kaspersky

Kaspersky Embedded Systems Security

© 2024 AO Kaspersky Lab

目錄

關於 Kaspersky Embedded Systems Security
新增功能
有關 Kaspersky Embedded Systems Security 的資訊來源
  可供自行查詢的資料來源
  在社區中討論 Kaspersky 應用程式
Kaspersky Embedded Systems Security
  分發套件
  硬體和軟體需求
  功能要求和限制
    安裝和移除
    檔案完整性監控
    防火牆管理
    其他限制
安裝和移除應用程式
  適用於 Windows Installer 服務的 Kaspersky Embedded Systems Security 軟體元件程式碼
    Kaspersky Embedded Systems Security 軟體元件
    "管理工具"軟體元件
  Kaspersky Embedded Systems Security 安裝後的系統變更
  Kaspersky Embedded Systems Security 處理程序
  Windows Installer 服務的安裝和移除設定及命令列選項
  Kaspersky Embedded Systems Security 安裝和移除記錄
  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
        新增 Windows 防火牆的輸出規則
      在安裝 Kaspersky Embedded Systems Security 後執行的操作
        啟動和配置 Kaspersky Embedded Systems Security 資料庫更新工作
        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
    安裝 Kaspersky Embedded Systems Security 的指令範例
    在安裝 Kaspersky Embedded Systems Security 後執行的操作
    新增和移除元件。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
透過 Active Directory 群組政策安裝和移除
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
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
應用程式介面
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
關於資料提供
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
產品授權到期後的功能限制
續約產品授權
刪除金鑰
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
導航
透過政策開啟一般設定
在應用程式內容視窗中開啟一般設定
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延展性、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
設定本機系統工作的排程啟動
在卡巴斯基安全管理中心中配置隔離和備份設定
建立和設定政策
建立政策
Kaspersky Embedded Systems Security 政策設定部分
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

- 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
- 在卡巴斯基安全管理中心中設定群組工作
  - 啟動應用程式工作
  - 更新工作
  - 應用程式完整性控制
- 在卡巴斯基安全管理中心中設定當機診斷設定
- 管理工作排程
  - 排程工作
  - 啟用和停用排程工作
- 卡巴斯基安全管理中心中的報告

使用 Kaspersky Embedded Systems Security 主控台

- 關於 Kaspersky Embedded Systems Security 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
- 透過其他裝置上的應用程式主控台管理 Kaspersky Embedded Systems Security
- 透過應用程式主控台配置一般應用程式設定
- 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
  - 管理工作排程
    - 配置工作啟動排程設定
    - 啟用和停用排程工作
  - 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
  - 使用安全性設定範本
    - 關於安全性設定範本
    - 建立安全性設定範本
    - 檢視範本中的安全性設定
    - 套用安全性設定範本
    - 刪除安全性設定範本
- 檢視防護狀態和 Kaspersky Embedded Systems Security 資訊

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 外掛程式配置延展性、介面和掃描設定
    - 在 Web 外掛程式中配置安全性設定
    - 在 Web 外掛程式中配置連線設定
    - 設定本機系統工作的排程啟動
  - 在 Web 外掛程式配置隔離和備份設定
- 建立和設定政策

建立政策
Kaspersky Embedded Systems Security 政策設定部分
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 外掛程式中配置啟動應用程式工作
在 Web 外掛程式中配置更新工作
在 Web 外掛程式中配置當機診斷設定
管理工作排程
排程工作
啟用和停用排程工作
卡巴斯基安全管理中心中的報告
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 Dump 和偵錯檔案寫入
更新 Kaspersky Embedded Systems Security 資料庫和軟體模組
關於更新工作
關於軟體模組更新
關於資料庫更新
組織內使用的病毒防護資料庫和模組的更新方案
設定更新工作
配置使用 Kaspersky Embedded Systems Security 更新來源的設定
在執行資料庫更新工作時最佳化磁碟 I/O
配置複製更新工作設定
配置軟體模組更新工作設定
回溯 Kaspersky Embedded Systems Security 資料庫更新
回溯應用程式模組更新
更新工作統計
隔離物件和複製備份
隔離可能受感染物件。隔離
關於隔離可疑感染物件
檢視隔離物件
排序隔離的物件
篩選隔離的物件
隔離區掃描
還原隔離的物件
將物件移到隔離
從隔離區刪除物件
傳送可疑感染物件到 Kaspersky 以供分析
配置隔離區設定
隔離統計
製作物件的備份副本。備份
關於備份物件後再解毒或刪除
檢視備份中儲存的物件

排序備份中的檔案
篩選備份中的檔案
從備份還原檔案
從備份刪除檔案
配置備份設定
備份統計
封鎖存取網路資源。封鎖的主機
關於封鎖的主機儲存
透過管理外掛程式管理已封鎖的主機
啟用封鎖不信任主機
配置"封鎖的主機"設定
透過應用程式主控台管理已封鎖的主機
啟用封鎖不信任主機
配置"封鎖的主機"設定
透過 Web 外掛程式管理已封鎖的主機
啟用主機封鎖
配置"封鎖的主機"設定
事件註冊。Kaspersky Embedded Systems Security 記錄
註冊 Kaspersky Embedded Systems Security 事件的方式
系統稽核記錄
在系統稽核記錄中排序事件
在系統稽核記錄中篩選事件
刪除系統稽核記錄中的事件
工作記錄
關於工作記錄
在工作記錄中檢視事件清單
排序工作記錄
篩選工作記錄
在工作記錄中檢視有關 Kaspersky Embedded Systems Security 工作的統計和資訊
匯出工作記錄中的資訊
刪除工作記錄
安全記錄
在事件檢視器中檢視 Kaspersky Embedded Systems Security 事件記錄
在管理外掛程式中配置記錄設定
關於 SIEM 整合
配置 SIEM 整合設定
配置記錄和通知
配置記錄設定
安全記錄
配置 SIEM 整合設定
配置通知設定
配置與管理伺服器的互動
通知設定
管理員和使用者通知方式
設定管理員和使用者通知
啟動和停止 Kaspersky Embedded Systems Security
啟動 Kaspersky Embedded Systems Security 管理外掛程式
從開始功能表啟動 Kaspersky Embedded Systems Security 主控台

- 啟動和停止 Kaspersky Security 服務
- 在作業系統安全模式下啟動 Kaspersky Embedded Systems Security
  - 關於在作業系統安全模式下工作的 Kaspersky Embedded Systems Security
  - 在安全模式下啟動 Kaspersky Embedded Systems Security
- Kaspersky Embedded Systems Security 自我防護
  - 關於 Kaspersky Embedded Systems Security 自我防護
  - 防止包含已安裝的 Kaspersky Embedded Systems Security 元件的資料夾被變更
  - 防止 Kaspersky Embedded Systems Security 登入機碼被變更
  - 將 Kaspersky Security 服務註冊為受防護服務
  - 管理 Kaspersky Embedded Systems Security 功能的存取權限
    - 關於 Kaspersky Embedded Systems Security 的管理權限
    - 關於管理註冊服務的權限
    - 關於 Kaspersky Security 管理服務的存取權限
    - 關於 Kaspersky Security 服務的管理權限
    - 透過管理外掛程式管理存取權限
      - 配置 Kaspersky Embedded Systems Security 和 Kaspersky Security 服務的存取權限
      - 對 Kaspersky Embedded Systems Security 功能進行受密碼防護的存取
    - 透過應用程式主控台管理存取權限
      - 配置用於管理 Kaspersky Embedded Systems Security 和 Kaspersky Security 服務的存取權限
      - 對 Kaspersky Embedded Systems Security 功能進行受密碼防護的存取
    - 透過 Web 外掛程式管理存取權限
      - 配置 Kaspersky Embedded Systems Security 和 Kaspersky Security 服務的存取權限
      - 對 Kaspersky Embedded Systems Security 功能進行受密碼防護的存取
- 即時檔案防護
  - 關於“即時檔案防護”工作
  - 關於工作防護範圍和安全設定
  - 關於虛擬防護範圍
  - 預定義的防護範圍
  - 關於預定義安全等級
  - “即時檔案防護”工作中預設掃描的檔案副檔名
  - “即時檔案防護”工作預設設定
  - 透過管理外掛程式管理“即時檔案防護”工作
    - 導航
      - 開啟“即時檔案防護”工作的政策設定
      - 開啟“即時檔案防護”工作內容
    - 配置“即時檔案防護”工作
      - 選擇防護模式
      - 配置啟發式分析以及與其他應用程式元件的整合
      - 排程工作
    - 建立和配置工作防護範圍
    - 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
      - 配置一般工作設定
      - 配置操作
      - 配置效能
  - 透過應用程式主控台管理“即時檔案防護”工作
    - 導航
      - 開啟“即時檔案防護”工作設定

開啟“即時檔案防護”工作範圍設定
配置“即時檔案防護”工作
選擇防護模式
配置啟發式分析以及與其他應用程式元件的整合
配置工作啟動排程設定
建立防護範圍
配置網路檔案資源的視圖
建立防護範圍
在防護範圍內包含網路物件
建立虛擬防護範圍
手動配置安全性設定
為即時檔案防護工作選擇預定義安全等級
配置一般工作設定
配置操作
配置效能
即時檔案防護工作統計
透過 Web 外掛程式管理“即時檔案防護”工作
配置“即時檔案防護”工作
配置工作防護範圍
KSN 使用
關於“KSN 使用”工作
“KSN 使用”工作預設設定
透過管理外掛程式管理“KSN 使用”
配置“KSN 使用”工作
配置資料處理
透過應用程式主控台管理“KSN 使用”
配置“KSN 使用”工作
配置資料處理
透過 Web 外掛程式管理“KSN 使用”
設定其他資料傳輸
“KSN 使用”工作統計
網路威脅防護
關於“網路威脅防護”工作
“網路威脅防護”工作預設設定
透過應用程式主控台配置“網路威脅防護”工作
一般工作設定
新增排除
透過管理外掛程式配置“網路威脅防護”工作
一般工作設定
新增排除
透過 Web 外掛程式配置“網路威脅防護”工作
一般工作設定
新增排除
應用程式啟動控制
關於“應用程式啟動控制”工作
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”工作的 KSN 使用

關於應用程式啟動控制規則產生
"應用程式啟動控制"工作預設設定
透過管理外掛程式管理應用程式啟動控制
導航
開啟"應用程式啟動控制"工作的政策設定
開啟應用程式啟動控制規則清單
開啟"應用程式啟動控制規則產生器"工作精靈和內容
配置"應用程式啟動控制"工作設定
配置軟體分發控制
配置"應用程式啟動控制規則產生器"工作
透過卡巴斯基安全管理中心配置應用程式啟動控制規則
新增應用程式啟動控制規則
啟用預設允許模式
從卡巴斯基安全管理中心事件建立允許規則
從有關受封鎖應用程式的卡巴斯基安全管理中心報告中匯入規則
從 XML 設定檔匯入應用程式啟動控制規則
檢查應用程式啟動
建立"應用程式啟動控制規則產生器"工作
限制工作使用範圍
自動規則產生期間要執行的操作
自動規則產生完成後要執行的操作
透過應用程式主控台管理應用程式啟動控制
導航
開啟"應用程式啟動控制"工作設定
開啟應用程式啟動控制規則視窗
開啟"應用程式啟動控制規則產生器"工作設定
配置"應用程式啟動控制"工作設定
選擇"應用程式啟動控制"工作的模式
配置"應用程式啟動控制"工作的範圍
配置 KSN 使用
軟體分發控制
配置應用程式啟動控制規則
新增應用程式啟動控制規則
啟用預設允許模式
根據"應用程式啟動控制"工作事件建立允許規則
匯出應用程式啟動控制規則
從 XML 設定檔匯入應用程式啟動控制規則
刪除應用程式啟動控制規則
配置"應用程式啟動控制規則產生器"工作
限制工作使用範圍
自動規則產生期間要執行的操作
自動規則產生完成後要執行的操作
透過 Web 外掛程式管理應用程式啟動控制
裝置控制
關於裝置控制工作
關於裝置控制規則
關於裝置控制規則產生
關於裝置控制規則產生器工作

"裝置控制"工作預設設定
透過管理外掛程式管理裝置控制
導航
開啟"裝置控制"工作的政策設定
開啟裝置控制規則清單
開啟"裝置控制規則產生器"工作精靈和內容
配置"裝置控制"工作
配置"裝置控制規則產生器"工作
透過卡巴斯基安全管理中心配置裝置控制規則
基於卡巴斯基安全管理中心政策中的系統資料建立允許規則
為已連線的裝置建立規則
從有關被封鎖裝置的卡巴斯基安全管理中心報告中匯入規則
使用"裝置控制規則產生器"工作建立規則
將建立的規則新增到裝置控制規則清單
透過應用程式主控台管理裝置控制
導航
開啟"裝置控制"工作設定
開啟"裝置控制規則"視窗
開啟"裝置控制規則產生器"工作設定
配置裝置控制工作設定
配置裝置控制規則
從 XML 檔案匯入裝置控制規則
基於裝置控制工作事件填寫規則清單
為一個或多個外部裝置新增允許規則
刪除裝置控制規則
匯出裝置控制規則
啟動和停用裝置控制規則
延伸裝置控制規則使用範圍
配置裝置控制規則產生器工作
透過應用程式主控台 Web 外掛程式管理裝置控制
防火牆管理
關於防火牆管理工作
關於防火牆規則
防火牆管理工作預設設定
透過管理外掛程式管理防火牆規則
啟用和停用防火牆規則
手動新增防火牆規則
刪除防火牆規則
透過應用程式主控台管理防火牆規則
啟用和停用防火牆規則
手動新增防火牆規則
刪除防火牆規則
透過 Web 外掛程式管理防火牆規則
啟用和停用防火牆規則
手動新增防火牆規則
刪除防火牆規則
檔案完整性監控
關於"檔案完整性監控"工作

- 關於檔案操作監控規則
- “檔案完整性監控”工作預設設定
- 透過管理外掛程式管理“檔案完整性監控”
  - 配置“檔案完整性監控”工作
  - 配置監控規則
- 透過應用程式主控台管理“檔案完整性監控”
  - 配置“檔案完整性監控”工作設定
  - 配置監控規則
- 透過 Web 外掛程式管理“檔案完整性監控”
  - 配置“檔案完整性監控”工作
  - 配置監控規則

註冊表存取監控

- 關於註冊表存取監控工作
- 關於系統註冊表監控規則
- 「註冊表存取監控」工作預設設定
- 透過管理外掛程式管理「註冊表存取監控」
  - 配置註冊表存取監控工作設定
  - 配置監控規則
- 透過管理主控台管理「註冊表存取監控」
  - 配置註冊表存取監控工作設定
  - 配置監控規則
- 透過 Web 外掛程式管理「註冊表存取監控」
  - 配置註冊表存取監控工作
  - 配置監控規則

記錄審查

- 關於“記錄審查”工作
- “記錄審查”工作預設設定
- 透過管理外掛程式管理記錄審查規則
  - 配置預定義工作規則
  - 透過管理外掛程式新增記錄審查規則
- 透過應用程式主控台管理記錄審查規則
  - 配置預定義工作規則
  - 透過應用程式主控台新增記錄審查規則
- 透過 Web 外掛程式管理記錄審查規則

自訂掃描

- 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
- 關於卸除式磁碟機掃描
- 關於“基線檔案完整性監控”工作
- 從內容功能表中啟用自訂掃描工作的啟動
- 預設自訂掃描工作設定
- 透過管理外掛程式管理自訂掃描工作
  - 導航
    - 開啟自訂掃描工作精靈
    - 開啟自訂掃描工作內容

- 建立自訂掃描工作
  - 為自訂掃描工作分配關鍵區域掃描狀態
  - 在背景執行自訂掃描工作
  - 記錄關鍵區域掃描執行
- 配置工作掃描範圍
- 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
  - 配置一般工作設定
  - 配置操作
  - 配置效能
- 配置卸除式磁碟機掃描
- 配置"基線檔案完整性監控"工作
- 透過應用程式主控台管理自訂掃描工作
- 導航
  - 開啟自訂掃描工作設定
  - 開啟自訂掃描工作範圍設定
- 建立和配置自訂掃描工作
- 自訂掃描工作中的掃描範圍
  - 配置網路檔案資源的視圖
  - 建立掃描範圍
  - 在掃描範圍內包含網路物件
  - 建立虛擬掃描範圍
- 配置安全性設定
  - 為自訂掃描工作選擇預定義的安全等級
  - 配置一般工作設定
  - 配置操作
  - 配置效能
  - 配置分級儲存
- 掃描卸除式磁碟機
- 自訂掃描工作統計
- 建立和配置"基線檔案完整性監控"工作
- 透過 Web 外掛程式管理自訂掃描工作
- 開啟自訂掃描工作精靈
- 開啟自訂掃描工作內容
- 配置工作掃描範圍
- 配置工作設定

信任區域

- 關於信任區域
- 透過管理外掛程式管理信任區域
- 導航
  - 開啟信任區域政策設定
  - 開啟信任區域內容視窗
- 透過管理外掛程式配置信任網域設定
  - 新增排除
  - 新增受信任處理程序
  - 套用 not-a-virus 遮罩
- 透過應用程式主控台管理信任區域
- 在應用程式主控台中對工作套用信任區域

在應用程式主控台中配置信任區域設定
將排除新增至信任區域
新增受信任處理程序
套用 not-a-virus 遮罩
透過 Web 外掛程式管理信任區域
弱點利用防禦
關於弱點利用防禦
透過管理外掛程式管理弱點利用防禦
導航
開啟弱點利用防禦的政策設定
開啟弱點利用防禦內容視窗
配置處理程序記憶體防護設定
將處理程序新增到防護範圍
透過應用程式主控台管理弱點利用防禦
導航
開啟弱點利用防禦一般設定
開啟弱點利用防禦處理程序防護設定
配置處理程序記憶體防護設定
將處理程序新增到防護範圍
透過 Web 外掛程式管理弱點利用防禦
配置處理程序記憶體防護設定
將處理程序新增到防護範圍
弱點利用防禦技術
與協力廠商系統整合
系統監視器的效能計數器
關於 Kaspersky Embedded Systems Security 效能計數器
拒絕需求總數
略過請求總數
因為系統資源不足而未處理的需求數
傳送以供處理的需求數
檔案攔截調度程式執行緒的平均數
檔案攔截調度程式執行緒的最大數
受感染物件佇列中的元素數
每秒處理的物件數
Kaspersky Embedded Systems Security SNMP 計數器和 TRAP
關於 Kaspersky Embedded Systems Security SNMP 計數器和 TRAP
Kaspersky Embedded Systems Security SNMP 計數器
效能計數器
隔離計數器
備份計數器
一般計數器
更新計數器
即時檔案防護計數器
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
與 WMI 整合
從命令列使用 Kaspersky Embedded Systems Security
指令

顯示 Kaspersky Embedded Systems Security 指令說明：KAVSHELL HELP
啟動和停止 Kaspersky Security 服務：KAVSHELL START，KAVSHELL STOP
掃描指定區域：KAVSHELL SCAN
啟動"關鍵區域掃描"工作：KAVSHELL SCANCRITICAL
非同步管理工作：KAVSHELL TASK
刪除 PPL 內容：KAVSHELL CONFIG
啟動和停止即時電腦防護工作：KAVSHELL RTP
管理應用程式啟動控制工作：KAVSHELL APPCONTROL /CONFIG
應用程式啟動控制規則產生器：KAVSHELL APPCONTROL /GENERATE
填寫應用程式啟動控制規則清單：KAVSHELL APPCONTROL
填寫裝置控制規則清單：KAVSHELL DEVCONTROL
啟動資料庫更新工作：KAVSHELL UPDATE
回溯 Kaspersky Embedded Systems Security 資料庫更新：KAVSHELL ROLLBACK
管理記錄審查：KAVSHELL TASK LOG-INSPECTOR
啟動應用程式：KAVSHELL LICENSE
啟用、設定和停用偵錯記錄：KAVSHELL TRACE
對 Kaspersky Embedded Systems Security 記錄檔案進行磁碟整理：KAVSHELL VACUUM
清理 iSwift 基礎：KAVSHELL FBRESET
啟用和停用建立傾印檔案：KAVSHELL DUMP
匯入設定：KAVSHELL IMPORT
匯出設定：KAVSHELL EXPORT
與 Microsoft Operations Management Suite 整合：KAVSHELL OMSINFO
管理"基線檔案完整性監控"工作：KAVSHELL FIM /BASELINE
指令回傳代碼
KAVSHELL START 和 KAVSHELL STOP 指令的回傳代碼
KAVSHELL SCAN 和 KAVSHELL SCANCRITICAL 指令的回傳代碼
KAVSHELL TASK LOG-INSPECTOR 指令的回傳代碼
KAVSHELL TASK 指令的回傳代碼
KAVSHELL RTP 命令的傳回代碼。
KAVSHELL UPDATE 命令的傳回代碼。
KAVSHELL ROLLBACK 指令的回傳代碼
KAVSHELL LICENSE 指令的回傳代碼
KAVSHELL TRACE 命令的傳回代碼。
KAVSHELL FBRESET 指令的回傳代碼
KAVSHELL DUMP 命令的傳回代碼。
KAVSHELL IMPORT 命令的傳回代碼。
KAVSHELL EXPORT 命令的傳回代碼。
KAVSHELL FIM /BASELINE 指令的回傳代碼
聯絡技術支援
如何獲取技術支援
透過 Kaspersky CompanyAccount 取得技術支援
使用偵錯檔案和 AVZ 指令碼
詞彙表
OLE 物件
SIEM
事件嚴重性
備份
卡巴斯基安全網路 (KSN)

- 受感染的物件
- 可感染的檔案
- 壓縮檔案
- 安全等級
- 工作
- 工作設定
- 弱點
- 政策
- 啟動物件
- 啟動金鑰
- 啟發式分析
- 更新
- 本機工作
- 檔案遮罩
- 產品授權期限
- 病毒特徵碼資料庫
- 管理伺服器
- 解毒
- 誤報
- 防護狀態
- 隔離

有關協力廠商程式碼資訊

商標聲明

關於 Kaspersky Embedded Systems Security

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。

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。
- **自訂掃描**。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**。該元件可偵錯使用者啟動應用程式的嘗試並控制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。
- **防火牆管理**。此元件提供管理 Windows 防火牆的能力：配置設定和作業系統防火牆規則，並封鎖從外部配置防火牆的任何可能性。
- **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：

- **資料庫更新**和**軟體模組更新**。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**。Kaspersky Embedded Systems Security 透過將疑似感染物件從原始位置移動到*隔離*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**。您可以設定程式通知受防護裝置的管理員和使用者，有關 Kaspersky Embedded Systems Security 操作中的事件和裝置上病毒防護的狀態。
- **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**。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性設定，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設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。
- **信任區域**。您可以從防護範圍或掃描範圍中生成排除清單，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代理來防護處理程序記憶體免受弱點利用。

在美國使用的軟體將無法提供更新功能（包括防毒軟體簽章更新和程式碼庫更新）和 KSN 功能。

新增功能

Kaspersky Embedded Systems Security 的新版本引入了以下新功能和改進：

- 目前已支援下列作業系統：
  - Microsoft Windows 10 21H2
  - Microsoft Windows 11
- 產品授權：當產品授權金鑰過期時，除了資料庫更新元件和卡巴斯基安全網路服務外，系統元件仍可操作。
- 產品授權：實作了啟動碼支援。
- 系統稽核設定改進：檔案完整性監控工作，建立對應規則後，您可禁止特定監控範圍變更檔案。此外，您也可以套用信任區域，將受信任物件和受信任使用者從監控區域排除。
- 系統稽核設定改進：註冊表存取監控工作，建立對應規則後，您可編制統計資料或禁止變更所選監控區域中的註冊表參數或值。此外，您也可以套用信任區域，將受信任處理程序和受信任使用者從監控區域排除。
- 新增可以提前啟動 Kaspersky Embedded Systems Security 服務的選項。
- 對於卡巴斯基安全管理中心元件狀態報告，將展開標準狀態集。元件是否可在啟動模式下操作或僅能編制統計資料與通知相關威脅的資訊將以新狀態提供。
- 改進自我防護設定：在 Kaspersky Embedded Systems Security 主控台和 Kaspersky Embedded Systems Security 管理外掛程式政策內容中，現在可以啟用或停用 Kaspersky Embedded Systems Security 檔案防護和註冊檔參數，避免受到外部威脅。
- 當您啟動 Kaspersky Embedded Systems Security，應用程式會為受防護裝置分配個別的標籤。標籤可幫助您識別受防護裝置池中使用相同名稱和相同 IP 位址註冊的不同裝置。
- 卡巴斯基安全管理中心使用者現在可以使用以下應用程式 Web 外掛程式對話框：
  - 檔案完整性監控
  - 應用程式啟動控制
  - 記錄審查
- 您可以將 Kaspersky Embedded Systems Security 作為卡巴斯基雲端主控台的一部分使用。
- 在 Kaspersky Embedded Systems Security，您可以配置 Kaspersky Security 服務的延遲啟動模式。在此模式中，當所有作業系統元件皆載入時，會啟動 Kaspersky Security 服務。
- 變更裝置控制工作：現在您可以配置工作來編制統計資料或禁止透過支援 UAS 技術的 USB 連線裝置。
- 線上文件中現已提供應用程式生命週期表的連結。
- 修復之前版本的錯誤：應用程式包含針對之前版本發佈的錯誤修復。

有關 Kaspersky Embedded Systems Security 的資訊來源

本章節介紹程式的相關資訊來源。

您可依據問題的緊急性或重要性等級，來選取最適宜的來源。

可供自行查詢的資料來源

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。
- 手冊。

如果您有無法自行排除的問題，請與 Kaspersky 技術支援 聯絡。

若要使用 Kaspersky 網站資訊來源，您必須連線網際網路。

Kaspersky 網站上的 Kaspersky Embedded Systems Security 頁面

在 Kaspersky Embedded Systems Security 頁面 上，您可以檢視有關應用程式、它的功能和特色的基本資訊。

Kaspersky Embedded Systems Security 頁面包含指向 eStore 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一部分。

在知識庫 中的 Kaspersky Embedded Systems Security 頁面上，您可以閱讀文章，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 文件

《Kaspersky Embedded Systems Security 管理手冊》包含有關應用程式安裝、移除、設定配置和使用的資訊。

在社區中討論 Kaspersky 應用程式

如果您的問題不需要立即性的回答，您可以在我們的社群 中與 Kaspersky 專家及其他使用者進行討論。

在我們的線上社區中，您可以檢視現有主題、留下評論和建立新討論主題。

Kaspersky Embedded Systems Security

本節介紹了 Kaspersky Embedded Systems Security 的功能、元件以及分發套件，並提供了 Kaspersky Embedded Systems Security 的硬體和軟體需求清單。

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。
- 啟動將安裝 Kaspersky Embedded Systems Security 管理外掛程式的安裝精靈以透過卡巴斯基安全管理中心管理應用程式。
- 閱讀《管理手冊》。
- 前往 Kaspersky 網站上的 Kaspersky Embedded Systems Security 頁面。
- 存取技術支援網站。
- 閱讀有關 Kaspersky Embedded Systems Security 目前版本的資訊。

\console 資料夾包含應用程式主控台的安裝檔案（“Kaspersky Embedded Systems Security 管理工具”元件集）。

\product 資料夾包含：

- 用於在執行 32 位元或 64 位元 Microsoft Windows 作業系統的受防護裝置上安裝 Kaspersky Embedded Systems Security 元件的檔案。
- 用於安裝管理外掛程式的檔案，以便透過卡巴斯基安全管理中心管理 Kaspersky Embedded Systems Security。
- 程式發佈時最新病毒資料庫的壓縮檔案。
- 包含最終使用者產品授權協議和隱私政策文字的檔案。

\product_no_avbases 資料夾包含不帶防毒資料庫的 Kaspersky Embedded Systems Security 元件和管理外掛程式的安裝檔案。

\setup 資料夾包含問候程式啟動檔案。

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。
release_notes.txt	該檔案包含發佈資訊。
migration.txt	該檔案介紹從以前的應用程式版本進行移轉。

setup.exe	程式安裝檔（啟動 setup.hta）。
\console\esstools_x86.msi	Windows Installer 軟體套件；在執行 32 位元 Microsoft Windows 作業系統的受防護裝置上安裝應用程式主控台。
\console\esstools_x64.msi	Windows Installer 套件；在執行 64 位元 Microsoft Windows 作業系統的受防護裝置上安裝應用程式主控台。
\console\setup.exe	該檔案啟動元件的"管理工具"元件集（包括應用程式主控台）的安裝精靈；它可使用在安裝精靈中指定的設定啟動 esstools.msi 安裝套件檔案。
\product\bases.cab	程式發佈時最新病毒資料庫的壓縮檔案。
\product\setup.exe	用於在受防護裝置上透過精靈安裝 Kaspersky Embedded Systems Security 的檔案；它使用精靈中指定的安裝設定啟動安裝套件檔案 ess.msi。
\product\ess_x86.msi	Windows Installer 軟體套件；在執行 32 位元 Microsoft Windows 作業系統的受防護裝置上安裝 Kaspersky Embedded Systems Security 的"**使用防毒基礎技術保護電腦**"配置。 如果選擇"使用病毒基礎技術防護電腦"配置，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 Kaspersky Embedded Systems Security 的"使用病毒基礎技術防護電腦"配置時，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 • 自訂掃描 • 網路威脅防護
\product\ess_x64.msi	Windows Installer 軟體套件；在執行 64 位元 Microsoft Windows 作業系統的受防護裝置上安裝 Kaspersky Embedded Systems Security 的**使用防毒基礎技術保護電腦**配置。 如果選擇"使用病毒基礎技術防護電腦"配置，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 Kaspersky Embedded Systems Security 的"使用病毒基礎技術防護電腦"配置時，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 • 自訂掃描 • 網路威脅防護
\product\ess.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 Kaspersky Embedded Systems Security 的安裝套件的說明。
\product\klcfginst.exe	管理外掛程式的安裝程式，以便透過卡巴斯基安全管理中心管理 Kaspersky Embedded Systems Security。如果您排程使用管理外掛程

	式來管理 Kaspersky Embedded Systems Security，請在每台已安裝卡巴斯基安全管理中心管理主控台的電腦上安裝該外掛程式。
\product\license.txt	最終使用者產品授權協議和隱私政策的文字。
\product_long_term\setup.exe	用於在受防護裝置上透過精靈安裝 Kaspersky Embedded Systems Security 的檔案；它使用精靈中指定的安裝設定啟動安裝套件檔案 ess.msi。
\product_long_term\ess_x86.msi	Windows Installer 軟體套件；在執行 32 位元 Microsoft Windows 作業系統的受防護裝置上安裝 Kaspersky Embedded Systems Security 的 "**使用預設拒絕技術保護電腦**"配置。 啟用更新的元件不包括在"使用預設拒絕技術保護電腦"配置中。 如果選擇"使用預設拒絕技術保護電腦"配置，則預設包含以下元件： • Core • 弱點利用防禦 • 應用程式啟動控制 • 系統托盤圖示 在使用特徵分析和防毒資料庫來保護電腦的應用程式版本上安裝 Kaspersky Embedded Systems Security 的"使用預設拒絕技術保護電腦"配置時，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 • 自訂掃描 • - 啟用更新的元件。 建議使用此配置來保護資源有限的系統。在這種情況下，您可以長期啟動應用程式，並且"應用程式啟動控制"元件會提供電腦防護。
\product_long_term\ess_x64.msi	Windows Installer 軟體套件；在執行 64 位元 Microsoft Windows 作業系統的受防護裝置上安裝 Kaspersky Embedded Systems Security 的 **使用預設拒絕技術保護電腦**配置。

	啟用更新的元件不包括在"使用預設拒絕技術保護電腦"配置中。 如果選擇"使用預設拒絕技術保護電腦"配置，則預設包含以下元件： • Core • 弱點利用防禦 • 應用程式啟動控制 • 系統托盤圖示 在使用特徵分析和防毒資料庫來保護電腦的應用程式版本上安裝 Kaspersky Embedded Systems Security 的"使用預設拒絕技術保護電腦"配置時，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 • 自訂掃描 • - 啟用更新的元件。 建議使用此配置來保護資源有限的系統。在這種情況下，您可以長期啟動應用程式，並且"應用程式啟動控制"元件會提供電腦防護。
\product_long_term\ess_light.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 Kaspersky Embedded Systems Security 的安裝套件的說明。
\product_long_term\klcfginst.exe	管理外掛程式的安裝程式，以便透過卡巴斯基安全管理中心管理 Kaspersky Embedded Systems Security。如果您排程使用管理外掛程式來管理 Kaspersky Embedded Systems Security，請在每台已安裝卡巴斯基安全管理中心管理主控台的電腦上安裝該外掛程式。
\product_long_term\license.txt	最終使用者產品授權協議和隱私政策的文字。
\setup\setup.hta	程式安裝檔。

硬體和軟體需求

在安裝 Kaspersky Embedded Systems Security 之前，您必須先從裝置移除其他防毒程式。

對受防護裝置的軟體需求

您可以在執行 32 位元或 64 位元 Microsoft Windows 作業系統的裝置上安裝 Kaspersky Embedded Systems Security。

Windows Installer 3.1 是在執行 Microsoft Windows XP 的受防護裝置上正常安裝和使用應用程式所必需的。

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。

在安裝 Kaspersky Embedded Systems Security 之前，請確保在受防護裝置的作業系統上安裝涵蓋 SHA-2 支援的所需更新。如果不支援 SHA-2，安裝的應用程式模組可能無法正常執行，從而導致作業系統故障。詳細資訊，請參閱：https://support.kaspersky.com/15728。

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：

- Windows XP Embedded SP3（32 位元）
- Windows Embedded POSReady 2009（32 位元）
- Windows Embedded Standard 7 SP1（32 位元、64 位元）
- Windows Embedded Enterprise 7 SP1（32 位元、64 位元）
- Windows Embedded POSReady 7（32 位元、64 位元）
- Windows Embedded 8.0 Standard（32 位元、64 位元）
- Windows Embedded 8.1 Industry Professional / Enterprise（32 位元、64 位元）
- Windows 10 IoT Enterprise（32 位元、64 位元）
- Windows XP Professional SP2 / SP3（32 位元）
- Windows 7 Professional / Enterprise SP1（32 位元、64 位元）
- Windows 8 Professional / Enterprise（32 位元、64 位元）
- Windows 8.1 Professional / Enterprise（32 位元、64 位元）
- Windows 10 Professional / Enterprise（32 位元、64 位元）
- Windows 10 1607 Professional / Enterprise / IoT Enterprise（32 位元、64 位元）
- Windows 10 1703 Professional / Enterprise / IoT Enterprise（32 位元、64 位元）
- Windows 10 1709 Professional / Enterprise / IoT Enterprise（32 位元、64 位元）
- Windows 10 1803 Professional / Enterprise / IoT Enterprise（32 位元、64 位元）
- Windows 10 1809 Professional / Enterprise / IoT Enterprise（32 位元、64 位元）
- Windows 10 19H2 Professional / Enterprise / IoT Enterprise（32 位元、64 位元）
- Windows 10 21H2 Professional / Enterprise / IoT Enterprise（32 位元、64 位元）

- Windows 10 Enterprise LTSC 2016（32 位元、64 位元）
- Windows 10 Enterprise LTSC 2019（32 位元、64 位元）
- Windows 10 Enterprise LTSC 2021（32 位元、64 位元）
- Windows 11 21H2 Professional / Enterprise（64 位元）

對受防護裝置的硬體需求

受保護裝置的硬體要求會隨著安裝的 Windows 作業系統而有不同：

- 執行 Windows XP（32/64 位元）、Windows Embedded XP、Windows Embedded POSReady 2009 或 Windows Embedded POSReady 7 作業系統的裝置硬體要求：
  - 最低需求：
    - 磁碟空間需求：
      - 安裝"應用程式啟動控制"元件 – 50 MB。
      - 安裝所有 Kaspersky Embedded Systems Security 元件 – 2 GB。
    - 記憶體：
      - 256 MB，僅在執行 Microsoft Windows 作業系統的裝置上安裝"應用程式啟動控制"元件。
      - 512 MB，執行所有元件的完整安裝。
    - 處理器要求：
      - 對於 32 位元 Microsoft Windows 作業系統：

        1.4 GHz 單核處理器。

        Intel® Pentium® III。
      - 對於 64 位元 Microsoft Windows 作業系統：

        1.4 GHz 單核處理器。

        Intel Pentium IV。
  - 建議需求：
    - 磁碟空間需求：
      - 安裝"應用程式啟動控制"元件 – 2 GB。
      - 安裝所有 Kaspersky Embedded Systems Security 元件 – 4 GB。
    - 記憶體：2 GB。
    - 處理器要求：2.4 GHz 四核處理器。

- 執行 Windows Embedded 7、Windows Embedded 8 或 Windows Embedded 10 作業系統下的裝置硬體要求：
  - 最低需求：
    - 磁碟空間需求：
      - 安裝"應用程式啟動控制"元件 – 50 MB。
      - 安裝所有 Kaspersky Embedded Systems Security 元件 – 2 GB。
    - 記憶體：1 GB。
    - 處理器要求：1.4 GHz 單核處理器 Intel Pentium IV。
  - 建議需求：
    - 磁碟空間需求：
      - 安裝"應用程式啟動控制"元件 – 2 GB。
      - 安裝所有 Kaspersky Embedded Systems Security 元件 – 4 GB。
    - 記憶體：2 GB。
    - 處理器要求：2.4 GHz 四核處理器。
- 執行 Windows 7（64 位元）、Windows 8（64 位元）、Windows 10（64 位元）或 Windows 11（64 位元）作業系統的裝置硬體要求：
  - 最低需求：
    - 磁碟空間需求：
      - 安裝"應用程式啟動控制"元件 – 50 MB。
      - 安裝所有 Kaspersky Embedded Systems Security 元件 – 2 GB。
    - 記憶體：
      - 1 GB，僅在執行 Microsoft Windows 作業系統的裝置上安裝"應用程式啟動控制"元件。
      - 2 GB，執行所有元件的完整安裝。
    - 處理器要求：

      1.4 GHz 單核處理器。

      Intel Pentium IV。
  - 建議需求：
    - 磁碟空間需求：
      - 安裝"應用程式啟動控制"元件 – 2 GB。
      - 安裝所有 Kaspersky Embedded Systems Security 元件 – 4 GB。

- 記憶體：
  - 2 GB，僅在執行 Microsoft Windows 作業系統的裝置上安裝"應用程式啟動控制"元件。
  - 4 GB，執行所有元件的完整安裝。
- 處理器要求：2.4 GHz 四核處理器。

- 執行 Windows 7（32 位元）、Windows 8（32 位元）或 Windows 10（32 位元）作業系統的裝置硬體要求：
  - 最低需求：
    - 磁碟空間需求：
      - 安裝"應用程式啟動控制"元件 – 50 MB。
      - 安裝所有 Kaspersky Embedded Systems Security 元件 – 2 GB。
    - 記憶體：
      - 256 MB，僅在執行 Microsoft Windows 作業系統的裝置上安裝"應用程式啟動控制"元件。
      - 1 GB，執行所有元件的完整安裝。
    - 處理器要求：
      - 對於 32 位元 Microsoft Windows 作業系統：

        1.4 GHz 單核處理器。

        Intel Pentium III。
      - 對於 64 位元 Microsoft Windows 作業系統：

        1.4 GHz 單核處理器。

        Intel Pentium IV。
  - 建議需求：
    - 磁碟空間需求：
      - 安裝"應用程式啟動控制"元件 – 2 GB。
      - 安裝所有 Kaspersky Embedded Systems Security 元件 – 4 GB。
    - 記憶體：2 GB。
    - 處理器要求：2.4 GHz 四核處理器。

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

- 在應用程式安裝過程中，如果 Kaspersky Embedded Systems Security 安裝資料夾的新路徑包含超過 150 個符號，將顯示一條警告。該警告不會影響安裝過程：Kaspersky Embedded Systems Security 將成功安裝並執行。
- 要安裝 SNMP 協議支援元件，必須重新啟動 SNMP 服務（如果其正在執行）。
- 要在執行內嵌式作業系統管理的裝置上安裝和執行 Kaspersky Embedded Systems Security，必須安裝"篩選管理器"元件。
- 無法透過 Microsoft Active Directory® 群組政策安裝 Kaspersky Embedded Systems Security 管理工具。
- 在執行無法接收定期更新的早期作業系統的受防護裝置上安裝應用程式時，應檢查以下根憑證：DigiCert Assured ID Root CA、DigiCert_High_Assurance_EV_Root_CA、DigiCertAssuredIDRootCA。如果缺少這些憑證，應用程式可能無法正確執行。建議以任何可能的方式安裝這些憑證。

檔案完整性監控

預設情況下，"檔案完整性監控"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。使用者無法手動在監控範圍中包含此類資料夾。

以下資料夾/檔案從監控範圍中排除：

- 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）。

防火牆管理

- 當指定的規則範圍包含一個位址時，不能使用 IPv6 位址。
- 預設的防火牆政策支援受防護裝置與管理伺服器之間的基本互動方案。要充分利用卡巴斯基安全管理中心功能，您需要手動設定連接埠規則。您可以在卡巴斯基安全管理中心知識庫（https://support.kaspersky.com/ksc10, article 9297）中找到有關連接埠號、通訊協定及其功能的資訊。
- 如果在安裝應用程式時未將 Windows 防火牆規則和規則群組新增到工作配置中，則在防火牆管理工作期間，應用程式不對這些規則的修改進行控制。要更新狀態和包含此類規則，必須重新啟動防火牆管理工作。
- 啟動"防火牆管理"工作後，以下類型的規則會自動從作業系統的防火牆設定中刪除：
  - 拒絕規則；
  - 監控傳出流量的規則。

其他限制

自訂掃描，**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**對啟動處理程序進行更深入的分析（處理程序啟動被封鎖，直到分析結束）**核取方塊和 **KSN 使用**服務同時啟用，任何接收 URL 網址作為參數的啟動處理程序都將被封鎖，即使選擇了「僅統計」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**服務
  - 停用**對啟動處理程序的更深入分析（在分析結束之前阻止處理程序啟動）**核取方塊

  建議選項：停用對啟動處理程序的更深入分析核取方塊

產品授權：

- 如果金鑰儲存在使用 SUBST 指令建立的磁碟上，或者金鑰檔案的路徑是網路路徑，則無法透過安裝精靈使用金鑰啟動應用程式。

更新：

- 安裝 Kaspersky Embedded Systems Security 關鍵模組更新後，應用程式圖示預設隱藏。
- 執行 Windows XP 或 Windows 2003 作業系統的受防護裝置不支援 KLRAMDISK。

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。幾個正確的遮罩範例包括：“C:\Temp\Temp*”或“C:\Temp\Temp???.doc”以及“C:\Temp\Temp*.doc”。此限制不影響信任區域的配置。

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 KAVWSEE 管理員群組，才能透過點擊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視窗或 Microsoft 管理控制台管理單元的使用者身分登入。
- 如果已啟用“使用者帳戶控制”，則無法透過 Microsoft Windows 的“**程式和功能**”視窗移除應用程式。

與卡巴斯基安全管理中心整合：

- 管理伺服器在收到更新包後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。管理伺服器不驗證軟體模組更新。
- 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，確保在與管理伺服器設定的互動中選中所需核取方塊。

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”元件與執行 Microsoft Windows 10 作業系統的受防護裝置上的 Microsoft EMET 實用程式不相容：如果在安裝了 EMET 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。

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。

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

\product_long_term\ess_x86.msi 和 \product_long_term\ess_x64.msi 文件旨在安裝 Kaspersky Embedded Systems Security 的“**使用預設拒絕技術保護電腦**”配置，\product\ess_x86.msi 和 \product\ess_x64.msi 文件旨在安裝 Kaspersky Embedded Systems Security 的“**使用防毒基礎技術保護電腦**”配置。

如果選擇“使用病毒基礎技術防護電腦”配置，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 Kaspersky Embedded Systems Security 的“使用病毒基礎技術防護電腦”配置時，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
- 自訂掃描
- 網路威脅防護

啟用更新的元件不包括在“使用預設拒絕技術保護電腦”配置中。

如果選擇“使用預設拒絕技術保護電腦”配置，則預設包含以下元件：

- Core
- 弱點利用防禦
- 應用程式啟動控制
- 系統托盤圖示

在使用特徵分析和防毒資料庫來保護電腦的應用程式版本上安裝 Kaspersky Embedded Systems Security 的“使用預設拒絕技術保護電腦”配置時，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
- 自訂掃描
- - 啟用更新的元件。

建議使用此配置來保護資源有限的系統。在這種情況下，您可以長期啟動應用程式，並且“應用程式啟動控制”元件會提供電腦防護。

\console\esstools_x86.msi 和 \console\esstools_x64.msi 檔案安裝“管理工具”集內所有的軟體元件。

以下各節列出了適用於 Windows Installer 服務的 Kaspersky Embedded Systems Security 元件程式碼。透過命令列安裝 Kaspersky Embedded Systems Security 時，可使用這些代碼來定義要安裝的元件清單。

Kaspersky Embedded Systems Security 軟體元件

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

Kaspersky Embedded Systems Security 軟體元件的說明

元件	識別碼	執行功能
基本功能	Core	此元件包含基本應用程式功能集合並確保其操作。 如果您從命令列安裝 Kaspersky Embedded Systems Security 時，指定其他 Kaspersky Embedded Systems Security 元件，但未指定 Core 元件，將自動安裝 Core 元件。
應用程式啟動控制	AppCtrl	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。 它在"應用程式啟動控制"工作中執行。
裝置控制	DevCtrl	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。 該元件在"裝置控制"工作中實施。
病毒防護	AVProtection	此元件確保病毒防護並包含以下元件： • 自訂掃描 • 即時檔案防護 • 網路威脅防護
網路威脅防護	IDS	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。
自訂掃描	Ods	此元件安裝 Kaspersky Embedded Systems Security 系統檔案並提供自訂掃描工作（依要求掃描受防護裝置的物件）。
即時檔案防護	Oas	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。 其執行"即時檔案防護"工作。
卡巴斯基安全網路使用	Ksn	此元件基於 Kaspersky 雲端技術提供防護。 它執行"KSN 使用"工作（向卡巴斯基安全網路服務傳送請求及從該服務接收結論）。
檔案完整性監控	Fim	此元件可記錄指定監控範圍內針對檔案執行的操作。 該元件會執行"檔案完整性監控"工作。
註冊表存取監控	RegMonitor	此元件的設計目的是為了追蹤針對工作設定中定義的監控範圍內的指定註冊表子目錄和參數執行的操作。您可以使用該工作來偵測可能對受防護裝置造成安全弱點的變更。 該元件會實作"註冊表存取監控"工作。
弱點利用防禦	AntiExploit	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。
防火牆管理	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。 該元件執行防火牆管理工作。

整合卡巴斯基安全管理中心網路代理模組	AKIntegration	此元件提供 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。
"系統監控器"效能計數器群組	PerfMonCounters	此元件可安裝一組系統監控效能計數器。效能計數器可用來衡量 Kaspersky Embedded Systems Security 的效能，並在使用 Kaspersky Embedded Systems Security 和其他程式配合使用時確定受防護裝置潛在的瓶頸。
SNMP 計數器與 TRAP	SnmpSupport	此元件可透過 Microsoft Windows 中的簡單網路管理通訊協定 (SNMP) 發佈 Kaspersky Embedded Systems Security 計數器與 TRAP。只有受防護裝置上安裝了 Microsoft SNMP 服務時，才能在同一裝置上安裝此元件。
通知區域中的 Kaspersky Embedded Systems Security 圖示	TrayApp	此元件在受防護裝置的工作列通知區域顯示 Kaspersky Embedded Systems Security 圖示。Kaspersky Embedded Systems Security 圖示顯示裝置保護的狀態，可以用於在 Microsoft 管理主控台（如果已安裝）和"**關於應用程式**"視窗中開啟 Kaspersky Embedded Systems Security 主控台。

"管理工具"軟體元件

下表含有"管理工具"軟體元件的代碼及說明。

"管理工具"軟體元件說明

元件	代碼	元件功能
Kaspersky Embedded Systems Security 管理單元	MmcSnapin	此元件透過 Kaspersky Embedded Systems Security 主控台安裝用來管理應用程式的 Microsoft 管理主控台管理單元。 如果您透過命令列安裝"管理工具"時，指定其他元件，但未指定 MmcSnapin 元件，將自動安裝此元件。

Kaspersky Embedded Systems Security 安裝後的系統變更

當 Kaspersky Embedded Systems Security 和"管理工具"集（包括應用程式主控台）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受防護裝置上建立 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。

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，其中包含 Kaspersky Embedded Systems Security 可執行檔，具體取決於作業系統位集。因此，預設安裝資料夾如下所示：
  - 在 32 位元版本的 Microsoft Windows： %ProgramFiles%\Kaspersky Lab\Kaspersky Embedded Systems Security
  - 在 64 位元版本的 Microsoft Windows：%ProgramFiles(x86)%\Kaspersky Lab\Kaspersky Embedded Systems Security
- 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：
  - %Kaspersky Embedded Systems Security%\mibs
- 64 位元版本 Kaspersky Embedded Systems Security 可執行檔（將僅在 64 位元版本 Microsoft Windows 中安裝 Kaspersky Embedded Systems Security 的過程中建立該資料夾）：
  - %Kaspersky Embedded Systems Security%\x64
- Kaspersky Embedded Systems Security 服務檔案：
  - %ProgramData%\Kaspersky Lab\Kaspersky Embedded Systems Security\3.1\Data
  - %ProgramData%\Kaspersky Lab\Kaspersky Embedded Systems Security\3.1\Settings
  - %ProgramData%\Kaspersky Lab\Kaspersky Embedded Systems Security\3.1\Dskm

  對於 Windows XP，Kaspersky Lab 資料夾的路徑為 %ALLUSERSPROFILE%\Application Data
- 具有更新來源設定的檔案：

  %ProgramData%\Kaspersky Lab\Kaspersky Embedded Systems Security\3.1\Update

  %ProgramData%\Kaspersky Lab\Kaspersky Embedded Systems Security\3.1\Update
- 使用"複製更新"工作下載的資料庫和軟體模組更新（在第一次使用"複製更新"工作下載更新時會建立此資料夾）。

  %ProgramData%\Kaspersky Lab\Kaspersky Embedded Systems Security\3.1\Update\Distribution
- 工作記錄和系統稽核記錄。

  %ProgramData%\Kaspersky Lab\Kaspersky Embedded Systems Security\3.1\Reports
- 目前使用的資料庫集。

  %ProgramData%\Kaspersky Lab\Kaspersky Embedded Systems Security\3.1\Bases\Current
- 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\Kaspersky Embedded Systems Security\3.1\Bases\Backup
- 執行更新工作時所建立的暫存檔。

  %ProgramData%\Kaspersky Lab\Kaspersky Embedded Systems Security\3.1\Bases\Temp
- 隔離的物件（預設資料夾）。

%ProgramData%\Kaspersky Lab\Kaspersky Embedded Systems Security\3.1\Quarantine

- 備份中的物件（預設資料夾）。

  %ProgramData%\Kaspersky Lab\Kaspersky Embedded Systems Security\3.1\Backup

- 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\Kaspersky Embedded Systems Security\3.1\Restored

在應用程式主控台安裝過程中建立的資料夾

應用程式主控台預設安裝資料夾，其中包含"管理工具"檔案，具體取決於作業系統位集。因此，預設安裝資料夾如下所示：

- 在 32 位元版本的 Microsoft Windows：%ProgramFiles%\Kaspersky Lab\Kaspersky Embedded Systems Security Admins Tools
- 在 64 位元版本的 Microsoft Windows：%ProgramFiles(x86)%\Kaspersky Lab\Kaspersky Embedded Systems Security Admins Tools

Kaspersky Embedded Systems Security 服務

以下 Kaspersky Embedded Systems Security 服務使用本機系統 (SYSTEM)帳戶啟動：

- Kaspersky Security 服務 (KAVFS) – 用於管理 Kaspersky Embedded Systems Security 工作和工作流的基本 Kaspersky Embedded Systems Security 服務。
- Kaspersky Security 管理服務 (KAVFSGT) – 此服務用於透過應用程式主控台進行 Kaspersky Embedded Systems Security 應用程式。
- Kaspersky Security 弱點利用防禦服務 (KAVFSSLP) – 用作將安全設定傳輸給外部安全代理並接收有關安全事件資料的媒介的服務。

Kaspersky Embedded Systems Security 群組

"ESS 管理員"是受防護裝置上的使用者群組，其中的使用者對 Kaspersky Security 管理服務和所有 Kaspersky Embedded Systems Security 功能擁有完全存取權限。

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 的內容：
  [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\KAVFS]
- Kaspersky Embedded Systems Security 事件記錄設定（Kaspersky 事件記錄）：
  [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Eventlog\Kaspersky Security]
- Kaspersky Embedded Systems Security 管理服務的內容：
  [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\KAVFSGT]
- 效能計數器設定：

- 在 32 位元版本的 Microsoft Windows 中：
  [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Kaspersky Security\Performance]
- 在 64 位元版本的 Microsoft Windows 中：
  [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Kaspersky Security x64\Performance]

- SNMP 協定支援元件設定：
  - 在 32 位元版本的 Microsoft Windows：
    [HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\ESS\3.1\SnmpAgent]
  - 在 64 位元版本的 Microsoft Windows：
    [HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\KasperskyLab\ESS\3.1\SnmpAgent]
- Dump 檔案設定：
  - 在 32 位元版本的 Microsoft Windows：
    [HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\ESS\3.1\CrashDump]
  - 在 64 位元版本的 Microsoft Windows：
    [HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\KasperskyLab\ESS\3.1\CrashDump]
- 偵錯檔案設定：
  - 在 32 位元版本的 Microsoft Windows：
    [HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\ESS\3.1\Trace]
  - 在 64 位元版本的 Microsoft Windows：
    [HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\KasperskyLab\ESS\3.1\Trace]
- 應用程式的任務和函式的組態：
  [HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\KasperskyLab\ESS\3.1\Environment]

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
kavfswp.exe	Kaspersky Embedded Systems Security 工作流
kavtray.exe	系統托盤圖示的流程
kavfsmui.exe	小型診斷視窗元件的處理程序
kavshell.exe	命令列實用工具處理程序
kavfsrcn.exe	Kaspersky Embedded Systems Security 遠端管理處理程序
kavfs.exe	Kaspersky Security 服務處理程序
kavfsgt.exe	Kaspersky Security 管理服務處理程序
kavfswh.exe	Kaspersky Security 弱點利用防禦服務處理程序

Windows Installer 服務的安裝和移除設定及命令列選項

本節包含安裝和移除 Kaspersky Embedded Systems Security 的設定說明和預設值，以及變更安裝設定值及可變動參數。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。

Windows Installer 中的安裝設定和命令列選項

- 接受最終使用者產品授權協議的條款：您必須接受條款才能安裝 Kaspersky Embedded Systems Security。

  `EULA=<value>` 命令列選項的可能值如下：

  - `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。

- 接受隱私政策的條款：您必須接受條款才能安裝 Kaspersky Embedded Systems Security。

  `PRIVACYPOLICY=<值>` 命令列選項的可能值如下：

  - `0` – 拒絕隱私政策條款（預設值）。
  - `1` – 接受隱私政策條款。

- 如果未安裝 KB4528760 更新，允許安裝 Kaspersky Embedded Systems Security。如需 KB4528760 更新的詳細資訊，請造訪 Microsoft 網站。

  `SKIPCVEWINDOWS10=<值>` 命令列選項的可能值如下：

  - `0` – 如果未安裝 KB4528760 更新，則取消安裝 Kaspersky Embedded Systems Security（預設值）。
  - `1` – 如果未安裝 KB4528760 更新，允許安裝 Kaspersky Embedded Systems Security。

  > KB4528760 更新修復了 CVE-2020-0601 安全弱點。如需 CVE-2020-0601 安全弱點的詳細資訊，請造訪 Microsoft 網站。

- 安裝 Kaspersky Embedded Systems Security 並初步掃描活動處理程序與本機磁碟機的開機磁區。

  `PRESCAN=<值>` 命令列選項的可能值如下：

  - `0` – 在安裝過程中不執行對活動處理程序和本機磁碟機引導扇區的初步掃描（預設值）。
  - `1` – 在安裝過程中執行對活動處理程序和本機磁碟機引導扇區的初步掃描。

- 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=<資料夾的完整路徑>` 命令列選項的預設值如下：

  - Kaspersky Embedded Systems Security：%ProgramFiles%\Kaspersky Lab\Kaspersky Embedded Systems Security
  - 管理工具：%ProgramFiles%\Kaspersky Lab\Kaspersky Embedded Systems Security Admins Tools
  - 在 x64 位元版本的 Microsoft Windows 中：%ProgramFiles(x86)%

- “即時檔案防護”工作在 Kaspersky Embedded Systems Security 啟動後立即啟動。開啟該設定可在 Kaspersky Embedded Systems Security 啟動時啟動“即時檔案防護”（建議）。

  RUNRTP=<值> 命令列選項的可能值如下：

  - 1 – 啟動（預設值）。
  - 0 – 不啟動。

- Microsoft Corporation 建議的防護排除項目。在“即時檔案防護”範圍中排除裝置上 Microsoft Corporation 建議排除的物件。當防毒應用程式攔截或修改受防護裝置上某些應用程式使用的檔案時，這些應用程式可能變得不穩定。例如，當 Microsoft Corporation 將某些網域控制站應用程式納入此類物件清單時。

  ADDMSEXCLUSION=<值> 命令列選項的可能值如下：

  - 1 – 排除（預設值）。
  - 0 – 不排除。

- 按照 Kaspersky 建議從防護範圍中排除的物件。在“即時檔案防護”工作中，從防護範圍中排除裝置 Kaspersky 建議排除的物件。

  ADDKLEXCLUSION=<值> 命令列選項的可能值如下：

  - 1 – 排除（預設值）。
  - 0 – 不排除。

- 允許遠端連線到應用程式主控台。預設情況下，不允許遠端連線到安裝在受防護裝置上的應用程式主控台。安裝過程中，可允許連線。Kaspersky Embedded Systems Security 針對所有連接埠使用 TCP 協定為處理程序 kavfsgt.exe 建立允許規則。

  ALLOWREMOTECON=<值> 命令列選項的可能值如下：

  - 1 – 允許。
  - 0 – 拒絕（預設值）。

- 金鑰檔案的路徑 (LICENSEKEYPATH
)

  。預設情況下，Windows Installer 會嘗試在分發套件的 \product 資料夾中尋找副檔名為 .key 的檔案。如果 \product 資料夾包含多個金鑰檔案，Windows Installer 將選擇到期日期最晚的金鑰檔案。可以預先將金鑰檔案儲存在 \product 資料夾中，也可以使用“**新增金鑰**”設定為金鑰檔案指定其他路徑。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。

  CONFIGPATH=<設定檔名稱> 的預設值未指定。

- 使用“為應用程式主控台啟用網路連線”選項在另一台裝置上安裝 Kaspersky Embedded Systems Security 主控台。您可以從安裝了 Kaspersky Embedded Systems Security 主控台的另一台裝置遠端管理裝置防護。在 Microsoft Windows 防火牆中開放連接埠 135 (TCP)，允許透過網路連線到可執行檔 kavfsrcn.exe 以遠端管理 Kaspersky Embedded Systems Security，並授予對 DCOM 應用程式的存取權限。安裝完成後，將使用者新增到“ESS 管理員”群組中，以允許他們遠端管理應用程式並允許透過網路連線到受防護裝置上的 Kaspersky

Security 管理服務（kavfsgt.exe 檔案）。在另一台裝置上安裝 Kaspersky Embedded Systems Security 主控台後，您可以閱讀有關其他設定的更多資訊。

ADDWFEXCLUSION=<值> 命令列選項的可能值如下：

- 1 – 允許。
- 0 – 拒絕（預設值）。

- 停用不相容軟體檢查。使用此設定可啟用或停用在受防護裝置上後台安裝應用程式期間對不相容軟體的檢查。不管此設定的值如何，在 Kaspersky Embedded Systems Security 安裝期間，應用程式始終會針對受防護裝置上安裝的其他版本的應用程式發出警告。

  SKIPINCOMPATIBLESW=<值> 命令列選項的可能值如下：

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

Windows Installer 中的移除設定和命令列選項

- 還原隔離的物件。

  RESTOREQTN=<值> 命令列選項的可能值如下：

  - 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 \Quarantine 子資料夾中。

- 還原備份內容。

  RESTOREBCK=<值> 命令列選項的可能值如下：

  - 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 \Backup 子資料夾中。

- 輸入目前密碼以確認移除（如果已啟用密碼防護）。

  UNLOCK_PASSWORD=<指定密碼> 的預設值未指定。

- 還原物件的資料夾。還原的物件將儲存到指定的資料夾。

  RESTOREPATH=<資料夾的完整路徑> 命令列選項的預設值為 %ALLUSERSPROFILE%\Application Data\Kaspersky Lab\Kaspersky Embedded Systems Security\3.1\Restored

Kaspersky Embedded Systems Security 安裝和移除記錄

如果使用安裝（移除）精靈安裝（移除）Kaspersky Embedded Systems Security，Windows Installer 服務會建立安裝（移除）記錄。一個名為 ess_v3.0_install_<uid>.log（其中 <uid> 是唯一的八個字元記錄識別碼）的記錄檔案將儲存在用於啟動 setup.exe 檔案的帳戶所屬使用者的 %temp% 資料夾中。

如果從**開始**功能表執行應用程式主控台或 Kaspersky Embedded Systems Security 的**修改或移除**選項，則會在 %temp% 資料夾中自動建立名為 ess_3.0_maintenance.log 的記錄檔案。

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：

- `msiexec /i ess_x86.msi /l*v C:\ess.log /qn EULA=1 PRIVACYPOLICY=1`
- `msiexec /i ess_x86.msi /l*v C:\ess.log /qn EULA=1 PRIVACYPOLICY=1`

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。

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。

應用程式主控台含在"管理工具"應用程式元件集內。

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。

命令列實用工具包含在 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 3.1 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 \product\klcfginst.exe 包含在 Kaspersky Embedded Systems Security 分發套件中。

選擇安裝類型

指定 Kaspersky Embedded Systems Security 安裝的軟體元件後，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：

- 透過分發套件中包含的 \product\setup.exe 檔案在受防護裝置上安裝 Kaspersky Embedded Systems Security 元件。

- 透過分發套件中的 \console\setup.exe 檔案在受防護裝置或其他區網主機上安裝 Kaspersky Embedded Systems Security 主控台。

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。

您希望透過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，請執行附加配置以允許應用程式主控台使用者遠端管理 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防毒程式。
2. 確認用來啟動安裝精靈的帳戶屬於受防護裝置上的管理員群組。

完成上述操作後，繼續安裝程式。依照安裝精靈的指示，指定安裝 Kaspersky Embedded Systems Security 的安裝設定。可以在安裝精靈的任何一個步驟停止 Kaspersky Embedded Systems Security 安裝過程。若要停止安裝，請在安裝精靈視窗中點擊**"取消"**按鈕。

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. 在受防護裝置上啟動 setup.exe 檔案。
2. 在開啟的視窗的**"安裝"**部分中，按一下**"使用預設拒絕技術保護電腦"**或**"使用防毒基礎技術保護電腦"**連結。

   如果選擇"使用病毒基礎技術防護電腦"配置，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 Kaspersky Embedded Systems Security 的"使用病毒基礎技術防護電腦"配置時，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
   - 自訂掃描
   - 網路威脅防護

   啟用更新的元件不包括在"使用預設拒絕技術保護電腦"配置中。

   如果選擇"使用預設拒絕技術保護電腦"配置，則預設包含以下元件：

   - Core
   - 弱點利用防禦
   - 應用程式啟動控制
   - 系統托盤圖示

   在使用特徵分析和防毒資料庫來保護電腦的應用程式版本上安裝 Kaspersky Embedded Systems Security 的"使用預設拒絕技術保護電腦"配置時，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
   - 自訂掃描
   - - 啟用更新的元件。

   建議使用此配置來保護資源有限的系統。在這種情況下，您可以長期啟動應用程式，並且"應用程式啟動控制"元件會提供電腦防護。

3. 在 Kaspersky Embedded Systems Security 安裝精靈的歡迎頁面，點擊**"下一步"**按鈕。

   將開啟**"最終使用者產品授權協議和隱私政策"**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政策的條款和條件，請選取「**我確認我已完全閱讀、理解並接受此最終使用者產品授權協議的條款和條件**」和「**我瞭解並同意我的資料將按照隱私政策中所述進行處理和傳**

輸（包括傳輸到第三國）」。「我確認我已完全閱讀與理解隱私權政策」核取方塊以繼續安裝。

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. 點擊**"下一步"**按鈕。
   將開啟**"自訂安裝"**視窗。

7. 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。

8. 要取消所有變更，請從**"自訂安裝"**視窗中點擊**"重設"**按鈕。點擊**"下一步"**按鈕。

9. 在**"選擇目的資料夾"**視窗中：

   - 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。

   點擊**"下一步"**按鈕。

10. 在**"進階安裝設定"**視窗中，配置以下安裝設定：

    - **安裝應用程式後啟用即時防護**。
    - **將 Microsoft 建議的檔案新增到排除清單**。
    - **將 Kaspersky 建議的檔案新增到排除清單**。
      點擊**"下一步"**按鈕。

11. 在**"從設定檔匯入設定"**視窗中：

    a. 指定設定檔以從在任何先前相容版本的應用程式中建立的現有設定檔匯入 Kaspersky Embedded Systems Security 設定。

    b. 點擊**"下一步"**按鈕。

12. 在**"啟動應用程式"**視窗中，執行下列操作之一：

    - 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 \product 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。

      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"**按鈕在應用程式中套用金鑰檔案。

13. 在“**已準備安裝**”視窗中點擊“**安裝**”按鈕。精靈將開始安裝 Kaspersky Embedded Systems Security 元件。

14. 完成安裝時，會開啟“**安裝完成**”視窗。

15. 選中“**檢視發佈說明**”核取方塊，可於安裝精靈完成安裝時檢視發佈資訊。

16. 點擊“**完成**”。

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 setup.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 主控台**”連結。
   隨即會開啟“安裝精靈”歡迎視窗。

4. 點擊“**下一步>**”按鈕。

5. 在打开的窗口中，查看最终用户授权许可协议和隐私策略的条款，然后选中“**我確認我已完全閱讀、理解並接受此最終使用者產品授權協議的條款和條件**”标题下的复选框以继续安装。

6. 點擊“**下一步>**”按鈕。
   將開啟“**進階安裝設定**”視窗。

7. 在“**進階安裝設定**”視窗中：

   - 如果希望使用應用程式主控台管理遠端裝置上安裝的 Kaspersky Embedded Systems Security，請選中“**允許遠端存取**”核取方塊。
   - 將開啟“**自訂安裝**”視窗並選擇元件：

     a. 點擊“**進階**”按鈕。
        將開啟“**自訂安裝**”視窗。

     b. 從清單中選擇“管理工具”元件。
        預設情況下，安裝所有元件。

     c. 點擊“**下一步>**”按鈕。

   您可以找到有關 Kaspersky Embedded Systems Security 元件的更多詳細資訊。

8. 在“**選擇目的資料夾**”視窗中：

a. 如有需要，指定要安裝的檔案應儲存到的其他資料夾。

b. 點擊**"下一步>"**按鈕。

9. 在**"已準備安裝"**視窗中點擊**"安裝"**按鈕。

該精靈將開始安裝所選的元件。

10. 點擊**"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"集已安裝在網路中除了受防護裝置以外的任何裝置上，請設定進階設定。

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：

- 在受防護裝置上將 Kaspersky Embedded Systems Security 使用者新增到 ESS 管理員群組中。
- 如果受防護裝置使用 Windows 防火牆或協力廠商防火牆，則允許 Kaspersky Security 管理服務 (kavfsgt.exe) 進行網路連線。
- 如果在執行 Microsoft Windows 的裝置上安裝應用程式主控台期間未選中**"允許遠端存取"**核取方塊，則透過裝置的防火牆手動允許應用程式主控台的網路連線。

遠端裝置上的應用程式主控台將使用 DCOM 協議從受防護裝置上的 Kaspersky Security 管理服務接收關於 Kaspersky Embedded Systems Security 事件的資訊（如物件掃描、工作完成等）。需要在"Windows 防火牆設定"中允許應用程式主控台的網路連線，才能在應用程式主控台和 Kaspersky Security 管理服務之間建立連線。

在安裝了應用程式主控台的遠端裝置上，執行以下操作：

- 確保允許遠端匿名存取 COM 應用程式（但不是遠端啟動和啟動 COM 應用程式）。
- 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可執行檔 kavfsrcn.exe 的網路連線。

  安裝應用程式主控台的裝置將使用連接埠 TCP 135 存取受防護裝置並接收回應。

- 設定 Windows 防火牆的輸出規則以允許連線。

  與單個協定具有固定連接埠的傳統 TCP/IP 和 UDP/IP 服務不同，DCOM 會為遠端 COM 物件動態分配連接埠。如果用戶端（其中安裝了應用程式主控台）與 DCOM 端點（受防護裝置）之間存在防火牆，則必須開放很大範圍的連接埠。

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 kavfsrcn.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。
2. 選取**開始 → 執行**。
3. 輸入指令 `dcomcnfg`。
4. 點擊**"確定"**。
5. 展開受防護裝置上**元件服務主控台**中的**"電腦"**節點。
6. 開啟**"我的電腦"**節點的內容功能表。
7. 選擇**"內容"**。
8. 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。
9. 請確認在**"允許遠端存取"**視窗中為"匿名登入"使用者選定**"允許遠端存取"**的核取方塊。
10. 點擊**"確定"**。

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. 執行以下步驟之一：
   - 在 Microsoft Windows XP SP2 或更高版本中：
     a. 選擇**"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“**確定**”。

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“**確定**”。

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

新增 Windows 防火牆的輸出規則

設定的名稱可能有所不同，具體取決於安裝的 Windows 作業系統。

要為 Windows 防火牆新增輸出規則：

1. 選取**開始** > **主控台** > **Windows 防火牆**。

2. 在“**Windows 防火牆**”視窗中，點擊“**進階設定**”連結。
將開啟“**進階安全 Windows 防火牆**”視窗。

3. 選擇“**輸出規則**”子節點。

4. 在“**操作**”窗格中點擊“**新建規則**”選項。

5. 在開啟的“**新建輸出規則精靈**”視窗中，選擇“**連接埠**”選項，然後點擊“**下一步**”。

6. 選擇“**TCP**”協定。

7. 在“**特定遠端連接埠**”欄位中，指定以下允許傳出連線的連接埠範圍：1024-65535。

8. 在“**操作**”視窗中，選擇“**允許連線**”選項。

9. 儲存新規則，然後關閉“**進階安全 Windows 防火牆**”視窗。

Windows 防火牆現在將允許應用程式主控台與 Kaspersky Security 管理服務之間進行網路連線。

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 期間選中**"安裝應用程式後啟用即時防護"**（預設選項），當裝置的檔案系統物件被存取時，應用程式會掃描這些物件。Kaspersky Embedded Systems Security 將在每週五的 20:00 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 之前受防護裝置上未安裝任何具有即時檔案防護的病毒防護軟體，請在裝置上執行"關鍵區域掃描"。

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

啟動和配置 Kaspersky Embedded Systems Security 資料庫更新工作

要在安裝後更新應用程式資料庫：

1. 在"資料庫更新"工作設定中，配置與更新來源的連線 – Kaspersky HTTP 或 FTP 更新伺服器。
2. 啟動"資料庫更新"工作。

您的網路中可能未配置 Web 代理自動發現協議 (WPAD) 以在 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. 開啟"**Kaspersky Embedded Systems Security**"節點的內容功能表。
2. 選擇"**內容**"項。

   將開啟"**應用程式設定**"視窗。
3. 選擇"**連線設定**"標籤。
4. 在"**代理伺服器設定**"部分中，選中"**使用指定代理伺服器**"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. 在"**代理伺服器身分驗證設定**"部分的下拉清單中選擇必要的身分驗證方法：

   - 如果代理伺服器支援內建 Microsoft Windows NTLM 驗證方式，請**使用 NTLM 身分驗證**方式。Kaspersky Embedded Systems Security 將使用工作設定中指定的使用者帳戶存取代理伺服器（預設情況下，該工作會在**本機系統 (SYSTEM)** 使用者帳戶下執行）。

   - 如果代理伺服器支援內建 Microsoft Windows NTLM 驗證方式，請**使用帶使用者名稱和密碼的 NTLM 身分驗證**方式。Kaspersky Embedded Systems Security 將使用您指定的帳戶來存取代理伺服器。輸入使用者名

稱與密碼，或從清單選擇一個使用者。

- **套用使用者名稱和密碼**，以選擇基本身分驗證。輸入使用者名稱與密碼，或從清單選擇一個使用者。

7. 在**應用程式設定**視窗中點擊**應用程式設定**。

要設定與 Kaspersky 的更新伺服器的連線，在"資料庫更新"工作中：

1. 透過以下方式之一啟動應用程式主控台：

   - 在受防護裝置上開啟應用程式主控台。要執行此操作，請選取**開始** > **所有程式** > **Kaspersky Embedded Systems Security** > **管理工具** > **Kaspersky Embedded Systems Security 3.1 主控台**。
   - 如果應用程式主控台已在不受防護的裝置上啟動，請連線到受防護裝置：

     a. 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。

     b. 選擇"**連線至其他電腦**"項。

     c. 在"**選取受防護的裝置**"視窗中，選擇"**其他裝置**"，然後在文字欄位中，指定受防護裝置的網路名稱。

     如果用於登入到 Microsoft Windows 的帳戶沒有 Kaspersky Security 管理服務的存取權限，請指定具有所需權限的帳戶。

   將開啟應用程式主控台視窗。

2. 在應用程式主控台樹狀目錄中，展開"**更新**"節點。
3. 選擇"**資料庫更新**"子節點。
4. 在結果窗格中點擊"**內容**"連結。
5. 在開啟的"**工作設定**"視窗中，開啟"**連線設定**"標籤。
6. 選中"**使用代理伺服器設定以連線至 Kaspersky 更新伺服器**"。
7. 在**工作設定**視窗中點擊**確定**。

將儲存"資料庫更新"工作中連線更新來源的設定。

要執行"資料庫更新"工作，請執行以下操作：

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，選擇"**啟動**"項。

"資料庫更新"工作啟動。

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“**自訂掃描**”節點。
2. 在“**關鍵區域掃描**”子節點的內容功能表中，選擇“**啟動**”指令。

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。您需要先停止“即時檔案防護”工作，才能刪除“即時檔案防護”元件。其他情況下，將不需停止即時檔案防護工作或 Kaspersky 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“**開始”功能表中，選擇“**所有程式**”>“**Kaspersky Embedded Systems Security**”>“**修改或移除 Kaspersky Embedded Systems Security**”。

   將開啟安裝精靈的“**修改、修復或移除安裝**”視窗。

2. 選擇“**修改元件集**”。點擊“**下一步>**”按鈕。

   將開啟“**自訂安裝**”視窗。

3. 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：
     - “**元件將被安裝在本機硬碟上**”（如果您想要安裝一個元件）；
     - “**程式將在本機磁碟上安裝元件及其子元件**”（如果您想要安裝一組元件）。
   - 要移除先前安裝的元件，請點擊所選元件名稱旁邊的按鈕。然後在內容功能表中選擇“**元件將變為不可用**”。

   點擊“**下一步>**”按鈕。

4. 在“**已準備安裝**”視窗中，透過點擊“**安裝**”按鈕確認軟體元件集的變更。
5. 在安裝完成後開啟的視窗中，點擊“**確定**”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），您可嘗試修復 Kaspersky Embedded Systems Security。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“**開始**”功能表中，選擇“**所有程式**”。
2. 選擇“**Kaspersky Embedded Systems Security**”。
3. 選擇“**修改或移除 Kaspersky Embedded Systems Security**”。
   將開啟安裝精靈的“**修改、修復或移除安裝**”視窗。
4. 選擇“**修復已安裝元件**”。點擊“**下一步>**”按鈕。
   這會開啟“**修復已安裝元件**”視窗。
5. 在“**修復已安裝元件**”視窗中，如果您希望重設應用程式設定並使用其預設設定還原 Kaspersky Embedded Systems Security，則選中“**還原建議的應用程式設定**”核取方塊。點擊“**下一步>**”按鈕。
6. 在“**準備進行修復**”視窗中，透過點擊“**安裝**”按鈕確認修復操作。
7. 在修復操作完成後開啟的視窗中，點擊“**確定**”按鈕。

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。

在不同 Windows 作業系統中，設定的名稱可能會有所不同。

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。

如果作業系統使用 UAC 功能（使用者帳戶控制）或對應用程式的存取受密碼防護，則不能透過 Windows 控制台移除、修復和安裝應用程式。

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。

要移除 Kaspersky Embedded Systems Security：

1. 在**"開始"**功能表中，選擇**"所有程式"**。
2. 選擇**"Kaspersky Embedded Systems Security"**。
3. 選擇**"修改或移除 Kaspersky Embedded Systems Security"**。
   將開啟安裝精靈的**"修改、修復或移除安裝"**視窗。
4. 選擇**"移除軟體元件"**。點擊**"下一步>"**按鈕。
   將開啟**"進階應用程式移除設定"**視窗。
5. 如有必要，在**"進階應用程式移除設定"**視窗中：
   a. 選中**"匯出隔離區物件"**核取方塊，以從 Kaspersky Embedded Systems Security 隔離區匯出物件。預設取消選定該核取方塊。
   b. 選取**匯出備份區物件**核取方塊，以從 Kaspersky Embedded Systems Security 備份區匯出物件。預設取消選定該核取方塊。
   c. 點擊**"儲存到"**按鈕並選擇您希望將物件匯出到的資料夾。預設情況下，會將物件匯出到 %ProgramData%\Kaspersky Lab\Kaspersky Embedded Systems Security\Uninstall。
   點擊**"下一步>"**按鈕。
6. 在**"已準備移除"**視窗中，透過點選**"移除"**按鈕確認移除。
7. 在移除完成後開啟的視窗中，點擊**"確定"**按鈕。

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

Kaspersky Embedded Systems Security 主控台移除

在不同 Windows 作業系統中，設定的名稱可能會有所不同。

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**"開始"**功能表中，選擇**"所有程式"**。
2. 選擇**"Kaspersky Embedded Systems Security"**。
3. 選取**修改或移除 Kaspersky Embedded Systems Security**。
   將開啟精靈的**"修改、修復或移除安裝"**視窗。

4. 選擇“**移除軟體元件**”並點擊“**下一步>**”按鈕。

5. 將開啟“**已準備移除**”視窗。點擊“**移除**”按鈕。

   將開啟“**移除完成**”視窗。

6. 點擊“**確定**”。

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。

在使用金鑰指定安裝設定後，可透過命令列執行 \product\ess_x86.msi 或 \product\ess_x64.msi 安裝套件檔案，來安裝或移除 Kaspersky Embedded Systems Security，以及新增或移除其元件。

您可在受防護裝置或網路的另一台裝置上安裝“管理工具”集，以本機或遠端方式和應用程式主控台搭配使用。若要安裝，請使用 \console\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。

如果在沒有備用金鑰的受防護裝置上執行 \product\ess_x86.msi 或 \product\ess_x64.msi 檔案，將使用建議的安裝設定安裝 Kaspersky Embedded Systems Security。

您可使用 ADDLOCAL 命令列選項，透過列出所選的元件或元件集的代碼，來指定要安裝的元件集。

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。

在執行 32 位元版本的 Microsoft Windows 的受防護裝置上，執行分發套件中帶有 x86 尾碼的檔案。在執行 64 位元版本的 Microsoft Windows 的受防護裝置上，執行分發套件中帶有 x64 尾碼的檔案。

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.exe 檔案安裝 Kaspersky Embedded Systems Security 的範例

若要在無需與使用者互動的情況下使用建議的安裝設定安裝 Kaspersky Embedded Systems Security，請執行以下指令：

```
\product\setup.exe /s /p EULA=1 /p PRIVACYPOLICY=1
```

您可以使用以下設定安裝 Kaspersky Embedded Systems Security：

- 僅安裝"即時檔案防護"和"自訂掃描"元件；
- 在啟動 Kaspersky Embedded Systems Security 時不執行即時檔案防護；
- 不排除 Microsoft Corporation 建議從掃描範圍中排除的檔案。

要執行此操作，請執行以下指令：

```
\product\setup.exe /p ADDLOCAL=Oas /p RUNRTP=0 /p ADDMSEXCLUSION=0
```

用於安裝的指令範例：執行 .msi 檔案

若要在無需與使用者互動的情況下使用建議的安裝設定安裝 Kaspersky Embedded Systems Security，請執行以下指令：

```
msiexec /i ess.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，請執行以下指令：

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

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

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

若要安裝 Kaspersky Embedded Systems Security 並初步掃描活動處理程序與本機磁碟機的開機磁區，請執行以下指令：

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

要將 Kaspersky Embedded Systems Security 安裝在安裝資料夾 C:\ESS 中，請執行以下指令：

```
msiexec /i ess.msi INSTALLDIR=C:\ESS /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，請執行以下指令：

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

若要安裝Kaspersky Embedded Systems Security 主控台，請執行以下指令：

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

若要使用 C:\0000000A.key 檔案的金鑰安裝 Kaspersky Embedded Systems Security，並根據 C:\settings.xml 設定檔中的設定配置 Kaspersky Embedded Systems Security，請執行以下指令：

```
msiexec /i ess.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，請執行以下指令：

```
msiexec /p "<msp 檔案名及路徑>" UNLOCK_PASSWORD=<密碼>
```

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防護」，當裝置的檔案系統物件被存取時，應用程式會掃描這些物件。Kaspersky Embedded Systems Security 將在每週五晚上 8:00 鐘執行「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 資料庫更新工作。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。若要進行更新，您必須執行"資料庫更新"工作。之後，資料庫將根據預設排程，每小時更新一次。

  例如，您可執行以下指令來啟動"資料庫更新"工作：

  ```
  KAVSHELL UPDATE /KL /PROXY:proxy.company.com:8080 /AUTHTYPE:1 /PROXYUSER:inetuser
  /PROXYPWD:123456
  ```

  在此情況下，將從 Kaspersky 更新伺服器下載 Kaspersky Embedded Systems Security 資料庫更新。透過代理伺服器（代理伺服器位址：proxy.company.com，連接埠：8080）與更新來源建立連線，使用內建 Windows NTLM 驗證存取伺服器（登入帳戶的使用者名稱：inetuser；密碼：123456）。

- 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"。

若要使用命令列啟動"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。

新增和移除元件。指令範例

已自動安裝應用程式啟動控制元件。

若要安裝自訂掃描元件，請執行下列指令：

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

或

```
\product\setup.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.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.msi
ADDLOCAL=AKIntegration,AVProtection,AntiExploit,AppCtrl,DevCtrl,Fim,Ksn,LogInspector,Oas
EULA=1 PRIVACYPOLICY=1 /qn
```

列出您要安裝和移除的元件之後，Kaspersky Embedded Systems Security 會據此安裝並移除元件。

Kaspersky Embedded Systems Security 移除。指令範例

要從受防護裝置移除 Kaspersky Embedded Systems Security，請執行以下指令：

```
msiexec /x ess.msi /qn
```

或

- 對於 32 位元作業系統：
  ```
  msiexec /x {941B0F6E-2DFA-4557-90AE-D9DF81E985C2} /qn
  ```
- 對於 64 位元作業系統：
  ```
  msiexec /x {6BF23C65-7BE8-44F8-8B7F-3A6B419F6816} /qn
  ```

要移除 Kaspersky Embedded Systems Security 主控台，請執行以下指令：

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

或

```
msiexec /x {71FB9E57-9F23-4D72-B762-E0314EF3C814} /qn
```

要從已啟用密碼防護的裝置上移除 Kaspersky Embedded Systems Security，請執行以下指令：

- 對於 32 位元作業系統：
  ```
  msiexec /x {941B0F6E-2DFA-4557-90AE-D9DF81E985C2} UNLOCK_PASSWORD=*** /qn
  ```
- 對於 64 位元作業系統：
  ```
  msiexec /x {6BF23C65-7BE8-44F8-8B7F-3A6B419F6816} UNLOCK_PASSWORD=*** /qn
  ```

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	敘述
1324	目的資料夾名稱包含無效的字元。
25001	沒有足夠權限安裝 Kaspersky Embedded Systems Security。要安裝該應用程式，請使用本機管理員權限啟動安裝精靈。

25003	Kaspersky Embedded Systems Security 不能安裝在執行此版本的 Microsoft Windows 的裝置上。請啟動用於 64 位元版本 Microsoft Windows 的安裝精靈。
25004	偵測到不相容的軟體。要繼續安裝，請移除以下軟體：<不相容的軟體清單>。
25010	指定的路徑不能用於儲存已隔離的物件。
25011	用於儲存已隔離的物件的資料夾名包含無效的字元。
26251	無法下載效能計數器 DLL。
26252	無法下載效能計數器 DLL。
27300	不能安裝驅動程式。
27301	不能移除驅動程式。
27302	不能安裝網路元件。已達到所支援的篩選裝置的最大數量。
27303	無法找到病毒特徵碼資料庫。

使用卡巴斯基安全管理中心安裝和移除應用程式

本章節包含有關透過卡巴斯基安全管理中心安裝 Kaspersky Embedded Systems Security 的一般資訊。同時也介紹如何透過卡巴斯基安全管理中心安裝和移除 Kaspersky Embedded Systems Security 以及安裝 Kaspersky Embedded Systems Security 後執行的操作。

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"**遠端安裝**"方式進行安裝時，遠端安裝工作會在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

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實施手冊》。

如果希望以後透過卡巴斯基安全管理中心管理 Kaspersky Embedded Systems Security，請確保符合以下條件：

- 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還安裝了管理外掛程式（Kaspersky Embedded Systems Security 分發套件中的 \product\klcfginst.exe 檔案）。
- 請在受防護裝置上安裝卡巴斯基安全管理中心網路代理。如果卡巴斯基安全管理中心網路代理未安裝在受防護裝置上，可以使用遠端安裝工作同時安裝它與 Kaspersky Embedded Systems Security。

也可以將多台裝置整合在同一個管理群組中，以便之後使用卡巴斯基安全管理中心政策和群組工作管理防護設定。

要使用遠端安裝工作安裝 Kaspersky Embedded Systems Security：

1. 啟動卡巴斯基安全管理中心管理主控台。
2. 在卡巴斯基安全管理中心中，展開"**進階**"節點。
3. 展開"**遠端安裝**"子節點。
4. 在"**安裝套件**"子節點的結果窗格中，點擊"**建立安裝套件**"按鈕。
5. 選擇"**建立 Kaspersky 應用程式的安裝套件**"安裝套件類型。
6. 輸入安裝套件名稱。
7. 指定 Kaspersky Embedded Systems Security 分發套件中的 ess.kud 檔案為安裝套件檔案。

   將開啟"**最終使用者產品授權協議和隱私政策**"視窗。

8. 如果您同意最終使用者產品授權協議和隱私政策的條款和條件，請選取「**我確認我已完全閱讀、理解並接受此最終使用者產品授權協議的條款和條件**」和「**我瞭解並同意我的資料將按照隱私政策中所述進行處理和傳輸（包括傳輸到第三國）**」。「**我確認我已完全閱讀與理解隱私權政策**」核取方塊以繼續安裝。

   您必須接受產品授權協議和隱私政策才能繼續。

9. 要變更要安裝的 Kaspersky Embedded Systems Security 元件集以及安裝套件中的預設安裝設定：

   a. 在卡巴斯基安全管理中心中，展開**"遠端安裝"**節點。

   b. 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"**。

   c. 在**屬性：在<安裝套件名稱>**視窗中開啟**設定**部分。

      在**"要安裝的元件"**設定群組中，選中要安裝的 Kaspersky Embedded Systems Security 元件名稱旁邊的核取方塊。

   d. 要指定預設資料夾以外的目的資料夾，請在**"目的資料夾"**欄位指定資料夾名稱和路徑。

      目的資料夾的路徑可能包含系統環境變數。受防護裝置上若沒有您指定的資料夾，就會建立資料夾。

   e. 在**"進階安裝設定"**群組中，配置以下設定：

      - **在安裝之前對伺服器進行病毒掃描**
      - **安裝應用程式後啟用即時防護**
      - **將 Microsoft 建議的檔案新增到排除清單**
      - **將 Kaspersky 建議的檔案新增到排除清單**
      - **允許在作業系統啟動後，延遲啟動 Kaspersky Security 服務**

   f. 在**屬性：在<安裝套件名稱>**對話視窗中，點擊**確定**。

10. 在**"安裝套件"**節點中，建立一個工作，於選定的受防護裝置（管理群組）上遠端安裝 Kaspersky Embedded Systems Security。配置工作設定。

    要瞭解建立和配置遠端安裝工作的詳細資訊，請參見 *卡巴斯基安全管理中心說明*。

11. 執行 Kaspersky Embedded Systems Security 遠端安裝工作。

Kaspersky Embedded Systems Security 將安裝於在工作中指定的受防護裝置上。

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“資料庫更新”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. 依需要使用“關鍵區域掃描”狀態建立“自訂掃描”群組工作。卡巴斯基安全管理中心根據此工作的結果（而不是根據“關鍵區域掃描工作”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**執行系統工作**子區段的設定中停用對管理群組受防護裝置的資料庫更新工作。

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實施手冊》。

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. 在安裝套件子節點的結果窗格中，點擊“**建立安裝套件**”按鈕。建立新的安裝套件時：

   a. 在“**新建安裝套件精靈**”視窗中，選擇“**建立**指定可執行檔的安裝套件”作為安裝套件類型。

   b. 輸入新安裝套件名稱。

   c. 選擇 Kaspersky Embedded Systems Security 分發套件資料夾中的 console\setup.exe 檔案，然後選中“**將整個資料夾複製到安裝套件**”核取方塊。

   d. 如有需要，可以使用 ADDLOCAL 命令列選項來修改要在“**可執行檔啟用設定**”（可選）欄位中安裝的元件集，並修改目的資料夾。

   例如，若要在 C:\KasperskyConsole 資料夾中安裝應用程式主控台但不安裝說明檔案和文件，請使用以下命令列選項：

   ```
   /s /p "ADDLOCAL=MmcSnapin INSTALLDIR=C:\KasperskyConsole EULA=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。配置工作設定。

   要瞭解建立和配置遠端安裝工作的詳細資訊，請參見卡巴斯基安全管理中心說明。

5. 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。您只可以使用預設移除設定移除 Kaspersky Embedded Systems Security。

透過 Active Directory 群組政策安裝和移除

本章節介紹透過 Active Directory 群組政策安裝和移除 Kaspersky Embedded Systems Security。同時也包含有關透過群組政策安裝 Kaspersky Embedded Systems Security 後執行的操作的資訊。

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。

要安裝 Kaspersky Embedded Systems Security，請使用 ess_x86.msi 或 ess_x64.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. 將對應於已安裝的 Microsoft Windows 作業系統版本位元數（32 位元或 64 位元）的 msi 檔案儲存到網域控制站上的公共資料夾中。
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公共資料夾中，建立一個包含以下內容的 install_props.json 檔案，表示您接受產品授權協議和隱私政策的條款。

```
{
"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. 如同所選群組的“**使用者設定**”節點與“**電腦設定**”節點一樣，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。

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，請確認已停用該磁碟機的即時檔案防護設定。

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“**受感染**”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。要進行檢查，使用文字編輯器開啟 eicar.com 檔案，將該檔案開頭幾行文字所列的前置詞加入另一個新建檔案中，然後以新的檔案名稱（例如 eicar_cure.com）儲存。

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“受感染”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**"受感染"**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 發現包含惡意程式碼的物件。要進行檢查，您可以使用 EICAR 的測試病毒。

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公用資料夾中。

   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"工作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，工作記錄的狀態為"*緊急*"。日誌中有一行新資訊與 eicar.com 檔案中的威脅有關。（若要檢視任務日誌，在應用程式主控台樹狀結構中，展開**即時電腦防護**節點，選取**即時檔案防護**任務，在該節點的結果面板上點擊**開啟工作記錄**連結）。
  - 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公用資料夾中。

   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。

3. 執行以下操作：

   a. 在應用程式主控台樹狀目錄中展開**"自訂掃描"**節點。

   b. 選擇**"關鍵區域掃描"**子節點。

   c. 在**"設定掃描範圍"**標籤上，開啟**"網路"**節點上的內容功能表，並選擇**"新增網路檔案"**。

   d. 以 UNC 格式（通用命名慣例）輸入 eicar.com 檔在遠端裝置中的網路路徑。

   e. 選取將網路路徑新增到掃描範圍的核取方塊。

   f. 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，工作記錄的狀態為*"緊急"*。關鍵領域掃描任務日誌有一個新行與 eicar.com 檔案中的威脅資訊有關。（若要檢視任務日誌，請在應用程式主控台樹狀結構中，展開**自訂掃描**子節點，選取「關鍵領域掃描」任務，並在結果面板中，點擊**開啟工作記錄**連結）。

應用程式介面

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

- 本機應用程式主控台。
- 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 Web 主控台。
- 卡巴斯基安全管理中心雲端主控台。

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 Web 主控台和雲端主控台

卡巴斯基安全管理中心 Web 主控台（以下簡稱"Web 主控台"）是一個 Web 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。Web 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 Web 主控台的詳細資訊，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雲端主控台（以下簡稱"雲端主控台"）是以雲端為基礎的解決方案，用來防護和管理組織網路。有關卡巴斯基安全管理中心雲端主控台的詳細資訊，請參見 *卡巴斯基安全管理中心雲端主控台說明*。

使用 Web 主控台和雲端主控台可以執行以下操作：

- 監控組織安全系統的狀態。
- 在網路中的裝置上安裝 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。

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。

您可以透過以下方法檢視使用者產品授權協議的條款：

- 在 Kaspersky Embedded Systems Security 安裝期間
- 閱讀 license.txt 檔案。本檔案包含在應用程式的安裝套件中

一旦在安裝程式時確認您同意最終使用者產品授權協議，即表示您接受最終使用者產品授權協議的條款。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

*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。

有效的產品授權可使您享有以下各種服務：

- 依照最終使用者產品授權協議的條款使用應用程式
- 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

*商用版產品授權*是指購買應用程式時授予的付費產品授權。

您可以購買 Kaspersky Embedded Systems Security 標準產品授權或 Kaspersky Embedded Systems Security Compliance Edition 擴充產品授權，其中包括三個額外的系統稽核元件：File Integrity Monitor、Log Inspection 和 Registry Access Monitor。

當商業產品授權到期時，應用程式會繼續執行，但下列功能將無法使用：

- 與卡巴斯基安全網路整合
- Kaspersky Embedded Systems Security 資料庫更新

當試用產品授權到期時，應用程式繼續執行；**自訂掃描**和**即時檔案防護**工作仍然可用，但其他所有工作和 Kaspersky Embedded Systems Security 資料庫更新則無法使用。若您移除產品授權或產品授權被新增到拒絕清單中，也會發生同樣的情況。

要繼續使用 Kaspersky Embedded Systems Security 的所有功能，您必須對您的產品授權進行續約。

為確保您的裝置獲得最佳防護，我們建議您在產品授權到期之前進行續約。

確認備用金鑰的到期日在啟動日之後

關於產品授權憑證

*產品授權憑證*是您與金鑰檔案或啟動碼（如果適用）一起收到的檔案。

產品授權憑證包含以下有關目前產品授權的相關資訊：

- 訂單編號
- 有關被授予產品授權的使用者的資訊
- 有關可以使用所提供的產品授權啟動的應用程式的資訊
- 授權單元數限制（例如，執行可以使用所提供的產品授權的應用程式的裝置數量）
- 產品授權有效開始日期
- 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。

您可以透過金鑰檔案在應用程式中新增產品授權。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。

金鑰可以是“啟動金鑰”或“備用金鑰”。

*啟動金鑰*是指目前正在使用的金鑰檔案以使應用程式正常工作。可以將正式產品授權或試用產品授權的金鑰新增為啟動金鑰。應用程式只能有一個啟動金鑰。

*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。只有在具有啟動金鑰時，才能新增備用金鑰。

關於金鑰檔案

*金鑰檔案*是 Kaspersky 提供的帶有 .key 副檔名的檔案。金鑰檔案旨在透過新增產品授權金鑰來啟動應用程式。

您在購買 Kaspersky Embedded Systems Security 或訂購 Kaspersky Embedded Systems Security 試用版時提供的電子郵件信箱會收到金鑰檔案。

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。

如果意外刪除了金鑰檔案，您可以將其還原。例如，您可能需要金鑰檔案來註冊 Kaspersky CompanyAccount。

要還原金鑰檔案，請執行以下任一操作：

- 聯絡產品授權銷售商。
- 使用您可用的啟動碼透過 Kaspersky 網站 接收金鑰檔案。

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。您在購買 Kaspersky Embedded Systems Security 或訂購 Kaspersky Embedded Systems Security 試用版時提供的電子郵件信箱會收到啟動碼。

要使用啟動碼啟動應用程式，您需要網際網路存取權限以連線到 Kaspersky 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。要還原啟動碼，請聯絡 Kaspersky 技術支援。

關於資料提供

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 會在受防護電腦上本機處理和儲存一系列資料。

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。

對報告中包含的資料進行處理和儲存

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 Embedded Systems Security\<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，包括在移除 Kaspersky Embedded Systems Security 期間。

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、核對總和（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。

- 對受防護電腦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：可執行檔案的核對總和（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。
- 對受防護電腦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、核對總和和屬性。
- 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。

對使用者指定之參數的資料進行處理和儲存

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 Embedded Systems Security\<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**"匯出隔離區物件"**和**"匯出備份區物件"**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"工作規則中的可執行檔案的核對總和（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。
- 排除設定中指定的核對總和（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 允許您為本機處理的資料配置防護層級（管理 Kaspersky Embedded Systems Security 功能的存取權限，事件註冊。Kaspersky Embedded Systems Security 日誌）：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日誌記錄的功能，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，從受防護裝置移除 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。

帶診斷資訊的檔案（偵錯和 Dump 檔案）、Windows 事件記錄中的應用程式事件以及具有匯出 Kaspersky Embedded Systems Security 設定的檔案 - 建議手動刪除這些檔案。

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。

您可以透過作業系統的標準方式刪除包含 Kaspersky Embedded Systems Security 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。該元件包含在 Kaspersky Embedded Systems Security 管理工具集中，由 Microsoft 管理主控台管理單元表示。

- 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（使用透過點擊**"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參數、卡巴斯基安全管理中心政策的參數、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。

應用程式協助元件的偵錯檔案是例外，建議手動刪除這些檔案。

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：

- Kaspersky Embedded Systems Security 在主機上執行的操作。
- 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。

如果已經向 Kaspersky Embedded Systems Security 新增了啟動金鑰，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。

如果已經向 Kaspersky Embedded Systems Security 新增了備用金鑰，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。

如果已經向 Kaspersky Embedded Systems Security 新增了啟動金鑰和備用金鑰，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。

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**"授權"**節點。
2. 在**"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"**。
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。若要新增金鑰作為備用金鑰，請選中**"作為備用金鑰使用"**核取方塊。

5. 點擊**"確定"**。

將會套用選定的金鑰檔案。**"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，應用程式會建議您聯絡 Kaspersky 技術支援。

您可以使用應用程式主控台，或透過管理外掛程式或透過 Web 外掛程式建立「應用程式」群組工作的啟動程序，以啟動碼來啟動 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**"授權"**節點。
2. 在**"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，請啟用**"作為備用金鑰使用"**核取方塊。
   - 如果要檢視產品授權資訊，請點擊**"顯示產品授權資訊"**按鈕；資訊將顯示在**"產品授權資訊"**部分中。
4. 點擊**"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

檢視產品授權資訊

有關目前產品授權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。金鑰可以具有以下狀態：

- **檢查金鑰狀態** – Kaspersky Embedded Systems Security 正在檢查已套用的金鑰檔案或啟動碼，等待有關目前金鑰狀態的回應。
- **產品授權到期日期** – Kaspersky Embedded Systems Security 已啟動，且在指定日期和時間之前有效。在以下情況下，金鑰狀態突出顯示為黃色：
  - 產品授權將在 14 天後到期，並且未套用任何備用金鑰。
  - 新增金鑰已新增至拒絕清單且將被封鎖。
- **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。
- **已違反最終使用者產品授權協議** – 由於違反了最終使用者產品授權協議的條款，Kaspersky Embedded Systems Security 未啟動。狀態紅色醒目提示。

- **金鑰已在黑名單中**– 新增的金鑰已被 Kaspersky 封鎖並列入拒絕清單，例如，金鑰被協力廠商用來非法啟動程式。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**"授權"**節點。

有關目前產品授權的一般資訊顯示在**"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	敘述
啟動碼	啟動碼。如果您使用啟動碼啟動應用程式，請填寫此欄位。
啟動狀態	有關應用程式的啟動狀態的資訊。**"啟動狀態"**節點的詳細資訊窗格中**"授權"**列可具有以下狀態： • **已套用** – 如果您已使用啟動碼或金鑰檔案啟動應用程式。 • **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	用於啟動應用程式的金鑰。
產品授權類型	產品授權類型：正式或試用。
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。
啟動碼狀態或金鑰狀態	啟動碼狀態或金鑰狀態：*活動*或*附加*。

要檢視有關產品授權的詳細資訊，

在**"授權"**節點上，開啟包含您要展開的產品授權資料的行的內容功能表，然後選擇**"內容"**。

在**"金鑰內容"**視窗中，**"一般"**索引標籤顯示有關目前產品授權的詳細資訊，**"進階"**索引標籤顯示有關客戶的資訊以及 Kaspersky 或向您出售 Kaspersky Embedded Systems Security 的經銷商的聯絡人詳細資訊（請參見下表）。

"內容 <啟動碼狀態或金鑰狀態>"視窗中的詳細產品授權資訊

欄位	敘述
"一般"標籤	
金鑰	用於啟動應用程式的金鑰。
金鑰新增日期	金鑰新增到應用程式的日期。
產品授權類型	產品授權類型：正式或試用。
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。
到期日	與啟動金鑰相關聯的產品授權的到期日期和時間。如果在無期限訂購下啟動應用程式，此欄位的

期	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*。
應用程式	使用金鑰檔案或啟動碼啟動的應用程式的名稱。
金鑰使用限制	對使用金鑰的限制（如果有）。
符合技術支援需求	有關 Kaspersky 或合作夥伴之一是否將在產品授權期限下提供技術支援的資訊。
“進階”標籤	
關於產品授權的資訊	当前授权许可密钥。
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	有關產品授權所有者的資訊：客戶名稱和獲取產品授權的組織的名稱。

產品授權到期後的功能限制

產品授權到期後，以下限制將套用於功能元件：

- 除了「即時檔案防護」、「自訂掃描」和「應用程式完整性控制」工作以外，所有工作都將停止。
- 無法啟動除了「即時檔案防護」、「自訂掃描」和「應用程式完整性控制」以外的所有工作。這些工作繼續使用舊的病毒資料庫執行。
- 弱點利用防禦功能受限制：
  - 處理程序受防護至重新啟動為止。
  - 新處理程序無法新增到防護範圍中。

其他功能（儲存區、記錄、診斷資訊）仍將可用。

續約產品授權

預設情況下，當產品授權還有 14 天就要到期時，Kaspersky Embedded Systems Security 會通知您即將到期的情況。在這種情況下，“**產品授權到期日期**”節點的結果窗格中將以黃色突出顯示“**Kaspersky Embedded Systems Security**”狀態。

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，開啟“**授權**”節點。

3. 在**"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"**連結。

  b. 在開啟的視窗中，點擊**"瀏覽"**。

  c. 選擇具有 .key 副檔名的新金鑰檔案。

  d. 選中**"作為備用金鑰使用"**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"**連結。

  b. 在開啟的視窗中輸入購買的啟動碼。

  c. 選中**"作為備用金鑰使用"**核取方塊。

套用啟動碼需要網際網路連線。

4. 點擊**"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

您可以刪除新增的金鑰。

如果向 Kaspersky Embedded Systems Security 新增了備用金鑰，並且您刪除了啟動金鑰，則備用金鑰會自動變為啟動金鑰。

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。

刪除所新增的金鑰：

1. 在應用程式主控台樹狀目錄中，選擇**"授權"**節點。
2. 在包含有關已新增金鑰的資訊的表格中的**"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。

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 並包括在管理群組中的受防護裝置。 Kaspersky Security Center can also separately configure each protected device in the administration group.

*管理群組*會透過卡巴斯基安全管理中心手動建立。該群組包含您要為其設定相同的控制和防護設定且已安裝 Kaspersky Embedded Systems Security 的多部裝置。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定義相同的防護設定。在活动策略中指定的任务设置的优先级高于在应用程序控制台中本地配置或在 Kaspersky Security Center 的 "**属性：<受保护设备名称>**"窗口中远程配置的任务设置。

  您可使用政策設定一般應用程式設定、即時電腦防護工作設定、本機行為控制工作設定和排程的本機系統工作啟動設定。

- **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"**属性：<受保护设备名称>**"窗口中，您可远程配置管理组中包含的单台受保护设备的任务设置。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。

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 Web 主控台中配置 Kaspersky Embedded Systems Security 一般設定的資訊。

導航

瞭解如何透過所選介面導航到所需工作設定。

透過政策開啟一般設定

要透過政策開啟 Kaspersky Embedded Systems Security 的應用程式設定：

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。
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。
5. 在打开的**"属性：<策略名称>"**窗口中，选择**"应用程序设置"**部分。
6. 在您要配置的設定的子區段中點擊**設定**按鈕。

在應用程式內容視窗中開啟一般設定

要開啟單台受防護裝置的 Kaspersky Embedded Systems Security 內容視窗：

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**"裝置"**標籤。
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。
   - 在受防護裝置的內容功能表中選擇**"內容"**項。

   將打开**"属性：<受保护设备名称>"**窗口。
5. 在**應用程式**區段中，選取 **Kaspersky Embedded Systems Security 3.1**。
6. 點擊**"內容"**按鈕。

   Kaspersky Embedded Systems Security 3.1 設定視窗隨即開啟。
7. 選擇**"應用程式設定"部分。**

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延展性、介面和掃描設定

要配置延伸性、介面和掃描設定：

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細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"**標籤，然後開啟**"內容：<政策名稱>"**視窗。
   - 要為單台受防護裝置配置應用程式，請選擇**"裝置"**標籤，然後開啟**"應用程式設定"**視窗。

   如果某個啟動卡巴斯基安全管理中心政策已套用於裝置，並且該政策封鎖對應用程式設定的變更，則無法在**"應用程式設定"**視窗中編輯這些設定。
4. 在**"應用程式設定"**部分的**"延伸性和介面"**子區段，點擊**"設定"**。
5. 在**"進階應用程式設定"**視窗中**"一般"**標籤上，配置以下設定：
   - 在**"延伸性設定"**部分中，配置用於定義 Kaspersky Embedded Systems Security 使用的處理程序數的設定：
     - **自動偵測延伸性設定**
     - **手動設定工作處理程序數**
       - **最大活動處理程序數**
       - **用於即時防護的處理程序數**
       - **背景自訂掃描工作的處理程序數**
   - 在**"使用者互動"**部分中，透過清除或選中**"在工作列中顯示系統匣圖示"**核取方塊來配置是否在通知區域中顯示應用程式系統欄圖示。
6. 在**效能**頁籤上，配置以下設定：
   - **掃描後還原檔案屬性**
   - **限制掃描執行緒的 CPU 使用率**
     - **上限（百分比）**
   - **掃描期間建立的臨時檔案資料夾**
7. 在**"分級儲存"**標籤上，選擇存取分級儲存的選項。
8. 點擊**"確定"**。

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細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"**標籤，然後開啟**"內容：<政策名稱>"**視窗。
   - 要為單台受防護裝置配置應用程式，請選擇**"裝置"**標籤，然後開啟**"應用程式設定"**視窗。

     如果某個啟動卡巴斯基安全管理中心政策已套用於裝置，並且該政策封鎖對應用程式設定的變更，則無法在**"應用程式設定"**視窗中編輯這些設定。
4. 在**"應用程式設定"**部分，點擊**"安全性"**子區段中**"設定"**按鈕。
5. 在**"安全性設定"**視窗中，配置以下設定：
   - 在**自我防護**區段中，啟用或停用**為應用程序防護外來威脅**選項。
   - 在**"密碼防護設定"**部分中，設定用於防護存取 Kaspersky Embedded Systems Security 功能的密碼。
   - 在**"可靠性設定"**部分，您可以配置當應用程式返回錯誤或終止時 Kaspersky Embedded Systems Security 工作的還原設定。
     - **重新啟動工作**
     - **還原自訂掃描工作的次數不超過（次）**
   - 在**"轉換至 UPS 備份電源時的操作"**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：
     - **不啟動排程掃描工作**
     - **停止目前掃描工作**
   - 在**"密碼防護設定"**部分中，設定用於防護存取 Kaspersky Embedded Systems Security 功能的密碼。
6. 點擊**"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 KSN 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細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"**標籤，然後開啟**"內容：<政策名稱>"**視窗。
   - 要為單台受防護裝置配置應用程式，請選擇**"裝置"**標籤，然後開啟**"應用程式設定"**視窗。

     如果某個啟動卡巴斯基安全管理中心政策已套用於裝置，並且該政策封鎖對應用程式設定的變更，則無法在**"應用程式設定"**視窗中編輯這些設定。
4. 在**應用程式設定**區段中，點擊**連線**子區段中的**設定**按鈕。
   將開啟**"連線設定"**視窗。
5. 在**"連線設定"**視窗中，配置以下設定：
   - 在**"代理伺服器設定"**部分中，選擇代理伺服器使用設定：
     - **不使用代理伺服器**。
     - **使用指定的代理伺服器設定**。
     - 代理伺服器和埠號的 IP 位址或符號名稱。
     - **對於本機位址不使用代理伺服器**。
   - 在**"代理伺服器身分驗證設定"**部分中，指定身分驗證設定：
     - 在下拉清單中選擇身分驗證設定。
       - **不使用身分驗證** – 不執行身分驗證。預設選擇該方式。
       - **使用 NTLM 身分驗證** – 使用由 Microsoft 開發的 NTLM 網路身分驗證協定執行身分驗證。
       - **使用帶使用者名稱和密碼的 NTLM 身分驗證** – 透過由 Microsoft 開發的 NTLM 網路身分驗證協定，使用名稱和密碼執行身分驗證。
       - **套用使用者名稱和密碼** – 使用使用者名和密碼執行身分驗證。
     - 需要時，輸入使用者名稱和密碼。
   - 在**產品授權**區段中，清除或選取**啟動應用程式時使用卡巴斯基安全管理中心作為代理伺服器**。
6. 點擊**"確定"**。

將儲存設定的連線設定。

設定本機系統工作的排程啟動

您可以使用政策，根據管理群組中的每個受防護裝置上本機配置的排程，允許或封鎖啟動本機系統自訂掃描工作和更新工作：

- 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隨需掃描工作，則允許在政策中啟動本機系統工作：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、隔離區掃描、在作業系統啟動時掃描、應用程式完整性控制、基線檔案完整性監控。
- 更新工作：資料庫更新、軟體模組更新和複製更新。

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。

要在政策中允許或封鎖 Kaspersky Embedded Systems Security 系統工作的排程啟動：

1. 展開管理主控台中的**"管理服務"**節點，展開所需的群組並在**"政策"**節點中選擇該群組。
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**屬性**。
3. 在**"屬性：<策略名称>"**窗口中，打开**"应用程序设置"**部分。在**執行系統工作**區段中，點擊**設定**按鈕並執行以下操作：
   - 選中**"允許啟動自訂掃描工作"**和**"允許啟動更新工作和複製更新工作"**核取方塊以允許所列工作的排程啟動。
   - 清除**"允許啟動自訂掃描工作"**和**"允許啟動更新工作和複製更新工作"**核取方塊以停用所列工作的排程啟動。

   選擇或清除該核取方塊將不會影響任何此類本機自訂工作的啟動設定。
4. 確保您所配置的政策為啟動政策且套用於選定受防護裝置群組。
5. 點擊**"確定"**。

將為所選工作套用配置的排程工作啟動設定。

在卡巴斯基安全管理中心中配置隔離和備份設定

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細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"**標籤，然後開啟**"內容：<政策名稱>"**視窗。
   - 要為單台受防護裝置配置應用程式，請選擇**"裝置"**標籤，然後開啟**"應用程式設定"**視窗。

   > 如果某個啟動卡巴斯基安全管理中心政策已套用於裝置，並且該政策封鎖對應用程式設定的變更，則無法在**"應用程式設定"**視窗中編輯這些設定。

4. 在**"補充"**部分中，點擊**"儲存"**子區段中的**"設定"**按鈕。

5. 使用**"儲存設定"**視窗的**"備份"**標籤配置以下備份設定：

   - 若要指定備份資料夾，請使用**"備份資料夾"**欄位在受防護裝置的本機硬碟上選擇所需的資料夾，或輸入資料夾的完整路徑。
   - 若要設定最大備份大小，請選取**最大備份空間 (MB)**選取方塊，然後在輸入欄位中指定此參數的值（單位為 MB）。
   - 設定備份可用空間閾值：
     - 定義**最大備份大小 (MB)** 設定的值。
     - 選取**可用空間的閾值 (MB)** 核取方塊。
     - 指定備份資料夾中的可用空間最小值 (MB)。
   - 要為還原的物件指定資料夾，請執行以下操作之一：
     - 在**恢復設定**區段中，選取受防護裝置的本機驅動程式上的相關資料夾。
     - 在**適用於還原物件的目標資料夾**欄位中輸入資料夾的名稱及其完整路徑。

6. 在**"儲存設定"**視窗的**"隔離"**標籤上，配置以下隔離設定：

   - 若要變更隔離資料夾，請在**"隔離資料夾"**輸入欄位中指定受防護裝置本機硬碟上的資料夾完整路徑。
   - 若要設定最大隔離容量，請選定**"最大隔離區空間(MB)"**核取方塊，然後在輸入欄位中指定此參數的值（單位為 MB）。
   - 若要設定隔離儲存中的最小可用空間量，請選定**"最大隔離區空間(MB)"**核取方塊和**"可用空間上限值(MB)"**核取方塊，然後在輸入欄位中指定此參數值（單位為 MB）。
   - 若要變更將隔離中的物件還原到指定資料夾，請在**還原物件的指定資料夾**欄位中指定在受防護裝置本機硬碟上的資料夾完整路徑。

7. 點擊**"確定"**。

將儲存配置的隔離和備份設定。

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。

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

政策會在一個管理群組中的所有受防護裝置上，實行指定的 Kaspersky Embedded Systems Security 設定、功能和工作。

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。可在應用程式主控台的"**系統稽核記錄**"節點中檢視該資訊。

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*。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選取的 圖示所對應的設定值。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 圖示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（政策中標記 圖示）可在應用程式主控台中編輯。

活动策略中配置的且标记 图标的设置也会阻止在 Kaspersky Security Center 的"**属性：<受保护设备名称>**"窗口中针对一台受保护设备进行更改。

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。

如果政策為即時電腦防護工作定義設定時，此工作若正在執行中，則一旦套用政策，便將立即修改該政策所定義的設定。如果該工作未執行，就會在啟動時套用其設定。

建立政策

建立政策的過程涉及下列步驟：

1. 使用政策精靈建立政策。可以使用精靈對話方塊配置即時電腦防護工作設定。
2. 配置政策設定。在已建立政策的"**內容：<政策名稱>**"視窗中，您可以定義即時電腦防護工作設定、Kaspersky Embedded Systems Security 一般設定、隔離和備份設定、工作記錄的詳細等級以及有關 Kaspersky Embedded Systems Security 事件的使用者和管理員通知。

若要為一組執行已安裝 Kaspersky Embedded Systems Security 的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. 在選定管理群組的詳細資訊視窗中，選擇"**政策**"標籤，然後點擊"**建立政策**"連結以啟動精靈並建立政策。

   將開啟"**新建政策精靈**"視窗。

3. 在“**選擇要為其建立群組政策的應用程式**”視窗中，選擇 Kaspersky Embedded Systems Security，然後點擊“**下一步**”。

4. 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：" * < : > ? \ |。

5. 要套用以前版本的應用程式中使用的政策配置：

   a. 選中“**使用先前應用程式版本的政策設定**”核取方塊。

   b. 點擊“**選擇**”按鈕。

   c. 選擇要套用的政策。

   d. 點擊“**下一步**”。

6. 在**選取操作類型**視窗中，選取以下選項之一：

   - “**新增**”，以建立具有預設設定的新政策。
   - “**匯入使用以前版本的 Kaspersky Embedded Systems Security 建立的政策**”，以將匯入的政策當作範本。
   - 點擊“**瀏覽**”，然後選擇含有現有政策的設定檔。

7. 在“**即時電腦防護**”視窗中，根據需要配置“即時檔案防護”、“KSN 使用”工作、“弱點利用防禦”和“指令碼監控”。允許或封鎖在網路上的受防護裝置上使用配置的政策工作：

   - 點擊 按鈕允許變更網路受防護裝置上的工作設定，並封鎖套用政策中配置的工作設定。
   - 點擊 按鈕拒絕變更網路受防護裝置上的工作設定，並允許套用政策中配置的工作設定。

   新建政策使用即時電腦防護工作的預設設定。

   - 要編輯“即時檔案防護”工作的預設設定，請點擊“**即時檔案防護**”子區段中的“**設定**”按鈕。在開啟的視窗中，根據需要設定工作。點擊“**確定**”。
   - 要編輯“KSN 使用”工作的預設設定，請點擊“**KSN 使用**”子區段中的“**設定**”按鈕。在開啟的視窗中，根據需要設定工作。點擊“**確定**”。

     要啟動“KSN 使用”工作，您需要接受“**KSN 資料處理**”視窗中的 KSN 聲明。

   - 要編輯“弱點利用防禦”元件的預設設定，請點擊“**弱點利用防禦**”子區段中的“**設定**”按鈕。在開啟的視窗中，根據需要配置該功能。點擊“**確定**”。

8. 在“**為應用程式建立群組政策**”視窗中選擇下列之一的政策狀態：

   - “**啟動政策**”，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。
   - “**非啟動政策**”，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。

- 選中**"建立政策後立即開啟政策內容"**核取方塊以在點擊**"下一步"**按鈕後自動關閉**新建政策精靈**並設定新建立的政策。

9. 點擊**"完成"**按鈕。

所建立的政策將顯示在選定管理群組的**"政策"**標籤上的政策清單中。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。

Kaspersky Embedded Systems Security 政策設定部分

一般

在**"一般"**部分中，您可配置以下政策設定：

- 指定政策狀態。
- 為父政策和子政策配置繼承設定。

事件通知

在**"事件通知"**部分中，您可配置以下事件類別的設定：

- *緊急事件*
- *功能故障*
- *警告*
- *資訊訊息*
  可以使用**"內容"**按鈕來配置選定事件的以下設定：
- 指定有關記錄事件的資訊的儲存位置和保留期限。
- 指定所記錄事件的通知方式。

應用程式設定

應用程式設定的設定部分

部分	選項
延伸性和介面	在**"延伸性和介面"**子區段中，可以點擊**"設定"**按鈕來配置以下設定： • 選擇手動或自動配置延伸性設定。 • 配置應用程式圖示顯示設定。
安全性	在**"安全性"**子區段中，可以點擊**"設定"**按鈕來配置以下設定： • 配置工作執行設定。 • 指定當受防護裝置使用 UPS 電源執行時應用程式的行為。 • 啟用或停用應用程式功能的密碼防護。

連線	在“**連線**”子區段中，可以使用“**設定**”按鈕來配置與更新伺服器、啟動伺服器和 KSN 連線的以下代理伺服器設定： • 配置代理伺服器設定。 • 指定代理伺服器身分驗證設定。
執行系統工作	在**執行系統工作**子區段中，可以使用**設定**按鈕來根據受防護裝置上配置的排程允許或封鎖啟動以下本機系統工作： • 自訂掃描工作。 • 更新工作和複製更新工作。

補充

補充的設定部分

部分	選項
信任區域	點擊“**信任區域**”子區段上的“**設定**”按鈕，以配置以下信任區域應用程式設定： • 建立信任區域排除項目清單。 • 啟用或停用檔案備份操作的掃描。 • 建立受信任處理程序清單。
卸除式磁碟機掃描	在“**卸除式磁碟機掃描**”子區段中，可以使用“**設定**”按鈕來配置卸除式磁碟機的掃描設定。
應用程式管理的使用者存取權限	在“**應用程式管理的使用者存取權限**”子區段中，可以配置管理 Kaspersky Embedded Systems Security 的使用者權限和使用者群組權限。
Security 服務管理的使用者存取權限	在“**Security 服務管理的使用者存取權限**”子區段中，可以配置管理 Kaspersky Security 服務的使用者權限和使用者群組權限。
儲存	在“**儲存**”子區段中，點擊“**設定**”按鈕以配置以下“隔離”、“備份”和“封鎖的主機”設定： • 指定您想要放置隔離或備份物件的資料夾的路徑。 • 設定備份和隔離的最大大小，並指定可用空間上限值。 • 指定您想要放置從隔離區或備份區還原的物件的資料夾位置。 • 配置封鎖主機的時長。

即時電腦防護

即時電腦防護的設定部分

部分	選項
即時檔案防護	在“**即時檔案防護**”子區段中，可以點擊“**設定**”按鈕來配置以下工作設定： • 指定防護模式。

	• 配置啟發式分析的使用。 • 配置信任區域的使用。 • 指定防護範圍。 • 設定選定防護範圍的安全等級：您可選擇預定義的安全等級或手動配置安全性設定。 • 配置工作啟動設定。
KSN 使用	在“**KSN 使用**”子區段中，可以點擊“**設定**”按鈕來配置以下工作設定： • 指定要對 KSN 不信任的物件執行的操作。 • 配置卡巴斯基安全管理中心作為 KSN 代理伺服器的資料傳輸和使用。 點擊「**資料處理**」按鈕可接受或拒絕 KSN 聲明，並配置資料交換設定。
弱點利用防禦	在“**弱點利用防禦**”子區段中，可以點擊“**設定**”按鈕來配置以下工作設定： • 選擇處理程序記憶體防護模式。 • 指定降低弱點利用風險的操作。 • 新增到和編輯受防護的處理程序清單。

本機活動控制

“本機活動控制的設定”部分

部分	選項
應用程式啟動控制	在“**應用程式啟動控制**”子區段中，可以點擊“**設定**”按鈕來配置以下工作設定： • 選擇工作執行模式。 • 配置控制隨後應用程式啟動的設定。 • 指定應用程式啟動控制規則的範圍。 • 配置 KSN 的使用。 • 配置工作啟動設定。
裝置控制	在“**裝置控制**”子區段中，可以點擊“**設定**”按鈕來配置以下工作設定： • 選擇工作執行模式。 • 配置工作啟動設定。

網路活動控制

網路活動控制的設定部分

部分	選項

防火牆管理	在“**防火牆管理**”子區段中，可以點擊“**設定**”按鈕來配置以下工作設定： • 配置防火牆規則。 • 配置工作啟動設定。

系統稽核

系統稽核的設定部分

部分	選項
檔案完整性監控	在“**檔案完整性監控**”子區段中，可以配置對錶示受防護裝置上遭到安全入侵的檔案變更的控制。
記錄審查	在**記錄審查**部分中，可以根據 Windows 事件記錄分析結果配置受防護裝置的完整性監控。

記錄和通知

記錄和通知的設定部分

部分	選項
工作記錄	在“**工作記錄**”子區段中，可以點擊“**設定**”按鈕以配置以下設定： • 為選定的軟體元件指定記錄事件的重要性等級。 • 指定工作記錄儲存設定。 • 指定 SIEM 與卡巴斯基安全管理中心整合的設定。
事件通知	在“**事件通知**”子區段中，可以點擊“**設定**”按鈕以配置以下設定： • 指定“*偵測到物件*”、“*偵測到不受信任的外部裝置並已限制此裝置*”和“*不信任主機清單*”事件的使用者通知設定。 • 為“**通知設定**”部分中的事件清單中選定的任何事件指定管理員通知設定。
與管理伺服器互動	在“**與管理伺服器互動**”部分中，可以點擊“**設定**”按鈕來選擇 Kaspersky Embedded Systems Security 將報告給管理伺服器的物件類型（包括隔離物件和備份物件）。

修訂歷史

在“**修訂歷史**”部分中，可以管理修訂：與目前版本或其他政策對比、新增修訂說明、儲存修訂到檔案或執行回溯。

設定政策

<政策名稱>視窗，您可以配置：

- Kaspersky Embedded Systems Security 設定。
- 隔離和備份設定。
- 受信任區域、即時電腦防護和本機活動控制設定。
- 工作記錄的詳細層級。
- Kaspersky Embedded Systems Security 事件的使用者和管理員通知。
- 用於管理應用程式和 Kaspersky Security Service 的存取權限。

要配置政策設定：

1. 在卡巴斯基安全管理中心的管理主控台樹狀目錄中，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. 选择您想要配置的策略，然后使用以下方法之一打开"属性：<策略名称>"窗口：
   - 在政策的內容功能表中選取**屬性**選項。
   - 在所選政策的右側詳細資訊視窗中，點擊**配置政策**連結。
   - 按兩下所選政策。
4. 在**"政策狀態"**部分的**"一般"**標籤下，啟用或停用政策。為此，請選擇以下一個選項：
   - **啟動政策**，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。
   - **非啟動政策**，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。

   當管理 Kaspersky Embedded Systems Security 時，**"漫遊政策"**設定無法使用。
5. 在**"事件配置"**、**"應用程式設定"**、**"選項"**、**"記錄和通知"**以及**"修訂歷程"**部分中，可以修改應用程式配置（請參見以下表格）。
6. 在**"即時電腦防護"**、**"本機活動控制"**、**"網路活動控制"**和**"系統審查"**中，配置應用程式設定和應用程式啟動設定（參見下表）。

   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。
7. 點擊**"確定"**。

將在政策中套用配置的設定。

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：

- 啟動應用程式
- 複製更新
- 資料庫更新
- 軟體模組更新
- 資料庫更新回溯
- 自訂掃描
- 應用程式完整性控制
- 基線檔案完整性監控
- 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結果窗格中的**工作**頁籤上。
- 對於一組受防護裝置：在**裝置分類**節點的結果窗格中。

您可以使用政策停用同一管理群組中所有受防護伺服器上的更新和自訂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，並且選擇受防護裝置所屬的群組。
     b. 在**裝置**頁籤的結果窗格中，開啟受防護裝置的內容功能表，然後選取**屬性**。

c. 在開啟的視窗中，點擊**"工作"**部分中的**"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"**標籤，然後選擇**"建立工作"**。

- 要為自訂的一組受防護裝置建立工作：

  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. 選擇包含受防護裝置的管理群組。

  c. 選擇一台受防護裝置或自訂的一組受防護裝置。

  d. 從**"執行操作"**下拉清單中，選擇**"建立工作"**選項。

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 3.1** 標題下，選取要建立的工作類型。

3. 如果選擇了除"資料庫更新回溯"、"應用程式完整性控制"或"應用程式啟動"外的任何工作類型，將開啟**"設定"**視窗。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. 在**"更新來源"**視窗中選擇更新來源。

     b. 點擊**"連線設定"**按鈕。將開啟**"連線設定"**視窗。

     c. 在**連線設定**視窗上：

     指定用於連線到受防護裝置的 FTP 伺服器模式。

     根據需要修改連線到更新來源時的連線逾時值。

     配置連線到更新來源時的代理伺服器存取設定。

     指定受防護裝置的位置以最佳化更新下載。

   - 若要建立"軟體模組更新"工作，請在**"有關應用程式軟體模組更新的設定"**視窗中配置所需應用程式模組更新設定：

     a. 選擇是複製並安裝關鍵軟體模組更新，還是僅檢查它們的可用性而不安裝。

     b. 如果選擇了**"複製並安裝重要軟體模組更新"**：可能需要重新開機受防護裝置才能套用已安裝的軟體模組。如果希望工作完成時 Kaspersky Embedded Systems Security 自動重新啟動受防護裝置，請選定**"允許作業系統重新啟動"**核取方塊。

     c. 若要獲得有關 Kaspersky Embedded Systems Security 模組升級的資訊，請選擇**"接收有關可用的排程軟體模組更新的資訊"**。

     Kaspersky 不會在更新伺服器上發佈排程的軟體更新套件以供自動安裝；您可以手動從 Kaspersky 網站下載這些軟體更新套件。您可以設定有關**"有新的排程軟體模組更新可用"**事件的管理員通知。該通知將包含我們網站的 URL，以便您從中下載排程的更新。

- 若要建立“複製更新”工作，請在“**複製更新設定**”視窗中指定更新和目的資料夾。
- 要建立“啟動應用程式”工作：
  a. 在“**啟動設定**”視窗中，指定您要使用的金鑰檔案來啟動應用程式。
  b. 如果您想要建立用於續約產品授權的工作，請選中“**作為備用金鑰使用**”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。
   您可以為除「資料庫更新回溯」工作以外的所有工作類型配置排程。
5. 點擊“**確定**”。
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**選取帳戶以執行工作**視窗中，指定您要用來執行工作的帳戶。
8. 在“**定义任务名称**”窗口中，输入任务名称（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**完成建立工作**視窗中：
   a. 如果您希望工作在建立後立即啟動，請選取**精靈完成後運行工作**核取方塊。
   b. 點擊“**完成**”。

建立的工作將會在“**工作**”清單中顯示。

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

要設定單台網路受防護裝置的本機工作或一般應用程式設定：

1. 展開卡巴斯基安全管理中心管理伺服器樹狀結構中的“**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**”標籤。
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。
   - 開啟受防護裝置名稱的內容功能表，然後選擇“**內容**”。

   将打开“**属性：<受保护设备名称>**”窗口。
4. 要設定本機工作設定，請執行以下步驟：
   a. 轉至“**工作**”部分。
   b. 在工作清單中，選擇要配置的本機工作：

- 在工作清單中點擊工作名稱。
- 選擇工作名稱，然後點擊**"內容"**按鈕。
- 在所選工作的內容功能表中，選擇**"內容"**。
  將打开**"屬性：<任务名称>"**窗口。

5. 若要設定應用程式設定，請執行以下步驟：

   a. 轉至**"應用程式"**部分。

   b. 在安裝的應用程式清單中，選擇要配置的應用程式：

   - 在安裝的應用程式清單中點兩下應用程式名稱。
   - 在安裝的應用程式清單中選擇應用程式名稱，然後點擊**"內容"**按鈕。
   - 在安裝程式的單中開啟應用程式名稱的內容功能表，然後選擇**"內容"**項。
     將開啟**"<應用程式名稱>設定"**視窗。

   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，則您無法透過 **<應用程式名稱> 設定**視窗編輯這些設定。

在卡巴斯基安全管理中心中設定群組工作

從卡巴斯基安全管理中心雲端主控台管理 Kaspersky Embedded Systems Security 時，不能手動新增自訂 HTTP 和 FTP 伺服器或網路資料夾。

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選擇工作名稱，然後點擊**"配置工作"**連結。
   - 在建立的工作清單中開啟工作名稱的內容功能表，然後選擇**"內容"**項。

   在**"通知"**部分中，配置工作事件通知設定。關於本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. 根據配置的工作類型，執行下列一種操作：

- 要設定自訂掃描工作：
  - 在“**掃描範圍**”部分中，配置掃描範圍。
  - 在“**選項**”部分中，配置工作優先順序水準及與其他軟體元件的整合。
- 要配置更新工作，請根據您的需要調整工作設定：
  - 在“**設定**”部分中，配置更新來源設定和磁碟子系統最佳化。
  - 點擊“**連線設定**”按鈕以配置更新來源連線設定。
- 要配置“軟體模組更新”工作：
  - 轉到**應用程式軟體模組更新設定**區段。
  - 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。
- 若要配置“複製更新”工作，請在“**複製更新設定**”部分中指定更新和目的資料夾。
- 要建立「啟動應用程式」工作：
  - 在**啟動設定**部分中，套用您要使用的金鑰檔案來啟動應用程式。
  - 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“**作為備用金鑰使用**”核取方塊。
- 要配置裝置控制允許規則的自動建立，請在“**設定**”部分中指定將用於建立允許規則清單的設定。

6. 在“**排程**”部分中配置工作排程。您可以計劃所有工作類型，但資料庫更新回溯除外。

7. 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，請參見 *卡巴斯基安全管理中心說明*。

8. 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*。

9. 在“**內容：<工作名稱>**”視窗中，點擊“**確定**”。

將儲存新配置的群組工作設定。

下表匯總了可配置的群組工作設定。

Kaspersky Embedded Systems Security 群組工作設定

Kaspersky Embedded Systems Security 工作類型	“內容：<工作名稱>”視窗中的部分	工作設定
應用程式啟動控制規則產生器	**設定**	在配置“應用程式啟動控制規則產生器”工作設定時，您可以選擇如何建立允許規則： • **基於正在執行的應用程式建立允許規則** • **為資料夾中的應用程式建立允許規則**

	選項	當建立應用程式啟動控制的允許規則時，您可以指定執行的操作： • **使用數位憑證** • **使用數位憑證主旨和指紋** • **憑證遺失則使用** • **使用 SHA256 雜湊** • **為使用者或使用者群組產生規則** 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。
	排程	您可以配置設定以排程工作。
裝置控制規則產生器	**設定**	• 選取執行模式：考慮曾經連接過的所有外部裝置的系統資料，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。
	排程	您可以配置按排程啟動工作的設定。
啟動應用程式	**啟動設定**	要啟動應用程式或續約產品授權，可以新增金鑰檔案。
	排程	您可以配置按排程啟動工作的設定。
複製更新	**更新來源**	您可以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。
	"連線設定"視窗	在連結自**"更新來源"**部分的**"連線設定"**視窗中，您可指定是否應使用代理伺服器來建立與 Kaspersky 更新伺服器或任何其他伺服器的連線。
	複製更新設定	您可指定用於複製的更新集。 在**"用於本機儲存已複製更新的資料夾"**欄位中，指定 Kaspersky Embedded Systems Security 將用於儲存已複製更新的資料夾的路徑。
	排程	您可以配置按排程啟動工作的設定。
資料庫更新	**設定**	您可在**"更新來源"**部分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。 在"磁碟 I/O 使用最佳化"部分中，您可以配置能夠減少磁碟子系統工作負載的功能： • **降低磁碟 I/O 上的負載** • **用於最佳化 RAM(MB)**
	"連線設定"視窗	在連結自**"更新來源"**部分的**"連線設定"**視窗中，您可指定是否應使用代理伺服器來建立與 Kaspersky 更新伺服器或任何其他伺服器的連線。
	排程	您可以配置按排程啟動工作的設定。

軟體模組更新	**更新來源**	您可以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。
	"連線設定"視窗	在**"更新來源連線設定"**部分中，您可指定是否應使用代理伺服器來建立與 Kaspersky 更新伺服器或任何其他伺服器的連線。
	有關應用程式軟體模組更新的設定	您可指定關鍵軟體模組更新可用或已安裝時 Kaspersky Embedded Systems Security 應執行的操作，還可指定 Kaspersky Embedded Systems Security 是否應接收有關排程的更新的資訊。
	排程	您可以配置按排程啟動工作的設定。
自訂掃描設定	**掃描範圍**	您可指定"自訂掃描"工作的掃描範圍，並配置安全等級設定。
	"自訂掃描設定"視窗	在連結自**"掃描範圍"**部分的**"自訂掃描設定"**視窗中，可以選擇預定義安全等級之一，或手動自訂安全等級。
	選項	您可啟動或取消啟動為"自訂掃描"工作使用啟發式分析，並在**"啟發式分析"**部分中使用滑塊設定分析等級。 在**"與其他元件整合"**部分中，可以配置以下設定： • "為自訂掃描套用信任區域"工作。 • "為自訂掃描應用 KSN 使用"工作。 • 設定"自訂掃描"工作的優先順序：在背景模式下執行工作（低優先順序）或將工作視為關鍵區域掃描。
	排程	您可以配置按排程啟動工作的設定。
應用程式完整性控制	**排程**	您可以配置按排程啟動工作的設定。
基線檔案完整性監控	**排程**	您可以配置按排程啟動工作的設定。

對於"資料庫更新回溯"工作，可在**"通知"**和**"工作範圍的排除項目"**部分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*。

啟動應用程式工作

若要設定"啟動應用程式"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選擇工作名稱，然後點擊**"配置工作"**連結。
   - 在建立的工作清單中開啟工作名稱的內容功能表，然後選擇**"內容"**項。

   在**"通知"**部分中，配置工作事件通知設定。關於本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，指定您要使用的金鑰檔案來啟動應用程式。如果您想要新增用於延長產品授權的金鑰，請選中**"作為備用金鑰使用"**核取方塊。

6. 在**"排程"**部分中配置工作排程（您可以為除**"資料庫更新回溯"**以外的所有工作類型配置排程）。

7. 在**"帳戶"**部分中，指定將使用其權限執行工作的帳戶。

8. 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*。

9. 在**"內容：<工作名稱>"**視窗中，點擊**"確定"**。

   將儲存新配置的群組工作設定。

更新工作

*要配置**"複製更新"**、**"資料庫更新"**或**"軟體模組更新"**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選擇工作名稱，然後點擊**"配置工作"**連結。
   - 在建立的工作清單中開啟工作名稱的內容功能表，然後選擇**"內容"**項。

   在**"通知"**部分中，配置工作事件通知設定。關於本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**更新來源**區段中，執行以下操作：

   a. 選取更新來源：

   - 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. 點擊**"連線設定"**按鈕。

   c. 在**連線設定**區段中，配置使用代理伺服器連線到 Kaspersky 更新伺服器和其他伺服器。

   d. 對於資料庫更新工作，在**磁碟 I/O 使用最佳化**區段中，配置能夠減少磁碟子系統工作負載的功能：

   磁碟 I / O 使用率最佳化區段僅可用於「資料庫更新」工作。

   - **降低磁碟 I/O 上的負載**
   - **用於最佳化 RAM(MB)**

6. 對於「軟體模組更新」工作，在**應用程式軟體模組更新的設定**區段中，指定當關鍵軟體模組更新可用或有關計劃更新的資訊可用時，Kaspersky Embedded Systems Security 應該執行哪些操作。

   您還可以指定在安裝關鍵更新時，Kaspersky Embedded Systems Security 應該執行哪些操作。

   應用程式軟體模組更新的設定區段僅可用於「軟體模組更新」工作。

7. 對於「複製更新」工作，在**複製更新設定**區段中，指定更新集和目的地資料夾。

   複製更新設定區段僅適用於「複製更新」工作。

8. 在**"排程"**部分中配置工作排程（您可以為除"資料庫更新回溯"以外的所有工作類型配置排程）。

9. 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*。

10. 在**"內容：<工作名稱>"**視窗中，點擊**"確定"**。

將儲存新配置的群組工作設定。

對於"資料庫更新回溯"工作，可在**"通知"**和**"工作範圍的排除項目"**部分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

要配置"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選擇工作名稱，然後點擊**"配置工作"**連結。
   - 在建立的工作清單中開啟工作名稱的內容功能表，然後選擇**"內容"**項。

   在**"通知"**部分中，配置工作事件通知設定。關於本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**"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。
6. 在**"排程"**部分中配置工作排程（您可以為除"資料庫更新回溯"以外的所有工作類型配置排程）。
7. 在**"帳戶"**部分中，指定將使用其權限執行工作的帳戶。
8. 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*。
9. 在**"內容：<工作名稱>"**視窗中，點擊**"確定"**。

   將儲存新配置的群組工作設定。

在卡巴斯基安全管理中心中設定當機診斷設定

如果在操作 Kaspersky Embedded Systems Security 時發生問題（例如，應用程式當機），則可以對其進行診斷。為此，您可以為 Windows Server Kaspersky Security 程序啟用建立偵錯檔案和 Dump 檔案，並將這些檔案傳送給 Kaspersky 技術支援進行分析。

Kaspersky Embedded Systems Security 不會自動傳送任何偵錯或 Dump 檔案。診斷資料只能由具有所需權限的使用者傳送。

Kaspersky Embedded Systems Security 會以未加密的形式將資訊寫入到偵錯檔案和 Dump 檔案。儲存檔案的資料夾由使用者選擇，由作業系統配置和 Kaspersky Embedded Systems Security 設定管理。您可以配置存取權限並只允許所需使用者存取記錄、偵錯檔案和 Dump 檔案。

要在卡巴斯基安全管理中心中配置當機診斷設定：

1. 在卡巴斯基安全管理中心管理主控台中，開啟"**應用程式設定**"視窗。
2. 開啟**故障診斷**區段。
3. 如果您要應用程式將診斷資訊寫入檔案，請選中"**將診斷資訊寫入至檔案**"核取方塊。
4. 在下面的欄位中指定 Kaspersky Embedded Systems Security 將會儲存偵錯檔案的資料夾。
5. 設定診斷資訊的詳細等級。
6. 指定偵錯檔案的最大大小。
7. 指定一個偵錯記錄的最大檔案數。

   Kaspersky Embedded Systems Security 將為每個要診斷的元件建立多達最大數量的偵錯檔案。

8. 指定要診斷的元件。元件代碼必須用分號分隔。代碼區分大小寫（請參閱下表）。

Kaspersky Embedded Systems Security 子系統代碼

元件代碼	元件名稱
*	所有元件。
gui	使用者介面子系統，Microsoft 管理主控台中的 Kaspersky Embedded Systems Security 管理單元。
ak_conn	整合網路代理和卡巴斯基安全管理中心的子系統。
bl	控制處理程序，執行 Kaspersky Embedded Systems Security 控制工作。
wp	工作處理程序，處理病毒防護工作。
blgate	Kaspersky Embedded Systems Security 遠端管理處理程序。
ods	自訂掃描子系統。
oas	即時檔案防護子系統。
qb	隔離和備份子系統。
scandll	病毒掃描輔助模組。
core	基本病毒防護功能子系統。
avscan	病毒防護處理子系統。
avserv	控制病毒防護內核子系統。
prague	基本功能子系統。
updater	更新資料庫和軟體模組的子系統。
snmp	SNMP 協定支援子系統。
perfcount	效能計數器子系統。

Kaspersky Embedded Systems Security 管理單元 (gui) 和卡巴斯基安全管理中心的管理外掛程式 (ak_conn) 的偵錯設定在這些元件重新啟動後應用。SNMP 協定支援子系統 (snmp) 的偵錯設定在 SNMP 服務重新啟動後應用。效能計數器子系統 (perfcount) 的偵錯設定在所有使用效能計數器的處理程序都重新開機之後應用。當機診斷設定儲存後，其他 Kaspersky Embedded Systems Security 子系統的偵錯設定就會立刻應用。

預設情況下，Kaspersky Embedded Systems Security 會記錄所有 Kaspersky Embedded Systems Security 元件的診斷資訊。

如果選中"**將診斷資訊寫入至檔案**"核取方塊，則該輸入欄位才可用。

9. 如果您希望應用程式建立 Dump 檔案，請選中"**建立 Dump 檔案**"核取方塊。
10. 在下面的欄位中，指定 Kaspersky Embedded Systems Security 將用於儲存 Dump 檔案的資料夾。
11. 點擊"**確定**"。

已設定的應用程式設定將套用於受防護裝置上。

管理工作排程

您可以排程 Kaspersky Embedded Systems Security 工作。

排程工作

您可以在應用程式主控台中排程本機系統和自訂工作。您無法透過應用程式主控台排程群組工作。

若要使用管理外掛程式排成群組工作，請執行以下操作：

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。
2. 選取受防護裝置所屬的群組。
3. 在結果窗格中，選取"**工作**"標籤。
4. 採用以下方法之一開啟"**內容：<工作名稱>**"視窗：
   - 點擊工作的名稱。
   - 開啟工作名稱的內容功能表，然後選取"內容"項。
5. 選取"**排程**"部分。
6. 在"**排程設定**"設定塊中，選中"**依排程執行**"核取方塊。

   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。

7. 根據需要配置排程設定。為此，請執行以下操作：
   a. 在"**週期**"清單中，選擇以下值之一：
      - **每小時**，如果您希望該工作在指定的小時數內間隔執行，請在"**每 <數量> 小時**"欄位中指定小時數。

- **每天**，如果您希望該工作在指定的天數內間隔執行，請在"**每 <數量> 天**"欄位中指定天數。
- **每週**，如果您希望該工作在指定的週數內間隔執行，請在"**每 <數量> 週**"欄位中指定週數。指定啟動工作在星期中的日期（預設在星期一啟動工作）。
- **在應用程式啟動時**，如果您希望在每次啟動 Kaspersky Embedded Systems Security 時執行該工作。
- **應用程式資料庫更新後**，如果您希望在每次更新應用程式資料庫後執行該工作。

b. 在"**開始時間**"欄位中指定首次啟動工作的時間。

c. 在**開始日期**欄位中，指定啟動排程的開始日期。

在排程工作的開始時間、日期和頻率之後，會顯示下一次開始的預估時間。

前往**排程**頁籤，然後開啟**工作設定**視窗。在視窗上方的**下次開始**欄位中，會顯示預估的開始時間。每次您開啟視窗時，此預估的開始時間都會更新並顯示。

如果卡巴斯基安全管理中心政策設定禁止啟動排程的本機系統工作，則**下次開始**欄位將顯示**政策不允許**值。

8. 根據需要使用"**進階**"標籤來配置以下排程設定。
   - 在"**工作停止設定**"部分中：
     a. 選中"**持續時間**"核取方塊，並在右側的欄位中輸入工作執行的最大持續時間（小時和分鐘）。
     b. 選中"**暫停時間**"核取方塊，並在右側的欄位中輸入暫停工作執行的時間隔（小於 24 小時）的開始值和結束值。
   - 在"**進階設定**"部分中：
     a. 選中"**取消排程，從**"核取方塊，並指定停止套用排程的日期。
     b. 選定"**執行錯過的工作**"核取方塊以允許啟動略過的工作。
     c. 選中"**在該時間間隔內隨機啟動工作**"核取方塊，並按分鐘指定該值。
9. 點擊"**確定**"。
10. 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。

啟用和停用排程工作

可在配置排程設定之前或之後啟用和停用排程工作。

要啟用或停用工作啟動排程：

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，選取**"工作"**標籤。
4. 採用以下方法之一開啟**"內容：<工作名稱>"**視窗：
   - 點擊工作的名稱。
   - 開啟工作名稱的內容功能表，然後選取"內容"項。
5. 選取**"排程"**部分。
6. 執行以下操作之一：
   - 如果您希望啟用工作的啟動排程，請選中**"依排程執行"**核取方塊。
   - 如果您希望停用工作的啟動排程，請清除**"依排程執行"**核取方塊。

     不會刪除已配置的工作啟動排程設定，並將在排程的下一次工作啟動時間套用該設定。
7. 點擊**"確定"**。
8. 點擊**套用**。

將儲存已配置的工作啟動排程設定。

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*、*故障*、*未安裝*、*正在啟動*。

*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"**標籤，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. 開啟**"報告"**標籤。
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。

要檢視有關在僅統計模式下禁止的應用程式的報告：

1. 在"僅統計"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. 開啟**"報告"**標籤。

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. 在“啟動”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. 開啟“**報告**”標籤。
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。

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。

關於 Kaspersky Embedded Systems Security 主控台

Kaspersky Embedded Systems Security 主控台是您可新增到 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應用程式。

在其他裝置上安裝應用程式主控台後，需要進行進階配置。

您可以在分配給不同網域的不同受防護裝置上，安裝應用程式主控台和 Windows Server Kaspersky Security。在這種情況下，將資訊從應用程式傳送到應用程式主控台可能會受到限制。例如，任何應用程式工作啟動之後，其在應用程式主控台中的狀態可能保持不變。

在應用程式主控台安裝過程中，安裝精靈在安裝資料夾中建立了 kavfs.msc 檔案並將 Kaspersky Embedded Systems Security 管理單元新增到 Microsoft Windows 獨立管理單元的清單。

您可以從“**開始**”功能表啟動應用程式主控台。您可以執行 Kaspersky Embedded Systems Security 管理單元 msc 檔案，也可以將其作為樹狀目錄中的一個新項目新增到 Microsoft 管理主控台中。

在 64 位元版本的 Microsoft Windows 下，Kaspersky Embedded Systems Security 管理元件只能新增到 32 位元版本的 Microsoft 管理主控台中。若要新增 Kaspersky Embedded Systems Security 管理單元，請透過執行以下命令從命令行開啟 Microsoft 管理主控台：mmc.exe / 32。

您可以將多個 Kaspersky Embedded Systems Security 管理單元新增到在作者模式下開啟的 Microsoft 管理主控台中。然後，您可以管理安裝 Windows Server Kaspersky Security 的多裝置防護。

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

Kaspersky Embedded Systems Security 主控台以節點的形式顯示在 Microsoft 管理主控台樹狀目錄中。

与其他受保护设备上安装的 Kaspersky Embedded Systems Security 建立连接后，将在节点名称后面附加已安装应用程序的受保护设备的名称和建立连接时所使用的用户账户名称：**Kaspersky Embedded Systems Security < 受保护设备名称> 作为 <账户名称>**。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**。

應用程式主控台樹狀目錄

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**：管理即時電腦防護工作和 KSN 服務。**"即時電腦防護"**節點允許配置以下工作：
  - **即時檔案防護**
  - **KSN 使用**
  - **弱點利用防禦**
- **電腦控制**：控制受防護裝置上安裝的應用程式的啟動以及外部裝置連線。**"電腦控制"**節點允許配置以下工作：
  - **應用程式啟動控制**
  - **裝置控制**
  - **防火牆管理**
- **自動規則產生器**：配置"應用程式啟動控制"工作和"裝置控制"工作的群組和系統規則的自動產生。
  - **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。您無法透過應用程式主控台管理群組工作。
- **系統稽核**：設定檔操作控制和 Windows 事件記錄審查設定。
  - **檔案完整性監控**
  - **記錄審查**
- **自訂掃描**：管理自訂掃描工作。每個工作具有單獨的節點：
  - **在作業系統啟動時掃描**
  - **關鍵區域掃描**
  - **隔離區掃描**
  - **應用程式完整性控制**
  - 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 資料庫和模組更新以及將更新複製到本機更新的原始資料夾中。此節點包含一些子節點，以管理每個更新工作和上次**應用程式資料庫更新回溯**工作：
  - **資料庫更新**
  - **軟體模組更新**

- **複製更新**
- **應用程式資料庫更新回溯**

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**：管理隔離和備份設定。
  - **隔離**
  - **備份**
- **記錄和通知**：管理本機工作記錄、安全記錄和 Kaspersky Embedded Systems Security 系統稽核記錄。
  - **安全記錄**
  - **系統稽核記錄**
  - **工作記錄**
- **授權**：新增或刪除 Kaspersky Embedded Systems Security 產品授權金鑰，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，詳細資訊窗格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** 节点的上下文菜单项执行以下操作：

- **連線至其他電腦**。連線至其他裝置以管理其上安裝的 Kaspersky Embedded Systems Security。也可以點擊 **Kaspersky Embedded Systems Security** 節點的詳細資訊視窗右下角的連結來執行此操作。
- **啟動服務 / 停止服務**。啟動或停止應用程式或選定工作。要執行這些操作，您還可以使用工具列上的按鈕。也可以在程式工作的內容功能表中執行這些操作。
- **配置卸除式磁碟機掃描設定**。您可以配置透過 USB 連接埠連線到受防護裝置上的卸除式磁碟機掃描。
- **配置信任區域設定**。檢視和配置信任區域設定。
- **修改應用程式管理的使用者權限**。檢視和配置 Kaspersky Embedded Systems Security 功能的存取權限。
- **修改 Kaspersky Security 服務管理的使用者權限**。檢視和配置 Kaspersky Security 服務管理使用者權限。
- **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。
- **關於應用程式和可用模組更新的資訊**。檢視有關 Kaspersky Embedded Systems Security 和目前可用應用程式模組更新的資訊。

- **重新整理**。重新整理應用程式主控台視窗的內容。也可以在應用程式工作的內容功能表中執行此操作。
- **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。

  也可以使用 **應用程式內容** 節點的詳細資訊視窗中「**應用程式內容**」連結或工具列上的按鈕執行此操作。

- **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

可以使用應用程式主控台樹狀目錄中每個工作的內容功能表項來管理 Kaspersky Embedded Systems Security 工作。

可使用內容功能表項執行以下操作：

- **啟動 / 停止**。啟動或停止工作執行。要執行這些操作，您還可以使用工具列上的按鈕。
- **繼續/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“即時電腦防護”工作和“自訂掃描”工作。
- **新增工作**。新建自訂工作。此操作適用於自訂掃描工作。
- **開啟記錄**。檢視和管理工作記錄。此操作適用於所有工作。
- **移除工作**。刪除自訂工作。此操作適用於自訂掃描工作。
- **設定範本**。管理範本。此操作適用於“即時檔案防護”和“自訂掃描”。

通知區域中的系統托盤圖示

每次重啟受防護裝置之後，當 Kaspersky Embedded Systems Security 自動啟動時，系統托盤圖示將顯示在工具列通知區域 中。如果在應用程式設定期間安裝了“系統托盤圖示”元件，則預設情況下將顯示該圖示。

系統匣圖示的外觀反映了目前裝置的防護狀態。狀態有兩種：

	啟動（彩色圖示）- 如果目前有以下至少一個工作正在執行：即時檔案防護、應用程式啟動控制
	不啟動（灰色圖示）- 如果目前未執行任何工作：即時檔案防護、應用程式啟動控制

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	敘述
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	開啟小型診斷視窗。

視窗	
關於應用程式	開啟**關於應用程式**視窗，其中包含有關 Kaspersky Embedded Systems Security 的資訊。 對於註冊的 Kaspersky Embedded Systems Security 使用者，**關於應用程式**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**開始**功能表中，選擇「**所有程式** > **Kaspersky Embedded Systems Security** > **系統匣圖示**」。

設定的名稱可能有所不同，具體取決於安裝的作業系統。

在 Kaspersky Embedded Systems Security 的一般設定中，您可以啟用或停用系統托盤圖示在每次受防護裝置重啟後應用程式自動啟動時的顯示。

透過其他裝置上的應用程式主控台管理 Kaspersky Embedded Systems Security

您可透過遠端裝置上安裝的應用程式主控台管理 Kaspersky Embedded Systems Security。

要使用遠端裝置上的 Kaspersky Embedded Systems Security 主控台管理應用程式，請確保：

- 遠端裝置上的應用程式主控台使用者已新增到受防護裝置上的 ESS 管理員群組。
- 如果在受防護裝置上啟用 Windows 防火牆，將允許 Kaspersky Security 管理服務處理程序 (kavfsgt.exe) 連線網路。
- 在安裝 Kaspersky Embedded Systems Security 的過程中，在"安裝精靈"視窗中選中**"允許遠端存取"**核取方塊。

如果遠端裝置上的 Kaspersky Embedded Systems Security 受密碼防護，輸入密碼以透過應用程式主控台獲取對應用程式管理的存取權限。

透過應用程式主控台配置一般應用程式設定

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，則無法在應用程式主控台中配置這些設定。

要配置 Kaspersky Embedded Systems Security 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：

   - 在節點的詳細資訊視窗中，點擊**"應用程式內容"**連結。
   - 在節點的內容功能表中選取**內容**。

   將開啟**"應用程式設定"**視窗。

2. 在開啟的視窗中，根據需要配置 Kaspersky Embedded Systems Security 一般設定：

   - 可在**"延伸性和介面"**標籤上配置以下設定：
     - 在**"延伸性設定"**部分：
       - Kaspersky Embedded Systems Security 可以執行的最大工作處理程序數
       - 用於即時電腦防護的處理程序數
       - 背景自訂掃描工作的工作處理程序數量
   - 在**"使用者互動"**部分中，選擇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。
   - 可在**"安全性和可靠性"**標籤上配置以下設定：
     - 在**密碼防護設定**部分，配置對應用程式處理程序的防護。
     - 在**"密碼防護設定"**部分中，配置應用程式功能的密碼防護設定。
     - 在**"自主防禦"**部分中，指定自訂掃描工作崩潰後還原該工作的嘗試次數。
   - 在**復原隨需掃描工作不超過 (次數)**部分，指定在轉換為 UPS 備份電源後 Kaspersky Embedded Systems Security 執行的操作。
   - 在**掃描設定**頁籤上：
     - **掃描後還原檔案屬性**
     - **限制掃描執行緒的 CPU 使用率**
       - **上限（百分比）**
     - **掃描期間建立的臨時檔案資料夾**
   - 在**"連線設定"**選項上：
     - 在**"代理伺服器設定"**部分中，指定代理伺服器使用設定。
     - 在**"代理伺服器身分驗證設定"**部分中，指定在代理伺服器上進行身分驗證所需的身分驗證類型和詳細資訊。
     - 在**"授權"**部分中，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**"故障診斷"**選項上：

- 如果您要應用程式將診斷資訊寫入檔案，請選中“**將診斷資訊寫入至檔案**”核取方塊。
  - 在下面的欄位中指定 Kaspersky Embedded Systems Security 將會儲存偵錯檔案的資料夾。
  - 設定診斷資訊的詳細等級。
  - 指定偵錯檔案的最大大小。
  - 指定一個偵錯記錄的最大檔案數。Kaspersky Embedded Systems Security 將為每個要診斷的元件建立多達最大數量的偵錯檔案。
  - 指定要診斷的元件。
- 如果您希望應用程式建立 Dump 檔案，請選中“**建立故障傾印檔案**”核取方塊。

Kaspersky Embedded Systems Security 不會自動傳送任何偵錯或 Dump 檔案。診斷資料只能由具有相應權限的使用者傳送。

- 在下面的欄位中，指定 Kaspersky Embedded Systems Security 將用於儲存 Dump 檔案的資料夾。

Kaspersky Embedded Systems Security 會以未加密的形式將資訊寫入到偵錯檔案和 Dump 檔案。儲存檔案的資料夾由使用者選擇，由作業系統配置和 Kaspersky Embedded Systems Security 設定管理。您可以配置存取權限並只允許所需使用者存取記錄、偵錯檔案和 Dump 檔案。

3. 點擊“**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、自訂掃描和更新功能作為工作實現。

您可以使用應用程式主控台樹狀目錄中的工作內容功能表、工具列和快速存取工作列來管理工作。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。您可以編輯除了「隔離區掃描」和「資料庫更新回溯」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，您可建立自訂掃描工作。在卡巴斯基安全管理中心中，您可建立自訂掃描、資料庫更新、資料庫更新回溯和複製更新工作。您可以重新命名，配置和刪除自訂工作。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

您可以只暫停和還原即時電腦防護和自訂掃描工作。不能手動暫停或恢復其他工作。

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. 選擇以下工作之一：**"啟動"**、**"暫停"**、**"繼續"**或**"停止"**。

   該操作將執行並記錄到系統稽核記錄中。

當您恢復隨需掃描工作時，Kaspersky Embedded Systems Security 將從暫停掃描的物件恢復掃描。

管理工作排程

您可以排程 Kaspersky Embedded Systems Security 工作。

配置工作啟動排程設定

在應用程式主控台中，您可以排程何時啟動本機系統和自訂工作。但是，您無法排程何時開始群組工作。

要排程工作：

1. 開啟要排程的內容功能表。
2. 選擇**"內容"**。
   將開啟**"工作設定"**視窗。
3. 在開啟的視窗中的**"排程"**標籤上，選中**"依排程執行"**核取方塊。
4. 請按照以下步驟指定排程設定：

a. 在**週期**下拉功能表中，選取以下值之一：

- **每小時**：每隔一小時執行一次工作；在**每 <數目> 小時**欄位中指定時數。
- **每天**：每天執行一次工作；在**每** <數目> **天天**欄位中指定天數。
- **每週**：每週執行一次工作；在**每**<數目> **週**欄位中指定週數。指定工作啟動的星期中的日期（預設在星期一啟動工作）。
- **在應用程式啟動時**，如果您希望在每次啟動 Kaspersky Embedded Systems Security 時執行該工作。
- **應用程式資料庫更新後**，如果您希望在每次更新應用程式資料庫後執行該工作。

b. 在**開始時間**欄位中，指定首次啟動工作的時間。

c. 在**開始日期**欄位中，指定首次啟動工作的日期。

指定了工作啟動頻率之後，將在視窗頂部的**"下次開始"**欄位中顯示工作的首次啟動時間、排程的開始套用日期以及預計下一個工作啟動時間的相關資訊。每次開啟**"工作設定"**視窗的**"排程"**標籤時，將更新並顯示下次工作開啟的估計時間。

如果卡巴斯基安全管理中心活動政策設定禁止啟動排程的本機系統工作，則**下次開始**欄位將顯示**政策不允許**值。

5. 使用**進階**頁籤可以指定以下排程設定：

- 在**"工作停止設定"**部分中：
  a. 選取**持續時間**核取方塊。在右側的欄位中，以小時和分鐘為單位輸入最大工作持續時間。
  b. 選取**暫停開始於**核取方塊。在右側的欄位中，輸入暫停和繼續執行工作的時間（24小時以內）。
- 在**"進階設定"**部分中：
  a. 選取**取消排程開始於**核取方塊，然後指定工作排程的結束日期。
  b. 所選**執行錯過的工作**核取方塊以允許啟動略過的工作。
  c. 選中**"在該時間間隔內隨機啟動工作"**核取方塊，並按分鐘指定該值。

6. 點擊**"確定"**。

工作排程設定隨即儲存。

啟用和停用排程工作

可在指定工作排程設定之前或之後啟用和停用排程工作。

要啟用或停用排程工作啟動：

1. 在應用程式主控台樹狀目錄中，開啟排程工作的內容功能表。

2. 選擇“**內容**”。
   將開啟“**工作設定**”視窗。
3. 在開啟的視窗中的**排程**標籤上，選取其中一個以下選項：
   - 請選取**依排程執行**核取方塊啟用工作的啟動排程。
   - 請清除**依排程執行**核取方塊來停用工作的啟動排程。

     工作排程設定不會被刪除，而是在您下次啟用排程的工作啟動時套用。
4. 點擊“**確定**”。

工作排程設定隨即儲存。

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
- 自訂掃描
- 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：

- **更新**工作：如果您已指定在網路上其他裝置的公共資料夾作為更新來源。
- **更新**工作，如果使用內建 Windows NTLM 身分驗證的代理伺服器來存取更新來源。
- **隨選掃描**工作：如果系統帳戶對已掃描的物件不具有存取權限（例如，對受防護裝置上的共用資料夾中檔案的存取權限）。
- **應用程式啟動控制規則產生器**工作：如果在完成工作後，將建立的規則匯出到位於系統帳戶無法存取（例如，受防護裝置上的共用資料夾）的設定檔。

您可以使用系統帳戶權限執行更新、自訂掃描和規則產生器工作。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

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，開啟要使用特定帳戶啟動的工作的內容功能表。
2. 選擇**"內容"**。
   將開啟**"工作設定"**視窗。
3. 在開啟的視窗中，在**執行帳戶**頁籤上，請按照下列步驟操作：
   a. 選擇**"使用者名稱"**。
   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，或者與該受防護裝置在同一網域中。

   c. 確認密碼。
4. 點擊**"確定"**。

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。您還將學習如何將特定的軟體設定匯出到 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
- KSN 使用
- 裝置控制
- 應用程式啟動控制
- 裝置控制規則產生器
- 應用程式啟動控制規則產生器

- 自訂掃描工作
- 檔案完整性監控
- 記錄審查器
- Kaspersky Embedded Systems Security 資料庫和軟體模組更新
- 隔離
- 備份
- 記錄
- 管理員和使用者通知
- 信任區域
- 弱點利用防禦
- 密碼防護

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。

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。將設定匯入至其他受防護裝置之後，必須手動輸入所有密碼。

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。

可以從包含 Kaspersky Embedded Systems Security 個別元件參數的設定檔（例如從未安裝完整元件的 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. 在應用程式主控台樹狀目錄中，執行以下操作之一：
   - 在 **Kaspersky Embedded Systems Security** 節點的內容功能表中，選擇**"匯出設定"**可匯出所有 Kaspersky Embedded Systems Security 設定。
   - 在特定工作的內容功能表中，選取**匯出設定**來匯出程式的單一功能元件的設定。

- 要匯出「信任的區域」設定，請執行以下操作：

  a. 在應用程式主控台樹狀目錄中，開啟 **Kaspersky Embedded Systems Security** 節點內容功能表。

  b. 選擇**"配置信任區域設定"**。
  將開啟**"信任區域"**視窗。

  c. 點擊**"匯出"**按鈕。
  設定匯出精靈隨即開啟。

2. 按照**匯出設定精靈**的說明操作：指定要用來儲存設定目標的設定檔名稱和路徑。
   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. 點擊**"關閉"**視窗中的**"程式設定匯出已完成"**按鈕。

設定匯出精靈將關閉並儲存匯出設定。

匯入設定

若要從儲存的設定檔匯入設定：

1. 在應用程式主控台樹狀目錄中，執行以下操作之一：

   - 在 **Kaspersky Embedded Systems Security** 節點的內容功能表中，選擇**"匯入設定"**可匯入所有 Kaspersky Embedded Systems Security 設定。
   - 在指定工作的內容功能表中，選取**匯入設定**來匯入程式的單一功能元件的設定。
   - 要匯入「信任的區域」設定，請執行以下操作：

     a. 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。

     b. 選擇**"配置信任區域設定"**。
     將開啟**"信任區域"**視窗。

     c. 點擊**"匯入"**按鈕。
     「設定匯入精靈」隨即開啟。

2. 請按照**匯入設定精靈**的指示操作：指定要匯入且含設定的組態檔案。

   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。

3. 在**"關閉"**視窗中，點擊**"程式設定匯入已完成"**按鈕。
   設定匯入精靈將關閉並儲存匯入的設定。

4. 在「應用程式主控台」工具列中，點擊**重新整理**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。

使用安全性設定範本

本節包含有關在 Kaspersky Embedded Systems Security 防護和掃描工作中使用安全性設定範本的資訊。

關於安全性設定範本

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性設定，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。

您可使用範本來指定以下 Kaspersky Embedded Systems Security 工作的安全性設定：

- 即時檔案防護
- 在作業系統啟動時掃描
- 關鍵區域掃描
- 自訂掃描工作

套用到受防護裝置檔案資源樹狀目錄中的父節點的範本中的安全性設定將套用到所有子節點中。以下情況中父節點的範本不套用於子節點：

- 如果單獨指定的子節點的安全設定。
- 如果子節點為虛擬節點。在此情況下，您必須針對每個虛擬節點單獨套用範本。

建立安全性設定範本

要手動將節點的安全性設定儲存到範本：

1. 在應用程式主控台樹狀目錄中，選取要為其建立安全性設定範本的工作。
2. 在所選工作的詳細資訊視窗中，點擊**"配置防護範圍"**或**"配置掃描範圍"**連結。
3. 在受防護裝置的網路檔案資源樹狀目錄或清單中，選取要檢視的範本。
4. 在**安全等級**頁籤上，點擊**另存為範本**按鈕。
   將開啟**"範本內容"**視窗。

5. 在**"範本名稱"**欄位中，輸入範本名稱。

6. 在**描述**欄位中，輸入其他範本資訊。

7. 點擊**"確定"**。

安全等級設定隨即儲存。

檢視範本中的安全性設定

要在您建立的範本中查看安全性設定，請執行以下操作：

1. 在「應用程式主控台」樹狀目錄中，選取要查看其安全性設定範本的工作。

2. 在選定工作的內容功能表中，選擇**"設定範本"**。
   將開啟**"範本"**視窗。

3. 在開啟的視窗中的範本清單中，選取要檢視的範本。

4. 點擊**"檢視"**按鈕。

將開啟**"<範本名稱>"**視窗。**一般**頁籤顯示範本名稱和有關範本的其他資訊。**選項**頁籤列出了範本中儲存的安全設定。

套用安全性設定範本

要將範本中的安全性設定套用於所選節點：

1. 在應用程式主控台樹狀目錄中，選擇要對其套用安全性設定範本的工作。

2. 在所選工作的詳細資訊視窗中，點擊**"配置防護範圍"**或**"配置掃描範圍"**連結。

3. 在受防護裝置網路檔案資源樹狀目錄或清單中，開啟要對其套用範本的節點或項的內容選單。

4. 選取**"套用範本"**→**"<範本名稱>"**。

5. 點擊**"儲存"**按鈕。

這會將安全設定範本應用於受防護裝置的檔案資源樹中的所選節點。所選節點的**安全等級**頁籤上的值將更改為**自訂**。

若套用到受防護裝置檔案資源樹狀目錄中，父節點範本中的安全性設定將套用到所有子節點中。

您可以在受防護裝置的檔案資源樹狀目錄中分別配置子節點的防護或掃描範圍。在這種情況下，應用於父節點的範本的安全設定不會自動應用於子節點。

要將範本中的安全性設定套用於所有所選節點：

1. 在應用程式主控台樹狀目錄中，選擇要對其套用安全性設定範本的工作。

2. 在所選工作的詳細資訊視窗中，點擊**"配置防護範圍"**或**"配置掃描範圍"**連結。

3. 在受防護裝置網路檔案資源樹狀目錄或清單中，選取一個父節點，以將範本套用於所選的節點和其子節點。

4. 在右鍵選單中，選取**"套用範本 → <範本名稱>"**。

5. 點擊**"儲存"**按鈕。

將對受防護裝置檔案資源樹狀目錄中的父節點和所有子節點套用安全性設定範本。所選節點的**安全等級**頁籤上的值將更改為**自訂**。

刪除安全性設定範本

要刪除安全性設定範本：

1. 在「應用程式主控台」樹狀目錄中，選取要刪除的帶有安全性設定範本的工作。

2. 在選定工作的內容功能表中，選擇**"設定範本"**。
將開啟**"範本"**視窗。

> 在**自訂掃描**父節點的結果窗格中，您可以查看自訂掃描工作的設定範本。

3. 在開啟的視窗中的範本清單中，選取要刪除的範本。

4. 點擊**"刪除"**按鈕。
將開啟一個視窗，提示您確認刪除。

5. 在開啟的視窗中，點擊**"是"**。

將刪除所選範本。

> 您可以應用安全設定範本來防護或掃描受防護裝置的檔案資源樹狀目錄中的節點。在這種情況下，刪除範本後，此類節點的安全設定將保持不變。

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，

在應用程式主控台樹狀目錄中，選擇**"Kaspersky Embedded Systems Security"**節點。

預設情況下，將自動重新整理應用程式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。

應用程式主控台的詳細資訊窗格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。

使用不同的顏色指示防護狀態：

- *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。

"**卡巴斯基安全網路使用情況**"部分顯示目前工作狀態，例如，*正在執行*、*已停止*或*從未執行*。該指示器可以使用的設定值如下：

- 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。
- 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。

電腦防護

"**電腦防護**"部分（請參見下表）顯示有關裝置目前防護狀態的資訊。

有關裝置防護狀態的資訊

"防護"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： • 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。 • 黃色 – "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。

	• 紅色 – "即時檔案防護"工作未執行。
即時檔案防護	**工作狀態** – 目前工作狀態，例如，"*正在執行*"或"*已停止*"。 **偵測到** – 由 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應用程式，該欄位中的值將增加 1。如果偵測到的惡意應用程式數量超過 0，此值會以紅色醒目提示。
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。
弱點利用防禦	**狀態** – 弱點利用防禦技術的目前狀態，例如，"*已應用*"或"*未套用*"。 **防禦模式** – 可用的兩個模式之一，在配置處理程序記憶體防護的過程中選擇：**發現弱點利用時終止**或**僅統計**。 **防護的處理程序** – 根據選定的模式新增到防護範圍並處理的處理程序總數。
已備份物件	*已超過備份區可用空間上限值* – 當備份區可用空間量接近指定限制時會發生該事件。Kaspersky Embedded Systems Security 繼續將物件移至備份區。在這種情況下，"**已用空間**"欄位高亮顯示為黃色。 *已超過最大備份容量* – 當備份區大小已達到指定限制時會發生此事件。Kaspersky Embedded Systems Security 繼續將物件移至備份區。在這種情況下，"**已用空間**"欄位高亮顯示為紅色。 **已備份物件** – 目前在備份區中的物件數量。 **已用空間** – 已使用的備份區空間容量。

更新

"**更新**"部分（請參見下表）顯示有關病毒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

"更新"部分	資訊
資料庫和軟體模組狀態指示器	帶有部分名稱的面板的顏色反映了應用程式資料庫和模組的狀態。該指示器可以使用的設定值如下： • 綠色 – 預設顯示此顏色，指示應用程式資料庫處於最新狀態，並且最近的資料庫更新工作已成功完成。 • 黃色 – 資料庫已過期，或上次資料庫更新工作失敗。 • 紅色 – 發生*應用程式資料庫已嚴重過期*或*應用程式資料庫已損壞*事件。
資料庫更新和**軟體模組更新**	**資料庫狀態** – 資料庫更新狀態的評估。 它可能呈現是以下設定值： • **應用程式資料庫為最新** – 應用程式資料庫在之前 7 天內進行過更新（預設）。 • **應用程式資料庫已過期** – 應用程式資料庫在之前 7 至 14 天內進行過更新（預設）。 • **應用程式資料庫已嚴重過期** – 應用程式資料庫在超過 14 天前進行過更新（預設）。您可以變更用於建立*應用程式資料庫為最新*和*應用程式資料庫已嚴重過期*的事件上限值。 **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 – 最新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，則欄位為紅色。 **可用模組更新數** – 可供下載和安裝的 Kaspersky Embedded Systems Security 模組更新數量。 **已安裝模組更新數** – 已安裝的 Kaspersky Embedded Systems Security 模組更新數量。

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"防火牆管理"工作的資訊。

有關受防護裝置控制狀態的資訊

"控制"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： • 綠色 – 預設顯示此顏色，指示"應用程式啟動控制"元件已安裝，且工作在"**活動**"模式下執行。 • 黃色 – "應用程式啟動控制"在"**僅統計**"模式下執行。 • 紅色 – "應用程式啟動控制"工作未執行或失敗。
應用程式啟動控制	**工作狀態** – 目前工作狀態，例如，"*正在執行*"或"*已停止*"。 **執行模式** – "應用程式啟動控制"工作兩種可用模式中的一種："**活動**"或"**僅統計**" **應用程式啟動被拒絕** – 在"應用程式啟動控制"工作執行期間，嘗試啟動 Kaspersky Embedded Systems Security 已封鎖的應用程式的次數。如果已封鎖的應用程式啟動次數超過 0，則該欄位為紅色。 **平均處理時間(毫秒)** – Kaspersky Embedded Systems Security 處理嘗試在受防護裝置上啟動應用程式所用的時間。
裝置控制	**工作狀態** – 目前工作狀態，例如，"*正在執行*"或"*已停止*"。 **執行模式** – "裝置控制"工作兩種可用模式中的一種："**活動**"或"**僅統計**"。 **已封鎖的裝置** – 在執行"裝置控制"工作期間，Kaspersky Embedded Systems Security 封鎖的連接外部裝置的嘗試次數。如果已封鎖的外部裝置數量超過 0，則該欄位值為紅色。
防火牆管理	**工作狀態** – 目前工作狀態，例如，"*正在執行*"或"*已停止*"。 **封鎖的連線嘗試次數** – 被指定防火牆規則封鎖的與受防護裝置的連線的數量。

診斷

"**診斷**"部分（請參見下表）顯示有關"檔案完整性監控"和"記錄審查"工作的資訊。

有關系統稽核狀態的資訊

"診斷"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 – 預設顯示此顏色，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"*未執行*"事件。

	• 紅色 – 其中一個工作失敗。
檔案完整性監控	**工作狀態** – 目前工作狀態，例如，“*正在執行*”或“*已停止*”。 **未批准的檔案操作** – 對監控範圍內的檔案的變更次數。這些變更可能表示受防護裝置遭到安全入侵。
記錄審查	**工作狀態** – 目前工作狀態，例如，“*正在執行*”或“*已停止*”。 **違反設定規則** – 根據來自 Windows 事件記錄的資料，所記錄的違規數量。基於指定的工作規則或使用啟發式分析來確定此數量。

Kaspersky Embedded Systems Security 產品授權資訊顯示在 **Kaspersky Embedded Systems Security** 節點的詳細資訊窗格左下角的行中。

您可以按照**應用程式內容**配置 Kaspersky Embedded Systems Security 內容。

您可以按照“**連線至其他電腦**”連結連線至其他受防護裝置。

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 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

透過 Kaspersky Embedded Systems Security Web 外掛程式可以集中管理多台已安裝 Kaspersky Embedded Systems Security 並包括在管理群組中的受防護裝置。 Kaspersky Security Center Web Console and Kaspersky Security Center Cloud Console also let you separately configure each protected device in the administration group.

*管理群組*會在卡巴斯基安全管理中心 Web Console上手動建立。「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 Web 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。在啟動政策中指定的工作設定的優先順序高於在應用程式主控台中本機設定或在卡巴斯基安全管理中心 Web 主控台的裝置內容視窗中遠端配置的工作設定。您可使用政策設定一般應用程式設定、即時電腦防護工作設定、本機行為控制工作設定和排程的本機系統工作啟動設定。

- **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卡巴斯基安全管理中心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：

- 要新增使用者和/或使用者群組，您需要使用安全性描述元定義語言 (SDDL) 指定安全性描述元字串。

- 無法為「即時檔案防護」工作變更預定義安全等級。

- 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」工作規則。

- 無法根據連線的裝置或系統資料產生「裝置控制」工作規則。

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 Web 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 外掛程式配置延展性、介面和掃描設定

要配置延伸性設定和應用程式介面：

1. 在 Web 控制的主視窗中，選取**裝置 → 政策和設定檔案**。
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**"標籤。
4. 選擇"**應用程式設定**"部分。
5. 在"**設定**"子區段中，點擊"**延伸性、介面和掃描設定**"。
6. 按下表所述配置設定。

延伸性設定

設定	敘述
自動偵測延伸性設定	Kaspersky Embedded Systems Security 自動控制使用的處理程序數量。 這是預設值。
手動設定工作處理程序數	Kaspersky Embedded Systems Security 根據指定的值控制啟動的工作處理程序數。
最大活動程序數	Kaspersky Embedded Systems Security 使用的最大處理程序數。如果選擇了"**手動設定工作處理程序數**"選項，該輸入欄位才可用。
用於即時防護的程序數	即時電腦防護工作元件使用的最大處理程序數。如果選擇了"**手動設定工作處理程序數**"選項，該輸入欄位才可用。
背景自訂掃描工作的程序數	在背景模式下執行"自訂掃描"工作時"自訂掃描"元件使用的最大處理程序數。如果選擇了"**手動設定工作處理程序數**"選項，該輸入欄位才可用。
在工作列中顯示系統匣圖示	設定是否在通知區域中顯示系統托盤圖示。

掃描後還原檔案屬性	當 Kaspersky Embedded Systems Security 執行自訂掃描工作時，將更新上次存取每個掃描檔案的時間。掃描後，Kaspersky Embedded Systems Security 將上次存取該檔案的時間重設為初始值。 此行為會導致為未更改的檔案建立備份副本，從而影響備份系統的工作。這也可能導致檔案更改追蹤應用程式中的錯誤偵測。 預設情況下會啟用此選項。
限制執行緒掃描的 CPU 使用率	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（百分比）**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。 預設情況下會停用此選項。
上限（百分比）	Kaspersky Embedded Systems Security 最大允許的 CPU 使用率。 如果選取**限制掃描執行緒的 CPU 使用率**選項，則輸入欄位可用。
掃描期間建立的臨時檔案資料夾	Kaspersky Embedded Systems Security 在掃描期間需要將壓縮檔案解壓縮到的資料夾。 預設情況下使用 C:\Windows\Temp 資料夾。
HSM 系統設定	選擇用於存取分級儲存的選項。

在 Web 外掛程式中配置安全性設定

若要手動設定安全性設定，請執行以下步驟：

1. 在 Web 控制的主視窗中，選取**裝置 → 政策和設定檔案**。
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**"標籤。
4. 選擇"**應用程式設定**"部分。
5. 點擊"**設定**"子區段中的"**安全性和可靠性**"。
6. 按下表所述配置設定。

安全性設定

設定	敘述
為應用程序防護外來威脅	如果選取了**為應用程序防護外來威脅**核取方塊，則應用程式將保護其程序免受程式碼注入或程序資料的存取。 啟用或停用該選項時，無需重新啟動應用程式服務即可套用更改。 預設情況下會啟用該選項。
重新啟動工作	該核取方塊用於允許或禁止當應用程式返回錯誤或終止時 Kaspersky Embedded Systems Security 工作的還原。

	如果選中該核取方塊，則當應用程式返回錯誤或終止時，Kaspersky Embedded Systems Security 會自動還原 Kaspersky Embedded Systems Security 工作。 如果清除該核取方塊，則當應用程式返回錯誤或終止時，Kaspersky Embedded Systems Security 不會還原 Kaspersky Embedded Systems Security 工作。 預設將會選定該核取方塊。
還原自訂掃描工作的嘗試次數不超過 (1 - 10)	Kaspersky Embedded Systems Security 傳回錯誤後嘗試還原“自訂掃描”工作的次數。如果選中“**重新啟動工作**”核取方塊，則該輸入欄位才可用。
不啟動已排程掃描工作	該核取方塊用於啟用或停用在受防護裝置轉換為 UPS 電源後、還原標準電源前啟動排程掃描工作。 如果選中該核取方塊，在受防護裝置轉換為 UPS 電源後、還原標準電源前 Kaspersky Embedded Systems Security 不會啟動排程掃描工作。 如果清除該核取方塊，不論電源如何，Kaspersky Embedded Systems Security 都會啟動排程掃描工作。 預設將會選定該核取方塊。
停止目前掃描工作	該核取方塊用於啟用或停用在受防護裝置轉換為 UPS 電源後執行掃描工作的選項。 如果選中該核取方塊，Kaspersky Embedded Systems Security 會在受防護裝置轉換為 UPS 電源後暫停執行掃描工作。 如果清除該核取方塊，Kaspersky Embedded Systems Security 會在受防護裝置轉換為 UPS 電源後繼續執行掃描工作。 預設將會選定該核取方塊。
套用密碼防護	設定密碼以防護對 Kaspersky Embedded Systems Security 功能的存取權限。

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 KSN 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 Web 控制的主視窗中，選取**裝置 → 政策和設定檔案**。
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**”標籤。
4. 選擇“**應用程式設定**”部分。
5. 在“**設定**”子區段中，點擊“**延伸性、介面和掃描設定**”。
6. 按下表所述配置設定。

連線設定

設定	敘述
不使用代理伺服器	如果選擇此選項，Kaspersky Embedded Systems Security 會直接連線到 KSN 服務，而不使用任何代理伺服器。

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連線到 KSN。
對於本機位址不使用代理伺服器	此核取方塊用於在存取與安裝了 Kaspersky Embedded Systems Security 的受防護裝置位於同一網路上的裝置時啟用/停用代理伺服器。 如果選中該核取方塊，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。不使用代理服務器。 如果取消選中該核取方塊，將使用代理伺服器連線到本機裝置。 預設將會選定該核取方塊。
代理伺服器身分驗證設定	指定身分驗證設定
不使用身分驗證	不執行身分驗證。預設選擇該方式。
使用 NTLM 身分驗證	使用由 Microsoft 開發的 NTLM 網路身分驗證協定執行身分驗證。
使用帶使用者名稱和密碼的 NTLM 身分驗證	使用由 Microsoft 開發的 NTLM 網路身分驗證協定執行含使用者名稱和密碼的身分驗證。
套用使用者名稱和密碼	使用使用者名稱和密碼執行身分驗證。

設定本機系統工作的排程啟動

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、隔離區掃描、在作業系統啟動時掃描、應用程式完整性控制、基線檔案完整性監控。
- 更新工作：資料庫更新、軟體模組更新和複製更新。

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。

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 Web 控制的主視窗中，選取**裝置 → 政策和設定檔案**。
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**"標籤。
4. 選擇"**應用程式設定**"部分。
5. 點擊"**設定**"子區段中的"**執行本機系統工作**"。
6. 按下表所述配置設定。

本機系統工作的排程啟動設定

設定	敘述
允許啟動自訂掃描工作	選取或清除該核取方塊可允許或禁止自訂掃描工作的排程啟動。
允許啟動更新工作和複製更新工作	選取或清除該核取方塊可允許或禁止更新工作和複製更新工作的排程啟動。

在 Web 外掛程式配置隔離和備份設定

要在卡巴斯基安全管理中心中配置一般隔離和備份設定：

1. 在 Web 控制的主視窗中，選取**裝置 → 政策和設定檔案**。
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**"標籤。
4. 選擇"**補充**"部分。
5. 點擊"**設定**"子區段中的"**儲存**"。
6. 按下表所述配置設定。

隔離和備份設定

設定	敘述
備份資料夾	指定備份資料夾。
最大備份空間(MB)	設定最大備份大小。
可用空間上限值(MB)	指定備份資料夾中的可用空間最小值。
還原物件的指定資料夾	指定用於儲存還原物件的資料夾。
隔離區資料夾	指定備份資料夾。

最大隔離容量 (MB)	設定最大備份大小。
可用空間上限值(MB)	指定備份資料夾中的可用空間最小值。
還原物件的指定資料夾	指定用於儲存還原物件的資料夾。
主機封鎖期限	指定此後受封鎖主機在被封鎖後還原存取網路檔案資源的天數、小時數和分鐘數。

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實行該政策中指定的 Kaspersky Embedded Systems Security 設定、功能和工作。

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。可在應用程式主控台的**"系統稽核記錄"**節點中檢視該資訊。

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*。下套用政策後，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。

活动策略中配置的且标记 图标的设置也会阻止在 Kaspersky Security Center 的**"属性：<受保护设备名称>"**窗口中针对一台受保护设备进行更改。

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。

如果政策為任何即時電腦防護工作定義設定時，此工作若正在執行中，則一旦套用政策，便將立即修改該政策所定義的設定。如果該工作未執行，就會在啟動時套用其設定。

建立政策

要建立政策：

1. 在 Web 控制的主視窗中，選取**裝置 → 政策和設定檔案**。
2. 點擊**"新增"**按鈕。
3. 將開啟**"新建政策"**視窗。

4. 在“**選擇應用程式**”部分中，選擇 Kaspersky Embedded Systems Security，然後點擊“**下一步**”。

5. 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：

     - **啟動**。下一次同步後，該政策將作為電腦上的啟動政策使用。
     - **非啟動**。備份政策。如有必要，可以將非啟動政策切換為啟動狀態。
     - **漫遊** 。當電腦離開組織網路邊緣時，將啟動該政策。

   - 配置設定的繼承：

     - **從父政策繼承設定** 。如果開啟此切換按鈕，則政策設定值從頂層政策繼承。如果為父政策設定了，則無法編輯政策設定。
     - **強制繼承子政策中的設定**。如果該切換按鈕開啟，則政策設定的值將傳播到子政策。在子政策設定中，將自動選中“**從父政策繼承設定**”核取方塊。子政策設定繼承自父政策，但標記了 的設定除外。如果為父政策設定了，則無法編輯子政策設定。

6. 在“**應用程式設定**”標籤上，根據需要配置政策設定。

7. 點擊“**儲存**”。

所建立的政策將顯示在選定管理群組的“**政策和設定檔案**”標籤上的政策清單中。在“**<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。

Kaspersky Embedded Systems Security 政策設定部分

一般

在“**一般**”部分中，您可配置以下政策設定：

- 指定政策狀態。
- 為父政策和子政策配置繼承設定。

事件配置

在“**事件配置**”部分中，您可配置以下事件類別的設定：

- *緊急事件*
- *功能故障*
- *警告*

- *資訊訊息*
  可以使用“**內容**”按鈕來配置選定事件的以下設定：
- 指定有關記錄事件的資訊的儲存位置和保留期限。
- 指定所記錄事件的通知方式。

應用程式設定

應用程式設定的設定部分

部分	選項
延伸性、介面和掃描設定	在“**延伸性、介面和掃描設定**”子區段中，可以點擊“**設定**”按鈕來配置以下設定： • 選擇手動或自動配置延伸性設定。 • 配置應用程式圖示顯示設定。
安全性和可靠性	在“**安全性和可靠性**”子區段中，可以點擊“**設定**”按鈕來配置以下設定： • 配置工作執行設定。 • 指定當受防護裝置使用 UPS 電源執行時應用程式的行為。 • 啟用或停用應用程式功能的密碼防護。
連線	在“**連線**”子區段中，可以使用“**設定**”按鈕來配置與更新伺服器、啟動伺服器和 KSN 連線的以下代理伺服器設定： • 配置代理伺服器設定。 • 指定代理伺服器身分驗證設定。
執行本機系統工作	在**執行本機系統工作**子區段中，可以使用**設定**按鈕來根據受防護裝置上配置的排程允許或封鎖啟動以下本機系統工作： • 自訂掃描工作。 • 更新工作和複製更新工作。

補充

補充的設定部分

部分	選項
信任區域	點擊“**設定**”子區段上的“**信任區域**”按鈕，以配置以下信任區域應用程式設定： • 建立信任區域排除項目清單。 • 啟用或停用檔案備份操作的掃描。 • 建立受信任處理程序清單。
卸除式磁碟機掃描	在“**卸除式磁碟機掃描**”子區段中，可以使用“**設定**”按鈕來配置卸除式磁碟機的

	掃描設定。
應用程式管理的使用者存取權限	在“**應用程式管理的使用者存取權限**”子區段中，可以配置管理 Kaspersky Embedded Systems Security 的使用者權限和使用者群組權限。
Kaspersky Security 服務管理的使用者存取權限	在“**Kaspersky Security 服務管理的使用者存取權限**”子區段中，可以配置管理 Kaspersky Security 服務的使用者權限和使用者群組權限。
儲存	在“**儲存**”子區段中，點擊“**設定**”按鈕以配置以下“隔離”、“備份”和“封鎖的主機”設定： • 指定您想要放置隔離或備份物件的資料夾的路徑。 • 設定備份和隔離的最大大小，並指定可用空間上限值。 • 指定您想要放置從隔離區或備份區還原的物件的資料夾位置。 • 設定關於隔離和備份物件到管理伺服器的資訊的傳輸。 • 配置封鎖主機的時長。

即時電腦防護

即時伺服器防護的設定部分

部分	選項
即時檔案防護	在“**即時檔案防護**”子區段中，可以點擊“**設定**”按鈕來配置以下工作設定： • 指定防護模式。 • 配置啟發式分析的使用。 • 配置信任區域的使用。 • 指定防護範圍。 • 設定選定防護範圍的安全等級：您可選擇預定義的安全等級或手動配置安全性設定。 • 配置工作啟動設定。
KSN 使用	在“**KSN 使用**”子區段中，可以點擊“**設定**”按鈕來配置以下工作設定： • 指定要對 KSN 不信任的物件執行的操作。 • 配置卡巴斯基安全管理中心作為 KSN 代理伺服器的資料傳輸和使用。
弱點利用防禦	在“**弱點利用防禦**”子區段中，可以點擊“**設定**”按鈕來配置以下工作設定： • 選擇處理程序記憶體防護模式。 • 指定降低弱點利用風險的操作。 • 新增到和編輯受防護的處理程序清單。

本機活動控制

"本機活動控制的設定"部分

部分	選項
應用程式啟動控制	在**"應用程式啟動控制"**子區段中，可以點擊**"設定"**按鈕來配置以下工作設定： • 選擇工作執行模式。 • 配置控制隨後應用程式啟動的設定。 • 指定應用程式啟動控制規則的範圍。 • 配置 KSN 的使用。 • 配置工作啟動設定。
裝置控制	在**"裝置控制"**子區段中，可以點擊**"設定"**按鈕來配置以下工作設定： • 選擇工作執行模式。 • 配置工作啟動設定。

網路活動控制

網路活動控制的設定部分

部分	選項
防火牆管理	在**"防火牆管理"**子區段中，可以點擊**"設定"**按鈕來配置以下工作設定： • 配置防火牆規則。 • 配置工作啟動設定。

系統稽核

系統稽核的設定部分

部分	選項
檔案完整性監控	在**"檔案完整性監控"**子區段中，可以配置對錶示受防護裝置上遭到安全入侵的檔案變更的控制。
記錄審查	在**"記錄審查"**部分中，可以根據 Windows 事件記錄分析結果配置受防護裝置的完整性監控。

記錄和通知

記錄和通知的設定部分

部分	選項
工作記錄	在**"工作記錄"**子區段中，可以點擊**"設定"**按鈕以配置以下設定： • 為選定的軟體元件指定記錄事件的重要性等級。

	• 指定工作記錄儲存設定。 • 指定 SIEM 與卡巴斯基安全管理中心整合的設定。
事件通知	在"**事件通知**"子區段中，可以點擊"**設定**"按鈕以配置以下設定： • 指定"*偵測到物件*"、"*偵測到並限制不受信任的大容量儲存*"和"*不信任主機清單*"事件的使用者通知設定。 • 為"**通知設定**"部分中的事件清單中選定的任何事件指定管理員通知設定。
與管理伺服器互動	在"**與管理伺服器互動**"部分中，可以點擊"**設定**"按鈕來選擇 Kaspersky Embedded Systems Security 將報告給管理伺服器的物件類型。

修訂歷史

在"**修訂歷史**"部分中，可以管理修訂：與目前版本或其他政策對比、新增修訂說明、儲存修訂到檔案或執行回溯。

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

您可為管理群組和受防護裝置集建立群組工作。您可以建立以下類型的工作：

- 啟動應用程式
- 複製更新
- 資料庫更新
- 軟體模組更新
- 資料庫更新回溯
- 自訂掃描
- 應用程式完整性控制
- 基線檔案完整性監控
- 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視窗中的**工作**頁籤上。
- 對於一組受防護裝置：在**裝置分類**節點的詳細資訊視窗中。

您可以使用政策停用同一管理群組中所有受防護伺服器上的更新和自訂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. 在網頁主控台的主視窗中，選取**裝置 → 受管理裝置**。
     b. 點擊**"群組"**標籤以選擇受防護裝置所屬的管理群組。
     c. 點擊受防護裝置的名稱。
     d. 在開啟的**"<裝置名稱>"**視窗中，選擇**"工作"**標籤。
     e. 點擊**"新增"**。
   - 建立群組工作：
     a. 在網頁主控台的主視窗中，選取**裝置 → 受管理裝置**。
     b. 點擊**"群組"**標籤以選取要為其建立工作的管理群組。
     c. 點擊**"新增"**。
   - 要為自訂的一組受防護裝置建立工作：
     a. 在網頁主控台的主視窗中，選取**裝置 → 裝置分類**。
     b. 選取要為其建立工作的選項。
     c. 點擊**"開始"**。
     d. 在**"選擇結果"**視窗中，選擇要為其建立工作的裝置。
     e. 點擊**"建立工作"**。

   將開啟工作精靈視窗。
2. 在**應用程式**下拉清單中，選取**Kaspersky Embedded Systems Security**。
3. 在**工作類型**下拉清單中，選取要建立的工作類型。

如果選擇了除"資料庫更新回溯"、"應用程式完整性控制"或"應用程式啟動"外的任何工作類型，將開啟設定視窗。

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. 在"**資料庫更新來源**"部分中選擇更新來源。

     b. 在**連線設定**視窗中，配置代理伺服器設定。

   - 在建立"軟體模組更新"工作後，在"**軟體模組更新**"視窗中配置所需應用程式模組更新設定：

     a. 選擇是複製並安裝關鍵軟體模組更新，還是僅檢查它們的可用性而不安裝。

     b. 如果選擇了"**複製並安裝軟體模組的重要更新**"：可能需要重新開機受防護裝置才能套用已安裝的軟體模組。如果希望工作完成時 Kaspersky Embedded Systems Security 自動重新啟動受防護裝置，請選定"**允許作業系統重新啟動**"核取方塊。

     c. 若要獲得有關 Kaspersky Embedded Systems Security 模組升級的資訊，請選擇"**接收有關可用的排程軟體模組更新的資訊**"。

     Kaspersky 不會在更新伺服器上發佈排程的軟體更新套件以供自動安裝；您可以手動從 Kaspersky 網站下載這些軟體更新套件。您可以設定有關"**有新的排程軟體模組更新可用**"事件的管理員通知。該通知將包含我們網站的 URL，以便您從中下載排程的更新。

   - 若要建立"複製更新"工作，請在"**複製更新**"視窗中指定更新集和目的資料夾。
   - 要建立"啟動應用程式"工作：

     a. 在"**卡巴斯基安全管理中心儲存中的金鑰清單**"視窗中，指定您要用來啟動應用程式的金鑰檔案。

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

   - 建立和配置"應用程式啟動控制規則產生器"工作。
   - 建立和配置"裝置控制規則產生器"工作。

5. 點擊"**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. 點擊"**下一步**"。
8. 如果要配置工作設定，請在**完成建立**視窗中，選取**建立完成後開啟工作詳細資訊**核取方塊。
9. 點擊"**完成**"按鈕。

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。

   將開啟**"<工作名稱>"**視窗。
3. 根據配置的工作類型，請執行下列一種操作：

   - 要設定自訂掃描工作：

     a. 在**"掃描範圍"**部分中，配置掃描範圍。

     b. 在**"選項"**部分中，配置工作優先順序水準及與其他軟體元件的整合。

   - 要配置更新工作，請根據您的需要調整工作設定：

     a. 在**"更新來源"**部分中，設定更新來源和代理伺服器設定。

     b. 在**最佳化**區段中，配置磁碟子系統最佳化。

   - 若要配置"軟體模組更新"工作，在**"進階設定"**部分中選擇要執行的操作：複製並安裝應用程式模組的重要更新或僅進行檢查。

   - 若要配置"複製更新"工作，請在**"複製更新設定"**部分中指定更新和目的資料夾。

   - 要配置"啟動應用程式"工作，請套用您要用於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啟動碼或金鑰檔案，請選中**"作為備用金鑰使用"**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。
4. 在**"排程"**部分中配置工作排程（您可以為除"資料庫更新回溯"以外的所有工作類型配置排程）。
5. 在**"帳戶"**部分中的**"設定"**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*。
6. 點擊**"儲存"**。

將儲存新配置的群組工作設定。

在 Web 外掛程式中配置啟動應用程式工作

若要設定"啟動應用程式"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。

   將開啟**"<工作名稱>"**視窗。
3. 在**"通用"**部分中，指定您要使用的金鑰檔案來啟動應用程式。如果您想要新增用於延長產品授權的金鑰，請選中**"作為備用金鑰使用"**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“**確定**”。

在 Web 外掛程式中配置更新工作

要配置“複製更新”、“資料庫更新”或“軟體模組更新”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。
   將開啟“**<工作名稱>**”視窗。
3. 在“**更新來源**”部分中，配置更新來源設定：
   - 在“**資料庫更新來源**”部分中，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。

     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。

     透過雲端主控台配置更新工作時，只有“**發佈點**”和“**Kaspersky 更新伺服器**”設定可用於指定更新來源。
   - 在“**連線設定**”部分中，配置使用代理伺服器連線到 Kaspersky 更新伺服器和其他伺服器。
4. 在資料庫更新工作的“**最佳化**”部分中，可以配置能夠減少磁碟子系統工作負載的功能：
   - **磁碟 I/O 使用最佳化**
   - **用於最佳化的 RAM（400 - 9999 MB）**
5. 在“**排程**”部分中配置工作排程（您可以為除“資料庫更新回溯”以外的所有工作類型配置排程）。
6. 在“**<工作名稱>**”視窗中，點擊“**確定**”。

在 Web 外掛程式中配置當機診斷設定

如果 Kaspersky Embedded Systems Security 執行期間發生問題（例如，Kaspersky Embedded Systems Security 當機），且您想要進行診斷，您可啟用建立 Kaspersky Embedded Systems Security 處理程序的偵錯檔案和 Dump 檔案，並將這些檔案傳送到 Kaspersky 技術支援進行分析。

Kaspersky Embedded Systems Security 不會自動傳送任何偵錯或 Dump 檔案。診斷資料只能由具有所需權限的使用者傳送。

Kaspersky Embedded Systems Security 會以未加密的形式將資訊寫入到偵錯檔案和 Dump 檔案。儲存檔案的資料夾由使用者選擇，由作業系統配置和 Kaspersky Embedded Systems Security 設定管理。您可以配置存取權限並只允許所需使用者存取記錄、偵錯檔案和 Dump 檔案。

要在卡巴斯基安全管理中心中配置當機診斷設定：

1. 在卡巴斯基安全管理中心管理主控台中，開啟"**應用程式設定**"視窗。
2. 開啟"**故障診斷**"部分，然後執行以下操作：
   - 如果您要應用程式將診斷資訊寫入檔案，請選中"**將診斷資訊寫入至檔案**"核取方塊。
     - 在下面的欄位中指定 Kaspersky Embedded Systems Security 將會儲存偵錯檔案的資料夾。
     - 設定診斷資訊的詳細等級。
     - 指定偵錯檔案的最大大小。
     - 指定一個偵錯記錄的最大檔案數。

       Kaspersky Embedded Systems Security 將為每個要診斷的元件建立多達最大數量的偵錯檔案。
     - 指定要診斷的元件。元件代碼必須用分號分隔。代碼區分大小寫（請參見下表）。

Kaspersky Embedded Systems Security 子系統代碼

元件代碼	元件名稱
*	所有元件。
gui	使用者介面子系統，Microsoft 管理主控台中的 Kaspersky Embedded Systems Security 管理單元。
ak_conn	整合網路代理和卡巴斯基安全管理中心的子系統。
bl	控制處理程序，執行 Kaspersky Embedded Systems Security 控制工作。
wp	工作處理程序，處理病毒防護工作。
blgate	Kaspersky Embedded Systems Security 遠端管理處理程序。
ods	自訂掃描子系統。
oas	即時檔案防護子系統。
qb	隔離和備份子系統。
scandll	病毒掃描輔助模組。
core	基本病毒防護功能子系統。
avscan	病毒防護處理子系統。
avserv	控制病毒防護內核子系統。
prague	基本功能子系統。
updater	更新資料庫和軟體模組的子系統。
snmp	SNMP 協定支援子系統。
perfcount	效能計數器子系統。

Kaspersky Embedded Systems Security 管理單元 (gui) 和卡巴斯基安全管理中心的管理外掛程式 (ak_conn) 的偵錯設定在這些元件重新啟動後應用。SNMP 協定支援子系統 (snmp) 的偵錯設定在 SNMP 服務重新啟動後應用。效能計數器子系統 (perfcount) 的偵錯設定在所有使用效能計數器的處理程序都重新開機之後應用。當機診斷設定儲存後，其他 Kaspersky Embedded Systems Security 子系統的偵錯設定就會立刻應用。

預設情況下，Kaspersky Embedded Systems Security 會記錄所有 Kaspersky Embedded Systems Security 元件的診斷資訊。

如果選中"**將診斷資訊寫入至檔案**"核取方塊，則該輸入欄位才可用。

- 如果您希望應用程式建立 Dump 檔案，請選中"**建立 Dump 檔案**"核取方塊。
  - 在下面的欄位中，指定 Kaspersky Embedded Systems Security 將用於儲存 Dump 檔案的資料夾。

3. 點擊"**確定**"。

已設定的應用程式設定將套用於受防護裝置上。

管理工作排程

您可以配置 Kaspersky Embedded Systems Security 工作的啟動排程，並配置依排程執行工作的設定。

排程工作

您可以在應用程式主控台中排程本機系統和自訂工作。您無法透過應用程式主控台排程群組工作。

要使用 Web 外掛程式排程群組工作，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。
   將開啟"**<工作名稱>**"視窗。
3. 選擇"**應用程式設定**"部分。
4. 在"**排程**"部分中，選中"**依排程執行**"核取方塊。

   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。

5. 根據需要配置排程設定。為此，請執行以下操作：
   a. 在"**頻率**"清單中，選擇以下值之一：
      - **每小時**，如果您希望該工作在指定的小時數內間隔執行，請在"**每 <數量> 小時**"欄位中指定小時數。
      - **每天**，如果您希望該工作在指定的天數內間隔執行，請在"**每 <數量> 天**"欄位中指定天數。
      - **每週**，如果您希望該工作在指定的週數內間隔執行，請在"**每 <數量> 週**"欄位中指定週數。指定工作啟動的星期中的日期（預設在星期一啟動工作）。

- **在應用程式啟動時**，如果您希望在每次啟動 Kaspersky Embedded Systems Security 時執行該工作。
- **應用程式資料庫更新後**，如果您希望在每次更新應用程式資料庫後執行該工作。

b. 在**"開始時間"**欄位中指定首次啟動工作的時間。

c. 在**開始日期**欄位中，指定啟動排程的開始日期。

6. 在**"工作停止設定"**部分中：

a. 選中**"持續時間"**核取方塊，並在右側的欄位中輸入工作執行的最大持續時間（小時和分鐘）。

b. 選中**"暫停工作"**核取方塊，並在右側的欄位中輸入暫停工作執行的時間隔（小於 24 小時）的開始值和結束值。

7. 在**"進階排程設定"**部分中：

a. 選中**"取消排程"**核取方塊，並指定停止套用排程的日期。

b. 選定**"執行錯過的工作"**核取方塊以允許啟動略過的工作。

c. 選中**"在此時段內隨機化工作開始時間"**核取方塊，並按分鐘指定該值。

8. 點擊**"儲存"**按鈕儲存工作啟動設定。

啟用和停用排程工作

可在配置排程設定之前或之後啟用和停用排程工作。

要啟用或停用工作啟動排程：

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。
   將開啟**"<工作名稱>"**視窗。
3. 選擇**"應用程式設定"**部分。
4. 選取**"排程"**部分。
5. 執行以下操作之一：
   - 如果您希望啟用工作的啟動排程，請選中**"依排程執行"**核取方塊。
   - 如果您希望停用工作的啟動排程，請清除**"依排程執行"**核取方塊。

   不會刪除已配置的工作啟動排程設定，並將在排程的下一次工作啟動時間套用該設定。

6. 點擊**"儲存"**。

將儲存已配置的工作啟動排程設定。

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*、*故障*、*未安裝*、*正在啟動*。

*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*。

要在應用程式設定中檢視元件狀態：

1. 在網頁主控台的主視窗中，選取**裝置 → 受管理裝置**。
2. 點擊受防護裝置的名稱。
3. 在"**一般**"標籤上，選擇"**元件**"部分。
4. 檢視狀態表。

   此狀態表中不提供有關「弱點利用防禦」元件狀態的資訊。

要檢視卡巴斯基安全管理中心 Web 主控台標準報告：

1. 選取**監控和報告 → 報告**。
2. 選取**有關應用程式元件狀態的報告**清單項，然後點擊**顯示報告**按鈕。
   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。

要檢視有關在僅統計模式下禁止的應用程式的報告：

1. 在"僅統計"模式下啟動"應用程式啟動控制"工作。
2. 選取**監控和報告 → 報告**。
3. 選取**有關在測試模式下禁止的應用程式的報告**清單項，然後點擊**顯示報告**按鈕。
   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. 在"啟動"模式下啟動"應用程式啟動控制"工作。
2. 選取**監控和報告 → 報告**。
3. 選取**有關在測試模式下禁止的應用程式的報告**清單項，然後點擊**顯示報告**按鈕。
   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。

小型診斷視窗

本節介紹如何使用小型診斷視窗檢視受防護裝置狀態或目前活動，以及如何配置 Dump 和偵錯檔案寫入。

關於小型診斷視窗

"小型診斷視窗"元件（也稱為"CDI"）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。CDI 透過系統托盤圖示啟動，或透過執行受防護裝置上的應用程式資料夾中的 kavfsmui.exe 啟動。

在 CDI 視窗中可執行以下操作：

- 檢視有關一般應用程式狀態的資訊。
- 檢視已發生的安全事件。
- 檢視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。
- 開啟含有已安裝更新和可用修補程式清單的"**關於應用程式**"視窗。

即使對 Kaspersky Embedded Systems Security 功能的存取受密碼防護，CDI 仍然可用。無需任何密碼。

CDI 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

要開啟"小型診斷視窗"視窗，請執行以下操作：

1. 用滑鼠右鍵按一下工具列通知區域中的 Kaspersky Embedded Systems Security 系統托盤圖示。
2. 選擇"**開啟小型診斷視窗**"選項。

   "**小型診斷視窗**"視窗將開啟。

在"**防護狀態**"標籤上檢視金鑰、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）。

小型診斷視窗防護狀態。

部分	狀態
即時防護狀態	在以下情況之一中（滿足任意條件），面板呈*綠色*： • 建議需求： • "即時檔案防護"工作以預設設定啟動。

	• “應用程式啟動控制”工作在“**活動**”模式下以預設設定啟動。
	• 可接受配置：
	  • “即時檔案防護”工作由使用者配置。
	  • “應用程式啟動控制”工作設定被修改。

	如果滿足以下一個或多個條件，面板呈*黃色*： • “即時檔案防護”工作暫停（使用者暫停或按排程暫停）。 • “應用程式啟動控制”工作在“**僅統計**”模式下啟動。 • “弱點利用防禦”和“應用程式啟動控制”在“**僅統計**”模式下啟動。
	如果同時滿足以下兩個條件，面板呈*紅色*： • “即時檔案防護”元件未安裝或者工作停止或暫停。 • “應用程式啟動控制”元件未安裝或工作在“**僅統計**”模式下啟動。
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。* • *已違反最終使用者產品授權協議。* • *金鑰已在黑名單中。*
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**”標籤顯示所有安全事件。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。

要檢視統計：

1. 用滑鼠右鍵按一下工具列通知區域中的 Kaspersky Embedded Systems Security 系統托盤圖示。
2. 選擇“**開啟小型診斷視窗**”選項。
   “**小型診斷視窗**”視窗將開啟。
3. 開啟“**統計**”標籤。
4. 檢視防護工作的安全事件。

檢視目前應用程式活動

在該標籤上，您可以檢視目前工作和應用程式處理程序的狀態，並迅速獲得關於所發生的緊急事件的通知。

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”工作已啟動。
  - *黃色*。KSN 聲明被接受，但工作未啟動。

要檢視受防護裝置上的目前應用程式活動：

1. 用滑鼠右鍵按一下工具列通知區域中的 Kaspersky Embedded Systems Security 系統托盤圖示。
2. 選擇“**開啟小型診斷視窗**”選項。
   “**小型診斷視窗**”視窗將開啟。
3. 開啟“**目前應用程式活動**”標籤。
4. 在“**工作**”部分中檢視以下資訊：
   - **長時間未掃描關鍵區域。**

     僅當應用程式返回相應的關鍵區域掃描警告時，才會顯示該欄位。

   - **正在執行**
   - **執行失敗**

- **由排程定義的下次啟動**

5. 在“**卡巴斯基安全網路**”部分中檢視以下資訊：

   - **KSN 已開啟，檔案信譽服務已啟用防護關閉**檔案信譽服務已啟用或防護關閉。
   - **KSN 已開啟，檔案信譽服務已啟用應用程式統計資訊正在傳送到 KSN**檔案信譽服務已啟用，應用程式統計資訊正在傳送到 KSN。

     應用程式將傳送有關在「即時檔案防護」工作和「自訂掃描」工作執行過程中偵測到的惡意軟體（包括詐欺軟體）的資訊，以及有關掃描過程中的錯誤的偵錯資訊。

     如果在“KSN 使用”工作設定中選中“**傳送卡巴斯基安全網路統計資訊**”核取方塊，將顯示該欄位。

6. 在“**與卡巴斯基安全管理中心整合**”部分中檢視以下資訊：

   - **允許本機管理**。
   - **已套用政策：<管理服务器名称>**。

配置 Dump 和偵錯檔案寫入

您可以透過 CDI 配置 Dump 和偵錯檔案的寫入。

還可以透過應用程式主控台配置故障診斷。

要開始寫入 Dump 和偵錯檔案，請執行以下操作：

1. 用滑鼠右鍵按一下工具列通知區域中的 Kaspersky Embedded Systems Security 系統托盤圖示。
2. 選擇“**開啟小型診斷視窗**”選項。
   “**小型診斷視窗**”視窗將開啟。
3. 開啟“**故障排除**”標籤。
4. 如果必要，變更以下偵錯設定：
   a. 選中“**將偵錯資訊寫入以下資料夾中的偵錯檔案**”核取方塊。
   b. 點擊**瀏覽**按鈕以指定 Kaspersky Embedded Systems Security 將會儲存偵錯檔案的資料夾。
   將對所有元件啟用跟蹤（採用預設參數，使用“*診斷*”等級的詳細資訊，預設最大記錄大小為 50 MB）。
5. 如果必要，變更以下 Dump 檔案設定：
   a. 選中“**在以下資料夾中建立故障傾印檔案**”核取方塊。
   b. 點擊**瀏覽**按鈕以指定 Kaspersky Embedded Systems Security 將會儲存 Dump 檔案的資料夾。
6. 點擊“**套用**”按鈕。
   將套用新設定。

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

本節提供有關 Kaspersky Embedded Systems Security 資料庫和軟體模組更新工作、複製更新和回溯 Kaspersky Embedded Systems Security 資料庫更新的資訊，以及有關如何設定資料庫和軟體模組更新工作的說明。

在美國使用的軟體將無法提供更新功能（包括防毒軟體簽章更新和程式碼庫更新）和 KSN 功能。

關於更新工作

Kaspersky Embedded Systems Security 支援四種系統更新工作：資料庫更新、軟體模組更新、複製更新和資料庫更新回溯。

預設情況下，Kaspersky Embedded Systems Security 每小時連線一次更新來源（Kaspersky 的更新受防護裝置之一）。您可配置所有更新工作，除"資料庫更新回溯"工作外。修改工作設定後，Kaspersky Embedded Systems Security 會在下次啟動工作時套用新值。

不允許暫停和還原更新工作。

資料庫更新

預設情況下，Kaspersky Embedded Systems Security 會將資料庫從更新來源複製到裝置，並透過執行"即時電腦防護"工作來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。

預設情況下，Kaspersky Embedded Systems Security 每小時執行一次"資料庫更新"工作。

軟體模組更新

預設情況下，Kaspersky Embedded Systems Security 檢查更新來源上是否有軟體模組更新可用。要開始使用安裝的軟體模組，可能需要重新啟動受防護裝置和/或重新啟動 Kaspersky Embedded Systems Security。

預設情況下，Kaspersky Embedded Systems Security 將在每週五下午 4:00（時間根據受防護裝置的地區時間設定）執行"軟體模組更新"工作。在執行工作期間，應用程式會檢查 Kaspersky Embedded Systems Security 模組的重要排程更新的可用性，而不分發這些更新。

複製更新

預設情況下，在執行工作期間，Kaspersky Embedded Systems Security 會下載資料庫更新檔案，並將它們儲存到指定的網路或本機資料夾，不進行應用。

預設情況下，停用"複製更新"工作。

資料庫更新回溯

執行工作期間，Kaspersky Embedded Systems Security 將資料庫還原為使用之前安裝的更新。

預設情況下，停用"資料庫更新回溯"工作。

關於軟體模組更新

Kaspersky 會發佈 Kaspersky Embedded Systems Security 模組的更新套件。更新套件可以為*緊急*（或*重要*）或排程。重要更新套件可修復弱點和錯誤；排程更新可新增新功能或增強現有功能。

緊急（重要）更新套件會上傳到 Kaspersky 更新伺服器。您可以使用"軟體模組更新"工作來設定自動安裝這些更新。預設情況下，Kaspersky Embedded Systems Security 將在每週五下午 4:00（時間根據受防護裝置的地區時間設定）執行"軟體模組更新"工作。

Kaspersky 不會在其用於自動更新的更新伺服器上發佈排程更新；已排程更新可從 Kaspersky 網站進行下載。"軟體模組更新"工作可用於接收有關排程的 Kaspersky Embedded Systems Security 更新發佈的資訊。

關鍵更新可以從網際網路獲取並套用於每台受防護裝置，或者將一台受防護裝置用作中間裝置，將所有更新複製給它，然後再將更新分發給網路受防護裝置。若要複製並儲存更新而不進行安裝，請使用"複製更新"工作。

在安裝模組更新之前，Kaspersky Embedded Systems Security 會為之前安裝的模組建立備份副本。如果軟體模組更新過程中斷或產生錯誤，Kaspersky Embedded Systems Security 將自動還原為使用之前安裝的軟體模組。您可以手動將軟體模組回溯到之前安裝的更新。

在安裝下載的更新期間，Kaspersky Security 服務會自動停止，然後重新啟動。

關於資料庫更新

儲存於受防護裝置上的 Kaspersky Embedded Systems Security 資料庫將很快過期。Kaspersky 的病毒分析師每天會偵測到幾百個新威脅，他們會為這些威脅建立識別記錄，然後將其新增到應用程式資料庫更新中。資料庫更新是一個檔案或套件，其中包含自上次更新以來發現威脅特徵碼的記錄。若要維持所需等級的裝置防護，建議您定期接收資料庫更新。

預設情況下，如果 Kaspersky Embedded Systems Security 資料庫在所安裝的資料庫更新建立後一週內未更新，將發生"*應用程式資料庫已過期*"事件。如果資料庫在兩週內沒有更新，則會發生"*應用程式資料庫已嚴重過期*"事件。資料庫目前狀態資訊顯示在應用程式主控台樹狀目錄的 **Kaspersky Embedded Systems Security** 節點的結果窗格中。您可以使用 Kaspersky Embedded Systems Security 一般設定來指定這些事件出現之前的不同天數。您還可以配置關於這些事件的管理員通知。

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。

您可以將更新下載至每個受防護裝置，或者將一個受防護裝置用作中間裝置，將所有更新複製給它，然後再將更新分發給其他受防護裝置。如果使用卡巴斯基安全管理中心來集中管理公司內的裝置防護，則可以使用卡巴斯基安全管理中心管理伺服器作為下載更新的中介。

可以手動啟動資料庫更新工作，也可以按排程啟動。預設情況下，Kaspersky Embedded Systems Security 每小時執行一次"資料庫更新"工作。

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。

組織內使用的病毒防護資料庫和模組的更新方案

更新工作中更新來源的選擇取決於用於更新組織內資料庫和程式模組的方案。

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。
  已安裝以下所列軟體的任何裝置均可用作中間裝置：
  - 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。

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“資料庫更新”工作和“軟體模組更新”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 HTTP 或 FTP 伺服器配置為更新來源。

圖 1：直接從 Internet 更新資料庫和模組

Scheme 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進行 Kaspersky Embedded Systems Security 更新：

1. 將更新複製到選定的受防護裝置。為此，請執行以下操作：
   - 在選定受防護裝置上設定“複製更新”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。為此，請執行以下操作：
   - 在每台受防護裝置上，配置“資料庫更新”工作和“軟體模組更新”工作的設定（請參見下圖）：
     a. 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。

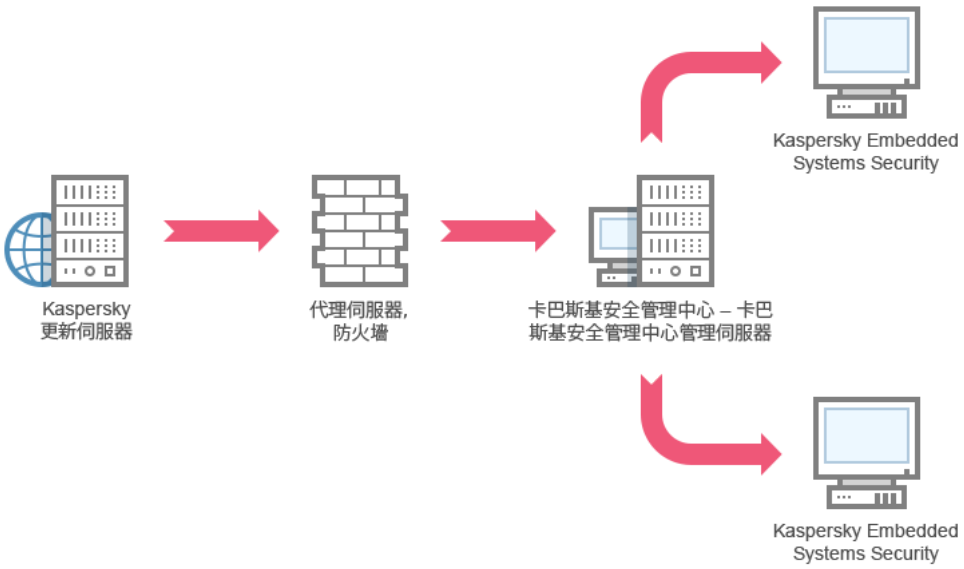

圖 2：透過一個受防護裝置更新資料庫和模組

Scheme 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

如果使用卡巴斯基安全管理中心集中管理病毒防護裝置防護，則可透過區域網路中安裝的卡巴斯基安全管理中心管理伺服器下載更新（請參見下圖）。

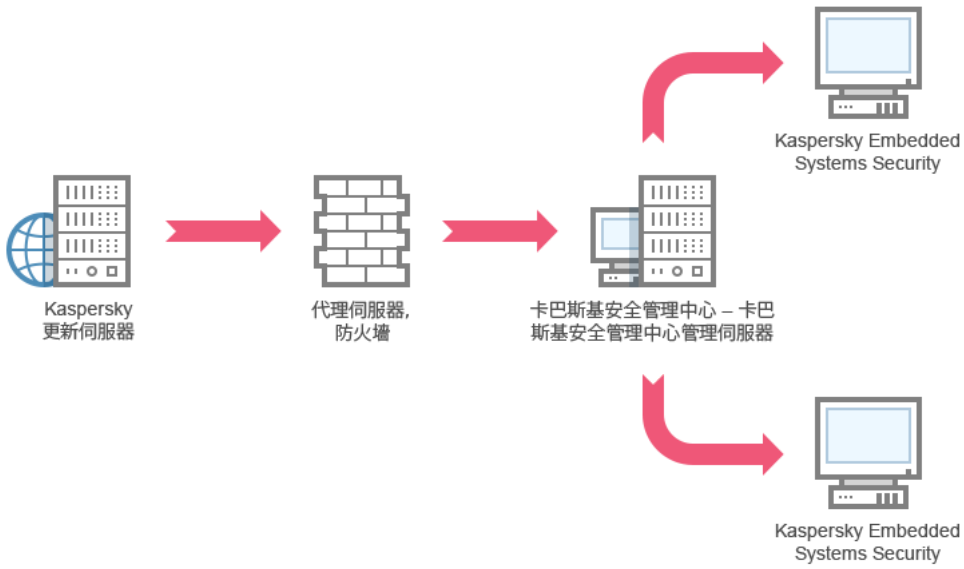

圖 3：透過卡巴斯基安全管理中心管理伺服器更新資料庫和模組

要設定透過卡巴斯基安全管理中心管理伺服器進行 Kaspersky Embedded Systems Security 更新：

1. 將更新從 Kaspersky 的更新伺服器下載到卡巴斯基安全管理中心管理伺服器。為此，請執行以下操作：
   - 為指定的一組受防護裝置配置“按管理伺服器檢索更新”工作：
     a. 指定 Kaspersky 的更新伺服器作為更新來源。
2. 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：

a. 在工作排程中，指定**"管理伺服器檢索更新之後"**作為啟動頻率。

管理伺服器將在每次接收到更新時啟動該工作（建議）。

不能在應用程式主控台中指定**"管理伺服器檢索更新之後"**啟動頻率。

- 在每個受防護裝置上，設定"資料庫更新"工作和"軟體模組更新"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。

如果 Kaspersky Embedded Systems Security 病毒資料庫很少更新（從每月一次至每年一次），則能夠偵測到危險的可能性就會降低，且假報警的頻率會隨著應用程式元件的增加而增大。

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。

如果您計劃使用卡巴斯基安全管理中心管理伺服器分發更新，請將網路代理（卡巴斯基安全管理中心發佈套件中包含的一個應用程式元件）安裝到每台受防護裝置上。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*。

設定更新工作

本節提供有關如何設定 Kaspersky Embedded Systems Security 更新工作的說明。

配置使用 Kaspersky Embedded Systems Security 更新來源的設定

對於除"資料庫更新回溯"工作外的每個更新工作，您可指定一個或多個更新來源，新增使用者定義的更新來源，以及設定與指定來源的連線設定。

在修改了更新工作設定後，將不會在正執行的更新工作中立即應用新設定。僅當重新開機工作時才會應用設定的設定。

要指定更新來源的類型：

1. 在應用程式主控台樹狀目錄中，展開**"更新"**節點。
2. 選擇與要設定的更新工作相應的子節點。
3. 在所選節點的結果窗格中，點擊**"內容"**連結。

將開啟**"工作設定"**視窗的**"一般"**標籤。

4. 在**"更新來源"**部分中，選擇 Kaspersky Embedded Systems Security 更新來源的類型：

- **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**

5. 如有需要，為使用者定義的更新來源設定進階設定：

   a. 點擊“**自訂 HTTP 或 FTP 伺服器，或網路資料夾**”連結。

      1. 在開啟的“**更新伺服器**”視窗中，選中或清除使用者定義的更新來源旁邊的核取方塊，以便開始或停止使用它們。

      2. 點擊“**確定**”。

   b. 在“**更新來源**”部分的“**一般**”標籤中，選中或清除“**如果指定的伺服器無法使用，則使用 Kaspersky 更新伺服器**”核取方塊。

6. 在“**工作設定**”視窗中，選擇“**連線設定**”標籤以設定用於連線到更新來源的設定：

   - 清除或選中“**使用代理伺服器設定以連線至 Kaspersky 更新伺服器**”核取方塊。
   - 清除或選中“**使用代理伺服器設定連線至其他伺服器**”核取方塊。

   有關配置用於存取代理伺服器的可選代理伺服器設定和身分驗證設定的資訊，請參閱“啟動和配置 Kaspersky Embedded Systems Security 資料庫更新工作”部分。

7. 點擊“**確定**”。

Kaspersky Embedded Systems Security 更新來源的已配置設定將被儲存並在下次工作啟動時套用。

您可管理使用者定義的 Kaspersky Embedded Systems Security 更新來源清單。

編輯使用者定義的應用程式更新來源清單：

1. 在應用程式主控台樹狀目錄中，展開“**更新**”節點。
2. 選擇與要設定的更新工作相應的子節點。
3. 在所選節點的結果窗格中，點擊“**內容**”連結。

   將開啟“**工作設定**”視窗的“**一般**”標籤。
4. 點擊“**自訂 HTTP 或 FTP 伺服器，或網路資料夾**”連結。

   將開啟“**更新伺服器**”視窗。
5. 執行以下操作：

   - 要新增新的使用者定義更新來源，請點擊“**新增**”，然後在輸入欄位中指定 FTP 或 HTTP 伺服器上包含更新檔案的資料夾的位址。以 UNC（通用命名約定）格式指定本機或網路資料夾。點擊 **ENTER** 鍵。

     預設情況下，已新增的資料夾用作更新來源。
   - 要停用使用者定義的更新來源，則清除清單中的更新來源旁邊的核取方塊。
   - 要啟用使用者定義的更新來源，則選中清單中的更新來源旁邊的核取方塊。

- 若要變更 Kaspersky Embedded Systems Security 存取使用者定義更新來源的順序，請使用“**上移**”和“**下移**”按鈕將選定的源向清單的開頭或末尾移動，具體取決於是在其他來源之前還是之後使用該來源。
- 若要變更使用者定義的更新來源的路徑，請在清單中選擇來源，點擊“**編輯**”按鈕，在輸入欄位中進行所需的變更，然後按 **ENTER** 鍵。
- 若要刪除使用者定義的來源，請在清單中選擇該來源，然後點擊“**刪除**”按鈕。

  您無法從清單中刪除剩餘的唯一一個使用者定義的來源。

6. 點擊“**確定**”。

將儲存使用者定義的應用程式更新來源清單的變更。

在執行資料庫更新工作時最佳化磁碟 I/O

執行“資料庫更新”工作時，Kaspersky Embedded Systems Security 會將更新檔案儲存在受防護裝置的本機磁碟上。您可以在執行更新工作時將更新檔案儲存在記憶體中的虛擬磁碟機上，從而降低受防護裝置的磁碟 I/O 子系統的工作負載。

此功能可用於 Microsoft Windows 7 作業系統及更高版本。

在執行“資料庫更新”工作時使用此功能，會在作業系統中出現一個額外的邏輯磁碟機。工作完成之後，此邏輯磁碟機將從作業系統中刪除。

要降低資料庫更新工作期間受防護裝置磁碟 I/O 子系統的工作負載：

1. 在應用程式主控台樹狀目錄中，展開“**更新**”節點。
2. 選擇“**資料庫更新**”子節點。
3. 在“**內容**”節點的結果窗格中，點擊“**資料庫更新**”連結。

   將開啟“**工作設定**”視窗的“**一般**”標籤。
4. 在“**磁碟 I/O 使用最佳化**”部分中，定義以下設定：
   - 清除或選中“**降低磁碟 I/O 上的負載**”核取方塊。
   - 在“**用於最佳化 RAM，MB**”欄位中，指定記憶體量（以 MB 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 512 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“資料庫更新”工作時，根據為該功能分配的 RAM 大小，可能會發生以下情況之一：

     - 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。
     - If the value is too large, at the start of the Database Update task, it might be impossible to create a virtual drive of a selected size in RAM. As a result, the disk subsystem optimization feature automatically

disables, and the Database Update task runs without the optimization feature.
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. 點擊**"確定"**。

已設定的設定將被儲存，並在下次工作啟動時應用。

配置複製更新工作設定

要設定複製更新工作：

1. 在應用程式主控台樹狀目錄中，展開**"更新"**節點。
2. 選擇**"複製更新"**子節點。
3. 在**"內容"**節點的結果窗格中，點擊**"複製更新"**連結。
將開啟**"工作設定"**視窗。
4. 在**"一般"**和**"連線設定"**標籤，配置使用更新來源的設定。
5. 在**"一般"**標籤上的**"複製更新設定"**部分：
   - 指定複製更新的條件：
     - **複製資料庫更新**。
     - **複製軟體模組的重要更新**。
     - **複製資料庫更新與軟體模組的重要更新**。
   - 指定 Kaspersky Embedded Systems Security 用來分發下載更新的本機或網路資料夾。
6. 在**"排程"**和**"進階"**標籤上，配置工作啟動排程。
7. 在**"執行帳戶"**標籤上，將工作設定為使用特定使用者帳戶啟動。
8. 點擊**"確定"**。

已設定的設定將被儲存，並在下次工作啟動時應用。

配置軟體模組更新工作設定

要配置"軟體模組更新"工作：

1. 在應用程式主控台樹狀目錄中，展開**"更新"**節點。
2. 選擇**"軟體模組更新"**子節點。
3. 在**"內容"**節點的結果窗格中，點擊**"軟體模組更新"**連結。
將開啟**"工作設定"**視窗。
4. 在**"一般"**和**"連線設定"**標籤，配置使用更新來源的設定。

5. 在“**一般**”標籤上的“**更新設定**”部分，配置用於更新應用程式模組的設定：

   - **僅檢查可用的重要軟體模組更新**
   - **複製並安裝軟體模組的重要更新**
   - **允許作業系統重新啟動**
   - **接收有關可用的排程軟體模組更新的資訊**

6. 在“**排程**”和“**進階**”標籤上，配置工作啟動排程。預設情況下，Kaspersky Embedded Systems Security 將在每週五下午 4:00（時間根據受防護裝置的地區時間設定）執行“軟體模組更新”工作。

7. 在“**執行帳戶**”標籤上，將工作設定為使用特定使用者帳戶啟動。

8. 點擊“**確定**”。

   已設定的設定將被儲存，並在下次工作啟動時應用。

Kaspersky 不會在更新伺服器上發佈排程的軟體更新套件以供自動安裝；您可以手動從 Kaspersky 網站下載這些軟體更新套件。您可以設定有關“*有可用的重要與排程更新*”事件的管理員通知；該通知將包含可以下載排程更新網頁的 URL。

回溯 Kaspersky Embedded Systems Security 資料庫更新

在應用資料庫更新之前，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。

如果在您已更新後出現任何問題，則可透過“資料庫更新回溯”工作將資料庫回溯到之前安裝的更新。

若要啟動“資料庫更新回溯”工作，請執行以下操作：

在“**啟動**”節點的結果視窗中，點擊“**應用程式資料庫更新回溯**”連結。

回溯應用程式模組更新

在不同 Windows 作業系統中，設定的名稱可能會有所不同。

在套用軟體模組更新之前，Kaspersky Embedded Systems Security 會為目前使用的模組建立備份副本。如果模組更新過程中斷或發生錯誤，Kaspersky Embedded Systems Security 將自動還原為使用最近所安裝更新的模組。

要回溯軟體模組，請使用 Microsoft Windows 中的“**安裝和刪除應用程式**”功能。

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訊。

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：

1. 在應用程式主控台樹狀目錄中，展開**"更新"**節點。
2. 選擇與要檢視其統計的工作相應的子節點。

   工作統計顯示在選定節點的結果窗格的**"統計"**部分中。

如果您正檢視"資料庫更新"工作或"複製更新"工作，則**"統計"**部分將顯示截至目前 Kaspersky Embedded Systems Security 已下載的資料量（**"已接收資料"**）。

下表包含軟體模組更新工作的詳細資訊。

有關"軟體模組更新"工作的資訊

欄位	敘述
已接收資料	已下載資料的總量。
可用的重要更新	可進行安裝的重要更新數。
可用的排程更新	可進行安裝的排程更新數。
套用更新時發生錯誤	如果該欄位的值不為零，則表示未應用更新。可在工作記錄中檢視導致出錯的更新的名稱。

隔離物件和複製備份

本節提供了有關在清除或刪除之前備份偵測到的惡意物件的資訊，以及有關隔離可疑感染物件的資訊。

隔離可能受感染物件。隔離

本章節介紹如何隔離可能受感染物件以及配置隔離區設定。

關於隔離可疑感染物件

Kaspersky Embedded Systems Security 透過將疑似感染物件從原始位置移動到*隔離*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。

檢視隔離物件

您可以從應用程式主控台的**"隔離"**節點檢視已隔離的物件。

要檢視隔離物件：

1. 在應用程式主控台樹狀目錄中，展開**"儲存"**節點。
2. 選擇**"隔離"**子節點。

   有關已隔離物件的資訊顯示在選定節點的結果窗格中。

要在已隔離物件清單中尋找所需物件，

排序物件或篩選物件。

排序隔離的物件

預設情況下，已隔離物件清單中的物件按照隔離日期倒序排列。要尋找所需物件，可以點擊包含物件資訊的欄位來排序物件。如果關閉**"隔離"**節點，然後重新開啟，則將儲存排序結果；如果關閉應用程式主控台，則儲存 msc 檔案，然後從該檔案重新開啟排序結果。

要排序物件：

1. 在應用程式主控台樹狀目錄中，展開**"儲存"**節點。
2. 選擇**"隔離"**子節點。
3. 在**"隔離"**節點的結果窗格中，選擇想要用於對清單中的物件進行排序的欄位標題。

   清單中的物件將基於選定設定排序。

篩選隔離的物件

要尋找所需的已隔離物件，可以篩選清單中的物件，例如，只顯示符合您指定的篩選標準（篩選器）的物件。如果關閉再重新開啟**"隔離"**節點，或者先關閉應用程式主控台，儲存 msc 檔案，再從該檔案重新開啟應用程式主控台，將儲存篩選結果。

要指定一或多個篩選：

1. 在應用程式主控台樹狀目錄中，展開**"儲存"**節點。
2. 選擇**"隔離"**子節點。
3. 在節點名稱的內容功能表中，選擇**"篩選"**。

   將開啟**"篩選設定"**視窗。
4. 若要新增篩選器，請執行以下步驟：

   a. 在**"欄位名稱"**清單中，選擇將構成篩選基礎的欄位。

   b. 在**"運算子"**清單中選擇篩選條件。清單中的篩選條件可能有所不同，具體取決於您在**"欄位名稱"**清單中選擇的值。

   c. 在**"欄位值"**欄位中輸入篩選值，或者從清單中進行選擇。

   d. 點擊**"新增"**按鈕。

   已新增的篩選將出現在**"篩選設定"**視窗的篩選清單中。 Repeat steps a-d for each filter you add. Use the following guidelines while working with filters:

   - 要使用邏輯運算子"AND"組合多個篩選，請選擇**"如果符合所有條件"**。
   - 要使用邏輯運算子"OR"組合多個篩選，請選擇**"如果符合任何條件"**。
   - 要刪除篩選，請在篩選清單中選擇要刪除的篩選，然後點擊**"刪除"**按鈕。
   - 要編輯篩選，請從**"篩選設定"**視窗的清單中選擇篩選。然後在**"欄位名稱"**、**"運算子"**或**"欄位值"**欄位中變更所設定值，並按點擊**"取代"**按鈕。
5. 新增所有篩選後，點擊**"套用"**按鈕。

   將儲存已建立的篩選器。

要還原顯示所有已隔離物件，

在**"移除篩選"**節點的內容功能表中，選擇**"隔離"**篩選。

隔離區掃描

預設情況下，每次資料庫更新之後，Kaspersky Embedded Systems Security 都會執行「隔離區掃描」本機系統工作。下表描述了工作設定。無法修改"隔離區掃描"工作的設定。

您可以設定工作啟動排程，手動啟動它以及修改用於啟動工作的帳戶權限。

透過在更新資料庫後掃描隔離物件，Kaspersky Embedded Systems Security 可能將某些物件重新歸類為未被感染：此類物件的狀態會變更為**"誤報"**。其他物件可被重新歸類為受感染，在這種情況下，Kaspersky Embedded Systems Security 會根據"隔離區掃描"工作設定（解毒，或解毒失敗則刪除）所指定來處理此類物件。

隔離區掃描工作設定

隔離區掃描工作設定	值
掃描範圍	隔離區資料夾
安全性設定	對於整個掃描範圍都一樣；它們的值在下一個清單中提供

"隔離區掃描"工作中的掃描設定

安全性設定	值
掃描物件	包含在掃描範圍內的所有物件
效能	已停用
對受感染物件和其他物件執行的操作	解毒，如果無法解毒則刪除
對可疑物件執行的操作	略過
排除檔案	否
不偵測	否
超過以下時間則停止掃描(秒)	未配置
不掃描大於以下大小的物件(MB)	未配置
掃描 NTFS 交換資料串流	已啟用
掃描開機磁區和 MBR	已停用
使用 iChecker 技術	已停用
使用 iSwift 技術	已停用
掃描複合檔案	• **壓縮檔案*** • **SFX 壓縮檔案*** • **封裝的物件*** • **嵌入的 OLE 物件*** * **"僅掃描新增與變更過的檔案"**已停用。
在檔案中檢查 Microsoft 簽章	未執行
使用啟發式分析	已啟用**深度**分析等級
信任區域	未套用

還原隔離的物件

Kaspersky Embedded Systems Security 以加密形式將可疑感染物件放入隔離區資料夾中，以防護受防護裝置免受任何可能的有害影響。

您可以從隔離區還原任意物件。在以下情況下，可能需要執行以下操作：

- 使用更新的資料庫進行隔離區掃描之後，物件的狀態變更為**"誤報"**或**"已解毒"**。
- 您認為該物件對於受防護裝置無害，並且要使用它。如果您不希望 Kaspersky Embedded Systems Security 在後續掃描期間將該物件隔離，可以將該物件從"即時檔案防護"工作和"自訂掃描"工作的處理中排除。要執行此操作，請在這些工作的**"排除檔案"**（按檔案名稱）或**"不偵測"**安全性設定中指定物件，或者將物件新增到信任區域。

在還原物件時，您可以選擇將儲存還原的物件的位置：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或者網路中的其他裝置。

您可以指定受防護裝置上用於儲存還原物件的資料夾。您可以為需要掃描的物件配置特殊的安全性設定。該資料夾的路徑由隔離區設定。

從隔離區中還原物件可能會導致受防護裝置感染病毒。

您可以還原物件，並將其副本儲存到隔離區資料夾中以備稍後使用，例如資料庫更新之後重新掃描物件。

如果已隔離物件包含在複合檔案中（例如壓縮檔案），Kaspersky Embedded Systems Security 還原期間將不會將隔離物件包括在複合檔案中，而是將隔離物件單獨儲存到選定的資料夾。

您可以還原一個或多個物件。

若要還原已隔離的物件，請執行以下步驟：

1. 在應用程式主控台樹狀目錄中，展開**"儲存"**節點。
2. 選擇**"隔離"**子節點。
3. 在**"隔離"**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"**。

   將開啟**"還原物件"**視窗。
4. 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。
5. 執行以下步驟之一：
   - 要將物件還原到原始位置，請選擇**"還原到來源資料夾"**。
   - 要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或共用資料夾，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。

6. 如果希望於還原之後在*隔離*資料夾中儲存物件的副本，請清除**"還原物件後從儲存區中刪除物件"**核取方塊。

7. 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。

   所有選定物件都將還原並儲存到指定位置。如果選擇**"還原到來源資料夾"**，則每個物件都將儲存到其原始位置；如果選擇**"還原到預設還原資料夾"**或**"還原至本機電腦上的資料夾"**，則所有物件都將儲存到您所指定的資料夾。

8. 點擊**"確定"**。

   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**重新命名**）套用於其餘選定物件。如果選擇了**"重新命名"**，**"套用至所有選擇的物件"**核取方塊將無法使用。

   c. 點擊**"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。

   如果您在**"套用至所有選擇的物件"**視窗中未選中**"還原物件"**，**"還原物件"**視窗可能再次開啟。使用該視窗可指定儲存下個選定物件的位置（請參閱流程的步驟 4）。

將物件移到隔離

您可以手動隔離檔案。

要隔離檔案：

1. 在應用程式主控台樹狀目錄中，開啟**"隔離"**節點的內容功能表。

2. 選擇**"新增"**。

3. 在**"開啟"**視窗中，選擇磁碟上您想要隔離的檔案。

4. 點擊**"確定"**。

Kaspersky Embedded Systems Security 將隔離選定檔案。

從隔離區刪除物件

根據"隔離區掃描"工作設定，如果在使用更新的資料庫進行隔離區掃描期間物件狀態變更為*受感染*，並且 Kaspersky Embedded Systems Security 無法解毒這些物件，Kaspersky Embedded Systems Security 將自動從隔離區資料夾刪除這些物件。Kaspersky Embedded Systems Security 不會從隔離中刪除其他物件。

可以從隔離區刪除一個或多個物件。

要從隔離區刪除一個或多個物件：

1. 在應用程式主控台樹狀目錄中，展開**"儲存"**節點。
2. 選擇**"隔離"**子節點。
3. 執行以下步驟之一：
   - 要刪除一個物件，請從物件名稱的內容功能表中選擇**"刪除"**。
   - 要刪除多個物件，請使用 **Ctrl** 或 **Shift** 鍵選擇想要刪除的物件，並在其中任何一個選定物件上開啟內容功能表，然後選擇**"刪除"**。
4. 在確認視窗中點擊**"是"**按鈕以確認操作。

將從隔離區刪除選定物件。

傳送可疑感染物件到 Kaspersky 以供分析

如果某個檔案的行為使您懷疑該檔案可能包含威脅，並且 Kaspersky Embedded Systems Security 認定該檔案需要解毒，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。您可以將此檔案傳送到 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。

僅能傳送已隔離的檔案以供分析。已隔離的檔案會以加密的形式儲存，且在傳送時不會被安裝在郵件伺服器上的病毒防護程式刪除。

產品授權到期後，無法將隔離的物件傳送到 Kaspersky 進行分析。

要將待分析的檔案傳送到 Kaspersky：

1. 如果檔案未被隔離，請首先**隔離**。
2. 在**"隔離"**節點中，開啟想要傳送以進行分析的檔案的內容功能表，然後選擇內容功能表中的**"傳送物件進行分析"**。
3. 如果您確定要傳送選定物件以供分析，在開啟的確認視窗中，點擊**"是"**。
4. 如果安裝應用程式主控台的受防護裝置上已設定郵件用戶端，則將新建電子郵件。檢視該訊息並點擊**"傳送"**按鈕。

   "收件者"欄位包含 Kaspersky 電子郵件信箱 newvirus@kaspersky.com。"主旨"欄位將包含"已隔離的物件"文字。

   訊息文字將包含以下文字："此檔案將傳送到 Kaspersky 以供分析"。您可以在訊息文字中包含有關該檔案任何的附加資訊：您為何認為該檔案為可能受感染或存在危險、該檔案的行為如何或該檔案對系統有何影響。

   一個名為 <物件名稱>.cab 的壓縮檔案將附加到郵件。該壓縮檔案將包含一個 <uuid>.klq 檔案，其中包含加密形式的物件；一個 <uuid>.txt 檔案，其中包含有關 Kaspersky Embedded Systems Security 擷取物件的資訊；以及一個 Sysinfo.txt 檔案，其中包含有關受防護裝置上安裝的 Kaspersky Embedded Systems Security 和作業系統的以下資訊：

   - 作業系統的名稱和版本。

- Kaspersky Embedded Systems Security 的名稱和版本。
- 已安裝最新資料庫更新的發佈日期。
- 啟動金鑰。

Kaspersky 的病毒分析人員需要上述資訊才能更快更有效地分析您的檔案。但是，如果您不想傳送此資訊，可以刪除壓縮檔案中的 Sysinfo.txt 檔案。

如果具有應用程式主控台的受防護裝置上未安裝郵件用戶端，則應用程式會提示您將選定已加密物件儲存到檔案。手動將該檔案傳送到 Kaspersky。

若要將已加密物件儲存到檔案：

1. 在開啟提示儲存物件的視窗中，點擊**"確定"**。
2. 選擇受防護裝置磁碟上的資料夾或網路資料夾，其中將儲存包含物件的檔案。

會將物件儲存到 CAB 檔案。

配置隔離區設定

您可設定隔離區設定。儲存後將立即套用新的隔離設定。

要配置隔離區設定：

1. 在應用程式主控台樹狀目錄中，展開**"儲存"**節點。
2. 開啟**"隔離"**子節點的內容功能表。
3. 選擇**"內容"**。
4. 在**隔離內容**視窗中，根據您的要求配置所需的隔離區設定：
   - 在**"隔離設定"**部分中：
     - **隔離資料夾**
     - **最大隔離區空間(MB)**
     - **可用空間上限值(MB)**

     如果隔離區中的物件大小超過最大隔離區容量或超過可用空間上限值，在您繼續將物件放入隔離區時，Kaspersky Embedded Systems Security 將通知您此情況。
   - 在**"還原設定"**部分中：
     - **還原物件的指定資料夾**
5. 點擊**"確定"**。

將儲存新配置的隔離設定。

隔離統計

您可以檢視有關已隔離物件數量的資訊，即，隔離統計。

要檢視隔離統計，

在應用程式主控台樹狀目錄的**"隔離"**節點的內容功能表中，選擇**"統計"**。

"隔離區統計"視窗將顯示目前儲存在隔離區的物件數量的相關資訊（請參閱下表）：

欄位	敘述
疑似感染的物件	Kaspersky Embedded Systems Security 發現的可能受感染的物件數。
隔離區已使用空間	隔離區資料夾中的資料總量。
誤報	因在使用更新的資料庫進行隔離區掃描期間歸類為未被感染而獲得*"誤報"*狀態的物件數。
物件已解毒	隔離區掃描之後獲得*"已解毒"*狀態的物件數。
物件總數	隔離區中的物件總數。

製作物件的備份副本。備份

本章節提供有關在解毒或刪除之前備份偵測到的惡意物件以及設定備份的說明。

關於備份物件後再解毒或刪除

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。

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或者區域網路中的其他裝置。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。

從備份中還原檔案可能會導致受防護裝置感染病毒。

檢視備份中儲存的物件

只能使用應用程式主控台中的**"備份"**節點檢視備份資料夾中的物件。您無法使用 Microsoft Windows 檔案管理員檢視這些檔案。

要檢視備份中的物件，

1. 在應用程式主控台樹狀目錄中，展開**"儲存"**節點。
2. 選擇**"備份"**子節點。

   有關置於備份中的物件的資訊顯示在選定節點的結果窗格中。

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。

排序備份中的檔案

設情況下，按備份日期倒序排序備份中的檔案。要尋找所需要的檔案，可以根據結果窗格中任意欄的內容排序檔案。

如果關閉再重新開啟**"備份"**節點，或者先關閉應用程式主控台，儲存 msc 檔案，再從該檔案重新開啟應用程式主控台，將儲存排序結果。

要排序備份中的檔案：

1. 在應用程式主控台樹狀目錄中，展開**"儲存"**節點。
2. 選擇**"備份"**子節點。
3. 在**備份**的檔案清單中，選擇想要用於排序物件的標題列。

   將基於選定標準排序備份中的檔案。

篩選備份中的檔案

要在備份中尋找所需檔案，您可以篩選檔案：在**"備份"**節點中只顯示符合您指定的篩選標準（篩選器）的檔案。

如果關閉再重新開啟**"備份"**節點，或者先關閉應用程式主控台，儲存 msc 檔案，再從該檔案重新開啟應用程式主控台，將儲存排序結果。

要篩選備份中的檔案：

1. 在應用程式主控台樹狀目錄中，開啟**"備份"**節點的內容功能表，並選擇**"篩選"**。

   將開啟**"篩選設定"**視窗。

2. 若要新增篩選器，請執行以下步驟：

a. 在**"欄位名稱"**清單中，選擇將構成篩選基礎的欄位。

b. 在**"運算子"**清單中選擇篩選條件。清單中篩選條件的值可能有所不同，具體取決於您在**"欄位名稱"**欄位中選定的值。

c. 在**"欄位值"**欄位中輸入篩選值或者選擇篩選值。

d. 點擊**"新增"**按鈕。

已新增的篩選將出現在**"篩選設定"**視窗的篩選清單中。 Repeat these steps for each filter you add. The following guidelines can be used while working with filters:

- 要使用邏輯運算子"AND"組合多個篩選，請選擇**"如果符合所有條件"**。
- 要使用邏輯運算子"OR"組合多個篩選，請選擇**"如果符合任何條件"**。
- 要刪除篩選，請在篩選清單中選擇要刪除的篩選，然後點擊**"刪除"**按鈕。
- 若要編輯篩選，請從**"篩選設定"**視窗的篩選清單中選擇篩選器，修改**"欄位名稱"**、**"運算子"**或**"欄位值"**欄位中的設定值，並點擊**"取代"**按鈕。

新增所有篩選後，點擊**"套用"**按鈕。只有與您指定篩選相比對的檔案將顯示在清單中。

要顯示備份儲存物件清單中包括的所有檔案，

在**"移除篩選"**節點的內容功能表，選擇**"備份"**。

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或可疑感染，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。為此，請在對應工作的**"排除檔案"**或**"不偵測"**設定中指定檔案。

從備份中還原檔案可能會導致受防護裝置感染病毒。

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或者網路中的其他裝置。

您可以指定受防護裝置上用於儲存還原物件的資料夾。您可以為需要掃描的物件配置特殊的安全性設定。此資料夾的路徑由"備份設定"指定。

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。

要從備份還原檔案：

1. 在應用程式主控台樹狀目錄中，展開**"儲存"**節點。
2. 選擇**"備份"**子節點。
3. 在**"備份"**節點的結果窗格中執行以下之一操作：
   - 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"**。

   將開啟**"還原物件"**視窗。
4. 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。

5. 執行以下步驟之一：
   - 要將物件還原到原始位置，請選擇**"還原到來源資料夾"**。
   - 要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或共用資料夾，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。
6. 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）。
7. 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。

   所有選定物件都將還原並儲存到指定位置。如果選擇**"還原到來源資料夾"**，則每個物件都將儲存到其原始位置；如果選擇**"還原到預設還原資料夾"**或**"還原至本機電腦上的資料夾"**，則所有物件都將儲存到您所指定的資料夾。
8. 點擊**"確定"**。

   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**重新命名**）套用於其餘選定物件。如果選擇了**"重新命名"**，**"套用至所有選擇的物件"**核取方塊將無法使用。

c. 點擊**"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。

如果您在**"套用至所有選擇的物件"**視窗中未選中**"還原物件"**，**"還原物件"**視窗可能再次開啟。使用該視窗可指定儲存下個選定物件的位置（請參閱流程的步驟 4）。

從備份刪除檔案

要從備份刪除一個或多個檔案：

1. 在應用程式主控台樹狀目錄中，展開**"儲存"**節點。
2. 選擇**"備份"**子節點。
3. 執行以下步驟之一：
   - 要刪除一個物件，請從物件名稱的內容功能表中選擇**"刪除"**。
   - 要刪除多個物件，請使用 **Ctrl** 或 **Shift** 鍵選擇想要刪除的物件，並在其中任何一個選定物件上開啟內容功能表，然後選擇**"刪除"**。
4. 在確認視窗中點擊**"是"**按鈕以確認操作。

將從備份中刪除選定檔案。

配置備份設定

要配置備份設定：

1. 在應用程式主控台樹狀目錄中，展開**"儲存"**節點。
2. 開啟**"備份"**子節點的內容功能表。
3. 選擇**"內容"**。
4. 備份在**備份內容**視窗中，根據您的要求設定所需的備份設定：

   在**"備份設定"**部分中：

   - **備份資料夾**
   - **最大備份空間(MB)**
   - **可用空間上限值(MB)**

     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。

   在**"還原設定"**部分中：

   - **還原物件的指定資料夾**

5. 點擊**"確定"**。

將儲存已設定的備份設定。

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。

若要檢視備份統計，

請在應用程式主控台樹狀目錄的**"備份"**節點上開啟內容功能表並選擇**"統計"**。將開啟**"備份區統計"**視窗。

備份區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	敘述
備份區已使用空間	備份資料夾中的資料量；程式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。封鎖的主機

本節介紹如何封鎖遠端裝置和配置封鎖的主機儲存設定。

關於封鎖的主機儲存

如果安裝以下任一元件，則預設安裝封鎖的主機儲存：即時檔案防護、網路威脅防護。這些元件根據封鎖的主機清單，發現遠端主機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主機的資訊將傳送到卡巴斯基安全管理中心。Kaspersky Embedded Systems Security 會封鎖"封鎖的主機"清單中的所有遠端主機存取受防護裝置的共用資料夾或網路附加儲存資料夾。

在啟動模式下啟動以下至少一個工作（在指定條件下）時，將填充封鎖的主機儲存：

- 對於「即時檔案防護」工作：偵測到正在存取網路檔案資源的裝置存在惡意活動，並且在「即時檔案防護」工作設定中已選取**封鎖對顯示惡意活動的主機的網路共用資源的存取**核取方塊。
- 對於"網路威脅防護"工作：偵測到典型的網路攻擊活動。

偵測到惡意活動或惡意加密嘗試後，工作會將攻擊主機的資訊傳送到封鎖的主機儲存，應用程式將為主機封鎖建立一個*警告*事件。該主機存取受防護共用網路資料夾的嘗試都將被封鎖。

如果攻擊主機的本機唯一識別碼 (LUID) 已新增到封鎖的主機清單中，Kaspersky Embedded Systems Security 會確定該主機的 IP 位址，並將其新增到封鎖的主機清單中來替換攻擊主機的 LUID。

預設情況下，當封鎖的主機被新增到清單 30 分鐘後，Kaspersky Embedded Systems Security 將從清單中移除該主機。從封鎖的主機清單刪除電腦後，電腦對網路檔案資源的存取將自動還原。您可以指定之後自動解除封鎖受封鎖主機的時段。

請注意，當限制任何使用者帳戶管理儲存的存取權限時，封鎖的主機儲存仍將可用。“封鎖的主機”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**。

透過管理外掛程式管理已封鎖的主機

在本節中，學習如何透過管理外掛程式介面配置已封鎖的主機儲存設定。

啟用封鎖不信任主機

要將出現任何惡意或惡意加密活動的主機新增到**“封鎖的主機”**儲存並封鎖這些主機存取網路檔案資源，以下至少一個工作必須在活動模式下執行：

- 即時檔案防護
- 網路威脅防護

配置“即時檔案防護”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。
2. 選擇**政策** 標籤並在**即時檔案防護**區塊中開啟 **<政策名稱> >即時電腦防護 > 設定**。

   將開啟**“即時電腦防護”**視窗。
3. 如果您希望 Kaspersky Embedded Systems Security 在“即時檔案防護”工作執行時封鎖在其中偵測到惡意活動的主機存取網路檔案資源，則在**“與其他元件整合”**部分中選中**“將顯示惡意活動的主機列為不受信任”**核取方塊。
4. 如果工作尚未啟動，請開啟**“工作管理”**標籤：
   a. 選定**“依排程執行”**核取方塊。
   b. 在下拉清單中選擇**“在應用程式啟動時”**頻率。
5. 在**“即時電腦防護”**視窗中，點擊**“確定”**。

將儲存新配置的設定。

配置“網路威脅防護”工作：

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。
5. 在打开的**“属性：<策略名称>”**窗口中，选择相应部分。

6. 點擊**"網路威脅防護"**子區段中的**"設定"**按鈕。

   將開啟**"網路威脅防護"**視窗。

7. 開啟**"一般"**標籤。

8. 在**"處理模式"**部分中，選擇**"偵測到攻擊時封鎖連線"**處理模式。

   該核取方塊用於啟用或停用將出現典型網路攻擊活動的主機新增到封鎖的主機清單中。

   如果選擇此模式，Kaspersky Embedded Systems Security 會掃描傳入的網路流量中是否存在典型網路攻擊活動，記錄有關偵測到的活動事件，並將出現典型網路攻擊活動的主機的 IP 位址新增到封鎖的主機清單中。

   預設選擇該模式。

   您可以在封鎖的主機儲存中檢視封鎖的主機清單。

   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。

9. 如果工作尚未啟動，請開啟**"工作管理"**標籤：

   a. 選定**"依排程執行"**核取方塊。

   b. 在下拉清單中選擇**"在應用程式啟動時"**頻率。

10. 在視窗中，點擊**"確定"**。

11. 將儲存新配置的設定。

配置"封鎖的主機"設定

要配置封鎖的主機儲存：

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細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"**標籤，然後開啟**"內容：<政策名稱>"**視窗。
   - 要為單台受防護裝置配置應用程式，請選擇**"裝置"**標籤，然後開啟**"應用程式設定"**視窗。

     如果某個啟動卡巴斯基安全管理中心政策已套用於裝置，並且該政策封鎖對應用程式設定的變更，則無法在**"應用程式設定"**視窗中編輯這些設定。

4. 在**"補充"**部分中，點擊**"儲存"**子區段中的**"設定"**按鈕。

   將顯示**"儲存設定"**視窗。

5. 在**封鎖的主機儲存**標籤的**主機封鎖期限**區段中，指定此後受封鎖主機在被封鎖後還原存取網路檔案資源的天數、小時數和分鐘數。

6. 點擊**"確定"**。

透過應用程式主控台管理已封鎖的主機

在本節中，學習如何透過應用程式主控台介面配置已封鎖的主機儲存設定。

啟用封鎖不信任主機

要將出現任何惡意或惡意加密活動的主機新增到**已封鎖的主機**儲存並封鎖這些主機存取網路檔案資源，以下至少一個工作必須在啟動模式下執行：

- 即時檔案防護
- 網路威脅防護

配置"即時檔案防護"工作：

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**"即時檔案防護"**子節點。
3. 在結果窗格中點擊**"內容"**連結。
   將開啟**"工作設定"**視窗。
4. 如果您希望 Kaspersky Embedded Systems Security 在"即時檔案防護"工作執行時封鎖在其中偵測到惡意活動的主機，請在**"深度"**部分中選中**"封鎖對顯示惡意活動的主機的網路共用資源的存取"**核取方塊。
5. 如果工作尚未啟動，請開啟**"排程"**標籤：
   a. 選定**"依排程執行"**核取方塊。
   b. 在下拉清單中選擇**"在應用程式啟動時"**頻率。
6. 在**"工作設定"**視窗中點擊**"確定"**。

將儲存新配置的設定。

配置"網路威脅防護"工作：

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**"網路威脅防護"**子節點。
3. 在**內容**節點的詳細資訊視窗中，點擊**網路威脅防護**連結。
4. 將開啟**"工作設定"**視窗。
5. 開啟**"一般"**標籤。
6. 在**"處理模式"**部分中，選擇**"偵測到攻擊時封鎖連線"**處理模式。

該核取方塊用於啟用或停用將出現典型網路攻擊活動的主機新增到封鎖的主機清單中。

如果選擇此模式，Kaspersky Embedded Systems Security 會掃描傳入的網路流量中是否存在典型網路攻擊活動，記錄有關偵測到的活動事件，並將出現典型網路攻擊活動的主機的 IP 位址新增到封鎖的主機清單中。

預設選擇該模式。

您可以在封鎖的主機儲存中檢視封鎖的主機清單。

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。

7. 選中或清除**"工作未執行時不停止流量分析"**核取方塊。

如果選中此核取方塊，當"網路威脅防護"工作停止後，Kaspersky Embedded Systems Security 會掃描傳入的網路流量中是否存在典型網路攻擊活動，並根據所選處理模式封鎖攻擊電腦的網路活動。

如果清除此核取方塊，當"網路威脅防護"工作停止後，Kaspersky Embedded Systems Security 不會掃描傳入的網路流量中是否存在典型網路攻擊活動，也不會封鎖攻擊電腦的網路活動。

預設取消選定該核取方塊。

8. 如果工作尚未啟動，請開啟**"排程"**標籤：
   a. 選定**"依排程執行"**核取方塊。
   b. 在下拉清單中選擇**"在應用程式啟動時"**頻率。
9. 在**"工作設定"**視窗中點擊**"確定"**。

將儲存新配置的設定。

配置"封鎖的主機"設定

要配置封鎖的主機儲存：

1. 在應用程式主控台樹狀目錄中，展開**"儲存"**節點。
2. 開啟**已封鎖的主機**子節點的內容功能表。
3. 選擇**"內容"**功能表選項。
   將顯示**"封鎖的主機儲存設定"**視窗。
4. 在**主機封鎖期限**部分中，指定此後封鎖的主機在被封鎖後還原存取網路檔案資源的天數、小時數和分鐘數。
5. 點擊**"確定"**。
6. 要還原對所有封鎖的主機的存取：
   a. 開啟**已封鎖的主機**子節點的內容功能表。
   b. 選擇**"全部解除封鎖"**選項。
      所有主機都將從清單刪除並解除封鎖。

7. 要從封鎖的主機清單中刪除多個主機：

   a. 在結果窗格中顯示的封鎖的主機清單中，選擇一個或多個主機。

   b. 開啟**已封鎖的主機**子節點的內容功能表。

   c. 選擇**"解除封鎖選定項目"**選項。
   將解除封鎖選定的主機。

透過 Web 外掛程式管理已封鎖的主機

在本節中，學習如何透過 Web 外掛程式介面配置已封鎖的主機儲存設定。

啟用主機封鎖

要將出現任何惡意或惡意加密活動的主機新增到**已封鎖的主機**儲存並封鎖這些主機存取網路檔案資源，以下至少一個工作必須在啟動模式下執行：

- 即時檔案防護
- 網路威脅防護

配置"即時檔案防護"工作：

1. 在 Web 主控台的主視窗中，選擇**"裝置"**→**"政策和設定檔案"**。
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"**標籤。
4. 選擇**"即時電腦防護"**部分。
5. 點擊**"設定"**子區段中的**"即時檔案防護"**。
6. 如果您希望 Kaspersky Embedded Systems Security 在"即時檔案防護"工作執行時封鎖在其中偵測到惡意活動的主機存取網路檔案資源，請在**"與其他元件整合"**部分中選中**"封鎖對顯示惡意活動的主機的網路共用資源的存取"**核取方塊。
7. 如果工作尚未啟動，請開啟**"工作管理"**標籤：

   a. 選定**"依排程執行"**核取方塊。

   b. 在下拉清單中選擇**"在應用程式啟動時"**頻率。

8. 點擊**"儲存"**。

將儲存新配置的設定。

配置"封鎖的主機"設定

要配置封鎖的主機儲存：

1. 在 Web 主控台的主視窗中，選擇**“裝置”**→**“政策和設定檔案”**。
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”**標籤。
4. 選擇**“補充”**部分。
5. 點擊**“設定”**子區段中的**“儲存”**。
6. 在**“補充”**部分中，點擊**“儲存”**子區段中的**“設定”**按鈕。
   將顯示**“儲存”**視窗。
7. 在**主機封鎖期限**標籤的**封鎖的主機儲存**區段中，指定此後受封鎖主機在被封鎖後還原存取網路檔案資源的天數、小時數和分鐘數。
8. 點擊**“確定”**。

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：系統稽核記錄、工作執行記錄和事件記錄。

註冊 Kaspersky Embedded Systems Security 事件的方式

Kaspersky Embedded Systems Security 的事件分為兩組：

- 與 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：

- **工作記錄**。工作記錄包含有關目前工作狀態以及執行工作期間發生事件的資訊。
- **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。
- **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。
- **安全記錄**。安全記錄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。

如果 Kaspersky Embedded Systems Security 執行期間發生問題（例如，Kaspersky Embedded Systems Security 或個別工作異常終止或者無法啟動），您可以建立偵錯檔案和 Kaspersky Embedded Systems Security 處理程序的 Dump 檔案，並將包含該資訊的檔案傳送給 Kaspersky 技術支援進行分析來診斷問題。

Kaspersky Embedded Systems Security 不會自動傳送任何偵錯或 Dump 檔案。診斷資料只能由具有所需權限的使用者傳送。

Kaspersky Embedded Systems Security 會以未加密的形式將資訊寫入到偵錯檔案和 Dump 檔案。儲存檔案的資料夾由使用者選擇，由作業系統配置和 Kaspersky Embedded Systems Security 設定管理。您可以配置存取權限並只允許所需使用者存取記錄、偵錯檔案和 Dump 檔案。

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 KESS-WEL-EVENTS.ZIP

- Kaspersky Embedded Systems Security 傳送到管理伺服器的事件。

  下載 KESS-KSC-EVENTS.ZIP

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。例如，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。當您在應用程式主控台中選擇**"系統稽核記錄"**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 會無期限地儲存系統稽核記錄中的記錄。您可以指定系統稽核記錄中記錄的儲存週期。

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。

在系統稽核記錄中排序事件

預設情況下，系統稽核記錄節點中的事件按時間倒序顯示。

事件可按除**"事件"**以外的任何欄位內容進行排序。

要在系統稽核記錄中排序事件：

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**"系統稽核記錄"**子節點。
3. 在結果窗格中，選擇要用於排序清單中事件的欄位標題。

在您下次檢視系統稽核記錄前，將儲存排序結果。

在系統稽核記錄中篩選事件

您可以將系統稽核記錄設定僅顯示符合指定篩選條件（篩選器）的事件記錄。

要在系統稽核記錄中篩選事件：

1. 在應用程式主控台樹狀目錄中，展開**"記錄和通知"**節點。
2. 開啟**"系統稽核記錄"**子節點的內容功能表，然後選擇**"篩選"**。
   將開啟**"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"**中，選擇要篩選事件的列。
   b. 在**"運算子"**清單中選擇篩選條件。篩選條件因您在**"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. 點擊**"新增"**按鈕。

   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"**如果符合所有條件**"。
- 要使用邏輯運算子"OR"組合多個篩選，請選擇"**如果符合任何條件**"。

5. 點擊"**套用**"按鈕以在系統稽核記錄中儲存篩選條件。

   系統稽核記錄的事件清單將僅顯示符合篩選條件的事件。在您下次檢視系統稽核記錄前，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. 開啟"**系統稽核記錄**"子節點的內容功能表，然後選擇"**移除篩選**"。

   系統稽核記錄的事件清單隨後將顯示所有事件。

刪除系統稽核記錄中的事件

預設情況下，Kaspersky Embedded Systems Security 會無限期地儲存系統稽核記錄中的記錄。您可以指定系統稽核記錄中記錄的儲存週期。

可以手動刪除系統稽核記錄中的所有事件。

要刪除系統稽核記錄中的事件：

1. 在應用程式主控台樹狀目錄中，展開"**記錄和通知**"節點。
2. 開啟"**系統稽核記錄**"子節點的內容功能表，然後選擇"**清除**"。
3. 執行以下步驟之一：
   - 如果要在刪除系統稽核記錄中的事件之前將記錄內容另存為 CSV 或 TXT 格式的檔案，則請點擊刪除確認視窗中的"**是**"按鈕。在開啟的視窗中，指定檔案名稱和位置。
   - 如果不想將記錄內容另存，則點擊刪除確認視窗中的"**否**"按鈕。

系統稽核記錄將被清除。

工作記錄

本章節提供有關 Kaspersky Embedded Systems Security 工作記錄的資訊以及如何管理它們的說明。

關於工作記錄

在應用程式主控台中選擇"**工作記錄**"節點後，結果窗格中會顯示有關 Kaspersky Embedded Systems Security 工作執行情況的資訊。

在每個工作的記錄中，可以檢視工作執行情況的統計、自工作啟動起應用程式已處理每個物件的詳細資訊以及工作設定。

預設情況下，當工作完成後，Kaspersky Embedded Systems Security 將記錄儲存在工作記錄中 30 天。您可以變更記錄在工作記錄中的儲存期間。

您可以指定 Kaspersky Embedded Systems Security 儲存包含工作記錄檔案所使用的資料夾，而不使用預設的資料夾。還可以選擇 Kaspersky Embedded Systems Security 將在工作記錄中記錄的事件。

在工作記錄中檢視事件清單

要查看的工作記錄：

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**"工作記錄"**子節點。

   Kaspersky Embedded Systems Security 工作記錄中儲存的事件清單將顯示在結果視窗中。

事件可以按任意欄位進行排序，也可以進行篩選。

排序工作記錄

預設情況下，工作記錄將按時間倒序顯示。可以按任意欄位進行排序。

要排序工作記錄：

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**"工作記錄"**子節點。
3. 在結果窗格中，選擇要用於排序 Kaspersky Embedded Systems Security 工作記錄的欄位標題。

   在您下次檢視工作記錄前，將儲存排序結果。

篩選工作記錄

您可以設定工作記錄清單，以僅顯示符合指定篩選條件（篩選器）的工作記錄。

要篩選工作記錄：

1. 在應用程式主控台樹狀目錄中，展開**"記錄和通知"**節點。
2. 開啟**"工作記錄"**子節點的內容功能表，然後選擇**"篩選"**。
   將開啟**"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"**中，選擇要篩選工作記錄的列。
   b. 在**"運算子"**清單中選擇篩選條件。篩選條件因您在**"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. 點擊**"新增"**按鈕。

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**"如果符合所有條件"**。
- 要使用邏輯運算子"OR"組合多個篩選，請選擇**"如果符合任何條件"**。

5. 點擊**"套用"**按鈕以在工作記錄中儲存篩選條件。

工作記錄清單將僅顯示符合篩選條件的工作記錄。在您下次檢視工作記錄前，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. 開啟**"工作記錄"**子節點的內容功能表，然後選擇**"移除篩選"**。

工作記錄清單隨後將顯示所有工作記錄。

在工作記錄中檢視有關 Kaspersky Embedded Systems Security 工作的統計和資訊

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**"工作記錄"**子節點。
3. 在結果視窗中，透過以下某種方法開啟**"記錄"**視窗：

- 點擊要檢視的工作記錄。
- 開啟要檢視的工作記錄的內容功能表，選擇**"檢視記錄"**。

4. 在開啟的視窗中，將顯示以下詳細資訊：

- **"統計"**選項顯示工作啟動和完成時間及工作統計。
- **"事件"**標籤顯示工作執行期間所記錄事件的清單。
- **"選項"**標籤顯示工作設定。

5. 如有需要，請點擊**"篩選"**按鈕以在工作記錄中篩選事件。
6. 如有需要，請點擊**"匯出"**按鈕以將工作記錄中的資料匯出至 CSV 或 TXT 格式的檔案中。
7. 點擊**"關閉"**按鈕。

"記錄"視窗將關閉。

匯出工作記錄中的資訊

您可以將工作記錄中的資料匯出至 CSV 或 TXT 格式的檔案中。

要匯出工作記錄中的資訊：

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**"工作記錄"**子節點。
3. 在結果視窗中，透過以下某種方法開啟**"記錄"**視窗：
   - 點擊要檢視的工作記錄。
   - 開啟要檢視的工作記錄的內容功能表，選擇**"檢視記錄"**。
4. 在**"記錄"**視窗下部，點擊**"匯出"**按鈕。
   將開啟**"另存為"**視窗。
5. 指定要將資料從工作記錄匯出到的檔案的名稱、位置、類型和編碼。
6. 點擊**"儲存"**按鈕。

   將儲存指定設定。

刪除工作記錄

預設情況下，當工作完成後，Kaspersky Embedded Systems Security 將記錄儲存在工作記錄中 30 天。您可以變更記錄在工作記錄中的儲存期間。

您可以手動刪除已完成的工作記錄。

對於目前正在執行的工作及其他使用者正在使用的工作，不會刪除其記錄中的事件。

要刪除工作記錄：

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**"工作記錄"**子節點。
3. 執行以下步驟之一：
   - 如果要刪除已完成的所有工作的記錄，請開啟**"工作記錄"**子節點的內容功能表，然後選擇**"清除"**。
   - 如果要清除單個工作記錄，則在結果窗格中，開啟要清除的工作記錄的內容功能表，然後選擇**"刪除"**。
   - 如果要清除多個工作的記錄：
     a. 在結果窗格中，使用 **Ctrl** 或 **Shift** 鍵選擇要清除的工作記錄。

b. 開啟任一選定工作記錄的內容功能表，然後選擇**"刪除"**。

4. 在刪除確認視窗中點擊**"是"**按鈕以確認您要刪除這些記錄。

選擇的工作記錄將被清除。工作記錄的刪除將記錄在系統稽核記錄中。

安全記錄

Kaspersky Embedded Systems Security 保持有與受防護裝置上的安全入侵或嘗試進行安全入侵相關的事件的記錄。本記錄中記錄以下事件：

- 弱點利用防禦事件。
- 關鍵記錄審查事件。
- 表示嘗試進行安全入侵的嚴重事件（對於"即時電腦防護"、"自訂掃描"、"檔案完整性監控"、"應用程式啟動控制"和"裝置控制"工作）。

您可以清除安全記錄以及系統稽核記錄。此外，當清除安全記錄時，Kaspersky Embedded Systems Security 會記錄一個系統稽核事件。

在事件檢視器中檢視 Kaspersky Embedded Systems Security 事件記錄

您可以使用 Microsoft 管理主控台的 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。

在管理外掛程式中配置記錄設定

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。
- *應用程式資料庫已過期*、*應用程式資料庫已嚴重過期*和 *長時間未執行關鍵區域掃描*的事件產生上限值。
- 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。
- 用於將稽核事件和工作執行事件透過 Syslog 協定發佈到 syslog 伺服器的設定。

要設定 Kaspersky Embedded Systems Security 記錄，請執行下列步驟：

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，並選擇**"內容"**。
   將開啟**"記錄和通知設定"**視窗。
2. 在**"記錄和通知設定"**視窗中，根據需要設定記錄。為此，請執行以下操作：
   - 在**"一般"**標籤上，如有必要，選擇 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。為此，請執行以下操作：
     - 在**"元件"**清單中，選擇您要設定其詳細等級的 Kaspersky Embedded Systems Security 元件。

       對於"即時檔案防護"、"自訂掃描"和"更新"元件，事件記錄在工作記錄和事件記錄中。對於這些元件，事件表格包含**"工作記錄"**和**"Windows 事件記錄"**欄位。"隔離"和"備份"元件的事件記錄在系統稽核記錄和事件記錄中。對於這些元件，事件表格包含**"稽核"**和**"Windows 事件記錄"**欄位。

     - 在**"重要性等級"**清單中，選擇事件在工作記錄、系統稽核記錄和選定元件的事件記錄中的詳細等級。
       在包含事件清單的下表中，使用工作記錄、系統稽核記錄和事件記錄，根據目前詳細等級記錄的事件選取旁邊的核取方塊。
     - 如果您想手動為選定的元件啟用記錄特定事件，請執行以下操作：
     a. 在**"重要性等級"**清單中選擇**"自訂"**。
     b. 在包含事件清單的表格中，選定您想要記錄到工作記錄、系統稽核記錄和事件記錄中事件旁邊的核取方塊。
   - 在**"進階"**標籤上，配置裝置防護狀態的記錄儲存設定和事件產生上限值：
     - 在**"記錄儲存"**部分中：
       - **記錄資料夾**
       - **刪除早於該天數的工作記錄**

- **刪除早於該天數的系統稽核記錄事件(天)**

- 在"**事件產生上限值**"部分：

- 指定*應用程式資料庫已過期*、*應用程式資料庫已嚴重過期*和*長時間未執行關鍵區域掃描*的事件將發生的天數。

- 在"**SIEM 整合**"標籤上，配置用於將審核事件和工作執行事件發佈到 syslog 伺服器的設定。

3. 點擊"**確定**"以儲存變更。

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。

可靠性設定

透過定義連線到映像 syslog 伺服器的設定，可以降低事件傳輸到 SIEM 伺服器不成功的風險。

映像 syslog 伺服器是一個額外的 syslog 伺服器，如果與主 syslog 伺服器的連線無法使用或不能使用主要伺服器，應用程式會自動轉換到該伺服器。

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。

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（參見下表）。

SIEM 整合設定

設定	預設值	敘述
透過 syslog 協定傳送事件到遠端 syslog 伺服器	未套用	可以分別透過選擇或清除該核取方塊來啟用或停用 SIEM 整合。
刪除已被傳送到遠端 syslog 伺服器的事件本機副本	未套用	可以透過選中或清除核取方塊來配置將記錄傳送到 SIEM 伺服器後儲存記錄本機副本的設定。
事件格式	結構化資料	可以選擇兩種格式之一，應用程式在將事件傳送到 syslog 伺服器以便 SIEM 伺服器能夠更好進行識別之前，將事件轉換為該格式。
連線協定	TCP	可以使用下拉清單來配置透過 UDP 或 TCP 協定與主 syslog 伺服器和映像 syslog 伺服器的連線。
主 syslog 伺服器連線設定	IP 位址：127.0.0.1 連接埠：514	可以使用適當的欄位來配置用於連線到主 syslog 伺服器的 IP 位址和連接埠。 可以指定 IP 位址僅為 IPv4 格式。
如果無法存取主伺服器則使用映像 syslog 伺服器	未套用	可以使用核取方塊來啟用或停用映像 syslog 伺服器。
映像 syslog 伺服器連線設定	IP 位址：127.0.0.1 連接埠：514	可以使用適當的欄位來配置用於連線到映像 syslog 伺服器的 IP 位址和連接埠。 可以指定 IP 位址僅為 IPv4 格式。

要配置 SIEM 整合設定：

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"**。
   將開啟**"記錄和通知設定"**視窗。
3. 選擇**"SIEM 整合"**標籤。
4. 在**"整合設定"**部分中，選擇**"透過 syslog 協定傳送事件到遠端 syslog 伺服器"**核取方塊。
5. 如果需要，在**"整合設定"**部分中，選擇**"刪除已被傳送到遠端 syslog 伺服器的事件本機副本"**核取方塊。

   "刪除已被傳送到遠端 syslog 伺服器的事件本機副本"核取方塊的狀態不會影響儲存安全記錄檔案事件的設定：應用程式永遠不會自動刪除安全記錄事件。

6. 在**"事件格式"**部分中，指定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，應用程式將它們轉換為結構化資料格式。
7. 在**"連線設定"**部分中：
   - 指定 SIEM 連線協定。
   - 指定用於連線到主 syslog 伺服器的設定。
     只能指定 IPv4 格式的 IP 位址。

- 當無法傳送事件到主 syslog 伺服器時，如果想讓應用程式使用其他連線設定，請選中**"如果無法存取主伺服器則使用映像 syslog 伺服器"**核取方塊。

  指定用於連線到映像 syslog 伺服器的設定：**"位址"**和**"埠號"**。

  如果已清除**"如果無法存取主伺服器則使用映像 syslog 伺服器"**核取方塊，則無法編輯映像 syslog 伺服器的**"位址"**和**"埠號"**欄位。

  只能指定 IPv4 格式的 IP 位址。

8. 點擊**"確定"**。

   將套用已配置的 SIEM 整合設定。

配置記錄和通知

可以使用卡巴斯基安全管理中心管理主控台為管理員和使用者設定通知，以使其瞭解下列與 Kaspersky Embedded Systems Security 和裝置上的防毒防護狀態有關的事件：

- 管理員可以收到有關選定類型事件的資訊；
- 存取受防護裝置的區網使用者和終端伺服器使用者可以收到關於*偵測到物件*事件的資訊。

可使用選定受保護設備的**"屬性:<受保護設備名稱>"**窗口為單個受保護設備，或使用選定管理組的**"屬性：<策略名稱>"**窗口為一組受保護設備配置有關 Kaspersky Embedded Systems Security 事件的通知。

在**"事件通知"**標籤上或在**"通知設定"**視窗中，可以配置以下類型的通知：

- 可以使用**"事件通知"**選項（卡巴斯基安全管理中心中的標準標籤）配置有關選定類型事件的管理員通知。有關通知方法的詳細資訊，請參閱*卡巴斯基安全管理中心說明*。
- 在**"通知設定"**視窗中，可以配置管理員通知和使用者通知。

某些事件類型的通知只能在視窗或標籤中配置；其他事件類型的通知可以同時在視窗和標籤中配置。

如果同時在兩個標籤（**"事件通知"**標籤上和**"通知設定"**視窗中）上使用相同模式配置關於同一類型事件的通知，系統管理員將以相同的模式收到兩次這些事件的通知。

配置記錄設定

要設定 Kaspersky Embedded Systems Security 記錄，請執行下列步驟：

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細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"**標籤，然後開啟**"內容：<政策名稱>"**視窗。
   - 要為單台受防護裝置配置應用程式，請選擇**"裝置"**標籤，然後開啟**"應用程式設定"**視窗。

如果某個啟動卡巴斯基安全管理中心政策已套用於裝置，並且該政策封鎖對應用程式設定的變更，則無法在**"應用程式設定"**視窗中編輯這些設定。

4. 在**"記錄和通知"**部分中，點擊**"工作記錄"**子區段中的**"設定"**按鈕。
5. 在**記錄設定**視窗中，根據您的需要定義以下 Kaspersky Embedded Systems Security 設定：
   - 配置記錄中的事件詳細等級。為此，請執行以下操作：
     a. 在**"元件"**清單中，選擇您要設定其詳細等級的 Kaspersky Embedded Systems Security 元件。
     b. 若要定義選定元件的工作記錄和系統稽核記錄中的詳細等級，請從**"重要性等級"**中選擇所需等級。
   - 要變更記錄的預設位置，請指定資料夾的絕對路徑，或點擊**"瀏覽"**按鈕進行選擇。
   - 指定工作記錄的儲存天數。
   - 指定**"系統稽核記錄"**節點中顯示的資訊儲存天數。
6. 點擊**"確定"**。

已儲存配置的記錄設定。

安全記錄

Kaspersky Embedded Systems Security 保持有與受防護裝置上的安全入侵或嘗試進行安全入侵相關的事件的記錄。本記錄中記錄以下事件：

- 弱點利用防禦事件。
- 關鍵記錄審查事件。
- 表示嘗試進行安全入侵的嚴重事件（對於"即時電腦防護"、"自訂掃描"、"檔案完整性監控"、"應用程式啟動控制"和"裝置控制"工作）。

您可以清除安全記錄以及系統稽核記錄。此外，當清除安全記錄時，Kaspersky Embedded Systems Security 會記錄一個系統稽核事件。

配置 SIEM 整合設定

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。

為降低事件傳輸到 SIEM 伺服器不成功的風險，您可以定義連線到映像 syslog 伺服器的設定。

映像 syslog 伺服器是一個額外的 syslog 伺服器，如果與主 syslog 伺服器的連線無法使用或不能使用主要伺服器，應用程式會自動轉換到該伺服器。

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（參見下表）。

SIEM 整合設定

設定	預設值	敘述
透過 syslog 協定傳送事件到遠端 syslog 伺服器	未套用	可以分別透過選擇或清除該核取方塊來啟用或停用 SIEM 整合。
刪除已被傳送到遠端 syslog 伺服器的事件本機副本	未套用	可以透過選中或清除核取方塊來配置將記錄傳送到 SIEM 伺服器後儲存記錄本機副本的設定。
事件格式	結構化資料	可以選擇兩種格式之一，應用程式在將事件傳送到 syslog 伺服器以便 SIEM 伺服器能夠更好進行識別之前，將事件轉換為該格式。
連線協定	TCP	可以使用下拉清單來配置透過 UDP 或 TCP 協定與主 syslog 伺服器的連線，以及透過 TCP 協定與映像 syslog 伺服器的連線。
主 syslog 伺服器連線設定	IP 位址：127.0.0.1 連接埠：514	可以使用適當的欄位來配置用於連線到主 syslog 伺服器的 IP 位址和連接埠。 可以指定 IP 位址僅為 IPv4 格式。
如果無法存取主伺服器則使用映像 syslog 伺服器	未套用	可以使用核取方塊來啟用或停用映像 syslog 伺服器。
映像 syslog 伺服器連線設定	IP 位址：127.0.0.1 連接埠：514	可以使用適當的欄位來配置用於連線到映像 syslog 伺服器的 IP 位址和連接埠。 可以指定 IP 位址僅為 IPv4 格式。

要配置 SIEM 整合設定：

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細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"**標籤，然後開啟**"內容：<政策名稱>"**視窗。

- 要為單台受防護裝置配置應用程式，請選擇“**裝置**”標籤，然後開啟“**應用程式設定**”視窗。

  如果某個啟動卡巴斯基安全管理中心政策已套用於裝置，並且該政策封鎖對應用程式設定的變更，則無法在“**應用程式設定**”視窗中編輯這些設定。

4. 在“**記錄和通知**”部分中，點擊“**工作記錄**”子區段中的“**設定**”按鈕。

   將開啟“**記錄和通知設定**”視窗。

5. 選擇“**SIEM 整合**”標籤。

6. 在“**整合設定**”部分中，選擇“**透過 syslog 協定傳送事件到遠端 syslog 伺服器**”核取方塊。

7. 如果需要，在“**整合設定**”部分中，選擇“**刪除已被傳送到遠端 syslog 伺服器的事件本機副本**”核取方塊。

   “**刪除已被傳送到遠端 syslog 伺服器的事件本機副本**”核取方塊的狀態不會影響儲存安全記錄檔案事件的設定：應用程式永遠不會自動刪除安全記錄事件。

8. 在“**事件格式**”部分中，指定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，應用程式將它們轉換為結構化資料格式。

9. 在“**連線設定**”部分中：

   - 指定 SIEM 連線協定。
   - 指定用於連線到主 syslog 伺服器的設定。

     只能指定 IPv4 格式的 IP 位址。
   - 當無法傳送事件到主 syslog 伺服器時，如果想讓應用程式使用其他連線設定，請選中“**如果無法存取主伺服器則使用映像 syslog 伺服器**”核取方塊。

     指定用於連線到映像 syslog 伺服器的設定：“**位址**”和“**埠號**”。

     如果已清除“**如果無法存取主伺服器則使用映像 syslog 伺服器**”核取方塊，則無法編輯映像 syslog 伺服器的“**位址**”和“**埠號**”欄位。

     只能指定 IPv4 格式的 IP 位址。

10. 點擊“**確定**”。

    將套用已配置的 SIEM 整合設定。

配置通知設定

要設定 Kaspersky Embedded Systems Security 通知，請執行下列步驟：

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細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**”標籤，然後開啟“**內容：<政策名稱>**”視窗。
- 要為單台受防護裝置配置應用程式，請選擇“**裝置**”標籤，然後開啟“**應用程式設定**”視窗。

如果某個啟動卡巴斯基安全管理中心政策已套用於裝置，並且該政策封鎖對應用程式設定的變更，則無法在“**應用程式設定**”視窗中編輯這些設定。

4. 在**記錄和通知**區段中，點擊**事件通知**子區段中的**設定**按鈕。
5. 在**通知設定**視窗中，根據您的需要定義以下 Kaspersky Embedded Systems Security 設定：
   - 在**通知設定**清單中，選取想要配置其設定的通知類型。
   - 在**通知使用者**區段中，配置使用者通知方式。如有必要，輸入通知訊息的文字。
   - 在**通知管理員**區段中，配置管理員通知方式。如有必要，輸入通知訊息的文字。如有必要，透過點擊**設定**按鈕配置附加通知設定。
   - 在**事件產生上限值**區段中，指定 Kaspersky Embedded Systems Security 記錄*應用程式資料庫已過期*、*應用程式資料庫已嚴重過期*和*長時間未執行關鍵區域掃描*事件的時間間隔。
     - **應用程式資料庫已過期（天）**
     - **資料庫已長時間未更新（天）**
     - **已很長時間未執行關鍵區域掃描（天）**
6. 點擊“**確定**”。

將儲存設定的通知設定。

配置與管理伺服器的互動

要選擇 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：

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細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**”標籤，然後開啟“**內容：<政策名稱>**”視窗。
   - 要為單台受防護裝置配置應用程式，請選擇“**裝置**”標籤，然後開啟“**應用程式設定**”視窗。

如果某個啟動卡巴斯基安全管理中心政策已套用於裝置，並且該政策封鎖對應用程式設定的變更，則無法在“**應用程式設定**”視窗中編輯這些設定。

4. 在“**記錄和通知**”部分中，點擊“**與管理伺服器互動**”子區段中的“**設定**”按鈕。

將開啟“**管理伺服器網路清單**”視窗。

5. 在**"管理伺服器網路清單"**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：

   - 隔離的物件。
   - 已備份物件。

6. 點擊**"確定"**。

   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。

通知設定

本章節提供有關如何設定向 Kaspersky Embedded Systems Security 的使用者和管理員通知應用程式事件和裝置防護狀態資訊的方法。

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。

程式將確認執行以下工作：

- 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。

在應用程式主控台中，使用多種方式啟動管理員或使用者通知：

- 使用者通知方式：
  a. 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。
  b. 訊息服務工具。
     您可以透過 Microsoft Windows 訊息服務使用此方式來進行通知。
- 管理員通知方式：
  a. 訊息服務工具。
     您可以透過 Microsoft Windows 訊息服務使用此方式來進行通知。
  b. 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。
  c. 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。

要配置事件通知設定：

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，並選擇"**內容**"。
   將開啟"**記錄和通知設定**"視窗。

2. 在**"通知"**標籤中，選擇通知模式：

   a. 從**"事件類型"**清單中選擇您希望為其選擇通知方式的事件。

   b. 在**"通知管理員"**或**"通知使用者"**設定中，選定您希望配置的通知方式旁邊的核取方塊。

   只能為以下事件配置使用者通知**"偵測到物件"**事件、**"偵測到不受信任的外部裝置並已限制此裝置"**事件和**"不信任主機清單"**事件。

3. 新增訊息文字：

   a. 點擊**"訊息文字"**按鈕。

   b. 在開啟的視窗中輸入要在相應的事件訊息中顯示的文字。

   您可以為多個事件類型建立相同訊息：為一個事件類型選擇通知方式後，使用 **Ctrl** 或 **Shift** 鍵選擇要使用相同訊息的其他事件類型，然後點擊**"訊息文字"**按鈕。

   a. 若要新增有關事件資訊的欄位，請點擊**"巨集"**按鈕，然後從下拉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。

   b. 若要還原預設事件訊息文字，請點擊**"使用預設值"**按鈕。

4. 要配置選定事件的管理員通知方式，請點擊**"通知"**標籤，點擊**"設定"**部分中的**"通知管理員"**按鈕，並在**"進階設定"**視窗中配置選定的方式。為此，請執行以下操作：

   a. 對於電子郵件通知，請開啟**"電子郵件"**標籤，然後在相應的欄位中指定收件者的電子郵件信箱（位址使用分號隔開）、SMTP 伺服器的名稱或網路位址以及埠號。若有需要，請指定在**"主旨"**和**"寄件者"**欄位中顯示的文字。在**"主旨"**欄位中也可以包括有關事件資訊的變數（請參閱下表）。

   如果您希望在連線 SMTP 伺服器時應用帳戶身分驗證，請在**"需要 SMTP 驗證"**群組中選擇**"身分驗證設定"**，然後指定要身分驗證帳戶的使用者名稱和密碼。

   b. 對於使用 Windows Messenger 服務的通知，請在**"Windows Messenger 服務"**標籤上建立的通知收件者受防護裝置的清單：對於您希望新增的每台受防護裝置，請點擊**"新增"**按鈕並在輸入欄位中輸入其網路名稱。

   c. 要執行可執行檔，請在受防護裝置的本機磁碟機上選擇當發生事件時在受防護裝置上執行的檔案，或在**"可執行檔"**標籤上輸入其完整路徑。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。

   如果您希望限制一種事件類型在一段時間內的訊息數量，請在**"進階"**選項上選擇**"不要傳送相同的通知超過"**，然後指定次數和時間間隔。

5. 點擊**"確定"**。

將儲存設定的通知設定。

事件資訊欄位

變數	敘述
%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%	根据病毒百科全书分类确定的对象名称。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”。它包含在 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，存取了裝置上物件的使用者的電腦名稱。
%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）。

啟動和停止 Kaspersky Embedded Systems Security

本節包含有關啟動應用程式主控台的資訊，以及有關啟動和停止 Kaspersky Security 服務的資訊。

啟動 Kaspersky Embedded Systems Security 管理外掛程式

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該外掛程式後，它會與卡巴斯基安全管理中心一起啟動。有關啟動卡巴斯基安全管理中心的詳細資訊，請參見《*卡巴斯基安全管理中心說明*》。

從開始功能表啟動 Kaspersky Embedded Systems Security 主控台

在不同 Windows 作業系統中，設定的名稱可能會有所不同。

*要從"**開始**"功能表啟動應用程式主控台：*

1. 在**開始**功能表中，選取**程式** > **Kaspersky Embedded Systems Security** > **管理工具** > **Kaspersky Embedded Systems Security** 主控台。

要向應用程式主控台中新增其他管理單元，請以作者模式啟動應用程式主控台。

要以作者模式啟動應用程式主控台：

1. 在**開始**選單中，選取**程式** > **Kaspersky Embedded Systems Security** > **管理工具**。
2. 在應用程式主控台的內容功能表中，選擇"**作者**"指令。

   將以作者模式啟動應用程式主控台。

如果已在受防護裝置上啟動應用程式主控台，應用程式主控台視窗將開啟。

如果在非受防護裝置上啟動了應用程式主控台，請連線到受防護裝置。

要連線到受防護裝置：

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"**連線至其他電腦**"指令。
   將開啟"**選取受防護的裝置**"視窗。
3. 在開啟的視窗中選擇"**其他裝置**"。
4. 在右側的輸入欄位中指定受防護裝置的網路名稱。
5. 點擊"**確定**"。

   應用程式主控台將連線到受防護裝置。

如果用來登入 Microsoft Windows 的使用者帳戶沒有足夠權限來存取受防護裝置上的 Kaspersky Security 管理服務，則選擇“**使用以下帳戶身分連線**”核取方塊，然後指定具有所需權限的使用者帳戶。

啟動和停止 Kaspersky Security 服務

預設情況下，Kaspersky Security 服務會在作業系統啟動後立即自動啟動。Kaspersky Security 服務管理的工作處理程序執行“即時電腦防護”、“電腦控制”、“自訂掃描”和更新工作。

預設情況下，當 Kaspersky Embedded Systems Security 啟動時，將啟動“即時檔案防護”和“在作業系統啟動時掃描”工作以及其他排程在“**在應用程式啟動時**”啟動的工作。

如果停止 Kaspersky Security 服務，則會停止所有正在執行的工作。重新啟動 Kaspersky Security 服務之後，應用程式只會自動啟動已排程為“**在應用程式啟動時**”執行的工作，而其他工作必須手動啟動。

您可以使用 **Kaspersky Embedded Systems Security** 節點的內容功能表或使用 Microsoft Windows 服務管理單元啟動和停止 Kaspersky Security 服務。

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。

要使用應用程式主控台停止或啟動應用程式：

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. 選擇以下之一項目：
   - **停止服務**。
   - **啟動服務**。

將啟用或停止 Kaspersky Security 服務。

在作業系統安全模式下啟動 Kaspersky Embedded Systems Security

本節提供有關在作業系統安全模式下工作的 Kaspersky Embedded Systems Security 的資訊。

關於在作業系統安全模式下工作的 Kaspersky Embedded Systems Security

Kaspersky Embedded Systems Security 元件可以在作業系統以安全模式載入時啟動。除了 Kaspersky Security 服務 (kavfs.exe)，還將載入 klam.sys 驅動程式。它用於在作業系統啟動期間將 Kaspersky Security 服務註冊為受防護服務。有關詳細資訊，請參見“將 Kaspersky Security 服務註冊為受防護服務”部分。

Kaspersky Embedded Systems Security 可以在作業系統的以下安全模式下啟動：

- 最小安全模式 - 選擇作業系統安全模式的標準選項時，將啟動此模式。此時，Kaspersky Embedded Systems Security 可以啟動以下元件：
  - 即時檔案防護。
  - 自訂掃描。

- 應用程式啟動控制和應用程式啟動控制規則產生器。
- 記錄審查。
- 檔案完整性監控。
- 基線檔案完整性監控。
- 應用程式完整性控制。

網路安全模式 – 在此模式下，作業系統以帶有網路驅動程式的安全模式載入。除了在最小安全模式下啟動的元件，Kaspersky Embedded Systems Security 在此模式下還可以啟動以下元件：

- 資料庫更新。
- 軟體模組更新。

在安全模式下啟動 Kaspersky Embedded Systems Security

預設情況下，在作業系統以安全模式載入時，不啟動 Kaspersky Embedded Systems Security。

要使 Kaspersky Embedded Systems Security 在作業系統安全模式下啟動：

1. 啟動 Windows 登錄檔編輯程式 (C:Windowsregedit.exe)。
2. 開啟系統登錄檔的 [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\klam\Parameters] 項。
3. 開啟 LoadInSafeMode 參數。
4. 將值設定為 **1**。
5. 點擊**"確定"**。

要取消 Kaspersky Embedded Systems Security 在作業系統安全模式下啟動：

1. 啟動 Windows 登錄檔編輯程式 (C:Windowsregedit.exe)。
2. 開啟系統登錄檔的 [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\klam\Parameters] 項。
3. 開啟 LoadInSafeMode 參數。
4. 將值設定為 1。
5. 點擊**"確定"**。

Kaspersky Embedded Systems Security 自我防護

有關 Kaspersky Embedded Systems Security 自我防護機制的資訊。

關於 Kaspersky Embedded Systems Security 自我防護

Kaspersky Embedded Systems Security 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。

防止包含已安裝的 Kaspersky Embedded Systems Security 元件的資料夾被變更

Kaspersky Embedded Systems Security 會封鎖任何使用者帳戶對包含已安裝的應用程式元件的資料夾進行重新命名和刪除。預設情況下，應用程式安裝資料夾的路徑如下：

- 在32 位元版本的 Microsoft Windows 中 – %ProgramFiles%\Kaspersky Lab\Kaspersky Embedded Systems Security\
- 在64 位元版本的 Microsoft Windows 中：%ProgramFiles(x86)%\Kaspersky Lab\Kaspersky Embedded Systems Security\

防止 Kaspersky Embedded Systems Security 登入機碼被變更

Kaspersky Embedded Systems Security 會限制對以下登入分支和登入機碼的存取，這些登入機碼提供了應用程式驅動程式和服務的載入：

- [HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\KasperskyLab\ESS]
- [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\kavfs]
- [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\kavfsgt]
- [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\kavfsslp]
- [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\klam]
- [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\klelaml]
- [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\klfltdev]
- [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\klramdisk]
- [HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\ESS\3.0\CrashDump]
- [HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\KasperskyLab\ESS\3.1]（在 64 位版本的 Microsoft Windows 上）
- [HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\ESS\3.0\Trace]

變更這些登入分支和登入機碼的權限僅授予給本機系統 (SYSTEM) 帳戶。使用者和管理員帳戶被授予唯讀權限。

防止程式服務部分的記憶體發生變化

為了防護程式服務部分，避免受第三方處理程序的影響，Kaspersky Embedded Systems Security 驅動程式限制對以下可執行檔的存取：

- kavfs.exe
- kavfswp.exe
- kavfswh.exe
- kavfsgt.exe

預設情況下，限制第三方處理程序存取 Kaspersky Embedded Systems Security 服務部分的記憶體。

您可以在 Kaspersky Embedded Systems Security 主控台和 Kaspersky Embedded Systems Security 管理外掛程式政策屬性中啟用自我防護功能。

將 Kaspersky Security 服務註冊為受防護服務

輕度受防護處理程序（也稱為“PPL”）技術確保作業系統只載入受信任的服務和處理程序。對於要作為受防護服務執行的服務，必須在受防護裝置上安裝*早期啟動惡意軟體防護*驅動程式。

早期啟動惡意軟體防護（也稱為“ELAM”）驅動程式在網路中的裝置啟動時及協力廠商驅動程式初始化之前為這些裝置提供防護。

ELAM 驅動程式在 Kaspersky Embedded Systems Security 安裝期間自動安裝，用於在作業系統啟動時將 Kaspersky Security 服務註冊為 PPL。Kaspersky Security 服務 (KAVFS) 作為系統防護處理程序啟動後，系統中的其他非受防護處理程序將不能注入執行緒、寫入受防護處理程序的虛擬記憶體或停止服務。

當某個處理程序以 PPL 的形式啟動時，使用者無法對其進行管理，不管分配的使用者權限如何。Microsoft Windows 10 及更高版本作業系統支援使用 ELAM 驅動程式將 Kaspersky Security 服務註冊為 PPL。如果在執行支援 PPL 的作業系統的伺服器上安裝 Kaspersky Embedded Systems Security，Kaspersky Security 服務 (KAVFS) 的權限管理將不可用。

要將 Kaspersky Embedded Systems Security 安裝為 PPL，請執行以下指令：

```
msiexec /i ess_x64.msi NOPPL=0 EULA=1 PRIVACYPOLICY=1 /qn
```

管理 Kaspersky Embedded Systems Security 功能的存取權限

本節包含有關 Kaspersky Embedded Systems Security 和該應用程式註冊的作業系統服務的管理權限的資訊，以及如何設定這些權限的說明。

關於 Kaspersky Embedded Systems Security 的管理權限

預設情況下，為受防護裝置上的管理員組的使用者、在安裝 Kaspersky Embedded Systems Security 的過程中在受防護裝置上建立的 ESS 管理員群組的使用者以及 SYSTEM 群組授予對所有 Kaspersky Embedded Systems Security 功能的存取權限。

對 Kaspersky Embedded Systems Security 有"編輯"權限存取等級的使用者可以向受防護裝置上註冊的其他使用者或者該網域中包含的使用者授予對 Kaspersky Embedded Systems Security 功能的存取權限。

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。

您可以為使用者或群組選擇以下預設存取權限等級之一：

- **完整控制** – 所有應用程式功能的存取權限：可檢視和編輯 Kaspersky Embedded Systems Security 一般設定、元件設定和 Kaspersky Embedded Systems Security 使用者權限，還可以檢視 Kaspersky Embedded Systems Security 統計。
- **修改** – 除編輯使用者權限以外的所有應用程式功能的存取權限：可以檢視和編輯 Kaspersky Embedded Systems Security 一般設定和 Kaspersky Embedded Systems Security 元件設定。
- **讀取** – 可以檢視 Kaspersky Embedded Systems Security 一般設定、Kaspersky Embedded Systems Security 元件設定、Kaspersky Embedded Systems Security 統計和 Kaspersky Embedded Systems Security 使用者權限。

您還可以配置進階存取權限：允許或封鎖存取 Kaspersky Embedded Systems Security 的特定功能。

如果您已為某個使用者或群組手動設定存取權限，則為該使用者或群組設定"**特殊權限**"存取層級。

關於 Kaspersky Embedded Systems Security 功能的存取權限

使用者權限	敘述
工作管理	可啟動/停止/暫停/還原 Kaspersky Embedded Systems Security 工作。
建立和刪除自訂掃描工作	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。
管理儲存區	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。
讀取統計	可檢視每個 Kaspersky Embedded Systems Security 工作的統計。
應用程式產品授權	能啟動 Kaspersky Embedded Systems Security。
移除應用程式	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。

關於管理註冊服務的權限

安裝過程中，Kaspersky Embedded Systems Security 會在 Windows 中註冊 Kaspersky Security 服務 (KAVFS) 和 Kaspersky Security 管理服務 (KAVFSGT) 以及 Kaspersky Security 弱點利用防禦 (KAVFSSLP)。

Microsoft Windows 10 及更高版本的作業系統上，可以使用 ELAM 驅動程式將 Kaspersky Security 服務註冊為輕度受防護處理程序。當某個處理程序以 PPL 的形式啟動時，使用者無法對其進行管理，不管分配的使用者權限如何。如果在執行支援 PPL 的作業系統的受防護裝置上安裝 Kaspersky Embedded Systems Security，權限管理將無法使用於 Kaspersky Security 服務 (KAVFS)。

Kaspersky Security 服務

預設情況下，將管理 Kaspersky Security 服務的存取權限授予受防護裝置上"管理員"群組中的使用者，以及具有讀取權限的 SERVICE 和 INTERACTIVE 群組，和具有讀取和執行權限的 SYSTEM 群組。

有權限存取"編輯權限"等級的使用者可以向在受防護伺服器上註冊的其他使用者或者該網域中包含的其他使用者授予對管理 Kaspersky Security 服務的存取權限。

Kaspersky Security 管理服務

要透過安裝在其他受防護裝置上的應用程式主控台來管理應用程式，使用其權限與 Kaspersky Embedded Systems Security 建立連線的帳戶必須對受防護裝置上的 Kaspersky Security 管理服務具有完全存取權限。

預設情況下，系統向以下兩組使用者授予存取所有 Kaspersky Security 管理服務的權限：受防護裝置上的管理員群組的使用者，以及安裝 Kaspersky Embedded Systems Security 時在受防護裝置上建立的 ESS 管理員群組的使用者。

只能透過 Microsoft Windows 服務管理單元管理 Kaspersky Security 管理服務。

Kaspersky Security 弱點利用防禦

預設情況下，將管理 Kaspersky Security 弱點利用防禦服務的存取權限授予受防護伺服器上"管理員"群組中的使用者，以及具有讀取和執行權限的 SYSTEM 群組。

關於 Kaspersky Security 管理服務的存取權限

您可以檢視 Kaspersky Embedded Systems Security 服務的清單。

在安裝過程中，Kaspersky Embedded Systems Security 會註冊 Kaspersky Security 管理服務 (KAVFSGT)。要透過安裝在其他受防護裝置上的應用程式主控台來管理應用程式，用來連線到 Kaspersky Embedded Systems Security 的帳戶必須對受防護裝置上的 Kaspersky Security 管理服務具有完全存取權限。

預設情況下，系統向以下兩組使用者授予存取所有 Kaspersky Security 管理服務的權限：受防護裝置上的管理員群組的使用者，以及安裝 Kaspersky Embedded Systems Security 時在受防護裝置上建立的 ESS 管理員群組的使用者。

只能透過 Microsoft Windows 服務管理單元管理 Kaspersky Security 管理服務。

您不能透過配置 Kaspersky Embedded Systems Security 來允許或封鎖使用者存取 Kaspersky Security 管理服務。

您可以從本機帳戶連線到 Kaspersky Embedded Systems Security，只要在受防護裝置上註冊具有相同使用者名稱和密碼的帳戶即可。

關於 Kaspersky Security 服務的管理權限

在安裝 Kaspersky Embedded Systems Security 的過程中在 Windows 中註冊 Kaspersky Security 服務 (KAVFS)，並在內部啟用在啟動作業系統時啟動的功能元件。為了降低協力廠商透過 Kaspersky Security 服務的管理存取應用程式功能和受防護裝置上安全性設定的風險，可以從應用程式主控台或管理外掛程式限制管理 Kaspersky Security 服務的權限。

預設情況下，用於管理 Kaspersky Security 服務的存取權限被授予受防護裝置上管理員群組中的使用者。讀取權限被授予 SERVICE 和 INTERACTIVE 群組，讀取和執行權限被授予 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，則當儲存變更時會還原此帳戶的最大權限。

有權限存取需要"編輯"權限的功能的使用者可以向在受防護伺服器上註冊的其他使用者或者該網域中包含的其他使用者授予對管理 Kaspersky Security 服務的存取權限。

您可以為 Kaspersky Embedded Systems Security 使用者或使用者組選擇以下預設的權限等級之一以管理 Kaspersky Security 服務：

- **完整控制**：可檢視和編輯 Kaspersky Security 服務的一般設定和使用者權限，以及啟動和停止 Kaspersky Security 服務。
- **讀取**：可檢視 Kaspersky Security 服務一般設定和使用者權限。
- **修改**：可檢視和編輯 Kaspersky Security 服務一般設定和使用者權限。

- **執行**：可啟動和停止 Kaspersky 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）。

如果您已為某個使用者或群組手動設定存取權限，則為該使用者或群組設定**"特殊權限"**存取層級。

Kaspersky Security 服務功能的存取權限

功能	敘述
檢視服務設定	可檢視 Kaspersky Security 服務一般設定和使用者權限。
從服務管理員請求服務狀態	可從 Microsoft Windows 服務控制管理員請求 Kaspersky Security 服務的執行狀態。
從服務請求狀態	可從 Kaspersky Security 服務請求服務執行狀態。
讀取依存服務清單	可檢視 Kaspersky Security 服務依存的以及依存於 Kaspersky Security 服務的服務清單。
編輯服務設定	可檢視和編輯 Kaspersky Security 服務一般設定和使用者權限。
啟動服務	可啟動 Kaspersky Security 服務。
停止服務	可停止 Kaspersky Security 服務。
暫停/還原服務	可暫停和還原 Kaspersky Security 服務。
讀取權限	可檢視 Kaspersky Security 服務使用者清單和每個使用者的存取權限。
編輯權限	可執行以下操作： • 新增和刪除 Kaspersky Security 服務使用者。 • 編輯 Kaspersky Security 服務的使用者存取權限。
刪除服務	可在 Microsoft Windows 服務控制管理員中取消註冊 Kaspersky Security 服務。
使用者定義的服務請求	可建立和傳送對 Kaspersky Security 服務的使用者請求。

透過管理外掛程式管理存取權限

在本節中，學習如何導航管理外掛程式介面，以及如何為網路中的一台或所有受防護裝置配置存取權限。

配置 Kaspersky Embedded Systems Security 和 Kaspersky Security 服務的存取權限

您可以編輯有權存取 Kaspersky Embedded Systems Security 功能和管理 Kaspersky Security 服務的使用者和使用者群組清單。還可以編輯這些使用者和使用者群組的存取權限。

要從清單中新增或刪除使用者或群組：

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細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**”標籤，然後開啟“**內容：<政策名稱>**”視窗。
   - 要為單台受防護裝置配置應用程式，請選擇“**裝置**”標籤，然後開啟“**應用程式設定**”視窗。

     如果某個啟動卡巴斯基安全管理中心政策已套用於裝置，並且該政策封鎖對應用程式設定的變更，則無法在“**應用程式設定**”視窗中編輯這些設定。

4. 在“**補充**”部分，執行以下步驟之一：

   - 如果您希望編輯具有用於管理 Kaspersky Embedded Systems Security 功能的存取權限的使用者清單，請點擊“**應用程式管理的使用者存取權限**”子區段中的“**設定**”。
   - 如果您希望編輯具有用於管理 Kaspersky Security 服務的存取權限的使用者清單，請點擊“**Security 服務管理的使用者存取權限**”子區段中的“**設定**”。

     Kaspersky Embedded Systems Security 權限群組視窗隨即開啟。

5. 在開啟的視窗中，執行以下操作：

   - 要向清單中新增使用者或群組，請點擊“**新增**”按鈕，然後選擇要授予權限的使用者或群組。
   - 要從清單中刪除使用者或群組，請選擇要限制其存取權限的使用者或群組，然後點擊“**刪除**”按鈕。

6. 點擊“**套用**”按鈕。

將新增或刪除所選使用者（群組）。

編輯使用者或群組對管理 Kaspersky Embedded Systems Security 或 Kaspersky Security 服務的權限：

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細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**”標籤，然後開啟“**內容：<政策名稱>**”視窗。
   - 要為單台受防護裝置配置應用程式，請選擇“**裝置**”標籤，然後開啟“**應用程式設定**”視窗。

     如果某個啟動卡巴斯基安全管理中心政策已套用於裝置，並且該政策封鎖對應用程式設定的變更，則無法在“**應用程式設定**”視窗中編輯這些設定。

4. 在“**補充**”部分，執行以下步驟之一：

   - 如果您希望編輯具有用於管理 Kaspersky Embedded Systems Security 功能的存取權限的使用者清單，請點擊“**應用程式管理的使用者存取權限**”子區段中的“**設定**”。
   - 如果您希望編輯具有用於透過 Kaspersky Security 服務管理應用程式的存取權限的使用者清單，請點擊“**Security 服務管理的使用者存取權限**”子區段中的“**設定**”。

Kaspersky Embedded Systems Security 權限群組視窗隨即開啟。

5. 在開啟的視窗的**"群組或使用者"**清單中，選擇要變更其權限的使用者或群組。

6. 在**"<使用者（群組）> 的權限"**部分中，選中與以下存取權限等級對應的**"允許"**或**"拒絕"**核取方塊：

   - **完整控制**：可管理 Kaspersky Embedded Systems Security 或 Kaspersky Security 服務的全套權限。
   - **讀取**：
     - 用於管理 Kaspersky Embedded Systems Security 的以下權限：**檢索統計**、**讀取設定**、**讀取記錄**和**讀取權限**。
     - 用於管理 Kaspersky Security 服務的以下權限：**讀取服務設定**、**從服務控制管理員請求狀態**、**從服務請求狀態**、**讀取依存服務清單**、**讀取權限**。
   - **修改**：
     - 除**編輯權限**之外的所有 Kaspersky Embedded Systems Security 管理權限。
     - 用於管理 Kaspersky Security 服務的以下權限：**修改服務設定**、**讀取權限**。
   - **特殊權限**：用於管理 Kaspersky Security 服務的以下權限：**正在啟動服務**、**停止服務**、**暫停/還原服務**、**讀取權限**、**使用者定義的服務請求**。

7. 要配置某個使用者或群組的進階權限（**特殊權限**），請點擊**"進階"**按鈕。

   a. 在開啟的 **Kaspersky Embedded Systems Security 進階安全性設定**視窗中，選取所需的使用者或群組。

   b. 點擊**"編輯"**按鈕。

   c. 在視窗頂部的下拉清單中，選擇存取控制類型（**"允許"**或**"封鎖"**）。

   d. 選中與要為所選使用者或群組允許或封鎖的功能旁邊的核取方塊。

   e. 點擊**"確定"**。

   f. 在 **Kaspersky Embedded Systems Security的進階安全設定**視窗中，點擊**確定**。

8. 在 **Kaspersky Embedded Systems Security** 權限視窗中，點擊**套用**按鈕。

已配置的用於管理 Kaspersky Embedded Systems Security 或 Kaspersky Security 服務的權限將被儲存。

對 Kaspersky Embedded Systems Security 功能進行受密碼防護的存取

您可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。

當您嘗試存取以下應用程式功能時，Kaspersky Embedded Systems Security 會請求密碼：

- 連線到應用程式主控台；
- 移除 Kaspersky Embedded Systems Security；

- 修改 Kaspersky Embedded Systems Security 元件；
- 執行命令列指令。

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 (%)。

您可匯出和匯入受密碼防護的應用程式設定。透過匯出受防護應用程式配置而建立的設定檔包含密碼核對總和以及用於填充密碼字串的修飾符值。

請勿變更設定檔中的核對總和或修飾符。匯入已手動變更的密碼防護配置可能會導致存取應用程式完全被封鎖。

要防護對 Kaspersky Embedded Systems Security 功能的存取權限：

1. 在卡巴斯基安全管理中心管理主控台樹狀目錄中，展開**"受管理裝置"**節點。選擇包含要配置其應用程式設定的受防護裝置的管理群組。
2. 在選定的管理群組的詳細視窗中執行以下之一操作：
   - 要設定一組受防護裝置的政策設定，請選擇**"政策"**標籤，然後透過內容功能表開啟**"<政策名稱>"**的內容。
   - 如果要為單台受防護裝置配置應用程式設定，請在卡巴斯基安全管理中心中的**"應用程式設定"**視窗中開啟所需設定。
3. 在**"應用程式設定"**標籤的**"安全性"**部分中，點擊**"設定"**按鈕。

   將開啟**"安全性設定"**視窗。
4. 在**"密碼防護設定"**部分中，選中**"套用密碼防護"**核取方塊。

   "密碼"和**"確認密碼"**欄位變為啟動狀態。
5. 在**"密碼"**欄位中，輸入想要用於防護對 Kaspersky Embedded Systems Security 功能進行存取的密碼。
6. 在**"確認密碼"**欄位中，再次輸入您的密碼。

7. 點擊**"確定"**。

將儲存指定設定。Kaspersky Embedded Systems Security 將請求指定密碼以存取受防護的功能。

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，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**"套用密碼防護"**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。

透過應用程式主控台管理存取權限

在本節中，學習如何導航應用程式主控台介面以及如何配置受防護裝置的存取權限。

配置用於管理 Kaspersky Embedded Systems Security 和 Kaspersky Security 服務的存取權限

您可以編輯有權存取 Kaspersky Embedded Systems Security 功能和管理 Kaspersky Security 服務的使用者和使用者群組清單。還可以編輯這些使用者和使用者群組的存取權限。

要從清單中新增或刪除使用者或群組：

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細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"**標籤，然後開啟**"內容：<政策名稱>"**視窗。
   - 要為單台受防護裝置配置應用程式，請選擇**"裝置"**標籤，然後開啟**"應用程式設定"**視窗。

     如果某個啟動卡巴斯基安全管理中心政策已套用於裝置，並且該政策封鎖對應用程式設定的變更，則無法在**"應用程式設定"**視窗中編輯這些設定。
4. 在**"補充"**部分，執行以下步驟之一：
   - 如果您希望編輯具有用於管理 Kaspersky Embedded Systems Security 功能的存取權限的使用者清單，請點擊**"應用程式管理的使用者存取權限"**子區段中的**"設定"**。
   - 如果您希望編輯具有用於管理 Kaspersky Security 服務的存取權限的使用者清單，請點擊**"Security 服務管理的使用者存取權限"**子區段中的**"設定"**。

     Kaspersky Embedded Systems Security 權限群組視窗隨即開啟。
5. 在開啟的視窗中，執行以下操作：
   - 要向清單中新增使用者或群組，請點擊**"新增"**按鈕，然後選擇要授予權限的使用者或群組。

- 要從清單中刪除使用者或群組，請選擇要限制其存取權限的使用者或群組，然後點擊**"刪除"**按鈕。

6. 點擊**"套用"**按鈕。

將新增或刪除所選使用者（群組）。

編輯使用者或群組對 Kaspersky Embedded Systems Security 或 Kaspersky Security 服務的管理權限：

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細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"**標籤，然後開啟**"內容：<政策名稱>"**視窗。
   - 要為單台受防護裝置配置應用程式，請選擇**"裝置"**標籤，然後開啟**"應用程式設定"**視窗。

   如果某個啟動卡巴斯基安全管理中心政策已套用於裝置，並且該政策封鎖對應用程式設定的變更，則無法在**"應用程式設定"**視窗中編輯這些設定。
4. 在**"補充"**部分，執行以下步驟之一：
   - 如果您希望編輯具有用於管理 Kaspersky Embedded Systems Security 功能的存取權限的使用者清單，請點擊**"應用程式管理的使用者存取權限"**子區段中的**"設定"**。
   - 如果您希望編輯具有用於透過 Kaspersky Security 服務管理應用程式的存取權限的使用者清單，請點擊**"Security 服務管理的使用者存取權限"**子區段中的**"設定"**。

     Kaspersky Embedded Systems Security 權限群組視窗隨即開啟。
5. 在開啟的視窗的**"群組或使用者"**清單中，選擇要變更其權限的使用者或群組。
6. 在**"<使用者（群組）> 的權限"**部分中，選中與以下存取權限等級對應的**"允許"**或**"拒絕"**核取方塊：
   - **完整控制**：可管理 Kaspersky Embedded Systems Security 或 Kaspersky Security 服務的全套權限。
   - **讀取**：
     - 用於管理 Kaspersky Embedded Systems Security 的以下權限：**檢索統計**、**讀取設定**、**讀取記錄**和**讀取權限**。
     - 用於管理 Kaspersky Security 服務的以下權限：**讀取服務設定**、**從服務控制管理員請求狀態**、**從服務請求狀態**、**讀取依存服務清單**、**讀取權限**。
   - **修改**：
     - 除**編輯權限**之外的所有 Kaspersky Embedded Systems Security 管理權限。
     - 用於管理 Kaspersky Security 服務的以下權限：**修改服務設定**、**讀取權限**。
   - **特殊權限**：用於管理 Kaspersky Security 服務的以下權限：**正在啟動服務**、**停止服務**、**暫停/還原服務**、**讀取權限**、**使用者定義的服務請求**。
7. 要配置某個使用者或群組的進階權限（**特殊權限**），請點擊**"進階"**按鈕。

a. 在開啟的 **Kaspersky Embedded Systems Security 進階安全性設定**視窗中，選取所需的使用者或群組。

b. 點擊**"編輯"**按鈕。

c. 在視窗頂部的下拉清單中，選擇存取控制類型（**"允許"**或**"封鎖"**）。

d. 選中與要為所選使用者或群組允許或封鎖的功能旁邊的核取方塊。

e. 點擊**"確定"**。

f. 在 **Kaspersky Embedded Systems Security的進階安全設定**視窗中，點擊**確定**。

8. 在 **Kaspersky Embedded Systems Security** 權限視窗中，點擊**套用**按鈕。

9. 已配置的用於管理 Kaspersky Embedded Systems Security 或 Kaspersky Security 服務的權限將被儲存。

對 Kaspersky Embedded Systems Security 功能進行受密碼防護的存取

您可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。

當您嘗試存取以下應用程式功能時，Kaspersky Embedded Systems Security 會請求密碼：

- 連線到應用程式主控台；
- 移除 Kaspersky Embedded Systems Security；
- 修改 Kaspersky Embedded Systems Security 元件；
- 執行命令列指令。

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。

您可匯出和匯入受密碼防護的應用程式設定。透過匯出受防護應用程式配置而建立的設定檔包含密碼核對總和以及用於填充密碼字串的修飾符值。

請勿變更設定檔中的核對總和或修飾符。匯入已手動變更的密碼防護配置可能會導致存取應用程式完全被封鎖。

要防護對 Kaspersky Embedded Systems Security 功能的存取權限：

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**"內容"**。

   將開啟**"應用程式設定"**視窗。

2. 在**"安全性和可靠性"**標籤上的**"密碼防護設定"**部分中，選中**"套用密碼防護"**核取方塊。
   "密碼"和**"確認密碼"**欄位變為啟動狀態。

3. 在**"密碼"**欄位中，輸入想要用於防護對 Kaspersky Embedded Systems Security 功能進行存取的密碼。

4. 在**"確認密碼"**欄位中，再次輸入密碼。

5. 點擊**"確定"**。

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，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**"套用密碼防護"**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。

透過 Web 外掛程式管理存取權限

在本節中，學習如何導航 Web 外掛程式介面，以及如何為網路中的一台或所有受防護裝置配置存取權限。

配置 Kaspersky Embedded Systems Security 和 Kaspersky Security 服務的存取權限

要配置用戶或群組的存取權限，您需要使用安全性描述元定義語言 (SDDL) 指定安全性描述元字串。有關安全性描述元字串的詳細資訊，請至 Microsoft 網站。

要配置使用者或群組的存取權限：

1. 在 Web 控制的主視窗中，選取**裝置 → 政策和設定檔案**。

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"**標籤。

4. 選擇**"補充"**部分。

5. 執行以下步驟之一：

   - 如果您希望編輯具有用於管理 Kaspersky Embedded Systems Security 功能的存取權限的使用者清單，請點擊**"設定"**子區段中的**"應用程式管理的使用者存取權限"**。

   - 如果您希望編輯具有用於管理 Kaspersky Security 服務的存取權限的使用者清單，請點擊**"設定"**子區段中的**"Kaspersky Security 服務管理的使用者存取權限"**。

6. 透過在**"應用程式管理的使用者存取權限"**或**"Kaspersky Security 服務管理的使用者存取權限"**視窗中指定安全性描述元字串來新增使用者或群組。

7. 點擊**"確定"**。

對 Kaspersky Embedded Systems Security 功能進行受密碼防護的存取

您可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。

當您嘗試存取以下應用程式功能時，Kaspersky Embedded Systems Security 會請求密碼：

- 連線到應用程式主控台；
- 移除 Kaspersky Embedded Systems Security；
- 修改 Kaspersky Embedded Systems Security 元件；
- 執行命令列指令。

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。

您可匯出和匯入受密碼防護的應用程式設定。透過匯出受防護應用程式配置而建立的設定檔包含密碼核對總和以及用於填充密碼字串的修飾符值。

請勿變更設定檔中的核對總和或修飾符。匯入已手動變更的密碼防護配置可能會導致存取應用程式完全被封鎖。

要防護對 Kaspersky Embedded Systems Security 功能的存取權限：

1. 在 Web 控制的主視窗中，選取**裝置 → 政策和設定檔案**。
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"**標籤。
4. 選擇**"應用程式設定"**部分。
5. 在**"安全性"**部分，點擊**"設定"**按鈕。
6. 在**"密碼防護設定"**部分中，選中**"套用密碼防護"**核取方塊。
7. 在**"密碼"**欄位中，輸入想要用於防護對 Kaspersky Embedded Systems Security 功能進行存取的密碼。
8. 點擊**"確定"**。

將儲存指定設定。Kaspersky Embedded Systems Security 將請求指定密碼以存取受防護的功能。

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，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**"套用密碼防護"**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。

即時檔案防護

本節包含有關即時檔案防護工作以及如何設定的資訊。

關於"即時檔案防護"工作

"即時檔案防護"工作執行期間，在存取以下受防護裝置物件時，Kaspersky Embedded Systems Security 會對這些物件進行掃描：

- 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。

當任何應用程式將檔案寫入受防護裝置或從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 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。對於此類處理程序，"即時檔案防護"工作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，即時檔案防護工作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樹狀目錄或清單的形式顯示。預設情況下，裝置的網路檔案資源以清單形式顯示。

在管理外掛程式中，只有清單視圖可用。

要在應用程式主控台中以樹狀目錄形式顯示網路檔案資源，

請開啟"**設定防護範圍**"視窗左上角部分中的下拉清單，然後選擇"**樹狀檢視**"。

無論受防護裝置的檔案資源以清單還是樹狀目錄的形式顯示，節點圖示的含義均如下：

☑ 節點包含在防護範圍內。

☐ 節點排除在防護範圍之外。

☑ 該節點至少有一個子節點排除在掃描範圍之外，或子節點的安全性設定與父節點的安全性設定不同（僅限樹狀目錄檢視）。

如果選擇了所有子節點，但未選擇父節點，則顯示 ☑ 圖示。在這種情況下，在為所選子節點建立了防護範圍後，如果父節點所包含的檔案和資料夾發生變更，將自動略過這些變更。

使用應用程式主控台，您還可以新增虛擬磁碟機到防護範圍中。虛擬節點的名稱以藍色顯示。

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樹狀目錄或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。
- 手動為檔案資源樹狀目錄或清單中的選定節點或項配置安全性設定（安全等級變更為**"自訂"**）。

可以將節點或項的一組設定儲存為範本，以便以後套用至其他節點或項。

關於虛擬防護範圍

Kaspersky Embedded Systems Security 不僅可以掃描硬碟磁碟機和卸除式磁碟機上的現有資料夾和檔案，還可以掃描由各種應用程式和服務在受防護裝置上動態建立的磁碟機。

若所有裝置物件均包含在防護範圍內，則這些動態節點將自動包含在防護範圍內。但是，如果您要為這些動態節點的安全性設定指定特殊值，或者只選擇了裝置的一部分進行防護，則為了將虛擬磁碟機、檔案或資料夾包含在防護範圍內，您必須首先在應用程式主控台中建立它們：即指定虛擬防護範圍。建立的磁碟機、檔案和資料夾將僅存在於應用程式主控台中，而非受防護裝置的檔案結構中。

若在建立防護範圍時選擇了所有子資料夾或檔案，但未選擇父資料夾，則其中顯示的所有虛擬資料夾或檔案將不會自動包含在防護範圍內。應在應用程式主控台中建立這些動態資料夾或檔案的"虛擬複本"並將其新增至防護範圍。

預定義的防護範圍

檔案資源樹狀目錄或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：

- **本機磁碟**。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。
- **虛擬磁碟機**。虛擬資料夾、檔案和暫時連線到裝置的磁碟機可包含在防護範圍內，例如，一般叢集磁碟機。

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。

預設情況下，防護範圍包括除虛擬磁碟機外的所有預定義區域。

使用 SUBST 指令建立的虛擬磁碟機不會顯示在應用程式主控台的受防護裝置檔案資源樹狀目錄中。要將虛擬磁碟機中的物件包含在防護範圍內，請將與此虛擬磁碟機關聯的裝置資料夾包含在防護範圍內。

已連線的網路磁碟也不會顯示在受防護裝置檔案資源清單中。若要將網路磁碟中的物件包含在防護範圍內，請以 UNC 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：“**最佳效能**”、“**建議**”和“**最佳防護**”。這些等級均有各自的安全設定集（請參閱下表）。

最佳效能

如果您的網路除了在受防護裝置上使用 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“**最佳效能**”安全等級。

建議

“**建議**”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**”安全等級。

最佳防護

如果組織的網路有更高的裝置安全要求，則建議使用“**最佳防護**”安全等級。

預設安全等級和相應的設定值

選項	安全等級		
	最佳效能	建議	最佳防護
物件防護	依副檔名	依格式	依格式
僅防護新增與變更過的檔案	已啟用	已啟用	已停用
對受感染物件和其他物件執行的操作	封鎖存取並解毒。解毒失敗則刪除	僅通知	封鎖存取並解毒。解毒失敗則刪除
對可疑物件執行的操作	封鎖存取並隔離	僅通知	封鎖存取並隔離
排除檔案	否	否	否
不偵測	否	否	否
超過以下時間則停止掃描(秒)	60 秒	60 秒	60 秒

不掃描超過此值複合檔案(MB)	8 MB	8 MB	未設定
掃描 NTFS 交換資料串流	是	是	是
掃描開機磁區和 MBR	是	是	是
複合物件防護	• 封裝的物件* *僅新物件和已修改的物件	• SFX 壓縮檔案* • 封裝的物件* • 內嵌的 OLE 物件* *僅新物件和已修改的物件	• SFX 壓縮檔案* • 封裝的物件* • 內嵌的 OLE 物件* *所有物件
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	否	否	是

預定義安全等級的設定中不包含**"物件防護"**、**"使用 iChecker 技術"**、**"使用 iSwift 技術"**和**"使用啟發式分析"**設定。若在選擇了其中一個預先定義的安全等級之後編輯**"物件防護"**、**"使用 iChecker 技術"**、**"使用 iSwift 技術"**或**"使用啟發式分析"**，所選的安全等級不會變更。

"即時檔案防護"工作中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?。*

“即時檔案防護”工作預設設定

預設情況下，“即時檔案防護”工作將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”工作預設設定

設定	預設值	敘述

防護範圍	整個受防護裝置，虛擬磁碟機除外。	您可以變更防護範圍。
安全性設定	整個防護範圍的一般設定；對應**"建議"**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性設定儲存為範本，以便在以後將其套用至其他節點。
物件防護模式	**智慧模式**	您可以選擇防護模式，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	套用**"中度"**安全等級。	可以啟用或停用"啟發式分析"並設定分析等級。
套用信任區域	已套用。	可以在選定工作中使用的一般排除清單。
在防護中使用 KSN	已套用。	您可以使用卡巴斯基安全網路雲端服務提高您的裝置防護能力（如果接受 KSN 聲明則可用）。
工作啟動排程	程式啟動時。	您可以配置為排程工作啟動。
封鎖對顯示惡意活動的主機的網路共用資源的存取	未套用。	可以將出現惡意活動的主機新增到封鎖的主機清單中。
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 將建立並啟動臨時的"關鍵區域掃描"工作。

透過管理外掛程式管理"即時檔案防護"工作

在本節中，學習如何導航管理外掛程式介面，以及如何為網路中的一台或所有受防護裝置配置工作設定。

導航

瞭解如何透過所選介面導航到所需工作設定。

開啟"即時檔案防護"工作的政策設定

要透過卡巴斯基安全管理中心政策開啟"即時檔案防護"工作設定：

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。

5. 在開啟的“**內容：<政策名稱>**”視窗中，選擇“**即時電腦防護**”部分。

6. 點擊“**即時檔案防護**”子區段中的“**設定**”按鈕。
   將開啟“**即時檔案防護**”視窗。

如果某個受防護裝置受卡巴斯基安全管理中心啟動政策管理，且該政策禁止變更應用程式設定，則無法透過應用程式主控台編輯這些設定。

開啟“即時檔案防護”工作內容

要開啟單台網路裝置的“即時檔案防護”工作設定視窗：

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“**裝置**”標籤。

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。
   - 在受防護裝置的內容功能表中選擇“**內容**”項。

   将打开“**属性：<受保护设备名称>**”窗口。

5. 在**工作**區段中，選取**即時檔案防護**工作。

6. 點擊“**內容**”按鈕。
   即時檔案防護将打开“属性：实时文件保护”窗口。

配置“即時檔案防護”工作

要配置“即時檔案防護”工作設定：

1. 開啟“**即時檔案防護**”視窗。

2. 配置以下工作設定：

   - 在“**一般**”標籤上：
     - **攔截參數**
     - **啟發式分析**
     - **與其他元件的整合**
   - 在“**工作管理**”標籤上：

- 排程工作啟動設定。

3. 選擇**"防護範圍"**標籤，然後執行以下操作：

- 點擊**"新增"**或**"編輯"**按鈕編輯防護範圍。
  - 在開啟的視窗中，選擇要包含到工作防護範圍的內容：
    - **預定義範圍**
    - **磁碟、資料夾或網路資料夾**
    - **檔案**
  - 選擇一項預設安全等級或手動配置防護設定。

4. 點擊**即時檔案防護**視窗中的**確定**。

Kaspersky Embedded Systems Security 將對正在執行的工作立即套用新設定。設定修改日期和時間以及修改前後工作設定值儲存在系統稽核記錄中。

選擇防護模式

在"即時檔案防護"工作中，可以選擇防護模式。在**"物件防護模式"**部分中，您可以指定 Kaspersky Embedded Systems Security 掃描物件時的存取嘗試類型。

"物件防護模式"設定的值套用於工作中指定的整個防護範圍。無法為防護範圍內的單個節點指定不同的設定值。

要選擇防護模式：

1. 開啟**"即時檔案防護"**視窗。

2. 在開啟的視窗中，開啟**"一般"**標籤，然後選擇要設定的防護模式：

- **智慧模式**
- **存取及修改時**
- **存取時**
- **執行時**
- **對啟動處理程序的更深入分析（在分析結束之前阻止處理程序啟動）**

3. 點擊**"確定"**。

選中防護模式將生效。

配置啟發式分析以及與其他應用程式元件的整合

要啟動“KSN 使用”工作，您必須接受卡巴斯基安全網路聲明。

要配置啟發式分析以及與其他元件的整合：

1. 開啟“**即時檔案防護**”視窗。
2. 在“**一般**”標籤上，清除或選中“**使用啟發式分析**”核取方塊。
3. 如有必要，使用滑塊調整分析等級。
4. 在“**與其他元件的整合**”部分中，配置以下設定：
   - 選中或清除“**套用信任區域**”核取方塊。
   - 選中或清除“**使用 KSN 防護**”核取方塊。

     在“KSN 使用”工作設定中必須選中“**傳送關於已掃描檔案的資料**”核取方塊。
   - 選中或清除“**封鎖對顯示惡意活動的主機的網路共用資源的存取**”核取方塊。
   - 選中或清除“**偵測到活動感染時啟動關鍵區域掃描**”核取方塊。
5. 點擊“**確定**”。

配置的工作設定將立即套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。

排程工作

您可以在應用程式主控台中排程本機系統和自訂工作。您無法透過應用程式主控台排程群組工作。

若要使用管理外掛程式排成群組工作，請執行以下操作：

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。
2. 選取受防護裝置所屬的群組。
3. 在結果窗格中，選取“**工作**”標籤。
4. 採用以下方法之一開啟“**內容：<工作名稱>**”視窗：
   - 點擊工作的名稱。
   - 開啟工作名稱的內容功能表，然後選取“內容”項。
5. 選取“**排程**”部分。
6. 在“**排程設定**”設定塊中，選中“**依排程執行**”核取方塊。

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。

7. 根據需要配置排程設定。為此，請執行以下操作：

   a. 在**"週期"**清單中，選擇以下值之一：

   - **每小時**，如果您希望該工作在指定的小時數內間隔執行，請在**"每 <數量> 小時"**欄位中指定小時數。
   - **每天**，如果您希望該工作在指定的天數內間隔執行，請在**"每 <數量> 天"**欄位中指定天數。
   - **每週**，如果您希望該工作在指定的週數內間隔執行，請在**"每 <數量> 週"**欄位中指定週數。指定啟動工作在星期中的日期（預設在星期一啟動工作）。
   - **在應用程式啟動時**，如果您希望在每次啟動 Kaspersky Embedded Systems Security 時執行該工作。
   - **應用程式資料庫更新後**，如果您希望在每次更新應用程式資料庫後執行該工作。

   b. 在**"開始時間"**欄位中指定首次啟動工作的時間。

   c. 在**開始日期**欄位中，指定啟動排程的開始日期。

   在排程工作的開始時間、日期和頻率之後，會顯示下一次開始的預估時間。

   前往**排程**頁籤，然後開啟**工作設定**視窗。在視窗上方的**下次開始**欄位中，會顯示預估的開始時間。每次您開啟視窗時，此預估的開始時間都會更新並顯示。

   如果卡巴斯基安全管理中心政策設定禁止啟動排程的本機系統工作，則**下次開始**欄位將顯示**政策不允許**值。

8. 根據需要使用**"進階"**標籤來配置以下排程設定。

   - 在**"工作停止設定"**部分中：

     a. 選中**"持續時間"**核取方塊，並在右側的欄位中輸入工作執行的最大持續時間（小時和分鐘）。

     b. 選中**"暫停時間"**核取方塊，並在右側的欄位中輸入暫停工作執行的時間隔（小於 24 小時）的開始值和結束值。

   - 在**"進階設定"**部分中：

     a. 選中**"取消排程，從"**核取方塊，並指定停止套用排程的日期。

     b. 選定**"執行錯過的工作"**核取方塊以允許啟動略過的工作。

     c. 選中**"在該時間間隔內隨機啟動工作"**核取方塊，並按分鐘指定該值。

9. 點擊**"確定"**。

10. 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。

建立和配置工作防護範圍

要透過卡巴斯基安全管理中心建立和配置工作防護範圍：

1. 開啟**"即時檔案防護"**視窗。
2. 選擇**"防護範圍"**標籤。
   已經受工作防護的所有項目都列在**"防護範圍"**表中。
3. 點擊**"新增"**按鈕向清單中新增新項目。
   將開啟**"新增物件至防護範圍"**視窗。
4. 選擇物件類型以將其新增到防護範圍中：
   - **預定義範圍**，將一個預定義範圍包含在裝置的防護範圍中。然後在下拉清單中，選擇所需的防護範圍。
   - **磁碟、資料夾或網路資料夾**，將單個磁碟機、資料夾或網路物件包括在防護範圍中。然後透過點擊**"瀏覽"**按鈕選擇所需的防護範圍。
   - **檔案**，將單個檔案包括在防護範圍中。然後透過點擊**"瀏覽"**按鈕選擇所需的防護範圍。

   如果某個物件已經作為防護範圍的排除新增，則不能再將其新增到防護範圍中。
5. 要從防護範圍中排除單個項目，請清除這些項目名稱旁邊的核取方塊，或者執行以下步驟：
   a. 右鍵點擊防護範圍開啟其內容功能表。
   b. 在內容功能表中，選擇**"新增排除項目"**選項。
   c. 在**"新增排除"**視窗中選擇物件類型，將按照將物件新增到防護範圍中時使用的步驟，將該物件類型作為防護範圍的排除新增。
6. 要修改防護範圍或現有排除，請選擇所需防護範圍內容功能表中的**"編輯範圍"**選項。
7. 若要在網路檔案資源清單中隱藏之前新增的防護範圍或排除，請在所需防護範圍的內容功能表中選擇**"刪除範圍"**選項。

   將防護範圍從網路檔案資源清單中刪除時，該防護範圍也從"即時檔案防護"工作範圍中刪除。
8. 點擊**"確定"**。

"設定防護範圍"視窗關閉。將儲存新配置的設定。

僅在至少有一個裝置檔案資源節點包含在防護範圍內時，才可啟動**"即時檔案防護"**工作。

為自訂掃描工作選擇預定義的安全等級

可以為裝置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：**"最佳效能"**、**"建議"**和**"最佳防護"**。

要選擇其中一個預定義安全等級：

1. 打开**"属性：即時檔案防護"**窗口。
2. 選擇**"防護範圍"**標籤。
3. 在受防護裝置清單中，選擇一個包含在防護範圍中的項目以設定預定義安全等級。
4. 點擊**"配置"**按鈕。
   將開啟**"即時檔案防護設定"**視窗。
5. 在**"安全等級"**標籤上，選擇要套用的安全等級。
   該視窗將顯示與選定安全等級相對應的安全性設定清單。
6. 點擊**"確定"**。
7. 单击**"属性：即時檔案防護"**窗口中的**"确定"**。
   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。

手動配置安全性設定

預設情況下，"即時檔案防護"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"**預定義安全等級。

可以透過將安全性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，來修改安全性設定的預設值。

要手動設定所選節點的安全性設定：

1. 開啟**"即時檔案防護"**視窗。
2. 在**"防護範圍"**標籤上，選擇您要配置其安全設定的節點，然後點擊**"配置"**。
   將開啟**"即時檔案防護設定"**視窗。
3. 在**"安全等級"**標籤上，點擊**"設定"**按鈕以自訂設定。
4. 您可以根據需求配置選定節點的自訂安全性設定：
   - 一般設定
   - 操作
   - 效能
5. 點擊**即時檔案防護**視窗中的**確定**。

將儲存新的防護範圍設定。

配置一般工作設定

要配置"即時檔案防護"工作的一般安全設定：

1. 開啟"**即時檔案防護**"視窗。
2. 選擇"**一般**"標籤。
3. 在"**物件防護**"部分中，指定要包含在防護範圍內的物件類型：
   - 所有物件
   - **按格式掃描物件**
   - **按病毒資料庫中指定的副檔名清單掃描物件**
   - **按指定的副檔名清單掃描物件**
   - **掃描開機磁區和 MBR**
   - **掃描 NTFS 交換資料串流**
4. 在"**效能**"部分中，選中或清除"**僅防護新增與變更過的檔案**"核取方塊。

   如果清除該核取方塊，要在可用選項之間轉換，請點擊每個複合物件類型對應的"全部/僅新建"連結。

5. 在"**複合物件防護**"部分中，指定要包含在防護範圍內的複合物件：
   - **僅新的壓縮檔案**全部/僅新建的壓縮檔案
   - **僅新的 SFX 壓縮檔案**全部/僅新建的 SFX 壓縮檔案
   - **僅新的電子郵件資料庫**全部/僅新建的電子郵件資料庫
   - **僅新的封裝的物件**全部/僅新封裝的物件
   - **僅新的純文字電子郵件**全部/僅新建的純文字電子郵件
   - **僅新嵌入的 OLE 物件**全部/僅新的內嵌 OLE 物件
6. 點擊"**儲存**"。

將儲存新的工作配置。

配置操作

要配置在"即時檔案防護"工作期間對受感染的物件和其他偵測到的物件的操作：

1. 開啟“**即時檔案防護**”視窗。
2. 選擇“**操作**”標籤。
3. 選擇要對受感染的物件和其他偵測到的物件執行的操作：
   - **僅通知**。
   - **封鎖存取**。
   - **執行附加操作**。
     從下拉清單中選擇操作：
     - **解毒**。
     - **解毒，無法解毒時刪除**解毒失敗則刪除。
     - **刪除**。
     - **建議**。
4. 選擇要對可能受感染的物件執行操作：
   - **僅通知**。
   - **封鎖存取**。
   - **執行附加操作**。
     從下拉清單中選擇操作：
     - **隔離**。
     - **刪除**。
     - **建議**。
5. 選擇依威脅類型對物件執行的操作：
   a. 清除或選中“**根據偵測到的物件的類型執行操作**”核取方塊。
   b. 點擊“**設定**”按鈕。
   c. 在開啟的視窗中，選擇針對每種偵測到的物件類型的主要操作和次要操作（如果主要操作失敗則執行）。
   d. 點擊“**確定**”。
6. 選擇要對不可修改的複合檔案執行的操作：選擇或清除“**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。
7. 點擊“**儲存**”。

將儲存新的工作配置。

配置效能

要配置"即時檔案防護"工作的效能設定：

1. 開啟"**即時檔案防護**"視窗。
2. 選擇"**效能**"標籤。
3. 在"**排除**"部分中：
   - 清除或選中"**排除檔案**"核取方塊。
   - 清除或選中"**不偵測**"核取方塊。
   - 針對每個設定點擊"**編輯**"按鈕以新增排除項目。
4. 在"**進階設定**"部分中：
   - **超過以下時間則停止掃描(秒)**
   - **不掃描超過此值複合檔案(MB)**
   - **使用 iSwift 技術**
   - **使用 iChecker 技術**

透過應用程式主控台管理"即時檔案防護"工作

在本節中，學習如何導航應用程式主控台介面以及如何在受防護裝置上配置工作設定。

導航

瞭解如何透過所選介面導航到所需工作設定。

開啟"即時檔案防護"工作設定

要開啟一般工作設定視窗：

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"**即時檔案防護**"子節點。
3. 在結果窗格中點擊"**內容**"連結。
   將開啟"**工作設定**"視窗。

開啟"即時檔案防護"工作範圍設定

要開啟"即時檔案防護"工作的設定防護範圍視窗：

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**"即時檔案防護"**子節點。
3. 在結果窗格中點擊**"配置防護範圍"**連結。
   開啟**"設定防護範圍"**視窗。

配置"即時檔案防護"工作

要配置"即時檔案防護"工作設定：

1. 開啟**"工作設定"**視窗。
2. 在**"一般"**標籤上，配置以下工作設定：
   - 物件防護模式
   - **啟發式分析**
   - **與其他元件整合**
3. 在**"排程"**和**"進階"**標籤上，指定排程的啟動設定。
4. **工作設定**在工作設定視窗中點擊確定。
   將儲存修改的設定。
5. 在**"即時檔案防護"**節點的結果窗格中，點擊**"配置防護範圍"**連結。
6. 執行以下操作：
   - 在裝置檔案資源樹狀目錄或清單中，選擇要包含在工作防護範圍內的節點或項目。
   - 選擇一項預設安全等級或手動配置物件防護設定。
7. 在**"設定防護範圍"**視窗中，點擊**"儲存"**按鈕。

Kaspersky Embedded Systems Security 將對正在執行的工作立即套用新設定。設定修改日期和時間以及修改前後的工作設定值儲存在系統稽核記錄中。

選擇防護模式

在"即時檔案防護"工作中，可以選擇防護模式。在**"物件防護模式"**部分中，您可以指定 Kaspersky Embedded Systems Security 掃描物件時的存取嘗試類型。

"物件防護模式"設定的值套用於工作中指定的整個防護範圍。無法為防護範圍內的單個節點指定不同的設定值。

要選擇防護模式：

1. 開啟“**工作設定**”視窗。
2. 在開啟的視窗中，開啟“**一般**”標籤，然後選擇要設定的防護模式：
   - **智慧模式**
   - **存取及修改時**
   - **存取時**
   - **執行時**
   - **對啟動處理程序的更深入分析（在分析結束之前阻止處理程序啟動）**
3. 點擊“**確定**”。

選中防護模式將生效。

配置啟發式分析以及與其他應用程式元件的整合

要啟動“KSN 使用”工作，您必須接受卡巴斯基安全網路聲明。

要配置啟發式分析以及與其他元件的整合：

1. 開啟“**工作設定**”視窗。
2. 在“**一般**”標籤上，清除或選中“**使用啟發式分析**”核取方塊。
3. 如有必要，使用滑塊調整分析等級。
4. 在“**與其他元件整合**”部分中，配置以下設定：
   - 選中或清除“**套用信任區域**”核取方塊。
     點擊“**信任區域**”連結開啟“信任區域”設定。
   - 選中或清除“**在防護中使用 KSN**”核取方塊。

     在“KSN 使用”工作設定中必須選中“**傳送關於已掃描檔案的資料**”核取方塊。
   - 選中或清除“**封鎖對顯示惡意活動的主機的網路共用資源的存取**”核取方塊。
   - 選中或清除“**偵測到活動感染時啟動關鍵區域掃描**”核取方塊。
5. 點擊“**確定**”。

將套用新設定的設定。

配置工作啟動排程設定

在應用程式主控台中，您可以排程何時啟動本機系統和自訂工作。但是，您無法排程何時開始群組工作。

要排程工作：

1. 開啟要排程的內容功能表。
2. 選擇"**內容**"。
   將開啟"**工作設定**"視窗。
3. 在開啟的視窗中的"**排程**"標籤上，選中"**依排程執行**"核取方塊。
4. 請按照以下步驟指定排程設定：
   a. 在**週期**下拉功能表中，選取以下值之一：
      - **每小時**：每隔一小時執行一次工作；在**每 <數目> 小時**欄位中指定時數。
      - **每天**：每天執行一次工作；在**每** <數目> **天天**欄位中指定天數。
      - **每週**：每週執行一次工作；在**每**<數目> **週**欄位中指定週數。指定工作啟動的星期中的日期（預設在星期一啟動工作）。
      - **在應用程式啟動時**，如果您希望在每次啟動 Kaspersky Embedded Systems Security 時執行該工作。
      - **應用程式資料庫更新後**，如果您希望在每次更新應用程式資料庫後執行該工作。
   b. 在**開始時間**欄位中，指定首次啟動工作的時間。
   c. 在**開始日期**欄位中，指定首次啟動工作的日期。

   指定了工作啟動頻率之後，將在視窗頂部的"**下次開始**"欄位中顯示工作的首次啟動時間、排程的開始套用日期以及預計下一個工作啟動時間的相關資訊。每次開啟"**工作設定**"視窗的"**排程**"標籤時，將更新並顯示下次工作開啟的估計時間。

   如果卡巴斯基安全管理中心活動政策設定禁止啟動排程的本機系統工作，則**下次開始**欄位將顯示**政策不允許**值。

5. 使用**進階**頁籤可以指定以下排程設定：
   - 在"**工作停止設定**"部分中：
     a. 選取**持續時間**核取方塊。在右側的欄位中，以小時和分鐘為單位輸入最大工作持續時間。
     b. 選取**暫停開始於**核取方塊。在右側的欄位中，輸入暫停和繼續執行工作的時間（24小時以內）。
   - 在"**進階設定**"部分中：
     a. 選取**取消排程開始於**核取方塊，然後指定工作排程的結束日期。
     b. 所選**執行錯過的工作**核取方塊以允許啟動略過的工作。
     c. 選中"**在該時間間隔內隨機啟動工作**"核取方塊，並按分鐘指定該值。

6. 點擊**"確定"**。

工作排程設定隨即儲存。

建立防護範圍

本節提供有關在即時檔案防護工作中建立和管理防護範圍的說明。

配置網路檔案資源的視圖

要在配置防護範圍設定期間選擇網路檔案資源的視圖：

1. 開啟**"設定防護範圍"**視窗。
2. 開啟左上角部分中的下拉清單，然後選擇以下選項之一：
   - 選擇**"樹狀檢視"**選項以樹狀目錄的形式顯示網路檔案資源。
   - 選擇**"清單檢視"**選項以清單形式顯示網路檔案資源。

   預設情況下，受防護裝置的網路檔案資源以清單形式顯示。
3. 點擊**"儲存"**按鈕。

建立防護範圍

建立"即時檔案防護"工作範圍的過程取決於所選的網路檔案資源視圖。您可以檢視樹狀目錄或清單（設定為預設）形式的網路檔案資源。

要對工作應用新的設定防護範圍，必須重新啟動"即時檔案防護"工作。

要使用網路檔案資源樹狀目錄建立防護範圍：

1. 開啟**"設定防護範圍"**視窗。
2. 在視窗的左側部分中，開啟網路檔案資源樹狀目錄以顯示所有節點和子節點。
3. 執行以下操作：
   - 要從防護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。
   - 要從防護範圍中包含單個節點，請清除**"我的電腦"**核取方塊，然後執行以下步驟：
     - 如果要將某一類型的所有磁碟機均包含在防護範圍內，請核取所需磁碟類型名稱旁的方塊（例如，若要新增裝置上的所有卸除式硬碟，則啟用**"卸除式磁碟機"**核取方塊）。

- 如果要將特定類型的單個磁碟包含在防護範圍內，請展開包含此類型磁碟清單的節點，並核取所需磁碟名稱旁的方塊。例如，若要选择可移动驱动器 F:，请展开**"卸除式磁碟機"**节点，然后选中驱动器 **F:** 对应的框。

- 如果您想要僅包含磁碟機上的單個資料夾或檔案，請選中該資料夾或檔案名稱旁邊的核取方塊。

4. 點擊**"儲存"**按鈕。

"設定防護範圍"視窗關閉。將儲存新配置的設定。

要使用網路檔案資源清單建立防護範圍：

1. 開啟**"設定防護範圍"**視窗。

2. 要從防護範圍中包含單個節點，請清除**"我的電腦"**核取方塊，然後執行以下步驟：

   a. 右鍵點擊防護範圍開啟其內容功能表。

   b. 在按鈕的內容功能表中，選擇**"新增防護範圍"**。

   c. 在**"新增防護範圍"**視窗中，選擇一個物件類型以將其新增到防護範圍中：

   - **預設的範圍**，將一個預定義範圍包含在裝置的防護範圍中。然後在下拉清單中，選擇所需的防護範圍。

   - **磁碟、資料夾或網路資料夾**，將單個磁碟機、資料夾或網路物件包括在防護範圍中。然後透過點擊**"瀏覽"**按鈕選擇所需的範圍。

   - **檔案**，將單個檔案包括在防護範圍中。然後透過點擊**"瀏覽"**按鈕選擇所需的範圍。

   如果某個物件已經作為防護範圍的排除新增，則不能再將其新增到防護範圍中。

3. 要從防護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，或者執行以下步驟：

   a. 右鍵點擊防護範圍開啟其內容功能表。

   b. 在內容功能表中，選擇**"新增排除項目"**選項。

   c. 在**"新增排除項目"**視窗中選擇物件類型，將按照將物件新增到防護範圍中時使用的步驟，將該物件類型作為防護範圍的排除新增。

4. 要修改防護範圍或現有排除，請選擇所需防護範圍內容功能表中的**"編輯範圍"**選項。

5. 若要在網路檔案資源清單中隱藏之前新增的防護範圍或排除，請在所需範圍的內容功能表中選擇**"從清單刪除"**選項。

   將防護範圍從網路檔案資源清單中刪除時，該防護範圍也從**"**即時檔案防護**"**工作範圍中刪除。

6. 點擊**"儲存"**按鈕。

"設定防護範圍"視窗關閉。將儲存新配置的設定。

僅在至少有一個裝置檔案資源節點包含在防護範圍內時，才可啟動"即時檔案防護"工作。

若指定了複雜防護範圍，例如，為裝置檔案資源樹狀目錄中的多個節點指定了不同的安全性設定值，則將可能導致掃描遭存取物件的速度緩慢。

在防護範圍內包含網路物件

您可以按照 UNC（通用命名慣例）格式指定網路磁碟機、資料夾或檔案的路徑以將它們新增至防護範圍。

您可以在系統帳戶下掃描網路資料夾。

要將網路位置新增到防護範圍：

1. 開啟"**設定防護範圍**"視窗。
2. 開啟左上角部分中的下拉清單，然後選擇"**樹狀檢視**"。
3. 在"**網路**"節點的內容功能表中：
   - 如果您想要向防護範圍中新增網路資料夾，選擇"**新增網路資料夾**"。
   - 如果您想要向防護範圍中新增網路檔案，選擇"**新增網路檔案**"。
4. 輸入 UNC 格式的網路資料夾或檔案路徑。
5. 點擊 **ENTER** 鍵。
6. 選中新增的網路物件旁邊的核取方塊以將其包含在防護範圍內。
7. 如有必要，變更已新增的網路物件的安全性設定。
8. 點擊"**儲存**"按鈕。

   將儲存修改的工作設定。

建立虛擬防護範圍

僅當防護/掃描範圍以檔案資源樹狀目錄的形式顯示時，您才可透過新增單個虛擬磁碟機、資料夾或檔案來延伸防護/掃描範圍。

要新增虛擬磁碟機至防護範圍：

1. 開啟"**設定防護範圍**"視窗。
2. 開啟視窗左上角的下拉清單部分，然後選擇**樹狀檢視**。

3. 開啟**"虛擬磁碟機"**節點的內容功能表。

4. 選擇**"新增虛擬磁碟機"**選項。

5. 在可用名稱清單中，為所建立的虛擬磁碟機選擇名稱。

6. 選中磁碟機旁的核取方塊以將磁碟機包含在防護範圍內。

7. 在**"設定防護範圍"**視窗中，點擊**"儲存"**按鈕。

將儲存新配置的設定。

要新增虛擬資料夾或虛擬檔案至防護範圍：

1. 開啟**"設定防護範圍"**視窗。

2. 開啟左上角部分中的下拉清單，然後選擇**"樹狀檢視"**。

3. 開啟要新增資料夾或檔案的虛擬磁碟機的內容功能表，然後選擇以下選項之一：

   - **新增虛擬資料夾**，如果您想要向防護範圍中新增虛擬資料夾。
   - **新增虛擬檔案**，如果您想要向防護範圍中新增虛擬檔案。

4. 在輸入欄位中指定資料夾或檔案的名稱。

5. 在已建立資料夾或已建立檔案的名稱列中，選擇核取方塊，以將此資料夾檔案包含在防護範圍內。

6. 在**"設定防護範圍"**視窗中，點擊**"儲存"**按鈕。

將儲存修改的工作設定。

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"**預定義安全等級。

可以透過將安全性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，來修改安全性設定的預設值。

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性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。

要手動配置安全設定：

1. 開啟**"設定防護範圍"**視窗。

2. 在左側視窗部分中，選擇用於配置安全設定的節點。
   可以為防護範圍內的選定節點或項目套用包含安全設定的預設範本。
   在視窗的左側部分，您可以選擇網路檔案資源的視圖、建立防護範圍或建立虛擬防護範圍 。

3. 在視窗的右側部分，執行下列操作之一：

   - 在**"安全等級"**標籤上，選擇要套用的安全等級。

- 在以下標籤中，根據需求配置選定節點或項目的所需安全設定：
  - **一般**
  - **操作**
  - **效能**

4. 在**"設定防護範圍"**視窗中，點擊**"儲存"**按鈕。

將儲存新的防護範圍設定。

為即時檔案防護工作選擇預定義安全等級

可以為受防護裝置檔案資源樹狀目錄或清單中的選定節點套用以下預定義安全等級之一：**"最佳效能"**、**"建議"**和**"最佳防護"**。

要選擇其中一個預定義安全等級：

1. 開啟**"設定防護範圍"**視窗。
2. 在受防護裝置網路檔案資源樹狀目錄或清單中，選擇要設定預定義安全等級的節點或項。
3. 確保選定的節點或項目包含在防護範圍中。
4. 在視窗右側的**"安全等級"**標籤中，選擇要應用的安全等級。

   該視窗將顯示與選定安全等級相對應的安全性設定清單。
5. 點擊**"儲存"**按鈕。

   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。

配置一般工作設定

要配置"即時檔案防護"工作的一般安全設定：

1. 開啟**"設定防護範圍"**視窗。
2. 選擇**"一般"**標籤。
3. 在**"物件防護"**部分中，指定要包含在防護範圍內的物件：
   - **所有物件**
   - **按格式掃描物件**
   - **按病毒資料庫中指定的副檔名清單掃描物件**
   - **按指定的副檔名清單掃描物件**

- **掃描開機磁區和 MBR**
- **掃描 NTFS 交換資料串流**

4. 在“**效能**”部分中，選中或清除“**僅防護新增與變更過的檔案**”核取方塊。

> 如果清除該核取方塊，要在可用選項之間轉換，請點擊每個複合物件類型對應的“**全部/僅新建**”連結。

5. 在“**複合物件防護**”部分中，指定要包含在防護範圍內的複合物件：
   - **全部/僅新的壓縮檔案**
   - **全部/僅新的 SFX 壓縮檔案**
   - **全部/僅新的電子郵件資料庫**
   - **全部/僅新的封裝的物件**
   - **全部/僅新的純文字電子郵件**
   - **全部/僅新嵌入的 OLE 物件**
6. 點擊“**儲存**”。

將儲存新的工作配置。

配置操作

要為“即時檔案防護”工作配置對受感染的物件和其他偵測到的物件的操作：

1. 開啟“**設定防護範圍**”視窗。
2. 選擇“**操作**”標籤。
3. 選擇要對受感染的物件和其他偵測到的物件執行的操作：
   - **僅通知**。
   - **封鎖存取**。
   - **執行附加操作**。
     從下拉清單中選擇操作：
     - **解毒**。
     - **解毒，無法解毒時刪除**解毒失敗則刪除。
     - **刪除**。
     - **建議**。
4. 選擇要對可能受感染的物件執行操作：

- **僅通知**。
- **封鎖存取**。
- **執行附加操作**。
  從下拉清單中選擇操作：
  - **隔離**。
  - **刪除**。
  - **建議**。

5. 選擇依威脅類型對物件執行的操作：
   a. 清除或選中**"根據偵測到的物件的類型執行操作"**核取方塊。
   b. 點擊**"設定"**按鈕。
   c. 在開啟的視窗中，選擇針對每種偵測到的物件類型的主要操作和次要操作（如果主要操作失敗則執行）。
   d. 點擊**"確定"**。
6. 選擇要對不可修改的複合檔案執行的操作：選擇或清除**"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。
7. 點擊**"儲存"**。

將儲存新的工作配置。

配置效能

要配置"即時檔案防護"工作的效能設定：

1. 開啟**"設定防護範圍"**視窗。
2. 選擇**"效能"**標籤。
3. 在**"排除"**部分中：
   - 清除或選中**"排除檔案"**核取方塊。
   - 清除或選中**"不偵測"**核取方塊。
   - 針對每個設定點擊**"編輯"**按鈕以新增排除項目。
4. 在**"進階設定"**部分中：
   - **超過以下時間則停止掃描(秒)**
   - **不掃描超過此值複合檔案(MB)**
   - **使用 iSwift 技術**

- 使用 iChecker 技術

即時檔案防護工作統計

即時檔案防護工作執行時，您可以檢視有關 Kaspersky Embedded Systems Security 自工作啟動以來已處理的物件數量的詳細即時資訊。

要檢視"即時檔案防護"工作統計：

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"**即時檔案防護**"子節點。

   工作統計顯示在選定節點的結果窗格的"**統計**"部分中。

可以檢視 Kaspersky Embedded Systems Security 自啟動以來已處理的物件的資訊（請參閱下表）。

即時檔案防護工作統計

欄位	敘述
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。
偵測到受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。
偵測到疑似感染的物件	Kaspersky Embedded Systems Security 偵測到的疑似感染物件數。
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。
物件未移至隔離區	Kaspersky Embedded Systems Security 嘗試隔離未成功（例如，由於磁碟空間不足）的物件數。
物件未刪除	Kaspersky Embedded Systems Security 嘗試刪除未成功（例如，其他應用程式封鎖存取物件）的物件數。
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。
物件未備份	Kaspersky Embedded Systems Security 嘗試在備份中儲存副本但未成功（例如，由於磁碟空間不足）的物件數。
處理錯誤	處理中導致錯誤的物件數目。
物件已解毒	Kaspersky Embedded Systems Security 已解毒的物件的數量。
已移至隔離區	Kaspersky Embedded Systems Security 已隔離的物件的數量。
已移至備份區	Kaspersky Embedded Systems Security 儲存至備份的檔案數目。

物件已刪除	Kaspersky Embedded Systems Security 已移除的物件的數量。
受密碼防護的物件	由於受密碼防護而導致 Kaspersky Embedded Systems Security 錯過的物件（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。
物件已處理	Kaspersky Embedded Systems Security 已刪除的物件的總數。

透過點擊詳細資訊窗格中"**開啟工作記錄**"部分的"**管理**"連結，可以在工作記錄中檢視即時檔案防護工作統計。

如果"即時檔案防護工作記錄"視窗中的"**總計事件**"欄位的值大於 0，則建議手動處理"**事件**"標籤上的工作記錄中的事件。

透過 Web 外掛程式管理"即時檔案防護"工作

在本部分中，學習如何透過 Web 外掛程式介面管理"即時檔案防護"工作。

配置"即時檔案防護"工作

無法透過 Web 外掛程式為"即時檔案防護"工作變更預定義安全等級。

要透過 Web 外掛程式配置"即時檔案防護"工作：

1. 在 Web 控制的主視窗中，選取**裝置 → 政策和設定檔案**。
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**"標籤。
4. 選擇"**即時電腦防護**"部分。
5. 點擊"**設定**"子區段中的"**即時檔案防護**"。
6. 按下表所述配置設定。

"即時檔案防護"工作設定

設定	敘述
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。
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。
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。
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。
對啟動處理程序的更深入分析（在分析結束之前阻止處理程序啟動）	Kaspersky Embedded Systems Security 對啟動處理程序執行更長時間的分析，偵測到威脅的可能性更高。在分析結束之前，將阻止處理程序啟動。
使用啟發式分析	此核取方塊可在物件掃描過程中啟用/停用啟發式分析。 如果選中該核取方塊，則啟用啟發式分析。 如果取消選中該核取方塊，則停用啟發式分析。 預設將會選定該核取方塊。
啟發式分析層級	啟發式分析等級用於在威脅搜尋的徹底程度、作業系統資源負荷和掃描所需時間之間建立平衡。 以下掃靈敏度等級可用： • **輕度**。啟發式分析在可執行檔中執行較少指令。在該模式下偵測出威脅的可能性較小。掃描速度較快，而且占用資源較少。 • **中度**。啟發式分析執行 Kaspersky 專家建議的可執行檔指令數。 預設選中該等級。 • **深度**。啟發式分析在可執行檔中執行較多指令。在該模式下偵測出威脅的可能性較大。掃描使用更多的系統資源、花費更多時間且可導致更多的誤報。 如果選中“**使用啟發式分析**”核取方塊，則該設定才可用。
套用信任區域	使用此核取方塊可啟用/停用工作的信任區域。 如果選中該核取方塊，Kaspersky Embedded Systems Security 會將受信任處理程序的檔案操作新增到工作設定中配置的掃描排除中。 如果清除該核取方塊，Kaspersky Embedded Systems Security 會在建立工作的防護範圍時略過受信任處理程序的檔案操作。 預設將會選定該核取方塊。
在防護中使用 KSN	該核取方塊可啟用或停用 KSN 服務的使用。 如果選中該核取方塊，應用程式將使用卡巴斯基安全網路資料確保應用程式更快速地對新威脅做出回應，並降低誤報的可能性。 如果清除該核取方塊，則工作將不使用 KSN 服務。 預設將會選定該核取方塊。
封鎖對顯示惡意活動的主機的網路共用資源的存取	該核取方塊用於啟用或停用將出現惡意活動的主機新增到封鎖的主機清單中。 如果選中該核取方塊，Kaspersky Embedded Systems Security 會將出現惡意活動的主機新增到封鎖的主機清單中。 如果清除該核取方塊，Kaspersky Embedded Systems Security 不會將出現惡意活動的主機新增到封鎖的主機清單中。 預設取消選定該核取方塊。 您可以在封鎖的主機儲存中檢視封鎖的主機清單。

	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。
偵測到活動感染時啟動關鍵區域掃描	如果選中此核取方塊，在偵測到活動感染時，Kaspersky Embedded Systems Security 將建立並啟動臨時的"關鍵區域掃描"工作。當"關鍵區域掃描"暫時工作完成後，Kaspersky Embedded Systems Security 會刪除此暫時工作。 如果清除此核取方塊，在偵測到活動感染時，Kaspersky Embedded Systems Security 不會建立和啟動"關鍵區域掃描"工作。 預設將會選定該核取方塊。
防護範圍	您可以配置防護範圍的安全性設定。

配置工作防護範圍

要配置"即時檔案防護"工作的防護範圍：

1. 在 Web 控制的主視窗中，選取**裝置 → 政策和設定檔案**。
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**"標籤。
4. 選擇"**即時電腦防護**"部分。
5. 點擊"**設定**"子區段中的"**即時檔案防護**"。
6. 選擇"**防護範圍**"部分。
7. 執行以下操作之一：
   - 點擊"**新增**"按鈕以新增新規則。
   - 選擇一個現有規則，然後單擊"**編輯**"按鈕。

   將開啟"**編輯範圍**"視窗。
8. 將切換按鈕切換到"**活動**"，然後選擇一個物件類型。
9. 在"**物件防護**"部分中，配置以下設定：
   - **物件防護模式**：
     - **所有物件**
     - **按格式掃描物件**
     - **按病毒資料庫中指定的副檔名清單掃描物件**
     - **按指定的副檔名清單掃描物件**
   - **掃描開機磁區和 MBR**

- **掃描 NTFS 交換資料串流**

10. 在"**物件防護**"部分中，選中或清除"**僅防護新增與變更過的檔案**"核取方塊。
11. 在"**複合物件防護**"部分中，指定要包含在掃描範圍內的複合物件：
    - **壓縮檔案**
    - **SFX 壓縮檔案**
    - **封裝的物件**
    - **電子郵件資料庫**
    - **純文字電子郵件**
    - **嵌入的 OLE 物件**
    - 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
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：
    - **僅通知**。
    - **封鎖存取**。
    - **執行附加操作**。
      從下拉清單中選擇操作：
      - **解毒**。
      - **解毒，無法解毒時刪除**解毒失敗則刪除。
      - **刪除**。
      - **建議**。
13. 選擇要對可能受感染的物件執行操作：
    - **僅通知**。
    - **封鎖存取**。
    - **執行附加操作**。
      從下拉清單中選擇操作：
      - **隔離**。
      - **刪除**。
      - **建議**。
14. 選擇依威脅類型對物件執行的操作：
    a. 清除或選中"**根據偵測到的物件的類型執行操作**"核取方塊。

b. 點擊**"設定"**按鈕。

c. 在開啟的視窗中，選擇針對每種偵測到的物件類型的主要操作和次要操作（如果主要操作失敗則執行）。

d. 點擊**"確定"**。

15. 在**"排除"**部分中，配置以下設定：

- 清除或選中**"排除檔案"**核取方塊。
- 清除或選中**"不偵測"**核取方塊。

16. 在**"效能"**部分中，配置以下設定：

- **超過以下時間則停止掃描(秒)**
- **不掃描超過此值的複合物件 (MB)**
- **使用 iSwift 技術**
- **使用 iChecker 技術**

17. 點擊**"確定"**按鈕。

KSN 使用

本節包含有關“KSN 使用”工作以及如何設定的資訊。

在美國使用的軟體將無法提供更新功能（包括防毒軟體簽章更新和程式碼庫更新）和 KSN 功能。

關於“KSN 使用”工作

卡巴斯基安全網路（也稱為“KSN”）是一個線上服務的基礎架構，提供存取 Kaspersky 有效的知識庫。該知識庫中包含了檔案信譽、網頁資源和程式的相關資訊。卡巴斯基安全網路允許 Kaspersky Embedded Systems Security 十分迅速地對新威脅作出反應，提高許多防護元件的效能，以降低誤報可能性。

要啟動“KSN 使用”工作，您必須接受卡巴斯基安全網路聲明。

Kaspersky Embedded Systems Security 從卡巴斯基安全網路接收的資訊僅與程式的信譽有關。

加入 KSN 使 Kaspersky 能夠接收有關新威脅類型和來源的資訊，研發出使其失效的方法，並減少應用程式元件中的誤報數量。

資料處理有關傳輸、處理、儲存和銷毀有關應用程式使用情況的更多詳細資訊在“KSN 使用”工作的“資料處理”視窗中和 Kaspersky 網站上的隱私政策中提供。

加入卡巴斯基安全網路完全出於自願。在安裝 Kaspersky Embedded Systems Security 後，做出關參加卡巴斯基安全網路的決定。您可以隨時變更有關參加卡巴斯基安全網路的決定。

可在以下 Kaspersky Embedded Systems Security 工作中使用卡巴斯基安全網路：

- 即時檔案防護。
- 自訂掃描。
- 應用程式啟動控制。

卡巴斯基專屬安全網路

如需如何配置卡巴斯基私人安全網路（以下稱「私人 KSN」）的詳細資訊，請參閱 *卡巴斯基安全管理中心說明*。

如果在裝置上使用專屬 KSN，則在“KSN 使用”工作的“**資料處理**”視窗中，可以透過選中“**我接受卡巴斯基安全網路聲明的條款**”核取方塊來閱讀 KSN 聲明和啟用該工作。接受該條款，即表示您同意將 KSN 聲明中提到的各類資料（安全請求、統計資料）傳送到 KSN 服務。

接受私有 KSN 條款後，用於調整全球 KSN 使用的核取方塊將無法使用。

如果在"KSN 使用"工作執行時停用私有 KSN，則將出現*產品授權衝突*錯誤且工作將停止。要繼續防護裝置，您需要接受"**資料處理**"視窗中的 KSN 聲明並重新啟動該工作。

撤銷接受 KSN 聲明

您可以隨時撤銷接受聲明並停止與卡巴斯基安全網路的任何資料交換。以下操作被視為完全或部分撤銷 KSN 聲明：

- 清除"**傳送關於已掃描檔案的資料**"核取方塊：應用程式停止將掃描的檔案的核對總和傳送到 KSN 服務進行分析。
- 清除"**傳送卡巴斯基安全網路統計資訊**"核取方塊：應用程式停止處理附加 KSN 統計的資料。
- 清除"**我接受卡巴斯基安全網路聲明的條款**"核取方塊：應用程式停止所有與 KSN 相關的資料處理，"KSN 使用"工作停止。
- 移除"KSN 使用"元件：所有與 KSN 相關的資料處理都將停止。
- 移除 Kaspersky Embedded Systems Security：所有與 KSN 相關的資料處理都將停止。
- 解除安裝 Kaspersky Embedded Systems Security 的產品授權金鑰或產品授權被暫停：所有與 KSN 相關的資料處理將停止。

"KSN 使用"工作預設設定

您可以變更「KSN 使用」工作的預設設定（請參閱下表）。

"KSN 使用"工作預設設定

設定	預設值	敘述
對 KSN 不信任的物件執行的操作	刪除	您可以指定 Kaspersky Embedded Systems Security 對 KSN 標識為不受信任的物件執行的操作。
資料傳輸	為大小不超過 2 MB 的檔案計算檔案核對總和（MD5 雜湊）。	您可以指定要使用 MD5 演算法為其計算核對總和以提交給 KSN 的檔案的最大大小。如果清除該核取方塊，Kaspersky Embedded Systems Security 將為任意大小的檔案計算 MD5 雜湊。
工作啟動排程	不設定工作的初次啟動排程。	您可以手動啟動該工作或設定排程啟動。
使用卡巴斯基安全管理中心作為 KSN 代理	選中	預設情況下，資料透過卡巴斯基安全管理中心傳送到 KSN。 只能透過管理外掛程式變更此設定。
我接受卡巴斯基安全網路聲明的條款	已解毒	如已選取，即接受安裝後加入 KSN。您可以隨時變更決定。
傳送卡巴斯基安全網路統計資訊	選中（僅當接受 KSN 聲明時應用）	如果接受 KSN 聲明，將自動傳送 KSN 統計，除非清除相應核取方塊。
傳送關於掃	選中（僅當接受 KSN	如果接受 KSN 聲明，將傳送自工作啟動以來掃描和分析的檔案的

描的檔案的資料	聲明時應用）	資料。您可以隨時清除該核取方塊。

透過管理外掛程式管理“KSN 使用”

在本節中，學習如何透過管理外掛程式配置“KSN 使用”工作和資料處理。

配置“KSN 使用”工作

要配置“KSN 使用”工作：

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細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**”標籤，然後開啟“**內容：<政策名稱>**”視窗。
   - 要為單台受防護裝置配置應用程式，請選擇“**裝置**”標籤，然後開啟“**應用程式設定**”視窗。

   如果某個啟動卡巴斯基安全管理中心政策已套用於裝置，並且該政策封鎖對應用程式設定的變更，則無法在“**應用程式設定**”視窗中編輯這些設定。
4. 在“**即時電腦防護**”部分中，點擊“**KSN 使用**”子區段中的“**設定**”按鈕。
   將開啟“**KSN 使用**”視窗。
5. 在“**一般**”標籤上，配置以下工作設定：
   - 在“**對 KSN 不信任的物件執行的操作**”部分中，指定 Kaspersky Embedded Systems Security 在偵測到 KSN 確定為不受信任的物件時將執行的操作：
     - **刪除**
     - **記錄資訊**
   - 在“**資料傳輸**”部分中，限制要為其計算核對總和的檔案的大小：
     - 清除或選中“**如果檔案大小超過以下大小(MB)，則在傳送到 KSN 之前不計算核對總和**”核取方塊。
     - 如果需要，在右側欄位中指定 Kaspersky Embedded Systems Security 要為其計算核對總和的最大檔案大小。
   - 在“**KSN 代理**”部分中，清除或選中“**使用卡巴斯基安全管理中心作為 KSN 代理**”核取方塊。

     要啟用 KSN 代理，必須接受 KSN 聲明並正確配置卡巴斯基安全管理中心。有關詳細資訊，請參閱 *卡巴斯基安全管理中心說明*。

6. 如果需要，在**“工作管理”**標籤上配置工作啟動排程。例如，如果您希望在重新啟動受防護裝置時自動執行該工作，可以按排程啟動工作並指定**“在應用程式啟動時”**頻率。

   應用程式將按排程自動啟動“KSN 使用”工作。

7. 在啟動工作前配置資料處理。

8. 點擊**“確定”**。

將套用修改的設定。修改設定的日期和時間以及有關修改前後的工作設定的資訊均儲存在系統稽核記錄中。

配置資料處理

要設定哪些資料將被 KSN 服務處理並接受 KSN 聲明：

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細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”**標籤，然後開啟**“內容：<政策名稱>”**視窗。
   - 要為單台受防護裝置配置應用程式，請選擇**“裝置”**標籤，然後開啟**“應用程式設定”**視窗。

   > 如果某個啟動卡巴斯基安全管理中心政策已套用於裝置，並且該政策封鎖對應用程式設定的變更，則無法在**“應用程式設定”**視窗中編輯這些設定。

4. 在**“即時電腦防護”**部分中，點擊**“KSN 使用”**子區段中的**“資料處理”**按鈕。

   將開啟**“KSN 資料處理”**視窗。

5. 在**“統計和服務”**標籤上，閱讀聲明並選中**“我接受卡巴斯基安全網路聲明的條款”**核取方塊。

6. 為提高防護等級，以下核取方塊會自動選中：

   - **傳送關於掃描的檔案的資料**。
   - **傳送卡巴斯基安全網路統計資訊**。

   您可以隨時清除這些核取方塊並停止傳送附加資料。

7. **“傳送卡巴斯基安全網路統計資訊”**核取方塊預設情況下處於選中狀態。如果您不希望 Kaspersky Embedded Systems Security 將其他統計傳送到 Kaspersky，可以隨時清除該核取方塊。

8. 點擊**“確定”**。

   將儲存資料處理配置。

透過應用程式主控台管理“KSN 使用”

在本節中，學習如何透過應用程式主控台配置“KSN 使用”工作和資料處理。

配置“KSN 使用”工作

要配置“KSN 使用”工作：

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“**KSN 使用**”子節點。
3. 在結果窗格中點擊“**內容**”連結。
   將開啟“**工作設定**”視窗的“**一般**”標籤。
4. 設定工作：
   - 在“**對 KSN 不信任的物件執行的操作**”部分中，指定 Kaspersky Embedded Systems Security 在偵測到 KSN 確定為不受信任的物件時將執行的操作：
     - **刪除**
     - **記錄資訊**
   - 在“**資料傳輸**”部分中，限制要為其計算核對總和的檔案的大小：
     - 清除或選中“**如果檔案大小超過以下大小(MB)，則在傳送到 KSN 之前不計算核對總和**”核取方塊。
     - 如果需要，在右側欄位中指定 Kaspersky Embedded Systems Security 要為其計算核對總和的最大檔案大小。
5. 如果需要，在“**排程**”和“**進階**”標籤上設定工作啟動排程。例如，如果您希望在重新啟動受防護裝置時自動執行該工作，可以啟用按排程啟動工作並指定“**在應用程式啟動時**”的啟動頻率。
   應用程式將按排程自動啟動“KSN 使用”工作。
6. 在啟動工作前配置資料處理。
7. 點擊“**確定**”。

將套用修改的設定。修改設定的日期和時間以及有關修改前後的工作設定的資訊均儲存在系統稽核記錄中。

配置資料處理

要設定哪些資料將被 KSN 服務處理並接受 KSN 聲明：

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“**KSN 使用**”子節點。
3. 在結果窗格中點擊“**資料處理**”連結。
   將開啟“**資料處理**”視窗。

4. 在“**統計和服務**”標籤上，閱讀聲明並選中“**我接受卡巴斯基安全網路聲明的條款**”核取方塊。

5. 為提高防護等級，以下核取方塊會自動選中：

   - **傳送關於掃描的檔案的資料**。
   - **傳送卡巴斯基安全網路統計資訊**。

   您可以隨時清除這些核取方塊並停止傳送附加資料。

6. “**傳送卡巴斯基安全網路統計資訊**”核取方塊預設情況下處於選中狀態。如果您不希望 Kaspersky Embedded Systems Security 將其他統計傳送到 Kaspersky，可以隨時清除該核取方塊。

7. 點擊“**確定**”。

將儲存資料處理配置。

透過 Web 外掛程式管理“KSN 使用”

要透過 Web 外掛程式配置“KSN 使用”工作和資料處理：

1. 在 Web 控制的主視窗中，選取**裝置 → 政策和設定檔案**。

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**”標籤。

4. 選擇“**即時電腦防護**”部分。

5. 點擊「**KSN 使用**」子區段中的「**設定**」。

6. 按下表所述配置設定。

透過管理外掛程式配置“KSN 使用”工作和資料處理

設定	敘述
刪除	Kaspersky Embedded Systems Security 將刪除具有 KSN 不信任狀態的物件，並在備份中放置副本。 預設選中該選項。
記錄資訊	Kaspersky Embedded Systems Security 將在工作記錄中記錄有關具有 KSN 不信任狀態的物件的資訊。Kaspersky Embedded Systems Security 不會刪除不受信任的物件。
如果檔案大小超過以下大小，則在傳送到 KSN 之前不計算校正總和	此核取方塊可啟用或停用為指定大小的檔案計算核對總和，以將此資訊提交至 KSN 服務。 核對總和計算的持續時間取決於檔案大小。 如果選中此核取方塊，則 Kaspersky Embedded Systems Security 不會為超過指定大小（以 MB 為單位）的檔案計算核對總和。 如果清除該核取方塊，Kaspersky Embedded Systems Security 將為任意大小的檔案計算核對總和。 預設將會選定該核取方塊。
我確認已完	

全閱讀、瞭解並接受參加卡巴斯基安全網路聲明的條款	選中此核取方塊即表示您確認您已閱讀並接受卡巴斯基安全網路聲明的條款。
傳送關於已掃描檔案的資料	如果選中該核取方塊，Kaspersky Embedded Systems Security 會將掃描的檔案的核對總和傳送到 Kaspersky。關於每個檔案的安全性的結論基於從 KSN 收到的信譽。 如果清除該核取方塊，Kaspersky Embedded Systems Security 不會將檔案的核對總和傳送到 KSN。 請注意，檔案信譽請求可能在受限制模式下傳送。限制用於防護 Kaspersky 信譽伺服器免受 DDoS 攻擊。在這種情況下，所傳送的檔案信譽請求的參數由 Kaspersky 專家建立的規則和方法定義，使用者無法在受防護裝置上進行設定。這些規則和方法的更新與應用程式資料庫更新一起接收。如果應用限制，“KSN 使用”工作統計中將顯示“*由 Kaspersky 啟用以防護 KSN 伺服器免受 DDoS*”狀態。 預設將會選定該核取方塊。
同意處理資料作為卡巴斯基安全網路統計的一部分	如果選中該核取方塊，Kaspersky Embedded Systems Security 會傳送附加統計，其中可能包括個人資料。作為 KSN 統計傳送的所有資料的清單在 KSN 聲明中有所說明。Kaspersky 收到的資料用於改善應用程式質量和提高威脅偵測速率等級。 如果清除該核取方塊，Kaspersky Embedded Systems Security 不會傳送其他統計。 預設將會選定該核取方塊。
工作管理	您可以配置按排程啟動工作的設定。

設定其他資料傳輸

Kaspersky Embedded Systems Security 可以設定為將以下資料傳送到 Kaspersky：

- 掃描的檔案的核對總和（“**傳送關於掃描的檔案的資料**”核取方塊）。
- 附加統計資訊，包括個人資料（“**傳送卡巴斯基安全網路統計資訊**”核取方塊）。

有關傳送到 Kaspersky 的資料的詳細資訊，請參見本手冊的“本機資料處理”部分。

僅**在選取我接受卡巴斯基安全網路聲明的條款**核取方塊時，才能選取或清除相應的核取方塊。

預設情況下，當您接受 KSN 聲明後，Kaspersky Embedded Systems Security 將傳送檔案的核對總和和附加統計。

僅當卡巴斯基安全管理中心政策封鎖資料處理設定的變更時，“**我接受卡巴斯基安全網路聲明的條款**”核取方塊才可編輯。

可能的核取方塊狀態和相應條件

核取方塊狀態	“傳送關於已掃描檔案的資料”核取方塊狀態的條件	“傳送卡巴斯基安全網路統計資訊”核取方塊狀態的條件	“我接受卡巴斯基安全網路聲明的條款”核取方塊狀態的條件
☑	• 已傳送信譽請求	• 已傳送附加統計	• 已接受卡巴斯基安全網路聲明的條款

	• 核取方塊可編輯	• 核取方塊可編輯	• 核取方塊可編輯
☑	• 已傳送信譽請求 • 核取方塊不可編輯	• 已傳送附加統計 • 核取方塊不可編輯	• 已接受卡巴斯基安全網路聲明的條款 • 核取方塊不可編輯
☐	• 未傳送信譽請求 • 核取方塊可編輯	• 未傳送附加統計 • 核取方塊可編輯	• 未接受卡巴斯基安全網路聲明的條款 • 核取方塊可編輯
☐	• 未傳送信譽請求 • 核取方塊不可編輯	• 未傳送附加統計 • 核取方塊不可編輯	• 未接受卡巴斯基安全網路聲明的條款 • 核取方塊不可編輯

"KSN 使用"工作統計

在執行"KSN 使用"工作期間，可以即時檢視 Kaspersky Embedded Systems Security 自啟動以來已處理的物件數量的相關詳細資訊。有關工作執行期間發生的所有事件的資訊記錄在工作記錄中。

要檢視"KSN 使用"工作統計：

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"**KSN 使用**"子節點。

工作統計顯示在選定節點的詳細資訊視窗的"**統計**"部分中。

您可以檢視自工作啟動以來 Kaspersky Embedded Systems Security 已處理物件的相關資訊（請參閱下表）。

"KSN 使用"工作統計

欄位	敘述
請求傳送錯誤	對其處理產生工作錯誤的 KSN 請求數。
統計資訊已形成	傳送到 KSN 的產生的統計封包數量。
物件已刪除	Kaspersky Embedded Systems Security 在執行"KSN 使用"工作時刪除的物件數。
已移至備份區	Kaspersky Embedded Systems Security 儲存至備份的檔案數目。

物件未刪除	Kaspersky Embedded Systems Security 嘗試刪除但因某些原因（例如，另一程式封鎖存取物件）而無法刪除的物件數目。有關此類物件的資訊記錄在工作記錄中。
物件未備份	Kaspersky Embedded Systems Security 嘗試將其副本儲存至備份但因出錯而無法執行此操作的物件數目。程式不會解毒或刪除無法移動到備份中的檔案。有關此類物件的資訊記錄在工作記錄中。
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。

網路威脅防護

本節包含有關“網路威脅防護”工作以及如何設定該工作的資訊。

關於“網路威脅防護”工作

“網路威脅防護”只能安裝在執行 Microsoft Windows 7 及更高版本或 Windows Server 2008 R2 及更高版本的裝置上。

“網路威脅防護”工作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。然後，您的螢幕將顯示一則警告，指出有網路攻擊的企圖，並顯示有關攻擊電腦的資訊。

預設情況下，“網路威脅防護”工作會在“**偵測到攻擊時封鎖連線**”模式下執行。在此模式下，Kaspersky Embedded Systems Security 會將出現典型網路攻擊活動的主機 IP 位址新增到封鎖的主機清單中。

您可以在封鎖的主機儲存中檢視封鎖的主機清單。

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。
- “網路威脅防護”工作已停止，並且清除了“**工作未執行時不停止流量分析**”核取方塊。
- “**偵測到攻擊時封鎖連線**”模式已關閉。

“網路威脅防護”工作預設設定

“網路威脅防護”工作使用下表描述的預設設定。您可以變更這些設定值。

“網路威脅防護”工作預設設定

設定	預設值	敘述
處理模式	**偵測到攻擊時封鎖連線**	「網路威脅防護」工作可以在**直通**、**僅通知網路攻擊**或**偵測到攻擊時封鎖連線**模式下啟動。

		該核取方塊用於啟用或停用將出現典型網路攻擊活動的主機新增到封鎖的主機清單中。 如果選擇此模式，Kaspersky Embedded Systems Security 會掃描傳入的網路流量中是否存在典型網路攻擊活動，記錄有關偵測到的活動事件，並將出現典型網路攻擊活動的主機的 IP 位址新增到封鎖的主機清單中。 預設選擇該模式。 您可以在封鎖的主機儲存中檢視封鎖的主機清單。 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。 如果選擇此模式，Kaspersky Embedded Systems Security 會掃描傳入的網路流量中是否存在典型網路攻擊活動，記錄有關偵測到的活動事件，但不會封鎖攻擊電腦的網路活動。 如果選擇此模式，Kaspersky Embedded Systems Security 會掃描傳入的網路流量中是否存在典型網路攻擊活動，但不會記錄有關偵測到的活動事件，也不會封鎖攻擊電腦的網路活動。 例如，當受防護裝置的效能下降時，可以使用此模式。
排除	不套用排除清單。	指定要從工作防護範圍中排除的區域。
排程設定	預設情況下，當 Kaspersky Embedded Systems Security 啟動時，「網路威脅防護」工作將自動啟動。	您可以配置排程。

透過應用程式主控台配置“網路威脅防護”工作

在本節中，學習如何透過應用程式主控台介面管理“網路威脅防護”工作。

一般工作設定

要配置一般工作設定：

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“**網路威脅防護**”子節點。
3. 在**內容**節點的詳細資訊視窗中，點擊**網路威脅防護**連結。
   將開啟“**工作設定**”視窗。

4. 開啟“**一般**”標籤。

5. 在“**處理模式**”部分中選擇處理模式：

- **直通**。

  如果選擇此模式，Kaspersky Embedded Systems Security 會掃描傳入的網路流量中是否存在典型網路攻擊活動，但不會記錄有關偵測到的活動事件，也不會封鎖攻擊電腦的網路活動。

  例如，當受防護裝置的效能下降時，可以使用此模式。

- **僅通知網路攻擊**。

  如果選擇此模式，Kaspersky Embedded Systems Security 會掃描傳入的網路流量中是否存在典型網路攻擊活動，記錄有關偵測到的活動事件，但不會封鎖攻擊電腦的網路活動。

- **偵測到攻擊時封鎖連線**。

  該核取方塊用於啟用或停用將出現典型網路攻擊活動的主機新增到封鎖的主機清單中。

  如果選擇此模式，Kaspersky Embedded Systems Security 會掃描傳入的網路流量中是否存在典型網路攻擊活動，記錄有關偵測到的活動事件，並將出現典型網路攻擊活動的主機的 IP 位址新增到封鎖的主機清單中。

  預設選擇該模式。

  您可以在封鎖的主機儲存中檢視封鎖的主機清單。

  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。

6. 選中或清除“**工作未執行時不停止流量分析**”核取方塊。

   如果選中此核取方塊，當“網路威脅防護”工作停止後，Kaspersky Embedded Systems Security 會掃描傳入的網路流量中是否存在典型網路攻擊活動，並根據所選處理模式封鎖攻擊電腦的網路活動。

   如果清除此核取方塊，當“網路威脅防護”工作停止後，Kaspersky Embedded Systems Security 不會掃描傳入的網路流量中是否存在典型網路攻擊活動，也不會封鎖攻擊電腦的網路活動。

   預設取消選定該核取方塊。

7. 點擊“**確定**”。

新增排除

要新增「網路威脅防護」工作的排除項目，請執行以下步驟：

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“**網路威脅防護**”子節點。

3. 在**內容**節點的詳細資訊視窗中，點擊**網路威脅防護**連結。

   將開啟“**工作設定**”視窗。

4. 在“**排除**”標籤上，選中“**不控制排除的 IP 位址**”核取方塊。

   如果選中此核取方塊，Kaspersky Embedded Systems Security 不會掃描排除的 IP 位址的傳入網路流量。
   如果清除該核取方塊，Kaspersky Embedded Systems Security 不會套用排除清單。

5. 指定 IP 位址，然後點擊“**新增**”按鈕。

6. 點擊“**確定**”。

透過管理外掛程式配置“網路威脅防護”工作

在本節中，學習如何透過管理外掛程式介面管理“網路威脅防護”工作。

一般工作設定

要配置一般工作設定：

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細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**”標籤，然後開啟“**內容：<政策名稱>**”視窗。
   - 要為單台受防護裝置配置應用程式，請選擇“**裝置**”標籤，然後開啟“**應用程式設定**”視窗。

     如果某個啟動卡巴斯基安全管理中心政策已套用於裝置，並且該政策封鎖對應用程式設定的變更，則無法在“**應用程式設定**”視窗中編輯這些設定。

4. 在“**即時電腦防護**”部分中，點擊“**網路威脅防護**”子區段中的“**設定**”按鈕。
   將開啟“**網路威脅防護**”視窗。

5. 開啟“**一般**”標籤。

6. 在“**處理模式**”部分中選擇處理模式：

   - **直通**。

     如果選擇此模式，Kaspersky Embedded Systems Security 會掃描傳入的網路流量中是否存在典型網路攻擊活動，但不會記錄有關偵測到的活動事件，也不會封鎖攻擊電腦的網路活動。
     例如，當受防護裝置的效能下降時，可以使用此模式。

   - **僅通知網路攻擊**。

如果選擇此模式，Kaspersky Embedded Systems Security 會掃描傳入的網路流量中是否存在典型網路攻擊活動，記錄有關偵測到的活動事件，但不會封鎖攻擊電腦的網路活動。

- **偵測到攻擊時封鎖連線**。

  該核取方塊用於啟用或停用將出現典型網路攻擊活動的主機新增到封鎖的主機清單中。

  如果選擇此模式，Kaspersky Embedded Systems Security 會掃描傳入的網路流量中是否存在典型網路攻擊活動，記錄有關偵測到的活動事件，並將出現典型網路攻擊活動的主機的 IP 位址新增到封鎖的主機清單中。

  預設選擇該模式。

  您可以在封鎖的主機儲存中檢視封鎖的主機清單。

  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。

7. 選中或清除“**工作未執行時不停止流量分析**”核取方塊。

   如果選中此核取方塊，當“網路威脅防護”工作停止後，Kaspersky Embedded Systems Security 會掃描傳入的網路流量中是否存在典型網路攻擊活動，並根據所選處理模式封鎖攻擊電腦的網路活動。

   如果清除此核取方塊，當“網路威脅防護”工作停止後，Kaspersky Embedded Systems Security 不會掃描傳入的網路流量中是否存在典型網路攻擊活動，也不會封鎖攻擊電腦的網路活動。

   預設取消選定該核取方塊。

8. 點擊“**確定**”。

新增排除

要新增「網路威脅防護」工作的排除項目，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細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**”標籤，然後開啟“**內容：<政策名稱>**”視窗。
   - 要為單台受防護裝置配置應用程式，請選擇“**裝置**”標籤，然後開啟“**應用程式設定**”視窗。

     如果某個啟動卡巴斯基安全管理中心政策已套用於裝置，並且該政策封鎖對應用程式設定的變更，則無法在“**應用程式設定**”視窗中編輯這些設定。

4. 在“**即時電腦防護**”部分中，點擊“**網路威脅防護**”子區段中的“**設定**”按鈕。

   將開啟“**網路威脅防護**”視窗。

5. 在“**排除**”標籤上，選中“**不控制排除的 IP 位址**”核取方塊。

如果選中此核取方塊，Kaspersky Embedded Systems Security 不會掃描排除的 IP 位址的傳入網路流量。
如果清除該核取方塊，Kaspersky Embedded Systems Security 不會套用排除清單。

6. 指定 IP 位址，然後點擊**"新增"**按鈕。
7. 點擊**"確定"**。

透過 Web 外掛程式配置"網路威脅防護"工作

在本節中，學習如何透過 Web 外掛程式介面管理"網路威脅防護"工作。

一般工作設定

要配置一般工作設定：

1. 在 Web 控制的主視窗中，選取**裝置 → 政策和設定檔案**。
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"**標籤。
4. 選擇**"即時電腦防護"**部分。
5. 點擊**"設定"**子區段中的**"網路威脅防護"**。
6. 開啟**"一般"**標籤。
7. 在**"處理模式"**部分中選擇處理模式：

- **直通**。

  如果選擇此模式，Kaspersky Embedded Systems Security 會掃描傳入的網路流量中是否存在典型網路攻擊活動，但不會記錄有關偵測到的活動事件，也不會封鎖攻擊電腦的網路活動。
  例如，當受防護裝置的效能下降時，可以使用此模式。

- **僅通知網路攻擊**。

  如果選擇此模式，Kaspersky Embedded Systems Security 會掃描傳入的網路流量中是否存在典型網路攻擊活動，記錄有關偵測到的活動事件，但不會封鎖攻擊電腦的網路活動。

- **偵測到攻擊時封鎖連線**。

該核取方塊用於啟用或停用將出現典型網路攻擊活動的主機新增到封鎖的主機清單中。

如果選擇此模式，Kaspersky Embedded Systems Security 會掃描傳入的網路流量中是否存在典型網路攻擊活動，記錄有關偵測到的活動事件，並將出現典型網路攻擊活動的主機的 IP 位址新增到封鎖的主機清單中。

預設選擇該模式。

您可以在封鎖的主機儲存中檢視封鎖的主機清單。

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。

8. 選中或清除“**工作未執行時不停止流量分析**”核取方塊。

如果選中此核取方塊，當“網路威脅防護”工作停止後，Kaspersky Embedded Systems Security 會掃描傳入的網路流量中是否存在典型網路攻擊活動，並根據所選處理模式封鎖攻擊電腦的網路活動。

如果清除此核取方塊，當“網路威脅防護”工作停止後，Kaspersky Embedded Systems Security 不會掃描傳入的網路流量中是否存在典型網路攻擊活動，也不會封鎖攻擊電腦的網路活動。

預設取消選定該核取方塊。

9. 點擊“**確定**”。

新增排除

要新增「網路威脅防護」工作的排除項目，請執行以下步驟：

1. 在 Web 控制的主視窗中，選取**裝置 → 政策和設定檔案**。
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**”標籤。
4. 選擇“**即時電腦防護**”部分。
5. 點擊“**設定**”子區段中的“**網路威脅防護**”。
6. 在“**排除**”標籤上，選中“**不控制排除的 IP 位址**”核取方塊。

如果選中此核取方塊，Kaspersky Embedded Systems Security 不會掃描排除的 IP 位址的傳入網路流量。

如果清除該核取方塊，Kaspersky Embedded Systems Security 不會套用排除清單。

7. 指定 IP 位址，然後點擊“**新增**”按鈕。
8. 點擊“**確定**”。

應用程式啟動控制

本節包含有關“應用程式啟動控制”工作以及如何設定的資訊。

關於“應用程式啟動控制”工作

在執行“應用程式啟動控制”工作時，Kaspersky Embedded Systems Security 會監控使用者啟動應用程式的嘗試，並允許或拒絕這些應用程式啟動。“應用程式啟動控制”工作依賴於“預設拒絕”原則，這意味著工作設定中不允許的任何應用程式都會被自動封鎖。

您可以使用以下方法之一允許應用程式啟動：

- 設定受信任的應用程式的允許規則。
- 啟動時在 KSN 中檢查受信任應用程式的聲譽。

該工作為拒絕應用程式啟動賦予最高優先順序。例如，如果某個應用程式被封鎖規則之一封鎖啟動，該應用程式將被拒絕啟動，不管 KSN 的受信任結論如何。而且，如果應用程式不受 KSN 服務信任，但包括在允許規則範圍中，此應用程式會被拒絕啟動。

所有啟動應用程式的嘗試將記錄在工作記錄中。

“應用程式啟動控制”工作可以執行在以下兩種模式之一：

- **活動**。Kaspersky Embedded Systems Security 使用一組規則來控制處於應用程式啟動控制規則範圍內的應用程式的啟動。應用程式啟動控制規則的範圍在該工作的設定中指定。如果應用程式處於應用程式啟動控制規則範圍內，並且工作設定不滿足任何指定規則，此應用程式會被拒絕啟動。

  不在「應用程式啟動控制」工作設定中指定的任何規則範圍內的應用程式會被拒絕啟動，不管「應用程式啟動控制」工作設定如何。

  如果未建立任何規則或為一台受防護裝置建立了超過 65,535 條規則，則“**應用程式啟動控制**”工作無法在啟動模式下啟動。

- **僅統計**。Kaspersky Embedded Systems Security 不使用應用程式啟動控制規則來允許或拒絕應用程式啟動。相反，它只記錄有關應用程式啟動、正在執行的應用程式所滿足的規則以及如果工作在“**活動**”模式下執行已執行的操作的資訊。所有應用程式均允許啟動。預設設定此模式。

  您可以使用此模式基於工作記錄中記錄的資訊建立應用程式啟動控制規則。

您可根據以下方案之一配置“應用程式啟動控制”工作：

- 進階規則配置及其在應用程式啟動控制中的使用。
- 基本規則配置和應用程式啟動控制的 KSN 使用。

如果作業系統檔案在“應用程式啟動控制”工作的範圍內，建議在建立應用程式啟動控制規則時確保新建立的規則允許此類應用程式。否則，作業系統可能無法啟動。

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”工作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*允許*或*拒絕*規則。要為“應用程式啟動控制”建立允許規則清單，可以使用規則產生器允許規則或在“**僅統計**”模式下使用“應用程式啟動控制”工作。您也可以手動新增允許規則。

- 使用者和/或使用者群組。

  應用程式啟動控制規則可以按使用者或群組控制指定應用程式的啟動。

- 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會控制滿足規則設定中指定的其中一個標準的檔案的啟動：由指定*數位憑證*簽章、比對指定 *SHA256 雜湊*或位於指定*路徑*。

  如果將“**數位憑證**”設定為規則觸發條件，則建立的規則會控制作業系統中所有受信任應用程式的啟動。您可透過選中以下核取方塊為此條件設定更加嚴格的條件：

  - **使用主旨**
  - **使用指紋**

  > 指紋最嚴格地限制了基於數位憑證的應用程式啟動規則的觸發，因為指紋唯一標識了數位憑證且無法偽造，這一點與數位憑證的主旨不同。

您可以指定應用程式啟動控制規則的排除。應用程式啟動控制規則的排除基於用於觸發規則的相同條件：數位憑證、SHA256 雜湊和檔案路徑。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。

> 如果作業系統檔案在“應用程式啟動控制”工作的範圍內，建議在建立應用程式啟動控制規則時確保新建立的規則允許此類應用程式。否則，作業系統可能無法啟動。

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：

- 手動新增規則。

- 自動建立和新增規則。
- 刪除規則。
- 將規則匯出到檔案。
- 檢查所選檔案是否存在允許執行這些檔案的規則。
- 根據指定的條件篩選清單中的規則。

關於軟體分發控制

如果您還需要控制受防護裝置（例如，所安裝軟體會定期自動更新的受防護裝置）上的軟體分發，則應用程式啟動控制規則產生器可能很複雜。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"工作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"子系統。

軟體分發套件（下文稱為"軟體套件"）表示要在受防護裝置上安裝的軟體應用程式。每個軟體套件都包含至少一個應用程式，除了應用程式外，可能還包含單個檔案、更新，甚至單個指令，尤其是在您安裝軟體應用程式或更新時。

"軟體分發控制"子系統作為附加排除清單實施。將軟體分發套件新增到此清單時，應用程式允許解壓縮這些受信任套件，並允許受信任套件所安裝或修改的軟體自動啟動。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。

Kaspersky Embedded Systems Security 僅控制完整軟體分發週期。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，應用程式將無法正確處理由受信任套件修改的檔案的啟動。

如果在"應用程式啟動控制"工作設定中清除"**將規則套用於可執行檔**"核取方塊，軟體分發控制將無法使用。

軟體分發快取

Kaspersky Embedded Systems Security 使用動態產生的軟體分發快取（"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，並將檔案核對總和及路徑儲存在分發快取中。然後預設允許分發快取中的所有檔案啟動。

您不能透過使用者介面檢視、清除或手動修改分發快取。快取由 Kaspersky Embedded Systems Security 填充和控制。

您可以將分發快取匯出到設定檔（XML 格式），同時使用命令列選項清除快取。

要將分發快取匯出到設定檔，請執行以下指令：

```
kavshell appcontrol /config /savetofile:<full path> /sdc
```

要清除分發快取，請執行以下指令：

```
kavshell appcontrol /config /clearsdc
```

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核對總和發生變化，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"工作在啟動模式下啟動，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，因為核對總和儲存在分發快取內。

處理擷取的檔案

第一次啟動軟體套件時，從受信任軟體套件擷取的所有檔案都會繼承受信任內容。如果在第一次啟動後清除該核取方塊，從軟體套件擷取的所有檔案都將保留繼承的內容。要重設所有擷取檔案中的繼承內容，您需要在再次啟動受信任分發套件之前清除分發快取並清除"**允許進一步分發套件透過此分法套件建立的程式**"核取方塊。

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會在它們的核對總和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。預設情況下，受信任內容的繼承等級數是無限制的。

作業系統重新啟動後，擷取的檔案將保留受信任內容。

檔案處理在"軟體分發控制"設定中透過選中或清除"**允許進一步分發套件透過此分法套件建立的程式**"核取方塊來進行配置。

例如，假設您將包含幾個其他套件和應用程式的 test.msi 套件新增到排除清單中並選中該核取方塊。在這種情況下，將允許執行或擷取 test.msi 套件中包含的所有套件和應用程式（如果它們包含其他檔案）。此方案適用於所有嵌套等級上的擷取檔案。

如果將 test.msi 套件新增到排除清單中並清除"**允許進一步分發套件透過此分法套件建立的程式**"核取方塊，應用程式只會將受信任內容分配到直接從主受信任套件擷取的套件和可執行檔（在第一個嵌套等級上）。此類檔案的核對總和儲存在分發快取中。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。

使用應用程式啟動控制規則清單

軟體分發控制子系統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）。

使用 KSN 結論

KSN 的檔案不受信任的結論具有比軟體分發控制排除項目更高的優先順序：如果 KSN 報告受信任套件建立過修改的檔案不受信任，則受信任套件的解壓縮和這些檔案的啟動都將被封鎖。

而且，在從受信任套件解壓縮後，所有子檔案都將被允許執行，不管是否在應用程式啟動控制範圍內使用 KSN。此時，"**拒絕 KSN 不信任的應用程式**"和"**允許 KSN 信任的應用程式**"核取方塊的狀態不影響"**允許進一步分發套件透過此分法套件建立的程式**"核取方塊的操作。

關於“應用程式啟動控制”工作的 KSN 使用

要啟動“KSN 使用”工作，您必須接受 KSN 聲明。

如果有關某個應用程式聲譽的 KSN 資料被“應用程式啟動控制”工作使用，則 KSN 應用程式聲譽將被視為允許或拒絕該應用程式啟動的條件。如果 KSN 在使用者嘗試啟動某個應用程式時向 Kaspersky Embedded Systems Security 報告該應用程式不受信任，應用程式啟動將被拒絕。如果 KSN 在使用者嘗試啟動某個應用程式時向 Kaspersky Embedded Systems Security 報告該應用程式受信任，應用程式啟動將被允許。KSN 可與應用程式啟動控制規則一起使用，或作為拒絕應用程式啟動的獨立條件。

使用 KSN 結論作為拒絕應用程式啟動的獨立條件

此方案允許在受防護裝置上安全地控制應用程式啟動，而無需對規則清單進行進階配置。

您可以將 KSN 結論連同唯一指定的規則一起套用於 Kaspersky Embedded Systems Security。該應用程式將僅允許啟動 KSN 中信任的或指定規則允許的應用程式。

對於此類方案，建議設定一條根據數位憑證允許應用程式啟動的規則。

按照“預設拒絕”政策，將拒絕所有其他應用程式。當沒有應用任何規則時，使用 KSN 來防護裝置免受 KSN 認為會造成威脅的應用程式的侵害。

與應用程式啟動控制規則一起套用 KSN 結論

將 KSN 結論與應用程式啟動控制規則同時使用時，以下條件適用：

- 如果某個應用程式包括在至少一條拒絕規則的範圍內，Kaspersky Embedded Systems Security 將始終拒絕該應用程式的啟動。如果應用程式被視為受 KSN 信任，則相應結論具有較低優先順序且不被考慮；仍將拒絕應用程式啟動。這允許您延伸封鎖的應用程式清單。
- 如果禁止啟動在 KSN 中不受信任的應用程式並且某個應用程式在 KSN 中不受信任，則 Kaspersky Embedded Systems Security 將始終拒絕該應用程式啟動。如果為應用程式設定了允許規則，則此規則具有較低優先順序且不被考慮；仍將拒絕應用程式啟動。這樣可以防護裝置免受被 KSN 視為威脅（但在首次配置規則時未被考慮）的應用程式的侵害。

關於應用程式啟動控制規則產生

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，以基於單台受防護裝置上執行的應用程式建立規則清單。

“應用程式啟動控制”元件安裝後具有兩條預設的允許規則：

- 針對作業系統信任的指令碼和帶憑證的 Windows Installer 軟體套件的允許規則。
- 針對作業系統信任的帶憑證的可執行檔的允許規則。

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。

  在此方案下，一個群組工作會為網路上的每台受防護裝置建立其自己的應用程式啟動控制規則清單，並將這些清單儲存到指定共用資料夾中的 XML 檔案。“應用程式啟動控制規則產生器”工作產生的 XML 檔案包含工作啟動前工作設定中指定的允許規則。不會為指定工作設定中不允許啟動的應用程式建立任何規則。預設情況下將拒絕此類應用程式啟動。然後，您可將建立的規則清單手動匯入卡巴斯基安全管理中心政策的“應用程式啟動控制”工作。

  您可將建立的規則配置為自動匯入“應用程式啟動控制”工作的規則清單。

  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。建議僅當套用的允許規則包含您知道安全的資料夾和檔案時，才配置“應用程式啟動控制規則產生器”工作的排程啟動。

  在網路中使用“應用程式啟動控制”工作之前，請確保所有受防護裝置都能夠存取共用資料夾。如果組織的政策未規定使用網路中的共用資料夾，建議在測試受防護裝置群組中的受防護裝置或範本機上啟動“應用程式啟動控制規則產生器”工作。

- 基於在“**僅統計**”模式下執行的“應用程式啟動控制”工作在卡巴斯基安全管理中心中建立的工作事件報告。

  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”在“**僅統計**”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**”標籤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。

  您需要設定工作執行期限，以便可在指定時間期限內執行所有可能的受防護裝置和受防護裝置群組操作方案以及至少一次受防護裝置重新啟動。工作執行期限結束後，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工作。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。建議透過在測試管理群組中的受防護裝置上以“**僅統計**”模式執行“應用程式啟動控制規則產生器”工作或“應用程式啟動控制”工作來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工作分析建立。為了在建立規則清單時將網路上利用的所有應用程式考慮在內，建議在範本機上以“**僅統計**”模式啟動“應用程式啟動控制規則產生器”工作和“應用程式啟動控制”工作。

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。

“應用程式啟動控制”工作預設設定

預設情況下，“應用程式啟動控制”工作具有下表所述的設定。您可以變更這些設定值。

“應用程式啟動控制”工作預設設定

設定	預設值	敘述
工作模式	**僅統計**。該工作根據設定的規則記錄拒絕的啟動事件和允許的啟動事件。應用程式啟動實際不會被拒絕。	在建立最終規則清單後，您可以選擇**“活動”**模式。
為檔案隨後的所有啟動重複執行該檔案第一次啟動時的操作	未套用	您可以為檔案隨後的所有啟動重複執行該檔案第一次啟動時的操作。
在沒有可執行的指令時拒絕指令解釋器啟動	未套用。	您可以在沒有可執行的指令時拒絕命令列編譯器啟動。
規則管理	**將政策規則新增到本機規則**	可以選擇將政策中指定的規則與受防護裝置上的規則一起套用的模式。
規則使用範圍	此工作可控制執行檔、指令碼和 MSI 套件的啟動。此工作還可監控 DLL 模組載入。	您可以指定要使用規則控制其啟動的檔案類型。
KSN 使用	不使用 KSN 應用程式聲譽資料。	在執行“應用程式啟動控制”工作時，您可以使用 KSN 應用程式聲譽資料。
自動允許透過所列應用程式和資料套件分發軟體	未套用。	可以使用安裝程式和設定中指定的應用程式允許軟體分發。預設情況下，僅允許使用 Windows Installer 進行軟體分發。
始終允許透過 Windows Installer 進行軟體分發	已套用（僅當**“自動允許透過所列應用程式和資料套件分發軟體”**設定啟用時可以變更）。	如果透過 Windows Installer 執行操作，您可允許任何軟體安裝或更新。
始終允許使用背景智慧傳輸服務透過 SCCM 進行軟體分發	未套用（僅當**“自動允許透過所列應用程式和資料套件分發軟體”**設定啟用時可以變更）。	可以使用 System Center Configuration Manager 開啟或關閉軟體分發。
啟動工作	不設定工作的初次啟動排程。	“應用程式啟動控制”工作不會在 Kaspersky Embedded Systems Security 啟動時自動啟動。您可以手動啟動該工作或設定排程啟動。

“應用程式啟動控制規則產生器”工作的預設設定

設定	預設值	敘述
允許規則名稱前置詞	與安裝了 Kaspersky Embedded Systems Security 的受防護裝置的名稱相同。	您可以變更允許規則的名稱前置詞。
允許規則的使	預設情況下，允許規則的範圍包括以下檔案類別：	您可以透過新增或刪除資料夾路徑並指定將被自動建立的規則允許啟動的檔案類型來變更防護範圍。您還可以在建立允許規則時略過正在執行的應用程式。

用範圍	• 位於以下資料夾中的具有 EXE 副檔名的檔案：C:\Windows、C:\Program Files (x86) 和 C:\Program Files • 儲存在 C:\Windows 資料夾中的 MSI 安裝套件 • 儲存在 C:\Windows 資料夾中的指令碼 該工作還會為所有正在執行的應用程式建立規則，而不管其位置和格式。	
建立允許規則的條件	使用數位憑證主旨和指紋；為所有使用者和使用者群組建立規則。	在建立允許規則時，可以使用 SHA256 雜湊。 您可以選擇需要為其自動建立允許規則的使用者和使用者群組。
工作完成時的操作	允許規則新增到應用程式啟動控制規則清單；新規則與現有規則合併；重複規則被刪除。	您可以將規則新增到現有規則，而不進行合併和刪除重複規則，或將現有規則替換為新的允許規則，或設定將允許規則匯出到檔案。
工作啟動設定及權限	在系統帳戶下啟動工作。	您可以允許"應用程式啟動控制規則產生器"工作在系統帳戶下或使用指定使用者的權限啟動。
工作啟動排程	不設定工作的初次啟動排程。	"應用程式啟動控制規則產生器"工作不會在 Kaspersky Embedded Systems Security 啟動時自動啟動。您可以手動啟動該工作或設定排程啟動。

透過管理外掛程式管理應用程式啟動控制

在本節中，學習如何導航管理外掛程式介面，以及如何為網路中的一台或所有受防護裝置配置工作設定。

導航

瞭解如何透過所選介面導航到所需工作設定。

開啟"應用程式啟動控制"工作的政策設定

要透過卡巴斯基安全管理中心政策開啟"應用程式啟動控制"工作設定：

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。
5. 在打开的**"属性：<策略名称>"**窗口中，选择**"本地活动控制"**部分。
6. 點擊**"應用程式啟動控制"**子區段中的**"設定"**按鈕。
   將開啟**"應用程式啟動控制"**視窗。

根據需要設定政策。

開啟應用程式啟動控制規則清單

要透過卡巴斯基安全管理中心開啟應用程式啟動控制規則清單：

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。
5. 在打开的**"属性：<策略名称>"**窗口中，选择**"本地活动控制"**部分。
6. 點擊**"應用程式啟動控制"**子區段中的**"設定"**按鈕。
   將開啟**"應用程式啟動控制"**視窗。
7. 在**"一般"**標籤上，點擊**"規則清單"**按鈕。
   將開啟**"應用程式啟動控制規則"**視窗。

根據需要設定規則清單。

開啟"應用程式啟動控制規則產生器"工作精靈和內容

要開始建立"應用程式啟動控制規則產生器"工作：

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**"工作"**標籤。
4. 點擊**"建立工作"**按鈕。
   將開啟**"新建工作精靈"**視窗。
5. 選擇**"應用程式啟動控制規則產生器"**工作。
6. 點擊**"下一步"**。

將開啟**"設定"**視窗。

要配置現有"應用程式啟動控制規則產生器"工作：

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**"工作"**標籤。
4. 按兩下卡巴斯基安全管理中心工作清單中的工作名稱。
   將打開**"屬性：應用程式啟動控制規則產生器"**窗口。

有關配置該工作的詳細資訊，請參見"配置'應用程式啟動控制規則產生器'工作"部分。

配置"應用程式啟動控制"工作設定

要配置一般"應用程式啟動控制"工作設定：

1. 開啟**"應用程式啟動控制"**視窗。
2. 在**"一般"**標籤上，選擇**"工作模式"**部分的以下設定：
   - 在**"工作模式"**下拉清單中，指定工作模式。
   - 清除或選中**"為檔案隨後的所有啟動重複執行該檔案第一次啟動時的操作"**核取方塊。
   - 清除或選中**"在沒有可執行的指令時拒絕命令列編譯器啟動"**核取方塊。
3. 在**"規則管理"**部分中，配置應用規則的設定：
   a. 點擊**"規則清單"**按鈕以新增"應用程式啟動控制"工作的允許規則。

   > Kaspersky Embedded Systems Security 無法辨識包含斜線"/"的路徑。請使用反斜線"\"來正確輸入路徑。

   b. 選擇套用規則的模式：
      - **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。
      - **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。可以使用"應用程式啟動控制規則產生器"工作編輯本機規則清單。
4. 在**"規則使用範圍"**部分中，指定以下設定：
   - **將規則套用於可執行檔**。
   - **監控 DLL 模組的載入**。

控制 DLL 模組的載入可能影響作業系統的效能。

- **將規則套用於指令碼和 MSI 資料套件**。

5. 在"**KSN 使用**"方塊中，配置以下應用程式啟動設定：
   - **拒絕 KSN 不信任的應用程式**。
   - **允許 KSN 信任的應用程式**。
   - 允許啟動 KSN 中信任的應用程式的使用者和/或使用者群組。
6. 在"**軟體分發控制**"標籤上，配置軟體分發控制的設定。
7. 在"**工作管理**"標籤上，配置排程的工作啟動設定。
8. 點擊**應用程式啟動控制**視窗中的**儲存**。

Kaspersky Embedded Systems Security 將對正在執行的工作立即套用新設定。有關設定修改日期和時間以及修改前後工作設定值的資訊儲存在系統稽核記錄中。

配置軟體分發控制

要新增受信任分發套件：

1. 開啟"**應用程式啟動控制**"視窗。
2. 在「**軟體分發控制**」標籤上，選取「自動允許透過所列應用程式和資料套件分發軟體」核取方塊。

   如果在"**自動允許透過所列應用程式和資料套件分發軟體**"工作設定中選中"**將規則套用於可執行檔**"標籤中的"**一般**"核取方塊，則您可選中"**應用程式啟動控制**"。

3. 根據需要清除"**始終允許透過 Windows Installer 進行軟體分發**"核取方塊。

   僅當在絕對必要時才建議清除"**始終允許透過 Windows Installer 進行軟體分發**"核取方塊。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。

4. 如果需要，請選擇"**始終允許使用背景智慧傳輸服務透過 SCCM 進行軟體分發**"核取方塊。

   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應用程式之前已執行分發的任何階段，則應用程式不會控制過程。

5. 要編輯受信任分發套件的清單，請點擊"**變更分發套件清單**"，然後在開啟的視窗中選擇以下方法之一：
   - **新增一個分發套件**。
     a. 點擊"**瀏覽**"按鈕。

b. 選擇可執行檔或分發套件。

“**信任條件**”部分會使用有關選定檔案的資料自動進行填充。

c. 清除或選中“**允許進一步分發套件透過此分法套件建立的程式**”核取方塊。

d. 選擇兩個可用條件選項中的一個，用於決定檔案或安裝套件是否受信任：

- **使用數位憑證**
- **使用 SHA256 雜湊**

- **按雜湊新增多個分發套件**。

  您可以選擇無限數量的可執行檔和分發套件，並同時將它們新增到清單。Kaspersky Embedded Systems Security 將檢查雜湊並允許作業系統啟動指定的檔案。

- **變更選定的分發套件**。

  使用此選項可以選擇不同的可執行檔或分發套件，或變更信任條件。

- **從檔案匯入分發套件清單**。

  在“開啟”視窗中，指定包含受信任分發套件清單的設定檔。

6. 如果要刪除受信任清單中以前新增的應用程式或分發套件，請點擊“**刪除分發套件**”按鈕。將允許執行擷取的檔案。

   要封鎖擷取的檔案啟動，請在受防護裝置上移除應用程式，或在應用程式啟動控制工作設定中建立拒絕規則。

7. 點擊“確定”。

將儲存新配置的設定。

配置“應用程式啟動控制規則產生器”工作

要配置“應用程式啟動控制規則產生器”工作：

1. 打开“**屬性：應用程式啟動控制規則產生器**”窗口。
2. 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，請參見 *卡巴斯基安全管理中心說明*。

3. 在“**設定**”部分中，您可配置以下設定：
   - 為規則名稱的前置詞。
   - 選擇如何建立允許規則：
     - **基於正在執行的應用程式建立允許規則**

- **為資料夾中的應用程式建立允許規則**

4. 在“**選項**”部分中，可以指定在建立應用程式啟動控制允許規則時執行的操作：

   - **使用數位憑證**
   - **使用數位憑證主旨和指紋**
   - **憑證遺失則使用**
     - **SHA256 hash**.將用於建立規則的檔案的核對總和設定為觸發應用程式啟動控制允許規則的條件。應用程式將允許啟動使用帶指定核對總和的檔案啟動的程式。
     - **檔案路徑**。將用於建立規則的檔案的路徑設定為觸發應用程式啟動控制允許規則的條件。此時，應用程式將允許啟動使用位於“**設定**”部分的“**為以下資料夾中的應用程式建立允許規則**”表中指定的資料夾中的檔案啟動的程式。
   - **使用 SHA256 雜湊**
   - **為使用者或使用者群組產生規則**。

   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。

5. 在“**排程**”部分中配置工作排程（您可以為除“資料庫更新回溯”以外的所有工作類型配置排程）。

6. 在“**帳戶**”部分中，指定將使用其權限執行工作的帳戶。

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“**內容：<工作名稱>**”視窗中，點擊“**確定**”。
   將儲存新配置的群組工作設定。

透過卡巴斯基安全管理中心配置應用程式啟動控制規則

瞭解如何使用“應用程式啟動控制”工作根據各種條件產生規則清單，或手動建立允許或拒絕規則。

新增應用程式啟動控制規則

要新增應用程式啟動控制規則：

1. 開啟“**應用程式啟動控制規則**”視窗。

2. 點擊“**新增**”按鈕。

3. 在按鈕的內容功能表中，選擇“**新增一項規則**”。
   將開啟“**規則設定**”視窗。

4. 指定以下設定：

a. 在“**名稱**”欄位中，輸入規則的名稱。

b. 在“**類型**”下拉清單中，選擇規則類型：

- **允許**，如果您希望規則根據規則設定中指定的條件允許應用程式啟動。
- **拒絕**，如果您希望規則根據規則設定中指定的條件封鎖應用程式啟動。

c. 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。

d. 在“**使用者或群組**”欄位中，指定根據規則類型將允許或不允許啟動程式的使用者。為此，請執行以下操作：

1. 點擊“**瀏覽**”按鈕。
2. 將開啟標準 Microsoft Windows「選擇使用者或群組」視窗。
3. 指定使用者和/或使用者群組清單。
4. 點擊“確定”。

e. 如果您希望從特定檔案獲取“**規則觸發條件**”部分中列出的規則觸發條件的值：

1. 點擊“**從檔案內容設定規則觸發條件**”按鈕。
   將開啟標準 Microsoft Windows“開啟”視窗。
2. 選擇檔案。
3. 點擊“開啟”按鈕。
   檔案中的條件值顯示在“**規則觸發條件**”部分的欄位中。預設選擇檔案內容中提供有其資料的條件。

f. 在“**規則觸發條件**”部分中，選擇以下選項之一：

- **數位憑證**，如果您希望規則控制使用數位憑證簽章的檔案啟動的應用程式的啟動：
  - 如果您希望規則控制由僅具有指定標題的數位憑證簽章的檔案的啟動，請選中“**使用主旨**”核取方塊。
  - 如果您希望規則僅控制使用具有指定指紋的數位憑證簽章的檔案的啟動，請選中“**使用指紋**”核取方塊。
- **SHA256 雜湊**，如果您希望規則控制使用其核對總和與指定值比對的檔案啟動的程式的啟動。
- **檔案路徑**，如果您希望規則控制使用位於指定路徑的檔案啟動的程式的啟動。

  Kaspersky Embedded Systems Security 無法辨識包含斜線“/”的路徑。請使用反斜線“\”來正確輸入路徑。

指定物件時，可以使用檔案遮罩（透過 ? 和 * 字元）和以下類型的環境變數：%WINDIR%、%SYSTEM32%、%OSDRIVE%、%PROGRAMFILES%。

g. 如果希望新增規則排除：

1. **從規則排除**在「從規則排除」部分中，點擊「新增」按鈕。
   將開啟"**從規則排除**"視窗。
2. 在"**名稱**"欄位中，輸入排除項目的名稱。
3. 指定從應用程式啟動控制規則中排除應用程式檔案的設定。可點擊"**基於檔案內容設定排除**"按鈕從檔案內容填充設定欄位。
   - 數位憑證
   - **使用主旨**
   - **使用指紋**
   - **SHA256 雜湊**
   - **檔案路徑**
4. 點擊"**確定**"。
5. 如有必要，重複步驟 (i)-(iv) 以新增更多排除。

5. 在"**確定**"視窗中點擊"**規則設定**"。

建立的規則顯示在"**應用程式啟動控制規則**"視窗中的清單中。

啟用預設允許模式

"預設允許"模式允許所有應用程式啟動，只要它們未被規則或被 KSN 的不受信任結論封鎖。可以透過新增特定允許規則來啟用預設允許模式。您可以僅為指令碼或為所有可執行檔啟用"預設允許"模式。

要新增預設允許規則：

1. 開啟"**應用程式啟動控制規則**"視窗。
2. 點擊"**新增**"按鈕，然後在該按鈕的內容功能表中選擇"**新增一項規則**"。
   將開啟"**規則設定**"視窗。
3. 在"**名稱**"欄位中，輸入規則的名稱。
4. 在"**類型**"下拉清單中，選擇"**允許**"規則類型。
5. 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。

6. 在“**規則觸發條件**”部分中，選擇“**檔案路徑**”選項。

7. 輸入以下遮罩：**?:**

8. 在“**確定**”視窗中點擊“**規則設定**”。

Kaspersky Embedded Systems Security 將套用預設允許模式。

從卡巴斯基安全管理中心事件建立允許規則

要在“應用程式啟動控制”中從卡巴斯基安全管理中心事件為應用程式建立允許規則：

1. 開啟“**應用程式啟動控制規則**”視窗。

2. 點擊“**新增**”按鈕，然後在該按鈕的內容功能表中選擇“**從卡巴斯基安全管理中心事件為應用程式建立允許規則**”。

3. 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。
   - **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。

   將開啟“**應用程式啟動控制規則產生器**”視窗。

4. 選擇您希望規則產生工作使用的事件類型：

   - **僅統計模式: 應用程式啟動被拒絕**。
   - **應用程式啟動被拒絕**。

5. 從“**請求在該期間內產生的事件**”下拉清單中選擇時間段。

6. 選中或清除“**產生規則時優先使用雜湊**”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。

7. 點擊“**產生規則**”按鈕。

8. 點擊“**應用程式啟動控制規則**”視窗中的“**儲存**”按鈕。

   將使用基於安裝了卡巴斯基安全管理中心管理主控台的受防護裝置的系統資料建立的新規則填充“應用程式啟動控制”工作中的規則清單。

如果政策中已指定應用程式啟動控制規則清單，則 Kaspersky Embedded Systems Security 將從封鎖事件中新增選定的規則到已指定的規則。不新增具有相同雜湊的規則，因為清單中的所有規則都必須是唯一的。

從有關受封鎖應用程式的卡巴斯基安全管理中心報告中匯入規則

您可從在**"僅統計"**模式下執行"應用程式啟動控制"工作後卡巴斯基安全管理中心中建立的報告匯入有關受封鎖應用程式啟動的資料，並使用此資料在所設定政策中建立應用程式啟動控制允許規則清單。

建立有關"應用程式啟動控制"工作期間發生的事件的報告後，您可以跟蹤被封鎖啟動的應用程式。

將資料從有關受封鎖應用程式的報告匯入到政策設定時，確保您所使用的清單僅包含您希望允許啟動的應用程式。

要根據卡巴斯基安全管理中心中的受封鎖應用程式報告為一組受防護裝置指定應用程式啟動控制允許規則：

1. 開啟**"應用程式啟動控制"**視窗。
2. 在**"工作模式"**部分中，選擇**"僅統計"**模式。
3. 在**"事件通知"**部分中的政策內容中，確保：
   - 對於**緊急事件**，**應用程式啟動被拒絕**事件的工作記錄保留期超過以**"僅統計"**模式執行工作的排程期（預設值為 30 天）。
   - 對於重要性等級為**"警告"**的事件，**僅統計模式: 應用程式啟動被拒絕**事件的工作記錄保留期超過以**"僅統計"**模式執行工作的排程期（預設值為 30 天）。

     當事件保留期過後，有關記錄的事件的資訊會被刪除且不會反映在報告檔案中。在**"僅統計"**模式下執行應用程式啟動控制工作之前，確保工作執行時間不超過為指定事件設定的時間段。
4. 當工作完成後，將記錄的事件匯出到 TXT 檔案：
   a. 在卡巴斯基安全管理中心中的**"管理伺服器"**節點的工作區中，選擇**"事件"**標籤。
   b. 點擊**"建立選擇"**按鈕以基於"封鎖"條件建立一系列事件，以檢視"應用程式啟動控制"工作將封鎖啟動的應用程式。
   c. 在所選項的結果窗格中，點擊**"將事件匯出到檔案"**以將受封鎖應用程式啟動報告儲存到 TXT 檔案。

在政策中匯入和應用建立的報告之前，確保報告僅包含有關您希望允許啟動的應用程式的資料。

5. 將有關受封鎖應用程式啟動的資料匯入到應用程式啟動控制工作。為此，在政策內容的"應用程式啟動控制"工作設定中：
   a. 在**"一般"**標籤上，點擊**"規則清單"**按鈕。
   將開啟**"應用程式啟動控制規則"**視窗。

b. 點擊**"新增"**按鈕，然後在該按鈕的內容功能表中選擇**"從卡巴斯基安全管理中心報告匯入封鎖的應用程式的資料"**。

c. 選擇將來自根據卡巴斯基安全管理中心報告建立的清單的規則新增到先前設定的應用程式啟動控制規則清單的政策：

- **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。
- **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。

d. 在開啟的標準 Microsoft Windows 視窗中，選擇已將來自受封鎖應用程式啟動報告的事件匯出到的 TXT 檔案。

e. 點擊**"應用程式啟動控制規則"**視窗中的**"儲存"**。

根據有關受封鎖應用程式的卡巴斯基安全管理中心報告建立的規則將被新增到應用程式啟動控制規則清單。

從 XML 設定檔匯入應用程式啟動控制規則

您可匯入由"應用程式啟動控制規則產生器"群組工作建立的報告，並將它們作為允許規則清單套用於所設定的政策中。

當"應用程式啟動控制規則產生器"群組工作完成後，應用程式會將建立的允許規則匯入指定的共用資料夾中儲存的 XML 檔案。包含規則清單的每個檔案透過對公司網路中每台單獨受防護裝置上執行的檔案和啟動的應用程式進行分析所建立。這些清單包含類型與"應用程式啟動控制規則產生器"群組工作中指定的類型比對的檔案和應用程式的允許規則。

要根據自動建立的允許規則清單為一組受防護裝置指定應用程式啟動控制允許規則：

1. 在所設定受防護裝置群組的詳細資訊窗格中的**"工作"**標籤上，建立一個"應用程式啟動控制規則產生器"群組工作或選擇一個現有工作。
2. 在建立的"應用程式啟動控制規則產生器"群組工作的內容中或在工作精靈中，指定以下設定：

- 在**"通知"**部分中，設定用於儲存工作執行報告的設定。

  有關此節中配置設定的詳細說明，請參見 *卡巴斯基安全管理中心說明*。

- 在**"設定"**部分中，指定所建立規則將允許啟動的應用程式類型。您可編輯包含允許的應用程式的資料夾集合：從工作範圍排除預設資料夾或手動新增新資料夾。
- 在**"選項"**部分中，指定工作在執行時及完成後執行的操作。指定規則建立條件和建立的規則將匯出到的檔案的名稱。
- 在**"排程"**部分中設定工作啟動排程設定。
- 在**"帳戶"**部分中，指定將用於執行工作的使用者帳戶。
- 在**"工作範圍的排除項目"**部分中，指定要從工作範圍排除的受防護裝置群組。

Kaspersky Embedded Systems Security 不會為在排除的受防護裝置上啟動的應用程式建立允許規則。

3. 在所配置受防護裝置群組的詳細資訊窗格上的"**工作**"標籤上，從群組工作清單中選擇您已建立的"應用程式啟動控制規則產生器"工作，然後點擊"**啟動**"按鈕啟動工作。

   工作完成後，自動建立的允許規則清單將儲存在共用資料夾中的 XML 檔案中。

   在網路中使用"應用程式啟動控制"工作之前，請確保所有受防護裝置都能夠存取共用資料夾。如果組織的政策未規定使用網路中的共用資料夾，建議在測試受防護裝置群組中的受防護裝置或參考電腦上啟動"應用程式啟動控制規則產生器"工作。

4. 要將建立的允許規則清單新增到"應用程式啟動控制"工作：

   a. 開啟"**應用程式啟動控制規則**"視窗。

   b. 點擊"**新增**"按鈕，然後在開啟的清單中選擇"**從 XML 檔案匯入規則**"。

   c. 選擇將自動建立的允許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。
      - **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。

   d. 在開啟的標準 Microsoft Windows 視窗中，選擇"應用程式啟動控制規則產生器"群組工作完成後建立的 XML 檔案。

   e. 點擊"**應用程式啟動控制規則**"視窗中的"**儲存**"。

5. 如果您希望將建立的規則套用於控制應用程式啟動，則在政策中的"應用程式啟動控制"工作內容中，為工作選擇"**啟動**"模式。

基於每台單獨的受防護裝置上的工作執行自動建立的允許規則將被套用於所設定政策涵蓋的所有網路受防護裝置。在這些受防護裝置上，應用程式將允許僅啟動已為其建立允許規則的這些應用程式。

檢查應用程式啟動

在套用所配置的應用程式啟動控制規則前，您可以測試任何應用程式以確定該應用程式會觸發哪些應用程式啟動控制規則。

預設情況下，Kaspersky Embedded Systems Security 將拒絕啟動不被單個規則允許啟動的應用程式。為避免拒絕啟動重要的應用程式，您需要為它們建立允許規則。

如果某個應用程式的啟動受多條不同類型的規則控制，拒絕規則將優先：即使應用程式只在一條拒絕規則下，也將拒絕該應用程式啟動。

要測試應用程式啟動控制規則：

1. 開啟"**應用程式啟動控制規則**"視窗。
2. 在開啟的視窗中，點擊"**顯示檔案規則**"按鈕。

將開啟標準的 Microsoft Windows 視窗。

3. 選擇要測試其啟動控制的檔案。

指定檔案的路徑顯示在搜尋欄位中。清單包含在啟動所選檔案時將觸發的所有規則。

建立“應用程式啟動控制規則產生器”工作

要建立和配置“應用程式啟動控制規則產生器”工作設定：

1. 開啟“新建工作精靈”中的“**設定**”視窗。
2. 進行以下設定：
   - 指定規則名稱的前置詞。
   - 配置允許規則使用範圍。
3. 點擊“下一步”。
4. 指定 Kaspersky Embedded Systems Security 必須執行的操作：
   - 建立允許規則時。
   - 工作完成後。
5. 在“**排程**”視窗中，設定排程的工作啟動設定。
6. 點擊“下一步”。
7. 在“選擇帳戶以執行工作”視窗中，指定要使用的帳戶。
8. 點擊“下一步”。
9. 指定工作名稱。
10. 點擊“下一步”。

> 工作名稱不應超過 100 個字元，並且不能包含以下符號：" * < > & \ : |

將開啟“完成建立工作”視窗。

11. 您可以透過選中“精靈完成後執行工作”核取方塊來在精靈完成後執行工作。
12. 點擊“完成”完成建立工作。

要在卡巴斯基安全管理中心中設定現有規則，

應用程式啟動控制規則產生器開啟“內容：應用程式啟動控制規則產生器”視窗並調整上述設定。

有關設定修改日期和時間以及修改前後工作設定值的資訊儲存在系統稽核記錄中。

限制工作使用範圍

要限制"應用程式啟動控制規則產生器"工作的範圍：

1. 打开**"屬性：應用程式啟動控制規則產生器"**窗口。
2. 選擇如何建立允許規則：
   - **基於正在執行的應用程式建立允許規則**
   - **為資料夾中的應用程式建立允許規則**
3. 點擊"確定"。

將儲存指定設定。

自動規則產生期間要執行的操作

要配置在"應用程式啟動控制規則產生器"工作執行期間 Kaspersky Embedded Systems Security 要執行的操作：

1. 打开**"屬性：應用程式啟動控制規則產生器"**窗口。
2. 開啟**"選項"**標籤。
3. 在**"產生允許規則時"**部分中，配置以下設定：
   - **使用數位憑證**
   - **使用數位憑證主旨和指紋**
   - **憑證遺失則使用**
     - **SHA256 hash**.將用於建立規則的檔案的核對總和設定為觸發應用程式啟動控制允許規則的條件。應用程式將允許啟動使用帶指定核對總和的檔案啟動的程式。
     - **檔案路徑**。將用於建立規則的檔案的路徑設定為觸發應用程式啟動控制允許規則的條件。此時，應用程式將允許啟動使用位於**"設定"**部分的**"為以下資料夾中的應用程式建立允許規則"**表中指定的資料夾中的檔案啟動的程式。
   - **使用 SHA256 雜湊**
   - **為使用者或使用者群組產生規則**。
4. 點擊**"確定"**。

將儲存指定設定。

自動規則產生完成後要執行的操作

要配置在"應用程式啟動控制規則產生器"工作完成後 Kaspersky Embedded Systems Security 要執行的操作：

1. 打开**"屬性：應用程式啟動控制規則產生器"**窗口。
2. 開啟**"選項"**標籤。
3. 在**"工作完成後"**部分中，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**。
   - **將電腦詳細資訊新增到檔案名稱**。
4. 點擊"確定"。

   將儲存指定設定。

透過應用程式主控台管理應用程式啟動控制

在本節中，學習如何導航應用程式主控台介面以及如何在受防護裝置上配置工作設定。

導航

瞭解如何透過所選介面導航到所需工作設定。

開啟"應用程式啟動控制"工作設定

要透過應用程式主控台開啟"應用程式啟動控制"一般工作設定：

1. 在應用程式主控台樹狀目錄中，展開**"電腦控制"**節點。
2. 選擇**"應用程式啟動控制"**子節點。
3. 在**應用程式啟動控制**子節點的詳細資訊視窗中，點擊**內容**連結。
   將開啟**"工作設定"**視窗。

開啟應用程式啟動控制規則視窗

要透過應用程式主控台開啟應用程式啟動控制規則清單：

1. 在應用程式主控台樹狀目錄中，展開**"電腦控制"**節點。
2. 選擇**"應用程式啟動控制"**子節點。
3. 在**"應用程式啟動控制"**節點的結果窗格中，點擊**"應用程式啟動控制規則"**連結。

將開啟**"應用程式啟動控制規則"**視窗。

4. 根據需要設定規則清單。

開啟"應用程式啟動控制規則產生器"工作設定

要配置"應用程式啟動控制規則產生器"工作：

1. 在應用程式主控台樹狀目錄中，展開**"自動規則產生器"**節點。
2. 選擇**"應用程式啟動控制規則產生器"**子節點。
3. 在**"應用程式啟動控制規則產生器"**子節點的結果窗格中，點擊**"內容"**連結。
   將開啟**"工作設定"**視窗。
4. 根據需要配置工作。

配置"應用程式啟動控制"工作設定

要配置一般"應用程式啟動控制"工作設定：

1. 開啟**"工作設定"**視窗。
2. 配置以下工作設定：
   - 在**"一般"**標籤上：
     - "应應用程式啟動控制"工作模式。
     - 工作中的規則使用範圍。
     - KSN 使用。
   - **軟體分發控制**頁籤上的軟體發佈控制設定。
   - **排程**和**進階**頁籤上的工作啟動排程設定。
3. **工作設定**在工作設定視窗中點擊確定。
   將儲存修改的設定。

Kaspersky Embedded Systems Security 將對正在執行的工作立即套用新設定。有關設定修改日期和時間以及修改前後工作設定值的資訊儲存在系統稽核記錄中。

選擇"應用程式啟動控制"工作的模式

要配置"應用程式啟動控制"工作的模式：

1. 開啟“**工作設定**”視窗。
2. 在“**一般**”標籤上的“**工作模式**”下拉清單中，指定工作模式。
3. 清除或選中“**為檔案隨後的所有啟動重複執行該檔案第一次啟動時的操作**”核取方塊。

   每次修改“應用程式啟動控制”工作設定後，Kaspersky Embedded Systems Security 都會建立一個新的快取事件清單。這意味著“應用程式啟動控制”按照目前安全設定執行。

4. 清除或選中“**在沒有可執行的指令時拒絕指令解釋器啟動**”。
5. 在**工作設定**視窗中點擊**確定**。

將儲存指定設定。

所有啟動應用程式的嘗試都將記錄在工作記錄中。

配置“應用程式啟動控制”工作的範圍

要定義“應用程式啟動控制”工作的範圍：

1. 開啟“**工作設定**”視窗。
2. 在“**一般**”標籤上的“**規則使用範圍**”部分中，指定以下設定：
   - **將規則套用於可執行檔**
   - **監控 DLL 模組的載入**

     控制 DLL 模組的載入可能影響作業系統的效能。

   - **將規則套用於指令碼和 MSI 資料套件**
3. 在**工作設定**視窗中點擊**確定**。

將儲存指定設定。

配置 KSN 使用

要配置“應用程式啟動控制”工作的 KSN 服務的使用：

1. 開啟“**工作設定**”視窗。
2. 在“**一般**”標籤上的“**KSN 使用**”部分中，指定 KSN 服務的使用設定：
   - 如果必要，請選中“**拒絕 KSN 不信任的應用程式**”核取方塊。

- 如果必要，請選中“**允許 KSN 信任的應用程式**”核取方塊。
- 如果選擇了“**允許 KSN 信任的應用程式**”核取方塊，則請指定可以在 KSN 中啟動應用程式的使用者和/或使用者群組。為此，請執行以下操作：

  a. 點擊“**編輯**”按鈕。

  將開啟標準的 Microsoft Windows“**選擇使用者或群組**”視窗。

  > 預設情況下，所有使用者都可以存取受 KSN 信任的程式。

  b. 指定使用者和/或使用者群組清單。

  c. 點擊“**確定**”。

3. 在**工作設定**視窗中點擊**確定**。

將儲存指定設定。

軟體分發控制

要新增受信任分發套件：

1. 開啟“**工作設定**”視窗。
2. 在“**軟體分發控制**”標籤上，選中“**自動允許透過所列應用程式和資料套件分發軟體**”核取方塊。

> 如果在“**自動允許透過所列應用程式和資料套件分發軟體**”工作設定中選中“**將規則套用於可執行檔**”標籤中的“**一般**”核取方塊，則您可選中“**應用程式啟動控制**”。

3. 根據需要清除“**始終允許透過 Windows Installer 進行軟體分發**”核取方塊。

> 僅當在絕對必要時才建議清除“**始終允許透過 Windows Installer 進行軟體分發**”核取方塊。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。

4. 如果需要，請選擇“**始終允許使用背景智慧傳輸服務透過 SCCM 進行軟體分發**”核取方塊。

> 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應用程式之前已執行分發的任何階段，則應用程式不會控制過程。

5. 要編輯受信任分發套件的清單，請點擊“**變更分發套件清單**”，然後在開啟的視窗中選擇以下方法之一：

- **新增一個分發套件**。

  a. 點擊“**瀏覽**”按鈕。

  b. 選擇可執行檔或分發套件。

  “**信任條件**”部分會使用有關選定檔案的資料自動進行填充。

c. 清除或選中**"允許進一步分發套件透過此分法套件建立的程式"**核取方塊。

d. 選擇兩個可用條件選項中的一個，用於決定檔案或安裝套件是否受信任：

- **使用數位憑證**
- **使用 SHA256 雜湊**

- **按雜湊新增多個分發套件**。

  您可以選擇無限數量的可執行檔和分發套件，並同時將它們新增到清單。Kaspersky Embedded Systems Security 將檢查雜湊並允許作業系統啟動指定的檔案。

- **變更選定的分發套件**。
  使用此選項可以選擇不同的可執行檔或分發套件，或變更信任條件。

- **從檔案匯入分發套件清單**。
  在**"開啟"**視窗中，指定包含受信任分發套件清單的設定檔。

6. 如果要刪除受信任清單中以前新增的應用程式或分發套件，請點擊**"刪除分發套件"**按鈕。將允許執行擷取的檔案。

   要封鎖擷取的檔案啟動，請在受防護裝置上移除應用程式，或在應用程式啟動控制工作設定中建立拒絕規則。

7. 點擊**"確定"**。

將儲存新配置的設定。

配置應用程式啟動控制規則

瞭解如何使用"應用程式啟動控制"工作產生、匯入和匯出規則清單，或手動建立允許或拒絕規則。

新增應用程式啟動控制規則

要新增應用程式啟動控制規則：

1. 開啟**"應用程式啟動控制規則"**視窗。
2. 點擊**"新增"**按鈕。
3. 在按鈕的內容功能表中，選擇**"新增一項規則"**。
   將開啟**"規則設定"**視窗。
4. 指定以下設定：

   a. 在**"名稱"**欄位中，輸入規則的名稱。

b. 在**"類型"**下拉清單中，選擇規則類型：

- **允許**，如果您希望規則根據規則設定中指定的條件允許應用程式啟動。
- **拒絕**，如果您希望規則根據規則設定中指定的條件封鎖應用程式啟動。

c. 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。

d. 在**"使用者或群組"**欄位中，指定根據規則類型將允許或不允許啟動程式的使用者。為此，請執行以下操作：

1. 點擊**"瀏覽"**按鈕。
2. 將開啟標準 Microsoft Windows「選擇使用者或群組」視窗。
3. 指定使用者和/或使用者群組清單。
4. 點擊"確定"。

e. 如果您希望從特定檔案獲取**"規則觸發條件"**部分中列出的規則觸發條件的值：

1. 點擊**"從檔案內容設定規則觸發條件"**按鈕。
   將開啟標準 Microsoft Windows"開啟"視窗。
2. 選擇檔案。
3. 點擊"開啟"按鈕。
   檔案中的條件值顯示在**"規則觸發條件"**部分的欄位中。預設選擇檔案內容中提供有其資料的條件。

f. 在**"規則觸發條件"**部分中，選擇以下選項之一：

- **數位憑證**，如果您希望規則控制使用數位憑證簽章的檔案啟動的應用程式的啟動：
  - 如果您希望規則控制由僅具有指定標題的數位憑證簽章的檔案的啟動，請選中**"使用主旨"**核取方塊。
  - 如果您希望規則僅控制使用具有指定指紋的數位憑證簽章的檔案的啟動，請選中**"使用指紋"**核取方塊。
- **SHA256 雜湊**，如果您希望規則控制使用其核對總和與指定值比對的檔案啟動的程式的啟動。
- **檔案路徑**，如果您希望規則控制使用位於指定路徑的檔案啟動的程式的啟動。

  Kaspersky Embedded Systems Security 無法辨識包含斜線"/"的路徑。請使用反斜線"\"來正確輸入路徑。

  指定物件時，可以使用檔案遮罩（透過 ? 和 * 字元）和以下類型的環境變數：%WINDIR%、%SYSTEM32%、%OSDRIVE%、%PROGRAMFILES%。

g. 如果希望新增規則排除：

1. **從規則排除**在「從規則排除」部分中，點擊「新增」按鈕。

   將開啟**"從規則排除"**視窗。

2. 在**"名稱"**欄位中，輸入排除項目的名稱。

3. 指定從應用程式啟動控制規則中排除應用程式檔案的設定。可點擊**"基於檔案內容設定排除"**按鈕從檔案內容填充設定欄位。

   - **數位憑證**
   - **使用主旨**
   - **使用指紋**
   - **SHA256 雜湊**
   - **檔案路徑**

4. 點擊**"確定"**。

5. 如有必要，重複步驟 (i)-(iv) 以新增更多排除。

5. 在**"確定"**視窗中點擊**"規則設定"**。

建立的規則顯示在**"應用程式啟動控制規則"**視窗中的清單中。

啟用預設允許模式

"預設允許"模式允許所有應用程式啟動，只要它們未被規則或被 KSN 的不受信任結論封鎖。可以透過新增特定允許規則來啟用預設允許模式。您可以僅為指令碼或為所有可執行檔啟用"預設允許"模式。

要新增預設允許規則：

1. 開啟**"應用程式啟動控制規則"**視窗。

2. 點擊**"新增"**按鈕。

3. 在按鈕的內容功能表中，選擇**"新增一項規則"**。

   將開啟**"規則設定"**視窗。

4. 在**"名稱"**欄位中，輸入規則的名稱。

5. 在**"類型"**下拉清單中，選擇**"允許"**規則類型。

6. 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。

7. 在**"規則觸發條件"**部分中，選擇**"檔案路徑"**選項。

8. 輸入以下遮罩：`?:\`

9. 在“**確定**”視窗中點擊“**規則設定**”。

Kaspersky Embedded Systems Security 將套用預設允許模式。

根據“應用程式啟動控制”工作事件建立允許規則

要建立包含根據“應用程式啟動控制”工作事件產生的允許規則的設定檔：

1. 以“**僅統計**”模式啟動“應用程式啟動控制”工作，以便在工作記錄中記錄有關受防護裝置上的所有應用程式啟動的資訊。

2. 當工作在“**僅統計**”模式下執行完成後，透過點擊“**開啟工作記錄**”節點詳細資訊窗格的“**管理**”部分中的“**應用程式啟動控制**”按鈕，開啟工作記錄。

3. 在“**記錄**”視窗中，點擊“**基於事件建立規則**”。

Kaspersky Embedded Systems Security 將會建立一個 XML 設定檔，其中包含基於“**僅統計**”模式下的“應用程式啟動控制”工作事件的規則清單。您可以在“應用程式啟動控制”工作中套用此清單。

在應用根據記錄的工作事件建立的規則清單前，建議檢視並手動處理清單，以確定指定規則允許關鍵檔案（例如系統檔案）啟動。

無論工作模式如何，所有工作事件都將記錄在工作記錄中。您可以根據當工作在“**活動**”模式下執行時所建立的記錄來產生包含規則清單的設定檔。除了緊急情況外，不建議使用此方案，因為在“**活動**”模式下執行工作前必須產生最終規則清單才能使其生效。

匯出應用程式啟動控制規則

要將應用程式啟動控制規則匯出到設定檔：

1. 開啟“**應用程式啟動控制規則**”視窗。

2. 點擊“**匯出至檔案**”按鈕。

將開啟標準的 Microsoft Windows 視窗。

3. 在開啟的視窗中，指定想要將規則匯出到其中的檔案。如果不存在此類檔案，則將建立它。如果具有指定名稱的檔案已存在，其內容在規則匯出後將被覆蓋。

4. 點擊“**儲存**”按鈕。

規則設定將匯出到指定檔案。

從 XML 設定檔匯入應用程式啟動控制規則

要匯入應用程式啟動控制規則：

1. 開啟“**應用程式啟動控制規則**”視窗。

2. 點擊**"新增"**按鈕。

3. 在按鈕的內容功能表中，選擇**"從 XML 檔案匯入規則"**。

4. 指定新增匯入規則的方法。要執行此操作，請從**"從 XML 檔案匯入規則"**按鈕的內容功能表中選擇一個選項：

   - **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。
   - **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。

   將開啟標準 Microsoft Windows**"開啟"**視窗。

5. 在**"開啟"**視窗中，選擇包含應用程式啟動控制規則的 XML 檔案。

6. 點擊**"開啟"**按鈕。

匯入的規則將顯示在**"應用程式啟動控制規則"**視窗中的清單中。

刪除應用程式啟動控制規則

要刪除應用程式啟動控制規則：

1. 開啟**"應用程式啟動控制規則"**視窗。

2. 在清單中，選擇要刪除的一項或多項規則。

3. 點擊**"刪除選取的項目"**按鈕。

4. 點擊**"儲存"**按鈕。

將刪除所選應用程式啟動控制規則。

配置"應用程式啟動控制規則產生器"工作

要配置"應用程式啟動控制規則產生器"工作設定：

1. 開啟**應用程式啟動控制規則產生器**的**工作設定**視窗。

2. 配置以下設定：

   - 在**"一般"**標籤上：
     - 指定**規則名稱前置詞**。
     - 配置允許規則使用範圍。
   - 在**"操作"**標籤上，指定 Kaspersky Embedded Systems Security 必須執行的操作。
   - 在**"排程"**和**"進階"**標籤上，配置排程工作啟動設定。

- 在**"執行帳戶"**標籤上，配置使用帳戶權限的工作啟動設定。

3. 在**工作設定**視窗中點擊**確定**。

Kaspersky Embedded Systems Security 將對正在執行的工作立即套用新設定。有關設定修改日期和時間以及修改前後工作設定值的資訊。

限制工作使用範圍

要限制"應用程式啟動控制規則產生器"工作的範圍：

1. 開啟**應用程式啟動控制規則產生器**的**工作設定**視窗。
2. 選擇如何建立允許規則：
   - **基於正在執行的應用程式建立允許規則**。
   - **為以下資料夾中的應用程式建立允許規則**。
3. 在**工作設定**視窗中點擊**確定**。

將儲存指定設定。

自動規則產生期間要執行的操作

要配置 Kaspersky Embedded Systems Security 在"應用程式啟動控制規則產生器"工作執行時和完成後執行的操作：

1. 開啟**應用程式啟動控制規則產生器**的**工作設定**視窗。
2. 開啟**"選項"**標籤。
3. 在**"產生允許規則時"**部分中，配置以下設定：
   - **使用數位憑證**
   - **使用數位憑證主旨和指紋**
   - **憑證遺失則使用**
     - **SHA256 hash**.將用於建立規則的檔案的核對總和設定為觸發應用程式啟動控制允許規則的條件。應用程式將允許啟動使用帶指定核對總和的檔案啟動的程式。
     - **檔案路徑**。將用於建立規則的檔案的路徑設定為觸發應用程式啟動控制允許規則的條件。此時，應用程式將允許啟動使用位於**"設定"**部分的**"為以下資料夾中的應用程式建立允許規則"**表中指定的資料夾中的檔案啟動的程式。
   - **使用 SHA256 雜湊**
   - **為使用者或使用者群組產生規則**。

4. 在**"工作完成後"**部分中，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**。
   - **將電腦詳細資訊新增到檔案名稱**。

5. 在**工作設定**視窗中點擊**確定**。

將儲存指定設定。

自動規則產生完成後要執行的操作

要配置在"應用程式啟動控制規則產生器"工作完成後 Kaspersky Embedded Systems Security 要執行的操作：

1. 開啟**應用程式啟動控制規則產生器**的**工作設定**視窗。
2. 開啟**"選項"**標籤。
3. 在**"工作完成後"**部分中，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**。
   - **將電腦詳細資訊新增到檔案名稱**。

4. 在**工作設定**視窗中點擊**確定**。

將儲存指定設定。

透過 Web 外掛程式管理應用程式啟動控制

要透過 Web 外掛程式管理"應用程式啟動控制"工作：

1. 在 Web 控制的主視窗中，選取**裝置 → 政策和設定檔案**。
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"**標籤。
4. 選擇**"本機活動控制"**部分。
5. 點擊**"設定"**子區段中的**"應用程式啟動控制"**。
6. 按下表所述配置設定。

"應用程式啟動控制"工作設定

設定	敘述
工作模式	在此下拉清單中，可選擇"應用程式啟動控制"工作的模式： • **啟動**。Kaspersky Embedded Systems Security 使用指定的規則控制任何應用程式的啟動。 • **僅統計**。Kaspersky Embedded Systems Security 不使用指定的規則控制應用程式啟動。相反，它僅在工作記錄中記錄有關啟動事件的資訊。所有應用程式均允許啟動。您可以使用此模式根據工作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。 預設情況下，"應用程式啟動控制"工作在"**僅統計**"模式下執行。
為檔案隨後的所有啟動重複執行該檔案第一次啟動時的操作	此核取方塊用於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。 如果選中此核取方塊，Kaspersky Embedded Systems Security 將根據工作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。 如果清除該核取方塊，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。 預設取消選定該核取方塊。
在沒有可執行的指令時拒絕指令解釋器啟動	如果選中該核取方塊，Kaspersky Embedded Systems Security 將拒絕命令列編譯器啟動，即使允許編譯器啟動。只有同時滿足以下兩個條件時，才能在沒有指令的情況下啟動命令列編譯器： • 允許命令列編譯器啟動。 • 要執行的指令獲得允許。 如果清除該核取方塊，Kaspersky Embedded Systems Security 在啟動命令列編譯器時只考慮允許規則。如果未套用任何允許規則或可執行處理程序不受 KSN 信任，啟動將被拒絕。如果套用了允許規則或處理程序受 KSN 信任，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 可辨識以下命令列編譯器： • cmd.exe • powershell.exe • python.exe • perl.exe 預設取消選定該核取方塊。
將規則套用於可執行檔	該核取方塊用於啟用或停用可執行檔的啟動控制。 如果選中此核取方塊，則 Kaspersky Embedded Systems Security 將使用指定的規則（其設定指定**可執行檔**為範圍）允許或封鎖程式可執行檔的啟動。 如果清除此核取方塊，則 Kaspersky Embedded Systems Security 不使用指定的規則控制程式可執行檔的啟動。將允許可執行檔啟動。 預設將會選定該核取方塊。
監控 DLL 模組的載入	該核取方塊用於啟用或停用 DLL 模組的載入控制。

	如果選中此核取方塊，則 Kaspersky Embedded Systems Security 將使用指定的規則（其設定將**可執行檔**指定為範圍）允許或封鎖 DLL 模組的載入。 如果清除此核取方塊，則 Kaspersky Embedded Systems Security 不使用指定的規則控制 DLL 模組的載入。將允許 DLL 模組載入。 如果選中**"將規則套用於可執行檔"**核取方塊，則此核取方塊處於啟動狀態。 預設將會選定該核取方塊。
將規則套用於指令碼和 MSI 資料套件	此核取方塊用於啟用或停用指令碼和 MSI 資料套件的啟動。 如果選中此核取方塊，Kaspersky Embedded Systems Security 將使用指定的規則（其設定將指令碼和 MSI 資料套件指定為範圍）允許或封鎖指令碼和 MSI 資料套件啟動。 如果清除此核取方塊，則 Kaspersky Embedded Systems Security 不使用指定的規則控制指令碼和 MSI 資料套件的啟動。將允許指令碼和 MSI 資料套件的啟動。 預設將會選定該核取方塊。
拒絕 KSN 不信任的應用程式	此核取方塊用於啟用或停用根據 KSN 中的應用程式聲譽資料進行應用程式啟動控制。 如果選中此核取方塊，則 Kaspersky Embedded Systems Security 將封鎖任何在 KSN 中不受信任的應用程式執行。適用於在 KSN 中不受信任的應用程式的應用程式啟動控制允許規則不會被觸發。選中此核取方塊將會提供額外的惡意軟體防護。 如果清除此核取方塊，則 Kaspersky Embedded Systems Security 將不考慮 KSN 中不受信任的應用程式的聲譽，並根據適用於此類應用程式的規則允許或封鎖啟動。 預設取消選定該核取方塊。
允許 KSN 信任的應用程式	此核取方塊用於啟用或停用根據 KSN 中的應用程式聲譽資料進行應用程式啟動控制。 如果選中此核取方塊，則 Kaspersky Embedded Systems Security 將允許在 KSN 中受到信任的應用程式執行。適用於 KSN 信任的應用程式的拒絕應用程式啟動控制規則具有更高優先順序：如果某個應用程式受到 KSN 服務信任，應用程式啟動將被拒絕。 如果清除此核取方塊，則 Kaspersky Embedded Systems Security 將不考慮 KSN 信任的應用程式的聲譽，並根據適用於此類應用程式的規則允許或拒絕啟動。 預設取消選定該核取方塊。
允許執行 KSN 信任的應用程式的使用者和/或使用者群組	如果選取**允許 KSN 信任的應用程式**核取方塊，則可以在此處指定允許啟動 KSN 信任的應用程式的使用者和使用者群組。 By default, the following users are specified: **所有人** and **NT AUTHORITY\SYSTEM**.
規則	為"應用程式啟動控制"工作設定允許或拒絕規則。
軟體分發控制	您可以新增受信任分發套件。
工作管理	您可以配置按排程啟動工作的設定。

裝置控制

本節包含有關"裝置控制"工作以及如何設定的資訊。

關於裝置控制工作

Kaspersky Embedded Systems Security 控制外部裝置和 CD/DVD 磁碟機的註冊和使用，以防護裝置免受電腦安全性威脅的侵害，與快閃記憶體磁碟機或透過 USB 連線的其他類型的外部裝置進行檔案交換的過程中可能出現這些威脅。

Kaspersky Embedded Systems Security 控制以下 USB 外部裝置連線：

- USB 連線的快閃記憶體磁碟機
- CD/DVD ROM 磁碟機
- USB 連線的軟碟磁碟機
- USB 連線的網路介面卡
- USB 連線的 MTP 行動裝置

Kaspersky Embedded Systems Security 會通知您透過 USB 連線的所有裝置，並在工作和事件記錄中記錄相應事件。事件詳細資訊包括裝置類型和連線路徑。"裝置控制"工作啟動後，Kaspersky Embedded Systems Security 將檢查並列出透過 USB 連線的所有裝置。您可以在卡巴斯基安全管理中心通知設定部分中配置通知。

"裝置控制"工作監控外部裝置透過 USB 連線到受防護裝置的所有連線嘗試，如果沒有此類裝置的允許規則，則封鎖連線。封鎖連線後，裝置將無法使用。

應用程式為每個連線的外部裝置規定了以下狀態之一：

- *受信任*。您想允許其進行檔案交換的裝置。產生規則清單後，*裝置實例路徑*值將包含在至少一個規則的使用範圍中。
- *不受信任*。您想限制其進行檔案交換的裝置。裝置實例路徑不會包含在任何允許規則的使用範圍中。

您可以使用"裝置控制規則產生器"工作為外部裝置建立允許規則，以允許資料交換。您還可以延伸已指定規則的使用範圍。不能手動建立允許規則。

Kaspersky Embedded Systems Security 使用"裝置實例路徑"值標識在系統中註冊的外部裝置。裝置實例路徑是專門為每個外部裝置指定的預設功能。將在每個外部裝置的 Windows 內容中為其指定"裝置實例路徑"值，並且該值將在產生規則期間由 Kaspersky Embedded Systems Security 自動確定。

裝置控制工作可在兩種模式下執行：

- **活動**。Kaspersky Embedded Systems Security 會將規則套用於控制快閃記憶體磁碟機和其他外部裝置的連線，並根據預設拒絕政策和指定允許規則允許或封鎖使用所有裝置。允許使用受信任外部裝置。預設情況下，封鎖使用不受信任的外部裝置。

如果當"裝置控制"工作在**活動**模式下執行前您認為不受信任的外部裝置連線到受防護裝置，應用程式不會封鎖該裝置。建議您手動斷開不信任裝置或重新啟動受防護裝置。否則，不會將"預設拒絕"原則套用於裝置。

- **僅統計**。Kaspersky Embedded Systems Security 不會控制快閃記憶體磁碟機和其他外部裝置的連線，但僅記錄有關外部裝置在受防護裝置上的連接和註冊，以及有關相連裝置觸發的裝置控制允許規則的資訊。允許使用所有外部裝置。預設設定此模式。

  您可以基於工作執行期間記錄的有關封鎖裝置的資訊對規則產生套用此模式。

關於裝置控制規則

對於 MTP 連線的行動裝置，Kaspersky Embedded Systems Security 不會套用允許規則。

如果目前連線到或曾經連線到受防護裝置的每台裝置的資訊儲存在系統登錄檔中，將為每台裝置建立具有唯一性的規則。

要產生裝置控制的允許規則：

- 套用"裝置控制規則產生器"工作。
- 以"僅統計"模式執行裝置控制工作。
- 應用有關之前連線的裝置的系統資訊。
- 延伸已指定規則的使用範圍。

Kaspersky Embedded Systems Security 支援的裝置控制規則的最大數量為 3072。

下文介紹了裝置控制規則。

規則類型

規則類型允許為*允許*。如果快閃記憶體磁碟機和其他外部裝置不包含在任何允許規則的使用範圍內，預設情況下，裝置控制工作會封鎖所有這些裝置連線。

觸發條件和規則使用範圍

裝置控制規則基於*裝置實例路徑*識別快閃記憶體磁碟機和其他外部裝置。裝置實例路徑是裝置建立連接並註冊為外部裝置或 CD/DVD 光碟機（例如，IDE 或 SCSI）時系統分配給裝置的唯一條件。

無論用於連線的匯流排如何，Kaspersky Embedded Systems Security 都控制 CD/DVD 磁碟機的連線。當透過 USB 安裝此類裝置時，作業系統會註冊兩個裝置實例路徑值：針對外部裝置和針對 CD/DVD 光碟機（例如，IDE 或 SCSI）。要直接連接此類裝置，必須設定每個實例路徑值的允許規則。

Kaspersky Embedded Systems Security 自動定義裝置實例路徑並將獲取的值解析為以下元素：

- 裝置製造商 (VID)
- 裝置控制器類型 (PID)
- 裝置序號

您不能手動設定裝置實例路徑。允許規則觸發條件定義規則使用範圍。預設情況下，新建立的規則使用範圍包括一台初始裝置，具體是哪台裝置取決於 Kaspersky Embedded Systems Security 基於哪台裝置的內容建立該規則。您可以配置建立的規則設定中的值並使用遮罩延伸規則使用範圍。

初始裝置值

Kaspersky Embedded Systems Security 用於建立允許規則以及在 Windows 裝置管理器中為每台連線的裝置顯示的裝置內容。

初始裝置值包含以下資訊：

- **裝置實例路徑**。Kaspersky Embedded Systems Security 根據此內容定義規則觸發條件並填寫以下欄位：**"製造商 (VID)"**視窗的**"控制器類型 (PID)"**部分中的**"序號"**、**"規則使用範圍"**和**"規則內容"**。
- **易記名稱**。裝置製造商在裝置內容中設定的明確名稱。

Kaspersky Embedded Systems Security 會在建立規則時自動定義初始裝置值。以後您可以使用這些值識別產生規則時所依據的裝置。初始裝置值無法編輯。

敘述

您可以在**"描述"**欄位中為建立的每個裝置控制規則新增更多資訊，例如，您可以記錄所連線的快閃記憶體磁碟機的名稱或定義其擁有者。敘述顯示在**"裝置控制規則"**視窗內的相應圖表中。

敘述和初始設定值不用於觸發規則，只為了說明使用者識別裝置。

關於裝置控制規則產生

您可以從在"裝置控制"或"裝置控制規則產生器"工作執行期間自動建立的 XML 檔案匯入裝置控制允許規則。

預設情況下，如果任何快閃記憶體磁碟機或其他外部裝置不包含在指定的裝置控制規則的使用範圍內，Kaspersky Embedded Systems Security 會限制這些裝置的連線。

裝置控制規則建立目標和方案

規則建立方案	目標
裝置控制規則產生器工作	• 在裝置控制工作第一次啟動之前，為之前連接受信任裝置新增允許規則。 • 為受防護裝置網路中的受信任裝置產生規則清單。
基於系統資料的規則產生	為一台或多台外部裝置新增允許規則，這些裝置的資料已儲存在系統中。

根據有關目前連線的裝置的資料產生規則	需要信任少量新外部裝置時，更新已經指定的規則清單。
"**僅統計**"模式中的裝置控制工作	為大量受信任裝置建立允許規則。

裝置控制規則產生器工作使用

在"裝置控制規則產生器"工作完成時建立的 XML 檔案包含其資料曾儲存在系統登錄檔中的那些快閃記憶體磁碟機和其他外部裝置的允許規則。

在規則建立過程中使用此方案可考慮系統在所有網路受防護裝置上註冊的所有連線過的外部裝置，或只考慮目前連線到所有網路受防護裝置的裝置的資料。該工作還會考慮在工作執行的那一刻處於連接狀態的所有外部裝置。群組工作完成時，Kaspersky Embedded Systems Security 會為在網路中註冊的所有外部裝置建立允許規則清單，並將這些清單儲存在指定資料夾內的 XML 檔案中。然後，您可以在裝置控制工作設定中手動匯入建立的規則。與受防護裝置上的工作不同的是，政策不允許設定在"裝置控制規則產生器"群組工作完成時將建立的規則自動新增到裝置控制規則清單。

建議在裝置控制工作第一次啟動之前使用此方案建立允許規則清單，以便建立的允許規則涵蓋受防護裝置上使用的所有受信任外部裝置。

使用有關所有連線的裝置的系統資料

在工作執行期間，Kaspersky Embedded Systems Security 會收到有關曾經或目前連線到受防護裝置的所有外部裝置的系統資料，並在"**基於系統資訊產生規則**"視窗的清單中顯示偵測到的裝置。

對於偵測到的每個裝置，Kaspersky Embedded Systems Security 會分析製造商 (VID)、控制器類型 (PID)、易記名稱、序號和裝置實例路徑的值。您可以為其資料儲存在系統中的任何外部裝置建立允許規則，並直接將新建立的規則新增到裝置控制規則清單中。

根據此方案，Kaspersky Embedded Systems Security 會為曾經或目前連線到安裝有卡巴斯基安全管理中心的受防護裝置的外部裝置建立允許規則。

需要信任少量新外部裝置，建議使用此方案更新已經指定的規則清單。

有關目前連線的裝置的資料使用

在本方案中，Kaspersky Embedded Systems Security 僅為目前已連線的外部裝置建立允許規則。可以選擇要為其產生允許規則的一個或多個外部裝置。

"僅統計"模式中的裝置控制工作的使用

將基於工作記錄建立在"**僅統計**"模式的裝置控制工作完成時收到的 XML 檔案。

在工作執行期間，Kaspersky Embedded Systems Security 會記錄有關與受防護裝置連線的快閃記憶體磁碟機和其他外部裝置的資訊。您可以基於工作事件建立允許規則並將它們匯出到 XML 檔案。以"**僅統計**"模式啟動工作之前，建議您配置工作執行時段，以便在該時段內，將執行與受防護裝置的所有可能的外部裝置連線。

如果需要允許大量新的外部裝置，建議使用此方案更新已經建立的規則清單。

如果根據此方案在範本機上產生規則清單，您可以在透過卡巴斯基安全管理中心配置“裝置控制”工作時應用建立的允許規則清單。這樣，您可以允許在所有受防護裝置上使用連接到範本機的外部裝置。

關於裝置控制規則產生器工作

“裝置控制規則產生器”工作可以基於有關曾連線到受防護裝置的所有外部裝置的系統資料，自動為連線的快閃記憶體磁碟機和其他外部裝置建立允許規則清單。

在工作完成後，Kaspersky Embedded Systems Security 會建立一個 XML 設定檔，其中包含所有偵測到的外部裝置的允許規則清單，或者直接在“裝置控制”清單中新增建立的規則，具體取決於“裝置控制規則產生器”設定。隨後，應用程式將允許自動為其建立允許規則的裝置。

建立的規則和新增到工作中的規則顯示在“**裝置控制規則**”視窗中。

“裝置控制”工作預設設定

預設情況下，“裝置控制”工作具有下表所述的設定。您可以變更這些設定值。

預設裝置控制工作設定

設定	預設值	敘述
工作模式	**僅統計**	該工作記錄有關根據指定的規則封鎖或允許的外部裝置的資訊。實際上，不會封鎖外部裝置。 您可以為裝置防護選擇“**活動**”模式以實際封鎖使用外部裝置。
未執行裝置控制任務時，允許使用所有外部裝置	未套用	無論裝置控制工作狀態如何，Kaspersky Embedded Systems Security 都封鎖使用外部裝置。與外部裝置交換檔案時，可提供最佳防護等級，以防止電腦安全威脅。 您可以調整設定，以便 Kaspersky Embedded Systems Security 在裝置控制工作未執行時允許使用所有外部裝置。
工作啟動排程	不設定工作的初次啟動排程。	“裝置控制”工作不會在 Kaspersky Embedded Systems Security 啟動時自動啟動。 您可以配置工作啟動排程。

“裝置控制規則產生器”工作的預設設定

設定	預設值	敘述
工作模式	**考慮曾連線的所有外部裝置的系統資料**	工作執行模式。 您可以選擇“**僅考慮目前連線的外部裝置**”工作模式。
工作完成時的操作	將允許規則新增到裝置控制規則清單；新規則與現有規則合併；刪除重複的規則。	您可以將規則新增到現有規則，而不進行合併並刪除重複的規則，或將現有規則替換為新的允許規則，或設定將允許規則匯出到檔案。
工作啟動排程	不設定工作的初次啟動排程。	“裝置控制規則產生器”工作不會在 Kaspersky Embedded Systems Security 啟動時自動啟動。您可以手動啟動該工作或設定排程啟動。

透過管理外掛程式管理裝置控制

在本節中，學習如何透過管理外掛程式介面進行導航，以及如何透過卡巴斯基安全管理中心為受防護裝置群組建立規則清單來管理任意外部裝置與網路上所有受防護裝置的連線。

導航

瞭解如何透過所選介面導航到所需工作設定。

開啟“裝置控制”工作的政策設定

要透過卡巴斯基安全管理中心政策開啟“裝置控制”工作設定：

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。
5. 在打开的**“属性：<策略名称>”**窗口中，选择**“本地活动控制”**部分。
6. 在**“裝置控制”**子區段中點擊**“設定”**按鈕。
   將開啟**“裝置控制”**視窗。
7. 根據需要設定政策。

開啟裝置控制規則清單

要透過卡巴斯基安全管理中心開啟裝置控制規則清單：

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。
5. 在打开的**“属性：<策略名称>”**窗口中，选择**“本地活动控制”**部分。
6. 在**“裝置控制”**子區段中點擊**“設定”**按鈕。
   將開啟**“裝置控制”**視窗。
7. 在**“一般”**標籤上，點擊**“規則清單”**按鈕。
   將開啟**“裝置控制規則”**視窗。
8. 根據需要設定政策。

開啟“裝置控制規則產生器”工作精靈和內容

要初始化“裝置控制規則產生器”工作的建立：

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“**工作**”標籤。
4. 點擊“**建立工作**”按鈕。
   將開啟“**新建工作精靈**”視窗。
5. 選擇“**裝置控制規則產生器**”工作。
6. 點擊“**下一步**”。
   將開啟“**設定**”視窗。

要配置現有“裝置控制規則產生器”工作：

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“**工作**”標籤。
4. 按兩下卡巴斯基安全管理中心工作清單中的工作名稱。
   將打開“**屬性：裝置控制規則產生器**”窗口。

有關配置該工作的詳細資訊，請參見“配置‘裝置控制規則產生器’工作”部分。

配置“裝置控制”工作

要配置“裝置控制”工作設定：

1. 開啟“**裝置控制**”視窗。
2. 在“**一般**”標籤上，配置以下工作設定：
   - 在“**工作模式**”部分中，選擇以下工作模式之一：
     - **活動**。

       如果當“裝置控制”工作在啟動模式下執行前您認為不受信任的外部裝置連線到受防護裝置，應用程式不會封鎖該裝置。建議您手動斷開不信任裝置或重新啟動受防護裝置。否則，不會將“預設拒絕”原則套用於裝置。

     - **僅統計**。

- 選中或清除“**當未執行裝置控制工作時允許使用所有外部裝置**”核取方塊。

3. 點擊“**規則清單**”按鈕以編輯裝置控制規則清單。
4. 如有必要，在“**工作管理**”標籤上配置排程的工作啟動設定。
5. 在“裝置控制”視窗中，點擊“確定”。

Kaspersky Embedded Systems Security 將對正在執行的工作立即套用新設定。有關設定修改日期和時間以及修改前後工作設定值的資訊儲存在系統稽核記錄中。

配置“裝置控制規則產生器”工作

要配置“裝置控制規則產生器”工作：

1. 打開“**屬性：裝置控制規則產生器**”窗口。
2. 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，請參見 *卡巴斯基安全管理中心說明*。

3. 在“**設定**”部分中，您可配置以下設定：
   - 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。
4. 在“**排程**”部分中配置工作排程（您可以為除“資料庫更新回溯”以外的所有工作類型配置排程）。
5. 在“**帳戶**”部分中，指定將使用其權限執行工作的帳戶。
6. 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*。

7. 在“**內容：<工作名稱>**”視窗中，點擊“**確定**”。
   將儲存新配置的群組工作設定。

透過卡巴斯基安全管理中心配置裝置控制規則

學習如何使用裝置控制工作根據各種條件產生規則清單，或手動建立允許或拒絕規則。

基於卡巴斯基安全管理中心政策中的系統資料建立允許規則

*要使用裝置控制工作中的“**基於系統資料產生規則**”選項指定允許規則：*

1. 如有必要，將您希望信任的新的外部裝置連線到安裝了卡巴斯基安全管理中心管理主控台的受防護裝置。
2. 開啟**"裝置控制規則"**視窗。
3. 點擊**"新增"**按鈕，在開啟的內容功能表中，選擇**"基於系統資料產生規則"**選項。
4. 在**"基於系統資訊產生規則"**視窗中，選擇一個裝置。
5. 點擊**"為所選裝置新增規則"**。
6. 在**"裝置控制規則"**視窗中點擊**"儲存"**按鈕。

"裝置控制"工作中的規則清單將使用基於安裝了卡巴斯基安全管理中心管理主控台的受防護裝置的系統資料建立的新規則填充。

為已連線的裝置建立規則

*要使用裝置控制工作中的**"基於連線的裝置建立規則"**選項指定允許規則：*

1. 開啟**"裝置控制規則"**視窗。
2. 點擊**"新增"**按鈕，然後在內容功能表中，選擇**"基於連接的裝置產生規則"**。
   將開啟**"基於系統資訊產生規則"**視窗。
3. 在偵測到的已連線到受防護裝置的裝置清單中，選擇您要為其產生允許規則的裝置。
4. 點擊**"為所選裝置新增規則"**按鈕。
5. 在**"裝置控制規則"**視窗中點擊**"儲存"**按鈕。

"裝置控制"工作中的規則清單將使用基於安裝了卡巴斯基安全管理中心管理主控台的受防護裝置的系統資料建立的新規則填充。

從有關被封鎖裝置的卡巴斯基安全管理中心報告中匯入規則

您可從在**"僅統計"**模式下完成裝置控制工作後卡巴斯基安全管理中心中產生的報告匯入有關被封鎖裝置連線的資料，並使用此資料在所配置政策中產生裝置控制允許規則清單。

建立裝置控制工作期間發生的附隨報告時，您可跟蹤其連接受限制的裝置。

要基於有關被封鎖裝置的卡巴斯基安全管理中心報告為一組受防護裝置指定裝置連線允許規則：

1. 在**"事件通知"**部分中的政策內容中，確保：
   - 對於**"關鍵事件"**重要性等級，*"偵測到不受信任的外部裝置並已限制此裝置"*事件的工作記錄的儲存時間段超過在**"僅統計"**模式下的執行排程時間段（預設值為 30 天）。
   - 對於**"警告"**重要性等級，*"僅統計：偵測到不受信任的外部裝置"*事件的工作記錄的儲存時間段超過在**"僅統計"**模式下的工作執行排程時間段（預設值為 30 天）。

當事件的儲存時間段過後，有關記錄的事件的資訊會被刪除且不會反映在報告檔案中。在**"僅統計"**模式下執行裝置控制工作之前，確保工作執行時間不超過為指定事件配置的儲存時間。

2. 以**"僅統計"**模式啟動"裝置控制"工作。

   a. 在卡巴斯基安全管理中心中的**"管理伺服器"**節點的工作區中，選擇**"事件"**標籤。

   b. 點擊**"建立選擇"**按鈕並基於"*偵測到不受信任的外部裝置並已限制此裝置*"條件建立一系列事件，以檢視"裝置控制"工作將限制其連線的裝置。

   c. 在選擇的結果窗格中，點擊**"將事件匯出到檔案"**連結以將有關限制的連線的報告儲存到 TXT 檔案。

在政策中匯入和應用建立的報告之前，確保報告僅包含有關您希望允許其連線的裝置的資料。

3. 將有關受限制裝置連線的資料匯入裝置控制工作：

   a. 開啟**"裝置控制規則"**視窗。

   b. 點擊**"新增"**按鈕，然後在該按鈕的內容功能表中選擇**"從卡巴斯基安全管理中心報告匯入封鎖的裝置的資料"**。

   c. 選擇將來自根據卡巴斯基安全管理中心報告建立的清單的規則新增到先前配置的裝置控制規則清單的政策：

   - **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。
   - **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。

   d. 在開啟的 Microsoft Windows 標準視窗中，選擇已將來自受限制裝置報告的事件匯出到的 TXT 檔案。

   e. 在**"裝置控制規則"**視窗中點擊**"儲存"**按鈕。

4. 在**裝置控制**視窗中，點擊**確定**。

根據有關受限制裝置的卡巴斯基安全管理中心報告建立的規則將被新增到裝置控制規則清單。

使用"裝置控制規則產生器"工作建立規則

要使用"裝置控制規則產生器"工作為一組受防護裝置指定裝置控制規則：

1. 開啟"新建工作精靈"中的**"設定"**視窗。

2. 進行以下設定：

- 在**"模式"**部分中：
  - **考慮曾經連接過的所有外部裝置的系統資料**。
  - **僅考慮目前連線的外部裝置** 。

- 在“**工作完成後**”部分中：
  - **將允許規則新增到裝置控制規則清單**。
  - **新增原則**。
  - **將允許規則匯出到檔案**。
  - **將受防護裝置詳細資訊新增到檔案名稱**。

3. 點擊“下一步”。
4. 在“**排程**”視窗中，設定排程的工作啟動設定。
5. 點擊“下一步”。
6. 在“選擇帳戶以執行工作”視窗中，指定要使用的帳戶。
7. 點擊“下一步”。
8. 指定工作名稱。
9. 點擊“下一步”。

   工作名稱不應超過 100 個字元，並且不能包含以下符號：" * < > & \ : |

   將開啟“完成建立工作”視窗。
10. 您可以透過選中“精靈完成後執行工作”核取方塊來在精靈完成後執行工作。
11. 點擊“完成”完成建立工作。
12. 在所配置受防護裝置群組的工作區上的「工作」標籤上，從群組工作清單中選擇您已建立的「裝置控制規則產生器」。
13. 點擊「啟動」按鈕啟動工作。

    工作完成後，自動建立的允許規則清單將儲存在共用資料夾中的 XML 檔案中。

    在網路中使用裝置控制政策之前，請確保所有受防護裝置都能夠存取共用網路資料夾。如果不提供組織的政策用於網路中的共用網路資料夾，則建議為測試受防護裝置群組或範本機上的受防護裝置控制規則啟動“裝置控制規則產生器”工作。

將建立的規則新增到裝置控制規則清單

要將建立的允許規則清單新增到“裝置控制”工作：

1. 開啟“**裝置控制規則**”視窗。
2. 點擊“**新增**”按鈕。

3. 在**"新增"**按鈕的內容功能表中選擇**"從 XML 檔案匯入規則"**選項。

4. 選擇將自動建立的允許規則新增到先前建立的裝置控制規則清單中的政策：

   - **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。
   - **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。

5. 在開啟的 Microsoft Windows 標準視窗中，選擇"裝置控制規則產生器"群組工作完成後建立的 XML 檔案。

6. 點擊「開啟」。

   XML 檔案中所有產生的規則將按照所選原則新增到清單中。

7. 在**"裝置控制規則"**視窗中點擊**"儲存"**按鈕。

8. 如果想要應用建立的裝置控制規則，請在**"裝置控制"**政策設定中選擇**"啟動"**工作模式。

基於每台單獨的受防護裝置上的系統資料自動建立的允許規則將被套用於所設定政策涵蓋的所有網路受防護裝置。在這些受防護裝置上，應用程式將僅允許已為其建立允許規則的那些裝置進行連接。

透過應用程式主控台管理裝置控制

在本節中，學習如何導航應用程式主控台介面以及如何在受防護裝置上配置工作設定。

導航

瞭解如何透過所選介面導航到所需工作設定。

開啟"裝置控制"工作設定

要透過應用程式主控台開啟"裝置控制"工作設定：

1. 在應用程式主控台樹狀目錄中，展開**"電腦控制"**節點。

2. 選擇**"裝置控制"**子節點。

3. 在**裝置控制**子節點的詳細資訊視窗中，點擊**內容**連結。

   將開啟**"工作設定"**視窗。

4. 根據需要配置工作。

開啟"裝置控制規則"視窗

要透過應用程式主控台開啟裝置控制規則清單：

1. 在應用程式主控台樹狀目錄中，展開**"電腦控制"**節點。
2. 選擇**"裝置控制"**子節點。
3. 在**"裝置控制"**節點的結果窗格中，點擊**"裝置控制規則"**連結。
   將開啟**"裝置控制規則"**視窗。
4. 根據需要設定規則清單。

開啟"裝置控制規則產生器"工作設定

要配置"裝置控制規則產生器"工作：

1. 在應用程式主控台樹狀目錄中，展開**"自動規則產生器"**節點。
2. 選擇**"裝置控制規則產生器"**子節點。
3. 在**"裝置控制規則產生器"**子節點的結果窗格中，點擊**"內容"**連結。
   將開啟**"工作設定"**視窗。
4. 根據需要配置工作。

配置裝置控制工作設定

要配置"裝置控制"工作設定：

1. 開啟**"工作設定"**視窗。
2. 在**"一般"**標籤上，配置以下工作設定：
   - 在**"工作模式"**部分中，選擇以下工作模式之一：
     - 活動。

       如果當"裝置控制"工作在啟動模式下執行前您認為不受信任的外部裝置連線到受防護裝置，應用程式不會封鎖該裝置。建議您手動斷開不信任裝置或重新啟動受防護裝置。否則，不會將"預設拒絕"原則套用於裝置。

     - **僅統計**。
   - 選中或清除**"未執行裝置控制任務時，允許使用所有外部裝置"**核取方塊。
3. 如有必要，在**"排程"**和**"進階"**標籤上，配置排程的工作啟動設定。
4. 要編輯裝置控制規則清單，請在**"裝置控制規則"**節點的結果窗格的下部，點擊**"裝置控制"**連結。

Kaspersky Embedded Systems Security 將對正在執行的工作立即套用新設定。有關設定修改日期和時間以及修改前後工作設定值的資訊儲存在系統稽核記錄中。

配置裝置控制規則

瞭解如何使用"裝置控制"工作產生、匯入和匯出規則清單，或手動建立允許或拒絕規則。

從 XML 檔案匯入裝置控制規則

要匯入裝置控制規則：

1. 開啟"**裝置控制規則**"視窗。
2. 點擊"**新增**"按鈕。
3. 在按鈕的內容功能表中，選擇"**從 XML 檔案匯入規則**"。
4. 指定新增匯入規則的方法。要執行此操作，請從"**從 XML 檔案匯入規則**"按鈕的內容功能表中選擇一個選項：
   - **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。
   - **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。

   將開啟標準 Microsoft Windows"**開啟**"視窗。
5. 在"**開啟**"視窗中，選擇包含裝置控制規則的設定的 XML 檔案。
6. 點擊"**開啟**"按鈕。

匯入的規則將顯示在"**裝置控制規則**"視窗中的清單中。

基於裝置控制工作事件填寫規則清單

要基於"裝置控制"工作事件建立包含裝置控制規則清單的設定檔：

1. 以"**僅統計**"模式啟動裝置控制工作，以記錄與受防護裝置連接的快閃記憶體磁碟機和其他外部裝置的所有事件。
2. "**僅統計**"模式中的工作完成後，透過點擊"**開啟工作記錄**"節點結果窗格的"**管理**"部分中的"**裝置控制**"按鈕，開啟工作記錄。
3. 在"**記錄**"視窗中，點擊"**基於事件建立規則**"。

Kaspersky Embedded Systems Security 將會建立一個 XML 設定檔，其中包含基於"**僅統計**"模式中的"裝置控制"工作事件建立的規則清單。您可以在"裝置控制"工作中套用此清單。

在套用基於工作事件建立的規則清單之前，建議您仔細檢查，然後手動處理規則清單，以確保指定的規則沒有允許不信任裝置。

在將包含工作事件 XML 檔案轉換為規則清單期間，應用程式將為所有註冊的事件建立允許規則，包括裝置限制。

無論工作模式如何，所有工作事件都將記錄在工作記錄中。您可以基於處於**"活動"**模式的工作事件建立包含規則清單的設定檔。除非出現緊急情況，例如工作效率要求在工作以啟動模式執行之前建立最終規則清單版本，否則不建議使用此方案。

為一個或多個外部裝置新增允許規則

裝置控制工作中支援手動逐個新增規則的功能。但是，如果您需要為一個或多個新外部裝置新增規則，可以使用**"基於系統資料產生規則"**選項。如果應用此方案，應用程式將使用有關所有曾經連接過的外部裝置的 Windows 資料，並且還允許目前連線的裝置，以填寫允許規則清單。

要為目前連線的一個或多個外部裝置新增允許規則：

1. 開啟**"裝置控制規則"**視窗。
2. 點擊**"新增"**按鈕。
3. 在開啟的內容功能表中，選擇**"基於系統資料產生規則"**選項。
4. 在開啟的視窗中，檢視偵測到的裝置清單並選擇要在受防護裝置上信任的一個或多個裝置。
5. 點擊**"為所選裝置新增規則"**按鈕。

   將會建立新規則並新增到裝置控制規則清單中。

刪除裝置控制規則

要刪除裝置控制規則：

1. 開啟**"裝置控制規則"**視窗。
2. 在清單中，選擇要刪除的一項或多項規則。
3. 點擊**"刪除選取的項目"**按鈕。
4. 點擊**"儲存"**按鈕。

   將刪除所選裝置控制規則。

匯出裝置控制規則

要將裝置控制規則匯出到設定檔：

1. 開啟“**裝置控制規則**”視窗。
2. 點擊“**匯出至檔案**”按鈕。

   將開啟標準的 Microsoft Windows 視窗。
3. 在開啟的視窗中，指定想要將規則匯出到其中的檔案。如果不存在此類檔案，則將建立它。如果具有指定名稱的檔案已存在，則將在匯出規則後重寫其內容。
4. 點擊“**儲存**”按鈕。

規則及其設定將匯出到指定檔案中。

啟動和停用裝置控制規則

您可以啟動和停用已建立的裝置控制規則，而不必刪除它們。

若要啟動或停用已建立的裝置控制規則：

1. 開啟“**裝置控制規則**”視窗。
2. 在指定規則清單中，透過點擊要配置其內容的規則，開啟“**規則內容**”視窗。
3. 在開啟的視窗中，選中或清除“**套用規則**”核取方塊。
4. 點擊“**確定**”。

將為指定規則儲存和顯示規則應用狀態。

延伸裝置控制規則使用範圍

每個自動建立的裝置控制規則都只涵蓋一個外部裝置。您可以透過在任何指定規則的內容中設定裝置實例路徑遮罩，來手動延伸規則使用範圍。

應用裝置實例路徑可減少指定的總規則數並簡化規則處理。但是延伸規則使用範圍可能會降低外部裝置控制效率。

要在裝置控制規則內容中應用裝置實例路徑遮罩：

1. 開啟“**裝置控制規則**”視窗。
2. 在開啟的視窗中，選擇一個規則以使用其內容來套用遮罩。
3. 透過點擊選定的裝置控制規則，開啟“**規則內容**”視窗。
4. 在開啟的視窗中，執行以下操作：
   - 如果您希望某選定規則允許所有符合指定的裝置製造商和控制器類型資訊的外部裝置的連線，請選中“**使用遮罩**”欄位旁邊的“**控制器類型 (PID)**”核取方塊。
   - 如果您希望某選定規則允許所有符合指定的裝置製造商和裝置序號資訊的外部裝置的連線，請選中“**使用遮罩**”欄位旁邊的“**序號**”核取方塊。

- 如果您希望某選定規則允許所有符合指定的裝置製造商以及控制器類型和裝置序號資訊的外部裝置的連線，請選中**"使用遮罩"**欄位和**"控制器類型 (PID)"**欄位旁邊的**"序號"**核取方塊。

如果在至少一個欄位中選中了**"使用遮罩"**核取方塊，則將使用 * 符號代替核取方塊被選中的欄位的資料，並且在套用規則時不會考慮這些資料。

5. 如有必要，請在**"描述"**欄位中指定有關規則的附加資訊。例如，指定受規則影響的裝置。
6. 點擊**"確定"**。

將儲存新配置的規則內容。規則使用範圍將根據指定的裝置實例路徑遮罩進行延伸。

配置裝置控制規則產生器工作

要配置"裝置控制規則產生器"工作：

1. 在應用程式主控台樹狀目錄中，展開**"自動規則產生器"**節點。
2. 選擇**"裝置控制規則產生器"**子節點。
3. 在**"內容"**節點的結果窗格中，點擊**"裝置控制規則產生器"**連結。
   將開啟**"工作設定"**視窗。
4. 在**"一般"**標籤上的**"工作模式"**部分中選擇工作執行模式：
   - **考慮曾連線的所有外部裝置的系統資料**。
   - **僅考慮目前連線的外部裝置** 。
5. 在**"工作完成後"**部分中，指定 Kaspersky Embedded Systems Security 在工作完成後必須執行的操作：
   - **將允許規則新增到裝置控制規則清單**。
   - **新增原則**。
   - **將允許規則匯出到檔案**。
   - **將受防護裝置詳細資訊新增到檔案名稱**。
6. 在**"排程"**和**"進階"**標籤上，配置排程的工作啟動設定。
7. 在**工作設定**視窗中點擊**確定**。

Kaspersky Embedded Systems Security 將對正在執行的工作立即套用新設定。有關設定修改日期和時間以及修改前後工作設定值的資訊儲存在系統稽核記錄中。

透過應用程式主控台 Web 外掛程式管理裝置控制

在本節中，您將學習如何導航應用程式 Web 外掛程式介面以及如何在受防護裝置上配置工作設定。

1. 在 Web 控制的主視窗中，選取**裝置 → 政策和設定檔案**。

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**”標籤。

4. 選擇“**本機活動控制**”部分。

5. 在“**設定**”子區段中點擊“**裝置控制**”。

6. 按下表所述配置設定。

裝置控制工作設定

設定	敘述
活動	Kaspersky Embedded Systems Security 會將規則套用於控制卸除式磁碟機和其他外部裝置的連線，並根據預設拒絕政策和指定允許規則允許或封鎖使用所有裝置。允許使用受信任外部裝置。預設情況下，封鎖使用不受信任的外部裝置。
僅統計	Kaspersky Embedded Systems Security 不會控制卸除式磁碟機和其他外部裝置的連線，但僅記錄有關外部裝置在受防護裝置上的連接和註冊，以及有關相連裝置觸發的裝置控制允許規則的資訊。允許使用所有外部裝置。預設設定此模式。
未執行裝置控制任務時，允許使用所有外部裝置	使用此核取方塊可允許或封鎖在「裝置控制」工作未執行時使用外部裝置。 如果選取該核取方塊且裝置控制工作未執行，則 Kaspersky Embedded Systems Security 允許在受防護裝置上使用任何外部裝置。 如果清除此核取方塊，應用程式在以下情況下將封鎖在受防護裝置上使用不受信任的外部裝置：「裝置控制」工作未執行或 Kaspersky Security 服務已關閉。建議使用該選項以最大限度防護您的電腦在與外部裝置交換檔案時免受安全威脅。 預設取消選定該核取方塊。
裝置控制規則	您可以編輯裝置控制規則清單。
工作管理	您可以配置按排程啟動工作的設定。

防火牆管理

本節包含有關防火牆管理工作以及如何設定的資訊。

關於防火牆管理工作

Kaspersky Embedded Systems Security 會提供一個可靠方便的解決方案，以便使用防火牆管理工作防護網路連線。

防火牆管理工作不會執行獨立的網路流量篩選，但它允許您透過 Kaspersky Embedded Systems Security 圖形介面管理 Windows 防火牆。在防火牆管理工作期間，Kaspersky Embedded Systems Security 接管對作業系統防火牆的設定和政策的管理，並封鎖任何配置防火牆的外部嘗試。

在應用程式安裝期間，防火牆管理元件會讀取並複製 Windows 防火牆狀態及所有指定規則。此後，只能變更規則集和規則參數，且防火牆只能在 Kaspersky Embedded Systems Security 中開啟或關閉。

如果在安裝 Kaspersky Embedded Systems Security 期間 Windows 防火牆關閉，則在安裝完成後將不會執行防火牆管理工作。如果在安裝應用程式期間 Windows 防火牆開啟，則會在安裝完成後執行防火牆管理工作，從而封鎖指定規則不允許的所有網路連線。

預設情況下，不會安裝防火牆管理元件，因為其未包括在建議安裝元件集中。

防火牆管理工作強制封鎖工作的指定規則不允許的所有傳入和傳出連接。

該工作會定期輪詢 Windows 防火牆並監控其狀態。預設情況下，輪詢間隔設定為 1 分鐘且無法變更。如果 Kaspersky Embedded Systems Security 偵測到 Windows 防火牆設定和防火牆管理工作設定之間存在不匹配，應用程式會強制應用作業系統防火牆上的工作設定。

每分鐘輪詢 Windows 防火牆時，Kaspersky Embedded Systems Security 監控以下資訊：

- Windows 防火牆的執行狀態。
- 安裝 Kaspersky Embedded Systems Security 後其他應用程式或工具新增的規則的狀態（例如，使用 wf.msc 的某個連接埠/應用程式新增的新應用程式規則）。

将新规则应用于 Windows 防火墙时，Kaspersky Embedded Systems Security 会在 Windows 防火墙管理单元中创建一个 Kaspersky Security Group 规则集。该规则集包含 Kaspersky Embedded Systems Security 使用“防火墙管理”任务创建的所有规则。在輪詢期間，應用程式不會監控 Kaspersky Embedded Systems Security 群組中的規則，且該規則不會自動與防火牆管理工作設定中指定的規則清單同步。

要手動更新 Kaspersky Embedded Systems Security 群組規則，

請重新啟動 Kaspersky Embedded Systems Security 防火牆管理工作。

您還可使用 Windows 防火牆管理單元手動編輯 Kaspersky Security 群組規則。

如果按卡巴斯基安全管理中心群組政策管理 Windows 防火牆，則防火牆管理工作無法啟動。

關於防火牆規則

防火牆管理工作使用工作執行期間強制套用於 Windows 防火牆的允許規則控制傳入和傳出網路流量的篩選。

初次啟動工作時，Kaspersky Embedded Systems Security 會讀取 Windows 防火牆設定中指定的所有傳入網路流量規則，並將其複製到防火牆管理工作設定。然後，應用程式根據以下規則執行：

- 如果在 Windows 防火牆設定中建立新規則（在安裝新應用程式期間手動或自動建立），Kaspersky Embedded Systems Security 會刪除該規則。
- 如果從 Windows 防火牆設定中刪除現有規則，則重新啟動工作後 Kaspersky Embedded Systems Security 會還原該規則。
- 如果在 Windows 防火牆設定中變更現有規則的參數，Kaspersky Embedded Systems Security 會回溯變更。
- 如果在防火牆管理設定中建立新規則，Kaspersky Embedded Systems Security 會將該規則強制套用於 Windows 防火牆。
- 如果從防火牆管理設定中刪除現有規則，Kaspersky Embedded Systems Security 會從 Windows 防火牆設定中強制刪除該規則。

Kaspersky Embedded Systems Security 不會使用封鎖規則或控制傳出網路流量的規則。在防火牆管理工作啟動後，Kaspersky Embedded Systems Security 會從 Windows 防火牆設定中刪除所有此類規則。

您可為傳入網路流量設定、刪除和編輯篩選規則。

您無法在防火牆管理工作設定中指定新規則以控制傳出網路流量。Kaspersky Embedded Systems Security 中指定的所有防火牆規則僅控制傳入網路流量。

您可以管理不同類型的防火牆規則：針對應用程式和針對連接埠。

應用程式規則

此類型的規則允許指定應用程式的目的網路連線。這些規則的觸發條件基於可執行檔的路徑。

您可管理應用程式規則：

- 新增新規則。
- 刪除現有規則。
- 啟用或停用指定規則。
- 編輯指定規則的參數：指定規則名稱、可執行檔的路徑以及規則使用範圍。

連接埠規則

此類型的規則允許指定連接埠和協定 (TCP/UDP) 的網路連線。這些規則的觸發條件基於埠號和協定類型。

您可管理連接埠規則：

- 新增新規則。
- 刪除現有規則。
- 啟用或停用指定規則。
- 編輯指定規則的參數：設定規則名稱、埠號、協定類型以及規則的應用範圍。

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連線，會下降受防護裝置的安全等級。

防火牆管理工作預設設定

防火牆管理工作使用下表描述的預設設定。您可以變更這些設定值。

防火牆管理工作預設設定

設定	預設值	敘述
針對應用程式的防火牆規則	已啟用兩條針對應用程式的預設規則	您可以停用預設規則或新增新規則。
針對連接埠的防火牆規則	已啟用六條針對連接埠的預設規則	您可以停用預設規則或新增新規則。
工作啟動排程	不設定工作的初次啟動排程。	“防火牆管理”工作不會在 Kaspersky Embedded Systems Security 啟動時自動啟動。 您可以配置工作啟動排程。

透過管理外掛程式管理防火牆規則

在本節中，學習如何透過管理外掛程式介面管理防火牆規則。

啟用和停用防火牆規則

要啟用或停用篩選傳入網路流量的現有規則，請執行以下操作：

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細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**”標籤，然後開啟“**內容：<政策名稱>**”視窗。
   - 要為單台受防護裝置配置應用程式，請選擇“**裝置**”標籤，然後開啟“**應用程式設定**”視窗。

如果某個啟動卡巴斯基安全管理中心政策已套用於裝置，並且該政策封鎖對應用程式設定的變更，則無法在**"應用程式設定"**視窗中編輯這些設定。

4. 在**"網路活動控制"**部分中，點擊**"防火牆管理"**子區段中的**"設定"**按鈕。
5. 點擊開啟的視窗中的**"規則清單"**按鈕。
   將開啟**"防火牆規則"**視窗。
6. 根據想要修改器狀態的規則類型，選擇**"應用程式"**或**"連接埠"**標籤。
7. 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。
8. 在**防火牆規則**視窗中，點擊**儲存**。
9. 在**防火牆管理**視窗中，點擊**確定**。
10. 在**"內容：<政策名稱>"**視窗中，點擊**"確定"**。

將儲存指定工作設定。新規則參數將傳送到 Windows 防火牆。

手動新增防火牆規則

您只能新增和編輯應用程式和連接埠的規則。不能新增或編輯現有群組規則。

要新增篩選傳入網路流量的新規則或編輯現有規則：

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細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"**標籤，然後開啟**"內容：<政策名稱>"**視窗。
   - 要為單台受防護裝置配置應用程式，請選擇**"裝置"**標籤，然後開啟**"應用程式設定"**視窗。

如果某個啟動卡巴斯基安全管理中心政策已套用於裝置，並且該政策封鎖對應用程式設定的變更，則無法在**"應用程式設定"**視窗中編輯這些設定。

4. 在**"網路活動控制"**部分中，點擊**"防火牆管理"**子區段中的**"設定"**按鈕。
5. 點擊開啟的視窗中的**"規則清單"**按鈕。
   將開啟**"防火牆規則"**視窗。

6. 根據您要新增的規則類型，選擇**"應用程式"**或**"連接埠"**標籤，然後執行以下操作之一：

   - 要編輯現有規則，在規則清單中選擇要編輯的規則，然後點擊**"編輯"**。
   - 要新增新規則，點擊**"新增"**。
     根據配置的規則類型，將開啟**"應用程式規則"**視窗或**"連接埠規則"**視窗。

7. 在開啟的視窗中，執行以下操作：

   - 如果您使用的是應用程式規則，請執行以下操作：

     a. 在**"規則名稱"**欄位中，輸入所編輯規則的名稱。

     b. 指定您透過修改此規則允許其連線的應用程式的可執行檔的**"應用程式路徑"**。
     您可手動或透過使用**"瀏覽"**按鈕設定路徑。

     c. 在**"規則使用範圍"**欄位中，指定將為其套用已修改規則的網路位址。

     > 只能使用 IPv4 位址。

   - 如果您使用的是連接埠規則，請執行以下操作：

     a. 在**"規則名稱"**欄位中，輸入所編輯規則的名稱。

     b. 指定應用程式將允許連線的**"埠號"**。

     c. 選擇應用程式將允許連線的協定類型 (TCP/UDP)。

     d. 在**"規則使用範圍"**欄位中，指定將為其套用已修改規則的網路位址。

     > 只能使用 IPv4 位址。

8. 在**"確定"**或**"應用程式規則"**視窗中，點擊**"連接埠規則"**。

9. 在**防火牆管理**視窗中，點擊**確定**。

10. 在**"內容：<政策名稱>"**視窗中，點擊**"確定"**。

將儲存指定工作設定。新規則參數將傳送到 Windows 防火牆。

刪除防火牆規則

> 您只能刪除應用程式和連接埠規則。您無法刪除現有群組規則。

要刪除篩選傳入網路流量的現有規則，請執行以下操作：

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細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"**標籤，然後開啟**"內容：<政策名稱>"**視窗。
   - 要為單台受防護裝置配置應用程式，請選擇**"裝置"**標籤，然後開啟**"應用程式設定"**視窗。

   如果某個啟動卡巴斯基安全管理中心政策已套用於裝置，並且該政策封鎖對應用程式設定的變更，則無法在**"應用程式設定"**視窗中編輯這些設定。

4. 在**"網路活動控制"**部分中，點擊**"防火牆管理"**子區段中的**"設定"**按鈕。
5. 點擊開啟的視窗中的**"規則清單"**按鈕。
   將開啟**"防火牆規則"**視窗。
6. 根據想要修改器狀態的規則類型，選擇**"應用程式"**或**"連接埠"**標籤。
7. 在規則清單中，選擇要刪除的規則。
8. 點擊**"刪除"**按鈕。
   將刪除所選規則。
9. 在**防火牆規則**視窗中，點擊**儲存**。
10. 在**防火牆管理**視窗中，點擊**確定**。
11. 在**"內容：<政策名稱>"**視窗中，點擊**"確定"**。

將儲存指定防火牆管理工作設定。新規則參數將傳送到 Windows 防火牆。

透過應用程式主控台管理防火牆規則

在本節中，學習如何透過應用程式主控台介面管理防火牆規則。

啟用和停用防火牆規則

要啟用或停用篩選傳入網路流量的現有規則，請執行以下操作：

1. 在應用程式主控台樹狀目錄中，展開**"電腦控制"**節點。
2. 選擇**"防火牆管理"**子節點。
3. 在**"防火牆規則"**節點的詳細資訊窗格中，點擊**"防火牆管理"**連結。
   將開啟**"防火牆規則"**視窗。
4. 根據想要修改器狀態的規則類型，選擇**"應用程式"**或**"連接埠"**標籤。
5. 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. 在**"儲存"**視窗中，點擊**"防火牆規則"**。

將儲存指定工作設定。新規則參數將傳送到 Windows 防火牆。

手動新增防火牆規則

要新增篩選傳入網路流量的新規則或編輯現有規則：

1. 在應用程式主控台樹狀目錄中，展開**"電腦控制"**節點。
2. 選擇**"防火牆管理"**子節點。
3. 在**"防火牆規則"**節點的詳細資訊窗格中，點擊**"防火牆管理"**連結。
   將開啟**"防火牆規則"**視窗。
4. 根據您要新增的規則類型，選擇**"應用程式"**或**"連接埠"**標籤，然後執行以下操作之一：
   - 要編輯現有規則，在規則清單中選擇要編輯的規則，然後點擊**"編輯"**。
   - 要新增新規則，點擊**"新增"**。
     根據配置的規則類型，將開啟**"應用程式規則"**視窗或**"連接埠規則"**視窗。
5. 在開啟的視窗中，執行以下操作：
   - 如果您使用的是應用程式規則，請執行以下操作：
     a. 在**"規則名稱"**欄位中，輸入所編輯規則的名稱。
     b. 指定您透過修改此規則允許其連線的應用程式的可執行檔的**"應用程式路徑"**。
     您可手動或透過使用**"瀏覽"**按鈕設定路徑。
     c. 在**"規則使用範圍"**欄位中，指定將為其套用已修改規則的網路位址。

     只能使用 IPv4 位址。

   - 如果您使用的是連接埠規則，請執行以下操作：
     a. 在**"規則名稱"**欄位中，輸入所編輯規則的名稱。
     b. 指定應用程式將允許連線的**"埠號"**。
     c. 選擇應用程式將允許連線的協定類型 (TCP/UDP)。
     d. 在**"規則使用範圍"**欄位中，指定將為其套用已修改規則的網路位址。

只能使用 IPv4 位址。

6. 在**“確定”**或**“應用程式規則”**視窗中，點擊**“連接埠規則”**。
7. 在**“儲存”**視窗中，點擊**“防火牆規則”**。

將儲存指定工作設定。新規則參數將傳送到 Windows 防火牆。

刪除防火牆規則

您只能刪除應用程式和連接埠規則。您無法刪除現有群組規則。

要刪除篩選傳入網路流量的現有規則，請執行以下操作：

1. 在應用程式主控台樹狀目錄中，展開**“電腦控制”**節點。
2. 選擇**“防火牆管理”**子節點。
3. 在**“防火牆規則”**節點的詳細資訊窗格中，點擊**“防火牆管理”**連結。
   將開啟**“防火牆規則”**視窗。
4. 根據想要修改器狀態的規則類型，選擇**“應用程式”**或**“連接埠”**標籤。
5. 在規則清單中，選擇要刪除的規則。
6. 點擊**“刪除”**按鈕。
   將刪除所選規則。
7. 在**“儲存”**視窗中，點擊**“防火牆規則”**。

將儲存指定工作設定。新規則參數將傳送到 Windows 防火牆。

透過 Web 外掛程式管理防火牆規則

要透過 Web 外掛程式管理防火牆規則：

1. 在 Web 控制的主視窗中，選取**裝置 → 政策和設定檔案**。
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”**標籤。
4. 選擇**“網路活動控制”**部分。
5. 在**“設定”**子區段中，點擊**“防火牆管理”**。
6. 按下表所述配置設定。

防火牆管理工作設定

設定	敘述
應用程式規則	您可管理應用程式規則。 此類型的規則允許指定應用程式的目的網路連線。這些規則的觸發條件基於可執行檔的路徑。
連接埠規則	您可管理連接埠規則。 此類型的規則允許指定連接埠和協定 (TCP/UDP) 的網路連線。這些規則的觸發條件基於埠號和協定類型。
工作管理	您可以配置按排程啟動工作的設定。

啟用和停用防火牆規則

要啟用或停用篩選傳入網路流量的現有規則，請執行以下操作：

1. 在 Web 控制的主視窗中，選取**裝置 → 政策和設定檔案**。
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**"標籤。
4. 選擇"**網路活動控制**"部分。
5. 在"**設定**"子區段中，點擊"**防火牆管理**"。
6. 根據您要修改其狀態的規則類型，選擇"**應用程式規則**"或"**連接埠規則**"標籤。
7. 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，請開啟規則名稱左側的切換按鈕。
   - 如果您想要停用已啟用的規則，請關閉規則名稱左側的切換按鈕。
8. 點擊"**確定**"。

將儲存指定工作設定。新規則參數將傳送到 Windows 防火牆。

手動新增防火牆規則

要新增篩選傳入網路流量的新規則或編輯現有規則：

1. 在 Web 控制的主視窗中，選取**裝置 → 政策和設定檔案**。
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**"標籤。
4. 選擇"**網路活動控制**"部分。
5. 在"**設定**"子區段中，點擊"**防火牆管理**"。

6. 根據您要修改其狀態的規則類型，選擇**"應用程式規則"**或**"連接埠規則"**標籤，然後執行以下操作之一：

   - 要編輯現有規則，請選擇要編輯的規則，然後點擊**"編輯"**。
   - 要新增新規則，點擊**"新增"**。

7. 在畫面的右側部分，執行下列操作：

   - 如果您使用的是應用程式規則，請執行以下操作：

     a. 在**"規則名稱"**欄位中，輸入所編輯規則的名稱。

     b. 指定您透過修改此規則允許其連線的應用程式的可執行檔的**"應用程式路徑"**。

     c. 在**"規則套用範圍"**欄位中，指定將為其套用已修改規則的網路位址。

     > 只能使用 IPv4 位址。

   - 如果您使用的是連接埠規則，請執行以下操作：

     a. 在**"規則名稱"**欄位中，輸入所編輯規則的名稱。

     b. 指定應用程式將允許連線的埠號。

     c. 選擇應用程式將允許連線的協定類型 (TCP/UDP)。

     d. 在**"規則套用範圍"**欄位中，指定將為其套用已修改規則的網路位址。

     > 只能使用 IPv4 位址。

8. 點擊**"確定"**。

9. 在**防火牆管理**視窗中，點擊**防火牆管理**。

將儲存指定工作設定。新規則參數將傳送到 Windows 防火牆。

刪除防火牆規則

> 您只能刪除應用程式和連接埠規則。您無法刪除現有群組規則。

要刪除篩選傳入網路流量的現有規則，請執行以下操作：

1. 在 Web 控制的主視窗中，選取**裝置 → 政策和設定檔案**。
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"**標籤。
4. 選擇**"網路活動控制"**部分。

5. 在**"設定"**子區段中，點擊**"防火牆管理"**。

6. 根據您要刪除的規則類型，選擇**"應用程式規則"**或**"連接埠規則"**標籤。

7. 在規則清單中，選擇要刪除的規則。

8. 點擊**"刪除"**按鈕。
   將刪除所選規則。

9. 點擊**"確定"**。

將儲存指定工作設定。新規則參數將傳送到 Windows 防火牆。

檔案完整性監控

本節包含有關啟動和設定“檔案完整性監控”工作的資訊。

關於“檔案完整性監控”工作

“檔案完整性監控”工作的設計目的是為了跟蹤針對工作設定中指定的監控範圍內的特定檔案和資料夾執行的操作。可以使用該工作來刪除可能對受防護裝置造成安全入侵的檔案變更。還可以配置監控被中斷期間要對其進行跟蹤的檔案變更。

當監控範圍暫時位於工作範圍之外時（例如，如果工作停止或如果受防護裝置上沒有物理顯示外部裝置），會出現*監控中斷*。一旦重新連線外部裝置，Kaspersky Embedded Systems Security 將報告監控範圍內偵測到的檔案操作。

如果由於重新安裝“檔案完整性監控”元件造成指定監控範圍內的工作停止執行，則不構成監控中斷。這種情況下，“檔案完整性監控”工作並未執行。

環境要求

要啟動“檔案完整性監控”工作，必須滿足以下條件：

- 受防護裝置上必須使用 ReFS 或 NTFS 檔案系統。
- 必須啟用 Windows USN 記錄。元件查詢此記錄來獲取有關檔案操作的資訊。

  如果為某個磁區建立規則後啟用了 USN 記錄且已啟動“檔案完整性監控”工作，則必須重新啟動該工作。如果不重新啟動，則監控過程中不會套用該規則。

排除監控範圍

您可以建立排除監控範圍。排除針對每個單獨的規則進行指定，並且僅對指定的監控範圍產生作用。可以為每個規則指定無限數量的排除。

排除比監控範圍具有更高的優先順序，且即使指定的資料夾或檔案位於監控範圍內，也不受工作的監控。如果其中一個規則的設定指定的監控範圍比排除中指定的資料夾具有更低的等級，則當工作執行時將不會考慮監控範圍。

要指定排除，可以使用與用於指定監控範圍相同的遮罩。

關於檔案操作監控規則

“檔案完整性監控”工作根據檔案操作監控規則執行。可以使用規則觸發條件來配置觸發工作的條件，以及調整工作記錄中記錄的已刪除檔案操作事件的重要性等級。

針對每個監控範圍指定了檔案操作監控規則。

可以配置以下規則觸發條件：

- 受信任使用者
- 檔案操作標記

受信任使用者

預設情況下，應用程式將所有操作視為潛在安全入侵。受信任使用者清單為空。可以透過在檔案操作監控規則設定中建立受信任使用者清單來配置事件重要性等級。

*不受信任使用者*是分配給監控範圍規則設定中受信任使用者清單裡未指定之任何使用者的狀態。如果 Kaspersky Embedded Systems Security 偵測到不受信任使用者執行的檔案操作，則"檔案完整性監控"工作將在工作記錄中記錄一個緊急事件。

*受信任使用者*是分配給經過產品授權可在指定的監控範圍內執行檔案操作之使用者或群組的狀態。如果 Kaspersky Embedded Systems Security 偵測到受信任使用者執行的檔案操作，則"檔案完整性監控"工作將在工作記錄中記錄一個"資訊事件"。

Kaspersky Embedded Systems Security 在監控中斷期間無法確定發起操作的使用者。在此情況下，使用者狀態被確定為未知。

未知使用者 — 如果由於工作中斷或者資料同步驅動程式或 USN 記錄失敗導致 Kaspersky Embedded Systems Security 無法獲取有關使用者的資料，則將此狀態分配給使用者。如果 Kaspersky Embedded Systems Security 偵測到未知使用者執行的檔案操作，則"檔案完整性監控"工作將在工作記錄中記錄一個"*警告*事件"。

檔案操作標記

當"檔案完整性監控"工作執行時，Kaspersky Embedded Systems Security 使用檔案操作標記來確定已對檔案執行了操作。

檔案操作標記是可以對檔案操作進行特徵化的獨特敘述符。

每個檔案操作可以是針對檔案進行的單個操作或系列操作。每個此類操作等同於一個檔案操作標記。如果您指定作為規則觸發條件的標記在檔案操作鏈中被刪除，則應用程式將記錄一個事件，表示已執行指定的檔案操作。

已記錄事件的重要性等級不取決於選定的檔案操作標記或事件的數量。

預設情況下，Kaspersky Embedded Systems Security 考慮所有可用的檔案操作標記。可以在工作規則設定中手動選擇檔案操作標記。

檔案操作標記

檔案操作 ID	檔案操作標記	支援的檔案系統
BASIC_INFO_CHANGE	已變更檔案或資料夾的內容或時間標記	NTFS、ReFS
COMPRESSION_CHANGE	已變更檔案或資料夾的壓縮	NTFS、ReFS
DATA_EXTEND	已變更檔案或資料夾的大小	NTFS、ReFS
DATA_OVERWRITE	已覆蓋檔案或資料夾中的資料	NTFS、ReFS
DATA_TRUNCATION	已截斷檔案或資料夾	NTFS、ReFS

EA_CHANGE	已變更延伸的檔案或資料夾內容	僅限 NTFS
ENCRYPTION_CHANGE	已變更檔案或資料夾的加密狀態	NTFS、ReFS
FILE_CREATE	首次建立檔案或資料夾	NTFS、ReFS
FILE_DELETE	使用 SHIFT+DEL 組合鍵永久刪除的檔案或資料夾	NTFS、ReFS
HARD_LINK_CHANGE	已為建立或刪除檔案或資料夾的硬連結	僅限 NTFS
INDEXABLE_CHANGE	已變更檔案或資料夾的索引狀態	NTFS、ReFS
INTEGRITY_CHANGE	已變更命名的檔案流的完整性內容	僅限 ReFS
NAMED_DATA_EXTEND	已增大命名的檔案流的大小	NTFS、ReFS
NAMED_DATA_OVERWRITE	已覆蓋命名的檔案流	NTFS、ReFS
NAMED_DATA_TRUNCATION	已截斷命名的檔案流	NTFS、ReFS
OBJECT_ID_CHANGE	已變更檔案或資料夾識別碼	NTFS、ReFS
RENAME_NEW_NAME	已為檔案或資料夾分配新名稱	NTFS、ReFS
REPARSE_POINT_CHANGE	已為檔案或資料夾建立新的重分析點或變更其現有重分析點	NTFS、ReFS
SECURITY_CHANGE	已變更檔案或資料夾存取權限	NTFS、ReFS
STREAM_CHANGE	已建立新的命名的檔案流或變更現有命名的檔案流	NTFS、ReFS
TRANSACTED_CHANGE	TxF 事務已變更命名的檔案流	僅限 ReFS

“檔案完整性監控”工作預設設定

預設情況下，“檔案完整性監控”工作具有下表所述的設定。您可以在下列元件中變更這些設定值：

- 管理外掛程式
- 應用程式主控台
- Web 外掛程式

“檔案完整性監控”工作預設設定

設定	預設值	敘述
監控範圍	未配置	使用此選項可以指定操作將監控的資料夾和檔案。將針對指定監控範圍內的資料夾和檔案產生監控事件。
受信任使用者清單	未配置	使用此選項可以指定使用者和/或使用者群組，其在指定資料夾中的操作將被元件視為安全。
記錄監控中斷期間發生的檔案操作資訊	已使用	使用此選項可以在工作未執行期間，啟用或停用指定監控範圍內執行的檔案操作記錄。 預設情況下，系統不會考量配置規則，為受信任的使用者編譯統計資訊。
封鎖入侵 USN 記錄的嘗試	已使用	使用此選項可以啟用或停用對 USN 記錄的防護。
套用信任區域	已停用	除了設定為規則外，可以選擇或清除 **套用受信任區域**核取方塊，來套用

		受信任區域排除項目。
偵測或封鎖選定的檔案操作	已停用	若您想對所選監控區域的所有變更進行封鎖，選擇或清除**偵測或封鎖選定的檔案操作**核取方塊。
從控制中排除以下資料夾	未套用	使用此選項可以針對無需監控檔案操作的資料夾檢查排除的使用情況。當"檔案完整性監控"工作執行時，Kaspersky Embedded Systems Security 將略過指定為排除的監控範圍。
核對總和計算	未套用	使用此選項可以配置對檔案進行變更後的檔案核對總和計算。
設定檔案操作標記	考慮所有可用的檔案操作標記	使用此選項可以指定檔案操作標記集。如果在監控範圍內執行的檔案操作被一個或多個指定標記進行過特徵化，則 Kaspersky Embedded Systems Security 會產生一個稽核事件。
工作啟動排程	不設定工作的初次啟動排程	您可以配置按排程啟動工作的設定。

透過管理外掛程式管理"檔案完整性監控"

在本節中，學習如何透過管理外掛程式配置"檔案完整性監控"工作。

配置"檔案完整性監控"工作

配置一般"檔案完整性監控"工作設定：

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細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**"標籤，然後開啟"**內容：<政策名稱>**"視窗。
   - 要為單台受防護裝置配置應用程式，請選擇"**裝置**"標籤，然後開啟"**應用程式設定**"視窗。

     如果某個啟動卡巴斯基安全管理中心政策已套用於裝置，並且該政策封鎖對應用程式設定的變更，則無法在"**應用程式設定**"視窗中編輯這些設定。
4. 在**系統稽核**區段的**檔案完整性監控**子區段中，點擊**設定**按鈕。
   將開啟"**檔案完整性監控**"視窗。
5. 在顯示的視窗的"**檔案操作監控設定**"標籤中，配置以下設定：
   - 清除或選取**記錄監控中斷期間發生的檔案操作資訊**核取方塊。

當由於任何原因（拆除硬碟磁碟機、使用者停止工作、軟體錯誤）工作未執行時，該核取方塊可以啟用或停用"檔案完整性監控"設定中指定的檔案操作的監控。

如果選中該核取方塊，則當"檔案完整性監控"工作未執行時，Kaspersky Embedded Systems Security 將記錄所有監控範圍內的事件。

如果清除該核取方塊，則當工作未執行時，應用程式將不記錄監控範圍內的檔案操作。

預設將會選定該核取方塊。

- 清除或選中"**封鎖入侵 USN 記錄的嘗試**"核取方塊。

  該核取方塊用於啟用或停用對 USN 記錄的防護。

  如果選中該核取方塊，Kaspersky Embedded Systems Security 將封鎖刪除 USN 記錄或破壞 USN 記錄內容的嘗試。

  如果清除該核取方塊，則應用程式不會監控對 USN 記錄的變更。

  預設將會選定該核取方塊。

- 根據需要，選取或清除"**套用受信任區域**"核取方塊。

  如果選取了套用受信任區域核取方塊，配置在受信任區域的排除和受信任處理程序將套用到除了配置規則以外的監控範圍中。

  如果選取了套用受信任區域核取方塊，配置在受信任區域的排除和受信任處理程序將套用到監控範圍中。

  預設情況下，會取消勾選核取方塊。

- 新增工作要監控的監控範圍。

6. 在"**工作管理**"標籤上，基於排程設定用於啟動工作的工作設定。
7. 點擊"**確定**"以儲存變更。

Kaspersky Embedded Systems Security 將對正在執行的工作立即套用新設定。有關設定修改日期和時間的資訊將儲存在系統稽核記錄中。

配置監控規則

要新增監控範圍：

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細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**"標籤，然後開啟"**內容：<政策名稱>**"視窗。
   - 要為單台受防護裝置配置應用程式，請選擇"**裝置**"標籤，然後開啟"**應用程式設定**"視窗。

如果某個啟動卡巴斯基安全管理中心政策已套用於裝置，並且該政策封鎖對應用程式設定的變更，則無法在**"應用程式設定"**視窗中編輯這些設定。

4. 在**系統稽核**區段的**檔案完整性監控**子區段中，點擊**設定**按鈕。
   將開啟**"檔案完整性監控"**視窗。
5. 在**"監控範圍"**部分中，點擊**"新增"**按鈕。
   將開啟**"檔案操作監控規則"**視窗。
6. 透過以下方式之一新增監控範圍：
   - 如果要透過標準的 Microsoft Windows 對話方塊來選擇資料夾：
     a. 點擊**"瀏覽"**按鈕。
        將開啟標準的 Microsoft Windows **瀏覽資料夾**視窗。
     b. 在開啟的 **瀏器資料夾**中，選擇要監控操作的資料夾，然後點擊**"確定"**按鈕。
   - 如果想要手動指定監控範圍，請使用支援的遮罩新增路徑：
     - <*.ext> — 帶有 <ext> 副檔名的所有檔案，與其位置無關
     - <*\name.ext> — 帶有 <name> 名稱和 <ext> 副檔名的所有檔案，與其位置無關
     - <\dir*> — 位於 <\dir> 資料夾中的所有檔案
     - <\dir*\name.ext> — <\dir> 資料夾及其所有子資料夾中帶有 <name> 名稱和 <ext> 副檔名的所有檔案

當手動指定監控範圍時，請確保路徑為以下格式：<卷字母>:\<遮罩>。如果缺少磁區字母，則 Kaspersky Embedded Systems Security 將不會新增指定的監控範圍。

7. 在「**受信任使用者**」標籤中，點擊「**新增**」按鈕。
   將顯示標準的 Microsoft Windows**"選擇使用者或群組"**視窗。
8. 選擇在選定監控範圍中允許其檔案操作的使用者或群組，然後點擊**"確定"**按鈕。

預設情況下，Kaspersky Embedded Systems Security 將未列入受信任使用者清單的所有使用者視為不受信任，並為他們產生嚴重事件。針對受信任使用者，將編譯統計資料。

9. 選擇**"檔案操作標記"**標籤。
10. 執行以下操作，以根據需要選擇多個標記：
    a. 選擇**"基於以下標記偵測檔案操作"**選項。
    b. 在可用檔案操作清單中，選中要監控的操作旁邊的核取方塊。

預設情況下，Kaspersky Embedded Systems Security 將偵測所有檔案操作標記，已選擇**"基於所有可辨識的標記偵測檔案操作"**選項。

11. 如果要封鎖所選區域的所有檔案操作，請選取**偵測並封鎖所選檔案操作**核取方塊。
12. 如果執行操作後，您想要 Kaspersky Embedded Systems Security 計算檔案核對總和，請執行以下操作：
    a. **選中"如果可能，計算檔案的核對總和。**核對總和將可在工作報告中檢視"核取方塊。
    b. 在"**核對總和類型**"下拉清單中，選擇以下選項之一：
    - **MD5 雜湊**
    - **使用 SHA256 雜湊**
13. 如果您不希望監控所有檔案操作，則在可用檔案操作清單中，選中要監控的操作旁邊的核取方塊。
14. 根據需要新增排除的監控範圍：
    a. 選擇"**排除**"標籤。
    b. 選中"**將以下資料夾從控制範圍中排除**"核取方塊。
    c. 點擊"**新增**"按鈕。
    將開啟"**選擇要新增的資料夾**"視窗。
    d. 在開啟的視窗中，指定要從監控範圍中排除的資料夾。
    e. 點擊"**確定**"。
    指定的資料夾被新增到排除範圍清單。
15. 在"**檔案操作監控規則**"視窗中點擊"**確定**"。
    指定的規則設定將套用於"檔案完整性監控"工作的選定監控範圍。

透過應用程式主控台管理"檔案完整性監控"

在本節中，學習如何透過應用程式主控台配置"檔案完整性監控"工作。

配置"檔案完整性監控"工作設定

配置一般"檔案完整性監控"工作設定：

1. 在應用程式主控台樹狀目錄中，展開"**系統稽核**"節點。
2. 選擇"**檔案完整性監控**"子節點。
3. 在"**內容**"節點的結果窗格中，點擊"**檔案完整性監控**"連結。
「**工作設定**」視窗隨即出現。
4. 在"**一般**"標籤的視窗上，配置以下設定：
    a. 清除或選中"**記錄監控中斷期間發生的檔案操作資訊**"核取方塊。

當由於任何原因（拆除硬碟磁碟機、使用者停止工作、軟體錯誤）工作未執行時，該核取方塊可以啟用或停用"檔案完整性監控"設定中指定的檔案操作的監控。

如果選中該核取方塊，則當"檔案完整性監控"工作未執行時，Kaspersky Embedded Systems Security 將記錄所有監控範圍內的事件。

如果清除該核取方塊，則當工作未執行時，應用程式將不記錄監控範圍內的檔案操作。

預設將會選定該核取方塊。

b. 清除或選中"**封鎖入侵 USN 記錄的嘗試**"核取方塊。

該核取方塊用於啟用或停用對 USN 記錄的防護。

如果選中該核取方塊，Kaspersky Embedded Systems Security 將封鎖刪除 USN 記錄或破壞 USN 記錄內容的嘗試。

如果清除該核取方塊，則應用程式不會監控對 USN 記錄的變更。

預設將會選定該核取方塊。

c. 根據需要，選取或清除"**套用受信任區域**"核取方塊。

如果選取了套用受信任區域核取方塊，配置在受信任區域的排除和受信任處理程序將套用到除了配置規則以外的監控範圍中。

如果選取了套用受信任區域核取方塊，配置在受信任區域的排除和受信任處理程序將套用到監控範圍中。

預設情況下，會取消勾選核取方塊。

5. 在"**排程**"和"**進階**"標籤上，配置工作啟動排程。

6. 點擊"**確定**"以儲存變更。

Kaspersky Embedded Systems Security 將對正在執行的工作立即套用新設定。有關設定修改日期和時間的資訊將儲存在系統稽核記錄中。

配置監控規則

要新增監控範圍：

1. 在應用程式主控台樹狀目錄中，展開"**系統稽核**"節點。

2. 選擇"**檔案完整性監控**"子節點。

3. 在"**檔案操作監控規則**"節點的結果窗格中，點擊"**檔案完整性監控**"連結。

   將開啟"**檔案操作監控**"視窗。

4. 透過以下方式之一新增監控範圍：

   - 如果要透過標準的 Microsoft Windows 對話方塊來選擇資料夾：

     a. 在視窗的左側，點擊"**瀏覽**"按鈕。

     將顯示標準的 Microsoft Windows"**瀏覽資料夾**"視窗。

b. 在**瀏覽資料夾**視窗中，選擇要監控操作的資料夾，然後點擊**"確定"**按鈕。

c. 點擊**"新增"**按鈕可讓 Kaspersky Embedded Systems Security 開始監控指定監控範圍內的檔案操作。

- 如果想要手動指定監控範圍，請使用支援的遮罩新增路徑：
  - <*.ext> — 帶有 <ext> 副檔名的所有檔案，與其位置無關
  - <*\name.ext> — 帶有 <name> 名稱和 <ext> 副檔名的所有檔案，與其位置無關
  - <\dir*> — 位於 <\dir> 資料夾中的所有檔案
  - <\dir*\name.ext> — <\dir> 資料夾及其所有子資料夾中帶有 <name> 名稱和 <ext> 副檔名的所有檔案

當手動指定監控範圍時，請確保路徑為以下格式：<卷字母>:\<遮罩>。如果缺少磁區字母，則 Kaspersky Embedded Systems Security 將不會新增指定的監控範圍。

在螢幕的右側，**"規則敘述"**標籤將顯示受信任使用者和為此監控範圍選定的檔案操作標記。

5. 在新增的監控範圍清單中，選擇您要配置其設定的範圍。
6. 選擇**"受信任使用者"**標籤。
7. 點擊**"新增"**按鈕。
   將顯示標準的 Microsoft Windows**"選擇使用者或群組"**視窗。
8. 選擇針對選定的監控範圍 Kaspersky Embedded Systems Security 將視為受信任的使用者或群組。
9. 點擊**"確定"**。

預設情況下，Kaspersky Embedded Systems Security 將未列入受信任使用者清單的所有使用者視為不受信任，並為他們產生嚴重事件。針對受信任使用者，將編譯統計資料。

10. 選擇**"設定檔案操作標記"**標籤。
11. 如果需要，執行以下操作來選擇多個標記：

    a. 選擇**"根據以下標記偵測檔案操作"**選項。

    b. 在可用檔案操作清單中，選中要監控的操作旁邊的核取方塊。

預設情況下，Kaspersky Embedded Systems Security 將偵測所有檔案操作標記，即，已選擇**"根據所有可辨識的標記偵測檔案操作"**選項。

12. 如果要封鎖所選區域的所有檔案操作，請選取**偵測並封鎖所選檔案操作**核取方塊。
13. 如果執行操作後，您想要 Kaspersky Embedded Systems Security 計算檔案核對總和，請執行以下操作：

    a. **核對總和計算如果可能，在檔案變更後計算檔案最終版本的核對總和。 該核對總和將可在工作記錄中檢視。**"核對總和將可在工作記錄中檢視"核取方塊。

b. 在“**用演算法計算核對總和**”下拉清單中，選擇以下選項之一：

- **MD5 雜湊**。
- **SHA256 雜湊**.

14. 根據需要新增排除的監控範圍：

a. 選擇“**設定排除**”標籤。

b. 選中“**考慮排除的監控範圍**”核取方塊。

c. 點擊“**瀏覽**”按鈕。
將顯示標準的 Microsoft Windows“**瀏覽資料夾**”視窗。

d. 在**瀏覽資料夾**視窗中，指定要從監控範圍中排除的資料夾。

e. 點擊“**確定**”。

f. 點擊“**新增**”按鈕。
指定的資料夾被新增到排除範圍清單。

> 您也可以使用與用於指定監控範圍相同的遮罩來新增排除的監控範圍。

15. 點擊“**儲存**”按鈕以套用新的規則配置。

指定的規則設定將立刻套用到「**檔案完整性監控**」工作定義的監控範圍中。

透過 Web 外掛程式管理“檔案完整性監控”

在本節中，學習如何透過 Web 外掛程式配置“檔案完整性監控”工作。

配置“檔案完整性監控”工作

要透過 Web 外掛程式配置“檔案完整性監控”工作：

1. 在 Web 控制的主視窗中，選取**裝置 → 政策和設定檔案**。
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**”標籤。
4. 選擇“**系統稽核**”部分。
5. 點擊“**設定**”子區段中的“**檔案完整性監控**”。
6. 在顯示的“**檔案完整性監控**”視窗中，在“**檔案操作監控設定**”標籤上配置以下設定：

a. 清除或選中“**記錄監控中斷期間發生的檔案操作資訊**”核取方塊。

當由於任何原因（拆除硬碟磁碟機、使用者停止工作、軟體錯誤）工作未執行時，該核取方塊可以啟用或停用"檔案完整性監控"設定中指定的檔案操作的監控。

如果選中該核取方塊，則當"檔案完整性監控"工作未執行時，Kaspersky Embedded Systems Security 將記錄所有監控範圍內的事件。

如果清除該核取方塊，則當工作未執行時，應用程式將不記錄監控範圍內的檔案操作。

預設將會選定該核取方塊。

b. 清除或選中"**封鎖對 USN 記錄的入侵嘗試**"核取方塊。

該核取方塊用於啟用或停用對 USN 記錄的防護。

如果選中該核取方塊，Kaspersky Embedded Systems Security 將封鎖刪除 USN 記錄或破壞 USN 記錄內容的嘗試。

如果清除該核取方塊，則應用程式不會監控對 USN 記錄的變更。

預設將會選定該核取方塊。

c. 根據需要，選取或清除"**套用受信任區域**"核取方塊。

如果選取了套用受信任區域核取方塊，配置在受信任區域的排除和受信任處理程序將套用到除了配置規則以外的監控範圍中。

如果選取了套用受信任區域核取方塊，配置在受信任區域的排除和受信任處理程序將套用到監控範圍中。

預設情況下，會取消勾選核取方塊。

7. 在"**工作管理**"標籤上配置工作啟動排程。

8. 點擊"**確定**"以儲存變更。

Kaspersky Embedded Systems Security 將對正在執行的工作立即套用新設定。有關設定修改日期和時間的資訊將儲存在系統稽核記錄中。

配置監控規則

要新增監控範圍：

1. 在 Web 控制的主視窗中，選取**裝置 → 政策和設定檔案**。
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**"標籤。
4. 選擇"**系統稽核**"部分。
5. 點擊"**設定**"子區段中的"**檔案完整性監控**"。
6. 在顯示的"**檔案完整性監控**"視窗中，開啟"**檔案操作監控設定**"標籤。
7. 在"**USN 記錄**"部分中，點擊"**新增**"按鈕。

將顯示“**檔案操作監控規則**”視窗。

8. 在“ **監控此範圍的檔案操作** ”中，使用受支援的遮罩指定路徑：
   - <*.ext> – 帶有 <ext> 副檔名的所有檔案，與其位置無關
   - <*\name.ext> – 帶有 <name> 名稱和 <ext> 副檔名的所有檔案，與其位置無關
   - <\dir*> – 位於 <\dir> 資料夾中的所有檔案
   - <\dir*\name.ext> – <\dir> 資料夾及其所有子資料夾中帶有 <name> 名稱和 <ext> 副檔名的所有檔案

   當手動指定監控範圍時，請確保路徑為以下格式：<卷字母>:\<遮罩>。如果缺少磁區字母，則 Kaspersky Embedded Systems Security 將不會新增指定的監控範圍。

9. 在“**受信任使用者**”區段中，執行以下操作之一：
   - 點擊**新增**按鈕，然後在開啟的視窗中使用 SID 符號在**使用者名稱**欄位中指定使用者。
   - 點擊**從管理伺服器新增**按鈕，然後畫面上顯示的視窗中從清單中選取使用者。

   預設情況下，Kaspersky Embedded Systems Security 將未列入受信任使用者清單的所有使用者視為不受信任，並為他們產生嚴重事件。針對受信任使用者，將編譯統計資料。

10. 點擊“**確定**”。
11. 選擇“**檔案操作標記**”標籤。
12. 執行以下操作，以根據需要選擇多個標記：
    a. 選擇“**根據以下標記偵測檔案操作**”選項。
    b. 在可用檔案操作清單中，選中要監控的操作旁邊的核取方塊。

    預設情況下，Kaspersky Embedded Systems Security 將偵測所有檔案操作標記，已選擇“**根據所有可辨識的標記偵測檔案操作**”選項。

13. 如果要封鎖所選區域的所有檔案操作，請選取**偵測並封鎖所選檔案操作**核取方塊。
14. 如果執行操作後，您想要 Kaspersky Embedded Systems Security 計算檔案核對總和：
    a. **如果可能，計算檔案的核對總和。該核對總和將可在工作記錄中檢視**核對總和將可在工作報告中檢視”核取方塊。
    b. 在“**核對總和類型**”下拉清單中，選擇以下選項之一：
       - **SHA256 雜湊**
       - **MD5 雜湊**
15. 如果您不希望監控所有檔案操作，則在可用檔案操作清單中，選中要監控的操作旁邊的核取方塊。

16. 根據需要新增排除的監控範圍：

    a. 選擇**"排除"**標籤。

    b. 選中**"從控制中排除以下資料夾"**核取方塊。

    c. 點擊**"新增"**按鈕。
    將開啟**"選擇要新增的資料夾"**視窗。

    d. 在右側開啟的窗格中，指定要從監控範圍中排除的資料夾。

    e. 點擊**"確定"**。
    指定的資料夾被新增到排除範圍清單。

17. 在**檔案操作監控規則**視窗中點擊**檔案操作監控規則**。
    指定的規則設定將套用於"檔案完整性監控"工作的選定監控範圍。

註冊表存取監控

本節說明如何啟動和配置「註冊表存取監控」工作。

關於註冊表存取監控工作

「註冊表存取監控」工作的設計目的是為了追蹤針對工作設定中指定的監控範圍內的註冊表子目錄和參數執行的操作。您可以使用該工作來偵測可能對受防護裝置造成安全弱點的變更。

要啟動註冊表存取監控工作，您必須至少配置一個監控規則。

關於系統註冊表監控規則

註冊表存取監控工作是根據系統註冊表監控規則執行的。您可以使用規則觸發條件來配置觸發工作的條件，以及調整工作記錄中記錄的已偵測事件的重要性等級。

針對每個監控範圍指定了系統註冊表監控規則。

可以配置以下規則觸發條件：

- **操作**
- **註冊表值**
- **受信任使用者**

操作

當註冊表存取監控工作啟動時，Kaspersky Embedded Systems Security 會使用一組操作清單來監控註冊表（參見下表）。

如果偵測到指定為規則觸發條件的操作，則應用程式會記錄相應的事件。

已記錄事件的重要性等級不取決於選定的操作或事件的數量。

預設情況下，Kaspersky Embedded Systems Security 會考慮所有操作。您可以在工作規則設定中手動配置操作清單。

操作

操作	限制	作業系統
建立金鑰	• 對於 Windows XP 和 Windows Server 2003，如果新增**建立金鑰**到**操作**清單中，然後選擇**根據規則封鎖操作**模式，由於系統限制，不會在指定的作業系統中封鎖金鑰的建立。金鑰是透過傳送到事件記錄的相應通知建立的。	Windows XP 及更高版本

	• 如果要禁止透過註冊表編輯器建立特定參數，請為父註冊表參數建立規則並確保將**建立子參數**新增到**操作**清單，然後選擇**根據規則封鎖操作**模式。	
刪除鍵	如果要刪除父參數，對於已配置的註冊表參數請務必同時清除監控清單中**操作**選項的**刪除鍵**和**刪除子參數**，因為您只能刪除帶有子參數的父參數。	Windows XP 及更高版本
重新命名金鑰	N/A	Windows XP 及更高版本
變更金鑰安全設定	N/A	Windows Vista 及更高版本
刪除值	N/A	Windows XP 及更高版本
設定值	如果新增**設定值**到**操作**清單中，在參數規則中定義預設的**註冊表值**，然後選擇**根據規則封鎖操作**模式，則將不會建立金鑰，因為您只能使用預設值建立新金鑰。	Windows XP 及更高版本
建立子參數	N/A	Windows XP 及更高版本
刪除子參數	N/A	Windows XP 及更高版本
重新命名子參數	N/A	Windows XP 及更高版本
變更子參數安全設定	N/A	Windows Vista 及更高版本

註冊表值

除了註冊表參數監控之外，您還可以封鎖或監控現有的註冊表值變更。以下選項為可用選項：

- **設定值** – 建立新的註冊表值或變更現有的註冊表值
- **刪除值** – 刪除現有的註冊表值。

重新命名和變更安全設定不適用於註冊表值。

受信任使用者

預設情況下，應用程式將所有操作視為潛在安全入侵。受信任使用者清單為空。您可以透過在系統註冊表監控規則設定中建立受信任使用者清單來配置事件重要性等級。

不受信任使用者 – 監控範圍規則設定中的受信任使用者清單中未指定的任何使用者。如果 Kaspersky Embedded Systems Security 偵測到不受信任的使用者執行的操作，則「註冊表存取監控」工作將在工作記錄中記錄一個緊急事件。

受信任使用者 – 經過授權可在指定的監控範圍內執行操作的使用者或使用者群組。如果 Kaspersky Embedded Systems Security 偵測到受信任使用者執行的操作，則「註冊表存取監控」工作將在工作記錄中記錄一個資訊事件。

「註冊表存取監控」工作預設設定

註冊表存取監控工作的預設設定描述如下表。您可以在下列元件中變更這些設定值：

- 管理外掛程式
- 應用程式主控台
- Web 外掛程式

「註冊表存取監控」工作預設設定

設定	預設值	敘述
監控範圍	未定義	使用此選項可以定義要監控的父註冊表參數和子參數。為指定的監控範圍內的父註冊表參數和子健值產生監控事件。
操作	選擇操作清單的所有項目	使用此選項可以透過選取和清除相應的核取方塊來配置適用的操作清單。
註冊表值	未定義	使用此選項可以為定義的監控範圍新增、修改和刪除要監控的註冊表值。
受信任使用者	未定義	使用此選項可以指定被授權對指定註冊表健值執行定義操作的使用者和/或使用者群組。
工作模式	僅統計	您可以選擇工作模式為**根據規則封鎖操作**，或者您可以選擇**僅統計**為接收通知的模式。
套用信任區域	已停用	除了設定為規則外，您可以選擇或清除 套用受信任區域核取方塊，來套用受信任區域排除項目。
工作啟動排程	未定義	您可以配置按排程啟動工作的設定。

透過管理外掛程式管理「註冊表存取監控」

在本節中，學習如何透過管理外掛程式配置「註冊表存取監控」工作。

配置註冊表存取監控工作設定

要配置一般註冊表存取監控工作設定：

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細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"**標籤，然後開啟**"內容：<政策名稱>"**視窗。
   - 要為單台受防護裝置配置應用程式，請選擇**"裝置"**標籤，然後開啟**"應用程式設定"**視窗。

     如果某個啟動卡巴斯基安全管理中心政策已套用於裝置，並且該政策封鎖對應用程式設定的變更，則無法在**"應用程式設定"**視窗中編輯這些設定。
4. 在**登錄存取監控**子區段的**系統稽核**部分，點擊**設定**按鈕。

   登錄存取監控視窗隨即開啟。
5. 在**註冊表存取監控設定**標籤上，配置以下設定：
   - 在**工作模式**群組的清單中選擇所需的選項：
     - **根據規則封鎖操作**

       如果您選擇**根據規則封鎖操作**模式，Kaspersky Embedded Systems Security 會封鎖為監控範圍定義的**操作**。另外，如果選取了**套用受信任區域**核取方塊，Kaspersky Embedded Systems Security 不會封鎖**受信任區域**下定義的處理程序。

       預設情況下，會套用**僅統計**模式。
     - **僅統計**

       如果監控範圍選取了**僅統計**模式，Kaspersky Embedded Systems Security 軟體會根據配置的規則編譯註冊表參數操作的統計資訊。另外，如果選取了**套用受信任區域**核取方塊，Kaspersky Embedded Systems Security 不會編譯**受信任區域**下定義的處理程序統計資料。

       預設情況下，會套用**僅統計**模式。
   - 根據需要，選取或清除**"套用受信任區域"**核取方塊。

     如果選取了**套用受信任區域**核取方塊，配置在**受信任區域**的**受信任處理程序**將套用到除了配置規則以外的監控範圍中。

     如果選取了**套用受信任區域**核取方塊，配置在**受信任區域**的**受信任處理程序**將套用到監控範圍中。

     預設情況下，會取消勾選核取方塊。
6. 新增工作要監控的監控範圍。
7. 在**工作管理**標籤上，配置工作的排程設定。
8. 點擊**"確定"**以儲存變更。

Kaspersky Embedded Systems Security 將對正在執行的工作立即套用新設定。有關設定修改日期和時間的資訊將儲存在系統稽核記錄中。

配置監控規則

監控規則會依次套用，因為它們位於配置的規則清單中。

要新增監控範圍：

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細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"**標籤，然後開啟**"內容：<政策名稱>"**視窗。
   - 要為單台受防護裝置配置應用程式，請選擇**"裝置"**標籤，然後開啟**"應用程式設定"**視窗。

     如果某個啟動卡巴斯基安全管理中心政策已套用於裝置，並且該政策封鎖對應用程式設定的變更，則無法在**"應用程式設定"**視窗中編輯這些設定。
4. 在**系統稽核**部分的**登錄存取監控**子區段中，點擊**設定**按鈕。
   登錄存取監控視窗隨即開啟。
5. 在**監控範圍內的註冊表操作**部分，點擊**新增**按鈕。
6. 在**註冊表存取監控區域**視窗中新增監控範圍，使用**支援的遮罩**指定一個路徑。

您可以使用 ? 和 * 作為輸入路徑時的遮罩。

如果您是對根註冊表參數輸入路徑，請確保指定不含遮罩的完整路徑，例如 HKEY_USERS。以下是有效的根註冊表參數清單：

- HKEY_LOCAL_MACHINE
- HKLM
- HKEY_CURRENT_USER
- HKCU
- HKEY_USERS
- HKUS
- HKU
- HKEY_CURRENT_CONFIG
- HKEY_CLASSES_ROOT
- HKCR

建立規則時，避免為根目錄參數使用受支援的遮罩。
如果只指定了一個根目錄參數，如 HKEY_CURRENT_USER，或對所有帶有遮罩的子參數指定了一個根目錄參數，如 HKEY_CURRENT_USER*，則會產生大量關於尋找指定子參數的通知，從而導致系統效能下降問題。如果指定根目錄參數，如 HKEY_CURRENT_USER，或為所有子參數指定了帶有遮罩的根目錄參數，如 HKEY_CURRENT_USER*，並選擇**根據規則封鎖操作**模式，系統將無法讀取或變更作業系統執行所需的參數並且無法回應。

7. 在**新增**標籤上，根據需要配置操作清單。

8. 如果您想監控某些**註冊表值**，請執行下列操作：

   - 在「**註冊表值**」標籤中，點擊「**新增**」按鈕。
   - 在**註冊表值規則**視窗中，輸入 **值遮罩**並設定 **受控制的操作**。
   - 點擊「**確定**」以儲存變更。

9. 如果您想定義**受信任使用者**，請執行下列操作：

   - 在「**受信任使用者**」標籤中，點擊「**新增**」按鈕。
   - 在**選擇使用者或群組**視窗，選擇有權執行定義操作的使用者或使用者群組。
   - 點擊**“ 確定**”以儲存變更。

預設情況下，Kaspersky Embedded Systems Security 將未列入受信任使用者清單的所有使用者視為不受信任，並為他們產生嚴重事件。針對受信任使用者，將編譯統計資料。

10. 在「**註冊表存取監控區域**」視窗中點擊「**確定**」。

指定的規則設定將立刻套用到「**登錄存取監控**」工作定義的監控範圍中。

透過管理主控台管理「註冊表存取監控」

在本節中，學習如何透過應用程式主控台配置「註冊表存取監控」工作。

配置註冊表存取監控工作設定

要配置一般註冊表存取監控工作設定：

1. 在應用程式主控台樹狀目錄中，展開"**系統稽核**"節點。
2. 選擇「**登錄存取監控**」子節點。
3. 在「**登錄存取監控**」節點的結果窗格中，點擊「**內容**」連結。
   「**工作設定**」視窗隨即出現。
4. 在「**一般**」標籤的「**工作設定**」視窗上，配置以下設定：
   - 在**工作模式**群組的清單中選擇所需的選項：
     - **根據規則封鎖操作**

       如果您選擇**根據規則封鎖操作**模式，Kaspersky Embedded Systems Security 會封鎖為監控範圍定義的**操作**。另外，如果選取了**套用受信任區域**核取方塊，Kaspersky Embedded Systems Security 不會封鎖**受信任區域**下定義的處理程序。

       預設情況下，會套用**僅統計**模式。

     - **僅統計**

       如果監控範圍選取了**僅統計**模式，Kaspersky Embedded Systems Security 軟體會根據配置的規則編譯註冊表參數操作的統計資訊。另外，如果選取了**套用受信任區域**核取方塊，Kaspersky Embedded Systems Security 不會編譯**受信任區域**下定義的處理程序統計資料。

       預設情況下，會套用**僅統計**模式。

   - 根據需要，選取或清除"**套用受信任區域**"核取方塊。

如果選取了**套用受信任區域**核取方塊，配置在**受信任區域**的**受信任處理程序**將套用到除了配置規則以外的監控範圍中。

如果選取了**套用受信任區域**核取方塊，配置在**受信任區域**的**受信任處理程序**將套用到監控範圍中。

預設情況下，會取消勾選核取方塊。

5. 在"**排程**"和"**進階**"標籤上，配置工作啟動排程。

6. 點擊"**確定**"以儲存變更。

Kaspersky Embedded Systems Security 將對正在執行的工作立即套用新設定。有關設定修改日期和時間的資訊將儲存在系統稽核記錄中。

配置監控規則

監控規則會依次套用，因為它們位於配置的規則清單中。

要新增監控範圍：

1. 在應用程式主控台樹狀目錄中，展開"**系統稽核**"節點。

2. 選擇「**登錄存取監控**」子節點。

3. 在「**登錄存取監控**」節點的結果窗格中，點擊「**註冊表存取監控規則**」連結。
   註冊表存取監控視窗隨即開啟。

4. 在**註冊表存取監控**視窗中，使用支援的遮罩對**新增系統註冊表參數**指定一個路徑並點擊**新增**按鈕。

建立規則時，避免在根參數使用支援的遮罩。
如果只指定了一個根參數，如 HKEY_CURRENT_USER，或為所有子參數指定了帶有遮罩的根參數，如 HKEY_CURRENT_USER*，則會產生大量關於尋找指定子參數的通知，從而導致系統效能下降問題。
如果您指定一個根參數，例如 HKEY_CURRENT_USER，或為所有子參數指定了帶有遮罩的根參數，例如 HKEY_CURRENT_USER*，並選擇**根據規則封鎖操作**模式，系統將無法讀取或變更執行作業系統所需的金鑰並且無法回應。

5. 在**操作**標籤選定的監控區域，根據需求配置適用的操作清單。

6. 如果您想監控某些**註冊表值**，請執行下列操作：

   a. 在「**註冊表值**」標籤中，點擊「**新增**」按鈕。

   b. 在**註冊表值規則**視窗中，輸入 **值遮罩**並設定所需的 **控制操作**。

   c. 點擊「**確定**」以儲存變更。

7. 如果您想定義**受信任使用者**，請執行下列操作：

   a. 在「**受信任使用者**」標籤中，點擊「**新增**」按鈕。

b. 在**選擇使用者或群組**視窗，選擇有權執行定義操作的使用者或使用者群組。

c. 點擊「**確定**」以儲存變更。

預設情況下，Kaspersky Embedded Systems Security 將未列入受信任使用者清單的所有使用者視為不受信任，並為他們產生嚴重事件。針對受信任使用者，將編譯統計資料。

8. 在**註冊表存取監控區域**視窗中點擊**儲存**。
指定的規則設定將立刻套用到「**登錄存取監控**」工作定義的監控範圍中。

透過 Web 外掛程式管理「註冊表存取監控」

在本節中，學習如何透過 Web 外掛程式配置「註冊表存取監控」工作。

配置註冊表存取監控工作

要透過 Web 外掛程式配置「註冊表存取監控」工作：

1. 在 Web 控制的主視窗中，選取**裝置 → 政策和設定檔案**。
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**"標籤。
4. 選擇"**系統稽核**"部分。
5. 點擊**登錄存取監控**子區段中的**設定**。
6. 在**登錄存取監控**視窗的**登錄存取監控設定**標籤，配置以下設定：
   - 在**工作模式**群組的清單中選擇所需的選項：
     - **根據規則封鎖操作**

       如果您選擇**根據規則封鎖操作**模式，Kaspersky Embedded Systems Security 會封鎖為監控範圍定義的**操作**。另外，如果選取了**套用受信任區域**核取方塊，Kaspersky Embedded Systems Security 不會封鎖**受信任區域**下定義的處理程序。

       預設情況下，會套用**僅統計**模式。

     - **僅統計**

       如果監控範圍選取了**僅統計**模式，Kaspersky Embedded Systems Security 軟體會根據配置的規則編譯註冊表參數操作的統計資訊。另外，如果選取了**套用受信任區域**核取方塊，Kaspersky Embedded Systems Security 不會編譯**受信任區域**下定義的處理程序統計資料。

       預設情況下，會套用**僅統計**模式。

- 根據需要，選取或清除“**套用信任區域**”核取方塊。

  如果選取了**套用受信任區域**核取方塊，配置在**受信任區域**的**受信任處理程序**將套用到除了配置規則以外的監控範圍中。

  如果選取了**套用受信任區域**核取方塊，配置在**受信任區域**的**受信任處理程序**將套用到監控範圍中。

  預設情況下，會取消勾選核取方塊。

7. 在“**工作管理**”標籤上配置工作啟動排程。

8. 點擊“**確定**”以儲存變更。

Kaspersky Embedded Systems Security 將對正在執行的工作立即套用新設定。有關設定修改日期和時間的資訊將儲存在系統稽核記錄中。

配置監控規則

監控規則會依次套用，因為它們位於配置的規則清單中。

1. 在 Web 控制的主視窗中，選取**裝置 → 政策和設定檔案**。

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**”標籤。

4. 選擇“**系統稽核**”部分。

5. 點擊**登錄存取監控**子區段中的**設定**。

6. 在開啟的「**登錄存取監控**」視窗中，開啟「**登錄存取監控設定**」標籤。

7. 在「**登錄存取監控規則**」部分，點擊「**新增**」按鈕。

8. 在**登錄存取監控範圍**視窗中，使用**支援的遮罩**為**監控此範圍的登錄操作**指定一個路徑。

您可以使用 ? 和 * 作為輸入路徑時的遮罩。

如果您是對根註冊表參數輸入路徑，請確保指定不含遮罩的完整路徑，例如 HKEY_USERS。以下是有效的根註冊表參數清單：

- HKEY_LOCAL_MACHINE
- HKLM
- HKEY_CURRENT_USER
- HKCU
- HKEY_USERS
- HKUS
- HKU
- HKEY_CURRENT_CONFIG
- HKEY_CLASSES_ROOT
- HKCR

建立規則時，避免在根參數使用支援的遮罩。
如果只指定了一個根參數，如 HKEY_CURRENT_USER，或為所有子參數指定了帶有遮罩的根參數，如 HKEY_CURRENT_USER*，則會產生大量關於尋找指定子參數的通知，從而導致系統效能下降問題。
如果您指定一個根參數，例如 HKEY_CURRENT_USER，或為所有子參數指定了帶有遮罩的根參數，例如 HKEY_CURRENT_USER*，並選擇**根據規則封鎖操作**模式，系統將無法讀取或變更執行作業系統所需的金鑰並且無法回應。

9. 在**操作**標籤選定的監控區域，根據需求配置適用的操作清單。
10. 如果您想監控某些**註冊表值**，請執行下列操作：
    a. 在「**註冊表值**」標籤中，點擊「**新增**」按鈕。
    b. 在**註冊表值規則**視窗中，輸入 **值遮罩**並設定所需的**操作清單**。
    c. 點擊「**確定**」以儲存變更。
11. 如果您想定義**受信任使用者**，請執行下列操作：
    a. 在「**受信任使用者**」標籤中，點擊「**新增**」按鈕。
    b. 輸入**使用者名稱**或點擊**設定 SID 每個人**，以定義授權執行選定操作的使用者。
    c. 點擊「**確定**」以儲存變更。

預設情況下，Kaspersky Embedded Systems Security 將未列入受信任使用者清單的所有使用者視為不受信任，並為他們產生嚴重事件。針對受信任使用者，將編譯統計資料。

12. 在**登錄存取監控範圍**視窗中點擊**確定**以儲存變更。

    指定的規則設定將立刻套用到「**登錄存取監控**」工作定義的監控範圍中。

記錄審查

本節包含有關“記錄審查”工作和工作設定的資訊。

關於“記錄審查”工作

當“記錄審查”工作執行時，Kaspersky Embedded Systems Security 將根據 Windows 事件記錄的審查結果監控受防護環境的完整性。應用程式在偵測到可能表示嘗試進行實體攻擊的異常行為時會通知管理員。

Kaspersky Embedded Systems Security 會分析 Window 事件記錄，並根據使用者指定的規則或啟發式分析的設定（工作用它來審查記錄）來識別入侵。

預定義規則和啟發式分析

透過套用基於現有啟發的預定義規則，可以使用“記錄審查”工作來監控受防護系統的狀態。啟發式分析可識別受防護裝置上的異常活動，這些異常活動可作為嘗試攻擊的憑證。用於辨識異常行為的範本包括在預定義規則設定中的可用規則內。

“記錄審查”工作的規則清單中包含七條規則。您可以啟用或停用任一規則。不能刪除現有規則或建立新規則。

可以為監控以下操作事件的規則配置觸發條件：

- 密碼暴力破解偵測
- 網路登入偵測

還可在工作設定中配置排除。當登入由受信任使用者執行或從受信任的 IP 位址執行時，不會啟動啟發式分析。

如果工作不使用啟發式分析，則 Kaspersky Embedded Systems Security 不會使用啟發來審查 Windows 記錄。預設情況下，啟用啟發式分析。

當套用規則時，應用程式將在“記錄審查”工作記錄中記錄一個*緊急事件*。

自訂記錄審查工作的規則

可以使用規則設定來指定和變更在 Windows 記錄中偵測到選定事件時的觸發規則條件。預設情況下，記錄審查規則的清單包含四條規則。您可以啟用和停用這些規則、刪除規則以及編輯規則設定。

可以為每種規則配置以下規則觸發條件：

- Windows 事件記錄中的記錄識別碼清單。

  如果事件內容包含規則中指定的事件識別碼，則當在 Windows 事件記錄中建立新的記錄時將觸發該規則。也可以為每個指定的規則新增和刪除識別碼。

- 事件來源。

  對於每條規則，都可以在 Windows 事件記錄內定義一個記錄。應用程式將僅在此記錄中搜尋帶有指定事件識別碼的記錄。您可以選擇其中一個標準記錄（應用程式、安全性或系統）或在來源選擇欄位中輸入名稱來指定自訂記錄。

應用程式不會驗證指定的記錄是否確實存在於 Windows 事件記錄中。

觸發規則後，Kaspersky Embedded Systems Security 將在"記錄審查"工作記錄中記錄一個緊急事件。

預設情況下，記錄審查工作套用自訂規則。

在啟動"記錄審查"工作前，請確保系統系統稽核記錄政策已正確設定。有關詳細資訊，請參見 Microsoft 文章。

"記錄審查"工作預設設定

預設情況下，"記錄審查"工作具有下表所述的設定。您可以變更這些設定值。

"記錄審查"工作預設設定

設定	預設值	敘述
對"記錄審查"套用自訂規則	未套用。	您可以啟用、停用、新增或修改自訂規則。
針對記錄審查套用預定義規則	已套用。	您可以啟用或停用啟發式分析，它可以偵測受防護裝置上的異常活動。
暴力破解攻擊偵測	每 300 秒 10 次登入失敗。	您可以設定嘗試次數和使用的時間範圍，這將被視為啟發式分析的觸發器。
網路登入	上午 12:00:00。	您可以指定時間間隔的開始和結束時間，在此時間間隔中 Kaspersky Embedded Systems Security 將登入嘗試視為異常活動。
排除	未套用。	您可以指定不會觸發啟發式分析的使用者和 IP 位址。
工作啟動排程	不設定工作的初次啟動排程。	您可以配置按排程啟動工作的設定。

透過管理外掛程式管理記錄審查規則

在本節中，學習如何透過管理外掛程式新增和配置記錄審查規則。

配置預定義工作規則

執行以下操作為"記錄審查"工作配置預定義規則：

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細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"**標籤，然後開啟**"內容：<政策名稱>"**視窗。
- 要為單台受防護裝置配置應用程式，請選擇**"裝置"**標籤，然後開啟**"應用程式設定"**視窗。

  如果某個啟動卡巴斯基安全管理中心政策已套用於裝置，並且該政策封鎖對應用程式設定的變更，則無法在**"應用程式設定"**視窗中編輯這些設定。

4. 在**"系統稽核"**部分中，點擊**"記錄審查"**子區段中的**"設定"**按鈕。
   將開啟**"記錄審查"**視窗。
5. 選擇**"預定義規則"**標籤。
6. 選中或清除**"針對記錄審查套用預定義規則"**核取方塊。

   為了能夠執行工作，必須選擇至少一種記錄審查規則。

7. 從預定義規則清單中選擇要套用的規則：
   - 系統中存在可能的暴力破解攻擊的模式。
   - 系統中存在可能的 Windows 事件記錄濫用的模式。
   - 偵測到表示已安裝新服務的異常活動。
   - 偵測到使用顯式憑證的異常登入。
   - 系統中存在可能的 Kerberos 偽造 PAC (MS14-068) 攻擊的模式。
   - 偵測到特權內建群組 Administrators 發出的異常操作。
   - 在網路登入工作階段期間偵測到異常活動。
8. 要配置選定規則，請點擊**"進階設定"**按鈕。
   將開啟**"記錄審查"**視窗。
9. 在**"暴力破解攻擊偵測"**部分中，設定用作啟發式分析觸發器的嘗試次數和時間範圍。
10. 在**"網路登入偵測"**部分中，指定時間間隔的開始和結束時間，在此時間間隔中 Kaspersky Embedded Systems Security 將登入嘗試視為異常活動。
11. 選擇**"排除"**標籤。
12. 執行以下操作新增受信任使用者：
    a. 點擊**"瀏覽"**按鈕。
    b. 選擇使用者。
    c. 點擊**"確定"**。
       選定的使用者將被新增到受信任使用者清單中。
13. 執行以下操作新增受信任的 IP 位址：

a. 輸入 IP 位址。

b. 點擊**"新增"**按鈕。

14. 輸入的 IP 位址將被新增到受信任的 IP 位址清單中。

15. 在**"工作管理"**標籤上配置工作啟動排程。

16. 在**記錄審查**視窗中點擊**確定**。

儲存記錄審查工作配置。

透過管理外掛程式新增記錄審查規則

執行以下操作可新增和配置新的自訂記錄審查規則：

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細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"**標籤，然後開啟**"內容：<政策名稱>"**視窗。
   - 要為單台受防護裝置配置應用程式，請選擇**"裝置"**標籤，然後開啟**"應用程式設定"**視窗。

   如果某個啟動卡巴斯基安全管理中心政策已套用於裝置，並且該政策封鎖對應用程式設定的變更，則無法在**"應用程式設定"**視窗中編輯這些設定。

4. 在**"系統稽核"**部分中，點擊**"記錄審查"**子區段中的**"設定"**按鈕。
   將開啟**"記錄審查"**視窗。

5. 在**"自訂規則"**標籤上，選中或清除**"套用記錄審查的自訂規則"**標籤。

   可以控制是否對記錄審查套用預設的規則。選擇您要對記錄審查套用的規則所對應的核取方塊。

6. 要新增新的自訂規則，請點擊**"新增"**按鈕。
   將開啟**"自訂記錄審查規則"**視窗。

7. 在**"一般"**部分中，指定有關新規則的以下資訊：

   - **規則名稱**
   - **來源**

8. 在**"已觸發的事件 ID"**部分中，指定將觸發規則的事件 ID：

   a. 輸入 ID。

   b. 點擊**"新增"**按鈕。

輸入的事件 ID 將新增到清單中。可以為每個規則新增無限數量的識別碼。

9. 點擊**"確定"**。
   記錄審查規則即新增到規則清單中。

透過應用程式主控台管理記錄審查規則

在本節中，學習如何透過應用程式主控台新增和配置記錄審查規則。

配置預定義工作規則

執行以下操作可以為記錄審查工作配置啟發式分析：

1. 在應用程式主控台樹狀目錄中，展開**"系統稽核"**節點。
2. 選擇**"記錄審查"**子節點。
3. 在**"內容"**節點的結果窗格中，點擊**"記錄審查"**連結。
   將開啟**"工作設定"**視窗。
4. 選擇**"預定義規則"**標籤。
5. 選中或清除**"針對記錄審查套用預定義規則"**核取方塊。

   > 為了能夠執行工作，必須選擇至少一種記錄審查規則。

6. 從預定義規則清單中選擇要套用的規則：
   - 系統中存在可能的暴力破解攻擊的模式。
   - 系統中存在可能的 Windows 事件記錄濫用的模式。
   - 偵測到表示已安裝新服務的異常活動。
   - 偵測到使用顯式憑證的異常登入。
   - 系統中存在可能的 Kerberos 偽造 PAC (MS14-068) 攻擊的模式。
   - 偵測到特權內建群組 Administrators 發出的異常操作。
   - 在網路登入工作階段期間偵測到異常活動。
7. 要設定選定的規則，請轉至**"延伸"**標籤。
8. 在**"暴力破解攻擊偵測"**部分中，設定用作啟發式分析觸發器的嘗試次數和時間範圍。
9. 在**"網路登入"**部分中，指定時間間隔的開始和結束時間，在此時間間隔中 Kaspersky Embedded Systems Security 將登入嘗試視為異常活動。

10. 選擇“**排除**”標籤。
11. 執行以下操作新增受信任使用者：
    a. 點擊“**瀏覽**”按鈕。
    b. 選擇使用者。
    c. 點擊“**確定**”。
    選定的使用者將被新增到受信任使用者清單中。
12. 執行以下操作新增受信任的 IP 位址：
    a. 輸入 IP 位址。
    b. 點擊“**新增**”按鈕。
    輸入的 IP 位址將被新增到受信任的 IP 位址清單中。
13. 選擇“**排程**”和“**進階**”標籤以配置工作啟動排程。
14. 在**工作設定**視窗中點擊**確定**。
    儲存記錄審查工作配置。

透過應用程式主控台新增記錄審查規則

要新增和配置新的自訂記錄審查規則：

1. 在應用程式主控台樹狀目錄中，展開“**系統稽核**”節點。
2. 選擇“**記錄審查**”子節點。
3. 在“**記錄審查**”節點的結果窗格中，點擊“**記錄審查規則**”連結。
4. 將開啟“**記錄審查規則**”視窗。
5. **對記錄審查套用自訂規則。在選中此核取方塊之前，不套用已配置的規則。**“核對總和將可在工作記錄中檢視”核取方塊。

   可以控制是否對“記錄審查”工作套用預定義的規則。選擇您要對記錄審查套用的規則所對應的核取方塊。

6. 要建立新的自訂規則：
    a. 輸入新規則的名稱。
    b. 點擊“**新增**”按鈕。
    建立的規則將新增到一般規則清單中。
7. 要配置任何規則：
    a. 從清單中選擇一個規則。

在視窗的右側區域中，**"敘述"**標籤將顯示有關該規則的一般資訊。

新規則的敘述為空白。

b. 選擇**"規則敘述"**標籤。

8. 在**"一般"**部分中，指定有關新規則的以下資訊：

- **規則名稱**
- **記錄名稱**
- **來源**

9. 在**"事件識別碼"**部分中，指定將觸發規則的事件 ID：

a. 輸入事件 ID。

b. 點擊**"新增"**按鈕。
輸入的事件 ID 將新增到清單中。可以為每個規則新增無限數量的識別碼。

10. 點擊**"儲存"**按鈕。
將套用已配置的記錄審查規則。

透過 Web 外掛程式管理記錄審查規則

要透過 Web 外掛程式新增記錄審查規則：

1. 在 Web 控制的主視窗中，選取**裝置 → 政策和設定檔案**。
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"**標籤。
4. 選擇**"系統稽核"**部分。
5. 在**"設定"**子區段中點擊**"記錄審查"**。
6. 按下表所述配置設定。

"記錄審查"工作設定

設定	敘述
對"記錄審查"套用自訂規則	您可以啟用、停用、新增或修改自訂規則。 表格中提供設定及自訂規則清單。
針對記錄審查套用預定義規則	您可以啟用或停用啟發式分析，它可以偵測受防護裝置上的異常活動。 表格中提供設定及自訂規則清單。
如果以定義的頻率輸入不正確的密碼，則偵測為暴力破解攻擊	您可以設定嘗試次數和使用的時間範圍，這將被視為啟發式分析的觸發器。

如果在定義的時段內登入，則偵測為網路登入	您可以指定時間間隔的開始和結束時間，在此時間間隔中 Kaspersky Embedded Systems Security 將登入嘗試視為異常活動。
使用者排除	您可以指定不會觸發啟發式分析的使用者。
排除的 IP 位址	您可以指定不會觸發啟發式分析的 IP 位址。
工作管理	您可以配置按排程啟動工作的設定。

自訂掃描

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性設定。

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：

- Kaspersky Embedded Systems Security 每次啟動時都會執行“在作業系統啟動時掃描”工作。Kaspersky Embedded Systems Security 將掃描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 每次執行該工作時，都會建立未感染的開機磁區的副本。如果在這些磁區中偵測到威脅，則下次工作啟動時，會將這些磁區取代為備份副本。

  如果受防護裝置在睡眠或休眠模式後喚醒，則可能不會執行“在作業系統啟動時掃描”工作。僅當受防護裝置重新啟動或在完全關閉後啟動時才執行該工作。

- 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。應用程式會掃描系統資料夾中的檔案，例如 %windir%\system32 中的檔案。Kaspersky Embedded Systems Security 將套用與建議等級相應的安全設定。您可以修改“關鍵區域掃描”工作的設定。

- 預設在每次資料庫更新後依排程執行“隔離區掃描”工作。無法修改“隔離區掃描”工作範圍。

- “應用程式完整性控制”工作每天執行。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。

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樹狀目錄或清單的形式顯示。預設情況下，受防護裝置的網路檔案資源以清單圖示模式顯示。

在管理外掛程式中，只有清單視圖可用。

若要在應用程式主控台中以樹狀檢視模式顯示網路檔案資源，

請開啟“**設定掃描範圍**”視窗中的下拉清單，然後選擇“**樹狀檢視**”。

項或節點將顯示在受防護裝置檔案資源的清單檢視或樹狀檢視模式中，如下所示：

☑ 節點包括在掃描範圍內。

☐ 此節點已從掃描範圍中排除。

☑ 該節點至少有一個子節點排除在掃描範圍之外，或子節點的安全設定與父節點的安全設定不同（僅限樹狀檢視模式）。

如果選擇了所有子節點，但未選擇父節點，則顯示 ☑ 圖示。在這種情況下，在為所選子節點建立了掃描範圍後，如果父節點所包含的檔案和資料夾發生變更，將自動略過這些變更。

使用應用程式主控台，您還可以新增虛擬磁碟機到掃描範圍中。虛擬節點的名稱以藍色字體顯示。

安全性設定

在所選的自訂掃描工作中，若要修改預設安全性設定，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，或為裝置檔案資源樹狀目錄或清單中的不同節點或項配置不同設定。

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：

- 從三個預定義的安全等級中選擇一個等級（**最佳效能**、**建議**或**最佳防護**）。
- 在受防護裝置檔案資源樹狀目錄或清單中手動變更選定節點或項的安全性設定（安全等級變更為**"自訂"**）。

您可以將一組節點設定儲存為範本，以便隨後套用至其他節點。

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樹狀目錄或清單顯示在**"設定掃描範圍"**視窗中。

檔案資源樹狀目錄或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：

- **我的電腦**。Kaspersky Embedded Systems Security 掃描整個受防護裝置。
- **本機磁碟**。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。
- **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。
- **網路**。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。

- **系統記憶體**。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。
- **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。
- **共用資料夾**。您可以將受防護裝置上的共用資料夾包含在掃描範圍中。
- **虛擬磁碟機**。虛擬資料夾、檔案以及連線到受防護裝置的磁碟機可包含在掃描範圍內，例如，一般叢集磁碟機。

  使用 SUBST 指令建立的虛擬磁碟機不會顯示在應用程式主控台的受防護裝置檔案資源樹狀目錄中。為了掃描虛擬磁碟機上的物件，請將與虛擬磁碟機關聯的受防護裝置資料夾包含在掃描範圍中。

預設情況下，您可以在網路檔案資源樹狀目錄中檢視和配置預定義掃描範圍；還可以在網路檔案資源清單形成期間在設定掃描範圍中向該清單新增預定義範圍。

預設情況下，"自訂掃描"工作在以下範圍下執行：

- "在作業系統啟動時掃描"工作：
  - **本機磁碟**
  - **卸除式磁碟機**
  - **系統記憶體**
- 關鍵區域掃描：
  - **本機磁碟**（排除 Windows 資料夾）
  - **卸除式磁碟機**
  - **系統記憶體**
  - **啟動物件**
- 其他工作：
  - **本機磁碟**（排除 Windows 資料夾）
  - **卸除式磁碟機**
  - **系統記憶體**
  - **啟動物件**
  - **共用資料夾**

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。該應用程式支援新的 OneDrive 檔案隨需功能。

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 自訂檔案"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"工作的防護範圍中。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 。這樣該檔案可以被"即時檔案防護"工作處理。
- 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。
- 應用程式控制規則產生和使用：您可以使用"應用程式啟動控制規則產生器"工作為 和 檔案建立允許和拒絕規則。"應用程式啟動控制"工作應用"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"工作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 iChecker 技術"、**"使用 iSwift 技術"**、**"使用啟發式分析"**和**"在檔案中檢查 Microsoft 簽章"**安全性設定並未包含在預設安全等級設定中。如果**"使用 iChecker 技術"**、**"使用 iSwift 技術"**、**"使用啟發式分析"**和**"在檔案中檢查 Microsoft 簽章"**等設定發生改變，您選擇的預設安全等級不會變更。

可以為裝置檔案資源樹狀目錄中的選定節點套用以下預定義安全等級之一：**"最佳效能"**、**"建議"**和**"最佳防護"**。每個等級都包含其自有的預定義安全設定（請參閱下表）。

最佳效能

如果您的網路除了在受防護裝置上使用 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**"最佳效能"**安全等級。

建議

"建議"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"**安全等級。

最佳防護

如果組織的網路有更高的裝置安全要求，則建議使用**"最佳防護"**安全等級。

預定義安全等級和相應的安全性設定值

選項	安全等級		
	最佳效能	建議	最佳防護
掃描物件	依格式	所有物件	所有物件
僅掃描新增與變更過的檔案	已啟用	已停用	已停用
對受感染物件和其他物件執行的操作	解毒。解毒失敗則刪除	執行建議的操作（解毒。解毒失敗則刪除）	解毒。解毒失敗則刪除
對可疑物件執行的操作	隔離	執行建議的操作（隔離）	隔離
排除檔案	否	否	否
不偵測	否	否	否
超過以下時間則停止掃描 (秒)	60 秒	否	否
不掃描超過此值複合檔案 (MB)	8 MB	否	否
掃描 NTFS 交換資料串流	是	是	是

掃描開機磁區和 MBR	是	是	是
掃描複合檔案	• SFX 壓縮檔案* • 封裝的物件* • 內嵌的 OLE 物件* *僅新物件和已修改的物件	• SFX 壓縮檔案* • 封裝的物件* • 內嵌的 OLE 物件* *所有物件	• 壓縮檔案* • SFX 壓縮檔案* • 電子郵件資料庫* • 純文字郵件* • 封裝的物件* • 內嵌的 OLE 物件* *所有物件

關於卸除式磁碟機掃描

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。

Kaspersky Embedded Systems Security 使用自訂掃描工作掃描卸除式磁碟機。當卸除式磁碟機已連線並在完成掃描後刪除工作時，應用程式會自動建立新的自訂掃描工作。系統會根據為卸除式磁碟機掃描定義的預定義安全等級來執行建立的工作。您不能配置臨時自訂掃描工作的設定。

如果您已安裝不帶病毒資料庫的 Kaspersky Embedded Systems Security，則將無法執行卸除式磁碟機掃描。

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工作封鎖，則應用程式不會掃描卸除式磁碟機。應用程式不會掃描 MTP 連線的行動裝置。

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記錄中。

可以變更卸除式磁碟機掃描元件的設定（請參見以下表格）。

卸除式磁碟機掃描設定

設定	預設值	敘述
掃描透過 USB 連接的卸除式磁碟機	已清除核取方塊	您可以開啟或關閉透過 USB 連線到受防護裝置上的卸除式磁碟機的掃描。
掃描卸除式磁碟機，如果其儲存的資料量未超過 (MB)	8192 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。
掃描時使用的安全等級	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： • **最佳防護**

		• **建議** • **最佳效能** 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。

關於“基線檔案完整性監控”工作

在“基線檔案完整性監控”工作期間，Kaspersky Embedded Systems Security 不會檢查鎖定的檔案、資料夾、檔案捷徑和雲端檔案。

“基線檔案完整性監控”工作透過將檔案的雜湊（MD5 雜湊或 SHA256 雜湊）與基線進行比較來對監控範圍內檔案的完整性進行監控。

當“基線檔案完整性監控”工作首次執行時，Kaspersky Embedded Systems Security 透過計算和儲存工作監控範圍內檔案的雜湊來建立基線。如果變更了“基線檔案完整性監控”工作監控範圍，Kaspersky Embedded Systems Security 會在“基線檔案完整性監控”工作下次執行時透過計算和儲存工作監控範圍內檔案的雜湊來更新基線。如果刪除了“基線檔案完整性監控”工作，Kaspersky Embedded Systems Security 會刪除此“基線檔案完整性監控”工作的基線。

您可以使用指令行刪除基線 ，而不刪除“基線檔案完整性監控”工作。

“基線檔案完整性監控”工作會追蹤監控範圍內檔案的以下變更：

- 監控範圍包含基線中不存在的檔案
- 監控範圍不包含基線中存在的檔案
- 監控範圍中檔案的雜湊與基線中此檔案的雜湊不同

“基線檔案完整性監控”工作不會追蹤檔案內容和交換流程的變更。

如果某個檔案或資料夾無法存取，則 Kaspersky Embedded Systems Security 在基線建立過程中不會將此檔案或資料夾新增到基線，並且將在執行“基線檔案完整性監控”工作期間建立一個關於計算檔案核對總和失敗的事件。

檔案或資料夾不可存取可能由於以下原因：

- 指定的路徑不存在
- 指定的路徑下不存在遮罩指定的檔案類型
- 指定的檔案被鎖定
- 指定的檔案為空

從內容功能表中啟用自訂掃描工作的啟動

您可以從 Microsoft Windows 資源管理器的內容功能表中啟用針對一個或多個檔案之自訂掃描工作的啟動。

要從內容功能表啟用自訂掃描工作的啟動：

1. 建立以下 REG 檔案：

   ```
   Windows 登錄檔編輯器版本 5.0.0

   [HKEY_CLASSES_ROOT\Directory\shell\kess\command]

   @="C:\\Temp\\scan.cmd \"%1\""

   [HKEY_CLASSES_ROOT\*\shell\kess\command]

   @="C:\\Temp\\scan.cmd \"%1\""

   [HKEY_CLASSES_ROOT\Directory\shell\kess]

   @="Scan with Kaspersky Embedded Systems Security\"

   "Icon"="\"C:\\Program Files (x86)\\Kaspersky Lab\\Kaspersky Embedded Systems
   Security\\kavtrayr.dll\",0"

   [HKEY_CLASSES_ROOT\Directory\shell\kess\DefaultIcon]

   @="\"C:\\Program Files (x86)\\Kaspersky Lab\\Kaspersky Embedded Systems
   Security\\kavtrayr.dll\",0"

   [HKEY_CLASSES_ROOT\*\shell\kess]

   @="Scan with Kaspersky Embedded Systems Security\"

   "Icon"="\"C:\\Program Files (x86)\\Kaspersky Lab\\Kaspersky Embedded Systems
   Security\\kavtrayr.dll\",0"

   [HKEY_CLASSES_ROOT\*\shell\kess\DefaultIcon]
   @="\"C:\\Program Files (x86)\\Kaspersky Lab\\Kaspersky Embedded Systems
   Security\\kavtrayr.dll\",0"

   [HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows
   NT\CurrentVersion\AppCompatFlags\Layers]

   "C:\\Program Files (x86)\\Kaspersky Lab\\Kaspersky Embedded Systems
   Security\\kavshell.exe"="~ RUNASADMIN"
   ```

   > 您需要指定 Kaspersky Embedded Systems Security 安裝資料夾的實際位置。

2. 建立具有以下內容的 `scan.cmd` 檔案：

   ```
   @echo off
   set LOGNAME=%RANDOM%

   "C:\Program Files (x86)\Kaspersky Lab\Kaspersky Embedded Systems
   Security\kavshell.exe" scan "%~1" /W:c:\temp\%LOGNAME%.txt

   echo Scanning is in progress...
   type c:\temp\%LOGNAME%.txt
   del c:\temp\%LOGNAME%.txt

   timeout /t -1
   ```

   `scan.cmd` 檔案必須包含以下資訊：

   - `kavshell.exe` 檔案的位置。

- 包含掃描結果的暫時檔案位置。
- KAVSHELL SCAN 指令的參數。
- 用於在工作完成後關閉主控台視窗的逾時值。

3. 將 scan.cmd 檔案複製到 [HKEY_CLASSES_ROOT\Directory\shell\kess\command] REG 檔案中指定的資料夾。

   範例中使用了 C:\Temp 資料夾。

您無需重新啟動作業系統。

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

設定	預設值	敘述
掃描範圍	套用於系統和自訂工作： • **在作業系統啟動時掃描**：整個受防護裝置，排除共用資料夾和自動執行的物件。 • **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。 • **自訂掃描**工作：整個受防護裝置。	您可以變更掃描範圍。不能為**隔離區掃描**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**”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性設定儲存為範本，以便在以後將其套用至其他節點。
使用啟發式分析	與“關鍵區域掃描”、“在作業系統啟動時掃描”和自訂工作的“**中度**”分析等級結合使用。 與“隔離區掃描”工作的“**深度**”分析等級結合使用。	可以啟用或停用“啟發式分析”並設定分析等級。不能配置“隔離區掃描”工作分析級別。 “應用程式完整性控制”和“基線檔案完整性監控”工作不使用啟發式分析。
套用信任區域	已套用（不適用於“隔離區掃描”工作）	可以在選定工作中使用的一般排除清單。
在掃描中使用 KSN	已套用	您可以使用卡巴斯基安全網路雲端服務基礎架構提高您的裝置防護能力。

以特定權限啟動工作的設定	在系統帳戶下啟動工作。	您可以為所有系統和自訂掃描工作編輯以特定帳戶權限啟動工作的設定，但"隔離區掃描"和"應用程式完整性控制"工作除外。
在背景模式下執行工作（低優先順序）	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	套用於本機系統工作： • 在作業系統啟動時掃描 – **在應用程式啟動時** • 關鍵區域掃描 – **每週** • 隔離區掃描 – **應用程式資料庫更新後** • 應用程式完整性控制 – **每天** 新建自訂工作中未使用。	您可以配置排程工作啟動的設定。
記錄掃描執行並更新裝置防護狀態	執行關鍵區域掃描後，每週更新一次裝置防護狀態。	可透過以下方式配置記錄關鍵區域掃描執行記錄的相關設定： • 編輯關鍵區域掃描工作啟動排程的設定。 • 編輯關鍵區域掃描工作的掃描範圍。 • 建立自訂的自訂掃描工作。

透過管理外掛程式管理自訂掃描工作

在本節中，學習如何導航管理外掛程式介面，以及如何為網路中的一台或所有受防護裝置配置工作設定。

導航

瞭解如何透過所選介面導航到所需工作設定。

開啟自訂掃描工作精靈

要開始建立新的自訂掃描工作：

1. 若要建立本機工作，請執行以下步驟：
   a. 展開卡巴斯基安全管理中心管理主控台中的"**受管理裝置**"節點。
   b. 選擇受防護裝置所屬的管理群組。
   c. 在結果窗格的"**裝置**"標籤上，開啟受防護裝置的內容功能表。

d. 選擇**"內容"**功能表選項。

e. 在開啟的視窗中，點擊**"工作"**部分中的**"新增"**按鈕。

將開啟**"新建工作精靈"**視窗。

2. 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. 開啟**"工作"**標籤。

d. 點擊**"建立工作"**按鈕。

將開啟**"新建工作精靈"**視窗。

3. 要為自訂的一組受防護裝置建立工作：

a. 在卡巴斯基安全管理中心管理主控台樹狀目錄的**"裝置選擇"**節點中，點擊**"執行選擇"**按鈕以執行裝置選擇。

b. 開啟**"選擇結果'選擇名稱'"**標籤。

c. 在**"執行選擇"**下拉清單中，選擇**"為選擇結果建立工作"**選項。

將開啟**"新建工作精靈"**視窗。

4. 在 Kaspersky Embedded Systems Security 的可用工作清單中選取**自訂掃描**工作。

5. 點擊**"下一步"**。
將開啟**"設定"**視窗。

根據需要配置工作設定。

要配置現有自訂掃描工作，

按兩下卡巴斯基安全管理中心工作清單中的工作名稱。

將打开**"属性：自訂掃描"**窗口。

開啟自訂掃描工作內容

要開啟單台受防護裝置的自訂掃描工作的應用程式內容：

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. 選擇受防護裝置所屬的管理群組。

3. 選擇**"裝置"**標籤。

4. 點擊要為其配置掃描範圍的受防護裝置的名稱。
將打开**"属性：<受保护设备名称>"**窗口。

5. 選擇“**工作**”部分。

6. 在為裝置建立的工作清單中，選擇您建立的自訂掃描工作。

7. 點擊“**內容**”按鈕。
   將打开“**属性：自訂掃描**”窗口。

根據需要配置工作設定。

建立自訂掃描工作

要建立自訂掃描工作：

1. 開啟“新建工作精靈”中的“**設定**”視窗。

2. 選擇所需的**工作建立方法**。

3. 點擊“**下一步**”。

4. 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性設定。

   - 要從掃描中排除所有關鍵區域，請在每行上開啟內容功能表並選擇“**刪除範圍**”選項。
   - 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. 右鍵點擊“**掃描範圍**”表，然後選擇“**新增範圍**”或點擊“**新增**”按鈕。
     b. 在“**新增物件至掃描範圍**”視窗中，選擇“**預定義範圍**”清單中的預定義範圍，指定受防護裝置或另外一台網路受防護裝置上的磁碟機、資料夾、網路物件或檔案，然後點擊“**確定**”按鈕。
   - 要從掃描中排除子資料夾或檔案，請在精靈的“**掃描範圍**”視窗中選擇已新增的資料夾（磁碟）：
     a. 開啟內容功能表，然後選擇“**配置**”選項。
     b. 在“**安全等級**”視窗中點擊“**設定**”按鈕。
     c. 在“**自訂掃描設定**”設定視窗的“**一般**”標籤上，清除“**子資料夾**和**子檔案**”核取方塊。
   - 要變更掃描範圍安全性設定：
     a. 開啟您希望配置其設定的範圍的內容功能表，然後選擇“**配置**”。
     b. 在“**自訂掃描設定**”視窗中，選擇預定義的安全等級之一，或者點擊“**設定**”按鈕以手動配置安全性設定。

安全性設定的配置方式與即時檔案防護工作的配置方式相同。

- 要略過新增的掃描範圍中的內嵌式物件：

  a. 開啟"**掃描範圍**"表的內容功能表，選擇"**新增排除項目**"。

  b. 指定要排除的物件：在"**預定義範圍**"清單中選擇預定義範圍，指定受防護裝置或另一台網路受防護裝置上的磁碟、資料夾、網路物件或檔案。

  c. 點擊"**確定**"按鈕。

5. 在"**選項**配置卸除式磁碟機掃描"視窗中，配置啟發式分析以及與其他元件的整合：

   - 配置啟發式分析的使用。
   - 如果您希望從工作的掃描範圍中排除已新增到信任區域清單的物件，則選中"**套用信任區域**"核取方塊。
   - 如果您想要在工作中使用卡巴斯基安全網路雲端服務，請選取**使用 KSN 掃描**核取方塊。
   - 若要向將執行該工作的處理程序分配 *低*優先順序，請選取**選項**視窗中的**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）。

   - 要將所建立的工作當作關鍵區域掃描工作，請選取**選項**視窗的**將工作視為關鍵區域掃描**核取方塊。

6. 點擊"**下一步**"。
7. 在"**排程**"視窗中，設定排程的工作啟動設定。
8. 點擊"**下一步**"。
9. 在"**選擇帳戶以執行工作**"視窗中，指定要使用的帳戶。
10. 點擊"**下一步**"。
11. 指定工作名稱。
12. 點擊"**下一步**"。

    工作名稱不應超過 100 個字元，並且不能包含以下符號：" * < > & \ : |

    將開啟"**完成建立工作**"視窗。

13. 您可以透過選中"**精靈完成後執行工作**"核取方塊來在精靈完成後執行工作。
14. 點擊"**完成**"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自訂掃描工作。

為自訂掃描工作分配關鍵區域掃描狀態

預設情況下，如果在 Kaspersky Embedded Systems Security 中，「關鍵區域掃描」工作的執行時間少於 *長時間未執行關鍵區域掃描*指定的頻率，則卡巴斯基安全管理中心將 *警告*狀態分配給受防護的裝置。

要為單個管理群組中的所有受防護裝置配置掃描：

1. 建立群組自訂掃描工作。
2. 在工作建立精靈**"選項"**視窗中，選中**"將工作視為關鍵區域掃描"**核取方塊。指定的工作設定（掃描範圍與安全性設定）將套用至群組中的所有受防護裝置。配置工作排程。

   您可以在为一组受保护设备创建按需扫描任务时选中**"将任务视为关键区域扫描"**复选框，或稍后在**"属性：<任务名称>"**窗口中选中该复选框。

3. 使用新的或現有政策會停用群組受防護裝置上的隨選掃描本機系統工作的排程啟動。

隨後，卡巴斯基安全管理中心管理伺服器將評估受防護裝置的安全狀態，並且將根據上次執行具有「關鍵區域掃描」狀態工作的結果而非根據「關鍵區域掃描」本機系統工作的結果通知您有關該安全狀態的資訊。

您可以為自訂掃描群組工作和受防護裝置群組的工作分配*"關鍵區域掃描"*狀態。

可以使用應用程式主控台檢視"自訂掃描"工作是否為"關鍵區域掃描"工作。

在應用程式主控台中，**"將工作視為關鍵區域掃描"**核取方塊會顯示在工作設定中，但不可對其進行編輯。

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。

可以將執行自訂掃描工作的程序分配為*"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。您可以指定自訂掃描背景工作的最大處理程序數。

要變更現有自訂掃描工作的優先順序：

1. 打開**"屬性：自訂掃描"**窗口。
2. 選中或清除**"在背景模式下執行工作"**核取方塊。
3. 點擊**"確定"**。

   將儲存已配置的工作設定，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。

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** 節點的結果視窗中，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。預設情況下，僅針對"關鍵區域掃描"工作選中該核取方塊且無法針對該工作進行修改。

只能在卡巴斯基安全管理中心中選擇與裝置防護狀態相關聯的自訂掃描工作。

配置工作掃描範圍

如果在「在作業系統啟動時掃描」和「關鍵區域掃描」工作中修改掃描範圍，可以透過修復 Kaspersky Embedded Systems Security 本身的設定來還原這些工作中的預設掃描範圍（**開始 > 程式 > Kaspersky Embedded Systems Security > 修改或移除 Kaspersky Embedded Systems Security**）。在安裝精靈中，選擇**"修復已安裝元件"**並點擊**"下一步>"**。然後選中**"還原建議的應用程式設定"**核取方塊。

要配置現有自訂掃描工作的掃描範圍：

1. 打开**"属性：自訂掃描"**窗口。
2. 選擇**"掃描範圍"**標籤。
3. 要在掃描範圍中包括項目：
   a. 在掃描範圍清單的空白部分中開啟內容功能表。
   b. 選擇內容功能表中的**"新增範圍"**選項。
   c. 在開啟的**"新增物件至掃描範圍"**視窗中，選擇想要新增的物件類型：
      - **預定義範圍** – 在受防護裝置上新增一個預定義範圍。然後在下拉清單中，選擇所需掃描範圍。
      - **磁碟、資料夾或網路資料夾** – 在掃描範圍中包括單個磁碟機、資料夾或網路物件。然後透過點擊**"瀏覽"**按鈕選擇所需的範圍。
      - **檔案** – 在掃描範圍中包括單個檔案。然後透過點擊**"瀏覽"**按鈕選擇所需的範圍。

   如果某個物件已經作為掃描範圍的排除項新增，則不能再將其新增到掃描範圍中。
4. 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，或者執行以下步驟：
   a. 按右鍵掃描範圍開啟其內容功能表。
   b. 在內容功能表中，選擇**"新增排除項目"**選項。
   c. 在**"新增排除"**視窗中選擇物件類型，將按照將物件新增到掃描範圍中時使用的步驟，將該物件類型作為掃描範圍的排除新增。

5. 要修改掃描範圍或所新增的排除項目，請選擇相應掃描範圍內容功能表中的**"編輯範圍"**選項。

6. 若要在網路檔案資源清單中隱藏之前新增的掃描範圍或排除項目，請在所需掃描範圍的內容功能表中選擇**"刪除範圍"**選項。

   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。

7. 點擊**"確定"**按鈕。

掃描範圍設定視窗關閉。將儲存新配置的設定。

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預定義安全等級之一：**"最佳效能"**、**"建議"**和**"最佳防護"**。

要選擇其中一個預定義安全等級：

1. 打开**"屬性：自訂掃描"**窗口。

2. 選擇**"掃描範圍"**標籤。

3. 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。

4. 點擊**"配置"**按鈕。

   將開啟**"自訂掃描設定"**視窗。

5. 在**"安全等級"**標籤上，選擇要套用的安全等級。

   該視窗將顯示與選定安全等級相對應的安全性設定清單。

6. 點擊**"確定"**按鈕。

7. 在**"屬性：自訂掃描"**窗口中单击**"確定"**按钮。

   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。

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性設定。

這些設定對應于**"建議"**預定義安全等級。

可以透過將安全性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，來修改安全性設定的預設值。

要手動配置安全設定：

1. 打开**"屬性：自訂掃描"**窗口。

2. 選擇**"掃描範圍"**標籤。

3. 在您要為其配置安全性設定的掃描範圍清單中選擇項目。

> 可以為掃描範圍內的選定節點或項目套用包含安全設定的預定義範本。

4. 點擊**"配置"**按鈕。
   將開啟**"自訂掃描設定"**視窗。

5. 在以下標籤上根據需求配置選定節點或項目的安全設定：

   - **一般**
   - **操作**
   - **效能**
   - **分級儲存**

6. 在**隨需掃描設定**視窗中點擊**確定**。

7. 在**設定掃描範圍**視窗中，點擊**儲存**。

將儲存新的掃描範圍設定。

配置一般工作設定

要配置一般自訂掃描工作設定：

1. 打開**"屬性：自訂掃描"**窗口。

2. 選擇**"掃描範圍"**標籤。

3. 點擊**"配置"**按鈕。
   將開啟**"自訂掃描設定"**視窗。

4. 點擊**"設定"**按鈕。

5. 在**"一般"**標籤的**"掃描物件"**部分中，指定要包含在掃描範圍內的物件類型：

   - **掃描物件**：
     - **所有物件**
     - **按格式掃描物件**
     - **按病毒資料庫中指定的副檔名清單掃描物件**
     - **按指定的副檔名清單掃描物件**
   - **子資料夾**
   - **子檔案**

- **掃描開機磁區和 MBR**
- **掃描 NTFS 交換資料串流**

6. 在“**效能**”部分中，選中或清除“**僅掃描新增與變更過的檔案**”核取方塊。

> 如果清除該核取方塊，要在可用選項之間轉換，請點擊每個複合物件類型對應的“**全部/僅新建**”連結。

7. 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：

- **全部/僅新建的壓縮檔案**
- **全部/僅新建的 SFX 壓縮檔案**
- **全部/僅新建的電子郵件資料庫**
- **全部/僅新封裝的物件**
- **全部/僅新建的純文字電子郵件**
- **全部/僅新的內嵌 OLE 物件**

8. 點擊“**確定**”。

將儲存新的工作配置。

配置操作

要配置“自訂掃描”工作過程中對受感染的物件和其他偵測到的物件執行的操作：

1. 打开“**属性：自訂掃描**”窗口。
2. 選擇“**掃描範圍**”標籤。
3. 點擊“**配置**”按鈕。
   將開啟“**自訂掃描設定**”視窗。
4. 點擊“**設定**”按鈕。
5. 選擇“**操作**”標籤。
6. 選擇要對受感染的物件和其他偵測到的物件執行的操作：

- **僅通知**。
- **解毒**。
- **解毒。**解毒失敗則刪除。
- **刪除**。
- **執行建議的操作**。

7. 選擇要對可能受感染的物件執行操作：

   - **僅通知**。
   - **隔離**。
   - **刪除**。
   - **執行建議的操作**。

8. 選擇依威脅類型對物件執行的操作：

   a. 清除或選中"**根據偵測到的物件的類型執行操作**"核取方塊。

   b. 點擊"**設定**"按鈕。

   c. 在開啟的視窗中，選擇針對每種偵測到的物件類型的主要操作和次要操作（如果主要操作失敗則執行）。

   d. 點擊"**確定**"。

9. 選擇要對不可還原的複合物件執行的操作：選擇或清除"**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. 點擊"**確定**"。

    將儲存新的工作配置。

配置效能

要配置"自訂掃描"工作的效能設定：

1. 打開"**屬性：自訂掃描**"窗口。
2. 選擇"**掃描範圍**"標籤。
3. 點擊"**配置**"按鈕。
   將開啟"**自訂掃描設定**"視窗。
4. 點擊"**設定**"按鈕。
5. 選擇"**效能**"標籤。
6. 在"**排除**"部分中：

   - 清除或選中"**排除檔案**"核取方塊。
   - 清除或選中"**不偵測**"核取方塊。
   - 針對每個設定點擊"**編輯**"按鈕以新增排除項目。

7. 在"**進階設定**"部分中：

   - **超過以下時間則停止掃描(秒)**

- **不掃描超過此值複合檔案(MB)**
- **使用 iSwift 技術**
- **使用 iChecker 技術**

8. 點擊**"確定"**。

將儲存新的工作配置。

配置卸除式磁碟機掃描

要配置在卸除式磁碟機連線到受防護裝置時對其進行的掃描：

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。
   在打开的**"属性：<策略名称>"**窗口中，选择**"补充"**部分。
5. 點擊**"卸除式磁碟機掃描"**子區段中的**"設定"**按鈕。
   將開啟**"卸除式磁碟機掃描"**視窗。
6. 在**"連接時掃描"**部分中，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**"掃描透過 USB 連接的卸除式磁碟機"**核取方塊。
   - 如果需要，選中**"掃描卸除式磁碟機，如果其儲存的資料量未超過(MB)"**，然後在右側的欄位中指定最大值。
   - 在**"掃描時使用的安全等級"**下拉清單中，指定卸除式磁碟機掃描所需設定的安全等級。
7. 點擊**"確定"**。

即會儲存並套用指定設定。

配置"基線檔案完整性監控"工作

要配置"基線檔案完整性監控"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選擇工作名稱，然後點擊**"配置工作"**連結。
- 在建立的工作清單中開啟工作名稱的內容功能表，然後選擇**"內容"**項。

在**"通知"**部分中，配置工作事件通知設定。關於本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**"監控範圍"**部分中，執行以下操作：

   a. 要將資料夾包括在"基線檔案完整性監控"工作範圍中：

      1. 點擊**"新增"**按鈕。
         將開啟**"掃描區內容"**視窗。
      2. 選中或清除**"監控此區域"**核取方塊。
      3. 點擊**瀏覽**按鈕以指定要包括在"基線檔案完整性監控"工作範圍中的資料夾。
      4. 如果要在"基線檔案完整性監控"工作範圍中包括所有子資料夾，請選中**"同時監控子資料夾"**核取方塊。

   b. 要包括或排除先前新增到"基線檔案完整性監控"工作範圍中的資料夾，請選中或清除**"監控範圍"**表中資料夾路徑左側的核取方塊。

   c. 要刪除先前新增到"基線檔案完整性監控"工作範圍中的資料夾，請在**"監控範圍"**表中選擇此資料夾，然後點擊**"刪除"**按鈕。

6. 在**"排程"**部分中配置工作排程（您可以為除"資料庫更新回溯"以外的所有工作類型配置排程）。
7. 在**"帳戶"**部分中，指定將使用其權限執行工作的帳戶。
8. 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*。

9. 在**"內容：<工作名稱>"**視窗中，點擊**"確定"**。
   將儲存新配置的群組工作設定。

透過應用程式主控台管理自訂掃描工作

在本節中，學習如何導航應用程式主控台介面以及如何在受防護裝置上配置工作設定。

導航

瞭解如何透過所選介面導航到所需工作設定。

開啟自訂掃描工作設定

要透過應用程式主控台開啟自訂掃描工作的一般設定：

1. 在應用程式主控台樹狀目錄中展開**"自訂掃描"**節點。
2. 選擇與要設定的工作相應的子節點。
3. 在子節點結果窗格中，點擊**"內容"**連結。
   將開啟**"工作設定"**視窗。

開啟自訂掃描工作範圍設定

要透過應用程式主控台開啟設定掃描範圍視窗：

1. 在應用程式主控台樹狀目錄中展開**"自訂掃描"**節點。
2. 選擇與要設定的自訂掃描工作相應的子節點。
3. 在已選擇的節點結果窗格，點擊**配置掃描範圍**連結。
   將開啟**"設定掃描範圍"**視窗。

建立和配置自訂掃描工作

單台受防護裝置的自訂工作可以在**"自訂掃描"**節點中建立。不能在 Kaspersky Embedded Systems Security 其他功能元件中建立自訂工作。

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**"自訂掃描"**節點的內容功能表。
2. 選擇**"新增工作"**。
   將開啟**"新增工作"**視窗。
3. 配置以下工作設定：
   - **名稱** – 包含不超過 100 個字元的工作名稱。可以包含除 " * < > & \ :

     如果未指定工作名稱，則無法在**"排程"**、**"進階"**和**"執行帳戶"**上儲存工作或配置新工作。

   - **描述** – 有關工作的任何附加資訊。不超過 2000 個字元。此資訊將顯示在工作內容視窗中。
   - **使用啟發式分析**。
   - **在背景模式下執行工作**。

- **套用信任區域**。
- **將工作視為關鍵區域掃描**。
- **在掃描中使用 KSN**。

4. 在**排程**和**進階**標籤上配置工作啟動排程設定。
5. 在**"執行帳戶"**標籤上，配置使用特定帳戶權限啟動工作的設定。
6. 在**新增工作**視窗中點擊**新增工作**。

   將建立新的自訂掃描工作。將在應用程式主控台樹狀目錄中顯示包含新工作名稱的節點。此操作將會記錄到系統稽核記錄中。
7. 如果需要，在所選節點的結果窗格中，選擇**"配置掃描範圍"**。

   將開啟**"設定掃描範圍"**視窗。
8. 在受防護裝置檔案資源樹狀目錄或清單中，選擇要包含在掃描範圍內的節點或項。
9. 選擇一項預設安全等級或手動配置掃描設定。
10. 在**設定掃描範圍**視窗中，點擊**設定掃描範圍**。

    將在下次啟動工作時應用設定的設定。

自訂掃描工作中的掃描範圍

本節包含有關在"自訂掃描"工作中建立和使用掃描範圍的資訊。

配置網路檔案資源的視圖

要在配置掃描範圍設定期間選擇網路檔案資源的視圖：

1. 開啟**"設定掃描範圍"**視窗。
2. 開啟左上角部分中的下拉清單，然後選擇以下選項之一：
   - 選擇**"樹狀檢視"**選項以樹狀目錄的形式顯示網路檔案資源。
   - 選擇**"清單檢視"**選項以清單形式顯示網路檔案資源。

   預設情況下，受防護裝置的網路檔案資源以清單形式顯示。
3. 點擊**"儲存"**按鈕。

建立掃描範圍

如果您正在使用管理員工作站上安裝的應用程式主控台遠端管理受防護裝置上的 Kaspersky Embedded Systems Security，您必須是受防護裝置上管理員群組成員才能檢視資料夾。

在不同 Windows 作業系統中，設定的名稱可能會有所不同。

如果在「在作業系統啟動時掃描」和「關鍵區域掃描」工作中修改掃描範圍，可以透過修復 Kaspersky Embedded Systems Security 本身的設定來還原這些工作中的預設掃描範圍（**開始** > **程式** > **Kaspersky Embedded Systems Security** > **修改或移除 Kaspersky Embedded Systems Security**）。在安裝精靈中，選擇**"修復已安裝元件"**並點擊**"下一步>"**。然後選中**"還原建議的應用程式設定"**核取方塊。

建立自訂掃描工作範圍的過程取決於網路檔案資源視圖。您可以將網路檔案資源的視圖配置為樹狀目錄或清單（預設視圖）。

要使用網路檔案資源樹狀目錄建立掃描範圍：

1. 開啟**"設定掃描範圍"**視窗。
2. 在視窗的左側部分中，開啟網路檔案資源樹狀目錄以顯示所有節點和子節點。
3. 執行以下操作：
   - 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。
   - 要從掃描範圍中排除單個節點，請清除**"我的電腦"**核取方塊，然後執行以下步驟：
     - 如果要將特定類型的所有磁碟機均包含在防護範圍內，請選中所需磁碟機類型名稱旁邊的核取方塊（例如，要新增受防護裝置上的所有卸除式磁碟機，請選中**"卸除式磁碟機"**核取方塊）。
     - 如果要將特定類型的單個磁碟機包含在掃描範圍內，請展開包含該類型磁碟機的節點，然後選中所需磁碟機代號旁邊的核取方塊。例如，要选择可移动驱动器 **F:**，请展开**"卸除式磁碟機"**节点，然后选中驱动器 **F:** 对应的复选框。
     - 如果您想要僅包含磁碟機上的單個資料夾或檔案，請選中該資料夾或檔案名稱旁邊的核取方塊。
4. 點擊**"儲存"**按鈕。

"設定掃描範圍"視窗將關閉。將儲存新配置的設定。

要使用網路檔案資源清單建立掃描範圍：

1. 開啟**"設定掃描範圍"**視窗。
2. 要從掃描範圍中排除單個節點，請清除**"我的電腦"**核取方塊，然後執行以下步驟：
   a. 按右鍵掃描範圍開啟其內容功能表。
   b. 在按鈕的內容功能表中，選擇**"新增掃描範圍"**。
   c. 在開啟的**"新增掃描範圍"**視窗中，選擇要新增的物件類型：
      - **預設的範圍** – 在受防護裝置上新增一個預定義範圍。然後在下拉清單中，選擇所需掃描範圍。
      - **磁碟、資料夾或網路資料夾** – 在掃描範圍中包括單個磁碟機、資料夾或網路物件。然後透過點擊**"瀏覽"**按鈕選擇所需的範圍。

- **檔案** - 在掃描範圍中包括單個檔案。然後透過點擊**"瀏覽"**按鈕選擇所需的範圍。

如果某個物件已經作為掃描範圍的排除項新增，則不能再將其新增到掃描範圍中。

3. 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，或者執行以下步驟：

   a. 按右鍵掃描範圍開啟其內容功能表。

   b. 在內容功能表中，選擇**"新增排除項目"**選項。

   c. 在**"新增排除項目"**視窗中選擇物件類型，將按照將物件新增到掃描範圍中時使用的步驟，將該物件類型作為掃描範圍的排除新增。

4. 要修改新增的掃描範圍或排除項，請選擇所需掃描範圍內容功能表中的**"編輯範圍"**選項。

5. 若要在網路檔案資源清單中隱藏之前新增的掃描範圍或排除項，請在相應掃描範圍的內容功能表中選擇**"從清單刪除"**選項。

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。

6. 點擊**"儲存"**按鈕。

"設定掃描範圍"視窗將關閉。將儲存新配置的設定。

在掃描範圍內包含網路物件

您可以按照 UNC（通用命名慣例）格式指定網路磁碟機、資料夾或檔案的路徑以將它們新增至掃描範圍。

您可以在系統帳戶下掃描網路資料夾。

要將網路位置新增到掃描範圍：

1. 開啟**"設定掃描範圍"**視窗。

2. 開啟左上角部分中的下拉清單，然後選擇**"樹狀檢視"**。

3. 在**"網路"**節點的內容功能表中：

   - 選擇**"新增網路資料夾"**，如果您想要向掃描範圍中新增網路資料夾。
   - 選擇**"新增網路檔案"**，如果您想要向掃描範圍中新增網路檔案。

4. 以 UNC 格式輸入網路資料夾或檔案路徑，然後點擊 **ENTER** 鍵。

5. 選中新新增的網路物件旁邊的核取方塊以將其包含在掃描範圍內。

6. 如有必要，變更已新增的網路物件的安全性設定。

7. 點擊**"儲存"**按鈕。

將儲存修改的工作設定。

建立虛擬掃描範圍

可以將虛擬磁碟機、資料夾和檔案包含在掃描範圍內以建立虛擬掃描範圍。

僅當掃描範圍以檔案資源樹狀目錄的形式顯示時，您才可透過新增單個虛擬磁碟機、資料夾或檔案來延伸掃描範圍。

要新增虛擬磁碟機至掃描範圍：

1. 開啟**"設定掃描範圍"**視窗。
2. 開啟左上角部分中的下拉清單，然後選擇**"樹狀檢視"**。
3. 在受防護裝置檔案資源樹狀目錄中開啟**"虛擬磁碟機"**節點的內容功能表，點擊**"新增虛擬磁碟機"**，然後從可用名稱清單中選擇虛擬磁碟機名稱。
4. 選中已新增的磁碟機旁邊的核取方塊，以將該磁碟機包括在掃描範圍中。
5. 點擊**"儲存"**按鈕。

將儲存修改的工作設定。

要新增虛擬資料夾或虛擬檔案至掃描範圍：

1. 開啟**"設定掃描範圍"**視窗。
2. 開啟左上角部分中的下拉清單，然後選擇**"樹狀檢視"**。
3. 在受防護裝置檔案資源樹狀目錄中，開啟節點的內容功能表以新增資料夾或檔案，然後選擇以下選項之一：
   - **新增虛擬資料夾**，如果您想要向掃描範圍中新增虛擬資料夾。
   - **新增虛擬檔案**，如果您想要向掃描範圍中新增虛擬檔案。
4. 在輸入欄位中指定資料夾或檔案的名稱。
5. 在包含資料夾（或檔案）名稱的欄位中，選定相應的核取方塊以將該資料夾（或檔案）包含在掃描範圍中。
6. 點擊**"儲存"**按鈕。

將儲存修改的工作設定。

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性設定。

這些設定對應于**"建議"**預定義安全等級。

可以透過將安全性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，來修改安全性設定的預設值。

在使用網路檔案資源樹狀目錄時，為所選父節點配置的安全性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。

要手動配置安全設定：

1. 開啟**"設定掃描範圍"**視窗。
2. 在視窗的左側部分中，選擇要配置其安全性設定的節點或項目。

   可以為掃描範圍內的選定節點或項目套用包含安全設定的預定義範本。

   在視窗的左側部分，您可以選擇網路檔案資源的視圖、建立掃描範圍或建立虛擬掃描範圍。
3. 在視窗的右側部分，執行下列操作之一：
   - 在**"安全等級"**標籤上，選擇要套用的安全等級。
   - 在以下標籤上根據要求配置選定節點或項目的所需安全設定：
     - **一般**
     - **操作**
     - **效能**
     - **分級儲存**
4. 在**"儲存"**視窗中，點擊**"設定掃描範圍"**。

   將儲存新的掃描範圍設定。

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樹狀目錄或清單中的選定節點套用以下預定義安全等級之一：**"最佳效能"**、**"建議"**和**"最佳防護"**。

要選擇其中一個預定義安全等級：

1. 開啟**"設定掃描範圍"**視窗。
2. 在受防護裝置網路檔案資源樹狀目錄或清單中，選擇要設定預定義安全等級的節點或項。
3. 確保選定的節點或項包含在掃描範圍中。
4. 在視窗右側的**"安全等級"**標籤中，選擇要應用的安全等級。

   該視窗將顯示與選定安全等級相對應的安全性設定清單。
5. 點擊**"儲存"**按鈕。

   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。

配置一般工作設定

要配置自訂掃描工作的一般安全性設定：

1. 開啟“**設定掃描範圍**”視窗。
2. 選擇“**一般**”標籤。
3. 在“**掃描物件**”部分中，指定要包含在掃描範圍內的物件類型：
   - **掃描物件**：
     - **所有物件**
     - **按格式掃描物件**
     - **按病毒資料庫中指定的副檔名清單掃描物件**
     - **按指定的副檔名清單掃描物件**
   - **掃描開機磁區和 MBR**
   - **掃描 NTFS 交換資料串流**
4. 在“**效能**”部分中，選中或清除“**僅掃描新增與變更過的檔案**”核取方塊。

   要在該核取方塊處於清除狀態時轉換可用選項，請點擊每個複合物件類型對應的“**全部/僅新建**”連結。
5. 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：
   - **全部/僅新的壓縮檔案**
   - **全部/僅新的 SFX 壓縮檔案**
   - **全部/僅新的電子郵件資料庫**
   - **全部/僅新的封裝的物件**
   - **全部/僅新的純文字電子郵件**
   - **全部/僅新嵌入的 OLE 物件**
6. 點擊“**儲存**”。

將儲存新的工作配置。

配置操作

要為“自訂掃描”工作配置對受感染的物件和其他偵測到的物件的操作：

1. 開啟“**設定掃描範圍**”視窗。
2. 選擇“**操作**”標籤。
3. 選擇要對受感染的物件和其他偵測到的物件執行的操作：
   - **僅通知**。
   - **解毒**。
   - **解毒，無法解毒時刪除**解毒失敗則刪除。
   - **刪除**。
   - **執行建議的操作**。
4. 選擇要對可能受感染的物件執行操作：
   - **僅通知**。
   - **隔離**。
   - **刪除**。
   - **執行建議的操作**。
5. 選擇依威脅類型對物件執行的操作：
   a. 清除或選中“**根據偵測到的物件的類型執行操作**”核取方塊。
   b. 點擊“**設定**”按鈕。
   c. 在開啟的視窗中，選擇針對每種偵測到的物件類型的主要操作和次要操作（如果主要操作失敗則執行）。
   d. 點擊“**確定**”。
6. 選擇要對不可還原的複合物件執行的操作：選擇或清除“**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。
7. 點擊“**儲存**”。

將儲存新的工作配置。

配置效能

要配置“自訂掃描”工作的效能設定：

1. 開啟“**設定掃描範圍**”視窗。
2. 選擇“**效能**”標籤。
3. 在“**排除**”部分中：
   - 清除或選中“**排除檔案**”核取方塊。

- 清除或選中“**不偵測**”核取方塊。
- 針對每個設定點擊“**編輯**”按鈕以新增排除項目。

4. 在“**進階設定**”部分中：
   - **超過以下時間則停止掃描(秒)**
   - **不掃描超過此值複合檔案(MB)**
   - **使用 iSwift 技術**
   - **使用 iChecker 技術**
5. 點擊“**儲存**”。

將儲存新的工作配置。

配置分級儲存

要為“自訂掃描”工作配置對受感染的物件和其他偵測到的物件執行的操作：

1. 開啟“**設定掃描範圍**”視窗。
2. 選擇“**分級儲存**”標籤。
3. 選擇要對檔案執行的操作：
   - **不掃描**。
   - **僅掃描常駐檔案**。
   - **掃描完整檔案**。
     如果選擇此操作，則可以指定以下操作：
     - 選中或清除“**僅當指定週期內存取了檔案(天)**”核取方塊並指定天數。
     - 選中或清除“**如果可以，不複製檔案到本機硬碟磁碟機**”核取方塊。
4. 點擊“**儲存**”。

將儲存新的工作配置。

掃描卸除式磁碟機

要在應用程式主控台中配置在卸除式磁碟機連線到受防護裝置時對其進行的掃描：

1. 在應用程式主控台樹狀目錄中，開啟“**Kaspersky Embedded Systems Security**”節點的內容功能表並選擇“**配置卸除式磁碟機掃描設定**”選項。
   將開啟“**卸除式磁碟機掃描**”視窗。
2. 在“**連接時掃描**”部分中，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“**掃描透過 USB 連接的卸除式磁碟機**”核取方塊。
- 如果需要，選中“**掃描卸除式磁碟機，如果其儲存的資料量未超過(MB)**”，然後在右側的欄位中指定最大值。
- 在“**掃描時使用的安全等級**”下拉清單中，指定卸除式磁碟機掃描所需設定的安全等級。

3. 點擊“**確定**”。

即會儲存並套用指定設定。

自訂掃描工作統計

執行自訂掃描工作時，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。

要檢視自訂掃描工作統計：

1. 在應用程式主控台樹狀目錄中展開“**自訂掃描**”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**”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	敘述
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。
偵測到受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。
偵測到疑似感染的物件	Kaspersky Embedded Systems Security 偵測到的疑似感染物件數。
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。
物件未移至隔離區	Kaspersky Embedded Systems Security 嘗試隔離未成功（例如，由於磁碟空間不足）的物件數。
物件未刪除	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。

物件未備份	Kaspersky Embedded Systems Security 嘗試在備份中儲存副本但未成功（例如，由於磁碟空間不足）的物件數。
處理錯誤	處理中導致錯誤的物件數目。
物件已解毒	Kaspersky Embedded Systems Security 已解毒的物件的數量。
已移至隔離區	Kaspersky Embedded Systems Security 已隔離的物件的數量。
已移至備份區	Kaspersky Embedded Systems Security 儲存至備份的檔案數目。
物件已刪除	Kaspersky Embedded Systems Security 已移除的物件的數量。
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。
物件已處理	Kaspersky Embedded Systems Security 已刪除的物件的總數。

透過點擊結果窗格中**"開啟工作記錄"**部分的**"管理"**連結，還可以在選定工作記錄中檢視自訂掃描工作統計。

建議您在工作完成後手動處理工作記錄中**"事件"**標籤上記錄的事件。

建立和配置"基線檔案完整性監控"工作

要建立或配置新的"基線檔案完整性監控"工作：

1. 在應用程式主控台樹狀目錄中，開啟**"系統稽核"**節點的內容功能表。
2. 選擇**"建立基準檔案完整性監控工作"**。
   將開啟**"新增工作"**視窗。
3. 在**"哈希計算演算法"**下拉清單中，選擇以下選項之一：
   - **MD5**
   - **SHA256**
4. 在**"監控區域"**表中，執行以下操作：
   a. 要在"基線檔案完整性監控"工作範圍中新增檔案或資料夾：
      1. 點擊**"新增"**按鈕。
         將開啟**"監控區域內容"**視窗。
      2. 選中或清除**"監控此區域"**核取方塊。
      3. 點擊**瀏覽**按鈕以指定要包括在「基線檔案完整性監控」工作範圍中的檔案或資料夾。
      4. 如果要在"基線檔案完整性監控"工作範圍中包括所有子資料夾，請選中**"同時監控子資料夾"**核取方塊。

5. 點擊**"確定"**。

b. 要變更先前新增到**"基線檔案完整性監控"**工作範圍的檔案或資料夾：

1. 點擊**"變更"**按鈕。

將開啟**"監控區域內容"**視窗。

2. 選中或清除**"監控此區域"**核取方塊。

3. 點擊**瀏覽**按鈕以指定要包括在「基線檔案完整性監控」工作範圍中的檔案或資料夾。

4. 如果要在**"基線檔案完整性監控"**工作範圍中包括或排除所有子資料夾，請選中或清除**"同時監控子資料夾"**核取方塊。

5. 點擊**"確定"**。

c. 要刪除先前新增到**"基線檔案完整性監控"**工作範圍中的檔案或資料夾，請在**"監控區域"**表中選擇此檔案或資料夾，然後點擊**"刪除"**按鈕。

5. 在**排程**和**進階**標籤上配置工作啟動排程設定。

6. 在**"執行帳戶"**標籤上，配置使用特定帳戶權限啟動工作的設定。

7. 在**新增工作**視窗中點擊**新增工作**。

即建立一個新的自訂**"基線檔案完整性監控"**工作。將在應用程式主控台樹狀目錄中顯示包含新工作名稱的節點。此操作將會記錄到系統稽核記錄中。

要開啟"基線檔案完整性監控"工作的設定：

1. 在應用程式主控台樹狀目錄中，展開**"系統稽核"**節點。

2. 選擇與要設定的工作相應的子節點。

3. 在子節點結果窗格中，點擊**"內容"**連結。

將開啟**"工作設定"**視窗。

透過 Web 外掛程式管理自訂掃描工作

在本節中，學習如何針對網路中的一台或所有受防護裝置導航 Web 外掛程式介面。

開啟自訂掃描工作精靈

要開始建立新的本機自訂掃描工作：

1. 在 Web 主控台的主視窗中，選擇**"裝置"**→**"受管理裝置"**。

2. 點擊**"群組"**標籤以選擇受防護裝置所屬的管理群組。

3. 點擊受防護裝置的名稱。

4. 在開啟的**"<裝置名稱>"**視窗中，選擇**"工作"**標籤。

5. 點擊**"新增"**。
   將開啟**"新增工作精靈"**視窗。
6. 在**"應用程式"**下拉清單中，選擇**"Kaspersky Embedded Systems Security"**。
7. 在**"工作類型"**下拉清單中，選擇**"自訂掃描"**工作。
8. 點擊**"下一步"**。

根據需要配置工作設定。

要開始建立新的群組自訂掃描工作：

1. 在 Web 主控台的主視窗中，選擇**"裝置"**→**"工作"**。
2. 點擊**"群組"**標籤以選取要為其建立工作的管理群組。
3. 點擊**"新增"**。
   將開啟**"新增工作精靈"**視窗。
4. 在**"應用程式"**下拉清單中，選擇**"Kaspersky Embedded Systems Security"**。
5. 在**"工作類型"**下拉清單中，選擇**"自訂掃描"**工作。
6. 點擊**"下一步"**。

根據需要配置工作設定。

要開始為自訂群組建立新的自訂掃描工作：

1. 在 Web 主控台的主視窗中，選擇**"裝置"**→**"裝置選擇"**。
2. 選取要為其建立工作的選項。
3. 點擊**"開始"**。
4. 在**"選擇結果"**視窗中，選擇要為其建立工作的裝置。
5. 點擊**"建立工作"**。
6. 在**"應用程式"**下拉清單中，選擇**"Kaspersky Embedded Systems Security"**。
7. 在**"工作類型"**下拉清單中，選擇**"自訂掃描"**工作。
8. 點擊**"下一步"**。

根據需要配置工作設定。

要配置現有自訂掃描工作：

1. 在 Web 主控台的主視窗中，選擇**"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。

將開啟“**<工作名稱>**”視窗。

開啟自訂掃描工作內容

要開啟單台受防護裝置的自訂掃描工作的應用程式內容：

1. 在 Web 主控台的主視窗中，選擇“**裝置**”→“**受管理裝置**”。
2. 點擊“**群組**”標籤以選擇受防護裝置所屬的管理群組。
3. 點擊受防護裝置的名稱。
4. 在開啟的“**<裝置名稱>**”視窗中，選擇“**工作**”標籤。
5. 在為裝置建立的工作清單中，選擇您建立的自訂掃描工作。
6. 開啟“**應用程式設定**”標籤。

配置工作掃描範圍

要配置現有自訂掃描工作的掃描範圍：

1. 開啟自訂掃描工作內容。
2. 選擇“**掃描範圍**”部分。
3. 執行以下操作之一：
   - 點擊“**新增**”按鈕以新增新規則。
   - 選擇一個現有規則，然後單擊“**編輯**”按鈕。

   將開啟“**編輯範圍**”視窗。
4. 將切換按鈕切換到“**活動**”，然後選擇一個物件類型。
5. 在“**物件防護**”部分中，配置以下設定：
   - **物件防護模式**：
     - **所有物件**
     - **按格式掃描物件**
     - **按病毒資料庫中指定的副檔名清單掃描物件**
     - **按指定的副檔名清單掃描物件**
   - **子資料夾**
   - **子檔案**

- **掃描開機磁區和 MBR**
- **掃描 NTFS 交換資料串流**
- 僅防護新增與變更過的檔案

6. 在“**複合物件防護**”部分中，指定要包含在掃描範圍內的複合物件：
   - **壓縮檔案**
   - **SFX 壓縮檔案**
   - **封裝的物件**
   - **電子郵件資料庫**
   - **純文字電子郵件**
   - **嵌入的 OLE 物件**
7. 在“**對受感染物件和其他物件執行的操作**”部分中，選擇要對受感染物件和其他偵測到的物件執行的操作。
   - **僅通知**。
   - **解毒**。
   - **解毒，無法解毒時刪除**解毒失敗則刪除。
   - **刪除**。
   - **建議**。
8. 在“**對可疑物件執行的操作**”部分中，選擇要對可疑感染物件執行的操作。
   - **僅通知**。
   - **隔離**。
   - **刪除**。
   - **建議**。
9. 在“**對可疑物件執行的操作**”部分中，選中或清除“**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“**排除**”部分中，配置以下設定：
    - 清除或選中“**排除檔案**”核取方塊。
    - 清除或選中“**不偵測**”核取方塊。
11. 在“**進階設定**”部分中，配置以下設定：
    - **超過以下時間則停止掃描(秒)**
    - **不掃描超過此值的複合物件 (MB)**

- **使用 iSwift 技術**
- **使用 iChecker 技術**

12. 在“**掃描離線檔案**”部分中，選取要對檔案執行的操作：
    - **不掃描**。
    - **僅掃描常駐檔案**。
    - **掃描完整檔案**。
      如果選擇此操作，則可以指定以下操作：
      - 選中或清除“**僅當指定週期內存取了檔案(天)**”核取方塊並指定天數。
      - 選中或清除“**如果可以，不複製檔案到本機硬碟磁碟機**”核取方塊。
13. 點擊“**確定**”按鈕。

配置工作設定

要配置現有自訂掃描工作的設定：

1. 開啟自訂掃描工作內容。
2. 選取“**選項**”部分。
3. 清除或選中“**使用啟發式分析**”核取方塊。
4. 如有必要，使用“**啟發式分析層級**”下拉清單選擇分析級別。
5. 在“**與其他元件整合**”部分中，配置以下設定：
    - 如果您希望從工作的掃描範圍中排除已新增到信任區域清單的物件，則選中“**套用信任區域**”核取方塊。
    - 如果您想要在工作中使用卡巴斯基安全網路雲端服務，請選取**在掃描中使用 KSN**核取方塊。
    - 若要向將執行該工作的處理程序分配“*低*”優先順序，請選中“**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）。
    - 要將所建立的工作當作關鍵區域掃描工作，請選中“**將工作視為關鍵區域掃描**”核取方塊。

信任區域

章節提供了有關 Kaspersky Embedded Systems Security 信任區域的資訊，以及如何在執行工作時將物件新增至信任區域的說明。

關於信任區域

受信任區域是防護或掃描範圍的排除清單，除了可以用來隔離掃描工作，還可以產生並套用到自訂掃描和即時檔案防護工作、新建立的自訂掃描工作和所有系統自訂掃描工作中。

預設情況下，在即時檔案防護和自訂掃描工作中套用信任區域。

可以將用於建立信任區域的規則清單匯出為 XML 設定檔，然後再將其匯入到其他受防護裝置上執行的 Kaspersky Embedded Systems Security 中。

受信任處理程序

套用到即時檔案防護工作。

如果受防護裝置上某些應用程式存取的檔案被 Kaspersky Embedded Systems Security 攔截，則這些應用程式運作上可能會不穩定。這些應用程式包括系統網域控制站的應用程式。

為了避免此類應用程式執行中斷，您可以對這些應用程式的正在執行的處理程序所存取的檔案停用防護（從而在信任區域中建立受信任處理程序清單）。

Microsoft Corporation 建議從即時檔案防護排除某些 Microsoft Windows 作業系統檔案和 Microsoft 應用程式檔案，因為程式不會被感染。Microsoft 網站（文章代碼：KB822158）上列出了一些此類別檔案的名稱。

您可以在信任區域中啟用或停用受信任處理程序。

如果可執行檔被修改（例如更新），Kaspersky Embedded Systems Security 會將其從受信任處理程序清單中排除。

應用程式不使用檔案在受防護裝置上的路徑來信任處理程序。受防護裝置上的檔案路徑僅用於搜尋檔案、計算核對總和以及為使用者提供有關可執行檔來源的資訊。

備份操作

套用於即時電腦防護工作。

當將儲存在硬碟磁碟機上的資料備份到外部裝置時，可以停用備份操作過程中存取的物件的防護。Kaspersky Embedded Systems Security 將掃描備份應用程式開啟並以 FILE_FLAG_BACKUP_SEMANTICS 內容讀取的物件。

排除

- 套用到即時檔案防護。

- 可在受防護裝置的指定區域中偵測到的所有物件。
- 在整個防護或掃描範圍內按名稱或名稱遮罩指定的偵測物件。

透過管理外掛程式管理信任區域

在本節中，學習如何透過管理外掛程式介面導航，以及如何為網路中的一台或所有受防護裝置配置信任區域。

導航

瞭解如何透過所選介面導航到所需工作設定。

開啟信任區域政策設定

要透過卡巴斯基安全管理中心政策開啟信任區域：

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。
5. 在打开的**"属性：<策略名称>"**窗口中，选择**"补充"**部分。
6. 在**"信任區域"**子區段中點擊**"設定"**按鈕。
   將開啟**"信任區域"**視窗。

根據需要配置信任區域。

如果某個受防護裝置受卡巴斯基安全管理中心啟動政策管理，且該政策禁止變更應用程式設定，則無法透過應用程式主控台編輯這些設定。

開啟信任區域內容視窗

要在"應用程式內容"視窗中配置信任區域：

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**"裝置"**標籤。

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。
   - 在受防護裝置的內容功能表中選擇**"內容"**項。

   將打开**"属性：<受保护设备名称>"**窗口。

5. 在**應用程式**區段中，選取 **Kaspersky Embedded Systems Security 3.1**。
6. 點擊**"內容"**按鈕。
   將開啟 **Kaspersky Embedded Systems Security 3.1** 應用程式設定視窗。
7. 選擇**"補充"部分。**
8. 在**"信任區域"**子區段中點擊**"設定"**按鈕。
   將開啟**"信任區域"**視窗。

根據需要配置信任區域。

透過管理外掛程式配置信任網域設定

預設情況下，信任區域套用於所有新建立的政策和工作。

要配置信任區域設定：

1. 在**"排除"**標籤上指定 Kaspersky Embedded Systems Security 在工作執行過程中略過的物件。
2. 在**"受信任處理程序"**標籤上指定 Kaspersky Embedded Systems Security 在工作執行過程中略過的處理程序。
3. 套用 not-a-virus 遮罩。

新增排除

要透過卡巴斯基安全管理中心政策向信任區域新增排除：

1. 開啟**"信任區域"**視窗。
2. 在「**排除**」標籤上，指定 Kaspersky Embedded Systems Security 在掃描和防護過程中要略過的物件：

   - 要建立建議的排除項目，請點擊「新增建議的排除項目」按鈕。
   - 要匯入預先配置的排除項目，請點擊**匯入**按鈕，然後在開啟的視窗中選擇儲存在裝置上的 XML 格式設定檔。

     XML 檔案中的排除項目將新增到排除項目清單中。
   - 要手動指定將物件視為受信任的條件，請點擊「**新增**」按鈕並執行下一個步驟。
     將開啟**"排除"**視窗。

3. 如果您在「**如果滿足以下條件，將不掃描物件**」部分指定了新增按鈕，指定要從防護/掃描範圍中排除的物件以及要從可偵測物件中排除的物件：

   - 如果要從防護或掃描範圍中排除物件：

     a. 選中"**要掃描的物件**"核取方塊。

     b. 點擊"**編輯**"按鈕。
     將開啟"**選擇物件**"視窗。

     c. 指定要從掃描範圍中排除的物件。

     > 指定物件時，可以使用名稱遮罩（透過 ? 和 * 字元）和所有類型的環境變數。當啟動工作或將新設定套用於正在執行的工作（不適用於自訂掃描工作）時，Kaspersky Embedded Systems Security 執行環境變數的解析（將變數取代為其值）。Kaspersky Embedded Systems Security 在用於啟動工作的帳戶下解析環境變數。有關環境變數的詳細資訊，請參閱 Microsoft 知識庫。

     d. 點擊"**確定**"。

     e. 如果要從防護或掃描範圍中排除指定物件的所有子檔案和資料夾，則選中"**套用於子資料夾**"核取方塊。

   - 如果要指定可偵測物件的名稱：

     a. 選中"**偵測物件**"核取方塊。

     b. 點擊"**編輯**"按鈕。
     將開啟"**偵測物件清單**"視窗。

     c. 按照病毒百科全書分類指定可偵測物件的名稱或名稱遮罩。

     d. 點擊"**新增**"按鈕。

     e. 點擊"**確定**"。

4. 在"**排除使用範圍**"部分中，選中應將排除套用於的工作的名稱旁邊的核取方塊。

5. 點擊"**確定**"。

排除顯示在"**排除**"視窗的"**信任區域**"標籤上的清單中。

新增受信任處理程序

要向受信任處理程序清單中新增一個或多個處理程序：

1. 開啟"**信任區域**"視窗。

2. 選擇"**受信任處理程序**"標籤。

3. 選取「不檢查檔案備份操作」核取方塊可略過對檔案讀取操作的掃描。

4. 選中"**不檢查指定處理程序的檔案活動**"核取方塊可跳過對受信任處理程序的檔案操作掃描。

5. 您可以使用以下其中一種方法將處理程序新增至受信任處理程序清單：

- 要匯入預先配置的受信任處理程序，請點擊**匯入**按鈕，然後在開啟的視窗中選擇儲存在裝置上的 XML 格式設定檔。

  XML 檔案中的處理程序將新增到受信任處理程序清單中。

- 要手動指定處理程序，請點擊**新增**按鈕並繼續下一步。

6. 如果您點擊**新增**按鈕，在按鈕的內容功能表中，選擇以下選項之一：

- **多個處理程序**。

  在開啟的**"新增信任處理程序"**視窗中，配置以下設定：

  a. **使用磁碟上的完整處理程序路徑來將它視為受信任**。

  b. **使用處理程序檔案雜湊來將它視為受信任**。

  c. 點擊**"瀏覽"**按鈕以根據可執行處理程序新增資料。

  d. 在開啟的視窗中選擇可執行檔。

  一次只能新增一個可執行檔。重複步驟 c-d 以新增其他可執行檔。

  e. 點擊**"處理程序"**按鈕以根據正在執行的處理程序新增資料。

  f. 在開啟的視窗中選擇處理程序。要選擇多個處理程序，請在選擇時按住 CTRL 鍵。

  g. 點擊**"確定"**。

  執行即時檔案防護工作的帳戶在裝有 Kaspersky Embedded Systems Security 的裝置上必須具有管理員權限，才允許檢視活動處理程序清單。您可以按檔案名稱、處理程序識別碼 (PID) 或處理程序的可執行檔在受防護裝置上的路徑來對活動處理程序清單中的處理程序進行排序。請注意，只有在受防護裝置上或透過卡巴斯基安全管理中心以指定的主機設定使用應用程式主控台時，才能透過點擊**"處理程序"**按鈕來選擇正在執行的處理程序。

- **一個基於檔案名稱和路徑的處理程序**。

  在開啟的**"新增處理程序"**視窗中，執行以下操作：

  a. 輸入可執行檔的路徑（包括檔案名稱）。

  指定物件時，可以使用名稱遮罩（透過 ? 和 * 字元）和所有類型的環境變數。當啟動工作或將新設定套用於正在執行的工作（不適用於自訂掃描工作）時，Kaspersky Embedded Systems Security 執行環境變數的解析（將變數取代為其值）。Kaspersky Embedded Systems Security 在用於啟動工作的帳戶下解析環境變數。有關環境變數的詳細資訊，請參閱 Microsoft 知識庫。

  b. 點擊**"確定"**。

- **一個基於物件內容的處理程序**。

  在開啟的**"新增受信任處理程序"**視窗中，配置以下設定：

  a. 點擊**"瀏覽"**按鈕以選擇處理程序。

b. **使用磁碟上的完整處理程序路徑來將它視為受信任**。

c. **使用處理程序檔案雜湊來將它視為受信任**。

d. 點擊**"確定"**。

要將所選處理程序新增到受信任處理程序清單，必須選擇至少一種信任條件。

7. **信任區域**在"信任區域"視窗中，點擊"確定"按鈕。

選定的檔案或處理程序將新增到**"信任區域"**視窗中的受信任處理程序清單。

套用 not-a-virus 遮罩

not-a-virus 遮罩允許略過可能被視為有害的合法軟體檔案和 Web 資源的掃描。該遮罩影響以下工作：

- 即時檔案防護。
- 自訂掃描。

如果未向排除清單新增該遮罩，Kaspersky Embedded Systems Security 將對此類別下的軟體套用在工作設定中指定的操作。

要套用 not-a-virus 遮罩：

1. 開啟**"信任區域"**視窗。
2. 如果清除該核取方塊，則在"排除"標籤上的"偵測物件"列中，捲動清單並選擇具有"not-a-virus:*"的行。
3. 點擊"確定"。

即套用新設定。

透過應用程式主控台管理信任區域

在本節中，學習如何透過應用程式主控台介面導航以及如何在受防護裝置上設定信任區域。

在應用程式主控台中對工作套用信任區域

預設情況下，信任區域套用於"即時檔案防護"工作、新增的自訂"自訂掃描"工作以及除"隔離區掃描"工作之外的所有系統"自訂掃描"工作。

啟用或停用信任域後，會在執行的工作內立即應用或停止套用指定的排除。

要在 Kaspersky Embedded Systems Security 工作中啟用和停用信任區域：

1. 在應用程式主控台樹狀目錄中，開啟要為其配置信任區域的工作的內容功能表。
2. 選擇**"內容"**。

將開啟**"工作設定"**視窗。

3. 在開啟的視窗中，選擇**"一般"**標籤，然後執行以下操作之一：

   - 要在工作中套用信任區域，請選定**"套用信任區域"**核取方塊。
   - 要在工作中停用信任區域，請清除**"套用信任區域"**核取方塊。

4. 如果要設定信任區域設定，請點擊**"套用信任區域"**核取方塊的名稱中的連結。
   將開啟**"信任區域"**視窗。
   在**"信任區域"**視窗中，配置排除項和受信任處理程序 ，然後點擊**"確定"**。

5. **工作設定**在工作設定視窗中點擊確定以儲存變更。

在應用程式主控台中配置信任區域設定

要配置信任區域設定：

1. 在**"排除"**標籤上指定 Kaspersky Embedded Systems Security 在工作執行過程中略過的物件。
2. 在**"受信任處理程序"**標籤上指定 Kaspersky Embedded Systems Security 在工作執行過程中略過的處理程序。
3. 對應用程式工作套用信任區域。
4. 套用 not-a-virus 遮罩。

將排除新增至信任區域

要透過應用程式主控台手動向信任區域新增排除項目：

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"**功能表選項。
   將開啟**"信任區域"**視窗。
3. 選擇**"排除"**標籤。
4. 指定 Kaspersky Embedded Systems Security 在掃描和防護過程中略過的物件：

   - 要匯入預先配置的排除項目，請點擊**匯入**按鈕，然後在開啟的視窗中選擇儲存在裝置上的 XML 格式設定檔。
     XML 檔案中的排除項目將新增到排除項目清單中。
   - 要手動指定將物件視為受信任的條件，請點擊「**新增**」按鈕並執行下一個步驟。
     將開啟**"排除"**視窗。

5. 如果您在「**如果滿足以下條件，將不掃描物件**」部分指定了新增按鈕，指定要從防護/掃描範圍中排除的物件以及要從可偵測物件中排除的物件：

- 如果要從防護或掃描範圍中排除物件：

  a. 選中“**要掃描的物件**”核取方塊。

  b. 點擊“**編輯**”按鈕。
  將開啟“**選擇物件**”視窗。

  c. 指定要從掃描範圍中排除的物件。

  > 指定物件時，可以使用名稱遮罩（透過 ? 和 * 字元）和所有類型的環境變數。當啟動工作或將新設定套用於正在執行的工作（不適用於自訂掃描工作）時，Kaspersky Embedded Systems Security 執行環境變數的解析（將變數取代為其值）。Kaspersky Embedded Systems Security 在用於啟動工作的帳戶下解析環境變數。有關環境變數的詳細資訊，請參閱 Microsoft 知識庫。

  d. 點擊“**確定**”。

  e. 如果要從防護或掃描範圍中排除指定物件的所有子檔案和資料夾，則選中“**套用於子資料夾**”核取方塊。

- 如果要指定可偵測物件的名稱：

  a. 選中“**偵測物件**”核取方塊。

  b. 點擊“**編輯**”按鈕。
  將開啟“**偵測物件清單**”視窗。

  c. 按照病毒百科全書分類指定可偵測物件的名稱或名稱遮罩。

  d. 點擊“**新增**”按鈕。

  e. 點擊“**確定**”。

6. 在“**排除使用範圍**”部分中，選中應將排除套用於的工作的名稱旁邊的核取方塊。
7. 點擊“**確定**”。

排除顯示在“**排除**”視窗的“**信任區域**”標籤上的清單中。

新增受信任處理程序

您可以使用以下某種方法將程序新增至受信任處理程序清單：

- 從受防護裝置上正在執行的處理程序清單中選擇。
- 選擇處理程序的可執行檔（不管程序目前是否正在執行）。

> 如果應用程式的可執行檔已修改，Kaspersky Embedded Systems Security 會將此處理程序從受信任處理程序清單排除。

要向受信任處理程序清單中新增一個或多個處理程序：

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**”功能表選項。

   將開啟“**信任區域**”視窗。

3. 選擇“**受信任處理程序**”標籤。

4. 選中“**不檢查檔案備份操作**”核取方塊可跳過對檔案讀取操作的掃描。

5. 選中“**不檢查指定處理程序的檔案活動**”核取方塊可跳過對受信任處理程序的檔案操作掃描。

6. 您可以使用以下其中一種方法將處理程序新增至受信任處理程序清單：

   - 要匯入預先配置的受信任處理程序，請點擊**匯入**按鈕，然後在開啟的視窗中選擇儲存在裝置上的 XML 格式設定檔。

     XML 檔案中的處理程序將新增到受信任處理程序清單中。

   - 要手動指定處理程序，請點擊**新增**按鈕並繼續下一步。

7. 如果您點擊**新增**按鈕，在按鈕的內容功能表中，選擇以下選項之一：

   - **多個處理程序**。

     在開啟的“**新增信任處理程序**”視窗中，配置以下設定：

     a. **使用磁碟上的完整處理程序路徑來將它視為受信任**。

     b. **使用處理程序檔案雜湊來將它視為受信任**。

     c. 點擊“**瀏覽**”按鈕以根據可執行處理程序新增資料。

     d. 在開啟的視窗中選擇可執行檔。

     > 一次只能新增一個可執行檔。重複步驟 c-d 以新增其他可執行檔。

     e. 點擊“**處理程序**”按鈕以根據正在執行的處理程序新增資料。

     f. 在開啟的視窗中選擇處理程序。要選擇多個處理程序，請在選擇時按住 **CTRL** 鍵。

     g. 點擊“**確定**”。

     > 執行即時檔案防護工作的帳戶在裝有 Kaspersky Embedded Systems Security 的裝置上必須具有管理員權限，才允許檢視活動處理程序清單。您可以按檔案名稱、處理程序識別碼 (PID) 或處理程序的可執行檔在受防護裝置上的路徑來對活動處理程序清單中的處理程序進行排序。請注意，只有在受防護裝置上或透過卡巴斯基安全管理中心以指定的主機設定使用應用程式主控台時，才能透過點擊“**處理程序**”按鈕來選擇正在執行的處理程序。

   - **一個基於檔案名稱和路徑的處理程序**。

     在開啟的“**新增處理程序**”視窗中，執行以下操作：

     a. 輸入可執行檔的路徑（包括檔案名稱）。

指定物件時，可以使用名稱遮罩（透過 **?** 和 ***** 字元）和所有類型的環境變數。當啟動工作或將新設定套用於正在執行的工作（不適用於自訂掃描工作）時，Kaspersky Embedded Systems Security 執行環境變數的解析（將變數取代為其值）。Kaspersky Embedded Systems Security 在用於啟動工作的帳戶下解析環境變數。有關環境變數的詳細資訊，請參閱 Microsoft 知識庫。

b. 點擊**"確定"**。

- **一個基於物件內容的處理程序**。

  在開啟的**"新增受信任處理程序"**視窗中，配置以下設定：

  a. 點擊**"瀏覽"**按鈕以選擇處理程序。

  b. **使用磁碟上的完整處理程序路徑來將它視為受信任**。

  c. **使用處理程序檔案雜湊來將它視為受信任**。

  d. 點擊**"確定"**。

要將所選處理程序新增到受信任處理程序清單，必須選擇至少一種信任條件。

8. 在**"信任區域"**視窗中，點擊**"確定"**按鈕。

選定的檔案或處理程序將新增到**"信任區域"**視窗中的受信任處理程序清單。

套用 not-a-virus 遮罩

not-a-virus 遮罩允許略過可能被視為有害的合法軟體檔案和 Web 資源的掃描。該遮罩影響以下工作：

- 即時檔案防護。
- 自訂掃描。

如果未向排除清單新增該遮罩，Kaspersky Embedded Systems Security 將對此類別下的軟體或 Web 資源套用在工作設定中指定的操作。

要套用 not-a-virus 遮罩：

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"**功能表選項。
   將開啟**"信任區域"**視窗。
3. 選擇**"排除"**標籤。
4. 捲動清單以尋找 *not-a-virus:** 值。
5. 選中相應的核取方塊（如果其處於清除狀態）。
6. 點擊**"確定"**。

即套用新設定。

透過 Web 外掛程式管理信任區域

要透過 Web 外掛程式管理信任區域：

1. 在 Web 控制的主視窗中，選取**裝置 → 政策和設定檔案**。
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**”標籤。
4. 選擇“**補充**”部分。
5. 在“**設定**”子區段中點擊“**信任區域**”。
6. 根據需要配置信任區域。

弱點利用防禦

本節包含有關如何配置處理程序記憶體防護設定的說明。

關於弱點利用防禦

Kaspersky Embedded Systems Security 提供防護處理程序記憶體免受弱點利用的能力。此功能在"弱點利用防禦"元件中實現。可以變更該元件的啟動狀態和配置處理程序記憶體防護設定。

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"（"代理"）防護處理程序記憶體免受弱點利用。

"處理程序防護代理"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：如果已移除"弱點利用防禦"元件，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。

Kaspersky Security 弱點利用防禦服務

受防護裝置上必須提供 Kaspersky Security 弱點利用防禦服務，這樣"弱點利用防禦"元件才能發揮最大效果。此服務和"弱點利用防禦"元件是建議安裝的一部分。在受防護裝置上安裝該服務的過程中，將建立和啟動 kavfswh 處理程序。此處理程序從元件將有關受防護的處理程序的資訊傳輸到安全性代理。

Kaspersky Security 弱點利用防禦服務停止後，Kaspersky Embedded Systems Security 繼續防護已新增到受防護的處理程序清單中的處理程序，同時也載入到新新增的處理程序中，並使用所有可用的弱點利用防禦技術來防護處理程序記憶體。

如果裝置正在執行 Windows 10 或更高版本的作業系統，在 Kaspersky Security 弱點利用防禦服務停止後，應用程式將不會繼續防護處理程序和處理程序記憶體。

如果 Kaspersky Security 弱點利用防禦服務已停止，則應用程式將不會接收隨受防護的處理程序出現的有關事件的資訊（包括有關弱點利用攻擊和處理程序終止的資訊）。此外，代理將無法接收新防護設定和新增新處理程序到受防護的處理程序清單中的有關資訊。

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：

- **發現弱點利用時終止**：當嘗試進行弱點利用時，應用此模式可終止處理程序。

  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。

- **僅通知**：應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。
  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。

透過管理外掛程式管理弱點利用防禦

在本節中，學習如何導航管理外掛程式介面，以及如何為網路中的一台或所有受防護裝置配置元件設定。

導航

瞭解如何透過所選介面導航到所需工作設定。

開啟弱點利用防禦的政策設定

要透過卡巴斯基安全管理中心政策開啟弱點利用防禦設定：

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。
5. 在打开的"**属性：<策略名称>**"窗口中，选择"**实时服务器保护**"部分。
6. 在"**弱點利用防禦**"子區段中點擊"**弱點利用防禦**"按鈕。
   將開啟"**弱點利用防禦**"視窗。

根據需要配置弱點利用防禦。

開啟弱點利用防禦內容視窗

要開啟弱點利用防禦內容視窗：

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**"裝置"**標籤。
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。
   - 在受防護裝置的內容功能表中選擇**"內容"**項。

   將打开**"属性：<受保护设备名称>"**窗口。
5. 在**應用程式**區段中，選取 **Kaspersky Embedded Systems Security 3.1**。
6. 點擊**"內容"**按鈕。
   將開啟 **Kaspersky Embedded Systems Security 3.1** 應用程式設定視窗。
7. 選擇**"即時電腦防護"部分。**
8. 在**"弱點利用防禦"**子區段中點擊**"設定"**按鈕。
   將開啟**"弱點利用防禦"**視窗。

根據需要配置弱點利用防禦。

配置處理程序記憶體防護設定

要配置設定以防護新增到受防護的處理程序清單中的處理程序記憶體，請執行以下操作：

1. 開啟**"弱點利用防禦"**視窗。
2. 在**"弱點利用防禦模式"**設定塊中，配置以下設定：
   - **防止易受感染的處理程序被利用弱點**。
     - **發現弱點利用時終止**。
     - **僅通知**。
3. 在**"防禦操作"**設定塊中，配置以下設定：
   - **透過"終端服務"通知被利用的處理程序**。
   - **即使 Kaspersky Security 服務已停用，也會防止易受感染的處理程序弱點遭到利用**。
4. 在**弱點利用防禦**視窗中點擊**確定**。

Kaspersky Embedded Systems Security 將儲存並套用配置的處理程序記憶體防護設定。

將處理程序新增到防護範圍

預設情況下，“弱點利用防禦”元件防護多個處理程序。可以透過清除清單中的相應核取方塊來將處理程序從防護範圍中排除。

要向受防護的處理程序清單中新增處理程序：

1. 開啟“**弱點利用防禦**”視窗。
2. 在“**受防護處理程序**”標籤上，點擊“**瀏覽**”按鈕。
   將開啟一個 Microsoft Windows 資源管理器視窗。
3. 選擇您要新增到該清單的處理程序。
4. 點擊“**開啟**”按鈕。
   處理程序名稱顯示在行中。
5. 點擊“**新增**”按鈕。
   處理程序將被新增到受防護的處理程序清單中。
6. 選擇新增的處理程序。
7. 點擊“**設定弱點利用防禦技術**”。
   將開啟“**弱點利用防禦技術**”視窗。
8. 選擇其中一個選項以應用攻擊緩解技術：
   - **套用所有可用的弱點利用防禦技術**。
     如果選擇此選項，則不能編輯清單。預設情況下，對處理程序套用所有可用技術。
   - **套用選定的弱點利用防禦技術**。
     如果選擇此選項，則您可以編輯已應用攻擊緩解技術：
     a. 選擇您要應用的技術旁邊的核取方塊，以防護選定的處理程序。
     b. 選中或清除“**套用受攻擊面減少技術**”核取方塊。
9. 配置“受攻擊面減少”技術的設定：
   - 輸入其啟動將受到“**拒絕模組**”欄位中受防護的處理程序封鎖的模組的名稱。
   - 在“**不拒絕已載入至“網際網路區域”中的模組**”欄位中，選擇您要在其下方允許模組啟動的選項旁邊的核取方塊：
     - **網際網路**
     - **本機網際網路**
     - **受信任的網站**

- **受限制的網站**
- **電腦**

> 這些設定僅適用於 Internet Explorer。

10. 點擊**"確定"**。

該處理程序將新增到工作防護範圍中。

透過應用程式主控台管理弱點利用防禦

在本節中，學習如何導航應用程式主控台介面以及如何在受防護裝置上配置元件設定。

導航

瞭解如何透過所選介面導航到所需工作設定。

開啟弱點利用防禦一般設定

*要開啟**"弱點利用防禦設定"**視窗：*

1. 在應用程式主控台樹狀目錄中，展開**即時檔案防護**節點。
2. 選取**弱點利用防禦**節點。
3. 在**處理程序防護設定**區段中，點擊**內容**連結。
   將開啟**"弱點利用防禦設定"**視窗。

根據需要配置弱點利用防禦的一般設定。

開啟弱點利用防禦處理程序防護設定

*要開啟「**處理程序防護設定**」視窗：*

1. 在應用程式主控台樹狀目錄中，展開**即時檔案防護**節點。
2. 選取**弱點利用防禦**節點。

在**處理程序防護設定**區段中，點擊**處理程序防護參數**連結。

將開啟**"處理程序防護設定"**視窗。

根據需要配置弱點利用防禦的處理程序防護設定。

配置處理程序記憶體防護設定

要向受防護的處理程序清單中新增處理程序：

1. 開啟“**弱點利用防禦設定**”視窗。
2. 在“**弱點利用防禦模式**”設定塊中，配置以下設定：
   - **防止易受感染的處理程序被利用弱點**。
     - **發現弱點利用時終止**。
     - **僅通知**。
3. 在“**防禦操作**”設定塊中，配置以下設定：
   - **透過“終端服務”通知被利用的處理程序**。
   - **即使 Kaspersky Security 服務已停用，也會防止易受感染的處理程序弱點遭到利用**。
4. 在**弱點利用防禦設定**視窗中點擊**弱點利用防禦設定**。

Kaspersky Embedded Systems Security 將儲存並套用配置的處理程序記憶體防護設定。

將處理程序新增到防護範圍

預設情況下，“弱點利用防禦”元件防護多個處理程序。您可以在受防護處理程序清單中取消選中您不想防護的處理程序。

要向受防護的處理程序清單中新增處理程序：

1. 開啟“**處理程序防護設定**”視窗。
2. 要新增處理程序以防護其不被濫用並減少可能的弱點利用影響，請執行以下操作：
   a. 點擊“**瀏覽**”按鈕。
   將開啟標準 Microsoft Windows“**開啟**”視窗。
   b. 在開啟的視窗中，選擇您要新增到該清單的處理程序。
   c. 點擊“**開啟**”按鈕。
   d. 點擊“**新增**”按鈕。
   處理程序將被新增到受防護的處理程序清單中。
3. 在清單中選擇處理程序。
4. 目前配置顯示在「**處理程序防護設定**」標籤上：
   - **處理程序名稱**。

- **正在執行**。
- **已套用弱點利用防禦技術**。
- **受攻擊面減少設定**。

5. 要修改套用於該處理程序的弱點利用防禦技術，請選擇**"弱點利用防禦技術"**標籤。
6. 選擇其中一個選項以應用攻擊緩解技術：
   - **套用所有可用的弱點利用防禦技術**。
     如果選擇此選項，則不能編輯清單。預設情況下，對處理程序套用所有可用技術。
   - **針對處理程序套用列出的弱點利用防禦技術**。
     如果選擇此選項，則您可以編輯已應用攻擊緩解技術：
     a. 選擇您要應用的技術旁邊的核取方塊，以防護選定的處理程序。
7. 配置"受攻擊面減少"技術的設定：
   - 輸入其啟動將受到**"拒絕模組"**欄位中受防護的處理程序封鎖的模組的名稱。
   - 在**不拒絕已載入至網際網路區域中的模組**區段中，選取您要允許模組啟動的選項旁邊的核取方塊：
     - **網際網路**
     - **本機網際網路**
     - **受信任的網站**
     - **受限制的網站**
     - **電腦**

     這些設定僅適用於 Internet Explorer。
8. 點擊**"儲存"**。

該處理程序將新增到工作防護範圍中。

透過 Web 外掛程式管理弱點利用防禦

在本節中，學習如何導航 Web 外掛程式介面以及如何在受防護裝置上配置元件設定。

配置處理程序記憶體防護設定

要配置設定以防護新增到受防護的處理程序清單中的處理程序記憶體，請執行以下操作：

1. 在 Web 控制的主視窗中，選取**裝置 → 政策和設定檔案**。

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**"標籤。
4. 選擇"**即時電腦防護**"部分。
5. 在"**設定**"子區段中點擊"**弱點利用防禦**"。
6. 開啟"**弱點利用防禦設定**"標籤。
7. 在"**弱點利用防禦模式**"設定塊中，配置以下設定：
   - **防止易受感染的處理程序被利用弱點**。
     - **發現弱點利用時終止**。
     - **僅通知**。
8. 在"**防禦操作**"設定塊中，配置以下設定：
   - **透過"終端服務"通知被利用的處理程序**。
   - **即使 Kaspersky Security 服務已停用，也會防止易受感染的處理程序弱點遭到利用**。
9. 在**弱點利用防禦**視窗中點擊**弱點利用防禦**。

Kaspersky Embedded Systems Security 將儲存並套用配置的處理程序記憶體防護設定。

將處理程序新增到防護範圍

要配置設定以防護新增到受防護的處理程序清單中的處理程序記憶體，請執行以下操作：

1. 在 Web 控制的主視窗中，選取**裝置 → 政策和設定檔案**。
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**"標籤。
4. 選擇"**即時電腦防護**"部分。
5. 在"**設定**"子區段中點擊"**弱點利用防禦**"。
6. 開啟"**受防護處理程序**"標籤。
7. 點擊"**新增**"按鈕。
8. 將開啟"**弱點利用防禦技術**"視窗。
9. 指定程序名稱。
10. 選擇其中一個選項以應用攻擊緩解技術：
    - **套用所有可用的弱點利用防禦技術**。
      如果選擇此選項，則不能編輯清單。預設情況下，對處理程序套用所有可用技術。

- **套用選定的弱點利用防禦技術**。

  如果選擇此選項，則您可以編輯已應用攻擊緩解技術：

  a. 選擇您要應用的技術旁邊的核取方塊，以防護選定的處理程序。

  b. 選中或清除**"應用攻擊面減少技術"**核取方塊。

11. 配置"受攻擊面減少"技術的設定：

- 輸入其啟動將受到**"拒絕模組"**欄位中受防護的處理程序封鎖的模組的名稱。
- 在**"不拒絕在網際網路區域中啟動的模組"**欄位中，選擇您要在其下方允許模組啟動的選項旁邊的核取方塊：
  - **網際網路**
  - **本機 Intranet**
  - **信任的 URL**
  - **限制的 URL**
  - **電腦**

> 這些設定僅適用於 Internet Explorer。

12. 點擊**"確定"**。

該處理程序將新增到工作防護範圍中。

弱點利用防禦技術

弱點利用防禦技術

弱點利用防禦技術	敘述
資料執行防護 (DEP)	資料執行防護封鎖在受防護的記憶體區域中執行任意代碼。
位址空間佈局隨機化 (ASLR)	改變處理程序位址空間內資料結構佈局。
結構化例外處理常式覆蓋防護 (SEHOP)	異常記錄的取代或異常處理程式的取代。
空頁分配	防護重定向空指針。
LoadLibrary 網路調用檢查（ROP 防護）	防止從網路路徑載入 DLL。
可執行檔堆疊（ROP 防護）	封鎖堆疊區域的非授權執行。
RET 防護檢查（ROP 防護）	檢查確保安全調用 CALL 指令。
堆疊透視防護（ROP 防護）	防止將 ESP 堆疊指標重新定位到可執行檔位址。
簡單匯出位址表存取監視（EAT 存取監視和透過診斷寄存器的 EAT 存取監視）	防止對 kernel32.dll、kernelbase.dll 和 ntdll.dll 匯出位址表的讀取存取
堆噴射分配 (Heapspray)	防止將記憶體分配用於執行惡意程式碼。
執行流模擬（返回導向編程防護）	偵測 Windows API 元件中可能存在危險的指令鏈（潛在

	ROP 小工具）。
IntervalProfile 調用監視（協助工具驅動程式防護 (AFDP)）	防止透過 AFD 驅動程式中的弱點進行提權（透過 QueryIntervalProfile 調用在 Ring 0 中執行任意代碼）。
受攻擊面減少 (ASR)	透過受防護的處理程序封鎖啟動易受攻擊的載入項。
處理程序挖空防護 (Hollowing)	防止建立和執行受信任處理程序的惡意副本。
AtomBombing 防護(APC)	透過非同步程序呼叫 (APC) 利用全域原子表弱點。
CreateRemoteThread 防護 (RThreadLocal)	其他處理程序已在受防護處理程序中建立執行緒。
CreateRemoteThread 防護 (RThreadRemote)	受防護處理程序已在其他處理程序中建立執行緒。

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

本節包含有關安裝期間由 Kaspersky Embedded Systems Security 註冊的 Microsoft Windows 系統監視器的效能計數器的資訊。

關於 Kaspersky Embedded Systems Security 效能計數器

預設情況下，"效能計數器"元件包含在 Kaspersky Embedded Systems Security 的已安裝元件中。Kaspersky Embedded Systems Security 在安裝期間在 Microsoft Windows 系統監視器中註冊其自己的效能計數器。

使用 Kaspersky Embedded Systems Security 計數器，您可用於監視執行即時電腦防護工作時應用程式的效能。當它與其他應用程式一起執行並出現資源不足時，您可以確定瓶頸。您可以診斷 Kaspersky Embedded Systems Security 崩潰並確定不合要求的設定。

透過在 Windows 控制台的"**管理**"部分中開啟"**效能**"主控台，來檢視 Kaspersky Embedded Systems Security 效能計數器。

下列章節列出了計數器定義、獲取讀數的建議時間間隔、上限值以及在計數器值超過上限值時建議的 Kaspersky Embedded Systems Security 設定。

拒絕需求總數

拒絕需求總數

名稱	拒絕需求總數
定義	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。
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： • 計數器在較長的時間段內顯示了許多被拒絕的請求：由於完全載入了所有 Kaspersky Embedded Systems Security 處理程序，Kaspersky Embedded Systems Security 無法掃

	描物件。 若要避免略過物件，請增加用於完成即時電腦防護工作的應用程式處理程序的數量。您可以使用**最大活動處理程序數**和**用於即時防護的處理程序數**等 Kaspersky Embedded Systems Security 設定。 • 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

名稱	略過請求總數
定義	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。

因為系統資源不足而未處理的需求數

因為系統資源不足而未處理的需求數

名稱	因為資源不足而未處理的要求數。
定義	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 工作處理程序需要更多 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。

傳送以供處理的需求數

傳送以供處理的需求數

名稱	傳送以供處理的需求數。
定義	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

檔案攔截調度程式執行緒的平均數

檔案攔截調度程式執行緒的平均數

名稱	檔案攔截調度程式執行緒的平均數。
定義	一個處理程序中的檔案攔截調度程式流數量，對於目前參與即時電腦防護工作的所有處理程序而言，則為檔案攔截調度程式流的平均數量。
用途	該計數器可用於偵測並消除由於 Kaspersky Embedded Systems Security 處理程序滿負荷工作而可能導致的即時電腦防護能力下降的情況。
標準值/上限值	視情況有所不同 / 40
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	每個工作程序中最多可建立 60 個檔案攔截調度程式執行緒。如果計數器接近 60，則可能會有工作程序無法處理佇列中下一個檔案攔截驅動程式要求的風險，且 Kaspersky Embedded Systems Security 會略過物件。 請增加用於完成即時電腦防護工作的 Kaspersky Embedded Systems Security 處理程序的數量。您可以使用**最大活動處理程序數**和**用於即時防護的處理程序數**等 Kaspersky Embedded Systems Security 設定。

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最大數

名稱	檔案攔截調度程式執行緒的最大數。

定義	一個處理程序中的檔案攔截調度程式流數量，對於目前參與即時電腦防護工作的所有處理程序而言，則為檔案攔截調度程式流的最大數量。
用途	此計數器可讓您偵測與修除因執行中程序負載分配不平均所造成的效能低落。
標準值/上限值	視情況有所不同 / 40
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	如果計數器的值超過"**檔案攔截調度程式執行緒的平均數**"計數器的值並繼續增加，則表示 Kaspersky Embedded Systems Security 正在執行的處理程序分配負載時不夠平均。 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

名稱	受感染物件佇列中的元素數。
定義	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"工作中有大量受感染或可能受感染物件，也表示病毒爆發。可以在工作統計或工作記錄中檢視有關偵測到的物件的數量的資訊。

每秒處理的物件數

每秒處理的物件數

名稱	每秒處理的物件數。

定義	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。如果一般計數器值下降，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。

Kaspersky Embedded Systems Security SNMP 計數器和 TRAP

本節包含有關 Kaspersky Embedded Systems Security 計數器和 TRAP 的資訊。

關於 Kaspersky Embedded Systems Security SNMP 計數器和 TRAP

如果要安裝一組防毒元件中包括 SNMP 計數器和 TRAP，則可以使用簡單網路管理協定 (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	傳送以供處理的需求數
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

隔離計數器

隔離計數器

計數器	定義
totalObjects	目前在隔離中的物件數
totalSuspiciousObjects	目前在隔離中的可能受感染物件數
currentStorageSize	隔離區中的資料總量 (MB)

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	受防護裝置關鍵區域自上次完成掃描以來的期限（自從上次完成"關鍵區域掃描"的工作後所經過的時間，單位為秒）。
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	資料庫"時效"（自最新安裝的資料庫更新的建立日期以來所經歷的時間，單位為百分之一秒）。

即時檔案防護計數器

計數器	定義
totalObjectsProcessed	上次執行"即時檔案防護"工作時掃描的物件總數
totalInfectedObjectsFound	上次"執行即時檔案防護"工作時受感染和其他的物件總數
totalSuspiciousObjectsFound	上次執行"即時檔案防護"工作時可能受感染物件總數
totalVirusesFound	上次執行"即時檔案防護"工作時偵測到的威脅總數
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 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
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

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：偵測到一個物件。
  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。備份區中的資料總量超過"**最大備份空間 (MB)**"所指定的值。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：已達到備份可用空間上限值。備份區中的可用空間容量小於或等於"**可用空間上限值 (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

- eventQuarantineStorageSizeExceeds：已超過最大隔離容量。隔離中資料的總大小已超過"**隔離區最大容量 (MB)**"所指定的值。Kaspersky Embedded Systems Security 會繼續隔離可能受感染物件。

  TRAP 具有以下選項：

  - eventDateAndTime
  - eventSeverity
  - eventSource

- eventThresholdQuarantineStorageSizeExceeds：已達到隔離區可用空間上限值。"**可用空間上限值(MB)**"指派的隔離區可用空間量等於或低於指定值。Kaspersky Embedded Systems Security 繼續備份受感染的物件。

  TRAP 具有以下選項：

  - eventDateAndTime
  - eventSeverity
  - eventSource

- eventObjectNotQuarantined：隔離區錯誤。

  TRAP 具有以下選項：

  - eventSeverity
  - eventDateAndTime
  - eventSource
  - userName
  - computerName
  - objectName

- storageObjectNotAddedEventReason

- eventObjectNotBackuped：在備份區中儲存物件副本時發生錯誤。

  TRAP 具有以下選項：

  - eventSeverity
  - eventDateAndTime
  - eventSource
  - objectName
  - userName
  - computerName
  - storageObjectNotAddedEventReason

- eventQuarantineInternalError：隔離區內部錯誤。

  TRAP 具有以下選項：

  - eventSeverity
  - eventDateAndTime
  - eventSource
  - eventReason

- eventBackupInternalError：備份錯誤。

  TRAP 具有以下選項：

  - eventSeverity
  - eventDateAndTime
  - eventSource
  - eventReason

- eventAVBasesOutdated：防毒軟體資料庫已過期。自上次執行資料庫更新工作（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：防毒軟體資料庫嚴重過期。自上次執行資料庫更新工作（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：Kaspersky Embedded Systems Security 正在執行。
  TRAP 具有以下選項：
  - eventSeverity
  - eventDateAndTime
  - eventSource
- eventApplicationShutdown：Kaspersky Embedded Systems Security 已停止。
  TRAP 具有以下選項：
  - eventSeverity
  - eventDateAndTime
  - eventSource
- eventCriticalAreasScanWasntPerformForALongTime：很長時間未掃描關鍵區域。自上次"關鍵區域掃描"工作完成以來的天數。
  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

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) - 不明的功能性元件
- 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) - 僅有在無法使用隔離或備份時，才適用於隔離或備份的事件（存取權限不足，或在隔離設定中指定錯誤的資料夾，例如指定了網路路徑）。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確定的物件名稱。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 - 木馬程式
  - 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：

- 可疑 (suspicious) - Kaspersky Embedded Systems Security 在物件的一段程式碼中偵測到部分符合不明威脅程式碼的結果。
- 確定 (Sure) - Kaspersky Embedded Systems Security 偵測到物件程式碼的一部分與已知惡意程式碼部分完全符合。

- 天數 (days)：天數（例如，產品授權到期日前的天數）。
- errorCode：錯誤代碼。
- knowledgeBaseId：知識庫文章的位址（例如說明特定錯誤之文章的位址）。
- 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 - 無效的特徵碼。
  - reasonCantCreateFolder - 無法建立資料夾。
  - reasonFileOperError - 檔案操作錯誤。
  - reasonDataCorrupted - 物件已損毀。
  - reasonConnectionReset - 連線重設。
  - reasonTimeOut - 已超過連線逾時。
  - reasonProxyAuthError - 代理驗證錯誤。
  - reasonServerAuthError - 伺服器驗證錯誤。
  - reasonHostNotFound - 未找到裝置。
  - reasonServerBusy - 無法使用伺服器。
  - 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。
- storageObjectNotAddedEventReason：未備份或未隔離物件的原因。
  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，必須還原 Kaspersky Embedded Systems Security；b) Kaspersky Embedded Systems Security 檔案所在的磁碟已毀損。
- 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。

與 WMI 整合

Kaspersky Embedded Systems Security 支援與 Windows Management Instrumentation (WMI) 整合：您可以使用支援 WMI 的用戶端系統透過基於 Web 的企業管理 (WBEM) 標準接收資料，以接收有關 Kaspersky Embedded Systems Security 及其元件的狀態的資訊。

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形式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	敘述	值
ProductName	已安裝的應用程式的名稱。	不帶版本號的應用程式全名。
ProductVersion	已安裝的應用程式的完整版	應用程式完整版本號，包括內部版本號。

	本。	
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 - 產品授權金鑰尚未新增到應用程式。 • True - 產品授權金鑰已新增到應用程式。
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 - 無法獲取目前金鑰的資訊，或者指定金鑰無法用於啟動應用程式（例如，根據金鑰拒絕名單將其封鎖）。
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，則該欄位的值為“未安裝”。
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”元件已啟用並正在提供防護。 • False -“弱點利用防禦”元件未提供防護。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，該欄位的值為“無”。
IsAppControlRunning	“應用程式啟動控制”工作的狀態。	“應用程式啟動控制”工作的狀態。 • True - “應用程式啟動控制”工作目前正在執行。 • False -“應用程式啟動控制”工作目前未執行或“應用程式啟動控制”元件未安裝。
AppControlMode	“應用程式啟動控制”工作模式。	敘述“應用程式啟動控制”元件的目前狀態，以及相應工作的選定模式。 可能的值： • 啟動 - 工作設定中選擇了**“活動”**模式。 • 僅統計 - 工作設定中選擇了**“僅統計”**模式。

		• 未安裝 - “應用程式啟動控制”元件未安裝。
AppControlRulesNumber	應用程式啟動控制規則總數。	“應用程式啟動控制”工作設定中目前指定的規則數量。
AppControlLastBlocking	“應用程式啟動控制”工作上次在任一模式下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時的日期和時間。該欄位包括所有已封鎖的應用程式，不管工作模式為何。 如果在處理 WMI 查詢時未註冊已封鎖的應用程式啟動的實例，該欄位將被分配值“無”。
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，則該欄位的值為“無”。
ConnectionState	WMI 提供程式元件與 Kaspersky Security 服務 (KAVFS) 之間的連線的狀態。	有關 WMI 提供程式元件與 Kaspersky Security 服務之間的連線狀態的資訊。 可能的值： • 成功 - 連線已成功建立：WMI 用戶端可以接收應用程式狀態。 • 失敗。錯誤代碼：<代碼> - 由於出現指定代碼的錯誤，無法建立連線。

此資料表示實例內容 KasperskySecurity_ProductInfo.ProductName=Kaspersky Embedded Systems Security，其中：

- KasperskySecurity_ProductInfo 是 Kaspersky Embedded Systems Security 類的名稱
- .ProductName=Kaspersky Embedded Systems Security 是 Kaspersky Embedded Systems Security 關鍵屬性

該實例在 ROOT\Kaspersky\Security 命名空間中建立。

從命令列使用 Kaspersky Embedded Systems Security

本節敘述從命令列使用 Kaspersky Embedded Systems Security。

指令

您可以使用命令列實用工具元件從受防護裝置的命令列執行基本的 Kaspersky Embedded Systems Security 管理命令，該元件包含在 Kaspersky Embedded Systems Security 軟體元件群組中。

使用命令列僅可管理那些可以根據 Kaspersky Embedded Systems Security 分配給您的權限來存取的功能。

某些 Kaspersky Embedded Systems Security 指令在以下模式下執行：

- 同步模式：只有指令完成後，控制權才會返回到主控台。
- 非同步模式：指令啟動後，控制權立即返回到主控台。

要在同步模式下中斷被執行的指令，

按 **Ctrl+C** 鍵盤快速鍵。

輸入 Kaspersky Embedded Systems Security 指令時，應遵循以下規則：

- 使用大寫和小寫輸入參數和指令。
- 使用空白分隔參數。
- 如果指定為一個值的檔案/資料夾位置包含空白，請使用引號將路徑括起來，例如：`"C:\TEST\test cpp.exe"`。
- 若有需要，可以在檔案名稱或路徑中使用萬用字元，例如：`"C:\Temp\Temp*\"`、`"C:\Temp\Temp???.doc"`、`"C:\Temp\Temp*.doc"`。

您可以使用指令行執行 Kaspersky Embedded Systems Security 的管理所需的每個操作（請參見下表）。

Kaspersky Embedded Systems Security 指令

指令	敘述
KAVSHELL APPCONTROL	根據選定匯入規則更新規則清單。
KAVSHELL APPCONTROL /CONFIG	設定“應用程式啟動控制”工作的執行模式
KAVSHELL APPCONTROL /GENERATE	啟動“應用程式啟動控制規則產生器”工作。
KAVSHELL VACUUM	對 Kaspersky Embedded Systems Security 記錄檔案進行磁碟整理。
KAVSHELL PASSWORD	管理密碼防護設定。
KAVSHELL HELP	顯示 Kaspersky Embedded Systems Security 指令說明。
KAVSHELL START	啟動 Kaspersky Security 服務。
KAVSHELL STOP	停止 Kaspersky Security 服務。

KAVSHELL SCAN	建立並啟動暫時自訂掃描工作，其掃描範圍和安全性設定由命令列選項指定。
KAVSHELL SCANCRITICAL	啟動「關鍵區域掃描」本機系統工作。
KAVSHELL TASK	非同步開始、暫停/繼續、停止指定工作、返回目前工作狀態/統計。
KAVSHELL RTP	開始或停止所有即時電腦防護工作。
KAVSHELL UPDATE	以命令列選項指定的設定啟動資料庫更新工作。
KAVSHELL ROLLBACK	將資料庫回復至之前版本。
KAVSHELL LICENSE	新增或刪除金鑰。顯示有關已新增的金鑰資訊。
KAVSHELL TRACE	啟用或停用追蹤。管理追蹤設定。
KAVSHELL DUMP	啟用或停用當 Kaspersky Embedded Systems Security 處理程序異常終止時建立 Dump 檔案。
KAVSHELL IMPORT	從設定檔匯入一般 Kaspersky Embedded Systems Security 設定、功能及工作。
KAVSHELL EXPORT	將所有 Kaspersky Embedded Systems Security 設定和現有工作匯出至設定檔。
KAVSHELL DEVCONTROL	根據選定的方法新增到已產生的裝置控制規則清單中。

顯示 Kaspersky Embedded Systems Security 指令說明：KAVSHELL HELP

要檢視所有 Kaspersky Embedded Systems Security 指令的清單，請執行以下指令之一：

```
KAVSHELL

KAVSHELL HELP

KAVSHELL /?
```

要檢視指令概覽及其語法，請執行下列一個指令：

```
KAVSHELL HELP <指令>

KAVSHELL <指令> /?
```

KAVSHELL HELP 範例

若要檢視有關 KAVSHELL SCAN 指令的詳細資訊，請執行下列指令：

```
KAVSHELL HELP SCAN
```

啟動和停止 Kaspersky Security 服務：KAVSHELL START，KAVSHELL STOP

若要停止 Kaspersky Security 服務，請執行以下指令：

```
KAVSHELL START
```

預設情況下，Kaspersky Security 服務啟動時，"即時檔案防護"和"在作業系統啟動時掃描"工作以及其他排程在"**在應用程式啟動時**"啟動的工作也會一起啟動。

要停止 Kaspersky Security 服務，請執行以下指令：

```
KAVSHELL STOP
```

執行此指令可能需要密碼。要輸入目前密碼，請使用 `[/pwd:<密碼>]`。

掃描指定區域：KAVSHELL SCAN

要啟動掃描受防護裝置特定區域的工作，請使用 `KAVSHELL SCAN`。命令列選項指定選定節點的掃描範圍和安全性設定。

使用 `KAVSHELL SCAN` 指令啟動的自訂掃描工作為暫時工作。它僅在執行時才顯示在應用程式主控台中（您無法在應用程式主控台中檢視其工作設定）。但是，將建立工作效能記錄，並顯示在應用程式主控台中的"**工作記錄**"節點下。

在自訂掃描工作中指定路徑時，可以使用環境變數。如果使用使用者環境變數，請以相應使用者身分執行 `KAVSHELL SCAN` 指令。

`KAVSHELL SCAN` 指令在同步模式下執行。

要從命令列啟動現有自訂掃描工作，請使用 KAVSHELL TASK 指令。

KAVSHELL SCAN 指令語法

```
KAVSHELL SCAN <掃描範圍> [/MEMORY|/SHARED|/STARTUP|/REMDRIVES|/FIXDRIVES|/MYCOMP] [/L:<具有掃描範圍清單的檔案路徑>] [/F<A|C|E>] [/NEWONLY] [/AI:<DISINFECT|DISINFDEL|DELETE|REPORT|AUTO>] [/AS:<QUARANTINE|DELETE|REPORT|AUTO>] [/DISINFECT|/DELETE] [/E:<ABMSPO>] [/EM:<"遮罩">] [/ES:<大小>] [/ET:<秒數>] [/TZOFF] [/OF:<SKIP|RESIDENT|SCAN[=<天數>] [NORECALL]>] [/NOICHECKER][/NOISWIFT][/ANALYZERLEVEL] [/NOCHECKMSSIGN][/W:<工作記錄檔案的路徑>] [/ANSI] [/ALIAS:<工作別名>]
```

KAVSHELL SCAN 指令有必需和可選參數/選項（請參閱下表）。

KAVSHELL SCAN 指令範例

```
KAVSHELL SCAN Folder56 D:\Folder1\Folder2\Folder3\ C:\Folder1\ C:\Folder2\3.exe "\\another server\Shared\" F:\123\*.fgb /SHARED /AI:DISINFDEL /AS:QUARANTINE /FA /E:ABM /EM:"*.xtx;*.fff;*.ggg;*.bbb;*.info" /NOICHECKER /ANALYZERLEVEL:1 /NOISWIFT /W:log.log
```

```
KAVSHELL SCAN /L:scan_objects.lst /W:c:\log.log
```

KAVSHELL SCAN 命令列參數/選項

參數/選項	敘述
掃描範圍。必需參數。	
<檔案>	指定掃描範圍 – 檔案清單、資料夾、網路路徑及預先定義的區域。 指定通用命名約定 (UNC) 格式的網路路徑。 在下面的範例中，指定 Folder4 資料夾時沒有路徑，表示該資料夾位於執行 KAVSHELL 指令的資料夾中： KAVSHELL SCAN Folder4 如果要掃描的物件的名稱包含空白，則必須將其擴在引號內。
<資料夾>	
<網路路徑>	如果指定資料夾，Kaspersky Embedded Systems Security 還將掃描其所有子資料夾。 可以使用符號 * 或 ? 來掃描一組檔案。
/MEMORY	掃描 RAM 中的物件
/SHARED	掃描受防護裝置上的共用資料夾
/STARTUP	掃描自動執行物件
/REMDRIVES	掃描卸除式磁碟機
/FIXDRIVES	掃描硬碟
/MYCOMP	掃描受防護裝置所有的區域
/L: <帶有掃描範圍清單的檔案路徑>	帶有掃描範圍清單的檔案的完整路徑。 使用換行鍵界定檔案的掃描範圍。您可以指定預定義的掃描區域，如以下包含掃描範圍清單的檔案內容範例： C:\ D:\Docs*.doc E:\My Documents /STARTUP /SHARED
掃描物件（檔案類型）。如果您指定此選項，Kaspersky Embedded Systems Security 將依據物件格式掃描物件。	
/FA	掃描所有物件
/FC	依據格式掃描物件（預設）。Kaspersky Embedded Systems Security 只掃描其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。Kaspersky Embedded Systems Security 只掃描受感染物件副檔名清單中包含的副檔名物件。
/NEWONLY	僅掃描新增與變更過的檔案。 如果不指定此選項，Kaspersky Embedded Systems Security 將掃描所有物件。
對受感染物件和其他物件執行的操作。如果未指定此指令參數，Kaspersky Embedded Systems Security 將執行"**略過**"操作。	
DISINFECT	解毒，如果無法解毒則略過 最新版本的 Kaspersky Embedded Systems Security 中保留了 DISINFECT 和 DELETE 選項，以確保與以前版本的相容性。可以使用這些選項代替 /AI 和 /AS 選項。這種情況下，Kaspersky Embedded Systems Security 不會處理可疑物件。

DISINFDEL	解毒，如果無法解毒則刪除
DELETE	刪除 最新版本的 Kaspersky Embedded Systems Security 中保留了 DISINFECT 和 DELETE 選項，以確保與以前版本的相容性。可以使用這些選項代替 /AI 和 /AS 選項。這種情況下，Kaspersky Embedded Systems Security 不會處理可疑物件。
REPORT	傳送報告（預設）
AUTO	執行建議的操作
/AS：**對可疑物件執行的操作**。如果不指定此選項，Kaspersky Embedded Systems Security 將執行"**略過**"操作。	
QUARANTINE	隔離
DELETE	刪除
REPORT	傳送報告（預設）
AUTO	執行建議的操作
排除	
/E:ABMSPO	排除以下複合檔案類型的指令參數： A – 壓縮檔案（僅掃描 SFX 壓縮檔案） B – 電子郵件資料庫 M – 一般郵件 S – 壓縮檔案和 SFX 壓縮檔案 P – 封裝的物件 O – 內嵌 OLE 物件
/EM:<"遮罩">	透過遮罩排除檔案 您可以指定數個遮罩，例如：`EM:"*.txt; *.png; C\Videos\*.avi"`。
/ET:<秒數>	如果花費時間超過 <秒數> 所指定的秒數，則停止處理物件。 預設情況下，沒有時間限制。
/ES:<大小>	不要掃描比 <大小> 值中所指定之大小 (MB) 還要大的複合物件。 預設情況下，Kaspersky Embedded Systems Security 掃描所有大小的物件。
/TZOFF	停用"信任區域"排除
進階設定（選項）	
/NOICHECKER	停用 iChecker（預設為啟用狀態）
/NOISWIFT	停用 iSwift（預設為啟用狀態）
/ANALYZERLEVEL:<啟發式分析等級>	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 如果刪除此選項，Kaspersky Embedded Systems Security 將不會使用啟發式分析。
/ALIAS:<工作別名>	為自訂掃描工作分配一個暫時名稱，允許您在其執行時對其進行引用，例如，使用 TASK 指令檢視其統計資訊。在 Kaspersky Embedded Systems Security 的所有元件的工作別名中，每一個工作別名都必須是唯一的。

	如果不指定此選項，則分配 scan_<kavshell_pid> 格式的暫時名稱，例如 scan_1234。在應用程式主控台中，工作被分配名稱“掃描物件 <日期和時間>”，例如，掃描物件 8/16/2007 5:13:14 PM。
工作記錄設定（報告設定）	
/W:<工作記錄檔案的路徑>	如果指定了此參數，Kaspersky Embedded Systems Security 將用該參數值指定的名稱儲存工作記錄檔案。 該記錄檔包含工作執行統計、工作開啟及結束（停止）的時間，以及有關該工作期間發生的事件資訊。 該記錄用於在事件檢視器中註冊由工作記錄設定和 Kaspersky Embedded Systems Security 事件記錄設定所定義的事件。 您可以指定記錄檔案的絕對路徑或相對路徑。如果僅指定檔案名稱但未指定路徑，則記錄檔將於目前所在的資料夾中建立。 以相同的記錄設定重新執行此指令將覆寫現有的記錄檔。 執行工作時，可檢視此記錄檔案。 此記錄會出現在應用程式主控台的“工作記錄”節點中。 如果 Kaspersky Embedded Systems Security 無法建立記錄檔案，它將顯示一條錯誤訊息，但仍將執行指令。
/ANSI	此選項使用 ANSI 編碼將事件記錄到工作記錄中。 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。

啟動“關鍵區域掃描”工作：KAVSHELL SCANCRITICAL

使用 `KAVSHELL SCANCRITICAL` 指令可使用在應用程式主控台中定義的設定啟動“關鍵區域掃描”工作。

KAVSHELL SCANCRITICAL 指令語法

```
KAVSHELL SCANCRITICAL [/W:<工作記錄檔案的路徑>]
```

KAVSHELL SCANCRITICAL 指令範例

要執行“關鍵區域掃描”工作並將名為 scancritical.log 的工作記錄儲存到當前資料夾中，請執行以下指令：

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

您可以使用 /W 參數配置工作記錄的位置（請參見下表）。

KAVSHELL SCANCRITICAL 指令的 /W 參數的語法

參數/選項	敘述
/W:<工作記錄檔案的路徑>	如果指定了此參數，Kaspersky Embedded Systems Security 將用該參數值指定的名稱儲存工作記錄檔案。 該記錄檔包含工作執行統計、工作開啟及結束（停止）的時間，以及有關該工作期間發生的事件資訊。 該記錄用於在事件檢視器中註冊由工作記錄設定和 Kaspersky Embedded Systems Security 事件記錄設定所定義的事件。

	您可以指定記錄檔案的絕對路徑或相對路徑。如果僅指定檔案名稱但未指定路徑，則記錄檔將於目前所在的資料夾中建立。 以相同的記錄設定重新執行此指令將覆寫現有的記錄檔。 執行工作時，可檢視此記錄檔案。 此記錄會出現在應用程式主控台的"**工作記錄**"節點中。 如果 Kaspersky Embedded Systems Security 無法建立記錄檔案，它將顯示一條錯誤訊息，但仍將執行指令。

非同步管理工作：KAVSHELL TASK

`KAVSHELL TASK` 指令可用來管理指定的工作，如執行、暫停、繼續和停止工作與檢視目前的工作狀態和統計。此指令應在非同步模式下執行。

執行此指令可能需要密碼。要輸入目前密碼，請使用 `[/pwd:<密碼>]`。

KAVSHELL TASK 指令語法

```
KAVSHELL TASK [<工作名稱別名> </START | /STOP | /PAUSE | /RESUME | /STATE | /STATISTICS >]
```

KAVSHELL TASK 指令範例

```
KAVSHELL TASK
```

```
KAVSHELL TASK on- access /START
```

```
KAVSHELL TASK user-task_1 /STOP
```

```
KAVSHELL TASK scan- computer /STATE
```

```
KAVSHELL TASK network-attack-blocker /START
```

`KAVSHELL TASK` 指令可以不帶參數/選項執行，或帶一個或多個參數/選項執行（請參見下表）。

KAVSHELL UPDATE 命令列參數/選項

參數/選項	敘述
無參數	回傳所有現有 Kaspersky Embedded Systems Security 工作的清單。該清單包括以下列：工作別名、工作類別（系統或自訂）和目前工作狀態。
<工作別名>	除工作名稱外，SCAN TASK 指令中可另外使用 Kaspersky Embedded Systems Security 指定給工作的附加縮寫名稱。要檢視 Kaspersky Embedded Systems Security 工作別名，請輸入不帶任何參數的指令 KAVSHELL TASK。
/START	在非同步模式下啟動指定工作。
/STOP	停止指定工作。
/PAUSE	暫停指定工作。
/RESUME	在非同步模式下還原指定工作。

/STATE	回傳目前的工作狀態（例如，*正在執行*、*已完成*、*已暫停*、*已停止*、*已失敗*、*正在啟動*、*還原中*）。
/STATISTICS	檢索工作統計 - 有關從工作啟動開始所處理的物件數量的資訊

請注意，並非所有 Kaspersky Embedded Systems Security 工作都完全支援 /PAUSE、/RESUME 和 /STATE 鍵。

KAVSHELL TASK 指令的回傳代碼。

刪除 PPL 內容：KAVSHELL CONFIG

`KAVSHELL CONFIG` 指令允許您使用在應用程式安裝期間安裝的 ELAM 驅動程式刪除 Kaspersky Security 服務的 PPL（輕度受防護處理程序）內容。

KAVSHELL CONFIG 指令語法

```
KAVSHELL CONFIG /PPL:<OFF>
```

KAVSHELL APPCONTROL /CONFIG 命令列參數/選項

參數/選項	敘述
/PPL:OFF	刪除 Kaspersky Security 服務的 PPL 內容。

啟動和停止即時電腦防護工作：KAVSHELL RTP

`KAVSHELL RTP` 指令可用來啟動或停止所有的即時電腦防護工作。

執行此指令可能需要密碼。要輸入目前密碼，請使用 `[/pwd:<密碼>]`。

KAVSHELL RTP 指令語法

```
KAVSHELL RTP {/START | /STOP}
```

KAVSHELL RTP 指令範例

若要啟動所有即時電腦防護工作，請執行以下指令：

```
KAVSHELL RTP /START
```

`KAVSHELL RTP` 指令必須包括兩個選項中的一個（請參見下表）。

KAVSHELL RTP 命令列選項

參數/選項	敘述
/START	啟動所有即時電腦防護工作：“即時檔案防護”和“KSN 使用”。

/STOP	停止所有即時電腦防護工作。

管理應用程式啟動控制工作：KAVSHELL APPCONTROL /CONFIG

可以使用 KAVSHELL APPCONTROL /CONFIG 指令來配置模式，在該模式中"應用程式啟動控制"工作將執行和監控 DLL 模組的載入。

KAVSHELL APPCONTROL /CONFIG 指令語法

```
/config /mode:<applyrules|statistics> [/dll:<no|yes>] | /config /savetofile:<XML 檔案路徑>
```

KAVSHELL APPCONTROL /CONFIG 指令示例

*要在"**活動**"模式中執行"應用程式啟動控制"工作而不監控 DLL 載入並在完成時儲存工作設定，請執行以下指令：*

```
KAVSHELL APPCONTROL /CONFIG /mode:applyrules /dll:<no>
/savetofile:c:\appcontrol\config.xml
```

可以使用命令列參數來配置"應用程式啟動控制"工作設定（請參閱以下表格）。

KAVSHELL APPCONTROL /CONFIG 命令列參數/選項

參數/選項	敘述
/mode:<applyrules|statistics>	"應用程式啟動控制"工作的執行模式。 您可以選擇以下模式之一： • 啟動 – 套用"應用程式啟動控制規則"； • 統計 – 僅建立統計。
/dll:<no|yes>	啟用或停用 DLL 載入監控。
/savetofile: <XML 文件路徑>	將指定規則匯出到指示的 XML 格式的檔案。
/savetofile: <XML 文件全名>	將規則清單儲存到檔案。
/savetofile: <XML 文件全名> /sdc	將軟體分發控制規則清單儲存到檔案。
/clearsdc	從清單中移除軟體分發控制規則。

應用程式啟動控制規則產生器：KAVSHELL APPCONTROL /GENERATE

可以使用 KAVSHELL APPCONTROL /GENERATE 指令建立應用程式啟動控制規則清單。

執行此指令可能需要密碼。要輸入目前密碼，請使用 [/pwd:<密碼>]。

KAVSHELL APPCONTROL /GENERATE 指令語法

```
KAVSHELL APPCONTROL /GENERATE <資料夾路徑> | /source:<包含資料夾清單的檔案路徑> [/masks:<edms>] [/runapp] [/rules:<ch|cp|h>] [/strong] [/user:<使用者或使用者組>] [/export:<XML 檔案路徑>] [/import:<a|r|m>] [/ prefix:<規則名稱首碼>] [/unique]
```

KAVSHELL APPCONTROL /GENERATE 指令示例

若要為指定資料夾中的檔產生規則，請執行以指令：

```
KAVSHELL APPCONTROL /GENERATE /source:c\folderslist.txt
/export:c:\rules\appctrlrules.xml
```

要為指定資料夾中所有副檔名的可執行檔產生規則，並在工作完成時將建立的規則儲存在指定的 XML 檔案中，請執行以下指令：

```
KAVSHELL APPCONTROL /GENERATE c:\folder /masks:edms /export:c\rules\appctrlrules.xml
```

您可以使用命令列參數/選項配置"應用程式啟動控制"工作的自動規則建立設定（請參見下表）。

KAVSHELL APPCONTROL /GENERATE 命令列參數/選項

參數/選項	敘述
允許規則範圍	
<資料夾路徑>	指定將為其自動建立允許規則的可執行檔所在資料夾的路徑。
/source: <包含文件夹列表的文件路径>	指定含有資料夾清單的 TXT 檔案的路徑，這些資料夾包含將為其自動建立允許規則的可執行檔。
/masks: <edms>	指定將為其自動建立允許規則的可執行檔的副檔名。 可以將具有以下副檔名的檔案包括在規則範圍中： • e – EXE 檔案 • d – DLL 檔案 • m – MSI 檔案 • s – 指令碼
/runapp	建立允許規則時，考慮目前在受防護裝置上執行的應用程式。
自動建立允許規則時的操作	
/rules: <ch|cp|h>	指定當建立"應用程式啟動控制"工作的允許規則時執行的操作： • 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	在自動建立"應用程式啟動控制"工作的允許規則時使用數位憑證的主旨和指紋。如果指定 /rules: <ch|cp> 參數，則將执行该命令。

/user: <用户或用户组>	指定將套用規則的使用者或使用者群組。應用程式將監控透過指定的使用者和/或使用者群組執行的任何應用程式。
“應用程式啟動控制規則產生器”工作完成後的操作	
/export <XML 檔案路徑>	將建立的規則儲存到 XML 檔案。
/unique	新增有關安裝了特定應用程式的受防護裝置的資訊，這些應用程式是建立應用程式啟動控制允許規則的基礎。
/prefix：<規則名稱前置詞>	為“應用程式啟動控制”允許規則的名稱指定首碼。
/import: <a|r|m>	根據選定匯入規則將建立的規則匯入到指定的應用程式啟動控制規則清單中： • a - **新增到現有規則**（將複製具有相同設定的規則） • r - **取代現有規則**（不新增具有相同設定的規則；如果至少一個規則設定是唯一的，則會新增規則） • m - **與現有規則合併**（不新增具有相同設定的規則；如果至少一個規則設定是唯一的，則會新增規則）

填寫應用程式啟動控制規則清單：KAVSHELL APPCONTROL

可以使用 KAVSHELL APPCONTROL 指令根據所選匯入規則將規則從 XML 檔案新增到應用程式啟動控制工作規則清單，以及從清單中刪除所有現有規則。

執行此指令可能需要密碼。要輸入目前密碼，請使用 [/pwd:<密碼>]。

KAVSHELL APPCONTROL 指令語法

```
KAVSHELL APPCONTROL /append <XML 檔案路徑> | /replace <XML 檔案路徑> | /merge <XML 檔案路徑> | /clear
```

KAVSHELL APPCONTROL 指令示例

要根據“新增到現有規則”匯入規則從 XML 檔案向現有應用程式啟動控制規則新增規則，請執行以下指令：

```
KAVSHELL APPCONTROL /append c:\rules\appctrlrules.xml
```

您可以使用命令列參數選擇原則來將新規則從指定 XML 檔案新增到定義的應用程式啟動控制規則清單（請參見下表）。

KAVSHELL APPCONTROL 命令列參數/選項

參數/選項	敘述
/append <XML 檔案路徑>	基於指定的 XML 檔案更新應用程式啟動控制規則清單。匯入規則 - **新增到現有規則**（將複製具有相同設定的規則）。

/replace <XML 檔案路徑>	基於指定的 XML 檔案更新應用程式啟動控制規則清單。匯入規則 - **取代現有規則**（不新增具有相同設定的規則；如果至少一個規則設定是唯一的，則會新增規則）。
/merge <XML 檔案路徑>	基於指定的 XML 檔案更新應用程式啟動控制規則清單。匯入規則 - **與現有規則合併**（新規則不會複製現有規則）。
/clear	填寫應用程式啟動控制規則清單。

填寫裝置控制規則清單：KAVSHELL DEVCONTROL

可以使用 KAVSHELL DEVCONTROL 指令根據所選匯入規則將規則從 XML 檔案新增到裝置控制工作規則清單，以及從清單中刪除所有現有規則。

執行此指令可能需要密碼。要輸入目前密碼，請使用 [/pwd:<密碼>]。

KAVSHELL DEVCONTROL 指令語法

```
KAVSHELL DEVCONTROL /append <XML 檔案路徑> | /replace <XML 檔案路徑> | /merge <XML 檔案路徑> | /clear
```

KAVSHELL DEVCONTROL 指令示例

要根據"新增到現有規則"匯入規則從 XML 檔案向裝置控制工作的現有規則新增規則，請執行以下指令：

```
KAVSHELL DEVCONTROL /append c:\rules\devctrlrules.xml
```

您可以使用命令列參數選擇用於將新規則從指定 XML 檔案新增到定義的裝置控制規則清單的匯入規則（請參見下表）。

KAVSHELL DEVCONTROLL 命令列參數/選項

鍵	敘述
/append <XML 檔案路徑>	基於指定的 XML 檔更新裝置控制規則清單。匯入規則 - **新增到現有規則**（將複製具有相同設定的規則）。
/replace <XML 檔案路徑>	基於指定的 XML 檔更新裝置控制規則清單。新增原則 - **取代現有規則**（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）。
/merge <XML 檔案路徑>	基於指定的 XML 檔更新裝置控制規則清單。匯入規則 - **與現有規則合併**（新規則不會複製現有規則）。
/clear	清除裝置控制規則清單。

啟動資料庫更新工作：KAVSHELL UPDATE

KAVSHELL UPDATE 指令可以用於按同步模式啟動 Kaspersky Embedded Systems Security 資料庫更新工作。

使用 KAVSHELL UPDATE 指令啟動的資料庫更新工作是暫時工作。它僅在執行時顯示在應用程式主控台中。但是，將建立工作記錄，並顯示在應用程式主控台的"**工作記錄**"中。卡巴斯基安全管理中心政策可套用到使用 KAVSHELL UPDATE 指令所建立與啟動的更新工作，以及病毒防護應用程式主控台中所建立的更新工作。有關使用卡巴斯基安全管理中心管理受防護裝置腦上的 Kaspersky Embedded Systems Security 的資訊，請參見"使用卡巴斯基安全管理中心管理 Kaspersky Embedded Systems Security"部分。

在此工作中指定更新來源路徑時，可設定環境變數。如果使用使用者環境變數，請以相應使用者身分執行 KAVSHELL UPDATE 指令。

KAVSHELL UPDATE 指令語法

KAVSHELL UPDATE <更新來源路徑 | /AK | /KL> [/NOUSEKL] [/PROXY:<位址>:<連接埠>] [/AUTHTYPE:<0-2>] [/PROXYUSER:<使用者名稱>] [/PROXYPWD:<密碼>] [/NOPROXYFORKL] [/USEPROXYFORCUSTOM] [/NOFTPPASSIVE] [/TIMEOUT:<秒>] [/REG:<iso3166 程式碼>] [/W:<工作記錄檔案路徑>] [/ALIAS:<工作別名>]

KAVSHELL UPDATE 指令有必需和可選參數/選項（請參閱下表）。

KAVSHELL UPDATE 指令範例

要啟動自訂的資料庫更新工作，請執行以下指令：

```
KAVSHELL UPDATE
```

要使用 \\server\databases 網路資料夾中的更新檔案啟動資料庫更新工作，請執行以下指令：

```
KAVSHELL UPDATE \\server\databases
```

要從 FTP 伺服器 ftp://dnl-ru1.kaspersky-labs.com/ 啟動資料庫更新並將所有工作事件寫入到名為 c:\update_report.log 的檔案中，請執行以下指令：

```
KAVSHELL UPDATE ftp://dnl-ru1.kaspersky-labs.com /W:c:\update_report.log
```

要從 Kaspersky 的更新伺服器下載 Kaspersky Embedded Systems Security 資料庫更新檔案，請透過代理伺服器（代理伺服器位址：proxy.company.com，連接埠 8080）連線更新來源。要使用內建的 Microsoft Windows NTLM 身分驗證及使用者名稱"inetuser"和密碼"123456"存取受防護裝置，請執行以下指令：

```
KAVSHELL UPDATE /KL /PROXY:proxy.company.com:8080 /AUTHTYPE:1 /PROXYUSER:inetuser /PROXYPWD:123456
```

KAVSHELL UPDATE 命令列參數/選項

參數/選項	敘述
更新來源（必需參數）。指定一或多個來源。Kaspersky Embedded Systems Security 將按照更新來源的清單順序存取更新來源。使用空白分隔源。	
<UNC 格式中的路徑>	使用者定義的更新來源。UNC 格式中的網路更新資料夾路徑。
<URL>	使用者定義的更新來源。更新資料夾所在的 HTTP 或 FTP 伺服器位址。
<本機資料夾>	使用者定義的更新來源。受防護裝置上的資料夾。
/AK	將卡巴斯基安全管理中心管理伺服器用作更新來源。

/KL	將 Kaspersky 的更新伺服器用作更新來源。
/NOUSEKL	如果其他更新來源無法使用，則不使用 Kaspersky 的更新伺服器（預設情況下使用）。
代理伺服器設定	
/PROXY:<位址>:<連接埠>	代理伺服器的網路名稱或 IP 位址及埠號。如果未指定此參數，Kaspersky Embedded Systems Security 將自動偵測區域網路中使用的代理伺服器設定。
/AUTHTYPE:<0-2>	該參數指定存取代理伺服器的身分驗證方法。它可能呈現是以下設定值： **0** - Microsoft Windows NTLM 身分驗證；Kaspersky Embedded Systems Security 將使用**本機系統 (SYSTEM)** 帳戶連線代理伺服器 **1** - Microsoft Windows NTLM 身分驗證；Kaspersky Embedded Systems Security 將使用 /PROXYUSER 和 /PROXYPWD 參數指定的使用者名稱和密碼連線代理伺服器 **2** - 使用 /PROXYUSER 和 /PROXYPWD 參數指定的使用者名稱和密碼進行身分驗證（基本身分驗證） 如果代理伺服器不需要身分驗證，則無需指定此參數。
/PROXYUSER:<使用者名稱>	存取代理伺服器所需的使用者名稱。如果指定了 /AUTHTYPE:0，則將略過 /PROXYUSER:<使用者名稱> 和 /PROXYPWD:<密碼> 參數。
/PROXYPWD:<密碼>	存取代理伺服器所需的使用者密碼。如果指定了 /AUTHTYPE:0，則將略過 /PROXYUSER:<使用者名稱> 和 /PROXYPWD:<密碼> 參數。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	不使用代理伺服器設定連線到 Kaspersky 的更新伺服器（預設情況下使用）。
/USEPROXYFORCUSTOM	使用代理伺服器設定連線使用者定義的更新來源（預設為不使用）。
/USEPROXYFORLOCAL	使用代理伺服器連線本機更新來源。如果不指定，將套用"**對於本機位址不使用代理伺服器**"設定。
FTP 和 HTTP 伺服器一般設定	
/NOFTPPASSIVE	如果指定了指令參數，Kaspersky Embedded Systems Security 將使用主動 FTP 伺服器模式連線至受防護裝置。如果未指定指令參數，Kaspersky Embedded Systems Security 將使用被動 FTP 伺服器模式（如果可能的話）。
/TIMEOUT:<秒數>	FTP 或 HTTP 伺服器連線逾時。如果不指定此參數，Kaspersky Embedded Systems Security 將使用預設值 - 10 秒。該值必須是一個整數。
/REG:<iso3166 代碼>	區域設定。從 Kaspersky 的更新伺服器接收更新時需使用此參數。Kaspersky Embedded Systems Security 會選擇最近的更新伺服器以最大程度地降低受防護裝置的負荷。 此參數的值應該是受防護裝置所在國家/地區的 ISO 3166-1 alpha-2 代碼，例如 /REG: gr 或 /REG:US。如果省略該鍵或指定無效的國家/地區代碼，Kaspersky Embedded Systems Security 將會基於安裝應用程式主控台的受防護裝置上的地區設定偵測受防護裝置的位置。
/ALIAS:<工作別名>	透過此參數可以為工作分配暫時名稱，允許您在工作執行時對其進行引用。例如，您可使用 TASK 指令檢視工作統計。在 Kaspersky Embedded Systems Security 的所有元件的工作別名中，每一個工作別名都必須是唯一的。 如果不指定該鍵，則會使用 update_<kavshell_pid> 格式的暫時名稱，例如 update_1234。在應用程式主控台中，工作被分配名稱"Update-databases <日期時間>"；例如，Update-databases 8/16/2007 5:41:02 PM。
/W:<工作記錄檔案的路徑>	如果指定了此參數，Kaspersky Embedded Systems Security 將用該參數值指定的名稱儲存工作記錄檔案。 該記錄檔包含工作執行統計、工作開啟及結束（停止）的時間，以及有關該工作期間發生的事件資訊。

	該記錄用於在事件檢視器中註冊由工作記錄設定和 Kaspersky Embedded Systems Security 事件記錄設定所定義的事件。 您可以指定記錄檔案的絕對路徑或相對路徑。如果僅指定檔案名稱但未指定路徑，則記錄檔將於目前所在的資料夾中建立。 以相同的記錄設定重新執行此指令將覆寫現有的記錄檔。 執行工作時，可檢視此記錄檔案。 此記錄會出現在應用程式主控台的"**工作記錄**"節點中。 如果 Kaspersky Embedded Systems Security 無法建立記錄檔案，它將顯示一條錯誤訊息，但仍將執行指令。

KAVSHELL UPDATE 命令的傳回代碼。

回溯 Kaspersky Embedded Systems Security 資料庫更新：KAVSHELL ROLLBACK

KAVSHELL ROLLBACK 指令可用來執行資料庫更新回溯本機系統工作（將 Kaspersky Embedded Systems Security 資料庫回溯至上一個安裝版）。此指令會同步執行。

指令語法：

```
KAVSHELL ROLLBACK
```

KAVSHELL ROLLBACK 指令的回傳代碼。

管理記錄審查：KAVSHELL TASK LOG-INSPECTOR

KAVSHELL TASK LOG-INSPECTOR 指令可用於根據 Windows 事件記錄的分析來監控環境完整性。

指令語法

```
KAVSHELL TASK LOG-INSPECTOR
```

指令範例

```
KAVSHELL TASK LOG-INSPECTOR /stop
```

KAVSHELL TASK LOG-INSPECTOR 命令列選項

選項	敘述
/START	在非同步模式下啟動指定工作。
/STOP	停止指定工作。
/STATE	回傳目前的工作狀態（例如，*正在執行*、*已完成*、*已暫停*、*已停止*、*已失敗*、*正在啟動*、*還原中*）
/STATISTICS	檢索工作統計 - 有關從工作啟動開始所處理的物件數量的資訊。

KAVSHELL TASK LOG-INSPECTOR 指令的回傳代碼。

啟動應用程式：KAVSHELL LICENSE

可使用 KAVSHELL LICENSE 指令管理 Kaspersky Embedded Systems Security 金鑰和啟動碼。

執行此指令可能需要密碼。要輸入目前密碼，請使用 [/pwd:<密碼>]。

KAVSHELL LICENSE 指令語法

KAVSHELL LICENSE [/ADD:<金鑰檔案 | 啟動碼>[/R]| /DEL:<金鑰 | 啟動碼編號>]

KAVSHELL LICENSE 指令範例

要啟動應用程式，請執行以下指令：

KAVSHELL.EXE LICENSE / ADD: <激活码或密钥>

若要檢視有關新增金鑰檔案的資訊，請執行以下指令：

KAVSHELL LICENSE

要移除安裝序號 0000-000000-00000001 的產品授權檔案，請執行以下指令：

KAVSHELL LICENSE /DEL:0000-000000-00000001

KAVSHELL LICENSE 指令可搭配指令參數或不搭配指令參數執行（請參閱下表）。

KAVSHELL LICENSE 命令列參數/選項

參數	敘述
不搭配指令參數	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:<金鑰檔案名稱或啟動碼>	透過指定的檔案或啟動碼新增金鑰。 指定金鑰路徑時可以使用系統環境變數；不允許使用者環境變數。
/R	/R 啟動碼或金鑰是 /ADD 啟動碼或金鑰的附加項，表示所新增的啟動碼或金鑰是備用啟動碼或金鑰檔案。
/DEL:<金鑰或啟動碼>	刪除具有指定編號或啟動碼的金鑰。

KAVSHELL LICENSE 指令的回傳代碼。

啟用、設定和停用偵錯記錄：KAVSHELL TRACE

KAVSHELL TRACE 指令可用來啟用或停用 Kaspersky Embedded Systems Security 所有子系統的即時偵錯記錄，以及設定記錄詳細等級。

Kaspersky Embedded Systems Security 會以未加密的形式將資訊寫入到偵錯檔案和 Dump 檔案。

KAVSHELL TRACE 指令語法

```
KAVSHELL TRACE </ON /F:<偵錯記錄檔資料夾路徑> [/S:<記錄大小上限 (MB)>]
[/LVL:debug|info|warning|error|critical] | /OFF>
```

如果啟用了偵錯記錄並且您希望變更其設定，請輸入 KAVSHELL TRACE 指令並帶 /ON 選項，同時使用 /S 和 /LVL 參數指定偵錯記錄設定（請參閱下表）。

KAVSHELL TRACE 指令參數

鍵	敘述
/ON	啟用偵錯記錄。
/F:<偵錯記錄的檔案資料夾>	該參數指定將儲存跟蹤記錄檔案的資料夾的完整路徑（必需）。 如果指定的資料夾路徑不存在，將不會建立偵錯記錄。不能指定其他受防護裝置的網路磁碟機上的資料夾位置。 如果該參數指定的路徑包含空白，則需要用引號將路徑括起來，例如 /F:"C:\Trace Folder"。 指定偵錯檔案路徑時可以使用系統環境變數；不允許使用者環境變數。
/S: <最大日志文件大小（单位为 MB）>	此指令可設定一個偵錯記錄檔的大小上限。一旦記錄檔案大小達到上限時，Kaspersky Embedded Systems Security 會將資訊記錄到新檔案中；之前的記錄檔案會被儲存。 如果未指定此指令參數的值，一個記錄檔的大小上限為 50 MB。
/LVL:debug|info|warning|error|critical	該參數設定記錄詳細級別，從所有事件都記錄到記錄中的最大級別（“**所有診斷資訊**”）到僅記錄嚴重事件的最小級別（“**緊急事件**”）。 如果未指定該參數，“**所有診斷資訊**”詳細級別中包括的所有事件都會記錄到偵錯記錄中。
/OFF	此選項停用偵錯記錄。

KAVSHELL TRACE 指令範例

*要啟用使用“**所有診斷資訊**”詳細級別和最大記錄大小 200MB 的偵錯記錄，並且將記錄檔案儲存到資料夾“C:\Trace Folder”，請執行以下指令：*

```
KAVSHELL TRACE /ON /F:"C:\Trace Folder" /S:200
```

*要啟用使用“**重要事件**”詳細級別的偵錯記錄，並且將記錄檔案儲存到資料夾“C:\Trace Folder”，請執行以下指令：*

```
KAVSHELL TRACE /ON /F:"C:\Trace Folder" /LVL:warning
```

要停用偵錯記錄，請執行以下指令：

```
KAVSHELL TRACE /OFF
```

KAVSHELL TRACE 命令的傳回代碼。

對 Kaspersky Embedded Systems Security 記錄檔案進行磁碟整理：KAVSHELL VACUUM

使用 KAVSHELL VACUUM 指令對應用程式記錄檔案進行磁碟整理。這有助於避免由於儲存大量包含應用程式事件的記錄檔案而出現系統和應用程式錯誤。

執行此指令可能需要密碼。要輸入目前密碼，請使用 [/pwd:<密碼>]。

如果自訂掃描和更新工作頻繁執行，建議套用 KAVSHELL VACUUM 指令最佳化記錄檔案儲存。此指令使 Kaspersky Embedded Systems Security 更新儲存在受防護裝置上指定路徑的應用程式記錄檔案的邏輯結構。

預設情況下，應用程式記錄檔案儲存在"C:\ProgramData\Kaspersky Lab\Kaspersky Embedded Systems Security\3.1\Reports"。如果您手動為記錄儲存指定了另一個路徑，KAVSHELL VACUUM 指令將對 Kaspersky Embedded Systems Security 記錄設定中指定的資料夾中的檔案執行磁碟整理。

較大的檔案大小會增加 KAVSHELL VACUUM 指令完成碎片整理操作所需的時間。

執行 KAVSHELL VACUUM 指令時，"即時防護"和"電腦控制"工作不可用。磁碟整理過程會限制對 Kaspersky Embedded Systems Security 記錄的存取並封鎖事件記錄。為避免防護能力下降，建議計畫何時執行 KAVSHELL VACUUM 指令。

若要對 Kaspersky Embedded Systems Security 記錄檔案進行磁碟整理，請執行以下指令：

```
KAVSHELL VACUUM
```

此指令需要本機系統帳戶權限。

清理 iSwift 基礎：KAVSHELL FBRESET

Kaspersky Embedded Systems Security 使用的 iSwift 技術可避免應用程式重新掃描上次掃描後未修改的檔案（**使用 iSwift 技術**）。

Kaspersky Embedded Systems Security 會在 %SYSTEMDRIVE%\System Volume Information 資料夾建立 klamfb.dat 和 klamfb2.dat 檔案。這兩個檔案包含有關已掃描的乾淨物件的資訊。檔案 klamfb.dat (klamfb2.dat) 隨著 Kaspersky Embedded Systems Security 掃描的檔案數目的增加而增大。它僅包含有關系統中的檔案的目前資訊：如果刪除一個檔案，Kaspersky Embedded Systems Security 將從 klamfb.dat 清除相應資訊。

要清除某個檔案，請使用 KAVSHELL FBRESET指令。

使用 KAVSHELL FBRESET 指令時，請注意以下說明：

- 使用 KAVSHELL FBRESET 指令清除 klamfb.dat 檔案時，Kaspersky Embedded Systems Security 不會暫停防護（與手動刪除 klamfb.dat 的情況不同）。
- 清除 klamfb.dat 中的資料後，Kaspersky Embedded Systems Security 可能會增加受防護裝置工作負載。在這種情況下，Kaspersky Embedded Systems Security 將掃描在清除 klamfb.dat 後第一次存取的所有檔案。掃描後，Kaspersky Embedded Systems Security 將有關每個掃描物件的資訊放回 klamfb.dat。如果有新的存取物件的嘗試，iSwift 技術會封鎖重新掃描未變更的檔案。

只有在 SYSTEM 帳戶下啟動命令列編譯器時，才能使用 KAVSHELL FBRESET 指令。

啟用和停用建立傾印檔案：KAVSHELL DUMP

可以使用 KAVSHELL DUMP 指令啟用或停用在 Kaspersky Embedded Systems Security 處理程序異常終止時建立處理程序快照（Dump 檔案）（請參閱下表）。此外，還可以隨時建立正在執行的 Kaspersky Embedded Systems Security 處理程序的 Dump 檔案。

為了成功建立 Dump 檔案，必須在本機系統帳戶 (SYSTEM) 下執行 KAVSHELL DUMP 指令。

Kaspersky Embedded Systems Security 會以未加密的形式將資訊寫入到偵錯檔案和 Dump 檔案。

KAVSHELL DUMP 指令不能用於 x64 處理程序。

KAVSHELL DUMP 指令語法

```
KAVSHELL DUMP </ON /F:<傾印檔案的資料夾>|/SNAPSHOT /F:< 傾印檔案的資料夾> / P:<pid> | /OFF>
```

KAVSHELL UPDATE 命令列參數/選項

鍵	敘述
/ON	啟用當處理程序異常終止時建立 Dump 檔案。
/F:< Dump 檔案的資料夾路徑 >	這是必需參數。它可指定要儲存 Dump 檔案的資料夾路徑。不允許指定其他不受防護裝置的網路磁碟機上的資料夾位置。 在指定 Dump 檔案的資料夾的路徑時，可以使用系統環境變數；不允許使用使用者環境變數。
/SNAPSHOT	獲取正在執行的具有指定 PID 的處理程序的記憶體快照，並將 Dump 檔案儲存在 /F 參數指定的資料夾中。
/P	處理程序識別碼 (PID) 顯示在 Microsoft Windows 工作管理員中。
/OFF	停用當處理程序異常終止時建立 Dump 檔案。

KAVSHELL DUMP 命令的傳回代碼。

KAVSHELL DUMP 指令範例

要啟用建立 Dump 檔案的功能，並將 Dump 檔案儲存到"C:\Dump Folder"資料夾，請執行以下指令：

```
KAVSHELL DUMP /ON /F:"C:\Dump Folder"
```

要使用 ID 1234 將處理程序的 Dump 檔案儲存到 "C:/Dumps" 資料夾，請執行以下指令：

```
KAVSHELL DUMP /SNAPSHOT /F:C:\dumps /P:1234
```

要停用產生 Dump 檔案的功能，請執行以下指令：

```
KAVSHELL DUMP /OFF
```

匯入設定：KAVSHELL IMPORT

您可以使用 `KAVSHELL IMPORT` 指令將 Kaspersky Embedded Systems Security 的設定和目前工作從設定檔匯入到受防護裝置上的 Kaspersky Embedded Systems Security 副本。您可使用 `KAVSHELL EXPORT` 指令建立設定檔。

執行此指令可能需要密碼。要輸入目前密碼，請使用 `[/pwd:<密碼>]`。

KAVSHELL IMPORT 指令語法

```
KAVSHELL IMPORT <設定檔名稱及檔案路徑>
```

KAVSHELL IMPORT 指令範例

```
KAVSHELL IMPORT Host1.xml
```

KAVSHELL IMPORT 命令列參數

參數	敘述
<設定檔名稱及檔案路徑>	設定檔名稱可當作匯入設定來源使用。 指定檔案路徑時可以使用系統環境變數；不允許使用者環境變數。

KAVSHELL IMPORT 命令的傳回代碼。

匯出設定：KAVSHELL EXPORT

`KAVSHELL EXPORT` 指令可用來匯出 Kaspersky Embedded Systems Security 及其現有工作所有的設定，以便之後將設定匯入其他受防護裝置所安裝的 Kaspersky Embedded Systems Security 副本。

KAVSHELL EXPORT 指令語法

```
KAVSHELL IMPORT <設定檔名稱及檔案路徑>
```

KAVSHELL EXPORT 指令範例

```
KAVSHELL EXPORT Host1.xml
```

KAVSHELL EXPORT 命令列參數

參數	敘述
<設定檔名稱及檔案路徑>	包含設定的設定檔名稱。 設定檔可指派任何檔案副檔名。 指定檔案路徑時可以使用系統環境變數；不允許使用者環境變數。

KAVSHELL LICENSE 指令的回傳代碼。

與 Microsoft Operations Management Suite 整合：KAVSHELL OMSINFO

使用 KAVSHELL OMSINFO 指令檢視應用程式的狀態以及反病毒資料庫和 KSN 服務偵測到的威脅的相關資訊。有關威脅的資訊取自可用的事件記錄。

KAVSHELL OMSINFO 指令語法

```
KAVSHELL OMSINFO <產生的檔案的完整路徑與檔名>
```

KAVSHELL OMSINFO 指令範例

```
KAVSHELL OMSINFO C:\Users\Admin\Desktop\omsinfo.json
```

KAVSHELL OMSINFO 命令列參數

參數	敘述
<產生的檔案的路徑與檔案名稱>	產生的檔案的名稱，該檔案將包含應用程式狀態和任何偵測到的威脅的相關資訊。

管理“基線檔案完整性監控”工作：KAVSHELL FIM /BASELINE

可以使用 KAVSHELL FIM /BASELINE 指令來配置“基線檔案完整性監控”工作執行和監控 DLL 模組的載入模式。

執行此指令可能需要密碼。要輸入目前密碼，請使用 [/pwd:<密碼>]。

KAVSHELL FIM /BASELINE 指令語法

```
KAVSHELL FIM /BASELINE [/CREATE: [<监控范围> | /L:<包含监控区域列表的 TXT 文件的路径>] [/MD5 | /SHA256] [/SF]] | [/CLEAR [/BL:<基线 id> | /ALIAS:<现有别名>]] | [/EXPORT:<TXT 文件的路径> [/BL:<基线 id> | /ALIAS:<现有别名>]] | [/SHOW [/BL:基线 id> | /ALIAS:<现有别名>]] | [/SCAN [/BL:<基线 id> | /ALIAS:<现有别名>]] | [/PWD:<密码>]
```

KAVSHELL FIM /BASELINE 指令示例

要刪除基線，請執行以下指令：

```
KAVSHELL FIM /BASELINE /CLEAR /BL:<基線 id>
```

可以使用命令列參數來配置“基線檔案完整性監控”工作設定（請參閱以下表格）。

KAVSHELL FIM/ BASELINE 命令列參數/選項

參數/選項	敘述
/CREATE	建立新的“基線檔案完整性監控”工作。 Kaspersky Embedded Systems Security 將啟動新的“基線檔案完整性監控”工作以建立基線。
/L	指定包含監控區域清單的 TXT 檔案的路徑。
/MD5	指定用於計算核對總和的 MD5 算法（可選參數）。 /MD5 參數不能與 /SHA256 一起使用。 預設情況下使用 MD5 算法。
/SHA256	指定用於計算核對總和的 MD5 算法（可選參數）。 /MD5 參數不能與 /SHA256 一起使用。 預設情況下使用 MD5 算法。
/SF	將所有子資料夾包括在“基線檔案完整性監控”工作範圍中（可選參數）。 預設情況下，所有子資料夾都從“基線檔案完整性監控”工作範圍中排除。
/CLEAR	刪除具有指定 <基線 id> 的基線或具有指定 <現有別名> 的工作的基線。 如果 <基線 id> 和 <現有別名> 均未指定，則刪除所有基線。 可選參數。
/BL	指定基線的唯一 ID（可選參數）。
/EXPORT	將所有基線的相關資料匯出到 TXT 檔案。
/SHOW	顯示所有基線的相關資料。
/SCAN	以指定的 <基線 id> 或指定的 <現有別名> 啟動新的“基線檔案完整性監控”工作。
/ALIAS	指定現有工作的名稱或新工作的名稱。
<監控範圍>	指定要包括在「基線檔案完整性監控」工作範圍中的檔案或資料夾。 此參數僅允許指定一個區域。
<包含監控區域清單的 TXT 檔案的路徑>	指定包含監控區域清單的 TXT 檔案的路徑。 該檔案必須為 UTF-8 編碼，並且每個監控區域路徑都必須在單獨的行中指定。
<TXT 檔案路徑>	指定要將所有基準的相關資料匯出到的檔案的路徑。
<基線 id>	指定基線的唯一 ID。 您可以使用 /SHOW 參數來學習基線的 ID。

<現有別名>	指定現有工作的名稱。
<新別名>	指定新工作的名稱。

指令回傳代碼

KAVSHELL START 和 KAVSHELL STOP 指令的回傳代碼

KAVSHELL START 和 KAVSHELL STOP 指令的回傳代碼

回傳代碼	敘述
0	操作順利完成
-3	權限錯誤
-5	指令語法無效
-6	操作無效（例如，Kaspersky Security 服務已經執行或已經停止）
-7	服務未註冊
-8	已停用自動服務啟動。
-9	使用其他使用者帳戶啟動受防護裝置的嘗試失敗（預設情況下，Kaspersky Security 服務在本機系統使用者帳戶下執行）
-99	未知錯誤

KAVSHELL SCAN 和 KAVSHELL SCANCRITICAL 指令的回傳代碼

KAVSHELL SCAN 和 KAVSHELL SCANCRITICAL 指令的回傳代碼

回傳代碼	敘述
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	權限錯誤
-4	找不到物件（找不到含有掃描區域清單的檔案）
-5	指令語法無效或未定義掃描區域
-80	偵測到受感染物件和其他物件
-81	偵測到可能受感染的物件
-82	偵測到處理程序錯誤
-83	發現未掃描的物件
-84	偵測到已損毀物件
-85	建立工作記錄失敗

-99	未知錯誤
-301	金鑰無效

KAVSHELL TASK LOG-INSPECTOR 指令的回傳代碼

KAVSHELL TASK LOG-INSPECTOR 指令的回傳代碼

回傳代碼	敘述
0	操作順利完成
-6	操作無效（例如，Kaspersky Security 服務已經執行或已經停止）
402	工作已經執行（針對 /STATE 選項）

KAVSHELL TASK 指令的回傳代碼

KAVSHELL TASK 指令的回傳代碼

回傳代碼	敘述
0	操作順利完成
-2	未執行服務
-3	權限錯誤
-4	找不到物件（找不到工作項目）
-5	指令語法無效
-6	操作無效（例如，工作未執行、工作執行中或無法暫停）
-99	未知錯誤
-301	金鑰無效
401	工作未執行（針對 /STATE 選項）
402	工作已經執行（針對 /STATE 選項）
403	工作已經暫停（針對 /STATE 選項）
-404	操作失敗（工作狀態變更導致崩潰）

KAVSHELL RTP 命令的傳回代碼。

KAVSHELL RTP 命令的傳回代碼。

回傳代碼	敘述
0	操作順利完成
-2	未執行服務
-3	權限錯誤
-4	找不到物件（找不到其中一個即時電腦防護工作或全部的即時防護工作）

-5	指令語法無效
-6	操作無效（例如，工作已執行中或已停止工作）
-99	未知錯誤
-301	金鑰無效

KAVSHELL UPDATE 命令的傳回代碼。

KAVSHELL UPDATE 命令的傳回代碼。

回傳代碼	敘述
0	操作順利完成
200	所有物件都是最新的（資料庫或程式元件為最新的）
-2	未執行服務
-3	權限錯誤
-5	指令語法無效
-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	連線安全管理中心時發生錯誤
-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壞
-301	金鑰無效

KAVSHELL ROLLBACK 指令的回傳代碼

KAVSHELL ROLLBACK 指令的回傳代碼

回傳代碼	敘述
0	操作順利完成
-2	未執行服務
-3	權限錯誤
-99	未知錯誤
-221	找不到資料庫備份副本或資料庫已損毀
-222	資料庫備份副本已損毀

KAVSHELL LICENSE 指令的回傳代碼

KAVSHELL LICENSE 指令的回傳代碼

回傳代碼	敘述
0	操作順利完成
-2	未執行服務
-3	權限不足無法管理金鑰
-4	找不到指定的金鑰序號
-5	指令語法無效
-6	操作無效（已安裝金鑰）
-99	未知錯誤
-301	金鑰無效
-303	產品授權適用於其他程式

KAVSHELL TRACE 命令的傳回代碼。

KAVSHELL TRACE 命令的傳回代碼。

回傳代碼	敘述
0	操作順利完成
-2	未執行服務
-3	權限錯誤
-4	找不到物件（找不到偵錯記錄資料夾的指定路徑）
-5	指令語法無效
-6	操作無效（偵錯記錄已被停用時試圖執行 KAVSHELL TRACE /OFF 指令）
-99	未知錯誤

KAVSHELL FBRESET 指令的回傳代碼

KAVSHELL FBRESET 指令的回傳代碼

回傳代碼	敘述
0	操作順利完成
-99	未知錯誤

KAVSHELL DUMP 命令的傳回代碼。

KAVSHELL DUMP 命令的傳回代碼。

回傳代碼	敘述
0	操作順利完成
-2	未執行服務

-3	權限錯誤
-4	找不到物件（找不到 Dump 檔案資料夾的指定路徑；找不到含有指定 PID 的處理程序）
-5	指令語法無效
-6	操作無效（如果已停用傾印檔案建立功能，試圖執行 KAVSHELL DUMP/OFF 指令）
-99	未知錯誤

KAVSHELL IMPORT 命令的傳回代碼。

KAVSHELL IMPORT 命令的傳回代碼。

回傳代碼	敘述
0	操作順利完成
-2	未執行服務
-3	權限錯誤
-4	找不到物件（無法找到可以匯入的設定檔）
-5	無效的語法
-99	未知錯誤
501	操作順利完成，但有一個錯誤 / 備註，例如 Kaspersky Embedded Systems Security 未匯入某些功能元件的設定
-502	匯入檔案缺失或其格式無法辨識
-503	不相容的設定（設定檔從不同的程式或新版或不相容的 Kaspersky Embedded Systems Security 匯出）

KAVSHELL EXPORT 命令的傳回代碼。

KAVSHELL EXPORT 命令的傳回代碼。

回傳代碼	敘述
0	操作順利完成
-2	未執行服務
-3	權限錯誤
-5	無效的語法
-10	無法建立設定檔（例如，無法存取檔案路徑中所指定的資料夾）
-99	未知錯誤
501	操作順利完成，但有一個錯誤 / 備註，例如 Kaspersky Embedded Systems Security 未匯出某些功能元件的設定

KAVSHELL FIM /BASELINE 指令的回傳代碼

KAVSHELL FIM /BASELINE 指令的回傳代碼

回傳代碼	敘述
0	操作順利完成
-2	未執行服務
-3	權限錯誤
-4	找不到物件（找不到工作項目）
-5	指令語法無效
-6	無效操作（例如，基線已被刪除）
-10	無法建立設定檔（例如，無法存取檔案路徑中所指定的資料夾）
-12	無效密碼
-80	與偵測到的基線物件不一致
-85	建立工作記錄失敗
-99	內部錯誤
-303	無效產品授權金鑰
-502	工作未執行
200	所有物件均與基線一致
501	工作成功完成，但有錯誤/備註

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

如果您無法透過手冊及相關資源自行排除問題，建議您與技術支援聯絡。技術支援服務專家會為您解答關於安裝和使用該應用程式的任何問題。

技術支援服務僅適用擁有正式版產品授權的使用者。試用版產品授權授權的使用者將不包含在技術支援服務範圍內。

根據應用程式生命週期提供應用程式支援（請參閱應用程式生命週期頁面）。

與技術支援部門聯絡之前，請通讀技術支援規則。

您可以在 Kaspersky CompanyAccount 頁面上將您的請求傳送給 Kaspersky 技術支援中心。

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

有關 Kaspersky CompanyAccount 操作的更多資訊，請參閱技術支援網站。

使用偵錯檔案和 AVZ 指令碼

向 Kaspersky 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 Kaspersky 技術支援部門。Kaspersky 技術支援專家還可能需要您建立偵錯檔案。偵錯檔案可以追蹤程式指令的每一步執行，以偵測錯誤發生時的程式執行階段。

在 Kaspersky 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，掃描受防護裝置以尋找威脅，清除或刪除感染的檔案以及建立系統掃描報告。

詞彙表

OLE 物件

附加到其他檔案或透過使用物件連結與內嵌 (OLE) 技術內嵌其他檔案的物件。一個 OLE 物件範例是內嵌到 Microsoft Office Word 文件中的 Microsoft Office Excel® 電子表格。

SIEM

一種用於分析來源於各種網路裝置和應用程式的安全事件的技術。

事件嚴重性

在 Kaspersky 應用程式執行過程中遇到的事件的內容。有以下嚴重等級：

- 緊急事件
- 功能故障
- 警告
- 資訊

同一類型的事件可能有不同的嚴重等級，具體取決於發生事件時的情況。

備份

用來儲存檔案備份副本的特殊儲存，在嘗試解毒或刪除前建立。

卡巴斯基安全網路 (KSN)

一個雲端服務基礎架構，提供對 Kaspersky 資料庫的存取，該資料庫不斷更新關於檔案、Web 資源和軟體的信譽的資訊。卡巴斯基安全網路允許 Kaspersky 十分迅速地對新威脅作出回應，提高許多防護元件的效能，以降低誤報可能性。

受感染的物件

其部分程式碼完全比對已知惡意軟體部分程式碼的物件。Kaspersky 不建議存取此類物件。

可感染的檔案

一種由於其結構或格式，可被罪犯用作儲存和傳播惡意程式碼的"容器"的檔案。通常為可執行檔，此類檔案副檔名為 .com、.exe 和 .dll。此類檔案被惡意程式碼侵入的風險非常高。

壓縮檔案

一個或多個檔案透過壓縮封裝到單個檔案中。壓縮和解壓縮資料需要一個名為壓縮應用程式的專用應用程式。

安全等級

安全等級定義為一組預先配置的應用程式元件設定。

工作

Kaspersky 程式執行的功能是以工作形式呈現，如：即時檔案防護、電腦完整掃描和資料庫更新。

工作設定

特定於每個類型工作的程式設定。

弱點

作業系統或應用程式存在的弱點，惡意軟體研發者會利用這種弱點入侵作業系統或應用程式並破壞其完整性。作業系統中的許多弱點都會導致作業系統不可靠，因為侵入作業系統的病毒可能會導致作業系統本身和安裝的應用程式損壞。

政策

政策確定應用程式的設定並管理在管理群組內的電腦上配置該應用程式的能力。必須為每個應用程式建立單獨政策。您可以為每個管理群組內的電腦上安裝的應用程式建立多個政策，但在一個管理群組內一次只能對每個應用程式套用一個政策。

啟動物件

電腦上安裝的作業系統和軟體正常啟動和執行所需的一組應用程式集。每次啟動作業系統時，都會執行這些物件。有些病毒專門感染此類物件，例如，可能會導致作業系統無法啟動。

啟動金鑰

應用程式目前使用的產品授權金鑰。

啟發式分析

用於偵測其資訊尚未新增到 Kaspersky 資料庫中的威脅技術。啟發式分析用於透過偵測運作行為，判斷對作業系統構成安全威脅的物件。啟發式分析偵測到的物件將被視為可能受感染。例如，如果一個物件包含惡意物件通常具有的運作行為（檔案開啟、寫入），則可能會將該物件視為可能受感染。

更新

替換或新增從 Kaspersky 更新伺服器上擷取的新檔案（資料庫或應用程式模組）的過程。

本機工作

定義為在單台用戶端電腦上執行的工作。

檔案遮罩

使用萬用字元表示檔案名稱。檔案遮罩中使用的標準萬用字元為 * 和 ?，其中 * 表示任意數量的任意字元，? 表示單個任意字元。

產品授權期限

一個時間段，在此時間段內您可以存取應用程式功能，並有權使用附加服務。您可以使用的服務取決於產品授權類型。

病毒特徵碼資料庫

該資料庫中包含截至病毒資料庫發佈日期為止 Kaspersky 已知的電腦安全威脅相關資訊。資料庫中的項目用於在掃描物件時偵測到惡意程式。Kaspersky 的專家維護資料庫每小時更新一次。

管理伺服器

卡巴斯基安全管理中心的一個元件，可集中儲存公司網路內所有安裝 Kaspersky 應用程式的資訊。它也可用於管理這些應用程式。

解毒

一種處理受感染檔案的方法，該方法會導致完全或部分還原資料，或裁定無法解毒檔案。不是所有的受感染物件都可以解毒。

誤報

Kaspersky 應用程式因物件的程式碼與病毒的程式碼類似而將未感染的物件視為受感染物件的情況。

防護狀態

目前防護狀態，反映電腦安全性的等級。

隔離

Kaspersky 應用程式將偵測到的可能受感染物件移動到的資料夾。在此以加密形式儲存在隔離，以避免對電腦造成任何影響。

有關協力廠商程式碼資訊

有關協力廠商程式碼資訊被包含在檔案 legal_notices.txt 中，並位於應用程式的安裝資料夾中。

商標聲明

註冊商標和服務標誌均為其各自所有者擁有的財產。

CVE 為 MITRE Corporation 的註冊商標。

Core、Intel、Pentium 是 Intel Corporation 在美國和/或其他國家/地區的商標。

Linux 是 Linus Torvalds 在美國和/或其他國家/地區註冊的商標。

Microsoft、Active Directory、Excel、Internet Explorer、Outlook、Windows、Windows Server、Windows Vista 是 Microsoft Corporation 在美國和其他國家/地區的註冊商標。

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。