kaspersky

Kaspersky Security for Mobile

目錄

Kaspersky Security for Mobile 說明

Kaspersky Security for Mobile 旨在保護和管理公司行動裝置以及公司員工用於公司目的的個人行動裝置。

Kaspersky Security for Mobile 的元件和功能取決於您用來保護和管理行動裝置介面的卡巴斯基安全管理中心主控台而定。

根據您的卡巴斯基安全管理中心主控台選擇必要的說明部分：

- 以 Microsoft 管理主控台為基礎的管理主控台
- 卡巴斯基安全管理中心網頁主控台或 Kaspersky Security Center Cloud Console

獨立說明區段描述 Kaspersky Endpoint Security for Android 應用程式和 Kaspersky Security for iOS 應用程式使用者可用的功能和操作。

新增功能

Kaspersky Endpoint Security for Android Technical Release 44

- Android 13 目前已提供支援。
- 對於 SOTI MobiControl 主控台使用者，已在卡巴斯基安全管理中心新增用來指定 SOTI MobiControl 裝置名稱的選項。
- 一般錯誤修正和改善。

Kaspersky Endpoint Security for Android Technical Release 43

- 在 Android 12 或更高版本，Kaspersky Endpoint Security for Android 應用程式需要權限才能在背景中執行。
- 在 Android 13，Kaspersky Endpoint Security for Android 應用程式會提示傳送通知的權限。
- 一般錯誤修正和改善。

Kaspersky Security for iOS Technical Release 1

新的 Kaspersky Security for iOS 應用程式用於保護和管理企業 iOS 和 iPadOS 裝置。該應用程式提供下列關鍵功能：

- 防禦線上威脅。
- 破解偵測。
- 使用卡巴斯基安全管理中心網頁主控台和 Cloud Console 管理企業裝置。

Kaspersky Endpoint Security for Android Technical Release 42

- Kaspersky Endpoint Security for Android 應用程式中的使用者介面加強事項。
- Kaspersky Endpoint Security for Android 應用程式現在對 Android 12 或更高版本需要「鄰近藍牙裝置」權限，才能允許管理員限制藍牙使用。
- 一般錯誤修正和改善。

Kaspersky Endpoint Security for Android Technical Release 41

- Kaspersky Endpoint Security for Android 應用程式中的使用者介面加強事項。
- 卡巴斯基安全管理中心網頁主控台和 Cloud Console 的 Kaspersky Security for Mobile (Policies) 外掛程式政策設定中的使用者介面加強事項。
- 一般錯誤修正和改善。

Kaspersky Endpoint Security for Android Technical Release 40

- 一般錯誤修正和改善。

Kaspersky Endpoint Security for Android Technical Release 39

- Android 12L 目前已提供支援。
- 更新下列協議和聲明：
  - 最終使用者產品授權協議
  - 卡巴斯基安全網路聲明
  - 有關將資料處理用於市場行銷的聲明

  請注意，管理員可以在管理主控台中接受新的協議和聲明。這可讓裝置上 Kaspersky Endpoint Security for Android 應用程式的使用者略過此步驟。
- 一般錯誤修正和改善。

Kaspersky Endpoint Security for Android Technical Release 33

- 使用第三方 EMM 系統管理 Kaspersky Endpoint Security for Android 應用程式時，現在可以使用單一命令接受多個最終使用者產品授權協議。
- 您不再需要密鑰來啟動 Samsung KNOX。
- Kaspersky Security for Mobile 元件版本的結構已修改為包含版本號碼。

Kaspersky Endpoint Security for Android Technical Release 32

- Kaspersky Endpoint Security for Android 應用程式已修改，以支援更新的 Android 要求。

Kaspersky Endpoint Security for Android Technical Release 31

- 如果您的組織中未佈署卡巴斯基安全管理中心或行動裝置無法存取卡巴斯基安全管理中心，使用者可以在其裝置上手動啟動 Kaspersky Endpoint Security for Android 應用程式。
- Kaspersky Security for Mobile 現在支援 Google Chrome 的自訂標籤功能。

Kaspersky Endpoint Security for Android Technical Release 30

- Kaspersky Security for Mobile 現在允許您在卡巴斯基安全管理中心雲端主控台中保護和管理行動裝置。
- Kaspersky Security for Mobile 現已支援 iOS 15 和 iPadOS 15。

Kaspersky Endpoint Security for Android Technical Release 29

- Kaspersky Endpoint Security for Android 應用程式現已支援 Android 12。

Kaspersky Endpoint Security for Android Technical Release 27

- Kaspersky Security for Mobile 現在允許您在卡巴斯基安全管理中心網頁主控台中保護和管理行動裝置。

Kaspersky Endpoint Security for Android Technical Release 26

- Kaspersky Endpoint Security 現在支援自動續訂的產品授權和訂閱。

Kaspersky Endpoint Security for Android Technical Release 22

- Kaspersky Endpoint Security 現在支援卡巴斯基私人安全網路，此解決方案允許存取卡巴斯基安全網路的信譽資料庫，而無需在公司網路外部傳送資料。
- Kaspersky Endpoint Security for Android 不再支援在執行Android 4.2 – 4.4.4 版本的裝置上進行安裝。

Kaspersky Endpoint Security for Android Technical Release 20

- 若管理員選擇接受全域聲明，使用者並不會收到接受法律聲明的提示。
- 應用程式效能已經過最全化。

Kaspersky Endpoint Security for Android Technical Release 19

- 管理員現在可以透過卡巴斯基安全管理中心代表最終使用者接受卡巴斯基安全網路和其他聲明。
- 修復了幾個錯誤，且改進了操作穩定性。

Kaspersky Endpoint Security for Android Technical Release 18

- Kaspersky Security for Mobile 現在支援 Huawei Mobile 服務。
- Kaspersky Endpoint Security for Android 現在可用於從 Huawei AppGallery 安裝。

Kaspersky Endpoint Security for Android Technical Release 17

- 卡巴斯基安全管理中心現在鎖定 API 第 29 級和更高層級，為執行 Android 10 或更新版本的裝置在應用程式行為上帶來一些改變。
- 新增密碼強度設定，供使用者設置所需複雜度的密碼。
- 配置使用指紋解鎖螢幕的方法，現在只適用於 Android 工作設定檔。
- 修復了幾個錯誤，且改進了操作穩定性。

Kaspersky Endpoint Security for Android Technical Release 16

- Kaspersky Endpoint Security for Android 現已支援 Android 11。
- Android 11 推出的地理定位和相機權限的新要求。您可以在本章節閱讀更多關於相機和位置存取權限的新規則。
- 現在您可以在協力廠商 EMM 主控台中指定使用者的企業電子郵件地址。只要您設定好新的 KscCorporateEmail，這些郵件就會顯示在卡巴斯基安全管理中心。

Kaspersky Endpoint Security for Android Technical Release 14

- 每當有使用者允許或撤銷應用程式的裝置管理權限，系統就會事件傳送至管理主控台。
- 「KscGroup」參數現在可以在協力廠商 EMM 主控台中設定。裝置連線至卡巴斯基安全管理中心時，系統會自動新增至未分配裝置資料夾的子資料夾中，並使用與在 EMM 主控台配置的群組相同的名稱。

Kaspersky Endpoint Security for Android Technical Release 13

- Kaspersky Endpoint Security for Android 的全新使用者介面設計。
- 所有說明區段都採線上提供。
- 受管裝置的 IP 位址現在會傳送至卡巴斯基安全管理中心，並且可在裝置資訊區段中檢視。

Kaspersky Endpoint Security for Android Technical Release 12

- 新增遠端接受卡巴斯基安全管理中心 12.1 最終使用者產品授權協議 (EULA) 的功能。若管理員在管理主控台接受產品授權協議的條款與隱私權政策，則應用程式會在安全期間略過這些步驟。
- 為使用 VMware AirWatch 的使用者新增在卡巴斯基安全管理中心編輯裝置名稱的功能。我們在設定檔中新增了一個設定，您可以用它來設定應用程式。您可以將更多資訊新增到裝置名稱中 (例如，裝置序號)。這麼做可讓使用者在卡巴斯基安全管理中心輕鬆尋找與排序裝置。

Kaspersky Endpoint Security for Android Technical Release 11

修復了幾個錯誤，且改進了操作穩定性。

Kaspersky Endpoint Security for Android Technical Release 10

- Kaspersky Security for Mobile 現在支援卡巴斯基安全管理中心 12。
- 卡巴斯基安全管理中心 12 不再支援 Kaspersky Safe Browser。卡巴斯基安全管理中心 11 以上版本提供 Kaspersky Safe Browser 功能。
- 修復了幾個錯誤，且改進了操作穩定性。

Kaspersky Endpoint Security for Android Service Pack 4 Maintenance Release 3

- 已驗證在 Microsoft Intune 中支援 Kaspersky Endpoint Security for Android（一種企業移動管理 (EMM) 解決方案）。Kaspersky 加入 AppConfig Community 以確保應用程式可與協力廠商 EMM 解決方案一起執行。

- 已新增應用程式在背景模式時停用通知和彈出訊息的功能。請記住，在背景模式下執行這些動作並不安全。如果應用程式在背景模式且停用通知和彈出訊息時，應用程式將無法針對威脅即時警告使用者。行動裝置使用者只有在開啟應用程式時才能得知裝置的防護狀態。

- 新增在 VMware AirWatch 中同意最終使用者產品授權協議 (EULA) 和隱私政策的功能。如果管理員在 AirWatch 主控台同意最終使用者產品授權協議和隱私政策，Kaspersky Endpoint Security for Android 將能夠略過初始配置精靈的接受步驟。

- 已新增利用 Web 防護進行資料處理的聲明（Web 防護聲明）。您必須接受聲明才能夠使用 Web 防護。Kaspersky Endpoint Security for Android 使用卡巴斯基安全網路 (KSN) 來掃描網站。Web 防護聲明包含與 KSN 交換資料的條件和條款。您可以在政策中同意 Web 防護聲明，或是請求裝置使用者同意。

- 修復了幾個錯誤，且改進了操作穩定性。

不同管理工具的應用程式功能比較

您可以使用以下管理工具在卡巴斯基安全管理中心管理行動裝置：

- 以 Microsoft Management Console（以下簡稱「MMC 型」）為基礎的卡巴斯基安全管理中心管理主控台
- 卡巴斯基安全管理中心網頁主控台
- 卡巴斯基安全管理中心雲端主控台

下表比較了這些工具中可用的功能。

功能的可用性視管理工具而定

	MMC 型主控台	網頁主控台	雲端主控台
一般			
Android 裝置管理	可用	可用	可用
iOS 裝置管理	可用（透過 APN 憑證）	可用（透過 Kaspersky Security for iOS 應用程式）	可用（透過 Kaspersky Security for iOS 應用程式）
行動裝置管理			
使用 Google Play 連結來新增裝置	可用	可用	可用
使用 App Store 連結新增裝置	無法使用	可用	可用
使用 iOS MDM 設定檔新增 iOS 裝置	可用	無法使用	無法使用
建立安裝套件來新增裝置	可用	無法使用	無法使用
傳送命令至行動裝置	可用	可用（臉部快照命令除外）	可用（臉部快照命令除外）
從卡巴斯基安全管理中心移除行動裝置	可用	可用（僅限從裝置清單中移除。必須手動從裝置中移除該應用程式。）	可用（僅限從裝置清單中移除。必須手動從裝置中移除該應用程式。）
憑證管理			
簽發郵件憑證	可用	無法使用	無法使用
簽發 VPN 憑證	可用	無法使用	無法使用
簽發手機憑證	可用	可用	可用
透過管理伺服器工具簽發手機憑證	可用	可用	可用
指定憑證檔案	可用	無法使用	無法使用
與公用金鑰基礎架構整合	可用	無法使用	無法使用
政策管理			

根據角色存取設定群組政策	可用	無法使用	無法使用
使用卡巴斯基安全管理中心設定行動裝置的同步	可用	可用	可用
在行動裝置上設定病毒掃描	可用	可用	可用
設定行動裝置保護	可用	可用	可用
設定病毒資料庫更新	可用	可用	可用
為被竊取或遺失的裝置資料設定防護	可用	可用	可用
設定使用者對網站的存取	可用	可用	可用
設定應用程式控制	可用	可用	可用
設定合規性控制	可用	可用	可用
設定 Android 工作設定檔	可用	無法使用	無法使用
設定與 Wi-Fi 網路的連線	可用	無法使用	無法使用
Samsung KNOX	可用	無法使用	無法使用
其他功能			
全域接受卡巴斯基安全管理中心 EULA	可用	無法使用	無法使用
設定卡巴斯基私人安全網路	可用	無法使用	無法使用

分發套件

Kaspersky Security for Mobile 分發套件可能包含各種元件，具體取決於所選的應用程式版本。

卡巴斯基安全管理中心網頁主控台中的行動裝置管理

- `on_prem_ksm_devices_xx.x.x.x.zip`
  包含安裝 Kaspersky Security for Mobile (Devices) 外掛程式所需檔案的存檔：
  - `plugin.zip`
    包含 Kaspersky Security for Mobile (Devices) 外掛程式的存檔。
  - `signature.txt`
    包含 Kaspersky Security for Mobile (Devices) 外掛程式簽名的檔案。
- `on_prem_ksm_policies_xx.x.x.x.zip`
  包含安裝 Kaspersky Security for Mobile (Policies) 外掛程式所需檔案的存檔：
  - `plugin.zip`
    包含 Kaspersky Security for Mobile (Policies) 外掛程式的存檔。
  - `signature.txt`
    包含 Kaspersky Security for Mobile (Policies) 外掛程式簽名的檔案。

卡巴斯基安全管理中心雲端主控台中的行動裝置管理

要在卡巴斯基安全管理中心雲端主控台中管理行動裝置，您無需下載分發套件。您只需要在卡巴斯基安全管理中心雲端主控台中建立一個帳戶。有關建立帳戶的更多資訊，請參閱*卡巴斯基安全管理中心雲端主控台說明*。

以 MMC 為基礎的管理主控台中的行動裝置管理

- `Klcfginst_en.exe`
  透過卡巴斯基安全管理中心遠端管理系統來管理應用程式所用的 Kaspersky Endpoint Security for Android 管理外掛程式的安裝檔案。
- `Klmdminst.exe`
  透過卡巴斯基安全管理中心遠端管理系統來管理應用程式所用的 Kaspersky Device Management for iOS 管理外掛程式的安裝檔案。

Kaspersky Endpoint Security for Android 應用程式的檔案

`KES10_xx_xx_xxx.apk` — Kaspersky Endpoint Security for Android 應用程式的 Android 套件檔案。

輔助檔案

- `sc_package_xx.exe`

自動解壓縮存檔，其中包含透過建立安裝套件安裝 Kaspersky Endpoint Security for Android 應用程式所需的檔案：

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

  建立安裝套件所需的檔案。

- `installer.ini`

  包含管理伺服器連線設定的設定檔。

- `KES10_xx_xx_xxx.apk`

  Kaspersky Endpoint Security for Android 應用程式的 Android 套件檔案。

- `kmlisten.exe`

  用於透過管理員電腦傳送安裝套件的公用程式。

- `kmlisten.ini`

  包含 `kmlisten.exe` 公用程式設定的設定檔。

- `kmlisten.kpd`

  應用程式描述檔案。

- `SigningUtility.zip`

  包含公用程式的存檔，該存檔用於對 iOS 裝置的 Kaspersky Endpoint Security for Android 應用程式和容器的分發套件進行簽章。

文件

- Kaspersky Security for Mobile 的說明。

在卡巴斯基安全管理中心網頁主控台和卡巴斯基安全管理中心雲端主控台中工作

本說明部分介紹了使用卡巴斯基安全管理中心網頁主控台（以下簡稱網頁主控台）或卡巴斯基安全管理中心雲端主控台（以下簡稱雲端主控台）對行動裝置的防護和管理。

關於卡巴斯基安全管理中心網頁主控台和雲端主控台中的行動裝置管理

您可以使用以下元件在卡巴斯基安全管理中心網頁主控台和雲端主控台中進行行動裝置管理：

- **Kaspersky Endpoint Security for Android 應用程式**

  Kaspersky Endpoint Security for Android 應用程式能確保為行動裝置提供保護，幫助抵禦網路威脅、病毒和其他會造成威脅的程式攻擊。

- **Kaspersky Security for iOS 應用程式**

  Kaspersky Security for iOS 應用程式可確保保護行動裝置以防網路釣魚和網路威脅。

- **Kaspersky Security for Mobile (Devices) 外掛程式**

  Kaspersky Security for Mobile (Devices) 外掛程式提供了用於透過卡巴斯基安全管理中心網頁主控台和 Cloud Console 管理行動裝置和安裝在其上的行動應用程式的介面。

- **Kaspersky Security for Mobile (Policies) 外掛程式**

  Kaspersky Security for Mobile (Policies) 外掛程式允許您使用群組政策為連線到卡巴斯基安全管理中心的裝置定義配置設定。

外掛程式已整合到*卡巴斯基安全管理中心遠端管理系統*中。您可以使用卡巴斯基安全管理中心網頁主控台或雲端主控台來管理行動裝置以及用戶端電腦和虛擬系統。將行動裝置連線至管理伺服器後，行動裝置就變成託管裝置。您可以遠端監控受管理裝置。

在卡巴斯基安全管理中心網頁主控台和雲端主控台中管理行動裝置的主要功能

Kaspersky Security for Mobile 包括以下功能：

- 發佈電子郵件訊息，以使用連結從 Google Play 下載 Kaspersky Endpoint Security for Android 應用程式，將 Android 行動裝置連線至卡巴斯基安全管理中心。
- 發佈電子郵件訊息，以使用連結從 App Store 下載 Kaspersky Security for iOS 應用程式，將 iOS 行動裝置連線至卡巴斯基安全管理中心。
- 遠端連線行動裝置到卡巴斯基安全管理中心和其他第三方 EMM 系統（例如，VMWare AirWatch、MobileIron、IBM Maas360、SOTI MobiControl）。
- 行動應用程式的遠端配置，以及服務、應用程式和行動裝置功能的遠端配置。
- 根據企業安全需求遠端管理行動裝置。
- 預防行動裝置在遺失或被竊時儲存的企業資訊洩露（竊盜防護）。僅支援 Android 裝置。

- 企業安全需求合規性控制（合規性控制）。僅支援 Android 裝置。
- 控制線上威脅防護並控制行動裝置上的網際網路使用（Web 防護）。
- 設定在 Kaspersky Endpoint Security for Android 和 Kaspersky Security for iOS 應用程式上向使用者顯示的通知。
- Kaspersky Endpoint Security for Android 和 Kaspersky Security for iOS 應用程式的狀態和事件的管理員通知可以在卡巴斯基安全管理中心中或透過郵件通訊。
- 政策設定的變更控制（修訂歷史記錄）。

Kaspersky Security for Mobile 包括以下防護和管理元件：

- 病毒防護（適用於 Android 裝置）
- 竊盜防護（適用於 Android 裝置）
- 網頁防護（適用於 Android 和 iOS 裝置）
- 應用程式控制（適用於 Android 裝置）
- 合規控制（適用於 Android 裝置）
- Android 裝置上的根權限偵測和 iOS 裝置上的破解偵測

關於 Kaspersky Endpoint Security for Android 應用程式

Kaspersky Endpoint Security for Android 應用程式能確保為行動裝置提供保護，幫助抵禦網路威脅、病毒和其他會造成威脅的程式攻擊。

Kaspersky Endpoint Security for Android 應用程式包括以下元件：

- **病毒防護**。此元件會使用病毒資料庫及卡巴斯基安全網路雲端服務偵測並消除威脅。病毒防護功能包含以下元件：
  - **防護**。此功能會在開啟的檔案中偵測威脅、掃描新應用程式並即時防護裝置受感染。
  - **掃描**。它根據需要針對整個檔案系統、僅針對已安裝的應用程式或針對選定的檔案或資料夾啟動。
  - **更新**。「更新」功能允許您為應用程式下載新的病毒資料庫。
- **竊盜防護**。該元件在裝置遺失或被竊時防護裝置上的資訊，防禦未經授權的存取。此元件允許您向裝置發送以下命令：
  - **定位**。取得裝置位置的座標。
  - **警報**。使裝置大聲發出警報。
  - **抹除**。抹除企業資料以保護敏感的公司資訊。
- **Web 防護**。該元件可以封鎖用於擴散惡意程式碼的惡意網站。Web 防護也可以封鎖用於偷竊使用者機密資料（例如，網路銀行或電子錢包系統的密碼）並存取使用者財務資訊的虛假（釣魚）網站。Web 防護將在您開啟網站前使用卡巴斯基安全網路雲端服務掃描網站。掃描之後，Web 防護將允許可信的網站載入並封鎖惡意

網站。Web 防護也支援按卡巴斯基安全網路雲端服務中所定義類別篩選網站。這允許管理員限制使用者對某些類別網頁的存取（例如「賭博、彩票、抽獎」或「網際網路通訊」類別中的網頁）。

- **應用程式控制。**此元件可讓您透過指向分發套件的直接連結或指向 Google Play 的連結，將推薦和所需的應用程式安裝到您的裝置上。應用程式控制還允許您移除那些違反企業安全需求的已封鎖應用程式。

- **合規性控制。**此元件允許檢查受管理裝置是否符合企業安全需求法規，並對不符合法規之裝置的某些功能施加限制。

您可以透過定義群組政策設定，在卡巴斯基安全管理中心網頁主控台和雲端主控台中配置 Kaspersky Endpoint Security for Android 應用程式的元件。

關於 Kaspersky Security for iOS 應用程式

Kaspersky Security for iOS 應用程式可確保保護行動裝置以防網路釣魚和網路威脅。

Kaspersky Security for iOS 應用程式提供以下主要功能：

- **Web 防護**。該元件可以封鎖用於擴散惡意程式碼的惡意網站。Web 防護也可以封鎖用於偷竊使用者機密資料（例如，網路銀行或電子錢包系統的密碼）並存取使用者財務資訊的虛假（釣魚）網站。Web 防護將在您開啟網站前使用卡巴斯基安全網路雲端服務掃描網站。掃描之後，Web 防護將允許可信的網站載入並封鎖惡意網站。您可以定義群組政策的設定，以在卡巴斯基安全管理中心網頁主控台和 Cloud Console 中設定此元件。

- **破解偵測**。Kaspersky Security for iOS 偵測到破解時，這會顯示重大訊息並向您告知該問題。

關於 Kaspersky Security for Mobile (Devices) 外掛程式

Kaspersky Security for Mobile (Devices) 外掛程式提供了用於透過卡巴斯基安全管理中心網頁主控台和 Cloud Console 管理行動裝置和安裝在其上的行動應用程式的介面。Kaspersky Security for Mobile (Devices) 外掛程式允許您執行以下操作：

- 將行動裝置連線到卡巴斯基安全管理中心。

- 管理行動裝置的憑證。

- 設定 Firebase Cloud Messaging（僅適用於 Android 裝置）。

- 向行動裝置傳送命令（僅適用於 Android 裝置）。

配置卡巴斯基安全管理中心網頁主控台時可以安裝 Kaspersky Security for Mobile (Devices) 外掛程式。如果您使用的是卡巴斯基安全管理中心雲端主控台，則無需安裝此外掛程式。不同類型主控台的佈署場景，請參見「佈署場景」部分。

關於 Kaspersky Security for Mobile (Policies) 外掛程式

Kaspersky Security for Mobile (Policies) 外掛程式允許您使用群組政策為連線到卡巴斯基安全管理中心的裝置定義配置設定。Kaspersky Security for Mobile (Policies) 外掛程式可用於執行以下操作：

- 為行動裝置建立群組安全性政策。

- 遠端設定使用者行動裝置上的行動應用程式操作設定。
- 接收關於使用者行動裝置上的行動應用程式操作情況的報告和統計資料。

配置卡巴斯基安全管理中心網頁主控台時可以安裝 Kaspersky Security for Mobile (Policies) 外掛程式。如果您使用的是卡巴斯基安全管理中心雲端主控台，則無需安裝此外掛程式。不同類型主控台的佈署場景，請參見「佈署場景」部分。

硬體和軟體需求

此區段針對用來在卡巴斯基安全管理中心網頁主控台和 Cloud Console 中安裝 Kaspersky Security for Mobile (Devices) 外掛程式和 Kaspersky Security for Mobile (Policies) 外掛程式的管理員電腦，列出硬體和軟體要求，以及行動應用程式的硬體和軟體要求。

管理員電腦的硬體和軟體需求

要安裝 Kaspersky Security for Mobile (Devices) 外掛程式和 Kaspersky Security for Mobile (Policies) 外掛程式，管理員的電腦必須符合卡巴斯基安全管理中心的硬體要求。有關卡巴斯基安全管理中心的硬體和軟體要求的更多資訊：

- 如果您使用卡巴斯基安全管理中心網頁主控台，請參閱*卡巴斯基安全管理中心說明*。
- 如果您使用的是卡巴斯基安全管理中心雲端主控台，請參閱*卡巴斯基安全管理中心雲端主控台說明*。

要在卡巴斯基安全管理中心網頁主控台中使用 Kaspersky Security for Mobile (Devices) 外掛程式和 Kaspersky Security for Mobile (Policies) 外掛程式，必須在管理員的電腦上安裝卡巴斯基安全管理中心網頁主控台。

要在 Kaspersky Security Center Cloud Console 中使用 Kaspersky Security for Mobile (Devices) 外掛程式和 Kaspersky Security for Mobile (Policies) 外掛程式，您必須在 Kaspersky Security Center Cloud Console 中建立一個帳戶。有關建立帳戶的更多資訊，請參閱*卡巴斯基安全管理中心雲端主控台說明*。

Kaspersky Endpoint Security for Android 應用程式可以與下列協力廠商 EMM 系統一起運作：

- 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

支援安裝 Kaspersky Endpoint Security for Android 應用程式對使用者行動裝置的硬體和軟體要求

Kaspersky Endpoint Security for Android 應用程式具有以下硬體和軟體要求：

- 智慧手機或平板電腦的解析度為 320x480 畫素或更高
- 裝置的主記憶體具有 65 MB 的可用空間

- Android 5.0–13（包含 Android 12L，不包含 Go Edition）
- x86、x86-64、Arm5、Arm6、Arm7 或 Arm8 處理器架構

應用程式僅安裝到裝置的主記憶體。

支援安裝 Kaspersky Security for iOS 應用程式對使用者行動裝置的硬體和軟體要求

Kaspersky Security for iOS 應用程式具有下列硬體需求：

- iPhone 6S 或更高版本
- iPad Air 2 或更高版本

Kaspersky Security for iOS 應用程式具有下列軟體需求：

- iOS 14.1 或更新
- iPadOS 14.1 或更新

具有作用中 VPN 連線的 VPN 用戶端在相同的行動裝置上執行時，Kaspersky Security for iOS 應用程式無法正常操作。

已知問題和考量事項

Kaspersky Endpoint Security for Android 和 Kaspersky Security for iOS 有數個對這些應用程式的操作不會太嚴重的已知問題。

Kaspersky Security for iOS 的已知問題

- 具有作用中 VPN 連線的 VPN 用戶端在相同的行動裝置上執行時，Kaspersky Security for iOS 應用程式無法正常操作。

Kaspersky Endpoint Security for Android 的已知問題

在卡巴斯基安全管理中心網頁主控台中啟動行動裝置管理時的已知問題

- 您可以在卡巴斯基安全管理中心管理主控台根據 MMC 進行初始配置期間（在執行快速啟動精靈時）或稍後透過管理主控台中顯示行動裝置管理資料夾來啟動行動裝置管理。

安裝應用程式時的已知問題

- Kaspersky Endpoint Security for Android 僅安裝在裝置的主記憶體中。
- 在執行 Android 7.0 的裝置上，當 Kaspersky Endpoint Security for Android 被禁止覆蓋其他視窗時，試圖停用 Kaspersky Endpoint Security for Android 的管理員權限時可能發生錯誤。該問題是因一個眾所周知的 Android

7 缺陷導致。

- 在執行 Android 7.0 或更新版本的裝置上，Kaspersky Endpoint Security for Android 不支援多視窗模式。
- Kaspersky Endpoint Security for Android 與執行 Chrome 作業系統的 Chromebook 裝置不相容。
- Kaspersky Endpoint Security for Android 與執行 Android（Go Edition）作業系統的裝置不相容。
- 當將 Kaspersky Endpoint Security for Android 應用程式與協力廠商 EMM 系統（例如，VMWare AirWatch）一起使用時，僅病毒防護和 Web 防護元件可用。管理員可以在 EMM 系統主控台中配置病毒防護和 Web 防護的設定。在這種情況下，有關應用程式執行的通知僅在 Kaspersky Endpoint Security for Android 應用程式的介面（報告）中可用。

升級應用程式時的已知問題

- 您只能將 Kaspersky Endpoint Security for Android 升級至最近的應用程式版本。Kaspersky Endpoint Security for Android 不能降級至較老版本。

病毒防護操作的已知問題

- 由於技術限制，Kaspersky Endpoint Security for Android 無法掃描大小為 2 GB 或更大的檔案。在掃描期間，應用程式將略過此類別檔案，而不會通知您此類別檔案被略過。
- 要對裝置進行資訊尚未新增到病毒資料庫中的新威脅的附加分析，您必須啟用卡巴斯基安全網路。*卡巴斯基安全網路 (KSN)* 是個雲端服務基礎結構，向 Kaspersky 的線上知識庫提供檔案信譽、網路資源和軟體等資訊。若要使用 KSN，行動裝置必須已連線至網際網路。
- 在某些情況下，從行動裝置上的管理伺服器更新病毒資料庫可能會失敗。在這種情況下，請在管理伺服器上執行病毒資料庫更新工作。
- 在某些裝置上，Kaspersky Endpoint Security for Android 不會偵測透過 USB OTG 連線的裝置。無法對此類別裝置執行病毒掃描。
- 在執行 Android 11.0 或更高版本的裝置上，使用者必須授予「允許存取管理所有檔案」權限。
- 在執行 Android 7.0 或更新版本的裝置上，病毒掃描執行排程的配置視窗可能顯示不正確（管理元件未顯示）。該問題是因一個眾所周知的 Android 7 缺陷導致。
- 在執行 Android 7.0 的裝置上，於延伸模式下執行即時防護並不會偵測儲存在外部 SD 卡上的檔案威脅。
- 在執行 Android 6.0 的裝置上，Kaspersky Endpoint Security for Android 不偵測下載惡意檔案到裝置記憶體的操作。當惡意檔案執行時，或者在裝置病毒掃描過程中，惡意軟體可以被病毒防護偵測到。該問題是因一個眾所周知的 Android 6.0 缺陷導致。要確保裝置安全，建議設定排除病毒掃描。

Web 防護操作中的已知問題

- Android 裝置上的 Web 防護僅在 Google Chrome 瀏覽器（包括自訂標籤功能）、Huawei Browser 和 Samsung Internet Browser 中可用。
- 要使 Web 防護工作，您必須啟用卡巴斯基安全網路。Web 防護會基於有關網站信譽和類別的 KSN 資料封鎖網站。

- 如果透過以下方式開啟被攔截的網站，在執行 Android 6.0 並安裝 Google Chrome 51 版（或任何更早版本）的裝置上，Web 防護可能會保持解除封鎖這些網站（該問題是因一個眾所周知的 Google Chrome 缺陷導致）：
  - 透過搜尋結果。
  - 透過書簽清單。
  - 透過搜尋歷史記錄。
  - 使用網址自動填寫功能。
  - 在 Google Chrome 中的新標籤頁中開啟網站。
- 如果透過 Google 搜尋結果開啟被攔截的網站，當瀏覽器設定中啟用了「**合併標籤和應用程式**」功能時，這些網站可能在 Google Chrome 50 版（或任何更早版本）中保持解除封鎖。該問題是因一個眾所周知的 Google Chrome 缺陷導致。
- 如果使用者從其他應用程式開啟網站，例如從 IM 用戶端應用程式開啟，則封鎖類別的網站可能在 Google Chrome 中保持不被封鎖。該問題關乎可存取功能服務與 Chrome 自訂標籤功能如何配合使用。
- 如果使用者從上下文功能表或其他應用程式（例如從 IM 用戶端應用程式）以背景模式開啟網站，被攔截的網站可能在 Samsung Internet Browser 中保持不被封鎖。
- 必須將 Kaspersky Endpoint Security for Android 設定為可存取功能以確保 Web 防護能正常執行。
- 當重新整理頁面時，Samsung Internet Browser 在「**僅允許列出的網站**」Web 防護模式下可能會封鎖允許的網站。如果一般運算式包含進階設定（例如，`^https?:\/\/example\.com\/pictures\/`），則會封鎖網站。建議使用不含附加設定的一般運算式（例如，`^https?:\/\/example\.com`）。

竊盜防護操作中的已知問題

- 為了將命令及時傳送到 Android 裝置，應用會使用 Firebase Cloud Messaging (FCM) 服務。如果未設定 FCM，將僅在與卡巴斯基安全管理中心同步期間按照政策中定義的排程（例如，每 24 小時）將命令傳送到裝置。
- 要鎖定裝置，必須將 Kaspersky Endpoint Security for Android 設定為裝置管理員。
- 要鎖定執行 Android 7.0 或更高版本的裝置，必須將 Kaspersky Endpoint Security for Android 設定為可存取功能。
- 在某些裝置上，如果裝置上啟用了低電量模式，竊盜防護命令可能無法執行。此缺陷已在 Alcatel 5080X 上確認。
- 若要定位執行 Android 10.0 或更新版本的裝置，使用者必須授與「任何時間」均可存取裝置位置的權限。

應用程式控制操作中的已知問題

- 必須將 Kaspersky Endpoint Security for Android 設定為可存取功能以確保應用程式控制能正常執行。
- 要使應用程式控制（應用程式類別）工作，您必須啟用卡巴斯基安全網路。應用程式控制會基於 KSN 中可用的資料確定應用程式的類別。若要使用 KSN，行動裝置必須已連線至網際網路。對於應用程式控制，您可以將單個應用程式新增到封鎖和允許的應用程式清單。在這種情況下，無需 KSN。

- 當配置應用程式控制時，建議清除「**封鎖系統應用程式**」核取方塊。封鎖系統應用程式可能會導致裝置執行問題。

配置裝置解鎖密碼強度的已知問題

- 在執行 Android 10.0 或更高版本的裝置上，Kaspersky Endpoint Security 會將密碼強度要求解析為其中一個系統值：中度或高度。

  如果要求的密碼長度是 1 到 4 個符號，那麼應用程式會提示使用者設定中等強度的密碼。密碼必須是數字（PIN）且沒有重複或有順序（如 1234）的序列或英數字母。PIN 或密碼的長度必須至少有 4 個字元。

  如果要求的密碼長度為 5 個以上的符號，那麼應用程式會提示使用者設定高強度密碼。密碼必須是數字（PIN），沒有重複或有順序的序列或英數字母（password）。 PIN 必須至少有 8 位數，密碼長度必須至少有6個字元。

- 在執行 Android 7.1.1 的裝置上，如果解鎖密碼不符合企業安全需求（合規性控制），嘗試透過 Kaspersky Endpoint Security for Android 變更解鎖密碼時，「設定」系統應用程式可能無法正常執行。該問題是因一個眾所周知的 Android 7.1.1 缺陷 導致。這種情況下，僅可使用設定系統應用程式來變更解鎖密碼。

- 在一些執行 Android 6.0 或更新版本的裝置上，如果裝置資料被加密，輸入螢幕解鎖密碼時可能發生錯誤。該問題關乎 MIUI 韌體可存取功能服務的特定功能。

應用程式核准保護的已知問題

- 必須將 Kaspersky Endpoint Security for Android 設定為裝置管理員。

- 要防護在執行 Android 7.0 或更高版本的裝置上的應用程式不會被移除，必須將 Kaspersky Endpoint Security for Android 設定為可存取功能。

- 在某些小米和華為裝置上，Kaspersky Endpoint Security for Android 移除防護不工作。該問題是由小米上的 MIUI 7 和 8 韌體和華為上的 EMUI 韌體的特定功能導致。

設定裝置限制的已知問題

- 在執行 Android 10.0 或更高版本的裝置上，不支援禁止使用 Wi-Fi 網路。

- 在執行 Android 10.0 的裝置上，無法完全禁止使用相機。

- 在執行 Android 11 或更高版本的裝置上，必須將 Kaspersky Endpoint Security for Android 設定為可存取功能。Kaspersky Endpoint Security for Android 會提示使用者透過初始配置精靈將該應用程式設定為輔助使用功能。使用者可以略過此步驟或以後在裝置設定中停用此服務。如果是這種情況，您將無法限制相機的使用。

向行動裝置傳送命令時的已知問題

- 在執行 Android 12 或更高版本的裝置上，如果使用者授予「使用大致位置」權限，Kaspersky Endpoint Security for Android 應用程式首先會嘗試取得準確的裝置位置。如果這麼做不成功，則僅在不超過 30 分鐘前收到裝置的大致位置時才傳回該裝置的大致位置。否則，**定位裝置**命令將失敗。

特定裝置的已知問題

- 在特定裝置上（例如 Huawei、Meizu 和Xiaomi），您必須授與 Kaspersky Endpoint Security for Android 自動啟動權限或手動將其新增至與作業系統一起啟動的應用程式清單。如果未將該應用程式新增到清單，在行動裝

置重新啟動後，Kaspersky Endpoint Security for Android 會停止執行其所有功能。此外，如果裝置已鎖定，您無法使用命令解鎖裝置。您只能透過使用一次性密碼解鎖裝置。

- 在執行 Android 6.0 或更新版本的某些裝置（例如，魅族和 Asus）上，在加密資料和重啟 Android 裝置後，您必須輸入數字密碼才能解鎖裝置。如果使用者使用圖形密碼解鎖裝置，您必須將圖形密碼轉換為數字密碼。對於更多轉換圖形密碼到數字密碼的詳情，請參考行動裝置生產商的技術支援網站。該問題關乎可存取功能服務的操作。

- 在某些執行 Android 5.X 的華為裝置上，在 Kaspersky Endpoint Security for Android 設定為可存取功能後，您可能會看到一則有關缺少適當權限的錯誤訊息。若要隱藏此訊息，請在裝置設定中將該應用程式啟用為受保護的應用程式。

- 在某些執行 Android 5.X 或 6.X 的華為裝置上，當為 Kaspersky Endpoint Security for Android 啟用低電量模式時，使用者可以手動終止該應用程式。那樣之後，使用者裝置變成無防護狀態。該問題是因華為軟體的一些功能所導致。若要還原裝置防護，請手動執行 Kaspersky Endpoint Security for Android。建議您在裝置設定中停用 Kaspersky Endpoint Security for Android 的低電量模式。

- 在執行基於 Android 7.0 的 EMUI 韌體的華為裝置上，使用者可以隱藏關於 Kaspersky Endpoint Security for Android 防護狀態的通知。該問題是由於華為軟體的一些功能導致的。

- 在某些小米裝置上，當在政策中設定超過 5 個字元的密碼長度時，使用者將被提示變更螢幕解鎖密碼而不是 PIN 碼。您設定的 PIN 碼不能超過 5 個字元。該問題是由於小米軟體的一些功能導致的。

- 在執行基於 Android 6.0 的 MIUI 韌體的小米裝置上，Kaspersky Endpoint Security for Android 圖示可能在狀態列中隱藏。該問題是由於小米軟體的一些功能所導致。建議您在「通知」設定中允許顯示通知圖示。

- 在一些執行 Android 6.0.1 的 Nexus 裝置上，正常操作所需的權限無法透過 Kaspersky Endpoint Security for Android 快速啟動精靈授予。該問題由眾所周知的 Google 的 Android 安全修補程式缺陷導致。為確保正常執行，必須在裝置設定中手動授予所需權限。

- 在某些執行 Android 7.0 或更高版本的 Samsung 裝置上，當使用者嘗試配置不受支援的方法（例如，圖形密碼）來解鎖裝置時，如果滿足以下條件，裝置可能會鎖定：Kaspersky Endpoint Security for Android 移除防護已啟用並且設定了螢幕解鎖密碼長度要求。要解鎖裝置，您必須傳送特殊命令到裝置。

- 在某些 Samsung 裝置上，無法封鎖使用指紋解鎖螢幕。

- 如果裝置連線到 3G/4G 網路，啟用了低電量模式並限制背景資料，Web 防護無法在一些 Samsung 裝置上啟用。建議您在「低電量」設定中停用「限制背景資料」的功能。

- 在某些 Samsung 裝置上，如果解鎖密碼不符合企業安全需求，Kaspersky Endpoint Security for Android 不會封鎖使用指紋解鎖螢幕。

- 在某些榮耀和華為裝置上，您無法限制藍牙的使用。當 Kaspersky Endpoint Security for Android 試圖限制藍芽使用時，作業系統顯示包含拒絕或允許該限制的選項的通知。使用者可以拒絕該限制並繼續使用藍牙。

- 在 Blackview 裝置上，使用者可以清除 Kaspersky Endpoint Security for Android 應用程式的記憶體。因此，裝置防護和管理被停用，所有定義的設定都變得無效，並且 Kaspersky Endpoint Security for Android 應用程式將從輔助功能中刪除。這是因為該供應商的裝置提供了具有提升權限的可自訂最近畫面的應用程式。此應用程式可以覆寫 Kaspersky Endpoint Security for Android 設定並且無法替換，因為它是 Android 作業系統的一部分。

- 在某些執行 Android 11 的裝置上，Kaspersky Endpoint Security for Android 應用程式在啟動後立即當機。該問題是因一個眾所周知的 Android 11 缺陷 導致。

在 Android 13 上操作應用程式的已知問題

- 在 Android 13，使用者可以使用前景服務工作管理員阻止 Kaspersky Endpoint Security 在背景中執行。這是因一個眾所周知的 Android 13 問題 導致。
- 在 Android 13，初始應用程式設定開始時，會請求傳送通知的權限。這是由於 Android 13 作業系統的詳細規格。

在卡巴斯基安全管理中心網頁主控台或雲端主控台中佈署行動裝置管理解決方案

要使用卡巴斯基安全管理中心網頁主控台或雲端主控台管理行動裝置，您必須佈署行動裝置管理解決方案。

佈署場景

在卡巴斯基安全管理中心網頁主控台中佈署

在卡巴斯基安全管理中心網頁主控台中佈署行動裝置管理解決方案包括以下步驟：

1. **準備卡巴斯基安全管理中心網頁主控台以進行佈署**
2. **佈署管理外掛程式**
3. **佈署行動應用程式**
4. **（可選，僅適用於 Android）設定與 Firebase Cloud Messaging 交換的資訊**

   建議執行此步驟以確保在變更政策設定時，及時將命令傳遞到行動裝置並強制同步。

在卡巴斯基安全管理中心雲端主控台中佈署

在卡巴斯基安全管理中心雲端主控台中佈署行動裝置管理解決方案包括以下步驟：

1. **準備卡巴斯基安全管理中心雲端主控台以進行佈署**
2. **佈署行動應用程式**
3. **（可選，僅適用於 Android）設定與 Firebase Cloud Messaging 交換的資訊**

   建議執行此步驟以確保在變更政策設定時，及時將命令傳遞到行動裝置並強制同步。

準備卡巴斯基安全管理中心網頁主控台和雲端主控台以進行佈署

本節提供有關準備卡巴斯基安全管理中心網頁主控台和雲端主控台以進行佈署的說明。

配置連線行動裝置的管理伺服器

為了使行動裝置能夠連線到管理伺服器，在行動裝置上安裝 Kaspersky Endpoint Security for Android 應用程式或 Kaspersky Security for iOS 應用程式之前，您必須在管理伺服器屬性中定義行動裝置連線設定。

為行動裝置連線定義管理伺服器設定：

1. 在管理伺服器中啟動行動裝置管理。

   您可以在卡巴斯基安全管理中心管理主控台根據 MMC 進行初始配置期間（在執行快速啟動精靈時）或稍後透過管理主控台中顯示行動裝置管理資料夾來啟動行動裝置管理。

2. 在卡巴斯基安全管理中心網頁主控台或雲端主控台的主視窗中，點擊**設定**（ ）。

   「管理伺服器內容」視窗將開啟。

3. 配置行動裝置將使用的管理伺服器連接埠：

   a. 選擇**其他連結埠**區域。

   b. 啟用**開啟行動裝置連接埠**的切換按鈕。

   c. 在**行動裝置連接埠同步**欄位中，指定行動裝置連線至管理伺服器的連接埠。

   預設情況下使用 13292 連接埠。

   如果關閉**開啟行動裝置連接埠**切換按鈕，或者指定的連接埠錯誤，行動裝置將無法連線至管理伺服器。

   d. 請在**行動裝置啟動連接埠**欄位中，指定行動裝置用於連線到管理伺服器以啟動行動應用程式的連接埠。

   預設情況下使用 17100 連接埠。

   如果您指定了錯誤的連線連接埠，行動裝置使用者將無法使用管理伺服器啟用行動應用程式。

4. 如有必要，編輯將用於連線到管理伺服器的行動裝置憑證。

   預設情況下，管理伺服器會使用在管理伺服器安裝期間建立的憑證。如有需要，請將透過管理伺服器簽發的憑證替換為另一個憑證或重新簽發透過管理伺服器簽發的憑證。

   編輯憑證：

   a. 選擇**憑證**區域。

   b. 定義所需的設定。

   有關憑證的詳細資訊，請參閱*卡巴斯基安全管理中心說明*。

5. 點擊**儲存**按鈕以儲存對設定所做的變更並結束管理伺服器內容視窗。

配置行動裝置連線設定後，您可以在行動裝置上安裝 Kaspersky Endpoint Security for Android 應用程式或 Kaspersky Security for iOS 應用程式，並使用指定的設定將它們連線到管理伺服器。

建立管理群組

群組政策是為了供使用者行動裝置上安裝之 Kaspersky Endpoint Security for Android 和 Kaspersky Security for iOS 應用程式進行集中配置之用。

若要將政策套用於裝置群組，建議您在使用者裝置上安裝行動應用程式之前，先在**受管理裝置**上為這些裝置建立單獨的群組。

建立管理群組後，建議配置此選項以將要安裝應用程式的裝置自動分配到此群組。然後使用群組政策配置所有裝置通用的設定。

若要建立管理群組：

1. 在卡巴斯基安全管理中心網頁主控台或雲端主控台的主視窗中，選取**裝置** > **群組階層**。
2. 在管理群組結構中，選取要包括新管理群組的管理群組。
3. 按一下**新增**按鈕。
4. 在開啟的**新管理群組名稱**視窗中，輸入群組的名稱，然後點擊**新增**按鈕。

   具有指定名稱的新管理群組將出現在管理群組階層結構中。

為自動分配裝置至管理群組建立規則

當 Kaspersky Endpoint Security for Android 應用程式或 Kaspersky Security for iOS 應用程式安裝在行動裝置上時，它們會顯示在卡巴斯基安全管理中心網頁主控台或 Cloud Console 的**發現與佈署** > **未分配的裝置**頁面上。為了管理新連線的裝置，您可以手動將它們移動到管理群組或建立規則以將它們自動分配到管理群組。

要建立將行動裝置自動分配給管理群組的規則：

1. 在卡巴斯基安全管理中心網頁主控台或雲端主控台的主視窗中，選取**發現與佈署** > **佈署與分配** > **移動規則**。
2. 在開啟的**新規則**視窗中，點擊**新增**按鈕。
3. 在**規則名稱**欄位中，指定規則名稱。
4. 在**管理群組**欄位中，安裝應用程式之後，選取應將行動裝置分配到的管理群組。
5. 在**套用規則**區域中，選擇**為每個裝置執行一次**。
6. 選取**僅移動未新增至管理群組的裝置**核取方塊，防止在套用規則時移動分配到其他管理群組的行動裝置。
7. 選取**啟用規則**核取方塊，以在建立規則後立即應用該規則。

   您可以在以後隨時使用**移動規則**頁面上的切換按鈕啟用該規則。
8. 選取**規則條件** > **應用程式**並執行以下操作：
   a. 啟用**作業系統版本**切換按鈕。
   b. 在開啟的作業系統清單中，選取 **Android** 或 **iOS**。

   該規則將套用於對應的裝置。您必須至少指定一個條件才能建立規則。
9. 點擊**儲存**以建立規則。

新建立的規則會顯示在**移動規則**頁面上。根據規則，卡巴斯基安全管理中心會將所有新連線的裝置分配到選定的管理群組。

有關未分配裝置之管理群組的管理和操作詳細資訊：

- 如果您使用卡巴斯基安全管理中心網頁主控台，請參閱*卡巴斯基安全管理中心說明*。
- 如果您使用的是卡巴斯基安全管理中心雲端主控台，請參閱*卡巴斯基安全管理中心雲端主控台說明*。

佈署管理外掛程式

要在卡巴斯基安全管理中心網頁主控台中管理行動裝置，必須安裝以下管理外掛程式：

- Kaspersky Security for Mobile (Devices) 外掛程式
- Kaspersky Security for Mobile (Policies) 外掛程式

如果您使用的是卡巴斯基安全管理中心雲端主控台，則無需安裝管理外掛程式。您只需要在卡巴斯基安全管理中心雲端主控台中建立一個帳戶。有關建立帳戶的更多資訊，請參閱*卡巴斯基安全管理中心雲端主控台說明*。

您可以使用以下方法安裝管理外掛程式：

- 透過使用卡巴斯基安全管理中心網頁主控台的快速啟動精靈。

  卡巴斯基安全管理中心網頁主控台會在初次連線時，自動提示您在安裝管理伺服器後執行快速啟動精靈。您也可以隨時手動啟動快速啟動精靈。

  如需卡巴斯基安全管理中心快速啟動精靈的更多資訊，請參閱*卡巴斯基安全管理中心說明*。

- 透過使用卡巴斯基安全管理中心網頁主控台中的可用分發套件清單。

  推出新版 Kaspersky 應用程式後，可用分發套件清單會自動更新。

- 從外部來源下載分發套件並將管理外掛程式新增到卡巴斯基安全管理中心網頁主控台。

  例如，您可在卡巴斯基網站上下載管理外掛程式的分發套件。

從可用分發套件清單安裝管理外掛程式

若要安裝管理外掛程式：

1. 在卡巴斯基安全管理中心網頁主控台的主視窗中，選取**主控台設定** > **WEB 外掛程式**。
2. 按一下**新增**按鈕。

   這會開啟 Kaspersky 應用程式的最新版本清單。
3. 安裝管理外掛程式：
   a. 在可用應用程式清單中，按一下**行動裝置**區域將其展開。
   b. 選取 **Kaspersky Security for Mobile (Devices)** 外掛程式，然後按一下**安裝外掛程式**。
   c. 選取 **Kaspersky Security for Mobile (Policies)**，然後按一下**安裝外掛程式**。

下載分發套件並安裝外掛程式。當每個外掛程式安裝並新增到卡巴斯基安全管理中心網頁主控台時，會顯示一個確認視窗。

從分發套件下載管理外掛程式

您可以在卡巴斯基網站上下載分發套件。

從分發套件安裝 Kaspersky Security for Mobile (Devices) 外掛程式：

1. 將 `plugin.zip` 和 `signature.txt` 檔案從分發套件的 `on_prem_ksm_devices_xx.x.x.x.zip` 存檔複製到管理員的工作站。
2. 在卡巴斯基安全管理中心網頁主控台的主視窗中，選取**主控台設定** > **WEB 外掛程式**。
3. 點擊**從檔案新增**。
4. 在開啟的**從檔案新增**視窗中，按一下**上傳 ZIP 檔案**，然後瀏覽 `plugin.zip`。
5. 點擊**上傳簽名檔**，然後瀏覽 `signature.txt`。
6. 按一下**新增**按鈕。

Kaspersky Security for Mobile (Devices) 外掛程式已安裝並新增到卡巴斯基安全管理中心網頁主控台。

從分發套件安裝 Kaspersky Security for Mobile (Policies) 外掛程式：

1. 將 `plugin.zip` 和 `signature.txt` 檔案從分發套件的 `on_prem_ksm_policies_xx.x.x.x.zip` 存檔複製到管理員的工作站。
2. 在卡巴斯基安全管理中心網頁主控台的主視窗中，選取**主控台設定** > **WEB 外掛程式**。
3. 點擊**從檔案新增**。
4. 在開啟的**從檔案新增**視窗中，按一下**上傳 ZIP 檔案**，然後瀏覽 `plugin.zip`。
5. 點擊**上傳簽名檔**，然後瀏覽 `signature.txt`。
6. 按一下**新增**按鈕。

Kaspersky Security for Mobile (Policies) 外掛程式已安裝並新增到卡巴斯基安全管理中心網頁主控台。

您可以透過查看**主控台設定** > **WEB 外掛程式**頁面上已安裝的外掛程式清單，來確保已安裝管理外掛程式。

佈署行動應用程式

要在卡巴斯基安全管理中心網頁主控台或 Cloud Console 中管理行動裝置，您必須在行動裝置上佈署 Kaspersky Endpoint Security for Android 應用程式或 Kaspersky Security for iOS 應用程式。您可以使用卡巴斯基安全管理中心網頁主控台或 Cloud Console 在行動裝置上佈署應用程式。

使用卡巴斯基安全管理中心網頁主控台或 Cloud Console 佈署行動應用程式

對於已新增到卡巴斯基安全管理中心的使用者帳戶，系統會將行動應用程式佈署到該帳戶使用者的行動裝置上。如需更多卡巴斯基安全管理中心的使用者帳戶資訊：

- 如果您使用卡巴斯基安全管理中心網頁主控台，請參閱*卡巴斯基安全管理中心說明*。
- 如果您使用的是卡巴斯基安全管理中心雲端主控台，請參閱*卡巴斯基安全管理中心雲端主控台說明*。

您可以透過向行動裝置傳送安裝連結，使用 Kaspersky Security for Mobile (Devices) 外掛程式，從卡巴斯基安全管理中心網頁主控台和 Cloud Console 安裝應用程式。

- 在 Android 裝置上，使用者會接收 Google Play 連結以下載 Kaspersky Endpoint Security for Android 應用程式。可透過執行 Android 平台的標準安裝程式，安裝該應用程式。安裝應用程式後，使用者必須提供所需的權限。

  有些 Huawei 和 Honor 裝置沒有 Google 服務，因此沒有 Google Play 應用程式的存取權限。如果部分 Huawei 和 Honor 裝置的使用者無法從 Google Play 安裝應用程式，請指導他們從 Huawei App Gallery 安裝應用程式。

- 在 iOS 裝置上，使用者會接收 App Store 連結，以下載 Kaspersky Security for iOS 應用程式。可透過執行 iOS 平台的標準安裝程式，安裝該應用程式。

  連線 iOS 裝置之前，請將卡巴斯基安全管理中心的位址傳送至裝置使用者，以改善連線安全性。使用者將會在應用程式安裝期間查看此位址，若顯示的位址不符合您傳送的位址，可以取消連線。

該連結內含以下資料：

- 卡巴斯基安全管理中心同步設定
- 一般憑證

若要在行動裝置上佈署應用程式：

1. 啟動行動裝置連線精靈：
   - 在卡巴斯基安全管理中心網頁主控台或雲端主控台的主視窗中，選取**裝置** > **行動** > **裝置**，然後點擊**新增**。
   - 在卡巴斯基安全管理中心網頁主控台或雲端主控台的主視窗中，選取**使用者和角色** > **使用者**。點擊要向其傳送連線行動裝置連結的使用者或使用者群組名稱，然後選取**裝置**。按一下**新增行動裝置**。在此情況下，略過步驟 3。

   使用**下一步**按鈕繼續完成精靈。
2. 選取要新增之裝置的作業系統：
   - **Android**
   - **iOS 和 iPadOS**

3. 選取您要向其傳送連線行動裝置連結的使用者或使用者群組。

4. 選取要傳送連結的電子郵件地址：

   - **所有電子郵件信箱**
   - **主要電子郵件信箱**
   - **替代電子郵件信箱**
   - **其他電子郵件信箱**

     如果選取此選項，請在下面指定電子郵件地址。

5. 隨即顯示連結摘要。

   確保該連結的所有參數都正確，然後按一下**傳送**。

6. 將開啟一個視窗，確認已傳送新增行動裝置的連結。

   按一下**確定**以完成精靈。

使用者安裝 Kaspersky Endpoint Security for Android 應用程式或 Kaspersky Security for iOS 應用程式後，使用者的裝置將會顯示在網頁主控台或 Cloud Console 的**裝置** > **行動** > **裝置**索引標籤。在使用者的行動裝置上安裝應用程式後，您將能夠使用群組政策進行裝置和應用程式的設定。如果裝置遺失或被竊，您還可以向行動裝置傳送命令（僅適用於Android）以便防護資料。

啟用行動應用程式

卡巴斯基安全管理中心產品授權可應用於不同群組的功能。為了確保 Kaspersky Endpoint Security for Android 應用程式和 Kaspersky Security for iOS 應用程式完全正常執行，組織購買的卡巴斯基安全管理中心產品授權必須提供**行動裝置管理**功能。**行動裝置管理**功能旨在將行動裝置連線到卡巴斯基安全管理中心並管理它們。

有關卡巴斯基安全管理中心產品授權和產品授權選項的詳細資訊：

- 如果您使用卡巴斯基安全管理中心網頁主控台，請參閱*卡巴斯基安全管理中心說明*。
- 如果您使用的是卡巴斯基安全管理中心雲端主控台，請參閱*卡巴斯基安全管理中心雲端主控台說明*。

在行動裝置上啟用 Kaspersky Endpoint Security for Android 應用程式或 Kaspersky Security for iOS 應用程式是透過向應用程式提供有效的產品授權資訊來完成的。當裝置與卡巴斯基安全管理中心同步時，產品授權資訊將與政策一起傳遞到行動裝置。

如果在行動裝置上安裝行動應用程式之後 30 天內未完成行動應用程式的啟用，應用程式將自動轉換至受限功能模式。在此模式中，大部分應用程式元件都無法執行。當轉換到受限功能模式時，應用程式將停止執行與卡巴斯基安全管理中心的自動同步。因此，如果未在應用程式安裝後 30 天內完成應用程式啟用，使用者必須手動與卡巴斯基安全管理中心同步裝置。

如果您的組織中未佈署卡巴斯基安全管理中心或行動裝置無法存取卡巴斯基安全管理中心，使用者可以在其裝置上手動啟動行動應用程式。

若要啟用行動應用程式：

1. 開啟政策內容視窗：

   - 在卡巴斯基安全管理中心網頁主控台或雲端主控台的主視窗中，選取**裝置** > **政策和設定檔**。在開啟的群組政策清單中，點擊要配置的政策名稱。

- 在卡巴斯基安全管理中心網頁主控台或雲端主控台的主視窗中，選取**裝置 > 行動 > 裝置**。點擊您要設定政策的行動裝置，然後在**使用中的政策和政策設定檔**標籤上選取該政策。

2. 在政策內容頁面中，選取**應用程式設定 > 產品授權**。

3. 使用下拉清單從管理伺服器的金鑰儲存空間中選取所需的產品授權金鑰。

   產品授權金鑰的詳細資訊會顯示在下面的欄位中。

   如果行動裝置上現有的啟用金鑰與上面下拉清單中選取的金鑰不同，您可以替換它。為此，請選定**如裝置上的金鑰不同，請使用特定金鑰取代**核取方塊。

4. 點擊**儲存**按鈕儲存對政策所做的變更並結束政策內容視窗。

下次與卡巴斯基安全管理中心執行裝置同步之後，可進行行動裝置設定。

為 Kaspersky Endpoint Security for Android 應用程式提供所需的權限

Kaspersky Endpoint Security for Android 應用程式的某些功能需要權限。Kaspersky Endpoint Security for Android 會在安裝期間以及安裝之後和使用應用程式的各個功能之前要求強制授權。如果未提供必需權限，將無法安裝 Kaspersky Endpoint Security for Android。

在某些裝置（例如 Huawei、Meizu 和 Xiaomi）上，您必須手動將 Kaspersky Endpoint Security for Android 新增到會與作業系統同時啟動的應用程式清單。如果未將該應用程式新增到清單，在行動裝置重新啟動後，Kaspersky Endpoint Security for Android 會停止執行其所有功能。

在執行 Android 11 或更高版本的裝置上，您必須停用「**如果不使用應用程式時刪除權限**」系統設定。否則，在幾個月未使用該應用程式後，系統會自動重設使用者授予該應用程式的權限。

Kaspersky Endpoint Security for Android 應用程式所要求的權限

權限	應用程式功能
手機（適用於 Android 5.0–9.X）	連線到卡巴斯基安全管理中心（裝置 ID）
儲存空間（必填）	病毒防護
存取以管理所有檔案（適用於 Android 11 或更高版本）	病毒防護
鄰近藍牙裝置（僅適用於 Android 12 或更高版本）	限制使用藍芽
通知（適用於 Android 13）	向使用者通知安全性問題和應用程式事件
允許在背景中執行（適用於 Android 12 或更高版本）	確保持續操作應用程式。若未授予權限，應用程式可能會從記憶體卸載且無法重新啟動。
裝置管理員（必	竊盜防護 – 鎖定裝置（僅適用於 Android 5.0–6.X）

需）	竊盜防護 – 使用前置相機拍攝臉部快照 儘管卡巴斯基安全管理中心網頁主控台和雲端主控台不支援拍攝臉部快照，但 Kaspersky Endpoint Security for Android 應用程式需要此權限，以便所有卡巴斯基安全管理中心主控台都可以對其進行管理。
	竊盜防護 – 發出警報
	竊盜防護 – 還原出廠設定
	密碼防護
	應用程式移除防護
	安裝安全憑證
	應用程式控制
	限制使用攝影鏡頭、藍芽和 Wi-Fi
攝影鏡頭	竊盜防護 – 使用前置相機拍攝臉部快照 儘管卡巴斯基安全管理中心網頁主控台和雲端主控台不支援拍攝臉部快照，但 Kaspersky Endpoint Security for Android 應用程式需要此權限，以便所有卡巴斯基安全管理中心主控台都可以對其進行管理。 在執行 Android 11.0 或更新版本的裝置上，使用者在收到提示時必須授與「使用應用程式期間」的權限。
定位	竊盜防護 – 定位裝置 在執行 Android 10.0 或更新版本的裝置上，使用者在收到提示時必須授予「任何時間」均可存取裝置位置的權限。
可存取功能	竊盜防護 – 鎖定裝置（僅適用於 Android 7.0 或更高版本）
	Web 防護
	應用程式控制
	應用程式移除防護（僅適用於 Android 7.0 或更高版本）
	顯示 Kaspersky Endpoint Security for Android 的警告（僅適用於 Android 10.0 或更高版本）
	限制使用相機（僅適用於 Android 11 或更高版本）

管理憑證

行動憑證可用來識別管理伺服器上行動裝置的使用者。

卡巴斯基安全管理中心網頁主控台和雲端主控台允許您以使用者行動憑證執行以下操作：

- 查看憑證及其狀態。
- 建立新憑證。
- 更新即將到期的憑證。
- 刪除憑證。

有關卡巴斯基安全管理中心憑證的更多資訊：

- 如果您使用卡巴斯基安全管理中心網頁主控台，請參閱*卡巴斯基安全管理中心說明*。
- 如果您使用的是卡巴斯基安全管理中心雲端主控台，請參閱*卡巴斯基安全管理中心雲端主控台說明*。

查看憑證清單

卡巴斯基安全管理中心網頁主控台和雲端主控台允許您查看套用的使用者行動憑證、其狀態和屬性。

查看套用的使用者行動憑證清單：

1. 在卡巴斯基安全管理中心網頁主控台或雲端主控台的主視窗中，選取**裝置** > **行動** > **裝置**。
2. 選取**管理憑證**。

   行動憑證頁面隨即開啟，其中包含有關套用的使用者行動憑證資訊。您可以透過在**使用者名稱**欄位中點擊憑證來查看憑證的詳細資訊。

定義憑證設定

您可以使用卡巴斯基安全管理中心網頁主控台或雲端主控台配置行動憑證的生命週期、自動更新和密碼防護。

定義行動憑證設定：

1. 在卡巴斯基安全管理中心網頁主控台或雲端主控台的主視窗中，選取**裝置** > **行動** > **裝置**。
2. 選取**管理憑證**。
3. 選取**憑證設定**。
4. 在開啟的**產生行動憑證**視窗中，您可以配置以下內容：

   - **憑證有效期（天）**

     憑證的生命週期期間，以天為單位。憑證的預設生命週期為 365 天。當此期限到期時，行動裝置將無法連線到管理伺服器。

   - **憑證於後續天數到期後更新**

     管理伺服器在目前憑證到期之前應簽發新憑證的剩餘天數。例如，如果該欄位的值為 4，則管理伺服器會在目前憑證到期前四天簽發新憑證。預設值是 1。

- **自動補發憑證（如有可能）**

  如果可能，憑證將自動重新簽發。如果停用此選項，則必須在憑證到期時手動重新簽發憑證。預設情況下，此選項處於停用狀態。

- **憑證安裝期間提示密碼**

  當憑證安裝在行動裝置上時，將提示使用者輸入密碼。密碼僅使用一次 — 在行動裝置上安裝憑證期間。密碼將由管理伺服器自動產生並透過電子郵件傳送給使用者。您可以在**密碼長度**欄位中指定密碼長度。

5. 點擊**儲存**以套用變更並關閉視窗。

卡巴斯基安全管理中心將使用指定的設定來建立、更新和防護行動憑證。

建立一個憑證

您可以在卡巴斯基安全管理中心網頁主控台和雲端主控台中建立行動憑證，以識別行動裝置的使用者。

要建立行動憑證：

1. 在卡巴斯基安全管理中心網頁主控台或雲端主控台的主視窗中，選取**裝置 > 行動 > 裝置**。
2. 選取**管理憑證**。
3. 在開啟的**行動憑證**視窗中，點擊**新增**以啟動**行動憑證建立精靈**。使用**下一步**按鈕繼續完成精靈。
4. 選擇要使用新憑證管理其行動裝置的使用者或使用者群組。
5. 指定**發佈參數**：
   - 如果要通知使用者有關新憑證的資訊，請選取**通知使用者新憑證的相關資訊**核取方塊。
   - 如果您希望允許在同一裝置上多次使用一個憑證，請選取**允許在相同裝置上多次使用一個憑證 (僅適用於已安裝 Kaspersky Endpoint Security for Android 的裝置)**核取方塊。
6. 選取**身分驗證類型**：
   - 如果您希望使用者使用其憑據存取憑證，請選取**憑證 (網域登入或使用者名稱)**。
   - 如果您希望使用者使用一次性密碼來存取憑證，選取**一次性密碼**。

     如果您沒有在上一步中選取**允許在相同裝置上多次使用一個憑證 (僅適用於已安裝 Kaspersky Endpoint Security for Android 的裝置)**核取方塊，則此選項可用。
   - 如果您希望使用者透過使用密碼來存取憑證，選取**密碼**。

     如果您在上一步中選取了**允許在相同裝置上多次使用一個憑證 (僅適用於已安裝 Kaspersky Endpoint Security for Android 的裝置)**核取方塊，則此選項可用。
7. 在**憑證傳輸**欄位中指定憑證傳送方法：
   - 如果您在上一步中選取了**一次性密碼**，請選取以下選項之一：
     - 如果您想透過電子郵件傳送密碼，請選取**透過電子郵件通知使用者**。

       然後選取要使用的電子郵件地址或**其他電子郵件信箱**以指定另一個電子郵件地址。
     - 如果您想透過其他方式通知使用者密碼，請選取**完成精靈後顯示密碼**。

- 如果您在上一步選取了**憑證 (網域登入或使用者名稱)**，請選取要使用的電子郵件地址或選取**其他電子郵件信箱**以指定另一個電子郵件地址。

8. 隨即顯示憑證摘要。

   確保所有的參數都正確，然後點擊**建立**。

這樣，**行動憑證建立精靈**會建立使用者可以安裝在行動裝置上的一般憑證。該憑證在下一次行動裝置與卡巴斯基安全管理中心同步後可用。

有關建立憑證和配置簽發憑證之規則的更多資訊：

- 如果您使用卡巴斯基安全管理中心網頁主控台，請參閱*卡巴斯基安全管理中心說明*。
- 如果您使用的是卡巴斯基安全管理中心雲端主控台，請參閱*卡巴斯基安全管理中心雲端主控台說明*。

更新憑證

如果有任何套用的行動憑證即將過期，您可以使用卡巴斯基安全管理中心網頁主控台或雲端主控台進行更新。

要更新行動憑證：

1. 在卡巴斯基安全管理中心網頁主控台或雲端主控台的主視窗中，選取**裝置** > **行動** > **裝置**。
2. 選取**管理憑證**。
3. 選擇要更新的憑證，然後點擊**補發**。

   憑證狀態會變更為**已補發憑證**。

刪除憑證

您可以使用卡巴斯基安全管理中心網頁主控台或雲端主控台刪除行動憑證。

若刪除行動憑證，裝置將無法再與管理伺服器同步，並且無法透過卡巴斯基安全管理中心進行管理。要再次開始管理行動裝置，您需要在其上重新安裝 Kaspersky Endpoint Security for Android 應用程式。

刪除行動憑證：

1. 在卡巴斯基安全管理中心網頁主控台或雲端主控台的主視窗中，選取**裝置** > **行動** > **裝置**。
2. 選取**管理憑證**。
3. 選取要刪除的憑證，然後點擊**刪除**。

   憑證會被刪除並從憑證清單中移除。

與 Firebase Cloud Messaging 交換資訊

Kaspersky Endpoint Security for Android 使用 Firebase Cloud Messaging (FCM) 服務以確保向行動裝置的命令傳送並在政策設定被變更時強制同步。

要使用 Firebase Cloud Messaging 服務，您必須在卡巴斯基安全管理中心網頁主控台或雲端主控台定義服務設定。

要在卡巴斯基安全管理中心網頁主控台或雲端主控台中啟用 Firebase Cloud Messaging：

1. 在卡巴斯基安全管理中心網頁主控台或雲端主控台的主視窗中，選取**裝置** > **行動** > **ANDROID 裝置同步**。
   Android 裝置同步視窗隨即開啟。
2. 在**傳送者 ID** 和**伺服器金鑰**欄位中，指定 Firebase Cloud Messaging 設定：SENDER_ID 和 API 金鑰。

Firebase Cloud Messaging 隨即啟用。

要取得寄件者 ID 和伺服器金鑰：

1. 在Google 入口網站上註冊。
2. 前往 Google Cloud 平台。
3. 建立一個新專案。
   等待專案建立完成。
4. 找到專案的相關 SENDER_ID。
5. 為 Android 啟用 Google Firebase Cloud Messaging。
6. 按照螢幕上的說明建立憑證。
7. 從新建立的憑證屬性中檢索 API 金鑰。

Google Cloud 平台操作的詳細資訊請參考其文件。

您現在有一個**傳送者 ID** 和一個**伺服器金鑰**來配置 Firebase Cloud Messaging 設定。

如果未定義 Firebase Cloud Messaging 設定，當行動裝置根據政策中設定的排程（例如，每 24 小時一次）與卡巴斯基安全管理中心同步時，裝置上的命令和政策設定將被傳送。換句話說，命令和政策設定將被延遲傳送。

出於支援產品主要功能的目的，您同意自動提供 Firebase Cloud Messaging 服務應用安裝的獨一 ID（實例 ID）以及以下資料：

- 已安裝軟體的資訊：應用版本、應用 ID、應用版本號、應用套件名稱。
- 安裝了軟體的電腦資訊：OS 版本、裝置 ID、Google 服務版本。
- FCM 資訊：FCM 中應用 ID、FCM 使用者 ID、協議版本。

資料透過安全連線傳輸到 Firebase 服務。資訊的存取和防護受 Firebase 服務的以下相關使用條款監管：Firebase 資料處理和安全條款、Firebase 中的隱私和安全。

封鎖與 Firebase Cloud Messaging 服務交換資訊：

1. 在卡巴斯基安全管理中心網頁主控台或雲端主控台的主視窗中，選取**裝置** > **行動** > **ANDROID 裝置同步**。

Android 裝置同步視窗隨即開啟。

2. 點擊**重設**。

3. 在開啟的視窗中，點擊**確定**按鈕以確認重設。

Firebase Cloud Messaging 設定已清除。

卡巴斯基安全管理中心網頁主控台和雲端主控台中的行動裝置管理

您可以在卡巴斯基安全管理中心網頁主控台和 Cloud Console 中透過使用群組政策和向行動裝置傳送命令（僅適用於 Android）來管理行動裝置。

要在卡巴斯基安全管理中心網頁主控台中管理行動裝置，您必須安裝管理外掛程式。

將行動裝置連線到卡巴斯基安全管理中心

要使用卡巴斯基安全管理中心網頁主控台或雲端主控台管理行動裝置，裝置必須連線到卡巴斯基安全管理中心。您可以在網頁主控台或雲端主控台的**裝置 > 行動 > 裝置**標籤上，查看連線到卡巴斯基安全管理中心的行動裝置清單。

連線 iOS 裝置之前，請將卡巴斯基安全管理中心的位址傳送至裝置使用者，以改善連線安全性。使用者將會在應用程式安裝期間查看此位址，若顯示的位址不符合您傳送的位址，可以取消連線。

要連線行動裝置到卡巴斯基安全管理中心：

1. 啟動行動裝置連線精靈：

   - 在卡巴斯基安全管理中心網頁主控台或雲端主控台的主視窗中，選取**裝置 > 行動 > 裝置**，然後點擊**新增**。
   - 在卡巴斯基安全管理中心網頁主控台或雲端主控台的主視窗中，選取**使用者和角色 > 使用者**。點擊要向其傳送連線行動裝置連結的使用者或使用者群組名稱，然後選取**裝置。**按一下**新增行動裝置**。在此情況下，略過步驟 3。

   使用**下一步**按鈕繼續完成精靈。

2. 選取要新增之裝置的作業系統：

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

3. 選取您要向其傳送連線行動裝置連結的使用者或使用者群組。

4. 選取要傳送連結的電子郵件地址：

   - **所有電子郵件信箱**
   - **主要電子郵件信箱**

- **替代電子郵件信箱**
- **其他電子郵件信箱**

  如果選取此選項，請在下面指定電子郵件地址。

5. 隨即顯示連結摘要。

   確保該連結的所有參數都正確，然後按一下**傳送**。

6. 將開啟一個視窗，確認已傳送新增行動裝置的連結。

   按一下**確定**以完成精靈。

當使用者安裝 Kaspersky Endpoint Security for Android 應用程式或 Kaspersky Security for iOS 應用程式時，使用者的裝置將顯示在網頁主控台或 Cloud Console 的**裝置** > **行動** > **裝置**標籤上。

將未分配的行動裝置移至管理群組

當 Kaspersky Endpoint Security for Android 應用程式或 Kaspersky Security for iOS 應用程式安裝在行動裝置上時，它們會顯示在卡巴斯基安全管理中心網頁主控台或 Cloud Console 的**發現與佈署** > **未分配的裝置**頁面上。為了管理新連線的裝置，您可以為它們自動分配到管理群組建立規則或手動將它們移動到管理群組。

要將未分配的行動裝置移至管理群組：

1. 在卡巴斯基安全管理中心網頁主控台或雲端主控台的主視窗中，選取**發現與佈署** > **未分配的裝置**。
2. 選取要移至管理群組的裝置，然後點擊**移至群組**。
3. 在開啟的管理群組樹狀結構中，選取要將裝置移動到哪個目標群組。

   您可以透過選取現有群組，然後點擊**新增子群組**來建立新的管理群組。

4. 點擊**移動**。

裝置會被移動到指定的管理群組並且套用群組政策。

傳送命令至行動裝置

您可以向 Android 行動裝置傳送命令以保護遺失或被竊之行動裝置上的資料，或者強制執行行動裝置與卡巴斯基安全管理中心的同步。

您無法向 iOS 裝置 傳送命令。

支援下列命令：

- **裝置鎖定**

  行動裝置將被鎖定。

- **解除封鎖裝置**

  行動裝置已解鎖。解鎖執行著 Android 5.0 – 6.X 的行動裝置後，螢幕解鎖密碼 (PIN code) 重設為「1234」。解鎖執行著 Android 7.0 或更新版本的裝置後，螢幕解鎖密碼不變。

- **還原出廠設定**

所有資料都將從行動裝置中刪除，設定將回溯至其預設值。

- **抹除企業資料**

  容器化資料和公司電子郵件帳戶將從行動裝置中抹除。

- **定位裝置**

  裝置將被定位並顯示在 Google Maps 中。行動服務提供商可能會收取網際網路存取費用。

  在執行 Android 12 或更高版本的裝置上，如果使用者授予「使用大致位置」權限，Kaspersky Endpoint Security for Android 應用程式首先會嘗試取得準確的裝置位置。如果這麼做不成功，則僅在不超過 30 分鐘前收到裝置的大致位置時才傳回該裝置的大致位置。否則，**定位裝置**命令將失敗。

- **響起警報**

  行動裝置發出警報。警報響 5 分鐘（如果裝置的電池電量低，則響 1 分鐘）。

- **同步裝置**

  將行動裝置與卡巴斯基安全管理中心同步。

Kaspersky Endpoint Security for Android 應用程式需要特定權限才能執行命令。當初始配置精靈正在執行時，Kaspersky Endpoint Security for Android 會提示使用者授予應用程式所有必需的權限。使用者可以略過這些步驟或以後在裝置設定中停用這些權限。如果是這種情況，您無法執行命令。

在執行 Android 10.0 或更新版本的裝置上，使用者必須授與「任何時間」均可存取裝置位置的權限。在執行 Android 11.0 或更新版本的裝置上，使用者也必須授與「使用應用程式期間」的權限來存取相機。否則，竊盜防護命令將無法運作。使用者會收到此限制的通知，並且會再次收到要求授與所需層級權限的提示。若使用者選取「只有這次」選項來授與相機權限，則會視為是應用程式授與存取權限。若系統再次要求存取相機的權限，建議您直接聯絡使用者。

向行動裝置傳送命令：

1. 在卡巴斯基安全管理中心網頁主控台或雲端主控台的主視窗中，選取**裝置** > **行動** > **裝置**。
2. 選取要向其傳送命令的裝置，然後點擊**控制**或**管理**。
3. **可用命令**清單中選取所需的命令，然後點擊**確定**。
4. 如果系統提示您確認操作，請點擊**確定**。

   指定的命令會被傳送到行動裝置並顯示確認視窗。

從卡巴斯基安全管理中心移除行動裝置

如果您不再需要管理行動裝置，您可以使用網頁主控台或雲端主控台從卡巴斯基安全管理中心中刪除它。

從卡巴斯基安全管理中心刪除行動裝置：

1. 從裝置移除行動應用程式或確認使用者已從所需的裝置移除應用程式。
2. 在卡巴斯基安全管理中心網頁主控台或雲端主控台的主視窗中，選取**裝置** > **行動** > **裝置**。

3. 選取要移除的行動裝置，然後點擊**刪除**。

4. 點擊**確定**確認操作。

該裝置將從卡巴斯基安全管理中心中移除。

管理群組政策

本章節介紹如何在卡巴斯基安全管理中心網頁主控台和雲端主控台中管理群組政策。

用於管理行動裝置的群組政策

*群組政策*是用於管理屬於管理群組的行動裝置和管理裝置上安裝的行動 APP 的設定套件。

您可以使用政策設定單個裝置和裝置群組的設定。對於一組裝置，可在群組政策內容視窗中設定管理設定。

政策中的每個參數都有「鎖定」內容，這會顯示是否允許在本機應用程式設定中，修改層級結構的政策（對嵌套群組和次要管理伺服器而言）。

在本機應用程式中和政策中設定的設定值，將儲存在管理伺服器上，在同步期間分發至行動裝置，並將其作為目前設定儲存在裝置中。如果使用者指定了未被「鎖定」的其他設定值，在裝置與管理伺服器下次同步期間，設定新值將被傳遞給管理伺服器，並儲存在應用程式本機設定中，而不是先前由管理員指定的值。

為了使 Android 行動裝置的企業安全防護保持最新，您可以監控使用者的裝置是否符合企業安全需求。

有關在卡巴斯基安全管理中心網頁主控台和雲端主控台中管理政策和管理群組的更多詳細資訊：

- 如果您使用卡巴斯基安全管理中心網頁主控台，請參閱*卡巴斯基安全管理中心說明*。
- 如果您使用的是卡巴斯基安全管理中心雲端主控台，請參閱*卡巴斯基安全管理中心雲端主控台說明*。

查看群組政策清單

卡巴斯基安全管理中心網頁主控台和雲端主控台允許您查看群組政策、其狀態和內容。

要檢視群組政策清單，

在卡巴斯基安全管理中心網頁主控台或雲端主控台的主視窗中，選取**裝置 > 政策和設定檔**。

群組政策清單將開啟，其中包含有關群組政策的簡要資訊。在此頁面上，您可以建立、修改、複製、移動和刪除群組政策。

查看政策分發結果

卡巴斯基安全管理中心網頁主控台和雲端主控台允許您查看群組政策的分佈圖以及該政策所屬之所有裝置的相關資訊。

查看群組政策的分佈結果：

1. 在卡巴斯基安全管理中心網頁主控台或雲端主控台的主視窗中，選取**裝置** > **政策和設定檔**。
2. 在開啟的群組政策清單中，選取要查看其分佈結果之政策名稱旁邊的核取方塊，然後點擊**分佈**。

政策分佈結果頁面隨即開啟。此頁面包含政策摘要、政策分佈圖以及該政策所屬之所有裝置的相 關資訊表格。您可以透過點擊**設定政策**按鈕開啟政策內容視窗。

建立群組政策

卡巴斯基安全管理中心網頁主控台和雲端主控台允許您建立群組政策以管理行動裝置。

若要建立群組政策，請執行以下操作：

1. 在卡巴斯基安全管理中心網頁主控台或雲端主控台的主視窗中，選取**裝置** > **政策和設定檔**。
2. 在開啟的卡巴斯基安全管理中心群組政策清單中，點擊**目前路徑**以選取要為其建立政策的管理群組。
   預設情況下，新群組政策會套用到**受管理裝置**群組。
3. 點擊**新增**以啟動政策建立精靈。使用**下一步**按鈕繼續完成精靈。
4. 根據平台選取應用程式：
   - **Kaspersky Endpoint Security for Android**
   - **Kaspersky Security for iOS**
5. 在**名稱**欄位中輸入新政策的名稱。如果您指定了現有政策的名稱，它將在最後自動新增 (1)。
6. 選取政策狀態：
   - **使用中**

     精靈將在管理伺服器上儲存已建立的政策。在行動裝置下次與管理伺服器同步時，該政策將在裝置上用作活動政策。
   - **非使用中**

     精靈將在管理伺服器上以備份政策的方式儲存已建立的政策。在後續某個特殊事件之後該政策將被啟動。若有需要可將未啟動的政策轉換為啟動狀態。

     > 可以為群組中一個應用程式建立若干個政策，但是只能啟動它們其中的一個政策。當建立新的啟動政策時，先前的啟動政策將自動變為停用狀態。
7. 您可以啟用或停用兩個繼承選項，**從父政策繼承設定**和**強制繼承子政策中的設定**：
   - 如果您為子管理群組啟用**從父政策繼承設定**並鎖定父政策中的某些設定，則您無法在子群組的政策中變更這些設定。但是，您可以變更未在父政策中鎖定的設定。
   - 如果您為子管理群組停用**從父政策繼承設定**，那麼您可以變更子群組中的所有設定，即使某些設定在父政策中被鎖定。

- 如果在父管理群組中啟用**強制繼承子政策中的設定**，這將為每個子政策啟用**從父政策繼承設定**選項。在這種情況下，您不能為任何子政策停用此選項。所有鎖定在父政策中的設定都在子群組中強制繼承，您不能在子群組中變更這些設定。

- 在**受管理裝置**群組的政策中，**從父政策繼承設定**選項不會影響任何設定，因為**受管理裝置**群組並沒有任何上游群組，因此不會繼承任何政策。

預設情況下，**從父政策繼承設定**選項會處於啟用狀態，而**在子政策中強制繼承設定**選項則會處於停用狀態。

8. 如果需要，您可以定義新建立之政策的設定。為此，請選取**應用程式設定**標籤，然後按照「定義政策設定」部分的說明繼續操作。

   或者，您可以稍後再執行此操作。

9. 點擊**儲存**以建立政策。

建立用於管理行動裝置的新群組政策。

修改群組政策

卡巴斯基安全管理中心網頁主控台和雲端主控台允許您修改群組政策的設定。

若要修改群組政策，請執行以下操作：

1. 開啟政策內容視窗：

   - 在卡巴斯基安全管理中心網頁主控台或雲端主控台的主視窗中，選取**裝置 > 政策和設定檔**。在開啟的群組政策清單中，點擊要配置的政策名稱。

   - 在卡巴斯基安全管理中心網頁主控台或雲端主控台的主視窗中，選取**裝置 > 行動 > 裝置**。點擊您要設定政策的行動裝置，然後在**使用中的政策和政策設定檔**標籤上選取該政策。

2. 在政策內容視窗中，選取**應用程式設定**，然後按照「定義政策設定」部分的說明定義政策設定。

   > 您還可以配置一般設定、設定繼承、事件記錄和通知、政策設定檔以及查看修訂記錄。如需詳細資訊，請參閱*卡巴斯基安全管理中心說明*。

3. 點擊**儲存**按鈕儲存對政策所做的變更並結束政策內容視窗。

下次與卡巴斯基安全管理中心執行裝置同步之後，可進行行動裝置設定。

複製群組政策

卡巴斯基安全管理中心網頁主控台和雲端主控台允許您建立群組政策的副本。

要建立群組政策的副本：

1. 在卡巴斯基安全管理中心網頁主控台或雲端主控台的主視窗中，選取**裝置 > 政策和設定檔**。

2. 在開啟的群組政策清單中，選取要為其建立副本之政策名稱旁邊的核取方塊，然後點擊**複製**。

3. 在開啟的管理群組樹狀結構中，選取要在其中建立政策副本的目標群組。
   您可以透過選取現有群組，然後點擊**新增子群組**來建立新的管理群組。
4. 點擊**複製**。
5. 點擊**確定**確認操作。

隨即將在目標群組中以相同的名稱建立政策的副本。目標群組中每個複製或移動的政策，其狀態將為**非使用中**。您可以隨時將狀態變更為**使用中**。

如果目標群組中已經存在與新建立或移動之政策名稱相同的政策，則在新建立或移動之政策名稱中新增（<next sequence number>）索引，例如：(1)。

將政策移動到另一個管理群組

卡巴斯基安全管理中心網頁主控台和雲端主控台允許您將政策移動到另一個管理群組。

將政策移動到另一個管理群組：

1. 在卡巴斯基安全管理中心網頁主控台或雲端主控台的主視窗中，選取**裝置 > 政策和設定檔**。
2. 在開啟的群組政策清單中，選取要移動到另一個管理群組之政策名稱旁邊的核取方塊，然後點擊**移動**。
3. 在開啟的管理群組樹狀結構中，選取政策要移動到哪個目標群組。
   您可以透過選取現有群組，然後點擊**新增子群組**來建立新的管理群組。
4. 點擊**移動**。
5. 點擊**確定**確認操作。

結果取決於政策繼承內容而定：

- 如果來源群組中未繼承該政策，則將其移至目標群組。
- 如果政策是在來源群組中繼承的，則不會移動它。相反，將在目標群組中建立此政策的副本。

目標群組中每個複製或移動的政策，其狀態將為**非使用中**。您可以隨時將狀態變更為**使用中**。

如果目標群組中已經存在與新建立或移動之政策名稱相同的政策，則在新建立或移動之政策名稱中新增（<next sequence number>）索引，例如：(1)。

刪除群組政策

卡巴斯基安全管理中心網頁主控台和雲端主控台允許您刪除群組政策。

您只能刪除目前管理群組中未繼承的政策。如果政策是繼承而來的，則只能在為其建立的上級群組中刪除它。

若要刪除群組政策，請執行以下操作：

1. 在卡巴斯基安全管理中心網頁主控台或雲端主控台的主視窗中，選取**裝置 > 政策和設定檔**。
2. 在開啟的群組政策清單中，選取要刪除之政策名稱旁邊的核取方塊，然後點擊**刪除**。
3. 點擊**確定**確認操作。

群組政策將被刪除。

定義政策設定

本節介紹如何定義卡巴斯基安全管理中心的政策設定，以管理行動裝置。

您可以在建立或修改政策時定義政策設定。

設定病毒防護

您只能為 Android 定義這些政策設定。

為了及時偵測威脅、病毒和其他惡意應用程式，您應設定即時防護和自動執行病毒掃描。

Kaspersky Endpoint Security for Android 可偵測以下類型的物件：

- 病毒、蠕蟲、木馬和惡意工具
- 廣告軟體
- 可偵測被犯罪分子用來損害裝置或個人資料的應用程式

由於技術限制，Kaspersky Endpoint Security for Android 無法掃描大小為 2 GB 或更大的檔案。在掃描期間，應用程式將略過大型檔案，且不會通知您已略過大型檔案。

設定即時防護

您只能為 Android 定義這些政策設定。

要設定即時防護：

1. 開啟政策內容視窗：

- 在卡巴斯基安全管理中心網頁主控台或雲端主控台的主視窗中，選取**裝置 > 政策和設定檔**。在開啟的群組政策清單中，點擊要配置的政策名稱。
- 在卡巴斯基安全管理中心網頁主控台或雲端主控台的主視窗中，選取**裝置 > 行動 > 裝置**。點擊您要設定政策的行動裝置，然後在**使用中的政策和政策設定檔**標籤上選取該政策。

2. 在政策內容視窗中，選取**應用程式設定 > 基本防護**。

3. 在**病毒防護**區段中，設定行動裝置檔案系統防護：

- 要啟動行動裝置的即時防護，選取**啟用即時病毒防護**核取方塊。
- 指定防護級別：
  - 如果您希望 Kaspersky Endpoint Security for Android 僅掃描下載資料夾中的新應用程式和檔案，請選取**僅掃描新應用程式**。
  - 要為行動裝置啟用針對威脅的延伸防護，請選取**掃描所有應用程式並監控檔案的動作**。

    Kaspersky Endpoint Security for Android 將掃描使用者在裝置上開啟、修改、移動、複製、安裝或儲存的所有檔案，以及新安裝的行動應用程式。

    在執行 Android 8.0 或更高版本的裝置上，Kaspersky Endpoint Security for Android 將掃描使用者修改、移動、安裝和儲存的檔案，以及檔案副本。在開啟檔案或複製原始檔案時，Kaspersky Endpoint Security for Android 不會進行掃描。
- 要在使用者裝置首次啟動時使用卡巴斯基安全網路雲端服務啟用新應用程式的附加掃描，請選取**卡巴斯基安全網路的其他防護**核取方塊。
- 要封鎖可被犯罪分子利用來損害裝置或使用者資料的廣告軟體和應用程式，請選取**偵測廣告軟體、自動撥號軟體和可能會被犯罪分子利用並造成使用者裝置和資料受損的應用程式**核取方塊。

4. 在**病毒防護設定**區段，選取要對威脅偵測執行的操作：

- **刪除並儲存隔離中檔案的備份**

  偵測到的物件將被自動刪除。不要求使用者做任何其他操作。在刪除物件之前，Kaspersky Endpoint Security for Android 將建立檔案的備份副本並將其儲存在隔離區中。
- **刪除**

  偵測到的物件將被自動刪除。不要求使用者做任何其他操作。移除物件之前，Kaspersky Endpoint Security for Android 會顯示偵測到物件的暫時通知。
- **略過**

  如果偵測到的物件遭略過，Kaspersky Endpoint Security for Android 會警告使用者裝置防護方面存在問題。有關略過的物件資訊會顯示在應用程式的**狀態**區域。對於每個略過的威脅，應用程式都提供使用者可以執行以消除威脅的操作。略過的威脅清單可能會變更，例如，如果可疑檔案遭刪除或移動。若要接收最新的威脅清單，請執行完整裝置掃描。為了確保可靠地防護您的資料，請解毒所有偵測到的物件。

5. 點擊**儲存**按鈕儲存對政策所做的變更並結束政策內容視窗。

下次與卡巴斯基安全管理中心執行裝置同步之後，可進行行動裝置設定。

在行動裝置上設定自動執行病毒掃描

您只能為 Android 定義這些政策設定。

要在行動裝置上設定自動執行病毒掃描，請執行以下操作：

1. 開啟政策內容視窗：
   - 在卡巴斯基安全管理中心網頁主控台或雲端主控台的主視窗中，選取**裝置** > **政策和設定檔**。在開啟的群組政策清單中，點擊要配置的政策名稱。
   - 在卡巴斯基安全管理中心網頁主控台或雲端主控台的主視窗中，選取**裝置** > **行動** > **裝置**。點擊您要設定政策的行動裝置，然後在**使用中的政策和政策設定檔**標籤上選取該政策。
2. 在政策內容視窗中，選取**應用程式設定** > **基本防護**。
3. 要封鎖可能被犯罪分子利用來損害裝置或使用者資料的廣告軟體和應用程式，請選取**裝置掃描**區域中的**偵測廣告軟體、自動撥號軟體和可能會被犯罪分子利用並造成使用者裝置和資料受損的應用程式**核取方塊。
4. 在**偵測到威脅時執行的操作**清單中，請選取以下選項之一：
   - **刪除並儲存隔離中檔案的備份**

     偵測到的物件將被自動刪除。不要求使用者做任何其他操作。在刪除物件之前，Kaspersky Endpoint Security for Android 將建立檔案的備份副本並將其儲存在隔離區中。
   - **刪除**

     偵測到的物件將被自動刪除。不要求使用者做任何其他操作。移除物件之前，Kaspersky Endpoint Security for Android 會顯示偵測到物件的暫時通知。
   - **略過**

     如果偵測到的物件遭略過，Kaspersky Endpoint Security for Android 會警告使用者裝置防護方面存在問題。有關略過的物件資訊會顯示在應用程式的**狀態**區域。對於每個略過的威脅，應用程式都提供使用者可以執行以消除威脅的操作。略過的威脅清單可能會變更，例如，如果可疑檔案遭刪除或移動。若要接收最新的威脅清單，請執行完整裝置掃描。為了確保可靠地防護您的資料，請解毒所有偵測到的物件。
   - **詢問使用者**

     Kaspersky Endpoint Security for Android 應用程式將顯示一則通知，提示使用者選擇要對偵測到的物件採取的操作：**略過**或**刪除**。

     當應用程式偵測到多個物件時，**詢問使用者**選項允許裝置使用者透過使用**套用到所有威脅**核取方塊將所選操作套用到每個檔案。

您必須將 Kaspersky Endpoint Security for Android 設定為可存取功能，以確保 Android 10.0 或更高版本的行動裝置能顯示通知。Kaspersky Endpoint Security for Android 會提示使用者透過初始配置精靈將該應用程式設定為輔助使用功能。使用者可以略過此步驟或以後在裝置設定中停用此服務。在這種情況下，Kaspersky Endpoint Security for Android 顯示 Android 系統視窗，提示使用者選擇要對偵測到的物件採取的操作：「略過」或「刪除」。要將操作套用於多個物件，您需要開啟 Kaspersky Endpoint Security。

5. 在**排程掃描**區段，您可以設定自動完整掃描裝置檔案系統。

   選取以下選項之一：

   - **已停用**

     裝置檔案系統的掃描不會自動啟動。

   - **資料庫更新後**

     每次病毒資料庫更新時都會自動掃描裝置檔案系統。

   - **每天**

     裝置檔案系統將每天自動掃描。

     如果選取此選項，您還可以在**開始時間**欄位中指定掃描時間。

   - **每週在以下時間進行**

     裝置檔案系統將每週自動掃描一次。

     如果選取此選項，還可以使用下拉清單選取一週的哪幾天要執行掃描，並在**開始時間**欄位中指定掃描時間。

在 Android 12 或更高版本上，若裝置處於省電模式，應用程式執行此任務的時間可能會晚於指定時間。

6. 點擊**儲存**按鈕儲存對政策所做的變更並結束政策內容視窗。

下次與卡巴斯基安全管理中心執行裝置同步之後，可進行行動裝置設定。

設定病毒資料庫更新

您只能為 Android 定義這些政策設定。

設定病毒資料庫更新：

1. 開啟政策內容視窗：

   - 在卡巴斯基安全管理中心網頁主控台或雲端主控台的主視窗中，選取**裝置 > 政策和設定檔**。在開啟的群組政策清單中，點擊要配置的政策名稱。

   - 在卡巴斯基安全管理中心網頁主控台或雲端主控台的主視窗中，選取**裝置 > 行動 > 裝置**。點擊您要設定政策的行動裝置，然後在**使用中的政策和政策設定檔**標籤上選取該政策。

2. 在政策內容視窗中，選取**應用程式設定 > 資料庫更新**。

3. 在**資料庫更新**區段中，設定使用者裝置上自動更新病毒資料庫的排程。

   選取以下選項之一：

   - **已停用**

     病毒資料庫的自動更新將被停用。

   - **每天**

     病毒資料庫將每天更新。

     如果選取此選項，您還可以在**更新時間**欄位中指定更新時間。

   - **每週**

     病毒資料庫將每週更新一次。

     如果選取此選項，您還可以在**更新時間**欄位中指定更新時間，並在**週間日**下拉清單中指定一週的哪幾天要執行更新。

   在 Android 12 或更高版本上，若裝置處於省電模式，應用程式執行此任務的時間可能會晚於指定時間。

4. 在**資料庫更新來源**區段，指定 Kaspersky Endpoint Security for Android 接收與安裝病毒資料庫更新所需的更新來源：

   - **Kaspersky 伺服器**

     Kaspersky Endpoint Security for Android 將使用卡巴斯基更新伺服器作為將病毒資料庫下載到使用者裝置的更新來源。

   - **管理伺服器**

     僅當您使用卡巴斯基安全管理中心網頁主控台時可用。

     Kaspersky Endpoint Security for Android 將使用卡巴斯基安全管理中心管理伺服器的儲存庫作為將病毒資料庫下載到使用者裝置的更新來源。

   - **其他更新來源**

     Kaspersky Endpoint Security for Android 將使用第三方伺服器作為將病毒資料庫下載到使用者裝置的更新來源。

     如果選取此選項，則必須在**使用其他伺服器作為病毒資料庫的更新來源**欄位中指定 HTTP 伺服器的位址。

5. 如果您希望 Kaspersky Endpoint Security for Android 在使用者裝置位於漫遊區域時，依照更新排程下載病毒資料庫更新，請選取**漫遊時更新病毒防護資料庫**區段中的**允許漫遊時更新資料庫**核取方塊。

6. 點擊**儲存**按鈕儲存對政策所做的變更並結束政策內容視窗。

下次與卡巴斯基安全管理中心執行裝置同步之後，可進行行動裝置設定。

定義裝置解鎖設定

您只能為 Android 定義這些政策設定。

要確保行動裝置安全，您需要設定使用密碼，在裝置從睡眠模式喚醒時提示使用者輸入密碼。

如果解鎖密碼不強，您可以對裝置上的使用者活動施加限制（例如鎖定裝置）。您可以使用合規性控制元件施加限制。

在某些執行 Android 7.0 或更高版本的 Samsung 裝置上，當使用者嘗試配置不受支援的方法（例如，圖形密碼）來解鎖裝置時，如果滿足以下條件，裝置可能會鎖定：Kaspersky Endpoint Security for Android 移除防護已啟用並且設定了螢幕解鎖密碼長度要求。要解鎖裝置，您必須傳送特殊命令到裝置。

要設定裝置解鎖密碼強度：

1. 開啟政策內容視窗：
   - 在卡巴斯基安全管理中心網頁主控台或雲端主控台的主視窗中，選取**裝置 > 政策和設定檔**。在開啟的群組政策清單中，點擊要配置的政策名稱。
   - 在卡巴斯基安全管理中心網頁主控台或雲端主控台的主視窗中，選取**裝置 > 行動 > 裝置**。點擊您要設定政策的行動裝置，然後在**使用中的政策和政策設定檔**標籤上選取該政策。
2. 在政策內容視窗中，選取**應用程式設定 > 基本防護**。
3. 如果您希望應用程式檢查是否設定了解鎖密碼，請選取**密碼防護**區段中的**需要設定螢幕解鎖密碼**核取方塊。

   如果應用程式偵測到裝置上未設定任何系統密碼，請提示使用者進行設定。密碼根據管理員定義的參數來設定（請參閱下圖）。
4. 指定使用者密碼的最小字元數。

   可能值：4 到 16 個字元。

   預設情況下，使用者的密碼包含 4 個字元。

   在執行 Android 10.0 或更高版本的裝置上，Kaspersky Endpoint Security 會將密碼強度要求解析為其中一個系統值：中度或高度。

   執行 Android 10.0 或更新版本裝置的數值將由以下規則決定：
   - 如果要求的密碼長度是 1 到 4 個符號，那麼應用程式會提示使用者設定中等強度的密碼。密碼必須是數字 (PIN) 且沒有重複或按順序 (如 1234) 的序列或英數字母。PIN 或密碼的長度必須至少有 4 個字元。
   - 如果要求的密碼長度為 5 個以上的符號，那麼應用程式會提示使用者設定高強度密碼。密碼必須是數字 (PIN) 且沒有重複或按順序的序列或英數字母 (password)。 PIN 必須至少有 8 位數，密碼長度必須至少有 6 個字元。
5. 如果您希望使用者能夠使用指紋解鎖螢幕，請選取**允許使用指紋（適用於 Android 9 或更早版本的裝置）**核取方塊。如果解鎖密碼不符合企業安全需求，則無法使用指紋掃描器解鎖螢幕。

   在執行 Android 10.0 或更高版本的裝置上，不支援使用指紋解鎖螢幕。

   Kaspersky Endpoint Security for Android 不會限制使用指紋掃描器來登入應用程式或確認購買。

   在某些 Samsung 裝置上，無法封鎖使用指紋解鎖螢幕。

在某些 Samsung 裝置上，如果解鎖密碼不符合企業安全需求，Kaspersky Endpoint Security for Android 不會封鎖使用指紋解鎖螢幕。

在裝置設定中新增指紋後，使用者可以使用以下方法解鎖螢幕：

- 將手指按在指紋掃描器上（主要方法）。
- 輸入解鎖密碼（備用方法）。

6. 點擊**儲存**按鈕儲存對政策所做的變更並結束政策內容視窗。

下次與卡巴斯基安全管理中心執行裝置同步之後，可進行行動裝置設定。

為被竊取或遺失的裝置資料設定防護

您只能為 Android 定義這些政策設定。

為了在行動裝置遺失或被竊時保護公司資料，您必須設定未經授權的存取防護。

為保護被竊或遺失的裝置資料，必須將 Kaspersky Endpoint Security for Android 設定為輔助功能。Kaspersky Endpoint Security for Android 會提示使用者透過初始配置精靈將該應用程式設定為輔助使用功能。使用者可以略過此步驟或以後在裝置設定中停用此服務。

保護被竊取或遺失的裝置資料：

1. 開啟政策內容視窗：
   - 在卡巴斯基安全管理中心網頁主控台或雲端主控台的主視窗中，選取**裝置 > 政策和設定檔**。在開啟的群組政策清單中，點擊要配置的政策名稱。
   - 在卡巴斯基安全管理中心網頁主控台或雲端主控台的主視窗中，選取**裝置 > 行動 > 裝置**。點擊您要設定政策的行動裝置，然後在**使用中的政策和政策設定檔**標籤上選取該政策。
2. 在政策內容視窗中，選取**應用程式設定 > 基本防護**。
3. 在**竊盜防護**區段，設定裝置鎖定：
   - 指定解鎖代碼中的字元數。
   - 指定裝置鎖定時要顯示的文字。
4. 點擊**儲存**按鈕儲存對政策所做的變更並結束政策內容視窗。

下次與卡巴斯基安全管理中心執行裝置同步之後，可進行行動裝置設定。

設定應用程式控制

您只能為 Android 定義這些政策設定。

*應用程式控制*會檢查安裝在行動裝置上的應用程式，確認是否符合企業安全需求。在卡巴斯基安全管理中心，管理員根據企業安全需求建立允許、封鎖、強制和建議的應用程式的清單。因應用程式控制的原因，Kaspersky Endpoint Security 會提示您安裝必要和建議的應用程式以及移除被封鎖的應用程式。您無法在使用者的行動裝置上啟動被封鎖的應用程式。

在卡巴斯基安全管理中心網頁主控台和雲端主控台中，您可以透過套用預先定義的規則來管理使用者裝置上的應用程式。您可以設定兩種類型的**應用程式控制**規則：應用程式規則和類別規則。

應用程式規則可套用於特定應用程式，而**類別規則**可套用於屬於預先定義類別的任何應用程式。應用程式類別由卡巴斯基專家指定。

*要設定**應用程式控制**：*

1. 開啟政策內容視窗：
   - 在卡巴斯基安全管理中心網頁主控台或雲端主控台的主視窗中，選取**裝置 > 政策和設定檔**。在開啟的群組政策清單中，點擊要配置的政策名稱。
   - 在卡巴斯基安全管理中心網頁主控台或雲端主控台的主視窗中，選取**裝置 > 行動 > 裝置**。點擊您要設定政策的行動裝置，然後在**使用中的政策和政策設定檔**標籤上選取該政策。
2. 在政策內容頁面中，選取**應用程式設定 > 安全性控制**。
3. 在**應用程式控制**區段下的表格中，新增定義哪些應用程式將被控制的規則。
   - 要為特定應用程式新增規則：
     a. 在表格中，點擊**應用程式規則**。
     b. 在開啟的**應用程式規則**視窗中，選取將對建立之規則涵蓋的應用程式執行的操作。
     c. 透過填寫**連至安裝套件的連結 (例如 https://play.google.com/store/apps/details?id=com.kaspersky.kes)**、**套件名稱 (例如 katana.facebook.com)**和**應用程式名稱**來指定將受規則約束的應用程式。
     d. 點擊**儲存**。

     該規則將新增到**應用程式控制**規則清單中。
   - 要為應用程式類別新增規則：
     a. 在**應用程式控制**區段下的表格中，點擊**類別規則**。
     b. 在開啟的**類別規則**視窗中，從下拉清單中選取應用程式類別。
     所選類別中的應用程式將受建立的規則約束。
     c. 在**操作模式**區段中，選取所選類別中任意應用程式嘗試啟動時將執行的操作：**被禁止的應用程式**或**允許的應用程式**。

d. 填寫**偵測到指定類別的應用程式時，要顯示在使用者裝置的其他註解**（如有必要）。

e. 點擊**儲存**。

該規則將新增到**應用程式控制**規則清單中。

4. 在**對封鎖的應用程式採取的措施**區段中，選取對封鎖的應用程式執行的操作：

- 如果您不希望 Kaspersky Endpoint Security for Android 在使用者行動裝置上啟動封鎖的應用程式，請選取**封鎖應用程式啟動**。
- 如果您要 Kaspersky Endpoint Security for Android 在封鎖的應用程式上傳送資料到事件記錄而不封鎖它們，選取**不要封鎖禁止的應用程式，僅回報**。

5. 在**操作模式**區段，選取您新增的規則是否可以定義允許的應用程式還是封鎖的應用程式：

- 如果您希望規則可以定義允許哪些應用程式，請選取**被禁止的應用程式**。

  在**被禁止的應用程式**模式下，如果您希望 Kaspersky Endpoint Security for Android 在使用者行動裝置上封鎖啟動系統應用程式（例如行事曆、相機和設定），請選取**封鎖系統應用程式**核取方塊。

  > Kaspersky 專家建議不要封鎖系統應用程式，因為這會導致裝置操作故障。

- 如果您希望規則定義封鎖哪些應用程式，請選取**允許的應用程式**。

6. 要接收有關安裝在行動裝置上的所有應用程式資訊，請在**應用程式報告**區段中，選取**傳送在所有行動裝置已安裝應用程式的清單**核取方塊。

   Kaspersky Endpoint Security for Android 在每次應用被安裝或從裝置移除時傳送資料到事件記錄。

7. 點擊**儲存**按鈕儲存對政策所做的變更並結束政策內容視窗。

下次與卡巴斯基安全管理中心執行裝置同步之後，可進行行動裝置設定。

使用企業安全需求設定行動裝置的合規性控制

> 您只能為 Android 定義這些政策設定。

合規性控制允許您監控 Android 裝置是否符合企業安全需求，並在不合規的情況下採取措施。企業安全需求規範使用者可以如何使用裝置。例如，必須在裝置上啟用即時防護，病毒資料庫必須是最新的，並且裝置密碼必須足夠強。合規性控制基於規則清單。合規性規則包括以下組成部分：

- 裝置不合規標準。
- 如果使用者未在規定的時段內解決不合規問題，將對裝置採取的措施。
- 分配給使用者以解決不合規問題的時間段（例如，24 小時）。

  當指定的時段結束時，將在使用者的裝置上執行選定的操作。

> 在 Android 12 或更高版本上，若裝置處於省電模式，應用程式執行此任務的時間可能會晚於指定時間。

要設定合規性控制，您可以執行以下操作：

- 啟用或停用現有的合規性規則。
- 編輯現有的合規性規則。
- 新增規則。
- 刪除規則。

啟用和停用合規性規則

您只能為 Android 定義這些政策設定。

要啟用或停用具有企業安全需求的行動裝置現有合規性控制規則：

1. 開啟政策內容視窗：
   - 在卡巴斯基安全管理中心網頁主控台或雲端主控台的主視窗中，選取**裝置** > **政策和設定檔**。在開啟的群組政策清單中，點擊要配置的政策名稱。
   - 在卡巴斯基安全管理中心網頁主控台或雲端主控台的主視窗中，選取**裝置** > **行動** > **裝置**。點擊您要設定政策的行動裝置，然後在**使用中的政策和政策設定檔**標籤上選取該政策。
2. 在政策內容頁面中，選取**應用程式設定** > **安全性控制**。
3. 在**合規性控制**區段，使用**狀態**欄位中的切換按鈕，啟用或停用現有的合規性規則。
4. 點擊**儲存**按鈕儲存對政策所做的變更並結束政策內容視窗。

下次與卡巴斯基安全管理中心執行裝置同步之後，可進行行動裝置設定。

編輯合規性規則

您只能為 Android 定義這些政策設定。

要編輯具有企業安全需求的行動裝置合規性控制規則：

1. 開啟政策內容視窗：
   - 在卡巴斯基安全管理中心網頁主控台或雲端主控台的主視窗中，選取**裝置** > **政策和設定檔**。在開啟的群組政策清單中，點擊要配置的政策名稱。
   - 在卡巴斯基安全管理中心網頁主控台或雲端主控台的主視窗中，選取**裝置** > **行動** > **裝置**。點擊您要設定政策的行動裝置，然後在**使用中的政策和政策設定檔**標籤上選取該政策。
2. 在政策內容頁面中，選取**應用程式設定** > **安全性控制**。

3. 在**合規性控制**區段，選取要編輯的規則，然後點擊**編輯**。

4. 在開啟的**規則**視窗中，依照以下方法編輯規則：

   a. 在**動作**欄位中，透過新增操作、編輯現有操作或刪除操作來設定不符合規則時要執行的操作清單。

   b. 或者，透過使用每個操作的**修正時間限制**欄位來指定使用者可以修復不合規的時段。

   c. 點擊**儲存**按鈕儲存規則。

5. 點擊**儲存**按鈕儲存對政策所做的變更並結束政策內容視窗。

下次與卡巴斯基安全管理中心執行裝置同步之後，可進行行動裝置設定。

新增合規性規則

您只能為 Android 定義這些政策設定。

要新增具有企業安全需求的行動裝置合規性控制規則：

1. 開啟政策內容視窗：

   - 在卡巴斯基安全管理中心網頁主控台或雲端主控台的主視窗中，選取**裝置 > 政策和設定檔**。在開啟的群組政策清單中，點擊要配置的政策名稱。
   - 在卡巴斯基安全管理中心網頁主控台或雲端主控台的主視窗中，選取**裝置 > 行動 > 裝置**。點擊您要設定政策的行動裝置，然後在**使用中的政策和政策設定檔**標籤上選取該政策。

2. 在政策內容頁面中，選取**應用程式設定 > 安全性控制**。

3. 在**合規性控制**區段，點擊**規則**。

4. 在開啟的**規則**視窗中，按照以下方式定義規則：

   a. 選取規則的不合規標準。

   b. 點擊**新增**，然後在**動作**欄位中選取不合規時要執行的操作。
   您可以新增多個操作。

   c. 透過使用每個操作的**修正時間限制**欄位來指定使用者可以修復不合規的時段。

   d. 點擊**儲存**按鈕儲存規則。

5. 點擊**儲存**按鈕儲存對政策所做的變更並結束政策內容視窗。

下次與卡巴斯基安全管理中心執行裝置同步之後，可進行行動裝置設定。

刪除合規性規則

您只能為 Android 定義這些政策設定。

要刪除具有企業安全需求的行動裝置合規性控制規則：

1. 開啟政策內容視窗：
   - 在卡巴斯基安全管理中心網頁主控台或雲端主控台的主視窗中，選取**裝置 > 政策和設定檔**。在開啟的群組政策清單中，點擊要配置的政策名稱。
   - 在卡巴斯基安全管理中心網頁主控台或雲端主控台的主視窗中，選取**裝置 > 行動 > 裝置**。點擊您要設定政策的行動裝置，然後在**使用中的政策和政策設定檔**標籤上選取該政策。
2. 在政策內容頁面中，選取**應用程式設定 > 安全性控制**。
3. 在**合規性控制**區段，選取要刪除的規則，然後點擊**刪除**。
4. 點擊**儲存**按鈕儲存對政策所做的變更並結束政策內容視窗。

下次與卡巴斯基安全管理中心執行裝置同步之後，可進行行動裝置設定。

不合規標準清單

您只能為 Android 定義這些政策設定。

為確保 Android 裝置符合企業安全需求，Kaspersky Endpoint Security for Android 可以根據以下標準檢查裝置：

- **已停用即時防護**。
  必須啟用即時防護。
  有關設定即時防護的詳細資訊，請參閱「設定即時防護」部分。
- **病毒資料庫已過期**。
  Kaspersky Endpoint Security for Android 的病毒資料庫必須定期更新。
  有關定義病毒資料庫更新設定的更多資訊，請參閱「設定病毒防護」部分。
- **已安裝被禁止的應用程式**。
  裝置不得安裝被歸類為**封鎖啟動**的應用程式，如**應用程式控制**部分所述。
  有關為應用程式建立規則的更多資訊，請參閱「設定應用程式控制」部分。
- **已安裝被禁止類別中的應用程式**。
  裝置不得安裝屬於**封鎖啟動**類別的應用程式，如**應用程式控制**部分所述。
  有關為應用程式類別建立規則的更多資訊， 請參閱「設定應用程式控制」部分。
- **並非已安裝所有所需的應用程式**。
  裝置必須安裝這些被歸類為**強制安裝**的特定應用程式，如**應用程式控制**部分所述。
  有關為應用程式建立規則的更多資訊，請參閱「設定應用程式控制」部分。
- **作業系統版本已過時**。

裝置必須擁有允許使用的作業系統版本。

要使用此不合規標準，您必須在**作業系統最低版本**和**作業系統最高版本**下拉清單中指定允許使用的作業系統版本範圍。

- **裝置已長時間未同步**。

  裝置必須定期與管理伺服器同步。

  要使用此不合規標準，您必須在**同步期間**下拉清單中指定同步裝置的最大時間間隔。

- **裝置已取得 Root 權限**。

  裝置不得 Root。

  更多相關資訊，請參閱「偵測裝置駭客 (root)」部分。

- **解鎖密碼不符合安全性政策**。

  必須使用符合解鎖密碼強度要求的解鎖密碼來防護裝置。

不合規時的行動清單

您只能為 Android 定義這些政策設定。

如果使用者未在指定時間內修復不合規問題，則可進行以下操作：

- **封鎖系統應用程式以外的所有應用程式**。

  封鎖使用者行動裝置上的所有應用程式（系統應用程式除外）啟動。

- **裝置鎖定**。

  行動裝置將被鎖定。要獲取對資料的存取，您必須解鎖裝置。如果裝置解鎖後，解鎖裝置的原因未變更，裝置將在指定時間段後再次被鎖定。

- **抹除企業資料**。

  抹除容器化資料、企業電子郵件帳戶、連線企業 Wi-Fi 網路和 VPN 的設定以及存取點名稱 (APN)。

- **將裝置完全重設為出廠設定**。

  所有資料都將從行動裝置中刪除，設定將回溯至其出廠值。

設定使用者對網站的存取

您可以為 Android 和 iOS 裝置定義這些政策設定。

為了在網際網路瀏覽期間，保護儲存在行動裝置上的個人和企業資料，您可以使用 Web 防護設定使用者的網站存取權限。Web 防護會在使用者開啟網站之前對其進行掃描，然後封鎖散佈惡意程式碼的網站和專門竊取機密資料和存取金融帳戶的網路釣魚網站。

對於 Android 裝置，此功能也支援按卡巴斯基安全網路雲端服務中所定義的類別篩選網站。篩選允許您限制使用者對某些網站或某些類別網站的存取（例如「**賭博、彩票、抽獎**」或「**網際網路通訊**」類別中的網站）。

在 Android 裝置上，Web 防護僅在 Google Chrome 瀏覽器、Huawei Browser 和 Samsung Internet Browser 中可用。

為確保 Web 防護可正常操作，必須將 Kaspersky Endpoint Security for Android 設定為輔助功能。Kaspersky Endpoint Security for Android 會提示使用者透過初始配置精靈將該應用程式設定為輔助使用功能。使用者可以略過此步驟或以後在裝置設定中停用此服務。

在 iOS 裝置上，使用者必須允許 Kaspersky Security for iOS 應用程式新增 Web 防護的 VPN 設定以便運作。

要設定使用者的網站存取權限：

1. 開啟政策內容視窗：
   - 在卡巴斯基安全管理中心網頁主控台或雲端主控台的主視窗中，選取**裝置** > **政策和設定檔**。在開啟的群組政策清單中，點擊要配置的政策名稱。
   - 在卡巴斯基安全管理中心網頁主控台或雲端主控台的主視窗中，選取**裝置** > **行動** > **裝置**。點擊您要設定政策的行動裝置，然後在**使用中的政策和政策設定檔**標籤上選取該政策。
2. 在政策內容頁面中，選取**應用程式設定** > **安全性控制**。
3. 在 **Web 防護**區段，選取**啟用 Web 防護**核取方塊來啟用此功能。
4. 對於 Android 裝置，您可以選取下列選項之一：
   - 要根據網站內容限制使用者存取網站：
     a. 選取**封鎖指定類別的網站**。
     b. 選取 Kaspersky Endpoint Security for Android 將封鎖存取之網站類別旁邊的核取方塊。

     若已啟用 Web 防護，將一律封鎖使用者存取**釣魚網站**和**惡意軟體網站**類別中的網站。
   - 要指定允許的網站清單：
     a. 選取**僅允許指定的網站**。
     b. 透過新增應用程式不會封鎖存取的網站位址，來建立網站清單。Kaspersky Endpoint Security for Android 僅支援正規運算式。輸入允許的網站的位址時，請使用以下範本：
        - `http:\/\/www\.example\.com.*` – 網站的所有子頁面都被允許（例如，`http://www.example.com/about`）。
        - `https:\/\/.*example\.com` – 網站的所有子網域頁面都被允許（例如，`https://pictures.example.com`）。

     c. 您也可以使用運算式 `https?` 來選取 HTTP 和 HTTPS。對於更多正規運算式的詳情，請參考 Oracle 技術支援網站。
   - 要封鎖使用者存取所有網站，請選取**封鎖所有網站**。
5. 點擊**儲存**按鈕儲存對政策所做的變更並結束政策內容視窗。

下次與卡巴斯基安全管理中心執行裝置同步之後，可進行行動裝置設定。

設定功能限制

您只能為 Android 定義這些政策設定。

卡巴斯基安全管理中心網頁主控台使您能夠設定以下行動裝置功能的使用者存取權限：

- Wi-Fi
- 攝影鏡頭
- 藍牙

預設情況下，使用者可以在裝置上無限制地使用 Wi-Fi、攝影鏡頭和藍芽。

若要在裝置上配置 Wi-Fi、攝影鏡頭和藍芽的使用限制，請執行以下步驟：

1. 開啟政策內容視窗：
   - 在卡巴斯基安全管理中心網頁主控台或雲端主控台的主視窗中，選取**裝置 > 政策和設定檔**。在開啟的群組政策清單中，點擊要配置的政策名稱。
   - 在卡巴斯基安全管理中心網頁主控台或雲端主控台的主視窗中，選取**裝置 > 行動 > 裝置**。點擊您要設定政策的行動裝置，然後在**使用中的政策和政策設定檔**標籤上選取該政策。
2. 在政策內容頁面中，選取**應用程式設定 > 安全性控制**。
3. 在**功能管理**區段，設定 Wi-Fi、相機和藍牙的使用：
   - 要在使用者行動裝置上停用 Wi-Fi 模組，則選取**禁止使用 Wi-Fi (僅適用於執行 Android 第 9 版或更新版本的裝置)** 核取方塊。

     在執行 Android 10.0 或更高版本的裝置上，不支援禁止使用 Wi-Fi 網路。
   - 要在使用者行動裝置上停用相機，則選取**封鎖使用攝影鏡頭**核取方塊。

     在執行 Android 10.0 的裝置上，無法完全禁止使用相機。

     在執行 Android 11 或更高版本的裝置上，必須將 Kaspersky Endpoint Security for Android 設定為可存取功能。Kaspersky Endpoint Security for Android 會提示使用者透過初始配置精靈將該應用程式設定為輔助使用功能。使用者可以略過此步驟或以後在裝置設定中停用此服務。如果是這種情況，您將無法限制相機的使用。
   - 要在使用者行動裝置上停用藍牙，則選取**封鎖使用藍芽**核取方塊。

在 Android 12 或更高版本，只有在裝置使用者授予**鄰近藍牙裝置**權限時，才能停用藍牙。使用者可以在初始設定精靈期間或之後授予此權限。

4. 點擊**儲存**按鈕儲存對政策所做的變更並結束政策內容視窗。

下次與卡巴斯基安全管理中心執行裝置同步之後，可進行行動裝置設定。

防止 Kaspersky Endpoint Security for Android 被移除

為了保護行動裝置和遵守企業安全需求，您可以啟用防護以防止移除 Kaspersky Endpoint Security for Android。在這種情況下，使用者無法使用 Kaspersky Endpoint Security for Android 介面移除該應用程式。當使用 Android 作業系統工具移除應用程式時，系統會提示您停用 Kaspersky Endpoint Security for Android 的管理員權限。停用權限後，行動裝置將被鎖定。

要啟用防護以防止移除 Kaspersky Endpoint Security for Android，請執行以下操作：

1. 開啟政策內容視窗：
   - 在卡巴斯基安全管理中心網頁主控台或雲端主控台的主視窗中，選取**裝置 > 政策和設定檔**。在開啟的群組政策清單中，點擊要配置的政策名稱。
   - 在卡巴斯基安全管理中心網頁主控台或雲端主控台的主視窗中，選取**裝置 > 行動 > 裝置**。點擊您要設定政策的行動裝置，然後在**使用中的政策和政策設定檔**標籤上選取該政策。
2. 在政策內容頁面中，選取**應用程式設定 > 安全性控制**。
3. 在**管理行動裝置的應用程式**區段，清除**允許從裝置移除 Kaspersky Endpoint Security for Android** 核取方塊。

要防護在執行 Android 7.0 或更高版本的裝置上的應用程式不會被移除，必須將 Kaspersky Endpoint Security for Android 設定為可存取功能。當初始配置精靈正在執行時，Kaspersky Endpoint Security for Android 會提示使用者授予應用程式所有必需的權限。使用者可以略過這些步驟或以後在裝置設定中停用這些權限。在這種情況下，不防護該應用程式不被移除。

4. 點擊**儲存**按鈕儲存對政策所做的變更並結束政策內容視窗。

下次與卡巴斯基安全管理中心執行裝置同步之後，可進行行動裝置設定。

如果嘗試移除應用程式，行動裝置將被鎖定。

設定行動裝置與卡巴斯基安全管理中心的同步

您可以為 Android 和 iOS 裝置定義這些政策設定。

要管理行動裝置並從行動裝置接收報告或統計資訊，必須定義同步設定。行動裝置與卡巴斯基安全管理中心的同步可透過以下方式執行：

- **按排程**。使用 HTTP 按排程執行同步。您可以在政策內容中設定同步排程。當行動裝置按照排程（即帶有延遲）與卡巴斯基安全管理中心同步時，才會執行對政策設定、命令和工作的修改。預設情況下，行動裝置每隔 6 小時與卡巴斯基安全管理中心同步一次。

  在 Android 12 或更高版本上，若裝置處於省電模式，應用程式執行此任務的時間可能會晚於指定時間。

- **強制**（適用於 Android 裝置）。使用 FCM 服務 (Firebase Cloud Messaging) 的推播通知執行強制同步。強制同步主要用於及時傳遞命令到行動裝置。如果您要使用強制同步，請務必在卡巴斯基安全管理中心設定 FCM。

要使用卡巴斯基安全管理中心設定行動裝置的同步：

1. 開啟政策內容視窗：
   - 在卡巴斯基安全管理中心網頁主控台或雲端主控台的主視窗中，選取**裝置 > 政策和設定檔**。在開啟的群組政策清單中，點擊要配置的政策名稱。
   - 在卡巴斯基安全管理中心網頁主控台或雲端主控台的主視窗中，選取**裝置 > 行動 > 裝置**。點擊您要設定政策的行動裝置，然後在**使用中的政策和政策設定檔**標籤上選取該政策。
2. 在政策內容頁面中，選取**應用程式設定 > 同步**。
3. 在**與管理伺服器的同步**區段，使用**同步期間**下拉清單選取同步週期。

   預設情況下，每 6 小時執行一次同步。
4. 對於 Android 裝置，您可以在裝置漫遊時停用同步。為此，請選取**漫遊時不同步**核取方塊。

   預設情況下，會啟用漫遊時同步。
5. 點擊**儲存**按鈕儲存對政策所做的變更並結束政策內容視窗。

下次與卡巴斯基安全管理中心執行裝置同步之後，可進行行動裝置設定。

卡巴斯基安全網路

若要更有效地防護行動裝置，Kaspersky Endpoint Security for Android 和 Kaspersky Security for iOS 會使用從全球使用者獲得的資料。*卡巴斯基安全網路*使用者處理此類資料。

卡巴斯基安全網路 (KSN) 是一個雲端服務基礎架構，向 Kaspersky 的線上知識庫提供檔案信譽、網路資源和軟體等資訊。使用卡巴斯基安全網路中的資料，可確保在遇到威脅時 Kaspersky 程式能夠做出更快速的回應，提高某些防護元件的效能，並降低誤報的風險。

您加入卡巴斯基安全網路可幫助 Kaspersky 獲取關於新威脅的類型和來源的即時資、開發出抵銷威脅的方法並減少誤報數量。加入卡巴斯基安全網路也允許您存取應用程式和網站信譽統計資料。

當您加入卡巴斯基安全網路後，行動應用程式執行時會獲得某些統計資訊並自動傳送給卡巴斯基。該資訊有助於即時跟蹤威脅。可能會被入侵者用來入侵以損壞電腦或使用者的內容或其部分也會被傳送至 Kaspersky 以進行額外的檢查。

下列應用程式元件使用卡巴斯基安全網路雲端服務：

- Kaspersky Endpoint Security for Android 應用程式中的病毒防護、Web 防護和應用程式控制元件。

- Kaspersky Security for iOS 應用程式中的 Web 防護元件。

若要開始使用 KSN，您必須接受最終使用者產品授權協議的條款與條件。如需更多關於將資料傳送至 KSN 的資訊，請參閱與卡巴斯基安全網路交換資訊。

拒絕參與 KSN 會降低裝置防護等級，這將引發裝置感染和資料丟失。

要改善行動應用程式效能，您可以另外提供統計資料至卡巴斯基安全網路。

向卡巴斯基安全網路提供資訊是自願性質。

與卡巴斯基安全網路交換資訊

Kaspersky Endpoint Security for Android 的資訊交換

為改進即時防護功能，Kaspersky Endpoint Security for Android 將使用卡巴斯基安全網路雲端服務執行以下元件：

- **病毒防護**。應用獲得到關於檔案和應用信譽的 Kaspersky 線上知識庫的存取。此項掃描旨在掃描威脅資訊尚未新增到病毒資料庫但已包含在 KSN 中的威脅。卡巴斯基安全網路雲端服務提供病毒防護的完整操作並降低誤報。
- **Web 防護**。在開啟網站之前，該應用程式使用從 KSN 接收的資料對網站執行掃描。該應用程式還可基於允許和封鎖的類別清單（例如，「網際網路通訊」類別），確定控制使用者對網際網路存取的網站類別。
- **應用程式控制**。該應用程式可基於允許和封鎖的類別（例如，「遊戲」類別）清單，確定限制不符合企業安全需求的應用程式啟動的應用程式類別。

最終使用者產品授權協議列出使用者若在操作防毒軟體或 App 應用程式時使用 KSN，該應用程式會提交給 Kaspersky 的資料類型相關資訊。接受產品授權協議的條件和條款即表明您同意傳輸此資訊。

有關在 Web 防護執行期間使用 KSN 時提交給 Kaspersky 的資料類型資訊，請參見有關 Web 防護資料處理的聲明。接受聲明的條件和條款即表明您同意傳輸此資訊。

如需更多關於將資料佈建至 KSN 的資訊，請參閱 Kaspersky Endpoint Security for Android 中的資料佈建。

向 KSN 提供資料屬自願行為。如有需要，您可以停用與 KSN 交換資料。

Kaspersky Security for iOS 的資訊交換

為改進即時防護功能，Kaspersky Security for iOS 將使用卡巴斯基安全網路雲端服務執行 **Web 防護**元件。在開啟網站之前，該應用程式使用從 KSN 接收的資料對 Web 資源執行掃描。

最終使用者產品授權協議列出使用者若在操作 Web 防護時使用 KSN，該應用程式會提交給 Kaspersky 的資料類型相關資訊。接受產品授權協議的條件和條款即表明您同意傳輸此資訊。

如需更多關於將資料佈建至 KSN 的資訊，請參閱 Kaspersky Security for iOS 中的資料佈建。

向 KSN 提供資料屬自願行為。如有需要，您可以停用與 KSN 交換資料。

將統計資料從 Android 和 iOS 應用程式傳送至 KSN

要與 KSN 交換資料以提高應用程式的效能，必須滿足以下條件：

- 行動裝置使用者必須閱讀與接受卡巴斯基安全網路聲明的條款。
- 您必須將群組政策設定配置為允許傳送統計資訊到 KSN。

您可以隨時選擇結束傳送統計資料到卡巴斯基安全網路。卡巴斯基安全網路聲明列出使用者若在操作行動應用程式時使用 KSN，該應用程式會提交給 Kaspersky 的統計資料類型相關資訊。

啟用和停用卡巴斯基安全網路

預設情況下，會啟用卡巴斯基安全網路的使用。

若停用卡巴斯基安全網路，則會自動停用 Web 防護、應用程式控制和卡巴斯基安全網路中的其他防護，其設定也會無法使用。

若要啟用和停用使用卡巴斯基安全網路，請執行以下操作：

1. 開啟政策內容視窗：
   - 在卡巴斯基安全管理中心網頁主控台或雲端主控台的主視窗中，選取**裝置 > 政策和設定檔**。在開啟的群組政策清單中，點擊要配置的政策名稱。
   - 在卡巴斯基安全管理中心網頁主控台或雲端主控台的主視窗中，選取**裝置 > 行動 > 裝置**。點擊您要設定政策的行動裝置，然後在**使用中的政策和政策設定檔**標籤上選取該政策。
2. 在政策內容頁面中，選取**應用程式設定 > KSN 與統計資料**。
3. 要啟用或停用卡巴斯基安全網路的使用，請選取或清除**使用卡巴斯基安全網路**核取方塊。
4. 如果啟用了卡巴斯基安全網路的使用並且您同意向卡巴斯基提交資料，請選取**允許統計資料傳送至卡巴斯基安全網路**核取方塊。警報此資料將說明行動應用程式在遇到威脅時更快地作出回應，提高防護元件的效能以及降低誤報的風險。
5. 點擊**儲存**按鈕儲存對政策所做的變更並結束政策內容視窗。

下次與卡巴斯基安全管理中心執行裝置同步之後，可進行行動裝置設定。

與 Google Analytics for Firebase、SafetyNet Attestation、Firebase Performance Monitoring 和 Crashlytics 交換資訊

您只能為 Android 定義這些政策設定。

Kaspersky Endpoint Security for Android 會與 Google Analytics for Firebase、SafetyNet Attestation、Firebase Performance Monitoring 和 Crashlytics 服務交換資料，以透過分析使用者體驗、功能、狀態和使用的裝置設定來提高 Kaspersky 軟體、產品、服務和基礎架構的品質、外觀和效能。

依照預設，會停用與 Google Analytics for Firebase、SafetyNet Attestation、Firebase Performance Monitoring 和 Crashlytics 服務交換資訊。

若要啟用資料交換：

1. 開啟政策內容視窗：

   - 在卡巴斯基安全管理中心網頁主控台或雲端主控台的主視窗中，選取**裝置 > 政策和設定檔**。在開啟的群組政策清單中，點擊要配置的政策名稱。

   - 在卡巴斯基安全管理中心網頁主控台或雲端主控台的主視窗中，選取**裝置 > 行動 > 裝置**。點擊您要設定政策的行動裝置，然後在**使用中的政策和政策設定檔**標籤上選取該政策。

2. 在政策內容頁面中，選取**應用程式設定 > KSN 與統計資料**。

3. 在**傳送統計資料**區段，選取**允許資料傳輸，以協助改善應用程式的品質、外觀和效能** 核取方塊。

4. 點擊**儲存**按鈕儲存對政策所做的變更並結束政策內容視窗。

下次與卡巴斯基安全管理中心執行裝置同步之後，可進行行動裝置設定。

在行動裝置上設定通知

您只能為 Android 定義這些政策設定。

如果不希望 Kaspersky Endpoint Security for Android 通知分散行動裝置使用者的注意力，您可以停用某些通知。

Kaspersky Endpoint Security 使用下列工具顯示裝置防護狀態：

- **防護狀態通知**。此通知會釘選到通知列。防護狀態通知無法移除。通知會顯示裝置防護狀態（例如，  ）以及問題數量，如有。您可以輕觸裝置防護狀態通知，在應用程式中查看問題清單。

- **應用程式通知**。這些通知會告知裝置使用者關於應用程式的資訊（例如，威脅偵測）。

- **彈出訊息**。彈出訊息需要裝置使用者採取行動（例如，偵測到威脅時採取行動）。

所有 Kaspersky Endpoint Security for Android 通知均為預設啟用。

在 Android 13，裝置使用者應在初始設定精靈期間或之後授予權限，才能傳送通知。

Android 裝置使用者可以在通知列的設定中停用來自 Kaspersky Endpoint Security for Android 的所有通知。如果停用通知，使用者不會監控應用程式的執行，並且可能會略過重要資訊（例如，有關裝置與卡巴斯基安全管理中心同步期間發生的故障資訊）。在這種情況下，要瞭解應用程式執行狀態，使用者必須開啟 Kaspersky Endpoint Security for Android。

要設定在行動裝置上顯示 Kaspersky Endpoint Security for Android 操作通知，請執行以下操作：

1. 開啟政策內容視窗：

- 在卡巴斯基安全管理中心網頁主控台或雲端主控台的主視窗中，選取**裝置** > **政策和設定檔**。在開啟的群組政策清單中，點擊要配置的政策名稱。

- 在卡巴斯基安全管理中心網頁主控台或雲端主控台的主視窗中，選取**裝置** > **行動** > **裝置**。點擊您要設定政策的行動裝置，然後在**使用中的政策和政策設定檔**標籤上選取該政策。

2. 在政策內容頁面中，選取**應用程式設定** > **通知和報告**。

3. 在**通知**區段，設定通知的顯示：

   - 要隱藏所有通知和彈出訊息，停用**Kaspersky Endpoint Security 在背景執行時顯示通知**切換按鈕。

     Kaspersky Endpoint Security for Android 將僅顯示防護狀態通知。通知會顯示裝置防護狀態（例如，  ）以及問題數量。此應用程式還會在使用者使用應用程式時顯示通知（例如，使用者手動更新病毒資料庫）。

     Kaspersky 專家建議您啟用通知和彈出訊息。如果應用程式在背景模式且停用通知和彈出訊息時，應用程式將無法針對威脅即時警告使用者。行動裝置使用者只有在開啟應用程式時，才能得知裝置的防護狀態。

   - 在**使用者裝置顯示的安全性問題清單**中，選取您希望在使用者行動裝置上顯示的 Kaspersky Endpoint Security for Android 問題。

4. 點擊**儲存**按鈕儲存對政策所做的變更並結束政策內容視窗。

下次與卡巴斯基安全管理中心執行裝置同步之後，可進行行動裝置設定。

偵測裝置上的駭客攻擊

卡巴斯基安全管理中心網頁主控台可讓您偵測 Android 裝置上的裝置駭客攻擊（根權限）和 iOS 裝置上的破解。被駭客入侵的裝置系統檔案將不受防護，因此可能會被修改。此外，來自未知來源的其他應用程式可能會安裝在被駭客入侵的裝置上。在偵測到駭客嘗試後，建議您立即還原裝置的正常操作。

Kaspersky Endpoint Security for Android 在使用者取得根權限時使用下列服務偵測：

- *內嵌 Kaspersky Endpoint Security for Android 服務*。這是用來檢查行動裝置使用者是否已獲得 Root 權限（卡巴斯基行動安全 SDK）的 Kaspersky 服務。

- *SafetyNet Attestation*。這是一種 Google 服務，用來檢查作業系統的完整性、分析裝置硬體和軟體，以及識別其他安全問題。如需 SafetyNet Attestation 的詳細資訊，請造訪 Android 技術支援網站。

Kaspersky Security for iOS 使用下列服務偵測破解：

- *內嵌 Kaspersky Security for iOS 服務*。這是用來檢查行動裝置是否遭到破解（卡巴斯基行動安全 SDK）的卡巴斯基服務。

如果裝置被駭客入侵，您會收到一條通知。您可以在卡巴斯基安全管理中心網頁主控台的**監控和報告** > **主控台**標籤上查看駭客通知。還可以在事件通知設定中停用有關駭客的通知。

在 Android 裝置上，如果裝置被駭客入侵，您可以對裝置上的使用者活動施加限制（例如鎖定裝置）。您可以使用合規性控制元件施加限制。為此，請使用**裝置已取得 Root 權限** 標準建立合規性規則。

定義產品授權設定

您可以為 Android 和 iOS 裝置定義這些政策設定。

要在卡巴斯基安全管理中心網頁主控台或 Cloud Console 中管理行動裝置，您必須在行動裝置上啟用行動應用程式。在行動裝置上啟用 Kaspersky Endpoint Security for Android 應用程式或 Kaspersky Security for iOS 應用程式是透過向應用程式提供有效的產品授權資訊來完成的。當裝置與卡巴斯基安全管理中心同步時，產品授權資訊將與政策一起傳遞到行動裝置。

如果在行動裝置上安裝行動應用程式之後 30 天內未完成行動應用程式的啟用，應用程式將自動轉換至受限功能模式。在此模式中，大部分應用程式元件都無法執行。當轉換到受限功能模式時，應用程式將停止執行與卡巴斯基安全管理中心的自動同步。因此，如果未在應用程式安裝後 30 天內完成應用程式啟用，使用者必須手動與卡巴斯基安全管理中心同步裝置。

要定義群組政策的產品授權設定，您可以執行以下操作：

1. 開啟政策內容視窗：
   - 在卡巴斯基安全管理中心網頁主控台或雲端主控台的主視窗中，選取**裝置 > 政策和設定檔**。在開啟的群組政策清單中，點擊要配置的政策名稱。
   - 在卡巴斯基安全管理中心網頁主控台或雲端主控台的主視窗中，選取**裝置 > 行動 > 裝置**。點擊您要設定政策的行動裝置，然後在**使用中的政策和政策設定檔**標籤上選取該政策。
2. 在政策內容頁面中，選取**應用程式設定 > 產品授權**。
3. 使用下拉清單從管理伺服器的金鑰儲存空間中選取所需的產品授權金鑰。

   產品授權金鑰的詳細資訊會顯示在下面的欄位中。

   如果行動裝置上現有的啟用金鑰與上面下拉清單中選取的金鑰不同，您可以替換它。為此，請選定**如裝置上的金鑰不同，請使用特定金鑰取代**核取方塊。
4. 點擊**儲存**按鈕儲存對政策所做的變更並結束政策內容視窗。

下次與卡巴斯基安全管理中心執行裝置同步之後，可進行行動裝置設定。

配置事件

您可以為 Android 和 iOS 裝置定義這些政策設定。

您可以定義發生在使用者裝置上並傳送到卡巴斯基安全管理中心的事件的儲存和通知設定。

只有在修改政策時才能配置事件。

事件按重要性級別分佈在以下標籤上：

- **緊急**

  緊急事件表示可能導致資料遺失、操作故障或嚴重錯誤的問題。

- **功能故障**

  功能故障表示應用程式執行過程中發生的嚴重問題、錯誤或故障。

- **警告**

  警告不一定是嚴重的，但仍然表示未來可能出現的問題。

- **資訊**

  資訊事件通知有關操作或程序的成功完成，或應用程式的正常執行。

在每個部分，清單會顯示事件類型和卡巴斯基安全管理中心的預設事件儲存期限（以天為單位）。

從事件清單中，您可以執行以下操作：

- 在傳送到卡巴斯基安全管理中心的事件類型清單中新增或移除事件類型。
- 為每種事件類型定義儲存和通知設定，例如：此類事件必須在管理伺服器資料庫中儲存多長時間，或者是否將透過電子郵件通知您此類事件。

有關在卡巴斯基安全管理中心網頁主控台和雲端主控台中配置事件的更多詳細資訊：

- 如果您使用卡巴斯基安全管理中心網頁主控台，請參閱*卡巴斯基安全管理中心說明*。
- 如果您使用的是卡巴斯基安全管理中心雲端主控台，請參閱*卡巴斯基安全管理中心雲端主控台說明*。

配置有關在使用者裝置上安裝、更新和移除應用程式的事件

您可以為 Android 和 iOS 裝置定義這些政策設定。

如果您使用卡巴斯基安全管理中心雲端主控台，在您的使用者裝置上發生並傳送到卡巴斯基安全管理中心的事件類型清單不包括裝置上應用程式的安裝、更新和移除。這是因為此類事件經常發生，當達到事件計數限制時，這些事件可能會替換卡巴斯基安全管理中心資料庫中的其他重要事件。它們還可能影響管理伺服器或 DBMS 的效能以及與卡巴斯基安全管理中心雲端主控台的網際網路連線頻寬。

如果您仍然想要儲存這種類型的事件並收到有關它們的通知，請按照本節中的說明操作。

要在使用者裝置上配置有關安裝、更新和移除應用程式的事件：

1. 在政策設定的**"事件配置"**標籤上，將**"應用程式已被安裝或移除(已安裝應用程式的清單)**資訊事件類型新增到儲存在管理伺服器資料庫中的事件清單中。

   有關配置事件的更多詳細資訊，請參閱*卡巴斯基安全管理中心雲端主控台說明*。

2. 啟用**傳送在所有行動裝置已安裝應用程式的清單**選項。

有關在使用者裝置上安裝、更新和移除應用程式的事件會儲存在卡巴斯基安全管理中心資料庫中。您會收到有關這些事件的通知。

網路負載

本節包含有關行動裝置和卡巴斯基安全管理中心之間交換的網路流量的資訊。

流量

工作	外出流量	內進流量	總流量
應用程式初始佈署，MB	0.08	17.76	17.84
病毒資料庫初始更新（流量可能會因病毒資料庫的大小而不同），MB	0.04	2.21	2.25
行動裝置與卡巴斯基安全管理中心同步，MB	0.03	0.02	0.05
病毒資料庫定期更新（流量可能會因病毒資料庫的大小而不同），MB	0.08	3.06	3.14
執行竊盜防護命令。定位裝置（流量可能會因嵌入式攝影鏡頭規格和影像品質而不同），MB	0.09	0.8	0.17
執行竊盜防護命令。拍攝臉部快照，MB	1.0	0.02	1.02
執行竊盜防護命令。裝置鎖定，MB	0.06	0.05	0.11
平均每日流量，MB	0.22	6.96	7.18

在以 MMC 為基礎的管理主控台中工作

本「說明」部分描述如何使用卡巴斯基安全管理中心以 MMC 為基礎的管理主控台來防護和管理行動裝置。

關鍵用例

安裝

如何遠端安裝 Kaspersky Endpoint Security for Android？

如何封鎖使用者移除 Kaspersky Endpoint Security for Android？

如何啟動 Kaspersky Endpoint Security for Android？

防護

如何鎖定遺失或被竊的裝置？

如何保護自己以防範網際網路威脅？

如何禁止使用空白密碼？

使用協力廠商解決方案

Android Enterprise（具有公事包圖示的應用程式、配置 Android 工作設定檔）

VMware AirWatch、MobileIron、IBM Maas360、SOTI MobiControl

控制

如何封鎖使用者在裝置上玩遊戲？

如何在裝置上配置存取網站的權限？

如何偵測根權限？

管理

如何在裝置上配置信箱？

如何將行動裝置連線到 Wi-Fi？

如何安裝企業應用程式？

關於 Kaspersky Security for Mobile

Kaspersky Security for Mobile 是一款用於防護和管理公司行動裝置的整合方案，同時也是公司員工為公司目的使用的個人行動裝置安全解決方案。

Kaspersky Security for Mobile 包括以下元件：

- Kaspersky Endpoint Security for Android 應用程式

  Kaspersky Endpoint Security for Android 應用程式能確保為行動裝置提供保護，幫助抵禦網路威脅、病毒和其他會造成威脅的程式攻擊。

- Kaspersky Endpoint Security for Android 管理外掛程式

  Kaspersky Endpoint Security for Android 的管理外掛程式提供介面，用於透過卡巴斯基安全管理中心管理主控台，管理行動裝置以及安裝在這些裝置上的行動 APP。

- Kaspersky Device Management for iOS 管理外掛程式

Kaspersky Device Management for iOS 管理外掛程式允許您在不使用 iPhone 設定公用程式或 Exchange 管理主控台的情況下，為透過 iOS MDM 協定連線到卡巴斯基安全管理中心的裝置（以下簡稱「iOS MDM 裝置」）和透過 Exchange ActiveSync 協定連線到卡巴斯基安全管理中心的裝置（以下簡稱「EAS 裝置」）定義來配置設定。

管理外掛程式整合到*卡巴斯基安全管理中心遠端管理系統*中。管理員可以使用單個的卡巴斯基安全管理中心管理主控台管理公司網路中所有行動裝置，也可以管理用戶端電腦和虛擬系統。將行動裝置連線至管理伺服器後，行動裝置就變成託管裝置。管理員可以遠端監控託管裝置。

Kaspersky Endpoint Security for Android 行動應用程式也隨附於 *Kaspersky Endpoint Security Cloud 遠端管理系統*，隨系統一起執行。如需透過 Kaspersky Endpoint Security Cloud 使用應用程式的詳細資訊，請參閱 *Kaspersky Endpoint Security Cloud 線上說明*。

Kaspersky Endpoint Security for Android 行動 APP 也可能作為 AppConfig Community 參與者的協力廠商 EMM 解決方案的一部分執行。

在 MMC 為基礎的管理主控台中管理行動裝置的主要功能

Kaspersky Security for Mobile 包括以下功能：

- 透過使用 Google Play 連結將連線 Android 裝置的郵件訊息分發到卡巴斯基安全管理中心。
- 遠端連線行動裝置到卡巴斯基安全管理中心和其他第三方 EMM 系統（例如，VMWare AirWatch、MobileIron、IBM Maas360、SOTI MobiControl）。
- Kaspersky Endpoint Security for Android 應用程式的遠端配置，以及服務、應用程式和 Android 裝置功能的遠端配置。
- 根據企業安全需求遠端管理行動裝置。
- 預防行動裝置在遺失或被竊時儲存的企業資訊洩露（竊盜防護）。
- 企業安全需求合規性控制（合規性控制）。
- 行動裝置網際網路使用控制（網頁防護）。
- 在行動裝置上設定企業郵件，包括在公司佈署了 Microsoft Exchange 郵件伺服器的組織（僅適用於 iOS 和 Samsung 裝置）。
- 設定企業網路 (Wi-Fi、VPN)，以便在行動裝置上使用後者。VPN 只能在 iOS 和 Samsung 裝置上配置。
- 配置當政策規則被違反時將顯示在卡巴斯基安全管理中心中的行動裝置狀態：緊急、警告、正常。
- 設定在 Kaspersky Endpoint Security for Android 應用程式上顯示給使用者的通知。
- 支援 Samsung KNOX 2.6 或更新版本的裝置的設定配置。
- 在支援 Android 工作設定檔之裝置上配置設定。
- 透過 Samsung KNOX Mobile Enrollment 主控台佈署 Kaspersky Endpoint Security for Android 應用程式。Samsung KNOX Mobile Enrollment 設計用於在從官方提供商購買的 Samsung 裝置上批量安裝和初始化應用設定。

- 升級 Kaspersky Endpoint Security for Android 應用程式到指定版本可以使用卡巴斯基安全管理中心政策來執行。
- Kaspersky Endpoint Security for Android 應用程式的狀態和事件的管理員通知可以在卡巴斯基安全管理中心中或透過郵件通訊。
- 政策設定的變更控制（修訂歷史記錄）。

Kaspersky Security for Mobile 包括以下防護和管理元件：

- 病毒防護（適用於 Android 裝置）
- 竊盜防護（適用於 Android 裝置）
- 網頁防護（適用於 Android 和 iOS 裝置）
- 應用程式控制（適用於 Android 裝置）
- 合規控制（適用於 Android 裝置）
- 偵測裝置上的 root 權限（適用於 Android 裝置）

關於 Kaspersky Endpoint Security for Android 應用程式

Kaspersky Endpoint Security for Android 應用程式能確保為行動裝置提供保護，幫助抵禦網路威脅、病毒和其他會造成威脅的程式攻擊。

Kaspersky Endpoint Security for Android 應用程式包括以下元件：

- **病毒防護**。病毒防護功能會使用病毒資料庫及卡巴斯基安全網路雲端服務偵測並消除威脅。病毒防護功能包含以下元件：
  - 防護。功能在開啟的檔中偵測威脅、掃描新應用、即時防護裝置。
  - 掃描。它根據需要針對整個檔案系統、僅針對已安裝的應用程式或針對選定的檔案或資料夾啟動。
  - 更新。「更新」功能允許您為應用程式下載新的病毒資料庫。
- **竊盜防護。**該元件在裝置遺失或被竊時防護裝置上的資訊，防禦未經授權的存取。此元件允許您向裝置發送以下命令：
  - **定位**以取得裝置位置的座標。
  - **警報**以使裝置大聲發出警報。
  - **臉部快照**可讓裝置在有人試圖解鎖時，用前相機拍照。
  - **抹除**企業資料以保護敏感的公司資訊。
- **Web 防護。**該元件可以封鎖用於擴散惡意程式碼的惡意網站。Web 防護也可以封鎖用於竊盜使用者機密資料（例如，網路銀行或電子錢包系統的密碼）並存取使用者財務資訊的虛假（釣魚）網站。Web 防護將在您開啟網站前使用卡巴斯基安全網路雲端服務掃描網站。掃描之後，Web 防護將允許可信的網站載入並封鎖惡意網站。Web 防護也支援按卡巴斯基安全網路雲端服務中所定義類別篩選網站。這允許管理員限制使用者對某些類別網頁的存取（例如「賭博、彩票、抽獎」或「網際網路通訊」類別中的網頁）。

- **應用程式控制。**此元件可讓您透過指向分發套件的直接連結或指向 Google Play 的連結，將推薦和所需的應用程式安裝到您的裝置上。應用程式控制還允許您移除那些違反企業安全需求的已封鎖應用程式。

- **合規性控制。**此元件允許檢查受管裝置是否符合企業安全需求，並對不符合要求裝置的某些功能施加限制。

關於 Kaspersky Device Management for iOS

Kaspersky Device Management for iOS 可確保連線至卡巴斯基安全管理中心的移動裝置進行保護和控制，並包含裝置管理功能，例如：

- **密碼保護**。此功能可以設定密碼複雜度要求，讓使用者使用符合企業密碼政策的複雜密碼。

- **網路管理**。此功能可讓您新增核准的 VPN 和 Wi-Fi 網路，或限制其他人的存取。

- **抹除企業資料**。萬一裝置遺失或遭竊，可以向其發送「抹除」命令，保護公司的敏感資訊。

- **Web 防護**。該元件可以封鎖用於擴散惡意程式碼的惡意網站。Web 防護也可以封鎖用於竊盜使用者機密資料（例如，網路銀行或電子錢包系統的密碼）並存取使用者財務資訊的虛假（釣魚）網站。Web 防護將在您開啟網站前使用卡巴斯基安全網路雲端服務掃描網站。掃描之後，Web 防護將允許可信的網站載入並封鎖惡意網站。Web 防護也支援按卡巴斯基安全網路雲端服務中所定義類別篩選網站。這允許管理員限制使用者對某些類別網頁的存取（例如「賭博、彩票、抽獎」或「網際網路通訊」類別中的網頁）。

- **應用程式限制。**此元件讓您可以控制裝置本機應用程式（如 iTunes、Safari 或 Game Center）是否可以在監控裝置上使用。

- **功能限制。**此元件允許檢查受管裝置是否符合企業安全需求，並對不符合要求裝置的某些功能施加限制。

關於 Exchange 信箱

*Exchange 信箱*是 Exchange ActiveSync 服務的用戶端應用程式。該應用程式旨在協助企業使用者使用電子郵件、行事曆、聯絡人和工作。Exchange 信箱允許您將行動裝置連線到 Microsoft Exchange 伺服器。如需 Exchange ActiveSync 服務的詳細資訊，請存取 *Microsoft 技術支援網站*。

若要使用 Exchange ActiveSync 協定管理行動裝置，必須在 Microsoft Exchange 伺服器上佈署 Exchange 伺服器。如需安裝 Exchange Server 的詳細資訊，請參閱*卡巴斯基安全管理中心說明*。不需要在行動裝置上進行其他設定。

使用 Exchange 信箱，您就可以透過群組政策遠端設定 EAS 裝置，並傳送資料抹除命令。以下作業系統支援 Exchange ActiveSync 協定：

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

- iOS
- Symbian

Exchange ActiveSync 裝置的一組管理設定取決於行動裝置執行的作業系統。有關適用於特定作業系統的 Exchange ActiveSync 協定的支援功能的詳細資訊，請參閱特定作業系統的文件。

關於 Kaspersky Endpoint Security for Android 管理外掛程式

Kaspersky Endpoint Security for Android 的管理外掛程式提供介面，用於透過卡巴斯基安全管理中心管理主控台，管理行動裝置以及安裝在這些裝置上的行動 APP。Kaspersky Endpoint Security for Android 管理外掛程式可用於：

- 為行動裝置建立群組安全性政策。
- 遠端配置使用者行動裝置中的 Kaspersky Endpoint Security for Android 應用程式的運作設定。
- 接收關於使用者裝置中的 Kaspersky Endpoint Security for Android 行動應用程式運作情況的報告和統計資料。

預設情況下，佈署卡巴斯基安全管理中心時會安裝 Kaspersky Endpoint Security for Android 管理外掛程式。該外掛程式不需要單獨安裝。

關於 Kaspersky Device Management for iOS 管理外掛程式

Kaspersky Device Management for iOS 的管理外掛程式提供了介面，用途是透過卡巴斯基安全管理中心管理主控台，來管理透過 iOS MDM 和 Exchange ActiveSync 協定連線的行動裝置。Kaspersky Device Management for iOS 管理外掛程式可用於以下用途：

- 為行動裝置建立群組安全性政策。
- 遠端設定使用 Exchange ActiveSync 協定連線的裝置（以下簡稱「EAS 裝置」）。
- 遠端設定使用 iOS MDM 協定連線的裝置（以下簡稱「iOS MDM 裝置」）。
- 接收使用者行動裝置的執行報告和統計資料。

有關透過 iOS MDM 和 Exchange ActiveSync 協定將行動裝置連線到卡巴斯基安全管理中心的更多詳細資訊，請參閱*卡巴斯基安全管理中心說明*。

預設情況下，佈署卡巴斯基安全管理中心時會安裝 Kaspersky Device Management for iOS 管理外掛程式。該外掛程式不需要分開安裝。

硬體和軟體需求

本節列出用於在行動裝置上佈署應用程式的管理員電腦的硬體和軟體需求，以及 Kaspersky Security for Mobile 支援的行動裝置作業系統。

管理員電腦的硬體和軟體需求

若要佈署 Kaspersky Security for Mobile 整合解決方案，管理員的電腦必須符合卡巴斯基安全管理中心的硬體需求。如需卡巴斯基安全管理中心的硬體需求詳細資訊，請參閱*卡巴斯基安全管理中心說明*。

若要使用 Kaspersky Endpoint Security for Android 的管理外掛程式，必須在管理員的電腦上安裝卡巴斯基安全管理中心 12 或更高版本的管理主控台。

若要使用 Kaspersky Device Management for iOS 管理外掛程式，管理員的電腦必須滿足以下軟體要求：

- 卡巴斯基安全管理中心 12 或更高版本的管理主控台
- Exchange 伺服器元件
- iOS MDM 伺服器元件
- SSE2 版本或最近版本的手冊

若要透過管理伺服器佈署 Kaspersky Endpoint Security for Android 行動 APP，管理員的電腦必須滿足以下軟體要求：

- 卡巴斯基安全管理中心 12 或更高版本
- Kaspersky Endpoint Security for Android 管理外掛程式

從相關線上商店佈署 Kaspersky Endpoint Security for Android 行動 APP 時，對管理員的電腦沒有任何軟體要求。

Kaspersky Endpoint Security for Android 行動應用程式也隨附於 Kaspersky Endpoint Security Cloud 遠端管理系統（6.0 版以上）供使用者使用。如需透過 Kaspersky Endpoint Security Cloud 使用應用程式的詳細資訊，請參閱*Kaspersky Endpoint Security Cloud 說明*。

Kaspersky Endpoint Security for Android 行動 APP 可以與協力廠商 EMM 系統一起工作：

- 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

支援安裝 Kaspersky Endpoint Security for Android 應用程式對使用者行動裝置的硬體和軟體要求

Kaspersky Endpoint Security for Android 應用程式具有以下硬體和軟體要求：

- 智慧手機或平板電腦的解析度為 320x480 畫素或更高
- 裝置的主記憶體具有 65 MB 的可用空間
- Android 5.0–13（包含 Android 12L，不包含 Go Edition）
- x86、x86-64、Arm5、Arm6、Arm7 或 Arm8 處理器架構

應用程式僅安裝到裝置的主記憶體。

iOS MDM 設定檔的硬體和軟體需求

對於 iOS MDM 設定檔，裝置必須滿足以下硬體和軟體需求：

- iOS 10.0–15.0 或 iPadOS 13–15
- 網際網路連線

已知問題和考量事項

Kaspersky Endpoint Security for Android 有許多已知問題，這些問題對於應用程式的運作狀態並不會造成關鍵影響。

安裝應用程式時的已知問題

- Kaspersky Endpoint Security for Android 僅安裝在裝置的主記憶體中。
- 在執行 Android 7.0 的裝置上，當 Kaspersky Endpoint Security for Android 被禁止覆蓋其他視窗時，試圖停用 Kaspersky Endpoint Security for Android 的管理員權限時可能發生錯誤。該問題是因一個眾所周知的 Android 7 缺陷 導致。
- 在執行 Android 7.0 或更新版本的裝置上，Kaspersky Endpoint Security for Android 不支援多視窗模式。
- Kaspersky Endpoint Security for Android 與執行 Chrome 作業系統的 Chromebook 裝置不相容。
- Kaspersky Endpoint Security for Android 與執行 Android（Go Edition）作業系統的裝置不相容。
- 當將 Kaspersky Endpoint Security for Android 應用程式與協力廠商 EMM 系統（例如，VMWare AirWatch）一起使用時，僅病毒防護和 Web 防護元件可用。管理員可以在 EMM 系統主控台中配置病毒防護和 Web 防護的設定。在這種情況下，有關應用程式執行的通知僅在 Kaspersky Endpoint Security for Android 應用程式的介面（報告）中可用。

升級應用程式時的已知問題

- 您只能將 Kaspersky Endpoint Security for Android 升級至最近的應用程式版本。Kaspersky Endpoint Security for Android 不能降級至較老版本。
- 若要使用獨立安裝套件升級 Kaspersky Endpoint Security for Android，必須允許在使用者的行動裝置上安裝來自未知來源的應用程式。
- 如果 Kaspersky Endpoint Security for Android 是從 Google Play 安裝的，則可以透過 Google Play 更新。如果該應用程式是使用其他方法安裝的，則不能透過 Google Play 更新。
- 如果您透過卡巴斯基安全管理中心安裝了 Kaspersky Endpoint Security for Android，則可以透過卡巴斯基安全管理中心進行更新。如果該應用程式是從 Google Play 安裝的，則不能透過卡巴斯基安全管理中心更新應用程式。

- 將管理外掛程式升級到技術版本 33 後，Kaspersky Endpoint Security for Android 應用程式也必須升級到技術版本 33。否則，您將無法在某些使用者的裝置上啟動 Samsung KNOX。

病毒防護操作的已知問題

- 由於技術限制，Kaspersky Endpoint Security for Android 無法掃描大小為 2 GB 或更大的檔案。在掃描期間，應用程式將略過此類別檔案，而不會通知您此類別檔案被略過。
- 要對裝置進行資訊尚未新增到病毒資料庫中的新威脅的附加分析，您必須啟用卡巴斯基安全網路。*卡巴斯基安全網路 (KSN)* 是個雲端服務基礎結構，向 Kaspersky 的線上知識庫提供檔案信譽、網路資源和軟體等資訊。若要使用 KSN，行動裝置必須已連線至網際網路。
- 在某些情況下，從行動裝置上的管理伺服器更新病毒資料庫可能會失敗。在這種情況下，請在管理伺服器上執行病毒資料庫更新工作。
- 在某些裝置上，Kaspersky Endpoint Security for Android 不會偵測透過 USB OTG 連線的裝置。無法對此類別裝置執行病毒掃描。
- 在執行 Android 11.0 或更高版本的裝置上，使用者必須授予「允許存取管理所有檔案」權限。
- 在執行 Android 7.0 或更新版本的裝置上，病毒掃描執行排程的配置視窗可能顯示不正確（管理元件未顯示）。該問題是因一個眾所周知的 Android 7 缺陷 導致。
- 在執行 Android 7.0 的裝置上，於延伸模式下執行即時防護並不會偵測儲存在外部 SD 卡上的檔案威脅。
- 在執行 Android 6.0 的裝置上，Kaspersky Endpoint Security for Android 不偵測下載惡意檔案到裝置記憶體的操作。當惡意檔案執行時，或者在裝置病毒掃描過程中，惡意軟體可以被病毒防護偵測到。該問題是因一個眾所周知的 Android 6.0 缺陷 導致。要確保裝置安全，建議設定排除病毒掃描。

Web 防護操作中的已知問題

- Android 裝置上的 Web 防護僅在 Google Chrome 瀏覽器（包括自訂標籤功能）、Huawei Browser 和 Samsung Internet Browser 中可用。如果使用工作設定檔且只針對工作設定檔啟用 Web 防護，則 Samsung Internet Browser 的 Web 防護不會封鎖行動裝置上的網站。
- 工作設定檔中的 Kaspersky Endpoint Security 僅掃描 HTTPS 流量中的網站網域。如果應用程式安裝在工作設定檔，惡意和釣魚網站可能保持不被封鎖。如果網域受到信任，Web 防護可能會略過威脅（例如，`https://trusted.domain.com/phishing/`）。如果網域不受到信任，Web 防護則會封鎖惡意和釣魚網站。
- 要使 Web 防護工作，您必須啟用卡巴斯基安全網路。Web 防護會基於有關網站信譽和類別的 KSN 資料封鎖網站。
- 如果透過以下方式開啟被攔截的網站，在執行 Android 6.0 並安裝 Google Chrome 51 版（或任何更早版本）的裝置上，Web 防護可能會保持解除封鎖這些網站（該問題是因一個眾所周知的 Google Chrome 缺陷導致）：
  - 透過搜尋結果。
  - 透過書簽清單。
  - 透過搜尋歷史記錄。
  - 使用網址自動填寫功能。

- 在 Google Chrome 中的新標籤頁中開啟網站。

- 如果透過 Google 搜尋結果開啟被攔截的網站，當瀏覽器設定中啟用了「**合併標籤和應用程式**」功能時，這些網站可能在 Google Chrome 50 版（或任何更早版本）中保持解除封鎖。該問題是因一個眾所周知的 Google Chrome 缺陷導致。

- 如果使用者從其他應用程式開啟網站，例如從 IM 用戶端應用程式開啟，則封鎖類別的網站可能在 Google Chrome 中保持不被封鎖。該問題關乎可存取功能服務與 Chrome 自訂標籤功能如何配合使用。

- 如果使用者從上下文功能表或其他應用程式（例如從 IM 用戶端應用程式）以背景模式開啟網站，被攔截的網站可能在 Samsung Internet Browser 中保持不被封鎖。

- 必須將 Kaspersky Endpoint Security for Android 設定為可存取功能以確保 Web 防護能正常執行。

- 當在 Web 防護設定中輸入網址時，請遵守以下規則：

  - 對於 Android 裝置，採用一般運算式格式指定位址（例如，`http:\/\/www\.example\.com.*`）。

  - 對於 iOS MDM 裝置，指定 HTTP 或 HTTPS 資料傳輸協議（例如，`http://www.example.com`）。

- 當重新整理頁面時，Samsung Internet Browser 在「**僅允許列出的網站**」Web 防護模式下可能會封鎖允許的網站。如果一般運算式包含進階設定（例如，`^https?:\/\/example\.com\/pictures\/`），則會封鎖網站。建議使用不含附加設定的一般運算式（例如，`^https?:\/\/example\.com`）。

竊盜防護操作中的已知問題

- 為了將命令及時傳送到 Android 裝置，應用會使用 Firebase Cloud Messaging (FCM) 服務。如果未設定 FCM，將僅在與卡巴斯基安全管理中心同步期間按照政策中定義的排程（例如，每 24 小時）將命令傳送到裝置。

- 要鎖定裝置，必須將 Kaspersky Endpoint Security for Android 設定為裝置管理員。

- 要鎖定執行 Android 7.0 或更高版本的裝置，必須將 Kaspersky Endpoint Security for Android 設定為可存取功能。

- 在某些裝置上，如果裝置上啟用了低電量模式，竊盜防護命令可能無法執行。此缺陷已在 Alcatel 5080X 上確認。

- 若要定位執行 Android 10.0 或更新版本的裝置，使用者必須授與「任何時間」均可存取裝置位置的權限。

- 若要在執行 Android 11.0 或更新版本的裝置上拍攝臉部快照，使用者必須授與「使用應用程式期間」的權限來存取相機。

應用程式控制操作中的已知問題

- 必須將 Kaspersky Endpoint Security for Android 設定為可存取功能以確保應用程式控制能正常執行。

- 要使應用程式控制（應用程式類別）工作，您必須啟用卡巴斯基安全網路。應用程式控制會基於 KSN 中可用的資料確定應用程式的類別。若要使用 KSN，行動裝置必須已連線至網際網路。對於應用程式控制，您可以將單個應用程式新增到封鎖和允許的應用程式清單。在這種情況下，無需 KSN。

- 當配置應用程式控制時，建議清除「**封鎖系統應用程式**」核取方塊。封鎖系統應用程式可能會導致裝置執行問題。

配置電子郵件的已知問題

- 遠端配置信箱僅在以下裝置上可用：
  - iOS MDM 裝置。
  - Samsung 裝置 (Exchange ActiveSync)。
  - 安裝了 TouchDown 郵件用戶端的 Android 裝置。

    在 Kaspersky Endpoint Security for Android 的先前版本中，您可以使用卡巴斯基安全管理中心在使用者裝置上遠端配置 TouchDown 設定檔設定。Kaspersky Endpoint Security for Android Service Pack 4 不再支援 TouchDown。如需詳細資訊，請參閱 *Symantec 技術支援網站*。

    升級 Kaspersky Endpoint Security for Android 管理外掛程式後，政策中的 TouchDown 設定被隱藏但被儲存。當有新裝置被連線時，TouchDown 設定將在套用政策後被配置。

    在政策被修改和儲存後，TouchDown 設定將被刪除。使用者裝置上的 TouchDown 設定在套用政策後將被清除。

配置裝置解鎖密碼強度的已知問題

- 在執行 Android 10.0 或更高版本的裝置上，Kaspersky Endpoint Security 會將密碼強度要求解析為其中一個系統值：中度或高度。

  如果要求的密碼長度是 1 到 4 個符號，那麼應用程式會提示使用者設定中等強度的密碼。密碼必須是數字（PIN）且沒有重複或有順序（如 1234）的序列或英數字母。PIN 或密碼的長度必須至少有 4 個字元。

  如果要求的密碼長度為 5 個以上的符號，那麼應用程式會提示使用者設定高強度密碼。密碼必須是數字（PIN），沒有重複或有順序的序列或英數字母（password）。 PIN 必須至少有 8 位數，密碼長度必須至少有6個字元。

- 在執行 Android 10.0 或更高版本的裝置上，螢幕指紋解鎖的使用僅可針對工作設定檔來加以管理。

- 在執行 Android 7.1.1 的裝置上，如果解鎖密碼不符合企業安全需求（合規性控制），嘗試透過 Kaspersky Endpoint Security for Android 變更解鎖密碼時，「設定」系統應用程式可能無法正常執行。該問題是因一個眾所周知的 Android 7.1.1 缺陷導致。這種情況下，僅可使用設定系統應用程式來變更解鎖密碼。

- 在一些執行 Android 6.0 或更新版本的裝置上，如果裝置資料被加密，輸入螢幕解鎖密碼時可能發生錯誤。該問題關乎 MIUI 韌體可存取功能服務的特定功能。

配置 Wi-Fi 的已知問題

- 在執行 Android 版本 8.0 或更新版本的裝置上，Wi-Fi 代理伺服器設定無法由政策重定義。然而，您可以在行動裝置上手動為 Wi-Fi 網路配置代理伺服器設定。

配置 APN 的已知問題

- 遠端配置 APN 僅在執行 iOS MDM 裝置或 Samsung 裝置上可用。

- 在**手機通訊**區域中為 iOS MDM 裝置配置 APN。「**APN**」區域已棄用。調整 APN 設定前，請確認您未勾選 **APN** 區域中的**套用於裝置**核取方塊。

防火牆的已知問題

- 防火牆的使用僅適用於 Samsung 裝置。

配置 VPN 的已知問題

- 遠端配置 VPN 僅在以下裝置上可用：
  - iOS MDM 裝置。
  - Samsung 裝置。

使用容器的已知問題

- 在 Kaspersky Security for Mobile Service Pack 3 Maintenance Release 2 中，不再支援為行動應用程式建立容器。但是，在早期版本的應用程式中建立的容器可以新增到 Android 裝置。
- 要安裝集裝式應用程式，必須在使用者行動裝置上允許從未知來源安裝應用程式。如需不使用 Google Play 安裝應用程式的詳細資訊，請參考 *Android 說明指南*。
- 對於 Android 裝置上包含多於 65,536 個方法（multidex 配置）的應用，不支援應用程式集裝。

應用程式核准保護的已知問題

- 必須將 Kaspersky Endpoint Security for Android 設定為裝置管理員。
- 要防護在執行 Android 7.0 或更高版本的裝置上的應用程式不會被移除，必須將 Kaspersky Endpoint Security for Android 設定為可存取功能。
- 在某些小米和華為裝置上，Kaspersky Endpoint Security for Android 移除防護不工作。該問題是由小米上的 MIUI 7 和 8 韌體和華為上的 EMUI 韌體的特定功能導致。

設定裝置限制的已知問題

- 在執行 Android 10.0 或更高版本的裝置上，不支援禁止使用 Wi-Fi 網路。
- 在執行 Android 10.0 的裝置上，無法完全禁止使用相機。
- 在執行 Android 11 或更高版本的裝置上，必須將 Kaspersky Endpoint Security for Android 設定為可存取功能。Kaspersky Endpoint Security for Android 會提示使用者透過初始配置精靈將該應用程式設定為輔助使用功能。使用者可以略過此步驟或以後在裝置設定中停用此服務。如果是這種情況，您將無法限制相機的使用。

向行動裝置傳送命令時的已知問題

- 在執行 Android 12 或更高版本的裝置上，如果使用者授予「使用大致位置」權限，Kaspersky Endpoint Security for Android 應用程式首先會嘗試取得準確的裝置位置。如果這麼做不成功，則僅在不超過 30 分鐘前

收到裝置的大致位置時才傳回該裝置的大致位置。否則，**定位裝置**命令將失敗。

Android 工作設定檔的已知問題

- 如果您使用政策建立 Android 工作設定檔，使用者必須向安裝在執行 Android 11 或更高版本的裝置上且與工作設定檔相關的 Kaspersky Endpoint Security for Android 授予「允許存取以管理所有檔案」權限。

特定裝置的已知問題

- 在特定裝置上（例如 Huawei、Meizu 和Xiaomi），您必須授與 Kaspersky Endpoint Security for Android 自動啟動權限或手動將其新增至與作業系統一起啟動的應用程式清單。如果未將該應用程式新增到清單，在行動裝置重新啟動後，Kaspersky Endpoint Security for Android 會停止執行其所有功能。此外，如果裝置已鎖定，您無法使用命令解鎖裝置。您只能透過使用一次性密碼解鎖裝置。

- 在執行 Android 6.0 或更新版本的某些裝置（例如，魅族和 Asus）上，在加密資料和重啟 Android 裝置後，您必須輸入數字密碼才能解鎖裝置。如果使用者使用圖形密碼解鎖裝置，您必須將圖形密碼轉換為數字密碼。對於更多轉換圖形密碼到數字密碼的詳情，請參考行動裝置生產商的技術支援網站。該問題關乎可存取功能服務的操作。

- 在某些執行 Android 5.X 的華為裝置上，在 Kaspersky Endpoint Security for Android 設定為可存取功能後，您可能會看到一則有關缺少適當權限的錯誤訊息。若要隱藏此訊息，請在裝置設定中將該應用程式啟用為受保護的應用程式。

- 在某些執行 Android 5.X 或 6.X 的華為裝置上，當為 Kaspersky Endpoint Security for Android 啟用低電量模式時，使用者可以手動終止該應用程式。那樣之後，使用者裝置變成無防護狀態。該問題是因華為軟體的一些功能所導致。若要還原裝置防護，請手動執行 Kaspersky Endpoint Security for Android。建議您在裝置設定中停用 Kaspersky Endpoint Security for Android 的低電量模式。

- 在執行基於 Android 7.0 的 EMUI 韌體的華為裝置上，使用者可以隱藏關於 Kaspersky Endpoint Security for Android 防護狀態的通知。該問題是由於華為軟體的一些功能導致的。

- 在某些小米裝置上，當在政策中設定超過 5 個字元的密碼長度時，使用者將被提示變更螢幕解鎖密碼而不是 PIN 碼。您設定的 PIN 碼不能超過 5 個字元。該問題是由於小米軟體的一些功能導致的。

- 在執行基於 Android 6.0 的 MIUI 韌體的小米裝置上，Kaspersky Endpoint Security for Android 圖示可能在狀態列中隱藏。該問題是由於小米軟體的一些功能所導致。建議您在「通知」設定中允許顯示通知圖示。

- 在一些執行 Android 6.0.1 的 Nexus 裝置上，正常操作所需的權限無法透過 Kaspersky Endpoint Security for Android 快速啟動精靈授予。該問題由眾所周知的 Google 的 Android 安全修補程式缺陷導致。為確保正常執行，必須在裝置設定中手動授予所需權限。

- 在某些執行 Android 7.0 或更高版本的 Samsung 裝置上，當使用者嘗試配置不受支援的方法（例如，圖形密碼）來解鎖裝置時，如果滿足以下條件，裝置可能會鎖定：Kaspersky Endpoint Security for Android 移除防護已啟用並且設定了螢幕解鎖密碼長度要求。要解鎖裝置，您必須傳送特殊命令到裝置。

- 在某些 Samsung 裝置上，無法封鎖使用指紋解鎖螢幕。

- 如果裝置連線到 3G/4G 網路，啟用了低電量模式並限制背景資料，Web 防護無法在一些 Samsung 裝置上啟用。建議您在「低電量」設定中停用「限制背景資料」的功能。

- 在某些 Samsung 裝置上，如果解鎖密碼不符合企業安全需求，Kaspersky Endpoint Security for Android 不會封鎖使用指紋解鎖螢幕。

- 在執行竊盜防護命令（如，定位、裝置鎖定、解鎖和拍攝臉部快照）後，某些 Samsung 裝置上可能會刪除一般憑證和 VPN 憑證。必須重新安裝憑證才能繼續。此問題源於 Mobile Device Fundamentals Protection

Profile（MDFPP）安全標準。

- 在某些榮耀和華為裝置上，您無法限制藍牙的使用。當 Kaspersky Endpoint Security for Android 試圖限制藍芽使用時，作業系統顯示包含拒絕或允許該限制的選項的通知。使用者可以拒絕該限制並繼續使用藍牙。
- 在某些 Samsung 裝置上，從獨立安裝套件安裝或更新 Kaspersky Endpoint Security 後，無法啟用 KNOX MDM 設定檔。
- 在 Blackview 裝置上，使用者可以清除 Kaspersky Endpoint Security for Android 應用程式的記憶體。因此，裝置防護和管理被停用，所有定義的設定都變得無效，並且 Kaspersky Endpoint Security for Android 應用程式將從輔助功能中刪除。這是因為該供應商的裝置提供了具有提升權限的可自訂最近畫面的應用程式。此應用程式可以覆寫 Kaspersky Endpoint Security for Android 設定並且無法替換，因為它是 Android 作業系統的一部分。
- 在某些執行 Android 11 的裝置上，Kaspersky Endpoint Security for Android 應用程式在啟動後立即當機。該問題是因一個眾所周知的 Android 11 缺陷 導致。

在 Android 13 上操作應用程式的已知問題

- 在 Android 13，使用者可以使用前景服務工作管理員阻止 Kaspersky Endpoint Security 在背景中執行。這是因一個眾所周知的 Android 13 問題 導致。
- 在 Android 13，初始應用程式設定開始時，會請求傳送通知的權限。這是由於 Android 13 作業系統的詳細規格。

佈署

本說明部分面向安裝 Kaspersky Security for Mobile 的專家，以及向使用 Kaspersky Security for Mobile 的組織提供技術支援的專家。

解決方案架構

Kaspersky Security for Mobile 包括以下元件：

- Kaspersky Endpoint Security for Android 應用程式

  Kaspersky Endpoint Security for Android 應用程式能確保為行動裝置提供保護，幫助抵禦網路威脅、病毒和其他會造成威脅的程式攻擊。它支援行動裝置與卡巴斯基安全管理中心管理伺服器之間使用 Firebase Cloud Messaging 進行互動。

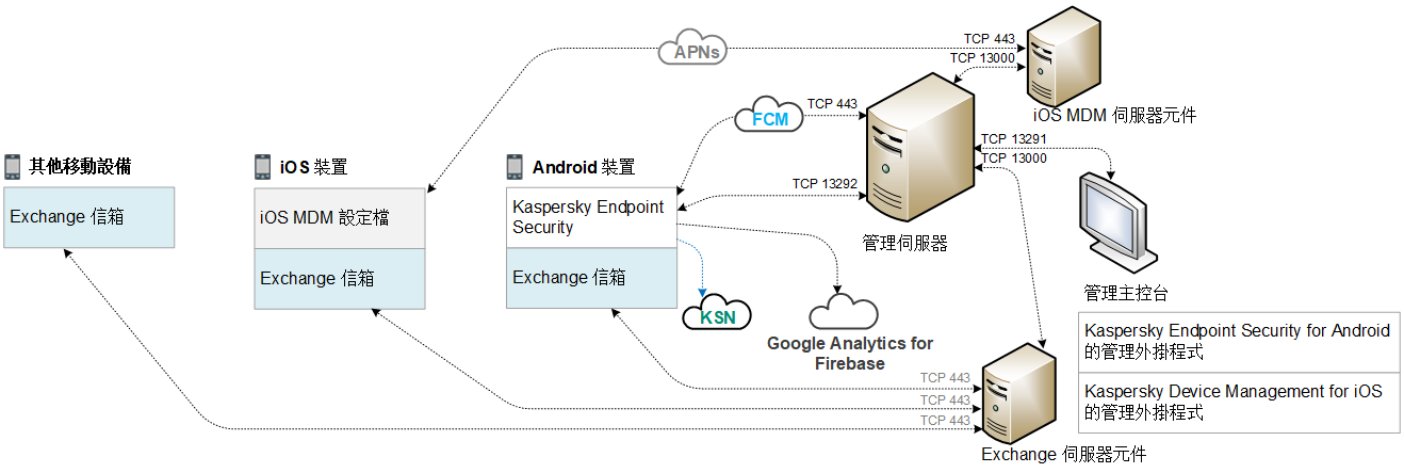
- Kaspersky Endpoint Security for Android 管理外掛程式

  Kaspersky Endpoint Security for Android 的管理外掛程式提供介面，用於透過卡巴斯基安全管理中心管理主控台，管理行動裝置以及安裝在這些裝置上的行動 APP。

- Kaspersky Device Management for iOS 管理外掛程式

  Kaspersky Device Management for iOS 的管理外掛程式提供了介面，用途是透過卡巴斯基安全管理中心管理主控台，來管理透過 iOS MDM 和 Exchange ActiveSync 協定連線的行動裝置。

Kaspersky Security for Mobile 整合解決方案的基礎結構如下圖所示。



Kaspersky Security for Mobile 的基礎結構

如需管理主控台、管理伺服器、Exchange 伺服器和 iOS MDM 伺服器的詳細資訊，請參閱 *卡巴斯基安全管理中心說明*。

常見整合解決方案佈署方案

本節涵蓋了 Kaspersky Security for Mobile 整合解決方案的常見佈署方案。

可以使用不同的佈署方案來在 Android 裝置和 iOS 裝置上佈署整合解決方案。如果組織使用了執行不同作業系統的行動裝置，則應按照相應的佈署方案，分別為每種作業系統安裝應用程式。

Kaspersky Endpoint Security for Android 的佈署方案

Kaspersky Endpoint Security for Android 可透過多種方式佈署在企業網路中的行動裝置上。您可以使用最適合您組織的佈署方式，或者結合使用多種佈署方案。

如需在 Kaspersky Endpoint Security Cloud 中佈署 Kaspersky Endpoint Security for Android 的詳細資訊，請參閱「*Kaspersky Endpoint Security Cloud 說明*」。

透過卡巴斯基安全管理中心佈署 Kaspersky Endpoint Security for Android

您可以使用以下方法透過卡巴斯基安全管理中心佈署 Kaspersky Endpoint Security for Android：

- 傳送包含 Google Play 連結的訊息（建議）
- 傳送包含獨立應用程式套裝連結的訊息

使用 Google Play 佈署 Kaspersky Endpoint Security for Android 包括從管理主控台向裝置使用者傳送包含 Google Play 連結的郵件。

透過提供的獨立包佈署 Kaspersky Endpoint Security for Android 包括由管理員執行的以下幾個步驟：

1. 建立應用程式安裝套件。
2. 配置安裝套件設定。

3. 建立獨立安裝套件。

4. 傳送訊息，其中包含用於將獨立安裝套件下載到 Android 使用者裝置的連結。可使用群發郵件。

使用者在收到包含 Google Play 連結或用於從卡巴斯基安全管理中心網頁伺服器下載安裝套件的連結的郵件後，在行動裝置上安裝 Kaspersky Endpoint Security for Android。無需任何其他準備，即可開始使用應用程式。

從 Google Play 佈署 Kaspersky Endpoint Security for Android

如果無法進行遠端安裝，則建議使用 Google Play 佈署方案。

裝置使用者可從 Google Play 獨立安裝 Kaspersky Endpoint Security for Android。使用者從 Google Play 下載行動 APP 安裝套件，然後在裝置上安裝應用程式。在裝置上安裝應用程式之後，在能夠開始使用它之前，您還需要進行其他準備工作：配置與管理伺服器的連線設定及安裝一般憑證。

透過 KNOX Mobile Enrollment 佈署 Kaspersky Endpoint Security for Android

佈署 Kaspersky Endpoint Security for Android 包括將 KNOX MDM 設定檔新增到行動裝置。KNOX MDM 設定檔包含指向卡巴斯基安全管理中心網頁伺服器或其他伺服器上佈署的應用程式的連結。在行動裝置上安裝應用程式後，您還必須安裝一個一般憑證。

您可以在 Samsung KNOX 一節閱讀關於透過 KNOX Mobile Enrollment 安裝的詳細資訊。

IOS MDM 設定檔佈署方案

*IOS MDM 設定檔*是一個包含用於將執行 iOS 的行動裝置連線到卡巴斯基安全管理中心的設定的設定檔。安裝 iOS MDM 設定檔並與卡巴斯基安全管理中心同步後，裝置將成為受管裝置。行動裝置透過 Apple 推送通知服務 (APN) 進行管理。如需安裝 iOS MDM 設定檔和使用 APN 的詳細資訊，請參閱*卡巴斯基安全管理中心說明*。

使用 iOS MDM 設定檔，您可以執行下列動作：

- 使用群組政策遠端設定 iOS MDM 裝置的設定。
- 傳送裝置鎖定和資料抹除命令。
- 遠端安裝 Kaspersky 應用程式和其他應用程式。

IOS MDM 設定檔可透過多種方式佈署在企業網路中的行動裝置上。您可以使用最適合您組織的佈署方式，或者結合使用多種佈署方案。

在佈署 iOS MDM 設定檔之前，管理員必須執行以下操作：

1. 安裝 iOS MDM 伺服器。
2. 獲取 Apple 推送通知服務憑證（以下簡稱 APN 憑證）。
3. 將 APN 憑證安裝到 iOS MDM 伺服器。

如需安裝 iOS MDM 伺服器和使用 APN憑證的詳細資訊，請參閱*卡巴斯基安全管理中心幫助*。

如需在 Kaspersky Endpoint Security Cloud 中佈署 iOS MDM 設定檔的詳細資訊，請參閱 *Kaspersky Endpoint Security Cloud 說明*。

透過卡巴斯基安全管理中心佈署 iOS MDM 設定檔

透過傳送包含用於下載 iOS MDM 設定檔的連結的郵件，可以透過卡巴斯基安全管理中心佈署 iOS MDM 設定檔。可使用群發郵件。

使用者在收到包含卡巴斯基安全管理中心網頁伺服器連結的郵件後，可將 iOS MDM 設定檔安裝到行動裝置上。無需為 iOS MDM 設定檔進行其他準備工作。

如需建立 iOS MDM 設定檔的詳細資訊，請參閱*卡巴斯基安全管理中心說明*。

準備管理主控台以便佈署整合解決方案

本節提供有關準備管理主控台以便佈署整合解決方案的說明。

配置連線行動裝置的管理伺服器設定

為了讓行動裝置能夠連線到管理伺服器，請先在「管理伺服器」內容中設定行動裝置連線設定，再安裝 Kaspersky Endpoint Security 行動應用程式。

配置連線行動裝置的管理伺服器設定：

1. 在管理伺服器的上下文功能表中，選擇「**內容**」。
   「管理伺服器設定」視窗將開啟。
2. 選擇「**伺服器連線設定 → 其他連接埠**」。
3. 選中「**開啟行動裝置連接埠**」核取方塊。
4. 在「**行動裝置連接埠**」欄位中，指定行動裝置連線至管理伺服器的連接埠。
   預設情況下使用 13292 連接埠。如果取消「**開啟行動裝置連接埠**」核取方塊，或者指定錯誤的連接埠，行動裝置將無法連線至管理伺服器。
5. 請在「**用於啟動行動用戶端的連接埠**」欄位中，指定行動裝置用於連線到管理伺服器以啟動 Kaspersky Endpoint Security for Android 應用程式的連接埠。預設情況下使用 17100 連接埠。
6. 點擊「**確定**」。

在管理主控台中顯示“行動裝置管理”資料夾

透過在管理主控台中顯示「**行動裝置管理**」資料夾，您可以檢視管理伺服器管理的行動裝置清單，配置行動裝置管理設定，在使用者的行動裝置上安裝憑證。

*在管理主控台中顯示「**行動裝置管理**」資料夾：*

1. 在管理伺服器的上下文功能表中，選擇「**檢視**」→「**配置介面**」。
2. 在開啟的視窗中，選擇「**顯示行動裝置管理**」核取方塊。
3. 點擊「**確定**」。

重新啟動管理主控台之後，「**行動裝置管理**」資料夾將顯示在管理主控台樹狀目錄中。

建立管理群組

若要集中設定使用者行動裝置所安裝的 Kaspersky Endpoint Security for Android 應用程式，您必須先將群組政策套用到這些裝置。

若要將政策套用於裝置群組，建議您在使用者裝置上安裝行動 APP 之前，先在「**受管裝置**」中為這些裝置建立單獨的群組。

建立管理群組後，建議配置選項以將要安裝應用程式的裝置自動分配到此群組。然後使用群組政策配置所有裝置通用的設定。

若要建立管理群組，執行以下步驟：

1. 在主控台樹狀目錄中，選擇「**受管裝置**」資料夾。
2. 在「**管理裝置**」資料夾或子資料夾的工作台中，選擇「**裝置**」頁籤。
3. 點擊「**新群組**」按鈕。

   這將開啟可供您建立新群組的視窗。
4. 在「**群組名稱**」視窗中輸入群組名稱，然後點擊「**確定**」。

主控台樹狀目錄中將顯示帶有指定名稱的新管理群組資料夾。如需使用管理群組的詳細資訊，請參閱*卡巴斯基安全管理中心說明*。

為裝置自動分配至管理群組建立規則

您可以集中管理已安裝 Kaspersky Endpoint Security for Android 應用程式的使用者行動裝置設定，但前提是這些裝置必須屬於已事先建立，且已設定群組政策的管理群組。

如果未配置用於自動將在網路上偵測到的行動裝置分配至管理群組的規則，則在裝置第一次與管理伺服器同步時，會將此裝置自動傳送至管理主控台中的「**其他**」→「**網路輪詢**」→「**網域**」→「**KES10**」資料夾中。群組政策不套用至此裝置。

若要建立規則自動將行動裝置分配至管理群組，則遵循以下步驟：

1. 在主控台樹狀目錄中，選擇「**未分配的裝置**」資料夾。
2. 從「**未分配的裝置**」資料夾的上下文功能表中，選擇「**內容**」。

   「**內容：未配置的裝置**」視窗便會出現。
3. 在「**行動裝置**」區域中點擊「**新增**」開始建立自動將裝置分配至管理群組的規則。

   此時將開啟「**新規則**」視窗。

4. 輸入規則名稱。

5. 在行動裝置上安裝了 Kaspersky Endpoint Security for Android 行動 APP 之後，指定應將行動裝置分配到的管理群組。若要執行這項動作，請按一下「**移動裝置的目的地群組**」欄位右側的「**瀏覽**」，並在出現的視窗中選擇群組。

6. 在「**規則套用**」區域中選擇「**為每個裝置執行一次**」。

7. 選中「**僅移動未新增至管理群組的裝置**」核取方塊，防止在套用規則時將選定群組內的行動裝置移動至其他管理群組。

8. 選擇「**啟用規則**」核取方塊，以便規則可以套用至新偵測到的裝置。

9. 開啟「**應用程式**」區域並執行以下操作：

   a. 選擇「**作業系統版本**」核取方塊。

   b. 選擇要分配至指定群組的一個或多個類型的裝置作業系統：Android 或 iOS。

10. 點擊「**確定**」。

新建立的規則會顯示在「**未配置的裝置**」資料夾內容視窗中的「**移動裝置**」區域。

根據規則，卡巴斯基安全管理中心會將所有滿足要求的裝置從「**未分配的裝置**」資料夾中分配至選定群組。也可以手動將先前分配至「**未分配的裝置**」資料夾中的行動裝置分配至「**受管裝置**」資料夾的所需管理群組中。如需管理群組以及未配置裝置的操作詳細資訊，請參閱*卡巴斯基安全管理中心說明*。

建立一般憑證

您必須在管理主控台中建立用於識別行動裝置使用者的一般憑證。

若要建立一般憑證，請執行以下操作：

1. 在主控台樹狀目錄中，選擇「**行動裝置管理**」→「**憑證**」資料夾。

2. 在「**憑證**」資料夾的工作台中，點擊「**新增憑證**」按鈕，啟動「憑證安裝精靈」。

3. 在精靈的「**憑證類型**」視窗中，選擇「**一般憑證**」選項。

4. 在精靈的「**使用者選擇**」視窗中，指定您要為其建立一般憑證的使用者。

5. 在精靈的「**憑證來源**」視窗中，選擇建立一般憑證的方法。

   - 若要自動使用管理伺服器工具建立一般憑證，請選擇「**透過管理伺服器工具頒發憑證**」。

   - 若要向使用者分配先前建立的憑證，請選擇「**指定憑證檔案**」選項。點擊「**指定**」按鈕，開啟「**憑證**」視窗並在其中指定憑證檔案。

     如果您不想指定行動裝置的類型和通知使用者有關憑證建立的方法，請清除「**發佈憑證**」核取方塊。

6. 在精靈的「**使用者通知方法**」視窗中，指定有關使用短訊息或透過電子郵件通知行動裝置使用者有關憑證建立的設定。

7. 在精靈的「**產生憑證**」視窗中，點擊「**已完成**」，完成憑證安裝精靈。

這樣，憑證建立精靈建立使用者可以安裝在行動裝置上的一般憑證。若要獲取憑證，請啟動行動裝置與管理伺服器的同步。如需建立憑證和配置憑證頒發規則的詳細資訊，請參閱 *卡巴斯基安全管理中心說明*。

安裝 Kaspersky Endpoint Security for Android

本節介紹在企業網路上佈署 Kaspersky Endpoint Security for Android 的方法。

權限

對於應用程式的所有功能，Kaspersky Endpoint Security for Android 將提示使用者授予所需權限。在完成安裝精靈時以及在安裝後使用應用程式的各項功能之前，Kaspersky Endpoint Security for Android 將提示授予必需權限。如果未提供必需權限，將無法安裝 Kaspersky Endpoint Security for Android。

在某些裝置（例如 Huawei、Meizu 和 Xiaomi）上，您必須手動將 Kaspersky Endpoint Security for Android 新增到會與作業系統同時啟動的應用程式清單。如果未將該應用程式新增到清單，在行動裝置重新啟動後，Kaspersky Endpoint Security for Android 會停止執行其所有功能。

在執行 Android 11 或更高版本的裝置上，您必須停用「**如果不使用應用程式時刪除權限**」系統設定。否則，在幾個月未使用該應用程式後，系統會自動重設使用者授予該應用程式的權限。

在 Kaspersky Endpoint Security for Android Service Pack 4 Update 4 (版本 10.8.0.103) 中不再支援來電與簡訊篩選功能或 SIM Watch。此種情況下，Kaspersky Endpoint Security for Android 不提示使用者 SMS 管理權限。要啟用來電與簡訊篩選以及 SIM 卡監控的所有功能，您必須使用早期版本的 Kaspersky Endpoint Security for Android。

Kaspersky Endpoint Security for Android 所需的權限

權限	應用程式功能
手機（適用於 Android 5.0 – 9.X）	連線到卡巴斯基安全管理中心（裝置 ID）
儲存空間（必填）	病毒防護
存取以管理所有檔案（適用於 Android 11 或更高版本）	病毒防護
鄰近藍牙裝置（僅適用於 Android 12 或更高版本）	限制使用藍芽
通知（適用於 Android 13）	向使用者通知安全性問題和應用程式事件
允許在背景中執行（適用於 Android 12 或更高版本）	確保持續操作應用程式。若未授予權限，應用程式可能會從記憶體卸載且無法重新啟動。
裝置管理員（必需）	竊盜防護 – 鎖定裝置（僅適用於 Android 5.0 – 6.X）
	竊盜防護 - 使用前置相機拍攝臉部快照
	竊盜防護 – 发出警报声
	竊盜防護 – 還原出廠設定
	密碼防護

	應用程式移除防護
	安裝安全憑證
	應用程式控制
	管理 KNOX（僅適用於 Samsung 裝置）
	配置 Wi-Fi
	配置 Exchange ActiveSync
	限制使用攝影鏡頭、藍芽和 Wi-Fi
攝影鏡頭	竊盜防護 - 使用前置相機拍攝臉部快照 在執行 Android 11.0 或更新版本的裝置上，使用者在收到提示時必須授與「使用應用程式期間」的權限。
定位	竊盜防護 – 定位裝置 在執行 Android 10.0 或更新版本的裝置上，使用者在收到提示時必須授予「任何時間」均可存取裝置位置的權限。
可存取功能	竊盜防護 – 鎖定裝置（僅適用於 Android 7.0 或更高版本）
	Web 防護
	應用程式控制
	應用程式移除防護（僅適用於 Android 7.0 或更高版本）
	顯示 Kaspersky Endpoint Security for Android 的警告（僅適用於 Android 10.0 或更高版本）
	限制使用相機（僅適用於 Android 11 或更高版本）

使用 Google Play 連結安裝 Kaspersky Endpoint Security for Android

對於已新增到卡巴斯基安全管理中心的使用者帳戶，系統會將 Kaspersky Endpoint Security for Android 安裝該帳戶的行動裝置上。如需卡巴斯基安全管理中心的使用者帳戶詳細資訊，請參閱 卡巴斯基安全管理中心說明。

Kaspersky Security for Mobile 允許您使用 Google Play 連結（建議方法）透過卡巴斯基安全管理中心安裝應用程式。

使用者將收到指向 Google Play 的連結。可透過執行 Android 平台的標準安裝程式，安裝該應用程式。安裝後不需要對 Kaspersky Endpoint Security for Android 進行其他配置。

有些 Huawei 和 Honor 裝置沒有 Google 服務，因此沒有 Google Play 應用程式的存取權限。如果部分 Huawei 和 Honor 裝置的使用者無法從 Google Play 安裝應用程式，請指導他們從 Huawei App Gallery 安裝應用程式。

該連結內含以下資料：

- 卡巴斯基安全管理中心同步設定。
- 一般憑證。
- 是否接受 Kaspersky Endpoint Security for Android 最終使用者產品授權協議的條款與條件和其他聲明的指示符。若管理員在管理主控台中接受產品授權協議的條款和其他聲明，Kaspersky Endpoint Security for Android 會在應用程式安裝期間略過接受步驟。

若要使用 Google Play 連結透過卡巴斯基安全管理中心安裝 Kaspersky Endpoint Security for Android：

1. 在主控台樹狀目錄中，選取「**行動裝置管理**」→「**行動裝置**」。
2. 在「**行動裝置**」資料夾的工作台中，點擊「**新增行動裝置**」按鈕。

   這將啟動新建行動裝置連線精靈。按照精靈的描述進行操作。
3. 在精靈的「**作業系統**」視窗中，選擇「**Android**」。

   卡巴斯基安全管理中心會檢查管理外掛程式更新。若卡巴斯基安全管理中心偵測到更新，您可安裝新本的管理外掛程式。當更新管理外掛程式時，您可接受 Kaspersky Endpoint Security for Android 最終使用者產品授權協議 (EULA) 的條款與條件和其他聲明。如果管理員在管理主控台同意產品授權協議和其他聲明，Kaspersky Endpoint Security for Android 會在安裝應用程式期間略過接受步驟。此功能在卡巴斯基安全管理中心 12 版中有提供。
4. 在 **Kaspersky Endpoint Security for Android 安裝方法**頁面上，選取應用程式安裝方法**透過使用 Google Play 連結**。
5. 在精靈的「**選擇使用者**」頁面中，選取要將 Kaspersky Endpoint Security for Android 安裝到其行動裝置的一個或多個使用者。

   如果使用者不在清單中，您可以新增新使用者帳戶，而不必退出新建行動裝置連線精靈。
6. 在精靈的「**憑證來源**」頁面上，選取用於防護 Kaspersky Endpoint Security for Android 和卡巴斯基安全管理中心之間的資料傳輸的憑證來源：
   - **透過管理伺服器工具頒發憑證。**在這種情況下，將自動建立憑證。
   - **指定憑證檔案**。在這種情況下，必須提前準備您自己的憑證，然後在精靈的視窗中選擇它。如果您要將 Kaspersky Endpoint Security for Android 安裝到多個行動裝置，則無法使用此選項。必須為每個使用者建立單獨的憑證。
7. 在精靈的「**使用者通知方法**」頁面上，選擇用於轉發應用程式安裝連結的通道：
   - 若要透過電子郵件傳送連結，請選擇「**傳送指向 Kaspersky Endpoint Security 的連結**」，並在「**透過電子郵件**」區域中配置設定。確保在使用者帳戶的設定中指定了電子郵件信箱。
   - 若要透過簡訊傳送連結，請選擇「**傳送指向 Kaspersky Endpoint Security 的連結**」，並在「**透過簡訊**」區域中配置設定。確保在使用者帳戶的設定中指定了電話號碼。
   - 若要使用 QR 代碼安裝 Kaspersky Endpoint Security for Android，請選擇「**顯示安裝套件連結**」並使用行動裝置的攝影鏡頭掃描 QR 代碼。
   - 如果列出的方法都不適合您，請選擇「**顯示安裝套件連結**」→「**複製**」，將用於安裝 Kaspersky Endpoint Security for Android 的連結複製到剪貼板。使用任何可用的方法傳送應用程式安裝連結。您也可以使用安裝 Kaspersky Endpoint Security for Android 的其他方法。
8. 按一下「**完成**」以關閉新建行動裝置連線精靈。

將 Kaspersky Endpoint Security for Android 安裝到使用者的行動裝置後，您可以使用群組政策來配置裝置和應用程式的設定。如果裝置遺失或被竊，您還可以向行動裝置傳送命令以便防護資料。

安裝 Kaspersky Endpoint Security for Android 的其他方法

您可以使用前往您自己網頁伺服器的連結來安裝 Kaspersky Endpoint Security for Android，或指示使用者手動安裝該應用程式。

從 Google Play 或 Huawei AppGallery 手動安裝

使用者可以從 Google Play 或 Huawei AppGallery 手動安裝 Kaspersky Endpoint Security for Android。可透過執行 Android 平台的標準安裝程式，安裝該應用程式。使用者使用他們自己的 Google 帳戶安裝應用程式。

有關從 Google Play 安裝 Kaspersky Endpoint Security for Android 的詳細資訊，請參閱 Google 技術支援網站。

如需從 Google Play 安裝 Kaspersky Endpoint Security for Android 的詳細資訊，請參閱 HUAWEI 支援網站。

有些 Huawei 和 Honor 裝置沒有 Google 服務，因此沒有 Google Play 應用程式的存取權限。如果部分 Huawei 和 Honor 裝置的使用者無法從 Google Play 安裝應用程式，請指導他們從 Huawei App Gallery 安裝應用程式。

從 Google Play 或 Huawei AppGallery 安裝 Kaspersky Endpoint Security for Android 之後，必須準備應用程式以供使用。為使用做準備的過程包括以下步驟：

1. 管理員使用任何適用方法（例如透過傳送電子郵件），傳送行動裝置與管理伺服器同步的設定（伺服器位址和埠號）。
2. 使用者可在執行初始設定精靈時，或者在 Kaspersky Endpoint Security for Android 設定中，配置行動裝置與管理伺服器同步的設定。
3. 管理員為行動裝置使用者建立一般憑證。
4. 使用者接收自動通知，包含安裝一般憑證的提示。確認安裝後，一般憑證安裝在行動裝置上。

應在行動裝置上啟用網際網路存取，以便與管理伺服器同步。

有關如何配置行動裝置與管理伺服器同步以及如何接收一般憑證的詳細資訊，請參閱卡巴斯基安全管理中心說明。

安裝了 Kaspersky Endpoint Security for Android 的使用者行動裝置會在下一次與管理伺服器同步時，移至安裝應用程式時指定的管理群組（預設群組為 **KES10**）中的**「其他」→「網路輪詢」→「網域」**資料夾。您可以手動或使用自動分配規則，將行動裝置移至在「受管裝置」中建立的管理群組。

如果您想安裝特定版本的 Kaspersky Endpoint Security for Android，此安裝方法非常方便。

若要使用指向您自己的網頁伺服器的連結安裝 Kaspersky Endpoint Security for Android，請執行以下操作：

1. 建立一個安裝套件並進行其設定。

   *安裝套件*是為透過卡巴斯基安全管理中心遠端安裝 Kaspersky 應用程式所建立的一組檔案。

2. 建立獨立安裝套件。

   *獨立安裝套件*是行動應用程式的安裝檔案，其中包含應用程式連線管理伺服器的設定，以及是否接受 Kaspersky Endpoint Security for Android 最終使用者產品授權協議 (EULA) 條款與條件的指示符。它是基於 Kaspersky Endpoint Security for Android 安裝套件建立的。獨立安裝套件是一種特殊形式的安裝套件。

使用者將收到指向託管 Kaspersky Endpoint Security for Android 的獨立安裝套件的網頁伺服器的連結。若要安裝應用程式，使用者必須執行 APK 檔案。安裝後不需要對 Kaspersky Endpoint Security for Android 進行其他配置。

若要使用指向您自己的網頁伺服器的連結安裝 Kaspersky Endpoint Security for Android，必須允許在使用者的行動裝置上安裝來自未知來源的應用程式。

建立和設定安裝套件

Kaspersky Endpoint Security for Android 安裝套件是 `sc_package.exe` 自解壓縮檔案。壓縮檔案包括在裝置上安裝行動 APP 所必需的檔案：

- `adb.exe`、`AdbWinApi.dll`、`AdbWinUsbApi.dll` – 安裝 Kaspersky Endpoint Security for Android 所需的一組檔案。
- `installer.ini` – 包含管理伺服器連線設定的設定檔。
- `KES10_xx_xx_xxx.apk` – Kaspersky Endpoint Security for Android 安裝檔案。
- `kmlisten.exe` – 透過工作站傳送應用程式安裝套件的公用程式。
- `kmlisten.ini` – 包含安裝套件傳送公用程式設定的設定檔。
- `kmlisten.kpd` – 應用程式描述檔案。

建立 Kaspersky Endpoint Security for Android 安裝套件：

1. 在主控台樹狀目錄中，選擇「**其他**」→「**遠端安裝**」→「**安裝套件**」資料夾。
2. 在「**安裝套件**」資料夾的工作台中，按一下「**建立安裝套件**」按鈕。

   安裝套件建立精靈將會啟動。按照精靈的描述進行操作。
3. 在精靈的「**選擇安裝套件類型**」視窗中，點擊「**建立 Kaspersky 程式安裝套件**」按鈕。
4. 在精靈的「**定義安裝套件名稱**」視窗中，輸入將在「**安裝套件**」資料夾的工作台中顯示的安裝套件名稱。
5. 在精靈的**為安裝選擇應用程式安裝套件**視窗中，選擇包括在分發工具套件中的 `sc_package.exe` 自解壓縮檔案。

   如果您已經解壓縮了壓縮檔案，則選擇應用程式說明檔案 `kmlisten.kpd`。在輸入欄位中會顯示應用程式名稱和版本號。
6. 在精靈的**接受 EULA**視窗中，閱讀、理解與接受最終使用者產品授權協議的條款和條件。

   您必須接受最終使用者產品授權協議的條款和條件，才能建立安裝套件。若您在管理主控台中接受產品授權協議的條款，Kaspersky Endpoint Security for Android 會在應用程式安裝期間略過接受步驟。

若您決定停止行動裝置防護，您可解除安裝 Kaspersky Endpoint Security for Android 應用程式，並撤銷該應用程式的最終使用者產品授權協議 (EULA)。如需瞭解更多撤銷 EULA 的相關資訊，請參閱 *卡巴斯基安全管理中心說明*。

精靈完成後，建立的安裝套件將顯示在「**安裝套件**」資料夾工作台中。安裝套件儲存在「套件」資料夾中，在管理伺服器公共共用資料夾內。

配置安裝套件設定：

1. 在主控台樹狀目錄中，選擇「**其他**」→「**遠端安裝**」→「**安裝套件**」資料夾。
2. 在 Kaspersky Endpoint Security for Android 安裝套件的上下文功能表中，選擇「**內容**」。
3. 在「**設定**」標籤中，指定行動裝置的管理伺服器連線設定，以及第一次與管理伺服器同步之後自動接收行動裝置的管理群組。執行以下步驟：
   - 在「**管理伺服器連線**」區域中，在「**伺服器位址**」欄位中輸入管理伺服器安裝期間用於安裝「**行動裝置支援**」的行動裝置管理伺服器名稱。

     根據「**行動裝置支援**」元件的管理伺服器名稱格式的不同，指定管理伺服器的 DNS 名稱或 IP 位址。在「**SSL 埠號**」欄位中，指定管理伺服器連線行動裝置的開放的埠號。預設情況下使用 13292 連接埠。
   - 在「**將電腦分配至群組**」區域中，在「**群組名稱**」欄位中，輸入第一次與管理伺服器同步之後接收行動裝置的群組名稱（預設使用「**KES10**」）。

     指定的群組將在「**其他**」>「**網路輪詢**」>「**網域**」資料夾中自動建立。
   - 在「**安裝期間的操作**」區域中，如果您希望應用程式在首次啟動時要求使用者提供公司電子郵件信箱，請選中「**請求電子郵件信箱**」核取方塊。

     將行動裝置新增至管理群組時，使用者電子郵件信箱用於組成行動裝置的名稱。
4. 要套用指定設定，點擊「**套用**」。

建立獨立安裝套件

若要建立獨立安裝套件，請執行以下步驟：

1. 在主控台樹狀目錄中，選擇「**其他**」→「**遠端安裝**」→「**安裝套件**」資料夾。
2. 選擇 Kaspersky Endpoint Security for Android 安裝套件。
3. 在安裝套件的上下文功能表中，選擇「**建立獨立安裝套件**」。

   系統將啟動建立獨立安裝套件的精靈。按照精靈的描述進行操作。
4. 配置分發獨立安裝套件的方式：
   - 若要透過電子郵件發佈已建立獨立安裝套件的路徑，可在「**後續操作**」區域中點擊連結「**透過電子郵件傳送獨立安裝套件連結**」。

     訊息編輯器視窗將會開啟，視窗中的文字包含帶有獨立安裝套件共用資料夾路徑。
   - 若要在公司網站上發佈已建立獨立安裝套件連結，可點擊連結「**用於在網站上發佈連結的簡易 HTML 代碼**」。

     包含 HTML_RJL 連結的 tmp 檔案將會開啟。

5. 若要在卡巴斯基安全管理中心網頁伺服器上發佈已建立的獨立安裝套件，並檢視獨立安裝套件的完整清單以尋找選定安裝套件，可在「**獨立安裝套件精靈成功完成**」視窗中選擇「**開啟獨立安裝套件清單**」核取方塊。

精靈關閉後，將開啟「**安裝套件 <Installation package name>獨立套件清單**」視窗。

「**安裝套件 <Installation package name> 獨立套件清單**」視窗包含以下資訊：

- 獨立安裝套件清單。
- 在「**路徑**」欄位中顯示的共用資料夾網路路徑。
- 在「**網址**」欄位中顯示的卡巴斯基安全管理中心 Web 服務上的獨立安裝套件位址。

傳送電子郵件通知時，您可以在「**網址**」欄位中指定位址，或在「**路徑**」欄位中指定路徑，以便使用者下載應用程式安裝檔案。將文字訊息通知傳送給使用者時，您可以指定「**網址**」欄位中顯示的下載連結。

建議您將已建立獨立安裝套件的位址複製到剪下板，然後將所需安裝套件的連結貼上到電子郵件或文字訊息通知中。

配置同步設定

要管理行動裝置並從使用者的行動裝置接收報告或統計資訊，必須配置同步設定。行動裝置與卡巴斯基安全管理中心的同步可透過以下方式執行：

- **按排程**。使用 HTTP 協定按排程執行同步。您可以在群組政策設定中配置同步排程。當裝置按照排程與卡巴斯基安全管理中心同步時，才會執行對群組政策設定、命令和工作的修改，即，有一個延遲。預設情況下，行動裝置每隔 6 小時與卡巴斯基安全管理中心自動同步一次。

  在 Android 12 或更高版本上，若裝置處於省電模式，應用程式執行此任務的時間可能會晚於指定時間。

- **強制**。使用 FCM 服務 (Firebase Cloud Messaging) 的推送通知執行強制同步。強制同步主要用於及時傳遞命令到行動裝置。如果您要使用強制同步，請確保在卡巴斯基安全管理中心配置 GSM 設定。如需詳細資訊，請參閱卡巴斯基安全管理中心說明。

配置行動裝置與卡巴斯基安全管理中心的同步設定：

1. 在主控台樹狀目錄的「**受管裝置**」資料夾中，選擇 Android 裝置所屬的管理群組。
2. 在所選群組的工作台中，選擇「**政策**」標籤。
3. 透過按兩下任何資料欄來開啟政策內容視窗。
4. 在政策「**內容**」視窗中選擇「**同步**」區域。
5. 在「**同步**」下拉清單中選擇同步頻率。
6. 要停用裝置在漫遊時與卡巴斯基安全管理中心同步，請選中「**漫遊時不同步**」核取方塊。

   裝置使用者可在應用程式設定中手動執行同步（ → **設定** → **同步** → **同步**）。

7. 要在應用程式設定中隱藏使用者的同步設定（伺服器位址、連接埠和管理群組），請清除「**在裝置上顯示同步設定**」核取方塊。無法修改隱藏的設定。

8. 點擊「**套用**」按鈕以儲存所作的變更。

與卡巴斯基安全管理中心的下次裝置同步之後可配置行動裝置設定。您可以透過使用特殊命令來手動同步行動裝置。要詳細瞭解如何使用行動裝置命令，請參閱*卡巴斯基安全管理中心說明*。

啟動 Kaspersky Endpoint Security for Android 應用程式

卡巴斯基安全管理中心產品授權可應用於不同群組的功能。為了確保 Kaspersky Endpoint Security for Android 完全正常執行，組織購買的卡巴斯基安全管理中心產品授權必須提供**行動裝置管理**功能。**行動裝置管理**功能旨在將行動裝置連線到卡巴斯基安全管理中心並管理它們。

如需卡巴斯基安全管理中心的產品授權和產品授權選項的詳細資訊，請參閱*卡巴斯基安全管理中心說明*。

在行動裝置上啟用 Kaspersky Endpoint Security for Android 應用程式是透過向應用程式提供有效的產品授權資訊來完成的。當裝置與卡巴斯基安全管理中心同步時，產品授權資訊將與政策一起傳遞到行動裝置。

如果在行動裝置上安裝應用程式之後 30 天內未完成 Kaspersky Endpoint Security for Android 應用程式的啟用，應用程式將自動轉換至受限功能模式。在此模式中，大部分應用程式元件都無法執行。當轉換到受限功能模式時，應用程式將停止執行與卡巴斯基安全管理中心的自動同步。因此，如果未在應用程式安裝後 30 天內完成應用程式啟用，使用者必須手動與卡巴斯基安全管理中心同步裝置。

如果您的組織中未佈署卡巴斯基安全管理中心或行動裝置無法存取卡巴斯基安全管理中心，使用者可以在其裝置上手動啟動 Kaspersky Endpoint Security for Android 應用程式。

若要啟動 Kaspersky Endpoint Security for Android 應用程式，請：

1. 在主控台樹狀目錄的「**受管裝置**」資料夾中，選擇 Android 裝置所屬的管理群組。

2. 在所選群組的工作台中，選擇「**政策**」標籤。

3. 透過按兩下任何資料欄來開啟政策內容視窗。

4. 在政策「**內容**」視窗中選擇「**產品授權管理**」區域。

5. 在「**產品授權**」區域，開啟「**金鑰**」下拉清單，從卡巴斯基安全管理中心管理伺服器的金鑰儲存區選擇所需的應用程式啟用金鑰。

   下面的欄位中顯示已購買產品授權的應用程式的詳情。

6. 選擇「**用來自卡巴斯基安全管理中心儲存空間的金鑰進行啟動操作**」核取方塊。

   如果啟動應用程式時未使用卡巴斯基安全管理中心儲存空間中儲存的金鑰，Kaspersky Security for Mobile 會用「**金鑰**」下拉清單中選擇的活動金鑰更換該金鑰。

7. 若要在使用者的行動裝置上啟動應用程式，請封鎖變更設定。

8. 點擊「**套用**」按鈕以儲存所作的變更。

   與卡巴斯基安全管理中心的下個裝置同步之後可配置行動裝置設定。

安裝 iOS MDM 設定檔

本節介紹在企業網路上佈署 iOS MDM 設定檔的方法。

在佈署 iOS MDM 設定檔之前，管理員必須執行以下操作：

1. 安裝 iOS MDM 伺服器。
2. 獲取 Apple 推送通知服務憑證（以下簡稱 APN 憑證）。
3. 將 APN 憑證安裝到 iOS MDM 伺服器。

如需安裝 iOS MDM 伺服器和使用 APN憑證的詳細資訊，請參閱*卡巴斯基安全管理中心幫助*。

如需在 Kaspersky Endpoint Security Cloud 中佈署 iOS MDM 設定檔的詳細資訊，請參閱 *Kaspersky Endpoint Security Cloud 說明*。

關於 iOS 裝置管理模式

您可以採用多種不同方式佈署 iOS 裝置管理系統。管理模式取決於行動裝置的所有者（個人或公司）和企業安全需求。您可以選擇最適合您公司的管理模式，並同時使用多種模式。

不受監控的裝置

「*不受監控的 iOS 裝置*」是指連線到卡巴斯基安全管理中心的員工個人裝置。在此模式下，允許使用者使用個人 Apple ID，使用任何應用程式，並在裝置上儲存個人資料。您可以使用 Kaspersky Device Management for iOS 群組政策配置對公司資源的存取權限、安全設定和其他設定。預設情況下，所有 iOS 裝置均處於不受監控狀態。

監控裝置

「*監控 iOS 裝置*」是指連線到卡巴斯基安全管理中心的公司裝置。在 Apple Configurator 中執行行動裝置的初始配置。「*Apple Configurator*」是一個專門用於準備和配置 iOS 裝置的應用程式。Apple Configurator 會安裝在執行 OS X 的電腦上。如需使用 Apple Configurator 的詳細資訊，請參閱 Apple 技術支援網站。您可以使用 Kaspersky Device Management for iOS 群組政策執行進一步配置。在監控裝置上，您可以存取延伸的設定選項。例如，您可以配置全域 HTTP 代理和附加限制（例如，封鎖使用 iMessage 和遊戲中心），還可以封鎖修改使用者帳戶。

要使用受監控和不受監控的 iOS 裝置，iOS MDM 伺服器必須安裝有 APN 憑證，並在使用者的行動裝置上安裝 iOS MDM 設定檔。

透過卡巴斯基安全管理中心安裝

iOS MDM 設定檔安裝到其使用者帳戶已新增到卡巴斯基安全管理中心的使用者的行動裝置上。如需卡巴斯基安全管理中心的使用者帳戶詳細資訊，請參閱 *卡巴斯基安全管理中心說明*。

若要安裝 iOS MDM 設定檔，請執行以下動作：

1. 在主控台樹狀目錄中，選取「**行動裝置管理**」→「**行動裝置**」。
2. 在「**行動裝置**」資料夾的工作台中，點擊「**新增行動裝置**」按鈕。

   這將啟動新建行動裝置連線精靈。按照精靈的描述進行操作。
3. 在精靈的「**作業系統**」視窗中，選擇「**iOS**」。
4. 在精靈的「**iOS MDM 裝置防護方法**」視窗中，選擇「**使用 iOS MDM 伺服器的 iOS MDM 設定檔**」並指定清單中的 iOS MDM 設定檔。
5. 在精靈的「**選擇使用者**」視窗中，選擇要將 iOS MDM 設定檔安裝到其行動裝置的一個或多個使用者。

   如果使用者不在清單中，您可以新增新使用者帳戶，而不必退出新建行動裝置連線精靈。
6. 在精靈的「**憑證來源**」視窗中，選擇用於防護行動裝置和卡巴斯基安全管理中心之間的資料傳輸的憑證來源：
   - **透過管理伺服器工具頒發憑證**。在這種情況下，將自動建立憑證。
   - **指定憑證檔案**。在這種情況下，必須提前準備您自己的憑證，然後在精靈的視窗中選擇它。如果您要將 iOS MDM 設定檔安裝到多個行動裝置，則無法使用此選項。必須為每個使用者建立單獨的憑證。
7. 在精靈的「**使用者通知方法**」視窗中，選擇用於轉發應用程式安裝連結的通道：
   - 若要透過電子郵件傳送連結，請選擇「**傳送指向 iOS MDM 設定檔的連結**」，並在「**透過電子郵件**」區域中配置設定。確保在使用者帳戶的設定中指定了電子郵件信箱。
   - 若要透過簡訊傳送連結，請選擇「**傳送指向 iOS MDM 設定檔的連結**」，並在「**透過簡訊**」區域中配置設定。確保在使用者帳戶的設定中指定了電話號碼。
   - 若要使用 QR 代碼安裝 iOS MDM 設定檔，請選擇「**顯示安裝套件連結**」並使用行動裝置的攝影鏡頭掃描 QR 代碼。
   - 如果列出的方法都不適合您，請選擇「**顯示安裝套件連結**」→「**複製**」，將 iOS MDM 設定檔安裝連結複製到剪貼板。使用任何可用的方法傳送應用程式安裝連結。
8. 完成新建行動裝置連線精靈。

將 iOS MDM 設定檔安裝到使用者的行動裝置後，您可以使用群組政策來配置應用程式設定。如果裝置遺失或被竊，您還可以向行動裝置傳送命令以便防護資料。

在執行 iOS 12.1 或更新版本的行動裝置上，您必須手動確認 iOS MDM 設定檔在行動裝置上的安裝。您必須授予遠端管理裝置的權限。

安裝管理外掛程式

若要管理行動裝置，必須在管理員的工作站上安裝以下管理外掛程式：

- Kaspersky Endpoint Security for Android 的管理外掛程式提供介面，用於透過卡巴斯基安全管理中心管理主控台，管理行動裝置以及安裝在這些裝置上的行動 APP。
- Kaspersky Device Management for iOS 的管理外掛程式提供了介面，用途是透過卡巴斯基安全管理中心管理主控台，來管理透過 iOS MDM 和 Exchange ActiveSync 協定連線的行動裝置。

您可使用以下方法安裝管理外掛程式：

- 使用卡巴斯基安全管理中心快速啟動精靈安裝管理外掛程式。

  應用程式會在初次連線時，自動提示您在安裝管理伺服器後執行快速啟動精靈。您也可以隨時手動啟動快速啟動精靈。

  > 透過快速啟動精靈，您可在管理主控台中的接受 Kaspersky Endpoint Security for the Android 應用程式最終使用者產品授權協議 (EULA) 的條款與條件。若管理員在管理主控台接受產品授權協議，Kaspersky Endpoint Security for Android 會在安裝應用程式期間略過接受步驟。如須卡巴斯基安全管理中心快速啟動精靈的詳細資訊，請參閱*卡巴斯基安全管理中心說明*。

- 使用在卡巴斯基安全管理中心管理主控台中的可用分發套件清單安裝管理外掛程式。

  推出新版 Kaspersky 應用程式後，可用分發套件清單會自動更新。

- 使用 EXE 檔案從外部來源下載分發套件並安裝管理外掛程式。

  例如，您可在 Kaspersky 網站上下載管理外掛程式的分發套件。

從管理主控台的清單安裝管理外掛程式

若要安裝管理外掛程式：

1. 在主控台樹狀目錄中，選取「**進階**」→「**遠端安裝**」→「**安裝套件**」。
2. 在工作台中選取「**其他動作**」→「**檢視 Kaspersky 應用程式的最新版本**」。

   這會開啟 Kaspersky 應用程式的最新版本清單。
3. 在**行動裝置**區段中，選取 **Kaspersky Endpoint Security for Android** 或 **Kaspersky Device Management for iOS** 外掛程式。
4. 按一下「**下載分發套件**」按鈕。

   外掛程式分發套件會下載至電腦的記憶體中 (EXE 檔案)。
5. 執行 EXE 檔案並遵循安裝精靈的指示。

從分發套件下載管理外掛程式

若要安裝 Kaspersky Endpoint Security for Android 管理外掛程式，

請從整合解決方案安裝套件中複製外掛程式安裝檔案 `klcfinst.exe`，然後在管理員工作站上執行它。

安裝進程由精靈完成，您無需配置設定。

要安裝 Kaspersky Device Management for iOS 管理外掛程式，請執行以下操作：

請從整合解決方案安裝套件中複製外掛程式安裝檔案 `klmdminst.exe`，然後在管理員工作站上執行它。

安裝進程由精靈完成，您無需配置設定。

您可透過在「**進階**」→「**已安裝應用程式管理外掛程式的詳細資訊**」區域中，檢視管理伺服器內容視窗中的已安裝應用程式管理外掛程式清單，確認管理外掛程式已安裝。

更新先前版本的應用程式

應用程式升級必須滿足以下要求：

- Kaspersky Endpoint Security 管理外掛程式的版本和 Kaspersky Endpoint Security for Android 移動應用程式的版本必須比對。

  您可以在 Kaspersky Security for Mobile 的發行說明中檢視管理外掛程式和移動應用程式版本的版本號。

- 確保卡巴斯基安全管理中心滿足 Kaspersky Security for Mobile 的軟體要求。

- 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) 及更高版本的管理外掛程式可以自動升級到目前版本。不支援升級早期版本的管理外掛程式。

  若要升級早期版本的管理外掛程式，您必須刪除已安裝的管理外掛程式和使用它們建立的群組政策。然後安裝管理外掛程式的新版本。如需刪除管理外掛程式的詳細資訊，請造訪 *Kaspersky 技術支援網站*。

- 在組織的所有行動裝置上使用相同版本的 Kaspersky Endpoint Security for Android。

可在*Kaspersky 技術支援網站*上檢視 Kaspersky Security for Mobile 版本的技術支援條款和條件。

若要檢視管理外掛程式的版本和內部版本號，請執行以下操作：

1. 在主控台樹狀目錄中的管理伺服器的上下文功能表中，選擇「**內容**」。
2. 在管理伺服器內容視窗中，選擇**進階→已安裝應用程式管理外掛程式的詳細資訊**。

   工作台將以 `<Plug-in name> <Version> <Build>` 格式顯示已安裝的管理外掛程式的資訊。

您可以使用以下方法檢視 Kaspersky Endpoint Security for Android 應用程式的版本和內部版本號：

- 如果 Kaspersky Endpoint Security for Android 是使用獨立安裝套件安裝的，您可以在套件內容中檢視應用程式的版本和內部版本號。
- 若您透過 Google Play 安裝 Kaspersky Endpoint Security for Android，便可以在應用程式設定中檢視版本號碼（ →**關於應用程式**）。

升級先前版本的 Kaspersky Endpoint Security for Android

Kaspersky Endpoint Security for Android 可透過下列方式更新：

- 使用 Google Play。行動裝置使用者可以從 Google Play 中下載應用程式的新版本，然後在裝置中進行安裝。
- 使用卡巴斯基安全管理中心。您可以使用卡巴斯基安全管理中心遠端管理系統遠端更新裝置上的應用程式版本。

您可以選擇最適合您組織的應用程式更新方法。您可以僅使用一種更新方法。

從 Google Play 更新應用程式

透過執行 Android 平台的標準更新步驟，您可以從 Google Play 更新本應用程式。要更新應用程式，必須滿足下列條件：

- 行動裝置使用者必須擁有 Google 帳戶。
- 裝置必須已連線至您的 Google 帳戶。
- 裝置必須已連線網際網路。

從 Google Play 下載應用程式後，Kaspersky Endpoint Security for Android 會檢查最終使用者產品授權協議 (EULA) 的條款與條件。如果 EULA 條款更新，該應用程式會傳送要求至卡巴斯基安全管理中心。如果管理員在管理主控台接受 EULA，Kaspersky Endpoint Security for Android 會在安裝應用程式期間略過接受步驟。若管理員使用過時的管理員外掛程式版本，卡巴斯基安全管理中心會提示您更新管理外掛程式。更新管理外掛程式時，管理員可在 Kaspersky Endpoint Security for Android 的管理主控台中接受 EULA 的條款。

如果 Kaspersky Endpoint Security for Android 是從 Google Play 安裝的，則可以透過 Google Play 更新應用程式。如果該應用程式是使用其他方法安裝的，則不能透過 Google Play 更新應用程式。

透過卡巴斯基安全管理中心更新應用程式

套用群組政策之後，可以使用卡巴斯基安全管理中心升級 Kaspersky Endpoint Security for Android。在群組政策設定中，可以選擇符合企業安全性政策的版本的 Kaspersky Endpoint Security for Android 獨立安裝套件。

如果您透過卡巴斯基安全管理中心安裝了 Kaspersky Endpoint Security for Android，則可以透過卡巴斯基安全管理中心進行更新。如果該應用程式是從 Google Play 安裝的，則不能透過卡巴斯基安全管理中心更新應用程式。

若要使用獨立安裝套件升級 Kaspersky Endpoint Security for Android，必須允許在使用者的行動裝置上安裝來自未知來源的應用程式。如需不使用 Google Play 安裝應用程式的詳細資訊，請參考 *Android 說明指南*。

若要更新應用程式版本，請執行以下操作：

1. 在主控台樹狀目錄的「**受管裝置**」資料夾中，選擇 Android 裝置所屬的管理群組。
2. 在所選群組的工作台中，選擇「**政策**」標籤。
3. 透過按兩下任何資料欄來開啟政策內容視窗。
4. 在政策「**內容**」視窗中選擇「**其他**」區域。
5. 在「**正在升級 Kaspersky Endpoint Security for Android**」區域中，點擊「**選擇**」按鈕。
   「**正在升級 Kaspersky Endpoint Security for Android**」視窗隨即開啟。
6. 在 Kaspersky Endpoint Security 獨立安裝套件清單中，選擇其版本滿足企業安全需求的安裝套件。

   您只能將 Kaspersky Endpoint Security 升級至最近的應用程式版本。Kaspersky Endpoint Security 無法升級至較老版本。

7. 按一下「**選擇**」按鈕。

「**正在升級 Kaspersky Endpoint Security for Android**」區域中將顯示所選獨立安裝套件的描述。

8. 點擊「**套用**」按鈕以儲存所作的變更。

與卡巴斯基安全管理中心的下次裝置同步之後可配置行動裝置設定。行動裝置使用者將獲得啟示安裝新版本應用程式。使用者同意後，新版應用程式將安裝在行動裝置上。

安裝先前版本的 Kaspersky Endpoint Security for Android

如果您要防止應用自動更新和使用特別版本的 Kaspersky Endpoint Security for Android，在 Google Play 設定中停用應用的自動更新。如需詳細資訊，請參閱 Google 技術支援網站。

Kaspersky Endpoint Security for Android 的自動更新僅在應用從 Google Play 或透過卡巴斯基安全管理中心使用 Google Play 連結安裝時可用。如果應用程式透過卡巴斯基安全管理中心使用您自己網頁伺服器的連結（使用獨立安裝套件），自動更新不可用。此種情況下，您可以使用群組政策手動更新 Kaspersky Endpoint Security for Android。

要安裝先前版本的 Kaspersky Endpoint Security for Android：

1. 從使用者行動裝置中刪除 Kaspersky Endpoint Security for Android。
2. 使用指向您自己的網頁伺服器的連結透過卡巴斯基安全管理中心安裝 Kaspersky Endpoint Security for Android。為此，您將需要被別版本的安裝套件。您可以在 Kaspersky 技術支援網站下載早期版本 Kaspersky Endpoint Security for Android 的分發套件。

對於早期版本 Kaspersky Endpoint Security for Android 的詳情，請參考 *Kaspersky Security for Mobile 適當版本的說明*。

升級先前版本的管理外掛程式

您可使用以下方法升級管理外掛程式：

- 使用卡巴斯基安全管理中心管理主控台中可用分發套件的清單來安裝新版管理外掛程式。

  推出新版 Kaspersky 應用程式後，可用分發套件清單會自動更新。

- 從外部來源下載分發套件，並使用 EXE 檔案安裝管理外掛程式。

  若要升級 Kaspersky Endpoint Security for Android 和 Kaspersky Device Management for iOS 管理外掛程式，您需要從 Kaspersky Security for Mobile 網頁下載最新版本的應用程式，然後為兩個外掛程式分別執行安裝精靈。在安裝精靈執行過程中，先前版本的外掛程式會自動移除。

Kaspersky 專家建議使用相同版本的應用程式的管理外掛程式。如果使用者從 Google Play 升級應用程式，卡巴斯基安全管理中心會顯示通知，提示您升級管理外掛程式。

管理外掛程式更新之後，「**受管裝置**」資料夾中的現有管理群組，以及「**未分配的裝置**」資料夾中的裝置自動分配到這些群組的規則，都會儲存起來。現有的行動裝置群組政策也將保留。實施 Kaspersky Security for Mobile 整合解決方案的新功能的新政策設定將新增到現有政策中，並且擁有預設值。

如果在管理外掛程式新版本中新增了新設定或者預設值被變更，變更僅在開啟群組政策後被套用。先前版本外掛程式的設定在管理員開啟群組政策之前都被套用到行動裝置，即使外掛程式版本被更新。

從管理主控台中的清單升級

若要升級管理外掛程式：

1. 在主控台樹狀目錄中，選取「**進階**」→「**遠端安裝**」→「**安裝套件**」。
2. 在工作台中選取「**其他動作**」→「**檢視 Kaspersky 應用程式的最新版本**」。
   這會開啟 Kaspersky 應用程式的最新版本清單。
3. 在**行動裝置**區段中，選取 **Kaspersky Endpoint Security for Android** 或 **Kaspersky Device Management for iOS** 外掛程式。
4. 按一下「**下載分發套件**」按鈕。
   外掛程式分發套件將會下載至電腦的記憶體 (EXE 檔案)。執行 EXE 檔案。按照安裝精靈的指示進行操作。

從分發套件升級

若要升級 Kaspersky Endpoint Security for Android 管理外掛程式，

請從整合解決方案安裝套件中複製外掛程式安裝檔案 `klcfinst.exe`，然後在管理員工作站上執行它。

精靈會完成安裝程序，您無需配置設定。

若要安裝 Kaspersky Device Management for iOS 管理外掛程式：

請從整合解決方案安裝套件中複製外掛程式安裝檔案 `klmdminst.exe`，然後在管理員工作站上執行它。

精靈會執行外掛程式安裝，您無需配置設定。

您可在「**進階**」→「**已安裝應用程式管理外掛程式的詳細資訊**」區段，檢視管理伺服器內容視窗中的已安裝應用程式管理外掛程式清單，確認管理外掛程式已升級。

移除 Kaspersky Endpoint Security for Android

Kaspersky Endpoint Security for Android 可透過下列方式移除：

1. 由使用者移除應用程式
   使用者使用應用程式介面，手動移除 Kaspersky Endpoint Security for Android。要讓使用者能夠移除應用程式，應該在套用於裝置的政策中允許應用程式移除。
2. 由管理員移除應用程式
   管理員使用卡巴斯基安全管理中心的管理主控台，遠端移除應用程式。應用程式既可從單獨裝置移除，也可從多部裝置同時移除。

遠端移除應用程式

您可透過以下方式，遠端從使用者的行動裝置上移除 Kaspersky Endpoint Security for Android：

- 使用群組政策。如果您要將應用程式同時從多部裝置上移除，這種方法是非常方便的。
- 透過配置本機應用程式設定。如果您要將應用程式從單獨裝置上移除，這種方法是非常方便的。

應用群組政策移除應用程式：

1. 在主控台樹狀目錄的「**受管裝置**」資料夾中，選擇 Android 裝置所屬的管理群組。
2. 在所選群組的工作台中，選擇「**政策**」標籤。
3. 透過按兩下任何資料欄來開啟政策內容視窗。
4. 在政策「**內容**」視窗中選擇「**其他**」區域。
5. 在「**移除 Kaspersky Endpoint Security for Android 應用程式**」區域中，選擇「**從裝置上移除 Kaspersky Endpoint Security for Android**」核取方塊。
6. 點擊「**套用**」按鈕以儲存所作的變更。

在與管理伺服器同步之後，Kaspersky Endpoint Security for Android 將從行動裝置上移除。行動裝置使用者收到關於應用程式已移除的通知。

透過配置本機設定移除應用程式：

1. 在主控台樹狀目錄中，選擇「**行動裝置管理**」→「**行動裝置**」。
2. 在裝置清單中，選擇您要在其上移除應用程式的裝置。
3. 透過點擊開啟裝置內容視窗。
4. 選取**應用程式 → Kaspersky Endpoint Security for Android**。
5. 透過點擊開啟 Kaspersky Endpoint Security 內容視窗。
6. 選擇「**其他**」區域。
7. 在「**移除 Kaspersky Endpoint Security for Android**」區域中，選擇「**從裝置上移除 Kaspersky Endpoint Security for Android**」核取方塊。
8. 點擊「**套用**」按鈕以儲存所作的變更。

因此，Kaspersky Endpoint Security for Android 在與管理伺服器同步之後，便會從行動裝置中移除。行動裝置使用者會收到有關應用程式已移除的通知。

允許使用者移除應用程式

要防護在執行 Android 7.0 或更高版本的裝置上的應用程式不會被移除，必須將 Kaspersky Endpoint Security for Android 設定為可存取功能。當初始配置精靈正在執行時，Kaspersky Endpoint Security for Android 會提示使用者授予應用程式所有必需的權限。使用者可以略過這些步驟或以後在裝置設定中停用這些權限。在這種情況下，不防護該應用程式不被移除。

您可以透過以下方式，允許使用者將 Kaspersky Endpoint Security for Android 從他們的行動裝置上移除：

- 使用群組政策。如果您希望允許使用者同時將應用程式從多部裝置上移除，這種方法是非常方便的。
- 使用本機應用程式設定。如果您希望允許單獨裝置的使用者移除應用程式，這種方法是非常方便的。

在群組政策中允許移除應用程式：

1. 在主控台樹狀目錄的「**受管裝置**」資料夾中，選擇 Android 裝置所屬的管理群組。
2. 在所選群組的工作台中，選擇「**政策**」標籤。
3. 透過按兩下任何資料欄來開啟政策內容視窗。
4. 在政策「**內容**」視窗中選擇「**其他**」區域。
5. 在「**移除 Kaspersky Endpoint Security for Android**」區域中，選中「**允許移除 Kaspersky Endpoint Security for Android**」核取方塊。
6. 點擊「**套用**」按鈕以儲存所作的變更。

在與管理伺服器同步之後，將允許使用者從行動裝置上移除該應用程式。移除應用程式按鈕在 Kaspersky Endpoint Security for Android 設定中變成可用狀態。

允許在本機應用程式設定中移除應用程式：

1. 在主控台樹狀目錄中，選擇「**其他**」→「**行動裝置管理**」→「**行動裝置**」。
2. 在裝置清單中，選擇您要允許使用者從其移除應用程式的裝置。
3. 透過點擊開啟裝置內容視窗。
4. 選取**應用程式→ Kaspersky Endpoint Security for Mobile**。
5. 透過點擊開啟 Kaspersky Endpoint Security 內容視窗。
6. 選擇「**其他**」區域。
7. 在「**移除 Kaspersky Endpoint Security for Android**」區域中，選中「**允許移除 Kaspersky Endpoint Security for Android**」核取方塊。
8. 點擊「**套用**」按鈕以儲存所作的變更。

與管理伺服器同步之後，將允許使用者從行動裝置上移除應用程式。移除應用程式按鈕在 Kaspersky Endpoint Security for Android 設定中變成可用狀態。

由使用者移除應用程式

若要從行動裝置上獨立地移除 Kaspersky Endpoint Security for Android，使用者必須執行以下操作：

1. 在 Kaspersky Endpoint Security for Android 的主視窗中，輕觸→「**移除應用程式**」。

螢幕中將出現確認提示資訊。

如果未顯示「**移除應用程式**」按鈕，則意味著管理員已啟用 Kaspersky Endpoint Security for Android 移除防護。

2. 確認移除 Kaspersky Endpoint Security for Android。

Kaspersky Endpoint Security for Android 應用程式將從使用者的行動裝置中移除。

組態和管理

本說明部分面向管理 Kaspersky Security for Mobile 的專家，以及向使用 Kaspersky Security for Mobile 的組織提供技術支援的專家。

開始使用

本節介紹在開始使用 Kaspersky Security for Mobile 時建議您執行的操作。

啟動和停止應用程式

卡巴斯基安全管理中心將自動啟用和停止 Kaspersky Endpoint Security 和 Kaspersky Device Management for iOS 的管理外掛程式。

作業系統啟動時 Kaspersky Endpoint Security for Android 也會啟動並在整個連線中防護行動裝置。使用者可以透過停用所有 Kaspersky Endpoint Security for Android 元件來停止應用程式。您可以使用群組政策配置使用者管理應用程式元件的權限。

在某些裝置（例如，華為、魅族和小米）上，您必須手動將 Kaspersky Endpoint Security for Android 新增到在作業系統啟動時啟動的應用程式清單（「**安全**」→「**權限**」→「**自動執行**」）。如果未將該應用程式新增到清單，在行動裝置重新啟動後，Kaspersky Endpoint Security for Android 會停止執行其所有功能。

您還必須為 Kaspersky Endpoint Security for Android 停用低電量模式。這對於要在後台執行的應用程式（例如，執行排程的病毒掃描或將裝置與卡巴斯基安全管理中心同步）來說是必需的。此問題歸因於這些裝置內嵌的軟體的特定功能。

建立管理群組

若要集中設定使用者行動裝置所安裝的 Kaspersky Endpoint Security for Android 應用程式，您必須先將群組政策套用到這些裝置。

若要將政策套用於裝置群組，建議您在使用者裝置上安裝行動 APP 之前，先在「**受管裝置**」中為這些裝置建立單獨的群組。

建立管理群組後，建議配置選項以將要安裝應用程式的裝置自動分配到此群組。然後使用群組政策配置所有裝置通用的設定。

若要建立管理群組，執行以下步驟：

1. 在主控台樹狀目錄中，選擇「**受管裝置**」資料夾。

2. 在「**管理裝置**」資料夾或子資料夾的工作台中，選擇「**裝置**」頁籤。

3. 點擊「**新群組**」按鈕。

   這將開啟可供您建立新群組的視窗。

4. 在「**群組名稱**」視窗中輸入群組名稱，然後點擊「**確定**」。

主控台樹狀目錄中將顯示帶有指定名稱的新管理群組資料夾。如需使用管理群組的詳細資訊，請參閱*卡巴斯基安全管理中心說明*。

用於管理行動裝置的群組政策

*群組政策*是用於管理屬於管理群組的行動裝置和管理裝置上安裝的行動 APP 的設定套件。您可以使用政策精靈建立群組政策。

您可以使用政策設定單個裝置和裝置群組的設定。對於一組裝置，可在群組政策內容視窗中設定管理設定。對於個別裝置，您可在本機應用程式設定視窗中設定。為一個裝置指定的單個管理設定可能會與為該裝置所屬組的政策中設定的設定值有所不同。

政策中的每個參數都有「鎖定」內容，這會顯示是否允許在本機應用程式設定中，修改層級結構的政策（對嵌套群組和次要管理伺服器而言）。

在本機應用程式中和政策中設定的設定值，將儲存在管理伺服器上，在同步期間分發至行動裝置，並將其作為目前設定儲存在裝置中。如果使用者指定了未被「鎖定」的其他設定值，在裝置與管理伺服器下次同步期間，設定新值將被傳遞給管理伺服器，並儲存在應用程式本機設定中，而不是先前由管理員指定的值。

為了使行動裝置的企業安全防護保持最新，您可以監控使用者的裝置是否符合群組管理政策。

安全等級指示器在群組政策視窗的上部顯示。安全等級指示器將顯示幫助您設定政策以確保高等級裝置防護。防護等級指示器狀態根據政策設定而變更：

- **高防護等級** – 提供適當等級的裝置防護。全部防護元件根據 Kaspersky 的設定來執行。
- **中防護等級** – 防護等級低於推薦等級。一些關鍵防護元件被顯示(例如，Web 防護)。重要問題使用圖示來標記。
- **低防護等級** – 表示存在可能導致裝置感染和資料遺失的問題。一些關鍵防護元件被顯示(例如，裝置即時防護被停用)。關鍵問題使用圖示來標記。

如需管理政策和卡巴斯基安全管理中心管理主控台中管理群組的詳細資訊，請參閱*卡巴斯基安全管理中心說明*。

建立群組政策

本節說明為已安裝 Kaspersky Endpoint Security for Android 行動應用程式的裝置建立群組政策，以及為 EAS 裝置和 iOS MDM 裝置建立政策的程序。

為管理員組建立的政策顯示在卡巴斯基安全管理中心管理主控台群組工作區的「**政策**」標籤中。指示政策狀態（活動/不活動）的圖示顯示在政策名稱前。可以在一個群組中建立多個用於不同應用程式的政策。對於每個應用程式，僅一個政策處於活動狀態。當建立新的活動政策時，先前的活動政策將變為不活動狀態。

您可以在政策建立後修改政策。

若要建立用於管理行動裝置的群組政策：

1. 從主控台樹狀目錄中，選擇您要為其建立政策的管理群組。
2. 在所選群組的工作台中，選擇「**政策**」標籤。
3. 點擊「**建立政策**」連結以執行政策精靈。

這會啟動政策精靈。

步驟 1.選擇要建立群組政策的應用程式

此步驟中，在應用程式清單中選擇在您要為其建立群組政策的應用程式：

- **Kaspersky Endpoint Security for Android** – 適用於使用 Kaspersky Endpoint Security for Android 行動應用程式的裝置。

建議為沒有 Google play 服務的 Huawei 和 Honor 裝置單獨制定政策。這樣您就可以將 Huawei AppGallery 的連結發送給所有這類裝置的使用者。

- **Kaspersky Device Management for iOS** – 對於 EAS 裝置和 iOS MDM 裝置。

如果管理員桌面上安裝了 Kaspersky Endpoint Security for Android 管理外掛程式和 Kaspersky Device Management for iOS 管理外掛程式，則可以為行動裝置建立政策。如果未安裝這些外掛程式，相關應用程式的名稱不會顯示在應用程式清單中。

繼續政策精靈的下一步。

步驟 2.輸入群組政策名稱

在此步驟中，在「**名稱**」欄位中輸入新政策的名稱。如果您指定了現有政策的名稱，它將在最後自動新增 (1)。

繼續政策精靈的下一步。

步驟 3.為應用程式建立群組政策

在這一步中，精靈將提示您選擇政策狀態：

- **活動政策**。精靈將在管理伺服器上儲存已建立的政策。在行動裝置下次與管理伺服器同步時，該政策將在裝置上用作活動政策。
- **停用政策**。精靈將在管理伺服器上以備份政策的方式儲存已建立的政策。在後續某個特殊事件之後該政策將被啟動。若有需要可將未啟動的政策轉換為啟動狀態。

可以為群組中一個應用程式建立若干個政策，但是只能啟動它們其中的一個政策。當建立新的啟動政策時，先前的啟動政策將自動變為停用狀態。

退出精靈。

配置同步設定

要管理行動裝置並從使用者的行動裝置接收報告或統計資訊，必須配置同步設定。行動裝置與卡巴斯基安全管理中心的同步可透過以下方式執行：

- **按排程**。使用 HTTP 協定按排程執行同步。您可以在群組政策設定中配置同步排程。當裝置按照排程與卡巴斯基安全管理中心同步時，才會執行對群組政策設定、命令和工作的修改，即，有一個延遲。預設情況下，行動裝置每隔 6 小時與卡巴斯基安全管理中心自動同步一次。

  在 Android 12 或更高版本上，若裝置處於省電模式，應用程式執行此任務的時間可能會晚於指定時間。

- **強制**。使用 FCM 服務 (Firebase Cloud Messaging) 的推送通知執行強制同步。強制同步主要用於及時傳遞命令到行動裝置。如果您要使用強制同步，請確保在卡巴斯基安全管理中心配置 GSM 設定。如需詳細資訊，請參閱卡巴斯基安全管理中心說明。

配置行動裝置與卡巴斯基安全管理中心的同步設定：

1. 在主控台樹狀目錄的「**受管裝置**」資料夾中，選擇 Android 裝置所屬的管理群組。
2. 在所選群組的工作台中，選擇「**政策**」標籤。
3. 透過按兩下任何資料欄來開啟政策內容視窗。
4. 在政策「**內容**」視窗中選擇「**同步**」區域。
5. 在「**同步**」下拉清單中選擇同步頻率。
6. 要停用裝置在漫遊時與卡巴斯基安全管理中心同步，請選中「**漫遊時不同步**」核取方塊。

   裝置使用者可在應用程式設定中手動執行同步（ → **設定** → **同步** → **同步**）。
7. 要在應用程式設定中隱藏使用者的同步設定（伺服器位址、連接埠和管理群組），請清除「**在裝置上顯示同步設定**」核取方塊。無法修改隱藏的設定。
8. 點擊「**套用**」按鈕以儲存所作的變更。

與卡巴斯基安全管理中心的下次裝置同步之後可配置行動裝置設定。您可以透過使用特殊命令來手動同步行動裝置。要詳細瞭解如何使用行動裝置命令，請參閱*卡巴斯基安全管理中心說明*。

管理對群組政策的修訂

卡巴斯基安全管理中心允許您跟蹤群組政策修改。每次儲存對群組政策進行的變更時，都會建立一個*修訂*。每個修訂都有一個編號。

您只能管理 Kaspersky Endpoint Security for Android 政策的修訂。您不能管理 Kaspersky Device Management for iOS 政策的修訂。

您可以對群組政策執行以下操作：

- 將所選修訂與目前修訂進行比較。

- 比較所選修訂。
- 將政策與另一個政策的所選修訂進行比較。
- 檢視所選修訂。
- 將政策變更回溯至所選修訂。
- 將修訂另存新檔 .txt 檔案。

如需管理群組政策和其他物件（例如使用者帳戶）修訂版本的詳細資訊，請參閱*卡巴斯基安全管理中心說明*。

檢視群組政策修訂的歷史記錄：

1. 在主控台樹狀目錄的「**受管裝置**」資料夾中，選擇 Android 裝置所屬的管理群組。
2. 在所選群組的工作台中，選擇「**政策**」標籤。
3. 透過按兩下任何資料欄來開啟政策內容視窗。
4. 在政策「**內容**」視窗中選擇「**修訂歷史記錄**」區域。
   將顯示政策修訂清單。它包含以下資訊：
   - 政策修訂編號。
   - 修改政策的日期和時間。
   - 修改政策的使用者名稱。
   - 對政策執行的操作。
   - 對政策設定進行的修訂的說明。

刪除群組政策

若要刪除群組政策，請執行以下操作：

1. 在主控台樹狀目錄中，選擇您要為其建立政策的管理群組。
2. 在管理群組的工作台中，在「**政策**」標籤上選擇要刪除的政策。
3. 在政策的上下文功能表中，選擇「**刪除**」。

這樣，群組政策已刪除。在套用新的群組政策之前，屬於管理群組的行動裝置繼續使用在已刪除的政策中指定的設定。

限制設定群組政策的權限

卡巴斯基安全管理中心管理員可以根據使用者工作職責設定管理主控台使用者的權限以使用不同的 Kaspersky Security for Mobile 整合解決方案。

在管理主控台介面中，您可以在「管理伺服器內容」視窗的「**安全性**」和「**使用者角色**」標籤上設定存取權限。在「**使用者角色**」標籤上，您可以新增具有預定義權限群組的標準使用者角色。在「**安全性**」區域，您可以為一個使用者或一組使用者設定權限，也可以為一個使用者或一組使用者分配角色。使用者對於每個應用程式的權限根據*功能範圍*進行設定。

您也可以設定特定於功能區域的使用者權限。附錄中提供了有關功能區域和政策標籤的對應關係的資訊。

對於每個功能方面，管理員可以分配以下權限：

- **允許編輯**。允許管理主控台使用者在內容視窗中變更政策設定。
- **封鎖編輯**。禁止管理主控台使用者在內容視窗中變更政策設定。屬於該權限分配至的功能範圍的政策標記不會顯示在介面中。

如需在卡巴斯基安全管理中心的管理主控台中管理使用者權限和角色的詳細資訊，請參閱*卡巴斯基安全管理中心說明*。

防護

本部分包含有關如何在卡巴斯基安全管理中心管理主控台中遠端管理行動裝置的防護的資訊。

在 Android 裝置上設定病毒防護

為了及時偵測威脅、病毒和其他惡意應用程式，您應配置即時防護和病毒掃描自動執行設定。

Kaspersky Endpoint Security for Android 可偵測以下類型的物件：

- 病毒、蠕蟲、木馬和惡意工具
- 廣告軟體
- 可偵測被犯罪分子用來損害裝置或個人資料的應用程式

病毒防護有一些限制：

- 當病毒防護正在執行時，在裝置外部記憶體（例如 SD 卡）中偵測到的威脅無法在工作設定檔中自動解毒（具備公事包圖示的應用程式、配置 Android 工作設定檔）。Kaspersky Endpoint Security for Android 在工作設定檔中不能存取外部記憶體。已偵測物件的相關資訊會顯示在應用程式的**狀態**區域。要解毒在外部記憶體中偵測到的物件，物件檔案必須被手動移除且裝置掃描必須重啟。
- 由於技術限制，Kaspersky Endpoint Security for Android 無法掃描大小為 2 GB 或更大的檔案。在掃描期間，應用程式將略過此類別檔案，而不會通知您此類別檔案被略過。

若要配置行動裝置即時防護設定，請執行以下步驟：

1. 在主控台樹狀目錄的「**受管裝置**」資料夾中，選擇 Android 裝置所屬的管理群組。
2. 在所選群組的工作台中，選擇「**政策**」標籤。
3. 透過按兩下任何資料欄來開啟政策內容視窗。
4. 在政策**內容**視窗中選擇**防護**區域。

5. 在**防護**區域中，配置行動裝置檔案系統防護設定：

- 若要啟動即時防護行動裝置，防禦威脅，選擇**啟用防護**方塊。

  Kaspersky Endpoint Security for Android 僅掃描下載資料夾中的新應用程式和檔案。

- 若要啟動行動裝置延伸防護，防禦威脅，請勾選**延伸防護模式**方塊。

  Kaspersky Endpoint Security for Android 將掃描使用者在裝置上開啟、修改、移動、複製、安裝或儲存檔案時，以及新安裝的行動 APP。

  在執行 Android 8.0 或更高版本的裝置上，Kaspersky Endpoint Security for Android 將掃描使用者修改、移動、安裝和儲存的檔案，以及檔案複本。在開啟檔案或複製原始檔案時，Kaspersky Endpoint Security for Android 不會進行掃描。

- 若要啟用新應用程式在使用者裝置上首次啟動時在卡巴斯基安全網路雲端服務的協助下附加掃描，請選取**雲端防護 (KSN)**核取方塊。

- 要封鎖可被犯罪分子利用來損害裝置或使用者資料的廣告軟體和應用程式，請選取**偵測可被犯罪分子用來對使用者的裝置和資料造成損害的廣告軟體、自動撥號程式和應用程式**核取方塊。

6. 在**偵測到威脅時執行的操作**清單中，請選取以下選項之一：

- **刪除**

  偵測到的物件將被自動刪除。不要求使用者做任何其他操作。移除物件之前，Kaspersky Endpoint Security for Android 會顯示偵測到物件的暫時通知。

- **略過**

  如果偵測到的物件遭略過，Kaspersky Endpoint Security for Android 會警告使用者裝置防護方面存在問題。有關略過的物件的資訊會顯示在應用程式的「**狀態**」部分中。對於每個略過的威脅，應用程式都提供使用者可以執行以消除威脅的操作。略過的威脅清單可能會變更，例如，如果可疑檔案遭刪除或移動。若要接收最新的威脅清單，請執行完整裝置掃描。為了確保可靠地防護您的資料，請解毒所有偵測到的物件。

- **隔離**

7. 點擊「**套用**」按鈕以儲存所作的變更。

與卡巴斯基安全管理中心的下個裝置同步之後可配置行動裝置設定。

若要在行動裝置上設定病毒掃描的自動執行，請執行以下操作：

1. 在主控台樹狀目錄的「**受管裝置**」資料夾中，選擇 Android 裝置所屬的管理群組。
2. 在所選群組的工作台中，選擇「**政策**」標籤。
3. 透過按兩下任何資料欄來開啟政策內容視窗。
4. 在政策**內容**視窗中選擇**掃描**區段。
5. 要封鎖可被犯罪分子利用來損害裝置或使用者資料的廣告軟體和應用程式，請選取**偵測可被犯罪分子用來對使用者的裝置和資料造成損害的廣告軟體、自動撥號程式和應用程式**核取方塊。

6. 在**偵測到威脅時執行的操作**清單中，請選取以下選項之一：

- **刪除**

  偵測到的物件將被自動刪除。不要求使用者做任何其他操作。移除物件之前，Kaspersky Endpoint Security for Android 會顯示偵測到物件的暫時通知。

- **略過**

  如果偵測到的物件遭略過，Kaspersky Endpoint Security for Android 會警告使用者裝置防護方面存在問題。有關略過的物件的資訊會顯示在應用程式的「**狀態**」部分中。對於每個略過的威脅，應用程式都提供使用者可以執行以消除威脅的操作。略過的威脅清單可能會變更，例如，如果可疑檔案遭刪除或移動。若要接收最新的威脅清單，請執行完整裝置掃描。為了確保可靠地防護您的資料，請解毒所有偵測到的物件。

- **隔離**

- **詢問使用者**

  Kaspersky Endpoint Security for Android 應用程式將顯示一條通知，提示使用者選擇要對偵測到的物件採取的操作：**略過**或**刪除**。

  當應用程式偵測到多個物件時，**詢問使用者**選項允許裝置使用者透過使用**套用到所有威脅**核取方塊將所選操作應用於每個檔案。

  您必須將 Kaspersky Endpoint Security for Android 設定為可存取功能，以確保 Android 10.0 或更高版本的行動裝置能顯示通知。Kaspersky Endpoint Security for Android 會提示使用者透過初始配置精靈將該應用程式設定為輔助使用功能。使用者可以略過此步驟或以後在裝置設定中停用此服務。在這種情況下，Kaspersky Endpoint Security for Android 顯示 Android 系統視窗，提示使用者選擇要對偵測到的物件採取的操作：「略過」或「刪除」。若要將操作套用於多個物件，您需要開啟 Kaspersky Endpoint Security。

7. **排程掃描**區域允許您設定自動啟動完整掃描裝置系統檔案的設定。若要執行操作，點擊**排程**按鈕，在**排程**視窗中指定完整掃描頻率和啟動時間。

   在 Android 12 或更高版本上，若裝置處於省電模式，應用程式執行此任務的時間可能會晚於指定時間。

8. 點擊「**套用**」按鈕以儲存所作的變更。

與卡巴斯基安全管理中心的下個裝置同步之後可配置行動裝置設定。Kaspersky Endpoint Security for Android 會掃描所有檔案，包括封存內容。

為了保持行動裝置防護為最新，請配置病毒資料庫更新設定。

預設情況下裝置漫遊時會停用病毒資料庫更新。排程的病毒資料庫更新不會執行。

若要配置病毒資料庫更新的設定，請執行以下操作：

1. 在主控台樹狀目錄的「**受管裝置**」資料夾中，選擇 Android 裝置所屬的管理群組。
2. 在所選群組的工作台中，選擇「**政策**」標籤。
3. 透過按兩下任何資料欄來開啟政策內容視窗。

4. 在政策**內容**視窗中選擇**資料庫更新**區段。

5. 如果您希望 Kaspersky Endpoint Security for Android 在裝置位於漫遊區域時依照更新排程下載資料庫更新，請選取**在漫遊時更新資料庫**區段中的**允許漫遊時更新資料庫**核取方塊。

   即使清空了此方塊，使用者可以在裝置漫遊時手動啟動病毒資料庫更新。

6. 在「**資料庫更新來源**」區域中，指定 Kaspersky Endpoint Security for Android 接收並安裝病毒資料庫更新所需的更新來源：

   - **Kaspersky 伺服器**

     將 Kaspersky 更新伺服器用作更新來源，以將 Kaspersky Endpoint Security for Android 的資料庫下載到使用者行動裝置上。要從 Kaspersky 伺服器更新資料庫，Kaspersky Endpoint Security for Android 傳輸資料到 Kaspersky（例如，更新工作執行 ID）。資料庫更新過程中傳輸的資料清單提供在最終使用者產品授權協議中。

   - **管理伺服器**

     將卡巴斯基安全管理中心管理伺服器的儲存區用作更新來源，以將 Kaspersky Endpoint Security for Android 的資料庫下載到使用者行動裝置上。

   - **其他來源**

     將第三方伺服器用作更新來源，以將 Kaspersky Endpoint Security for Android 的資料庫下載到使用者行動裝置上。在啟動更新前，您應在下面的欄位中輸入 HTTP 伺服器的位址（範例，http://domain.com/）。

7. 在**排程的資料庫更新**區段中，配置使用者裝置上病毒資料庫自動更新設定。若要執行操作，點擊**排程**按鈕，在**排程**視窗中指定更新頻率和啟動時間。

   在 Android 12 或更高版本上，若裝置處於省電模式，應用程式執行此任務的時間可能會晚於指定時間。

8. 點擊「**套用**」按鈕以儲存所作的變更。

與卡巴斯基安全管理中心的下個裝置同步之後可配置行動裝置設定。

在網際網路上防護 Android 裝置

要在網際網路上保護行動裝置使用者的個人資料，請啟用 Web 防護。Web 防護可封鎖散佈惡意程式碼的惡意網站和釣魚網站，例如用於竊取個人資料和銀行帳戶的網站。Web 防護將在您開啟網站前使用卡巴斯基安全網路雲端服務掃描網站。Web 防護還允許您根據預定義的允許的網站和封鎖的網站的清單，配置使用者對網站的存取權限。

您必須將 Kaspersky Endpoint Security for Android 設定為輔助使用功能。Kaspersky Endpoint Security for Android 會提示使用者透過初始配置精靈將該應用程式設定為輔助使用功能。使用者可以略過此步驟或以後在裝置設定中停用此服務。

Android 裝置上的 Web 防護僅在 Google Chrome 瀏覽器（包括自訂標籤功能）、Huawei Browser 和 Samsung Internet Browser 中可用。如果使用工作設定檔且只針對工作設定檔啟用 Web 防護，則 Samsung Internet Browser 的 Web 防護不會封鎖行動裝置上的網站。

若要在 Google Chrome、Huawei 瀏覽器或 Samsung Internet Browser 中啟用 Web 防護：

1. 在主控台樹狀目錄的「**受管裝置**」資料夾中，選擇 Android 裝置所屬的管理群組。
2. 在所選群組的工作台中，選擇「**政策**」標籤。
3. 透過按兩下任何資料欄來開啟政策內容視窗。
4. 在政策的**內容**視窗中選擇**Web 防護**。
5. 若要使用 Web 防護，您或裝置使用者必須閱讀並同意利用 Web 防護進行資料處理的聲明（Web 防護聲明）：
   a. 按一下連結 **Web 防護聲明**。
      這會開啟**利用 Web 防護進行資料處理的聲明**視窗。若要同意 Web 防護聲明，您必須閱讀並同意隱私權政策。
   b. 按一下隱私權政策連結。閱讀並同意隱私權政策。
      若您不同意隱私權政策，行動裝置使用者可在初始設定精靈或應用程式中同意隱私權政策（ → **關於** → **條款和條件** → **隱私權政策**）。
   c. 選擇 Web 防護聲明同意模式：
      - **我已閱讀並同意 Web 防護聲明**
      - **向裝置使用者要求同意 Web 防護聲明**
      - **我不同意 Web 防護聲明**
6. 若您選擇**我不同意 Web 防護聲明**，Web 防護就不會封鎖行動裝置上的網站。行動裝置使用者無法在 Kaspersky Endpoint Security 中啟用 Web 防護。
7. 選取**啟用 Web 防護**核取方塊。
8. 點擊「**套用**」按鈕以儲存所作的變更。

與卡巴斯基安全管理中心的下個裝置同步之後可配置行動裝置設定。

防護被竊取或遺失的裝置資料

本節介紹了如何在裝置被竊取或遺失時配置非授權存取防護設定。

向行動裝置傳送指令

要防護遺失或被竊取的行動裝置上的資料，您可以傳送特殊命令（請參閱下表）。

用於防護遺失或被竊取裝置上的資料的命令

連線到卡巴斯基安全管理中心的方法	命令	命令執行結果
Kaspersky Endpoint	鎖定	行動裝置將被鎖定。
	解鎖	解鎖執行著 Android 5.0 – 6.X 的行動裝置後，螢幕解鎖密碼 (PIN code) 重設為

Security for Android		「1234」。解鎖執行著 Android 7.0 或更新版本的裝置後，螢幕解鎖密碼不變。
	裝置定位	裝置將被定位並顯示在 Google Maps 中。行動服務提供商會收取傳送簡訊和上網的費用。 在執行 Android 12 或更高版本的裝置上，如果使用者授予「使用大致位置」權限，Kaspersky Endpoint Security for Android 應用程式首先會嘗試取得準確的裝置位置。如果這麼做不成功，則僅在不超過 30 分鐘前收到裝置的大致位置時才傳回該裝置的大致位置。否則，**定位裝置**命令將失敗。
	臉部快照	行動裝置將被鎖定。當犯罪分子試圖解鎖裝置時，裝置的前置相機會拍攝臉部快照。行動服務提供商會收取傳送簡訊和上網的費用。 當試圖解鎖裝置時，使用者自動同意臉部快照。 如果相機的使用權限已被撤銷，行動裝置會顯示通知並提示提供權限。在執行 Android 12 或更高版本的行動裝置上，如果透過快速設定撤銷了使用相機的權限，則不會顯示通知，但拍攝的照片會是黑色。
	警報	行動裝置發出警報。警報響 5 分鐘（如果裝置的電池電量低，則響 1 分鐘）。
	抹除企業資料	抹除容器中的資料、公司電子郵件帳戶、用於連線至公司 Wi-Fi 網路和 VPN 的設定、接入點名稱 (APN)、Android 工作設定檔、KNOX 容器和 KNOX License Manager 金鑰。
	重設為出廠設定	所有資料都將從行動裝置中刪除，設定將回溯至其出廠值。執行此命令後，裝置將無法接收或執行後續命令。
iOS MDM 設定檔	鎖定	行動裝置將被鎖定。
	解鎖	將停用使用 PIN 碼鎖定的行動裝置。之前指定的 PIN 碼已重設。
	抹除企業資料	將從裝置中刪除所有已安裝的配置設定檔、佈建設定檔、iOS MDM 設定檔以及已選擇**與 iOS MDM 設定檔一起刪除**核取方塊的應用程式。
	重設為出廠設定	所有資料都將從行動裝置中刪除，設定將回溯至其出廠值。執行此命令後，裝置將無法接收或執行後續命令。
Exchange 信箱	重設為出廠設定	所有資料都將從行動裝置中刪除，設定將回溯至其出廠值。執行此命令後，裝置將無法接收或執行後續命令。

執行 Kaspersky Endpoint Security for Android 的命令需要特殊的權利和權限。當初始設定精靈正在執行時，Kaspersky Endpoint Security for Android 會提示使用者授予應用程式所有必需的權利和權限。使用者可以略過這些步驟或以後在裝置設定中停用這些權限。如果是這種情況，您無法執行命令。

在執行 Android 10.0 或更新版本的裝置上，使用者必須授與「任何時間」均可存取裝置位置的權限。在執行 Android 11.0 或更新版本的裝置上，使用者也必須授與「使用應用程式期間」的權限來存取相機。否則，竊盜防護命令將無法運作。使用者會收到此限制的通知，並且會再次收到要求授與所需層級權限的提示。若使用者選取「只有這次」選項來授與相機權限，則會視為是應用程式授與存取權限。若系統再次要求存取相機的權限，建議您直接聯絡使用者。

若要深入瞭解如何在管理主控台透過行動裝置清單傳送命令，請參閱 *卡巴斯基安全管理中心說明*。

解鎖行動裝置

您可以使用以下方法解鎖行動裝置：

- 傳送行動裝置解鎖命令。
- 在行動裝置上輸入一次性解鎖碼（僅適用于 Android 裝置）。

在某些裝置（例如，Huawei、Meizu 和 Xiaomi）上，您必須手動將 Kaspersky Endpoint Security for Android 新增到在作業系統啟動時啟動的應用程式清單。如果未將該應用程式新增到清單，只能使用一次性解鎖代碼解鎖裝置。不能使用命令解鎖裝置。

若要深入瞭解如何在管理主控台透過行動裝置清單傳送命令，請參閱 *卡巴斯基安全管理中心說明*。

*一次性解鎖碼*是用於解鎖行動裝置的應用程式密碼。一次性密碼由應用程式對於每個行動裝置建立唯一的代碼。您可以在群組政策設定中的「**竊盜防護**」區域變更一次性代碼的長度（4、8 或 16 位數）。

要使用一次性密碼解鎖行動裝置：

1. 在主控台樹狀目錄中，選擇「**行動裝置管理**」→「**行動裝置**」。
2. 選擇您要獲取其一次性解鎖代碼的行動裝置。
3. 透過點擊開啟行動裝置內容視窗。
4. 選取**應用程式** → **Kaspersky Endpoint Security for Android**。
5. 透過點擊開啟 Kaspersky Endpoint Security 內容視窗。
6. 選擇「**竊盜防護**」區域。
7. 選定裝置唯一的密碼將顯示在「**一次性裝置解鎖碼**」區域的「**一次性密碼**」欄位中。
8. 使用任意可用的方法（例如電子郵件）將一次性密碼告知已鎖定裝置的使用者。
9. 使用者在 Kaspersky Endpoint Security for Android 鎖定的裝置的螢幕上輸入一次性密碼。

行動裝置會被解鎖。解鎖執行著 Android 5.0 – 6.X 的行動裝置後，螢幕解鎖密碼 (PIN code) 重設為「1234」。解鎖執行著 Android 7.0 或更新版本的裝置後，螢幕解鎖密碼不變。

資料加密

要防護資料以防非授權的存取，您必須啟用裝置上所有資料的加密（例如，帳戶憑證、外部裝置和應用、以及電子郵件訊息、SMS 訊息、聯絡人、照片和其他檔案）。對於加密資料的存取，您必須指定特殊金鑰 – 裝置解鎖密碼。如果資料被加密，對它的存取僅在裝置解鎖時可行。

在密碼鎖定 iOS 裝置上資料加密預設被啟用（**設定 → Touch ID / Face ID 和密碼 → 啟用密碼**）。

要在 Android 裝置上加密所有資料：

1. 在 Android 裝置上啟用螢幕鎖（**設定 → 安全 → 螢幕鎖定**）。
2. 設定與企業安全需求合規的裝置解鎖密碼。

   建議使用圖形密碼以解鎖裝置。在執行 Android 6.0 或更新版本的 Android 裝置上，在加密資料和重啟 Android 裝置後，您必須輸入數字密碼而不是圖形密碼來解鎖裝置。該問題關乎可存取功能服務的操作。要在該情況下解鎖裝置，轉換圖形密碼到數字密碼。對於更多轉換圖形密碼到數字密碼的詳情，請參考行動裝置生產商的技術支援網站。

3. 在裝置上啟用對所有裝置的加密（**設定 → 安全 → 加密資料**）。

設定解鎖密碼強度

要防護對使用者行動裝置的存取，您應該設定裝置解鎖密碼。

本節包含有關如何在 Android 和 iOS 裝置上設定密碼防護的資訊。

為 Android 裝置設定強式解鎖密碼

若要確保 Android 裝置安全，您需要配置使用密碼，在裝置從睡眠模式喚醒時提示使用者輸入密碼。

如果解鎖密碼不強，您可以對裝置上的使用者活動施加限制（例如鎖定裝置）。您可以使用合規性控制元件施加限制。為此，在掃描規則設定中，您必須選擇**解鎖密碼不符合安全要求**標準。

在某些執行 Android 7.0 或更高版本的 Samsung 裝置上，當使用者嘗試配置不受支援的方法（例如，圖形密碼）來解鎖裝置時，如果滿足以下條件，裝置可能會鎖定：Kaspersky Endpoint Security for Android 移除防護已啟用並且設定了螢幕解鎖密碼長度要求。要解鎖裝置，您必須傳送特殊命令到裝置。

若要配置使用解鎖密碼，請執行以下操作：

1. 在主控台樹狀目錄的「**受管裝置**」資料夾中，選擇 Android 裝置所屬的管理群組。
2. 在所選群組的工作台中，選擇「**政策**」標籤。
3. 透過按兩下任何資料欄來開啟政策內容視窗。
4. 在政策「**內容**」視窗中選擇「**裝置管理**」區域。
5. 如果您希望應用程式確認是否設定了解鎖密碼，請選擇**螢幕鎖定**區段中的**需要設定螢幕解鎖密碼**核取方塊。

如果應用程式偵測到裝置上未設定任何系統密碼，請提示使用者進行設定。密碼根據管理員定義的參數來設定（請參閱下圖）。

6. 指定最少字元數。

   使用者密碼的最小字元數。可能值：4 到 16 個字元。

   預設情況下，使用者的密碼包含 4 個字元。

   在執行 Android 10.0 或更高版本的裝置上，Kaspersky Endpoint Security 會將密碼強度要求解析為其中一個系統值：中度或高度。

   執行 Android 10.0 或更新版本裝置的數值將由以下規則決定：

   - 如果要求的密碼長度是 1 到 4 個符號，那麼應用程式會提示使用者設定中等強度的密碼。密碼必須是數字 (PIN) 且沒有重複或有順序 (如 1234) 的序列或字母/英數字母。PIN 或密碼的長度必須至少有 4 個字元。
   - 如果要求的密碼長度為 5 個以上的符號，那麼應用程式會提示使用者設定高強度密碼。密碼必須是數字 (PIN)，沒有重複或有順序的序列或字母/英數字母 (password)。 PIN 必須至少有 8 位數，密碼長度必須至少有 6個字元。

7. 如果您希望使用者能使用指紋解鎖螢幕，請選取**允許使用指紋**方塊。如果解鎖密碼不符合企業安全需求，則無法使用指紋掃描器解鎖螢幕。

   在執行 Android 10.0 或更高版本的裝置上，螢幕指紋解鎖的使用僅可針對工作設定檔來加以管理。

   Kaspersky Endpoint Security for Android 不會限制使用指紋掃描器來登入應用程式或確認購買。

   在某些 Samsung 裝置上，無法封鎖使用指紋解鎖螢幕。在某些 Samsung 裝置上，如果解鎖密碼不符合企業安全需求，Kaspersky Endpoint Security for Android 不會封鎖使用指紋解鎖螢幕。

   在裝置設定中新增指紋後，使用者可以使用以下方法解鎖螢幕：

   - 將手指按在指紋掃描器上（主要方法）。
   - 輸入解鎖密碼（備用方法）。

8. 點擊「**套用**」按鈕以儲存所作的變更。

與卡巴斯基安全管理中心的下個裝置同步之後可配置行動裝置設定。

為 iOS MDM 裝置設定強解鎖密碼

若要防護 iOS MDM 裝置資料，請配置解鎖密碼強度設定。

預設情況下，使用者可以使用簡單密碼。*簡單密碼*是包含連續或重複字元的密碼，例如「abcd」或「2222」。使用者不需要輸入包含特殊字元的字母數字密碼。預設情況下，密碼有效期和密碼輸入嘗試次數不受限制。

若要配置 iOS MDM 裝置解鎖密碼的強度設定，請執行以下步驟：

1. 在主控台樹狀目錄的「**受管裝置**」資料夾中，選擇 iOS MDM 裝置所屬的管理群組。

2. 在所選群組的工作台中，選擇「**政策**」標籤。

3. 透過點擊開啟政策內容視窗。

4. 在政策「**內容**」視窗中選擇「**密碼**」區域。

5. 在**密碼設定**區域中，選中**將設定套用於裝置**方塊。

6. 配置解鎖密碼強度設定：

   - 若要允許使用者使用簡單密碼，請選擇「**允許簡單密碼**」核取方塊。
   - 若要要求使用者在密碼中使用字母和數字，請選擇「**提示輸入字母數字值**」核取方塊。
   - 在「**最小密碼長度**」清單中，選擇最小密碼長度（以字元為單位）。
   - 在「**特殊字元最小數量**」清單中，選擇密碼中特殊字元（例如，「$」、「&」和「!」）的最少數量。
   - 在「**密碼最長有效期**」欄位中，指定密碼保持為目前密碼的時間期限（單位：天數）。這段時間過後，Kaspersky Device Management for iOS 會提示使用者變更密碼。
   - 在「**啟用自動鎖定**」清單中，選擇在多長時間後啟用 iOS MDM 裝置自動鎖定。
   - 在「**密碼歷史**」欄位中，指定已使用密碼的數量（包括目前密碼），在使用者變更舊密碼時，Kaspersky Device Management for iOS 會將舊密碼和新密碼進行對比。如果密碼比對，新密碼將被拒絕。
   - 在「**不需輸入密碼解鎖的閒置時間**」清單中，選擇使用者在多長時間內不用輸入密碼即可解鎖 iOS MDM 裝置。
   - 在「**存取嘗試的最大次數**」清單中，選擇使用者在輸入 iOS MDM 裝置解鎖密碼時可進行的存取嘗試次數。

7. 點擊「**套用**」按鈕以儲存所作的變更。

這樣，在套用政策後，Kaspersky Device Management for iOS 將在使用者的行動裝置上檢查設定的密碼的強度。如果裝置解鎖密碼強度不符合政策，將提示使用者變更密碼。

為 EAS 裝置設定強解鎖密碼

設定強解鎖密碼，防護 EAS 裝置資料。

預設情況下，在行動裝置開機時，Kaspersky Device Management for iOS 不會提示使用者輸入或設定解鎖密碼。

若要配置 EAS 裝置解鎖密碼的強度設定，請執行以下操作：

1. 在主控台樹狀目錄的「**受管裝置**」資料夾中，選擇 EAS 裝置所屬的管理群組。

2. 在所選群組的工作台中，選擇「**政策**」標籤。

3. 透過點擊開啟政策內容視窗。

4. 在政策「內容」視窗中，選擇「**密碼**」區域。

5. 在**密碼設定**區域中，選中**提示輸入密碼**方塊。

6. 配置解鎖密碼強度設定：

- 若需要要求使用者在密碼中使用字母和數字，請選擇「**提示輸入字母數字值**」核取方塊。在「**最少字元集數量**」欄位中，指定字母數字密碼的強度級別。可能值：1到 4。值「1」對應的是最低的強度級別。
- 若要允許使用者使用密碼還原功能，請選擇「**啟用密碼還原**」核取方塊。
- 如果您要在裝置記憶體中加密檔案，請選擇「**需要加密裝置**」核取方塊。
- 如果您要加密記憶體卡上的檔案，請選擇「**需要加密記憶體卡**」核取方塊。
- 若要允許使用者使用僅包含數字的簡單密碼，請選擇「**允許簡單密碼**」核取方塊。
- 若要限制輸入存取裝置的密碼的嘗試次數，請選擇「**存取嘗試的最大次數**」核取方塊。在該方塊右側的欄位中，指定使用者為解鎖裝置可進行的密碼輸入嘗試次數。如果使用者在指定的連續嘗試次數後未能輸入正確的密碼，Kaspersky Device Management for iOS 會抹除所有裝置資料。
- 若要指定使用者密碼的最短長度，請選擇「**最小字元數量**」核取方塊。在該方塊右側的欄位中指定密碼字元的最少數量。可能值：4 到 16 個字元。
- 若要提示使用者在裝置空閒一段時間後輸入密碼，請選中**密碼輸入的新嘗試前的閒置時間（分鐘）**方塊。在該方塊右側的欄位中指定空閒分鐘數。這段時間過後，應用程式會提示使用者輸入密碼。
- 若要限制密碼有效期，請選擇「**密碼有效期（天）**」核取方塊。在該方塊右側的欄位中指定密碼有效期。這段時間過後，應用程式會提示使用者變更密碼。
- 在「**密碼記錄**」字段中，欄位中，您可以指定不能重複使用的最近的舊密碼的數量。

7. 點擊「**套用**」按鈕以儲存所作的變更。

與卡巴斯基安全管理中心的下次裝置同步之後可配置行動裝置設定。一旦套用該政策，Kaspersky Device Management for iOS 將檢查使用者的行動裝置上是否設定了密碼。如果裝置上尚未設定解鎖密碼，則會提示使用者進行設定。設定密碼時應考慮政策設定。如果已設定裝置解鎖密碼，但它不符合政策，將提示使用者變更密碼。

設定虛擬私人網路 (VPN)

本節包含有關配置虛擬私人網路絡 (VPN) 設定以安全連線到 Wi-Fi 網路的資訊。

在 Android 裝置上配置 VPN（僅限 Samsung）

若要將 Android 裝置安全地連線到 Wi-Fi 網路並保護資料傳輸，您應該配置 VPN（虛擬私人網路）設定。

VPN 配置僅適用於 Samsung 裝置。

在使用虛擬私人網路時應考慮以下要求：

- 必須在在防火牆設定中允許使用 VPN 連線的應用程式。
- 在該政策中配置的虛擬私人網路設定不能套用于系統應用程式。系統應用程式的 VPN 連線必須手動配置。

- 某些使用 VPN 連線的應用程式需要在第一次啟動時配置附加設定。若要配置設定，必須在應用程式設定中啟用 VPN 連線。

若要設定使用者行動裝置上的 VPN，請執行以下操作：

1. 在主控台樹狀目錄的「**受管裝置**」資料夾中，選擇 Android 裝置所屬的管理群組。
2. 在所選群組的工作台中，選擇「**政策**」標籤。
3. 透過按兩下任何資料欄來開啟政策內容視窗。
4. 在政策「**內容**」視窗中選擇「**管理 Samsung KNOX**」→「**管理 Samsung 裝置**」區域。
5. 在「**VPN**」區域中，點擊「**配置**」按鈕。
   這將開啟「**VPN 網路**」視窗。
6. 在「**連線類型**」下拉清單中選擇 VPN 連線的類型。
7. 在「**網路名稱**」欄位中輸入 VPN 通道的名稱。
8. 在「**伺服器位址**」欄位中，輸入 VPN 伺服器的網路名稱或 IP 位址。
9. 在「**DNS 搜尋網域**」清單中，輸入要自動新增到 DNS 伺服器名稱中的 DNS 搜尋網域。
   您可以指定多個 DNS 搜尋網域，用空格將它們分隔。
10. 在「**DNS 伺服器**」欄位中，輸入 DNS 伺服器的完整網域名稱或 IP 位址。
    您可以指定多個 DNS 伺服器，用空格將它們分隔。
11. 在「**路由**」欄位中，輸入透過 VPN 連線與其交換資料的網路 IP 位址的範圍。

    如果未在**路由**欄位中指定 IP 位址的範圍，所有網際網路流量都將透過 VPN 連線傳輸。

12. 附加配置「**IPSec Xauth PSK**」和「**L2TP IPSec PSK** 」類型網路的以下設定：
    a. 在「**IPSec 共用金鑰**」欄位中，輸入預設 IPSec 安全金鑰的密碼。
    b. 在「**IPSec ID**」欄位中輸入行動裝置使用者的名稱。
13. 對於 **L2TP IPSec PSK** 網路，您還可以在「**L2TP 金鑰**」欄位中為 L2TP 金鑰指定密碼。
14. 對於 **PPTP** 網路，選擇「**使用 SSL 連線**」核取方塊，以便在行動裝置連線至 VPN 伺服器時應用程式使用 MPPE（Microsoft Point-to-Point Encryption）資料加密方法防護資料傳輸。
15. 點擊「**套用**」按鈕以儲存所作的變更。

與卡巴斯基安全管理中心的下個裝置同步之後可配置行動裝置設定。

在 iOS MDM 裝置上配置 VPN

若要將 iOS MDM 裝置連線至虛擬私人網路 (VPN) 並在連線至 VPN 期間防護資料，請配置 VPN 連線設定。

若要在使用者的 iOS MDM 裝置上配置 VPN 連線，請執行以下操作：

1. 在主控台樹狀目錄的「**受管裝置**」資料夾中，選擇 iOS MDM 裝置所屬的管理群組。

2. 在所選群組的工作台中，選擇「**政策**」標籤。

3. 透過點擊開啟政策內容視窗。

4. 在政策「**內容**」視窗中選擇「**VPN**」區域。

5. 按一下「**VPN 網路**」區域中的「**新增**」按鈕。
   這將開啟「**VPN 網路**」視窗。

6. 在「**網路名稱**」欄位中輸入 VPN 通道的名稱。

7. 在「**連線類型**」下拉清單中選擇 VPN 連線的類型：

   - **L2TP**（第 2 層通道協定）。該連線支援使用 MS-CHAP v2 密碼、雙重身分驗證和使用公開金鑰的自動身分驗證對 iOS MDM 行動裝置使用者進行身分驗證。
   - **PPTP**（點對點通道通訊協定）。該連線支援使用 MS-CHAP v2 密碼和雙重身分驗證對 iOS MDM 行動裝置使用者進行身分驗證。
   - **IPSec (Cisco)**。該連線支援基於密碼的使用者認證、雙重身分驗證和使用公開金鑰與憑證的自動身分驗證。
   - **Cisco AnyConnect**。該連線支援版本 8.0(3).1 或更高版本的 Cisco Adaptive Security Appliance (ASA) 防火牆。若要設定 VPN 連線，請從 App Store 將 Cisco AnyConnect 應用程式安裝到 iOS MDM 行動裝置上。
   - **Juniper SSL**。該連線支援版本 6.4 或更高版本的 SA 系列 Juniper Networks SSL VPN 閘道，該閘道包含版本 7.0 或更高版本的 Juniper Networks IVE 套裝程式。若要設定 VPN 連線，請從 App Store 將 JUNOS 應用程式安裝到 iOS MDM 行動裝置上。
   - **F5 SSL**。該連線支援 F5 BIG-IP Edge Gateway、Access Policy Manager 和 Fire SSL VPN 解決方案。若要設定 VPN 連線，請從 App Store 將 F5 BIG-IP Edge Client 應用程式安裝到 iOS MDM 行動裝置上。
   - **SonicWALL Mobile Connect**。該連線支援版本 10.5.4 或更高版本的 SonicWALL Aventail E-Class Secure Remote Access 裝置、版本 5.5 或更高版本的 SonicWALL SRA 裝置以及 SonicWALL Next-Generation Firewall 裝置，包括 TZ、NSA 和包含版本 5.8.1.0 或更高版本的 SonicOS 的 E-Class NSA。若要設定 VPN 連線，請從 App Store 將 SonicWALL Mobile Connect 應用程式安裝到 iOS MDM 行動裝置上。
   - **Aruba VIA**。該連線支援 Aruba Networks 行動存取控制。若要配置它們，請從 App Store 將 Aruba Networks VIA 應用程式安裝到 iOS MDM 行動裝置上。
   - **自訂 SSL**。該連線支援使用密碼、憑證和雙重身分驗證對 iOS MDM 行動裝置使用者進行身分驗證。

8. 在「**伺服器位址**」欄位中，輸入 VPN 伺服器的網路名稱或 IP 位址。

9. 在**帳戶名稱**欄位中，輸入要在 VPN 伺服器上進行身分驗證的帳戶名稱。您可以使用「**可用巨集**」下拉清單中的巨集。

10. 根據選擇的虛擬私人網路類型配置 VPN 連線的安全設定。

11. 如有必要，配置透過代理伺服器連線 VPN 的設定。

    a. 選擇「**代理伺服器設定**」標籤。

    b. 選擇代理伺服器配置模式和指定連線設定。

c. 點擊「**確定**」。

這樣，已在 iOS MDM 裝置上配置裝置透過代理伺服器連線 VPN 的設定。

12. 點擊「**確定**」。
新的 VPN 將顯示在清單中。

13. 點擊「**套用**」按鈕以儲存所作的變更。

這樣，一旦套用該政策，將在使用者的 iOS MDM 裝置上配置 VPN 連線。

在 Android 裝置上設定防火牆（僅限 Samsung）

組配置防火牆設定，監控使用者的行動裝置上的網路連線。

若要在行動裝置上設定防火牆，請執行以下步驟：

1. 在主控台樹狀目錄的「**受管裝置**」資料夾中，選擇 Android 裝置所屬的管理群組。
2. 在所選群組的工作台中，選擇「**政策**」標籤。
3. 透過按兩下任何資料欄來開啟政策內容視窗。
4. 在政策「**內容**」視窗中選擇「**管理 Samsung KNOX**」→「**管理 Samsung 裝置**」區域。
5. 在「**防火牆**」視窗中，點擊「**設定**」。
「**防火牆**」視窗將開啟。
6. 選擇防火牆設定：
   - 若要允許所有傳送和接收連線，請將滑塊滑動到「**全部允許**」。
   - 若要封鎖除排除清單中的應用程式的網路活動以外的所有網路活動，請將滑桿向上滑動到「**全部封鎖（排除項目除外）**」。
7. 如果您已將防火牆模式設定為「**全部封鎖（排除項目除外）**」，請建立排除清單：
   a. 點擊「**新增**」。
   這將開啟「**防火牆排除項目**」視窗。
   b. 在「**應用程式名稱**」欄位中輸入行動 APP 的名稱。
   c. 在「**套件名稱**」欄位中輸入行動 APP 套件的系統名稱（例如 `com.mobileapp.example`）。
   d. 點擊「**確定**」。
8. 點擊「**套用**」按鈕以儲存所作的變更。

與卡巴斯基安全管理中心的下個裝置同步之後可配置行動裝置設定。

防止 Kaspersky Endpoint Security for Android 被移除

為了防護行動裝置和遵守企業安全需求，您可以啟用防護以防止移除 Kaspersky Endpoint Security for Android。在這種情況下，使用者無法使用 Kaspersky Endpoint Security for Android 介面移除該應用程式。當使用 Android 作業系統的工具刪除應用程式時，系統會提示您停用 Kaspersky Endpoint Security for Android 的管理員權限。停用權限後，行動裝置將被鎖定。

在某些執行 Android 7.0 或更高版本的 Samsung 裝置上，當使用者嘗試配置不受支援的方法（例如，圖形密碼）來解鎖裝置時，如果滿足以下條件，裝置可能會鎖定：Kaspersky Endpoint Security for Android 移除防護已啟用並且設定了螢幕解鎖密碼長度要求。要解鎖裝置，您必須傳送特殊命令到裝置。

若要啟用防護以防止移除 Kaspersky Endpoint Security for Android，請執行以下操作：

1. 在主控台樹狀目錄的「**受管裝置**」資料夾中，選擇 Android 裝置所屬的管理群組。
2. 在所選群組的工作台中，選擇「**政策**」標籤。
3. 透過按兩下任何資料欄來開啟政策內容視窗。
4. 在政策「**內容**」視窗中選擇「**其他**」區域。
5. 在「**移除 Kaspersky Endpoint Security for Android**」區域中，清除「**允許移除 Kaspersky Endpoint Security for Android**」核取方塊。

   要防護在執行 Android 7.0 或更高版本的裝置上的應用程式不會被移除，必須將 Kaspersky Endpoint Security for Android 設定為可存取功能。當初始配置精靈正在執行時，Kaspersky Endpoint Security for Android 會提示使用者授予應用程式所有必需的權限。使用者可以略過這些步驟或以後在裝置設定中停用這些權限。在這種情況下，不防護該應用程式不被移除。

6. 點擊「**套用**」按鈕以儲存所作的變更。

與卡巴斯基安全管理中心的下次裝置同步之後可配置行動裝置設定。如果嘗試移除應用程式，行動裝置將被鎖定。

偵測裝置上的駭客攻擊（根權限）

Kaspersky Security for Mobile 可以讓您偵測到裝置上的駭客攻擊（根權限）。被駭客入侵的裝置上的系統檔案不受防護，因此可能會遭修改。此外，來自未知來源的其他應用程式可能會安裝在被駭客入侵的裝置上。在偵測到駭客嘗試後，建議您立即還原裝置的正常操作。

為了偵測使用者何時獲取根權限，Kaspersky Endpoint Security for Android 會使用以下服務：

- *Embedded service of Kaspersky Endpoint Security for Android* 是一種 Kaspersky 服務，用於檢查行動裝置使用者是否已獲取根權限 (Kaspersky Mobile Security SDK)。
- *SafetyNet Attestation* 是一種 Google 服務，用於檢查作業系統的完整性、分析裝置硬體和軟體，以及識別其他安全問題。如需 SafetyNet Attestation 的詳細資訊，請造訪Android 技術支援網站。

如果裝置被駭客入侵，您會收到一條通知。您可以在管理伺服器工作台的**監控**標籤上檢視駭客入侵通知。還可以在事件通知設定中停用有關駭客的通知。

在執行 Android 的裝置上，如果裝置被駭客入侵，您可以對裝置上的使用者活動施加限制（例如鎖定裝置）。您可以透過使用合規性控制元件施加限制（請參閱下圖）。為此，請在掃描規則設定中，選擇**裝置已取得最高權限**條件。

在 iOS MDM 裝置上設定全域 HTTP 代理

若要防護使用者的網際網路流量，請配置透過代理伺服器將 iOS MDM 裝置連線至網際網路。

僅受控制的裝置可以透過代理伺服器自動連線至網際網路。

若要在 iOS MDM 裝置上配置全域 HTTP 代理設定，請執行以下操作：

1. 在主控台樹狀目錄的「**受管裝置**」資料夾中，選擇 iOS MDM 裝置所屬的管理群組。
2. 在所選群組的工作台中，選擇「**政策**」標籤。
3. 透過點擊開啟政策內容視窗。
4. 在政策「**內容**」視窗中選擇「**全域 HTTP 代理**」區域。
5. 在「**全域 HTTP 代理設定**」區域中，選中「**將設定套用於裝置**」核取方塊。
6. 選擇全域 HTTP 代理配置的類型。

   預設情況下，選擇手動配置全域 HTTP 代理的類型，禁止使用者在不連接代理伺服器的情況下連線到受控網路。*受控網路*是需要在不連接代理伺服器的情況下，對行動裝置進行初步身分驗證的無線網路。

   - 若要手動指定代理伺服器連線設定，請執行以下操作：
     a. 在「**代理設定類型**」下拉清單中，選擇「**手動**」。
     b. 在「**代理伺服器位址和連接埠**」欄位中，輸入主機的名稱或代理伺服器的 IP 位址和代理伺服器埠號。
     c. 在「**使用者名稱**」欄位中，設定用於代理伺服器身分驗證的使用者帳戶名稱。您可以使用「**可用巨集**」下拉清單中的巨集。
     d. 在「**密碼**」欄位中，設定用於代理伺服器身分驗證的使用者帳戶密碼。
     e. 若要允許使用者存取受控網路，請選擇「**允許存取強制網路而不用連線到代理**」核取方塊。
   - 若要使用預定義的 PAC（代理自動配置）檔配置代理伺服器連線設定，請執行以下步驟：
     a. 在「**代理設定類型**」下拉清單中，選擇「**自動**」。
     b. 在「**PAC 檔案的位址**」欄位中輸入 PAC 檔案的網址（例如：http://www.example.com/filename.pac）。
     c. 若要允許使用者在無法存取 PAC 檔案時，不使用代理伺服器將行動裝置連線至無線網路，請選中「**如果無法存取 PAC 檔案，則允許直接連線**」核取方塊。
     d. 若要允許使用者存取受控網路，請選擇「**允許存取強制網路而不用連線到代理**」核取方塊。
7. 點擊「**套用**」按鈕以儲存所作的變更。

這樣，一旦套用該政策，行動裝置使用者將透過代理伺服器連線至網際網路。

向 iOS MDM 裝置新增安全憑證

為了簡化使用者身分驗證和確保資料安全，請在使用者的 iOS MDM 裝置上新增憑證。在網路交換過程中，防護使用憑證簽章的資料不被變更。使用憑證加密資料，可提高資料安全級別。憑證還可以用於驗證使用者的身分。

Kaspersky Device Management for iOS 支援以下憑證標準：

- **PKCS#1** – 使用基於 RSA 演算法的公開金鑰加密。
- **PKCS#12** – 儲存和傳輸憑證與私密金鑰。

若要在使用者的 iOS MDM 裝置上新增安全憑證，請執行以下操作：

1. 在主控台樹狀目錄的「**受管裝置**」資料夾中，選擇 iOS MDM 裝置所屬的管理群組。
2. 在所選群組的工作台中，選擇「**政策**」標籤。
3. 透過點擊開啟政策內容視窗。
4. 在政策「**內容**」視窗中選擇「**憑證**」區域。
5. 按一下「**憑證**」區域中的「**新增**」按鈕。
   「**憑證**」視窗將開啟。
6. 在「**檔案名稱**」欄位中，指定憑證的路徑：

   PKCS#1 憑證檔案的副檔名為 cer、crt 或 der。PKCS#12 憑證檔案的副檔名為 p12 或 pfx。

7. 點擊「**開啟**」。
   如果憑證受密碼防護，請指定密碼。新的憑證顯示在清單中。
8. 點擊「**套用**」按鈕以儲存所作的變更。

這樣，一旦套用該政策，將提示使用者安裝已建立的清單中的憑證。

向 iOS MDM 裝置新增 SCEP 設定檔

您必須新增 SCEP 設定檔，以便 iOS MDM 裝置使用者透過網際網路自動接收來自憑證中心的憑證。SCEP 設定檔可支援簡單憑證註冊協定。

預設新增具有以下設定的 SCEP 設定檔：

- 不使用備用主題名稱註冊憑證。
- 進行三次 SCEP 伺服器輪詢嘗試，每次間隔 10 秒。如果憑證簽章的所有嘗試失敗，您必須產生新的憑證簽章請求。
- 接收的憑證不能用於資料簽章或加密。

您可以在新增 SCEP 設定檔時編輯指定的設定。

若要新增 SCEP 設定檔，請執行以下操作：

1. 在主控台樹狀目錄的「**受管裝置**」資料夾中，選擇 iOS MDM 裝置所屬的管理群組。
2. 在所選群組的工作台中，選擇「**政策**」標籤。
3. 透過點擊開啟政策內容視窗。
4. 在政策「**內容**」視窗中選擇「**SCEP**」區域。
5. 按一下「**SCEP 設定檔**」區域中的「**新增**」按鈕。
   「**SCEP 設定檔**」視窗將開啟。
6. 在「**伺服器網址**」欄位中，輸入認證中心佈署所在的 SCEP 伺服器的網址。
   網址可以包含 IP 位址或完整的網域名稱 (FQDN)。例如：http://10.10.10.10/certserver/companyscep。
7. 在「**名稱**」欄位中，輸入佈署在 SCEP 伺服器上的認證中心的名稱。
8. 在「**主題**」欄位中，輸入具有 X.500 憑證中包含的 iOS MDM 裝置使用者內容的字串。
   內容可以包含國家/地區 (C)、組織 (O) 和通用使用者名稱 (CN) 的詳細資訊。範例：/C=RU/O=MyCompany/CN=User/。您也可以使用 RFC 5280 中指定的其他內容。
9. 在**使用者可選名稱類型**下拉清單中，選擇 SCEP 伺服器的主題的備用名稱的類型：
   - **否** – 不使用備用名稱識別。
   - **RFC 822 名稱** – 使用電子郵件信箱識別。必須根據 RFC 822 指定電子郵件信箱。
   - **DNS 名稱** – 使用網域名稱識別。
   - **URI** – 使用 IP 位址或 FQDN 格式位址識別。

   您可以使用主題的備用名稱識別 iOS MDM 行動裝置的使用者。
10. 在「**使用者可選名稱**」欄位中，輸入 X.500 憑證的主題備用名稱。使用者可選名稱的值取決於主題類型：使用者電子郵件信箱、網域或網址。
11. 在「**NT 使用者名稱**」欄位中，輸入 Windows NT 網路上的 iOS MDM 行動裝置使用者的 DNS 名稱。
    NT 使用者名稱包含在傳送至 SCEP 伺服器的憑證請求中。
12. 在「**SCEP 伺服器上輪詢嘗試次數**」欄位中，指定輪詢 SCEP 伺服器以獲取簽章憑證的最大嘗試次數。
13. 在「**嘗試頻率（秒）**」欄位中，指定輪詢 SCEP 伺服器以獲取簽章憑證的嘗試之間的時間間隔（單位：秒）。
14. 在「**註冊申請**」欄位中，輸入預發佈的註冊金鑰。
    在進行憑證簽章之前，SCEP 伺服器請求行動裝置使用者提供金鑰。如果該欄位留空，則 SCEP 不會請求提供金鑰。
15. 在「**金鑰大小**」下拉清單中，選擇註冊金鑰的大小（單位：位元）：1024 或 2048 位元。
16. 若要允許使用者使用從 SCEP 伺服器接收的憑證作為簽章憑證，請選擇「**用於簽章**」核取方塊。
17. 若要允許使用者將從 SCEP 伺服器接收的憑證用於資料加密，請選擇「**用於加密**」核取方塊。

禁止將 SCEP 伺服器憑證同時用作資料簽章憑證和資料加密憑證。

18. 在「**憑證指紋**」欄位中，輸入一個用於驗證認證中心回應的真實性的唯一的憑證指紋。您可以將憑證指紋與 SHA-1 或 MD5 雜湊演算法配合使用。您可以手動複製憑證指紋或使用「**從憑證建立**」按鈕選擇憑證。在使用「**從憑證建立**」按鈕建立指紋時，指紋會自動新增到該欄位。

如果行動裝置和認證中心之間的資料交換透過 HTTP 協定進行，則必須指定憑證指紋。

19. 點擊「**確定**」。

新的 SCEP 設定檔顯示在清單中。

20. 點擊「**套用**」按鈕以儲存所作的變更。

這樣，一旦套用該政策，使用者的行動裝置將配置成透過網際網路自動接收來自憑證中心的憑證。

控制

本節包含有關如何在卡巴斯基安全管理中心管理主控台中遠端監控行動裝置的資訊。

設定限制

本節提供有關如何配置行動裝置功能的使用者存取的說明。

執行 Android 版本 10 和更新版本的特別考量事項

Android 10 推出許多針對 API 29 或更新版本的變化和限制。其中有些更改會影響到應用程式某些功能的可用性或功能。這些考量事項僅適用於執行 Android 10 或更新版本的裝置。

啟用、停用和配置 Wi-Fi 的能力

- Wi-Fi 網路可以在卡巴斯基安全管理中心的管理主控台中新增、刪除和配置。將 Wi-Fi 網路新增到政策時，Kaspersky Endpoint Security 會在首次連線到卡巴斯基安全管理中心時收到該網路組態。
- 當裝置偵測到透過卡巴斯基安全管理中心配置的網路時，Kaspersky Endpoint Security 會提示使用者連線到該網路。如果使用者選擇連線到網路，則會自動套用透過卡巴斯基安全管理中心配置的所有設定。當裝置在範圍內時，就會自動連線到該網路，而不會向使用者顯示進一步通知。
- 如果使用者的裝置已連線到另一個 Wi-Fi 網路，則使用者有時可能不會收到核准加入網路的提示。在這種情況下，使用者必須先關閉 Wi-Fi，之後再開啟 Wi-Fi 以收到建議。
- 當 Kaspersky Endpoint Security 建議使用者連線到 Wi-Fi 網路，但使用者拒絕連線時，應用程式改變 Wi-Fi 狀態的權限將遭撤銷。然後，Kaspersky Endpoint Security 就無法建議使用者連線到 Wi-Fi 網路，直到使用者再次透過 **"設定" → "應用程式和通知" → "特殊應用程式存取" → "Wi-Fi 控制"→ "Kaspersky Endpoint Security"** 來授予該權限。
- 僅開放式網路和使用 WPA2-PSK 加密的網路受到支援。不支援 WEP 和 WPA 加密。

- 如果變更應用程式之前建議的網路密碼，則使用者必須手動從已知網路清單中刪除該網路。之後裝置就能收到 Kaspersky Endpoint Security 的網路建議並進行連線。
- 當裝置作業系統從 Android 9 或更舊版本更新到 Android 10 或更新版本，和/或更新執行 Android 10 或更舊版本的裝置上安裝的 Kaspersky Endpoint Security 時，之前透過卡巴斯基安全管理中心新增的網路，無法透過卡巴斯基安全管理中心政策加以修改或刪除。不過，使用者可以在裝置設定中手動修改或刪除此類網路。
- 在執行 Android 10 的裝置上，當使用者試圖手動連線到受保護的建議網路時，系統會提示使用者輸入密碼。自動連線不需要輸入密碼。如果使用者的裝置連線到其他 Wi-Fi 網路，使用者必須先中斷該網路的連線，才能自動連線到其中一個建議的網路。
- 在執行 Android 11 的裝置上，使用者可以手動連線到應用程式建議的受保護網路，而無需輸入密碼。
- 將 Kaspersky Endpoint Security 從裝置中移除時，應用程式之前建議的網路就會遭到忽略。
- 不支援禁用的 Wi-Fi 網路。

攝影鏡頭存取權限

- 在執行 Android 10 的裝置上，無法完全禁止使用攝影鏡頭。針對工作設定檔禁用攝影鏡頭的功能仍可使用。
- 如果其他應用程式試圖存取裝置的設以鏡頭，系統會阻止該應用程式，並通知使用者此問題的相關資訊。但是，背景模式執行期間使用攝影鏡頭的應用程式則不會遭到系統封鎖。
- 當外接攝影鏡頭與裝置中斷連接時，在某些情況下可能會顯示攝影鏡頭無法使用的通知。

管理螢幕解鎖方法

- Kaspersky Endpoint Security 現在會將密碼強度要求解析為其中一個系統值：中度或高度。
  - 如果要求的密碼長度是 1 到 4 個符號，那麼應用程式會提示使用者設定中等強度的密碼。密碼必須是數字（PIN）且沒有重複或有順序（如 1234）的序列或英數字母。PIN 或密碼的長度必須至少有 4 個字元。
  - 如果要求的密碼長度為 5 個以上的符號，那麼應用程式會提示使用者設定高強度密碼。密碼必須是數字（PIN），沒有重複或有順序的序列或英數字母（password）。 PIN 必須至少有 8 位數，密碼長度必須至少有 6個字元。
- 螢幕指紋解鎖的使用僅可針對工作設定檔來加以管理。

配置 Android 裝置的限制

為確保 Android 裝置安全，請在裝置上配置 Wi-Fi、攝影鏡頭和藍芽的使用設定。

預設情況下，使用者可以在裝置上無限制地使用 Wi-Fi、攝影鏡頭和藍芽。

若要在裝置上配置 Wi-Fi、攝影鏡頭和藍芽的使用限制，請執行以下步驟：

1. 在主控台樹狀目錄的「**受管裝置**」資料夾中，選擇 Android 裝置所屬的管理群組。
2. 在所選群組的工作台中，選擇「**政策**」標籤。
3. 透過按兩下任何資料欄來開啟政策內容視窗。

4. 在政策「**內容**」視窗中選擇「**裝置管理**」區域。

5. 在「**限制**」區域中，配置 Wi-Fi、攝影鏡頭和藍芽的使用：

   - 若要在使用者行動裝置上停用 Wi-Fi 模組，則選擇「**禁止使用 Wi-Fi**」核取方塊。

     在執行 Android 10.0 或更高版本的裝置上，不支援禁止使用 Wi-Fi 網路。

   - 若要在使用者行動裝置上停用攝影鏡頭，則選擇**"禁止使用攝影鏡頭"**方塊。

     在執行 Android 10.0 的裝置上，無法完全禁止使用相機。

     在執行 Android 11 或更高版本的裝置上，必須將 Kaspersky Endpoint Security for Android 設定為可存取功能。Kaspersky Endpoint Security for Android 會提示使用者透過初始配置精靈將該應用程式設定為輔助使用功能。使用者可以略過此步驟或以後在裝置設定中停用此服務。如果是這種情況，您將無法限制相機的使用。

   - 若要在使用者行動裝置上停用藍芽，則選擇**"禁止使用藍芽"**方塊。

     在 Android 12 或更高版本，只有在裝置使用者授予**鄰近藍牙裝置**權限時，才能停用藍牙。使用者可以在初始設定精靈期間或之後授予此權限。

6. 點擊「**套用**」按鈕以儲存所作的變更。

與卡巴斯基安全管理中心的下個裝置同步之後可配置行動裝置設定。

配置 iOS MDM 裝置功能限制

為確保符合企業安全需求，請配置 iOS MDM 裝置執行限制。

若要配置 iOS MDM 裝置功能限制，請執行以下操作：

1. 在主控台樹狀目錄的「**受管裝置**」資料夾中，選擇 iOS MDM 裝置所屬的管理群組。
2. 在所選群組的工作台中，選擇「**政策**」標籤。
3. 透過點擊開啟政策內容視窗。
4. 在政策「**內容**」視窗中選擇「**功能限制**」區域。
5. 在「**功能限制設定**」區域中，選中「**將設定套用於裝置**」核取方塊。
6. 配置 iOS MDM 裝置功能限制。
7. 點擊「**套用**」按鈕以儲存所作的變更。
8. 選擇**應用程式限制**區域。
9. 在「**應用程式限制設定**」區域中選擇「**將設定套用於裝置**」核取方塊。

10. 在 iOS MDM 裝置上設定應用程式限制。
11. 點擊「**套用**」按鈕以儲存所作的變更。
12. 選擇**對媒體內容的限制**區域。
13. 在「**媒體內容限制設定**」區域中選擇「**將設定套用於裝置**」核取方塊。
14. 在 iOS MDM 裝置上配置對媒體內容的限制。
15. 點擊「**套用**」按鈕以儲存所作的變更。

這樣，一旦套用該政策，將在使用者的行動裝置上配置對功能、應用程式和媒體內容的限制。

配置 EAS 裝置功能限制

配置裝置功能限制，防護 EAS 裝置。

預設情況下，使用者可以無限制地使用 EAS 裝置的功能。

若要配置 EAS 裝置功能限制，請執行以下操作：

1. 在主控台樹狀目錄的「**受管裝置**」資料夾中，選擇 EAS 裝置所屬的管理群組。
2. 在所選群組的工作台中，選擇「**政策**」標籤。
3. 透過點擊開啟政策內容視窗。
4. 在政策「內容」視窗中選擇「**功能限制**」區域。
5. 在「**功能限制設定**」區域，啟用或停用 EAS 裝置功能：
   - 若要允許將儲存卡和其他卸除式磁碟機連線至本裝置，請選擇「**允許卸除式磁碟**」核取方塊。
   - 若要允許使用攝影鏡頭，請選擇「**允許使用攝影鏡頭**」核取方塊。
   - 若要允許 Wi-Fi 連線，請選擇「**允許使用 Wi-Fi**」核取方塊。
   - 若要允許使用紅外線連線連接埠，請選擇「**允許紅外線連線**」核取方塊。
   - 若要允許將裝置用作建立無線網路的 Wi-Fi 存取點，請選擇「**允許裝置使用 Wi-Fi 存取點**」核取方塊。
   - 若要允許裝置連線遠端桌面，請選擇「**允許遠端桌面連線**」核取方塊。
   - 若要允許使用者在裝置上使用 Desktop ActiveSync 用戶端，請選擇「**允許桌面同步**」核取方塊。
   - 在「**使用藍芽**」下拉清單中，在 EAS 裝置上啟用或停用 Bluetooth：
     - **允許**。允許在行動裝置上使用藍芽。
     - **在使用免提時**。在行動裝置連接有無線耳機時啟用 Bluetooth。
     - **拒絕**。封鎖在行動裝置上使用藍芽。
6. 點擊「**套用**」按鈕以儲存所作的變更。

與卡巴斯基安全管理中心的下個裝置同步之後可配置行動裝置設定。

設定使用者對網站的存取

本節包含有關如何設定在 Android 和 iOS 裝置上存取網站的說明。

在 Android 裝置上配置網站存取權限

您可以使用 Web 防護來配置 Android 裝置使用者對網站的存取權限（請參閱下圖）。Web 防護支援會依卡巴斯基安全網路雲端服務中所定義類別篩選網站。篩選允許您限制使用者對某些網站或某些類別網站的存取（例如「賭博、彩票、抽獎」或「網際網路通訊」類別中的網站）。Web 防護也會在網際網路上防護使用者的個人資料。

您必須將 Kaspersky Endpoint Security for Android 設定為輔助使用功能。Kaspersky Endpoint Security for Android 會提示使用者透過初始配置精靈將該應用程式設定為輔助使用功能。使用者可以略過此步驟或以後在裝置設定中停用此服務。在這種情況下不會執行 Web 防護。

Android 裝置上的 Web 防護僅在 Google Chrome 瀏覽器（包括自訂標籤功能）、Huawei Browser 和 Samsung Internet Browser 中可用。如果使用工作設定檔且只針對工作設定檔啟用 Web 防護，則 Samsung Internet Browser 的 Web 防護不會封鎖行動裝置上的網站。

預設已啟用 Web 防護：封鎖使用者存取**釣魚**和**惡意軟體**類別中的網站。

若要配置裝置使用者存取網站的設定，請執行以下步驟：

1. 在主控台樹狀目錄的「**受管裝置**」資料夾中，選擇 Android 裝置所屬的管理群組。
2. 在所選群組的工作台中，選擇「**政策**」標籤。
3. 透過按兩下任何資料欄來開啟政策內容視窗。
4. 在政策**內容**視窗中選擇 **Web 防護**。
5. 選取**啟用 Web 防護**核取方塊。
6. 若要使用 Web 防護，您或裝置使用者必須閱讀並同意利用 Web 防護進行資料處理的聲明（Web 防護聲明）：
   a. 按一下連結 **Web 防護聲明**。
      這會開啟**利用 Web 防護進行資料處理的聲明**視窗。若要同意 Web 防護聲明，您必須閱讀並同意隱私權政策。
   b. 按一下隱私權政策連結。閱讀並同意隱私權政策。
      若您不同意隱私權政策，行動裝置使用者可在初始設定精靈或應用程式中同意隱私權政策（ → **關於** → **條款和條件** → **隱私權政策**）。
   c. 選擇 Web 防護聲明同意模式：
      - **我已閱讀並同意 Web 防護聲明**

- **向裝置使用者要求同意 Web 防護聲明**
- **我不同意 Web 防護聲明**

若您選擇**我不同意 Web 防護聲明**，Web 防護就不會封鎖行動裝置上的網站。行動裝置使用者無法在 Kaspersky Endpoint Security 中啟用 Web 防護。

7. 如果您希望應用程式根據網站內容限制使用者對網站的存取，請執行以下操作：
   a. 在 **Web 防護**區段中，在下拉清單中選擇**禁止所選類別的網站**。
   b. 選擇應用程式將封鎖存取的網站類別旁邊的核取方塊，建立遭封鎖類別的網站清單。
8. 如果您希望應用程式僅允許使用者存取管理員指定的網站，請執行以下操作：
   a. 在 **Web 防護**區段中，在下拉清單中選擇**僅允許列出的網站**。
   b. 新增應用程式將不會封鎖存取的網站位址，建立網站清單。Kaspersky Endpoint Security for Android 僅支援正規運算式。輸入允許的網站的位址時，請使用以下範本：
      - `http:\/\/www\.example\.com.*` – 網站的所有子頁面都被允許（例如，`http://www.example.com/about`）。
      - `https:\/\/.*example\.com` – 網站的所有子網域頁面都被允許（例如，`https://pictures.example.com`）。

      您也可以使用運算式`https?` 來選擇 HTTP 和 HTTPS 協定。對於更多正規運算式的詳情，請參考 Oracle 技術支援網站。
9. 如果您希望應用程式封鎖使用者存取所有網站，請在 **Web 防護**區段中，在下拉清單選擇**封鎖所有網站**。
10. 若要去除根據內容對使用者存取網站的限制，請取消選取**啟用 Web 防護**方塊。
11. 點擊「**套用**」按鈕以儲存所作的變更。

與卡巴斯基安全管理中心的下個裝置同步之後可配置行動裝置設定。

在 iOS MDM 裝置上設定網站存取

配置「Web 防護」設定來控制 iOS MDM 裝置使用者的網站存取權限。「Web 防護」會根據允許與封鎖的網站清單來控制使用者存取網站的權限。透過 Web 防護，您還可以在 Safari 的書簽面板上新增網站書簽。

依預設，存取網站的權限不會受到限制。

「Web 防護」設定僅可針對監控裝置配置。

若要在使用者的 iOS MDM 裝置上配置網站存取，請執行以下操作：

1. 在主控台樹狀目錄的「**受管裝置**」資料夾中，選擇 iOS MDM 裝置所屬的管理群組。
2. 在所選群組的工作台中，選擇「**政策**」標籤。
3. 透過點擊開啟政策內容視窗。

4. 在政策「**內容**」視窗中選擇「**Web 防護**」區域。

5. 在「**Web 防護設定**」區域中，選中「**將設定套用於裝置**」核取方塊。

6. 若要封鎖存取封鎖的網站，允許存取允許的網站，請執行以下操作：

   a. 在「**Web 篩選器模式**」下拉清單中，選擇「**限制色情**」模式。

   b. 在「**允許的網站**」區域，建立允許的網站清單。

   網站應以「`http://`」或「`https://`」開頭。Kaspersky Device Management for iOS 允許存取該網域中的所有網站。例如，如果已將 http://www.example.com 新增到允許的網站清單中，則允許存取 http://pictures.example.com 和 http://example.com/movies。如果允許存取的網站清單為空，應用程式將允許存取除被攔截的網站清單中包含的網站以外的所有網站。

   c. 在「**禁止的網站**」區域中，建立封鎖的網站清單。

   網站應以「`http://`」或「`https://`」開頭。Kaspersky Device Management for iOS 封鎖存取該網域中的所有網站。

7. 若要封鎖存取除該標籤清單上的允許的網站以外的所有網站，請執行以下步驟：

   a. 在「**Web 篩選器模式**」下拉清單中，選擇「**僅允許加入書籤的網站**」模式。

   b. 在「**書籤**」區域，建立允許的網站的書籤清單。

   網站應以「`http://`」或「`https://`」開頭。Kaspersky Device Management for iOS 允許存取該網域中的所有網站。如果書籤清單為空，則應用程式允許存取所有網站。在使用者的行動裝置中，Kaspersky Device Management for iOS 在 Safari 的書籤標籤上新增書籤清單中的網站。

8. 點擊「**套用**」按鈕以儲存所作的變更。

這樣，一旦套用該政策，將根據選擇的模式和建立的清單在使用者的行動裝置上配置 Web 防護。

使用公司安全性政策控制 Android 裝置的合規性

您可以控制 Android 裝置以符合公司的安全要求。企業安全需求規範使用者可以如何使用裝置。例如，必須在裝置上啟用即時防護，病毒資料庫必須是最新的，並且裝置密碼必須足夠強。合規性控制基於規則清單。合規性規則包括以下組成部分：

- 裝置檢查條件（例如，裝置上不存在被封鎖的應用程式）。
- 分配給使用者以解決不合規問題的時間段（例如，24 小時）。
- 如果使用者未在規定的時間段內解決不合規問題，將對裝置採取的措施（例如鎖定裝置）。

> 在 Android 12 或更高版本上，若裝置處於省電模式，應用程式執行此任務的時間可能會晚於指定時間。

如果使用者不修復指定時間內的不相容，則以下操作可用：

- **封鎖除系統應用程式之外的所有應用程式**。封鎖使用者行動裝置上的所有應用程式（系統應用程式除外）啟動。
- **鎖定裝置**。行動裝置將被鎖定。要獲取對資料的存取，您必須解鎖裝置。如果裝置解鎖後，解鎖裝置的原因未變更，裝置將在指定時間段後再次被鎖定。

- **抹除企業資料**。抹除容器中的資料、公司電子郵件帳戶、用於連線至公司 Wi-Fi 網路和 VPN 的設定、接入點名稱 (APN)、Android 工作設定檔、KNOX 容器和 KNOX License Manager 金鑰。

- **還原出廠設定**。所有資料都將從行動裝置中刪除，設定將回溯至其出廠值。該操作完成後，裝置將不再是受管理裝置。要連線裝置到卡巴斯基安全管理中心，您必須重新安裝 Kaspersky Endpoint Security for Android。

若要建立掃描規則，檢查裝置是否符合合規性，請執行以下操作：

1. 在主控台樹狀目錄的「**受管裝置**」資料夾中，選擇 Android 裝置所屬的管理群組。

2. 在所選群組的工作台中，選擇「**政策**」標籤。

3. 透過按兩下任何資料欄來開啟政策內容視窗。

4. 在政策「**內容**」視窗中選擇「**合規性控制**」區域。

5. 若要接收關於違反政策的裝置的通知，則在「**不合規通知**」區域中選擇「**通知管理員**」核取方塊。

   如果裝置不符政策規定，Kaspersky Endpoint Security for Android 會在裝置與管理伺服器同步時，在事件記錄中寫入「**發現違規：<name of the criterion checked>**」項目。可以在「管理伺服器」內容的「**事件**」標籤上或在應用程式的本機內容中檢視事件記錄。

6. 若要通知裝置使用者其裝置不符合政策，則可以在「**不合規通知**」區域中選擇「**通知使用者**」核取方塊。

   如果在裝置與管理伺服器同步期間發現裝置違反政策，Kaspersky Endpoint Security for Android 將在「**狀態**」區域中通知使用者。

7. 在「**合規性規則**」區域中，編撰一個用於檢查裝置是否符合政策的規則清單。執行以下步驟：

   a. 點擊「**新增**」。

      「掃描規則精靈」將啟動。

   b. 按照「掃描規則精靈」的描述進行操作。

      精靈完成時，「**合規性規則**」區域中將顯示新規則。

8. 若要臨時停用建立的掃描規則，可使用選定的規則旁邊的轉換開關。

9. 點擊「**套用**」按鈕以儲存所作的變更。

與卡巴斯基安全管理中心的下次裝置同步之後可配置行動裝置設定。如果使用者裝置不符合規則，您在掃描規則中指定的限制將套用至該裝置。

應用程式啟動控制

本節提供有關如何在行動裝置上配置應用程式的使用者存取的說明。

Android 裝置上的應用程式啟動控制

若要確保使用者的行動裝置安全，您必須在裝置上配置應用程式啟動設定（請參閱下圖）。

您可以在安裝了被封鎖的應用或所需應用未安裝的裝置上施加對使用者活動的限制（例如，鎖定裝置）。您可以使用合規性控制元件施加限制。為此，在掃描規則設定中，您必須選擇**已安裝禁止的應用程式**、**已安裝禁止類別中的應用程式**或**並非已安裝所有所需的應用程式**標準。

必須將 Kaspersky Endpoint Security for Android 設定為可存取功能以確保應用程式控制能正常執行。Kaspersky Endpoint Security for Android 會提示使用者透過初始配置精靈將該應用程式設定為輔助使用功能。使用者可以略過此步驟或以後在裝置設定中停用此服務。在這種情況下不會執行應用程式控制。

若要在行動裝置上配置應用程式啟動設定，請執行以下操作：

1. 在主控台樹狀目錄的「**受管裝置**」資料夾中，選擇 Android 裝置所屬的管理群組。
2. 在所選群組的工作台中，選擇「**政策**」標籤。
3. 透過按兩下任何資料欄來開啟政策內容視窗。
4. 在政策「**內容**」視窗中選擇「**應用程式控制**」區域。
5. 在**執行模式**區段中，選擇使用者行動裝置上的應用程式啟動的模式：
   - 若要允許使用者啟動除類別和應用程式清單中指定為被封鎖的應用程式外的所有應用程式，請選擇**被封鎖的應用程式**模式。
   - 若要允許使用者只能啟動類別和應用程式清單中指定為允許的應用程式、建議的應用程式或所需的應用程式，請選擇**允許的應用程式**模式。
6. 如果您要 Kaspersky Endpoint Security for Android 在禁止的應用程式上傳送資料到事件記錄而不封鎖它們，選擇**不封鎖禁止的應用程式，僅寫入事件記錄**核取方塊。

   在使用者行動裝置與管理伺服器同步期間，Kaspersky Endpoint Security for Android 將在事件記錄中建立**已安裝禁止的應用程式**項目。可以在「管理伺服器」內容的「**事件**」標籤上或在應用程式的本機內容中檢視事件記錄。
7. 如果您希望 Kaspersky Endpoint Security for Android 封鎖使用者行動裝置上的系統應用程式（例如行事曆，攝影鏡頭和設定）在**允許的應用程式**模式下啟動，請選擇**封鎖系統應用程式**方塊。

   Kaspersky 專家建議不要封鎖系統應用程式，因為這會導致裝置操作故障。
8. 建立類別和應用程式清單以配置應用程式的啟動。

   如需應用程式類別的詳細資訊，請參閱附錄。

   如需屬於每個類別的應用程式的清單，請造訪 Kaspersky 網站。
9. 點擊「**套用**」按鈕以儲存所作的變更。

與卡巴斯基安全管理中心的下個裝置同步之後可配置行動裝置設定。

為應用程式配置 EAS 裝置限制

為防護 EAS 裝置安全，請配置應用程式活動限制（網頁瀏覽器，未簽章的應用程式）。

預設情況下，使用者可以在 EAS 裝置上無限制地使用應用程式。

若要配置 EAS 裝置上的應用程式活動限制，請執行以下操作：

1. 在主控台樹狀目錄的「**受管裝置**」資料夾中，選擇 EAS 裝置所屬的管理群組。

2. 在所選群組的工作台中，選擇「**政策**」標籤。

3. 透過點擊開啟政策內容視窗。

4. 在政策「內容」視窗中選擇「**應用程式限制**」區域。

5. 在「**應用程式限制設定**」區域中，配置應用程式活動限制：

   - 若要允許使用者使用網頁瀏覽器，請選擇「**允許使用瀏覽器**」核取方塊。
   - 若要允許使用者建立個人電子郵件帳戶（POP3 或 IMAP4），請選擇「**允許個人郵件**」核取方塊。
   - 若要允許使用者啟動未使用身分驗證憑證簽章的應用程式，請選擇「**允許未簽章的應用程式**」核取方塊。
   - 若要允許使用者安裝未使用身分驗證憑證簽章的應用程式，請選擇「**允許未簽章的安裝套件**」核取方塊。

6. 點擊「**套用**」按鈕以儲存所作的變更。

與卡巴斯基安全管理中心的下個裝置同步之後可配置行動裝置設定。

Android 裝置上的軟體清單

您可以清點已連線到卡巴斯基安全管理中心的 Android 裝置上的應用程式。Kaspersky Endpoint Security for Android 會接收有關行動裝置上安裝的所有應用程式的資訊。在清點期間獲取的資訊顯示在**活動**區域的裝置內容中。您可以檢視有關每個已安裝的應用程式的詳細資訊，包括其版本和發佈者。

啟用軟體清單：

1. 在主控台樹狀目錄的「**受管裝置**」資料夾中，選擇 Android 裝置所屬的管理群組。

2. 在所選群組的工作台中，選擇「**政策**」標籤。

3. 透過按兩下任何資料欄來開啟政策內容視窗。

4. 在政策「**內容**」視窗中選擇「**應用程式控制**」區域。

5. 在**軟體清單**區域，選擇**在已安裝應用上傳送資料**核取方塊。

6. 點擊「**套用**」按鈕以儲存所作的變更。

與卡巴斯基安全管理中心的下次裝置同步之後可配置行動裝置設定。Kaspersky Endpoint Security for Android 在每次應用被安裝或從裝置移除時傳送資料到事件記錄。

在卡巴斯基安全管理中心中設定 Android 裝置的顯示

為了便於使用行動裝置清單進行操作，您應該配置在卡巴斯基安全管理中心顯示裝置的相應設定。預設情況下，行動裝置清單顯示在「**其他**」→「**行動裝置管理**」→「**行動裝置**」主控台樹狀目錄中。裝置資訊將自動更新。您也可以點擊右上角的「**更新**」按鈕，手動更新行動裝置清單。

將裝置連線至卡巴斯基安全管理中心後，會自動將裝置新增到行動裝置清單中。行動裝置清單可能含有裝置的詳細資，如：型號、作業系統、IP 位址及其他等。

您可以設定裝置名稱格式並選擇裝置狀態。裝置狀態會告知您 Kaspersky Endpoint Security for Android 的元件在使用者行動裝置上的執行情況。

Kaspersky Endpoint Security for Android 元件可能因以下原因而無法執行：

- 使用者在裝置設定中停用了元件。
- 使用者未向應用程式授予元件執行所需的權限（例如，相應的竊盜防護命令無權確定裝置位置）。

若要顯示裝置狀態，您必須在管理群組內容中啟用「**由應用程式確定**」條件（「**內容**」→「**裝置狀態**」→「**在以下情況下將裝置狀態設定為緊急**」以及「**在以下情況下將裝置狀態設定為警告**」）。在管理群組內容中，您還可以選擇形成行動裝置狀態的其他條件。

若要在卡巴斯基安全管理中心中設定 Android 裝置的顯示，請執行以下操作：

1. 在主控台樹狀目錄的「**受管裝置**」資料夾中，選擇 Android 裝置所屬的管理群組。
2. 在所選群組的工作台中，選擇「**政策**」標籤。
3. 透過按兩下任何資料欄來開啟政策內容視窗。
4. 在政策「**內容**」視窗中選擇「**裝置資訊**」區域。
5. 在**卡巴斯基安全管理中心裝置名稱**區域中，選擇管理主控台中的裝置名稱要使用的裝置名稱格式：
   - 裝置型號 [電子郵件，裝置 ID]
   - 裝置型號 [電子郵件（如果有）或裝置 ID]

   *裝置 ID*是 Kaspersky Endpoint Security for Android 根據從裝置接收的資料產生的唯一 ID。對於執行在 Android 10 或更新版本的行動裝置，Kaspersky Endpoint Security for Android 使用 SSAID (Android ID) 或從裝置接收的其他資料的校驗碼。對於早期版本的 Android，應用使用 IMEI。
6. 將「鎖定」內容設定在鎖定位置（ ）。
7. 在「**卡巴斯基安全管理中心中的裝置狀態**」區域，如果某個 Kaspersky Endpoint Security for Android 元件未執行，則選擇相應的裝置狀態：（**緊急**）、（**警告**）或（**正常**）。

   在行動裝置清單中，裝置狀態將根據所選狀態而變更。
8. 將「鎖定」內容設定在鎖定位置。
9. 點擊「**套用**」按鈕以儲存所作的變更。

與卡巴斯基安全管理中心的下個裝置同步之後可配置行動裝置設定。

管理

本節包含有關如何在卡巴斯基安全管理中心管理主控台中遠端管理行動裝置設定的資訊。

設定與 Wi-Fi 網路的連線

本節提供有關如何在 Android 和 iOS MDM 裝置上配置自動連線到公司 Wi-Fi 網路的說明。

將 Android 裝置連線至 Wi-Fi 網路

若要將行動裝置連線至 Wi-Fi 網路，請執行以下操作：

1. 在主控台樹狀目錄的「**受管裝置**」資料夾中，選擇 Android 裝置所屬的管理群組。
2. 在所選群組的工作台中，選擇「**政策**」標籤。
3. 透過按兩下任何資料欄來開啟政策內容視窗。
4. 在政策「**內容**」視窗中選擇「**Wi-Fi**」區域。
5. 在「**Wi-Fi 網路**」區域中點擊「**新增**」。

   這將開啟「**Wi-Fi 網路**」視窗。
6. 在「**服務集識別字 (SSID)**」欄位中，輸入包含存取點 (SSID) 的 Wi-Fi 網路的名稱。
7. 在「**網路防護**」區域中，選擇 Wi-Fi 網路安全類型（受 WEP 或 WPA/WPA2 PSK 協議防護的公用網或安全網路）。
8. 如果您在上一步中選擇了安全網路，則在「**密碼**」欄位中設定網路存取密碼。
9. 如有必要，在「**代理伺服器位址和連接埠**」欄位中，輸入代理伺服器的 IP 位址或 DNS 名稱（網址）和埠號。

   在執行 Android 版本 8.0 或更新版本的裝置上，Wi-Fi 代理伺服器設定無法由政策重定義。然而，您可以在行動裝置上手動為 Wi-Fi 網路配置代理伺服器設定。

   如果您正使用代理伺服器連線到 Wi-Fi 網路，您可以使用政策配置網路連線設定。在執行 Android 8.0 或更新版本的裝置上，您必須手動配置代理伺服器設定。在執行 Android 8.0 或更新版本的裝置上，您無法使用政策變更 Wi-Fi 網路連線設定，除了網路存取密碼。

   如果您不使用代理伺服器連線到 Wi-Fi 網路，則沒有使用政策管理 Wi-Fi 網路連線的限制。
10. 在「**不使用代理伺服器位址**」欄位中，生成不使用代理伺服器可存取的網址清單。

    例如，您可以輸入位址 `example.com`。在這種情形下，`pictures.example.com`、`example.com/movies` 等位址不會使用該代理伺服器。協定（例如：`http://`）可以省略。

    在執行 Android 版本 8.0 或更高版本的裝置上，網址的代理伺服器排除不起作用。
11. 點擊「**確定**」。

    「**Wi-Fi 網路**」清單中將顯示新增的 Wi-Fi 網路。

    您可以使用清單頂端的「**編輯**」和「**刪除**」按鈕，來編輯或刪除網路清單中的 Wi-Fi 網路。
12. 點擊「**套用**」按鈕以儲存所作的變更。

與卡巴斯基安全管理中心的下次裝置同步之後可配置行動裝置設定。在行動裝置上套用該政策後，使用者無需指定網路設定，即可連線到已新增的 Wi-Fi 網路。

在執行 Android 10.0 或更新版本的裝置上，如果使用者拒絕連線到建議的 Wi-Fi 網路，應用程式改變 Wi-Fi 狀態的權限將遭撤銷。使用者必須手動授予此權限。

將 iOS MDM 裝置連線至 Wi-Fi 網路

用於使 iOS MDM 裝置自動連線至可用的 Wi-Fi 網路，在連接期間防護資料，您應配置連接設定。

若要配置 iOS MDM 裝置與 Wi-Fi 網路的連線，請執行以下操作：

1. 在主控台樹狀目錄的「**受管裝置**」資料夾中，選擇 iOS MDM 裝置所屬的管理群組。
2. 在所選群組的工作台中，選擇「**政策**」標籤。
3. 透過點擊開啟政策內容視窗。
4. 在政策「**內容**」視窗中選擇「**Wi-Fi**」區域。
5. 按一下「**Wi-Fi 網路**」區域中的「**新增**」按鈕。
   這將開啟「**Wi-Fi 網路**」視窗。
6. 在「**服務集識別字 (SSID)**」欄位中，輸入包含存取點 (SSID) 的 Wi-Fi 網路的名稱。
7. 如果您希望 iOS MDM 裝置自動連線至 Wi-Fi 網路，請選擇「**自動連線**」核取方塊。
8. 若要使 iOS MDM 裝置無法連線到需要初步驗證的 Wi-Fi 網路（受控網路），請選中「**停用強制網路偵測**」核取方塊。
   若要使用受管網路，您必須訂購，接受協議或付款。例如，受管網路可能佈署在咖啡館和酒店。
9. 如果您希望在 iOS MDM 裝置上的可用網路清單中隱藏 Wi-Fi 網路，請選擇「**隱藏的網路**」核取方塊。
   在這種情況下，若要連線到網路，使用者需要手動輸入在行動裝置上的 Wi-Fi 路由器的設定中指定的服務集識別字 (SSID)。
10. 在「**網路防護**」下拉清單中選擇 Wi-Fi 網路連線的防護類型：
    - **停用**。無需進行使用者認證。
    - **WEP**。使用無線加密協定 (WEP) 防護網路。
    - **WPA / WPA2（個人）**。使用 WPA/WPA2 協定（Wi-Fi 安全存取）防護網路。
    - **WPA2（個人）**。使用 WPA2 協定（Wi-Fi 安全存取 2.0）防護網路。執行 iOS 版本 8 或更高版本的裝置提供了 WPA2 防護。Apple TV 裝置不支援 WPA2。
    - **任何（個人）**。根據 Wi-Fi 路由器的類型，使用 WEP、 WPA 或 WPA2 加密協定防護網路。使用對於每個使用者唯一的加密金鑰進行身分驗證。
    - **WEP（動態）**。使用 WEP 協定和動態金鑰防護網路。

- **WPA/WPA2（企業）**。使用 WPA/WPA2 加密協定與 802.1X 協定防護網路。
- **WPA2（企業）**。使用 WPA2 加密協定和所有使用者共用的一個金鑰（802.1X）防護網路。執行 iOS 版本 8 或更高版本的裝置提供了 WPA2 防護。Apple TV 裝置不支援 WPA2。
- **任何（企業）**。根據 Wi-Fi 路由器類型使用 WEP 或 WPA/WPA2 協定防護網路。使用所有使用者共用的一個加密金鑰進行身分驗證。

若您在「**網路防護**」清單中選擇了「**WEP（動態）**」、「**WPA/WPA2（企業）**」、「**WPA2（企業）**」或「**任何（企業）**」，您在「**協議**」區域中便能選擇使用者在 Wi-Fi 網路上驗證身分所使用的 EAP 協議（可延伸的驗證通訊協定）類型。

在「**可信憑證**」區域，您還可以建立可信憑證清單，用於受信任的伺服器上的 iOS MDM 裝置使用者身分驗證。

11. 配置在 iOS MDM 裝置連線至 Wi-Fi 網路時用於使用者身分驗證的帳戶的設定：

    a. 在「**身分驗證**」區域中，點擊「**設定**」按鈕。

    「**身分驗證**」視窗將開啟。

    b. 在「**使用者名稱**」欄位中，輸入在連線至 Wi-Fi 網路時用於使用者身分驗證的帳戶名稱。

    c. 若要允許使用者在每次連線 Wi-Fi 網路時手動輸入密碼，請選擇「**每次連線時提示輸入密碼**」核取方塊。

    d. 在「**密碼**」欄位中，輸入用於 Wi-Fi 網路上身分驗證的帳戶的密碼。

    e. 在「**身分驗證憑證**」下拉清單中，選擇用於 Wi-Fi 網路上的使用者身分驗證的憑證。如果該清單未包含任何憑證，**您可以在「憑證」區域新增**。

    f. 在「**使用者 ID**」欄位中，輸入在進行身分驗證時的資料傳輸過程中顯示的使用者 ID，而不是真正的使用者名稱。

    使用者 ID 旨在使身分驗證過程更加安全，因為使用者名稱不會公開顯示，而是透過加密的 TLS 通道傳輸。

    g. 點擊「**確定**」。

這樣，將在 iOS MDM 裝置上配置在連線至 Wi-Fi 網路時用於使用者身分驗證的帳戶的設定。

12. 如有必要，配置透過代理伺服器連線 Wi-Fi 網路的設定：

    a. 在「**代理伺服器**」區域中，點擊「**設定**」按鈕。

    b. 在開啟的「**代理伺服器**」視窗中，選擇代理伺服器配置模式並指定連線設定。

    c. 點擊「**確定**」。

這樣，已在 iOS MDM 裝置上配置裝置透過代理伺服器連線 Wi-Fi 網路的設定。

13. 點擊「**確定**」。

新的 Wi-Fi 網路將顯示在清單中。

14. 點擊「**套用**」按鈕以儲存所作的變更。

這樣，一旦套用該政策，將在使用者的 iOS MDM 裝置上配置 Wi-Fi 網路連線。使用者的行動裝置將自動連線至可用的 Wi-Fi 網路。身分驗證技術可確保 Wi-Fi 網路連線期間資料的安全。

設定電子郵件

本節包含有關在行動裝置上配置信箱的資訊。

在 iOS MDM 裝置上配置信箱

要允許 iOS MDM 裝置使用者使用電子郵件，請將該使用者的電子郵件帳號新增到 iOS MDM 裝置上的帳號清單中。

預設情況下，新增的電子郵件帳戶具有以下設定：

- 電子郵件協定 – IMAP。
- 使用者可以在使用者的多個帳戶之間移動電子郵件，並同步帳戶位址。
- 使用者可以透過任何電子郵件用戶端（Mail 除外）使用電子郵件。
- 傳輸郵件時不使用 SSL 連線。

您可以在新增帳戶時編輯指定的設定。

若要新增 iOS MDM 裝置使用者的電子郵件帳戶，請執行以下步驟：

1. 在主控台樹狀目錄的「**受管裝置**」資料夾中，選擇 iOS MDM 裝置所屬的管理群組。
2. 在所選群組的工作台中，選擇「**政策**」標籤。
3. 透過點擊開啟政策內容視窗。
4. 在政策「**內容**」視窗中選擇「**電子郵件**」。
5. 按一下「**電子郵件帳戶**」區域中的「**新增**」按鈕。
   「**電子郵件帳戶**」視窗將開啟。
6. 在「**描述**」欄位中，輸入使用者的電子郵件帳戶的描述。
7. 選擇電子郵件協定：
   - **POP**
   - **IMAP**
8. 如有必要，在「**IMAP 路徑首碼**」欄位中指定 IMAP 路徑首碼。
   IMAP 路徑前置詞必須使用大寫字母輸入（範例：GMAIL 代表 Google Mail）。如果選擇了 IMAP 帳戶協定，則該欄位可用。
9. 在「**郵件中顯示的使用者名稱**」欄位中，輸入要顯示在所有待發郵件的「**寄件者:**」欄位中的使用者名稱。
10. 在「**電子郵件信箱**」欄位中，指定 iOS MDM 裝置使用者的電子郵件信箱。
11. 配置電子郵件帳戶的其他設定：

- 若要允許使用者在使用者的多個帳戶之間移動電子郵件，請選擇「**允許在帳戶之間移動郵件**」核取方塊。
- 若要允許在使用者帳戶之間同步位址，請選中「**允許同步最近位址**」核取方塊。
- 若要允許使用者使用郵件投遞服務轉發大尺寸附件，請選中「**允許郵件遞送**」核取方塊。
- 如果您希望使用者僅使用標準的 iOS 郵件用戶端，請選擇「**僅允許使用郵件應用程式**」核取方塊。

12. 配置在郵件應用程式中使用 S/MIME 協定的設定。*S/MIME* 是用於傳送數位簽章加密郵件的協定。
    - 要使用 S/MIME 協定對傳送郵件進行簽章，請選中「**簽章訊息**」核取方塊並選擇用於簽章的憑證。數位簽章確認寄件者的真實性，並指示郵件的內容在傳送給收件者的過程中未被修改。執行 iOS 版本 10.3 或更高版本的裝置支援郵件簽章。
    - 要使用 S/MIME 協定對傳送郵件進行加密，請選中「**預設加密訊息**」核取方塊並選擇用於簽章的憑證（公開金鑰）。執行 iOS 版本 10.3 或更高版本的裝置支援郵件加密。
    - 要使使用者能夠加密單個郵件，請選中「**顯示用於加密訊息的切換按鈕**」核取方塊。若要傳送加密訊息，使用者必須按一下郵件應用程式中「**收件人**」欄位裡的圖示。
13. 在「**接收郵件伺服器**」和「**傳送郵件伺服器**」區域，點擊「**設定**」按鈕以配置伺服器連線設定：
    - **伺服器位址和連接埠**：主機的名稱或接收郵件伺服器和傳送郵件伺服器的 IP 位址以及伺服器埠號。
    - **帳戶名稱**：用於接收和傳送郵件伺服器身分驗證的使用者帳戶的名稱。
    - **身分驗證類型**：接收郵件伺服器和傳送郵件伺服器上使用者電子郵件帳戶身分驗證的類型。
    - **密碼**：用於使用選定的身分驗證方法驗證防護的接收和傳送郵件伺服器的帳戶密碼。
    - **對傳送和內送郵件伺服器使用一個密碼**：對傳送和內送郵件伺服器使用一個密碼進行使用者身分驗證。
    - **使用 SSL 連線**：使用 SSL（安全通訊端層）資料傳輸協定，該協定使用加密和基於憑證的身分驗證防護資料傳輸。
14. 點擊「**確定**」。

    新的電子郵件帳戶顯示在清單中。
15. 點擊「**套用**」按鈕以儲存所作的變更。

這樣，一旦套用該政策，編制的清單中的電子郵件帳戶將新增到使用者的行動裝置上。

在 iOS MDM 裝置上配置 Exchange 信箱

若要使 iOS MDM 裝置使用者可以使用公司電子郵件、行事曆、聯絡人、記事本和工作，請將使用者的 Exchange ActiveSync 帳戶新增到 Microsoft Exchange 伺服器上。

預設情況下，具有以下設定的帳戶將新增到 Microsoft Exchange 伺服器上：

- 每週同步一次電子郵件。
- 使用者可以在使用者的多個帳戶之間移動郵件，並同步帳戶位址。
- 使用者可以透過任何電子郵件用戶端（Mail 除外）使用電子郵件。

- 傳輸郵件時不使用 SSL 連線。

您可以在新增 Exchange ActiveSync 帳戶時編輯指定的設定。

若要新增 iOS MDM 裝置使用者的 Exchange ActiveSync 帳戶，請執行以下操作：

1. 在主控台樹狀目錄的「**受管裝置**」資料夾中，選擇 iOS MDM 裝置所屬的管理群組。
2. 在所選群組的工作台中，選擇「**政策**」標籤。
3. 透過點擊開啟政策內容視窗。
4. 在政策「**內容**」視窗中選擇「**Exchange ActiveSync**」區域。
5. 按一下「**Exchange ActiveSync 帳戶**」區域中的「**新增**」按鈕。
   「**Exchange ActiveSync 帳戶**」視窗在「**一般**」標籤上開啟。
6. 在**帳戶名稱**欄位中，輸入要在 Microsoft Exchange 伺服器上進行身分驗證的帳戶名稱。您可以使用「**可用巨集**」下拉清單中的巨集。
7. 在「**伺服器位址**」欄位中，輸入 Microsoft Exchange 伺服器的網路名稱或 IP 位址。
8. 若要使用 SSL（安全通訊端層）資料傳輸協定防護資料傳輸，請選擇「**使用 SSL 連線**」核取方塊。
9. 在「**網域**」欄位中，輸入 iOS MDM 裝置使用者的網域名稱。您可以使用「**可用巨集**」下拉清單中的巨集。
10. 在「**帳戶使用者名稱**」欄位中輸入 iOS MDM 裝置使用者的名稱。
    如果您將該欄位留空，在 iOS MDM 裝置上套用該政策時，Kaspersky Device Management for iOS 會提示使用者輸入使用者名稱。您可以使用「**可用巨集**」下拉清單中的巨集。
11. 在「**電子郵件信箱**」欄位中，指定 iOS MDM 裝置使用者的電子郵件信箱。您可以使用「**可用巨集**」下拉清單中的巨集。
12. 在「**密碼**」欄位中，輸入用於在 Microsoft Exchange 伺服器上進行身分驗證的 Exchange ActiveSync 帳戶的密碼。
13. 選擇「**其他**」標籤並配置 Exchange ActiveSync 帳戶的其他設定：
    - **郵件同步天數（指定時段內）<time period>**。
    - **身分驗證類型**。
    - **允許在帳戶之間移動郵件**。
    - **允許同步最近位址**。
    - **僅允許使用郵件應用程式**。
14. 配置在郵件應用程式中使用 S/MIME 協定的設定。*S/MIME* 是用於傳送數位簽章加密郵件的協定。
    - 要使用 S/MIME 協定對傳送郵件進行簽章，請選中「**簽章訊息**」核取方塊並選擇用於簽章的憑證。數位簽章確認寄件者的真實性，並指示郵件的內容在傳送給收件者的過程中未被修改。執行 iOS 版本 10.3 或更高版本的裝置支援郵件簽章。
    - 要使用 S/MIME 協定對傳送郵件進行加密，請選中「**預設加密訊息**」核取方塊並選擇用於簽章的憑證（公開金鑰）。執行 iOS 版本 10.3 或更高版本的裝置支援郵件加密。

- 要使使用者能夠加密單個郵件，請選中「**顯示用於加密訊息的切換按鈕**」核取方塊。若要傳送加密訊息，使用者必須按一下郵件應用程式中「**收件人**」欄位裡的圖示。

15. 點擊「**確定**」。

    新的 Exchange ActiveSync 帳戶顯示在清單中。

16. 點擊「**套用**」按鈕以儲存所作的變更。

這樣，一旦套用該政策，編制的清單中的 Exchange ActiveSync 帳戶將新增到使用者的行動裝置上。

在 Android 裝置上設定 Exchange 信箱（僅限 Samsung）

若要在行動裝置上使用公司郵件、聯絡人和行事曆，應配置 Exchange 信箱設定。

Exchange 信箱的配置僅適用於 Samsung 裝置。

若要在行動裝置上配置 Exchange 信箱，請執行以下操作：

1. 在主控台樹狀目錄的「**受管裝置**」資料夾中，選擇 Android 裝置所屬的管理群組。
2. 在所選群組的工作台中，選擇「**政策**」標籤。
3. 透過按兩下任何資料欄來開啟政策內容視窗。
4. 在政策「**內容**」視窗中選擇「**管理 Samsung KNOX**」→「**管理 Samsung 裝置**」區域。
5. 在「**Exchange ActiveSync**」區域中，點擊「**配置**」按鈕。

   「**Exchange 郵件伺服器設定**」視窗將開啟。
6. 在「**伺服器位址**」欄位中，輸入託管郵件伺服器的伺服器的 IP 位址或 DNS 名稱。
7. 在「**網域**」欄位中，輸入公司網路上的行動裝置使用者的網域名稱。
8. 在「**同步間隔**」下拉清單中，選擇行動裝置與 Microsoft Exchange 伺服器所需的同步時間間隔。
9. 若要使用 SSL（安全通訊端層）資料傳輸協議，請選擇「**使用 SSL 連線**」核取方塊。
10. 若要使用數位憑證防護行動裝置與 Microsoft Exchange 伺服器之間的資料傳輸，請選擇「**驗證伺服器憑證**」核取方塊。
11. 點擊「**套用**」按鈕以儲存所作的變更。

與卡巴斯基安全管理中心的下個裝置同步之後可配置行動裝置設定。

管理協力廠商行動 APP

您可以使用容器監控使用者裝置上啟動的行動 APP 的活動。*容器*是一個為行動應用程式準備的特殊封裝，可控制容器化應用程式的活動，以此防護裝置上的使用者個人和公司資料。

在 Kaspersky Security for Mobile Service Pack 3 Maintenance Release 2 中，不再支援為行動應用程式建立容器。但是，在早期版本的應用程式中建立的容器可以新增到 Android 裝置。

您可以按照以下方式之一在使用者裝置上安裝容器化應用程式：

- 向使用者傳送帶有容器化應用程式安裝套件連結的郵件訊息。
- 在政策內容視窗的「**應用程式控制**」區域中將容器化的應用程式指定為必需的或允許的應用程式。行動裝置與卡巴斯基安全管理中心同步之後，容器中的應用程式安裝套件將自動複製到使用者裝置中。

要安裝集裝式應用程式，必須在使用者行動裝置上允許從未知來源安裝應用程式。要在安裝集裝式應用後防護您的裝置和資料，建議禁止從未知源安裝應用。如需不使用 Google Play 安裝應用程式的詳細資訊，請參考 *Android 說明指南*。

設定 Kaspersky Endpoint Security for Android 的通知

如果不希望 Kaspersky Endpoint Security for Android 通知分散行動裝置使用者的注意力，您可以停用某些通知。

Kaspersky Endpoint Security 會使用下列工具顯示裝置防護狀態：

- **防護狀態通知**。此通知會釘選到通知列。您無法移除防護狀態通知。通知會顯示裝置防護狀態（例如，）以及問題數量，如有。您可以輕點裝置防護狀態通知，在應用程式中查看問題清單。
- **應用程式通知**。這些通知會告知裝置使用者關於應用程式的資訊（例如，威脅偵測）。
- **彈出訊息**。彈出訊息會要求裝置使用者採取行動（例如，在偵測到威脅時採取行動）。

所有 Kaspersky Endpoint Security for Android 通知均為預設啟用。

在 Android 13，裝置使用者應在初始設定精靈期間或之後授予權限，才能傳送通知。

Android 裝置使用者可以在通知列的設定中停用來自 Kaspersky Endpoint Security for Android 的所有通知。如果停用通知，使用者不會監控應用程式的執行，並且可能會略過重要資訊（例如，有關裝置與卡巴斯基安全管理中心同步期間發生的故障資訊）。在這種情況下，要瞭解應用程式執行狀態，使用者必須開啟 Kaspersky Endpoint Security for Android。

要設定 Kaspersky Endpoint Security for Android 操作的通知顯示，請執行以下操作：

1. 在主控台樹狀目錄的「**受管裝置**」資料夾中，選擇 Android 裝置所屬的管理群組。
2. 在所選群組的工作台中，選擇「**政策**」標籤。
3. 透過按兩下任何資料欄來開啟政策內容視窗。
4. 在政策「**內容**」視窗中選擇「**其他**」區域。
5. 在**應用程式通知**區域中，按一下**設定**按鈕。

   裝置通知設定視窗將開啟。
6. 選擇要在使用者行動裝置上隱藏的 Kaspersky Endpoint Security for Android 問題，然後按一下**確定**按鈕。

Kaspersky Endpoint Security for Android 將不會在防護狀態通知中及應用程式中的**狀態**區域顯示問題。Kaspersky Endpoint Security for Android 將會繼續顯示防護狀態通知和應用程式通知。

某些 Kaspersky Endpoint Security for Android 問題為強制顯示，無法停用（例如，有關產品授權到期的問題）。

7. 若要隱藏所有通知和彈出訊息，請選擇**應用程式在背景模式時停用通知和彈出訊息**。

   Kaspersky Endpoint Security for Android 將僅顯示防護狀態通知。通知會顯示裝置防護狀態（例如，）以及問題數量。此外，使用者操作應用程式時，應用程式會顯示通知（例如，使用者手動更新病毒資料庫）。

   Kaspersky 專家建議您啟用通知和彈出訊息。如果應用程式在背景模式且停用通知和彈出訊息時，應用程式將無法針對威脅即時警告使用者。行動裝置使用者只有在開啟應用程式時，才能得知裝置的防護狀態。

8. 點擊「**套用**」按鈕以儲存所作的變更。

與卡巴斯基安全管理中心的下次裝置同步之後可配置行動裝置設定。您停用的 Kaspersky Endpoint Security for Android 通知將不會顯示在使用者的行動裝置上。

將 iOS MDM 裝置連線到 AirPlay

配置與 AirPlay 裝置的連線，以便將音樂、照片和視訊從 iOS MDM 裝置資料流到 AirPlay 裝置。行動裝置和 AirPlay 裝置必須連線到相同的行動網路，才能使用 AirPlay 技術。AirPlay 裝置包括（第二代和第三代）Apple TV 裝置、AirPort Express 裝置、揚聲器或支援 AirPlay 的收音機。

僅受控制的裝置可以自動連線至 AirPlay 裝置。

若要配置 iOS MDM 裝置與 AirPlay 裝置的連線，請執行以下操作：

1. 在主控台樹狀目錄的「**受管裝置**」資料夾中，選擇 iOS MDM 裝置所屬的管理群組。
2. 在所選群組的工作台中，選擇「**政策**」標籤。
3. 透過點擊開啟政策內容視窗。
4. 在政策「**內容**」視窗中選擇「**AirPlay**」區域。
5. 在「**AirPlay 裝置**」區域中選擇「**將設定套用於裝置**」核取方塊。
6. 按一下「**密碼**」區域中的「**新增**」按鈕。

   在密碼表格中新增一個空白的行。
7. 在「**裝置名稱**」列中，輸入無線網路上的 AirPlay 裝置的名稱。
8. 在「**密碼**」列中，輸入 AirPlay 裝置的密碼。
9. 若要限制 iOS MDM 裝置對 AirPlay 裝置的存取，請在「**允許的裝置**」區域建立允許的裝置清單。為此，將 AirPlay 裝置的 MAC 位址新增到允許的裝置清單中。

封鎖存取不在允許的裝置清單上的 AirPlay 裝置。如果允許的裝置清單留空，Kaspersky Device Management for iOS 將允許存取所有 AirPlay 裝置。

10. 點擊「**套用**」按鈕以儲存所作的變更。

這樣，一旦套用該政策，使用者的行動裝置將自動連線至 AirPlay 裝置，以流式傳輸媒體內容。

將 iOS MDM 裝置連線到 AirPrint

若要能夠使用 AirPrint 技術從 iOS MDM 裝置無線列印文件，請配置自動連線至 AirPrint 印表機。行動裝置和印表機必須連線到同一無線網路。必須在 AirPrint 印表機上配置所有使用者的共用存取權限。

若要配置 iOS MDM 裝置與 AirPrint 印表機的連線，請執行以下步驟：

1. 在主控台樹狀目錄的「**受管裝置**」資料夾中，選擇 iOS MDM 裝置所屬的管理群組。
2. 在所選群組的工作台中，選擇「**政策**」標籤。
3. 透過點擊開啟政策內容視窗。
4. 在政策「**內容**」視窗中選擇「**AirPrint**」區域。
5. 按一下「**AirPrint 印表機**」區域中的「**新增**」按鈕。
   「**印表機**」視窗將開啟。
6. 在「**IP 位址**」欄位中，輸入 AirPrint 印表機的 IP 位址。
7. 在「**資源路徑**」欄位中，輸入 AirPrint 印表機的路徑。
   印表機的路徑與 Bonjour 協定 的 RP（資源路徑）金鑰相對應。例如：
   - printers/Canon_MG5300_series
   - ipp/print
   - Epson_IPP_Printer
8. 點擊「**確定**」。
   新增的 AirPrint 印表機顯示在清單上。
9. 點擊「**套用**」按鈕以儲存所作的變更。

這樣，一旦套用該政策，行動裝置使用者可以在 AirPrint 印表機上無線列印文件。

配置存取點名稱 (APN)

若要將行動裝置連線到移動網路上的資料傳輸服務，您應配置 APN（存取點名稱）設定。

在 Android 裝置上配置 APN（僅限 Samsung）

APN 的配置僅適用於 Samsung 裝置。

必須插入 SIM 卡才能在使用者的行動裝置上使用存取點。存取點設定由行動電話運營商提供。存取點設定有誤可能產生額外的行動電話費用。

要配置存取點名稱 (APN) 設定，請執行以下操作：

1. 在主控台樹狀目錄的「**受管裝置**」資料夾中，選擇 Android 裝置所屬的管理群組。
2. 在所選群組的工作台中，選擇「**政策**」標籤。
3. 透過按兩下任何資料欄來開啟政策內容視窗。
4. 在政策「**內容**」視窗中選擇「**管理 Samsung KNOX**」→「**APN**」區域。
5. 在「**APN**」區域中，點擊「**配置**」按鈕。
   「**APN 設定**」視窗將開啟。
6. 在「**一般**」標籤上，指定以下存取點設定：
   a. 在「**APN 類型**」下拉清單中選擇存取點的類型。
   b. 在「**APN 名稱**」欄位中，指定存取點的名稱。
   c. 在「**MCC**」欄位中，輸入行動裝置國家/地區代碼 (MCC)。
   d. 在「**MNC**」欄位中，輸入行動裝置網路代碼 (MCC)。
   e. 如果您選擇 **MMS** 或**網際網路和 MMS** 作為存取點類型，請指定以下附加 MMS 設定：
      - 在「**MMS 伺服器**」欄位中，指定用於 MMS 交換的移動運營商伺服器的完整網域名稱。
      - 在「**MMS 代理伺服器**」欄位中，指定代理伺服器的網路名稱或 IP 位址和用於 MMS 交換的移動運營商伺服器的埠號。
7. 在「**其他**」標籤上，配置存取點 (APN) 的其他設定：
   a. 在「**身分驗證類型**下拉清單中，選擇用於網路存取的移動運營商伺服器上的行動裝置使用者認證的類型。
   b. 在「**伺服器位址**」欄位中，指定透過其存取資料傳輸服務的移動運營商伺服器的網路名稱。
   c. 在「**代理伺服器位址**」欄位中，指定用於網路存取的移動運營商代理伺服器的網路名稱或 IP 位址和埠號。
   d. 在「**使用者名稱**」欄位中，輸入行動網路上要進行身分驗證的使用者名稱。
   e. 在「**密碼**」欄位中，輸入用於行動網路上的使用者認證的密碼。
8. 點擊「**套用**」按鈕以儲存所作的變更。

與卡巴斯基安全管理中心的下個裝置同步之後可配置行動裝置設定。

在 iOS MDM 裝置上配置 APN

必須配置存取點名稱 (APN)，以便在使用者的 iOS MDM 裝置上啟用行動網路資料傳輸服務。

「**APN**」區域已棄用。建議在「**手機通訊**」區域配置 APN 設定。配置手機通訊設定之前，請確保未在裝置上應用「**APN**」部分的設定（「**將設定套用於裝置**」核取方塊未選中）。「**APN**」和「**手機通信**」區域的設定不能同時使用。

若要在使用者的 iOS MDM 裝置上配置存取點，請執行以下操作：

1. 在主控台樹狀目錄的「**受管裝置**」資料夾中，選擇 iOS MDM 裝置所屬的管理群組。
2. 在所選群組的工作台中，選擇「**政策**」標籤。
3. 透過點擊開啟政策內容視窗。
4. 在政策「**內容**」視窗中選擇「**手機通訊**」區域。
5. 在「**手機通訊設定**」區域中，選中「**將設定套用於裝置**」核取方塊。
6. 在 **APN 類型**清單中，選擇 GPRS/3G/4G 行動網路上用於資料傳輸的存取點類型：
   - **內建 APN** – 透過可支援使用內建 Apple SIM 卡運作的移動網路運營商，配置用於資料傳輸的手機通訊設定。如需具有內建 Apple SIM 卡裝置的詳細資訊，請造訪 Apple 技術支援網站。
   - **APN** – 透過插入的 SIM 卡的移動網路運營商配置用於資料傳輸的手機通訊設定。
   - **內建 APN 與 APN** – 透過插入的 SIM 卡和內建 Apple SIM 卡的移動網路運營商，配置用於資料傳輸的手機通訊設定。有關具有內建 Apple SIM 卡和 SIM 卡插槽的裝置的詳細資訊，請造訪 Apple 技術支援網站。
7. 在「**APN 名稱**」欄位中，指定存取點的名稱。
8. 在**身分驗證類型**下拉清單中，選取用於網路存取的行動運營商伺服器上的裝置使用者身分驗證類型（網際網路和 MMS）：
9. 在「**使用者名稱**」欄位中，輸入行動網路上要進行身分驗證的使用者名稱。
10. 在「**密碼**」欄位中，輸入用於行動網路上的使用者認證的密碼。
11. 在「**代理伺服器位址和連接埠**」欄位中，輸入主機的名稱或代理伺服器的 IP 位址和代理伺服器埠號。
12. 點擊「**套用**」按鈕以儲存所作的變更。

這樣，在套用該政策後，在使用者的行動裝置上配置存取點名稱 (APN)。

配置 Android for Work 設定檔

本節包含使用 Android 工作設定檔的資訊。

關於 Android 工作設定檔

*Android Enterprise*是專供管理企業行動基礎結構的平台，提供企業員工可以使用行動裝置的工作環境。如需深入瞭解如何使用 Android Enterprise，請參閱Google 支援網站。

您可以在使用者的行動裝置上建立 Android 工作設定檔（以下簡稱「工作設定檔」）。*Android 工作設定檔*是使用者裝置上的安全環境，在該環境中，管理員可以在不限制使用者使用其自己的資料的情況下，管理應用程式和使用者帳戶。在使用者的行動裝置上建立了工作設定檔後，下列公司應用程式將自動安裝到該工作設定檔中：Google Play Market、Google Chrome、Downloads、Kaspersky Endpoint Security for Android 等等。工作設定檔中安裝的應用程式，以及這些應用程式的通知，都會標上圖示。您必須為 Google Play Market 應用程式建立單獨的 Google 公司帳戶。工作設定檔中安裝的應用程式會顯示在常用應用程式清單中。

配置工作設定檔

若要配置 Android 工作設定檔的設定，請執行以下操作：

1. 在主控台樹狀目錄的「**受管裝置**」資料夾中，選擇 Android 裝置所屬的管理群組。
2. 在所選群組的工作台中，選擇「**政策**」標籤。
3. 透過按兩下任何資料欄來開啟政策內容視窗。
4. 在政策「**內容**」視窗中選擇「**Android 工作設定檔**」。
5. 在「**Android 工作設定檔**」工作台中，選擇「**建立工作設定檔**」核取方塊。
6. 指定工作設定檔設定：

   - 若要在 Android 工作設定檔中啟用 App Control 並在個人設定檔中停用它，請選擇「**僅在工作設定檔中啟用應用程式控制**」核取方塊。

     在「**使用者**」區域，您可以選擇「**應用程式控制**」，並使用工作台建立允許、封鎖、推薦和所需的應用程式清單，以及區域中允許和封鎖的應用程式類別。

   - 若要在工作設定檔中啟用 Google Chrome 的 Web 防護並在個人設定檔中停用，請在「**Android 工作設定檔**」區域的工作台中選擇「**僅在工作設定檔中啟用 Web 防護**」核取方塊。

     Samsung Internet Browser 的 Web 防護會封鎖工作和個人設定檔中的網站。您無法在 Samsung Internet Browser 中僅針對工作設定檔啟用 Web 防護。若要在工作設定檔中使用 Samsung Internet Browser 的 Web 防護，請停用「**僅在工作設定檔中啟用 Web 防護**」選項。如果啟用此選項，則不會執行 Samsung Internet Browser 的 Web 防護。Web 防護在工作設定檔中預設為停用。

     > Android 裝置上的 Web 防護僅在 Google Chrome 瀏覽器和 Samsung Internet Browser 中可用。

     您可以在「**Web 防護**」區域，指定網站存取設定（建立封鎖網站類別清單或允許網站清單）。

   - 若要防止使用者透過剪貼板從工作設定檔應用程式將資料複製至個人應用程式，請選擇「**禁止從工作設定檔向個人設定檔傳輸資料**」核取方塊。
   - 若要封鎖使用者在行動裝置上的工作設定檔中使用 USB 調試模式，請選中「**禁止啟動 USB 調試模式**」核取方塊。

舉例來說，在 USB 偵錯模式中，使用者可以利用工作站下載應用程式。

- 若要禁止使用者從除 Google Play 之外的所有源在 Android 工作設定檔中安裝應用程式，請選擇「**禁止從未知源透過工作設定檔安裝應用程式**」核取方塊。
- 若要禁止使用者從 Android 工作設定檔中移除應用程式，請選擇「**禁止從工作設定檔中移除應用程式**」核取方塊。

7. 若要在使用者的行動裝置上配置工作設定檔，請封鎖變更設定。
8. 點擊「**套用**」按鈕以儲存所作的變更。

與卡巴斯基安全管理中心的下次裝置同步之後可配置行動裝置設定。使用者行動裝置的空間分為工作設定檔和個人設定檔區。

新增 LDAP 帳戶

若要使 iOS MDM 裝置使用者可以存取 LDAP 伺服器上的企業聯絡人，請新增 LDAP 帳戶。

若要新增 iOS MDM 裝置使用者的 LDAP 帳戶，請執行以下操作：

1. 在主控台樹狀目錄的「**受管裝置**」資料夾中，選擇 iOS MDM 裝置所屬的管理群組。
2. 在所選群組的工作台中，選擇「**政策**」標籤。
3. 透過點擊開啟政策內容視窗。
4. 在政策「**內容**」視窗中選擇「**LDAP**」區域。
5. 按一下「**LDAP 帳戶**」區域中的「**新增**」按鈕。
   「**LDAP 帳戶**」視窗將開啟。
6. 在「**描述**」欄位中，輸入使用者的 LDAP 帳戶的描述。您可以使用「**可用巨集**」下拉清單中的巨集。
7. 在**帳戶名稱**欄位中，輸入要在 LDAP 伺服器上進行身分驗證的帳戶名稱。您可以使用「**可用巨集**」下拉清單中的巨集。
8. 在「**密碼**」欄位中，輸入用於在 LDAP 伺服器上進行身分驗證的 LDAP 帳戶的密碼。
9. 在「**伺服器位址**」欄位中輸入 LDAP 伺服器的網域名稱。您可以使用「**可用巨集**」下拉清單中的巨集。
10. 若要使用 SSL（安全通訊端層）資料傳輸協定防護郵件傳輸，請選擇「**使用 SSL 連線**」核取方塊。
11. 編制搜尋查詢清單，以便 iOS MDM 行動裝置使用者存取 LDAP 伺服器上的企業資料：
    a. 按一下「**搜尋設定**」區域中的「**新增**」按鈕。
       包含搜尋查詢的表格中會顯示一個空白的行。
    b. 在「**名稱**」列中輸入搜尋查詢的名稱。
    c. 在「**搜尋範圍**」列中，選擇 LDAP 伺服器上的企業資料搜尋的資料夾嵌套級別：
       - **基本** – 在 LDAP 伺服器的基本資料夾中搜尋。

- **一級** – 在從基本資料夾算起的第一個嵌套等級上的資料夾中搜尋。
- **子樹** – 在從基本資料夾算起的所有嵌套等級上的資料夾中搜尋。

d. 在「**搜尋庫**」列中，輸入 LDAP 伺服器上首先搜尋的資料夾的路徑（例如：「ou=people」，「o=example corp」）。

e. 對您要新增到 iOS MDM 裝置的所有搜尋查詢重複步驟 a-d。

12. 點擊「**確定**」。

新的 LDAP 帳戶顯示在清單中。

13. 點擊「**套用**」按鈕以儲存所作的變更。

這樣，一旦套用該政策，編制的清單中的 LDAP 帳戶將新增到使用者的行動裝置上。使用者可以存取標準 iOS 應用程式中的企業聯絡人：聯絡人、訊息和郵件。

新增行事曆帳戶

若要使 iOS MDM 裝置使用者可以存取 CalDAV 伺服器上的使用者行事曆事件，請新增 CalDAV 帳戶。與 CalDAV 伺服器同步，以便使用者建立和接收邀請、接收事件更新，以及與 Reminders 應用程式同步工作。

若要新增 iOS MDM 裝置使用者的 CalDAV 帳戶，請執行以下操作：

1. 在主控台樹狀目錄的「**受管裝置**」資料夾中，選擇 iOS MDM 裝置所屬的管理群組。
2. 在所選群組的工作台中，選擇「**政策**」標籤。
3. 透過點擊開啟政策內容視窗。
4. 在政策「**內容**」視窗中選擇「**行事曆**」區域。
5. 按一下「**CalDAV 帳戶**」區域中的「**新增**」按鈕。

「**CalDAV 帳戶**」視窗將開啟。

6. 在「**描述**」欄位中，輸入使用者的 CalDAV 帳戶的描述。
7. 在「**伺服器位址和連接埠**」欄位中，輸入主機的名稱或 CalDAV 伺服器的 IP 位址和 CalDAV 伺服器埠號。
8. 在「**主位址**」欄位中，指定 CalDAV 伺服器上的 iOS MDM 裝置使用者的 CalDAV 帳戶的網址（例如：http://example.com/caldav/users/mycompany/user）。

該網址的開頭應是「`http://`」或「`https://`」。

9. 在「**帳戶名稱**」欄位中，輸入用於在 CalDAV 伺服器上進行身分驗證的帳戶名稱。
10. 在「**密碼**」欄位中，設定用於在 CalDAV 伺服器上進行身分驗證的 CalDAV 帳戶密碼。
11. 若要使用 SSL（安全通訊端層）資料傳輸協定防護 CalDAV 伺服器與行動裝置之間的事件傳輸，請選擇「**使用 SSL 連線**」核取方塊。
12. 點擊「**確定**」。

新的 CalDAV 帳戶顯示在清單中。

13. 點擊「**套用**」按鈕以儲存所作的變更。

這樣，一旦套用該政策，編制的清單中的 CalDAV 帳戶將新增到使用者的行動裝置上。

新增聯絡人帳戶

若要使 iOS MDM 裝置使用者可以與 CardDAV 伺服器同步資料，請新增 CardDAV 帳戶。與 CardDAV 伺服器同步，以便使用者從任何裝置存取聯絡人詳細資訊。

若要新增 iOS MDM 裝置使用者的 CardDAV 帳戶，請執行以下操作：

1. 在主控台樹狀目錄的「**受管裝置**」資料夾中，選擇 iOS MDM 裝置所屬的管理群組。
2. 在所選群組的工作台中，選擇「**政策**」標籤。
3. 透過點擊開啟政策內容視窗。
4. 在政策「**內容**」視窗中選擇「**聯絡人**」區域。
5. 按一下「**CardDAV 帳戶**」區域中的「**新增**」按鈕。
   「**CardDAV 帳戶**」視窗將開啟。
6. 在「**描述**」欄位中，輸入使用者的 CardDAV 帳戶的描述。您可以使用「**可用巨集**」下拉清單中的巨集。
7. 在「**伺服器位址和連接埠**」欄位中，輸入主機的名稱或 CardDAV 伺服器的 IP 位址和 CardDAV 伺服器埠號。
8. 在「**主位址**」欄位中，指定 CardDAV 伺服器上的 iOS MDM 裝置使用者的 CardDAV 帳戶的網址（例如：http://example.com/carddav/users/mycompany/user）。
   該網址的開頭應是「`http://`」或「`https://`」。
9. 在「**帳戶名稱**」欄位中，輸入用於在 CardDAV 伺服器上進行身分驗證的帳戶名稱。您可以使用「**可用巨集**」下拉清單中的巨集。
10. 在「**密碼**」欄位中，設定用於在 CardDAV 伺服器上進行身分驗證的 CardDAV 帳戶密碼。
11. 若要使用 SSL（安全通訊端層）資料傳輸協定防護 CardDAV 伺服器與行動裝置之間的聯絡人傳輸，請選擇「**使用 SSL 連線**」核取方塊。
12. 點擊「**確定**」。
    新的 CardDAV 帳戶顯示在清單中。
13. 點擊「**套用**」按鈕以儲存所作的變更。

這樣，一旦套用該政策，編制的清單中的 CardDAV 帳戶將新增到使用者的行動裝置上。

配置行事曆訂購

若要使 iOS MDM 裝置使用者可以向使用者的行事曆新增共用行事曆（例如企業行事曆）的事件，請新增該行事曆的訂購。*共用行事曆*是其他具有 CalDAV 帳戶的使用者的行事曆、iCal 行事曆以及其他公開發佈的行事曆。

若要新增行事曆訂購，請執行以下步驟：

1. 在主控台樹狀目錄的「**受管裝置**」資料夾中，選擇 iOS MDM 裝置所屬的管理群組。
2. 在所選群組的工作台中，選擇「**政策**」標籤。
3. 透過點擊開啟政策內容視窗。
4. 在政策「**內容**」視窗中選擇「**行事曆訂購**」區域。
5. 按一下「**訂閱行事曆**」區域中的「**新增**」按鈕。
   將開啟「**行事曆訂購**」視窗。
6. 在「**描述**」欄位中，輸入行事曆訂購的描述。
7. 在「**伺服器網址**」欄位中，指定其他行事曆的網址。
   在該欄位中，您可以輸入您正在訂購其行事曆的使用者的 CalDAV 帳戶的郵件網址。您還可以指定 iCal 行事曆或其他公開發佈的行事曆的網址。
8. 在「**使用者名稱**」欄位中，輸入用於在其他行事曆伺服器上進行身分驗證的使用者帳戶的名稱。
9. 在「**密碼**」欄位中，輸入用於在其他行事曆伺服器上進行身分驗證的行事曆訂購密碼。
10. 若要使用 SSL（安全通訊端層）資料傳輸協定防護 CalDAV 伺服器與行動裝置之間的事件傳輸，請選擇「**使用 SSL 連線**」核取方塊。
11. 點擊「**確定**」。
12. 新的行事曆訂購顯示在清單中。
13. 點擊「**套用**」按鈕以儲存所作的變更。

這樣，一旦套用該政策，清單中共享行事曆的事件將新增到使用者的行動裝置上的行事曆中。

新增我的最愛

*網路我的最愛*是一個可從行動裝置的主螢幕開啟網站的應用程式。透過點擊裝置主螢幕上的網路我的最愛圖示，使用者可以快速開啟網站（例如公司網站）。您可以向使用者裝置新增網路我的最愛，配置螢幕上顯示的網路我的最愛圖示的外觀。

預設情況下，套用以下網路我的最愛使用限制：

- 使用者不能手動從行動裝置刪除網路我的最愛。
- 使用者點擊網路我的最愛時開啟的網站不會以全螢幕模式開啟。
- 對螢幕上的網路我的最愛圖示套用圓角、陰影和光澤視覺效果。

若要在使用者的 iOS MDM 裝置上新增網路我的最愛，請執行以下操作：

1. 在主控台樹狀目錄的「**受管裝置**」資料夾中，選擇 iOS MDM 裝置所屬的管理群組。
2. 在所選群組的工作台中，選擇「**政策**」標籤。
3. 透過點擊開啟政策內容視窗。

4. 在政策「**內容**」視窗中選擇「**Web Clips**」區域。

5. 按一下「**Web Clip**」區域中的「**新增**」按鈕。
   「**Web Clip**」視窗將開啟。

6. 在「**名稱**」欄位中，輸入要顯示在 iOS MDM 裝置主螢幕上的網路我的最愛的名稱。

7. 在「**網址**」欄位中，輸入點擊網路我的最愛圖示時將開啟的網站的網址。該網址應以「`http://`」或「`https://`」開頭。

8. 若要允許使用者從 iOS MDM 裝置移除我的最愛，請選擇「**允許刪除**」核取方塊。

9. 點擊「**選擇**」按鈕，指定包含我的最愛圖示圖片的檔案。
   該圖片顯示在 iOS MDM 行動裝置的主螢幕上。該圖片必須符合以下需求：

   - 圖片的尺寸不超過 400*400 畫素。
   - 檔案格式：GIF、JPEG 或 PNG。
   - 檔案大小不超過 1 MB。

   可在「**圖示**」欄位中預覽網路我的最愛圖示。如果您沒有選擇 Web Clip 圖片，顯示的圖示是正方形空白圖片。
   如果您希望顯示的網路我的最愛圖示不帶特殊的視覺效果（圖示圓角和光澤效果），請選中**預製作的圖示**方塊。

10. 如果您希望在點擊該圖示時網站在 iOS MDM 裝置上以全螢幕模式開啟，請選擇「**全螢幕 Web Clip**」核取方塊。

11. 點擊「**確定**」。
    新的網路我的最愛顯示在清單中。

12. 點擊「**套用**」按鈕以儲存所作的變更。

這樣，一旦套用該政策，您建立的清單中的網路我的最愛圖示將新增到使用者的行動裝置的主螢幕上。

新增字型

若要在使用者的 iOS MDM 裝置上新增字型，請執行以下步驟：

1. 在主控台樹狀目錄的「**受管裝置**」資料夾中，選擇 iOS MDM 裝置所屬的管理群組。

2. 在所選群組的工作台中，選擇「**政策**」標籤。

3. 透過點擊開啟政策內容視窗。

4. 在政策「**內容**」視窗中選擇「**字型**」區域。

5. 按一下「**字型**」區域中的「**新增**」按鈕。
   「**字型**」視窗將開啟。

6. 在「**檔案名稱**」欄位中，指定字型檔案（副檔名為 .ttf 或 .otf 的檔案）的路徑。

不支援副檔名為 ttc 或 otc 的字型。

字型使用 PostScript 名稱標識。請勿安裝具有相同的 PostScript 名稱的字型，即使它們的內容不同。安裝具有相同的 PostScript 名稱的字型將導致出現未定義的錯誤。

7. 點擊「**開啟**」。
   新的字型顯示在清單中。
8. 點擊「**套用**」按鈕以儲存所作的變更。

這樣，一旦套用該政策，將提示使用者安裝已建立的清單中的字型。

使用協力廠商 EMM 系統管理應用程式（僅限 Android）。

您可在沒有 Kaspersky 管理系統的情況下使用 Kaspersky Endpoint Security for Android 應用程式。使用其他 EMM 服務提供者的解決方案（企業移動管理）來佈署並管理 Kaspersky Endpoint Security for Android 應用程式。Kaspersky 加入 AppConfig Community 以確保應用程式可與協力廠商 EMM 解決方案一起執行。

您只能在執行 Android 版本的裝置上透過協力廠商 EMM 解決方案管理 Kaspersky Endpoint Security for Android 應用程式。

您僅可使用第三方 EMM 解決方案來佈署 Kaspersky Endpoint Security for Android 應用程式。將裝置連線至卡巴斯基安全管理中心並在管理主控台中管理應用程式。在此情況下，您無法在 EMM 主控台中管理 Kaspersky Endpoint Security for Android 應用程式。

若您使用第三方 EMM 系統佈署 Kaspersky Endpoint Security for Android 應用程式，您無法在 Kaspersky Endpoint Security Cloud 管理應用程式。您可在 EMM 主控台中管理 Kaspersky Endpoint Security for Android 應用程式。

以下 EMM 解決方案支援使用 Kaspersky Endpoint Security for Android 應用程式：

- VMware AirWatch
- MobileIron
- IBM Maas360
- Microsoft Intune
- SOTI MobiControl

您可以在 EMM 主控台中執行以下操作：

- 將應用程式佈署到使用者裝置上的 Android 工作設定檔。
- 啟動應用程式。
- 配置應用程式設定：

- 啟用網際網路惡意和釣魚網站防禦。
- 配置連線裝置到卡巴斯基安全管理中心的設定。
- 配置病毒防護設定。
- 配置對裝置執行病毒掃描排程。
- 啟用可偵測被犯罪分子用來損壞使用者的裝置或個人資料的廣告軟體和應用程式。
- 配置應用程式資料庫更新排程。

開始使用

要在使用者的行動裝置上佈署該應用程式，您必須將 Kaspersky Endpoint Security for Android 新增到 EMM 應用商店。您可以透過使用 Google Play 連結將 Kaspersky Endpoint Security for Android 新增到 EMM 應用商店。有關與 EMM 主控台中的應用程式一起使用的更多詳細資訊，請存取 *EMM 服務供應商的技術支援網站*。

Kaspersky Endpoint Security for Android 應用程式在 Android 工作設定檔中佈署。該應用程式與使用者的個人資料隔離，並只防護工作設定檔中的企業資料。建議確保防護 Kaspersky Endpoint Security for Android 免遭 EMM 主控台工具移除。

如何安裝應用程式

根據 EMM 主控台，選擇將應用程式安裝到裝置上的方法：靜默安裝、將包含連結的電子郵件傳送至 Google Play 中的應用程式或其他可用方法。

應用程式需要以下權限才可運作：

- 當病毒防護執行時的檔案存取儲存空間授權（僅對 Android 6.0 或更新）。
- 辨識裝置的電話授權，例如，當啟動應用程式時。
- 請求將 Kaspersky Endpoint Security for Android 新增到在作業系統啟動時啟動的應用程式清單（在某些裝置上，如華為、魅族和小米）。如果未顯示新增請求，將 Kaspersky Endpoint Security for Android 手動新增到啟動應用程式清單。如果工作設定檔中未安裝 Security 應用程式，該請求可能不會顯示。

您可先在 EMM 主控台中授予必要權限，再佈署 Kaspersky Endpoint Security for Android 應用程式。有關在 EMM 主控台中授予權限的更多詳細資訊，請造訪 *EMM 服務供應商的技術支援網站*。您也可在裝置上完成 Kaspersky Endpoint Security for Android 初始設定精靈時授予權限。

Kaspersky Endpoint Security for Android 應用程式將安裝在 Android 工作設定檔中。

要使 Web 防護執行，您還必須在 Google Chrome 設定中配置代理伺服器：

- 代理伺服器配置模式：手動。
- 代理伺服器位址和連接埠：127.0.0.1:3128。
- SPDY 協定支援：停用。
- 透過代理伺服器壓縮資料：停用。

如何啟動應用程式

有關產品授權的資訊與設定檔中的其他設定一起傳輸至行動裝置。

如果應用程式在行動裝置上安裝後 30 天內未啟動，試用產品授權將到期。試用版產品授權到期後，Kaspersky Endpoint Security for Android 行動 APP 的所有功能都將被停用。

正式產品授權到期後，該行動 APP 將在受限功能模式下繼續執行（例如 Kaspersky Endpoint Security for Android 的資料庫更新將不可用）。若要繼續在全功能模式下使用該應用程式，必須對正式產品授權進行續約。

若要啟動 Kaspersky Endpoint Security for Android，請執行以下操作：

1. 在 EMM 主控台中，開啟 Kaspersky Endpoint Security for Android 應用程式的設定。
2. 在 `LicenseActivationCode` 欄位中，輸入應用程式啟動碼。

   要在裝置上啟動應用程式，您必須具有存取 Kaspersky 啟動伺服器的權限。

如何連線裝置到卡巴斯基安全管理中心

在 Kaspersky Endpoint Security for Android 被安裝到行動裝置上後，您可以連線該裝置到卡巴斯基安全管理中心。連線裝置到卡巴斯基安全管理中心的必要資料與設定檔中列出的其他設定一起被傳輸到行動裝置。連線裝置到卡巴斯基安全管理中心後，您可以使用群組政策集中配置應用設定。您可以接收 Kaspersky Endpoint Security for Android 效能的報告和統計資訊。

在連線裝置到卡巴斯基安全管理中心之前，確保以下條件被滿足：

- Kaspersky Endpoint Security for Android 管理外掛程式已安裝到管理員工作站。
- 連線行動裝置的連接埠在管理伺服器內容中被開啟。
- 顯示**行動裝置管理**資料夾在管理主控台中被啟用。
- 用於辨識行動裝置使用者的一般憑證已在卡巴斯基安全管理中心憑證中被建立。

連線裝置到卡巴斯基安全管理中心之前，建議做以下：

- 如果您要為行動裝置建立工作和政策，請為行動裝置建立單獨的管理群組。
- 如果您要將行動裝置自動行動到單獨的管理群組，請從**未分配的裝置**資料夾建立一個自動移動裝置的規則。
- 如果您要集中配置 Kaspersky Endpoint Security for Android，建立群組政策。

要連線裝置到卡巴斯基安全管理中心：

1. 在 EMM 主控台中，開啟 Kaspersky Endpoint Security for Android 應用程式的設定。
2. 在 `KscServer` 欄位，輸入卡巴斯基安全管理中心管理伺服器的 DNS 名稱或 IP 位址。預設連接埠是 13292。
3. 如果不希望 Kaspersky Endpoint Security for Android 通知分散使用者的注意力，請停用應用通知。為此，設定 `DisableNotification = True` 設定。

連線之後，應用顯示所有通知。您可以在政策設定中停用特定應用通知。

如果您不使用卡巴斯基安全管理中心則不停用應用通知。這可以導致使用者不接收產品授權到期通知。結果，應用將停止執行其功能。

在配置連線設定後，Kaspersky Endpoint Security for Android 顯示通知提示您授予以下附加權限和授權：

- 使用攝影鏡頭進行竊盜防護操作（**臉部快照**命令）的權限。
- 使用定位進行竊盜防護操作（**定位裝置**命令）的權限。
- 裝置管理員權限（Android work 設定檔所有者）以操作以下應用功能：
  - 安裝安全憑證。
  - 配置 Wi-Fi。
  - 配置 Exchange ActiveSync。
  - 限制使用攝影鏡頭、藍芽和 Wi-Fi。

由於 Android work 設定檔的特別內容（沒有 Accessibility 服務），應用控制和竊盜防護功能在應用上不可用。

當使用者授予必要權限和授權時，裝置將被連線到卡巴斯基安全管理中心。如果自動移動裝置到管理群組的規則未被建立，裝置將自動新增到**未分配的裝置**資料夾中。如果自動移動裝置到管理群組的規則已建立，裝置將自動新增到定義的群組中。

Kaspersky Endpoint Security 提供下列裝置名稱格式：

- 裝置型號 [電子郵件，裝置 ID]
- 裝置型號 [電子郵件（如果有）或裝置 ID]

裝置 ID是 Kaspersky Endpoint Security for Android 根據從裝置接收的資料產生的唯一 ID。對於執行在 Android 10 或更新版本的行動裝置，Kaspersky Endpoint Security for Android 使用 SSAID (Android ID) 或從裝置接收的其他資料的校驗碼。對於早期版本的 Android，應用使用 IMEI。您可以在群組政策中設定裝置名稱格式。

在 SOTI MobiControl 中，您可以在 `KscDeviceName` 欄位中使用 %DEVICENAME% 巨集。此巨集可讓您從 SOTI MobiControl 主控台至卡巴斯基安全管理中心自動取得裝置名稱。

您也可以將標籤新增到裝置名稱中。這麼做可讓使用者在卡巴斯基安全管理中心輕鬆尋找與排序裝置。此標籤僅適用於 VMware AirWatch。

若要將標籤新增到裝置名稱中：

1. 在 EMM 主控台中，開啟 Kaspersky Endpoint Security for Android 應用程式的設定。
2. 在 `KscDeviceNameTag` 欄位，選擇各值：
   - `{DeviceSerialNumber}` – 裝置序號。
   - `{DeviceUid}` – 唯一的裝置識別碼 (UDID).

- `{DeviceAssetNumber}` – 裝置資源號碼。此號碼會在您的組織內部建立。

我們建議您僅使用這些值。VMware AirWatch 支援其他數值，但 Kaspersky Endpoint Security 不保證這些值都可以正常使用。

您可以新增一些值 (例如，`{DeviceSerialNumber} {DeviceUid}`)。此標籤將新增到卡巴斯基安全管理中心的裝置名稱。標籤與裝置名稱之間會空一格。例如，裝置名稱為 `Google Pixel 2 a10c6b75f7b31de9 22:7D:78:9E:C5:1E`，然後 `22:7D:78:9E:C5:1E` 為 UDID 標籤。若您使用卡巴斯基安全管理中心和 VMwareAirWatch，此標籤可讓您識別兩個主控台中的裝置。若要配對裝置，裝置名稱請選擇相同的值 (例如，裝置序號)。

在裝置連線到卡巴斯基安全管理中心之後，應用設定將根據群組政策被變更。Kaspersky Endpoint Security for Android 略過在 EMM 控制台中配置的設定檔中的應用設定。您可以配置政策的所有區域，除了以下區域：

- **竊盜防護**（裝置鎖定）
- **容器**
- **裝置管理**（螢幕鎖定）
- **應用程式控制**（封鎖封鎖的應用程式）
- **Android 工作設定檔**
- **管理 Samsung KNOX**

根據佈署工作設定檔所使用的方法，您無法從 **Android 工作設定檔**區域套用群組政策設定。這些設定僅在 work 設定檔是使用卡巴斯基安全管理中心建立時可以被套用。

AppConfig 檔案

系統將產生設定檔，以在 EMM 主控台中配置該應用程式。下表顯示了設定檔中的應用程式設定。

設定檔設定

配置鍵	描述	類型	值
`LicenseActivationCode`	應用程式啟動碼	String	由 20 個拉丁字母和數字組成的應用程式啟用啟動碼啟動應用程式，需透過網際網路 Kaspersky 啟動伺服器。 如果您將此欄位留空，將使用試用版產品程式。試用版產品授權的有效期為 30 天，授權到期後，Kaspersky Endpoint Security 行動 APP 的所有功能都將被停用。若要繼程式，您必須購買正式產品授權。
`EulaAcceptanceConfirmationV1`	<License Agreement link>	Choice	此設定僅適用於 VMware AirWatch。 `Accepted` – 我確認我已完整閱讀、瞭解和使用者產品授權協議的條款和條件

			`Declined` – 我不同意此最終使用者產品授 (EULA) 的條款和條件。 若要為所有行動裝置同意 EULA 的條款和 存取網際網路來與 Kaspersky 伺服器連線 若您選擇`Declined`，應用程式將請使用者 條款和條件。行動裝置使用者可在初始設 條件。
`EulaAcceptanceCodeV1`	產品授權協議代碼	String	這些設定僅適用於 VMware AirWatch。 如果您想接受單一最終使用者產品授權協 使用 `EulaAcceptanceCodeV1`。如果您想 EULA，請使用 `EulaAcceptanceCodesV2` `EulaAcceptanceCodesV2` 欄位必須包含 EULA 代碼清單：`"<EULAid1>;<EULAid2>;<EULAid3>;..."`。 產品授權協議代碼包含在最終使用者產品 *若需產品授權協議代碼：* 1. 從 EMM 主控台複製產品授權連結 (`EulaAcceptanceConfirmationV1`)。 2. 將連結貼到瀏覽器。 最終使用者產品授權協議 (EULA) 開啟 3. 閱讀 EULA 的條款和條件，並找到產品 碼。 若要為所有行動裝置同意 EULA 的條款 要存取網際網路來與 Kaspersky 伺服器 若您將欄位留白，應用程式將請使用者同 款和條件。行動裝置使用者可在初始設定 件。 如果您指定了兩個欄位的值，則將接受其 EULA 的條款和條件。
`EulaAcceptanceCodesV2`	產品授權協議代碼	String	
`KscServer`	卡巴斯基安全管理中心管理伺服器位址和連接埠	String	卡巴斯基安全管理中心管理伺服器的 DNS 址和連接埠號。按照以下格式輸入位址： `address>:<port>`。如果您輸入了伺服器 連接埠，應用將使用預設連接埠 13292。
`DisableNotification`	在連線到卡巴斯基安全管理中心之前停用應用通知	Boolean	`True` – Kaspersky Endpoint Security for A 有應用通知。Kaspersky Endpoint Security 隱藏通知直到裝置連線到卡巴斯基安全管 之後，應用顯示所有通知。您可以在政策 定應用通知。 如果您不使用卡巴斯基安全管理中心則 通知。這會導致使用者無法接收產品授 知。在此情況下，應用程式會停止執行

			`False` – Kaspersky Endpoint Security for 所有應用通知。
`ScanScheduleType`	掃描執行模式	Choice	`AfterUpdate` – 在資料庫更新後啟動病毒 式將按照定義的排程更新病毒資料庫 (`UpdateScheduleType`)。 `Daily` – 每日啟動一次病毒掃描。配置掃 (`ScanScheduleTime`)。 `Weekly` – 每週啟動一次病毒掃描。選擇一 毒掃描的一天 (`ScanScheduleDay`) 並配置 (`ScanScheduleTime`)。 `Off` – 停用病毒掃描的自動啟動。 無論設定哪個值，裝置使用者均可手動啟
`ScanScheduleDay`	掃描日期	Choice	`Monday / Tuesday / Wednesday / Th Friday / Saturday / Sunday` 您只能為此設定選擇一個值。
`ScanScheduleTime`	掃描時間	String	時間可以採用 24 小時格式（例如，13:00 式（例如，10:30 P.M.）指示。
`ScanScheduleLock`	封鎖配置掃描執行模式	Boolean	`True` – 使用者無法存取應用程式設定內的 模式設定。 `False` – 使用者可以配置病毒掃描執行模 用病毒掃描自動啟動。
`ScanOnlyExecutableFiles`	要掃描的檔案類型（病毒掃描）	Choice	`AllFiles` – 掃描所有檔案。 `OnlyExecutables` – 僅掃描可執行檔。可 .apk (.zip)、.dex 或 .so 副檔名的檔案。 在 Kaspersky Endpoint Security for Andro Pack 4 Maintenance Release 1 中，您無法 檔掃描。
`ScanArchives`	掃描壓縮檔案並解壓縮	Boolean	`True` – 應用程式會解壓壓縮檔案並掃描其 `False` – 應用程式僅掃描壓縮檔案。 應用僅掃描帶有 .zip (.apk) 副檔名的存檔。 在 Kaspersky Endpoint Security for Andro Pack 4 Maintenance Release 1 中，您無法 內容掃描。
`ScanActionOnThreatFound`	偵測到威脅後的操作（病毒掃描）	Choice	`Quarantine` – 應用程式會將偵測到的物件 區。應用程式會將存檔形式隔離檔案，不 傷害。隔離區允許您刪除或還原移動至隔 `Delete` – 刪除偵測到的物件。 `Skip` – 應用程式會將偵測到的物件保留不 到的物件被略過，Kaspersky Endpoint Sec Android 會警告使用者裝置防護方面存在問 存取裝置上的某個物件（如，嘗試複製或 應用程式會封鎖存取該物件。 `AskUser` – 應用程式會提示使用者為偵測 選擇一種操作：略過、隔離或刪除。當偵 時，使用者可以對所有物件套用所選操作 有關偵測到的威脅以及對它們執行的操作 應用程式報告中。
`ScanLock`	封鎖配置掃描	Boolean	`True` – 使用者無法存取應用程式設定中的

	設定		定：要掃描的檔案類型、壓縮檔案掃描以的威脅採取的操作。 `False` – 使用者可以配置掃描設定，以及測到的威脅選擇 `Skip` 操作。
`ScanAndProtectionAdwareRiskware`	封鎖犯罪分子可以用來對使用者的裝置和資料造成損害的廣告軟體、自動撥號程式和應用程式	Boolean	`True` – 應用程式會偵測可被犯罪分子用來置或資料的廣告軟體和其他應用程式。 `False` – 應用程式會略過可被犯罪分子用裝置或資料的廣告軟體和其他應用程式。
`ProtectionMode`	即時防護模式	Choice	`Recommended` – 應用程式僅掃描新安裝的並立即掃描「下載」資料夾中的檔案。 `Extended` – 應用程式掃描使用者在裝置上改、複製、執行和儲存的所有檔案。應用「下載」資料夾中的新應用程式和檔案。 `Disabled` – 停用即時防護。
`UseKsnMode`	卡巴斯基安全網路模式	Choice	`Recommended` – 應用程式會與卡巴斯基安交換資料。Kaspersky Endpoint Security f用 KSN 即時防護裝置防禦威脅（雲端防護護 Web 防護在網際網路上的執行。 `Extended` – 應用程式會與卡巴斯基安全網料，而且還會將來自 Kaspersky Endpoint S Android 的某些效能統計資訊傳送到病毒實訊有助於即時跟蹤威脅。KSN 服務不會收存個人資料。 `Disabled` – 應用程式不會使用來自卡巴斯的資料。您不能啟用 Web 防護 (`EnableWe`雲端防護元件對病毒防護不可用。
`ProtectScanOnlyExecutableFiles`	要掃描的檔案類型（即時防護）	Boolean	`AllFiles` – 掃描所有檔案。 `OnlyExecutables` – 僅掃描可執行檔。可 .apk (.zip)、.dex 或 .so 副檔名的檔案。 在 Kaspersky Endpoint Security for Andro Pack 4 Maintenance Release 1 中，您無法檔掃描。
`ProtectionActionOnThreatFound`	偵測到威脅後的操作（即時防護）	Choice	`Quarantine` – 應用程式會將偵測到的物件區。應用程式會將存檔形式隔離檔案，不傷害。隔離區允許您刪除或還原移動至隔 `Delete` – 刪除偵測到的物件。 `Skip` – 應用程式會將偵測到的物件保留不到的物件被略過，Kaspersky Endpoint Sec Android 會警告使用者裝置防護方面存在問存取裝置上的某個物件（如，嘗試複製或應用程式會封鎖存取該物件。 有關偵測到的威脅以及對它們執行的操作應用程式報告中。
`ProtectionLock`	封鎖配置即時防護設定	Boolean	`True` – 使用者無法存取應用程式設定中的設定：即時防護模式、要掃描的檔案類型到的威脅執行的操作。

			`False` – 使用者可以配置即時防護設定， 為偵測到的威脅選擇 `Skip` 操作。
`UpdateScheduleType`	資料庫更新執行模式	Choice	`Daily` – 每天檢查一次是否有新的病毒資 下載到裝置。配置資料庫更新啟動時間 (`UpdateScheduleTime`)。 `Weekly` – 每週檢查一次是否有新的病毒資 們下載到裝置。選擇一周中啟動資料庫更 (`UpdateScheduleDay`) 並配置時間 (`UpdateScheduleTime`)。 `Off` – 停用自動更新病毒資料庫。 無論設定哪個值，裝置使用者均可手動啟 更新。

`UpdateScheduleDay`	啟動資料庫更新的日期	Choice	`Monday / Tuesday / Wednesday / Th`
			`Friday / Saturday / Sunday`
			您只能為此設定選擇一個值。

`UpdateScheduleTime`	資料庫更新啟動時間	String	時間可以採用 24 小時格式（例如，13:00 式（例如，10:30 P.M.）指示。
`UpdateScheduleLock`	封鎖配置資料庫更新執行模式	Boolean	`True` – 使用者無法存取應用程式設定內的 行模式設定。 `False` – 使用者可以配置資料庫更新執行 停用病毒資料庫更新自動啟動。
`AllowUpdateInRoaming`	漫遊時更新資料庫	Boolean	`True` – 如果裝置在漫遊區域，應用程式會 庫。應用程式將按照定義的排程下載病毒 (`UpdateScheduleType`)。 `False` – 僅當裝置在家用網路中時，應用 病毒資料庫。

`EnableWebFilter`	Web 防護	Boolean	`True` – 應用程式使用 Web 防護元件封鎖
			惡意和釣魚網站。Web 防護僅支援 Googl
			如果網域受到信任，使用 HTTPS 協定的
			網站仍不會被封鎖。如果網域不受到信
			護則會封鎖惡意和釣魚網站。
			`False` – 停用惡意和釣魚網站防禦。
			要使 Web 防護元件工作，必須滿足以下條
			• 裝置使用者在初始設定精靈或應用程式
			私權政策和 Web 防護聲明。
			• 在瀏覽器設定中配置代理伺服器：
			`ProxyMode = "fixed_servers"`
			`ProxyServer = "127.0.0.1:3128"`
			`DisableSpdy = true`
			`DataCompressionProxyEnabled =`
			代理伺服器配置可能依 Google Chrom
			如需配置 Google Chrome 的詳細資訊
			Chromium 項目網站。
			在從行動裝置上移除 Kaspersky Endpo
			for Android 應用程式之後，重設代理伺

			• 使用 KSN 已在應用程式設定中啟用；U Recommended 或 UseKsnMode = Exte • 建議選擇 Google Chrome 作為作業系統 設瀏覽器。
EnableWebFilterLock	封鎖配置 Web 防護	Boolean	True – 使用者無法存取應用程式設定內的 定。 False – 使用者可以配置 Web 防護設定， 停用網際網路上的惡意和釣魚網站防禦。
UpdateServer	資料庫更新原始伺服器位址	String	託管資料庫更新的伺服器的位址，例如， http://update.server.com。 如果您將此欄位留空，Kaspersky Endpoin Android 將使用 Kaspersky 資料庫更新伺服
AllowGoogleAnalytics	將資料提交至 Google Analytics for Firebase、SafetyNet Attestation、Firebase Performance Monitoring 和 Crashlytics 服務	Boolean	True – 應用程式將 Kaspersky Endpoint S Android 操作資料自動提交至 Google Anal Firebase、SafetyNet Attestation、Fireba Performance Monitoring 和 Crashlytics 服 必要資料，用來改進該應用程式的效能並 意度。資料透過安全連線傳輸到 Google A Firebase、SafetyNet Attestation、Fireba Performance Monitoring 和 Crashlytics 服 存取和防護符合 Google Analytics for Fireb SafetyNet Attestation、Firebase Perform Monitoring 和 Crashlytics 服務的相關使用 False – 停用將資料提交至 Google Analyt Firebase、SafetyNet Attestation、Fireba Performance Monitoring 和 Crashlytics 服
KscDeviceNameTag	卡巴斯基安全管理中心的裝置名稱標籤	String	此設定僅適用於 VMware AirWatch。 此標籤將新增到卡巴斯基安全管理中心的 籤與裝置名稱之間會空一格。這麼做可讓 斯基安全管理中心輕鬆尋找與排序裝置。 • {DeviceSerialNumber} – 裝置序號， • {DeviceUid} – 唯一的裝置識別碼 (UI • {DeviceAssetNumber} – 裝置資源號 在您的組織內部建立。 您可以新增一些值 (例如，{DeviceSe {DeviceUid})。 我們建議您僅使用這些值。VMware Air 其他數值，但 Kaspersky Endpoint Secu 這些值都可以正常使用。
KscGroup	裝置群組名稱	字串	您可在 EMM 主控台指定裝置群組。當裝置 斯基安全管理中心，系統會自動將其新增

			資料夾的子資料夾中。子資料夾的名稱將定的群組名稱相符。之後，您可以建立規置從未分配裝置資料夾的子資料夾移至受夾內的管理群組。 若您將欄位留空，系統會自動將裝置新增資料夾的根。
`KscCorporateEmail`	使用者的企業電子郵件	String	您可在 EMM 主控台指定使用者的企業電子電子郵件將會顯示在卡巴斯基安全管理中 字串必須為有效的電子郵件地址。系統將值。
`KscDeviceName`	卡巴斯基安全管理中心內的應用程式名稱	String	此設定僅適用於 SOTI MobiControl。 您可以指定顯示在卡巴斯基安全管理中心您可以輸入任何名稱或使用 %DEVICENAM從 SOTI MobiControl 主控台自動取得裝置欄位空白，將會根據卡巴斯基安全管理中指定的格式產生裝置名稱。

網路負載

本節包含有關行動裝置和卡巴斯基安全管理中心之間交換的網路流量的資訊。

流量

工作	外出流量	內進流量	總流量
應用程式初始佈署，Mb	0.08	17.76	17.84
病毒資料庫初始更新（流量可能會因病毒資料庫的大小而不同），MB	0.04	2.21	2.25
行動裝置與卡巴斯基安全管理中心同步，MB	0.03	0.02	0.05
病毒資料庫定期更新（流量可能會因病毒資料庫的大小而不同），MB	0.08	3.06	3.14
執行竊盜防護命令。定位裝置（流量可能會因嵌入式攝影鏡頭規格和影像品質而不同），MB	0.09	0.8	0.17
執行竊盜防護命令。拍攝臉部快照，MB	1.0	0.02	1.02
執行竊盜防護命令。裝置鎖定，MB	0.06	0.05	0.11
平均每日流量，MB	0.22	6.96	7.18

加入卡巴斯基安全網路

若要有效防護行動裝置，Kaspersky Endpoint Security for Android 會使用從全球使用者所獲取的資料。*卡巴斯基安全網路*使用者處理此類資料。

卡巴斯基安全網路 (KSN) 是個雲端服務基礎結構，向 Kaspersky 的線上知識庫提供檔案信譽、網路資源和軟體等資訊。使用卡巴斯基安全網路中的資料，可確保在遇到威脅時 Kaspersky 程式能夠做出更快速的回應，提高某些防護元件的效能，並降低誤報的風險。

您加入卡巴斯基安全網路可幫助 Kaspersky 獲取關於新威脅的類型和來源的即時資、開發出抵銷威脅的方法並減少 Kaspersky Endpoint Security for Android 的誤報數量。加入卡巴斯基安全網路也允許您存取應用程式和網站信譽統計資料。

當您加入卡巴斯基安全網路後，Kaspersky Endpoint Security for Android 執行時會收集某些統計資訊並自動傳送給 Kaspersky。該資訊有助於即時跟蹤威脅。可能會被入侵者用來入侵以損壞電腦或使用者資料的檔案或其部分也會被傳送至 Kaspersky 以進行額外的檢查。

使用者必須操作 Kaspersky Endpoint Security for Android 才能使用卡巴斯基安全網路。KSN 被用於應用程式的主要元件：病毒防護、Web 防護和應用程式控制。拒絕參與 KSN 會降低裝置防護等級，這將引發裝置感染和資料丟失。要開始使用卡巴斯基安全網路，您必須在安裝應用程式時接受最終使用者產品授權協議的條款。閱讀最終使用者產品授權協議可知道哪些資料遭 Kaspersky Endpoint Security for Android 傳輸到卡巴斯基安全網路。

要改進應用程式效能，您可以另外提供統計資料到卡巴斯基安全網路。將上述資訊提供給 KSN 屬自願行為。若要開始使用卡巴斯基安全網路，您必須接受特殊的協議條款 - *卡巴斯基安全網路聲明*。您可以隨時選擇退出卡巴斯基安全網路。卡巴斯基安全網路聲明說明了 Kaspersky Endpoint Security for Android 向卡巴斯基安全網路傳輸的資料的類型。

與卡巴斯基安全網路交換資訊

為改進即時防護功能，Kaspersky Security for Mobile 將使用卡巴斯基安全網路雲端服務執行以下元件：

- **病毒防護。**應用獲得到關於檔案和應用信譽的 Kaspersky 線上知識庫的存取。此項掃描旨在掃描威脅資訊尚未新增到病毒資料庫但已包含在 KSN 中的威脅。卡巴斯基安全網路雲端服務提供病毒防護的完整操作並降低誤報。
- **Web 防護。**在開啟網站之前，該應用程式使用從 KSN 接收的資料對網站執行掃描。該應用程式還可基於允許和封鎖的類別清單（例如，「網際網路通訊」類別），確定控制使用者對網際網路存取的網站類別。
- **應用程式控制。**該應用程式可基於允許和封鎖的類別（例如，「網際網路通訊」類別）清單，確定限制不符合企業安全需求的應用程式啟動的應用程式類別。

最終使用者產品授權協議列出使用者若在操作防毒軟體或 App 應用程式時使用 KSN，該應用程式會提交給 Kaspersky 的資料類型相關資訊。接受產品授權協議的條件和條款即表明您同意傳輸此資訊。

有關在 Web 防護執行期間使用 KSN 時提交給 Kaspersky 的資料類型資訊，請參見有關 Web 防護資料處理的聲明。接受聲明的條件和條款即表明您同意傳輸此資訊。

為了識別新出現的資訊安全威脅、入侵威脅和難以偵測的威脅（及其各自的來源），以及改進對裝置上儲存和處理的資訊的防護，您可以延伸對卡巴斯基安全網路的參與。

要與 KSN 交換資料以提高應用程式的效能，必須滿足以下條件：

- 您或行動裝置使用者必須閱讀與接受卡巴斯基安全網路聲明的條款。若您選擇讓使用者接受聲明，他們將會在主應用程式畫面收到通知提示，以接受該聲明條款。使用者也可以在 Kaspersky Endpoint Security for Android 設定中的**關於應用程式**區段接受聲明。

  若您選擇接受全域聲明，透過卡巴斯基安全管理中心接受的版本聲明必須與使用者已接受的版本相符。否則，使用者將收到問題通知與提示，以接受符合管理員全域接受之版本的版本聲明。Kaspersky Security for Mobile (Devices) 外掛程式中的裝置狀態也將變更為*警告*。

- 您必須將群組政策設定配置為允許傳送統計資訊到 KSN。

您可以隨時選擇結束傳送統計資料到卡巴斯基安全網路。卡巴斯基安全網路聲明列出使用者若在操作 Kaspersky Endpoint Security for Android 行動應用程式時使用 KSN，該應用程式會提交給 Kaspersky 的統計資料類型相關資訊。

關於向 KSN 提供資料的更多資訊，請參閱「提供資料」部分。

向 KSN 提供資料屬自願行為。如有需要，您可以停用與 KSN 交換資料。

啟用和停用使用卡巴斯基安全網路

要執行使用卡巴斯基安全網路的 Kaspersky Endpoint Security for Android 元件，應用程式會向雲端服務傳送請求。請求包含「資料提供」區域中描述的資料。

如果裝置上停用了使用卡巴斯基安全網路，則雲端防護、Web 防護和應用程式控制元件將被自動停用。

若要啟用和停用使用卡巴斯基安全網路，請執行以下操作：

1. 開啟視窗，顯示已安裝 Kaspersky Endpoint Security for Android 的行動裝置的管理政策設定。
2. 在政策「**內容**」視窗中選擇「**其他**」區域。
3. 在「**卡巴斯基安全網路 (KSN) 設定**」區域中，配置使用卡巴斯基安全網路的設定：
   - 要執行以下元件，請選中「**使用卡巴斯基安全網路**」核取方塊：病毒防護（雲端防護）、Web 防護和應用程式控制（應用程式類別）。
   - 選中「**允許傳送統計資訊到 KSN**」核取方塊以將資料提交給 Kaspersky。此資料將說明 Kaspersky Endpoint Security for Android 應用程式在遇到威脅時更快地作出回應，提高防護元件的效能以及降低誤報的風險。
4. 點擊「**套用**」按鈕以儲存所作的變更。

與卡巴斯基安全管理中心的下次裝置同步之後可配置行動裝置設定。套用政策後，使用卡巴斯基安全網路的元件將被停用，元件裝置將不再可用。

使用卡巴斯基私人安全網路

卡巴斯基私人安全網路（以下也稱為*私有 KSN* 或 *KPSN*）是一種解決方案，此解決方案授予對卡巴斯基安全網路信譽資料庫的存取權限，而無需將資料從使用者裝置傳送到卡巴斯基安全網路。

物件（檔案或 URL）信譽資料庫儲存在卡巴斯基私人安全網路伺服器上，而未儲存在卡巴斯基安全網路伺服器上。KPSN 信譽資料庫儲存在公司網路內，並由公司管理員管理。

啟用 KPSN 時，Kaspersky Endpoint Security 不會從使用者裝置向 KSN 傳送任何統計資料。

要透過卡巴斯基安全管理中心啟用私有 KSN，請執行以下操作：

1. 在卡巴斯基安全管理中心網頁主控台或雲端主控台的主視窗中，點擊**設定**（ ）。

   「管理伺服器內容」視窗將開啟。

2. 在**一般**標籤上，選取 **KSN 代理設定**部分。

3. 將切換按鈕切換到**使用卡巴斯基私人安全網路啟用**位置。

4. 點擊「**使用 KSN 代理伺服器選擇檔案設定**」按鈕，然後瀏覽具有 pkcs7 或 pem 副檔名（由卡巴斯基提供）的設定檔。

5. 點擊「**開啟**」。

6. 如果您在管理伺服器內容中配置了代理伺服器設定，但您的網路架構要求您直接使用私有 KSN，請啟用**連線到私有 KSN 時忽略 KSC 代理伺服器設定**選項。否則，來自受管理應用程式的請求將無法到達私有 KSN。

7. 點擊「**儲存**」按鈕。

下載設定後，介面會顯示提供商的名稱和聯絡人，以及帶有私有 KSN 設定的檔案建立日期。KPSN 設定將套用到行動裝置上。

當您切換到專用 KSN 時，應用程式控制不支援使用全域 KSN 時可用的應用程式類別。如果您選擇切換回 KSN，則可以進行應用程式分類。

對第三方服務的資料提供

Kaspersky Endpoint Security for Android 使用 Google™ 服務，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) 服務以確保向行動裝置的命令傳送並在政策設定被變更時強制同步。Kaspersky Endpoint Security for Android 使用 Google Analytics for Firebase、SafetyNet Attestation、Firebase Performance Monitoring 和 Crashlytics 服務以改進應用程式效能並幫助 Kaspersky 建立更有效的行銷資料。

與 Firebase Cloud Messaging 交換資訊

Kaspersky Endpoint Security for Android 使用 Firebase Cloud Messaging (FCM) 服務以確保向行動裝置的命令傳送並在政策設定被變更時強制同步。該應用程式還使用推送通知。

要使用 Firebase Cloud Messaging 服務，您必須在卡巴斯基安全管理中心中配置服務設定。如需配置卡巴斯基安全管理中心的 Firebase Cloud Messaging 詳細資訊，請參閱*卡巴斯基安全管理中心說明*。如果未配置 Firebase Cloud Messaging 設定，當行動裝置根據政策中設定的排程（例如，每 24 小時一次）與卡巴斯基安全管理中心同步時，裝置上的命令和政策設定將被傳送。換句話說，命令和政策設定將被延遲傳送。

出於支援產品主要功能的目的，您同意自動提供 Firebase Cloud Messaging 服務應用安裝的獨一 ID（實例 ID）以及以下資料：

- 已安裝軟體的資訊：應用版本、應用 ID、應用版本號、應用套件名稱。
- 安裝了軟體的電腦資訊：OS 版本、裝置 ID、Google 服務版本。
- FCM 資訊：FCM 中應用 ID、FCM 使用者 ID、協議版本。

資料透過安全連線傳輸到 Firebase 服務。對資訊的存取和防護依照 Firebase 服務的相關使用條款：https://firebase.google.com/terms/data-processing-terms/、https://firebase.google.com/support/privacy/。

封鎖與 Firebase Cloud Messaging 服務交換資訊：

1. 在主控台樹狀目錄中，選擇「**行動裝置管理**」→「**行動裝置**」。
2. 從「**行動裝置**」資料夾的右鍵功能表中，選擇「**內容**」。
3. 在「**行動裝置**」資料夾的內容視窗中，選擇「**Google Firebase Cloud Messaging 設定**」區域。
4. 點擊「**重設**」按鈕。

與 Google Analytics for Firebase、SafetyNet Attestation、Firebase Performance Monitoring 和 Crashlytics 交換資訊

若您使用先前版本的管理外掛程式並且已啟用與 Google Analytics 服務的資料交換，Kaspersky Endpoint Security for Android Service Pack 4 Maintenance Release 3 將與 Google Analytics for Firebase 服務執行交換資料。Google Analytics 支援已中止。

Kaspersky Security for Mobile 與 Google Analytics for Firebase、SafetyNet Attestation、Firebase Performance Monitoring 和 Crashlytics 服務交換資料為達到以下目的：

- 提高應用程式的效能。

  要與 Google Analytics for Firebase、SafetyNet Attestation、Firebase Performance Monitoring 和 Crashlytics 服務交換資料以提高應用程式的效能，必須滿足以下條件：

  - 管理員或行動裝置使用者必須閱讀與接受卡巴斯基安全網路聲明的條款。若您選擇讓使用者接受聲明，他們將會在主應用程式畫面收到通知提示，以接受該聲明條款。使用者也可以在 Kaspersky Endpoint Security for Android 設定中的**關於應用程式**區段接受聲明。

    若您選擇接受全域聲明，透過卡巴斯基安全管理中心接受的版本聲明必須與使用者已接受的版本相符。否則，使用者將收到問題通知與提示，以接受符合管理員全域接受之版本的版本聲明。Kaspersky Security for Mobile (Devices) 外掛程式中的裝置狀態也將變更為*警告*。

  - 管理員必須將群組政策設定配置為允許傳送統計資訊到 KSN（參見下文）。

- 幫助 Kaspersky 建立更有效的市場行銷材料。

  要與 Google Analytics for Firebase、SafetyNet Attestation、Firebase Performance Monitoring 和 Crashlytics 服務交換資料以幫助 Kaspersky 建立有效的市場行銷材料，必須滿足以下條件：

  - 管理員或行動裝置使用者必須閱讀與接受有關將資料處理用於市場行銷的聲明條款。若您選擇讓使用者接受聲明，他們可以在安裝應用程式或在 Kaspersky Endpoint Security for Android 設定的**關於應用程式**區段中，接受聲明條款。

  - 管理員必須將群組政策設定配置為允許向 Google Analytics for Firebase、SafetyNet Attestation、Firebase Performance Monitoring 和 Crashlytics 傳送資料（參見下文）。

在有關將資料處理用於市場行銷的聲明下對 Google Analytics for Firebase、SafetyNet Attestation、Firebase Performance Monitoring 和 Crashlytics 的資料提供

權利持有人採用協力廠商資訊系統對資料進行處理。權利持有人的資料處理受此類協力廠商資訊系統的隱私聲明約束。以下為權利持有人採用的服務以及權利持有人所處理的資料：

Google Analytics for Firebase

在使用軟體時，下列資料將自動定期寄送至 Google Analytics for Firebase，以達成前述載明之目的：

- 應用程式資訊 (應用程式版本、應用程式 ID，以及 Firebase 服務中的應用程式 ID、Firebase 服務中的副本 ID、獲取應用程式的商店名稱、軟體首次啟動的時間戳記)
- 裝置上應用程式安裝的 ID 以及安裝方法
- 關於地區與語言本地化的資訊
- 關於裝置螢幕解析度的資訊
- 取得 root 權限之使用者的相關資訊
- SafetyNet Attestation 服務所提供的裝置診斷資訊
- 將 Kaspersky Endpoint Security for Android 設定為協助工具功能的相關資訊
- 有關應用程式熒幕間、會話期間、熒幕會話開始和結束時資料傳輸以及熒幕名稱相關的資訊
- 關於用來將資料提交給 Firebase 服務的通訊協定、其版本以及使用的資料提交方式識別碼的資訊
- 提交資料目標事件之類型和參數的詳細資訊
- 關於應用程式授權、可用性以及裝置數量的資訊
- 防毒資料庫更新頻率以及與管理伺服器同步頻率的相關資訊
- 關於管理主控台（Kaspersky Security Center或協力廠商 EMM 系統）
- Android ID
- 廣告 ID
- 有關使用者的資訊： 年齡類別與性別、居住國家/地區的識別碼以及興趣清單
- 有關安裝了該軟體的使用者電腦的資訊： 電腦製造商名稱、電腦類型、機型、作業系統的版本與語言（地區設定）、在過去 7 天首次開啟的應用程式相關資訊，以及超過過去 7 天首次開啟的應用程式相關資訊

  資料將透過安全通道轉寄到 Firebase。Firebase 中資料處理方式的相關資訊會發布於下列網址：https://firebase.google.com/support/privacy.

SafetyNet Attestation

使用軟體期間，系統會定期將下列資料自動傳送給 SafetyNet Attestation 以達到宣告目的：

- 裝置檢查時間
- 軟體相關資訊、軟體憑證的名稱與資料
- 裝置檢查結果

- 驗證檢查裝置的隨機識別碼檢查

  資料將透過安全通道轉寄到 SafetyNet Attestation。SafetyNet Attestation 中資料處理方式的相關資訊會發布於下列網址：https://policies.google.com/privacy.

Firebase Performance Monitoring

在軟體使用期間，系統會定期將下列資料自動傳送給Firebase Performance Monitoring，以達成前述載明之目的：

- 唯一安裝 ID
- 應用程式套件名稱
- 已安裝軟體的版本
- 電池充電狀態與電池電量
- 電訊廠商
- 應用前台或後台狀態
- 地理
- IP 位址
- 裝置語言代碼
- 有關無線電/網路連線的資訊
- 匿名軟體實例 ID
- RAM 與磁碟大小
- 表示裝置是否越獄或取得根權限的標誌
- 訊號強度
- 自動追蹤持續時間
- 網路和以下相應資訊： 回應代碼，承載（位元），回應時間
- 裝置描述

  資料將透過安全通道轉寄到Firebase Performance Monitoring。Firebase Performance Monitoring 中資料處理方式的相關資訊會發布於下列網址：https://firebase.google.com/support/privacy.

Crashlytics

在軟體使用期間，系統會定期將下列資料自動傳送給 Crashlytics，以達成前述載明之目的：

- 軟體 ID
- 已安裝軟體的版本
- 表示軟體是否在背景執行的標誌

- CPU 基礎架構
- 唯一事件 ID
- 事件日期與時間
- 裝置型號
- 總計磁碟空間與目前用量
- 作業系統名稱及版本
- 總計 RAM 與目前用量
- 表示裝置是否取得根權限的標誌
- 發生事件時的螢幕方向
- 產品/硬體製造商
- 唯一安裝 ID
- 所發送之統計資料集的版本
- 軟體例外類型
- 錯誤訊息文字
- 表示軟體例外是由巢狀例外引起的標誌
- 執行緒 ID
- 表示框架是否軟體錯誤原因的標誌
- 表示執行緒引起軟體意外終止的標誌
- 有關引起軟體意外終止的訊號的資訊： 訊號名稱，訊號代碼，訊號位址
- 對於和執行緒、例外或錯誤關聯的每個框架： 框架檔案名稱，框架檔案行號，偵錯符號，二進位檔映像的位置和位移，帶有框架的庫的顯示名稱，框架類型，表示框架是否是錯誤原因的標誌
- OS ID
- 與事件關聯的問題 ID
- 有關軟體意外終止前發生的事件的資訊： 事件標識符，事件日期與時間，事件類型和值
- CPU 登錄檔值
- 事件類型和值

  資料將透過安全通道轉寄到Crashlytics。Crashlytics 中資料處理方式的相關資訊會發布於下列網址：https://firebase.google.com/terms/crashlytics-app-distribution-data-processing-terms.

基於自願原則出於行銷目的提供上述處理資訊。

若要停用與 Google Analytics for Firebase、SafetyNet Attestation、Firebase Performance Monitoring 和 Crashlytics 服務的資料交換：

1. 開啟安裝了 Kaspersky Endpoint Security for Android 應用程式的行動裝置的管理政策的配置視窗。
2. 在政策「**內容**」視窗中選擇「**其他**」區域。
3. 在**資料傳輸**區域中，清除**允許資料傳輸以協助改善應用程式的品質、外觀和效能**核取方塊。
4. 點擊「**套用**」按鈕以儲存所作的變更。

與卡巴斯基安全管理中心的下個裝置同步之後可配置行動裝置設定。

全域接受其他聲明

若要啟用 Kaspersky Endpoint Security for Android 所提供的防護功能，必須接受最終使用者產品授權協議條款和其他聲明（參見下文）。您為所有使用者設定了全域接受下列聲明的政策。針對下列已全域接受之協議和聲明，使用者將不會收到閱讀與接受這些協議和聲明的提示：

- 卡巴斯基安全網路聲明
- 有關將資料處理用於 Web 防護的聲明
- 有關將資料處理用於市場行銷的聲明

若您選擇接受全域聲明，透過卡巴斯基安全管理中心接受的版本聲明必須與使用者已接受的版本相符。否則，使用者將收到問題通知與提示，以接受符合管理員全域接受之版本的版本聲明。Kaspersky Security for Mobile (Devices) 外掛程式中的裝置狀態也將變更為 *警告*。

若要選擇是否必須全域接受條款或由使用者接受條款，可套用群組政策：

1. 在主控台樹狀目錄的「**受管裝置**」資料夾中，選擇 Android 裝置所屬的管理群組。
2. 在所選群組的工作台中，選擇「**政策**」標籤。
3. 透過按兩下任何資料欄來開啟政策內容視窗。
4. 在政策「**內容**」視窗中選擇「**其他**」區域。
5. 在**資料傳輸**區域中，選擇是否全域接受或由使用者接受將資料處理用於市場行銷的聲明。
6. 在**卡巴斯基安全網路 (KSN) 設定**區域，選擇是否全域接受或由使用者接受卡巴斯基安全網路聲明。
7. 點擊「**套用**」按鈕以儲存所作的變更。

使用者可以隨時在 Kaspersky Endpoint Security for Android 設定的「**關於應用程式**」區域中接受或拒絕聲明的條款。

Samsung KNOX

Samsung KNOX 是一個配置和防護執行 Android 作業系統的 Samsung 行動裝置的行動裝置解決方案。有關 Samsung KNOX 的更多詳細資訊，請造訪*Samsung 技術支援網站*。

透過 KNOX Mobile Enrollment 安裝 Kaspersky Endpoint Security for Android 應用程式

KNOX Mobile Enrollment (KME) 是 Samsung KNOX 行動解決方案的一部分。它用於在透過官方供應商購買的全新 Samsung 裝置上批量安裝應用程式和初始配置。

透過 KNOX Mobile Enrollment 安裝 Kaspersky Endpoint Security for Android 應用程式包括以下步驟：

1. **使用 Kaspersky Endpoint Security for Android 應用程式建立 KNOX MDM 設定檔。**
2. **在 KNOX Mobile Enrollment 中新增裝置。**
3. **在使用者的行動裝置上安裝 Kaspersky Endpoint Security for Android 應用程式。**

有關使用 KNOX Mobile Enrollment 的更多詳細資訊，請參閱 *KNOX Mobile Enrollment 使用者手冊*。

只有 Samsung 裝置可以透過 KNOX Mobile Enrollment 進行佈署。如需支援的裝置清單，請造訪 *Samsung 技術支援網站*。

建立 KNOX MDM 設定檔

KNOX MDM 設定檔是一種包含指向應用程式的連結以便在行動裝置上進行快速佈署和初始配置的設定檔。

要建立 KNOX MDM 設定檔，請執行以下動作：

1. 登入 Samsung KNOX 主控台 → **KNOX Mobile Enrollment**。
2. 選擇「**MDM 設定檔**」部分。
3. 點擊「**新增**」。
   新 KNOX MDM 設定檔精靈將啟動。
4. 在「**MDM 伺服器連線**」步驟，選擇「**我的 MDM 服務無需伺服器 URI**」，然後點擊「**下一步**」。
5. 在「**MDM 設定檔資訊**」步驟：
   a. 輸入有關 KNOX MDM 設定檔的一般資訊：「**設定檔名稱**」和「**描述**」。
   b. 點擊「**新增 MDM 應用程式**」按鈕，然後輸入 APK 安裝檔案的路徑。
      Kaspersky Endpoint Security for Android 的安裝檔案包含在 Kaspersky Security for Mobile 分發套件中。提前將 APK 安裝檔案放在卡巴斯基安全管理中心網頁伺服器或可存取以便從裝置上下載的其他伺服器上。
   c. 採用以下格式在「**JSON 使用者資料**」欄位中輸入用於將裝置連線到卡巴斯基安全管理中心的設定：`{"serverAddress":"ksc.server.com","serverPort":"12345","groupName":"MOBILE GROUP"}`。
      必須將裝置連線到卡巴斯基安全管理中心才能啟動應用程式，配置裝置以及傳送命令。

d. 選中「**新增 Knox 協定**」核取方塊。

要透過 KNOX Mobile Enrollment 安裝 Kaspersky Endpoint Security for Android，行動裝置使用者必須接受 Samsung 產品授權協議的條款。您可以在名為「**最終使用者產品授權協議、服務條款和使用者協議**」的區域中檢視 Samsung 產品授權協議的條款。您還可以透過點擊「**新增使用者協議**」按鈕來新增佈署 KNOX MDM 設定檔所需的公司其他法律文件。

e. 清除「**將 KNOX 產品授權繫結到此設定檔**」核取方塊。

當裝置與卡巴斯基安全管理中心同步時，Samsung KNOX 產品授權資訊將與政策一起傳遞到行動裝置。

6. 點擊「**儲存**」按鈕。

因此，帶有 Kaspersky Endpoint Security for Android 應用程式的新 KNOX MDM 設定檔將新增到 KME 主控台中的清單中。

在 KNOX Mobile Enrollment 中新增裝置

可以採用以下方式將裝置新增到 KNOX Mobile Enrollment (KME) 主控台中：

- 在購買裝置後，供應商會將裝置自動新增到 KME 主控台中。

  如果您的組織使用 Samsung 裝置的官方供應商，請選擇此方法。

- 管理員可透過 Google Play 在行動裝置上安裝 KNOX 佈署應用程式，然後透過藍芽或 NFC（近場通訊）將 KNOX MDM 設定檔遷移到使用者裝置。在佈署 KNOX MDM 設定檔後，裝置將自動新增到 KME 主控台中。

  如果 Samsung 裝置不是從官方供應商處購買的，請選擇此方法。

透過供應商新增裝置

Samsung 裝置的官方供應商在 Samsung KNOX 中有註冊。有關官方供應商清單，請存取 *Samsung 技術支援網站*。在購買裝置後，供應商會立即將裝置自動新增到您的 Samsung 帳戶的 KME 主控台中。要使供應商新增裝置，您必須在 Samsung 帳戶的 KME 主控台中註冊供應商。您將需要有一個經銷商 ID 才能在 KME 主控台中新增 Samsung 裝置的供應商。要接收經銷商 ID，您必須向供應商傳送請求。在請求中，指定您的 KNOX 用戶端 ID。

若要檢視您的 KNOX 用戶端 ID，請執行以下操作：

1. 登入 Samsung KNOX 主控台 → **KNOX Mobile Enrollment**。
2. 選擇**經銷商**區域。
3. 您的 ID 將在**KNOX 用戶端 ID**欄位中顯示。

在您從供應商處收到包含經銷商 ID 的回應後，在 KME 主控台中註冊供應商。在註冊供應商之前，您可以建立一個 KNOX MDM 設定檔，以便在新增裝置時可以自動佈署該設定檔。

若要在 KME 主控台中註冊官方供應商，請執行以下操作：

1. 登入 Samsung KNOX 主控台 → **KNOX Mobile Enrollment**。
2. 選擇**經銷商**區域。
3. 點擊**註冊經銷商**按鈕。

   這會開啟一個視窗，用於註冊裝置供應商。

4. 在**經銷商 ID** 欄位中，輸入從 Samsung 裝置官方經銷商處接收的 ID。

5. 如果您建立了一個 KNOX MDM 設定檔，請在供應商註冊視窗中選擇該 KNOX MDM 設定檔。

   在您新增新裝置時，該 KNOX MDM 設定檔會自動安裝。

6. 在**偏好的下載確認方法**清單中，選擇一種確認供應商新增裝置的方法。

   - **您必須確認所有下載**。當供應商新增裝置時，您將需要確認此操作。
   - **自動確認此經銷商的所有下載**。該供應商的裝置將自動新增到 KME 主控台中。

7. 點擊「**確定**」。

Samsung 裝置的供應商將新增到 KME 主控台的供應商清單中。

在從官方供應商處購買新裝置後，在將裝置連線到網際網路時，Kaspersky Endpoint Security for Android 應用程式將自動安裝到裝置上。有關使用 KNOX Mobile Enrollment 的更多詳細資訊，請參閱 *KNOX Mobile Enrollment 使用者手冊*。如果您在 KME 主控台中已有裝置清單，則將包含 KNOX MDM 應用程式的 KNOX MDM 設定檔新增到裝置。

要將 KNOX MDM 設定檔傳送到裝置，請執行以下操作：

1. 登入 Samsung KNOX 主控台 → **KNOX Mobile Enrollment**。

2. 選擇「**裝置**」→「**所有裝置**」。

3. 選擇您要安裝 KNOX MDM 設定檔的裝置。

4. 點擊**配置**按鈕。

   裝置資訊視窗將開啟。

5. 在 **MDM 設定檔**清單中，選擇包含 Kaspersky Endpoint Security for Android 應用程式的 KNOX MDM 設定檔。

6. 在**標籤**欄位中，輸入用於分群組和標記裝置，以及 KME 主控台中的搜尋最佳化的標籤。

7. 將裝置的使用者帳戶憑據輸入到**使用者 ID** 和**密碼**欄位。

   接收一般憑證需要帳戶憑據。使用者 ID 和密碼必須與卡巴斯基安全管理中心中的使用者帳戶憑證相符（使用者帳戶內容中的「全名」和「密碼」）。

8. 為剩餘裝置選擇 KNOX MDM 設定檔。

9. 點擊「**儲存**」按鈕。

在將裝置連線到網際網路之後，系統將提示使用者安裝 KNOX MDM 設定檔。

透過 KNOX 佈署應用程式新增裝置

如果您未從官方供應商處購買 Samsung 裝置，您可以透過藍牙或 NFC 將裝置新增到 KNOX Mobile Enrollment。這將需要使用管理員的行動裝置來將 KNOX MDM 設定檔傳送到使用者的行動裝置。

要使用 KNOX 佈署應用程式新增裝置，必須滿足以下條件：

- 根據所選傳送模式，您必須在行動裝置上啟用藍芽或 NFC 模組。

- 行動裝置必須連線至網際網路。

要使用 KNOX 佈署應用程式傳送 KNOX MDM 設定檔，請執行以下操作：

1. 透過 Google Play 在管理員的行動裝置上安裝 KNOX 佈署應用程式。
2. 啟動 KNOX 佈署應用程式。
3. 輸入您的 Samsung 帳戶憑證。
4. 在 **KNOX 佈署**視窗中，配置佈署 KNOX MDM 設定檔的設定：
   - 選擇 KNOX MDM 設定檔。
   - 選擇佈署模式：**藍芽**或 **NFC**。
     當使用藍芽時，您可將一個 KNOX MDM 設定檔同時新增到多台裝置。
5. 點擊**開始佈署**：
   - **藍牙**。在使用者的行動裝置上，開啟網站 https://configure.samsungknox.com。
     這會啟動 Samsung KNOX 裝置註冊精靈。按照螢幕上的說明操作。
     安裝 KNOX MDM 設定檔之後，帶有**藍牙**標籤的新裝置將新增到 KME 主控台中。
   - **NFC**。將管理員的行動裝置帶至使用者的行動裝置附近，並傳輸 KNOX MDM 設定檔。
     在使用者的行動裝置上，將提示安裝 KNOX MDM 設定檔。帶有 **NFC** 標籤的新裝置會新增到 KME 主控台中。

安裝應用程式

在安裝 Kaspersky Endpoint Security for Android 應用程式之前，在卡巴斯基安全管理中心管理主控台中為行動裝置使用者頒發一般憑證。辨識卡巴斯基安全管理中心管理主控台中的行動裝置使用者需要一般憑證。

在開始佈署 KNOX MDM 設定檔之後，APK 安裝檔案將自動下載到行動裝置上。Kaspersky Endpoint Security for Android 應用程式安裝將自動啟動。使用者必須接受 Samsung KNOX 產品授權協議和 Kaspersky Endpoint Security for Android 產品授權協議。無需其他應用程式配置。在安裝了應用程式之後，將自動執行與卡巴斯基安全管理中心同步。行動裝置將新增至卡巴斯基安全管理中心管理主控台中 KNOX MDM 設定檔設定中指定的管理群組中 (`groupName`)。

配置 KNOX 容器

本節包含有關在執行 Android 的 Samsung 裝置上使用 KNOX 容器的資訊。

只能在執行 Android 版本 6.0 或更高版本的 Samsung 裝置上使用 KNOX 容器。

關於 KNOX 容器

*KNOX 容器*是使用者裝置上的一個安全環境，具有自己的桌面、啟動面板、應用程式和小工具。KNOX 容器可讓您將企業應用程式和資料與個人應用程式和資料隔離。KNOX 容器是 Samsung KNOX 行動解決方案的一個元件。

Samsung KNOX 是一個配置和防護執行 Android 作業系統的 Samsung 行動裝置的行動裝置解決方案。有關 Samsung KNOX 的更多詳細資訊，請造訪*Samsung 技術支援網站*。

KNOX 容器允許您在行動裝置上隔離個人資料和公司資料。例如，使用個人信箱無法傳送位於 KNOX 容器中的檔案。如果員工的個人行動裝置用於處理公司資料，建議您佈署 KNOX 容器。

若要使用 KNOX 容器，必須啟動 Samsung KNOX。在將裝置與卡巴斯基安全管理中心同步後，將提示行動裝置的使用者安裝 KNOX 容器。在安裝 KNOX 容器之前，使用者必須接受 Samsung 最終使用者授權合約的條款。

安裝 KNOX 容器後，將向行動裝置的桌面新增 KNOX 圖示  。否則工作台將新增至行動裝置的應用程式清單。若要使用公司資料，使用者需要從 KNOX 容器啟動應用程式。

Kaspersky Endpoint Security for Android 不會安裝至 KNOX 容器，並且不會保護企業資料。Kaspersky Endpoint Security for Android 不會在 KNOX 容器中偵測惡意檔案下載並封鎖惡意網站。您無法在 KNOX 容器中控制應用程式或禁止使用相機。Kaspersky Endpoint Security for Android 僅會保護私密資料。您可透過 Samsung KNOX 工具保護企業資料。有關 Samsung KNOX 的更多詳細資訊，請造訪*Samsung 技術支援網站*。

啟動 Samsung KNOX

若要在使用者的行動裝置上使用 KNOX 的功能，您必須啟動 Samsung KNOX。啟動 Samsung KNOX 的過程取決於使用者裝置上安裝的 Kaspersky Endpoint Security for Android 版本：

- 如果裝置上安裝了目前版本的 Kaspersky Endpoint Security for Android，您不需要任何金鑰來啟動 Samsung KNOX。
- 如果裝置上安裝了舊版本的 Kaspersky Endpoint Security for Android（10.8.3.174 或更早版本），您需要從 Samsung 獲取 KNOX License Manager 金鑰（以下簡稱 KLM 金鑰）。*KNOX License Manager 金鑰*是 Samsung KNOX 產品授權系統使用的唯一代碼。如需 KLM 金鑰的詳細資訊，請參閱 Samsung KNOX 技術支援網站。

只有在 Samsung 裝置上才能使用 KNOX 容器。

若要啟動 Samsung KNOX，請執行以下操作：

1. 在主控台樹狀目錄的「**受管裝置**」資料夾中，選擇 Android 裝置所屬的管理群組。
2. 在所選群組的工作台中，選擇「**政策**」標籤。
3. 透過按兩下任何資料欄來開啟政策內容視窗。
4. 在政策「**內容**」視窗中選擇「**管理 Samsung KNOX**」→「**KNOX 容器**」區域。
5. 在**KNOX License Manager 金鑰**欄位中，指定以下內容：
   - 如果裝置上安裝了目前版本的 Kaspersky Endpoint Security for Android，請鍵入任意字元。

- 如果裝置上安裝了舊版本的 Kaspersky Endpoint Security for Android（10.8.3.174 或更早版本），請輸入從 Samsung 收到的 KLM 金鑰。

6. 將「鎖定」內容設定在鎖定位置。
7. 點擊「**套用**」按鈕以儲存所作的變更。

Samsung KNOX 將在下一次與卡巴斯基安全管理中心同步後啟動。系統將提示使用者接受 Samsung 的最終使用者授權協議條款並安裝 KNOX 容器。

若要停用 Samsung KNOX，請執行以下操作：

1. 在主控台樹狀目錄的「**受管裝置**」資料夾中，選擇 Android 裝置所屬的管理群組。
2. 在所選群組的工作台中，選擇「**政策**」標籤。
3. 透過按兩下任何資料欄來開啟政策內容視窗。
4. 在政策「**內容**」視窗中選擇「**管理 Samsung KNOX**」→「**KNOX 容器**」區域。
5. 清除 **KNOX License Manager 金鑰**欄位值。
6. 點擊「**套用**」按鈕以儲存所作的變更。

Samsung KNOX 將在下一次與卡巴斯基安全管理中心同步後啟動。將封鎖對 KNOX 容器的存取。

Samsung KNOX 限制

- KNOX 容器僅適用於 Samsung 裝置。
- 在支援 KNOX 2.6、2.7 和 2.7.1 的Samsung裝置上，Web 防護和應用程式控制無法在 KNOX 容器中執行。該問題與 KNOX 容器中缺少所需權限有關（輔助使用功能服務）。在支援 KNOX 2.8 或更新版本的裝置上，應用程式的所有元件可以無限制執行。
- 由於 Samsung KNOX 的更新，Service Pack 4 Maintenance Release 3 Update 2 以前的 Kaspersky Endpoint Security for Android 版本在 Samsung Android 10 裝置上的運作可能會不穩定。建議將 Kaspersky Endpoint Security for Android 更新至 Service Pack 4 Maintenance Release 3 Update 2 版本。

在 KNOX 中設定防火牆

您應配置防火牆設定以監視 KNOX 容器中的網路連線。

若要在 KNOX 容器中設定防火牆，請執行以下操作：

1. 在主控台樹狀目錄的「**受管裝置**」資料夾中，選擇 Android 裝置所屬的管理群組。
2. 在所選群組的工作台中，選擇「**政策**」標籤。
3. 透過按兩下任何資料欄來開啟政策內容視窗。
4. 在政策「**內容**」視窗中選擇「**管理 Samsung KNOX**」→「**KNOX 容器**」區域。

5. 在「**防火牆**」視窗中，點擊「**設定**」。
   「**防火牆**」視窗將開啟。

6. 選擇防火牆設定：

   - 若要允許所有傳送和接收連線，請將滑塊滑動到「**全部允許**」。
   - 若要封鎖除排除清單中的應用程式的網路活動以外的所有網路活動，請將滑桿向上滑動到「**全部封鎖（排除項目除外）**」。

7. 如果您已將防火牆模式設定為「**全部封鎖（排除項目除外）**」，請建立排除清單：

   a. 點擊「**新增**」。
      這將開啟「**防火牆排除項目**」視窗。

   b. 在「**應用程式名稱**」欄位中輸入行動 APP 的名稱。

   c. 在「**套件名稱**」欄位中輸入行動 APP 套件的系統名稱（例如 `com.mobileapp.example`）。

   d. 點擊「**確定**」。

8. 點擊「**套用**」按鈕以儲存所作的變更。

與卡巴斯基安全管理中心的下個裝置同步之後可配置行動裝置設定。

在 KNOX 中設定 Exchange 信箱

若要在 KNOX 容器中使用公司郵件、聯絡人和行事曆，應配置 Exchange 信箱設定。

若要在 KNOX 容器中設定 Exchange 信箱，請執行以下操作：

1. 在主控台樹狀目錄的「**受管裝置**」資料夾中，選擇 Android 裝置所屬的管理群組。
2. 在所選群組的工作台中，選擇「**政策**」標籤。
3. 透過按兩下任何資料欄來開啟政策內容視窗。
4. 在政策「**內容**」視窗中選擇「**管理 Samsung KNOX**」→「**KNOX 容器**」區域。
5. 在「**Exchange ActiveSync**」區域中，點擊「**配置**」按鈕。
   「**Exchange 郵件伺服器設定**」視窗將開啟。
6. 在「**伺服器位址**」欄位中，輸入託管郵件伺服器的伺服器的 IP 位址或 DNS 名稱。
7. 在「**網域**」欄位中，輸入公司網路上的行動裝置使用者的網域名稱。
8. 在「**同步間隔**」下拉清單中，選擇行動裝置與 Microsoft Exchange 伺服器所需的同步時間間隔。
9. 若要使用 SSL（安全通訊端層）資料傳輸協議，請選擇「**使用 SSL 連線**」核取方塊。
10. 若要使用數位憑證防護行動裝置與 Microsoft Exchange 伺服器之間的資料傳輸，請選擇「**驗證伺服器憑證**」核取方塊。

11. 點擊「**套用**」按鈕以儲存所作的變更。

與卡巴斯基安全管理中心的下個裝置同步之後可配置行動裝置設定。

附錄

本章節提供補充文件內容的資訊。

設定群組政策的權限

卡巴斯基安全管理中心管理員可以根據管理主控台使用者的工作職責，配置該使用者存取不同應用程式功能的權限。

對於每個功能方面，管理員可以分配以下權限：

- **允許編輯**。允許管理主控台使用者在內容視窗中變更政策設定。
- **封鎖編輯**。禁止管理主控台使用者在內容視窗中變更政策設定。屬於該權限分配至的功能範圍的政策標記不會顯示在介面中。

存取 Kaspersky Endpoint Security 管理外掛程式的權限

功能範圍	政策區域
Android 企業	Android 工作設定檔
竊盜防護	竊盜防護
應用程式控制	應用程式控制
防護	防護，掃描，更新
規性控制	規性控制
容器	容器
裝置設定	裝置控制，同步
管理 Samsung 裝置	APN、管理 Samsung 裝置、KNOX 容器
系統管理	進階，Wi-Fi
Web 防護	Web 防護

存取 Kaspersky Device Management for iOS 管理外掛程式各部分的權限

功能範圍	政策區域
其他	網路我的最愛，字型，AirPlay，AirPrint
Exchange ActiveSync	一般，密碼，同步，功能限制，應用程式限制
一般	一般，單點登入，Web 防護，Wi-Fi，存取點名稱 (APN)，Exchange ActiveSync，電子郵件，自訂有效載荷
LDAP（行事曆/聯絡人）	LDAP，行事曆，聯絡人，行事曆訂購
限制和安全	功能限制，應用程式限制，對媒體內容的限制，密碼，VPN，全域 HTTP 代理，憑證，SCEP

應用程式類別

應用程式控制支援應用程式類別。為應用程式類別配置的執行模式將套用至該類別中的所有應用程式。每個應用程式的類別由卡巴斯基安全網路雲端服務進行確定。

應用程式類別

類別	描述
娛樂	互動娛樂應用程式。
即時通訊用戶端，移動訊息傳送應用程式	透過 IP 的即時訊息，語音和視訊通訊應用程式。
社群網路	使用社群網路和博客的應用程式。
商業軟體	稅務計算、銀行操作管理、表格處理、記帳和其他商用應用程式。文字編輯器。
家庭，家人，愛好，健康	菜譜，時尚小貼士應用程式。鍛煉，工作外排程、獲得節食、健康營養、安全和預防事故的應用程式。
醫療	包括症狀和藥物類別的應用程式，提供健康護理專家、健康護理雜誌和新聞資訊的應用程式。
多媒體	提供電影訂購、媒體模仿其和視訊播放機的服務。音樂服務，播放機，廣播。
圖形設計軟體	使用攝影鏡頭、圖形編輯器的應用程式，用於管理和發佈照片的應用程式。
閱讀新聞和 RSS 的外掛程式	用於閱讀報紙、雜誌、博客、新聞聚合的應用程式。
天氣	顯示天氣預報的應用程式。
教育應用程式	閱讀器，手冊，課本，字典，索銀典，百科全書。有助於考試、培訓材料、字典、智力開發遊戲、語言學習工具的應用程式。
線上購物	用於線上購物和競價，禮品券，比價工具的應用程式，購物單應用程式，用於閱讀產品回饋的應用程式。
啟動實用程式	用於重新設計桌面、小工具和捷徑的應用程式。
作業系統和實用程式	提供作業系統管理、使用者互動和記憶體管理的系統應用程式。
地圖檢視	城市手冊，有關當地商業的資訊，旅行規劃工具。
其他應用程式	軟體庫，技術展示版本應用程式。未包含在任何類別中的應用程式。
運輸	使用公共交通、導航工具的應用程式，司機使用的應用程式。
遊戲	街機遊戲、博彩、賽車、其他、老虎機、棋牌遊戲、音樂、桌遊、遊覽、拼圖、冒險、RPG、模擬器、單詞遊戲、體育遊戲、戰略遊戲、動作。
瀏覽器	用於檢視網站的應用程式，網頁文件和檔案的內容。用於管理網頁應用程式的應用程式。
開發工具	用於開發軟體的應用程式。偵錯工具、編譯器、代碼編輯器、圖形化使用者介面編輯器。
OS 應用程式	與作業系統一起使用的應用程式，作業系統正常執行所需的應用程式。
網際網路應用程式	下載管理器、郵件用戶端、網頁搜尋應用程式和其他方便瀏覽網際網路的應用程式。
網路基礎結構軟體	用於管理公司網路內伺服器、資料儲存裝置、網路裝置、軟體的應用程式和完整

	基礎結構自動化和集成應用程式。
聯網軟體	用於組織多個裝置上使用者組協作，在裝置間溝通的應用程式。
系統實用程式	與作業系統一起提供的應用程式：檔案管理員、壓縮工具、用於軟硬體診斷的實用程式、記憶體優化工具、移除程式、處理器管理實用程式。
安全軟體	裝置資料防護應用程式。偵測和消除裝置上威脅的應用程式。防火牆。資料加密應用程式。
下載管理器	用於從外部資源下載檔案的應用程式。
用於在網際網路上儲存檔案的應用程式	用於管理檔案、備註和多媒體的線上儲存。
參考系統	閱讀器，手冊，課本，字典，索銀典，維琪百科全書。
電子郵件應用程式	用於傳送和接收電子郵件訊息的應用程式。

使用 Kaspersky Endpoint Security for Android 應用程式

本說明部分介紹了 Kaspersky Endpoint Security for Android 應用程使用者可用的功能和操作。

本節文章說明可在行動裝置上使用或顯示的選項。該應用程式的實際版面配置與行為將根據遠端管理系統實作情況而定，以及管理員如何根據企業安全需求配置您的裝置。本節說明的有些功能與選項可能不是用於您在該應用程式中的實際體驗。如對您特定裝置的應用程式有任何問題，請聯絡您的管理員。

程式功能

Kaspersky Endpoint Security 提供以下主要功能：

病毒和其他惡意軟體防護

該應用程式使用病毒防護元件防護裝置，防禦病毒和其他惡意軟體。

病毒防護可執行以下功能：

- 掃描整個裝置、已安裝的應用程式或者選定的資料夾以搜尋威脅
- 即時防護您的裝置
- 在已安裝的應用程式第一次啟動之前掃描
- 更新病毒資料庫

如果在行動裝置上安裝的應用程式會收集資訊並傳送這些資訊進行處理，則 Kaspersky Endpoint Security for Android 會將此應用程式歸類為惡意軟體。

應用程式控制

根據企業安全性需求，*遠端管理系統的管理員*會建立建議、封鎖和所需應用程式的清單。應用程式控制元件用於安裝建議和所需的應用程式，更新它們並且移除被封鎖的應用程式。

利用應用程式控制，您可以透過指向分發套件的直接連結或指向 Google Play 的連結，將推薦和必需的應用程式安裝到您的裝置上。應用程式控制還允許您移除那些違反企業安全需求的已封鎖應用程式。

必須將 Kaspersky Endpoint Security 設定為可存取功能服務以確保應用程式控制能正常執行。如果在應用程式的初始配置精靈階段沒有啟用這個服務，則您可以在「**狀態**」區域中選擇適當的通知或裝置設定 (**Android 設定 → 可存取 → 服務**)，就能夠以可存取功能服務的方式來啟用 Kaspersky Endpoint Security。

防護被竊取或遺失的裝置資料

竊盜防護元件防護您的資料免受未授權的存取，裝置遺失或被竊時能定位裝置位置。

竊盜防護功能可以遠端執行以下動作：

- 鎖定裝置。

  要防止駭客擁有鎖定該裝置的能力，必須在執行 Android 7.0 或更新版本的行動裝置上將 Kaspersky Endpoint Security 啟用為可存取功能服務。

- 開啟裝置的聲音警報，即使該裝置已停用聲音。
- 獲取裝置的位置地圖座標。
- 抹除裝置上儲存的資料。
- 重設為出廠設定。
- 秘密拍下使用您裝置的人員臉部快照。

要啟用竊盜防護操作，必須將 Kaspersky Endpoint Security 啟用為裝置管理員。如果在應用程式的初始配置時沒有授予管理員權限，則您可以在「**狀態**」區域中選擇適當的通知，或是在裝置設定中 (**Android 設定 → 安全 → 裝置管理員**) 授予 Kaspersky Endpoint Security 此權限。

防禦線上威脅

Web 防護元件防護裝置防禦線上威脅。

Web 防護可封鎖散佈惡意程式碼的惡意網站和釣魚網站，例如用於竊取個人資料和銀行帳戶的網站。Web 防護將在您開啟網站前使用卡巴斯基安全網路雲端服務掃描網站。

啟用 Web 防護：

- 必須將 Kaspersky Endpoint Security 啟用為可存取功能服務。
- 您必須同意利用 Web 防護進行資料處理的聲明 (Web 防護聲明)。Kaspersky Endpoint Security 使用卡巴斯基安全網路 (KSN) 來掃描網站。Web 防護聲明包含與 KSN 交換資料的條款。

  您的管理員能夠在卡巴斯基安全管理中心代您接受 Web 防護條款。在這個情況下，您不需要進行任何動作。

  如果管理員沒有接受 Web 防護條款，並要求您進行接受，則您必須在應用程式設定中閱讀並接受 Web 防護條款。

  如果管理員沒有同意 Web 防護條款，則 Web 防護不可用。

Android 裝置上的 Web 防護僅在 Google Chrome 瀏覽器（包括自訂標籤功能）、Huawei Browser 和 Samsung Internet Browser 中可用。如果使用工作設定檔且只針對工作設定檔啟用 Web 防護，則 Samsung Internet Browser 的 Web 防護不會封鎖行動裝置上的網站。

主介面總覽

主視窗的介面根據螢幕解析度不同而有輕微變化。

在出現可能會導致防護等級降低、裝置感染或資訊遺失問題時，主螢幕的外觀會發生變化。

狀態區段會顯示以下資訊：

- 裝置防護相關問題
- 有關您的裝置是否符合企業安全需求的資訊
- 有關裝置防護狀態的資訊

輕觸 Kaspersky Endpoint Security 主介面的上方就能夠開啟「**狀態**」區域。

裝置防護方面的問題

防護問題按類別分組。針對每一個問題，列出解決問題可以採取的行動。

狀態區域也顯示應用程式偵測到但略過的威脅。略過的威脅清單可能會變更，例如，如果可疑檔案被刪除或移動。若要接收最新的威脅清單，請執行完整裝置掃描。為了確保可靠地防護您的資料，請解毒所有偵測到的物件。

共有兩種防護問題類型。

- *通知問題*。用黃色突出顯示。通知問題告知使用者會影響裝置安全的事件 (舉例來說：上次掃描距今已超過 14 天，或是新安裝的應用程式尚未掃描)。您可以隱藏通知問題。之後，問題的相關資訊能夠在「**隱藏的問題**」功能表中取得。
- *緊急*。用紅色突出顯示。緊急問題通知對裝置安全極為重要的事件（例如病毒資料庫很久沒有更新，或是在裝置上安裝被封鎖的應用程式）。重要問題無法隱藏。

規性控制

應用程式自動檢查裝置是否符合公司安全性需求。「**狀態**」區域還顯示有關裝置是否符合公司安全性需求的資訊。

- 裝置不符合企業安全需求的原因 (例如，在裝置上偵測到被封鎖的應用程式)。
- 您必須消除不合規問題的時間段 (例如，24 小時)。
- 如果您未在規定的時間內解決不合規問題，將對裝置採取的措施（例如鎖定裝置）。
- 為了解決裝置不符合企業安全需求而執行的操作。

狀態欄中的圖示

首次安裝精靈結束後，Kaspersky Endpoint Security 圖示會顯示在狀態欄。

該圖示顯示應用程式的動作並提供存取 Kaspersky Endpoint Security 主介面的方法。

該圖示表示 Kaspersky Endpoint Security 正在執行，並反映裝置的防護狀態：

– 裝置受到防護。

– 發生防護問題（例如，病毒資料庫過時，或尚未掃描新安裝的應用程式）。

裝置掃描

病毒防護有一些限制：

- 當病毒防護正在執行時，在裝置外部記憶體（例如 SD 卡）中偵測到的威脅無法在工作設定檔中自動解毒（具備公事包圖示的應用程式、配置 Android 工作設定檔）。Kaspersky Endpoint Security for Android 在工作設定檔中不能存取外部記憶體。已偵測物件的相關資訊會顯示在應用程式的**狀態**區域。要解毒在外部記憶體中偵測到的物件，物件檔案必須被手動移除且裝置掃描必須重啟。

- 由於技術限制，Kaspersky Endpoint Security for Android 無法掃描大小為 2 GB 或更大的檔案。在掃描期間，應用程式將略過此類別檔案，而不會通知您此類別檔案被略過。

開始裝置掃描的步驟：

1. 在 Kaspersky Endpoint Security 主介面的快速啟動面板中輕觸「**掃描**」。

2. 選擇裝置掃描範圍：

   - **掃描整個裝置**。應用程式掃描裝置的整個檔案系統。

   - **掃描已安裝的應用程式**。應用程式僅掃描已安裝的應用程式。

   - **自訂掃描**。應用程式掃描指定資料夾或單個檔案。可選擇單個物件 (資料夾或檔案) 或以下裝置儲存區之一：

     - **裝置記憶體**。整個裝置的可讀儲存區。還包括用於儲存作業系統檔案的系統儲存區。

     - **內部記憶體**。用於安裝應用程式和儲存媒體內容、文件和其他檔案的裝置記憶體分割區。

     - **外部記憶體**。外部 SD 卡儲存區。如果未安裝外部 SD 卡，則將隱藏此選項。

到病毒掃描設定的存取可能被管理員限制。

配置病毒掃描：

1. 在 Kaspersky Endpoint Security 主視窗的快速啟動面板中，輕觸 → **設定** → **病毒防護** → **掃描**。

2. 如果您要讓應用在執行掃描時偵測可以被駭客使用以損壞您的裝置或資料的惡意軟體和應用，開啟**廣告軟體，撥號軟體和其他**按鈕。

3. 點擊**偵測到威脅時執行的操作**，然後選擇應用程式預設執行的操作：

   - **隔離**

     應用程式會將存檔形式隔離檔案，不會對裝置造成傷害。隔離區允許您刪除或還原移動至隔離區的檔案。

   - **請求操作**

     應用會提示您為偵測到的每個物件選擇一種操作：略過、隔離或刪除。當偵測到多個物件時，您可以對所有物件套用所選操作。

   - **刪除**

偵測到的物件將被自動刪除。不需要附加操作。移除物件之前，Kaspersky Endpoint Security 將顯示偵測到物件的暫時通知。

- **略過**

  如果偵測到的物件被略過，Kaspersky Endpoint Security 會警告您裝置防護方面存在的問題。有關略過的物件的資訊會顯示在應用程式的「**狀態**」部分中。對於每個略過的威脅，應用程式都提供您可以執行以消除威脅的操作。略過的威脅清單可能會變更，例如，如果可疑檔案被刪除或移動。若要接收最新的威脅清單，請執行完整裝置掃描。為了確保可靠地防護您的資料，請解毒所有偵測到的物件。

關於偵測到的威脅以及對它們執行的操作的資訊都會記錄在應用程式報告中。（ → **報告**）您可以選擇顯示病毒防護操作報告。

執行排程掃描

病毒防護有一些限制：

- 當病毒防護正在執行時，在裝置外部記憶體（例如 SD 卡）中偵測到的威脅無法在工作設定檔中自動解毒（具備公事包圖示的應用程式、配置 Android 工作設定檔）。Kaspersky Endpoint Security for Android 在工作設定檔中不能存取外部記憶體。已偵測物件的相關資訊會顯示在應用程式的**狀態**區域。要解毒在外部記憶體中偵測到的物件，物件檔案必須被手動移除且裝置掃描必須重啟。

- 由於技術限制，Kaspersky Endpoint Security for Android 無法掃描大小為 2 GB 或更大的檔案。在掃描期間，應用程式將略過此類別檔案，而不會通知您此類別檔案被略過。

要為裝置配置完整掃描排程：

1. 在 Kaspersky Endpoint Security 主視窗的快速啟動面板中，輕觸 → **設定** → **病毒防護** → **掃描**。
2. 輕觸**排程**並選擇完整掃描的頻率：
   - **每週**
   - **每天**
   - **已停用**
   - **資料庫更新之後**
3. 點擊**開始日期**並選擇一周中預計啟動病毒掃描的那一天。
4. 點擊**開始時間**並選擇啟動完整掃描的時間。

根據排程啟動裝置完整掃描。

在 Android 12 或更高版本上，若裝置處於省電模式，應用程式執行此任務的時間可能會晚於指定時間。

變更防護模式

即時防護允許您偵測正在開啟檔案中的威脅，並掃描被即時安裝到裝置的應用。病毒防護資料庫和卡巴斯基安全網路雲端服務 (雲端防護) 用於自動確保安全。

變更裝置防護模式的步驟：

1. 在 Kaspersky Endpoint Security 主介面的快速啟動視窗中，輕觸 → **設定→病毒防護→即時防護模式**。
2. 選擇裝置防護模式：
   - **停用**。關閉「防護」功能。
   - **建議**。病毒防護僅掃描從 Downloads 資料夾中安裝的應用程式和檔案。新應用程式安裝完畢後，病毒防護會立即對其掃描。
   - **Extended**。在對所有裝置檔案執行任何操作 (例如當儲存、移動或變更裝置檔案時)，病毒防護掃描這些檔案是否存在惡意物件。另外，新應用程式安裝完畢時，病毒防護也會立即對其掃描。

有關目前防護模式的資訊顯示在元件敘述下方。

到即時防護設定的存取可能被管理員限制。

雲端防護 (KSN)：

1. 在 Kaspersky Endpoint Security 主介面的快速啟動面板中輕觸 → **設定 →病毒防護**。
2. 開啟**雲端防護 (KSN)** 按鈕。

   雲端防護 (KSN) 按鈕僅為裝置的即時防護管理卡巴斯基安全網路的使用。如果清空該方塊，Kaspersky Endpoint Security 繼續使用 KSN 以方便應用其他元件的操作。

結果，應用獲得到關於檔案和應用信譽的 Kaspersky 線上知識庫的存取。此項掃描旨在掃描威脅資訊尚未新增到病毒資料庫但已包含在 KSN 中的威脅。卡巴斯基安全網路雲端服務提供病毒防護的完整操作並降低誤報。僅您的管理員可以完全停用卡巴斯基安全網路的使用。

要設定即時防護：

1. 在 Kaspersky Endpoint Security 主介面的快速啟動視窗中，輕觸 →「**設定**」→「**病毒防護**」→「**即使防護模式**」。
2. 如果您要讓應用在執行掃描時偵測可以被駭客使用以損壞您的裝置或資料的惡意軟體和應用，開啟**廣告軟體，撥號軟體和其他**按鈕。
3. 點擊**偵測到威脅時執行的操作**，然後選擇應用程式預設執行的操作：
   - **隔離**

     應用程式會將存檔形式隔離檔案，不會對裝置造成傷害。隔離區允許您刪除或還原移動至隔離區的檔案。
   - **刪除**

     偵測到的物件將被自動刪除。不需要附加操作。移除物件之前，Kaspersky Endpoint Security 將顯示偵測到物件的暫時通知。
   - **略過**

如果偵測到的物件被略過，Kaspersky Endpoint Security 會警告您裝置防護方面存在的問題。有關略過的物件的資訊會顯示在應用程式的「**狀態**」部分中。對於每個略過的威脅，應用程式都提供您可以執行以消除威脅的操作。略過的威脅清單可能會變更，例如，如果可疑檔案被刪除或移動。若要接收最新的威脅清單，請執行完整裝置掃描。為了確保可靠地防護您的資料，請解毒所有偵測到的物件。

有關偵測到的威脅以及對它們執行的操作的資訊會記錄在應用程式報告中（→ **設定** → **報告**）。您可以選擇顯示病毒防護操作報告。

病毒資料庫更新

更新應用程式的病毒資料庫的步驟：

在 Kaspersky Endpoint Security 主介面的快速啟動面板中輕觸**資料庫更新**。

排程的資料庫更新

應用程式可以根據您指定的排程自動更新病毒資料庫。

配置更新排程的步驟：

1. 在 Kaspersky Endpoint Security 主介面的快速啟動面板中，輕觸→ **設定** → **病毒防護** → **資料庫更新**。
2. 點擊**排程**並選擇更新的頻率：
   - **每週**
   - **每天**
   - **已停用**
3. 點擊**開始日期**並選擇一周中預計執行更新的那一天。
4. 點擊**開始時間**並選擇啟動更新的時間。

根據排程啟動病毒資料庫更新。

在 Android 12 或更高版本上，若裝置處於省電模式，應用程式執行此任務的時間可能會晚於指定時間。

裝置遺失或被竊取時該如何操作

若您的裝置遺失或遭竊，請聯絡您的系統管理員。管理員可根據企業安全需求，在您的裝置上遠端執行竊盜防護命令。

如果向裝置發送完全重設命令，則將失去對裝置的控制，其餘的防盜命令將無法運作。

Web 防護

啟用 Web 防護：

- 必須將 Kaspersky Endpoint Security 啟用為可存取功能服務。
- 您必須同意利用 Web 防護進行資料處理的聲明 (Web 防護聲明)。Kaspersky Endpoint Security 使用卡巴斯基安全網路 (KSN) 來掃描網站。Web 防護聲明包含與 KSN 交換資料的條款。

  您的管理員能夠在卡巴斯基安全管理中心代您接受 Web 防護條款。在這個情況下，您不需要進行任何動作。

  如果管理員沒有接受 Web 防護條款，並要求您進行接受，則您必須在應用程式設定中閱讀並接受 Web 防護條款。

  如果管理員沒有同意 Web 防護條款，則 Web 防護不可用。

Android 裝置上的 Web 防護僅在 Google Chrome 瀏覽器（包括自訂標籤功能）、Huawei Browser 和 Samsung Internet Browser 中可用。如果使用工作設定檔且只針對工作設定檔啟用 Web 防護，則 Samsung Internet Browser 的 Web 防護不會封鎖行動裝置上的網站。

若要在瀏覽網路時始終使用 Web 防護，請將 Google Chrome 或 Samsung Internet Browser 設定為預設瀏覽器。

要將支援的瀏覽器設定為預設瀏覽器並在瀏覽網頁時始終使用 Web 防護：

1. 在 Kaspersky Endpoint Security 主介面的快速啟動面板中輕觸→**設定**→**Web 防護**。
2. 將 **Web 防護**切換開關設為「開啟」。
3. 點按**設定預設瀏覽器**。

   如果 Web 防護已啟用且支援的瀏覽器並未設為預設瀏覽器，則會顯示這個按鈕。

   啟動預設瀏覽器選擇精靈。
4. 按照精靈指示執行操作。

   精靈可將 Google Chrome、Huawei Browser 或 Samsung Internet Browser 設定為預設瀏覽器。在您瀏覽網頁時，「Web 防護」功能將會始終掃描網站。

應用程式控制

*應用程式控制*會檢查安裝在行動裝置上的應用程式，確認是否符合企業安全性政策。在卡巴斯基安全管理中心，管理員根據企業安全需求建立允許、封鎖、強制和建議的應用程式的清單。作為應用程式控制的結果，Kaspersky Endpoint Security 會提示您安裝必要和建議的應用程式以及移除被封鎖的應用程式。您無法在行動裝置上啟動被封鎖的應用程式。

若要安裝必要和建議的應用程式或移除被封鎖的應用程式，請執行以下操作：

1. 請參閱 Kaspersky Endpoint Security 中的「**狀態**」區域。
2. 選擇應用程式控制工作。
3. 執行建議的操作。

取得憑證

獲取用於目前公司網路資源的憑證的步驟：

1. 在 Kaspersky Endpoint Security 主介面的快速啟動面板中輕觸 → **設定** → **其他** → **取得憑證**。
2. 指定您的公司網路帳戶憑證。
3. 如果您收到管理員傳來的一次性密碼，請選擇「**一次性密碼**」核取方塊並輸入收到的密碼。
   將啟動憑證安裝精靈。
4. 按照精靈指示執行操作。

與卡巴斯基安全管理中心同步

若要按照企業安全需求來防護或設定裝置，您需要將行動裝置與卡巴斯基安全管理中心遠端管理系統同步。裝置可與卡巴斯基安全管理中心自動同步，並且您也可以手動啟動同步。第一次同步後，您的裝置會新增到透過卡巴斯基安全管理中心管理的行動裝置清單中。然後，管理員可以依據企業安全需求配置您的裝置。

您可以在執行初始設定精靈或在 Kaspersky Endpoint Security 的設定中配置同步設定。如果使用 Google Play 安裝 Kaspersky Endpoint Security，必須配置同步設定。向系統管理員請求同步設定值。

僅當管理員要求時，才可以使用卡巴斯基安全管理中心遠端管理系統修改裝置同步設定。

要將您的裝置與卡巴斯基安全管理中心同步：

1. 在 Kaspersky Endpoint Security 主介面的快速啟動面板中輕觸 → **設定** → **同步**。
2. 在**同步設定**區域中指定下列設定的數值：
   - **伺服器**
   - **連接埠**
   - **群組**
   - **企業電子郵件地址**

   管理員可以隱藏同步設定。
3. 輕觸「**同步**」。

不使用卡巴斯基安全管理中心啟動 Kaspersky Endpoint Security for Android 應用程式

在大多數情況下，安裝在您裝置上的 Kaspersky Endpoint Security for Android 應用程式是由管理員在卡巴斯基安全管理中心遠程管理系統中集中啟用。如果您的裝置未連線卡巴斯基安全管理中心，您可以手動輸入啟動碼。要獲取啟用碼，請聯絡管理員。

僅在管理員指示時手動啟用應用程式。

輸入啟動碼：

1. 在顯示您的產品授權即將過期或已過期並且您的裝置未連線到管理伺服器的錯誤訊息中，點擊**啟用**。
2. 在啟動視窗中，輸入管理員給您的啟動碼，然後點擊**啟動**。
3. 如果啟動碼正確，則會顯示一則通知，說明該應用程式已啟用以及授權到期日期。

您裝置上的 Kaspersky Endpoint Security for Android 應用程式已啟用。

在 Android 13 啟用協助工具

在 Android 13，對於不是從 Google Play 或 Huawei AppGallery 下載的應用程式，協助工具服務受到限制。若您已從卡巴斯基安全管理中心伺服器或卡巴斯基網站下載 Kaspersky Endpoint Security for Android，您應手動允許協助工具服務。

協助工具用於下列用途：

- 檢查卡巴斯基安全網路中的網站和應用程式
- 在遭竊時鎖定裝置
- 顯示警告
- 在受到管理員限制時封鎖相機

若要為 Kaspersky Endpoint Security 啟用協助工具：

1. 在裝置設定中開啟**協助工具**頁面，並找到 Kaspersky Endpoint Security。
2. 開啟 Kaspersky Endpoint Security 開關。在表示協助工具服務受到限制的對話方塊中，點選**確定**。
   您現在可以向 Kaspersky Endpoint Security 提供受限設定的存取權限。
3. 在裝置設定中開啟 Kaspersky Endpoint Security 資訊頁面。例如，前往**設定** > **應用程式**，然後在應用程式清單中尋找應用程式。
4. 在 Kaspersky Endpoint Security 資訊頁面，點選右上角的 ⋮ 並選取**允許受限設定**功能表項目。
   Kaspersky Endpoint Security 現在可存取受限設定。
5. 返回裝置設定中的**協助工具**頁面，並找到 Kaspersky Endpoint Security。
6. 開啟 **Kaspersky Endpoint Security** 開關。在開啟的對話方塊中，允許應用程式完全控制裝置。

現在已為 Kaspersky Endpoint Security 啟用協助工具服務。
若要為 Kaspersky Endpoint Security 啟用協助工具：

1. 在要求您開啟協助工具服務的對話方塊中，點選**開啟**。
   就會開啟裝置設定中的**協助工具**頁面。
2. 開啟 Kaspersky Endpoint Security 開關。在表示協助工具服務受到限制的對話方塊中，點選**確定**。
   您現在可以向 Kaspersky Endpoint Security 提供受限設定的存取權限。
3. 在裝置設定中開啟 Kaspersky Endpoint Security 資訊頁面。例如，前往**設定** > **應用程式**，然後在應用程式清單中尋找應用程式。
4. 在 Kaspersky Endpoint Security 資訊頁面，點選右上角的 ⋮ 並選取**允許受限設定**功能表項目。
   Kaspersky Endpoint Security 現在可存取受限設定。
5. 透回應用程式並在要求您開啟協助工具服務的對話方塊中，點選**開啟**。
   就會開啟裝置設定中的**協助工具**頁面。
6. 開啟 **Kaspersky Endpoint Security** 開關。在開啟的對話方塊中，允許應用程式完全控制裝置。

現在已為 Kaspersky Endpoint Security 啟用協助工具服務。

更新應用程式

Kaspersky Endpoint Security 可透過下列方式更新：

- 使用 Google Play 手動更新。您可以從 Google Play 中下載應用程式的新版本，然後在您的裝置中進行安裝。
- 在管理員的幫助下更新。管理員可以使用卡巴斯基安全管理中心遠端管理系統，遠端更新您裝置上的應用程式版本。

從 Google Play 更新應用程式

管理員可以封鎖您從 Google Play 更新應用程式。

透過執行 Android 平台的標準更新步驟，您可以從 Google Play 更新本應用程式。要更新應用程式，必須滿足下列條件：

- 您必須擁有 Google 帳戶。
- 裝置必須已連線至您的 Google 帳戶。
- 裝置必須已連線網際網路。

若要深入瞭解如何建立 Google 帳戶，將裝置連結至您的帳戶，或是利用 Google Play Store 操作，請參閱 Google 支援網站。

透過卡巴斯基安全管理中心更新應用程式

透過卡巴斯基安全管理中心更新套用應用程式含以下步驟：

1. 管理員向您的行動裝置傳送其版本符合企業安全需求的應用程式安裝套件。
   將顯示在您的裝置上安裝 Kaspersky Endpoint Security 的提示。
2. 接受更新條款和條件。
   新版本的應用程式將安裝到您的裝置。該應用程式更新後不需要其他配置。

移除應用程式

管理員可以封鎖您自行刪除應用程式。在這種情況下，您不能刪除 Kaspersky Endpoint Security。

Kaspersky Endpoint Security 可透過下列方法刪除：

- 在應用程式設定中手動刪除。
- 在裝置設定中手動刪除。
- 在管理員的幫助下更新。管理員可以使用卡巴斯基安全管理中心遠端管理系統，遠端移除您裝置上的應用程式。

在應用程式設定中刪除

從裝置刪除 Kaspersky Endpoint Security 的步驟：

1. 在 Kaspersky Endpoint Security 主介面的快速啟動面板中，輕觸 → **移除應用程式**。
   這將啟動應用程式刪除精靈。
2. 按照精靈指示執行操作。

在裝置設定中刪除

可透過執行 Android 平台的標準程式來刪除該應用程式。要移除應用程式，必須在裝置安全性設定中停用 Kaspersky Endpoint Security 管理員權限。

在執行 Android 7.0 或更新版本的裝置上，如果管理員已封鎖刪除，那麼，試圖移除 Android 設定中的應用程式時，該裝置將被鎖定。要解鎖該裝置，請聯絡您的管理員。

透過卡巴斯基安全管理中心刪除

使用卡巴斯基安全管理中心刪除應用程式包含以下步驟：

1. 管理員將應用程式刪除命令傳送到您的行動裝置。
   您的行動裝置會顯示確認刪除 Kaspersky Endpoint Security 的提示。
2. 確認應用程式刪除。
   該應用程式將從您的裝置上刪除。

帶有手提箱圖示的應用程式

Android 工作設定檔中的應用程式圖示

帶有手提箱圖示的應用程式 (公司應用程式) 存放於您裝置的 Android 工作設定檔 (下稱「工作設定檔」)中。*Android 工作設定檔*是您裝置上的安全環境，在此環境中，管理員可以管理應用程式和帳戶，而不限制您處理個人資料的能力。

您可以使用工作設定檔將公司資料與個人資料分開存放。這樣可使公司資料保持機密狀態，免遭惡意軟體的攻擊。當您裝置上建立了工作設定檔後，下列公司應用將自動安裝在工作設定檔中：Google Play Market、Google Chrome、Downloads、Kaspersky Endpoint Security for Android 等等。

KNOX 應用程式

KNOX 圖示

KNOX 應用程式會在您的裝置上開啟一個 KNOX 容器。*KNOX 容器*是您裝置上的一個安全環境，具有自己的桌面、啟動面板、應用程式和小工具。管理員可以在 KNOX 容器中管理應用程式和帳戶，而不會限制您處理個人資料的能力。

您可以使用 KNOX 容器將公司資料與個人資料分開存放。這樣可使公司資料保持機密狀態，免遭惡意軟體的攻擊。

在 KNOX 容器中，您可以存取公司信箱、企業員工的聯絡資訊、檔案儲存和其他應用程式。

如需 Samsung KNOX 的詳細資訊，請造訪 *Samsung 技術支援網站*。

使用 Kaspersky Security for iOS 應用程式

本說明部分介紹了 Kaspersky Security for iOS 應用程使用者可用的功能和操作。

本節文章說明可在行動裝置上使用或顯示的選項。該應用程式的實際版面配置與行為將根據遠端管理系統實作情況而定，以及管理員如何根據企業安全需求配置您的裝置。本節說明的有些功能與選項可能不是用於您在該應用程式中的實際體驗。如對您特定裝置的應用程式有任何問題，請聯絡您的管理員。

程式功能

Kaspersky Security for iOS 提供以下主要功能：

防禦線上威脅

Web 防護元件防護裝置防禦線上威脅。

Web 防護可封鎖散佈惡意程式碼的惡意網站和釣魚網站，例如用於竊取個人資料和銀行帳戶的網站。Web 防護將在您開啟網站前使用卡巴斯基安全網路雲端服務掃描網站。Web 防護也能檢查裝置上應用程式的線上活動。

為了讓 Web 防護順利運作，您必須允許應用程式新增 VPN 設定。

破解偵測

Kaspersky Security for iOS 偵測到破解時，這會顯示重大訊息並向管理員告知該問題。

應用程式無法保證裝置的安全性，因為破解會繞過安全性功能，可能造成許多問題，包括：

- 安全性弱點
- 穩定性問題
- Apple 服務中斷
- 潛在毀損和凍結
- 縮短電池使用壽命
- 無法套用 iOS 更新

安裝應用程式

若要安裝 Kaspersky Security for iOS 應用程式，請：

1. 尋找含有管理員邀請的電子郵件訊息，以從 App Store 安裝 Kaspersky Security for iOS 應用程式。

2. 以下列方式之一前往 App Store：

   - 若您正在想要安裝該應用程式的 iOS 裝置上讀取，請點選訊息中的連結。
   - 若您正在電腦上讀取訊息，請使用您想安裝該應用程式的 iOS 裝置掃描 QR 代碼。

   邀請連結有效時間為 24 小時。若您無法及時安裝應用程式，請聯絡管理員以獲得新的邀請。

3. 按照 iOS 平台上的標準安裝程序，從 App Store 下載並安裝應用程式。

Kaspersky Security for iOS 應用程式已安裝在裝置上。若要保護裝置，請啟用該應用程式。

啟用應用程式

若要啟動 Kaspersky Security for iOS 應用程式，請：

1. 在裝置上啟動應用程式。
2. 選取**最終使用者產品授權協議**和**產品與服務的隱私政策**核取方塊以接受協議和聲明。

   也可以接受**卡巴斯基安全網路聲明**以允許統計資料傳送至卡巴斯基安全網路。這可改善應用程式效能並確保操作不中斷。

3. 點選**下一步**。應用程式會連線至卡巴斯基安全管理中心遠端管理系統並取得產品授權資訊。
4. 允許應用程式新增 VPN 設定。應用程式可使用 VPN 設定檢查網站是否為網路釣魚網站，並保護裝置以防網路威脅。
5. 允許應用程式傳送推播通知。應用程式可使用通知向您告知安全性問題和產品授權狀態。

您裝置上的 Kaspersky Security for iOS 應用程式已啟用。

使用啟動碼啟用應用程式

在裝置上安裝 Kaspersky Security for iOS 應用程式時，應用程式會連線至卡巴斯基安全管理中心遠端管理系統並自動取得產品授權資訊。如果您的裝置未連線卡巴斯基安全管理中心，您可以手動輸入啟動碼。要獲取啟動碼，請聯絡管理員。

僅在管理員指示時手動啟用應用程式。

輸入啟動碼：

1. 在表示應用程式未啟用的訊息中，點選**啟用應用程式**。
2. 在啟動視窗中，輸入管理員給您的啟動碼，然後點選**啟動**。

   如果啟動碼正確，則會顯示一則通知，說明該應用程式已啟用以及授權到期日期。

您裝置上的 Kaspersky Security for iOS 應用程式已啟用。

主介面總覽

主視窗的介面根據螢幕解析度不同而有輕微變化。

主要視窗顯示：

- 裝置的整體防護狀態。
- 指示應用程式元件狀態和防護問題的訊息。

有三種訊息類型：

- 用綠色突出顯示。向您告知防護在指定區域作用中的狀態訊息。
- 用黃色突出顯示。向您告知事件可能影響裝置安全性的資訊訊息。
- 用紅色突出顯示。向您告知事件對裝置安全性有關鍵重要性的重大訊息。

您可以點選訊息取得詳細資訊。

更新應用程式

您可以從 App Store 下載最新版本的 Kaspersky Security for iOS 應用程式，並按照 iOS 平台上的標準更新程序安裝在裝置上。您也可以開啟自動更新。該應用程式更新後不需要任何其他配置。

要更新應用程式，必須滿足下列條件：

- 您必須有 Apple ID。
- 裝置必須已連結至您的 Apple ID。
- 裝置必須已連線網際網路。

若要進一步瞭解建立 Apple ID，請將裝置連結至 Apple ID，或使用 App Store，查看 Apple 支援網站。

移除應用程式

若要移除 Kaspersky Security for iOS 應用程式，按照 iOS 平台上的標準程序：

1. 在首頁畫面上，點選並按住應用程式圖示。
2. 移除應用程式。

Kaspersky Security for iOS 應用程式已從裝置移除。

程式產品授權

本章節提供了與 Kaspersky Security for Mobile 產品授權有關的一般條款資訊。

關於最終使用者授權協議

最終使用者授權協議 (EULA) 是您和 AO Kaspersky Lab 之間的合作協議，其中規定了您使用 Kaspersky Security for Mobile 應遵守的條款與條件。

我們建議您先仔細閱讀 EULA 的條款與條件，然後再開始使用 Kaspersky Security for Mobile。

您可使用下列方式檢視 EULA 條款與條件：

- Kaspersky Security for Mobile 元件安裝期間。
- 讀取分發套件的自我解壓縮封存檔中包含的 license.txt 檔案，以安裝 Kaspersky Endpoint Security for Android 應用程式。
- 在 Kaspersky Endpoint Security for Android 的「**關於應用程式**」區域中。
- 在 Kaspersky Security for iOS 的**關於應用程式 → 協議與聲明**區段中。
- 在管理伺服器內容的「**進階**」→「**接受的產品授權協議**」區段。此功能在卡巴斯基安全管理中心 12.1 版和更高版本中有提供。

安裝 Kaspersky Security for Mobile 元件時確認同意最終使用者授權協議 (EULA)，即表示您接受最終使用者授權協議的條款與條件。若不接受最終使用者授權協議的條款，則必須取消安裝 Kaspersky Security for Mobile 元件並停止使用。

關於產品授權

*產品授權*是指在有限時間內使用 Kaspersky Security for Mobile 整合解決方案的權限，其根據最終使用者產品授權協議提供給使用者。

目前產品授權可使您享受以下各種服務：

- 依照最終使用者授權協議的條款在行動裝置上使用應用程式。
- 獲得技術支援。

可用服務的範圍和程式使用條款取決於用於啟動該程式的產品授權的類型。

我們提供下列產品授權類型：

- *試用版*。

  用於試用 Kaspersky Security for Mobile 的免費產品授權。

  試用版產品授權的有效期為 30 天。在試用版產品授權到期後，除與管理伺服器同步外，Kaspersky Endpoint Security for Android 行動應用程式和 Kaspersky Security for iOS 行動應用程式會停止執行大部分的功能。若要繼續使用該應用程式，您必須購買正式產品授權。

- *商業版*。

  購買 Kaspersky Security for Mobile 時提供的產品授權。

  在正式產品授權到期後，行動 APP 會繼續工作，但功能受到限制。

  在受限功能模式中，下列元件可根據應用程式使用。

  - Kaspersky Endpoint Security for Android 應用程式：
    - **病毒防護**。可對裝置進行即時防護和病毒掃描，但無法使用病毒資料庫更新。
    - **竊盜防護**。只能向行動裝置傳送命令。
    - **與管理伺服器同步**。

    若卡巴斯基金鑰遭封鎖、試用授權到期，或授權遺失（啟動碼自群組政策中移除），Kaspersky Endpoint Security for Android 便會停止與卡巴斯基安全網路、Google Analytics for Firebase、SafetyNet Attestation、Firebase Performance Monitoring 和 Crashlytics 交換資訊。

  - Kaspersky Security for iOS 應用程式：
    - **與管理伺服器同步**。

    若試用版產品授權到期或者若產品授權遺失（從群組政策移除啟動碼），Kaspersky Security for iOS 會停止與卡巴斯基安全網路交換資訊。

  行動應用程式的其餘元件對裝置使用者不可用。管理員可使用群組政策在受限功能模式下管理這些元件。您不能使用群組政策配置應用程式的其他元件。

  若要繼續在全功能模式下使用該應用程式，必須對正式產品授權進行續約。我們建議在目前產品授權到期之前進行續約或購買新的產品授權，以確保電腦得到最大限度防護並能防禦所有安全威脅。

關於訂購

*Kaspersky Security for Mobile 訂購*是根據訂購到期日期、受防護的行動裝置數量等選定的參數使用行動 APP 的訂購方式。可以透過 ISP 等服務提供者訂購 Kaspersky Security for Mobile。可以手動或自動續訂訂購，也可以取消訂購。您可以在服務提供者的網站上管理您的訂購。

訂購可以是有限的（例如一年）或是無限的（無到期日）。要在有限訂購到期後繼續使用 Kaspersky Security for Mobile，必須續訂訂購。無限訂購則自動續訂更新，及時預付費給服務提供者。

如果訂購受限，當訂購到期時，會向您提供一個訂購續約寬限期，在此期間應用程式將保留其功能。此類寬限期的可用性和持續時間由服務提供者自行決定。

要在訂購下使用 Kaspersky Security for Mobile，必須使用從服務提供者處接收到的啟動碼進行啟動。套用啟動碼後，即會安裝與產品授權相對應的金鑰，從而可在訂購狀態下使用應用程式。

可用的訂購管理選項可能各異，具體取決於服務提供者。服務提供者可能不提供訂購續約寬限期，在此期間應用程式將保留其功能。

根據訂購購買的啟動碼不能用於啟動早期版本的 Kaspersky Security for Mobile。

關於金鑰

*金鑰*是一串位元資料，您可以用其啟動整合解決方案 Kaspersky Security for Mobile，並在隨後依照終端使用者產品授權協議的條款，使用該解決方案。金鑰是由 Kaspersky 專家產生的。

使用金鑰檔案或啟動碼即可新增行動應用程式的金鑰：

- 如果您的組織已佈署了卡巴斯基安全管理中心軟體套件，您必須套用金鑰檔案並將其分配給 Android 行動應用程式。金鑰以唯一字母數字序列的形式顯示在卡巴斯基安全管理中心介面和 Android 行動應用程式介面中。

  新增金鑰後，可以用其他金鑰來更換。

  > 您無法使用金鑰檔案啟用 Kaspersky Security for iOS 應用程式。

- 若組織沒有使用卡巴斯基安全管理中心，您必須與使用者分享啟動碼。使用者在 Android 或 iOS 行動應用程式中輸入此啟動碼。金鑰以唯一的英數順序顯示在行動應用程式介面中。

Kaspersky 可能會凍結金鑰，例如，當最終使用者產品授權協議的條款被違反時。如果金鑰被封鎖，除與管理伺服器同步外，行動應用程式會停止執行其所有功能。要繼續使用該應用程式，您需要新增不同的金鑰。

關於啟動碼

*啟動碼*是由 20 個字母數字字元組成的唯一序列。您輸入啟動碼以新增啟用 Kaspersky Endpoint Security for Android 行動應用程式或 Kaspersky Security for iOS 行動應用程式的金鑰。在購買整合解決方案 Kaspersky Security for Mobile 或訂購 Kaspersky Security for Mobile 試用版本時指定郵件信箱，並透過此信箱接收啟動碼。

要使用啟動碼啟動行動應用程式，需透過網際網路連線到 Kaspersky 啟動伺服器。

啟動應用程式後，啟動碼即使遺失，也是可以找回的。您可能需要使用啟動碼，例如在 Kaspersky CompanyAccount 中進行註冊。若要還原啟動碼，請聯絡 Kaspersky 技術支援。

關於金鑰檔案

*金鑰檔案*是 Kaspersky 提供的帶 .key 副檔名的檔案。金鑰檔案的用途是新增啟用 Kaspersky Endpoint Security for Android 應用程式的金鑰。

> 您無法使用金鑰檔案啟用 Kaspersky Security for iOS 應用程式。

在購買 Kaspersky Security for Mobile 整合解決方案或訂購 Kaspersky Security for Mobile 試用版本時指定電子郵件地址，並透過此地址接收金鑰檔案。

您無需連線到 Kaspersky 啟動伺服器，即可使用金鑰檔案啟動應用程式。

金鑰檔案如果遭意外刪除，是可以還原的。例如，您可能需要金鑰檔案來註冊 Kaspersky CompanyAccount。

要還原金鑰檔案，請執行以下操作之一：

- 聯絡產品授權銷售者。

- 使用可用的啟動碼透過 Kaspersky 網站接收金鑰檔案。

Kaspersky Endpoint Security for Android 的資料佈建

Kaspersky Security for Mobile 符合通用資料防護條例 (GDPR)。

若要安裝應用程式，您或裝置使用者必須閱讀和接受《最終使用者產品授權協議》條款。此外，您可為所有使用者設定全域接受下列聲明的政策。否則，使用者將在主應用程式畫面收到接受下列有關處理使用者個人資料的通知：

- 卡巴斯基安全網路聲明
- 有關將資料處理用於 Web 防護的聲明
- 有關將資料處理用於市場行銷的聲明

若您選擇接受全域聲明，透過卡巴斯基安全管理中心接受的版本聲明必須與使用者已接受的版本相符。否則，使用者將收到問題通知與提示，以接受符合管理員全域接受之版本的版本聲明。Kaspersky Security for Mobile (Devices) 外掛程式中的裝置狀態也將變更為 *警告*。

使用者可以隨時在 Kaspersky Endpoint Security for Android 設定的「**關於應用程式**」區域中接受或拒絕聲明的條款。

與卡巴斯基安全網路交換資訊

為改進即時防護功能，Kaspersky Endpoint Security for Android 將使用卡巴斯基安全網路雲端服務執行以下元件：

- **病毒防護**。應用獲得到關於檔案和應用信譽的 Kaspersky 線上知識庫的存取。此項掃描旨在掃描威脅資訊尚未新增到病毒資料庫但已包含在 KSN 中的威脅。卡巴斯基安全網路雲端服務提供病毒防護的完整操作並降低誤報。
- **Web 防護**。在開啟網站之前，該應用程式使用從 KSN 接收的資料對網站執行掃描。該應用程式還可基於允許和封鎖的類別清單（例如，「網際網路通訊」類別），確定控制使用者對網際網路存取的網站類別。
- **應用程式控制**。該應用程式可基於允許和封鎖的類別（例如，「遊戲」類別）清單，確定限制不符合企業安全需求的應用程式啟動的應用程式類別。

最終使用者產品授權協議列出使用者若在操作防毒軟體或 App 應用程式時使用 KSN，該應用程式會提交給 Kaspersky 的資料類型相關資訊。接受產品授權協議的條件和條款即表明您同意傳輸此資訊。

有關在 Web 防護執行期間使用 KSN 時提交給 Kaspersky 的資料類型資訊，請參見有關 Web 防護資料處理的聲明。接受聲明的條件和條款即表明您同意傳輸此資訊。

卡巴斯基安全網路聲明列出使用者若在操作 Kaspersky Endpoint Security for Android 行動應用程式時使用 KSN，該應用程式會提交給 Kaspersky 的統計資料類型相關資訊。接受聲明的條件和條款即表明您同意傳輸此資訊。

在最終使用者產品授權協議下的資料提供

使用啟動碼啟動軟體時，為驗證使用軟體的合法性，最終使用者同意定期提供權利持有人下列資訊：

- 權利持有人基礎架構請求資料格式； 網路服務所存取的 IPv4 位址； 權利持有人基礎架構請求內容大小； 通訊協定 ID； 軟體啟動碼； 資料壓縮類型； 軟體 ID； 可在使用者裝置上啟動的軟體 ID 集； 軟體本地化； 所安裝軟體的完整版本； 唯一服務 ID； 使用者裝置上的日期和時間； 軟體安裝 ID（PCID）； 作業系統版本、作業系統組建編號、作業系統更新編號、作業系統版本、作業系統版本的延伸資訊； 裝置型號； 作業系統系列； 權利持有人基礎架構請求資料格式； 目前處理中物件的總和檢查碼類型； 軟體授權標頭； 區域啟動中心的 ID； 軟體授權金鑰建立日期和時間； 軟體授權 ID； 用於提供軟體授權的資訊模型 ID； 軟體授權到期日期和時間； 軟體授權金鑰的目前狀態； 使用的軟體授權類型； 用於啟動軟體的授權類型； 得自授權的軟體 ID。

為了防護本電腦免遭資訊安全威脅入侵,最終使用者同意定期向權利持有人提供以下資訊:

- 目前處理中物件的總和檢查碼類型； 目前處理中物件的總和檢查碼； 軟體元件 ID；
- 軟體病毒資料庫中的已觸發記錄 ID； 軟體病毒資料庫中的已觸發記錄時間戳記； 軟體病毒資料庫中的已觸發記錄類型； 偵測到的惡意軟體名稱或是可能用於傷害使用者裝置或資料的合法軟體名稱；
- 安裝應用程式的商店名稱； 應用程式套件名稱； 用於簽署 APK 檔案的公開金鑰； 用於簽署 APK 檔案的憑證總和檢查碼； 數位憑證時間戳記；
- 所安裝軟體的完整版本； 軟體更新 ID； 所安裝軟體的類型； 設定識別符； 軟體動作結果； 錯誤碼；
- 根據特定數學規則取自 Android 應用程式 APK 檔案並且不允許復原原始檔案內容的數字； 此資料不包含檔案名稱、檔案路徑、地址、電話號碼或使用者的其他個人資訊。

若您使用權利持有人的更新伺服器下載更新，為提升更新程序的效率，最終使用者同意定期提供以下資訊給權利持有人：

- 得自授權的軟體 ID； 所安裝軟體的完整版本； 軟體授權 ID； 使用的軟體授權類型； 軟體安裝 ID（PCID）； 軟體更新開始的 ID； 目前處理的網址。

權利所有人也可以使用此類別資訊接收關於軟體的分發和使用的統計資訊。

Kaspersky 根據相關法律要求防護所接收的資訊。原始接收的資訊以加密形式儲存，並且隨著資訊的累積而銷毀（每年兩次）或按使用者請求銷毀。程式將無限期地儲存一般統計資訊。

在卡巴斯基安全網路聲明下的資料提供

使用 KSN 可提高軟體所提供防護的有效性，防範資訊和網路安全威脅。

如果您使用 5 個或更多節點的授權，在使用 KSN 的過程中，權利所有人將自動接收並處理以下資料：

- 軟體病毒資料庫中的已觸發記錄 ID； 軟體病毒資料庫中的已觸發記錄時間戳記； 軟體病毒資料庫中的已觸發記錄類型； 軟體資料庫的發佈日期與時間； 作業系統版本、作業系統組建編號、作業系統更新編號、作業系統版本、作業系統版本的延伸資訊； OS Service Pack 版本； 偵測特性； 目前處理中物件的總和檢查碼 (MD5)； 所處理的物件名稱； 表示目前處理中物件為可攜式執行檔的標誌； 封鎖網路服務的遮罩的總和檢查碼 (MD5)； 目前處理中物件的總和檢查碼(SHA256)； 所處理的物件大小； 物件類型碼； 軟體對於目前處理中物件的決策； 所處理物件的路徑； 目錄碼； 軟體元件版本； 所發送之統計資料集的版本； 網路服務的已存取位址（URL、IP）； 用於存取網路服務的用戶端類型； 網路服務所存取的 IPv4 位址； 網路服務所存取的 IPv6 位址； 網路服務請求來源（推薦者）的網址； 目前處理的網址；
- 關於已掃描物件的資訊（來自 AndroidManifest.xml 的應用程式版本； 軟體的應用程式決策； 取得軟體應用程式決策所使用的方法； 商店安裝套件名稱； AndroidManifest.xml 的套件名稱（或套件組合名稱）； Google SafetyNet 類別； 表示裝置是否啟用 SafetyNet 的標誌； Google SafetyNet 回應提供的 SHA256 值； APK 憑證的 APK 特徵碼配置； 已安裝軟體的版本代碼； 用於簽署 APK 檔案的憑證序號； 目前安裝的 APK 檔案名稱； 目前安裝的 APK 檔案路徑； 用於簽署 APK 檔案的憑證發行者； 用於簽署 APK 檔案的公開金鑰； 用於簽署 APK 檔案的憑證總和檢查碼； 憑證的到期日期和時間； 憑證的發行日期和時間； 所發送之統計資料集的

版本； 用於計算數位憑證指紋的演算法； 已安裝 APK 檔案的 MD5 雜湊； APK 檔案中的 DEX 檔案 MD5 雜湊； 動態授予應用程式的權限； 第三方軟體版本； 表示應用程式是否為預設 SMS 通訊軟體的標誌； 表示應用程式是否取得裝置管理員權限的標誌； 表示應用程式是否位於系統目錄的標誌； 表示應用程式是否使用可存取功能服務的標誌）；

- 有關潛在惡意物件和活動的資訊（當前正在處理的物件的片段內容； 憑證的到期日期和時間； 憑證的發行日期和時間； 用於加密的 Keystore 金鑰 ID； 用於與 KSN 交換資料的通訊協定； 目前處理中物件的片段順序； 病毒防護軟體模組針對目前處理中物件所產生的內部記錄資料； 認證發佈者的名稱； 認證的公開金鑰； 憑證公開金鑰的計算演算法； 認證序號； 簽署物件的日期與時間； 認證所有者的名稱與設定； 所掃描物件與雜湊演算法的數位憑證指紋； 目前處理中物件的上次修改日期和時間； 目前處理中物件的建立日期和時間； 目前處理中的物件或其部分； 目前處理中物件的描述，如物件內容中所定義； 所處理物件的格式； 目前處理中物件的總和檢查碼類型； 目前處理中物件的總和檢查碼(MD5)； 所處理的物件名稱； 目前處理中物件的總和檢查碼(SHA256)； 所處理的物件大小； 軟體廠商名稱； 軟體對於目前處理中物件的決策； 所處理物件的版本； 目前處理中物件的決策來源； 目前處理中物件的總和檢查碼； 上層應用程式名稱； 所處理物件的路徑； 檔案簽章檢查結果的相關資訊； 登入工作階段金鑰； 登入工作階段金鑰的加密算法； 目前處理中物件的儲存時間； 用於計算數位憑證指紋的演算法；

- 版本類型，例如「user」或「eng」； 完整產品名稱； 產品/硬體製造商； 是否能夠透過 Google Play 外部安裝應用程式； Google 應用程式驗證的雲端服務狀態； 透過 AOB 安裝之 Google 應用程式驗證的雲端服務狀態； 目前的開發代碼名稱或用於正式版本的「REL」； 增量版本號； 使用者可見的版本字串； 使用者裝置名稱； 使用者可見的軟體建置 ID； 韌體指紋； 韌體 ID； 表示裝置是否取得根權限的標誌； 作業系統； 軟體名稱； 使用的軟體授權類型；

- 有關KSN 服務品質的資訊（用於與 KSN 交換資料的協議）； 軟體所存取的 KSN 服務 ID； 停止接收統計資訊的日期和時間； 快取中的 KSN 連線數量； 在本機請求資料庫中找到回應的請求數量； KSN 連線失敗次數； KSN 交易失敗次數； 已取消 KSN 請求的時間分佈； 已失敗 KSN 連線的時間分佈； 已失敗 KSN 交易的時間分佈； 成功 KSN 連線的時間分佈； 成功 KSN 交易的時間分佈； 成功 KSN 請求的時間分佈； 超時 KSN 請求的時間分佈； 新 KSN 連線次數； 因路由錯誤致使 KSN 請求失敗的次數； 因在軟體設定中停用 KSN 而致使請求失敗的次數； 因網路問題致使 KSN 請求失敗的次數； 成功 KSN 連線次數； 成功 KSN 交易次數； 對 KSN 的請求總數； 開始接收統計資訊的日期和時間；

- 裝置 ID； 所安裝軟體的完整版本； 軟體更新 ID； 軟體安裝 ID（PCID）； 所安裝軟體的類型；

- 裝置螢幕高度； 裝置螢幕寬度； 重疊應用程式的相關資訊： APK 檔案的 MD5 雜湊； 重疊應用程式的相關資訊： Classes.dex 檔案的 MD5 雜湊； 重疊應用程式的相關資訊： APK 檔案名稱； 重疊應用程式的相關資訊： 沒有檔案名稱的 APK 檔案路徑； 重疊高度； 重疊軟體的相關資訊： APK 檔案的 MD5 雜湊； 重疊應用程式資訊： Classes.dex 檔案 MD5 雜湊； 重疊應用程式資訊： APK 檔案名稱； 重疊應用程式資訊： 沒有檔案名稱的 APK 檔案路徑； 重疊應用程式資訊： 應用程式套件名稱（對於重疊應用程式： 如果廣告顯示在空桌面上，值應該是"驅動程式")； 重疊日期和名稱； 重疊應用程式的相關資訊： 應用程式套件名稱； 重疊寬度；

- 在使用過程中設定Wi-Fi 存取點（監測到的裝置類型； DHCP 設定 (閘道本機 IPv6 的總和檢查碼、DHCP IPv6、DNS1 IPv6、DNS2 IPv6； 網路前綴長度的總和檢查碼； 本機 IPv6 位址總和檢查碼）； DHCP 設定（閘道本機 IP 位址的總和檢查碼、DHCP IP、DNS1 IP、DNS2 IP 和子網路遮罩）； 表示是否具有 DNS 網域的標誌； 已分配的本機 IPv6 位址總和檢查碼； 已分配的本機 IPv4 位址總和檢查碼； 表示裝置是否插入的標誌； Wi-Fi 網路驗證類型； 可用 Wi-Fi 網路清單及網路設定； 存取點的 MAC 位址總和檢查碼（進行 salt 處理的 MD5）； 存取點的 MAC 位址總和檢查碼 (進行 salt 處理的 SHA256)； Wi-Fi 存取點支援的連線類型； Wi-Fi 網路加密類型； 開始與結束 Wi-Fi 網路連線的本機時間； 根據存取點 MAC 位址的 Wi-Fi 網路 ID； 根據 Wi-Fi 網路名稱的 Wi-Fi 網路 ID； 根據 Wi-Fi 網路名稱和存取點 MAC 位址的 Wi-Fi 網路 ID； Wi-Fi 訊號強度； Wi-Fi 網路名稱； 此配置支援的驗證通訊協定集； 用於 WPA-EAP 連線的驗證通訊協定； 內部驗證通訊協定； 此配置支援的群組加密集； 此配置支援的金鑰管理通訊協定集； 軟體中的網路最終隱私類別； 軟體中的網路最終安全類別； 此配置支援的 WPA 區塊編碼器集； 此配置支援的安全通訊協定集；

- 軟體的安裝日期和時間； 軟體啟動日期； 下定軟體授權訂單所經由的合作夥伴組織識別碼； 得自授權的軟體 ID； 軟體授權金鑰的序號； 軟體本地化； 表示是否啟用加入 KSN 的標誌； 授權軟體的 ID； 軟體授權 ID； OS ID； 作業系統位元版本。

而且，為了實現提高軟體所提供防護有效性而宣稱的目的，權利所有人可接收入侵者為損害電腦和造成資訊安全威脅而利用的物件。

將上述資訊提供給 KSN 屬自願行為。您可以隨時選擇退出卡巴斯基安全網路。

根據 Web 防護相關資料處理的聲明，所為的資料提供

根據 Web 防護聲明，權利持有人處理資料的目的是用於 Web 防護功能。聲明的目的包括偵測網路威脅，和使用雲端服務卡巴斯基安全網路 (KSN) 確定存取網站的類別。

在您同意的情況下，以下資料將按照 Web 防護聲明，自動定期傳送給權利持有人：

- 產品版本、唯一裝置識別碼、安裝 ID、產品類型。
- 網頁的 URL 位址、連接埠號、URL 協定、URL（有關已請求資訊）。

在有關將資料處理用於市場行銷的聲明下的資料提供

權利持有人採用協力廠商資訊系統對資料進行處理。權利持有人的資料處理受此類協力廠商資訊系統的隱私聲明約束。以下為權利持有人採用的服務以及權利持有人所處理的資料：

Google Analytics for Firebase

在使用軟體時，下列資料將自動定期寄送至 Google Analytics for Firebase，以達成前述載明之目的：

- 應用程式資訊 (應用程式版本、應用程式 ID，以及 Firebase 服務中的應用程式 ID、Firebase 服務中的副本 ID、獲取應用程式的商店名稱、軟體首次啟動的時間戳記)
- 裝置上應用程式安裝的 ID 以及安裝方法
- 關於地區與語言本地化的資訊
- 關於裝置螢幕解析度的資訊
- 取得 root 權限之使用者的相關資訊
- SafetyNet Attestation 服務所提供的裝置診斷資訊
- 將 Kaspersky Endpoint Security for Android 設定為協助工具功能的相關資訊
- 有關應用程式熒幕間、會話期間、熒幕會話開始和結束時資料傳輸以及熒幕名稱相關的資訊
- 關於用來將資料提交給 Firebase 服務的通訊協定、其版本以及使用的資料提交方式識別碼的資訊
- 提交資料目標事件之類型和參數的詳細資訊
- 關於應用程式授權、可用性以及裝置數量的資訊
- 防毒資料庫更新頻率以及與管理伺服器同步頻率的相關資訊
- 關於管理主控台（Kaspersky Security Center或協力廠商 EMM 系統）
- Android ID
- 廣告 ID

- 有關使用者的資訊： 年齡類別與性別、居住國家/地區的識別碼以及興趣清單
- 有關安裝了該軟體的使用者電腦的資訊： 電腦製造商名稱、電腦類型、機型、作業系統的版本與語言（地區設定）、在過去 7 天首次開啟的應用程式相關資訊，以及超過過去 7 天首次開啟的應用程式相關資訊

  資料將透過安全通道轉寄到 Firebase。Firebase 中資料處理方式的相關資訊會發布於下列網址：https://firebase.google.com/support/privacy.

SafetyNet Attestation

使用軟體期間，系統會定期將下列資料自動傳送給 SafetyNet Attestation 以達到宣告目的：

- 裝置檢查時間
- 軟體相關資訊、軟體憑證的名稱與資料
- 裝置檢查結果
- 驗證檢查裝置的隨機識別碼檢查

  資料將透過安全通道轉寄到 SafetyNet Attestation。SafetyNet Attestation 中資料處理方式的相關資訊會發布於下列網址：https://policies.google.com/privacy.

Firebase Performance Monitoring

在軟體使用期間，系統會定期將下列資料自動傳送給Firebase Performance Monitoring，以達成前述載明之目的：

- 唯一安裝 ID
- 應用程式套件名稱
- 已安裝軟體的版本
- 電池充電狀態與電池電量
- 電訊廠商
- 應用前台或後台狀態
- 地理
- IP 位址
- 裝置語言代碼
- 有關無線電/網路連線的資訊
- 匿名軟體實例 ID
- RAM 與磁碟大小
- 表示裝置是否越獄或取得根權限的標誌
- 訊號強度
- 自動追蹤持續時間
- 網路和以下相應資訊： 回應代碼，承載（位元），回應時間

- 裝置描述

  資料將透過安全通道轉寄到Firebase Performance Monitoring。Firebase Performance Monitoring 中資料處理方式的相關資訊會發布於下列網址：https://firebase.google.com/support/privacy.

Crashlytics

在軟體使用期間，系統會定期將下列資料自動傳送給 Crashlytics，以達成前述載明之目的：

- 軟體 ID
- 已安裝軟體的版本
- 表示軟體是否在背景執行的標誌
- CPU 基礎架構
- 唯一事件 ID
- 事件日期與時間
- 裝置型號
- 總計磁碟空間與目前用量
- 作業系統名稱及版本
- 總計 RAM 與目前用量
- 表示裝置是否取得根權限的標誌
- 發生事件時的螢幕方向
- 產品/硬體製造商
- 唯一安裝 ID
- 所發送之統計資料集的版本
- 軟體例外類型
- 錯誤訊息文字
- 表示軟體例外是由巢狀例外引起的標誌
- 執行緒 ID
- 表示框架是否軟體錯誤原因的標誌
- 表示執行緒引起軟體意外終止的標誌
- 有關引起軟體意外終止的訊號的資訊： 訊號名稱，訊號代碼，訊號位址
- 對於和執行緒、例外或錯誤關聯的每個框架： 框架檔案名稱，框架檔案行號，偵錯符號，二進位檔映像的位置和位移，帶有框架的庫的顯示名稱，框架類型，表示框架是否是錯誤原因的標誌
- OS ID

- 與事件關聯的問題 ID
- 有關軟體意外終止前發生的事件的資訊： 事件標識符，事件日期與時間，事件類型和值
- CPU 登錄檔值
- 事件類型和值

  資料將透過安全通道轉寄到Crashlytics。Crashlytics 中資料處理方式的相關資訊會發布於下列網址：https://firebase.google.com/terms/crashlytics-app-distribution-data-processing-terms.

基於自願原則出於行銷目的提供上述處理資訊。

Kaspersky Security for iOS 的資料佈建

Kaspersky Security for Mobile 符合通用資料防護條例 (GDPR)。

若要安裝應用程式，裝置使用者必須閱讀並接受下列關於使用者個人資料處理之聲明的條款：

- 最終使用者產品授權協議
- 產品與服務的隱私權政策

或者，使用者也可以閱讀並接受下列聲明的條款：

- 卡巴斯基安全網路聲明

使用者可以隨時在 Kaspersky Security for iOS 設定的**關於應用程式 → 協議與聲明**區段檢視這些文件的條款。在此區段中，使用者也可以接受或拒絕 KSN 聲明的條款。

與卡巴斯基安全網路交換資訊

為改進即時防護功能，Kaspersky Security for iOS 將使用卡巴斯基安全網路雲端服務執行 **Web 防護**元件。在開啟網站之前，該應用程式使用從 KSN 接收的資料對 Web 資源執行掃描。

最終使用者產品授權協議列出使用者若在操作 Web 防護時使用 KSN，該應用程式會提交給 Kaspersky 的資料類型相關資訊。接受產品授權協議的條件和條款即表明您同意傳輸此資訊。

卡巴斯基安全網路聲明列出使用者若在操作 Kaspersky Security for iOS 行動應用程式時使用 KSN，該應用程式會提交給 Kaspersky 的統計資料類型相關資訊。接受聲明的條件和條款即表明您同意傳輸此資訊。

在最終使用者產品授權協議下的資料提供

使用啟動碼啟動軟體時，為驗證使用軟體的合法性，最終使用者同意定期提供權利持有人下列資訊：

- 權利持有人基礎架構請求資料格式； 網路服務所存取的 IPv4 位址； 權利持有人基礎架構請求內容大小； 通訊協定 ID； 軟體啟動碼； 資料壓縮類型； 軟體 ID； 可在使用者裝置上啟動的軟體 ID 集； 軟體本地化； 所安裝軟體的完整版本； 唯一服務 ID； 使用者裝置上的日期和時間； 軟體安裝 ID（PCID）； 目前使用過的軟體啟動碼； 作業系統版本、作業系統組建編號、作業系統更新編號、作業系統版本、作業系統版本的延伸資訊； 裝置型號； 行動電訊廠商代碼； 作業系統系列； 得自授權的軟體 ID； 軟體展示給使用者的協議清單；

使用者在使用軟體時接受的法律協議類型； 使用者在使用軟體時接受的法律協議版本； 表示使用者在使用軟體時是否接受法律協議條款的標誌； 目前處理中物件的總和檢查碼類型； 軟體授權標頭； 區域啟動中心的 ID； 軟體授權金鑰建立日期和時間； 軟體授權 ID； 用於提供軟體授權的資訊模型 ID； 軟體授權到期日期和時間； 軟體授權金鑰的目前狀態； 使用的軟體授權類型； 用於啟動軟體的授權類型； 得自授權的軟體 ID。

權利持有人亦可利用該等資訊收集有關權利持有人之軟體的發布與使用的統計資訊。

為了防護本電腦免遭資訊安全威脅入侵,最終使用者同意定期向權利持有人提供以下資訊:

- 權利持有人基礎架構請求資料格式； 網路服務的已存取位址（URL、IP）； 通訊埠編號； 網路服務請求來源（推薦者）的網址。
- 所安裝軟體的完整版本； 軟體更新 ID； 已安裝軟體的類型； 軟體 ID； 配置識別碼； 軟體動作結果； 錯誤碼。
- 目前處理的網址； 網路服務所存取的 IPv4 位址； 所掃描物件與雜湊演算法的數位憑證指紋； 憑證類型； 目前處理中的數位憑證的內容。

在卡巴斯基安全網路聲明下的資料提供

接受 KSN 聲明後，權利持有人會自動接收並處理下列資料：

- 有關 KSN 服務品質的資訊（用於與 KSN 交換資料的協議）； 軟體所存取的 KSN 服務 ID； 停止接收統計資訊的日期和時間； 快取中的 KSN 連線數量； 在本機請求資料庫中找到回應的請求數量； KSN 連線失敗次數； KSN 交易失敗次數； 已取消 KSN 請求的時間分佈； 已失敗 KSN 連線的時間分佈； 已失敗 KSN 交易的時間分佈； 成功 KSN 連線的時間分佈； 成功 KSN 交易的時間分佈； 成功 KSN 請求的時間分佈； 超時 KSN 請求的時間分佈； 新 KSN 連線次數； 因路由錯誤致使 KSN 請求失敗的次數； 因在軟體設定中停用 KSN 而致使請求失敗的次數； 因網路問題致使 KSN 請求失敗的次數； 成功 KSN 連線次數； 成功 KSN 交易次數； 對 KSN 的請求總數； 開始接收統計資訊的日期和時間。
- 裝置 ID； 所安裝軟體的完整版本； 軟體更新 ID； 軟體安裝 ID（PCID）； 已安裝軟體的類型。
- 軟體的安裝日期和時間； 軟體啟動日期； 軟體本地化； 表示是否啟用加入 KSN 的標誌； 授權軟體的 ID； 軟體授權 ID； OS ID； 使用者電腦上安裝的作業系統版本； 作業系統位元版本。

將上述資訊提供給 KSN 屬自願行為。您可以隨時選擇退出卡巴斯基安全網路。

聯絡技術支援

本章節說明如何獲得技術支援和提供技術支援的條件。

如何獲得技術支援

如果在 Kaspersky Security for Mobile 說明文件中，或關於 Kaspersky Security for Mobile 的任何資訊來源中，都找不到問題的解決方案，請聯絡技術支援。技術支援專家會為您解答關於安裝和使用 Kaspersky Security for Mobile 的所有問題。

> 卡巴斯基會在 Kaspersky Security for Mobile 的生命週期期間提供支援（參見產品生命週期支援頁面）。在聯絡技術支援之前，請閱讀支援規則。

您可以使用下列方式之一與技術支援服務部門聯絡：

- 透過存取技術支援網站
- 從 Kaspersky CompanyAccount 入口網站向技術支援傳送要求

透過 Kaspersky CompanyAccount 取得技術支援

Kaspersky CompanyAccount 是為使用 Kaspersky 應用程式的公司提供的入口網站。Kaspersky CompanyAccount 入口網站的目的是透過線上請求，促進使用者和 Kaspersky 專家之間的互動。您可以使用 Kaspersky CompanyAccount 追蹤線上要求的狀態，並儲存要求的歷史紀錄。

您可以在 Kaspersky CompanyAccount 上將您所在組織的所有員工註冊到同一個帳戶下。單一帳戶使您可以集中管理註冊員工向 Kaspersky 傳送的電子請求，並且透過 Kaspersky CompanyAccount 管理這些員工的權限。

可提供以下語言的 Kaspersky CompanyAccount 網站：

- 英語
- 西班牙語
- 義大利語
- 德語
- 波蘭語
- 葡萄牙語
- 俄語
- 法語
- 日語

如需深入瞭解 Kaspersky CompanyAccount 的詳細資訊，請造訪技術支援網站。

有關應用程式的資訊來源

Kaspersky 網站上的 Kaspersky Security for Mobile 網頁

在 Kaspersky Security for Mobile 頁面 上，您可以找到應用程式及其功能和操作參數的一般資訊。

Kaspersky Security for Mobile 網頁提供 eStore 連結。您可以在此購買或續約程式。

知識庫中的 Kaspersky Security for Mobile 網頁

*知識庫*是技術支援網站上的一個區域。

在知識庫中的 Kaspersky Security for Mobile 頁面 上，您可以尋找相關文章，這些文章包含有用的資訊、建議以及有關如何購買、安裝和使用應用程式的常見問題解答。

知識庫文章不僅可以解答與 Kaspersky Security for mobile 有關的問題，而且可以解答與其他 Kaspersky 應用程式有關的問題。知識庫文章還可能包含技術支援的最新情況。

線上說明

程式的線上說明由說明檔案組成。

Kaspersky Security for Mobile 管理外掛程式的上下文說明提供有關卡巴斯基安全管理中心視窗的資訊：Kaspersky Security for Mobile 設定描述，以及使用這些設定的工作描述的連結。

Kaspersky Endpoint Security for Android 和 Kaspersky Security for iOS 應用程式的完整說明提供有關如何設定和使用行動應用程式的資訊。

在卡巴斯基支援論壇上討論卡巴斯基應用程式

如果您的問題不需要立即回答，您可以在我們的論壇 與卡巴斯基專家和其他使用者一起進行討論。

在論壇，您可以檢視討論主題、發表評論並建立新的討論主題。

詞彙

Android 工作設定檔

一個使用者裝置上的安全環境，在該環境中，管理員可以在不限制使用者使用個人資料的情況下，管理應用程式和帳戶。當使用者裝置上建立了工作設定檔後，下列公司應用將自動安裝在工作設定檔中：Google Play Market、Google Chrome、Downloads、Kaspersky Endpoint Security for Android 等等。工作設定檔中安裝的應用程式，以及這些應用程式的通知，都將被標上紅色手提箱圖示。您必須為 Google Play Market 應用程式建立單獨的 Google 公司帳戶。工作設定檔中安裝的應用程式會顯示在常用應用程式清單中。

Apple 推送通知服務 (APNs) 憑證

Apple 簽章的憑證，讓您得以使用 Apple 推播通知。iOS MDM 伺服器可透過 Apple 推送通知管理 iOS 裝置。

EAS 裝置

透過 Exchange ActiveSync 協定連線至管理伺服器的行動裝置。

Exchange 行動裝置伺服器

即 Kaspersky Endpoint Security 的元件，可讓您將 Exchange ActiveSync 行動裝置連線到管理伺服器。

IMAP

用於存取電子郵件的協定。與 POP3 協定相反，IMAP 提供了用於處理信箱的延伸功能，例如管理資料夾和處理郵件，而不從郵件伺服器複製其內容。IMAP 協定使用連接埠 134。

iOS MDM 伺服器

Kaspersky Endpoint Security 的一個元件，安裝於用戶端裝置，可用於建立 iOS 行動裝置至管理伺服器的連線，並透過 Apple 推送通知 (APN) 管理 iOS 行動裝置。

iOS MDM 裝置

由 iOS MDM 伺服器控制的 iOS 行動裝置。

iOS MDM 設定檔

包含一系列將 iOS 行動裝置連線至管理伺服器的設定集合的設定檔。iOS MDM 設定檔用於透過 iOS MDM 伺服器以背景模式傳送 iOS 設定檔，接收關於行動裝置的延伸診斷資訊。需要將 iOS MDM 設定檔連結傳送給使用者，以便啟動 iOS MDM 伺服器發現並連線使用者的 iOS 行動裝置。

Kaspersky 更新伺服器

在 Kaspersky 的 HTTP(S) 伺服器，Kaspersky 應用程式從這些伺服器下載資料庫和應用程式模組更新。

Kaspersky 類別

Kaspersky 專家開發的預定義資料類別。可以在應用程式資料庫更新期間更新類別。安全人員無法修改或移除預定義類別。

POP3

郵件用戶端用來從郵件伺服器接收郵件的網路協定。

SSL

用於網際網路和本機網路的資料加密協定。安全通訊端層 (SSL) 協定用於 Web 應用程式，以便在用戶端和伺服器之間建立安全連線。

代理伺服器

允許使用者向其他網路服務發出間接請求的電腦網路服務。首先，使用者連線到代理伺服器並請求位於另一伺服器上的資源（例如檔案）。然後，代理伺服器連線到指定的伺服器並從中獲取資源，或者從自己的快取中返回資源（如果代理有自己的快取）。在有些情況下，代理伺服器可能會出於某些目的修改使用者的請求或伺服器的回應。

供給設定檔

iOS 行動裝置上應用程式運作情況的設定集。供給設定檔包含產品授權資訊；並且連接至特定應用程式。

最終使用者產品授權協議

您與 AO Kaspersky Lab 之間的合作協議，其中規定了您使用應用程式時應遵守的條款。

卡巴斯基安全管理中心管理員

透過卡巴斯基安全管理中心的遠端集中管理系統，負責管理應用程式運作情況的人員。

卡巴斯基安全管理中心網頁伺服器

卡巴斯基安全管理中心元件，與管理伺服器一同安裝。網頁伺服器用以透過網路傳輸獨立安裝套件、iOS MDM 設定檔，以及共用資料夾的檔案。

卡巴斯基安全網路 (KSN)

屬於雲端服務基礎結構，可存取 Kaspersky 資料庫，接收不斷更新的檔案信譽、網路資源和軟體相關資訊。卡巴斯基安全網路可確保在遇到威脅時 Kaspersky 程式能夠做出更快速的回應，提高某些防護元件的效能，並降低誤報的風險。

卡巴斯基私人安全網路（私有 KSN）

卡巴斯基私人安全網路是一種解決方案，使安裝了卡巴斯基應用程式的裝置使用者可以存取卡巴斯基安全網路的信譽資料庫和其他統計資料，而無需將資料從其裝置傳送到卡巴斯基安全網路。卡巴斯基私人安全網路是為因以下任何原因而無法加入卡巴斯基安全網路的企業客戶設計的：

- 使用者裝置未連線網際網路。
- 法律或公司安全政策禁止在國家或公司區域網路之外傳輸任何資料。

安裝套件

使用遠端管理系統建立的一組用於遠端安裝 Kaspersky 程式的檔案。安裝套件是以應用程式分發套件內的專用檔案為基礎所建立而成。安裝套件包含了安裝應用程式並立即開始所需的一系列設定。安裝套件中設定值對應于應用程式設定的預設值。

憑證簽發請求

即帶有管理伺服器設定的檔案，經由 Kaspersky 批准，再傳送到 Apple 以獲取 APN 憑證。

應用程式管理外掛程式

專用元件，透過管理主控台提供管理 Kaspersky 應用程式的介面。每個可透過 Kaspersky 安全管理中心 SPE 管理的應用程式都有自己的管理外掛程式。所有可透過 Kaspersky 安全管理中心管理的 Kaspersky 應用程式皆附有管理外掛程式。

政策

一套應用程式設定集合，Kaspersky Endpoint Security 行動 APP 將其套用至管理群組中的裝置上，或套用至單個裝置上。可將不同的政策套用至不同的管理群組中。政策包括 Kaspersky Endpoint Security 行動 APP 所有功能的配置設定。

啟動碼

即購買 Kaspersky Endpoint Security 授權時收到的代碼。啟動應用程式時需要此啟動碼。

啟動碼是由 20 個字母和數字組成的格式為 xxxxx-xxxxx-xxxxx-xxxxx 的唯一序列。

啟動程式

將應用程式轉換到全功能模式。使用者在安裝應用程式期間或之後執行應用程式啟動。需有啟動碼或金鑰檔案才能啟動應用程式。

清單檔案

PLIST 格式的檔案，包含網頁伺服器中應用程式檔案（ipa 檔案）的連結。使用 iOS 裝置從網頁伺服器中尋找、下載並安裝應用程式。

獨立安裝套件

適用于 Android 作業系統的 Kaspersky Endpoint Security 安裝檔案，其包含應用程式連線管理伺服器的設定。基於該應用程式的安裝套件進行建立，並且是一個特殊的行動 APP 安裝套件。

產品授權

根據最終使用者產品授權協議授予的應用程式限時使用權利。

產品授權的有效期

您可以存取應用程式功能並有權使用其他服務的時間段。您可以使用的服務取決於授權類型。

病毒

一種會感染其他程式的程式，這種程式透過將其程式碼新增到其他程式中，在受感染檔案執行時獲得控制權。以這項簡明的定義，即可判別任何病毒執行的主要動作：即感染。

病毒資料庫

即內含病毒資料庫發佈之際 Kaspersky 已知的電腦安全威脅的相關資訊的資料庫。病毒資料庫中的條目可用以偵測掃描物件中的惡意程式碼。病毒資料庫由 Kaspersky 專家建立，每小時更新一次。

監控裝置

意指其設定受到 Apple Configurator 監控的 iOS 裝置，Apple Configurator 是 iOS 裝置的群組配置程式。監控裝置在 Apple Configurator 中的狀態為「*受監管*」。每次監控裝置連線至電腦時，Apple Configurator 就會檢查該裝置的配置是否符合指定的參考設定，並根據需要進行調整。監控裝置不能與安裝在其他電腦上的 Apple Configurator 同步。

與非監控裝置相比，每部監控裝置都提供了更多設定，可透過 Kaspersky Device Management for iOS 政策重新加以定義。舉例來說，您可以設定 HTTP 代理伺服器，以便監控企業網路內裝置的網際網路流量。預設情況下，所有行動裝置皆非監控裝置。

管理伺服器

卡巴斯基安全管理中心的一個元件，可集中儲存公司網路內安裝的所有 Kaspersky 程式的資訊。它也可用于管理這些應用程式。

管理員工作站

即已佈署卡巴斯基安全管理中心管理主控台的電腦。如果管理員工作站上安裝了應用程式管理外掛程式，Kaspersky Endpoint Security 行動 APP 將佈署在使用者裝置上。

管理群組

一組受管裝置，例如根據其執行的功能和其上所安裝應用程式集合進行群組的行動裝置。將受管電腦群組便於以一個整體的形式進行管理。例如，可將執行相同作業系統的行動裝置合併為一個管理群組。一個群組可包含其他管理群組。您可以為群組裝置建立群組政策和群組工作。

網路釣魚

一種網際網路詐欺的類型，目標在於獲取未經授權的存取權，以便取得使用者機密資料。

群組工作

為群組中所有受管裝置執行的管理群組工作。

裝置管理員

一套 Android 裝置上應用程式權限集合，可允許應用程式使用裝置管理政策。有必要在 Android 裝置上套用 Kaspersky Endpoint Security on Android 的全部功能。

規性控制

驗證行動裝置和 Kaspersky Endpoint Security for Android 的設定是否符合公司的安全要求。企業安全需求會規範裝置使用情形。例如，必須在裝置上啟用即時防護，病毒資料庫必須是最新的，並且裝置密碼強度必須足夠。合規性控制基於規則清單。合規性規則包括以下組成部分：

- 裝置檢查條件（例如，裝置上不存在遭禁止的應用程式）
- 分配給使用者以解決不合規問題的時間間隔（例如，24 小時）
- 如果使用者未在規定的時間內解決不合規問題，將對裝置採取的措施（例如鎖定裝置）

解鎖碼

您可以在卡巴斯基安全管理中心中獲取的代碼。在執行**鎖定和定位**、**警示音警報**或**臉部快照**命令後，且觸發自我防護的情況下，必須解鎖裝置。

訂購

允許在所選參數（到期日期和裝置數量）範圍內使用應用程式。您可以暫停或復原訂購、自動續約或取消。

金鑰檔案

即 xxxxxxxx.key 格式的檔案，在取得試用授權或正式產品授權後，即可透過金鑰檔案使用 Kaspersky 應用程式。應用程式會根據啟動碼產生金鑰檔案。擁有金鑰檔案才能使用應用程式。

隔離

Kaspersky 應用程式將已偵測到的疑似感染物件移動到其中的資料夾。物件以加密形式儲存在隔離區中，以免對電腦造成任何影響。

有關協力廠商代碼的資訊

您可以在下列檔案中下載和閱讀有關第三方代碼的資訊：

- legal_notices_Android.txt（適用於 Kaspersky Endpoint Security for Android 應用程式）
- legal_notices_iOS.txt（適用於 Kaspersky Security for iOS 應用程式）

在行動裝置上，可在行動應用程式的**關於應用程式**區段取得關於第三方代碼的資訊。

商標聲明

註冊商標及服務標誌均為其各自所有人的財產。

PostScript 是 Adobe 在美國和/或其他國家/地區的註冊商標或商標。

AirDrop 和 AirPrint 是 Apple Inc. 的商標。

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 皆是 Apple Inc. 在美國和其他國家及地區的註冊商標。

Aruba Networks 是 Aruba Networks, Inc. 在美國和特定其他國家/地區的商標。

Bluetooth 字樣、符號和標誌皆為 Bluetooth SIG, Inc. 所有。

Cisco、Cisco AnyConnect 和 IOS 是 Cisco Systems, Inc. 和/或其附屬公司在美國和特定其他國家/地區的註冊商標或商標。

SecurID 是 EMC Corporation 在美國和/或其他國家/地區的註冊商標或商標。

Google、Android、Chrome、Chromebook、Chromium、Crashlytics、Firebase、Google Analytics、Google Chrome、Google Mail、Google Maps、Google Play、Nexus 和 SPDY 皆是 Google LLC 的商標。

HTC 是 HTC 公司的商標。

Huawei、HUAWEI 和 EMUI 是 Huawei Technologies Co., Ltd 在中國和其他國家/地區的註冊商標。

IBM 和 Maas360 是 International Business Machines Corporation 在世界多個地區的註冊商標。

Juniper Networks、Juniper 和 JUNOS 是 Juniper Networks, Inc. 在美國和其他國家/地區的商標或註冊商標。

Microsoft、ActiveSync、Microsoft Intune、Tahoma、Windows、Windows Mobile 和 Windows Phone 是 Microsoft 公司集團的商標。

MOTOROLA 和 Stylized M 標誌是 Motorola Trademark Holdings, LLC 的商標或註冊商標。

Oracle 和 JavaScript 是 Oracle 和/或其附屬公司的註冊商標。

BlackBerry 商標由 Research In Motion Limited 擁有，並在美國註冊，在其他國家/地區可能正在申請中或已註冊。

Samsung 是 SAMSUNG 在美國或其他國家/地區的註冊商標。

Aventail、SonicWALL 和 SonicWALL Mobile Connect 是 SonicWall, Inc. 的商標。

SOTI 和 MobiControl 是 SOTI Inc. 在美國和其他地區的註冊商標。

Symantec 是 Symantec Corporation 或其相關企業在美國和其他國家/地區的商標或註冊商標。

Symbian 商標為 Symbian Foundation Ltd. 所有。

AirWatch、VMware 和 VMware Workspace ONE 是 VMware, Inc. 在美國和/或其他地區的註冊商標或商標。

F5 是 F5 Networks, Inc. 在美國和特定其他國家/地區的商標。