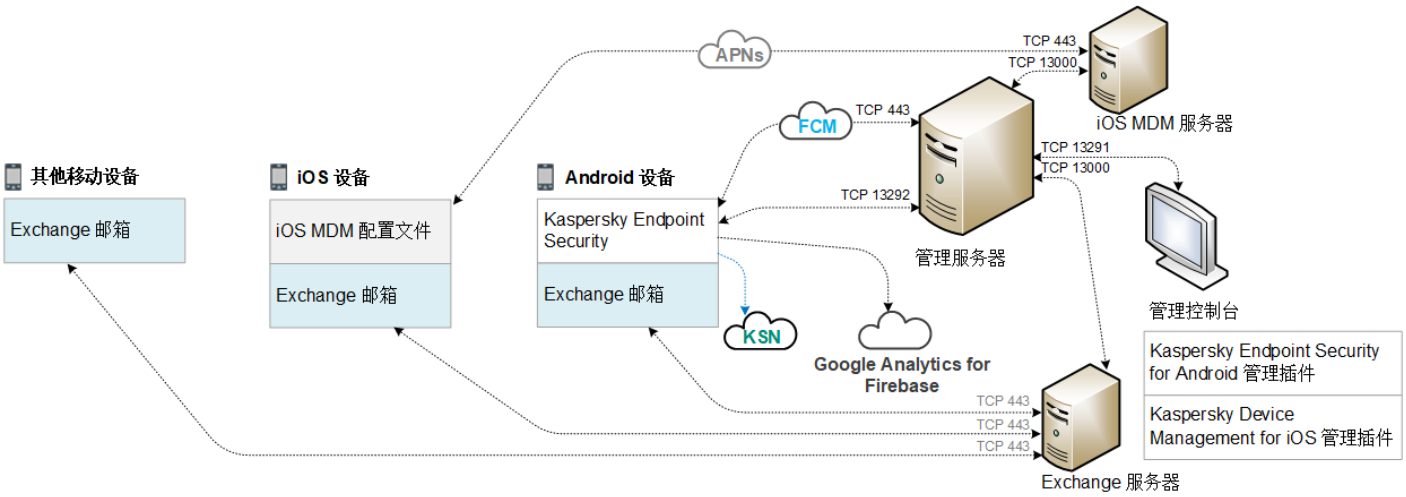
- Kaspersky Endpoint Security for Android 管理插件。

  Kaspersky Endpoint Security for Android 的管理插件提供界面，用于通过 Kaspersky Security Center 管理控制台，管理移动设备以及安装在这些设备上的移动应用程序。

- Kaspersky Device Management for iOS 管理插件

  Kaspersky Device Management for iOS 的管理插件提供了界面，用于通过 Kaspersky Security Center 管理控制台管理通过 iOS MDM 和 Exchange ActiveSync 协议连接的移动设备。

Kaspersky Security for Mobile 集成解决方案的基础结构如下图所示。



Kaspersky Security for Mobile 的基础架构

有关管理控制台、管理服务器、Exchange 服务器和 iOS MDM 服务器的详细信息，请参阅 *Kaspersky Security Center 帮助*。

常见集成解决方案部署方案

本节涵盖了 Kaspersky Security for Mobile 集成解决方案的常见部署方案。

可以使用不同的部署方案来在 Android 设备和 iOS 设备上部署集成解决方案。如果组织使用了运行不同操作系统的移动设备，则应按照相应的部署方案，分别为每种操作系统安装应用程序。

Kaspersky Endpoint Security for Android 的部署方案

Kaspersky Endpoint Security for Android 可通过多种方式部署在企业网络中的移动设备上。您可以使用最适合您组织的部署方式，或者结合使用多种部署方案。

有关在 Kaspersky Endpoint Security Cloud 中部署 Kaspersky Endpoint Security for Android 的详细信息，请参阅 *Kaspersky Endpoint Security Cloud 帮助*。

通过 Kaspersky Security Center 部署 Kaspersky Endpoint Security for Android

您可以使用以下方法通过 Kaspersky Security Center 部署 Kaspersky Endpoint Security for Android：

- 发送包含 Google Play 链接的邮件（推荐）
- 发送包含独立应用程序包链接的邮件

使用 Google Play 部署 Kaspersky Endpoint Security for Android 包括从管理控制台向设备用户发送包含 Google Play 链接的邮件。

通过提供的独立包部署Kaspersky Endpoint Security for Android 包括由管理员执行的以下几个步骤：

1. 创建应用程序安装包。
2. 配置安装包设置。

3. 创建独立安装包。

4. 发送消息，其中包含用于将独立安装包下载到 Android 用户设备的链接。可使用群发邮件。

用户在收到包含 Google Play 链接或用于从 Kaspersky Security Center Web Server 下载安装包的链接的邮件后，在移动设备上安装 Kaspersky Endpoint Security for Android。无需任何其他准备，即可开始使用应用程序。

从 Google Play 部署 Kaspersky Endpoint Security for Android

如果无法进行远程安装，则建议使用 Google Play 部署方案。

设备用户可从 Google Play 独立地安装 Kaspersky Endpoint Security for Android。用户从 Google Play 下载移动应用程序分发包，然后在设备上安装应用程序。在设备上安装应用程序之后，在能够开始使用它之前，您还需要进行其他准备工作：配置与管理服务器的连接设置以及安装常规证书。

通过 KNOX Mobile Enrollment 部署 Kaspersky Endpoint Security for Android

部署 Kaspersky Endpoint Security for Android 包括将 KNOX MDM 配置文件添加到移动设备。KNOX MDM 配置文件包含指向 Kaspersky Security Center Web 服务器或其他服务器上部署的应用程序的链接。在移动设备上安装应用程序后，您还必须安装一个常规证书。

您可以在“三星 KNOX”部分中了解如何通过 KNOX Mobile Enrollment 安装。

iOS MDM 配置文件的部署方案

iOS MDM 配置文件 是一个包含用于将运行 iOS 的移动设备连接到 Kaspersky Security Center 的设置的配置文件。安装 iOS MDM 配置文件并与 Kaspersky Security Center 同步后，设备将成为受管设备。移动设备通过 Apple 推送通知服务 (APN) 进行管理。有关安装 iOS MDM 配置文件和使用 APNs 的详细信息，请参阅 *Kaspersky Security Center 帮助*。

使用 iOS MDM 配置文件，您可以：

- 使用组策略远程配置 iOS MDM 设备的设置。
- 发送设备锁定和数据擦除命令。
- 远程安装 Kaspersky 应用程序和其他第三方应用程序。

iOS MDM 配置文件可通过多种方式部署在企业网络中的移动设备上。您可以使用最适合您组织的部署方式，或者结合使用多种部署方案。

在部署 iOS MDM 配置文件之前，管理员必须执行以下操作：

1. 安装 iOS MDM 服务器。
2. 获取 Apple 推送通知服务证书（APN 证书）。
3. 将 APN 证书安装到 iOS MDM 服务器。

有关安装 iOS MDM 服务器和使用 APNs 证书的详细信息，请参阅 *Kaspersky Security Center 帮助*。

有关在 Kaspersky Endpoint Security Cloud 中部署 iOS MDM 配置文件的详细信息，请参阅 *Kaspersky Endpoint Security Cloud 帮助*。

通过 Kaspersky Security Center 部署 iOS MDM 配置文件

通过发送包含用于下载 iOS MDM 配置文件的链接的邮件，可以通过 Kaspersky Security Center 部署 iOS MDM 配置文件。可使用群发邮件。

用户在收到包含 Kaspersky Security Center Web Server 链接的邮件后，可将 iOS MDM 配置文件安装到移动设备上。无需为 iOS MDM 配置文件进行其他准备工作。

有关创建 iOS MDM 配置文件的详细信息，请参阅 *Kaspersky Security Center 帮助*。

准备管理控制台以便部署集成解决方案

本节提供有关准备管理控制台以便部署集成解决方案的说明。

配置连接移动设备的管理服务器设置

要让移动设备能够连接到管理服务器，在安装 Kaspersky Endpoint Security 移动应用程序之前，请在管理服务器属性中配置移动设备连接设置。

配置连接移动设备的管理服务器设置：

1. 在管理服务器的上下文菜单中，选择“**属性**”。
   “管理服务器设置”窗口将开启。
2. 选择“**服务器连接设置 → 其他端口**”。
3. 选中“**打开移动设备端口**”复选框。
4. 在“**移动设备端口**”字段中，指定移动设备连接至管理服务器的端口。
   默认情况下使用 13292。如果清空了“**打开移动设备端口**”选框，或者指定了错误的连接端口，移动设备将无法连接至管理服务器。
5. 在“**用于激活移动客户端的端口**”字段中，指定移动设备用于连接到管理服务器以便激活 Kaspersky Endpoint Security for Android 应用程序的端口。默认情况下使用 13292。
6. 单击“**确定**”。

在管理控制台中显示“移动设备管理”文件夹

通过在管理控制台中显示“**移动设备管理**”文件夹，您可以查看管理服务器管理的移动设备列表，配置移动设备管理设置，在用户的移动设备上安装证书。

*在管理控制台中显示“**移动设备管理**”文件夹：*

1. 在管理服务器的上下文菜单中，选择“**查看**” → “**配置界面**”。
2. 在打开的窗口中，选择“**显示移动设备管理**”选框。
3. 单击“**确定**”。

重新启动管理控制台之后，“**移动设备管理**”文件夹将显示在管理控制台树中。

创建管理组

若要集中配置用户移动设备上安装的 Kaspersky Endpoint Security for Android 应用程序，必须将组策略应用至这些设备。

若要将策略应用于设备组，建议您在用户设备上安装移动应用程序之前，先在“**受管设备**”中为这些设备创建单独的组。

创建管理组后，建议配置选项以将要安装应用程序的设备自动分配到此组。然后使用组策略配置所有设备通用的设置。

若要创建管理组，执行以下步骤：

1. 在控制台树中，选择“**受管设备**”文件夹。
2. 在“**受管设备**”文件夹或子文件夹的工作区中，选择“**设备**”选项卡。
3. 单击“**新建组**”按钮。

   这将打开可供您创建新组的窗口。
4. 在“**组名称**”窗口中输入组名称，然后单击“**确定**”。

控制台树中将显示带有指定名称的新管理组文件夹。有关使用管理组的详细信息，请参阅 *Kaspersky Security Center 帮助*。

为设备自动分配至管理组创建规则

您可以集中管理在用户移动设备上安装的 Kaspersky Endpoint Security for Android 应用程序的设置，但前提是这些设备必须属于先前创建的、已经配置了组策略的管理组。

如果未配置用于自动将在网络上检测到的移动设备分配至管理组的规则，则在设备第一次与管理服务器同步时，会将该设备自动发送到管理控制台中的“**其他**” → “**网络轮询**” → “**域**” → “**KES10**”文件夹中。组策略不应用至此设备。

若要创建规则自动将移动设备分配至管理组，则遵循以下步骤：

1. 在控制台树中，选择“**未分配的设备**”文件夹。
2. 从“**未分配的设备**”文件夹的上下文菜单中，选择“**属性**”。

   将显示“**属性: 未分配的设备**”窗口。
3. 在“**移动设备**”区域中单击“**添加**”开始创建自动将设备分配至管理组的规则。

   此时将打开“**新规则**”窗口。

4. 输入规则名称。

5. 在移动设备上安装了 Kaspersky Endpoint Security for Android 移动应用程序之后，指定应将移动设备分配到的管理组。若要执行操作，单击“**将设备移动至组**”字段右侧的“**浏览**”，然后在显示的窗口中选择组。

6. 在“**规则应用**”区域中选择“**为每个设备运行一次**”。

7. 选中“**仅移动未添加至管理组的设备**”复选框，防止在应用规则时将选定组内的移动设备移动至其他管理组。

8. 选择“**启用规则**”选框，以便规则可以应用至新检测到的设备。

9. 打开“**应用程序**”区域并执行以下操作：

   a. 选择“**操作系统版本**”复选框。

   b. 选择要分配至指定组的一个或多个类型的设备操作系统：Android 或 iOS。

10. 单击“**确定**”。

新创建的规则将显示在“**未分配的设备**”文件夹属性窗口的“**移动设备**”区域的设备分配规则列表中。

根据规则，Kaspersky Security Center 会将所有满足要求的设备从“**未分配的设备**”文件夹中分配至选定组。也可以手动将先前分配至“**未分配的设备**”文件夹中的移动设备分配至“**受管设备**”文件夹的所需管理组中。有关管理组管理的详细信息，以及针对未分配设备的操作详情，请参阅 *Kaspersky Security Center 帮助*。

创建常规证书

您必须在管理控制台中创建用于识别移动设备用户的常规证书。

若要创建常规证书，请执行以下操作：

1. 在控制台树中，选择“**移动设备管理**”→“**证书**”文件夹。

2. 在“**证书**”文件夹的工作区中，单击“**添加证书**”按钮，启动“证书安装向导”。

3. 在向导的“**证书类型**”窗口中，选择“**常规证书**”选项。

4. 在向导的“**用户选择**”窗口中，指定您要为其创建常规证书的用户。

5. 在向导的“**证书来源**”窗口中，选择创建常规证书的方法。

   - 若要自动使用管理服务器工具创建常规证书，请选择“**通过管理服务器工具颁发证书**”。
   - 若要向用户分配先前创建的证书，请选择“**指定证书文件**”选项。单击“**指定**”按钮，打开“**证书**”窗口并在其中指定证书文件。

     如果您不想指定移动设备的类型和通知用户有关证书创建的方法，请清除“**发布证书**”选框。

6. 在向导的“**用户通知方法**”窗口中，指定有关使用短消息或通过电子邮件通知移动设备用户有关证书创建的设置。

7. 在向导的“**生成证书**”窗口中，单击“**已完成**”，完成证书安装向导。

这样，证书创建向导创建用户可以安装在移动设备上的常规证书。若要获取证书，请启动移动设备与管理服务器的同步。有关创建证书和配置证书颁发规则的更多信息，请参阅*Kaspersky Security Center 帮助*。

安装 Kaspersky Endpoint Security for Android

本节介绍在企业网络上部署 Kaspersky Endpoint Security for Android 的方法。

权限

对于应用程序的所有功能，Kaspersky Endpoint Security for Android 将提示用户授予所需权限。在完成安装向导时以及在安装后使用应用程序的各项功能之前，Kaspersky Endpoint Security for Android 将提示授予必需权限。如果未提供必需权限，将无法安装 Kaspersky Endpoint Security for Android。

在某些设备（例如，华为、魅族和小米）上，您必须手动将 Kaspersky Endpoint Security for Android 添加到在操作系统启动时启动的应用程序列表中。如果未将该应用程序添加到列表，在移动设备重新启动后，Kaspersky Endpoint Security for Android 会停止执行其所有功能。

在运行 Android 11 或更高版本的设备上，必须禁用"**如果不使用应用程序则移除权限**"系统设置。否则，在几个月未使用该应用程序后，系统会自动重置用户授予该应用程序的权限。

在 Kaspersky Endpoint Security for Android Service Pack 4 Update 4（内部版本 10.8.0.103）中，不再支持来电和短信过滤或 SIM 卡监控功能。此种情况下，Kaspersky Endpoint Security for Android 不提示用户 SMS 管理权限。要启用来电和短信过滤以及 SIM 卡监控的所有功能，您必须使用早期版本的 Kaspersky Endpoint Security for Android。

Kaspersky Endpoint Security for Android 所需的权限

权限	应用程序功能
电话（适用于 Android 5.0 – 9.X）	连接到 Kaspersky Security Center（设备 ID）
存储（必需）	反病毒
管理所有文件的访问权限（适用于 Android 11 或更高版本）	反病毒
附近的蓝牙设备（适用于 Android 12 或更高版本）	限制使用蓝牙
通知（适用于 Android 13）	通知用户安全问题和应用程序事件
允许在后台运行（适用于 Android 12 或更高版本）	确保应用程序持续运行。如果未授予权限，应用程序可能会从内存中卸载并且无法重新启动。
设备管理员（必需）	反盗窃 – 锁定设备（仅适用于安卓 5.0 – 6.X）
	反盗窃 – 使用前置摄像头拍摄面部照片
	反盗窃 – 发出警报声
	反盗窃 – 恢复出厂设置
	密码保护
	应用程序卸载保护
	安装安全证书

	应用程序控制
	管理 KNOX（仅适用于三星设备）
	配置 Wi-Fi
	配置 Exchange ActiveSync
	限制使用摄像头、蓝牙和 Wi-Fi
摄像头	反盗窃 – 使用前置摄像头拍摄面部照片 在运行 Android 11.0 或更高版本的设备上，用户必须在收到提示时授予“使用应用程序时”权限。
定位	反盗窃 – 定位设备 在运行 Android 10.0 或更高版本的设备上，用户必须在收到提示时授予“始终”权限。
可访问功能	反盗窃 – 锁定设备（仅适用于安卓 7.0 或更高版本）
	Web 保护
	应用程序控制
	应用程序卸载保护（仅适用于安卓 7.0 或更高版本）
	显示 Kaspersky Endpoint Security for Android 的警告（仅适用于 Android 10.0 或更高版本）
	限制使用摄像头（仅适用于 Android 11 或更高版本）

使用 Google Play 链接安装 Kaspersky Endpoint Security for Android

Kaspersky Endpoint Security for Android 安装到其用户账户已添加到 Kaspersky Security Center 的用户的移动设备上。有关 Kaspersky Security Center 中的用户账户的详细信息，请参阅 Kaspersky Security Center 帮助。

Kaspersky Security for Mobile 让您可以使用 Google Play 链接通过 Kaspersky Security Center 安装应用程序（推荐方法）。

用户将收到指向 Google Play 的链接。可通过执行 Android 平台上的标准安装步骤，安装该应用程序。安装后不需要对 Kaspersky Endpoint Security for Android 进行其他配置。

某些华为和荣耀设备未安装 Google 服务，因此无法访问 Google Play 中的应用程序。如果某些华为和荣耀设备用户无法从 Google Play 安装应用，应指导他们从华为应用市场安装应用。

链接包含以下数据：

- Kaspersky Security Center 同步设置。
- 常规证书。

- 接受 Kaspersky Endpoint Security for Android 最终用户授权许可协议以及附加声明的条款和条件的指示。如果管理员在管理控制台中接受授权许可协议以及附加声明的条款，则 Kaspersky Endpoint Security for Android 会在安装应用程序时跳过接受步骤。

要使用 Google Play 链接通过 Kaspersky Security Center 安装 Kaspersky Endpoint Security for Android，请执行以下操作：

1. 在控制台树中，选择“**移动设备管理**”→“**移动设备**”文件夹。
2. 在“**移动设备**”文件夹的工作区中，单击“**添加移动设备**”按钮。

   这将启动新建移动设备连接向导。按照向导的描述进行操作。
3. 在向导的“**操作系统**”窗口中，选择“**安卓**”。

   Kaspersky Security Center 会检查管理插件更新。如果 Kaspersky Security Center 检测到更新，您可以安装新版本的管理插件。更新管理插件后，您可以接受 Kaspersky Endpoint Security for Android 的最终用户授权许可协议 (EULA) 以及附加声明的条款和条件。如果管理员在管理控制台中接受授权许可协议以及附加声明，则 Kaspersky Endpoint Security for Android 会在安装应用程序时跳过接受步骤。此功能在 Kaspersky Security Center 12 版本中提供。
4. 在 **Kaspersky Endpoint Security for Android 安装方法**页面上，**使用 Google Play 链接**选择应用程序安装方法。
5. 在向导的“**选择用户**”页面上，选择要将 Kaspersky Endpoint Security for Android 安装到其移动设备的一个或多个用户。

   如果用户不在列表中，您可以添加新用户账户，而不必退出新建移动设备连接向导。
6. 在向导的“**证书来源**”窗口上，选择用于保护 Kaspersky Endpoint Security for Android 和 Kaspersky Security Center 之间的数据传输的证书来源：
   - **通过管理服务器工具颁发证书。**在这种情况下，将自动创建证书。
   - **指定证书文件**。在这种情况下，必须提前准备您自己的证书，然后在向导的窗口中选择它。如果您要将 Kaspersky Endpoint Security for Android 安装到多个移动设备，则无法使用此选项。必须为每个用户创建单独的证书。
7. 在向导的“**用户通知方法**”页面上，选择用于转发应用程序安装链接的通道：
   - 若要通过电子邮件发送链接，请选择“**发送指向 Kaspersky Endpoint Security 的链接**”，并在“**通过电子邮件**”区域中配置设置。确保在用户账户的设置中指定了电子邮件地址。
   - 若要通过短信发送链接，请选择“**发送指向 Kaspersky Endpoint Security 的链接**”，并在“**通过短信**”区域中配置设置。确保在用户账户的设置中指定了电话号码。
   - 若要使用二维码安装 Kaspersky Endpoint Security for Android，请选择“**显示安装包链接**”并使用移动设备的摄像头扫描二维码。
   - 如果列出的方法都不适合您，请选择“**显示安装包链接**” → “**复制**”，将用于安装 Kaspersky Endpoint Security for Android 的链接复制到剪贴板。使用任何可用的方法发送应用程序安装链接。您还可以使用 Kaspersky Endpoint Security for Android 的其他安装方法。
8. 单击“**完成**”关闭“新建移动设备连接向导”。

将 Kaspersky Endpoint Security for Android 安装到用户的移动设备后，您可以使用组策略来配置设备和应用程序的设置。如果设备丢失或被盗，您还可以向移动设备发送命令以便保护数据。

Kaspersky Endpoint Security for Android 的其他安装方法

您可以使用指向您自己的 Web 服务器的链接来安装 Kaspersky Endpoint Security for Android，或指示用户手动安装该应用程序。

从 Google Play 或华为应用市场手动安装

用户可以从 Google Play 或华为应用市场手动安装 Kaspersky Endpoint Security for Android。可通过执行 Android 平台的标准安装程序，安装该应用程序。用户使用他们自己的 Google 帐户安装应用程序。

有关从 Google Play 安装 Kaspersky Endpoint Security for Android 的详细信息，请参阅 Google 技术支持网站。

有关从华为应用市场安装 Kaspersky Endpoint Security for Android 的过程的详细信息，请参阅华为支持网站。

某些华为和荣耀设备未安装 Google 服务，因此无法访问 Google Play 中的应用程序。如果某些华为和荣耀设备用户无法从 Google Play 安装应用，应指导他们从华为应用市场安装应用。

从 Google Play 或华为应用市场安装 Kaspersky Endpoint Security for Android 之后，必须准备应用程序以供使用。为使用做准备的过程包括以下步骤：

1. 管理员使用任何适用方法（例如通过发送电子邮件），发送移动设备与管理服务器同步的设置（服务器地址和端口号）。
2. 用户可在运行初始配置向导时，或者在 Kaspersky Endpoint Security for Android 设置中，配置移动设备与管理服务器同步的设置。
3. 管理员为移动设备用户创建常规证书。
4. 用户接收自动通知，包含安装常规证书的提示。确认安装后，常规证书安装在移动设备上。

应在移动设备上启用 Internet 访问，以便与管理服务器同步。

有关如何配置移动设备与管理服务器同步以及如何接收常规证书的详细信息，请参阅"Kaspersky Security Center 帮助"。

下一次移动设备与管理服务器进行同步时，已安装有 Kaspersky Endpoint Security for Android 的用户移动设备将被移动至在应用程序安装期间指定的管理组（默认组为**"KES10"**）的**"其他" → "网络轮询" → "域"**文件夹中。您可以手动或使用自动分配规则将移动设备移动至您在"受管设备"文件夹中创建的管理组。

如果您想安装特定版本的 Kaspersky Endpoint Security for Android，此安装方法非常方便。

若要使用指向您自己的 Web 服务器的链接安装 Kaspersky Endpoint Security for Android，请执行以下操作：

1. 创建一个安装包并配置其设置。

   *安装包*是为通过 Kaspersky Security Center 远程安装 Kaspersky 应用程序创建的一组文件。

2. 创建独立安装包。

*独立安装包*是移动应用程序的安装文件，其中包含与管理服务器的应用程序连接的设置，以及接受 Kaspersky Endpoint Security for Android 最终用户授权许可协议 (EULA) 的条款和条件的指示。它是基于 Kaspersky Endpoint Security for Android 安装包创建的。独立安装包是一种特殊形式的安装包。

用户将收到指向托管 Kaspersky Endpoint Security for Android 的独立安装包的 Web 服务器的链接。若要安装应用程序，用户必须运行 APK 文件。安装后不需要对 Kaspersky Endpoint Security for Android 进行其他配置。

若要使用指向您自己的 Web 服务器的链接安装 Kaspersky Endpoint Security for Android，必须允许在用户的移动设备上安装来自未知来源的应用程序。

创建和配置安装包

Kaspersky Endpoint Security for Android 安装包是 `sc_package.exe` 自解压压缩文件。压缩文件包括在设备上安装移动应用程序所必需的文件：

- `adb.exe`、`AdbWinApi.dll`、`AdbWinUsbApi.dll` – 安装 Kaspersky Endpoint Security for Android 所需的一组文件。
- `installer.ini` – 包含管理服务器连接设置的配置文件。
- `KES10_xx_xx_xxx.apk` – Kaspersky Endpoint Security for Android 安装文件。
- `kmlisten.exe` – 通过工作站传送应用程序安装包的实用工具。
- `kmlisten.ini` – 包含安装包传送实用工具设置的配置文件。
- `kmlisten.kpd` – 应用程序说明文件。

创建 Kaspersky Endpoint Security for Android 安装包：

1. 在控制台树中，选择“**其他**”→“**远程安装**”→“**安装包**”文件夹。
2. 在“**安装包**”文件夹的工作区中，单击“**创建安装包**”按钮。
   安装包创建向导将会启动。按照向导的描述进行操作。
3. 在向导的“**选择安装包类型**”窗口中，单击“**创建 Kaspersky 程序安装包**”按钮。
4. 在向导的“**定义安装包名称**”窗口中，输入将要在“**安装包**”文件夹的工作区中显示的安装包名称。
5. 在向导的“**为安装选择应用程序安装包**”窗口中，选择包括在分发包中的 `sc_package.exe` 自解压压缩文件。
   如果您已经解压缩了压缩包，则选择应用程序说明文件 `kmlisten.kpd`。在输入字段中会显示应用程序名称和版本号。
6. 在向导的“**接受 EULA**”窗口中，阅读、理解并接受《最终用户授权许可协议》的条件与条款。
   您必须接受《最终用户授权许可协议》的条件与条款后才能创建安装包。如果您在管理控制台中接受授权许可协议的条款，则 Kaspersky Endpoint Security for Android 会在安装应用程序时跳过接受步骤。
   如果您要停止对移动设备的保护，可以卸载 Kaspersky Endpoint Security for Android 应用，并撤销该应用的最终用户授权许可协议 (EULA)。要了解关于撤销 EULA 的更多信息，请参阅“*Kaspersky Security Center 帮助*”。

向导完成后，创建的安装包将显示在“**安装包**”文件夹工作区中。安装包存储在“包”文件夹中，在管理服务器公共共享文件夹内。

配置安装包设置：

1. 在控制台树中，选择“**其他**”→“**远程安装**”→“**安装包**”文件夹。
2. 在 Kaspersky Endpoint Security for Android 安装包的上下文菜单中，选择“**属性**”。
3. 在“**设置**”选项卡中，指定移动设备的管理服务器连接设置，以及第一次与管理服务器同步之后自动接收移动设备的管理组。执行以下步骤：
   - 在“**管理服务器连接**”区域中，在“**服务器地址**”字段中输入管理服务器安装期间用于安装“**移动设备支持**”的移动设备管理服务器名称。

     根据“**移动设备支持**”组件的管理服务器名称格式的不同，指定管理服务器的 DNS 名称或 IP 地址。在“**SSL 端口号**”字段中，指定管理服务器连接移动设备的开放的端口号。默认情况下使用 13292。
   - 在**将计算机分配至组**区域中，在**组名称**字段中，输入第一次与管理服务器同步之后接收移动设备的群组名称（默认使用 **KES10**）。

     指定的组将在“**其他**”>“**网络轮询**”>“**域**”文件夹中自动创建。
   - 在“**安装期间的操作**”区域中，如果您希望应用程序在首次启动时要求用户提供公司电子邮件地址，请选中“**请求电子邮件地址**”复选框。

     将移动设备添加至管理组时，用户电子邮件地址用于组成移动设备的名称。
4. 要应用指定设置，单击“**应用**”。

创建独立安装包

若要创建独立安装包，请执行以下步骤：

1. 在控制台树中，选择“**其他**”→“**远程安装**”→“**安装包**”文件夹。
2. 选择 Kaspersky Endpoint Security for Android 安装包。
3. 在安装包的上下文菜单中，选择“**创建独立安装包**”。

   系统将启动创建独立安装包的向导。按照向导的描述进行操作。
4. 配置分发独立安装包的方式：
   - 若要通过电子邮件发布已创建独立安装包的路径，可在“**后续操作**”区域中单击链接“**通过电子邮件发送独立安装包链接**”。

     消息编辑器窗口将会打开，窗口中的文本包含带有独立安装包共享文件夹路径。
   - 若要在公司网站上发布已创建独立安装包链接，可单击链接“**用于在网站上发布链接的简易 HTML 代码**”。

     包含 HTML_RJL 链接的 tmp 文件将会打开。
5. 若要在 Kaspersky Security Center Web Server 上发布已创建的独立安装包，并查看独立安装包的完整列表以查找选定安装包，可在“**独立安装包向导成功完成**”窗口中选择“**打开独立安装包列表**”选框。

向导关闭后，将打开“**安装包 <安装包名称> 独立包列表**”窗口。

“安装包 <安装包名称> 独立包列表”窗口包含以下信息：

- 独立安装包列表。
- 在“**路径**”字段中显示的共享文件夹网络路径。
- 在“**网址**”字段中显示的 Kaspersky Security Center Web Server 上的独立安装包地址。

发送电子邮件通知时，您可以在“**网址**”字段中指定地址，或在“**路径**”字段中指定路径，以便用户下载应用程序源文件。将文本消息通知发送给用户时，您可以指定“**网址**”字段中显示的下载链接。

建议您将已创建独立安装包的地址复制到剪切板，然后将所需安装包的链接粘贴到电子邮件或文本消息通知中。

配置同步设置

要管理移动设备并从用户的移动设备接收报告或统计信息，必须配置同步设置。移动设备与 Kaspersky Security Center 的同步可通过以下方式执行：

- **按计划**。使用 HTTP 协议按计划执行同步。您可以在组策略设置中配置同步计划。当设备按照计划与 Kaspersky Security Center 同步时，才会执行对组策略设置、命令和任务的修改，即，有一个延迟。默认情况下，移动设备每隔 6 小时与 Kaspersky Security Center 自动同步一次。

  在 Android 12 或更高版本上，如果设备处于省电模式，应用程序可能会晚于指定的时间执行此任务。

- **强制**。使用 FCM 服务 (Firebase Cloud Messaging) 的推送通知执行强制同步。强制同步主要用于及时传递命令到移动设备。如果您要使用强制同步，请确保在 Kaspersky Security Center 中配置 GSM 设置。有关详细信息，请参阅 Kaspersky Security Center 帮助。

配置移动设备与Kaspersky Security Center的同步设置：

1. 在控制台树的“**受管设备**”文件夹中，选择 Android 设备所属的管理组。
2. 在所选组的工作区中，选择“**策略**”选项卡。
3. 通过双击任意列打开策略属性窗口。
4. 在策略“**属性**”窗口中选择“**同步**”区域。
5. 在“**同步**”下拉列表中选择同步频率。
6. 要禁用设备在漫游时与 Kaspersky Security Center 同步，请选中“**漫游时不同步**”选框。

   设备用户可在应用程序设置中手动执行同步（ → **设置** → **同步** → **同步**）。
7. 要在应用程序设置中隐藏用户的同步设置（服务器地址、端口和管理组），请清除“**在设备上显示同步设置**”选框。无法修改隐藏的设置。
8. 单击“**应用**”按钮以保存所作的更改。

与 Kaspersky Security Center 的下次设备同步之后可配置移动设备设置。您可以通过使用特殊命令来手动同步移动设备。要详细了解如何使用移动设备命令，请参阅*"Kaspersky Security Center 帮助"*。

激活 Kaspersky Endpoint Security for Android 应用程序

Kaspersky Security Center 授权许可可应用于不同组的功能。为了确保 Kaspersky Endpoint Security for Android 应用程序完全正常运行，组织购买的 Kaspersky Security Center 授权许可必须提供**移动设备管理**功能。**移动设备管理**功能旨在将移动设备连接到 Kaspersky Security Center 并管理它们。

有关 Kaspersky Security Center 授权和授权选项的详细信息，请参阅 *Kaspersky Security Center 帮助*。

在移动设备上激活 Kaspersky Endpoint Security for Android 应用程序是通过向该应用程序提供有效的授权许可信息来完成的。当设备与 Kaspersky Security Center 同步时，授权许可信息将与策略一起传递到移动设备。

如果在移动设备上安装 Kaspersky Endpoint Security for Android 应用程序后 30 天内未完成激活，该应用程序将自动切换至受限功能模式。在此模式中，大部分应用程序组件都无法运行。切换到受限功能模式后，该应用程序将停止执行与 Kaspersky Security Center 的自动同步。因此，如果在应用程序安装后 30 天内未完成激活，用户必须手动与 Kaspersky Security Center 同步设备。

如果您的组织中未部署 Kaspersky Security Center 或移动设备无法访问 Kaspersky Security Center，用户可以在其设备上手动激活 Kaspersky Endpoint Security for Android 应用程序。

若要激活 Kaspersky Endpoint Security for Android 应用程序，请执行以下操作：

1. 在控制台树的"**受管设备**"文件夹中，选择 Android 设备所属的管理组。
2. 在所选组的工作区中，选择"**策略**"选项卡。
3. 通过双击任意列打开策略属性窗口。
4. 在策略"**属性**"窗口中选择"**授权许可管理**"区域。
5. 在"**授权许可**"区域，打开"**密钥**"下拉列表，然后从 Kaspersky Security Center 管理服务器的密钥存储区选择所需的应用程序激活密钥。

   下面的字段中显示已购买授权许可的应用程序的详情。
6. 选择"**用来自 Kaspersky Security Center 存储空间的密钥进行激活操作**"选框。

   如果激活应用程序时未使用 Kaspersky Security Center 存储空间中存储的密钥，Kaspersky Security for Mobile 会用"**密钥**"下拉列表中选择的激活密钥替换该密钥。
7. 若要在用户的移动设备上激活应用程序，请阻止更改设置。
8. 单击"**应用**"按钮以保存所作的更改。

   与 Kaspersky Security Center 的下次设备同步之后可配置移动设备设置。

安装 iOS MDM 配置文件

本节介绍在企业网络上部署 iOS MDM 配置文件的方法。

在部署 iOS MDM 配置文件之前，管理员必须执行以下操作：

1. 安装 iOS MDM 服务器。
2. 获取 Apple 推送通知服务证书（APN 证书）。
3. 将 APN 证书安装到 iOS MDM 服务器。

有关安装 iOS MDM 服务器和使用 APNs 证书的详细信息，请参阅 *Kaspersky Security Center 帮助*。

有关在 Kaspersky Endpoint Security Cloud 中部署 iOS MDM 配置文件的详细信息，请参阅 *Kaspersky Endpoint Security Cloud 帮助*。

关于 iOS 设备管理模式

您可以采用多种不同方式部署 iOS 设备管理系统。管理模式取决于移动设备的所有者（个人或公司）和公司安全要求。您可以选择最适合您公司的管理模式，并同时使用多种模式。

不受监控的设备

"*不受监控的 iOS 设备*"是指连接到 Kaspersky Security Center 的员工个人设备。在此模式下，允许用户使用个人 Apple ID，使用任何应用程序，并在设备上存储个人数据。您可以使用 Kaspersky Device Management for iOS 组策略配置对公司资源的访问权限、安全设置和其他设置。默认情况下，所有 iOS 设备均处于不受监控状态。

监控设备

"*监控 iOS 设备*"是指连接到 Kaspersky Security Center 的公司设备。在 Apple Configurator 中执行移动设备的初始配置。"*Apple Configurator*"是一个专门用于准备和配置 iOS 设备的应用程序。Apple Configurator 安装在运行 OS X 的计算机上。有关使用 Apple Configurator 的更多详细信息，请参阅 Apple 技术支持网站。您可以使用 Kaspersky Device Management for iOS 组策略执行进一步配置。在监控设备上，您可以访问扩展的设置选项。例如，您可以配置全局 HTTP 代理和附加限制（例如，阻止使用 iMessage 和游戏中心），还可以阻止修改用户账户。

要使用受监控和不受监控的 iOS 设备，iOS MDM 服务器必须安装有 APN 证书，并在用户的移动设备上安装 iOS MDM 配置文件。

通过 Kaspersky Security Center 安装

iOS MDM 配置文件安装到其用户账户已添加到 Kaspersky Security Center 的用户的移动设备上。有关 Kaspersky Security Center 中的用户账户的详细信息，请参阅 *Kaspersky Security Center 帮助*。

若要安装 iOS MDM 配置文件，请执行以下操作：

1. 在控制台树中，选择"**移动设备管理**"→"**移动设备**"文件夹。
2. 在"**移动设备**"文件夹的工作区中，单击"**添加移动设备**"按钮。
   这将启动新建移动设备连接向导。按照向导的描述进行操作。
3. 在向导的"**操作系统**"窗口中，选择"**iOS**"。
4. 在向导的"**iOS MDM 设备保护方法**"窗口中，选择"**使用 iOS MDM 服务器的 iOS MDM 配置文件**"并指定列表中的 iOS MDM 配置文件。

5. 在向导的“**选择用户**”窗口中，选择要将 iOS MDM 配置文件安装到其移动设备的一个或多个用户。

   如果用户不在列表中，您可以添加新用户账户，而不必退出新建移动设备连接向导。

6. 在向导的“**证书来源**”窗口中，选择用于保护移动设备和 Kaspersky Security Center 之间的数据传输的证书来源：

   - **通过管理服务器工具颁发证书**。在这种情况下，将自动创建证书。
   - **指定证书文件**。在这种情况下，必须提前准备您自己的证书，然后在向导的窗口中选择它。如果您要将 iOS MDM 配置文件安装到多个移动设备，则无法使用此选项。必须为每个用户创建单独的证书。

7. 在向导的“**用户通知方法**”窗口中，选择用于转发应用程序安装链接的通道：

   - 若要通过电子邮件发送链接，请选择“**发送指向 iOS MDM 配置文件的链接**”，并在“**通过电子邮件**”区域中配置设置。确保在用户账户的设置中指定了电子邮件地址。
   - 若要通过短信发送链接，请选择“**发送指向 iOS MDM 配置文件的链接**”，并在“**通过短信**”区域中配置设置。确保在用户账户的设置中指定了电话号码。
   - 若要使用二维码安装 iOS MDM 配置文件，请选择“**显示安装包链接**”并使用移动设备的摄像头扫描二维码。
   - 如果列出的方法都不适合您，请选择“**显示安装包链接**” → “**复制**”，将 iOS MDM 配置文件安装链接复制到剪贴板。使用任何可用的方法发送应用程序安装链接。

8. 完成新建移动设备连接向导。

将 iOS MDM 配置文件安装到用户的移动设备后，您可以使用组策略来配置应用程序设置。如果设备丢失或被盗，您还可以向移动设备发送命令以便保护数据。

在运行 iOS 12.1 或更新版本的移动设备上，您必须手动确认 iOS MDM 配置文件在移动设备上的安装。您必须授予远程管理设备的权限。

安装管理插件

若要管理移动设备，必须在管理员的工作站上安装以下管理插件：

- Kaspersky Endpoint Security for Android 的管理插件提供界面，用于通过 Kaspersky Security Center 管理控制台，管理移动设备以及安装在这些设备上的移动应用程序。
- Kaspersky Device Management for iOS 的管理插件提供了界面，用于通过 Kaspersky Security Center 管理控制台管理通过 iOS MDM 和 Exchange ActiveSync 协议连接的移动设备。

您可以使用以下方法安装管理插件：

- 使用 Kaspersky Security Center 的快速启动向导安装管理插件。

  安装管理服务器后，应用程序会在您第一次连接时自动提示您运行快速启动向导。您也可以随时手动启动快速启动向导。

快速启动向导允许您在管理控制台中接受 Kaspersky Endpoint Security for the Android 应用程序的最终用户授权许可协议 (EULA) 的条款和条件。如果管理员在管理控制台中接受授权许可协议的条款，则 Kaspersky Endpoint Security for Android 会在安装应用程序时跳过接受步骤。有关 Kaspersky Security Center 快速启动向导的详细信息，请参阅 *Kaspersky Security Center 帮助*。

- 在 Kaspersky Security Center 的管理控制台中使用可用分发包列表安装管理插件。
  在新版本的 Kaspersky 应用程序发布后，可用分发包列表会自动更新。
- 从外部源下载分发包，然后使用 EXE 文件安装管理插件。
  例如，可以在 Kaspersky 网站上下载管理插件的分发包。

在管理控制台中通过列表安装管理插件

要安装管理插件：

1. 在控制台树中，选择“**高级**”→“**远程安装**”→“**安装包**”。
2. 在工作区中，选择“**其他操作**”→“**查看 Kaspersky 应用程序的当前版本**”。
   这将打开 Kaspersky 应用程序最新版本的列表。
3. 在“**移动设备**”区域中，选择“**Kaspersky Endpoint Security for Android**”或“**Kaspersky Device Management for iOS**”插件。
4. 单击“**下载分发包**”按钮。
   一个插件分发包将下载到计算机内存中（EXE 文件）。
5. 运行该 EXE 文件并按照安装向导的说明操作。

从分发包安装管理插件

要安装 Kaspersky Endpoint Security for Android 管理插件，

从集成的解决方案分发包中复制插件安装文件 `klcfinst.exe`，然后在管理员工作站上运行它。

安装由向导执行，您无需配置设置。

要安装 Kaspersky Device Management for iOS 管理插件，请执行以下操作：

从集成解决方案分发包中复制插件安装文件 `klmdminst.exe`，然后在管理员工作站上运行它。

安装由向导执行，您无需配置设置。

您可通过在“**高级**”→“**已安装的应用程序管理插件的详细信息**”区域中，查看管理服务器属性窗口中的已安装应用程序管理插件列表，来确认管理插件已安装。

更新先前版本的应用程序

应用程序升级必须满足以下要求：

- Kaspersky Endpoint Security 管理插件的版本和 Kaspersky Endpoint Security for Android 移动应用程序的版本必须匹配。

  您可以在 Kaspersky Security for Mobile 的发行说明中查看管理插件和移动应用程序版本的版本号。

- 确保 Kaspersky Security Center 满足 Kaspersky Security for Mobile 的软件要求。

- Kaspersky Endpoint Security 10.0 Service Pack 2 (Build 10.6.0.1801) 和 Kaspersky Device Management for iOS 10.0 Service Pack 2 (Build 10.6.0.1767) 及更高版本的管理插件可以自动升级到当前版本。不支持升级早期版本的管理插件。

  若要升级早期版本的管理插件，您必须删除已安装的管理插件和使用它们创建的组策略。然后安装管理插件的新版本。有关删除管理插件的详细信息，请访问 *Kaspersky 技术支持网站*。

- 在组织的所有移动设备上使用相同版本的 Kaspersky Endpoint Security for Android。

可在 *Kaspersky 技术支持网站* 上查看 Kaspersky Security for Mobile 版本的技术支持的条款和条件。

若要查看管理插件的版本和内部版本号，请执行以下操作：

1. 在控制台树中的管理服务器上下文菜单中，选择“**属性**”。
2. 在管理服务器属性窗口中，选择“**高级**”→“**已安装的应用程序管理插件的详细信息**”。

工作区将以 `<Plug-in name> <Version> <Build>` 格式显示已安装的管理插件的信息。

您可以使用以下方法查看 Kaspersky Endpoint Security for Android 应用程序的版本和内部版本号：

- 如果 Kaspersky Endpoint Security for Android 是使用独立安装包安装的，您可以在包属性中查看应用程序的版本和内部版本号。
- 如果 Kaspersky Endpoint Security for Android 是通过 Google Play 安装的，您可以在应用程序设置中查看内部版本号（☰ → **关于应用程序**）。

升级先前版本的 Kaspersky Endpoint Security for Android

Kaspersky Endpoint Security for Android 可通过下列方式更新：

- 使用 Google Play。移动设备用户可以从 Google Play 中下载应用程序的新版本，然后在设备中进行安装。
- 使用 Kaspersky Security Center。您可以使用 Kaspersky Security Center 远程管理系统远程更新设备上的应用程序版本。

您可以选择最适合您组织的应用程序更新方法。您可以仅使用一种更新方法。

从 Google Play 更新应用程序

通过执行 Android 平台的标准更新步骤，您可以从 Google Play 更新本应用程序。要更新应用程序，必须满足下列条件：

- 移动设备用户必须拥有 Google 帐户。
- 设备必须已链接至您的 Google 账户。
- 设备必须连接到互联网。

从 Google Play 下载应用程序后，Kaspersky Endpoint Security for Android 会检查最终用户授权许可协议 (EULA) 的条款和条件。如果 EULA 的条款有更新，则该应用程序会向 Kaspersky Security Center 发送请求。如果管理员在管理控制台中接受 EULA，则 Kaspersky Endpoint Security for Android 会在安装应用程序时跳过接受步骤。如果管理员使用过时版本的管理插件，Kaspersky Security Center 会提示您更新管理插件。更新管理插件时，管理员可以在管理控制台中接受 Kaspersky Endpoint Security for Android 的 EULA 条款。

如果 Kaspersky Endpoint Security for Android 是从 Google Play 安装的，则可以通过 Google Play 更新该应用程序。如果该应用程序是使用其他方法安装的，则不能通过 Google Play 更新该应用程序。

通过 Kaspersky Security Center 更新应用程序

应用组策略之后，可以使用 Kaspersky Security Center 升级 Kaspersky Endpoint Security for Android。在组策略设置中，可以选择符合企业安全要求的版本的 Kaspersky Endpoint Security for Android 独立安装包。

如果通过 Kaspersky Security Center 安装了 Kaspersky Endpoint Security for Android，则可以通过 Kaspersky Security Center 更新。如果该应用程序是从 Google Play 安装的，则不能通过 Kaspersky Security Center 更新应用程序。

若要使用独立安装包升级 Kaspersky Endpoint Security for Android，必须允许在用户的移动设备上安装来自未知来源的应用程序。关于不使用 Google Play 安装应用的详情，请参考 *Android 帮助向导*。

若要更新应用程序版本，请执行以下操作：

1. 在控制台树的“**受管设备**”文件夹中，选择 Android 设备所属的管理组。
2. 在所选组的工作区中，选择“**策略**”选项卡。
3. 通过双击任意列打开策略属性窗口。
4. 在策略“**属性**”窗口中选择“**其他**”区域。
5. 在“**正在升级 Kaspersky Endpoint Security for Android**”区域中，单击“**选择**”按钮。

   “**正在升级 Kaspersky Endpoint Security for Android**”窗口随即打开。
6. 在 Kaspersky Endpoint Security 独立安装包列表中，选择其版本满足公司安全要求的安装包。

   您只能将 Kaspersky Endpoint Security 升级至最近的应用程序版本。Kaspersky Endpoint Security 无法升级至较老版本。
7. 单击“**选择**”按钮。

   “**正在升级 Kaspersky Endpoint Security for Android**”区域中将显示所选独立安装包的描述。
8. 单击“**应用**”按钮以保存所作的更改。

与 Kaspersky Security Center 的下次设备同步之后可配置移动设备设置。移动设备用户将获得启示安装新版本应用程序。用户同意后，新版应用程序将安装在移动设备上。

安装先前版本的 Kaspersky Endpoint Security for Android

如果您要防止应用自动更新和使用特别版本的 Kaspersky Endpoint Security for Android，在 Google Play 设置中禁用应用的自动更新。对于更多详情，请参考 Google 技术支持网站。

Kaspersky Endpoint Security for Android 的自动更新仅在应用从 Google Play 或通过 Kaspersky Security Center 使用 Google Play 链接安装时可用。如果应用通过 Kaspersky Security Center 使用您自己的 Web 服务器的链接（使用独立安装包）安装，自动更新不可用。此种情况下，您可以使用组策略手动更新 Kaspersky Endpoint Security for Android。

要安装先前版本的 Kaspersky Endpoint Security for Android：

1. 从用户移动设备中删除 Kaspersky Endpoint Security for Android。
2. 使用指向您自己的 Web 服务器的链接安装 Kaspersky Endpoint Security for Android。为此，您将需要被别版本的安装包。您可以在 Kaspersky 技术支持网站下载早期版本 Kaspersky Endpoint Security for Android 的分发包。

有关早期版本的 Kaspersky Endpoint Security for Android 的详细信息，请参阅*相应 Kaspersky Security for Mobile 版本的帮助*。

升级先前版本的管理插件

您可以使用以下方法升级管理插件：

- 在 Kaspersky Security Center 的管理控制台中从可用分发包列表安装新版本管理插件。

  在新版本的 Kaspersky 应用程序发布后，可用分发包列表会自动更新。

- 从外部源下载分发包，然后使用 EXE 文件安装新版本管理插件。

  若要升级 Kaspersky Endpoint Security for Android 和 Kaspersky Device Management for iOS 管理插件，您需要从 Kaspersky Security for Mobile 网页下载最新版本的应用程序，然后为两个插件分别运行安装向导。在安装向导运行过程中，先前版本的插件会自动删除。

Kaspersky 专家建议使用相同版本的应用程序和管理插件。如果用户从 Google Play 升级应用程序，则 Kaspersky Security Center 会显示通知，提示升级管理插件。

管理插件更新之后，“**受管设备**”文件夹中的现有管理组和“**未分配的设备**”文件夹中设备自动分配到这些组的规则将保存。现有的移动设备组策略也将保留。实施 Kaspersky Security for Mobile 集成解决方案的新功能的新策略设置将添加到现有策略中，并且拥有默认值。

如果在管理插件新版本中添加了新设置或者默认值被更改，更改仅在打开组策略后被应用。先前版本插件的设置在管理员打开组策略之前都被应用到移动设备，即使插件版本被更新。

在管理控制台中通过列表升级

要升级管理插件：

1. 在控制台树中，选择“**高级**”→“**远程安装**”→“**安装包**”。
2. 在工作区中，选择“**其他操作**”→“**查看 Kaspersky 应用程序的当前版本**”。

   这将打开 Kaspersky 应用程序最新版本的列表。
3. 在“**移动设备**”区域中，选择“**Kaspersky Endpoint Security for Android**”或“**Kaspersky Device Management for iOS**”插件。
4. 单击“**下载分发包**”按钮。

   一个插件分发包将下载到计算机内存中（EXE 文件）。允许该 EXE 文件。按照安装向导的说明进行操作。

从分发包升级

要升级 Kaspersky Endpoint Security for Android 管理插件，

从集成的解决方案分发包中复制插件安装文件 `klcfinst.exe`，然后在管理员工作站上运行它。

安装由向导执行，您无需配置设置。

要升级 Kaspersky Device Management for iOS 管理插件，

从集成解决方案分发包中复制插件安装文件 `klmdminst.exe`，然后在管理员工作站上运行它。

插件安装由向导执行，您无需配置设置。

您可通过在“**高级**”→“**已安装的应用程序管理插件的详细信息**”区域中，查看管理服务器属性窗口中的已安装应用程序管理插件列表，来确认管理插件已升级。

删除 Kaspersky Endpoint Security for Android

Kaspersky Endpoint Security for Android 可通过下列方式删除：

1. 由用户删除应用程序

   用户使用应用程序界面，手动删除 Kaspersky Endpoint Security for Android。要让用户能够删除应用程序，应该在应用于设备的策略中允许应用程序删除。
2. 由管理员删除应用程序。

   管理员使用 Kaspersky Security Center 的管理控制台，远程删除应用程序。应用程序既可从单独设备删除，也可从多部设备同时删除。

远程删除应用程序

您可通过以下方式，远程从用户的移动设备上删除 Kaspersky Endpoint Security for Android：

- 使用组策略。如果您要将应用程序同时从多部设备上删除，这种方法是非常方便的。
- 通过配置本地应用程序设置。如果您要将应用程序从单独设备上删除，这种方法是非常方便的。

应用组策略删除应用程序：

1. 在控制台树的“**受管设备**”文件夹中，选择 Android 设备所属的管理组。
2. 在所选组的工作区中，选择“**策略**”选项卡。
3. 通过双击任意列打开策略属性窗口。
4. 在策略“**属性**”窗口中选择“**其他**”区域。
5. 在“**卸载 Kaspersky Endpoint Security for Android 应用程序**”区域中，选中“**从设备上卸载 Kaspersky Endpoint Security for Android**”复选框。
6. 单击“**应用**”按钮以保存所作的更改。

在与管理服务器同步之后，Kaspersky Endpoint Security for Android 将从移动设备上删除。移动设备用户收到关于应用程序已删除的通知。

通过配置本地设置删除应用程序：

1. 在控制台树中，选择“**移动设备管理**”→“**移动设备**”。
2. 在设备列表中，选择您要在其上删除应用程序的设备。
3. 通过双击打开设备属性窗口。
4. 选择“**应用**”→“**Kaspersky Endpoint Security for Android**”。
5. 通过双击打开 Kaspersky Endpoint Security 属性窗口。
6. 选择“**其他**”区域。
7. 在“**卸载 Kaspersky Endpoint Security for Android**”区域中，选中“**从设备上卸载 Kaspersky Endpoint Security for Android**”选框。
8. 单击“**应用**”按钮以保存所作的更改。

在与管理服务器同步之后，Kaspersky Endpoint Security for Android 将从移动设备上删除。移动设备用户收到关于应用程序已删除的通知。

允许用户删除应用程序

要保护在运行安卓 7.0 或更高版本的设备上的应用程序不会被卸载，必须将 Kaspersky Endpoint Security for Android 设置为可访问功能。当初始配置向导正在运行时，Kaspersky Endpoint Security for Android 会提示用户授予应用程序所有必需的权限。用户可以跳过这些步骤或以后在设备设置中禁用这些权限。在这种情况下，不保护该应用程序不被卸载。

您可以通过以下方式，允许用户将 Kaspersky Endpoint Security for Android 从他们的移动设备上删除：

- 使用组策略。如果您希望允许用户同时将应用程序从多部设备上删除，这种方法是非常方便的。
- 使用本地应用程序设置。如果您希望允许单独设备的用户删除应用程序，这种方法是非常方便的。

在组策略中允许删除应用程序：

1. 在控制台树的“**受管设备**”文件夹中，选择 Android 设备所属的管理组。
2. 在所选组的工作区中，选择“**策略**”选项卡。
3. 通过双击任意列打开策略属性窗口。
4. 在策略“**属性**”窗口中选择“**其他**”区域。
5. 在“**卸载 Kaspersky Endpoint Security for Android**”区域中，选中“**允许卸载 Kaspersky Endpoint Security for Android**”复选框。
6. 单击“**应用**”按钮以保存所作的更改。

在与管理服务器同步之后，将允许用户从移动设备上删除该应用程序。删除应用程序按钮在 Kaspersky Endpoint Security for Android 设置中变成可用状态。

允许在本地应用程序设置中删除应用程序：

1. 在控制台树中，选择“**其他**” → “**移动设备管理**” → “**移动设备**”。
2. 在设备列表中，选择您要允许用户从其删除应用程序的设备。
3. 通过双击打开设备属性窗口。
4. 选择“**应用程序**”→“**Kaspersky Endpoint Security for Mobile**”。
5. 通过双击打开 Kaspersky Endpoint Security 属性窗口。
6. 选择“**附加**”区域。
7. 在“**卸载 Kaspersky Endpoint Security for Android**”区域中，选中“**允许卸载 Kaspersky Endpoint Security for Android**”复选框。
8. 单击“**应用**”按钮以保存所作的更改。

与管理服务器同步之后，将允许用户从移动设备上删除应用程序。删除应用程序按钮在 Kaspersky Endpoint Security for Android 设置中变成可用状态。

由用户删除应用程序

若要从移动设备上独立地删除 Kaspersky Endpoint Security for Android，用户必须执行以下操作：

1. 在 Kaspersky Endpoint Security for Android 的主窗口中，点击 → “**卸载应用程序**”。
   屏幕中将出现确认提示信息。
   如果未显示“**卸载应用程序**”按钮，则意味着管理员已启用 Kaspersky Endpoint Security for Android 卸载保护。
2. 确认删除 Kaspersky Endpoint Security for Android。

Kaspersky Endpoint Security for Android 应用程序将从用户的移动设备中删除。

配置和管理

本帮助部分面向管理 Kaspersky Security for Mobile 的专家，以及向使用 Kaspersky Security for Mobile 的组织提供技术支持的专家。

开始使用

本节介绍在开始使用 Kaspersky Security for Mobile 时建议您执行的操作。

启动和停止应用程序

Kaspersky Security Center 将自动启用和停止 Kaspersky Endpoint Security 和 Kaspersky Device Management for iOS 的管理插件。

操作系统启动时 Kaspersky Endpoint Security for Android 也会启动并在整个会话中保护移动设备。用户可以通过禁用所有 Kaspersky Endpoint Security for Android 组件来停止应用程序。您可以使用组策略配置用户管理应用程序组件的权限。

在某些设备（例如，华为、魅族和小米）上，您必须手动将 Kaspersky Endpoint Security for Android 添加到在操作系统启动时启动的应用程序列表（“**安全**” → “**权限**” → “**自动运行**”）。如果未将该应用程序添加到列表，在移动设备重新启动后，Kaspersky Endpoint Security for Android 会停止执行其所有功能。

您还必须为 Kaspersky Endpoint Security for Android 禁用低电量模式。这对于要在后台运行的应用程序（例如，运行计划的病毒扫描或将设备与 Kaspersky Security Center 同步）来说是必需的。此问题归因于这些设备内嵌的软件的特定功能。

创建管理组

若要集中配置用户移动设备上安装的 Kaspersky Endpoint Security for Android 应用程序，必须将组策略应用至这些设备。

若要将策略应用于设备组，建议您在用户设备上安装移动应用程序之前，先在“**受管设备**”中为这些设备创建单独的组。

创建管理组后，建议配置选项以将要安装应用程序的设备自动分配到此组。然后使用组策略配置所有设备通用的设置。

若要创建管理组，执行以下步骤：

1. 在控制台树中，选择“**受管设备**”文件夹。
2. 在“**受管设备**”文件夹或子文件夹的工作区中，选择“**设备**”选项卡。

3. 单击“**新建组**”按钮。

这将打开可供您创建新组的窗口。

4. 在“**组名称**”窗口中输入组名称，然后单击“**确定**”。

控制台树中将显示带有指定名称的新管理组文件夹。有关使用管理组的详细信息，请参阅 *Kaspersky Security Center 帮助*。

用于管理移动设备的组策略

组策略 是用于管理属于管理组的移动设备和管理设备上安装的移动应用程序的设置包。您可以使用策略向导创建组策略。

您可以使用策略配置单个设备和设备组的设置。对于一组设备，可在组策略属性窗口中配置管理设置。对于单个设备，可在本地应用程序设置窗口中配置。为一个设备指定的单个管理设置可能会与为该设备所属组的策略中配置的设置值有所不同。

策略中的每个参数都有“锁”属性，该“锁定”显示是否允许在嵌套层次结构级别（对嵌套组和辅助管理服务器而言）、任务设置和本地应用程序设置修改策略。

在本地应用程序中和策略中配置的设置值将保存在管理服务器上，在同步期间分发至移动设备并将其作为当前值保存在设备中。如果用户指定了未被“锁定”的其他设置值，在设备与管理服务器下次同步期间，设置新值将被传递给管理服务器，并保存在应用程序本地设置中，而不是先前由管理员指定的值。

为了使移动设备的企业安全保护保持最新，您可以监控用户的设备是否符合组管理策略。

安全级别指示器在组策略窗口的上部显示。安全级别指示器将显示帮助您配置策略以确保高级别设备保护。保护级别指示器状态根据策略设置而更改：

- **高保护级别** – 提供适当级别的设备保护。全部保护组件根据 Kaspersky 的设置来运行。
- **中保护级别** – 保护级别低于推荐级别。一些关键保护组件被显示(例如，Web 保护)。重要问题使用 ● 图标来标记。
- **低保护级别** – 表示存在可能导致设备感染病毒和数据丢失的问题。一些关键保护组件被显示(例如，设备实时保护被禁用)。关键问题使用 ● 图标来标记。

有关在 Kaspersky Security Center 管理控制台中对策略和管理组进行管理的详细信息，请参阅 *Kaspersky Security Center 帮助*。

创建组策略

本节介绍为安装了 Kaspersky Endpoint Security for Android 移动应用程序的设备创建组策略的过程以及为 EAS 设备和 iOS MDM 设备创建策略的过程。

为管理员组创建的策略显示在 Kaspersky Security Center 管理控制台组工作区的“**策略**”选项卡中。指示策略状态（活动/不活动）的图标显示在策略名称前。可以在一个组中创建多个用于不同应用程序的策略。对于每个应用程序，仅一个策略处于活动状态。当创建新的活动策略时，先前的活动策略将变为不活动状态。

您可以在策略创建后修改策略。

若要创建用于管理移动设备的组策略：

1. 从控制台树中，选择您要为其创建策略的管理组。

2. 在所选组的工作区中，选择“**策略**”选项卡。

3. 单击“**创建策略**”链接以运行策略向导。

这会启动策略向导。

步骤 1.选择要创建组策略的应用程序

在此步骤中，在应用程序列表中选择您要为其创建组策略的应用程序：

- **Kaspersky Endpoint Security for Android** – 对于使用 Kaspersky Endpoint Security for Android 移动应用程序的设备。

建议为没有 Google play 服务的华为和荣耀设备创建单独策略。这样，可以将华为应用市场的链接发送给所有这类设备的用户。

- **Kaspersky Device Management for iOS** – 对于 EAS 设备和 iOS MDM 设备。

如果管理员桌面上安装了 Kaspersky Endpoint Security for Android管理插件和 Kaspersky Device Management for iOS 管理插件，则可以为移动设备创建策略。如果未安装这些插件，相关应用程序的名称不会显示在应用程序列表中。

继续策略向导的下一步。

步骤 2.输入组策略名称

在此步骤中，在“**名称**”字段中输入新策略的名称。如果您指定了现有策略的名称，它将在最后自动添加 (1)。

继续策略向导的下一步。

步骤 3.为应用程序创建组策略

在这一步中，向导将提示您选择策略状态：

- **活动策略**。向导将在管理服务器上保存已创建的策略。在移动设备下次与管理服务器同步时，该策略将在设备上用作活动策略。

- **非活动策略**。向导将在管理服务器上以备份策略的方式保存已创建的策略。在后续某个特殊事件之后该策略将被激活。如有必要可将不活动的策略切换为活动状态。

可以为组中一个应用程序创建若干个策略，但是只能激活它们中的一个策略。当创建新的活动策略时，先前的活动策略将自动变为不活动状态。

退出向导。

配置同步设置

要管理移动设备并从用户的移动设备接收报告或统计信息，必须配置同步设置。移动设备与 Kaspersky Security Center 的同步可通过以下方式执行：

- **按计划**。使用 HTTP 协议按计划执行同步。您可以在组策略设置中配置同步计划。当设备按照计划与 Kaspersky Security Center 同步时，才会执行对组策略设置、命令和任务的修改，即，有一个延迟。默认情况下，移动设备每隔 6 小时与 Kaspersky Security Center 自动同步一次。

  在 Android 12 或更高版本上，如果设备处于省电模式，应用程序可能会晚于指定的时间执行此任务。

- **强制**。使用 FCM 服务 (Firebase Cloud Messaging) 的推送通知执行强制同步。强制同步主要用于及时传递命令到移动设备。如果您要使用强制同步，请确保在 Kaspersky Security Center 中配置 GSM 设置。有关详细信息，请参阅 Kaspersky Security Center 帮助。

配置移动设备与Kaspersky Security Center的同步设置：

1. 在控制台树的“**受管设备**”文件夹中，选择 Android 设备所属的管理组。
2. 在所选组的工作区中，选择“**策略**”选项卡。
3. 通过双击任意列打开策略属性窗口。
4. 在策略“**属性**”窗口中选择“**同步**”区域。
5. 在“**同步**”下拉列表中选择同步频率。
6. 要禁用设备在漫游时与 Kaspersky Security Center 同步，请选中“**漫游时不同步**”选框。

   设备用户可在应用程序设置中手动执行同步（ → **设置** → **同步** → **同步**）。
7. 要在应用程序设置中隐藏用户的同步设置（服务器地址、端口和管理组），请清除“**在设备上显示同步设置**”选框。无法修改隐藏的设置。
8. 单击“**应用**”按钮以保存所作的更改。

与 Kaspersky Security Center 的下次设备同步之后可配置移动设备设置。您可以通过使用特殊命令来手动同步移动设备。要详细了解如何使用移动设备命令，请参阅*“Kaspersky Security Center 帮助”*。

管理对组策略的修订

Kaspersky Security Center 允许您跟踪组策略修改。每次保存对组策略进行的更改时，都会创建一个*修订*。每个修订都有一个编号。

您只能管理 Kaspersky Endpoint Security for Android 策略的修订。您不能管理 Kaspersky Device Management for iOS 策略的修订。

您可以对组策略修订执行以下操作：

- 将所选修订与当前修订进行比较。

- 比较所选修订。
- 将策略与另一个策略的所选修订进行比较。
- 查看所选修订。
- 将策略更改回滚至所选修订。
- 将修订另存为 .txt 文件。

有关管理组策略和其他对象（例如，用户账户）的修订的更多详细信息，请参阅 *Kaspersky Security Center 帮助*。

查看组策略修订的历史记录：

1. 在控制台树的“**受管设备**”文件夹中，选择 Android 设备所属的管理组。
2. 在所选组的工作区中，选择“**策略**”选项卡。
3. 通过双击任意列打开策略属性窗口。
4. 在策略“**属性**”窗口中选择“**修订历史记录**”区域。
   将显示策略修订列表。它包含以下信息：
   - 策略修订编号。
   - 修改策略的日期和时间。
   - 修改策略的用户名。
   - 对策略执行的操作。
   - 对策略设置进行的修订的说明。

删除组策略

若要删除组策略，请执行以下操作：

1. 在控制台树中，选择您要为其创建策略的管理组。
2. 在管理组的工作区中，在“**策略**”选项卡上选择要删除的策略。
3. 在策略的上下文菜单中，选择“**删除**”。

这样，组策略已删除。在应用新的组策略之前，属于管理组的移动设备继续使用在已删除的策略中指定的设置。

限制配置组策略的权限

Kaspersky Security Center 管理员可以根据用户工作职责配置管理控制台用户的权限以使用不同的 Kaspersky Security for Mobile 集成解决方案。

在管理控制台界面中，您可以在“管理服务器属性”窗口的“**安全性**”和“**用户角色**”选项卡上配置访问权限。在“**用户角色**”选项卡上，您可以添加具有预定义权限组的标准用户角色。在“**安全性**”区域，您可以为一个用户或一组用户配置权限，也可以为一个用户或一组用户分配角色。用户对于每个应用程序的权限根据*功能范围*进行配置。

您也可以配置特定于功能区域的用户权限。附录中提供了有关功能区域和策略选项卡的对应关系的信息。

对于每个功能方面，管理员可以分配以下权限：

- **允许编辑**。允许管理控制台用户在属性窗口中更改策略设置。
- **阻止编辑**。禁止管理控制台用户在属性窗口中更改策略设置。属于该权限分配至的功能范围的策略标记不会显示在界面中。

有关在 Kaspersky Security Center 的管理控制台中管理用户权限和角色的详情，请参阅 *Kaspersky Security Center 帮助*。

保护

本部分包含有关如何在 Kaspersky Security Center 管理控制台中远程管理移动设备的保护的信息。

在安卓设备上配置防病毒保护

为了及时检测威胁、病毒和其他恶意应用程序，您应配置实时防护和病毒扫描自动运行设置。

Kaspersky Endpoint Security for Android 可检测以下类型的对象：

- 病毒、蠕虫、木马和恶意工具。
- 广告软件。
- 检测可被犯罪分子入侵以损害您的设备或个人数据的应用程序。

反病毒有一些限制：

- 当反病毒正在运行时，在设备外部内存（例如 SD 卡）中检测到的威胁无法在工作配置文件中被自动清除（带有手提箱图标的应用程序， 配置安卓工作配置文件）。Kaspersky Endpoint Security for Android 在工作配置文件中不能访问外部内存。关于检测到对象的信息显示在应用的状态区域。要清除在外部内存中检测到的对象，对象文件必须被手动删除且设备扫描必须重启。
- 由于技术限制，Kaspersky Endpoint Security for Android 无法扫描大小为 2 GB 或更大的文件。在扫描期间，应用程序将跳过此类文件，而不会通知您此类文件被跳过。

若要配置移动设备实时保护设置，请执行以下步骤：

1. 在控制台树的“**受管设备**”文件夹中，选择 Android 设备所属的管理组。
2. 在所选组的工作区中，选择“**策略**”选项卡。
3. 通过双击任意列打开策略属性窗口。
4. 在策略“**属性**”窗口中选择“**保护**”区域。

5. 在“保护”区域中，配置移动设备文件系统保护设置：

- 若要启动实时保护移动设备，防御威胁，选择“启用保护”选框。

  Kaspersky Endpoint Security for Android 仅扫描下载文件夹中的新应用程序和文件。

- 若要启动移动设备扩展保护，防御威胁，选择“扩展保护模式”选框。

  Kaspersky Endpoint Security for Android 将扫描用户在设备上打开、修改、移动、复制、安装或保存的所有文件，以及新安装的移动应用程序。

  > 在运行 Android 8.0 或更高版本的设备上，Kaspersky Endpoint Security for Android 将扫描用户修改、移动、安装和保存的文件，以及文件副本。在打开文件或复制源文件时，Kaspersky Endpoint Security for Android 不会进行扫描。

- 若要启用在新应用程序在用户设备上首次启动时在卡巴斯基安全网络云服务的协助下附加扫描，请选中“云保护 (KSN)”复选框。

- 要阻止可被犯罪分子利用来损害设备或用户数据的广告软件和应用程序，请选中“检测可被犯罪分子用来对用户的设备和数据造成损害的广告软件、自动拨号程序和应用程序”复选框。

6. 在“检测到威胁时执行的操作”列表中，选择以下选项之一：

- 删除

  检测到的对象将被自动删除。不要求用户做任何其他操作。删除对象之前，Kaspersky Endpoint Security for Android 将显示检测到对象的临时通知。

- 跳过

  > 如果检测到的对象被跳过，Kaspersky Endpoint Security for Android 会警告用户设备保护方面存在问题。有关跳过的对象的信息会显示在应用程序的“状态”部分中。对于每个跳过的威胁，应用程序都提供用户可以执行以消除威胁的操作。跳过的威胁列表可能会更改，例如，如果可疑文件被删除或移动。若要接收最新的威胁列表，请运行完整设备扫描。为了确保可靠地保护您的数据，请消除所有检测到的对象。

- 隔离

7. 单击“应用”按钮以保存所作的更改。

与 Kaspersky Security Center 的下次设备同步之后可配置移动设备设置。

若要在移动设备上配置病毒扫描的自动运行，请执行以下操作：

1. 在控制台树的“受管设备”文件夹中，选择 Android 设备所属的管理组。
2. 在所选组的工作区中，选择“策略”选项卡。
3. 通过双击任意列打开策略属性窗口。
4. 在策略“属性”窗口中选择“扫描”区域。
5. 要阻止可被犯罪分子利用来损害设备或用户数据的广告软件和应用程序，请选中“检测可被犯罪分子用来对用户的设备和数据造成损害的广告软件、自动拨号程序和应用程序”复选框。

6. 在“检测到威胁时执行的操作”列表中，选择以下选项之一：

- 删除

  检测到的对象将被自动删除。不要求用户做任何其他操作。删除对象之前，Kaspersky Endpoint Security for Android 将显示检测到对象的临时通知。

- 跳过

  如果检测到的对象被跳过，Kaspersky Endpoint Security for Android 会警告用户设备保护方面存在问题。有关跳过的对象的信息会显示在应用程序的“状态”部分中。对于每个跳过的威胁，应用程序都提供用户可以执行以消除威胁的操作。跳过的威胁列表可能会更改，例如，如果可疑文件被删除或移动。若要接收最新的威胁列表，请运行完整设备扫描。为了确保可靠地保护您的数据，请消除所有检测到的对象。

- 隔离

- 询问用户

  Kaspersky Endpoint Security for Android 应用程序将显示一条通知，提示用户选择要对检测到的对象采取的操作：“跳过”或“删除”。

  当应用程序检测到多个对象时，“询问用户”选项允许设备用户通过使用“应用到所有威胁”复选框将所选操作应用于每个文件。

  必须将 Kaspersky Endpoint Security for Android 设置为辅助功能，以确保在运行安卓 10.0 或更高版本的移动设备上显示通知。Kaspersky Endpoint Security for Android 会提示用户通过初始配置向导将该应用程序设置为可访问功能。用户可以跳过此步骤或以后在设备设置中禁用此服务。在这种情况下，Kaspersky Endpoint Security for Android 将显示一个 Android 系统窗口，提示用户选择要对检测到的对象采取的操作：“跳过”或“删除”。要对多个对象应用操作，您需要打开 Kaspersky Endpoint Security。

7. “计划扫描”区域允许您配置自动启动全部扫描设备系统文件的设置。若要执行操作，单击“计划”按钮，在“计划”窗口中指定全盘扫描频率和启动时间。

   在 Android 12 或更高版本上，如果设备处于省电模式，应用程序可能会晚于指定的时间执行此任务。

8. 单击“应用”按钮以保存所作的更改。

与 Kaspersky Security Center 的下次设备同步之后可配置移动设备设置。Kaspersky Endpoint Security for Android 将扫描所有文件，包括压缩文件的内容。

为了保持移动设备保护为最新，请配置反病毒数据库更新设置。

默认情况下设备漫游时禁用反病毒数据库更新。计划的反病毒数据库更新不会执行。

若要配置反病毒数据库更新的设置，请执行以下操作：

1. 在控制台树的“受管设备”文件夹中，选择 Android 设备所属的管理组。
2. 在所选组的工作区中，选择“策略”选项卡。
3. 通过双击任意列打开策略属性窗口。

4. 在策略“**属性**”窗口中选择“**数据库更新**”区域。

5. 如果您希望 Kaspersky Endpoint Security for Android 在设备漫游时根据更新计划下载数据库更新，请选择“**漫游时数据库更新**”区域中的“**允许漫游时数据库更新**”选框。

   即使清空了此选框，用户可以在设备漫游时手动启动反病毒数据库更新。

6. 在“**数据库更新源**”区域中，指定 Kaspersky Endpoint Security for Android 接收并安装反病毒数据库更新所需的更新源：

   - **Kaspersky 服务器**

     将 Kaspersky 更新服务器用作更新源，将 Kaspersky Endpoint Security for Android 的数据库下载到用户移动设备上。要从 Kaspersky 服务器更新数据库，Kaspersky Endpoint Security for Android 传输数据到 Kaspersky（例如，更新任务运行 ID）。数据库更新过程中传输的数据列表提供在最终用户授权许可协议中。

   - **管理服务器**

     将 Kaspersky Security Center 管理服务器的存储库用作更新源，将 Kaspersky Endpoint Security for Android 的数据库下载到用户移动设备上。

   - **其他更新源**

     将第三方服务器用作更新源，将 Kaspersky Endpoint Security for Android 的数据库下载到用户移动设备上。在启动更新前，您应在下面的字段中输入 HTTP 服务器的地址（例如，http://domain.com/）。

7. 在“**计划的数据库更新**”区域中，配置用户设备上反病毒数据库自动更新设置。要执行此操作，请单击“**计划**”按钮，然后在“**计划**”窗口中指定更新的频率和开始时间。

   在 Android 12 或更高版本上，如果设备处于省电模式，应用程序可能会晚于指定的时间执行此任务。

8. 单击“**应用**”按钮以保存所作的更改。

与 Kaspersky Security Center 的下次设备同步之后可配置移动设备设置。

在互联网上保护 Android 设备

要保护移动设备用户在互联网上的个人数据，请启用 Web 保护。网页保护拦截散布恶意代码的恶意网站和钓鱼网站，这些网站以盗窃个人机密信息和获取财务账号权限为目的。Web 保护将在您打开网站前使用卡巴斯基安全网络云服务扫描网站。Web 保护还允许您根据预定义的允许的网站和阻止的网站的列表，配置用户对网站的访问。

Kaspersky Endpoint Security for Android 必须被设置为可访问功能。Kaspersky Endpoint Security for Android 会提示用户通过初始配置向导将该应用程序设置为可访问功能。用户可以跳过此步骤或以后在设备设置中禁用此服务。

安卓设备上的 Web 保护仅在 Google Chrome 浏览器（包括自定义标签功能）、Huawei Browser 和 Samsung Internet Browser 中可用。如果工作配置文件被使用且 Web 保护仅为工作配置文件所启用，Samsung Internet Browser 中的 Web 保护不阻止移动设备上的网站。

要在 Google Chrome、 Huawei browser 或 Samsung Internet Browser 中启用 Web 保护：

1. 在控制台树的“**受管设备**”文件夹中，选择 Android 设备所属的管理组。
2. 在所选组的工作区中，选择“**策略**”选项卡。
3. 通过双击任意列打开策略属性窗口。
4. 在策略“**属性**”窗口中选择“**Web 保护**”。
5. 要使用 Web 保护，您的设备用户必须阅读并接受关于以使用 Web 保护为目的的数据处理声明 (Web 保护声明)：
   a. 点击链接 **Web 保护声明**。
      这将打开**关于以使用 Web 保护为目的的数据处理声明**窗口。要接受 Web 保护声明，您必须阅读并接受隐私策略。
   b. 点击“隐私策略”链接。阅读并接受隐私策略。
      如果您不接受隐私策略，移动设备用户可以在初始化配置向导或应用中接受隐私策略（ → **关于** → **条款和条件** → **隐私策略**）。
   c. 选择 Web 保护声明接受模式：
      - **我已阅读并接受 Web 保护声明**
      - **请求从设备用户处接受 Web 保护声明**
      - **我不接受 Web 保护声明**
6. 如果您选择**我不接受 Web 保护声明**，Web 保护不阻止移动设备上的网站。移动设备用户无法在 Kaspersky Endpoint Security 中启用 Web 保护。
7. 选中“**启用 Web 保护**”选框。
8. 单击“**应用**”按钮以保存所作的更改。

与 Kaspersky Security Center 的下次设备同步之后可配置移动设备设置。

保护被盗或丢失设备的数据

本节介绍了如何在设备被盗或丢失时配置非授权访问保护设置。

向移动设备发送命令

要保护丢失或被盗的移动设备上的数据，您可以发送特殊命令（请参阅下表）。

用于保护丢失或被盗设备上的数据的命令

连接到 Kaspersky Security Center 的方法	命令	命令执行结果
Kaspersky	锁定	移动设备将被锁定。

Endpoint Security for Android	解锁	解锁运行着 Android 5.0 – 6.X 的移动设备后，屏幕解锁密码 (PIN code) 重置为“1234”。解锁运行着 Android 7.0 或更新版本的设备后，屏幕解锁密码不变。
	定位设备	设备将被定位并显示在 Google Maps 中。移动服务提供商收取发送短信和上网的费用。 在运行 Android 12 或更高版本的设备上，如果用户授予了“使用大致位置”权限，Kaspersky Endpoint Security for Android 应用程序首先会尝试获取精确的设备位置。如果获取不成功，则只有在不超过 30 分钟前已收到设备的大致位置时，才会返回该位置。否则，“**定位设备**”命令将失败。
	正面照	移动设备将被锁定。当有人试图解锁设备时，面部照片由设备的前置摄像头拍摄。移动服务提供商收取发送短信和上网的费用。 当试图解锁设备时，用户自动同意面部照片。 如果摄像头的使用权限已被撤销，移动设备会显示通知并提示提供权限。在运行 Android 12 或更高版本的移动设备上，如果通过“快速设置”撤销了使用摄像头的权限，则不会显示通知，但拍摄的照片为黑色。
	警报	移动设备发出警报。警报响 5 分钟（如果设备的电池电量低，则响 1 分钟）。
	擦除公司数据	擦除容器中的数据、公司电子邮件账户、用于连接至公司 Wi-Fi 网络和 VPN 的设置、接入点名称 (APN)、安卓工作配置文件、KNOX 容器和 KNOX License Manager 密钥。
	恢复出厂设置	所有数据都将从移动设备中删除，设置将回滚至其出厂值。执行此命令后，设备将无法接收或执行后续命令。
iOS MDM 配置文件	锁定	移动设备将被锁定。
	解锁	将禁用使用 PIN 码锁定的移动设备。之前指定的 PIN 码已重置。
	擦除公司数据	将从设备中删除所有已安装的配置配置文件、供给配置文件、iOS MDM 配置文件以及已选择“**与 iOS MDM 配置文件一起删除**”选框的应用程序。
	恢复出厂设置	所有数据都将从移动设备中删除，设置将回滚至其出厂值。执行此命令后，设备将无法接收或执行后续命令。
Exchange 邮箱	恢复出厂设置	所有数据都将从移动设备中删除，设置将回滚至其出厂值。执行此命令后，设备将无法接收或执行后续命令。

执行 Kaspersky Endpoint Security for Android 的命令需要特殊的权利和权限。当初始配置向导正在运行时，Kaspersky Endpoint Security for Android 会提示用户授予应用程序所有必需的权利和权限。用户可以跳过这些步骤或以后在设备设置中禁用这些权限。如果是这种情况，将不可能执行命令。

在运行 Android 10.0 或更高版本的设备上，用户必须授予“始终”权限才能访问位置。在运行 Android 11.0 或更高版本的设备上，用户必须授予“使用应用程序时”权限才能访问摄像头。否则，反盗窃命令将不起作用。用户将被通知这一限制，并再次被提示授予所需级别的权限。如果用户为摄像头权限选择“仅此一次”选项，则认为应用程序授予了访问权限。如果再次请求摄像头权限，建议直接联系用户。

要详细了解如何在管理控制台通过移动设备列表发送命令，请参阅 *Kaspersky Security Center 帮助*。

解锁移动设备

您可以使用以下方法解锁移动设备：

- 发送移动设备解锁命令。
- 在移动设备上输入一次性解锁码（仅适用于安卓设备）。

在某些设备（例如，华为、魅族和小米）上，您必须手动将 Kaspersky Endpoint Security for Android 添加到在操作系统启动时启动的应用程序列表。如果未将该应用程序添加到列表，只能使用一次性解锁代码解锁设备。不能使用命令解锁设备。

要详细了解如何在管理控制台通过移动设备列表发送命令，请参阅 *Kaspersky Security Center 帮助*。

一次性解锁码 是用于解锁移动设备的应用程序密码。一次性代码由应用程序生成，对于每个移动设备唯一。您可以在组策略设置中的“**反盗窃**”区域更改一次性代码的长度（4、8 或 16 位数）。

要使用一次性代码解锁移动设备：

1. 在控制台树中，选择“**移动设备管理**”→“**移动设备**”。
2. 选择您要获取其一次性解锁代码的移动设备。
3. 通过双击打开移动设备属性窗口。
4. 选择“**应用**”→“**Kaspersky Endpoint Security for Android**”。
5. 通过双击打开 Kaspersky Endpoint Security 属性窗口。
6. 选择“**反盗窃**”区域。
7. 选定设备的唯一代码将显示在“**一次性设备解锁码**”区域的“**一次性代码**”字段中。
8. 使用任意可用的方法（例如电子邮件）将一次性代码告知已锁定设备的用户。
9. 用户在 Kaspersky Endpoint Security for Android 锁定的设备的屏幕上输入一次性代码。

移动设备会被解锁。解锁运行着 Android 5.0 – 6.X 的移动设备后，屏幕解锁密码 (PIN code) 重置为“1234”。解锁运行着 Android 7.0 或更新版本的设备后，屏幕解锁密码不变。

数据加密

要保护数据以防非授权的访问，您必须启用设备上所有数据的加密（例如，账户凭据、外部设备和应用、以及电子邮件消息、SMS 消息、联系人、照片和其他文件）。对于加密数据的访问，您必须指定特殊密钥 – 设备解锁密码。如果数据被加密，对它的访问仅在设备解锁时可行。

在密码锁定 iOS 设备上数据加密默认被启用（**设置 → Touch ID / Face ID 和密码 → 启用密码**）。

要在 Android 设备上加密所有数据：

1. 在 Android 设备上启用屏幕锁(**设置 → 安全 → 屏幕锁**)。

2. 设置与企业安全需求合规的设备解锁密码。

不建议使用图案锁来解锁设备。在某些运行 Android 6.0 或更高版本的 Android 设备上，在加密数据和重启 Android 设备后，您必须输入数字密码而不是图案锁来解锁设备。该问题关乎可访问功能服务的操作。要在该情况下解锁设备屏幕，请将图案锁转换为数字密码。有关将图案锁转换为数字密码的详细信息，请参考移动设备制造商的技术支持网站。

3. 在设备上启用对所有设备的加密(**设置** → **安全** → **加密数据**)。

配置设备解锁密码强度

要保护对用户移动设备的访问，您应该设置设备解锁密码。

本节包含有关如何在安卓和 iOS 设备上配置密码保护的信息。

为安卓设备配置强解锁密码

若要确保安卓设备安全，您需要配置使用密码，在设备从睡眠模式唤醒时提示用户输入密码。

如果解锁密码太弱，您可以对设备上的用户活动施加限制（例如锁定设备）。您可以使用“合规性控制”组件施加限制。为此，在扫描规则设置中，您必须选择 **解锁密码不符合安全要求** 标准。

在某些运行 Android 7.0 或更高版本的三星设备上，当用户尝试配置不受支持的方法（例如，图形密码）来解锁设备时，如果满足以下条件，设备可能会锁定：Kaspersky Endpoint Security for Android 卸载保护已启用并且设置了屏幕解锁密码长度要求。要解锁设备，您必须 发送特殊命令到设备。

若要配置使用解锁密码，请执行以下操作：

1. 在控制台树的“**受管设备**”文件夹中，选择 Android 设备所属的管理组。
2. 在所选组的工作区中，选择“**策略**”选项卡。
3. 通过双击任意列打开策略属性窗口。
4. 在策略“**属性**”窗口中选择“**设备管理**”区域。
5. 如果您希望应用程序检查是否设置了解锁密码，请在“**屏幕锁定**”区域中选中“**需要设置屏幕解锁密码**”选框。

   如果应用程序检测到设备上未设置任何系统密码，则提示用户进行设置。密码根据管理员定义的参数来设置。
6. 指定“最小字符数”。

   用户密码的最小字符数。可能值：4 到 16 个字符。

   默认情况下，用户的密码包含 4 个字符。

在运行 Android 10.0 或更高版本的设备上，Kaspersky Endpoint Security 将密码强度要求解析为系统值之一：中或高。

运行 Android 10.0 或更高版本的设备的值通过以下规则确定：

- 如果所需的密码长度是 1 到 4 个符号，该应用程序会提示用户设置中等强度的密码。它必须是没有重复并且没有顺序（例如 1234）的数字 (PIN)，或者是字母/字母数字。PIN 或密码必须至少有 4 个字符长。
- 如果所需的密码长度是 5 个或更多符号，该应用程序会提示用户设置高强度密码。它必须是没有重复并且没有顺序的数字 (PIN)，或者是字母/字母数字（密码）。PIN 必须至少为 8 位数字；密码必须至少有 6 个字符长。

7. 如果您希望用户能使用指纹解锁屏幕，请选中“**允许使用指纹**”选框。如果解锁密码不符合公司安全要求，则无法使用指纹扫描器解锁屏幕。

在运行 Android 10.0 或更高版本的设备上，使用指纹解锁屏幕只能在工作配置文件中管理。

Kaspersky Endpoint Security for Android 不会限制使用指纹扫描器来登录应用程序或确认购买

在某些三星设备上，无法阻止使用指纹解锁屏幕。在某些三星设备上，如果解锁密码不符合企业安全要求，Kaspersky Endpoint Security for Android 不会阻止使用指纹解锁屏幕。

在设备设置中添加指纹后，用户可以使用以下方法解锁屏幕：

- 将手指按在指纹扫描器上（主要方法）。
- 输入解锁密码（备用方法）。

8. 单击“**应用**”按钮以保存所作的更改。

与 Kaspersky Security Center 的下次设备同步之后可配置移动设备设置。

为 iOS MDM 设备配置强解锁密码

若要保护 iOS MDM 设备数据，请配置解锁密码强度设置。

默认情况下，用户可以使用简单密码。*简单密码*是包含连续或重复字符的密码，例如“abcd”或“2222”。用户不需要输入包含特殊字符的字母数字密码。默认情况下，密码有效期和密码输入尝试次数不受限制。

若要配置 iOS MDM 设备解锁密码的强度设置，请执行以下步骤：

1. 在控制台树的“**受管设备**”文件夹中，选择 iOS MDM 设备所属的管理组。
2. 在所选组的工作区中，选择“**策略**”选项卡。
3. 通过双击打开策略属性窗口。
4. 在策略“**属性**”窗口中选择“**密码**”区域。
5. 在**密码设置**区域中，选中**将设置应用于设备**选框。
6. 配置解锁密码强度设置：
   - 若要允许用户使用简单密码，请选择“**允许简单密码**”选框。

- 若要要求用户在密码中使用字母和数字，请选择“**提示输入字母数字值**”选框。
- 在“**最小密码长度**”列表中，选择最小密码长度（以字符为单位）。
- 在“**特殊字符最小数量**”列表中，选择密码中特殊字符（例如，“$”、“&”和“!”）的最少数量。
- 在“**密码最长有效期**”字段中，指定密码保持为当前密码的时间期限（单位：天数）。这段时间过后，Kaspersky Device Management for iOS 会提示用户更改密码。
- 在“**启用自动锁定**”列表中，选择在多长时间后启用 iOS MDM 设备自动锁定。
- 在“**密码历史**”字段中，指定已使用密码的数量（包括当前密码），在用户更改旧密码时，Kaspersky Device Management for iOS 会将旧密码和新密码进行对比。如果密码匹配，新密码将被拒绝。
- 在**无需密码解锁的最长时间**列表中，选择用户在多长时间内不用输入密码即可解锁 iOS MDM 设备。
- 在“**访问尝试的最大次数**”列表中，选择用户在输入 iOS MDM 设备解锁密码时可进行的访问尝试次数。

7. 单击“**应用**”按钮以保存所作的更改。

这样，在应用策略后，Kaspersky Device Management for iOS 将在用户的移动设备上检查设置的密码的强度。如果设备解锁密码强度不符合策略，将提示用户更改密码。

为 EAS 设备配置强解锁密码

设置强解锁密码，保护 EAS 设备数据。

默认情况下，在移动设备开机时，Kaspersky Device Management for iOS 不会提示用户输入或设置解锁密码。

若要配置 EAS 设备解锁密码的强度设置，请执行以下操作：

1. 在控制台树的“**受管设备**”文件夹中，选择 EAS 设备所属的管理组。
2. 在所选组的工作区中，选择“**策略**”选项卡。
3. 通过双击打开策略属性窗口。
4. 在策略“属性”窗口中，选择“**密码**”区域。
5. 在**密码设置**区域中，选中**提示输入密码**选框。
6. 配置解锁密码强度设置：
   - 若需要要求用户在密码中使用字母和数字，请选择“**提示输入字母数字值**”选框。在“**最少字符集数量**”字段中，指定字母数字密码的强度级别。可能值：1 到 4。值“1”对应的是最低的强度级别。
   - 若要允许用户使用密码恢复功能，请选择“**启用密码恢复**”选框。
   - 如果您要子啊设备内存中加密文件，请选择“**需要加密设备**”选框。
   - 如果您要加密内存卡上的文件，请选择“**需要加密内存卡**”选框。
   - 若要允许用户使用仅包含数字的简单密码，请选择“**允许简单密码**”选框。

- 若要限制输入访问设备的密码的尝试次数，请选择“**访问尝试的最大次数**”选框。在该选框右侧的字段中，指定用户为解锁设备可进行的密码输入尝试次数。如果用户在指定的连续尝试次数后未能输入正确的密码，Kaspersky Device Management for iOS 会擦除所有设备数据。

- 若要指定用户密码的最短长度，请选择“**最小密码长度**”选框。在该选框右侧的字段中指定密码字符的最少数量。可能值：4 到 16 个字符。

- 若要提示用户在设备空闲一段时间后输入密码，请选中**密码输入的新尝试前的空闲时间（分钟）**选框。在该选框右侧的字段中指定空闲分钟数。这段时间过后，应用程序会提示用户输入密码。

- 若要限制密码有效期，请选择“**密码有效期（天）**”选框。在该选框右侧的字段中指定密码有效期。这段时间过后，应用程序会提示用户更改密码。

- 在“**密码历史**”字段中，您可以指定不能重复使用的最近的旧密码的数量。

7. 单击“**应用**”按钮以保存所作的更改。

与 Kaspersky Security Center 的下次设备同步之后可配置移动设备设置。一旦应用该策略，Kaspersky Device Management for iOS 将检查是否在用户的移动设备上设置了密码。如果设备上尚未设置解锁密码，则会提示用户进行设置。设置密码时应考虑策略设置。如果已设置设备解锁密码，但它不符合策略，将提示用户更改密码。

配置虚拟专用网 (VPN)

本节包含有关配置虚拟专用网络 (VPN) 设置以安全连接到 Wi-Fi 网络的信息。

在安卓设备上配置 VPN（仅限三星）

若要将安卓设备安全地连接到 Wi-Fi 网络并保护数据传输，您应该配置 VPN（虚拟专用网）设置。

只能为三星设备配置 VPN。

在使用虚拟专用网时应考虑以下要求：

- 必须在防火墙设置中允许使用 VPN 连接的应用程序。

- 在该策略中配置的虚拟专用网设置不能应用于系统应用程序。系统应用程序的 VPN 连接必须手动配置。

- 某些使用 VPN 连接的应用程序需要在第一次启动时配置附加设置。若要配置设置，必须在应用程序设置中启用 VPN 连接。

若要配置用户移动设备上的 VPN，请执行以下操作：

1. 在控制台树的“**受管设备**”文件夹中，选择 Android 设备所属的管理组。

2. 在所选组的工作区中，选择“**策略**”选项卡。

3. 通过双击任意列打开策略属性窗口。

4. 在策略“**属性**”窗口中选择“**管理三星 KNOX**”→“**管理三星设备**”区域。

5. 在“**VPN**”区域中，单击“**配置**”按钮。
   这将打开“**VPN 网络**”窗口。

6. 在“**连接类型**”下拉列表中选择 VPN 连接的类型。

7. 在“**网络名称**”字段中输入 VPN 隧道的名称。

8. 在“**服务器地址**”字段中，输入 VPN 服务器的网络名称或 IP 地址。

9. 在“**DNS 搜索域**”列表中，输入要自动添加到 DNS 服务器名称中的 DNS 搜索域。
   您可以指定多个 DNS 搜索域，用空格将它们分隔。

10. 在“**DNS 服务器**”字段中，输入 DNS 服务器的完整域名或 IP 地址。
    您可以指定多个 DNS 服务器，用空格将它们分隔。

11. 在“**路由**”字段中，输入通过 VPN 连接与其交换数据的网络 IP 地址的范围。

    如果未在“**路由**”字段中指定 IP 地址的范围，所有互联网流量都将通过 VPN 连接传输。

12. 附加配置“**IPSec Xauth PSK**”和“**L2TP IPSec PSK** ”类型网络的以下设置：

    a. 在“**IPSec 共享密钥**”字段中，输入预设 IPSec 安全密钥的密码。

    b. 在“**IPSec ID**”字段中输入移动设备用户的名称。

13. 对于 **L2TP IPSec PSK** 网络，您还可以在“**L2TP 密钥**”字段中为 L2TP 密钥指定密码。

14. 对于 **PPTP** 网络，选择“**使用 SSL 连接**”选框，以便在移动设备连接至 VPN 服务器时应用程序使用 MPPE (Microsoft Point-to-Point Encryption) 数据加密方法保护数据传输。

15. 单击“**应用**”按钮以保存所作的更改。

与 Kaspersky Security Center 的下次设备同步之后可配置移动设备设置。

在 iOS MDM 设备上配置 VPN

若要将 iOS MDM 设备连接至虚拟专用网 (VPN) 并在连接至 VPN 期间保护数据，请配置 VPN 连接设置。

若要在用户的 iOS MDM 设备上配置 VPN 连接，请执行以下操作：

1. 在控制台树的“**受管设备**”文件夹中，选择 iOS MDM 设备所属的管理组。

2. 在所选组的工作区中，选择“**策略**”选项卡。

3. 通过双击打开策略属性窗口。

4. 在策略“**属性**”窗口中选择“**VPN**”区域。

5. 在“**VPN 网络**”区域中单击“**添加**”按钮。
   这将打开“**VPN 网络**”窗口。

6. 在“**网络名称**”字段中输入 VPN 隧道的名称。

7. 在“**连接类型**”下拉列表中选择 VPN 连接的类型：

   - **L2TP**（第 2 层隧道协议）。该连接支持使用 MS-CHAP v2 密码、双重身份验证和使用公钥的自动身份验证对 iOS MDM 移动设备用户进行身份验证。
   - **PPTP**（点对点隧道协议）。该连接支持使用 MS-CHAP v2 密码和双重身份验证对 iOS MDM 移动设备用户进行身份验证。
   - **IPSec (Cisco)**。该连接支持基于密码的用户认证、双重身份验证和使用公钥与证书的自动身份验证。
   - **Cisco AnyConnect**。该连接支持版本 8.0(3).1 或更高版本的 Cisco Adaptive Security Appliance (ASA) 防火墙。若要配置 VPN 连接，请从 App Store 将 Cisco AnyConnect 应用程序安装到 iOS MDM 移动设备上。
   - **Juniper SSL**。该连接支持版本 6.4 或更高版本的 SA 系列 Juniper Networks SSL VPN 网关，该网关包含版本 7.0 或更高版本的 Juniper Networks IVE 程序包。若要配置 VPN 连接，请从 App Store 将 JUNOS 应用程序安装到 iOS MDM 移动设备上。
   - **F5 SSL**。该连接支持 F5 BIG-IP Edge Gateway、Access Policy Manager 和 Fire SSL VPN 解决方案。若要配置 VPN 连接，请从 App Store 将 F5 BIG-IP Edge Client 应用程序安装到 iOS MDM 移动设备上。
   - **SonicWALL Mobile Connect**。该连接支持版本 10.5.4 或更高版本的 SonicWALL Aventail E-Class Secure Remote Access 设备、版本 5.5 或更高版本的 SonicWALL SRA 设备以及 SonicWALL Next-Generation Firewall 设备，包括 TZ、NSA 和包含版本 5.8.1.0 或更高版本的 SonicOS 的 E-Class NSA。若要配置 VPN 连接，请从 App Store 将 SonicWALL Mobile Connect 应用程序安装到 iOS MDM 移动设备上。
   - **Aruba VIA**。该连接支持 Aruba Networks 移动访问控制器。若要配置它们，请从 App Store 将 Aruba Networks VIA 应用程序安装到 iOS MDM 移动设备上。
   - **自定义 SSL**。该连接支持使用密码、证书和双重身份验证对 iOS MDM 移动设备用户进行身份验证。

8. 在“**服务器地址**”字段中，输入 VPN 服务器的网络名称或 IP 地址。
9. 在**账户名**字段中，输入要在 VPN 服务器上进行身份验证的帐户名。您可以使用“**可用宏**”下拉列表中的宏。
10. 根据选择的虚拟专用网类型配置 VPN 连接的安全设置。
11. 如有必要，配置通过代理服务器连接 VPN 的设置。

    a. 选择“**代理服务器设置**”选项卡。

    b. 选择代理服务器配置模式和指定连接设置。

    c. 单击“**确定**”。

    这样，已在 iOS MDM 设备上配置设备通过代理服务器连接 VPN 的设置。

12. 单击“**确定**”。

    新的 VPN 将显示在列表中。

13. 单击“**应用**”按钮以保存所作的更改。

这样，一旦应用该策略，将在用户的 iOS MDM 设备上配置 VPN 连接。

在安卓设备上配置防火墙（仅限三星）

配置防火墙设置，监控用户的移动设备上的网络连接。

若要在移动设备上配置防火墙，请执行以下操作：

1. 在控制台树的“**受管设备**”文件夹中，选择 Android 设备所属的管理组。
2. 在所选组的工作区中，选择“**策略**”选项卡。
3. 通过双击任意列打开策略属性窗口。
4. 在策略“**属性**”窗口中选择“**管理三星 KNOX**”→“**管理三星设备**”区域。
5. 在“**防火墙**”窗口中，单击“**配置**”。
   “**防火墙**”窗口将打开。
6. 选择防火墙设置：
   - 若要允许所有入站和出站连接，请将滑块移动到“**全部允许**”。
   - 若要阻止除排除列表中的应用程序的网络活动以外的所有网络活动，请将滑块向上滑动到“**全部阻止(排除项除外)**”。
7. 如果您已将防火墙模式设置为“**全部阻止(排除项除外)**”，请创建排除列表：
   a. 单击“**添加**”。
      这将打开“**防火墙排除项**”窗口。
   b. 在“**应用程序名称**”字段中输入移动应用程序的名称。
   c. 在“**包名称**”字段中输入移动应用程序包的系统名称（例如 `com.mobileapp.example`）。
   d. 单击“**确定**”。
8. 单击“**应用**”按钮以保存所作的更改。

与 Kaspersky Security Center 的下次设备同步之后可配置移动设备设置。

防止 Kaspersky Endpoint Security for Android 被删除

为了保护移动设备和遵守企业安全要求，您可以启用保护以防止删除 Kaspersky Endpoint Security for Android。在这种情况下，用户无法使用 Kaspersky Endpoint Security for Android 界面删除该应用程序。当使用安卓操作系统的工具删除应用程序时，系统会提示您禁用 Kaspersky Endpoint Security for Android 的管理员权限。禁用权限后，移动设备将被锁定。

在某些运行 Android 7.0 或更高版本的三星设备上，当用户尝试配置不受支持的方法（例如，图形密码）来解锁设备时，如果满足以下条件，设备可能会锁定：Kaspersky Endpoint Security for Android 卸载保护已启用并且设置了屏幕解锁密码长度要求。要解锁设备，您必须 发送特殊命令到设备。

若要启用保护以防止删除 Kaspersky Endpoint Security for Android，请执行以下操作：

1. 在控制台树的“**受管设备**”文件夹中，选择 Android 设备所属的管理组。

2. 在所选组的工作区中，选择“**策略**”选项卡。

3. 通过双击任意列打开策略属性窗口。

4. 在策略“**属性**”窗口中选择“**其他**”区域。

5. 在“**卸载 Kaspersky Endpoint Security for Android**”区域中，清除“**允许卸载 Kaspersky Endpoint Security for Android**”选框。

   要保护在运行安卓 7.0 或更高版本的设备上的应用程序不会被卸载，必须将 Kaspersky Endpoint Security for Android 设置为可访问功能。当初始配置向导正在运行时，Kaspersky Endpoint Security for Android 会提示用户授予应用程序所有必需的权限。用户可以跳过这些步骤或以后在设备设置中禁用这些权限。在这种情况下，不保护该应用程序不被卸载。

6. 单击“**应用**”按钮以保存所作的更改。

与 Kaspersky Security Center 的下次设备同步之后可配置移动设备设置。如果尝试删除应用程序，移动设备将被锁定。

检测设备入侵（根权限）

Kaspersky Security for Mobile 允许您检测设备入侵（根权限/越狱）。被黑客入侵的设备上的系统文件不受保护，因此可能会被修改。此外，来自未知来源的第三方应用可能会安装在被黑客入侵的设备上。在检测到黑客尝试后，建议您立即恢复设备的正常操作。

若要检测用户何时获取根权限，Kaspersky Endpoint Security for Android 将使用以下服务：

- *Embedded service of Kaspersky Endpoint Security for Android* 是一种 Kaspersky 服务，用于检查移动设备用户是否已获取根权限 (Kaspersky Mobile Security SDK)。
- *SafetyNet Attestation* 是一种 Google 服务，用于检查操作系统的完整性，分析设备硬件和软件，以及识别其他安全问题。有关 SafetyNet Attestation 的更多详细信息，请访问 Android 技术支持网站。

如果设备被黑客入侵，您会收到一条通知。您可以在管理服务器工作区的“**监控**”选项卡上查看黑客入侵通知。还可以在事件通知设置中停用有关黑客的通知。

在运行安卓的设备上，如果设备被黑客入侵，您可以对设备上的用户活动施加限制（例如锁定设备）。您可以通过使用 合规性控制 组件施加限制（参见下图）。为此，请在扫描规则设置中，选择“**设备已取得根权限**”条件。

在 iOS MDM 设备上配置全局 HTTP 代理

若要保护用户的互联网流量，请配置通过代理服务器将 iOS MDM 设备连接至互联网。

仅受控制的设备可以通过代理服务器自动连接至互联网。

若要在 iOS MDM 设备上配置全局 HTTP 代理设置，请执行以下操作：

1. 在控制台树的“**受管设备**”文件夹中，选择 iOS MDM 设备所属的管理组。

2. 在所选组的工作区中，选择“**策略**”选项卡。

3. 通过双击打开策略属性窗口。

4. 在策略“**属性**”窗口中选择“**全局 HTTP 代理**”区域。

5. 在“**全局 HTTP 代理设置**”区域中，选中“**将设置应用于设备**”选框。

6. 选择全局 HTTP 代理配置的类型。

> 默认情况下，选择手动配置全局 HTTP 代理的类型，禁止用户在不连接代理服务器的情况下连接到受控网络。*受控网络* 是需要在不连接代理服务器的情况下，对移动设备进行初步身份验证的无线网络。

- 若要手动指定代理服务器连接设置，请执行以下操作：

  a. 在“**代理设置类型**”下拉列表中，选择“**手动**”。

  b. 在“**代理服务器地址和端口**”字段中，输入主机的名称或代理服务器的 IP 地址和代理服务器端口号。

  c. 在“**用户名**”字段中，设置用于代理服务器身份验证的用户帐户名。您可以使用“**可用宏**”下拉列表中的宏。

  d. 在“**密码**”字段中，设置用于代理服务器身份验证的用户帐户密码。

  e. 若要允许用户访问受控网络，请选择“**允许访问强制网络而不用连接到代理**”选框。

- 若要使用预定义的 PAC（代理自动配置）文件配置代理服务器连接设置，请执行以下步骤：

  a. 在“**代理设置类型**”下拉列表中，选择“**自动**”。

  b. 在“**PAC 文件的地址**”字段中输入 PAC 文件的网址（例如：http://www.example.com/filename.pac）。

  c. 若要允许用户在无法访问 PAC 文件时，不使用代理服务器将移动设备连接至无线网络，请选中“**如果无法访问 PAC 文件，则允许直接连接**”选框。

  d. 若要允许用户访问受控网络，请选择“**允许访问强制网络而不用连接到代理**”选框。

7. 单击“**应用**”按钮以保存所作的更改。

这样，一旦应用该策略，移动设备用户将通过代理服务器连接至互联网。

向 iOS MDM 设备添加安全证书

为了简化用户身份验证和确保数据安全，请在用户的 iOS MDM 设备上添加证书。在网络交换过程中，保护使用证书签名的数据不被更改。使用证书加密数据，可提高数据安全级别。证书还可以用于验证用户的身份。

Kaspersky Device Management for iOS 支持以下证书标准：

- **PKCS#1** – 使用基于 RSA 算法的公钥加密。
- **PKCS#12** – 存储和传输证书与私钥。

若要在用户的 iOS MDM 设备上添加安全证书，请执行以下操作：

1. 在控制台树的“**受管设备**”文件夹中，选择 iOS MDM 设备所属的管理组。

2. 在所选组的工作区中，选择“策略”选项卡。

3. 通过双击打开策略属性窗口。

4. 在策略“属性”窗口中选择“证书”区域。

5. 在“证书”区域中单击“添加”按钮。
   “证书”窗口将打开。

6. 在“文件名”字段中，指定证书的路径：

   > PKCS#1 证书文件的扩展名为 cer、crt 或 der。PKCS#12 证书文件的扩展名为 p12 或 pfx。

7. 单击“打开”。
   如果证书受密码保护，请指定密码。新的证书显示在列表中。

8. 单击“应用”按钮以保存所作的更改。

这样，一旦应用该策略，将提示用户安装已创建的列表中的证书。

向 iOS MDM 设备添加 SCEP 配置文件

您必须添加 SCEP 配置文件，以便 iOS MDM 设备用户通过互联网自动接收来自认证中心的证书。SCEP 配置文件可支持简单证书注册协议。

默认添加具有以下设置的 SCEP 配置文件：

- 不使用备用主题名称注册证书。
- 进行三次 SCEP 服务器轮询尝试，每次间隔 10 秒。如果证书签名的所有尝试失败，您必须生成新的证书签名请求。
- 接收的证书不能用于数据签名或加密。

您可以在添加 SCEP 配置文件时编辑指定的设置。

若要添加 SCEP 配置文件，请执行以下操作：

1. 在控制台树的“受管设备”文件夹中，选择 iOS MDM 设备所属的管理组。

2. 在所选组的工作区中，选择“策略”选项卡。

3. 通过双击打开策略属性窗口。

4. 在策略“属性”窗口中选择“SCEP”区域。

5. 在“SCEP 配置文件”区域中单击“添加”按钮。
   “SCEP 配置文件”窗口将打开。

6. 在“服务器网址”字段中，输入认证中心部署所在的 SCEP 服务器的网址。
   网址可以包含 IP 地址或完整的域名 (FQDN)。例如：http://10.10.10.10/certserver/companyscep。

7. 在“**名称**”字段中，输入部署在 SCEP 服务器上的认证中心的名称。

8. 在“**主题**”字段中，输入具有 X.500 证书中包含的 iOS MDM 设备用户属性的字符串。

   属性可以包含国家/地区 (C)、组织 (O) 和通用用户名 (CN) 的详细信息。例如：/C=RU/O=MyCompany/CN=User/。您也可以使用 RFC 5280 中指定的其他属性。

9. 在**使用者可选名称类型**下拉列表中，选择 SCEP 服务器的主题的备用名称的类型：

   - **否** – 不使用备用名称识别。
   - **RFC 822 名称** – 使用电子邮件地址识别。必须根据 RFC 822 指定电子邮件地址。
   - **DNS 名称** – 使用域名识别。
   - **URI** – 使用 IP 地址或 FQDN 格式地址识别。

   您可以使用主题的备用名称识别 iOS MDM 移动设备的用户。

10. 在**使用者可选名称**字段中，输入 X.500 证书的主题的备用名称。使用者可选名称的值取决于主题类型：用户电子邮件地址、域或网址。

11. 在**NT 使用者名称**字段中，输入 Windows NT 网络上的 iOS MDM 移动设备用户的 DNS 名称。

    NT 使用者名称包含在发送至 SCEP 服务器的证书请求中。

12. 在“**SCEP 服务器上轮询尝试次数**”字段中，指定轮询 SCEP 服务器以获取签名证书的最大尝试次数。

13. 在“**尝试频率（秒）**”字段中，指定轮询 SCEP 服务器以获取签名证书的尝试之间的时间间隔（单位：秒）。

14. 在“**注册申请**”字段中，输入预发布的注册密钥。

    在进行证书签名之前，SCEP 服务器请求移动设备用户提供密钥。如果该字段留空，则 SCEP 不会请求提供密钥。

15. 在“**密钥大小**”下拉列表中，选择注册密钥的大小（单位：位）：1024 或 1024 位。

16. 若要允许用户使用从 SCEP 服务器接收的证书作为签名证书，请选择“**用于签名**”选框。

17. 若要允许用户将从 SCEP 服务器接收的证书用于数据加密，请选择“**用于加密**”选框。

    禁止将 SCEP 服务器证书同时用作数据签名证书和数据加密证书。

18. 在“**证书指纹**”字段中，输入一个用于验证认证中心响应的真实性的唯一的证书指纹。您可以将证书指纹与 SHA-1 或 MD5 哈希算法配合使用。您可以手动复制证书指纹或使用“**从证书创建**”按钮选择证书。在使用“**从证书创建**”按钮创建指纹时，指纹会自动添加到该字段。

    如果移动设备和认证中心之间的数据交换通过 HTTP 协议进行，则必须指定证书指纹。

19. 单击“**确定**”。

    新的 SCEP 配置文件显示在列表中。

20. 单击“**应用**”按钮以保存所作的更改。

这样，一旦应用该策略，用户的移动设备将配置成通过互联网自动接收来自认证中心的证书。

控制

本节包含有关如何在 Kaspersky Security Center 管理控制台中远程监控移动设备的信息。

配置限制

本节提供有关如何配置移动设备功能的用户访问的说明。

运行 Android 10 及更高版本的设备的特殊注意事项

Android 10 引入了针对 API 29 或更高版本的诸多更改和限制。其中一些更改会影响某些应用程序特性的可用性或功能。以下注意事项仅适用于运行 Android 10 或更高版本的设备。

启用、禁用和配置 Wi-Fi 的能力

- 可以在 Kaspersky Security Center 的管理控制台中添加、删除和配置 Wi-Fi 网络。将 Wi-Fi 网络添加到策略后，Kaspersky Endpoint Security 在首次连接到 Kaspersky Security Center 时会收到此网络配置。
- 当设备检测到通过 Kaspersky Security Center 配置的网络时，Kaspersky Endpoint Security 会提示用户连接到该网络。如果用户选择连接到该网络，则自动应用通过 Kaspersky Security Center 配置的所有设置。随后，当设备在有效范围内时就会自动连接到该网络，而不会向用户显示进一步的通知。
- 如果用户的设备已经连接到其他 Wi-Fi 网络，有时可能不会提示用户批准增加网络。在这种情况下，用户必须关闭 Wi-Fi 再重新打开才能收到建议。
- 当 Kaspersky Endpoint Security 建议用户连接到 Wi-Fi 网络，但用户拒绝连接时，应用程序更改 Wi-Fi 状态的权限将被撤销。Kaspersky Endpoint Security 随后便无法建议连接到 Wi-Fi 网络，直到用户转到“**设置 → 应用程序和通知 → 特殊应用程序访问权限 → Wi-Fi 控制 → Kaspersky Endpoint Security**”再次授予权限。
- 仅支持开放网络和使用 WPA2-PSK 加密的网络。不支持 WEP 和 WPA 加密。
- 如果应用程序先前建议的网络密码发生变化，用户必须手动从已知网络列表中删除该网络。然后，设备将能够从 Kaspersky Endpoint Security 收到网络建议并连接到该网络。
- 当设备操作系统从 Android 9 或更早版本更新到 Android 10 或更高版本，并且/或者运行 Android 10 或更高版本的设备上安装的 Kaspersky Endpoint Security 更新后，以前通过 Kaspersky Security Center 添加的网络无法通过 Kaspersky Security Center 策略进行修改或删除。但是，用户可以在设备设置中手动修改或删除此类网络。
- 在运行 Android 10 的设备上，用户尝试手动连接到受保护的建议网络时会被提示输入密码。自动连接不需要输入密码。如果用户的设备已连接到某个其他 Wi-Fi 网络，则用户必须先断开与该网络的连接，然后才能自动连接到建议的网络之一。
- 在运行 Android 11 的设备上，用户可以手动连接到应用程序建议的受保护网络，而无需输入密码。
- 从设备中删除 Kaspersky Endpoint Security 后，该应用程序先前建议的网络将被忽略。
- 不支持禁止使用 Wi-Fi 网络。

摄像头访问权限

- 在运行 Android 10 的设备上，不能完全禁止使用摄像头。但仍然可以在工作配置文件中禁止使用摄像头。
- 如果第三方应用程序尝试访问设备的摄像头，则该应用程序将被阻止，并且用户将收到问题通知。但是，无法阻止在后台模式下运行的应用程序使用摄像头。
- 当外置摄像头与设备断开连接时，在某些情况下，可能会显示摄像头不可用的通知。

管理屏幕解锁方式

- Kaspersky Endpoint Security 现在将密码强度要求解析为系统值之一：中或高。
  - 如果所需的密码长度是 1 到 4 个符号，该应用程序会提示用户设置中强度密码。它必须是没有重复并且没有顺序（例如 1234）的数字（PIN），或者是字母数字。PIN 或密码必须至少有 4 个字符长。
  - 如果所需的密码长度是 5 个或更多符号，该应用程序会提示用户设置高强度密码。它必须是没有重复并且没有顺序的数字（PIN），或者是字母数字（密码）。PIN 必须至少为 8 位数字；密码必须至少有 6 个字符长。
- 使用指纹解锁屏幕只能在工作配置文件中管理。

配置安卓设备的限制

为确保安卓设备安全，请在设备上配置 Wi-Fi、摄像头和蓝牙的使用设置。

默认情况下，用户可以在设备上无限制地使用 Wi-Fi、摄像头和蓝牙。

若要在设备上配置 Wi-Fi、摄像头和蓝牙的使用限制，请执行以下步骤：

1. 在控制台树的“**受管设备**”文件夹中，选择 Android 设备所属的管理组。
2. 在所选组的工作区中，选择“**策略**”选项卡。
3. 通过双击任意列打开策略属性窗口。
4. 在策略“**属性**”窗口中选择“**设备管理**”区域。
5. 在“**限制**”区域中，配置 Wi-Fi、摄像头和蓝牙的使用：
   - 若要在用户移动设备上禁用 Wi-Fi 模块，则选择“**禁止使用 Wi-Fi**”选框。

     在运行 Android 10.0 或更高版本的设备上，不支持禁止使用 Wi-Fi 网络。

   - 若要在用户移动设备上禁用摄像头，则选择“**禁止使用摄像头**”选框。

     在运行 Android 10.0 或更高版本的设备上，不能完全禁止使用摄像头。

在运行 Android 11 或更高版本的设备上，必须将 Kaspersky Endpoint Security for Android 设置为无障碍功能。Kaspersky Endpoint Security for Android 会提示用户通过初始配置向导将该应用程序设置为可访问功能。用户可以跳过此步骤或以后在设备设置中禁用此服务。如果是这种情况，您将无法限制使用摄像头。

- 若要在用户移动设备上禁用蓝牙，则选择“**禁止使用蓝牙**”选框。

在 Android 12 或更高版本上，只有设备用户授予了“**附近的蓝牙设备**”权限后，才能禁用蓝牙。用户可以在初始配置向导期间或稍后授予此权限。

6. 单击“**应用**”按钮以保存所作的更改。

与 Kaspersky Security Center 的下次设备同步之后可配置移动设备设置。

配置 iOS MDM 设备功能限制

为确保符合公司安全要求，请配置 iOS MDM 设备运行限制。

若要配置 iOS MDM 设备功能限制，请执行以下操作：

1. 在控制台树的“**受管设备**”文件夹中，选择 iOS MDM 设备所属的管理组。
2. 在所选组的工作区中，选择“**策略**”选项卡。
3. 通过双击打开策略属性窗口。
4. 在策略“**属性**”窗口中选择“**功能限制**”区域。
5. 在“**功能限制设置**”区域中，选中“**将设置应用于设备**”选框。
6. 配置 iOS MDM 设备功能限制。
7. 单击“**应用**”按钮以保存所作的更改。
8. 选择**应用程序限制**区域。
9. 在“**应用程序限制设置**”区域中选择“**将设置应用于设备**”选框。
10. 在 iOS MDM 设备上配置应用程序限制。
11. 单击“**应用**”按钮以保存所作的更改。
12. 选择**对媒体内容的限制**区域。
13. 在“**媒体内容限制设置**”区域中选择“**将设置应用于设备**”选框。
14. 在 iOS MDM 设备上配置对媒体内容的限制。
15. 单击“**应用**”按钮以保存所作的更改。

这样，一旦应用该策略，将在用户的移动设备上配置对功能、应用程序和媒体内容的限制。

配置 EAS 设备功能限制

配置设备功能限制，保护 EAS 设备。

默认情况下，用户可以无限制地使用 EAS 设备的功能。

若要配置 EAS 设备功能限制，请执行以下操作：

1. 在控制台树的“**受管设备**”文件夹中，选择 EAS 设备所属的管理组。
2. 在所选组的工作区中，选择“**策略**”选项卡。
3. 通过双击打开策略属性窗口。
4. 在策略“属性”窗口中选择“**功能限制**”区域。
5. 在“**功能限制设置**”区域，启用或禁用 EAS 设备功能：
   - 若要允许将存储卡和其它可移动驱动器连接至本设备，请选中“**允许可移动磁盘**”选框。
   - 若要允许使用摄像头，请选择“**允许使用摄像头**”选框。
   - 若要允许 Wi-Fi 连接，请选择“**允许使用 Wi-Fi**”选框。
   - 若要允许使用红外线连接端口，请选择“**允许红外线连接**”选框。
   - 若要允许将设备用作创建无线网络的 Wi-Fi 接入点，请选择“**允许将设备用作 Wi-Fi 接入点**”选框。
   - 若要允许设备连接远程桌面，请选择“**允许远程桌面连接**”选框。
   - 若要允许用户在设备上使用 Desktop ActiveSync 客户端，请选择“**允许桌面同步**”选框。
   - 在“**使用蓝牙**”下拉列表中，在 EAS 设备上启用或禁用 Bluetooth：
     - **允许**。允许在移动设备上使用蓝牙。
     - **在使用免提时**。在移动设备连接有无线耳机时启用 Bluetooth。
     - **拒绝**。阻止在移动设备上使用蓝牙。
6. 单击“**应用**”按钮以保存所作的更改。

与 Kaspersky Security Center 的下次设备同步之后可配置移动设备设置。

配置用户对网站的访问

本节包含有关如何配置在安卓和 iOS 设备上访问网站的说明。

在安卓设备上配置网站访问

您可以使用 Web 保护来配置安卓设备用户对网站的访问。Web 保护支持按 Kaspersky Security Network 云服务中所定义类别过滤网站。过滤允许您限制用户对某些网站或某些类别网站的访问（例如“赌博、彩票、抽奖”或“互联网通信”类别中的网站）。Web 保护还保护用户在互联网上的个人数据。

Kaspersky Endpoint Security for Android 必须被设置为可访问功能。Kaspersky Endpoint Security for Android 会提示用户通过初始配置向导将该应用程序设置为可访问功能。用户可以跳过此步骤或以后在设备设置中禁用此服务。在这种情况下，Web 保护不会运行。

安卓设备上的 Web 保护仅在 Google Chrome 浏览器（包括自定义标签功能）、Huawei Browser 和 Samsung Internet Browser 中可用。如果工作配置文件被使用且 Web 保护仅为工作配置文件所启用，Samsung Internet Browser 中的 Web 保护不阻止移动设备上的网站。

默认已启用上网保护：阻止用户访问“**钓鱼**”和“**恶意软件**”类别中的网站。

若要配置设备用户访问网站的设置，请执行以下步骤：

1. 在控制台树的“**受管设备**”文件夹中，选择 Android 设备所属的管理组。
2. 在所选组的工作区中，选择“**策略**”选项卡。
3. 通过双击任意列打开策略属性窗口。
4. 在策略“**属性**”窗口中选择“**Web 保护**”。
5. 选中“**启用 Web 保护**”选框。
6. 要使用 Web 保护，您的设备用户必须阅读并接受关于以使用 Web 保护为目的的数据处理声明 (Web 保护声明)：
   a. 点击链接 **Web 保护声明**。
      这将打开**关于以使用 Web 保护为目的的数据处理声明**窗口。要接受 Web 保护声明，您必须阅读并接受隐私策略。
   b. 点击“隐私策略”链接。阅读并接受隐私策略。
      如果您不接受隐私策略，移动设备用户可以在初始化配置向导或应用中接受隐私策略（→ **关于** → **条款和条件** → **隐私策略**）。
   c. 选择 Web 保护声明接受模式：
      - **我已阅读并接受 Web 保护声明**
      - **请求从设备用户处接受 Web 保护声明**
      - **我不接受 Web 保护声明**

   如果您选择**我不接受 Web 保护声明**，Web 保护不阻止移动设备上的网站。移动设备用户无法在 Kaspersky Endpoint Security 中启用 Web 保护。
7. 如果您希望应用程序根据网站内容限制用户对网站的访问，请执行以下操作：
   a. 在**Web 保护**区域中，在下拉列表中选中**所选类别的网站被禁止**。
   b. 通过选择应用将阻止访问的网站类别旁边的复选框来创建阻止类别列表。

8. 如果您希望应用程序仅允许用户访问管理员指定的网站，请执行以下操作：

   a. 在**Web 保护**区域中，在下拉列表中选中**仅允许列出的网站**。

   b. 通过添加应用不会阻止访问的网站地址创建网站列表。Kaspersky Endpoint Security for Android 仅支持正规表达式。输入允许的网站的地址时，请使用以下模板：

   - `http:\/\/www\.example\.com.*` – 网站的所有子页面都被允许(例如，`http://www.example.com/about`)。
   - `https:\/\/.*example\.com` – 网站的所有子域页面都被允许(例如，`https://pictures.example.com`)。

   您也可以使用表达式 `https?` 来选择 HTTP 和 HTTPS 协议。对于更多正规表达式的详情，请参考 Oracle 技术支持网站。

9. 如果您希望应用程序阻止用户访问所有网站，请在“**Web 保护**”区域的下拉列表中选择“**阻止所有网站**”。

10. 若要去除根据内容对用户访问网站的限制，则清空“**启用 Web 保护**”选框。

11. 单击“**应用**”按钮以保存所作的更改。

与 Kaspersky Security Center 的下次设备同步之后可配置移动设备设置。

在 iOS MDM 设备上配置网站访问

配置 Web 保护设置以控制 iOS MDM 设备用户对网站的访问。Web 保护根据允许的网站和阻止的网站的列表，控制用户对网站的访问。通过上网保护，您还可以在 Safari 的书签面板上添加网站书签。

默认情况下，网站访问不受限制。

只能为受监控的设备配置 Web 保护设置。

若要在用户的 iOS MDM 设备上配置网站访问，请执行以下操作：

1. 在控制台树的“**受管设备**”文件夹中，选择 iOS MDM 设备所属的管理组。
2. 在所选组的工作区中，选择“**策略**”选项卡。
3. 通过双击打开策略属性窗口。
4. 在策略“**属性**”窗口中选择“**Web 保护**”区域。
5. 在“**Web 保护设置**”区域中，选中“**将设置应用于设备**”选框。
6. 若要阻止访问阻止的网站，允许访问允许的网站，请执行以下操作：

   a. 在“**Web 过滤器模式**”下拉列表中，选择“**限制成人内容**”模式。

   b. 在“**允许的网站**”区域，创建允许的网站列表。

网址应以“http://”或“https://”开头。Kaspersky Device Management for iOS 允许访问该域中的所有网站。例如，如果已将 http://www.example.com 添加到允许的网站列表中，则允许访问 http://pictures.example.com 和 http://example.com/movies。如果允许访问的网站列表为空，应用程序将允许访问除被拦截的网站列表中包含的网站以外的所有网站。

c. 在“**禁止的网站**”区域中，创建阻止的网站列表。

网址应以“http://”或“https://”开头。Kaspersky Device Management for iOS 阻止访问该域中的所有网站。

7. 若要阻止访问除该选项卡列表上的允许的网站以外的所有网站，请执行以下步骤：

a. 在“**Web 过滤器模式**”下拉列表中，选择“**仅允许加入书签的网站**”模式。

b. 在“**书签**”区域，创建允许的网站的书签列表。

网址应以“http://”或“https://”开头。Kaspersky Device Management for iOS 允许访问该域中的所有网站。如果书签列表为空，则应用程序允许访问所有网站。在用户的移动设备中，Kaspersky Device Management for iOS 在 Safari 的书签选项卡上添加书签列表中的网站。

8. 单击“**应用**”按钮以保存所作的更改。

这样，一旦应用该策略，将根据选择的模式和创建的列表在用户的移动设备上配置上网保护。

使用公司安全要求控制安卓设备的合规性

您可以控制安卓设备以符合公司的安全要求。公司安全要求规范用户可以如何使用设备。例如，必须在设备上启用实时保护，反病毒数据库必须是最新的，并且设备密码必须足够强。合规性控制基于规则列表。合规性规则包括以下组成部分：

- 设备检查条件（例如，设备上不存在被阻止的应用程序）。
- 分配给用户以解决不合规问题的时间段（例如，24 小时）。
- 如果用户未在规定的时间段内解决不合规问题，将对设备采取的措施（例如锁定设备）。

> 在 Android 12 或更高版本上，如果设备处于省电模式，应用程序可能会晚于指定的时间执行此任务。

如果用户不修复指定时间内的不兼容，则以下操作可用：

- **阻止除系统应用程序之外的所有应用程序**。阻止用户移动设备上的所有应用程序（系统应用程序除外）启动。
- **锁定设备**。移动设备将被锁定。要获取对数据的访问，您必须 解锁设备。如果设备解锁后，解锁设备的原因未更改，设备将在指定时间段后再次被锁定。
- **擦除企业数据**。擦除容器中的数据、公司电子邮件账户、用于连接至公司 Wi-Fi 网络和 VPN 的设置、接入点名称 (APN)、安卓工作配置文件、KNOX 容器和 KNOX License Manager 密钥。
- **恢复出厂设置**。所有数据都将从移动设备中删除，设置将回滚至其出厂值。该操作完成后，设备将不再是受管理设备。要连接设备到 Kaspersky Security Center，您比必须 重新安装 Kaspersky Endpoint Security for Android。

若要创建扫描规则，检查设备是否符合合规性，请执行以下操作：

1. 在控制台树的“**受管设备**”文件夹中，选择 Android 设备所属的管理组。
2. 在所选组的工作区中，选择“**策略**”选项卡。
3. 通过双击任意列打开策略属性窗口。
4. 在策略“**属性**”窗口中选择“**合规性控制**”区域。
5. 若要接收关于违反策略的设备的通知，则在“**不合规通知**”区域中选择“**通知管理员**”选框。

   如果设备的使用不符合策略，在与管理服务器同步期间，Kaspersky Endpoint Security for Android 将在事件日志中生成“**检测到违规: <检查的条件的名称>**”条目。可以在“管理服务器”属性的“**事件**”选项卡上或在应用程序的本地属性中查看事件日志。
6. 若要通知设备用户其设备不符合策略，则可以在“**不合规通知**”区域中选择“**通知用户**”选框。

   如果在设备与管理服务器同步期间发现设备违反策略，Kaspersky Endpoint Security for Android 将在“**状态**”区域中通知用户。
7. 在“**合规性规则**”区域中，编撰一个用于检查设备是否符合策略的规则列表。执行以下步骤：

   a. 单击“**添加**”。

   “扫描规则向导”将启动。

   b. 按照“扫描规则向导”的描述进行操作。

   向导完成时，“**合规性规则**”区域中将显示新规则。
8. 若要临时禁用创建的扫描规则，可使用选定的规则旁边的切换开关。
9. 单击“**应用**”按钮以保存所作的更改。

与 Kaspersky Security Center 的下次设备同步之后可配置移动设备设置。如果用户设备不符合规则，您在扫描规则中指定的限制将应用至该设备。

应用程序启动控制

本节提供有关如何在移动设备上配置应用程序的用户访问的说明。

安卓设备上的应用程序启动控制

若要确保用户的移动设备安全，您必须在设备上配置应用程序启动设置。

您可以在安装了被阻止的应用或所需应用未安装的设备上施加对用户活动的限制（例如，锁定设备）。您可以使用“合规性控制”组件施加限制。为此，在扫描规则设置中，您必须选择 **已安装被禁止的应用、已安装被禁止类别中的应用** 或 **并非已安装所有所需的应用程序** 标准。

必须将 Kaspersky Endpoint Security for Android 设置为无障碍功能才能确保“应用程序控制”正常运行。Kaspersky Endpoint Security for Android 会提示用户通过初始配置向导将该应用程序设置为可访问功能。用户可以跳过此步骤或以后在设备设置中禁用此服务。在这种情况下，应用程序控制不会运行。

若要在移动设备上配置应用程序启动设置，请执行以下操作：

1. 在控制台树的“**受管设备**”文件夹中，选择 Android 设备所属的管理组。
2. 在所选组的工作区中，选择“**策略**”选项卡。
3. 通过双击任意列打开策略属性窗口。
4. 在策略“**属性**”窗口中选择“**应用程序控制**”区域。
5. 在“**运行模式**”区域中，选择用户移动设备上的应用程序启动的模式：
   - 若要允许用户启动除类别和应用程序列表中指定为被阻止的应用程序外的所有应用程序，请选择“**被阻止的应用程序**”模式。
   - 若要允许用户只能启动类别和应用程序列表中指定为允许的应用程序、推荐的应用程序或所需的应用程序，请选择“**允许的应用程序**”模式。
6. 如果您要 Kaspersky Endpoint Security for Android 在禁止的应用上发送数据到事件日志而不阻止它们，选择**不阻止禁止的应用，仅写入事件日志**复选框。

   在用户移动设备与管理服务器同步期间，Kaspersky Endpoint Security for Android 将在事件日志中生成“**已安装被禁止的应用程序**”条目。可以在“管理服务器”属性的“**事件**”选项卡上或在应用程序的本地属性中查看事件日志。
7. 如果您希望 Kaspersky Endpoint Security for Android 阻止用户移动设备上的系统应用程序（例如日历、摄像头和设置）在“**允许的应用程序**”模式下启动，请选择“**阻止系统应用程序**”选框。

   > Kaspersky 专家建议不要阻止系统应用程序，因为这会导致设备操作故障。
8. 创建类别和应用程序列表以配置应用程序的启动。

   有关应用程序类别的详细信息，请参阅附录。

   有关属于每个类别的应用程序的列表，请访问 Kaspersky 网站。
9. 单击“**应用**”按钮以保存所作的更改。

与 Kaspersky Security Center 的下次设备同步之后可配置移动设备设置。

为应用程序配置 EAS 设备限制

为保护 EAS 设备安全，请配置应用程序活动限制（网页浏览器，未签名的应用程序）。

默认情况下，用户可以在 EAS 设备上无限制地使用应用程序。

若要配置 EAS 设备上的应用程序活动限制，请执行以下操作：

1. 在控制台树的“**受管设备**”文件夹中，选择 EAS 设备所属的管理组。
2. 在所选组的工作区中，选择“**策略**”选项卡。
3. 通过双击打开策略属性窗口。
4. 在策略“属性”窗口中选择“**应用程序限制**”区域。
5. 在“**应用程序限制设置**”区域中，配置应用程序活动限制：

- 若要允许用户使用网页浏览器，请选择“**允许使用浏览器**”选框。
- 若要允许用户创建个人电子邮件账户（POP3 或 IMAP4），请选择“**允许个人邮件**”选框。
- 若要允许用户启动未使用身份验证证书签名的应用程序，请选择“**允许未签名的应用程序**”选框。
- 若要允许用户安装未使用身份验证证书签名的应用程序，请选择“**允许未签名的安装包**”选框。

6. 单击“**应用**”按钮以保存所作的更改。

与 Kaspersky Security Center 的下次设备同步之后可配置移动设备设置。

安卓设备上的软件清单

您可以清点已连接到 Kaspersky Security Center 的安卓设备上的应用程序。Kaspersky Endpoint Security for Android 会接收有关移动设备上安装的所有应用程序的信息。在清点期间获取的信息显示在“**事件**”区域的设备属性中。您可以查看有关每个已安装的应用程序的详细信息，包括其版本和发布者。

启用软件清单：

1. 在控制台树的“**受管设备**”文件夹中，选择 Android 设备所属的管理组。
2. 在所选组的工作区中，选择“**策略**”选项卡。
3. 通过双击任意列打开策略属性窗口。
4. 在策略“**属性**”窗口中选择“**应用程序控制**”区域。
5. 在**软件清单**区域，选择**在已安装应用上发送数据**复选框。
6. 单击“**应用**”按钮以保存所作的更改。

与 Kaspersky Security Center 的下次设备同步之后可配置移动设备设置。Kaspersky Endpoint Security for Android 在每次应用被安装或从设备卸载时发送数据到事件日志。

在 Kaspersky Security Center 中配置安卓设备的显示

为了便于使用移动设备列表进行操作，您应该配置在 Kaspersky Security Center 显示设备的相应设置。默认情况下，移动设备列表显示在“**其他**” → “**移动设备管理**” → “**移动设备**”控制台树中。设备信息将自动更新。您也可以单击右上角的“**更新**”按钮，手动更新移动设备列表。

将设备连接到 Kaspersky Security Center 后，设备将被自动添加到移动设备列表中。移动设备列表可包含有关设备型号、操作系统、IP 地址和其他内容的详细信息。

您可以配置设备名称格式并选择设备状态。设备状态会告知您 Kaspersky Endpoint Security for Android 的组件在用户移动设备上的运行情况。

Kaspersky Endpoint Security for Android 组件可能因以下原因而无法运行：

- 用户在设备设置中禁用了组件。
- 用户未向应用程序授予组件运行所需的权限（例如，相应的反盗窃命令无权确定设备位置）。

若要显示设备状态，您必须在管理组属性中启用“**由应用程序确定**”条件（“**属性**”→“**设备状态**”→“**在以下情况下将设备状态设置为紧急**”以及“**在以下情况下将设备状态设置为警告**”）。在管理组属性中，您还可以选择形成移动设备状态的其他条件。

若要在 Kaspersky Security Center 中配置安卓设备的显示，请执行以下操作：

1. 在控制台树的“**受管设备**”文件夹中，选择 Android 设备所属的管理组。
2. 在所选组的工作区中，选择“**策略**”选项卡。
3. 通过双击任意列打开策略属性窗口。
4. 在策略“**属性**”窗口中选择“**设备信息**”区域。
5. 在“**Kaspersky Security Center 中的设备名称**”区域中，选择管理控制台中的设备名称的格式：
   - 设备型号 [电子邮件、设备 ID]
   - 设备型号 [电子邮件(如果有)或设备 ID]

   设备 ID 是 Kaspersky Endpoint Security for Android 根据从设备收到的数据生成的唯一 ID。对于运行 Android 10 或更高版本的移动设备，Kaspersky Endpoint Security for Android 使用 SSAID (Android ID) 或从设备收到的其他数据的校验码。对于 Android 的更早版本，该应用使用 IMEI。
6. 将“锁定”属性设置在锁定位置 （）。
7. 在“**Kaspersky Security Center 中的设备状态**”区域，如果某个 Kaspersky Endpoint Security for Android 组件未运行，则选择相应的设备状态：（**紧急**）、（**警告**）或（**正常**）。

   在移动设备列表中，设备状态将根据所选状态而更改。
8. 将“锁定”属性设置在锁定位置。
9. 单击“**应用**”按钮以保存所作的更改。

与 Kaspersky Security Center 的下次设备同步之后可配置移动设备设置。

管理

本节包含有关如何在 Kaspersky Security Center 管理控制台中远程管理移动设备设置的信息。

配置与 Wi-Fi 网络的连接

本节提供有关如何在安卓和 iOS MDM 设备上配置自动连接到公司 Wi-Fi 网络的说明。

将安卓设备连接至 Wi-Fi 网络

若要将移动设备连接至 Wi-Fi 网络，请执行以下操作：

1. 在控制台树的“**受管设备**”文件夹中，选择 Android 设备所属的管理组。
2. 在所选组的工作区中，选择“**策略**”选项卡。
3. 通过双击任意列打开策略属性窗口。
4. 在策略“**属性**”窗口中选择“**Wi-Fi**”区域。
5. 在“**Wi-Fi 网络**”区域中单击“**添加**”。

   这将打开“**Wi-Fi 网络**”窗口。
6. 在“**服务集标识符 (SSID)**”字段中，输入包含接入点 (SSID) 的 Wi-Fi 网络的名称。
7. 在“**网络保护**”区域中，选择 Wi-Fi 网络安全类型（受 WEP 或 WPA/WPA2 PSK 协议保护的公用网或安全网络）。
8. 如果您在上一步中选择了安全网络，则在“**密码**”字段中设置网络访问密码。
9. 如有必要，在“**代理服务器地址和端口**”字段中，输入代理服务器的 IP 地址或 DNS 名称（网址）和端口号。

   在运行 Android 版本 8.0 或更新版本的设备上，Wi-Fi 代理服务器设置无法由策略重定义。然而，您可以在移动设备上手动为 Wi-Fi 网路配置代理服务器设置。

   如果您正使用代理服务器连接到 Wi-Fi 网络，您可以使用策略配置网络连接设置。在运行 Android 8.0 或更新版本的设备上，您必须手动配置代理服务器设置。在运行 Android 8.0 或更新版本的设备上，您无法使用策略更改 Wi-Fi 网络连接设置，除了网络访问密码。

   如果您不使用代理服务器连接到 Wi-Fi 网络，则没有使用策略管理 Wi-Fi 网络连接的限制。
10. 在“**不使用代理服务器地址**”字段中，生成不使用代理服务器可访问的网址列表。

    例如，您可以输入地址 `example.com`。在这种情况下，对于地址 `pictures.example.com`、`example.com/movies` 等将不使用代理服务器。可以忽略协议（例如 `http://`）。

    在运行 Android 版本 8.0 或更高版本的设备上，网址的代理服务器排除不起作用。
11. 单击“**确定**”。

    “**Wi-Fi 网络**”列表中将显示添加的 Wi-Fi 网络。

    您可以使用网络列表顶部的“**编辑**”和“**删除**”按钮修改或删除该列表中的 Wi-Fi 网络。
12. 单击“**应用**”按钮以保存所作的更改。

与 Kaspersky Security Center 的下次设备同步之后可配置移动设备设置。在移动设备上应用该策略后，用户无需指定网络设置，即可连接到已添加的 Wi-Fi 网络。

在运行 Android 10.0 或更高版本的设备上，如果用户拒绝连接到建议的 Wi-Fi 网络，则该应用程序更改 Wi-Fi 状态的权限将被撤销。用户必须手动授予此权限。

将 iOS MDM 设备连接至 Wi-Fi 网络

用于使 iOS MDM 设备自动连接至可用的 Wi-Fi 网络，在连接期间保护数据，您应配置连接设置。

若要配置 iOS MDM 设备与 Wi-Fi 网络的连接，请执行以下操作：

1. 在控制台树的“**受管设备**”文件夹中，选择 iOS MDM 设备所属的管理组。
2. 在所选组的工作区中，选择“**策略**”选项卡。
3. 通过双击打开策略属性窗口。
4. 在策略“**属性**”窗口中选择“**Wi-Fi**”区域。
5. 在“**Wi-Fi 网络**”区域中单击“**添加**”按钮。

   这将打开“**Wi-Fi 网络**”窗口。
6. 在“**服务集标识符 (SSID)**”字段中，输入包含接入点 (SSID) 的 Wi-Fi 网络的名称。
7. 如果您希望 iOS MDM 设备自动连接至 Wi-Fi 网络，请选择“**自动连接**”选框。
8. 若要使 iOS MDM 设备无法连接到需要初步验证的 Wi-Fi 网络（受控网络），请选中“**禁用强制网络检测**”选框。

   若要使用受控网络，您必须订阅，接受协议或付款。例如，受控网络可能部署在咖啡馆和酒店。
9. 如果您希望在 iOS MDM 设备上的可用网络列表中隐藏 Wi-Fi 网络，请选择“**隐藏的网络**”选框。

   在这种情况下，若要连接到网络，用户需要手动输入在移动设备上的 Wi-Fi 路由器的设置中指定的服务集标识符 (SSID)。
10. 在“**网络保护**”下拉列表中选择 Wi-Fi 网络连接的保护类型：

    - **禁用**。无需进行用户认证。
    - **WEP**。使用无线加密协议 (WEP) 保护网络。
    - **WPA/WPA2 (个人)**。使用 WPA/WPA2 协议（Wi-Fi 安全访问）保护网络。
    - **WPA2 (个人)**。使用 WPA2 协议（Wi-Fi 安全访问 2.0）保护网络。运行 iOS 版本 8 或更高版本的设备提供了 WPA2 保护。Apple TV 设备不支持 WPA2。
    - **任何(个人)**。根据 Wi-Fi 路由器的类型，使用 WEP、WPA 或 WPA2 加密协议保护网络。使用对于每个用户唯一的加密密钥进行身份验证。
    - **WEP (动态)**。使用 WEP 协议和动态密钥保护网络。
    - **WPA/WPA2 (企业)**。使用 WPA/WPA2 加密协议与 802.1X 协议保护网络。
    - **WPA2 (企业)**。使用 WPA2 加密协议和所有用户共享的一个密钥 (802.1X) 保护网络。运行 iOS 版本 8 或更高版本的设备提供了 WPA2 保护。Apple TV 设备不支持 WPA2。
    - **任何(企业)**。根据 Wi-Fi 路由器类型使用 WEP 或 WPA/WPA2 协议保护网络。使用所有用户共享的一个加密密钥进行身份验证。

如果在“网络保护”列表中选择了“WEP（动态）”、“WPA/WPA2（企业）”、“WPA2（企业）”或“任何（企业）”，则在“协议”区域中可以为 Wi-Fi 网络上的用户识别选择 EAP 协议（可扩展身份验证协议）的类型。

在“可信证书”区域，您还可以创建可信证书列表，用于受信任的服务器上的 iOS MDM 设备用户身份验证。

11. 配置在 iOS MDM 设备连接至 Wi-Fi 网络时用于用户身份验证的帐户的设置：

    a. 在“身份验证”区域中，单击“配置”按钮。

    “身份验证”窗口将打开。

    b. 在“用户名”字段中，输入在连接至 Wi-Fi 网络时用于用户身份验证的帐户名。

    c. 若要允许用户在每次连接 Wi-Fi 网络时手动输入密码，请选择“每次连接时提示输入密码”选框。

    d. 在“密码”字段中，输入用于 Wi-Fi 网络上身份验证的帐户的密码。

    e. 在“身份验证证书”下拉列表中，选择用于 Wi-Fi 网络上的用户身份验证的证书。如果该列表未包含任何证书，您可以在“证书”区域进行添加。

    f. 在“用户 ID”字段中，输入在进行身份验证时的数据传输过程中显示的用户 ID，而不是真正的用户名。

    用户 ID 旨在使身份验证过程更加安全，因为用户名不会公开显示，而是通过加密的 TLS 隧道传输。

    g. 单击“确定”。

这样，将在 iOS MDM 设备上配置在连接至 Wi-Fi 网络时用于用户身份验证的帐户的设置。

12. 如有必要，配置通过代理服务器连接 Wi-Fi 网络的设置：

    a. 在“代理服务器”区域中，单击“配置”按钮。

    b. 在打开的“代理服务器”窗口中，选择代理服务器配置模式并指定连接设置。

    c. 单击“确定”。

这样，已在 iOS MDM 设备上配置设备通过代理服务器连接 Wi-Fi 网络的设置。

13. 单击“确定”。

新的 Wi-Fi 网络将显示在列表中。

14. 单击“应用”按钮以保存所作的更改。

这样，一旦应用该策略，将在用户的 iOS MDM 设备上配置 Wi-Fi 网络连接。用户的移动设备将自动连接至可用的 Wi-Fi 网络。身份验证技术可确保 Wi-Fi 网络连接期间数据的安全。

配置电子邮件

本节包含有关在移动设备上配置邮箱的信息。

在 iOS MDM 设备上配置邮箱

要允许 iOS MDM 设备用户使用电子邮件，请将该用户的电子邮件账号添加到 iOS MDM 设备上的账号列表中。

默认情况下，添加的电子邮件帐户具有以下设置：

- 电子邮件协议 – IMAP。
- 用户可以在用户的多个帐户之间移动电子邮件，并同步帐户地址。
- 用户可以通过任何电子邮件客户端（Mail 除外）使用电子邮件。
- 传输邮件时不使用 SSL 连接。

您可以在添加帐户时编辑指定的设置。

若要添加 iOS MDM 设备用户的电子邮件帐户，请执行以下步骤：

1. 在控制台树的“**受管设备**”文件夹中，选择 iOS MDM 设备所属的管理组。
2. 在所选组的工作区中，选择“**策略**”选项卡。
3. 通过双击打开策略属性窗口。
4. 在策略“**属性**”窗口中选择“**电子邮件**”。
5. 在“**电子邮件账户**”区域中单击“**添加**”按钮。
   “**电子邮件账户**”窗口将打开。
6. 在“**描述**”字段中，输入用户的电子邮件帐户的描述。
7. 选择电子邮件协议：
   - POP
   - IMAP
8. 如有必要，在“**IMAP 路径前缀**”字段中指定 IMAP 路径前缀。
   IMAP 路径前缀必须使用大写字母输入（例如：GMAIL 代表 Google Mail）。如果选择了 IMAP 帐户协议，则该字段可用。
9. 在“**邮件中显示的用户名**”字段中，输入要显示在所有待发邮件的“**发件人:**”字段中的用户名。
10. 在“**电子邮件地址**”字段中，指定 iOS MDM 设备用户的电子邮件地址。
11. 配置电子邮件帐户的其他设置：
    - 若要允许用户在用户的多个帐户之间移动电子邮件，请选择“**允许在账户之间移动邮件**”选框。
    - 若要允许在用户帐户之间同步地址，请选中“**允许同步最近地址**”选框。
    - 若要允许用户使用邮件投递服务转发大尺寸附件，请选中“**允许邮件递送**”选框。
    - 如果您希望用户仅使用标准的 iOS 邮件客户端，请选择“**仅允许使用邮件应用程序**”选框。
12. 配置在邮件应用程序中使用 S/MIME 协议的设置。*S/MIME* 是用于发送数字签名加密邮件的协议。
    - 要使用 S/MIME 协议对发送邮件进行签名，请选中“**签名消息**”复选框并选择用于签名的证书。数字签名确认发件人的真实性，并指示邮件的内容在发送给收件人的过程中未被修改。运行 iOS 版本 10.3 或更高版本

的设备支持邮件签名。

- 要使用 S/MIME 协议对发送邮件进行加密，请选中“**默认加密消息**”复选框并选择用于签名的证书（公钥）。运行 iOS 版本 10.3 或更高版本的设备支持邮件加密。
- 要使用户能够加密单个邮件，请选中“**显示用于加密消息的切换按钮**”复选框。要发送加密邮件，用户必须单击邮件应用程序的“**收件人**”字段中的 图标。

13. 在“**入站邮件服务器**”和“**出站邮件服务器**”区域，单击“**设置**”按钮以配置服务器连接设置：
    - **服务器地址和端口**：主机的名称或入站邮件服务器和出站邮件服务器的 IP 地址以及服务器端口号。
    - **账户名**：用于入站和出站邮件服务器身份验证的用户帐户的名称。
    - **身份验证类型**：入站邮件服务器和出站邮件服务器上用户电子邮件帐户身份验证的类型。
    - **密码**：用于使用选定的身份验证方法验证保护的入站和出站邮件服务器的帐户密码。
    - **对发送和接收邮件服务器使用一个密码**：对发送和接收邮件服务器使用一个密码进行用户身份验证。
    - **使用 SSL 连接**：使用 SSL（安全套接字层）数据传输协议，该协议使用加密和基于证书的身份验证保护数据传输。
14. 单击“**确定**”。
    新的电子邮件帐户显示在列表中。
15. 单击“**应用**”按钮以保存所作的更改。

这样，一旦应用该策略，编制的列表中的电子邮件帐户将添加到用户的移动设备上。

在 iOS MDM 设备上配置 Exchange 邮箱

若要使 iOS MDM 设备用户可以使用公司电子邮件、日历、联系人、记事本和任务，请将用户的 Exchange ActiveSync 帐户添加到 Microsoft Exchange 服务器上。

默认情况下，具有以下设置的帐户将添加到 Microsoft Exchange 服务器上：

- 每周同步一次电子邮件。
- 用户可以在用户的多个帐户之间移动邮件，并同步帐户地址。
- 用户可以通过任何电子邮件客户端（Mail 除外）使用电子邮件。
- 传输邮件时不使用 SSL 连接。

您可以在添加 Exchange ActiveSync 帐户时编辑指定的设置。

若要添加 iOS MDM 设备用户的 Exchange ActiveSync 帐户，请执行以下操作：

1. 在控制台树的“**受管设备**”文件夹中，选择 iOS MDM 设备所属的管理组。
2. 在所选组的工作区中，选择“**策略**”选项卡。
3. 通过双击打开策略属性窗口。

4. 在策略“**属性**”窗口中选择“**Exchange ActiveSync**”区域。

5. 在“**Exchange ActiveSync 账户**”区域中单击“**添加**”按钮。

   “**Exchange ActiveSync 账户**”窗口在“**常规**”选项卡上打开。

6. 在**账户名**字段中，输入要在 Microsoft Exchange 服务器上进行身份验证的帐户名。您可以使用“**可用宏**”下拉列表中的宏。

7. 在“**服务器地址**”字段中，输入 Microsoft Exchange 服务器的网络名称或 IP 地址。

8. 若要使用 SSL（安全套接字层）数据传输协议保护数据传输，请选择“**使用 SSL 连接**”选框。

9. 在“**域**”字段中，输入 iOS MDM 设备用户的域名。您可以使用“**可用宏**”下拉列表中的宏。

10. 在“**账户用户名**”字段中输入 iOS MDM 设备用户的名称。

    如果您将该字段留空，在 iOS MDM 设备上应用该策略时，Kaspersky Device Management for iOS 会提示用户输入用户名。您可以使用“**可用宏**”下拉列表中的宏。

11. 在“**电子邮件地址**”字段中，指定 iOS MDM 设备用户的电子邮件地址。您可以使用“**可用宏**”下拉列表中的宏。

12. 在“**密码**”字段中，输入用于在 Microsoft Exchange 服务器上进行身份验证的 Exchange ActiveSync 帐户的密码。

13. 选择“**其他**”选项卡并配置 Exchange ActiveSync 帐户的其他设置：

    - **邮件同步天数（指定时段内）**。
    - **身份验证类型**。
    - **允许在账户之间移动邮件**。
    - **允许同步最近地址**。
    - **仅允许使用邮件应用程序**。

14. 配置在邮件应用程序中使用 S/MIME 协议的设置。*S/MIME* 是用于发送数字签名加密邮件的协议。

    - 要使用 S/MIME 协议对发送邮件进行签名，请选中“**签名消息**”复选框并选择用于签名的证书。数字签名确认发件人的真实性，并指示邮件的内容在发送给收件人的过程中未被修改。运行 iOS 版本 10.3 或更高版本的设备支持邮件签名。
    - 要使用 S/MIME 协议对发送邮件进行加密，请选中“**默认加密消息**”复选框并选择用于签名的证书（公钥）。运行 iOS 版本 10.3 或更高版本的设备支持邮件加密。
    - 要使用户能够加密单个邮件，请选中“**显示用于加密消息的切换按钮**”复选框。要发送加密邮件，用户必须单击邮件应用程序的“**收件人**”字段中的 图标。

15. 单击“**确定**”。

    新的 Exchange ActiveSync 帐户显示在列表中。

16. 单击“**应用**”按钮以保存所作的更改。

这样，一旦应用该策略，编制的列表中的 Exchange ActiveSync 帐户将添加到用户的移动设备上。

在安卓设备上配置 Exchange 邮箱（仅限三星）

若要在移动设备上使用公司邮件、联系人和日历，应配置 Exchange 邮箱设置。

只能为三星设备配置 Exchange 邮箱。

若要在移动设备上配置 Exchange 邮箱，请执行以下操作：

1. 在控制台树的“**受管设备**”文件夹中，选择 Android 设备所属的管理组。
2. 在所选组的工作区中，选择“**策略**”选项卡。
3. 通过双击任意列打开策略属性窗口。
4. 在策略“**属性**”窗口中选择“**管理三星 KNOX**”→“**管理三星设备**”区域。
5. 在“**Exchange ActiveSync**”区域中，单击“**配置**”按钮。
   “**Exchange 邮件服务器设置**”窗口将打开。
6. 在“**服务器地址**”字段中，输入托管邮件服务器的服务器的 IP 地址或 DNS 名称。
7. 在“**域**”字段中，输入公司网络上的移动设备用户的域名。
8. 在“**同步间隔**”下拉列表中，选择移动设备与 Microsoft Exchange 服务器所需的同步时间间隔。
9. 若要使用 SSL（安全套接字层）数据传输协议，请选择“**使用 SSL 连接**”选框。
10. 若要使用数字证书保护移动设备与 Microsoft Exchange 服务器之间的数据传输，请选择“**验证服务器证书**”选框。
11. 单击“**应用**”按钮以保存所作的更改。

与 Kaspersky Security Center 的下次设备同步之后可配置移动设备设置。

管理第三方移动应用程序

您可以使用容器监控用户设备上启动的移动应用程序的活动。*容器* 是一个为移动应用程序准备的特殊的壳，可控制容器化应用程序的活动，以此保护设备上用户的个人和公司数据。

在 Kaspersky Security for Mobile Service Pack 3 Maintenance Release 2 中，不再支持为移动应用程序创建容器。但是，在早期版本的应用程序中创建的容器可以添加到 Android 设备。

您可以按照以下方式之一在用户设备上安装容器化应用程序：

- 向用户发送带有容器化应用程序安装包链接的邮件消息。
- 在策略属性窗口的“**应用程序控制**”区域中将容器化的应用程序指定为必需的或允许的应用程序。移动设备与 Kaspersky Security Center 同步之后，容器中的应用程序分发包将自动复制到用户设备中。

要安装集装式应用，用户的移动设备上必须允许安装来自未知来源的应用程序。要在安装集装式应用后保护您的设备和数据，建议禁止从未知源安装应用。关于不使用 Google Play 安装应用的详情，请参考 *Android 帮助向导*。

配置 Kaspersky Endpoint Security for Android 的通知

如果不希望 Kaspersky Endpoint Security for Android 通知分散移动设备用户的注意力，可以禁用某些通知。

Kaspersky Endpoint Security 使用以下工具显示设备保护状态：

- **保护状态通知**。该通知位于通知栏。保护状态通知无法被删除。通知显示设备保护状态（例如，）和可能的问题数量。有可以轻触设备保护状态并查看应用问题列表。
- **应用通知**。这些通知提示设备用户应用程序信息（例如，威胁检测）。
- **弹出消息**。弹出消息需要设备用户的操作（例如，当检测到威胁时要采取的操作）。

所有 Kaspersky Endpoint Security for Android 通知均为默认启用。

在 Android 13 中，设备用户应在初始配置向导期间或之后授予发送通知的权限。

Android 设备用户可以在通知栏的设置中禁用来自 Kaspersky Endpoint Security for Android 的所有通知。如果禁用通知，用户不会监控应用程序的运行，并且可能会忽略重要信息（例如，有关设备与 Kaspersky Security Center 同步期间发生的故障的信息）。在这种情况下，要了解应用程序运行状态，用户必须打开 Kaspersky Endpoint Security for Android。

要配置 Kaspersky Endpoint Security for Android 操作的通知显示，请执行以下操作：

1. 在控制台树的“**受管设备**”文件夹中，选择 Android 设备所属的管理组。
2. 在所选组的工作区中，选择“**策略**”选项卡。
3. 通过双击任意列打开策略属性窗口。
4. 在策略“**属性**”窗口中选择“**其他**”区域。
5. 在“**应用通知**”区域中，单击“**配置**”按钮。
   “**设备通知设置**”窗口将打开。
6. 选择要在用户移动设备上隐藏的 Kaspersky Endpoint Security for Android 问题，然后点击“**确定**”按钮。
   Kaspersky Endpoint Security for Android 在保护状态通知中和应用的**状态**区域中将不显示问题。Kaspersky Endpoint Security for Android 将继续显示保护状态通知和应用通知。

   某些 Kaspersky Endpoint Security for Android 问题是强制显示的，不可能禁用（例如，有关授权许可到期的问题）。
7. 要隐藏所有通知和弹出消息，选择**当应用处于后台时禁用通知和弹出消息**。
   Kaspersky Endpoint Security for Android 将仅显示保护状态通知。通知显示设备保护状态（例如，）和问题数量。用户使用应用时（例如，用户手动更新反病毒数据库），应用显示通知。

Kaspersky 专家建议您启用通知和弹出消息。如果当应用处于后台模式时您禁用通知和弹出消息，应用将不会警告用户实时威胁。移动设备用户仅在打开应用时才可以学习设备保护状态。

8. 单击“**应用**”按钮以保存所作的更改。

与 Kaspersky Security Center 的下次设备同步之后可配置移动设备设置。您禁用的 Kaspersky Endpoint Security for Android 通知将不会显示在用户的移动设备上。

将 iOS MDM 设备连接到 AirPlay

配置与 AirPlay 设备的连接，以便将音乐、照片和视频从 iOS MDM 设备流式传输到 AirPlay 设备。移动设备和 AirPlay 设备必须连接到相同的移动网络，才能使用 AirPlay 技术。AirPlay 设备包括（第二代和第三代）Apple TV 设备、AirPort Express 设备、扬声器或支持 AirPlay 的收音机。

仅受控制的设备可以自动连接至 AirPlay 设备。

若要配置 iOS MDM 设备与 AirPlay 设备的连接，请执行以下操作：

1. 在控制台树的“**受管设备**”文件夹中，选择 iOS MDM 设备所属的管理组。
2. 在所选组的工作区中，选择“**策略**”选项卡。
3. 通过双击打开策略属性窗口。
4. 在策略“**属性**”窗口中选择“**AirPlay**”区域。
5. 在“**AirPlay 设备**”区域中选择“**将设置应用于设备**”选框。
6. 在“**密码**”区域中单击“**添加**”按钮。
   在密码表格中添加一个空白的行。
7. 在“**设备名称**”列中，输入无线网络上的 AirPlay 设备的名称。
8. 在“**密码**”列中，输入 AirPlay 设备的密码。
9. 若要限制 iOS MDM 设备对 AirPlay 设备的访问，请在“**允许的设备**”区域创建允许的设备列表。为此，将 AirPlay 设备的 MAC 地址添加到允许的设备列表中。
   阻止访问不在允许的设备列表上的 AirPlay 设备。如果允许的设备列表留空，Kaspersky Device Management for iOS 将允许访问所有 AirPlay 设备。
10. 单击“**应用**”按钮以保存所作的更改。

这样，一旦应用该策略，用户的移动设备将自动连接至 AirPlay 设备，以流式传输媒体内容。

将 iOS MDM 设备连接到 AirPrint

若要能够使用 AirPrint 技术从 iOS MDM 设备无线打印文档，请配置自动连接至 AirPrint 打印机。移动设备和打印机必须连接到同一无线网络。必须在 AirPrint 打印机上配置所有用户的共享访问权限。

若要配置 iOS MDM 设备与 AirPrint 打印机的连接，请执行以下步骤：

1. 在控制台树的“**受管设备**”文件夹中，选择 iOS MDM 设备所属的管理组。
2. 在所选组的工作区中，选择“**策略**”选项卡。
3. 通过双击打开策略属性窗口。
4. 在策略“**属性**”窗口中选择“**AirPrint**”区域。
5. 在“**AirPrint 打印机**”区域中单击“**添加**”按钮。
   “**打印机**”窗口将打开。
6. 在“**IP 地址**”字段中，输入 AirPrint 打印机的 IP 地址。
7. 在“**资源路径**”字段中，输入 AirPrint 打印机的路径。
   打印机的路径与 Bonjour 协议 的 RP（资源路径）密钥相对应。例如：
   - printers/Canon_MG5300_series；
   - ipp/print；
   - Epson_IPP_Printer。
8. 单击“**确定**”。
   新添加的 AirPrint 打印机显示在列表上。
9. 单击“**应用**”按钮以保存所作的更改。

这样，一旦应用该策略，移动设备用户可以在 AirPrint 打印机上无线打印文档。

配置访问点名称 (APN)

若要将移动设备连接到移动网络上的数据传输服务，您应配置 APN（接入点名称）设置。

在安卓设备上配置 APN（仅限三星）

只能为三星设备配置 APN。

必须插入 SIM 卡才能在用户的移动设备上使用访问点。访问点设置由移动电话运营商提供。访问点设置有误可能产生额外的移动电话费用。

要配置访问点名称 (APN) 设置，请执行以下操作：

1. 在控制台树的“**受管设备**”文件夹中，选择 Android 设备所属的管理组。
2. 在所选组的工作区中，选择“**策略**”选项卡。

3. 通过双击任意列打开策略属性窗口。

4. 在策略“**属性**”窗口中选择“**管理三星 KNOX**”→“**APN**”区域。

5. 在“**APN**”区域中，单击“**配置**”按钮。
“**APN 设置**”窗口将打开。

6. 在“**常规**”选项卡上，指定以下访问点设置：

   a. 在“**APN 类型**”下拉列表中选择访问点的类型。

   b. 在“**APN 名称**”字段中，指定访问点的名称。

   c. 在“**MCC**”字段中，输入移动设备国家/地区代码 (MCC)。

   d. 在“**MNC**”字段中，输入移动设备网络代码 (MCC)。

   e. 如果您选择 **MMS** 或 **Internet 和 MMS** 作为访问点类型，请指定以下附加 MMS 设置：

   - 在“**MMS 服务器**”字段中，指定用于 MMS 交换的移动运营商服务器的完整域名。
   - 在“**MMS 代理服务器**”字段中，指定代理服务器的网络名称或 IP 地址和用于 MMS 交换的移动运营商服务器的端口号。

7. 在“**其他**”选项卡上，配置访问点 (APN) 的其他设置：

   a. 在“**身份验证类型**下拉列表中，选择用于网络访问的移动运营商服务器上的移动设备用户认证的类型。

   b. 在“**服务器地址**”字段中，指定通过其访问数据传输服务的移动运营商服务器的网络名称。

   c. 在“**代理服务器地址**”字段中，指定用于网络访问的移动运营商代理服务器的网络名称或 IP 地址和端口号。

   d. 在“**用户名**”字段中，输入移动网络上要进行身份验证的用户名。

   e. 在“**密码**”字段中，输入用于移动网络上的用户认证的密码。

8. 单击“**应用**”按钮以保存所作的更改。

与 Kaspersky Security Center 的下次设备同步之后可配置移动设备设置。

在 iOS MDM 设备上配置 APN

必须配置访问点名称 (APN)，以便在用户的 iOS MDM 设备上启用移动网络数据传输服务。

“**APN**”区域已弃用。建议在“**手机通信**”区域配置 APN 设置。配置手机通信设置之前，请确保未在设备上应用“**APN**”部分的设置（“**将设置应用于设备**”选框未选中）。“**APN**”和“**手机通信**”区域的设置不能同时使用。

若要在用户的 iOS MDM 设备上配置访问点，请执行以下操作：

1. 在控制台树的“**受管设备**”文件夹中，选择 iOS MDM 设备所属的管理组。

2. 在所选组的工作区中，选择“**策略**”选项卡。

3. 通过双击打开策略属性窗口。

4. 在策略“**属性**”窗口中选择“**手机通信**”区域。

5. 在“**手机通信设置**”区域中，选中“**将设置应用于设备**”选框。

6. 在 **APN 类型**列表中，选择 GPRS/3G/4G 移动网络上用于数据传输的接入点类型：

   - **内置 APN** – 通过支持使用内置 Apple SIM 卡操作的移动网络运营商配置用于数据传输的手机通信设置。有关具有内置 Apple SIM 卡的设备的详细信息，请访问 Apple 技术支持网站。
   - **APN** – 通过插入的 SIM 卡的移动网络运营商配置用于数据传输的手机通信设置。
   - **内置 APN 和 APN** – 通过插入的 SIM 卡和内置 Apple SIM 卡的移动网络运营商配置用于数据传输的手机通信设置。有关具有内置 Apple SIM 卡和 SIM 卡插槽的设备的详细信息，请访问 Apple 技术支持网站。

7. 在“**APN 名称**”字段中，指定访问点的名称。

8. 在“**身份验证类型**”下拉列表中，选择用于网络访问的移动运营商服务器上的设备用户身份验证类型（互联网和 MMS）：

9. 在“**用户名**”字段中，输入移动网络上要进行身份验证的用户名。

10. 在“**密码**”字段中，输入用于移动网络上的用户认证的密码。

11. 在“**代理服务器地址和端口**”字段中，输入主机的名称或代理服务器的 IP 地址和代理服务器端口号。

12. 单击“**应用**”按钮以保存所作的更改。

这样，在应用该策略后，在用户的移动设备上配置访问点名称 (APN)。

配置安卓工作配置文件

本节包含使用安卓工作配置文件的信息。

关于安卓工作配置文件

*安卓企业*是一个用于管理移动基础设施的平台。该平台可给公司员工提供一个可以使用移动设备的工作环境。要详细了解如何使用安卓企业，请参阅 Google 支持网站。

您可以在用户的移动设备上创建安卓工作配置文件（以下简称“工作配置文件”）。*安卓工作配置文件*是用户设备上的安全环境，在该环境中，管理员可以在不限制用户使用其自己的数据的情况下，管理应用程序和用户帐户。在用户的移动设备上创建了工作配置文件后，下列公司应用程序将自动安装到该工作配置文件中：Google Play Market、Google Chrome、Downloads、Kaspersky Endpoint Security for Android 等等。工作配置文件中安装的应用程序，以及这些应用程序的通知，都将被标上 图标。您必须为 Google Play Market 应用程序创建单独的 Google 公司账户。工作配置文件中安装的应用程序会显示在常用应用程序列表中。

配置工作配置文件

若要配置安卓工作配置文件的设置，请执行以下操作：

1. 在控制台树的“**受管设备**”文件夹中，选择 Android 设备所属的管理组。
2. 在所选组的工作区中，选择“**策略**”选项卡。
3. 通过双击任意列打开策略属性窗口。
4. 在策略“**属性**”窗口中选择“**安卓工作配置文件**”。
5. 在“**安卓工作配置文件**”工作区中，选择“**创建工作配置文件**”选框。
6. 指定工作配置文件设置：
   - 若要在安卓工作配置文件中启用 App Control 并在个人配置文件中禁用它，请选择“**仅在工作配置文件中启用应用程序控制**”选框。

     在“**用户**”区域中，您可以选择“应用程序控制”，并使用该区域的工作区创建允许、阻止、推荐和必需的应用程序列表，以及允许和阻止的应用程序类别。
   - 要在工作配置文件中启用 Google Chrome 的 Web 保护并在个人配置文件中禁用它，在**安卓工作配置文件**区域的工作区选择**仅在工作配置文件中启用 Web 保护**复选框。

     Samsung Internet Browser 的 Web 保护阻止工作和个人配置文件中的网站。您无法仅在工作配置文件中启用 Samsung Internet Browser 的 Web 保护。要在工作配置文件中启用 Samsung Internet Browser 的 Web 保护，禁用**仅在工作配置文件中启用 Web 保护**选项。如果启用该选项，Samsung Internet Browser 的 Web 保护不运行。工作配置文件中的 Web 保护默认被禁用。

     > 安卓设备上的 Web 保护仅在 Google Chrome 浏览器和 Samsung Internet Browser 中可用。

     您可以在“**Web 保护**”区域指定网站访问设置（创建阻止网站分类列表或允许网站列表）。
   - 若要防止用户通过剪贴板从工作配置文件向个人配置文件复制数据，请选择“**禁止从工作配置文件向个人配置文件传输数据**”选框。
   - 若要阻止用户在移动设备上的工作配置文件中使用 USB 调试模式，请选中“**禁止激活 USB 调试模式**”复选框。

     在 USB 调试模式中，用户可以通过使用工作站（举例说明）下载应用程序。
   - 若要禁止用户从除 Google Play 之外的所有源在安卓工作配置文件中安装应用程序，请选择“**禁止从未知源通过工作配置文件安装应用程序**”选框。
   - 若要禁止用户从安卓工作配置文件中卸载应用程序，请选择“**禁止从工作配置文件中删除应用程序**”选框。
7. 若要在用户的移动设备上配置工作配置文件，请阻止更改设置。
8. 单击“**应用**”按钮以保存所作的更改。

与 Kaspersky Security Center 的下次设备同步之后可配置移动设备设置。用户移动设备的空间分为工作配置文件和个人配置文件区。

添加 LDAP 帐户

若要使 iOS MDM 设备用户可以访问 LDAP 服务器上的企业联系人，请添加 LDAP 帐户。

若要添加 iOS MDM 设备用户的 LDAP 帐户，请执行以下操作：

1. 在控制台树的“**受管设备**”文件夹中，选择 iOS MDM 设备所属的管理组。
2. 在所选组的工作区中，选择“**策略**”选项卡。
3. 通过双击打开策略属性窗口。
4. 在策略“**属性**”窗口中选择“**LDAP**”区域。
5. 在“**LDAP 账户**”区域中单击“**添加**”按钮。
   “**LDAP 账户**”窗口将打开。
6. 在“**描述**”字段中，输入用户的 LDAP 帐户的描述。您可以使用“**可用宏**”下拉列表中的宏。
7. 在**账户名**字段中，输入要在 LDAP 服务器上进行身份验证的帐户名。您可以使用“**可用宏**”下拉列表中的宏。
8. 在“**密码**”字段中，输入用于在 LDAP 服务器上进行身份验证的 LDAP 帐户的密码。
9. 在“**服务器地址**”字段中输入 LDAP 服务器的域名。您可以使用“**可用宏**”下拉列表中的宏。
10. 若要使用 SSL（安全套接字层）数据传输协议保护邮件传输，请选择“**使用 SSL 连接**”选框。
11. 编制搜索查询列表，以便 iOS MDM 移动设备用户访问 LDAP 服务器上的企业数据：
    a. 在“**搜索设置**”区域中单击“**添加**”按钮。
       包含搜索查询的表格中会显示一个空白的行。
    b. 在“**名称**”列中输入搜索查询的名称。
    c. 在“**搜索范围**”列中，选择 LDAP 服务器上的企业数据搜索的文件夹嵌套级别：
       - **基本** – 在 LDAP 服务器的基本文件夹中搜索。
       - **一级** – 在从基本文件夹算起的第一个嵌套级别上的文件夹中搜索。
       - **子树** – 在从基本文件夹算起的所有嵌套级别上的文件夹中搜索。
    d. 在“**搜索库**”列中，输入 LDAP 服务器上首先搜索的文件夹的路径（例如：“ou=people”，“o=example corp”）。
    e. 对您要添加到 iOS MDM 设备的所有搜索查询重复步骤 a-d。
12. 单击“**确定**”。
    新的 LDAP 帐户显示在列表中。
13. 单击“**应用**”按钮以保存所作的更改。

这样，一旦应用该策略，编制的列表中的 LDAP 帐户将添加到用户的移动设备上。用户可以访问标准 iOS 应用程序中的企业联系人：联系人、消息和邮件。

添加日历帐户

若要使 iOS MDM 设备用户可以访问 CalDAV 服务器上的用户日历事件，请添加 CalDAV 帐户。与 CalDAV 服务器同步，以便用户创建和接收邀请、接收事件更新，以及与 Reminders 应用程序同步任务。

若要添加 iOS MDM 设备用户的 CalDAV 帐户，请执行以下操作：

1. 在控制台树的“**受管设备**”文件夹中，选择 iOS MDM 设备所属的管理组。
2. 在所选组的工作区中，选择“**策略**”选项卡。
3. 通过双击打开策略属性窗口。
4. 在策略“**属性**”窗口中选择“**日历**”区域。
5. 在“**CalDAV 账户**”区域中单击“**添加**”按钮。
   “**CalDAV 账户**”窗口将打开。
6. 在“**描述**”字段中，输入用户的 CalDAV 账户的描述。
7. 在“**服务器地址和端口**”字段中，输入主机的名称或 CalDAV 服务器的 IP 地址和 CalDAV 服务器端口号。
8. 在“**主地址**”字段中，指定 CalDAV 服务器上的 iOS MDM 设备用户的 CalDAV 帐户的网址（例如：http://example.com/caldav/users/mycompany/user）。
   网址应以“`http://`”或“`https://`”开头。
9. 在**账户名**字段中，输入用于在 CalDAV 服务器上进行身份验证的帐户名。
10. 在“**密码**”字段中，设置用于在 CalDAV 服务器上进行身份验证的 CalDAV 帐户密码。
11. 若要使用 SSL（安全套接字层）数据传输协议保护 CalDAV 服务器与移动设备之间的事件传输，请选择“**使用 SSL 连接**”选框。
12. 单击“**确定**”。
    新的 CalDAV 帐户显示在列表中。
13. 单击“**应用**”按钮以保存所作的更改。

这样，一旦应用该策略，编制的列表中的 CalDAV 帐户将添加到用户的移动设备上。

添加联系人帐户

若要使 iOS MDM 设备用户可以与 CardDAV 服务器同步数据，请添加 CardDAV 帐户。与 CardDAV 服务器同步，以便用户从任何设备访问联系人详细信息。

若要添加 iOS MDM 设备用户的 CardDAV 帐户，请执行以下操作：

1. 在控制台树的“**受管设备**”文件夹中，选择 iOS MDM 设备所属的管理组。
2. 在所选组的工作区中，选择“**策略**”选项卡。
3. 通过双击打开策略属性窗口。
4. 在策略“**属性**”窗口中选择“**联系人**”区域。
5. 在“**CardDAV 账户**”区域中单击“**添加**”按钮。
   “**CardDAV 账户**”窗口将打开。

6. 在“**描述**”字段中，输入用户的 CardDAV 帐户的描述。您可以使用“**可用宏**”下拉列表中的宏。

7. 在“**服务器地址和端口**”字段中，输入主机的名称或 CardDAV 服务器的 IP 地址和 CardDAV 服务器端口号。

8. 在“**主地址**”字段中，指定 CardDAV 服务器上的 iOS MDM 设备用户的 CardDAV 帐户的网址（例如：http://example.com/carddav/users/mycompany/user）。

   网址应以“`http://`”或“`https://`”开头。

9. 在“**账户名**”字段中，输入用于在 CardDAV 服务器上进行身份验证的帐户名。您可以使用“**可用宏**”下拉列表中的宏。

10. 在“**密码**”字段中，设置用于在 CardDAV 服务器上进行身份验证的 CardDAV 帐户密码。

11. 若要使用 SSL（安全套接字层）数据传输协议保护 CardDAV 服务器与移动设备之间的联系人传输，请选择“**使用 SSL 连接**”选框。

12. 单击“**确定**”。

    新的 CardDAV 帐户显示在列表中。

13. 单击“**应用**”按钮以保存所作的更改。

这样，一旦应用该策略，编制的列表中的 CardDAV 帐户将添加到用户的移动设备上。

配置日历订阅

若要使 iOS MDM 设备用户可以向用户的日历添加共享日历（例如企业日历）的事件，请添加该日历的订阅。*共享日历*是其他具有 CalDAV 帐户的用户的日历、iCal 日历以及其他公开发布的日历。

若要添加日历订阅，请执行以下步骤：

1. 在控制台树的“**受管设备**”文件夹中，选择 iOS MDM 设备所属的管理组。

2. 在所选组的工作区中，选择“**策略**”选项卡。

3. 通过双击打开策略属性窗口。

4. 在策略“**属性**”窗口中选择“**日历订阅**”区域。

5. 在“**日历订阅**”区域中单击“**添加**”按钮。

   将打开“**日历订阅**”窗口。

6. 在“**描述**”字段中，输入日历订阅的描述。

7. 在“**服务器网址**”字段中，指定第三方日历的 URL。

   在该字段中，您可以输入您正在订阅其日历的用户的 CalDAV 帐户的邮件网址。您还可以指定 iCal 日历或其他公开发布的日历的网址。

8. 在“**用户名**”字段中，输入用于在第三方日历服务器上进行身份验证的用户账户的名称。

9. 在“**密码**”字段中，输入用于在第三方日历服务器上进行身份验证的日历订阅密码。

10. 若要使用 SSL（安全套接字层）数据传输协议保护 CalDAV 服务器与移动设备之间的事件传输，请选择“**使用 SSL 连接**”选框。

11. 单击“**确定**”。

12. 新的日历订阅显示在列表中。

13. 单击“**应用**”按钮以保存所作的更改。

这样，一旦应用该策略，列表中共享日历的事件将添加到用户的移动设备上的日历中。

添加网络收藏夹

*网络收藏夹*是一个可从移动设备的主屏幕打开网站的应用程序。通过单击设备主屏幕上的网络收藏夹图标，用户可以快速打开网站（例如公司网站）。您可以向用户设备添加网络收藏夹，配置屏幕上显示的网络收藏夹图标的外观。

默认情况下，应用以下网络收藏夹使用限制：

- 用户不能手动从移动设备删除网络收藏夹。
- 用户单击网络收藏夹时打开的网站不会以全屏模式打开。
- 对屏幕上的网络收藏夹图标应用圆角、阴影和光泽视觉效果。

若要在用户的 iOS MDM 设备上添加网络收藏夹，请执行以下操作：

1. 在控制台树的“**受管设备**”文件夹中，选择 iOS MDM 设备所属的管理组。
2. 在所选组的工作区中，选择“**策略**”选项卡。
3. 通过双击打开策略属性窗口。
4. 在策略“**属性**”窗口中选择“**Web Clips**”区域。
5. 在“**Web Clip**”区域中单击“**添加**”按钮。
   “**Web Clip**”窗口将打开。
6. 在“**名称**”字段中，输入要显示在 iOS MDM 设备主屏幕上的网络收藏夹的名称。
7. 在“**网址**”字段中，输入单击网络收藏夹图标时将打开的网站的网址。该网址应以“`http://`”或“`https://`”开头。
8. 若要允许用户从 iOS MDM 设备删除网络收藏夹，请选择“**允许删除**”选框。
9. 单击“**选择**”按钮，指定包含网络收藏夹图标图片的文件。
   该图标显示在 iOS MDM 设备的主屏幕上。该图片必须满足以下要求：
   - 图片的尺寸不超过 400 x 400 像素。
   - 文件格式：GIF、JPEG 或 PNG。
   - 文件大小不超过 1 MB。

   可在“**图标**”字段中预览网络收藏夹图标。如果您没有选择 Web Clip 图片，显示的图标是一个空白方形。

如果您希望显示的网络收藏夹图标不带特殊的视觉效果（图标圆角和光泽效果），请选中**预制作的图标**选框。

10. 如果您希望在单击该图标时网站在 iOS MDM 设备上以全屏模式打开，请选择“**全屏 Web Clip**”选框。

11. 单击“**确定**”。
    新的网络收藏夹显示在列表中。

12. 单击“**应用**”按钮以保存所作的更改。

这样，一旦应用该策略，您创建的列表中的网络收藏夹图标将添加到用户的移动设备的主屏幕上。

添加字体

若要在用户的 iOS MDM 设备上添加字体，请执行以下步骤：

1. 在控制台树的“**受管设备**”文件夹中，选择 iOS MDM 设备所属的管理组。

2. 在所选组的工作区中，选择“**策略**”选项卡。

3. 通过双击打开策略属性窗口。

4. 在策略“**属性**”窗口中选择“**字体**”区域。

5. 在“**字体**”区域中单击“**添加**”按钮。
    “**字体**”窗口将打开。

6. 在“**文件名**”字段中，指定字体文件（扩展名为 .ttf 或 .otf 的文件）的路径。

    不支持扩展名为 ttc 或 otc 的字体。

    字体使用 PostScript 名称标识。请勿安装具有相同的 PostScript 名称的字体，即使它们的内容不同。安装具有相同的 PostScript 名称的字体将导致出现未定义的错误。

7. 单击“**打开**”。
    新的字体显示在列表中。

8. 单击“**应用**”按钮以保存所作的更改。

这样，一旦应用该策略，将提示用户安装已创建的列表中的字体。

使用第三方 EMM 系统管理应用程序（仅限 Android）

您可以在不安装 Kaspersky 管理系统的情况下使用 Kaspersky Endpoint Security for Android 应用。使用其他 EMM（企业移动管理）服务提供商的解决方案部署和管理 Kaspersky Endpoint Security for Android 应用。Kaspersky 加入 AppConfig Community 以确保应用程序可与第三方 EMM 解决方案一起运行。

您只能在运行 Android 的设备上通过第三方 EMM 解决方案管理 Kaspersky Endpoint Security for Android 应用程序。

您只能使用第三方 EMM 解决方案部署 Kaspersky Endpoint Security for Android 应用。将设备连接到 Kaspersky Security Center，然后在管理控制台中管理应用。在这种情况下，将无法在 EMM 控制台中管理 Kaspersky Endpoint Security for Android 应用。

如果您使用第三方 EMM 系统部署了 Kaspersky Endpoint Security for Android 应用，则无法在 Kaspersky Endpoint Security Cloud 中管理该应用。您可以在 EMM 控制台中管理 Kaspersky Endpoint Security for Android 应用。

以下 EMM 解决方案支持使用 Kaspersky Endpoint Security for Android 应用。

- VMware AirWatch
- MobileIron
- IBM Maas360
- Microsoft Intune
- SOTI MobiControl

您可以在 EMM 控制台中执行以下操作：

- 将应用程序部署到用户设备上的安卓工作配置文件。
- 激活应用程序。
- 配置应用程序设置：
  - 启用对互联网上恶意和钓鱼网站的防御。
  - 配置连接设备到 Kaspersky Security Center 的设置。
  - 配置反病毒设置。
  - 配置对设备运行病毒扫描计划。
  - 启用检测可被犯罪分子入侵以损坏用户的设备或个人数据的广告软件和应用程序。
  - 配置应用程序数据库更新计划。

开始使用

要在用户的移动设备上部署该应用程序，您必须将 Kaspersky Endpoint Security for Android 添加到 EMM 应用商店。您可以通过使用 Google Play 链接将 Kaspersky Endpoint Security for Android 添加到 EMM 应用商店。有关与 EMM 控制台中的应用程序一起使用的更多详细信息，请访问 *EMM 服务提供商的技术支持网站*。

Kaspersky Endpoint Security for Android 应用程序在安卓工作配置文件中部署。该应用程序与用户的个人数据隔离，并只保护工作配置文件中的企业数据。建议确保保护 Kaspersky Endpoint Security for Android 免遭 EMM 控制台工具卸载。

如何安装应用程序

根据 EMM 控制台，选择将应用程序安装到设备上的方法：静默安装、将包含链接的电子邮件发送至 Google Play 中的应用程序或其他可用方法。

要使应用正常工作，需要以下权限：

- 用于在反病毒运行时访问文件的存储权限（仅针对 Android 6.0 或更高版本）。
- 用于标识设备（例如，当激活应用时）的电话权限。
- 请求将 Kaspersky Endpoint Security for Android 添加到在操作系统启动时启动的应用程序列表（在某些设备上，如华为、魅族和小米）。如果未显示添加请求，将 Kaspersky Endpoint Security for Android 手动添加到启动应用程序列表。如果工作配置文件中未安装 Security 应用程序，该请求可能不会显示。

您可以在部署 Kaspersky Endpoint Security for Android 应用前，在 EMM 控制台中授予所需权限。有关在 EMM 控制台中授予权限的更多详细信息，请访问 *EMM 服务提供商的技术支持网站*。您也可以在设备上完成 Kaspersky Endpoint Security for Android 的初始配置向导时授予权限。

Kaspersky Endpoint Security for Android 应用程序将安装在安卓工作配置文件中。

要使 Web 保护运行，您还必须在 Google Chrome 设置中配置代理服务器：

- 代理服务器配置模式：手动。
- 代理服务器地址和端口：127.0.0.1:3128。
- SPDY 协议支持：禁用。
- 通过代理服务器压缩数据：禁用。

如何激活应用程序

有关授权许可的信息与配置文件中的其他设置一起传输至移动设备。

如果应用程序在移动设备上安装后 30 天内未激活，试用授权许可将过期。试用版授权许可过期后，Kaspersky Endpoint Security for Android 移动应用程序的所有功能都将被禁用。

商业授权许可过期后，该移动应用程序将在受限功能模式下继续运行（例如 Kaspersky Endpoint Security for Android 的数据库更新将不可用）。若要继续在全功能模式下使用该应用程序，必须对商业授权许可进行续费。

若要激活 Kaspersky Endpoint Security for Android，请执行以下操作：

1. 在 EMM 控制台中，打开 Kaspersky Endpoint Security for Android 应用程序的设置。
2. 在 `LicenseActivationCode` 字段中，输入应用程序激活码。

   要在设备上激活应用程序，您必须具有访问 Kaspersky 激活服务器的权限。

如何连接设备到 Kaspersky Security Center

在 Kaspersky Endpoint Security for Android 被安装到移动设备上后，您可以连接该设备到 Kaspersky Security Center。连接设备到 Kaspersky Security Center 的必要数据与配置文件中列出的其他设置一起被传输到移动设备。连接设备到 Kaspersky Security Center 后，您可以使用组策略集中配置应用设置。您可以接收 Kaspersky Endpoint Security for Android 性能的报告和统计信息。

在连接设备到 Kaspersky Security Center 之前，确保以下条件被满足：

- Kaspersky Endpoint Security for Android 管理插件已安装到管理员工作站。
- 连接移动设备的端口在管理服务器属性中被打开。
- **移动设备管理**文件夹的显示已在管理控制台中启用。
- 用于识别移动设备用户的常规证书已在 Kaspersky Security Center 证书中被创建。

连接设备到 Kaspersky Security Center 之前，建议做以下：

- 如果要为移动设备创建任务和策略，请为移动设备创建单独的管理组。
- 如果要自动将移动设备移动到单独的管理组，请创建从**未分配的设备**文件夹自动移动设备的规则。
- 如果要集中配置 Kaspersky Endpoint Security for Android，请创建组策略。

要连接设备到 Kaspersky Security Center：

1. 在 EMM 控制台中，打开 Kaspersky Endpoint Security for Android 应用程序的设置。
2. 在“`KscServer`”字段中，输入 Kaspersky Security Center 管理服务器的 DNS 名称或 IP 地址。默认端口是 13292。
3. 如果不希望 Kaspersky Endpoint Security for Android 通知分散用户的注意力，请禁用应用通知。为此，设置 `DisableNotification = True`。
   连接之后，应用显示所有通知。您可以在策略设置中禁用特定应用通知。

   如果您不使用 Kaspersky Security Center 则不禁用应用通知。这可以导致用户不接收授权许可过期通知。结果，应用将停止执行其功能。

在配置连接设置后，Kaspersky Endpoint Security for Android 显示通知提示您授予以下附加权限和许可：

- 使用摄像头进行反盗窃操作的权限（“**面部照片**”命令）。
- 使用定位进行反盗窃操作的权限（“**定位设备**”命令）。
- 设备管理员权限（Android work 配置文件所有者）以操作以下应用功能：
  - 安装安全证书。
  - 配置 Wi-Fi。
  - 配置 Exchange ActiveSync。

- 限制使用摄像头、蓝牙和 Wi-Fi。

> 由于 Android work 配置文件的特别属性（没有 Accessibility 服务），应用控制和反盗窃功能在应用上不可用。

当用户授予必要权限和许可时，设备将被连接到 Kaspersky Security Center。如果自动将设备移动到管理组的规则尚未创建，设备将自动添加到"**未分配的设备**"文件夹。如果自动将设备移动到管理组的规则已创建，设备将自动添加到已定义的组。

Kaspersky Endpoint Security 提供以下设备名称格式：

- 设备型号 [电子邮件、设备 ID]
- 设备型号 [电子邮件(如果有)或设备 ID]

设备 ID 是 Kaspersky Endpoint Security for Android 根据从设备收到的数据生成的唯一 ID。对于运行 Android 10 或更高版本的移动设备，Kaspersky Endpoint Security for Android 使用 SSAID (Android ID) 或从设备收到的其他数据的校验码。对于 Android 的更早版本，该应用使用 IMEI。您可以在组策略中配置设备名称格式。

在 SOTI MobiControl 中，可以在 `KscDeviceName` 字段中使用 %DEVICENAME% 宏。通过该宏可以自动从 SOTI MobiControl 控制台获取设备名称到 Kaspersky Security Center。

还可以添加标签到设备名称。这样可以更加便于在 Kaspersky Security Center 中查找和排序设备。该标签仅对 VMware AirWatch 可用。

要添加标签到设备名称：

1. 在 EMM 控制台中，打开 Kaspersky Endpoint Security for Android 应用程序的设置。
2. 在"`KscDeviceNameTag`"字段中，选择以下各值：
   - `{DeviceSerialNumber}` – 设备的序列号。
   - `{DeviceUid}` – 唯一的设备标识符 (UDID)。
   - `{DeviceAssetNumber}` – 设备资产编号。此编号由您的公司内部创建。

> 我们推荐仅使用这些值。VMware AirWatch 支持其他值，但 Kaspersky Endpoint Security 不能保证这些值能正常工作。

您可以添加某些值（例如，`{DeviceSerialNumber} {DeviceUid}`）。标签将在 Kaspersky Security Center 中被添加到设备名称。使用空格分隔标签和设备名称。例如，如果设备名称为 `Google Pixel 2 a10c6b75f7b31de9 22:7D:78:9E:C5:1E`，则 `22:7D:78:9E:C5:1E` 为 UDID 标签。如果使用 Kaspersky Security Center 和 VMwareAirWatch，则标签使您可以同时在这两种控制台中识别设备。为了匹配设备，请为设备名称选择相同的值（例如，设备的序列号）。

在设备连接到 Kaspersky Security Center 之后，应用设置将根据组策略被更改。Kaspersky Endpoint Security for Android 忽略在 EMM 控制台中配置的配置文件中的应用设置。您可以配置策略的所有区域，除了以下区域：

- **反盗窃**（设备锁）
- **容器**

- 设备管理（屏幕锁）
- 应用程序控制（阻止已禁止的应用）
- 安卓工作配置文件
- 管理三星 KNOX

由于部署工作配置文件所使用的方法，您无法从“安卓工作配置文件”区域应用组策略设置。这些设置仅在 work 配置文件是使用 Kaspersky Security Center 创建时可以被应用。

AppConfig 文件

系统将生成一个配置文件，用于在 EMM 控制台中配置该应用程序。下表显示了配置文件中的应用程序设置。

配置文件设置

配置键	描述	类型	值
`LicenseActivationCode`	应用程序激活码	String	由 20 个拉丁字母和数字组成的应用程序激用激活码激活应用程序，需通过互联网连Kaspersky 激活服务器。 如果您将此字段留空，将使用试用版授权程序。试用版授权许可的有效期为 30 天。许可过期后，Kaspersky Endpoint Security移动应用程序的所有功能都将被禁用。若应用程序，您必须购买商业授权许可。
`EulaAcceptanceConfirmationV1`	<授权许可协议链接>	Choice	该设置仅对 VMware AirWatch 可用. `Accepted` – 我确认我已完整阅读、理解并用户授权许可协议的条款和条件。 `Declined` – 我不接受该最终用户授权许可的条款和条件。 要为所有移动设备接受 EULA 的条款和条联网访问权限以连接到 Kaspersky 服务器。 如果您选择`Declined`，应用程序将提示用的条款和条件。移动设备用户可以在初始接受条件。
`EulaAcceptanceCodeV1`	授权许可协议代码	String	这些设置仅适用于 VMware AirWatch。 如果要接受单个最终用户授权许可协议 (E`EulaAcceptanceCodeV1`。如果要同时接EULA，请使用 `EulaAcceptanceCodesV2``EulaAcceptanceCodesV2` 字段必须包含EULA 代码列表：`"<EULAid1>;<EULAid2<EULAid3>;..."`。
`EulaAcceptanceCodesV2`	授权许可协议代码	String	

			授权许可协议代码被包含在最终用户授权 *要了解授权许可协议代码：* 1. 从 EMM 控制台复制授权许可协议链接 (`EulaAcceptanceConfirmationV1`)。 2. 将链接粘贴到浏览器。 最终用户授权许可协议 (EULA) 打开。 3. 阅读该 EULA 的条款和条件并查找授权码。 要为所有移动设备接受 EULA 的条款和互联网访问权限以连接到 Kaspersky 服 如果将字段留空，应用将提示用户接受 EU条件。移动设备用户可以在初始化配置向件。 如果指定这两个字段的值，它们中指定的条款和条件都将被接受。
`KscServer`	Kaspersky Security Center 管理服务器地址和端口	String	Kaspersky Security Center 管理服务器的地址和端口号。按照以下格式输入地址：>:<端口>。如果您输入了服务器地址而不用将使用默认端口 13292。
`DisableNotification`	在连接到 Kaspersky Security Center 之前禁用应用通知	Boolean	`True` – Kaspersky Endpoint Security for A有应用程序通知。Kaspersky Endpoint Sec Android 隐藏通知直到设备连接到 Kaspers Center。连接之后，应用显示所有通知。设置中禁用特定应用通知。 如果您不使用 Kaspersky Security Cente应用通知。这可以导致用户接收不到授通知。如果出现这种情况，应用将停止能。 `False` – Kaspersky Endpoint Security for 所有应用通知。
`ScanScheduleType`	扫描运行模式	Choice	`AfterUpdate` – 在数据库更新后启动病毒序将按照定义的计划更新反病毒数据库 (`UpdateScheduleType`)。 `Daily` – 每日启动一次病毒扫描。配置扫 (`ScanScheduleTime`)。 `Weekly` – 每周启动一次病毒扫描。选择一毒扫描的一天 (`ScanScheduleDay`) 并配置 (`ScanScheduleTime`)。 `Off` – 禁用病毒扫描的自动启动。 无论设置哪个值，设备用户均可手动启动
`ScanScheduleDay`	扫描日期	Choice	`Monday / Tuesday / Wednesday / Th Friday / Saturday / Sunday` 您只能为此设置选择一个值。

ScanScheduleTime	扫描时间	String	时间可以采用 24 小时格式（例如，13:00）式（例如，10:30 P.M.）指示。
ScanScheduleLock	阻止配置扫描运行模式	Boolean	True – 用户无法访问应用程序设置内的病式设置。 False – 用户可以配置病毒扫描运行模式病毒扫描自动启动。
ScanOnlyExecutableFiles	要扫描的文件类型（病毒扫描）	Choice	AllFiles – 扫描所有文件。 OnlyExecutables – 仅扫描可执行文件。带有 apk (.zip)、.dex 等扩展名的文件。 在 Kaspersky Endpoint Security for Andro Pack 4 Maintenance Release 1 中，您无法文件扫描。
ScanArchives	扫描压缩文件并解压缩	Boolean	True – 应用程序会解压缩压缩文件并扫描 False – 应用程序仅扫描压缩文件。 应用仅扫描带有 .zip (.apk) 扩展名的存档。 在 Kaspersky Endpoint Security for Andro Pack 4 Maintenance Release 1 中，您无法内容扫描。
ScanActionOnThreatFound	检测到威胁后的操作（病毒扫描）	Choice	Quarantine – 应用程序会将检测到的对区。应用程序会将存档形式隔离文件，不伤害。隔离区允许您删除或恢复移动至隔 Delete – 删除检测到的对象。 Skip – 应用程序会将检测到的对象保留不到的对象被跳过，Kaspersky Endpoint Se Android 会警告用户设备保护方面存在问题问设备上的某个对象（如，尝试复制或打用程序会阻止访问该对象。 AskUser – 应用程序会提示用户为检测到择一种操作：跳过、隔离或删除。当检测时，用户可以对所有对象应用所选操作。 有关检测到的威胁以及对它们执行的操作应用程序报告中。
ScanLock	阻止配置扫描设置	Boolean	True – 用户无法访问应用程序设置中的以要扫描的文件类型、压缩文件扫描以及当要执行的操作。 False – 用户可以配置扫描设置，以及，到的威胁选择 Skip 操作。
ScanAndProtectionAdwareRiskware	阻止可被犯罪分子用来对用户的设备和数据造成损害的广告软件、自动拨号程序和应用程序	Boolean	True– 应用程序会检测可被犯罪分子用来和数据造成损害的广告软件和其他应用程 False – 应用程序会跳过可被犯罪分子用备和数据造成损害的广告软件和其他应用
ProtectionMode	实时保护模式	Choice	Recommended – 应用程序仅扫描新安装的载"文件夹中的文件。 Extended – 应用程序扫描用户在设备上复制、运行和保存的所有文件。应用程序载"文件夹中的新应用程序和文件。

			Disabled – 禁用实时保护。
UseKsnMode	卡巴斯基安全网络模式	Choice	Recommended – 应用程序会与卡巴斯基安交换数据。Kaspersky Endpoint Security f用 KSN 实时保护设备免受威胁（云保护）运行 Web 保护。 Extended – 应用程序会与卡巴斯基安全网据，而且还会将来自 Kaspersky Endpoint Android 的某些性能统计信息发送到病毒实息有助于实时跟踪威胁。KSN 服务不会收储个人数据。 Disabled – 应用程序不会使用来自卡巴斯的数据。您不能启用 Web 保护 (EnableWe云保护组件对反病毒不可用。
ProtectScanOnlyExecutableFiles	要扫描的文件类型（实时保护）	Boolean	AllFiles – 扫描所有文件。 OnlyExecutables – 仅扫描可执行文件。带有 apk (.zip)、.dex 等扩展名的文件。 在 Kaspersky Endpoint Security for Andro Pack 4 Maintenance Release 1 中，您无法文件扫描。
ProtectionActionOnThreatFound	检测到威胁后的操作（实时保护）	Choice	Quarantine – 应用程序会将检测到的对区。应用程序会将存档形式隔离文件，不伤害。隔离区允许您删除或恢复移动至隔 Delete – 应用程序删除检测到的对象。 Skip – 应用程序会将检测到的对象保留不到的对象被跳过，Kaspersky Endpoint Sec Android 会警告用户设备保护方面存在问题问设备上的某个对象（如尝试复制或打开程序会阻止访问该对象。 有关检测到的威胁以及对它们执行的操作应用程序报告中。
ProtectionLock	阻止配置实时保护设置	Boolean	True – 用户无法访问应用程序设置中的以置：实时保护模式、要扫描的文件类型以胁时要执行的操作。 False – 用户可以配置实时保护设置，以检测到的威胁选择 Skip 操作。
UpdateScheduleType	数据库更新运行模式	Choice	Daily – 每天检查一次是否有新的反病毒们下载到设备。配置数据库更新启动时间 (UpdateScheduleTime)。 Weekly – 每周检查一次是否有新的反病毒它们下载到设备。选择一周中启动数据库 (UpdateScheduleDay) 并配置时间 (UpdateScheduleTime)。 Off – 禁用自动更新反病毒数据库。 无论设置哪个值，设备用户均可手动启动更新。
UpdateScheduleDay	启动数据库更新的日期	Choice	Monday / Tuesday / Wednesday / Th Friday / Saturday / Sunday 您只能为此设置选择一个值。

UpdateScheduleTime	数据库更新启动时间	String	时间可以采用 24 小时格式（例如，13:00）式（例如，10:30 P.M.）指示。
UpdateScheduleLock	阻止配置数据库更新运行模式	Boolean	True – 用户无法访问应用程序设置内的数模式设置。 False – 用户可以配置数据库更新运行模式用反病毒数据库更新自动启动。
AllowUpdateInRoaming	漫游时更新数据库	Boolean	True – 如果设备在漫游区域，应用程序会据库。应用程序将按照定义的计划下载反(UpdateScheduleType)。 False – 仅当设备在家庭网络中时，应用反病毒数据库。
EnableWebFilter	Web 保护	Boolean	True – 应用程序使用 Web 保护组件阻止意和钓鱼网站。Web 保护仅支持 Google 如果域是受信任的，使用 HTTPS 协议的网站将保持为不被阻止。如果域是不受Web 保护阻止恶意和钓鱼网站。 False – 禁用恶意和钓鱼网站防御。 要使 Web 保护组件工作，必须满足以下条 • 设备用户在初始化配置向导或应用设置略和 Web 保护声明。 • 在浏览器设置中配置代理服务器：ProxyMode = "fixed_servers" ProxyServer = "127.0.0.1:3128" DisableSpdy = true DataCompressionProxyEnabled = 代理服务器配置可能因 Google Chrom而有所不同。有关配置 Google Chrom信息，请访问 Chromium 项目网站。在从移动设备上卸载 Kaspersky Endpo for Android 应用程序之后，重置代理服 • 在应用程序设置中启用 KSN 的使用：UseKsnMode = Recommended 或 UseKsnMode = Exte • 建议选择 Google Chrome 作为操作系统认浏览器。
EnableWebFilterLock	阻止配置 Web 保护	Boolean	True – 用户无法访问应用程序设置内的 W置。 False – 用户可以配置 Web 保护设置，例联网上恶意和钓鱼网站的防护。
UpdateServer	数据库更新源服务器地址	String	托管数据库更新的服务器的地址，例如，http://update.server.com。 如果您将此字段留空，Kaspersky Endpoin Android 将使用 Kaspersky 更新服务器。
AllowGoogleAnalytics	将数据提交到 Google	Boolean	True – 应用程序将 Kaspersky Endpoint S Android 操作数据自动提交至 Google Anal

	Analytics for Firebase、SafetyNet Attestation、Firebase Performance Monitoring 和 Crashlytics 服务		Firebase、SafetyNet Attestation、Fireba Performance Monitoring 和 Crashlytics 服 于改进该应用程序的性能并分析用户满意 安全连接传输到 Google Analytics for Firel SafetyNet Attestation、Firebase Perform Monitoring 和 Crashlytics 服务。对数据的 合 Google Analytics for Firebase、Safetyl Attestation、Firebase Performance Monit Crashlytics 服务的相关使用条款的要求。 `False` – 禁止将数据提交至 Google Analyt Firebase、SafetyNet Attestation、Fireba Performance Monitoring 和 Crashlytics 服
`KscDeviceNameTag`	Kaspersky Security Center 的设备名称标签	String	该设置仅对 VMware AirWatch 可用. 标签将在 Kaspersky Security Center 中被 称。使用空格分隔标签和设备名称。这样 在 Kaspersky Security Center 中查找和排 • `{DeviceSerialNumber}` – 设备的序列 • `{DeviceUid}` – 唯一的设备标识符 (UI • `{DeviceAssetNumber}` – 设备资产编 您的公司内部创建。 您可以添加某些值（例如， `{DeviceSerialNumber} {DeviceUi` 我们推荐仅使用这些值。VMware AirWa 他值，但 Kaspersky Endpoint Security 些值能正常工作。
`KscGroup`	设备组名称	String	您可以在 EMM 控制台中指定设备组。当设 Kaspersky Security Center 后，它将自动 配的设备"文件夹的子文件夹中。该子文件 配此参数中指定的组名称。然后，可以创 自动将"未分配的设备"文件夹的子文件夹中 到"受管设备"文件夹的管理组中。 如果将该字段留空，设备将自动添加到"未 文件夹的根目录中。
`KscCorporateEmail`	用户的公司电子邮件	String	您可以在 EMM 控制台中指定用户的公司电 址。这些电子邮件将显示在 Kaspersky Se 中。 字符串必须是有效的电子邮件地址。其他
`KscDeviceName`	Kaspersky Security Center 中的设备名称	String	该设置仅对 SOTI MobiControl 可用。

			您可以指定 Kaspersky Security Center 中称。您可以输入任意名称或使用 %DEVICE 动从 SOTI MobiControl 控制台获取设备名字段留空，设备名称将根据 Kaspersky Se 组策略中指定的格式生成。

网络负载

本节包含有关移动设备和 Kaspersky Security Center 之间交换的网络流量的信息。

流量

任务	外出流量	内进流量	总流量
应用程序初始部署，Mb	0.08	17.76	17.84
反病毒数据库初始更新（流量可能会因反病毒数据库的大小而不同），MB	0.04	2.21	2.25
移动设备与 Kaspersky Security Center 同步，MB	0.03	0.02	0.05
反病毒数据库定期更新（流量可能会因反病毒数据库的大小而不同），MB	0.08	3.06	3.14
执行反盗窃命令。定位设备（流量可能会因嵌入式摄像头规格和图像质量而不同），MB	0.09	0.8	0.17
执行反盗窃命令。拍摄面部照片，MB	1.0	0.02	1.02
执行反盗窃命令。设备锁定，MB	0.06	0.05	0.11
平均每日流量，MB	0.22	6.96	7.18

加入卡巴斯基安全网络

为了更有效地保护移动设备，Kaspersky Endpoint Security for Android 会使用从全球用户处获取的数据。*卡巴斯基安全网络*用户处理此类数据。

卡巴斯基安全网络 (KSN) 是一种云服务基础设施，它提供对 Kaspersky 在线知识库的访问，该知识库包含有关文件、Web 资源和软件的信誉的信息。使用卡巴斯基安全网络中的数据，可确保在遇到威胁时 Kaspersky 程序能够做出更快速的响应，提高某些保护组件的性能，并降低误报的风险。

您加入卡巴斯基安全网络将帮助 Kaspersky 获取有关新威胁的类型和来源的实时信息，研究消除威胁的办法并降低 Kaspersky Endpoint Security for Android 的误报数量。加入卡巴斯基安全网络也允许您访问应用程序和网站信誉统计数据。

加入卡巴斯基安全网络后，当 Kaspersky Endpoint Security for Android 运行时，会获取一些统计信息并自动发送至 Kaspersky。该信息有助于实时跟踪威胁。可能会被入侵者用来入侵以损坏计算机或用户资料的文件或其部分也会被发送至 Kaspersky 以进行额外的检查。

Kaspersky Endpoint Security for Android 的操作需要使用卡巴斯基安全网络。KSN 被用于应用程序的主要组件：反病毒、Web 保护和应用程序控制。拒绝参与 KSN 会降低设备保护级别，这将引发设备感染和数据丢失。要开始使用卡巴斯基安全网络，您必须在安装应用程序时接受最终用户授权许可协议的条款。通过阅读最终用户授权许可协议，您可以知道哪些数据被 Kaspersky Endpoint Security for Android 传输到卡巴斯基安全网络。

要改进应用程序性能，您可以另外提供统计数据到卡巴斯基安全网络。将上述信息提供给 KSN 属自愿行为。若要开始使用卡巴斯基安全网络，您必须接受特殊的协议条款 - *卡巴斯基安全网络声明*。您可以随时选择退出卡巴斯基安全网络。卡巴斯基安全网络声明说明了 Kaspersky Endpoint Security for Android 向卡巴斯基安全网络传输的数据的类型。

与卡巴斯基安全网络交换信息

为改进实时保护功能，Kaspersky Security for Mobile 将使用卡巴斯基安全网络云服务执行以下组件：

- 反病毒。应用获得到关于文件和应用信誉的 Kaspersky 在线知识库的访问。此项扫描旨在扫描威胁信息尚未添加到反病毒数据库但已包含在 KSN 中的威胁。卡巴斯基安全网络云服务提供反病毒的完整操作并降低误报。
- **Web 保护。**在打开网站之前，该应用程序使用从 KSN 接收的数据对网站运行扫描。该应用程序会根据允许和阻止的类别（例如，“互联网通信”类别）列表来确定网站类别，以控制用户的互联网访问权限。
- 应用程序控制。该应用程序可基于允许和阻止的类别（例如，“互联网通信”类别）列表，确定限制不符合公司安全要求的应用程序启动的应用程序类别。

最终用户授权许可协议中提供了有关在运行反病毒和应用程序控制的过程中使用 KSN 时提交到 Kaspersky 的数据类型的信息。接受授权许可协议的条款和条件即表明您同意传输此信息。

关于 Web 保护的数据处理的声明中提供了有关在运行 Web 保护的过程中使用 KSN 时提交到 Kaspersky 的数据类型的信息。接受声明的条款和条件即表明您同意传输此信息。

为了识别新出现的信息安全威胁、入侵威胁和难以检测的威胁（及其各自的来源），以及改进对设备上存储和处理的信息的保护，您可以扩展对卡巴斯基安全网络的参与。

要与 KSN 交换数据以提高应用程序的性能，必须满足以下条件：

- 您或设备用户必须阅读并接受卡巴斯基安全网络声明的条款。如果您选择由用户接受声明，则会在应用程序主屏幕上显示一条通知，提示用户接受声明的条款。用户还可以在 Kaspersky Endpoint Security for Android 设置的“**关于应用程序**”区域中接受声明。

  如果您选择全局接受声明，则通过 Kaspersky Security Center 接受的声明版本必须与用户已经接受的版本相匹配。否则，用户将被告知有问题，并被提示接受与管理员全局接受的版本相匹配的声明版本。Kaspersky Security for Mobile (Devices) 插件中的设备状态也将更改为“*警告*”。

- 您必须将组策略设置配置为允许发送统计信息到 KSN。

您可以随时选择退出发送统计数据到卡巴斯基安全网络。如果卡巴斯基安全网络声明中规定了在运行 Kaspersky Endpoint Security for Android 移动应用程序的过程中使用 KSN，则会将有关统计数据类型的信息提交到 Kaspersky。

有关向 KSN 提供数据的更多信息，请参阅“数据提供”部分。

向 KSN 提供数据是自愿的。如果需要，您可以禁用与 KSN 的数据交换。

启用和禁用使用卡巴斯基安全网络

为运行使用卡巴斯基安全网络的 Kaspersky Endpoint Security for Android 组件，应用程序会向云服务发送请求。请求包含“数据提供”部分中所述的数据。

如果设备上禁用了卡巴斯基安全网络，则云保护、Web 保护和应用程序控制组件将被自动禁用。

若要启用和禁用使用卡巴斯基安全网络，请执行以下操作：

1. 打开提供用于管理安装了 Kaspersky Endpoint Security for Android 的移动设备策略设置的窗口。
2. 在策略“**属性**”窗口中选择“**其他**”区域。
3. 在“**卡巴斯基安全网络 (KSN) 设置**”区域中，配置使用卡巴斯基安全网络的设置：
   - 要运行以下组件，请选中“**使用卡巴斯基安全网络**”复选框：反病毒（云保护）、Web 保护和应用程序控制（应用程序类别）。
   - 选中“**允许发送统计信息到 KSN**”复选框以将数据提交给 Kaspersky。此数据将帮助 Kaspersky Endpoint Security for Android 应用程序在遇到威胁时更快地作出响应，提高保护组件的性能以及降低误报的风险。
4. 单击“**应用**”按钮以保存所作的更改。

与 Kaspersky Security Center 的下次设备同步之后可配置移动设备设置。应用策略后，使用卡巴斯基安全网络的组件将被禁用，组件设置将不可用。

使用卡巴斯基私有安全网络

卡巴斯基私有安全网络（以下也称为*私有 KSN*或 *KPSN*）解决方案可授予对卡巴斯基安全网络信誉数据库的访问权限，无需将用户设备中的数据发送到卡巴斯基安全网络。

对象（文件或 URL）的信誉数据库存储在卡巴斯基私有安全网络服务器上，而不存储在卡巴斯基安全网络服务器上。KPSN 信誉数据库存储在公司网络内，由公司管理员管理。

启用 KPSN 后，Kaspersky Endpoint Security 不会将用户设备的任何统计数据发送到 KSN。

要通过 Kaspersky Security Center 启用私有 KSN：

1. 在 Kaspersky Security Center Web Console 或云控制台的主窗口中，单击“**设置**”()。
   将打开管理服务器属性窗口。
2. 在“**常规**”选项卡上，选择“**KSN 代理设置**”区域。
3. 将切换按钮切换到“**使用卡巴斯基私人安全网络已启用**”位置。
4. 单击“**选择含有 KSN 代理设置的文件**”按钮，然后浏览查找具有 pkcs7 或 pem 扩展名的配置文件（由 Kaspersky 提供）。
5. 单击“**打开**”。
6. 如果您在管理服务器属性中配置了代理服务器设置，但您的网络架构要求您直接使用私人 KSN，请启用“**连接到私人 KSN 时忽略 KSC 代理服务器设置**”选项。否则，来自受管理应用程序的请求无法到达私人 KSN。
7. 单击“**保存**”按钮。

下载设置后，界面将显示提供商的名称和联系人，以及包含私人 KSN 设置的文件的创建日期。KPSN 设置将应用于移动设备。

切换到私有 KSN 后，“应用程序控制”将不支持使用全球 KSN 时可用的应用程序类别。如果选择切换回 KSN，将可以进行应用程序分类。

对第三方服务的数据提供

Kaspersky Endpoint Security for Android 使用 Google™ 服务，即 Firebase Cloud Messaging、Google Analytics for Firebase™、SafetyNet Attestation、Firebase Performance Monitoring 和 Crashlytics。Kaspersky Endpoint Security for Android 使用 Firebase Cloud Messaging (FCM) 服务以确保向移动设备的命令传送并在策略设置被更改时强制同步。Kaspersky Endpoint Security for Android 使用 Google Analytics for Firebase、SafetyNet Attestation、Firebase Performance Monitoring 和 Crashlytics 服务改进应用性能并帮助 Kaspersky 创建更有效的营销资料。

与 Firebase Cloud Messaging 交换信息

Kaspersky Endpoint Security for Android 使用 Firebase Cloud Messaging (FCM) 服务以确保向移动设备的命令传送并在策略设置被更改时强制同步。该应用程序还使用推送通知。

要使用 Firebase Cloud Messaging 服务，您必须在 Kaspersky Security Center 中配置服务设置。有关在 Kaspersky Security Center 中配置 Firebase Cloud Messaging 的详细信息，请参阅 *Kaspersky Security Center 帮助*。如果未配置 Firebase Cloud Messaging 设置，当移动设备根据策略中设置的计划（例如，每 24 小时一次）与 Kaspersky Security Center 同步时，设备上的命令和策略设置将被传送。换句话说，命令和策略设置将被延迟传送。

出于支持产品主要功能的目的，您同意自动提供 Firebase Cloud Messaging 服务应用安装的独一 ID（实例 ID）以及以下数据：

- 已安装软件的信息：应用版本、应用 ID、应用版本号、应用包名称。
- 安装了软件的计算机信息：OS 版本、设备 ID、Google 服务版本。
- FCM 信息：FCM 中应用 ID、FCM 用户 ID、协议版本。

数据通过安全连接传输到 Firebase 服务。对信息的访问和保护依照 Firebase 服务的相关使用条款：https://firebase.google.com/terms/data-processing-terms/、https://firebase.google.com/support/privacy/。

阻止与 Firebase Cloud Messaging 服务交换信息：

1. 在控制台树中，选择“**移动设备管理**”→“**移动设备**”。
2. 从“**移动设备**”文件夹的上下文菜单中，选择“**属性**”。
3. 在“**移动设备**”文件夹的属性窗口中，选择“**Google Firebase Cloud Messaging 设置**”区域。
4. 单击“**重置设置**”按钮。

与 Google Analytics for Firebase、SafetyNet Attestation、Firebase Performance Monitoring 和 Crashlytics 交换信息

如果使用以前版本的管理插件并启用了与 Google Analytics 服务的数据交换，Kaspersky Endpoint Security for Android Service Pack 4 Maintenance Release 3 将执行与 Google Analytics for Firebase 服务的数据交换。Google Analytics 支持已停止。

Kaspersky Security for Mobile 与 Google Analytics for Firebase、SafetyNet Attestation、Firebase Performance Monitoring 和 Crashlytics 服务交换数据的目的如下：

- 提高应用程序的性能。

  要与 Google Analytics for Firebase、SafetyNet Attestation、Firebase Performance Monitoring 和 Crashlytics 服务交换数据以提高应用程序的性能，必须满足以下条件：

  - 管理员或设备用户必须阅读并接受卡巴斯基安全网络声明的条款。如果您选择由用户接受声明，则会在应用程序主屏幕上显示一条通知，提示用户接受声明的条款。用户还可以在 Kaspersky Endpoint Security for Android 设置的“**关于应用程序**”区域中接受声明。

    如果您选择全局接受声明，则通过 Kaspersky Security Center 接受的声明版本必须与用户已经接受的版本相匹配。否则，用户将被告知有问题，并被提示接受与管理员全局接受的版本相匹配的声明版本。Kaspersky Security for Mobile (Devices) 插件中的设备状态也将更改为“*警告*”。

  - 管理员必须将组策略设置配置为允许发送统计信息到 KSN（参见下文）。

- 帮助 Kaspersky 创建更有效的市场营销材料。

  要与 Google Analytics for Firebase、SafetyNet Attestation、Firebase Performance Monitoring 和 Crashlytics 服务交换数据以帮助 Kaspersky 创建有效的市场营销材料，必须满足以下条件：

  - 管理员或设备用户必须阅读并接受有关将数据处理用于市场营销的声明的条款。如果您选择由用户接受声明，他们可以在安装应用程序时或在 Kaspersky Endpoint Security for Android 设置的“**关于应用程序**”区域中接受声明的条款。

  - 管理员必须将组策略设置配置为允许向 Google Analytics for Firebase、SafetyNet Attestation、Firebase Performance Monitoring 和 Crashlytics 发送数据（参见下文）。

[在有关将数据处理用于市场营销的声明下向 Google Analytics for Firebase、SafetyNet Attestation、Firebase Performance Monitoring 和 Crashlytics 提供数据]

权利持有人采用第三方信息系统对数据进行处理。权利持有人的数据处理受此类第三方信息系统的隐私声明约束。以下为权利持有人采用的服务以及权利持有人所处理的数据：

Google Analytics for Firebase

在本软件使用期间，下列数据将自动定期发送至 Google Analytics for Firebase 以实现所宣称的目的：

- 应用信息（应用版本、应用 ID 和 Firebase 服务中的应用 ID、Firebase 服务中的实例 ID、获取应用程序的商店名称、本软件首次启动的时间戳）
- 设备上应用程序安装的 ID 以及安装方法
- 有关区域和语言本地化的信息
- 有关设备屏幕分辨率的信息
- 有关获取根的用户的信息
- 有关源自 SafetyNet Attestation 服务的设备的诊断信息
- 有关将 Kaspersky Endpoint Security for Android 设置为可访问性的信息。
- 有关应用程序屏幕之间的转换、会话持续时间、屏幕会话的开始和结束、屏幕名称的信息
- 有关用于向 Firebase 服务提交数据的协议、其版本以及所采用的数据提交方法 ID 的信息
- 有关所提交数据相关事件的类型和参数的详细信息
- 有关应用许可证、其可用性以及设备数量的信息
- 有关反病毒数据库更新频率和与管理服务器同步的信息
- 有关管理控制台（卡巴斯基安全中心或第三方 EMM 系统）的信息
- Android ID
- 广告 ID
- 有关用户的信息： 年龄类别和性别、居住国家/地区的标识符以及兴趣列表
- 有关安装了该软件的用户计算机的信息： 计算机制造商名称、计算机类型、型号、操作系统的版本和语言（区域设置）、有关最近 7 天内首次打开的应用程序和超过 7 天前首次打开的应用程序的信息

  数据将通过安全通道转发给 Firebase。有关 Firebase 如何处理数据的信息发布于：https://firebase.google.com/support/privacy.

SafetyNet Attestation

在本软件使用期间，为了实现所宣称的目的，将自动定期向 SafetyNet Attestation 发送以下数据：

- 设备检查时间
- 有关软件的信息以及有关软件证书的名称和数据
- 设备检查结果

- 随机 ID 检查，以验证设备检查结果

  数据通过安全通道转发到 SafetyNet Attestation。有关 SafetyNet Attestation 如何处理数据的信息发布于：https://policies.google.com/privacy.

Firebase 性能监测

使用本软件期间，以下信息将自动定期发送至“Firebase 性能监测”(FPM) 以实现宣称的目的：

- 唯一的安装 ID
- 应用程序包名称
- 已安装软件的版本
- 电池电量和电池充电状态
- 载体
- 应用程序前景或背景状态
- 地理位置
- IP 地址
- 设备语言代码
- 有关无线电 / 网络连接的信息
- 假名的软件实例 ID
- 内存和磁盘大小
- 指示设备是否已越狱或获得根权限 (root) 的标志
- 信号强度
- 自动跟踪持续时间
- 网络及以下相应信息： 响应代码、有效负载大小（字节）、响应时间
- 设备描述

  数据通过安全通道转发至“Firebase 性能监测”(FPM)。有关 Firebase Performance Monitoring 如何处理数据的信息发布于：https://firebase.google.com/support/privacy.

Crashlytics

使用本软件期间，以下信息将自动定期发送至 Crashlytics 以实现宣称的目的：

- 软件 ID
- 已安装软件的版本
- 指示软件是否在后台运行的标志
- CPU 架构

- 唯一事件标识符
- 事件日期和时间
- 设备型号
- 总磁盘空间和当前占用量
- 操作系统的名称和版本
- 总内存和当前占用量
- 指示设备是否已获得根权限 (root) 的标志
- 事件发生时的屏幕定位
- 产品 / 硬件制造商
- 唯一的安装 ID
- 所发送的统计数据的版本
- 软件异常类型
- 错误消息文本
- 指示软件异常是由嵌套异常所引起的标志
- 线程 ID
- 指示帧是否是软件错误原因的标志
- 指示线程导致软件意外终止的标志
- 有关导致软件意外终止的信号的信息： 信号名称、信号代码、信号地址
- 对于与线程、异常或错误关联的每个帧： 帧文件的名称、帧文件的行号、调试符号、二进制图像中的地址和偏移量、带帧的库的显示名称、帧的类型、指示帧是否是错误原因的标志
- OS ID
- 与事件关联的问题的 ID
- 有关软件意外终止前发生的事件的信息： 事件标识符、事件日期和时间、事件类型和值
- CPU 注册表值
- 事件类型和值

  数据通过安全渠道转发至 Crashlytics。有关 Crashlytics 如何处理数据的信息发布于：https://firebase.google.com/terms/crashlytics-app-distribution-data-processing-terms.

基于自愿原则出于营销目的提供上述处理信息。

要禁用与 Google Analytics for Firebase、SafetyNet Attestation、Firebase Performance Monitoring 和 Crashlytics 服务的数据交换：

1. 打开安装了 Kaspersky Endpoint Security for Android 应用程序的移动设备的管理策略的配置窗口。
2. 在策略“**属性**”窗口中选择“**其他**”区域。
3. 在“**数据传输**”区域中，清除“**允许数据传输以帮助改进应用程序的质量、外观和性能**”复选框。
4. 单击“**应用**”按钮以保存所作的更改。

与 Kaspersky Security Center 的下次设备同步之后可配置移动设备设置。

全局接受附加声明

要启用 Kaspersky Endpoint Security for Android 提供的保护，必须接受最终用户授权许可协议以及附加声明的条款（参见下文）。您将配置全局接受下列声明的策略，适用于所有用户。用户将不会被提示阅读和接受以下已经被全局接受的协议和声明的条款：

- 卡巴斯基安全网络声明
- 有关用于 Web 保护的数据处理声明
- 有关将数据处理用于市场营销的声明

如果您选择全局接受声明，则通过 Kaspersky Security Center 接受的声明版本必须与用户已经接受的版本相匹配。否则，用户将被告知有问题，并被提示接受与管理员全局接受的版本相匹配的声明版本。Kaspersky Security for Mobile (Devices) 插件中的设备状态也将更改为“*警告*”。

要选择必须全局接受条款还是通过应用组策略由用户接受条款：

1. 在控制台树的“**受管设备**”文件夹中，选择 Android 设备所属的管理组。
2. 在所选组的工作区中，选择“**策略**”选项卡。
3. 通过双击任意列打开策略属性窗口。
4. 在策略“**属性**”窗口中选择“**其他**”区域。
5. 在“**数据传输**”区域中，选择用于市场营销的数据处理声明将被全局接受还是由用户接受。
6. 在“**卡巴斯基安全网络 (KSN) 设置**”区域中，选择卡巴斯基安全网络声明将被全局接受还是由用户接受。
7. 单击“**应用**”按钮以保存所作的更改。

用户可以随时在 Kaspersky Endpoint Security for Android 的“**关于应用程序**”区域中接受或拒绝声明的条款。

三星 KNOX

三星 KNOX 是一个配置和保护运行安卓操作系统的三星移动设备的移动设备解决方案。有关 Samsung KNOX 的更多详细信息，请访问*三星技术支持网站*。

通过 KNOX Mobile Enrollment 安装 Kaspersky Endpoint Security for Android 应用程序

KNOX Mobile Enrollment (KME) 是三星 KNOX 移动解决方案的一部分。它用于在通过官方供应商购买的全新三星设备上批量安装应用程序和初始配置。

通过 KNOX Mobile Enrollment 安装 Kaspersky Endpoint Security for Android 应用程序包括以下步骤：

1. 使用 Kaspersky Endpoint Security for Android 应用程序创建 KNOX MDM 配置文件。
2. 在 KNOX Mobile Enrollment 中添加设备。
3. 在用户的移动设备上安装 Kaspersky Endpoint Security for Android 应用程序。

有关使用 KNOX Mobile Enrollment 的更多详细信息，请参阅 *KNOX Mobile Enrollment 用户指南*。

只有三星设备可以通过 KNOX Mobile Enrollment 进行部署。有关支持的设备列表，请访问*三星技术支持网站*。

创建 KNOX MDM 配置文件

KNOX MDM 配置文件是一种包含指向应用程序的链接以便在移动设备上进行快速部署和初始配置的配置文件。

要创建 KNOX MDM 配置文件，请执行以下操作：

1. 登录三星 KNOX 控制台 → **KNOX Mobile Enrollment**。
2. 选择“**MDM 配置文件**”部分。
3. 单击“**添加**”。
   新 KNOX MDM 配置文件向导将启动。
4. 在“**MDM 服务器连接**”步骤，选择“**我的 MDM 服务无需服务器 URI**”，然后单击“**下一步**”。
5. 在“**MDM 配置文件信息**”步骤：
   a. 输入有关 KNOX MDM 配置文件的一般信息：“**配置文件名称**”和“**描述**”。
   b. 单击“**添加 MDM 应用程序**”按钮，然后输入 APK 安装文件的路径。
      Kaspersky Endpoint Security for Android 的安装文件包含在 Kaspersky Security for Mobile 分发包中。提前将 APK 安装文件放在 Kaspersky Security Center Web 服务器或可访问以便从设备上下载的其他服务器上。
   c. 采用以下格式在“**JSON 用户数据**”字段中输入用于将设备连接到 Kaspersky Security Center 的设置：`{"serverAddress":"ksc.server.com","serverPort":"12345","groupName":"MOBILE GROUP"}`。
      必须将设备连接到 Kaspersky Security Center 才能激活应用程序，配置设备以及发送命令。
   d. 选中“**添加 Knox 协议**”选框。

要通过 KNOX Mobile Enrollment 安装 Kaspersky Endpoint Security for Android，移动设备用户必须接受 Samsung 授权许可协议的条款。您可以在名为“**最终用户授权许可协议、服务条款和用户协议**”的区域中查看 Samsung 授权许可协议的条款。您还可以通过单击“**添加用户协议**”按钮来添加部署 KNOX MDM 配置文件所需的公司其他法律文档。

e. 清除“**将 KNOX 授权许可绑定到此配置文件**”复选框。

当设备与 Kaspersky Security Center 同步时，Samsung KNOX 授权许可信息将与策略一起传递到移动设备。

6. 单击“**保存**”按钮。

因此，带有 Kaspersky Endpoint Security for Android 应用程序的新 KNOX MDM 配置文件将添加到 KME 控制台中的列表中。

在 KNOX Mobile Enrollment 中添加设备

可以采用以下方式将设备添加到 KNOX Mobile Enrollment (KME) 控制台中：

- 在购买设备后，供应商会将设备自动添加到 KME 控制台中。

  如果您的组织使用三星设备的官方供应商，请选择此方法。

- 管理员可通过 Google Play 在移动设备上安装 KNOX 部署应用程序，然后通过蓝牙或 NFC（近场通信）将 KNOX MDM 配置文件迁移到用户设备。在部署 KNOX MDM 配置文件后，设备将自动添加到 KME 控制台中。

  如果三星设备不是从官方供应商处购买的，请选择此方法。

通过供应商添加设备

三星设备的官方供应商在三星 KNOX 中有注册。有关官方供应商列表，请访问*三星技术支持网站*。在购买设备后，供应商会立即将设备自动添加到您的三星账户的 KME 控制台中。要使供应商添加设备，您必须在三星账户的 KME 控制台中注册供应商。您将需要一个经销商 ID 才能在 KME 控制台中添加三星设备的供应商。要接收经销商 ID，您必须向供应商发送请求。在请求中，指定您的 KNOX 客户端 ID。

要查看您的 KNOX 客户端 ID，请执行以下操作：

1. 登录三星 KNOX 控制台 → **KNOX Mobile Enrollment**。
2. 选择“**经销商**”区域。
3. 您的 ID 将在“**KNOX 客户端 ID**”字段中显示。

在您从供应商处收到包含经销商 ID 的响应后，在 KME 控制台中注册供应商。在注册供应商之前，您可以创建一个 KNOX MDM 配置文件，以便在添加新设备时可以自动部署该配置文件。

要在 KME 控制台中注册官方供应商，请执行以下操作：

1. 登录三星 KNOX 控制台 → **KNOX Mobile Enrollment**。
2. 选择“**经销商**”区域。
3. 单击“**注册经销商**”按钮。

   这会打开一个窗口，用于注册设备供应商。

4. 在“**经销商 ID**”字段中，输入从三星设备官方经销商处接收的 ID。

5. 如果您创建了一个 KNOX MDM 配置文件，请在供应商注册窗口中选择该 KNOX MDM 配置文件。

   在您添加新设备时，该 KNOX MDM 配置文件会自动安装。

6. 在“**首选下载确认方法**”列表中，选择一种确认供应商添加设备的方法。

   - **必须确认所有下载**。当供应商添加设备时，您将需要确认此操作。
   - **自动确认此经销商的所有下载**。该供应商的设备将自动添加到 KME 控制台中。

7. 单击“**确定**”。

三星设备的供应商将添加到 KME 控制台的供应商列表中。

从官方供应商处购买新设备后，将设备连接到互联网时，Kaspersky Endpoint Security for Android 应用程序将自动安装到设备上。有关使用 KNOX Mobile Enrollment 的更多详细信息，请参阅“*KNOX Mobile Enrollment 用户指南*”。如果您在 KME 控制台中已有设备列表，则将包含 KNOX MDM 应用程序的 KNOX MDM 配置文件添加到设备。

要将 KNOX MDM 配置文件传送到设备，请执行以下操作：

1. 登录三星 KNOX 控制台 → **KNOX Mobile Enrollment**。

2. 选择“**设备**”→“**所有设备**”。

3. 选择您要安装 KNOX MDM 配置文件的设备。

4. 单击“**配置**”按钮。

   “**设备信息**”窗口将打开。

5. 在“**MDM 配置文件**”列表中，选择包含 Kaspersky Endpoint Security for Android 应用程序的 KNOX MDM 配置文件。

6. 在“**标签**”字段中，输入用于分组和标记设备，以及 KME 控制台中的搜索优化的标签。

7. 将设备的用户账户凭据输入到“**用户 ID**”和“**密码**”字段。

   接收常规证书需要账户凭据。用户 ID 和密码必须与 Kaspersky Security Center 中的用户账户凭据匹配（用户账户属性中的“全名”和“密码”）。

8. 为剩余设备选择 KNOX MDM 配置文件。

9. 单击“**保存**”按钮。

在将设备连接到互联网之后，系统将提示用户安装 KNOX MDM 配置文件。

通过 KNOX 部署应用程序添加设备

如果您未从官方供应商处购买三星设备，您可以通过蓝牙或 NFC 将设备添加到 KNOX Mobile Enrollment。这将需要使用管理员的移动设备来将 KNOX MDM 配置文件传送到用户的移动设备。

要使用 KNOX 部署应用程序添加设备，必须满足以下条件：

- 根据所选传送模式，必须在移动设备上启用蓝牙或 NFC 模块。

- 移动设备必须连接到互联网。

要使用 KNOX 部署应用程序传送 KNOX MDM 配置文件，请执行以下操作：

1. 通过 Google Play 在管理员的移动设备上安装 KNOX 部署应用程序。
2. 启动 KNOX 部署应用程序。
3. 输入您的三星账户凭据。
4. 在“**KNOX 部署**”窗口中，配置部署 KNOX MDM 配置文件的设置：
   - 选择“KNOX MDM 配置文件”。
   - 选择部署模式：“**蓝牙**”或“**NFC**”。
     当使用蓝牙时，您可将一个 KNOX MDM 配置文件同时添加到多台设备。
5. 单击“**开始部署**：
   - **蓝牙**”。在用户的移动设备上，打开网站 https://configure.samsungknox.com。
     这会启动三星 KNOX 设备注册向导。按照屏幕上的说明操作。
     安装 KNOX MDM 配置文件之后，带有“**蓝牙**”标签的新设备将添加到 KME 控制台中。
   - **NFC**。将管理员的移动设备带至用户的移动设备附近，并传输 KNOX MDM 配置文件。
     在用户的移动设备上，将提示安装 KNOX MDM 配置文件。带有“**NFC**”标签的新设备将添加到 KME 控制台中。

安装应用程序

在安装 Kaspersky Endpoint Security for Android 应用程序之前，在 Kaspersky Security Center 管理控制台中为移动设备用户颁发常规证书。识别 Kaspersky Security Center 管理控制台中的移动设备用户需要常规证书。

在开始部署 KNOX MDM 配置文件之后，APK 安装文件将自动下载到移动设备上。Kaspersky Endpoint Security for Android 应用程序安装将自动启动。用户必须接受三星 KNOX 授权许可协议和 Kaspersky Endpoint Security for Android 授权许可协议。无需其他应用程序配置。在安装了应用程序之后，将自动执行与 Kaspersky Security Center 同步。移动设备将添加至 Kaspersky Security Center 管理控制台中 KNOX MDM 配置文件设置中指定的管理组中 (`groupName`)。

配置 KNOX 容器

本节包含有关在运行安卓的三星设备上使用 KNOX 容器的信息。

只能在运行安卓版本 6.0 或更高版本的三星设备上使用 KNOX 容器。

关于 KNOX 容器

*KNOX 容器*是用户设备上的一个安全环境，具有自己的桌面、启动面板、应用程序和小部件。KNOX 容器可让您将企业应用程序和数据与个人应用程序和数据隔离。KNOX 容器是 Samsung KNOX 移动解决方案的一个组件。

三星 KNOX 是一个配置和保护运行安卓操作系统的三星移动设备的移动设备解决方案。有关 Samsung KNOX 的更多详细信息，请访问*三星技术支持网站*。

KNOX 容器允许您在移动设备上隔离个人数据和公司数据。例如，使用个人邮箱无法发送位于 KNOX 容器中的文件。如果员工的个人移动设备用于处理公司数据，建议部署 KNOX 容器。

若要使用 KNOX 容器，必须激活 Samsung KNOX。在将设备与 Kaspersky Security Center 同步后，将提示移动设备的用户安装 KNOX 容器。在安装 KNOX 容器之前，用户必须接受三星的最终用户授权许可协议的条款。

安装 KNOX 容器后，将向移动设备的桌面添加 KNOX 图标  。或者将向移动设备上的应用列表中添加工作区。若要使用公司数据，用户需要从 KNOX 容器启动应用。

Kaspersky Endpoint Security for Android 不会安装到 KNOX 容器中，也不会保护公司数据。Kaspersky Endpoint Security for Android 不检测恶意文件的下载，也不在 KNOX 容器中阻止恶意网站。您无法在 KNOX 容器中控制应用启动或禁止使用摄像头。Kaspersky Endpoint Security for Android 仅保护私人数据。您可以使用三星 KNOX 工具保护公司数据。有关 Samsung KNOX 的更多详细信息，请访问*三星技术支持网站*。

激活 Samsung KNOX

若要在用户的移动设备上使用 KNOX 容器，您必须激活 Samsung KNOX。Samsung KNOX 的激活过程取决于用户设备上安装的 Kaspersky Endpoint Security for Android 版本：

- 如果设备上安装了当前版本的 Kaspersky Endpoint Security for Android，则无需任何密钥即可激活 Samsung KNOX。
- 如果设备上安装了旧版本的 Kaspersky Endpoint Security for Android（10.8.3.174 或更早版本），则需要从三星获取 KNOX License Manager 密钥（以下简称为 KLM 密钥）。*KNOX License Manager 密钥*是由 Samsung KNOX 授权许可系统使用的唯一代码。有关 KLM 密钥的详细信息，请访问 Samsung KNOX 技术支持网站。

KNOX 容器只能在三星设备上使用。

若要激活 Samsung KNOX，请执行以下操作：

1. 在控制台树的“**受管设备**”文件夹中，选择 Android 设备所属的管理组。
2. 在所选组的工作区中，选择“**策略**”选项卡。
3. 通过双击任意列打开策略属性窗口。
4. 在策略“**属性**”窗口中选择“**管理三星 KNOX**”→“**KNOX 容器**”区域。
5. 在“**KNOX License Manager 密钥**”字段中，指定以下内容：

- 如果设备上安装了当前版本的 Kaspersky Endpoint Security for Android，则输入任意字符。
- 如果设备上安装了旧版本的 Kaspersky Endpoint Security for Android（10.8.3.174 或更早版本），则输入三星提供的 KLM 密钥。

6. 将“锁定”属性设置在锁定位置。
7. 单击“**应用**”按钮以保存所作的更改。

Samsung KNOX 将在下一次与 Kaspersky Security Center 同步后激活。系统将提示用户接受三星的最终用户授权许可协议条款并安装 KNOX 容器。

若要停用 Samsung KNOX，请执行以下操作：

1. 在控制台树的“**受管设备**”文件夹中，选择 Android 设备所属的管理组。
2. 在所选组的工作区中，选择“**策略**”选项卡。
3. 通过双击任意列打开策略属性窗口。
4. 在策略“**属性**”窗口中选择“**管理三星 KNOX**”→“**KNOX 容器**”区域。
5. 清除“**KNOX License Manager 密钥**”字段值。
6. 单击“**应用**”按钮以保存所作的更改。

Samsung KNOX 将在下一次与 Kaspersky Security Center 进行设备同步后停用。将阻止对 KNOX 容器的访问。

三星 KNOX 限制

- KNOX 容器只能在三星设备上使用。
- 在支持 KNOX 2.6、2.7 和 2.7.1 的三星设备上，Web 保护和应用程序控制在 KNOX 容器中不起作用。该问题关乎 KNOX 容器中缺少所需权限（可访问功能服务）。在支持 KNOX 2.8 或更高版本的设备上，应用程序的所有组件可以无限制运行。
- 由于三星 KNOX 更新，Kaspersky Endpoint Security for Android Service Pack 4 Maintenance Release 3 Update 2 以前的版本在三星安卓 10 设备上可能工作不稳定。建议将 Kaspersky Endpoint Security for Android 更新到 Service Pack 4 Maintenance Release 3 Update 2 版本。

在 KNOX 中配置防火墙

您应配置防火墙设置以监视 KNOX 容器中的网络连接。

若要在 KNOX 容器中配置防火墙，请执行以下操作：

1. 在控制台树的“**受管设备**”文件夹中，选择 Android 设备所属的管理组。
2. 在所选组的工作区中，选择“**策略**”选项卡。
3. 通过双击任意列打开策略属性窗口。

4. 在策略“**属性**”窗口中选择“**管理三星 KNOX**”→“**KNOX 容器**”区域。

5. 在“**防火墙**”窗口中，单击“**配置**”。
   “**防火墙**”窗口将打开。

6. 选择防火墙设置：

   - 若要允许所有入站和出站连接，请将滑块移动到“**全部允许**”。
   - 若要阻止除排除列表中的应用程序的网络活动以外的所有网络活动，请将滑块向上滑动到“**全部阻止(排除项除外)**”。

7. 如果您已将防火墙模式设置为“**全部阻止(排除项除外)**”，请创建排除列表：

   a. 单击“**添加**”。
      这将打开“**防火墙排除项**”窗口。

   b. 在“**应用程序名称**”字段中输入移动应用程序的名称。

   c. 在“**包名称**”字段中输入移动应用程序包的系统名称（例如 `com.mobileapp.example`）。

   d. 单击“**确定**”。

8. 单击“**应用**”按钮以保存所作的更改。

与 Kaspersky Security Center 的下次设备同步之后可配置移动设备设置。

在 KNOX 中配置 Exchange 邮箱

若要在 KNOX 容器中使用公司邮件、联系人和日历，应配置 Exchange 邮箱设置。

若要在 KNOX 容器中配置 Exchange 邮箱，请执行以下操作：

1. 在控制台树的“**受管设备**”文件夹中，选择 Android 设备所属的管理组。

2. 在所选组的工作区中，选择“**策略**”选项卡。

3. 通过双击任意列打开策略属性窗口。

4. 在策略“**属性**”窗口中选择“**管理三星 KNOX**”→“**KNOX 容器**”区域。

5. 在“**Exchange ActiveSync**”区域中，单击“**配置**”按钮。
   “**Exchange 邮件服务器设置**”窗口将打开。

6. 在“**服务器地址**”字段中，输入托管邮件服务器的服务器的 IP 地址或 DNS 名称。

7. 在“**域**”字段中，输入公司网络上的移动设备用户的域名。

8. 在“**同步间隔**”下拉列表中，选择移动设备与 Microsoft Exchange 服务器所需的同步时间间隔。

9. 若要使用 SSL（安全套接字层）数据传输协议，请选择“**使用 SSL 连接**”选框。

10. 若要使用数字证书保护移动设备与 Microsoft Exchange 服务器之间的数据传输，请选择**“验证服务器证书”**选框。

11. 单击**“应用”**按钮以保存所作的更改。

与 Kaspersky Security Center 的下次设备同步之后可配置移动设备设置。

附录

本节提供补充文档内容的信息。

配置组策略的权限

Kaspersky Security Center 管理员可以根据管理控制台用户的工作职责，配置该用户访问不同应用程序功能的权限。

对于每个功能方面，管理员可以分配以下权限：

- **允许编辑**。允许管理控制台用户在属性窗口中更改策略设置。
- **阻止编辑**。禁止管理控制台用户在属性窗口中更改策略设置。属于该权限分配至的功能范围的策略标记不会显示在界面中。

访问 Kaspersky Endpoint Security 管理插件的权限

功能范围	策略区域
安卓企业	安卓工作配置文件
反盗窃	反盗窃
应用程序控制	应用程序控制
保护	保护，扫描，更新
合规性控制	合规性控制
容器	容器
设备设置	设备控制，同步
管理三星设备	APN、管理三星设备、KNOX 容器
系统管理	高级，Wi-Fi
Web 保护	Web 保护

访问 Kaspersky Device Management for iOS 管理插件各部分的权限

功能范围	策略区域
其他	网络收藏夹，字体，AirPlay，AirPrint
Exchange ActiveSync	常规，密码，同步，功能限制，应用程序限制
常规	常规，单点登录，上网保护，Wi-Fi，访问点名称 (APN)，Exchange ActiveSync，电子邮件，自定义有效载荷
LDAP（日历/联	LDAP，日历，联系人，日历订阅

系人）	
限制和安全	功能限制，应用程序限制，对媒体内容的限制，密码，VPN，全局 HTTP 代理，证书，SCEP

应用程序类别

应用程序控制支持应用程序类别。为应用程序类别配置的运行模式将应用至该类别中的所有应用程序。每个应用程序的类别由 Kaspersky Security Network 云服务进行确定。

应用程序类别

类别	描述
娱乐	互动娱乐应用程序。
IM 客户端，移动消息发送应用程序	通过 IP 的即时消息，语音和视频通讯应用程序。
社交网络	使用社交网络和博客的应用程序。
商业软件	税务计算、银行操作管理、表格处理、记账和其他商用应用程序。文本编辑器。
家庭，家人，爱好，健康	菜谱，时尚小贴士应用程序。锻炼，工作外计划、获得节食、健康营养、安全和预防事故的应用程序。
医疗	包括症状和药物类别的应用程序，提供健康护理专家、健康护理杂志和新闻信息的应用程序。
多媒体	提供电影订阅、媒体模仿其和视频播放器的服务。音乐服务，播放器，广播。
图形设计软件	使用摄像头、图形编辑器的应用程序，用于管理和发布照片的应用程序。
阅读新闻和 RSS 的插件	用于阅读报纸、杂志、博客、新闻聚合的应用程序。
天气	显示天气预报的应用程序。
教育应用程序	阅读器，手册，课本，字典，索银典，百科全书。有助于考试、培训材料、字典、智力开发游戏、语言学习工具的应用程序。
在线购物	用于在线购物和竞价，礼品券，比价工具的应用程序，购物单应用程序，用于阅读产品反馈的应用程序。
启动实用程序	用于重新设计桌面。小程序，快捷方式的应用程序。
操作系统和实用程序	提供操作系统管理、用户互动和内存管理的系统应用程序。
地图查看	城市指南，有关当地商业的信息，旅行规划工具。
其他应用程序	软件库，技术演示版应用程序。未包含在任何类别中的应用程序。
运输	使用公共交通、导航工具的应用程序，司机使用的应用程序。
游戏	街机游戏、博彩、赛车、其他、老虎机、棋牌游戏、音乐、桌游、游览、拼图、冒险、RPG、模拟器、单词游戏、体育游戏、战略游戏、动作。
浏览器	用于查看网站的应用程序，网页文档和文件的内容。用于管理网页应用程序的应用程序。
开发工具	用于开发软件的应用程序。调试程序、编译器、代码编辑器、图形用户界面编辑器。
OS 应用程序	与操作系统一起使用的应用程序，操作系统正常运行所需的应用程序。

互联网应用程序	下载管理器、邮件客户端、网页搜索应用程序和其他方便浏览互联网的应用程序。
网络基础结构软件	用于管理公司网络内服务器、数据存储设备、网络设备、软件的应用程序和完整基础结构自动化和集成应用程序。
联网软件	用于组织多个设备上用户组协作，在设备间沟通的应用程序。
系统实用程序	与操作系统一起提供的应用程序：文件管理器、压缩工具、用于软硬件诊断的实用程序、内存优化工具、卸载程序、处理器管理实用程序。
安全软件	设备数据保护应用程序。检测和消除设备上威胁的应用程序。防火墙。数据加密应用程序。
下载管理程序	用于从外部资源下载文件的应用程序。
用于在互联网上存储文件的应用程序	用于管理文件、备注和多媒体的在线存储。
参考系统	阅读器，手册，课本，字典，索银典，维基百科全书。
电子邮件应用程序	用于发送和接收电子邮件消息的应用程序。

使用 Kaspersky Endpoint Security for Android 应用程序

本帮助部分介绍 Kaspersky Endpoint Security for Android 应用用户可使用的功能和操作。

本部分中的文章包含在移动设备上可用或可见的所有选项。应用程序的实际布局和行为取决于实施的远程管理系统以及管理员如何根据公司安全要求配置您的设备。本部分中介绍的某些功能和选项可能不适用于您的实际应用程序体验。如果您对特定设备上的应用程序有任何疑问，请与管理员联系。

程序功能

Kaspersky Endpoint Security 提供了下列主要功能：

防御病毒和其他恶意软件

该应用程序使用反病毒组件保护设备，防御病毒和其他恶意软件。

反病毒可执行以下功能：

- 扫描整个设备、已安装的应用程序或者选定的文件夹以查找威胁
- 实时保护您的设备
- 在已安装的应用程序第一次启动之前扫描它们
- 更新反病毒数据库

如果在移动设备上安装的应用程序会收集信息并发送这些信息进行处理，则 Kaspersky Endpoint Security for Android 会将此应用程序归类为恶意软件。

应用程序控制

根据公司安全性要求，*远程管理系统的管理员*（以下简称“管理员”）创建推荐的应用程序列表、阻止的应用程序列表和必需的应用程序列表。应用程序控制组件用于安装推荐的和所需的应用程序，更新它们并且卸载被阻止的应用程序。

利用应用程序控制，您可以通过指向分发包的直接链接或指向 Google Play 的链接，将推荐和必需的应用程序安装到您的设备上。应用程序控制还允许您卸载那些违反公司安全要求的已阻止应用程序。

Kaspersky Endpoint Security 必须以“无障碍功能”服务的形式启用，才能确保“应用程序控制”正常运行。如果未在运行初始化配置向导期间为该应用程序启用此服务,可在 " **状态** " 部分或设备设置（ " **安卓设置** " → " **可访问性** " → " **服务** " ）中选择适当的通知，从而将 Kaspersky Endpoint Security 启用为可访问功能服务。

保护被盗或丢失设备的数据

防盗组件保护您的数据免受未授权的访问，设备丢失或被盗时定位设备。

反盗窃功能可以远程执行以下操作：

- 锁定设备。

  要防止黑客拥有锁定该设备的能力，必须在运行 Android 7.0 或更新版本的移动设备上将 Kaspersky Endpoint Security 启用为可访问功能服务。

- 打开设备的声音警报，即使该设备已禁用声音。
- 获取设备的位置地图坐标。
- 擦除设备上存储的数据。
- 恢复出厂设置。
- 秘密拍摄使用您的设备的人员的面部照片。

要启用反盗窃操作，必须将 Kaspersky Endpoint Security 启用为设备管理员。如果未在运行应用程序初始化配置期间授予设备管理员权限，可在 " **状态** " 部分或设备设置（ " **安卓设置** " → " **安全性** " → " **设备管理员** " ）中选择适当的通知，从而授予 Kaspersky Endpoint Security 管理员权限。

防御在线威胁

上网保护组件保护设备防御在线威胁。

网页保护拦截散布恶意代码的恶意网站和钓鱼网站，这些网站以盗窃个人机密信息和获取财务账号权限为目的。Web 保护将在您打开网站前使用卡巴斯基安全网络云服务扫描网站。

要启用 Web 保护：

- 必须将 Kaspersky Endpoint Security 启用为可访问功能服务。
- 您必须接受关于以使用 Web 保护为目的的数据处理声明 (Web 保护声明)。Kaspersky Endpoint Security 使用卡巴斯基安全网络 (KSN) 扫描网站。Web 保护声明包含与 KSN 交换数据的条款。

  您的管理员可以在 Kaspersky Security Center 为您接受 Web 保护声明。此种情况下，您不必采取任何操作。

  如果您的管理员未接受 Web 保护声明并向您发送了接受请求，您必须在应用设置中阅读并接受 Web 保护声明。

  如果您的管理员未接受 Web 保护声明，Web 保护不可用。

安卓设备上的 Web 保护仅在 Google Chrome 浏览器（包括自定义标签功能）、Huawei Browser 和 Samsung Internet Browser 中可用。如果工作配置文件被使用且 Web 保护仅为工作配置文件所启用，Samsung Internet Browser 中的 Web 保护不阻止移动设备上的网站。

主界面概览

主窗口的界面根据屏幕分辨率不同而轻微变化。

在出现可能会导致保护级别降低、设备感染或信息丢失问题时，主屏幕的外观会发生变化。

"**状态**"区域显示以下信息：

- 您的设备保护方面的问题
- 有关您的设备是否符合公司安全要求的信息
- 有关设备保护状态的信息

您可以轻触 Kaspersky Endpoint Security 主窗口的顶部以打开"**状态**"区域。

设备保护方面的问题

保护问题按类别分组。针对每一个问题，列出解决问题可以采取的行动。

> "**状态**"区域还会显示应用程序检测到的已跳过对象的列表。跳过的威胁列表可能会更改，例如，如果可疑文件被删除或移动。若要接收最新的威胁列表，请运行完整设备扫描。为了确保可靠地保护您的数据，请消除所有检测到的对象。

存在两类保护问题。

- *通知问题*。黄色高亮标记：通知问题告知用户潜在影响设备安全的事件（例如，上次扫描是 14 天前，或未扫描新安装的应用程序）。您可以隐藏通知问题。通过**隐藏问题**菜单可获知相关问题信息。
- *关键问题*。红色高亮标记：关键问题通知告知用户关于影响设备安全的重要事件（例如，长时间未更新反病毒数据库，或者设备上安装了被阻止的应用程序）。关键问题不可隐藏。

合规性控制

应用程序自动检查设备是否符合公司安全性要求。"**状态**"区域还显示有关设备是否符合公司安全性要求的信息。

- 设备不符合公司安全要求的原因（例如，在设备上检测到被阻止的应用程序）。
- 您必须消除不合规问题的时间段（例如，24 小时）。
- 如果您未在规定的时间段内解决不合规问题，将对设备采取的措施（例如，设备将被锁定）。
- 为了解决设备不符合公司安全要求而执行的操作。

状态栏图标

首次安装向导结束后，Kaspersky Endpoint Security 图标会显示在状态栏。

该图标显示应用程序的操作并提供访问 Kaspersky Endpoint Security 的主界面的方法。

该图标表明 Kaspersky Endpoint Security 正在运行，并反映设备的保护状态：

– 设备被保护。

– 保护存在问题（例如：反病毒数据库已过期或尚未扫描新安装的应用程序）。

设备扫描

反病毒有一些限制：

- 当反病毒正在运行时，在设备外部内存（例如 SD 卡）中检测到的威胁无法在工作配置文件中被自动清除（带有手提箱图标的应用程序， 配置安卓工作配置文件）。Kaspersky Endpoint Security for Android 在工作配置文件中不能访问外部内存。关于检测到对象的信息显示在应用的状态区域。要清除在外部内存中检测到的对象，对象文件必须被手动删除且设备扫描必须重启。
- 由于技术限制，Kaspersky Endpoint Security for Android 无法扫描大小为 2 GB 或更大的文件。在扫描期间，应用程序将跳过此类文件，而不会通知您此类文件被跳过。

开始设备扫描的步骤：

1. 在 Kaspersky Endpoint Security 主界面的快速启动窗格中轻触“**扫描**”。
2. 选择设备扫描范围：
   - **扫描整个设备**。应用程序扫描设备的整个文件系统。
   - **扫描已安装的应用程序**。应用程序仅扫描已安装的应用程序。
   - **自定义扫描**。应用程序扫描选定文件夹或单个文件。可选择单个对象（文件夹或文件）或以下设备存储区之一：
     - **设备内存**。整个设备的可读存储区。还包括用于存储操作系统文件的系统存储区。
     - **内部内存**。用于安装应用程序和存储媒体内容、文档和其他文件的设备存储区。
     - **外部内存**。外部 SD 卡存储区。如果未安装外部 SD 卡，则将隐藏此选项。

到病毒扫描设置的访问可能被管理员限制。

要配置病毒扫描：

1. 在 Kaspersky Endpoint Security 主窗口的快速启动面板中，轻触 → **设置** → **反病毒** → **扫描**。
2. 如果您要让应用在执行扫描时检测可以被黑客使用以损坏您的设备或数据的恶意软件和应用，开启**广告软件，拨号软件和其他**按钮。
3. 点击“**检测到威胁时的操作**”，然后选择应用程序默认执行的操作：
   - **隔离**

     应用程序会将存档形式隔离文件，不会对设备造成伤害。隔离区允许您删除或恢复移动至隔离区的文件。
   - **请求操作**

     应用会提示您为检测到的每个对象选择一种操作：跳过、隔离或删除。当检测到多个对象时，您可以对所有对象应用所选操作。
   - **删除**

检测到的对象将被自动删除。不需要附加操作。删除对象之前，Kaspersky Endpoint Security 将显示检测到对象的临时通知。

- **跳过**

  如果检测到的对象被跳过，Kaspersky Endpoint Security 会警告您设备保护方面存在的问题。有关跳过的对象的信息会显示在应用程序的“**状态**”部分中。对于每个跳过的威胁，应用程序都提供您可以执行以消除威胁的操作。跳过的威胁列表可能会更改，例如，如果可疑文件被删除或移动。若要接收最新的威胁列表，请运行完整设备扫描。为了确保可靠地保护您的数据，请消除所有检测到的对象。

有关检测到的威胁以及对它们执行的操作的信息记录在应用程序报告（→ **报告**）中。您可以选择显示反病毒操作报告。

运行计划扫描

反病毒有一些限制：

- 当反病毒正在运行时，在设备外部内存（例如 SD 卡）中检测到的威胁无法在工作配置文件中被自动清除（带有手提箱图标的应用程序， 配置安卓工作配置文件）。Kaspersky Endpoint Security for Android 在工作配置文件中不能访问外部内存。关于检测到对象的信息显示在应用的状态区域。要清除在外部内存中检测到的对象，对象文件必须被手动删除且设备扫描必须重启。

- 由于技术限制，Kaspersky Endpoint Security for Android 无法扫描大小为 2 GB 或更大的文件。在扫描期间，应用程序将跳过此类文件，而不会通知您此类文件被跳过。

要为设备配置全盘扫描计划：

1. 在 Kaspersky Endpoint Security 主窗口的快速启动面板中，轻触 → **设置** → **反病毒** → **扫描**。
2. 轻触“**计划**”，然后选择完整扫描频率：
   - **每周**
   - **每天**
   - **已禁用**
   - **数据库更新之后**
3. 点击“**开始日期**”，然后选择要在一周中的哪一天开始完全扫描。
4. 点击“**开始时间**”，然后选择开始完全扫描的时间。

根据计划启动设备全盘扫描。

在 Android 12 或更高版本上，如果设备处于省电模式，应用程序可能会晚于指定的时间执行此任务。

更改保护模式

实时保护允许您检测正在打开文件中的威胁，并扫描被实时安装到设备的应用。反病毒数据库和卡巴斯基安全网络云服务（云保护）用于自动确保安全。

更改设备保护模式的步骤：

1. 在 Kaspersky Endpoint Security 主窗口的快速启动窗格中，轻触 ☰ →“设置”→“反病毒”→“实时保护模式”。
2. 选择设备保护模式：
   - **禁用**。关闭“保护”功能。
   - **推荐**。反病毒仅扫描从 Downloads 文件夹中安装的应用程序和文件。新应用程序安装完毕后，反病毒会立即对其扫描。
   - **扩展模式**。在对所有设备文件执行任何操作（例如当保存、移动或更改设备文件时），反病扫描这些文件是否存在恶意对象。另外，新应用程序安装完毕时，反病毒也会立即对其扫描。

有关当前保护模式的信息显示在组件描述下方。

到实时保护设置的访问可能被管理员限制。

要启用云保护（KSN）：

1. 在 Kaspersky Endpoint Security 主界面的快速启动窗格中轻触 ☰ →“设置”→“反病毒”。
2. 开启**云保护(KSN)**按钮。

   云保护(KSN)按钮仅为设备的实时保护管理卡巴斯基安全网络的使用。如果清空该选框，Kaspersky Endpoint Security 继续使用 KSN 以方便应用其他组件的操作。

结果，应用获得到关于文件和应用信誉的 Kaspersky 在线知识库的访问。此项扫描旨在扫描威胁信息尚未添加到反病毒数据库但已包含在 KSN 中的威胁。卡巴斯基安全网络云服务提供反病毒的完整操作并降低误报。仅您的管理员可以完全禁用卡巴斯基安全网络的使用。

要配置实时保护：

1. 在 Kaspersky Endpoint Security 主窗口的快速启动窗格中，轻触 ☰ →“设置”→“反病毒”→“实时保护模式”。
2. 如果您要让应用在执行扫描时检测可以被黑客使用以损坏您的设备或数据的恶意软件和应用，开启**广告软件，拨号软件和其他**按钮。
3. 点击“**检测到威胁时的操作**”，然后选择应用程序默认执行的操作：
   - **隔离**

     应用程序会将存档形式隔离文件，不会对设备造成伤害。隔离区允许您删除或恢复移动至隔离区的文件。
   - **删除**

     检测到的对象将被自动删除。不需要附加操作。删除对象之前，Kaspersky Endpoint Security 将显示检测到对象的临时通知。
   - **跳过**

如果检测到的对象被跳过，Kaspersky Endpoint Security 会警告您设备保护方面存在的问题。有关跳过的对象的信息会显示在应用程序的“**状态**”部分中。对于每个跳过的威胁，应用程序都提供您可以执行以消除威胁的操作。跳过的威胁列表可能会更改，例如，如果可疑文件被删除或移动。若要接收最新的威胁列表，请运行完整设备扫描。为了确保可靠地保护您的数据，请消除所有检测到的对象。

有关检测到的威胁以及对它们执行的操作的信息记录在应用程序报告中（ → **设置** → **报告**）。您可以选择显示反病毒操作报告。

反病毒数据库更新

更新应用程序的反病毒数据库的步骤：

在 Kaspersky Endpoint Security 主界面的快速启动面板中，轻触“**数据库更新**”。

计划的数据库更新

应用程序可以根据您指定的计划自动更新反病毒数据库。

配置更新计划的步骤：

1. 在 Kaspersky Endpoint Security 主界面的快速启动面板中，轻触 →“**设置**”→“**反病毒**”→“**数据库更新**”。
2. 点击“**计划**”，然后选择更新频率：
   - **每周**
   - **每天**
   - **已禁用**
3. 点击“**开始日期**”，然后选择要在一周中的哪一天运行更新。
4. 点击“**开始时间**”，然后选择开始更新的时间。

根据计划启动反病毒数据库更新。

在 Android 12 或更高版本上，如果设备处于省电模式，应用程序可能会晚于指定的时间执行此任务。

设备丢失或被盗时如何操作

如果您的设备丢失或被盗，请联系系统管理员。管理员可根据公司安全要求，在您的设备上远程执行防盗保护命令。

如果向设备发送“完全重置”命令，将失去对该设备的控制，并且其余防盗窃命令将失效。

Web 保护

要启用 Web 保护：

- 必须将 Kaspersky Endpoint Security 启用为可访问功能服务。
- 您必须接受关于以使用 Web 保护为目的的数据处理声明 (Web 保护声明)。Kaspersky Endpoint Security 使用卡巴斯基安全网络 (KSN) 扫描网站。Web 保护声明包含与 KSN 交换数据的条款。

  您的管理员可以在 Kaspersky Security Center 为您接受 Web 保护声明。此种情况下，您不必采取任何操作。

  如果您的管理员未接受 Web 保护声明并向您发送了接受请求，您必须在应用设置中阅读并接受 Web 保护声明。

  如果您的管理员未接受 Web 保护声明，Web 保护不可用。

安卓设备上的 Web 保护仅在 Google Chrome 浏览器（包括自定义标签功能）、Huawei Browser 和 Samsung Internet Browser 中可用。如果工作配置文件被使用且 Web 保护仅为工作配置文件所启用，Samsung Internet Browser 中的 Web 保护不阻止移动设备上的网站。

若要在浏览网络时始终使用 Web 保护，请将 Google Chrome 或 Samsung Internet Browser 设为默认浏览器。

要将支持的浏览器设为默认浏览器并在浏览网页时始终使用网页保护：

1. 在 Kaspersky Endpoint Security 主界面的快速启动窗格中轻触 ☰ →“**设置**”→“**Web 保护**”。
2. 将“**Web 保护**”切换按钮切换到“开”。
3. 轻触“**设置默认浏览器**”。

   启用 Web 保护且未将支持的浏览器设为默认浏览器时显示此按钮。

   默认浏览器选择向导启动。
4. 按照向导指示执行操作。

向导可将 Google Chrome、Huawei Browser 或 Samsung Internet Browser 设为默认浏览器。在您浏览网页时，“Web 保护”功能将会持续扫描网站。

应用程序控制

*应用程序控制*会检查移动设备上安装的应用程序是否符合公司安全要求。在 Kaspersky Security Center，管理员根据公司安全要求创建允许、阻止、强制和推荐的应用程序的列表。作为应用程序控制的结果，Kaspersky Endpoint Security 会提示您安装必需和推荐的应用程序以及删除被阻止的应用程序。您无法在移动设备上启动被阻止的应用程序。

要安装必需和推荐的应用程序，或要删除阻止的应用程序：

1. 转到 Kaspersky Endpoint Security“**状态**”区域。
2. 选择应用程序控制任务。
3. 执行推荐的操作。

获取证书

获取用于访问公司网络资源的证书的步骤：

1. 在 Kaspersky Endpoint Security 主窗口的快速启动窗格中，轻触 →“**设置**”→“**其他**”→“**获取证书**”。
2. 指定您的公司网络帐号凭据。
3. 如果您从管理员处接收到了一次性密码，请选择“**一次性密码**”选框，然后输入您收到的密码。
   将启动证书安装向导。
4. 按照向导指示执行操作。

与 Kaspersky Security Center 同步

要依照公司安全要求来保护和配置您的设备，需要将移动设备与 Kaspersky Security Center 远程管理系统进行同步。设备可与 Kaspersky Security Center 自动同步，并且您也可以手动启动同步。第一次同步后，您的设备会添加到通过 Kaspersky Security Center 管理的移动设备列表中。然后，管理员可以依据公司安全要求配置您的设备。

您可以在运行初始配置向导或在 Kaspersky Endpoint Security 的设置中配置同步设置。如果使用 Google Play 安装了 Kaspersky Endpoint Security，必须配置同步设置。向系统管理员请求同步设置值。

仅当管理员要求时，才可以使用 Kaspersky Security Center 远程管理系统修改设备同步设置。

要将您的设备与 Kaspersky Security Center 同步：

1. 在 Kaspersky Endpoint Security 主界面的快速启动窗格中轻触 →“**设置**”→“**同步**”。
2. 在“**同步设置**”区域，指定以下设置的值：
   - **服务器**
   - **端口**
   - **组**
   - **企业电子邮件地址**

   管理员可以隐藏同步设置。
3. 轻触“**同步**”。

不使用 Kaspersky Security Center 激活 Kaspersky Endpoint Security for Android 应用程序

在大多数情况下，您的设备上安装的 Kaspersky Endpoint Security for Android 应用程序由管理员在 Kaspersky Security Center 远程管理系统中集中激活。如果您的设备未连接到 Kaspersky Security Center，您可以手动输入激活码。要获取激活码，请联系管理员。

只有在管理员的指示下，才能手动激活应用程序。

要输入激活码：

1. 在指出您的许可证即将过期或已过期并且您的设备未连接到管理服务器的错误消息中，点击“**激活**”。
2. 在激活窗口中，输入管理员提供的激活码，然后轻触“**激活**”。
3. 如果激活码正确，将显示一条通知，说明该应用程序已激活并显示授权许可到期日期。

您设备上的 Kaspersky Endpoint Security for Android 应用程序已激活。

启用 Android 13 上的辅助功能

在 Android 13 中，对于未从 Google Play 或 Huawei AppGallery 下载的应用程序，辅助功能服务受到限制。如果您从 Kaspersky Security Center 服务器或卡巴斯基网站下载了 Kaspersky Endpoint Security for Android，您应该手动允许辅助功能服务。

辅助功能用于以下目的：

- 在卡巴斯基安全网络中检查网站和应用程序
- 锁定设备以防被盗
- 显示警告
- 受管理员限制时阻止使用摄像头

要针对 Kaspersky Endpoint Security 启用辅助功能：

1. 在设备设置中打开“**辅助功能**”页面，并找到 Kaspersky Endpoint Security。
2. 打开 Kaspersky Endpoint Security 开关。在显示辅助功能服务受限的对话框中，点击“**确定**”。

   现在，您可以授予 Kaspersky Endpoint Security 访问受限设置的权限。
3. 在设备设置中打开 Kaspersky Endpoint Security 信息页面。例如，转到“**设置**”>“**应用程序**”，然后在应用程序列表中找到该应用程序。
4. 在 Kaspersky Endpoint Security 信息页面上，点击右上角的 ⋮，并选择“**允许受限设置**”菜单项。

   Kaspersky Endpoint Security 现在可以访问受限设置。
5. 返回设备设置中的“**辅助功能**”页面，并找到 Kaspersky Endpoint Security。

6. 打开 **Kaspersky Endpoint Security** 开关。在打开的对话框中，允许该应用程序完全控制您的设备。

现在已为 Kaspersky Endpoint Security 启用辅助功能服务。

要针对 Kaspersky Endpoint Security 启用辅助功能：

1. 在要求您打开辅助功能服务的对话框中，点击“**打开**”。
   将在设备设置中打开“**辅助功能**”页面。
2. 打开 Kaspersky Endpoint Security 开关。在显示辅助功能服务受限的对话框中，点击“**确定**”。
   现在，您可以授予 Kaspersky Endpoint Security 访问受限设置的权限。
3. 在设备设置中打开 Kaspersky Endpoint Security 信息页面。例如，转到“**设置**”>“**应用程序**”，然后在应用程序列表中找到该应用程序。
4. 在 Kaspersky Endpoint Security 信息页面上，点击右上角的 ⋮，并选择“**允许受限设置**”菜单项。
   Kaspersky Endpoint Security 现在可以访问受限设置。
5. 返回应用程序，在要求您打开辅助功能服务的对话框中，点击“**打开**”。
   将在设备设置中打开“**辅助功能**”页面。
6. 打开 **Kaspersky Endpoint Security** 开关。在打开的对话框中，允许该应用程序完全控制您的设备。

现在已为 Kaspersky Endpoint Security 启用辅助功能服务。

更新应用程序

Kaspersky Endpoint Security 可通过下列方式更新：

- 使用 Google Play 手动更新。您可以从 Google Play 中下载应用程序的新版本，然后在您的设备部中进行安装。
- 在管理员的帮助下更新。管理员可以使用 Kaspersky Security Center 远程管理系统来远程更新您设备上的应用程序版本。

从 Google Play 更新应用程序

管理员可以阻止您从 Google Play 更新应用程序。

通过执行 Android 平台的标准更新步骤，您可以从 Google Play 更新本应用程序。要更新应用程序，必须满足下列条件：

- 您必须拥有 Google 账户。
- 设备必须已链接至您的 Google 账户。
- 设备必须连接到互联网。

要详细了解如何创建 Google 账户、如何将设备链接至账户，以及如何操作 Google Play Store，请参阅 Google 的支持网站。

通过 Kaspersky Security Center 更新应用程序

通过 Kaspersky Security Center 更新应用程序包含以下步骤：

1. 管理员向您的移动设备发送其版本符合公司安全要求的应用程序分发包。
   将显示在您的设备上安装 Kaspersky Endpoint Security 的提示。
2. 接受更新条款和条件。
   新版本的应用程序将安装到您的设备。该应用程序更新后不需要其他配置。

卸载应用程序

管理员可以阻止您自行删除应用程序。在这种情况下，您不能删除 Kaspersky Endpoint Security。

Kaspersky Endpoint Security 可通过下列方法删除：

- 在应用程序设置中手动删除。
- 在设备设置中手动删除。
- 在管理员的帮助下更新。管理员可以使用 Kaspersky Security Center 远程管理系统来远程删除您设备上的应用程序。

在应用程序设置中删除

从设备删除 Kaspersky Endpoint Security 的步骤：

1. 在 Kaspersky Endpoint Security 主窗口的快速启动面板中，轻触 → **"卸载应用程序"**。
   这将启动应用程序删除向导。
2. 按照向导指示执行操作。

在设备设置中删除

可通过执行 Android 平台的标准程序来删除应用程序。要删除应用程序，必须在设备安全性设置中禁用 Kaspersky Endpoint Security 管理员权限。

在运行 Android 7.0 或更新版本的设备上，如果管理员已阻止删除，那么，试图删除安卓设置中的应用程序时，该设备将被锁定。要解锁该设备，请联系您的管理员。

通过 Kaspersky Security Center 删除

使用 Kaspersky Security Center 删除应用程序包含以下步骤：

1. 管理员将应用程序删除命令发送到您的移动设备。

您的移动设备会显示一条确认删除 Kaspersky Endpoint Security 的提示。

2. 确认应用程序删除。

该应用程序将从您的设备上删除。

带有手提箱图标的应用程序

安卓工作配置文件中的应用程序图标

带有手提箱图标的应用程序（公司应用程序）存放于您设备上的安卓工作配置文件（下称"工作配置文件"）中。*安卓工作配置文件*是您设备上的安全环境，在该环境中，管理员可以管理应用程序和账户，而不限制您处理个人数据的能力。

您可以使用工作配置文件将公司数据与个人数据分开存放。这样可使公司数据保持机密状态，免遭恶意软件的攻击。当您设备上创建了工作配置文件后，下列公司应用将自动安装在工作配置文件中：Google Play Market、Google Chrome、Downloads、Kaspersky Endpoint Security for Android 等等。

KNOX 应用程序

KNOX 图标

KNOX 应用程序会在您的设备上打开一个 KNOX 容器。*KNOX 容器*是您设备上的一个安全环境，具有自己的桌面、启动面板、应用程序和小部件。管理员可以在 KNOX 容器中管理应用程序和账户，而不会限制您处理个人数据的能力。

您可以使用 KNOX 容器将公司数据与个人数据分开存放。这样可使公司数据保持机密状态，免遭恶意软件的攻击。

在 KNOX 容器中，您可以访问公司邮箱、企业员工的联系信息、文件存储和其他应用程序。

有关使用 KNOX 的更多详细信息，请访问*三星技术支持网站*。

使用 Kaspersky Security for iOS 应用程序

本帮助部分介绍 Kaspersky Security for iOS 应用用户可使用的功能和操作。

本部分中的文章包含在移动设备上可用或可见的所有选项。应用程序的实际布局和行为取决于实施的远程管理系统以及管理员如何根据公司安全要求配置您的设备。本部分中介绍的某些功能和选项可能不适用于您的实际应用程序体验。如果您对特定设备上的应用程序有任何疑问，请与管理员联系。

程序功能

Kaspersky Security for iOS 提供了下列主要功能：

防御在线威胁

Web 保护组件提供针对在线威胁的保护。

Web 保护拦截散布恶意代码的恶意网站和钓鱼网站，这些网站以盗窃个人机密信息和获取财务账号权限为目的。Web 保护将在您打开网站前使用卡巴斯基安全网络云服务扫描网站。Web 保护还会检查您的设备上的应用的在线活动。

要使 Web 保护正常运行，必须允许应用添加 VPN 配置。

越狱检测

当 Kaspersky Security for iOS 检测到越狱时，会显示一条重要消息并通知您的管理员该问题。

该应用无法保证您的设备的安全，因为越狱会绕过安全功能并造成很多问题，包括：

- 安全漏洞
- 稳定性问题
- Apple 服务中断
- 潜在的崩溃和冻结
- 电池寿命缩短
- 无法应用 iOS 更新

安装应用程序

要安装 Kaspersky Security for iOS 应用，请执行以下操作：

1. 找到包含管理员邀请从 App Store 安装 Kaspersky Security for iOS 应用的电子邮件消息。

2. 使用以下方法之一转到 Apple Store：

   - 如果您在想安装该应用的 iOS 设备上读到该消息，轻触消息中的链接。
   - 如果您在一台计算机上读到该消息，则使用您想安装该应用的 iOS 设备扫描二维码。

   邀请链接有效期为 24 个小时。如果您无法即时安装应用，请联系管理员获取新的邀请。

3. 按照 iOS 平台上的标准安装程序操作，从 App Store 下载该应用并安装。

Kaspersky Security for iOS 应用已安装在您的设备上。要保护设备，请激活该应用。

激活应用

要激活 Kaspersky Security for iOS 应用，请执行以下操作：

1. 在您的设备上启动应用。
2. 选中**最终用户授权许可协议**和**产品和服务隐私策略**复选框，接受协议和声明。

   或者，接受**卡巴斯基安全网络声明**，以允许将统计数据发送至卡巴斯基安全网络。这样可以提高该应用的性能并确保其运行不中断。
3. 点击**下一步**。该应用将连接到 Kaspersky Security Center 远程管理系统并获得授权许可信息。
4. 允许应用添加 VPN 配置。该应用使用 VPN 配置来检查网站是否存在网络钓鱼，并保护您的设备免受 Web 威胁的侵害。
5. 允许该应用发送推送通知。该应用采用通知来告诉您有关安全问题和您的授权许可状态的信息。

您设备上的 Kaspersky Security for iOS 应用已激活。

使用激活码激活应用

在您的设备上安装 Kaspersky Security for iOS 应用时，该应用会连接到 Kaspersky Security Center 远程管理系统，并自动获得授权许可信息。如果您的设备未连接到 Kaspersky Security Center，您可以手动输入激活码。要获取激活码，请联系管理员。

只有在管理员的指示下，才能手动激活应用程序。

要输入激活码：

1. 在表明该应用尚未激活的消息中，轻触**激活应用程序**。
2. 在激活窗口中，输入管理员提供的激活码，然后轻触**激活**。

   如果激活码正确，将显示一条通知，说明该应用程序已激活并显示授权许可到期日期。

您设备上的 Kaspersky Security for iOS 应用已激活。

主界面概览

主窗口的界面根据屏幕分辨率不同而轻微变化。

主窗口会显示：

- 您的设备的整体保护状态。
- 指示应用组件状态和保护问题的消息。

消息分三种类型：

- 绿色高亮显示。此为状态消息，通知您保护在指定区域内有效。
- 黄色高亮显示。此为通知消息，通知您可能会影响设备安全性的事件。
- 红色高亮显示。此为重要消息，通知您对设备安全性至关重要的事件。

轻触消息可查看详细信息。

更新应用程序

您可以从 App Store 下载最新版本的 Kaspersky Security for iOS 应用，并按照 iOS 平台上的标准更新程序将其安装到您的设备上。您也可以开启自动更新。该应用更新后不需要任何其他配置。

要更新应用程序，必须满足下列条件：

- 必须拥有 Apple ID。
- 设备必须与您的 Apple ID 关联。
- 设备必须连接到互联网。

要了解有关创建 Apple ID、将您的设备与 Apple ID 关联或使用 App Store 的更多信息，请参阅 Apple 支持网站。

卸载应用程序

要卸载 Kaspersky Security for iOS 应用，请按 iOS 平台上的标准程序操作：

1. 在主屏幕上，轻触并按住该应用程序图标。
2. 卸载应用。

Kaspersky Security for iOS 应用已从您的设备卸载。

程序授权许可

本节提供与 Kaspersky Security for Mobile 授权许可有关的一般性条款的信息。

关于最终用户许可协议

最终用户授权许可协议 (EULA) 是您和 AO Kaspersky Lab 之间的合作协议，其中规定了您使用 Kaspersky Security for Mobile 应遵守的条款和条件。

我们建议您仔细阅读 EULA 的条款和条件，然后再开始使用 Kaspersky Security for Mobile。

您可以通过以下方式查看 EULA 的条款和条件：

- Kaspersky Security for Mobile 组件安装期间。
- 阅读用于安装 Kaspersky Endpoint Security for Android 应用程序的分发包的自解压压缩文件中包含的 license.txt 文件。
- 在 Kaspersky Endpoint Security for Android 的**"关于应用程序"**区域中。
- 在 Kaspersky Security for iOS 的**"关于本应用程序"→"协议和声明"**区域中。
- 在管理服务器属性中的**"高级"→"已接受的授权许可协议"**区域中。此功能在 Kaspersky Security Center 12.1 及更高版本中提供。

安装 Kaspersky Security for Mobile 组件时确认同意最终用户授权许可协议 (EULA)，即表示您接受最终用户授权许可协议的条款和条件。若不接受最终用户授权许可协议的条款，则必须取消安装 Kaspersky Security for Mobile 组件并停止使用。

关于授权许可

*授权许可*是指根据最终用户授权许可协议的条款，提供给您的在有限时间内使用 Kaspersky Security for Mobile 集成解决方案的权限。

当前授权许可可使您享受以下各种服务：

- 依照最终用户许可协议的条款在移动设备上使用应用程序。
- 获得技术支持。

可用服务的范围和程序使用条款取决于用于激活该程序的授权许可的类型。

我们提供下列授权许可类型：

- *试用版*。

  用于试用 Kaspersky Security for Mobile 的免费授权许可。

  试用版授权许可的有效期为 30 天。试用版授权许可到期后，Kaspersky Endpoint Security for Android 移动应用程序和 Kaspersky Security for iOS 移动应用程序会停止执行大多数功能，与管理服务器同步除外。若要继续使用该应用程序，您必须购买商业授权许可。

- *商业版*。

  购买 Kaspersky Security for Mobile 时提供的授权许可。

  在商业授权许可到期后，移动应用程序会继续工作，但功能受到限制。

  在受限功能模式下，以下组件可用，具体取决于应用程序。

  - Kaspersky Endpoint Security for Android 应用程序：
    - **反病毒**。可对设备进行实时保护和病毒扫描，但不能更新反病毒数据库。
    - **反盗窃**。只能向移动设备发送命令。
    - **与管理服务器同步**。

    如果卡巴斯基密钥被阻止、试用授权许可过期或缺少授权许可（激活码被从组策略中删除），Kaspersky Endpoint Security for Android 将停止与卡巴斯基安全网络、Google Analytics for Firebase、SafetyNet Attestation、Firebase Performance Monitoring 和 Crashlytics 交换信息。

  - Kaspersky Security for iOS 应用程序：
    - **与管理服务器同步**。

    如果试用版授权许可过期或授权许可丢失（激活码从组策略中删除），Kaspersky Security for iOS 将停止与卡巴斯基安全网络交换信息。

  该移动应用程序的其余组件对设备用户不可用。管理员可使用组策略在受限功能模式下管理这些组件。您不能使用组策略配置应用程序的其他组件。

  若要继续在全功能模式下使用该应用程序，必须对商业授权许可进行续费。我们建议在当前授权许可过期之前进行续费或购买新的授权许可，以确保计算机得到最大限度保护并能防御所有安全威胁。

关于订阅

*Kaspersky Security for Mobile 订阅*是根据订阅到期日期、受保护的移动设备数量等选定的参数使用移动应用程序的订购方式。可以通过 ISP 等服务提供商订阅 Kaspersky Security for Mobile。可以手动或自动续订订阅，也可以取消订阅。您可以在服务提供商的网站上管理您的订阅。

订阅可以是有限的（例如一年）或是无限的（无到期日）。要在有限订阅到期后继续使用 Kaspersky Security for Mobile，必须续订订阅。无限订阅则自动续订更新，及时预付费给服务提供商。

如果订阅受限，当订阅过期时，会向您提供一个订阅续费宽限期，在此期间应用程序将保留其功能。此类宽限期的可用性和持续时间由服务提供商自行决定。

要在订阅下使用 Kaspersky Security for Mobile，必须使用从服务提供商处接收到的激活码进行激活。应用激活码后，即会安装与授权许可相对应的密钥，从而可在订阅状态下使用应用程序。

可用的订阅管理选项可能各异，具体取决于服务提供商。服务提供商可能不提供订阅续费宽限期，在此期间应用程序将保留其功能。

根据订阅购买的激活码不能用于激活早期版本的 Kaspersky Security for Mobile。

关于密钥

*密钥*是一串位数据，您可以用其激活集成解决方案 Kaspersky Security for Mobile 并在随后依照最终用户授权许可协议的条款使用该解决方案。密钥是由 Kaspersky 专家生成的。

使用密钥文件或激活码即可添加移动应用程序密钥。

- 如果您的组织已部署 Kaspersky Security Center 软件套件，您必须应用密钥文件并将其分发给 Android 移动应用程序。密钥以唯一字母数字序列的形式显示在 Kaspersky Security Center 界面和 Android 移动应用程序界面中。

  添加密钥后，可以用其他密钥来替换。

  > 您不能使用密钥文件激活 Kaspersky Security for iOS 应用程序。

- 如果您的组织不使用 Kaspersky Security Center，您必须与用户共享激活码。用户在 Android 或 iOS 移动应用程序中输入此激活码。密钥在移动应用程序界面中显示为唯一的字母数字序列。

Kaspersky 可能会冻结密钥，例如，当最终用户授权许可协议的条款被违反时。如果密钥被阻止，除与管理服务器同步外，移动应用程序会停止执行其所有功能。要继续使用该应用程序，您需要添加不同的密钥。

关于激活码

*激活码*是由 20 个字母数字字符组成的唯一序列。您输入激活码添加一个用于激活 Kaspersky Endpoint Security for Android 移动应用程序或 Kaspersky Security for iOS 移动应用程序的密钥。在购买集成解决方案 Kaspersky Security for Mobile 或订购 Kaspersky Security for Mobile 试用版本时指定邮件地址，并通过此地址接收激活码。

要使用激活码激活移动应用程序，您需要互联网访问权限以连接到 Kaspersky 激活服务器。

激活应用程序后，激活码即使丢失，也是可以找回的。您可能需要使用激活码，例如在 Kaspersky CompanyAccount 中进行注册。若要恢复激活码，请联系 Kaspersky 技术支持。

关于密钥文件

*密钥文件*是 Kaspersky 提供的带 .key 扩展名的文件。密钥文件的用途是添加用于激活 Kaspersky Endpoint Security for Android 应用程序的密钥。

> 您不能使用密钥文件激活 Kaspersky Security for iOS 应用程序。

您将在您购买 Kaspersky Security for Mobile 集成解决方案或订购 Kaspersky Security for Mobile 试用版后指定的电子邮件地址收到密钥文件。

您无需连接到 Kaspersky 激活服务器，即可使用密钥文件激活应用程序。

密钥文件如果遭意外删除，是可以恢复的。例如，您可能需要密钥文件来注册 Kaspersky CompanyAccount。

要恢复密钥文件，请执行以下操作之一：

- 联系授权许可销售者。
- 使用可用的激活码通过 Kaspersky 网站接收密钥文件。

Kaspersky Endpoint Security for Android 中的数据提供

Kaspersky Security for Mobile 符合通用数据保护条例 (GDPR)。

要安装应用程序，您或设备用户必须阅读并接受最终用户授权许可协议的条款。此外，您还将配置全局接受下列声明的策略，适用于所有用户。否则，应用程序主屏幕上将显示一条通知，提示用户接受以下关于处理用户个人数据的声明：

- 卡巴斯基安全网络声明
- 有关用于 Web 保护的数据处理声明
- 有关将数据处理用于市场营销的声明

如果您选择全局接受声明，则通过 Kaspersky Security Center 接受的声明版本必须与用户已经接受的版本相匹配。否则，用户将被告知有问题，并被提示接受与管理员全局接受的版本相匹配的声明版本。Kaspersky Security for Mobile (Devices) 插件中的设备状态也将更改为“*警告*”。

用户可以随时在 Kaspersky Endpoint Security for Android 的“**关于应用程序**”区域中接受或拒绝声明的条款。

与卡巴斯基安全网络交换信息

为改进实时保护功能，Kaspersky Endpoint Security for Android 将使用卡巴斯基安全网络云服务来运行以下组件：

- 反病毒。应用获得到关于文件和应用信誉的 Kaspersky 在线知识库的访问。此项扫描旨在扫描威胁信息尚未添加到反病毒数据库但已包含在 KSN 中的威胁。卡巴斯基安全网络云服务提供反病毒的完整操作并降低误报的可能性。
- Web 保护。在打开网站之前，该应用程序使用从 KSN 接收的数据来扫描网站。该应用程序会根据允许和阻止的类别（例如，“互联网通信”类别）列表来确定网站类别，以控制用户的互联网访问权限。
- 应用程序控制。该应用程序会根据允许和阻止的类别（例如，“游戏”类别）列表来确定应用程序类别，以限制不符合公司安全要求的应用程序启动。

最终用户授权许可协议中提供了有关在运行反病毒和应用程序控制的过程中使用 KSN 时提交到 Kaspersky 的数据类型的信息。接受授权许可协议的条款和条件即表明您同意传输此信息。

关于 Web 保护的数据处理的声明中提供了有关在运行 Web 保护的过程中使用 KSN 时提交到 Kaspersky 的数据类型的信息。接受声明的条款和条件即表明您同意传输此信息。

如果卡巴斯基安全网络声明中规定了在运行 Kaspersky Endpoint Security for Android 移动应用程序的过程中使用 KSN，则会将有关统计数据类型的信息提交到 Kaspersky。接受声明的条款和条件即表明您同意传输此信息。

在最终用户授权许可协议下的数据提供

如果使用激活码来激活本软件，为了验证本软件的合法用途，最终用户同意定期向权利持有人提供以下信息：

- 向权利持有人基础设施发出的请求中的数据格式 已访问的 Web 服务的 IPv4 地址； 向权利持有人基础设施发出的请求的内容大小； 协议 ID； 软件激活码； 数据压缩类型； 软件 ID； 可在用户设备上激活的软件 ID 集； 软件本地化版本； 软件的完整版本； 唯一的设备 ID； 用户设备上的日期和时间； 软件安装 ID (PCID)； 操作系统版本、操作系统构建号、操作系统更新号、操作系统发行版本、有关操作系统发行版本的扩展信息； 设备型号 操作系统系列； 向权利持有人基础设施发出的请求中的数据格式 所处理对象的校验码类型； 软件许可证标题； 区域激活中心的 ID； 软件许可证密钥的创建日期和时间； 软件授权许可 ID； 用于提供软件授权许可的信息模型的 ID； 软件许可证的过期日期和时间； 软件许可证密钥的当前状态； 所使用的软件许可证类型； 用于激活本软件的许可证的类型； 通过授权许可得出的软件 ID

为了保护本计算机免遭信息安全威胁入侵,最终用户同意定期向权利持有人提供以下信息:

- 所处理对象的校验码类型； 所处理对象的校验和； 软件组件 ID；

- 软件防病毒数据库中的触发记录 ID； 软件防病毒数据库中的触发记录时间戳； 软件防病毒数据库中的触发记录类型； 检测到的可用于损坏用户设备或数据的恶意软件或合法软件的名称；

- 从中安装应用程序的软件商店名称； 应用程序包名称； 用于签署 APK 文件的公钥； 用于签署 APK 文件的证书的校验和； 数字证书时间戳；

- 软件的完整版本； 软件更新 ID； 已安装软件的类型； 配置标识符； 软件操作的结果 错误代码；

- 根据特定数学规则从 Android 应用程序 APK 文件导出，并且不允许恢复原始文件内容的数字； 此数据不包含文件名、文件路径、地址、电话号码或用户的其他个人信息。

如果您使用权利持有人的更新服务器下载更新，最终用户为了提高更新程序的效率，同意定期向权利持有人提供以下信息：

- 通过授权许可得出的软件 ID； 软件的完整版本； 软件授权许可 ID； 所使用的软件许可证类型； 软件安装 ID (PCID)； 软件更新启动 ID； 正在处理的网址。

权利持有人也可以使用此类信息接收关于软件的分发和使用的统计信息。

Kaspersky 根据相关法律要求保护所接收的信息。原始接收的信息以加密形式存储，并且随着信息的累积而销毁（每年两次）或按用户请求销毁。程序将无限期地存储常规统计信息。

在卡巴斯基安全网络声明下的数据提供

使用 KSN 可提高软件所提供保护的有效性，防范信息和网络安全威胁。

如果使用 5 个或更多节点的授权许可，在使用 KSN 的过程中，权利持有人将自动接收并处理以下数据。

- 软件防病毒数据库中的触发记录 ID； 软件防病毒数据库中的触发记录时间戳； 软件防病毒数据库中的触发记录类型； 软件数据库的发布日期和时间； 操作系统版本、操作系统构建号、操作系统更新号、操作系统发行版本、有关操作系统发行版本的扩展信息； 操作系统服务包版本； 检测特征； 所处理对象的校验和 (MD5)； 所处理对象的名称； 指示所处理对象是否是 PE 文件的标志； 屏蔽 Web 服务的掩码的校验码 (MD5)； 所处理对象的校验码 (SHA256)； 所处理对象的格式； 对象类型代码； 软件对于所处理对象的决策； 所处理对象的路径； 目录代码； 软件组件的版本； 所发送的统计数据的版本； Web 服务的访问地址（URL、IP）； 用于访问 Web 服务的客户端类型； 已访问的 Web 服务的 IPv4 地址； 已访问的 Web 服务的 IPv6 地址； Web 服务请求的来源网址 (Referer)； 正在处理的网址；

- 有关所扫描对象的信息（AndroidManifest.xml 中的应用程序版本； 软件对应用程序的决定； 用于获取软件对应用程序的决定的方法； 商店安装包名称； AndroidManifest. xml 中的软件包名称（或捆绑名称）； Google SafetyNet 类别； 指示设备上是否启用 SafetyNet 的标志； Google SafetyNet 响应中的 SHA256 值； APK 证书的 APK 签名方案； 已安装的软件的版本代码； 用于对 APK 文件签名的证书的序列号； 正在安装的 APK 文

件的名称； 正在安装的 APK 文件的路径； 用于对 APK 文件签名的证书的颁发者； 用于签署 APK 文件的公钥； 用于签署 APK 文件的证书的校验和； 证书过期的日期和时间； 证书签发的日期和时间； 所发送的统计数据的版本； 用于计算数字证书指纹的算法； 已安装的 APK 文件的 MD5 哈希； APK 文件内的 DEX 文件的 MD5 哈希； 动态授予应用程序的权限； 第三方软件版本； 指示应用程序是否为默认 SMS 通信程序的标志； 指示应用程序是否具有设备管理员权限的标志； 指示应用程序是否在系统目录中的标志； 指示应用程序是否使用辅助功能服务的标志）；

- 有关所有潜在恶意对象和活动的信息（所处理对象的片段内容； 证书过期的日期和时间； 证书签发的日期和时间； 密钥存储库中用于加密的密钥的 ID； 用于与 KSN 交换数据的协议； 所处理对象中的片段顺序； 由反病毒软件模块为所处理对象生成的内部日志数据； 证书颁发者名称； 证书的公钥； 用于计算证书公钥的算法； 证书序列号； 对象的签名日期和时间； 证书所有者的名称和设置； 扫描的对象的数字证书指纹和哈希算法； 所处理对象的上次修改日期和时间； 所处理对象的创建日期和时间； 所处理的对象或其组成部分； 对象属性中定义的所处理对象的描述； 所处理对象的格式； 所处理对象的校验码类型； 所处理对象的校验和 (MD5)； 所处理对象的名称； 所处理对象的校验码 (SHA256)； 所处理对象的格式； 软件供应商名称； 软件对于所处理对象的决策； 所处理对象的版本； 为所处理对象做出决策的来源； 所处理对象的校验和； 父应用程序名称； 所处理对象的路径； 有关文件签名检查结果的信息； 登录会话密钥； 登录会话密钥的加密算法； 所处理对象的存储时间； 用于计算数字证书指纹的算法）；

- 构建类型，例如“用户” 或“工程师”； 产品全称； 产品 / 硬件制造商； 是否可以从 Google Play 以外的地方安装应用程序； 用于验证谷歌应用程序的云服务的状态； 用于验证正在通过 ADB 安装的谷歌应用程序的云服务状态； 当前开发代号或 生产构建的“REL”； 递增的构建号； 用户可见的版本字符串； 用户设备名称； 用户可见的软件构建 ID； 固件指纹； 固件 ID； 指示设备是否已获取根权限 (root) 的标志； 操作系统； 软件名称； 所使用的软件许可证类型；

- 有关 KSN 服务质量的信息（用于与 KSN 交换数据的协议； 软件访问的 KSN 服务的 ID； 停止接收统计信息的日期和时间； 从缓存中获取的 KSN 连接的数量； 在本地请求数据库中找到响应的请求数； 不成功的 KSN 连接数； 不成功的 KSN 事务数； 已取消的 KSN 请求的时间分布； 不成功的 KSN 连接的时间分布； 不成功的 KSN 事务的时间分布； 成功的 KSN 连接的时间分布； 成功的 KSN 事务的时间分布； 对 KSN 的成功请求的时间分布； 对 KSN 的超时请求的时间分布； 新的 KSN 连接数； 由路由错误引起的对于 KSN 的不成功请求数； 由于在软件设置中禁用 KSN 而导致的不成功请求数； 由网络问题引起的对于 KSN 的不成功请求数； 成功的 KSN 连接数； 成功的 KSN 事务数； 向 KSN 发出的请求总数； 开始接收统计数据的日期和时间；

- 设备 ID； 软件的完整版本； 软件更新 ID； 软件安装 ID (PCID)； 已安装软件的类型；

- 设备屏幕高度； 设备屏幕宽度； 有关重叠应用程序的信息： APK 文件的 MD5 哈希值； 有关重叠应用程序的信息： classes.dex 文件的 MD5 哈希； 有关重叠应用程序的信息： APK 文件的名称； 有关重叠应用程序的信息： 不含文件名的 APK 文件路径； 重叠高度； 关于重叠软件的信息： APK 文件的 MD5 哈希值； 重叠应用程序的信息： classes.dex 文件 MD5 哈希； 重叠应用程序的信息： APK 文件名； 重叠应用程序的信息： 不含文件名的 APK 文件路径； 重叠应用程序的信息： 应用程序包名称（对于重叠应用程序： 如果广告显示在空白桌面上，则值应为“launcher”）； 重叠日期和时间； 有关重叠应用程序的信息： 应用程序包名称； 重叠宽度；

- 正在使用的 Wi-Fi 接入点的设置（检测到的设备类型； DHCP 设置（网关本地 IPv6、DHCP IPv6、DNS1 IPv6、DNS2 IPv6 的校验和； 网络前缀长度的校验和； 本地地址 IPv6 的校验和）； DHCP 设置（网关本地IP 地址、DHCP IP、DNS1 IP、DNS2 IP 和子网掩码的校验和）； 指示DNS 域是否存在的标志； 已分配的本地 IPv6 地址的校验和； 已分配的本地 IPv4 地址的校验和； 指示设备是否已插入的标志； Wi-Fi 网络认证类型； 可用的 Wi-Fi 网络及其设置的列表； 接入点 MAC 地址的校验和（MD5 加盐）； 接入点 MAC 地址的校验和（SHA256 加盐）； Wi-Fi 接入点支持的连接类型； Wi-Fi 网络加密类型； Wi-Fi 网络连接开始和结束的当地时间； 基于接入点 MAC 地址的 Wi-Fi 网络 ID； 基于Wi-Fi 网络名称的 Wi-Fi 网络 ID； 基于Wi-Fi 网络名称和接入点 MAC 地址的 Wi-Fi 网络 ID； Wi-Fi 信号强度； Wi-Fi 网络名称； 该配置所支持的认证协议集； 用于 WPA-EAP 连接的认证协议； 内部认证协议； 该配置支持的组密码集； 该配置支持的密钥管理协议集； 网络在软件中的最终隐私类别； 网络在软件中的最终安全类别； 该配置支持的 WPA 分组密码集； 该配置支持的安全协议集）；

- 软件的安装日期和时间； 软件激活日期； 通过其下达软件授权许可订单的合作伙伴组织的标识符； 通过授权许可得出的软件 ID； 软件授权许可密钥的序列号； 软件本地化版本； 指示是否启用了参与 KSN 的标志； 授权许可软件的 ID； 软件授权许可 ID； OS ID； 操作系统位数版本。

而且，为了实现提高软件所提供保护有效性而宣称的目的，权利持有人可接收入侵者为损害计算机和造成信息安全威胁而利用的对象。

将上述信息提供给 KSN 属自愿行为。您可以随时选择退出卡巴斯基安全网络。

在有关用于 Web 保护的数据处理声明下的数据提供

根据 Web 保护声明，权利人为实现 Web 保护功能而处理数据。上述目的包括检测 Web 威胁和使用卡巴斯基安全网络 (KSN) 决定所访问网站的类别。

在您的同意下，以下数据在 Web 保护声明下将被定期自动发送给权利人：

- 产品版本；独一设备 ID；安装 ID；产品类型。
- 网页的 URL 地址、端口号、URL 协议、URL（有关已请求信息）。

在有关将数据处理用于市场营销的声明下的数据提供

权利持有人采用第三方信息系统对数据进行处理。权利持有人的数据处理受此类第三方信息系统的隐私声明约束。以下为权利持有人采用的服务以及权利持有人所处理的数据：

Google Analytics for Firebase

在本软件使用期间，下列数据将自动定期发送至 Google Analytics for Firebase 以实现所宣称的目的：

- 应用信息（应用版本、应用 ID 和 Firebase 服务中的应用 ID、Firebase 服务中的实例 ID、获取应用程序的商店名称、本软件首次启动的时间戳）
- 设备上应用程序安装的 ID 以及安装方法
- 有关区域和语言本地化的信息
- 有关设备屏幕分辨率的信息
- 有关获取根的用户的信息
- 有关源自 SafetyNet Attestation 服务的设备的诊断信息
- 有关将 Kaspersky Endpoint Security for Android 设置为可访问性的信息。
- 有关应用程序屏幕之间的转换、会话持续时间、屏幕会话的开始和结束、屏幕名称的信息
- 有关用于向 Firebase 服务提交数据的协议、其版本以及所采用的数据提交方法 ID 的信息
- 有关所提交数据相关事件的类型和参数的详细信息
- 有关应用许可证、其可用性以及设备数量的信息
- 有关反病毒数据库更新频率和与管理服务器同步的信息
- 有关管理控制台（卡巴斯基安全中心或第三方 EMM 系统）的信息
- Android ID

- 广告 ID
- 有关用户的信息： 年龄类别和性别、居住国家/地区的标识符以及兴趣列表
- 有关安装了该软件的用户计算机的信息： 计算机制造商名称、计算机类型、型号、操作系统的版本和语言（区域设置）、有关最近 7 天内首次打开的应用程序和超过 7 天前首次打开的应用程序的信息

  数据将通过安全通道转发给 Firebase。有关 Firebase 如何处理数据的信息发布于：https://firebase.google.com/support/privacy.

SafetyNet Attestation

在本软件使用期间，为了实现所宣称的目的，将自动定期向 SafetyNet Attestation 发送以下数据：

- 设备检查时间
- 有关软件的信息以及有关软件证书的名称和数据
- 设备检查结果
- 随机 ID 检查，以验证设备检查结果

  数据通过安全通道转发到 SafetyNet Attestation。有关 SafetyNet Attestation 如何处理数据的信息发布于：https://policies.google.com/privacy.

Firebase 性能监测

使用本软件期间，以下信息将自动定期发送至“Firebase 性能监测”(FPM) 以实现宣称的目的：

- 唯一的安装 ID
- 应用程序包名称
- 已安装软件的版本
- 电池电量和电池充电状态
- 载体
- 应用程序前景或背景状态
- 地理位置
- IP 地址
- 设备语言代码
- 有关无线电 / 网络连接的信息
- 假名的软件实例 ID
- 内存和磁盘大小
- 指示设备是否已越狱或获得根权限 (root) 的标志
- 信号强度
- 自动跟踪持续时间

- 网络及以下相应信息： 响应代码、有效负载大小（字节）、响应时间
- 设备描述

  数据通过安全通道转发至“Firebase 性能监测”(FPM)。有关 Firebase Performance Monitoring 如何处理数据的信息发布于：https://firebase.google.com/support/privacy.

Crashlytics

使用本软件期间，以下信息将自动定期发送至 Crashlytics 以实现宣称的目的：

- 软件 ID
- 已安装软件的版本
- 指示软件是否在后台运行的标志
- CPU 架构
- 唯一事件标识符
- 事件日期和时间
- 设备型号
- 总磁盘空间和当前占用量
- 操作系统的名称和版本
- 总内存和当前占用量
- 指示设备是否已获得根权限 (root) 的标志
- 事件发生时的屏幕定位
- 产品 / 硬件制造商
- 唯一的安装 ID
- 所发送的统计数据的版本
- 软件异常类型
- 错误消息文本
- 指示软件异常是由嵌套异常所引起的标志
- 线程 ID
- 指示帧是否是软件错误原因的标志
- 指示线程导致软件意外终止的标志
- 有关导致软件意外终止的信号的信息： 信号名称、信号代码、信号地址
- 对于与线程、异常或错误关联的每个帧： 帧文件的名称、帧文件的行号、调试符号、二进制图像中的地址和偏移量、带帧的库的显示名称、帧的类型、指示帧是否是错误原因的标志

- OS ID
- 与事件关联的问题的 ID
- 有关软件意外终止前发生的事件的信息： 事件标识符、事件日期和时间、事件类型和值
- CPU 注册表值
- 事件类型和值

  数据通过安全渠道转发至 Crashlytics。有关 Crashlytics 如何处理数据的信息发布于：https://firebase.google.com/terms/crashlytics-app-distribution-data-processing-terms.

基于自愿原则出于营销目的提供上述处理信息。

Kaspersky Security for iOS 中的数据提供

Kaspersky Security for Mobile 符合通用数据保护条例 (GDPR)。

要安装应用程序，设备用户必须阅读并接受以下有关处理用户个人数据的声明的条款：

- 最终用户授权许可协议
- 产品与服务隐私政策

用户可以选择阅读并接受以下声明的条款：

- 卡巴斯基安全网络声明

用户可以随时在 Kaspersky Security for iOS 设置中的“关于本应用程序”→“协议和声明”区域中查看这些文档的条款。在此区域中，用户还可以接受或拒绝 KSN 声明的条款。

与卡巴斯基安全网络交换信息

为改进实时保护，Kaspersky Security for iOS 使用卡巴斯基安全网络云服务来运行 Web 保护组件：在打开 Web 资源之前，该应用程序使用从 KSN 接收的数据来扫描 Web 资源。

最终用户授权许可协议中提供了有关在运行 Web 保护的过程中使用 KSN 时提交到卡巴斯基的数据类型的信息。接受授权许可协议的条款和条件即表明您同意传输此信息。

如果卡巴斯基安全网络声明中规定了在运行 Kaspersky Security for iOS 移动应用程序的过程中使用 KSN，则会将有关统计数据类型的信息提交到 Kaspersky。接受声明的条款和条件即表明您同意传输此信息。

在最终用户授权许可协议下的数据提供

如果使用激活码来激活本软件，为了验证本软件的合法用途，最终用户同意定期向权利持有人提供以下信息：

- 向权利持有人基础设施发出的请求中的数据格式； 已访问的 Web 服务的 IPv4 地址； 向权利持有人基础设施发出的请求的内容大小； 协议 ID； 软件激活码； 数据压缩类型； 软件 ID； 可在用户设备上激活的软件 ID 集； 软件本地化版本； 软件的完整版本； 唯一的设备 ID； 用户设备上的日期和时间； 软件安装 ID (PCID)；

当前使用的软件激活码； 操作系统版本、操作系统构建号、操作系统更新号、操作系统发行版本、有关操作系统发行版本的扩展信息； 设备型号； 移动运营商代码； 操作系统系列； 通过授权许可得出的软件 ID； 软件向用户展示的协议列表； 用户使用软件时接受的法律协议类型； 用户使用软件时接受的法律协议版本； 表示用户使用软件时是否接受法律协议条款的标志； 所处理对象的校验码类型； 软件许可证标题； 区域激活中心的 ID； 软件许可证密钥的创建日期和时间； 软件授权许可 ID； 用于提供软件授权许可的信息模型的 ID； 软件许可证的过期日期和时间； 软件许可证密钥的当前状态； 所使用的软件许可证类型； 用于激活本软件的许可证的类型； 通过授权许可得出的软件 ID

权利持有人也可以将此类信息用于收集与权利持有人的软件的分发和使用有关的统计信息。

为了保护本计算机免遭信息安全威胁入侵,最终用户同意定期向权利持有人提供以下信息:

- 向权利持有人基础设施发出的请求中的数据格式； Web 服务的访问地址（URL、IP）； 端口号； Web 服务请求的来源网址 (referrer)。
- 软件的完整版本； 软件更新 ID； 已安装软件的类型； 软件 ID； 配置标识符； 软件操作的结果； 错误代码。
- 正在处理的网址； 已访问的 Web 服务的 IPv4 地址； 扫描的对象的数字证书指纹和哈希算法； 证书类型； 正在处理的数字证书的内容。

在卡巴斯基安全网络声明下的数据提供

接受 KSN 声明后，权利持有人自动接收和处理以下数据：

- 有关 KSN 服务质量的信息（用于与 KSN 交换数据的协议； 软件访问的 KSN 服务的 ID； 停止接收统计信息的日期和时间； 从缓存中获取的 KSN 连接的数量； 在本地请求数据库中找到响应的请求数； 不成功的 KSN 连接数； 不成功的 KSN 事务数； 已取消的 KSN 请求的时间分布； 不成功的 KSN 连接的时间分布； 不成功的 KSN 事务的时间分布； 成功的 KSN 连接的时间分布； 成功的 KSN 事务的时间分布； 对 KSN 的成功请求的时间分布； 对 KSN 的超时请求的时间分布； 新的 KSN 连接数； 由路由错误引起的对于 KSN 的不成功请求数； 由于在软件设置中禁用 KSN 而导致的不成功请求数； 由网络问题引起的对于 KSN 的不成功请求数； 成功的 KSN 连接数； 成功的 KSN 事务数； 向 KSN 发出的请求总数； 开始接收统计数据的日期和时间）。
- 设备 ID； 软件的完整版本； 软件更新 ID； 软件安装 ID (PCID)； 已安装软件的类型。
- 软件的安装日期和时间； 软件激活日期； 软件本地化版本； 指示是否启用了参与 KSN 的标志； 授权许可软件的 ID； 软件授权许可 ID； OS ID； 用户计算机上安装的操作系统版本； 操作系统位数版本。

将上述信息提供给 KSN 属自愿行为。您可以随时选择退出卡巴斯基安全网络。

联系技术支持

本节介绍了如何获取技术支持以及提供技术支持的时间段。

如何获得技术支持

如果在 Kaspersky Security for Mobile 文档或有关 Kaspersky Security for Mobile 的任何信息来源中找不到问题的解决方案，请联系技术支持。技术支持专家将回答您关于安装和使用 Kaspersky Security for Mobile 的所有问题。

Kaspersky 在 Kaspersky Security for Mobile 的生命周期内为其提供支持（请参见产品支持生命周期页面）。在联系技术支持之前，请阅读支持规则。

您可以使用下列方式之一与技术支持服务联系：

- 通过访问技术支持网站
- 通过从 Kaspersky CompanyAccount 门户向技术支持发送请求

通过“Kaspersky CompanyAccount”获得技术支持

Kaspersky CompanyAccount 是为使用 Kaspersky 应用程序的公司提供的一个门户。Kaspersky CompanyAccount 门户的目的是通过在线请求促进用户和 Kaspersky 专家之间的互动。您可以使用 Kaspersky CompanyAccount 跟踪您在线请求的状态并存储其历史。

您可以在 Kaspersky CompanyAccount 上将您所在组织的所有员工注册到同一个帐户下。单一帐号使您可以集中管理注册员工向 Kaspersky 发送的电子请求，并且通过 Kaspersky CompanyAccount 管理这些员工的权限。

可提供以下语言的 Kaspersky CompanyAccount 门户：

- 英语
- 西班牙语
- 意大利语
- 德语
- 波兰语
- 葡萄牙语
- 俄语
- 法语
- 日语

如需了解 Kaspersky CompanyAccount 详情，请访问技术支持网站。

有关应用程序的信息源

Kaspersky 网站上的 Kaspersky Security for Mobile 网页

在 Kaspersky Security for Mobile 页面上，您可以找到有关应用程序及其功能和操作参数的一般信息。

Kaspersky Security for Mobile 网页提供 eStore 链接。您可以在此购买或续订程序。

知识库中的 Kaspersky Security for Mobile 网页

知识库 是技术支持网站上的一个区域。

在知识库中的 Kaspersky Security for Mobile 页面上，您可以找到相关文章，这些文章包含有用的信息、建议以及有关如何购买、安装和使用应用程序的常见问题解答。

知识库文章不仅可以解答与 Kaspersky Security for mobile 有关的问题，而且可以解答与其他 Kaspersky 应用程序有关的问题。知识库文章还可能包含技术支持的最新情况。

在线帮助

程序的在线帮助由帮助文件组成。

Kaspersky Security for Mobile 管理插件的上下文帮助提供有关 Kaspersky Security Center 窗口的信息：Kaspersky Security for Mobile 设置描述，以及使用这些设置的任务描述的链接。

Kaspersky Endpoint Security for Android 和 Kaspersky Security for iOS 应用程序的完整帮助提供有关如何配置和使用移动应用程序的信息。

在卡巴斯基支持论坛上讨论卡巴斯基应用程序

如果您的问题不需要立即答复，您可以在我们的论坛中与 Kaspersky 专家和其他用户进行讨论。

在论坛上，您可以查看现有讨论主题、发表评论并创建新的讨论主题。

术语

Apple 推送通知服务 (APNs) 证书

由 Apple 签名的证书，允许您使用 Apple 推送通知。通过 Apple 推送通知，iOS MDM 服务器可以管理 iOS 设备。

EAS 设备

通过 Exchange ActiveSync 协议连接至管理服务器的移动设备。

Exchange Mobile Devices Server

Kaspersky Endpoint Security 的一个组件，允许您将 Exchange ActiveSync 移动设备连接到管理服务器。

IMAP

用于访问电子邮件的协议。与 POP3 协议相反，IMAP 提供了用于处理邮箱的扩展功能，例如管理文件夹和处理邮件，而不从邮件服务器复制其内容。IMAP 协议使用端口 134。

iOS MDM 服务器

Kaspersky Endpoint Security 的一个组件，安装到客户端设备，允许将 iOS 移动设备连接到管理服务器，并通过 Apple 推送通知 (APN) 管理这些 iOS 移动设备。

iOS MDM 设备

由 iOS MDM 服务器控制的 iOS 移动设备。

iOS MDM 配置文件

包含一系列将 iOS 移动设备连接至管理服务器的设置集合的配置文件。iOS MDM 配置文件用于通过 iOS MDM 服务器以后台模式发送 iOS 配置文件，接收关于移动设备的扩展诊断信息。需要将 iOS MDM 配置文件链接发送给用户，以便启动 iOS MDM 服务器发现并连接用户的 iOS 移动设备。

Kaspersky Security Center Web Server

Kaspersky Security Center 的一个组件，与管理服务器一同安装。Web Server 用于通过网络传输独立安装包、iOS MDM 配置文件和共享文件夹中的文件。

Kaspersky Security Center 管理员

通过 Kaspersky Security Center 远程集中管理系统管理应用程序运行的人员。

Kaspersky 更新服务器

Kaspersky 的 HTTP(S) 服务器，Kaspersky 应用程序从这些服务器下载数据库和应用程序模块更新。

Kaspersky 类别

Kaspersky 专家开发的预定义数据类别。可以在应用程序数据库更新期间更新类别。安全人员无法修改或删除预定义类别。

POP3

邮件客户端用来从邮件服务器接收邮件的网络协议。

SSL

互联网和局域网上使用的数据加密协议。在 Web 应用程序中使用安全套接字层 (SSL) 协议在客户端和服务器之间创建安全连接。

代理服务器

允许用户向其他网络服务发出间接请求的计算机网络服务。首先，用户连接到代理服务器并请求位于另一服务器上的资源（例如文件）。然后，代理服务器连接到指定的服务器并从中获取资源，或者从自己的缓存中返回资源（如果代理有自己的缓存）。在有些情况下，代理服务器可能会出于某些目的修改用户的请求或服务器的响应。

供给配置文件

应用程序对 iOS 移动设备的操作的设置集合。供给配置文件包含有关授权许可的信息；它链接到一个特定应用程序。

最终用户授权许可协议

您与 AO Kaspersky Lab 之间的合作协议，其中规定了您使用应用程序时应遵守的条款。

卡巴斯基安全网络 (KSN)

一种云基础架构，提供对 Kaspersky 数据库的访问。该数据库具有不断更新的关于文件、网页资源和软件的信誉信息。卡巴斯基安全网络确保 Kaspersky 应用程序对威胁做出更快速的响应，提高某些保护组件的性能，并降低误报的可能性。

卡巴斯基私有安全网络（私有 KSN）

卡巴斯基私有安全网络解决方案让安装了 Kaspersky 应用程序的设备的用户可以访问卡巴斯基安全网络的信誉数据库和其他统计数据，而无需将其设备中的数据发送到卡巴斯基安全网络。卡巴斯基私有安全网络面向因以下任何原因无法加入卡巴斯基安全网络的公司客户所设计：

- 用户设备未连接到互联网。
- 法律或公司安全策略禁止在所在国家/地区或公司局域网之外传输任何数据。

反病毒数据库

包含截至反病毒数据库发布时 Kaspersky 已知的计算机安全威胁的相关信息的数据库。通过反病毒数据库中的条目可以在扫描的对象中检测恶意代码。反病毒数据库由 Kaspersky 专家创建，每小时更新一次。

合规性控制

验证移动设备和 Kaspersky Endpoint Security for Android 的设置是否符合公司的安全要求。公司安全要求控制设备使用情况。例如，必须在设备上启用实时保护，反病毒数据库必须是最新的，并且设备密码必须足够强。合规性控制基于规则列表。合规性规则包括以下组成部分：

- 设备检查条件（例如，设备上不存在被禁止的应用程序）
- 分配给用户以解决不合规问题的时间间隔（例如，24 小时）
- 如果用户未在规定的时间段内解决不合规问题，将对设备采取的措施（例如锁定设备）

安卓工作配置文件

一个用户设备上的安全环境，在该环境中，管理员可以在不限制用户使用个人数据的情况下，管理应用程序和账户。当用户设备上创建了工作配置文件后，下列公司应用将自动安装在工作配置文件中：Google Play Market、Google Chrome、Downloads、Kaspersky Endpoint Security for Android 等等。工作配置文件中安装的应用程序，以及这些应用程序的通知，都将被标上红色手提箱图标。您必须为 Google Play Market 应用程序创建单独的 Google 公司账户。工作配置文件中安装的应用程序会显示在常用应用程序列表中。

安装包

使用远程管理系统创建的一组用于远程安装 Kaspersky 程序的文件。基于应用程序分发包中包括的专用文件所创建的安装包。安装包包含了安装应用程序并立即运行所需的一系列设置。分发包中设置值对应于应用程序设置的默认值。

密钥文件

xxxxxxxx.key 格式的文件，允许基于试用或商业授权许可使用 Kaspersky 应用程序。应用程序基于激活码生成密钥文件。仅当您有密钥文件时，才能使用应用程序。

应用程序管理插件

一个专用组件，它通过管理控制台提供管理 Kaspersky 应用程序的界面。每个可通过 Kaspersky Security Center SPE 管理的应用程序都有自己的管理插件。管理插件包含在可通过 Kaspersky Security Center 管理的所有 Kaspersky 应用程序中。

授权许可

有时间限制的应用程序使用权利，在最终用户授权许可协议下授予。

授权许可的有效期

您可以访问应用程序功能并有权使用其他服务的时间段。您可以使用的服务取决于授权许可的类型。

清单文件

PLIST 格式的文件，包含网页服务器中应用程序文件（ipa 文件）的链接。使用 iOS 设备从网页服务器中查找、下载并安装应用程序。

激活码

在购买 Kaspersky Endpoint Security 授权许可时收到的代码。此代码是激活应用程序所必需的。

激活码是由 20 个字母和数字组成的格式为 xxxxx-xxxxx-xxxxx-xxxxx 的唯一序列。

激活程序

将应用程序切换到全功能模式。用户在安装应用程序期间或之后执行应用程序激活。您应该有激活码或密钥文件以激活应用程序。

独立安装包

适用于安卓操作系统的 Kaspersky Endpoint Security 安装文件，其包含应用程序连接管理服务器的设置。基于该应用程序的安装包进行创建，并且是一个特殊的移动应用程序包。

病毒

一种感染其他程序的程序，通过将其代码添加到其他程序中，在受感染文件运行时获得控制权。这一简单定义允许标识由任何病毒执行的主要操作：感染。

监控设备

其设置受 Apple Configurator（用于对 iOS 设备进行组配置的程序）监控的 iOS 设备。监控设备在 Apple Configurator 中的状态为*受监控*。每当监控设备连接到计算机时，Apple Configurator 都会针对指定的参考设置检查设备配置，然后在必要时重新定义这些设置。监控设备不能与安装在其他计算机上的 Apple Configurator 同步。

相比非监控设备，每个监控设备都提供更多设置以通过 Kaspersky Device Management for iOS 策略重新定义。例如，您可以配置 HTTP 代理服务器来监控公司网络内的设备上的互联网流量。默认情况下，所有移动设备均不受监控。

策略

一套应用程序设置集合，Kaspersky Endpoint Security 移动应用程序将其应用至管理组中的设备上，或应用至单个设备上。可将不同的策略应用至不同的管理组中。策略包括 Kaspersky Endpoint Security 移动应用程序所有功能的配置设置。

管理员工作站

部署了 Kaspersky Security Center 管理控制台的计算机。如果管理员工作站上安装了应用程序管理插件，Kaspersky Endpoint Security 移动应用程序将部署在用户设备上。

管理服务器

Kaspersky Security Center 的一个组件，可集中存储公司网络内安装的所有 Kaspersky 程序的信息。它也可用于管理这些应用程序。

管理组

一组受管设备，例如根据其执行的功能和其上所安装应用程序集合进行群组的移动设备。将受管计算机群组便于以一个整体的形式进行管理。例如，可将运行相同操作系统的移动设备合并为一个管理组。一个组可包含其他管理组。您可以为组设备创建组策略和组任务。

组任务

为组中所有受管设备执行的管理组任务。

网络钓鱼

一种旨在对用户机密数据进行未授权访问的互联网欺诈。

解锁码

可以在 Kaspersky Security Center 中获取的代码。在执行了“**锁定和定位**”、“**警报**”或“**拍摄面部照片**”命令之后，以及当触发自我保护时，解锁设备需要此代码。

订阅

允许在所选参数（到期日期和设备数量）范围内使用应用程序。您可以暂停或恢复订阅、自动续费或取消。

设备管理员

一套安卓设备上应用程序权限集合，可允许应用程序使用设备管理策略。有必要在安卓设备上应用 Kaspersky Endpoint Security on Android 的全部功能。

证书签名请求

包含管理服务器设置的文件，由 Kaspersky 批准，随后发送到 Apple 以获取 APN 证书。

隔离

Kaspersky 应用程序将已检测到的疑似感染对象移动到其中的文件夹。对象以加密形式存储在隔离区中，以避免对计算机产生任何影响。

有关第三方代码的信息

您可以下载并阅读以下文件中有关第三方代码的信息：

- legal_notices_Android.txt（对于 Kaspersky Endpoint Security for Android 应用程序）
- legal_notices_iOS.txt（对于 Kaspersky Security for iOS 应用程序）

在移动设备上，有关第三方代码的信息在移动应用程序的“**关于本应用程序**”区域中提供。

商标声明

注册商标和服务标志均为其各自拥有者的财产。

PostScript 是 Adobe 在美国和/或其他国家/地区的注册商标或商标。

AirDrop 和 AirPrint 是 Apple Inc. 的商标

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 和 Touch ID 是 Apple Inc. 在美国以及其他国家和地区注册的商标。

Aruba Networks 是 Aruba Networks, Inc. 在美国和其他国家/地区注册的商标。

Bluetooth 词语、掩码和标识由 Bluetooth SIG, Inc. 所有。

Cisco、Cisco AnyConnect 和 IOS 是 Cisco Systems, Inc. 和/或其附属公司在美国和其他国家/地区的注册商标或商标。

SecurID 是 EMC Corporation 在美国和/或其他国家/地区的注册商标或商标。

Google、Android、Chrome、Chromebook、Chromium、Crashlytics、Firebase、Google Analytics、Google Chrome、Google Mail、Google Maps、Google Play、Nexus 和 SPDY 是 Google LLC 的商标。

HTC 是 HTC Corporation 的商标。

Huawei、HUAWEI 和 EMUI 是 Huawei Technologies Co., Ltd 在中国和其他国家/地区注册的商标。

IBM 和 Maas360 是 International Business Machines Corporation 在世界多个地区注册的商标。

Juniper Networks、Juniper 和 JUNOS 是 Juniper Networks, Inc. 在美国和其他国家/地区的商标或注册商标。

Microsoft、ActiveSync、Microsoft Intune、Tahoma、Windows、Windows Mobile 和 Windows Phone 是 Microsoft 集团公司的商标。

MOTOROLA 和 Stylized M 标识是 Motorola Trademark Holdings, LLC 的商标或注册商标。

Oracle 和 JavaScript 是 Oracle 和/或其附属公司的注册商标。

BlackBerry 商标由 Research In Motion Limited 拥有，并在美国注册，在其他国家/地区可能正在申请中或已注册。

Samsung 是 SAMSUNG 在美国和其他国家/地区注册的商标。

SonicWALL、Aventail 和 SonicWALL Mobile Connect 是 SonicWall, Inc. 的商标。

SOTI 和 MobiControl 是 SOTI Inc. 在美国和其他国家/地区的注册商标。

Symantec 是 Symantec Corporation 或其附属公司在美国和其他国家/地区的商标或注册商标。

Symbian 商标由 Symbian Foundation Ltd. 所有。

AirWatch、VMware 和 VMware Workspace ONE 是 VMware, Inc 在美国和/或其他地区的注册商标或商标。

F5 是 F5 Networks, Inc. 在美国和某些其他国家/地区的商标。