kaspersky

Kaspersky Embedded Systems Security 4.1 for Windows

© 2026 AO Kaspersky Lab

目錄

Kaspersky Embedded Systems Security for Windows
- 新增功能
- 已修正的問題
- 分發套件
- 硬體和軟體需求
- 卡巴斯基安全管理中心的支援版本
- 功能要求和限制
  - 安裝和移除應用程式
  - 系統完整性監控
  - Firewall
  - 對過時 Windows 版本的限制
  - 與卡巴斯基安全管理中心整合
  - 其他限制
- 與其他應用程式的相容性

安裝和移除應用程式
- 安裝排程
  - 選擇管理工具
  - 選擇安裝類型
- 基於精靈安裝和移除應用程式
  - 使用安裝精靈安裝
    - Kaspersky Embedded Systems Security 安裝
    - Kaspersky Embedded Systems Security 主控台安裝
    - 在其他裝置上安裝應用程式主控台以後的進階設定
      - 允許匿名遠端存取 COM 應用程式
      - 允許 Kaspersky Embedded Systems Security 遠端管理處理程序的網路連線
    - 在安裝 Kaspersky Embedded Systems Security 後執行的操作
      - 啟動並配置資料庫和應用程式模組更新工作
      - 關鍵區域掃描
  - 修改元件集和修復 Kaspersky Embedded Systems Security
  - 使用安裝精靈移除
    - Kaspersky Embedded Systems Security 移除
    - Kaspersky Embedded Systems Security 主控台移除
- 透過命令列安裝或移除應用程式
  - 關於從命令列安裝和移除 Kaspersky Embedded Systems Security
  - 適用於 Windows Installer 服務的 Kaspersky Embedded Systems Security 軟體元件程式碼
  - 安裝和復原設定以及 Windows 安裝程式命令列選項
  - 安裝 Kaspersky Embedded Systems Security 的指令範例
  - 在安裝 Kaspersky Embedded Systems Security 後執行的操作
  - 新增/移除元件。指令範例
  - Kaspersky Embedded Systems Security 移除。指令範例
  - 回傳代碼

使用卡巴斯基安全管理中心安裝和移除應用程式
有關透過卡巴斯基安全管理中心安裝的一般資訊
安裝或移除 Kaspersky Embedded Systems Security 的權限
透過卡巴斯基安全管理中心安裝 Kaspersky Embedded Systems Security
在安裝 Kaspersky Embedded Systems Security 後執行的操作
透過卡巴斯基安全管理中心安裝應用程式主控台
透過卡巴斯基安全管理中心移除 Kaspersky Embedded Systems Security
使用卡巴斯基安全管理中心變更應用程式元件集
透過 Active Directory 群組政策安裝和解除安裝應用程式
透過 Active Directory 群組政策安裝 Kaspersky Embedded Systems Security
在安裝 Kaspersky Embedded Systems Security 後執行的操作
透過 Active Directory 群組政策移除 Kaspersky Embedded Systems Security
Kaspersky Embedded Systems Security 安裝和移除記錄
Kaspersky Embedded Systems Security 安裝後的系統變更
Kaspersky Embedded Systems Security 處理程序
檢查 Kaspersky Embedded Systems Security 功能。使用 EICAR 測試病毒
關於 EICAR 測試病毒
檢查即時檔案防護和自訂掃描功能
將舊版的 Kaspersky Embedded Systems Security 升級至版本 4.1
更新 Kaspersky Embedded Systems Security
更新 Kaspersky Embedded Systems Security 管理工具
遷移政策和工作
遷移正在更新的應用程式版本的設定
Kaspersky Embedded Systems Security 3.4 和 4.1 版本中的元件和工作的對應關係
應用程式介面
使用管理外掛程式
從卡巴斯基安全管理中心管理 Kaspersky Embedded Systems Security
管理應用程式設定
在卡巴斯基安全管理中心中設定一般應用程式設定
在卡巴斯基安全管理中心中配置介面和掃描設定
在卡巴斯基安全管理中心中配置安全性設定
使用卡巴斯基安全管理中心配置連線設定
設定本機工作執行模式
在卡巴斯基安全管理中心中配置備份設定
建立和設定政策
建立政策
設定政策
安全等級指示器
使用卡巴斯基安全管理中心建立和管理工作
關於卡巴斯基安全管理中心中的工作建立
使用卡巴斯基安全管理中心建立工作
前往個別電腦的本機工作設定和一般應用程式設定
在卡巴斯基安全管理中心中設定群組工作
應用程式啟動工作
更新工作
應用程式完整性控制
排程工作

卡巴斯基安全管理中心中的報告
即時防護狀態
使用 Kaspersky Embedded Systems Security 主控台
啟動應用程式主控台
Kaspersky Embedded Systems Security 主控台介面
Kaspersky Embedded Systems Security 主控台視窗
通知區域中的系統托盤圖示
透過應用程式主控台配置一般設定
管理 Kaspersky Embedded Systems Security 工作
Kaspersky Embedded Systems Security 工作類別
手動啟動/暫停/還原/停止工作
排程工作
使用使用者帳戶啟動工作
關於使用帳戶啟動工作
指定使用者帳戶以啟動工作
匯入和匯出設定
關於匯入和匯出設定
匯出設定
匯入設定
檢視防護狀態和 Kaspersky Embedded Systems Security 資訊
如何在應用程式主控台中配置備份設定
從 Web 主控台和雲端主控台使用 Web 外掛程式
從 Web 主控台和雲端主控台管理 Kaspersky Embedded Systems Security
Web 外掛程式限制
管理應用程式設定
在 Web 外掛程式中配置一般應用程式設定
在 Web 外掛程式配置介面和掃描設定
在 Web 外掛程式中配置安全性和可靠性設定
在 Web 外掛程式中配置連線設定
在 Web 外掛程式中設定本機工作的排程啟動
在 Web 外掛程式中配置備份設定
建立和設定政策
使用卡巴斯基安全管理中心建立和管理工作
關於 Web 外掛程式中的工作建立
在 Web 外掛程式中建立工作
在 Web 外掛程式中配置群組工作
在 Web 外掛程式中設定應用程式啟動工作
在 Web 外掛程式中配置更新工作
排程工作
卡巴斯基安全管理中心中的報告
應用程式產品授權
關於最終使用者產品授權協議
關於產品授權
關於產品授權憑證
關於金鑰
關於金鑰檔案
關於啟動碼

- 依據產品授權類型對比應用程式功能
- 使用金鑰檔案啟動應用程式
- 使用啟動碼啟動應用程式
- 檢視有關目前產品授權的資訊
- 續約產品授權
- 刪除金鑰

啟動和停止 Kaspersky Embedded Systems Security

- 啟動和停止應用程式
- 暫停和還原電腦防護和控制

小型診斷視窗

- 關於小型診斷視窗
- 透過小型診斷視窗檢視 Kaspersky Embedded Systems Security 狀態
- 檢視安全事件統計
- 檢視目前應用程式活動
- 配置應用程式追蹤和記憶體傾印記錄

Kaspersky Embedded Systems Security 自我防護

- 啟用和停用自我防護
- 支援 AM-PPL 技術
- 防護作業系統服務
- 配置使用者權限以管理 Kaspersky Embedded Systems Security
- 設定管理 Kaspersky Embedded Systems Security 服務的使用者存取權限
- 對 Kaspersky Embedded Systems Security 功能進行受密碼防護的存取
- Secure Desktop 通知

信任區域

- 建立掃描排除項目
- 選擇可偵測的威脅類型
- 編輯信任應用程式清單
- 建立本機信任區域
- 匯出和匯入受信任區域
- 使用受信任的系統憑證儲存
- 預先定義的掃描排除項目和受信任的應用程式

即時檔案防護

- 關於工作防護範圍和安全設定
- 預定義的防護範圍
- 關於預定義安全等級
- “即時檔案防護”元件預設掃描的檔案副檔名
- 配置“即時檔案防護”元件
- 配置即時檔案防護元件的防護範圍
- 手動配置安全性設定
- 容器掃描

KSN 使用

- 啟用卡巴斯基安全網路
- 卡巴斯基安全網路使用統計資料
- 卡巴斯基私有安全網路的限制
- KSN 代理設定

弱點利用防禦
弱點利用防禦模式
啟用和停用弱點利用防禦
啟用和停用記憶體防護
建立受防護的處理程序清單
修復引擎
行為偵測
啟用和停用本機資料夾的加密防護
防止共用資料夾被外部加密
啟用和停用共用資料夾對外部加密的防護
編輯防護範圍
新增受信任的電腦以進行外部資料加密
配置不受信任電腦的封鎖時間
匯出和匯入防止共用資料夾被外部加密的排除項目清單
網路威脅防護
啟用和配置網路威脅防護
建立封鎖排除項目
匯出和匯入防止共用資料夾被外部加密的排除項目清單
AMSI 掃描器
啟用和停用 AMSI 掃描程式
AMSI 掃描程式設定
應用程式啟動控制
關於應用程式啟動控制規則
關於軟體分發控制
關於應用程式啟動控制規則產生器
啟用和配置應用程式啟動控制
配置軟體分發控制
使用應用程式啟動控制規則
新增應用程式啟動控制規則
為應用程式控制規則新增觸發條件
新增應用程式啟動控制規則範圍的排除項目
允許所有應用程式執行
匯出應用程式啟動控制規則
使用選定的卡巴斯基安全管理中心封鎖的應用程式事件來產生 TXT 檔案
配置"應用程式啟動控制規則產生器"群組工作
使用"應用程式啟動控制規則產生器"群組工作建立規則。
裝置控制
裝置存取規則
按類型管理對裝置的存取
Wi-Fi 連線控制
列印控制
輸入裝置控制（HID）
管理存取行動裝置的權限
監視卸除式磁碟機的使用
管理存取藍牙裝置的權限
區分使用者對裝置的存取權限
關於裝置控制規則產生器

- 新增受信任裝置
- 匯出和匯入受信任裝置的清單

Firewall

- 關於防火牆規則
- 配置防火牆
  - 配置一般防火墻設定
  - 建立和設定防火牆規則
  - 啟用和停用防火牆規則

BadUSB 攻擊防護

系統完整性監控

- 關於系統完整性監控規則
- 即時系統完整性監控
- 按需系統完整性檢查
- 匯出和匯入系統完整性監控規則
- 檢視系統完整性監控報告

記錄審查

- 新增自訂規則
- 配置預定義規則

按需掃描

- 關於自訂掃描工作
- 關於工作掃描範圍和安全設定
- 預定義的掃描範圍
- 線上儲存檔案掃描
- 關於預定義安全等級
- 卸除式磁碟機掃描
- 預設自訂掃描工作設定
- 管理自訂掃描工作
  - 建立自訂掃描工作
    - 在背景執行自訂掃描工作
    - 記錄關鍵區域掃描執行
  - 配置按需掃描工作中的掃描範圍
  - 配置按需掃描工作設定
  - 配置卸除式磁碟機掃描
  - 為自訂掃描工作選擇預定義的安全等級
  - 手動配置安全性設定
  - 自訂掃描工作統計

Kaspersky Embedded Systems Security 資料庫和軟體模組更新

- 更新資料庫和應用程式模組
- 關於更新工作
- Kaspersky Embedded Systems Security 資料庫和模組更新方案
- 設定更新工作
- 應用程式的 SMU 更新
- 安全複製應用程式資料庫
- 安全更新應用程式資料庫
- 回溯 Kaspersky Embedded Systems Security 資料庫更新
- 更新工作統計

製作物件的備份副本
製作物件的備份副本。備份
檢視備份中的物件
從備份還原檔案
從備份刪除檔案
傳送可疑感染物件到 Kaspersky 以供分析
配置備份設定
備份統計
封鎖存取網路資源。已封鎖的網路工作階段
已封鎖的網路工作階段清單
管理已封鎖的網路工作階段清單
事件註冊。Kaspersky Embedded Systems Security 記錄
註冊 Kaspersky Embedded Systems Security 事件的方式
設定記錄設定
對記錄中的事件進行排序
篩選記錄中的事件
從記錄中刪除事件
匯出記錄中的資訊
系統稽核記錄
元件和工作日誌
在事件檢視器中檢視 Kaspersky Embedded Systems Security 事件記錄
關於 SIEM 整合
配置 SIEM 整合設定
管理員和使用者通知方式
設定管理員和使用者通知
配置電子郵件通知
配置與管理伺服器的互動
BitLocker 完整磁碟加密管理
啟動 BitLocker 磁碟機加密
解密受 BitLocker 防護的硬碟磁碟機
還原對 BitLocker 防護的磁碟機的存取權限
暫停 BitLocker 防護以更新軟體
與協力廠商系統整合
系統監視器的效能計數器
因為資源不足而未處理的要求數
已提交進行處理的請求數量
每秒處理的物件數
受感染物件佇列中的元素數
拒絕需求總數
略過請求總數
檔案攔截調度程式執行緒的最大數
檔案攔截調度程式執行緒的平均數
Kaspersky Embedded Systems Security SNMP 計數器和 TRAP
Kaspersky Embedded Systems Security SNMP 計數器
效能計數器
備份計數器
一般計數器

更新計數器
即時檔案防護計數器
AMSI 掃描程式計數器
Kaspersky Embedded Systems Security SNMP 陷阱及其選項
Kaspersky Embedded Systems Security SNMP 陷阱選項說明和可能值
WMI 整合
Managed Detection and Response
配置 MDR 整合
透過命令列管理 Kaspersky Embedded Systems Security
APPCONTROL.匯入應用程式啟動控制規則
APPCONTROL /CONFIG。設定 應用程式啟動控制 元件
APPCONTROL /GENERATE。應用程式啟動控制規則產生器
CONFIG.支援 AM-PPL 技術
DEVCONTROL。匯入裝置控制規則
DUMP。記錄記憶體傾印
EXITPOLICY。停用裝置上的政策
EXPORT。匯出應用程式設定
FBRESET。清除 iSwift 資料庫
FIM /BASELINE。基於基線的系統完整性監控
HELP.顯示指令說明
IMPORT。匯入應用程式設定
KSN。使用 KSN/KPSN
LICENSE。應用程式啟動
MDR。設定託管式偵測與回應整合
OMSINFO。建立包含應用程式資訊的 JSON 檔案
密碼。對 Kaspersky Embedded Systems Security 功能進行受密碼防護的存取
PATCHCOMPATIBILITYRESET。從不相容修補程式清單中移除修補程式
REMOTEACCESS.管理應用程式主控台遠端連線設定
RESETMDRMACHINEID。重設裝置 ID
ROLLBACK。上次更新回溯
RTP。即時檔案防護
SCAN。按需掃描
SCANCRITICAL。關鍵區域掃描
SERVERBINDINGDISABLE。停用管理員伺服器連線防護
START。啟動應用程式服務
STARTPOLICY。啟用政策
STOP。停止應用程式服務
TASK。管理工作
TRACE。追蹤應用程式作業
UPDATE。更新資料庫和程式模組
聯絡技術支援
如何獲取技術支援
透過 Kaspersky CompanyAccount 取得技術支援
向技術支援專家提供延伸診斷資訊
追蹤應用程式作業
偵錯檔案的內容和儲存
記錄記憶體傾印

防護傾印檔案和偵錯檔案
取得作業系統資料 (Kaspersky Get System Info)
有關 Kaspersky Embedded Systems Security 的資訊來源
附錄
用於快速掃描的檔案副檔名
應用程式元件規則中的使用者帳戶
法律資訊
資料提供
在最終使用者產品授權協議下的資料提供
使用卡巴斯基安全網路時的資料提供
符合歐洲聯盟法規（GDPR）
有關協力廠商程式碼資訊
商標聲明

Kaspersky Embedded Systems Security for Windows

Kaspersky Embedded Systems Security for Windows（以下也稱為 Kaspersky Embedded Systems Security）可防護執行 Microsoft® Windows® 的電腦和其他嵌入式系統（以下也稱為受防護裝置）抵禦病毒和其他電腦威脅。Kaspersky Embedded Systems Security 管理者是負責公司網路病毒防護的系統管理員和專業人員。

該應用程式不適用於涉及自動化控制系統的技術流程。為了防護此類系統中的裝置，建議使用 Kaspersky Industrial CyberSecurity for Nodes 應用程式。

您可以在執行 Windows 的各種嵌入式系統上安裝 Kaspersky Embedded Systems Security，包括以下裝置類型：

- ATM（自動櫃員機）。
- POS（銷售終端）。

可透過以下方式管理 Kaspersky Embedded Systems Security：

- 透過與 Kaspersky Embedded Systems Security 安裝在同一台受防護裝置上或安裝在其他裝置上的應用程式主控台來管理。
- 在命令列中使用指令
- 透過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也可以集中管理執行 Kaspersky Embedded Systems Security 的多台受防護裝置。

您可以檢視針對“系統監控器”應用的 Kaspersky Embedded Systems Security 效能計數器以及 SNMP 計數器和 TRAP。

Kaspersky Embedded Systems Security 元件和功能

應用程式包含以下元件：

- **即時檔案防護**Kaspersky Embedded Systems Security 在物件被存取時掃描物件。Kaspersky Embedded Systems Security 掃描以下物件：
  - 檔案
  - 交換檔案系統執行緒（NTFS 執行緒）
  - 本機磁碟和卸除式磁碟機上的主開機紀錄區和啟動磁區
- **按需掃描**Kaspersky Embedded Systems Security 可在指定區域執行單獨的掃描，以偵測病毒和其他電腦安全威脅。應用程式會掃描受防護裝置上的檔案、RAM 和自動執行物件。
- **應用程式啟動控制**該元件會監控使用者啟動應用程式的嘗試並調節受防護裝置上的應用程式啟動。

- **裝置控制**該元件可控制外部裝置的註冊和使用，以便防護裝置在與 USB 連線的快閃記憶體磁碟機或其他類型的外部裝置交換檔案時，免受可能產生的電腦安全威脅。

- **防火牆**根據其模式，此元件：會監控 Windows 防火牆的流量篩選；僅在元件的記錄中記錄有關受防護電腦的網路活動事件；或根據防火牆設定篩選網路流量。

- **檔案完整性監控**Kaspersky Embedded Systems Security 可以偵測工作設定中指定的監控範圍內的檔案變更。這些變更可能表示受防護裝置遭到安全入侵。

- **記錄審查**此元件根據 Windows 事件記錄的審查結果，對受防護環境的完整性進行監控。

應用程式中佈署了以下功能：

- **更新**Kaspersky Embedded Systems Security 會從 Kaspersky 的 FTP 或 HTTP 更新伺服器、卡巴斯基安全管理中心管理伺服器或其他更新來源下載應用程式資料庫和模組更新。

- **隔離區**Kaspersky Embedded Systems Security 透過將疑似感染物件從原始位置移動到*隔離區*資料夾來進行隔離。出於安全考慮，隔離資料夾中的物件以加密形式儲存。

- **備份**對於被歸類為"*已感染*"的物件，Kaspersky Embedded Systems Security 會在對其進行解毒或刪除之前，在*備份*中儲存這些物件的加密副本。

- **管理員和使用者通知**。您可以將應用程式設定為向管理員和存取受防護裝置的使用者通知 Kaspersky Embedded Systems Security 執行中的事件和裝置的病毒防護狀態。

- **匯入和匯出設定**。可以將 Kaspersky Embedded Systems Security 設定匯出到 XML 設定檔，也可以將設定檔中的設定匯入到 Kaspersky Embedded Systems Security 中。可以將所有應用程式設定或僅將單個元件的設定儲存到設定檔。

- **套用範本**。您可以在受防護裝置的檔案資源樹狀目錄或清單中手動配置節點的安全設定，並將配置好的設定值儲存為範本。然後可在 Kaspersky Embedded Systems Security 防護和掃描工作中使用該範本來指定其他節點的安全設定。

- **管理 Kaspersky Embedded Systems Security 功能的存取權限**。您可以為使用者和使用者群組設定管理 Kaspersky Embedded Systems Security 的權限和管理應用程式註冊的 Windows 服務的權限。

- **將事件寫入 Windows 事件記錄**。Kaspersky Embedded Systems Security 將記錄有關軟體元件設定的資訊、目前工作狀態、工作執行過程中發生的事件、與 Kaspersky Embedded Systems Security 管理相關的事件，以及 Kaspersky Embedded Systems Security 錯誤診斷所需的資訊。

- **受信任區域**您可以從防護範圍或掃描範圍中產生排除清單，Kaspersky Embedded Systems Security 將在自訂和即時電腦防護工作中套用該清單。

- **弱點利用防禦**您可以使用注入處理程序的防護代理來防護處理程序記憶體免受弱點利用。

更新功能（包括提供防毒簽章更新和程式碼庫更新）以及 KSN 功能在美國的軟體中可能無法使用。

新增功能

更新 4.1

Kaspersky Embedded Systems Security 4.1 for Windows 引入了以下功能和改進：

- Windows BitLocker 加密管理功能現已可用。此應用程式支援使用 Kaspersky Security Center 加密及解密受防護裝置的硬碟，並恢復加密磁碟機的存取權。
- 您現在可以設定排程工作，使其僅在指定的星期幾，依指定的週數間隔執行。排程在卡巴斯基安全管理中心 16.1 或更高版本中可用。
- 您現在可以將自訂掃描工作暫停一段選定的時間，例如，以執行例行維護。
- 「*對裝置的操作被禁止，直到 Kaspersky Embedded Systems Security 啟動為止*」和「*裝置連線被封鎖，直到 Kaspersky Embedded Systems Security 啟動為止*」事件現已可用。現在，如果裝置在應用程式啟動前遭到封鎖，系統將產生相應的事件並將其傳送至管理伺服器。
- 目前支援以下作業系統：
  - Windows 11 26H2
  - Windows 11 IoT 25H2
- 透過減少 I/O 作業次數，已最佳化受防護裝置上硬碟子系統的效能。
- 在開發此版本的 Kaspersky Embedded Systems Security 時，我們納入了以下專用修補程式中包含的變更：PF23074、PF23088、PF23089、PF23099、PF23102、PF23104、PF23105。

更新 4.0

Kaspersky Embedded Systems Security 4.0 提供以下功能和改進：

- 極大地更新了應用程式主控台的使用者介面和使用卡巴斯基安全管理中心應用程式的外掛程式。
- 支援 Windows 11 24H2。
- 現在，您可以變更應用程式主控台用來連線到安裝了應用程式的電腦的連接埠。
- 在*受信任區域*中，您可以：
  - 以更精細的方式設定受信任處理程序。
  - 使用受信任憑證儲存。
- 用來管理應用程式的使用者和群組權限的新設定。

- 新的*Rootkit 防護*元件。預設情況下，如果啟用*即時檔案防護*則啟用此元件。您可以在安裝應用程式時、使用*變更 Kaspersky Embedded Systems Security 的元件* 工作、或者在應用程式安裝套件的內容中停用該元件。
- 在*弱點利用防禦*設定中，應用程式現在可以自動辨識身分受防護的處理程序。
- 新的*修復引擎*元件。
- 網路威脅防護元件可以監控網路流量以偵測連接埠掃描和高強度網路請求。
- 應用程式現在與 Windows 防火牆相容。您再也不需要移除 Windows 防火牆來安裝應用程式。
- *行為偵測*元件可監控共用資料夾以及本機資料夾。
- 修訂了*應用程式啟動控制*元件：
  - 元件設定的結構中有重大變更。
  - 若要指定應用程式啟動控制規則觸發條件和排除項目，您現在可以使用磁碟機類型、KL 類別和 KSN 群組。
- 修訂了*裝置控制*元件：
  - 預設情況下，*裝置控制*元件被設定為允許連線所有裝置。
  - *Wi-Fi 控制*不再是單獨元件，現在是裝置控制的一部分。
  - 新增了根據連線匯流排控制已連線裝置的可能。
  - 新增了從先前版本的應用程式升級到版本 4.0 時遷移存取卸除式磁碟機的設定的功能。
- *防火牆管理*元件被修訂加入*防火牆*元件，它除了與 Windows 防火牆互動外，現在額外作為防火牆運作。
- *檔案完整性監控*和 *登錄檔存取監控*元件的功能被合併入新的*系統完整性監控*元件中。這一改進可讓您有效追蹤檔案系統和 Windows 登錄檔中的變更，從而提高對未經授權修改資料的防護。
- 應用程式不支援排程單個元件。如果啟用這些元件，它們會在應用程式執行時繼續執行。
- 現在支援卡巴斯基安全管理中心 Windows 15.1。
- 新增了群組工作：
  - *管理員伺服器連線防護*
  - *變更了 Kaspersky Embedded Systems Security 元件集*
  - *基線系統完整性監控*取代*基線檔案完整性監控*
  - "*更新*"取代"*複製更新*"、"*應用程式資料庫更新*"和"*軟體模組更新*"
  - "*更新回溯*"取代"*應用程式資料庫更新回溯*"
  - *移除金鑰*

- 應用程式在儲存設定之前會先檢查控制元件的組態。新增了對「應用程式控制」、「裝置控制」、「系統完整性監控」元件的檢查。現在，如果控制元件的當前設定可能會增加電腦負載或導致系統故障，應用程式會顯示警告。例如，就「應用程式控制」而言，若您選取了封鎖除允許的應用程式之外的所有應用程式的模式，並且沒有新增任何允許規則，應用程式會顯示警告，因為此類組態可能會導致系統故障。

- 新增了自動建立應用程式啟動控制的允許規則並將這些規則匯出至檔案的可能。為此，請執行*應用程式啟動控制的規則產生器*工作，並啟用基於正在執行的應用程式自動建立允許規則以及匯出允許規則。您可以使用產生的檔案清查安裝在裝置上的軟體。

- 新元件，*BadUSB 攻擊防護*。BadUSB 攻擊防護元件可以防止受感染的模擬鍵盤的 USB 裝置連線至電腦。當被作業系統識別為鍵盤的 USB 裝置連線至電腦時，應用程式會提示使用者在此鍵盤上鍵入以授權鍵盤。

- *安全等級指示器*已新增。安全等級指示器顯示在政策屬性視窗的頂部，顯示安全設定對 Kaspersky Lab 建議的遵守程度。安全等級指示器可讓您快速配置政策和啟用所需的防護元件。

已修正的問題

下表列出在 Kaspersky Embedded Systems Security 先前版本中發現，並已在目前版本中修正的所有問題。

4.1 版本中修正的問題清單

識別碼	問題描述
9986614	在 Web Console 和 Kaspersky Security Center 管理主控台中，無法從 TXT 檔案匯入受信任裝置清單；該檔案包含從 Web Console 匯出的 Kaspersky Security Center 事件選取項目，這些事件與遭封鎖的裝置有關。
10700703	在 系統完整性監控、受信任區域、應用程式啟動控制 和 裝置控制 元件的介面中，無法立即看出如何選取清單項目以執行 **匯出所選** 命令。應用程式說明中的描述已擴充。
10720231	Kaspersky Security Center 管理主控台之政策的 **裝置控制** 區段中未顯示受信任裝置計數器。
10729552	即使已啟用此類事件的記錄功能，仍不會產生與卸除式磁碟機上檔案操作相關的事件。
10752491	在 Web Console 中，無法從 TXT 檔案匯入受信任裝置清單；該檔案包含從管理主控台匯出的 Kaspersky Security Center 事件選取項目，這些事件與遭封鎖的裝置有關。

分發套件

分發套件包含常用的應用程式，您可以用它來執行以下操作：

- 啟動 Kaspersky Embedded Systems Security 安裝精靈。

- 啟動 Kaspersky Embedded Systems Security 主控台安裝精靈。

- 啟動卡巴斯基病毒清除工具。

- 閱讀此版本的 Kaspersky Embedded Systems Security。

- 開啟 Kaspersky Embedded Systems Security 4.1 說明。

- 前往 Kaspersky 網站上的 Kaspersky Embedded Systems Security 頁面。

- 造訪卡巴斯基網站。
- 造訪技術支援網站。

分發套件檔案儲存在不同的資料夾中，具體位置取決於它們的目標用途（請參見以下表格）。

Kaspersky Embedded Systems Security 分發套件檔案

檔案	用途
autorun.inf	從卸除式磁碟機安裝應用程式時，Kaspersky Embedded Systems Security 安裝精靈的自動執行檔案。
setupui.exe	應用程式歡迎螢幕啟動檔案。
ess_win.kud	Kaspersky Unicode 定義格式的檔案，帶有用於透過卡巴斯基安全管理中心遠端安裝應用程式的安裝套件的說明。
\console\esstools.msi	Windows Installer 安裝套件；在受防護的裝置上安裝 Kaspersky Embedded Systems Security 主控台。
\console\setup_esstool.exe	用於啟動 Kaspersky Embedded Systems Security Console for Windows 安裝精靈的檔案。安裝套件檔案 esstools.msi 使用精靈中指定的安裝設定來啟動。
\console\license.txt	Kaspersky Embedded Systems Security 管理主控台最終使用者產品授權協議和隱私權政策文字檔案。
\exec\bases.cab	應用程式發佈時最新病毒資料庫的壓縮檔案。
\exec\cleaner_v2.cab \exec\cleanerapi_v2.cab	用於刪除不相容軟體的檔案。
\exec\ess.cab	應用程式圖形介面檔案。
\exec\ess_win.kud	Kaspersky Unicode 定義格式的檔案，帶有用於透過卡巴斯基安全管理中心遠端安裝應用程式的安裝套件的說明。
\exec\ess_win.msi	Windows Installer 安裝套件：這會在受防護的裝置上安裝 Kaspersky Embedded Systems Security。
\exec\incompatible.txt	卡巴斯基不保證 Kaspersky Embedded Systems Security 系統與檔案中列出的應用程式的相容性。
\exec\installer.ini	包含分發套裝內部設定的檔案。
\exec\klcfginst.msi	Kaspersky Embedded Systems Security 管理外掛程式的安裝程式可透過卡巴斯基安全中心取得。如果您打算使用管理外掛程式來管理 Kaspersky Embedded Systems Security，請在安裝了卡巴斯基安全管理中心管理主控台的每個受防護裝置上安裝管理外掛程式。
\exec\ksn_en.txt	包含 KSN 聲明文字的檔案。
\exec\license.txt	Kaspersky Embedded Systems Security 最終使用者產品授權協議和隱私權政策文字檔案。
\exec\包.kcat	包含分發套件檔案的簽章的檔案。
\exec\setup_ess.exe	啟動用於在受防護裝置上安裝 Kaspersky Embedded Systems Security 的精靈的檔案；它使用精靈中指定的安裝設定啟動安裝程式套件檔案 ess_win.msi。
\kvrt\KVRT.exe	卡巴斯基病毒清除工具的安裝程式。
\product_long_term\cleaner_v2.cab \product_long_term\cleanerapi_v2.cab	用於刪除不相容軟體的檔案。
\product_long_term\ess.cab	應用程式圖形介面檔案。
\product_long_term\ess_win.kud	Kaspersky Unicode 定義格式的檔案，帶有用於透過卡巴斯基安全管理中心遠端安裝應用程式的安裝套件的說明。
\product_long_term\ess_win.msi	Windows Installer 安裝套件；此安裝套件用於在受防護裝置上以 **使用預設拒絕技術防護電腦**配置安裝 Kaspersky Embedded Systems Security for Windows。
\product_long_term\incompatible.txt	卡巴斯基不保證 Kaspersky Embedded Systems Security 系統與檔案中列出的應用程式的相容性。
\product_long_term\installer.ini	包含分發套裝內部設定的檔案。
\product_long_term\klcfginst.exe	Kaspersky Embedded Systems Security 管理外掛程式的安裝程式可透過卡巴斯基安全中心取得。如果您打算使用管理外掛程式來管理 Kaspersky Embedded Systems Security，請在安裝了卡巴斯基安全管理中心管理主控台的每個受防護裝置上安裝管理外掛程式。
\product_long_term\ksn_en.txt	包含俄語版 KSN 聲明文本的檔案。
\product_long_term\license.txt	Kaspersky Embedded Systems Security 最終使用者產品授權協議和隱私權政策文字檔案。
\product_long_term\package.kcat	包含分發套件檔案的簽章的檔案。

檔案	用途
\product_long_term\setup_ess.exe	啟動用於在受防護裝置上安裝 Kaspersky Embedded Systems Security 的精靈的檔案；它使用精靈中指定的安裝設定啟動安裝程式套件檔案 ess_win.msi。
\setup\images	包含應用程式歡迎螢幕啟動檔案的資料夾。
\setup\setup.hta	應用程式歡迎螢幕啟動檔案。
\setup\SETUP_STRINGS.JS	包含應用程式字串資源的檔案。

分發套件檔案可以從安裝 CD 執行。如果您已事先將分發套件檔案複製到本機磁碟機，請確保分發套件檔案的結構已保留。

硬體和軟體需求

對受防護裝置的軟體需求

本文列出應用程式已測試且保證可正常運作的軟體版本。應用程式也可能適用於其他軟體版本，但這些設定尚未經過完整測試週期，因此未包含在保證支援的版本清單中。

在執行 Microsoft Windows XP 的受防護裝置上正確安裝和操作應用程式需要 Windows Installer 3.1。

要在執行內嵌式作業系統的受防護裝置上安裝和使用 Kaspersky Embedded Systems Security，必須有篩選管理器元件 (Filter Manager)。

為使 Kaspersky Embedded Systems Security 正確操作，Microsoft Windows 需要 SHA-2 支援。如需瞭解詳細資訊，請參閱 技術支援網站上的知識庫。

您可以在執行下列 32 位元或 64 位元 Microsoft Windows 作業系統的伺服器上安裝 Kaspersky Embedded Systems Security：

工作站：

- Windows XP Professional SP2 32 位元 / 64 位元
- Windows XP Professional SP3 32 位元
- Windows Vista SP2 32 位元 / 64 位元
- Windows 7 SP1 Home / Pro / Enterprise / Ultimate 32 位元 / 64 位元
- Windows 8 Pro / Enterprise 32 位元 / 64 位元
- Windows 8.1 Pro / Enterprise 32 位元 / 64 位元

- Windows 10 TH1 Home / Pro / Pro for Workstations / Education / Enterprise 32 位元 / 64 位元
- Windows 10 TH2 Home / Pro / Pro for Workstations / Education / Enterprise 32 位元 / 64 位元
- Windows 10 RS1 Home / Pro / Pro for Workstations / Education / Enterprise 32 位元 / 64 位元
- Windows 10 RS2 Home / Pro / Pro for Workstations / Education / Enterprise 32 位元 / 64 位元
- Windows 10 RS3 Home / Pro / Pro for Workstations / Education / Enterprise 32 位元 / 64 位元
- Windows 10 RS4 Home / Pro / Pro for Workstations / Education / Enterprise 32 位元 / 64 位元
- Windows 10 RS5 Home / Pro / Pro for Workstations / Education / Enterprise 32 位元 / 64 位元
- Windows 10 RS6 Home / Pro / Pro for Workstations / Education / Enterprise 32 位元 / 64 位元
- Windows 10 19H2 Home / Pro / Pro for Workstations / Education / Enterprise 32 位元 / 64 位元
- Windows 10 20H1 Home / Pro / Pro for Workstations / Education / Enterprise 32 位元 / 64 位元
- Windows 10 20H2 Home / Pro / Pro for Workstations / Education / Enterprise 32 位元 / 64 位元
- Windows 10 21H1 Home / Pro / Pro for Workstations / Education / Enterprise 32 位元 / 64 位元
- Windows 10 21H2 Home / Pro / Pro for Workstations / Education / Enterprise 64 位元
- Windows 10 22H2 Home / Pro / Pro for Workstations / Education / Enterprise 64 位元
- Windows 11 21H2 Home / Pro / Pro for Workstations / Education / Enterprise 64 位元
- Windows 11 22H2 Home / Pro / Pro for Workstations / Education / Enterprise 64 位元
- Windows 11 23H2 Home / Pro / Pro for Workstations / Education / Enterprise 64 位元
- Windows 11 24H2 Home / Pro / Pro for Workstations / Education / Enterprise 64 位元
- Windows 11 25H2 Home / Pro / Pro for Workstations / Education / Enterprise 64 位元
- Windows 11 26H2 Home / Pro / Pro for Workstations / Education / Enterprise 64 位元

伺服器作業系統：

- Windows Server 2003 SP1 Standard / Enterprise 32 位元 / 64 位元
- Windows Server 2003 SP2 Standard / Enterprise 32 位元 / 64 位元
- Windows Server 2003 R2 SP2 Standard / Enterprise 64 位元
- Windows Server 2008 SP2 Standard / Enterprise 32 位元 / 64 位元
- Windows Server 2008 R2 SP2 Foundation / Standard / Enterprise 64 位元

內嵌系統：

- Windows XP Embedded Service Pack 3 32 位元
- Windows Embedded POSReady 7 32 位元 / 64 位元
- Windows Embedded Standard 7 Service Pack 1 32 位元 / 64 位元
- Windows Embedded 8 Standard 32 位元 / 64 位元
- Windows Embedded 8.1 Industry Pro 32 位元 / 64 位元
- Windows 10 IoT Enterprise 版本 1507 32 位元 / 64 位元
- Windows 10 IoT Enterprise 版本 1607 32 位元 / 64 位元
- Windows 10 IoT Enterprise 版本 1803 32 位元 / 64 位元
- Windows 10 IoT Enterprise 版本 1809 32 位元 / 64 位元
- Windows 10 IoT Enterprise 版本 1909 32 位元 / 64 位元
- Windows 10 IoT Enterprise 版本 21H2 32 位元 / 64 位元
- Windows 10 IoT Enterprise 版本 22H2 32 位元 / 64 位元
- Windows 11 IoT Enterprise 版本 21H2 64 位元
- Windows 11 IoT Enterprise 版本 22H2 64 位元
- Windows 11 IoT Enterprise 版本 23H2 64 位元
- Windows 11 IoT Enterprise 版本 24H2 64 位元
- Windows 11 IoT Enterprise 版本 25H2 64 位元

對受防護裝置的硬體需求

對受防護裝置的硬體需求

作業系統類型	作業系統名稱	最低要求	推薦要求

工作站	Windows XP x86 / x64	• 處理器：1.4 GHz 單核心處理器 Pentium III (x32)、Pentium IV (x64)
		• 記憶體：
		  • 僅安裝"應用程式啟動控制"元件 – 256 MB
		  • 安裝所有應用程式元件 – 512 MB
		• 可用磁碟空间：
		  • 僅安裝"應用程式啟動控制"元件 – 50 MB
		  • 安裝所有應用程式元件 – 2 GB
			• 處理器：2.4 GHz 四核
			• 記憶體：2 GB
			• 可用磁碟空间：
			  • 僅安裝"應用程式啟動控制"元件 – 2 GB
			  • 安裝所有應用程式元件 – 4 GB

	Windows 7 / 8 / 10 x86	• 處理器：1.4 GHz 單核心處理器 Pentium III (x32)、Pentium IV (x64)
		• 記憶體：
		  • 僅安裝"應用程式啟動控制"元件 – 256 MB
		  • 安裝所有應用程式元件 – 1 GB
		• 可用磁碟空间：
		  • 僅安裝"應用程式啟動控制"元件 – 50 MB
		  • 安裝所有應用程式元件 – 2 GB
			• 處理器：2.4 GHz 四核
			• 記憶體：2 GB
			• 可用磁碟空间：
			  • 僅安裝"應用程式啟動控制"元件 – 2 GB
			  • 安裝所有應用程式元件 – 4 GB

	Windows 7 / 8 / 10 / 11 x64	• 處理器：1.4 GHz 單核心處理器 Pentium IV (x64)
		• 記憶體：
		  • 僅安裝"應用程式啟動控制"元件 – 256 MB
		  • 安裝所有應用程式元件 – 1 GB
		• 可用磁碟空间：
		  • 僅安裝"應用程式啟動控制"元件 – 50 MB
		  • 安裝所有應用程式元件 – 2 GB
			• 處理器：2.4 GHz 四核
			• 記憶體：
			  • 僅安裝"應用程式啟動控制"元件 – 2 GB
			  • 安裝所有應用程式元件 – 4 GB
			• 可用磁碟空间：
			  • 僅安裝"應用程式啟動控制"元件 – 2 GB
			  • 安裝所有應用程式元件 – 4 GB

內嵌系統	Windows XP Embedded	• 處理器：1.4 GHz 單核心處理器 Pentium III (x32)、Pentium IV (x64)
		• 記憶體：
		  • 僅安裝"應用程式啟動控制"元件 – 256 MB
		  • 安裝所有應用程式元件 – 512 MB
		可用磁碟空间：
		• 僅安裝"應用程式啟動控制"元件 – 50 MB
		• 安裝所有應用程式元件 – 2 GB
			• 處理器：2.4 GHz 四核
			• 記憶體：2 GB
			• 可用磁碟空间：
			  • 僅安裝"應用程式啟動控制"元件 – 2 GB
			  • 安裝所有應用程式元件 – 4 GB

	Windows 7 / 8 Embedded
	Windows 10 / 11 IoT
		• 處理器：1.4 GHz 單核心處理器 Pentium IV (x64)
		• 記憶體：256 MB
		• 可用磁碟空间：
		  • 僅安裝"應用程式啟動控制"元件 – 50 MB
		  • 安裝所有應用程式元件 – 2 GB
			• 處理器：2.4 GHz 四核
			• 記憶體：2 GB
			• 可用磁碟空间：
			  • 僅安裝"應用程式啟動控制"元件 – 2 GB
			  • 安裝所有應用程式元件 – 4 GB

卡巴斯基安全管理中心的支援版本

Kaspersky Embedded Systems Security 與以下版本的卡巴斯基安全管理中心相容：

- 卡巴斯基安全管理中心 Linux 版本 14.2、15、15.1、15.2、15.3、15.4、16、16.1、16.2、16.3、17.0。透過卡巴斯基安全管理中心網頁主控台支援 Kaspersky Embedded Systems Security 的管理。
- 卡巴斯基安全管理中心 Windows 版本 14.2、15.1。透過卡巴斯基安全管理中心管理主控台版本以及卡巴斯基安全管理中心網頁主控台版本支援對 Kaspersky Embedded Systems Security 的管理。
- 卡巴斯基安全管理中心 Windows 版本 10.5、11。透過卡巴斯基安全管理中心管理主控台和卡巴斯基安全管理中心網頁主控台，支援管理安裝在執行 Microsoft Windows XP SP2 作業系統之裝置上的 Kaspersky Embedded Systems Security。

若要透過卡巴斯基安全管理中心管理 Kaspersky Embedded Systems Security，需要卡巴斯基安全管理中心網路代理程式。

卡巴斯基安全管理中心網路代理程式不包含在 Kaspersky Embedded Systems Security 分發套件中。您可以在**卡巴斯基安全管理中心**部分的應用程式下載頁面上下載。

功能要求和限制

本節介紹 Kaspersky Embedded Systems Security 元件的附加功能要求和現有限制。

安裝和移除應用程式

- 為使 Kaspersky Embedded Systems Security 正確操作，Microsoft Windows 需要 SHA-2 支援。
- 安裝應用程式時，如果前往 Kaspersky Embedded Systems Security 安裝資料夾的指定路徑包含超過 150 個字元，畫面上可能會出現警告。該警告不會影響安裝流程：您可以安裝並執行 Kaspersky Embedded Systems Security。
- 如果要安裝 SNMP 通訊協定支援元件，請確保在 SNMP 服務正在執行時重新啟動 SNMP 服務。
- 如果您想在執行內嵌作業系統的裝置上安裝並執行 Kaspersky Embedded Systems Security，請確保安裝篩選器管理員元件。
- 您無法透過 Microsoft Active Directory® 群組政策安裝管理工具。
- 如果從已安裝的應用程式元件清單中排除病毒防護節點，則此節點會在安裝完成後從可用元件清單中消失。若要安裝病毒防護節點的元件，請從安裝套件啟動安裝精靈，因為安裝套件包含完整的元件清單。
- 如果安裝了 Kaspersky Embedded Systems Security 管理主控台，安裝精靈可能會提示重新啟動電腦。在這種情況下，重新開機不是強制性質。只要結束安裝管理主控台之使用者的工作階段並重新登入系統即可。

- 在 Windows XP 或 Windows Vista 裝置上安裝應用程式時，您可能需要安裝 DigiCert Assured ID Root CA 憑證以啟用驅動程式簽章驗證。如有必要，該憑證將從應用程式的安裝套件自動安裝到作業系統的受信任根憑證儲存區。

- 在 Windows XP 或 Windows Vista 裝置上安裝應用程式時，您需要檢查 DigiCert High Assurance EV Root CA. 是否存在。

  如果未安裝此根憑證，應用程式可能無法正常運作。我們建議您盡快安裝憑證。

- 如果安裝資料夾的路徑與以下資料夾中至少之一的路徑相同，則應用程式安裝結束時會出現錯誤：應用程式資料庫資料夾、備份資料夾、用於從隔離區還原物件的資料夾、暫存檔資料夾。

- 如果您使用卡巴斯基安全管理中心雲端主控台管理 Kaspersky Embedded Systems Security，則不允許在本機更新應用程式。在本機更新應用程式時，無法接受卡巴斯基安全管理中心雲端主控台的資料處理協定。

系統完整性監控

預設情況下，系統完整性監控元件不監控系統資料夾或檔案系統清理檔案的變化，以免有關作業系統不斷執行的例程檔案變更的資訊混雜在工作報告中。您無法在監控範圍中包含此類資料夾。

以下資料夾和檔案被從監控範圍中排除：

- 檔案 id 從 0 到 33 的 NTFS 清理檔案
- %SystemRoot%\Prefetch\
- %SystemRoot%\ServiceProfiles\LocalService\AppData\Local\
- %SystemRoot%\System32\LogFiles\Scm\
- %SystemRoot%\Microsoft.NET\Framework\v4.0.30319\
- %SystemRoot%\Microsoft.NET\Framework64\v4.0.30319\
- %SystemRoot%\Microsoft.NET\
- %SystemRoot%\System32\config\
- %SystemRoot%\Temp\
- %SystemRoot%\ServiceProfiles\LocalService\
- %SystemRoot%\System32\winevt\Logs\
- %SystemRoot%\System32\wbem\repository\
- %SystemRoot%\System32\wbem\Logs\
- %ProgramData%\Microsoft\Windows\WER\ReportQueue\
- %SystemRoot%\SoftwareDistribution\DataStore\
- %SystemRoot%\SoftwareDistribution\DataStore\Logs\

- %ProgramData%\Microsoft\Windows\AppRepository\
- %ProgramData%\Microsoft\Search\\Data\Applications\Windows\
- %SystemRoot%\Logs\SystemRestore\
- %SystemRoot%\System32\Tasks\Microsoft\Windows\TaskScheduler\

應用程式會排除頂層資料夾。

該元件不監控繞過 ReFS/NTFS 檔案系統的檔案變更（透過 BIOS、LiveCD 等進行的檔案變更）。

Firewall

- 您應該指定多個位址。否則，無法使用 IPv6。
- 預設的防火牆規則支援受防護裝置與管理伺服器之間的基本互動方案。若要充分利用卡巴斯基安全管理中心功能，您需要設定連接埠規則。您可以在卡巴斯基安全管理中心知識庫中找到有關連接埠號、通訊協定及其功能的資訊。
- 安裝應用程式並設定防火牆規則後，應用程式將在防火牆元件執行時監控 Windows 防火牆規則和規則群組的變更。若要更新狀態並新增必要的 Windows 防火牆規則，請重新啟動防火牆元件。
- 當您啟動防火牆元件時，拒絕規則和控制出站流量的規則會被自動從 Windows 防火牆設定中刪除。
- 字元 `*` 和 `?` 無法用於應用程式路徑和應用程式的防火牆規則名稱。
- 如果選取 *觀察 Windows 防火牆狀態* 模式，Windows 防火牆設定（**設定 → 更新與安全性 → Windows 安全性 → 防火牆與網路保護**）將顯示 Kaspersky Embedded Systems Security 防火牆已停用。如果您點擊啟用防火牆的按鈕，其運作模式將變更為 *封鎖*。
- 在執行 Windows 7 和 Windows Server 2008 R2 的電腦上，基於服務名稱為 TermService 服務配置的防火牆規則不會限制透過 RDP 的存取。
- 當防火牆在 **封鎖** 模式下執行時，應用程式會阻止從 DHCP 伺服器取得 IP 位址。若要取得 IP 位址，請設定防火牆以允許 svchost.exe 系統處理程序。

對過時 Windows 版本的限制

- Windows XP SP2 版本不允許封鎖遠端裝置和配置被封鎖的網路工作階段設定清單。在該 Windows 版本中，**封鎖對顯示惡意活動的工作階段的網路共用資源的存取**選項處於不活動狀態。

- Kaspersky Embedded Systems Security 安裝：

  - 在執行 Windows XP SP2 Professional（32 位元/64 位元）、Windows Server 2003 和 Windows Server 2003 R2 的電腦上，您應該使用應用程式分發套件，或將標準安裝套件「卡巴斯基安全管理中心 10.5 網路代理 for Windows XP」中的 setup.exe 可執行檔放入卡巴斯基安全管理中心的應用程式安裝套件資料夾中。

  - 在執行 Windows XP SP3 Professional（32 位元）和 Windows XP Embedded SP3（32 位元）的電腦上，需要使用應用程式分發套件或將在卡巴斯基安全管理中心 14 中建立的應用程式安裝套件中的 setup.exe 可執行檔或來自標準安裝套件「卡巴斯基安全管理中心14 網路代理 for Windows XP」的 setup.exe 可執行檔放入到卡巴斯基安全管理中心中的應用程式安裝套件資料夾中。

  如何從標準卡巴斯基安全管理中心安裝套件中提取 setup.exe 檔案

  1. 在卡巴斯基安全管理中心管理主控台樹狀目錄中，選擇 **進階 → 遠端安裝 → 安裝套件**。
  2. 在工作區中點擊**附加操作**然後從下拉式清單中選擇**檢視卡巴斯基應用程式的目前版本**。
  3. 從清單中選擇必要的應用程式。例如，適用於 Windows XP 的卡巴斯基安全管理中心10.5 網路代理。
  4. 點擊**下載並建立安裝套件**按鈕。

     建立的安裝套件將顯示在**安裝套件**清單中。
  5. 開啟已建立的安裝套件的屬性。
  6. 在**一般**部分，將路徑複製到安裝套件資料夾。
  7. 開啟安裝套件資料夾。
  8. 複製 setup.exe 檔案。

- 若要透過卡巴斯基安全管理中心管理 Kaspersky Embedded Systems Security：

  - 在執行 Windows XP SP2 Professional（32 位元/64 位元）、Windows Server 2003 或 Windows Server 2003 R2 的電腦上，您必須使用卡巴斯基安全管理中心網路代理程式 (klnagent) 版本 10.5.1781。

  - 在執行 Windows XP SP3 Professional（32 位元）和 Windows XP Embedded SP3（32 位元）的電腦上，您必須使用卡巴斯基安全管理中心網路代理程式 (klnagent) 版本 14.0.0.20023。

- 在 Windows XP 電腦上，無法使用 MQTT 通信協定將遙測資料傳送到資料二極管。

與卡巴斯基安全管理中心整合

- 收到更新套件後，管理伺服器會先驗證資料庫更新，然後再將更新傳送到網路上的受防護裝置。卡巴斯基安全管理中心管理伺服器不驗證應用程式模組更新。
- 當借助網路清單（隔離、備份）使用將動態資料傳輸到卡巴斯基安全管理中心的元件時，確保在與卡巴斯基安全管理中心管理伺服器設定的互動中選中所需核取方塊。
- 網路代理 10.5 不會將已安裝元件的資訊傳送至卡巴斯基安全管理中心管理伺服器。因此，在卡巴斯基安全管理中心管理主控台和卡巴斯基安全管理中心網頁主控台中，具有網路代理 10.5 的裝置的設定不會顯示已安裝的 Kaspersky Embedded Systems Security 元件及其設定。
- 如果裝置上安裝了卡巴斯基安全管理中心網路代理程式 10.5，您將無法使用卡巴斯基安全管理中心網頁主控台下載備份中的檔案。
- 如果 Kaspersky Embedded Systems Security 安裝時啟用了卡巴斯基安全管理中心網路代理的低資源消耗模式（預設情況下， `SKIP_KLNAG_FLAG_TEST_VM_PERF=0` ）然後安裝網路代理，則 Kaspersky Embedded Systems Security 不會在 Windows 防火牆中為網路代理建立排除項目，因此 Windows 防火牆會封鎖網路代理。
- 如果 Kaspersky Embedded Systems Security 安裝時啟用了卡巴斯基安全管理中心網路代理的低資源消耗模式（預設情況下， `SKIP_KLNAG_FLAG_TEST_VM_PERF=0` ），網路清單的修改會延遲大約十分鐘反映在卡巴斯基安全管理中心管理主控台中。
- 在卡巴斯基安全管理中心管理主控台中搜尋受管理裝置時， **應用程式元件** 頁簽可能會同時顯示相同應用程式元件名稱的多個變體，包括與舊版 Kaspersky Embedded Systems Security 對應的名稱。某些元件的名稱也可能重複。

  要按元件搜索，您只需選擇顯示的其中一個變體即可。有關裝置發現的詳細資訊，請參閱卡巴斯基安全管理中心說明。

其他限制

按需掃描 和 即時檔案防護

- 不能掃描已連線的 MTP 裝置。
- 如果沒有 SFX 壓縮檔案掃描，壓縮檔案掃描無法使用：如果 Kaspersky Embedded Systems Security 的防護設定中啟用了壓縮檔案掃描，應用程式會自動掃描壓縮檔案和 SFX 壓縮檔案中的物件。如果沒有壓縮檔案掃描，SFX 壓縮檔案掃描仍可用。
- 如果「**深度分析正在啟動的處理程序（分析期間封鎖處理程序啟動）**」核取方塊和 **KSN 使用**同時啟用，任何將 URL 網址作為參數接收的已啟動處理程序都會被封鎖，即使選擇了「通知」模式。為避免封鎖處理程序，請選擇以下選項之一：
  - 停用**KSN 使用**。
  - 停用**深度分析正在啟動的處理程序（分析期間封鎖處理程序啟動）**核取方塊

建議選項：清除「**深度分析正在啟動的處理程序（分析期間封鎖處理程序啟動）**」核取方塊。

產品授權

- 如果使用 SUBST 指令建立金鑰，或者金鑰檔案的路徑是網路路徑，則您無法透過安裝精靈使用金鑰啟動應用程式。
- 如果您計畫使用卡巴斯基安全管理中心代理伺服器在用戶端裝置上啟動產品，請在安裝卡巴斯基安全管理中心網路代理程式時在該裝置上停用 VDI 最佳化。

更新

- 在 Windows XP 裝置上安裝及解除安裝 Kaspersky Embedded Systems Security 修補程式時，由於此作業系統的特殊性，可能需要重新啟動裝置。
- 預設情況下，安裝 Kaspersky Embedded Systems Security 關鍵模組更新後，會隱藏應用程式圖示。
- 執行 Windows XP 或 Windows Server® 2003 作業系統的受防護裝置不支援 KLRAMDISK。
- 如果 Kaspersky Embedded Systems Security 修補程式安裝失敗，修補程式將會被回溯，並提示您重新啟動作業系統。

介面

- 在應用程式主控台中，隔離區、備份區、系統稽核記錄或工作記錄中的篩選大小寫視為相異。
- 在應用程式主控台中配置防護或掃描範圍時，只能使用一個遮罩，並且只能在路徑末尾使用。下列是正確遮罩的範例：`C:\Temp\Temp*`、`C:\Temp\Temp???.doc`、`C:\Temp\Temp*.doc`。此限制不影響信任區域的配置。
- 應用程式主控台中的**遙測資料收集伺服器**區域，不顯示工作排程執行的時間。「**開始時間**」列為空。
- 在卡巴斯基安全管理中心管理主控台或應用程式主控台中，不會顯示長度超過 256 個字元的介面文字元素的彈出通知。
- 在卡巴斯基安全管理中心管理主控台中，**請選擇一個使用者或一組使用者** 視窗僅顯示卡巴斯基安全管理中心使用者清單中的前 50,000 位使用者。有關詳細資訊，請參閱卡巴斯基安全管理中心說明。

安全性

- 如果作業系統的使用者帳戶控制功能已啟用，則使用者帳戶必須屬於 ESS 管理員群組，才能透過按兩下工作列通知區域中的應用程式圖示來開啟應用程式主控台。否則，需要以被允許開啟小型診斷介面或 Microsoft 管理主控台管理單元的使用者身分登入。

- 如果啟用了使用者帳戶控制，則無法透過 Microsoft Windows 程式和功能視窗解除安裝應用程式。

弱點利用防禦

- 如果目前環境配置中未載入 apphelp.dll 庫，則弱點利用防禦無法使用。

- 弱點利用防禦與執行 Microsoft Windows 10 作業系統的受防護裝置上的 Microsoft 提供之 EMET 實用工具不相容。如果在安裝了 EMET 實用工具的受防護裝置上安裝弱點利用防禦元件，Kaspersky Embedded Systems Security 會封鎖 EMET。

- 弱點利用防禦 與 SQL Server® 的 2012 資料庫引擎不相容。如果您在安裝 MS SQL Server 2012 的電腦上安裝 Kaspersky Embedded Systems Security，您必須將資料庫伺服器的 sqlos.dll 庫新增至弱點利用防禦工作的排除清單中。

Detection and Response

- 如果在威脅回應過程中發生共用資料夾存取錯誤，則此類錯誤不會反映在威脅回應歷史記錄中（卡巴斯基安全中心網頁主控台 → 已安裝應用程式的主機的屬性 → **Detection and Response – 回應歷史** 部分）。

事件組態

可以在卡巴斯基安全管理中心政策的**事件組態**部分中配置的 *受控區域內的受控檔案操作* 事件的設定也會被套用到以下事件：

- *在受控區域內由受信任使用者執行的受允許檔案操作*

- *在受控區域內被禁止的檔案操作*

- *僅統計：在受控區域內被禁止的檔案操作*

- *受控區域內的受控檔案操作*

小型診斷視窗

在 Windows XP 電腦上，小型診斷視窗需要 Terminal Service 才能運作

在 Windows 安全性模式下工作

應用程式無法在 Windows Safe Mode 下工作。

與其他應用程式的相容性

Kaspersky Embedded Systems Security 與屬於協力廠商端點防護系統（端點防護平台，EPP）的應用程式不相容。Kaspersky Embedded Systems Security 也可能與其他應用程式和某些卡巴斯基應用程式不相容。為了確定相容性，Kaspersky Embedded Systems Security 會查閱卡巴斯基準備的軟體清單。該清單包含在 incomplete.txt 檔案中。該檔案包括在分發套件中。

如果偵測到 incompatible.txt 清單中的應用程式，則安裝程式會放棄安裝 Kaspersky Embedded Systems Security。您需要移除協力廠商病毒防護應用程式。安裝程式可能會自動從清單中刪除某些應用程式。

如果電腦上安裝了 Windows Firewall，安裝程式會將其關閉以繼續安裝 Kaspersky Embedded Systems Security。

如果儘管存在這些風險，您仍然需要和 incompatible.txt 清單中的應用程式一起安裝 Kaspersky Embedded Systems Security，則可以略過檢查已安裝的協力廠商病毒防護應用程式。為此，當執行安裝程式時，請指定以下參數：`SKIPPRODUCTCHECK=1` 和 `SKIPPRODUCTUNINSTALL=1`。

範例:

```
setup_ess.exe /s EULA=1 PRIVACYPOLICY=1 SKIPPRODUCTCHECK=1 SKIPPRODUCTUNINSTALL=1
```

安裝和移除應用程式

本節提供安裝和移除 Kaspersky Embedded Systems Security 的逐步說明。

安裝排程

本節包含 Kaspersky Embedded Systems Security 管理工具集的說明以及使用精靈、命令列、使用卡巴斯基安全管理中心和透過 Active Directory 群組政策安裝和移除 Kaspersky Embedded Systems Security 的特殊方面。

如果您在刪除 Kaspersky Industrial CyberSecurity for Nodes 或 Kaspersky Endpoint Security for Windows 後安裝 Kaspersky Embedded Systems Security，則必須重新啟動電腦。

在開始安裝 Kaspersky Embedded Systems Security 前，請計劃安裝的主要階段。

1. 確定管理和設定 Kaspersky Embedded Systems Security 所使用的管理工具。
2. 選擇 選擇安裝所需的應用程式元件。
3. 選擇安裝方式。

選擇管理工具

確定將用於配置 Kaspersky Embedded Systems Security 設定和管理該應用程式的管理工具。可以使用應用程式主控台、命令列實用工具和卡巴斯基安全管理中心管理主控台管理 Kaspersky Embedded Systems Security。

Kaspersky Embedded Systems Security 主控台

Kaspersky Embedded Systems Security 主控台是新增到 Microsoft 管理主控台的獨立管理元件。您可以透過安裝在受防護裝置或公司網路中其他裝置上的應用程式主控台來管理 Kaspersky Embedded Systems Security。

您可以將多個 Kaspersky Embedded Systems Security 管理元件新增到在作者模式中開啟單獨的 Microsoft 管理主控台中，以便用它來管理多台已安裝 Kaspersky Embedded Systems Security 的裝置的防護。

命令列實用工具

您可以從受防護裝置的命令列管理 Kaspersky Embedded Systems Security。

命令列公用程式包含在 Kaspersky Embedded Systems Security 軟體元件群組中。

卡巴斯基安全管理中心

若您為了集中管理公司裝置的病毒防護工作而使用卡巴斯基安全管理中心，您可使用卡巴斯基安全管理中心的管理主控台來管理 Kaspersky Embedded Systems Security。

必須安裝下列元件：

- **整合卡巴斯基安全管理中心網路代理模組**。此元件包含在 Kaspersky Embedded Systems Security 軟體元件群組中。它允許 Kaspersky Embedded Systems Security 與網路代理通信。請在受防護裝置上安裝與卡巴斯基安全管理中心網路代理程式整合的模組。

- **卡巴斯基安全管理中心網路代理**。請在每一台受防護裝置上安裝此元件。該元件支援受防護裝置上安裝的 Kaspersky Embedded Systems Security 與卡巴斯基安全管理中心管理主控台之間的互動。網路代理程式安裝檔案包含在卡巴斯基安全管理中心的分發套件資料夾中。

- **Kaspersky Embedded Systems Security 管理外掛程式**。此外，安裝該外掛程式，以在安裝了卡巴斯基安全管理中心管理伺服器的受防護裝置上透過管理主控台管理 Kaspersky Embedded Systems Security。此外掛程式提供了透過卡巴斯基安全管理中心進行應用程式管理的介面。管理外掛程式安裝檔案 \exec\klcfginst.exe 包含在 Kaspersky Embedded Systems Security 分發套件中。

選擇安裝類型

指定 用於安裝 Kaspersky Embedded Systems Security 的軟體元件後，您需要選擇應用程式安裝方法。

根據網路架構並參考下列情況選擇安裝方法：

- 是需要特殊的 Kaspersky Embedded Systems Security 安裝設定，還是建議的安裝設定。

- 所有受防護裝置是否採用相同的安裝設定或個別為每台受防護裝置使用不同的設定。

使用者可使用背景模式在命令列指定適當的安裝設定，或利用互動式安裝精靈安裝 Kaspersky Embedded Systems Security。您可使用 Active Directory 群組政策或卡巴斯基安全管理中心遠端安裝工作，以遠端方式統一安裝Kaspersky Embedded Systems Security。

Kaspersky Embedded Systems Security 可以在單台受防護裝置上安裝和配置，其設定儲存到一個設定檔中；該檔案隨後可用於在其他受防護裝置上安裝 Kaspersky Embedded Systems Security。請注意，當使用 Active Directory 群組政策安裝應用程式時，此功能不存在。

啟動安裝精靈

您可使用安裝精靈安裝下列內容：

- 受防護裝置上的 Kaspersky Embedded Systems Security 元件，按一下歡迎應用程式中的連結後，可以開啟 setupui.exe或直接使用分發套件中的\exec\setup_ess.exe檔案，以啟動該應用程式。

- 受防護裝置或 LAN 的其他裝置上的 Kaspersky Embedded Systems Security 主控台，按一下歡迎應用程式中的連結後，可以開啟 setupui.exe 或直接使用分發套件中的 \console\setup_esstools.exe 檔案，以啟動該應用程式。

透過命令列使用必要的安裝設定來啟動安裝套件檔案

如果不以任何命令列選項啟動安裝套件檔案，則 Kaspersky Embedded Systems Security 將以預設設定安裝。可以使用 Kaspersky Embedded Systems Security 選項修改安裝設定。

應用程式主控台可以安裝在受防護裝置和/或管理員工作站上。

您還可以使用示例指令安裝 Kaspersky Embedded Systems Security 和應用程式主控台。

透過卡巴斯基安全管理中心集中安裝

如果卡巴斯基安全管理中心在您的網路中的用途是管理網路裝置的病毒防護，則可以使用遠端安裝工作在多台裝置上安裝 Kaspersky Embedded Systems Security。

您希望在上面使用卡巴斯基安全管理中心安裝 Kaspersky Embedded Systems Security 的受防護裝置可以與卡巴斯基安全管理中心位於同一網域中，也可以在不同的網域中，或完全不屬於任何一個網域。

使用 Active Directory 群組政策集中安裝

您可使用 Active Directory 群組政策在受防護裝置上安裝 Kaspersky Embedded Systems Security。應用程式主控台可以安裝在受防護裝置或管理員工作站上。

可以僅使用建議的安裝設定安裝 Kaspersky Embedded Systems Security。

使用 Active Directory 群組政策安裝 Kaspersky Embedded Systems Security 的受防護裝置必須位於相同網域或相同的組織單元中。安裝作業會在受防護裝置啟動，登入 Microsoft Windows 之前執行。

基於精靈安裝和移除應用程式

本節介紹透過安裝精靈安裝和移除 Kaspersky Embedded Systems Security 和應用程式主控台，並包含有關 Kaspersky Embedded Systems Security 的附加配置以及要在安裝後執行的操作的資訊。

使用安裝精靈安裝

以下各節包含有關安裝 Kaspersky Embedded Systems Security 和應用程式主控台的資訊。

要安裝和繼續使用 Kaspersky Embedded Systems Security：

1. 在受防護裝置上安裝 Kaspersky Embedded Systems Security。
2. 在您打算用來管理 Kaspersky Embedded Systems Security 的裝置上安裝應用程式主控台。

3. 如果應用程式主控台不是安裝在受防護裝置上，而是安裝在網路中的其他裝置上，請執行其他設定，讓應用程式主控台使用者能夠遠端管理 Kaspersky Embedded Systems Security。

4. 安裝 Kaspersky Embedded Systems Security 後執行操作。

Kaspersky Embedded Systems Security 安裝

在安裝 Kaspersky Embedded Systems Security 之前，請執行以下操作：

1. 確認受防護裝置上未安裝任何病毒防護應用程式。您必須刪除 Kaspersky Anti-Virus 8.0 for Windows Servers Enterprise Edition。您無需刪除 Kaspersky Security 10 for Windows Server 即可安裝 Kaspersky Embedded Systems Security。

2. 確認用來執行安裝精靈的帳戶屬於受防護裝置上的管理員群組。

Kaspersky Embedded Systems Security 包含以下預先定義的組態：

使用預設拒絕技術保護電腦

可啟用更新的元件不包含在 **使用預設拒絕技術防護電腦** 配置中。

如果選擇 **使用預設拒絕技術防護電腦** 配置，則預設包含以下元件：

- 弱點利用防禦
- 應用程式啟動控制
- 系統托盤圖示

在使用特徵分析和病毒資料庫來防護電腦的應用程式版本上安裝**使用預設拒絕技術防護電腦**設定時，將刪除以下元件來自動縮減應用程式元件集：

- 即時檔案防護
- 按需掃描
- 啟用更新的元件

建議使用此配置來防護資源有限的裝置。在此情況下，您可以長期啟動應用程式，而應用程式啟動控制元件會為電腦提供防護。

使用防毒資料庫保護電腦

如果選擇**使用病毒資料庫防護電腦**設定，則預設包括除「防火牆管理」和「效能計數器」元件之外的所有 Kaspersky Embedded Systems Security 元件。

在不使用特徵分析和病毒資料庫來防護電腦的應用程式版本上安裝**使用病毒資料庫防護電腦**設定時，將新增以下元件來自動延伸應用程式元件集：

- 即時檔案防護
- 按需掃描
- 網路威脅防護

您可以閱讀有關安裝（移除）設定的詳細資訊。

使用安裝精靈安裝 Kaspersky Embedded Systems Security：

1. 在受防護裝置上執行 setupui.exe 檔案。
2. 在開啟的視窗中，前往 **安裝** 區段，然後點擊 **使用預設拒絕技術防護電腦** 連結或 **使用病毒資料庫防護電腦** 連結。
3. 在 Kaspersky Embedded Systems Security 安裝精靈的歡迎頁面，點擊“**下一步 >**”按鈕。

   開啟“**最終使用者產品授權協議**”視窗。
4. 檢視產品授權協議和隱私政策的條款。
5. 如果您同意最終使用者產品授權協議和隱私權政策的條款和條件，請選擇 **我確認我已完全閱讀、理解並接受這些最終使用者產品授權協議的條款和條件** 和 **我瞭解並同意按照隱私權政策所述來處理和傳輸我的資料(包括傳輸到協力廠商國家/地區)。我確認我已完全閱讀並理解隱私權政策** 核取方塊。

   如果您不接受最終使用者產品授權協議和/或隱私政策，安裝將中止。
6. 單擊“**下一步 >**”。

   開啟“**自訂安裝**”視窗。

   請選擇您想安裝的元件。

   只有在受防護裝置安裝了 Microsoft Windows SNMP 服務的情況下，建議的安裝元件清單中才會出現 Kaspersky Embedded Systems Security 的 “SNMP 協定支援”元件。
7. 要取消所有變更，請在“**自訂安裝**”視窗中點擊“**重設**”按鈕。單擊“**下一步 >**”。
8. 在“**選擇目標資料夾**”視窗中執行下列操作之一：
   - 如果需要，指定 Kaspersky Embedded Systems Security 檔案將複製到的資料夾。
   - 如果需要，點擊“**磁碟**”按鈕檢視有關本地磁碟機上可用空間的資訊。

   單擊“**下一步 >**”。
9. 在 **配置** 視窗中，您可以從防護範圍中排除物件和資料夾並配置即時檔案防護。

10. 如果您要從在應用程式早期版本中建立的現有設定檔匯入 Kaspersky Embedded Systems Security 設定，請在**從設定檔匯入設定**視窗中指定設定檔的路徑。

11. 在"**啟動應用程式**"視窗中執行以下操作之一：

    - 如果您想要啟動應用程式，請指定 Kaspersky Embedded Systems Security 金鑰檔案以啟動應用程式。
    - 如果您想要稍後啟動應用程式，請點擊"**下一步 >**"按鈕。
    - 如果金鑰檔案之前已儲存在分發套件的 \exec 資料夾中，該檔案的名稱將顯示在**金鑰**欄位中。
    - 若要使用儲存在其他資料夾的金鑰檔案新增金鑰，請指定金鑰檔案。

    安裝精靈不允許使用啟動碼啟動應用程式。如果您想使用啟動碼來啟動應用程式，可以在安裝應用程式後指定啟動碼。

    新增金鑰檔案後，視窗中將顯示產品授權資訊。Kaspersky Embedded Systems Security 會顯示計算出的產品授權到期日期。產品授權期限從您新增金鑰開始計算，並於金鑰檔案的有效期間到期前結束。

    點擊**下一步 >** 將金鑰檔案新增至應用程式。

12. 必要的話，在**遠端存取設定**部分中變更應用程式主控台用來遠端連線到安裝了應用程式的電腦的連接埠號。

    使用 Windows 憑據進行連線的預設連接埠號為 13032，使用手動建立的使用者的憑據進行連線的預設連接埠號為 13031。可能的連接埠號範圍：1–65535。

    為了防止使用手動建立的使用者帳戶的憑據進行連線，請清除 **使用手動建立的使用者的憑證**核取方塊。

13. 如有需要，在 **準備安裝** 視窗中，您可以停用 **防護安裝處理程序** 選項。安裝防護包括防止分發套件被更換為惡意應用程式、封鎖對 Kaspersky Embedded Systems Security 安裝資料夾的存取，以及封鎖對包含應用程式金鑰的系統登錄檔部分的存取。但是，如果無法安裝應用程式（例如，藉助 Windows Remote Desktop 執行遠端安裝），我們建議您停用安裝過程的防護。

14. 如有需要，將 kavshell.exe 檔案路徑新增到 %PATH% 系統變數中，以方便使用命令列介面。

15. 單擊"**安裝**"。

16. 完成安裝時，會開啟"**安裝完成。**"視窗。

17. 點擊"**完成**"按鈕。

安裝精靈關閉。完成安裝後，如果已新增啟動金鑰，即可使用 Kaspersky Embedded Systems Security。

Kaspersky Embedded Systems Security 主控台安裝

依照安裝精靈說明配置應用程式主控台的安裝設定。您可於安裝精靈的任何一個步驟停止安裝程序。若要停止安裝，請在安裝精靈視窗中點擊"**取消**"按鈕。

要安裝應用程式主控台：

1. 確認用來執行安裝精靈的帳戶屬於裝置上的管理員群組。

2. 在受防護裝置上執行 setupui.exe 檔案。

   隨即會開啟一個歡迎安裝程式視窗。

3. 點擊"**安裝 Kaspersky Embedded Systems Security for Windows 主控台**"連接。

   隨即會開啟"安裝精靈"歡迎視窗。單擊"**下一步 >**"。

4. 如果您同意最終使用者產品授權協議和隱私權政策的條款和條件，請選擇 **我確認我已完全閱讀、理解並接受這些最終使用者產品授權協議的條款和條件** 和 **我瞭解並同意按照隱私權政策所述來處理和傳輸我的資料(包括傳輸到協力廠商國家/地區)。我確認我已完全閱讀並理解隱私權政策** 核取方塊。單擊"**下一步 >**"。

5. 在 **選擇目標資料夾** 視窗中指定要儲存正在安裝的檔案的資料夾。

6. 單擊"**下一步 >**"。

7. 在**準備安裝**視窗中，按一下**安裝**按鈕。

   該精靈將開始安裝所選的元件。

8. 單擊"**完成**"。

安裝精靈關閉。將在受防護裝置上安裝應用程式主控台。

如果管理工具已安裝在網路中除了受防護裝置以外的任何裝置上，請配置進階設定。

在其他裝置上安裝應用程式主控台以後的進階設定

如果應用程式主控台已經安裝在網路中的其他裝置上，而不是安裝在受防護裝置上，請執行以下操作，以允許使用者遠端管理 Kaspersky Embedded Systems Security：

- 在應用程式設定中使用具有遠端連線權限的使用者帳戶。預設情況下，管理員群組和 ESS 管理員群組中的所有使用者都擁有此權限。

- 在遠端裝置的 Windows 防火牆設定中，開啟 TCP 13032 連接埠以供 Windows 系統使用者帳戶連線，並開啟 TCP 13031 連接埠以供在應用程式設定中手動建立的使用者帳戶連線。另外，也要允許 Kaspersky Embedded Systems Security 遠端管理進程的可執行檔 avp.exe 進行網路連線。在命令列上安裝該應用程式時，您可以使用 `ADDWFEXCLUSION=1` 選項管理此設定。

如果您需要遠端執行 Kaspersky Embedded Systems Security，請另外執行以下操作：

遠端啟動應用程式的使用者帳戶必須是管理員群組的成員。

- 在遠端裝置上的 Windows 防火牆設定中，啟用**檔案和印表機共用 (SMB-In)** 規則（連接埠 TCP 445）。同時建議開啟 TCP 135 連接埠以方便與裝置連線。

- 對於執行 Windows Vista 或更高版本且不屬於某個網域或不是由本機使用者帳戶管理的遠端裝置，**停用使用者帳戶 (UAC) 的遠端控制。**

  1. 在電腦上開啟登錄檔編輯器。

  2. 在登錄檔編輯器中，開啟 HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System 金鑰。

3. 開啟 LocalAccountTokenFilterPolicy 值。

   如果此金鑰下缺少 LocalAccountTokenFilterPolicy 值，請使用此名稱建立 DWORD（32 位元）值（有關詳細信息，請參閱 Microsoft 技術支援網站）。

4. 將其設定為 **1** 並點擊**確定**。

   停用遠端 UAC 不會影響本機 UAC。

- 如果安裝了應用程式主控台的裝置或受防護的裝置執行的是 Windows 8.1 或更早版本的 Windows，**在執行 Windows 10 或更高版本的裝置上啟用對 SMB 1.0/CIFS 檔案的共用存取支援。**
  - 在「Windows 功能」應用程式中：
    1. 選取**開始 → 控制面板 → 程式和功能 → 開啟或關閉 Windows 功能**。
    2. 在「**Windows 功能**」視窗中，選取「**SMB 1.0/CIFS 檔案共用支援**」核取方塊。
    3. 點擊**OK**。
  - 在 Windows PowerShell 中：
    1. 以管理員身分執行 Windows PowerShell。
    2. 執行以下指令：

```
Enable-WindowsOptionalFeature -Online -FeatureName SMB1Protocol
```

設定任何其他軟體或硬體防火牆應該套用相同步驟。

如果在配置受防護裝置與安裝了應用程式主控台的裝置之間的連線時，應用程式主控台處於開啟狀態：

1. 關閉應用程式主控台。
2. 等待至 Kaspersky Embedded Systems Security 遠端管理處理程序 avp.exe 結束。
3. 重新啟動應用程式主控台。

將套用新的連線設定。

允許匿名遠端存取 COM 應用程式

設定的名稱可能有所不同，具體取決於安裝的 Windows 作業系統。

要允許匿名遠端存取 COM 應用程式：

1. 在安裝了 Kaspersky Embedded Systems Security 主控台的遠端裝置上，開啟**元件服務**主控台。為此：
   a. 選取**開始 → 執行**。
   b. 執行以下指令：

   ```
   dcomcnfg
   ```

   c. **元件服務** 主控台將開啟。
2. 在受防護裝置上的「**元件服務**」主控台中，展開「**電腦**」節點。
3. 開啟"**我的電腦**"節點的內容功能表。
4. 選擇"**內容**"。
5. 在屬性視窗的 **COM 安全性**標籤上，點擊**存取權限**設定群組中的**編輯限制**按鈕。
6. 請確認在「**允許遠端存取**」視窗中，已為「匿名登入」使用者選取「**允許遠端存取**」核取方塊。
7. 點擊**OK**。

允許 Kaspersky Embedded Systems Security 遠端管理處理程序的網路連線

設定的名稱可能有所不同，具體取決於安裝的 Windows 作業系統。

要在 Windows 防火牆中開放 TCP 連接埠 135 並允許 Kaspersky Embedded Systems Security 遠端管理處理程序的網路連線：

1. 關閉遠端裝置上的 Kaspersky Embedded Systems Security 主控台。
2. 執行以下操作之一：
   - 在 Microsoft Windows XP SP2 或更高版本中：
     a. 選取「**開始**」→「**Windows 防火牆**」。
     b. 在"**Windows 防火牆**"視窗（或"Windows 防火牆設定"）中點擊"**排除**"選項上的"**新增連接埠**"按鈕。
     c. 在"**名稱**"欄位中指定連接埠名稱 RPC (TCP/135) 或輸入其他名稱，例如"Kaspersky Embedded Systems Security DCOM"，並在"**連接埠名稱**"欄位中指定埠號 (135)。
     d. 選擇"**TCP**"協定。
     e. 點擊**OK**。
     f. 點擊"**排除**"標籤上的"**新增**"按鈕。

- 在 Microsoft Windows 7 或更高版本中：

  a. 選取「**開始**」→「**主控台**」>「**Windows 防火牆**」。

  b. 在"**Windows 防火牆**"視窗中，選擇"**允許程式或功能透過 Windows 防火牆**"。

  c. 在"**允許程式透過 Windows 防火牆通訊**"視窗中點擊"**允許其他程式**"按鈕。

3. 在"**新增應用程式**"視窗中指定 kavfsrcn.exe 檔案。在使用 Microsoft 管理主控台安裝 Kaspersky Embedded Systems Security 主控台的過程中，該檔案位於指定的目的資料夾中。

4. 點擊**OK**。

5. 在「**Windows 防火牆（Windows 防火牆設定）**」視窗中，點擊「**確定**」按鈕。

在安裝 Kaspersky Embedded Systems Security 後執行的操作

如果您已啟動 Kaspersky Embedded Systems Security，該應用程式在安裝後立即啟動防護和掃描工作。如果在安裝 Kaspersky Embedded Systems Security 期間選取 **安裝應用程式後啟用即時檔案防護（建議）** 核取方塊，應用程式會在存取裝置的檔案系統物件時進行掃描。如果指令碼監控元件是作為自訂安裝的一部分安裝的，則 Kaspersky Embedded Systems Security 會在啟動指令碼時掃描所有指令碼的原始程式碼。Kaspersky Embedded Systems Security 將在每週五晚上 8:00 執行*關鍵區域掃描*工作。

建議在安裝 Kaspersky Embedded Systems Security 後執行下列步驟：

- 啟動應用程式資料庫更新工作。安裝後 Kaspersky Embedded Systems Security 將使用應用程式發行套件中的資料庫掃描物件。

  > 我們建議立即更新 Kaspersky Embedded Systems Security 資料庫，因為它們可能已過期。

  之後，應用程式將根據預設排程每小時更新一次資料庫。

- 如果安裝 Kaspersky Embedded Systems Security 之前受防護伺服器上未安裝任何具有即時檔案防護的病毒防護軟體，請對裝置執行"關鍵區域掃描"。

- 配置有關 Kaspersky Embedded Systems Security 事件的管理員通知。

啟動並配置資料庫和應用程式模組更新工作

要在安裝後更新應用程式資料庫：

1. 在*更新*下面，配置更新來源連線。

2. 執行"*更新*"工作。

> 您的網路中可能未設定 Web Proxy Auto-Discovery Protocol (WPAD)，無法在 LAN 中自動偵測代理伺服器設定。而且，在存取代理伺服器時，您的網路可能需要身分驗證。

要為存取代理伺服器指定可選的代理伺服器設定和身分驗證設定：

1. 在應用程式主控台中，開啟"**Kaspersky Embedded Systems Security**"節點的內容功能表。
2. 選擇"**應用程式內容**"。
3. 這會開啟一個視窗；在該視窗中，選擇**網路設定**頁簽。
4. 在**代理伺服器設定**部分中，點擊 **設定** 並在顯示的視窗中選擇 **使用指定的代理伺服器設定** 核取方塊。
5. 在**位址**欄位中輸入代理伺服器位址，在**連接埠**欄位中輸入代理伺服器的埠號。
6. 如有必要，清除"**本機位址略過代理伺服器**"核取方塊。如果啟用此功能，則會直接透過託管已安裝了 Kaspersky Embedded Systems Security 的受防護裝置的網路存取裝置。預設啟用該選項。
7. 在"**代理伺服器身分驗證設定**"部分的下拉式清單中選擇必要的身分驗證方法：
   - **不使用身分驗證**
   - **NTLM 身分驗證**使用目前使用者帳戶進行 NTLM 身分驗證（預設）。
   - **使用使用者名稱和密碼進行 NTLM 身分驗證**使用手動指定的憑據進行 NTLM 身分驗證。
   - **Kerberos 身分驗證**使用目前使用者帳戶進行 Kerberos 身分驗證。

     若要確保在使用 CNAME 記錄作為代理伺服器位址時 Kerberos 身分驗證正常運作，您必須為每個 CNAME 記錄註冊一個服務主體名稱 (SPN)。

   - **使用使用者名稱和密碼進行 Kerberos 身分驗證**使用手動指定的憑據進行 Kerberos 身分驗證。
   - **使用者名稱和密碼**使用手動指定的憑據進行身分驗證。

   需要時，輸入使用者名稱和密碼。

   如果選擇 Kerberos 驗證，Kaspersky Embedded Systems Security 可以根據代理伺服器設定使用 Kerberos 或 NTLM 協定執行身分驗證。
8. 點擊**OK**。

要執行"更新"工作：

1. 在應用程式主控台樹狀目錄中，展開"**更新**"節點。
2. 在**資料庫更新**子節點的內容功能表中，選取"**啟動**"項目。

更新 工作開始。

工作成功完成後，您可以在 **Kaspersky Embedded Systems Security** 節點的結果視窗中檢視安裝的最新資料庫更新的發佈日期。

關鍵區域掃描

更新 Kaspersky Embedded Systems Security 資料庫後，使用「*關鍵區域掃描*」工作掃描受防護裝置是否有惡意軟體。

要執行"關鍵區域掃描"工作：

1. 在應用程式主控台樹狀目錄中，展開"**按需掃描**"節點。
2. 在**關鍵區域掃描**子節點的內容功能表中，選取"**啟動**"命令。

工作啟動；結果窗格中顯示工作狀態"**正在執行**"。

要檢視工作記錄，請執行下列操作：

在**關鍵區域掃描** 節點的結果窗格中，點擊**開啟工作記錄**連結。

修改元件集和修復 Kaspersky Embedded Systems Security

可以新增或移除 Kaspersky Embedded Systems Security 元件。在移除即時檔案防護元件之前，您需要停止即時檔案防護工作。在其他情況下，不需要停止 即時檔案防護 工作或 Kaspersky Embedded Systems Security 服務。

如果應用程式管理受密碼防護，Kaspersky Embedded Systems Security 會在您在安裝精靈中嘗試移除元件或修改元件集時請求密碼。

要修改 Kaspersky Embedded Systems Security 元件集：

1. 在 Windows 的**控制面板**中，選擇 **應用程式和功能**。"**修改或移除**"視窗將開啟。
2. 右鍵點擊 **Kaspersky Embedded Systems Security** 並選擇 **編輯**。
   這將開啟設定精靈 **修改、修復或移除應用程式**。
3. 選擇"**修改**"。
   開啟"**自訂安裝**"視窗。選擇 **完整功能** 然後點擊 **下一步(N) >**。
4. 在"**自訂安裝**"視窗的可用元件清單中，選擇要從 Kaspersky Embedded Systems Security 新增或移除的元件。為此，請執行以下操作：
   - 要變更元件集，請點擊所選元件名稱旁邊的按鈕。然後在右鍵選單中選取：
     - **該功能將被安裝到本機硬碟磁碟機上。**，如果您想安裝一個元件；
     - **安裝所有功能及其子功能至本機硬碟磁碟機。**，如果要安裝該組元件；
   - 要移除先前安裝的元件，請點擊所選元件名稱旁邊的按鈕。在內容功能表中，選取"**功能將不可用。**"。

   單擊"**下一步(N) >**"。

5. 在 **準備安裝** 視窗中，點擊**安裝**確認應用程式元件的選擇。

6. 在安裝完成後開啟的視窗中，點擊**"完成"**按鈕。

將根據指定設定修改 Kaspersky Embedded Systems Security 元件集。

如果 Kaspersky Embedded Systems Security 於運作時發生問題（Kaspersky Embedded Systems Security 當機；工作損毀或無法啟動），您可為 Kaspersky Embedded Systems Security 執行修復。您可在儲存 Kaspersky Embedded Systems Security 的目前設定時執行修復，或選擇一個選項以將所有 Kaspersky Embedded Systems Security 設定重設為預設值。

要在應用程式或工作崩潰後修復 Kaspersky Embedded Systems Security：

1. 在 Windows 的**控制面板**中，選擇 **應用程式和功能**。**"修改或移除"**視窗將開啟。

2. 右鍵點擊 **Kaspersky Embedded Systems Security** 並選擇 **編輯**。

3. 這將開啟設定精靈 **修改、修復或移除應用程式**。

4. 請選擇**修復**選項。

開啟**"修復 Kaspersky Embedded Systems Security"**視窗。單擊**"下一步(N) >"**。

5. 等待還原操作完成，然後在開啟的視窗中點擊**完成**。

將使用指定設定修復 Kaspersky Embedded Systems Security。

使用安裝精靈移除

本節包含有關使用安裝/移除精靈從受防護裝置上移除 Kaspersky Embedded Systems Security 和應用程式主控台的說明。

Kaspersky Embedded Systems Security 移除

移除 Kaspersky Embedded Systems Security 時不會刪除 Dump 和偵錯檔案。您可以手動刪除在配置 Dump 和偵錯檔案寫入期間指定的資料夾中的 Dump 和偵錯檔案。

設定的名稱可能有所不同，具體取決於安裝的 Windows 作業系統。

可以使用安裝/移除精靈從受防護裝置移除 Kaspersky Embedded Systems Security。

從受防護裝置解除安裝 Kaspersky Embedded Systems Security 後，可能需要重新啟動裝置。重新啟動可以推遲。

該應用程式無法透過 Windows 控制面板進行解除安裝、修復和安裝。

當使用者嘗試在安裝精靈中移除或修改元件集時，Kaspersky Embedded Systems Security 提示使用者輸入帳戶憑據。您需要輸入具有足夠權限的使用者的憑據。如果為執行刪除操作的使用者帳戶設定了空的 Windows 密碼，請在開始刪除之前停用**請求密碼以確認關鍵操作**功能。

要移除 Kaspersky Embedded Systems Security：

1. 在 Windows 的**控制面板**中，選擇 **應用程式和功能**。"**修改或移除**"視窗將開啟。
2. 右鍵點擊 **Kaspersky Embedded Systems Security** 並選擇 **編輯**。
3. 這將開啟設定精靈 **修改、修復或移除應用程式**。
4. 選擇"**移除**"。
   開啟"**儲存物件**"視窗。
5. 如有需要，在"**儲存物件**"視窗中執行下列操作：
   在 **儲存物件** 下面，指定要保留的物件或設定。預設情況下，會取消勾選核取方塊。
   - 選擇"**啟動資料**"核取方塊。
   - 選擇"**備份檔案**"核取方塊。
   - 選擇"**程式的操作設定**"核取方塊。

   在 **匯出物件** 下面，指定要匯出的物件。預設情況下，會取消勾選核取方塊。
   - 選中"**匯出隔離物件**"核取方塊，以從 Kaspersky Embedded Systems Security 隔離區匯出物件。預設情況下，會取消勾選核取方塊。
   - 選取**匯出備份物件**核取方塊，以從 Kaspersky Embedded Systems Security 備份區匯出物件。預設情況下，會取消勾選核取方塊。
   - 點擊"**儲存**"按鈕並選擇您希望將物件匯出到的資料夾。預設情況下，物件將會匯出到 %ProgramData%\Kaspersky Lab\KESS.4.1\QB。
     單擊"**下一步**"。
6. 在 **準備移除** 視窗中，點擊 **移除** 確認刪除。
7. 在移除完成後開啟的視窗中，點擊"**完成**"按鈕。

Kaspersky Embedded Systems Security 將從受防護裝置移除。

Kaspersky Embedded Systems Security 主控台移除

設定的名稱可能有所不同，具體取決於安裝的 Windows 作業系統。

您可以使用安裝/移除精靈，從受防護裝置移除應用程式主控台。

移除應用程式主控台後，無需重新啟動受防護裝置。

要移除應用程式主控台，請執行下列步驟：

1. 在 Windows 的**控制面板**中，選擇 **應用程式和功能**。**"修改或移除"**視窗將開啟。
2. 右鍵點擊 **Kaspersky Embedded Systems Security 主控台** 並選擇 **編輯**。
   這將開啟 **修改、修復或移除應用程式** 精靈的視窗。
3. 選擇**"移除"**。
   開啟**"準備移除"**視窗。單擊**"解除安裝"**。
4. 在移除完成後開啟的視窗中，點擊**"確定"**按鈕。

此時，移除完成，且安裝精靈關閉。

透過命令列安裝或移除應用程式

本章節介紹從命令列安裝和移除 Kaspersky Embedded Systems Security 的詳細資訊，包含從命令列安裝和移除 Kaspersky Embedded Systems Security 的指令範例，以及從命令列新增和移除 Kaspersky Embedded Systems Security 元件的指令範例。

關於從命令列安裝和移除 Kaspersky Embedded Systems Security

移除 Kaspersky Embedded Systems Security 時不會刪除 Dump 和偵錯檔案。您可以手動刪除在配置 Dump 和偵錯檔案寫入期間指定的資料夾中的 Dump 和偵錯檔案。

在使用命令列選項指定安裝設定後，您可以從命令列執行 \exec\ess_win.msi 安裝套件檔案，以安裝或解除安裝 Kaspersky Embedded Systems Security 並新增或移除其元件。

Kaspersky Embedded Systems Security Console 可以安裝在受防護裝置或網路的另一台裝置上，以本機或遠端方式和應用程式搭配使用。若要安裝，請使用 \client\esstools.msi 安裝套件。

在安裝了該應用程式的受防護裝置上，使用包含在管理員群組中的帳戶執行安裝。

如果在沒有其他命令列選項的受防護裝置上執行 \exec\ess_win.msi 檔案，將使用預設安裝設定安裝 Kaspersky Embedded Systems Security。

您可以使用 ADDLOCAL 命令列選項和列出所選的元件或元件集的代碼，來指派要安裝的元件集。

適用於 Windows Installer 服務的 Kaspersky Embedded Systems Security 軟體元件程式碼

\product_long_term\ess_win.msi檔案旨在安裝 Kaspersky Embedded Systems Security 的"**使用預設拒絕技術防護電腦**"配置，\exec\ess_win.msi檔案旨在安裝 Kaspersky Embedded Systems Security 的"**使用病毒資料庫防護電腦**"配置。

如果選擇**使用病毒資料庫防護電腦**設定，則預設包括除「防火牆管理」和「效能計數器」元件之外的所有 Kaspersky Embedded Systems Security 元件。

在不使用特徵分析和病毒資料庫來防護電腦的應用程式版本上安裝**使用病毒資料庫防護電腦**設定時，將新增以下元件來自動延伸應用程式元件集：

- 即時檔案防護
- 按需掃描
- 網路威脅防護

可啟用更新的元件不包含在 **使用預設拒絕技術防護電腦** 配置中。

如果選擇 **使用預設拒絕技術防護電腦** 配置，則預設包含以下元件：

- 弱點利用防禦
- 應用程式啟動控制
- 系統托盤圖示

在使用特徵分析和病毒資料庫來防護電腦的應用程式版本上安裝**使用預設拒絕技術防護電腦**設定時，將刪除以下元件來自動縮減應用程式元件集：

- 即時檔案防護
- 按需掃描
- 啟用更新的元件

建議使用此配置來防護資源有限的裝置。在此情況下，您可以長期啟動應用程式，而應用程式啟動控制元件會為電腦提供防護。

\console\esstools.msi檔案用於安裝 Kaspersky Embedded Systems Security 主控台。

下表含有 Kaspersky Embedded Systems Security 軟體元件的代碼和說明。

元件	代碼	元件功能
即時檔案防護	`FileThreatProtection`	此元件在受防護裝置上的檔案被存取時對這些檔案執行病毒掃描。
AMSI 掃描器	`AMSI`	此元件旨在支援 Microsoft 的惡意軟體防護掃描介面。惡意軟體防護掃描介面 (AMSI) 允許具有 AMSI 支援的協力廠商應用程式將物件（例如，PowerShell 指令碼）傳送到 Kaspersky Embedded Systems Security 進行附加掃描，然後接收這些物件的掃描結果。
行為偵測	`BehaviorDetection`	此元件使用顯示惡意活動的遠端裝置的名稱填充被封鎖的主機清單。
弱點利用防禦	`ExploitPrevention`	此元件可管理設定，以便防護裝置記憶體中的處理程序所使用的記憶體。
修復引擎	`RemediationEngine`	此元件允許 Kaspersky Embedded Systems Security 回溯惡意軟體在作業系統中執行的操作。
Firewall	`Firewall`	此元件可透過 Kaspersky Embedded Systems Security 圖形化使用者介面來管理 Windows 防火牆。
網路威脅防護	`NetworkThreatProtection`	此元件會掃描傳入的網路流量中是否存在典型網路攻擊活動。在偵測到以您的電腦為目標的網路攻擊企圖時，Kaspersky Embedded Systems Security 將封鎖攻擊電腦的網路活動。
應用程式啟動控制	`ApplicationControl`	此元件監控使用者啟動應用程式的嘗試，並根據指定的應用程式啟動控制規則來允許或拒絕這些應用程式啟動。
裝置控制	`DeviceControl`	此元件會偵錯將外部裝置連線到受防護裝置的嘗試，並根據指定的裝置控制規則來允許或拒絕這些裝置的使用。
整合卡巴斯基安全管理中心網路代理模組	`AdminKitConnector`	提供 Kaspersky Embedded Systems Security 與卡巴斯基安全管理中心網路代理之間的連線。 如果想透過卡巴斯基安全管理中心管理應用程式，請在受防護裝置上安裝此元件。
記錄審查	`LogInspector`	此元件根據 Windows 事件記錄的審查結果，對受防護環境的完整性進行監控。
系統完整性監控	`SystemIntegrityMonitor`	此元件包括檔案完整性監控的所有功能，此外還允許監控登錄機碼變更和外部裝置的連線。
BadUSB 攻擊防護	`BadUSBAttackPrevention`	該元件可以防止受感染的模擬鍵盤的 USB 裝置連線至電腦。
Managed Detection and Response	`MDR`	該元件有助於與 Kaspersky Managed Detection and Response 解決方案進行交互。

安裝和復原設定以及 Windows 安裝程式命令列選項

本節介紹 Kaspersky Embedded Systems Security 的安裝與復原設定。該部分也包含用於變更安裝設定的參數和可能的參數值。透過命令列安裝 Kaspersky Embedded Systems Security 時，您可以使用參數及 Windows Installer 服務中 `msiexec` 指令適用的標準指令。

安裝設定以及 Windows 安裝程式命令列選項

- 接受最終使用者產品授權協議條款。

  `EULA=<value>` 可以使用的值如下。

  - `0` - 拒絕最終使用者產品授權協議條款（預設值）。
  - `1` - 接受最終使用者產品授權協議條款。

- 接受隱私權政策的條款。

PRIVACYPOLICY=<value> 可以使用的值如下。

- 0 – 拒絕隱私政策條款（預設值）。
- 1 – 接受隱私政策條款。

- 安裝過程中將儲存在 Kaspersky Embedded Systems Security 檔案的目標資料夾。您可指定不同的資料夾。

  INSTALLDIR=<full path to the folder> 命令列選項的預設值如下：

  - 對於 32 位元版本的 Microsoft Windows：
    - Kaspersky Embedded Systems Security: %ProgramFiles%\Kaspersky Lab\Kaspersky Embedded Systems Security.4.1.0
    - Kaspersky Embedded Systems Security Console: %ProgramFiles%\Kaspersky Lab\Kaspersky Embedded Systems Security Console 4.1.0
  - 對於 64 位元版本的 Microsoft Windows：與 32 位元版本的 Microsoft Windows 的路徑類似的 %ProgramFiles(x86)% 等。

- Kaspersky Embedded Systems Security 啟動後立即啟動 *即時檔案防護*工作。

  RUNRTP=<value> 可以使用的值如下。

  - 1 – 啟動（預設值）。
  - 0 – 不啟動。

- 金鑰檔案的路徑 (LICENSEKEYPATH)。預設情況下，Windows Installer 會嘗試在分發套件的 \exec 資料夾中尋找副檔名為 .key 的檔案。如果 \exec 資料夾包含數個金鑰檔案，Windows Installer 將選擇到期日期最晚的金鑰檔案。參數檔案可以預先儲存在 \exec 資料夾中或儲存在 LICENSEKEYPATH 參數中指定的另一個路徑。

  LICENSEKEYPATH 可以使用的值如下。

  - 包括其名稱的金鑰檔案的完整路徑。
  - 儲存參數檔案的資料夾路徑。

  您可以在安裝 Kaspersky Embedded Systems Security 後使用所選的管理工具（例如，應用程式主控台）新增金鑰。如果您在應用程式安裝期間未新增金鑰，Kaspersky Embedded Systems Security 將不會發揮功能。

- 設定檔的路徑。Kaspersky Embedded Systems Security 從在應用程式中建立的指定設定檔匯入設定。Kaspersky Embedded Systems Security 無法從設定檔匯入密碼，例如，用來啟動工作的帳戶密碼或用來連線代理伺服器的密碼。一旦匯入設定，將需手動輸入所有密碼。如果未指定設定檔，安裝後應用程式將開始使用預設設定。

  沒有指定CONFIGPATH=<configuration file name>的預設值。

- *作業系統啟動時掃描* 模式（ SCANSTARTUP_BLOCKING ）。如果安裝 Kaspersky Embedded Systems Security 時沒有使用SCANSTARTUP_BLOCKING金鑰，請依下列資訊設定「*作業系統啟動時掃描*」工作中的**掃描範圍**參數：
  - 對受感染物件和其他物件執行的操作：**通知**。
  - 針對疑似感染的物件執行的操作：**通知**。

如果安裝 Kaspersky Embedded Systems Security 時使用了 SCANSTARTUP_BLOCKING 金鑰，請依下列資訊設定「*作業係統啟動時掃描*」工作中的**掃描範圍**參數：

- 對受感染物件和其他物件執行的操作：**Perform recommended action**。
- 針對疑似感染的物件執行的操作：**Perform recommended action**。

「*作業係統啟動時掃描*」工作由系統自動建立。預設套用**通知**模式。在這種情況下，在裝置上部署 Kaspersky Embedded Systems Security 後，如果在掃描期間未發現系統服務問題，您可以啟用「*作業係統啟動時掃描*」工作。如果應用程式將關鍵系統服務偵測為受感染或疑似感染的物件，**通知**模式會讓您有時間找出原因並解決問題。如果應用程式套用 **Perform recommended action** 模式，則執行**Disinfect. Delete if disinfection fails**操作。解毒或移除系統檔案可能會導致作業系統啟動出現嚴重問題。

- 停用不相容軟體檢查。使用此設定可在受防護裝置上的應用程式背景安裝期間啟用或停用不相容軟體檢查。無論此設定的值如何，在安裝 Kaspersky Embedded Systems Security 期間，應用程式一律會警告受防護裝置上安裝之應用程式的其他版本。

  SKIPPRODUCTCHECK=<value> 命令列選項可能的取值選項如下（您也可以使用 SKIPINCOMPATIBLESW=<value>）：

  - 0 – 執行不相容軟體檢查（預設值）。
  - 1 – 不執行不相容軟體檢查。

- 停用自動移除不相容軟體。

  如果指定了 SKIPPRODUCTUNINSTALL=1 選項，Kaspersky Embedded Systems Security 不會刪除不相容的軟體。如果未指定此選項，Kaspersky Embedded Systems Security 會自動嘗試刪除不相容的軟體。

  > 使用 msiexec 安裝程式安裝 Kaspersky Embedded Systems Security 時，不會執行刪除不相容軟體。若要自動刪除可能導致相容性問題的軟體，請使用 setup_ess.exe 檔案。

- 停用檢查 KB5007186 作業系統更新。

  安裝 KB5007186 更新後，應用程式繼續正常運作，系統安全性不會受到損害，但無法對應用程式進行細微版本更新。在安裝應用程式之前，安裝程式會檢查已安裝的作業系統更新。如果發現更新 KB5007186，安裝程式將中止安裝。您可以使用命令列上的 SKIPKB5007186CHECK 鍵啟用或停用 KB5007186 作業系統更新檢查。

  SKIPKB5007186CHECK=<value> 可以使用的值如下。

  - 0 — 安裝程式檢查是否安裝了 KB5007186 作業系統更新。
  - 1 — 安裝程式不會檢查是否安裝了 KB5007186 作業系統更新。

  預設不設定該值，它對應 0。

- 配置作業係統防護服務功能。

  如果啟用了此功能，則協力廠商應用程式無法對作業系統的處理程序採取行動。PROTECTOSSERVICES=<value> 可以使用的值如下。

  - 1 表示作業係統服務防護已啟用（預設設定）。
  - 0 表示作業係統服務防護已停用。

- 設定應用程式主控台與安裝應用程式的電腦的遠端連線所使用的連接埠：

要設定用於連線 Windows 憑據的連接埠，您可以使用`UIPORT=<port number>`參數。可能的連接埠號範圍：1–65535。如果數字超出指定的間隔，則使用預設連接埠號。預設值為 13032。

如果需要，您可以使用`ENABLEUIKLPORT=<value>`參數關閉使用手動建立的使用者憑據進行連線的連接埠：

- `1` 開啟連接埠（預設設定）。
- `0` 關閉連接埠。

此連接埠的預設值為 13031。您可以透過指定`UIKLPORT=<value>`參數來變更連接埠號。可能的連接埠號範圍：1–65535。

- 網路連線啟用設定，適用於使用安裝在不同電腦上的應用程式主控台遠端管理 Kaspersky Embedded Systems Security。

  `ADDWFEXCLUSION=<value>` 可以使用的值如下。

  - `1` 如果指定了此值，則為應用程式主控台與安裝了該應用程式的電腦的遠端連線配置的 TCP 連接埠（`UIPORT=<value>` 和 `UIKLPORT=<value>`參數）將在 Windows 防火牆中開啟，並允許 Kaspersky Embedded Systems Security 遠端管理處理程序的可執行檔 avp.exe 進行網路連線。

    另請閱讀 在另一台裝置上安裝應用程式時進行額外配置。

  - `0` 如果指定此值，則不會發生任何事情。

- 跳過安裝 DigiCert Assured ID Root CA 根憑證到作業系統的受信任憑證儲存區。

  如果在安裝應用程式時指定了 `SKIPINSTALLROOTCACERTIFICATES` 選項。則不安裝 DigiCert Assured ID Root CA 根憑證。預設情況下，憑證會從應用程式安裝套件自動安裝。

復原設定以及 Windows 安裝程式命令列選項

- 還原隔離的物件。

  `RESTOREQTN=<value>` 可以使用的值如下。

  - `0` – 刪除隔離內容（預設值）。
  - `1` – 將隔離內容還原到 RESTOREPATH 參數所指定的資料夾的 \QB 子資料夾中。

- 還原備份內容。

  `RESTOREBCK=<value>` 可以使用的值如下。

  - `0` – 刪除備份內容（預設值）。
  - `1` – 將備份內容還原到 RESTOREPATH 參數所指定的資料夾 \QB 子資料夾中。

- 輸入目前密碼以確認還原（如果已啟用密碼防護）。

  沒有指定`UNLOCK_PASSWORD=<specified password>`的預設值。

- 還原物件的資料夾。還原的物件將儲存到指定的資料夾。

  `RESTOREPATH=<full path to the folder>` 命令列選項的預設值為 %ALLUSERSPROFILE%\Program Data\Kaspersky Lab\KESS.4.1.0\QB\Restored

安裝 Kaspersky Embedded Systems Security 的指令範例

本章節提供安裝 Kaspersky Embedded Systems Security 所使用的指令範例。

在受防護裝置上執行分發套件中的 ess_win.msi 檔案。

有關使用 Windows Installer 標準指令和命令列選項的詳細資訊，提供在 Microsoft 提供的文件中。

從 setup_ess.exe 檔案安裝 Kaspersky Embedded Systems Security 的範例

若要在無需與使用者參與的情況下使用建議的安裝設定安裝 Kaspersky Embedded Systems Security：

```
\exec\setup_ess.exe EULA=1 PRIVACYPOLICY=1
```

要安裝元件，例如裝置控制：

```
\exec\setup_ess.exe /p ADDLOCAL=DevCtrl /p RUNRTP=0
```

若在具有網路裝置和 SCSI 裝置的電腦上安裝 Kaspersky Embedded Systems Security，並在安裝後導致系統毀損，您可以用此命令使用以下附加選項：

```
/p SKIP_NETWORK_UPPERFILTERS=<1|0>
```

啟用 (`1`) 或停用 (`0`) 網路介面卡連線攔截。

```
/p SKIP_SCSIADAPTER_UPPERFILTERS=<1|0>
```

啟用 (`1`) 或停用 (`0`) SCSI 介面卡連線攔截。

若要使用金鑰檔案安裝和啟動 Kaspersky Embedded Systems Security：

```
setup_ess.exe /s EULA=1 PRIVACYPOLICY=1 /p LICENSEKEYPATH=C:\0000000A.key
```

若要變更用於將應用程式主控台與在其上使用 Windows 使用者憑據安裝了應用程式的電腦進行遠端連線的連接埠：

```
setup_ess.exe /pUIPORT=<port number>
```

可能的連接埠號範圍：1–65535。預設值為 13032。

用於安裝的命令清單：執行 .msi 檔案

若要在無需與使用者參與的情況下使用建議的安裝設定安裝 Kaspersky Embedded Systems Security：

```
msiexec /i ess_win.msi /qn EULA=1 PRIVACYPOLICY=1
```

若要使用建議的安裝設定安裝 Kaspersky Embedded Systems Security 並顯示安裝介面：

```
msiexec /i ess_win.msi /qf EULA=1 PRIVACYPOLICY=1
```

若要使用建議的安裝設定安裝 Kaspersky Embedded Systems Security，並在偵錯檔案數量達到指定的數量上限時啟用偵錯檔案輪替：

```
msiexec /i ess_win.msi TRACE_FOLDER=C:\Traces TRACE_MAX_ROLL_COUNT=50 /qn EULA=1 PRIVACYPOLICY=1
```

TRACE_FOLDER 參數為必要性質。

以下規則適用於 TRACE_MAX_ROLL_COUNT 參數：

- 如果指定此參數，則當偵錯檔案數量達到參數中指定的數量上限時，會啟用偵錯檔案輪替。可用參數值範圍：從 1 到 999。
- 如果偵錯檔案的數量上限指定為 0，則會停用偵錯檔案輪替。
- 如果指定了參數值，但該值無效或超出可用值範圍（從 1 到 999），則會啟用偵錯檔案輪替，並將偵錯檔案的預設數量上限設為 5。
- 如果未指定該參數：
  - 如果裝置上已設定偵錯檔案輪替，則其設定不會變更。應用程式將忽略輸入的參數。
  - 如果裝置上未設定偵錯檔案輪替，則將啟用輪替選項，並將偵錯檔案的預設數量上限設為 5。

若要以 C:\0000000A.key 的金鑰檔案安裝 Kaspersky Embedded Systems Security：

```
msiexec /i ess_win.msi     LICENSEKEYPATH=C:\0000000A.key /qn EULA=1 PRIVACYPOLICY=1
```

若要安裝 Kaspersky Embedded Systems Security 並初步掃描啟動處理程序與本機磁碟機的開機磁區：

```
msiexec /i ess_win.msi PRESCAN=1 /qn EULA=1 PRIVACYPOLICY=1
```

要將 Kaspersky Embedded Systems Security 安裝在安裝資料夾 C:\KESS 中：

```
msiexec /i ess_win.msi INSTALLDIR=C:\KESS/qn EULA=1 PRIVACYPOLICY=1
```

若要安裝 Kaspersky Embedded Systems Security 並將名稱為 ess.log 的安裝記錄檔案儲存在儲存 Kaspersky Embedded Systems Security msi 檔案的資料夾中：

```
msiexec /i ess_win.msi/l*v ess.log /qn EULA=1 PRIVACYPOLICY=1
```

若要安裝 Kaspersky Embedded Systems Security 主控台：

```
msiexec /i esstools.msi /qn EULA=1
```

若要使用參數檔案 C:\0000000A.key 安裝並啟用 Kaspersky Embedded Systems Security，並根據 C:\settings.xml 設定檔中的設定配置 Kaspersky Embedded Systems Security：

```
msiexec /i ess_win.msi LICENSEKEYPATH=C:\0000000A.key CONFIGPATH=C:\settings.xml /qn EULA=1 PRIVACYPOLICY=1
```

若要在 Kaspersky Embedded Systems Security 受密碼防護的情況下安裝應用程式修補程式：

```
msiexec /p "<MSP file path>" UNLOCK_PASSWORD=<password>
```

在安裝 Kaspersky Embedded Systems Security 後執行的操作

如果您已啟動 Kaspersky Embedded Systems Security，該應用程式在安裝後立即啟動防護和掃描工作。如果在安裝 Kaspersky Embedded Systems Security 期間選取 **安裝應用程式後啟用即時檔案防護（建議）** 核取方塊，應用程式會在存取裝置的檔案系統物件時進行掃描。如果指令碼監控元件是作為自訂安裝的一部分安裝的，則 Kaspersky Embedded Systems Security 會在啟動指令碼時掃描所有指令碼的原始程式碼。Kaspersky Embedded Systems Security 將在每週五晚上 8:00 執行*關鍵區域掃描*工作。

建議在安裝 Kaspersky Embedded Systems Security 後執行下列步驟：

- 啟動 Kaspersky Embedded Systems Security 更新工作。安裝後，Kaspersky Embedded Systems Security 會使用其分發套件中的資料庫掃描物件。我們建議立即更新 Kaspersky Embedded Systems Security 資料庫。為此，請執行*更新*工作。之後，更新將根據預設排程每小時執行一次。

  例如，您可以透過執行以下指令來啟動 *更新* 工作：

  ```
  KAVSHELL UPDATE /KL /PROXY:proxy.company.com:8080 /AUTHTYPE:1 /PROXYUSER:inetuser /PROXYPWD:p@ssw0rd
  ```

  在此情況下，將從 Kaspersky 更新伺服器下載 Kaspersky Embedded Systems Security 資料庫更新。

- 如果安裝 Kaspersky Embedded Systems Security 之前受防護裝置上未安裝任何具有即時檔案防護的病毒防護軟體，請啟動*關鍵區域掃描*工作。

  您可以透過從命令列執行以下指令來啟動 *關鍵區域掃描* 工作：

  ```
  KAVSHELL SCANCRITICAL /W:scancritical.log
  ```

  此指令會將工作記錄儲存在目前資料夾內名為 scancritical.log 檔案中。

- 配置有關 Kaspersky Embedded Systems Security 事件的管理員通知。

新增/移除元件。指令範例

要安裝按需掃描元件，請執行以下指令：

```
msiexec /i ess_win.msi ADDLOCAL=Oas,Ods /qn
```

或

```
\exec\setup_ess.exe /s /p ADDLOCAL=Oas,Ods
```

將元件新增至清單後，Kaspersky Embedded Systems Security 會重新安裝現有元件並安裝指定的元件。

要刪除已安裝的元件，請執行以下指令：

```
msiexec /i ess_win.msi REMOVE=Firewall,PerfMonCounters EULA=1 PRIVACYPOLICY=1 /qn
```

要安裝新的元件，請執行以下指令：

```
msiexec /i ess_win.msi
ADDLOCAL=AKIntegration,AVProtection,AntiExploit,AppCtrl,DevCtrl,Fim,Ksn,LogInspector,Oas,Ods,SnmpSupport,TrayApp,IDS,
EULA=1 PRIVACYPOLICY=1 /qn
```

列出您要安裝和移除的元件之後，Kaspersky Embedded Systems Security 會安裝並移除對應的元件。

Kaspersky Embedded Systems Security 移除。指令範例

要在靜默模式下從受防護裝置移除 Kaspersky Embedded Systems Security，請執行以下指令：

```
msiexec /x ess_win.msi KLLOGIN=<user name> KLPASSWD=<password> /qn
```

或

```
msiexec /x {6202AB29-4AC2-4A92-AF8E-977AADD4B27F} KLLOGIN=<user name> KLPASSWD=<password> /qn
```

或

```
setup_ess.exe /pKLLOGIN=<user name> /pKLPASSWD=<password> /s /x
```

其中 `<user name>` 是具有足夠 權限 解除安裝的使用者的姓名和登入名稱。

如果為執行刪除操作的使用者帳戶設定了空的 Windows 密碼，請在開始刪除之前停用**請求密碼以確認關鍵操作**功能。

要在靜默模式下移除 Kaspersky Embedded Systems Security，請執行以下指令：

```
msiexec /x esstools.msi /qn
```

或

```
msiexec /x {E827CBBA-974C-4386-B50E-8F202D41E428} /qn
```

回傳代碼

應用程式安裝程式可以返回 本文 中所述的回傳代碼。

下表包含了命令列的回傳代碼清單。

回傳代碼

代碼	描述
27100	在電腦上偵測到在測試模式下安裝了身分驗證代理程式的磁碟機。
27101	在電腦上偵測到在測試模式下安裝了身分驗證代理程式的磁碟機。
27102	無法找到加密磁碟。
27200	無法從 RAM 卸載應用程式。
27201	啟動 AVP.exe 處理程序時發生錯誤。您的電腦可能已被感染。
27204	無法快取分發套件。
27205	遷移產品授權資訊失敗。
27206	無法刪除產品授權資訊。
27207	無法刪除不相容的軟體。
27208	無法檢查不相容的軟體。
27209	無法從文件櫃中提取檔案。
27210	無法配置自我防禦。
27211	無法啟用自我防禦。
27212	無法取得作業系統版本資訊。
27213	無法取得啟動目錄。
27214	無法驗證安裝目錄。
27215	無法配置服務。
27216	無法配置 klcp 升級。
27217	升級 klcp 失敗。
27218	無法配置 kl1 驅動程式參數。
27219	無法配置 klelam 驅動程式參數。
27220	無法配置 klwfp 驅動程式參數。
27221	無法配置驅動程式相容模式。
27222	無法刪除登錄機碼。
27223	無法重新啟動作業系統。
27224	無法安裝驅動程式。
27225	無法遷移驅動程式設定。

代碼	描述
27226	無法停止驅動程式。
27227	無法阻止驅動程式啟動。
27228	無法驗證文件的簽名。
27230	無法準備 kldl 驅動程式設定。
27231	無法配置 kldl 驅動程式設定。
27300	安裝驅動程式錯誤。
27301	刪除驅動程式時發生錯誤。
27302	安裝網路元件時發生錯誤。
27303	驅動程式的註冊資料不一致或不完整。請重新啟動作業系統並重試。
27305	停用驅動程式時發生錯誤。
27310	無法安裝數位簽章的目錄檔案。
27311	無法卸載數位簽章的目錄檔案。
27312	無法安裝憑證。
27313	無法刪除憑證。
27320	無法配置服務。
27321	無法取消防護服務。
27350	修補程式<修補程式名稱>不適用於<應用程式名稱>應用程式當地語係化。
27352	完整磁碟加密修補程式無法被刪除。
27353	修補程式<patch 1 name>只能與修補程式<patch 2 name>一起安裝。
27354	在修改/還原應用程式之前，必須重新啟動電腦才能套用修補程式。
27355	無法鎖定完整磁碟碟加密管理。無法鎖定完整磁碟碟加密管理。您必須完成加密才能安裝完整磁碟加密的更新。
27356	無法安裝修補程式。
27357	發現安裝套件包含召回的修補程式。安裝將被中止。
27360	無法註冊修補程式。
27361	設定修補程式安裝參數失敗。
27363	修補程式包含與已安裝的加密庫不相容的加密庫。
27370	初始化 .NET 8.0 解壓縮時發生錯誤。
27371	解壓縮 .NET 8.0 時發生錯誤。
27372	先前應用程式版本的註冊資訊已被刪除。請重新開始安裝。
27373	無法刪除先前應用程式版本的註冊資訊。
27374	應用程式正在升級。請稍後重試。
27375	解除安裝密碼或使用者名稱未指定或不正確。
27376	無法解除安裝 Kaspersky Endpoint Agent。請自行解除安裝或在設定中停用密碼防護。然後重新啟動應用程式的安裝。
27377	無法解除安裝 Kaspersky Security for Windows Server。請自行解除安裝或在設定中停用密碼防護。然後重新啟動應用程式的安裝。
27378	磁碟空間不足。
27379	由於選擇了不相容的元件，因此無法安裝應用程式。請變更元件集並重新開始安裝。
27380	選擇了無效的設定檔。
27381	選擇了無效的產品授權金鑰。
27382	無法建立應用程式管理群組。
27383	您選擇的資料夾無效。目標資料夾的名稱不能超過 160 個字元。
27384	您選擇了無效的資料夾或磁碟機。該應用程式必須安裝在本機硬碟上。

代碼	描述
27385	您選擇的資料夾無效。該應用程式無法被安裝到根資料夾。
27386	您選擇的資料夾無效。該應用程式無法被安裝到 Windows 資料夾或其子資料夾中。
27387	您選擇的資料夾無效。無法將應用程式安裝到包含 Temp 子資料夾的資料夾中。
27388	您選擇的資料夾無效。應用程式不能直接安裝在 Program Files 資料夾中。
27389	您選擇的資料夾無效。應用程式無法安裝在虛擬磁碟上。
27390	您選擇了無效的資料夾或磁碟機。應用程式無法安裝到安裝該應用程式先前版本的資料夾。
27391	選定的資料夾或磁碟機已包含檔案。應用程式無法安裝到包含其他資料的資料夾中，因為啟用自我防禦後這些資料將變得不可用。
27392	應用程式無法安裝到包含重新解析點的資料夾中。請選擇其他安裝資料夾。
27393	無法將應用程式安裝到名稱中包含分號 (;) 的資料夾中。請選擇其他安裝資料夾。
27394	您選擇的資料夾無效。無法指定根資料夾。
27395	您選擇的資料夾無效。無法指定 Windows 資料夾或其子資料夾。
27396	您選擇的資料夾無效。無法直接指定 Program Files 資料夾。
27397	您選擇的資料夾無效。無法指定包含 Temp 子資料夾的資料夾。
27400	初始化檔案更新時發生錯誤。
27450	無法安裝 CAB 檔案。
27451	移除時發生錯誤。
27452	刪除檔案時發生錯誤。
27453	移動文件時出錯。
27454	無法建立登錄檔檔案。
27455	無法取得作業系統版本資訊。
27456	無法排程回溯登錄檔值。
27457	無法取得知名的安全識別碼 (SID)。
27460	建立安全描述符時出錯。
27461	還原安全描述符時出錯。
27462	無法為 Microsoft Windows 防火牆建立規則。
27463	無法刪除 Microsoft Windows 防火牆規則。

使用卡巴斯基安全管理中心安裝和移除應用程式

本部分包含使用卡巴斯基安全管理中心安裝 Kaspersky Embedded Systems Security 的資訊、透過卡巴斯基安全管理中心安裝和解除安裝 Kaspersky Embedded Systems Security 的程序說明以及安裝 Kaspersky Embedded Systems Security 之後要採取的動作說明。

有關透過卡巴斯基安全管理中心安裝的一般資訊

您可以透過卡巴斯基安全管理中心，使用遠端安裝工作來安裝 Kaspersky Embedded Systems Security。

完成遠端安裝工作後，將可在多台受防護裝置上使用相同的設定安裝 Kaspersky Embedded Systems Security。

所有受防護裝置可以整合到一個管理群組中，並且可以建立群組工作來在該群組的受防護裝置上安裝 Kaspersky Embedded Systems Security。

您可以建立一個工作，在不屬於相同管理群組的一組受防護裝置上遠端安裝 Kaspersky Embedded Systems Security。建立此工作時，您必須建立一份要安裝 Kaspersky Embedded Systems Security 的各個受防護裝置的清單。

有關遠端安裝工作的詳細資訊，請參閱卡巴斯基安全管理中心說明。

安裝或移除 Kaspersky Embedded Systems Security 的權限

在除下述以外的所有情況下，在遠端安裝（移除）工作中指定的帳戶必須包含在每個受防護裝置的管理員群組中：

- 如果卡巴斯基安全管理中心網路代理已安裝在要安裝 Kaspersky Embedded Systems Security 的受防護裝置上（不論這些受防護裝置位於哪個網域，或它們是否屬於任何網域）。

  如果受防護裝置上尚未安裝網路代理，您可使用遠端安裝工作安裝網路代理程式與 Kaspersky Embedded Systems Security。安裝網路代理程式前，請確保要在該工作中指定的帳戶包含在每台受防護裝置的管理員群組中。

- 要安裝 Kaspersky Embedded Systems Security 的所有受防護裝置都在相同網域中作為管理伺服器使用，且管理伺服器以**網域管理員**帳戶身分註冊（如果此帳戶在該網域的受防護裝置上有本機管理員權限）。

預設情況下，使用"**強制安裝**"方式時，遠端安裝工作會從執行管理伺服器下的帳戶執行。

以強制安裝（移除）模式執行群組工作或整組受防護裝置的工作時，受防護裝置上的帳戶必須有下列權限：

- 遠端執行應用程式的權限。
- **Admin$** 共用的權限。
- **作為服務登入**的權限。

透過卡巴斯基安全管理中心安裝 Kaspersky Embedded Systems Security

透過卡巴斯基安全管理中心安裝 Kaspersky Embedded Systems Security 需要以下步驟：

1. **建立安裝套件**

   *安裝套件*是為透過卡巴斯基安全管理中心遠端安裝 Kaspersky 應用程式而建立的一組檔案。安裝套件中包含安裝應用程式以及安裝後立即執行應用程式所需的一系列設定。安裝套件透過應用程式分發套件中包括的副檔名為 .kpd 和 .kud 的檔案建立。

   如何在卡巴斯基安全管理中心管理主控台中建立安裝傲嬌

   1. 在卡巴斯基安全管理中心管理主控台樹狀目錄中，選取**進階** → **遠端安裝** → **安裝套件**資料夾。
   2. 在結果窗格中，點擊**建立安裝套件** 按鈕。

新安裝套件精靈啟動。按照精靈的說明進行操作。

步驟 1. 選取安裝套件類型

請選擇**為卡巴斯基應用程式建立安裝套件**選項。

步驟 2. 定義安裝套件名稱

輸入安裝套件的名稱，例如，*Kaspersky Embedded Systems Security*。

步驟 3. 選取用於安裝的分發套件

指定 Kaspersky Embedded Systems Security 分發套件的 ess_win.kud 檔案作為安裝套件檔案。

如果您打算使用「**使用病毒資料庫防護電腦**」設定（而不是使用應用程式設定，該應用程式設定不會使用特徵碼分析和病毒資料庫來保護電腦）來安裝應用程式，或是相反，您應該先在 ess_win.kud 檔案指定具有安裝應用程式的權限的帳戶的登入名稱和密碼。為此，請在文字編輯器中開啟 ess_win.kud 檔案，並將以下參數新增至 `Params` 行：`/pKLLOGIN=<login>` 和 `/pKLPASSWD=<password>`。

如有必要，請選擇 **從儲存區複製更新至安裝套件** 核取方塊更新安裝套件中的病毒資料庫。

步驟 4. 最終使用者產品授權協議和隱私政策

如果您同意最終使用者產品授權協議和隱私權政策的條款和條件，請選擇 **本人確認已完整閱讀、理解並接受本《最終使用者產品授權協議》的條款和條件** 和 **我瞭解並同意按照隱私權政策所述來處理和傳輸我的資料（包括傳輸到第三個國家/地區）。我確認我已完整閱讀並理解隱私權政策** 核取方塊。

您必須接受產品授權協議和隱私政策才能繼續。

安裝套件將被建立並新增到卡巴斯基安全管理中心中。使用安裝套件，您可以在企業網路電腦上安裝 Kaspersky Embedded Systems Security 或更新應用程式版本。

要變更要安裝的 Kaspersky Embedded Systems Security 元件集以及已建立的安裝套件中的預設安裝設定：

1. 在卡巴斯基安全管理中心管理主控台中，展開"**遠端安裝**"節點。
2. 在"**安裝套件**"子節點的結果窗格中，開啟已建立 Kaspersky Embedded Systems Security 安裝套件的內容功能表，然後選擇"**內容**"。
3. 在"**內容：<安裝套件名稱>**"視窗中開啟"**設定**"部分。
4. 點擊 **配置** 按鈕配置受信任區域。

5. 在“**元件選擇**”塊中，選中要安裝的 Kaspersky Embedded Systems Security 元件名稱旁邊的核取方塊。

6. 在 **即時檔案防護模式** 塊中，選擇 **安裝應用程式後啟用即時檔案防護（建議）** 核取方塊並選擇元件運作模式。

7. 如有必要，請變更應用程式主控台用於遠端連線到安裝了該應用程式的電腦的 TCP 連接埠號。

   使用 Windows 憑據進行連線的預設連接埠號為 13032，使用手動建立的使用者的憑據進行連線的預設連接埠號為 13031。可能的連接埠號範圍：1–65535。

   為了防止使用手動建立的使用者帳戶的憑據進行連線，請清除 **使用手動建立的使用者的憑證**核取方塊。

8. 要指定預設資料夾以外的安裝資料夾，請在“**設定應用程式安裝路徑**”塊中點擊**設定**按鈕指定資料夾名稱和路徑。

9. 若要使用預定義設定安裝應用程式，請上傳 設定檔。

10. 儲存變更。

如何在網頁主控台中建立安裝套件

1. 執行以下操作之一：

   - 在網頁主控台的主視窗中，選擇**發現和佈署 → 佈署和指派 → 安裝套件**。
   - 在網頁主控台的主視窗中，選擇**操作 → 儲存區 → 安裝套件**。

   這將開啟已下載到卡巴斯基安全管理中心的安裝套件清單。

2. 點擊“**新增**”。

新安裝套件精靈啟動。按照精靈的說明進行操作。

步驟 1. 選取安裝套件類型

請選擇**為卡巴斯基應用程式建立安裝套件**選項。

精靈將根據 Kaspersky 伺服器上的分發套件建立安裝套件。該清單在新版本的應用程式發佈時會自動更新。

您還可以從檔案建立安裝套件。

步驟 2. 安裝套件

選擇 Kaspersky Embedded Systems Security for Windows 安裝套件。安裝套件建立過程啟動。在安裝套件建立期間，您必須接受最終使用者產品授權協議和隱私權政策的條款。

> 您必須接受產品授權協議和隱私政策才能繼續。

安裝套件將被建立並新增到卡巴斯基安全管理中心中。使用安裝套件，您可以在企業網路電腦上安裝 Kaspersky Embedded Systems Security 或更新應用程式版本。

要變更要安裝的 Kaspersky Embedded Systems Security 元件集以及已建立的安裝套件中的預設安裝設定：

1. 在 **安裝套件** 視窗中，按一下已建立的 Kaspersky Embedded Systems Security 安裝套件的名稱。
2. 在開啟的視窗中選擇**"設定"**標籤。
3. 選擇 **防護元件** 部分。
4. 點擊 **配置** 按鈕配置受信任區域。
5. 在**"選擇要安裝的元件"**部分，選中要安裝的 Kaspersky Embedded Systems Security 元件名稱旁邊的核取方塊。
6. 在 **即時檔案防護模式** 塊中，選擇 **安裝應用程式後啟用即時檔案防護（建議）** 核取方塊並選擇元件運作模式。
7. 如有必要，請變更應用程式主控台用於遠端連線到安裝了該應用程式的電腦的 TCP 連接埠號。

   使用 Windows 憑據進行連線的預設連接埠號為 13032，使用手動建立的使用者的憑據進行連線的預設連接埠號為 13031。可能的連接埠號範圍：1–65535。

   為了防止使用手動建立的使用者帳戶的憑據進行連線，請清除 **用於使用手動建立的使用者憑證進行遠端連線的連接埠**核取方塊。
8. 選擇 **安裝設定** 部分。
9. 在**"進階設定"**部分中，配置以下設定：

   - **將應用程式位置新增至環境變數 %PATH% 中**您可以將安裝路徑新增到 %PATH% 變數中，以方便使用命令列進行應用程式管理。
   - **在工作列上顯示系統托盤圖示**如果選取該核取方塊，安裝 Kaspersky Embedded Systems Security 後，應用程式圖示將出現在 Microsoft Windows 工作列通知區域。
10. 如有必要，請停用 **防護安裝處理程序** 功能。
11. 如有必要，請變更應用程式安裝期間在受防護裝置上建立的預設資料夾。
12. 若要使用預定義設定安裝應用程式，請按一下 **新增設定檔** 連結並上傳 設定檔。

    在卡巴斯基安全管理中心網頁主控台中使用安裝套件時，受支援的上傳設定檔的最大大小為 4 MB。如果您在卡巴斯基安全管理中心管理主控台中使用安裝套件，則此限制不適用。
13. 儲存變更。

2 建立遠端安裝工作

遠端安裝應用程式 工作可讓您遠端安裝 Kaspersky Embedded Systems Security。*遠端安裝應用程式*工作允許您將應用程式的安裝套件佈署到組織中的所有電腦裡。

如何在卡巴斯基安全管理中心管理主控台中建立遠端安裝工作

1. 開啟卡巴斯基安全管理中心管理主控台。
2. 在主控台樹狀目錄中，選擇**"工作"**。
   工作清單開啟。
3. 單擊**"新工作"**。

啟動"工作精靈"。按照精靈的說明進行操作。

步驟 1. 選取工作類型

選擇**"卡巴斯基安全管理中心管理伺服器 → 遠端安裝應用程式"**。

步驟 2. 選取安裝套件

從清單中選擇 Kaspersky Embedded Systems Security 安裝套件。如果清單不包含 Kaspersky Embedded Systems Security 安裝套件，可以在精靈中建立該套件。

您可以在卡巴斯基安全管理中心配置安裝套件設定。例如，您可以選取將安裝到電腦的應用程式元件。

網路代理也將與 Kaspersky Embedded Systems Security 一起安裝。*網路代理*可促進管理伺服器與用戶端電腦之間的互動。如果電腦上已安裝網路代理，則不會再次安裝。

步驟 3. 其他

選取網路代理安裝套件。所選版本的網路代理將與 Kaspersky Embedded Systems Security 一起安裝。

步驟 4. 設定

配置以下其他應用程式設定：

- **強制下載安裝套件**選取應用程式安裝方法：
  - **使用網路代理**網路代理負責將 Kaspersky Embedded Systems Security 安裝套件分發到用戶端電腦。如果未安裝網路代理，該工作將以錯誤結束。在這種情況下，請將網路代理安裝套件新增至 *遠端安裝應用程式* 工作並透過作業系統資源啟用檔案傳輸。然後，網路代理將使用作業系統資源進行安裝。Kaspersky Embedded Systems Security 然後使用網路代理進行安裝 。
  - **透過發佈點使用作業系統資源**透過發佈點使用作業系統資源將安裝套件傳輸到用戶端電腦。如果網路中有至少一個發佈點，則可以選取此選項。有關發佈點的詳細資訊，請參閱卡巴斯基安全管理中心說明 。
  - **透過管理伺服器使用作業系統資源**檔案將透過管理伺服器使用作業系統資源傳送到用戶端電腦。如果用戶端電腦上未安裝網路代理，但用戶端電腦與管理伺服器在同一網路中，可以選取此選項。
- **透過其他管理伺服器管理的裝置的行為**選擇 Kaspersky Embedded Systems Security 安裝方式。如果網路中安裝了多個管理伺服器，這些管理伺服器可能看到相同的用戶端電腦。例如，這可能導致透過不同的管理伺服器在同一用戶端電腦上多次遠端安裝同一應用程式，或產生其他衝突。
- **如果已經安裝應用程式則不再重新安裝**例如，如果要安裝較早版本的應用程式，則清除此核取方塊。

步驟 5. 選取作業系統重新啟動設定

選取當需要重新啟動電腦時所執行的操作。安裝 Kaspersky Embedded Systems Security 時無需重新啟動。僅當在安裝前必須移除不相容的應用程式時，才需要重新啟動。更新應用程式版本時也可能需要重新啟動。

步驟 6. 選取將要對其分配工作的裝置

選取將在上面安裝 Kaspersky Embedded Systems Security 的電腦。下列選項可用：

- 將工作分配給管理群組。在這種情況下，工作分配給先前建立的管理群組中包括的電腦。
- 選取管理伺服器在網路中偵測到的電腦：*未分配裝置*。網路代理不會安裝在未配置裝置上。在這種情況下，工作將分配給特定裝置。特定裝置可包括管理群組中的裝置以及未配置裝置。
- 手動指定裝置位址或從清單中匯入位址。您可以指定您要將工作分配給的裝置的 NetBIOS 名稱、IP 位址和 IP 子網路。

步驟 7. 選取要執行工作的帳戶

選取用於使用作業系統工具安裝網路代理的帳戶。在這種情況下，存取電腦需要管理員權限。您可以新增多個帳戶。如果某個帳戶沒有足夠權限，安裝精靈將使用下一個帳戶。如果使用網路代理工具安裝 Kaspersky Embedded Systems Security，則無需選取帳戶。

步驟 8. 設定工作啟動排程

配置啟動工作的排程，例如，手動或在電腦空閒時。

步驟 9. 定義工作名稱

輸入工作的名稱，例如“*安裝 Kaspersky Embedded Systems Security for Windows 4.1*”。

步驟 10.完成工作建立

結束精靈。如有必要，選中“**精靈完成時執行工作**”核取方塊。您可以在工作內容中監控工作進度。應用程式將以靜默模式安裝。安裝後， 圖示將新增到使用者電腦的通知區域。如果圖示看起來像 ，請確保您已啟動應用程式。

如何在網頁主控台中建立遠端安裝工作

1. 在網頁主控台的主視窗中，選擇**資產管理 → 工作**。

   工作清單開啟。

2. 單擊“**新增**”。

啟動“工作精靈”。按照精靈的說明進行操作。

步驟 1. 配置一般工作設定

配置一般工作設定：

1. 在“**應用程式**”下拉清單中，選取“**卡巴斯基安全管理中心**”。
2. 在“**工作類型**”下拉式清單中，選取“**遠端安裝應用程式**”。
3. 在“**工作名稱**”欄位中，輸入簡要說明，例如，“*為經理安裝 Kaspersky Embedded Systems Security*”。
4. 在“**要將工作指派給的裝置**”塊中，選取工作範圍。

步驟 2. 選取要進行安裝的電腦

在此步驟中，按照選定的工作範圍選項，選取要安裝 Kaspersky Embedded Systems Security 的電腦。

步驟 3. 配置安裝套件

在此步驟中，配置安裝套件：

1. 選擇 Kaspersky Embedded Systems Security for Windows (4.1) 安裝套件。
2. 選取網路代理安裝套件。

   所選版本的網路代理將與 Kaspersky Embedded Systems Security 一起安裝。*網路代理*可促進管理伺服器與用戶端電腦之間的互動。如果電腦上已安裝網路代理，則不會再次安裝。
3. 在**強制下載安裝套件**區塊中，選擇應用程式安裝方法：

   - **使用網路代理**網路代理負責將 Kaspersky Embedded Systems Security 安裝套件分發到用戶端電腦。如果未安裝網路代理，該工作將以錯誤結束。在這種情況下，請將網路代理安裝套件新增至 *遠端安裝應用程式* 工作並透過作業系統資源啟用檔案傳輸。然後，網路代理將使用作業系統資源進行安裝。Kaspersky Embedded Systems Security 然後使用網路代理進行安裝 。
   - **透過發佈點使用作業系統資源**透過發佈點使用作業系統資源將安裝套件傳輸到用戶端電腦。如果網路中有至少一個發佈點，則可以選取此選項。有關發佈點的詳細資訊，請參閱卡巴斯基安全管理中心說明 。
   - **透過管理伺服器使用作業系統資源**檔案將透過管理伺服器使用作業系統資源傳送到用戶端電腦。如果用戶端電腦上未安裝網路代理，但用戶端電腦與管理伺服器在同一網路中，可以選取此選項。
4. 在**同時下載的最大數量**欄位中，設定傳送到管理伺服器的安裝套件下載請求數量限制。限制請求數有助於防止網路超載。
5. 在"**安裝嘗試次數上限**"欄位中，設定安裝應用程式嘗試次數限制。如果安裝 Kaspersky Embedded Systems Security 以出錯結束，工作將自動再次啟動安裝。
6. 如有必要，清除"**如果已經安裝應用程式則不再重新安裝**"核取方塊。例如，這樣可以安裝應用程式的一個先前版本。
7. 如有必要，清除"**下載之前驗證作業系統類型**"核取方塊。這樣可避免在電腦的作業系統不符合軟體需求時下載應用程式分發套件。如果您確定電腦的作業系統符合軟體需求，可以略過此驗證。
8. 如有必要，選中"**在 Active Directory 群組政策中指派安裝套件的安裝**"核取方塊。Kaspersky Embedded Systems Security 透過網路代理安裝或透過 Active Directory 手動安裝。要安裝網路代理，必須以網域管理員權限執行遠端安裝工作。
9. 如有必要，選中"**提示使用者關閉執行中的應用程式**"核取方塊。安裝 Kaspersky Embedded Systems Security 會佔用電腦資源。為方便使用者，應用程式安裝精靈會在開始安裝前提示您關閉正在執行的應用程式。這有助於防止其他應用程式執行中端，並防止可能的電腦故障。
10. 在"**透過其他管理伺服器管理的裝置的行為**"塊中，選取 Kaspersky Embedded Systems Security 安裝方法。如果網路中安裝了多個管理伺服器，這些管理伺服器可能看到相同的用戶端電腦。例如，這可能導致透過不同的管理伺服器在同一用戶端電腦上多次遠端安裝同一應用程式，或產生其他衝突。

步驟 4. 選取要執行工作的帳戶

選取用於使用作業系統工具安裝網路代理的帳戶。在這種情況下，存取電腦需要管理員權限。您可以新增多個帳戶。如果某個帳戶沒有足夠權限，安裝精靈將使用下一個帳戶。如果使用網路代理工具安裝 Kaspersky Embedded Systems Security，則無需選取帳戶。

步驟 5. 完成工作建立

點擊**"完成"**按鈕結束精靈。在工作清單中將顯示一個新工作。要執行工作，請選中與工作對應的核取方塊，然後點擊**"開始"**按鈕。應用程式將以靜默模式安裝。安裝後， 圖示將新增到使用者電腦的通知區域。如果圖示看起來像 ，請確保您已啟動應用程式。

如需更多有關產生安裝套件和遠端安裝工作的資訊，請參閱卡巴斯基安全管理中心說明。

在安裝 Kaspersky Embedded Systems Security 後執行的操作

安裝 Kaspersky Embedded Systems Security 後，建議更新裝置上的 Kaspersky Embedded Systems Security 資料庫；若安裝 Kaspersky Embedded Systems Security 前，裝置上未安裝任何防毒應用程式並啟用即時防護功能，則還建議對裝置執行關鍵區域掃描。

如果安裝了 Kaspersky Embedded Systems Security 的受防護裝置在卡巴斯基安全管理中心中屬於同一個管理群組，您可以使用以下方法執行這些工作：

1. 為安裝了 Kaspersky Embedded Systems Security 的受防護裝置群組建立*更新*工作。將卡巴斯基安全管理中心管理伺服器設定為更新來源。
2. 建立具有「*關鍵區域掃描*」狀態的自訂掃描群組工作。卡巴斯基安全管理中心會根據此工作的結果（而不是根據「*關鍵區域掃描*」的結果）評估群組中每台受防護裝置的安全狀態。
3. 為受防護裝置組建立新的政策。在政策內容的**應用程式設定**區段中，停用系統自訂掃描工作的排程啟動，並在**執行本機系統工作**子區域的設定中停用管理群組受防護裝置上的*更新*工作。

您還可以配置有關 Kaspersky Embedded Systems Security 事件的管理員通知。

透過卡巴斯基安全管理中心安裝應用程式主控台

如需更多有關建立安裝套件和遠端安裝工作的資訊，請參閱卡巴斯基安全管理中心說明。

要使用遠端安裝工作安裝應用程式主控台，請執行下列操作：

1. 在卡巴斯基安全管理中心管理主控台中，展開**"進階"**節點。
2. 展開**"遠端安裝"**子節點。

3. 建立安裝套件：

   a. 在“**安裝套件**”子節點的結果窗格中，點擊“**建立安裝套件**”按鈕。

   b. 在“**新套件精靈**”視窗中，選擇“**建立指定可執行檔的安裝套件**”作為套件類型。

   c. 輸入新安裝套件名稱。

   d. 選取 Kaspersky Embedded Systems Security 分發套件資料夾中的 \client\setup_esstool.exe 檔案，然後選取「**將整個資料夾複製到安裝套件**」核取方塊。

   e. 在 **可執行檔啟動設定（可選）** 欄位中，指定參數值 EULA=1 和 PRIVACYPOLICY=1:

   ```
   /s /p "EULA=1 PRIVACYPOLICY=1"
   ```

   否則無法安裝元件。

   f. 如有必要，在**可執行檔啟動設定（選用）**欄位中，您可以指定 ADDLOCAL 命令列參數，以變更要安裝的元件集，並使用 INSTALLDIR 命令列參數，以指定預設資料夾以外的目的地資料夾。例如，若要在 C:\KasperskyConsole 資料夾中執行應用程式主控台的獨立安裝，請使用以下命令列選項：

   ```
   /s /p "INSTALLDIR=C:\KasperskyConsole EULA=1 PRIVACYPOLICY=1"
   ```

4. 在“**安裝套件**”子節點中，建立一個工作， 在選定的受防護裝置（管理群組）上遠端安裝應用程式主控台。

5. 配置工作設定。

6. 執行遠端安裝工作。

應用程式主控台安裝到此工作指定的受防護裝置上。

透過卡巴斯基安全管理中心移除 Kaspersky Embedded Systems Security

移除 Kaspersky Embedded Systems Security 時不會刪除 Dump 和偵錯檔案。您可以手動刪除在配置 Dump 和偵錯檔案寫入期間指定的資料夾中的 Dump 和偵錯檔案。

如果網路裝置上的 Kaspersky Embedded Systems Security 管理受密碼防護，在建立用於移除多個應用程式的工作時請輸入密碼。如果未透過卡巴斯基安全管理中心政策集中管理，Kaspersky Embedded Systems Security 將從裝置成功移除，在該裝置上輸入的密碼與設定值比對。不會從其他受防護裝置移除 Kaspersky Embedded Systems Security。

要移除 Kaspersky Embedded Systems Security：

1. 在卡巴斯基安全管理中心管理主控台中，建立並啟動應用程式刪除工作。

2. 在該工作中，選擇移除方法（與選擇安裝方法類似，請參見上一節）並指定管理伺服器將用來存取受防護裝置的帳戶。您只可以使用預設解除安裝設定移除 Kaspersky Embedded Systems Security。

使用卡巴斯基安全管理中心變更應用程式元件集

「*變更應用程式元件*」工作允許您在安裝應用程式後變更 Kaspersky Embedded Systems Security 元件集。

如何在卡巴斯基安全管理中心管理主控台中變更應用程式元件集

1. 在卡巴斯基安全管理中心管理主控台樹狀目錄中，選取**工作**。
   工作清單開啟。
2. 單擊**"新工作"**。

啟動"工作精靈"。按照精靈的說明進行操作。

步驟 1. 選取工作類型

選取 **Kaspersky Embedded Systems Security for Windows (4.1) → 變更應用程式元件**。

步驟 2. 變更應用程式元件的工作設定

選取將在使用者電腦上可用的應用程式元件。為工作配置進階設定（請參閱下表）。

步驟 3. 選取將要對其分配工作的裝置

選取將要執行工作的電腦。下列選項可用：

- 將工作分配給管理群組。在這種情況下，工作分配給先前建立的管理群組中包括的電腦。
- 選取管理伺服器在網路中偵測到的電腦：*未分配裝置*。特定裝置可包括管理群組中的裝置以及未配置裝置。
- 手動指定裝置位址或從清單中匯入位址。您可以指定您要將工作分配給的裝置的 NetBIOS 名稱、IP 位址和 IP 子網路。

步驟 4. 設定工作啟動排程

配置啟動工作的排程，例如，手動或在電腦空閒時。

步驟 5. 定義工作名稱

輸入工作的名稱，例如，“*新增應用程式控制元件*”。

步驟 6. 完成工作建立

結束精靈。如有必要，選中“**精靈完成時執行工作**”核取方塊。您可以在工作內容中監控工作進度。

如何在網頁主控台中變更應用程式元件集

1. 在網頁主控台的主視窗中，選擇**資產管理 → 工作**。
   工作清單開啟。
2. 單擊“**新增**”。

啟動“工作精靈”。按照精靈的說明進行操作。

步驟 1. 配置一般工作設定

配置一般工作設定：

1. 在“**應用程式**”下拉式清單中，選取“**Kaspersky Embedded Systems Security 4.1.0**”。
2. 在“**工作類型**”下拉式清單中，選取“**變更 Kaspersky Embedded Systems Security 元件**”。
3. 在“**工作名稱**”欄位中，輸入簡要說明，例如，“*新增應用程式控制元件*”。
4. 在“**要將工作指派給的裝置**”塊中，選取工作範圍。

步驟 2. 選取將要對其分配工作的裝置

選取將要執行工作的電腦。例如，選取單獨的管理群組或構建一個選項。

步驟 3. 完成工作建立

1. 選擇 **建立完成時開啟工作詳情** 核取方塊並完成精靈。
2. 在工作內容中，選取“**應用程式設定**”區域。
3. 選取將在使用者電腦上可用的應用程式元件。為工作配置進階設定（請參閱下表）。

結果，使用者電腦上的 Kaspersky Embedded Systems Security 元件集將在靜默模式下變更。

參數	描述
受信任區域	對於*變更應用程式元件*工作，您只能將掃描排除項和受信任應用程式新增至受信任區域。
設定用於修改應用程式元件集的密碼	管理員通常啟用密碼防護以限制對 Kaspersky Embedded Systems Security 的存取。也就是說，要修改應用程式元件的選擇，您必須輸入具有**移除/修改/還原應用程式**權限的使用者認證。例如，您可以使用 KLAdmin 帳戶。
檢查不相容的協力廠商應用程式	預設情況下，Kaspersky Embedded Systems Security 檢查已安裝應用程式的相容性。分發套件中包含的incompatible.txt檔案提供了不相容軟體清單。如果啟用了不相容軟體檢查，Kaspersky Embedded Systems Security 會在偵測到清單中的應用程式時停止工作。如果協力廠商軟體的供應商文件聲稱與 Endpoint Protection Platform （ EPP ）相容，您可以停用掃描已安裝的軟體。
移除不相容的協力廠商應用程式	變更元件集之前，自動從incompatible.txt清單中移除應用程式。如果啟用此功能，Kaspersky Embedded Systems Security 會嘗試移除可能導致相容性問題的應用程式，以便繼續工作。預設啟用該選項。

透過 Active Directory 群組政策安裝和解除安裝應用程式

本部分介紹如何透過 Active Directory 群組政策安裝和解除安裝 Kaspersky Embedded Systems Security，以及透過群組政策安裝 Kaspersky Embedded Systems Security 後必須執行的動作相關資訊。

透過 Active Directory 群組政策安裝 Kaspersky Embedded Systems Security

您可以透過 Active Directory 群組政策在多台受防護裝置上安裝 Kaspersky Embedded Systems Security。您可以用相同的方式安裝應用程式主控台。

要安裝 Kaspersky Embedded Systems Security 或應用程式主控台的受防護裝置必須在同一個網域中和一個組織單元中。

要使用政策安裝 Kaspersky Embedded Systems Security 的受防護裝置的作業系統必須為相同的位數（ 32 位元或 64 位元 ）。

您必須有該網域的管理員權限。

若要安裝 Kaspersky Embedded Systems Security，請使用 ess_win.msi 安裝套件。要安裝應用程式主控台，請使用 esstools.msi 安裝套件。

有關使用 Active Directory 群組政策的詳細資訊，提供在 Microsoft 提供的文件中。

若要安裝 Kaspersky Embedded Systems Security 或應用程式主控台：

1. 將 ess_win.msi 儲存到網域控制器的共用資料夾。
2. 將金鑰檔案儲存在網域控制器上的同一公共資料夾中。
3. 在網域控制器上的相同共用資料夾中，建立包含下列行的 install_props.json 檔案。這表示，您同意最終使用者產品授權協議和隱私權政策的條款。

```
{
"EULA": "1",
```

```
"PRIVACYPOLICY": "1"
}
```

4. 在網域控制器上，為受防護裝置所屬的群組建立新政策。
5. 使用"**群組政策物件編輯器**"，在"**電腦設定**"節點中建立新的安裝套件。以 UNC 格式（通用命名慣例）指定 Kaspersky Embedded Systems Security（或應用程式主控台） msi 檔案的路徑。
6. 在「**電腦設定**」節點和所選群組的「**使用者設定**」節點中，都選中 Windows Installer 的「**永遠以較高的權限安裝**」核取方塊。
7. 使用 `gpupdate / force` 指令採納變更。

Kaspersky Embedded Systems Security 將在該群組的受防護裝置重新啟動後安裝到這些裝置上。

在安裝 Kaspersky Embedded Systems Security 後執行的操作

在受防護裝置上安裝 Kaspersky Embedded Systems Security 後，建議您立即更新應用程式資料庫並執行關鍵區域掃描。您可以從應用程式主控台執行這些操作。

您還可以配置有關 Kaspersky Embedded Systems Security 事件的管理員通知。

透過 Active Directory 群組政策移除 Kaspersky Embedded Systems Security

移除 Kaspersky Embedded Systems Security 時不會刪除 Dump 和偵錯檔案。您可以手動刪除在配置 Dump 和偵錯檔案寫入期間指定的資料夾中的 Dump 和偵錯檔案。

如果在受防護裝置群組中使用了 Active Directory 群組政策安裝 Kaspersky Embedded Systems Security（或應用程式主控台），則可以使用該政策移除 Kaspersky Embedded Systems Security（或應用程式主控台）。

您可以僅使用預設的移除參數來移除應用程式。

有關使用 Active Directory 群組政策的詳細資訊，提供在 Microsoft 提供的文件中。

如果應用程式管理受密碼防護，則無法使用 Active Directory 群組政策移除 Kaspersky Embedded Systems Security。

要移除 Kaspersky Embedded Systems Security（或應用程式主控台）：

1. 在網域控制器上，從要移除 Kaspersky Embedded Systems Security 或應用程式主控台的受防護裝置中選擇組織單元。
2. 在"**群組政策編輯器**"中選擇為安裝 Kaspersky Embedded Systems Security 所建立的政策，在"**軟體安裝**"節點（"**電腦配置** > **軟體設定** > **軟體安裝**"）中開啟 Kaspersky Embedded Systems Security（或應用程式主控台）安裝套件的內容功能表，然後選擇"**所有工作** > **刪除**"指令。

3. 選擇移除方法“**立即從使用者處和電腦中移除軟體**”。

4. 使用 `gpupdate /force` 指令採納變更。

受防護裝置重新啟動並登入 Microsoft Windows 前，就會從受防護裝置上移除 Kaspersky Embedded Systems Security。

Kaspersky Embedded Systems Security 安裝和移除記錄

如果使用安裝（解除安裝）精靈安裝（解除安裝）Kaspersky Embedded Systems Security 或應用程式主控台，Windows Installer 服務會建立安裝（解除安裝）記錄。一個名為 kl-install-<uid>.log（其中 <uid> 是唯一的 8 個字元記錄識別碼）的記錄檔案將儲存在用於啟動 setup_ess.exe 或者 setup_esstool.exe file 檔案的帳戶所屬使用者的 %temp% 資料夾中。

預設情況下，若您是從命令列安裝或移除 Kaspersky Embedded Systems Security，就不會建立該安裝記錄檔案。

要安裝 Kaspersky Embedded Systems Security 並在磁碟 C:\ 上建立記錄檔案，請執行以下命令：

```
msiexec /i ess_win.msi /l*v C:\<log_name>.log /qn EULA=1 PRIVACYPOLICY=1
```

Kaspersky Embedded Systems Security 安裝後的系統變更

當 Kaspersky Embedded Systems Security 和 Kaspersky Embedded Systems Security 主控台同時安裝時，Windows Installer 服務將對受防護裝置進行以下變更：

- 在受防護裝置與安裝了應用程式主控台的裝置上建立 Kaspersky Embedded Systems Security 資料夾。
- 註冊 Kaspersky Embedded Systems Security 服務。
- 建立一個 Kaspersky Embedded Systems Security 使用者群組。
- 在系統登錄檔中註冊 Kaspersky Embedded Systems Security 項。
- 已建立 Windows 工作排程器中顯示的 Kaspersky Embedded Systems Security 作業系統升級偵測系統工作。

下文介紹了這些變更。

受防護裝置上的 Kaspersky Embedded Systems Security 資料夾

安裝 Kaspersky Embedded Systems Security 後，受防護裝置上會建立以下資料夾：

- Kaspersky Embedded Systems Security 預設安裝資料夾包含 Kaspersky Embedded Systems Security 可執行檔。預設使用以下安裝資料夾：

  %ProgramFiles%\Kaspersky Lab\Kaspersky Embedded Systems Security.4.1.0

- 管理資訊庫 (MIB) 檔案，其中包含 Kaspersky Embedded Systems Security 透過 SNMP 通訊協定發佈的計數器與掛鉤說明：

  %ProgramFiles%\Kaspersky Lab\Kaspersky Embedded Systems Security.4.1.0\mibs

- Kaspersky Embedded Systems Security 服務檔案：

  - %ProgramData%\Kaspersky Lab\KESS.4.1\Data
  - %ProgramData%\Kaspersky Lab\KESS.4.1\Settings
  - %ProgramData%\Kaspersky Lab\KESS.4.1\Dskm

- 具有更新來源設定的檔案：

  %ProgramData%\Kaspersky Lab\KESS.4.1\Data

- 使用「*更新*」工作下載的資料庫和軟體模組更新（在第一次使用「*更新*」工作下載更新時會建立此資料夾）。

  %ProgramData%\Kaspersky Lab\KESS.4.1\Update distribution

- 工作記錄和系統稽核記錄：

  %ProgramData%\Kaspersky Lab\KESS.4.1\Reports

- 目前使用的資料庫集：

  %ProgramData%\Kaspersky Lab\KESS.4.1\Bases

- 資料庫的備份副本；每次更新資料庫時將會覆寫這些副本：

  %ProgramData%\Kaspersky Lab\KESS.4.1\QB

- 執行更新工作時所建立的暫存檔：

  %ProgramData%\Kaspersky Lab\KESS.4.1\Data\temp\temporaryFolder

- 隔離的物件（預設資料夾）：

  %ProgramData%\Kaspersky Lab\KESS.4.1\QB

- 備份中的物件（預設資料夾）：

  %ProgramData%\Kaspersky Lab\KESS.4.1\QB

- 從備份和隔離還原的物件（用於還原物件的預設資料夾）：

  %ProgramData%\Kaspersky Lab\KESS.4.1\QB\Restored

在應用程式主控台安裝過程中建立的資料夾

應用程式主控台的預設安裝資料夾取決於作業系統位集。預設使用以下安裝資料夾：

%ProgramFiles%\Kaspersky Lab\Kaspersky Embedded Systems Security Console 4.1.0

Kaspersky Embedded Systems Security 服務

以下 Kaspersky Embedded Systems Security 服務以 SYSTEM 帳戶執行：

- Kaspersky Embedded Systems Security 服務 (AVP.KESS.4.1)。Kaspersky Embedded Systems Security 的主系統服務，防護裝置抵禦病毒和其他威脅。
- Kaspersky Embedded Systems Security 並列服務 (AVP.KESS.4.1.SbS)。系統服務，可在 Kaspersky Embedded Systems Security 更新、還原或者經歷元件變更時防護裝置。
- Kaspersky Seamless Update Service (avpsus.KESS.4.1)。系統服務，可以安裝和回溯應用程式模組的重大更新和批准的更新。
- Kaspersky Embedded Systems Security 遠端控制服務 (avpcos.KESS.4.1)。用於從應用程式主控台遠端重新啟動和停止 Kaspersky Embedded Systems Security 服務的系統服務。

Kaspersky Embedded Systems Security 群組

ESS 管理員是受防護裝置上的群組，其成員對所有 Kaspersky Embedded Systems Security 功能擁有完整存取權限。

系統登錄註冊參數

安裝 Kaspersky Embedded Systems Security 後，將建立以下系統登錄機碼：

- Kaspersky Embedded Systems Security 設定：

  [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\AVP.ESS.4.1]
- Kaspersky Embedded Systems Security 事件記錄設定（Kaspersky 事件記錄）：

  [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Eventlog\Kaspersky Embedded Systems Security]
- 偵錯檔案設定：

  [HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\KasperskyLab\protected\KESS.4.1\Trace]
- 應用程式工作和功能的設定：

  [HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\KasperskyLab\protected\KESS.4.1\environment]

Kaspersky Embedded Systems Security 作業系統升級偵測系統工作

Windows Installer 服務在應用程式安裝期間會建立「Kaspersky Embedded Systems Security OS Upgrade Detect」工作。該工作在建立後立即啟動，之後在每次作業系統啟動時啟動。該工作檢查應用程式使用的驅動程式版本：如果更新了作業系統版本，則應用程式會更新對應作業系統版本的驅動程式。

該工作不會影響應用程式，可以刪除。我們建議牢記作業系統升級情境。

Windows 防火牆規則

根據指定的安裝設定，可在受保護的裝置上建立下表所述、允許傳入連線的 Windows 防火牆規則。

Windows 防火牆規則

規則名稱	規則描述	規則建立條件
AVP.KESS.4.1	允許可執行檔 avp.exe 的規則。	一律建立。
AVP.KESS.4.1 遠端 UI 連線	允許 TCP 連接埠 13032 的規則。	使用 `ADDWFEXCLUSION=1` 參數安裝應用程式。
AVP.KESS.4.1 遠端 UI 連線	允許 TCP 連接埠 13031 的規則。 預設會使用此連接埠號碼。您可以透過指定 `UIKLPORT=<port>` 參數來變更連接埠號。在此情況下，應用程式將為指定的連接埠號碼建立規則。	使用 `ADDWFEXCLUSION=1` 和 `UIKLPORT=13031` 參數安裝應用程式。如果傳遞 `ENABLEUIKLPORT=0` 參數，則不會建立規則

Kaspersky Embedded Systems Security 處理程序

Kaspersky Embedded Systems Security 將啟動下表中敘述的處理程序。

Kaspersky Embedded Systems Security 處理程序

檔案名稱	用途
avp.exe	Kaspersky Embedded Systems Security 工作流
avpsus.exe	此處理程序可以安裝和回溯關鍵且已批准的應用程式模組更新。

檢查 Kaspersky Embedded Systems Security 功能。使用 EICAR 測試病毒

本章節介紹 EICAR 測試病毒以及如何使用 EICAR 測試病毒檢查 Kaspersky Embedded Systems Security 的即時檔案防護和自訂掃描功能。

關於 EICAR 測試病毒

測試病毒的設計目的在於驗證防毒應用程式的運作功能。它由歐洲電腦防毒研究協會 (EICAR) 開發。

測試病毒不是惡意物件，不包含針對裝置的可執行程式碼。不過，大部分廠商的防毒應用程式可透過它來辨認威脅。

含有此測試病毒的檔案稱為 eicar.com。您可從 EICAR 網站下載此檔案。

在您將該檔案下載到裝置硬碟中的資料夾前，請確認已在該磁碟機上停用即時檔案防護。

eicar.com 檔案含有一行文字。掃描檔案時，Kaspersky Embedded Systems Security 會偵測到這行文字中有威脅等字，接著對檔案指派**"被感染"**狀態並刪除檔案。檔案中偵測到的威脅資訊將出現在應用程式主控台及工作記錄中。

您可以使用 eicar.com 檔案來檢查 Kaspersky Embedded Systems Security 如何解毒感染物件和如何偵測可能受感染物件。為此，使用文字編輯器開啟檔案，將下表中所列的前置詞之一新增至檔案中文字行的開頭，然後以新的名稱（例如 eicar_cure.com）儲存檔案。

為確保 Kaspersky Embedded Systems Security 處理帶有首碼的 eicar.com 檔案，在**"物件防護"**安全設定部分中，為 Kaspersky Embedded Systems Security 的"即時電腦防護"工作和"預設自訂掃描"工作設定**"所有物件"**值。

EICAR 檔案前置詞

前置詞	掃描後的檔案狀態及 Kaspersky Embedded Systems Security 操作
無前置詞	**Kaspersky Embedded Systems Security 會指派"被感染"狀態給物件並刪除物件。**
SUSP-	Kaspersky Embedded Systems Security 向啟發式分析偵測到的物件分配**"疑似被感染"**狀態並刪除它，因為不會解毒可能受感染物件。
WARN-	Kaspersky Embedded Systems Security 向物件（物件的程式碼與已知威脅的程式碼部分比對）分配**"疑似被感染"**狀態並刪除它，因為不會解毒可能受感染物件。
CURE-	Kaspersky Embedded Systems Security 會指派**"被感染"**狀態給物件並解毒物件。如果解毒成功，則檔案中整段文字將以 "CURE" 取代。

檢查即時檔案防護和自訂掃描功能

安裝 Kaspersky Embedded Systems Security 後，您可以確認 Kaspersky Embedded Systems Security 偵測到包含惡意程式碼的物件。為此，請使用 EICAR 測試病毒。

要檢查"即時檔案防護"功能：

1. 從 EICAR 網站 下載 eircar.com 檔案。將它儲存到網路上任一裝置的本機磁碟機上的共用資料夾中。

   在您將檔案儲存到資料夾前，請確認已停用該資料夾的即時檔案防護設定。

2. 如果要檢查網路使用者通知是否正常工作，請確保受防護裝置和儲存 eicar.com 檔案的裝置均啟用了 Microsoft Windows Messenger 服務。

3. 在受防護裝置上開啟應用程式主控台。

4. 使用以下其中一種方法，將儲存的 eicar.com 檔案複製到受防護裝置的本機磁碟上：

   - 若要透過"終端服務"視窗進行通知測試，請在使用遠端桌面連線實用程式連線到受防護裝置後，將 eicar.com 檔案複製到受防護裝置。

   - 若要透過"Microsoft Windows Messenger 服務"進行測試通知，請使用裝置的網路位置從您儲存 eicar.com 檔案的裝置複製它。

即時檔案防護只有在下列條件符合時才會運作：

- 受防護裝置上的 eicar.com 檔已刪除。

- 在應用程式主控台中，工作記錄取得*緊急*狀態。記錄有一個新行，其中包含關於 eicar.com 檔案中威脅的資訊。

- 您從中複製該檔案的裝置上會顯示以下 Microsoft Windows Messenger 服務訊息：Kaspersky Embedded Systems Security 已在 <事件發生時間> 封鎖對電腦 <裝置的網路名稱> 上的 <裝置上的檔案路徑>\eicar.com 的存取。原因：偵測到威脅。病毒名稱：EICAR-Test-File。使用者名稱：<使用者名稱>。電腦名稱：<從中複製該檔案的裝置的網路名稱>。

  在從中複製 eicar.com 檔案的裝置上，確保 Microsoft Windows Messenger Service 正在執行。

要檢查自訂掃描功能：

1. 從 EICAR 網站 下載 eircar.com 檔案。將它儲存到網路上任一裝置的本機磁碟機上的共用資料夾中。

   在您將檔案儲存到資料夾前，請確認已停用該資料夾的即時檔案防護設定。

2. 開啟應用程式主控台並展開應用程式主控台樹狀目錄中的**按需掃描**節點。

3. 選擇"**關鍵區域掃描**"子節點。

4. 將「**所有網路磁碟機**」新增到「按需掃描」工作的範圍。

5. 執行"關鍵區域掃描"工作。

自訂掃描只有在下列條件符合時才會運作：

- eicar.com 檔案已從裝置的硬碟磁碟機中刪除。

- 在應用程式主控台中，工作記錄取得*緊急*狀態。按需掃描工作記錄有一個新行，其中包含關於 eicar.com 檔案中威脅的資訊。

將舊版的 Kaspersky Embedded Systems Security 升級至版本 4.1

將舊版的 Kaspersky Embedded Systems Security 升級至 4.1 版時，請遵循以下建議：

- 提前規劃並排程升級。選擇伺服器在最輕負載下執行的時間，例如周末。
- 升級完成後，逐一開啟應用程式元件。即，例如，首先單獨啟用即時檔案防護元件，然後啟用其他防護元件，再啟用控制元件，依此類推。我們建議在每個步驟中測試該應用程式。
- 逐步進行升級。先升級單台電腦，然後升級多台電腦，最後升級組織的所有電腦。

升級過程的步驟

依下列順序將 Kaspersky Embedded Systems Security 升級至版本 4.1：

1. **升級卡巴斯基安全管理中心**

   將所有卡巴斯基安全管理中心元件升級到版本 14.2 或更高版本，包括使用者電腦和卡巴斯基安全管理中心網頁主控台上的網路代理。

2. **升級 Kaspersky Embedded Systems Security Web 外掛程式**

   在卡巴斯基安全管理中心網頁主控台中，將 Kaspersky Embedded Systems Security Web 外掛程式升級到 4.1 版本。

3. **遷移 Kaspersky Embedded Systems Security 工作與政策**

   遷移政策和工作後，您必須配置 遷移精靈無法遷移的設定，這在舊版本的應用程式中並不存在。我們還建議檢查遷移精靈是否正確遷移了所有設定。

4. **安裝 Kaspersky Embedded Systems Security 4.1**

   > Kaspersky Embedded Systems Security 4.1 版本使用 HTTPS 協定而非 DCOM 協定。因此，在安裝新版本的 Kaspersky Embedded Systems Security 之前，需要配置應用程式將在其上進行更新的裝置以啟用 KESS 服務的遠端啟動。如果不進行這樣的配置，遠端服務將無法啟動。

   您可以在刪除該應用程式的早期版本後或在其基礎上安裝 Kaspersky Embedded Systems Security 4.1。

   在舊版的應用程式上安裝時，將安裝同一組應用程式元件，同時考慮到 某些元件的新名稱和內容。

   遠端安裝時，安裝程式會安裝您在安裝套件的屬性中選擇的元件。

5. **如果有必要，啟動 Kaspersky Embedded Systems Security 4.1**

   在舊版的應用程式上安裝 Kaspersky Embedded Systems Security 4.1 時，目前產品授權將自動套用於該應用程式，並且新的應用程式元件和工作完全可用。產品授權期限保持不變。

6 確保應用程式正常工作

升級 Kaspersky Embedded Systems Security 後，請確保應用程式正常運作。確保應用程式沒有報告任何錯誤，還要檢查最後一次連線到管理伺服器的時間、最後一次更新的時間和電腦防護狀態。

注意排除清單、受信任的應用程式、裝置控制規則和應用程式啟動控制規則的遷移。

更新 Kaspersky Embedded Systems Security

版本 2.3、3.1 和更高版本支援升級到 Kaspersky Embedded Systems Security 4.1。若要從應用程式的更早版本更新，必須移除已安裝的版本並安裝版本 4.1。

更新執行方式是在已安裝的應用程式版本上安裝新版應用程式，不需要重新啟動電腦。

預設情況下，應用程式會根據現有應用程式安裝資料夾的路徑，以新應用程式版本的名稱建立新的安裝資料夾。您可以手動指定應用程式安裝資料夾的新路徑。

將 Kaspersky Embedded Systems Security 升級至版本 4.1 時，將會自動刪除先前安裝的應用程式版本。

更新受密碼防護的 Kaspersky Embedded Systems Security時，請透過以下方式之一將密碼傳遞至安裝程式：

- 如果透過安裝精靈介面或互動式 CLI 模式進行本機安裝，請在請求時指定密碼。
- 如果在非互動式 CLI 模式下進行本機安裝，請在 `UNLOCK_PASSWORD` 參數中指定密碼。
- 如果使用 Active Directory 群組政策安裝應用程式，請在 install_props.json 設定檔中使用`UNLOCK_PASSWORD`的值。

當您透過卡巴斯基安全管理中心遠端升級的應用程式受密碼防護時，您必須先使用卡巴斯基安全管理中心政策停用密碼防護。

更新應用程式時，目前產品授權將自動套用至 Kaspersky Embedded Systems Security 版本 4.1，並且完全可以使用新的應用程式元件和工作。產品授權期限保持不變。

如果使用過期的產品授權更新應用程式，則新版應用程式在安裝後將以有限功能模式執行（例如，應用程式資料庫更新無法使用）。

更新 Kaspersky Embedded Systems Security 管理工具

您可以將使用卡巴斯基安全管理中心將用來管理應用程式的管理外掛程式從 2.3、3.1、3.2、3.3、3.4 或更高版本更新至 4.1 版本。若要更新管理外掛程式和應用程式主控台的早期版本，必須刪除已安裝的版本，然後安裝 4.1 版。

更新期間，新版本的管理外掛程式將安裝在先前安裝的版本上，不需要重新啟動電腦。

有關遷移管理外掛程式設定的資訊，請參閱此 文章。

遷移政策和工作

您可以透過以下方式將應用程式先前版本的政策和工作設定遷移到 4.1 版本：

- 使用政策和工作批次轉換精靈（僅在卡巴斯基安全中心管理主控台中可用）。
- 使用 Kaspersky Embedded Systems Security 4.1 政策和工作遷移精靈（僅在卡巴斯基安全管理中心網頁主控台中可用）。

建議先在單台電腦上開始遷移 Kaspersky Endpoint Security 的政策和工作，然後在一組電腦上執行，然後在組織的所有電腦上完成遷移。

如何使用政策和工作批量轉換精靈遷移政策和工作設定

1. 在卡巴斯基安全管理中心管理主控台中，選擇管理伺服器並按滑鼠右鍵開啟上下文功能表。
2. 選擇"**所有工作 → 政策和工作批量轉換精靈**"。

   這將啟動政策和工作批量轉換精靈。按照精靈的說明進行操作。

步驟 1. 選擇需要為其轉換政策和工作的應用程式

選擇 Kaspersky Embedded Systems Security 4.1。前往下一步。

步驟 2. 轉換政策

選擇要為 Kaspersky Embedded Systems Security 4.1 建立的要升級的應用程式版本的政策。前往下一步。

步驟 3. 轉換工作

選擇要為 Kaspersky Embedded Systems Security 4.1 建立的要升級的應用程式版本的工作。

目前步驟中不會顯示非群組工作（指派給單一裝置的工作）。

若要將非群組工作從您的應用程式版本轉換為 Kaspersky Embedded Systems Security 4.1：

1. 單擊"**下一步**"。

   開啟"**額外遷移排程和非群組工作**"視窗。
2. 選擇"**遷移非群組工作**"核取方塊。

3. 指定卡巴斯基安全管理中心管理伺服器的連線設定。

4. 單擊**"確定"**。

步驟 4. 精靈完成

結束精靈。結果，精靈將執行以下操作：

- Kaspersky Embedded Systems Security 4.1 的新政策已建立。

  新政策包含所選 Kaspersky Embedded Systems Security 政策的設定以及 Kaspersky Embedded Systems Security 4.1 中引入的新設定。新政策的名稱與轉換前的 Kaspersky Embedded Systems Security 政策的名稱相同，但新增了"（已轉換）"。新政策的狀態為*停用政策*。

- Kaspersky Embedded Systems Security 4.1 的新工作已建立。

  新工作包含所選 Kaspersky Embedded Systems Security 工作的設定以及 Kaspersky Embedded Systems Security 4.1 中引入的新設定。新工作的名稱與轉換前的 Kaspersky Embedded Systems Security 工作名稱相同，但新增了"（轉換）"。

- 選擇用於轉換的政策和工作保持不變。

如何使用遷移精靈遷移政策和工作設定

在網頁主控台的主視窗中，選擇**操作 → 移轉到 KESS 4.1.0**。

這會執行政策和工作遷移精靈。按照精靈的說明進行操作。

步驟 1. 政策遷移

選擇您想要為 Kaspersky Embedded Systems Security 4.1 建立的 Kaspersky Embedded Systems Security 政策。前往下一步。

步驟 2. 工作遷移

在工作清單中，選擇要為 Kaspersky Embedded Systems Security 4.1 建立的 Kaspersky Embedded Systems Security 工作。前往下一步。

步驟 3. 精靈完成

結束精靈。結果，精靈將執行以下操作：

- Kaspersky Embedded Systems Security 4.1 的新政策已建立。

  新政策包含遷移的 Kaspersky Embedded Systems Security 政策的設定以及 Kaspersky Embedded Systems Security 4.1 中引入的新設定。新政策的名稱與合併前的 Kaspersky Embedded Systems Security 政策的名稱相同，新增了"從 KESS 複製"短語。新政策的狀態為*停用政策*。

- Kaspersky Embedded Systems Security 4.1 的新工作已建立。

  新工作包含遷移的 Kaspersky Embedded Systems Security 工作的設定以及 Kaspersky Embedded Systems Security 4.1 中引入的新設定。新工作的名稱與遷移先前的 Kaspersky Embedded Systems Security 工作的名稱相同，但新增了"從 KESS 複製"短語。

遷移正在更新的應用程式版本的設定

在將應用程式及其外掛程式升級到版本 4.1 之後，以下遷移保持不變：

- 元件和工作的設定（重設為預設值的設定和在"設定和元件遷移的限制"下列出的設定除外）
- 工作記錄和系統稽核記錄，以及 Windows 事件記錄中的記錄
- 工作通知設定
- 啟動工作的使用者帳戶
- 應用程式管理的使用者存取權限
- 代理伺服器連線密碼
- 屬性狀態

在將應用程式及其外掛程式升級到版本 4.1 之後，以下設定將重設或設定為新版應用程式的預設值：

- 所有計數器，包括病毒資料庫狀態
- 關於應用程式模組和病毒資料庫的已安裝更新的資料
- 工作狀態
- 管理 Kaspersky Embedded Systems Security 服務 的使用者存取權限
- 透過登錄檔設定的應用程式和工作設定
- 在安裝重大修復期間變更的應用程式和工作設定
- 事件配置
- 資料傳輸到卡巴斯基安全管理中心管理伺服器的設定：預設情況下，啟用所有資料的傳輸

- 偵錯和傾印設定
- 應用程式本機工作的設定，位於「**通知**」索引標籤上。

您正在更新的應用程式版本中不存在的設定將取得預設值。

設定和元件遷移的限制

- 正在升級的版本的隔離區內容將被移至 4.1 版本的備份中。同時，備份的最大大小被提升至 400 Mb，可用空間閾值被提升至 100 MB。
- Kaspersky Embedded Systems Security 版本 3.4 的以下設定在 Kaspersky Embedded Systems Security 4.0 或更高版本中不存在，因此沒有遷移：**隔離資料夾**、 **備份資料夾**和 **用於還原物件的資料夾**。同樣，舊版本中存在但新版本中不存在的其他設定也不會被遷移。
- 用戶端電腦的已封鎖網路工作階段清單不會遷移。同時，在應用程式升級後，自動取消封鎖存取已封鎖的網路檔案資源的設定保持不變。
- 密碼防護設定未遷移。在 Kaspersky Embedded Systems Security 4.0 中，密碼防護發生了重大變化。如有需要，開啟密碼防護並設定密碼。
- 受信任區域：
  - 在 Kaspersky Embedded Systems Security 4.1 中，選擇受信任區域物件的方法已經改變。可以遷移被定義為單個檔案或檔案或資料夾路徑的排除項目。被定義為預先定義範圍 (例如，硬碟) 或指令碼 URL 的排除項目不會被遷移。遷移後，您必須手動新增此類排除項目。
  - 有助於在伺服器上設定應用程式的預定義掃描排除項目和受信任的應用程式已新增至受信任區域。
- 應用程式啟動控制 和 裝置控制 元件已經過大幅修改。升級版本的元件設定在遷移時會考慮 Kaspersky Embedded Systems Security 4.1 中的新設定結構。這表示您可能需要在管理伺服器上提供更多空間來儲存應用程式設定。
- 正在升級的應用程式版本的檔案完整性監控和登錄檔存取監控元件的設定將會被遷移到系統完整性監控元件的設定中。
- 防火牆管理元件被修訂加入防火牆元件，它除了與 Windows 防火牆互動外，現在額外作為防火牆運作。完成遷移後，您必須 從頭開始 配置元件模式。
- 要使用 KSN，您必須再次閱讀並接受 KSN 聲明。
- 該應用程式的 4.0 及更高版本不支援排程單個元件。如果啟用這些元件，它們會在應用程式執行時繼續執行。
- 在遷移工作時，工作的預定開始時間會偏移與執行遷移的電腦的作業系統設定中配置的時區數相符的小時數。例如，假設舊版應用程式中工作的開始時間是 7:00，而作業系統配置的時區是 UTC+3:00。那麼，工作遷移後，開始時間會改為10:00。
- 即時檔案防護元件和按需掃描工作的設定中刪除了設定對可能被感染的物件執行操作的部分。這些設定不會遷移到新的應用程式版本。
- 如果在將應用程式版本從 3.4 或更早版本升級到 4.0 或更高版本後遷移了備份物件，則卡巴斯基安全管理中心網頁主控台或管理主控台無法被用來將備份物件傳送給卡巴斯基進行分析。

- 遷移按需掃描工作時，預定義掃描範圍的預設安全等級將從 *通知* 變更為 *自訂*。
- 如果在本機升級 Kaspersky Embedded Systems Security 時未安裝先前包含在安裝中的元件，則該元件的設定將不會保留。如果您隨後安裝此元件，則將對其套用預設設定。

Kaspersky Embedded Systems Security 3.4 和 4.1 版本中的元件和工作的對應關係

將 Kaspersky Embedded Systems Security 3.4 升級至 4.1 版本時，僅當應用程式在本機安裝時才會移轉元件和工作集合。

Kaspersky Embedded Systems Security 版本 3.4 和 4.1 中的元件對應關係

Kaspersky Embedded Systems Security 3.4 的元件	Kaspersky Embedded Systems Security 4.1 的元件
信任區域	受信任區域
即時檔案防護	即時檔案防護
KSN 使用	KSN 使用
弱點利用防禦	弱點利用防禦
AMSI 掃描器	AMSI 掃描程式
應用程式啟動控制	應用程式啟動控制
裝置控制	裝置控制
防火牆管理	防火牆 Windows 防火牆可作為 Kaspersky Embedded Systems Security 3.4 的防火牆，而應用程式則管理 Windows 防火牆。在 Kaspersky Embedded Systems Security 4.1 中，一個單獨的元件負責防火牆功能。
網路威脅防護	網路威脅防護
檔案完整性監控	系統完整性監控 檔案完整性監控 和 註冊表存取監控 元件的功能已合併至系統完整性監控元件。
記錄審查	記錄審查
登錄檔存取監控	系統完整性監控 檔案完整性監控 和 註冊表存取監控 元件的功能已合併至系統完整性監控元件。
（無）	行為偵測
（無）	修復引擎
Kaspersky Embedded Systems Security 3.4 的工作	**Kaspersky Embedded Systems Security 4.1 的工作**
啟動應用程式	應用程式啟動
複製更新	更新 "複製更新"工作的功能已合併到"更新"工作中。
基線檔案完整性監控	基於基線的系統完整性監控
資料庫更新	更新 "資料庫更新"工作的功能已合併到"更新"工作中。
軟體模組更新	更新 "軟體模組更新"工作的功能已合併到"更新"工作中。
應用程式資料庫更新回溯	更新回溯
按需掃描	按需掃描
應用程式完整性控制	應用程式完整性控制

Kaspersky Embedded Systems Security 3.4 的元件	Kaspersky Embedded Systems Security 4.1 的元件
應用程式啟動控制規則產生器	應用程式啟動控制規則產生器
裝置控制規則產生器	裝置控制規則產生器
（無）	管理伺服器連線防護
（無）	變更 Kaspersky Embedded Systems Security 元件
（無）	系統完整性狀態重設

應用程式介面

您可以使用以下介面控制 Kaspersky Embedded Systems Security：

- 應用程式主控台。
- 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管理主控台

卡巴斯基安全管理中心允許您遠端安裝和移除、啟動和停止 Kaspersky Embedded Systems Security、配置應用程式設定、變更可用應用程式元件集、新增金鑰以及啟動和停止工作。

該應用程式可以透過卡巴斯基安全管理中心使用 Kaspersky Embedded Systems Security 管理外掛程式進行管理。有關卡巴斯基安全管理中心介面的詳細資訊，請參見卡巴斯基安全管理中心說明。

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網頁主控台（以下簡稱「網頁主控台」）是一個網頁應用程式，用來集中執行主要工作以管理和維護組織網路的安全系統。卡巴斯基安全管理中心網頁主控台是提供使用者介面的卡巴斯基安全管理中心元件。有關卡巴斯基安全管理中心網頁主控台的詳細資訊，請參閱卡巴斯基安全管理中心說明。

網頁主控台可以執行下列操作：

- 監控組織安全系統的狀態。
- 在網路內的裝置上安裝 Kaspersky 應用程式。
- 管理已安裝的應用程式。
- 檢視有關安全系統狀態的報告。

使用管理外掛程式

本節提供有關 Kaspersky Embedded Systems Security 管理外掛程式的資訊，並介紹如何管理一台或一組受防護裝置上安裝的應用程式。

從卡巴斯基安全管理中心管理 Kaspersky Embedded Systems Security

透過 Kaspersky Embedded Systems Security 管理外掛程式，您可以集中管理多台已安裝 Kaspersky Embedded Systems Security 並加入管理群組的受防護裝置。卡巴斯基安全管理中心還可以單獨配置管理群組中包括的每台受防護裝置的設定。

*管理群組*透過卡巴斯基安全管理中心手動建立。「管理群組」在卡巴斯基安全管理中心中手動建立，包含您要為其設定相同的控制和防護設定的已安裝 Kaspersky Embedded Systems Security 的多個裝置。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。

如果 Kaspersky Embedded Systems Security 在某台受防護裝置上的執行受啟動卡巴斯基安全管理中心政策的控制，則該受防護裝置的應用程式設定無法使用。

在卡巴斯基安全管理中心中啟動 Kaspersky Embedded Systems Security 管理外掛程式無需執行額外的操作。在管理員的受防護裝置上安裝管理外掛程式後，這會與任何類型的卡巴斯基安全管理中心管理主控台一起啟動。

可透過以下方式透過卡巴斯基安全管理中心管理 Kaspersky Embedded Systems Security：

- **使用卡巴斯基安全管理中心政策**。可使用卡巴斯基安全管理中心政策為一組裝置遠端設定相同的防護設定。在活动政策中指定的工作設定的优先级高于在应用程序主控台中本地配置或在卡巴斯基安全管理中心的"**属性：<受保护设备名称>**"視窗中遠端配置的工作設定。

  政策可用於設定一般應用程式設定、即時電腦防護工作的設定、裝置上的活動控制工作、網路儲存防護工作以及按排程啟動本機系統工作的設定。

- **使用卡巴斯基安全管理中心群組工作**。使用卡巴斯基安全管理中心群組工作可遠端設定工作的通用設定，一組裝置具有過期期限。

  您可使用群組工作來啟動應用程式，設定「自訂掃描」工作設定、「更新」工作設定，以及「應用程式啟動控制規則產生器」工作設定。

- **使用一組裝置的工作**。使用一組裝置的工作允許遠端配置通用工作設定，不屬於任何管理群組的受防護裝置具有的有限執行期限。

- **使用單個裝置的內容視窗**。在**屬性：<受防護裝置名稱>**視窗中，您可遠端配置管理群組中包含的個別受防護裝置的工作設定。如果選取受防護裝置不受啟動卡巴斯基安全管理中心政策的控制，您也可以配置一般應用程式設定和所有 Kaspersky Embedded Systems Security 工作的設定。

管理應用程式設定

本部分包含有關在卡巴斯基安全管理中心管理主控台中配置 Kaspersky Embedded Systems Security 一般設定的資訊。

在卡巴斯基安全管理中心中設定一般應用程式設定

您可以透過卡巴斯基安全管理中心為一組受防護裝置或一台受防護裝置配置 Kaspersky Embedded Systems Security 一般設定。

在卡巴斯基安全管理中心中配置介面和掃描設定

要配置延伸性設定和應用程式介面：

1. 展開卡巴斯基安全管理中心管理主控台樹狀目錄中的**受管理裝置**節點。
2. 選擇要為其配置應用程式設定的管理群組。
3. 在選定的管理群組的詳情視窗中執行以下之一操作：
   - 要為一組受防護裝置配置應用程式設定，請選擇**政策**頁簽，然後開啟"**內容：<政策名稱>**"視窗。
   - 若要為個別受防護裝置設定工作或應用程式的設定，請選擇**裝置**頁簽並前往本機工作設定或應用程式設定。
4. 在 **應用程式設定** 部分，點擊**介面設定** 子部分中的 **設定** 按鈕。
5. 在 **介面設定** 視窗中的 **一般** 頁簽上，配置以下設定：
   - 在"**使用者互動**"部分中，配置在每個應用程式啟動後，系統托盤圖示是否將顯示在工作列中。
     - **顯示使用者介面**在用戶端電腦上，Windows 托盤中有一個圖示。在該圖示的內容功能表中，使用者可以使用 Kaspersky Embedded Systems Security 執行操作。Kaspersky Embedded Systems Security 還會在應用程式圖示上方顯示通知。Windows 系統匣中圖示的上下文功能表可讓您開啟小型診斷視窗。點擊小型診斷視窗中的連結即可開啟應用程式主控台。
     - **不顯示使用者介面**在用戶端電腦上，不顯示 Kaspersky Embedded Systems Security 操作的跡象。Windows 通知區域中的圖示和通知不可用。
   - 在 **狀態** 部分，您可以指定希望在 Kaspersky Embedded Systems Security 系統匣圖示上看到哪些警告。
6. 點擊**OK**。

將儲存設定的應用程式設定。

在卡巴斯基安全管理中心中配置安全性設定

要手動配置安全設定：

1. 展開卡巴斯基安全管理中心管理主控台樹狀目錄中的**受管理裝置**節點。
2. 選擇要為其配置應用程式設定的管理群組。
3. 在選定的管理群組的詳情視窗中執行以下之一操作：
   - 要為一組受防護裝置配置應用程式設定，請選擇**政策**頁簽，然後開啟"**內容：<政策名稱>**"視窗。
   - 若要為個別受防護裝置設定工作或應用程式的設定，請選擇**裝置**頁簽並前往本機工作設定或應用程式設定。
4. 在 **應用程式設定** 部分，點擊**安全性和可靠性** 子部分中的 **設定** 按鈕。
5. 在 **安全設定** 視窗中的 **安全** 頁簽上，配置以下設定：
   - 在 **一般** 部分，我們建議保留 **在電腦啟動時啟動應用程式（建議）** 啟用（預設）。
   - 在 **自我防護** 部分，啟用或停用 **防護應用程式處理程序抵禦外部威脅** 功能。
   - 在"**切換到 UPS 備份電源時的動作**"部分，指定在轉換為 UPS 備份電源後 Kaspersky Embedded Systems Security 對受防護裝置產生的負荷的限制：
     - **不啟動排程的掃描工作**
     - **停止正在執行的掃描工作**
   - 在 **套用設定時的電腦狀態** 部分，配置當套用政策或執行工作發生錯誤時安裝有應用程式的用戶端電腦的狀態顯示。
   - 在"**相容性設定**"部分中，配置**與遠端管理軟體相容**設定。
6. 在**掃描設定**頁籤上，配置以下設定：
   - **限制掃描工作的 CPU 使用**Kaspersky Embedded Systems Security 在自訂掃描工作期間將其對受防護裝置 CPU 的使用限制為**上限**欄位中指定的值。啟用此選項可能會對 Kaspersky Embedded Systems Security 的效能產生負面影響。
   - **將資源讓給其他應用程式**Kaspersky Embedded Systems Security 掃描電腦時消耗的電腦資源可能會增加 CPU 和硬碟磁碟機子系統的負載。這可能減緩其他應用程式的速度。為了最佳化效能，Kaspersky Embedded Systems Security 提供了一種將資源傳輸到其他應用程式的模式。在此模式中，當 CPU 負載過高時，作業系統可降低 Kaspersky Embedded Systems Security 掃描工作執行緒的優先順序。這可允許重新分配作業系統資源到其他應用程式。因此，掃描工作將收到更少的 CPU 時間。結果，Kaspersky Embedded Systems Security 將花更多時間來掃描電腦。預設情況下，應用程式已設定為允許其他應用程式使用資源。
7. 單擊"**確定**"。

將儲存延伸性和可靠性設定。

使用卡巴斯基安全管理中心配置連線設定

設定的連線設定用於將 Kaspersky Embedded Systems Security 連線到更新和啟動伺服器，以及在將應用程式與卡巴斯基安全網路服務整合期間使用。

若要設定連線設定，請執行以下步驟：

1. 展開卡巴斯基安全管理中心管理主控台樹狀目錄中的**受管理裝置**節點。
2. 選擇要為其配置應用程式設定的管理群組。
3. 在選定的管理群組的詳情視窗中執行以下之一操作：
   - 要為一組受防護裝置配置應用程式設定，請選擇**政策**頁簽，然後開啟"**內容：<政策名稱>**"視窗。
   - 若要為個別受防護裝置設定工作或應用程式的設定，請選擇**裝置**頁簽並前往本機工作設定或應用程式設定。
4. 在 **應用程式設定** 部分，點擊**連線設定** 子部分中的 **設定** 按鈕。
   開啟"**連線設定**"視窗。
5. 在"**代理伺服器**"區域中點擊"**設定**"。
6. 這將開啟一個視窗；在此視窗的 **代理伺服器設定** 部分中選擇一個代理設定管理選項：
   - **不使用代理伺服器**如果選擇此選項，Kaspersky Embedded Systems Security 將不使用代理伺服器。
   - **自動偵測代理伺服器設定。** 如果選擇此選項，Kaspersky Embedded Systems Security 將使用作業系統的代理設定。
   - **使用指定的代理伺服器設定**如果選擇此選項，Kaspersky Embedded Systems Security 會使用手動指定的代理伺服器設定。輸入代理伺服器和埠號的 IP 位址或符號名稱
     如有必要，清除"**本機位址略過代理伺服器**"核取方塊。如果啟用此功能，則會直接透過託管已安裝了 Kaspersky Embedded Systems Security 的受防護裝置的網路存取裝置。預設啟用該選項。
7. 在 **代理伺服器身分驗證設定** 部分的下拉清單中，選擇代理伺服器的身分驗證方法：
   a. 如果您選擇 **自動偵測代理伺服器設定**：
      - **不使用身分驗證**
      - **NTLM 身分驗證**使用目前使用者帳戶進行 NTLM 身分驗證（預設）。
      - **Kerberos 身分驗證**使用目前使用者帳戶進行 Kerberos 身分驗證。
   b. 如果您選擇 **使用指定的代理伺服器設定**：
      - **不使用身分驗證**
      - **NTLM 身分驗證**使用目前使用者帳戶進行 NTLM 身分驗證（預設）。
      - **使用使用者名稱和密碼進行 NTLM 身分驗證**使用手動指定的憑據進行 NTLM 身分驗證。

- **Kerberos 身分驗證**使用目前使用者帳戶進行 Kerberos 身分驗證。

  若要確保在使用 CNAME 記錄作為代理伺服器位址時 Kerberos 身分驗證正常運作，您必須為每個 CNAME 記錄註冊一個服務主體名稱 (SPN)。

- **使用使用者名稱和密碼進行 Kerberos 身分驗證**使用手動指定的憑據進行 Kerberos 身分驗證。
- **使用者名稱和密碼**使用手動指定的憑據進行身分驗證。

必要時輸入使用者名稱和密碼。

如果選擇 Kerberos 驗證，Kaspersky Embedded Systems Security 可以根據代理伺服器設定使用 Kerberos 或 NTLM 協定執行身分驗證。

8. 在"**產品授權**"部分，選擇或者清除"**啟動應用程式時將卡巴斯基安全管理中心作為代理伺服器**"核取方塊。
9. 單擊"**確定**"。
10. 在 **監控的連接埠** 部分，指定網路連接埠選項：
    - **監控所有網路連接埠**在此網路連接埠監控模式下，防護元件會監控透過任何開放的電腦網路連接埠傳輸的資料流。
    - **僅監控選定網路連接埠**在此網路連接埠監視模式下，防護元件將監控電腦的選定連接埠和選定應用程式的網路活動。通常用於傳輸電子郵件和網路流量的網路連接埠的清單按照 Kaspersky 專家的建議進行配置。如有必要，您可以編輯網路連接埠清單。
11. 點擊**設定**按鈕並編輯以下設定：
    - **監控卡巴斯基建議的清單中的應用程式的所有連接埠**Kaspersky Embedded Systems Security 會監控預先定義清單中應用程式的網路連接埠。例如，此清單包括 Google Chrome、Adobe Reader、Java 和其他應用程式。
    - **監控指定應用程式的所有連接埠**Kaspersky Embedded Systems Security 會監控新增至清單中的應用程式的網路連接埠。
12. 單擊"**確定**"。

將儲存設定的連線設定。

設定本機工作執行模式

您可以使用政策來允許或阻止本機系統隨需掃描工作和更新工作的啟動。這會根據在管理群組中每個受防護裝置上本機配置的排程完成：

- 如果特定類型的本機系統工作的排程啟動受到政策禁止，則這些工作將不會按照排程在受防護裝置上執行。您可以手動啟動該本機系統工作。
- 如果特定類型的本機系統工作的排程啟動被政策允許，則這些工作將按照為此工作進行的本機配置的排程參數來執行。

預設情況下，政策會禁止本機系統工作的啟動。

如果更新或自訂掃描受卡巴斯基安全管理中心群組工作的管理，我們建議不要允許本機系統工作啟動。

如果不使用群組更新或自訂掃描工作，則在政策中允許本機系統工作啟動：Kaspersky Embedded Systems Security 將執行應用程式資料庫和模組更新，並根據預設排程啟動所有本機系統的自訂掃描工作。

您可使用政策允許或封鎖以下本機系統工作的排程啟動：

- 自訂掃描工作：*關鍵區域掃描*、*作業係統啟動時掃描*、*應用程式完整性控制*、*基於基線的系統完整性監控*。
- 更新工作：*資料庫和應用程式模組更新*、*應用程式更新*。

如果受防護裝置從管理群組中排除，則本機系統工作排程將自動啟用。

若要在政策中允許或阻止應用程式本機工作的啟動排程管理：

1. 在卡巴斯基安全管理中心管理主控台樹中，展開 **受管理裝置** 節點，展開相關群組，然後在結果窗格中選擇 **政策** 頁簽。
2. 在**政策**頁籤上，在用來排程受防護裝置群組上 Kaspersky Embedded Systems Security 本機系統工作啟動的政策右鍵選單中，選取**內容**。
3. 在政策內容視窗中，選取「**應用程式設定**」區域。
4. 在 **執行本機系統工作** 子部分中點擊 **設定**。
5. 選擇 **允許使用本機工作** 核取方塊。
6. 使用 **允許排程管理** 核取方塊以允許或阻止應用程式本機工作的啟動排程管理。

在卡巴斯基安全管理中心中配置備份設定

在卡巴斯基安全管理中心中管理一般備份設定：

1. 展開卡巴斯基安全管理中心管理主控台樹狀目錄中的**受管理裝置**節點。
2. 選擇要為其配置應用程式設定的管理群組。
3. 在選定的管理群組的詳情視窗中執行以下之一操作：
   - 要為一組受防護裝置配置應用程式設定，請選擇**政策**頁簽，然後開啟"**內容：<政策名稱>**"視窗。
   - 若要為個別受防護裝置設定工作或應用程式的設定，請選擇**裝置**頁簽並前往本機工作設定或應用程式設定。
4. 轉到"**補充**"區域。
5. 在**儲存**子區域中，按一下**設定**按鈕。

6. 按下表所述配置設定。

儲存設定

參數	描述
在 **報告** 頁簽上，指定報告設定：	
儲存報告不超過	如果選中該核取方塊，則最大報告儲存期限制為定義的時間隔。預設的報告最長儲存期限是 30 天。在此時間之後，Kaspersky Embedded Systems Security 將自動移除報告檔案中的最早項目。
限制報告檔案的大小為	如果選中該核取方塊，則最大報告檔案大小限制為定義值。預設情況下，最大檔案大小資料為 1024 MB。要避免超過最大報告檔案容量，當達到最大報告檔案容量時，Kaspersky Embedded Systems Security 將自動刪除報告檔案中的最早項目。
在 **備份** 頁簽上，指定備份設定：	
儲存物件的時間不超過	如果選中該核取方塊，則最大檔案儲存期限制為定義的時間間隔。預設的檔案最長儲存期限是 30 天。最長儲存期限超出後，Kaspersky Embedded Systems Security 將刪除備份區中最舊的檔案。
備份大小限制為	如果選中該核取方塊，則最大儲存大小限制為定義值。預設情況下，最大大小為 400 MB。為避免超過最大儲存大小，當達到最大儲存大小時，Kaspersky Embedded Systems Security 將自動刪除儲存中的最早檔案。
可用空間的閾值	該核取方塊用於啟用或停用監控備份中的最小可用空間大小（預設值為 100 MB）的功能。如果可用空間大小下降到低於指定上限值，Kaspersky Embedded Systems Security 會記錄"*已超過備份區可用空間上限值*"事件，並根據此事件類型的通知設定發佈通知。 如果選中該核取方塊，Kaspersky Embedded Systems Security 會監控備份中的可用空間的大小。 如果選擇了**備份大小限制為**核取方塊，則 **可用空間的閾值** 核取方塊處於活動狀態。

建立和設定政策

本節提供有關使用卡巴斯基安全管理中心政策在多個受防護裝置上管理 Kaspersky Embedded Systems Security 的資訊。

可以建立全域性卡巴斯基安全管理中心政策，以便管理多個已安裝 Kaspersky Embedded Systems Security 的裝置上的防護。

政策在一個管理群組中所有受防護裝置上強制執行 Kaspersky Embedded Systems Security 設定、功能和指定的工作。

可以為一個管理群組依次建立和實行多個政策。目前對某個群組有效的政策在管理主控台中處於*啟動*狀態。

Kaspersky Embedded Systems Security 系統稽核記錄中記錄了有關政策實行情況的資訊。該資訊可在應用程式主控台的"**記錄審查**"節點中檢視。

卡巴斯基安全管理中心提供一種在受防護裝置上套用政策的方式：*禁止編輯設定*。套用政策後，Kaspersky Embedded Systems Security 會使用您在受防護裝置上的政策內容中指定的 **已禁止編輯** 所對應的設定值。在這種情況下，Kaspersky Embedded Systems Security 不會使用應用該政策之前有效的設定值。Kaspersky Embedded Systems Security 不會套用在政策內容中選擇的 **已允許編輯** 所對應的啟動政策設定值。

如果政策為啟動的，則政策中標記圖示的設定的值在應用程式主控台中顯示，但無法編輯。其他設定的值可以在應用程式主控台中編輯。

在啟動政策中設定且標記圖示的設定，也會在**屬性：<受防護裝置名稱>**視窗中為個別的受防護裝置封鎖卡巴斯基安全管理中心的變更。

在停用啟動政策後，使用啟動政策指定併傳送到受防護裝置的設定將儲存在本機工作設定中。

如果政策定義目前正在執行的即時電腦防護工作或者 Network-Attached Storages Protection 工作的設定，則該政策定義的設定將在套用該政策後立即變更。如果該工作未執行，就會在啟動時套用其設定。

建立政策

在建立政策之前，您需要安裝管理外掛程式 klcfginst.exe。

若要為安裝並執行應用程式的一組受防護裝置建立政策：

1. 展開卡巴斯基安全管理中心管理主控台樹狀目錄中的**"受管理裝置"**節點，然後選擇包含您希望為其建立政策的受防護裝置的管理群組。
2. 在選定管理群組的結果窗格中，選擇**政策**頁簽，然後點擊**新政策**連結以啟動"新政策精靈"。

   開啟**"新政策精靈"**視窗。
3. 在**選取您要為其建立群組政策的應用程式**視窗中，選取 Kaspersky Embedded Systems Security。
4. 單擊**"下一步"**。
5. 在**名稱**欄位中輸入群組政策名稱。

   政策名稱不能包含以下符號：`" * < : > ? \ |` 。
6. 要套用以前版本的應用程式中使用的政策配置：
   a. 選擇**"使用早期版本應用程式的政策設定"**核取方塊。
   b. 點擊**"瀏覽"**。
   c. 選擇要套用的政策。
   d. 單擊**"下一步"**。
7. 在 **選擇操作類型** 視窗的 **配置即時檔案防護** 塊中，選擇 **啟用即時檔案防護** 核取方塊並指定安全等級。

   如果未選擇工作執行模式，則無法繼續執行新建政策精靈的下一步。
8. 配置即時電腦防護。
9. 配置掃描排除項目和受信任應用程式。
10. 在**建立新的應用程式群組政策**視窗中選擇以下政策狀態之一：

    - **啟用政策**，如果您希望在建立政策後立即套用該政策。如果群組中已經存在啟動政策，則會將其停用並套用新政策。
    - **停用政策**，如果您不希望立即套用所建立的政策。在此情況下，可在之後啟動該政策。

- **漫遊政策**，該政策將在電腦離開組織網路邊緣時啟動。

- 選擇 **建立政策後立即開啟內容** 核取方塊自動關閉 **新政策精靈**，然後在點擊**下一步**按鈕後配置新建立的政策。

11. 單擊**"完成"**。

所建立的政策將顯示在選定管理群組的**政策**頁簽的政策清單中。在**"內容：<政策名稱>"**視窗中，您可配置 Kaspersky Embedded Systems Security 的其他設定、工作和功能。

建立新政策後，會建立一組允許規則，防止應用程式遭到封鎖，確保應用程式不間斷地操作。

預設情況下，Kaspersky Embedded Systems Security 會在建立新政策時為傳入網路流量建立一組規則：

- 使用卡巴斯基安全管理中心網路代理程式共用 Windows 桌面之流程的兩個允許規則，這位於 %Program Files% 和 %Program Files (x86)% 資料夾中。狀態：已啟用。允許的外部位址：所有。通訊協定：TCP 和 UDP，每個通訊協定一條規則。

- 本機連接埠 15000 的兩個允許規則。狀態：已啟用。允許的外部位址：所有。通訊協定：TCP 和 UDP，每個通訊協定一條規則。

預設情況下，Kaspersky Embedded Systems Security 會在建立新政策時建立一組傳出網路流量規則：

- Kaspersky Embedded Systems Security 服務的兩個允許規則，這位於 %Program Files% 和 %Program Files (x86)% 資料夾中。狀態：已啟用。允許的外部位址：所有。通訊協定：TCP 和 UDP，每個通訊協定一條規則。

- Kaspersky Embedded Systems Security 之工作者處理程序的兩個允許規則，這位於 %Program Files% 和 %Program Files (x86)% 資料夾中。狀態：已啟用。允許的外部位址：所有。通訊協定：TCP 和 UDP，每個通訊協定一條規則。

- 本機連接埠 13000 的兩個允許規則。狀態：已啟用。允許的外部位址：所有。通訊協定：TCP 和 UDP，每個通訊協定一條規則。

設定政策

要配置政策設定：

1. 在卡巴斯基安全管理中心管理主控台中，展開**"受管理裝置"**節點。

2. 展開您希望為其配置關聯政策設定的管理群組，然後開啟詳細資訊視窗中的 **政策**頁籤。

3. 點擊要設定的政策名稱。

   採用以下方法之一開啟**"內容：<政策名稱>"**視窗：

   - 在政策的內容功能表中選取**內容**選項。

   - 按兩下所選政策。

4. 在**政策狀態**部分的**一般**頁簽上，啟用或停用政策。為此，請選擇以下一個選項：

   - **啟用政策**，如果您希望在選定管理群組內的所有受防護裝置上套用政策。
   - **漫遊政策**，該政策將在電腦離開組織網路邊緣時啟動。
   - **停用政策**，如果您不希望以後在選定管理群組內的所有受防護裝置上啟動政策。

5. 在政策的其他部分中配置應用程式設定。

   > 您可透過卡巴斯基安全管理中心政策啟用或停用在管理群組內的所有受防護裝置上執行任何工作。

   > 您可為每個單個軟體元件配置在所有網路受防護裝置上套用政策設定。

6. 點擊**OK**。

將在政策中套用配置的設定。

安全等級指示器

安全等級指示器顯示在政策內容視窗的頂部。此指示器的值可能如下：

- **高防護等級**如果以下類別的所有元件都已啟用並標記為 ，指示器會呈現此值並且顏色會變更為綠色：
  - **緊急**此類別包含以下元件：
    - 即時檔案防護
    - 行為偵測
    - 弱點利用防禦
    - 修復引擎
    - 啟用安全桌面通知
  - **重要**此類別包含KSN 使用元件：
- **中度防護等級**如果一個重要元件被停用或標記為 ，指示器會呈現此值並且顏色會變更為黃色。
- **低度防護等級**如果一個或多個關鍵元件被停用或標記為 ，指示器會呈現此值並且顏色會變更為紅色。

如果指示器顯示**中度防護等級**或者**低度防護等級**值，使用指示器右側的連結可打開「**建議的防護元件**」視窗。在此視窗中，您可以啟用任何建議的防護元件並防止它們被停用。

使用卡巴斯基安全管理中心建立和管理工作

本節包含有關 Kaspersky Embedded Systems Security 工作、如何建立工作、配置工作設定，以及啟動和停止工作的資訊。

關於卡巴斯基安全管理中心中的工作建立

您可為管理群組和受防護裝置集建立群組工作。您可以透過卡巴斯基安全管理中心建立以下類型的工作：

- *應用程式啟動*
- *管理伺服器連線防護*
- *變更 Kaspersky Embedded Systems Security 元件*
- *基於基線的系統完整性監控*
- *更新*
- *更新回溯*
- *按需掃描*
- *應用程式完整性控制*
- *移除金鑰*
- *應用程式啟動控制規則產生器*
- *裝置控制規則產生器*

您可採用以下方式建立本機和群組工作：

- 對於「**工作**」區域中的單個受防護裝置。
- 對於管理群組：在選定受防護裝置群組的節點的詳細資訊窗格中的「**工作**」索引標籤上。
- 對於一組受防護裝置：在**裝置分類**節點的詳細資訊窗格中。

您可以使用政策停用同一管理群組中所有受防護裝置上的*更新*和*按需掃描*本機系統工作的排程。

有關卡巴斯基安全管理中心工作的一般資訊，請參閱*卡巴斯基安全管理中心說明*。

使用卡巴斯基安全管理中心建立工作

要在卡巴斯基安全管理中心管理主控台中建立新工作：

1. 採用以下方式之一啟動工作精靈：

   - 若要建立本機工作，請執行以下步驟：

     a. 展開管理主控台樹狀目錄中的「**受管理裝置**」節點，選取受防護伺服器所屬的群組。

     b. 在「**裝置**」索引標籤的結果窗格中，開啟受防護裝置的內容功能表，然後選取「**內容**」。

     c. 在開啟的視窗中的「**工作**」區域中，點擊「**新增**」按鈕。

   - 建立群組工作：

     a. 展開卡巴斯基安全管理中心管理主控台樹狀目錄中的**受管理裝置**節點。

     b. 選取要為其建立工作的管理群組。

     c. 在結果窗格中，開啟「**工作**」索引標籤，然後選取「**新工作**」。

   將開啟工作精靈視窗。

2. 在「**選取工作類型**」視窗中，在「**Kaspersky Embedded Systems Security**」標題下，選取要建立的工作類型。

3. 根據工作類型，設定可能有所變化：

   - 建立自訂掃描工作。

   - 要建立更新工作，請根據您的需要配置工作設定：

     a. 您可以在**更新來源**區塊中將卡巴斯基安全管理中心管理伺服器或 Kaspersky 更新伺服器指定為應用程式更新來源。您也可以建立自訂更新來源清單：透過手動新增自訂 HTTP 和 FTP 伺服器或網路資料夾，並將他們設定為更新來源。

     如果手動自訂的伺服器無法使用，您可指定使用 Kaspersky 更新伺服器。

     b. 配置可減少磁碟子系統負載的功能設定：

     c. 您可以指定 Kaspersky Embedded Systems Security 在需要關鍵應用程式模組更新時以及關鍵更新安裝完成後將會執行的動作。此外，您也可以指定 Kaspersky Embedded Systems Security 是否接收可用排程更新的資訊。

     d. 指定要複製的更新集合以及 Kaspersky Embedded Systems Security 將用於儲存複製的更新的資料夾的路徑。

   - 要建立「*應用程式啟動*」工作：

     a. 在**"啟動設定"**視窗中，指定您要用來啟動應用程式的金鑰檔案或者啟動碼。

     b. 如果您想要建立用於續約產品授權的工作，請選中**"用作備用金鑰"**核取方塊。

- 建立應用程式啟動控制規則產生器工作。
- 建立裝置控制規則產生器工作。

4. 配置工作排程。
5. 點擊**OK**。
6. 如果是為一組受防護裝置建立的工作，請選取將執行該工作的受防護裝置網路（或群組）。
7. 在「**選取要執行此工作的帳戶**」視窗中，指定將要用於執行工作的帳戶。
8. 在「**定義工作名稱**」視窗中，输入工作名称（长度不得超过 100 个字符，不得包含符号 **" * < > ? \ | :**）。

   建議將工作類型新增到工作名稱中（例如，自訂掃描共用資料夾）。
9. 在**"完成工作建立"**視窗中執行下列操作之一：

   a. 如果您希望工作在建立後立即啟動，請選取「**精靈完成時執行工作**」核取方塊。

   b. 單擊**"完成"**。

建立的工作將會在**工作**清單中顯示。

前往個別電腦的本機工作設定和一般應用程式設定

如果應用程式目前受卡巴斯基安全管理中心政策管控，且該政策禁止變更應用程式設定，則您無法為個別電腦編輯這些設定。

若要前往個別電腦的本機工作設定：

1. 在卡巴斯基安全管理中心管理主控台樹狀目錄中，展開**"受管理裝置"**節點。
2. 選取受防護裝置所屬的群組。
3. 在結果窗格中，選擇**"裝置"**頁簽。
4. 采用以下方法之一打开**"属性：<受保护设备名称>"**窗口：

   - 按兩下受防護裝置的名稱。
   - 在受防護裝置名稱的內容功能表中，選擇**屬性**。

   将打开**"属性：<受保护设备名称>"**窗口。
5. 轉至**"工作"**部分。

6. 在工作清單中，選擇要以下列方式之一設定的本機工作：

   - 按兩下工作名稱
   - 在清單中選擇一個工作，然後按一下**屬性**按鈕
   - 在工作名稱的內容功能表中，選擇**屬性**。

   "**属性：<任务名称>**"視窗將開啟。

若要前往個別電腦的一般應用程式設定：

1. 展開卡巴斯基安全管理中心管理主控台樹狀目錄中的**受管理裝置**節點，選擇受防護裝置所屬的群組。
2. 在結果窗格中，選擇"**裝置**"頁簽。
3. 采用以下方法之一打开"**属性：<受保护设备名称>**"窗口：

   - 按兩下受防護裝置的名稱。
   - 在受防護裝置名稱的內容功能表中，選擇**屬性**。

   將打开"**属性：<受保护设备名称>**"窗口。
4. 轉至"**應用程式**"部分。
5. 在已安裝的應用程式清單中，透過以下方式之一選擇 Kaspersky Embedded Systems Security：

   - 按兩下 Kaspersky Embedded Systems Security 的名稱
   - 在清單中選擇 Kaspersky Embedded Systems Security，然後按一下**屬性**按鈕。
   - 在 Kaspersky Embedded Systems Security 名稱的內容功能表中，選擇**屬性**項目。

   Kaspersky Embedded Systems Security 的**設定**視窗將開啟。

在卡巴斯基安全管理中心中設定群組工作

要為多個受防護裝置配置群組工作：

1. 在卡巴斯基安全管理中心管理主控台樹狀目錄中，展開「**受管理裝置**」節點，然後選取要為其設定應用程式工作的管理群組。
2. 在所選管理群組的詳細資訊窗格中，開啟「**工作**」索引標籤。
3. 在先前建立的群組工作清單中，選擇您要配置的工作。
4. 採用以下方法之一開啟"**內容：<工作名稱>**"視窗：

   - 在建立的工作清單中點擊工作名稱。
   - 在建立的工作清單中選取工作名稱，然後點擊「**設定工作**」連結。
   - 在建立的工作清單中開啟工作名稱的內容功能表，然後選取「**內容**」項。

5. 在「**通知**」區域，配置工作事件通知設定。關於此節中配置設定的詳細資訊，請參閱卡巴斯基安全管理中心說明。

6. 根據配置的工作類型，請執行下列一種操作：

   - 要設定「*按需掃描*」工作：
     - 在"**掃描範圍**"部分中，配置掃描範圍。
     - 在"**設定**"部分中，配置工作優先順序水準及與其他軟體元件的整合。
   - 要設定「*更新*」工作：
     - 轉到 **設定** 部分並指定 **應用程式資料庫和模組更新設定**。
     - 選取要執行的操作：複製並安裝軟體模組的關鍵更新或僅檢查它們。
   - 要設定「*應用程式啟動*」工作：
     - 在"**設定**" 部分中，指定您要用來啟動應用程式的金鑰檔案或者啟動碼。
     - 如果您想要新增用於續約產品授權的啟動碼或金鑰檔案，請選中"**用作備用金鑰**"核取方塊。
   - 要設定「*裝置控制規則產生器*」工作，請在「**設定**」區域中指定要用於建立裝置控制規則清單的設定。

7. 在"**排程**"部分中配置工作排程。

8. 在"**帳戶**"部分中，指定將使用其權限執行工作的帳戶。關於此節中配置設定的詳細資訊，請參閱卡巴斯基安全管理中心說明。

9. 如有必要，在**工作範圍排除項目**部分中指定要從工作範圍中排除的物件。關於此節中配置設定的詳細資訊，請參閱卡巴斯基安全管理中心說明。

10. 在**屬性：<工作名稱>** 視窗中按一下**確定**按鈕。

    將儲存新配置的群組工作設定。

下面列出了群組工作的可配置設定。

- 應用程式啟動控制規則產生器

  在配置「*應用程式啟動控制規則產生器*」工作設定時，您可以選取如何在「**規則**」索引標籤上建立允許規則：

  - **基於正在執行的應用程式建立允許規則**
  - **為資料夾的應用程式建立允許規則**

  您可以在 **設定** 頁簽上指定在建立應用程式啟動控制允許規則時執行下列操作：

  - **使用數位憑證**
  - **使用數位憑證主旨和指紋**
  - **如果憑證缺失，則使用**

- **使用 SHA256 雜湊**
- **產生適用於使用者和/或使用者群組的規則**

  您可以使用 Kaspersky Embedded Systems Security 在工作完成時建立的允許規則清單為設定檔配置設定。

  您可以配置按排程啟動工作的設定。

- 裝置控制規則產生器
  - 選擇執行模式：考慮曾經連接過的所有外部的系統資料，或僅考慮目前連接的外部裝置。
  - 使用 Kaspersky Embedded Systems Security 在工作完成時建立的允許規則清單為設定檔配置設定。
  - 您可以配置按排程啟動工作的設定。
- 應用程式啟動
  - 要啟動應用程式或續約產品授權，可以新增金鑰檔案或者啟動碼。
  - 您可以配置按排程啟動工作的設定。
- 資料庫和應用程式模組更新
  - 您可以在**更新來源**設定區塊中將卡巴斯基安全管理中心管理伺服器或 Kaspersky 更新伺服器指定為應用程式更新來源。您也可以建立自訂更新來源清單：透過手動新增自訂 HTTP 和 FTP 伺服器或網路資料夾，並將他們設定為更新來源。

    如果手動自訂的伺服器無法使用，您可指定使用 Kaspersky 更新伺服器。
  - 您可以配置減少磁碟子系統負載的功能設定：
    - **降低磁碟 I/O 上的負載**
    - **用於最佳化的 RAM (MB)**
  - 您可以指定 Kaspersky Embedded Systems Security 在需要關鍵應用程式模組更新時以及關鍵更新安裝完成後將會執行的動作。此外，您也可以指定 Kaspersky Embedded Systems Security 是否接收可用排程更新的資訊。
  - 您可以指定要複製的更新集合以及 Kaspersky Embedded Systems Security 將用於儲存複製的更新的資料夾的路徑。
  - 您可以配置按排程啟動工作的設定。
- 按需掃描
  - 您可指定"自訂掃描"工作的掃描範圍，並配置安全等級設定。
  - 在**Heuristic analyzer**設定區塊中，您可以啟用或停用將啟發式分析器用於自訂掃描工作，並使用滑桿設定分析等級。

- 在“**Integration with other components**”塊中，您可配置以下設定：
  - 在背景模式下啟動指定工作。
  - 將工作視為關鍵區域掃描。
  - 停用同時啟動多個掃描工作。
- 您可以配置按排程啟動工作的設定。

- 應用程式完整性控制
  - 您可以配置按排程啟動工作的設定。
- 基於基線的系統完整性監控
  - 您可以配置指定對檔案、登錄檔和裝置執行操作的監控模式和規則。
  - 您可以配置按排程啟動工作的設定。

應用程式啟動工作

要設定應用程式啟動工作：

1. 在卡巴斯基安全管理中心管理主控台樹狀目錄中，展開“**受管理裝置**”節點，然後選擇要為其配置應用程式工作的管理群組。
2. 在所選管理群組的詳細資訊視窗中，開啟**工作**頁籤。
3. 在先前建立的群組工作清單中，選擇您要配置的工作。
4. 採用以下方法之一開啟“**內容：<工作名稱>**”視窗：
   - 在建立的工作清單中點擊工作名稱。
   - 在建立的工作清單中開啟工作名稱的內容功能表，然後選擇“**內容**”項。

   > 在“**通知**”部分中，配置工作事件通知設定。關於此節中配置設定的詳細資訊，請參閱卡巴斯基安全管理中心說明。
5. 在“**啟動設定**”部分中，指定您要用來啟動應用程式的金鑰檔案。如果您想要新增用於續約產品授權的金鑰，請選中**用作備用金鑰**核取方塊。
6. 在“**排程**”部分中，配置工作排程設定。
7. 如有需要，在“**工作範圍的排除項目**”部分中指定要從工作範圍中排除的物件。

   如需此節中配置設定的詳細資訊，請參閱卡巴斯基安全管理中心說明。
8. 在**屬性：<工作名稱>** 視窗中按一下**確定**按鈕。

將儲存新配置的群組工作設定。

更新工作

要設定更新工作：

1. 在卡巴斯基安全管理中心管理主控台樹狀目錄中，展開**"受管理裝置"**節點，然後選擇要為其配置應用程式工作的管理群組。
2. 在所選管理群組的詳細資訊視窗中，開啟**工作**頁籤。
3. 在先前建立的群組工作清單中，選擇您要配置的工作。
4. 採用以下方法之一開啟**"內容：<工作名稱>"**視窗：
   - 在建立的工作清單中點擊工作名稱。
   - 在建立的工作清單中開啟工作名稱的內容功能表，然後選擇**"內容"**項。
5. 在**"通知"**部分中，配置工作事件通知設定。關於此節中配置設定的詳細資訊，請參閱卡巴斯基安全管理中心說明。
6. 在**"設定"**部分中執行下列操作：
   a. 使用**應用程式資料庫和模組更新設定** 部分中的**設定**按鈕選擇更新來源：
      - 卡巴斯基安全管理中心管理伺服器。
      - Kaspersky 更新伺服器。
      - 自訂 HTTP 或 FTP 伺服器，或網路資料夾。

      要將 SMB 共用資料夾當作更新來源，您需要指定使用者帳戶以啟動工作。

      如果手動自訂的伺服器無法使用，您可指定使用 Kaspersky 更新伺服器。

   b. 配置可減少磁碟子系統負載的功能設定：
      - **降低磁碟 I/O 上的負載**此核取方塊可以啟用或停用透過將更新檔案儲存在記憶體中的虛擬磁碟機上實作磁碟子系統最佳化的功能。預設情況下，會取消勾選核取方塊。
      - **用於最佳化的 RAM (MB)**

   c. 指定當應用程式模組的關鍵更新可用或有關於已計劃更新的資訊時 Kaspersky Embedded Systems Security 應執行的操作。

   d. 指定更新複製設定。
7. 在「**排程**」區域中設定工作排程（您可以為除「更新回溯」以外的所有工作類型設定排程）。

8. 在**"帳戶"**部分中，指定將使用其權限執行工作的帳戶。

如需此節中配置設定的詳細資訊，請參閱卡巴斯基安全管理中心說明。

9. 在**"內容：<工作名稱>"**視窗中，點擊**"確定"**。

對於「*更新回溯*」工作，可在「**通知**」和「**工作範圍的排除項目**」區域中僅配置由卡巴斯基安全管理中心控制的標準工作設定。如需此節中配置設定的詳細資訊，請參閱卡巴斯基安全管理中心說明。

應用程式完整性控制

要設定「應用程式完整性控制」群組工作：

1. 在卡巴斯基安全管理中心管理主控台樹狀目錄中，展開**"受管理裝置"**節點，然後選擇要為其配置應用程式工作的管理群組。
2. 在所選管理群組的詳細資訊視窗中，開啟**工作**頁籤。
3. 在先前建立的群組工作清單中，選擇您要配置的工作。
4. 採用以下方法之一開啟**"內容：<工作名稱>"**視窗：
   - 在建立的工作清單中點擊工作名稱。
   - 在建立的工作清單中開啟工作名稱的內容功能表，然後選擇**"內容"**項。
5. 在**"通知"**部分中，配置工作事件通知設定。關於此節中配置設定的詳細資訊，請參閱卡巴斯基安全管理中心說明。
6. 在**"裝置"**部分中，選擇要為其配置*應用程式完整性控制*工作的裝置。
7. 在**"排程"**部分中，配置工作排程設定。
8. 在**"帳戶"**部分中，指定將使用其權限執行工作的帳戶。
9. 如有需要，在**"工作範圍的排除項目"**部分中指定要從工作範圍中排除的物件。

如需此節中配置設定的詳細資訊，請參閱卡巴斯基安全管理中心說明。

10. 在**屬性：<工作名稱>** 視窗中按一下**確定**按鈕。

排程工作

若要使用管理外掛程式排程工作，請執行以下操作：

1. 在管理主控台樹狀目錄的**"受管理裝置"**資料夾中，開啟相關用戶端電腦所屬的管理群組名稱的資料夾。
2. 在工作區選取**"裝置"**標籤。

3. 點擊以開啟電腦內容視窗。

4. 轉到“**工作**”區域。

5. 雙擊開啟要為其配置排程的工作的屬性視窗。

6. 選擇 **排程** 部分。

7. 根據需要配置排程設定（參見下表）。

如果卡巴斯基安全管理中心政策封鎖自訂掃描工作和更新工作的排程，則這些工作的排程設定的欄位無法使用。

8. 點擊“**套用**”按鈕儲存工作啟動設定。

如果要使用卡巴斯基安全管理中心配置單一工作的應用程式設定，請參閱在卡巴斯基安全管理中心的應用程式設定視窗中配置本機工作一節。

工作排程設定

參數	描述
排程開始	選擇工作執行模式： • **每 N 小時**該工作將每隔幾個小時定期執行。請指定工作的開始時間和持續時間（以小時為單位）。 • **每 N 天**該工作將每隔幾天定期執行。請指定工作的開始時間和持續時間（以天為單位）。 • **每 N 分鐘**該工作將每隔幾分鐘定期執行。請指定工作的開始時間和持續時間（以分鐘為單位）。 • **每週**該工作將在每週的特定一天執行。指定星期幾和開始時間。 • **每月**該工作將在每月特定日期執行。請指定開始日期和時間。 • **一次**該工作將在指定的日期和時間執行一次。 • **手動**執行模式，您可以在方便時手動開始掃描。 • **當新更新下載至儲存區時**每次向儲存庫下載更新時，該工作都會執行。 • **在完成其它工作時**該工作將在另一個工作完成後執行。選擇工作及其完成狀態。 Kaspersky Embedded Systems Security 不支援使用 **在完成其它工作時** 模式排程本機工作。 • **在偵測到病毒爆發時**如果偵測到病毒攻擊，該工作將執行。 • **在應用程式啟動時**每次 Kaspersky Embedded Systems Security 啟動時，該工作都會執行。
執行錯過的工作	如果選中此核取方塊，Kaspersky Embedded Systems Security 將在可能的情況下儘快啟動已略過的工作。工作在某些情況下可能被略過，例如，電腦在排程的工作啟動時關閉。當應用程式有機會執行錯過的工作時，它會在一定的時間間隔內隨機執行工作，以分配電腦上的負載。 如果清除此核取方塊，Kaspersky Embedded Systems Security 不會執行已略過的工作。它將按照目前排程執行下一次工作。
使用工作啟動自動隨機化延遲	如果選取此核取方塊，則該工作將在特定時間範圍內的隨機時間在電腦上執行。隨機開始時間有助於避免當工作按照排程執行時，大量電腦同時存取管理伺服器。 如果清除該核取方塊，則工作會準確在排程的時間執行。
使用工作啟動隨機延遲間隔（分鐘）	如果選取此核取方塊，則該工作將在特定時間範圍內的隨機時間在電腦上執行。隨機開始時間有助於避免當工作按照排程執行時，大量電腦同時存取管理伺服器。 如果清除該核取方塊，則工作會準確在排程的時間執行。
在啟動工作之前，使用 Wake-On-LAN 功能開啟裝置	如果選擇此核取方塊，則電腦的作業系統會被給與指定的前置重疊時間以在執行工作前完成啟動。預設前置重疊時間為 5 分鐘。 如果您希望在包括關機電腦在內的所有電腦上執行工作，請選擇此核取方塊。
完成工作後將裝置關機	如果選取此核取方塊，電腦將在工作完成後關機。 例如，您可以啟用此功能以在周五下班後掃描電腦。工作完成後，應用程式會在週末關閉電腦。
停止工作，若執行時間超過	限制工作執行時間。超出指定時間後，Kaspersky Embedded Systems Security 將停止工作。工作未標記為已完成。下次 Kaspersky Embedded Systems Security 執行該工作時，它將從頭開始按排程執行。

參數	描述
暫停工作	您可以指定暫停執行先前已排程工作的時間間隔。指定時間段結束後，工作將還原。例如，為了最大限度地減少 Kaspersky Embedded Systems Security 在高峰使用期間對電腦效能的影響，這樣做可能是必要的。 此功能僅適用於自訂掃描工作。
停用排程自	如果選取此核取方塊，Kaspersky Embedded Systems Security 將從指定日期開始停止執行已排程工作。工作將設定為 **手動** 模式。 此功能僅適用於自訂掃描工作。

卡巴斯基安全管理中心中的報告

卡巴斯基安全管理中心中的報告包含有關受管理裝置狀態的資訊。報告基於管理伺服器上儲存的資訊。

從卡巴斯基安全管理中心11 開始，對於 Kaspersky Embedded Systems Security，以下類型的報告可用：

- 有關應用程式元件狀態的資訊
- 有關已禁止的應用程式的報告
- 有關在測試模式下禁止的應用程式的報告

如需使用卡巴斯基安全管理中心報告的詳細資訊，請參閱 卡巴斯基安全管理中心說明。

有關 Kaspersky Embedded Systems Security 元件狀態的報告

您可以監視所有網路裝置的防護狀態，並獲得每個裝置上的元件集的結構化概覽。

報告顯示每個元件的以下狀態之一：*正在執行*、*已暫停*、*已停止*、*產品授權不支援*。

*未安裝*狀態指的是元件，而不是應用程式本身。如果未安裝應用程式，卡巴斯基安全管理中心會分配 N/A（無法使用）狀態。

您可以建立元件選擇並使用篩選來顯示具有指定元件集和狀態的網路裝置。

有關建立和使用選擇的詳細資訊，請參閱卡巴斯基安全管理中心說明。

要在應用程式設定中檢視元件狀態：

1. 展開卡巴斯基安全管理中心管理主控台樹狀目錄中的**"受管理裝置"**節點，然後選擇您希望為其配置應用程式設定的管理群組。
2. 選擇 **裝置** 頁簽然後開啟 **應用程式設定** 視窗。
3. 選擇**"元件"**部分。
4. 檢視狀態表。

要檢視卡巴斯基安全管理中心標準報告：

1. 在管理主控台樹狀目錄中選擇**"管理伺服器 <管理伺服器名稱>"**節點。
2. 選擇**"報告"**頁簽。
3. 點擊**"有關應用程式元件狀態的報告"**清單項。
   將產生報告。
4. 檢視以下報告詳細資訊：
   - 圖形化圖表。
   - 元件和安裝了每個元件的網路裝置總數以及裝置所屬的組的匯總表格。
   - 指定了元件狀態、版本、裝置和群組的詳細表格。

有關在啟動模式和測試模式下禁止的應用程式的報告

根據**"應用程式啟動控制"工作**的結果，可以產生兩種類型的報告：有關已禁止的應用程式的報告（如果在啟動模式下啟動該工作）和有關在測試模式下禁止的應用程式的報告（如果在僅統計模式下啟動該工作）。這兩種報告顯示了有關網路的受防護裝置上封鎖的應用程式的資訊。每個報告都針對所有管理組產生，並累積來自受防護裝置上安裝的所有 Kaspersky 應用程式的資料。

要檢視有關在"通知"模式下禁止的應用程式的報告：

1. 在**"通知"**模式下啟動"應用程式啟動控制"工作。
2. 在管理主控台樹狀目錄中選擇**"管理伺服器 <管理伺服器名稱>"**節點。
3. 選擇**"報告"**頁簽。
4. 點擊**"有關在測試模式下禁止的應用程式的報告"**項。
   將產生報告。

5. 檢視以下報告詳細資訊：

   - 顯示封鎖啟動次數最多的前10 個應用程式的圖形化圖表。
   - 應用程式封鎖行為的匯總表格，其中指定可執行檔名稱、原因、封鎖時間和發生封鎖的裝置數量。
   - 指定了有關裝置、檔案路徑和封鎖條件的資料的詳細表格。

要檢視有關在啟動模式下禁止的應用程式的報告：

1. 運行 應用程式啟動控制 任務 積極的 模式。
2. 在管理主控台樹狀目錄中選擇**"管理伺服器 <管理伺服器名稱>"**節點。
3. 選擇**"報告"**頁簽。
4. 點擊**"有關禁止的應用程式的報告"**項。
   將產生報告。

此報告包含的封鎖資料與有關在測試模式下禁止的應用程式的報告相同。

即時防護狀態

Kaspersky Embedded Systems Security 會將設定 **即時防護狀態** 傳送至卡巴斯基安全管理中心管理伺服器；此設定的值取決於受防護裝置上應用程式防護元件目前的狀態（請參閱下表）。

Kaspersky Embedded Systems Security 會根據下列應用程式元件的狀態判定即時防護狀態：

- 即時檔案防護
- 裝置控制
- 防火牆
- 網路威脅防護
- AMSI 掃描程式
- BadUSB 攻擊防護
- 修復引擎
- 弱點利用防禦

您可以在卡巴斯基安全管理中心主控台中查看應用程式的即時防護狀態。

如何在卡巴斯基安全管理中心管理主控台中查看即時防護狀態

1. 開啟卡巴斯基安全管理中心管理主控台。
2. 在主控台樹狀目錄中，選擇**"受管理裝置"**。

目前的即時防護狀態會顯示在裝置清單的 **即時防護狀態** 欄中。若未顯示 **即時防護狀態** 欄，請按一下 **新增/刪除欄位** 連結來管理欄設定。

1. 開啟卡巴斯基安全管理中心管理主控台。

2. 在主控台樹狀目錄中，選擇**"受管理裝置"**。

目前的即時防護狀態會顯示在裝置清單的 **即時防護狀態** 欄中。若未顯示 **即時防護狀態** 欄，請按一下 **新增/刪除欄位** 連結來管理欄設定。

如何在網頁主控台中查看即時電腦防護

在網頁主控台的主視窗中，選擇**資產管理 → 資產（裝置）**。

目前的即時防護狀態會顯示在裝置清單的 **即時防護狀態** 欄中。若未顯示 **即時防護狀態** 欄，請管理欄設定（⚙）。

即時防護狀態 設定的可能值

值	描述
未知	管理伺服器沒有此裝置即時防護狀態的相關資訊。
未安裝	未安裝任何元件。
不受產品授權支援	應用程式尚未啟用，或授權不允許已安裝的元件運作。
失敗	一或多個元件發生故障。
已停止	一或多個元件已停用。
已暫停	一或多個元件已暫停。
正在啟動	一或多個元件正在啟用。
執行中	應用程式元件已啟用且正在運作。

如果卡巴斯基安全管理中心中的 **即時防護狀態** 設定值與 *執行中* 不同，請確認清單中的 Kaspersky Embedded Systems Security 已安裝元件均已啟用，且 應用程式已啟用。

使用 Kaspersky Embedded Systems Security 主控台

本節提供有關 Kaspersky Embedded Systems Security 主控台的資訊，並介紹了如何使用安裝在受防護裝置或其他裝置上的應用程式主控台來管理該應用程式。

啟動應用程式主控台

要啟動應用程式主控台：

1. 採用以下方式之一開啟小型診斷視窗：

   - 執行受防護裝置上應用程式安裝資料夾中的 avpui.exe 檔案。預設情況下，該檔案位於 C:\Program Files (x86)\Kaspersky Lab\Kaspersky Embedded Systems Security.4.1.0。
   - 點擊工作列通知區域中的應用程式圖示。

2. 在開啟的小型診斷視窗中，點擊**Kaspersky Embedded Systems Security Console**連接。

   如果您已經設定了與受防護裝置的連線，則應用程式主控台會開啟。

   如果是第一次啟動應用程式主控台，您將被帶到 **選擇受防護的裝置** 視窗，您必須在其中 設定應用程式主控台與受防護電腦的連線。

   > 應用程式主控台 4.0 版與 Kaspersky Embedded Systems Security 4.1 及更新版本不相容。嘗試連線時，系統會提示您安裝應用程式主控台的相容性套件。相容性套件將從您要連線的裝置下載。

Kaspersky Embedded Systems Security 主控台介面

本節介紹程式介面的主要元素。

Kaspersky Embedded Systems Security 主控台視窗

與其他受防護裝置上安裝的 Kaspersky Embedded Systems Security 建立連線後，將在節點名稱後面附加已安裝應用程式的受防護裝置的名稱和建立連線時所使用的使用者帳戶名稱：**Kaspersky Embedded Systems Security <受防護裝置名稱> 作為 <帳戶名稱>**。透過應用程式主控台連線到同一台受防護裝置上安裝的 Kaspersky Embedded Systems Security 時，節點名稱為 Kaspersky Embedded Systems Security。

主控台樹狀目錄

應用程式主控台樹狀目錄顯示 **Kaspersky Embedded Systems Security** 節點和應用程式功能元件的子節點。

Kaspersky Embedded Systems Security 節點包含以下子節點：

- **即時電腦防護** 允許配置以下工作：
  - **即時檔案防護**
  - **卡巴斯基安全網路**
  - **弱點利用防禦**
  - **網路威脅防護**
  - **行為偵測**
  - **修復引擎**
  - **AMSI 掃描程式**
- **電腦控制**：控制受防護裝置和連線裝置上執行的應用程式。
  - **應用程式啟動控制**
  - **裝置控制**
  - **防火牆**
- **自動規則產生**：配置自動產生應用程式啟動控制元件和裝置控制元件的群組和系統規則。
  - **應用程式啟動控制規則產生器**
  - **裝置控制規則產生器**
  - 規則產生群組工作**<工作名稱>**（如果有）

    使用卡巴斯基安全管理中心建立群組工作。您無法透過 Kaspersky Embedded Systems Security 主控台管理群組工作。
- **系統稽核**：配置係統完整性監控和 Windows 事件記錄分析的設定。
  - **記錄審查**
  - **系統完整性監控**
- **按需掃描**：管理按需掃描工作。每個工作具有單獨的節點：
  - **關鍵區域掃描**
  - **應用程式完整性控制**
  - **卸除式磁碟機掃描**

- **完整掃描**
- 自訂工作**<工作名稱>**（如有）

該節點顯示安裝應用程式時建立的系統工作、自訂工作，以及使用卡巴斯基安全管理中心建立並傳送到受防護裝置的群組自訂掃描工作。

- **更新**：管理 Kaspersky Embedded Systems Security 資料庫和應用程式模組的更新，並提供回溯上次更新的可能性：
  - **資料庫和應用程式模組更新**
  - **上次更新回溯**
  - **應用程式更新**

  該節點顯示使用卡巴斯基安全管理中心建立並傳送到受防護裝置的所有自訂和群組更新工作。
- **儲存**：管理備份設定和被封鎖的網路工作階段清單。
  - **備份**
  - **被封鎖的網路工作階段**
- **記錄和通知**：管理本機工作記錄和 Kaspersky Embedded Systems Security 系統稽核記錄。
  - **系統稽核**
  - **應用程式啟動控制**
  - **裝置控制**
  - **應用程式完整性控制**
  - **記錄審查**
  - **系統完整性監控**
  - **網路威脅防護**
  - **按需掃描**
  - **防火牆**
  - **弱點利用防禦**
  - **行為偵測**
  - **AMSI 掃描程式**
  - **更新**

- **即時檔案防護**
- **備份**

- **產品授權**：新增或刪除 Kaspersky Embedded Systems Security 金鑰，檢視產品授權詳細資訊。

詳細資訊視窗

詳細資訊視窗顯示有關選定節點的資訊。如果選擇 **Kaspersky Embedded Systems Security** 節點，詳細資訊面板將顯示有關目前裝置防護狀態的資訊，以及有關 Kaspersky Embedded Systems Security、其功能元件的防護狀態和產品授權到期日期的資訊。

Kaspersky Embedded Systems Security 節點的內容功能表

可使用 **Kaspersky Embedded Systems Security** 節點的內容功能表項執行以下操作：

- **暫停防護**
- **配置信任區域設定**檢視和配置受信任區域設定。
- **卸除式磁碟機掃描**配置透過 USB 連接埠連線到受防護裝置上的卸除式磁碟機掃描。
- **應用程式管理的使用者存取權限**檢視和配置 Kaspersky Embedded Systems Security 功能的存取權限。
- **KESS 服務管理的使用者存取權限**檢視和設定管理 Kaspersky Embedded Systems Security 服務 的使用者權限。
- **儲存**
- **匯出設定**將應用程式設定儲存到 XML 格式的設定檔中。也可以在應用程式工作的內容功能表中執行此操作。
- **匯入設定**. 從 XML 格式的設定檔中匯入應用程式設定。也可以在應用程式工作的內容功能表中執行此操作。
- **重新整理**重新整理 Kaspersky Embedded Systems Security 主控台視窗的內容。也可以在應用程式工作的內容功能表中執行此操作。
- **應用程式內容**檢視和配置 Kaspersky Embedded Systems Security 或選定工作的設定。也可以在應用程式工作的內容功能表中執行此操作。

  為此，您也可以使用 Kaspersky Embedded Systems Security 節點的詳細資料面板中的 **應用程式內容** 連結。

- **說明**檢視 Kaspersky Embedded Systems Security 說明資訊。也可以在應用程式工作的內容功能表中執行此操作。

Kaspersky Embedded Systems Security 工作的工具列和內容功能表

您可以使用 Kaspersky Embedded Systems Security 主控台樹狀目錄中每個工作的內容功能表來管理 Kaspersky Embedded Systems Security 工作。

可使用內容功能表項執行以下操作：

- **還原/暫停**。還原或暫停執行工作。要執行這些操作，您還可以使用工具列上的按鈕。此操作適用於"即時防護"工作和"自訂掃描"工作。
- **建立工作**新建自訂工作。
- **刪除工作**刪除自訂工作。
- **匯出設定 / 匯入設定**。匯出或匯入工作設定。
- **內容**開啟"工作設定"視窗。
- **說明**開啟相應的線上說明主題。

通知區域中的系統托盤圖示

Kaspersky Embedded Systems Security 安裝完成後，程式圖示將立即出現在 Microsoft Windows 工作列通知區域。

如果工作列通知區域的應用程式圖示被隱藏，則管理員在政策中已停用顯示應用程式介面。

本圖示有以下功能：

- 顯示應用程式的活動。
- 是存取內容功能表和應用程式主視窗的快速方式。

提供以下應用程式圖示狀態以顯示應用程式執行資訊：

- 圖示表示應用程式至關重要的防護元件已啟用。如果需要使用者執行操作（例如，在更新應用程式後重新啟動電腦），則 Kaspersky Embedded Systems Security 將顯示警告 。
- 圖示表示應用程式至關重要的防護元件已停用或發生故障。例如，如果產品授權已到期或存在應用程式錯誤，則可能導致防護元件發生故障。Kaspersky Embedded Systems Security 將顯示警告 並敘述電腦防護中的問題。

用滑鼠右鍵按一下系統托盤圖示可開啟該圖示的內容功能表。

內容功能表提供了多個可用於顯示應用程式視窗的命令（請參閱下表）。

系統匣圖示中的內容功能表命令

指令	描述
開啟應用程式主控台	開啟 Kaspersky Embedded Systems Security 主控台（如已安裝）。
開啟小型診斷視窗	開啟小型診斷視窗。
關於	開啟包含有關 Kaspersky Embedded Systems Security 資訊的 **關於** 視窗。 對於註冊的 Kaspersky Embedded Systems Security 使用者，**關於** 視窗包含有關已安裝的緊急更新的資訊。
隱藏	隱藏工作列通知區域中的系統托盤圖示。

您可以隨時重新顯示隱藏的系統托盤圖示。

要再次顯示系統托盤圖示，

在 Microsoft Windows 的**啟動**功能表中，選擇「**所有程式** > **Kaspersky Embedded Systems Security**。該圖示將出現在 Microsoft Windows 工作列的通知區域中。

設定的名稱可能有所不同，具體取決於安裝的作業系統。

透過應用程式主控台配置一般設定

Kaspersky Embedded Systems Security 的一般設定和故障診斷設定設定了應用程式的一般執行條件。您可以透過這些設定來控制 Kaspersky Embedded Systems Security 所使用的工作處理程序數，在異常終止後還原 Kaspersky Embedded Systems Security 工作，維護記錄，在異常終止後建立 Kaspersky Embedded Systems Security 處理程序的 Dump 檔案，以及設定其他一般設定。

如果卡巴斯基安全管理中心啟動政策封鎖對應用程式設定的變更，則無法在 Kaspersky Embedded Systems Security 主控台中配置這些設定。

若要設定 Kaspersky Embedded Systems Security 的一般設定：

1. 在應用程式主控台樹狀目錄中，選擇"**Kaspersky Embedded Systems Security**"節點並執行以下操作之一：
   - 在節點的結果窗格中，點擊**應用程式內容**連結。
   - 在節點的內容功能表中選擇**應用程式內容**。

   開啟"**應用程式內容**"視窗。
2. 在 **介面** 頁簽上，您可以指定希望在 Kaspersky Embedded Systems Security 系統匣圖示上看到哪些警告。
3. 在**安全設定**頁籤上，配置以下設定：
   - 在"**一般**"部分中，配置**在電腦啟動時啟動應用程式（建議）**選項。
   - 在 **自我防護** 下面，配置 應用模組防護 和 作業系統服務。
   - 在"**切換到 UPS 備份電源時的動作**"部分，指定在轉換為 UPS 備份電源後 Kaspersky Embedded Systems Security 對受防護裝置產生的負荷的限制：
     - **不啟動排程的掃描工作**

- **停止正在執行的掃描工作**

- 在"**相容性設定**"部分中，配置**與遠端管理軟體相容**設定。

- 在 **掃描設定** 部分，配置限制掃描工作的 CPU 使用率 並允許 將資源讓給其他應用程式。

4. 在**網路設定**頁籤上，配置以下設定：

   - 在 **代理伺服器** 部分，指定代理伺服器設定：身分驗證類型以及在代理伺服器上進行身分驗證所需的詳細資訊。

   - 在**監控的連接埠**下面，指定網路連接埠監控選項：

     - **監控所有網路連接埠**在此網路連接埠監控模式下，防護元件會監控透過任何開放的電腦網路連接埠傳輸的資料流。

     - **僅監控選定網路連接埠**在此網路連接埠監視模式下，防護元件將監控電腦的選定連接埠和選定應用程式的網路活動。通常用於傳輸電子郵件和網路流量的網路連接埠的清單按照 Kaspersky 專家的建議進行配置。如有必要，您可以編輯網路連接埠清單。

   - 必要的話，在**用於遠端連線的連接埠**下面變更應用程式主控台用來連線到安裝了應用程式的電腦的連接埠。

     使用 Windows 憑據進行連線的預設連接埠號為 13032，使用手動建立的使用者的憑據進行連線的預設連接埠號為 13031。可能的連接埠號範圍：1–65535。

     先前儲存的連接埠號將一直使用直到應用程式重新啟動。

5. 在 **故障診斷** 頁簽上，點選 **設定** 並配置應用程式的追蹤和 記憶體傾印。

6. 單擊"**確定**"。

Kaspersky Embedded Systems Security 設定即被儲存。

管理 Kaspersky Embedded Systems Security 工作

本節包含有關如何為 Windows Server 工作建立、配置、啟動和停止 Kaspersky Security 的資訊。

Kaspersky Embedded Systems Security 工作類別

Kaspersky Embedded Systems Security 中的即時電腦防護、電腦控制、自動規則產生、系統稽核、按需掃描、工業網路防護、儲存管理和更新功能均作為工作實現。

您可以使用 Kaspersky Embedded Systems Security 主控台樹狀目錄中的工作內容功能表和結果窗格來管理這些工作。可在結果窗格中檢視工作狀態資訊。工作管理操作記錄在系統稽核記錄中。

Kaspersky Embedded Systems Security 工作分為兩種類型：*本機*和*群組*。

本機工作

本機工作只能在為其建立的受防護裝置上執行。根據啟動方式，存在以下幾種類型的本機工作：

- **本機系統工作**。這些工作會在安裝 Kaspersky Embedded Systems Security 的過程中自動建立。您可以變更除「*更新回溯*」工作之外的所有本機系統工作的設定。無法重新命名或刪除本機系統工作。您可以同時執行本機系統和自訂掃描工作。

- **本機自訂工作**。在應用程式主控台中，您可以建立按需掃描工作、更新工作和基線系統完整性監控工作。在卡巴斯基安全管理中心中，您可以建立按需掃描工作、更新工作等。您可以重命名、配置或者刪除自訂工作。可同時執行多個自訂工作。

群組工作

您可以從卡巴斯基安全管理中心管理群組工作和一組受防護裝置的工作。所有群組工作都是自訂工作。群組工作也會顯示在應用程式主控台中。在應用程式主控台中，只能檢視群組工作的狀態。您不能使用應用程式主控台來管理或配置群組工作。

手動啟動/暫停/還原/停止工作

您可以手動啟動、暫停、還原或停止工作。這些選項並非適用於所有 Kaspersky Embedded Systems Security 工作。

若要啟動/暫停/還原/停止工作：

1. 在應用程式主控台樹狀目錄中，開啟工作的內容功能表。

2. 選擇以下命令之一：**啟動**或者 **暫停**。

該操作將執行並記錄到系統稽核記錄中。

排程工作

在 Kaspersky Embedded Systems Security 主控台中，您可以設定執行本機系統工作和使用者工作的排程。但是，您無法設定執行群組工作的排程。

要排程工作：

1. 在主控台樹狀目錄中，選取要為其設定排程的工作。

2. 在結果窗格中，點擊“**內容**”連結。

3. 在開啟的視窗的**執行模式**部分中，執行以下操作之一：

   - 選取 **手動** 核取方塊，以便在您方便的時間手動執行工作。

   - 如果您希望啟用工作的啟動排程，請選中“**依排程**”核取方塊。

4. 如果選取 **依排程** 選項，請設定工作排程設定（請參閱下表）。

5. 如有必要，請選擇 **工作執行身分** 核取方塊，並指定將執行該工作的使用者帳戶的憑據。

6. 單擊**"確定"**。

工作排程設定隨即儲存。

工作排程設定

參數	描述
執行模式	選擇工作執行模式： • **分鐘**該工作將每隔幾分鐘定期執行。請指定工作的開始時間和持續時間（以分鐘為單位）。 • **小時**該工作將每隔幾個小時定期執行。請指定工作的開始時間和持續時間（以小時為單位）。 • **天**該工作將每隔幾天定期執行。請指定工作的開始時間和持續時間（以天為單位）。 • **週**工作將每隔指定週數，在指定的星期幾執行。指定排程，使用核取方塊選取要執行工作的星期幾，並指定工作的開始時間。 • **每月**該工作將在每月特定日期執行。請指定開始日期和時間。 • **在指定時間**該工作將在指定的日期和時間執行一次。 • **每次更新後**每次向儲存庫下載更新時，該工作都會執行。 • **在應用程式啟動後**每次 Kaspersky Embedded Systems Security 啟動時，該工作都會執行。
執行錯過的工作	如果選中此核取方塊，Kaspersky Embedded Systems Security 將在可能的情況下儘快啟動已略過的工作。工作在某些情況下可能被略過，例如，電腦在排程的工作啟動時關閉。當應用程式有機會執行錯過的工作時，它會在一定的時間間隔內隨機執行工作，以分配電腦上的負載。 如果清除此核取方塊，Kaspersky Embedded Systems Security 不會執行已略過的工作。它將按照目前排程執行下一次工作。
使用工作啟動自動隨機化延遲	如果選擇該核取方塊，則工作不會嚴格按照排程執行，而是在某個間隔內隨機執行，即工作的開始時間分散開。隨機開始時間有助於避免當工作按照排程執行時，大量電腦同時存取管理伺服器。 隨機開始時間的範圍在建立工作時自動計算，取決於分配了工作的電腦數量。隨後，工作會始終在計算的開始時間執行。不過，只要工作設定被修改或者手動執行工作，計算的開始時間就會變更。 如果清除該核取方塊，則工作會準確在排程的時間執行。
使用工作啟動隨機延遲間隔（分鐘）	如果選取此核取方塊，則該工作將在特定時間範圍內的隨機時間在電腦上執行。隨機開始時間有助於避免當工作按照排程執行時，大量電腦同時存取管理伺服器。 如果清除該核取方塊，則工作會準確在排程的時間執行。
暫停工作	您可以指定暫停執行先前已排程工作的時間間隔。指定時間段結束後，工作將還原。例如，為了最大限度地減少 Kaspersky Embedded Systems Security 在高峰使用期間對電腦效能的影響，這樣做可能是必要的。 此功能僅適用於自訂掃描工作。
停用排程自	如果選取此核取方塊，Kaspersky Embedded Systems Security 將從指定日期開始停止執行已排程工作。工作將設定為 **手動** 模式。 此功能僅適用於自訂掃描工作。

使用使用者帳戶啟動工作

您可以在系統帳戶下啟動工作，也可以指定其他帳戶。

關於使用帳戶啟動工作

您可以指定該帳戶來執行以下 Kaspersky Embedded Systems Security 工作：

- *應用程式啟動控制規則產生器*
- *裝置控制規則產生器*
- *記錄審查*
- *應用程式完整性控制*
- *更新*

預設情況下，使用系統帳戶權限執行這些工作。

在以下情況下，建議您使用具有正確存取權限的其他帳戶：

- 對於 *更新* 工作：
  - 如果您已指定在網路上其他裝置的共用資料夾作為更新來源。
  - 如果您使用代理伺服器並透過 NTLM 或 Kerberos 驗證來存取更新來源。
- 對於*應用程式啟動控制規則產生器*工作：如果產生的規則被匯出到位於系統帳戶無法存取的設定檔（例如，受防護裝置上的共用資料夾）。

您可以使用系統帳號權限啟動列出的工作。如果 Kaspersky Embedded Systems Security 需存取網路中的另一台裝置上的共用資料夾，且此裝置與受防護裝置在同一個網域中註冊。在這種情況下，系統帳戶必須具有對這些資料夾的存取權限。Kaspersky Embedded Systems Security 將使用帳戶 **<網域名稱\device_name>**的權限存取該裝置。

指定使用者帳戶以啟動工作

在應用程式主控台中指定帳戶的選項並非適用於所有工作。

要指定用於啟動工作的帳戶：

1. 在應用程式主控台樹狀目錄中，選擇要使用特定帳戶的權限啟動的工作。
2. 在結果窗格中，點擊**"執行模式"**連結。

   開啟**"排程和執行模式"**視窗。

3. 在開啟的視窗的**使用者**部分中，執行以下操作：

   a. 請選擇**工作執行身分**選項。

   b. 輸入您要使用的帳戶的使用者名稱和密碼。

   選定使用者必須在受防護裝置上經過註冊，或者與該電腦在同一網域中。

4. 點擊**OK**。

將儲存修改的設定。

匯入和匯出設定

本節說明如何匯出 Windows Server 設定的 Kaspersky Security。您還將學習如何將某些應用程式元件的設定匯出到 XML 組態檔案，以及如何將這些設定從組態檔案匯入回應用程式。

關於匯入和匯出設定

可以將 Kaspersky Embedded Systems Security 設定匯出到 XML 設定檔，也可以將設定檔中的設定匯入到 Kaspersky Embedded Systems Security 中。可以將所有應用程式設定或僅將單個元件的設定儲存到設定檔。

在將 Kaspersky Embedded Systems Security 的所有設定匯出到檔案時，將儲存一般程式設定以及下列 Kaspersky Embedded Systems Security 元件和功能的設定：

- 即時檔案防護
- 弱點利用防禦
- 網路威脅防護
- 行為偵測
- 修復引擎
- AMSI 掃描器
- 應用程式啟動控制
- 裝置控制
- Firewall
- 應用程式啟動控制規則產生器
- 裝置控制規則產生器
- 記錄審查
- 系統完整性監控

- 關鍵區域掃描
- 應用程式完整性控制
- 卸除式磁碟機掃描
- 完整掃描
- 更新資料庫和程式模組
- 最近更新還原
- 更新

此外，還可以在檔案中儲存 Kaspersky Embedded Systems Security 一般設定及使用者帳戶的權限。

如果在匯出時卡巴斯基安全管理中心政策有效，則應用程式將匯出該政策所使用的指定值。

無法匯出群組工作設定。

Kaspersky Embedded Systems Security 將匯出應用程式所使用的所有密碼，例如，用於執行工作或連線代理伺服器的使用者帳戶設定。匯出的密碼以加密的形式儲存在設定檔中。只有該受防護裝置上安裝的 Kaspersky Embedded Systems Security 未重新安裝或更新，才能使用它匯入密碼。

您無法使用安裝在其他受防護裝置上的 Kaspersky Embedded Systems Security 匯入之前儲存的密碼。將設定匯入至受防護裝置之後，必須手動輸入所有密碼。

如果在匯出設定是啟用了 **請求密碼以確認關鍵操作** 功能。 裝置上設定的密碼 將被匯出，然後在匯入設定時自動套用到其他裝置上。

可以從包含 Kaspersky Embedded Systems Security 元件的設定檔（例如從未安裝完整元件集的 Kaspersky Embedded Systems Security 建立的檔案）匯入設定。匯入設定後，只有該設定檔中包含的那些 Kaspersky Embedded Systems Security 設定會發生變化。所有其他設定保持不變。

匯入設定時，已被封鎖的啟動卡巴斯基安全管理中心政策的設定不會發生變更。

匯出設定

要將裝置匯出到設定檔：

1. 要匯出所有 Kaspersky Embedded Systems Security 設定，請在 **Kaspersky Embedded Systems Security** 節點的內容功能表中，選擇 **匯出設定** 命令。

   若要匯出單個元件的設定，請在結果窗格中點擊**匯出設定**。

   無法匯出卡巴斯基安全網路設定。必須手動配置卡巴斯基安全網路。

2. 在開啟的視窗中，指定您要將設定清單匯出到的 XML 檔案的名稱，然後選取要儲存此檔案的資料夾。

   指定路徑時可以使用系統環境變量，但不能使用使用者環境變量。

如果在匯出時卡巴斯基安全管理中心政策有效，則應用程式將匯出該政策使用的設定。

3. 儲存檔案。
4. 在**匯出設定已成功完成。**視窗中，按一下**確定**按鈕。

   Kaspersky Embedded Systems Security 會將設定清單匯出到 XML 檔案。

要匯出受信任應用程式的清單：

1. 在應用程式主控台樹狀目錄中，開啟"**Kaspersky Embedded Systems Security**"節點的內容功能表。
2. 選擇"**配置信任區域設定**"。
3. 開啟"**配置信任區域設定**"視窗。
4. 轉到 **受信任應用程式** 部分並點擊**設定**。

   這將開啟包含受信任應用程式清單的視窗。
5. 選擇您要匯出的受信任應用程式。

   如果您沒有選擇任何應用程式，Kaspersky Embedded Systems Security 將匯出所有受信任應用程式。
6. 按一下箭頭，然後在下拉式清單中選擇 **匯出**。
7. 這將開啟一個視窗；在此視窗中，輸入您要將受信任應用程式清單匯出到的 XML 檔案的名稱，然後選取要儲存此檔案的資料夾。
8. 儲存檔案。

   Kaspersky Embedded Systems Security 會將受信任應用程式清單匯出到 XML 檔案。

您也可以使用命令列匯出 Kaspersky Embedded Systems Security 設定。

匯入設定

若要從儲存的設定檔匯入設定：

1. 要匯入所有 Kaspersky Embedded Systems Security 設定，請在 **Kaspersky Embedded Systems Security** 節點的內容功能表中，選擇 **匯入設定** 命令。

   若要匯入單個元件的設定，請在結果窗格中點擊**匯入設定**。

在受防護裝置上匯入 Kaspersky Embedded Systems Security 或其功能元件的一般設定之後，您無法還原先前的設定。

無法匯入卡巴斯基安全網路設定。必須手動配置卡巴斯基安全網路。

2. 在顯示的視窗中，選擇要從其匯入設定的 XML 設定檔，然後點擊**開啟**。

3. 在**匯入設定已成功完成。**視窗中，按一下**確定**按鈕。

4. 在"應用程式主控台"工具列中，點擊**更新**按鈕。

「應用程式主控台」視窗顯示匯入的設定。

如果受防護裝置上的 Kaspersky Embedded Systems Security 進行了重新安裝或更新，Kaspersky Embedded Systems Security 不會從在其他受防護裝置上或同一受防護裝置上建立的檔案匯入密碼（用於啟動工作或連線到代理伺服器的帳戶憑證）。在匯入操作完成時，必須手動輸入密碼。

要匯入受信任應用程式的清單：

1. 在應用程式主控台樹狀目錄中，開啟"**Kaspersky Embedded Systems Security**"節點的內容功能表。

2. 選擇"**配置信任區域設定**"。

3. 開啟"**配置信任區域設定**"視窗。

4. 轉到 **受信任應用程式** 部分並點擊**設定**。

5. 按一下箭頭，然後在下拉式清單中選擇 **匯入**。

6. 這將開啟一個視窗；在此視窗中，選取要從中匯入受信任應用程式清單的 XML 檔案。

7. 開啟檔案。

如果電腦已經具有受信任應用程式清單，則 Kaspersky Embedded Systems Security 將提示您刪除現有清單或從 XML 檔案向其中新增新項目。

8. 該清單顯示在 **受信任應用程式** 頁簽上。單擊"**確定**"。

檢視防護狀態和 Kaspersky Embedded Systems Security 資訊

要檢視有關 Kaspersky Embedded Systems Security 的裝置防護狀態的資訊，

在 Kaspersky Embedded Systems Security 主控台樹狀目錄中，選擇"**Kaspersky Embedded Systems Security**"節點。

預設情況下，將自動重新整理 Kaspersky Embedded Systems Security 主控台的詳細資訊視窗中的資訊：

- 對於本機連線，每 10 秒鐘重新整理一次。
- 對於遠端連線，每 15 秒鐘重新整理一次。

您可以手動重新整理資訊。

*在"**Kaspersky Embedded Systems Security**"節點中手動重新整理資訊，*

在"**Kaspersky Embedded Systems Security**"節點的內容功能表中選擇**重新整理**指令。

Kaspersky Embedded Systems Security 主控台的詳細資訊面板中會顯示以下應用程式資訊：

- "卡巴斯基安全網路使用"狀態。
- 裝置防護狀態。
- 有關資料庫和應用程式模組更新的資訊。
- 實際診斷資料。
- 受防護裝置控制工作的資料。
- 產品授權資訊。
- 與卡巴斯基安全管理中心的整合狀態：已安裝與應用程式連線的卡巴斯基安全管理中心的伺服器的詳細資訊；有關啟動政策控制的應用程式工作的資訊。

使用色彩編碼顯示防護狀態：

- *綠色*。根據配置的設定執行工作。防護處於啟動狀態。
- *黃色*。工作未啟動，已暫停或已停止。可能會發生安全威脅。建議您配置並啟動工作。
- *紅色*。工作完成，但出現錯誤，或工作執行時偵測到安全威脅。建議您啟動工作或採取措施消除偵測到的安全威脅。

此塊中的某些詳細資訊（例如，工作名稱或偵測到的威脅數量）為點擊後將轉至相關工作的節點或開啟工作記錄的連結。

KSN 使用 部分顯示目前工作狀態，例如*正在執行*、*已停止* 或者 *從未執行*。該指示器可以使用的設定值如下：

- 面板為綠色表示**KSN 使用**工作正在執行，並且對狀態的檔案請求正在傳送到 KSN。
- 面板為黃色表示其中一項聲明已被接受，但工作未執行；或工作正在執行，但檔案請求未傳送到 KSN。
- 面板為紅色表示工作失敗。

電腦防護

電腦防護部分（請參見下表）顯示有關裝置的目前防護狀態的資訊。

有關裝置防護狀態的資訊

部分	資訊
裝置防護狀態指示器	帶有此部分名稱的面板的顏色反映了在該部分中正在執行的工作的狀態。該指示器可以使用的設定值如下： • 面板為綠色 – 預設顯示此顏色，指示即時檔案防護元件已安裝且工作正在執行。 • 面板為黃色 – 表示即時檔案防護元件未安裝，且*關鍵區域掃描*工作已長時間未執行。 • 面板為紅色 – 即時檔案防護工作未執行。
即時檔案防護	**狀態** – 元件的目前狀態，例如，*正在執行* 或 *已停用*。
關鍵區域掃描	**上次掃描日期** – 上次在關鍵區域掃描病毒和其他電腦安全威脅的日期和時間。 *從未執行* – 在過去 30 天或更長時間（預設值）內沒有執行「*關鍵區域掃描*」工作時所發生的一個事件。您可以變更產生此事件的上限值。

部分	資訊
網路威脅防護	**狀態** – 元件的目前狀態，例如，*正在執行* 或 *已停用*。
弱點利用防禦	**狀態** – 元件的目前狀態，例如，*正在執行* 或 *已停用*。 **作業模式** – 弱點利用防禦元件的兩種可用模式之一： **封鎖** 或者 **通知**。
行為偵測	**狀態** – 元件的目前狀態，例如，*正在執行* 或 *已停用*。 **作業模式** – 行為偵測工作的三種可用模式之一： **刪除**、**封鎖** 或者 **通知**。

更新

更新部分（請參見下表）顯示有關資料庫和應用程式模組的更新程度的資訊。

有關 Kaspersky Embedded Systems Security 資料庫和模組狀態的資訊

部分	資訊
資料庫和應用程式模組狀態指示器	帶有此部分名稱的面板的顏色反映了資料庫和應用程式模組的狀態。該指示器可以使用的設定值如下： • 面板為綠色 – 預設顯示此顏色，指示應用程式資料庫處於最新狀態，並且上次資料庫和模組更新工作已成功完成。 • 面板為黃色 – 表示資料庫已過期，或上次資料庫和模組更新工作失敗。 • 面板為紅色 - 事件 *資料庫已嚴重過期* 或者 *資料庫已為最新* 已經發生。
資料庫狀態	該選項可以採用以下值： • **資料庫已為最新** – 應用程式資料庫在之前 7 天內進行過更新（預設）。 • **資料庫已過期** – 應用程式資料庫在 7 到 14 天之間進行過更新（預設）。 • **資料庫已嚴重過期** – 應用程式資料庫在 14 天之前進行過更新（預設）。 您可以變更產生*資料庫已過期* 和 *資料庫已嚴重過期*事件的上限值。
資料庫發佈日期	最近資料庫更新的發佈日期和時間。日期和事件指定為 UTC 格式。
最新完成的"資料庫更新"工作的狀態	最近資料庫更新的日期和時間。日期和時間根據受防護裝置的當地時間指定。如果發生"*已失敗*"事件，則欄位中的值為紅色。

控制

"**控制**"部分（請參見下表）顯示有關應用程式啟動控制, 裝置控制和防火墻工作的資訊。

有關受防護裝置控制狀態的資訊

部分	資訊
受防護裝置控制狀態指示器	帶有此部分名稱的面板的顏色反映了在該部分中正在執行的工作的狀態。該指示器可以使用的設定值如下： • 面板為綠色 – 預設顯示此顏色，指示應用程式啟動控制元件已安裝且工作正在活動模式下執行；弱點利用防禦元件已安裝並啟動。 • 在以下一種或多種情況下，面板為黃色：弱點利用防禦未執行；應用程式啟動控制工作正在通知模式下執行；弱點利用防禦正在活動模式下執行，應用程式啟動控制工作未執行或失敗。 • 面板為紅色 – 應用程式啟動控制工作未執行或失敗，弱點利用防禦未執行或在**通知**模式下執行。
應用程式啟動控制	**狀態** – 元件的目前狀態，例如，*正在執行* 或 *已停用*。 **作業模式** – 應用程式啟動控制工作的可用模式之一： **套用規則** 或者 **測試規則**。
裝置控制	**狀態** – 元件的目前狀態，例如，*正在執行* 或 *已停用*。 **作業模式** – 裝置控制工作的兩種可用模式之一： **按規則** 或者 **通知**。
防火牆	**狀態** – 元件的目前狀態，例如，*正在執行* 或 *已停用*。

診斷

"診斷"部分（請參見下表）顯示有關系統完整性監控 和 記錄審查工作的資訊。

有關系統稽核狀態的資訊

部分	資訊
診斷狀態指示器	帶有此部分名稱的面板的顏色反映了在該部分中正在執行的工作的狀態。該指示器可以使用的設定值如下： • 綠色 – 預設顯示，指示一個或兩個系統稽核元件已安裝，且工作正在執行。 • 黃色 – 兩個元件均已安裝，但其中一個系統稽核工作未執行；發生*沒有執行*事件。 • 紅色 – 其中一個工作失敗。
系統完整性監控	**狀態** – 元件的目前狀態，例如，*正在執行* 或 *已停用*。
記錄審查	**狀態** – 元件的目前狀態，例如，*正在執行* 或 *已停用*。

Kaspersky Embedded Systems Security 產品授權資訊顯示在 **Kaspersky Embedded Systems Security** 節點的詳細資訊面板左下角的行中。

您可以按照應用程式內容連結配置 Kaspersky Embedded Systems Security 內容。

您可以按照連線至遠端電腦連結連線至其他受防護裝置。

如何在應用程式主控台中配置備份設定

要配置一般備份設定：

1. 在應用程式主控台樹狀目錄中，開啟**"Kaspersky Embedded Systems Security"**節點上的內容功能表，並選擇**"儲存"**。
2. 按下表所述配置設定。

儲存設定

參數	描述
在 **報告** 頁簽上，指定報告設定：	
儲存報告不超過	如果選中該核取方塊，則最大報告儲存期限制為定義的時間隔。預設的報告最長儲存期限是 30 天。在此時間之後，Kaspersky Embedded Systems Security 將自動移除報告檔案中的最早項目。
限制報告檔案的大小為	如果選中該核取方塊，則最大報告檔案大小限制為定義值。預設情況下，最大檔案大小資料為 1024 MB。要避免超過最大報告檔案容量，當達到最大報告檔案容量時，Kaspersky Embedded Systems Security 將自動刪除報告檔案中的最早項目。
在 **備份** 頁簽上，指定備份設定：	
儲存物件的時間不超過	如果選中該核取方塊，則最大檔案儲存期限制為定義的時間間隔。預設的檔案最長儲存期限是 30 天。最長儲存期限超出後，Kaspersky Embedded Systems Security 將刪除備份區中最舊的檔案。
備份大小限制為	如果選中該核取方塊，則最大儲存大小限制為定義值。預設情況下，最大大小為 400 MB。為避免超過最大儲存大小，當達到最大儲存大小時，Kaspersky Embedded Systems Security 將自動刪除儲存中的最早檔案。
可用空間的閾值	該核取方塊用於啟用或停用監控備份中的最小可用空間大小（預設值為 100 MB）的功能。如果可用空間大小下降到低於指定上限值，Kaspersky Embedded Systems Security 會記錄*"已超過備份區可用空間上限值"*事件，並根據此事件類型的通知設定發佈通知。 如果選中該核取方塊，Kaspersky Embedded Systems Security 會監控備份中的可用空間的大小。 如果選擇了**備份大小限制為**核取方塊，則 **可用空間的閾值** 核取方塊處於活動狀態。

從 Web 主控台和雲端主控台使用 Web 外掛程式

本節提供有關 Kaspersky Embedded Systems Security 網頁主控台管理外掛程式的資訊，並介紹如何管理一台或一組受防護裝置上安裝的應用程式。

從 Web 主控台和雲端主控台管理 Kaspersky Embedded Systems Security

使用 Kaspersky Embedded Systems Security Web 外掛程式，您可以集中管理多台已安裝 Kaspersky Embedded Systems Security 並加入管理群組的受防護裝置。卡巴斯基安全管理中心網頁主控台和雲端主控台也可以讓您分別配置管理群組中每個受防護裝置的設定。

*管理群組*要在卡巴斯基安全管理中心網頁主控台中手動建立。「管理群組」在卡巴斯基安全管理中心中手動建立，包含您要為其設定相同的控制和防護設定的已安裝 Kaspersky Embedded Systems Security 的多個裝置。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。

如果 Kaspersky Embedded Systems Security 在某台受防護裝置上的執行受啟動卡巴斯基安全管理中心政策的控制，則該受防護裝置的應用程式設定無法使用。

可透過以下方式透過卡巴斯基安全管理中心網頁主控台管理 Kaspersky Embedded Systems Security：

- **使用卡巴斯基安全管理中心政策**。可使用卡巴斯基安全管理中心政策為一組裝置遠端設定相同的防護設定。在活动政策中指定的工作設定的优先顺序高于在应用程序主控台中本地配置或在卡巴斯基安全管理中心網頁主控台的"属性：<受保护设备名称>"視窗中遠端配置的工作設定。政策可用於設定一般應用程式設定、即時電腦防護工作的設定、裝置上的活動控制工作、網路儲存防護工作以及按排程啟動本機系統工作的設定。

- **使用卡巴斯基安全管理中心群組工作**。使用卡巴斯基安全管理中心群組工作可遠端設定工作的通用設定，一組裝置具有過期期限。您可使用群組工作來啟動應用程式，設定「自訂掃描」工作設定、「更新」工作設定，以及「應用程式啟動控制規則產生器」工作設定。

- **使用一組裝置的工作**。使用一組裝置的工作允許遠端配置通用工作設定，不屬於任何管理群組的受防護裝置具有的有限執行期限。

- **使用單個裝置的內容視窗**。在裝置內容視窗中，您可遠端配置管理群組中包含的單台受防護裝置的工作設定。如果選取受防護裝置不受啟動卡巴斯基安全管理中心政策的控制，您也可以配置一般應用程式設定和所有 Kaspersky Embedded Systems Security 工作的設定。

卡巴斯基安全管理中心網頁主控台和雲端主控台可以配置應用程式設定和進階功能，並允許您使用記錄和通知。您可以為一組受防護裝置也可以為單台受防護裝置配置這些設定。

Web 外掛程式限制

與 Kaspersky Embedded Systems Security 管理外掛程式相比，Kaspersky Embedded Systems Security Web 外掛程式具有以下限制：

- 無法使用數位憑證或卡巴斯基安全管理中心事件建立應用程式啟動控制元件規則。
- 無法根據連線的裝置或系統資料產生裝置控制元件規則。

管理應用程式設定

本部分包含有關在卡巴斯基安全管理中心網頁主控台中配置 Kaspersky Embedded Systems Security 一般設定的資訊。

在 Web 外掛程式中配置一般應用程式設定

您可以在 Web 外掛程式中為一組受防護裝置或一台受防護裝置配置 Kaspersky Embedded Systems Security 一般設定。

在 Web 外掛程式配置介面和掃描設定

配置應用程式介面設定：

1. 在網頁主控台的主視窗中，選擇**資產管理 → 政策**。
2. 點擊要設定的政策名稱。
3. 在開啟的 **<政策名稱>** 視窗中，選擇**應用程式設定**頁簽。
4. 選擇 **應用程式設定** 部分。
5. 在 **介面設定** 子部分中點擊 **配置**。
6. 按下表所述配置設定。

使用者互動設定和掃描設定

參數	描述
使用者互動	**不顯示使用者介面**在用戶端電腦上，不顯示 Kaspersky Embedded Systems Security 操作的跡象。Windows 通知區域中的圖示和通知不可用。 **顯示使用者介面**在用戶端電腦上，Windows 托盤中有一個圖示。在該圖示的內容功能表中，使用者可以使用 Kaspersky Embedded Systems Security 執行操作。Kaspersky Embedded Systems Security 還會在應用程式圖示上方顯示通知。Windows 系統匣中圖示的上下文功能表可讓您開啟小型診斷視窗。點擊小型診斷視窗中的連結即可開啟應用程式主控台。
在通知區域顯示應用程式的狀態	選擇您想要在 Microsoft Windows 通知區域中看到通知的事件類型旁的核取方塊。

在 Web 外掛程式中配置安全性和可靠性設定

若要手動設定安全設定，請執行以下步驟：

1. 在網頁主控台的主視窗中，選擇**資產管理 → 政策**。
2. 點擊要設定的政策名稱。
3. 在開啟的 **<政策名稱>** 視窗中，選擇**應用程式設定**頁簽。
4. 選擇 **應用程式設定** 部分。
5. 在 **安全性和可靠性** 子部分中點擊 **配置**。
6. 按下表所述配置設定。

安全性和可靠性設定

參數	描述
在電腦啟動時啟動應用程式（建議）	選中此核取方塊後，將在載入作業系統過後啟動 Kaspersky Embedded Systems Security，從而在整個連線期間防護電腦。 清除此核取方塊後，不會在載入作業系統後啟動 Kaspersky Embedded Systems Security，直到使用者手動啟動此軟體。電腦防護已停用，使用者資料可能受到威脅。
為應用程序防護外來威脅	當選中此方塊時，Kaspersky Embedded Systems Security 可避免修改或刪除磁碟機中的應用程式檔案、記憶體程序和系統登錄中的項目。
防護作業係統服務	如果啟用了作業系統服務防護，則協力廠商應用程式無法對作業系統的處理程序採取行動。 如果停用了作業系統服務防護，則協力廠商應用程式可以對作業系統的處理程序採取行動。
使用電池供電時延遲排程工作	如果選擇該選項，則啟用節能模式。Kaspersky Embedded Systems Security 延遲排程工作。如果需要，您可以手動啟動掃描和更新工作。 啟用節能模式且電腦使用電池執行時，即使排程了以下工作，以下工作也不會執行： • *資料庫和應用程式模組更新* • *完整掃描* • *關鍵區域掃描* • *自訂掃描* • *應用程式完整性控制* • *IOC 掃描*
套用設定時的電腦狀態	套用政策或執行工作出錯時，安裝了 Kaspersky Embedded Systems Security 的用戶端電腦的狀態在網頁主控台中的顯示設定。以下狀態可以使用：*OK*、*警告* 和 *緊急*。

參數	描述
與遠端管理軟體相容	如果將 Kaspersky Embedded Systems Security 與 Remote Administration Tool (RAT) 搭配使用會導致問題，您可以啟用相容模式。這些問題可能與 RAT 和應用程式的「Secure Desktop」功能不相容有關。此功能的目的是確認可能降低電腦安全等級的操作。此功能允許應用程式顯示與其他處理程序隔離的確認對話方塊。此功能使用提升的權限來防護請求。這樣，只有使用者才能確認操作，而惡意軟體無法確認。 如果選擇此選項，則啟用 RAT 相容模式。應用程式會顯示一個沒有此功能的確認對話方塊。這會降低電腦的安全等級。如果 Kaspersky Embedded Systems Security 沒有導致您的 RAT 出現問題，我們不建議啟用相容模式。 如果清除此選項，則停用 RAT 相容模式。預設情況下，會取消勾選核取方塊。 示例：在 RemoteApp 模式中使用瀏覽器時，Kaspersky Embedded Systems Security 在訪問具有不受信任憑證的網站時可能不會顯示確認視窗，因為 RemoteApp 不支援應用程式的安全桌面功能。這可能會導致瀏覽器無響應。為了使瀏覽器在 RemoteApp 模式中正常工作，必須啟用相容模式。 如果您在使用其他協力廠商軟體時遇到安全桌面功能問題，也可以嘗試啟用相容模式。
限制掃描工作的 CPU 使用	Kaspersky Embedded Systems Security 在自訂掃描工作期間將其對受防護裝置 CPU 的使用限制為**上限**欄位中指定的值。 但是，由於其他元件的存在，應用程式可能會使用更多的 CPU 時間。 啟用此功能可能會對 Kaspersky Embedded Systems Security 的效能產生負面影響。 預設情況下會停用此功能。
將資源讓給其他應用程式	Kaspersky Embedded Systems Security 掃描電腦時消耗的電腦資源可能會增加 CPU 和硬碟磁碟機子系統的負載。這可能減緩其他應用程式的速度。為了最佳化效能，Kaspersky Embedded Systems Security 提供了一種將資源傳輸到其他應用程式的模式。在此模式中，當 CPU 負載過高時，作業係統可降低 Kaspersky Embedded Systems Security 掃描工作執行緒的優先順序。這可允許重新分配作業係統資源到其他應用程式。因此，掃描工作將收到更少的 CPU 時間。結果，Kaspersky Embedded Systems Security 將花更多時間來掃描電腦。預設情況下，應用程式已設定為允許其他應用程式使用資源。

在 Web 外掛程式中配置連線設定

設定的連線設定用於將 Kaspersky Embedded Systems Security 連線到更新和啟動伺服器，以及在將應用程式與卡巴斯基安全網路服務整合期間使用。

若要設定連線設定，請執行以下步驟：

1. 在網頁主控台的主視窗中，選擇**資產管理 → 政策**。
2. 點擊要設定的政策名稱。
3. 在開啟的 **<政策名稱>** 視窗中，選擇**應用程式設定**頁簽。
4. 選擇 **應用程式設定** 部分。
5. 在 **連線設定** 子部分中點擊 **配置**。
6. 按下表所述配置設定。

連線設定

參數	描述
連線按流量收費時限制流量	如果選擇該核取方塊，應用程式將在網際網路連線受限時限制其網路流量。Kaspersky Embedded Systems Security 會將高速移動網際網路連線辨識為受限制連線，將 Wi-Fi 連線辨識為無限制連線。 網路數據流量控制可在執行 Windows 8 或更高版本的電腦上使用。
不使用代理伺服器	如果選擇此選項，Kaspersky Embedded Systems Security 將不使用代理伺服器。
自動偵測代理伺服器設定	如果選擇此選項，Kaspersky Embedded Systems Security 將使用作業系統的代理設定。
使用指定的代理伺服器設定	如果選擇此選項，Kaspersky Embedded Systems Security 會使用手動指定的代理伺服器設定。輸入代理伺服器和埠號的 IP 位址或符號名稱

參數	描述
本機位址略過代理伺服器	如果啟用此功能，則會直接透過託管已安裝了 Kaspersky Embedded Systems Security 的受防護裝置的網路存取裝置。預設啟用該選項。
代理伺服器身分驗證設定	若要驗證代理伺服器上的應用程式的網際網路存取權限，您必須輸入使用者的憑據。Kaspersky Embedded Systems Security 支援代理伺服器上的自動身分驗證。如果自動身分驗證失敗，應用程式會提示您輸入憑據。 **不使用身分驗證** **NTLM 身分驗證**使用目前使用者帳戶進行 NTLM 身分驗證（預設）。 **使用使用者名稱和密碼進行 NTLM 身分驗證**使用手動指定的憑據進行 NTLM 身分驗證。 **使用者名稱和密碼**使用手動指定的憑據進行身分驗證。 **Kerberos 身分驗證**使用目前使用者帳戶進行 Kerberos 身分驗證。 若要確保在使用 CNAME 記錄作為代理伺服器位址時 Kerberos 身分驗證正常運作，您必須為每個 CNAME 記錄註冊一個服務主體名稱 (SPN)。 **使用使用者名稱和密碼進行 Kerberos 身分驗證**使用手動指定的憑據進行 Kerberos 身分驗證。 如果選擇 Kerberos 驗證，Kaspersky Embedded Systems Security 可以根據代理伺服器設定使用 Kerberos 或 NTLM 協定執行身分驗證。
監控所有網路連接埠	在此網路連接埠監控模式下，防護元件會監控透過任何開放的電腦網路連接埠傳輸的資料流。
僅監控選定網路連接埠	在此網路連接埠監視模式下，防護元件將監控電腦的選定連接埠和選定應用程式的網路活動。通常用於傳輸電子郵件和網路流量的網路連接埠的清單按照 Kaspersky 專家的建議進行配置。
啟動應用程式時將卡巴斯基安全管理中心作為代理伺服器	指定是否將卡巴斯基安全管理中心用作應用程式啟動的代理伺服器。

在 Web 外掛程式中設定本機工作的排程啟動

您可以使用政策來允許或阻止本機系統隨需掃描工作和更新工作的啟動。這會根據在管理群組中每個受防護裝置上本機配置的排程完成：

- 如果特定類型的本機系統工作的排程啟動受到政策禁止，則這些工作將不會按照排程在受防護裝置上執行。您可以手動啟動該本機系統工作。
- 如果特定類型的本機系統工作的排程啟動被政策允許，則這些工作將按照為此工作進行的本機配置的排程參數來執行。

預設情況下，政策會禁止本機系統工作的啟動。

如果更新或自訂掃描受卡巴斯基安全管理中心群組工作的管理，我們建議不要允許本機系統工作啟動。

如果不使用群組更新或自訂掃描工作，則在政策中允許本機系統工作啟動：Kaspersky Embedded Systems Security 將執行應用程式資料庫和模組更新，並根據預設排程啟動所有本機系統的自訂掃描工作。

您可使用政策允許或封鎖以下本機系統工作的排程啟動：

- 自訂掃描工作：*關鍵區域掃描*、*作業係統啟動時掃描*、*應用程式完整性控制*、*基於基線的系統完整性監控*。
- *更新* 工作。

如果受防護裝置從管理群組中排除，則本機系統工作排程將自動啟用。

要在政策中允許或封鎖 Kaspersky Embedded Systems Security 系統工作的排程啟動：

1. 在網頁主控台的主視窗中，選擇**資產管理 → 政策**。
2. 點擊要設定的政策名稱。
3. 在開啟的 **<政策名稱>** 視窗中，選擇**應用程式設定**頁簽。
4. 選擇 **應用程式設定** 部分。
5. 在 **執行本機系統工作** 子部分中點擊 **配置**。
6. 按下表所述配置設定。

用於啟動本機工作的設定

參數	描述
允許使用本機工作	如果選擇此核取方塊，本機工作將顯示在 Kaspersky Embedded Systems Security 的本機介面上。當沒有其他政策限制時，使用者可以配置並執行工作。不過，配置工作執行排程對於使用者仍然不可用。使用者只能手動執行工作。 如果此核取方塊被清空，則停止使用本機工作。在此模式中，本機工作不根據排程執行。工作無法在 Kaspersky Embedded Systems Security 本機介面中啟動或編輯，使用命令列工作時也無法進行。
允許排程管理	如果選擇了**允許使用本機工作**核取方塊，則此核取方塊可用。 如果選取該核取方塊，則排程管理將在應用程式主控台的本機工作屬性中可用。 預設情況下，會取消勾選核取方塊。
允許顯示群組工作	如果選擇此核取方塊，群組工作將顯示在 Kaspersky Embedded Systems Security 的本機介面上。使用者可以在應用程式主控台中查看所有工作的清單。 如果清除該核取方塊，則 Kaspersky Embedded Systems Security 將顯示空的工作清單。
允許管理群組工作	如果選取該核取方塊，則使用者可以啟動和停止在卡巴斯基安全管理中心中指定的群組工作。使用者可以在應用程式主控台或簡化的應用程式介面中啟動和停止工作。 如果清除該核取方塊，則 Kaspersky Embedded Systems Security 將自動啟動排程工作，或者由管理員在卡巴斯基安全管理中心中手動啟動工作。

在 Web 外掛程式中配置備份設定

在卡巴斯基安全管理中心中管理一般備份設定：

1. 在網頁主控台的主視窗中，選擇**資產管理 → 政策**。
2. 點擊要設定的政策名稱。
3. 在開啟的 **<政策名稱>** 視窗中，選擇**應用程式設定**頁簽。
4. 選擇 **補充** 部分。
5. 在 **儲存** 子部分中點擊 **配置**。
6. 按下表所述配置設定。

儲存設定

參數	描述
在 **報告** 頁簽上，指定報告設定：	
儲存報告不超過	如果選中該核取方塊，則最大報告儲存期限制為定義的時間隔。預設的報告最長儲存期限是 30 天。在此時間之後，Kaspersky Embedded Systems Security 將自動移除報告檔案中的最早項目。

參數	描述
限制報告檔案的大小為	如果選中該核取方塊，則最大報告檔案大小限制為定義值。預設情況下，最大檔案大小資料為 1024 MB。要避免超過最大報告檔案容量，當達到最大報告檔案容量時，Kaspersky Embedded Systems Security 將自動刪除報告檔案中的最早項目。
在 **備份** 頁簽上，指定備份設定：	
儲存物件的時間不超過	如果選中該核取方塊，則最大檔案儲存期限制為定義的時間間隔。預設的檔案最長儲存期限是 30 天。最長儲存期限超出後，Kaspersky Embedded Systems Security 將刪除備份區中最舊的檔案。
備份大小限制為	如果選中該核取方塊，則最大儲存大小限制為定義值。預設情況下，最大大小為 400 MB。為避免超過最大儲存大小，當達到最大儲存大小時，Kaspersky Embedded Systems Security 將自動刪除儲存中的最早檔案。
可用空間的閾值	該核取方塊用於啟用或停用監控備份中的最小可用空間大小（預設值為 100 MB）的功能。如果可用空間大小下降到低於指定上限值，Kaspersky Embedded Systems Security 會記錄"已超過備份區可用空間上限值"事件，並根據此事件類型的通知設定發佈通知。 如果選中該核取方塊，Kaspersky Embedded Systems Security 會監控備份中的可用空間的大小。 如果選擇了**備份大小限制為**核取方塊，則 **可用空間的閾值** 核取方塊處於活動狀態。 預設將會選定該核取方塊。

建立和設定政策

本節提供有關使用卡巴斯基安全管理中心政策在多個受防護裝置上管理 Kaspersky Embedded Systems Security 的資訊。

可以建立全域性卡巴斯基安全管理中心政策，以便管理多個已安裝 Kaspersky Embedded Systems Security 的裝置上的防護。

政策在一個管理群組中所有受防護裝置上強制執行 Kaspersky Embedded Systems Security 設定、功能和指定的工作。

可以為一個管理群組依次建立和實行多個政策。目前對某個群組有效的政策在網頁主控台中處於*啟動*狀態。

Kaspersky Embedded Systems Security 系統稽核記錄中記錄了有關政策實行情況的資訊。該資訊可在應用程式主控台的"**記錄和通知**"節點中檢視。

卡巴斯基安全管理中心提供一種在受防護裝置上套用政策的方式：*禁止變更設定*。T 套用政策後，Kaspersky Embedded Systems Security 會針對在受防護裝置上的政策屬性中的圖示使用您為其選取的設定。在這種情況下，系統會使用所選設定，而不套用政策之前生效的設定。Kaspersky Embedded Systems Security 不會套用在政策內容中選取的圖示所對應的啟動政策設定。

如果政策為啟動的，則政策中標記圖示的設定的值在應用程式主控台中顯示，但無法編輯。其他設定的值（政策中標記圖示）可在應用程式主控台中編輯。

在啟動政策中設定且標記圖示的設定，也會在**屬性：<受防護裝置名稱>**視窗中為個別的受防護裝置封鎖卡巴斯基安全管理中心的變更。

在停用啟動政策後，使用啟動政策指定併傳送到受防護裝置的設定將儲存在本機工作設定中。

如果政策定義目前正在執行的即時電腦防護工作或者網路儲存防護工作的設定，則為該政策定義的設定將在套用該政策後立即變更。如果該工作未執行，就會在啟動時套用其設定。

如何在卡巴斯基安全管理中心網頁主控台中建立政策

1. 在網頁主控台的主視窗中，選擇**資產管理 → 政策**。
2. 點擊**"新增"**。
3. 開啟**"新政策"**視窗。
4. 在**選取應用程式**部分中，選取 Kaspersky Embedded Systems Security。
5. 指定受防護裝置上 Kaspersky Embedded Systems Security 的模式。
6. 如有必要，請指定要從所有或某些應用程式元件的掃描中排除的檔案或資料夾以及物件名稱（根據病毒百科全書）。
7. 在**"一般"**標籤上，可以執行以下操作：
   - 變更政策名稱。

     政策名稱不能包含以下符號：`" * < : > ? \ |` 。
   - 選擇政策狀態：
     - **作用中**下次同步後，該政策將用作電腦上的活動政策。
     - **非作用中**備份政策。如有必要，不活動政策可切換為活動狀態。
     - **漫遊**當電腦離開組織網路周界時，將啟動該政策。
   - 配置設定繼承：
     - **從父政策繼承設定**如果開啟此開關，則政策設定值將從頂級政策繼承。如果為父政策設定了，則無法編輯政策設定。
     - **在子政策中強制繼承設定**如果開啟該切換按鈕，政策設定的值將傳播到子政策。在子政策設定中 **從父政策繼承設定** 核取方塊被自動選取。子政策設定繼承自父政策，除了標記有 的設定外。如果為父政策設定了，則無法編輯子政策設定。
8. 在**應用程式設定**頁簽上，根據需要配置政策設定。
9. 單擊**"儲存"**。

建立新政策後，會建立一組允許規則，防止應用程式遭到封鎖，確保應用程式不間斷地操作。

預設情況下，Kaspersky Embedded Systems Security 會在建立新政策時為傳入網路流量建立一組規則：

- 使用卡巴斯基安全管理中心網路代理程式共用 Windows 桌面之流程的兩個允許規則，這位於 %Program Files% 和 %Program Files (x86)% 資料夾中。狀態：已啟用。允許的外部位址：所有。通訊協定：TCP 和 UDP，每個通訊協定一條規則。
- 本機連接埠 15000 的兩個允許規則。狀態：已啟用。允許的外部位址：所有。通訊協定：TCP 和 UDP，每個通訊協定一條規則。

預設情況下，Kaspersky Embedded Systems Security 會在建立新政策時建立一組傳出網路流量規則：

- Kaspersky Embedded Systems Security 服務的兩個允許規則，這位於 %Program Files% 和 %Program Files (x86)% 資料夾中。狀態：已啟用。允許的外部位址：所有。通訊協定：TCP 和 UDP，每個通訊協定一條規則。
- Kaspersky Embedded Systems Security 之工作者處理程序的兩個允許規則，這位於 %Program Files% 和 %Program Files (x86)% 資料夾中。狀態：已啟用。允許的外部位址：所有。通訊協定：TCP 和 UDP，每個通訊協定一條規則。
- 本機連接埠 13000 的兩個允許規則。狀態：已啟用。允許的外部位址：所有。通訊協定：TCP 和 UDP，每個通訊協定一條規則。

使用卡巴斯基安全管理中心建立和管理工作

本節包含有關 Kaspersky Embedded Systems Security 工作、如何建立工作、配置工作設定，以及啟動和停止工作的資訊。

關於 Web 外掛程式中的工作建立

您可採用以下方式建立本機和群組工作：

- 對於一台受防護裝置：在**屬性 <受防護裝置名稱>**視窗的**工作**部分中。
- 對於管理群組：在選定受防護裝置群組的節點的詳細資訊窗格中的「**工作**」索引標籤上。
- 對於一組受防護裝置：在**裝置分類**節點的詳細資訊窗格中。

您可以使用政策停用同一管理群組中所有受防護裝置上的*更新*和*按需掃描*本機系統工作的排程。

有關卡巴斯基安全管理中心工作的一般資訊，請參閱卡巴斯基安全管理中心說明。

在 Web 外掛程式中建立工作

要在卡巴斯基安全管理中心網頁主控台中建立新工作：

1. 採用以下方式之一啟動工作精靈：
   - 若要建立本機工作，請執行以下步驟：
     a. 在網頁主控台的主視窗中，選擇**資產管理 → 資產（裝置）**。
     b. 點擊受防護裝置的名稱。
     c. 在開啟的 **<裝置名稱>** 視窗中，選擇**工作**頁簽。
     d. 單擊**"新增"**。

- 建立群組工作：

  a. 在網頁主控台的主視窗中，選擇**資產管理** → **工作**。

  b. 點擊**"新增"**。

將開啟工作精靈視窗。

2. 在**應用程式**下拉式清單中，選取 **Kaspersky Embedded Systems Security**。

3. 在**工作類型**下拉式清單中，選取要建立的工作類型。

4. 根據所選的工作類型，執行下列操作之一：

- 建立自訂掃描工作。

- 要建立更新工作，請根據您的需要配置工作設定：

  a. 您可以在**更新來源**區塊中將卡巴斯基安全管理中心管理伺服器或 Kaspersky 更新伺服器指定為應用程式更新來源。您也可以建立自訂更新來源清單：透過手動新增自訂 HTTP 和 FTP 伺服器或網路資料夾，並將他們設定為更新來源。

  如果手動自訂的伺服器無法使用，您可指定使用 Kaspersky 更新伺服器。

  b. 配置可減少磁碟子系統負載的功能設定：

  c. 您可以指定 Kaspersky Embedded Systems Security 在需要關鍵應用程式模組更新時以及關鍵更新安裝完成後將會執行的動作。此外，您也可以指定 Kaspersky Embedded Systems Security 是否接收可用排程更新的資訊。

  d. 指定要複製的更新集合以及 Kaspersky Embedded Systems Security 將用於儲存複製的更新的資料夾的路徑。

- 要建立「應用程式啟動」工作：

  a. 在**"選擇產品授權金鑰"**視窗中，指定您要用來啟動應用程式的金鑰檔案或者啟動碼。

  b. 如果您想要建立用於續約產品授權的工作，請選中**"用作備用金鑰"**核取方塊。

- 建立並設定應用程式啟動控制規則產生器工作。

- 建立並設定裝置控制規則產生器工作。

5. 單擊**"下一步"**。

6. 如果是為一組受防護裝置建立的工作，請選取將執行該工作的受防護裝置網路（或群組）。

7. 單擊**"下一步"**。

8. 如果要配置工作設定，請在 **完成工作建立** 視窗中選擇 **建立完成時開啟工作詳情** 核取方塊。

9. 單擊**"完成"**。

建立的工作將會在**工作**清單中顯示。

在 Web 外掛程式中配置群組工作

要為多個受防護裝置配置群組工作：

1. 在網頁主控台的主視窗中，選擇**資產管理 → 工作**。
2. 點擊卡巴斯基安全管理中心工作清單中的工作名稱。
   將開啟**"<工作名稱>"**視窗。
3. 轉至**應用程式設定**頁簽。
4. 根據配置的工作類型，請執行下列一種操作：
   - 要設定「*按需掃描*」工作：
     a. 在**"掃描範圍"**部分中，配置掃描範圍。
     b. 在**"選項"**部分中，配置啟發式分析等級及與其他應用程式元件的整合。
   - 要設定「*更新*」工作，請根據您的需要調整工作設定：
     a. 在**"更新來源"**部分中，配置更新來源設定。
     b. 在 **更新設定** 部分，管理磁碟子系統最佳化設定，指定在應用程式模組的關鍵更新可用或有關計劃更新的資訊可用時您希望 Kaspersky Embedded Systems Security 執行的操作；指定更新複製設定。
   - 要設定「*應用程式啟動*」工作，請套用您要用於啟動應用程式的金鑰檔案或者啟動碼。如果您想要新增用於續約產品授權的啟動碼或金鑰檔案，請選中**"用作備用金鑰"**核取方塊。
   - 要配置裝置控制允許規則的自動產生，請指定將用於建立允許規則清單的設定。
5. 在**排程**區域中設定工作排程（您可以為除*更新回溯*以外的所有工作類型設定排程）。
6. 在「**帳戶**」區域的「**設定**」索引標籤上，指定將使用其權限執行工作的帳戶。關於此節中配置設定的詳細資訊，請參閱卡巴斯基安全管理中心說明。
7. 單擊**"儲存"**。

將儲存新配置的群組工作設定。

在 Web 外掛程式中設定應用程式啟動工作

要設定應用程式啟動工作：

1. 在網頁主控台的主視窗中，選擇**資產管理 → 工作**。
2. 點擊卡巴斯基安全管理中心工作清單中的工作名稱。
   將開啟**"<工作名稱>"**視窗。

3. 在“**應用程式設定**”部分中，指定您要用來啟動應用程式的金鑰檔案。如果您想要新增用於續約產品授權的金鑰，請選中**用作備用金鑰**核取方塊。

4. 在“**排程**”部分中配置工作排程。

5. 在**<工作名稱>** 視窗中點擊**儲存**按鈕。

在 Web 外掛程式中配置更新工作

要設定更新工作：

1. 在網頁主控台的主視窗中，選取“**裝置**”→“**工作**”。

2. 點擊卡巴斯基安全管理中心工作清單中的工作名稱。

   “<工作名稱>”視窗將開啟。

3. 選擇“**應用程式設定**”標籤。

4. 在“**更新來源**”部分中，配置更新來源設定：

   a. 將卡巴斯基安全管理中心管理伺服器或 Kaspersky 更新伺服器指定為應用程式更新來源。您也可以建立自訂更新來源清單：透過手動新增自訂 HTTP 和 FTP 伺服器或網路資料夾，並將他們設定為更新來源。

   如果手動自訂的伺服器無法使用，您可指定使用 Kaspersky 更新伺服器。

   b. 配置可減少磁碟子系統負載的功能設定：

   - **降低磁碟 I/O 上的負載**
   - **用於最佳化的 RAM (MB)**

   c. 指定當應用程式模組的關鍵更新可用或有關於已計劃更新的資訊時 Kaspersky Embedded Systems Security 應執行的操作。

   d. 指定更新複製設定。

5. 在**排程**區域中設定工作排程（您可以為除*更新回溯*以外的所有工作類型設定排程）。

6. 在“**<工作名稱>**”視窗中，點擊“**確定**”。

排程工作

您可以在網頁主控台中排程本機系統和自訂工作。

要使用網頁主控台排程群組工作，請執行以下操作：

1. 在網頁主控台的主視窗中，選擇**資產管理 → 工作**。

2. 點擊卡巴斯基安全管理中心工作清單中的工作名稱。

   將開啟“**<工作名稱>**”視窗。

3. 轉到 **排程** 部分並根據需要配置排程設定（請參閱下表）。

如果卡巴斯基安全管理中心政策封鎖自訂掃描工作和更新工作的排程，則這些工作的排程設定的欄位無法使用。

4. 點擊**"儲存"**按鈕儲存工作啟動設定。

工作排程設定

參數	描述
排程開始	選擇工作執行模式： • **每 N 小時**該工作將每隔幾個小時定期執行。請指定工作的開始時間和持續時間（以小時為單位）。 • **每 N 天**該工作將每隔幾天定期執行。請指定工作的開始時間和持續時間（以天為單位）。 • **每 N 分鐘**該工作將每隔幾分鐘定期執行。請指定工作的開始時間和持續時間（以分鐘為單位）。 • **按每週中的指定日**工作將在指定的星期幾執行。選取星期幾並指定開始時間。如果需要每隔數週執行工作，請在 **間隔** 欄位中輸入所需的值。 • **每月**該工作將在每月特定日期執行。請指定開始日期和時間。 • **一次**該工作將在指定的日期和時間執行一次。 • **手動**執行模式，您可以在方便時手動開始掃描。 • **當新更新下載至儲存區時**每次向儲存庫下載更新時，該工作都會執行。 • **在完成其它工作時**該工作將在另一個工作完成後執行。選擇工作及其完成狀態。 Kaspersky Embedded Systems Security 不支援使用 **在完成其它工作時** 模式排程本機工作。 • **在偵測到病毒爆發時**如果偵測到病毒攻擊，該工作將執行。 • **在應用程式啟動後 N 分鐘啟動**每次 Kaspersky Embedded Systems Security 啟動時，該工作都會在指定的時間段後執行。請在 **工作啟動延遲（分鐘）** 欄位中指定分鐘數。
執行錯過的工作	如果選中此核取方塊，Kaspersky Embedded Systems Security 將在可能的情況下儘快啟動已略過的工作。工作在某些情況下可能被略過，例如，電腦在排程的工作啟動時關閉。當應用程式有機會執行錯過的工作時，它會在一定的時間間隔內隨機執行工作，以分配電腦上的負載。 如果清除此核取方塊，Kaspersky Embedded Systems Security 不會執行已略過的工作。它將按照目前排程執行下一次工作。
使用工作啟動自動隨機化延遲	如果選取此核取方塊，則該工作將在特定時間範圍內的隨機時間在電腦上執行。隨機開始時間有助於避免當工作按照排程執行時，大量電腦同時存取管理伺服器。 如果清除該核取方塊，則工作會準確在排程的時間執行。
對於在以下間隔內啟動的工作，使用工作啟動自動隨機化延遲	如果選取此核取方塊，則該工作將在特定時間範圍內的隨機時間在電腦上執行。隨機開始時間有助於避免當工作按照排程執行時，大量電腦同時存取管理伺服器。 如果清除該核取方塊，則工作會準確在排程的時間執行。
在啟動工作之前，使用 Wake-On-LAN 功能開啟裝置	如果選擇此核取方塊，則電腦的作業系統會被給與指定的前置重疊時間以在執行工作前完成啟動。預設前置重疊時間為 5 分鐘。 如果您希望在包括關機電腦在內的所有電腦上執行工作，請選擇此核取方塊。
完成工作後將裝置關機	如果選取此核取方塊，電腦將在工作完成後關機。 例如，您可以啟用此功能以在周五下班後掃描電腦。工作完成後，應用程式會在週末關閉電腦。
停止工作，若執行時間超過	限制工作執行時間。超出指定時間後，Kaspersky Embedded Systems Security 將停止工作。工作未標記為已完成。下次 Kaspersky Embedded Systems Security 執行該工作時，它將從頭開始按排程執行。
暫停工作執行	您可以指定暫停執行先前已排程工作的時間間隔。指定時間段結束後，工作將還原。例如，為了最大限度地減少 Kaspersky Embedded Systems Security 在高峰使用期間對電腦效能的影響，這樣做可能是必要的。 此功能僅適用於自訂掃描工作。
結束日期	如果選取此核取方塊，Kaspersky Embedded Systems Security 將從指定日期開始停止執行已排程工作。工作將設定為 **手動** 模式。 此功能僅適用於自訂掃描工作。

卡巴斯基安全管理中心中的報告

卡巴斯基安全管理中心中的報告包含有關受管理裝置狀態的資訊。報告基於管理伺服器上儲存的資訊。

從卡巴斯基安全管理中心11 開始，對於 Kaspersky Embedded Systems Security，以下類型的報告可用：

- 有關應用程式元件狀態的資訊
- 有關已禁止的應用程式的報告
- 有關在測試模式下禁止的應用程式的報告

有關所有卡巴斯基安全管理中心報告以及如何配置它們的詳細資訊，請參見卡巴斯基安全管理中心說明。

有關 Kaspersky Embedded Systems Security 元件狀態的報告

您可以監視所有網路裝置的防護狀態，並獲得每個裝置上的元件集的結構化概覽。

報告顯示每個元件的以下狀態之一：*正在執行*、*已暫停*、*已停止*、*產品授權不支援*。

*未安裝*狀態指的是元件，而不是應用程式本身。如果未安裝應用程式，卡巴斯基安全管理中心網頁主控台會分配 N/A（無法使用）狀態。

您可以建立元件選擇並使用篩選來顯示具有指定元件集和狀態的網路裝置。

有關建立和使用選擇的詳細資訊，請參閱卡巴斯基安全管理中心說明。

若要在卡巴斯基安全管理中心網頁主控台中檢視元件的狀態：

1. 在網頁主控台的主視窗中，選擇**資產（裝置）→受管理裝置**。
2. 點選裝置名稱然後轉至**應用程式**部分。
3. 點擊 Kaspersky Embedded Systems Security 的應用程式名稱。
4. 在開啟的視窗中的 **一般**頁簽上，點擊 **元件** 部分。
5. 檢視狀態表。

要在卡巴斯基安全管理中心網頁主控台中查看標準報告：

1. 選擇"**監控 → 報告**"。
2. 在清單中，選取 **應用程式元件狀態報告** 並按一下。
   將產生報告。
3. 檢視以下報告詳細資訊：
   - 圖形化圖表。
   - 元件和安裝了每個元件的網路裝置總數以及裝置所屬的組的匯總表格。
   - 指定了元件狀態、版本、裝置和群組的詳細表格。

有關在啟動模式和測試模式下禁止的應用程式的報告

根據應用程式啟動控制工作的結果，可以產生兩種類型的報告：有關已禁止的應用程式的報告（如果在啟動模式下啟動該工作）和有關在測試模式下禁止的應用程式的報告（如果在"通知"模式下啟動該工作）。這兩種報告顯示了有關網路的受防護裝置上封鎖的應用程式的資訊。每個報告都針對所有管理組產生，並累積來自受防護裝置上安裝的所有 Kaspersky 應用程式的資料。

要檢視有關在"通知"模式下禁止的應用程式的報告：

1. 以通知模式執行應用程式啟動控制工作。
2. 選擇"**監控 → 報告**"。
3. 在清單中，選取 **測試模式中禁止的應用程式報告** 並按一下。
   將產生報告。
4. 檢視以下報告詳細資訊：
   - 顯示封鎖啟動次數最多的前10 個應用程式的圖形化圖表。
   - 應用程式封鎖行為的匯總表格，其中指定可執行檔名稱、原因、封鎖時間和發生封鎖的裝置數量。
   - 指定了有關裝置、檔案路徑和封鎖條件的資料的詳細表格。

要檢視有關在啟動模式下禁止的應用程式的報告：

1. 運行 應用程式啟動控制 任務 積極的 模式。
2. 選擇"**監控 → 報告**"。
3. 在清單中，選取 **禁止的應用程式報告** 並按一下。
   將產生報告。

此報告包含的封鎖資料與有關在測試模式下禁止的應用程式的報告相同。

應用程式產品授權

本章節提供與應用程式產品授權有關的主要概念的資訊。

關於最終使用者產品授權協議

*最終使用者產品授權協議*是您和 AO Kaspersky Lab 之間達成的約束協議，它規定了您在使用所購買的軟體時須遵循的條款。

請仔細檢視最終使用者產品授權協議的條款，然後再開始使用程式。

您可以透過以下方式閱讀描述資料處理和傳輸的最終使用者產品授權協議和隱私權政策的條款：

- 在安裝 Kaspersky Embedded Systems Security 主控台期間。
- 在安裝 Kaspersky Embedded Systems Security 主控台期間。
- 透過閱讀分發套件中包含的檔案 license.txt 文件。
- 在卡巴斯基網站 (https://www.kaspersky.com/business/eula)上。

安裝程式時確認您同意最終使用者產品授權協議即表示您同意最終使用者產品授權協議中的條款。如果您不接受最終使用者產品授權協議的條款，則必須中止程式安裝，且不得使用程式。

關於產品授權

A *產品授權*是根據使用者產品授權協議在有限時間內授予使用本程式的權利。

有效的產品授權讓您有權根據最終使用者產品授權協議的條款使用該應用程式，並在必要時獲得技術支援。

服務範圍和應用程式的使用期限取決於用於啟動應用程式時使用的產品授權類型。

您可以兩種方式啟動應用程式：

- 使用金鑰檔案，授予您商業產品授權的使用權
- 使用啟動碼購買商用版產品授權

正式版產品授權到期後，只有以下應用程式元件和工作無需資料庫更新即可繼續使用：

- 即時檔案防護
- 系統完整性監控
- 自訂掃描工作

若要繼續使用 Kaspersky Embedded Systems Security 的所有功能，您必須續約您的正式版產品授權。建議在產品授權到期前延長其有效期，以確保最大程度的防護。

如果移除產品授權金鑰，應用程式將繼續執行。系統完整性監控元件仍然可用，其餘元件、工作和 Kaspersky Embedded Systems Security 資料庫更新均不可用。如果卡巴斯基將您的產品授權新增到拒絕清單，也會發生同樣的情況。

關於產品授權憑證

產品授權憑證 是傳送給使用者的一個帶有金鑰檔案或啟動碼的檔案。

產品授權憑證包含以下產品授權資訊：

- 產品授權 ID 或訂單號。
- 被授予產品授權的使用者詳情。
- 可以使用產品授權啟動的應用程式詳情。
- 授權單元的數量限制（例如，可以在此產品授權下使用應用程式的裝置數量）。
- 產品授權期限開始日期。
- 產品授權到期日期或產品授權期限。
- 產品授權類型。

關於金鑰

*金鑰*是一串位元資料，您可以依照最終使用者產品授權協議的條款，透過該金鑰來啟動並在啟動後使用程式。金鑰是由 Kaspersky 建立的。

您可以使用金鑰檔案或者啟動碼向應用程式新增金鑰。在應用程式中新增金鑰後，將在應用程式介面中以唯一的字母數字序列形式顯示。

由於違反產品授權協議，卡巴斯基可以將金鑰新增到拒絕清單中。如果封鎖了您的金鑰，則必須新增其他金鑰以使應用程式正常工作。

有兩種類型的金鑰：啟動金鑰和備用金鑰。

*啟動金鑰*是程式目前正在使用的金鑰。可以將正式產品授權的金鑰新增為啟動金鑰。本應用程式不能擁有兩個及以上啟動金鑰。

*備用金鑰*使用者可新增一組目前尚未使用的金鑰。在與目前啟動金鑰關聯的產品授權到期時，備用金鑰將自動變為啟動金鑰。在目前已有金鑰啟用下才能新增備用金鑰。

關於金鑰檔案

*金鑰檔案*是您從 Kaspersky 接收到的 .key 副檔名的檔案。金鑰檔案的目的是新增能夠啟動應用程式的產品授權金鑰。

購買 Kaspersky Embedded Systems Security，您會在指定的電子郵件地址收到一個金鑰檔案。

您不需要連線到 Kaspersky 啟動伺服器，即可利用金鑰檔案啟動應用程式。

如果金鑰檔案被意外刪除，則您可以還原它。您可能需要金鑰檔案註冊諸如卡巴斯基公司帳戶之類的服務。

若要還原金鑰檔案，請執行以下操作：

- 聯絡產品授權銷售商。
- 基於您現有的啟動碼在 Kaspersky 網站上 獲得金鑰檔案。

關於啟動碼

*啟動碼*是由 20 個字母和數字組成的唯一序列。您必須輸入啟動碼才能新增用於啟動 Kaspersky Embedded Systems Security 的金鑰。在購買 Kaspersky Embedded Systems Security 之後，您指定的電子郵件地址會收到啟動碼。

要用啟動碼啟動應用程式，需要網際網路接入連線到 Kaspersky 的啟動伺服器。

如果您在安裝應用程式後遺失了啟動碼，可以將其還原。例如，您可能需要啟動碼才能註冊 Kaspersky CompanyAccount。若要恢復您的啟動碼，請聯絡您購買產品授權的 Kaspersky 合作夥伴。

依據產品授權類型對比應用程式功能

Kaspersky Embedded Systems Security 功能集合取決於產品授權類型（請參閱下表）。

Kaspersky Embedded Systems Security 功能比較

功能	Kaspersky Embedded Systems Security	Kaspersky Embedded Systems Security 合規版
即時檔案防護	✓	✓
按需掃描	✓	✓
應用程式啟動控制	✓	✓
裝置控制	✓	✓
防火牆	✓	✓
檔案完整性監控	–	✓
記錄審查	–	✓

使用金鑰檔案啟動應用程式

您可以套用金鑰檔案啟動 Kaspersky Embedded Systems Security。

要使用金鑰檔案啟動 Kaspersky Embedded Systems Security：

1. 在應用程式主控台樹狀目錄中，展開**"產品授權"**節點。
2. 在**產品授權**節點的結果窗格中，點擊**新增金鑰**連結。
3. 在開啟的視窗中，點擊**"瀏覽"**按鈕。
4. 選擇具有 .key 副檔名的授權檔案。

   還可以新增金鑰作為備用金鑰。若要新增金鑰作為附加金鑰，請選中**"用作備用金鑰"**核取方塊。

5. 單擊**"確定"**。

將會套用選定的金鑰檔案。在這種情況下：

- 如果已經新增了啟動金鑰以啟動應用程式，並且您又另外新增一個金鑰作為啟動金鑰，則新金鑰會替換之前新增的金鑰。之前新增的金鑰將被刪除。
- 如果已經新增了備用金鑰以啟動應用程式，並且您又另外新增一個金鑰作為備用金鑰，則新金鑰會替換之前新增的金鑰。之前新增的備用金鑰會被刪除。
- 如果已經新增了啟動金鑰和備用金鑰以啟動應用程式，並且您又另外新增一個新金鑰作為啟動金鑰，則新金鑰會替換之前新增的啟動金鑰；備用金鑰不會被刪除。

"產品授權"節點將提供有關新增的金鑰的資訊。

使用啟動碼啟動應用程式

要使用啟動碼啟動應用程式，受防護裝置必須連線到網際網路。

您可以使用啟動碼啟動 Kaspersky Embedded Systems Security。

使用此方法啟動應用程式時，Kaspersky Embedded Systems Security 將資料傳送到啟動伺服器來驗證所輸入的代碼：

- 如果啟動碼驗證成功，應用程式將啟動。
- 如果啟動碼驗證失敗，將顯示相應通知。在這種情況下，您必須聯絡向您銷售 Kaspersky Embedded Systems Security 產品授權的軟體供應商。
- 如果已超過啟動碼的啟動數量，將顯示相應通知。應用程式啟動過程中斷，應用程式會提示您聯絡技術支援。

您可以使用應用程式主控台以啟動碼，或透過管理外掛程式或 Web 外掛程式建立「*應用程式啟動*」群組工作來啟動 Kaspersky Embedded Systems Security。

要使用應用程式主控台使用啟動碼來啟動 Kaspersky Embedded Systems Security，請執行以下操作：

1. 在應用程式主控台樹狀目錄中，展開**"產品授權"**節點。
2. 在**產品授權**節點的結果窗格中，點擊**新增啟動碼**連結。
3. 在開啟的視窗**"啟動碼"**欄位中輸入啟動碼。
   - 如果要將啟動碼用作備用金鑰，請選擇**"用作備用金鑰"**核取方塊。
   - 若要檢視關於產品授權的資訊，按一下**顯示產品授權資訊**按鈕。該資訊將顯示在**產品授權資訊**區塊中。
4. 單擊**"確定"**。

   Kaspersky Embedded Systems Security 會將有關套用的啟動碼的資訊傳送到啟動伺服器。

檢視有關目前產品授權的資訊

檢視產品授權狀態

有關目前產品授權狀態的資訊顯示在應用程式主控台的 **Kaspersky Embedded Systems Security** 節點的詳細資訊窗格中。產品授權狀態可能有以下值：

- **正在檢查金鑰狀態。** – Kaspersky Embedded Systems Security 正在檢查新增的金鑰檔案，等待有關目前狀態的回應。
- **到期日期** – Kaspersky Embedded Systems Security 已啟動，在指定日期之前有效。在以下情況下，狀態突出顯示為黃色：
  - 產品授權將在 30 天後到期，並且未新增任何備用金鑰。
  - 新增金鑰已新增至拒絕清單且將被封鎖。
- **應用程式未啟動。** – Kaspersky Embedded Systems Security 未啟動，因為尚未新增金鑰。狀態紅色醒目提示。
- **產品授權已到期。** – 由於產品授權已到期，Kaspersky Embedded Systems Security 未啟動。狀態紅色醒目提示。
- **違反了最終使用者產品授權協議。** – Kaspersky Embedded Systems Security 未啟動，因為違反了最終使用者產品授權協議的條款。狀態紅色醒目提示。
- **金鑰在拒絕清單上。** – 新增的金鑰檔案已被卡巴斯基封鎖並列入拒絕清單，例如，金鑰被協力廠商用來非法啟動應用程式。狀態紅色醒目提示。

檢視有關目前產品授權的資訊

要檢視有關目前產品授權的資訊，

在應用程式主控台樹狀目錄中，展開**"產品授權"**節點。

有關目前產品授權的一般資訊顯示在**"產品授權"**節點的詳細資訊視窗中（請參見下表）。

"授權"節點中有關產品授權的一般資訊

欄位	描述
啟動碼狀態或金鑰狀態	啟動碼狀態或金鑰狀態：*啟動金鑰* 或者 *備用*。
到期日期	與啟動金鑰相關聯的產品授權的到期日期和時間。
產品授權類型	產品授權類型。*正式版產品授權*。
啟動狀態	啟動狀態資訊可以採用以下值： • **已套用** – 如果您已使用金鑰啟動了應用程式。 • **應用程式啟動** – 如果您已套用啟動碼啟動應用程式，但啟動過程尚未最終完成。應用程式啟動完成並且節點的詳細資訊窗格的內容重新整理後，狀態變更為**"已套用"**。 • **啟動錯誤** – 如果應用程式啟動失敗。您可在工作記錄中檢視啟動不成功的原因。
金鑰	您用來啟動應用程式的金鑰號碼。

要檢視有關產品授權的詳細資訊，

在**"產品授權"**節點的詳情窗格中，開啟您想要檢視的產品授權的內容功能表，然後選擇**內容**。

屬性<Key number>視窗中的詳細產品授權資訊

欄位	描述
金鑰	您用來啟動應用程式的金鑰號碼。
應用程式	使用新增的金鑰啟動的應用程式的名稱。
產品授權類型	產品授權類型：正式或試用。
產品授權期限	從應用程式啟動日期開始、產品授權有效的天數。
啟動日期	金鑰新增到應用程式的日期。
到期日期	與啟動金鑰相關聯的產品授權的到期日期。如果在無期限訂購下啟動應用程式，此欄位的值為*無期限*。如果 Kaspersky Embedded Systems Security 無法確定產品授權到期日期，則此欄位的值設定為*未知*。
到期剩餘天數	與啟動金鑰相關的產品授權在到期前剩餘的天數。
符合技術支援需求	有關卡巴斯基或其合作夥伴是否會根據產品授權條款為客戶提供技術支援的資訊。
支援資訊	Kaspersky 或其提供技術支援的合作夥伴的聯絡人詳細資訊。如果不提供技術支援，則此欄位可為空。
所有者資訊	有關產品授權客戶的資訊：客戶名稱和獲取產品授權的組織的名稱。
產品授權資訊	目前產品授權的號碼和類型。
功能	在產品授權下提供的應用程式功能。

續約產品授權

預設情況下，當產品授權距離到期還剩 30 天時，Kaspersky Embedded Systems Security 會通知您。

您可以在到期日期前使用備用金鑰續約產品授權。這可確保在目前產品授權到期後和您使用新的產品授權啟動應用程式之前繼續防護您的裝置。

要續約產品授權：

1. 獲取新的啟動碼或金鑰檔案。
2. 在應用程式主控台樹狀目錄中，選擇**"產品授權** 節點。
3. 在**"產品授權"**節點的結果窗格中執行以下操作之一：
   - 如果您想要使用金鑰檔案續約產品授權：
     a. 點擊**"新增金鑰"**連接。
     b. 在開啟的視窗中，點擊**"瀏覽"**按鈕。
     c. 選擇具有 .key 副檔名的新金鑰檔案。
     d. 選擇**"用作備用金鑰"**核取方塊。
   - 如果您想要使用啟動碼續約產品授權：
     a. 點擊**"新增啟動碼"**連接。
     b. 在開啟的視窗中輸入購買的啟動碼。
     c. 選擇**"用作備用金鑰"**核取方塊。

     套用啟動碼需要網際網路連線。
4. 單擊**"確定"**。

目前 Kaspersky Embedded Systems Security 產品授權到期後，會新增並自動套用備用金鑰。

刪除金鑰

如果您刪除所新增的金鑰，則可以透過重新套用金鑰檔案來將其還原。

若要刪除先前新增的鍵：

1. 在應用程式主控台樹狀目錄中，選擇**"產品授權** 節點。
2. 在包含有關已新增金鑰的資訊的表格中的**"產品授權"**節點的結果窗格中，選擇您要刪除的金鑰。
3. 在包含有關所選金鑰的資訊的行的內容功能表中，選擇**"刪除"**。
4. 在確認視窗中點擊**"是"**按鈕以確認您希望刪除該金鑰。

選定的金鑰將被刪除。

啟動和停止 Kaspersky Embedded Systems Security

本節包含有關啟動和停止 Kaspersky Embedded Systems Security 以及有關啟動 Kaspersky Embedded Systems Security 主控台和卡巴斯基安全管理中心管理主控台的管理外掛程式的資訊。

啟動和停止應用程式

將 Kaspersky Embedded Systems Security 安裝到使用者的電腦後，該應用程式會自動啟動。預設情況下，Kaspersky Embedded Systems Security 在作業系統啟動後啟動。在作業系統設定中無法設定應用程式的自動啟動。

在作業系統啟動後下載 Kaspersky Embedded Systems Security 病毒資料庫最多可能需要兩分鐘，具體取決於電腦的功能。在該期間電腦防護等級降低。在已啟動的作業系統上啟動 Kaspersky Embedded Systems Security 時，下載病毒資料庫不會導致電腦防護等級降低。

如何在卡巴斯基安全管理中心管理主控台中設定應用程式自動啟動

1. 在卡巴斯基安全管理中心管理主控台樹狀目錄中，選取**政策**。
2. 選擇必要的政策並點擊以開啟政策內容。
3. 在政策視窗中，選擇 **應用程式設定 → 安全性和可靠性** 然後點擊 **設定**。
4. 在“**安全**”頁簽上，選擇或者清除“**在電腦啟動時啟動應用程式（建議）**“核取方塊來啟用或停用應用程式自動執行。
5. 儲存變更。

如何在卡巴斯基安全管理中心網頁主控台中設定應用程式自動啟動

1. 在網頁主控台的主視窗中，選擇**資產管理 → 政策**。
2. 點擊 Kaspersky Embedded Systems Security 政策的名稱。
   政策內容視窗將開啟。
3. 選擇“**應用程式設定**”標籤。
4. 轉到”**應用程式設定**”→”**安全性和可靠性**”。
5. 點擊“**配置**”。
   開啟“**安全性和可靠性**”視窗。
6. 使用“**在電腦啟動時啟動應用程式（建議）**“核取方塊可以啟用或停用對應用程式自動啟動。
7. 儲存變更。

如何在應用程式主控台中配置應用程式自動啟動

1. 在應用程式主控台樹狀目錄中，選擇"**Kaspersky Embedded Systems Security**"節點。
2. 在節點的內容功能表中選擇**應用程式內容**。
3. 這會開啟一個視窗；在該視窗中，選擇**安全設定**頁簽。
4. 使用"**在電腦啟動時啟動應用程式（建議）**"核取方塊可以啟用或停用對應用程式自動啟動。
5. 儲存變更。

如果您是受防護裝置上"管理員"群組的成員，您可以啟動和停止 Kaspersky Embedded Systems Security。

如何在卡巴斯基安全管理中心管理主控台中啟動或停止應用程式

1. 在管理主控台樹狀目錄的"**受管理裝置**"資料夾中，開啟相關用戶端電腦所屬的管理群組名稱的資料夾。
2. 在工作區選取"**裝置**"標籤。
3. 點擊以開啟電腦內容視窗。
4. 在電腦內容視窗中，選取"**應用程式**"區域。
5. 在電腦上安裝的卡巴斯基應用程式清單中，選擇"**Kaspersky Embedded Systems Security for Windows (4.0.1)**"。
6. 執行以下操作之一：
   - 要啟動應用程式，請點擊 Kaspersky 應用程式清單右側的 按鈕。
   - 要停止應用程式，請點擊 Kaspersky 應用程式清單右側的 按鈕。

如何在卡巴斯基安全管理中心網頁主控台中啟動或停止應用程式

1. 在網頁主控台的主視窗中，選擇**資產管理 → 資產（裝置）**。
2. 點擊您要在其上啟動或停止 Kaspersky Embedded Systems Security 的電腦的名稱。
   電腦內容視窗將開啟。
3. 選擇"**應用程式**"標籤。
4. 選擇 **Kaspersky Embedded Systems Security for Windows (4.0.1)** 對面的核取方塊。
5. 點擊"**開始**"或"**停止**"按鈕。

如何在應用程式主控台中啟動或停止應用程式

1. 若要停止 Kaspersky Embedded Systems Security：

   a. 開啟應用程式主控台。

   > 使用者帳戶必須擁有權限，才能存取 **結束應用程式** 功能。

   b. 在應用程式主控台樹狀目錄中，開啟**"Kaspersky Embedded Systems Security"**節點的內容功能表。

   c. 選擇**"停止應用程式"**。

   d. 在確認視窗中，點擊 **是** 按鈕以確認停止應用程式。
   應用程式將會停止。

2. 若要啟動 **Kaspersky Embedded Systems Security**：

   a. 在受防護裝置上的應用程式主控台安裝資料夾中執行 avpui.exe 檔案。預設情況下，該檔案位於 C:\Program Files (x86)\Kaspersky Lab\Kaspersky Embedded Systems Security Console 資料夾中。
   開啟**"選擇受防護的裝置"**視窗。

   b. 如果 Kaspersky Embedded Systems Security 和應用程式主控台安裝在同一台電腦上，請選擇 **本機電腦（應用程式主控台在其上執行的電腦）**。

   c. 如果 Kaspersky Embedded Systems Security 和應用程式主控台安裝在不同的電腦上：

      1. 選擇**"其它裝置"**。
      2. 點選 **瀏覽** 並指定安裝該應用程式的電腦的名稱。
      3. 指定用於連線至已安裝應用程式之電腦的連接埠：

         - **使用 Windows 憑證**用於使用 Windows 認證資料進行連線的連接埠。預設值為 13032。
         - **使用手動建立的使用者的憑證**供手動建立的使用者使用認證資料進行連線的連接埠。預設值為 13031。

   d. 如有必要，請啟用 **使用身分驗證** 功能，並輸入認證資料，以將應用程式主控台連線至安裝了應用程式的電腦。指定的使用者帳戶必須擁有權限，才能存取安裝了應用程式之電腦上的 **讀取設定** 和 **遠端連線到應用程式** 功能。

   e. 單擊**"應用程式管理服務"**。

   f. 在開啟的視窗中，點擊**"開始"**按鈕。
   應用程式將會啟動。

> 如果與安裝應用程式的電腦的連線遺失或 KESS 服務失敗，也會顯示**選擇受防護的裝置**視窗。您可以透過點擊 **啟動** 按鈕還原 KESS 服務。

您也可以透過命令列啟動或停止應用程式。

暫停和還原電腦防護和控制

暫停電腦防護和控制表示停用 Kaspersky Embedded Systems Security 的所有防護和控制元件一段時間。

應用程式狀態使用工作列通知區域中應用程式圖示進行顯示。

- 圖示表示電腦防護和控制已暫停。
- 圖示表示電腦防護和控制已啟用。

暫停或還原電腦防護和控制不影響掃描工作或程式更新工作。

如果在暫停或還原電腦防護和控制時已建立任何網路連線，系統會顯示關於終止這些網路連線的通知。

暫停電腦防護和控制：

1. 在應用程式主控台樹狀目錄中，開啟"**Kaspersky Embedded Systems Security**"節點的內容功能表。
2. 選擇"**暫停防護**"。
3. 從以下選項中選取一個選項：
   - **暫停防護時間 <時間段>** – 經過下面的下拉清單中所指定的時間後將還原電腦防護和控制。
   - **重新啟動程式後還原防護** – 重新啟動應用程式或重新啟動作業系統後還原電腦防護和控制。若要使用此選項，必須啟用應用程式的自動啟動。
   - **暫停** – 在您決定重新啟用時將還原電腦防護和控制。

Kaspersky Embedded Systems Security 將暫停政策中不帶鎖標記 () 的所有防護和控制元件的執行。

還原電腦防護和控制：

1. 開啟位於工作列通知區域的應用程式圖示的上下文功能表。
2. 在內容功能表中，選取"**還原防護**"。

如果您決定還原電腦防護和控制，可以隨時進行該操作，這與您之前選取的防護暫停選項無關。

小型診斷視窗

本節介小型診斷視窗的使用。

關於小型診斷視窗

“小型診斷視窗”元件連同“系統托盤圖示”元件獨立於應用程式主控台安裝和解除安裝，可在受防護裝置上未安裝應用程式主控台時使用。小型診斷介面透過系統托盤圖示啟動，或執行受防護裝置上的應用程式資料夾中的 avpui.exe 以啟動。

在小型診斷介面中，您可以執行以下操作：

- 開啟含有已安裝更新和可用修補程式清單的“**關於**”視窗。
- 檢閱有關一般應用程式狀態的資訊。
- 檢視已發生的安全事件。
- 檢閱受防護裝置上的目前活動。
- 啟動或停止寫入 Dump 和偵錯檔案。
- 開啟應用程式主控台。

即使對 Kaspersky Embedded Systems Security 功能的存取受密碼防護，小型診斷介面仍然可用。無需任何密碼。

小型診斷介面元件不能透過卡巴斯基安全管理中心進行配置。

透過小型診斷視窗檢視 Kaspersky Embedded Systems Security 狀態

若要使用小型診斷視窗檢視應用程式狀態：

1. 採用以下方式之一開啟小型診斷視窗：
   - 執行受防護裝置上應用程式安裝資料夾中的 avpui.exe 檔案。預設情況下，該檔案位於 C:\Program Files (x86)\Kaspersky Lab\Kaspersky Embedded Systems Security.4.1.0。
   - 點擊工作列通知區域中的應用程式圖示。
2. 在“**防護狀態**”部分中檢視金鑰、即時電腦防護工作和更新工作的目前狀態。使用不同的顏色來向使用者通知防護狀態（參見下表）。

小型診斷視窗中的顏色指示

部分	狀態
即時防護狀態	如果滿足以下條件，面板呈*綠色*： • 即時檔案防護元件已啟用。 • 應用程式啟動控制 元件正在**封鎖**模式下執行。
	如果滿足以下一個或多個條件，面板呈*黃色*： • 即時檔案防護元件已停用。 • 應用程式啟動控制 元件正在**通知**模式下執行。
	如果同時滿足以下兩個條件，面板呈*紅色*： • 即時檔案防護 元件已停用或未安裝。 • 應用程式啟動控制元件未安裝或在**"通知"**模式下執行。
產品授權	如果目前產品授權有效，面板呈*綠色*。
	*黃色*面板表示發生以下事件之一： • *檢查產品授權狀態。* • *產品授權將在 14 天後到期，且未新增備用金鑰或啟動碼。* • *新增金鑰已新增至拒絕清單且將被封鎖。*
	*紅色*面板表示發生以下事件之一： • *應用程式未啟動。* • *產品授權已到期。* • *違反了最終使用者產品授權協議。* • *金鑰在拒絕清單上。*
更新	應用程式資料庫為最新時，面板呈*綠色*。
	應用程式資料庫已過期時，面板呈*黃色*。
	應用程式資料庫已嚴重過期時，面板呈*紅色*。

檢視安全事件統計

統計資訊部分顯示所有安全事件。單獨塊中顯示的每個防護工作統計說明了事件數量和上次發生事件的日期和時間。記錄某個事件後，塊顏色變為紅色。

若要檢視統計：

1. 採用以下方式之一開啟小型診斷視窗：
   - 執行受防護裝置上應用程式安裝資料夾中的 avpui.exe 檔案。預設情況下，該檔案位於 C:\Program Files (x86)\Kaspersky Lab\Kaspersky Embedded Systems Security.4.1.0。
   - 點擊工作列通知區域中的應用程式圖示。
2. 轉到**"統計資訊"**區域。
3. 檢視防護工作的安全事件。

檢視目前應用程式活動

要檢視受防護裝置上的目前應用程式活動：

1. 採用以下方式之一開啟小型診斷視窗：
   - 執行受防護裝置上應用程式安裝資料夾中的 avpui.exe 檔案。預設情況下，該檔案位於 C:\Program Files (x86)\Kaspersky Lab\Kaspersky Embedded Systems Security.4.1.0。
   - 點擊工作列通知區域中的應用程式圖示。
2. 轉到"**目前應用程式活動**"區域。

使用不同的顏色指示應用程式啟動狀態：

- 在"**工作**"部分中：
  - *綠色*。沒有達到顯示黃色或紅色的條件。
  - *黃色*。很長時間未掃描關鍵區域。
  - *紅色*。符合以下至少一個條件：
    - 未啟動任何工作和沒有為任何工作設定啟動排程。
    - 應用程式啟動錯誤將記錄為緊急事件。
- 在"**卡巴斯基安全網路**"部分中：
  - *綠色*。**KSN 使用** 工作開始。
  - *黃色*。KSN 聲明被接受，但工作未啟動。

配置應用程式追蹤和記憶體傾印記錄

配置應用程式追蹤和記憶體傾印記錄：

1. 採用以下方式之一開啟小型診斷視窗：
   - 執行受防護裝置上應用程式安裝資料夾中的 avpui.exe 檔案。預設情況下，該檔案位於 C:\Program Files (x86)\Kaspersky Lab\Kaspersky Embedded Systems Security.4.1.0。
   - 點擊工作列通知區域中的應用程式圖示。
2. 轉到"**故障診斷**"區域。
3. 使用"**啟用傾印和偵錯檔案防護**"核取方塊可以啟用或停用對傾印檔案和偵錯檔案的防護。

如果啟用了傾印檔案和偵錯檔案的防護，則以下使用者可以存取這些檔案：

- 系統管理員和本機管理員以及啟用寫入傾印檔案和偵錯檔案的使用者可以存取傾印檔案。
- 只有系統管理員和本機管理員可以存取偵錯檔案。

4. 使用"**將偵錯資訊寫入追蹤檔案**"核取方塊可以啟用或停用對應用程式操作的追蹤。
   預設情況下，應用程式操作追蹤處於停用狀態。

5. 如有必要，請變更 Kaspersky Embedded Systems Security 儲存偵錯檔案的預設資料夾。為此，請點擊 **瀏覽** 按下按鈕並選擇所需的資料夾。

   該資料夾必須提前建立並且可由系統帳戶寫入。您無法指定網路資料夾、磁碟機或環境變數。

   在選定的資料夾中，Kaspersky Embedded Systems Security 會建立一個名為 logs-Kaspersky Embedded Systems Security-<uid> 的子資料用於儲存偵錯檔案，其中 <uid> 是一個唯一的 8 個字元日誌標識符。

6. 選擇偵錯資訊的詳細等級：

   - **正常**表示偵錯檔案保存有關所有錯誤、警告的訊息以及有關應用程式正常操作的資訊（預設）。
   - **緊急**表示偵錯檔案僅保存有關致命錯誤的訊息。
   - **診斷**表示偵錯檔案保存有關所有錯誤和警告的訊息。
   - **重要**表示偵錯檔案保存有關所有錯誤、警告和附加資訊的訊息。
   - **詳情**表示偵錯檔案保存有關應用程式作業的所有資訊。

   技術支援代表確定為解決任何潛在問題而需要設定的詳細等級。

7. 若要刪除舊的偵錯檔案，請啟用 **移除最早的追蹤檔案** 功能。
   如果此功能已啟用，請配置偵錯檔案的最大大小和數量：

   a. 指定**追蹤檔案大小上限（MB）**。
      可用值：從 1 到 4095 MB。預設值為 100 MB。

   b. 指定**偵錯檔案的最大數量**。
      可用值：從 1 到 999。預設值為 5。

8. 使用"**向資料夾建立故障傾印檔案**"核取方塊可以啟用或停用對應用程式操作的追蹤。
   預設情況下，記憶體傾印記錄功能處於停用狀態。

9. 如有必要，請變更 Kaspersky Embedded Systems Security 儲存偵錯檔案的預設資料夾。為此，請點擊 **瀏覽** 按下按鈕並選擇所需的資料夾。

   該資料夾必須提前建立並且可由系統帳戶寫入。您無法指定網路資料夾、磁碟機或環境變數。

10. 單擊"**套用**"。

Kaspersky Embedded Systems Security 自我防護

自我防禦可阻止其他應用程式執行可能幹擾 Kaspersky Embedded Systems Security 運作的操作。該應用程式具有自我防護機制，可防止該應用程式的資料夾、記憶體處理程序和系統登入機碼被修改或刪除。Kaspersky Embedded Systems Security 支援 Microsoft 的Antimalware Protected Process Light （ AM-PPL ），可防護應用程式處理程序免受惡意活動的侵害。此外，該應用程式還允許分別管理使用者對應用程式功能和應用程式服務的存取權限。

啟用和停用自我防護

Kaspersky Embedded Systems Security 可避免修改或刪除磁碟機中的應用程式檔案、記憶體程序和系統登錄中的項目。

該技術可封鎖對以下應用程式元件的存取：

- Kaspersky Embedded Systems Security 安裝資料夾中的檔案和應用程式的其他檔案；
- 記錄屬於應用程式的登錄機碼；
- 應用程式執行的處理程序。

> 自我防護機制不適用於由不受信任的父處理程序啟動的 Kaspersky Embedded Systems Security 處理程序。

Kaspersky Embedded Systems Security 的自我防禦機制預設為啟用狀態。

如何在卡巴斯基安全管理中心管理主控台中啟用或停用自我防禦

1. 在卡巴斯基安全管理中心管理主控台樹狀目錄中，選取**政策**。
2. 選擇必要的政策並點擊以開啟政策內容。
3. 在政策內容視窗中，轉至「**應用程式設定**」區域。
4. 在"**安全性和可靠性**"塊中，點擊"**設定**"按鈕。
5. 這會開啟一個視窗；在該視窗中，選擇**安全**頁簽。
6. 在"**自我防護**"塊中，使用"**防護應用程式處理程序抵禦外部威脅**"核取方塊來啟用或停用自我防禦。
7. 關上掛鎖 將政策套用至電腦。
8. 點擊**確定**以儲存變更。

如何在應用程式主控台中啟用或停用自我防護

1. 在應用程式主控台樹狀目錄中，選取 **Kaspersky Embedded Systems Security** 節點，並在結果窗格中依照「**應用程式內容**」連結進行操作。
2. 這會開啟一個視窗；在該視窗中，選擇**安全設定**頁簽。
3. 在"**自我防護**"塊中，使用"**防護應用程式處理程序抵禦外部威脅**"核取方塊來啟用或停用自我防禦。
4. 點擊**確定**以儲存變更。

如何在卡巴斯基安全管理中心網頁主控台中啟用或停用自我防禦

1. 在網頁主控台的主視窗中，選擇**資產管理 → 政策**。
2. 點擊 Kaspersky Embedded Systems Security 政策的名稱。
   政策內容視窗將開啟。
3. 選擇"**應用程式設定**"標籤。
4. 選擇 **應用程式設定** 部分。
5. 在"**安全性和可靠性**"塊中，點擊"**配置**"按鈕。
   開啟"**安全性和可靠性**"視窗。
6. 在"**自我防護**"塊中，使用"**為應用程序防護外來威脅**"核取方塊來啟用或停用自我防禦。
7. 關上掛鎖 將政策套用至電腦。
8. 點擊**確定**以儲存變更。

支援 AM-PPL 技術

Kaspersky Embedded Systems Security 支援 Microsoft 的 Antimalware Protected Process Light 技術（以下簡稱「AM-PPL」）。AM-PPL 會防護 Kaspersky Embedded Systems Security 處理程序免受惡意操作（例如，終止應用程式）。AM-PPL 僅允許執行受信任的處理程序。Kaspersky Embedded Systems Security 處理程序根據 Windows 安全需求進行簽章，因此它們是受信任的。有關 AM-PPL 技術的詳細資訊，請存取 Microsoft 網站。預設情況下啟用 AM-PPL 技術。

Kaspersky Embedded Systems Security 還具有用於防護應用程式處理程序的內建機制。AM-PPL 支援允許您將處理程序安全功能委派給作業系統。從而可以提高應用程式的速度並減少電腦資源的消耗。

該應用程式註冊了 Kaspersky Embedded Systems Security (AVP) 服務和 Kaspersky Seamless Update Service (AVPSUS) 服務。AM-PPL 技術僅對 AVP 服務進行保護。

始終保持 AM-PPL 技術處於活動狀態。AM-PPL 是作業系統防護的重要組成部分。僅允許在單獨的測試環境中停用 AM-PPL，用於排除應用程式故障。

AM-PPL 技術適用於 Windows 10 版本 1703 (RS2) 或更高版本以及 Windows Server 2019 作業系統。

要啟用或停用 AM-PPL 技術：

1. 關閉應用程式的自我防護機制。
   自我防護機制會封鎖修改和刪除電腦記憶體中的應用程式處理程序，包括變更 AM-PPL 狀態。
2. 以管理員身分執行命令列解譯器 (cmd)。
3. 轉到 Kaspersky Embedded Systems Security 可執行檔所在資料夾。
4. 若要啟用對 AM-PPL 技術的支援，請執行以下命令：

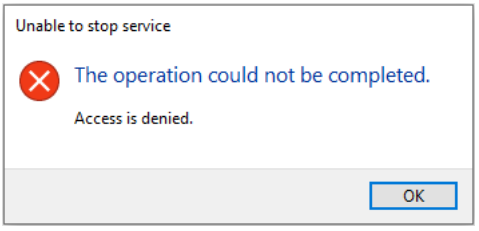
   ```
   klpsm.exe enable
   ```

5. 若要停用對 AM-PPL 技術的支援，請執行以下命令：

   ```
   klpsm.exe disable
   ```

6. 重新啟動 Kaspersky Embedded Systems Security。
7. 還原應用程式的自我防護機制。

結果，當使用者嘗試停止 AVP 服務時，會出現一個帶有錯誤訊息的系統視窗。使用者只能從 Kaspersky Embedded Systems Security 介面管理應用程式服務。



應用程式服務存取錯誤

防護作業系統服務

您可以使用 防護作業系統服務 功能來允許或禁止第三方應用程式對作業系統服務採取行動。

如何在卡巴斯基安全管理中心管理主控台中啟用或停用作業係統服務

1. 在卡巴斯基安全管理中心管理主控台樹狀目錄中，選取**政策**。
2. 選擇必要的政策並點擊以開啟政策內容。
3. 在政策內容視窗中，轉至「**應用程式設定**」區域。
4. 在"**安全性和可靠性**"塊中，點擊"**設定**"按鈕。
5. 這會開啟一個視窗；在該視窗中，選擇**安全**頁簽。
6. 使用"**防護作業系統服務**"核取方塊可以啟用或停用對作業係統服務的防護。

如果啟用了作業系統服務防護，則協力廠商應用程式無法對作業系統的處理程序採取行動。
如果停用了作業系統服務防護，則協力廠商應用程式可以對作業系統的處理程序採取行動。
啟用或停用該功能後，您必須重新啟動電腦才能套用變更。

7. 關上掛鎖將政策套用至電腦。

8. 點擊**確定**以儲存變更。

如何在應用程式主控台中啟用或停用作業係統服務

1. 在應用程式主控台樹狀目錄中，選取 **Kaspersky Embedded Systems Security** 節點，並在結果窗格中依照「**應用程式內容**」連結進行操作。

2. 這會開啟一個視窗；在該視窗中，選擇**安全設定**頁簽。

3. 使用**"防護作業系統服務"**核取方塊可以啟用或停用對作業係統服務的防護。
如果啟用了作業系統服務防護，則協力廠商應用程式無法對作業系統的處理程序採取行動。
如果停用了作業系統服務防護，則協力廠商應用程式可以對作業系統的處理程序採取行動。
啟用或停用該功能後，您必須重新啟動電腦才能套用變更。

4. 點擊**確定**以儲存變更。

如何在卡巴斯基安全管理中心網頁主控台中啟用或停用作業係統服務

1. 在網頁主控台的主視窗中，選擇**資產管理 → 政策**。

2. 點擊 Kaspersky Embedded Systems Security 政策的名稱。
政策內容視窗將開啟。

3. 選擇**"應用程式設定"**標籤。

4. 選擇 **應用程式設定** 部分。

5. 在**"安全性和可靠性"**塊中，點擊**"配置"**按鈕。
開啟**"安全性和可靠性"**視窗。

6. 使用**"防護作業系統服務"**核取方塊可以啟用或停用對作業係統服務的防護。
如果啟用了作業系統服務防護，則協力廠商應用程式無法對作業系統的處理程序採取行動。
如果停用了作業系統服務防護，則協力廠商應用程式可以對作業系統的處理程序採取行動。
啟用或停用該功能後，您必須重新啟動電腦才能套用變更。

7. 關上掛鎖將政策套用至電腦。

8. 點擊**確定**以儲存變更。

配置使用者權限以管理 Kaspersky Embedded Systems Security

預設情況下，受防護裝置上的「管理員」群組的成員、在安裝 Kaspersky Embedded Systems Security 的過程中在受防護裝置上建立的 ESS 管理員群組的成員以及 SYSTEM 群組可存取所有 Kaspersky Embedded Systems Security 功能。

未在 Kaspersky Embedded Systems Security 使用者清單中註冊的使用者無法開啟應用程式主控台。

您可以允許或封鎖單個使用者或使用者群組存取 Kaspersky Embedded Systems Security 的特定功能。

關於 Kaspersky Embedded Systems Security 功能的存取權限

使用者權限	描述
管理工作	可啟動/停止/暫停/還原 Kaspersky Embedded Systems Security 工作。
建立與刪除工作	可建立和刪除自訂掃描工作。
編輯設定	可執行以下操作： • 從設定檔匯入 Kaspersky Embedded Systems Security 設定。 • 編輯應用程式設定。
讀取設定	可執行以下操作： • 檢視 Kaspersky Embedded Systems Security 一般設定和工作設定。 • 將 Kaspersky Embedded Systems Security 設定匯出到設定檔。 • 檢視工作記錄、系統稽核記錄和通知設定。
管理儲存	可執行以下操作： • 將物件移到隔離。 • 從隔離和備份中刪除物件。 • 從隔離和備份中還原物件。
管理記錄	可刪除工作記錄和清除系統稽核記錄。
讀取記錄	可檢視工作記錄和系統稽核記錄中的病毒防護事件。
抓取統計資料	可檢視每個 Kaspersky Embedded Systems Security 工作的統計。
管理應用程式許可	能啟動 Kaspersky Embedded Systems Security。
解除安裝應用程式	可移除 Kaspersky Embedded Systems Security。
讀取權限	可檢視 Kaspersky Embedded Systems Security 使用者和使用者存取權限的清單。
編輯權限	可執行以下操作： • 編輯具有應用程式管理存取權限的使用者清單。 • 編輯 Kaspersky Embedded Systems Security 功能的使用者存取權限。
遠端連線到應用程式	能夠使用應用程式主控台遠端連線到應用程式。 對於遠端存取，使用者還必須具有**讀取設定**功能的存取權限。
結束應用程式	可使用應用程式主控台應用程式。
停用卡巴斯基安全管理中心政策	可停用卡巴斯基安全管理中心政策。
匯出設定	能夠匯出 Kaspersky Embedded Systems Security 設定。
編輯故障診斷	可以配置應用程式追蹤和記憶體傾印記錄。

如何在卡巴斯基安全管理中心管理主控台中設定使用者權限以管理 Kaspersky Embedded Systems Security

1. 在卡巴斯基安全管理中心管理主控台樹狀目錄中，選取**政策**。
2. 選擇必要的政策並點擊以開啟政策內容。
3. 在政策屬性視窗中，選取**"補充"**。
4. 在**"應用程式管理的使用者存取權限"**區域中點擊**"設定"**。
5. 這會開啟一個視窗；在該視窗中，點擊 **允許使用使用者手動建立的憑證確認應用程式操作** 核取方塊並為 KLAdmin 帳戶設定密碼。該使用者帳戶會被自動新增到使用者帳戶清單中。
6. 如有必要，請新增您想要授予應用程式管理存取權限的使用者帳戶。為此，在使用者帳戶表中點擊 **新增**。
   這將開啟用於配置使用者存取權限的表單。
7. 選擇要用來新增使用者的方法：
   - **從 Active Directory 中選擇一個使用者/群組**您可以授予 Kaspersky Embedded Systems Security 對 Active Directory 網域內的當個使用者或群組進行存取的權限。例如，如果 Everyone 群組被封鎖結束應用程式，您可以將**"結束應用程式"**權限授予給單個使用者。
   - **手動新增使用者/群組**您可以建立一個不在 Active Directory 中的使用者帳戶並向該使用者帳戶指派單個權限。即您可以建立一個*服務使用者帳戶*並使用它而不是 KLAdmin。這樣，您就無需與其他使用者共用您的 KLAdmin 密碼或建立新的 Active Directory 使用者帳戶。您可以指定任何使用者名稱和密碼。例如，您可以向服務使用者帳戶授予**讀取記錄**權限。因此，如果對"All"群組禁止了檢視報告，您可以使用服務使用者帳戶或 KLAdmin 使用者帳戶開啟報告。

     若要手動新增使用者或使用者群組，您必須啟用 密碼防護。
8. 選擇要授予其存取權限以管理應用程式的使用者或使用者群組。
9. 在 **權限** 清單中，配置使用者對應用程式功能的存取權限。
10. 儲存變更。若要在電腦上套用該政策，請關閉掛鎖。

如何設定使用者權限以在應用程式主控台中管理 Kaspersky Embedded Systems Security

1. 在應用程式主控台樹狀目錄中，選擇 **Kaspersky Embedded Systems Security** 節點然後從節點的上下文選單中選擇 **應用程式管理的使用者存取權限**。
2. 這會開啟一個視窗；在該視窗中，點擊 **允許使用使用者手動建立的憑證確認應用程式操作** 核取方塊並為 KLAdmin 帳戶設定密碼。該使用者帳戶會被自動新增到使用者帳戶清單中。
3. 如有必要，請新增您想要授予應用程式管理存取權限的使用者帳戶。為此，在使用者帳戶表中點擊 **新增**。
   這將開啟用於配置使用者存取權限的表單。

4. 選擇要用來新增使用者的方法：

   - **從 Active Directory 中選擇一個使用者/群組**您可以授予 Kaspersky Embedded Systems Security 對 Active Directory 網域內的當個使用者或群組進行存取的權限。例如，如果 Everyone 群組被封鎖結束應用程式，您可以將**"結束應用程式"**權限授予給單個使用者。

   - **手動新增使用者/群組**您可以建立一個不在 Active Directory 中的使用者帳戶並向該使用者帳戶指派單個權限。即您可以建立一個*服務使用者帳戶*並使用它而不是 KLAdmin。這樣，您就無需與其他使用者共用您的 KLAdmin 密碼或建立新的 Active Directory 使用者帳戶。您可以指定任何使用者名稱和密碼。例如，您可以向服務使用者帳戶授予**讀取記錄**權限。因此，如果對"All"群組禁止了檢視報告，您可以使用服務使用者帳戶或 KLAdmin 使用者帳戶開啟報告。

     若要手動新增使用者或使用者群組，您必須啟用 密碼防護。

5. 選擇要授予其存取權限以管理應用程式的使用者或使用者群組。

6. 在 **權限** 清單中，配置使用者對應用程式功能的存取權限。

7. 儲存變更。

如何在卡巴斯基安全管理中心網頁主控台中設定使用者對儲存裝置上的資料的存取權限

1. 在網頁主控台的主視窗中，選擇**資產管理 → 政策**。

2. 點擊 Kaspersky Embedded Systems Security 政策的名稱。
   政策內容視窗將開啟。

3. 選擇**"應用程式設定"**標籤。

4. 轉到**補充 → 應用程式管理的使用者存取權限** 並點擊 **配置** 按鈕。

5. 這會開啟一個視窗；在該視窗中，點擊 **允許使用使用者手動建立的憑證確認應用程式操作** 核取方塊並為 KLAdmin 帳戶設定密碼。該使用者帳戶會被自動新增到使用者帳戶清單中。

6. 如有必要，請新增您想要授予應用程式管理存取權限的使用者帳戶。為此，在使用者帳戶表中點擊 **新增**。
   這將開啟用於配置使用者存取權限的表單。

7. 選擇要用來新增使用者的方法：

   - **從 Active Directory 中選擇一個使用者/群組**您可以授予 Kaspersky Embedded Systems Security 對 Active Directory 網域內的當個使用者或群組進行存取的權限。例如，如果 Everyone 群組被封鎖結束應用程式，您可以將**"結束應用程式"**權限授予給單個使用者。

   - **手動新增使用者/群組**您可以建立一個不在 Active Directory 中的使用者帳戶並向該使用者帳戶指派單個權限。即您可以建立一個*服務使用者帳戶*並使用它而不是 KLAdmin。這樣，您就無需與其他使用者共用您的 KLAdmin 密碼或建立新的 Active Directory 使用者帳戶。您可以指定任何使用者名稱和密碼。例如，您可以向服務使用者帳戶授予**讀取記錄**權限。因此，如果對"All"群組禁止了檢視報告，您可以使用服務使用者帳戶或 KLAdmin 使用者帳戶開啟報告。

     若要手動新增使用者或使用者群組，您必須啟用 密碼防護。

8. 選擇要授予其存取權限以管理應用程式的使用者或使用者群組。

9. 在 **權限** 清單中，配置使用者對應用程式功能的存取權限。

10. 儲存變更。若要在電腦上套用該政策，請關閉掛鎖。

設定管理 Kaspersky Embedded Systems Security 服務的使用者存取權限

在安裝期間，Kaspersky Embedded Systems Security 會在 Windows 中註冊應用程式服務 *Kaspersky Embedded Systems Security 服務*。因此，該應用程式包括在作業系統啟動時啟動的功能元件。為降低第三方利用應用程式服務存取應用程式功能及受防護裝置安全性設定的風險，您可以限制管理 Kaspersky Embedded Systems Security 服務 的權限。

預設會將管理 Kaspersky Embedded Systems Security 服務 的權限授予受防護裝置上 Administrators 群組中的使用者。讀取權限被授予給 SERVICE 和 INTERACTIVE 群組，讀取和執行權限被授予給 SYSTEM 群組。

> 您無法刪除 SYSTEM 使用者帳戶或編輯此帳戶的權限。如果編輯 SYSTEM 帳戶的權限，則當您儲存變更時會還原此帳戶的最大權限。

具有「編輯權限」等級功能存取權限的使用者，可以將管理 Kaspersky Embedded Systems Security 服務 的存取權限授予在受防護裝置上註冊或包含在網域中的其他使用者。

您可以為 Kaspersky Embedded Systems Security 使用者或群組選取下列其中一個預設的 Kaspersky Embedded Systems Security 服務 管理存取等級：

- **完整控制**：能夠檢視及編輯 Kaspersky Embedded Systems Security 服務 的一般設定和使用者權限，以及啟動和停止 Kaspersky Embedded Systems Security 服務。
- **讀取**：能夠檢視 Kaspersky Embedded Systems Security 服務 的一般設定和使用者權限。
- **編輯**：能夠檢視及編輯 Kaspersky Embedded Systems Security 服務 的一般設定和使用者權限。
- **執行**：能夠啟動和停止 Kaspersky Embedded Systems Security 服務。

您還可以設定進階存取權限：允許或拒絕存取指定的 Kaspersky Embedded Systems Security 功能（請參見下表）。

Kaspersky Embedded Systems Security 服務 功能的存取權限

功能	描述
讀取服務設定	能夠檢視 Kaspersky Embedded Systems Security 服務 的一般設定和使用者權限。
從服務控制管理員請求服務狀態	能夠從 Microsoft Windows 服務控制管理員查詢 Kaspersky Embedded Systems Security 服務 的執行狀態。
請求服務狀態	能夠從 Kaspersky Embedded Systems Security 服務 查詢服務執行狀態。
讀取依賴服務清單	能夠檢視 Kaspersky Embedded Systems Security 服務 所依賴的服務以及依賴 Kaspersky Embedded Systems Security 服務 的服務清單。
修改服務設定	能夠檢視及編輯 Kaspersky Embedded Systems Security 服務 的一般設定和使用者權限。
啟動服務	能夠啟動 Kaspersky Embedded Systems Security 服務。
停止服務	能夠停止 Kaspersky Embedded Systems Security 服務。
暫停/還原服務	能夠暫停及繼續執行 Kaspersky Embedded Systems Security 服務。
讀取權限	能夠檢視 Kaspersky Embedded Systems Security 服務 使用者的清單以及每位使用者的存取權限。

功能	描述
編輯權限	可執行以下操作： • 新增或移除 Kaspersky Embedded Systems Security 服務 使用者。 • 編輯 Kaspersky Embedded Systems Security 服務 的使用者存取權限。
移除服務	能夠在 Microsoft Windows 服務控制管理員中取消註冊 Kaspersky Embedded Systems Security 服務。
使用者定義的服務請求	能夠建立使用者請求並傳送至 Kaspersky Embedded Systems Security 服務。

您可以編輯獲准管理 Kaspersky Embedded Systems Security 服務 的使用者和使用者群組清單，也可以編輯這些使用者和使用者群組的存取權限。

如何設定使用者權限，以在卡巴斯基安全管理中心管理主控台中管理 Kaspersky Embedded Systems Security 服務

1. 在卡巴斯基安全管理中心管理主控台樹狀目錄中，選取**政策**。
2. 選擇必要的政策並點擊以開啟政策內容。
3. 在政策屬性視窗中，選取**"補充"**。
4. 在**"KESS 服務管理的使用者存取權限"**區域中點擊**"設定"**。
   這將開啟用於配置使用者存取權限的表單。
5. 新增您想要設定 Kaspersky Embedded Systems Security 服務 使用者權限的 Active Directory 使用者或群組。
6. 選擇要授予其存取權限以管理應用程式的使用者或使用者群組。
7. 在權限清單中，設定使用者管理 Kaspersky Embedded Systems Security 服務 的權限。
8. 如果有必要，為使用者配置特殊權限：
   a. 點選 **其他**。
   b. 這會開啟一個視窗，在視窗中選擇一個使用者帳戶。
   c. 按兩下開啟使用者帳戶屬性。
   d. 這將開啟一個視窗；在該視窗中，按一下 **顯示其他權限** 連接。
   e. 這將開啟一個視窗；在該視窗中，為使用者配置特殊權限。
9. 儲存變更。若要在電腦上套用該政策，請關閉掛鎖。

如何設定使用者權限，以在應用程式主控台中管理 Kaspersky Embedded Systems Security 服務

1. 在應用程式主控台樹狀目錄中，選擇 **Kaspersky Embedded Systems Security** 節點然後從節點的上下文選單中選擇 **KESS 服務管理的使用者存取權限**。
2. 在開啟的視窗中的 **權限**塊中，點擊 **新增** 按鈕。
   這將開啟用於配置使用者存取權限的表單。
3. 新增您想要設定 Kaspersky Embedded Systems Security 服務 使用者權限的 Active Directory 使用者或群組。
4. 選擇要授予其存取權限以管理應用程式的使用者或使用者群組。
5. 在權限清單中，設定使用者管理 Kaspersky Embedded Systems Security 服務 的權限。

6. 如果有必要，為使用者配置特殊權限：

   a. 點選 **其他**。

   b. 這會開啟一個視窗，在視窗中選擇一個使用者帳戶。

   c. 按兩下開啟使用者帳戶屬性。

   d. 這將開啟一個視窗；在該視窗中，按一下 **顯示其他權限** 連接。

   e. 這將開啟一個視窗；在該視窗中，為使用者配置特殊權限。

7. 儲存變更。

如何設定使用者權限，以在卡巴斯基安全管理中心網頁主控台中管理 Kaspersky Embedded Systems Security 服務

1. 在網頁主控台的主視窗中，選擇**資產管理 → 政策**。
2. 點擊 Kaspersky Embedded Systems Security 政策的名稱。
   政策內容視窗將開啟。
3. 選擇**"應用程式設定"**標籤。
4. 轉到**補充 → KESS 服務管理的使用者存取權限** 並點擊 **配置** 按鈕。
   開啟**"KESS 服務管理的使用者存取權限"**視窗。
5. 新增您想要設定 Kaspersky Embedded Systems Security 服務 使用者權限的 Active Directory 使用者或群組。
6. 選擇要授予其存取權限以管理應用程式的使用者或使用者群組。

   > 您無法設定特殊權限來在網頁主控台中管理應用程式服務。

7. 儲存變更。若要在電腦上套用該政策，請關閉掛鎖。

對 Kaspersky Embedded Systems Security 功能進行受密碼防護的存取

配置使用者權限可讓您透過配置使用者權限來限制對應用程式管理和已註冊服務的存取。您也可在 Kaspersky Embedded Systems Security 設定中設定密碼防護，以提供關鍵操作的額外防護。

當使用者嘗試執行受密碼防護的操作時，Kaspersky Embedded Systems Security 會提示使用者輸入使用者名稱和密碼，或使用權杖進行驗證。

使用者名稱和密碼

密碼防護支援以下帳戶：

- **KLAdmin**。對 Kaspersky Embedded Systems Security 具有不受限制存取權限的管理員帳戶。KLAdmin 帳戶有權執行任何受密碼防護的操作。KLAdmin 帳戶的權限無法撤銷。當啟用密碼防護時，Kaspersky Embedded Systems Security 會提示您設定 KLAdmin 帳戶的密碼。
- **手動新增的帳戶**。一個 Active Directory 網域之外的帳戶。如果不想共用管理員密碼，您可以使用該服務帳戶而不是 KLAdmin。您可以使用任何使用者名稱和密碼並設定單個權限。
- **Everyone 群組**。Windows 內建的群組，包括公司網路內的所有使用者。Everyone 群組中的使用者可以根據其被分配的權限存取應用程式。
- **單個使用者或群組**。可以為其配置單個權限的使用者帳戶。例如，如果針對 Everyone 群組封鎖某個操作，您可以允許單個使用者或群組執行該操作。

Kaspersky Embedded Systems Security 介面會在螢幕上隱藏指定密碼。輸入密碼後，Kaspersky Embedded Systems Security 將密碼儲存為計算得出的核對總和。

多次嘗試失敗後，Kaspersky Embedded Systems Security 不會檢查密碼強度，也不會封鎖密碼輸入。

建立密碼時，建議符合以下條件：

- 密碼不包含帳戶名稱或電腦名稱。
- 密碼長度至少為 8 個字元。
- 密碼包含的字元與以下至少三個類別相符：
  - 大寫拉丁字母 (A-Z)
  - 小寫拉丁字母 (a-z)
  - 數字 (0-9)
  - 感嘆號 (!)、美元符號 ($)、英鎊符號 (#) 和百分號 (%)

權杖

若要存取 Kaspersky Embedded Systems Security 功能，您必須從已連線權杖上儲存的憑證清單中選取適當的使用者憑證，然後輸入您的 PIN 碼。權杖式身分驗證僅適用於 Active Directory 網域內的使用者。管理員可以設定個別使用者或群組的權限。若要使用權杖式身分驗證，您必須部署受信任的 PKI 基礎架構，並安裝用於管理權杖的專用軟體。

如何在卡巴斯基安全管理中心管理主控台中對 Kaspersky Embedded Systems Security 功能進行具有密碼防護的存取

1. 在卡巴斯基安全管理中心管理主控台樹狀目錄中，選取**政策**。
2. 選擇必要的政策並點擊以開啟政策內容。
3. 在政策屬性視窗中，選取**"補充"**。
4. 在**"應用程式管理的使用者存取權限"**區域中點擊**"設定"**。
5. 在開啟的視窗中，選中**"允許使用使用者手動建立的憑證確認應用程式操作"**核取方塊。
6. 如有必要，清除**"請求密碼以確認關鍵操作"**核取方塊。

   如果啟用此功能，應用程式會在刪除、修改或還原應用程式以及 在命令列上執行可能會降低裝置的防護等級的操作時請求使用者名稱和密碼。

   如果此功能已停用，且目前使用者擁有 必要權限，則 Kaspersky Embedded Systems Security不要求憑據。預設啟用該選項。

   > 如果為目前使用者設定了空的 Windows 密碼，則需要輸入擁有必要權限且密碼非空的使用者的憑據。

7. 指定 KLAdmin 使用者帳戶的密碼。
8. 如有必要，請新增您想要授予應用程式管理存取權限的使用者帳戶：

   a. 單擊**"新增"**。

   這將開啟用於配置使用者存取權限的表單。

   b. 在開啟的視窗中，選擇新增使用者的方法： **手動新增使用者/群組**。

   c. 指定使用者名稱和密碼。

   d. 在 **權限** 清單中，配置使用者對應用程式功能的存取權限。

9. 儲存變更。若要在電腦上套用該政策，請關閉掛鎖。

如何使用密碼防護對應用程式主控台中的 Kaspersky Embedded Systems Security 功能的存取

1. 在應用程式主控台樹狀目錄中，選擇 **Kaspersky Embedded Systems Security** 節點然後從節點的上下文選單中選擇 **應用程式管理的使用者存取權限**。
2. 在開啟的視窗中，選中**"允許使用使用者手動建立的憑證確認應用程式操作"**核取方塊。
3. 如有必要，清除**"請求密碼以確認關鍵操作"**核取方塊。

   如果啟用此功能，應用程式會在刪除、修改或還原應用程式以及 在命令列上執行可能會降低裝置的防護等級的操作時請求使用者名稱和密碼。

   如果此功能已停用，且目前使用者擁有 必要權限，則 Kaspersky Embedded Systems Security不要求憑據。預設啟用該選項。

   > 如果為目前使用者設定了空的 Windows 密碼，則需要輸入擁有必要權限且密碼非空的使用者的憑據。

4. 指定 KLAdmin 使用者帳戶的密碼。

5. 如有必要，請新增您想要授予應用程式管理存取權限的使用者帳戶：

   a. 單擊**"新增"**。

      這將開啟用於配置使用者存取權限的表單。

   b. 在開啟的視窗中，選擇新增使用者的方法： **手動新增使用者/群組**。

   c. 指定使用者名稱和密碼。

   d. 在 **權限** 清單中，配置使用者對應用程式功能的存取權限。

6. 儲存變更。

如何在卡巴斯基安全中心網頁主控台中使用密碼防護對 Kaspersky Embedded Systems Security功能的存取

1. 在網頁主控台的主視窗中，選擇**資產管理 → 政策**。

2. 點擊 Kaspersky Embedded Systems Security 政策的名稱。

   政策內容視窗將開啟。

3. 選擇**"應用程式設定"**標籤。

4. 轉到**補充 → 應用程式管理的使用者存取權限** 並點擊 **配置** 按鈕。

5. 在開啟的視窗中，選中**"允許使用使用者手動建立的憑證確認應用程式操作"**核取方塊。

6. 如有必要，清除**"請求密碼以確認關鍵操作"**核取方塊。

   如果啟用此功能，應用程式會在刪除、修改或還原應用程式以及 在命令列上執行可能會降低裝置的防護等級的操作時請求使用者名稱和密碼。

   如果此功能已停用，且目前使用者擁有 必要權限，則 Kaspersky Embedded Systems Security不要求憑據。預設啟用該選項。

   > 如果為目前使用者設定了空的 Windows 密碼，則需要輸入擁有必要權限且密碼非空的使用者的憑據。

7. 指定 KLAdmin 使用者帳戶的密碼。

8. 如有必要，請新增您想要授予應用程式管理存取權限的使用者帳戶：

   a. 單擊**"新增"**。

      這將開啟用於配置使用者存取權限的表單。

   b. 在開啟的視窗中，選擇新增使用者的方法： **手動新增使用者/群組**。

c. 指定使用者名稱和密碼。

d. 在 **權限** 清單中，配置使用者對應用程式功能的存取權限。

9. 儲存變更。若要在電腦上套用該政策，請關閉掛鎖。

此密碼無法還原。遺失密碼會導致完全失去對應用程式的控制。此外，您還將無法從受防護裝置移除應用程式。

您可以隨時重設密碼。為此，請清除**允許使用使用者手動建立的憑證確認應用程式操作**核取方塊並儲存變更。密碼防護將被停用，舊密碼核對總和將被刪除。使用新密碼重複密碼建立過程。

Secure Desktop 通知

Kaspersky Embedded Systems Security 支援 (Secure Desktop) 功能。此功能的目的是確認可能降低電腦安全等級的操作。此功能允許應用程式顯示與其他處理程序隔離的確認對話方塊。此功能使用提升的權限來防護請求。這樣，只有使用者才能確認操作，而惡意軟體無法確認。

Kaspersky Embedded Systems Security 會顯示 Secure Desktop 通知以確認以下操作：

- 偵錯已啟用或已停用
- 應用程式設定已匯出或匯入
- 保護已暫停
- 應用程式已退出
- 啟動金鑰已刪除
- Kaspersky Embedded Systems Security 已解除安裝
- 裝置控制已停用
- 即時檔案防護已停用
- 卡巴斯基安全管理中心政策已停用
- 報告已查看
- 檔案已從備份中還原
- Kaspersky Embedded Systems Security 設定已修改
- 應用程式工作已透過啟動以外的方式進行管理

如何在卡巴斯基安全管理中心管理主控台中啟用或停用 Secure Desktop 通知

1. 在卡巴斯基安全管理中心管理主控台樹狀目錄中，選取**政策**。

2. 選擇必要的政策並點擊以開啟政策內容。

3. 在政策內容視窗中，轉至「**應用程式設定**」區域。

4. 在"**安全性和可靠性**"塊中，點擊"**設定**"按鈕。

5. 這會開啟一個視窗；在該視窗中，選擇**安全**頁簽。

6. 在**自我防護**區塊中，選取或者清除**啟用安全桌面通知**核取方塊來啟用或停用 Secure Desktop 通知。

   如果自我防衛機制被停用，**啟用安全桌面通知**核取方塊不可用。

7. 關上掛鎖將政策套用至電腦。

8. 點擊**確定**以儲存變更。

如何在管理主控台中啟用或停用 Secure Desktop 通知

1. 在應用程式主控台樹狀目錄中，選取 **Kaspersky Embedded Systems Security** 節點，並在結果窗格中依照「**應用程式內容**」連結進行操作。

2. 這會開啟一個視窗；在該視窗中，選擇**安全設定**頁簽。

3. 在**自我防護**區塊中，選取或者清除**啟用安全桌面通知**核取方塊來啟用或停用 Secure Desktop 通知。

   如果自我防衛機制被停用，**啟用安全桌面通知**核取方塊不可用。

4. 點擊**確定**以儲存變更。

如何在卡巴斯基安全管理中心網頁主控台中啟用或停用 Secure Desktop 通知

1. 在網頁主控台的主視窗中，選擇**資產管理 → 政策**。

2. 點擊 Kaspersky Embedded Systems Security 政策的名稱。
   政策內容視窗將開啟。

3. 選擇"**應用程式設定**"標籤。

4. 選擇 **應用程式設定** 部分。

5. 在"**安全性和可靠性**"塊中，點擊"**配置**"按鈕。
   開啟"**安全性和可靠性**"視窗。

6. 在**自我防護**區塊中，選取或者清除**啟用安全桌面通知**核取方塊來啟用或停用 Secure Desktop 通知。

   如果自我防衛機制被停用，**啟用安全桌面通知**核取方塊不可用。

7. 關上掛鎖將政策套用至電腦。

8. 點擊**確定**以儲存變更。

信任區域

*信任區域*是在其有效時，管理員建立的 Kaspersky Embedded Systems Security 不進行監控的物件和應用程式的清單。

考慮到所處理物件的特點和安裝在電腦上的應用程式，管理員可以自主建立信任區域。當 Kaspersky Embedded Systems Security 封鎖存取特定物件或應用程式時，如果您確定此物件或應用程式是無害的，則有必要將其包含在信任區域中。管理員還可以允許使用者為特定電腦建立自己的本機受信任區域。這樣，除了政策中的一般受信任區域之外，使用者還可以建立自己的"排除項目"和"受信任應用程式"的本機清單。

預先定義的掃描排除項目和受信任的應用程式已被新增至受信任區域。預先定義的掃描排除項目和受信任應用程式可協助您快速設定 Kaspersky Embedded Systems Security，而不必手動建立信任區域。

建立掃描排除項目

"*掃描排除項目*"是一組條件，必須滿足這些條件，Kaspersky Embedded Systems Security 才不會掃描特定物件是否存在病毒和其他威脅。

掃描排除項目可供以下應用程式元件和工作使用：

- **即時檔案防護**
- **按需掃描**
- **行為偵測**
- **AMSI 掃描程式**
- **網路威脅防護**

如果包含某個物件的磁碟或資料夾在掃描工作啟動時包括在掃描範圍中，則 Kaspersky Embedded Systems Security 將不對此物件進行掃描。但是，當啟動了針對該特殊物件的自訂掃描工作時，掃描排除項目將不應用。

Kaspersky Embedded Systems Security 不支援包含超過 5000 個物件的排除清單。

如何在卡巴斯基安全管理中心管理主控台中建立掃描排除項目

1. 在卡巴斯基安全管理中心管理主控台樹狀目錄中，選取**政策**。
2. 選擇必要的政策並點擊以開啟政策內容。
3. 在政策視窗中，選擇 **補充 → 受信任區域** 然後點擊 **設定**。
4. 選擇"**掃描排除項目**"標籤。

5. 如果要為公司內的所有電腦建立排除項目的綜合清單，請選取**"繼承時合併值"**核取方塊。將合併父政策和子政策中的排除項目清單。如果啟用繼承時合併值，則將合併清單。父政策中的排除項目以唯讀視圖的形式顯示在子政策中。無法變更或刪除父政策的排除項目。

6. 如果想要使用者能夠建立本機排除項目清單，請選中**"允許使用本機排除項目"**核取方塊。這樣，除了在政策中產生的排除項目的一般清單外，使用者还可以建立自己的排除項目本機清單。管理員可以使用卡巴斯基安全管理中心檢視、新增、編輯或刪除電腦屬性中的清單項目。

   如果核取方塊被清理，使用者只能存取政策中產生的排除項目的一般清單。此外，如果清除此核取方塊，Kaspersky Embedded Systems Security 會在應用程式主控台中隱藏掃描排除項目的合併清單。

7. 點擊**新增** 並選擇一個操作：

   - **類別**您可以將掃描排除項目分組到不同的類別。若要建立新類別，請輸入類別名稱並在該類別中新增至少一個掃描排除項目。
   - **新排除項目**Kaspersky Embedded Systems Security 會將新的掃描排除項目新增至清單的根目錄。
   - **所選類別中新排除項目**若要將新的掃描排除項目新增至特定類別，請選擇一個類別。
   - **從清單中選取排除項目**若要快速設定 Kaspersky Embedded Systems Security，您可以從預先定義的掃描排除項目清單中新增排除項目。

8. 要從掃描中排除某個檔案或資料夾，請選擇**檔案或資料夾**核取方塊。點擊**選擇檔案或者資料夾**連結開啟一個視窗，然後在該視窗中點擊 **瀏覽** 選擇檔案或資料夾。

   您也可以手動輸入路徑。Kaspersky Embedded Systems Security 輸入遮罩時支援環境變量以及`*`和`?`字元：

   - `*`（星號）字元代表任意一組字元，但 `\` 和 `/` 字元除外（這兩個字元是檔案和資料夾路徑中的檔案和資料夾名稱的分隔符號）。例如，遮罩"`C:\*\*.txt`"將包括位於 C: 磁碟機但是不在子資料夾中所有帶 TXT 副檔名的檔案的路徑。
   - 兩個連續 `*` 字元在檔案或資料夾名稱中代表任意一組字元（包括空集），包括 `\` 和 `/` 字元（這兩個字元是檔案和資料夾路徑中的檔案和資料夾名稱的分隔符號）。例如，遮罩 `C:\Folder\**\*.txt` 將包括位於巢嵌在 `Folder` 內的資料夾（`Folder`自身除外）中所有帶 TXT 副檔名的檔案的路徑。遮罩必須包含至少一個嵌套等級。遮罩 `C:\**\*.txt` 不是有效遮罩。
   - `?`（問號）字元代表任意單個字元，但 `\` 和 `/` 字元除外（這兩個字元是檔案和資料夾路徑中的檔案和資料夾名稱的分隔符號）。例如，遮罩 `C:\Folder\???.txt` 將包括位於 `Folder` 資料夾中所有帶 TXT 副檔名且名稱由三個字元構成的檔案的路徑。

     您可以在路徑的開始、中間或者結尾使用遮罩。例如，如果您想要將一個針對所有使用者的資料夾新增到排除項目，請輸入 `?:\Users\*\Folder\` 遮罩。

9. 若要從掃描中排除預定義區域，請選擇 **預定義範圍** 核取方塊。點擊**選擇預定義範圍** 連結可開啟一個視窗，然後在該視窗中選擇受防護裝置上的一個標準範圍。

10. 若要從掃描中排除特定物件，請選擇 **偵測到的物件類型** 核取方塊。點擊**輸入物件名稱**連接，點擊 **新增** 按鈕，在顯示的視窗中根據 卡巴斯基百科全書 分類（例如，`Email-Worm`、`Rootkit` 或者 `RemoteAdmin`）輸入物件類型的名稱。

    您可以用`?`字元（替換任何單個字元）和`*`字元（替換任意數量的字元）來使用遮罩。例如，如果指定了`Client*`遮罩，則 Kaspersky Embedded Systems Security 將從掃描中排除`Client-IRC`、`Client-P2P`和`Client-SMTP`物件。

11. 若要從掃描中排除單個檔案，請選擇 **物件雜湊** 核取方塊。點擊 **輸入物件雜湊** 連結開啟一個視窗，然後在該視窗中輸入檔案雜湊。

    如果檔案被修改，檔案雜湊也將被修改。如果發生這種情況，修改後的檔案將不會新增到排除項目中。

12. 在“**規則使用範圍**“塊中，選擇要掃描排除項目套用的元件。

13. 如有必要，在“**註解**”欄位，輸入您建立的掃描排除項目的簡要說明。

14. 儲存變更以將排除項目新增至清單。您可以使用物件旁邊的核取方塊隨時停用排除項目。

如何在卡巴斯基安全管理中心網頁主控台中建立掃描排除項目

1. 在網頁主控台的主視窗中，選擇**資產管理 → 政策**。

2. 點擊 Kaspersky Embedded Systems Security 政策的名稱。

   政策內容視窗將開啟。

3. 選擇“**應用程式設定**”標籤。

4. 轉到**補充 → 受信任區域** 並點擊 **配置** 按鈕。

5. 選擇“**掃描排除項目**”標籤。

6. 如果要為公司內的所有電腦建立排除項目的綜合清單，請選取**“繼承時合併值**”核取方塊。將合併父政策和子政策中的排除項目清單。如果啟用繼承時合併值，則將合併清單。父政策中的排除項目以唯讀視圖的形式顯示在子政策中。無法變更或刪除父政策的排除項目。

7. 如果想要使用者能夠建立本機排除項目清單，請選中**“允許使用本機排除項目**“核取方塊。這樣，除了在政策中產生的排除項目的一般清單外，使用者还可以建立自己的排除項目本機清單。管理員可以使用卡巴斯基安全管理中心檢視、新增、編輯或刪除電腦屬性中的清單項目。

   如果核取方塊被清理，使用者只能存取政策中產生的排除項目的一般清單。此外，如果清除此核取方塊，Kaspersky Embedded Systems Security 會在應用程式主控台中隱藏掃描排除項目的合併清單。

8. 點擊**新增** 並選擇一個操作：

   - **類別**您可以將掃描排除項目分組到不同的類別。若要建立新類別，請輸入類別名稱並在該類別中新增至少一個掃描排除項目。

   - **新排除項目**Kaspersky Embedded Systems Security 會將新的掃描排除項目新增至清單的根目錄。

   - **從清單中選取排除項目**若要快速設定 Kaspersky Embedded Systems Security，您可以從預先定義的掃描排除項目清單中新增排除項目。

9. 如果您想要從掃描中排除檔案或資料夾，請選擇 **檔案或資料夾** 並選取欄位中同名的核取方塊。指定檔案或資料夾的路徑。

   Kaspersky Embedded Systems Security 輸入遮罩時支援環境變量以及 `*` 和 `?` 字元：

   - `*`（星號）字元代表任意一組字元，但 `\` 和 `/` 字元除外（這兩個字元是檔案和資料夾路徑中的檔案和資料夾名稱的分隔符號）。例如，遮罩“`C:\*\*.txt`”將包括位於 C: 磁碟機但是不在子資料夾中所有帶 TXT 副檔名的檔案的路徑。

   - 兩個連續 `*` 字元在檔案或資料夾名稱中代表任意一組字元（包括空集），包括 `\` 和 `/` 字元（這兩個字元是檔案和資料夾路徑中的檔案和資料夾名稱的分隔符號）。例如，遮罩 `C:\Folder\**\*.txt` 將包括位於巢嵌在 `Folder` 內的資料夾（`Folder`自身除外）中所有帶 TXT 副檔名的檔案的路徑。遮罩必須包含至少一個嵌套等級。遮罩 `C:\**\*.txt` 不是有效遮罩。

- `?`（問號）字元代表任意單個字元，但 `\` 和 `/` 字元除外（這兩個字元是檔案和資料夾路徑中的檔案和資料夾名稱的分隔符號）。例如，遮罩 `C:\Folder\???.txt` 將包括位於 `Folder` 資料夾中所有帶 TXT 副檔名且名稱由三個字元構成的檔案的路徑。

  您可以在路徑的開始、中間或者結尾使用遮罩。例如，如果您想要將一個針對所有使用者的資料夾新增到排除項目，請輸入 `?:\Users\*\Folder\` 遮罩。

10. 若要從掃描中排除預定義範圍，請選擇 **預定義範圍**。在下拉式清單中，選擇受防護裝置上的標準範圍之一。

11. 如果您想從掃描中排除某些物件，請選擇 **偵測到的物件類型** 核取方塊並根據卡巴斯基百科全書分類（例如，`Email-Worm`、`Rootkit` 或者 `RemoteAdmin`）輸入物件類型的名稱。

    您可以用`?`字元（替換任何單個字元）和`*`字元（替換任意數量的字元）來使用遮罩。例如，如果指定了 `Client*`遮罩，則 Kaspersky Embedded Systems Security 將從掃描中排除*Client-IRC*、*Client-P2P*和*Client-SMTP*物件。

12. 若要從掃描中排除單一檔案，請選擇 **物件雜湊** 核取方塊並新增檔案或事件清單中的雜湊。

    如果檔案被修改，檔案雜湊也將被修改。如果發生這種情況，修改後的檔案將不會新增到排除項目中。

13. 如有必要，在“**註解**”欄位，輸入您建立的掃描排除項目的簡要說明。

14. 在“**防護元件**“塊中，選擇要掃描排除項目套用的元件。

15. 新的排除項目將被新增到清單中。您可以隨時使用**狀態**列中的核取方塊停用排除項目。

16. 儲存變更。

如何在應用程式主控台中建立掃描排除項目

1. 在應用程式主控台樹狀目錄中，選擇 **Kaspersky Embedded Systems Security** 節點然後從節點的上下文選單中選擇 **受信任區域**。

   開啟“**配置信任區域設定**”視窗。

2. 在 **排除項目** 部分，點擊**掃描排除項目** 區塊旁邊的 **設定** 按鈕。

3. 點擊**新增** 並選擇一個操作：

   - **類別**您可以將掃描排除項目分組到不同的類別。若要建立新類別，請輸入類別名稱並在該類別中新增至少一個掃描排除項目。
   - **新排除項目**Kaspersky Embedded Systems Security 會將新的掃描排除項目新增至清單的根目錄。
   - **所選類別中新排除項目**若要將新的掃描排除項目新增至特定類別，請選擇一個類別。
   - **從清單中選取排除項目**若要快速設定 Kaspersky Embedded Systems Security，您可以從預先定義的掃描排除項目清單中新增排除項目。

4. 要從掃描中排除某個檔案或資料夾，請選擇**檔案或資料夾**核取方塊。點擊**選擇檔案或資料夾。** 連結開啟一個視窗，然後在該視窗中點擊 **瀏覽** 選擇檔案或資料夾。

您也可以手動輸入路徑。Kaspersky Embedded Systems Security 輸入遮罩時支援環境變量以及`*`和`?`字元：

- `*`（星號）字元代表任意一組字元，但`\`和`/`字元除外（這兩個字元是檔案和資料夾路徑中的檔案和資料夾名稱的分隔符號）。例如，遮罩"`C:\*\*.txt`"將包括位於 C: 磁碟機但是不在子資料夾中所有帶 TXT 副檔名的檔案的路徑。

- 兩個連續`*`字元在檔案或資料夾名稱中代表任意一組字元（包括空集），包括`\`和`/`字元（這兩個字元是檔案和資料夾路徑中的檔案和資料夾名稱的分隔符號）。例如，遮罩`C:\Folder\**\*.txt`將包括位於巢嵌在`Folder`內的資料夾（`Folder`自身除外）中所有帶 TXT 副檔名的檔案的路徑。遮罩必須包含至少一個嵌套等級。遮罩`C:\**\*.txt`不是有效遮罩。

- `?`（問號）字元代表任意單個字元，但`\`和`/`字元除外（這兩個字元是檔案和資料夾路徑中的檔案和資料夾名稱的分隔符號）。例如，遮罩`C:\Folder\???.txt`將包括位於`Folder`資料夾中所有帶 TXT 副檔名且名稱由三個字元構成的檔案的路徑。

  您可以在路徑的開始、中間或者結尾使用遮罩。例如，如果您想要將一個針對所有使用者的資料夾新增到排除項目，請輸入`?:\Users\*\Folder\`遮罩。

5. 若要從掃描中排除預定義區域，請選擇 **預定義範圍** 核取方塊。點擊**選擇預定義範圍** 連結可開啟一個視窗，然後在該視窗中選擇受防護裝置上的一個標準範圍。

6. 若要從掃描中排除特定物件，請選擇 **偵測到的物件類型** 核取方塊。點擊**輸入物件名稱**連接，點擊 **新增** 按鈕，在顯示的視窗中根據 卡巴斯基百科全書 分類（例如，`Email-Worm`、`Rootkit`或者`RemoteAdmin`）輸入物件類型的名稱。

   您可以用`?`字元（替換任何單個字元）和`*`字元（替換任意數量的字元）來使用遮罩。例如，如果指定了`Client*`遮罩，則 Kaspersky Embedded Systems Security 將從掃描中排除`Client-IRC`、`Client-P2P`和`Client-SMTP`物件。

7. 若要從掃描中排除單個檔案，請選擇 **物件雜湊** 核取方塊。點擊 **輸入物件雜湊** 連結開啟一個視窗，然後在該視窗中輸入檔案雜湊。

   如果檔案被修改，檔案雜湊也將被修改。如果發生這種情況，修改後的檔案將不會新增到排除項目中。

8. 在"**規則使用範圍**"塊中，選擇要掃描排除項目套用的元件。

9. 如有必要，在"**註解**"欄位，輸入您建立的掃描排除項目的簡要說明。

10. 儲存變更以將排除項目新增至清單。您可以使用物件旁邊的核取方塊隨時停用排除項目。

路徑遮罩示例：
位於任意資料夾的檔案的路徑：

- 遮罩 `*.exe` 將包括具有 exe 副檔名的檔案的所有路徑。
- 遮罩 `example*` 將包括名為 EXAMPLE 的檔案的所有路徑。

位於指定資料夾的檔案的路徑：

- 遮罩 `C:\dir\*.*` 將包括位於 C:\dir\ 資料夾中的所有檔案的路徑，但不包括 C:\dir\ 的子資料夾中的檔案的路徑。
- 遮罩 `C:\dir\*` 將包括位於 C:\dir\ 資料夾中的所有檔案的路徑，包括 C:\dir\ 的子資料夾中的檔案的路徑。
- 遮罩 `C:\dir\` 將包括位於 C:\dir\ 資料夾中的所有檔案的路徑，包括 C:\dir\ 的子資料夾中的檔案的路徑。
- 遮罩 `C:\dir\*.exe` 將包含位於 C:\dir\ 資料夾中且副檔名為 .EXE 的所有檔案路徑，但不包含 C:\dir\ 子資料夾中的檔案路徑。
- 遮罩 `C:\dir\test` 將包括位於 C:\dir\ 資料夾中名為"test"的所有檔案的路徑，但不包括 C:\dir\ 的子資料夾中的此類檔案的路徑。
- 遮罩 `C:\dir\*\test` 將包括位於 C:\dir\ 資料夾及 C:\dir\ 的子資料夾中名為"test"的所有檔案的路徑。
- 遮罩 `C:\dir1\*\dir3\` 將把 dir3 子資料夾一個級別中的所有檔案路徑包括在 C:\dir1\ 資料夾中。
- 遮罩 `C:\dir1\**\dirN\` 將包括 C:\dir1\ 資料夾中任何級別的 dirN 子資料夾中的所有檔案路徑。

位於所有資料夾中具有指定名稱的檔案的路徑：

- 遮罩 `dir\*.*` 將包括名為"dir"的資料夾中的所有檔案的路徑，但不包括這些資料夾的子資料夾中的檔案的路徑。
- 遮罩 `dir\*` 將包括名為"dir"的資料夾中的所有檔案的路徑，但不包括這些資料夾的子資料夾中的檔案的路徑。
- 遮罩 `dir\` 將包括名為"dir"的資料夾中的所有檔案的路徑，但不包括這些資料夾的子資料夾中的檔案的路徑。
- 遮罩 `dir\*.exe` 將包含名為「dir」的資料夾中且副檔名為 .EXE 的所有檔案路徑，但不包含這些資料夾之子資料夾中的檔案路徑。
- 遮罩 `dir\test` 將包括名為"dir"的資料夾中名為"test"的所有檔案的路徑，但不包括這些資料夾的子資料夾中的此類檔案的路徑。

選擇可偵測的威脅類型

若要選取可偵測的威脅類型，請執行以下操作：

1. 在應用程式主控台樹狀目錄中，選擇"**Kaspersky Embedded Systems Security**"節點並執行以下操作之一：
   - 在節點的結果窗格中，點擊**配置信任區域設定**連結。
   - 在節點的內容功能表中選擇**受信任區域**。

   開啟"**配置信任區域設定**"視窗。
2. 在"**偵測到的物件類型**"區域中點擊"**設定**"。
3. 在開啟的視窗中，選取您想要 Kaspersky Embedded Systems Security 偵測的物件類型旁邊的核取方塊：
   - **病毒和蠕蟲**

     子分類：病毒和蠕蟲 (Viruses_and_Worms)

     危險等級：高

     典型的病毒和蠕蟲會執行未經使用者授權的操作。它們會建立可自我複製的副本。

經典病毒

典型病毒侵入電腦後，會感染檔案，啟動並執行惡意操作，以及將自身的副本新增到其他檔案中。

典型病毒僅在電腦本機資源上複製副本，不會自行侵入其他電腦。僅當此病毒將其副本新增至儲存在共用資料夾或放入電腦中的 CD 中的檔案時，或者在使用者傳送附有受感染檔案的電子郵件訊息時，此病毒才會傳染給其他電腦。

典型病毒代碼可以入侵電腦、作業系統和應用程式的各種區域。根據具體的環境，病毒可分為*檔案病毒*、*引導磁區病毒*、*指令碼病毒*和*巨集病毒*。

病毒可以使用多種不同的技術來感染檔案。*覆蓋*病毒會使用其代碼覆蓋受感染檔案的代碼，從而抹除檔案的內容。感染的檔案會停止發揮作用，且無法還原。*寄生*病毒會修改檔案，從而使自身發揮全部或部分功能。*伴隨病毒*不會修改檔案，而是建立副本。當您開啟受感染的檔案時會啟動此檔案的副本（實際上是病毒）。您也會遇到以下類型的病毒：*連結病毒*、*OBJ 病毒*、*LIB 病毒*、*原始程式碼病毒*和許多其他病毒。

蠕蟲

與典型病毒一樣，蠕蟲在侵入電腦後，其代碼將啟動並執行惡意操作。之所以稱為蠕蟲，是因為它們能夠從一台電腦“爬”到另一台電腦，並不需使用者權限即可透過許多資料通道來傳播副本。

可用於區分各種類型蠕蟲的主要特徵是蠕蟲的傳播方式。下表提供了各種類型蠕蟲的概覽，這些蠕蟲按其傳播方式進行了分類。

蠕蟲傳播方式

類型	名稱	描述
電子郵件蠕蟲	電子郵件蠕蟲	這些蠕蟲透過電子郵件傳播。 受感染的電子郵件訊息包含帶有蠕蟲副本的附件，或指向上傳到可能已被攻擊或者專門建立用於傳播蠕蟲的網站上某檔案的連結。開啟此附件時，蠕蟲將被啟動。在您點擊此連結，進行下載，然後開啟檔案時，蠕蟲還會開始執行其惡意操作。之後，蠕蟲會繼續傳播其副本，搜尋其他電子郵件信箱，並向它們傳送受感染的郵件。
IM 蠕蟲	即時通訊用戶端蠕蟲	它們透過 IM 傳播。 通常，此類蠕蟲會利用使用者的連絡人清單傳送訊息，其中包含指向某網站上帶有蠕蟲副本的檔案的連結。使用者下載並開啟檔案時，蠕蟲將被啟動。
IRC 蠕蟲	網際網路聊天蠕蟲	這些蠕蟲會透過網際網路中繼聊天（允許透過網際網路與其他人即時通信的服務系統）傳播。 這些蠕蟲會在網際網路聊天中發佈包含自身副本的檔案或指向此檔案的連結。使用者下載並開啟檔案時，蠕蟲將被啟動。
網路蠕蟲	網路蠕蟲	這些蠕蟲透過電腦網路傳播。 與其他類型的蠕蟲不同，典型的網路蠕蟲不需使用者參與即可傳播。它會掃描區域網路來尋找安裝了有弱點的程式的電腦。為此，它會傳送特殊格式的網路封包（弱點），其中包含蠕蟲代碼或部分蠕蟲代碼。如果網路上存在“有弱點”的電腦，此電腦會接收到此種網路封包。蠕蟲完全入侵電腦後，將被啟動。
P2P 蠕蟲	檔案共用網路蠕蟲	它們透過點對點檔案共用網路傳播。 為了滲透到 P2P 網路，蠕蟲會將自身複製到通常位於使用者電腦上的檔案共用資料夾中。P2P 網路會顯示有關此檔案的資訊，以便使用者可以在網路中像任何其他檔案一樣“找到”受感染的檔案，然後下載並開啟此檔案。 更加狡猾的蠕蟲會模仿特定 P2P 網路的網路協定：它們會返回對搜尋程式的積極回應，並提供自身的副本供下載。
蠕蟲	其他類型的蠕蟲	其他類型的蠕蟲包括： • 透過網路資源傳播自身副本的蠕蟲。透過使用作業系統的功能，它們掃描可用的網路資料夾，連線到網際網路上的電腦，並嘗試獲取對磁碟機的完全存取。與之前描述的蠕蟲類型不同，其他類型的蠕蟲不會自行啟動，而是在使用者開啟包含蠕蟲副本的檔案時啟動。 • 不使用上表中所述的任何方式進行傳播的蠕蟲（例如，透過手機傳播的蠕蟲）。

- **木馬程式**

  子類別：木馬程式

  危險等級：高

  與蠕蟲和病毒不同，木馬不能進行自我複製。例如，使用者存取受感染的網頁時，它們會透過電子郵件或瀏覽器侵入電腦。木馬透過使用者參與而啟動。木馬啟動後即會開始執行惡意操作。

  在受感染的電腦上，不同的木馬會表現出不同的行為。木馬的主要功能包括封鎖、修改或破壞資訊，以及停用電腦或網路。木馬還可以接收或傳送檔案，在螢幕上顯示訊息，請求網頁，下載和安裝程式，以及重新啟動電腦。

  駭客通常使用各種不同木馬的"集合"。

  下表中介紹了木馬行為的類型。

  受感染電腦上木馬行為的類型

類型	名稱	描述
木馬炸彈	木馬 –"壓縮檔案炸彈"	解壓縮時，這些壓縮檔案的大小會急劇增加，從而影響電腦的操作。 使用者嘗試解壓縮這種壓縮檔案時，電腦可能會執行緩慢或停止執行；硬碟可能會充滿"空白"資料。"壓縮檔案炸彈"對於檔案和郵件伺服器尤為危險。如果伺服器使用自動系統處理接收資訊，則"壓縮檔案炸彈"可能會中斷伺服器執行。
後門	用於遠端管理的木馬	此種木馬被視為最危險的木馬類型。在功能方面，這些木馬與安裝在電腦上的遠端管理應用程式相似。 這些程式會在不被使用者發覺的情況下將自身安裝到電腦上，以便入侵者遠端管理電腦。
木馬	木馬	木馬包括以下惡意應用程式： • **典型木馬**。這些程式僅執行木馬的主要功能：封鎖、修改或破壞資訊，以及停用電腦或網路。它們沒有任何進階功能，與表中描述的其他類型的木馬不同。 • **萬能木馬**。這些程式具有多種典型木馬類型的進階功能。
勒索木馬	勒索木馬	這些木馬將使用者資訊作為"人質"，修改或封鎖資訊，或者影響電腦的操作，以使使用者無法使用資訊。入侵者向使用者進行勒索，許諾傳送應用程式來還原電腦的效能以及電腦上儲存的資料。
木馬點擊器	木馬點擊器	這些木馬透過自行向瀏覽器傳送指令或變更在作業系統檔案中指定的網址的方式，從使用者的電腦存取網頁。 透過使用這些程式，入侵者進行網路攻擊並提高網站存取量，從而增加條幅廣告的顯示次數。
木馬下載器	木馬下載器	這些木馬會存取入侵者的網頁，從中下載其他惡意應用程式，並將它們安裝到使用者的電腦。這些木馬包含要下載的惡意應用程式的檔案名稱，或從存取的網頁中接收此檔案名稱。
木馬釋放器	木馬釋放器	這些木馬包含安裝在硬碟磁碟機上並隨後進行安裝的其他木馬。 入侵者可能會使用木馬釋放器類型的程式來達到以下目的： • 未通知使用者就安裝惡意應用程式：木馬釋放器類型的程式不會顯示訊息，或者會顯示虛假訊息，例如通知壓縮檔案中存在錯誤或作業系統的版本不相容。 • 防護另一個已知惡意應用程式不被偵測：並非所有病毒防護軟體都可偵測到木馬釋放器類型應用程式中的惡意應用程式。
通知型木馬	通知型木馬	這些木馬會通知入侵者受感染的電腦可供存取，並向入侵者傳送有關電腦的資訊：IP 位址、已開放埠號或電子郵件信箱。它們透過電子郵件、FTP、存取入侵者的網頁或以其他方式與入侵者聯絡。 通知型木馬類型的程式通常用於包含多種木馬的集合中。這些木馬會通知入侵者其他木馬已成功安裝到使用者的電腦。
代理型木馬	代理型木馬	這些木馬允許入侵者使用使用者的電腦匿名存取網頁，它們通常用於傳送垃圾郵件。
木馬 PSW	密碼竊盜軟體	密碼竊盜軟體是竊盜使用者帳戶（如軟體註冊資料）的一種木馬。這些密碼會尋找系統檔案和登錄檔中包含的機密資料，並透過電子郵件、FTP、存取入侵者的網頁或以其他方式將機密資料傳送給"攻擊者"。 部分這些木馬分類為此表中敘述的單獨類型。這些木馬會盜竊銀行帳戶（網銀竊賊木馬），竊取 IM 用戶端使用者的資料（IM 木馬），以及盜竊線上遊戲使用者的資訊（遊戲竊賊木馬）。
間諜木馬	間諜木馬	這些木馬暗中監視使用者，收集有關使用者使用電腦時所做的操作的資訊。它們可能會攔截使用者透過鍵盤輸入的資料，截取螢幕，或收集活動應用程式的清單。收到資訊後，這些木馬會透過電子郵件、FTP、存取入侵者的網頁或以其他方式將資訊傳輸給入侵者。

類型	名稱	描述
分散式拒絕服務攻擊木馬	木馬網路攻擊者	這些木馬會從使用者電腦將大量請求傳送至遠端伺服器。伺服器缺少資源來處理所有請求，因此會停止執行（拒絕服務，或簡稱為 DoS）。駭客通常會使用這些程式感染許多電腦，以使用這些電腦來同時攻擊一個伺服器。 DoS 程式在使用者知悉的情況下從一台電腦發起攻擊。DDoS（分散式 DoS）程式在不被受感染電腦使用者發覺的情況下從多台電腦發起分散式攻擊。
木馬 IM	從 IM 用戶端使用者那裡竊取資訊的木馬	它們會竊取 IM 用戶端使用者的帳戶和密碼。這些木馬會透過電子郵件、FTP、存取入侵者的網頁或以其他方式將資料傳輸給入侵者。
Rootkit	Rootkits	這些木馬會掩蓋其他惡意應用程式及其活動，從而延長這些應用程式在作業系統中持續存在的時間。它們還會隱藏檔案、受感染電腦記憶體中的處理程序或執行惡意應用程式的登錄機碼。 Rootkit 會掩蓋使用者電腦上的應用程式與網路上其他電腦之間進行的資料交換。
簡訊型木馬	SMS 格式的木馬	這些木馬會感染手機，向額外收費的手機號碼傳送 SMS。
遊戲竊賊木馬	從線上遊戲使用者那裡竊取資訊的木馬	這些木馬會竊取線上遊戲使用者的帳戶憑證，然後將這些憑證透過電子郵件、FTP、存取駭客的網頁或以其他方式傳送給駭客。
網銀竊賊木馬	竊取銀行帳戶的木馬	這些木馬會竊取銀行帳戶資料或電子貨幣系統資料，然後將這些資料透過電子郵件、FTP、存取駭客的網頁或以其他方式傳送給駭客。
郵件偵測木馬	收集電子郵件信箱的木馬	這些木馬會收集儲存在電腦上的電子郵件信箱，然後透過電子郵件、FTP、存取入侵者的網頁或以其他方式將它們傳送給入侵者。入侵者可能會向收集到的位址傳送垃圾郵件。

- **惡意工具**

  子類別：惡意工具

  危險等級：中

  與其他類型的惡意軟體不同，惡意工具在啟動過後不會執行其操作。惡意工具可以在使用者的電腦上安全地儲存和啟動。入侵者通常使用這些程式的功能來建立病毒、蠕蟲和木馬，對遠端伺服器進行網路入侵，攻擊電腦或執行其他惡意操作。

  惡意工具的各種功能按下表中所述的類型進行分組。

  惡意工具的功能

類型	名稱	描述
構建器	構建器	透過它們可以建立新的病毒、蠕蟲和木馬。一些構建器揚言構建了基於視窗的標準介面，使用者可在此介面中選擇要建立的惡意應用程式的類型，對付偵錯工具的方式，以及其他功能。
拒絕服務攻擊	網路攻擊	這些木馬會從使用者電腦將大量請求傳送至遠端伺服器。伺服器缺少資源來處理所有請求，因此會停止執行（拒絕服務，或簡稱為 DoS）。
弱點利用	弱點	*弱點*是一組資料或程式碼，利用處理它們的應用程式的缺陷對電腦執行惡意操作。例如，弱點可以寫入或讀取檔案，或請求"受感染"的網頁。 不同的弱點會利用不同應用程式或網路服務的缺陷。弱點會偽裝成網路封包透過網路傳輸到許多電腦，然後搜尋網路服務存在缺陷的電腦。DOC 檔案中的弱點會利用文字編輯器的缺陷。在使用者開啟受感染的檔案時，它可能會開始執行駭客程式設計的操作。嵌入在電子郵件訊息中的弱點會搜尋電子郵件用戶端的缺陷。使用者在電子郵件用戶端中開啟受感染的郵件時，弱點會立即開始執行惡意操作。 網路蠕蟲會使用弱點透過網路進行傳播。Nuker 弱點是可停用電腦的網路封包。
檔案加密器	加密器	加密器會加密其他惡意應用程式，以隱藏它們不被防毒應用程式發現。
洪水攻擊器	用於"污染"網路的程式	這些程式會透過網路通道傳送大量郵件。例如，此類型的工具包括污染網際網路中繼聊天的程式。 洪水攻擊器工具不包括"污染"電子郵件、IM 用戶端以及行動通信系統所使用通道的程式。這些程式可分為表中介紹的各種類型（電子郵件洪水攻擊器、IM 洪水攻擊器和 SMS 洪水攻擊器）。
駭客工具	駭客工具	這些工具可以破壞其所在的電腦，或攻擊其他電腦（例如，未經使用者許可新增新系統帳戶，或清除系統日誌以隱藏在作業系統中的存在路徑）。這種類型的工具包括一些具有惡意功能的嗅探器，例如密碼截取。嗅探器是允許檢視網路流量的程式。
惡作劇程式	惡作劇程式	這些程式會警告使用者類似病毒的訊息：它們可能會在未受感染的檔案中"偵測到病毒"，或通知使用者磁碟已被格式化，儘管這些情況實際並未發生。

類型	名稱	描述
位址欺騙程式	位址欺騙工具	這些工具使用偽造的寄件者位址傳送郵件和網路請求。例如，入侵者會使用位址欺騙程式類型的工具來掩蓋他們作為郵件實際寄件者的事實。
病毒修改工具	修改惡意應用程式的工具	透過這些工具可以修改其他惡意軟體，隱藏它們不被防毒程式發現。
電子郵件洪水攻擊器	"污染"電子郵件信箱的程式	這些程式會向各種電子郵件信箱傳送大量郵件，從而"污染"這些位址。大量的接收郵件會妨礙使用者檢視收件箱中的有用郵件。
IM 洪水攻擊器	"污染"IM 流量的程式	它們向 IM 的使用者傳送大量訊息。大量的資訊會妨礙使用者檢視有用的接收資訊。
SMS 洪水攻擊器	使用 SMS"污染"流量的程式	這些程式向手機傳送大量 SMS。

- **廣告軟體**

  子類別：廣告軟體

  危險等級：中

  廣告軟體向使用者顯示廣告資訊。廣告軟體程式會在其他程式的介面中顯示條幅廣告，並將搜尋查詢重新導向至廣告網頁。某些廣告軟體程式會收集有關使用者的行銷資訊，並將其傳送給開發者：此資訊可能包括使用者存取的網站的名稱，或使用者搜尋查詢的內容。與間諜木馬類型的程式不同，廣告軟體程式會在使用者許可的情況下將此資訊傳送給開發者。

- **自動撥號程式**

  子類別：自動撥號器（Dialer）。

  危險等級：中

  自動撥號器可以使用資料機秘密地建立電話連線。

- **可被入侵者利用以破壞您的電腦或個人資料的合法軟體**

  子類別：可被入侵者利用以破壞您的電腦或個人資料的合法軟體。

  危險等級：中

  大多數這些應用程式都很有用，因此有許多使用者使用它們。這些應用程式包括 IRC 用戶端、自動撥號器、檔案下載程式、電腦系統活動監控器、密碼實用程式以及用於 FTP、HTTP 和 Telnet 的網際網路伺服器。

  但是，如果入侵者獲得了這些程式的存取權限，或如果他們在使用者的電腦上安置這些程式，應用程式的某些功能可能會被用來危害安全。

  這些應用程式具有不同的功能，下表介紹了它們的類型。

類型	名稱	描述
Client-IRC	網際網路聊天用戶端	使用者安裝這些程式與他人進行網際網路中繼聊天。入侵者使用這些程式來傳播惡意軟體。
下載器	用於下載的程式	這些程式可以在隱藏模式下從網頁下載檔案。
監控器	用於監控的程式	這些程式可監控其安裝到的電腦上的活動（檢視哪些應用程式正在活動，以及它們如何與安裝在其他電腦上的應用程式交換資料）。

類型	名稱	描述
密碼工具	密碼還原器	透過它們可以檢視和還原已忘記的密碼。入侵者出於相同的目的，秘密地將它們安置在使用者的電腦上。
遠端管理程式	遠端管理程式	系統管理員廣泛使用的一些程式。透過這些程式可以獲取對遠端電腦介面的存取權限，以監控和管理此電腦。入侵者出於同樣的目的，秘密地將它們安置在使用者的電腦上：用於監控和管理遠端電腦。 合法的遠端管理程式與實現遠端管理的後門類型的木馬不同。木馬能夠獨自入侵作業系統並自行安裝；合法的程式則無法做到這些。
FTP 服務程式	FTP 伺服器	這些程式可起到 FTP 伺服器的作用。入侵者將它們安置在使用者電腦上，以開啟透過 FTP 對此電腦的遠端存取。
代理服務程式	代理伺服器	這些程式可起到代理伺服器的作用。入侵者將它們安置在使用者電腦上，以使用者名義傳送垃圾郵件。
Telnet 服務程式	Telnet 伺服器	這些程式可起到 Telnet 伺服器的作用。入侵者將它們安置在使用者電腦上，以開啟透過 Telnet 對此電腦的遠端存取。
Web 服務程式	Web 伺服器	這些程式可起到 Web 伺服器的作用。入侵者將它們安置在使用者電腦上，以開啟透過 HTTP 對此電腦的遠端存取。
風險工具	在本機電腦上工作的工具	在使用者自己的電腦上工作時，這些工具會為使用者提供其他選項。透過這些工具，使用者可以隱藏檔案或活動應用程式的視窗，並終止活動的處理程序。
網路工具	網路工具	與網路上的其他電腦配合工作時，這些工具會為使用者提供其他選項。透過這些工具可以進行重新啟動，偵測開放的連接埠，以及啟動安裝在電腦上的應用程式。
P2P 用戶端	P2P 網路用戶端	透過它們可以在對等網路中工作。入侵者可能會利用它們傳播惡意軟體。
Client-SMTP	SMTP 用戶端	它們未經使用者的同意便傳送電子郵件。入侵者將它們安置在使用者電腦上，以使用者名義傳送垃圾郵件。
Web 工具列	Web 工具列	它們會向其他應用程式的介面中新增工具列，以使用搜尋引擎。
欺騙工具	欺騙程式	這些程式將自己偽裝為其他程式。例如，一些欺騙防毒程式會顯示有關惡意軟體偵測的資訊。但實際上，它們並未找到任何內容或進行解毒。

- **可能被用來防護惡意程式碼的封裝物件**

  子類別：可能造成損害的封裝檔案。

  危險等級：中。

  檔案使用特殊的封裝程式進行封裝，該封裝程式用於封裝惡意軟體：病毒、蠕蟲、木馬。Kaspersky Embedded Systems Security 會掃描 SFX（自解壓）存檔中的解壓縮工具模組。

  為了隱藏惡意軟體不被防毒軟體偵測到，駭客會使用特殊的封裝程式對其進行封裝。卡巴斯基專家已識別出駭客最常使用的解壓縮工具。

- **多重封裝物件**

  子類別：多重封裝檔案。

  危險等級：中。

  該檔案被一個或多個封裝程式封裝了 3 次或更多次。

  為了隱藏惡意軟體不被防毒軟體偵測到，駭客可能會多次封裝檔案。Kaspersky Embedded Systems Security 將掃描封裝的檔案。

4. 儲存變更。

編輯信任應用程式清單

*受信任應用程式清單*包含應用程式的檔案和網路活動（包括可疑活動）以及對系統登錄檔的存取不受 Kaspersky Embedded Systems Security 的監控。預設情況下，Kaspersky Embedded Systems Security 將監控任何應用程式處理程序開啟、執行或儲存的物件，並控制所有應用程式的活動及其產生的網路流量。應用程式被新增到受信任應用程式清單後，Kaspersky Embedded Systems Security 將停止監控該應用程式的活動。

掃描排除項目和受信任的應用程式之間的區別在於，對於排除項目，Kaspersky Embedded Systems Security 不掃描檔案，而對於受信任的應用程式，它不控制啟動的處理程序。如果受信任的應用程式在未包含在掃描排除項目中的資料夾中建立惡意檔案，Kaspersky Embedded Systems Security 將偵測該檔案並消除威脅。如果資料夾被新增到排除項目，Kaspersky Embedded Systems Security 將略過該檔案。

例如，如果您認為由標準 Microsoft Windows 記事本應用程式使用的物件是安全的，也即您信任此應用程式，則您可將 Microsoft Windows 記事本新增到受信任應用程式清單中，這樣該應用程式使用的物件就不會被監控。這會提高電腦效能，在使用伺服器應用程式時尤為重要。

此外，Kaspersky Embedded Systems Security 分類為危險的特定操作，在很多應用程式的功能環境中可能是安全的。例如，攔截鍵盤輸入的內容，是自動鍵盤設定切換器中的一種例行程式（例如 Punto Switcher）。考慮到此類程式的特點並將其行為從監控中排除，我們建議您可將此類程式新增到信任應用程式清單中。

受信任的應用程式有助於避免 Kaspersky Embedded Systems Security 與其他應用程式之間的相容性問題（例如，Kaspersky Embedded Systems Security 和另一個病毒防護應用程式對第三方電腦的網路流量進行雙重掃描的問題）。

同時，信任應用程式的可執行檔和處理程序仍然會掃描病毒和其他惡意軟體。您可以透過掃描排除項目將應用程式從 Kaspersky Embedded Systems Security 掃描中完全排除。

Kaspersky Embedded Systems Security 不支援包含超過 5000 個物件的受信任應用程式清單。

如何在卡巴斯基安全管理中心管理主控台中將應用程式新增到受信任清單中

1. 在卡巴斯基安全管理中心管理主控台樹狀目錄中，選取**政策**。
2. 選擇必要的政策並點擊以開啟政策內容。
3. 在政策視窗中，選取**"補充"**。
4. 在**"受信任區域"**塊中，點擊**"設定"**按鈕。
5. 在開啟的視窗中選擇**"受信任應用程式"**標籤。

   這將開啟包含受信任應用程式清單的視窗。
6. 如果檔案讀取操作由安裝在受防護裝置上的備份工具執行，而您想要略過掃描此類操作，請選擇**不檢查檔案備份作業**核取方塊。
7. 如果要為公司內的所有電腦建立受信任应用程式的綜合清單，請選取**"繼承時合併值"**核取方塊。將合併父政策和子政策中的受信任應用程式清單。如果啟用繼承時合併值，則將合併清單。父政策中的受信任應用程式以唯讀視圖的形式顯示在子政策中。無法變更或刪除父政策的受信任應用程式

8. 如果想要使用者能夠建立本機受信任應用程式清單，請選中**"允許編輯本機受信任應用程式"**核取方塊。這樣，除了在政策中產生的受信任應用程式的一般清單外，使用者还可以建立自己的受信任應用程式的本機清單。管理員可以使用卡巴斯基安全管理中心檢視、新增、編輯或刪除電腦屬性中的清單項目。

   如果核取方塊被清理，使用者只能存取政策中產生的受信任應用程式的一般清單。此外，如果清除此核取方塊，Kaspersky Embedded Systems Security 會在應用程式主控台中隱藏受信任應用程式的合併清單。

9. 選擇 **不檢查指定處理程序的檔案活動** 核取方塊可略過掃描受信任處理程序的檔案操作。

10. 點擊**新增** 並選擇一個操作：

    - **類別**您可以將受信任的應用程式分為不同的類別。若要建立新類別，請輸入類別名稱並在該類別中新增至少一個受信任的應用程式。
    - **新排除項目**Kaspersky Embedded Systems Security 會將新的受信任應用程式新增至清單的根目錄。
    - **所選類別中新排除項目**若要將新的受信任應用程式新增至特定類別，請選擇一個類別。
    - **從清單中選取排除項目**若要快速設定 Kaspersky Embedded Systems Security，您可以從預先定義的受信任應用程式清單中新增應用程式。

11. 在開啟的視窗中，選擇 **使用磁碟上的處理程序完整路徑將其視為受信任** 核取方塊並輸入檔案路徑以確定該處理程序是否受信任。

    Kaspersky Embedded Systems Security 輸入遮罩時支援環境變量以及`*`和`?`字元：

    > 當在卡巴斯基安全管理中心主控台中產生受信任應用程式清單時，Kaspersky Embedded Systems Security 不支援"`%userprofile%`"環境變量。若要將項目套用到所有使用者帳戶，您可以使用 * 字元（例如，`C:\Users\*\Documents\File.exe`）。無論何時新增新的環境變數，您都需要重啟應用程式。

12. 為受信任應用程式配置進階設定（請參閱下表）。

13. 點擊**"確定"**。

    新的受信任應用程式將被新增到清單中。您可以隨時使用物件旁邊的核取方塊將應用程式從受信任區域中排除。

14. 儲存變更。

如何在卡巴斯基安全管理中心網頁主控台中將應用程式新增到受信任清單中

1. 在卡巴斯基安全管理中心管理主控台樹狀目錄中，選取**政策**。
2. 選擇必要的政策並點擊以開啟政策內容。
3. 點擊 Kaspersky Embedded Systems Security 政策的名稱。

   政策內容視窗將開啟。

4. 選擇**"應用程式設定"**標籤。
5. 轉到**補充 → 受信任區域** 並點擊 **配置** 按鈕。
6. 在開啟的視窗中選擇**"受信任應用程式"**標籤。
7. 如果檔案讀取操作由安裝在受防護裝置上的備份工具執行，而您想要略過掃描此類操作，請選擇**不檢查檔案備份作業**核取方塊。

8. 如果要為公司內的所有電腦建立受信任应用程式的綜合清單，請選取**"繼承時合併值"**核取方塊。將合併父政策和子政策中的受信任應用程式清單。如果啟用繼承時合併值，則將合併清單。父政策中的受信任應用程式以唯讀視圖的形式顯示在子政策中。無法變更或刪除父政策的受信任應用程式

9. 如果想要使用者能夠建立本機受信任應用程式清單，請選中**"允許編輯本機受信任應用程式"**核取方塊。這樣，除了在政策中產生的受信任應用程式的一般清單外，使用者还可以建立自己的受信任應用程式的本機清單。管理員可以使用卡巴斯基安全管理中心檢視、新增、編輯或刪除電腦屬性中的清單項目。

   如果核取方塊被清理，使用者只能存取政策中產生的受信任應用程式的一般清單。此外，如果清除此核取方塊，Kaspersky Embedded Systems Security 會在應用程式主控台中隱藏受信任應用程式的合併清單。

10. 選擇 **不檢查指定處理程序的檔案活動** 核取方塊可略過掃描受信任處理程序的檔案操作。

11. 點擊**新增** 並選擇一個操作：

    - **類別**您可以將受信任的應用程式分為不同的類別。若要建立新類別，請輸入類別名稱並在該類別中新增至少一個受信任的應用程式。
    - **新排除項目**Kaspersky Embedded Systems Security 會將新的受信任應用程式新增至清單的根目錄。
    - **所選類別中新排除項目**若要將新的受信任應用程式新增至特定類別，請選擇一個類別。
    - **從清單中選取排除項目**若要快速設定 Kaspersky Embedded Systems Security，您可以從預先定義的受信任應用程式清單中新增應用程式。

12. 在開啟的視窗中，選擇 **使用磁碟上的處理程序完整路徑將其視為受信任** 核取方塊並輸入檔案路徑以確定該處理程序是否受信任。

    Kaspersky Embedded Systems Security 輸入遮罩時支援環境變量以及`*`和`?`字元：

    > 當在卡巴斯基安全管理中心主控台中產生受信任應用程式清單時，Kaspersky Embedded Systems Security 不支援**"%userprofile%"**環境變量。若要將項目套用到所有使用者帳戶，您可以使用 * 字元（例如，`C:\Users\*\Documents\File.exe`）。無論何時新增新的環境變數，您都需要重啟應用程式。

13. 為受信任應用程式配置進階設定（請參閱下表）。

14. 點擊**"確定"**。

    新的受信任應用程式將被新增到清單中。您可以隨時使用**操作**列中的核取方塊將應用程式排除在受信任區域之外。

15. 儲存變更。

如何在應用程式主控台中將應用程式新增到受信任清單中

1. 在應用程式主控台樹狀目錄中，選擇 **Kaspersky Embedded Systems Security** 節點然後從節點的上下文選單中選擇 **受信任區域**。

   開啟**"配置信任區域設定"**視窗。

2. 在 **排除項目** 部分，點擊**受信任應用程式** 區塊旁邊的 **設定** 按鈕。

3. 點擊**新增** 並選擇一個操作：

   - **類別**您可以將受信任的應用程式分為不同的類別。若要建立新類別，請輸入類別名稱並在該類別中新增至少一個受信任的應用程式。
   - **新排除項目**Kaspersky Embedded Systems Security 會將新的受信任應用程式新增至清單的根目錄。
   - **所選類別中新排除項目**若要將新的受信任應用程式新增至特定類別，請選擇一個類別。
   - **從清單中選取排除項目**若要快速設定 Kaspersky Embedded Systems Security，您可以從預先定義的受信任應用程式清單中新增應用程式。

4. 從清單中選擇一個檔案或輸入受信任應用程式的可執行檔的路徑。

   Kaspersky Embedded Systems Security 輸入遮罩時支援環境變量以及`*`和`?`字元：

   > Kaspersky Embedded Systems Security 支援環境變數同時，Kaspersky Embedded Systems Security 會在應用程式本機介面中轉換路徑。換言之，如果您輸入檔案路徑 `%userprofile%\Documents\File.exe`，將為使用者 Fred123 在應用程式的本機介面中新增 `C:\Users\Fred123\Documents\File.exe` 記錄。因此，Kaspersky Embedded Systems Security 會忽略針對其他使用者的 `File.exe` 受信任程式。若要將項目套用到所有使用者帳戶，您可以使用 `*` 字元（例如，`C:\Users\*\Documents\File.exe`）。

   > 無論何時新增新的環境變數，您都需要重啟應用程式。

5. 為受信任應用程式配置進階設定（請參閱下表）。

6. 點擊**"確定"**。

   新的受信任應用程式將被新增到清單中。您可以隨時使用物件名稱旁邊的核取方塊將應用程式從受信任區域中排除。

7. 儲存變更。

受信任應用程式設定

參數	描述
使用磁碟上的完整處理程序路徑來將它視為受信任	Kaspersky Embedded Systems Security 將使用檔案的完整路徑來確定處理程序是否受信任。
使用處理程序檔案雜湊來將它視為受信任	Kaspersky Embedded Systems Security 將使用選定的檔案雜湊來確定處理程序信任狀態。如果清除該核取方塊，則不使用檔案雜湊來確定處理程序信任狀態。
規則使用	您可以設定不監控受信任應用程式活動的 Kaspersky Embedded Systems Security 元件清單： • **即時檔案防護**如果啟用此功能，Kaspersky Embedded Systems Security 將排除掃描使用受信任應用程式開啟的所有檔案。預設啟用該選項。 • **註冊表存取監控**如果啟用此功能，Kaspersky Embedded Systems Security 不會監控受信任應用程式對 系統完整性監控 元件監控範圍內的登錄機碼所做的變更。預設情況下，該功能處於停用狀態。 • **行為偵測和弱點利用防禦**如果啟用此功能，Kaspersky Embedded Systems Security 不會使用行為偵測和 弱點利用防禦 元件監控作業系統中受信任應用程式的檔案和網路活動。預設情況下，該功能處於停用狀態。 • **與 AMSI 掃描程式元件的互動**如果啟用此功能，Kaspersky Embedded Systems Security 不會監控受信任應用程式向 AMSI 掃描程式 元件發出的要求。預設情況下，該功能處於停用狀態。 • **檔案完整性監控**如果啟用此功能，Kaspersky Embedded Systems Security 不會監控受信任應用程式對 系統完整性監控 元件監控範圍內的檔案所做的變更。預設情況下，該功能處於停用狀態。 • **應用程式啟動控制**如果啟用此功能，Kaspersky Embedded Systems Security 不會使用 應用程式啟動控制 元件監控受信任應用程式的啟動。預設情況下，該功能處於停用狀態。 對於預先定義的受信任應用程式，除了 **應用程式啟動控制** 外，所有功能預設皆為啟用。

參數	描述
允許與應用程式介面互動	Kaspersky Embedded Systems Security 可封鎖從遠端電腦管理應用程式服務的所有嘗試。如果選擇該核取方塊，則允許遠端存取應用程式透過 Kaspersky Embedded Systems Security 介面管理 Kaspersky Embedded Systems Security 設定。
不監控子應用程式活動	Kaspersky Embedded Systems Security 將不會監控該應用程式啟動的應用程式的檔案活動或網路活動。您可以遞歸套用排除項目。在此情況下，應用程式不會監控整個子應用程式鏈的活動。
不繼承父處理程序(應用程式)的限制	Kaspersky Embedded Systems Security 不會將為父程序配置的限制套用於子程序。父處理程序由為其配置了應用程式權限和應用程式網路規則的應用程式啟動。
不掃描處理程序記憶體	Kaspersky Embedded Systems Security 不會掃描處理程序記憶體。

建立本機信任區域

使用者現在可以為特定電腦建立自己的本機信任區域。這樣，除了政策中的一般受信任區域之外，使用者還可以建立自己的"掃描排除項目"和"受信任應用程式"的本機清單。管理員可以在政策設定中允許或封鎖使用本機排除項目或本機受信任的應用程式。為此，請使用政策的**受信任區域**部分中**掃描排除項目** 和 **受信任應用程式**頁簽上的**允許使用本機排除項目** 和 **允許編輯本機受信任應用程式**核取方塊。

如果管理員允許建立本機信任區域，則使用者可以在應用程式主控台中新增自己的掃描排除項目和受信任應用程式。同時，使用者無權修改或刪除政策中配置的信任區域中的物件。如果需要為單台電腦新增排除項目，管理員還可以在卡巴斯基安全管理中心主控台中查看、新增、修改或刪除清單項目。

如果管理員在主控台中封鎖受信任區域的配置（"關閉的鎖"符號）並且禁止本機掃描排除項目和受信任應用程式，Kaspersky Embedded Systems Security 將在應用程式主控台中隱藏掃描排除項目和受信任應用程式清單。

如何在卡巴斯基安全管理中心管理主控台中將物件新增到本機受信任區域中

1. 在管理主控台樹狀目錄的"**受管理裝置**"資料夾中，開啟相關用戶端電腦所屬的管理群組名稱的資料夾。
2. 在工作區選取"**裝置**"標籤。
3. 點擊以開啟電腦內容視窗。
4. 在電腦內容視窗中，選取"**應用程式**"區域。
5. 在電腦上安裝的 Kaspersky 應用程式清單中，選取 **Kaspersky Embedded Systems Security** 並點擊以開啟應用程式內容。
6. 在應用程式設定視窗中，選取**補充 → 受信任區域** 然後點擊 **設定**。
7. 在**掃描排除項目**頁簽上，製作本機掃描排除項目清單。

   建立本機掃描排除項目的規則與一般排除項目的規則相同。Kaspersky Embedded Systems Security 輸入遮罩時支援環境變量以及`*`和`?`字元：
8. 在**受信任應用程式**頁簽上，製作本機受信任應用程式清單。這將開啟包含本機受信任應用程式清單的視窗。

   新增應用程式到本機可信應用程式清單的規則與將它們新增到一般清單的規則相同。Kaspersky Embedded Systems Security 輸入遮罩時支援環境變量以及`*`和`?`字元：
9. 儲存變更。

如何在卡巴斯基安全管理中心網頁主控台中將物件新增到本機受信任區域中

1. 在網頁主控台的主視窗中，選擇**資產管理 → 資產（裝置）**。
2. 點擊您想要允許使用者在上面執行被封鎖操作的電腦的名稱。
3. 選擇**"應用程式"**標籤。
4. 點擊 **Kaspersky Embedded Systems Security**。

   這將開啟本機應用程式設定。
5. 選擇**"應用程式設定"**標籤。
6. 在應用程式設定視窗中，選取**補充 → 受信任區域** 然後點擊 **配置**。

   開啟**"排除項目和偵測到的物件類型"**視窗。
7. 在**掃描排除項目**頁簽上，製作本機掃描排除項目清單。

   建立本機排除項目的規則與建立一般排除項目的規則相同。Kaspersky Embedded Systems Security 輸入遮罩時支援環境變量以及`*`和`?`字元：
8. 在**受信任應用程式**頁簽上，製作本機受信任應用程式清單。

   新增應用程式到本機可信應用程式清單的規則與將它們新增到一般清單的規則相同。Kaspersky Embedded Systems Security 輸入遮罩時支援環境變量以及`*`和`?`字元：
9. 儲存變更。

如何在應用程式主控台中建立本機掃描排除項目

1. 在應用程式主控台樹狀目錄中，選擇 **Kaspersky Embedded Systems Security** 節點然後從節點的上下文選單中選擇 **受信任區域**。

   開啟**"配置信任區域設定"**視窗。
2. 在 **掃描排除項目和受信任應用程式** 部分，點擊**本機掃描排除項目** 區塊旁邊的 **設定** 按鈕。

   如果管理員在卡巴斯基安全管理中心管理主控台中封鎖掃描排除項目的配置（"關閉的鎖"符號）並且禁止本機掃描排除項目（ **允許使用本機排除項目** 核取方塊被清除），Kaspersky Embedded Systems Security 將在應用程式主控台中隱藏掃描排除項目清單。
3. 點擊**新增** 並選擇一個操作：

   - **類別**您可以將掃描排除項目分組到不同的類別。若要建立新類別，請輸入類別名稱並在該類別中新增至少一個掃描排除項目。
   - **新排除項目**Kaspersky Embedded Systems Security 會將新的掃描排除項目新增至清單的根目錄。
   - **所選類別中新排除項目**若要將新的掃描排除項目新增至特定類別，請選擇一個類別。
   - **從清單中選取排除項目**若要快速設定 Kaspersky Embedded Systems Security，您可以從預先定義的掃描排除項目清單中新增排除項目。
4. 選擇 **新排除項目** 可開啟 **掃描排除項目** 視窗。

5. 要從掃描中排除某個檔案或資料夾，請選擇**檔案或資料夾**核取方塊。點擊**選擇檔案或資料夾。** 連結開啟一個視窗，然後在該視窗中點擊 **瀏覽** 選擇檔案或資料夾。

   您也可以手動輸入路徑。Kaspersky Embedded Systems Security 輸入遮罩時支援環境變量以及`*`和`?`字元：

   - `*`（星號）字元代表任意一組字元，但 `\` 和 `/` 字元除外（這兩個字元是檔案和資料夾路徑中的檔案和資料夾名稱的分隔符號）。例如，遮罩"`C:\*\*.txt`"將包括位於 C: 磁碟機但是不在子資料夾中所有帶 TXT 副檔名的檔案的路徑。

   - 兩個連續 `*` 字元在檔案或資料夾名稱中代表任意一組字元（包括空集），包括 `\` 和 `/` 字元（這兩個字元是檔案和資料夾路徑中的檔案和資料夾名稱的分隔符號）。例如，遮罩 `C:\Folder\**\*.txt` 將包括位於巢嵌在 `Folder` 內的資料夾（`Folder`自身除外）中所有帶 TXT 副檔名的檔案的路徑。遮罩必須包含至少一個嵌套等級。遮罩 `C:\**\*.txt` 不是有效遮罩。

   - `?`（問號）字元代表任意單個字元，但 `\` 和 `/` 字元除外（這兩個字元是檔案和資料夾路徑中的檔案和資料夾名稱的分隔符號）。例如，遮罩 `C:\Folder\???.txt` 將包括位於 `Folder` 資料夾中所有帶 TXT 副檔名且名稱由三個字元構成的檔案的路徑。

     您可以在路徑的開始、中間或者結尾使用遮罩。例如，如果您想要將一個針對所有使用者的資料夾新增到排除項目，請輸入 `?:\Users\*\Folder\` 遮罩。

6. 若要從掃描中排除預定義區域，請選擇 **預定義範圍** 核取方塊。點擊**選擇預定義範圍** 連結可開啟一個視窗，然後在該視窗中選擇受防護裝置上的一個標準範圍。

7. 若要從掃描中排除特定物件，請選擇 **偵測到的物件類型** 核取方塊。點擊**輸入物件名稱**連接，點擊 **新增** 按鈕，在顯示的視窗中根據 卡巴斯基百科全書 分類（例如，`Email-Worm`、`Rootkit` 或者 `RemoteAdmin`）輸入物件類型的名稱。

   您可以用`?`字元（替換任何單個字元）和`*`字元（替換任意數量的字元）來使用遮罩。例如，如果指定了 `Client*`遮罩，則 Kaspersky Embedded Systems Security 將從掃描中排除`Client-IRC`、`Client-P2P`和 `Client-SMTP`物件。

8. 若要從掃描中排除單個檔案，請選擇 **物件雜湊** 核取方塊。點擊 **輸入物件雜湊** 連結開啟一個視窗，然後在該視窗中輸入檔案雜湊。

   如果檔案被修改，檔案雜湊也將被修改。如果發生這種情況，修改後的檔案將不會新增到排除項目中。

9. 在"**規則使用範圍**"塊中，選擇要掃描排除項目套用的元件。

10. 如有必要，在"**註解**"欄位，輸入您建立的掃描排除項目的簡要說明。

11. 儲存變更以將排除項目新增至清單。您可以使用物件旁邊的核取方塊隨時停用排除項目。

如何在應用程式主控台中將應用程式新增到本機受信任應用程式清單中

1. 在應用程式主控台樹狀目錄中，選擇 **Kaspersky Embedded Systems Security** 節點然後從節點的上下文選單中選擇 **受信任區域**。

   開啟"**配置信任區域設定**"視窗。

2. 在 **排除項目** 部分，點擊**本機受信任應用程式** 區塊旁邊的 **設定** 按鈕。

   如果管理員在卡巴斯基安全管理中心管理主控台中受信任應用程式的配置（"關閉的鎖"符號）並且禁止本機受信任應用程式（ **允許編輯本機受信任應用程式** 核取方塊被清除），Kaspersky Embedded Systems Security 將在應用程式主控台中隱藏受信任應用程式合併清單。

3. 點擊**新增** 並選擇一個操作：

   - **類別**您可以將受信任的應用程式分為不同的類別。若要建立新類別，請輸入類別名稱並在該類別中新增至少一個受信任的應用程式。
   - **新排除項目**Kaspersky Embedded Systems Security 會將新的受信任應用程式新增至清單的根目錄。
   - **所選類別中新排除項目**若要將新的受信任應用程式新增至特定類別，請選擇一個類別。
   - **從清單中選取排除項目**若要快速設定 Kaspersky Embedded Systems Security，您可以從預先定義的受信任應用程式清單中新增應用程式。

4. 選擇 **新排除項目** 可開啟 **掃描排除項目** 視窗。

5. 選擇 **使用磁碟上的處理程序完整路徑將其視為受信任** 核取方塊並輸入受信任應用程式的可執行檔的路徑。

   Kaspersky Embedded Systems Security 輸入遮罩時支援環境變量以及`*`和`?`字元：

   > Kaspersky Embedded Systems Security 支援環境變數同時，Kaspersky Embedded Systems Security 會在應用程式本機介面中轉換路徑。換言之，如果您輸入檔案路徑 `%userprofile%\Documents\File.exe`，將為使用者 Fred123 在應用程式的本機介面中新增 `C:\Users\Fred123\Documents\File.exe` 記錄。因此，Kaspersky Embedded Systems Security 會忽略針對其他使用者的 `File.exe` 受信任程式。若要將項目套用到所有使用者帳戶，您可以使用 `*` 字元（例如，`C:\Users\*\Documents\File.exe`）。

   > 無論何時新增新的環境變數，您都需要重啟應用程式。

6. 在"受信任應用程式屬性"視窗中，配置進階設定。

7. 儲存變更以將排除項目新增至清單。

匯出和匯入受信任區域

*信任區域*是在其有效時，管理員建立的 Kaspersky Embedded Systems Security 不進行監控的物件和應用程式的清單。信任區域由以下清單組成：*掃描排除項目*和*受信任應用程式*。然後，您可以修改檔案，例如，新增大量相同類型的排除項目。您還可以使用匯出/匯入功能來備份排除項目清單和受信任應用程式清單，或將清單遷移到其他伺服器。

該應用程式使用 XML 格式匯出和匯入 *排除項目清單* 和受信任應用程式。

> Kaspersky Embedded Systems Security 不支援包含超過 5000 個物件的排除清單和受信任應用程式清單。

如何在卡巴斯基安全管理中心管理主控台中匯出和匯入受信任區域

1. 在卡巴斯基安全管理中心管理主控台樹狀目錄中，選取**政策**。

2. 選擇必要的政策並點擊以開啟政策內容。

3. 在政策視窗中，選擇 **補充 → 受信任區域** 然後點擊 **設定**。

4. 要匯出規則清單：

   a. 選擇**"掃描排除項目"**標籤。

   b. 如果您要匯出整個清單，請按一下 按鈕，然後選取 **匯出**。

   c. 如果您只要匯出清單的一部分，請依照下列步驟操作：

      1. 使用 **CTRL** 或 **SHIFT** 鍵選取您要匯出的清單項目。若要選取所有項目，請按 **CTRL+A**。

      2. 按一下 按鈕，然後選取 **匯出所選**。

   d. 在開啟的視窗中，指定要匯出至的 XML 檔案名稱，然後選取要儲存該檔案的資料夾。點擊**"儲存"**按鈕。

   Kaspersky Embedded Systems Security 會將規則清單匯出到 XML 檔案。

5. 要匯出受信任應用程式的清單：

   a. 選擇**"受信任應用程式"**標籤。

   b. 如果您要匯出整個清單，請按一下 按鈕，然後選取 **匯出**。

   c. 如果您只要匯出清單的一部分，請依照下列步驟操作：

      1. 使用 **CTRL** 或 **SHIFT** 鍵選取您要匯出的清單項目。若要選取所有項目，請按 **CTRL+A**。

      2. 按一下 按鈕，然後選取 **匯出所選**。

   d. 在開啟的視窗中，指定要匯出至的 XML 檔案名稱，然後選取要儲存該檔案的資料夾。點擊**"儲存"**按鈕。

   Kaspersky Embedded Systems Security 會將規則清單匯出到 XML 檔案。

6. 若要匯入排除項目清單：

   a. 選擇**"掃描排除項目"**標籤。

   這將開啟包含排除項目清單的視窗。

   b. 點擊資料夾圖示並從下拉式清單中選擇 **匯入**。

   c. 在開啟的視窗中，選取要從中匯入排除項目清單的 XML 檔案。

   d. 開啟檔案。

   如果電腦已經具有排除項目清單，則 Kaspersky Embedded Systems Security 將提示您刪除現有清單或從 XML 檔案向其中新增新項目。

7. 要匯入受信任應用程式的清單：

   a. 選擇**"受信任應用程式"**標籤。

   這將開啟包含受信任應用程式清單的視窗。

   b. 點擊**"匯入"**。

   c. 這將開啟一個視窗；在此視窗中，選取要從中匯入受信任應用程式清單的 XML 檔案。

d. 開啟檔案。

如果電腦已經具有受信任應用程式清單，則 Kaspersky Embedded Systems Security 將提示您刪除現有清單或從 XML 檔案向其中新增新項目。

8. 儲存變更。

如何在網頁主控台中匯出或匯入信任區域

1. 在網頁主控台的主視窗中，選擇**資產管理 → 政策**。
2. 點擊 Kaspersky Embedded Systems Security 政策的名稱。

政策內容視窗將開啟。

3. 選擇"**應用程式設定**"標籤。
4. 轉到**補充 → 受信任區域** 並點擊 **配置** 按鈕。
5. 要匯出規則清單：

a. 在**掃描排除項目和受信任應用程式**頁簽上，選擇要匯出的排除項目。

b. 點擊三個點然後選擇 **匯出**。

c. 確認您只想匯出選定的排除項目，或匯出整個排除項目清單。

Kaspersky Embedded Systems Security 會將規則清單匯出到 XML 檔案。

6. 要匯出受信任應用程式的清單：

a. 在**掃描排除項目和受信任應用程式**頁簽上，選擇要匯出的應用程式。

b. 點擊三個點然後選擇 **匯出**。

c. 確認您只想匯出選定的應用程式，還是匯出整個清單。

Kaspersky Embedded Systems Security 會將規則清單匯出到 XML 檔案。

7. 若要匯入排除項目清單：

a. 如果您想要從在應用程式版本 3.4 或更早版本中建立的 XML 檔案匯入排除項目清單，請在**掃描排除項目和受信任應用程式**頁簽上點擊**從先前的版本匯入**。

如果您要從在 4.0 或更高版本中建立的 XML 檔案匯入規則，請點擊**匯入**。

b. 如果電腦已經具有排除項目清單，則 Kaspersky Embedded Systems Security 將提示您刪除現有清單或從 XML 檔案向其中新增新項目。

c. 在開啟的視窗中，選取要從中匯入排除項目清單的 XML 檔案。

d. 單擊"**匯入**"。

8. 要匯入受信任應用程式的清單：

a. 如果您想要從在應用程式版本 3.4 或更早版本中建立的 XML 檔案匯入受信任應用程式清單，請在**掃描排除項目和受信任應用程式**頁簽上點擊**從先前的版本匯入**。

如果您要從在 4.0 或更高版本中建立的 XML 檔案匯入受信任應用程式，請點擊**匯入**。

b. 如果電腦已經具有受信任應用程式清單，則 Kaspersky Embedded Systems Security 將提示您刪除現有清單或從 XML 檔案向其中新增新項目。

c. 這將開啟一個視窗；在此視窗中，選取要從中匯入受信任應用程式清單的 XML 檔案。

d. 單擊**"匯入"**。

9. 儲存變更。

如何在應用程式主控台中匯出或匯入信任區域

1. 在應用程式主控台樹狀目錄中，選擇 **Kaspersky Embedded Systems Security** 節點然後從節點的上下文選單中選擇 **受信任區域**。

   開啟**"配置信任區域設定"**視窗。

2. 要匯出排除項目或者受信任應用程式的清單：

   a. 在 **排除項目** 部分，點擊**掃描排除項目** 或者 **受信任應用程式** 旁邊的 **設定** 按鈕。

   這將開啟包含掃描排除項目清單或受信任應用程式清單的視窗。

   b. 如果您要匯出整個清單，請按一下 按鈕，然後選取 **匯出**。

   c. 如果您只要匯出清單的一部分，請依照下列步驟操作：

      1. 使用 **CTRL** 或 **SHIFT** 鍵選取您要匯出的清單項目。若要選取所有項目，請按 **CTRL+A**。

      2. 按一下 按鈕，然後選取 **匯出所選**。

   d. 在開啟的視窗中，指定要匯出至的 XML 檔案名稱，然後選取要儲存該檔案的資料夾。點擊**"儲存"**按鈕。

   Kaspersky Embedded Systems Security 會將規則清單匯出到 XML 檔案。

3. 要匯入排除項目或者受信任應用程式的清單：

   a. 在 **排除項目** 部分，點擊**掃描排除項目** 或者 **受信任應用程式** 旁邊的 **設定** 按鈕。

   b. 選擇您要匯入的排除項目或者受信任應用程式。

   c. 點擊資料夾圖示並選取「**匯入**」。

   d. 這將開啟一個視窗；在此視窗中，選取要從中匯入排除項目或者受信任應用程式清單的 XML 檔案。

   e. 開啟檔案。

   如果電腦已經具有排除項目清單，則 Kaspersky Embedded Systems Security 將提示您刪除現有清單或從 XML 檔案向其中新增新項目。

4. 儲存變更。

使用受信任的系統憑證儲存

使用系統憑證儲存允許您從病毒掃描中排除由受信任數位簽章簽發的應用程式。Kaspersky Embedded Systems Security 會自動將此類應用程式分配給*受信任*群組。

如何在卡巴斯基安全管理中心管理主控台中設定受信任系統憑證儲存的使用

1. 在卡巴斯基安全管理中心管理主控台樹狀目錄中，選取**政策**。
2. 選擇必要的政策並點擊以開啟政策內容。
3. 在政策視窗中，選擇 **補充 → 受信任區域** 然後點擊 **設定**。
4. 選擇**"受信任的系統憑證儲存"**標籤。
5. 選擇 **使用受信任的系統憑證儲存** 核取方塊，然後在下拉式清單中選擇您希望 Kaspersky Embedded Systems Security 視為受信任的系統儲存。
6. 儲存變更。

如何在卡巴斯基安全管理中心網頁主控台中設定受信任系統憑證儲存的使用

1. 在網頁主控台的主視窗中，選擇**資產管理 → 政策**。
2. 點擊 Kaspersky Embedded Systems Security 政策的名稱。
   政策內容視窗將開啟。
3. 選擇**"應用程式設定"**標籤。
4. 轉到**補充 → 受信任區域** 並點擊 **配置** 按鈕。
5. 選擇**"受信任的系統憑證儲存"**標籤。
6. 選擇 **使用受信任的系統憑證儲存** 核取方塊，然後在下拉式清單中選擇您希望 Kaspersky Embedded Systems Security 視為受信任的系統儲存。
7. 儲存變更。

如何在應用程式主控台中設定受信任系統憑證儲存的使用

1. 在應用程式主控台樹狀目錄中，選擇 **Kaspersky Embedded Systems Security** 節點然後從節點的上下文選單中選擇 **受信任區域**。
   開啟**"配置信任區域設定"**視窗。
2. 在**受信任的系統憑證儲存**下面，選擇**使用受信任的系統憑證儲存**核取方塊，然後在下拉式清單中選擇您希望 Kaspersky Embedded Systems Security 視為受信任的系統儲存。
3. 儲存變更。

預先定義的掃描排除項目和受信任的應用程式

預先定義的掃描排除項目和受信任應用程式，可讓您快速將下列軟體的處理程序和檔案新增至信任區域：

- Microsoft Exchange 伺服器
- Microsoft SQL Server
- Microsoft Hyper-V

- Microsoft Windows Server 中的資料重複刪除處理程序
- Microsoft 系統中心配置管理器

您可以透過以下方式選擇預先定義的排除項目和受信任的應用程式：

- 安裝應用程式。
  - 使用精靈在本機安裝應用程式
  - 安裝套件內容
- 制定政策。
  - 新政策精靈
  - 政策內容：掃描排除項目和受信任的應用程式
  - 在命令列中。

即時檔案防護

Kaspersky Embedded Systems Security 的即時檔案防護元件在存取以下受防護裝置物件時，會對他們進行掃描：

- 檔案
- NTFS 交換資料串流。
- 本機磁碟和外部裝置上的主開機紀錄區和啟動磁區。
- Windows Server 2016 和 Windows Server 2019 容器檔案。

當任何應用程式將檔案寫入受防護裝置或在受防護裝置上讀取檔案時，Kaspersky Embedded Systems Security 會攔截此檔案進行掃描以偵測其是否存在威脅；如果偵測到威脅，則執行預設操作或您所指定的操作：嘗試解毒檔案、將其置於隔離或將其刪除。在清除或刪除前，Kaspersky Embedded Systems Security 會將原始檔案的加密副本儲存到備份資料夾。

Kaspersky Embedded Systems Security 可攔截在 Windows Server 2016 和 Windows Server 2019 容器中執行的檔案操作。

一個 *容器* 是一個隔離環境，可以讓應用程式在其中執行而無需直接與作業系統交互。如果容器位於元件防護範圍內，Kaspersky Embedded Systems Security 會掃描使用者正在存取的容器檔案是否有電腦威脅。當偵測到威脅時，應用程式會嘗試對容器進行解毒。如果解毒成功，容器將繼續工作。如果解毒失敗，則關閉容器。

Kaspersky Embedded Systems Security 還會偵測在 Windows Subsystem for Linux® 下執行的處理程序是否存在惡意軟體。對於此類別處理程序，即時檔案防護元件將套用目前配置定義的操作。

關於工作防護範圍和安全設定

預設情況下，即時檔案防護元件將防護裝置檔案系統中的所有物件。如果不需要對檔案系統中的所有物件進行安全防護，或者您想從工作範圍中排除任何物件，則可以限制防護範圍。

在應用程式主控台中，防護範圍以 Kaspersky Embedded Systems Security 可以監控的裝置檔案資源清單的形式顯示。

安全性設定

工作安全設定可以配置為防護範圍中包括的所有節點或項的一般設定，或配置為裝置檔案資源清單中各個節點或項的不同設定。

為所選父節點配置的安全設定將自動套用到其所有子節點。父節點的安全設定不會套用到單獨配置的子節點。

可以使用以下方法之一配置選定防護範圍的設定：

- 選取三個預定義安全等級中的一個。
- 為選定節點或檔案資源清單中的項目手動配置安全設定（安全等級變更為“**自訂**”）。

預定義的防護範圍

檔案資源清單顯示基於配置的 Microsoft Windows 安全設定所擁有讀取存取權限的節點。

Kaspersky Embedded Systems Security 覆寫以下預定義防護範圍：

- **本機硬碟磁碟機**Kaspersky Embedded Systems Security 將防護裝置硬碟磁碟機上的檔案。
- **卸除式磁碟機**Kaspersky Embedded Systems Security 將防護外部裝置上的檔案，如 CD 或卸除式磁碟機。您可以在防護範圍中包含或排除所有卸除式裝置、單個磁碟、資料夾或檔案。
- **網路**Kaspersky Embedded Systems Security 將防護裝置上執行的應用程式寫入到網路資料夾或從網路資料夾讀取的檔案。當其他受防護裝置上的應用程式存取此類檔案時，Kaspersky Embedded Systems Security 不會防護此類檔案。

預設情況下，您可以在範圍清單中檢視和配置預定義防護範圍；還可以在清單形成期間在設定防護範圍中向該清單新增預定義範圍。

已連線的網路磁碟也不會顯示在受防護裝置的檔案資源清單中。若要將網路磁碟中的物件包含在防護範圍內，請以 UNC (Universal Naming Convention) 格式指定與該網路磁碟對應的資料夾的路徑。

關於預定義安全等級

可以為受防護裝置檔案資源樹狀目錄或檔案資源清單中的選定節點套用以下預定義安全等級之一：**最大效能**, **建議防護**、**最大防護**和**通知**。這些等級均有各自的預定義安全設定集合（請參閱下表）。

最大效能

如果您的網路除了在受防護裝置和工作站上使用 Kaspersky Embedded Systems Security 外，還有其他受防護裝置安全措施，例如防火牆和現有安全政策，則建議使用**"最大效能"**安全等級。

建議防護

"建議防護"安全等級確保防護與對裝置的效能影響的最佳組合。Kaspersky 專家建議此等級，因為其足以防護大多數公司網路上的裝置。預設情況下，將設定**"建議防護"**安全等級。

最大防護

如果組織的網路有更高的裝置安全要求，則建議使用"**最大防護**"安全等級。

通知

如果公司網路中可能存在許多受感染的電腦並且封鎖它們可能會嚴重破壞組織的運營，則建議使用**通知**安全等級。

預設安全等級和相應的設定值

選項	安全等級			
	最大效能	建議防護	最大防護	通知
物件防護	按病毒資料庫中指定的副檔名清單掃描物件	按格式掃描物件	按格式掃描物件	按格式掃描物件
Scan only new and modified files	已啟用	已啟用	已停用	已啟用
Scan of compound files	已停用	掃描 Microsoft Office 格式的檔案	掃描 Microsoft Office 格式的檔案	掃描 Microsoft Office 格式的檔案
對感染物件和其他物件執行的操作	封鎖存取並解毒。若解毒失敗則移除	封鎖存取權限並執行卡巴斯基專家建議的動作	封鎖存取並解毒。若解毒失敗則移除	通知
將操作套用到所選的物件類型	已停用	已停用	已停用	已停用
在偵測到內嵌物件時完全刪除應用程式無法修改的複合檔案	已停用	已停用	已啟用	已停用
系統關鍵物件是作業系統和 Kaspersky Embedded Systems Security 操作所需的檔案。無法刪除這些檔案。無法終止與此類物件關聯的程序。				
Unpack in the background compound files larger than (MB)				
Stop scanning if it takes longer than (sec)	60 秒	60 秒	60 秒	60 秒
Do not scan compound objects larger than (MB)	8 MB	8 MB	未設定	8 MB
使用 iSwift 技術	已啟用	已啟用	已啟用	已啟用
使用 iChecker 技術	已啟用	已啟用	已啟用	已啟用

"即時檔案防護"元件預設掃描的檔案副檔名

預設情況下，Kaspersky Embedded Systems Security 將掃描具有以下副檔名的檔案：

- *386 ;*
- *acm ;*
- *ade、adp ;*

- *asp ;*
- *asx ;*
- *ax ;*
- *bas ;*
- *bat ;*
- *bin ;*
- *chm ;*
- *cla、clas*;*
- *cmd ;*
- *com ;*
- *cpl ;*
- *crt ;*
- *dll ;*
- *dpl ;*
- *drv ;*
- *dvb ;*
- *dwg ;*
- *efi ;*
- *emf ;*
- *eml ;*
- *.exe*
- *fon ;*
- *fpm ;*
- *hlp ;*
- *hta ;*
- *htm、html* ;*
- *htt ;*
- *ico ;*

- *inf ;*
- *ini ;*
- *ins ;*
- *isp ;*
- *jpg、jpe ;*
- *js、jse ;*
- *lnk ;*
- *mbx ;*
- *msc ;*
- *msg ;*
- *msi ;*
- *msp ;*
- *mst ;*
- *nws ;*
- *ocx ;*
- *oft ;*
- *otm ;*
- *pcd ;*
- *pdf ;*
- *php ;*
- *pht ;*
- *phtm* ;*
- *pif ;*
- *plg ;*
- *png ;*
- *pot ;*
- *prf ;*
- *prg ;*

- *reg ;*
- *rsc ;*
- *rtf ;*
- *scf ;*
- *scr ;*
- *sct ;*
- *shb ;*
- *shs ;*
- *sht ;*
- *shtm* ;*
- *swf ;*
- *sys ;*
- *the ;*
- *them* ;*
- *tsp ;*
- *url ;*
- *vb ;*
- *vbe ;*
- *vbs ;*
- *vxd ;*
- *wma ;*
- *wmf ;*
- *wmv ;*
- *wsc ;*
- *wsf ;*
- *wsh ;*
- *do? ;*
- *md? ;*

- *mp? ;*
- *ov? ;*
- *pp? ;*
- *vs? ;*
- *xl?。*

配置“即時檔案防護”元件

預設情況下，即時檔案防護元件使用下表敘述的設定。您可以變更這些設定值。

即時檔案防護元件預設設定

參數	預設值	描述
防護範圍	整個受防護裝置，虛擬磁碟機除外。	使用此選項變更防護範圍。
安全性設定	整個防護範圍的一般設定；對應“**建議防護**”安全等級。	您可以對受防護裝置檔案資源清單或樹狀目錄中選定的節點執行以下操作： • 選擇不同的預定義安全等級 • 手動變更安全性設定 您可以將選定節點的一組安全設定儲存為範本，以便在以後將其套用至其他節點。
物件防護模式	**智慧模式**	使用此選項選擇防護模式，即定義 Kaspersky Embedded Systems Security 掃描物件所採用的存取嘗試類型。
啟發式分析器	套用“**中**”安全等級。	可以啟用或停用“啟發式分析”並設定分析等級。
Block access to network shared resources for the sessions that show malicious activity	未套用。	使用此選項可封鎖目前的工作階段並在封鎖的主機儲存區段中新增偵測到惡意活動的主機 IP 或主機 LUID。
偵測到活動感染時啟動關鍵區域掃描	已套用。	在偵測到活動感染時，Kaspersky Embedded Systems Security 將建立並啟動“關鍵區域掃描”工作。
如果清除失敗則停止容器	已套用。	應用程式對於偵測到的物件可能沒有足夠的讀寫權限。在這種情況下，不可能對檢測到的物件進行解毒或刪除。如果選取此核取方塊，應用程式將封鎖偵測到的物件並停止容器。如果清除此核取方塊，應用程式將僅封鎖偵測到的物件。
不掃描在 Windows 容器中排除的檔案操作	已套用。	如果選取該核取方塊，則應用程式僅在容器啟動時掃描容器。如果清除該核取方塊，應用程式將即時連續掃描容器。

如何在卡巴斯基安全管理中心管理主控台中啟用檔案病毒掃描

1. 在卡巴斯基安全管理中心管理主控台樹狀目錄中，選取**政策**。
2. 選擇必要的政策並點擊以開啟政策內容。
3. 在政策屬性視窗中，選取“**即時電腦防護**”。
4. 在“**即時檔案防護設定**”區域中點擊“**設定**”。
5. 選擇“**即時檔案防護**”核取方塊。

6. 在 **物件防護模式** 區塊的 **一般** 頁簽上，選擇即時檔案防護操作模式：

   - **智慧模式**Kaspersky Embedded Systems Security 自行選擇掃描物件。物件在開啟時被掃描，如果物件進行了修改，則在儲存物件後重新掃描該物件。如果處理程序多次存取並修改物件，只有處理程序最後一次儲存物件後，Kaspersky Embedded Systems Security 才會重新掃描物件。

   - **在存取及修改時**Kaspersky Embedded Systems Security 在物件開啟時掃描該物件，如果物件進行了修改，則在物件儲存後重新掃描該物件。預設選中該選項。

   - **存取時**Kaspersky Embedded Systems Security 在物件開啟以進行讀取、執行或修改時掃描所有物件。

   - **當執行時**僅在存取檔案以執行該檔案時，Kaspersky Embedded Systems Security 才掃描該檔案。

7. 清除或選中"**使用啟發式分析**"核取方塊。

8. 選擇或清除"**Block access to network shared resources for the sessions that show malicious activity**"核取方塊。

9. 清除或選中"**Launch critical areas scan when active infection is detected**"核取方塊。

   如果選取該核取方塊，當偵測到活動感染時，Kaspersky Embedded Systems Security 會執行預先定義的*關鍵區域掃描*工作。預設將會選定該核取方塊。

10. 指定在 Windows 容器中執行的掃描檔案操作的設定。

11. 儲存變更。

如何在卡巴斯基安全管理中心網頁主控台中啟用檔案病毒掃描

1. 在網頁主控台的主視窗中，選擇**資產管理 → 政策**。

2. 點擊 Kaspersky Embedded Systems Security 政策的名稱。

   政策內容視窗將開啟。

3. 選擇"**應用程式設定**"標籤。

4. 轉到**即時電腦防護 → 即時檔案防護** 並點擊 **配置** 按鈕。

5. 選擇"**啟用即時檔案防護**"核取方塊。

6. 在 **物件防護模式** 區塊的 **一般** 頁簽上，選擇即時檔案防護操作模式：

   - **智慧模式**Kaspersky Embedded Systems Security 自行選擇掃描物件。物件在開啟時被掃描，如果物件進行了修改，則在儲存物件後重新掃描該物件。如果處理程序多次存取並修改物件，只有處理程序最後一次儲存物件後，Kaspersky Embedded Systems Security 才會重新掃描物件。

   - **在存取及修改時**Kaspersky Embedded Systems Security 在物件開啟時掃描該物件，如果物件進行了修改，則在物件儲存後重新掃描該物件。預設選中該選項。

   - **存取時**Kaspersky Embedded Systems Security 在物件開啟以進行讀取、執行或修改時掃描所有物件。

   - **當執行時**僅在存取檔案以執行該檔案時，Kaspersky Embedded Systems Security 才掃描該檔案。

7. 清除或選中"**使用啟發式分析**"核取方塊。

8. 選擇或清除"**封鎖存取顯示惡意活動的網路工作階段的網路共用資源**"核取方塊。

9. 清除或選中“**偵測到活動感染時啟動關鍵區域掃描**”核取方塊。

   如果選取該核取方塊，當偵測到活動感染時，Kaspersky Embedded Systems Security 會執行預先定義的*關鍵區域掃描*工作。預設將會選定該核取方塊。

10. 指定在 Windows 容器中執行的掃描檔案操作的設定。

11. 儲存變更。

如何在應用程式主控台中啟用檔案病毒掃描

1. 在 Kaspersky Embedded Systems Security 主控台樹狀目錄中，選擇“**即時電腦防護 → 即時檔案防護**”。

2. 在 **即時檔案防護** 節點的結果窗格中，點擊 **內容**。

   內容: 即時檔案防護視窗將開啟。

3. 選擇“**即時檔案防護**”核取方塊。

4. 在 **物件防護模式** 區塊的 **一般** 頁簽上，選擇即時檔案防護操作模式：

   - **智慧模式**Kaspersky Embedded Systems Security 自行選擇掃描物件。物件在開啟時被掃描，如果物件進行了修改，則在儲存物件後重新掃描該物件。如果處理程序多次存取並修改物件，只有處理程序最後一次儲存物件後，Kaspersky Embedded Systems Security 才會重新掃描物件。

   - **在存取及修改時**Kaspersky Embedded Systems Security 在物件開啟時掃描該物件，如果物件進行了修改，則在物件儲存後重新掃描該物件。預設選中該選項。

   - **存取時**Kaspersky Embedded Systems Security 在物件開啟以進行讀取、執行或修改時掃描所有物件。

   - **當執行時**僅在存取檔案以執行該檔案時，Kaspersky Embedded Systems Security 才掃描該檔案。

5. 清除或選中“**使用啟發式分析**”核取方塊。

6. 選擇或清除“**Block access to network shared resources for the sessions that show malicious activity**”核取方塊。

7. 清除或選中“**Launch critical areas scan when active infection is detected**”核取方塊。

   如果選取該核取方塊，當偵測到活動感染時，Kaspersky Embedded Systems Security 會執行預先定義的*關鍵區域掃描*工作。預設將會選定該核取方塊。

8. 指定在 Windows 容器中執行的掃描檔案操作的設定。

9. 儲存變更。

配置即時檔案防護元件的防護範圍

預設情況下，即時檔案防護元件對整個防護範圍使用通用安全設定。這些設定對應于“**建議防護**”預定義安全等級。

可以透過將安全設定配置為用於整個防護範圍的一般設定，或配置為裝置檔案資源清單中節點的單個項目的不同設定，來修改安全設定的預設值。

如果相同物件包含在多個防護範圍條目中，且這些條目具有不同的安全級別，則清單中的最後一條規則優先。例如，假設有一個包含兩個條目的防護範圍：**所有硬碟磁碟機**（**Inform**安全級別）和`*\Users\*\Downloads\*`（**Custom**安全級別）。應用程式會根據「通知」等級掃描硬碟，但`Downloads`資料夾除外。應用程式會按照手動指定的設定掃描`Downloads`資料夾，因為此設定條目是防護範圍清單中的最後一個。

如何在卡巴斯基安全管理中心管理主控台中設定即時檔案防護的防護範圍

1. 在卡巴斯基安全管理中心管理主控台樹狀目錄中，選取**政策**。
2. 選擇必要的政策並點擊以開啟政策內容。
3. 在政策屬性視窗中，選取**"即時電腦防護"**。
4. 在**"即時檔案防護"**區域中點擊**"設定"**。
5. 選擇**"防護範圍"**標籤。
6. 在受防護裝置的檔案資源清單中，選擇要為其設定預定義安全等級的項目。
7. 如果檔案共用不在清單中，請手動新增：
   a. 單擊**"新增"**。
   b. 使用資料夾樹指定所需物件的路徑，或在 **物件** 欄位中輸入路徑。
   如果必要的話，使用特殊字元輸入物件路徑遮罩：
   - `*`（星號）字元代表任意一組字元，但`\`和`/`字元除外（這兩個字元是檔案和資料夾路徑中的檔案和資料夾名稱的分隔符號）。例如，遮罩**"**`C:\*\*.txt`**"**將包括位於 C: 磁碟機但是不在子資料夾中所有帶 TXT 副檔名的檔案的路徑。
   - 兩個連續`*`字元在檔案或資料夾名稱中代表任意一組字元（包括空集），包括`\`和`/`字元（這兩個字元是檔案和資料夾路徑中的檔案和資料夾名稱的分隔符號）。例如，遮罩`C:\Folder\**\*.txt`將包括位於巢嵌在`Folder`內的資料夾（`Folder`自身除外）中所有帶 TXT 副檔名的檔案的路徑。遮罩必須包含至少一個嵌套等級。遮罩`C:\**\*.txt`不是有效遮罩。
   - `?`（問號）字元代表任意單個字元，但`\`和`/`字元除外（這兩個字元是檔案和資料夾路徑中的檔案和資料夾名稱的分隔符號）。例如，遮罩`C:\Folder\???.txt`將包括位於`Folder`資料夾中所有帶 TXT 副檔名且名稱由三個字元構成的檔案的路徑。

   電腦檔案資源清單中的**此 PC**物件包含以下物件：**所有硬碟磁碟機**、**所有網路磁碟機**及**所有卸除式磁碟機**。
   c. 單擊**"確定"**。
8. 確保選定的檔案資源包含在防護範圍中。
9. 透過點擊**配置**，為選定的防護範圍指定一個 預定義的安全等級。預設情況下，相同的安全設定會套用於整個防護範圍。這些設定對應于**"建議防護"**預定義安全等級。您還可以 編輯預設安全設定。
10. 儲存變更。

如何在卡巴斯基安全管理中心網頁主控台中設定即時檔案防護的防護範圍

1. 在網頁主控台的主視窗中，選擇**資產管理 → 政策**。
2. 點擊 Kaspersky Embedded Systems Security 政策的名稱。
   政策內容視窗將開啟。
3. 選擇"**應用程式設定**"標籤。
4. 轉到**即時電腦防護 → 即時檔案防護** 並點擊 **配置** 按鈕。
5. 選擇"**防護範圍**"標籤。
6. 在受防護裝置的檔案資源清單中，選擇要為其設定預定義安全等級的項目。
7. 如果檔案共用不在清單中，請手動新增：
   a. 單擊"**新增**"。
   b. 在"**物件類型**"清單中，選取一個選項：
      對於 **遮罩** 選項，使用特殊字元輸入物件路徑遮罩：
      - `*`（星號）字元代表任意一組字元，但 `\` 和 `/` 字元除外（這兩個字元是檔案和資料夾路徑中的檔案和資料夾名稱的分隔符號）。例如，遮罩"`C:\*\*.txt`"將包括位於 C: 磁碟機但是不在子資料夾中所有帶 TXT 副檔名的檔案的路徑。
      - 兩個連續 `*` 字元在檔案或資料夾名稱中代表任意一組字元（包括空集），包括 `\` 和 `/` 字元（這兩個字元是檔案和資料夾路徑中的檔案和資料夾名稱的分隔符號）。例如，遮罩 `C:\Folder\**\*.txt` 將包括位於巢嵌在 `Folder` 內的資料夾（`Folder`自身除外）中所有帶 TXT 副檔名的檔案的路徑。遮罩必須包含至少一個嵌套等級。遮罩 `C:\**\*.txt` 不是有效遮罩。
      - `?`（問號）字元代表任意單個字元，但 `\` 和 `/` 字元除外（這兩個字元是檔案和資料夾路徑中的檔案和資料夾名稱的分隔符號）。例如，遮罩 `C:\Folder\???.txt` 將包括位於 `Folder` 資料夾中所有帶 TXT 副檔名且名稱由三個字元構成的檔案的路徑。

      電腦檔案資源清單中的**此 PC**物件包含以下物件：**所有硬碟磁碟機**、**所有網路磁碟機**及**所有卸除式磁碟機**。
   c. 單擊"**確定**"。
8. 使用清單項目旁的切換開關確保選定的檔案資源包含在防護範圍中。
9. 透過點擊**編輯**，為選定的防護範圍指定一個 預定義的安全等級。預設情況下，相同的安全設定會套用於整個防護範圍。這些設定對應于"**建議防護**"預定義安全等級。您還可以 編輯預設安全設定。
10. 儲存變更。

如何在應用程式主控台中設定即時檔案防護的防護範圍

1. 在 Kaspersky Embedded Systems Security 主控台樹狀目錄中，選擇"**即時電腦防護 → 即時檔案防護**"。
2. 在 **即時檔案防護** 節點的結果窗格中，點擊 **配置防護範圍**。
   內容: 即時檔案防護視窗將開啟。
3. 在受防護裝置的檔案資源清單中，選擇要為其設定預定義安全等級的項目。

4. 如果檔案共用不在清單中，請手動新增：

   a. 單擊**"新增"**。

   b. 使用資料夾樹指定所需物件的路徑，或在 **物件** 欄位中輸入路徑。

   如果必要的話，使用特殊字元輸入物件路徑遮罩：

   - `*`（星號）字元代表任意一組字元，但 `\` 和 `/` 字元除外（這兩個字元是檔案和資料夾路徑中的檔案和資料夾名稱的分隔符號）。例如，遮罩"`C:\*\*.txt`"將包括位於 C: 磁碟機但是不在子資料夾中所有帶 TXT 副檔名的檔案的路徑。

   - 兩個連續 `*` 字元在檔案或資料夾名稱中代表任意一組字元（包括空集），包括 `\` 和 `/` 字元（這兩個字元是檔案和資料夾路徑中的檔案和資料夾名稱的分隔符號）。例如，遮罩 `C:\Folder\**\*.txt` 將包括位於巢嵌在 `Folder` 內的資料夾（`Folder`自身除外）中所有帶 TXT 副檔名的檔案的路徑。遮罩必須包含至少一個嵌套等級。遮罩 `C:\**\*.txt` 不是有效遮罩。

   - `?`（問號）字元代表任意單個字元，但 `\` 和 `/` 字元除外（這兩個字元是檔案和資料夾路徑中的檔案和資料夾名稱的分隔符號）。例如，遮罩 `C:\Folder\???.txt` 將包括位於 `Folder` 資料夾中所有帶 TXT 副檔名且名稱由三個字元構成的檔案的路徑。

   電腦檔案資源清單中的**此 PC**物件包含以下物件：**所有硬碟磁碟機**、**所有網路磁碟機**及**所有卸除式磁碟機**。

   c. 單擊**"確定"**。

5. 確保選定的檔案資源包含在防護範圍中。

6. 透過點擊**配置**，為選定的防護範圍指定一個 預定義的安全等級。預設情況下，相同的安全設定會套用於整個防護範圍。這些設定對應于**"建議防護"**預定義安全等級。您還可以 編輯預設安全設定。

7. 儲存變更。

手動配置安全性設定

預設情況下，即時電腦防護工作對整個防護範圍使用通用安全設定。這些設定對應于**"建議防護"**預定義安全等級。

可以透過將安全設定配置為用於整個防護範圍的一般設定，或配置為裝置檔案資源清單或樹狀目錄中節點的單個項目的不同設定，來修改安全設定的預設值。

在使用受防護裝置檔案資源樹狀目錄時，為所選父節點配置的安全設定將自動套用於所有子節點。父節點的安全設定不會套用到單獨配置的子節點。

如何在卡巴斯基安全管理中心管理主控台中手動配置安全設定

1. 在卡巴斯基安全管理中心管理主控台樹狀目錄中，選取**政策**。

2. 選擇必要的政策並點擊以開啟政策內容。

3. 在政策屬性視窗中，選取**"即時電腦防護"**。

4. 在**"即時檔案防護"**區域中點擊**"設定"**。

5. 在 **即時檔案防護** 視窗中，轉到 **防護範圍** 頁簽。

6. 選擇要配置其安全設定的資源。

7. 單擊“**配置**”。

8. 在開啟的視窗中，選擇所需安全等級並按一下**設定**。

9. 在**一般**頁籤上，配置以下設定：

   - 應包括在防護範圍中的物件：

     - **所有物件**Kaspersky Embedded Systems Security 掃描所有物件。

     - **按格式掃描的物件**Kaspersky Embedded Systems Security 僅根據檔案格式掃描感染物件。Kaspersky 編制了該格式清單。它包含在 Kaspersky Embedded Systems Security 資料庫中。

     - **按病毒資料庫中指定的副檔名清單掃描的物件**Kaspersky Embedded Systems Security 僅根據檔案副檔名掃描感染的物件。Kaspersky 編制了該副檔名清單。它包含在 Kaspersky Embedded Systems Security 資料庫中。

     - **依照指定延伸程式清單掃描的物件**Kaspersky Embedded Systems Security 僅根據檔案副檔名掃描感染的物件。副檔名清單由使用者手動指定。

   - 在“**最佳化**“區塊中，選擇或者清除“**Scan only new and modified files**”核取方塊。

   - 在“**掃描複合檔案**”部分中，指定要包含在掃描範圍內的複合物件：

     - **掃描壓縮檔案**

     - **掃描分發套件**

     - **掃描 Microsoft Office 格式的檔案**

     - **掃描電子郵件格式檔案**

10. 在**操作**頁籤上，配置以下設定：

    - 選擇要對受感染的物件和其他偵測到的物件執行的操作：

      - **通知**

      - **封鎖**

      - **執行其他操作**
        從下拉清單中選擇操作：

        - **清除**

        - **Disinfect. Delete if disinfection fails**

        - **刪除**

        - **建議**

- 選擇依威脅類型對物件執行的操作：

  a. 清除或選中**"將操作套用到所選的物件類型"**核取方塊。

  b. 點擊 **設定** 並選擇要偵測的物件類型。

- 配置對不可修改的複合檔案的操作：清除或選擇 **在偵測到內嵌物件時完全刪除應用程式無法修改的複合檔案** 核取方塊。

11. 在**最佳化**頁籤上，配置以下設定：

    - **Unpack in the background compound files larger than (MB)**
    - **如果超過以下時間（秒）則停止掃描**
    - **如果複合物件大於 (MB) 則不掃描**
    - **使用 iSwift 技術**
    - **使用 iChecker 技術**

12. 儲存新的安全設定。

如何在卡巴斯基安全管理中心網頁主控台中手動配置安全設定

1. 在網頁主控台的主視窗中，選擇**資產管理 → 政策**。
2. 點擊 Kaspersky Embedded Systems Security 政策的名稱。
   政策內容視窗將開啟。
3. 選擇**"應用程式設定"**標籤。
4. 轉到**即時電腦防護 → 即時檔案防護** 並點擊 **配置** 按鈕。
5. 選擇**"防護範圍"**標籤。
6. 執行以下操作之一：

   - 點擊**新增** 按鈕新增規則並為其指定安全設定。
   - 選擇一個現有規則，然後點擊**"編輯"**按鈕。

   開啟**"編輯範圍"**視窗。
7. 將切換開關設定為 **作用中**。
8. 選擇一個 安全等級 並根據需要指定安全設定。

9. 在“**物件防護模式**”部分中，指定要包含在掃描範圍內的複合物件：

   - 應包括在防護範圍中的物件：

     - **所有物件**Kaspersky Embedded Systems Security 掃描所有物件。
     - **按格式掃描的物件**Kaspersky Embedded Systems Security 僅根據檔案格式掃描感染物件。Kaspersky 編制了該格式清單。它包含在 Kaspersky Embedded Systems Security 資料庫中。
     - **按病毒資料庫中指定的副檔名清單掃描的物件**Kaspersky Embedded Systems Security 僅根據檔案副檔名掃描感染的物件。Kaspersky 編制了該副檔名清單。它包含在 Kaspersky Embedded Systems Security 資料庫中。
     - **依照指定延伸程式清單掃描的物件**Kaspersky Embedded Systems Security 僅根據檔案副檔名掃描感染的物件。副檔名清單由使用者手動指定。

10. 在“**最佳化**”部分，選擇或者清除“**只防護新增及修改的檔案**”核取方塊。

11. 在“**復合物件防護**”部分中，指定要包含在掃描範圍內的複合物件：

    - **掃描壓縮檔案**
    - **掃描分發套件**
    - **掃描 Microsoft Office 格式的檔案**
    - **掃描電子郵件格式檔案**

12. 選擇要對受感染的物件和其他偵測到的物件執行的操作：

    - **通知**
    - **封鎖**
    - **執行其他操作**

      從下拉清單中選擇操作：

      - **清除**
      - **解毒；若解毒失敗則刪除**
      - **刪除**
      - **建議**

13. 選擇依威脅類型對物件執行的操作：

    a. 清除或選中“**將操作套用到所選的物件類型**”核取方塊。

    b. 如果選取該核取方塊，請點擊**設定** 並選擇要偵測的物件類型。

14. 配置對不可修改的複合檔案的操作：清除或選擇 **在偵測到內嵌物件時完全刪除應用程式無法修改的複合檔案** 核取方塊。

15. 在“**最佳化**”部分中，配置以下設定：

- **在背景解壓縮複合檔案**
- **如果超過以下時間（秒）則停止掃描**
- **如果複合物件大於 (MB) 則不掃描**
- **使用 iSwift 技術**
- **使用 iChecker 技術**

16. 儲存新的安全設定。

如何在應用程式主控台中配置安全性設定

1. 在 Kaspersky Embedded Systems Security 主控台樹狀目錄中，選擇“**即時電腦防護 → 即時檔案防護**”。
2. 在 **即時檔案防護** 節點的結果窗格中，點擊 **配置防護範圍**。
   內容: 即時檔案防護視窗將開啟。
3. 選擇要配置其安全設定的資源。
4. 單擊“**配置**”。
5. 在開啟的視窗中，選擇所需安全等級並按一下**設定**。
6. 在**一般**頁籤上，配置以下設定：
   - 應包括在防護範圍中的物件：
     - **所有物件**Kaspersky Embedded Systems Security 掃描所有物件。
     - **按格式掃描的物件**Kaspersky Embedded Systems Security 僅根據檔案格式掃描感染物件。Kaspersky 編制了該格式清單。它包含在 Kaspersky Embedded Systems Security 資料庫中。
     - **按病毒資料庫中指定的副檔名清單掃描的物件**Kaspersky Embedded Systems Security 僅根據檔案副檔名掃描感染的物件。Kaspersky 編制了該副檔名清單。它包含在 Kaspersky Embedded Systems Security 資料庫中。
     - **依照指定延伸程式清單掃描的物件**Kaspersky Embedded Systems Security 僅根據檔案副檔名掃描感染的物件。副檔名清單由使用者手動指定。
   - 在“**最佳化**“區塊中，選擇或者清除“**只防護新增及修改的檔案**”核取方塊。
   - 在“**掃描複合檔案**”部分中，指定要包含在掃描範圍內的複合物件：
     - **掃描壓縮檔案**掃描 ZIP、GZIP、BZIP、RAR、TAR、ARJ、CAB、LHA、JAR、ICE 和其它存檔。應用程式不僅依照副檔名而且依照格式掃描存檔。當檢查封存時，應用程式會執行巡迴解壓縮。這可讓人偵測多層封存（封存內的封存）內的威脅。
     - **掃描分發套件**該核取方塊用於啟用/停用對協力廠商分發套件的掃描。

- **掃描 Microsoft Office 格式的檔案**掃描 Microsoft Office 檔案（DOC、DOCX、XLS、PPT 和其他 Microsoft 副檔名）。Office 格式檔案也包含 OLE 物件。Kaspersky Embedded Systems Security 掃描小於 1 MB 的 office 格式檔案，無論該核取方塊是否被選中。

- **掃描電子郵件格式檔案**

7. 在**操作**頁籤上，配置以下設定：

- 選擇要對受感染的物件和其他偵測到的物件執行的操作：

  - **通知**

  - **封鎖**

  - **執行其他操作**

    從下拉清單中選擇操作：

    - **清除**

    - **Disinfect. Delete if disinfection fails**

    - **刪除**

    - **建議**

- 選擇依威脅類型對物件執行的操作：

  a. 清除或選中"**將操作套用到所選的物件類型**"核取方塊。

  b. 點擊 **設定** 並選擇要偵測的物件類型。

- 配置對不可修改的複合檔案的操作：清除或選擇 **在偵測到內嵌物件時完全刪除應用程式無法修改的複合檔案** 核取方塊。

8. 在**最佳化**頁籤上，配置以下設定：

- **Unpack in the background compound files larger than (MB)**

- **如果超過以下時間（秒）則停止掃描**

- **如果複合物件大於 (MB) 則不掃描**

- **使用 iSwift 技術**

- **使用 iChecker 技術**

9. 儲存新的安全設定。

容器掃描

一個 *容器* 是一個隔離環境，應用程式可以在其中執行而無需直接與作業系統交互。使用容器涉及以下風險：

- 駭客可能能夠利用容器化弱點來損害容器內的應用程式。
- 駭客可能會利用容器環境的不安全配置來獲得對電腦上資料未經授權的存取或損害系統的完整性。
- 對容器的成功攻擊可以讓駭客獲得對電腦上資料的存取權限。
- 駭客可能會利用網路弱點來攔截網路流量。

也就是說，Kaspersky Embedded Systems Security 是用於偵測容器內惡意活動的外部工具。這可以維持容器的效能並防止與容器內的其他應用程式發生衝突。不支援在容器內安裝 Kaspersky Embedded Systems Security。

除了提供容器安全性之外，Kaspersky Embedded Systems Security 還允許使用應用程式啟動控制元件管理容器內的應用程式。為容器配置應用程式啟動控制元件的方式與為電腦上安裝的應用程式配置的方式相同。系統完整性監控元件也支援容器。

容器要求

- 容器必須是 Docker 容器。其他容器化工具不受支援。
- 容器必須在處理程序隔離模式下執行。Hyper-V 隔離模式不受支援。
- 容器必須放置在 Windows Server 2016、2019 或 2022 伺服器（Docker Host）上。
- 容器必須包含 Windows 映像（Docker Image）。不支援 Windows 10 和 11。不支援 Linux 映像。
- 不支援掃描在 WSL2 – Windows Subsystem for Linux v2（Docker Wine）模式中執行的容器。

偵測到威脅後的動作

如果在容器內偵測到威脅，應用程式將套用 為即時檔案防護元件所選擇的操作。容器掃描有其他設定（請參閱下面的說明）。如果偵測到威脅，應用程式會封鎖惡意活動並執行選定的操作（例如，嘗試解毒物件）。如果 Kaspersky Embedded Systems Security 無法清除偵測到的物件，則可以停止容器。預設情況下啟用容器停止。

如何在卡巴斯基安全管理中心管理主控台中設定容器掃描

1. 在卡巴斯基安全管理中心管理主控台樹狀目錄中，選取**政策**。
2. 選擇必要的政策並點擊以開啟政策內容。
3. 在政策屬性視窗中，選取**"即時電腦防護"**。
4. 在**"即時檔案防護"**區域中點擊**"設定"**。

5. 在“**掃描在 Windows 容器中排除的檔案操作**“塊中，配置容器掃描設定：

   - **如果清除失敗則停止容器**應用程式對於偵測到的物件可能沒有足夠的讀寫權限。在這種情況下，不可能對檢測到的物件進行解毒或刪除。如果選取此核取方塊，應用程式將封鎖偵測到的物件並停止容器。如果清除此核取方塊，應用程式將僅封鎖偵測到的物件。

   - **不掃描在 Windows 容器中排除的檔案操作**如果選取該核取方塊，則應用程式僅在容器啟動時掃描容器。如果清除該核取方塊，應用程式將即時連續掃描容器。

6. 儲存新的安全設定。

如何在卡巴斯基安全管理中心網頁主控台中設定容器掃描

1. 在網頁主控台的主視窗中，選擇**資產管理 → 政策**。

2. 點擊 Kaspersky Embedded Systems Security 政策的名稱。

   政策內容視窗將開啟。

3. 選擇“**應用程式設定**”標籤。

4. 轉到**即時電腦防護 → 即時檔案防護** 並點擊 **配置** 按鈕。

5. 在“**掃描在 Windows 容器中排除的檔案操作**“塊中，配置容器掃描設定：

   - **如果清除失敗則停止容器**應用程式對於偵測到的物件可能沒有足夠的讀寫權限。在這種情況下，不可能對檢測到的物件進行解毒或刪除。如果選取此核取方塊，應用程式將封鎖偵測到的物件並停止容器。如果清除此核取方塊，應用程式將僅封鎖偵測到的物件。

   - **不掃描在 Windows 容器中排除的檔案操作**如果選取該核取方塊，則應用程式僅在容器啟動時掃描容器。如果清除該核取方塊，應用程式將即時連續掃描容器。

6. 儲存新的安全設定。

如何在應用程式主控台中設定容器掃描

1. 在 Kaspersky Embedded Systems Security 主控台樹狀目錄中，選擇“**即時電腦防護 → 即時檔案防護**”。

2. 在 **即時檔案防護** 節點的結果窗格中，點擊 **內容**。

   內容: 即時檔案防護視窗將開啟。

3. 在“**掃描在 Windows 容器中排除的檔案操作**“塊中，配置容器掃描設定：

   - **如果清除失敗則停止容器**應用程式對於偵測到的物件可能沒有足夠的讀寫權限。在這種情況下，不可能對檢測到的物件進行解毒或刪除。如果選取此核取方塊，應用程式將封鎖偵測到的物件並停止容器。如果清除此核取方塊，應用程式將僅封鎖偵測到的物件。

   - **不掃描在 Windows 容器中排除的檔案操作**如果選取該核取方塊，則應用程式僅在容器啟動時掃描容器。如果清除該核取方塊，應用程式將即時連續掃描容器。

4. 儲存變更。

KSN 使用

為了更有效地防護您的電腦，Kaspersky Embedded Systems Security 使用從全球使用者處接收的資料。卡巴斯基安全網路旨在獲取此資料。

KSN 功能可能無法在美國的應用程式中使用。

*卡巴斯基安全網路（KSN）*是雲端服務的基礎結構，可提供對線上卡巴斯基知識庫的存取，該知識庫包含有關檔案、網頁資源和軟體信譽的資訊。使用卡巴斯基安全網路的資料可確保 Kaspersky Embedded Systems Security 能夠更快地對新型威脅作出回應，提高一些防護元件的效能，並減少誤報風險。如果您正在參與卡巴斯基安全網路，KSN 服務將為 Kaspersky Embedded Systems Security 提供有關所掃描網址的信譽的資訊，以及有關所掃描檔案的類別和信譽的資訊。有關 KSN 存取權限配置的詳細資訊，請參閱卡巴斯基安全管理中心說明。

卡巴斯基安全網路的使用是自願的。應用程式將在初始化設定期間提示您使用 KSN。使用者可以隨時開始或停止加入 KSN。

有關在參與 KSN 期間產生的 Kaspersky 統計資訊的傳送詳情，以及有關此類資訊的儲存和銷毀，請參閱卡巴斯基安全網路聲明和 Kaspersky 網站。含有卡巴斯基安全網路聲明文字的 ksn_<語言 ID>.txt 檔案包括在應用程式分發套件中。

卡巴斯基信譽資料庫的基礎結構

Kaspersky Embedded Systems Security 支援以下用於使用 Kaspersky 信譽資料庫的基礎結構解決方案：

- *卡巴斯基安全網路 (KSN)* 是大多數 Kaspersky 應用程式使用的解決方案。KSN 參與者從卡巴斯基接收資訊，並向 Kaspersky 傳送使用者電腦上偵測到的物件的資訊，以便 Kaspersky 分析人員進行額外分析，並包括在信譽和統計資料庫中。
- *卡巴斯基安全網路 (KSN)* 是讓承載 Kaspersky Embedded Systems Security 或其他 Kaspersky 應用程式的電腦的使用者獲得卡巴斯基信譽資料庫以及其他統計資料的存取權限的解決方案，無需從他們自己的電腦向卡巴斯基傳送資料。KPSN 專為因以下任一原因無法參與卡巴斯基安全網路的公司客戶所設計：
  - 本機工作站未連線網際網路。
  - 法律禁止或公司安全政策限制將任何資料傳輸到國家/地區外部或公司 LAN 外部。

啟用卡巴斯基安全網路

如何在卡巴斯基安全管理中心管理主控台中啟用卡巴斯基安全網路

1. 在卡巴斯基安全網路管理主控台樹狀目錄中，選擇 **政策** 資料夾。
2. 選擇必要的 Kaspersky Embedded Systems Security 的政策然後按兩下開啟政策內容。
3. 這將開啟一個視窗；在該視窗的相關部分的清單中，選擇 **即時電腦防護 → KSN 使用**。

4. 單擊**"設定"**。

5. 選擇**"卡巴斯基安全網路"**核取方塊來啟用元件。

   如果啟用了使用 KSN，Kaspersky Embedded Systems Security 將顯示卡巴斯基安全網路聲明。如果同意，請接受《卡巴斯基安全網路(KSN)聲明》的使用條款。

   預設情況下，Kaspersky Embedded Systems Security 使用卡巴斯基安全網路的延伸模式。卡巴斯基安全網路延伸模式是 Kaspersky Embedded Systems Security 向 Kaspersky 傳送附加資料的一種模式。

6. 如有必要，清除**"啟用延伸 KSN 模式"**核取方塊。

7. 儲存變更。

如果啟用了卡巴斯基安全網路，則 Kaspersky Embedded Systems Security 會使用有關從卡巴斯基安全網路收到的檔案、網頁資源和應用程式信譽的資訊。

如何在 Kaspersky Embedded Systems Security 主控台中啟用卡巴斯基安全網路

1. 在應用程式主控台樹狀目錄中，展開**"即時電腦防護"**節點。

2. 選擇**"卡巴斯基安全網路"**子節點。

3. 在應用程式主視窗中，點擊**內容**。

4. 選擇**"卡巴斯基安全網路"**核取方塊來啟用元件。

   如果啟用了使用 KSN，Kaspersky Embedded Systems Security 將顯示卡巴斯基安全網路聲明。如果同意，請接受《卡巴斯基安全網路(KSN)聲明》的使用條款。

   預設情況下，Kaspersky Embedded Systems Security 使用卡巴斯基安全網路的延伸模式。卡巴斯基安全網路延伸模式是 Kaspersky Embedded Systems Security 向 Kaspersky 傳送附加資料的一種模式。

5. 如有必要，清除**"啟用延伸 KSN 模式"**核取方塊。

6. 儲存變更。

如果啟用了卡巴斯基安全網路，則 Kaspersky Embedded Systems Security 會使用有關從卡巴斯基安全網路收到的檔案、網頁資源和應用程式信譽的資訊。

如何在卡巴斯基安全管理中心網頁主控台中啟用卡巴斯基安全網路

1. 在網頁主控台的主視窗中，選擇**資產管理 → 政策**。

2. 點擊 Kaspersky Embedded Systems Security 政策的名稱。

   政策內容視窗將開啟。

3. 選擇**"應用程式設定"**標籤。

4. 轉到**即時電腦防護 → KSN 使用**部分並點擊**配置**按鈕。

5. 在顯示的視窗中，選擇 **啟用卡巴斯基安全網路** 核取方塊以啟用該元件。

   如果啟用了使用 KSN，Kaspersky Embedded Systems Security 將顯示卡巴斯基安全網路聲明。如果您同意，請接受卡巴斯基安全網路使用條款。

   預設情況下，Kaspersky Embedded Systems Security 使用卡巴斯基安全網路的延伸模式。卡巴斯基安全網路延伸模式是 Kaspersky Embedded Systems Security 向 Kaspersky 傳送附加資料的一種模式。

6. 如有必要，清除“**啟用延伸 KSN 模式**”核取方塊。

7. 儲存變更。

結果，如果啟用了卡巴斯基安全網路，則 Kaspersky Embedded Systems Security 會使用有關從卡巴斯基安全網路收到的檔案、網頁資源和應用程式信譽的資訊。

卡巴斯基安全網路使用統計資料

當「*KSN 使用*」工作執行時，您可以檢視有關 Kaspersky Embedded Systems Security 自工作啟動到目前處理之物件數量的即時資訊。

要檢視「KSN 使用」統計資料：

1. 在應用程式主控台樹狀目錄中，選取「**即時電腦防護**」區域。

2. 選擇“**卡巴斯基安全網路**”子節點。

結果窗格的「**統計資料**」區域會顯示工作統計資料（請參閱下表）。

KSN 統計資料

欄位	描述
檔案請求已傳送	Kaspersky Embedded Systems Security 傳送給 KSN 的物件信譽查詢數量。
檔案在 KSN 中不受信任	KSN 分配的信譽不受信任的物件數量。
請求傳送錯誤	處理時出現錯誤的 KSN 請求數量。
形成的統計資料	傳送到 KSN 的產生的統計封包數量。
物件被移除	被 Kaspersky Embedded Systems Security 成功刪除的物件數量。
未移除的物件	Kaspersky Embedded Systems Security 嘗試刪除但無法刪除（例如，由於其他應用程式封鎖存取物件）的物件數。
移動到備份	Kaspersky Embedded Systems Security 成功複製到備份的物件數量。
物件未移至備份區	Kaspersky Embedded Systems Security 無法複製到備份（例如，由於磁碟空間不足）的物件數量。程式不會解毒或刪除無法移動到備份中的檔案。
受限模式	該狀態表示應用程式是否在受限制模式下傳送檔案信譽請求。根據卡巴斯基專家的建議，在受限制模式下，Kaspersky Embedded Systems Security 僅傳送檔案信譽要求的一部分。

「**物件被移除**」、「**未移除的物件**」、「**移動到備份**」、「**物件未移至備份區**」欄位的值是根據即時檔案防護元件的統計資料產生。

卡巴斯基私有安全網路的限制

卡巴斯基安全網路 (KSN) 是讓承載 Kaspersky Embedded Systems Security 或其他 Kaspersky 應用程式的電腦的使用者獲得卡巴斯基信譽資料庫以及其他統計資料的存取權限的解決方案，無需從他們自己的電腦向卡巴斯基傳送資料。卡巴斯基私有安全網路使您可以使用自己的本機信譽資料庫來檢查物件（檔案或網址）的信譽。與新增到 KSN / KPSN 中的物件相比，新增到本機信譽資料庫中的物件的信譽具有更高的優先級。例如，假設 Kaspersky EEmbedded Systems Security 正在掃描電腦並請求 KSN / KPSN中 檔案的信譽。如果檔案在本機信譽資料庫中具有“*不信任群組*”的信譽，但在 KSN / KPSN 中具有“*受信任群組*”的信譽，則 Kaspersky Embedded Systems Security 會將檔案偵測為“*不信任群組*”，並將採取針對偵測到的威脅而定義的操作。

但是，在某些情況下，Kaspersky Embedded Systems Security 可能不會請求 KSN / KPSN 中物件的信譽。在這種情況下，Kaspersky Embedded Systems Security 將不會從 KPSN 的本機信譽資料庫接收資料。由於以下原因，Kaspersky Embedded Systems Security 可能不會請求 KSN / KPSN 中物件的信譽：

- 卡巴斯基應用程式正在使用離線信譽資料庫。離線信譽資料庫旨在在卡巴斯基應用程式運行期間最佳化資源，並防護電腦上的重要物件。離線信譽資料庫由卡巴斯基專家根據卡巴斯基安全網路中的資料建立。卡巴斯基應用程式使用特定應用程式的病毒資料庫更新離線信譽資料庫。如果離線信譽資料庫包含有關被掃描物件的資訊，則應用程式不會從 KSN / KPSN 請求該物件的信譽。
- 在應用程式設定中配置掃描排除項目（受信任區域）。在這種情況下，應用程式不會考慮本機信譽資料庫中物件的信譽。
- 該應用程式使用掃描最佳化技術（例如 iSwift 或 iChecker），或者正在將信譽請求快取到 KSN/KPSN。在這種情況下，應用程式不可請求先前掃描的物件的信譽。
- 為了最佳化其工作量，應用程式掃描特定格式和大小的檔案。有關格式和大小限制的清單由卡巴斯基專家確定。此清單已使用應用程式的病毒資料庫更新。

KSN 代理設定

受卡巴斯基安全管理中心管理伺服器管理的使用者電腦可以透過 KSN 代理服務與 KSN 互動。

KSN 代理服務提供以下功能：

- 使用者的電腦可以查詢的 KSN 和將資訊送交 KSN，即使沒有直接連線網際網路。
- KSN 代理服務暫存處理過的資料，從而減少外部網路通訊信道上的負荷，並加快使用者接收資料的速度。

預設情況下，在 KSN 被啟用和 KSN 聲明被接受後，應用程式將使用代理伺服器連線到卡巴斯基安全網路。應用程式使用的代理伺服器是透過 TCP 連接埠 13111 的卡巴斯基安全管理中心管理伺服器。因此，如果 KSN 代理不可用，您必須 檢查裝置作為 KSN 代理伺服器的運作情況。您必須檢查以下內容：

- *Ksnproxy* 服務正在管理伺服器上執行。
- 電腦上的防火墻沒有封鎖連接埠 13111。

您可以如下配置KSN 代理：啟用或停用 KSN 代理，然後配置用於連線的連接埠。為此，您需要開啟管理伺服器內容。有關 KSN 代理配置的詳細資訊，請參閱卡巴斯基安全管理中心說明。您也可以在 Kaspersky Embedded Systems Security 政策中為單台電腦啟用或停用 KSN 代理。

如何在卡巴斯基安全管理中心管理主控台中啟用 KSN 代理

1. 在卡巴斯基安全管理中心管理主控台樹狀目錄中，選取**政策**。
2. 選擇必要的 Kaspersky Embedded Systems Security 的政策然後按兩下開啟政策內容。
3. 這將開啟一個視窗；在該視窗的部分清單中，選擇 **即時電腦防護 → KSN 使用**。
4. 單擊**"設定"**。
5. 在"**KSN 代理設定**"塊中，使用"**使用管理伺服器為 KSN 代理伺服器**"核取方塊來啟用或停用 KSN 代理。

6. 如有必要，選中**"當 KSN 代理伺服器不可用時使用卡巴斯基安全網路伺服器"**核取方塊。

   如果選中該核取方塊，當 KSN 代理服務不可用時，Kaspersky Embedded Systems Security 將使用 KSN 伺服器。KSN 伺服器可以位於 Kaspersky 側，也可以位於協力廠商一側的伺服器（使用卡巴斯基私有安全網路時）。

7. 儲存變更。

如何在 Kaspersky Embedded Systems Security 主控台中啟用 KSN 代理

1. 在應用程式主控台樹狀目錄中，展開**"即時電腦防護"**節點。
2. 選擇**"卡巴斯基安全網路"**子節點。
3. 在應用程式主視窗中，點擊**內容**。
4. 在**"KSN 代理設定"**塊中，使用**"使用管理伺服器為 KSN 代理伺服器"**核取方塊來啟用或停用 KSN 代理。
5. 如有必要，選中**"當 KSN 代理伺服器不可用時使用卡巴斯基安全網路伺服器"**核取方塊。

   如果選中該核取方塊，當 KSN 代理服務不可用時，Kaspersky Embedded Systems Security 將使用 KSN 伺服器。KSN 伺服器可以位於 Kaspersky 側，也可以位於協力廠商一側的伺服器（使用卡巴斯基私有安全網路時）。

6. 儲存變更。

如何在卡巴斯基安全管理中心網頁主控台中啟用 KSN 代理

1. 在網頁主控台的主視窗中，選擇**資產管理 → 政策**。
2. 點擊 Kaspersky Embedded Systems Security 政策的名稱。

   政策內容視窗將開啟。

3. 選擇**"應用程式設定"**標籤。
4. 轉到**即時電腦防護 → KSN 使用** 並點擊 **配置** 按鈕。
5. 選擇或者清除**"使用管理伺服器為 KSN 代理伺服器"**核取方塊以啟用或停用 KSN 代理。
6. 如有必要，選中**"當 KSN 代理伺服器不可用時使用卡巴斯基安全網路伺服器"**核取方塊。

   如果選中該核取方塊，當KSN Proxy服務不可用時，Kaspersky Embedded Systems Security 將使用 KSN 伺服器。KSN 伺服器可以位於 Kaspersky 側，也可以位於協力廠商一側的伺服器（使用卡巴斯基私有安全網路時）。

7. 儲存變更。

KSN 代理位址與管理伺服器位址比對。如果管理伺服器網域名稱被變更，則您需要手動更新 KSN 代理位址。

弱點利用防禦

Kaspersky Embedded Systems Security 提供防護處理程序記憶體免受弱點利用的能力。此功能由弱點利用防禦元件實現，您可以使用該元件變更元件的活動狀態並配置處理程序弱點利用防禦。

弱點利用防禦元件可偵測利用電腦弱點來利用管理員權限或執行惡意活動的程式程式碼。例如，弱點利用程式可以利用緩衝區溢位攻擊。為此，弱點利用程式會向易受攻擊的應用程式傳送大量資料。處理此資料時，易受攻擊的應用程式會執行惡意程式碼。此攻擊的結果是，弱點利用程式可啟動未經授權的惡意軟體安裝。當存在從易於感染的應用程式執行可執行檔的嘗試，並且該嘗試並非由使用者執行時，Kaspersky Embedded Systems Security 將封鎖該檔案執行或通知使用者。該元件透過在受防護的處理程序中插入外部處理程序防護代理來防護處理程序記憶體免受弱點利用。

處理程序防護代理（以下也稱為*代理*）是一個動態載入的 Kaspersky Embedded Systems Security 模組，該模組可以插入到受防護的處理程序中，以便監控處理程序的完整性並降低被弱點利用的風險。

該代理在受防護的處理程序內的執行需要啟動和停止處理程序：只有處理程序已重新啟動，才能實現首次載入代理到已新增到受防護的處理程序清單中。此外，從受防護的處理程序清單中刪除處理程序後，只有該處理程序已重新啟動才能移除代理。

必須停止代理才能從受防護的處理程序中移除它：如果弱點利用防禦元件被解除安裝，則應用程式將凍結環境並強制從受防護的處理程序中移除代理。如果在元件移除過程中在任一受防護處理程序中插入代理，則必須終止受影響的處理程序。可能需要重新啟動受防護裝置（例如，如果系統處理程序正在受到防護）。

如果偵測到受防護的處理程序中存在弱點利用攻擊的跡象，則 Kaspersky Embedded Systems Security 執行以下操作之一：

- 如果進行弱點利用嘗試，則終止該處理程序。
- 報告處理程序已遭到入侵的事實。

您可採用以下方法之一停止處理程序防護：

- 移除該元件。
- 從受防護的處理程序清單中移除該處理程序並重新啟動該處理程序。

弱點利用防禦模式

可以選擇以下一種模式來配置所執行的操作，以降低弱點在受防護處理程序中被利用的風險：

- **封鎖**如果選擇此模式，則 Kaspersky Embedded Systems Security 在偵測到弱點利用嘗試時（如果已對該處理程序應用積極的攻擊緩解技術），將終止受防護的處理程序。

  當偵測到嘗試在受防護的關鍵作業系統處理程序中利用弱點時，無論弱點利用防禦元件設定中所指定的模式如何，Kaspersky Embedded Systems Security 都不會終止處理程序。

- **通知**（在卡巴斯基安全管理中心網頁主控台中工作時 – **通知**）。套用此模式可以使用安全記錄中的事件來接收受防護處理程序中的弱點實例的有關資訊。被利用的處理程序將繼續執行。

  如果選擇此模式，Kaspersky Embedded Systems Security 將建立事件來記錄所有弱點利用嘗試。預設情況下會選擇。

啟用和停用弱點利用防禦

Kaspersky Embedded Systems Security 可監控易受攻擊的應用程式執行的可執行檔。如果 Kaspersky Embedded Systems Security 偵測到某個易於感染的應用程式的可執行檔被除使用者以外的事物執行，Kaspersky Embedded Systems Security 將執行選擇的操作（例如，封鎖運行）。

如何在卡巴斯基安全管理中心管理主控台中啟用或停用弱點利用防禦

1. 在卡巴斯基安全管理中心管理主控台樹狀目錄中，選取**政策**。
2. 選擇必要的 Kaspersky Embedded Systems Security 的政策然後按兩下開啟政策內容。
3. 這將開啟一個視窗；在該視窗的相關部分的清單中，選擇 **即時電腦防護 → 弱點利用防禦**。
4. 單擊**"設定"**。
5. 選擇**"弱點利用防禦"**核取方塊來啟用元件。
6. 在**一般**頁簽上，選擇一個 弱點利用防禦模式：**封鎖** 或者 **通知**。
7. 如有必要，請清除 **弱點利用防禦** 核取方塊以停用該元件。
8. 儲存變更。

如何在 Kaspersky Embedded Systems Security 主控台中啟用或停用弱點利用防禦

1. 在應用程式主控台樹狀目錄中，展開**"即時電腦防護"**節點。
2. 選擇**"弱點利用防禦"**子節點。
3. 在應用程式主視窗中，點擊**內容**。
4. 選擇**"弱點利用防禦"**核取方塊來啟用元件。
5. 在**一般**頁簽上，選擇一個 弱點利用防禦模式：**封鎖** 或者 **通知**。
6. 如有必要，請清除 **弱點利用防禦** 核取方塊以停用該元件。
7. 儲存變更。

如何在卡巴斯基安全管理中心網頁主控台中啟用或停用弱點利用防禦

1. 在網頁主控台的主視窗中，選擇**資產管理 → 政策**。
2. 點擊 Kaspersky Embedded Systems Security 政策的名稱。

   政策內容視窗將開啟。

3. 選擇“**應用程式設定**”標籤。

4. 轉到**即時電腦防護 → 弱點利用防禦** 並點擊 **配置** 按鈕。

5. 這將開啟一個視窗；在此視窗中，在 **弱點利用防禦模式**下面，選擇 **防止易受感染的處理程序被利用弱點** 核取方塊以啟用該元件。

6. 選擇一個 弱點利用防禦模式：**封鎖** 或者 **通知**。

7. 如有必要，請清除 **防止易受感染的處理程序被利用弱點** 核取方塊以停用該元件。

8. 儲存變更。

啟用和停用記憶體防護

Kaspersky Embedded Systems Security 會封鎖嘗試存取系統處理程序的外部處理程序。預設情況下，啟用系統處理程序記憶體防護。

如何在卡巴斯基安全管理中心管理主控台中啟用或停用記憶體防護

1. 在卡巴斯基安全管理中心管理主控台樹狀目錄中，選取**政策**。

2. 選擇必要的 Kaspersky Embedded Systems Security 的政策然後按兩下開啟政策內容。

3. 這將開啟一個視窗；在該視窗的相關部分的清單中，選擇 **即時電腦防護 → 弱點利用防禦**。

4. 單擊**“設定”**。

5. 在**“一般”**頁簽上，選中**“啟用系統處理程序記憶體防護”**核取方塊。

6. 如有必要，清除**“啟用系統處理程序記憶體防護”**核取方塊。

7. 儲存變更。

如何在 Kaspersky Embedded Systems Security 主控台中啟用或停用記憶體防護

1. 在應用程式主控台樹狀目錄中，展開**“即時電腦防護”**節點。

2. 選擇**“弱點利用防禦”**子節點。

3. 在應用程式主視窗中，點擊**內容**。

4. 在**“一般”**頁簽上，選中**“啟用系統處理程序記憶體防護”**核取方塊。

5. 如有必要，清除**“啟用系統處理程序記憶體防護”**核取方塊。

6. 儲存變更。

如何在卡巴斯基安全管理中心網頁主控台中啟用或停用記憶體防護

1. 在網頁主控台的主視窗中，選擇**資產管理 → 政策**。
2. 點擊 Kaspersky Embedded Systems Security 政策的名稱。
   政策內容視窗將開啟。
3. 選擇**"應用程式設定"**標籤。
4. 轉到**即時電腦防護 → 弱點利用防禦** 並點擊 **配置** 按鈕。
5. 在開啟之視窗的**"系統處理程序記憶體防護"**塊中，選中**"系統處理程序記憶體防護"**核取方塊。
6. 如有必要，請清除 **系統處理程序記憶體防護** 核取方塊以停用系統處理程序記憶體防護。
7. 儲存變更。

建立受防護的處理程序清單

預設情況下，弱點利用防禦元件可防護多個處理程序。應用程式可以自動產生受防護處理程序的清單。您也可以手動新增或刪除處理程序。

如何在卡巴斯基安全管理中心管理主控台中管理受防護處理程序清單

1. 在卡巴斯基安全管理中心管理主控台樹狀目錄中，選取**政策**。
2. 選擇必要的 Kaspersky Embedded Systems Security 的政策然後按兩下開啟政策內容。
3. 這將開啟一個視窗；在該視窗的相關部分的清單中，選擇 **即時電腦防護 → 弱點利用防禦**。
4. 單擊**"設定"**。
5. 在**受防護的處理程序**頁簽上，選擇以下選項之一以防護處理程序免受惡意程式碼注入：
   - **自動偵測受防護的處理程序**如果選擇此選項，應用程式會自動建立受防護處理程序清單。
   - **僅防護以下清單中的處理程序**如果選擇此選項，您可以選擇要防護的處理程序。
6. 如果選擇了**僅防護以下清單中的處理程序**，您可以透過執行下列操作之一來編輯受防護處理程序的清單：
   - 如果需要，請點擊**新增**並選擇要新增至受防護處理程序清單中的處理程序。
   - 如果要從已建立的受防護處理程序清單中刪除某個處理程序，請在清單中選取該處理程序，然後點擊**刪除**。
     在清單中選擇一個或多個處理程序後，**刪除**按鈕將變為可用。
7. 儲存變更。

如何使用 Kaspersky Embedded Systems Security 主控台管理受防護處理程序清單

1. 在應用程式主控台樹狀目錄中，展開**"即時電腦防護"**節點。
2. 選擇**"弱點利用防禦"**子節點。

3. 在應用程式主視窗中，點擊**內容**。

4. 在**受防護的處理程序**頁簽上，選擇以下選項之一以防護處理程序免受惡意程式碼注入：

   - **自動偵測受防護的處理程序**如果選擇此選項，應用程式會自動建立受防護處理程序清單。
   - **僅防護以下清單中的處理程序**如果選擇此選項，您可以選擇要防護的處理程序。

5. 如果選擇了**僅防護以下清單中的處理程序**，您可以透過執行下列操作之一來編輯受防護處理程序的清單：

   - 如果需要，請點擊**新增**並選擇要新增至受防護處理程序清單中的處理程序。
   - 如果要從已建立的受防護處理程序清單中刪除某個處理程序，請在清單中選取該處理程序，然後點擊**刪除**。

     在清單中選擇一個或多個處理程序後，**刪除**按鈕將變為可用。

6. 儲存變更。

如何在卡巴斯基安全管理中心網頁主控台中管理受防護處理程序清單

1. 在網頁主控台的主視窗中，選擇**資產管理 → 政策**。
2. 點擊 Kaspersky Embedded Systems Security 政策的名稱。

   政策內容視窗將開啟。
3. 選擇**"應用程式設定"**標籤。
4. 轉到**即時電腦防護 → 弱點利用防禦**部分並點擊**配置**按鈕。
5. 在**受防護的處理程序清單**下面，選擇以下選項之一以防護處理程序免受惡意程式碼注入：

   - **自動偵測受防護的處理程序**如果選擇此選項，應用程式會自動建立受防護處理程序清單。
   - **僅防護以下清單中的處理程序**如果選擇此選項，您可以新增、編輯和移除要防護的處理程序。
6. 如果您選擇了**僅防護以下清單中的處理程序**，執行下列操作之一：

   - 點擊**新增**開啟**受防護的處理程序** 視窗，並在該視窗中：

     a. 選擇**"受防護的處理程序"**核取方塊。

     b. 在**"處理程序名稱"**欄位中輸入處理程序的名稱。

     c. 儲存變更。
   - 如有必要，編輯受防護處理程序清單中的處理程序設定。為此，請執行以下操作：

     a. 在受防護的處理程序清單中選擇一個處理程序。

     b. 單擊**"編輯"**。在清單中選擇一個或多個處理程序後，**編輯**按鈕將變為可用。

     c. 在**"受防護的處理程序"**視窗中，選擇或者清除**"受防護的處理程序"**核取方塊。

d. 如有必要，請在**處理程序名稱**欄位中編輯處理程序的名稱。

e. 儲存變更。

- 如有必要，您可以從受防護處理程序清單中刪除處理程序。為此，請執行以下操作：

  a. 在受防護的處理程序清單中選擇一個或多個處理程序。

  b. 單擊**"刪除"**。在清單中選擇一個或多個處理程序後，**刪除**按鈕將變為可用。

7. 儲存變更。

修復引擎

修復引擎允許 Kaspersky Embedded Systems Security 復原惡意軟體在作業系統中執行的操作。

當回溯作業系統中的惡意軟體活動時，Kaspersky Embedded Systems Security 會執行以下操作：

- **檔案活動**
  - 刪除惡意軟體在除網路磁碟外的所有介質上建立的可執行檔。
  - 移除已被惡意軟體入侵的程式所建立的可執行檔。
  - 還原被惡意軟體修改或刪除的檔案。

  檔案還原功能有**一些限制**。
  - 應用程式只能還原檔案系統為 NTFS 或 FAT32 的裝置上的檔案。
  - 應用程式可還原具有以下副檔名的檔案：odt, ods, odp, odm, odc, odb, doc, docx, docm, wps, xls, xlsx, xlsm, xlsb, xlk, ppt, pptx, pptm, mdb, accdb, pst, dwg, dxf, dxg, wpd, rtf, wb2, pdf, mdf, dbf, psd, pdd, eps, ai, indd, cdr, jpg, jpe, dng, 3fr, arw, srf, sr2, bay, crw, cr2, dcr, kdc, erf, mef, mrw, nef, nrw, orf, raf, raw, rwl, rw2, r3d, ptx, pef, srw, x3f, der, cer, crt, pem, pfx, p12, p7b, p7c, 1cd。
  - 無法還原位於網路磁碟機或可重寫 CD/DVD 上的檔案。
  - 無法還原使用加密檔案系統 (EFS) 加密的檔案。有關 EFS 操作的詳細資訊，請造訪 Microsoft 網站。
  - 應用程式不會監控由作業系統內核等級的處理程序對檔案執行的修改。
  - 應用程式不會監控透過網路介面對檔案執行的修改（例如，如果某個檔案儲存在共用資料夾中，並且處理程序從其他電腦上遠端啟動）。
- **登錄檔活動**
  - 刪除由惡意軟體建立的登錄機碼。

  Kaspersky Embedded Systems Security 不會還原被惡意軟體修改或刪除的登錄機碼。
- **系統活動**
  - 終止由惡意軟體啟動的處理程序。
  - 終止被惡意應用程式滲透的處理程序。

  Kaspersky Embedded Systems Security 不會還原被惡意程式掛起的處理程序。

- **網路活動**
  - 封鎖惡意軟體的網路活動。
  - 封鎖被惡意軟體入侵的處理程序的網路活動。

惡意應用程式操作回溯可以由即時檔案防護 元件或在按需掃描期間啟動。

回溯惡意程式操作的過程將會影響一組嚴格限定的資料。回溯對於作業系統或您的電腦中資料的完整性不會產生負面影響。

如何在卡巴斯基安全管理中心管理主控台中啟用或停用修復引擎元件

1. 在卡巴斯基安全管理中心管理主控台樹狀目錄中，選取**政策**。
2. 選擇必要的政策並點擊以開啟政策內容。
3. 在政策內容視窗中，轉至「**即時電腦防護**」區域。
4. 在"**修復引擎**"塊中，點擊"**設定**"按鈕。
5. **修復引擎**視窗將在**一般**頁簽上開啟。
6. 執行以下操作之一：
   - 如果您希望啟用修復引擎元件，請選中"**修復引擎**"核取方塊。
   - 如果您希望停用修復引擎元件，請清除"**修復引擎**"核取方塊。
7. 在**修復引擎**視窗中，按一下**確定**按鈕。
8. 在**屬性：<政策名稱>**視窗中按一下**確定**按鈕。

如何在卡巴斯基安全管理中心網頁主控台中啟用或停用修復引擎元件

1. 在網頁主控台的主視窗中，選擇**資產管理 → 政策**。
2. 點擊 Kaspersky Embedded Systems Security 政策的名稱。
   政策內容視窗將開啟。
3. 選擇"**應用程式設定**"標籤。
4. 選擇 **即時電腦防護** 部分。
5. 在"**修復引擎**"塊中，點擊"**配置**"按鈕。
6. 開啟"**修復引擎**"視窗。
7. 執行以下操作之一：
   - 如果您希望啟用修復引擎元件，請選中"**修復引擎**"核取方塊。
   - 如果您希望停用修復引擎元件，請清除"**修復引擎**"核取方塊。

8. 在**修復引擎**視窗中，按一下**確定**按鈕。

9. 在**<政策名稱>**視窗中按一下**儲存**按鈕。

如何在 Kaspersky Embedded Systems Security 主控台中啟用或停用修復引擎元件

1. 在管理主控台樹狀目錄中，選擇**即時電腦防護 → 修復引擎**資料夾。

2. 在結果窗格中點擊**"內容"**連結。
   修復引擎視窗將在**一般**頁簽上開啟。

3. 執行以下操作之一：

   - 如果您希望啟用修復引擎元件，請選中**"修復引擎"**核取方塊。
   - 如果您希望停用修復引擎元件，請清除**"修復引擎"**核取方塊。

4. 在**修復引擎**視窗中，按一下**確定**按鈕。

行為偵測

“行為偵測”元件接收您電腦上的應用程式操作的資料，並將此資訊提供給其他防護元件以提高效能。“行為偵測”元件將行為流簽章 (BSS) 用於應用程式。如果應用程式操作比對危險活動行為流簽章，Kaspersky Embedded Systems Security 將執行選定的回應操作。根據危險活動行為流簽章的 Kaspersky Embedded Systems Security 功能為電腦提供主動防禦。

啟用和停用本機資料夾的加密防護

如何在卡巴斯基安全管理中心管理主控台中啟用或停用行為偵測元件

1. 在卡巴斯基安全管理中心管理主控台樹狀目錄中，選取**政策**。
2. 選擇必要的政策並點擊以開啟政策內容。
3. 在政策屬性視窗中，選取“**即時電腦防護**”。
4. 在 **行為偵測** 部分中，點擊 **設定**。
5. 選擇或者清除“**行為偵測**“核取方塊來啟用或停用元件。
6. 轉至**一般**頁簽。
7. 使用“**啟用本機資料夾對外部加密的防護**“核取方塊來啟用或停用選項。如果選取該核取方塊，Kaspersky Embedded Systems Security 會使用以下指定操作回應惡意活動。
8. 在“**偵測到惡意軟體活動時的動作**”塊中選擇相關操作：
   - **刪除**如果選擇此項目，在偵測到惡意活動時，Kaspersky Embedded Systems Security 會刪除惡意應用程式的可執行檔，同時在備份區建立該檔案的備份副本。
   - **封鎖**如果選擇此項目，在偵測到惡意活動時，Kaspersky Embedded Systems Security 會終止該應用程式。
   - **通知**如果選擇此項目並且偵測到應用程式的惡意軟體活動，Kaspersky Embedded Systems Security 將應用程式惡意軟體活動的相關資訊新增至活動威脅清單。
9. 儲存變更。若要在電腦上套用該政策，請關閉掛鎖。

如何在卡巴斯基安全管理中心網頁主控台中啟用或停用行為偵測元件

1. 在網頁主控台的主視窗中，選擇**資產管理 → 政策**。
2. 點擊 Kaspersky Embedded Systems Security 政策的名稱。
   政策內容視窗將開啟。
3. 選擇“**應用程式設定**”標籤。
4. 轉到**即時電腦防護 → 行為偵測** 並點擊 **配置** 按鈕。
   開啟“**行為偵測**”視窗。
5. 使用“**啟用行為偵測**“核取方塊來啟用或停用元件。

6. 轉至**一般**頁簽。

7. 使用"**啟用本機資料夾對外部加密的防護**"核取方塊來啟用或停用選項。如果選取該核取方塊，Kaspersky Embedded Systems Security 會使用以下指定操作回應惡意活動。

8. 在"**偵測到共用資料夾的外部加密時**"塊中選擇相關操作：

   - **刪除**如果選擇此項目，在偵測到惡意活動時，Kaspersky Embedded Systems Security 會刪除惡意應用程式的可執行檔，同時在備份區建立該檔案的備份副本。
   - **封鎖**如果選擇此項目，在偵測到惡意活動時，Kaspersky Embedded Systems Security 會終止該應用程式。
   - **通知**如果選擇此項目並且偵測到應用程式的惡意軟體活動，Kaspersky Embedded Systems Security 將應用程式惡意軟體活動的相關資訊新增至活動威脅清單。

9. 儲存變更。若要在電腦上套用該政策，請關閉掛鎖。

如何在應用程式主控台中啟用或停用行為偵測元件

1. 在 Kaspersky Embedded Systems Security 主控台樹狀目錄中，選擇 **即時電腦防護 → 行為偵測**。

2. 在**行為偵測**節點的結果窗格中，點擊 **內容**。

   這將開啟**內容: 行為偵測**視窗。

3. 選中"**行為偵測**"核取方塊。

4. 轉至**一般**頁簽。

5. 使用"**啟用本機資料夾對外部加密的防護**"核取方塊來啟用或停用選項。如果選取該核取方塊，Kaspersky Embedded Systems Security 會使用以下指定操作回應惡意活動。

6. 在"**偵測到共用資料夾的外部加密時**"塊中選擇相關操作：

   - **刪除**如果選擇此項目，在偵測到惡意活動時，Kaspersky Embedded Systems Security 會刪除惡意應用程式的可執行檔，同時在備份區建立該檔案的備份副本。
   - **封鎖**如果選擇此項目，在偵測到惡意活動時，Kaspersky Embedded Systems Security 會終止該應用程式。
   - **通知**如果選擇此項目並且偵測到應用程式的惡意軟體活動，Kaspersky Embedded Systems Security 將應用程式惡意軟體活動的相關資訊新增至活動威脅清單。

7. 儲存變更。

防止共用資料夾被外部加密

此元件只能監控針對儲存在檔案系統為 NTFS 的大型儲存裝置上並且未使用 EFS 加密的檔案所進行的操作。

共用資料夾對外部加密的防護提供對共用資料夾中活動的分析。如果該活動與外部加密的典型行為流簽章比對，Kaspersky Embedded Systems Security 將執行選定操作。

如果偵測到嘗試修改共用資料夾中的檔案，Kaspersky Embedded Systems Security 將執行以下操作：

- 封鎖存取啟動惡意活動的工作階段的檔案修改（檔案將為只讀）。
- 建立被修改的檔案的備份副本。
- 向本機應用程式介面報告新增條目，並將有關偵測到的惡意活動的資訊傳送至卡巴斯基安全管理中心。
- 此外，如果啟用了"修復引擎"元件，被修改的檔案將從備份副本還原。

啟用和停用共用資料夾對外部加密的防護

預設情況下，共用資料夾對外部加密的防護已啟用，並按照卡巴斯基專家的建議運行。若要設定此功能，您可以建立防護範圍並配置排除項目（如有必要）。預設情況下，應用程式會自動識別共用資料夾並監視所有資料夾中的檔案活動。如果偵測到對共用資料夾中的檔案進行外部加密的嘗試，Kaspersky Embedded Systems Security 會封鎖遠端使用者的工作階段一小時（預設）。

安裝 Kaspersky Embedded Systems Security 後，共用資料夾對外部加密的防護將受到限制，直到電腦重新啟動為止。

如何在卡巴斯基安全管理中心管理主控台中啟用或停用防止共用資料夾被外部加密

1. 在卡巴斯基安全管理中心管理主控台樹狀目錄中，選取**政策**。
2. 選擇必要的政策並點擊以開啟政策內容。
3. 在政策屬性視窗中，選取"**即時電腦防護**"。
4. 在 **行為偵測** 部分中，點擊 **設定**。
5. 選擇或者清除"**行為偵測**"核取方塊來啟用或停用元件。
6. 轉至**防護共用資料夾**頁簽。
7. 使用"**防護共用資料夾**"核取方塊來啟用或停用選項。
8. 在"**共用資料夾對外部加密的防護**"塊中選擇相關操作：
   - **封鎖連線時間 N 分鐘**。如果選擇了該選項，則當 Kaspersky Embedded Systems Security 偵測到嘗試修改共用資料夾中的檔案時，它會封鎖啟動了惡意活動的工作階段的檔案修改存取權限，並建立修改檔案的備份副本。

     如果啟用了"修復引擎"元件，並且選擇"**封鎖連線時間 N 分鐘**"選項，被修改的檔案會被從備份副本還原。

   - **通知**如果選擇此選項，則如果偵測到修改共用資料夾中的檔案的嘗試，Kaspersky Embedded Systems Security 會將有關共用資料夾中此檔案修改嘗試的資訊新增至活動威脅清單中，將記錄新增至應用程式的本機介面報告中，並將有關惡意活動偵測的資訊傳送到卡巴斯基安全管理中心。

9. 如有必要，請建立防護範圍並配置排除項目。

10. 儲存變更。若要在電腦上套用該政策，請關閉掛鎖。

如何在卡巴斯基安全管理中心網頁主控台中啟用或停用防止共用資料夾被外部加密

1. 在網頁主控台的主視窗中，選擇**資產管理 → 政策**。

2. 點擊 Kaspersky Embedded Systems Security 政策的名稱。
   政策內容視窗將開啟。

3. 選擇"**應用程式設定**"標籤。

4. 轉到**即時電腦防護 → 行為偵測** 並點擊 **配置** 按鈕。
   開啟"**行為偵測**"視窗。

5. 使用"**啟用行為偵測**"核取方塊來啟用或停用元件。

6. 轉至**防護共用資料夾**頁簽。

7. 使用"**啟用共用資料夾對外部加密的防護**"核取方塊來啟用或停用選項。

8. 在"**外部加密偵測**"塊中選擇相關操作：

   - **封鎖連線**如果選擇了該選項，則當 Kaspersky Embedded Systems Security 偵測到嘗試修改共用資料夾中的檔案時，它會封鎖啟動了惡意活動的工作階段的檔案修改存取權限，並建立修改檔案的備份副本。

     如果啟用了"修復引擎"元件，並且選擇"**封鎖連線** 選項，被修改的檔案會被從備份副本還原。

   - **通知**如果選擇此選項，則如果偵測到修改共用資料夾中的檔案的嘗試，Kaspersky Embedded Systems Security 會將有關共用資料夾中此檔案修改嘗試的資訊新增至活動威脅清單中，將記錄新增至應用程式的本機介面報告中，並將有關惡意活動偵測的資訊傳送到卡巴斯基安全管理中心。

9. 如有必要，請建立防護範圍並配置排除項目。

10. 儲存變更。若要在電腦上套用該政策，請關閉掛鎖。

如何在應用程式主控台中啟用或停用防止共用資料夾被外部加密

1. 在 Kaspersky Embedded Systems Security 主控台樹狀目錄中，選擇 **即時電腦防護 → 行為偵測**。

2. 在**行為偵測**節點的結果窗格中，點擊 **內容**。
   這將開啟**內容: 行為偵測**視窗。

3. 選中"**行為偵測**"核取方塊。

4. 轉至**防護共用資料夾**頁簽。

5. 使用"**防護共用資料夾**"核取方塊來啟用或停用選項。

6. 在“**共用資料夾對外部加密的防護**”塊中選擇相關操作：

   - **封鎖連線時間 N 分鐘**。如果選擇了該選項，則當 Kaspersky Embedded Systems Security 偵測到嘗試修改共用資料夾中的檔案時，它會封鎖啟動了惡意活動的工作階段的檔案修改存取權限，並建立修改檔案的備份副本。

     如果啟用了修復引擎元件，並且選擇“**封鎖連線時間 N 分鐘**”選項，被修改的檔案會被從備份副本還原。

   - **通知**如果選擇此選項，則如果偵測到修改共用資料夾中的檔案的嘗試，Kaspersky Embedded Systems Security 會將有關共用資料夾中此檔案修改嘗試的資訊新增至活動威脅清單中，將記錄新增至應用程式的本機介面報告中，並將有關惡意活動偵測的資訊傳送到卡巴斯基安全管理中心。

7. 如有必要，請建立防護範圍並配置排除項目。

8. 儲存變更。

編輯防護範圍

防護範圍 是 Kaspersky Embedded Systems Security 監控其中檔案活動的共用資料夾的路徑清單。Kaspersky Embedded Systems Security 在輸入遮罩時支援環境變數以及 `*` 和 `?` 字元：預設情況下，應用程式會自動識別共用資料夾並監控所有資料夾中的檔案活動。

如果您的組織在使用共用資料夾交換檔案時使用資料加密，從防護範圍中排除資料夾可減少誤判的數量。例如，當使用者在共用資料夾中處理具有 ENC 副檔名的檔案時，行為偵測元件可能提高誤判數量。此類活動比對外部加密通常有的行為模式。如果您加密了共用資料夾中的檔案以防護資料，請將該資料夾新增到排除項目。

如果您希望忽略來自電腦的外部加密嘗試，您也可以排除這些電腦。

如何在卡巴斯基安全管理中心管理主控台中設定防護範圍

1. 在卡巴斯基安全管理中心管理主控台樹狀目錄中，選取**政策**。

2. 選擇必要的政策並點擊以開啟政策內容。

3. 在政策屬性視窗中，選取“**即時電腦防護**”。

4. 在 **行為偵測** 部分中，點擊 **設定**。

5. 選擇或者清除“**行為偵測**“核取方塊來啟用或停用元件。

6. 轉至**防護共用資料夾**頁簽。

7. 在”**防護範圍**”塊中，點擊”**配置**”按鈕。

8. 在開啟的視窗中，選擇“**僅指定的共用資料夾**”模式。

9. 單擊“**新增**”。

10. 這將開啟一個視窗；在該視窗中，輸入要包含在防護範圍中的共用資料夾的路徑（例如， `C:\Share` ）。

    若要將共用資料夾新增至防護範圍，請使用本機路徑。

11. 點擊**"確定"**。

12. 如有必要，定義防護範圍排除項目：

    a. 在**"排除項目"**塊中，點擊**"配置"**按鈕。

    b. 在開啟的視窗中，點擊**"新增"**按鈕。

    c. 在顯示的視窗中，輸入資料夾或者檔案路徑。

    使用遮罩：

    - `*`（星號）字元代表任意一組字元，但 `\` 和 `/` 字元除外（這兩個字元是檔案和資料夾路徑中的檔案和資料夾名稱的分隔符號）。例如，遮罩"`C:\*\*.txt`"將包括位於 C: 磁碟機但是不在子資料夾中所有帶 TXT 副檔名的檔案的路徑。

    - 兩個連續 `*` 字元在檔案或資料夾名稱中代表任意一組字元（包括空集），包括 `\` 和 `/` 字元（這兩個字元是檔案和資料夾路徑中的檔案和資料夾名稱的分隔符號）。例如，遮罩 `C:\Folder\**\*.txt` 將包括位於巢嵌在 `Folder` 內的資料夾（ `Folder` 自身除外）中所有帶 TXT 副檔名的檔案的路徑。遮罩必須包含至少一個嵌套等級。遮罩 `C:\**\*.txt` 不是有效遮罩。

    - `?`（問號）字元代表任意單個字元，但 `\` 和 `/` 字元除外（這兩個字元是檔案和資料夾路徑中的檔案和資料夾名稱的分隔符號）。例如，遮罩 `C:\Folder\???.txt` 將包括位於 `Folder` 資料夾中所有帶 TXT 副檔名且名稱由三個字元構成的檔案的路徑。

    您可以從掃描中排除物件，而無需將其從防護範圍內的物件清單中刪除。為此，請清除物件旁邊的核取方塊。

13. 儲存變更。若要在電腦上套用該政策，請關閉掛鎖。

如何在卡巴斯基安全管理中心網頁主控台中設定防護範圍

1. 在網頁主控台的主視窗中，選擇**資產管理 → 政策**。

2. 點擊 Kaspersky Embedded Systems Security 政策的名稱。

   政策內容視窗將開啟。

3. 選擇**"應用程式設定"**標籤。

4. 轉到**即時電腦防護 → 行為偵測** 並點擊 **配置** 按鈕。

   開啟**"行為偵測"**視窗。

5. 使用**"啟用行為偵測"**核取方塊來啟用或停用元件。

6. 轉至**防護共用資料夾**頁簽。

7. 在**防護範圍**下，選擇**僅指定的共用資料夾**模式。

8. 單擊**"新增"**。

9. 這將開啟一個視窗；在該視窗中，輸入要包含在防護範圍中的共用資料夾的路徑（例如， `C:\Share` ）。

   若要將共用資料夾新增至防護範圍，請使用本機路徑。

10. 點擊**"確定"**。

11. 如有必要，定義防護範圍排除項目：

    a. 在**"要排除的物件"**塊中，點擊**"新增"**按鈕。

    b. 在顯示的視窗中，輸入資料夾或者檔案路徑。

    使用遮罩：

    - `*`（星號）字元代表任意一組字元，但 `\` 和 `/` 字元除外（這兩個字元是檔案和資料夾路徑中的檔案和資料夾名稱的分隔符號）。例如，遮罩**"`C:\*\*.txt`"**將包括位於 C: 磁碟機但是不在子資料夾中所有帶 TXT 副檔名的檔案的路徑。

    - 兩個連續 `*` 字元在檔案或資料夾名稱中代表任意一組字元（包括空集），包括 `\` 和 `/` 字元（這兩個字元是檔案和資料夾路徑中的檔案和資料夾名稱的分隔符號）。例如，遮罩 `C:\Folder\**\*.txt` 將包括位於巢嵌在 `Folder` 內的資料夾（ `Folder`自身除外）中所有帶 TXT 副檔名的檔案的路徑。遮罩必須包含至少一個嵌套等級。遮罩 `C:\**\*.txt` 不是有效遮罩。

    - `?`（問號）字元代表任意單個字元，但 `\` 和 `/` 字元除外（這兩個字元是檔案和資料夾路徑中的檔案和資料夾名稱的分隔符號）。例如，遮罩 `C:\Folder\???.txt` 將包括位於 `Folder` 資料夾中所有帶 TXT 副檔名且名稱由三個字元構成的檔案的路徑。

    您可以從掃描中排除物件，而無需將其從防護範圍內的物件清單中刪除。為此，請清除物件旁邊的核取方塊。

12. 儲存變更。若要在電腦上套用該政策，請關閉掛鎖。

如何在應用程式主控台中配置防護範圍

1. 在政策屬性視窗中，選取**"即時電腦防護"**。

2. 在 **行為偵測** 部分中，點擊 **設定**。

3. 在 Kaspersky Embedded Systems Security 主控台樹狀目錄中，選擇 **即時電腦防護 → 行為偵測**。

4. 在**行為偵測**節點的結果窗格中，點擊 **內容**。

   這將開啟**內容: 行為偵測**視窗。

5. 選擇或者清除**"行為偵測"**核取方塊來啟用或停用元件。

6. 轉至**防護共用資料夾**頁簽。

7. 在**"防護範圍"**塊中，點擊**"配置"**按鈕。

8. 在開啟的視窗中，選擇**"僅指定的共用資料夾"**模式。

9. 在**"防護範圍"**塊中，點擊**"新增"**按鈕。

10. 這將開啟一個視窗；在該視窗中，輸入要包含在防護範圍中的共用資料夾的路徑（例如， `C:\Share` ）。

    若要將共用資料夾新增至防護範圍，請使用本機路徑。

11. 點擊"**確定**"。

12. 如有必要，定義防護範圍排除項目：

    a. 在"**排除項目**"塊中，點擊"**設定**"按鈕。

    b. 在顯示的"**按遮罩排除**"視窗中，點擊"**新增**"按鈕。

    c. 在顯示的視窗中，輸入資料夾或者檔案路徑。

    使用遮罩：

    - `*`（星號）字元代表任意一組字元，但 `\` 和 `/` 字元除外（這兩個字元是檔案和資料夾路徑中的檔案和資料夾名稱的分隔符號）。例如，遮罩"`C:\*\*.txt`"將包括位於 C: 磁碟機但是不在子資料夾中所有帶 TXT 副檔名的檔案的路徑。

    - 兩個連續 `*` 字元在檔案或資料夾名稱中代表任意一組字元（包括空集），包括 `\` 和 `/` 字元（這兩個字元是檔案和資料夾路徑中的檔案和資料夾名稱的分隔符號）。例如，遮罩 `C:\Folder\**\*.txt` 將包括位於巢嵌在 `Folder` 內的資料夾（ `Folder` 自身除外）中所有帶 TXT 副檔名的檔案的路徑。遮罩必須包含至少一個嵌套等級。遮罩 `C:\**\*.txt` 不是有效遮罩。

    - `?`（問號）字元代表任意單個字元，但 `\` 和 `/` 字元除外（這兩個字元是檔案和資料夾路徑中的檔案和資料夾名稱的分隔符號）。例如，遮罩 `C:\Folder\???.txt` 將包括位於 `Folder` 資料夾中所有帶 TXT 副檔名且名稱由三個字元構成的檔案的路徑。

    您可以從掃描中排除物件，而無需將其從防護範圍內的物件清單中刪除。為此，請清除物件旁邊的核取方塊。

13. 儲存變更。

新增受信任的電腦以進行外部資料加密

如果您的組織在檔案交換工作流程中使用外部資料加密，則您必須建立受信任電腦清單。Kaspersky Embedded Systems Security 不會監控來自受信任電腦的資料加密。

在執行 Windows XP 或 Windows Server 2003 的受保護裝置上，即使您將遠端電腦新增至受信任電腦清單，Kaspersky Embedded Systems Security 仍會監控共用資料夾加密嘗試。

必須啟用稽核登入服務，才能從共用資料夾對外部加密的防護中排除位址。預設情況下，稽核登入服務已停用（有關啟用稽核登入服務的詳細資訊，請存取 Microsoft 網站）。

如果遠端電腦在 Kaspersky Embedded Systems Security 啟動前啟動，從共用資料夾防護中排除位址的功能將不適用於該遠端電腦。您可以在 Kaspersky Embedded Systems Security 啟動後重啟該遠端電腦，確保從共用資料夾防護中排除位址的功能在此遠端電腦上有效。

如何在卡巴斯基安全管理中心管理主控台中新增受信任的電腦以對資料進行外部加密

1. 在卡巴斯基安全管理中心管理主控台樹狀目錄中，選取**政策**。
2. 選擇必要的政策並點擊以開啟政策內容。
3. 在政策屬性視窗中，選取**"即時電腦防護"**。
4. 在 **行為偵測** 部分中，點擊 **設定**。
5. 轉至**防護共用資料夾**頁簽。
6. 在**"IP 位址排除項目"**塊中，點擊**"配置"**按鈕。
7. 在開啟的視窗中，點擊**"新增"**按鈕。
8. 輸入不應處理其外部加密嘗試的電腦的 IP 位址或名稱。
9. 儲存變更。若要在電腦上套用該政策，請關閉掛鎖。

如何在卡巴斯基安全管理中心網頁主控台中新增受信任的電腦以對資料進行外部加密

1. 在網頁主控台的主視窗中，選擇**資產管理 → 政策**。
2. 點擊 Kaspersky Embedded Systems Security 政策的名稱。
   政策內容視窗將開啟。
3. 選擇**"應用程式設定"**標籤。
4. 轉到**即時電腦防護 → 行為偵測** 並點擊 **配置** 按鈕。
   開啟**"行為偵測"**視窗。
5. 轉至**防護共用資料夾**頁簽。
6. 在**"排除項目"**塊中，點擊**"新增"**按鈕。
7. 輸入不應處理其外部加密嘗試的電腦的 IP 位址或名稱。
8. 儲存變更。若要在電腦上套用該政策，請關閉掛鎖。

如何新增受信任的電腦以在應用程式主控台中對資料進行外部加密

1. 在 Kaspersky Embedded Systems Security 主控台樹狀目錄中，選擇 **即時電腦防護 → 行為偵測**。
2. 在**行為偵測**節點的結果窗格中，點擊 **內容**。
   這將開啟**內容: 行為偵測**視窗。
3. 轉至**防護共用資料夾**頁簽。
4. 在**"IP 位址排除項目"**塊中，點擊**"配置"**按鈕。
5. 在開啟的視窗中，點擊**"新增"**按鈕。

6. 輸入不應處理其外部加密嘗試的電腦的 IP 位址或名稱。

7. 儲存變更。

配置不受信任電腦的封鎖時間

*不受信任的電腦*是參與惡意活動或資料加密的遠端電腦。預設情況下，Kaspersky Embedded Systems Security 會封鎖遠端使用者的工作階段一小時。在封鎖期限到期後，Kaspersky Embedded Systems Security 將從封鎖清單中刪除電腦並還原對共用資料夾的存取。

如何在卡巴斯基安全管理中心管理主控台中設定不受信任電腦的封鎖期限

1. 在卡巴斯基安全管理中心管理主控台樹狀目錄中，選取**政策**。

2. 選擇必要的政策並點擊以開啟政策內容。

3. 在政策屬性視窗中，選取"**即時電腦防護**"。

4. 在 **行為偵測** 部分中，點擊 **設定**。

5. 選擇或者清除"**行為偵測**"核取方塊來啟用或停用元件。

6. 轉至**防護共用資料夾**頁簽。

7. 在**偵測到共用資料夾的外部加密時**下面，配置對從事惡意活動或資料加密的不受信任電腦的封鎖期限。

8. 儲存變更。若要在電腦上套用該政策，請關閉掛鎖 。

如何在卡巴斯基安全管理中心網頁主控台中設定不受信任電腦的封鎖期限

1. 在網頁主控台的主視窗中，選擇**資產管理 → 政策**。

2. 點擊 Kaspersky Embedded Systems Security 政策的名稱。
   政策內容視窗將開啟。

3. 選擇"**應用程式設定**"標籤。

4. 轉到**即時電腦防護 → 行為偵測** 並點擊 **配置** 按鈕。
   開啟"**行為偵測**"視窗。

5. 使用"**啟用行為偵測**"核取方塊來啟用或停用元件。

6. 轉至**防護共用資料夾**頁簽。

7. 在**外部加密偵測**下面，配置對從事惡意活動或資料加密的不受信任電腦的封鎖期限。

8. 儲存變更。若要在電腦上套用該政策，請關閉掛鎖 。

如何在應用程式主控台中設定不受信任電腦的封鎖期限

1. 在 Kaspersky Embedded Systems Security 主控台樹狀目錄中，選擇 **即時電腦防護 → 行為偵測**。
2. 在**行為偵測**節點的結果窗格中，點擊 **內容**。
   這將開啟**內容: 行為偵測**視窗。
3. 選中"**行為偵測**"核取方塊。
4. 轉至**防護共用資料夾**頁簽。
5. 在**共用資料夾對外部加密的防護**下面，配置對從事惡意活動或資料加密的不受信任電腦的封鎖期限。
6. 儲存變更。

匯出和匯入防止共用資料夾被外部加密的排除項目清單

您可以將排除項目清單匯出到 XML 檔案。然後，您可以修改檔案，例如，新增大量相同類型的位址。您還可以使用匯出/匯入功能來備份排除項目清單，或將清單遷移到其他伺服器。

如何在卡巴斯基安全管理中心管理主控台中匯出和匯入排除項目清單

1. 在卡巴斯基安全管理中心管理主控台樹狀目錄中，選取**政策**。
2. 選擇必要的政策並點擊以開啟政策內容。
3. 在政策屬性視窗中，選取"**即時電腦防護**"。
4. 在 **行為偵測** 部分中，點擊 **設定**。
5. 轉至**防護共用資料夾**頁簽。
6. 在"**IP 位址排除項目**"塊中，點擊"**配置**"按鈕。
7. 要匯出規則清單：
   a. 如有必要，選取您想要匯出的排除項目。
   b. 點擊 按鈕並選擇匯出模式：匯出整個排除項目清單或僅匯出選定的排除項目。
   c. 在開啟的視窗中，指定您要將排除項目清單匯出到的 XML 檔案的名稱，然後選取要儲存此檔案的資料夾。
   d. 儲存檔案。
      Kaspersky Embedded Systems Security 會將排除項目清單匯出到 XML 檔案。
8. 若要匯入排除項目清單：
   a. 點擊 → **匯入** 按鈕。
      在開啟的視窗中，選取要從中匯入排除項目清單的 XML 檔案。

b. 開啟檔案。

Kaspersky Embedded Systems Security 匯入排除項目。

9. 儲存變更。若要在電腦上套用該政策，請關閉掛鎖。

如何在網頁主控台中匯出和匯入排除項目清單

1. 在網頁主控台的主視窗中，選擇**資產管理 → 政策**。
2. 點擊 Kaspersky Embedded Systems Security 政策的名稱。
   政策內容視窗將開啟。
3. 選擇"**應用程式設定**"標籤。
4. 轉到**即時電腦防護 → 行為偵測** 並點擊 **配置** 按鈕。
   開啟"**行為偵測**"視窗。
5. 使用"**啟用行為偵測**"核取方塊來啟用或停用元件。
6. 轉至**防護共用資料夾**頁簽。
7. 要匯出"**排除項目**"塊中的排除項目清單：
   a. 如有必要，選取您想要匯出的排除項目。
   b. 點擊 **匯出** 按鈕並選擇匯出模式：匯出整個排除項目清單或僅匯出選定的排除項目。
   c. 儲存檔案。
   Kaspersky Embedded Systems Security 會將排除項目清單匯出到 XML 檔案。
8. 要匯入"**排除項目**"塊中的排除項目清單：
   a. 點擊**匯入**按鈕並選擇匯入模式：新增或替代。
   b. 在開啟的視窗中，選取要從中匯入排除項目清單的 XML 檔案。
   c. 開啟檔案。
   Kaspersky Embedded Systems Security 根據所選模式匯入排除項目。
9. 儲存變更。若要在電腦上套用該政策，請關閉掛鎖。

網路威脅防護

網路威脅防護元件會掃描傳入的網路流量中是否存在典型網路攻擊活動。在偵測到以您的電腦為目標的網路攻擊企圖時，Kaspersky Embedded Systems Security 將封鎖攻擊電腦的網路活動。應用程式資料庫提供目前已知類型的網路攻擊以及應對方法。網路威脅防護元件偵測到的網路攻擊清單會在資料庫和應用程式模組更新期間更新。

預設情況下，「*網路威脅防護*」工作在**封鎖**模式下執行。在此模式下，Kaspersky Embedded Systems Security 會封鎖連線到表現出典型網路攻擊活動的電腦，並且在某些情況下將此類電腦的 IP 位址新增至已封鎖的網路工作階段清單。

您可以在封鎖的主機儲存中檢視封鎖的主機清單。

重新啟動應用程式以及變更網路威脅防護設定時，Kaspersky Embedded Systems Security 會清除封鎖清單。

您可以透過設定封鎖的主機儲存設定來恢復對封鎖的主機的存取權限，並指定主機在被封鎖多少天、小時和分鐘後可重新獲得對網路檔案資源的存取權限。

在以下情況下，將從封鎖的主機清單中刪除出現典型網路攻擊活動的主機 IP 位址：

- Kaspersky Embedded Systems Security 已移除。
- 手動從封鎖的主機清單中刪除了 IP 位址。
- 主機封鎖期限已到期。
- **封鎖** 模式已關閉。

啟用和配置網路威脅防護

如何在卡巴斯基安全管理中心管理主控台中啟用和配置網路威脅防護

1. 在卡巴斯基安全管理中心管理主控台樹狀目錄中，選取**政策**。
2. 選擇必要的政策並點擊以開啟政策內容。
3. 在政策內容視窗中，轉至「**網路活動控制**」區域。
4. 在"**網路威脅防護**"塊中，點擊"**設定**"按鈕。
5. 在開啟的視窗中，選中"**網路威脅防護**"核取方塊。

6. 在**Operating mode** 部分中選擇工作模式：

   - **封鎖**如果選擇此模式，Kaspersky Embedded Systems Security 會掃描入站網路流量，尋找典型的網路攻擊活動，阻止與顯示此類活動的電腦的連接，並在某些情況下將電腦的 IP 位址新增至已封鎖的網路工作階段清單。應用程式還在元件日誌中記錄有關偵測到的典型網路攻擊活動的事件。

   - **Inform**如果選擇此模式，Kaspersky Embedded Systems Security 會掃描入站網路流量，尋找典型的網路攻擊活動，但不阻止與顯示此類活動的電腦的連線，不會將電腦的 IP 位址新增至已封鎖的網路工作階段清單。該應用程式在元件日誌中記錄有關偵測到的典型網路攻擊活動的事件。

7. 使用"**將連接埠掃描和網路洪水當做攻擊處理**"核取方塊來啟用或停用對相應攻擊的偵測。

8. 如有必要，選中"**Block attacking devices for N 分鐘**"核取方塊。

9. 在"**MAC spoofing protection**"區塊中，選擇或者清除"**Enable protection against MAC spoofing attacks**"核取方塊。

10. 如果有需要，您可以 新增封鎖的排除項目。

11. 儲存變更。

如何在卡巴斯基安全管理中心網頁主控台中啟用和配置網路威脅防護

1. 在網頁主控台的主視窗中，選擇**資產管理 → 政策**。

2. 點擊 Kaspersky Embedded Systems Security 政策的名稱。

   政策內容視窗將開啟。

3. 選擇"**應用程式設定**"標籤。

4. 選擇"**網路活動控制 → 網路威脅防護**"。

5. 在"**一般**"頁簽上，選中"**啟用網路威脅防護**"核取方塊。

6. 選擇工作執行模式：

   - **封鎖**如果選擇此模式，Kaspersky Embedded Systems Security 會掃描入站網路流量，尋找典型的網路攻擊活動，阻止與顯示此類活動的電腦的連接，並在某些情況下將電腦的 IP 位址新增至已封鎖的網路工作階段清單。應用程式還在元件日誌中記錄有關偵測到的典型網路攻擊活動的事件。

   - **通知**如果選擇此模式，Kaspersky Embedded Systems Security 會掃描入站網路流量，尋找典型的網路攻擊活動，但不阻止與顯示此類活動的電腦的連線，不會將電腦的 IP 位址新增至已封鎖的網路工作階段清單。該應用程式在元件日誌中記錄有關偵測到的典型網路攻擊活動的事件。

7. 使用「**將連接埠掃描和網路洪水當做攻擊處理**」核取方塊來啟用或停用對相應攻擊的偵測。

8. 如有必要，選中"**封鎖攻擊裝置 N 分鐘**"核取方塊。

9. 選擇或清除"**啟用防禦 MAC 欺騙攻擊**"核取方塊。

10. 如果有需要，您可以 新增封鎖的排除項目。

11. 儲存變更。

如何在應用程式主控台中啟用和配置網路威脅防護

1. 在應用程式主控台樹狀目錄中，選擇"**即時電腦防護 → 網路威脅防護**"節點。
2. 在結果窗格中點擊"**內容**"連結。
   內容: 網路威脅防護 視窗將開啟。
3. 選擇"**網路威脅防護**"核取方塊。
4. 在**作業模式** 部分中選擇工作模式：
   - **封鎖**如果選擇此模式，Kaspersky Embedded Systems Security 會掃描入站網路流量，尋找典型的網路攻擊活動，阻止與顯示此類活動的電腦的連接，並在某些情況下將電腦的 IP 位址新增至已封鎖的網路工作階段清單。應用程式還在元件日誌中記錄有關偵測到的典型網路攻擊活動的事件。
   - **通知**如果選擇此模式，Kaspersky Embedded Systems Security 會掃描入站網路流量，尋找典型的網路攻擊活動，但不阻止與顯示此類活動的電腦的連線，不會將電腦的 IP 位址新增至已封鎖的網路工作階段清單。該應用程式在元件日誌中記錄有關偵測到的典型網路攻擊活動的事件。
5. 使用"**將連接埠掃描和網路洪水當做攻擊處理**"核取方塊來啟用或停用對相應攻擊的偵測。
6. 如有必要，選中"**封鎖攻擊裝置 N 分鐘**"核取方塊。
7. 在"**MAC spoofing protection**"區塊中，選擇或者清除"**啟用防禦 MAC 欺騙攻擊**"核取方塊。
8. 如果有需要，您可以 新增封鎖的排除項目。
9. 儲存變更。

建立封鎖排除項目

Kaspersky Embedded Systems Security 可以識別網路攻擊並封鎖傳輸大量封包（例如，來自監視攝像機）的不安全網路連線。要使用受信任裝置，您可以將這些裝置的 IP 位址新增到排除項目清單中。您還可以選擇用於通信並允許特定網路活動的協定和連接埠。

Kaspersky Embedded Systems Security 4.0 中新增了選擇排除哪些協定和連接埠的功能。確保應用程式和管理外掛程式已更新至版本 4.0 或更高版本。如果您使用的是早期版本的應用程式或管理插件，Kaspersky Embedded Systems Security 只能依據 IP 位址允許網路活動。

如何在卡巴斯基安全管理中心管理主控台中建立封鎖排除項目

1. 在卡巴斯基安全管理中心管理主控台樹狀目錄中，選取**政策**。
2. 選擇必要的政策並點擊以開啟政策內容。
3. 在政策內容視窗中，轉至「**網路活動控制**」區域。
4. 在"**網路威脅防護**"塊中，點擊"**設定**"按鈕。
   開啟"**網路威脅防護**"視窗。
5. 轉至**排除項目**頁簽。

6. 選擇 **不控制被排除的位址** 核取方塊以防止 Kaspersky Embedded Systems Security 掃描入站網路流量以尋找被排除的 IP 位址。

7. 單擊**"新增"**。

8. 在**排除項目**視窗中，輸入不封鎖網路攻擊的裝置的 IP 位址。

9. 如果需要，選擇協定並指定透過其傳輸資料的連接埠。

10. 點擊**OK**。

11. 對每個新增的排除項目執行步驟 c-f。

12. 儲存變更。

如何在卡巴斯基安全管理中心網頁主控台中建立封鎖排除項目

1. 在網頁主控台的主視窗中，選擇**資產管理 → 政策**。

2. 點擊 Kaspersky Embedded Systems Security 政策的名稱。
   政策內容視窗將開啟。

3. 選擇**"應用程式設定"**標籤。

4. 選擇 **網路活動控制 → 網路威脅防護** 並點擊 **配置** 按鈕。

5. 轉至**排除項目**頁簽。

6. 選擇 **不控制排除的 IP 位址** 核取方塊以防止 Kaspersky Embedded Systems Security 掃描入站網路流量以尋找被排除的 IP 位址。

7. 單擊**"新增"**。

8. 在**新增排除項目**視窗中，輸入不封鎖網路攻擊的裝置的 IP 位址。

9. 如果需要，選擇協定並指定透過其傳輸資料的連接埠。

10. 點擊**OK**。

11. 對每個新增的排除項目執行步驟 c-f。

12. 儲存變更。

如何在應用程式主控台中建立封鎖排除項目

1. 在應用程式主控台樹狀目錄中，選擇**"即時電腦防護 → 網路威脅防護"**節點。

2. 在結果窗格中點擊**"內容"**連結。
   內容: 網路威脅防護 視窗將開啟。

3. 轉至**排除項目**頁簽。

4. 選擇 **不控制被排除的位址** 核取方塊以防止 Kaspersky Embedded Systems Security 掃描入站網路流量以尋找被排除的 IP 位址。

5. 單擊**"新增"**。

6. 在**排除項目**視窗中，輸入不封鎖網路攻擊的裝置的 IP 位址。

7. 如果需要，選擇協定並指定透過其傳輸資料的連接埠。

8. 點擊**OK**。

9. 對每個新增的排除項目執行步驟 c-f。

10. 儲存變更。

匯出和匯入防止共用資料夾被外部加密的排除項目清單

您可以將排除項目清單匯出到 XML 檔案。然後，您可以修改檔案，例如，新增大量相同類型的位址。您還可以使用匯出/匯入功能來備份排除項目清單，或將清單遷移到其他伺服器。

如何在卡巴斯基安全管理中心管理主控台中匯出和匯入排除項目清單

1. 在卡巴斯基安全管理中心管理主控台樹狀目錄中，選取**政策**。

2. 選擇必要的政策並點擊以開啟政策內容。

3. 在政策內容視窗中，轉至「**網路活動控制**」區域。

4. 在"**網路威脅防護**"塊中，點擊"**設定**"按鈕。
   開啟"**網路威脅防護**"視窗。

5. 轉至**排除項目**頁簽。

6. 若要匯出規則清單，請執行下列操作之一：

   - 使用核取方塊，選取您想要匯出的排除項目。按一下箭頭，然後在下拉式清單中選擇 **匯出所選**。
   - 若要匯出所有排除項目，請按一下箭頭，然後在下拉清單中選擇 **匯出**。
     Kaspersky Embedded Systems Security 會在標準下載資料夾中儲存一個名為 networkExclusions.xml 的檔案。

7. 若要匯入排除項目清單：

   a. 點擊箭頭並選擇 **匯入**。

   b. 在開啟的視窗中，選取要從中匯入排除項目清單的 XML 檔案。

   c. 開啟檔案。
      如果電腦已經具有排除項目清單，則 Kaspersky Embedded Systems Security 將提示您刪除現有清單或從 XML 檔案向其中新增新項目。

8. 儲存變更。

如何在網頁主控台中匯出和匯入排除項目清單

1. 在網頁主控台的主視窗中，選擇**資產管理 → 政策**。
2. 點擊 Kaspersky Embedded Systems Security 政策的名稱。
   政策內容視窗將開啟。
3. 選擇**"應用程式設定"**標籤。
4. 轉到**即時電腦防護 → 網路威脅防護** 並點擊 **配置** 按鈕。
5. 在開啟的視窗中選擇**"排除項目"**標籤。
6. 要匯出規則清單：
   a. 如有必要，選取您想要匯出的排除項目。
   b. 點擊 **匯出** 按鈕並選擇匯出模式：匯出整個排除項目清單或僅匯出選定的排除項目。
   c. 單擊**"匯出"**。
      Kaspersky Embedded Systems Security 會在標準下載資料夾中儲存一個名為 networkExclusions.xml 的檔案。
7. 若要匯入排除項目清單：
   a. 點擊**匯入**按鈕並選擇匯入模式：**選擇到現有項目** or **覆寫現有項目**。
   b. 在開啟的視窗中，選取要從中匯入排除項目清單的 XML 檔案。
   c. 開啟檔案。
      Kaspersky Embedded Systems Security 根據所選模式匯入排除項目。
8. 儲存變更。

AMSI 掃描器

當AMSI 掃描程式工作正在執行時，Kaspersky Embedded Systems Security 會控制使用 VBScript 或 JScript 等 Microsoft Windows 指令碼技術 (Active Scripting) 建立的指令碼的執行。應用程式也可以處理 PowerShell 指令碼以及在安裝了 Antimalware Scan Interface (AMSI) 的作業系統上的 Microsoft Office 應用程式中執行的指令碼。

AMSI 允許應用程式和服務與安裝在裝置上的任何反惡意軟體應用程式整合，以便反惡意軟體攔截和掃描所有執行的指令碼。您可以在 Microsoft 網站 上找到有關 AMSI 功能的更多資訊。

在元件設定中，您可以允許或拒絕危險指令碼的執行。如果 Kaspersky Embedded Systems Security 將指令碼識別為危險，這會根據您選擇的動作封鎖或允許執行該指令碼。如果您選擇 **封鎖** 操作，應用程式會封鎖危險指令碼並允許其他指令碼。

Kaspersky Embedded Systems Security 在 Microsoft Windows 10 和 Microsoft Windows Server 2016 及更高版本中支援 AMSI 技術。

啟用和停用 AMSI 掃描程式

如何在卡巴斯基安全管理中心管理主控台中啟用或停用 AMSI 掃描程式

1. 在卡巴斯基安全管理中心管理主控台樹狀目錄中，選取**政策**。
2. 選擇必要的政策並點擊以開啟政策內容。
3. 在政策內容視窗中，轉至「**即時電腦防護**」區域。
4. 在"**AMSI 掃描程式**"塊中，點擊"**設定**"按鈕。
   AMSI 掃描程式視窗將在**一般**頁簽上開啟。
5. 執行以下操作之一：
   - 如果您希望啟用 AMSI 掃描程式，請選中"**AMSI 掃描程式**"核取方塊。
   - 如果您希望停用 AMSI 掃描程式，請清除"**AMSI 掃描程式**"核取方塊。
6. 儲存變更。

如何在 Kaspersky Embedded Systems Security 主控台中啟用 AMSI 掃描程式

1. 在管理主控台樹狀目錄中，選擇**即時電腦防護 → AMSI 掃描程式**資料夾。
2. 在結果窗格中點擊"**內容**"連結。
   AMSI 掃描程式視窗將在**一般**頁簽上開啟。
3. 執行以下操作之一：
   - 如果您希望啟用 AMSI 掃描程式，請選中"**AMSI 掃描程式**"核取方塊。
   - 如果您希望停用 AMSI 掃描程式，請清除"**AMSI 掃描程式**"核取方塊。
4. 在"**AMSI 掃描程式**"塊中，點擊"確定"按鈕。

如何在卡巴斯基安全管理中心網頁主控台中啟用 AMSI 掃描器

1. 在網頁主控台的主視窗中，選擇**資產管理 → 政策**。
2. 點擊 Kaspersky Embedded Systems Security 政策的名稱。
   政策內容視窗將開啟。
3. 選擇"**應用程式設定**"標籤。
4. 選擇 **即時電腦防護** 部分。
5. 在"**AMSI 掃描程式**"塊中，點擊"**配置**"按鈕。
   開啟"**AMSI 掃描程式**"視窗。
6. 執行以下操作之一：
   - 如果您希望啟用 AMSI 掃描程式，請選中"**AMSI 掃描程式**"核取方塊。
   - 如果您希望停用 AMSI 掃描程式，請清除"**AMSI 掃描程式**"核取方塊。
7. 儲存變更。

AMSI 掃描程式設定

如何在卡巴斯基安全管理中心管理主控台中設定 AMSI 掃描程式設定

1. 在卡巴斯基安全管理中心管理主控台樹狀目錄中，選取**政策**。
2. 選擇必要的政策並點擊以開啟政策內容。
3. 在政策內容視窗中，轉至「**即時電腦防護**」區域。
4. 在"**AMSI 掃描程式**"塊中，點擊"**設定**"按鈕。
   AMSI 掃描程式視窗將在**一般**頁簽上開啟。
5. 選擇危險指令碼執行時您希望 Kaspersky Embedded Systems Security 執行的操作：
   - **通知**該應用程式允許執行可能危險的指令碼。對應的事件記錄在工作記錄中。
   - **封鎖**該應用程式會封鎖可能危險的指令碼。
6. 在"**掃描複合檔案**"塊中，指定您希望掃描的複合檔案類型：存檔、分發套件或 Office 格式檔案。
7. 在"**容量限制**"塊中執行以下操作之一：
   - 要封鎖AMSI 掃描程式元件解壓縮大型複合檔案，請選中"**複合檔案大於指定值時不解壓縮**"核取方塊，並在"**最大檔案容量(MB)**"欄位中指定所需值。AMSI 掃描程式元件不會解壓縮大於指定大小的複合檔案。
   - 要允許AMSI 掃描程式元件解壓縮大型複合檔案，請取消選中"**複合檔案大於指定值時不解壓縮**"核取方塊。

無論是否選中**"複合檔案大於指定值時不解壓縮"**核取方塊，AMSI 掃描程式元件均會掃描從存檔中提取的大型檔案。

8. 在"**AMSI 掃描程式**"塊中，點擊"確定"按鈕。
9. 在**屬性：<政策名稱>**視窗中按一下**OK**按鈕。

如何在 Kaspersky Embedded Systems Security 主控台中設定 AMSI 掃描程式設定

1. 在管理主控台樹狀目錄中，選擇**即時電腦防護 → AMSI 掃描程式**資料夾。
2. 在結果窗格中點擊**"內容"**連結。
   AMSI 掃描程式視窗將在**一般**頁簽上開啟。
3. 選擇危險指令碼執行時您希望 Kaspersky Embedded Systems Security 執行的操作：
   - **通知**該應用程式允許執行可能危險的指令碼。對應的事件記錄在工作記錄中。
   - **封鎖**該應用程式會封鎖可能危險的指令碼。
4. 在**"掃描複合檔案"**塊中，指定您希望掃描的複合檔案類型：存檔、分發套件或 Office 格式檔案。
5. 在**"容量限制"**塊中執行以下操作之一：
   - 要封鎖AMSI 掃描程式元件解壓縮大型複合檔案，請選中**"複合檔案大於指定值時不解壓縮"**核取方塊，並在**"最大檔案容量(MB)"**欄位中指定所需值。AMSI 掃描程式元件不會解壓縮大於指定大小的複合檔案。
   - 要允許AMSI 掃描程式元件解壓縮大型複合檔案，請取消選中**"複合檔案大於指定值時不解壓縮"**核取方塊。

無論是否選中**"複合檔案大於指定值時不解壓縮"**核取方塊，AMSI 掃描程式元件均會掃描從存檔中提取的大型檔案。

6. 在"**AMSI 掃描程式**"塊中，點擊"確定"按鈕。

如何在卡巴斯基安全管理中心網頁主控台中設定 AMSI 掃描程式設定

1. 在網頁主控台的主視窗中，選擇**資產管理 → 政策**。
2. 點擊 Kaspersky Embedded Systems Security 政策的名稱。
   政策內容視窗將開啟。
3. 選擇**"應用程式設定"**標籤。
4. 選擇 **即時電腦防護** 部分。
5. 在"**AMSI 掃描程式**"塊中，點擊**"配置"**按鈕。
   開啟**"AMSI 掃描程式"**視窗。

6. 選擇危險指令碼執行時您希望 Kaspersky Embedded Systems Security 執行的操作：

   - **通知**該應用程式允許執行可能危險的指令碼。對應的事件記錄在工作記錄中。
   - **封鎖**該應用程式會封鎖可能危險的指令碼。

7. 在“**掃描複合檔案**”塊中，指定您希望掃描的複合檔案類型：存檔、分發套件或 Office 格式檔案。

8. 在“**容量限制**”塊中執行以下操作之一：

   - 要封鎖AMSI 掃描程式元件解壓縮大型複合檔案，請選中“**複合檔案大於指定值時不解壓縮**”核取方塊，並在“**最大檔案容量(MB)**”欄位中指定所需值。AMSI 掃描程式元件不會解壓縮大於指定大小的複合檔案。
   - 要允許AMSI 掃描程式元件解壓縮大型複合檔案，請取消選中“**複合檔案大於指定值時不解壓縮**”核取方塊。

   無論是否選中“**複合檔案大於指定值時不解壓縮**”核取方塊，AMSI 掃描程式元件均會掃描從存檔中提取的大型檔案。

9. 在**AMSI 掃描程式**視窗中，按一下**確定**按鈕。

10. 在**<政策名稱>**視窗中按一下**儲存**按鈕。

應用程式啟動控制

Kaspersky Embedded Systems Security 的 應用程式啟動控制 元件可保護裝置，防止未經授權啟動應用程式。應用程式啟動控制依賴於"預設拒絕"原則，這意味著元件設定中不允許的任何應用程式都會被自動封鎖。您可以透過為應用程式建立元件允許規則，允許啟動這些應用程式。

如果已盡可能完整地建立應用程式啟動控制規則，Kaspersky Embedded Systems Security 會封鎖所有未經組織區域網路管理員驗證的新應用程式，使其無法啟動，但仍可確保作業系統及使用者履行工作職責所需的已驗證應用程式正常運作。您可以使用 *應用程式啟動控制規則產生器* 工作，取得受防護裝置上已安裝應用程式的相關資訊。

如果已啟用 應用程式啟動控制 元件，Kaspersky Embedded Systems Security 會攔截在受防護裝置上啟動執行檔時，與建立處理程序要求相關的每個作業系統事件。接著，本應用程式會收集正在啟動的執行檔、指令碼或 MSI 套件的相關資訊，並將其與觸發應用程式啟動控制規則的條件進行比較。如果至少一個允許規則的所有條件均符合，Kaspersky Embedded Systems Security 便會允許啟動該應用程式。如果正在啟動的應用程式不符合任何允許規則的條件，或觸發了封鎖規則，Kaspersky Embedded Systems Security 會取消建立處理程序，從而封鎖啟動該應用程式的嘗試。

所有啟動應用程式的嘗試將記錄在元件記錄中。

應用程式啟動控制 元件可以下列兩種模式之一運行：

- **封鎖**Kaspersky Embedded Systems Security 使用應用程式啟動控制規則來控制應用程式的啟動。應用程式啟動控制規則的範圍在應用程式啟動控制元件的一般設定中指定。如果應用程式符合應用程式啟動控制規則，但沒有任何規則與應用程式啟動控制規則的範圍匹配，則此類應用程式將被封鎖執行。

  禁止執行應用程式啟動控制規則未涵蓋的應用程式。

  如果未建立任何應用程式啟動控制規則或為一台受防護裝置建立了超過 65,535 條應用程式啟動控制規則，則"應用程式啟動控制"元件無法在啟動模式下啟動。

- **通知**Kaspersky Embedded Systems Security 允許啟動所有應用程式。僅記錄有關所有應用程式啟動、涵蓋已啟動應用程式的規則、以及如果工作在**封鎖**模式下執行時將執行的操作的資訊。預設設定此模式。

在建立應用程式啟動控制規則時，我們建議確保它們不會阻止作業系統的應用程式執行。

Kaspersky Embedded Systems Security 還會攔截在 Linux 的 Windows 子系統下啟動的處理程序（從 UNIX™ shell 或命令列編譯器執行的指令碼除外）。對於此類別處理程序，應用程式啟動控制元件將套用目前配置定義的操作。*應用程式啟動控制規則產生器*工作會偵測應用程式啟動，並為在 Linux 的 Windows 子系統下執行的應用程式產生相應規則。

關於應用程式啟動控制規則

應用程式啟動控制規則的工作原理

應用程式啟動控制規則的操作基於以下元件：

- 規則類型。

  應用程式啟動控制規則可以允許或拒絕應用程式啟動。相應地，它們被稱為*allowing*或*拒絕*規則。

- 規則使用範圍。

  應用程式啟動控制規則可套用於*可執行檔*、*指令碼*和 *MSI 安裝套件*。

- 規則觸發條件。

  應用程式啟動控制規則可管理至少符合規則設定中指定的一個觸發條件的檔案的啟動。例如，可執行檔使用指定的*數位憑證*簽章，有指定的*SHA256 雜湊*，位於指定的 *路徑*，比對指定的*命令列*參數。您必須新增至少一個規則觸發條件。否則，不會新增應用程式啟動控制規則。

- 規則的排除項目。

  您可以設定應用程式啟動控制規則的排除項目，這可能基於與規則觸發條件相同的條件。對於某些允許規則時，可能需要指定應用程式啟動控制規則的排除：例如，如果您希望允許使用者從 C:\Windows 路徑啟動應用程式，同時封鎖啟動檔案 Regedit.exe。

- 使用者或使用者群組。

  應用程式啟動控制規則可以按指定的使用者或群組控制指定應用程式的啟動。

在建立應用程式啟動控制規則時，我們建議確保新規則不會阻止作業系統的應用程式執行。

管理應用程式啟動控制規則

您可以對應用程式啟動控制規則執行以下操作：

- 手動新增。
- 自動建立和新增規則。
- 刪除。
- 匯入和匯出。
- 篩選規則清單。

關於軟體分發控制

如果您想控制軟體的分發，產生應用程式啟動控制可能會變得更加複雜。例如，您可能希望在受防護的裝置上執行此操作，這些裝置上安裝的軟體會定期自動更新。在這種情況下，必須在每次軟體更新後更新允許規則的清單，以便在應用程式啟動控制元件設定中考慮新建立的檔案。為了簡化軟體分發方案中的啟動控制，可以使用"軟體分發控制"。

軟體分發套件（下文稱為"套件"）表示要在受防護裝置上安裝的一個或者多個應用程式。安裝套件還可能包含更新和單獨命令。

"軟體分發控制"子系統作為附加排除清單實施。安裝套件新增至清單時，就會成為受信任狀態。允許解壓縮受信任套件，並且允許對從受信任套件安裝或更新的應用程式進行自動啟動。擷取的檔案可以繼承主分發套件的受信任內容。*主分發套件*是由使用者新增到軟體分發控制排除清單並成為受信任套件的軟體套件。

如果第一次啟動受信任套件時軟體分發控制關閉，或者應用程式啟動控制元件未安裝，Kaspersky Embedded Systems Security 將僅控制應用程式分發完整週期且無法正確處理由受信任套件修改的檔案的啟動。

若要使用軟體分發控制，您必須啟用應用程式啟動控制元件一般設定中的 **套用規則到可執行檔** 功能。

軟體分發快取

Kaspersky Embedded Systems Security 使用動態產生的軟體分發快取（下文稱為"分發快取"）在受信任套件與軟體分發期間建立的檔案之間建立關係。第一次啟動軟體套件時，Kaspersky Embedded Systems Security 將偵測該軟體套件在軟體分發過程中建立的所有檔案，並將檔案總和檢查碼及路徑儲存在分發快取中。然後，預設情況下，允許啟動所有在分發快取中儲存了資訊的檔案。

您不能透過使用者介面檢視、刪除或手動修改分發快取。快取由 Kaspersky Embedded Systems Security 填充和控制。

您可以將散佈快取匯出至設定檔（XML 格式），或在命令列上刪除散佈快取。

Kaspersky Embedded Systems Security 每 24 小時更新一次分發快取。如果先前允許的檔案的總和檢查碼發生變化，應用程式將從分發快取中刪除此檔案的記錄。如果應用程式啟動控制元件在啟動模式下執行，後續啟動該檔案的嘗試將被封鎖。如果先前允許的檔案的完整路徑發生變化，後續啟動該檔案的嘗試不會被封鎖，因為總和檢查碼儲存在分發快取內。

處理擷取的檔案

在第一次開啟排除清單中的軟體分發套件時，受信任的主分發套件所建立的擷取檔案和套件（在第一層嵌套）會在它們的總和檢查碼被新增到分發快取時繼承受信任內容。因此，分發套件本身和從該分發套件擷取的所有檔案也將被信任。

例如，如果將包含多個套件和應用程式的套件 test.msi 被新增至排除項目清單，並啟用了**允許將所有子檔案作為受信任發佈套件進行啟動**功能，則可以解壓縮並執行 test.msi 套件中包含的所有套件和應用程式，即使這包含其他巢狀檔案也是如此。此方案適用於所有嵌套等級上的擷取檔案。

如果 test.msi 套件被新增到排除項目清單中，並且 **允許將所有子檔案作為受信任發佈套件進行啟動** 功能被停用，應用程式僅將受信任屬性指派給那些直接從受信任封包（在第一層嵌套）中提取的封包和可執行檔。此類檔案的總和檢查碼儲存在分發快取中。在第二個和更後面的嵌套等級上的所有檔案都將被"預設拒絕"原則封鎖。

作業系統重新啟動後，擷取的檔案將保留受信任內容。

若要從所有提取的檔案中刪除繼承屬性，在再次執行受信任的安裝套件之前，您必須刪除分發快取並停用 **允許將所有子檔案作為受信任發佈套件進行啟動**功能。

使用應用程式啟動控制規則清單

軟體分發控制的受信任套件清單是一個排除項目清單，該清單擴大了但未更換應用程式啟動控制規則清單。

拒絕應用程式啟動控制規則具有最高優先順序：受信任套件的解壓縮和新檔案或已修改檔案的啟動將被封鎖（如果這些套件和檔案受應用程式啟動控制拒絕規則影響）。

軟體分發控制排除項適用於受信任套件和這些套件建立或修改的檔案（如果應用程式啟動控制清單中沒有拒絕規則適用於這些套件和檔案）。

關於應用程式啟動控制規則產生器

您可使用卡巴斯基安全管理中心工作和政策立同時為公司網路上的所有受防護裝置和受防護裝置群組建立應用程式啟動控制規則清單。如果公司網路沒有參考電腦，並且您無法基於範本機上安裝的應用程式建立允許規則清單，則建議使用下面列出的方案。

您可以透過應用程式主控台在本機執行*應用程式啟動控制規則產生器*工作，以基於單一受防護裝置上執行的應用程式建立規則清單。

您可以使用以下方式之一在卡巴斯基安全管理中心一側建立應用程式啟動控制規則清單：

- 使用 *應用程式啟動控制規則產生器* 群組工作。

  應用程式啟動控制規則產生器 工作可根據設定，收集受防護裝置上執行的應用程式，以及位於指定範圍內的執行檔和指令碼的相關資訊。工作會根據收集到的資訊，為 應用程式啟動控制 元件產生允許規則清單。

  您可以設定將產生的規則自動匯入 應用程式啟動控制 元件的規則清單，或手動匯入產生的規則。

  當您需要快速建立應用程式啟動控制規則清單時，建議使用此方案。建議僅當允許規則使用範圍包含您知道安全的資料夾和檔案時，才設定*應用程式啟動控制規則產生器*工作的排程啟動。

- 基於卡巴斯基安全管理中心中為應用程式啟動控制元件產生的事件報告，在 *通知* 模式下執行。

  在此方案下，Kaspersky Embedded Systems Security 不拒絕應用程式啟動。相反，當應用程式啟動控制元件在"*通知*"模式下執行時，它會在卡巴斯基安全管理中心中的管理伺服器節點的工作區的**事件**頁簽中報告所有網路受防護裝置中所有已允許和已拒絕的應用程式啟動。卡巴斯基安全管理中心使用報告來建立一個拒絕了應用程式啟動的事件清單。

在元件執行時，必須執行受防護裝置和受防護裝置群組的所有可能場景，包括至少重新啟動一次受防護裝置。然後您可從儲存的卡巴斯基安全管理中心事件報告（TXT 格式）匯入應用程式啟動資料，並基於此資料為此類應用程式建立應用程式啟動控制允許規則。

如果公司網路包含大量不同類型的受防護裝置（安裝了不同的軟體），則建議使用此方案。

- 根據透過卡巴斯基安全管理中心接收到的拒絕應用程式啟動事件，無需建立和匯入設定檔。

  要使用此功能，必須在有效的卡巴斯基安全管理中心政策下執行受防護裝置上的應用程式啟動控制元件。在本例中，受防護裝置上的所有事件均被傳送到管理伺服器。

建議當網路受防護裝置上安裝的應用程式集合變更時（例如，安裝更新或重新安裝作業系統時）更新規則清單。建議在測試管理群組的受防護裝置上執行 *應用程式啟動控制規則產生器* 工作，或以 *通知* 模式執行 應用程式啟動控制 元件，以產生更新的規則清單。測試管理群組包含在網路受防護裝置上安裝新的應用程式之前對這些應用程式的啟動進行測試所需的受防護裝置。

包含允許規則清單的 XML 檔案基於在受防護裝置上啟動的應用程式分析建立。為了在產生規則清單時將網路上使用的所有應用程式納入考量，建議在範本機器上啟動 *應用程式啟動控制規則產生器* 工作，並以 *通知* 模式啟動 應用程式啟動控制 元件。

在基於參考電腦上啟動的應用程式建立允許規則之前，確保範本機是安全的，並且不包含任何惡意軟體。

新增允許規則之前，請選擇其中一個可用的規則套用模式。卡巴斯基安全管理中心政策規則清單將僅顯示由政策指定的那些規則，與規則應用模式無關。本機規則清單包括所有已套用的規則 — 本機規則和透過政策新增的規則。

啟用和配置應用程式啟動控制

如何在卡巴斯基安全管理中心管理主控台中啟用和配置應用程式啟動控制的一般設定

1. 在卡巴斯基安全管理中心管理主控台樹狀目錄中，選取**政策**。
2. 選擇必要的政策並點擊以開啟政策內容。
3. 在政策內容視窗中，轉至「**本機活動控制**」區域。
4. 在"**應用程式啟動控制**"塊中，點擊"**設定**"按鈕。

   應用程式啟動控制視窗將在**一般**頁簽上開啟。
5. 選擇"**應用程式啟動控制**"核取方塊。
6. 在"**用於封鎖規則的操作模式**"塊中，選擇元件操作模式：

   - **封鎖**Kaspersky Embedded Systems Security 套用所有建立的應用程式啟動控制規則。
   - **通知**Kaspersky Embedded Systems Security 不使用應用程式啟動控制規則。這僅在元件記錄中記錄有關應用程式啟動的資訊。所有應用程式均允許啟動。您可以使用此模式根據元件記錄中記錄的有關拒絕的應用程式啟動的資訊應用程式啟動控制規則產生器清單。

7. 配置元件設定（參見下表）。

8. 儲存變更。

Kaspersky Embedded Systems Security 會立即套用新的元件設定。有關設定修改日期和時間以及修改前後設定值的資訊儲存在系統稽核記錄中。

如何在 Kaspersky Embedded Systems Security 主控台中啟用和配置應用程式啟動控制的一般設定

1. 在管理主控台樹狀目錄中，選擇**電腦控制 → 應用程式啟動控制**資料夾。

2. 在結果窗格中點擊**"內容"**連結。

   應用程式啟動控制視窗將在**一般**頁簽上開啟。

3. 選擇**"應用程式啟動控制"**核取方塊。

4. 在**"用於封鎖規則的操作模式"**塊中，選擇元件操作模式：

   - **封鎖**Kaspersky Embedded Systems Security 套用所有建立的應用程式啟動控制規則。

   - **通知**Kaspersky Embedded Systems Security 不使用應用程式啟動控制規則。這僅在元件記錄中記錄有關應用程式啟動的資訊。所有應用程式均允許啟動。您可以使用此模式根據元件記錄中記錄的有關拒絕的應用程式啟動的資訊應用程式啟動控制規則產生器清單。

5. 配置元件設定（參見下表）。

6. 儲存變更。

Kaspersky Embedded Systems Security 會立即套用新的元件設定。有關設定修改日期和時間以及修改前後設定值的資訊儲存在系統稽核記錄中。

如何在卡巴斯基安全管理中心網頁主控台中啟用和配置應用程式啟動控制的一般設定

1. 在網頁主控台的主視窗中，選擇**資產管理 → 政策**。

2. 點擊 Kaspersky Embedded Systems Security 政策的名稱。

   政策內容視窗將開啟。

3. 選擇**"應用程式設定"**標籤。

4. 選擇 **本機活動控制** 部分。

5. 在**"應用程式啟動控制"**塊中，點擊**"配置"**按鈕。

   應用程式啟動控制視窗將在**一般**頁簽上開啟。

6. 選擇**"啟用應用程式啟動控制"**核取方塊。

7. 在**"用於封鎖規則的操作模式"**塊中，選擇元件操作模式：

   - **封鎖**Kaspersky Embedded Systems Security 套用所有建立的應用程式啟動控制規則。

   - **通知**Kaspersky Embedded Systems Security 不使用應用程式啟動控制規則。這僅在元件記錄中記錄有關應用程式啟動的資訊。所有應用程式均允許啟動。您可以使用此模式根據元件記錄中記錄的有關拒絕的應用程式啟動的資訊應用程式啟動控制規則產生器清單。

8. 配置元件設定（參見下表）。

9. 儲存變更。

Kaspersky Embedded Systems Security 會立即套用新的元件設定。有關設定修改日期和時間以及修改前後設定值的資訊儲存在系統稽核記錄中。

"應用程式啟動控制"一般設定

參數	描述
對該檔案的所有隨後啟動重複為首次檔案啟動採取的操作	此選項可啟用或停用根據快取中儲存的事件資訊對第二次和後續應用程式啟動嘗試的啟動控制。 如果啟用此選項，Kaspersky Embedded Systems Security 將根據元件針對應用程式第一次啟動的結論允許或拒絕應用程式的後續啟動。例如，如果規則允許了第一次應用程式啟動，則有關此操作的資訊將儲存在快取中，第二次和所有後續啟動也將被允許，而不進行重複檢查。 如果應用程式安裝在執行 Windows XP 的電腦上，則透過 Explorer 處理檔案時，第一個應用程式啟動結論可能會被覆寫，導致該功能無法正常運作。 如果停用此選項，Kaspersky Embedded Systems Security 會在每次嘗試啟動應用程式時進行分析該應用程式。
拒絕沒有指令可執行的指令解釋器啟動	如果啟用此功能，當滿足下列任一條件時，Kaspersky Embedded Systems Security 將拒絕啟動命令列解釋器： • 命令列解釋器的啟動被應用程式啟動控制規則拒絕。 • 命令列解釋器啟動時不帶任何參數。 如果停用此選項，Kaspersky Embedded Systems Security 在啟動命令列編譯器時只考慮允許規則。如果應用程式啟動控制允許規則均不適用，則啟動將被封鎖。如果套用了應用程式啟動控制允許規則，則無論是否有要執行的指令，都可以啟動命令列編譯器。 Kaspersky Embedded Systems Security 可控制以下命令編譯器的啟動： • cmd.exe • powershell.exe • python.exe • perl.exe • wscript.exe 預設情況下，該功能處於停用狀態。
套用規則到可執行檔	該選項用於啟用或停用可執行檔的啟動控制。 如果啟用此功能，Kaspersky Embedded Systems Security 將允許或拒絕使用應用程式啟動控制規則啟動可執行檔。 如果停用此功能，Kaspersky Embedded Systems Security 不會使用應用程式啟動控制規則控制可執行檔的啟動。將允許可執行檔啟動。 預設啟用該選項。
控制 DLL 模組負載	控制 DLL 模組的載入可能影響作業系統的效能。 如果**套用規則到可執行檔** 功能已啟用，則此功能可用 。 此功能可啟用或停用 DLL 模組載入的控制。 如果啟用此功能，Kaspersky Embedded Systems Security 將允許或拒絕使用應用程式啟動控制規則載入 DLL 模組。 如果停用此功能，Kaspersky Embedded Systems Security 不會使用應用程式啟動控制規則控制 DLL 模組的載入。將允許 DLL 模組載入。 預設情況下，該功能處於停用狀態。
套用規則到指令碼和 MSI 套件	此選項用於啟用或停用指令碼和 MSI 套件的啟動。 如果啟用此功能，Kaspersky Embedded Systems Security 將允許或拒絕使用應用程式啟動控制規則啟動指令碼和 MSI 套件。 如果清除該核取方塊，Kaspersky Embedded Systems Security 將不會使用應用程式啟動控制規則控制 MSI 指令碼和套件的啟動。將允許指令碼和 MSI 資料套件的啟動。 預設啟用該選項。
驗證憑證式忽略缺失的簽章時間戳	如果啟用此功能，Kaspersky Embedded Systems Security 將允許啟動使用已過期或未定義過期日期的憑證簽署的應用程式。 如果停用此功能，Kaspersky Embedded Systems Security 將拒絕啟動使用已過期或未定義過期日期的憑證簽署的應用程式。 預設情況下，該功能處於停用狀態。

配置軟體分發控制

如何在卡巴斯基安全管理中心管理主控台中設定軟體分發控制

1. 在卡巴斯基安全管理中心管理主控台樹狀目錄中，選取**政策**。
2. 選擇必要的政策並點擊以開啟政策內容。
3. 在政策內容視窗中，轉至「**本機活動控制**」區域。
4. 在"**應用程式啟動控制**"塊中，點擊"**設定**"按鈕。
   應用程式啟動控制視窗將在**一般**頁簽上開啟。
5. 選擇"**軟體分發控制**"標籤。
6. 啟用 **自動允許透過所列的應用程式和套件發佈軟體** 功能。此功能會自動為使用清單中指定的可執行檔和安裝套件啟動的所有檔案建立排除項目。

   如果在**一般**頁簽上啟用了**套用規則到可執行檔**功能，則可以啟用**自動允許透過所列的應用程式和套件發佈軟體**功能。
7. 如有必要，請停用 **總是允許透過 Windows Installer 進行軟體發佈** 功能。此功能會自動為使用 Windows Installer 啟動的所有檔案建立排除項目。

   關閉此功能可能導致更新作業系統檔案出問題，還可能封鎖從分發套件擷取的檔案啟動。
8. 如有必要，啟用 **總是允許使用背景智慧型傳送服務透過 SCCM 進行軟體發佈** 功能。此功能可使用 System Center Configuration Manager 解決方案散佈軟體。
   如果啟用此功能，則 Kaspersky Embedded Systems Security 允許使用 System Center Configuration Manager 進行 Microsoft Windows 佈署。本應用程式僅允許透過 Background Intelligent Transfer Service 散佈軟體。應用程式可控制具有 EXE 和 .MSI 副檔名的可執行檔的啟動。

   應用程式控制受防護裝置上從套裝軟體傳送到安裝或更新的軟體分發週期。如果在受防護裝置上安裝 Kaspersky Embedded Systems Security 之前已執行分發的任何階段，則應用程式不會控制過程。
9. 新增您想要允許啟動的可執行檔和安裝套件：
   - **手動新增一項**
     a. 在**新增**按鈕的內容功能表中，選取"**新增一個分發套件**"。
     b. 在開啟的視窗中，點擊"**瀏覽**"按鈕。
     c. 選擇可執行檔或分發套件。
     信任條件下面的欄位被自動填入有關所選檔案的資訊。
     d. 如有必要，啟用 **允許將所有子檔案作為受信任發佈套件進行啟動** 功能。

e. 選擇決定可執行檔或安裝套件是否可信的標準：**憑證詳細資訊** 或者 **SHA256 雜湊**。

f. 點擊**OK**。

可執行檔或安裝套件將被新增至清單中。

- **按雜湊新增多個**

a. 在**新增**按鈕的內容功能表中，選取**"依照雜湊新增多個套件"**。

b. 這將開啟一個視窗；在該視窗中，選擇任意數量的檔案或安裝套件。

c. 點擊**開啟**。

可執行檔或安裝套件將被新增至清單中。SHA256 雜湊在其屬性中指定。

- **從檔案匯入**

a. 單擊**"匯入"**。

b. 在開啟的視窗中，選擇一個包含有關可執行檔和安裝套件的資訊的.TXT 檔案。

c. 點擊**開啟**。

可執行檔或安裝套件將被新增至清單中。SHA256 雜湊在其屬性中指定。

如果您根據可執行檔建立受信任分發套件，並且根據相同的可執行檔在信任區域設定中新增了處理程序，並使其受到應用程式啟動控制元件的信任，則信任區域設定具有更高的優先順序。Kaspersky Embedded Systems Security 阻止此可執行檔啟動，但認為可以信任該可執行檔的程序。

10. 如有必要，透過按一下**編輯**按鈕來編輯已新增的可執行檔和安裝套件的清單。

11. 如有必要，透過按一下**刪除**按鈕來移除已新增的可執行檔和安裝套件。在這種情況下，允許執行解壓縮的可執行檔。

若要阻止執行解壓縮的可執行檔，您必須從受防護裝置中刪除 Kaspersky Embedded Systems Security 或為解壓縮的檔案建立應用程式啟動控制拒絕規則。

12. 單擊**"確定"**。

如何在 Kaspersky Embedded Systems Security 主控台中設定軟體分發控制

1. 在管理主控台樹狀目錄中，選擇**電腦控制 → 應用程式啟動控制**資料夾。

2. 在結果窗格中點擊**"內容"**連結。

應用程式啟動控制視窗將在**一般**頁簽上開啟。

3. 選擇**"軟體分發控制"**標籤。

4. 啟用 **自動允許透過所列的應用程式和套件發佈軟體** 功能。此功能會自動為使用清單中指定的可執行檔和安裝套件啟動的所有檔案建立排除項目。

   如果在**一般**頁簽上啟用了**套用規則到可執行檔**功能，則可以啟用**自動允許透過所列的應用程式和套件發佈軟體**功能。

5. 如有必要，請停用 **總是允許透過 Windows Installer 進行軟體發佈** 功能。此功能會自動為使用 Windows Installer 啟動的所有檔案建立排除項目。

   關閉此功能可能導致更新作業系統檔案出問題，還可能封鎖從分發套件擷取的檔案啟動。

6. 如有必要，啟用 **總是允許使用背景智慧型傳送服務透過 SCCM 進行軟體發佈** 功能。此功能可使用 System Center Configuration Manager 解決方案散佈軟體。

   如果啟用此功能，則 Kaspersky Embedded Systems Security 允許使用 System Center Configuration Manager 進行 Microsoft Windows 佈署。本應用程式僅允許透過 Background Intelligent Transfer Service 散佈軟體。應用程式可控制具有 EXE 和 .MSI 副檔名的可執行檔的啟動。

   應用程式控制受防護裝置上從套裝軟體傳送到安裝或更新的軟體分發週期。如果在受防護裝置上安裝 Kaspersky Embedded Systems Security 之前已執行分發的任何階段，則應用程式不會控制過程。

7. 新增您想要允許啟動的可執行檔和安裝套件：

   - **手動新增一項**

     a. 在**新增**按鈕的內容功能表中，選取"**新增一個分發套件**"。

     b. 在開啟的視窗中，點擊"**瀏覽**"按鈕。

     c. 選擇可執行檔或分發套件。

     信任條件下面的欄位被自動填入有關所選檔案的資訊。

     d. 如有必要，啟用 **允許將所有子檔案作為受信任發佈套件進行啟動** 功能。

     e. 選擇決定可執行檔或安裝套件是否可信的標準：**憑證詳細資訊** 或者 **SHA256 雜湊**。

     f. 點擊**OK**。

     可執行檔或安裝套件將被新增至清單中。

   - **按雜湊新增多個**

     a. 在**新增**按鈕的內容功能表中，選取"**依照雜湊新增多個套件**"。

     b. 這將開啟一個視窗；在該視窗中，選擇任意數量的檔案或安裝套件。

     c. 點擊**開啟**。

     可執行檔或安裝套件將被新增至清單中。SHA256 雜湊在其屬性中指定。

- **從檔案匯入**

  a. 單擊**"匯入"**。

  b. 在開啟的視窗中，選擇一個包含有關可執行檔和安裝套件的資訊的.TXT 檔案。

  c. 點擊**開啟**。

  可執行檔或安裝套件將被新增至清單中。SHA256 雜湊在其屬性中指定。

如果您根據可執行檔建立受信任分發套件，並且根據相同的可執行檔在信任區域設定中新增了處理程序，並使其受到應用程式啟動控制元件的信任，則信任區域設定具有更高的優先順序。Kaspersky Embedded Systems Security 阻止此可執行檔啟動，但認為可以信任該可執行檔的程序。

8. 如有必要，透過按一下**編輯**按鈕來編輯已新增的可執行檔和安裝套件的清單。
9. 如有必要，透過按一下**刪除**按鈕來移除已新增的可執行檔和安裝套件。在這種情況下，允許執行解壓縮的可執行檔。

若要阻止執行解壓縮的可執行檔，您必須從受防護裝置中刪除 Kaspersky Embedded Systems Security 或為解壓縮的檔案建立應用程式啟動控制拒絕規則。

10. 單擊**"確定"**。

如何在卡巴斯基安全管理中心網頁主控台中設定軟體分發控制

1. 在網頁主控台的主視窗中，選擇**資產管理 → 政策**。
2. 點擊 Kaspersky Embedded Systems Security 政策的名稱。

   政策內容視窗將開啟。
3. 選擇**"應用程式設定"**標籤。
4. 選擇 **本機活動控制** 部分。
5. 在**"應用程式啟動控制"**塊中，點擊**"配置"**按鈕。

   應用程式啟動控制視窗將在**一般**頁簽上開啟。
6. 選擇**"軟體分發控制"**標籤。
7. 啟用 **自動允許透過所列應用程式和資料套件分發軟體** 功能。此功能會自動為使用清單中指定的可執行檔和安裝套件啟動的所有檔案建立排除項目。

如果在**一般**頁簽上啟用了**將規則套用於可執行檔**功能，則可以啟用**自動允許透過所列應用程式和資料套件分發軟體**功能。

8. 如有必要，請停用 **始終允許透過 Windows Installer 進行軟體分發** 功能。此功能會自動為使用 Windows Installer 啟動的所有檔案建立排除項目。

   關閉此功能可能導致更新作業系統檔案出問題，還可能封鎖從分發套件擷取的檔案啟動。

9. 如有必要，啟用 **始終允許使用背景智慧傳輸服務透過 SCCM 進行軟體分發** 功能。此功能可使用 System Center Configuration Manager 解決方案散佈軟體。

   如果啟用此功能，則 Kaspersky Embedded Systems Security 允許使用 System Center Configuration Manager 進行 Microsoft Windows 佈署。本應用程式僅允許透過 Background Intelligent Transfer Service 散佈軟體。應用程式可控制具有 EXE 和 .MSI 副檔名的可執行檔的啟動。

   應用程式控制受防護裝置上從套裝軟體傳送到安裝或更新的軟體分發週期。如果在受防護裝置上安裝 Kaspersky Embedded Systems Security 之前已執行分發的任何階段，則應用程式不會控制過程。

10. 新增您想要允許啟動的可執行檔和安裝套件：

    - **手動**

      a. 點擊**"新增"**按鈕。

      b. 在「**信任條件**」下：選取決定可執行檔或安裝套件是否可信的標準：「**使用數位憑證**」或者「**使用 SHA256 雜湊**」。

      c. 如果您選擇了**使用數位憑證**，請輸入用於簽署可執行檔或安裝套件的憑證的標頭和指紋，以及可執行檔或安裝套件的名稱。

      d. 如果選取「**使用 SHA256 雜湊**」，請點擊「**瀏覽**」來選取可執行檔或安裝套件。

      e. 如有必要，啟用 **允許啟動所有受信任分發套件形式的子檔案** 功能。

      f. 點擊**OK**。

      可執行檔或安裝套件將被新增至清單中。

    - **從檔案匯入**

      a. 單擊**"匯入"**。

      b. 在開啟的視窗中，選擇一個包含有關可執行檔和安裝套件的資訊的.TXT 檔案。

      c. 點擊**"開啟"**按鈕。

      可執行檔或安裝套件將被新增至清單中。SHA256 雜湊在其屬性中指定。

    如果您根據可執行檔建立受信任分發套件，並且根據相同的可執行檔在信任區域設定中新增了處理程序，並使其受到應用程式啟動控制元件的信任，則信任區域設定具有更高的優先順序。Kaspersky Embedded Systems Security 阻止此可執行檔啟動，但認為可以信任該可執行檔的程序。

11. 如有必要，透過按一下**編輯**按鈕來編輯已新增的可執行檔和安裝套件的清單。

12. 如有必要，透過按一下**刪除**按鈕來移除已新增的可執行檔和安裝套件。在這種情況下，允許執行解壓縮的可執行檔。

    若要阻止執行解壓縮的可執行檔，您必須從受防護裝置中刪除 Kaspersky Embedded Systems Security 或為解壓縮的檔案建立應用程式啟動控制拒絕規則。

13. 單擊**"確定"**。

14. 在**應用程式啟動控制**視窗中，按一下**確定**按鈕。

使用應用程式啟動控制規則

本節提供有關建立應用程式啟動控制規則清單的說明。

新增應用程式啟動控制規則

如何在卡巴斯基安全管理中心管理主控台中新增應用程式啟動控制規則

1. 在卡巴斯基安全管理中心管理主控台樹狀目錄中，選取**政策**。

2. 選擇必要的政策並點擊以開啟政策內容。

3. 在政策內容視窗中，轉至「**本機活動控制**」區域。

4. 在"**應用程式啟動控制**"塊中，點擊"**設定**"按鈕。

   應用程式啟動控制視窗將在**一般**頁簽上開啟。

5. 選擇**"規則"**標籤。

6. 在**"規則使用"**下拉式清單中，選取規則應用程式模式：

   - **新增政策規則到本機規則**應用程式將與本機規則清單一起套用政策中指定的規則清單。
   - **用政策規則替代本機規則**應用程式將針對受防護裝置群組上的應用程式啟動控制套用政策中指定的規則清單。不能建立、編輯或套用本機規則清單。

7. 如有必要，啟用 **拒絕使用者修改本機規則** 功能。

   如果啟用此功能，應用程式不允許在應用程式主控台中本機編輯應用程式啟動控制規則。預設情況下，該功能處於停用狀態。

8. 透過以下方式之一新增應用程式啟動控制規則：

   - **手動**

     a. 單擊**"新增"**。

        開啟**"應用程式啟動控制"**視窗。

     b. 在**"名稱"**欄位中輸入規則的名稱。

c. 如有必要，在"**敘述**"欄位中輸入規則的描述。

d. 在"**類型**"下拉式清單中，選取規則類型：

- **允許** 如果您希望規則允許執行規則描述的應用程式。
- **拒絕** 如果您希望規則封鎖該規則所描述的應用程式的啟動。

e. 在"**範圍**"下拉清單中，選擇將由規則控制執行的檔案類型：

- **可執行檔**，如果您希望規則控制可執行檔的啟動。
- **指令碼和 MSI 套件**，如果希望規則控制指令碼和 MSI 資料套件的啟動。以下副檔名的檔案受支援：.js、.vbs、.cmd、.bat、.py、.ps1、.pl、.msi、.msp、.mst、.com、.vbe、.jse、.psd1、.psm1、.pyc

f. 如果您想要 Kaspersky Embedded Systems Security 將符合規則觸發條件的應用程式視為受信任的更新程式，請選擇"**信任的更新程式**"核取方塊。信任的更新程式是被允許建立其它可執行檔的應用程式，這些可執行檔將被允許隨後執行。

如果一個應用程式觸發了多個規則，Kaspersky Embedded Systems Security 將在滿足以下條件的情況下設定"*信任的更新程式*"旗標：

- 所有規則允許應用程式執行。
- 至少一個規則選擇了"**信任的更新程式**"核取方塊。

g. 為應用程式啟動控制規則新增觸發條件。

h. 為應用程式啟動控制規則新增觸發條件排除項目。

i. 新增被允許或禁止啟動滿足規則的應用程式的使用者和/或使用者群組。

j. 點擊**OK**。

- **透過匯入包含應用程式啟動控制規則的 XML 檔案**

a. 在 按鈕的內容功能表中，選取在"**匯入 → 自 XML 檔案**"項目。

b. 選擇如何將裝置控制規則從 XML 檔案新增至政策中可用的項目：

- **替代現有規則**，如果您希望將現有規則取代為匯入的規則。
- **新增至現有規則**，如果您希望將匯入的規則新增到現有規則清單。將複製具有相同設定的規則。
- **與現有規則合併**，如果您希望將匯入的規則新增到現有規則清單。不會複製具有相同設定的規則。如果有至少一項規則設定是唯一性質，則新增該規則。

c. 在開啟的視窗中，指定在完成*應用程式啟動控制規則產生器*的本機工作或群組工作後建立的 XML 檔案的路徑。

d. 單擊"**開啟**"。

- **基於使用請求的卡巴斯基安全管理中心事件**

  a. 在 按鈕的內容功能表中，選取在"**匯入 → 建立基於卡巴斯基安全管理中心事件（請求）的允許規則**"項目。

  b. 選擇將規則新增到先前建立的應用程式啟動控制規則清單中的政策：

  - **新增至現有規則**，如果您希望將匯入的規則新增到現有規則清單。將複製具有相同設定的規則。
  - **替代現有規則**，如果您希望將現有規則取代為匯入的規則。
  - **與現有規則合併**，如果您希望將匯入的規則新增到現有規則清單。不新增具有相同設定的規則；如果至少一個規則參數是唯一的，則會新增規則。

  開啟"**應用程式啟動控制規則產生**"視窗。

  c. 選擇應用程式將據此建立應用程式啟動控制規則的事件類型：

  - **應用程式啟動被拒絕**
  - **僅統計模式：應用程式啟動被拒絕**

  d. 從**期間內產生的請求事件**下拉式清單中選擇一個時間段。

  e. 清除或選中"**優先排序產生規則時的雜湊使用**"核取方塊。

  如果選中此核取方塊，則當檔案的核對總和與憑證均可用時，Kaspersky Embedded Systems Security 將使用檔案的核對總和來產生規則。

  如果清除此核取方塊，則當檔案的核對總和與憑證均可用時，Kaspersky Embedded Systems Security 將使用檔案的數位憑證來產生規則。

  f. 單擊"**產生規則**"。

  g. 單擊"**確定**"。

- **透過匯入包含選定的卡巴斯基安全管理中心封鎖的應用程式事件的 TXT 檔案**

  1. 在卡巴斯基安全管理中心管理主控台樹狀目錄中，選取**政策**。
  2. 選擇必要的政策並點擊以開啟政策內容。
  3. 在政策內容視窗中，轉至「**記錄和通知**」區域。
  4. 在"**工作記錄**"塊中，點擊"**設定**"按鈕。
     開啟"**通知**"視窗。
  5. 展開 **本機活動控制** 節點。
  6. 選擇 **應用程式啟動控制** 部分。
  7. 在應用程式啟動控制事件清單中的**將事件傳送到卡巴斯基安全管理中心**列中，選取*已禁止應用程式啟動*和 *禁止應用程式在測試模式下啟動*旁邊的核取方塊。
  8. 儲存變更。

9. 在政策的**事件組態**部分，確保在**儲存在管理伺服器資料庫中（天）**欄位中指定的事件儲存持續時間大於您計劃收集的關於被防止的應用程式啟動的資訊的時間段（預設值為 30 天）。

   一旦應用程式啟動控制元件記錄保留期限到期，將會刪除記錄的事件，而且不會出現在報告中。

10. 啟動為收集有關被拒絕的應用程式啟動的資料而設定的政策。

11. 如有需要，修改應用程式啟動控制元件作業模式。

12. 當收集有關被封鎖的應用程式啟動的資訊的期限到期時，請從 *已禁止應用程式啟動* 和 *禁止應用程式在測試模式下啟動* 事件進行選擇並將其匯出到 TXT 檔案。詳情請參閱卡巴斯基安全管理中心說明中的“事件選擇”部分 。

13. 開啟匯出的 TXT 檔案。

14. 如有必要，編輯事件清單。

新增的應用程式啟動控制規則顯示在清單中。

9. 如有必要，請執行步驟 5 新增更多應用程式啟動控制規則。

10. 如有必要，透過點擊 **編輯**按鈕編輯新增的應用程式啟動控制規則。

11. 如有必要，透過點擊**刪除**按鈕刪除新增的應用程式啟動控制規則。

12. 單擊“**確定**”。

如何在 Kaspersky Embedded Systems Security 主控台中新增應用程式啟動控制規則

1. 在管理主控台樹狀目錄中，選擇**電腦控制 → 應用程式啟動控制**資料夾。

2. 在結果窗格中點擊“**內容**”連結。
   應用程式啟動控制視窗將在**一般**頁簽上開啟。

3. 選擇“**規則**”標籤。

4. 透過以下方式之一新增應用程式啟動控制規則：

   - **手動**

     a. 單擊“**新增**”。
     開啟“**應用程式啟動控制**”視窗。

     b. 在“**名稱**”欄位中輸入規則的名稱。

     c. 如有必要，在”**敘述**”欄位中輸入規則的描述。

     d. 在“**類型**”下拉式清單中，選取規則類型：

     - **允許** 如果您希望規則允許執行規則描述的應用程式。
     - **拒絕** 如果您希望規則封鎖該規則所描述的應用程式的啟動。

e. 在"**範圍**"下拉清單中，選擇將由規則控制執行的檔案類型：

- **可執行檔**，如果您希望規則控制可執行檔的啟動。
- **指令碼和 MSI 套件**，如果希望規則控制指令碼和 MSI 資料套件的啟動。以下副檔名的檔案受支援：.js、.vbs、.cmd、.bat、.py、.ps1、.pl、.msi、.msp、.mst、.com、.vbe、.jse、.psd1、.psm1、.pyc

f. 如果您想要 Kaspersky Embedded Systems Security 將符合規則觸發條件的應用程式視為受信任的更新程式，請選擇"**信任的更新程式**"核取方塊。信任的更新程式是被允許建立其它可執行檔的應用程式，這些可執行檔將被允許隨後執行。

如果一個應用程式觸發了多個規則，Kaspersky Embedded Systems Security 將在滿足以下條件的情況下設定"*信任的更新程式*"旗標：

- 所有規則允許應用程式執行。
- 至少一個規則選擇了"**信任的更新程式**"核取方塊。

g. 為應用程式啟動控制規則新增觸發條件。

h. 為應用程式啟動控制規則新增觸發條件排除項目。

i. 新增被允許或禁止啟動滿足規則的應用程式的使用者和/或使用者群組。

j. 點擊**OK**。

- **透過匯入包含應用程式啟動控制規則的 XML 檔案**

a. 在 按鈕的內容功能表中，選取在"**匯入 → 自 XML 檔案**"項目。

b. 選擇如何將裝置控制規則從 XML 檔案新增至政策中可用的項目：

- **替代現有規則**，如果您希望將現有規則取代為匯入的規則。
- **新增至現有規則**，如果您希望將匯入的規則新增到現有規則清單。將複製具有相同設定的規則。
- **與現有規則合併**，如果您希望將匯入的規則新增到現有規則清單。不會複製具有相同設定的規則。如果有至少一項規則設定是唯一性質，則新增該規則。

c. 在開啟的視窗中，指定在完成*應用程式啟動控制規則產生器*的本機工作或群組工作後建立的 XML 檔案的路徑。

d. 單擊"**開啟**"。

新增的應用程式啟動控制規則顯示在清單中。

5. 如有必要，請執行步驟 5 新增更多應用程式啟動控制規則。
6. 如有必要，透過點擊 **編輯**按鈕編輯新增的應用程式啟動控制規則。
7. 如有必要，透過點擊**刪除**按鈕刪除新增的應用程式啟動控制規則。
8. 單擊"**確定**"。

如何在卡巴斯基安全管理中心網頁主控台中新增應用程式啟動控制規則

1. 在網頁主控台的主視窗中，選擇**資產管理 → 政策**。
2. 點擊 Kaspersky Embedded Systems Security 政策的名稱。
   政策內容視窗將開啟。
3. 選擇**"應用程式設定"**標籤。
4. 選擇 **本機活動控制** 部分。
5. 在**"應用程式啟動控制"**塊中，點擊**"配置"**按鈕。
   應用程式啟動控制視窗將在**一般**頁簽上開啟。
6. 選擇**"規則"**標籤。
7. 在**"套用規則"**下拉式清單中，選取規則應用程式模式：
   - **將政策規則新增到本機規則**應用程式將與本機規則清單一起套用政策中指定的規則清單。
   - **使用政策規則取代本機規則**應用程式將針對受防護裝置群組上的應用程式啟動控制套用政策中指定的規則清單。不能建立、編輯或套用本機規則清單。
8. 如有必要，啟用 **拒絕使用者修改本機規則** 功能。
   如果啟用此功能，應用程式不允許在應用程式主控台中本機編輯應用程式啟動控制規則。預設情況下，該功能處於停用狀態。
9. 透過以下方式之一新增應用程式啟動控制規則：
   - **手動**
     a. 單擊**"新增"**。
        開啟**"規則設定"**視窗。
     b. 在**"名稱"**欄位中輸入規則的名稱。
     c. 在**"類型"**下拉式清單中，選取規則類型：
        - **允許** 如果您希望規則允許執行規則描述的應用程式。
        - **拒絕** 如果您希望規則封鎖該規則所描述的應用程式的啟動。
     d. 在**"範圍"**下拉清單中，選擇將由規則控制執行的檔案類型：
        - **可執行檔**，如果您希望規則控制可執行檔的啟動。
        - **指令碼和 MSI 資料套件**，如果希望規則控制指令碼和 MSI 資料套件的啟動。
     e. 如果您希望應用程式封鎖啟動未在 **使用者或群組** 頁簽上列出的所有使用者規則所描述的應用程式，請選取**拒絕其他使用者**核取方塊。
     f. 如果您想要 Kaspersky Embedded Systems Security 將符合規則觸發條件的應用程式視為受信任的更新程式，請選擇**"信任的更新程式"**核取方塊。信任的更新程式是被允許建立其它可執行檔的應用程式，這些可執行檔將被允許隨後執行。

如果一個應用程式觸發了多個規則，Kaspersky Embedded Systems Security 將在滿足以下條件的情況下設定"*信任的更新程式*"旗標：

- 所有規則允許應用程式執行。
- 至少一個規則選擇了"**信任的更新程式**"核取方塊。

g. 為應用程式啟動控制規則新增觸發條件。

h. 為應用程式啟動控制規則新增觸發條件排除項目。

i. **新增被允許或禁止啟動滿足規則的應用程式的使用者和/或使用者群組**。

a. 選擇"**使用者或群組**"標籤。

b. 點擊"**新增**"。

c. 這將開啟一個視窗；在該視窗中，輸入或選擇使用者或使用者群組的名稱。

d. 單擊"**選擇**"。

e. 為每個使用者或使用者群組完成步驟 b 到 d。

j. 點擊**OK**。

新增的應用程式啟動控制規則顯示在清單中。

- **透過匯入包含應用程式啟動控制規則的 XML 檔案**

a. 單擊"**匯入**"。

b. 在顯示的"**從檔案匯入**"視窗中，點擊"**選擇**"按鈕。

c. 指定在完成*應用程式啟動控制規則產生器*的本機工作或群組工作後建立的 XML 檔案的路徑。

d. 單擊"**開啟**"。

e. 單擊"**匯入**"。

匯入的應用程式啟動控制規則被新增到現有規則清單。不會複製具有相同設定的規則。如果有至少一項規則設定是唯一性質，則新增該規則。

- **透過匯入包含 Kaspersky Embedded Systems Security 3.4 應用程式啟動控制規則的 XML 檔案**

a. 單擊"**從先前的版本匯入**"。

b. 在顯示的"**從檔案匯入**"視窗中，點擊"**選擇**"按鈕。

c. 使用從 Kaspersky Embedded Systems Security 3.4 匯出的應用程式啟動控制規則指定 XML 檔案的路徑。

d. 點擊**開啟**。

e. 單擊"**匯入**"。

匯入的應用程式啟動控制規則被新增到現有規則清單。不會複製具有相同設定的規則。如果有至少一項規則設定是唯一性質，則新增該規則。

- **透過從卡巴斯基安全管理中心報告檔案匯入規則**

  a. 單擊**"從 KSC 報告匯入"**。

  b. 在開啟的視窗中，選擇報告中事件匯出其中的 TXT 檔案。

  c. 點擊**開啟**。

  基於卡巴斯基安全管理中心報告的規則被新增到政策中的規則清單中。

- **基於使用請求的卡巴斯基安全管理中心事件**

  a. 單擊**"允許來自 KSC 事件的規則"**。

  開啟**"應用程式啟動控制規則產生器"**視窗。

  b. 選擇應用程式將據此建立應用程式啟動控制規則的事件類型：

  - **所有事件**
  - **應用程式啟動被拒絕**
  - **僅統計模式：應用程式啟動被拒絕**

  c. 從**使用在以下期間內產生的事件**下拉式清單中選擇一個時間段。

  d. 清除或選中**"產生規則時優先考慮使用雜湊"**核取方塊。

  如果選中此核取方塊，則當檔案的核對總和與憑證均可用時，Kaspersky Embedded Systems Security 將使用檔案的核對總和來產生規則。

  如果清除此核取方塊，則當檔案的核對總和與憑證均可用時，Kaspersky Embedded Systems Security 將使用檔案的數位憑證來產生規則。

  e. 如有必要，請在**使用為受管理裝置群組產生的事件**欄位中指定受管理裝置群組的名稱。

  f. 單擊**"產生規則"**。

  g. 從**新增至主清單的規則**下拉式清單中，選擇將規則新增到先前建立的應用程式啟動控制規則清單中的原則：

  - **新增到現有規則**，如果您希望將匯入的規則新增到現有規則清單。將複製具有相同設定的規則。
  - **取代現有規則**，如果您希望將現有規則取代為匯入的規則。

  h. 選取要匯出至政策之應用程式啟動控制規則的規則，然後按一下 **匯出** 按鈕。

  i. 儲存變更。

10. 如有必要，請執行步驟 5 新增更多應用程式啟動控制規則。

11. 如有必要，透過點擊 **編輯**按鈕編輯新增的應用程式啟動控制規則。

12. 如有必要，透過點擊**刪除**按鈕刪除新增的應用程式啟動控制規則。

13. 單擊**"確定"**。

為應用程式控制規則新增觸發條件

如何在卡巴斯基安全管理中心管理主控台中新增應用程式啟動控制規則的觸發條件

1. 在卡巴斯基安全管理中心管理主控台樹狀目錄中，選取**政策**。

2. 選擇必要的政策並點擊以開啟政策內容。

3. 在政策內容視窗中，轉至「**本機活動控制**」區域。

4. 在"**應用程式啟動控制**"塊中，點擊"**設定**"按鈕。
   應用程式啟動控制視窗將在**一般**頁簽上開啟。

5. 選擇**"規則"**標籤。

6. 執行以下操作之一：

   a. 點擊**新增** 按鈕（如果您要新增新的應用程式啟動控制規則）。

   b. 在應用程式啟動控制規則清單中，選擇要新增觸發條件的規則，然後按一下 **編輯** 按鈕。

   開啟**"應用程式啟動控制"**視窗。

7. 在**條件**頁簽上，在**新增**按鈕的內容功能表中，選擇從應用程式啟動控制規則的觸發條件：

   - **檔案資訊**。 **所選檔案中的資訊**被用作規則觸發條件。

     a. 在**檔案資訊**視窗中，按一下**瀏覽**按鈕。
     標準 Microsoft Windows **開啟檔案**視窗將開啟。

     b. 選擇檔案。

     c. 點擊**開啟**。
     有關所選檔案的資訊顯示在**檔案資訊**視窗中。

     d. 選擇至少一個選項：

     - **憑證詳細資訊**如果選取此核取方塊，則規則不會控制使用具有指定資料的數位憑證簽署的應用程式的啟動。
     - **檔案內容**如果選取此核取方塊，則規則不會控制具有指定中繼資料的應用程式的啟動。
     - **檔案雜湊**如果選取此核取方塊，則規則不會控制具有指定 SHA256 雜湊的應用程式的啟動。
     - **檔案路徑**如果選取此核取方塊，則規則不會控制在指定路徑的應用程式的啟動。

e. 如有必要，在**命令行**欄位中，輸入用於在命令列上啟動應用程式的命令。此規則控制此應用程式的啟動。您可以使用？和 * 字元輸入遮罩。

> Kaspersky Embedded Systems Security 無法辨識包含斜線"/"的路徑。在路徑中使用反斜線字元（"\"）。

f. 單擊"**確定**"。

- **磁碟機類型**此規則可控制從連線到受防護電腦的所有卸除式磁碟機啟動應用程式。
- **KL 類別**此規則可控制屬於所選 KL 類別的應用程式的啟動。
- **受 KSN 信任**此規則可控制 KSN 中受信任的應用程式的啟動。
- **不受 KSN 信任**此規則可控制 KSN 中不受信任的應用程式的啟動。
- **受作業係統信任**此規則可控制作業係統中受信任的應用程式的啟動。

新增的條件將顯示在清單中。

8. 如有必要，請針對每個後續規則觸發條件執行說明的上一個步驟。
9. 如有必要，點擊**編輯** 按鈕編輯規則觸發條件。
10. 儲存變更。

如何在 Kaspersky Embedded Systems Security 主控台中新增應用程式啟動控制規則的觸發條件

1. 在管理主控台樹狀目錄中，選擇**電腦控制 → 應用程式啟動控制**資料夾。
2. 在結果窗格中點擊"**內容**"連結。
   應用程式啟動控制視窗將在**一般**頁簽上開啟。
3. 選擇"**規則**"標籤。
4. 執行以下操作之一：

   a. 點擊**新增** 按鈕（如果您要新增新的應用程式啟動控制規則）。

   b. 在應用程式啟動控制規則清單中，選擇要新增觸發條件的規則，然後按一下 **編輯** 按鈕。

   開啟"**應用程式啟動控制**"視窗。

5. 在**條件**頁簽上，在**新增**按鈕的內容功能表中，選擇從應用程式啟動控制規則的觸發條件：

   - **檔案資訊**。 **所選檔案中的資訊**被用作規則觸發條件。

     a. 在**檔案資訊**視窗中，按一下**瀏覽**按鈕。
     標準 Microsoft Windows **開啟檔案**視窗將開啟。

     b. 選擇檔案。

c. 點擊**開啟**。

有關所選檔案的資訊顯示在**檔案資訊**視窗中。

d. 選擇至少一個選項：

- **憑證詳細資訊**如果選取此核取方塊，則規則不會控制使用具有指定資料的數位憑證簽署的應用程式的啟動。
- **檔案內容**如果選取此核取方塊，則規則不會控制具有指定中繼資料的應用程式的啟動。
- **檔案雜湊**如果選取此核取方塊，則規則不會控制具有指定 SHA256 雜湊的應用程式的啟動。
- **檔案路徑**如果選取此核取方塊，則規則不會控制在指定路徑的應用程式的啟動。

e. 如有必要，在**命令行**欄位中，輸入用於在命令列上啟動應用程式的命令。此規則控制此應用程式的啟動。您可以使用？和 * 字元輸入遮罩。

> Kaspersky Embedded Systems Security 無法辨識包含斜線“/”的路徑。在路徑中使用反斜線字元（“\”）。

f. 單擊**“確定”**。

- **磁碟機類型**此規則可控制從連線到受防護電腦的所有卸除式磁碟機啟動應用程式。
- **KL 類別**此規則可控制屬於所選 KL 類別的應用程式的啟動。
- **受 KSN 信任**此規則可控制 KSN 中受信任的應用程式的啟動。
- **不受 KSN 信任**此規則可控制 KSN 中不受信任的應用程式的啟動。
- **受作業係統信任**此規則可控制作業係統中受信任的應用程式的啟動。

新增的條件將顯示在清單中。

6. 如有必要，請針對每個後續規則觸發條件執行說明的上一個步驟。
7. 如有必要，點擊**編輯** 按鈕編輯規則觸發條件。
8. 儲存變更。

如何在卡巴斯基安全管理中心網頁主控台中新增應用程式啟動控制規則的觸發條件

1. 在網頁主控台的主視窗中，選擇**資產管理 → 政策**。
2. 點擊 Kaspersky Embedded Systems Security 政策的名稱。

政策內容視窗將開啟。

3. 選擇**“應用程式設定”**標籤。
4. 選擇 **本機活動控制** 部分。
5. 在**”應用程式啟動控制”**塊中，點擊**”配置”**按鈕。

應用程式啟動控制視窗將在**一般**頁簽上開啟。

6. 選擇**"規則"**標籤。
7. 點擊**"新增"**。
   開啟**"規則設定"**視窗。
8. 在**"條件"**標籤上點擊**"新增"**按鈕 。
   開啟**"規則設定"**視窗。
9. 選擇應用程式控制規則的觸發條件：
   - **檔案資訊**。 **檔案中的資訊**被用作規則觸發條件。
     a. 在**規則觸發標準**下面，為至少一個條件指定一個值：
     - **數位憑證**如果選取此核取方塊，則規則不會控制使用具有指定資料的數位憑證簽署的應用程式的啟動。
     - **檔案內容**如果選取此核取方塊，則規則不會控制具有指定中繼資料的應用程式的啟動。
     - **SHA256 雜湊**如果選取此核取方塊，則規則不會控制具有指定 SHA256 雜湊的應用程式的啟動。
     - **檔案路徑**如果選取此核取方塊，則規則不會控制在指定路徑的應用程式的啟動。
     b. 單擊**"確定"**。
   - **自 KL 類別**此規則可控制屬於所選 KL 類別的應用程式的啟動。
   - **卸除式磁碟機**此規則可控制從連線到受防護電腦的所有卸除式磁碟機啟動應用程式。
   - **受作業係統信任**此規則可控制作業係統中受信任的應用程式的啟動。

   新增的條件將顯示在清單中。
10. 如有必要，請針對每個後續規則觸發條件執行說明的步驟 4 和 5。
11. 如有必要，點擊**編輯** 按鈕編輯規則觸發條件。
12. 儲存變更。

新增應用程式啟動控制規則範圍的排除項目

如何在卡巴斯基安全管理中心管理主控台中新增應用程式啟動控制規則範圍的排除項目

1. 在卡巴斯基安全管理中心管理主控台樹狀目錄中，選取**政策**。
2. 選擇必要的政策並點擊以開啟政策內容。
3. 在政策內容視窗中，轉至「**本機活動控制**」區域。
4. 在"**應用程式啟動控制**"塊中，點擊"**設定**"按鈕。
   應用程式啟動控制視窗將在**一般**頁簽上開啟。

5. 選擇“**規則**”標籤。

6. 執行以下操作之一：

   a. 點擊**新增** 按鈕（如果您要新增新的應用程式啟動控制規則）。

   b. 在應用程式啟動控制規則清單中，選擇要新增排除項目的規則，然後點擊**編輯** 按鈕。

   開啟“**應用程式啟動控制**”視窗。

7. 在**排除項目**頁簽上，在**新增**按鈕的內容功能表中，選擇從應用程式啟動控制規則範圍建立排除項目的條件：

   - **檔案資訊**。 **所選檔案中的資訊**被用作條件。

     a. 在**檔案資訊**視窗中，按一下**瀏覽**按鈕。
     標準 Microsoft Windows **開啟檔案**視窗將開啟。

     b. 選擇檔案。

     c. 點擊**開啟**。
     有關所選檔案的資訊顯示在**檔案資訊**視窗中。

     d. 選擇至少一個選項：

     - **憑證詳細資訊**如果選取此核取方塊，則規則不會控制使用具有指定資料的數位憑證簽署的應用程式的啟動。
     - **檔案內容**如果選取此核取方塊，則規則不會控制具有指定中繼資料的應用程式的啟動。
     - **檔案雜湊**如果選取此核取方塊，則規則不會控制具有指定 SHA256 雜湊的應用程式的啟動。
     - **檔案路徑**如果選取此核取方塊，則規則不會控制在指定路徑的應用程式的啟動。

     e. 如有必要，在**命令行**欄位中，輸入用於在命令列上啟動應用程式的命令。此規則不控制此應用程式的啟動。您可以使用？和 * 字元輸入遮罩。

     > Kaspersky Embedded Systems Security 無法辨識包含斜線“/”的路徑。在路徑中使用反斜線字元（“\”）。

     f. 單擊“**確定**”。

   - **磁碟機類型**此規則不控制從連線到受防護電腦的所有卸除式磁碟機啟動應用程式。
   - **KL 類別**此規則不控制屬於所選 KL 類別的應用程式的啟動。
   - **受 KSN 信任**此規則不控制 KSN 中受信任的應用程式的啟動。
   - **不受 KSN 信任**此規則不控制 KSN 中不受信任的應用程式的啟動。
   - **受作業係統信任**此規則不控制作業係統中受信任的應用程式的啟動。

   新增的排除項目將顯示在清單中。

8. 如有必要，請執行說明的上一步，以新增應用程式啟動控制規則範圍中的每一個後續排除項目。

9. 如有必要，點擊**編輯**按鈕編輯排除項目。

10. 儲存變更。

如何在 Kaspersky Embedded Systems Security 主控台中新增應用程式啟動控制規則範圍的排除項目

1. 在管理主控台樹狀目錄中，選擇**電腦控制 → 應用程式啟動控制**資料夾。

2. 在結果窗格中點擊**"內容"**連結。
   應用程式啟動控制視窗將在**一般**頁簽上開啟。

3. 選擇**"規則"**標籤。

4. 執行以下操作之一：

   a. 點擊**新增** 按鈕（如果您要新增新的應用程式啟動控制規則）。

   b. 在應用程式啟動控制規則清單中，選擇要新增排除項目的規則，然後點擊**編輯** 按鈕。

   開啟**"應用程式啟動控制"**視窗。

5. 在**排除項目**頁簽上，在**新增**按鈕的內容功能表中，選擇從應用程式啟動控制規則範圍建立排除項目的條件：

   - **檔案資訊**。 **所選檔案中的資訊**被用作條件。

     a. 在**檔案資訊**視窗中，按一下**瀏覽**按鈕。
     標準 Microsoft Windows **開啟檔案**視窗將開啟。

     b. 選擇檔案。

     c. 點擊**開啟**。
     有關所選檔案的資訊顯示在**檔案資訊**視窗中。

     d. 選擇至少一個選項：

     - **憑證詳細資訊**如果選取此核取方塊，則規則不會控制使用具有指定資料的數位憑證簽署的應用程式的啟動。
     - **檔案內容**如果選取此核取方塊，則規則不會控制具有指定中繼資料的應用程式的啟動。
     - **檔案雜湊**如果選取此核取方塊，則規則不會控制具有指定 SHA256 雜湊的應用程式的啟動。
     - **檔案路徑**如果選取此核取方塊，則規則不會控制在指定路徑的應用程式的啟動。

     e. 如有必要，在**命令行**欄位中，輸入用於在命令列上啟動應用程式的命令。此規則不控制此應用程式的啟動。您可以使用？和 * 字元輸入遮罩。

     > Kaspersky Embedded Systems Security 無法辨識包含斜線"/"的路徑。在路徑中使用反斜線字元（"\"）。

     f. 單擊**"確定"**。

- **磁碟機類型**此規則不控制從連線到受防護電腦的所有卸除式磁碟機啟動應用程式。
- **KL 類別**此規則不控制屬於所選 KL 類別的應用程式的啟動。
- **受 KSN 信任**此規則不控制 KSN 中受信任的應用程式的啟動。
- **不受 KSN 信任**此規則不控制 KSN 中不受信任的應用程式的啟動。
- **受作業係統信任**此規則不控制作業係統中受信任的應用程式的啟動。

新增的排除項目將顯示在清單中。

6. 如有必要，請執行說明的上一步，以新增應用程式啟動控制規則範圍中的每一個後續排除項目。
7. 如有必要，點擊**編輯**按鈕編輯排除項目。
8. 儲存變更。

如何在卡巴斯基安全管理中心網頁主控台中新增應用程式啟動控制規則範圍的排除項目

1. 在網頁主控台的主視窗中，選擇**資產管理 → 政策**。
2. 點擊 Kaspersky Embedded Systems Security 政策的名稱。
   政策內容視窗將開啟。
3. 選擇**"應用程式設定"**標籤。
4. 選擇 **本機活動控制** 部分。
5. 在**"應用程式啟動控制"**塊中，點擊**"配置"**按鈕。
   應用程式啟動控制視窗將在**一般**頁簽上開啟。
6. 選擇**"規則"**標籤。
7. 點擊**"新增"**。
   開啟**"規則設定"**視窗。
8. 在**"排除項目"**標籤上點擊**"新增"**按鈕 。
   開啟**"規則設定"**視窗。
9. 選擇從應用程式啟動控制規則範圍建立排除項目的條件：
   - **檔案資訊**此規則不控制資料與**檔案中的資料**匹配的應用程序的啟動。
     a. 在**規則觸發標準**下面，為至少一個條件指定一個值：
     - **數位憑證**如果選取此核取方塊，則規則不會控制使用具有指定資料的數位憑證簽署的應用程式的啟動。
     - **檔案內容**如果選取此核取方塊，則規則不會控制具有指定中繼資料的應用程式的啟動。

- **SHA256 雜湊**如果選取此核取方塊，則規則不會控制具有指定 SHA256 雜湊的應用程式的啟動。
- **檔案路徑**如果選取此核取方塊，則規則不會控制在指定路徑的應用程式的啟動。

b. 單擊**"確定"**。

- **KL 類別**此規則不控制屬於所選 KL 類別的應用程式的啟動。
- **磁碟機類型**此規則不控制從連線到受防護電腦的所有卸除式磁碟機啟動應用程式。
- **受作業係統信任**此規則不控制作業係統中受信任的應用程式的啟動。

新增的條件將顯示在清單中。

10. 如有必要，請執行說明的步驟 4 到 5，以新增應用程式啟動控制規則範圍中的每一個後續排除項目。
11. 如有必要，點擊**編輯**按鈕編輯排除項目。
12. 儲存變更。

允許所有應用程式執行

您可以使用專門配置的應用程式啟動控制允許規則來允許啟動所有應用程式。

要允許啟動所有應用程式：

1. 使用以下參數手動新增兩個應用程式啟動控制允許規則：
   - 規則類型：*允許*，範圍：*可執行檔*，檔案路徑：`?:\`。
   - 規則類型：*允許*，範圍：*指令碼和 MSI 套件*，檔案路徑：`?:\`。
2. 如果已新增應用程式啟動控制拒絕規則，請刪除這些拒絕規則。
3. 對於所有先前建立的應用程式啟動控制允許規則，刪除排除項目。
4. 儲存變更。

匯出應用程式啟動控制規則

您可以將應用程式啟動控制規則清單和軟體發佈控制的受信任安裝套件清單匯出至 XML 檔案。您可以使用匯出功能來備份應用程式啟動控制規則清單，或將該清單遷移至其他伺服器。

在卡巴斯基安全管理中心管理主控台中匯出應用程式啟動控制規則

1. 在卡巴斯基安全管理中心管理主控台樹狀目錄中，選取**政策**。
2. 選擇必要的政策並點擊以開啟政策內容。
3. 在政策內容視窗中，轉至「**本機活動控制**」區域。

4. 在"**應用程式啟動控制**"塊中，點擊"**設定**"按鈕。
   應用程式啟動控制視窗將在**一般**頁簽上開啟。

5. 前往 **規則** 索引標籤以匯出應用程式啟動控制規則，或前往 **軟體分發控制** 索引標籤以匯出軟體發佈控制規則。

6. 如果您要匯出整個清單，請按一下 按鈕，然後選取 **匯出**。

7. 如果您只要匯出清單的一部分，請依照下列步驟操作：

   a. 使用 **CTRL** 或 **SHIFT** 鍵選取您要匯出的清單項目。若要選取所有項目，請按 **CTRL+A**。

   b. 按一下 按鈕，然後選取 **匯出所選**。

8. 在開啟的視窗中，指定要匯出至的 XML 檔案名稱，然後選取要儲存該檔案的資料夾。點擊"**儲存**"按鈕。

Kaspersky Embedded Systems Security 會將規則清單匯出到 XML 檔案。

在 Kaspersky Embedded Systems Security 主控台中匯出應用程式啟動控制規則

1. 在管理主控台樹狀目錄中，選擇**電腦控制 → 應用程式啟動控制**資料夾。

2. 在結果窗格中點擊"**內容**"連結。
   應用程式啟動控制視窗將在**一般**頁簽上開啟。

3. 前往 **規則** 索引標籤以匯出應用程式啟動控制規則，或前往 **軟體分發控制** 索引標籤以匯出軟體發佈控制規則。

4. 如果您要匯出整個清單，請按一下 按鈕，然後選取 **匯出**。

5. 如果您只要匯出清單的一部分，請依照下列步驟操作：

   a. 使用 **CTRL** 或 **SHIFT** 鍵選取您要匯出的清單項目。若要選取所有項目，請按 **CTRL+A**。

   b. 按一下 按鈕，然後選取 **匯出所選**。

6. 在開啟的視窗中，指定要匯出至的 XML 檔案名稱，然後選取要儲存該檔案的資料夾。點擊"**儲存**"按鈕。

Kaspersky Embedded Systems Security 會將規則清單匯出到 XML 檔案。

在 Web Console 中匯出應用程式啟動控制規則

1. 在網頁主控台的主視窗中，選擇**資產管理 → 政策**。

2. 點擊 Kaspersky Embedded Systems Security 政策的名稱。
   政策內容視窗將開啟。

3. 選擇"**應用程式設定**"標籤。

4. 選擇 **本機活動控制** 部分。

5. 在"**應用程式啟動控制**"塊中，點擊"**配置**"按鈕。
   應用程式啟動控制視窗將在**一般**頁簽上開啟。

6. 前往 **規則** 索引標籤以匯出應用程式啟動控制規則，或前往 **軟體分發控制** 索引標籤以匯出軟體發佈控制規則。

7. 使用核取方塊，選取您要匯出的規則。

8. 點擊**匯出**按鈕。這會開啟一個視窗，在該視窗中，指定是要匯出選定規則還是所有規則，然後點擊**匯出**。

   如果您未選擇任何規則，則 Kaspersky Embedded Systems Security 將匯出所有規則。

Kaspersky Embedded Systems Security 會將規則清單匯出到 XML 檔案。

使用選定的卡巴斯基安全管理中心封鎖的應用程式事件來產生 TXT 檔案

您可以將選定的卡巴斯基安全管理中心封鎖的應用程式事件匯出到 TXT 檔案，然後匯入此資料以在您正在配置的政策中產生應用程式啟動控制允許規則清單。

如何使用卡巴斯基安全管理中心管理主控台產生包含所選卡巴斯基安全管理中心封鎖的應用程式事件的 TXT 檔案

1. 在卡巴斯基安全管理中心管理主控台樹狀目錄中，選取**政策**。

2. 選擇必要的政策並點擊以開啟政策內容。

3. 在政策內容視窗中，轉至「**記錄和通知**」區域。

4. 在"**工作記錄**"塊中，點擊"**設定**"按鈕。

   開啟"**通知**"視窗。

5. 展開 **本機活動控制** 節點。

6. 選擇 **應用程式啟動控制** 部分。

7. 在應用程式啟動控制事件清單中的**將事件傳送到卡巴斯基安全管理中心**列中，選取 *已禁止應用程式啟動* 和 *禁止應用程式在測試模式下啟動* 旁邊的核取方塊。

8. 儲存變更。

9. 在政策的**事件組態**部分，確保在**儲存在管理伺服器資料庫中（天）**欄位中指定的事件儲存持續時間大於您計劃收集的關於被防止的應用程式啟動的資訊的時間段（預設值為 30 天）。

   一旦應用程式啟動控制元件記錄保留期限到期，將會刪除記錄的事件，而且不會出現在報告中。

10. 啟動為收集有關被拒絕的應用程式啟動的資料而設定的政策。

11. 如有需要，修改應用程式啟動控制元件作業模式。

12. 當收集有關被封鎖的應用程式啟動的資訊的期限到期時，請從 *已禁止應用程式啟動* 和 *禁止應用程式在測試模式下啟動* 事件進行選擇並將其匯出到 TXT 檔案。詳情請參閱卡巴斯基安全管理中心說明中的"事件選擇"部分。

13. 開啟匯出的 TXT 檔案。

14. 如有必要，編輯事件清單。

如何使用卡巴斯基安全管理中心網頁主控台產生包含所選卡巴斯基安全管理中心封鎖的應用程式事件的 TXT 檔案

1. 在網頁主控台的主視窗中，選擇**資產管理 → 政策**。

2. 點擊 Kaspersky Embedded Systems Security 政策的名稱。

   政策內容視窗將開啟。

3. 選擇"**應用程式設定**"標籤。

4. 選擇 **記錄和通知** 部分。

5. 在"**工作記錄**"塊中，點擊"**配置**"按鈕。

   開啟"**工作記錄**"視窗。

6. 選擇 **應用程式啟動控制** 部分。

7. 在應用程式啟動控制事件清單中的**將事件傳送到卡巴斯基安全管理中心**列中，選取*已禁止應用程式啟動* 和 *禁止應用程式在測試模式下啟動*旁邊的核取方塊。

8. 儲存變更。

9. 在您正在設定的政策的**事件組態**頁簽上，確保在**儲存在管理伺服器資料庫中（天）**欄位中指定的事件儲存持續時間大於您計劃收集的關於被防止的應用程式啟動的資訊的時間段（預設值為 30 天）。

   一旦應用程式啟動控制元件記錄保留期限到期，將會刪除記錄的事件，而且不會出現在報告中。

10. 啟動為收集有關被拒絕的應用程式啟動的資料而設定的政策。

11. 如有需要，修改應用程式啟動控制元件作業模式。

12. 當收集有關被封鎖的應用程式啟動的資訊的期限到期時，請從 *已禁止應用程式啟動* 和 *禁止應用程式在測試模式下啟動* 事件進行選擇並將其匯出到 TXT 檔案。詳情請參閱卡巴斯基安全管理中心說明中的"事件選擇"部分。

13. 開啟匯出的 TXT 檔案。

14. 如有必要，編輯事件清單。

配置"應用程式啟動控制規則產生器"群組工作

如何在卡巴斯基安全管理中心管理主控台中設定「應用程式啟動控制規則產生器」群組工作

1. 在卡巴斯基安全管理中心管理主控台中，展開"**受管理裝置**"節點。

2. 選擇要為其設定工作的管理群組。

3. 選擇“**工作**”標籤。

4. 在群組工作清單中，雙擊工作名稱，開啟*應用程式啟動控制規則產生器*工作。

   內容: 應用程式啟動控制規則產生器視窗將開啟。

5. 轉到“**選項**”區域。

6. 如有必要，在**規則**頁簽上輸入規則名稱的前綴。

7. 在**允許規則使用範圍**下面，指定要用於建立允許規則的方法：

   - **基於正在執行的應用程式建立允許規則**
   - **為資料夾的應用程式建立允許規則**

8. 在**設定**頁簽上，選擇建立應用程式啟動控制允許規則時工作將套用的條件：

   - **使用數位憑證**

     如果選擇此選項，則會在新建立的應用程式啟動控制允許規則設定中將存在數位憑證指定為規則觸發條件。Kaspersky Embedded Systems Security 將允許具有數位憑證的檔案。如果希望允許作業系統中信任的任何應用程式啟動，建議使用此選項。預設選中該選項。

   - **使用數位憑證主旨和指紋**
   - **如果憑證缺失，則使用**
   - **使用 SHA256 雜湊**

     如果選擇此選項，則會在新建立的應用程式啟動控制允許規則的設定中，將用於建立規則的檔案的總和檢查碼指定為規則觸發條件。Kaspersky Embedded Systems Security 將允許使用具有指定總和檢查碼的檔案啟動的應用程式。使用 SHA256 總和檢查碼作為規則觸發條件會將規則使用範圍限制為一個檔案。

9. 配置 **為基於雜湊總和產生的規則新增一個檔案路徑** 設定。

   如果選取此核取方塊，則在匯出規則時， Kaspersky Embedded Systems Security 會將可執行檔的完整路徑新增至 XML 檔案。完整路徑可以幫助您判斷可執行檔屬於哪個軟體。

   如果清除該核取方塊，則 XML 檔案僅包含可執行檔的名稱和 SHA256 雜湊。預設情況下，會取消勾選核取方塊。

10. 新增將被允許啟動滿足使用工作建立的規則的應用程式的使用者和/或使用者群組：

    a. 在**新增**按鈕的內容功能表中，選擇新增使用者或者群組的方法。

    b. 這將開啟一個視窗；在該視窗中，輸入或選擇使用者或使用者群組的名稱。

    c. 單擊“**確定**”。

    d. 為每個使用者或使用者群組完成步驟 a 到 c。

11. 在“**工作完成後**”區塊中，配置以下設定：

    - **將允許規則新增到應用程式啟動控制規則清單**
    - **新增原則**
    - **將允許規則匯出到檔案**

- **將受防護裝置詳情新增至檔案名稱**

12. 如有必要，在**排除項目**頁簽上指定要從工作範圍中排除的物件。

13. 在**內容: 應用程式啟動控制規則產生器**視窗中，按一下**確定**按鈕。

如何在卡巴斯基安全管理中心網頁主控台中設定「應用程式啟動控制規則產生器」群組工作

1. 在網頁主控台的主視窗中，選擇**資產管理 → 工作**。

2. 在群組工作清單中，開啟應用程式啟動控制規則產生器工作。
   開啟"**應用程式啟動控制規則產生器**"視窗。

3. 開啟**應用程式設定**頁簽。

4. 如有必要，在**允許規則的使用範圍**部分中輸入規則名稱的前綴。

5. 在**允許規則的使用範圍**下面，指定要用於建立允許規則的方法：

   - **基於正在執行的應用程式建立允許規則**
   - **為資料夾的應用程式建立允許規則**

6. 在**參數**頁簽上，選擇建立應用程式啟動控制允許規則時工作將套用的條件：

   - **使用數位憑證**
   - **使用數位憑證主旨和指紋**
   - **如果憑證缺失，則使用**
   - **使用 SHA256 雜湊**

7. 配置 **為基於雜湊總和產生的規則新增一個檔案路徑** 設定。
   如果選取此核取方塊，則在匯出規則時， Kaspersky Embedded Systems Security 會將可執行檔的完整路徑新增至 XML 檔案。完整路徑可以幫助您判斷可執行檔屬於哪個軟體。
   如果清除該核取方塊，則 XML 檔案僅包含可執行檔的名稱和 SHA256 雜湊。預設情況下，會取消勾選核取方塊。

8. 新增將被允許啟動滿足使用工作建立的規則的應用程式的使用者和/或使用者群組：

   a. 單擊"**新增使用者或群組**"。

   b. 這將開啟一個視窗；在該視窗中，輸入或選擇使用者或使用者群組的名稱。

   c. 單擊"**選擇**"。

   d. 為每個使用者或使用者群組完成步驟 a 到 c。

9. 在"**工作完成後**"區塊中，配置以下設定：

   - **將允許規則新增到應用程式啟動控制規則清單**
   - **新增原則**

- **允許規則將被匯出到檔案。**在「**指定帶 .xml 副檔名之檔案的完整路徑**」欄位中，您可以指定「應用程式啟動控制規則產生器」工作完成時 Kaspersky Embedded Systems Security 將允許規則匯出到 XML 檔案的路徑。

- **將防護裝置詳細資訊新增到檔案名稱**

10. 如有必要，在**排除項目**頁簽上指定要從工作範圍中排除的物件。

11. 在**應用程式啟動控制規則產生器**視窗中，按一下**確定**按鈕。

使用"應用程式啟動控制規則產生器"群組工作建立規則。

要使用「應用程式啟動控制規則產生器」群組工作建立規則：

1. 建立"*應用程式啟動控制規則產生器*"群組工作或選取現有工作。

2. 設定「應用程式啟動控制規則產生器」工作。

3. 執行"應用程式啟動控制規則產生器"工作。

工作完成後，根據工作設定：

- 如果工作完成後您指定了**將允許規則新增到應用程式啟動控制規則清單**操作，產生的應用程式啟動控制規則將會被新增至應用程式主控台的應用程式啟動控制設定中的清單。

- 如果您指定了工作完成後執行**允許規則將被匯出到檔案。**操作，產生的應用程式啟動控制規則將被儲存到工作設定中指定的路徑處的 XML 檔案中。

這些清單包含類型與「應用程式啟動控制規則產生器」群組工作的設定匹配的應用程式啟動允許規則。

裝置控制

裝置控制管理使用者對安裝在電腦上或連線到電腦的裝置（例如，硬碟磁碟機、相機或 Wi-Fi 模組）的存取。這樣可以在連線此類裝置時防護電腦免受感染，並防止資料遺失或洩漏。

裝置控制 提供以下功能：

- 管理使用者對儲存裝置（例如卸除式磁碟機、行動電話、CD/DVD 磁碟機等）的存取權限。
- 控制沒有檔案系統的裝置（例如外部數據機、藍牙介面卡、USB 鍵盤等）的連線。
- 管理 Wi-Fi 連線。

預設情況下，裝置控制被停用。當您啟用 裝置控制時，Kaspersky Embedded Systems Security 預設拒絕存取以下裝置類型：

- 卸除式磁碟機（包括 USB 快閃磁碟機）
- 軟碟
- CD/DVD 磁碟機
- 可攜式裝置 (MTP)
- 數據機
- 智慧卡讀卡機
- 外部網路介面卡
- 藍牙（輸入裝置除外）

裝置控制等級

Kaspersky Embedded Systems Security 在以下等級控制裝置存取：

1. **裝置類型**。

   將裝置連線到電腦時，作業系統會決定裝置的類型：印表機、卸除式磁碟機、CD/DVD 磁碟機等。在此層級，您可以按類型允許或拒絕裝置連線。

2. **連線匯流排**。

   *連線匯流排*是用於將裝置連線到電腦的介面。某些裝置類型具有多個連線介面。例如，您可以將印表機連線到 USB 或串列 (COM) 連接埠。

   在此層級，您可以根據連線匯流排允許或拒絕對裝置的存取。

   例如，假設您拒絕透過 USB 進行的存取。如果裝置透過 USB 連線，Kaspersky Embedded Systems Security 會拒絕對所有採用**取決於連線匯流排**模式的裝置的存取。

如果為裝置選取了**允許**或者**封鎖**存取模式，則存取控制將忽略裝置的連線匯流排。

3. **受信任裝置**。

   *信任的裝置*是指在信任裝置設定中指定的使用者可隨時進行完全存取的裝置。

“裝置控制”操作模式

裝置控制可以下列模式運作：

- **主動模式**。

  Kaspersky Embedded Systems Security 根據配置的裝置存取規則拒絕或允許裝置。該應用程式還允許存取受信任裝置。應用程式註冊裝置連線和斷開連線事件。

- **通知**.

  Kaspersky Embedded Systems Security 允許所有裝置並記錄相應的事件。允許所有裝置。預設設定此模式。您可以啟用此模式 對組織中的裝置進行稽核並使用此資訊起草可信任裝置清單。

裝置存取規則

*裝置存取規則*是一組設定，用於確定使用者如何可以存取安裝到或連線到電腦的裝置。這些設定包括對特定裝置的存取、存取排程、讀取或寫入權限等。存取規則的設定群組根據裝置類型的不同而不同。

存取規則設定

裝置	使用者和/或使用者群組的分配	裝置存取排程	讀/寫權限	連線匯流排監控
硬碟磁碟機	✓	✓	✓	✓
卸除式磁碟機（包括 USB 快閃磁碟機）	✓	✓	✓	✓
軟碟	✓	✓	✓	✓
CD/DVD 磁碟機	✓	✓	✓	✓
可攜式裝置 (MTP)	✓	✓	✓	✓
本機印表機	✓	–	–	✓
網路印表機	✓	–	–	–
數據機	–	–	–	✓
Streamer	–	–	–	✓
多功能裝置	–	–	–	✓
智慧卡讀卡機	–	–	–	✓
Windows CE USB ActiveSync 裝置	–	–	–	✓
外部網路介面卡	–	–	–	✓
藍牙	–	–	–	–
攝影鏡頭和掃描器	–	–	–	✓
Wi-Fi	–	–	–	–

裝置	使用者和/或使用者群組的分配	裝置存取排程	讀/寫權限	連線匯流排監控
USB 鍵盤	–	–	–	✓
USB 滑鼠	–	–	–	✓

按類型管理對裝置的存取

裝置控制可按類型管理對裝置的存取。裝置類型由作業系統在裝置連線時決定。您可以使用作業系統內建的裝置管理器工具來尋找裝置類型。若要管理對裝置的存取，您必須配置規則。*裝置存取規則*是一組設定，用於確定使用者如何可以存取安裝到或連線到電腦的裝置。這些設定包括對特定裝置的存取、存取排程、讀取或寫入權限等。存取規則的設定群組根據裝置類型的不同而不同。

您可以按如下方式配置裝置存取權限：

- **允許**

  Kaspersky Embedded Systems Security 向所有使用者授予對裝置的完全存取權。

- **封鎖**

  Kaspersky Embedded Systems Security 可封鎖裝置連線。該應用程式允許 僅連接受信任的裝置。

- **取決於連線匯流排**

  Kaspersky Embedded Systems Security 會識別裝置的連線匯流排，並根據連線匯流排的存取模式執行存取控制。該應用程式還允許連線受信任裝置。

- **按規則**

  對於某些裝置類型，您可以 選擇使用者或一組使用者，他們將被允許使用裝置、配置裝置存取排程以及讀寫權限。該應用程式還允許 連線受信任的裝置。

配置對**硬碟磁碟機**類型裝置的存取時要小心。如果封鎖對系統磁碟的存取，應用程式可能會在引導作業系統時導致崩潰 (BSOD)。

如果裝置不符合裝置控制分類方案，則無法限制對該裝置的存取。

如何在卡巴斯基安全管理中心管理主控台中按類型控制對裝置的存取

1. 在卡巴斯基安全管理中心管理主控台樹狀目錄中，選取**政策**。
2. 選擇必要的政策並點擊以開啟政策內容。
3. 在政策屬性視窗中，選取**"本機活動控制"**。
4. 在**"裝置控制"**區域中點擊**"設定"**。
5. 選擇**"裝置控制"**核取方塊。
6. 在 **用於封鎖規則的操作模式** 塊中，選擇 **封鎖** 或者 **通知**。
7. 在**裝置控制設定**下，選擇**裝置類型**標籤。

   裝置類型 頁簽顯示裝置控制類別中包括的所有裝置的存取規則。

8. 配置裝置存取規則：

   a. 選擇存取模式：**允許**，**封鎖**，**取決於連線匯流排**，**按規則**。

      要選取「**按規則**」存取模式，您必須雙擊開啟存取規則內容。

   b. 如果您選擇了 **取決於連線匯流排** 存取模式，請轉到 **連線匯流排** 頁簽並配置連線介面的存取規則。

   c. 對於儲存裝置（例如，卸除式磁碟機），您可以 配置個人使用者的存取權限。您也可以配置裝置存取排程並配置讀寫權限。

   d. 如有需要， 配置列印規則。

   e. 如果有需要的話， 設定 Wi-Fi 連線規則。

9. 儲存變更。若要在電腦上套用該政策，請關閉掛鎖。

如何在卡巴斯基安全管理中心網頁主控台中按類型控制對裝置的存取

1. 在網頁主控台的主視窗中，選擇**資產管理 → 政策**。

2. 點擊 Kaspersky Embedded Systems Security 政策的名稱。

   政策內容視窗將開啟。

3. 選擇**"應用程式設定"**標籤。

4. 轉到**本機活動控制 → 裝置控制** 並點擊 **配置** 按鈕。

   開啟**"裝置控制"**視窗。

5. 選擇**"啟用裝置控制"**核取方塊。

6. 在 **用於封鎖規則的操作模式** 塊中，選擇 **封鎖** 或者 **通知**。

7. 在**"裝置控制設定"**塊中， 點擊**"裝置和 wi-fi 網路的存取規則"**。

   一個視窗將開啟，其中包含裝置控制元件類別中包括的所有裝置的存取規則。

8. 配置裝置存取規則：

   a. 選擇存取模式：**允許**，**封鎖**，**取決於連線匯流排**，**按規則**。

      如果下拉式清單中沒有提供存取模式，請雙擊裝置類型開啟存取規則的屬性。

   b. 如果您選擇**取決於連線匯流排**存取模式，則必須返回一般裝置控制設定視窗，點擊**連線匯流排**，並配置連線介面的存取規則。

   c. 對於儲存裝置（例如，卸除式磁碟機），您可以 配置個人使用者的存取權限。您也可以配置裝置存取排程並配置讀寫權限。

   d. 如有需要， 配置列印規則。

   e. 如果有需要的話， 設定 Wi-Fi 連線規則。

9. 儲存變更。若要在電腦上套用該政策，請關閉掛鎖。

如何在應用程式主控台中按類型控制裝置存取

1. 在 Kaspersky Embedded Systems Security 主控台樹狀目錄中，選擇"**電腦控制 → 裝置控制**"。
2. 在 **裝置控制** 節點的結果窗格中，點擊 **內容**。
   內容: 裝置控制視窗將開啟。
3. 選擇"**裝置控制**"核取方塊。
4. 在 **用於封鎖規則的操作模式** 塊中，選擇 **封鎖** 或者 **通知**。
5. 在**裝置控制設定**下，選擇**裝置類型**標籤。
   一個視窗將開啟，其中包含裝置控制元件類別中包括的所有裝置的存取規則。
6. 配置裝置存取規則：
   a. 選擇存取模式：**允許**， **封鎖**，**取決於連線匯流排**，**按規則**。
      要選取「**按規則**」存取模式，您必須雙擊開啟存取規則內容。
   b. 如果您選擇**取決於連線匯流排**存取模式，則必須在**連線匯流排**頁簽上設定連接介面的存取規則。
   c. 對於儲存裝置（例如，卸除式磁碟機），您可以 配置個人使用者的存取權限。您也可以配置裝置存取排程並配置讀寫權限。
   d. 如有需要， 配置列印規則。
   e. 如果有需要的話， 設定 Wi-Fi 連線規則。
7. 儲存變更。

結果，當使用者嘗試存取裝置時，應用程式會根據規則阻止存取。Kaspersky Embedded Systems Security 也會記錄對應的事件。如果您想授予對單一裝置的存取權限，您可以 將這些裝置新增至受信任裝置清單。

Wi-Fi 連線控制

裝置控制可管理電腦（終端）的 Wi-Fi 連線。公共 Wi-Fi 網路可能不安全，使用此類網路可能導致資料損失。裝置控制可讓您封鎖使用者連線到 Wi-Fi 或者只允許連線到受信任網路。例如，您可以允許只連線到足夠安全的公司 Wi-Fi 網路。裝置控制將封鎖存取除受信任清單中指定的 Wi-Fi 網路之外的所有網路。

在執行 Windows 11 的電腦上，您需要啟用位置服務才能控制 Wi-Fi 連線。為此，您需要在作業系統設定中啟用**定位服務**開關（**設定 → 隱私權 → 位置的**）。如果位置服務被停用，Kaspersky Embedded Systems Security 不會控制與 Wi-Fi 網路的連線。

如何在卡巴斯基安全管理中心管理主控台中限制 Wi-Fi 連線

1. 在卡巴斯基安全管理中心管理主控台樹狀目錄中，選取**政策**。
2. 選擇必要的政策並點擊以開啟政策內容。
3. 在政策屬性視窗中，選取"**本機活動控制**"。

4. 在**"裝置控制"**區域中點擊**"設定"**。

5. 選擇**"裝置控制"**核取方塊。

6. 在 **用於封鎖規則的操作模式** 塊中，選擇 **封鎖** 或者 **通知**。

7. 在**裝置控制設定**下，選擇**裝置類型**標籤。
   裝置類型 頁簽顯示裝置控制類別中包括的所有裝置的存取規則。

8. 對於**Wi-Fi**裝置，配置存取規則：

   a. 選擇存取模式：**允許**， **封鎖**， **封鎖但帶有例外**。

   b. 如果選擇了**封鎖但帶有例外**模式，您必須建立受信任的 Wi-Fi 網路清單：

      1. 點擊兩下開啟受信任 **Wi-Fi** 網路列表。

      2. 在開啟的視窗中，點擊**"新增"**按鈕。

      3. 這會開啟一個視窗；在此視窗中設定受信任的 Wi-Fi 網路：

         - **網路名稱**Wi-Fi 的名稱或者 SSID（Service Set Identifier）。
         - **身分驗證類型**連線到 Wi-Fi 網路時使用的身分驗證類型。
         - **加密類型**用於防護 Wi-Fi 流量的加密類型。
         - **註解**有關新增 Wi-Fi 網路的更多資訊。

   您可以在路由器設定中檢視受信任 Wi-Fi 網路的設定。

   > 如果某個 Wi-Fi 網路的設定比對規則中指定的所有設定則其被認定為受信任。

9. 儲存變更。若要在電腦上套用該政策，請關閉掛鎖。

如何在卡巴斯基安全管理中心網頁主控台中限制 Wi-Fi 連線

1. 在網頁主控台的主視窗中，選擇**資產管理 → 政策**。

2. 點擊 Kaspersky Embedded Systems Security 政策的名稱。
   政策內容視窗將開啟。

3. 選擇**"應用程式設定"**標籤。

4. 轉到**本機活動控制 → 裝置控制** 並點擊 **配置** 按鈕。
   開啟**"裝置控制"**視窗。

5. 選擇**"啟用裝置控制"**核取方塊。

6. 在 **用於封鎖規則的操作模式** 塊中，選擇 **封鎖** 或者 **通知**。

7. 在**"裝置控制設定"**塊中， 點擊**"裝置和 wi-fi 網路的存取規則"**。
   一個視窗將開啟，其中包含裝置控制元件類別中包括的所有裝置的存取規則。

8. 按兩下**Wi-Fi**裝置類型開啟存取規則屬性。
9. 選擇存取模式：**允許**， **封鎖**， **封鎖但帶有例外**。
10. 如果選擇了**封鎖但帶有例外**模式，您必須建立受信任的 Wi-Fi 網路清單：
    1. 在"**受信任的 Wi-Fi 網路**"塊中，點擊"**新增**"按鈕。
    2. 這會開啟一個視窗；在此視窗中設定受信任的 Wi-Fi 網路：
       - **網路名稱**Wi-Fi 的名稱或者 SSID（Service Set Identifier）。
       - **身分驗證類型**連線到 Wi-Fi 網路時使用的身分驗證類型。
       - **加密類型**用於防護 Wi-Fi 流量的加密類型。
       - **註釋**有關新增 Wi-Fi 網路的更多資訊。

    您可以在路由器設定中檢視受信任 Wi-Fi 網路的設定。

    > 如果某個 Wi-Fi 網路的設定比對規則中指定的所有設定則其被認定為受信任。

11. 儲存變更。若要在電腦上套用該政策，請關閉掛鎖。

如何在應用程式主控台中限制 Wi-Fi 連線

1. 在 Kaspersky Embedded Systems Security 主控台樹狀目錄中，選擇"**電腦控制 → 裝置控制**"。
2. 在 **裝置控制** 節點的結果窗格中，點擊 **內容**。
   內容: 裝置控制視窗將開啟。
3. 選擇"**裝置控制**"核取方塊。
4. 在 **用於封鎖規則的操作模式** 塊中，選擇 **封鎖** 或者 **通知**。
5. 在**裝置控制設定**下，選擇**裝置類型**標籤。
   一個視窗將開啟，其中包含裝置控制元件類別中包括的所有裝置的存取規則。
6. 對於**Wi-Fi**裝置，配置存取規則：
   a. 選擇存取模式：**允許**， **封鎖**， **封鎖但帶有例外**。
   b. 如果選擇了**封鎖但帶有例外**模式，您必須建立受信任的 Wi-Fi 網路清單：
      1. 點擊兩下開啟受信任 **Wi-Fi** 網路列表。
      2. 在開啟的視窗中，點擊"**新增**"按鈕。
      3. 這會開啟一個視窗；在此視窗中設定受信任的 Wi-Fi 網路：
         - **網路名稱**Wi-Fi 的名稱或者 SSID（Service Set Identifier）。
         - **身分驗證類型**連線到 Wi-Fi 網路時使用的身分驗證類型。

- **加密類型**用於防護 Wi-Fi 流量的加密類型。
- **註解**有關新增 Wi-Fi 網路的更多資訊。

您可以在路由器設定中檢視受信任 Wi-Fi 網路的設定。

如果某個 Wi-Fi 網路的設定比對規則中指定的所有設定則其被認定為受信任。

7. 儲存變更。

結果，當使用者嘗試連線到未被列為受信任的 Wi-Fi 網路時，應用程式將封鎖連線。

列印控制

裝置控制允許配置使用者對本機和網路印表機的存取。

本機印表機控制

Kaspersky Embedded Systems Security 透過以下匯流排控制本機印表機連線：USB，序列連接埠 (COM)，平行連接埠 (LPT)。

Kaspersky Embedded Systems Security 僅在匯流排級別控製本機印表機與 COM 和 LPT 連接埠的連線。即，要防止印表機連線到 COM 和 LPT 連接埠，對於**本機印表機**裝置類型，選擇**取決於連線匯流排**模式並禁止裝置類型連線到 COM 和 LPT 匯流排。

對於連線到 USB 的印表機，應用程式會在兩個級別上進行控制：裝置類型（本機印表機）和連線匯流排（USB）。

您可以選擇以下方式之一透過 USB 存取本機印表機：

- **允許**Kaspersky Embedded Systems Security 向所有使用者授予對本機印表機的完全存取權限。使用者可以使用作業系統提供的方式連線印表機和列印文件。
- **封鎖**Kaspersky Embedded Systems Security 封鎖本機的連線。該應用程式僅允許連連線受信任印表機。
- **取決於連線匯流排**Kaspersky Embedded Systems Security 允許根據 USB 連線狀態（**允許** 或 **封鎖** ）連線到本機印表機。
- **按規則**若要控制列印，您必須新增*列印規則*。在規則中，您可以選擇要允許或封鎖其存取在本機印表機上列印文件的使用者或使用者群組。

網路印表機控制

Kaspersky Embedded Systems Security 允許設定在網路印表機上列印的存取權限。您可以選擇以下一種網路印表機存取模式：

- **允許且不記錄** 。Kaspersky Embedded Systems Security 不控製網路印表機上的列印。該應用程式向所有使用者授予列印存取權限，不會將列印資訊儲存到事件記錄中。
- **允許** Kaspersky Embedded Systems Security 向所有使用者授予在網路印表機上列印的存取權限。
- **封鎖** 。Kaspersky Embedded Systems Security 向所有使用者限制對網路印表機的存取權限。應用程式僅允許存取受信任印表機。
- **按規則**若要控制列印，您必須新增*列印規則*。在規則中，您可以選擇要允許或封鎖其存取在網路印表機上列印文件的使用者或使用者群組。

為印表機新增列印規則

如何在卡巴斯基安全管理中心管理主控台中新增列印規則

1. 在卡巴斯基安全管理中心管理主控台樹狀目錄中，選取**政策**。
2. 選擇必要的政策並點擊以開啟政策內容。
3. 在政策屬性視窗中，選取"**本機活動控制**"。
4. 在"**裝置控制**"區域中點擊"**設定**"。
5. 選擇"**裝置控制**"核取方塊。
6. 在 **用於封鎖規則的操作模式** 塊中，選擇 **封鎖** 或者 **通知**。
7. 在**裝置控制設定**下，選擇**裝置類型**標籤。

   裝置類型 頁簽顯示裝置控制類別中包括的所有裝置的存取規則。
8. 設定印表機存取規則：
   a. 對於**本機印表機** 和 **網路印表機** 裝置類型，配置存取規則：**允許**， **封鎖**，**允許且不記錄** （僅適用於網路印表機），**取決於連線匯流排** （僅適用於本機印表機），**按規則**。
   b. 如果您選擇了 **取決於連線匯流排** 存取模式，請轉到 **連線匯流排** 頁簽並配置連線介面的存取規則。
   c. 如果您選擇**按規則**存取模式，則必須配置列印規則：
      1. 按兩下**本機印表機** 和 **網路印表機**裝置類型開啟存取規則屬性。
      2. 選擇要對其套用列印規則的使用者或使用者群組。要執行此操作，請點擊"**新增**"按鈕。

         這將開啟一個用於新增新列印規則的視窗。

3. 將優先順序分配到*規則項目*。一個規則項目包括以下屬性：使用者帳戶，動作（允許/封鎖）和優先順序。

   規則具有特定的優先順序。如果已將使用者新增到多個群組，則 Kaspersky Embedded Systems Security 會根據具有最高優先順序的規則來管理裝置存取。Kaspersky Embedded Systems Security 允許您分配從 0 到 10,000 的優先順序。值越高，優先順序越高。換言之，值為 0 的項目具有最低的優先順序。

   例如，您可以向 Everyone 群組授予只讀權限，向管理員群組授予讀/寫權限。為此，請為管理員群組分配優先順序 1，為 Everyone 群組分配優先順序 0。

   封鎖規則的優先等級高於允許規則的優先等級。換句話說，如果已將使用者新增到多個群組，並且所有規則的優先順序都相同，則 Kaspersky Embedded Systems Security 會根據任何現有的封鎖規則來管理裝置存取。

4. 在"**動作**"下方，設定使用者在印表機上列印的存取權限。

5. 點擊"**使用者和群組**"然後選擇存取列印的使用者或者使用者群組。您可以在 Active Directory 中、在卡巴斯基安全管理中心的账户清單中或透過手動輸入本機使用者名稱來選擇使用者。卡巴斯基建議僅在無法使用網域使用者帳戶的特殊情況下使用本機使用者帳戶。

6. 單擊"**確定**"。

9. 儲存變更。若要在電腦上套用該政策，請關閉掛鎖。

如何在卡巴斯基安全管理中心網頁主控台中新增列印規則

1. 在網頁主控台的主視窗中，選擇**資產管理 → 政策**。

2. 點擊 Kaspersky Embedded Systems Security 政策的名稱。
   政策內容視窗將開啟。

3. 選擇"**應用程式設定**"標籤。

4. 轉到**本機活動控制 → 裝置控制** 並點擊 **配置** 按鈕。
   開啟"**裝置控制**"視窗。

5. 選擇"**啟用裝置控制**"核取方塊。

6. 在 **用於封鎖規則的操作模式** 塊中，選擇 **封鎖** 或者 **通知**。

7. 在"**裝置控制設定**"塊中， 點擊"**裝置和 wi-fi 網路的存取規則**"。
   一個視窗將開啟，其中包含裝置控制元件類別中包括的所有裝置的存取規則。

8. 設定印表機存取規則：

   a. 對於**本機印表機** 和 **網路印表機** 裝置類型，選擇存取模式：**允許**， **封鎖**，**允許且不記錄** （僅適用於網路印表機），**取決於連線匯流排** （僅適用於本機印表機），**按規則**。
      如果下拉式清單中沒有提供存取模式，請雙擊裝置類型開啟存取規則的屬性。

   b. 如果您選擇**取決於連線匯流排**存取模式，則必須返回裝置控制元件一般設定視窗，點擊**連線匯流排**，並配置連線介面的存取規則。

c. 如果需要配置列印：

1. 按兩下**本機印表機** 或 **網路印表機**裝置類型開啟存取規則屬性。
2. 選擇**按規則**存取模式。
3. 選擇要對其套用列印規則的使用者或使用者群組。要執行此操作，請點擊**"新增"**按鈕。

   這將開啟一個用於新增新列印規則的視窗。
4. 將優先順序分配到*規則項目*。一個規則項目包括以下屬性：使用者帳戶，動作（允許/封鎖）和優先順序。

   規則具有特定的優先順序。如果已將使用者新增到多個群組，則 Kaspersky Embedded Systems Security 會根據具有最高優先順序的規則來管理裝置存取。Kaspersky Embedded Systems Security 允許您分配從 0 到 10,000 的優先順序。值越高，優先順序越高。換言之，值為 0 的項目具有最低的優先順序。

   例如，您可以向 Everyone 群組授予只讀權限，向管理員群組授予讀/寫權限。為此，請為管理員群組分配優先順序 1，為 Everyone 群組分配優先順序 0。

   封鎖規則的優先等級高於允許規則的優先等級。換句話說，如果已將使用者新增到多個群組，並且所有規則的優先順序都相同，則 Kaspersky Embedded Systems Security 會根據任何現有的封鎖規則來管理裝置存取。
5. 在**"操作"**下方，設定使用者在印表機上列印的存取權限。
6. 在**"使用者和群組"**下面點擊**新增**，然後選擇存取列印的使用者或者使用者群組。您可以在 Active Directory 中、在卡巴斯基安全管理中心的账户清單中或透過手動輸入本機使用者名稱來選擇使用者。卡巴斯基建議僅在無法使用網域使用者帳戶的特殊情況下使用本機使用者帳戶。
7. 單擊**"確定"**。

9. 儲存變更。若要在電腦上套用該政策，請關閉掛鎖。

如何在應用程式主控台中新增列印規則

1. 在 Kaspersky Embedded Systems Security 主控台樹狀目錄中，選擇**"電腦控制 → 裝置控制"**。
2. 在 **裝置控制** 節點的結果窗格中，點擊 **內容**。

   內容: 裝置控制視窗將開啟。
3. 選擇**"裝置控制"**核取方塊。
4. 在 **用於封鎖規則的操作模式** 塊中，選擇 **封鎖** 或者 **通知**。
5. 在**裝置控制設定**下，選擇**裝置類型**標籤。

   一個視窗將開啟，其中包含裝置控制元件類別中包括的所有裝置的存取規則。
6. 設定印表機存取規則：

   a. 對於**本機印表機** 和 **網路印表機** 裝置類型，配置存取規則：**允許**， **封鎖**，**允許且不記錄**（僅適用於網路印表機），**取決於連線匯流排**（僅適用於本機印表機），**按規則**。

   b. 如果您選擇了 **取決於連線匯流排** 存取模式，請轉到 **連線匯流排** 頁簽並配置連線介面的存取規則。

c. 如果您選擇**按規則**存取模式，則必須配置列印規則：

1. 按兩下**本機印表機** 和 **網路印表機**裝置類型開啟存取規則屬性。
2. 選擇要對其套用列印規則的使用者或使用者群組。要執行此操作，請點擊"**新增**"按鈕。

   這將開啟一個用於新增新列印規則的視窗。
3. 將優先順序分配到*規則項目*。一個規則項目包括以下屬性：使用者帳戶，動作（允許/封鎖）和優先順序。

   規則具有特定的優先順序。如果已將使用者新增到多個群組，則 Kaspersky Embedded Systems Security 會根據具有最高優先順序的規則來管理裝置存取。Kaspersky Embedded Systems Security 允許您分配從 0 到 10,000 的優先順序。值越高，優先順序越高。換言之，值為 0 的項目具有最低的優先順序。

   例如，您可以向 Everyone 群組授予只讀權限，向管理員群組授予讀/寫權限。為此，請為管理員群組分配優先順序 1，為 Everyone 群組分配優先順序 0。

   封鎖規則的優先等級高於允許規則的優先等級。換句話說，如果已將使用者新增到多個群組，並且所有規則的優先順序都相同，則 Kaspersky Embedded Systems Security 會根據任何現有的封鎖規則來管理裝置存取。
4. 在"**動作**"下方，設定使用者在印表機上列印的存取權限。
5. 點擊"**使用者和群組**"然後選擇存取列印的使用者或者使用者群組。您可以在 Active Directory 中、在卡巴斯基安全管理中心的账户清單中或透過手動輸入本機使用者名稱來選擇使用者。卡巴斯基建議僅在無法使用網域使用者帳戶的特殊情況下使用本機使用者帳戶。
6. 單擊"**確定**"。

7. 儲存變更。

輸入裝置控制（HID）

輸入裝置包括鍵盤、滑鼠、軌跡球、觸控板和其他此類裝置。您可以使用下列介面連線輸入裝置：USB、藍牙、PS/2 連接埠、RS-232 (COM) 連接埠、IR 連接埠等。

Kaspersky Embedded Systems Security 可控制 USB、藍牙滑鼠和鍵盤。裝置控制可記錄輸入裝置連線和斷開連線裝置。

> 當藍牙裝置連線或斷開連線時，應用程式可能會建立有關該裝置的多個事件。原因是作業系統可能會將一個藍牙裝置偵測為多個不同類型的裝置。Kaspersky Embedded Systems Security 還管理藍牙適配器，通過該適配器將裝置作為單獨的裝置進行連線。這就是應用程式為每個偵測到的裝置建立一個事件的原因。

Kaspersky Embedded Systems Security 可讓您允許或禁止使用輸入裝置以及 列出受信任裝置。

如何在卡巴斯基安全管理中心管理主控台中啟用裝置控制

1. 在卡巴斯基安全管理中心管理主控台樹狀目錄中，選取**政策**。
2. 選擇必要的政策並點擊以開啟政策內容。
3. 在政策屬性視窗中，選取"**本機活動控制**"。

4. 在**"裝置控制"**區域中點擊**"設定"**。

5. 選擇**"裝置控制"**核取方塊。

6. 在 **用於封鎖規則的操作模式** 塊中，選擇 **封鎖** 或者 **通知**。

7. 在**裝置控制設定**下，選擇**裝置類型**標籤。
   裝置類型 頁簽顯示裝置控制類別中包括的所有裝置的存取規則。

8. 對於 **藍芽** 裝置類型，選擇存取模式： **允許**，**封鎖**， **允許且不記錄**。
   您可以封鎖或允許所有藍牙裝置，也可以僅允許連線藍牙輸入裝置（HID（人機介面裝置）類別）。

   > 您只能在卡巴斯基安全管理中心網頁主控台中允許連線輸入裝置。您無法在管理主控台 (MMC) 或 Kaspersky Embedded Systems Security 主控台中允許連線輸入裝置。

9. 對於 **USB 鍵盤** 和 **USB 滑鼠** 裝置類型，選擇存取模式：**允許**， **封鎖**，**取決於連線匯流排**。

10. 儲存變更。若要在電腦上套用該政策，請關閉掛鎖。

如何在卡巴斯基安全管理中心網頁主控台中啟用裝置控制

1. 在網頁主控台的主視窗中，選擇**資產管理 → 政策**。

2. 點擊 Kaspersky Embedded Systems Security 政策的名稱。
   政策內容視窗將開啟。

3. 選擇**"應用程式設定"**標籤。

4. 轉到**本機活動控制 → 裝置控制** 並點擊 **配置** 按鈕。
   開啟**"裝置控制"**視窗。

5. 選擇**"啟用裝置控制"**核取方塊。

6. 在 **用於封鎖規則的操作模式** 塊中，選擇 **封鎖** 或者 **通知**。

7. 在**"裝置控制設定"**塊中， 點擊**"裝置和 wi-fi 網路的存取規則"**。
   一個視窗將開啟，其中包含裝置控制元件類別中包括的所有裝置的存取規則。

8. 點擊**藍芽**裝置類型開啟存取規則屬性。

9. 選擇存取模式：**允許**， **封鎖**， **允許且不記錄**。
   您可以封鎖或允許所有藍牙裝置，也可以僅允許連線藍牙輸入裝置（HID（人機介面裝置）類別）。

10. 對於 **USB 鍵盤** 和 **USB 滑鼠** 裝置類型，選擇存取模式：**允許**， **封鎖**，**取決於連線匯流排**。

11. 儲存變更。若要在電腦上套用該政策，請關閉掛鎖。

如何在應用程式主控台中設定裝置控制

1. 在 Kaspersky Embedded Systems Security 主控台樹狀目錄中，選擇**"電腦控制 → 裝置控制"**。
2. 在 **裝置控制** 節點的結果窗格中，點擊 **內容**。
   內容: 裝置控制視窗將開啟。
3. 選擇**"裝置控制"**核取方塊。
4. 在 **用於封鎖規則的操作模式** 塊中，選擇 **封鎖** 或者 **通知**。
5. 在**裝置控制設定**下，選擇**裝置類型**標籤。
   一個視窗將開啟，其中包含裝置控制元件類別中包括的所有裝置的存取規則。
6. 對於 **藍芽** 裝置類型，選擇存取模式： **允許**，**封鎖**， **允許且不記錄**。
   您可以封鎖或允許所有藍牙裝置，也可以僅允許連線藍牙輸入裝置（HID（人機介面裝置）類別）。

   > 您只能在卡巴斯基安全管理中心網頁主控台中允許連線輸入裝置。您無法在管理主控台 (MMC) 或 Kaspersky Embedded Systems Security 主控台中允許連線輸入裝置。

7. 對於 **USB 鍵盤** 和 **USB 滑鼠** 裝置類型，選擇存取模式：**允許**， **封鎖**，**取決於連線匯流排**。
8. 儲存變更。

管理存取行動裝置的權限

Kaspersky Embedded Systems Security 可讓您控制對執行 Android 和 iOS 的行動裝置上資料的存取。行動裝置屬於攜帶式裝置 (MTP) 類別。因此，若要配置對行動裝置上的資料的存取，您需要編輯攜帶式裝置 (MTP) 的存取設定。

當某個行動裝置連線到電腦時，作業系統會確定裝置類型。如果電腦上安裝了 iTunes 或類似的應用程式 Android Debug Bridge（如需 ADB 應用程式的詳細資訊，請參閱知識庫 和 Android 技術支援網站 ），作業系統會將行動裝置識別為 ADB 或 iTunes 裝置。在所有其他情況下，作業系統可能將行動裝置類型辨識為用於檔案傳輸的可攜式裝置 (MTP)、用於影像傳輸的 PTP 裝置（相機）或其他裝置。裝置類型取決於行動裝置的型號和所選的 USB 連線模式。Kaspersky Embedded Systems Security 可讓您在 ADB 應用程式、iTunes 或檔案管理器中，設定對行動裝置上資料的個別存取權限。在所有其他情況下，裝置控制允許根據攜帶式裝置 (MTP) 存取規則存取行動裝置。

存取行動裝置的權限

行動裝置屬於攜帶式裝置 (MTP) 類別，因此它們的設定相同。您可以選擇以下行動裝置存取模式之一：

- **允許**Kaspersky Embedded Systems Security 允許完整存取行動裝置。您可以使用檔案管理器或 ADB 和 iTunes 應用程式，開啟、建立、修改、複製或刪除行動裝置上的檔案。您還可以通過將行動裝置連線到電腦的 USB 連接埠來為裝置的電池充電。
- **封鎖**Kaspersky Embedded Systems Security 會限制在檔案管理器以及 ADB 和 iTunes 應用程式中存取行動裝置。應用程式僅允許存取受信任的行動裝置。您還可以通過將行動裝置連線到電腦的 USB 連接埠來為裝置的電池充電。
- **取決於連線匯流排**Kaspersky Embedded Systems Security 允許根據 USB 匯流排連線狀態（**允許** 或 **封鎖**）連線到行動裝置。
- **按規則**Kaspersky Embedded Systems Security 會根據規則限制對行動裝置的存取。在規則中，您可以設定存取權限（讀取/寫入）、選取可存取行動裝置的使用者或群組，以及設定行動裝置的存取排程。您也可以透過 ADB 和 iTunes 應用程式限制對行動裝置上資料的存取。

配置行動裝置存取規則

攜帶式裝置 (MTP)、ADB 裝置和 iTunes 裝置的存取規則配置不同。對於攜帶式裝置 (MTP) 和 ADB 裝置，您可以為單個使用者或使用者群組配置規則，並為何時套用規則建立排程。對於 iTunes 裝置，您不能這樣做。您只能允許或拒絕所有使用者透過 iTunes 應用程式存取資料。

如何在卡巴斯基安全管理中心管理主控台中配置行動裝置存取規則

1. 在卡巴斯基安全管理中心管理主控台樹狀目錄中，選取**政策**。
2. 選擇必要的政策並點擊以開啟政策內容。
3. 在政策屬性視窗中，選取**"本機活動控制"**。
4. 在**"裝置控制"**區域中點擊**"設定"**。
5. 在**裝置控制設定**下，選擇**裝置類型**標籤。
   表格列出了裝置控制元件分類中存在的所有裝置的存取規則。
6. 在 **可攜式裝置(MTP)** 裝置類型的內容功能表中，配置行動裝置存取模式：**允許**、**封鎖** 或 **取決於連線匯流排**。
7. 若要配置行動裝置存取規則，請點擊兩下開啟規則清單。
8. 配置行動裝置存取規則：
   a. 在**"存取規則"**塊中，點擊**"新增"**按鈕。
      這將開啟一個用於新增新行動裝置存取規則的視窗。
   b. 在**優先**欄位中，設定規則寫入優先順序。規則包括以下屬性：使用者帳戶，排程，權限（讀取/寫入/ADB 存取）和優先順序。

規則具有特定的優先順序。如果已將使用者新增到多個群組，則 Kaspersky Embedded Systems Security 會根據具有最高優先順序的規則來管理裝置存取。Kaspersky Embedded Systems Security 允許您分配從 0 到 10,000 的優先順序。值越高，優先順序越高。換言之，值為 0 的項目具有最低的優先順序。

例如，您可以向 Everyone 群組授予只讀權限，向管理員群組授予讀/寫權限。為此，請為管理員群組分配優先順序 1，為 Everyone 群組分配優先順序 0。

封鎖規則的優先等級高於允許規則的優先等級。換句話說，如果已將使用者新增到多個群組，並且所有規則的優先順序都相同，則 Kaspersky Embedded Systems Security 會根據任何現有的封鎖規則來管理裝置存取。

c. 在**"使用者和/或使用者群組規則"**，選擇使用者或使用者群組。您可以在 Active Directory 中、在卡巴斯基安全管理中心的账户清單中或透過手動輸入本機使用者名稱來選擇使用者。卡巴斯基建議僅在無法使用網域使用者帳戶的特殊情況下使用本機使用者帳戶。

d. 單擊**"確定"**。

9. 在**"所選存取規則的排程"**下方，設定使用者的行動裝置存取排程。

無法為 ADB 裝置配置單獨的存取排程。您可以為 ADB 裝置和攜帶式裝置 (MTP) 配置通用存取排程。

10. 在檔案管理器中配置使用者對行動裝置的存取權限（**讀取** / **寫入**）。

11. 使用**透過 ADB 存取**核取方塊配置透過 ADB 應用程式對行動裝置上資料進行存取 。

如果清除該核取方塊，當連線行動裝置時，ADB 應用程式將被阻止偵測該裝置。

12. 在**透過 iTunes 存取**下，配置透過 iTunes 應用程式對行動裝置上的資料進行存取。

Kaspersky Embedded Systems Security 會為所有使用者套用透過 iTunes 應用程式存取行動裝置的設定。無法為 iTunes 裝置配置單獨的存取排程。

13. 儲存變更。

如何在卡巴斯基安全管理中心網頁主控台中配置行動裝置存取規則

1. 在網頁主控台的主視窗中，選擇**資產管理 → 政策**。

2. 點擊 Kaspersky Embedded Systems Security 政策的名稱。

政策內容視窗將開啟。

3. 選擇**"應用程式設定"**標籤。

4. 轉到**本機活動控制 → 裝置控制** 並點擊 **配置** 按鈕。

開啟**"裝置控制"**視窗。

5. 在**"裝置控制設定"**塊中，點擊**"裝置和 wi-fi 網路的存取規則"**連接。

表格列出了裝置控制元件分類中存在的所有裝置的存取規則。

6. 選取**"可攜式裝置(MTP)"**裝置類型。

這將開啟攜帶式裝置 (MTP) 存取權限。

7. 配置行動裝置存取模式：**允許**, **封鎖**, **取決於連線匯流排**, or **按規則**。

8. 在**透過 iTunes 存取**下，配置透過 iTunes 應用程式對行動裝置上的資料進行存取。

   Kaspersky Endpoint Security 透過 iTunes 應用程式為所有使用者套用行動裝置存取設定。無法為 iTunes 裝置配置單獨的存取排程。

9. 如果選擇**"按規則"**模式，必須為裝置新增存取規則。為此，在**"使用者"**下方，點擊**"新增"**按鈕並配置行動裝置存取規則：

   a. 在**優先順序**欄位中，設定規則寫入優先順序。規則包括以下屬性：使用者帳戶，排程，權限（讀取/寫入/ADB 存取）和優先順序。

      規則具有特定的優先順序。如果已將使用者新增到多個群組，則 Kaspersky Embedded Systems Security 會根據具有最高優先順序的規則來管理裝置存取。Kaspersky Embedded Systems Security 允許您分配從 0 到 10,000 的優先順序。值越高，優先順序越高。換言之，值為 0 的項目具有最低的優先順序。

      例如，您可以向 Everyone 群組授予只讀權限，向管理員群組授予讀/寫權限。為此，請為管理員群組分配優先順序 1，為 Everyone 群組分配優先順序 0。

      封鎖規則的優先等級高於允許規則的優先等級。換句話說，如果已將使用者新增到多個群組，並且所有規則的優先順序都相同，則 Kaspersky Embedded Systems Security 會根據任何現有的封鎖規則來管理裝置存取。

   b. 在**"使用者"**下方，選擇存取行動裝置的使用者或者使用者群組。您可以在 Active Directory 中、在卡巴斯基安全管理中心的账户清單中或透過手動輸入本機使用者名稱來選擇使用者。卡巴斯基建議僅在無法使用網域使用者帳戶的特殊情況下使用本機使用者帳戶。

   c. 在**"裝置存取排程"**下方，設定使用者的行動裝置存取排程。

      無法為 ADB 裝置配置單獨的存取排程。您可以為 ADB 裝置和攜帶式裝置 (MTP) 配置通用存取排程。

   d. 在檔案管理器中配置使用者對行動裝置的存取權限（**讀取 / 寫入**）。

   e. 使用**透過 ADB 存取**核取方塊配置透過 ADB 應用程式對行動裝置上資料進行存取 。

      如果清除該核取方塊，當連線行動裝置時，ADB 應用程式將被阻止偵測該裝置。

10. 儲存變更。

如何在應用程式主控台中配置行動裝置存取規則

1. 在 Kaspersky Embedded Systems Security 主控台樹狀目錄中，選擇**"電腦控制 → 裝置控制"**。

2. 在 **裝置控制** 節點的結果窗格中，點擊 **內容**。

   內容: 裝置控制視窗將開啟。

3. 選擇**"裝置類型"**標籤。

   一個視窗將開啟，其中包含裝置控制元件類別中包括的所有裝置的存取規則。

4. 在 **可攜式裝置(MTP)** 裝置類型的內容功能表中，配置行動裝置存取模式：**允許**、**封鎖** 或 **取決於連線匯流排**。

5. 若要配置行動裝置存取規則，請點擊兩下開啟規則清單。

6. 配置行動裝置存取規則：

   a. 在"**存取規則**"塊中，點擊"**新增**"按鈕。

      這將開啟一個用於新增新行動裝置存取規則的視窗。

   b. 在**優先**欄位中，設定規則寫入優先順序。規則包括以下屬性：使用者帳戶，排程，權限（讀取/寫入/ADB 存取）和優先順序。

      規則具有特定的優先順序。如果已將使用者新增到多個群組，則 Kaspersky Embedded Systems Security 會根據具有最高優先順序的規則來管理裝置存取。Kaspersky Embedded Systems Security 允許您分配從 0 到 10,000 的優先順序。值越高，優先順序越高。換言之，值為 0 的項目具有最低的優先順序。

      例如，您可以向 Everyone 群組授予只讀權限，向管理員群組授予讀/寫權限。為此，請為管理員群組分配優先順序 1，為 Everyone 群組分配優先順序 0。

      封鎖規則的優先等級高於允許規則的優先等級。換句話說，如果已將使用者新增到多個群組，並且所有規則的優先順序都相同，則 Kaspersky Embedded Systems Security 會根據任何現有的封鎖規則來管理裝置存取。

   c. 在"**使用者和/或使用者群組規則**"，選擇使用者或使用者群組。您可以在 Active Directory 中、在卡巴斯基安全管理中心的账户清單中或透過手動輸入本機使用者名稱來選擇使用者。卡巴斯基建議僅在無法使用網域使用者帳戶的特殊情況下使用本機使用者帳戶。

   d. 單擊"**確定**"。

7. 在"**所選存取規則的排程**"下方，設定使用者的行動裝置存取排程。

   無法為 ADB 裝置配置單獨的存取排程。您可以為 ADB 裝置和攜帶式裝置 (MTP) 配置通用存取排程。

8. 在檔案管理器中配置使用者對行動裝置的存取權限（**讀取** / **寫入**）。

9. 使用**透過 ADB 存取**核取方塊配置透過 ADB 應用程式對行動裝置上資料進行存取 。

   如果清除該核取方塊，當連線行動裝置時，ADB 應用程式將被阻止偵測該裝置。

10. 在**透過 iTunes 存取**下，配置透過 iTunes 應用程式對行動裝置上的資料進行存取。

    Kaspersky Embedded Systems Security 會為所有使用者套用透過 iTunes 應用程式存取行動裝置的設定。無法為 iTunes 裝置配置單獨的存取排程。

11. 儲存變更。

結果，使用者對行動裝置的存取會根據規則受到限制。如果您在 ADB 和 iTunes 應用程式中禁止存取行動裝置，當您連線行動裝置時，ADB 和 iTunes 應用程式將被禁止偵測該行動裝置。

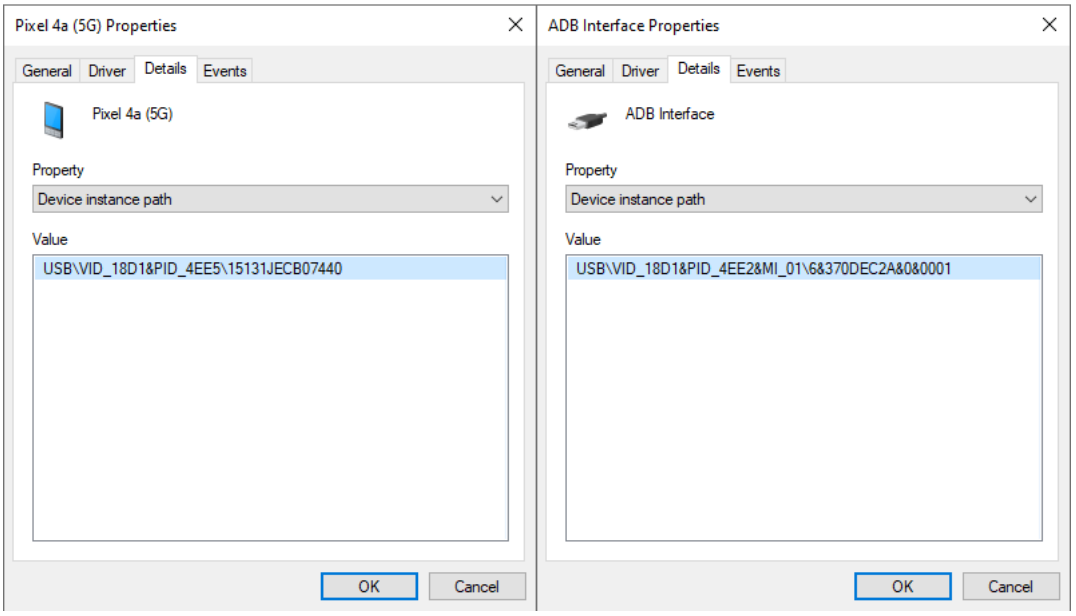
受信任行動裝置

新增受信任行動裝置的過程和新增其它類型受信任裝置的過程一模一樣。您可以依據 ID 或者裝置型號新增行動裝置。

若要依據 ID 新增受信任行動裝置，您將需要一個唯一 ID（Hardware ID – HWID）。您可以使用作業系統工具在裝置內容中找到 ID（請見下圖）。Device Manager工具可讓您做到這點。攜帶式裝置（MTP）和 ADB、iTunes 裝置的 ID 即使對於同一個行動裝置也不同。攜帶式裝置 (MTP) 的 ID 可能如下所示：`15131JECB07440`。ADB 裝置的 ID 可能如下所示：`6&370DEC2A&0&0001`。如果要新增多個特定裝置，則按 ID 新增裝置很方便。您也可以使用遮罩。

如果在將裝置連線到電腦後安裝了 ADB 或 iTunes 應用程式，則該裝置的唯一 ID 可能會重設。也就是說，Kaspersky Embedded Systems Security 會將此裝置識別為新裝置。如果該裝置受信任，請再次將其新增至受信任清單。

若要按裝置型號新增受信任行動裝置，您將需要其Vendor ID (VID) 和 Product ID (PID)。您可以使用作業系統工具在裝置內容中找到 ID（請見下圖）。用於輸入 VID 和 PID 的範本：`VID_18D1&PID_4EE5`。如果在組織中使用特定型號的裝置，則按型號新增裝置很方便。這樣，您就可以新增該型號的所有裝置了。



裝置管理器中的裝置 ID

監視卸除式磁碟機的使用

監視卸除式磁碟機的使用包括：

- 檢視卸除式磁碟機上的檔案的操作。
- 檢視受信任卸除式磁碟機的連線和斷開連線。

  Kaspersky Embedded Systems Security 允許檢視所有受信任裝置、而不只是卸除式磁碟機的連線和斷開連線。您可以為裝置控制元件的通知設定中開啟事件記錄。事件的嚴重性等級為*資訊*。

如何在卡巴斯基安全管理中心管理主控台中啟用卸除式磁碟機上的檔案操作監控

1. 在卡巴斯基安全管理中心管理主控台樹狀目錄中，選取**政策**。
2. 選擇必要的政策並點擊以開啟政策內容。
3. 在政策屬性視窗中，選取**"本機活動控制"**。
4. 在**"裝置控制"**區域中點擊**"設定"**。

5. 選擇**"裝置控制"**核取方塊。

6. 在 **用於封鎖規則的操作模式** 塊中，選擇 **封鎖** 或者 **通知**。

7. 在**裝置控制設定**下，選擇**裝置類型**標籤。
   裝置類型 頁簽顯示裝置控制類別中包括的所有裝置的存取規則。

8. 選擇**卸除式磁碟機**裝置類型並點擊**記錄**按鈕。
   這將開啟**"**事件記錄**"**視窗。

9. 選擇**"啟用記錄"**核取方塊。

10. 在**"檔案操作"**塊中，選擇要監視的操作：**寫入**， **刪除**。

11. 在**"依檔案格式篩選"**塊中，選擇其相關操作應由裝置控制進行記錄的檔案格式。

12. 選擇要監視其卸除式磁碟機使用情況的使用者或使用者群組。

13. 儲存變更。若要在電腦上套用該政策，請關閉掛鎖。

如何在卡巴斯基安全管理中心網頁主控台中啟用卸除式磁碟機上的檔案操作監控

1. 在網頁主控台的主視窗中，選擇**資產管理 → 政策**。

2. 點擊 Kaspersky Embedded Systems Security 政策的名稱。
   政策內容視窗將開啟。

3. 選擇**"應用程式設定"**標籤。

4. 轉到**本機活動控制 → 裝置控制** 並點擊 **配置** 按鈕。
   開啟**"裝置控制"**視窗。

5. 選擇**"啟用裝置控制"**核取方塊。

6. 在 **用於封鎖規則的操作模式** 塊中，選擇 **封鎖** 或者 **通知**。

7. 在**"裝置控制設定"**塊中， 點擊**"裝置和 wi-fi 網路的存取規則"**。
   一個視窗將開啟，其中包含裝置控制元件類別中包括的所有裝置的存取規則。

8. 按兩下**卸除式磁碟機**裝置類型開啟存取規則屬性。

9. 在開啟的視窗中選擇**"記錄"**標籤。

10. 將切換開關設定為 **記錄已啟用**。

11. 在**"檔案操作"**塊中，選擇要監視的操作：**寫入**， **刪除**。

12. 在**"依檔案格式篩選"**塊中，選擇其相關操作應由裝置控制進行記錄的檔案格式。

13. 選擇要監視其卸除式磁碟機使用情況的使用者或使用者群組。

14. 儲存變更。若要在電腦上套用該政策，請關閉掛鎖。

如何在應用程式主控台中啟用卸除式磁碟機上的檔案操作監控

1. 在 Kaspersky Embedded Systems Security 主控台樹狀目錄中，選擇“**電腦控制 → 裝置控制**”。
2. 在 **裝置控制** 節點的結果窗格中，點擊 **內容**。
   內容: 裝置控制視窗將開啟。
3. 選擇“**裝置控制**”核取方塊。
4. 在 **用於封鎖規則的操作模式** 塊中，選擇 **封鎖** 或者 **通知**。
5. 在**裝置控制設定**下，選擇**裝置類型**標籤。
   一個視窗將開啟，其中包含裝置控制元件類別中包括的所有裝置的存取規則。
6. 選擇**卸除式磁碟機**裝置類型並點擊**記錄**按鈕。
   這將開啟“事件記錄”視窗。
7. 選擇“**啟用記錄**”核取方塊。
8. 在“**檔案操作**“塊中，選擇要監視的操作：**寫入**， **刪除**。
9. 在“**依檔案格式篩選**“塊中，選擇其相關操作應由裝置控制進行記錄的檔案格式。
10. 選擇要監視其卸除式磁碟機使用情況的使用者或使用者群組。
11. 儲存變更。

因此，當使用者在卸除式磁碟機上寫入檔案或刪除檔案時，Kaspersky Embedded Systems Security 會將此類操作的資訊寫入事件記錄並將事件傳送至卡巴斯基安全管理中心。您可以在“**事件**“索引標籤上“**管理伺服器**”節點的工作區中的卡巴斯基安全管理中心主控台中檢視與卸除式磁碟機上的檔案關聯的事件。要使事件顯示在本機 Kaspersky Embedded Systems Security 事件記錄中，您必須在裝置控制元件的通知設定中選擇“**檔案操作已執行**“核取方塊。

管理存取藍牙裝置的權限

Kaspersky Embedded Systems Security 允許管理對藍牙裝置的存取。藍牙裝置包括無線鍵盤、滑鼠、耳機、印表機等。您還可以使用藍牙進行通信，例如與行動裝置通信。

當藍牙裝置連線或斷開連線時，應用程式可能會建立有關該裝置的多個事件。原因是作業系統可能會將一個藍牙裝置偵測為多個不同類型的裝置。Kaspersky Embedded Systems Security 還管理藍牙適配器，通過該適配器將裝置作為單獨的裝置進行連線。這就是應用程式為每個偵測到的裝置建立一個事件的原因。

您可以選擇以下藍牙裝置存取模式之一：

- **允許且不記錄**。Kaspersky Embedded Systems Security 允許連線任何藍牙裝置，不會在事件日誌中儲存有關連線的資訊。您可以連線藍牙輸入裝置（鍵盤、滑鼠等）、通過藍牙傳送資料、管理其他藍牙裝置（耳機等）。
- **允許**。Kaspersky Embedded Systems Security 允許連線任何藍牙裝置。您可以連線藍牙輸入裝置（鍵盤、滑鼠等）、通過藍牙傳送資料、管理其他藍牙裝置（耳機等）。
- **封鎖**。Kaspersky Embedded Systems Security 限制對藍牙裝置的存取。您可以僅允許連線藍牙輸入裝置（人機接口裝置類別）。這些裝置包括鍵盤、滑鼠、操縱桿等。

無法建立受信任的藍牙裝置清單。如果您限制了對藍牙裝置的存取，則只能連線藍牙輸入裝置。

您只能在應用程式主控台或者卡巴斯基安全管理中心網頁主控台中允許連線輸入裝置。不只能在卡巴斯基安全管理中心管理主控台中允許連線輸入裝置。

如何在卡巴斯基安全管理中心管理主控台中配置藍牙裝置存取規則

1. 在卡巴斯基安全管理中心管理主控台樹狀目錄中，選取**政策**。
2. 選擇必要的政策並點擊以開啟政策內容。
3. 在政策視窗中，選擇 **本機活動控制 → 裝置控制** 然後點擊 **設定**。
4. 在**裝置控制設定**下，選擇**裝置類型**標籤。

   表格列出了裝置控制元件分類中存在的所有裝置的存取規則。
5. 在**"藍芽"**裝置類型的內容功能表中，配置藍牙裝置存取模式：**允許**，**封鎖**，**允許且不記錄**。

   如果您封鎖了存取藍牙裝置的權限，則只可以在應用程式主控台或卡巴斯基安全管理中心網頁主控台中允許連線輸入裝置（鍵盤、滑鼠等）。不只能在卡巴斯基安全管理中心管理主控台中允許連線輸入裝置。
6. 儲存變更。

如何在卡巴斯基安全管理中心網頁主控台中配置藍牙裝置存取規則

1. 在網頁主控台的主視窗中，選擇**資產管理 → 政策**。
2. 點擊 Kaspersky Embedded Systems Security 政策的名稱。

   政策內容視窗將開啟。
3. 選擇**"應用程式設定"**標籤。
4. 在政策視窗中，選擇 **本機活動控制 → 裝置控制** 然後點擊 **設定**。
5. 在**"裝置控制設定"**塊中，點擊**"裝置和 wi-fi 網路的存取規則"**連接。

   表格列出了裝置控制元件分類中存在的所有裝置的存取規則。

6. 選取"**藍芽**"裝置類型。

   這將開啟藍牙裝置存取設定。

7. 配置藍牙裝置存取模式：**允許**，**封鎖**，**允許且不記錄**。

8. 如果選擇**封鎖**模式，您可以允許只連線藍牙輸入裝置（鍵盤、滑鼠等）。為此，在 **排除項目** 下面，選擇 **輸入裝置（滑鼠和鍵盤）** 核取方塊。

9. 儲存變更。

如何在應用程式主控台中配置藍牙裝置存取規則

1. 在 Kaspersky Embedded Systems Security 主控台樹狀目錄中，選擇"**電腦控制 → 裝置控制**"。

2. 在 **裝置控制** 節點的結果窗格中，點擊 **內容**。

   內容: 裝置控制視窗將開啟。

3. 在**裝置控制設定**下，選擇**裝置類型**標籤。

   表格列出了裝置控制元件分類中存在的所有裝置的存取規則。

4. 在**存取**下配置藍牙裝置存取模式：**允許**，**封鎖**，**允許且不記錄**。

5. 如果選擇**封鎖**模式，您可以允許只連線藍牙輸入裝置（鍵盤、滑鼠等）。為此，在 **排除項目** 下面，選擇 **輸入裝置（滑鼠和鍵盤）** 核取方塊。

6. 儲存變更。

區分使用者對裝置的存取權限

您可以按裝置類型或受信任裝置設定使用者存取權限。

按裝置類型區分使用者存取權限

裝置控制允許在*儲存裝置*上配置使用者對資料的存取權限。對於此類裝置，您可以配置寫入和讀取權限。裝置控制支援以下類型的儲存裝置：

- 硬碟磁碟機
- 卸除式磁碟機
- 軟碟
- CD/DVD 磁碟機
- 可攜式裝置 (MTP) 可攜式裝置 (MTP) 包括（例如）行動裝置、相機、媒體播放器等。

例如，透過這種方式，您可以僅允許管理員群組使用卸除式媒體。對於其他裝置類型，您可以拒絕或允許所有使用者存取。您還可以 設定使用者使用印表機的存取權限。

如何在卡巴斯基安全管理中心管理主控台中設定使用者對卸除式磁碟機上的資料的存取權限

1. 在卡巴斯基安全管理中心管理主控台樹狀目錄中，選取**政策**。
2. 選擇必要的政策並點擊以開啟政策內容。
3. 在政策屬性視窗中，選取**"本機活動控制"**。
4. 在**"裝置控制"**區域中點擊**"設定"**。
5. 選擇**"裝置控制"**核取方塊。
6. 在 **用於封鎖規則的操作模式** 塊中，選擇 **封鎖** 或者 **通知**。
7. 在**裝置控制設定**下，選擇**裝置類型**標籤。

   裝置類型 頁簽顯示裝置控制類別中包括的所有裝置的存取規則。
8. 若要配置儲存裝置存取規則，請點擊兩下開啟規則清單。
9. 配置儲存裝置存取規則：

   a. 在**"存取規則"**塊中，點擊**"新增"**按鈕。

   這將開啟一個用於新增新儲存裝置存取規則的視窗。

   b. 在**優先**欄位中，設定*規則寫入*優先順序。規則包括以下屬性：使用者帳戶，排程，權限（讀取/寫入）和優先順序。

   規則具有特定的優先順序。如果已將使用者新增到多個群組，則 Kaspersky Embedded Systems Security 會根據具有最高優先順序的規則來管理裝置存取。Kaspersky Embedded Systems Security 允許您分配從 0 到 10,000 的優先順序。值越高，優先順序越高。換言之，值為 0 的項目具有最低的優先順序。

   例如，您可以向 Everyone 群組授予只讀權限，向管理員群組授予讀/寫權限。為此，請為管理員群組分配優先順序 1，為 Everyone 群組分配優先順序 0。

   封鎖規則的優先等級高於允許規則的優先等級。換句話說，如果已將使用者新增到多個群組，並且所有規則的優先順序都相同，則 Kaspersky Embedded Systems Security 會根據任何現有的封鎖規則來管理裝置存取。

   c. 在**"使用者和/或使用者群組規則"**，選擇使用者或使用者群組。您可以在 Active Directory 中、在卡巴斯基安全管理中心的账户清單中或透過手動輸入本機使用者名稱來選擇使用者。卡巴斯基建議僅在無法使用網域使用者帳戶的特殊情況下使用本機使用者帳戶。

   d. 單擊**"確定"**。
10. 在**"所選存取規則的排程"**下方，設定使用者的儲存裝置存取排程。

    例如，您可以允許使用者僅在工作時間使用儲存裝置。
11. 在檔案管理器中配置使用者對儲存裝置的存取權限（**讀取 / 寫入**）。
12. 儲存變更。若要在電腦上套用該政策，請關閉掛鎖。

如何在卡巴斯基安全管理中心網頁主控台中設定使用者對儲存裝置上的資料的存取權限

1. 在網頁主控台的主視窗中，選擇**資產管理 → 政策**。
2. 點擊 Kaspersky Embedded Systems Security 政策的名稱。

   政策內容視窗將開啟。

3. 選擇**"應用程式設定"**標籤。

4. 轉到**本機活動控制 → 裝置控制** 並點擊 **配置** 按鈕。

   開啟**"裝置控制"**視窗。

5. 選擇**"啟用裝置控制"**核取方塊。

6. 在 **用於封鎖規則的操作模式** 塊中，選擇 **封鎖** 或者 **通知**。

7. 在**"裝置控制設定"**塊中， 點擊**"裝置和 wi-fi 網路的存取規則"**。

   一個視窗將開啟，其中包含裝置控制元件類別中包括的所有裝置的存取規則。

8. 在 **存取儲存裝置** 塊中，開啟儲存裝置存取規則的屬性。

9. 配置儲存裝置存取規則：

   a. 在**"使用者"**塊中，點擊**"新增"**按鈕。

      這將開啟一個用於新增新儲存裝置存取規則的視窗。

   b. 在**優先順序**欄位中，設定*規則寫入*優先順序。規則包括以下屬性：使用者帳戶，排程，權限（讀取/寫入）和優先順序。

      規則具有特定的優先順序。如果已將使用者新增到多個群組，則 Kaspersky Embedded Systems Security 會根據具有最高優先順序的規則來管理裝置存取。Kaspersky Embedded Systems Security 允許您分配從 0 到 10,000 的優先順序。值越高，優先順序越高。換言之，值為 0 的項目具有最低的優先順序。

      例如，您可以向 Everyone 群組授予只讀權限，向管理員群組授予讀/寫權限。為此，請為管理員群組分配優先順序 1，為 Everyone 群組分配優先順序 0。

      封鎖規則的優先等級高於允許規則的優先等級。換句話說，如果已將使用者新增到多個群組，並且所有規則的優先順序都相同，則 Kaspersky Embedded Systems Security 會根據任何現有的封鎖規則來管理裝置存取。

   c. 在**"使用者"**，選擇使用者或使用者群組。您可以在 Active Directory 中、在卡巴斯基安全管理中心的账户清單中或透過手動輸入本機使用者名稱來選擇使用者。卡巴斯基建議僅在無法使用網域使用者帳戶的特殊情況下使用本機使用者帳戶。

   d. 在**"裝置存取排程"**下方，設定使用者的儲存裝置存取排程。

      例如，您可以允許使用者僅在工作時間使用儲存裝置。

   e. 在檔案管理器中配置使用者對儲存裝置的存取權限（**讀取 / 寫入**）。

   f. 點擊**"確定"**。

10. 儲存變更。若要在電腦上套用該政策，請關閉掛鎖。

如何在 Kaspersky Embedded Systems Security 主控台中設定使用者對儲存裝置上的資料的存取權限

1. 在 Kaspersky Embedded Systems Security 主控台樹狀目錄中，選擇**"電腦控制 → 裝置控制"**。

2. 在 **裝置控制** 節點的結果窗格中，點擊 **內容**。

   內容: 裝置控制視窗將開啟。

3. 選擇**"裝置控制"**核取方塊。

4. 在 **用於封鎖規則的操作模式** 塊中，選擇 **封鎖** 或者 **通知**。

5. 在**裝置控制設定**下，選擇**裝置類型**標籤。

   一個視窗將開啟，其中包含裝置控制元件類別中包括的所有裝置的存取規則。

6. 若要配置儲存裝置存取規則，請點擊兩下開啟規則清單。

7. 配置儲存裝置存取規則：

   a. 在"**存取規則**"塊中，點擊"**新增**"按鈕。

      這將開啟一個用於新增新儲存裝置存取規則的視窗。

   b. 在**規則的優先順序**欄位中，設定*規則寫入*優先順序。規則包括以下屬性：使用者帳戶，排程，權限（讀取/寫入）和優先順序。

      規則具有特定的優先順序。如果已將使用者新增到多個群組，則 Kaspersky Embedded Systems Security 會根據具有最高優先順序的規則來管理裝置存取。Kaspersky Embedded Systems Security 允許您分配從 0 到 10,000 的優先順序。值越高，優先順序越高。換言之，值為 0 的項目具有最低的優先順序。

      例如，您可以向 Everyone 群組授予只讀權限，向管理員群組授予讀/寫權限。為此，請為管理員群組分配優先順序 1，為 Everyone 群組分配優先順序 0。

      封鎖規則的優先等級高於允許規則的優先等級。換句話說，如果已將使用者新增到多個群組，並且所有規則的優先順序都相同，則 Kaspersky Embedded Systems Security 會根據任何現有的封鎖規則來管理裝置存取。

   c. 在"**使用者和/或使用者群組規則**"，選擇使用者或使用者群組。您可以選擇 Active Directory 中的使用者或手動輸入本機使用者名稱。卡巴斯基建議僅在無法使用網域使用者帳戶的特殊情況下使用本機使用者帳戶。

   d. 單擊"**確定**"。

8. 在"**所選存取規則的排程**"下方，設定使用者的儲存裝置存取排程。

   例如，您可以允許使用者僅在工作時間使用儲存裝置。

9. 在檔案管理器中配置使用者對儲存裝置的存取權限（**讀取 / 寫入**）。

10. 儲存變更。

區分使用者對受信任裝置的存取權限

*信任的裝置*是指在信任裝置設定中指定的使用者可隨時進行完全存取的裝置。要使用受信任裝置，您可以為單一使用者、一組使用者或組織的所有使用者授予存取權限。您可以配置 受信任裝置屬性中的使用者存取權限。

關於裝置控制規則產生器

您可以使用卡巴斯基安全管理中心工作和政策，同時為公司網路上的所有受防護裝置和受防護裝置群組產生裝置控制規則。若要建立可信任裝置清單，您必須對組織中的外部裝置進行稽核。

若要根據連線至個別受防護裝置的裝置清單建立規則清單，您可以使用應用程式主控台在本機執行 *裝置控制規則產生器* 工作。

您可以透過下列方式使用卡巴斯基安全管理中心建立裝置控制規則：

- 使用“*裝置控制規則產生器*”工作。

  視其設定而定，*裝置控制規則產生器* 工作可以收集曾經連線至電腦且其資訊儲存在作業系統中的所有裝置相關資訊，或收集工作啟動時已連線之裝置的相關資訊。工作會根據收集到的資訊，為 裝置控制 元件產生允許規則清單。您可以設定將產生的規則自動匯入 裝置控制 元件的規則清單，或手動匯入產生的規則。

  例如，如果您需要在首次執行 裝置控制 元件之前，快速為過去曾使用的受信任裝置建立允許規則，便可以使用此案例。

  如何在卡巴斯基安全管理中心管理主控台中執行裝置控制規則產生器工作

  1. 開啟卡巴斯基安全管理中心管理主控台。
  2. 在主控台樹狀目錄中，選擇“**工作**”。
  3. 選擇*裝置控制規則產生器*工作並雙擊以開啟工作內容。

     如果有需要的話，建立新工作。
  4. 在 **模式** 部分，選擇工作的模式：

     - **考慮有關所有已連線的外部裝置的系統資料**

       應用程式將從作業系統記憶體中獲取有關已連線到電腦的所有裝置的資訊。

     - **僅考慮目前連線的外部裝置**

       應用程式會獲取有關工作啟動時連線的裝置的資訊。
  5. 輸入要儲存包含資料的檔案的路徑。
  6. 如果您在多台電腦上執行工作，我們建議選擇**將防護裝置詳細資訊新增到檔案名稱**核取方塊。
  7. 儲存變更。
  8. 執行工作。

  如何在網頁主控台中執行“裝置控制規則產生器”工作

  1. 在網頁主控台的主視窗中，選擇**資產管理 → 工作**。

     工作清單開啟。
  2. 選擇*裝置控制規則產生器*工作並雙擊以開啟工作內容。

     如果有需要的話，建立新工作。
  3. 在 **模式** 部分，選擇工作的模式：

     - **考慮曾連線的所有外部裝置的系統資料**

       應用程式將從作業系統記憶體中獲取有關已連線到電腦的所有裝置的資訊。

     - **僅考慮目前連線的外部裝置**

       應用程式會獲取有關工作啟動時連線的裝置的資訊。
  4. 輸入要儲存包含資料的檔案的路徑。
  5. 如果您在多台電腦上執行工作，我們建議選擇**將防護裝置詳細資訊新增到檔案名稱**核取方塊。

6. 儲存變更。

7. 執行工作。

如何在網頁主控台中執行"裝置控制規則產生器"工作

1. 在 Kaspersky Embedded Systems Security 主控台樹狀目錄中，選擇"**自動規則產生 → 裝置控制規則產生器**"。

2. 在 **裝置控制規則產生器** 節點的結果窗格中，點擊 **內容**。

   內容: 裝置控制規則產生器視窗將開啟。

3. 在 **模式** 部分，選擇工作的模式：

   - **考慮有關所有已連線的外部裝置的系統資料**

     應用程式將從作業系統記憶體中獲取有關已連線到電腦的所有裝置的資訊。

   - **僅考慮目前連線的外部裝置**

     應用程式會獲取有關工作啟動時連線的裝置的資訊。

4. 在「**工作完成後**」區域，選取工作完成後的應用程式操作：

   - **將允許規則新增至裝置控制規則清單**裝置控制規則清單可在裝置控制元件設定中找到。

     如果選取此核取方塊，則應用程式將根據所選的規則新增原則將工作產生的規則新增到裝置控制規則清單中。

     如果清除此核取方塊，則應用程式不會將新產生的允許規則新增到裝置控制規則清單中。應用程式僅將規則匯出到檔案。

   - **新增原則**用來將新產生的允許規則新增至裝置控制規則清單中的方法：

     - **新增至現有規則**應用程式會將規則新增到現有規則清單。在這種情況下，應用程式會重複相同的規則。

     - **替代現有規則**應用程式會新增新規則而不是現有規則。

     - **與現有規則合併**應用程式會將規則新增到現有規則清單。在這種情況下，應用程式合併相同的規則。

   - **將允許規則匯出到檔案**應用程式回將允許規則匯出到下面欄位中指定的檔案。然後，您可以在其他電腦上的應用程式設定中匯入該檔案以分發允許規則。該檔案也可用於備份允許規則。

   - **將受防護裝置詳情新增至檔案名稱**除了日期和時間之外，應用程式還可將電腦名稱新增至匯出的檔案名稱。如果您從多台電腦收集允許規則，這會很方便。

5. 儲存變更。

結果，Kaspersky Embedded Systems Security 會對外部裝置進行稽核並將資訊儲存在卡巴斯基安全管理中心的登錄檔中。外部裝置清單在 新增受信任裝置時可用。

> *裝置控制規則產生器* 工作不會收集連線至裝置的 網路印表機和 Wi-Fi 網路相關資訊。對於這些類型的裝置，您需要手動建立規則。

- 基於卡巴斯基安全管理中心中為裝置控制元件產生的事件報告，在 **通知** 模式下執行。

在此案例中，Kaspersky Embedded Systems Security 不會封鎖對裝置的存取。當 裝置控制 元件以 **通知** 模式執行時，應用程式允許使用所有裝置，並記錄外接裝置的連線和中斷連線事件。

如何在卡巴斯基安全管理中心管理主控台中以 通知 模式啟用 裝置控制

1. 在卡巴斯基安全管理中心管理主控台樹狀目錄中，選取**政策**。
2. 選擇必要的政策並點擊以開啟政策內容。
3. 在政策屬性視窗中，選取**"本機活動控制"**。
4. 在**"裝置控制"**區域中點擊**"設定"**。
5. 選擇**"裝置控制"**核取方塊。
6. 在**用於封鎖規則的操作模式**下面，選擇**通知**。
7. 儲存變更。若要在電腦上套用該政策，請關閉掛鎖。

如何在卡巴斯基安全管理中心網頁主控台中以 通知 模式啟用 裝置控制

1. 在網頁主控台的主視窗中，選擇**資產管理 → 政策**。
2. 點擊 Kaspersky Embedded Systems Security 政策的名稱。
   政策內容視窗將開啟。
3. 選擇**"應用程式設定"**標籤。
4. 轉到**本機活動控制 → 裝置控制** 並點擊 **配置** 按鈕。
   開啟**"裝置控制"**視窗。
5. 選擇**"啟用裝置控制"**核取方塊。
6. 在**用於封鎖規則的操作模式**下面，選擇**通知**。
7. 儲存變更。若要在電腦上套用該政策，請關閉掛鎖。

如何在應用程式主控台中以 通知 模式啟用 裝置控制

1. 在 Kaspersky Embedded Systems Security 主控台樹狀目錄中，選擇**"電腦控制 → 裝置控制"**。
2. 在 **裝置控制** 節點的結果窗格中，點擊 **內容**。
   內容: 裝置控制視窗將開啟。
3. 選擇**"裝置控制"**核取方塊。
4. 在**用於封鎖規則的操作模式**下面，選擇**通知**。
5. 儲存變更。

在元件執行期間，必須執行受防護裝置和受防護裝置群組的所有可能案例。接著，您可以將卡巴斯基安全管理中心事件報告中的資訊匯入 TXT 檔案，並在檢閱報告後新增受信任裝置。

如果公司網路包含大量不同類型的受防護裝置，且各自使用不同的外接裝置組合，則建議使用此案例。

新增受信任裝置

*信任的裝置*是指在信任裝置設定中指定的使用者可隨時進行完全存取的裝置。

要使用受信任裝置，您可以為單一使用者、一組使用者或組織的所有使用者授予存取權限。

例如，如果您的組織不允許使用卸除式磁碟機，但是管理員在工作中使用卸除式磁碟機，您可以僅允許一組管理員使用卸除式磁碟機。為此，請將卸除式磁碟機新增到受信任清單中，並配置使用者存取權限。

不建議新增超過 1000 個受信任裝置，因為這可能造成系統不穩定。

如何在卡巴斯基安全管理中心管理主控台中新增受信任裝置

1. 在卡巴斯基安全管理中心管理主控台樹狀目錄中，選取**政策**。
2. 選擇必要的政策並點擊以開啟政策內容。
3. 在政策屬性視窗中，選取**"本機活動控制"**。
4. 在**"裝置控制"**區域中點擊**"設定"**。
5. 在**裝置控制設定**下，選擇**受信任裝置**標籤。
   這將開啟受信任裝置的清單。
6. 如果要為公司內的所有電腦建立受信任裝置的綜合清單，請選取**"繼承時合併值"**核取方塊。
   將合併父政策和子政策中的受信任裝置清單。如果啟用繼承時合併值，則將合併清單。父政策中的受信任裝置以唯讀視圖的形式顯示在子政策中。無法變更或刪除父政策的受信任裝置。
7. 點擊**"新增"**按鈕，然後選取將裝置新增到受信任清單的方法：
   - **基於連線的裝置產生規則**
   - **基於系統資料產生規則**
   - **基於卡巴斯基安全管理中心登錄檔產生規則**

   如果裝置清單為空，您必須 對外部裝置進行稽核。為此，請執行*裝置控制規則產生器*工作。

   Kaspersky Embedded Systems Security 不支援將**軟碟**類型的裝置新增到受信任清單。
8. 單擊**"為選定裝置新增規則"**。
9. 儲存變更。若要在電腦上套用該政策，請關閉掛鎖。

如何在卡巴斯基安全管理中心網頁主控台中新增受信任裝置

1. 在網頁主控台的主視窗中，選擇**資產管理 → 政策**。
2. 點擊 Kaspersky Embedded Systems Security 政策的名稱。
   政策內容視窗將開啟。
3. 選擇"**應用程式設定**"標籤。
4. 轉到**本機活動控制 → 裝置控制** 並點擊 **配置** 按鈕。
   開啟"**裝置控制**"視窗。
5. 在"**裝置控制設定**"塊中， 點擊"**受信任裝置**"。
   這將開啟受信任裝置的清單。
6. 如果要為公司內的所有電腦建立受信任裝置的綜合清單，請選取"**繼承時合併值**"核取方塊。
   將合併父政策和子政策中的受信任裝置清單。如果啟用繼承時合併值，則將合併清單。父政策中的受信任裝置以唯讀視圖的形式顯示在子政策中。無法變更或刪除父政策的受信任裝置。
7. 點擊"**自 KSC 登錄檔**"。
   如果裝置清單為空，您必須 對外部裝置進行稽核。為此，請執行*裝置控制規則產生器*工作。

   > Kaspersky Embedded Systems Security 不支援將**軟碟**類型的裝置新增到受信任清單。

8. 儲存變更。若要在電腦上套用該政策，請關閉掛鎖。

如何在應用程式主控台中新增受信任裝置

1. 在 Kaspersky Embedded Systems Security 主控台樹狀目錄中，選擇"**電腦控制 → 裝置控制**"。
2. 在 **裝置控制** 節點的結果窗格中，點擊 **內容**。
   內容: 裝置控制視窗將開啟。
3. 在**裝置控制設定**下，選擇**受信任裝置**標籤。
   這將開啟受信任裝置的清單。
4. 點擊"**新增**"按鈕，然後選取將裝置新增到受信任清單的方法：
   - **基於連線的裝置產生規則**
   - **基於系統資料產生規則**
   - **基於卡巴斯基安全管理中心登錄檔產生規則**

   如果裝置清單為空，您必須 對外部裝置進行稽核。為此，請執行*裝置控制規則產生器*工作。

   > Kaspersky Embedded Systems Security 不支援將**軟碟**類型的裝置新增到受信任清單。

5. 單擊**"為選定裝置新增規則"**。

6. 儲存變更。

匯出和匯入受信任裝置的清單

要將受信任裝置的清單分發到組織中的其他電腦，可以使用匯出/匯入程序。您可以將受信任裝置清單匯出到 XML 檔案。然後，您可以修改檔案，例如，新增大量相同類型的裝置。您可以使用匯出/匯入功能來備份受信任裝置清單，或將清單遷移到其他伺服器。

Kaspersky Embedded Systems Security 允許從 Kaspersky Embedded Systems Security for Windows 匯入可信任裝置清單。這些應用程式的 XML 檔案格式相同。

如何在卡巴斯基安全管理中心管理主控台中匯出和匯入受信任裝置清單

1. 在卡巴斯基安全管理中心管理主控台樹狀目錄中，選取**政策**。

2. 選擇必要的政策並點擊以開啟政策內容。

3. 在政策屬性視窗中，選取**"本機活動控制"**。

4. 在**"裝置控制"**區域中點擊**"設定"**。

5. 在**裝置控制設定**下，選擇**受信任裝置**標籤。

   這將開啟受信任裝置的清單。

6. 要匯出信任裝置的清單：

   a. 如果您要匯出整個清單，請按一下 按鈕，然後選取 **匯出**。

   b. 如果您只要匯出清單的一部分，請依照下列步驟操作：

      1. 使用 **CTRL** 或 **SHIFT** 鍵選取您要匯出的清單項目。若要選取所有項目，請按 **CTRL+A**。

      2. 按一下 按鈕，然後選取 **匯出所選**。

   c. 在開啟的視窗中，指定要匯出至的 XML 檔案名稱，然後選取要儲存該檔案的資料夾。點擊**"儲存"**按鈕。

      Kaspersky Embedded Systems Security 會將受信任裝置清單匯出到 XML 檔案。

7. 要匯入信任裝置的清單：

   a. 點擊**新增 → 從 XML 檔案匯入規則**並選擇匯入模式：新增或替代。

      在開啟的視窗中，選取要從中匯入受信任裝置清單的 XML 檔案。

      在合併模式下，應用程式檢查受信任裝置清單並刪除重複條目。在新增模式下，應用程式將條目新增至受信任應用程式清單中而不檢查重複項。

   b. 開啟檔案。

      Kaspersky Embedded Systems Security 根據所選模式匯入受信任裝置。

8. 儲存變更。若要在電腦上套用該政策，請關閉掛鎖 。

如何在網頁主控台中匯出和匯入受信任裝置清單

1. 在網頁主控台的主視窗中，選擇**資產管理 → 政策**。
2. 點擊 Kaspersky Embedded Systems Security 政策的名稱。
   政策內容視窗將開啟。
3. 選擇**"應用程式設定"**標籤。
4. 轉到**本機活動控制 → 裝置控制** 並點擊 **配置** 按鈕。
   開啟**"裝置控制"**視窗。
5. 在**"裝置控制設定"**塊中， 點擊**"受信任裝置"**。
   這將開啟受信任裝置的清單。
6. 要匯出信任裝置的清單：
   a. 選擇您要匯出的受信任裝置。
   b. 點擊 **匯出** 按鈕並選擇匯出模式：匯出整個受信任裝置清單或僅匯出選定的受信任裝置。
   c. 儲存檔案。
      Kaspersky Embedded Systems Security 會將網頁資源位址清單匯出到 XML 檔案。
7. 要匯入信任裝置的清單：
   a. 點擊**匯入**按鈕並選擇匯入模式：新增或替代。
   b. 在開啟的視窗中，選取要從中匯入網頁資源清單的 XML 檔案。
   c. 開啟檔案。
      Kaspersky Embedded Systems Security 根據所選模式匯入受信任裝置。
8. 儲存變更。若要在電腦上套用該政策，請關閉掛鎖。

如何在應用程式主控台中匯出和匯入受信任裝置清單

1. 在 Kaspersky Embedded Systems Security 主控台樹狀目錄中，選擇**"電腦控制 → 裝置控制"**。
2. 在 **裝置控制** 節點的結果窗格中，點擊 **內容**。
   內容: 裝置控制視窗將開啟。
3. 在**裝置控制設定**下，選擇**受信任裝置**標籤。
   這將開啟受信任裝置的清單。

4. 要匯出信任裝置的清單：

   a. 如果您要匯出整個清單，請按一下 按鈕，然後選取 **匯出**。

   b. 如果您只要匯出清單的一部分，請依照下列步驟操作：

      1. 使用 **CTRL** 或 **SHIFT** 鍵選取您要匯出的清單項目。若要選取所有項目，請按 **CTRL+A**。

      2. 按一下 按鈕，然後選取 **匯出所選**。

   c. 在開啟的視窗中，指定要匯出至的 XML 檔案名稱，然後選取要儲存該檔案的資料夾。點擊**"儲存"**按鈕。

      Kaspersky Embedded Systems Security 會將受信任裝置清單匯出到 XML 檔案。

5. 要匯入信任裝置的清單：

   a. 點擊**新增 → 從 XML 檔案匯入規則**並選擇匯入模式：新增或替代。

      在開啟的視窗中，選取要從中匯入網頁資源清單的 XML 檔案。

      在合併模式下，應用程式檢查受信任裝置清單並刪除重複條目。在新增模式下，應用程式將條目新增至受信任應用程式清單中而不檢查重複項。

   b. 開啟檔案。

      Kaspersky Embedded Systems Security 根據所選模式匯入受信任裝置。

6. 儲存變更。

Firewall

防火牆元件可以在以下模式中工作：

- **觀察 Windows 防火牆狀態**此模式旨在從應用程式版本 3.4 及更早版本中的防火牆管理工作邏輯平穩過渡到應用程式版本 4.0 及更高版本中的全功能防火牆。當您升級應用程式版本 3.4 及更早時，整合到 Windows 防火牆中的防火牆管理工作的規則將被保留。但防火牆元件不再與 Windows 防火牆進行交互，而只是監視 Windows 防火牆的流量篩選，並在元件的運作日誌中記錄對應的事件。然後，您可以建立防火牆規則和/或匯入 Windows 防火牆規則並將防火牆操作模式變更為 **通知**。

- **通知**應用程式僅監控防火牆規則的運行，並在元件的運行日誌中記錄相應事件。此模式用於測試防火牆規則。您可以使用防火牆操作日誌評估它們的適用性。然後，如有必要，您可以調整防火牆規則並將防火牆運作模式變更為 **封鎖**。

- **封鎖**應用程式根據元件設定篩選網路流量，並在元件的操作日誌中記錄對應事件。

關於防火牆規則

如果選擇了 **封鎖** 模式，防火牆元件將使用防火牆規則篩選網路流量。

應用程式的防火牆規則控制指定應用程式的網路連線。這些規則的觸發條件基於可執行應用程式檔案的路徑。

防火牆連接埠規則控制指定連接埠和通訊協定 (TCP / UDP) 的網路連線。此類規則的觸發條件是協定類型和連接埠或連接埠範圍。

連接埠規則涉及的範圍比應用程式規則的範圍要廣。透過基於連接埠規則允許網路連線，會降低受防護電腦的安全等級。

配置防火牆

本部分提供有關設定防火牆元件的一般設定以及建立和設定防火牆規則的說明。

配置一般防火墻設定

在卡巴斯基安全管理中心管理主控台中配置防火牆元件的一般設定

1. 在卡巴斯基安全管理中心管理主控台樹狀目錄中，選取**政策**。
2. 選擇必要的政策並點擊以開啟政策內容。
3. 在 **網路活動控制** 部分，點擊**防火牆** 子部分中的 **設定** 按鈕。
   開啟“**防火牆**”視窗。

4. 在“**一般**”頁簽的**用於封鎖規則的操作模式**塊中，選擇元件操作模式：

   - **觀察 Windows 防火牆狀態**此模式旨在從應用程式版本 3.4 及更早版本中的防火牆管理工作邏輯平穩過渡到應用程式版本 4.0 及更高版本中的全功能防火牆。當您升級應用程式版本 3.4 及更早時，整合到 Windows 防火牆中的防火牆管理工作的規則將被保留。但防火牆元件不再與 Windows 防火牆進行交互，而只是監視 Windows 防火牆的流量篩選，並在元件的運作日誌中記錄對應的事件。然後，您可以建立防火牆規則和/或匯入 Windows 防火牆規則並將防火牆操作模式變更為 **通知**。

   - **通知**應用程式僅監控防火牆規則的運行，並在元件的運行日誌中記錄相應事件。此模式用於測試防火牆規則。您可以使用防火牆操作日誌評估它們的適用性。然後，如有必要，您可以調整防火牆規則並將防火牆運作模式變更為 **封鎖**。

   - **封鎖**應用程式根據元件設定篩選網路流量，並在元件的操作日誌中記錄對應事件。

5. 在**輸入連線**區塊中，設定傳入網路連線的設定：

   - 使用**針對接受連線的操作**下拉式清單指定應用程式對所有傳入網路連線執行的動作，除非在傳入連線的防火牆規則中另有定義。

   - 如有必要，新增傳入連線的防火牆規則。

     傳入連線的防火牆規則執行排除的角色。例如，如果您為傳入網路連線設定允許規則，並在 **針對接受連線的操作**下拉式清單中選擇**封鎖**，則應用程式將允許符合規則條件的傳入網路連線。

6. 在**輸出連線**區塊中，設定傳出網路連線的設定：

   - 使用**針對傳送連線的操作**下拉式清單指定應用程式對所有傳出網路連線執行的動作，除非在傳出連線的防火牆規則中另有定義。

   - 如有必要，新增傳出連線的防火牆規則。

     傳出連線的防火牆規則執行排除的角色。例如，如果您為傳出網路連線設定封鎖規則，並在**針對傳送連線的操作**下拉式清單中選擇**允許**，則應用程式將封鎖符合規則條件的傳出網路連線。

7. 儲存變更。

Kaspersky Embedded Systems Security 將套用新設定。變更設定時的日期和時間儲存在系統稽核記錄中。

在卡巴斯基安全管理中心網頁主控台中配置防火牆元件的一般設定

1. 在網頁主控台的主視窗中，選擇**資產管理 → 政策**。

2. 點擊 Kaspersky Embedded Systems Security 政策的名稱。

   政策內容視窗將開啟。

3. 選擇“**應用程式設定**”標籤。

4. 在 **網路活動控制** 部分，點擊**防火牆** 子部分中的 **配置** 按鈕。

   開啟“**防火牆**”視窗。

5. 將切換開關設定為 **防火牆已啟用**。

6. 在“**用於封鎖規則的操作模式**”塊中，選擇元件操作模式：

   - **觀察 Windows 防火牆狀態**此模式旨在從應用程式版本 3.4 及更早版本中的防火牆管理工作邏輯平穩過渡到應用程式版本 4.0 及更高版本中的全功能防火牆。當您升級應用程式版本 3.4 及更早時，整合到 Windows 防火牆中的防火牆管理工作的規則將被保留。但防火牆元件不再與 Windows 防火牆進行交互，而只是監視 Windows 防火牆的流量篩選，並在元件的運作日誌中記錄對應的事件。然後，您可以建立防火牆規則和/或匯入 Windows 防火牆規則並將防火牆操作模式變更為 **通知**。

   - **通知**應用程式僅監控防火牆規則的運行，並在元件的運行日誌中記錄相應事件。此模式用於測試防火牆規則。您可以使用防火牆操作日誌評估它們的適用性。然後，如有必要，您可以調整防火牆規則並將防火牆運作模式變更為 **封鎖**。

   - **封鎖**應用程式根據元件設定篩選網路流量，並在元件的操作日誌中記錄對應事件。

7. 在**輸入連線**區塊中，設定傳入網路連線的設定：

   - 使用**針對接受連線的操作**下拉式清單指定應用程式對所有傳入網路連線執行的動作，除非在傳入連線的防火牆規則中另有定義。

   - 如有必要，新增傳入連線的防火牆規則。

     傳入連線的防火牆規則執行排除的角色。例如，如果您為傳入網路連線設定允許規則，並在 **針對接受連線的操作**下拉式清單中選擇**封鎖**，則應用程式將允許符合規則條件的傳入網路連線。

8. 在**輸出連線**區塊中，設定傳出網路連線的設定：

   - 使用**針對傳送連線的操作**下拉式清單指定應用程式對所有傳出網路連線執行的動作，除非在傳出連線的防火牆規則中另有定義。

   - 如有必要，新增傳出連線的防火牆規則。

     傳出連線的防火牆規則執行排除的角色。例如，如果您為傳出網路連線設定封鎖規則，並在**針對傳送連線的操作**下拉式清單中選擇**允許**，則應用程式將封鎖符合規則條件的傳出網路連線。

9. 儲存變更。

Kaspersky Embedded Systems Security 將套用新設定。變更設定時的日期和時間儲存在系統稽核記錄中。

在應用程式主控台中設定防火牆元件的一般設定

1. 在 Kaspersky Embedded Systems Security 主控台樹狀目錄中，選擇“**電腦控制 → 防火牆**”。

2. 在 **防火牆** 節點的結果窗格中，點擊 **內容**。

   內容: 防火牆視窗將開啟。

3. 選擇“**防火牆**”核取方塊。

4. 在“**用於封鎖規則的操作模式**”塊中，選擇元件操作模式：

   - **觀察 Windows 防火牆狀態**此模式旨在從應用程式版本 3.4 及更早版本中的防火牆管理工作邏輯平穩過渡到應用程式版本 4.0 及更高版本中的全功能防火牆。當您升級應用程式版本 3.4 及更早時，整合到 Windows 防火牆中的防火牆管理工作的規則將被保留。但防火牆元件不再與 Windows 防火牆進行交互，而只是監視 Windows 防火牆的流量篩選，並在元件的運作日誌中記錄對應的事件。然後，您可以建立防火牆規則和/或匯入 Windows 防火牆規則並將防火牆操作模式變更為 **通知**。

   - **通知**應用程式僅監控防火牆規則的運行，並在元件的運行日誌中記錄相應事件。此模式用於測試防火牆規則。您可以使用防火牆操作日誌評估它們的適用性。然後，如有必要，您可以調整防火牆規則並將防火牆運作模式變更為 **封鎖**。

   - **封鎖**應用程式根據元件設定篩選網路流量，並在元件的操作日誌中記錄對應事件。

5. 在**輸入連線**區塊中，設定傳入網路連線的設定：

   - 使用**針對接受連線的操作**下拉式清單指定應用程式對所有傳入網路連線執行的動作，除非在傳入連線的防火牆規則中另有定義。

   - 如有必要，新增傳入連線的防火牆規則。

     傳入連線的防火牆規則執行排除的角色。例如，如果您為傳入網路連線設定允許規則，並在 **針對接受連線的操作**下拉式清單中選擇**封鎖**，則應用程式將允許符合規則條件的傳入網路連線。

6. 在**輸出連線**區塊中，設定傳出網路連線的設定：

   - 使用**針對傳送連線的操作**下拉式清單指定應用程式對所有傳出網路連線執行的動作，除非在傳出連線的防火牆規則中另有定義。

   - 如有必要，新增傳出連線的防火牆規則。

     傳出連線的防火牆規則執行排除的角色。例如，如果您為傳出網路連線設定封鎖規則，並在**針對傳送連線的操作**下拉式清單中選擇**允許**，則應用程式將封鎖符合規則條件的傳出網路連線。

7. 儲存變更。

Kaspersky Embedded Systems Security 將套用新設定。變更設定時的日期和時間儲存在系統稽核記錄中。

建立和設定防火牆規則

在卡巴斯基安全管理中心管理主控台中建立和配置防火牆規則

1. 在卡巴斯基安全管理中心管理主控台樹狀目錄中，選取**政策**。

2. 選擇必要的政策並點擊以開啟政策內容。

3. 在 **網路活動控制** 部分，點擊**防火牆** 子部分中的 **設定** 按鈕。

   開啟“**防火牆**”視窗。

4. 在”**輸入連線**”塊中，點擊”**規則清單**”按鈕。

   開啟“**針對接受連線的規則**”視窗。

5. **為傳入連線建立和設定防火牆規則**。

   1. 在**"應用程式"**標籤上點擊**"新增"**按鈕 。
      開啟**"應用程式規則"**視窗。

   2. 進行規則設定：

      a. 在**"規則名稱"**欄位中輸入規則的名稱。

      > 規則名稱，無論字元大小寫，都不能與保留的名稱 All、ICMPv4 和 ICMPv6 相符；這在傳入網路連線的所有規則清單中必須是唯一名稱。

      b. 在**"動作"**清單中，選取以下選項之一：

      - **允許**如果選擇此選項，應用程式將允許應用程式的傳入網路連線。
      - **封鎖**如果選擇此選項，應用程式將封鎖應用程式的傳入網路連線。

      c. 選擇 **協定** 核取方塊，以選擇應用程式控制傳入網路連線的協定類型。

      d. 在**連接埠** and **連接埠**區塊中，指定連接埠或連接埠範圍。

      e. 在**應用程式路徑**欄位中，手動或使用**瀏覽**按鈕，針對要為其設定規則的應用程式，指定可執行檔的路徑。

      f. 如有必要，請在 **服務名稱** 欄位中指定要套用該規則的服務的名稱。

      g. 在**規則使用範圍**欄位中，指定網路位址。該應用程式會根據規則設定監控來自指定網路位址的傳入連線。

      > IP 位址僅支援 IPv4 格式。

      h. 在**網路介面卡**區塊中，指定網路介面卡清單。

      i. 按一下**確定**按鈕以儲存規則。

   3. 在**"連接埠"**標籤上點擊**"新增"**按鈕 。
      開啟**"連接埠規則"**視窗。

   4. 進行規則設定：

      a. 在**"規則名稱"**欄位中輸入規則的名稱。

      b. 在**"動作"**清單中，選取以下選項之一：

      - **允許**如果選擇此選項，應用程式將允許連接埠的傳入網路連線。
      - **封鎖**如果選擇此選項，應用程式將封鎖連接埠的傳入網路連線。

      c. 選擇 **協定** 核取方塊，以選擇應用程式控制傳入網路連線的協定類型。

      d. 在**連接埠** and **連接埠**區塊中，指定連接埠或連接埠範圍。

e. 在**規則使用範圍**欄位中，指定網路位址。該應用程式會根據規則設定監控來自指定網路位址的傳入連線。

IP 位址僅支援 IPv4 格式。

f. 在**網路介面卡**區塊中，指定網路介面卡清單。

g. 按一下**確定**按鈕以儲存規則。

5. 在**針對接受連線的規則**視窗中，按一下**確定**按鈕。

6. 在"**輸出連線**"塊中，點擊"**規則清單**"按鈕。
開啟"**針對傳送連線的規則**"視窗。

7. **為傳出連線建立和設定防火牆規則**。

1. 在"**應用程式**"標籤上點擊"**新增**"按鈕 。
開啟"**應用程式規則**"視窗。

2. 進行規則設定：

a. 在"**規則名稱**"欄位中輸入規則的名稱。

規則名稱，無論字元大小寫，都不能與保留的名稱 All、ICMPv4 和 ICMPv6 相符；這在傳出網路連線的所有規則清單中必須是唯一名稱。

b. 在"**動作**"清單中，選取以下選項之一：

- **允許**如果選擇此選項，應用程式將允許應用程式的傳出網路連線。
- **封鎖**如果選擇此選項，應用程式將封鎖應用程式的傳出網路連線。

c. 選擇 **協定** 核取方塊，以選擇應用程式控制傳入網路連線的協定類型。

d. 在**連接埠** and **連接埠**區塊中，指定連接埠或連接埠範圍。

e. 在**應用程式路徑**欄位中，手動或使用**瀏覽**按鈕，針對要為其設定規則的應用程式，指定可執行檔的路徑。

f. 如有必要，請在 **服務名稱** 欄位中指定要套用該規則的服務的名稱。

g. 在**規則使用範圍**欄位中，指定網路位址。該應用程式會根據規則設定監控前往指定網路位址的傳出連線。

IP 位址僅支援 IPv4 格式。

h. 在**網路介面卡**區塊中，指定網路介面卡清單。

i. 按一下**確定**按鈕以儲存規則。

3. 在**"連接埠"**標籤上點擊**"新增"**按鈕 。
   開啟**"連接埠規則"**視窗。

4. 進行規則設定：

   a. 在**"規則名稱"**欄位中輸入規則的名稱。

   b. 在**"動作"**清單中，選取以下選項之一：

   - **允許**如果選擇此選項，應用程式將允許連接埠的傳出網路連線。
   - **封鎖**如果選擇此選項，應用程式將封鎖連接埠的傳出網路連線。

   c. 選擇 **協定** 核取方塊，以選擇應用程式控制傳入網路連線的協定類型。

   d. 在**連接埠** and **連接埠**區塊中，指定連接埠或連接埠範圍。

   e. 在**規則使用範圍**欄位中，指定網路位址。該應用程式會根據規則設定監控前往指定網路位址的傳出連線。

   > IP 位址僅支援 IPv4 格式。

   f. 在**網路介面卡**區塊中，指定網路介面卡清單。

   g. 按一下**確定**按鈕以儲存規則。

5. 在**針對傳送連線的規則**視窗中，按一下**確定**按鈕。

8. 如果要從 XML 檔案匯入或匯出自訂規則，請使用**匯入和匯出規則**區塊中的**匯入**或者**匯出**按鈕。

9. 儲存變更。

Kaspersky Embedded Systems Security 將套用新設定。變更設定時的日期和時間儲存在系統稽核記錄中。

在卡巴斯基安全管理中心網頁主控台中建立和配置防火牆規則

1. 在網頁主控台的主視窗中，選擇**資產管理 → 政策**。

2. 點擊 Kaspersky Embedded Systems Security 政策的名稱。
   政策內容視窗將開啟。

3. 選擇**"應用程式設定"**標籤。

4. 在 **網路活動控制** 部分，點擊**防火牆** 子部分中的 **配置** 按鈕。
   開啟**"防火牆"**視窗。

5. 將切換開關設定為 **防火牆已啟用**。

6. 在**"輸入連線"**塊中，點擊**"配置"**按鈕。
   開啟**"針對接受連線的規則"**視窗。

7. **為傳入連線建立和設定防火牆規則**。

   1. 在**"連接埠"**標籤上點擊**"新增"**按鈕 。
      開啟**"連接埠規則"**視窗。

   2. 進行規則設定：

      a. 在**"規則名稱"**欄位中輸入規則的名稱。

      b. 在**"操作"**清單中，選取以下選項之一：

         - **允許**如果選擇此選項，應用程式將允許連接埠的傳入網路連線。
         - **拒絕**如果選擇此選項，應用程式將封鎖連接埠的傳入網路連線。

      c. 選擇 **協定** 核取方塊，以選擇應用程式控制傳入網路連線的協定類型。

      d. 在**本機連接埠** and **遠端連接埠**區塊中，指定連接埠或連接埠範圍。

      e. 在**規則使用範圍**欄位中，指定網路位址。該應用程式會根據規則設定監控指定網路位址的傳入連線。

      > IP 位址僅支援 IPv4 格式。

      f. 在**網路介面卡**區塊中，指定網路介面卡清單。

      g. 按一下**確定**按鈕以儲存規則。

   3. 在**"應用程式"**標籤上點擊**"新增"**按鈕 。
      開啟**"應用程式規則"**視窗。

   4. 進行規則設定：

      a. 在**"規則名稱"**欄位中輸入規則的名稱。

      > 規則名稱，無論字元大小寫，都不能與保留的名稱 All、ICMPv4 和 ICMPv6 相符；這在傳入網路連線的所有規則清單中必須是唯一名稱。

      b. 在**"操作"**清單中，選取以下選項之一：

         - **允許**如果選擇此選項，應用程式將允許應用程式的傳入網路連線。
         - **拒絕**如果選擇此選項，應用程式將封鎖應用程式的傳入網路連線。

      c. 選擇 **協定** 核取方塊，以選擇應用程式控制傳入網路連線的協定類型。

      d. 在**本機連接埠** and **遠端連接埠**區塊中，指定連接埠或連接埠範圍。

      e. 在**應用程式路徑**欄位中，針對要為其設定規則的應用程式手動指定可執行檔的路徑。

      f. 如有必要，請在 **服務名稱** 欄位中指定要套用該規則的服務的名稱。

g. 在**規則使用範圍**欄位中，指定網路位址。該應用程式會根據規則設定監控來自指定網路位址的傳入連線。

> IP 位址僅支援 IPv4 格式。

h. 在**網路介面卡**區塊中，指定網路介面卡清單。

i. 按一下**確定**按鈕以儲存規則。

5. 在**針對接受連線的規則**視窗中，按一下**確定**按鈕。

8. 在"**輸出連線**"塊中，點擊"**配置**"按鈕。
開啟"**針對傳送連線的規則**"視窗。

9. **為傳出連線建立和設定防火牆規則**。

1. 在"**連接埠**"標籤上點擊"**新增**"按鈕 。
開啟"**連接埠規則**"視窗。

2. 進行規則設定：

a. 在"**規則名稱**"欄位中輸入規則的名稱。

b. 在"**操作**"清單中，選取以下選項之一：

- **允許**如果選擇此選項，應用程式將允許連接埠的傳出網路連線。
- **拒絕**如果選擇此選項，應用程式將封鎖連接埠的傳出網路連線。

c. 選擇 **協定** 核取方塊，以選擇應用程式控制傳入網路連線的協定類型。

d. 在**本機連接埠** and **遠端連接埠**區塊中，指定連接埠或連接埠範圍。

e. 在**規則使用範圍**欄位中，指定網路位址。該應用程式會根據規則設定監控前往指定網路位址的傳出連線。

> IP 位址僅支援 IPv4 格式。

f. 在**網路介面卡**區塊中，指定網路介面卡清單。

g. 按一下**確定**按鈕以儲存規則。

3. 在"**應用程式**"標籤上點擊"**新增**"按鈕 。
開啟"**應用程式規則**"視窗。

4. 進行規則設定：

   a. 在**"規則名稱"**欄位中輸入規則的名稱。

      規則名稱，無論字元大小寫，都不能與保留的名稱 All、ICMPv4 和 ICMPv6 相符；這在傳出網路連線的所有規則清單中必須是唯一名稱。

   b. 在**"操作"**清單中，選取以下選項之一：

      - **允許**如果選擇此選項，應用程式將允許應用程式的傳出網路連線。
      - **拒絕**如果選擇此選項，應用程式將封鎖應用程式的傳出網路連線。

   c. 選擇 **協定** 核取方塊，以選擇應用程式控制傳入網路連線的協定類型。

   d. 在**本機連接埠** and **遠端連接埠**區塊中，指定連接埠或連接埠範圍。

   e. 在**應用程式路徑**欄位中，針對要為其設定規則的應用程式手動指定可執行檔的路徑。

   f. 如有必要，請在 **服務名稱** 欄位中指定要套用該規則的服務的名稱。

   g. 在**規則使用範圍**欄位中，指定網路位址。該應用程式會根據規則設定監控前往指定網路位址的傳出連線。

      IP 位址僅支援 IPv4 格式。

   h. 在**網路介面卡**區塊中，指定網路介面卡清單。

   i. 按一下**確定**按鈕以儲存規則。

5. 在**針對傳送連線的規則**視窗中，按一下**確定**按鈕。

10. 如果要從 XML 檔案匯入或匯出自訂規則，請使用**匯入和匯出規則**區塊中的**匯入規則**或者**匯出規則**按鈕。

11. 儲存變更。

Kaspersky Embedded Systems Security 將套用新設定。變更設定時的日期和時間儲存在系統稽核記錄中。

在應用程式主控台中建立和配置防火牆規則

1. 在 Kaspersky Embedded Systems Security 主控台樹狀目錄中，選擇**"電腦控制 → 防火牆"**。
2. 在 **防火牆** 節點的結果窗格中，點擊 **內容**。
   內容: 防火牆視窗將開啟。
3. 在**"輸入連線"**塊中，點擊**"規則清單"**按鈕。
   開啟**"針對接受連線的規則"**視窗。
4. **為傳入連線建立和設定防火牆規則**。

   1. 在**"應用程式"**標籤上點擊**"新增"**按鈕 。
      開啟**"應用程式規則"**視窗。

2. 進行規則設定：

   a. 在“**規則名稱**”欄位中輸入規則的名稱。

      規則名稱，無論字元大小寫，都不能與保留的名稱 All、ICMPv4 和 ICMPv6 相符；這在傳入網路連線的所有規則清單中必須是唯一名稱。

   b. 在“**動作**”清單中，選取以下選項之一：

      - **允許**如果選擇此選項，應用程式將允許應用程式的傳入網路連線。
      - **封鎖**如果選擇此選項，應用程式將封鎖應用程式的傳入網路連線。

   c. 選擇 **協定** 核取方塊，以選擇應用程式控制傳入網路連線的協定類型。

   d. 在**連接埠** and **連接埠**區塊中，指定連接埠或連接埠範圍。

   e. 在**應用程式路徑**欄位中，手動或使用**瀏覽**按鈕，針對要為其設定規則的應用程式，指定可執行檔的路徑。

   f. 如有必要，請在 **服務名稱** 欄位中指定要套用該規則的服務的名稱。

   g. 在**規則使用範圍**欄位中，指定網路位址。該應用程式會根據規則設定監控來自指定網路位址的傳入連線。

      IP 位址僅支援 IPv4 格式。

   h. 在**網路介面卡**區塊中，指定網路介面卡清單。

   i. 按一下**確定**按鈕以儲存規則。

3. 在“**連接埠**”標籤上點擊“**新增**”按鈕 。
   開啟“**連接埠規則**”視窗。

4. 進行規則設定：

   a. 在“**規則名稱**”欄位中輸入規則的名稱。

   b. 在“**動作**”清單中，選取以下選項之一：

      - **允許**如果選擇此選項，應用程式將允許連接埠的傳入網路連線。
      - **封鎖**如果選擇此選項，應用程式將封鎖連接埠的傳入網路連線。

   c. 選擇 **協定** 核取方塊，以選擇應用程式控制傳入網路連線的協定類型。

   d. 在**連接埠** and **連接埠**區塊中，指定連接埠或連接埠範圍。

e. 在**規則使用範圍**欄位中，指定網路位址。該應用程式會根據規則設定監控來自指定網路位址的傳入連線。

IP 位址僅支援 IPv4 格式。

f. 在**網路介面卡**區塊中，指定網路介面卡清單。

g. 按一下**確定**按鈕以儲存規則。

5. 在**針對接受連線的規則**視窗中，按一下**確定**按鈕。

5. 在"**輸出連線**"塊中，點擊"**規則清單**"按鈕。

開啟"**針對傳送連線的規則**"視窗。

6. **為傳出連線建立和設定防火牆規則**。

1. 在"**應用程式**"標籤上點擊"**新增**"按鈕 。

開啟"**應用程式規則**"視窗。

2. 進行規則設定：

a. 在"**規則名稱**"欄位中輸入規則的名稱。

規則名稱，無論字元大小寫，都不能與保留的名稱 All、ICMPv4 和 ICMPv6 相符；這在傳出網路連線的所有規則清單中必須是唯一名稱。

b. 在"**動作**"清單中，選取以下選項之一：

- **允許**如果選擇此選項，應用程式將允許應用程式的傳出網路連線。
- **封鎖**如果選擇此選項，應用程式將封鎖應用程式的傳出網路連線。

c. 選擇 **協定** 核取方塊，以選擇應用程式控制傳入網路連線的協定類型。

d. 在**連接埠** and **連接埠**區塊中，指定連接埠或連接埠範圍。

e. 在**應用程式路徑**欄位中，手動或使用**瀏覽**按鈕，針對要為其設定規則的應用程式，指定可執行檔的路徑。

f. 如有必要，請在 **服務名稱** 欄位中指定要套用該規則的服務的名稱。

g. 在**規則使用範圍**欄位中，指定網路位址。該應用程式會根據規則設定監控前往指定網路位址的傳出連線。

IP 位址僅支援 IPv4 格式。

h. 在**網路介面卡**區塊中，指定網路介面卡清單。

i. 按一下**確定**按鈕以儲存規則。

3. 在**"連接埠"**標籤上點擊**"新增"**按鈕 。
   開啟**"連接埠規則"**視窗。

4. 進行規則設定：

   a. 在**"規則名稱"**欄位中輸入規則的名稱。

   b. 在**"動作"**清單中，選取以下選項之一：

   - **允許**如果選擇此選項，應用程式將允許連接埠的傳出網路連線。
   - **封鎖**如果選擇此選項，應用程式將封鎖連接埠的傳出網路連線。

   c. 選擇 **協定** 核取方塊，以選擇應用程式控制傳入網路連線的協定類型。

   d. 在**連接埠** and **連接埠**區塊中，指定連接埠或連接埠範圍。

   e. 在**規則使用範圍**欄位中，指定網路位址。該應用程式會根據規則設定監控前往指定網路位址的傳出連線。

   > IP 位址僅支援 IPv4 格式。

   f. 在**網路介面卡**區塊中，指定網路介面卡清單。

   g. 按一下**確定**按鈕以儲存規則。

5. 在**針對傳送連線的規則**視窗中，按一下**確定**按鈕。

7. 如果要從 XML 檔案匯入或匯出自訂規則，請使用**匯入和匯出規則**區塊中的**匯入**或者**匯出**按鈕。

8. 若要匯入 Windows 防火牆規則，請點擊**匯入 Windows Firewall 規則**。

> 在 Windows 11 24H2 電腦上，該應用程式可能會略過某些 Windows 防火牆規則。由於此版本作業系統的特殊功能，Kaspersky Embedded Systems Security 可能無法識別某些應用程式封包規則的參數。

9. 儲存變更。

Kaspersky Embedded Systems Security 將套用新設定。變更設定時的日期和時間儲存在系統稽核記錄中。

啟用和停用防火牆規則

在卡巴斯基安全管理中心管理主控台中啟用和停用防火牆規則

1. 在卡巴斯基安全管理中心管理主控台樹狀目錄中，選取**政策**。

2. 選擇必要的政策並點擊以開啟政策內容。

3. 在 **網路活動控制** 部分，點擊**防火牆** 子部分中的 **設定** 按鈕。
   開啟**"防火牆"**視窗。

4. 在開啟的視窗中，點擊 **輸入連線** 或者 **輸出連線** 部分中的**規則清單**按鈕，具體取決於您要變更其狀態的規則類型。

5. 在開啟的視窗中，選擇**"應用程式"**或者**連接埠**頁簽。
   在規則清單中，選擇要修改其狀態的規則，然後執行以下操作之一：

   - 如果您想要啟用已停用的規則，選中規則名稱左側的核取方塊。
     將啟用所選規則。
   - 如果您想要停用已啟用的規則，清除規則名稱左側的核取方塊。
     將停用所選規則。

6. 若要從清單中刪除規則，請選擇規則並點擊**刪除**。

7. 儲存變更。

在卡巴斯基安全管理中心網頁主控台中啟用和停用防火牆規則

1. 在網頁主控台的主視窗中，選擇**資產管理 → 政策**。

2. 點擊 Kaspersky Embedded Systems Security 政策的名稱。
   政策內容視窗將開啟。

3. 選擇**"應用程式設定"**標籤。

4. 在 **網路活動控制** 部分，點擊**防火牆** 子部分中的 **配置** 按鈕。
   開啟**"防火牆"**視窗。

5. 在開啟的視窗中，點擊 **輸入連線** 或者 **輸出連線** 部分中的**配置**按鈕，具體取決於您要變更其狀態的規則類型。

6. 在開啟的視窗中，選擇**"連接埠"**或者**應用程式**頁簽。
   在規則清單中，選擇要修改其狀態的規則，然後執行以下操作之一：

   - 如果您想要啟用已停用的規則，選中規則名稱左側的核取方塊。
     將啟用所選規則。
   - 如果您想要停用已啟用的規則，清除規則名稱左側的核取方塊。
     將停用所選規則。

7. 若要從清單中刪除規則，請選擇規則並點擊**刪除**。

8. 儲存變更。

在應用程式主控台中啟用和停用防火牆規則

1. 在 Kaspersky Embedded Systems Security 主控台樹狀目錄中，選擇**"電腦控制 → 防火牆"**。

2. 在 **防火牆** 節點的結果窗格中，點擊 **內容**。
   內容: 防火牆視窗將開啟。

3. 在開啟的視窗中，點擊 **輸入連線** 或者 **輸出連線** 部分中的**規則清單**按鈕，具體取決於您要變更其狀態的規則類型。

4. 在開啟的視窗中，選擇**"應用程式"**或者**連接埠**頁簽。
   在規則清單中，選擇要修改其狀態的規則，然後執行以下操作之一：

   - 如果您想要啟用已停用的規則，選中規則名稱左側的核取方塊。
     將啟用所選規則。

   - 如果您想要停用已啟用的規則，清除規則名稱左側的核取方塊。
     將停用所選規則。

5. 若要從清單中刪除規則，請選擇規則並點擊**刪除**。

6. 儲存變更。

BadUSB 攻擊防護

預設情況下，未安裝"BadUSB 攻擊防護"元件。您可以在應用程式安裝期間新增元件，也可以在應用程式安裝後變更應用程式元件集。

某些病毒會修改 USB 裝置的固件以欺騙作業系統，將 USB 偽裝為鍵盤。結果，該病毒可能在您的使用者帳戶下執行命令以下載惡意軟體（例如）。

BadUSB 攻擊防護元件可以防止受感染的模擬鍵盤的 USB 裝置連線至電腦。

當 USB 裝置連線至電腦並被作業系統識別為鍵盤時，應用程式將提示使用者使用此鍵盤或螢幕鍵盤（如果可用）輸入應用程式產生的數字代碼。這個步驟稱為鍵盤授權。

如果輸入的代碼正確，應用程式會將識別參數（鍵盤的 VID/PID 及其所連接的連接埠號碼）儲存在授權鍵盤清單之中。重新啟動作業系統後重新連線鍵盤時無需重複鍵盤授權。

經授權的鍵盤連接至該電腦不同 USB 連接埠時，程式將再次提示為該鍵盤授權。

如果錯誤輸入數位代碼，則程式將生成新的代碼。您可以設定輸入數字代碼的嘗試次數。如果數字代碼多次輸入不正確，或者鍵盤授權視窗被關閉，則應用程式封鎖來自此鍵盤的輸入。當 USB 裝置封鎖時間經過或者作業系統重新啟動後，程式將再次提示使用者重新執行鍵盤授權。

程式將允許使用經過授權的鍵盤並封鎖未經授權的鍵盤。

在 BadUSB 攻擊防護元件安裝前被電腦識別為鍵盤的 USB 裝置在該元件安裝後仍將被認定為經過授權。

如何在卡巴斯基安全管理中心管理主控台中啟用和配置 BadUSB 攻擊防護元件

1. 在卡巴斯基安全管理中心管理主控台樹狀目錄中，選取**政策**。
2. 選擇必要的政策並點擊以開啟政策內容。
3. 在政策內容視窗中，轉至「**本機活動控制**」區域。
4. 在"**BadUSB 攻擊防護**"塊中，點擊"**設定**"按鈕。
   開啟"**BadUSB 攻擊防護**"視窗。
5. 使用"**BadUSB 攻擊防護**"核取方塊來啟用或停用元件。
6. 在"**USB 裝置授權**"部分中，配置以下設定：
   - **USB 裝置授權嘗試最大次數**在授權碼不正確輸入達到指定次數時自動封鎖 USB 裝置。有效值為 1 到 10。例如，如果您允許嘗試輸入授權碼五次，則應用程式會在第五次嘗試失敗後封鎖 USB 裝置。Kaspersky Embedded Systems Security 會顯示 USB 裝置的阻止持續時間。該時間經過後，您可以有 5 次嘗試輸入授權碼。
   - **達到嘗試的最大次數時的逾時（分鐘）**授權碼輸入指定嘗試失敗數目後封鎖 USB 裝置的時長。有效值為 1 到 180（分鐘）。

7. 在**"連線時的 USB 裝置授權"**部分中，配置以下設定：

   - **禁止使用螢幕鍵盤授權 USB 裝置**如果選定此核取方塊，應用程式將封鎖使用螢幕鍵盤授權無法輸入認證的 USB 裝置（例如條碼掃描器）。
   - **禁止使用條形碼授權 USB 裝置**如果選取該核取方塊，應用程式將不會在條碼掃描器授權通知中顯示條碼。

8. 關上掛鎖將政策套用至電腦。

9. 點擊**確定**以儲存變更。

如何在卡巴斯基安全管理中心網頁主控台中啟用和配置 BadUSB 攻擊防護元件

1. 在網頁主控台的主視窗中，選擇**資產管理 → 政策**。

2. 點擊 Kaspersky Embedded Systems Security 政策的名稱。
   政策內容視窗將開啟。

3. 選擇**"應用程式設定"**標籤。

4. 選擇 **本機活動控制** 部分。

5. 在"**BadUSB 攻擊防護**"塊中，點擊"**配置**"按鈕。
   開啟"**BadUSB 攻擊防護**"視窗。

6. 使用"**BadUSB 攻擊防護**"切換開關可啟用或停用元件。

7. 啟用或停用「**禁止使用螢幕鍵盤授權 USB 裝置已啟用**」切換開關，以允許或封鎖使用螢幕鍵盤授權無法輸入授權碼的 USB 裝置（例如條碼掃描器）。

8. 啟用或停用「**禁止使用條形碼授權 USB 裝置已啟用**」切換開關，以允許或封鎖在條碼掃描器授權通知中顯示條碼。

9. 在"**USB 裝置授權**"部分中，配置以下設定：

   - **USB 裝置授權嘗試最大次數 (1-10)**在授權碼不正確輸入達到指定次數時自動封鎖 USB 裝置。有效值為 1 到 10。例如，如果您允許嘗試輸入授權碼五次，則應用程式會在第五次嘗試失敗後封鎖 USB 裝置。Kaspersky Embedded Systems Security 會顯示 USB 裝置的阻止持續時間。該時間經過後，您可以有 5 次嘗試輸入授權碼。
   - **達到嘗試的最大數量時逾時 (分鐘) (1-180)**授權碼輸入指定嘗試失敗數目後封鎖 USB 裝置的時長。有效值為 1 到 180（分鐘）。

10. 關上掛鎖將政策套用至電腦。

11. 點擊**確定**以儲存變更。

如何在應用程式主控台中啟用和配置 BadUSB 攻擊防護元件

1. 在管理主控台樹狀目錄中，選擇**電腦控制 → BadUSB 攻擊防護**資料夾。

2. 在結果窗格中點擊"**內容**"連結。
   開啟"**BadUSB 攻擊防護**"視窗。

3. 使用"**BadUSB 攻擊防護**"核取方塊來啟用或停用元件。

4. 在“**USB 裝置授權**”部分中，配置以下設定：

- **USB 裝置授權嘗試最大次數**在授權碼不正確輸入達到指定次數時自動封鎖 USB 裝置。有效值為 1 到 10。例如，如果您允許嘗試輸入授權碼五次，則應用程式會在第五次嘗試失敗後封鎖 USB 裝置。Kaspersky Embedded Systems Security 會顯示 USB 裝置的阻止持續時間。該時間經過後，您可以有 5 次嘗試輸入授權碼。

- **達到嘗試的最大次數時的逾時（分鐘）**授權碼輸入指定嘗試失敗數目後封鎖 USB 裝置的時長。有效值為 1 到 180（分鐘）。

5. 在“**連線時的 USB 裝置授權**”部分中，配置以下設定：

- **禁止使用螢幕鍵盤授權 USB 裝置**如果選定此核取方塊，應用程式將封鎖使用螢幕鍵盤授權無法輸入認證的 USB 裝置（例如條碼掃描器）。

- **禁止使用條形碼授權 USB 裝置**如果選取該核取方塊，應用程式將不會在條碼掃描器授權通知中顯示條碼。

6. 點擊**確定**以儲存變更。

系統完整性監控

Kaspersky Embedded Systems Security 4.0 現在包含系統完整性監控元件，而不是檔案完整性監視器元件。系統完整性監控包括檔案完整性監控的所有功能，此外還允許監控登錄機碼變更和外部裝置的連線。

系統完整性監控監視作業系統中可能表示電腦安全漏洞的變化。當偵測到此類變更時，Kaspersky Embedded Systems Security 會產生相應的事件並向管理員發出警報。系統完整性監控可以即時模式運行，也可以按需執行系統完整性檢查。

即時系統完整性監控

在即時模式下，系統完整性監控追蹤您包含在元件範圍（監控範圍）中的物件的變更。系統完整性監控還可以即時封鎖對此類物件的未經授權的存取。

按需系統完整性檢查

按需系統完整性檢查是一項可以手動或按排程執行的工作。若要執行**基於基線的系統完整性監控**工作，您必須配置元件的範圍（監控範圍）並建立基線。基線是系統中物件的記錄狀態，應用程式在與目前狀態進行比較時將其用作參考。基線在工作首次啟動時建立。

遷移檔案完整性監控設定

當您將 Kaspersky Embedded Systems Security 3.4 或者更早的版本更新至版本 4.1 時，檔案完整性監控和登錄檔存取監控設定會得到自動遷移。作為遷移的一部分，應用程式將監控規則移至系統完整性監控。

關於系統完整性監控規則

為了使系統完整性監控正常運作，您必須新增至少一個規則。*系統完整性監控規則*是定義使用者對檔案或登錄檔的存取權限的一組標準。系統完整性監控可偵測指定*監控範圍*內檔案或登錄檔的變更。監控範圍是系統完整性監控規則的標準之一。

系統完整性監控 允許監控以下物件：

- 檔案
- 登錄檔
- 外部裝置

檔案監控涉及的特殊注意事項

系統完整性監控監控監控檔案和資料夾的變更以及被新增至監控範圍或從監控範圍中刪除的檔案。這些變更可能表明有電腦安全入侵。我們建議新增很少修改的物件或者只有管理員有權存取的物件。這有助於減少系統完整性監控事件數量。

Kaspersky Embedded Systems Security 僅監控即時系統完整性監控開始運行時連線的磁碟上的檔案和資料夾的變更。如果即時系統完整性監控開始運行時未連線磁碟，則即使檔案和資料夾已新增至監控範圍，應用程式也不會監控該磁碟上的檔案和資料夾的變更。

當記錄以下操作之一時，應用程式會產生物件建立事件：建立檔案、增加檔案大小、重寫檔案資料或截斷檔案。因此，如果在應用程式啟動控制封鎖規則操作期間為檔案產生了物件建立事件，這可能是由於禁止建立檔案或禁止修改檔案（包括增加檔案大小、重寫資料和截斷等操作）造成的。

登錄檔監控涉及的特殊注意事項

系統完整性監控 可監控登錄檔。這些變更可能表明有電腦安全入侵。

系統完整性監控監控登錄的以下根鍵：

- HKCR
- HKLM
- HKU
- HKCC
- HKEY_CLASSES_ROOT
- HKEY_LOCAL_MACHINE
- HKEY_USERS
- HKEY_CURRENT_CONFIG

系統完整性監控不支援 HKEY_CURRENT_USER 鍵。您可以在下面指定 HKEY_USERS 下面的一個鍵作為 HKEY_USERS\<user profile ID>\<key>。

外部裝置監控涉及的特殊注意事項

系統完整性監控監控外部裝置的連線和斷開連線。為了防護電腦免受因與此類裝置交換檔案而導致的安全威脅，這樣很有必要。系統完整性監控不會監控對外部裝置的存取，也不會封鎖檔案交換。您可以使用不同的應用程式元件裝置控制配置對裝置的存取。

執行*基於基線的系統完整性監控*工作時，如果外部裝置在作業系統中具有相同的磁碟機字母，應用程式將忽略其重新連線。若要進行記錄，重新連線的裝置必須具有不同的磁碟機字母。

系統完整性監控可監控以下類型外部裝置的連線：

- 卸除式磁碟機（包括 USB 快閃磁碟機）
- 硬碟磁碟機
- 外接式網路卡
- CD/DVD/藍光磁碟機
- 掃描器/攝影機

即時系統完整性監控

系統完整性監控允許即時追蹤作業系統中的變化。您可以追蹤可能表明電腦上存在安全漏洞的變更。此元件可封鎖這些變更或僅記錄變更事件。

為了使系統完整性監控正常運作，您必須新增至少一個規則。系統完整性監控規則是定義使用者對檔案和登錄檔的存取權限的一組標準。系統完整性監控可偵測指定監控範圍內檔案和登錄檔的變更。監控範圍是系統完整性監控規則的標準之一。

如何在卡巴斯基安全管理中心管理主控台中啟用和配置即時系統完整性監控

1. 在卡巴斯基安全管理中心管理主控台樹狀目錄中，選取**政策**。
2. 選擇必要的政策並點擊以開啟政策內容。
3. 在政策屬性視窗中，選取**"系統稽核"**。
4. 在**"系統完整性監控"**區域中點擊**"設定"**。
5. 選擇**"系統完整性監控"**核取方塊。

6. 配置"檔案完整性監控"：

   a. 選擇**檔案**頁簽上的**監控檔案**核取方塊。

   b. 在**用於封鎖規則的操作模式**下面，選擇檔案完整性監控模式：

      - **封鎖**在此模式下，應用程式根據檔案完整性監控規則對檔案執行操作，並在系統完整性監控日誌中產生相應事件。

      - **通知**在此模式下，應用程式僅在系統完整性監控日誌中產生有關觸發的檔案完整性監控規則的事件。

   c. 使用 **新增** 按鈕手動新增檔案完整性監控規則或從 XML 檔案匯入。檔案完整性監控規則設定如下表所述。

   d. 在檔案完整性監視器規則清單中，管理核取方塊以保留需要啟用的規則。

7. 配置登錄檔存取監控：

   a. 選擇**登錄檔**頁簽上的**監控登錄檔**核取方塊。

   b. 在**用於封鎖規則的操作模式**下面，選擇登錄檔存取監控模式：

      - **封鎖**在此模式下，應用程式會根據登錄檔存取監控規則阻止對登錄檔的操作，並在系統完整性監控日誌中產生相應事件。

      - **通知**在此模式下，應用程式僅在系統完整性監控日誌中產生有關觸發的登錄檔存取監控規則的事件。

   c. 使用 **新增** 按鈕手動新增登錄檔存取監控規則或從 XML 檔案匯入。登錄檔存取監控規則設定如下表所述。

   d. 在登錄檔存取監控規則清單中，管理核取方塊以保留需要啟用的規則。

8. 配置外部裝置監控：

   a. 選擇**裝置**頁簽上的**監控裝置**核取方塊。

   b. 在**事件嚴重性級別**下拉式清單中，選擇外部裝置監控事件的重要性等級：*資訊*、 *警告*、*緊急*。

      套用外部裝置監控設定後，應用程式會記住目前的外部裝置連線。隨後，當外部裝置連線或斷開連線時，應用程式會在系統完整性監控日誌中產生相應的事件。

9. 儲存變更。

如何在卡巴斯基安全管理中心網頁主控台中啟用和配置即時系統完整性監控

1. 在網頁主控台的主視窗中，選擇**資產管理 → 政策**。

2. 點擊 Kaspersky Embedded Systems Security 政策的名稱。

   政策內容視窗將開啟。

3. 選擇"**應用程式設定**"標籤。

4. 轉到**系統稽核 → 系統完整性監控** 並點擊 **配置** 按鈕。

5. 選擇"**系統完整性監控**"核取方塊。

6. 配置"檔案完整性監控"：

   a. 選擇**檔案**頁簽上的**監控檔案**核取方塊。

   b. 在**用於封鎖規則的操作模式**下面，選擇檔案完整性監控模式：

      - **封鎖**在此模式下，應用程式根據檔案完整性監控規則對檔案執行操作，並在系統完整性監控日誌中產生相應事件。

      - **通知**在此模式下，應用程式僅在系統完整性監控日誌中產生有關觸發的檔案完整性監控規則的事件。

   c. 使用 **新增** 按鈕手動新增檔案完整性監控規則或從 XML 檔案匯入。檔案完整性監控規則設定如下表所述。

   d. 在檔案完整性監控規則清單中，管理 **狀態** 列以保留您需要啟用的規則。

7. 配置登錄檔存取監控：

   a. 選擇**登錄檔**頁簽上的**監控登錄檔**核取方塊。

   b. 在**用於封鎖規則的操作模式**下面，選擇登錄檔存取監控模式：

      - **封鎖**在此模式下，應用程式會根據登錄檔存取監控規則阻止對登錄檔的操作，並在系統完整性監控日誌中產生相應事件。

      - **通知**在此模式下，應用程式僅在系統完整性監控日誌中產生有關觸發的登錄檔存取監控規則的事件。

   c. 使用 **新增** 按鈕手動新增登錄檔存取監控規則或從 XML 檔案匯入。登錄檔存取監控規則設定如下表所述。

   d. 在登錄檔存取監控規則清單中，管理 **狀態** 列以保留您需要啟用的規則。

8. 配置外部裝置監控：

   a. 選擇**裝置**頁簽上的**監控裝置**核取方塊。

   b. 在**事件嚴重性級別**下拉式清單中，選擇外部裝置監控事件的重要性等級：*資訊*、 *警告*、*緊急*。

      系統完整性監控記錄外部裝置的目前連線情況。在應用程式設定中啟用該元件後，應用程式開始監控外部裝置的連線和中斷連線。隨後，當外部裝置連線或斷開連線時，應用程式會產生相應的事件。

9. 儲存變更。

如何在應用程式主控台中啟用和配置即時系統完整性監控

1. 在 Kaspersky Embedded Systems Security 主控台樹狀目錄中，選擇"**系統稽核 → 系統完整性監控**"。

2. 在 **系統完整性監控** 節點的結果窗格中，點擊 **內容**。

   內容: 系統完整性監控視窗將開啟。

3. 選擇"**系統完整性監控**"核取方塊。

4. 配置“檔案完整性監控”：

   a. 選擇**檔案**頁簽上的**監控檔案**核取方塊。

   b. 在**用於封鎖規則的操作模式**下面，選擇檔案完整性監控模式：

      - **封鎖**在此模式下，應用程式根據檔案完整性監控規則對檔案執行操作，並在系統完整性監控日誌中產生相應事件。
      - **通知**在此模式下，應用程式僅在系統完整性監控日誌中產生有關觸發的檔案完整性監控規則的事件。

   c. 使用 **新增** 按鈕手動新增檔案完整性監控規則或從 XML 檔案匯入。檔案完整性監控規則設定如下表所述。

   d. 在檔案完整性監視器規則清單中，管理核取方塊以保留需要啟用的規則。

5. 配置登錄檔存取監控：

   a. 選擇**登錄檔**頁簽上的**監控登錄檔**核取方塊。

   b. 在**用於封鎖規則的操作模式**下面，選擇登錄檔存取監控模式：

      - **封鎖**在此模式下，應用程式會根據登錄檔存取監控規則阻止對登錄檔的操作，並在系統完整性監控日誌中產生相應事件。
      - **通知**在此模式下，應用程式僅在系統完整性監控日誌中產生有關觸發的登錄檔存取監控規則的事件。

   c. 使用 **新增** 按鈕手動新增登錄檔存取監控規則或從 XML 檔案匯入。登錄檔存取監控規則設定如下表所述。

   d. 在登錄檔存取監控規則清單中，管理核取方塊以保留需要啟用的規則。

6. 配置外部裝置監控：

   a. 選擇**裝置**頁簽上的**監控裝置**核取方塊。

   b. 在**事件嚴重性級別**下拉式清單中，選擇外部裝置監控事件的重要性等級：*資訊*, *警告*, *緊急* 。

      套用外部裝置監控設定後，應用程式會記住目前的外部裝置連線。隨後，當外部裝置連線或斷開連線時，應用程式會在系統完整性監控日誌中產生相應的事件。

7. 儲存變更。

系統完整性監控規則設定

參數	描述
監控該範圍的檔案操作	您要套用檔案完整性監控的範圍。此欄位為必填欄位。 使用遮罩： Kaspersky Embedded Systems Security 輸入遮罩時支援環境變量以及`*`和`?`字元： `*`（星號）字元代表任意一組字元，但 `\` 和 `/` 字元除外（這兩個字元是檔案和資料夾路徑中的檔案和資料夾名稱的分隔符號）。例如，遮罩“`C:\*\*.txt`”將包括位於 C: 磁碟機但是不在子資料夾中所有帶 TXT 副檔名的檔案的路徑。 兩個連續 `*` 字元在檔案或資料夾名稱中代表任意一組字元（包括空集），包括 `\` 和 `/` 字元（這兩個字元是檔案和資料夾路徑中的檔案和資料夾名稱的分隔符號）。例如，遮罩 `C:\Folder\**\*.txt` 將包括位於巢嵌在 `Folder` 內的資料夾（`Folder`自身除外）中所有帶 TXT 副檔名的檔案的路徑。遮罩必須包含至少一個嵌套等級。遮罩 `C:\**\*.txt` 不是有效遮罩。 `?`（問號）字元代表任意單個字元，但 `\` 和 `/` 字元除外（這兩個字元是檔案和資料夾路徑中的檔案和資料夾名稱的分隔符號）。例如，遮罩 `C:\Folder\???.txt` 將包括位於 `Folder` 資料夾中所有帶 TXT 副檔名且名稱由三個字元構成的檔案的路徑。

參數	描述
被監控物件	您可以在此指定登錄機碼的名稱或值。 使用遮罩： Kaspersky Embedded Systems Security 輸入遮罩時支援`*`和`?`字元：
檔案作業	• **偵測**應用程式允許對監控範圍內的檔案進行操作。 • **偵測並封鎖**應用程式的功能取決於所選的檔案完整性監控模式。如果您選擇了*封鎖*模式，系統完整性監控將阻止對監控範圍內的檔案進行操作。如果您選擇了*通知*模式，系統完整性監控將允許對監控範圍內的檔案進行操作。
受信任的使用者和/或使用者群組	受信任使用者是被允許對監控範圍內的檔案和登錄機碼執行操作的使用者。 如果 Kaspersky Embedded Systems Security 偵測到受信任使用者執行的操作，系統完整性監控會產生一個 資訊事件。 您可以在 Active Directory 中、在卡巴斯基安全管理中心的账户清單中或透過手動輸入本機使用者名稱來選擇使用者。
檔案作業標誌/Actions	標記，標誌對應用程式將監視的檔案或登錄機碼採取的操作。
根據所有識別的標誌偵測檔案作業/根據所有識別的標誌偵測登錄檔作業	預設情況下，Kaspersky Embedded Systems Security 會偵測所有檔案/登錄檔操作標記。
根據以下標誌偵測檔案作業/根據以下標誌偵測登錄檔作業	在可用檔案/登錄檔操作清單中，選中要監控的操作旁邊的核取方塊。
可能的話在檔案作業後計算總和檢查碼。總和檢查碼將在工作記錄中予以指示。	如果選中該核取方塊，當偵測到至少帶有一個選定標記的檔案操作時，Kaspersky Embedded Systems Security 將計算修改後的檔案的總和檢查碼。 如果透過多個標記偵測到檔案操作，只計算所有修改後最終檔案的總和檢查碼。 如果清除該核取方塊，Kaspersky Embedded Systems Security 不計算修改的檔案的總和檢查碼。 以下情況不會執行任何總和檢查碼計算： • 如果檔案變為無法使用（例如，由於存取權限變更）。 • 如果偵測到檔案操作的檔案後來被刪除。 預設情況下，會取消勾選核取方塊。
總和檢查碼計算演算法	從下拉式清單中選擇一種總和檢查碼計算演算法： • MD5 雜湊 • SHA256 雜湊
排除項目	在**排除項目**頁簽上，您可以新增要從監控範圍中排除的物件： • 對於檔案完整性監視器規則，您可以指定資料夾清單。 • 對於登錄檔存取監控規則，您可以指定登錄機碼或值。 使用遮罩： **檔案** 元件監視的檔案和資料夾的清單。Kaspersky Embedded Systems Security 輸入遮罩時支援環境變量以及`*`和`?`字元： `*`（星號）字元代表任意一組字元，但`\`和`/`字元除外（這兩個字元是檔案和資料夾路徑中的檔案和資料夾名稱的分隔符號）。例如，遮罩“`C:\*\*.txt`”將包括位於 C: 磁碟機但是不在子資料夾中所有帶 TXT 副檔名的檔案的路徑。 兩個連續`*`字元在檔案或資料夾名稱中代表任意一組字元（包括空集），包括`\`和`/`字元（這兩個字元是檔案和資料夾路徑中的檔案和資料夾名稱的分隔符號）。例如，遮罩`C:\Folder\**\*.txt`將包括位於巢嵌在`Folder`內的資料夾（`Folder`自身除外）中所有帶 TXT 副檔名的檔案的路徑。遮罩必須包含至少一個嵌套等級。遮罩`C:\**\*.txt`不是有效遮罩。 `?`（問號）字元代表任意單個字元，但`\`和`/`字元除外（這兩個字元是檔案和資料夾路徑中的檔案和資料夾名稱的分隔符號）。例如，遮罩`C:\Folder\???.txt`將包括位於`Folder`資料夾中所有帶 TXT 副檔名且名稱由三個字元構成的檔案的路徑。 **登錄檔** Kaspersky Embedded Systems Security 在輸入遮罩時支援`*`和`?`字元：排除條目的優先順序高於監控範圍條目。
事件嚴重性級別	只要監控範圍中的檔案或登錄機碼被修改，Kaspersky Embedded Systems Security 就會記錄檔案修改事件。以下事件嚴重程度級別可用：**資訊**，**警告**，**緊急**。

按需系統完整性檢查

按需系統完整性檢查是一項可以手動或按排程執行的工作。當執行*基於基線的系統完整性監控*工作時，應用程式將監控範圍內包含的物件的目前狀態與它們的*基線*狀態進行比較 。基線在工作首次啟動時建立。

為了使系統完整性監控正常運作，您必須新增至少一個規則。系統完整性監控規則是定義使用者對檔案和登錄檔的存取權限的一組標準。系統完整性監控可偵測指定監控範圍內檔案和登錄檔的變更。監控範圍是系統完整性監控規則的標準之一。

配置基於基線的系統完整性監控工作的監控範圍

預設情況下，*基於基線的系統完整性監控*工作的監控範圍與系統完整性監控的監控範圍相同。您可以為工作配置不同的監控範圍。

系統完整性監控不支援為*系統完整性檢查*工作匯入 HKEY_CURRENT_USER 和 HKEY_CURRENT_CONFIG 金鑰。如果工作的監控範圍包含這些金鑰，應用程式會產生*監控範圍包括不正確的物件*事件。

如何在卡巴斯基安全管理中心管理主控台中為基於基線的系統完整性監控工作配置不同的監控範圍

1. 在卡巴斯基安全管理中心管理主控台樹狀目錄中，選取**工作**。
2. 選取必要的*基於基線的系統完整性監控*工作並雙擊以開啟工作內容。
3. 在開啟的視窗中選擇**"設定"**。
4. 配置檔案監控：
   a. 選擇**檔案**頁簽上的**監控檔案**核取方塊。
   b. 透過選取核取方塊來選擇清單中的規則。
   c. 如有必要，請按一下**新增**按鈕來新增規則 。基線系統完整性監控規則設定如下表所述。
   d. 您也可以從其他來源匯入規則。
5. 配置登錄檔監控：
   a. 選擇**登錄檔**頁簽上的**監控登錄檔**核取方塊。
   b. 透過選取核取方塊來選擇清單中的規則。
   c. 如有必要，請按一下**新增**按鈕來新增規則 。基線系統完整性監控規則設定如下表所述。
   d. 您也可以從其他來源匯入規則。
6. 配置外部裝置監控：
   a. 選擇**裝置**頁簽上的**監控裝置**核取方塊。
   b. 在**事件嚴重性級別**下拉式清單中，選擇外部裝置監控事件的重要性等級：*資訊*、 *警告*、*緊急*。
      基線系統完整性監控記錄在建立基線時已連線外部裝置的資訊。隨後，當連線外部裝置時，應用程式會產生相應的事件。當執行工作時，應用程式不會監控外部裝置的中斷連線。
7. 儲存變更。

如何在網頁主控台中為基於基線的系統完整性監控工作配置不同的監控範圍

1. 在網頁主控台的主視窗中，選擇**資產管理 → 工作**。
2. 選取必要的*基於基線的系統完整性監控*工作並雙擊以開啟工作內容。
3. 在開啟的視窗中選擇**"應用程式設定"**。
4. 配置檔案監控：
   a. 選擇**"監控檔案"**核取方塊。
   b. 透過選取核取方塊來選擇清單中的規則。
   c. 如有必要，請按一下**新增**按鈕來新增規則 。基線系統完整性監控規則設定如下表所述。
   d. 您也可以從其他來源匯入規則。
5. 配置登錄檔監控：
   a. 選擇**"監控登錄檔"**核取方塊。
   b. 透過選取核取方塊來選擇清單中的規則。
   c. 如有必要，請按一下**新增**按鈕來新增規則 。基線系統完整性監控規則設定如下表所述。
   d. 您也可以從其他來源匯入規則。
6. 配置外部裝置監控：
   a. 選擇**"監控裝置"**核取方塊。
   b. 在**事件嚴重性級別**下拉式清單中，選擇外部裝置監控事件的重要性等級：*資訊*, *警告*, *緊急* 。
      「*基於基線的系統完整性監控*」工作會記錄在建立基線時已連線的外部裝置的資訊。隨後，當連線外部裝置時，應用程式會產生相應的事件。當執行工作時，應用程式不會監控外部裝置的中斷連線。
7. 儲存變更。

如何在應用程式主控台中為基於基線的系統完整性監控工作配置不同的監控範圍

如果**基於基線的系統完整性監控**工作在本機建立，或如果在政策屬性的**應用程式設定 → 執行本機系統工作**部分中選擇了**允許使用本機工作**核取方塊，則該工作的屬性可在 Kaspersky Embedded Systems Security 主控台中進行編輯。

1. 在 Kaspersky Embedded Systems Security 主控台樹狀目錄中，選擇**"系統稽核 → 基於基線的系統完整性監控"**。
2. 在 **基於基線的系統完整性監控** 節點的結果窗格中，點擊 **內容**。
   內容: 基於基線的系統完整性監控視窗將開啟。
3. 配置檔案監控：
   a. 選擇**檔案**頁簽上的**監控檔案**核取方塊。
   b. 透過選取核取方塊來選擇清單中的規則。

c. 如有必要，請按一下**新增**按鈕來新增規則 。基線系統完整性監控規則設定如下表所述。

d. 您也可以從其他來源匯入規則。

4. 配置登錄檔監控：

a. 選擇**登錄檔**頁簽上的**監控登錄檔**核取方塊。

b. 透過選取核取方塊來選擇清單中的規則。

c. 如有必要，請按一下**新增**按鈕來新增規則 。基線系統完整性監控規則設定如下表所述。

d. 您也可以從其他來源匯入規則。

5. 配置外部裝置監控：

a. 選擇**裝置**頁簽上的**監控裝置**核取方塊。

b. 在**事件嚴重性級別**下拉式清單中，選擇外部裝置監控事件的重要性等級：*資訊*, *警告*, *緊急* 。

基線系統完整性監控記錄在建立基線時已連線外部裝置的資訊。隨後，當連線外部裝置時，應用程式會產生相應的事件。當執行工作時，應用程式不會監控外部裝置的中斷連線。

6. 儲存變更。

基於基線的系統完整性監控 工作規則的設定

參數	描述
監控該範圍的檔案操作	您要套用檔案完整性監控的範圍。此欄位為必填欄位。 使用遮罩： Kaspersky Embedded Systems Security 輸入遮罩時支援環境變量以及 * 和 ? 字元： *（星號）字元代表任意一組字元，但 \ 和 / 字元除外（這兩個字元是檔案和資料夾路徑中的檔案和資料夾名稱的分隔符號）。例如，遮罩"C:**.txt"將包括位於 C: 磁碟機但是不在子資料夾中所有帶 TXT 副檔名的檔案的路徑。 兩個連續 * 字元在檔案或資料夾名稱中代表任意一組字元（包括空集），包括 \ 和 / 字元（這兩個字元是檔案和資料夾路徑中的檔案和資料夾名稱的分隔符號）。例如，遮罩 C:\Folder***.txt 將包括位於巢嵌在 Folder 內的資料夾（Folder 自身除外）中所有帶 TXT 副檔名的檔案的路徑。遮罩必須包含至少一個嵌套等級。遮罩 C:***.txt 不是有效遮罩。 ?（問號）字元代表任意單個字元，但 \ 和 / 字元除外（這兩個字元是檔案和資料夾路徑中的檔案和資料夾名稱的分隔符號）。例如，遮罩 C:\Folder\???.txt 將包括位於 Folder 資料夾中所有帶 TXT 副檔名且名稱由三個字元構成的檔案的路徑。
被監控物件	您可以在此指定登錄機碼的名稱或值。 使用遮罩： Kaspersky Embedded Systems Security 輸入遮罩時支援 * 和 ? 字元：
排除項目	在**排除項目**頁簽上，您可以新增要從監控範圍中排除的物件： • 對於檔案完整性監視器規則，您可以指定資料夾清單。 • 對於登錄檔存取監控規則，您可以指定登錄機碼或值。 使用遮罩： **檔案** 元件監視的檔案和資料夾的清單。Kaspersky Embedded Systems Security 輸入遮罩時支援環境變量以及 * 和 ? 字元： *（星號）字元代表任意一組字元，但 \ 和 / 字元除外（這兩個字元是檔案和資料夾路徑中的檔案和資料夾名稱的分隔符號）。例如，遮罩"C:**.txt"將包括位於 C: 磁碟機但是不在子資料夾中所有帶 TXT 副檔名的檔案的路徑。 兩個連續 * 字元在檔案或資料夾名稱中代表任意一組字元（包括空集），包括 \ 和 / 字元（這兩個字元是檔案和資料夾路徑中的檔案和資料夾名稱的分隔符號）。例如，遮罩 C:\Folder***.txt 將包括位於巢嵌在 Folder 內的資料夾（Folder 自身除外）中所有帶 TXT 副檔名的檔案的路徑。遮罩必須包含至少一個嵌套等級。遮罩 C:***.txt 不是有效遮罩。 ?（問號）字元代表任意單個字元，但 \ 和 / 字元除外（這兩個字元是檔案和資料夾路徑中的檔案和資料夾名稱的分隔符號）。例如，遮罩 C:\Folder\???.txt 將包括位於 Folder 資料夾中所有帶 TXT 副檔名且名稱由三個字元構成的檔案的路徑。 **登錄檔** Kaspersky Embedded Systems Security 在輸入遮罩時支援 * 和 ? 字元：排除條目的優先順序高於監控範圍條目。
事件嚴重性級別	只要監控範圍中的檔案或登錄機碼被修改，Kaspersky Embedded Systems Security 就會記錄檔案修改事件。以下事件嚴重程度級別可用：**資訊**，**警告**，**緊急**。

執行“基於基線的系統完整性監控”工作

基於基線的系統完整性監控 工作允許檢查檔案或登錄機碼是否有變更以及檢查外部裝置的連線。要檢查檔案是否發生變更，您可以用以下模式執行**基於基線的系統完整性監控**工作：

- **完整掃描**在此模式下，應用程式檢查檔案的所有屬性和雜湊。
- **快速掃描**在此模式下，應用程式僅檢查檔案的屬性。

工作執行的模式不影響對登錄檔或外部裝置的檢查。

如何在卡巴斯基安全管理中心管理主控台中執行基於基線的系統完整性監控工作

1. 在卡巴斯基安全管理中心管理主控台樹狀目錄中，選取**工作**。

   工作清單開啟。

2. 單擊“**新工作**”。

   啟動“工作精靈”。按照精靈的說明進行操作。

3. 選擇“**Kaspersky Embedded Systems Security → 基於基線的系統完整性監控**”。選擇系統完整性監控模式：
   - **完整掃描**在此模式下，應用程式檢查檔案的所有屬性和雜湊。
   - **快速掃描**在此模式下，應用程式僅檢查檔案的屬性。
4. 選取將要執行工作的電腦。下列選項可用：
   - 選取管理伺服器在網路中偵測到的電腦：未分配裝置。特定裝置可包括管理群組中的裝置以及未配置裝置。
   - 手動指定裝置位址或從清單中匯入位址。您可以指定您要將工作分配給的裝置的 NetBIOS 名稱、IP 位址和 IP 子網路。
   - 指定要為其執行工作的所選裝置。
   - 將工作分配給管理群組。在這種情況下，工作分配給先前建立的管理群組中包括的電腦。
5. 選取要執行工作的帳戶。預設情況下，Kaspersky Embedded Systems Security 將使用本機使用者帳戶的權限啟動工作。
6. 配置工作的排程，例如手動或在一週的某一天。
7. 輸入工作的名稱。
8. 結束精靈。如有必要，選中“**精靈完成時執行工作**”核取方塊。您可以在工作內容中監控工作進度。

如何在網頁主控台中執行“基於基線的系統完整性監控”工作

1. 在網頁主控台的主視窗中，選擇**資產管理 → 工作**。

   工作清單開啟。

2. 單擊**"新增"**。

   啟動"工作精靈"。

3. 配置工作設定：

   a. 在**應用程式**下拉式清單中，選取 Kaspersky Embedded Systems Security。

   b. 在**"工作類型"**下拉式清單中，選取**"基於基線的系統完整性監控"**。

   c. 在**"工作名稱"**欄位中，輸入簡要說明，例如*"每週系統完整性檢查"*。

4. 在**"要將工作指派給的裝置"**塊中，選取工作範圍。

5. 按照所選工作範圍選項選取裝置。前往下一步。

6. 選擇總和檢查碼計算演算法。

7. 選取要執行工作的帳戶。預設情況下，Kaspersky Embedded Systems Security 將使用本機使用者帳戶的權限啟動工作。

8. 結束精靈。

   在工作清單中將顯示一個新工作。

9. 點擊新工作。

   工作內容視窗將開啟。

10. 選擇**"應用程式設定"**標籤。

11. 選擇系統完整性檢查模式：

    - **完整掃描**在此模式下，應用程式檢查檔案的所有屬性和雜湊。
    - **快速掃描**在此模式下，應用程式僅檢查檔案的屬性。

12. 儲存變更。

13. 選中該工作旁邊的核取方塊。

14. 點擊**"開始"**。

匯出和匯入系統完整性監控規則

您可以將系統完整性監控規則清單匯出到 XML 檔案。然後，您可以修改檔案，例如，新增大量相同類型的記錄。您可以使用匯出/匯入功能來備份系統完整性監控規則清單，或將清單遷移到其他伺服器。

系統完整性監控不支援為*系統完整性檢查*工作匯入 `HKEY_CURRENT_USER` 和 `HKEY_CURRENT_CONFIG` 金鑰。如果工作的監控範圍包含這些金鑰，應用程式會產生*監控範圍包括不正確的物件*事件。

如何在卡巴斯基安全管理中心管理主控台中匯出和匯入系統完整性監控規則清單

1. 在卡巴斯基安全管理中心管理主控台樹狀目錄中，選取**政策**。
2. 選擇必要的政策並點擊以開啟政策內容。
3. 在政策屬性視窗中，選取**"系統稽核"**。
4. 在**"系統完整性監控"**區域中點擊**"設定"**。
5. 視您要匯出或匯入的規則而定，前往 **檔案** 或 **登錄檔** 索引標籤。
6. 若要匯出檔案規則和登錄規則清單：
   a. 如果您要匯出整個清單，請按一下 按鈕，然後選取 **匯出**。
   b. 如果您只要匯出清單的一部分，請依照下列步驟操作：
      1. 使用 **CTRL** 或 **SHIFT** 鍵選取您要匯出的清單項目。若要選取所有項目，請按 **CTRL+A**。
      2. 按一下 按鈕，然後選取 **匯出所選**。
   c. 在開啟的視窗中，指定要匯出至的 XML 檔案名稱，然後選取要儲存該檔案的資料夾。點擊**"儲存"**按鈕。
   Kaspersky Embedded Systems Security 會將規則清單匯出到 XML 檔案。
7. 匯入檔案/登錄檔規則：
   a. 單擊**"匯入"**。
   在開啟的視窗中，選取要從中匯入規則清單的 XML 檔案。
   b. 開啟檔案。
   如果電腦已經具有規則清單，則 Kaspersky Embedded Systems Security 將提示您刪除現有清單或從 XML 檔案向其中新增新項目。
8. 儲存變更。

如何在網頁主控台中匯出和匯入系統完整性規則清單

1. 在網頁主控台的主視窗中，選擇**資產管理 → 政策**。
2. 點擊 Kaspersky Embedded Systems Security 政策的名稱。
   政策內容視窗將開啟。
3. 選擇**"應用程式設定"**標籤。
4. 轉到**系統稽核 → 系統完整性監控** 並點擊 **配置** 按鈕。
   開啟**"系統完整性監控設定"**視窗。
5. 匯出檔案/登錄檔規則：
   a. 在**檔案**或者**登錄檔**頁簽上，選擇要匯出的規則。
   b. 點擊**匯出**按鈕。這會開啟一個視窗，在該視窗中，指定是要匯出選定規則還是所有規則，然後點擊**匯出**。
   如果您未選擇任何規則，則 Kaspersky Embedded Systems Security 將匯出所有規則。

6. Kaspersky Embedded Systems Security 會將規則清單匯出到 XML 檔案。

7. 匯入檔案/登錄檔規則：

   a. 如果您想要從在 3.4 或更早版本的應用程式中建立的 XML 檔案匯入規則，請在**檔案**或者**登錄檔**頁簽上點擊**從先前的版本匯入**按鈕。

   如果您要從在 4.0 或更高版本中建立的 XML 檔案匯入規則，請點擊**匯入**。

   b. 如果電腦已經具有規則清單，則 Kaspersky Embedded Systems Security 將提示您刪除現有清單或從 XML 檔案向其中新增新項目。

   c. 在開啟的視窗中，選取要從中匯入規則清單的 XML 檔案。

   d. 單擊**"匯入"**。

8. 儲存變更。

如何在應用程式主控台中匯出和匯入系統完整性規則清單

1. 在 Kaspersky Embedded Systems Security 主控台樹狀目錄中，選擇**"系統稽核 → 系統完整性監控"**。

2. 在 **系統完整性監控** 節點的結果窗格中，點擊 **內容**。

   內容: 系統完整性監控視窗將開啟。

3. 視您要匯出或匯入的規則而定，前往 **檔案** 或 **登錄檔** 索引標籤。

4. 若要匯出檔案規則和登錄規則清單：

   a. 如果您要匯出整個清單，請按一下 按鈕，然後選取 **匯出**。

   b. 如果您只要匯出清單的一部分，請依照下列步驟操作：

      1. 使用 **CTRL** 或 **SHIFT** 鍵選取您要匯出的清單項目。若要選取所有項目，請按 **CTRL+A**。

      2. 按一下 按鈕，然後選取 **匯出所選**。

   c. 在開啟的視窗中，指定要匯出至的 XML 檔案名稱，然後選取要儲存該檔案的資料夾。點擊**"儲存"**按鈕。

   Kaspersky Embedded Systems Security 會將規則清單匯出到 XML 檔案。

5. 匯入檔案/登錄檔規則：

   a. 單擊**"匯入"**。

   在開啟的視窗中，選取要從中匯入規則清單的 XML 檔案。

   b. 開啟檔案。

   如果電腦已經具有規則清單，則 Kaspersky Embedded Systems Security 將提示您刪除現有清單或從 XML 檔案向其中新增新項目。

6. 儲存變更。

檢視系統完整性監控報告

若要分析系統完整性監控規則的效能，您可以查看應用程式產生的報告和事件。Kaspersky Embedded Systems Security 產生以下有關該元件的報告：

- 報告觸發監控規則次數最多的電腦
- 報告最常觸發的監控規則

  為了產生有關最常觸發的監控規則的報告，應用程式會記錄以下事件：

  - *偵測到對檔案或資料夾的變更*
  - *僅統計：在受控區域內被禁止的檔案操作*
  - *在受控區域內由受信任使用者執行的受允許檔案操作*
  - *受控區域內的受控檔案操作*

  若要配置這些事件的儲存持續時間，請在政策的**事件組態**部分中指定一般系統完整性監控事件*偵測到對檔案或資料夾的變更*的持續時間。

預設情況下，會建立過去 30 天的報告，包括建立報告的日期。

如何在卡巴斯基安全管理中心管理主控台中檢視系統完整性監控報告

1. 開啟卡巴斯基安全管理中心管理主控台。
2. 在管理主控台樹狀目錄的**"管理伺服器"**節點中選取**"報告"**標籤。
3. 點擊**"新增報告範本"**。

   "新報告範本精靈"將啟動。
4. 按照"報告範本精靈"的說明進行操作。在**選取報告範本類型**步驟，選擇系統完整性監控報告（**其他** 部分）：
   - **檔案完整性監控/系統完整性監控規則最常觸發的前 10 台裝置**
   - **在裝置上觸發頻率最高的檔案完整性監控器/系統完整性監控的前 10 條規則**

   完成新報告範本精靈之後，新報告範本將出現在**"報告"**標籤上。
5. 點擊報告將其開啟。

報告建立過程將開始。此報告將顯示在新視窗中。

如何在網頁主控台中檢視系統完整性監控報告

1. 在網頁主控台的主視窗中，選擇**監控 → 報告**。
2. 點擊**"新增"**。

   "新報告範本精靈"將啟動。

3. 在**其他**部分的**範本**下面，選擇系統完整性監控報告：

   - **檔案完整性監控/系統完整性監控規則最常觸發的前 10 台裝置**
   - **在裝置上觸發頻率最高的檔案完整性監控器/系統完整性監控的前 10 條規則**

   完成新報告範本精靈之後，新報告範本將出現在表格中。

4. 選擇並執行報告。

   報告建立過程將開始。此報告將顯示在新視窗中。

若要檢視應用程式產生的事件，您也可以使用在卡巴斯基安全管理中心主控台中的事件分類。

記錄審查

記錄檢查會基於 Windows 事件記錄分析監控受防護環境的完整性。如果應用程式在系統中偵測到有非典型行為的跡象，它會通知管理員，因為該行為可能表明有人嘗試網路攻擊。

Kaspersky Embedded Systems Security 根據規則分析 Windows 事件記錄和偵測違規。元件包括預定義規則。預定義規則由啟發式分析提供支援。您也可以新增您自己的規則（自訂規則）。當規則觸發時，應用程式會建立一個狀態為“*緊急*”的事件。

如果您想要使用記錄檢查，請確保安全稽核政策已配置且系統正在記錄相關事件（詳情請見 Microsoft 技術支援網站）。

參數	描述
預定義規則	記錄檢查規則清單。預定義規則包括受防護電腦上異常活動的範本。異常活動可能表明有人嘗試攻擊。
自訂規則	使用者新增的記錄檢查規則清單。您可以設定自己的記錄檢查規則觸發條件。為此，您必須輸入一個事件 ID 並選擇一個事件來源。 您可以從標準記錄中選擇一個事件來源：*Application*、*Security*或*System*。您也可以指定協力廠商應用程式的記錄。

新增自訂規則

您可以設定自己的記錄檢查規則觸發條件。為此，您必須輸入一個事件 ID 並選擇一個事件來源。您可以在 Microsoft 技術支援網站上查找事件 ID。您可以從標準記錄中選擇一個事件來源：*Application*、*Security*或*System*。您也可以指定協力廠商應用程式的記錄。您可以使用“事件檢視程式”工具查找協力廠商應用程式記錄的名稱。協力廠商應用程式記錄保留在“應用程式和服務記錄”資料夾（例如，*Windows PowerShell* 記錄）中。

應用程式不檢查指定記錄是否真的存在於 Windows 事件記錄中。如果記錄名稱中有錯誤，則應用程式不監控該記錄的事件。

自訂規則清單已包括卡巴斯基專家建立的多個規則。

如何在卡巴斯基安全管理中心管理主控台中新增自訂規則

1. 在卡巴斯基安全管理中心管理主控台樹狀目錄中，選取**政策**。
2. 選擇必要的政策並點擊以開啟政策內容。
3. 在政策屬性視窗中，選取“**系統稽核**”。
4. 在“**記錄審查**”區域中點擊“**設定**”。
5. 選擇“**記錄審查**”核取方塊。
6. 在“**自訂規則**“頁簽上，選中“**套用記錄審查的自訂規則**”核取方塊。
7. 選中要啟用的自訂規則旁邊的核取方塊。
8. 必要的話點擊**新增**建立您自己的自訂規則。

9. 這會開啟一個視窗；在該視窗中，配置自訂規則：

    - **規則名稱**
    - **記錄名稱**Windows 事件記錄。以下記錄可以使用： *Application*、*Security*、*System*。
    - **來源**協力廠商應用程式記錄。您可以使用"事件檢視程式"工具查找協力廠商應用程式記錄的名稱。協力廠商應用程式記錄保留在"應用程式和服務記錄"資料夾（例如，Windows PowerShell 記錄）中。
    - **事件識別符**Windows 事件記錄中的事件 ID。您可以在 Microsoft 技術文件中查找事件 ID。

10. 儲存變更。

如何在卡巴斯基安全管理中心網頁主控台中新增自訂規則

1. 在網頁主控台的主視窗中，選擇**資產管理 → 政策**。
2. 點擊 Kaspersky Embedded Systems Security 政策的名稱。
   政策內容視窗將開啟。
3. 選擇"**應用程式設定**"標籤。
4. 轉到**系統稽核 → 記錄審查** 並點擊 **配置** 按鈕。
5. 選擇"**啟用記錄審查**"核取方塊。
6. 在"**自訂規則**"頁簽上，選中"**套用記錄檢查的自訂規則**"核取方塊。
7. 使用切換按鈕配置自訂規則：
8. 必要的話點擊**新增**建立您自己的自訂規則。
9. 這會開啟一個視窗；在該視窗中，配置自訂規則：

    - **規則名稱**
    - **Windows 事件記錄名稱**Windows 事件記錄。以下記錄可以使用： *Application*、*Security*、*System*。
    - **來源**協力廠商應用程式記錄。您可以使用"事件檢視程式"工具查找協力廠商應用程式記錄的名稱。協力廠商應用程式記錄保留在"應用程式和服務記錄"資料夾（例如，Windows PowerShell 記錄）中。
    - **事件 ID**Windows 事件記錄中的事件 ID。您可以在 Microsoft 技術文件中查找事件 ID。

10. 儲存變更。

如何在應用程式主控台中新增自訂規則

1. 在 Kaspersky Embedded Systems Security 主控台樹狀目錄中，選擇"**系統稽核 → 記錄審查**"。
2. 在 **記錄審查** 節點的結果窗格中，點擊 **內容**。
   這將開啟 **屬性：記錄審查** 視窗。
3. 選擇"**記錄審查**"核取方塊。
4. 在"**自訂規則**"頁簽上，選中"**套用記錄審查的自訂規則**"核取方塊。

5. 選中要啟用的自訂規則旁邊的核取方塊。

6. 必要的話點擊**新增**建立您自己的自訂規則。

7. 這會開啟一個視窗；在該視窗中，配置自訂規則：

   - **規則名稱**
   - **記錄名稱**Windows 事件記錄。以下記錄可以使用： *Application*、*Security*、*System*。
   - **來源**協力廠商應用程式記錄。您可以使用"事件檢視程式"工具查找協力廠商應用程式記錄的名稱。協力廠商應用程式記錄保留在"應用程式和服務記錄"資料夾（例如，Windows PowerShell 記錄）中。
   - **事件識別符**Windows 事件記錄中的事件 ID。您可以在 Microsoft 技術文件中查找事件 ID。

8. 儲存變更。

結果，當規則觸發時，Kaspersky Embedded Systems Security 將建立"*緊急*"事件。

配置預定義規則

預定義規則包括受防護電腦上異常活動的範本。異常活動可能表明有人嘗試攻擊。預定義規則由啟發式分析提供支援。記錄檢查有七項預定義規則可用。您可以啟用或停用任何這些規則。預定義規則無法被刪除。

您可以為以下操作配置監控事件的規則觸發條件：

- 密碼暴力破解偵測
- 網路登入偵測

如何在卡巴斯基安全管理中心管理主控台中配置預定義規則

1. 在卡巴斯基安全管理中心管理主控台樹狀目錄中，選取**政策**。

2. 選擇必要的政策並點擊以開啟政策內容。

3. 在政策屬性視窗中，選取"**系統稽核**"。

4. 在"**記錄審查**"區域中點擊"**設定**"。

5. 選擇"**記錄審查**"核取方塊。

6. 在"**預定義規則**"頁簽上，選中"**套用預定義的記錄審查規則**"核取方塊。

7. 選擇或清除核取方塊以配置預定義規則：

   - **系統中存在疑似暴力破解攻擊模式**
   - **網路登入工作階段中偵測到一個非典型活動**
   - **存在可能的 Windows 事件記錄濫用模式**
   - **代替安裝的新服務偵測到了非典型操作**

- **偵測到使用明顯憑據的非典型登入名稱**
- **系統中存在疑似 Kerberos 偽造 PAC (MS14-068) 攻擊模式**
- **在有權限的內建管理員群組中偵測到可疑變更**

8. 必要的話配置**系統中存在疑似暴力破解攻擊模式**規則：
   a. 點擊規則旁邊的**"設定"**按鈕。
   b. 在開啟的視窗中，指定嘗試次數和在此期間必須執行密碼輸入嘗試以觸發規則的時間段。
   c. 點擊**OK**。
9. 如果選定**網路登入工作階段中偵測到一個非典型活動**規則，您需要配置其設定：
   a. 點擊規則旁邊的**"設定"**按鈕。
   b. 在開啟的視窗中的**網路登入偵測**塊中，指定時間間隔的開始和結束時間。
      Kaspersky Embedded Systems Security 將在定義的間隔期間執行的登入嘗試視為異常活動。
      預設情況下不設定間隔期間，應用程式不監控登入嘗試。若要讓應用程式持續監控登入嘗試，請將間隔期間設為 12:00 AM – 11:59 PM。間隔期間的開始和結束不得重合。如果它們一樣，應用程式將不監控登入嘗試。
   c. 建立一個受信任使用者和受信任 IP 位址（IPv4 和 IPv6）清單。
      您可以在 Active Directory 中、在卡巴斯基安全管理中心的账户清單中或透過手動輸入本機使用者名稱來選擇使用者。卡巴斯基建議僅在無法使用網域使用者帳戶的特殊情況下使用本機使用者帳戶。Kaspersky Embedded Systems Security 不監控這些使用者和電腦的登入嘗試。

      > 依 IP 位址排除受信任的電腦在 Windows XP 上執行的應用程式中不起作用。

   d. 單擊**"確定"**。
10. 儲存變更。

如何在卡巴斯基安全管理中心網頁主控台中設定預定義規則

1. 在網頁主控台的主視窗中，選擇**資產管理 → 政策**。
2. 點擊 Kaspersky Embedded Systems Security 政策的名稱。
   政策內容視窗將開啟。
3. 選擇**"應用程式設定"**標籤。
4. 轉到**系統稽核 → 記錄審查** 並點擊 **配置** 按鈕。
5. 選擇**"啟用記錄審查"**核取方塊。
6. 在**"預定義規則"**頁簽上，選中**"套用預定義的記錄檢查規則"**核取方塊。

7. 使用開關配置預定義規則：

   - **系統中存在疑似暴力破解攻擊模式**
   - **網路登入工作階段中偵測到一個非典型活動**
   - **存在可能的 Windows 事件記錄濫用模式**
   - **代替安裝的新服務偵測到了非典型操作**
   - **偵測到使用明顯憑據的非典型登入名稱**
   - **系統中存在疑似 Kerberos 偽造 PAC (MS14-068) 攻擊模式**
   - **在有權限的內建管理員群組中偵測到可疑變更**

8. 在**延伸**頁籤上，配置以下設定：

   - 為了觸發規則**系統中存在疑似暴力破解攻擊模式**必須執行的嘗試次數和在此期間內嘗試輸入密碼的時間段。
   - 若要觸發 **網路登入工作階段中偵測到一個非典型活動** 規則，指定應用程式將所有登入嘗試視為異常活動的時間間隔的開始和結束時間。

     預設情況下不設定間隔期間，應用程式不監控登入嘗試。若要讓應用程式持續監控登入嘗試，請將間隔期間設為 12:00 AM – 11:59 PM。間隔期間的開始和結束不得重合。如果它們一樣，應用程式將不監控登入嘗試。

9. 在相應頁簽上建立一個受信任使用者和受信任 IP 位址（IPv4 和 IPv6）清單。

   您可以從帳戶清單中選擇使用者，或手動輸入本機使用者名稱。

   > 依 IP 位址排除受信任的電腦在 Windows XP 上執行的應用程式中不起作用。

10. 儲存變更。

如何在應用程式主控台中配置預定義規則

1. 在 Kaspersky Embedded Systems Security 主控台樹狀目錄中，選擇“**系統稽核 → 記錄審查**”。
2. 在 **記錄審查** 節點的結果窗格中，點擊 **內容**。

   這將開啟 **屬性：記錄審查** 視窗。

3. 選擇“**記錄審查**”核取方塊。
4. 在“**預定義規則**“頁簽上，選中“**套用預定義的記錄審查規則**”核取方塊。
5. 選擇或清除核取方塊以配置預定義規則：

   - **系統中存在疑似暴力破解攻擊模式**
   - **網路登入工作階段中偵測到一個非典型活動**
   - **存在可能的 Windows 事件記錄濫用模式**

- **代替安裝的新服務偵測到了非典型操作**
- **偵測到使用明顯憑據的非典型登入名稱**
- **系統中存在疑似 Kerberos 偽造 PAC (MS14-068) 攻擊模式**
- **在有權限的內建管理員群組中偵測到可疑變更**

6. 必要的話配置**系統中存在疑似暴力破解攻擊模式**規則：
   a. 點擊規則旁邊的**"設定"**按鈕。
   b. 在開啟的視窗中，指定嘗試次數和在此期間必須執行密碼輸入嘗試以觸發規則的時間段。
   c. 點擊**OK**。
7. 如果選定**網路登入工作階段中偵測到一個非典型活動**規則，您需要配置其設定：
   a. 點擊規則旁邊的**"設定"**按鈕。
   b. 在開啟的視窗中的**網路登入偵測**塊中，指定時間間隔的開始和結束時間。

      Kaspersky Embedded Systems Security 將在定義的間隔期間執行的登入嘗試視為異常活動。

      預設情況下不設定間隔期間，應用程式不監控登入嘗試。若要讓應用程式持續監控登入嘗試，請將間隔期間設為 12:00 AM – 11:59 PM。間隔期間的開始和結束不得重合。如果它們一樣，應用程式將不監控登入嘗試。
   c. 建立一個受信任使用者和受信任 IP 位址（IPv4 和 IPv6）清單。

      您可以在 Active Directory 中、在卡巴斯基安全管理中心的账户清單中或透過手動輸入本機使用者名稱來選擇使用者。卡巴斯基建議僅在無法使用網域使用者帳戶的特殊情況下使用本機使用者帳戶。從 Active Directory 建立使用者清單。Kaspersky Embedded Systems Security 不監控這些使用者和電腦的登入嘗試。

      > 依 IP 位址排除受信任的電腦在 Windows XP 上執行的應用程式中不起作用。

   d. 單擊**"確定"**。
8. 儲存變更。

結果，當規則觸發時，Kaspersky Embedded Systems Security 將建立*"緊急"*事件。

按需掃描

本節提供有關自訂掃描工作的資訊，並說明如何配置自訂掃描工作設定和受防護裝置上的安全設定。

關於自訂掃描工作

Kaspersky Embedded Systems Security 會掃描指定區域，以偵測病毒和其他電腦安全威脅。Kaspersky Embedded Systems Security 將掃描受防護裝置檔案、記憶體以及自動執行物件。

Kaspersky Embedded Systems Security 提供以下自訂掃描工作：

- 預設情況下，根據排程每週執行一次「*關鍵區域掃描*」工作。Kaspersky Embedded Systems Security 將掃描作業系統關鍵區域中的物件：自動執行物件、硬碟磁碟機和卸除式磁碟機的開機磁區和主開機記錄、系統記憶體以及處理程序記憶體。Kaspersky Embedded Systems Security 將套用與**Inform**相應的安全設定。您可以修改「*關鍵區域掃描*」工作的設定。

- *應用程式完整性控制*工作每天執行一次。它提供了檢查 Kaspersky Embedded Systems Security 模組是否損壞或修改的選項。檢查程式安裝資料夾。工作執行統計指示檢查的模組數和發現損壞的模組數。預設情況下，工作設定已定義，無法編輯。可以編輯工作啟動排程設定。

- 「*卸除式磁碟機掃描*」工作會掃描您執行或複製的所有檔案，即使檔案位於卸除式磁碟機上也是如此。若要防止病毒和其它惡意軟體的傳播，您可以配置當卸除式磁碟機連線到電腦時對其自動掃描。

- 「*完整掃描*」工作每週執行一次。此工作可確保對受防護裝置進行徹底掃描，包括系統備份儲存、引導磁區和郵件資料庫。

此外，您還可以建立自訂的自訂掃描工作，例如，掃描受防護裝置上的共用資料夾的工作。

Kaspersky Embedded Systems Security 可以一次執行多個自訂掃描工作。

關於工作掃描範圍和安全設定

在應用程式主控台中，選定自訂掃描工作的掃描範圍以 Kaspersky Embedded Systems Security 可以控制的受防護裝置檔案資源清單的形式顯示。

項目或節點將顯示在受防護裝置檔案資源的清單檢視模式中，如下所示：

☑ 節點會包括在掃描範圍內。

☐ 此節點會從掃描範圍中排除。

安全性設定

在所選的自訂掃描工作中，若要修改預設安全設定，可透過將它們配置為用於整個防護或掃描範圍的一般設定，或為裝置檔案資源清單中的不同節點或項配置不同設定。

如果相同物件包含在多個防護範圍條目中，且這些條目具有不同的安全級別，則清單中的最後一條規則優先。例如，假設有一個包含兩個條目的防護範圍：**所有硬碟磁碟機**（**Inform**安全級別）和`*\Users\*\Downloads\*`（**Custom**安全級別）。應用程式會根據「通知」等級掃描硬碟，但`Downloads`資料夾除外。應用程式會按照手動指定的設定掃描`Downloads`資料夾，因為此設定條目是防護範圍清單中的最後一個。

為所選父節點配置的安全設定將自動套用到所有子節點。父節點的安全設定不會套用到單獨配置的子節點。

您可以使用以下方式之一配置選定掃描範圍或防護範圍的設定：

- 選取三個預定義安全等級中的一個（**最大效能**, **建議防護** 或者 **最大防護**）。
- 在受防護裝置檔案資源清單中手動變更選定節點或項的安全設定（安全等級變更為"**自訂**"）。

預定義的掃描範圍

所選自訂掃描工作的受防護裝置檔案資源清單顯示在"**掃描範圍**"視窗中。

檔案資源清單顯示基於配置的 Microsoft Windows 安全設定所擁有讀取存取權限的節點。

Kaspersky Embedded Systems Security 包含以下預定義掃描範圍：

- **所有硬碟磁碟機**Kaspersky Embedded Systems Security 掃描受防護裝置硬碟磁碟機上的物件。您可以在掃描範圍中包含或排除所有硬碟磁碟機、單個磁碟、資料夾或檔案。
- **所有卸除式磁碟機**Kaspersky Embedded Systems Security 掃描外部裝置（如 CD 或卸除式磁碟機）上的檔案。您可以在掃描範圍中包含或排除所有卸除式裝置、單個磁碟、資料夾或檔案。
- **所有網路磁碟機**您可以按照 UNC（通用命名慣例）格式指定網路資料夾或檔案路徑以將它們新增至掃描範圍。用於啟動工作的帳戶必須擁有對新增網路資料夾和檔案的存取權限。預設情況下，自訂掃描在系統帳戶下執行。

  已連線的網路磁碟也不會顯示在受防護裝置檔案資源樹狀目錄中。若要在掃描範圍中包含網路磁碟上的物件，請以 UNC 格式指定對應於該網路磁碟的資料夾。

- **內核記憶體**在啟動掃描之後，Kaspersky Embedded Systems Security 將掃描作業系統中正在執行的處理程序的可執行檔和模組。
- **正在執行的處理程序和啟動物件**Kaspersky Embedded Systems Security 掃描登入機碼和設定檔所引用的物件，例如 WIN.INI 或 SYSTEM.INI，以及在受防護裝置啟動時自動啟動的應用程式模組。
- **磁碟開機磁區**Kaspersky Embedded Systems Security 掃描硬碟磁碟機和卸除式媒體的開機磁區。

- **系統備份**Kaspersky Embedded Systems Security 掃描系統磁碟區資訊資料夾的內容。

  在 Kaspersky Embedded Systems Security 4.1 中，電子郵件被排除在應用程式掃描範圍之外。如果您使用的是較早版本的管理外掛程式，即使政策中包含電子郵件，該應用程式也會將電子郵件排除在掃描範圍之外。

預設情況下，標準掃描範圍顯示在網路檔案資源的樹狀目錄中。在掃描範圍設定中建立時，可以新增至網路檔案資源清單。

預設情況下，"自訂掃描"工作在以下範圍下執行：

- *關鍵區域掃描*工作：
  - **所有硬碟磁碟機**（不包括 Windows 資料夾）
  - **所有卸除式磁碟機**
  - **內核記憶體**
  - **正在執行的處理程序和啟動物件**
- *按需掃描*工作：
  - **所有硬碟磁碟機**（不包括 Windows 資料夾）
  - **所有卸除式磁碟機**
  - **內核記憶體**
  - **正在執行的處理程序和啟動物件**
- *完整掃描*工作：
  - **所有硬碟磁碟機**（不包括 Windows 資料夾）
  - **所有卸除式磁碟機**
  - **內核記憶體**
  - **正在執行的處理程序和啟動物件**
  - **系統備份**
  - **磁碟開機磁區**

線上儲存檔案掃描

關於雲端檔案

Kaspersky Embedded Systems Security 可以與 Microsoft OneDrive 雲端檔案進行互動。應用程式支援新的 OneDrive Files On-Demand 功能。

Kaspersky Embedded Systems Security 不支援其他線上儲存方式。

"OneDrive 檔案隨選"幫助您存取所有 OneDrive 檔案，而無需下載所有檔案和使用裝置上的儲存空間。您可以在需要時將檔案下載到硬碟磁碟機。

當"OneDrive Files On-Demand"功能開啟時，可以在檔案資源管理器的**"狀態"**列中看到每個檔案旁邊的狀態圖示。每個檔案都具有以下狀態之一：

此狀態圖示指示檔案*僅線上可用*。僅線上檔案不會物理儲存在您的硬碟磁碟機中。當裝置未連線到 Internet 時，無法開啟僅線上檔案。

此狀態圖示指示檔案*本機可用*。當開啟僅線上檔案時會顯示此圖示，該檔案會下載到您的裝置中。您可以隨時開啟本機可用的檔案，即使沒有 Internet 存取權限。要清理空間，可以將檔案變更回 僅線上。

此狀態圖示指示檔案*儲存在硬碟磁碟機中並且始終可用*。

雲端檔案掃描

Kaspersky Embedded Systems Security 只能掃描受防護裝置上本機儲存的雲端檔案。此類 OneDrive 檔案的狀態為 和 。在掃描期間會略過 檔案，因為這些檔案沒有物理儲存在受防護裝置上。

Kaspersky Embedded Systems Security 在掃描時不會自動從雲端下載 檔案，即使這些檔案已包括在掃描範圍中。

在各種方案中，雲端檔案由多種 Kaspersky Embedded Systems Security 工作處理，具體取決於工作類型：

- 即時雲端檔案掃描：您可以將包含雲端檔案的資料夾新增到即時檔案防護元件防護範圍中。當使用者存取該檔案時會對其進行掃描。如果使用者存取 檔案，系統會下載該檔案，該檔案將變為本機可用，並且其狀態將變更為 。這樣就可以讓檔案被即時檔案防護元件處理。

- 自訂雲端檔案掃描：您可以將包含雲端檔案的資料夾新增到"自訂掃描"工作的掃描範圍中。該工作會掃描狀態為 和 的檔案。如果在範圍中找到任何 檔案，在掃描期間將略過這些檔案，並在工作記錄中記錄資訊事件，指示所掃描的檔案只是雲端檔案的預留位置，並不存在於本機磁碟機中。

- 產生和使用應用程式啟動控制規則：您可以使用*應用程式啟動控制規則產生器*工作為 和 檔案建立允許規則和拒絕規則。應用程式啟動控制元件套用"預設拒絕"原則和所建立的規則來處理和封鎖雲端檔案。

  應用程式啟動控制元件會封鎖所有雲端檔案啟動，不管它們的狀態如何。應用程式不會將 檔案包括在規則產生範圍中，因為它們沒有實體儲存在硬碟磁碟機上。由於不能為此類檔案建立允許規則，因此對它們實施"預設拒絕"原則。

在 OneDrive 雲端檔案中偵測到威脅時，應用程式會應用執行掃描的工作的設定中指定的操作。因此，可以將檔案刪除、解毒、移至隔離區或備份。

按照相關 Microsoft OneDrive 文件中概述的政策，對本機檔案的變更將與 OneDrive 中儲存的副本進行同步。

關於預定義安全等級

使用啟發式分析 安全設定不包含在預設安全等級的設定中。變更此設定不會變更您選擇的預設安全等級。

您可以將四個預定義安全等級之一套用至裝置檔案資源樹中所選的節點：**最大效能**、**建議防護**、 **最大防護** 或 **通知**。每個等級都包含其自有的預定義安全設定（請參閱下表）。

最大效能

如果您的網路除了在受防護裝置和工作站上使用 Kaspersky Embedded Systems Security 外，還有其他受防護裝置安全措施，例如防火牆和現有安全政策，則建議使用"**最大效能**"安全等級。

建議防護

"**建議防護**"安全等級確保防護與對裝置的效能影響的最佳組合。Kaspersky 專家建議此等級，因為其足以防護大多數公司網路上的裝置。預設情況下，將設定"**建議防護**"安全等級。

最大防護

如果組織的網路有更高的裝置安全要求，則建議使用"**最大防護**"安全等級。

通知

如果公司網路中可能存在許多受感染的電腦並且封鎖它們可能會嚴重破壞組織的運營，則建議使用**通知**安全等級。

預定義安全等級和相應的安全設定值

選項	安全等級			
	最大效能	建議防護	最大防護	通知
Object types	按格式掃描物件	所有物件	所有物件	所有物件
Scan only new and modified files	已啟用	已停用	已停用	已停用
Action to perform on infected and other objects	解毒。若解毒失敗則移除	執行卡巴斯基專家建議的動作	解毒。若解毒失敗則移除	通知

選項	安全等級			
	最大效能	建議防護	最大防護	通知
Scan of compound files	掃描 Microsoft Office 格式的掃描分發套件和檔案	掃描 Microsoft Office 格式的所有存檔、分發套件和檔案	掃描 Microsoft Office 格式的所有存檔、分發套件和檔案	掃描 Microsoft Office 格式的所有存檔、分發套件和檔案
系統關鍵物件是作業系統和 Kaspersky Embedded Systems Security 操作所需的檔案。無法刪除這些檔案。無法終止與此類物件關聯的程序。				
將操作套用到所選的物件類型	預設情況下，掃描所有物件類型	預設情況下，掃描所有物件類型	預設情況下，掃描所有物件類型	預設情況下，掃描所有物件類型
Entirely remove the compound file that cannot be modified by the application in case of embedded object detection	否	否	否	否
排除檔案	否	否	否	否
Do not detect objects by type	否	否	否	否
Stop scanning if it takes longer than (sec)	60 秒	否	否	否
Do not scan compound objects larger than (MB)	8 MB	否	否	否
使用 iSwift 技術	是	是	是	是
使用 iChecker 技術	是	是	是	是

卸除式磁碟機掃描

可以配置透過 USB 連接埠連線到受防護裝置上的卸除式磁碟機的掃描。

當連接的卸除式磁碟機在作業系統中註冊為 USB 外部裝置時，Kaspersky Embedded Systems Security 將掃描這些卸除式磁碟機。如果連線被 裝置控制元件封鎖，則應用程式不會掃描卸除式磁碟機。

Kaspersky Embedded Systems Security 允許在掃描期間存取卸除式磁碟機。

每個卸除式磁碟機的掃描結果提供在連線卸除式磁碟機時建立的自訂掃描工作的工作記錄中。

您可以變更卸除式磁碟機掃描元件的設定（請參閱下表）。

卸除式磁碟機掃描設定

參數	預設值	描述
透過 USB 連線時掃描卸除式磁碟機	已解毒	您可以開啟或關閉透過 USB 連線到受防護裝置時對卸除式磁碟機的掃描。
掃描卸除式磁碟機，如果其大小不超過 (MB)	4096 MB	您可透過在卸除式磁碟機上設定最大資料量，來縮小元件的範圍。 如果儲存的資料量超出指定值，Kaspersky Embedded Systems Security 不會掃描卸除式磁碟機。
掃描使用安全等級	最佳防護	您可透過選擇以下三個安全等級之一來配置建立的自訂掃描工作： • **最大防護** • **建議防護** • **最大效能** • **通知** 當偵測到受感染、可能受感染和其他物件時使用的算法，以及每個安全等級的其他掃描設定，對應於自訂掃描工作中的預設安全等級。

預設自訂掃描工作設定

預設情況下，自訂掃描工作將使用下表所述的設定。您可以配置本機系統和自訂掃描工作。

預設自訂掃描工作設定

參數	預設值	描述
掃描範圍	套用於系統和自訂工作： • **關鍵區域掃描**：整個受防護裝置，排除共用資料夾和某些作業系統檔案。 • **按需掃描**（自訂工作）：整個受防護裝置。 • **完整掃描**：徹底地掃描整個裝置。	您可以變更掃描範圍。無法為**卸除式磁碟機掃描** 和 **應用程式完整性控制** 本機系統工作配置掃描範圍。
安全性設定	整個掃描範圍的一般設定；對應"**建議防護**"安全等級。	您可以對受防護裝置檔案資源清單中選定的節點執行以下操作： • 選擇不同的預定義安全等級 • 手動變更安全性設定
使用啟發式分析	適用於「*關鍵區域掃描*」、「*按需掃描*」和「*完整掃描*」工作的**中**分析層級。	可以啟用或停用"啟發式分析"並設定分析等級。
以特定權限啟動工作的設定	在系統帳戶下啟動工作。	您可以為所有系統工作和自訂掃描工作編輯以特定帳戶權限啟動工作的設定，但「*應用程式完整性控制*」工作除外。
在背景模式下執行工作	未套用	您可以配置自訂掃描工作的優先順序。
將工作視為關鍵區域掃描	適用於「*按需掃描*」、「*關鍵區域掃描*」和「*完整掃描*」工作。	您可以配置自訂掃描工作的優先順序。
不要同時執行多個掃描工作	未套用	您可以配置自訂掃描工作的優先順序。
工作啟動排程	適用於本機系統工作：*關鍵區域掃描*、*應用程式完整性控制*和*完整掃描* – **每月**。	您可以配置排程工作啟動的設定。

管理自訂掃描工作

本節介紹如何在受防護裝置上配置*按需掃描*工作。

建立自訂掃描工作

要在卡巴斯基安全管理中心管理主控台中建立按需掃描工作

1. 啟動新工作精靈。
2. 在**選取工作類型**視窗中，選擇 **按需掃描** 然後點擊 **下一步**。
3. 在"**掃描範圍**"視窗中建立掃描範圍：

根據預設，掃描範圍包括受防護裝置的關鍵區域。掃描範圍在表格中使用圖示 ☑ 標記。排除的掃描範圍在表中用圖示 ☐ 標記。掃描範圍可以修改：新增特定的預先定義的掃描範圍、磁碟、資料夾及檔案，並為每個新增的範圍指定特定的安全設定。

- 若要從掃描中排除某些範圍，請選擇相應的清單項目並點擊**刪除**。
- 要在掃描範圍中包括預定義的掃描範圍、磁碟、資料夾、網路物件或檔案：
  a. 單擊**"新增"**。
  b. 在**選取掃描範圍**視窗中，從清單中選擇預定義掃描範圍，然後點擊**確定**。
- 若要從掃描範圍中排除子資料夾或檔案：
  a. 在**掃描範圍**視窗中選擇新增的資料夾（或磁碟）。
  b. 單擊**"編輯"**。
  c. 停用**包含子資料夾**核取方塊
- 要變更掃描範圍安全設定：
  a. 選擇要編輯其設定的掃描範圍，然後點擊**配置**。
  b. 這將開啟一個視窗；在該視窗中，選擇預定義的安全等級之一，或點擊**設定** 按鈕手動配置安全設定。

安全設定的配置方式與即時檔案防護工作的配置方式相同。

4. 配置啟發式分析器以及與其他元件的整合：
   - 配置啟發式分析器的使用。
   - 您想指派*低*優先順序給工作將在其中執行的工作處理程序，請選擇**在背景模式下執行工作**核取方塊。

     預設情況下，執行 Kaspersky Embedded Systems Security 工作程序的優先順序為*"中"*（正常）。
   - 如果您想將該工作用作*關鍵區域掃描*工作，請選取**將工作視為關鍵區域掃描**核取方塊。
   - 選擇 **不要同時執行多個掃描工作** 核取方塊以最佳化電腦負載。
5. 在**選取要對其指派工作的裝置**視窗中，指定裝置清單並點擊**下一步**。
6. 在**選取要執行此工作的帳戶**視窗中，指定帳戶並點擊**下一步**。
7. 在**設定工作排程**視窗中，配置工作排程並點擊**下一步**。

8. 輸入工作的名稱。

   工作名稱不應超過 100 個字元，並且不能包含以下符號：" * < > & \ : |

9. 開啟“**完成工作建立**”視窗。按一下**完成**按鈕以完成建立工作。

   將為所選受防護裝置或受防護裝置群組建立新的*按需掃描*工作。

要在卡巴斯基安全管理中心網頁主控台中建立按需掃描工作

1. 啟動新工作精靈。
2. 在**新工作**視窗中，在**應用程式**下拉式清單中，選擇**Kaspersky Embedded Systems Security**。
3. 在“**工作類型**”下拉式清單中，選擇“**按需掃描**”，然後點擊“**下一步**”。
4. 選擇工作範圍並點擊 **下一步**。
5. 在**選取要執行此工作的帳戶**視窗中，指定帳戶並點擊**下一步**。
6. 輸入工作的名稱。

   工作名稱不應超過 100 個字元，並且不能包含以下符號：" * < > & \ : |

7. 開啟“**完成工作建立**”視窗。按一下**完成**按鈕以完成建立工作。

   將為所選受防護裝置或受防護裝置群組建立新的*按需掃描*工作。

在應用程式主控台中建立按需掃描工作

單台受防護裝置的自訂工作可以在“**按需掃描**”節點中建立。

要建立和配置新的自訂掃描工作：

1. 在應用程式主控台樹狀目錄中，開啟“**按需掃描**”節點的內容功能表。
2. 請選擇**建立工作**選項。
   開啟“**建立工作**”視窗。
3. 輸入工作名稱並點擊 **確定**。

針對單個受防護裝置的*按需掃描*工作已建立。

在背景執行自訂掃描工作

預設情況下，將為執行 Kaspersky Embedded Systems Security 工作的處理程序分配“*中度（正常）*”優先順序。

將執行*按需掃描*工作的處理程序可以被分配給“*低*”優先順序。將處理程序的優先順序降低會增加執行工作所需的時間，但可能對其他正在執行的程式的處理程序效能產生有利影響。

多個背景工作可以在單個具有低優先順序的工作處理程序中執行。

若要變更現有*按需掃描*工作的優先順序，請選擇或清除工作設定中的 **在背景模式下執行工作**核取方塊。

將儲存已配置的工作設定，這些設定會立即應用到正在執行的工作。如果工作未執行，則將在下次啟動時套用修改後的設定。

記錄關鍵區域掃描執行

預設情況下，裝置防護狀態顯示在「**Kaspersky Embedded Systems Security**」節點的結果窗格中，並在執行「*關鍵區域掃描*」工作後每週更新一次。

裝置防護狀態的更新時間與設定中已選中**將工作視為關鍵區域掃描**核取方塊的自訂掃描工作的排程相關聯。

配置按需掃描工作中的掃描範圍

如果修改了「*作業係統啟動時掃描*」和「*關鍵區域掃描*」工作中的掃描範圍，可以使用設定精靈透過修復 Kaspersky Embedded Systems Security 來還原這些工作中的預設掃描範圍。

在卡巴斯基安全管理中心管理主控台中設定按需掃描工作的掃描範圍

1. 在管理主控台樹狀目錄的**"受管理裝置"**資料夾中，開啟相關用戶端電腦所屬的管理群組名稱的資料夾。
2. 在工作區選取**"裝置"**標籤。
3. 點擊以開啟電腦內容視窗。
4. 轉到**"工作"**區域。
5. 雙擊開啟 **按需掃描** 工作的屬性視窗。
6. 選擇 **掃描範圍** 部分。
7. 若要將範圍新增至掃描範圍，請選取它們旁邊的核取方塊。
8. 如果要新增不在清單中的掃描範圍：
    a. 單擊**"新增"**。
    b. 在顯示的視窗中，選擇範圍、單個磁碟、資料夾或網路位置。
    c. 如果要在掃描範圍中包含子資料夾，請選擇 **包含子資料夾** 核取方塊。
9. 要從掃描範圍中排除單個節點，請清除這些節點名稱旁邊的核取方塊。
10. 若要編輯掃描範圍，請在清單中選擇掃描範圍，然後點擊**編輯**。
11. 若要從網路檔案資源清單中隱藏先前新增的掃描範圍，請選擇掃描範圍並點擊**刪除**。

    將掃描範圍從網路檔案資源清單中刪除時，該掃描範圍也從"自訂掃描"工作範圍中排除。

12. 點擊**OK**。

掃描範圍設定視窗關閉。將儲存新配置的設定。

在卡巴斯基安全管理中心網頁主控台中設定按需掃描工作的掃描範圍

1. 在網頁主控台的主視窗中，選擇**資產管理 → 資產（裝置）**。
2. 點擊您要在其上配置工作的電腦的名稱。
3. 選擇 **工作** 部分。
4. 這將開啟一個視窗；在該視窗中，雙擊以開啟 **按需掃描** 工作的屬性。
5. 選擇**"應用程式設定"**標籤。
6. 若要將範圍新增至掃描範圍，請啟用它們旁邊的開關。
7. 如果要新增不在清單中的掃描範圍：
   a. 單擊**"新增"**。
   b. 在顯示的視窗中，選擇範圍、單個磁碟、資料夾或網路位置。
   c. 如果要在掃描範圍中包含子資料夾，請選擇 **子資料夾** 核取方塊。
8. 要從掃描範圍中排除單個節點，請清除這些節點名稱旁邊的核取方塊。
9. 若要編輯掃描範圍，請在清單中選擇掃描範圍，然後點擊**編輯範圍**。
10. 若要從網路檔案資源清單中隱藏先前新增的掃描範圍，請選擇掃描範圍並點擊**刪除**。

    將掃描範圍從網路檔案資源清單中刪除時，該掃描範圍也從"自訂掃描"工作範圍中排除。

11. 單擊**"儲存"**。

掃描範圍設定視窗關閉。將儲存新配置的設定。

在應用程式主控台中設定按需掃描工作的掃描範圍

1. 在應用程式主控台樹狀目錄中，展開**"按需掃描"**節點。
2. 選擇與要設定的自訂掃描工作相應的子節點。
3. 在已選擇的節點的結果窗格中，點擊**配置防護範圍**連結。
4. 在顯示的視窗中，若要將範圍新增至掃描範圍，請選取它們旁邊的核取方塊。
5. 如果要新增不在清單中的掃描範圍：
   a. 單擊**"新增"**。
   b. 在顯示的視窗中，選擇範圍、單個磁碟、資料夾或網路位置。
   c. 如果要在掃描範圍中包含子資料夾，請選擇 **包含子資料夾** 核取方塊。

6. 要從掃描範圍中排除單個節點，請清除這些節點名稱旁邊的核取方塊。
7. 若要編輯掃描範圍，請在清單中選擇掃描範圍，然後點擊**編輯範圍**。
8. 若要從網路檔案資源清單中隱藏先前新增的掃描範圍，請選擇掃描範圍並點擊**刪除**。

將掃描範圍從網路檔案資源清單中刪除時，該掃描範圍也從"自訂掃描"工作範圍中排除。

9. 單擊"**確定**"。

掃描範圍設定視窗關閉。將儲存新配置的設定。

配置按需掃描工作設定

如何在卡巴斯基安全管理中心管理主控台中設定「按需掃描」工作

1. 在管理主控台樹狀目錄的"**受管理裝置**"資料夾中，開啟相關用戶端電腦所屬的管理群組名稱的資料夾。
2. 在工作區選取"**裝置**"標籤。
3. 點擊以開啟電腦內容視窗。
4. 轉到"**工作**"區域。
5. 雙擊開啟 **按需掃描** 工作的屬性視窗。
6. 選擇 **選項** 部分。
7. 清除或選中"**使用啟發式分析**"核取方塊。
8. 如有必要，請變更分析等級。
9. 您想指派*低*優先順序給工作將在其中執行的工作處理程序，請選擇**在背景模式下執行工作**核取方塊。

預設情況下，執行 Kaspersky Embedded Systems Security 工作程序的優先順序為"*中*"（正常）。

10. 如果您想將該工作用作*關鍵區域掃描*工作，請選取**將工作視為關鍵區域掃描**核取方塊。
11. 選擇 **不要同時執行多個掃描工作** 核取方塊以最佳化電腦負載。
12. 儲存變更。

如何在卡巴斯基安全管理中心網頁主控台中設定「按需掃描」工作

1. 在網頁主控台的主視窗中，選擇**資產管理 → 資產（裝置）**。
2. 點擊您要在其上配置工作的電腦的名稱。
3. 選擇 **工作** 部分。

4. 這將開啟一個視窗；在該視窗中，雙擊以開啟 **按需掃描** 工作的屬性。
5. 選擇 **應用程式設定** 部分。
6. 轉到**"設定"**區域。
7. 清除或選中**"使用啟發式分析"**核取方塊。
8. 如有必要，使用**"啟發式分析等級"**下拉式清單選擇分析級別。
9. 您想指派*低*優先順序給工作將在其中執行的工作處理程序，請選擇**僅在電腦空閒時執行**核取方塊。

> 預設情況下，執行 Kaspersky Embedded Systems Security 工作程序的優先順序為"*中*"（正常）。

10. 如果您想將該工作用作*關鍵區域掃描*工作，請選取**將工作視為關鍵區域掃描**核取方塊。
11. 選擇 **不要同時執行多個掃描工作** 核取方塊以最佳化電腦負載。
12. 儲存變更。

如何在應用程式主控台中設定「按需掃描」工作

1. 在應用程式主控台樹狀目錄中，展開**"按需掃描"**節點。
2. 選擇與要設定的自訂掃描工作相應的子節點。
3. 在所選節點的結果窗格中，點擊**內容**。
4. 選擇**"工作設定"**標籤。
5. 清除或選中**"使用啟發式分析"**核取方塊。
6. 如有必要，請變更分析等級。
7. 您想指派*低*優先順序給工作將在其中執行的工作處理程序，請選擇**在背景模式下執行工作**核取方塊。

> 預設情況下，執行 Kaspersky Embedded Systems Security 工作程序的優先順序為"*中*"（正常）。

8. 如果您想將該工作用作*關鍵區域掃描*工作，請選取**將工作視為關鍵區域掃描**核取方塊。
9. 選擇 **不要同時執行多個掃描工作** 核取方塊以最佳化電腦負載。
10. 儲存變更。

配置卸除式磁碟機掃描

在卡巴斯基安全管理中心管理主控台中設定卸除式磁碟機掃描

1. 展開卡巴斯基安全管理中心管理主控台樹狀目錄中的**"受管理裝置"**節點。
2. 選擇要為其設定工作的管理群組。

3. 選擇“**政策**”標籤。

4. 按兩下要設定的政策名稱。

   在政策內容視窗中，轉至「**補充**」區域。

5. 在 **卸除式磁碟機掃描** 子部分中點擊 **設定**。

   開啟“**卸除式磁碟機掃描**”視窗。

6. 執行以下操作：

   - 如果想讓 Kaspersky Embedded Systems Security 在卸除式磁碟機連線時自動掃描，請選擇“**透過 USB 連線時掃描卸除式磁碟機**”核取方塊。
   - 如果需要，請選擇 **掃描卸除式磁碟機，如果其大小不超過 (MB)** 並在右側欄位中指定最大值。
   - 在**掃描使用安全等級**下拉清單中，指定您想要用於卸除式磁碟機掃描工作之設定的安全等級。

7. 點擊**OK**。

即會儲存並套用指定設定。

在卡巴斯基安全管理中心網頁主控台中設定卸除式磁碟機掃描

1. 在網頁主控台的主視窗中，選擇**資產管理 → 政策**。

2. 點擊 Kaspersky Embedded Systems Security 政策的名稱。

   政策內容視窗將開啟。

3. 選擇“**應用程式設定**”標籤。

4. 轉到“**補充**”區域。

5. 在**卸除式磁碟機掃描**下面，點擊**配置**。

   開啟“**卸除式磁碟機掃描**”視窗。

6. 執行以下操作：

   - 如果想讓 Kaspersky Embedded Systems Security 在卸除式磁碟機連線時自動掃描，請選擇“**透過 USB 連線時掃描卸除式磁碟機**”核取方塊。
   - 如果需要，請選擇 **掃描卸除式磁碟機，如果其大小不超過 (MB)** 並在右側欄位中指定最大值。
   - 在**掃描使用安全等級**下拉清單中，指定您想要用於卸除式磁碟機掃描工作之設定的安全等級。

7. 點擊**OK**。

即會儲存並套用指定設定。

在應用程式主控台中設定卸除式磁碟機掃描

1. 在應用程式主控台樹狀目錄中，開啟“**Kaspersky Embedded Systems Security**”節點上的內容功能表，並選擇“**卸除式磁碟機掃描**”。

   開啟“**卸除式磁碟機掃描**”視窗。

2. 執行以下操作：

   - 如果想讓 Kaspersky Embedded Systems Security 在卸除式磁碟機連線時自動掃描，請選擇**"透過 USB 連線時掃描卸除式磁碟機"**核取方塊。
   - 如果需要，請選擇 **掃描卸除式磁碟機，如果其大小不超過 (MB)** 並在右側欄位中指定最大值。
   - 在**掃描使用安全等級**下拉清單中，指定您想要用於卸除式磁碟機掃描工作之設定的安全等級。

3. 單擊**"確定"**。

為自訂掃描工作選擇預定義的安全等級

可以為受防護裝置檔案資源清單中的選定節點套用以下三個預定義安全等級之一：**最大效能**、**建議防護**和**最大防護**。

在卡巴斯基安全管理中心管理主控台中選擇預定義的安全等級之一

1. 在管理主控台樹狀目錄的**"受管理裝置"**資料夾中，開啟相關用戶端電腦所屬的管理群組名稱的資料夾。
2. 在工作區選取**"裝置"**標籤。
3. 點擊以開啟電腦內容視窗。
4. 轉到**"工作"**區域。
5. 雙擊開啟 **按需掃描** 工作的屬性視窗。
6. 選擇 **掃描範圍** 部分。
7. 在受防護裝置清單中，選擇一個包含在掃描範圍中的項目以設定預定義安全等級。
8. 單擊**"配置"**。
9. 這將開啟一個視窗；在該視窗的**安全等級**頁簽上，選擇要套用的安全等級。
10. 單擊**"確定"**。
11. 在「**內容：按需掃描**」視窗中，點擊「**確定**」按鈕。

將儲存已配置的工作設定，這些設定會立即應用到正在執行的工作。如果工作未執行，則將在下次啟動時套用修改後的設定。

在應用程式主控台中選擇預定義的安全等級之一

1. 在應用程式主控台樹狀目錄中，展開**"按需掃描"**節點。
2. 選擇與要設定的自訂掃描工作相應的子節點。
3. 在所選節點的結果窗格中，點擊**配置防護範圍**。
4. 在受防護裝置的網路檔案資源清單中，選擇需要為其設定預定義安全等級的節點或項目。
5. 確保選定的節點或項包含在掃描範圍中。

6. 單擊**"配置"**。

7. 這將開啟一個視窗；在該視窗中，選擇您選擇的安全等級。

   該視窗將顯示與選定安全等級相對應的安全設定清單。

8. 單擊**"確定"**。

將儲存工作設定，並將這些設定立即應用到正在執行的工作。如果工作未執行，則將在下次啟動時套用修改後的設定。

手動配置安全性設定

預設情況下，自訂掃描工作對整個掃描範圍使用通用安全設定。

這些設定對應于**"建議防護"**預定義安全等級。

可以透過將安全設定配置為用於整個掃描範圍的一般設定，或配置為受防護裝置檔案資源清單或樹狀目錄中節點的不同項目的不同設定，來修改安全設定的預設值。

在卡巴斯基安全管理中心管理主控台中手動管理安全設定

1. 在管理主控台樹狀目錄的**"受管理裝置"**資料夾中，開啟相關用戶端電腦所屬的管理群組名稱的資料夾。

2. 在工作區選取**"裝置"**標籤。

3. 點擊以開啟電腦內容視窗。

4. 轉到**"工作"**區域。

5. 雙擊開啟 **按需掃描** 工作的屬性視窗。

6. 選擇 **掃描範圍** 部分。

7. 在受防護裝置清單中，選擇一個包含在掃描範圍中的項目以管理安全設定。

8. 單擊**"配置"**。

9. 這將開啟一個視窗；在該視窗的**安全等級**頁簽上，選擇要套用的安全等級。

10. 選擇要配置其安全設定的資源。

11. 單擊**"配置"**。

12. 在開啟的視窗中，選擇所需安全等級並按一下**設定**。

13. 在**一般**頁籤上，配置以下設定：

    - 應包括在防護範圍中的物件：

      - **所有物件**Kaspersky Embedded Systems Security 掃描所有物件。

      - **按格式掃描的物件**Kaspersky Embedded Systems Security 僅根據檔案格式掃描感染物件。Kaspersky 編制了該格式清單。它包含在 Kaspersky Embedded Systems Security 資料庫中。

- **按病毒資料庫中指定的副檔名清單掃描的物件**Kaspersky Embedded Systems Security 僅根據檔案副檔名掃描感染的物件。Kaspersky 編制了該副檔名清單。它包含在 Kaspersky Embedded Systems Security 資料庫中。
- **依照指定延伸程式清單掃描的物件**Kaspersky Embedded Systems Security 僅根據檔案副檔名掃描感染的物件。副檔名清單由使用者手動指定。

- 在"**最佳化**"區塊中，選擇或者清除"**只防護新增及修改的檔案**"核取方塊。
- 在"**掃描複合檔案**"部分中，指定要包含在掃描範圍內的複合物件：
  - **掃描壓縮檔案**
  - **掃描分發套件**
  - **掃描 Microsoft Office 格式的檔案**
  - **掃描電子郵件格式檔案**

14. 在**操作**頁籤上，配置以下設定：
- 選擇要對受感染的物件和其他偵測到的物件執行的操作：
  - **清除**
  - **Disinfect. Delete if disinfection fails**
  - **刪除**
  - **建議**
  - **通知**
- 選擇依威脅類型對物件執行的操作：
  a. 清除或選中"**將操作套用到所選的物件類型**"核取方塊。
  b. 點擊 **設定** 並選擇要偵測的物件類型。
- 配置對不可修改的複合檔案的操作：清除或選擇 **在偵測到內嵌物件時完全刪除應用程式無法修改的複合檔案** 核取方塊。

15. 在**最佳化**頁籤上，配置以下設定：
- 在**排除項目**塊中：
  - 清除或選中"**排除檔案**"核取方塊。
  - 清除或選中"**不依照類型偵測物件**"核取方塊。
    針對每個設定點擊"**編輯**"按鈕以新增排除項目。
- 在**進階設定**塊中：
  - **如果超過以下時間（秒）則停止掃描**

- 如果復合物件大於 (MB) 則不掃描
- 使用 iSwift 技術
- 使用 iChecker 技術

16. 儲存新的安全設定。

在卡巴斯基安全管理中心網頁主控台中手動管理安全設定

1. 在網頁主控台的主視窗中，選擇**資產管理 → 資產（裝置）**。
2. 點擊您要在其上配置工作的電腦的名稱。
3. 選擇 **工作** 部分。
4. 這將開啟一個視窗；在該視窗中，雙擊以開啟 **按需掃描** 工作的屬性。
5. 選擇 **應用程式設定** 部分。
6. 轉到**"掃描範圍"**區域。
7. 在受防護裝置的網路檔案資源清單中，選擇要管理其安全設定的項目。確保選定的項目包含在掃描範圍中。
8. 單擊**"編輯"**。
9. 在下拉式清單中選擇身分防護模式：
   - **所有物件**Kaspersky Embedded Systems Security 掃描所有物件。
   - **按格式掃描的物件**Kaspersky Embedded Systems Security 僅根據檔案格式掃描感染物件。Kaspersky 編制了該格式清單。它包含在 Kaspersky Embedded Systems Security 資料庫中。
   - **按病毒資料庫中指定的副檔名清單掃描的物件**Kaspersky Embedded Systems Security 僅根據檔案副檔名掃描感染的物件。Kaspersky 編制了該副檔名清單。它包含在 Kaspersky Embedded Systems Security 資料庫中。
   - **依照指定延伸程式清單掃描的物件**Kaspersky Embedded Systems Security 僅根據檔案副檔名掃描感染的物件。副檔名清單由使用者手動指定。
10. 選擇或清除 **只防護新增及修改的檔案** 核取方塊並指定是否要在掃描中包含 子資料夾。
11. 管理複合物件防護設定：
    - 掃描壓縮檔案
    - 掃描分發套件
    - 掃描 Microsoft Office 格式的檔案
    - 掃描電子郵件格式檔案

12. 選擇要對受感染的物件和其他偵測到的物件執行的操作：

    - **清除**
    - **Disinfect. Delete if disinfection fails**
    - **刪除**
    - **建議**
    - **通知**

13. 選擇依威脅類型對物件執行的操作：

    a. 清除或選中“**將操作套用到所選的物件類型**”核取方塊。

    b. 點擊 **設定** 並選擇要偵測的物件類型。

14. 配置對不可修改的複合檔案的操作：清除或選擇 **在偵測到內嵌物件時完全刪除應用程式無法修改的複合檔案** 核取方塊。

15. 在**排除項目**塊中：

    - 清除或選中“**排除檔案**”核取方塊。
    - 清除或選中“**不依照類型偵測物件**”核取方塊。

16. 在**新增金鑰**塊中：

    - **如果超過以下時間（秒）則停止掃描**
    - **如果復合物件大於 (MB) 則不掃描**
    - **使用 iSwift 技術**
    - **使用 iChecker 技術**

17. 儲存新的安全設定。

在應用程式主控台中手動管理安全設定

1. 在應用程式主控台樹狀目錄中，展開“**按需掃描**”節點。
2. 選擇與要設定的自訂掃描工作相應的子節點。
3. 在所選節點的結果窗格中，點擊**配置防護範圍**。
4. 在受防護裝置的網路檔案資源清單中，選擇要管理其安全設定的項目。
5. 確保選定的項目包含在掃描範圍中。
6. 單擊“**配置**”。
7. 在開啟的視窗中，選擇所需安全等級並按一下**設定**。

8. 在**一般**頁籤上，配置以下設定：

- 應包括在防護範圍中的物件：
  - **所有物件**Kaspersky Embedded Systems Security 掃描所有物件。
  - **按格式掃描的物件**Kaspersky Embedded Systems Security 僅根據檔案格式掃描感染物件。Kaspersky 編制了該格式清單。它包含在 Kaspersky Embedded Systems Security 資料庫中。
  - **按病毒資料庫中指定的副檔名清單掃描的物件**Kaspersky Embedded Systems Security 僅根據檔案副檔名掃描感染的物件。Kaspersky 編制了該副檔名清單。它包含在 Kaspersky Embedded Systems Security 資料庫中。
  - **依照指定延伸程式清單掃描的物件**Kaspersky Embedded Systems Security 僅根據檔案副檔名掃描感染的物件。副檔名清單由使用者手動指定。
- 在"**最佳化**"區塊中，選擇或者清除"**只防護新增及修改的檔案**"核取方塊。
- 在"**掃描複合檔案**"部分中，指定要包含在掃描範圍內的複合物件：
  - **掃描壓縮檔案**
  - **掃描分發套件**
  - **掃描 Microsoft Office 格式的檔案**
  - **掃描電子郵件格式檔案**

9. 在**操作**頁籤上，配置以下設定：

- 選擇要對受感染的物件和其他偵測到的物件執行的操作：
  - **清除**
  - **Disinfect. Delete if disinfection fails**
  - **刪除**
  - **建議**
  - **通知**
- 選擇依威脅類型對物件執行的操作：
  a. 清除或選中"**將操作套用到所選的物件類型**"核取方塊。
  b. 點擊 **設定** 並選擇要偵測的物件類型。
- 配置對不可修改的複合檔案的操作：清除或選擇 **在偵測到內嵌物件時完全刪除應用程式無法修改的複合檔案** 核取方塊。

10. 在**最佳化**頁籤上，配置以下設定：

- 在**排除項目**塊中：
  - 清除或選中**"排除檔案"**核取方塊。
  - 清除或選中**"不依照類型偵測物件"**核取方塊。

  針對每個設定點擊**"編輯"**按鈕以新增排除項目。
- 在**進階設定**塊中：
  - **如果超過以下時間（秒）則停止掃描**
  - **如果復合物件大於 (MB) 則不掃描**
  - **使用 iSwift 技術**
  - **使用 iChecker 技術**

11. 儲存新的安全設定。

自訂掃描工作統計

執行*按需掃描*工作時，您可以檢視有關 Kaspersky Embedded Systems Security 自啟動以來已處理的物件數量的資訊。

即使工作暫停，也仍可檢視該資訊。您可以在工作記錄中檢視工作統計。

要檢視「按需掃描」工作統計資料：

1. 在應用程式主控台樹狀目錄中，展開**"按需掃描"**節點。
2. 選擇您要檢視統計的自訂掃描工作。

   工作統計顯示在選定節點的結果窗格的**"統計資料"**部分中。

下表給出了 Kaspersky Embedded Systems Security 自啟動以來已處理的物件的資訊。

自訂掃描工作統計

欄位	描述
偵測到	Kaspersky Embedded Systems Security 偵測到的物件數量。例如，如果 Kaspersky Embedded Systems Security 在五個檔案中偵測到一個惡意軟體物件，該欄位中的值將增加 1。
感染物件和其他物件	Kaspersky Embedded Systems Security 發現並歸類為"受感染"的物件數量，或者發現的未從掃描中排除且歸類為可被入侵者用來破壞裝置或個人資料的合法軟體檔案數量。
物件未解毒	Kaspersky Embedded Systems Security 因以下原因未解毒的物件數： • 偵測到的物件是無法解毒的類型。 • 解毒時發生錯誤。
物件已解毒	Kaspersky Embedded Systems Security 已解毒的物件的數量。
物件被移除	被 Kaspersky Embedded Systems Security 成功刪除的物件數量。
物件未掃描	Kaspersky Embedded Systems Security 在防護範圍中無法掃描（例如，其他應用程式封鎖存取物件）的物件數。

欄位	描述
壓縮檔案	Kaspersky Embedded Systems Security 掃描的壓縮檔案數量。
壓縮物件	Kaspersky Embedded Systems Security 掃描的壓縮物件數量。
受密碼防護的物件	由於受密碼防護而導致 Kaspersky Embedded Systems Security 略過的物件（如壓縮檔案）數目。
已損壞的物件	由於格式遭損壞而導致 Kaspersky Embedded Systems Security 錯過的物件數目。
處理錯誤	處理中導致錯誤的物件數目。
未移除的物件	Kaspersky Embedded Systems Security 嘗試刪除但無法刪除（例如，由於其他應用程式封鎖存取物件）的物件數。
物件未處理	Kaspersky Embedded Systems Security 未處理的物件總數。

透過點擊結果窗格中**"管理"**部分的**"開啟工作記錄"**連結在選定工作記錄中檢視按需掃描工作統計。

建議您在工作完成後手動處理工作記錄中**"事件"**頁簽上記錄的事件。

Kaspersky Embedded Systems Security 資料庫和軟體模組更新

本部分包含有關 Kaspersky Embedded Systems Security 更新的更新工作和回溯的資訊，以及工作配置說明。

在美國使用的軟體可能無法提供更新功能（包括防毒軟體簽章更新和程式碼庫更新）。

更新資料庫和應用程式模組

更新 Kaspersky Embedded Systems Security 的資料庫和程式模組可為您的電腦提供最新防護。新病毒和其他類型的惡意程式每天都在全世界出現。Kaspersky Embedded Systems Security 資料庫包含關於威脅的資訊和解毒的方法。要快速偵測到威脅，建議您定期更新資料庫和應用程式模組。

定期更新需要一份程式要使用的活動授權檔案。如果目前沒有產品授權，您將只能執行一次更新。

Kaspersky Embedded Systems Security 會從 Kaspersky 的 HTTP 或 FTP 更新伺服器、卡巴斯基安全管理中心管理伺服器或其他更新來源下載應用程式資料庫和模組更新。

您可以將更新下載到每個受防護的裝置，或使用受防護的裝置作為中介。更新將複製到其中，然後分配到受防護裝置。如果您使用卡巴斯基安全管理中心集中管理組織的裝置安全，則可以運用管理伺服器作為下載更新的 Proxy。

如果更新下載過程中斷或者產生錯誤，Kaspersky Embedded Systems Security 將自動轉換至使用上次更新的資料庫。如果 Kaspersky Embedded Systems Security 資料庫損壞，可以手動回溯至先前安裝的更新。

當執行更新時，以下物件將下載並安裝到您的電腦中：

- Kaspersky Embedded Systems Security 資料庫。由於資料庫包含了威脅簽章和關於如何刪除威脅的資訊，電腦因此而獲得防護。當搜尋並為受感染檔案解毒時，防護元件將使用此資訊。資料庫將不斷更新應對它們的方法和新威脅記錄。因此，我們建議您定期更新資料庫。

  除了 Kaspersky Embedded Systems Security 資料庫之外，系統也會更新已啟用程式元件以攔截網路流量的網路驅動程式。

- 程式模組。更新程式模組可以修復 Kaspersky Embedded Systems Security 中的弱點、新增新功能或強化現有功能。

更新時，您的電腦上的程式模組和資料庫將與最新版本更新來源進行對比。如果您目前資料庫和程式模組與對應的最新版本不同，缺少的更新部分將安裝在您的電腦上。

如果資料庫過期，更新量可能會很大，這可能會花費更多的網際網路流量（最多達幾十 MB）。

Kaspersky Embedded Systems Security 資料庫的目前狀態相關資訊顯示在應用程式主視窗中，或者通知區域中當您將游標懸浮在應用程式圖示上看到的工具提示中。

有關更新工作執行期間更新結果和所有發生事件的資訊將記錄在更新工作記錄中。

關於更新工作

Kaspersky Embedded Systems Security 有兩個更新工作：*更新* 和 *更新回溯*。

更新

預設情況下，Kaspersky Embedded Systems Security 會將資料庫和（如果可用）應用程式模組從更新來源複製到裝置，並在防護元件中立即開始使用這些資料庫。"自訂掃描"工作將在下次啟動時開始使用更新的資料庫。

您可以配置*更新*工作的設定。修改工作設定後，Kaspersky Embedded Systems Security 會在下次啟動工作時套用新值。

預設會將 *更新* 工作設定為 **手動** 模式。不允許暫停和還原更新工作。

更新回溯

該工作將使 Kaspersky Embedded Systems Security 回到先前的資料庫和應用程式模組。

預設情況下，已停用*更新回溯*工作。

Kaspersky Embedded Systems Security 資料庫和模組更新方案

*更新*工作中更新來源的選擇取決於組織中使用的資料庫和軟體模組的更新方案。

您可以使用以下方案在受防護裝置上更新 Kaspersky Embedded Systems Security 資料庫和模組：

- 直接透過網際網路將更新下載到每個受防護裝置（方案 1）。
- 透過網際網路將更新下載到中間裝置，然後再將更新從該裝置分發到受防護裝置。
  任何安裝了以下應用程式的裝置都可以充當中介：
  - Kaspersky Embedded Systems Security（方案 2）。
  - 卡巴斯基安全管理中心管理伺服器（方案 3）。

  使用中間裝置進行更新不僅可減少網際網路流量，還提供了額外的網路受防護裝置安全性。
- 透過安全的卸除式磁碟機將資料庫更新下載到每個受防護的裝置（方案 4）。

下面說明了列出的更新方案。

方案 1。直接從 Internet 更新資料庫和模組

要設定直接透過網際網路進行 Kaspersky Embedded Systems Security 更新：

在每個受防護裝置上，在*更新*工作的設定中，將 Kaspersky 的更新伺服器指定為更新來源。

您可以將擁有更新資料夾的其他 HTTPS 或 HTTP 伺服器配置為更新來源。

方法 1：直接從網際網路更新資料庫和模組

方案 2。透過一個受防護裝置更新資料庫和模組

要設定透過一個受防護裝置接收 Kaspersky Embedded Systems Security 的更新：

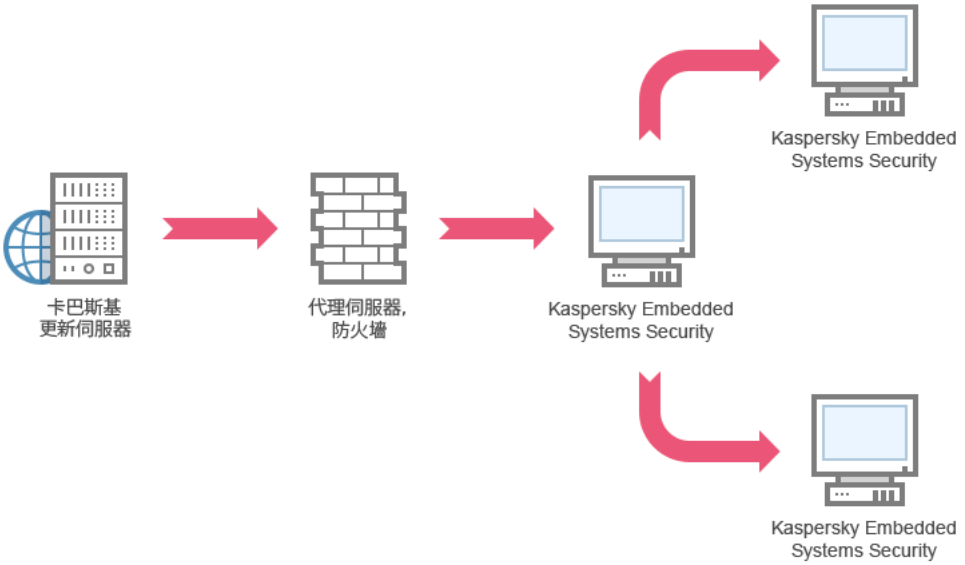
1. 將更新複製到選定的受防護裝置。
   - 在選定受防護裝置上設定*更新*工作設定：
     a. 指定 Kaspersky 的更新伺服器作為更新來源。
     b. 指定用作儲存更新的資料夾的共用資料夾。

2. 將更新分發到其他受防護裝置：

- 在每個受防護的裝置上設定*更新*工作。

  對於更新來源，在中間裝置磁碟機上指定一個用於儲存下載更新的資料夾。

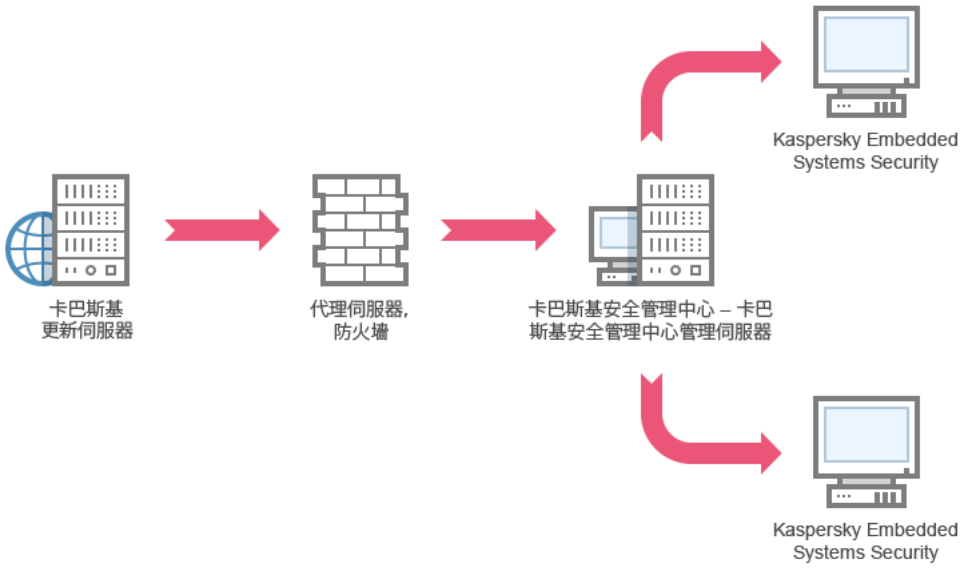
Kaspersky Embedded Systems Security 將透過一個受防護裝置獲取更新。



方法 2：透過一個受防護裝置更新資料庫和模組

方案 3。透過卡巴斯基安全管理中心管理伺服器更新資料庫和模組

如果您使用卡巴斯基安全管理中心集中管理裝置的防毒防護，您可以透過本機網路上安裝的卡巴斯基安全管理中心管理伺服器下載更新。



方法 3：透過卡巴斯基安全管理中心管理伺服器更新資料庫和模組

為了設定透過卡巴斯基安全管理中心管理伺服器接收 Kaspersky Embedded Systems Security 的更新：

1. 在每個受防護的裝置上安裝網路代理程式。網路代理程式是卡巴斯基安全管理中心分發套件中包含的軟體元件。這可確保受防護裝置上的管理伺服器與 Kaspersky Embedded Systems Security 進行互動。有關網路代理以及使用卡巴斯基安全管理中心對其進行配置的詳細資訊，請參見*卡巴斯基安全管理中心管理說明*。

2. 將更新從 Kaspersky 更新伺服器下載到卡巴斯基安全管理中心管理伺服器。

   - 針對指定的受防護裝置集合配置 *將更新下載至管理伺服器儲存區*。

     指定 Kaspersky 的更新伺服器作為更新來源。

3. 將更新分發到受防護裝置。為此，請執行以下操作之一：

   - 在卡巴斯基安全管理中心上，設定病毒資料庫（應用程式模組）更新群組工作以將更新發佈到受防護裝置：

   - 在每個受防護的裝置上設定*更新*工作：

     a. 指定卡巴斯基安全管理中心管理伺服器作為更新來源。

     b. 若有必要，設定工作排程。

Kaspersky Embedded Systems Security 將透過卡巴斯基安全管理中心管理伺服器獲取更新。

方案 4。從安全的卸除式磁碟機更新應用程式資料庫

若要使用安全卸除式磁碟機更新 Kaspersky Embedded Systems Security 資料庫：

1. 將安全卸除式磁碟機連接至已安裝 Kaspersky Embedded Systems Security 且可存取應用程式資料庫更新的裝置。

2. 為已連線的卸除式磁碟機新增 裝置控制 元件的允許規則。

3. 在應用程式主控台中，設定並啟動 *安全複製應用程式資料庫*工作。

4. 將包含資料庫更新的安全卸除式磁碟機連接至需要更新應用程式資料庫的裝置。

5. 在應用程式主控台中，設定並啟動 *應用程式資料庫安全更新* 工作。

Kaspersky Embedded Systems Security 將從安全卸除式磁碟機接收更新的應用程式資料庫。

設定更新工作

如何在卡巴斯基安全管理中心管理主控台中設定「更新」工作

1. 在卡巴斯基安全管理中心管理主控台中，轉至您要設定的 本機 或群組更新工作。

2. 開啟 **設定** 部分。

3. 在連線到卡巴斯基安全管理中心管理伺服器的 Kaspersky Embedded Systems Security 的**本機模式更新設定**下面，設定更新來源：

   a. 單擊**"設定"**。

   開啟**"資料庫和應用程式模組更新"**視窗。

   b. 選中要使用的更新來源旁邊的核取方塊：

   - 卡巴斯基安全管理中心管理伺服器
   - 卡巴斯基更新伺服器

   如有必要，請點擊 **新增** 按鈕新增自訂更新來源。

   c. 如果您選擇多個更新來源，請使用 **向上** 和 **向下** 按鈕依優先順序對更新來源進行排序。Kaspersky Embedded Systems Security 嚴格按照配置的順序存取更新來源，並使用第一個可用更新來源中的更新套件執行更新工作。

   預設情況下，Kaspersky Embedded Systems Security 使用卡巴斯基安全管理中心伺服器作為第一個更新來源。這有助於在更新時節省流量。如果政策未被套用到電腦，卡巴斯基伺服器將被選為本機*更新*工作設定中的第一個更新來源，因為應用程式可能無法存取卡巴斯基安全管理中心。

   d. 如果您選擇了 **卡巴斯基更新伺服器** 作為更新來源，請選擇 Kaspersky Embedded Systems Security 在選擇卡巴斯基更新伺服器時必須遵循的原則：

   - **自動偵測**應用程式使用最近的可用卡巴斯基更新伺服器。
   - **從清單中選取**應用程式使用清單中所選國家/地區的卡巴斯基更新伺服器。

   e. 在**"資料庫和應用程式模組更新"**塊中，點擊"確定"按鈕。

4. 配置應用程式資料庫更新：

   a. 選擇或清除**"下載應用程式資料庫更新"**核取方塊。

   b. 選擇或清除**"降低磁碟 I/O 上的負載"**核取方塊。此核取方塊可以啟用或停用透過將更新檔案儲存在記憶體中的虛擬磁碟機上實作磁碟子系統最佳化的功能。預設情況下，會取消勾選核取方塊。

   c. 如果您選擇了 **降低磁碟 I/O 上的負載** 核取方塊，請在 **用於最佳化的 RAM (MB)** 欄位中指定 RAM 數量（以兆位元組為單位）。作業系統臨時分配指定的記憶體容量，用於在執行工作時儲存更新檔案。預設記憶體大小為 640 MB。最小記憶體大小為 400 MB。

   在啟用磁碟子系統最佳化功能的情況下執行*更新*工作時，可能會出現下列情況之一：

   - 如果該值太小，則分配的 RAM 大小可能不足以完成資料庫更新工作（例如，在第一次更新過程中），這將導致工作完成並出現錯誤。

     在這種情況下，建議為磁碟子系統最佳化功能分配更多 RAM。

   - 如果該值太大，則在資料庫更新工作開始時，可能無法在 RAM 中建立選定大小的虛擬磁碟機。因此，磁碟子系統最佳化功能會自動停用，資料庫更新工作將在沒有最佳化功能的情況下執行。

     在這種情況下，建議為磁碟子系統最佳化功能分配更少 RAM。

5. 設定應用程式軟體模組更新：

   a. 選擇或清除**"下載應用程式模組更新"**核取方塊。

      如果選中此方塊，Kaspersky Embedded Systems Security 將會向使用者傳送關於可用應用程式模組更新的通知，並在執行*更新*工作時將應用程式模組更新包含到更新軟體套件中。將套用的應用程式模組更新的類型是單獨配置的。預設將會選定該核取方塊。

   b. 請選取您要套用的應用程式模組更新類型。

      - **安裝重大和指定的更新**如果選擇此選項，當有應用程式模組更新可用時，僅在這些更新透過應用程式介面或在卡巴斯基安全管理中心一側被本機批准後，Kaspersky Embedded Systems Security 才會自動安裝關鍵更新和所有其他應用程式模組更新。

      - **僅安裝指定的更新**如果選擇此選項，當有應用程式模組更新可用時，僅在這些更新透過應用程式介面或在卡巴斯基安全管理中心一側被本機批准後，Kaspersky Embedded Systems Security 才會安裝它們。預設選中該選項。

      如果應用程式模組更新需要檢視和接受最終使用者產品授權協議，應用程式將在最終使用者產品授權協議被接受後，安裝更新。

6. 配置將更新複製到本機儲存的資料夾：

   a. 選擇或清除**"將更新複製到資料夾用於本機儲存"**核取方塊。

   b. 選擇您希望應用程式複製到本機儲存資料夾的更新內容：

      - **複製資料庫更新**應用程式僅下載資料庫更新。

      - **複製關鍵應用程式模組更新**應用程式僅下載關鍵應用程式模組更新。

      - **複製資料庫更新和應用程式模組的關鍵更新**應用程式下載資料庫更新和關鍵應用程式模組更新。

   c. 指定 Kaspersky Embedded Systems Security 用來分發下載更新的本機或網路資料夾。

7. 儲存變更。

如何在應用程式主控台中設定「更新」工作

1. 在應用程式主控台樹狀目錄中，開啟**"更新 → 資料庫和應用程式模組更新"**節點。

2. 在結果窗格中點擊**"內容"**連結。

   內容: 資料庫和應用程式模組更新視窗將開啟。

3. 在連線到卡巴斯基安全管理中心管理伺服器的 Kaspersky Embedded Systems Security 的**本機模式更新設定**下面，設定更新來源：

   a. 單擊**"設定"**。

      開啟**"資料庫和應用程式模組更新"**視窗。

b. 選中要使用的更新來源旁邊的核取方塊：

- 卡巴斯基安全管理中心管理伺服器
- 卡巴斯基更新伺服器

如有必要，請點擊 **新增** 按鈕新增自訂更新來源。

c. 如果您選擇多個更新來源，請使用 **向上** 和 **向下** 按鈕依優先順序對更新來源進行排序。Kaspersky Embedded Systems Security 嚴格按照配置的順序存取更新來源，並使用第一個可用更新來源中的更新套件執行更新工作。

預設情況下，Kaspersky Embedded Systems Security 使用卡巴斯基安全管理中心伺服器作為第一個更新來源。這有助於在更新時節省流量。如果政策未被套用到電腦，卡巴斯基伺服器將被選為本機*更新*工作設定中的第一個更新來源，因為應用程式可能無法存取卡巴斯基安全管理中心。

d. 如果您選擇了 **卡巴斯基更新伺服器** 作為更新來源，請選擇 Kaspersky Embedded Systems Security 在選擇卡巴斯基更新伺服器時必須遵循的原則：

- **自動偵測**應用程式使用最近的可用卡巴斯基更新伺服器。
- **從清單中選取**應用程式使用清單中所選國家/地區的卡巴斯基更新伺服器。

e. 在"**資料庫和應用程式模組更新**"塊中，點擊"確定"按鈕。

4. 配置應用程式資料庫更新：

a. 選擇或清除"**下載應用程式資料庫更新**"核取方塊。

b. 選擇或清除"**降低磁碟 I/O 上的負載**"核取方塊。此核取方塊可以啟用或停用透過將更新檔案儲存在記憶體中的虛擬磁碟機上實作磁碟子系統最佳化的功能。預設情況下，會取消勾選核取方塊。

c. 如果您選擇了 **降低磁碟 I/O 上的負載** 核取方塊，請在 **用於最佳化的 RAM (MB)** 欄位中指定 RAM 數量（以兆位元組為單位）。作業系統臨時分配指定的記憶體容量，用於在執行工作時儲存更新檔案。預設記憶體大小為 640 MB。最小記憶體大小為 400 MB。

在啟用磁碟子系統最佳化功能的情況下執行*更新*工作時，可能會出現下列情況之一：

- 如果該值太小，則分配的 RAM 大小可能不足以完成資料庫更新工作（例如，在第一次更新過程中），這將導致工作完成並出現錯誤。

  在這種情況下，建議為磁碟子系統最佳化功能分配更多 RAM。

- 如果該值太大，則在資料庫更新工作開始時，可能無法在 RAM 中建立選定大小的虛擬磁碟機。因此，磁碟子系統最佳化功能會自動停用，資料庫更新工作將在沒有最佳化功能的情況下執行。

  在這種情況下，建議為磁碟子系統最佳化功能分配更少 RAM。

5. 設定應用程式軟體模組更新：

a. 選擇或清除"**下載應用程式模組更新**"核取方塊。

如果選中此方塊，Kaspersky Embedded Systems Security 將會向使用者傳送關於可用應用程式模組更新的通知，並在執行*更新*工作時將應用程式模組更新包含到更新軟體套件中。將套用的應用程式模組更新的類型是單獨配置的。預設將會選定該核取方塊。

b. 請選取您要套用的應用程式模組更新類型。

- **安裝重大和指定的更新**如果選擇此選項，當有應用程式模組更新可用時，僅在這些更新透過應用程式介面或在卡巴斯基安全管理中心一側被本機批准後，Kaspersky Embedded Systems Security 才會自動安裝關鍵更新和所有其他應用程式模組更新。
- **僅安裝指定的更新**如果選擇此選項，當有應用程式模組更新可用時，僅在這些更新透過應用程式介面或在卡巴斯基安全管理中心一側被本機批准後，Kaspersky Embedded Systems Security 才會安裝它們。預設選中該選項。

如果應用程式模組更新需要檢視和接受最終使用者產品授權協議，應用程式將在最終使用者產品授權協議被接受後，安裝更新。

6. 配置將更新複製到本機儲存的資料夾：

a. 選擇或清除"**將更新複製到資料夾用於本機儲存**"核取方塊。

b. 選擇您希望應用程式複製到本機儲存資料夾的更新內容：

- **複製資料庫更新**應用程式僅下載資料庫更新。
- **複製關鍵應用程式模組更新**應用程式僅下載關鍵應用程式模組更新。
- **複製資料庫更新和應用程式模組的關鍵更新**應用程式下載資料庫更新和關鍵應用程式模組更新。

c. 指定 Kaspersky Embedded Systems Security 用來分發下載更新的本機或網路資料夾。

7. 儲存變更。

如何在卡巴斯基安全管理中心網頁主控台中設定「更新」工作

1. 在網頁主控台中，轉至您要設定的本機或群組*更新*工作。
2. 開啟 **設定** 部分。
3. 選取**本機模式**索引標籤來設定連線到卡巴斯基安全管理中心管理伺服器的 Kaspersky Embedded Systems Security 的*更新*工作。
4. 配置更新來源：

a. 在**更新來源**下面，選取您要使用的更新來源旁的核取方塊：

- **卡巴斯基安全管理中心管理伺服器**
- **卡巴斯基更新伺服器**

如有必要，請點擊 **新增** 按鈕新增自訂更新來源。

b. 如果您選擇多個更新來源，請使用 **向上** 和 **向下** 按鈕依優先順序對更新來源進行排序。Kaspersky Embedded Systems Security 嚴格按照配置的順序存取更新來源，並使用第一個可用更新來源中的更新套件執行更新工作。

預設情況下，Kaspersky Embedded Systems Security 使用卡巴斯基安全管理中心伺服器作為第一個更新來源。這有助於在更新時節省流量。如果政策未被套用到電腦，卡巴斯基伺服器將被選為本機*更新*工作設定中的第一個更新來源，因為應用程式可能無法存取卡巴斯基安全管理中心。

5. 配置應用程式資料庫更新：

a. 選擇或清除**"下載應用程式資料庫更新"**核取方塊。

b. 選擇或清除**"降低磁碟 I/O 上的負載"**核取方塊。此核取方塊可以啟用或停用透過將更新檔案儲存在記憶體中的虛擬磁碟機上實作磁碟子系統最佳化的功能。預設情況下，會取消勾選核取方塊。

c. 如果您選擇了 **降低磁碟 I/O 上的負載** 核取方塊，請在 **用於最佳化的 RAM (MB)** 欄位中指定 RAM 數量（以兆位元組為單位）。作業系統臨時分配指定的記憶體容量，用於在執行工作時儲存更新檔案。預設記憶體大小為 640 MB。最小記憶體大小為 400 MB。

在啟用磁碟子系統最佳化功能的情況下執行*更新*工作時，可能會出現下列情況之一：

- 如果該值太小，則分配的 RAM 大小可能不足以完成工作（例如，在第一次更新過程中），這將導致工作完成並出現錯誤。

  在這種情況下，建議為磁碟子系統最佳化功能分配更多 RAM。

- 如果該值太大，則在工作開始時，可能無法在 RAM 中建立選定大小的虛擬磁碟機。因此，磁碟子系統最佳化功能會自動停用，資料庫更新工作將在沒有最佳化功能的情況下執行。

  在這種情況下，建議為磁碟子系統最佳化功能分配更少 RAM。

6. 設定應用程式軟體模組更新：

a. 選擇或清除**"下載應用程式模組更新"**核取方塊。

如果選中此方塊，Kaspersky Embedded Systems Security 將會向使用者傳送關於可用應用程式模組更新的通知，並在執行*更新*工作時將應用程式模組更新包含到更新軟體套件中。將套用的應用程式模組更新的類型是單獨配置的。預設將會選定該核取方塊。

b. 請選取您要套用的應用程式模組更新類型。

- **安裝重大和指定的更新**如果選擇此選項，當有應用程式模組更新可用時，僅在這些更新透過應用程式介面或在卡巴斯基安全管理中心一側被本機批准後，Kaspersky Embedded Systems Security 才會自動安裝關鍵更新和所有其他應用程式模組更新。

- **僅安裝指定的更新**如果選擇此選項，當有應用程式模組更新可用時，僅在這些更新透過應用程式介面或在卡巴斯基安全管理中心一側被本機批准後，Kaspersky Embedded Systems Security 才會安裝它們。預設選中該選項。

如果應用程式模組更新需要檢視和接受最終使用者產品授權協議，應用程式將在最終使用者產品授權協議被接受後，安裝更新。

7. 配置將更新複製到本機儲存的資料夾：

a. 選擇或清除“**將更新複製到資料夾**”核取方塊。

b. 選擇您希望應用程式複製到本機儲存資料夾的更新內容：

- **複製資料庫更新**應用程式僅下載資料庫更新。
- **複製關鍵應用程式模組更新**應用程式僅下載關鍵應用程式模組更新。
- **複製資料庫更新和應用程式模組的關鍵更新**應用程式下載資料庫更新和關鍵應用程式模組更新。

c. 指定 Kaspersky Embedded Systems Security 用來分發下載更新的本機或網路資料夾。

8. 儲存變更。

應用程式的 SMU 更新

若要使用卡巴斯基更新服務更新應用程式 (Seamless Update; SMU），您不需要執行安裝程式，這與 其他更新方法相反。Kaspersky Embedded Systems Security 獲得新版本應用程式的來源與病毒資料庫一樣。

SMU 更新可讓將組織中所有電腦上的應用程式更新至最新版本。在套用 SMU 更新之前，我們建議先在幾台電腦上測試新版本的應用程式。為此，您必須手動更新這些電腦上的應用程式（例如，在本機上使用 設定精靈）。執行 SMU 更新時無法選擇單獨的電腦。

應用程式的更新時間表由卡巴斯基工作人員確定。為了確保新版本的應用程式順利執行，卡巴斯基逐步提供更新。這意味著您可能會在新版本發布後兩個月後獲得 SMU 更新。

您可以使用 *更新* 工作管理應用程式的 SMU 更新。要將應用程式的新版本包含在與病毒資料庫相同的套件中，您必須允許 在 更新 工作設定中更新 *應用程式模組*。

應用程式 SMU 更新的步驟

1. **應用程式的新版本發布或者模組更新後，卡巴斯基會分發更新。**
2. **使用者批准應用程式的更新。**

   如果電腦已連線至卡巴斯基安全管理中心，則更新可以在卡巴斯基安全管理中心的**卡巴斯基資料庫和軟體模組更新**部分中找到。有關批准更新的詳細資訊，請參閱卡巴斯基安全管理中心說明。

   如果電腦未連線到卡巴斯基安全管理中心，則可以在應用程式主控台中取得更新。若要批准更新，請轉至 **更新 → 應用程式更新** 部分，選擇應用程式版本並在必要時接受協議的條款和條件。
3. **Kaspersky Embedded Systems Security 依照排程執行 更新 工作。**

結果，Kaspersky Embedded Systems Security 會以“靜默”模式更新應用程式。

安全複製應用程式資料庫

該工作只能在應用程式主控台中配置。此工作無法在卡巴斯基安全管理中心管理主控台或卡巴斯基安全管理中心網頁主控台中設定。

若要設定並啟動應用程式資料庫的安全複製工作：

1. 在應用程式主控台樹狀目錄中，在**更新**節點的內容功能表中，選擇**開始安全複製資料庫**。

   安全應用程式資料庫複製精靈的歡迎視窗將開啟。

2. 單擊"**下一步(N) >**"。

3. 在**更新來源**下面，選擇更新來源：

   - **卡巴斯基安全管理中心管理伺服器**

     只有網路中的 Kaspersky 應用程式使用卡巴斯基安全管理中心遠端存取系統進行管理，並且受防護裝置上安裝有網路代理（在受防護裝置與管理伺服器之間提供連線的卡巴斯基安全管理中心元件），才能選取該選項。

     預設選中該選項。

   - **卡巴斯基更新伺服器**

     Kaspersky 應用程式用來下載資料庫及應用程式模組更新的 Kaspersky HTTP 和 HTTPS 伺服器。

   - **自訂 HTTP 或 FTP 伺服器，或網路資料夾**

4. 如果您在上一步驟中選取了 **卡巴斯基安全管理中心管理伺服器**，請設定 **如果指定的伺服器不可用則使用卡巴斯基更新伺服器** 功能。如果啟用此選項，當 Kaspersky Security Center 管理伺服器無法使用時，Kaspersky Embedded Systems Security 將使用 Kaspersky 更新伺服器作為更新來源。

5. 在 **更新來源連線設定** 下方，設定使用 代理伺服器連線至更新來源。

6. 單擊"**下一步(N) >**"。

7. 從下拉式清單中，選擇要用來儲存應用程式病毒資料庫的已連線安全 Rutoken 卸除式磁碟機。

   只有透過 裝置控制 元件規則特別授權的 Rutoken 卸除式磁碟機才能用作安全卸除式磁碟機。

8. 在 **安全設定** 下方的 **輸入目前的管理員 PIN 代碼** 欄位中，輸入在 Rutoken 卸除式磁碟機上設定的管理員 PIN 碼，以防止潛在入侵者讀取、複製或寫入其內容。

9. 若要變更目前的管理員 PIN 碼：

   a. 選擇"**變更目前管理員 PIN 代碼（僅允許數字和拉丁符號）**"核取方塊。

   b. 輸入新的 PIN 碼。

   c. 確認新的 PIN 碼。

10. 設定使用者 PIN 碼。使用 *應用程式資料庫安全更新* 工作和所選 Rutoken 卸除式磁碟機更新應用程式資料庫的員工需要此 PIN 碼：

    a. 輸入使用者 PIN 碼。

    b. 確認使用者 PIN 碼。

11. 單擊“**下一步(N) >**”。

將應用程式資料庫安全複製到 Rutoken 卸除式磁碟機開始。工作執行時會儲存並套用設定。

安全更新應用程式資料庫

在封閉的公司網路中以及無法存取應用程式資料庫的裝置上，必須執行 *應用程式資料庫安全更新* 工作，使用可防止潛在入侵者讀取、複製及寫入的安全卸除式磁碟機更新應用程式資料庫。

此工作只能透過安裝在與 Kaspersky Embedded Systems Security 相同裝置上的應用程式主控台啟動。無法在管理主控台或網頁主控台中設定此工作。

要執行“應用程式資料庫安全更新”工作：

1. 在應用程式主控台樹狀目錄中，在**更新**節點的內容功能表中，選擇**開始安全更新資料庫**。

   安全應用程式資料庫更新精靈的歡迎視窗將開啟。點擊“**下一步(N) >**“按鈕。

2. 從下拉式清單中，選擇包含應用程式病毒資料庫的已連線安全卸除式磁碟機。

   只有透過 裝置控制 元件規則特別授權的 Rutoken 卸除式磁碟機才能用作安全卸除式磁碟機。

3. 輸入在 應用程式資料庫複製步驟中指定的 Rutoken 卸除式磁碟機 PIN 碼。

4. 單擊“**完成**”。

應用程式資料庫安全更新工作啟動。應用程式資料庫將從 Rutoken 卸除式磁碟機複製。

回溯 Kaspersky Embedded Systems Security 資料庫更新

在執行資料庫更新之前，Kaspersky Embedded Systems Security 會建立先前使用資料庫的備份副本。如果更新中斷或發生錯誤，Kaspersky Embedded Systems Security 將自動還原為使用之前安裝的資料庫。

如果在您已更新資料庫後出現任何問題，則可透過「*上次更新回溯*」工作回溯到之前安裝的更新。

要執行“上次更新回溯”工作：

1. 在應用程式主控台樹狀目錄中，開啟“**更新 → 上次更新回溯**”部分。

2. 在結果窗格中，點擊“**啟動**”連結。

更新工作統計

「更新」工作執行時，會顯示自工作啟動以來下載的資料量的即時資訊，以及其他工作執行統計資料。

工作完成或停止後，可以在工作記錄中檢視此資訊。

要檢視「更新」工作統計資料：

在應用程式主控台樹狀目錄中，開啟“**更新 → 資料庫和應用程式模組更新**”部分。

結果面板， 在**統計資料**下面，您可以查找到所獲取資料總量的資訊。

製作物件的備份副本

本節提供有關在清除或刪除之前備份偵測到的惡意物件的資訊。

製作物件的備份副本。備份

Kaspersky Embedded Systems Security 將已消毒或刪除的物件的加密副本保存在 備份 資料夾中。

如果該物件是複合檔案的一部分（例如壓縮檔案的一部分），Kaspersky Embedded Systems Security 會將此複合檔案整體儲存在備份中。例如，如果 Kaspersky Embedded Systems Security 偵測到郵件資料庫其中一個物件感染病毒，則會備份整個郵件資料庫。

Kaspersky Embedded Systems Security 放入備份中的大型檔案可能會降低系統速度，並減少硬碟上的可用磁碟空間。

您可以將檔案從備份還原到其原始資料夾或還原到受防護裝置上的其他資料夾。檔案可以從備份區還原，例如，如果某個已感染檔案包含重要資訊，但 Kaspersky Embedded Systems Security 無法在不破壞其完整性和遺失資訊的前提下解毒病毒。

從備份區還原檔案可能會導致受防護裝置受到感染。

檢視備份中的物件

本節提供有關如何檢視備份中的檔案清單的資訊。

如何在卡巴斯基安全管理中心管理主控台中檢視備份物件

1. 開啟卡巴斯基安全管理中心管理主控台。
2. 在主控台樹狀目錄中，選擇“**附加 → 儲存**”。
3. 前往 **備份** 資料夾。
4. 有關置於備份中的物件的資訊顯示在主控台的右側窗格中。

如何在卡巴斯基安全管理中心網頁主控台中檢視備份物件

1. 開啟網頁主控台。
2. 在主控台樹狀目錄中，選擇“**動作 → 儲存**”。
3. 前往 **備份** 資料夾。
4. 有關置於備份中的物件的資訊顯示在主控台的右側窗格中。

如何在應用程式主控台中檢視備份物件

1. 在 Kaspersky Embedded Systems Security 主控台樹狀目錄中，選擇**"儲存 → 備份"**。
2. 有關置於備份中的物件的資訊顯示在主控台的右側窗格中。

若要在備份中的物件清單中尋找所需物件，

排序物件或篩選物件。

從備份還原檔案

Kaspersky Embedded Systems Security 以加密形式將檔案儲存在備份資料夾中，以防護受防護裝置免受可能的有害影響。

所有檔案都可以從備份還原。

在下列情況下可能需要還原物件：

- 原始受感染檔案包含了重要資訊， Kaspersky Embedded Systems Security 將無法保證其完整性，檔案中的資訊可能會變得無法使用。
- 您認為檔案對受防護裝置無害並且要使用它。如果您不希望 Kaspersky Embedded Systems Security 將該檔案視為已感染，則在後續掃描期間，可以將其從即時檔案防護工作和"自訂掃描"工作的處理中排除。

從備份區還原檔案可能會導致受防護裝置受到感染。

還原檔案時，您可以選擇用於儲存檔案的位置：原始位置（預設）、受防護裝置上用於儲存還原物件的特殊資料夾、或者安裝應用程式主控台的受儲存裝置上的自訂資料夾。

預設情況下，Kaspersky Embedded Systems Security 還原檔案時，會在備份區中產生檔案的副本。還原之後，您可以從備份刪除檔案副本。

在卡巴斯基安全管理中心管理主控台中從備份還原檔案

1. 在卡巴斯基安全管理中心管理主控台樹狀目錄中，選取「**附加**」→「**儲存**」資料夾。
2. 前往 **備份** 資料夾。
3. 執行以下操作之一：
   - 要刪除一個物件，請從物件名稱的內容功能表中選擇**"還原"**。
   - 要還原多個物件，請使用 **CTRL** 或 **SHIFT** 鍵選取想要還原的物件，右鍵點擊其中一個選定的物件，然後在內容功能表中選取**"還原"**。
4. 該物件將被還原到原始資料夾。

在卡巴斯基安全管理中心網頁主控台中從備份還原檔案

1. 開啟網頁主控台。
2. 在主控台樹狀目錄中，選擇**"動作 → 儲存"**。
3. 前往 **備份** 資料夾。
4. 在清單中選擇物件，然後按一下**還原**按鈕。
5. 該物件將被還原到原始資料夾。

在應用程式主控台中從備份還原檔案

1. 在 Kaspersky Embedded Systems Security 主控台樹狀目錄中，選擇**"儲存 → 備份"**。
2. 在**"備份"**節點的結果窗格中執行以下操作之一：
   - 要還原一個物件，請從要還原的物件的內容功能表中選擇**"還原"**。
   - 要還原多個物件，請使用 **CTRL** 或 **SHIFT** 鍵選取想要還原的物件，右鍵點擊其中一個選定的物件，並在內容功能表中選取**"還原"**。
3. 在**"還原物件"**視窗中，為每個選定物件指定將儲存還原物件的資料夾。

   物件的名稱顯示在視窗上部的**"物件"**欄位中。如果選定多個物件，系統將顯示選定物件清單中第一個物件的名稱。

4. 執行以下操作之一：
   - 若要將物件還原到原始位置，請選擇 **還原到來源資料夾**。
   - 要在應用程式安裝期間將物件還原到設定中的適用於還原物件位置所指定的資料夾，請選擇**"還原到預設還原資料夾"**。
   - 要將物件儲存在安裝應用程式主控台的受防護裝置上的其他資料夾，請選擇**還原至本機電腦上的資料夾**，然後選擇所需資料夾或指定資料夾路徑。
5. 如果您不希望於還原之後在備份資料夾中儲存物件的副本，請取消選定**"還原物件後從儲存區中刪除物件"**核取方塊（預設情況下，清除此核取方塊）。
6. 要為其餘選定物件套用指定的還原條件，請選定**"套用至所有選擇的物件"**核取方塊。
7. 單擊**"確定"**。
8. Kaspersky Embedded Systems Security 將開始還原選定物件的第一個物件。

9. 如果指定位置已存在擁有該名稱的物件，則系統將開啟**"已存在具有此名稱的物件"**視窗。

   a. 選擇以下 Kaspersky Embedded Systems Security 操作之一：

   - **取代**，將現有物件取代為還原物件。
   - **重新命名**，使用其他名稱儲存還原的物件。在輸入欄位中輸入新還原物件的檔案名稱和完整路徑。
   - **"透過新增後置詞重命名"**，透過為物件檔案名稱新增後置詞重新命名還原物件。在輸入欄位中輸入後置詞。

   b. 如果選擇了多個物件進行還原，則選中**"套用至所有選擇的物件"**核取方塊以將選定操作（**取代** 或者 **重新命名**）套用於其餘選定物件。如果您選擇了 **重新命名**，**套用至所有選擇的物件** 核取方塊將不可用。

   c. 單擊**"確定"**。

   物件將被還原。有關還原操作的資訊將記錄到系統稽核記錄中。

如果您沒有在**還原物件**視窗中選擇**套用至所有選擇的物件**，**還原物件** 視窗可能會再次開啟。使用該視窗可指定儲存下個選定物件的位置。

從備份刪除檔案

在卡巴斯基安全管理中心管理主控台中刪除備份中的檔案

1. 開啟卡巴斯基安全管理中心管理主控台。
2. 在主控台樹狀目錄中，選擇**"附加 → 儲存"**。
3. 前往 **備份** 資料夾。右側面板將顯示備份中的物件清單。
4. 執行以下操作之一：
   - 要刪除一個物件，請從物件的內容功能表中選擇**"刪除"**。
   - 若要刪除多個物件，請使用 **CTRL** 或 **SHIFT** 鍵選取要刪除的物件，以滑鼠右鍵按一下其中一個選取的物件，然後從內容功能表中選取「**刪除**」。
5. 所選物件將從被備份中刪除。

在卡巴斯基安全管理中心網頁主控台中從備份中刪除檔案

1. 開啟網頁主控台。
2. 在主控台樹狀目錄中，選擇**"動作 → 儲存"**。
3. 前往 **備份** 資料夾。
4. 在清單中選擇物件，然後按一下**刪除**按鈕。
5. 所選物件將從被備份中刪除。

在應用程式主控台中從備份中刪除檔案

1. 在 Kaspersky Embedded Systems Security 主控台樹狀目錄中，選擇“**儲存 → 備份**”。
2. 右側面板將顯示備份中的物件清單。
3. 執行以下操作之一：
   - 要刪除一個物件，請從物件的內容功能表中選擇“**刪除**”。
   - 若要刪除多個物件，請使用 **CTRL** 或 **SHIFT** 鍵選取要刪除的物件，以滑鼠右鍵按一下其中一個選取的物件，然後從內容功能表中選取「**刪除**」。
4. 所選物件將從被備份中刪除。

傳送可疑感染物件到 Kaspersky 以供分析

如果某個物件的行為使您懷疑該檔案可能包含威脅，並且 Kaspersky Embedded Systems Security 認定該物件需要解毒，則您可能遇到未知威脅，而該威脅的特徵碼尚未新增到資料庫。您可以將此物件傳送到 Kaspersky 以供分析。Kaspersky 的病毒分析人員將對檔案進行分析，如果偵測到檔案中包含新威脅，則將在資料庫中新增記錄標識該威脅。當您在資料庫更新之後重新掃描物件時，有可能Kaspersky Embedded Systems Security 將此物件標識為已感染，並能夠將其解毒。您不僅能夠保留物件，而且能夠封鎖病毒爆發。

在卡巴斯基安全管理中心管理主控台中將物件傳送給 Kaspersky 專家進行分析

1. 開啟卡巴斯基安全管理中心管理主控台。
2. 在主控台樹狀目錄中，選擇“**附加 → 儲存**”。
3. 前往 **備份** 資料夾。
4. 執行以下操作之一：
   - 要刪除一個物件，請在物件名稱的內容功能表中選擇“**傳送到 Kaspersky**”。
   - 要傳送多個物件，請使用 CTRL 或 SHIFT 鍵選取想要傳送的物件，右鍵點擊其中一個選定的物件，然後在內容功能表中選取“**傳送到 Kaspersky**”。
5. 選擇電腦上用於儲存物件的資料夾。
6. 此後，您會被提示前往 Kaspersky Threat Intelligence Portal 並上傳已儲存的物件以獲取有關它的完整資訊。

在卡巴斯基安全管理中心網頁主控台中將物件傳送給 Kaspersky 專家進行分析

1. 開啟網頁主控台。
2. 在主控台樹狀目錄中，選擇“**動作 → 儲存**”。
3. 前往 **檔案備份** 資料夾。
4. 在清單中選擇物件，然後按一下**傳送到 Kaspersky**按鈕。

5. 選擇電腦上用於儲存物件的資料夾。

6. 此後，您會被提示前往 Kaspersky Threat Intelligence Portal 並上傳已儲存的物件以獲取有關它的完整資訊。

如果在將應用程式版本從 3.4 或更早版本升級到 4.0 或更高版本後遷移了備份物件，則卡巴斯基安全管理中心網頁主控台或管理主控台無法被用來將備份物件傳送給卡巴斯基進行分析。

配置備份設定

如何在卡巴斯基安全管理中心管理主控台中配置備份設定

1. 在卡巴斯基安全管理中心管理主控台樹狀目錄中，選取**政策**。

2. 選擇必要的政策並點擊以開啟政策內容。

3. 在政策視窗中，選擇 **補充** → **儲存** 然後點擊 **設定**。

4. 轉至**備份**頁簽。

5. 指定備份設定（參見下表）。

6. 儲存變更。

如何在卡巴斯基安全管理中心網頁主控台中配置備份設定

1. 在網頁主控台的主視窗中，選擇**資產管理** → **政策**。

2. 點擊 Kaspersky Embedded Systems Security 政策的名稱。
   政策內容視窗將開啟。

3. 選擇"**應用程式設定**"標籤。

4. 選擇 **補充** → **儲存** 並點擊 **配置** 按鈕。

5. 轉至**備份**頁簽。

6. 指定備份設定（參見下表）。

7. 儲存變更。

如何在應用程式主控台中配置備份設定

1. 在 Kaspersky Embedded Systems Security 主控台樹狀目錄中，選擇"**儲存** → **備份**"。

2. 在 **備份** 節點的結果窗格中，點擊 **內容**。

3. 在 **屬性：備份** 視窗中，指定備份設定（見下表）。

4. 儲存變更。

備份設定

參數	描述
儲存物件的時間不超過	如果啟用此功能，則最大檔案儲存期限制為定義的時間間隔。預設的檔案最長儲存期限是 30 天。最長儲存期限超出後，Kaspersky Embedded Systems Security 將刪除備份區中最舊的檔案。
備份大小限制為	如果啟用此功能，Kaspersky Embedded Systems Security 會監控置於備份中的物件的總大小。如果超過指定的值（預設值為 400 MB），Kaspersky Embedded Systems Security 會記錄"*已超過最大備份容量*"事件，並根據此事件類型的通知設定發佈通知。 如果啟用此功能，Kaspersky Embedded Systems Security 不會監控置於備份中的物件的總大小。 預設情況下，該功能處於停用狀態。
將可用空間的閾值限制為	如果啟用此功能，Kaspersky Embedded Systems Security 將監控備份中的最小可用空間（預設值為 100 MB）。如果可用空間大小下降到低於指定上限值，Kaspersky Embedded Systems Security 會記錄"*已超過備份區可用空間上限值*"事件，並根據此事件類型的通知設定發佈通知。 如果選擇了**備份大小限制為**核取方塊，則 **將可用空間的閾值限制為** 核取方塊處於活動狀態。 預設啟用該選項。

如果備份中的物件大小超過最大備份容量或超過可用空間上限值，在您繼續將物件放入備份時，Kaspersky Embedded Systems Security 將通知您此情況。

備份統計

您可以檢視有關目前備份狀態的資訊,即備份統計。

要檢視備份統計資料：

1. 在 Kaspersky Embedded Systems Security 主控台樹狀目錄中，選擇"**儲存 → 備份**"。
2. 在 **備份** 節點的結果窗格中，點擊 **統計資料**。

這將開啟**備份。「統計資料」**視窗。**備份：統計**視窗將顯示有關目前備份狀態的資訊（請參閱下表）。

有關目前備份狀態的資訊

欄位	描述
目前備份區大小	備份資料夾中的資料大小總計；應用程式會以加密形式計算檔案大小。
物件總數	備份中目前的物件總數。

封鎖存取網路資源。已封鎖的網路工作階段

本節介紹如何封鎖遠端裝置和進行已封鎖網路工作階段清單的設定。

已封鎖的網路工作階段清單

預設情況下，如果安裝了以下任何元件，則可以使用封鎖的網路工作階段清單：網路威脅防護或者行為偵測。這些元件根據封鎖的網路工作階段清單，發現遠端對受防護裝置或網路附加儲存共用資料夾中的物件進行加密、開啟或執行的嘗試。有關所有受防護裝置封鎖的網路工作階段的資訊將傳送到卡巴斯基安全管理中心。Kaspersky Embedded Systems Security 封鎖目前的工作階段，並且就目前的工作階段而言，讓共用資料夾或網路附加儲存資料夾無法使用。

在啟動模式下啟動以下至少一個工作（在指定條件下）時，將填充封鎖的網路工作階段清單：

- 「*網路威脅防護*」工作：偵測典型的網路攻擊活動。

  重新啟動應用程式以及變更網路威脅防護設定時，Kaspersky Embedded Systems Security 會清除封鎖清單。

- 「*行為偵測*」工作：偵測正在存取網路檔案資源的裝置的惡意加密。

在偵測到惡意活動或加密嘗試後，該工作會將有關攻擊網路工作階段的資訊傳送到封鎖的網路工作階段清單，而且應用程式會為攻擊主機的目前工作階段建立一個*警告*事件。該工作階段存取受防護共用網路資料夾的嘗試都將被封鎖。

如果發起網路工作階段攻擊的主機的本機唯一識別碼 (LUID) 已新增到封鎖的網路工作階段清單中，Kaspersky Embedded Systems Security 會確定該主機的 IP 位址，並將其新增到封鎖的網路工作階段清單中來替換攻擊主機的 LUID。

預設情況下，當封鎖的網路工作階段被新增到清單 30 分鐘後，Kaspersky Embedded Systems Security 將從清單中移除這些網路工作階段。從封鎖的網路工作階段清單中刪除網路工作階段後，會自動還原對網路檔案資源的存取。您可以指定之後自動解除封鎖受封鎖網路工作階段的時段。

請注意，當限制任何使用者帳戶管理儲存的存取權限時，封鎖的網路工作階段清單仍將可用。封鎖的網路工作階段設定無法變更，除非所選使用者帳戶具有可管理 Kaspersky Embedded Systems Security 的**編輯權限**。

管理已封鎖的網路工作階段清單

若要將出現任何惡意或加密活動的網路工作階段新增到封鎖的網路工作階段清單並針對這些工作階段封鎖對網路檔案資源的存取權限，以下至少一個元件應該已啟用：

- 網路威脅防護
- 行為偵測。

在卡巴斯基安全管理中心管理主控台中啟用對不受信任主機的封鎖

1. 在卡巴斯基安全管理中心管理主控台樹狀目錄中，選取**政策**。
2. 選擇必要的政策並點擊以開啟政策內容。

3. 在政策視窗中，選擇 **網路活動控制 → 網路威脅防護設定** 然後點擊 **設定**。

4. 在開啟的視窗中，選中**"網路威脅防護"**核取方塊。

5. 在**一般**頁簽上，啟用 **封鎖**模式。

6. 選擇 **封鎖攻擊裝置** 核取方塊並指定封鎖時長。

7. 儲存變更。

若要在政策屬性中為行為偵測元件配置封鎖不受信任的網路工作階段：

1. 在卡巴斯基安全管理中心管理主控台樹狀目錄中，選取**政策**。

2. 選擇必要的政策並點擊以開啟政策內容。

3. 在政策視窗中，選擇**即時電腦防護 → 行為偵測**然後點擊**設定**。

4. 在開啟的視窗中，選中**"行為偵測"**核取方塊。

5. 轉到**防護共用資料夾**頁簽並選擇 **防護共用資料夾** 核取方塊。

6. 選擇 **封鎖連線時間** 並指定封鎖時長。

7. 如有必要，按照 IP 位址和遮罩指定防護範圍和排除項目。

8. 儲存變更。

在卡巴斯基安全管理中心網頁主控台中啟用對不受信任主機的封鎖

1. 在網頁主控台的主視窗中，選擇**資產管理 → 政策**。

2. 點擊 Kaspersky Embedded Systems Security 政策的名稱。
   政策內容視窗將開啟。

3. 選擇**"應用程式設定"**標籤。

4. 轉到**網路活動控制 → 網路威脅防護** 並點擊 **配置** 按鈕。

5. 在開啟的視窗中，選中**"啟用網路威脅防護"**核取方塊。

6. 啟用 **封鎖** 模式。

7. 選擇 **封鎖攻擊裝置** 核取方塊並指定封鎖時長。

8. 如有必要，請按照 IP 位址指定排除項目。

9. 儲存變更。

若要為行為偵測元件配置封鎖不受信任的網路工作階段：

1. 在網頁主控台的主視窗中，選擇**資產管理 → 政策**。

2. 點擊 Kaspersky Embedded Systems Security 政策的名稱。
   政策內容視窗將開啟。

3. 選擇“**應用程式設定**”標籤。

4. 轉到**即時電腦防護 → 行為偵測** 並點擊 **配置** 按鈕。

5. 在開啟的視窗中，選中“**啟用行為偵測**”核取方塊。

6. 轉到**防護共用資料夾**頁簽並選擇 **啟用共用資料夾對外部加密的防護** 核取方塊。

7. 選擇 **封鎖連線** 並在 **偵測到共用資料夾的外部加密時。** 部分中指定封鎖時長。

8. 如有必要，按照 IP 位址和遮罩指定防護範圍和排除項目。

9. 儲存變更。

在應用程式主控台中啟用對不受信任主機的封鎖

1. 在 Kaspersky Embedded Systems Security 主控台樹狀目錄中，選擇“**即時電腦防護 → 網路威脅防護**”。

2. 在 **網路威脅防護** 節點的結果窗格中，點擊 **內容**。
   內容: 網路威脅防護視窗將開啟。

3. 在開啟的視窗中，選中“**網路威脅防護**”核取方塊。

4. 在**一般**頁簽上，啟用 **封鎖**模式。

5. 選擇 **封鎖攻擊裝置** 核取方塊並指定封鎖時長。

6. 儲存變更。

若要為行為偵測元件配置封鎖不受信任的網路工作階段：

1. 在 Kaspersky Embedded Systems Security 主控台樹狀目錄中，選擇“**即時電腦防護 → 加密軟體防護**”。

2. 在**行為偵測**節點的結果窗格中，點擊 **內容**。

3. 在開啟的視窗中，選中“**行為偵測**”核取方塊。

4. 轉到**防護共用資料夾**頁簽並選擇 **防護共用資料夾** 核取方塊。

5. 選擇 **封鎖連線時間** 並指定封鎖時長。

6. 如有必要，按照 IP 位址和遮罩指定防護範圍和排除項目。

7. 儲存變更。

在應用程式主控台中設定已封鎖的工作階段清單

1. 在應用程式主控台樹狀目錄中，展開“**儲存**”節點。

2. 選擇“**被封鎖的網路工作階段**”子節點。

3. 在結果窗格中，點擊**內容** 按鈕。

4. 在開啟的視窗中，選擇 **封鎖攻擊裝置** 核取方塊並指定封鎖持續時間。

5. 若要還原對所有已封鎖的網路工作階段的存取，請在視窗的上部點擊**全部解除封鎖**。

   所有網路工作階段都將從清單移除並解除封鎖。

6. 若要從封鎖的網路工作階段清單中刪除網路工作階段，請在結果窗格的清單中選擇一個或多個工作階段，然後在視窗的上部點擊**解除封鎖選定項目**。

   就會解除封鎖所選的網路工作階段。

事件註冊。Kaspersky Embedded Systems Security 記錄

本節提供有關使用 Kaspersky Embedded Systems Security 記錄的資訊。

註冊 Kaspersky Embedded Systems Security 事件的方式

Kaspersky Embedded Systems Security 的事件分為兩組：

- 與應用程式元件運作、Kaspersky Embedded Systems Security 工作中物件處理相關的事件。
- 與管理 Kaspersky Embedded Systems Security（例如啟動應用程式、建立或刪除工作，或者編輯工作設定）有關的事件。

Kaspersky Embedded Systems Security 使用以下方式來記錄事件：

- **應用元件運行日誌**。日誌包含有關應用程式元件運行期間發生的事件的資訊。
- **系統稽核記錄**。系統稽核記錄包含有關與管理 Kaspersky Embedded Systems Security 相關的事件的資訊。還包含有關與受防護裝置上的安全入侵或安全入侵嘗試相關的事件的資訊。
- **事件記錄**。事件記錄包含有關診斷 Kaspersky Embedded Systems Security 執行故障所需的事件資訊。可在 Microsoft Windows 事件檢視器中檢視事件記錄。

您可以透過以下連結下載的檔案，包含有 Kaspersky Embedded Systems Security 事件以下類別的完整清單表格：

- Kaspersky Embedded Systems Security 寫入事件記錄的事件 Event Log.

  下載 WEL-EVENTS.ZIP
- Kaspersky Embedded Systems Security 傳送到管理伺服器的事件。

  下載 KSC-EVENTS.ZIP

設定記錄設定

您可以編輯 Kaspersky Embedded Systems Security 記錄的以下設定：

- 事件在工作記錄和系統稽核記錄中儲存的時間長度。
- Kaspersky Embedded Systems Security 在其中儲存工作記錄檔案和系統稽核記錄檔案的資料夾的位置。
- *資料庫已過期*、*資料庫嚴重過期* 和 *長時間未執行關鍵區域掃描*的事件產生閾值。

- Kaspersky Embedded Systems Security 在事件檢視器中將儲存到工作記錄、系統稽核記錄和 Kaspersky Embedded Systems Security 事件記錄中的事件。
- Kaspersky Embedded Systems Security 傳送到 SIEM 伺服器的事件。

如何在卡巴斯基安全管理中心管理主控台中配置記錄設定

1. 在卡巴斯基安全管理中心管理主控台樹狀目錄中，選取**政策**。
2. 選擇必要的政策並點擊以開啟政策內容。
3. 在政策屬性視窗中，選取**"記錄和通知"**。
4. 在**"工作記錄"**區域中點擊**"設定"**。
   開啟**"通知"**視窗。
5. 在此視窗中，選擇要設定的記錄並指定單個事件的設定：
   - 事件保存的位置：本機報告或 Windows 事件記錄。
   - 事件通知：透過電子郵件通知、透過使用終端服務通知和/或透過執行可執行檔案通知。
   - 您是否要將事件傳送到 SIEM 伺服器和/或卡巴斯基安全中心。
6. 點選 **事件產生上限值設定**配置事件產生閾值。
7. 這將開啟一個視窗；在該視窗中，指定多少天後必須註冊下列事件：*資料庫已過期*、*資料庫嚴重過期*和*長時間未執行關鍵區域掃描*。
8. 按一下**電子郵件通知設定**設定電子郵件通知。
9. 儲存變更。

如何在卡巴斯基安全管理中心網頁主控台中配置記錄設定

1. 在網頁主控台的主視窗中，選擇**資產管理 → 政策**。
2. 點擊 Kaspersky Embedded Systems Security 政策的名稱。
   政策內容視窗將開啟。
3. 選擇**"應用程式設定"**標籤。
4. 轉到**記錄和通知 → 工作記錄** 並點擊 **配置** 按鈕。
5. 這將開啟一個視窗；在此視窗中的**通知**頁簽上，選擇要設定的記錄並指定單個事件的設定：
   - 事件保存的位置：本機報告或 Windows 事件記錄。
   - 事件通知：透過電子郵件通知、透過使用終端服務通知和/或透過執行可執行檔案通知。
   - 您是否要將事件傳送到 SIEM 伺服器和/或卡巴斯基安全中心。
6. 在**電子郵件通知設定**頁簽上配置電子郵件通知。
7. 儲存變更。

如何在應用程式主控台中配置記錄設定：

1. 在應用程式主控台樹狀目錄中，開啟**"記錄和通知"**節點的內容功能表。
2. 選擇**"內容"**。
   開啟**"通知"**視窗。
3. 在此視窗中，選擇要設定的記錄並指定單個事件的設定：
   - 事件保存的位置：本機報告或 Windows 事件記錄。
   - 事件通知：透過電子郵件通知、透過使用終端服務通知和/或透過執行可執行檔案通知。
   - 您是否要將事件傳送到 SIEM 伺服器和/或卡巴斯基安全中心。
4. 點選 **事件產生上限值設定**配置事件產生閾值。
5. 這將開啟一個視窗；在該視窗中，指定多少天後必須註冊下列事件：*資料庫已過期（天）*、*資料庫已嚴重過期（天）*和*長時間未執行關鍵區域掃描（天）*。
6. 按一下**電子郵件通知設定**設定電子郵件通知。
7. 儲存變更。

對記錄中的事件進行排序

預設情況下，記錄中的事件按時間倒序顯示。

要在記錄中排序事件：

1. 在應用程式主控台樹狀目錄中，開啟**"記錄和通知"**節點的內容功能表。
2. 選擇所需的記錄。
3. 在結果窗格中，選擇要用於排序清單中事件的欄位標題。

   在您下次檢視記錄前，將儲存排序結果。

篩選記錄中的事件

您可以將記錄設定僅顯示符合指定篩選條件（篩選器）的事件記錄。

要在記錄中篩選事件：

1. 在應用程式主控台樹狀目錄中，展開**"記錄和通知"**節點。
2. 選擇要為其設定篩選器的記錄，然後在結果窗格中按一下 **篩選器**。
   開啟**"篩選設定"**視窗。

3. 若要新增篩選器，請執行以下步驟：

   a. 在**欄位名稱**清單中，選擇要用於篩選事件的欄位。

   b. 在**操作員**清單中選擇篩選條件。篩選條件因在**欄位名稱**清單中選定的項目而有所不同。

   c. 在**欄位值**清單中，選擇篩選值。

   d. 單擊**"新增"**。

   已新增的篩選將出現在**篩選設定**視窗的篩選清單中。

4. 若有需要，請執行以下操作之一：

   - 要使用邏輯運算子"AND"組合多個篩選，請選擇**如果滿足所有條件**。
   - 要使用邏輯運算子"OR"組合多個篩選，請選擇**如果滿足任何條件**。

5. 點擊**確定**按鈕以儲存事件篩選條件。

   記錄的事件清單將僅顯示符合篩選條件的事件。在您下次檢視記錄前，將儲存篩選結果。

停用篩選器：

1. 在應用程式主控台樹狀目錄中，展開**"記錄和通知"**節點。
2. 選擇要刪除篩選器的記錄，然後按一下 **移除篩選器**。

   記錄將顯示所有事件。

從記錄中刪除事件

預設情況下，Kaspersky Embedded Systems Security 會保留 30 天的記錄。您可以變更記錄在日誌記錄中的儲存期間。

要刪除記錄中的事件：

1. 在應用程式主控台樹狀目錄中，展開**"記錄和通知"**節點。
2. 選擇要從中刪除事件的記錄，然後在結果窗格中按一下 **清除**。
3. 確認清除操作。

   記錄被清除。

匯出記錄中的資訊

您可以將資料從記錄匯出至 CSV 或 TXT 檔案中。

要從記錄匯出事件：

1. 在應用程式主控台樹狀目錄中，展開"**記錄和通知**"節點。
2. 選擇一個記錄，然後在結果窗格中按一下 **匯出記錄** 按鈕。
   開啟"**另存為**"視窗。
3. 指定要將資料從記錄匯出到的檔案的名稱、位置和類型。
4. 單擊"**儲存**"。

記錄中的資訊會保存到指定的檔案中。

系統稽核記錄

Kaspersky Embedded Systems Security 執行與 Kaspersky Embedded Systems Security 管理有關的事件的系統稽核。應用程式會記錄有關啟動應用程式、啟動和停止 Kaspersky Embedded Systems Security 工作、變更工作設定、建立和刪除自訂掃描工作的資訊。應用程式還記錄有關與受防護裝置上的安全入侵或安全入侵嘗試相關的事件的資訊。當您在應用程式主控台中選擇**系統稽核**節點時，所有這些事件的記錄都會顯示在結果窗格中。

預設情況下，Kaspersky Embedded Systems Security 會在系統稽核記錄中儲存記錄 30 天。您可以變更記錄在日誌記錄中的儲存期間。

您可以指定一個資料夾以供 Kaspersky Embedded Systems Security 用來儲存包含系統稽核記錄的檔案，而不使用預設值。

元件和工作日誌

當您在**記錄和通知**部分中選擇具有元件或工作名稱的節點時，有關 Kaspersky Embedded Systems Security 元件和工作運行的資訊將顯示在結果窗格的應用程式主控台中。

預設情況下，Kaspersky Embedded Systems Security 會在元件和工作的日誌中保留 30 天的記錄。對於工作 — 從完成的那一刻起。您可以變更工作日誌和元件日誌中的記錄的儲存期間。

您可以指定 Kaspersky Embedded Systems Security 儲存包含工作日誌和元件日誌的檔案所使用的資料夾，而不使用預設的資料夾。您還可以選擇 Kaspersky Embedded Systems Security 將在工作日誌和元件日誌中記錄的事件。

在工作記錄中，可以檢視自工作開始以來工作中發生的所有事件的詳細資訊，以及工作執行統計和工作設定。

要檢視有關 Kaspersky Embedded Systems Security 工作的統計和資訊：

1. 在應用程式主控台樹狀目錄中，展開"**記錄和通知**"節點。
2. 選擇一個工作，然後在結果窗格中按一下 **統計資料** 頁簽。

在事件檢視器中檢視 Kaspersky Embedded Systems Security 事件記錄

您可以使用適用於 Microsoft Management Console 的 Microsoft Windows 事件檢視器管理元件來檢視 Kaspersky Embedded Systems Security 的事件記錄。該記錄包含由 Kaspersky Embedded Systems Security 記錄且診斷執行故障所需的事件。

可以根據以下標準選擇將記錄在事件記錄中的事件：

- **按事件類型**。
- **按詳細等級**。詳細等級與記錄中的事件重要性等級相對應（資訊、重要或緊急事件）。最詳細的等級是"資訊"等級，將記錄所有事件。最不詳細的等級是"緊急"等級，只記錄緊急事件。

要檢視 Kaspersky Embedded Systems Security 事件記錄：

1. 點擊"**開始**"按鈕，在搜尋欄中輸入 `mmc` 指令，然後按 **ENTER** 鍵。

   Microsoft 管理主控台開啟。

2. 選擇"**檔案** > **新增或刪除管理單元**"。

   將開啟"**新增或刪除管理單元**"視窗。

3. 在可用管理單元清單中，選擇"**事件檢視器**"**管理單元**並點擊"**新增**"按鈕。

   將開啟"**選擇電腦**"視窗。

4. 在"**選擇電腦**"視窗中，指定已安裝 Kaspersky Embedded Systems Security 的裝置，然後點擊"**確定**"。

5. 在"**新增和刪除管理元件**"視窗中，點擊"**確定**"。

   在 Microsoft 管理主控台樹狀目錄中，將出現"**事件監視器**"節點。

6. 展開"事件檢視器"節點，並選擇"**應用程式和服務記錄** > **Kaspersky Embedded Systems Security**"子節點。

   將開啟 Kaspersky Embedded Systems Security 事件記錄。

關於 SIEM 整合

為了減小低效能裝置上的負載和降低由於應用程式記錄大小增大而造成系統效能降級的風險，可以透過 Syslog 協定將稽核事件和工作效能事件的發佈配置到 *syslog 伺服器*。

syslog 伺服器是用於聚合事件 (SIEM) 的外部伺服器。它會儲存和分析收到的事件，並執行其他記錄管理操作。

可以在兩種模式中使用 SIEM 整合：

- 在 syslog 伺服器上複製事件：在此模式下，其發佈在記錄設定中進行配置的所有工作效能事件以及所有系統稽核事件，即使在傳送到 SIEM 伺服器後仍繼續儲存在受防護裝置上。

  建議使用此模式以盡可能減少受防護裝置上的負載。

- 刪除事件的本機副本：在此模式下，在應用程式執行過程中註冊和發佈到 SIEM 的所有事件將從受防護裝置中刪除。

  應用程式永遠不會刪除安全記錄的本機版本。

Kaspersky Embedded Systems Security 可以將應用程式記錄中的事件轉換為 syslog 伺服器支援的格式，以便這些事件能夠被傳輸和被 SIEM 伺服器成功識別。應用程式支援轉換為結構化資料格式和 JSON 格式。

建議根據使用的 SIEM 伺服器的配置來選擇事件的格式。

配置 SIEM 整合設定

預設情況下，不使用 SIEM 整合。您可以啟用和停用 SIEM 整合，並配置相關設定。

您可以設定與多個 SIEM 伺服器的連線來降低事件無法傳送至 SIEM 伺服器的風險。

Kaspersky Embedded Systems Security 會連線到清單中的第一台 SIEM 伺服器。如果連線嘗試失敗，Kaspersky Embedded Systems Security 會逐一嘗試連線清單中的其他伺服器。

Kaspersky Embedded Systems Security 還使用系統稽核事件來通知您嘗試連線 SIEM 伺服器不成功以及將事件傳送到 SIEM 伺服器時出錯。

如何在卡巴斯基安全管理中心管理主控台中設定 SIEM 整合

1. 在卡巴斯基安全管理中心管理主控台樹狀目錄中，選取**政策**。
2. 選擇必要的政策並點擊以開啟政策內容。
3. 選擇 **記錄和通知** 部分。
4. 在"**SIEM 整合**"塊中，點擊"**設定**"按鈕。
   開啟"**SIEM 整合**"視窗。
5. 在"**整合設定**"塊中，選中"**啟用將安全事件傳輸到 SIEM 伺服器**"核取方塊。
6. 在**SIEM 伺服器連線設定**區塊中設定 SIEM 伺服器連線：
   a. 單擊"**新增**"。
   b. 這會開啟「**新增伺服器**」視窗，在該視窗中，輸入 SIEM 伺服器位址（IPv4、DNS）、連接埠和連線通訊協定。
   c. 單擊"**TCP 連線安全設定**"。
   d. 這將開啟**TCP 連線安全設定**視窗；在該視窗中，管理 SIEM 伺服器連線設定（請參閱下表）。

7. 如有必要，在**事件匯出至 SIEM 伺服器的設定**塊中選擇**刪除已被傳送到遠端 syslog 伺服器的事件的本機副本**核取方塊。如果選中該核取方塊，則應用程式在事件被成功發佈到 SIEM 伺服器後刪除事件的本機副本。建議在低效能裝置上使用此模式。如果清除該核取方塊，則應用程式僅將事件傳送到 SIEM 伺服器。記錄的副本將繼續儲存在本機。預設情況下，會取消勾選核取方塊。

   應用程式永遠不會刪除安全記錄的本機版本。

8. 在**事件格式**區塊中，選取您要將應用程式事件轉換成的格式，以便能夠將它們傳送到 SIEM 伺服器。預設情況下會選取「**將事件轉換為 STRUCTURED-DATA**」選項。建議根據使用的 SIEM 伺服器的配置來選擇事件的格式。

9. 關上掛鎖將政策套用至電腦。

10. 點擊**確定**以儲存變更。

如何在卡巴斯基安全管理中心網頁主控台中設定 SIEM 整合

1. 在網頁主控台的主視窗中，選擇**資產管理 → 政策**。

2. 點擊 Kaspersky Embedded Systems Security 政策的名稱。

   政策內容視窗將開啟。

3. 選擇**"應用程式設定"**標籤。

4. 選擇 **記錄和通知** 部分。

5. 在**"SIEM 整合"**塊中，點擊**"配置"**按鈕。

   開啟**"SIEM 整合"**視窗。

6. 選擇**"啟用將安全事件傳輸到 SIEM 伺服器"**核取方塊。

7. 在**SIEM 伺服器連線設定**區塊中設定 SIEM 伺服器連線：

   a. 單擊**"新增"**。

   b. 這會開啟「**SIEM 伺服器**」視窗，在該視窗中，輸入 SIEM 伺服器位址（IPv4、DNS）、連接埠和連線通訊協定。

   c. 在**"連線防護"**塊中，點擊**"SIEM 伺服器連線設定"**連接。

   d. 這將開啟**SIEM 伺服器連線設定**視窗；在該視窗中，管理 SIEM 伺服器連線設定（請參閱下表）。

   e. 在**事件格式**區塊中，選取您要將應用程式事件轉換成的格式，以便能夠將它們傳送到 SIEM 伺服器。預設情況下會選取「**將事件轉換為 STRUCTURED-DATA**」選項。建議根據使用的 SIEM 伺服器的配置來選擇事件的格式。

   f. 如有必要，在**連線設定**塊中選擇**刪除已被傳送到遠端 syslog 伺服器的事件的本機副本**核取方塊。如果選中該核取方塊，則應用程式在事件被成功發佈到 SIEM 伺服器後刪除事件的本機副本。建議在低效能裝置上使用此模式。如果清除該核取方塊，則應用程式僅將事件傳送到 SIEM 伺服器。記錄的副本將繼續儲存在本機。預設情況下，會取消勾選核取方塊。

      應用程式永遠不會刪除安全記錄的本機版本。

8. 關上掛鎖 將政策套用至電腦。

9. 點擊**確定**以儲存變更。

如何在應用程式主控台中設定 SIEM 整合

1. 在應用程式主控台樹狀目錄中，開啟**"記錄和通知"**節點的內容功能表。

2. 選擇**"SIEM 整合"**。
   開啟**"SIEM 整合"**視窗。

3. 在**"整合設定"**塊中，選中**"啟用將安全事件傳輸到 SIEM 伺服器"**核取方塊。

4. 在**SIEM 伺服器連線設定**區塊中設定 SIEM 伺服器連線：

   a. 單擊**"新增"**。

   b. 這會開啟「**新增伺服器**」視窗，在該視窗中，輸入 SIEM 伺服器位址（IPv4、DNS）、連接埠和連線通訊協定。

   c. 單擊**"TCP 連線安全設定"**。

   d. 這將開啟**TCP 連線安全設定**視窗；在該視窗中，管理 SIEM 伺服器連線設定（請參閱下表）。

5. 如有必要，在**事件匯出至 SIEM 伺服器的設定**塊中選擇**刪除已被傳送到遠端 syslog 伺服器的事件的本機副本**核取方塊。如果選中該核取方塊，則應用程式在事件被成功發佈到 SIEM 伺服器後刪除事件的本機副本。建議在低效能裝置上使用此模式。如果清除該核取方塊，則應用程式僅將事件傳送到 SIEM 伺服器。記錄的副本將繼續儲存在本機。預設情況下，會取消勾選核取方塊。

   應用程式永遠不會刪除安全記錄的本機版本。

6. 在**事件格式**區塊中，選取您要將應用程式事件轉換成的格式，以便能夠將它們傳送到 SIEM 伺服器。預設情況下會選取「**將事件轉換為 STRUCTURED-DATA**」選項。建議根據使用的 SIEM 伺服器的配置來選擇事件的格式。

7. 點擊**確定**以儲存變更。

SIEM 伺服器連線設定

參數	描述
逾時（秒）	SIEM 伺服器響應最大逾時。逾時結束後，Kaspersky Embedded Systems Security 會嘗試連線到不同的 SIEM 伺服器。
伺服器 TLS 憑證	用於與 SIEM 伺服器建立可信連線的 TLS 憑證。您可以使用 SIEM 管理介面取得 TLS 憑證。
使用雙向身分驗證	在 Kaspersky Embedded Systems Security 和 SIEM 之間建立安全連線時進行雙向身分驗證。要使用雙向身分驗證，您需要在 SIEM 設定中啟用雙向身分驗證，然後獲取加密容器並設定密碼以防護加密容器。加密容器是一個帶有憑證和私有金鑰的 PFX 封存檔案。配置 SIEM 設定後，您還需要在 Kaspersky Embedded Systems Security 設定中啟用雙向身分驗證並加載受密碼防護的加密容器。 加密容器必須受密碼防護。無法新增密碼為空的加密容器。

管理員和使用者通知方式

您可以將應用程式配置為將 Kaspersky Embedded Systems Security 執行中的下列事件和裝置的病毒防護狀態通知給管理員和存取裝置的使用者。

- 管理員可以收到有關選定類型事件的資訊。
- 存取裝置的區網使用者和終端裝置使用者可以收到即時檔案防護工作中"*偵測到物件*"類型事件的資訊。

管理員或使用者通知可以使用多種方式啟動：

- 終端服務工具。

  如果受防護裝置用作終端，則可以應用此方式來通知終端受防護裝置。
- 執行可執行檔。

  此方法是在發生事件時執行受防護裝置本機磁碟機上儲存的可執行檔。
- 透過電子郵件傳送。

  該方式使用電子郵件傳輸訊息。

您可以為單個事件類型建立訊息文字。它可以包括用以說明事件的訊息欄位。預設情況下，應用程式使用預設訊息通知使用者。

設定管理員和使用者通知

事件通知設定使您可以選擇配置和編寫訊息文字的方式。

如何在卡巴斯基安全管理中心管理主控台中配置事件通知

1. 在卡巴斯基安全管理中心管理主控台樹狀目錄中，選取**政策**。
2. 選擇必要的政策並點擊以開啟政策內容。
3. 在政策屬性視窗中，選取"**記錄和通知**"。
4. 在"**工作記錄**"區域中點擊"**設定**"。

   開啟"**通知**"視窗。
5. 選擇您希望為其選擇通知方式的事件，然後點擊**通知設定**。

   開啟"**通知設定**"視窗。
6. 對於電子郵件通知，您可以在 **電子郵件** 頁簽上新增事件通知訊息文字。

   若要新增有關事件資訊的欄位，請點擊"**變數**"按鈕，然後從下拉式清單中選擇相關欄位。事件資訊欄位在本部分中的清單中有所說明。

   若要還原預設事件訊息文字，請點擊"**根據預設**"按鈕。

7. 若要執行可執行檔進行通知，請在**可執行檔**頁簽上，選擇受防護裝置的本機磁碟機上的檔案，或輸入該檔案的完整路徑。當事件發生時，該檔案將在受防護裝置上執行。輸入用於執行檔的使用者名稱和密碼。

   指定可執行檔的路徑時可使用系統環境變數；不允許使用使用者環境變數。

8. 對於使用終端服務的通知，您可以在 **終端服務** 頁簽上新增事件通知訊息文字。

   若要新增有關事件資訊的欄位，請點擊**"變數"**按鈕，然後從下拉式清單中選擇相關欄位。事件資訊欄位在本部分中的清單中有所說明。

   若要還原預設事件訊息文字，請點擊**"根據預設"**按鈕。

9. 儲存變更。

如何在卡巴斯基安全管理中心網頁主控台中配置事件通知

1. 在網頁主控台的主視窗中，選擇**資產管理 → 政策**。

2. 點擊 Kaspersky Embedded Systems Security 政策的名稱。

   政策內容視窗將開啟。

3. 選擇**"應用程式設定"**標籤。

4. 轉到**記錄和通知 → 工作記錄** 並點擊 **配置** 按鈕。

5. 這將開啟一個視窗；在該視窗中，按一下要為其選擇通知方法的事件。

   開啟**"通知設定"**視窗。

6. 對於電子郵件通知，在 **通知使用者** 部分，選擇 **透過傳送電子郵件** 核取方塊並新增事件通知訊息文字。

   若要新增有關事件資訊的欄位，請點擊**"新增變數"**按鈕，然後從下拉式清單中選擇相關項目。事件資訊欄位在本部分中的清單中有所說明。

   若要還原預設事件訊息文字，請點擊**"重設"**按鈕。

7. 對於透過執行可執行檔進行的通知，在 **通知管理員** 部分，選擇 **透過執行可執行檔** 核取方塊並輸入受防護裝置本機磁碟上檔案的完整路徑。當事件發生時，該檔案將在受防護裝置上執行。輸入用於執行檔的使用者名稱和密碼。

   指定可執行檔的路徑時可使用系統環境變數；不允許使用使用者環境變數。

8. 對於使用終端服務的通知，在 **通知管理員** 部分，選擇 **使用終端服務** 核取方塊並新增事件通知訊息文字。

   若要新增有關事件資訊的欄位，請點擊**"新增變數"**按鈕，然後從下拉式清單中選擇相關項目。事件資訊欄位在本部分中的清單中有所說明。

   若要還原預設事件訊息文字，請點擊**"重設"**按鈕。

9. 儲存變更。

如何在應用程式主控台中配置事件通知

1. 在應用程式主控台樹狀目錄中，開啟**"記錄和通知"**節點的內容功能表。

2. 選擇**"內容"**。

   開啟**"通知"**視窗。

3. 選擇您希望為其選擇通知方式的事件，然後點擊**通知設定**。

   開啟**"通知設定"**視窗。

4. 對於電子郵件通知，您可以在 **電子郵件** 頁簽上新增事件通知訊息文字。

   若要新增有關事件資訊的欄位，請點擊**"變數"**按鈕，然後從下拉式清單中選擇相關欄位。事件資訊欄位在本部分中的清單中有所說明。

   若要還原預設事件訊息文字，請點擊**"根據預設"**按鈕。

5. 若要執行可執行檔進行通知，請在**可執行檔**頁簽上，選擇受防護裝置的本機磁碟機上的檔案，或輸入該檔案的完整路徑。當事件發生時，該檔案將在受防護裝置上執行。輸入用於執行檔的使用者名稱和密碼。

   指定可執行檔的路徑時可使用系統環境變數；不允許使用使用者環境變數。

6. 對於使用終端服務的通知，您可以在 **終端服務** 頁簽上新增事件通知訊息文字。

   若要新增有關事件資訊的欄位，請點擊**"變數"**按鈕，然後從下拉式清單中選擇相關欄位。事件資訊欄位在本部分中的清單中有所說明。

   若要還原預設事件訊息文字，請點擊**"根據預設"**按鈕。

7. 儲存變更。

事件資訊欄位

變數	描述
%EVENT_TYPE%	事件類型。
%EVENT_TIME%	事件時間。
%EVENT_SEVERITY%	重要性等級。
%OBJECT%	物件名稱（在"即時電腦防護"和"自訂掃描"工作中）。 "軟體模組更新"工作包括更新的名稱和帶有更新資訊的網頁位址。
%VIRUS_NAME%	根據病毒百科全書 分類的物件名稱。該名稱包含在 Kaspersky Embedded Systems Security 偵測物件時回傳的物件全名中。您可以在工作記錄中檢視偵測到的物件的全名。
%VIRUS_TYPE%	根據 Kaspersky 分類的偵測到的物件類型，例如"病毒"或"木馬"。這包含在 Kaspersky Embedded Systems Security 發現被感染的物件或疑似感染的物件時返回的偵測到的物件全名中。您可以在工作記錄中檢視偵測到的物件的全名。
%USER_COMPUTER%	在*即時檔案防護*工作中，存取裝置上物件的使用者的受防護裝置名稱。
%USER_NAME%	在*即時檔案防護*工作中，存取裝置上物件的使用者的名稱。
%FROM_COMPUTER%	發出通知的受防護裝置名稱。
%EVENT_REASON%	發生事件的原因（某些事件沒有該欄位）。
%ERROR_CODE%	錯誤代碼（僅用於"內部工作錯誤"事件）。
%TASK_NAME%	工作名稱（僅適用於與工作效能相關的事件）。
%PROTOCOL%	正在使用的協定。
%MESSAGE%	訊息文字。
%DEVICE_INSTANCEPATH%	裝置實例的路徑。
%DEVICE_VID%	裝置供應商
%DEVICE_PID%	控制器的類型。
%DEVICE_SERIALNUMBER%	裝置的序號。

配置電子郵件通知

如何在卡巴斯基安全管理中心管理主控台中配置電子郵件通知

1. 在卡巴斯基安全管理中心管理主控台樹狀目錄中，選取**政策**。
2. 選擇必要的政策並點擊以開啟政策內容。
3. 在政策屬性視窗中，選取**"記錄和通知"**。
4. 在**"工作記錄"**區域中點擊**"設定"**。
   開啟**"通知"**視窗。
5. 單擊**"電子郵件通知設定"**。
6. 在開啟的視窗中，選中**"傳送事件通知"**核取方塊。
7. 在**傳送通知時所使用的身分**下面，指定寄件者資訊：寄件者位址、SMTP 伺服器、SMTP 伺服器連接埠、使用者名稱和密碼。
8. 在**通知收件者**下面，指定收件者電子郵件信箱。
9. 若要測試設定，請點擊 **傳送測試訊息** 按鈕。

   測試訊息功能僅在卡巴斯基安全管理中心管理主控台和應用程式主控台中可用。

10. 指定傳送模式：**如果發生事件** 或者 **依排程(排程未指定)**。若要設定排程，請按一下 **編輯**。
11. 儲存變更。

如何在卡巴斯基安全管理中心網頁主控台中配置電子郵件通知

1. 在網頁主控台的主視窗中，選擇**資產管理 → 政策**。
2. 點擊 Kaspersky Embedded Systems Security 政策的名稱。
   政策內容視窗將開啟。
3. 選擇**"應用程式設定"**標籤。
4. 轉到**記錄和通知 → 工作記錄** 並點擊 **配置** 按鈕。
5. 這會開啟一個視窗；在該視窗中，選擇**電子郵件通知設定**頁簽。
6. 選擇**"傳送事件通知"**核取方塊。
7. 指定寄件者資訊：寄件者位址、SMTP 伺服器、SMTP 伺服器連接埠、使用者名稱和密碼。
8. 指定收件者的電子郵件信箱。

9. 指定傳送模式：**如果發生事件** 或者 **依排程**。如果適用，請配置排程。

10. 儲存變更。

如何在應用程式主控台中配置電子郵件通知

1. 在應用程式主控台樹狀目錄中，開啟**"記錄和通知"**節點的內容功能表。

2. 選擇**"內容"**。
   開啟**"通知"**視窗。

3. 單擊**"電子郵件通知設定"**。

4. 在開啟的視窗中，選中**"傳送事件通知"**核取方塊。

5. 在**傳送通知時所使用的身分**下面，指定寄件者資訊：寄件者位址、SMTP 伺服器、SMTP 伺服器連接埠、使用者名稱和密碼。

6. 在**通知收件者**下面，指定收件者電子郵件信箱。

7. 若要測試設定，請點擊 **傳送測試訊息** 按鈕。

   測試訊息功能僅在卡巴斯基安全管理中心管理主控台和應用程式主控台中可用。

8. 指定傳送模式：**如果發生事件** 或者 **依排程(排程未指定)**。若要設定排程，請按一下 **編輯**。

9. 儲存變更。

配置與管理伺服器的互動

您必須選擇 Kaspersky Embedded Systems Security 將其有關資訊傳送到卡巴斯基安全管理中心管理伺服器的物件類型。

如何在卡巴斯基安全管理中心管理主控台中設定與管理伺服器的整合

1. 在卡巴斯基安全管理中心管理主控台樹狀目錄中，選取**政策**。

2. 選擇必要的政策並點擊以開啟政策內容。

3. 在 **記錄和通知** 部分，點擊**與管理伺服器整合** 子部分中的 **設定** 按鈕。

4. 這將開啟一個視窗，在該視窗中，選擇 Kaspersky Embedded Systems Security 將其有關資訊傳送到卡巴斯基安全管理中心管理伺服器的物件類型：

   - **關於備份區中的檔案**
   - **關於未處理的檔案**
   - **關於已安裝的裝置**
   - **關於威脅發展鏈條**

5. 儲存變更。

   Kaspersky Embedded Systems Security 會將有關選定物件類型的資訊傳送到管理伺服器。

如何在卡巴斯基安全管理中心網頁主控台中設定與管理伺服器的整合

1. 在網頁主控台的主視窗中，選擇**資產管理 → 政策**。
2. 點擊 Kaspersky Embedded Systems Security 政策的名稱。

   政策內容視窗將開啟。
3. 選擇"**應用程式設定**"標籤。
4. 在 **記錄和通知** 部分，點擊**與管理伺服器整合** 子部分中的 **配置** 按鈕。
5. 這將開啟一個視窗，在該視窗中，選擇 Kaspersky Embedded Systems Security 將其有關資訊傳送到卡巴斯基安全管理中心管理伺服器的物件類型：

   - **備份檔案**
   - **關於未處理的檔案**
   - **已封鎖的網路工作階段**
   - **已安裝的裝置**
6. 儲存變更。

BitLocker 完整磁碟加密管理

BitLocker 是 Windows 作業系統內建的加密技術。Kaspersky Embedded Systems Security 允許您使用卡巴斯基安全管理中心控制和管理 Bitlocker。BitLocker 可對邏輯磁區進行加密。有關 BitLocker 的詳細資訊，請參閱 Microsoft 文件。

Kaspersky Embedded Systems Security 不支援在 Windows Vista 和 Windows Server 2008 電腦上管理 BitLocker 。

在加密磁碟時，BitLocker 會將啟動程式和其他輔助檔案存放於「system partition」。此分割區未加密。作業系統在安裝 Windows 時會自動建立系統分割區。如果在安裝 Windows 之前磁碟已完全分割，則作業系統無法建立系統分割區。在這種情況下，當啟動 BitLocker 磁碟加密時，作業系統會提示使用者對磁碟重新分割，並建立系統分割區。建立系統分割區後，作業系統啟動 BitLocker 加密。

Kaspersky Embedded Systems Security 不支援卸除式磁碟機的 BitLocker 加密。

BitLocker 使用受信任平台模組提供對存取金鑰的安全儲存。A *Trusted Platform Module* (TPM) 是一個與安全相關並提供基本功能的微晶片（例如用於儲存加密金鑰）。受信任平台模組通常安裝在電腦主機板上並且透過硬體匯流排與其他所有系統元件進行互動。使用 TPM 是儲存 BitLocker 存取金鑰最安全的方式，因為 TPM 提供了啟動前系統完整性驗證。您仍然可以在沒有 TPM 的電腦上對磁碟機進行加密。在這種情況下，將使用密碼對存取金鑰進行加密。BitLocker 使用以下身分驗證方式：

- TPM。
- TPM 和 PIN。
- 密碼。

在加密磁碟機之前，BitLocker 會建立修復金鑰。Kaspersky Embedded Systems Security 會讀取修復金鑰並將其傳送到卡巴斯基安全管理中心，以便您可以還原對磁碟的存取，例如，當使用者忘記密碼時。

對系統硬碟磁碟機進行加密後，使用者需要透過 BitLocker 身分驗證才能啟動作業系統。身分驗證完成後，BitLocker 將允許使用者登入。BitLocker 不支援單點登錄技術 (SSO)。

如果使用者使用 BitLocker 加密磁碟，Kaspersky Embedded Systems Security 會將磁碟加密資訊和修復金鑰傳送到卡巴斯基安全管理中心。

如果正在使用 Windows 群組政策，請在政策設定中關閉 BitLocker 管理。Windows 政策設定可能與 Kaspersky Embedded Systems Security 政策設定衝突。在對磁碟機進行加密時，可能會發生錯誤。

啟動 BitLocker 磁碟機加密

在開始完整磁碟加密之前，建議您確保電腦未受到感染。若要執行操作，應啟動完整掃描或關鍵區域掃描工作。在已被 rootkit 感染的電腦上執行完整磁碟加密可能導致電腦無法執行。

若要在執行適用於伺服器的 Windows 作業系統的電腦上使用 BitLocker 磁碟機加密，可能需要安裝“BitLocker 磁碟機加密”元件。可使用作業系統工具（新增角色和元件精靈）安裝該元件。有關安裝“BitLocker 磁碟機加密”的更多資訊，請參閱 Microsoft 文件。

如何在卡巴斯基安全管理中心管理主控台中執行 BitLocker 磁碟機加密

1. 在卡巴斯基安全管理中心管理主控台樹狀目錄中，選取**政策**。
2. 選擇必要的政策並點擊以開啟政策內容。
3. 選擇 **資料加密** 部分。
4. 在“**加密模式**”下拉式清單中，選取“**加密所有硬碟磁碟機**”。

   如果電腦安裝了多個作業系統，在加密後，您將能夠只載入執行了加密的作業系統。

5. 設定進階 BitLocker 磁碟機加密選項（參見下表）。
6. 點擊**確定**以儲存變更。

如何在卡巴斯基安全管理中心網頁主控台中執行 BitLocker 磁碟機加密

1. 在網頁主控台的主視窗中，選擇**資產管理 → 政策**。
2. 點擊 Kaspersky Embedded Systems Security 政策的名稱。
   政策內容視窗將開啟。
3. 選擇“**應用程式設定**”標籤。
4. 轉到“**資料加密**”區域。
5. 在**完整磁碟加密**子區域中，按一下**配置**按鈕。
6. 在“**加密模式**”下拉式清單中，選取“**加密所有硬碟磁碟機**”。

   如果電腦安裝了多個作業系統，在加密後，您將能夠只載入執行了加密的作業系統。

7. 設定進階 BitLocker 磁碟機加密選項（參見下表）。
8. 點擊**確定**以儲存變更。

您可以使用應用程式主控台來控制使用者電腦上的磁盤加密或解密過程。

套用政策後，根據身分驗證設定，應用程式會在"小型診斷視窗"視窗或應用程式主控台中顯示以下請求：

- 僅 TPM。無需使用者輸入。磁碟將在電腦重新啟動時被加密。
- TPM + PIN / 密碼。如果 TPM 模組可用，將顯示 PIN 碼提示視窗。如果 TPM 模組不可用，您將看到一個用於預啟動身分驗證的密碼提示視窗。
- 僅密碼。您將看到一個用於預啟動身分驗證的密碼提示視窗。

如果為電腦作業系統啟用聯邦資訊處理標準相容模式，則在 Windows 8 及更早版本的作業系統中，將顯示儲存裝置連線請求以儲存還原金鑰檔案。您可以將多個還原金鑰檔案儲存在單一儲存裝置上。

設定密碼或 PIN 碼後，BitLocker 會提示使用者重新啟動電腦，以檢查電腦與 BitLocker 的相容性。Kaspersky Embedded Systems Security 會在"小型診斷視窗"視窗或應用程式主控台中顯示對應的通知。接下來，使用者需要完成 BitLocker 身分驗證過程。完成身分驗證過程後，使用者必須登入到系統。載入作業系統後，BitLocker 將開始加密。

如果無法存取加密金鑰，使用者可以請求區域網路管理員提供還原金鑰（如果還原金鑰在較早前未儲存在儲存裝置上或已遺失）。

BitLocker 磁碟機加密元件設定

參數	描述
啟用需要在平板電腦上預啟動鍵盤輸入的 BitLocker 身分驗證	在預啟動環境中使用需要資料輸入的身分驗證，即使此平台沒有能力進行預啟動輸入（例如使用平板電腦上的觸控式螢幕鍵盤）。 平板電腦的觸控式螢幕在預啟動環境中不可用。例如，要在平板電腦上完成 BitLocker 身分驗證，使用者必須連線 USB 鍵盤。 如果選定此核取方塊，則允許使用需要預啟動輸入的身分驗證。我們建議在預啟動環境中僅對擁有備用資料輸入的裝置（例如除了觸控式螢幕鍵盤之外的 USB 鍵盤）使用此設定。 如果清除此核取方塊，則無法在平板電腦上使用 BitLocker 磁碟機加密。
使用硬體加密(Windows 8 和後續版本)	如果選定此核取方塊，則應用程式將應用硬體加密。這可以提高加密速度並使用較少的電腦資源。
僅加密使用的磁碟空間(Windows 8 和後續版本)	該核取方塊可啟用/停用將加密區域僅限為已用硬碟磁區的選項。該限制可減少加密時間。 在啟動加密後啟用或者停用"**僅加密使用的磁碟空間(Windows 8 和後續版本)**"功能不會修改此設定，直到硬碟磁碟機被解密為止。開始加密之前您必須選擇或清除該核取方塊。 如果選定該核取方塊，則僅加密使用的硬碟部分。Kaspersky Embedded Systems Security 會在新增資料時自動對其進行加密。 如果清空該核取方塊，整個硬碟將被加密，包括先前刪除和修改檔案殘留的碎片。 建議對尚未修改或刪除資料的新硬碟使用該選項。如果對已在使用中的硬碟應用加密，則建議加密整個硬碟。這樣可確保防護所有資料，甚至已刪除的資料也能夠部分還原。 預設情況下，會取消勾選核取方塊。

參數	描述
身分驗證方法	**受信任平台模組 (TPM)** 如果選擇此選項，則 BitLocker 使用受信任平台模組 (TPM)。 受信任平台模組 (TPM) 是一個與安全相關並提供基本功能的微晶片（例如用於儲存加密金鑰）。受信任平台模組通常安裝在電腦主機板上並且透過硬體匯流排與其他所有系統元件進行互動。 對於執行 Windows 7 或 Windows Server 2008 R2 的電腦，只能使用 TPM 模組進行加密。如果未安裝 TPM 模組，則無法進行 BitLocker 加密。不支援在這些電腦上使用密碼。 配有受信任平台模組的裝置可以建立只能使用此裝置解密的加密金鑰。受信任平台模組將使用其自有的根儲存金鑰加密加密金鑰。根儲存金鑰儲存在受信任平台模組中。這提供了防禦駭客攻擊加密金鑰的附加防護。 預設情況下已選擇此操作。 您可以為存取加密金鑰設定一層額外防護，用密碼或者 PIN 加密金鑰： **为 TPM 使用 PIN**如果選中此核取方塊，使用者可以使用 PIN 碼存取儲存在受信任平台模組 (TPM) 中的加密金鑰。如果清除此核取方塊，則會禁止使用者使用 PIN 碼。要存取加密金鑰，使用者必須輸入密碼。 **受信任平台模組 (TPM)，或密碼（如果 TMP 不可使用）** 如果選定此選項，當受信任平台模組 (TPM) 不可用時，使用者可使用密碼存取加密金鑰。如果清除該核取方塊且 TPM 不可用，則將不會啟動完整磁碟加密。 **僅限密碼（Windows 8 和後續版本）** 如果選定此選項，Kaspersky Embedded Systems Security 將在使用者嘗試存取加密磁碟時提示使用者輸入密碼。 沒有使用受信任平台模組 (TPM) 時可以選擇此選項。 選取的身分驗證方法必須透過指定密碼或 PIN 要求來進行設定： • **最小 PIN 長度(字元數)** • **使用增強型 PIN (字母和數字)**增強 PIN 允許使用除了數字字元的其它字元：大寫和小寫拉丁字母，特殊字元，和空格。 • **最小密碼長度(字元數)** • **限制 TPM 的密碼/PIN 代碼有效期（天）**
自動重新建立還原金鑰（天）	自動更新密碼以還原對 BitLocker 防護的磁碟機的存取權限。如果該核取方塊被選中，請指定還原金鑰密碼的有效期。

解密受 BitLocker 防護的硬碟磁碟機

使用者可以使用作業系統解密磁碟（"*關閉 BitLocker*"功能）。之後，Kaspersky Embedded Systems Security 會提示重新加密磁碟。除非在政策中啟用磁碟解密，否則 Kaspersky Embedded Systems Security 將提示您加密磁碟。

如何使用卡巴斯基安全管理中心管理主控台解密受 BitLocker 防護的硬碟磁碟機

1. 在卡巴斯基安全管理中心管理主控台樹狀目錄中，選取**政策**。
2. 選擇必要的政策並點擊以開啟政策內容。
3. 選擇 **資料加密** 部分。
4. 在"**加密模式**"下拉式清單中，選取"**解密所有硬碟磁碟機**"。
5. 點擊**確定**以儲存變更。

如何使用卡巴斯基安全管理中心網頁主控台解密受 BitLocker 防護的硬碟磁碟機

1. 在網頁主控台的主視窗中，選擇**資產管理 → 政策**。
2. 點擊 Kaspersky Embedded Systems Security 政策的名稱。

   政策內容視窗將開啟。
3. 選擇"**應用程式設定**"標籤。

4. 轉到**"資料加密"**區域。

5. 在**完整磁碟加密**子區域中，按一下**配置**按鈕。

6. 在**"加密模式"**下拉式清單中，選取**"解密所有硬碟磁碟機"**。

7. 點擊**確定**以儲存變更。

您可以使用應用程式主控台來控制磁碟加密或解密過程。

還原對 BitLocker 防護的磁碟機的存取權限

如果使用者忘記了由 BitLocker 加密的硬碟存取密碼，則需要啟動還原程序（請求-回應）。

> 如果電腦的作業系統啟用了聯邦資訊處理標準 (FIPS) 相容模式，則在 Windows 8 和更早版本中，還原金鑰檔案將在加密之前儲存到卸除式磁碟機中。要恢復對磁碟機的存取權限，請插入卸除式磁碟機，然後按照螢幕上的說明進行操作。

還原對 BitLocker 加密的硬碟存取權限包括以下步驟：

1. 使用者告知管理員還原金鑰 ID（請參見下圖）。

2. 管理員在卡巴斯基安全管理中心中驗證電腦內容中的還原金鑰 ID。使用者提供的 ID 必須與電腦內容中顯示的 ID 相符。

   如果還原金鑰 ID 匹配，管理員會將還原金鑰交給使用者。

3. 使用者輸入還原金鑰，然後獲得對硬碟的存取權限。

還原對 BitLocker 加密磁碟機的存取權限

還原對系統磁碟機的存取權限

要啟動還原程序，使用者需要在預先引導身分驗證階段按 **Esc** 鍵。

如何在卡巴斯基安全管理中心管理主控台中檢視由 BitLocker 加密的系統磁碟機的還原金鑰

1. 在卡巴斯基安全管理中心管理主控台樹狀目錄中，選取**受管理裝置**。
2. 轉至**裝置**頁簽。
3. 開啟請求還原加密資料存取的使用者電腦的上下文功能表。
4. 在內容功能表中，選取**"授予離線模式下的存取權限"**。
5. 要求使用者在 BitLocker 密碼輸入視窗中輸入還原金鑰 ID，然後與**"還原金鑰 ID"**欄位的**存取受 BitLocker 防護的系統磁碟機**頁簽上的 ID 進行比對。

   如果 ID 不比對，該金鑰無法用於還原指定系統磁碟的存取。請確保選定電腦的名稱與使用者電腦的名稱相符合。

6. 向使用者傳送**"還原金鑰"**欄位中指定的金鑰。

如何在卡巴斯基安全管理中心網頁主控台中檢視由 BitLocker 加密的系統磁碟機的還原金鑰

1. 在網頁主控台的主視窗中，選擇**資產管理 → 資產（裝置）**。
2. 選中要還原其磁碟機存取權限的電腦名稱旁邊的核取方塊。
3. 點擊**"同意存取離線模式下的裝置"**。
4. 驗證還原金鑰 ID使用者提供的 ID 必須與電腦設定中顯示的 ID 相符。

   如果 ID 不比對，該金鑰無法用於還原指定系統磁碟的存取。請確保選定電腦的名稱與使用者電腦的名稱相符合。

5. 點擊**"接收金鑰"**。
6. 向使用者傳送**"還原金鑰"**欄位中指定的金鑰。

載入作業系統後，Kaspersky Embedded Systems Security 會提示使用者變更密碼或 PIN 代碼。設定新密碼或 PIN 代碼後，BitLocker 將建立一個新的還原密碼，並將其傳送給卡巴斯基安全管理中心。

還原對非系統磁碟機的存取權限

要啟動還原程序，使用者需要在提供磁碟機存取的視窗中點擊**"Forgot your password"**連結。獲得對加密磁碟機的存取權限後，使用者可以在 BitLocker 設定中啟用在 Windows 身分驗證期間自動解鎖磁碟機。

如何在卡巴斯基安全管理中心管理主控台中檢視由 BitLocker 加密的非系統磁碟機的還原金鑰

1. 在卡巴斯基安全管理中心管理主控台樹狀目錄中，選取**進階 → 資料加密與防護 → 加密磁碟機**資料夾。
2. 在工作區中選取您想要為其建立存取金鑰檔案的加密裝置，然後在裝置的內容功能表中，點擊**"在 Kaspersky Embedded Systems Security 中獲取裝置的存取權限"**。
3. 提示使用者在 BitLocker 密碼輸入視窗中輸入還原金鑰 ID，然後在**"還原金鑰 ID"**欄位中對比該 ID。

   如果 ID 不比對，該金鑰無法用於還原指定磁碟的存取。請確保選定電腦的名稱與使用者電腦的名稱相符合。

4. 向使用者傳送**"還原金鑰"**欄位中指定的金鑰。

如何在卡巴斯基安全管理中心網頁主控台中檢視由 BitLocker 加密的非系統磁碟機的還原金鑰

1. 在網頁主控台的主視窗中，選擇**操作 → 資料加密與防護 → 加密磁碟機**。
2. 選中要還原其磁碟機存取權限的電腦名稱旁邊的核取方塊。
3. 點擊**"同意存取離線模式下的裝置"**。

   這將啟動用於授予裝置存取權限的精靈。

4. 按照精靈的說明授予對裝置的存取權限：
   a. 選擇 Kaspersky Embedded Systems Security 外掛程式。
   b. 驗證還原金鑰 ID使用者提供的 ID 必須與電腦設定中顯示的 ID 相符。

      如果 ID 不比對，該金鑰無法用於還原指定系統磁碟的存取。請確保選定電腦的名稱與使用者電腦的名稱相符合。

   c. 點擊**"接收金鑰"**。
5. 向使用者傳送**"還原金鑰"**欄位中指定的金鑰。

暫停 BitLocker 防護以更新軟體

更新作業系統、安裝作業系統的更新套件、或者更新開啟了 BitLocker 防護的其它軟體有眾多特殊考量。安裝更新可能需要多次重啟電腦。每次重啟後，使用者必須完成 BitLocker 身分驗證。為了確保更新正確安裝，您可以暫時關閉 BitLocker 身分驗證。在此情況下，磁碟機保持加密，使用者可以在登入系統後存取資料。若要管理 BitLocker 身分驗證，您可以使用*"BitLocker 防護管理"*工作。您可以使用此工作指定不需要 BitLocker 身分驗證的電腦重啟次數。按這種方式，在更新安裝和 *BitLocker 防護管理*工作完成後，BitLocker 身分驗證將自動啟用。您可以隨時啟用 BitLocker 身分驗證。

如何在卡巴斯基安全管理中心管理主控台中暫停 BitLocker 防護

1. 在卡巴斯基安全管理中心管理主控台樹狀目錄中，選取**工作**。
   工作清單開啟。
2. 單擊**"新工作"**。

啟動"工作精靈"。按照精靈的說明進行操作。

步驟 1. 選取工作類型

選取 **Kaspersky Embedded Systems Security for Windows (4.1) → BitLocker 防護管理**。

步驟 2. BitLocker 防護管理

配置 BitLocker 身份驗證.若要暫停 BitLocker 防護，請選擇**暫時允許略過 BitLocker 身分驗證**並輸入無需 BitLocker 身分驗證進行重啟的次數（1 到 15 次）。如有必要，輸入工作的到期日期和時間。工作會在指定時間關閉，當電腦重啟時使用者必須完成 BitLocker 身分驗證。

步驟 3. 選取將要對其分配工作的裝置

選取將要執行工作的電腦。下列選項可用：

- 將工作分配給管理群組。在這種情況下，工作分配給先前建立的管理群組中包括的電腦。
- 選取管理伺服器在網路中偵測到的電腦：*未分配裝置*。特定裝置可包括管理群組中的裝置以及未配置裝置。
- 手動指定裝置位址或從清單中匯入位址。您可以指定您要將工作分配給的裝置的 NetBIOS 名稱、IP 位址和 IP 子網路。

步驟 4. 定義工作名稱

輸入工作名稱，例如 *更新到 Windows 10*。

步驟 5. 完成工作建立

結束精靈。如有必要，選中**"精靈完成時執行工作"**核取方塊。您可以在工作內容中監控工作進度。

如何使用網頁主控台暫停 BitLocker 防護

1. 在網頁主控台的主視窗中，選擇**資產管理 → 工作**。
   工作清單開啟。
2. 單擊**"新增"**。

啟動"工作精靈"。按照精靈的說明進行操作。

步驟 1. 配置一般工作設定

配置一般工作設定：

1. 在**應用程式**下拉式清單中，選取 **Kaspersky Embedded Systems Security**。
2. 在"**工作類型**"下拉式清單中，選取"**BitLocker 防護管理**"。
3. 在"**工作名稱** "欄位中，輸入簡要說明，例如，"*更新到 Windows 10*"。
4. 在"**要將工作指派給的裝置**"塊中，選取工作範圍。

步驟 2. BitLocker 防護管理

配置 BitLocker 身份驗證.若要暫停 BitLocker 防護，請選擇**暫時允許略過 BitLocker 身分驗證**並輸入無需 BitLocker 身分驗證進行重啟的次數（1 到 15 次）。如有必要，輸入工作的到期日期和時間。工作會在指定時間關閉，當電腦重啟時使用者必須完成 BitLocker 身分驗證。

步驟 3. 完成工作建立

結束精靈。在工作清單中將顯示一個新工作。

要執行工作，請選中與工作對應的核取方塊，然後點擊**"開始"**按鈕。

因此，當工作執行時，下次電腦重啟後，BitLocker 不會提示使用者進行身分驗證。每次電腦未經 BitLocker 身分驗證重啟後，Kaspersky Embedded Systems Security 都會產生相應事件並記錄剩餘的重啟次數。

當達到指定的重啟次數或者工作的到期時間時，BitLocker 身分驗證會自動開啟。要獲得對資料的存取權限，使用者必須完成 BitLocker 身分驗證。

在執行 Windows 7 的電腦上，BitLocker 不能計數電腦重啟。計數 Windows 7 電腦上的重啟由 Kaspersky Embedded Systems Security 處理。因此，若要在每次重啟後自動開啟 BitLocker 身分驗證，必須啟動 Kaspersky Embedded Systems Security。

若要提前開啟 BitLocker 身分驗證，請開啟 *BitLocker 防護管理*工作內容並選擇**"每次重啟請求身分驗證"**。

與協力廠商系統整合

本節介紹 Kaspersky Embedded Systems Security 與協力廠商功能和技術的整合。

系統監視器的效能計數器

效能計數器是 Kaspersky Embedded Systems Security 的一個元件，可用於在防護元件運行期間監控應用程式效能。Kaspersky Embedded Systems Security 會在安裝過程中記錄效能計數器。

您可以使用 Windows 控制台中的「系統監視器」應用程式檢視應用程式效能計數器。有關使用效能計數器的詳情，請參閱Microsoft Technical Support 網站。

例如，您可以使用效能計數器識別 Kaspersky Embedded Systems Security 與其他應用程式一起運行時出現的資源短缺問題，還可以診斷崩潰並識別 Kaspersky Embedded Systems Security 的不良設定。

因為資源不足而未處理的要求數

因為資源不足而未處理的要求數

描述	因為系統資源（例如 RAM）不足，而未處理的檔案攔截驅動程式要求總數；從上次啟動 Kaspersky Embedded Systems Security 的時間算起。 Kaspersky Embedded Systems Security 會略過檔案攔截驅動程式未處理其掃描要求的物件。
用途	此計數器可用來消除即時電腦防護品質可能因系統資源不足而降低的情況。
標準值/上限值	0 / 1
建議的讀取間隔時間	1 小時。
如果值超過上限值時的設定建議	如果計數器值不為零，則表明 Kaspersky Embedded Systems Security 處理程序需要更多 RAM 來處理請求。 其他應用程式的活動處理程序可能正在使用所有可用的 RAM。

已提交進行處理的請求數量

已提交進行處理的請求數量

描述	等待工作處理程序處理的物件數量。
用途	此計數器可用於監視 Kaspersky Embedded Systems Security 工作程序的負載，以及受防護裝置上檔案活動的整體程度。
標準值/上限值	該計數器值可能因受防護裝置上的檔案活動水平而異。
建議的讀取間隔時間	1 分鐘。
如果值超過上限值時的設定建議	N/A

每秒處理的物件數

每秒處理的物件數

描述	已處理的物件數除以處理那些物件所花的時間量（以相等間隔時間來計算）。
用途	此計數器會反映物件處理的速度；可用於偵測與消除因分配至 Kaspersky Embedded Systems Security 處理程序的處理器時間不足，或 Kaspersky Embedded Systems Security 作業錯誤，所造成的受防護裝置效能低落。
標準值/上限值	視情況有所不同 / 無。
建議的讀取間隔時間	1 分鐘。
如果值超過上限值時的設定建議	此計數器中的值，要視 Kaspersky Embedded Systems Security 設定，以及受防護裝置上來自其他應用程式的負載而定。 觀察較長時間內的平均計數器值。如果平均計數器值下降，則可能發生以下情況之一： • Kaspersky Embedded Systems Security 處理程序處理物件的處理器時間不足。 確保 Kaspersky Embedded Systems Security 獲得額外的處理器時間（例如，透過降低受防護裝置上其他應用程式的負荷）。 • Kaspersky Embedded Systems Security 出錯（多個流空閒）。 重新啟動 Kaspersky Embedded Systems Security。

受感染物件佇列中的元素數

受感染物件佇列中的元素數

描述	目前等候處理（未受感染或已刪除）的受感染物件數。
用途	此計數器可讓您偵測： • 由於檔案攔截調度程式的潛在故障而導致的即時電腦防護中斷。 • 因不同工作處理程序與 Kaspersky Embedded Systems Security 間的處理器時間分配不平均，而造成的處理程序過載。 • 病毒爆發。
標準值/上限值	當 Kaspersky Embedded Systems Security 正在處理受感染或可能受感染物件時，此計數器值可能大於零；但當處理完成時會傳回零，或計數器值會長久保持非零的狀態。
建議的讀取間隔時間	1 分鐘。
如果值超過上限值時的設定建議	如果此計數器值常久未傳回零： • Kaspersky Embedded Systems Security 並未處理物件（檔案攔截調度程式可能已當機）。 重新啟動 Kaspersky Embedded Systems Security。 • 處理物件的處理器時間可能不足。 確保 Kaspersky Embedded Systems Security 獲得額外的處理器時間（例如，透過降低受防護裝置上其他應用程式的負荷）。 • 病毒已爆發。 在即時檔案防護元件中有大量受感染或可能受感染物件也是病毒爆發的跡象。您可以在元件統計或元件記錄中檢視有關偵測到的物件的數量的資訊。

拒絕需求總數

拒絕需求總數

描述	**由檔案攔截驅動程式發出但未被應用程式處理程序接受的物件處理請求總數；從 Kaspersky Embedded Systems Security 上次啟動時開始計數。** **應用程式將略過被 Kaspersky Embedded Systems Security 處理程序拒絕處理要求的物件。**
用途	此計數器可讓您偵測： • 由於 Kaspersky Embedded Systems Security 處理程序過載而導致的即時電腦防護能力下降。 • 由於檔案攔截調度程式故障而導致的即時電腦防護中斷。
標準值/上限值	0 / 1

描述	**由檔案攔截驅動程式發出但未被應用程式處理程序接受的物件處理請求總數；從 Kaspersky Embedded Systems Security 上次啟動時開始計數。** **應用程式將略過被 Kaspersky Embedded Systems Security 處理程序拒絕處理要求的物件。**
建議的讀取間隔時間	1 小時。
如果值超過上限值時的設定建議	遭拒的處理要求數等於略過的物件數。 視計數器的行為而定，可能會發生以下情況： • 計數器顯示一些請求被長時間拒絕：Kaspersky Embedded Systems Security 處理程序正在全力運作。應用程式無法掃描物件。 為防止物件被跳過，請增加分配給應用程式的系統資源。 • 被拒絕的要求數量明顯超過上限值，且還在快速成長中：檔案攔截調度程式已失效。Kaspersky Embedded Systems Security 在物件被存取時不掃描物件。 重新啟動 Kaspersky Embedded Systems Security。

略過請求總數

略過請求總數

描述	由檔案攔截驅動程式發出且被 Kaspersky Embedded Systems Security 收到但未產生處理完成事件的物件處理請求總數；此數字從應用程式上次啟動時開始計數。 如果某個物件處理請求被一個工作處理程序接受但未傳送處理完成事件，則驅動程式會將該請求轉移給其他處理程序，並且計數器**"要求略過總數"**的值會加 1。如果驅動程式已經遍歷所有工作處理程序，並且沒有任何處理程序收到該處理請求（全部都在忙碌）或傳送處理完成事件，則 Kaspersky Embedded Systems Security 將略過該物件，因此計數器**"要求略過總數"**的值會加 1。
用途	此計數器使您能夠偵測，因為檔案攔截調度程式故障而產生的效能降低情況。
標準值/上限值	0 / 1
建議的讀取間隔時間	1 小時。
如果值超過上限值時的設定建議	如果計數器並非零，表示有一或多個檔案攔截調度程式執行緒已凍結，且停止作業。計數器等於目前閒置的執行緒數。 如果掃描速度緩慢，請重新啟動 Kaspersky Embedded Systems Security 來還原離線的資料流。

檔案攔截調度程式執行緒的最大數

從 Kaspersky Embedded Systems Security 4.1 版開始，不再支援「檔案攔截分派器資料流數目上限」計數器。

檔案攔截調度程式執行緒的平均數

從 Kaspersky Embedded Systems Security 4.1 版開始，不再支援「檔案攔截分派器資料流平均數目」計數器。

Kaspersky Embedded Systems Security SNMP 計數器和 TRAP

如果要安裝的防毒元件集中包含 SNMP 協定支援 元件，您可以使用 Simple Network Management Protocol (SNMP) 檢視 Kaspersky Embedded Systems Security 計數器和 TRAP。

若要從管理員的工作站檢視 Kaspersky Embedded Systems Security 計數器與 TRAP，請啟動受防護裝置上的 SNMP 服務，並啟動管理員工作站上的 SNMP 與 SNMP TRAP 服務。

Kaspersky Embedded Systems Security SNMP 計數器

本節包含介紹 Kaspersky Embedded Systems Security SNMP 計數器設定的表格。

效能計數器

效能計數器

計數器	定義
currentRequestsAmount	已提交進行處理的請求數量
currentInfectedQueueLength	受感染物件佇列中的元素數
currentObjectProcessingRate	每秒處理的物件數
currentWorkProcessesNumber	Kaspersky Embedded Systems Security 所使用的工作處理程序的目前數量

備份計數器

備份計數器

計數器	定義
currentBackupStorageSize	備份區中的資料總量 (MB)

一般計數器

一般計數器

計數器	定義
lastCriticalAreasScanAge	自工作 *關鍵區域掃描* 完成後經過的時間間隔（以秒為單位）。
licenseExpirationDate	產品授權到期日期。如果新增了啟動金鑰和備用金鑰，則將顯示與備用金鑰關聯的產品授權的到期日期。
currentApplicationUptime	Kaspersky Embedded Systems Security 自從上次啟動起的執行時間（單位為百分之一秒）。

更新計數器

更新計數器

計數器	定義
avBasesAge	自最新安裝的資料庫更新建立日期起經過的時間，以百分之一秒為單位。

即時檔案防護計數器

即時檔案防護計數器

計數器	定義
totalObjectsProcessed	自上次啟動 即時檔案防護 元件以來掃描的物件總數
totalInfectedObjectsFound	自上次啟動 即時檔案防護 元件以來偵測到的受感染物件和其他物件總數
totalSuspiciousObjectsFound	自上次啟動 即時檔案防護 元件以來偵測到的可能受感染物件總數
totalVirusesFound	自上次啟動 即時檔案防護 元件以來偵測到的物件總數
totalObjectsQuarantined	Kaspersky Embedded Systems Security 放入隔離的受感染、可能受感染和其他物件的總數；從上次啟動"即時檔案防護"工作的時間算起
totalObjectsNotQuarantined	Kaspersky Embedded Systems Security 嘗試隔離但無法隔離成功的受感染或可能受感染物件總數；從上次啟動"即時檔案防護"工作的時間算起
totalObjectsDisinfected	Kaspersky Embedded Systems Security 已解毒的受感染物件總數；從上次啟動 即時檔案防護 元件時起計算
totalObjectsNotDisinfected	Kaspersky Embedded Systems Security 嘗試解毒但無法成功解毒的受感染物件總數；從上次啟動"即時檔案防護"工作的時間算起
totalObjectsDeleted	Kaspersky Embedded Systems Security 刪除的受感染、可能受感染和其他物件的總數；自上一次啟動"即時檔案防護"工作的時間算起
totalObjectsNotDeleted	Kaspersky Embedded Systems Security 嘗試刪除但未成功刪除的受感染、可能受感染和其他物件的總數；從上次啟動"即時檔案防護"工作的時間算起
totalObjectsBackedUp	Kaspersky Embedded Systems Security 放入備份中的受感染和其他物件的總數；從上次啟動"即時檔案防護"工作的時間算起
totalObjectsNotBackedUp	Kaspersky Embedded Systems Security 嘗試放入備份中但未成功的受感染和其他物件的總數；從上次啟動"即時檔案防護"工作的時間算起
currentFileMonitorTaskStatus	即時檔案防護 元件的狀態： • `1` 表示元件已啟用且正在提供防護。 • `0` 表示元件未提供防護。例如：已停用、未安裝、已違反產品授權協議。

AMSI 掃描程式計數器

AMSI 掃描程式計數器

計數器	定義
currentScriptCheckerTaskStatus	AMSI 掃描程式 元件的狀態： • `1` 表示元件已啟用且正在提供防護。 • `0` 表示元件未提供防護。例如：已停用、未安裝、已違反產品授權協議。
totalScriptsProcessed	自上次啟動 AMSI 掃描程式 元件以來處理的指令碼數目。
totalInfectedlDangerousScriptsFound	自上次啟動 AMSI 掃描程式 元件以來偵測到的危險指令碼數目。
totalSuspiciousScriptsFound	自上次啟動 AMSI 掃描程式 元件以來偵測到的可疑指令碼總數。
totalScriptsBlocked	自上次啟動 AMSI 掃描程式 元件以來封鎖的指令碼總數。如果已在 **封鎖** 中啟用元件，計數器值便會變更，並且等於 totalInfectedlDangerousScriptsFound 計數器的值。

Kaspersky Embedded Systems Security SNMP 陷阱及其選項

下面匯總了 Kaspersky Embedded Systems Security 中的 SNMP TRAP 選項：

- eventThreatDetected：偵測到物件。

  TRAP 具有以下選項：

  - eventDateAndTime
  - eventSeverity
  - computerName
  - userName
  - objectName
  - threatName
  - detectType
  - detectCertainty

- eventBackupStorageSizeExceeds：已超過最大備份容量。備份中的資料總量超過 **備份大小限制為** 指定的值。Kaspersky Embedded Systems Security 繼續備份受感染的物件。

  TRAP 具有以下選項：

  - eventDateAndTime
  - eventSeverity
  - eventSource

- eventThresholdBackupStorageSizeExceeds：已超過備份區可用空間上限值。備份中的可用空間小於或等於 **可用空間的閾值 (MB)** 指定的值。Kaspersky Embedded Systems Security 繼續備份受感染的物件。

  TRAP 具有以下選項：

  - eventDateAndTime
  - eventSeverity
  - eventSource

- eventObjectNotBackuped：物件未備份。

  TRAP 具有以下選項：

  - eventSeverity
  - eventDateAndTime
  - eventSource

- objectName
- userName
- computerName
- storageObjectNotAddedEventReason

- eventBackupInternalError：備份錯誤。

  TRAP 具有以下選項：

  - eventSeverity
  - eventDateAndTime
  - eventSource
  - eventReason

- eventAVBasesOutdated：資料庫已過期。自上次執行 *更新* 工作（本機工作、群組工作或受防護裝置集工作）以來的天數。

  TRAP 具有以下選項：

  - eventSeverity
  - eventDateAndTime
  - eventSource
  - days

- eventAVBasesTotallyOutdated：資料庫嚴重過期。自上次執行 *更新* 工作（本機工作、群組工作或受防護裝置集工作）以來的天數。

  TRAP 具有以下選項：

  - eventSeverity
  - eventDateAndTime
  - eventSource
  - days

- eventApplicationStarted：應用程式已啟動。

  TRAP 具有以下選項：

  - eventSeverity
  - eventDateAndTime
  - eventSource

- eventApplicationShutdown：應用程式已停止。

TRAP 具有以下選項：

- eventSeverity
- eventDateAndTime
- eventSource

- eventCriticalAreasScanWasntPerformForALongTime：長時間未執行關鍵區域掃描。自上次完成 *關鍵區域掃描* 工作以來的天數。

  TRAP 具有以下選項：

  - eventSeverity
  - eventDateAndTime
  - eventSource
  - days

- eventLicenseHasExpired：產品授權已到期。

  TRAP 具有以下選項：

  - eventSeverity
  - eventDateAndTime
  - eventSource

- eventLicenseExpiresSoon：產品授權即將到期。計算距離產品授權到期日之前的天數。

  TRAP 具有以下選項：

  - eventSeverity
  - eventDateAndTime
  - eventSource
  - days

- eventTaskInternalError：工作完成錯誤。

  TRAP 具有以下選項：

  - eventSeverity
  - eventDateAndTime
  - eventSource
  - errorCode
  - knowledgeBaseId
  - taskName

- eventUpdateError：執行 *更新* 工作時發生錯誤。
  TRAP 具有以下選項：
  - eventSeverity
  - eventDateAndTime
  - taskName
  - updaterErrorEventReason
  - eventSource

Kaspersky Embedded Systems Security SNMP 陷阱選項說明和可能值

下面給出了 TRAP 選項及其可能值的說明：

- eventDateAndTime：事件日期和時間
- eventSeverity：重要性等級
  該選項可以採用以下值：
  - critical (1) – 重要
  - warning (2) – 警告
  - info (3) – 資訊
- userName：使用者名稱（例如，嘗試存取受感染檔案之使用者的名稱）。
- computerName：受防護裝置名稱（例如，嘗試存取受感染檔案之使用者所用受防護裝置的名稱）。
- eventSource：產生了事件的功能性元件。
  該選項可以採用以下值：
  - unknown（0）– 未知的功能元件
  - quarantine (1) – 隔離
  - backup (2) – 備份
  - reporting (3) – 工作記錄
  - updates (4) – 更新
  - realTimeProtection (5) – 即時檔案防護
  - onDemandScanning (6) – 自訂掃描

- product (7) – 整體而言與操作 Kaspersky Embedded Systems Security 而非個別元件相關的事件
- systemAudit (8) – 系統稽核記錄

- eventReason：事件觸發：什麼觸發了事件。

  該選項可以採用以下值：

  - reasonUnknown (0) – 不明原因。
  - reasonInvalidSettings (1) – 僅適用於備份和隔離事件。如果隔離或備份資料夾不可用（存取權限不足或在隔離設定中指定了無效的資料夾，例如指定了網路路徑），則會顯示。在這種情況中，Kaspersky Embedded Systems Security 會使用預設的備份或隔離資料夾。

- objectName：物件名稱（例如，偵測到含病毒之檔案的名稱）。
- threatName：根據病毒百科全書分類的物件名稱。該名稱包含在 Kaspersky Embedded Systems Security 偵測物件時回傳的全名中。您可以在工作記錄中檢視偵測到的物件的全名。
- detectType：偵測到的威脅類型。

  該選項可以採用以下值：

  - undefined（0）– 未定義
  - virware – 典型病毒與網路蠕蟲
  - trojware – 木馬
  - malware – 其他惡意應用程式
  - adware – 廣告軟體
  - pornware – 色情軟體
  - riskware – 可能被入侵者用以破壞使用者裝置或個人資料的合法程式

- detectCertainty：偵測威脅的確認等級。

  該選項可以採用以下值：

  - Suspicion（可能已感染）– Kaspersky Embedded Systems Security 偵測到物件程式碼的某個區段與已知惡意程式碼區段部分相符。
  - Sure（已感染）– Kaspersky Embedded Systems Security 偵測到物件中的某個程式碼區段與已知惡意程式碼區段完全相符。

- days：天數（例如，授權到期日前的天數）。
- errorCode：錯誤碼。
- taskName：工作名稱。
- updaterErrorEventReason：更新錯誤的原因。

該選項可以採用以下值：

- reasonUnknown(0) – 不明原因。
- reasonAccessDenied – 存取遭拒。
- reasonUrlsExhausted – 已用盡更新來源的清單。
- reasonInvalidConfig – 無效的設定檔。
- reasonInvalidSignature – 簽章無效。
- reasonCantCreateFolder – 無法建立資料夾。
- reasonFileOperError – 檔案錯誤。
- reasonDataCorrupted – 物件已損毀。
- reasonConnectionReset – 連線已重設。
- reasonTimeOut – 已超過連線逾時。
- reasonProxyAuthError – 代理驗證錯誤。
- reasonServerAuthError – 伺服器驗證錯誤。
- reasonHostNotFound – 找不到裝置。
- reasonServerBusy – 伺服器無法使用。
- reasonConnectionError – 連線錯誤。
- reasonModuleNotFound – 找不到物件。
- reasonBlstCheckFailed (16) – 檢查列入拒絕名單的金鑰時發生錯誤。可能是在更新時正在發佈資料庫更新；請在幾分鐘後重複更新。

- storageObjectNotAthreatddedEventReason：物件未置於備份區或隔離區的原因。

  該選項可以採用以下值：

  - reasonUnknown (0) – 不明原因。
  - reasonStorageInternalError – 資料庫錯誤；必須還原 Kaspersky Embedded Systems Security。
  - reasonStorageReadOnly – 資料庫唯讀；必須還原 Kaspersky Embedded Systems Security。
  - reasonStorageIOError – 輸入輸出錯誤：a) Kaspersky Embedded Systems Security 已毀損，需要還原；b) 儲存 Kaspersky Embedded Systems Security 檔案的磁碟已毀損。
  - reasonStorageCorrupted – 儲存空間已毀損；必須還原 Kaspersky Embedded Systems Security。
  - reasonStorageFull – 資料庫已滿；需要可用磁碟空間。
  - reasonStorageOpenError – 無法開啟資料庫檔案；必須還原 Kaspersky Embedded Systems Security。

- reasonStorageOSFeatureError – 某些作業系統功能不符合 Kaspersky Embedded Systems Security 的需求。
- reasonObjectNotFound – 磁碟中沒有放置於隔離區中的物件。
- reasonObjectAccessError – 使用備份 API 的權限不足；執行操作的帳戶沒有備份操作程式的權限。
- reasonDiskOutOfSpace – 磁碟空間不足。

WMI 整合

Kaspersky Embedded Systems Security 支援與 Windows Management Instrumentation (WMI) 整合：您可以使用支援 WMI 的用戶端系統，透過 Web-Based Enterprise Management (WBEM) 標準接收資料，以取得 Kaspersky Embedded Systems Security 及其元件的狀態資訊。

Kaspersky Embedded Systems Security 安裝後，會在系統中註冊專有模組以在受防護裝置上建立 Kaspersky Embedded Systems Security 命名空間。透過 Kaspersky Embedded Systems Security 命名空間可以使用 Kaspersky Embedded Systems Security 類和實例及其內容。

某些實例內容的值取決於工作類型。

*非週期性工作*是沒有時間限制的應用程式工作，可以持續執行或停止。此類工作沒有執行進度。當工作作為單個事件執行（例如，任一"即時電腦防護"工作偵測受感染物件）時，將持續記錄工作結果。此類型的工作透過卡巴斯基安全管理中心政策進行管理。

*週期性工作*是有時間限制且以百分比顯示執行進度的應用程式工作。工作結果在工作完成後產生，並表示為單個項目或變更的應用程式狀態（例如，完成的應用程式資料庫更新、為規則產生工作產生的設定檔）。在單個受防護裝置上可以同時執行多個同一類型的週期性工作（例如，三個具有不同掃描範圍的自訂掃描工作）。可以透過卡巴斯基安全管理中心將週期性工作作為群組工作進行管理。

如果在公司網路中使用工具產生 WMI 命名空間查詢並從 WMI 命名空間接收動態資料，您將能夠接收有關目前應用程式狀態的資訊（請參見下表）。

有關應用程式狀態的資訊

實例內容	描述	參數值
`ProductName`	已安裝的應用程式的名稱。	不含版本號的應用程式全名。
`ProductVersion`	已安裝應用程式的完整版本號。	應用程式完整版本號，包括內部版本號。
`InstalledPatches`	已安裝的修補程式的顯示名稱集。	為應用程式安裝的關鍵修復程式清單。
`IsLicenseInstalled`	應用程式啟動狀態。	用於啟動應用程式的金鑰的狀態。 可能的值： • `False` 尚未新增產品授權金鑰。 • `True` 已新增產品授權金鑰。
`LicenseDaysLeft`	顯示目前產品授權到期前剩餘的天數。	目前產品授權到期前剩餘的天數。 可能的非正值： • `0` 產品授權已到期。 • `-1` 無法取得目前金鑰的資訊，或指定的金鑰無法用於啟動應用程式（例如，該金鑰已根據金鑰拒絕名單遭到封鎖）。
`AVBasesDatetime`	目前病毒資料庫版本的時間戳記。	目前使用中的病毒資料庫的建立日期和時間。 如果已安裝的應用程式不使用病毒資料庫，則該欄位值為 `{Not installed}`。

實例內容	描述	參數值
`IsExploitPreventionEnabled`	弱點利用防禦 元件的狀態。	弱點利用防禦 元件的狀態。 可能的值： • `True` 弱點利用防禦 元件已啟用並提供保護。 • `False` 弱點利用防禦 元件未提供保護。例如：已停用、未安裝、已違反產品授權協議。
`ProtectionTasksRunning`	目前正在執行的一系列防護工作。	目前正在執行的防護、控制和監控工作的清單。此欄位應表示所有正在執行的非週期性工作。 如果沒有非週期性工作正在執行，則該欄位值為 `{No}`。
`IsAppControlRunning`	應用程式啟動控制 元件的狀態。	可能的值 • `True` 應用程式啟動控制 元件已啟用並提供保護。 • `False` 應用程式啟動控制 元件未提供保護。例如：已停用、未安裝、已違反產品授權協議。
`AppControlMode`	應用程式啟動控制 元件的運作模式。	可能的值： • `Active` 元件設定中指定了 **封鎖** 模式。 • `Statistics Only` 元件設定中指定了 **通知** 模式。 • `Not installed` 未安裝 應用程式啟動控制 元件。 • `Unknown` 元件已停用。
`AppControlRulesNumber`	應用程式啟動控制規則總數。	目前在 應用程式啟動控制 元件設定中指定的規則數量。
`AppControlLastBlocking`	應用程式啟動控制 元件在任一模式下上次封鎖應用程式啟動的時間戳記。	應用程式啟動控制 元件上次封鎖應用程式啟動的日期和時間。該欄位包括所有已封鎖的應用程式，不論元件的運作模式為何。 如果處理 WMI 查詢時未記錄任何應用程式啟動遭封鎖的執行個體，則該欄位值設為 `{No}`。
`PeriodicTasksRunning`	目前正在執行的一系列週期性工作。	目前正在執行的自訂掃描、更新和清單編制工作的清單。此欄位應包括所有正在執行的週期性工作。 如果目前沒有週期性工作正在執行，則該欄位值為 `{No}`。
`ConnectionState`	WMI 提供程式元件與 Kaspersky Embedded Systems Security 服務 之間的連線狀態。	有關 WMI 提供程式元件與 Kaspersky Embedded Systems Security 服務 之間連線狀態的資訊。 可能的值： • `Success` 已成功建立連線：WMI 用戶端可以接收應用程式狀態。 • `Failed. Error Code: <code>` 由於發生指定代碼的錯誤，無法建立連線。
`IsDumpingEnabled`	記憶體傾印記錄狀態。	可能的值 • `True` 記憶體傾印記錄功能已啟用。 • `False` 記憶體傾印記錄功能已停用。
`DumpsFolder`	用於儲存傾印檔案的資料夾。	完整資料夾路徑。 如果已停用傾印記錄，則此欄位為空白。
`IsTracingEnabled`	應用程式追蹤狀態。	可能的值 • `True` 應用程式追蹤已啟用。 • `False` 應用程式追蹤已停用。
`TraceFolder`	用於儲存追蹤檔案的資料夾。	完整資料夾路徑。 如果已停用應用程式追蹤，則此欄位為空白。

實例內容	描述	參數值
AllTasksState	所有工作的狀態。	有關工作狀態的資訊，格式為 {<profile-name_1>, <profile-type_1>, <profile-state_1>,...<profile-name_N>, <profile-type_N>, <profile-state_N>}，其中 profile-name 是工作名稱，profile-type 是工作類型，而 profile-state 是工作的目前狀態。 可能的狀態值： • not started 工作尚未啟動。 • running 工作正在執行。 • running ma 工作正在執行，但執行期間發生故障。 • paused 工作已暫停。 • stopped 工作已停止。 • completed 工作已成功完成。 • failed 工作因錯誤而結束。 • disabled 工作已停用且無法執行。 • starting 工作正在啟動。 • pausing 工作正在暫停。 • stopping 工作正在停止。 • <unknown> 無法判斷狀態。
IsDevControlRunning	裝置控制 元件的狀態。	可能的值： • True 裝置控制 元件已啟用並提供保護。 • False 裝置控制 元件未提供保護。例如：已停用、未安裝、已違反產品授權協議。
IsKSNRunning	卡巴斯基安全網路 元件的狀態。	可能的值： • True 卡巴斯基安全網路 元件已啟用並提供保護。 • False 卡巴斯基安全網路 元件未提供保護。例如：已停用、未安裝、已違反產品授權協議。
IsOASRunning	即時檔案防護 元件的狀態。	可能的值： • True 即時檔案防護 元件已啟用並提供保護。 • False 即時檔案防護 元件未提供保護。例如：已停用、未安裝、已違反產品授權協議。

此資料表示實例屬性 KasperskySecurity_ProductInfo.ProductName=Kaspersky Embedded Systems Security，其中：

- KasperskySecurity_ProductInfo 是 Kaspersky Embedded Systems Security 類別的名稱。
- .ProductName=Kaspersky Embedded Systems Security 是 Kaspersky Embedded Systems Security 的索引鍵屬性。

此類別會在 ROOT\Kaspersky\Security 命名空間中具現化。

Managed Detection and Response

Kaspersky Endpoint Systems Security 支援與 Managed Detection and Response 解決方案整合。

Kaspersky Managed Detection and Response（也稱為 MDR）為難以找到專業知識和人員或內部資源有限的組織提供全天候保護，抵禦不斷增長、繞過自動化安全屏障的威脅。與市場上的類似產品不同，這項服務利用經過驗證的有效定向攻擊研究記錄，確保持續防禦即使是最複雜的威脅。該服務有助於提高企業應對網路威脅的韌性，同時釋放現有資源，使其能夠專注於其他工作。

MDR 會使用從端點和機學習收到的遙測資料。MDR 會將事件資料傳送給卡巴斯基專家。專家然後可以處理事件，並且，例如，新增新項目至病毒資料庫。或者，專家可以簽發事件處理建議，並且，例如，建議從網路中隔離電腦。如欲瞭解該解決方案如何工作的詳細資訊，請參閱 Kaspersky Managed Detection and Response 說明。

配置 MDR 整合

與 Kaspersky Managed Detection and Response 整合包括以下步驟：

1. **安裝Managed Detection and Response元件**

   為了使 Kaspersky Embedded Systems Security 與 Managed Detection and Response 解決方案整合，使用了 Managed Detection and Response元件。若要使用安裝套件設定或安裝精靈安裝此元件，或透過在 Windows 控制台中變更應用程式元件集來安裝此元件，請選取 **Managed Detection and Response**。您也可以使用 *變更 Kaspersky Embedded Systems Security 元件* 工作安裝此元件。

   > 若要使用 *變更 Kaspersky Embedded Systems Security 元件* 工作安裝 Managed Detection and Response 元件且不重新啟動電腦，您需要在工作設定中停用 **檢查不相容的協力廠商應用程式** 選項。

2. **配置卡巴斯基私有安全網路**

   從 2025 年 7 月的更新開始，Managed Detection and Response 解決方案支援在沒有 KPSN 設定檔的情況下運行。如欲瞭解 MDR 解決方案如何使用卡巴斯基安全網路的詳細資訊，請參閱 Kaspersky Managed Detection and Response 說明。

   如果您的配置不符合在沒有 KPSN 設定檔的情況下執行的要求，請在管理伺服器屬性中上傳 KPSN 設定檔。KPSN 設定檔位於 MDR 設定檔的 ZIP 壓縮檔案中。您也可以使用 命令列上傳 KPSN 設定檔。

   有關配置卡巴斯基私有安全網路的詳細資訊，請參閱 卡巴斯基安全管理中心說明。

3. **啟動 Kaspersky Managed Detection and Response**

   要在 Kaspersky Embedded Systems Security 中啟動 Managed Detection and Response 解決方案，您需要單獨的 Kaspersky Managed Detection and Response for Embedded Systems Security Add-on 產品授權。如欲瞭解如何啟動該解決方案的詳細資訊，請參閱 Kaspersky Managed Detection and Response 說明。

   > Kaspersky Embedded Systems Security 不支援 MDR 設定檔（BLOB 檔案）。所有資產都將放置在根租戶中。

4. **啟用 Managed Detection and Response 元件**

如何在卡巴斯基安全管理中心管理主控台中啟用 Managed Detection and Response 元件

1. 在卡巴斯基安全管理中心管理主控台樹狀目錄中，選取**政策**。
2. 選擇必要的政策並點擊以開啟政策內容。
3. 選擇 **遙測資料收集伺服器** 部分。
4. 在"**Managed Detection and Response**"塊中，點擊"**設定**"按鈕。
   開啟"**Managed Detection and Response**"視窗。
5. 選擇"**Managed Detection and Response**"核取方塊。
6. 儲存變更。

如何在網頁主控台中啟用 Managed Detection and Response 元件

1. 在網頁主控台的主視窗中，選擇**資產管理 → 政策**。
2. 點擊 Kaspersky Embedded Systems Security 政策的名稱。
   政策內容視窗將開啟。
3. 選擇"**應用程式設定**"標籤。
4. 選擇 **遙測資料收集伺服器** 部分。
5. 在"**Managed Detection and Response**"塊中，點擊"**設定**"按鈕。
   開啟"**Managed Detection and Response**"視窗。
6. 選擇"**已停用 Managed Detection and Response**"核取方塊。
7. 儲存變更。

如何在應用程式主控台中啟用 Managed Detection and Response 元件

1. 在管理主控台樹狀目錄中，選擇**遙測資料收集伺服器 → Managed Detection and Response**資料夾。
2. 在結果窗格中點擊"**內容**"連結。
   Managed Detection and Response視窗將在**一般**頁簽上開啟。
3. 選擇"**Managed Detection and Response**"核取方塊。
4. 儲存變更。

您也可以使用命令列啟用 Managed Detection and Response 元件。

5. **配置應用程式的其他元件以接收遙測資料**

您必須啟用延伸以下元件才能使 Kaspersky Managed Detection and Response 正常工作：

- 卡巴斯基安全網路（延伸模式）。
- 即時檔案防護
- AMSI 掃描程式

- 行為偵測。
- 弱點利用防禦
- 網路威脅防護
- 防火牆
- 按需掃描

若要透過卡巴斯基安全管理中心網頁主控台讓 Kaspersky Managed Detection and Response 和管理伺服器一起工作，您必須也建立一個新的安全連線，一個*背景連線*。Kaspersky Managed Detection and Response 提示您在部署解決方案時建立一個背景連線。確保背景連線已建立。

在卡巴斯基安全管理中心網頁主控台中建立背景連線

1. 在網頁主控台的主視窗中，選擇**設定** → **整合**。
2. 轉到**"整合"**區域。
3. 開啟**"整合的背景連線 已啟用"**開關。
4. 儲存變更。

透過命令列管理 Kaspersky Embedded Systems Security

您可以透過命令列管理和維護 Kaspersky Embedded Systems Security。

若要透過命令列管理 Kaspersky Embedded Systems Security：

1. 在裝置上，以本機管理員權限執行命令列解釋器（例如 cmd.exe）。
2. 使用 cd 指令導覽到 kavshell.exe 檔案所在的資料夾。

   範例

   ```
   cd C:\Program Files (x86)\Kaspersky Lab\Kaspersky Embedded Systems Security.4.1.0
   ```

   您也可以在應用程式安裝階段將可執行檔路徑新增至 %PATH% 系統變數並執行命令，而無需導覽至應用程式資料夾。
3. 使用以下模板來執行命令：

   ```
   KAVSHELL <command> [options]
   ```

   可以執行 `KAVSHELL HELP` 指令來檢視用於管理應用程式的指令清單。要閱讀特定指令的語法，請輸入 `KAVSHELL HELP <command>`。

因此，Kaspersky Embedded Systems Security 會執行指定的動作。

APPCONTROL.匯入應用程式啟動控制規則

`KAVSHELL APPCONTROL` 命令可從 XML 檔案匯入 應用程式啟動控制 元件的規則，以及從該元件的規則清單中移除所有規則。若要產生包含規則的 XML 檔案，您可以使用本機或群組 *應用程式啟動控制規則產生器* 工作。

指令語法

```
KAVSHELL APPCONTROL /APPEND <path to XML file> | /REPLACE <path to XML file> | /MERGE <path to XML file> | /CLEAR
/PWD:<password> [/LOGIN:<user name>]
```

命令選項

參數	描述
`/APPEND | /REPLACE | /MERGE | /CLEAR`	必需參數。 從指定的 XML 檔案匯入應用程式啟動控制規則： • `/APPEND` 會將檔案中的所有規則新增至元件的規則清單。如果規則已存在於清單中，則會重複新增。 • `/REPLACE` 會以檔案中的規則取代元件的整個現有規則清單。 • `/MERGE` 會將檔案中的規則與現有規則清單合併。如果規則已存在於清單中，則不會重複新增。 若要移除 應用程式啟動控制 元件的所有規則，請使用 `/CLEAR`。
`<path to XML file>`	傳遞 `/APPEND`、`/REPLACE` 和 `/MERGE` 時為必填。 含有規則的 XML 檔案完整路徑。

參數	描述
`/PWD:<password>`	必需參數。 KLAdmin 使用者帳戶或具有足夠權限之使用者帳戶的密碼。 如果未指定此選項，應用程式將在下一行提示您輸入密碼。
`/LOGIN:<user name>`	可選參數。 具有足夠權限的使用者帳戶名稱。 如果未指定此選項，應用程式將在下一行提示您輸入使用者名稱。 如果您已輸入 KLAdmin 密碼，則無需輸入此值。

範例

```
KAVSHELL APPCONTROL /APPEND c:\rules\appctrlrules.xml /PWD:p@ssw0rd
```

APPCONTROL /CONFIG。設定 應用程式啟動控制 元件

`KAVSHELL APPCONTROL /CONFIG` 命令可讓您管理 應用程式啟動控制 元件的設定。

指令語法

```
KAVSHELLKAVSHELL APPCONTROL /CONFIG [/MODE:<applyrules|statistics>] [/DLL:<no|yes>] [/SAVETOFILE:<path to XML file>] [/SDC] [/CLEARSDC] /PWD:<password> [/LOGIN:<user name>]
```

命令選項

參數	描述
`/MODE:<applyrules|statistics>`	可選參數。 應用程式啟動控制 元件的運作模式： • `applyrules`：Kaspersky Embedded Systems Security 使用應用程式啟動控制規則來控制應用程式的啟動。 • `statistics`（預設值）：Kaspersky Embedded Systems Security 允許啟動所有應用程式。在此模式下，應用程式只會記錄所有應用程式啟動的相關資訊、套用至已啟動應用程式的規則，以及元件以 `applyrules` 模式執行時原本會執行的動作。
`/DLL:<no|yes>`	可選參數。 DDL 載入監控： • no（預設值）：Kaspersky Embedded Systems Security 不會使用應用程式啟動控制規則控制 DLL 模組的載入。將允許 DLL 模組載入。 • `yes`：如果啟用此功能，Kaspersky Embedded Systems Security 將允許或拒絕使用應用程式啟動控制規則載入 DLL 模組。
`/SAVETOFILE:<path to XML file>`	可選參數。 將應用程式啟動控制規則清單儲存至指定的 XML 檔案。
`/SDC`	可選參數。 將應用程式分發快取匯出至 `/SAVETOFILE` 選項指定的 XML 組態檔案。
`/CLEARSDC`	可選參數。 刪除軟體分發快取。
`/PWD:<password>`	必需參數。 KLAdmin 使用者帳戶或具有足夠權限之使用者帳戶的密碼。 如果未指定此選項，應用程式將在下一行提示您輸入密碼。

/LOGIN:<user name>	可選參數。 具有足夠權限的使用者帳戶名稱。 如果未指定此選項，應用程式將在下一行提示您輸入使用者名稱。 如果您已輸入 KLAdmin 密碼，則無需輸入此值。

範例

```
KAVSHELL APPCONTROL /CONFIG /mode:applyrules /dll:<no> /savetofile:c:\appcontrol\config.xml /PWD:p@ssw0rd
```

APPCONTROL /GENERATE。應用程式啟動控制規則產生器

您可以使用 `KAVSHELL APPCONTROL /GENERATE` 命令管理 *應用程式啟動控制規則產生器* 工作。

指令語法

```
KAVSHELL APPCONTROL /GENERATE <path to folder> | /SOURCE:<path to file with folders list> [/MASKS:<edms>]
[/RUNAPP] [/RULES:<ch|cp|h>] [/STRONG] [/USER:<user or group of users>] [/EXPORT:<path to XML file>] [/IMPORT:
<a|r|m>] [/PREFIX:<prefix for rules names>] [/UNIQUE] [/ADDPATH] /PWD:<password> [/LOGIN:<user name>]
```

命令選項

參數	描述
<path to folder>	若未傳遞 /SOURCE，則為必填項。 包含可執行檔、MSI 套件和腳本的資料夾路徑。若啟動指定資料夾中指定類型的檔案，工作將建立允許規則。
/SOURCE:<path to file with folders list>	若未傳遞 <path to folder>，則為必填項。 TXT 檔案的路徑，其中包含具有可執行檔之資料夾的清單，系統將為這些可執行檔自動產生允許規則。
/MASKS:<edms>	可選參數。 系統將為其自動產生允許規則的可執行檔副檔名。 您可以將具有以下副檔名的檔案納入工作範圍： • e（適用於 EXE 檔案） • d（適用於 DLL 檔案） • m（適用於 MSI 檔案） • s（適用於腳本）
/RUNAPP	可選參數。 根據執行中的應用程式建立允許規則。
/RULES:<ch|cp|h>	可選參數。 工作建立應用程式啟動控制允許規則時將套用的條件： • ch 使用數位憑證。如果憑證缺失，則使用 SHA256 雜湊。 • cp 使用數位憑證。如果憑證缺失，則使用可執行檔路徑。 • h 使用 SHA256 雜湊。
/STRONG	可選參數。 使用檔案數位憑證的主旨和指紋，作為觸發應用程式啟動控制允許規則的條件。 與 /RULES:<ch|cp> 參數搭配使用。
/USER:<user or group of users>	可選參數。 將套用規則的使用者或使用者群組名稱。
/EXPORT:<path to XML file>	可選參數。 要用來儲存指定規則的 XML 檔案路徑和名稱。

/IMPORT:<a|r|m>	可選參數。 將產生的規則匯入應用程式啟動控制規則清單： • a 會將檔案中的所有規則新增至元件的規則清單。如果規則已存在於清單中，則會重複新增。 • r 會以檔案中的規則取代元件的整個現有規則清單。 • m 會將檔案中的規則與現有規則清單合併。如果規則已存在於清單中，則不會重複新增。
/PREFIX:<prefix for rules names>	指定應用程式啟動控制允許規則名稱的首碼。
/UNIQUE	將受保護裝置的相關資訊新增至規則，並依據該資訊產生應用程式啟動控制允許規則。
/ADDPATH	將可執行檔的路徑新增至根據雜湊值產生的規則。
/PWD:<password>	必需參數。 KLAdmin 使用者帳戶或具有足夠權限之使用者帳戶的密碼。 如果未指定此選項，應用程式將在下一行提示您輸入密碼。
/LOGIN:<user name>	可選參數。 具有足夠權限的使用者帳戶名稱。 如果未指定此選項，應用程式將在下一行提示您輸入使用者名稱。 如果您已輸入 KLAdmin 密碼，則無需輸入此值。

範例

```
KAVSHELL KAVSHELL APPCONTROL /GENERATE c:\folder /masks:edms /export:c\rules\appctrlrules.xml /PWD:p@ssw0rd
```

CONFIG.支援 AM-PPL 技術

KAVSHELL CONFIG 命令可讓您使用 AM-PPL 技術來管理應用程式處理程序保護。

若要讓命令正常運作，您需要停用自我防護機制。

指令語法

```
KAVSHELL CONFIG /PPL:<ON|OFF> /PWD:<password> [/LOGIN:<user name>]
```

命令選項

參數	描述
/PPL:<ON|OFF>	必需參數。 啟用或停用 AM-PPL 技術支援： • ON – 啟用對 AM-PPL 技術的支援。 • OFF – 停用對 AM-PPL 技術的支援。
/PWD:<password>	必需參數。 KLAdmin 使用者帳戶或具有足夠權限之使用者帳戶的密碼。 如果未指定此選項，應用程式將在下一行提示您輸入密碼。
/LOGIN:<user name>	可選參數。 具有足夠權限的使用者帳戶名稱。 如果未指定此選項，應用程式將在下一行提示您輸入使用者名稱。 如果您已輸入 KLAdmin 密碼，則無需輸入此值。

範例

```
KAVSHELL CONFIG /PPL:ON
KAVSHELL CONFIG /PPL:OFF
```

DEVCONTROL。匯入裝置控制規則

KAVSHELL DEVCONTROL 命令可讓您從 *裝置控制規則產生器* 命令產生的 XML 檔案匯入 裝置控制 元件的規則，或移除該元件規則清單中的所有規則。

指令語法

```
KAVSHELL DEVCONTROL /APPEND <path to XML file> | /REPLACE <path to XML file> | /MERGE <path to XML file> | /CLEAR
/PWD:<password> [/LOGIN:<user name>]
```

命令選項

參數	描述
/APPEND | /REPLACE | /MERGE | /CLEAR	必需參數。 從指定的 XML 檔案匯入裝置控制規則： • /APPEND 會將檔案中的所有規則新增至元件的規則清單。如果規則已存在於清單中，則會重複新增。 • /REPLACE 會以檔案中的規則取代元件的整個現有規則清單。 • /MERGE 會將檔案中的規則與現有規則清單合併。如果規則已存在於清單中，則不會重複新增。 若要移除 裝置控制 元件的所有規則，請使用 /CLEAR。
<path to XML file>	傳遞 /APPEND、/REPLACE 和 /MERGE 時為必填。 含有規則的 XML 檔案完整路徑。
/PWD:<password>	必需參數。 KLAdmin 使用者帳戶或具有足夠權限之使用者帳戶的密碼。 如果未指定此選項，應用程式將在下一行提示您輸入密碼。
/LOGIN:<user name>	可選參數。 具有足夠權限的使用者帳戶名稱。 如果未指定此選項，應用程式將在下一行提示您輸入使用者名稱。 如果您已輸入 KLAdmin 密碼，則無需輸入此值。

範例

```
KAVSHELL DEVCONTROL /MERGE c:\rules\appctrlrules.xml /PWD:p@ssw0rd
```

DUMP。記錄記憶體傾印

KAVSHELL DUMP 命令可讓您啟用或停用記憶體傾印。

指令語法

```
KAVSHELL DUMP </ON /F:<dump_file_folder> | /SNAPSHOT /F:<dump_file_folder> /P:<process_ID> | /OFF > [/PWD:
<password>] [/LOGIN:<user name>]
```

命令選項

參數	描述
/ON	啟用建立傾印檔案。
/F:<dump_file_folder>	必需參數。 設定儲存傾印檔案的資料夾。
/SNAPSHOT	建立具有指定 ID 之執行中處理程序的記憶體傾印。傾印檔案會儲存至 /F 選項所指定的資料夾。

/P:<process_ID>	若傳遞 /SNAPSHOT，則此項為必填。 設定處理程序 ID。您可以使用 tasklist 命令查詢處理程序 ID。
/OFF	停用建立傾印檔案。
/PWD:<password>	可選參數。 KLAdmin 使用者帳戶或具有足夠權限之使用者帳戶的密碼。 如果未指定此選項，應用程式將在下一行提示您輸入密碼。
/LOGIN:<user name>	可選參數。 具有足夠權限的使用者帳戶名稱。 如果未指定此選項，應用程式將在下一行提示您輸入使用者名稱。 如果您已輸入 KLAdmin 密碼，則無需輸入此值。

範例

```
KAVSHELL DUMP /ON /F:"C:\Dumps and others"
KAVSHELL DUMP /SNAPSHOT /F:"C:\Dumps and others" /P:1234 /PWD:p@ssw0rd
KAVSHELL DUMP /OFF
```

EXITPOLICY。停用裝置上的政策

KAVSHELL EXITPOLICY 命令會停用裝置上的卡巴斯基安全管理中心政策。停用政策後，所有 Kaspersky Embedded Systems Security 設定都可供設定，包括政策中以閉合掛鎖 (🔒) 標示的設定。

指令語法

```
KAVSHELL EXITPOLICY [/PWD:<password>] [/LOGIN:<user name>]
```

命令選項

參數	描述
/PWD:<password>	可選參數。 KLAdmin 使用者帳戶或具有足夠權限之使用者帳戶的密碼。 如果未指定此選項，應用程式將在下一行提示您輸入密碼。
/LOGIN:<user name>	可選參數。 具有足夠權限的使用者帳戶名稱。 如果未指定此選項，應用程式將在下一行提示您輸入使用者名稱。 如果您已輸入 KLAdmin 密碼，則無需輸入此值。

範例

```
KAVSHELL EXITPOLICY /PWD:p@ssw0rd
```

EXPORT。匯出應用程式設定

KAVSHELL EXPORT 命令可讓您從 XML 格式的設定檔匯出 Kaspersky Embedded Systems Security 設定。可以將所有應用程式設定或僅將單個元件的設定儲存到設定檔。

指令語法

```
KAVSHELL EXPORT <profile> <file name> [/LOGIN:<user name>] [/PWD:<password>]
```

命令選項

參數	描述
`<profile>`	必需參數。 輸入要匯出的設定檔名稱。設定檔是 Kaspersky Embedded Systems Security 的元件、工作或功能。您可以執行 `KAVSHELL EXPORT /?` 指令來檢視可用設定檔清單。 若要匯出所有應用程式設定，請指定 `product` 設定檔。
`<file name>`	必需參數。 指定用於匯出設定檔設定的 XML 格式檔案名稱。您也可以指定檔案路徑。 範例: `C:\Test\settings.xml` • 如果命令中只指定檔案名稱，應用程式會嘗試將檔案放置在應用程式的安裝資料夾中。如果已啟用應用程式的自我防護機制，匯出將會失敗，因為應用程式的自我防護功能會封鎖在應用程式資料夾中建立新檔案。若要匯出應用程式設定，請指定檔案路徑。
`/LOGIN:<user name>`	可選參數。 具有足夠權限的使用者帳戶名稱。 如果未指定此選項，應用程式將在下一行提示您輸入使用者名稱。 如果您已輸入 KLAdmin 密碼，則無需輸入此值。
`/PWD: <password>`	可選參數。 KLAdmin 使用者帳戶或具有足夠權限之使用者帳戶的密碼。 如果未指定此選項，應用程式將在下一行提示您輸入密碼。

範例

```
KAVSHELL EXPORT product C:\Test\settings.xml /LOGIN:Admin /PWD:p@ssw0rd
```

FBRESET。清除 iSwift 資料庫

Kaspersky Embedded Systems Security 可使用 iSwift 技術，讓應用程式避免重新掃描自上次掃描後未修改的檔案。`KAVSHELL FBRESET` 命令會清除用於儲存已掃描且未受感染檔案相關資訊的資料庫。清除資料庫後，Kaspersky Embedded Systems Security 會掃描其首次存取的所有檔案。

指令語法

```
KAVSHELL FBRESET
```

FIM /BASELINE。基於基線的系統完整性監控

您可以使用 `KAVSHELL FIM /BASELINE` 命令管理 *基於基線的系統完整性監控* 工作。

```
KAVSHELL FIM /BASELINE [[/CREATE {<monitoring scope>|/L:<path to TXT file containing the list of monitoring areas>}] [/MD5 | /SHA256] [/SF] [/W:<file name>] [/ANSI]] [/SCAN {[/BL:<id baseline>] | [/ALIAS:<existing task id>]} [/W:<file name>] [/ANSI]] [/CLEAR [/BL:<id baseline>] | [/ALIAS:<existing task id>]] [/SHOW [[/BL:<id baseline>] | [/ALIAS:<existing task id>]]] [/EXPORT:<path to folder>[[/BL:<id baseline>] | [/ALIAS:<existing task id>]]] [/PWD:<password>] [/LOGIN:<user name>]
```

命令選項

參數	描述
`/CREATE`	啟動新的 *基於基線的系統完整性監控* 任務，以建立系統狀態的快照。

/SCAN	使用系統快照 ID 或現有任務的替代名稱執行 *基於基線的系統完整性監控* 任務。
/CLEAR	刪除基準。指定系統快照的 ID，或建立該快照之任務的替代名稱。 如果未指定替代任務名稱或快照 ID，應用程式將刪除所有快照。
/EXPORT	將所有快照的資料或使用 /BL 選項指定之快照的資料，以 TXT 檔案匯出至指定資料夾。
/SHOW	顯示所有系統狀態快照的資料，或由 /BL 選項指定之快照的資料。
<monitoring scope>	若未指定 /L，則為必要項目。 設定任務的監控範圍。您可以使用 ? 和 * 字元輸入遮罩。
/L	若未指定 <monitoring scope>，則為必要項目。 可讓您指定包含監控範圍清單之 TXT 檔案的路徑。
/MD5	可選參數。 無法與 /SHA256 參數搭配使用。 設定用於計算總和檢查碼的 MD5 演算法。 預設使用 MD5 演算法。
/SHA256	可選參數。 無法與 /MD5 參數搭配使用。 設定用於計算總和檢查碼的 SHA256 演算法。 預設使用 MD5 演算法。
/SF	可選參數。 將所有子資料夾納入任務的監控範圍。 預設不會將子資料夾納入監控範圍。
/ALIAS:<existing task id>	若未指定 /BL，則為必要項目。 任務別名。 您可以使用 KAVSHELL FIM /BASELINE /SHOW 命令查明任務別名。
/BL:<id baseline>	若未指定 /ALIAS，則為必要項目。 設定系統快照的 ID。 您可以使用 KAVSHELL FIM /BASELINE /SHOW 命令查明基準 ID。
/PWD:<password>	可選參數。 KLAdmin 使用者帳戶或具有足夠權限之使用者帳戶的密碼。 如果未指定此選項，應用程式將在下一行提示您輸入密碼。
/LOGIN:<user name>	可選參數。 具有足夠權限的使用者帳戶名稱。 如果未指定此選項，應用程式將在下一行提示您輸入使用者名稱。 如果您已輸入 KLAdmin 密碼，則無需輸入此值。

範例

```
KAVSHELL FIM /BASELINE /CREATE "c:\program files\*" /MD5 /SF
KAVSHELL FIM /BASELINE /CREATE /L:c:\programdata\mytask\list.txt /ALIAS:SystemIntegrityMonitorOnDemandTask$001
/MD5 /SF
KAVSHELL FIM /BASELINE /SCAN /ALIAS:SystemIntegrityMonitorOnDemandTask$001
KAVSHELL FIM /BASELINE /EXPORT:c:\programdata\mytask\baselines\
```

HELP.顯示指令說明

要顯示所有可用的 Kaspersky Embedded Systems Security 指令清單，請執行以下任一指令：

```
KAVSHELL
KAVSHELL HELP
KAVSHELL /?
```

要顯示指令說明及其語法，請執行以下任一指令：

```
KAVSHELL HELP <command>
KAVSHELL <command> /?
```

範例

```
KAVSHELL HELP SCAN
```

IMPORT。匯入應用程式設定

`KAVSHELL IMPORT` 命令可讓您從 XML 格式的設定檔匯入 Kaspersky Embedded Systems Security 設定。您可使用 `KAVSHELL EXPORT` 命令建立設定檔。

指令語法

```
KAVSHELL IMPORT <file_name> /PWD:<password> [/LOGIN:<user name>]
```

命令選項

參數	描述
`<file name>`	必需參數。 指定要從中匯入設定的 XML 檔案完整路徑，包括檔案名稱和副檔名。
`/PWD:<password>`	必需參數。 KLAdmin 使用者帳戶或具有足夠權限之使用者帳戶的密碼。 如果未指定此選項，應用程式將在下一行提示您輸入密碼。
`/LOGIN:<user name>`	可選參數。 具有足夠權限的使用者帳戶名稱。 如果未指定此選項，應用程式將在下一行提示您輸入使用者名稱。 如果您已輸入 KLAdmin 密碼，則無需輸入此值。

範例

```
KAVSHELL IMPORT C:\Test\settings.xml /PWD:p@ssw0rd
```

指令返回值：

- 0：操作成功完成。
- -2：未執行服務。
- -3：執行指令的權限不足。
- -4：找不到物件。
- -9：嘗試以其他使用者帳戶執行受管理裝置失敗。
- -99：未知錯誤。
- -501：作業成功，但執行期間發生錯誤或警告（例如，應用程式未匯入某些元件的設定）。

- -502：匯入檔案遺失或其格式無法辨識。
- -503：設定不相容（設定檔是從其他應用程式或較新且不相容的 Kaspersky Embedded Systems Security 版本匯出的）。

KSN。使用 KSN/KPSN

您可以使用 `KAVSHELL KSN` 命令選擇用來判定檔案或網站信譽的卡巴斯基解決方案。Kaspersky Embedded Systems Security 支援以下用於使用 Kaspersky 信譽資料庫的基礎結構解決方案：

- *卡巴斯基安全網路 (KSN)* 是大多數 Kaspersky 應用程式使用的解決方案。KSN 參與者從卡巴斯基接收資訊，並向 Kaspersky 傳送使用者電腦上偵測到的物件的資訊，以便 Kaspersky 分析人員進行額外分析，並包括在信譽和統計資料庫中。
- *卡巴斯基安全網路 (KSN)* 是讓承載 Kaspersky Embedded Systems Security 或其他 Kaspersky 應用程式的電腦的使用者獲得卡巴斯基信譽資料庫以及其他統計資料的存取權限的解決方案，無需從他們自己的電腦向卡巴斯基傳送資料。KPSN 專為因以下任一原因無法參與卡巴斯基安全網路的公司客戶所設計：
  - 本機工作站未連線網際網路。
  - 法律禁止或公司安全政策限制將任何資料傳輸到國家/地區外部或公司 LAN 外部。

指令語法

```
KAVSHELL KSN /GLOBAL|/PRIVATE <settings-file> /PWD:<password> [/LOGIN:<user name>]
```

命令選項

參數	描述
`/GLOBAL`	切換為使用卡巴斯基安全網路。
`/PRIVATE <settings-file>`	切換為使用卡巴斯基私人安全網路。 指定包含卡巴斯基私人安全網路設定的設定檔名稱。此檔案具有 .PKCS7 或 .PEM 副檔名。
`/PWD:<password>`	必需參數。 KLAdmin 使用者帳戶或具有足夠權限之使用者帳戶的密碼。 如果未指定此選項，應用程式將在下一行提示您輸入密碼。
`/LOGIN:<user name>`	可選參數。 具有足夠權限的使用者帳戶名稱。 如果未指定此選項，應用程式將在下一行提示您輸入使用者名稱。 如果您已輸入 KLAdmin 密碼，則無需輸入此值。

範例

```
KAVSHELL KSN /GLOBAL /PWD:p@ssw0rd
KAVSHELL KSN /PRIVATE c:\settings.pkcs7 /PWD:p@ssw0rd
```

LICENSE。應用程式啟動

可使用 `KAVSHELL LICENSE` 指令管理 Kaspersky Embedded Systems Security 金鑰和啟動碼。

指令語法

```
KAVSHELL LICENSE [/ADD:<key_file | activation code> [/R]|/DEL:<license key serial number>|/REFRESH:<license id>]
/PWD:<password> [/LOGIN:<user name>]
```

命令選項

參數	描述
未指定選項。	該指令會回傳以下相關的安裝產品授權資訊： • 金鑰。 • 產品授權類型（正式版）。 • 與金鑰檔案相關聯的產品授權的有效期限。 • 產品授權檔案狀態（啟動或備用）。如果狀態為 *，此金鑰會安裝為備用金鑰。
`/ADD:<key_file | activation code>`	使用金鑰檔案啟動 Kaspersky Embedded Systems Security。如果應用程式已啟動，則該金鑰將作為備用金鑰新增。
`/R`	如果傳遞 `/R` 選項，則會將啟動碼或金鑰新增為備用啟動碼或金鑰。
`/DEL:<license key serial number>`	刪除指定的金鑰或啟動碼。
`/REFRESH:<license id>`	更新指定產品授權的狀態。
`/PWD:<password>`	必需參數。 KLAdmin 使用者帳戶或具有足夠權限之使用者帳戶的密碼。 如果未指定此選項，應用程式將在下一行提示您輸入密碼。
`/LOGIN:<user name>`	可選參數。 具有足夠權限的使用者帳戶名稱。 如果未指定此選項，應用程式將在下一行提示您輸入使用者名稱。 如果您已輸入 KLAdmin 密碼，則無需輸入此值。

指令返回值：

- 0：操作成功完成。
- -2：未執行服務。
- -3：執行指令的權限不足。
- -4：找不到指定序號的金鑰。
- -5：未知錯誤。
- -6：操作無效（已新增金鑰）。
- -99：未知錯誤。
- -301：產品授權無效。
- -303：產品授權適用於其他應用程式。

MDR。設定託管式偵測與回應整合

`KAVSHELL MDR` 命令可讓您設定 Kaspersky Embedded Systems Security 與託管式偵測與回應解決方案的整合。

指令語法

```
KAVSHELL MDR /ENABLE [/PWD:<password>] [/LOGIN:<user name>] | /DISABLE [/PWD:<password>] [/LOGIN:<user name>] |
/SHOW
```

命令選項

參數	描述
`MDR /<enable|disable|show>`	必需參數。 可讓您啟用、停用或檢視 Managed Detection and Response 元件的目前設定。
`/PWD:<password>`	可選參數。 KLAdmin 使用者帳戶或具有足夠權限之使用者帳戶的密碼。 如果未指定此選項，應用程式將在下一行提示您輸入密碼。
`/LOGIN:<user name>`	可選參數。 具有足夠權限的使用者帳戶名稱。 如果未指定此選項，應用程式將在下一行提示您輸入使用者名稱。 如果您已輸入 KLAdmin 密碼，則無需輸入此值。

範例

```
KAVSHELL MDR /ENABLE /PWD:p@ssw0rd
KAVSHELL MDR /DISABLE /PWD:p@ssw0rd
KAVSHELL MDR /SHOW
```

OMSINFO。建立包含應用程式資訊的 JSON 檔案

`KAVSHELL OMSINFO` 指令可建立包含應用程式目前狀態及偵測到的威脅相關資訊的 JSON 檔案，您隨後可將該檔案上傳至監控系統。

指令語法

```
KAVSHELL OMSINFO <oms_info_json_file_name>
```

命令選項

參數	描述
`<oms_info_json_file_name>`	JSON 檔案的完整路徑，包括其名稱和副檔名。

範例

```
KAVSHELL OMSINFO "C:\Dumps and others\omsinfo.json"
```

密碼。對 Kaspersky Embedded Systems Security 功能進行受密碼防護的存取

`KAVSHELL PASSWORD` 命令可讓您管理對 Kaspersky Embedded Systems Security 功能進行的受密碼防護存取。如果啟用此功能，應用程式會在刪除、修改或還原應用程式以及 在命令列上執行可能會降低裝置的防護等級的操作時請求使用者名稱和密碼。

指令語法

```
KAVSHELL PASSWORD /SET /NEW:<new password> | /RESET /PWD:<password> [/LOGIN:<user name>]
```

命令選項

參數	描述
`/SET`	啟用密碼提示以確認關鍵操作。

`/NEW:<new password>`	若傳遞 `/SET`，則此項為必填。
	設定新密碼。
	建立密碼時，建議符合以下條件：
	• 密碼不包含帳戶名稱或電腦名稱。
	• 密碼長度至少為 8 個字元。
	• 密碼包含的字元與以下至少三個類別相符：
	  • 大寫拉丁字母 (A-Z)
	  • 小寫拉丁字母 (a-z)
	  • 數字 (0-9)
	  • 感嘆號 (!)、美元符號 ($)、英鎊符號 (#) 和百分號 (%)

`/RESET`	停用用於確認關鍵操作的密碼提示。
`/PWD:<password>`	必需參數。 KLAdmin 使用者帳戶或具有足夠權限之使用者帳戶的密碼。 如果未指定此選項，應用程式將在下一行提示您輸入密碼。
`/LOGIN:<user name>`	可選參數。 具有足夠權限的使用者帳戶名稱。 如果未指定此選項，應用程式將在下一行提示您輸入使用者名稱。 如果您已輸入 KLAdmin 密碼，則無需輸入此值。

PATCHCOMPATIBILITYRESET。從不相容修補程式清單中移除修補程式

`KAVSHELL PATCHCOMPATIBILITYRESET` 指令可讓您從不相容修補程式清單中移除具有指定 GUID 的修補程式。您可以指定多個 GUID，並以空格分隔。

指令語法

```
KAVSHELL PATCHCOMPATIBILITYRESET <GUID> [GUID...]
```

範例

```
KAVSHELL PATCHCOMPATIBILITYRESET 01234567-890A-BCDE-F012-34567890ABCD
```

REMOTEACCESS.管理應用程式主控台遠端連線設定

`KAVSHELL REMOTEACCESS` 命令可讓您管理應用程式主控台與安裝 Kaspersky Embedded Systems Security 的裝置之間的遠端連線設定。

指令語法

```
KAVSHELL REMOTEACCESS /SET /PORT=<new_port> [/PWD:<password>] [/LOGIN:<user name>] | /RESET UIKLPORT [/PWD:
<password>] [/LOGIN:<user name>] | /SHOW
```

命令選項

參數	描述
`/SET [UIPORT | UIKLPORT]`	設定連接埠號碼： • `UIPORT` 是使用 Windows 認證進行連線的連接埠。 • `UIKLPORT` 是供手動建立的使用者使用認證進行連線的連接埠。
`/PORT=<new_port>`	若傳遞 `/SET`，則此項為必填。 連接埠編號。可能的值範圍：1–65535。
`/RESET UIKLPORT`	關閉供手動建立的使用者使用認證進行連線的連接埠。
`/SHOW`	輸出目前的連接埠編號。
`/PWD:<password>`	可選參數。 KLAdmin 使用者帳戶或具有足夠權限之使用者帳戶的密碼。 如果未指定此選項，應用程式將在下一行提示您輸入密碼。
`/LOGIN:<user name>`	可選參數。 具有足夠權限的使用者帳戶名稱。 如果未指定此選項，應用程式將在下一行提示您輸入使用者名稱。 如果您已輸入 KLAdmin 密碼，則無需輸入此值。

範例

```
KAVSHELL REMOTEACCESS /SET UIPORT /PORT=50000
KAVSHELL REMOTEACCESS /RESET UIKLPORT
KAVSHELL REMOTEACCESS /SHOW
```

RESETMDRMACHINEID。重設裝置 ID

`KAVSHELL RESETMDRMACHINEID` 命令可讓您重設託管式偵測與回應解決方案所使用的裝置 ID。

指令語法

```
KAVSHELL RESETMDRMACHINEID [/PWD:<password>] [/LOGIN:<user name>]
```

命令選項

參數	描述
`/PWD:<password>`	可選參數。 KLAdmin 使用者帳戶或具有足夠權限之使用者帳戶的密碼。 如果未指定此選項，應用程式將在下一行提示您輸入密碼。
`/LOGIN:<user name>`	可選參數。 具有足夠權限的使用者帳戶名稱。 如果未指定此選項，應用程式將在下一行提示您輸入使用者名稱。 如果您已輸入 KLAdmin 密碼，則無需輸入此值。

ROLLBACK。上次更新回溯

`KAVSHELL ROLLBACK` 命令會啟動 *上次更新回溯* 任務。

指令語法

```
KAVSHELL ROLLBACK [/PWD:<password>] [/LOGIN:<user name>]
```

命令選項

參數	描述
`/PWD:<password>`	可選參數。 KLAdmin 使用者帳戶或具有足夠權限之使用者帳戶的密碼。 如果未指定此選項，應用程式將在下一行提示您輸入密碼。
`/LOGIN:<user name>`	可選參數。 具有足夠權限的使用者帳戶名稱。 如果未指定此選項，應用程式將在下一行提示您輸入使用者名稱。 如果您已輸入 KLAdmin 密碼，則無需輸入此值。

範例

```
KAVSHELL ROLLBACK
```

指令返回值：

- 0：操作成功完成。
- -2：未執行服務。
- -3：執行指令的權限不足。

- -99：未知錯誤。
- -221：找不到資料庫備份副本或備份副本已損毀。
- -222：資料庫備份副本已損毀。

RTP。即時檔案防護

`KAVSHELL RTP` 指令可讓您啟用或停用 即時檔案防護 元件。

指令語法

```
KAVSHELL RTP </START|/STOP> [/PWD:<password>] [/LOGIN:<user name>]
```

命令選項

參數	描述
`</START|/STOP>`	啟用或停用 即時檔案防護 元件： • `/START` 會啟用元件。 • `/STOP` 會停用元件。
`/PWD:<password>`	`KAVSHELL RTP /STOP` 指令的必要選項。 KLAdmin 使用者帳戶或具有足夠權限之使用者帳戶的密碼。 如果未指定此選項，應用程式將在下一行提示您輸入密碼。
`/LOGIN:<user name>`	可選參數。 具有足夠權限的使用者帳戶名稱。 如果未指定此選項，應用程式將在下一行提示您輸入使用者名稱。 如果您已輸入 KLAdmin 密碼，則無需輸入此值。

範例

```
KAVSHELL RTP STOP /PWD:p@ssw0rd
```

SCAN。按需掃描

您可以使用 `KAVSHELL SCAN` 命令建立並啟動 *按需掃描* 工作。要從命令列啟動現有自訂掃描工作，請使用 `KAVSHELL TASK` 指令。

指令語法

```
KAVSHELL SCAN <scan_scope> [/MEMORY|/SHARED|/STARTUP|/REMDRIVES|/FIXDRIVES|/MYCOMP] [/L:<file_name>][/F<A|C|E>]
[/NEWONLY][/AI:<DISINFECT|DISINFDEL|DELETE|REPORT|AUTO>] [/AS:<QUARANTINE|DELETE|REPORT|AUTO>] [/DISINFECT|DELETE]
[/E:<ABMSPO>] [/EM:<"masks">] [/ES:<size>] [/ET:<s>][/TZOFF] [/NOICHECKER][/NOISWIFT][/NOCHECKMSSIGN]
[/ANALYSERLEVEL] [/W:<report_file>] [/ANSI] [/ALIAS:<alternate name>]
```

參數	描述
`<scan_scope>`	必需參數。 以空格分隔的檔案、資料夾、網路路徑或標準掃描範圍清單。 標準掃描範圍： • `/MEMORY` 會掃描記憶體中的所有處理程序。 • `/SHARED` 會掃描共用資料夾。 • `/STARTUP` 會掃描啟動物件。 • `/REMDRIVES` 會掃描卸除式磁碟機。 • `/FIXDRIVES` 會掃描所有本機硬碟。 • `/MYCOMP` 會掃描整台電腦。 您可以指定多個值，之間由空格分開。
`/L:<file_name>`	可選參數。 含掃描範圍清單的檔案路徑。必須手動建立該檔案並以 TXT 格式儲存。 檔案必須以不含 BOM 的 UTF-8 編碼儲存。
`/F<A|C|E>`	可選參數。 應包括在掃描範圍內的物件： • `/FA`：掃描所有物件。應用程式會掃描所有檔案，無一例外（所有格式和副檔名）。 • `/FC`：依據副檔名掃描物件。應用程式只會掃描格式包含在可感染物件格式清單中的物件。 • `/FE`：依據副檔名掃描物件。應用程式只會掃描副檔名包含在可感染物件副檔名清單中的物件。
`/NEWONLY`	可選參數。 僅掃描新增與變更過的檔案。 如果未傳遞此引數，Kaspersky Embedded Systems Security 會掃描所有物件。
`/AI:` `<DISINFECT|DISINFDEL|DELETE|REPORT|AUTO>`	可選參數。 您希望應用程式對受感染物件和其他物件執行的操作： • `DISINFECT`：解毒；若解毒失敗則通知。 • `DISINFDEL`：解毒；若解毒失敗則刪除。 • `DELETE`：刪除。 • `REPORT`（預設值）：通知。 • `AUTO`：建議防護。
`/AS:<QUARANTINE|DELETE|REPORT|AUTO>`	可選參數。 您希望應用程式對受感染物件執行的操作： • `QUARANTINE`：移至隔離區。 • `DELETE`：刪除。 • `REPORT`（預設值）：通知。 • `AUTO`：建議防護。
`/E:<ABMSPO>`	排除指定的物件類型。 可能的值： • `A`：ZIP、CAB、RAR 和 ARJ 壓縮檔案及其他壓縮檔案格式。 • `B`：Microsoft Outlook 和 Microsoft Outlook Express 郵件資料庫檔案。 • `M`：郵件格式檔案，例如 Microsoft Outlook 和 Microsoft Outlook Express 郵件。 • `S`：自解壓縮檔案。 • `P`：由二進位代碼封裝程式（例如 UPX 或 ASPack）封裝的可執行檔。 • `O`：內嵌於檔案中的物件（例如 Microsoft Word 巨集或電子郵件附件）。 您可以指定多個參數值。
`/EM=<file mask>`	與檔案遮罩比對的檔案將從掃描範圍中排除。範例： • *.exe 遮罩將包括副檔名為 EXE 的檔案的所有路徑。 • example* 遮罩將包括名為 EXAMPLE 的檔案的所有路徑。
`/ET=<scan duration in seconds>`	掃描時間長於指定時間限制（以秒為單位）的檔案將從掃描範圍中排除。預設值為 60 秒。
`/ES=<size in megabytes>`	大於指定大小限制（以百萬位元組為單位）的檔案將從掃描範圍中排除。預設值為 100 MB。

參數	描述
/TZOFF	不要套用受信任區域排除項目。
/NOICHECKER	停用 iChecker（預設為啟用狀態）。
/NOISWIFT	停用 iSwift（預設為啟用狀態）。
/NOCHECKMSSIGN	不要掃描由 Microsoft 進行數位簽署的檔案。
/ANALYSERLEVEL	啟用啟發式分析並配置分析等級。 以下啟發式分析等級可用： • 1：輕度。 • 2：中度。 • 3：深度。 如果未傳遞此參數，應用程式將不使用啟發式分析器。
/EXCLUDE=<list of exlusion	將從掃描工作範圍中排除的檔案、資料夾或網路路徑清單。您可以指定多個值，之間由空格分開。
/W=<file path>	任務記錄檔的路徑和名稱。 以相同的記錄設定重新執行此指令將覆寫現有的記錄檔。
/ANSI	針對寫入任務記錄的事件使用 ANSI 編碼。 如果未指定 /W 參數，則不會套用 /ANSI 選項。 如果未指定 /ANSI 選項，將使用 Unicode 建立工作記錄。
/ALIAS:<alternate name>	為任務指定一個暫用名稱，以便在任務執行期間參照該任務。例如，您可使用 KAVSHELL TASK 指令檢視工作統計。替代任務名稱在應用程式的所有替代任務名稱中必須是唯一的。 如果未傳遞此引數，則會依下列方式指定任務名稱：scan_<kavshell_pid>。例如：scan_1234。

範例

```
KAVSHELL SCAN Folder56 D:\Folder1\Folder2\Folder3\ C:\Folder1\ C:\Folder2\003.exe "\\another server\Shared\"
F:\123\*.fgb /SHARED /AI:DISINFDEL /AS:QUARANTINE /FA /E:ABM /EM:"*.xtx;*.fff;*.ggg;*.bbb;*.info" /NOICHECKER
/NOISWIFT /W:log.log
KAVSHELL SCAN /L:scan_objects.lst /W:log.log
```

指令返回值：

- 0：操作順利完成（未偵測到威脅）。
- 1：已取消操作。
- -2：未執行服務。
- -3：執行指令的權限不足。
- -4：找不到物件（找不到包含掃描範圍清單的檔案）。
- -5：語法錯誤或未設定掃描範圍。
- -80：偵測到受感染的物件。
- -81：偵測到可能受感染的物件。
- -82：掃描期間發生物件處理錯誤。
- -83：偵測到未掃描的物件。
- -84：偵測到損壞的物件。

- -85：建立工作記錄失敗。
- -99：未知錯誤。
- -301：產品授權無效。

SCANCRITICAL。關鍵區域掃描

`KAVSHELL SCANCRITICAL` 命令會啟動 *關鍵區域掃描* 任務。

指令語法

```
KAVSHELL SCANCRITICAL [/W:<path to task log file>] [/PWD:<password>] [/LOGIN:<user name>]
```

命令選項

參數	描述
`/W`	可選參數。 為匯出的工作記錄指定副檔名為 .LOG 的檔案名稱。您也可以指定檔案路徑。 如果命令中只指定檔案名稱，應用程式會嘗試將檔案放置在應用程式的安裝資料夾中。如果已啟用應用程式的自我防護機制，匯出將會失敗，因為應用程式的自我防護功能會封鎖在應用程式資料夾中建立新檔案。若要匯出工作記錄，請指定檔案路徑。
`/PWD:<password>`	可選參數。 KLAdmin 使用者帳戶或具有足夠權限之使用者帳戶的密碼。 如果未指定此選項，應用程式將在下一行提示您輸入密碼。
`/LOGIN:<user name>`	可選參數。 具有足夠權限的使用者帳戶名稱。 如果未指定此選項，應用程式將在下一行提示您輸入使用者名稱。 如果您已輸入 KLAdmin 密碼，則無需輸入此值。

範例

```
KAVSHELL SCANCRITICAL /W:scancritical.log
```

SERVERBINDINGDISABLE。停用管理員伺服器連線防護

`KAVSHELL SERVERBINDINGDISABLE` 命令會在本機停用與管理伺服器連線的防護。此命令會啟動 *管理伺服器連線防護* 工作，該工作會移除電腦與管理伺服器連線的密碼。

指令語法

```
KAVSHELL SERVERBINDINGDISABLE [/PWD:<password>] [/LOGIN:<user name>]
```

命令選項

參數	描述
`/PWD:<password>`	可選參數。 KLAdmin 使用者帳戶或具有足夠權限之使用者帳戶的密碼。 如果未指定此選項，應用程式將在下一行提示您輸入密碼。

/LOGIN:<user name>	可選參數。 具有足夠權限的使用者帳戶名稱。 如果未指定此選項，應用程式將在下一行提示您輸入使用者名稱。 如果您已輸入 KLAdmin 密碼，則無需輸入此值。

START。啟動應用程式服務

KAVSHELL START 命令會啟動 Kaspersky Embedded Systems Security 服務 服務。

指令語法

```
KAVSHELL START
```

STARTPOLICY。啟用政策

KAVSHELL STARTPOLICY 命令會在受防護裝置上啟用卡巴斯基安全管理中心政策。將根據政策配置應用程式設定。

指令語法

```
KAVSHELL STARTPOLICY
```

STOP。停止應用程式服務

KAVSHELL STOP 命令會停止 Kaspersky Embedded Systems Security 服務 服務。

指令語法

```
KAVSHELL STOP [/PWD:<password>] [/LOGIN:<user name>]
```

命令選項

參數	描述
/PWD:<password>	可選參數。 KLAdmin 使用者帳戶或具有足夠權限之使用者帳戶的密碼。 如果未指定此選項，應用程式將在下一行提示您輸入密碼。
/LOGIN:<user name>	可選參數。 具有足夠權限的使用者帳戶名稱。 如果未指定此選項，應用程式將在下一行提示您輸入使用者名稱。 如果您已輸入 KLAdmin 密碼，則無需輸入此值。

指令返回值：

- 0：操作成功完成。
- -3：執行指令的權限不足。

- -5：未知錯誤。
- -6：無效的操作（Kaspersky Embedded Systems Security 服務 已停止）。
- -7：服務未註冊
- -8：已停用服務自動啟動。
- -9：嘗試以其他使用者帳戶執行受管理裝置失敗。
- -99：未知錯誤。

TASK。管理工作

您可以使用 `KAVSHELL TASK` 指令管理 Kaspersky Embedded Systems Security 工作：執行、暫停、繼續和停止工作，以及檢視目前的工作狀態和統計資料。

指令語法

```
KAVSHELL TASK [<alternative name> </START | /STOP | /STATE | /STATISTICS>] /PWD:<password> [/LOGIN:<user name>]
```

命令選項

參數	描述
無參數	回傳所有現有 Kaspersky Embedded Systems Security 工作的清單。此清單包含以下欄位：工作的別名（Kaspersky Embedded Systems Security for Windows 指派給工作的額外簡短名稱）、工作類別（系統或使用者）以及工作的目前狀態。
`<alternative name>`	您要管理之工作的別名。若要檢視 Kaspersky Embedded Systems Security 工作別名，請輸入不帶任何參數的 `KAVSHELL TASK` 指令。
`/START`	啟動工作。
`/STOP`	停止工作。
`/STATE`	顯示工作的目前狀態。
`/STATISTICS`	顯示工作統計資料。
`/PWD: <password>`	`KAVSHELL TASK /STOP` 指令的必要選項。 KLAdmin 使用者帳戶或具有足夠權限之使用者帳戶的密碼。 如果未指定此選項，應用程式將在下一行提示您輸入密碼。
`/LOGIN:<user name>`	可選參數。 具有足夠權限的使用者帳戶名稱。 如果未指定此選項，應用程式將在下一行提示您輸入使用者名稱。 如果您已輸入 KLAdmin 密碼，則無需輸入此值。

指令語法

```
KAVSHELL TASK on-access /START
KAVSHELL TASK user-task_1 /STOP
KAVSHELL TASK scan-critical /STATE
```

指令返回值：

- 0：操作成功完成。
- -2：未執行服務。

- -3：執行指令的權限不足。
- -4：找不到物件（找不到工作）。
- -5：語法錯誤或未設定掃描範圍。
- -6：操作無效（例如，工作未執行、已在執行或無法暫停）。
- -99：未知錯誤。
- -301：產品授權無效。
- 401：工作未啟動（適用於 `KAVSHELL TASK <task name> /STATE` 指令）。
- 402：工作已啟動（適用於 `KAVSHELL TASK <task name> /STATE` 指令）。
- 403：工作已暫停（適用於 `KAVSHELL TASK <task name> /STATE` 指令）。
- -404：操作失敗（工作狀態變更導致當機）。

TRACE。追蹤應用程式作業

`KAVSHELL TRACE` 指令可讓您啟用或停用應用程式追蹤。

指令語法

```
KAVSHELL TRACE </ON /F:<traces_folder:>[/S:<traces_size_in_MB>] [/LVL:<debug|info|warning|error|critical>] /R:<max trace files to rotate> | /OFF > [/LOGIN:<user name>] [/PWD:<password>]
```

命令選項

參數	描述
`</ON | /OFF>`	必需參數。 啟用或停用應用程式追蹤。
`/F:<traces_folder>`	若傳遞 `/ON`，則此項為必填。 追蹤檔案的儲存資料夾路徑。
`/S:<traces_size_in_MB>`	可選參數。 追蹤檔案的大小上限（以 MB 為單位）。 可用值：從 1 到 4095 MB。預設值為 100 MB。
`/LVL: <debug|info|warning|error|critical>`	可選參數。 偵錯資訊的詳細程度。 • `critical` 表示追蹤檔案僅儲存有關嚴重錯誤的訊息。 • `error` 表示追蹤檔案儲存有關所有錯誤和警告的訊息。 • `warning` 表示追蹤檔案儲存有關所有錯誤、警告及其他資訊的訊息。 • `info`（預設值）表示追蹤檔案儲存有關所有錯誤和警告的訊息，以及應用程式正常運作的相關資訊。 • `debug` 表示追蹤檔案儲存應用程式運作的所有相關資訊。
`/R:<max trace files to rotate>`	可選參數。 追蹤記錄中的檔案數上限。 可用值：從 1 到 999。預設值為 5。
`/PWD:<password>`	可選參數。 KLAdmin 使用者帳戶或具有足夠權限之使用者帳戶的密碼。 如果未指定此選項，應用程式將在下一行提示您輸入密碼。

/LOGIN:<user name>	可選參數。 具有足夠權限的使用者帳戶名稱。 如果未指定此選項，應用程式將在下一行提示您輸入使用者名稱。 如果您已輸入 KLAdmin 密碼，則無需輸入此值。

範例

```
KAVSHELL TRACE /ON /F:"C:\Trace Folder" /LVL:info /R:50 /PWD:p@ssw0rd
KAVSHELL TRACE /OFF
```

UPDATE。更新資料庫和程式模組

您可以使用 KAVSHELL UPDATE 指令管理 *更新* 工作。

指令語法

```
KAVSHELL UPDATE <update_source | /AK | /KL> [/NOUSEKL] [/PROXY:<IP address>:<port>] [/AUTHTYPE:<0-2>] [/PROXYUSER:
<user_name>] [/PROXYPWD:<password>] [/NOPROXYFORKL] [/USEPROXYFORCUSTOM] [/USEPROXYFORLOCAL] [/NOFTPPASSIVE]
[/TIMEOUT:<s>] [/REG:<code_by_iso3166>] [/W:<report_file>] [/ANSI] [/ALIAS:<alternate name>]
```

命令選項

參數	描述
<update_source | /AK | /KL>	必需參數。 選擇更新來源： • 使用 <update_source> 以使用自訂更新來源。您可以指定受保護裝置上的資料夾路徑、UNC 格式的網路資料夾路徑，或更新資料夾所在之 HTTP 或 FTP 伺服器的位址。 • /AK – 使用卡巴斯基安全管理中心伺服器作為更新來源。 • /KL – 將 Kaspersky 的更新伺服器用作更新來源。 您可以指定多個值，之間由空格分開。
/NOUSEKL	可選參數。 如果其他更新來源無法使用，則不使用 Kaspersky 更新伺服器（預設值）。
/PROXY:<IP address>:<port>	可選參數。 代理伺服器的 IP 位址或符號名稱以及埠號。
/AUTHTYPE:<0-2>	可選參數。 代理伺服器身分驗證類型： • 0，用於使用目前使用者帳戶進行 NTLM 身分驗證。 • 1，用於使用其使用者名稱和密碼由 /PROXYUSER 與 /PROXYPWD 選項指定的使用者帳戶進行 NTLM 身分驗證。 • 2，用於使用由 /PROXYUSER 與 /PROXYPWD 選項指定的使用者名稱和密碼進行身分驗證。
/PROXYUSER:<user_name>	若傳遞 /AUTHTYPE:1 或 /AUTHTYPE:2 參數，則此為必要參數。 存取代理伺服器所需的使用者名稱。 如果指定 /AUTHTYPE:0，則會忽略 /PROXYUSER:<user_name> 和 /PROXYPWD:<password> 選項。
/PROXYPWD:<password>	若傳遞 /AUTHTYPE:1 或 /AUTHTYPE:2 參數，則此為必要參數。 存取代理伺服器所需的使用者密碼。 如果指定 /AUTHTYPE:0，則會忽略 /PROXYUSER:<user_name> 和 /PROXYPWD:<password> 選項。如果指定了 /PROXYUSER 參數但省略了 /PROXYPWD 參數，密碼將被視為空字串。
/NOPROXYFORKL	可選參數。 不要使用代理伺服器設定連線至 Kaspersky 更新伺服器。
/USEPROXYFORCUSTOM	可選參數。 使用代理伺服器設定連線至使用者定義的更新來源。
/USEPROXYFORLOCAL	可選參數。 使用代理伺服器連線本機更新來源。

/NOFTPPASSIVE	可選參數。 如果指定此選項，Kaspersky Embedded Systems Security 會使用主動模式連線至 FTP 伺服器。如果未傳遞此選項，Kaspersky Embedded Systems Security 會盡可能使用被動連線模式。
/TIMEOUT:<s>	可選參數。 FTP 或 HTTP 伺服器連線逾時時間（以秒為單位）。 預設值：10 秒。
/REG:<code_by_iso3166>	可選參數。 受防護裝置所在國家/地區的代碼，符合 ISO 3166-1 標準。範例： /REG:GR 。 如果省略此參數或指定無效的國家/地區代碼，Kaspersky Embedded Systems Security 會根據安裝應用程式主控台之受防護裝置的地區設定判斷位置。 應用程式會在選取更新伺服器時使用位置資訊。
/W=<file path>	任務記錄檔的路徑和名稱。 以相同的記錄設定重新執行此指令將覆寫現有的記錄檔。
/ANSI	針對寫入任務記錄的事件使用 ANSI 編碼。 如果未指定 /W 參數，則不會套用 /ANSI 選項。 如果未指定 /ANSI 選項，將使用 Unicode 建立工作記錄。
/ALIAS:<alternate name>	為任務指定一個暫用名稱，以便在任務執行期間參照該任務。例如，您可使用 KAVSHELL TASK 指令檢視工作統計。替代任務名稱在應用程式的所有替代任務名稱中必須是唯一的。 如果未傳遞此引數，則會依下列方式指定任務名稱：update_<kavshell_pid>。例如：update_1234。
/PWD:<password>	可選參數。 KLAdmin 使用者帳戶或具有足夠權限之使用者帳戶的密碼。 如果未指定此選項，應用程式將在下一行提示您輸入密碼。
/LOGIN:<user name>	可選參數。 具有足夠權限的使用者帳戶名稱。 如果未指定此選項，應用程式將在下一行提示您輸入使用者名稱。 如果您已輸入 KLAdmin 密碼，則無需輸入此值。

指令語法

```
KAVSHELL UPDATE "\\Server\kav bases\" ftp://bases.company.com /USEPROXYFORCUSTOM /PROXY:proxy.company.com:8080
/AUTHTYPE:2 /PROXYUSER:inetuser /PROXYPWD:p@ssw0rd /TIMEOUT:100 /REG:ru /W:"C:\KAVREPORTS\daily update.log"
KAVSHELL UPDATE "\\Server\kav bases\" ftp://bases.company.com /NOUSEKL /USEPROXYFORCUSTOM
/PROXY:proxy.company.com:8080 /AUTHTYPE:2 /PROXYUSER:inetuser /PROXYPWD:p@ssw0rd
KAVSHELL UPDATE /AK /NOUSEKL
KAVSHELL UPDATE /KL /W:"C:\KAVREPORTS\daily update.log"
KAVSHELL UPDATE /AK /W:"C:\KAVREPORTS\daily update.log"
```

指令返回值：

- 0：操作成功完成。
- 200：所有物件均為最新狀態。
- -2：未執行服務。
- -3：執行指令的權限不足。
- -5：未知錯誤。
- -99：未知錯誤。
- -206：指定來源中的更新檔遺失或檔案格式不明。
- -209：連線更新來源錯誤。
- -232：連線到代理伺服器時發生身分驗證錯誤。

- -234：Kaspersky Security Center 連線錯誤。
- -235：Kaspersky Embedded Systems Security 在連線到更新來源時未透過身分驗證。
- -236：應用程式資料庫已損毀。
- -301：產品授權無效。

聯絡技術支援

本章節提供有關如何與 Kaspersky 技術支援服務聯絡的資訊。

如何獲取技術支援

如果您無法在檔案中或Kaspersky Embedded Systems Security 相關資訊源中找到您問題的解決方案，建議您聯絡技術支援。技術支援會為您解答關於安裝和使用 Kaspersky Embedded Systems Security 的問題。

Kaspersky 在應用程式的生命週期內為 Kaspersky Embedded Systems Security 提供支援（請參閱應用程式生命週期頁面）。與技術支援部門聯絡之前，請閱讀支援規則。

您可以透過以下方式取得技術支援：

- 透過造訪技術支援網站
- 透過 Kaspersky CompanyAccount 網站向 Kaspersky 技術支援傳送請求

透過 Kaspersky CompanyAccount 取得技術支援

Kaspersky CompanyAccount 是一個入口網站，提供給使用 Kaspersky 應用程式的公司。Kaspersky CompanyAccount 設計用於方便使用者與 Kaspersky 專家之間透過線上請求進行互動。透過使用 Kaspersky CompanyAccount 網站，您可以監視 Kaspersky 專家處理電子請求的進度並儲存電子請求的歷史記錄。

可以在 Kaspersky CompanyAccount 上的單個使用者帳戶中註冊您組織的所有員工。透過使用單一帳戶，您可以集中管理註冊的員工傳送到 Kaspersky 的電子請求，以及在 Kaspersky CompanyAccount 中管理員工的權限。

Kaspersky CompanyAccount 適用於以下語言：

- 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

您可以在技術支援網站上進一步瞭解 Kaspersky CompanyAccount。

向技術支援專家提供延伸診斷資訊

為了更有效地支援和解決應用程式問題，技術支援專家可能會要求您臨時變更應用程式設定，以便在診斷期間進行偵錯。這可能需要執行以下操作：

- 啟動處理和儲存延伸診斷資訊的功能。
- 微調單個軟體元件的設定，這些設定無法透過標準使用者介面元素獲得。
- 變更已處理的診斷資訊的儲存和傳輸設定。
- 設定網路流量擷取和記錄。

執行列出的操作所需的所有資訊（步驟順序的描述、可變更的設定、設定檔、指令碼、附加命令列功能、偵錯模組、專用實用程式等），以及為了偵錯而分析的資料的組成，將由技術支援專家宣布。進階診斷資訊儲存在使用者的電腦中。儲存的資料不會自動傳輸到卡巴斯基。

向技術支援專家報告問題後，他們可能需求您建立一份包含有關 Kaspersky Embedded Systems Security 執行情況的資訊的報告，然後將報告傳送給技術支援部門。卡巴斯基技術支援專家也可能會要求您：建立偵錯檔案，傳送記憶體傾印檔案 和 提供一份來自 Kaspersky Get System Info 實用程式的報告。

在技術支援專家分析您所傳送的資料後，他們可以建立 AVZ 指令碼並將其傳送給您。透過使用 AVZ 指令碼，可以分析活動處理程序以尋找威脅，掃描電腦置以尋找威脅，清除或刪除感染的檔案以及建立系統掃描報告。

上述操作只能在技術支援專家的指導下按照技術支援專家的指示進行。以應用程式文件中或技術支援專家的建議中未描述的方式自行修改應用程式設定可能會導致作業系統速度變慢和故障、電腦防護等級降低以及違反處理資訊的可用性和完整性。

追蹤應用程式作業

*應用程式追蹤*是應用程式執行的操作以及有關應用程式執行期間發生的事件的訊息的詳細記錄。在追蹤過程中，應用程式會建立包含有關不同應用程式元件操作的資料的一組檔案。

應用程式追蹤應在 Kaspersky 技術支援的監督下執行。

偵錯檔案可以逐步跟蹤執行應用程式指令的過程，可確定應用程式操作中發生錯誤的階段。

如何在卡巴斯基安全管理中心管理主控台中啟用和配置應用程式跟踪

1. 在卡巴斯基安全管理中心管理主控台樹狀目錄中，選取**政策**。
2. 選擇必要的政策並點擊以開啟政策內容。
3. 在政策內容視窗中，轉至「**故障診斷**」區域。

4. 在"**故障診斷設定**"塊中，點擊"**設定**"按鈕。

   故障診斷設定視窗將在**應用程式偵錯設定**頁簽上開啟。

5. 使用"**啟用偵錯**"核取方塊可以啟用或停用對應用程式操作的追蹤。

   預設情況下，應用程式操作追蹤處於停用狀態。

6. 如有必要，請變更 Kaspersky Embedded Systems Security 儲存偵錯檔案的預設資料夾。為此，請在**偵測檔案資料夾**欄位中指定本機資料夾的完整路徑。

   該資料夾必須提前建立並且可由系統帳戶寫入。您無法指定網路資料夾、磁碟機或環境變數。

   在選定的資料夾中，Kaspersky Embedded Systems Security 會建立一個名為 logs-Kaspersky Embedded Systems Security-<uid> 的子資料用於儲存偵錯檔案，其中 <uid> 是一個唯一的 8 個字元日誌標識符。

7. 選擇偵錯資訊的詳細等級：

   - **正常**表示偵錯檔案保存有關所有錯誤、警告的訊息以及有關應用程式正常操作的資訊（預設）。
   - **緊急**表示偵錯檔案僅保存有關致命錯誤的訊息。
   - **診斷**表示偵錯檔案保存有關所有錯誤和警告的訊息。
   - **重要**表示偵錯檔案保存有關所有錯誤、警告和附加資訊的訊息。
   - **詳情**表示偵錯檔案保存有關應用程式作業的所有資訊。

   技術支援代表確定為解決任何潛在問題而需要設定的詳細等級。

8. 若要刪除舊的偵錯檔案，請啟用 **移除最早的追蹤檔案** 功能。

   如果此功能已啟用，請配置偵錯檔案的最大大小和數量：

   a. 指定**追蹤檔案大小上限（MB）**。

      可用值：從 1 到 4095 MB。預設值為 100 MB。

   b. 指定**一個追蹤記錄的最多檔案數量**。

      可用值：從 1 到 999。預設值為 5。

9. 儲存變更。

如何在應用程式主控台中啟用和配置應用程式追蹤

1. 在應用程式主控台樹狀目錄中，選擇"**Kaspersky Embedded Systems Security**"節點並執行以下操作之一：

   - 在節點的結果窗格中，點擊**應用程式內容**連結。
   - 在節點的內容功能表中選擇**應用程式內容**。

   開啟"**應用程式內容**"視窗。

2. 選擇"**故障診斷**"標籤。

3. 在"**故障診斷設定**"塊中，點擊"**設定**"按鈕。

   開啟"**故障診斷設定**"視窗。

4. 選取「偵錯設定」索引標籤：

   - **應用程式偵錯設定**Kaspersky Embedded Systems Security 開始對該應用程式進行偵錯。
   - **應用程式主控台偵錯設定**如果應用程式主控台和 Kaspersky Embedded Systems Security 安裝在不同的電腦上，則您只能啟動應用程式主控台的偵錯。

5. 使用"**啟用偵錯**"核取方塊可以啟用或停用對應用程式操作的追蹤。

   預設情況下，應用程式操作追蹤處於停用狀態。

6. 如有必要，請變更 Kaspersky Embedded Systems Security 儲存偵錯檔案的預設資料夾。為此，請點擊 **瀏覽** 按下按鈕並選擇所需的資料夾。

   該資料夾必須提前建立並且可由系統帳戶寫入。您無法指定網路資料夾、磁碟機或環境變數。

   在選定的資料夾中，Kaspersky Embedded Systems Security 會建立一個名為 logs-Kaspersky Embedded Systems Security-<uid> 的子資料用於儲存偵錯檔案，其中 <uid> 是一個唯一的 8 個字元日誌標識符。

7. 選擇偵錯資訊的詳細等級：

   - **正常**表示偵錯檔案保存有關所有錯誤、警告的訊息以及有關應用程式正常操作的資訊（預設）。
   - **緊急**表示偵錯檔案僅保存有關致命錯誤的訊息。
   - **診斷**表示偵錯檔案保存有關所有錯誤和警告的訊息。
   - **重要**表示偵錯檔案保存有關所有錯誤、警告和附加資訊的訊息。
   - **詳情**表示偵錯檔案保存有關應用程式作業的所有資訊。

   技術支援代表確定為解決任何潛在問題而需要設定的詳細等級。

8. 若要刪除舊的偵錯檔案，請啟用 **移除最早的追蹤檔案** 功能。

   如果此功能已啟用，請配置偵錯檔案的最大大小和數量：

   a. 指定**追蹤檔案大小上限（MB）**。

      可用值：從 1 到 4095 MB。預設值為 100 MB。

   b. 指定**一個追蹤記錄的最多檔案數量**。

      可用值：從 1 到 999。預設值為 5。

9. 儲存變更。

如何在卡巴斯基安全管理中心網頁主控台中啟用和配置應用程式跟踪

1. 在網頁主控台的主視窗中，選擇**資產管理 → 政策**。
2. 點擊 Kaspersky Embedded Systems Security 政策的名稱。

   政策內容視窗將開啟。

3. 選擇“**應用程式設定**”標籤。

4. 選擇 **故障診斷** 部分。

5. 在“**故障診斷設定**“塊中，使用“**啟用應用程式追蹤**”核取方塊來啟用或停用追蹤應用程式操作。
   預設情況下，應用程式操作追蹤處於停用狀態。

6. 如有必要，請變更 Kaspersky Embedded Systems Security 儲存偵錯檔案的預設資料夾。為此，請在**追蹤資料夾（資料夾的完整路徑，例如 C:\\Traces\\）**欄位中指定本機資料夾的完整路徑。

   > 該資料夾必須提前建立並且可由系統帳戶寫入。您無法指定網路資料夾、磁碟機或環境變數。

   在選定的資料夾中，Kaspersky Embedded Systems Security 會建立一個名為 logs-Kaspersky Embedded Systems Security-<uid> 的子資料用於儲存偵錯檔案，其中 <uid> 是一個唯一的 8 個字元日誌標識符。

7. 選擇偵錯資訊的詳細等級：

   - **正常**表示偵錯檔案保存有關所有錯誤、警告的訊息以及有關應用程式正常操作的資訊（預設）。
   - **緊急**表示偵錯檔案僅保存有關致命錯誤的訊息。
   - **診斷**表示偵錯檔案保存有關所有錯誤和警告的訊息。
   - **重要**表示偵錯檔案保存有關所有錯誤、警告和附加資訊的訊息。
   - **詳情**表示偵錯檔案保存有關應用程式作業的所有資訊。

   技術支援代表確定為解決任何潛在問題而需要設定的詳細等級。

8. 若要刪除舊的偵錯檔案，請啟用 **移除較早的追蹤檔案** 功能。
   如果此功能已啟用，請配置偵錯檔案的最大大小和數量：

   a. 指定**追蹤檔案的最大大小 (MB)**。
      可用值：從 1 到 4095 MB。預設值為 100 MB。

   b. 指定**一個追蹤記錄的最多檔案數量**。
      可用值：從 1 到 999。預設值為 5。

9. 儲存變更。

您也可以在小型診斷視窗中啟用和配置應用程式追蹤。

偵錯檔案的內容和儲存

> 您親自負責電腦上儲存的資料的安全性，尤其是在資料提交到 Kaspersky 前監控和限制對資料的存取。

只要應用程式在使用中，就會在電腦中儲存偵錯檔案，當應用程式被移除後，偵錯檔案將被永久移除。

偵錯檔案儲存在以下資料夾中：%ProgramData%\Kaspersky Lab\KESS.4.1\Traces。

偵錯檔案按如下方式命名：KESS<4.1_dateXX.XX_timeXX.XX_pidXXX.><偵錯檔案類型>.log。

您可以檢視偵錯檔案中儲存的資料。

所有偵錯檔案都包含下列一般資料：

- 事件時間
- 執行線程編號
- 引起該事件的應用程式元件
- 事件嚴重程度（通知性事件、警告、緊急事件、錯誤）
- 關於應用程式元件命令執行和命令執行結果的事件說明。

SRV.log、GUI.log 和 ALL.log 偵錯檔案的內容

SRV.log、GUI.log 和 ALL.log 偵錯檔案可儲存一般資料之外的下列資訊：

- 個人資料，包括姓氏、名字和中間名，如果此資料封包含在本機電腦檔案的路徑中。
- 使用者名稱和密碼，如果它們公開傳送。在網際網路流量掃描期間，此資料可被記錄偵錯檔案中。
- 使用者名稱和密碼，如果它們包含在 HTTP 標題中。
- Microsoft Windows 帳戶名稱，如果該帳戶名稱包含在檔案名中。
- 包含您的帳戶名和密碼的電子郵件位址或網頁位址，如果它們包含在被偵測的物件名中。
- 登入代理伺服器的代理伺服器位址、電腦名稱、連接埠、IP 位址和使用者名稱。當應用程式使用代理伺服器時，將會把此資料寫入偵錯檔案。
- 您的電腦要與其建立連線的遠端 IP 位址。
- 網路流量資料。如果啟用流量監控元件，則此資料將寫入偵錯檔案。
- 從 Kaspersky 伺服器接收的資料（如病毒資料庫的版本）。
- Kaspersky Embedded Systems Security 元件的狀態及其運作資料。
- 應用程式中的使用者活動資料。
- 作業系統事件。

HST.log、BL.log、Dumpwriter.log、WD.log 和 AVPCon.dll.log 偵錯檔案的內容

除了一般資料之外，HST.log 偵錯檔案包含關於資料庫執行和程式模組更新工作的資訊。

除了一般資料之外，BL.log 偵錯檔案包含應用程式執行期間發生的事件資訊，以及對應用程式錯誤進行故障排除所需的資料。如果使用 avp.exe –bl 參數啟動應用程式，將建立此檔案。

除了一般資料之外，當進行應用程式記憶體傾印時，Dumpwriter.log 偵錯檔案包含對錯誤進行故障排除時必要服務資訊。

除了一般資料之外，WD.log 偵錯檔案包含 avpsus 服務執行期間所發生的事件資訊，包括應用程式模組更新事件。

除了一般資料之外，AVPCon.dll.log 偵錯檔案包含卡巴斯基安全管理中心連線模組執行期間所發生的事件資訊。

AMSI 掃描器元件偵錯檔案的內容

除了一般資料，AMSI.log 偵錯檔案還包含有關對協力廠商應用程式的請求執行掃描的結果的資訊。

應用程式 Web 外掛程式偵錯檔案的內容

應用程式 Web 外掛程式的偵錯檔案儲存在部署了卡巴斯基安全管理中心網頁主控台的電腦上，位於資料夾 Program Files\Kaspersky Lab\Kaspersky Security Center Web Console\logs中。

應用程式 Web 外掛程式的偵錯檔案按如下方式命名： logs-ess_windows-<type of trace file>.DESKTOP-<date of file update>.log。網頁主控台在安裝後開始寫入資料，在刪除網頁主控台後會刪除偵錯檔案。

除了一般資料之外，應用程式 Web 外掛程式偵錯檔案包含以下資訊：

- KLAdmin 使用者密碼 用於解鎖 Kaspersky Embedded Systems Security 介面。
- 臨時密碼 用於解鎖 Kaspersky Embedded Systems Security 介面。
- SMTP 郵件伺服器的使用者名稱和密碼。
- 代理伺服器的使用者名稱和密碼。
- *變更應用程式元件* 工作的使用者名稱和密碼。
- 在 Kaspersky Embedded Systems Security 工作和政策內容中指定的帳戶憑據和路徑。

記錄記憶體傾印

記憶體傾印檔案包含應用程式發生故障時 Kaspersky Embedded Systems Security 處理程序的工作記憶體的所有資訊。

只要應用程式在使用中，就會在電腦中儲存記憶體傾印檔案，當應用程式被移除後，傾印檔案將被永久移除。

已儲存的傾印檔案可能包含機密資料。要控制資料的存取，必須單獨確保記憶體傾印檔案的安全性。

預設情況下，記憶體傾印檔案儲存在以下資料夾中：%ProgramData%\Kaspersky Lab\KESS.4.1\Traces。

如何在卡巴斯基安全管理中心管理主控台中啟用或停用記憶體傾印記錄

1. 在卡巴斯基安全管理中心管理主控台樹狀目錄中，選取**政策**。
2. 選擇必要的政策並點擊以開啟政策內容。
3. 在政策內容視窗中，轉至「**故障診斷**」區域。
4. 在"**故障診斷設定**"塊中，點擊"**設定**"按鈕。
   故障診斷設定視窗將在**應用程式偵錯設定**頁簽上開啟。
5. 選擇"**應用程式傾印設定**"標籤。
6. 使用"**建立傾印檔案**"核取方塊可以啟用或停用對應用程式操作的追蹤。
   預設情況下，記憶體傾印記錄功能處於停用狀態。
7. 如有必要，請變更 Kaspersky Embedded Systems Security 儲存偵錯檔案的預設資料夾。為此，請在**傾印檔案資料夾**欄位中指定本機資料夾的完整路徑。

   該資料夾必須提前建立並且可由系統帳戶寫入。您無法指定網路資料夾、磁碟機或環境變數。

8. 儲存變更。

如何在應用程式主控台中啟用或停用記憶體傾印記錄

1. 在應用程式主控台樹狀目錄中，選擇"**Kaspersky Embedded Systems Security**"節點並執行以下操作之一：
   - 在節點的結果窗格中，點擊**應用程式內容**連結。
   - 在節點的內容功能表中選擇**應用程式內容**。

   開啟"**應用程式內容**"視窗。
2. 選擇"**故障診斷**"標籤。
3. 在"**故障診斷設定**"塊中，點擊"**設定**"按鈕。
   開啟"**故障診斷設定**"視窗。
4. 選取「傾印設定」索引標籤：
   - **應用程式傾印設定**Kaspersky Embedded Systems Security 會記錄應用程式的所有傾印。
   - **應用程式主控台傾印設定**如果應用程式主控台和 Kaspersky Embedded Systems Security 安裝在不同的電腦上，則您只能記錄應用程式主控台的傾印。
5. 使用"**建立傾印檔案**"核取方塊可以啟用或停用對應用程式操作的追蹤。
   預設情況下，記憶體傾印記錄功能處於停用狀態。

6. 如有必要，請變更 Kaspersky Embedded Systems Security 儲存偵錯檔案的預設資料夾。為此，請點擊 **瀏覽** 按下按鈕並選擇所需的資料夾。

   該資料夾必須提前建立並且可由系統帳戶寫入。您無法指定網路資料夾、磁碟機或環境變數。

7. 儲存變更。

如何在卡巴斯基安全管理中心網頁主控台中啟用或停用記憶體傾印記錄

1. 在網頁主控台的主視窗中，選擇**資產管理 → 政策**。
2. 點擊 Kaspersky Embedded Systems Security 政策的名稱。
   政策內容視窗將開啟。
3. 選擇"**應用程式設定**"標籤。
4. 選擇 **故障診斷** 部分。
5. 在"**傾印檔案設定**"塊中，使用"**建立傾印檔案**"核取方塊來啟用或停用追蹤應用程式操作。
   預設情況下，記憶體傾印記錄功能處於停用狀態。
6. 如有必要，請變更 Kaspersky Embedded Systems Security 儲存偵錯檔案的預設資料夾。為此，請在**傾印檔案資料夾（資料夾的完整路徑，例如 C:\\Dumps\\）**欄位中指定本機資料夾的完整路徑。

   該資料夾必須提前建立並且可由系統帳戶寫入。您無法指定網路資料夾、磁碟機或環境變數。

7. 儲存變更。

您也可以在小型診斷介面中啟用或停用記憶體傾印記錄。

防護傾印檔案和偵錯檔案

傾印檔案和偵錯檔案包含作業系統的資訊，可能還包含使用者資料。為了防止未經授權地存取此類資料，您可以啟用防護傾印檔案和偵錯檔案。

如果啟用了傾印檔案和偵錯檔案的防護，則以下使用者可以存取這些檔案：

- 系統管理員和本機管理員以及啟用寫入傾印檔案和偵錯檔案的使用者可以存取傾印檔案。
- 只有系統管理員和本機管理員可以存取偵錯檔案。

如何在卡巴斯基安全管理中心管理主控台中啟用對傾印檔案和偵錯檔案的防護

1. 在網頁主控台的主視窗中，選擇**資產管理 → 政策**。
2. 點擊 Kaspersky Embedded Systems Security 政策的名稱。
   政策內容視窗將開啟。
3. 選擇"**應用程式設定**"標籤。

4. 選擇 **故障診斷** 部分。
5. 使用**"啟用傾印和偵錯檔案防護"**核取方塊可以啟用或停用對傾印檔案和偵錯檔案的防護。
6. 儲存變更。

1. 在卡巴斯基安全管理中心管理主控台樹狀目錄中，選取**政策**。
2. 選擇必要的政策並點擊以開啟政策內容。
3. 在政策內容視窗中，轉至「**故障診斷**」區域。
4. 在**"故障診斷設定"**塊中，點擊**"設定"**按鈕。
5. 開啟**"故障診斷設定"**視窗。
6. 使用**"啟用傾印和偵錯檔案防護"**核取方塊可以啟用或停用對傾印檔案和偵錯檔案的防護。
7. 儲存變更。

如何在應用程式主控台中啟用對傾印檔案和偵錯檔案的防護

1. 在應用程式主控台樹狀目錄中，選擇**"Kaspersky Embedded Systems Security"**節點並執行以下操作之一：
   - 在節點的結果窗格中，點擊**應用程式內容**連結。
   - 在節點的內容功能表中選擇**應用程式內容**。

   開啟**"應用程式內容"**視窗。
2. 選擇**"故障診斷"**標籤。
3. 在**"故障診斷設定"**塊中，點擊**"設定"**按鈕。
   開啟**"故障診斷設定"**視窗。
4. 使用**"啟用傾印和偵錯檔案防護"**核取方塊可以啟用或停用對傾印檔案和偵錯檔案的防護。
5. 儲存變更。

您也可以在小型診斷介面中啟用或停用對傾印檔案和偵錯檔案的防護。

防護有效期間寫入的傾印檔案和偵錯檔案即使該功能被停用也會保持為防護狀態。

取得作業系統資料 (Kaspersky Get System Info)

安裝 Kaspersky Embedded Systems Security 應用程式後，作業系統或應用程式可能無法正常運作。應用程式與電腦元件的軟體或驅動程式之間存在衝突。

為了確定問題的原因，卡巴斯基技術支援需要 Kaspersky Get System Info 實用程式（以下簡稱 GSI）的報告。有關使用該實用程式的詳細資訊，請參閱 卡巴斯基知識庫。

有關 Kaspersky Embedded Systems Security 的資訊來源

您可以使用以下來源尋找有關 Kaspersky Embedded Systems Security 的資訊：

- Kaspersky 網站上的 Kaspersky Embedded Systems Security 頁面
- 技術支援網站（知識庫）上的 Kaspersky Embedded Systems Security 頁面
- 線上說明
- 在論壇上討論應用程式

若要使用 Kaspersky 網站資訊來源，您必須連線網際網路。

在不支援現代加密通訊協定的瀏覽器中，可能無法檢視線上說明。

如果您有無法自行排除的問題，請與 卡巴斯基技術支援 聯絡。

Kaspersky 網站上的 Kaspersky Embedded Systems Security 頁面

在 Kaspersky Embedded Systems Security 頁面 上，您可以檢閱有關應用程式及其功能和特色的一般資訊。

Kaspersky Embedded Systems Security 頁面包含指向線上商店的連結。您可以在此購買或續約產品授權。

知識庫中的 Kaspersky Embedded Systems Security 頁面

知識庫是技術支援網站的區段。

在知識庫 中的 Kaspersky Embedded Systems Security 頁面上，您可以找到文章，這些文章提供實用的資訊、建議以及有關如何購買、安裝和使用程式的常見問題解答。

知識庫文章不僅可以解答與 Kaspersky Embedded Systems Security 有關的問題，而且還可以解答與其他 Kaspersky 應用程式有關的問題。它們還可能包含來自技術支援服務的新聞。

Kaspersky Embedded Systems Security 說明

線上說明包含有關配置和使用 Kaspersky Embedded Systems Security 的資訊。

在論壇上討論應用程式

如果您的問題不需要緊急回答，您可以在我們的論壇上與卡巴斯基專家和其他使用者討論。

在論壇中，您可以檢視現有主題、發表自己的評論以及建立新的討論主題。

附錄

本節包含的資訊是對文件本文的補充。

用於快速掃描的檔案副檔名

com – 大小不超過 64 KB 的應用程式的可執行檔

exe – 可執行檔或自解壓存檔

sys – Microsoft Windows 系統檔案

prg – dBase™ 程式文字、Clipper 或 Microsoft Visual FoxPro®，或 WAVmaker 程式

bin – 二進位檔案

bat – 批次檔案

cmd – Microsoft Windows NT 的指令檔案（相似於 DOS 的 bat 檔案）、OS/2

dpl – 壓縮的 Borland Delphi 庫

dll – 動態連結程式庫

scr – Microsoft Windows 屏保

cpl – Microsoft Windows 控制台模組

ocx – Microsoft OLE（物件連結和嵌入）物件

tsp – 以分時模式執行的程式

drv – 裝置驅動程式

vxd – Microsoft Windows 虛擬裝置驅動程式

pif – 程式資訊檔案

lnk – Microsoft Windows 連結檔案

reg – Microsoft Windows 系統登錄機碼檔案

ini – 包含 Microsoft Windows、Windows NT 和某些應用程式配置資料的設定檔

cla – Java 類

vbs – Visual Basic® 指令碼

vbe – BIOS 影片延伸程式

js, jse – JavaScript source text

htm – 超文字文件

htt – Microsoft Windows 超文字標頭

hta – Microsoft Internet Explorer® 超文字程式

asp – Active Server Pages 指令碼

chm – 編譯的 HTML 檔案

pht – 帶有 PHP 指令碼的 HTML 檔案

php – 集成到 HTML 檔案的指令碼

wsh – Microsoft Windows Script Host 檔案

wsf – Microsoft Windows 指令碼

the – Microsoft Windows 95 桌面壁紙檔案

hlp – Win 說明檔案

msg – Microsoft Mail 郵件

plg – 郵件

mbx – 已儲存的 Microsoft Office Outlook 郵件

doc* – Microsoft Office Word 文件，例如：doc（Microsoft Office Word 文件）、docx（帶 XML 支援的 Microsoft Office Word 2007 文件）、docm（帶巨集支援的 Microsoft Office Word 2007 文件）

dot* – Microsoft Office Word 文件模組，例如 dot（Microsoft Office Word 文件範本）、dotx（Microsoft Office Word 2007 文件範本）、dotm（帶巨集支援的 Microsoft Office Word 2007 文件範本）

fpm – 資料庫程式、Microsoft Visual FoxPro 開機檔案

rtf – 富文字格式文件

shs – Windows Shell Scrap Object Handler 片段

dwg – AutoCAD® 圖紙資料庫

msi – Microsoft Windows Installer 安裝套件

otm – 適用於 Microsoft Office Outlook 的 VBA 項目

pdf – Adobe Acrobat 文件

swf – Shockwave® Flash 封包文件

jpg, jpeg – 壓縮影像格式

emf – 增強元檔案格式檔案；

ico – 物件圖示檔案

ov? – Microsoft Office Word 可執行檔

xl* – Microsoft Office Excel 文件和檔案，例如：xla 對應 Microsoft Office Excel、xlc 對應圖表、xlt 對應文件範本、xlsx 對應 Microsoft Office Excel 2007 工作簿、xltm 對應支援巨集的 Microsoft Office Excel 2007 工作簿、xlsb 對應二進位格式（非 XML）的 Microsoft Office Excel 2007 工作簿、xltx 對應於 Microsoft Office Excel 2007 範本、xlsm 對應於支援巨集的 Microsoft Office Excel 2007 範本、xlam 對應於支援巨集的 Microsoft Office Excel 2007 外掛程式

pp* – Microsoft Office PowerPoint® 文件和檔案，例如：pps 代表 Microsoft Office PowerPoint 幻燈片、ppt 代表幻燈片、pptx 代表 Microsoft Office PowerPoint 2007 幻燈片、pptm 代表支援巨集的 Microsoft Office PowerPoint 2007 幻燈片、potx 代表 Microsoft Office PowerPoint 2007 幻燈片範本、potm 代表支援巨集的 Microsoft Office PowerPoint 2007 幻燈片、ppsx 代表 Microsoft Office PowerPoint 2007 幻燈片、ppsm 代表支援巨集的 Microsoft Office PowerPoint 2007 幻燈片、ppam 代表支援巨集的 Microsoft Office PowerPoint 2007 外掛程式

md* – Microsoft Office Access® 文件和檔案，例如：mda 代表 Microsoft Office Access 工作群組，mdb 代表資料庫

sldx – Microsoft PowerPoint 2007 幻燈片

sldm – 支援巨集的 Microsoft PowerPoint 2007 幻燈片

thmx – Microsoft Office 2007 主旨

應用程式元件規則中的使用者帳戶

要配置某些應用程式元件，您需要新增特殊規則，您可以在其中選擇應用程式將為其套用規則的使用者。

必須新增規則來配置以下應用程式元件：

- 應用程式啟動控制
- 裝置控制
- 行為偵測
- 系統完整性監控

您可以透過以下方式新增使用者：

- 從 Active Directory 中選擇（建議）
- 從卡巴斯基安全管理中心使用者清單中選擇
- 手動新增

卡巴斯基建議僅在無法使用網域使用者帳戶的特殊情況下使用本機使用者帳戶。使用本機帳戶的安全風險請參見微软知識庫。如果使用本機使用者帳戶，您將對電腦的安全承擔全部責任；特別是，這包括控制和限制對應用程式設定進行存取的責任。

應用程式使用使用者的 SID（安全識別符）來識別使用者。當使用 Active Directory 或卡巴斯基安全管理中心使用者清單中的使用者帳戶時，應用程式會確定管理伺服器上的 SID。這意味著應用程式不會為了識別使用者而給電腦帶來額外負載。如果您向應用程式規則新增了超過 1000 個本機使用者帳戶，應用程式將聯絡網域控制器來識別使用者。這意味著電腦的負載增加了。為了最佳化對電腦效能的影響，我們建議使用 Active Directory 或卡巴斯基安全管理中心使用者清單中的使用者帳戶。

Kaspersky Embedded Systems Security 支援規則中的嵌入式使用者和群組帳戶（例如"Everyone"群組）。由於使用者 SID 偵測的特殊性，應用程式僅允許使用從 Active Directory 或卡巴斯基安全管理中心使用者清單新增的嵌入式帳戶。手動新增嵌入式帳戶的規則不起作用。

法律資訊

資料提供

本節包含有關 Kaspersky Embedded Systems Security 應用程式可能儲存在裝置上並在運行期間自動傳輸給卡巴斯基的資料的資訊。

Kaspersky 將根據法律和 Kaspersky 應用程式管理規定防護收到的資訊。資料透過加密的通訊通道傳輸。

在最終使用者產品授權協議下的資料提供

Kaspersky Embedded Systems Security 的產品授權協議（特別是"資料處理條款"部分）指定了本手冊中指示的傳送和處理資料的條款、責任及過程。在接受產品授權協議前，請仔細檢視其條款以及產品授權協議連結到的所有文件。

Kaspersky 在您使用應用程式時收到的資料受到防護並按照隱私政策 www.kaspersky.com/Products-and-Services-Privacy-Policy 進行處理。

產品授權協議和隱私政策的條款在 Kaspersky Embedded Systems Security 安裝期間作為分發套件的一區段提供，在安裝後可以從**開始**功能表（**所有程式** > **Kaspersky Embedded Systems Security** > **EULA 和隱私政策**）存取。

移除 Kaspersky Embedded Systems Security 期間，Kaspersky Embedded Systems Security 在受防護裝置上儲存的所有資料都將被刪除。

接受最終使用者產品授權協議的條款，即表示您同意自動將以下資料傳送到 Kaspersky：

- 為支援接收更新的機制 — 有關已安裝的應用程式及其啟動的資訊：已安裝的應用程式及其完全版本的識別碼，包括內部版本號、類型以及產品授權識別碼、安裝識別碼、更新工作識別碼。
- 為在應用程式出錯時使用導航到知識庫文章的功能（重定向器服務）：有關應用程式和連結類型的資訊，具體為：名稱、區域設定以及應用程式的完全版本號、重定向連結的類型和錯誤識別碼。
- 為管理資料處理的確認：有關產品授權協議和規定了資料傳輸條款的其他文件的接受狀態的資訊：產品授權協議或其他文件（接受或拒絕作為其一部分的資料處理條款）的識別碼和版本；表示使用者操作（確認或撤銷接受條款）的內容；資料處理條款接受的狀態變更的日期和時間。

本機資料處理

在執行本手冊所述的應用程式主要功能時，Kaspersky Embedded Systems Security 會在受防護裝置上本機處理和儲存一組資料。

下表包含有關 Kaspersky Embedded Systems Security 對報告中包含的資料進行本機處理和儲存的資訊。

功能區域	事件註冊
使用類型	Kaspersky Embedded Systems Security 本機儲存資料，並將資料傳送到管理伺服器。管理伺服器的資料庫儲存有關在受管理之受防護裝置上發生的應用程式事件的資訊。
儲存	• %ALLUSERSPROFILE%\Kaspersky Lab\Kaspersky Security for Windows Server\<產品版本>\Reports • %SystemRoot%\System32\Winevt\Logs\Kaspersky Security.evtx • 管理伺服器的資料庫
安全措施	存取控制清單。
儲存期間	Kaspersky Embedded Systems Security 將一直儲存資料，直到移除 Kaspersky Embedded Systems Security 為止。 移除 Kaspersky Embedded Systems Security 期間，Kaspersky Embedded Systems Security 在受防護裝置上儲存的所有資料都將被刪除。
用途	提供主要功能。

Kaspersky Embedded Systems Security 不會刪除 Windows 事件記錄中的事件，包括在解除安裝 Kaspersky Embedded Systems Security 期間發生的事件。

為提供事件註冊功能，Kaspersky Embedded Systems Security 會在本機處理以下資料：

- 所處理檔案的名稱、總和檢查碼（MD5、SHA-256）和屬性，以及它們在被掃描媒體上的完整路徑。
- Kaspersky Embedded Systems Security 對掃描的檔案所採取的操作。
- 對受防護裝置上的被掃描檔案採取的使用者操作。
- 有關對受防護網路或受保防護裝置執行任何操作的使用者帳戶的資訊。
- 新增到裝置控制規則中之裝置的裝置實例路徑值。
- 有關系統上執行的處理程序和指令碼的資訊：可執行檔案的總和檢查碼（MD5、SHA-256）以及完整路徑，有關數位憑證的資訊。
- Windows 防火牆設定。
- Windows 事件記錄項目。
- 對受防護裝置上的被掃描檔案採取操作的使用者帳戶名稱。
- 正在啟動的可執行檔案實例，以及這些檔案的類型、名稱、總和檢查碼和屬性。
- 有關網路活動的資訊：
  - 被封鎖的外部裝置 IP 位址。
  - 處理的 IP 位址。
- 有關 Windows USN 記錄狀態的資訊。

下表包含有關 Kaspersky Embedded Systems Security 處理的服務資料資訊。服務資料包括：程式參數、隔離檔案和備份檔案、程式服務資料庫中的資訊、產品授權資料。

下表包含有關 Kaspersky Embedded Systems Security 對使用者指定之參數的資料進行本機處理和儲存的資訊。

功能區域	所有 Kaspersky Embedded Systems Security 功能
使用類型	Kaspersky Embedded Systems Security 本機儲存資料，並將資料傳送到管理伺服器。資料儲存在管理伺服器的資料庫中。 應用程式本機處理的資料不會自動傳送到 Kaspersky 或其他協力廠商系統。
儲存	• %ALLUSERSPROFILE%\Kaspersky Lab\Kaspersky Security for Windows Server\<產品版本>\ • 管理伺服器的資料庫
安全措施	存取控制清單。
處理週期	Kaspersky Embedded Systems Security 將一直儲存資料，直到移除 Kaspersky Embedded Systems Security 為止。 移除 Kaspersky Embedded Systems Security 期間，Kaspersky Embedded Systems Security 在受防護裝置上儲存的所有資料都將被刪除。 Kaspersky Embedded Systems Security 不會刪除匯出到設定檔中之參數的資料。 如果在安裝精靈中選中"**匯出隔離物件** 和 **匯出備份物件**"核取方塊，則 Kaspersky Embedded Systems Security 不會刪除隔離物件和備份物件。
用途	提供主要功能。

為達指定目的，Kaspersky Embedded Systems Security 在本機處理並儲存以下資料：

- 隔離區或備份區中放置的物件。
- 有關 Kaspersky Embedded Systems Security 執行工作所使用的使用者帳戶的資訊（使用者名稱和密碼）。
- Kaspersky Embedded Systems Security 密碼。
- 已封鎖的登入工作階段的 IP 位址和識別碼。
- Windows 防火牆設定和 Windows 防火牆規則設定。
- 新增到"應用程式啟動控制"規則中的可執行檔案的總和檢查碼（MD5、SHA-256）和路徑。
- 新增到裝置控制規則中之裝置的裝置實例路徑值。
- 有關包括在 Kaspersky Embedded Systems Security 工作範圍中的檔案和資料夾的資訊。
- 防護範圍中包括或排除的 IP 位址。
- 有關 Windows 事件記錄中的事件資訊。
- 有關使用 iSwift 或 iChecker 技術進行的偵測資訊。
- 排除設定中指定的總和檢查碼（MD5、SHA-256）、完整路徑和遮罩。
- 有關新增到信任區域中的處理程序資訊。
- 有關已新增的產品授權金鑰的資訊。
- 有關數位憑證的資訊。
- 在掃描過程中從壓縮檔案或其他複合物件中解壓縮的檔案。

作為應用程式基本功能的一部分，Kaspersky Embedded Systems Security 處理並儲存資料，包括記錄應用程式事件和接收診斷資料。本機處理的資料按照配置和應用的應用程式設定進行防護。

Kaspersky Embedded Systems Security 可讓您設定本機處理的資料的防護等級。您可以變更存取處理程序資料的使用者權限，變更此類別資料的資料保留期，完全或部分停用涉及資料記錄的功能，以及變更磁碟機上用於記錄資料的資料夾的路徑和內容。

應用程式本機處理的資料不會自動傳送到 Kaspersky 或其他協力廠商系統。

預設情況下，從受防護裝置解除安裝 Kaspersky Embedded Systems Security 後，將移除該應用程式執行期間本機處理的所有資料。

包含診斷資訊（追蹤和傾印檔案）的檔案、Windows 事件記錄中的應用程式事件以及包含已匯出 Kaspersky Embedded Systems Security 設定的檔案除外。我們建議您手動刪除這些檔案。

有關處理包含應用程式偵錯資料的檔案的詳細資訊，請參閱本手冊的相應章節。

您可以使用標準作業系統工具刪除包含 Kaspersky Embedded Systems Security 應用程式事件的 Windows 事件記錄檔案。

透過應用程式協助元件處理本機資料

Kaspersky Embedded Systems Security 安裝套件包含應用程式協助元件，這些協助元件可以安裝在裝置上，即使該裝置未安裝 Kaspersky Embedded Systems Security。這些協助元件為：

- 應用程式主控台。此元件是 Microsoft 管理主控台管理單元。
- 管理外掛程式。該元件提供與卡巴斯基安全管理中心應用程式的完全整合。

當執行本手冊所述的主要應用程式功能時，應用程式協助元件本機處理一群組資料並將資料儲存在安裝了這些元件的受防護裝置上，即使它們與 Kaspersky Embedded Systems Security 分開安裝也是如此。

這些應用程式元件本機處理並儲存以下資料：

- 應用程式主控台：應用程式主控台上次遠端連線到的安裝了 Kaspersky Embedded Systems Security 的受防護裝置的名稱（IP 位址或網域名稱）；在 Microsoft 管理主控台管理單元中配置的顯示參數；使用者上次透過應用程式主控台在其中選擇了物件（使用按一下**瀏覽**按鈕開啟的系統對話方塊）的資料夾的相關資料。應用程式主控台偵錯檔案還可能包含以下資料：建立了遠端連線的安裝了 Kaspersky Embedded Systems Security 應用程式的受防護裝置的名稱，以及用於建立遠端連線的使用者帳戶的名稱。
- 管理外掛程式可以處理和暫時儲存 Kaspersky Embedded Systems Security 處理的資料；例如，應用程式工作和元件的配置設定、卡巴斯基安全管理中心政策的設定、網路清單中傳送的資料。

下表包含有關 Kaspersky Embedded Systems Security 對寫入 Dump 和偵錯檔案的資料進行本機處理和儲存的資訊。

Kaspersky Embedded Systems Security 本機處理並儲存以下寫入 Dump 和偵錯檔案的資料：

- 有關 Kaspersky Embedded Systems Security 對受防護裝置執行的操作資訊。
- 有關 Kaspersky Embedded Systems Security 處理的物件資訊。
- 有關 Kaspersky Embedded Systems Security 處理的受防護裝置上的活動資訊。
- 有關 Kaspersky Embedded Systems Security 執行期間發生的錯誤資訊。

協助元件處理的資料不會自動傳送到 Kaspersky 或其他協力廠商系統。

預設情況下，在移除這些應用程式協助元件後，這些元件在執行期間本機處理的資料都將被刪除。

輔助應用程式元件的偵錯檔案除外。我們建議您手動刪除這些檔案。

偵錯和 Dump 檔案中的資料

Kaspersky Embedded Systems Security 可以根據設定在 Kaspersky Embedded Systems Security 執行期間將診斷資訊寫入偵錯檔案，以供技術支援之用。

Kaspersky Embedded Systems Security 的 Dump 檔案由作業系統在應用程式當機期間產生，並在下次當機時被覆蓋。

偵錯和 Dump 檔案可以包括使用者的任何個人資料或組織的機密資料。

請勿在組織政策禁止提交資料的裝置上使用 Kaspersky Embedded Systems Security。

預設情況下，Kaspersky Embedded Systems Security 不記錄所有診斷資訊。

偵錯和 Dump 檔案不會在產生它們的主機之外自動提交。可以使用標準文字檔案檢視器檢視偵錯檔案的內容。偵錯和 Dump 檔案將無限期保留，並且在移除 Kaspersky Embedded Systems Security 時不會被刪除。

診斷資訊對於技術支援很有用。

未提供特殊機制來限制對偵錯和 Dump 檔案的存取。管理員可以將此資料配置為寫入受防護資料夾。

預設情況下，不會配置偵錯和 Dump 檔案資料夾的路徑。要使用偵錯和 Dump 資料夾，管理員必須指定它。

偵錯和 Dump 檔案中的資料可以包含：

- 有關 Kaspersky Embedded Systems Security 對受防護裝置執行的操作資訊。
- 有關 Kaspersky 端點代理處理的物件資訊。
- Kaspersky 端點代理執行期間出現的錯誤。

使用卡巴斯基安全網路時的資料提供

Kaspersky Embedded Systems Security 傳送到 Kaspersky 的資料集合取決於產品授權的類型和卡巴斯基安全網路使用設定。

經產品授權在不超過 4 台電腦上使用 KSN

同意卡巴斯基安全網路聲明，表示您同意自動傳送以下資訊：

- 有關 KSN 配置更新的資訊：活動配置的識別碼、收到的配置的識別碼、配置更新的錯誤代碼；
- 有關要掃描的檔案和 URL 位址的資訊：所掃描檔案的核對總和 (MD5、SHA2-256、SHA1) 和檔案模式 (MD5)，模式大小，偵測到的威脅的類型及其在權利所有人分類中的名稱，病毒資料庫的識別碼，其信譽被請求的 URL 位址，以及引用頁 URL 位址，連線協定的識別碼和使用的連接埠號；
- 偵測到威脅的掃描工作的 ID；
- 有關需要用來驗證真實性的數位憑證的資訊：用於對掃描的物件進行簽章的憑證的核對總和 (SHA256) 以及憑證的公開金鑰；
- 執行掃描的軟體元件的識別碼；
- 病毒資料庫的 ID 以及這些病毒資料庫中的記錄的 ID；
- 有關電腦上的軟體啟動的資訊：來自啟動服務的已簽章票證頭（區域啟動中心的識別碼、啟動碼的核對總和、票證的核對總和、票證建立日期、票證的唯一識別碼、票證版本、產品授權狀態、票證有效期的開始/結束日期和時間、產品授權的唯一識別碼、產品授權版本），用於對票證頭簽章的憑證的識別碼，金鑰檔案的核對總和 (MD5)；
- 有關權利所有人的軟體的資訊：完整版本，類型，用於連線到 Kaspersky 服務的協定的版本。

經產品授權在 5 台或更多電腦上使用 KSN

同意卡巴斯基安全網路聲明，表示您同意自動傳送以下資訊：

如果選中“**卡巴斯基安全網路**”核取方塊並且清除“**啟用延伸 KSN 模式**”核取方塊，則應用程式會傳送以下資訊：

- 有關 KSN 配置更新的資訊：活動配置的識別碼、收到的配置的識別碼、配置更新的錯誤代碼；
- 有關要掃描的檔案和 URL 位址的資訊：所掃描檔案的核對總和 (MD5、SHA2-256、SHA1) 和檔案模式 (MD5)，模式大小，偵測到的威脅的類型及其在權利所有人分類中的名稱，病毒資料庫的識別碼，其信譽被請求的 URL 位址，以及引用頁 URL 位址，連線協定的識別碼和使用的連接埠號；
- 偵測到威脅的掃描工作的 ID；
- 有關需要用來驗證真實性的數位憑證的資訊：用於對掃描的物件進行簽章的憑證的核對總和 (SHA256) 以及憑證的公開金鑰；
- 執行掃描的軟體元件的識別碼；
- 病毒資料庫的 ID 以及這些病毒資料庫中的記錄的 ID；

- 有關電腦上的軟體啟動的資訊：來自啟動服務的已簽章票證頭（區域啟動中心的識別碼、啟動碼的核對總和、票證的核對總和、票證建立日期、票證的唯一識別碼、票證版本、產品授權狀態、票證有效期的開始/結束日期和時間、產品授權的唯一識別碼、產品授權版本），用於對票證頭簽章的憑證的識別碼，金鑰檔案的核對總和 (MD5)；

- 有關權利所有人的軟體的資訊：完整版本，類型，用於連線到 Kaspersky 服務的協定的版本。

如果除了**"卡巴斯基安全網路"**核取方塊之外，還選擇了**"啟用延伸 KSN 模式"**核取方塊，則除了上面列出的資訊之外，應用程式還會傳送以下資訊：

- 有關對請求的包含主機的被處理 URL 和 IP 位址的 Web 資源進行分類的結果的資訊，執行分類的軟體元件的版本，分類方法，以及針對 Web 資源定義的類別集；

- 有關電腦上安裝的軟體的資訊：軟體應用程式和軟體供應商的名稱，登錄機碼及其值，已安裝的軟體元件的檔案資訊（核對總和（MD5、SHA2-256、SHA1）、名稱、檔案在電腦上的路徑、大小、版本和數位簽章）；

- 有關電腦的病毒防護狀態的資訊：正在使用的病毒資料庫的版本和發行時間戳記，工作的 ID 和執行掃描的軟體的 ID；

- 有關最終使用者正在下載的檔案的資訊：下載的檔案和下載頁的 URL 和 IP 位址，下載協議識別符和連線連接埠號，表示 URL 是否為惡意的狀態，檔案的屬性、大小和核對總和（MD5、SHA2-256、SHA1），下載檔案的處理程序的相關資訊（核對總和（MD5、SHA2-256、SHA1）、建立/構建日期和時間、自動執行狀態、內容、封裝程式的名稱、簽章資訊、可執行檔標誌、格式識別符和熵），檔案名稱及其在電腦上的路徑，檔案的數位簽章及其產生時的時間戳記，發生偵測的 URL 位址，頁面上看上去可疑或有害的指令碼的編號，有關產生的 HTTP 請求以及對它們的回應的資訊；

- 有關正在執行的應用程式及其模組的資訊：系統中正在執行的處理程序的資料（處理程序 ID (PID)，處理程序名稱，有關啟動處理程序的帳戶的資訊，啟動處理程序的應用程式和指令，受信任程式或處理程序的標誌，處理程序檔案的完整路徑及其核對總和（MD5、SHA2-256、SHA1），啟動命令列，處理程序完整性等級，處理程序所屬產品的敘述（產品名稱和發佈者詳細資訊），以及所使用的數位憑證和驗證它們的真實性所需的資訊或者關於是否缺少檔案數位簽章的資訊），以及有關載入到處理程序中的模組的資訊（模組的名稱、大小、類型、建立日期、內容、核對總和（MD5、SHA2-256、SHA1）以及在電腦上的路徑），PE 檔案頭資訊，封裝程式的名稱（如果檔案已封裝）；

- 有關所有潛在惡意物件和活動的資訊：偵測到的物件的名稱，電腦上物件的完整路徑，所處理檔案的核對總和（MD5、SHA2-256、SHA1），偵測日期和時間，感染檔案的名稱、大小和路徑，路徑範本代碼，可執行檔標誌，表示物件是否為容器的指示器，封裝程式名稱（如果檔案已封裝），檔案類型代碼，檔案格式 ID，惡意軟體執行的操作清單以及軟體和使用者針對其做出的回應決策，病毒資料庫的 ID 和這些病毒資料庫中用於制定決策的記錄的 ID，潛在惡意物件的指示器，偵測到的威脅在權利所有人分類中的名稱，危險等級，偵測狀態和偵測方法，包含在已分析上下文中的原因及上下文中檔案的序號，核對總和（MD5、SHA2-256、SHA1），用於傳送感染訊息或連結的應用程式的可執行檔的名稱和內容，被封鎖物件的主機的去個性化 IP 位址（IPv4 和 IPv6），檔案熵，檔案自動執行指示器，在系統中首次偵測到檔案的時間，上次傳送統計資訊後檔案被執行的次數，透過其收到惡意物件的郵件用戶端的名稱、核對總和（MD5、SHA2-256、SHA1）和大小，執行掃描的軟體工作的 ID，表示檔案信譽或簽章是否經過檢查的指示器，檔案處理結果，為物件收集的模式的核對總和 (MD5)，模式大小（以位元組為單位），以及使用的偵測技術的技術規格；

- 有關掃描的物件的資訊：檔案移入或移出的指定信任群組，將檔案移入該類別的理由，類別識別符，有關類別源的資訊和類別資料庫版本，檔案的受信任憑證標誌，檔案的供應商名稱，檔案版本，包含該檔案的軟體應用程式的名稱和版本；

- 有關偵測到的弱點的資訊：弱點資料庫中的弱點 ID，弱點危險等級；

- 有關可執行檔類比的資訊：檔案大小及其核對總和（MD5、SHA2-256、SHA1），模擬元件的版本，模擬深度，類比過程中獲得的邏輯塊內的一系列內容和函數，可執行檔的 PE 頭中的資料；

- 發起攻擊的電腦的 IP 位址（IPv4 和 IPv6），被當作網路攻擊目的的電腦連接埠號，包含攻擊的 IP 封包的協定的識別符，攻擊目的（組織名稱、網站），攻擊響應標記，攻擊的權重，信任等級；

- 有關與欺詐網路資源相關的攻擊的資訊，所存取網站的 DNS 和 IP 位址（IPv4 和 IPv6）；

- 請求的 Web 資源的 DNS 和 IP 位址（IPv4 或 IPv6），有關存取該 Web 資源的檔案和 Web 用戶端的資訊，檔案的名稱、大小和核對總和（MD5、SHA2-256、SHA1），檔案的完整路徑和路徑範本代碼，檢查其數位簽章的結果，及其在 KSN 中的狀態；

- 有關惡意軟體操作回溯的資訊：有關其活動被回溯的檔案的資料（檔案名稱、檔案的完整路徑、檔案的大小和核對總和（MD5、SHA2-256、SHA1）），有關刪除、重命名和複製檔案以及還原登錄檔中的值（登錄機碼的指令和值）的成功和失敗操作的資料，有關惡意軟體修改的系統檔案的資訊（回溯前後）；

- 有關為適應性異常控制元件設定的排除項目的資訊：觸發的規則的 ID 和狀態，觸發規則時軟體執行的操作，處理程序或執行緒執行可疑活動時所用的使用者帳戶的類型，有關執行可疑活動或受可疑活動支配的處理程序的資訊（指令碼 ID 或處理程序檔案名稱，處理程序檔案的完整路徑，路徑範本代碼，處理程序檔案的總和檢查碼（MD5、SHA2-256、SHA1））；有關執行了可疑操作的物件的資訊以及受可疑活動支配的物件的資訊（登錄機碼名稱或檔案名稱，檔案的完整路徑，路徑範本代碼和檔案的總和檢查碼（MD5、SHA2-256、SHA1））。

- 有關載入的軟體模組的資訊：模組檔案的名稱、大小和核對總和（MD5、SHA2-256、SHA1），模組檔案的完整路徑和路徑範本代碼，模組檔案的數位簽章設定，簽章建立資料和時間，為模組檔案簽章的主體和組織的名稱，載入模組的處理程序的 ID，模組供應商的名稱，以及載入佇列中模組的序號；

- 有關軟體與 KSN 服務的互動品質的資訊：產生統計資訊的時間段的開始和結束日期及時間，有關對所用的每個 KSN 服務的請求和連線的品質的資訊（KSN 服務 ID，成功請求數量，含有來自快取的回應的請求數量，不成功請求數量（網路問題、軟體設定中停用 KSN、路由不正確），成功請求的時間分佈，取消的請求的時間分佈，超出時間限制的請求的時間分佈，與取自快取的 KSN 的連線數，與 KSN 的成功連線數，與 KSN 的不成功連線數，成功事務數，不成功事務數，與 KSN 的成功連線的時間分佈，與 KSN 的不成功連線的時間分佈，成功事務的時間分佈，不成功事務的時間分佈）；

- 如果偵測到潛在惡意物件，將提供處理程序的記憶體中的資料的相關資訊：系統物件階層架構 (ObjectManager) 的元素、UEFI BIOS 記憶體中的資料、登錄機碼的名稱及其值；

- 有關系統記錄中的事件的資訊：事件的時間戳記，在其中發現事件的記錄的名稱，事件的類型和類別，事件來源的名稱和事件的敘述；

- 有關網路連線的資訊：啟動了開啟連接埠的處理程序的檔案的版本和核對總和（MD5、SHA2-256、SHA1），處理程序檔案的路徑和數位簽章，本機和遠程 IP 位址，本機和遠程連線連接埠號，連線狀態，連接埠開啟時間戳記；

- 有關在電腦上安裝和啟動軟體的日期的資訊：出售產品授權的合作夥伴的 ID，產品授權的序列號，來自啟動服務的票證的簽章標頭（區域啟動中心的 ID，啟動碼的總和檢查碼，票證的總和檢查碼，票證的建立日期，票證的唯一 ID，票證版本，產品授權狀態，票證的開始/結束日期和時間，產品授權的唯一 ID，產品授權版本），用於簽署票頭的憑證的 ID，金鑰檔案的總和檢查碼（MD5），電腦上軟體安裝的唯一ID，要更新的應用程式的類型和 Id，更新工作的 ID；

- 有關所有已安裝的更新集的資訊以及最近安裝/刪除的更新集的資訊，導致傳送更新資訊的事件的類型，上次安裝更新後經過的時間，有關任何目前已安裝的病毒資料庫的資訊；

- 有關電腦上的軟體執行的資訊：CPU 使用率資料，記憶體使用率資料（專用位元組，未分頁緩衝集區，分頁緩衝集區），軟體處理程序中的活動執行緒數和掛起執行緒數，以及錯誤發生前的軟體執行時間；

- 自軟體安裝以來和上次更新以來軟體轉儲和系統轉儲 (BSOD) 的次數，當機的軟體模組的識別符和版本，軟體處理程序中的記憶體堆疊，以及當機時的病毒資料庫的相關資訊；

- 有關系統轉儲 (BSOD) 的資料：指示電腦上發生 BSOD 的標誌，導致 BSOD 的驅動程式的名稱，驅動程式中的位址和記憶體堆疊，指示發生 BSOD 之前作業系統連線持續時間的標誌，當機的驅動程式的記憶體堆疊、儲存的記憶體傾印的類型，指示 BSOD 之前作業系統連線持續 10 分鐘以上的標誌、轉儲的唯一識別符，BSOD 的時間戳記；

- 有關軟體元件執行期間出現的錯誤或效能問題的資訊：軟體的狀態 ID，錯誤類型，代碼和原因以及發生錯誤的時間，元件的 ID，出現錯誤的產品的元件、模組和處理程序的 ID，出現錯誤的工作或更新類別的 ID，軟體使用的驅動程式的記錄（錯誤代碼、模組名稱、原始檔案的名稱和出現錯誤的列）；

- 有關病毒資料庫和軟體元件更新的資訊：在上次更新過程中下載以及目前更新過程中正在下載的索引檔案的名稱、日期和時間；

- 有關軟體操作異常終止的資訊：轉儲的建立時間戳記、類型，導致軟體操作異常終止的事件的類型（意外斷電、協力廠商應用程式當機），意外斷電的日期和時間；

- 有關軟體驅動程式與硬體和軟體的相容性的資訊：有關限制軟體元件功能的作業系統內容的資訊（安全啟動、KPTI、WHQL 強制、BitLocker、區分大小寫），安裝的下載軟體的類型（UEFI、BIOS），受信任平台模組 (TPM) 識別符，TPM 規範版本，有關電腦上安裝的 CPU 的資訊，代碼完整性和 Device Guard 的執行模式和參數，驅動程式的執行模式和使用目前模式的原因，軟體驅動程式的版本，電腦的軟體和硬體虛擬化支援狀態；

- 有關導致出錯的協力廠商應用程式的資訊：應用程式名稱、版本和中文化，系統應用程式記錄中關於該錯誤的錯誤代碼和資訊，發生錯誤的位址和協力廠商應用程式的記憶體堆疊，指示軟體元件中出現錯誤的標誌，出錯之前協力廠商應用程式的執行時長，出錯的應用程式處理程序映射的核對總和（MD5、SHA2-256、SHA1），應用程式處理程序映射的路徑和路徑範本代碼，系統記錄中與該應用程式相關的錯誤說明資訊，發生錯誤的應用程式模組的相關資訊（異常識別符，應用程式模組中偏移量形式的當機記憶體位址，模組的名稱和版本，權利所有人外掛程式中的應用程式當機識別符以及當機的記憶體堆疊，當機之前應用程式工作階段的持續時間）；

- 軟體更新程式元件的版本，在元件的生命週期內執行更新工作時更新程式元件當機的次數，更新工作類型的 ID，更新程式元件完成更新工作的失敗嘗試次數；

- 有關軟體系統監控元件執行的資訊：元件的完整版本，啟動元件時的日期和時間，溢出事件佇列的事件的代碼及此類事件的數量，佇列溢出事件的總數，有關事件的發起程式的處理程序的檔案的資訊（檔案名稱及其在電腦上的路徑、檔案路徑的範本代碼、與檔案關聯的處理程序的核對總和（MD5、SHA2-256、SHA1）、檔案版本），發生的事件攔截的識別符，攔截篩選器的完整版本，攔截的事件的類型的識別符，事件佇列的大小和佇列中第一個事件與目前事件之間的事件數量，佇列中過期事件的數量，有關目前事件的發起程式處理程序的檔案的資訊（檔案名稱及其在電腦上的路徑，檔案路徑的範本代碼，與檔案關聯的處理程序的核對總和（MD5、SHA2-256、SHA1）），事件處理持續時間，事件處理最大持續時間，傳送統計資訊的概率，有關超過處理時間限制的作業系統事件的資訊（事件的日期和時間，病毒資料庫的重複初始化次數，病毒資料庫更新後最近一次重複初始化的日期和時間，每個系統監控元件的事件處理延遲時間，排隊的事件數量，已處理的事件數量，目前類型的延遲事件數量，目前類型的事件的總延遲時間，所有事件的總延遲時間）；

- 發生軟體效能問題時來自 Windows 事件追蹤工具（Event Tracing for Windows，ETW）的資訊，來自 Microsoft 的 SysConfig / SysConfigEx / WinSATAssesssment 事件的提供者：有關電腦的資訊（型號，製造商，外殼的外形規格，版本），有關 Windows 效能指標的資訊（WinSAT 評估，Windows 效能指標），網域名稱，有關物理和邏輯處理器的資訊（物理和邏輯處理器的數量，製造商，型號，步進級別，核心數量，時鐘頻率，CPUID，快取）特性，邏輯處理器特性，支援的模式和指令的指示），有關 RAM 模組的資訊（類型，表單係數，製造商，型號，容量，記憶體分配的規模），有關網路介面的資訊（IP 和 MAC 位址，名稱，描述，網路介面的配置，按類型對網路套件的數量和大小進行的細分，網路交換速度，按類型對網路錯誤的數量進行的細分），IDE 控制器的配置，DNS 伺服器的 IP 位址，有關視訊卡的資訊（型號，描述，製造商，相容性，視訊記憶體容量，熒幕權限，每像素位元數，BIOS 版本），有關即插即用裝置的資訊（名稱，描述，裝置識別符 [PnP，ACPI]，有關磁碟和儲存裝置的資訊（磁碟或快閃磁碟機的數量，製造商，型號，磁碟容量，磁柱數，每個磁柱的磁道，每個磁道的磁區數，磁區容量，快取特性，序列號，分割數，SCSI 控制器的配置），有關邏輯磁碟的資訊（序列號，分割容量，磁碟區容量，磁碟區字母，分割類型，檔案系統類型，叢集數目，叢集大小，每個叢集的磁區數，空叢集和已佔用叢集的數目，可開機磁碟區的字母，與磁碟啟動相關的分割偏移位址），有關 BIOS 主機板的資訊（製造商，發布日期，版本），有關主機板的資訊（製造商，型號，類型），有關物理記憶體的資訊（共用和可用容量），有關作業系統服務的資訊（名稱，描述，狀態，標籤，有關處理程序的資訊 [名稱和 PID]，電腦的能耗參數，中斷控制器的配置，Windows 系統資料夾的路徑（Windows 和 System32），有關作業系統的資訊（版本，內部版本，發行日期，名稱），類型，安裝日期），頁面檔案的大小，有關監視器的資訊（數量，製造商，熒幕權限，分辨率容量，類型），有關視訊卡驅動的資訊（製造商，發布日期，版本）；

- 來自 ETW 的資訊，Microsoft 的 EventTrace/EventMetadata 事件的提供方：有關系統事件序列的資訊（類型、時間、日期、時區），帶追蹤結果的檔案中繼資料（名稱、結構、追蹤參數、按類型細分的偵錯運算元），有關作業系統的資訊（名稱、類型、版本、內部版本號、發佈日期、啟動時間）；

- 來自 ETW 的資訊，Microsoft 的處理程序/Microsoft Windows 核心處理程序/Microsoft Windows 核心處理器電源事件的提供方：有關已啟動和已完成處理程序的資訊（名稱、PID、啟動參數、命令列、返回代碼、電源管理參數、啟動和完成時間、存取權杖類型、SID、SessionID、已安裝的敘述符數），有關執行緒優先順序變化的資訊（TID、優先順序、時間），有關處理程序的磁碟操作的資訊（類型、時間、容量、編號），可用記憶體處理程序的結構和容量的變更歷程記錄；

- 來自 ETW 的資訊，Microsoft 的 StackWalk/Perfinfo 事件的提供方：有關效能計數器的資訊（單個程式碼片段的效能、函式呼叫的序列、PID、TID、ISR 和 DPC 的位址和內容）；

- 來自 ETW 的資訊，Microsoft 的 KernelTraceControl-Image ID 事件的提供方：有關可執行檔和動態庫的資訊（名稱、映射大小、完整路徑），有關 PDB 檔案的資訊（名稱、識別符），可執行檔的 VERSIONINFO 資來源資料（名稱、敘述、建立者、當地語係化、應用程式版本和識別符、檔案版本和識別符）；

- 來自 ETW 的資訊，Microsoft 的 FileIo/DiskIo/映射/Windows 核心磁碟事件的提供方：有關檔案和磁碟操作的資訊（類型、容量、開始時間、完成時間、持續時間、完成狀態、PID、TID、驅動程式函式呼叫位址、I/O 請求封包 (IRP)、Windows 檔案物件內容），有關檔案和磁碟操作所涉及的檔案的資訊（名稱、版本、大小、完整路徑、內容、偏移、映射核對總和、開啟和存取選項）；

- 來自 ETW 的資訊，Microsoft 的 PageFault 事件的提供方：有關記憶體頁面存取錯誤的資訊（位址、時間、容量、PID、TID、Windows 檔案物件內容、記憶體分配參數）；

- 來自 ETW 的資訊，Microsoft 的執行緒事件的提供方：有關執行緒建立/完成的資訊，有關已啟動的執行緒的資訊（PID、TID、堆疊大小、CPU 資源的優先順序和分配、I/O 資源、執行緒間的記憶體頁面、堆疊位址、初始函數位址、執行緒環境塊 (TEB) 的位址、Windows 服務標籤）；

- 來自 ETW 的資訊，Microsoft 的 Windows 核心記憶體事件的提供方：有關記憶體管理操作的資訊（完成狀態、時間、數量、PID），記憶體分配結構（類型、容量、SessionID、PID）；

- 有關發生效能問題時軟體操作的資訊：軟體安裝識別符，效能下降的類型和值，有關軟體內的事件序列的資訊（時間、時區、類型、完成狀態、軟體元件識別符、軟體執行場景識別符、TID、PID、函式呼叫位址），有關要檢查的網路連線的資訊（URL、連線方向、網路封包大小），有關 PDB 檔案的資訊（名稱、識別符、可執行檔的映射大小），有關要檢查的檔案的資訊（名稱、完整路徑、核對總和），軟體效能監控參數；

- 有關作業系統上次重新啟動失敗的資訊：作業系統安裝以來重新啟動失敗的次數，系統轉儲資料（錯誤的代碼和參數，導致作業系統執行出錯的模組的名稱、版本和核對總和 (CRC32)，模組內偏移量形式的錯誤位址，系統轉儲的核對總和（MD5、SHA2-256、SHA1））；

- 驗證用於對檔案簽章的數位憑證的真實性所需的資訊：憑證的指紋，核對總和演算法，憑證的公開金鑰和序號，憑證頒發者的名稱，憑證驗證的結果和憑證的資料庫識別符；

- 有關對軟體的自我防護執行攻擊的處理程序的資訊：處理程序檔案的名稱和大小，其核對總和（MD5、SHA2-256、SHA1），處理程序檔案的完整路徑和檔案路徑的範本代碼，建立/構建時間戳記，可執行檔標誌，處理程序檔案的內容，用於對處理程序檔案簽章的憑證的相關資訊，用於啟動處理程序的帳戶的代碼，為存取處理程序所執行的操作的 ID，用於執行操作的資源的類型（處理程序，檔案，登錄檔物件，FindWindow 搜尋函數），用於執行操作的資源的名稱，表示操作成功的標誌，處理程序檔案的狀態及其在 KSN 中的簽章；

- 權利所有人軟體的資訊：使用的軟體的完整版本、類型、當地語係化和操作狀態，已安裝的軟體元件的版本及其操作狀態，有關已安裝的軟體更新的資訊，TARGET 篩選器的值，用於連線到權利所有人的服務所使用協定的版本；

- 有關電腦上安裝的硬體的資訊：類型、名稱、型號名稱、固件版本、內建和所連線裝置的參數、帶有已安裝軟體的電腦的唯一識別符；

- 有關作業系統和已安裝更新的版本的資訊，作業系統執行模式的字體大小、版本和參數，作業系統核心檔案的版本和總和檢查碼（MD5、SHA2-256、SHA1），以及作業系統啟動日期和時間；
- 可執行檔和非可執行檔，全部或部分；
- 電腦 RAM 的一部分；
- 作業系統引導過程中涉及的磁區；
- 網路流量封包；
- 包含可疑物件和惡意物件的網頁和電子郵件；
- WMI 儲存區的類別和類別執行個體的描述；
- 應用程式活動報告：
  - 傳送的檔案的名稱、大小和版本，其描述和總和檢查碼（MD5，SHA2-256，SHA1），檔案格式識別符，檔案廠商的名稱，檔案所屬產品的名稱，到電腦上的檔案的完整路徑，路徑的範本代碼，檔案的建立和修改時間戳記；
  - 憑證有效期的開始和結束日期/時間（如果檔案具有數位簽章），簽章的日期和時間，憑證頒發者的名稱，有關憑證持有者的資訊，指紋，憑證的公鑰和適當算法，以及憑證序列號；
  - 執行處理程序的帳戶的名稱；
  - 執行處理程序的電腦名稱的總和檢查碼（MD5，SHA2-256，SHA1）；
  - 處理程序視窗的標題；
  - 病毒資料庫的識別符，根據權利擁有人分類偵測到的威脅的名稱；
  - 有關已安裝的產品授權的資料，其識別符、類型和到期日期；
  - 提供資訊時電腦的本機時間；
  - 處理程序存取的檔案的名稱和路徑；
  - 處理程序存取的登錄機碼的名稱及其值；
  - 處理程序存取的 URL 和 IP 位址；
  - 從中下載執行檔案的 URL 和 IP 位址。

符合歐洲聯盟法規（GDPR）

在以下情況下，Kaspersky Embedded Systems Security 可能會將資料傳輸到卡巴斯基：

- 使用卡巴斯基安全網路。
- 用啟動碼啟動應用程式。

- 更新應用程式模組和病毒資料庫。
- 跟隨應用程式主控台中的連接。

無論資料分類和接收資料的地區如何，卡巴斯基都遵守高標準的資料安全性，並採取各種法律、組織和技術措施來防護使用者資料，確保資料安全性和機密性，並確保實現適用法律保證的使用者權利。隱私政策的文本包含在應用程式分發套件中，可以在卡巴斯基網站上找到。

在使用 Kaspersky Embedded Systems Security 之前，請仔細閱讀 最終使用者產品授權協議 以及卡巴斯基安全網路聲明（詳見卡巴斯基安全網路聲明）中的資料傳輸描述。如果根據您當地的法規或標準，在所述任何情況下從 Kaspersky Embedded Systems Security 傳輸的特定資料都可以歸類為個人資料，則您必須確保對這些資料進行合法處理並獲得最終使用者的同意，以收集和傳輸這樣的資料。

請閱讀最終使用者產品授權協議並存取 Kaspersky 網站瞭解當您接受《最終使用者產品授權協議》和同意《卡巴斯基安全網路聲明》之後我們如何接收、儲存和銷毀有關程式使用的資訊。license.txt 和 ksn_<語言 ID>.txt 檔案包含最終使用者產品授權協議的文字，卡巴斯基安全網路聲明包含在應用程式分發套件中。

如果您不想將資料傳輸到卡巴斯基，可以停用資料供應。

使用卡巴斯基安全網路

使用卡巴斯基安全網路即表明您同意自動提供卡巴斯基安全網路聲明中列出的資料。如果您不同意向卡巴斯基提供此資料，請使用卡巴斯基私有安全網路 (KPSN) 或停用 KSN。

使用啟動碼啟動應用程式

使用啟動碼即表明您同意自動提供最終使用者產品授權協議中列出的資料。如果您不同意提供此資料給 Kaspersky，請使用金鑰檔案來啟動 Kaspersky Embedded Systems Security。

更新應用程式模組和病毒資料庫

使用 Kaspersky 伺服器即表明您同意自動提供最終使用者產品授權協議中列出的資料。卡巴斯基需要此資訊以驗證 Kaspersky Embedded Systems Security 正在被合法使用。如果您不同意將這些資訊提供給 Kaspersky，請使用卡巴斯基安全管理中心進行資料庫更新。

跟隨應用程式主控台中的連接。

使用應用程式主控台中的連接即表明您同意自動提供最終使用者產品授權協議中列出的資料。在每個特定連接中傳輸的資料的精確清單取決於該連接在應用程式主控台中的位置以及它要解決的問題。如果您不同意向卡巴斯基提供該資訊， 停用顯示應用程式介面。

有關協力廠商程式碼資訊

有關協力廠商代碼的資訊包含在本應用程式安裝資料夾中的 legal_notices.txt 內。

商標聲明

註冊商標及服務標誌均為其各自所有人的財產。

Apache 是 Apache 軟體基金會在美國和/或其他國家的註冊商標或商標。

Citrix、XenApp 和 XenDesktop 是 Cloud Software Group, Inc. 和/或其子公司在美國和/或其他國家的註冊商標或商標。

CVE 是 MITRE 公司的註冊商標。

Dell Technologies、Dell、Dell Compellent 和其它商標是 Dell Inc. 或其子公司的商標。

EMC、Celerra、Isilon、OneFS 和 VNX 是 EMC 公司在美國和/或其他國家/地區的註冊商標或商標。

Hitachi 是日立有限公司的商標。

Linux 是 Linus Torvalds 在美國和/或其他國家/地區註冊的商標。

Microsoft、Active Directory、Internet Explorer、Excel、 Hyper-V、JScript、MultiPoint、Outlook、PowerShell、Windows、 Windows Server 和 Windows Vista 是 Microsoft 集團公司的商標。

NetApp 和 Data ONTAP 是 NetApp, Inc. 在美國和/或其國家的商標或註冊商標。

Oracle 是 Oracle 和/或其附屬公司的註冊商標。

UNIX 是在美國和其他國家/地區的註冊商標，透過 X/Open Company Limited 獨家授權。