kaspersky

Kaspersky Endpoint Security for Linux 12.5.0

© 2026 AO Kaspersky Lab

目錄

Kaspersky Endpoint Security for Linux
關於應用程式
主要功能
版本 12.5 新增功能
已修正的問題
硬體和軟體需求
分發套件
與其他應用程式的相容性
卡巴斯基解決方案之間的功能比較
部署與初始設定
模式和部署方案
準備應用程式安裝環境
選擇系統事件攔截機制
準備分發套件
卡巴斯基安全管理中心中的準備動作
使用卡巴斯基安全管理中心安裝應用程式
使用指令列安裝應用程式
在某些作業系統中安裝後的額外設定步驟
使用快速安裝指令碼移轉至卡巴斯基安全管理中心 Linux 的情境
從先前版本更新應用程式
更新 Kaspersky Endpoint Security 管理外掛程式
升級後的應用程式設定
解除安裝應用程式
使用應用程式
產品授權
如何切換到其他卡巴斯基解決方案
管理產品授權金鑰
檢視產品授權金鑰的資訊
應用程式的管理介面
使用卡巴斯基安全管理中心管理應用程式
卡巴斯基安全管理中心政策
政策管理
匯出和匯入政策設定
在卡巴斯基安全管理中心中建立的 Kaspersky EndpoinSecurity 工作
登入和登出網頁主控台和雲端主控台
使用指令列管理應用程式
Kaspersky Endpoint Security 本機工作
編輯工作設定
設定工作排程
管理一般應用程式設定
使用篩選器來限制查詢結果
匯出和匯入應用程式設定
透過圖形介面管理應用程式

防護狀態監控
即時保護狀態
事件和報告
配置將事件記錄到作業系統日誌中
配置應用程式事件記錄設定
檢視應用程式事件
檢視報告
獲取系統效能指標
應用程式穩定性監控
應用程式元件完整性檢查
應用程式存取控制
預先定義的角色
如何指派或撤銷使用者角色
卡巴斯基安全管理中心中的 RBAC 功能區域
受防護裝置典型角色的建議
更新應用程式資料庫和模組
如何選擇更新來源和散佈方案
如何設定資料庫更新工作
如何使用 Kaspersky Update Utility 進行更新
如何回溯應用程式資料庫和模組更新
主機威脅防護
檔案威脅防護
如何建立防護範圍
如何選擇偵測到檔案威脅時的動作
什麼是檔案掃描的智慧模式
如何最佳化檔案掃描
掃描符號連結和硬連結的特殊注意事項
惡意軟體掃描
如何建立掃描範圍
如何設定掃描排程
如何掃描單一檔案或目錄
如何最佳化自訂掃描任務
關鍵區域掃描
容器掃描
如何配置與容器管理工具的整合
如何為容器和映像建立自訂掃描範圍
如何最佳化容器掃描
如何選擇當偵測到受感染物件時要對容器執行的操作
如何對容器和映像執行自訂掃描
卸除式磁碟機掃描
行為偵測
弱點利用防禦
Anti-Cryptor
如何選擇偵測到惡意加密時的操作
如何建立防護範圍

BadUSB 攻擊防護
如何設定 USB 裝置授權
如何允許使用螢幕小鍵盤連接 USB 裝置
如何允許使用條碼掃描器連接 USB 裝置
通訊與 Web 防護
郵件威脅防護
偵測到郵件威脅時該怎麼辦
如何最佳化電子郵件附件掃描
電子郵件附件篩選器的用途
Web 威脅防護
如何在偵測到 Web 威脅時選擇操作
什麼是釣魚防護
網路威脅防護
如何選擇偵測到網路威脅時的動作
如何管理被封鎖的裝置
防火牆管理
如何建立網路封包規則
網路封包規則使用範例
如何將 IP 位址新增至網路區域：公用、本機、受信任
什麼是動態規則
如何建立連線至卡巴斯基安全管理中心的規則
安全控制
裝置控制
如何在指令列上管理受信任裝置清單
如何設定裝置存取模式
如何設定裝置存取規則
如何設定裝置控制訊息範本
授予對裝置的臨時存取權限
Web 控制
如何建立網頁資源的存取規則
如何修改 Web 控制訊息範本
用於建立 Web 資源位址遮罩的規則
應用程式控制
應用程式清查
如何設定應用程式控制操作模式
建立應用程式類別
黃金映像
關於應用程式控制規則
應用程式控制規則測試模式
系統完整性監控
即時系統完整性監控
系統完整性檢查
信任區域
如何新增防護排除項目
如何新增受信任的網址
如何新增電腦的受信任 IP 位址
如何選取受監控的網路連接埠

- 如何將憑證新增至受信任的根憑證清單
- 如何新增受信任網域
- 如何排除掛載點
- 如何新增受信任應用程式
- 如何新增受信任裝置

一般設定

- 偵測設定
- 卡巴斯基安全網路
  - 如何啟用或停用卡巴斯基安全網路
  - 應用程式的雲端模式是什麼
  - KSN 代理的用途
- 配置資料傳輸到卡巴斯基安全管理中心儲存
- 如何設定應用程式啟動
- 配置工作管理的權限
- 密碼防護
  - 關於自訂權限
  - 預設使用者權限
- 效能設定
- 網路設定
  - 如何管理代理伺服器設定
  - 應用程式如何攔截流量
  - 如何設定憑證驗證政策
  - 如何配置受監控的連接埠
  - 使用作業系統工具設定流量攔截排除項目
- 攔截檔案操作
- 設定系統事件攔截
- 管理其他遙測設定
- 備份

進階威脅和目標式攻擊防護

- 因應措施
  - 搜尋入侵指標
  - 網路隔離
    - 在網頁主控台中手動啟用或停用裝置的網路隔離
    - 設定自動網路隔離的持續時間
    - 手動設定網路隔離
    - 在網頁主控台中設定網路隔離排除項目
  - 隔離檔案
  - 從裝置接收檔案
  - 從裝置中刪除檔案
  - 啟動處理程序
  - 終止處理程序
  - 物件的執行防禦
  - 管理隔離區
- Endpoint Detection and Response Optimum
  - 如何啟用 EDR Optimum 整合
  - 如何確認 EDR Optimum 整合正常運作
  - Cloud Sandbox

Endpoint Detection and Response Expert (on-premises)
如何準備參考映像以便與 EDR Expert (on-premises) 正確整合
如何設定 EDR Expert (on-premises) 整合
如何驗證 EDR Expert (on-premises) 整合已啟動並正常執行
Endpoint Detection and Response Expert (cloud)
如何設定內建代理與 EDR Expert (cloud) 的整合
如何最佳化 EDR Expert (cloud) 遙測傳輸
如何設定 EDR Expert (cloud) 遙測資料排除項目
如何匯出或匯入 EDR Expert (cloud) 事件篩選器
Kaspersky Anti Targeted Attack Platform
如何配置 EDR (KATA) 整合
如何配置 NDR (KATA) 整合
如何驗證 KATA 整合已啟動並正在執行
Sandbox
如何設定 Sandbox 整合
如何確認 Sandbox 整合已啟動並正常執行
如何手動將檔案傳送到沙盒
Kaspersky Managed Detection and Response
建立參考映像以便與 MDR 正確整合的建議
上傳 KPSN 設定檔
如何設定 MDR 整合
如何驗證 MDR 整合是否已啟用
Kaspersky Unified Monitoring and Analysis Platform
如何設定 KUMA 整合
如何驗證 KUMA 整合已啟動並正在執行
虛擬環境防護
如何設定 SVM 探索
Light Agent 如何選擇 SVM
如何在 SVM 之間平衡 Light Agent 的連線
保護 Light Agent 與 SVM 之間的連線
如何查看 Light Agent 的狀態
最佳做法
最佳化應用程式的資源消耗
裝置上的應用程式效能分析
檔案威脅防護和掃描工作建議
關於 Web 威脅防護和網路威脅防護工作的建議
行為偵測建議
與卡巴斯基解決方案的互通性
卡巴斯基安全管理中心 Linux
Network Detection and Response (KATA)
Kaspersky Unified Monitoring and Analysis Platform
應用程式元件參考
用於管理 Kaspersky Endpoint Security 的指令
用於管理產品授權金鑰的指令
用於管理使用者和角色的指令

管理應用程式工作和設定
用於管理一般應用程式設定的指令
用於管理工作設定的指令
用於管理工作的命令
用於管理一般容器掃描設定的指令
用於管理網路流量掃描設定的指令
狀態和防護監控
統計指令
用於顯示事件的指令
用於管理應用程式事件的指令
用於管理系統效能指標的指令
安全控制
用於管理裝置控制的指令
用於管理應用程式控制的指令
Web 控制管理指令
網路連線防護
用於管理被封鎖裝置的指令
防火牆管理指令
進階威脅和目標式攻擊防護
用於管理隔離區的指令
用於管理 EDR Expert (on-premises) 元件的指令
用於管理 EDR Expert (cloud) 元件的指令
用於管理 NDR (KATA) 元件的命令
用於管理裝置網路隔離的命令
用於管理 KUMA 整合設定的指令
用於管理 Sandbox 整合設定的指令
用於管理 IOC 掃描的指令
Light Agent 模式下的應用程式指令
應用程式命令列選項
更新工作
主機威脅防護
檔案威脅防護工作
最佳化網路目錄掃描
惡意軟體掃描
惡意軟體掃描工作
自訂掃描工作
關鍵區域掃描工作
卸除式磁碟機掃描工作
容器掃描
容器掃描設定
容器掃描工作
與 Jenkins 整合
加密軟體防護工作
行為偵測工作
弱點利用防禦

- 使用卡巴斯基安全網路
  - 連線到卡巴斯基安全網路
  - 啟用或停用雲端模式
- BadUSB 攻擊防護工作
- 通訊與 Web 防護
- Web 威脅防護工作
- 掃描網路流量
  - 檢視和編輯網路流量掃描設定
  - 檢視加密連線掃描的排除項目
  - 管理受信任的根憑證清單
  - 設定與檢視流量攔截排除項目
- 網路威脅防護工作
- 防火牆管理
  - 設定網路封包規則清單
  - 設定網路區域
- 安全控制
- 裝置控制工作
- Web 控制
  - Web 控制工作
  - 檢視和編輯 Web 控制設定
- 應用程式控制
  - 應用程式控制工作
  - 建立和編輯類別清單
  - 檢視類別清單
  - 配置應用程式控制規則清單
- 設定清查
  - 清查工作
  - 檢視偵測到的應用程式清單
- 系統完整性監控工作
- 系統完整性檢查工作
- 進階威脅和目標式攻擊防護
- Kaspersky Endpoint Detection and Response Expert (on-premises) 整合
  - Kaspersky Endpoint Detection and Response Expert (on-premises) 整合設定
  - 管理用於連線到 OSMP EDR Expert (on-premises) 伺服器的憑證
- 卡巴斯基 Endpoint Detection and Response Expert (cloud) 整合
  - 卡巴斯基 Endpoint Detection and Response Expert (cloud) 整合設定
  - 管理 OSMP EDR Expert 伺服器 (cloud) 連線憑證
- Kaspersky Endpoint Detection and Response (KATA) 整合
  - Kaspersky Endpoint Detection and Response (KATA) 整合設定
  - 管理用於連線 KATA 伺服器的憑證
- Kaspersky Network Detection and Response (KATA) 整合
  - Kaspersky Network Detection and Response (KATA) 整合設定
  - 管理用於連線 NDR 伺服器的憑證
- Sandbox 整合
  - Sandbox 整合設定
  - 管理用於連線 Sandbox 伺服器的憑證
- 啟用或停用 Kaspersky Endpoint Detection and Response Optimum 整合

配置 Kaspersky Managed Detection and Response 整合
管理裝置網路隔離
管理隔離區設定
透過指令列管理被隔離的檔案
搜尋入侵指標
管理執行防護
配置 KUMA 整合
Kaspersky Unified Monitoring and Analysis Platform 整合工作
管理用於連線 KUMA 伺服器的憑證
一般設定
一般應用程式設定
工作排程
配置代理伺服器設定
配置備份設定
網路流量掃描設定
配置全域排除
密碼防護設定
管理主控台中的應用程式設定
資料庫更新
主機威脅防護
檔案威脅防護
掃描範圍視窗
「新增掃描範圍」視窗
掃描設定視窗
偵測到威脅後的動作視窗
檔案威脅防護排除項目
排除範圍視窗
新排除範圍視窗
依照遮罩排序排除項目視窗
依照威脅名稱排序排除項目視窗
依照處理程序使用排除項目視窗
受信任處理程序視窗
惡意軟體掃描
掃描範圍視窗
<新掃描範圍>視窗
掃描範圍設定視窗
掃描範圍視窗
掃描設定視窗
偵測到威脅後的動作視窗
排除項目部分
排除範圍視窗
新排除範圍視窗
依照遮罩排序排除項目視窗
依照威脅名稱排序排除項目視窗
關鍵區域掃描
掃描範圍視窗
「新增掃描範圍」視窗

掃描範圍設定視窗
掃描範圍視窗
掃描設定視窗
偵測到威脅後的動作視窗
排除項目部分
排除範圍視窗
新排除範圍視窗
依照遮罩排序排除項目視窗
依照威脅名稱排序排除項目視窗
容器監控
容器掃描設定視窗
容器掃描
容器掃描設定視窗
掃描設定視窗
偵測到威脅後的動作視窗
排除項目部分
依照遮罩排序排除項目視窗
依照威脅名稱排序排除項目視窗
卸除式磁碟機掃描
行為偵測
依照處理程序使用排除項目視窗
受信任處理程序視窗
弱點利用防禦
弱點利用防禦排除項目視窗
弱點利用防禦排除視窗
Anti-Cryptor
掃描範圍視窗
「新增掃描範圍」視窗
防護設定視窗
排除範圍視窗
新排除範圍視窗
依照遮罩排序排除項目視窗
卡巴斯基安全網路
卡巴斯基安全網路設定
卡巴斯基安全網路聲明
卡巴斯基私人安全網路聲明
BadUSB 攻擊防護
通訊與 Web 防護
郵件威脅防護
郵件威脅防護設定視窗
附件篩選視窗
Web 威脅防護
受信任網址視窗
掃描設定視窗
網路威脅防護
排除視窗

- 防火牆管理
  - 網路封包規則視窗
  - 增加了網路封包規則視窗
  - 新增 IP 位址視窗
  - 可用網路視窗
  - 網路連線視窗
- 安全控制
  - 裝置控制
    - 受信任裝置視窗
    - 受信任裝置（裝置 ID）視窗
    - 用戶端裝置上的裝置視窗
    - 基於裝置控制事件視窗的裝置清單
    - 存取受信任裝置的視窗
    - 使用者或群組視窗
    - 裝置類型視窗
    - 設定裝置存取規則視窗
    - 使用者或群組視窗
    - 存取排程視窗
    - 連線匯流排視窗
  - Web 控制
    - Web 控制規則視窗
    - 內容類別選取視窗
    - 資料類型類別選取視窗
    - 選擇位址視窗
    - 選擇位址群組視窗
    - 新增位址群組視窗
    - 選擇使用者視窗
    - 使用者或群組視窗
    - 存取排程視窗
  - 應用程式控制
    - 應用程式控制規則視窗
    - 新增規則視窗
    - 應用程式類別視窗
    - 使用者或群組視窗
    - 清查
      - 掃描範圍視窗
      - 「新增掃描範圍」視窗
      - 排除項目部分
      - 排除範圍視窗
      - 新排除範圍視窗
  - 系統完整性監控
    - 掃描範圍視窗
    - 「新增掃描範圍」視窗
    - 排除範圍視窗
    - 新排除範圍視窗
    - 依照遮罩排序排除項目視窗

系統完整性檢查
掃描範圍視窗
「新增掃描範圍」視窗
排除項目部分
排除範圍視窗
新排除範圍視窗
依照遮罩排序排除項目視窗
本機工作
工作管理
進階威脅和目標式攻擊防護
與 Kaspersky Managed Detection and Response 整合
Kaspersky Endpoint Detection and Response (on-premises) 整合
配置 KATA 伺服器連線
管理一般 KATA 伺服器連線設定
配置到 KATA 伺服器的資料傳輸
Kaspersky Network Detection and Response (KATA) 整合
配置 NDR 伺服器連線
管理一般 NDR 伺服器連線設定
配置到 NDR 伺服器的資料傳輸
與 KUMA 整合
KUMA 伺服器視窗
KUMA 伺服器視窗
KUMA 伺服器連線設定視窗
新增伺服器憑證視窗
新增用戶端憑證視窗
隔離
物件的執行防禦
一般設定
代理伺服器
代理伺服器排除項目視窗
掃描工作的 CPU 使用率
使用電池電源執行工作
啟動應用程式
收到關鍵更新時自動重新啟動
密碼防護
追蹤與傾印設定
應用程式的駐留記憶體使用率
加密連線掃描
受信任網域視窗
受信任憑證視窗
流量攔截排除項目視窗
流量攔截排除項目視窗
監控的連接埠
全域排除項目
掛載點路徑視窗
從掃描中排除處理程序記憶體
備份

偵測駭客可用來造成危害的應用程式
攔截檔案操作
傳送資訊至卡巴斯基安全管理中心儲存區
系統事件攔截
其他遙測設定
Light Agent 模式
連線至 Integration Server
連線至 Integration Server 視窗
驗證 Integration Server 憑證視窗
Integration Server 視窗中的身分驗證
SVM 發現設定
SVM 連線標籤
SVM 選擇演算法
防護連線
已知問題和限制
聯絡技術支援
透過 Kaspersky CompanyAccount 取得技術支援
獲取技術支援資訊
如何啟用和設定偵錯檔案的建立
如何啟用和設定傾印
使用卡巴斯基安全管理中心進行遠端裝置診斷
附錄
附錄 1。設定檔和預設應用程式設定
用於編輯工作設定檔的規則
初始設定檔
安裝套件中的初始設定
預設設定檔
指令列工作的預設設定
File_Threat_Protection 工作 (ID:1) 的預設設定
Scan_My_Computer 工作 (ID:2) 的預設設定
Scan_File 工作 (ID:3) 的預設設定
Critical_Areas_Scan 工作 (ID:4) 的預設設定
更新工作 (ID:6) 的預設設定
System_Integrity_Monitoring 工作 (ID:11) 的預設設定
Firewall_Management 工作 (ID:12) 的預設設定
Anti_Cryptor 工作的預設設定 (ID:13)
Web_Threat_Protection 工作（ID:14）的預設設定
Device_Control 工作 (ID:15) 的預設設定
Removable_Drives_Scan（ID:16）工作的預設設定
Network_Threat_Protection 工作（ID:17）的預設值
Container_Scan (ID:18) 和 Custom_Container_Scan (ID:19) 工作的預設設定
Behavior_Detection 工作的預設設定（ID:20）
Application_Control 工作的預設設定 (ID:21)
Inventory_Scan 工作的預設設定 (ID:22)
KATAEDR 工作的預設設定（ID:24）
Web_Control 工作（ID:26）的預設設定
Standalone_Sandbox 工作（ID:29）的預設設定

KATANDR 工作（ID:31）的預設設定
KUMA 工作（ID:33）的預設設定
郵件威脅防護工作（ID：35）的預設設定；
BadUSB 攻擊防護工作（ID：37）的預設設定；
KATANDR 工作（ID:31）的預設設定
附錄 2。配置與 Linux 版卡巴斯基防毒軟體郵件伺服器的互動
附錄 3。與外部服務互動的設定
附錄 4。檔案延伸程式，用於快速掃描卸除式磁碟機
附錄 5。訊息模板中的變數
附錄 6。應用程式事件
緊急
警告
資訊訊息
附錄 7。傳回碼
附錄 8。準備包含應用程式資料庫的壓縮檔
附錄 9。IOC 檔案的要求
法律聲明
資料提供
當使用啟動碼時提供的資料
從卡巴斯基更新伺服器下載更新時提供的資料
在 Light Agent 模式下使用應用程式時傳輸的資料
傳送至卡巴斯基安全管理中心的資料
在應用程式介面中點擊連結時提供的資料
使用卡巴斯基安全網路時提供的資料
與 Kaspersky Endpoint Detection and Response Optimum 整合時提供的資料
與 Kaspersky Endpoint Detection and Response (KATA) 元件整合時提供的資料
與 Kaspersky Endpoint Detection and Response Expert (on-premises) 元件整合時提供的資料
與 Kaspersky Endpoint Detection and Response Expert (cloud) 元件整合時提供的資料
與 Kaspersky Network Detection and Response (KATA) 元件整合時提供的資料
與卡巴斯基統一監控和分析平台整合時提供的資料
有關協力廠商代碼的資訊
商標聲明

Kaspersky Endpoint Security for Linux

瀏覽

Kaspersky Endpoint Security for Linux
版本 12.5 新增功能
典型部署方案
功能比較
已知問題和限制

快速入門

硬體和軟體需求
相容性
準備發佈套件
準備安裝環境
部署應用程式
移轉到卡巴斯基安全管理中心 Linux 的方案

使用應用程式

啟動
更新資料庫
使用 Kaspersky Update Utility 進行更新
檔案威脅防護
受信任區域
最佳化資源

在命令列中設定

使用指令列管理應用程式
管理命令
應用程式命令列選項

支援

保護狀態監控
升級先前版本的應用程式
聯絡技術支援服務

關於應用程式

Kaspersky Endpoint Security for Linux 為 Linux 裝置提供進階的全方位防護，並可預防、偵測及回應各種類型的威脅、網路攻擊和詐欺。此應用程式包含在許多卡巴斯基多平台解決方案中，且可彈性設定，以因應貴組織 IT 基礎架構的挑戰。

您可以在本機管理安裝於受防護裝置上的 Kaspersky Endpoint Security，也可以使用 卡巴斯基安全管理中心 進行集中管理。

應用程式不適用於使用自動控制系統的工業處理程序。為了防護這些系統中的裝置，建議使用 Kaspersky Industrial CyberSecurity for Linux Nodes 。

主要功能

防範大規模網路威脅

以先進技術為基礎的防護是您 IT 安全的基礎。Kaspersky Endpoint Security 可防止使用者裝置的檔案系統遭到感染、監控卸除式磁碟機與裝置的連線，並掃描是否有病毒。它會監控應用程式的惡意活動，並保護檔案免受惡意遠端加密。包含新型全球威脅（例如病毒、木馬程式、加密程式、駭客攻擊）相關資訊的資料庫會定期自動更新。

通訊與 Web 防護

Kaspersky Endpoint Security 可可靠地保護您組織的網路環境：在您開啟電子郵件與下載的檔案以及存取網站之前，掃描其中是否有病毒、網路蠕蟲和其他威脅。應用程式可掃描傳入網路流量中可能表示網路攻擊的活動、監控作業系統防火牆設定，並篩選網路活動。

工作場所安全控制

透過使用 Kaspersky Endpoint Security 控制使用者在工作場所對應用程式、Web 資源和連線裝置的存取，您可以為組織提供另一層安全防護。這有助於保護裝置免受感染，並防止資料遺失或外洩。

防範進階威脅和針對性攻擊

應用程式可以與卡巴斯基 Detection and Response 解決方案互動，亦即 Kaspersky Managed Detection and Response (MDR) 和 Kaspersky Anti Targeted Attack Platform (KATA)。卡巴斯基 SIEM 解決方案 Kaspersky Unified Monitoring and Analysis Platform (KUMA) 也受支援。Kaspersky Endpoint Security 會監控在使用者裝置上執行的處理程序、開啟的網路連線以及正在修改的檔案。與 Detection and Response 解決方案的互動可提供防護，以抵禦弱點利用、勒索軟體、無檔案攻擊，以及駭客可用來入侵裝置或資料的合法系統工具等威脅。

虛擬和雲端環境防護

Kaspersky Endpoint Security 作為 Kaspersky Security for Virtualization Light Agent 解決方案的一部分，可為在各種伺服器虛擬化平台和 VDI 平台上執行 Linux 客體作業系統的虛擬機提供防護。對物件的病毒掃描由安裝在獨立虛擬機 SVM (Secure Virtual Machine) 上的特殊元件執行。因此，應用程式會使用 SVM 的資源而非虛擬機的資源來提供安全防護，並結合智慧最佳化（例如使用共用快取），將 IT 基礎架構的整體負載降至最低。

版本 12.5 新增功能

Kaspersky Endpoint Security 12.5 for Linux 引入了以下功能和改進：

- 支援在具有 Elbrus CPU 的裝置上安裝 Kaspersky Endpoint Security 12.5 for Linux。應用程式為 Elbrus CPU 提供有限支援。

- 已實作與 Kaspersky Endpoint Detection and Response Expert (cloud) 的整合。此雲端解決方案旨在保護組織的 IT 基礎架構免受進階網路威脅的侵害，包括無法由安裝在公司資產上的 EPP 應用程式偵測到的威脅。此解決方案利用各種回應工具和資料來源（包括端點資產、網路資料和雲端環境資料），提供全面的可視性、關聯和自動化，並透過整合式元件和單一介面中的端對端工作流程實現統一的偵測和回應流程，進而提高安全專家的效率。

  Kaspersky Endpoint Security for Linux 與 Kaspersky Endpoint Detection and Response Expert (cloud) 解決方案的整合暫時無法使用，直至該解決方案推出為止，其計劃於 2026 年底推出。之後，我們預期此版本的 Kaspersky Endpoint Security 將可使用整合功能，無需進行額外升級。

- Kaspersky Endpoint Security 應用程式中某些操作的密碼防護。密碼防護可讓您根據授予使用者的權限，限制使用者可在 Kaspersky Endpoint Security 應用程式中執行的操作。限制對應用程式設定的存取權限，可降低對應用程式進行未授權或非故意變更的風險。

- 裝置控制元件得到了改進。現在，您可以將受信任裝置清單匯出到檔案，並從檔案匯入該清單。

- 改進了 BadUSB 攻擊防護 元件。現在，當您連接條碼掃描器時，可以掃描螢幕上的條碼來授權掃描器，而不必輸入授權碼來解鎖裝置。

- 對 可更新的內核模組 (ULKM) 的改進：

  - 新增支援在已啟用 Secure Boot 的系統上，以可更新的內核模組 (ULKM) 為基礎攔截系統事件。

  - 應用程式現在支援更多可使用可更新的內核模組攔截事件的作業系統。

  - 我們為加密軟體防護和裝置控制元件新增了可更新的內核模組支援。

- 我們改善了 Astra Linux Special Edition 封閉軟體環境模式中的安裝流程。現在，如果已安裝相容性套件，使用者在搭載 Astra Linux Special Edition 作業系統的裝置上安裝 Kaspersky Endpoint Security 應用程式後，無需手動執行其他操作即可啟動該應用程式。

- 現在，在安裝應用程式時，您可以使用 autoinstall.ini 設定檔修改 kesl.ini 設定檔的設定。

- 改進了應用程式安裝和解除安裝期間的錯誤診斷：

  - 傳回代碼變得更加詳細，以便更清楚地瞭解任何潛在問題。

  - 我們新增了關於安裝和應用程式正確執行所需的相依性（外部程式庫、元件、公用程式或其他程式）缺失的新訊息。

  - 我們新增了關於系統目錄存取權限設定不正確的新訊息。

- 卡巴斯基安全管理中心會顯示新的及更明確的錯誤訊息。
- 現在，您可以在安裝應用程式時忽略套件管理員錯誤。

- 現在，應用程式會在應用程式資料庫和模組首次更新後，於安裝期間自動重新啟動。現在，在安裝應用程式後的前 24 小時過後，您可以設定應用程式在收到關鍵更新時自動重新啟動。您可以在命令列中的一般應用程式設定，或使用網頁主控台或管理主控台在政策內容中，設定應用程式自動重新啟動。
- 現在，與 Detection and Response 解決方案整合時，您可以使用 kesl.ini 設定檔中的 `UseIncreasedXdrEventsCache` 設定來管理事件快取。高效能與 RAM 佔用量之間需要取捨。
- 現在，停止或重新啟動應用程式時，您可以使用 kesl.ini 設定檔中的 `FastShutdown` 設定快速關閉 kesl 行程，這有助於將高負載系統上應用程式的停機時間降至最低，並防止過度消耗資源。
- 現在，您可以使用 kesl.ini 設定檔中的 `ReduceSWMemoryConsumption` 設定，限制行為分析元件處理事件佇列時的記憶體消耗。使用此設定可能會影響保護等級。請務必檢閱文件。
- 我們改善了網路存取的穩定性。現在，如果 kesl 處理程序異常終止，Watchdog 伺服器會移除應用程式在 Web 威脅防護和網路威脅防護元件啟動時新增的防火牆規則，讓您避免失去網際網路連線，並在裝置上快速還原網路存取。
- 現在，您可以防止多個掃描工作同時執行，以最佳化應用程式效能。現在，啟用此選項後，如果同時啟動多個掃描工作，這些工作會排入佇列。
- 檔案威脅防護排除項目現在可以處理符號連結。路徑現在會轉換為最終檔案位址。
- 現在，您可以使用管理一般應用程式設定的命令，啟用並設定傾印檔案目錄，而無需重新啟動應用程式。這些傾印檔案設定已從 kesl.ini 設定檔中移除。
- 現在，與 Kaspersky Endpoint Detection and Response Expert (on-premises)、Kaspersky Anti Targeted Attack Platform 和 Kaspersky Unified Monitoring and Analysis Platform 解決方案整合時，必須使用密碼。現在，設定整合時，您必須為用戶端憑證指定密碼。
- 現在，在 Kaspersky Unified Monitoring and Analysis Platform 整合中傳送遙測事件時，應用程式可以壓縮流量，這有助於節省頻寬。
- 我們更新了支援的作業系統清單，其中包括對 CentOS 5.2、5.4、6.4 和 6.6 之 64 位元版本的支援。
- 應用程式介面提供新的語言版本：西班牙文（墨西哥）和葡萄牙文（巴西）。

舊版本中的變更

版本 12.4

Kaspersky Embedded Systems Security 12.4 for Linux 現在具備以下新功能和改進：

- 新增功能元件：郵件威脅防護。此元件會掃描收發電子郵件的附件，以偵測病毒和其他威脅性應用程式。
- 新增功能元件：BadUSB 攻擊防護。此元件可阻止將偽裝成鍵盤的受感染 USB 裝置連線到用戶端裝置。
- 裝置控制元件得到了改進。現在，您可以根據使用者要求授予對被封鎖裝置的臨時存取權限。
- 改進了弱點利用防禦元件。現在，您可以為物件設定特定元件的掃描排除項目。

- 可更內核模組的改進：
  - 現在，可更新的內核模組可讓您最佳化檔案操作攔截。透過使用無需掃描的檔案和處理程序快取，應用程式效能得到提高。
  - 現在，透過使用可更新內核模組，您可以更精細地配置全域排除項目。如果您使用以 fanotify 技術為基礎的攔截機制，則指定的掛載點會完全排除在檔案操作攔截之外。使用可更新內核模組，您可以排除裝置上掛載的特定本機或遠端目錄。
- 提供與 Kaspersky Endpoint Detection and Response (KATA) 整合的 EDR (KATA) 元件已重新命名為 EDR Expert (on-premises)。此元件也提供 Kaspersky Endpoint Detection and Response Expert (on-premises) 整合。整合工作已重新命名為 *Kaspersky Endpoint Detection and Response Expert (on-premises) 整合* (KATAEDR, ID: 24)。
- 現在，您可以設定與 Kaspersky Endpoint Detection and Response Expert (on-premises) 的整合，這是一款企業網路安全解決方案，可防禦大多數網路安全風險，並涵蓋威脅傳播的主要場景。卡巴斯基 Endpoint Detection and Response Expert (on-premises) 的元件部署在開放式單一管理平台 (OSMP) 上。與 Kaspersky Endpoint Detection and Response Expert (on-premises) 的整合支援 Kaspersky Endpoint Detection and Response (KATA) 整合的所有功能，以及新功能：
  - 啟動 YARA 掃描。在 *YARA 掃描*期間， Kaspersky Endpoint Security 使用 YARA 檔案搜尋裝置上的惡意活動特徵。
  - 收集取證資料，即在調查涉及網路犯罪和資料外洩的事件時可能有用的數位資料。
  - 將有關裝置上事件的延伸資料（遙測資料）傳送到 OSMP 平台上的遙測伺服器。
  - 僅傳送含攻擊指標 (IOA) 的遙測資料。現在，您也可以在網頁主控台政策中設定自訂篩選器。
  - 透過新增產品授權金鑰來啟動EDR Expert (on-premises) 元件，該元件提供與 Kaspersky Endpoint Detection and Response Expert (on-premises) 的整合以及與 Kaspersky Endpoint Detection and Response (KATA) 的整合。
  - 在命令列上的 *Kaspersky Endpoint Detection and Response Expert (on-premises) 整合*工作設定中，或在網頁主控台中的政策屬性中，選取整合模式。
- 應用程式可在 Endpoint Detection and Response Agent 模式下使用，以支援 Kaspersky Detection and Response 解決方案與受防護裝置上的協力廠商病毒防護解決方案協同工作。在此模式下，裝置將不受標準防護和 Kaspersky Endpoint Security 的控制元件的防護。協力廠商應用程式負責裝置的標準防護。
- 您可以在安裝後首次啟動應用程式時建立偵錯檔案。現在，您可以在網頁主控台、管理主控台或初始設定檔設定中啟用首次啟動應用程式時建立偵錯檔案的功能。
- 網頁主控台中的政策管理介面已更新。政策中的區段結構已重新設計，以協助您更快找到所需功能。
- 現在，您可以選擇流量攔截模式：eBPF 技術或 iptables 實用程式。
- 現在，您可以選擇遙測來源（僅 eBPF 或 eBPF 加 auditd）。對於 auditd，您也可以選擇一種作業模式（獨佔模式或組播模式）。
- 現在，您可以選取將檔案和目錄傳送至沙盒進行掃描的模式：手動、僅自動、自動和手動。

- 在 Light Agent 模式下使用應用程式時，可以使用更多功能：
  - 以可更新的內核模組為基礎的系統事件攔截機制可供使用。
  - 弱點利用防禦功能元件可用。
  - 威脅偵測得到了改進。
- 現在，您可以直接使用卡巴斯基私人安全網路 (KPSN)，而無需在管理伺服器上使用 KSN 代理服務。
- 現在，您可以在網頁主控台和管理主控台中建立漫遊政策。漫遊政策會在裝置離開組織網路時生效。
- 在網頁主控台或管理主控台中檢視和匯出掛載點清單時，或在命令列中檢視此清單時，現在也會顯示在命名空間中找到的掛載點相關資訊。
- 我們改善了在具備 eBPF 支援且內核版本為 4.18 或更新版本的 64 位元作業系統上，行為偵測元件中用於取得系統遙測資料的替代機制，這可釋放 auditd 內核稽核子系統的資源。
- 現在，與 Kaspersky Managed Detection and Response 整合時，您可以將下列資訊包含在遙測資料中：
  - 容器中發生的事件指示
  - 容器命名空間 ID
  - 容器名稱
- 我們更新了支援的作業系統清單。

版本 12.3

Kaspersky Embedded Systems Security 12.3 for Linux 現在具備以下新功能和改進：

- 我們新增了以可更新的內核模組為基礎的系統事件攔截機制（在 Light Agent 模式下不可用）。如果裝置的作業系統支援 fanotify，並且滿足安裝可更新內核模組的其他要求，則可以配置應用程式以使用可更新的內核模組。使用可更新的內核模組可讓您最佳化 Kaspersky Endpoint Security 對處理程序啟動的攔截。可更新的內核模組包含在應用程式分發套裝中。
- 可更新的內核模組可改善加密軟體防護元件的功能（在 Light Agent 模式下不可用）。應用程式現在可以偵測更多類型的勒索軟體。
- 我們新增了一個新的功能元件：弱點利用防禦（在 Light Agent 模式下不可用）。弱點利用防禦可監控利用裝置弱點取得管理權限或執行惡意動作的程式碼。
- 裝置控制元件得到了改進：
  - 我們新增了設定使用者或使用者群組清單的功能，新增的裝置對清單中的使用者或群組會視為受信任。
  - 我們新增了允許對儲存裝置進行唯讀存取的功能。
  - 我們也改善了透過事件向使用者發出通知的方式，新增了事件，並在外掛程式和命令列中釐清和系統化了事件文字。

- 擴展了與 Kaspersky Managed Detection and Response 解決方案的整合：
  - 現在，您可以將裝置從網路隔離。
  - 您可以隔離檔案或從隔離區還原檔案。
  - 您可以啟動或終止一個處理程序。
- 我們新增了透過新增產品授權金鑰來啟動 MDR 元件的功能，該元件可提供與 Kaspersky Managed Detection and Response 整合。
- 行為偵測元件得到了改進。現在，您可以啟用或停用將處理程序從 MDR 和 EDR (KATA) 掃描中排除。
- 現在，您可以配置代理伺服器排除項目。您可以指定哪些 Kaspersky Endpoint Security 元件必須繞過代理伺服器，也可以建立一個不會為其使用代理伺服器的位址清單。如果在 Light Agent 模式下使用 Kaspersky Endpoint Security 以防護虛擬環境，則不支援使用代理伺服器連線卡巴斯基安全網路、SVM 和Integration Server。
- 現在，您可以設定流量攔截排除項目。現在，您可以使用應用程式的管理外掛程式或命令列，指定應用程式應從流量攔截中排除的連線。
- 現在，您可以暫時將資料庫記錄檔案從掃描中排除，以最佳化檔案威脅防護掃描。如果資料庫記錄檔案在上次掃描後的 10 分鐘內被相同處理程序重複使用，則應用程式將跳過對該記錄檔案的掃描。
- 現在，您可以在繼承父政策的設定時啟用合併父政策及其子政策中的排除清單項目。
- 現在，您可以使用管理 Web 外掛程式來匯出和匯入政策和工作中的排除項目清單。
- 我們新增了在建立安裝套件時或在安裝套件的屬性中在卡巴斯基安全管理中心管理主控台中配置 Kaspersky Endpoint Security 應用程式的初始配置設定的功能。
- 現在，您可以設定在使用電池供電的裝置上取消排程的工作。
- 我們新增了在 Kaspersky Endpoint Security 與 KSN 伺服器互動時啟用或停用 KSN 代理伺服器的功能（在 Light Agent 模式下不可用）。如果啟用了 KSN 代理伺服器，Kaspersky Endpoint Security 將使用管理伺服器上的 KSN 代理服務與 KSN 伺服器進行通訊。如果停用 KSN 代理伺服器，Kaspersky Endpoint Security 將直接與 KSN 伺服器互動。
- 在命令列上，您可以使用命令，該命令會顯示應用程式功能清單、其狀態（已使用或未使用）的資訊，以及實作這些應用程式功能所採用的 Linux 技術。
- 我們新增了在命令列和圖形介面中顯示裝置上生效的政策和政策設定檔相關資訊的功能。
- 現在，您可以使用命令列在未安裝 Perl 解釋器的裝置上安裝該應用程式。
- 我們改善了流量攔截。現在本機流量（同一裝置上處理程序之間的流量）不會被攔截。
- 現在，您可以在與 Kaspersky Managed Detection and Response 整合時傳遞傳送遙測所需的必要設定，而無需使用 KPSN 設定檔。如果您正在使用卡巴斯基安全網路基礎架構解決方案，或者您的唯一租用戶是根租用戶，則不需要 KPSN 設定檔即可與 Kaspersky Managed Detection and Response 整合。
- 最佳化了應用程式事件記錄中大量事件的儲存機制。現在，開啟和關閉事件資料庫以及擷取事件的速度都更快。

- 我們改善了應用程式的圖形介面（如果應用程式以 Light Agent 模式使用，則不支援圖形介面）：
  - 現在，您可以啟用或停用Web 控制元件。
  - 我們重新設計了圖形介面的風格（新顏色、所有視窗的圓角）。
- 變更了檔案威脅防護設定和掃描工作中可套用於感染物件的操作名稱。
- 新增了在 64 位元作業系統（內核版本 5.3 或更高版本，具有 eBPF 支援）上在行為偵測元件中取得系統遙測的替代機制，這可以釋放 auditd 內核稽核子系統的資源。如果作業系統符合需求，應用程式在 Light Agent 模式下也會自動使用 eBPF。
- 所有應用程式管理介面（命令列介面除外）的日期時間均以符合 RFC 3339 的統一格式顯示，例如 2023-12-25 23:55:59。
- 我們更新了支援的作業系統清單。

版本 12.2

Kaspersky Embedded Systems Security 12.2 for Linux 現在具備以下新功能和改進：

- 新增支援與 Kaspersky Network Detection and Response (KATA) 整合，這是 Kaspersky Anti Targeted Attack Platform 解決方案的元件，可保護企業內部網路，並允許將裝置上發生事件的相關資訊（遙測資料）傳送至具有中央節點元件的 Kaspersky Anti Targeted Attack Platform 伺服器（以下亦稱為 NDR 伺服器）。
- 新增支援與 KATA Sandbox 整合，這是 Kaspersky Anti Targeted Attack Platform 解決方案的元件，可讓您使用已部署作業系統虛擬映像的特殊伺服器，分析和掃描物件以偵測惡意活動和企業 IT 基礎架構所遭受目標式攻擊的指標。
- 新增支援與 Kaspersky Unified Monitoring and Analysis Platform 整合，這是一套全方位軟體解決方案，結合以下功能：接收、處理和儲存資訊安全事件；分析和關聯傳入資料；搜尋已接收的事件，以及建立關於偵測到資訊安全威脅指標的通知。
- 已擴充與 Kaspersky Endpoint Detection and Response (KATA) 整合的功能，Kaspersky Endpoint Detection and Response (KATA) 是 Kaspersky Anti Targeted Attack Platform 解決方案的元件：
  - 新的物件執行防禦功能。
  - 新的檔案隔離功能。
  - 已擴充裝置上事件（遙測資料）的相關資訊。
- 已擴充Endpoint Detection and Response Optimum 整合功能：
  - 新的物件執行防禦功能。
  - 新的檔案隔離功能。
  - 現在，您可以依處理程序名稱，將處理程序從網路隔離中排除。
- 現在，您可以使用 Cloud Sandbox 技術，該技術可偵測裝置上的複雜威脅。Kaspersky Endpoint Security 應用程式會自動將偵測到的檔案傳送到 Cloud Sandbox 進行分析。Cloud Sandbox 在隔離環境中執行這些檔案以偵測惡意活動並確定這些檔案的信譽。

- 現在，您可以檢視最常掃描的檔案和應用程式的統計資料，以及受防護裝置上偵測到的掛載點清單。為了提高效能，現在您可以排除檔案威脅防護元件最常掃描的檔案、行為偵測元件最常掃描的應用程式路徑，以及裝置上偵測到的掛載點。

- 現在，您可以收集應用程式效能指標，這些指標可協助分析 Kaspersky Endpoint Security 對作業系統效能的影響。

- 已改進防火牆管理元件。現在，您可以為網路封包規則指定多個 IP 位址或 IP 位址範圍。

- 新的作業系統凍結追蹤機制。此機制會檢查部分系統函數是否凍結，其中一個函數是 execve 函數。每隔三秒，wdserver Watchdog 伺服器處理程序會啟動另一個 wdserver 處理程序，並在其中呼叫這些系統函數（execve 函數呼叫會啟動至少一個額外的 wdserver 處理程序）。如果 wdserver 偵測到沒有回應的系統功能，Watchdog 伺服器過載會重新啟動 kesl 處理程序。

- 現在，您可以在管理應用程式的圖形使用者介面時，設定快顯通知的顯示。現在，您可以使用網頁主控台、管理主控台或指令列，在 GUI 中啟用或停用快顯通知的顯示。

- 已改進指令列的工作排程選項。現在，您可以設定工作在達到允許的最長執行時間時停止。

- 已變更建立卡巴斯基安全管理中心政策設定檔時「掛鎖」屬性的狀態。現在，建立設定檔時，所有「掛鎖」預設均為開啟狀態，這表示預設情況下，設定檔設定不會覆寫「基本」政策的設定。

- 新增了在 64 位元作業系統（核心版本 5.3 或更高版本，且具有支援 BTF 的 eBPF）上取得系統遙測資料的替代機制，這可釋放 auditd 核心稽核子系統的資源。如果作業系統符合指定要求，應用程式將自動使用 eBPF 運作。

- 所有管理外掛程式中的日期和時間均以符合 RFC 3339 的統一格式顯示，例如 2023-12-25 23:55:59。

- 我們更新了支援的作業系統清單。

版本 12.1

Kaspersky Embedded Systems Security 12.1 for Linux 現在具備以下新功能和改進：

- 現在，您可以設定與 Kaspersky Endpoint Detection and Response Optimum 整合，此功能可保護組織的 IT 基礎設施免受漏洞利用、勒索軟體、無檔案攻擊，以及攻擊者使用合法系統工具損害裝置或資料等威脅。

- 現在，您可以為應用程式新增兩個作用中產品授權金鑰：用於啟動應用程式的主金鑰，以及用於啟動 Kaspersky Endpoint Detection and Response Optimum 功能的額外金鑰。如果您的主產品授權不包含 Kaspersky Endpoint Detection and Response Optimum 功能，則需要額外金鑰。

- 新增了新的 *Web 控制* 元件，此元件可控制使用者對 Web 資源的存取。這可讓您減少流量消耗，並減少工作時間的不當使用。如果使用者嘗試開啟受 Web 控制限制存取的網站，Kaspersky Endpoint Security 會阻止存取或顯示警告。

- 新增的 Kaspersky Endpoint Security 穩定性監控功能可讓您追蹤應用程式異常終止的次數，並將應用程式運作不穩定的情況通知管理員。

- 改善了使用卡巴斯基安全管理中心網頁主控台安裝 Kaspersky Endpoint Security 的程序：在應用程式安裝套件的內容中，您現在可以指定初始組態設定，這些設定先前僅可在 autoinstall.ini 設定檔中使用。

- 現在，您可以使用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管理主控台指定更多應用程式設定：您可以編輯先前只能透過編輯 kesl.ini 設定檔來設定的設定。

- 現在，您可以在執行掃描工作時啟用或停用全域排除項目和檔案威脅防護排除項目。

- 現在，您可以設定與 Kaspersky Symphony XDR 的整合：如果 Kaspersky Endpoint Security 應用程式以標準模式使用，該應用程式可以執行「開始惡意軟體掃描」和「資料庫更新」回應動作。
- 現在，當使用卡巴斯基安全管理中心管理應用程式時，您可以將安裝在用戶端裝置上或連線到用戶端裝置的所有裝置（包括先前已安裝和連線但目前已中斷連線的裝置）的相關資訊傳送到管理伺服器。
- 已改進流量攔截規則，以支援同一網路上容器之間的互動。
- 我們更新了支援的作業系統清單。

已修正的問題

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

12.5 版本中修正的問題清單

識別碼	描述
10306343	檢查目前產品授權金鑰的狀態時，錯誤產生了關於移除和安裝產品授權金鑰的通知。
10295949	目前政策設定檔中為裝置控制元件指定的設定未套用。因此，該元件繼續使用政策中指定的設定運作。
10171454	如果設定中指定的第一個更新來源無法使用，則會錯誤顯示更新問題訊息。
10109293	如果選取了 iptables 網路流量攔截模式 (`NetInterceptorMode=UseIPTables`)，則開啟繫結至特定網路介面的網路通訊端之應用程式流量會被錯誤處理。
10024219	卡巴斯基安全管理中心管理主控台錯誤顯示受管理裝置上可更新的內核模組狀態。
9995631	應用程式對常駐 RAM 使用量的限制（`MaxMemory` 設定）在沒有交換分割區的系統上無法正常運作。現在，當達到設定的限制時，Kaspersky Endpoint Security 會重新啟動。
9937329	在已停用裝置控制 (Device_Control) 工作的系統上，錯誤產生了 *裝置已連線* 和 *裝置已斷開連線*。
9934846	在高負載系統上，應用程式無法啟動。應用程式連線至 Watchdog 伺服器的逾時時間已延長。
9846405	在已設定 EFI 開機載入器的系統上，錯誤產生了 *物件未處理* 事件。
9815051	在受管理裝置上以 eBPF 網路流量攔截模式 (`NetInterceptorMode=UseEBPF`) 執行 Web 威脅防護 (Web_Threat_Protection) 和網路威脅防護 (Network_Threat_Protection) 工作時，先前建立的網路連線可能會停止回應。現在，當嘗試傳輸資料時，這類連線會被終止。
9807202	在某些 ROSA 作業系統上，使用 mkfs.ext2 公用程式進行安裝時遇到問題。
9704644	以 EDR 代理程式模式使用應用程式時，裝置狀態顯示不正確。已變更以 EDR 代理程式模式使用應用程式時的裝置防護狀態值。
9643969	在某些情況下，於 eBPF 模式使用網路流量攔截時，Scylla 主機之間可能會發生網路連線問題。
9633030	在政策中清除 **啟用物件執行防禦** 核取方塊時，物件執行防禦 (EDR Expert (on-premises)) 工作仍會執行。
9627894	在停用 IPv6 的作業系統上，以 eBPF 技術為基礎的網路流量攔截模式無法正常運作。
9606448	使用卡巴斯基安全管理中心管理伺服器作為存取卡巴斯基啟動伺服器的代理伺服器來啟動應用程式時發生問題（在政策中選取 **使用卡巴斯基安全管理中心作為啟動代理伺服器** 核取方塊時）。
9508605	啟用 Kaspersky Endpoint Detection and Response Expert 整合時，在具有容器環境的系統上，應用程式會使用大量記憶體。
9456741	由於在攔截新程序啟動時無法判斷檔案直譯器，應用程式當機。

Web 外掛程式 6.1 版中修正的問題清單

識別碼	描述
9558745	用於設定 Kaspersky Endpoint Security 圖形介面中通知顯示的 **在圖形使用者介面中顯示快顯通知** 設定未顯示在政策內容中 (**應用程式設定 → 一般設定 → 事件設定 → 進階設定**)。
9622658	透過物件雜湊值新增惡意軟體掃描排除項目時，這些排除項目未儲存。
9798821	將單一網站新增至 Web 控制規則時，政策變更未儲存。
9990129	在新增受信任應用程式的表單中，顯示了不相關的 **註解** 欄位。
9977884	在郵件威脅防護元件的設定中，顯示了不相關的 **安全等級** 切換開關。
9944635	**掃描郵件資料庫** 旗標的名稱重複顯示。現在顯示正確的名稱：**掃描郵件資料庫** 和 **掃描電子郵件格式檔案**。
10010439	建立 Web 控制規則時，未正確新增從 Active Directory 清單指派給該規則的使用者。
10218308	變更政策設定時，卡巴斯基安全網路模式已重設。

硬體和軟體需求

最小硬體條件

若要安裝應用程式

- 採用 AMD64 架構、2 GHz 或更高、兩個或多個核心並支援 SSE2 指令集的 CPU。
- 交換空間至少 1 GB
- RAM:
  - 64 位元作業系統：可供應用程式使用的 RAM 為 2 GB
  - 32 位元作業系統：可供應用程式使用的 RAM 為 1 GB
- 4 GB 可用硬碟空間用於安裝應用程式以及儲存臨時檔案和記錄檔案

  需要額外的磁碟空間來儲存偵錯檔案和應用程式記憶體傾印檔案。

  當使用 `ScanArchived=Yes` 和或 `ScanSfxArchived=Yes` 掃描壓縮檔案和複合物件時（預設情況下，對於掃描工作設定為 `Yes`，對於檔案威脅防護設定為 `No`），檔案威脅防護和掃描工作需要額外的磁碟空間，取決於此類物件的類型和解壓大小。

  我們建議確保 /tmp 目錄中有足夠的可用空間來掃描壓縮檔案和複合物件。您也可以透過為每個工作指定 `SizeLimit` 來限制可掃描的檔案的大小（處於存檔狀態）。

若要安裝圖形使用者介面

- 能夠顯示寬 1000 像素、高 600 像素視窗的顯示器。如果套用螢幕縮放，這些尺寸也會隨之縮放。

Arm 架構的最低硬體需求

若要安裝應用程式

- Armv8.2-A Kunpeng 920 或 Armv8-A Baikal-M (BE-M1000) CPU 或 m-TrusT 終端平台
- 交換分區至少 1 GB
- 應用程式可使用 2 GB 的 RAM。
- 3 GB 可用硬碟空間用於安裝應用程式以及儲存臨時檔案和記錄檔案

  需要額外的磁碟空間來儲存偵錯檔案和應用程式記憶體傾印檔案。

  當使用 `ScanArchived=Yes` 和或 `ScanSfxArchived=Yes` 掃描壓縮檔案和複合物件時（預設情況下，對於掃描工作設定為 `Yes`，對於檔案威脅防護設定為 `No`），檔案威脅防護和掃描工作需要額外的磁碟空間，取決於此類物件的類型和解壓大小。

  我們建議確保 /tmp 目錄中有足夠的可用空間來掃描壓縮檔案和複合物件。您也可以透過為每個工作指定 `SizeLimit` 來限制可掃描的檔案的大小（處於存檔狀態）。

若要安裝圖形使用者介面

- 能夠顯示寬 1000 像素、高 600 像素視窗的顯示器。如果套用螢幕縮放，這些尺寸也會隨之縮放。

Elbrus (E2K) 架構的最低硬體需求

若要安裝應用程式

- CPU v3：Elbrus-4S；v4：Elbrus-8S 或 Elbrus-1S+
- 交換分區至少 2 GB
- 應用程式可使用 2 GB 的 RAM。
- 2 GB 可用硬碟空間用於安裝應用程式以及儲存臨時檔案和記錄檔案

若要安裝圖形使用者介面

- 能夠顯示寬 1000 像素、高 600 像素視窗的顯示器。如果套用螢幕縮放，這些尺寸也會隨之縮放。

軟體要求

若要安裝 Kaspersky Endpoint Security，裝置上必須安裝表格中列出的其中一種作業系統：

本文列出應用程式經過測試並保證能夠正常運作的軟體版本。應用程式也可能與其他軟體版本搭配使用，但這些組態尚未經過完整的測試週期，且未包含在保證支援版本清單中。

由於 fanotify 的技術限制，應用程式不支援下列檔案系統：autofs、binfmt_misc、cgroup、configfs、debugfs、devpts、devtmpfs、gfs2、gvfs、hugetlbfs、mqueue、nfsd、proc、parsecfs、pipefs、pstore、usbfs、rpc_pipefs、securityfs、selinuxfs、sysfs、tracefs。

若未由作業系統管理員完成其他步驟，則透過 FUSE 技術對掛載點執行的檔案威脅防護會受到限制。您可以將 user_allow_other 設定新增至 /etc/fuse.conf 檔案，並為每個掛載點新增 allow_root 掛載選項，讓應用程式能夠監控這些掛載點的檔案事件。

64 位元作業系統	適用於 Arm 架構的 64 位元作業系統	適用於 Elbrus (E2K) 架構的 64 位元作業系統	32 位元作業系統
• AlmaLinux OS 8.6、8.7、8.8、8.9。 • AlmaLinux OS 9.4、9.5、9.6。 • AlterOS® 2025。 • Amazon™ Linux 2023。 • Astra Linux Common Edition 2.12。 • Astra Linux Special Edition RUSB.10015-01（作業更新 1.5、1.6、1.7、1.8）。 • Astra Linux Special Edition RUSB.10015-03 (operational update 7.6)。 • Astra Linux Special Edition RUSB.10015-16 (release 1) (operational update 1.6)。 • Astra Linux Special Edition RUSB.10015-17 (operational update 1.7.3)。 • Astra Linux Special Edition RUSB.10015-37 (operational update 7.7)。 「Mobile」模式下的 Astra Linux 作業系統僅支援桌面模式。 • CentOS 5.2、5.4、6.4、6.6、7.2、7.3、7.4、7.5、7.6、7.7、7.8、7.9。 在 Kaspersky Endpoint Security Cloud 解決方案中，應用程式不支援在 CentOS 5.2、5.4、6.4、6.6 裝置上執行。 在卡巴斯基安全管理中心雲端主控台中，應用程式不支援在 CentOS 5.2、5.4、6.4、6.6 裝置上執行。 • CentOS Stream 8、9、10。 • Debian GNU/Linux 12.8、12.9、12.10、12.11、12.12、12.13。 • Debian GNU/Linux 13.1、13.2、13.3。 • EMIAS 1.0。 • EulerOS 2.0 SP10。 • Fedora Linux 41。 • Kylin Desktop OS V10 SP1。 • Linux Mint 21.3。 • Linux Mint 22.2。 • Mostech 12 版本 2021.1。 • openSUSE Leap 15.6。 • Oracle Linux 7.3、7.4、7.5、7.6、7.7、7.8、7.9。 • Oracle Linux 8.5、8.6、8.7、8.8、8.9。 • Oracle Linux 9.4、9.5、9.6。 • Red Hat Enterprise Linux 7.2、7.3、7.4、7.5、7.6、7.7、7.8、7.9。 • Red Hat Enterprise Linux 8.5、8.6、8.7、8.8、8.9、8.10。 • Red Hat Enterprise Linux 9.4、9.5、9.6。 • Red Hat Enterprise Linux 10.0、10.1。 • Rocky Linux 8.6、8.7、8.8、8.9。 • Rocky Linux 9.4、9.5、9.6。 • SberLinux 8.10、9.1、9.5、9.6、9.7。 • SberOS 3.4.0、3.5.0、3.6.1。 • SUSE Linux Enterprise Server 12.5、12.6、12.7。 • SUSE Linux Enterprise Server 15.4、15.5、15.6、15.7。 • Ubuntu® 24.04 LTS。 • Ubuntu 26.04 LTS。 • ALT Education 10、11。 • ALT Workstation 11。 • ALT Server 11。 • ALT SP Workstation 版本 10。 • ALT SP Server 版本 10。	• Astra Linux Special Edition RUSB.10152-02 (operational update 4.7)。 • CentOS Stream 9。 • EulerOS 2.0 SP10。 • SUSE Linux Enterprise Server 15.4、15.5、15.6、15.7。 • Ubuntu 26.04 LTS。 • ALT Workstation 11.2。 • ALT Server 11.1。 • ALT SP Workstation 版本 10。 • ALT SP Server 版本 10。 • RED OS 8.0。	• OS Elbrus 9.3.6。 • Astra Linux Special Edition RUSB.10015-16 (release 2) (operational update 8.1)。 • Astra Linux Special Edition RUSB.10265-01 (operational update 8.1)。 • ALT SP Workstation 版本 8、10。 • ALT SP Server 版本 8、10。	• Debian GNU/Linux 12.8、12.9、12.10、12.11、12.12、12.13。

64 位元作業系統	適用於 Arm 架構的 64 位元作業系統	適用於 Elbrus (E2K) 架構的 64 位元作業系統	32 位元作業系統
• Atlant，Alcyone 內建版本，版本 2022.02。 • GosLinux 7.2。 • M OS 12 伺服器版本 2021.1。 • Mos OS 15.5 Arbat。 • MSVSphere 9.5 工作站。 • MSVSphere 9.5 伺服器。 • MES OS 12 Panel 版本 2025。 • MES OS 12 Desktop 版本 2025。 • OSnova 3.1。 • RED OS® 7.3。 • RED OS 8.0。 • ROSA "Cobalt" 7.9 Workstation。 • ROSA "Cobalt" 7.9 Server。 • ROSA "Chrome" 12 Workstation。 • ROSA "Chrome" 12 Server。 • SintezM-Client 8.6。 • SintezM-Server 8.6。			

Light Agent 模式的附加軟體和硬體要求

Kaspersky Endpoint Security 可以作為Kaspersky Security for Virtualization Light Agent 6.5的一部分用作 Light Agent。您可以在Kaspersky Security for Virtualization Light Agent 說明中檢視應用程式在 Light Agent 模式下的虛擬基礎架構要求 。

虛擬機

Kaspersky Endpoint Security 的軟體和硬體要求適用於以 Light Agent 模式執行 Kaspersky Endpoint Security 的虛擬機，但有以下限制：

- 必須具備頻寬為 100 Mbps 的虛擬化網路介面
- Arm 裝置不支援 Light Agent 模式的 Kaspersky Endpoint Security。
- Astra Linux Special Edition 作業系統在強制存取控制模式和封閉軟體環境模式下不支援 Light Agent 模式的應用程式。

虛擬機上的 BIOS 必須支援 SMBIOS 規範版本 2.1 或更新版本。

根據您的虛擬基礎架構，虛擬機必須安裝以下項目：

- 在 Microsoft Hyper-V 基礎架構中，必須安裝 Integration Services 套件。
- 在 VMware vSphere 基礎架構中，必須安裝 VMware Tools 套件。
- 在 XenServer 基礎架構中，必須安裝 XenTools 軟體。
- 在 HUAWEI FusionSphere 基礎架構中，必須安裝 HUAWEI Tools 套件。
- 在 KVM（核心型虛擬機）基礎架構中，必須安裝 QEMU Guest Agent。

受支援的終端伺服器類型

- Astra Linux 3.0.5 終端伺服器。

分發套件

Kaspersky Endpoint Security 分發套件包含以下檔案：

主要應用程式檔案

- 適用於 32 位元作業系統的處理器：

  `kesl-12.5.0-<build number>.i386.rpm`

  `kesl_12.5.0-<build number>_i386.deb`

- 適用於 64 位元作業系統的處理器：

  `kesl-12.5.0-<build number>.x86_64.rpm`

  `kesl_12.5.0-<build number>_amd64.deb`

- 適用於 Arm® 處理器、64 位元作業系統：

  `kesl-12.5.0-<build number>.aarch64.rpm`

  `kesl_12.5.0-<build number>_arm64.deb`

- 適用於 Elbrus CPU：

  `kesl-12.5.0-<build number>.e2k.rpm`

  `kesl_12.5.0-<build number>_e2k.deb`

應用程式的圖形介面

- 適用於 32 位元作業系統的處理器：

  `kesl-gui-12.5.0-<build number>.i386.rpm`

  `kesl-gui_12.5.0-<build number>_i386.deb`

- 適用於 64 位元作業系統的處理器：

  `kesl-gui-12.5.0-<build number>.x86_64.rpm`

  `kesl-gui_12.5.0-<build number>_amd64.deb`

- 適用於 Arm® 處理器、64 位元作業系統：

  `kesl-gui-12.5.0-<build number>.aarch64.rpm`

  `kesl-gui_12.5.0-<build number>_arm64.deb`

- 適用於 Elbrus CPU：

  `kesl-gui-12.5.0-<build number>.e2k.rpm`

  `kesl-gui_12.5.0-<build number>_e2k.deb`

若要在支援受限的作業系統（CentOS 5.2、CentOS 5.4、CentOS 6.4、CentOS 6.6）上安裝 Kaspersky Endpoint Security 應用程式，請選取標示為 OLD 的發佈套件。

使用卡巴斯基安全管理中心遠端安裝應用程式的封存檔

`kesl-12.5.0.<build number>.zip`

此封存檔還包含使用者協議的文字。

使用者協議的文字

- `ksn_license.<language ID>` 包含 卡巴斯基安全網路 聲明的文字。
- `license.<language ID>` 包含最終使用者產品授權協議的文字。最終使用者產品授權協議指定了使用應用程式的條款。

卡巴斯基安全管理中心網路代理不包含在分發套件中。您可以在的卡巴斯基安全管理中心部分的**應用程式下載頁面**中下載它。

與其他應用程式的相容性

支援的卡巴斯基安全管理中心版本

依據 Kaspersky Endpoint Security 的 模式，您可以使用表格中列出的卡巴斯基安全管理中心版本來管理應用程式。

模式	卡巴斯基安全管理中心版本
標準模式下的 Kaspersky Endpoint Security	卡巴斯基安全管理中心 Windows 14.2、15.1。 透過管理主控台使用 MMC 管理外掛程式，以及透過卡巴斯基安全管理中心網頁主控台使用 Web 管理外掛程式進行管理。 卡巴斯基安全管理中心 Linux 15.1、15.2、15.3、15.4、16.0、16.1、16.2、16.3。 透過卡巴斯基安全管理中心網頁主控台使用 Web 管理外掛程式進行管理。
含有 Endpoint Detection and Response Optimum 元件之標準模式下的 Kaspersky Endpoint Security	卡巴斯基安全管理中心 Windows 15.1。 卡巴斯基安全管理中心 Linux 15.3、15.4、16.0、16.1、16.2。
Light Agent 模式下的 Kaspersky Endpoint Security	卡巴斯基安全管理中心 Windows 15.1。 卡巴斯基安全管理中心 Linux 16.1、16.2、16.3。
EDR Agent 模式下的 Kaspersky Endpoint Security	卡巴斯基安全管理中心 Windows 14.2、15.1。 卡巴斯基安全管理中心 Linux 15.3、15.4、16.0、16.1、16.2、16.3。

Kaspersky Security for Virtualization Light Agent 的支援版本

Kaspersky Endpoint Security 可以作為Kaspersky Security for Virtualization Light Agent 6.5的一部分用作 Light Agent。

KATA 和 OSMP 平台上支援的解決方案版本

Kaspersky Endpoint Security 與下列版本的 以 Kaspersky Anti Targeted Attack Platform 為基礎的解決方案以及 Kaspersky Endpoint Detection and Response Expert (on-premises) 解決方案相容：

- Kaspersky Anti Targeted Attack Platform 6.0、6.1、7.0、7.1（Kaspersky Endpoint Detection and Response (KATA)、Kaspersky Network Detection and Response (KATA)，包括將檔案傳送到沙盒進行掃描的情境）。
- Kaspersky Anti Targeted Attack Platform 8.0（Kaspersky Network Detection and Response (KATA)，包括將檔案傳送到沙盒進行掃描的情境）。

  關於 Kaspersky Anti Targeted Attack Platform 解決方案的更多詳細資訊，請參閱Kaspersky Anti Targeted Attack Platform 說明。
- Open Single Management Platform（以下亦稱 OSMP）上的 Kaspersky Endpoint Detection and Response Expert (on-premises) 8.0、8.1，包括將檔案傳送到沙盒進行掃描的情境。

  如需 Kaspersky Endpoint Detection and Response Expert (on-premises) 的詳細資訊，請參閱 Kaspersky Endpoint Detection and Response Expert (on premise) 說明。

支援與 Kaspersky Endpoint Detection and Response Expert (cloud) 整合的網路代理版本

若要將應用程式與 Kaspersky Endpoint Detection and Response Expert (cloud) 整合，您需要特定版本的卡巴斯基安全管理中心雲端主控台網路代理，這些版本已在 卡巴斯基安全管理中心雲端主控台說明 中說明。

與協力廠商解決方案的相容性

EDR Agent 模式下的 Kaspersky Endpoint Security 可以與 Dr. Web 病毒防護應用程式協同工作。

卡巴斯基解決方案之間的功能比較

Kaspersky Endpoint Security 包含在許多卡巴斯基多平台解決方案中。可用的應用程式功能取決於您從所在地區的服務供應商購買的解決方案。

功能	Kaspersky Next EDR Foundations	Kaspersky Next EDR Optimum	Kaspersky Next XDR Optimum	Kaspersky Next MXDR Optimum	Kaspersky Next EDR Expert	Kaspersky Next XDR Expert	Kaspersky Hybrid Cloud Security，桌面	Kaspersky Hybrid Cloud Security Enterprise 桌面/CPU/伺服器	Kaspersky Hybrid Cloud Security 核心/CPU/伺服器
檔案威脅防護	✓	✓	✓	✓	✓	✓	✓	✓	✓
郵件威脅防護	✓	✓	✓	✓	✓	✓	✓	✓	✓
Web 威脅防護	✓	✓	✓	✓	✓	✓	✓	✓	✓

網路威脅防護	✓	✓	✓	✓	✓	✓	✓	✓	✓
防火牆管理	✓	✓	✓	✓	✓	✓	✓	✓	✓
行為偵測	✓	✓	✓	✓	✓	✓	✓	✓	✓
BadUSB 攻擊防護	–	✓	✓	✓	✓	✓	✓	✓	✓
裝置控制	✓	✓	✓	✓	✓	✓	✓	✓	✓
卸除式磁碟機掃描	✓	✓	✓	✓	✓	✓	✓	✓	✓
加密軟體防護（用於共用資料夾）	✓	✓	✓	–	✓	✓	–	✓	✓
容器掃描	–	–	–	–	–	✓	–	✓	–
應用程式控制	✓	✓	✓	✓	✓	✓	✓	✓	–
Web 控制	✓	✓	✓	✓	✓	✓	✓	✓	✓
與卡巴斯基統一監控和分析平台整合	–	–	–	–	–	✓	–	–	–
與 Kaspersky Endpoint Detection and Response Expert (cloud) 整合	–	–	–	–	✓	✓	–	–	–
與 Kaspersky Endpoint Detection and Response Expert (on-premises) 整合	–	–	–	–	✓	✓	–	–	–
Kaspersky Endpoint Detection and Response Optimum	✓	✓	✓	✓	–	–	–	–	–
與 Kaspersky Managed Detection and Response 整合	–	–	–	✓	–	–	–	–	–

部署與初始設定

您可以依照此案例部署 Kaspersky Endpoint Security 應用程式，並準備好供使用。

1 選擇應用程式使用模式

在您於 卡巴斯基官方網站 或透過我們的合作夥伴購買卡巴斯基解決方案後，您將在購買時指定的電子郵件地址收到一封郵件。此郵件將包含啟動碼，以及如何取得金鑰檔案的資訊。如果您的組織不支援使用代碼線上啟動應用程式，您可能需要金鑰檔案。

您選擇的 解決方案 會決定您可以使用應用程式的模式：

- 如果您擁有 Kaspersky Endpoint Security 產品授權，可以在標準模式下使用應用程式。
- 如果您擁有 Kaspersky Security for Virtualization Light Agent 產品授權，可以在 Light Agent 模式下使用應用程式。
- 如果您擁有 Kaspersky Endpoint Detection and Response Expert (on-premises) 產品授權，可以在 EDR 代理程式模式下使用應用程式。

應用程式部署取決於所選模式。

安裝 Kaspersky Endpoint Security 後，您無法變更應用程式使用模式。

2 準備環境

請根據您的基礎架構完成必要的準備動作。

3 選擇系統事件攔截機制

如果您裝置的作業系統支援 fanotify，您可以在安裝期間選擇用於攔截系統事件的機制。

4 準備發佈套件

下載安裝應用程式所需的檔案。您需要哪些檔案取決於受防護裝置的作業系統和應用程式部署方法。

5 卡巴斯基安全管理中心中的準備動作

在卡巴斯基安全管理中心中執行準備動作。我們建議使用卡巴斯基安全管理中心集中管理貴組織的防護。如果您將在 EDR 代理程式模式或 Light Agent 模式下使用 Kaspersky Endpoint Security，也需要卡巴斯基安全管理中心。

6 安裝應用程式

使用符合貴組織需求的方法在裝置上安裝應用程式：

- 使用卡巴斯基安全管理中心安裝應用程式
- 使用指令列安裝應用程式

7 在某些作業系統中安裝後的額外設定步驟

某些 Linux 作業系統在安裝 Kaspersky Endpoint Security 後需要額外設定。

模式和部署方案

Kaspersky Endpoint Security 是許多卡巴斯基解決方案的一部分。您選擇的解決方案會決定應用程式的運作模式和部署方案。

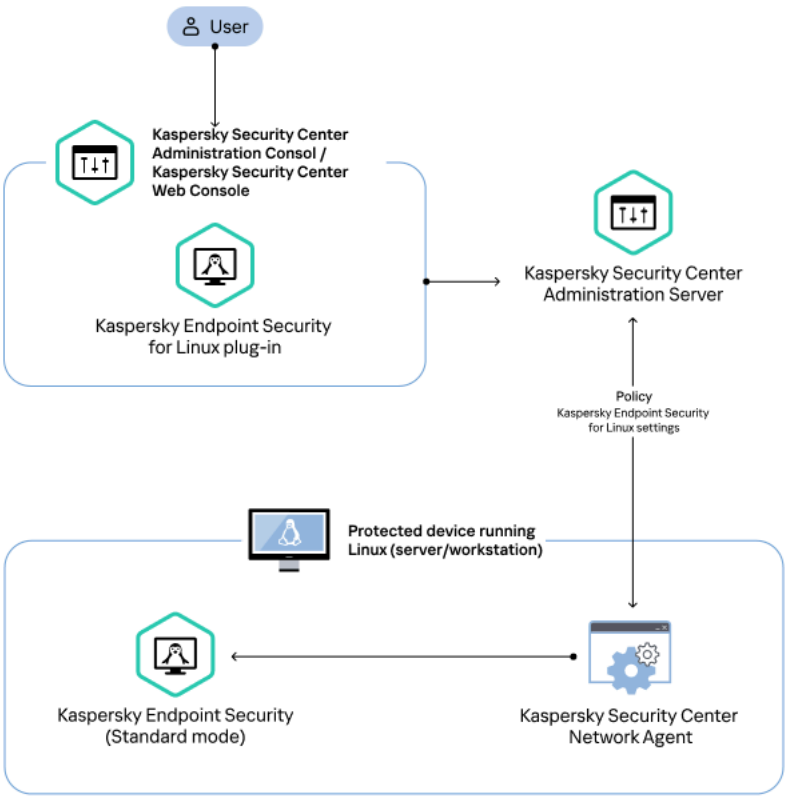
標準模式

應用程式的預設模式。Kaspersky Endpoint Security 為 Linux 工作站和伺服器提供針對各種類型威脅、網路攻擊和詐騙的全面防護。

在此模式下，應用程式會使用裝置防護和控制元件，例如 檔案威脅防護 或 行為偵測，以及 內建代理，以防範進階威脅和針對性攻擊。

您可以在此模式下將應用程式作為 Kaspersky EPP（Endpoint Protection Platform）解決方案的一部分進行安裝。例如，標準模式下的 Kaspersky Endpoint Security 是 Kaspersky Endpoint Security for Business 的一部分。

Kaspersky Endpoint Security 的主要部署方案是 透過卡巴斯基安全管理中心集中部署。在每台受防護裝置上，您需要安裝 Kaspersky Endpoint Security 和卡巴斯基安全管理中心網路代理元件。此元件會將裝置連線至卡巴斯基安全管理中心管理伺服器，並可使用卡巴斯基安全管理中心管理裝置。



Kaspersky Endpoint Security 在標準模式下的部署方案

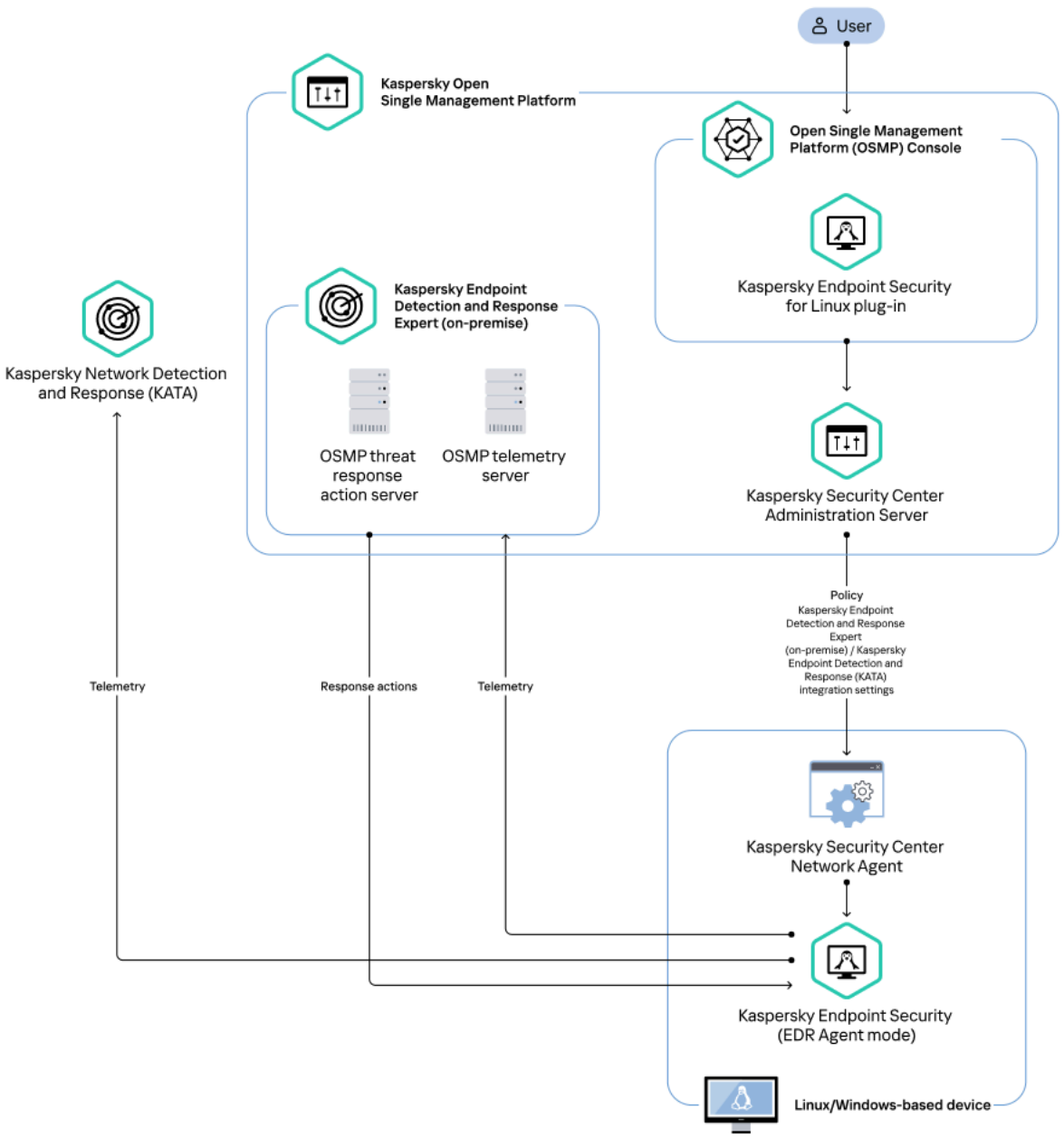
Endpoint Detection and Response Agent (EDR Agent) 模式

此模式可將卡巴斯基 Detection and Response 解決方案與協力廠商病毒防護解決方案一起部署。Detection and Response 解決方案包括：

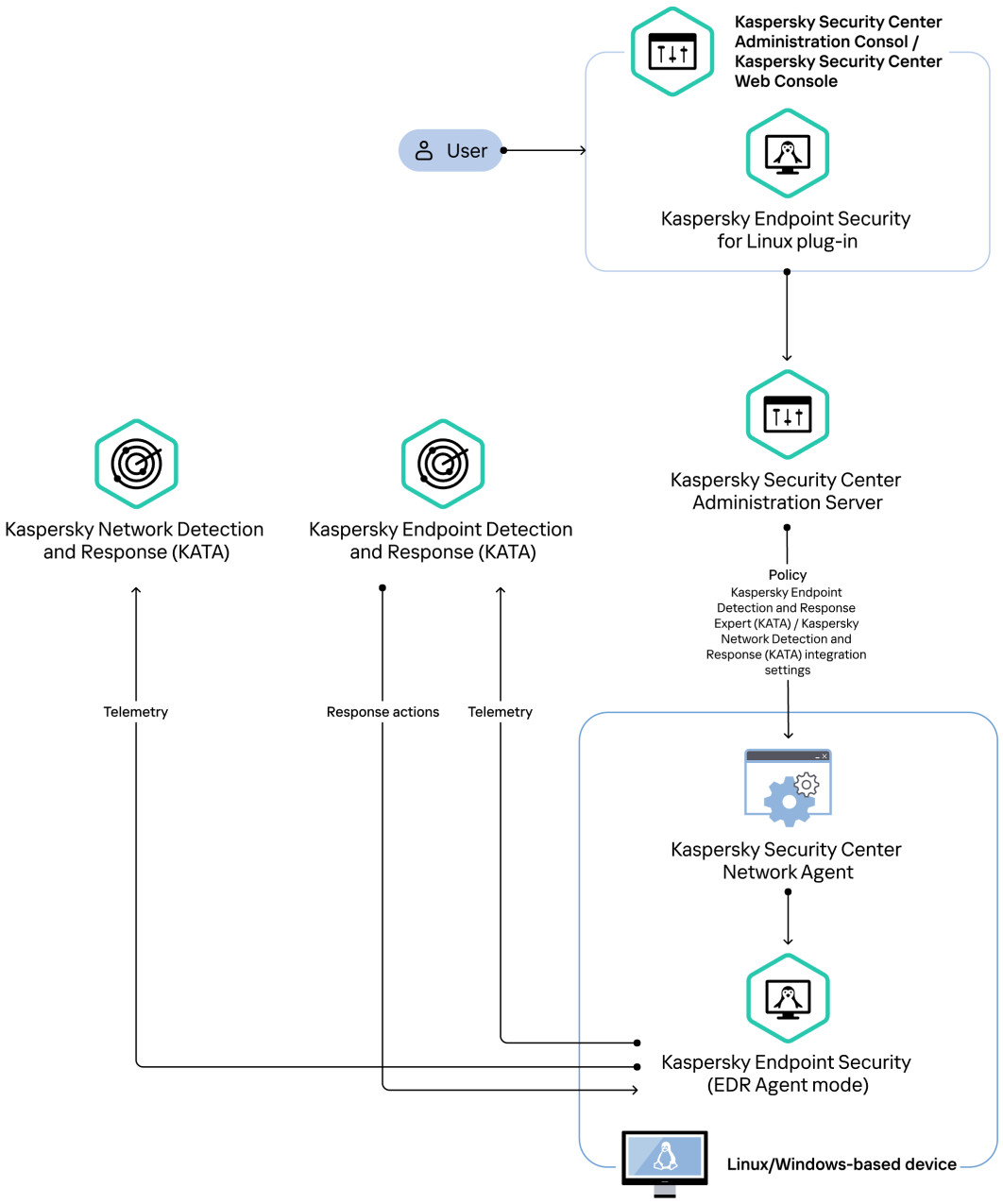
- 於開放式單一管理平台上的 Kaspersky Endpoint Detection and Response Expert (on-premises)（以下也稱為 "OSMP"）。
- 於 Kaspersky Anti Targeted Attack Platform 上的 Kaspersky Endpoint Detection and Response 和 Kaspersky Network Detection and Response（以下也稱為 "KATA"）。

在 EDR Agent 模式下，檔案威脅防護或 Web 威脅防護等防護和控制元件無法使用。裝置由協力廠商病毒防護應用程式進行防護。EDR 代理會持續監控這些裝置上執行的處理程序、正在開啟的網路連線和正在修改的檔案，並與 Detection and Response 解決方案互動，以防範進階威脅和針對性攻擊。

若要讓 Kaspersky Endpoint Security 在 EDR Agent 模式下運作，您必須部署適當的基礎架構；如需更多資訊，請參閱您所選 Detection and Response 解決方案的說明章節。若要深入瞭解 EDR Agent 模式的特殊方面，請參閱已知問題和限制一文。



Kaspersky Endpoint Security 在 EDR Agent 模式下與 Kaspersky Endpoint Detection and Response Expert (on-premises) 搭配使用的部署方案



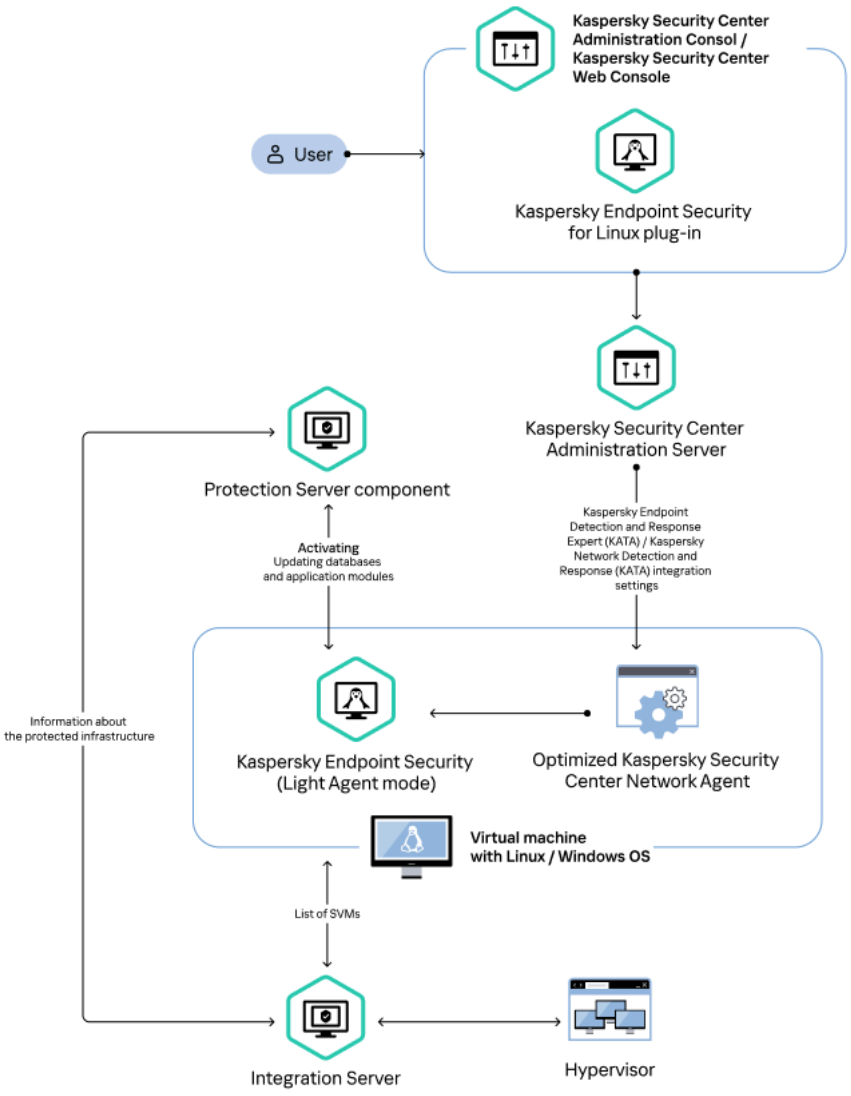
Kaspersky Endpoint Security 在 EDR Agent 模式下與 Kaspersky Endpoint Detection and Response 和 Kaspersky Network Detection and Response 搭配使用的部署方案

Light Agent 模式

Light Agent 模式下的 Kaspersky Endpoint Security 是 Kaspersky Security for Virtualization Light Agent 解決方案的一部分，用於防護執行 Linux 來賓作業系統的虛擬機。

此模式下提供與標準模式相同的防護和控制元件。不同之處在於，物件的病毒和其他惡意軟體掃描、產品授權金鑰新增，以及資料庫和模組更新，均由安裝在獨立虛擬機 SVM (Secure Virtual Machine) 上的特殊解決方案元件執行。這有助於減輕 Hypervisor 的負擔，因為 Light Agent 模式下的應用程式會使用 SVM 的資源來防護基礎架構，而不是使用虛擬機的資源。

若要讓 Kaspersky Endpoint Security 在 Light Agent 模式下運作，您必須部署適當的基礎架構；如需更多資訊，請參閱 Kaspersky Security for Virtualization Light Agent 說明。若要深入瞭解 Light Agent 模式的特殊方面，請參閱 已知問題和限制 一文。



Kaspersky Endpoint Security 在 Light Agent 模式下的部署方案

選擇應用程式模式後，您可以返回部署情境，並從 準備環境 步驟繼續。

準備應用程式安裝環境

準備基礎架構

卡巴斯基安全管理中心

如果您打算使用卡巴斯基安全管理中心集中管理應用程式，請在您的基礎架構中安裝卡巴斯基安全管理中心。如果您已安裝卡巴斯基安全管理中心 Windows，並計劃移轉到卡巴斯基安全管理中心 Linux，請依照以下說明操作：將資料移轉到卡巴斯基安全管理中心 Linux。

EDR Agent 模式下的 Kaspersky Endpoint Security

若要讓 Kaspersky Endpoint Security 在 EDR Agent 模式下運作，您必須部署適當的基礎架構；如需更多資訊，請參閱您所選 Detection and Response 解決方案的說明章節。

Light Agent 模式下的 Kaspersky Endpoint Security

若要讓 Kaspersky Endpoint Security 以 Light Agent 模式執行，您需要部署 Kaspersky Security for Virtualization Light Agent 解決方案：

1. 安裝 Kaspersky Security for Virtualization Light Agent 解決方案的元件，即 Integration Server 和 Protection Server。

2. 透過啟動解決方案並設定 Protection Server 和 Light Agent 的資料庫更新，準備好 Protection Server 以供運作。

   如需有關安裝和設定解決方案元件的詳細資訊，請參閱 Kaspersky Security for Virtualization Light Agent 的說明。

3. 請確保您要防護的虛擬機符合 Light Agent 模式的要求。

4. 確保監控虛擬機之間流量的網路裝置或軟體的設定允許網路流量通過用於 Kaspersky Endpoint Security 在 Light Agent 模式下與 Kaspersky Hybrid Cloud Security for Virtualization Light Agent 的其他元件之間進行互動的連接埠。Light Agent 使用的連接埠清單請參閱Kaspersky Security for Virtualization Light Agent 說明。

Kaspersky Endpoint Security 的 Light Agent 模式不支援基於 Arm 架構的裝置和搭載 Elbrus CPU 的裝置。

準備裝置以進行安裝

- 請檢查您的裝置是否符合應用程式的硬體和軟體要求。

- 如果您想要以標準模式或 Light Agent 模式安裝 Kaspersky Endpoint Security，請確保您的裝置上未安裝任何第三方病毒防護軟體。在 EDR Agent 模式下，Kaspersky Endpoint Security 可以與 Dr. 應用程式搭配運作。Web 病毒防護應用程式。

- 請確保您的裝置上未安裝 Kaspersky Endpoint Agent for Linux。如果已安裝 Kaspersky Endpoint Agent for Linux，請將其解除安裝。

- 請確保您的裝置上已安裝 iptables 公用程式。應用程式需要 iptables 公用程式來攔截網路流量。

- 請確保 root 是下列目錄的擁有者，且只有擁有者具有寫入權限：/var、/var/opt、/opt、/usr/bin、/usr/lib、/usr/lib64。這是應用程式正確啟動和運作所必需的。

- 當應用程式執行時，作業系統使用的檔案描述符數量可能會大幅增加。請確保描述符數量限制足夠高。若要檢查限制，請執行指令 `cat /proc/sys/fs/file-max`。一般而言，我們建議透過在 /etc/sysctl.conf 檔案中指定 `fs.file-max=9223372036854775807` 來停用此限制。完成此變更後，請重新啟動作業系統。

- 請確保作業系統中 `kernel.yama.ptrace_scope=0`。`kernel.yama.ptrace_scope` 參數的其他值可能會影響 Kaspersky Endpoint Security 應用程式的運作；如需詳細資訊，請參閱已知問題與限制一節。

此外，若要安裝應用程式的圖形介面：

- 您要安裝的 kesl-gui 套件版本必須與 kesl 套件版本相符。
- 若要讓 Kaspersky Endpoint Security 的圖形介面正確運作，您的作業系統中必須安裝 Zenity 公用程式。
- 如果您的裝置可以存取套件管理器的儲存庫，則在安裝應用程式的圖形介面期間，會自動安裝所有必要的相依性。如果裝置位於私有網段，且無法存取套件管理器的儲存庫：
  1. 請檢查參考裝置上的相依性清單（libice6、libsm6、zlib1g、kesl）。
  2. 執行下列操作之一：
     - 在安裝圖形介面之前，請將套件下載到所有裝置，然後使用套件管理器安裝這些套件。
     - 請確保套件會在圖形介面安裝期間下載到裝置。

此外，若要支援 MMC 外掛程式

如果您打算使用卡巴斯基安全管理中心管理主控台來管理應用程式，請在已安裝管理伺服器的裝置上安裝 Microsoft® Visual C++® 2015 可轉散發套件更新 3 RC（請參閱 https://www.microsoft.com/en-us/download/details.aspx?id=52685）。這是 Kaspersky Endpoint Security MMC 管理外掛程式運作所必需的。

此外，適用於某些作業系統

處於封閉軟體環境模式的 Astra Linux

安裝相容性套件

在下列情況下，您需要安裝相容性套件：

- 在封閉軟體環境模式下安裝應用程式之前。
- 應用程式已安裝，且將作業系統切換到封閉軟體環境模式時。

安裝套件

```
apt install astra-digsig-oldkeys
```

這將允許在 Astra Linux Special Edition 作業系統（適用於 Arm 架構的更新 4.7，以及更新 1.6、1.7 和 1.8）中，以封閉軟體環境模式執行應用程式。

重新允許 ptrace

預設情況下，Astra Linux 作業系統會阻止 ptrace（停用 ptrace 功能），這可能會影響 Kaspersky Endpoint Security 的運作。若要讓 Kaspersky Endpoint Security 正常運作，建議在安裝 Astra Linux 時解除 ptrace 的封鎖。如果已安裝 Astra Linux，請參閱Astra Linux 幫助中心網站瞭解如何啟用/停用此模式（**封鎖 ptrace**部分中**配置防護和封鎖機制**）。

SUSE Linux Enterprise Server 15

在執行 SUSE Linux Enterprise Server 15 作業系統的裝置上安裝應用程式之前，必須先安裝 insserv-compat 套件。

封閉軟體環境模式下的 ALT SP

在封閉軟體環境模式下，將應用程式安裝到搭載 ALT SP 作業系統的裝置之前：

1. 停用封閉軟體環境模式：

```
integrity-remover
```

2. 建立 kesl 群組，以便進一步變更 IMA 政策：

```
groupadd kesl
```

3. 找出所建立群組的唯一識別碼 (GID)：

```
cat /etc/group | grep kesl
```

4. 使用該公用程式編輯 IMA 政策，將 kesl 群組從 應用程式元件完整性檢查 中排除，以確保應用程式正常運作。為此，請執行以下操作：

   a. 複製 /usr/share/integrity/policy 檔案：

   ```
   cp /usr/share/integrity/policy /etc/integrity/policy
   ```

   b. 開啟 /etc/integrity/policy 檔案以在文字編輯器中編輯（例如 vim）：

   ```
   vim /etc/integrity/policy
   ```

   c. 在 `dont_measure fsmagic=0xf97cff8c` 行之後（這通常是 `dont_measure` 區段的最後一行），新增以下行：

   ```
   dont_measure fgroup=<GID>
   ```

   其中 `<GID>` 是依照這些說明的步驟 2 建立之群組的唯一 ID。

   d. 在 `dont_appraise fsmagic=0x27e0eb` 行之後（這通常是 `dont_appraise` 區段的最後一行），新增以下行：

   ```
   dont_appraise fgroup=<GID>
   ```

   其中 `<GID>` 是依照這些說明的步驟 2 建立之群組的唯一 ID。

   e. 儲存變更。

5. 在 /usr/sbin/integrity-sign 檔案中，編輯 list_all_files 函數，將 Kaspersky Endpoint Security 應用程式包括在被允許在封閉環境模式下執行的應用程式允許清單中。為此，請執行以下操作：

   a. 開啟 /usr/sbin/integrity-sign 檔案以在文字編輯器中編輯（例如 vim）：

   ```
   vim /usr/sbin/integrity-sign
   ```

   b. 找到 list_all_files 函數，在函數本文中，在以 `find -P` 開頭的行中，將 Kaspersky Endpoint Security 應用程式在 /var/opt 和 /opt 目錄下的目錄新增至每個目錄枚舉的結尾。

   c. 儲存變更。

在應用程式的初始設定期間，請勿啟動應用程式資料庫更新。

安裝完成後，啟用封閉軟體環境模式，並執行啟動應用程式所需的動作。

OSnova

如果您打算使用卡巴斯基安全管理中心安裝和管理應用程式，請在安裝應用程式之前，準備裝置以安裝網路代理：

1. 開啟 /usr/lib/systemd/logind.conf.d/10-enable-kill-user-processes.conf 檔案進行編輯，並在 `[Login]` 區段中，註解掉 KillUserProcesses=yes 行。

   ```
   #KillUserProcesses=yes
   ```

2. 開啟 /usr/lib/NESS/pam-user-session 檔案進行編輯，並註解掉 loginctl terminate-session "$XDG_SESSION_ID" 行。

   ```
   #loginctl terminate-session "$XDG_SESSION_ID"
   ```

支援 SELinux 的作業系統

如果您的作業系統中未安裝 semanage 公用程式，請在安裝應用程式之前，根據您的套件管理器安裝 policycoreutils-python 或 policycoreutils-python-utils 套件。

policycoreutils-python-utils 套件提供給以下類型的套件管理器：適用於 Fedora、Debian、Ubuntu 以及 RHEL 7 及更新版本的 dnf、apt 和 yum。

policycoreutils-python 套件提供給以下類型的套件管理器：適用於 CentOS/RHEL 7 及更早版本的 yum。

麒麟作業系統

在麒麟作業系統裝置上安裝應用程式之前：

1. 在 UKUI (Ubuntu Kylin 使用者介面) 中，關閉 Firewall。若要這麼做，請前往 **Kylin 安全中心 → Firewall 與網路防護**區段，然後在 **Firewall** 下方停用 **公用網路**和**私人網路**切換開關。

2. 在 UKUI 中，停用應用程式網路控制。若要這麼做，請前往 **Kylin 安全中心 → Firewall 與網路防護** 區段，然後在 **應用程式網路控制** 下方，選取 **停用**。

3. 在 UKUI 中，停用應用程式來源檢查。若要這麼做，請前往 **Kylin 安全中心 → 應用程式保護** 區段，然後在 **應用程式來源檢查** 下方，選取 **停用**。

4. 停用 KYSEC 安全機制。若要這樣做，請在終端機中執行以下動作：

   a. 檢查目前狀態：

   ```
   getstatus
   ```

   b. 停用 KYSEC 安全機制：

   ```
   setstatus disable -p
   ```

   c. 確認 KYSEC 安全機制已停用：

   ```
   getstatus
   ```

5. 解除安裝內建的病毒防護應用程式。若要這樣做，請在終端機中執行以下命令：

   ```
   sudo dpkg -P pksav
   ```

6. 如果您的裝置上安裝了 Qaxsafe 病毒防護軟體，您需要將其解除安裝。為此，請執行以下操作：

   a. 停用自我防護：

      1. 在工作列的通知區域中尋找應用程式圖示，然後按兩下應用程式圖示以開啟內容功能表。

      2. 在內容功能表中，選取 **設定 → 防護中心**。

      3. 這會開啟一個視窗；在該視窗中，取消選取 **啟用自我防護** 核取方塊，並在系統提示時輸入密碼。

   b. 解除安裝 Qaxsafe 病毒防護軟體。若要這樣做，請在終端機中執行以下命令：

   ```
   sudo dpkg -P qaxsafe
   ```

   c. 刪除所有殘留檔案。若要這樣做，請在終端機中執行以下命令：

   ```
   sudo rm -rf /opt/qaxsafe
   ```

不支援 fanotify 的作業系統

在開始安裝應用程式之前，請確認裝置上已安裝以下項目：

- 用於編譯應用程式和執行工作的套件 (gcc、binutils、glibc、glibc-devel、make)
- 包含用於編譯 Kaspersky Endpoint Security 模組的作業系統核心標頭檔案的套件

實用文章

麒麟作業系統問題疑難排解

準備好安裝環境後，您可以返回部署情境，並從 選擇系統事件攔截機制 步驟繼續。

選擇系統事件攔截機制

為了正常運作，應用程式必須攔截檔案操作和處理程序啟動的系統事件。所有應用程式模式（標準模式、Light Agent 模式和 EDR 代理模式）都需要系統事件攔截。如果應用程式不使用系統事件攔截，則不會執行即時檔案掃描，並且裝置的保護等級會降低。

系統事件攔截機制

應用程式可以使用以下機制來攔截系統事件：

- **基於 fanotify 的系統攔截機制。** *Fanotify* 是 Linux 核心的子系統，可監控檔案系統中的事件（例如開啟、讀取、寫入或關閉檔案），並允許應用程式即時攔截這些事件。

- **基於可更新的內核模組的攔截機制。** *可更新的內核模組*會搭配以 fanotify 技術為基礎的系統攔截機制運作。如此一來，Kaspersky Endpoint Security 便可透過在 kernel space 而非 user space 中處理系統事件，最佳化檔案操作攔截和處理程序啟動攔截。可更新的內核模組會在檔案被開啟、重新命名或修改時攔截檔案操作。由於採用檔案和處理程序掃描結果快取，應用程式效能得以提升。

  可更新的內核模組也用於以下工作和元件：

  - 檔案威脅防護
  - Anti-Cryptor
  - 弱點利用防禦
  - 行為偵測
  - 應用程式控制
  - 物件的執行防禦（與 Kaspersky Endpoint Detection and Response Expert (on-premises) 和 Kaspersky Endpoint Detection and Response Optimum 整合時）

  透過使用可更新內核模組，您可以更精細地配置全域排除項目。以 fanotify 技術為基礎的攔截機制可完全排除指定掛載點的檔案操作攔截。使用可更新內核模組，您可以排除裝置上掛載的特定本機或遠端目錄。

  可更新的內核模組包含在應用程式分發套裝中。

- **適用於沒有 fanotify 的作業系統的檔案威脅防護核心模組**。如果裝置上的作業系統不支援 fanotify 技術（CentOS 5.2、CentOS 5.4、CentOS 6.4、CentOS 6.6），應用程式會編譯並使用特殊模組來攔截系統事件。當啟動檔案威脅防護時，如果所有依賴項和建置工具都可用，則會自動編譯此模組。

如何選取系統事件攔截機制

如果作業系統支援 fanotify，您可以在部署應用程式時選取系統事件攔截機制：僅 fanotify，或可更新的內核模組加上 fanotify。預設設定為 fanotify。安裝後，您可以在應用程式設定中變更系統事件攔截機制。

對於不支援 fanotify 的作業系統，無法選取攔截機制。

如果作業系統符合安裝可更新的內核模組的要求，則應用程式可以使用基於可更新的內核模組的攔截機制。

可更新的內核模組安裝要求

若要安裝和使用可更新的內核模組，裝置必須安裝以下 64 位元作業系統之一：

- Astra Linux Special Edition RUSB.10015-01 (operational update 1.6.5, 1.6.6)。
- Astra Linux Special Edition RUSB.10015-01 (operational update 1.7.3, 1.7.4, 1.7.6, 1.7.7, 1.7.8, 1.7.9)。
- Astra Linux Special Edition RUSB.10015-01 (operational update 1.8.2, 1.8.3, 1.8.4, 1.8.5)。

  如果 Kaspersky Endpoint Security 應用程式在基本模式下使用，則可更新的內核模組可以在安裝有 Astra Linux作業系統的裝置上在封閉軟體環境模式下使用。

- CentOS 7.x。
- CentOS 8.x。
- Debian GNU/Linux 12.7、12.8、12.9、12.1012.12。
- Red Hat Enterprise Linux 7.4。
- Red Hat Enterprise Linux 8.10。
- SberLinux 8.10。
- SberLinux 9.0.1。
- SberLinux 9.1。
- SberLinux 9.6。
- SberLinux 9.7。
- SberOS 3.4。
- SberOS 3.5。
- Ubuntu 16.04 LTS。
- Ubuntu 18.04 LTS。
- Ubuntu 20.04 LTS。

- Ubuntu 22.04 LTS。
- Ubuntu 24.04 LTS。
- ALT SP Workstation 版本 10。
- ALT SP Server 版本 10。
- ALT Education 10。
- ALT Workstation 11。
- ALT Server 11。
- ALT Education 11。
- RED OS 7.3。
- RED OS 8.0。
- ROSA "Cobalt" 7.9 Workstation。
- ROSA "Cobalt" 7.9 Server。
- ROSA "Chrome" 12 Workstation。
- ROSA "Chrome" 12 Server。

不支援 32 位元作業系統、Arm 架構的作業系統，以及 Elbrus 架構的作業系統。

可更新的內核模組可能會與某些版本的 Linux 內核和某些第三方應用程式發生衝突。

檢查是否可以安裝可更新的內核模組

可更新的內核模組版本不取決於 Kaspersky Endpoint Security 的版本。可更新的內核模組功能會作為 Kaspersky Endpoint Security 資料庫和應用程式模組更新的一部分定期擴充。因此，上述支援的作業系統清單可能並非詳盡無遺。若要確認您的裝置是否符合安裝可更新的內核模組的要求，請使用卡巴斯基 ULKM 工具。

如何使用網頁主控台或管理主控台進行遠端檢查

1. 從 Kaspersky Endpoint Security for Linux 區域的**應用程式下載頁面**下載 ulkmtool2.zip 壓縮檔案。
2. 為該公用程式建立安裝套件。

如何在網頁主控台中建立安裝套件

1. 將下載的 ulkmtool.zip 壓縮檔案放在卡巴斯基安全管理中心管理伺服器可存取的資料夾中。
2. 在主網頁主控台視窗中，選擇以下部分之一：
   - **裝置發現和部署→部署和分配→安裝套件**。
   - **操作→儲存庫→安裝套件**。

   管理伺服器上可用的安裝套件清單將開啟。
3. 點擊"**新增**"按鈕。
   建立安裝套件的精靈將啟動。
4. 選取**從檔案建立安裝套件**作為安裝套件建立方法。
5. 輸入新安裝套件的名稱，點擊**瀏覽**按鈕並指定下載的 ulkmtool.zip 壓縮檔案的路徑。
6. 完成精靈。

   套件將被建立並加入到套件清單中。

如何在管理主控台中建立安裝套件

1. 將 ulkmtool.zip 壓縮檔案解壓縮到卡巴斯基安全管理中心伺服器可存取的資料夾中。
2. 在主控台樹狀目錄中，選擇**其它 → 遠端安裝 → 安裝套件**。
   管理伺服器上可用的安裝套件清單將開啟。
3. 點擊"**建立安裝套件**"按鈕。
   建立安裝套件的精靈將啟動。
4. 點擊**建立卡巴斯基應用程式安裝套件**按鈕。
5. 輸入新安裝套件的名稱，然後繼續精靈的下一步。
6. 點擊**瀏覽**按鈕並指定 ulkmtool.kud 檔案的路徑。該檔案位於您解壓縮 ulkmtool.zip 壓縮檔案的資料夾中。
   繼續精靈的下一步。
7. 等待檔案下載完成並完成精靈。

   套件將被建立並加入到套件清單中。

3. 在要檢查是否符合可更新核心模組要求的裝置上安裝卡巴斯基安全管理中心網路代理。請參閱 卡巴斯基安全管理中心說明 瞭解更多詳情。
4. 在卡巴斯基安全管理中心網頁主控台或管理主控台中，針對您要檢查其是否符合可更新的內核模組要求的裝置，建立並執行遠端安裝工作。在工作設定中，選取您所建立的安裝套件。

   每個裝置的工作結果都會表明該裝置是否支援可更新的內核模組的安裝和執行。

根據工作結果，每個裝置將取得一個標籤：

- *UpdatableKernelModule=No* 表示裝置不支援可更新的內核模組安裝。
- *UpdatableKernelModule=Yes* 表示裝置符合安裝和執行可更新的內核模組的要求。

您可以使用這些標籤來建立裝置選取。例如，您可以選取符合可更新的內核模組要求的裝置，並在這些裝置上安裝具有可更新的內核模組的 Kaspersky Endpoint Security。

如何在裝置本機進行檢查

1. 從 Kaspersky Endpoint Security for Linux 區域的**應用程式下載頁面**下載 ulkmtool2.zip 壓縮檔案。
2. 在要檢查是否符合可更新核心模組要求的裝置上安裝卡巴斯基安全管理中心網路代理。請參閱 卡巴斯基安全管理中心說明 瞭解更多詳情。
3. 在您要掃描的裝置上本機執行 Kaspersky ULKM tool 公用程式。

   ```
   ulkmtool --check remote
   ```

4. 檢查傳回碼。

   ```
   echo $?
   ```

   此工具會在命令列傳回下列代碼：

   0 = Success 表示裝置符合安裝和執行可更新的內核模組的要求。

   1 = NotSupported 表示裝置不支援安裝可更新的內核模組。

檢查可更新的內核模組的狀態

在卡巴斯基安全管理中心網頁主控台或管理主控台中，您可以檢查已安裝 Kaspersky Endpoint Security 的裝置上可更新的內核模組的狀態。為此，您可以檢視指派給裝置的標籤：

- *UpdatableKernelModule=Use* 表示裝置上安裝了可更新的內核模組，且該模組正在執行。
- *UpdatableKernelModule=Error* 表示裝置上安裝了可更新的內核模組，但是啟動該模組時發生錯誤，該模組並未執行。

有關檢視指派給裝置的標籤的詳細資訊，請參閱卡巴斯基安全管理中心說明。

安全啟動支援

可更新的內核模組支援 Secure Boot。若要在已啟用 Secure Boot 的作業系統上使用以可更新的內核模組為基礎的攔截機制，您需要將用來簽署該模組的 Kaspersky Endpoint Security 公用憑證新增至作業系統，然後重新啟動作業系統。

下載憑證

在 Ubuntu 中新增憑證的範例

1. 請確定您的作業系統中已啟用安全啟動：

```
mokutil --sb-state
```

2. 使用 mokutil 工具將下載的憑證新增至您的作業系統：

```
mokutil --import <path to certificate>
```

3. 重新啟動 Kaspersky Endpoint Security。

4. 執行下列命令，檢查可更新的內核模組是否正常運作：

```
kesl-control --app-info
```

選擇系統事件攔截機制後，您可以返回部署場景，並從準備分發套件步驟繼續。

準備分發套件

*Kaspersky Endpoint Security 分發套件*是一組用於安裝和更新應用程式的檔案，以及使用者協議（最終使用者產品授權協議、隱私權政策和卡巴斯基安全網路聲明）的文字。您也可以另外下載包含圖形介面的分發套件，以便在本機管理和監控應用程式。

您需要分發套件，以使用卡巴斯基安全管理中心建立在企業網路中的裝置上部署所需的安裝套件，以及使用命令列部署應用程式。

若要使用卡巴斯基安全管理中心進行部署，您還需要*用於遠端安裝應用程式的分發套件*。此分發套件包含遠端部署應用程式所需的檔案以及使用者協議的文字。

> 使用者協議的文字可在卡巴斯基網站（**EULA** 區段）以及安裝應用程式後的 `/opt/kaspersky/kesl/doc/` 目錄中取得。

您可以在建立安裝套件步驟中，選取要自行部署 Kaspersky Endpoint Security 或使用卡巴斯基安全管理中心部署所需的分發套件。

如何選擇用於 Kaspersky Endpoint Security 部署的分發套件

分發套件的選擇取決於以下因素：

- Kaspersky Endpoint Security 版本：已認證或未認證
- 部署方法：使用卡巴斯基安全管理中心或使用命令列
- 視作業系統而定的套件格式

- 作業系統架構和 CPU 類型
- Kaspersky Endpoint Security 管理方法
- 是否需要安裝應用程式的圖形使用者介面

1. **判斷您的應用程式版本：已認證或未認證**

   - 如果您需要**已認證**版本，請從商業應用程式支援生命週期頁面下載一組分發套件。

     已認證版本包含主要應用程式檔案和圖形介面檔案（`kesl` 目錄）、用於遠端安裝應用程式的封存檔（`remote install` 目錄）、MMC 外掛程式 (`SCPlugin`) 和 Web 外掛程式 (`web plugin`)。

     轉至步驟 3。

   - 如果您需要**未認證**版本，請前往下一步。

2. **判斷部署方法：使用卡巴斯基安全管理中心或使用命令列**

   若要**使用卡巴斯基安全管理中心進行部署**，請從下列其中一個來源下載分發套件：

   - 從卡巴斯基網站
   - 如果您有 Kaspersky CompanyAccount，透過向技術支援提出請求

   若要**使用命令列進行部署**，請從卡巴斯基網站下載分發套件：

   - 主要應用程式分發套件（`Distributive`）
   - 如有必要，包含圖形使用者介面的分發套件（`Product GUI`）

   如果您想要從卡巴斯基網站下載分發套件，將需要下列檔案：

   - 主要應用程式分發套件（`Distributive`）
   - 如有必要，包含圖形使用者介面的分發套件（`Product GUI`）
   - 使用卡巴斯基安全管理中心遠端安裝應用程式的分發套件（**附加分發套件** → `Files for Product remote installation`）
   - 卡巴斯基安全管理中心網路代理的分發套件（卡巴斯基安全管理中心分發區段 → `Network agent`）

   > 應用程式的分發套件在所有本地化版本中都相同。Kaspersky Endpoint Security 的語言是在應用程式初始設定期間選取。本地化支援取決於作業系統中安裝的語言。

3. **根據受防護裝置的作業系統判斷套件格式**

作業系統	套件格式
Debian、Ubuntu、Astra Linux、Linux Mint	`.deb`
Red Hat Enterprise Linux、CentOS、Oracle Linux、RED OS、SUSE Linux Enterprise、openSUSE、Rocky Linux、AlmaLinux、ALT 系列作業系統、GosLinux、Rosa 系列作業系統、Amazon Linux 2023	`.rpm`

   如果您的作業系統未列出，請根據作業系統文件選取套件格式。

4. **判斷作業系統架構和 CPU 類型**

CPU 類型和作業系統位元	分發套件
Arm CPU，64 位元作業系統	arm64 aarch64
Elbrus CPU	e2k
其他處理器，32 位元作業系統	i386
其他處理器，64 位元作業系統	x86_64 x64 amd64

若要在支援受限的作業系統（CentOS 5.2、CentOS 5.4、CentOS 6.4、CentOS 6.6）上安裝 Kaspersky Endpoint Security 應用程式，請選取標示為 OLD 的發佈套件。

使用應用程式文件中未描述或非技術支援團隊建議的方法自行編輯應用程式的設定檔可能會導致應用程式和作業系統效能不佳和故障、裝置防護程度降低、資料無法存取和損壞，以及開啟向 KSN 發送額外統計資料的情況。

準備好分發套件後，您可以返回部署情境，並從 卡巴斯基安全管理中心中的準備動作 步驟繼續。

卡巴斯基安全管理中心中的準備動作

在安裝 Kaspersky Endpoint Security 應用程式之前，建議您在卡巴斯基安全管理中心中執行以下操作。

1 配置裝置的管理群組

若要使用卡巴斯基安全管理中心管理應用程式，您需要將安裝該應用程式的裝置放入管理群組。預設情況下，卡巴斯基安全管理中心會將所有已安裝管理代理程式且已連線至管理伺服器的裝置移至 **未指派的裝置** 群組。

建議您預先設定管理群組中的裝置自動放置規則，並透過為每種裝置類型建立單獨群組，依照其類型將裝置分配到群組。這可讓您根據裝置套用不同的應用程式設定。

您也可以手動將裝置放入管理群組。

2 網路代理的安裝和初始配置

網路代理可協助裝置連線至卡巴斯基安全管理中心管理伺服器。它必須安裝在將連線至卡巴斯基安全管理中心的每個裝置上。

1. 準備 Linux 裝置以安裝網路代理。該步驟取決於作業系統。

2. 執行網路代理的安裝和初始配置。請參閱卡巴斯基安全管理中心說明以取得操作說明。

因此，已安裝網路代理的裝置會顯示在與為這些裝置配置的移動規則相對應的群組中。如果您尚未配置任何移動規則，裝置會顯示在 **未指派的裝置** 群組中。

3 安裝 Kaspersky Endpoint Security 管理外掛程式

根據您使用的卡巴斯基安全管理中心管理主控台，安裝 Kaspersky Endpoint Security 管理外掛程式：

- **Kaspersky Endpoint Security 管理 MMC 外掛程式**可讓您使用卡巴斯基安全管理中心管理主控台來管理應用程式。MMC 外掛程式安裝在安裝了卡巴斯基安全管理中心管理主控台的裝置上。

  如何安裝 Kaspersky Endpoint Security MMC 外掛程式

  > 在安裝 Kaspersky Endpoint Security MMC 管理外掛程式之前，請確保已安裝卡巴斯基安全管理中心和 Redist C++ 2015（Microsoft Visual C++ 2015 Redistributable）。

  若要安裝 MMC 外掛程式：

  1. 在 應用程式下載頁面 的 **Kaspersky Endpoint Security for Linux** 區段中下載 klcfginst.msi 檔案（**組建 → 管理外掛程式**）。

  2. 在已安裝卡巴斯基安全管理中心管理主控台的裝置上，執行 klcfginst.msi 檔案。

  安裝後，管理 MMC 外掛程式將顯示在卡巴斯基安全管理中心伺服器屬性中已安裝的 MMC 管理外掛程式清單中。

  若要檢視已安裝的管理 MMC 外掛程式清單：

  1. 在卡巴斯基安全管理中心管理主控台樹中，選擇**管理伺服器<伺服器名稱>**節點並透過以下方式之一開啟管理伺服器屬性視窗：

     - 開啟 **管理伺服器 <伺服器名稱>** 節點的內容功能表，並選取 **屬性** 項目。

     - 在 **管理伺服器** 區段中，按一下 **管理伺服器 <伺服器名稱>** 節點工作區內的 **管理伺服器屬性** 連結。

  2. 在**進階**區域的左側清單中，選取**安裝應用程式管理外掛程式相關資訊**區域。

     在視窗右側，已安裝的管理外掛程式清單會顯示Kaspersky Endpoint Security 的管理 MMC 外掛程式：**Kaspersky Endpoint Security <版本號> for Linux**。

如果您使用卡巴斯基安全管理中心管理主控台管理 Kaspersky Endpoint Security 應用程式，且已安裝多個版本的應用程式，則需要為每個版本的 Kaspersky Endpoint Security 應用程式安裝一個管理外掛程式。這使您可以使用為不同管理外掛程式版本建立的政策來管理應用程式。您也可以將使用先前版本的管理外掛程式建立的政策和工作轉換為較新版本。

- **Kaspersky Endpoint Security 管理 Web 外掛程式**可讓您使用卡巴斯基安全管理中心網路主控台和卡巴斯基安全管理中心雲端主控台來管理應用程式。Web 外掛程式安裝在已安裝卡巴斯基安全管理中心網頁主控台的裝置上。所有可以透過瀏覽器存取卡巴斯基安全管理中心網頁主控台的管理員都可以使用該 Web 外掛程式的功能。

  如何安裝 Kaspersky Endpoint Security Web 外掛程式

  您可以透過以下方式安裝 Web 外掛程式：

  - 使用卡巴斯基安全管理中心網頁主控台的快速啟動精靈。

    首次將卡巴斯基安全管理中心網頁主控台連線至管理伺服器時，卡巴斯基安全管理中心網頁主控台會自動提示您執行快速啟動精靈。您也可以在卡巴斯基安全管理中心網頁主控台介面中執行初始配置精靈（**裝置發現和部署→部署和指派→快速啟動精靈**）。快速啟動精靈還可以檢查已安裝的 Web 外掛程式是否為最新，並下載必需的更新。如需卡巴斯基安全管理中心網頁主控台快速啟動精靈的詳細資訊，請參閱 卡巴斯基安全管理中心說明。

  - 手動安裝，使用卡巴斯基 Web 外掛程式清單中的發佈套件或檔案中的發佈套件。

  若要從卡巴斯基安全管理中心手動安裝 Kaspersky Endpoint Security Web 外掛程式：

  1. 在卡巴斯基安全管理中心網頁主控台的主視窗中，選擇 **設定 → Web 外掛程式**。

     已安裝的 Web 外掛程式清單將開啟。

  2. 點擊**"新增"**按鈕。

     這會開啟可用管理外掛程式清單。當 Web 外掛程式有新版本發布後，該清單會自動更新。

  3. 在可用外掛程式清單中，選取 **Kaspersky Endpoint Security <版本號碼> for Linux** Web 外掛程式。

  4. 在開啟的帶有 Web 外掛程式描述的視窗中，點擊**安裝外掛程式**按鈕。

  5. 等待安裝完成，然後在資訊視窗中點擊**確定**。

  新的外掛程式將顯示在已安裝的 Web 外掛程式清單中（**設定 → Web 外掛程式**）。

  若要從檔案手動安裝 Kaspersky Endpoint Security Web 外掛程式：

  1. 在 應用程式下載頁面 的 **Kaspersky Endpoint Security for Linux** 區段中下載包含 Web 外掛程式的封存檔（**附加發佈套件 → 網頁主控台外掛程式**）。

  2. 將下載的封存檔解壓縮到本機。

  3. 在卡巴斯基安全管理中心網頁主控台主視窗中，選取**設定 → Web 外掛程式**。

     已安裝的 Web 外掛程式清單將開啟。

  4. 點擊**從檔案新增**按鈕。

  5. 這會開啟一個視窗；請在該視窗中指定 plugin.zip 檔案的路徑和 signature.txt 檔案的路徑。這些檔案位於您解壓縮包含 Web 外掛程式之封存檔的資料夾中。

6. 點擊“**新增**”按鈕。

7. 等待安裝完成，然後在資訊視窗中點擊**確定**。

新的外掛程式顯示在已安裝的 Web 外掛程式清單中（**設定→ Web 外掛程式**）。

如果您在卡巴斯基安全管理中心伺服器的屬性中選擇了 Kaspersky EndpoinSecurity 分發套件中未包含的語言，則產品授權協議和整個卡巴斯基安全管理中心網頁主控台介面將以英文顯示。

影片：使用精靈安裝管理 Web 外掛程式

影片：在隔離網路中安裝管理 Web 外掛程式

4 建立 Kaspersky Endpoint Security 政策

在 卡巴斯基安全管理中心網頁主控台 或管理主控台中建立 Kaspersky Endpoint Security 的政策（取決於您使用的卡巴斯基安全管理中心管理主控台）。

根據您要使用應用程式的模式，管理以下設定：

針對標準模式

若您已在管理主控台精靈中建立政策，請指定應用程式使用模式：**標準模式或 Endpoint Detection and Response Agent 模式**。若您已在卡巴斯基安全管理中心網頁主控台精靈中建立政策，請略過應用程式模式的選擇。

針對 EDR 代理程式模式

1. 若您已在管理主控台精靈中建立政策，請指定應用程式使用模式：**標準模式或 Endpoint Detection and Response Agent 模式**。若您已在卡巴斯基安全管理中心網頁主控台精靈中建立政策，請略過應用程式模式的選擇。

2. 依照精靈的指示完成政策建立。

3. 在 卡巴斯基安全管理中心網頁主控台 或管理主控台中開啟已建立政策的內容，並啟用與您要用來保護裝置之 Detection and Response 解決方案的整合：

   - 若要在 OSMP 平台上進行 Kaspersky Endpoint Detection and Response Expert (on-premises) 整合，您需要啟用並設定 EDR Expert (on-premises) 元件。這些設定可在 卡巴斯基安全管理中心網頁主控台 中使用

   - 若要與 Kaspersky Anti Targeted Attack Platform 上的 Kaspersky Endpoint Detection and Response 整合，您需要啟用並設定 EDR Expert (on-premises) 元件。這些設定可在 卡巴斯基安全管理中心網頁主控台 和 管理主控台 中使用。

   - 若要與 Kaspersky Anti Targeted Attack Platform 上的卡巴斯基 Network Detection and Response 整合，您需要啟用並設定 NDR (KATA) 元件。這些設定可在卡巴斯基安全管理中心網頁主控台和 管理主控台 中使用。

針對 Light Agent 模式

在新政策精靈中：

1. 指定 **用於防護虛擬環境的 Light Agent 模式**。

2. 管理 SVM 偵測設定：

   a. 選擇 Light Agent 用於發現可連線的 SVM 的方法。

      - **使用 Integration Server**如果選擇此選項，Light Agent 將連線至 Integration Server 以獲取可用於連線的 SVM 清單和其詳情。

      - **使用 SVM 位址自訂清單**如果選擇此選項，您可以指定此政策管理的 Light Agent 可以連線到的 SVM 清單。Light Agent 將僅連線到清單中指定的 SVM。

      如果您選取 **使用 SVM 位址自訂清單** 選項，Light Agent 使用延伸 SVM 選擇演算法，且 SVM 已啟用大型基礎架構防護模式，則只有在忽略 SVM 路徑時，才能將 Light Agent 連線到此 SVM。在 **SVM 選擇演算法** 區段中，您需要將 **SVM 路徑** 設定設為 **略過**。如果設定了任何其他值，Light Agent 將無法連線到 SVM。如需更多詳細資訊，請參閱 Kaspersky Security for Virtualization Light Agent 說明 。

   b. 如果選擇 Integration Server，精靈將顯示將 Light Agent 連線到 Integration Server 的目前設定：用於連線的位址和連接埠。如有必要，請指定新的連線設定：用於連線至 Integration Server 的 IPv4 位址或完整網域名稱 (FQDN) 和連接埠。

      如果您的基礎架構中部署了基於 Linux 的高可用性 Integration Server 叢集，則需要將負載均衡器的位址和連接埠指定為用於連線到 Integration Server 的位址和連接埠。如需更多詳細資訊，請參閱 Kaspersky Security for Virtualization Light Agent 說明 。

c. 如果您選擇手動定義的 SVM 位址清單，請建立此政策管理的 Light Agent 可以連線到的 SVM 清單。若要將 SVM 新增至清單，請按一下 **新增** 按鈕，並在開啟的視窗中指定 SVM 的 IPv4 格式 IP 位址或完整網域名稱 (FQDN)。您可以透過換行輸入 SVM 的多個 IP 位址或完整網域名稱。

> 僅指定對應到單一 IP 位址的完全限定網域名稱 (FQDN)。使用與多個 IP 位址相對應的完全限定網域名稱可能會導致應用程式出現錯誤。

其餘政策設定可以保留預設值。預設設定提供基本的防護等級。安裝 Kaspersky Endpoint Security 後，您可以根據組織的要求設定政策。若要執行此操作，您可以使用 管理應用程式 說明區段中的元件設定情境。

影片：建立政策

5 設定應用程式資料庫和模組的集中式更新

預設情況下，Kaspersky Endpoint Security 在裝置上安裝時不包含病毒防護資料庫。應用程式只有在資料庫下載到裝置後才能運作。若要確保安裝應用程式後立即開始防護，請設定集中式資料庫更新。

在卡巴斯基安全管理中心網頁主控台或管理主控台中（取決於您使用的卡巴斯基安全管理中心管理主控台）：

1. 啟動管理伺服器工作 *將更新下載至管理伺服器儲存區*。此工作由管理伺服器快速啟動精靈自動建立。

   此工作會將 Kaspersky Endpoint Security 的更新套件下載到管理伺服器上的更新目錄。

2. 為 Kaspersky Endpoint Security 應用程式建立 *更新* 類型的群組工作。在 工作設定 中，指定：

   - 更新來源：卡巴斯基安全管理中心。
   - 工作排程：至少每天一次。建議每天執行此工作 4 至 6 次。

影片：設定集中式資料庫更新

6 新增產品授權金鑰並建立啟動工作

若要在標準模式下啟動應用程式，您必須將產品授權金鑰新增至應用程式。如果您的產品授權未涵蓋某些元件，您可能需要另一個產品授權金鑰：

若要以 EDR 代理程式模式啟動 Kaspersky Endpoint Security 應用程式，您需要 EDR Expert (on-premises) 產品授權金鑰。

您可以根據基礎架構和組織的要求選擇啟動方法：

- 如果所有裝置上安裝的應用程式具有相同的功能集，請使用產品授權金鑰自動分發。要分發的產品授權金鑰必須先使用金鑰檔案或啟動碼新增至卡巴斯基安全管理中心金鑰儲存區。如需詳細資訊，請參閱 卡巴斯基安全管理中心說明。

- 如果各裝置的應用程式功能集不同，您將需要不同的產品授權金鑰進行啟動。在此情況下，請將受保護的裝置置於不同的管理群組中，並為每個管理群組設定一個用於新增金鑰的 群組工作。

Light Agent 模式下的 Kaspersky Endpoint Security 在連線至 SVM 後，會從 Protection Server 接收產品授權資訊。您不需要另外啟動 Light Agent 模式下的 Kaspersky Endpoint Security。

影片：使用啟動碼啟動應用程式

影片：使用金鑰檔案啟動應用程式

準備好卡巴斯基安全管理中心後，您可以返回部署情境，並從 安裝應用程式 步驟繼續。

使用卡巴斯基安全管理中心安裝應用程式

安裝時的特殊注意事項：

- 配備 Elbrus CPU 的裝置不支援 Kaspersky Endpoint Security 的 EDR Agent 模式和 Light Agent 模式。
- Arm 裝置不支援 Light Agent 模式的 Kaspersky Endpoint Security。

使用卡巴斯基安全管理中心安裝應用程式的建議情境包含以下步驟：

您也可以使用 快速啟動精靈 和防護部署精靈，透過卡巴斯基安全管理中心安裝 Kaspersky Endpoint Security 應用程式。

1 建立安裝套件

Kaspersky Endpoint Security 應用程式的安裝套件包含以下內容：

- 主要分發套件
- 用於遠端安裝應用程式的分發套件
- 含有應用程式圖形介面的分發套件
- 安裝期間套用的初始組態設定

您可以透過以下方式建立安裝套件：

- **使用託管於卡巴斯基伺服器上的分發套件**。在卡巴斯基安全管理中心，會根據指定的分發套件自動建立安裝套件。

影片：在卡巴斯基安全管理中心自動建立安裝套件

若要在支援受限的作業系統（CentOS 5.2、CentOS 5.4、CentOS 6.4、CentOS 6.6）上安裝 Kaspersky Endpoint Security 應用程式，請選取標示為 `for legacy OS` 的發佈套件。

- **手動使用在準備分發套件步驟中準備的檔案**。如果您想要使用設定檔指定初始組態設定，或想要將已建立的安裝套件用於不同的作業系統或不同的套件管理器，建議使用此方法。

  影片：在卡巴斯基安全管理中心手動建立安裝套件

  您可以將預先下載的應用程式資料庫新增到安裝套件中。如果您使用的是含有整合資料庫的安裝套件，則應用程式已與資料庫一起安裝；在這種情況下，您不需要在安裝後立即更新資料庫。

同一個安裝套件可以多次使用。

如何手動準備安裝套件

1. 在本機解壓縮包含用於遠端安裝 Kaspersky Endpoint Security 之檔案的封存檔。

2. 將含有主要應用程式檔案的套件放在同一個目錄中。

   如果您想要將已建立的安裝套件用於不同的作業系統或套件管理器，請將您需要的所有類型的作業系統和套件管理器的分發套件放在目錄中。

3. 如果您想要使用應用程式的圖形介面，請將圖形介面套件放在同一個目錄中。

   若要啟用圖形介面，請在已建立的安裝套件內容中或在 autoinstall.ini 設定檔中編輯適當的設定 (`USE_GUI=Yes`)。預設不會安裝圖形介面。

如果在 Light Agent 模式下使用 Kaspersky Endpoint Security，則不支援圖形使用者介面。

4. 如果您想要使用設定檔設定應用程式的初始組態，請開啟 autoinstall.ini 設定檔並視需要進行編輯。autoinstall.ini 檔案位於您解壓縮包含用於遠端安裝 Kaspersky Endpoint Security 之檔案的封存檔所在的資料夾中。

   a. 應用程式預設以標準模式使用。

      若要以 EDR Agent 模式使用應用程式，請設定 `ENDPOINT_AGENT_MODE=Yes`。

      若要以 Light Agent 模式使用應用程式，請設定 `KSVLA_MODE=Yes`。

      安裝 Kaspersky Endpoint Security 後，您無法變更應用程式使用模式。

   b. 若要以 Light Agent 模式安裝應用程式：

      - 如果您要將應用程式安裝在將用於建立暫時虛擬機的範本上，請設定 `VDI_MODE=Yes`。此設定會啟用 VDI 防護模式，以最佳化應用程式在暫時虛擬機上的效能。
      - 指定您要保護的虛擬機在虛擬基礎架構中的角色 (伺服器或工作站) (`SERVER_MODE=Yes|No`)。虛擬機的角色決定了應用程式在此虛擬機上使用的產品授權以及可用的功能。

   您也可以稍後在已建立的安裝套件內容中的 **設定**標籤上變更應用程式的初始組態。

5. 將所有準備好的檔案放入 ZIP、CAB、TAR 或 TAR.GZ 格式的壓縮檔案中，並以任意名稱命名。

如何在網頁主控台中建立安裝套件

1. 在主網頁主控台視窗中，選擇以下部分之一：

   - **發現和佈署 → 佈署和指派 → 安裝套件**.
   - **操作→儲存庫→安裝套件**。

   管理伺服器上可用的安裝套件清單將開啟。

2. 點擊"**新增**"按鈕。

   建立安裝套件的精靈將啟動。

3. 如果您使用的是網頁主控台，請選擇建立安裝套件的方式：

   - **從檔案建立安裝套件**安裝套件將從您預先準備好的壓縮檔案中建立。
   - **為卡巴斯基應用程式建立安裝套件**安裝套件將從位於卡巴斯基伺服器上的分發套件中建立。

   如果您使用的是卡巴斯基安全管理中心雲端主控台，則會從託管在卡巴斯基伺服器上的分發套件建立安裝套件。

4. 視套件建立方法而定：

   - 指定套件名稱，點擊 **瀏覽** 按鈕，然後指定您為建立安裝套件所準備之封存檔的路徑。
   - 選擇 Kaspersky Endpoint Security 分發套件。在右側視窗中，閱讀分發套件的相關資訊，然後點擊 **下載並建立安裝套件** 按鈕。安裝套件建立過程啟動。

5. 閱讀您與 Kaspersky 簽訂的《最終使用者產品授權協議》以及描述資料處理和傳輸的《隱私政策》。若要繼續建立安裝套件，您必須確認您已閱讀並接受最終使用者產品授權協議和隱私權政策的完整條款。

6. 完成精靈。

   套件將被建立並加入到套件清單中。

7. 開啟安裝套件的內容，然後前往 **設定** 標籤。

   - 如果您以 EDR Agent 模式安裝應用程式，請針對 **使用模式** 設定，選取 **Endpoint Detection and Response Agent**。

   - 如果您以 Light Agent 模式安裝應用程式，請指定以下設定：

     使用模式，選取 **Light Agent 防護虛擬環境** 選項。

     啟用 VDI 防護模式選取此核取方塊可啟用 VDI 防護模式。如果您要在用於建立暫時虛擬機的虛擬機範本上安裝該應用程式，則建議這樣做。預設情況下已清空此核取方塊。

     受防護的虛擬機被用作伺服器將安裝應用程式的虛擬機的角色：伺服器或工作站。預設情況下，此核取方塊處於選取狀態（虛擬機在虛擬基礎架構中用作伺服器）。

   - 如有必要，請管理其他初始組態設定。

     如需安裝套件中應用程式所有初始組態設定的說明，請參閱 附錄 1。

如何在管理主控台中建立安裝套件

若要使用準備好的檔案建立安裝套件：

1. 在主控台樹狀目錄中，選擇**其它** → **遠端安裝** → **安裝套件**。

2. 點擊"**建立安裝套件**"按鈕。

   建立安裝套件的精靈將啟動。

3. 點擊**建立卡巴斯基應用程式安裝套件**按鈕。

4. 輸入新安裝套件的名稱，然後繼續精靈的下一步。

5. 指定 kesl.kud 檔案的路徑。該檔案位於您在 準備分發套件 步驟中解壓縮包含應用程式安裝檔案之封存檔 (kesl.zip) 的資料夾中。

   視窗中會顯示應用程式的名稱和版本。繼續精靈的下一步。

6. 閱讀您與 Kaspersky 簽訂的《最終使用者產品授權協議》以及描述資料處理和傳輸的《隱私政策》。

   若要繼續，請確認您已閱讀並接受最終使用者產品授權協議和隱私權政策的完整條款。為了確認，請在開啟的視窗中選取兩個核取方塊。

   繼續精靈的下一步。

7. 此精靈會將安裝應用程式所需的檔案下載至卡巴斯基安全管理中心伺服器。等待下載完成，然後完成精靈。

8. 開啟安裝套件的內容，然後前往 **應用程式設定** 標籤。

   - 如果您以 EDR Agent 模式安裝應用程式，請針對 **應用程式模式** 設定，選取 **Endpoint Detection and Response Agent**。

   - 如果您以 Light Agent 模式安裝應用程式，請指定以下設定：

     應用程式模式請選擇**用於防護虛擬環境的 Light Agent**選項。

啟用 VDI 防護模式選取此核取方塊可啟用 VDI 防護模式。如果您要在用於建立暫時虛擬機的虛擬機範本上安裝該應用程式，則建議這樣做。預設情況下已清空此核取方塊。

受防護的虛擬機被用作伺服器將安裝應用程式的虛擬機的角色：伺服器或工作站。預設情況下已選擇此核取方塊。

Light Agent 模式下無法使用：

- 設定應用程式資料庫的更新來源並啟動更新
- 配置代理伺服器設定
- 應用程式啟動

以 Light Agent 模式執行的應用程式連線到 SVM 後，會從 Protection Server 接收資料庫更新和產品授權資訊。您不需要另外啟動 Kaspersky Endpoint Security 或設定資料庫更新。

- 如有必要，請管理其他初始組態設定。

  如需安裝套件中應用程式所有初始組態設定的說明，請參閱 附錄 1。

您可以稍後在已建立之安裝套件內容的 **應用程式設定** 區段中執行應用程式的初始組態。

精靈會根據卡巴斯基伺服器上的分發套件建立安裝套件。

1. 在主控台樹狀目錄中，選擇**其它** → **遠端安裝** → **安裝套件**。
2. 點擊 **其他操作** → **檢視卡巴斯基應用程式的目前版本** 按鈕。
3. 從清單中選取 Kaspersky Endpoint Security 分發套件，然後點擊 **下載並建立安裝套件** 按鈕。
4. 閱讀您與 Kaspersky 簽訂的《最終使用者產品授權協議》以及描述資料處理和傳輸的《隱私政策》。

   若要繼續，請確認您已閱讀並接受最終使用者產品授權協議和隱私權政策的完整條款。若要確認，請在確認視窗中選取兩個核取方塊，然後點擊 **全部接受** 按鈕。
5. 請等待下載完成。套件將被建立並加入到套件清單中。
6. 開啟安裝套件的內容，然後前往 **應用程式設定** 區段。

   - 如果您以 EDR Agent 模式安裝應用程式，請針對 **應用程式模式** 設定，選取 **Endpoint Detection and Response Agent**。
   - 如果您以 Light Agent 模式安裝應用程式，請指定以下設定：

     應用程式模式請選擇**用於防護虛擬環境的 Light Agent**選項。

     啟用 VDI 防護模式選取此核取方塊可啟用 VDI 防護模式。如果您要在用於建立暫時虛擬機的虛擬機範本上安裝該應用程式，則建議這樣做。預設情況下已清空此核取方塊。

     受防護的虛擬機被用作伺服器將安裝應用程式的虛擬機的角色：伺服器或工作站。預設情況下已選擇此核取方塊。

     以下設定在 Light Agent 模式下無法使用：

     - 設定應用程式資料庫的更新來源並啟動更新
     - 配置代理伺服器設定
     - 應用程式啟動

以 Light Agent 模式執行的應用程式連線到 SVM 後，會從 Protection Server 接收資料庫更新和產品授權資訊。您不需要另外啟動 Kaspersky Endpoint Security 或設定資料庫更新。

- 如有必要，請管理其他初始組態設定。

  如需安裝套件中應用程式所有初始組態設定的說明，請參閱 附錄 1。

您可以稍後在已建立之安裝套件內容的 **應用程式設定** 區段中執行應用程式的初始組態。

2 在企業網路中的裝置上安裝應用程式

您可以使用 遠端應用程式安裝工作，透過卡巴斯基安全管理中心安裝應用程式。

如有必要，您可以使用卡巴斯基安全管理中心用戶端裝置的遠端診斷來檢視應用程式遠端安裝記錄。

應用程式的初始組態會根據 安裝套件 內容中所做的設定，或安裝套件中包含的設定檔自動執行。

影片：安裝、更新資料庫以及檢查 Kaspersky Endpoint Security 的效能

3 應用程式資料庫更新

如果您已在標準模式或 EDR Agent 模式下安裝應用程式，請執行在網頁主控台或管理主控台中「設定應用程式資料庫和模組的集中式更新」步驟建立的 *更新* 群組工作（視您使用的卡巴斯基安全管理中心管理主控台而定）。如需有關更新 Kaspersky Endpoint Security 資料庫的詳細資訊，請參閱 更新應用程式資料庫和模組 區段。

4 應用程式健全狀況檢查

因此，Kaspersky Endpoint Security 應用程式已安裝並啟動，且應用程式資料庫已更新。安裝完成後，應用程式會自動啟動。預設會啟用以下元件：

- 檔案威脅防護。
- 裝置控制。

- 行為偵測。
- Web 威脅防護— 僅當作業系統中安裝了受支援的瀏覽器之一併且允許在裝置上本機管理 Web 威脅防護設定（未套用政策或未在政策屬性中設定"鎖定"）時。
- 網路威脅防護— 僅當裝置上的網路威脅防護設定是透過政策定義時。預設情況下，網路威脅防護在政策屬性中啟用。如果在裝置上套用本機配置的設定，則預設會停用網路威脅防護。

請確認應用程式已準備就緒可供使用。

如何在網頁主控台中檢查裝置的防護狀態

1. 在網頁主控台的主視窗中，選取 **資產管理 → 資產 (裝置)**。

   受管理裝置的清單將開啟。

2. 選擇包含必要裝置的管理群組。若要選取巢狀群組，請按一下視窗上方的 **顯示階層結構** 按鈕。

   此清單僅顯示選定管理群組的受管理裝置。

3. 按一下裝置名稱。

   這會開啟受管理裝置的內容視窗。

4. 在 **一般** 索引標籤上，選取 **防護** 區段。**裝置狀態** 欄位應顯示 *正常*。

   如果 **裝置狀態** 欄位顯示系統目錄權限不足的相關資訊，請在此裝置本機檢查下列目錄的權限：/var/opt/kaspersky、/var/log/kaspersky 和 /opt/kaspersky。請確定擁有者為 root，且只有擁有者具有這些目錄的寫入存取權限。

5. 前往 **應用程式** 索引標籤。

6. 在裝置上安裝的應用程式清單中，點擊 Kaspersky Endpoint Security。

   應用程式屬性視窗隨即開啟。

7. 在 **一般** 索引標籤的 **資訊** 區段中，查看 **應用程式資料庫** 下方的內容。請確定應用程式資料庫是最新狀態。

8. 前往 **一般** 索引標籤上的 **產品授權** 區段，並確認應用程式已啟動。

9. 如果您已在 EDR Agent 模式下安裝應用程式，請前往 **一般** 索引標籤上的 **元件** 區段，並確認您在「建立 Kaspersky Endpoint Security 政策」步驟中設定的整合具有 *執行中* 狀態。

10. 如果您已在 Light Agent 模式下安裝應用程式，請前往 **一般** 索引標籤上的 **元件** 區段，並確認 **用於防護虛擬環境的 Light Agent 模式** 這一行顯示狀態為 *執行中*。這表示應用程式正以 Light Agent 模式使用。

如何在管理主控台中檢查裝置的防護狀態

1. 在管理主控台樹狀圖中的**管理裝置**資料夾中，選擇包含必要裝置的管理群組。

2. 在工作區選取"**裝置**"標籤。

3. 在受管理裝置清單中，選擇所需的裝置並雙擊它以開啟**屬性：<工作名稱>**視窗。

   這會開啟受管理裝置的內容視窗。

4. 選取 **防護** 區段。**裝置狀態** 欄位應顯示 *正常/在網路中可見*。

   如果 **裝置狀態** 欄位顯示系統目錄權限不足的相關資訊，請在此裝置本機檢查下列目錄的權限：/var/opt/kaspersky、/var/log/kaspersky 和 /opt/kaspersky。請確定擁有者為 root，且只有擁有者具有這些目錄的寫入存取權限。

5. 前往 **應用程式** 區段。

6. 在裝置上安裝的應用程式清單中，選取 Kaspersky Endpoint Security 應用程式並連按兩下，以開啟應用程式內容視窗。

7. 在 **一般** 區段中查看 **應用程式資料庫** 欄位。請確定應用程式資料庫是最新狀態。

8. 前往 **產品授權金鑰** 區段，並確認應用程式已啟動。

9. 如果您已在 EDR Agent 模式下安裝應用程式，請前往 **元件** 區段，並確認您在「建立 Kaspersky Endpoint Security 政策」步驟中設定的整合具有 *執行中* 狀態。

10. 如果您已在 Light Agent 模式下安裝應用程式，請前往 **元件** 區段，並確認 **用於防護虛擬環境的 Light Agent 模式** 這一行顯示 *執行中* 狀態。這表示應用程式正以 Light Agent 模式使用。

實用文章

如果工作未執行或政策未套用，該怎麼辦

如果裝置具有以下狀態，該怎麼辦：「政策設定無效。政策尚未套用。」

錯誤：「目前版本的卡巴斯基安全管理中心網頁主控台不支援應用程式，或未安裝應用程式 Web 外掛程式」

疑難排解安裝 GUI 時的問題

安裝錯誤代碼說明

Kaspersky Endpoint Security 安裝後的錯誤

安裝 Kaspersky Endpoint Security 後，您可以返回部署情境，並從 在某些作業系統中安裝後的其他設定步驟 步驟繼續。

使用指令列安裝應用程式

安裝時的特殊注意事項：

- 配備 Elbrus CPU 的裝置不支援 Kaspersky Endpoint Security 的 EDR Agent 模式和 Light Agent 模式。
- Arm 裝置不支援 Light Agent 模式的 Kaspersky Endpoint Security。
- 您需要 root 權限才能安裝應用程式和圖形介面。
- 必須以根使用者身分執行「初始設定」精靈。
- 如果 apt 套件管理器版本低於 1.1.X，您需要使用 dpkg 套件管理器（依作業系統而定）進行安裝。

使用命令列安裝應用程式的建議方案包含以下步驟：

1 安裝 Kaspersky Endpoint Security 應用程式

在開始安裝之前，請將下載的包含應用程式主要檔案的套件放置在裝置上的 /tmp 目錄中。

如何從 RPM 套件安裝應用程式

在 32 位元作業系統上

```
yum install kesl-12.5.0-<build number>.i386.rpm
```

在 64 位元作業系統上

```
yum install kesl-12.5.0-<build number>.x86_64.rpm
```

在 64 位元 ALT 作業系統上

```
apt-get install kesl-12.5.0-<build number>.x86_64.rpm
```

在 Arm 架構的 64 位元作業系統上

```
yum install kesl-12.5.0-<build number>.aarch64.rpm
```

在 Arm 架構的 64 位元 ALT 作業系統上

```
apt-get install kesl-12.5.0-<build number>.aarch64.rpm
```

在 Elbrus 架構的 64 位元作業系統上

```
yum install kesl-12.5.0-<build number>.2ek.rpm
```

在 Elbrus 架構的 64 位元 ALT 作業系統上

```
apt-get install kesl-12.5.0-<build number>.2ek.rpm
```

在支援有限的 64 位元作業系統上（CentOS 5.2、CentOS 5.4、CentOS 6.4、CentOS 6.6）

```
rpm -i kesl-12.5.0-<build number>.x86_64.rpm
```

若要在 CentOS 5.2、CentOS 5.4、CentOS 6.4 或 CentOS 6.6 上安裝應用程式，您需要從網站下載標示為 OLD 的發行套件。

如何從 DEB 套件安裝應用程式

在 32 位元作業系統上

```
apt-get install ./kesl_12.5.0-<build number>_i386.deb
```

在 64 位元作業系統上

```
apt-get install ./kesl_12.5.0-<build number>_amd64.deb
```

在 Arm 架構的 64 位元作業系統上

```
apt-get install ./kesl_12.5.0-<build number>_arm64.deb
```

在 Elbrus 架構的 64 位元作業系統上

```
apt-get install ./kesl_12.5.0-<build number>_2ek.deb
```

2 安裝應用程式的圖形介面

如果您想要使用圖形介面管理應用程式，您需要將圖形介面安裝在與應用程式相同的裝置上。

應用程式圖形介面的特殊功能：

- 您無法在未安裝 Kaspersky Endpoint Security 應用程式的裝置上安裝圖形介面。
- 如果應用程式以 Light Agent 模式使用，則不支援圖形使用者介面。

在開始安裝之前，請將下載的包含應用程式圖形介面檔案的套件放置在裝置上的 /tmp 目錄中。

如何從 RPM 套件安裝應用程式的圖形介面

在 32 位元作業系統上

```
yum install kesl-gui-12.5.0-<build number>.i386.rpm
```

在 64 位元作業系統上

```
yum install kesl-gui-12.5.0-<build number>.x86_64.rpm
```

在 64 位元 ALT 作業系統上

```
apt-get install kesl-gui-12.5.0-<build number>.x86_64.rpm
```

在 Arm 架構的 64 位元作業系統上

```
yum install kesl-gui-12.5.0-<build number>.aarch64.rpm
```

在 Arm 架構的 64 位元 ALT 作業系統上

```
apt-get install kesl-gui-12.5.0-<build number>.aarch64.rpm
```

在 Elbrus 架構的 64 位元作業系統上

```
yum install kesl-gui-12.5.0-<build number>.2ek.rpm
```

在 Elbrus 架構的 64 位元 ALT 作業系統上

```
apt-get install kesl-gui-12.5.0-<build number>.2ek.rpm
```

在支援有限的 64 位元作業系統上（CentOS 6.4、CentOS 6.6）

```
rpm -i kesl-gui-12.5.0-<build number>.x86_64.rpm
```

若要在 CentOS 6.4 或 CentOS 6.6 上安裝應用程式，您需要從網站下載標示為 OLD 的發行套件。

如何從 DEB 套件安裝應用程式的圖形介面

在 32 位元作業系統上

```
apt-get install ./kesl-gui_12.5.0-<build number>_i386.deb
```

在 64 位元作業系統上

```
apt-get install ./kesl-gui_12.5.0-<build number>_amd64.deb
```

在 Arm 架構的 64 位元作業系統上

```
apt-get install ./kesl-gui_12.5.0-<build number>_arm64.deb
```

在 Elbrus 架構的 64 位元作業系統上

```
apt-get install ./kesl-gui_12.5.0-<build number>_2ek.deb
```

3 應用程式的初始設定

應用程式需要初始配置以準備運行並啟用用戶端裝置的防護。

如果應用程式在裝置上的初始配置尚未完成，則您無法在該裝置上使用或更新應用程式。

應用程式的初始設定使用 Kaspersky Endpoint Security 發行套件中的初始設定精靈執行。您可以在互動模式或自動模式下執行初始設定。

如何以互動方式執行應用程式的初始設定。

步驟 1. 啟動精靈

啟動初始設定精靈

```
/opt/kaspersky/kesl/bin/kesl-setup.pl
```

依照精靈的提示，逐步指定 Kaspersky Endpoint Security 初始設定的參數值。

如果裝置上已安裝網路代理，且您正以標準模式或 EDR Agent 模式安裝應用程式，則可以略過初始設定精靈中與更新應用程式資料庫和啟動應用程式相關的步驟。

步驟 2. 選擇標準模式或 Light Agent 模式

輸入 yes 以 Light Agent 模式使用應用程式。

輸入 no 以標準模式使用應用程式。

如果您打算以 EDR Agent 模式使用應用程式，在此步驟中，您需要輸入 no，並在下一步選擇 EDR Agent 模式。

初始配置完成後，您無法變更應用程式使用模式。

步驟 3. 選擇模式：標準模式或 Endpoint Detection and Response Agent

如果您在步驟 2 選擇以標準模式使用應用程式，則會顯示此步驟。

輸入 yes 以 EDR Agent 模式使用應用程式。

輸入 no 以標準模式使用應用程式。

初始配置完成後，您無法變更應用程式使用模式。

步驟 4. Kaspersky Endpoint Detection and Response Expert (cloud) 整合

如果您在步驟 3 選擇以標準模式使用應用程式，則會顯示此步驟。

輸入 yes 以使用 Kaspersky Endpoint Detection and Response Expert (cloud) 整合。

輸入 no 以使用 Kaspersky Endpoint Detection and Response Expert (on-premises) 整合。

步驟 5. 選擇虛擬機的角色

如果您在步驟 2 選擇以 Light Agent 模式使用應用程式，則會顯示此步驟。

指定您要安裝 Kaspersky Endpoint Security 的虛擬機（伺服器或工作站）的角色：

- 如果您使用虛擬機作為伺服器，請輸入 yes 。
- 如果您使用虛擬機作為工作站，請輸入 no 。

虛擬機的角色決定了應用程式在此虛擬機上使用的產品授權以及可用的功能。

步驟 6. 啟用 VDI 防護模式

如果您在步驟 2 選擇以 Light Agent 模式使用應用程式，則會顯示此步驟。

VDI 防護模式可最佳化 Kaspersky Endpoint Security 在暫時虛擬機上的運作。如果啟用了 VDI 防護模式，則不會安裝需要重新啟動虛擬機的更新。當收到需要重新啟動的更新時，安裝在虛擬機上的 Light Agent 會向卡巴斯基安全管理中心傳送一則訊息，提示需要更新受防護的虛擬機範本。

如果要啟用 VDI 防護模式，請指定 yes 。如果您要在用於建立暫時虛擬機的虛擬機範本上安裝 Kaspersky Endpoint Security，則建議這樣做。

如果不想啟用 VDI 防護模式，請指定 no 。如果您要在持久虛擬機或用於建立持久虛擬機的虛擬機範本上安裝 Kaspersky Endpoint Security，建議這樣做。

步驟 7. 選擇區域設定

在此步驟中，精靈會以 RFC 3066 格式顯示支援的區域設定清單。

請依照此處所列指定區域設定。此區域設定用於以下目的：

- 將安裝期間顯示的《最終使用者產品授權協議》、《隱私權政策》及《卡巴斯基安全網路聲明》文字本地化。
- 將傳送到卡巴斯基安全管理中心的應用程式事件本地化。

> 圖形介面和應用程式指令列的區域設定取自 LANG 環境變數。如果應用程式不支援此本地化，則預設為英語本地化。

步驟 8. 檢視最終使用者產品授權協議和隱私權政策

在此步驟中，請閱讀您與卡巴斯基簽訂的《最終使用者產品授權協議》，以及說明資料處理和傳輸的《隱私權政策》。

步驟 9. 接受最終使用者產品授權協議

結束檢視模式後，輸入以下值之一：

- yes（或y），如果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，則為 no（或n）。

如果您不接受《最終使用者產品授權協議》的條款和條件，Kaspersky Endpoint Security 安裝處理程序將終止。

步驟 10. 接受隱私權政策

結束檢視模式後，輸入以下值之一：

- yes（或y），如果您接受隱私權政策的條款。
- 如果您不接受隱私權政策的條款，則為no（或n）。

如果您不接受《隱私權政策》的條款和條件，Kaspersky Endpoint Security 安裝處理程序會中止。

步驟 11. 使用卡巴斯基安全網路

在此步驟中，請接受或拒絕 卡巴斯基安全網路 的使用條款：

- 如果您接受《卡巴斯基安全網路聲明》的條款和條件，請輸入 yes（或 y）。這將啟用延伸 KSN 模式。
- 如果您不接受《卡巴斯基安全網路聲明》的條款和條件，請輸入 no（或 n）。

檔案 ksn_license.<語言 ID> 包含卡巴斯基安全網路聲明文字，位於目錄 /opt/kaspersky/kesl/doc/ 中。

拒絕加入卡巴斯基安全網路不會中斷 Kaspersky Endpoint Security 的初始配置。您可以隨時啟用、停用或變更卡巴斯基安全網路模式。

如果啟用卡巴斯基安全網路，將自動啟用雲端模式，Kaspersky Endpoint Security 會在此模式下使用輕量版的惡意軟體資料庫。

步驟 12. 從特權群組中刪除使用者

如果在 kesladmin 和/或 keslaudit 群組中偵測到使用者，則會顯示此步驟。

指定是否要從 kesladmin 和 keslaudit 特權群組中移除使用者。kesladmin 和 keslaudit 群組中的使用者有權存取該應用程式的功能。

輸入yes從 kesladmin 和/或 keslaudit 群組中刪除所有偵測到的使用者。主要群組為 kesladmin 或 keslaudit 的使用者將被移至 nogroup 群組。如果沒有 nogroup 群組，安裝將會失敗，您會被提示手動從特權使用者群組中刪除使用者。

如果您不希望應用程式從特權群組中刪除使用者，請輸入no。

步驟 13. 為使用者指派管理員角色

在此步驟中，精靈會提示您授予管理員 角色 (admin)。

輸入您想要授予管理員角色的使用者的名稱。必須具備管理員角色才能在不使用 sudo 命令的情況下，在應用程式的圖形介面和命令列中管理應用程式設定與工作設定。

完成初始設定後，您可以稍後將管理員角色指派給使用者。

步驟 14.設定系統事件攔截機制

如果作業系統符合安裝要求，則應用程式可以使用基於可更新的內核模組的攔截機制。如果作業系統不符合這些要求但支援 fanotify 技術，則應用程式會使用 fanotify 來攔截系統事件。如果作業系統不支援 fanotify 技術，則應用程式將編譯並使用特殊的內核模組來攔截檔案威脅防護的系統事件。如果已安裝所有必要套件，則在檔案威脅防護啟動時，將自動開始編譯內核模組。如果無法在裝置上找到任何依賴項，Kaspersky Endpoint Security 應用程式會建議安裝相關套件。如果套件下載失敗，則會顯示錯誤訊息。

- 若想使用可更新的內核模組，請輸入 yes。
- 若想使用 fanotify，請輸入 no。

如果選取可更新的內核模組作為攔截機制，請指定以下設定：

- 如果可更新的內核模組未能啟動，應用程式會採取的動作：
  - 如果想要應用程式在可更新的內核模組啟動失敗時回退到使用 fanotify 進行系統事件攔截，請輸入 yes。
  - 如果想要應用程式在可更新的內核模組啟動失敗時繼續執行而不進行系統事件攔截，請輸入 no。

    如果應用程式不使用系統事件攔截，則不會執行即時檔案掃描，並且裝置的保護等級會降低。

- 切換到使用可更新的內核模組時的應用程式重新啟動模式。要執行該模組，必須自動或手動重新啟動應用程式。

  我們建議自動重新啟動應用程式以切換到使用可更新的內核模組。重新啟動應用程式後手動啟動可更新的內核模組可能會導致應用程式錯誤。

如果想要允許自動重新啟動應用程式來執行模組，請輸入 yes。

步驟 15. 啟用 SELinux 的自動配置

如果您的作業系統中安裝了 SELinux 存取控制系統，則會顯示此步驟。

請輸入 yes 以自動設定 SELinux，使其與 Kaspersky Endpoint Security 搭配使用。如果應用程式無法自動設定 SELinux（例如，缺少 semanage 實用程式），精靈會顯示錯誤訊息並提示使用者手動設定 SELinux。

如果您不想執行 SELinux 系統的自動設定，請輸入 no。

預設情況下，精靈建議使用 yes。

如有必要，您可以在完成應用程式的初始設定後，稍後手動設定 SELinux 以與應用程式搭配使用。

步驟 16.設定更新來源

如果您以標準模式或 EDR Agent 模式安裝 Kaspersky Endpoint Security，則會顯示此步驟。

指定資料庫和應用程式模組的更新來源。應用程式資料庫包含威脅特徵的描述及其應對方法。應用程式在搜尋和消除威脅時使用這些記錄。卡巴斯基病毒分析師會定期新增關於威脅的新記錄。

輸入以下值之一：

- `KLServers` – 應用程式從其中一個卡巴斯基更新伺服器接收更新。
- `SCServer` – 應用程式從您組織中安裝的卡巴斯基安全管理中心伺服器下載更新到受防護裝置。如果您使用卡巴斯基安全管理中心集中管理組織中的裝置防護，則可以選擇此更新來源。
- `Custom`：應用程式從自訂來源下載更新。您可以將自訂更新來源的位址指定為本機目錄（例如 /home/databases）或遠端 HTTP 或 HTTPS 伺服器（例如 http://example.com/databases/）。

步驟 17. 設定代理伺服器設定

如果您以標準模式或 EDR Agent 模式安裝 Kaspersky Endpoint Security，則會顯示此步驟。

如果您使用代理伺服器連線至網際網路，請以下列格式之一輸入代理伺服器的位址：

- `[<connection protocol>://]<address of proxy server>:<port>`，如果連線到代理伺服器不需要身分驗證；
- `[<connection protocol>://][<user name>:<password>@]<address of proxy server>:<port>`，如果連線到代理伺服器需要身分驗證。指定 IPv6 位址時，請將其輸入方括號中。

> 不支援透過 HTTPS 連線到代理伺服器。透過 HTTP 代理連線時，我們建議使用不用於登入其他系統的單獨帳戶。HTTP 代理程式使用不安全的連線，帳戶可能會受到損害。

如果您不使用代理伺服器，請輸入 no。

預設情況下，應用程式建議no。

完成初始設定後，您可以稍後管理代理伺服器設定。

步驟 18. 開始應用程式資料庫更新

如果您以標準模式或 EDR Agent 模式安裝 Kaspersky Endpoint Security，則會顯示此步驟。

在此步驟中，精靈會提示您在安裝後立即在用戶端裝置上執行應用程式資料庫更新工作。

如果您不想開始下載應用程式資料庫，請輸入no。

預設情況下，精靈建議使用 `yes`。

如果選擇`yes`，則資料庫更新後應用程式將自動重新啟動。

> 只有當應用程式資料庫更新後，Kaspersky Endpoint Security 才會防護裝置。

完成初始設定後，您可以稍後執行更新工作。

步驟 19. 啟用應用程式資料庫自動更新

如果您以標準模式或 EDR Agent 模式安裝 Kaspersky Endpoint Security，則會顯示此步驟。

輸入 yes 以啟用應用程式資料庫自動更新。預設情況下，應用程式每 60 分鐘檢查一次可用的資料庫的更新。如果有更新可用，應用程式將下載更新的資料庫。

如果您不希望應用程式自動更新資料庫，請輸入 no。

完成初始設定後，您可以透過設定更新工作排程稍後啟用自動資料庫更新。

步驟 20.應用程式啟動

如果您以標準模式或 EDR Agent 模式安裝 Kaspersky Endpoint Security，則會顯示此步驟。

如果您想要在安裝後立即啟動應用程式，請輸入啟動碼或指定金鑰檔案的完整路徑。

> 如果未指定啟動碼或金鑰檔案，則應用程式使用試用金鑰來啟動一個月。

完成初始化設定後，您可以稍後啟動應用程式。

如何在自動模式下執行初始設定

1. 建立包含初始設定的設定檔。您可以從 autoinstall.ini 設定檔複製設定，該設定檔用於透過卡巴斯基安全管理中心遠端安裝應用程式，並視需要進行變更。

2. 在設定檔中指定以下必要設定：

   - 接受最終使用者產品授權協議 (EULA) 和隱私權政策：

     `EULA_AGREED=Yes`

     `PRIVACY_POLICY_AGREED=Yes`

     您可以在應用程式發佈套件中隨附的 license.<language ID> 檔案中閱讀最終使用者產品授權協議和隱私權政策的條款和條件：

     > 如果您不接受最終使用者產品授權協議和隱私權政策的條款和條件，安裝程序將中止。

   - 卡巴斯基安全網路應用程式預設以標準模式使用。

     若要以 EDR Agent 模式使用應用程式，請指定以下設定：

     `ENDPOINT_AGENT_MODE=Yes`

     若要以 Light Agent 模式使用應用程式，請指定以下設定：

     `KSVLA_MODE=Yes`

   - 使用卡巴斯基安全網路。接受或拒絕卡巴斯基安全網路的使用條款：

     `USE_KSN=Yes|No`

     檔案 ksn_license.<語言 ID> 包含卡巴斯基安全網路聲明文字，位於目錄 /opt/kaspersky/kesl/doc/ 中。如果您接受卡巴斯基安全網路聲明的條款和條件，將啟用延伸 KSN 模式。您可以隨時啟用、停用或變更卡巴斯基安全網路模式。

     > 如果啟用卡巴斯基安全網路，將自動啟用雲端模式，Kaspersky Endpoint Security 會在此模式下使用輕量版的惡意軟體資料庫。

- 安裝應用程式之前，自動從 kesladmin 和 keslaudit 特權群組中移除使用者：

  `GROUP_CLEAN=Yes|No`

3. 選擇 Kaspersky Endpoint Security 使用的系統事件攔截機制。如果您想要使用可更新的內核模組攔截系統事件，請設定以下值：

   `INTERCEPTOR_MODE=UseUpdatableKernelModule`

   預設情況下，會使用 fanotify 技術來攔截系統事件。

4. 如果您要以標準模式或 EDR Agent 模式安裝應用程式，請指定以下設定：

   - 代理伺服器設定。如果您使用代理伺服器連線至網際網路，請以下列格式之一輸入代理伺服器的位址：

     - `PROXY_SERVER=[<connection protocol>://]<address of proxy server>:<port>`，如果連線到代理伺服器不需要身分驗證；

     - `PROXY_SERVER=[<connection protocol>://][<user name>:<password>@]<address of proxy server>:<port>`，如果連線到代理伺服器需要身分驗證。指定 IPv6 位址時，請將其輸入方括號中。

     > 不支援透過 HTTPS 連線到代理伺服器。

   - 安裝並使用應用程式的圖形介面：

     `USE_GUI=Yes|No`

5. 如果您以 Light Agent 模式安裝應用程式，請指定以下設定：

   - 受防護的虛擬機的角色：

     - `SERVER_MODE=Yes`，如果受防護的虛擬機用作伺服器。

     - `SERVER_MODE=No`，如果受防護的虛擬機用作工作站。

   - 啟用 VDI 防護模式以最佳化暫時虛擬機上的應用程式效能。如果您要在虛擬機範本上安裝應用程式，且將從該範本建立暫時虛擬機，請設定下列值：

     `VDI_MODE=Yes`

6. 啟動初始設定精靈：

   ```
   /opt/kaspersky/kesl/bin/kesl-setup.pl --autoinstall=<initial configuration file>
   ```

   其中 `<initial configuration file>` 是包含初始設定的設定檔路徑。

當「初始設定」精靈完成並釋放主控台後，應用程式的安裝後設定就完成了。

檢查傳回碼

```
echo $?
```

如果命令傳回 0，則應用程式的安裝後設定已成功完成。

4 應用程式健全狀況檢查

因此，Kaspersky Endpoint Security 應用程式已安裝並啟動，且應用程式資料庫已更新。安裝完成後，應用程式會自動啟動。預設會啟用以下元件：

- 檔案威脅防護。
- 裝置控制。
- 行為偵測。
- Web 威脅防護— 僅當作業系統中安裝了受支援的瀏覽器之一併且允許在裝置上本機管理 Web 威脅防護設定（未套用政策或未在政策屬性中設定"鎖定"）時。
- 網路威脅防護— 僅當裝置上的網路威脅防護設定是透過政策定義時。預設情況下，網路威脅防護在政策屬性中啟用。如果在裝置上套用本機配置的設定，則預設會停用網路威脅防護。

檢查標準模式下裝置的防護狀態

若要檢查裝置的防護狀態，請執行下列命令：

```
kesl-control --app-info [--json]
```

其中 `--json` 表示以 JSON 格式輸出資料。如果不指定`--json`選項，設定將被輸出到主控台。

請確定：

- 應用程式已啟動（**應用程式產品授權資訊** 行）。
- 應用程式資料庫為最新（**應用程式資料庫已加載** 和 **資料庫的上次發佈日期** 行）。
- 已啟用檔案威脅防護（**檔案威脅防護** 行）。
- **應用程式狀態** 行會顯示 OK。

  如果 **應用程式狀態** 行顯示有關系統目錄權限不足的資訊，請在此裝置本機檢查下列目錄的權限：/var/opt/kaspersky、/var/log/kaspersky 和 /opt/kaspersky。請確定擁有者為 root，且只有擁有者具有這些目錄的寫入存取權限。

檢查 EDR Agent 模式下裝置的防護狀態

若要檢查裝置的防護狀態，請執行下列命令：

```
kesl-control --app-info [--json]
```

其中 `--json` 表示以 JSON 格式輸出資料。如果不指定`--json`選項，設定將被輸出到主控台。

請確定：

- 應用程式已啟動（**EDR Expert (on-premises) 產品授權資訊** 行）
- 應用程式資料庫為最新（**應用程式資料庫已加載** 和 **資料庫的上次發佈日期** 行）。
- 應用程式是以 EDR Agent 模式使用（**Endpoint Detection and Response Agent 模式** 行）。
- 針對您在政策中設定的整合，會顯示「可用且正在執行」狀態。

- **應用程式狀態** 行會顯示 OK。

  如果 **應用程式狀態** 行顯示有關系統目錄權限不足的資訊，請在此裝置本機檢查下列目錄的權限：/var/opt/kaspersky、/var/log/kaspersky 和 /opt/kaspersky。請確定擁有者為 root，且只有擁有者具有這些目錄的寫入存取權限。

檢查 Light Agent 模式下裝置的防護狀態

1. 執行以下指令：

   ```
   kesl-control --ksvla-info
   ```

   請確定應用程式是以 Light Agent 模式使用（**用於防護虛擬環境的 Light Agent 模式** 行）。

2. 如果您已在政策中選取 Integration Server 以偵測可供連線的 SVM，請執行下列命令：

   ```
   kesl-control --viis-info
   ```

   請確定 Light Agent 已連線至 Integration Server（**Integration Server 連線狀態** 行）。

3. 執行以下指令：

   ```
   kesl-control --svm-info
   ```

   請確定 Light Agent 已連線至 SVM：會顯示已建立連線的 SVM 相關資訊。

4. 執行以下指令：

   ```
   kesl-control --app-info [--json]
   ```

   其中 `--json` 表示以 JSON 格式輸出資料。如果不指定`--json`選項，設定將被輸出到主控台。

   請確定：

   - Light Agent 會接收用於啟動 Kaspersky Security for Virtualization Light Agent 的產品授權相關資訊（**應用程式產品授權資訊** 行）。
   - 應用程式資料庫為最新（**應用程式資料庫已加載** 和 **資料庫的上次發佈日期** 行）。
   - **應用程式狀態** 行會顯示 OK。

     如果 **應用程式狀態** 行顯示有關系統目錄權限不足的資訊，請在此裝置本機檢查下列目錄的權限：/var/opt/kaspersky、/var/log/kaspersky 和 /opt/kaspersky。請確定擁有者為 root，且只有擁有者具有這些目錄的寫入存取權限。

實用文章

如果工作未執行或政策未套用，該怎麼辦

如果裝置具有以下狀態，該怎麼辦：「政策設定無效。政策尚未套用。」

錯誤：「目前版本的卡巴斯基安全管理中心網頁主控台不支援應用程式，或未安裝應用程式 Web 外掛程式」

疑難排解安裝 GUI 時的問題

安裝錯誤代碼說明

Kaspersky Endpoint Security 安裝後的錯誤

安裝 Kaspersky Endpoint Security 後，您可以返回部署情境，並從 在某些作業系統中安裝後的其他設定步驟 步驟繼續。

在某些作業系統中安裝後的額外設定步驟

在為安裝 Kaspersky Endpoint Security 準備環境並安裝應用程式後，某些作業系統需要額外設定。

手動配置 SELinux 以與應用程式配合使用

如果您的作業系統在 `Enforcing` 模式下使用 SELinux 存取控制系統，則在安裝期間，預設會自動將其設定為與應用程式搭配使用。

如果應用程式無法自動設定 SELinux（例如，缺少 semanage 公用程式），精靈會顯示錯誤訊息，並提示使用者手動設定 SELinux。在此情況下，或如果您拒絕自動設定，請在完成應用程式的初始設定後，手動設定 SELinux 系統以與 Kaspersky Endpoint Security 應用程式搭配使用。

此設定需要 root 權限。

若要手動配置 SELinux 以與應用程式配合使用：

1. 將 SELinux 切換到權限模式：
   - 如果已啟用 SELinux，請執行以下指令：

     ```
     setenforce Permissive
     ```

   - 如果已停用 SELinux，請在 /etc/selinux/config 設定檔中設定 `SELINUX=permissive`，然後重新啟動作業系統。
2. 確保系統上安裝了 semanage 實用程式。如果未安裝該實用程式，請根據套件管理器安裝 policycoreutils-python 或 policycoreutils-python-utils 套件。
3. 如果您使用自訂 SELinux 政策，而不是預設的 'targeted' 政策，請根據您的 SELinux 政策，為每個原始 Kaspersky Endpoint Security 可執行檔指派標籤。

   ```
   semanage fcontext -a -t bin_t <executable file>
   restorecon -v <executable file>
   ```

   其中 `<executable file>` 為：

   - /var/opt/kaspersky/kesl/<內部版本號_*>/opt/kaspersky/kesl/libexec/kesl
   - /var/opt/kaspersky/kesl/<內部版本號_*>/opt/kaspersky/kesl/bin/kesl-control
   - /var/opt/kaspersky/kesl/<內部版本號_*>/opt/kaspersky/kesl/libexec/kesl-gui

- /var/opt/kaspersky/kesl/<內部版本號_*>/opt/kaspersky/kesl/shared/kesl
- /var/opt/kaspersky/kesl/<內部版本號_*>/opt/kaspersky/kesl/bin/response

4. 執行以下工作：

執行檔案威脅防護工作

```
kesl-control --start-task 1
```

執行關鍵區域掃描工作

```
kesl-control --start-task 4 -W
```

建議您執行未來打算執行的所有 Kaspersky Endpoint Security 工作。

5. 如果您打算使用圖形使用者介面，請啟動它。
6. 請確保 audit.log 檔案中沒有錯誤。

檢視 audit.log 檔案

```
grep kesl /var/log/audit/audit.log
```

7. 如果 audit.log 檔案中有錯誤，請根據封鎖記錄建立並下載新的規則模組以修復錯誤，然後重新啟動您日後計劃執行的所有工作。

根據封鎖記錄建立並載入新的規則模組：

```
grep kesl /var/log/audit/audit.log | audit2allow -M kesl
semodule -i kesl.pp
```

如果出現與 Kaspersky Endpoint Security 相關的新稽核訊息，則必須更新包含規則模組檔案的檔案。

8. 將 SELinux 切換為強制模式。

```
setenforce Enforcing
```

如果您使用自訂 SELinux 政策，請在安裝應用程式更新後手動為 Kaspersky Endpoint Security 來源可執行檔指派標籤（依照步驟 1、3-8 操作）。

您可以在作業系統的文件中找到更多資訊。

設定 SELinux 以進行回應操作

如果您計劃在作業系統上以 `Enforcing` 模式使用 SELinux，則若要在與 Detection and Response 解決方案整合時執行回應操作，您需要另外管理 SELinux 設定。

此 SELinux 設定需要 root 權限。

若要設定 SELinux 以執行回應操作：

1. 將 SELinux 切換到權限模式：

   - 如果已啟用 SELinux，請執行以下指令：

     將 SELinux 切換為寬容模式

     ```
     setenforce Permissive
     ```

   - 如果已停用 SELinux，請在 /etc/selinux/config 設定檔中設定 `SELINUX=permissive`，然後重新啟動作業系統。

2. 確保系統上安裝了 semanage 實用程式。如果未安裝該實用程式，請根據套件管理器安裝 policycoreutils-python 或 policycoreutils-python-utils 套件。

3. 請執行所有工作，以執行您要在與 Detection and Response 解決方案整合時使用的回應操作。

4. 若要使用「取得記憶體傾印」工作和「取得處理程序記憶體傾印」工作收集鑑識資料，請在 SELinux 中允許 Kaspersky Endpoint Security 應用程式存取工作中指定的 SMB 伺服器。

5. 請確保 audit.log 檔案中沒有錯誤。

   檢視 audit.log 檔案

   ```
   grep kesl /var/log/audit/audit.log
   ```

6. 如果 audit.log 檔案中有任何錯誤，請根據封鎖記錄建立並載入新的規則模組以修復錯誤，然後再次執行回應操作工作。

   根據封鎖記錄建立並載入新的規則模組：

   ```
   grep kesl /var/log/audit/audit.log | audit2allow -M kesl
   semodule -i kesl.pp
   ```

7. 將 SELinux 切換為強制模式。

   ```
   setenforce Enforcing
   ```

在 OSnova 作業系統中設定應用程式啟動

安裝應用程式後，請按照以下步驟設定應用程式及其圖形介面的啟動：

1. 開啟 `/etc/NESS/systemd/kesl.service.config` 檔案並設定 `NESSCTX_MODIFY="t+ADDEQUSOCK,OMIT,OMIT_PID,SSUID_SAVE_CTX_PERMANENT"`。

2. 開啟 `/etc/sysctl.d/30-disable-ptrace.conf` 檔案並設定 `kernel.yama.ptrace_scope=0`。`kernel.yama.ptrace_scope` 參數的其他值可能會影響 Kaspersky Endpoint Security 應用程式的運作；如需詳細資訊，請參閱已知問題與限制一節。

3. 如果您想要執行處理程序記憶體和核心記憶體掃描，您需要停用核心中的 mprotect（或 PaX）記憶體保護機制。若要執行此操作，請將 `mprotect=off` 選項新增至核心的命令列。更多詳細資訊請參閱OSnova 文件。

4. 重新啟操作業系統。

設定在封閉軟體環境模式下於 ALT SP 上啟動應用程式

安裝應用程式後，請按照以下步驟啟動應用程式：

1. 為 Kaspersky Endpoint Security 的可更新元件指派 kesl 群組和目錄權限的繼承：

```
cd /var/opt/kaspersky/kesl/<build number_*>/var/opt/kaspersky/kesl/private
chown -R root:kesl updates/
find updates -type d -exec chmod g+s {} \;
cd /opt/kaspersky/kesl/lib64
chown -R root:kesl updatable_modules/
find updatable_modules -type d -exec chmod g+s {} \;
cd /var/opt/kaspersky/kesl/common/
chown -R root:kesl temp/
find temp -type d -exec chmod g+s {} \;
```

2. 為網路代理的可更新元件指派 kesl 群組和目錄權限的繼承：

```
cd /var/opt/kaspersky/
chown -R root:kesl klnagent/
find klnagent/ -type d -exec chmod g+s {} \;
cd /opt/kaspersky/
chown -R root:kesl klnagent64/
find klnagent64/ -type d -exec chmod g+s {} \;
```

3. 透過啟動系統簽署來啟用封閉軟體環境模式：

```
integrity-applier -i -A
```

4. 確認 IMA 子系統已啟用：

```
cat /proc/cmdline
```

此指令的輸出應包含 `lsm=integrity ima_hash=sha512 ima_appraise=enforce` 行。

5. 執行資料庫更新工作：

```
kesl-control --start 6 -W
```

如果資料庫更新工作的輸出包含 *EventType=BasesApplied* 事件，表示資料庫更新已正確執行。

6. 重新啟動應用程式：

```
systemctl restart kesl
```

使用快速安裝指令碼移轉至卡巴斯基安全管理中心 Linux 的情境

此方案包含以下將解決方案及其資料遷移至新管理伺服器裝置的使用案例範例：

- 從 Kaspersky Security Center Windows (MS SQL 和 PostgreSQL) 遷移至 Kaspersky Security Center Linux (PostgreSQL)。
- 為更換硬體而遷移 Kaspersky Security Center Linux (PostgreSQL)。

新的管理伺服器會使用快速安裝指令碼進行部署。

其他資料傳輸方式請參閱「移轉至卡巴斯基安全管理中心 Linux」一節。

1 建立備份副本的先決條件

此步驟包含準備先前已設定的管理伺服器以供後續遷移至新的 Kaspersky Security Center Linux 管理伺服器的說明。準備程序包含以下步驟：

1. 檢查管理伺服器的版本，以建立與 Kaspersky Security Center Linux 相容的備份副本。

   所有目前版本的 **Kaspersky Security Center Linux** 均支援在將應用程式升級至較新版本的同時進行資料遷移。備份副本只能在相同 DBMS 類型內建立和還原。

   對於 **Kaspersky Security Center Windows**，您需要在 **內容 → 一般 → 版本** 中檢查管理伺服器的版本。如果版本早於 15.1.0.22239，請將卡巴斯基安全管理中心 Windows 升級至最新版本。

   將卡巴斯基安全管理中心 Windows 升級至最新版本。

   1. 在 卡巴斯基網站 上，下載與已安裝管理伺服器的本地化語言相符的分發套件：`Version 15.1.0.22239 | Windows | Full distributive`。

      可執行檔會以以下名稱儲存到 **下載** 資料夾：`ksc_15.1_<build number>_full_<language>.exe`。

   2. 將分發套件複製到管理伺服器。
   3. 以管理員身分執行 `ksc_15.1_<build number>_full_<language>.exe` 可執行檔。
   4. 在顯示的視窗中，按一下 **安裝卡巴斯基安全管理中心** 連結。

      管理伺服器安裝精靈會啟動。

   5. 檢閱最終使用者產品授權協議和隱私權政策的條款。如果您同意最終使用者產品授權協議和隱私權政策的所有條款和條件，請在 **本人確認已完整閱讀、理解並接受以下條款和條件** 區段中選取以下核取方塊：

      - **該 EULA 的條款和條件**
      - **描述資料處理的隱私政策**

   6. 選取 **升級管理伺服器和網頁型主控台（建議）**，然後前往下一步。

7. 若要建立新的備份副本，請選取 **我要建立資料備份副本** 選項，並遵循備份精靈的步驟。

8. 點擊“**升級**”。

9. 在升級期間，於網頁主控台安裝精靈中，確認升級版本的所有步驟。

   管理伺服器升級的安裝將需要一些時間。安裝精靈完成後，在資料庫初始化完成之前，管理主控台可能不會接受連線。

10. 請等待升級完成。

2. 驗證是否符合管理伺服器憑證的要求。

   在建立備份副本之前，您需要確保憑證包含 Subject Alternative Name (SAN)。如果不包含，請務必取代憑證，否則從備份還原後將無法登入網頁主控台。

   若要驗證憑證是否包含主體替代名稱：

   - 對於執行 Windows 的裝置：

     a. 在管理主控台中，選取您要檢查的管理伺服器。

     b. 在內容功能表中，選取 **內容 → 一般 → 檢視管理伺服器憑證**。

     c. 這會開啟一個視窗；請在該視窗中檢查 **主體替代名稱** 項目的值。

   - 對於 Linux 裝置，執行以下命令：

     ```
     sudo openssl x509 -in /var/opt/kaspersky/klnagent_srv/1093/cert/klserver.cer -noout -ext subjectAltName
     ```

   確保主體替代名稱包含管理伺服器裝置的網域名稱 (DNS)。

   如果該值僅包含外部 IP 位址而沒有網域名稱 (DNS)，或完全缺少該值，請手動將憑證取代為符合卡巴斯基安全管理中心 Linux 要求的憑證。使用 klsetsrvcert 公用程式取代管理伺服器的通用憑證。

   使用 klsetsrvcert 公用程式取代管理伺服器的通用憑證

   1. 透過執行以下命令，在裝置上建立具有延遲開始日期的新憑證：

      - 對於卡巴斯基安全管理中心 Windows：

        ```
        "%ProgramFiles(x86)%\Kaspersky Lab\Kaspersky Security Center\klsetsrvcert.exe" -t CR -g "
        <oldksc.example.internal>" -o "RsaKeyLen:2048"
        ```

      - 對於卡巴斯基安全管理中心 Linux：

        ```
        /opt/kaspersky/ksc64/sbin/klsetsrvcert -t CR -g "<oldksc.example.internal>" -o "RsaKeyLen:2048"
        ```

      其中 `"<oldksc.example.internal>"` 是用於連線至管理伺服器的 FQDN。

      > 此值請勿使用 IP 位址。

2. 透過執行以下命令，為所有裝置上的新憑證設定開始日期：

   - 對於卡巴斯基安全管理中心 Windows：

     ```
     "%ProgramFiles(x86)%\Kaspersky Lab\Kaspersky Security Center\klsetsrvcert.exe" -f "DD-MM-YYYY hh:mm"
     ```

   - 對於卡巴斯基安全管理中心 Linux：

     ```
     /opt/kaspersky/ksc64/sbin/klsetsrvcert -f "DD-MM-YYYY hh:mm"
     ```

   其中 `"DD-MM-YYYY hh:mm"` 是比目前日期至少晚 30 天的日期。預設情況下，新憑證 (`CR`) 的分發期間為 90 天。

   > 到了設定的時間後，您將需要 重新安裝網頁主控台，以還原其存取權並更新其憑證。

3. 如有必要，遷移到新的管理伺服器後，請執行 klmover 公用程式，以還原裝置與管理伺服器的連線。如果裝置在整個憑證分發期間一直處於關閉狀態，或從未連線到管理伺服器，您可能需要啟動此公用程式。

2 建立先前安裝之管理伺服器的備份副本

建立卡巴斯基安全管理中心 Windows 的備份副本

1. 從 **開始功能表 → 卡巴斯基安全管理中心 → 卡巴斯基 Backup 公用程式**，執行位於卡巴斯基安全管理中心 Linux 安裝資料夾中的 `klbackup.exe` 公用程式。

   啟動“安裝精靈”。在以 Server Core 模式執行的 Microsoft Windows 上，請使用 klbackup 公用程式的主控台版本。

2. 在第一個步驟中，選取 **執行管理伺服器資料備份**。

3. 在 **備份設定** 步驟中：

   a. 按一下 **瀏覽** 按鈕，然後建立新資料夾，以便將備份副本儲存在與預設目錄不同的位置，例如 `C:\kscbackups`。

   b. 如果您使用 Microsoft SQL Server，請選取 **移轉資料庫 → 移轉至 Postgres** 選項，以搭配快速安裝指令碼使用。使用標準方法部署卡巴斯基安全管理中心 Linux 時，您也可以將資料移轉至 MySQL/MariaDB 資料庫。

   c. 為備份副本設定密碼，以保護其免受未經授權的資料存取。

4. 等待備份副本建立完成，然後結束公用程式。

系統會在指定的目錄中建立一個以備份時間戳記命名的新子目錄。

建立卡巴斯基安全管理中心 Linux 的備份副本

1. 在管理伺服器裝置上，透過命令列執行以下命令：

```
sudo /opt/kaspersky/ksc64/sbin/klbackup -path /root/kscbackups -use_ts
```

2. 等待備份程序完成。

系統會在 `-path` 選項中指定的目錄內，建立一個以備份時間戳記命名的新子目錄。

建立舊管理伺服器的備份副本後，請停用管理伺服器裝置。

停用管理伺服器裝置

1. 將取得的資料遷移備份副本複製到管理員的裝置。
2. 關閉管理伺服器的作業系統。
3. 將網路介面卡從公司網路拔除。
4. 如果您計劃將裝置的 IP 位址重複用於全新安裝的卡巴斯基安全管理中心 Linux，請釋放該 IP 位址。
5. 確保裝置電源已完全關閉。

仍留在網路上的舊管理伺服器可能會導致裝置管理故障，並干擾新管理伺服器的網頁主控台登入程序，也可能會使網路代理安裝工作在啟動時連線到舊伺服器。

3 使用快速安裝指令碼初始部署卡巴斯基安全管理中心 Linux

本指南說明如何使用快速安裝指令碼初始部署卡巴斯基安全管理中心 Linux 執行個體。

特殊考量事項：

- 卡巴斯基安全管理中心的所有元件都安裝在與管理伺服器相同的裝置上。
- 管理伺服器的作業系統必須為以下其中一種：
  - Astra Linux Special Edition RUSB.10015-01（作業更新 1.8.5），搭配 PostgreSQL 15
  - Ubuntu Server 26.04 LTS，搭配 PostgreSQL 18
  - CentOS Stream 10 搭配 PostgreSQL 18
  - RED OS 8.0 搭配 PostgreSQL 16
- 快速安裝指令碼僅會自動執行卡巴斯基安全管理中心應用程式的設定與安裝。管理員必須在作業系統中設定管理伺服器裝置的名稱，並在作業系統層級設定網路介面卡和安全性 Firewall，以及設定硬體。

使用快速安裝指令碼初始部署卡巴斯基安全管理中心 Linux 執行個體，涉及以下步驟：

1.準備部署

在繼續執行安裝步驟之前，您必須準備：

- 作業系統的安裝磁碟映像，以及應用程式套件的存放庫。
- 用於登入網頁主控台時進行 雙因素身分驗證 (2FA) 的驗證器應用程式。
- 新的 FQDN（例如，*ksclinux.example.com*）。如果您具備足夠的解決方案設定經驗，可以在安裝期間使用自己的指令碼，將先前的 FQDN 指派給新伺服器。在此情況下，請在步驟 5「從備份副本還原後設定應用程式」中略過步驟 4「將受管理裝置與先前管理伺服器 FQDN 的連線還原」。
- 配備瀏覽器的管理員裝置，用於透過網際網路下載發佈套件並管理網頁主控台。
- 確保應用程式元件可使用 DNS 和時間伺服器 (NTP)。
- 視您的情境而定，如果先前的 IP 位址曾用於連接受管理裝置，請釋放該 IP 位址。
- 根據以下要求設定網路設備和代理伺服器：
  - 應用程式元件之間通訊使用的連接埠。
  - 存取卡巴斯基伺服器。
  - 強化指南的建議。

2.作業系統規模估算與設定

1. 根據管理伺服器將管理的裝置數量來設定設備。

   每項規模估算都會考量卡巴斯基應用程式可用的資源。此計算會將管理伺服器、網路代理、DBMS、網頁主控台伺服器和 Kaspersky Endpoint Security for Linux 全部在同一部裝置上執行的情況納入考量。不過，此計算未將管理伺服器備份副本的儲存空間納入考量。

   > 使用外部檔案共用作為掛載點，以將備份副本儲存在另一部裝置上，或在考量備份儲存空間的情況下提高可用硬碟空間需求。

   建議為作業系統額外增加 4–6 GB 的 RAM 和 20 GB 的可用硬碟空間。

   根據受管理裝置數量估算裝置規模：

   - **S**（最多 1000 台裝置）：8 個 CPU 核心、16 GB 的 RAM、用於 `/var` 目錄的 70 GB 可用硬碟空間、300 IOPS 以上。
   - **M**（最多 10,000 台裝置）：12 個 CPU 核心、24 GB 的 RAM、用於 `/var` 目錄的 340 GB 可用硬碟空間、300 IOPS 以上。
   - **L**（最多 30,000 台裝置）：20 個 CPU 核心、40 GB 的 RAM、用於 `/var` 目錄的 490 GB 可用硬碟空間、300 IOPS 以上。
   - **XL**（最多 50,000 台裝置）：28 個 CPU 核心、54 GB 的 RAM、用於 `/var` 目錄的 640 GB 可用硬碟空間、300 IOPS 以上。

2. 依照選定的規格，準備卡巴斯基安全管理中心伺服器的硬體。
3. 在卡巴斯基安全管理中心伺服器上安裝作業系統。

在安裝期間，如果您打算透過命令列遠端管理管理伺服器裝置，請啟用 **SSH 遠端連線工具** 選項。

> 安裝 Astra Linux 時，必須停用 **強制存取控制** 選項。此外，若要讓 Kaspersky Endpoint Security for Linux 正常運作，請停用 **封鎖 ptrace 追蹤** 選項。

4. 如果 `/var` 目錄是單獨掛載的，請檢查其可用磁碟空間；否則，請檢查根目錄 `/` 的可用磁碟空間。

   M 設定的範例：

   Astra Linux

   ```
   administrator@ksclinux:~$ df -h
   Filesystem                 Size  Used Avail Use% Mounted on
   /dev/mapper/astra48242-01  406G  8,0G 377G    3% /
   <...>
   ```

   Ubuntu

   ```
   administrator@ksclinux:~$ df -h
   Filesystem                        Size  Used Avail Use% Mounted on
   /dev/mapper/ubuntu--vg-ubuntu--lv  406G   11G  374G   3% /
   <...>
   ```

5. 如果受管理裝置是使用 IP 位址連線，請在新伺服器上設定舊管理伺服器的 IP 位址。

影片：設定作業系統

3.下載發佈檔案

1. 從 卡巴斯基網站 下載所需地區設定的發佈套件，並將其儲存在個別目錄中（例如 *kscdistr*）。

   適用於 Ubuntu 和 Astra Linux

   - 管理伺服器的 deb 格式發佈套件：

     `Version 16.3.0.1207 | Debian x64 | Administration server`

   - 網頁主控台的 deb 格式發佈套件：

     `Version 16.3.0.1207 | Debian x64 | Web console`

   - 快速安裝指令碼：

     `Version 16.3.0.1207 | Linux | KSC installation script`

適用於 CentOS 和 RED OS

- 管理伺服器的 rpm 格式發佈套件：

  `Version 16.3.0.1207 | Red Hat Enterprise Linux x64 | Administration server`

- 網頁主控台的 rpm 格式發佈套件：

  `Version 16.3.0.1207 | Red Hat Enterprise Linux x64 | Web console`

- 快速安裝指令碼：

  `Version 16.3.0.1207 | Linux | KSC installation script`

2. 為了讓卡巴斯基應用程式能夠在 Astra Linux 的封閉式軟體環境模式下運作，請下載公開金鑰檔案 kaspersky_astra_pub_key.gpg。

3. 使用卸除式媒體或透過網路，將下載的檔案複製到新的卡巴斯基安全管理中心管理伺服器裝置。

   以下是使用命令列透過網路進行複製的操作。

   > 能否使用 scp 公用程式來複製檔案，取決於管理伺服器裝置的作業系統中是否正在執行 SSH 服務，以及貴組織的安全政策。

   a. 在命令列中，使用 cd 命令切換至 *kscdistr* 目錄的上一層目錄，例如：

   適用於 Linux

   ```
   cd /home/administrator/Desktop
   ```

   適用於 Windows

   ```
   cd C:\Users\Administrator\Downloads
   ```

   b. 使用 scp 公用程式透過網路複製發佈檔案：

   ```
   scp -r <kscdistr> <administrator>@<ksclinux.example.com>:
   ```

   其中：

   `<kscdistr>` 是包含已下載卡巴斯基安全管理中心發佈套件的本機目錄。

   `<administrator>` 是新管理伺服器上已獲授權可使用 SSH 連線的超級使用者。

   `<ksclinux.example.com>` 是新管理伺服器的 FQDN 位址。

   檔案會複製到指定使用者主目錄的根目錄。

4.配置安裝設定

1. 在新管理伺服器裝置上，以超級使用者身分登入並開啟終端機。

2. 移至包含已複製發佈套件的目錄。

   範例

   ```
   cd ~/kscdistr
   ```

3. 將快速安裝指令碼的壓縮檔解壓縮到包含發佈檔案的目前目錄中。

範例

```
tar -xf ./ksc_fast_install.tar.gz
```

4. 執行以下指令，檢查所有檔案是否存在：

```
ls -la
```

ls -la 命令輸出範例

```
administrator@ksclinux:~$ ls -la
drwxr-xr-x  3 administrator administrator      4096 jul 17 20:32 .
drwx------ 17 administrator administrator      4096 jul 17 17:54 ..
-rw-r--r--  1 administrator administrator       493 apr 20  2023 kaspersky_astra_pub_key.gpg
-rw-r--r--  1 administrator administrator 199128488 jul 10 21:38 ksc64_16.3.0-1207_amd64.deb
-rwxr-xr--  1 administrator administrator    143288 jul 22 17:22 ksc_fast_install.py
-rw-r--r--  1 administrator administrator 158144492 jul 10 21:37 ksc-web-console-16.3.12907.x86_64.deb
-rw-r--r--  1 administrator administrator     15561 jul 22 23:17 nwc_license.txt
-rw-r--r--  1 administrator administrator        64 jul 22 23:17 nwc_license.txt.sha256
-rw-r--r--  1 administrator administrator       493 jul 22 17:22 params.txt
-rw-r--r--  1 administrator administrator     70869 jul 22 23:17 server_license.txt
-rw-r--r--  1 administrator administrator        64 jul 22 23:17 server_license.txt.sha256
```

5. 在包含發佈套件的目錄中，開啟安裝指令碼設定文字檔進行編輯，例如：

```
nano ./params.txt
```

6. 設定先前準備的值，並移除相關行中的第一個註解字元 (`#`)，或新增包含以下值的新行：

- 設備規模調整（S/M/L/XL 組態的值）。

  範例

  ```
  klfi_netsize=S
  ```

- 檔案中兩項設定內的管理伺服器 FQDN 位址。

  ```
  klfi_klserver_address=ksclinux.example.com
  ```

  ```
  klfi_kliam_address=ksclinux.example.com
  ```

已安裝之管理伺服器的語言取決於所下載發佈套件的地區設定。

7. 檢查管理伺服器的 FQDN 是否在新管理伺服器的作業系統中正確解析為回送 IP 位址。為此，請執行以下操作：

   a. 執行 `ping` 命令，並指定新管理伺服器的位址。

   成功取得回送 IP 位址的範例

   ```
   administrator@ksclinux:~$ ping ksclinux.example.com
   ping ksclinux.example.com
   PING ksclinux.example.com (127.0.1.1) 56(84) bytes of data.
   64 bytes from ksclinux.example.com (127.0.1.1): icmp_seq=1 ttl=64 time=0.037 ms
   ```

   b. 如果未取得位址或取得外部 IP 位址，請將管理伺服器的位址新增至新管理伺服器上作業系統的 `/etc/hosts` 檔案。

   為此，請執行以下操作：

   - 執行以下命令，開啟 `/etc/hosts` 檔案進行編輯：

     ```
     sudo nano /etc/hosts
     ```

   - 輸入管理伺服器裝置的 FQDN 作為伺服器位址，例如：

     ```
     127.0.0.1       localhost
     127.0.1.1       ksclinux.example.com ksclinux
     <...>
     ```

> 在受管理裝置上，管理伺服器的 FQDN 必須解析為伺服器的外部 IP 位址。請確定 DNS 伺服器上的記錄已正確設定。

5.啟動快速安裝指令碼

若要執行快速安裝指令碼：

1. 重新啟動裝置後，返回包含發佈套件的目錄：

   ```
   cd ~/kscdistr
   ```

2. 執行以下命令，讓檔案可執行：

   ```
   chmod +x ./ksc_fast_install.py
   ```

3. 請在執行指令碼之前，以您的當地語系語言閱讀最終使用者產品授權協議，因為快速安裝指令碼本身僅提供英文版本。

4. 將網路套件存放庫連接至作業系統或作業系統安裝磁碟映像，以便在安裝期間下載套件。

5. 執行快速安裝指令碼：

   ```
   sudo ./ksc_fast_install.py
   ```

6. 請依照安裝精靈的步驟操作。

> 如果指令碼在資源檢查步驟中誤報 RAM 不足，請在安裝期間停用動態 RAM 配置。

7. 等待安裝完成。從指令碼的文字輸出中，儲存網頁主控台的使用者名稱 (`User`) 和密碼 (`Pass`)。

範例

```
[+] Creating KSC user 'kscadmin' ...
[+] An internal user has been created:
[+]     User: kscadmin
[+]     Pass: ############
[!] If the password is lost, you must create a user by running the command:
        /opt/kaspersky/ksc64/sbin/kladduser -n <user>
[+] OK
[+] Success
```

影片：執行適用於 Ubuntu 的快速安裝指令碼

6.首次登入網頁主控台

1. 在瀏覽器中開啟網頁主控台位址：`https://<FQDN>:8080`
   其中 `<FQDN>` 是安裝指令碼設定中的管理伺服器位址，例如 *https://ksclinux.example.com:8080*。

2. 使用指令碼輸出中的使用者名稱和密碼登入網頁主控台。

3. 設定驗證器應用程式：

   a. 將用於取得一次性確認碼的秘密金鑰複製到應用程式，或從網頁主控台身分驗證精靈掃描 QR 碼。

   b. 輸入產生的確認碼以進行身分驗證並登入網頁主控台。

4. 檢閱並確認強化指南。

5. 如果您不打算從備份副本還原管理伺服器的資料，請在初始設定精靈中設定管理伺服器。

4 還原管理伺服器的備份副本

在從卡巴斯基安全管理中心 Windows 移轉，或將卡巴斯基安全管理中心 Linux 資料移轉到新硬體的情境中，您可能需要從舊管理伺服器安裝中建立的備份副本還原資料。

> 新伺服器上的 PostgreSQL 版本必須至少與備份副本中的版本相符。

如果不需要還原資料，請略過此步驟。

如果先前尚未建立備份副本：

- 使用 PostgreSQL 資料格式類型建立舊管理伺服器安裝的備份副本。
- 安裝新的卡巴斯基安全管理中心 Linux 伺服器，並首次登入網頁主控台。

從備份副本還原管理伺服器包括下列步驟：

1.將備份副本放置在管理伺服器上

使用卸除式媒體或網路，將舊管理伺服器的備份副本放置到新的管理伺服器裝置上。

若要透過網路將備份副本複製到管理伺服器：

> 能否使用 scp 公用程式來複製檔案，取決於管理伺服器裝置的作業系統中是否正在執行 SSH 服務，以及貴組織的安全政策。

1. 在命令列中，使用 *cd* 命令前往包含舊管理伺服器備份檔案的目錄，例如：

   Windows
   ```
   cd C:\kscbackups
   ```

   Linux
   ```
   cd /root/kscbackups
   ```

2. 使用 scp 公用程式複製包含備份檔案的目錄：

   ```
   scp -r <klbackup202x-xx-xx> <administrator>@<ksclinux.example.com>:
   ```

   其中：

   `<klbackup202x-xx-xx>` 是儲存備份檔案的目錄。

   `<administrator>` 是新管理伺服器上已獲授權可使用 SSH 連線的超級使用者。

   `<ksclinux.example.com>` 是新管理伺服器的 FQDN 位址。

   包含備份副本的目錄會複製到指定使用者的主目錄。

2.從備份還原的程序

1. 在新的管理伺服器裝置上，開啟終端機。
2. 從備份副本還原資料時，請將 PostgreSQL 超級使用者權限授予管理伺服器用於連線至資料庫的標準 klserver 和 kliam 帳戶：

```
sudo -i -u postgres psql -c "ALTER ROLE klserver WITH SUPERUSER;"
```

```
sudo -i -u postgres psql -c "ALTER ROLE kliam WITH SUPERUSER;"
```

3. 使用 klbackup 公用程式，從舊管理伺服器的備份副本啟動資料還原：

```
sudo /opt/kaspersky/ksc64/sbin/klbackup -path </home/administrator/klbackup202x-xx-xx> -restore
```

其中 `</home/administrator/klbackup202x-xx-xx>` 是備份檔案所在目錄的完整路徑。

4. 如果未設定備份密碼，當系統提示輸入備份密碼時，請不要輸入密碼，直接按 **Enter**。
5. 請等待公用程式完成。
大型安裝環境可能需要很長時間。
6. 還原管理伺服器用於連線至資料庫之 PostgreSQL 帳戶的原始權限。

```
sudo -i -u postgres psql -c "ALTER ROLE klserver WITH NOSUPERUSER;"
```

```
sudo -i -u postgres psql -c "ALTER ROLE kliam WITH NOSUPERUSER;"
```

5 從備份副本還原後設定應用程式

如果您未從備份副本還原資料，請略過此步驟。

從備份副本還原後設定應用程式包括下列步驟：

1.還原網頁主控台

1. 從 IAM Server 設定檔取得舊伺服器的位址：

```
sudo grep "ksc_address:" /var/opt/kaspersky/klnagent_srv/iam/iam_config.yaml
```

範例

```
ksc_address: "oldksc.example.internal"
```

2. 檢查舊管理伺服器的 FQDN 是否正確解析為新管理伺服器的回送 IP 位址。為此，請執行以下操作：

   a. 使用舊管理伺服器的位址執行 `ping` 命令。

   成功取得回送 IP 位址的範例

   ```
   administrator@ksclinux:~$ ping oldksc.example.internal
   ping oldksc.example.internal
   PING ksclinux (127.0.1.1) 56(84) bytes of data.
   64 bytes from ksclinux (127.0.1.1): icmp_seq=1 ttl=64 time=0.037 ms
   ```

   b. 如果未取得位址或取得外部 IP 位址，請將管理伺服器的位址新增至新管理伺服器上作業系統的 `/etc/hosts` 檔案。為此，請執行以下操作：

   - 開啟 /etc/hosts 檔案進行編輯：

     ```
     sudo nano /etc/hosts
     ```

   - 輸入舊伺服器的名稱，作為管理伺服器裝置位址的其他別名。

     範例

     ```
     127.0.0.1       localhost
     127.0.1.1       ksclinux.example.com ksclinux oldksc.example.internal
     <...>
     ```

3. 重新安裝網頁主控台：

   a. 解除安裝本機網頁主控台伺服器：
   根據您的卡巴斯基安全管理中心 Linux 發佈套件，執行以下其中一個命令：

   - 在以 Debian 為基礎的作業系統上：

     ```
     sudo apt remove ksc-web-console -y
     ```

   - 在執行以 Red Hat Enterprise Linux 為基礎之作業系統的裝置上：

     ```
     sudo dnf remove ksc-web-console -y
     ```

   b. 從包含發佈套件的目錄安裝網頁主控台套件：

   - 在以 Debian 為基礎的作業系統上：

     ```
     sudo apt install ~/kscdistr/ksc-web-console-16.3.12907.x86_64.deb -y
     ```

   - 在執行以 Red Hat Enterprise Linux 為基礎之作業系統的裝置上：

     ```
     sudo dnf install ~/kscdistr/ksc-web-console-16.3.12907.x86_64.rpm -y
     ```

2.從卡巴斯基安全管理中心 Windows 遷移時還原 kscadmin 使用者的存取權

使用者資料庫已遭覆寫；請重新建立 kscadmin 使用者並設定雙重身分驗證。

1. 在管理伺服器裝置的作業系統中開啟終端機，並執行下列命令以建立使用者：

   ```
   sudo /opt/kaspersky/ksc64/sbin/kladduser -n kscadmin
   ```

   按 **Enter** 後，輸入密碼，然後再次輸入。

2. 在瀏覽器中開啟網頁主控台位址：

   ```
   https://<FQDN>:8080
   ```

   其中 `<FQDN>` 是安裝指令碼設定中的管理伺服器位址，例如 *https://ksclinux.example.com:8080*。

3. 使用已建立的使用者名稱和密碼登入網頁主控台。

4. 設定驗證器應用程式。為此，請執行以下操作：

   a. 還原管理伺服器的備份副本之前，請從驗證器應用程式刪除舊的 kscadmin 使用者設定檔。

   b. 將用於取得一次性確認碼的秘密金鑰複製到應用程式，或從網頁主控台身分驗證精靈掃描 QR 碼。

   c. 輸入產生的確認碼以進行身分驗證並登入網頁主控台。

3.測試管理伺服器

1. 確認以 kscadmin 和其他使用者身分登入時，網頁主控台介面是否正常運作。

2. 依序執行下列工作：

   - 下載更新至管理伺服器儲存區
   - 管理伺服器維護
   - 管理伺服器資料備份

   將工作設定中的 Windows 路徑取代為新管理伺服器上的 Linux 目錄，或刪除工作並從頭開始進行設定。

3. 檢查工作的結果，並視需要變更工作設定、管理政策及管理伺服器設定。

4.還原受管理裝置與先前管理伺服器 FQDN 的連線

如果您已為新的管理伺服器指派新的 FQDN（例如 ksclinux.example.com），請新增下列其中一種類型的 DNS 記錄：

- 一筆 CNAME 記錄，將管理伺服器的舊名稱對應至管理伺服器的新名稱。
  如需設定必要記錄的詳細資訊，請參閱 DNS 伺服器的說明文件。

- 舊管理伺服器位址的 A 和 AAAA 記錄，指向管理伺服器的新 IP 位址。
  對於以 Windows Server 為基礎的 DNS 服務，請使用適用於您基礎架構的值來執行命令。

若要為以 Windows Server 為基礎的 DNS 服務新增 DNS A 記錄，請使用適用於您基礎架構的值執行命令：

1. 連線到您的 DNS 伺服器。

2. 開啟 PowerShell，並執行下列命令從現有 A 記錄中取得 IP 位址：

```
Get-DnsServerResourceRecord -ZoneName "<zone name>" -RRType A -Name "<name of the administration server>"
```

3. 執行下列命令以變更 A 記錄中的 IP 位址：

```
$OldKSC = Get-DnsServerResourceRecord -ZoneName "<zone name>" -RRType A -Name "<name of the administration
server>"
```

```
$NewKSC = $OldKSC.Clone()
```

```
$NewKSC.RecordData.IPv4Address = [System.Net.IPAddress]::parse('<IP-address of the administration server>')
```

```
Set-DnsServerResourceRecord -OldInputObject $OldKSC -NewInputObject $NewKSC -ZoneName "<zone name>"
```

4. 執行下列命令，驗證 A 記錄中的 IP 位址是否已更新：

```
Get-DnsServerResourceRecord -ZoneName "<zone name>" -RRType A -Name "<name of the administration server>"
```

命令的輸出包含卡巴斯基安全管理中心 Linux 管理伺服器的 IP 位址。本機 DNS 快取更新後，受管理裝置將重新連線。

6 設定管理伺服器的病毒防護

為遵循強化指南的建議以便為管理伺服器提供病毒防護，請在管理伺服器上安裝卡巴斯基應用程式並設定管理政策。若要部署 Kaspersky Endpoint Security for Linux，請參閱部署指南。

安裝與設定包含下列步驟：

1.建立個別的管理群組

1. 在網頁主控台的主視窗中，選擇**資產管理 → 群組的階層**。

2. 選取 **受管理裝置** 群組旁邊的核取方塊。

3. 點擊“**新增**”。

4. 在顯示的視窗中，指定新群組的名稱（例如 *kscserver*），然後按一下 **新增** 按鈕以確認建立。

2.建立不繼承設定的網路代理政策

1. 在網頁主控台主視窗中，前往 **資產管理 → 政策** 區段。

2. 點擊“**新增**”按鈕。

3. 在新政策精靈中，選取 **卡巴斯基安全管理中心網路代理** 應用程式，然後按一下 **下一步**。

4. 停用 **從父政策繼承設定** 選項，然後按一下 **儲存**。

3.從卡巴斯基安全管理中心或手動安裝 Kaspersky Endpoint Security for Linux 管理外掛程式

您可以透過下列方式安裝 Kaspersky Endpoint Security for Linux 管理外掛程式：

- 從網頁主控台中的可用分發套件清單安裝。
- 從檔案手動安裝。

若要從網頁主控台中的可用分發套件清單安裝 Kaspersky Endpoint Security 管理外掛程式：

1. 在網頁主控台主視窗中，選取 **設定** → **Web 外掛程式**。

   已安裝的 Web 外掛程式清單將開啟。

2. 點擊"**新增**"按鈕。

   這會開啟可用管理外掛程式清單。當 Web 外掛程式有新版本發布後，該清單會自動更新。

3. 在可用的外掛程式清單中，選取最新可用版本的 Kaspersky Endpoint Security for Linux Web 外掛程式。

4. 在開啟的帶有 Web 外掛程式描述的視窗中，點擊**安裝外掛程式**按鈕。

5. 等待安裝完成，然後在資訊視窗中點擊**確定**。

新的外掛程式將顯示在已安裝的 Web 外掛程式清單中。

影片：使用精靈安裝管理 Web 外掛程式

若要從檔案手動安裝 Kaspersky Endpoint Security 管理外掛程式：

1. 從 Kaspersky Endpoint Security for Linux 區段的應用程式下載頁面下載包含 Web 外掛程式的封存檔：**應用程式控制外掛程式** → **網頁主控台外掛程式**。

2. 將下載的封存檔解壓縮到本機。

3. 在網頁主控台主視窗中，選取 **設定** → **Web 外掛程式**。

   已安裝的 Web 外掛程式清單將開啟。

4. 點擊**從檔案新增**按鈕。

5. 這會開啟一個視窗；請在該視窗中指定 plugin.zip 檔案的路徑和 signature.txt 檔案的路徑。
   這些檔案位於您解壓縮包含 Web 外掛程式之封存檔的資料夾中。

6. 點擊"**新增**"按鈕。

7. 等待安裝完成，然後在資訊視窗中點擊**確定**。

新的外掛程式將顯示在已安裝的 Web 外掛程式清單中（**設定** → **Web 外掛程式**）。

影片：在隔離網路中安裝管理 Web 外掛程式

4.建立不繼承設定的 Kaspersky Endpoint Security for Linux 政策

將 Kaspersky Endpoint Security for Linux 搭配卡巴斯基安全管理中心 Linux 使用時，您需要根據卡巴斯基專家的建議管理政策設定。

1. 在網頁主控台的主視窗中，選擇**資產管理** → **政策**。

2. 為管理伺服器選取管理群組。

3. 點擊"**新增**"。
   啟動"政策精靈"。

4. 在顯示的視窗中，從清單中選取 Kaspersky Endpoint Security for Linux。

5. 指定 Kaspersky Endpoint Security for Linux 應用程式的 **標準模式或者 Endpoint Detection and Response Agent 模式**。

6. 決定是否要參與卡巴斯基安全網路。

7. 檢閱受管理裝置的最佳化建議。

8. 在政策名稱中，指出該政策屬於管理伺服器。

9. 停用 **來自父政策的繼承** 選項。

10. 儲存變更。

影片：建立政策

5.建立 Kaspersky Endpoint Security for Linux 的更新群組工作

1. 在網頁主控台的主視窗中，選擇 **工作** 區段。

2. 為管理伺服器選取管理群組。

3. 點擊“**新增**”。
   啟動“工作精靈”。

4. 在顯示的視窗中，從清單中選取 Kaspersky Endpoint Security for Linux。

5. 指定 *更新* 工作類型，然後執行後續步驟，而不變更設定。
   工作內容視窗將開啟。

6. 在 **應用程式設定 → 更新來源** 區段中，啟用卡巴斯基安全管理中心來源並提高其優先順序。

在隔離網路中，使用 Kaspersky Update Utility 建立更新工作的儲存庫。

影片：設定集中式資料庫更新

6.將產品授權金鑰新增至具備自動金鑰分發功能的管理伺服器儲存區

1. 在卡巴斯基安全管理中心網頁主控台的主視窗中，前往 **產品授權** 區段。
2. 點擊“**新增**”。
3. 指定 **啟動碼** 選項，然後按一下 **傳送**。
   在隔離網路中，使用可透過 https://keyfile.kaspersky.com/en-US 服務申請的金鑰檔案。
4. 在產品授權清單中，按一下產品授權的名稱。
5. 選擇“**自動分發產品授權金鑰到受管理裝置**”核取方塊。
6. 儲存變更。

影片：使用啟動碼啟動應用程式

影片：使用金鑰檔案啟動應用程式

7.建立網路代理和 Kaspersky Endpoint Security for Linux 的安裝套件

1. 在網頁主控台的主視窗中，選擇**軟體管理 → 安裝套件**。
2. 點擊"**新增**"。
   建立安裝套件的精靈將會啟動。
3. 選擇"**為卡巴斯基應用程式建立安裝套件**"。
4. 在應用程式清單中，尋找最新版 Kaspersky Endpoint Security for Linux，然後按一下其名稱。
5. 在側邊欄中，按一下 **下載並建立安裝套件** 按鈕以開始下載。
   檢閱並接受最終使用者產品授權協議以開始使用應用程式。
6. 返回應用程式清單，然後下載最新版的 Linux 版網路代理。
   檢閱並接受最終使用者產品授權協議以開始使用應用程式。
7. 在網頁主控台的主視窗中，在已下載應用程式清單中，按一下應用程式的名稱。

在隔離網路中，從卡巴斯基網站下載分發套件，然後在新套件精靈中選取 **從檔案建立安裝套件** 選項。

影片：在卡巴斯基安全管理中心自動建立安裝套件

影片：在卡巴斯基安全管理中心手動建立安裝套件

8.安裝 Linux 版網路代理

1. 在網頁主控台主視窗中，選取 **軟體管理** → **安裝套件**。
2. 選取 **卡巴斯基 Linux 版網路代理** 套件旁的核取方塊。
3. 按一下 **展開**。

   保護部署精靈將會啟動。
4. 選取 **使用獨立套件** 選項。
5. 在 **將裝置移至受管理裝置資料夾** 步驟，略過設定將裝置移至管理群組的規則。此選項不適用於管理伺服器裝置。
6. 在 **獨立安裝套件建立結果** 步驟，選取並複製應用程式安裝指令碼的完整路徑。
7. 在管理伺服器的作業系統中，開啟命令列。
8. 開始安裝獨立套件：

   ```
   sudo bash "</var/opt/.../stand-alone_package_sh>"
   ```

   其中，`</var/opt/.../stand-alone_package_sh>` 是先前複製的應用程式獨立安裝套件指令碼檔案完整路徑。

   如果安裝成功，將會顯示對應的通知。
9. 將管理伺服器裝置（例如 *ksclinux*）從 **受管理裝置** 群組移至先前準備好的管理群組（例如 *kscserver*）。

9.安裝 Kaspersky Endpoint Security for Linux

1. 在網頁主控台主視窗中，選取 **軟體管理** → **安裝套件**。
2. 選取 Kaspersky Endpoint Security for Linux 套件旁的核取方塊。
3. 按一下 **展開**。

   保護部署精靈將會啟動。
4. 選取 **使用獨立套件** 選項。

5. 在 **獨立安裝套件建立結果** 步驟，選取並複製應用程式安裝指令碼的完整路徑。

6. 在管理伺服器的作業系統中，開啟命令列。

7. 開始安裝獨立套件：

```
sudo bash "</var/opt/.../stand-alone_package_sh>"
```

其中，`</var/opt/.../stand-alone_package_sh>` 是先前複製的應用程式獨立安裝套件指令碼檔案完整路徑。

如果安裝成功，將會顯示對應的通知。

8. 在網頁主控台主視窗的 **工作** 區段中，選取管理群組清單中以管理伺服器名稱命名的根節點。

9. 從管理伺服器工作清單中，依序啟動下列工作：

   - 下載更新至管理伺服器儲存區
   - 更新 (Kaspersky Endpoint Security for Linux)

10. 在網頁主控台的主視窗中，選取 **資產管理 → 資產 (裝置)**。

11. 按一下管理伺服器裝置物件的名稱。

12. 檢查裝置狀態的主要指標：

    - 病毒防護資料庫的上次更新（目前）。
    - 已連線至管理伺服器（目前）。
    - 防護狀態（執行中）。
    - *金鑰成功新增*事件（存在）。

使用 Kaspersky Endpoint Security for Linux 部署指南，在網路中的裝置上部署安全解決方案。

從先前版本更新應用程式

可透過在受保護的裝置上遠端或本機安裝新版本的應用程式來升級 Kaspersky Endpoint Security 應用程式。

您只能從 Kaspersky Endpoint Security 12.4 for Linux 升級到 Kaspersky Endpoint Security 12.5 for Linux。

不支援將早期版本的 Kaspersky Endpoint Security 升級到版本 12.5。如果您安裝了早期版本的 Kaspersky Endpoint Security，則需要先將其解除安裝，然後安裝 Kaspersky Endpoint Security 12.5 for Linux。

您可以依照以下步驟升級應用程式。

1 準備環境

開始升級 Kaspersky Endpoint Security 之前，請根據您的基礎架構完成必要的準備步驟。

2 準備分發套件

請根據您的作業系統、其架構和 CPU 類型選擇發佈套件。

3 更新 Kaspersky Endpoint Security 管理外掛程式

如果您使用卡巴斯基安全管理中心管理 Kaspersky Endpoint Security，請根據您用於管理卡巴斯基安全管理中心的主控台，更新 Kaspersky Endpoint Security 管理 Web 外掛程式或 MMC 外掛程式。

4 更新受防護裝置上的應用程式和圖形介面

請在受保護的裝置上安裝新版本的應用程式。更新後的應用程式將保留安裝時選擇的應用程式使用模式。如果您想以不同的模式使用該應用程式，您必須解除安裝該應用程式，然後執行應用程式的安裝和初始配置。

如果您以基本模式或 EDR Agent 模式使用 Kaspersky Endpoint Security，並且使用應用程式的圖形介面，則還需要更新圖形介面。

您可以透過下列方式更新應用程式和應用程式的圖形介面：

- 遠端使用卡巴斯基安全管理中心
- 本機使用命令列

如何使用命令列從 RPM 套件升級應用程式

在命令列上升級應用程式相當於在裝置上安裝新版本的應用程式。

> 您需要 root 權限才能更新應用程式。

若要升級應用程式，請執行以下指令：

```
# [KESL_EULA_AGREED=yes] [KESL_PRIVACY_POLICY_AGREED=yes] [KESL_USE_KSN=<yes|no>] rpm -U --replacefiles --
replacepkgs kesl-12.5.0-<build number>.<arch>.rpm [kesl-gui-12.5.0-<build number>.<arch>.rpm]
```

Kaspersky Endpoint Security 將自動重新啟動。

符號

命令選項

設定	描述
KESL_EULA_AGREED=yes	接受《最終使用者產品授權協議》的條款和條件。
KESL_PRIVACY_POLICY_AGREED=yes	接受《隱私權政策》的條款和條件。
KESL_USE_KSN=yes/no	使用卡巴斯基安全網路： yes – 接受卡巴斯基安全網路聲明的條款，並啟用卡巴斯基安全網路。 no – 拒絕卡巴斯基安全網路聲明的條款，並停用卡巴斯基安全網路。

設定	描述
<arch>	架構類型： i386 – 適用於 32 位元作業系統 x86_64 – 適用於 64 位元作業系統 aarch64 – 適用於 Arm 架構的 64 位元作業系統

Kaspersky Endpoint Security 將自動重新啟動。

範例：

同時更新 RPM 應用程式套件與適用於 64 位元作業系統的 GUI 套件：

```
# KESL_EULA_AGREED=yes KESL_PRIVACY_POLICY_AGREED=yes KESL_USE_KSN=yes rpm -U --replacefiles --replacepkgs kesl-12.5.0-<build number>.x86_64.rpm kesl-gui-12.5.0-<build number>.x86_64.rpm
```

更新完成後、應用程式重新啟動先前對應用程式設定所做的變更不會被儲存。

如何使用命令列從 DEB 套件升級應用程式

在命令列上升級應用程式相當於在裝置上安裝新版本的應用程式。

您需要 root 權限才能更新應用程式。

若要升級應用程式，請執行以下指令：

```
# [KESL_EULA_AGREED=yes] [KESL_PRIVACY_POLICY_AGREED=yes] [KESL_USE_KSN=<yes|no>] apt-get install ./kesl_12.5.0-<build number>_<arch>.deb [./kesl-gui_12.5.0-<build number>_<arch>.deb]
```

Kaspersky Endpoint Security 將自動重新啟動。

符號

命令選項

設定	描述
KESL_EULA_AGREED=yes	接受《最終使用者產品授權協議》的條款和條件。
KESL_PRIVACY_POLICY_AGREED=yes	接受《隱私權政策》的條款和條件。
KESL_USE_KSN=yes/no	使用卡巴斯基安全網路： yes – 接受卡巴斯基安全網路聲明的條款，並啟用卡巴斯基安全網路。 no – 拒絕卡巴斯基安全網路聲明的條款，並停用卡巴斯基安全網路。
<arch>	架構類型： i386 – 適用於 32 位元作業系統 amd64 – 適用於 64 位元作業系統 arm64 – 適用於 Arm 架構的 64 位元作業系統

範例：

同時更新 DEB 應用程式套件與適用於 64 位元作業系統的 GUI 套件：

```
# KESL_EULA_AGREED=yes KESL_PRIVACY_POLICY_AGREED=yes KESL_USE_KSN=yes apt-get install ./kesl_12.5.0-<build number>_amd64.deb [./kesl-gui_12.5.0-<build number>_amd64.deb]
```

更新完成後、應用程式重新啟動先前對應用程式設定所做的變更不會被儲存。

5 更新卡巴斯基安全管理中心網路代理

選用步驟。如果您使用卡巴斯基安全管理中心集中管理 Kaspersky Endpoint Security，請更新受防護裝置上的網路代理。此升級透過安裝新版本的網路代理來執行。

在執行 Astra Linux 特別版作業系統的裝置上，我們建議使用卡巴斯基安全管理中心遠端更新網路代理，因為使用卡巴斯基安全管理中心管理主控台中的指令列進行更新會建立相同受管理裝置的新副本，而舊副本將無法存取。如需詳細資訊，請參閱卡巴斯基安全管理中心說明。

網路代理更新期間，應用程式繼續正常運作。

升級先前版本應用程式的特點

- 如果在更新應用程式時發生錯誤，則會回溯更新並啟動應用程式的先前版本。在這種情況下，將會顯示錯誤訊息，但套件管理器（rpm/dpkg）會指示新版本。
- 在包含 rpm 類型套件管理器的作業系統中，如果同時安裝了應用程式套件和 GUI 套件，則建議避免單獨更新其中任一套件。

  在包含 dpkg 類型套件管理器的作業系統中，如果同時安裝了應用程式套件和 GUI 套件，則無法單獨更新其中任一套件。
- 如果最終使用者產品授權協議和/或隱私權政策的條款和條件在應用程式的新版本中發生變化，您必須在更新期間接受新的條款和條件。使用者協議的文字可在卡巴斯基網站（**最終使用者產品授權協議**區段）以及 ~/.kesl/12.5/license.<language ID> 目錄中取得。

  如果您不接受最終使用者產品授權協議和/或隱私權政策的條款，則應用程式將不會更新。
- 如果《卡巴斯基安全網路聲明》的條款在應用程式的新版本中發生變化，您需要接受或拒絕參與卡巴斯基安全網路的新使用條款。您可以在 ~/.kesl/12.5/ksn_license.<language ID> 中找到卡巴斯基安全網路聲明的文字。拒絕使用卡巴斯基安全網路不會中斷更新過程。您可以稍後啟用、停用或變更卡巴斯基安全網路模式。

  如果您在應用程式的先前版本中使用過 KSN 並接受了《卡巴斯基安全網路聲明》的條款，則需要在更新應用程式時接受《卡巴斯基安全網路聲明》的條款。否則，KSN 的使用將被停用。
- 即使 Kaspersky Endpoint Security 在更新處理程序開始之前啟動，如果更新成功完成，也會啟動新的應用程式版本。
- 當您將應用程式更新到較新的版本時，先前版本的傾印檔案將被刪除。

- 當您更新應用程式時，先前版本的事件記錄檔會成為目前版本檔案組中的首個事件檔案。在剩余檔案中的事件數達到指定的最大數量（`MaxEventsNumber` 設定）之前，都會保留該檔案。因此，可能會出現這種暫時的情況，即應用程式儲存的事件數量將達到 `MaxEventsNumber` 設定值的兩倍。

- 如果 Kaspersky Endpoint Security 是以基本模式或 EDR Agent 模式使用，建議在更新應用程式後啟動資料庫更新工作。

更新 Kaspersky Endpoint Security 管理外掛程式

Kaspersky Endpoint Security 的管理插件透過安裝新版本的管理外掛程式來更新。根據您使用的卡巴斯基安全管理中心管理主控台，您必須安裝：

- Kaspersky Endpoint Security 管理 Web 外掛程式

- Kaspersky Endpoint Security MMC 管理外掛程式

如何安裝管理 Web 外掛程式

您可以透過以下方式安裝 Web 外掛程式：

- 使用卡巴斯基安全管理中心網頁主控台的快速啟動精靈。

  首次將卡巴斯基安全管理中心網頁主控台連線至管理伺服器時，卡巴斯基安全管理中心網頁主控台會自動提示您執行快速啟動精靈。您也可以在卡巴斯基安全管理中心網頁主控台介面中執行初始配置精靈（**裝置發現和部署→部署和指派→快速啟動精靈**）。快速啟動精靈還可以檢查已安裝的 Web 外掛程式是否為最新，並下載必需的更新。如需卡巴斯基安全管理中心網頁主控台快速啟動精靈的詳細資訊，請參閱 卡巴斯基安全管理中心說明。

- 手動安裝，使用卡巴斯基 Web 外掛程式清單中的發佈套件或檔案中的發佈套件。

若要從卡巴斯基安全管理中心手動安裝 Kaspersky Endpoint Security Web 外掛程式：

1. 在卡巴斯基安全管理中心網頁主控台的主視窗中，選擇 **設定 → Web 外掛程式**。

   已安裝的 Web 外掛程式清單將開啟。

2. 點擊“**新增**”按鈕。

   這會開啟可用管理外掛程式清單。當 Web 外掛程式有新版本發布後，該清單會自動更新。

3. 在可用外掛程式清單中，選取 **Kaspersky Endpoint Security <版本號碼> for Linux** Web 外掛程式。

4. 在開啟的帶有 Web 外掛程式描述的視窗中，點擊**安裝外掛程式**按鈕。

5. 等待安裝完成，然後在資訊視窗中點擊**確定**。

新的外掛程式將顯示在已安裝的 Web 外掛程式清單中（**設定 → Web 外掛程式**）。

若要從檔案手動安裝 Kaspersky Endpoint Security Web 外掛程式：

1. 在 應用程式下載頁面 的 **Kaspersky Endpoint Security for Linux** 區段中下載包含 Web 外掛程式的封存檔（**附加發佈套件 → 網頁主控台外掛程式**）。

2. 將下載的封存檔解壓縮到本機。

3. 在卡巴斯基安全管理中心網頁主控台主視窗中，選取**設定** → **Web 外掛程式**。

   已安裝的 Web 外掛程式清單將開啟。

4. 點擊**從檔案新增**按鈕。

5. 這會開啟一個視窗；請在該視窗中指定 plugin.zip 檔案的路徑和 signature.txt 檔案的路徑。這些檔案位於您解壓縮包含 Web 外掛程式之封存檔的資料夾中。

6. 點擊"**新增**"按鈕。

7. 等待安裝完成，然後在資訊視窗中點擊**確定**。

新的外掛程式顯示在已安裝的 Web 外掛程式清單中（**設定**→ **Web 外掛程式**）。

如果您在卡巴斯基安全管理中心伺服器的屬性中選擇了 Kaspersky EndpoinSecurity 分發套件中未包含的語言，則產品授權協議和整個卡巴斯基安全管理中心網頁主控台介面將以英文顯示。

如何安裝 MMC 管理外掛程式

在安裝 Kaspersky Endpoint Security MMC 管理外掛程式之前，請確保已安裝卡巴斯基安全管理中心和 Redist C++ 2015（Microsoft Visual C++ 2015 Redistributable）。

若要安裝 MMC 外掛程式：

1. 在 應用程式下載頁面 的 **Kaspersky Endpoint Security for Linux** 區段中下載 klcfginst.msi 檔案（**組建** → **管理外掛程式**）。

2. 在已安裝卡巴斯基安全管理中心管理主控台的裝置上，執行 klcfginst.msi 檔案。

安裝後，管理 MMC 外掛程式將顯示在卡巴斯基安全管理中心伺服器屬性中已安裝的 MMC 管理外掛程式清單中。

若要檢視已安裝的管理 MMC 外掛程式清單：

1. 在卡巴斯基安全管理中心管理主控台樹中，選擇**管理伺服器<伺服器名稱>**節點並透過以下方式之一開啟管理伺服器屬性視窗：

   - 開啟 **管理伺服器 <伺服器名稱>** 節點的內容功能表，並選取 **屬性** 項目。

   - 在 **管理伺服器** 區段中，按一下 **管理伺服器 <伺服器名稱>** 節點工作區內的 **管理伺服器屬性** 連結。

2. 在**進階**區域的左側清單中，選取**安裝應用程式管理外掛程式相關資訊**區域。

   在視窗右側，已安裝的管理外掛程式清單會顯示Kaspersky Endpoint Security 的管理 MMC 外掛程式：**Kaspersky Endpoint Security <版本號> for Linux**。

轉換政策和工作

為先前版本的 Kaspersky Endpoint Security 配置的政策和工作與應用程式的更新版本不相容。如果使用卡巴斯基安全管理中心管理主控台來管理應用程式，則在更新 MMC 管理外掛程式後，您可以使用卡巴斯基安全管理中心「政策和工作批量轉換」精靈轉換政策和工作（有關詳細資訊，請參閱卡巴斯基安全管理中心說明）。

轉換後的政策和工作會命名為「*<原始政策或工作的名稱>（已轉換）*」。

對於大多數設定，轉換後的政策和工作使用為應用程式先前版本配置的值。一些設定被分配了特殊值。先前版本的政策和工作中未配置的設定在轉換後的政策和工作中採用預設值。

> 您無法在卡巴斯基安全管理中心網頁主控台中轉換政策和工作。

如果您使用網頁主控台來管理應用程式，則必須在卡巴斯基安全管理中心中為應用程式建立新的政策和工作。您可以透過匯出和匯入設定，將政策和工作的某些設定值從政策或工作的先前版本遷移到新版本。

管理外掛程式的特殊注意事項

- 安裝新版本的 Kaspersky Endpoint Security 管理外掛程式後，先前版本的管理外掛程式仍可繼續運作。您可以使用它們來管理 Kaspersky Endpoint Security 的先前版本。

  如果您已在所有用戶端裝置上更新了應用程式，則可以解除安裝先前版本的 Kaspersky Endpoint Security 管理外掛程式。

- 為相同版本的應用程式安裝新版本的 MMC 管理外掛程式時，必須先解除安裝目前已安裝的該版本的 MMC 外掛程式，然後再安裝該版本的新 MMC 外掛程式。

升級後的應用程式設定

如果您使用卡巴斯基安全管理中心管理主控台來管理應用程式，則可以*轉換政策*，以便讓新版本使用為先前版本應用程式指定的政策設定值（如需詳細資訊，請參閱卡巴斯基安全管理中心說明）。

> 您無法在卡巴斯基安全管理中心網頁主控台中轉換政策。

使用指令列更新應用程式後，大多數設定都會從應用程式的先前版本延續下來。您也可以透過將設定匯出到檔案，然後從該檔案匯入它們來遷移應用程式設定。

預設值被指派給應用程式先前版本中不存在的設定。一些設定被分配了特殊值。

系統事件攔截設定

如果在應用程式的先前版本中選擇了基於可更新內核模組的系統事件攔截機制，則更新後，應用程式將切換到使用 fanotify 攔截系統事件。然後，在資料庫更新和應用程式模組更新並自動重新啟動後，應用程式將再次恢復使用可更新內核模組。

卡巴斯基安全網路設定

在 MMC 外掛程式中轉換政策後，政策內容中的卡巴斯基安全網路設定取決於您是接受還是拒絕了「政策和工作批量轉換」精靈中的卡巴斯基安全網路聲明的條款：

- 如果您接受聲明的條款，則選擇**延伸 KSN 模式**選項。
- 如果您拒絕聲明的條款，則選擇**不使用 KSN**選項。

透過命令列更新應用程式後，`UseKSN` 設定會修改如下：

- 如果您在升級期間設定 `KESL_USE_KSN=No`，則 `UseKSN=No`。
- 如果您在升級期間設定 `KESL_USE_KSN=Yes`，則 `UseKSN=Extended`。
- 在其他情況下，`UseKSN`設定的值在更新後不會改變。

雲端模式設定

在 MMC 外掛程式中轉換政策後，雲端模式使用設定可能會發生變化，具體取決於您是否接受或拒絕政策和工作批次轉換精靈中的卡巴斯基安全網路聲明的條款：

- 如果您接受聲明的條款，則會選取**啟用雲端模式**核取方塊。
- 如果您拒絕聲明的條款，則**啟用雲端模式**核取方塊將被清除。

在命令列上更新應用程式後，`CloudMode` 設定為：

- 若升級後 `UseKSN=No`，則 `CloudMode=No`。
- 如果在更新後設定了 `UseKSN=Basic/Extended`，且在更新前設定了 `CloudMode=Yes`，則為 `CloudMode=Yes`。

如果啟用 KSN，則可以使用雲端模式。要啟用雲端模式：

- 在管理主控台或網頁主控台中，選取 **延伸 KSN 模式** 選項，然後選取 **啟用雲端模式** 核取方塊。
- 在命令列中，設定下列設定：

```
UseKSN=<Basic|Extended>
CloudMode=Yes
```

Kaspersky Managed Detection and Response 整合设定

如果已啟用 MDR 元件，則在 MMC 外掛程式中轉換政策後，MDR 元件的狀態取決於您是接受还是拒絕了「政策和工作批量轉換」精靈中的卡巴斯基安全網路聲明的條款：

- 如果您接受了該聲明的條款，MDR 元件將保持啟用（選取**啟用 Managed Detection and Response** 核取方塊）。
- 如果您拒絕了該聲明的條款，則**啟用 Managed Detection and Response** 核取方塊將被清除。

在命令列上更新應用程式後，`UseMDR` 設定為：

- 若升級後 `UseKSN=No`，則 `UseMDR=No`。
- 如果在更新後設定了 `UseKSN=Basic/Extended`，且在更新前設定了 `UseMDR=Yes`，則為 `UseMDR=Yes`。

> 如果您希望使用 Kaspersky Managed Detection and Response 功能，則需要啟用卡巴斯基安全網路的延伸模式。

Endpoint Detection and Response Expert 整合設定

新版應用程式提供 Kaspersky Endpoint Detection and Response Expert (cloud) 整合模式。

> Kaspersky Endpoint Security for Linux 與 Kaspersky Endpoint Detection and Response Expert (cloud) 的整合暫時無法使用。此功能計劃於 2026 年底前獲得支援。請持續關注我們的版本說明，以瞭解應用程式升級與新功能。

在 MMC 外掛程式中轉換政策後，與 Endpoint Detection and Response Expert (cloud) 的整合將停用（**啟用 Endpoint Detection and Response Expert (cloud)** 核取方塊會被清除）。應用程式使用 Endpoint Detection and Response Expert (on-premises) 整合。

透過命令列更新應用程式後，`EDR_EXPERT_CLOUD_MODE` 會設定為：`EDR_EXPERT_CLOUD_MODE=No`（預設值）。

使用者權限設定

新版應用程式支援 密碼防護。

在 MMC 外掛程式中轉換政策後，密碼防護將停用。

透過命令列升級應用程式後，會根據在先前版本的應用程式中設定的使用者角色（*kesladmin*、*kesluser*、*keslaudit*、*nokesl*）保留使用者權限。

解除安裝應用程式

您可以依照下列步驟解除安裝 Kaspersky Endpoint Security。

移除 Kaspersky Endpoint Security for Linux 的特殊考量

- 在解除安裝應用程式時，裝置上的所有 Kaspersky Endpoint Security 工作都將停止。
- 解除安裝應用程式後，應用程式儲存的所有資訊都會遭到刪除，包括任何已安裝的應用程式憑證。產品授權資料庫已儲存，您可以使用它重新安裝應用程式。唯一的電腦 ID（SensorID）也會儲存。
- 如果應用程式安裝在 systemd 中，則應用程式解除安裝後 systemd 設定將被還原到其初始狀態。

1 解除安裝應用程式及其圖形介面

從受防護裝置解除安裝應用程式套件和圖形介面套件。

您可以同時解除安裝應用程式套件和圖形介面套件，或僅解除安裝圖形介面套件。如果安裝了圖形介面套件，則無法僅解除安裝應用程式套件。

您可以透過下列方式解除安裝應用程式及其圖形介面：

遠端使用卡巴斯基安全管理中心

本機使用命令列

解除安裝需要 root 權限。

解除安裝過程完成後，將顯示關於解除安裝結果的訊息。

刪除應用程式套件和圖形使用者介面套件

解除安裝從 RPM 套件安裝的應用程式和圖形介面

```
rpm -e kesl kesl-gui
```

解除安裝從 DEB 套件安裝的應用程式和圖形使用者介面

```
apt-get purge kesl kesl-gui
```

移除在無圖形介面下使用的應用程式套件

刪除透過 RPM 套件安裝的應用程式

```
rpm -e kesl
```

刪除透過 DEB 套件安裝的應用程式

```
apt-get purge kesl
```

刪除圖形使用者介面套件

解除安裝從 RPM 套件安裝的應用程式圖形介面

```
rpm -e kesl-gui
```

解除安裝從 DEB 套件安裝的應用程式圖形介面

```
apt-get purge kesl-gui
```

解除安裝在後台進行。

2 移除網路代理

如果您使用卡巴斯基安全管理中心來管理Kaspersky Endpoint Security ，則必須從受防護的裝置中解除安裝網路代理。

您可以透過以下方式解除安裝網路代理：

遠端使用卡巴斯基安全管理中心

本機使用命令列

解除安裝需要 root 權限。

解除安裝過程完成後，將顯示關於解除安裝結果的訊息。

解除安裝從 RPM 套件安裝在 32 位元作業系統上的網路代理

```
rpm -e klnagent
```

解除安裝從 RPM 套件安裝在 64 位元作業系統上的網路代理

```
rpm -e klnagent64
```

解除安裝從 DEB 套件安裝在 32 位元作業系統上的網路代理

```
apt-get purge klnagent
```

解除安裝從 DEB 套件安裝在 64 位元作業系統上的網路代理

```
apt-get purge klnagent64
```

❸ 解除安裝 Kaspersky Endpoint Security 管理外掛程式

如果您使用卡巴斯基安全管理中心管理 Kaspersky Endpoint Security，則必須解除安裝 Kaspersky Endpoint Security 管理 Web 外掛程式或 MMC 外掛程式，具體取決於您用來管理卡巴斯基安全管理中心的主控台。

如何移除 Kaspersky Endpoint Security MMC 管理外掛程式

1. 關閉卡巴斯基安全管理中心管理主控台。
2. 在安裝了卡巴斯基安全管理中心管理主控台的裝置上，開啟 Windows 登錄檔編輯器並前往：

   ```
   HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\KasperskyLab\Components\28\Plugins
   ```

   此項目包含關於管理主控台中安裝的所有管理外掛程式的資訊。受管理應用程式的名稱位於**DisplayName**值中。
3. 選擇與 Kaspersky Endpoint Security 應用程式外掛程式相關版本相對應的部分。
4. 開啟並複製**UninstallString**值。
5. 以管理員身分開啟指令提示符，貼上複製的值並按**Enter**。

如何移除 Kaspersky Endpoint Security Web 外掛程式

1. 在卡巴斯基安全管理中心網頁主控台的主視窗中，選擇 **設定** → **Web 外掛程式**。

   已安裝的 Web 外掛程式清單將開啟。
2. 選取 **Kaspersky Endpoint Security <version number> for Linux** 核取方塊。
3. 點擊“**刪除**”。

   確認解除安裝 Web 外掛程式。

使用應用程式

預設情況下，Kaspersky Endpoint Security 會在作業系統啟動時自動啟動（在每個作業系統的預設執行層級）。

當應用程式以預設設定啟動時，將啟動以下元件：

- 檔案威脅防護。
- 裝置控制。
- 行為偵測。
- Web 威脅防護— 僅當作業系統中安裝了受支援的瀏覽器之一併且允許在裝置上本機管理 Web 威脅防護設定（未套用政策或未在政策屬性中設定"鎖定"）時。
- 網路威脅防護— 僅當裝置上的網路威脅防護設定是透過政策定義時。預設情況下，網路威脅防護在政策屬性中啟用。如果在裝置上套用本機配置的設定，則預設會停用網路威脅防護。

當應用程式啟動時，裝置上會自動啟動服務工作，以確保其他應用程式功能的運作：應用程式啟動功能和備份功能。

預設情況下，應用程式也會啟動在指令列上配置的使用者工作，為此配置了"應用程式啟動後"執行模式（PS 執行模式）。

如果停止應用程式，裝置上執行的所有工作都將中斷。以 PS 執行模式執行但遭到中斷的使用者工作，不會從中斷之處繼續執行。下次啟動應用程式時，此類工作將從頭開始執行，而不會從中斷之處繼續執行。如需有關工作類型的詳細資訊，請參閱「Kaspersky Endpoint Security 本機工作」一節。

Kaspersky Endpoint Security 狀態由看門狗服務監控。應用程式啟動時，看門狗服務會自動啟動。如果應用程式崩潰，則會產生傾印檔案並自動重新啟動應用程式。

如何使用網頁主控台啟動或停止應用程式

1. 在網頁主控台主視窗中，選擇**資產（裝置）→受管理裝置**。
   受管理裝置的清單將開啟。
2. 在清單中，選擇要在其上啟動或停止應用程式的裝置，然後點擊帶有裝置名稱的連結以開啟裝置屬性視窗。
3. 選取"**應用程式**"標籤。
4. 選擇 Kaspersky Endpoint Security 核取方塊。
5. 執行下列操作之一：
   - 要啟動應用程式，請點擊**啟動**按鈕。
   - 要停止應用程式，請點擊**停止**按鈕。

您可以使用**監控和報告/儀表板**視窗中的**防護狀態**小工具來監控應用程式的運作狀態。

如何使用管理主控台啟動或停止應用程式

1. 在管理主控台樹狀圖中的**管理裝置**資料夾中，選擇包含必要裝置的管理群組。
2. 在工作區選取“**裝置**”標籤。
3. 在受管理裝置清單中，選擇要啟動或停止應用程式的裝置。在裝置內容功能表中，選擇**屬性**。
4. 在**屬性中：<裝置名稱>**視窗中，選擇**應用程式**部分。
   視窗右側顯示裝置上安裝的卡巴斯基應用程式清單。
5. 選取“Kaspersky Endpoint Security”。
6. 執行下列操作之一：
   – 啟動應用程式。
   – 停止應用程式。
   您也可以從內容功能表管理應用程式。

如何使用命令列啟動或停止應用程式

要執行應用程式，root 帳戶必須是以下目錄的所有者，並且只有所有者必須對這些目錄具有寫入存取權限：/var、/var/opt、/var/opt/kaspersky、/var/log/kaspersky、/opt、/opt/kaspersky、/usr/bin、/usr/lib、/u

配備 systemd 的作業系統

啟動應用程式

```
systemctl start kesl
```

停止應用程式

```
systemctl stop kesl
```

重新啟動應用程式

```
systemctl restart kesl
```

顯示應用程式的目前狀態

```
systemctl status kesl
```

配備 init 的作業系統

啟動應用程式

```
service kesl start
```

停止應用程式

```
service kesl stop
```

重新啟動應用程式

```
service kesl restart
```

顯示應用程式的目前狀態

```
service kesl status
```

產品授權

*產品授權*是根據最終使用者產品授權協議授予的使用 Kaspersky Endpoint Security 的有時間限制的權利。應用程式的可用功能清單和有效期取決於使用該應用程式的產品授權。

產品授權類型

免費

- *試用版* - 用於試用應用程式的免費產品授權。

  試用版產品授權擁有短暫有效期。當試用版授權到期，所有 Kaspersky Endpoint Security 功能將轉為停用。要繼續使用程式，您需要獲得正式版的產品授權。

  您只能使用試用產品授權啟動應用程式一次。使用正式產品授權啟動應用程式後，就無法再使用試用產品授權啟動。

- *卡巴斯基安全管理中心雲端主控台試用產品授權*是供評估雲端主控台使用的產品授權。透過此產品授權，您可以在 30 天內於工作區中執行操作。所有受管理應用程式（包括 Kaspersky Endpoint Security）均在卡巴斯基安全管理中心雲端主控台試用版產品授權下自動啟動。不過，當雲端主控台的試用版產品授權到期時，您無法使用 Kaspersky Endpoint Security 自己的試用版產品授權來啟動它。

  試用工作區會在 30 天期限到期後連同其所有內容自動刪除。

付費

- *正式版* – 購買應用程式時提供的付費產品授權。

  當正式產品授權到期時，應用程式的主要功能將停止運作。要繼續使用 Kaspersky Endpoint Security，您需要續約正式產品授權。產品授權到期後，您將無法再使用該應用程式，並且必須將其從裝置上解除安裝。

- *訂購*是針對應用程式的購買訂單，具有特定參數（訂購到期日期、受保護的裝置數量）。您可以向所在地區的服務供應商購買訂購。

訂購可以是有限訂購（範例一年時間）或無限訂購（無到期時間）。有限訂購到期時，您可能得到訂購續費寬限期，在此期間應用程式繼續執行。服務提供者決定是否給予寬限期，如果給予，則確定寬限期的持續時間。

您可以在服務供應商的網站上管理您的訂購，包括取消訂購。

產品授權的運作方式

1. **您將收到啟動碼**

   在您於 卡巴斯基官方網站 或透過我們的合作夥伴購買卡巴斯基解決方案後，您將在購買時指定的電子郵件地址收到一封郵件。此郵件將包含啟動碼，以及如何取得金鑰檔案的資訊。如果您的組織不支援使用代碼線上啟動應用程式，您可能需要金鑰檔案。

   > 如果您已購買 Kaspersky Endpoint Security 訂購，服務供應商將只會提供啟動碼給您。

2. **啟動應用程式**

   接下來，您需要*啟動應用程式*，也就是讓應用程式產品授權生效。為此，您需要使用啟動碼或金鑰檔案，將產品授權金鑰新增至應用程式。

   提供下列啟動方法：

   - 使用卡巴斯基安全管理中心進行遠端啟動
   - 在指令列上
   - 透過圖形介面

   標準模式

   若要在標準模式下使用應用程式，您可以使用涵蓋不同功能範圍的產品授權。如果您的產品授權未涵蓋某些元件，您可能需要其他產品授權金鑰：

   - Kaspersky Endpoint Detection and Response Optimum Add-on 產品授權金鑰（以下也稱為 *EDR Optimum 金鑰*），用於啟動 Kaspersky EDR Optimum 元件
   - Kaspersky Unified Monitoring and Analysis Platform Add-on 產品授權金鑰（以下也稱為 *KUMA 金鑰*），用於啟動與 Kaspersky Unified Monitoring and Analysis Platform 功能的整合
   - Kaspersky Managed Detection and Response Optimum/Expert Add-on 產品授權金鑰（以下也稱為 *MDR 金鑰*），用於啟動 Kaspersky MDR 元件
   - Kaspersky Endpoint Detection and Response Expert (on-premises) Add-on 產品授權金鑰（以下也稱為 *EDR Expert（on-premises）金鑰*），用於啟動 EDR Expert（on-premises）元件
   - Kaspersky Endpoint Detection and Response Expert (cloud) Add-on 產品授權金鑰（以下也稱為 *EDR Expert (cloud) 金鑰*），用於啟動 EDR Expert (cloud) 元件
   - Kaspersky Workload Security Module Add-on 產品授權金鑰（以下也稱為 *KWSM 金鑰*），用於啟動 系統完整性監控 和 容器掃描 元件

   如果您的產品授權未涵蓋這些元件，您只能在啟動 Kaspersky Endpoint Security 應用程式本身之後啟動它們。

   EDR Agent 模式

如果您在 EDR Agent 模式下使用 Kaspersky Endpoint Security 應用程式，您需要 EDR Expert (on-premises) 產品授權金鑰才能啟動該應用程式。

Light Agent 模式

如果您在 Light Agent 模式下使用 Kaspersky Endpoint Security，則不需要將金鑰新增至應用程式。您需在 Protection Server 端啟動 Kaspersky Security for Virtualization Light Agent。

Endpoint Detection and Response Optimum 元件以及與卡巴斯基解決方案整合的元件也會在 Protection Server 端啟動。

排除應用程式啟動問題

3. **續訂產品授權或訂購**

建議您留意產品授權或訂購狀態，以便及時續訂。建議在產品授權到期前續訂，以確保您的裝置持續受到保護，免受安全威脅。

為了及時續訂產品授權，您可以使用備用金鑰。您可以在服務供應商網站上手動或自動續訂您的訂購。如果已按時對供應商的服務進行預付，無限期訂購會自動續約。

新增金鑰時的特殊注意事項

- 試用產品授權金鑰或訂購金鑰無法新增為備用金鑰。
- 備用金鑰的到期日必須晚於啟動金鑰的到期日。
- 如果已將啟動金鑰和備用金鑰新增至應用程式，而您新增了新的啟動金鑰，則新金鑰會取代先前新增的啟動金鑰；如果您新增了新的備用金鑰，則它會取代先前新增的備用金鑰。
- 如果已將啟動金鑰以及用於啟動 Endpoint Detection and Response Optimum 元件和與卡巴斯基解決方案整合之元件的金鑰新增至應用程式，而您已新增一個產品授權的備用金鑰，且該產品授權也涵蓋 Endpoint Detection and Response Optimum 元件和用於整合的元件，則啟動金鑰到期後，備用金鑰會成為啟動金鑰，並釋放其他啟動金鑰。之後，您可以使用這些金鑰在另一台裝置上啟動 Endpoint Detection and Response Optimum 元件和整合元件。

4. **檢視已新增產品授權金鑰的資訊**

您可以使用卡巴斯基安全管理中心遠端，或在受防護裝置本機使用指令列或圖形介面，檢視新增至應用程式的產品授權金鑰資訊。

實用文章

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 之間具約束力的協議，其中明定使用者使用應用程式的條款。

在開始使用應用程式之前，請仔細閱讀最終使用者產品授權協議的條款。

您可以閱讀最終使用者產品授權協議和隱私權政策，其中說明資料處理與提供方式：

- 在安裝應用程式之前，可在 license.<language identifier> 檔案中閱讀。此檔案包含在應用程式分發套裝中。
- 在Kaspersky Endpoint Security 安裝期間。

  在建立應用程式安裝套件時（如果使用卡巴斯基安全管理中心安裝），或在初始應用程式設定期間（如果使用指令列安裝），透過確認您同意最終使用者產品授權協議和隱私權政策的條款與條件，即表示您接受最終使用者產品授權協議和隱私權政策的條款與條件。如果您不接受最終使用者產品授權協議或隱私權政策的條款，則必須取消應用程式安裝，並且不得使用該應用程式。

- 應用程式安裝後，包含卡巴斯基應用程式最終使用者產品授權協議和隱私權政策文字的檔案位於受防護裝置的 /opt/kaspersky/kesl/doc/license.<language ID> 目錄中。

啟動碼

*啟動碼*是由 20 個字母數字字元組成的唯一序號。

要使用啟動碼啟動應用程式，您需要存取網際網路以便連線到卡巴斯基啟動伺服器。

如果啟動應用程式後丟失了啟動碼，請聯絡從其購買產品授權的卡巴斯基合作夥伴。

金鑰檔案

*金鑰檔案*是您從 Kaspersky 接收到的 .key 副檔名的檔案。若要使用金鑰檔案啟動應用程式，您不需要連線到卡巴斯基啟動伺服器。

如果金鑰檔案被意外刪除，您可以還原它。您可能需要金鑰檔案註冊諸如卡巴斯基公司帳戶之類的服務。

若要還原您的金鑰檔案，執行下面任何的操作：

- 聯絡產品授權銷售商。
- 根據您現有的啟動碼，在卡巴斯基網站上取得金鑰檔案。

產品授權金鑰

*產品授權金鑰*是一個序號，可用於按照最終使用者產品授權協議條款啟動和使用應用程式。產品授權金鑰由卡巴斯基專家產生。

應用程式目前用來啟動的金鑰會成為*作用中產品授權金鑰*。您可以新增試用產品授權金鑰、正式產品授權金鑰（正式金鑰）或訂購金鑰作為啟動金鑰。

備用金鑰

*備用產品授權金鑰*是允許使用者使用應用程式但目前未使用的產品授權金鑰。與目前啟動的產品授權金鑰相關聯的產品授權到期時，備用產品授權金鑰將自動成為目前產品授權金鑰。只有在已新增啟動金鑰後，才能新增備用金鑰。

試用版產品授權金鑰只能被新增為啟動產品授權金鑰。試用產品授權的產品授權金鑰無法新增為備用產品授權金鑰。

如何切換到其他卡巴斯基解決方案

如果應用程式以 Light Agent 模式使用，產品授權金鑰會在 Kaspersky Security for Virtualization Light Agent 解決方案中管理。

如果您的組織已部署卡巴斯基解決方案、Kaspersky Endpoint Security 以標準模式或 EDR Agent 模式使用，而且您需要切換到另一個卡巴斯基解決方案，請依照下列步驟操作。

1. **準備新的產品授權**

   在 卡巴斯基網站 或透過我們的合作夥伴購買另一個卡巴斯基解決方案。您將在購買時指定的電子郵件地址收到一封電子郵件。此郵件將包含啟動碼，以及如何取得金鑰檔案的資訊。

   如果您先前使用啟動碼啟動 Kaspersky Endpoint Security 應用程式，這次您也需要使用啟動碼。如果您先前使用金鑰檔案啟動應用程式，則需要使用金鑰檔案。

2. **取代您的產品授權**

   您可以透過以下方式取代產品授權：

   - 遠端使用卡巴斯基安全管理中心。將產品授權金鑰新增至管理伺服器儲存區，並將其分發到受防護的裝置。
   - 在 命令列上使用以下命令：`kesl-control [-L] --add-active-key <path to key file / activation code>`。
   - 在圖形介面中，刪除目前套用至應用程式的金鑰，並新增新的金鑰。

3. **確認產品授權已成功取代**

   若要執行此操作，請檢視產品授權金鑰的詳細資訊，此金鑰用於您受防護的裝置。

實用文章

啟動碼

*啟動碼*是由 20 個字母數字字元組成的唯一序號。

要使用啟動碼啟動應用程式，您需要存取網際網路以便連線到卡巴斯基啟動伺服器。

如果啟動應用程式後丟失了啟動碼，請聯絡從其購買產品授權的卡巴斯基合作夥伴。

金鑰檔案

*金鑰檔案*是您從 Kaspersky 接收到的 .key 副檔名的檔案。若要使用金鑰檔案啟動應用程式，您不需要連線到卡巴斯基啟動伺服器。

如果金鑰檔案被意外刪除，您可以還原它。您可能需要金鑰檔案註冊諸如卡巴斯基公司帳戶之類的服務。

若要還原您的金鑰檔案，執行下面任何的操作：

- 聯絡產品授權銷售商。
- 根據您現有的啟動碼，在卡巴斯基網站上取得金鑰檔案。

管理產品授權金鑰

如果應用程式以 Light Agent 模式使用，產品授權金鑰會在 Kaspersky Security for Virtualization Light Agent 解決方案中管理。產品授權金鑰管理命令傳回錯誤。

使用卡巴斯基安全管理中心進行金鑰管理

在 卡巴斯基安全管理中心 中，您可以透過以下方式將金鑰新增至受管理裝置：

- 使用 *新增金鑰* 工作。此方法可讓您將金鑰新增至個別裝置或管理群組中所有裝置上的應用程式。建立工作時，它使用新增到卡巴斯基安全管理中心金鑰儲存的金鑰。您可以事先將產品授權金鑰新增至金鑰庫，或在建立「新增金鑰」工作時新增。
- 透過將儲存在卡巴斯基安全管理中心管理伺服器上的金鑰分發到裝置。此方法可讓您自動將金鑰新增至已連線到卡巴斯基安全管理中心的受管理裝置以及新的受管理裝置。要使用此方法，首先將金鑰新增至卡巴斯基安全管理中心金鑰儲存。

  在將金鑰自動分發為啟動金鑰或備用金鑰期間，將考慮裝置數量的許可限制（在金鑰屬性中設定）。如果達到許可限制，則會自動停止向裝置分發此金鑰。您可以在金鑰屬性的“**裝置**”索引標籤中檢視已新增該金鑰的裝置數量以及其他資訊。

如何使用網頁主控台將金鑰新增至卡巴斯基安全管理中心金鑰儲存區

1. 在網頁主控台主視窗中，選擇**操作** → **卡巴斯基產品授權**。
2. 點擊“**新增**”按鈕。
3. 在開啟的視窗中，選擇如何將金鑰新增至儲存庫：
   - **輸入啟動碼**以使用啟動碼新增金鑰。
   - **新增金鑰檔案**以使用金鑰檔案新增金鑰。
4. 根據您在上一個步驟中選擇的金鑰新增方法，執行下列其中一項操作：
   - 輸入啟動碼並點擊**提交**。
   - 點擊**選取金鑰檔案**按鈕，然後在開啟的視窗中選擇一個副檔名為 .key 的檔案。
5. 點擊“**關閉**”按鈕。

新增的金鑰將出現在金鑰清單中。

如何使用「新增金鑰」工作透過網頁主控台將金鑰新增至應用程式

1. 在網頁主控台的主視窗中，選擇**工作**。
   工作清單開啟。

2. 點擊“**新增**”按鈕。
   啟動“工作精靈”。

3. 配置工作設定：

   a. 在**應用程式**下拉清單中，選擇應用程式名稱：Kaspersky Endpoint Security。

   b. 在**工作類型**下拉清單中，選擇**新增金鑰**。

   c. 在**工作名稱**欄位中輸入簡短描述，例如 *啟動 Kaspersky Endpoint Security*。

   d. 在**將分配工作之裝置**部分中，選擇工作範圍。按一下**下一步**。

4. 按照所選工作範圍選項選取裝置。按一下**下一步**。
   這會開啟 **選擇產品授權** 視窗。

5. 如果您之前已將金鑰新增至卡巴斯基安全管理中心金鑰儲存，請從清單中選擇該金鑰，然後點擊**下一步**。

6. 如果您需要的金鑰不在金鑰庫中，請點擊 **新增產品授權金鑰** 連結。

   a. 在開啟的視窗中，選擇如何將金鑰新增至儲存庫：

      - **輸入啟動碼**以使用啟動碼新增金鑰。
      - **新增金鑰檔案**以使用金鑰檔案新增金鑰。

   b. 根據您在上一個步驟中選擇的金鑰新增方法，執行下列其中一項操作：

      - 輸入啟動碼並點擊**提交**。
      - 點擊**選取金鑰檔案**按鈕，然後在開啟的視窗中選擇一個副檔名為 .key 的檔案。

   c. 閱讀關於金鑰的資訊，然後點擊**關閉**。

   d. 新增的金鑰將出現在金鑰清單中。從清單中選擇它並點擊**下一步**。

7. 閱讀關於產品授權的資訊，然後點擊**“下一步”**。

8. 在 **應用程式設定** 索引標籤上，您可以選取 **用作備用金鑰** 核取方塊。新增為備用金鑰的金鑰會在目前金鑰到期後成為啟動金鑰。

9. 完成精靈。
   在工作清單中將顯示一個新工作。

10. 選中該工作旁邊的核取方塊。點擊“**開始**”按鈕。

如何使用網頁主控台透過將金鑰分發到裝置來將金鑰新增至應用程式

1. 在網頁主控台主視窗中，選擇**操作→卡巴斯基產品授權**。
2. 使用帶有該金鑰所針對的應用程式名稱的連結開啟金鑰屬性。
3. 在**一般**索引標籤上，選取**自動將產品授權金鑰分發給受管理裝置**核取方塊。
4. 點擊“**儲存**”按鈕。

   產品授權金鑰會被自動分發到適當的用戶端裝置。

> 只有當應用程式尚未在裝置上啟動或產品授權在 14 天內到期時，新的產品授權金鑰才會被新增至裝置。

指令列中的金鑰管理

若要管理裝置上的產品授權金鑰，您可以使用產品授權金鑰管理指令。

如何將金鑰新增至應用程式

您可以使用這些命令新增用於啟動應用程式的金鑰，以及新增用於啟動不在您產品授權涵蓋範圍內之元件的金鑰。您不需要在指令中指定金鑰的類型。

將作用中產品授權金鑰新增至應用程式

```
kesl-control [-L] --add-active-key <path to key file / activation code>
```

其中：

- `path to key file` 是金鑰檔案的路徑。如果金鑰檔案位於目前目錄中，則僅指定檔案名稱就足夠了。
- `activation code` 是啟動碼。

將備用產品授權金鑰新增至應用程式

```
kesl-control [-L] --add-reserve-key <path to key file / activation code>
```

> 如果尚未將活動金鑰新增至裝置上的應用程式，則指令失敗。

如何刪除金鑰

有多種命令可用於刪除金鑰。

刪除啟動金鑰

```
kesl-control [-L] --remove-active-key
```

刪除備用金鑰

```
kesl-control [-L] --remove-reserve-key
```

刪除 EDR Optimum 啟動金鑰

```
kesl-control [-L] --remove-active-key --edr-optimum
```

刪除 EDR Optimum 備用金鑰

```
kesl-control [-L] --remove-reserve-key --edr-optimum
```

刪除 KUMA 啟動金鑰

```
kesl-control [-L] --remove-active-key --kuma
```

刪除 KUMA 備用金鑰

```
kesl-control [-L] --remove-reserve-key --kuma
```

刪除 MDR 啟動金鑰

```
kesl-control [-L] --remove-active-key --mdr
```

刪除 MDR 備用金鑰

```
kesl-control [-L] --remove-reserve-key --mdr
```

刪除 EDR Expert (on-premises) 作用中產品授權金鑰

```
kesl-control [-L] --remove-active-key --edr-kata
```

刪除 EDR Expert (on-premises) 備用產品授權金鑰

```
kesl-control [-L] --remove-reserve-key --edr-kata
```

刪除 EDR Expert (cloud) 啟動金鑰

```
kesl-control [-L] --remove-active-key --cxdr
```

刪除 EDR Expert (cloud) 備用金鑰

```
kesl-control [-L] --remove-reserve-key --cxdr
```

刪除 KWSM 啟動金鑰

```
kesl-control [-L] --remove-active-key --khcs
```

刪除 KWSM 備用金鑰

```
kesl-control [-L] --remove-reserve-key --khcs
```

圖形介面中的金鑰管理

如何新增作用中產品授權金鑰

1. 開啟應用程式圖形介面的主視窗。

2. 請執行以下操作之一：

   - 在主視窗的下方，點擊顯示關於產品授權和金鑰的資訊的區域。

   - 在主視窗下方，點擊**支援**按鈕開啟**支援**視窗，然後在該視窗中，點擊**產品授權金鑰**或視窗下方的**產品授權**連結。

   這將開啟**產品授權**視窗。

   點擊此視窗中的**購買產品授權**按鈕將開啟卡巴斯基線上商店，您可以在那裡購買產品授權。

3. 如果您想在正式產品授權下啟動應用程式：

   a. 點擊**正式金鑰**部分中的**新增**按鈕，然後執行以下操作，具體取決於您用於新增金鑰的方法：

      - 如果您想使用啟動碼新增金鑰，請輸入啟動碼並點擊**下一步**按鈕。

      - 如果您想要使用金鑰檔案來新增金鑰，請點擊**選取金鑰檔案**連結以開啟檔案選擇視窗，在該視窗中選擇副檔名為 .key 的檔案。

      此視窗會顯示金鑰及其相關產品授權的資訊。

   b. 點擊**啟動**按鈕。

4. 如果您想在試用版產品授權下啟動應用程式，請點擊**試用版金鑰**部分中的**啟動**按鈕。此視窗會顯示試用產品授權及其相關金鑰的資訊。

如何新增備用產品授權金鑰

1. 開啟應用程式圖形介面的主視窗。

2. 請執行以下操作之一：

   - 在主視窗的下方，點擊顯示關於產品授權和金鑰的資訊的區域。

   - 在主視窗下方，點擊**支援**按鈕開啟**支援**視窗，然後在該視窗中，點擊**產品授權金鑰**或視窗下方的**產品授權**連結。

   這將開啟**產品授權**視窗。此視窗將顯示關於先前新增的產品授權金鑰的資訊。

3. 點擊**新增**按鈕並執行以下操作，具體取決於您用來新增金鑰的方法：

   - 如果您想使用啟動碼新增金鑰，請輸入啟動碼並點擊**下一步**按鈕。

   - 如果您想要使用金鑰檔案來新增金鑰，請點擊**選取金鑰檔案**連結以開啟檔案選擇視窗，在該視窗中選擇副檔名為 .key 的檔案。

此視窗會顯示金鑰及其相關產品授權的資訊。

4. 點擊“**新增**”按鈕。

如何移除產品授權金鑰

1. 開啟應用程式圖形介面的主視窗。

2. 請執行以下操作之一：

   - 在主視窗的下方，點擊顯示關於產品授權和金鑰的資訊的區域。

   - 在主視窗下方，點擊**支援**按鈕開啟**支援**視窗，然後在該視窗中，點擊**產品授權金鑰**或視窗下方的**產品授權**連結。

   這將開啟**產品授權**視窗。此視窗將顯示關於先前新增的產品授權金鑰的資訊。

3. 點擊要刪除的金鑰資訊右側的**刪除**按鈕。

4. 在開啟的視窗中確認刪除。

實用文章

[排除應用程式啟動問題](#)

檢視產品授權金鑰的資訊

卡巴斯基安全管理中心中的產品授權金鑰資訊

您可以透過以下方式檢視關於 Kaspersky Endpoint Security 正在使用的產品授權金鑰的資訊：

- 在用於啟動應用程式的 *新增金鑰* 工作的屬性中，您可以找到此工作新增至應用程式之金鑰的資訊。

- 在安裝於用戶端裝置的卡巴斯基應用程式屬性中，您可以找到在此裝置上新增至應用程式的活動金鑰和備用金鑰的資訊。

  如何使用網頁主控台檢視裝置上的產品授權金鑰資訊

  1. 在網頁主控台的主視窗中，選取 **資產管理 → 資產 (裝置)**。

     受管理裝置的清單將開啟。

  2. 選擇包含必要裝置的管理群組。若要選取巢狀群組，請按一下視窗上方的 **顯示階層結構** 按鈕。

     此清單僅顯示選定管理群組的受管理裝置。

  3. 按一下裝置名稱。

  4. 這將開啟受管理裝置屬性視窗；在該視窗中，轉到**應用程式**索引標籤。

5. 在裝置上安裝的應用程式清單中，點擊 Kaspersky Endpoint Security。

6. 這會開啟應用程式屬性視窗；在該視窗中，前往 **一般** 索引標籤上的 **產品授權** 區段。
   此部分顯示關於新增至應用程式的產品授權金鑰以及與這些金鑰關聯的產品授權的資訊。

   - **產品授權金鑰狀態**是金鑰類型：活動或備用。
   - **應用程式名稱**是與金鑰關聯的產品授權的名稱以及關於此產品授權的資訊。
   - **產品授權金鑰**是產品授權金鑰，一個唯一的字母數字序列。
   - **產品授權類型**可以是試用版、正式版或訂購。
   - **啟動日期**是新增此金鑰的日期。
   - **到期日期**是您使用透過新增此金鑰啟動的應用程式的權利到期日期。

如何使用管理主控台檢視裝置上的產品授權金鑰資訊

1. 在卡巴斯基安全管理中心管理主控台樹中的**受管理裝置**資料夾中，選擇包含所需裝置的管理群組。

2. 在工作區選取"**裝置**"標籤。

3. 在受管理裝置清單中，選擇所需的裝置並雙擊它以開啟**屬性：<工作名稱>**視窗。

4. 在顯示的受管理裝置屬性視窗中，選取「**應用程式**」區段。
   視窗右側顯示裝置上安裝的卡巴斯基應用程式清單。

5. 選擇 Kaspersky Endpoint Security 並雙擊它以開啟應用程式屬性視窗。或者，您可以使用視窗下部的**屬性**按鈕。

6. 這將開啟一個視窗；在該視窗中，轉到**產品授權金鑰**部分。
   本節包含關於活動和備用產品授權金鑰的資訊：

   - **序號**：唯一的字母數字序列。
   - **狀態**：產品授權金鑰的狀態，例如啟用或備用。
   - **類型**：產品授權類型（正式或試用）。
   - **產品授權有效期限**：透過新增此金鑰啟動應用程式後，可使用該應用程式的天數。
   - **產品授權限制**：可使用此金鑰的裝置數量。
   - **啟動日期**（此欄位僅適用於啟動金鑰）：新增啟動金鑰時的日期。
   - **產品授權到期日**（此欄位僅適用於啟動金鑰）：應用程式不再能使用目前啟動金鑰所使用的日期。

- 產品授權金鑰使用報告會顯示使用卡巴斯基安全管理中心新增的所有金鑰的資訊。您可以使用網頁主控台（「**監控和報告**」→「**報告**」）以及管理主控台（「**報告**」索引標籤）檢視產品授權金鑰使用報告。若要檢視報告，您需要在報告清單中選擇"產品授權金鑰使用情況報告"範本並開始產生報告。

- 卡巴斯基安全管理中心產品授權金鑰儲存區會顯示新增至卡巴斯基安全管理中心管理伺服器的所有金鑰資訊。您可以使用網頁主控台（**操作 → 卡巴斯基產品授權**）或使用管理主控台（**卡巴斯基產品授權**資料夾）開啟金鑰儲存。

您也可以使用關於卡巴斯基安全管理中心事件的通知來取得關於已使用的產品授權金鑰及與其關聯的產品授權的資訊。應用程式將關於過期產品授權和產品授權違規的資訊傳送到卡巴斯基安全管理中心伺服器。

受保護裝置上的產品授權金鑰資訊

如何在命令列檢視產品授權金鑰資訊

檢視裝置上的產品授權金鑰和產品授權資訊

```
kesl-control -L --query [--json]
```

其中 `--json` 表示以 JSON 格式輸出資料。如果不指定`--json`選項，設定將被輸出到主控台。

此命令向主控台輸出以下資訊：

- 作用中產品授權金鑰的資訊：
  - 產品授權到期日期和時間。
  - 距離產品授權期限結束的天數。
  - 有關保護功能限制的資訊（此行僅針對用於啟動 Kaspersky Endpoint Security 應用程式的金鑰顯示）。
  - 應用程式資料庫更新限制的資訊。
  - 關於產品授權金鑰狀態的資訊。
  - 與金鑰關聯的產品授權類型。
  - 金鑰的許可限制（許可單元數量）。
  - 該金鑰要啟動的應用程式的名稱。
  - 啟動的產品授權金鑰（唯一的字母數字序列）。
  - 啟動日期。
- 備用產品授權金鑰的資訊。如果應用程式以標準模式或 EDR Agent 模式使用，且已新增備用金鑰，則會顯示此資訊。如果應用程式以 Light Agent 模式使用，則不會顯示備用金鑰資訊。
  - 產品授權到期日期和時間。
  - 有關保護功能限制的資訊（此行僅針對可用於啟動 Kaspersky Endpoint Security 應用程式的金鑰顯示）。
  - 應用程式資料庫更新限制的資訊。
  - 關於產品授權金鑰狀態的資訊。
  - 與金鑰關聯的產品授權類型。
  - 金鑰的許可限制（許可單元數量）。
  - 該金鑰要啟動的應用程式的名稱。

- 備用產品授權金鑰（唯一的字母數字序列）。
- 與啟動金鑰關聯的產品授權到期的日期和時間（UTC）。

在檢視應用程式詳細資訊時，您也可以取得應用程式所使用之產品授權的相關資訊：

```
kesl-control --app-info
```

如何在應用程式圖形介面中檢視產品授權和金鑰資訊

1. 開啟應用程式圖形介面的主視窗。
2. 請執行以下操作之一：
   - 在主視窗的下方，點擊顯示關於產品授權和金鑰的資訊的區域。
   - 在主視窗下方，點擊**支援**按鈕開啟**支援**視窗，然後在該視窗中，點擊**產品授權金鑰**或視窗下方的**產品授權**連結。

   這將開啟**產品授權**視窗。

   此視窗顯示關於新增至應用程式的啟動金鑰和備用金鑰的資訊。點擊**更多資訊**連結以檢視關於產品授權和金鑰的完整資訊。

目前產品授權區段會顯示已新增的啟動金鑰和關聯產品授權的資訊：

- 產品授權類型、產品授權限制和產品授權期限。
- **產品授權金鑰** — 唯一的字母數字序列。
- **金鑰狀態** — 金鑰的狀態或與金鑰關於的問題的訊息（如果有）。
- **有效自** — 透過新增此金鑰來啟動應用程式的日期。
- **到期日** — 產品授權到期前的天數以及產品授權到期日 (UTC)。
- **名稱**— 為其新增啟動金鑰的應用程式的名稱。
- **防護**— 關於防護功能限制和更新應用程式資料庫的能力的資訊。

備用金鑰區段會顯示已新增的備用金鑰和關聯產品授權的資訊：

- 備用金鑰的類型、產品授權限制以及與該金鑰關聯的產品授權期限。
- **產品授權金鑰** — 唯一的字母數字序列。
- **產品授權類型** — 與備用金鑰關聯的產品授權類型。
- **名稱**— 為其新增啟動金鑰的應用程式的名稱。
- **防護**— 關於防護功能限制和更新應用程式資料庫的能力的資訊。

如果您以標準模式或 EDR Agent 模式使用 Kaspersky Endpoint Security 應用程式，並使用卡巴斯基安全管理中心管理該應用程式，則預設會將產品授權金鑰新增和移除的資訊以及產品授權期限到期的資訊記錄在作業系統日誌中。

應用程式的管理介面

若要管理 Kaspersky Endpoint Security，您可以使用：

- 卡巴斯基安全管理中心
- 命令列
- 應用程式的圖形介面

> 您只能使用 Kaspersky Endpoint Security 圖形介面執行有限的動作。

如果 Kaspersky Endpoint Security 用於防護虛擬環境的 Light Agent 模式，則無法使用卡巴斯基安全管理中心雲端主控台和應用程式的圖形介面來管理應用程式。

如果應用程式以 EDR Agent 模式使用，則僅提供有限的應用程式元件和任務。您可以管理某些防護元件、啟動應用程式，以及更新資料庫。若要深入瞭解 EDR Agent 模式的特殊方面，請參閱 已知問題和限制 一文。

請根據您組織的 IT 基礎架構，以及管理員的角色和工作流程，選擇管理工具。我們建議使用卡巴斯基安全管理中心，以集中方式遠端管理用戶端裝置上的應用程式。

使用卡巴斯基安全管理中心管理應用程式

卡巴斯基安全管理中心可讓您遠端和集中管理用戶端裝置上 Kaspersky Endpoint Security 的操作。您可以遠端安裝和解除安裝、啟動和停止Kaspersky Endpoint Security；配置應用程式的設定，以及應用程式的各個元件和工作的設定；並在受管理裝置上啟動和停止工作。

卡巴斯基安全管理中心管理群組

若要使用卡巴斯基安全管理中心來管理安裝在裝置上的 Kaspersky Endpoint Security，您需要將這些裝置新增至*管理群組*。您可以在安裝 Kaspersky Endpoint Security 之前在卡巴斯基安全管理中心中建立管理群組，並設定規則以自動將裝置移至管理群組。您也可以在安裝應用程式後手動將裝置移至管理群組（詳細資訊，請參閱卡巴斯基安全管理中心說明）。

管理主控台和管理外掛程式

您可以使用以下卡巴斯基安全管理中心管理主控台透過卡巴斯基安全管理中心來管理 Kaspersky Endpoint Security：

- 卡巴斯基安全管理中心管理主控台（以下也稱為“管理主控台”）。這是安裝在管理員工作站上的 Microsoft 管理主控台 (MMC) 管理單元，為管理伺服器和網路代理管理服務提供使用者介面。

  透過卡巴斯基安全管理中心管理主控台管理 Kaspersky Endpoint Security 的介面由 Kaspersky Endpoint Security MMC 管理外掛程式（以下也稱為 "MMC 外掛程式"）提供。

MMC 外掛程式必須安裝在已安裝卡巴斯基安全管理中心管理主控台的裝置上。

- 卡巴斯基安全管理中心網頁主控台（以下也稱為 *網頁主控台*）。這是用於管理基於卡巴斯基應用程式的防護系統的 Web 介面。您可以在任何裝置上使用瀏覽器操作卡巴斯基安全管理中心網頁主控台。

  透過卡巴斯基安全管理中心網頁主控台管理 Kaspersky Endpoint Security 的介面由 Kaspersky Endpoint Security 管理 Web 外掛程式（以下也簡稱為 Web 外掛程式）提供。

  Web 外掛程式必須安裝在已安裝卡巴斯基安全管理中心網頁主控台的裝置上。

- 卡巴斯基安全管理中心雲端主控台。這是卡巴斯基安全管理中心安全應用程式雲端版本中的基於雲端的管理主控台，也稱為卡巴斯基安全管理中心雲端主控台。雲端主控台的介面與卡巴斯基安全管理中心網頁主控台介面類似。透過卡巴斯基安全管理中心雲端主控台管理 Kaspersky Endpoint Security 的介面也由 Web 外掛程式提供。

  如果 Kaspersky Endpoint Security 以 Light Agent 模式使用，則無法使用卡巴斯基安全管理中心雲端主控台管理應用程式。

Kaspersky Endpoint Security 是 Kaspersky Next Pro View 解決方案的一部分。關於此解決方案中應用程式可用功能的更多資訊，請參閱Kaspersky Next 說明。

卡巴斯基安全管理中心政策與工作

MMC 外掛程式和 Web 外掛程式可讓您在卡巴斯基安全管理中心中建立政策和工作來管理 Kaspersky EndpoinSecurity 的運作：

- *政策*是套用於管理群組內所有裝置的一組設定。政策可讓您將相同的應用程式設定套用至管理群組內的所有用戶端裝置。

  Kaspersky Endpoint Security 安全政策定義了 Kaspersky Endpoint Security 運行的一般設定以及套用該政策的裝置上應用程式各個功能元件運行的設定。

- 在卡巴斯基安全管理中心中建立的 Kaspersky Endpoint Security *工作*在受防護的裝置上執行，並實施 Kaspersky Endpoint Security 功能，例如按需掃描、應用程式啟動以及應用程式資料庫和模組的更新。

  在卡巴斯基安全管理中心中，您可以建立在單個裝置上執行的工作（本機工作）、管理群組中所有裝置的工作（群組工作）或隨機裝置分類的工作（裝置集工作）。

卡巴斯基安全管理中心政策

*政策*是一組套用於管理群組中包含的所有用戶端裝置的 Kaspersky Endpoint Security 設定。政策具有以下狀態之一：

政策狀態

狀態	描述
啟動	目前套用至裝置的政策。
非作用中	目前未套用於裝置的政策。
漫遊	如果選擇此選項，則當裝置離開組織網路時，政策將生效。

政策遵循以下規則：

- 您可以為一個應用程式設定多個具有不同設定的政策。
- 每個應用程式只能有一個作用中政策。
- 政策可以有子政策。

鎖定設定

每個政策設定都有「掛鎖」屬性。此屬性的狀態會決定設定是否傳遞至管理群組中的受管理裝置。

- 如果「掛鎖」已關閉 (🔒)，則表示該設定會套用到已套用此政策的裝置。使用者無法在受管理應用程式的使用者介面中變更此類設定。此類設定被稱為 *已鎖定*。
- 如果「掛鎖」已開啟 (🔓)，則表示未在政策中指定該設定。使用者可以在受管理應用程式的使用者介面中變更此類設定。此類設定被稱為 *已解鎖*。

建議您鎖定想要套用至受管理裝置的政策設定。未鎖定的政策設定可在受管理裝置上被覆寫。

網頁主控台和管理主控台中帶有「掛鎖」的設定數量可能不同。

政策設定檔

為避免必須支援大量政策，例如在只有少數設定應可變更的情況下，您可以使用政策設定檔。

*政策設定檔*是一組個別的政策設定，這些設定與「基礎」政策設定不同，並且會在符合設定的條件（啟動規則）時套用至用戶端裝置。使用政策設定檔可讓您靈活地對不同裝置進行應用程式設定。

使用“掛鎖”鎖定的個人檔案設定將覆蓋政策設定。也就是說，如果用掛鎖鎖定的個人檔案設定與政策設定不同，則應用程式將會套用個人檔案中的設定。不過，設定清單會合併，互相補充。也就是說，如果個人檔案清單中的設定在'基本"政策中缺失，則這些設定將會被新增至結果設定清單中。

政策設定檔遵循以下規則：

- 政策設定檔會在滿足特定啟動條件時生效。
- 政策設定檔包含與政策中設定的值不同的設定值。
- 啟動政策設定檔會變更受管理裝置的有效設定（目前套用至裝置的設定）。
- 政策最多可以有 100 個設定檔。

設定繼承

政策有一個層次結構，類似管理群組。*子政策*是嵌套層次結構的政策，即嵌套管理群組和從屬管理伺服器的政策。

預設情況下，子政策從父政策繼承設定。如果父政策中的設定已鎖定 (🔒)，子政策和應用程式的本機設定會取得相同的值，且該設定會被鎖定。如有必要，您可以停用從父政策繼承設定。漫遊政策不透過管理群組的階層架構影響其他政策。

> 如果子政策的設定已鎖定（*存取被拒絕* 錯誤），請檢查使用者的存取權限。如果使用者有權編輯政策設定，請啟動卡巴斯基安全管理中心的 *將更新下載至管理伺服器儲存區* 工作，然後重複授權。在卡巴斯基安全管理中心中升級管理外掛程式後，可能會發生此錯誤：下載更新後，應用程式會取得新版管理外掛程式所需的檔案。

對於某些以清單作為值的設定（例如規則清單、排除清單），您可以啟用清單項目的合併。若要合併清單項目，請依下列步驟操作：

- 在子政策的內容中，於 **一般** 索引標籤上啟用 **從父政策繼承設定** 設定。
- 在父政策的內容中，點擊掛鎖 (🔒) 圖示將其「鎖定」。
- 在父政策的內容中，透過選取**合併繼承的值**核取方塊來啟用設定合併功能。如果選取該核取方塊，則卡巴斯基安全管理中心的父政策清單中的項目將顯示在子政策中，並且可以將項目新增至子原則清單。如果取消選中此核取方塊，則在繼承政策設定時不會合併清單項目。

您無法刪除或修改子政策中的繼承清單項目。繼承時合併的清單項目只能在父政策中刪除或修改。可在較低層級新增、修改或刪除清單項目。因此，您可以在父政策中設定一個清單，該設定將套用於所有子政策，並且您還可以在子政策中向清單新增更多項目。

> 如果從父政策中透過繼承合併的清單刪除某個項目，該項目不會從子政策中刪除。若要從子政策中刪除此項目，您必須開啟這些政策的內容並手動刪除該項目。

有些清單未合併。如果發生這種情況，設定檔中的設定將覆蓋“基準”政策的設定：

- 按檔案威脅防護和行為偵測元件中的處理程序排除
- 檔案威脅防護和加密軟體防護元件中的防護範圍
- 系統完整性監控元件中的監控範圍
- 應用程式元件控制中的規則清單（在**應用程式控制規則**視窗中）
- Web 控制中的規則清單
- 應用程式設定中的處理程序記憶體排除項目
- 網路設定中的受信任網域
- 網路設定中的受信任根憑證

- 網路設定中的監控的連接埠
- SVM 偵測設定中的 SVM 位址清單

首次套用政策後，應用程式設定將根據政策設定而變更。

如需關於政策與政策設定檔以及設定繼承機制的詳細資訊，請參閱 卡巴斯基安全管理中心說明。

政策管理

如何在網頁主控台中建立政策

1. 在網頁主控台的主視窗中，選擇**資產管理 → 政策**。

   政策和政策個人檔案的清單將開啟。

2. 選擇您要套用政策的管理群組。若要選取巢狀群組，請按一下視窗上方的 **顯示階層結構** 按鈕。

3. 點擊"**新增**"。

   啟動"政策精靈"。

4. 在顯示的視窗中，從清單中選取 Kaspersky Endpoint Security。

   繼續精靈的下一步。

5. 指定 Kaspersky Endpoint Security 使用模式：

   - 在 **標準模式或者 Endpoint Detection and Response Agent 模式** 中，該應用程式可作為獨立應用程式，或作為支援卡巴斯基 Detection and Response 解決方案與協力廠商病毒防護解決方案協同工作的應用程式，用於防護 Linux 裝置。

     若要選擇此模式，請前往精靈的下一步。

   - **Light Agent 防護虛擬環境** – 作為卡巴斯基 Security for Virtualization Light Agent 解決方案的一部分，應用程式用於防護執行 Linux 來賓作業系統的虛擬機。

6. 如果您在 Light Agent 模式下使用應用程式，請配置 SVM 偵測設定：

   a. 選擇 Light Agent 用於發現可連線的 SVM 的方法。

      - **使用 Integration Server**如果選擇此選項，Light Agent 將連線至 Integration Server 以獲取可用於連線的 SVM 清單和其詳情。
      - **使用 SVM 位址自訂清單**如果選擇此選項，您可以指定此政策管理的 Light Agent 可以連線到的 SVM 清單。Light Agent 將僅連線到清單中指定的 SVM。

      如果您選取 **使用 SVM 位址自訂清單** 選項，Light Agent 使用延伸 SVM 選擇演算法，且 SVM 已啟用大型基礎架構防護模式，則只有在忽略 SVM 路徑時，才能將 Light Agent 連線到此 SVM。在 **SVM 選擇演算法** 區段中，您需要將 **SVM 路徑** 設定設為 **略過**。如果設定了任何其他值，Light Agent 將無法連線到 SVM。如需更多詳細資訊，請參閱 Kaspersky Security for Virtualization Light Agent 說明。

b. 如果選擇 Integration Server，精靈將顯示將 Light Agent 連線到 Integration Server 的目前設定：用於連線的位址和連接埠。如有必要，指定新的連線設定：

a. 點擊 **配置** 按鈕，並在開啟的視窗中指定新的連線設定：

- **位址**安裝 Integration Server 的裝置的 IP 位址（IPv4 格式）或完全限定網域名稱 (FQDN)。如果將位址指定為 NetBIOS 名稱、localhost 或 127.0.0.1，與 Integration Server 的連線將完成並顯示錯誤。
- **連接埠**連線 Integration Server 的連接埠。預設情況下，指定連接埠為 7271。

> 如果您的基礎架構中部署了基於 Linux 的高可用性 Integration Server 叢集，則需要將負載均衡器的位址和連接埠指定為用於連線到 Integration Server 的位址和連接埠。如需更多詳細資訊，請參閱 Kaspersky Security for Virtualization Light Agent 說明。

b. 點擊"**檢查**"。

c. Web 外掛程式檢查從 Integration Server 收到的 SSL 憑證。如果憑證包含錯誤或不受信任，則會在 **Integration Server 連線設定** 視窗中顯示對應的訊息。

您可以透過點擊**驗證收到的憑證**行來檢視關於從 Integration Server 收到的憑證的資訊。

> 如果您遇到 SSL 憑證問題，我們建議您確保使用的資料傳輸通道是安全的。

若要儲存收到的憑證並繼續連線到 Integration Server，請在**選取一個動作**區塊中選擇**略過**選項。

d. 指定 Integration Server 管理員的密碼（`admin`帳號的密碼），點擊**測試**按鈕。

新政策精靈連線到 Integration Server。如果連線失敗，視窗中會出現一條錯誤訊息。如果連線成功，則**連線到 Integration Server**視窗將會關閉，並且新政策精靈視窗的**連線到 Integration Server**欄位將顯示**已連線**狀態。

c. 如果您選擇手動定義的 SVM 位址清單，請建立此政策管理的 Light Agent 可以連線到的 SVM 清單。若要將 SVM 新增至清單，請按一下 **新增** 按鈕，並在開啟的視窗中指定 SVM 的 IPv4 格式 IP 位址或完整網域名稱 (FQDN)。您可從新行輸入多個 SVM IP 位址或完全限定網域名稱。

> 僅指定對應到單一 IP 位址的完全限定網域名稱 (FQDN)。使用與多個 IP 位址相對應的完全限定網域名稱可能會導致應用程式出現錯誤。

您可以透過點擊**刪除**按鈕來刪除清單中選擇的位址。

繼續精靈的下一步。

7. 決定是否要使用卡巴斯基安全網路。仔細閱讀卡巴斯基安全網路聲明並執行以下操作之一：

- 如果您同意聲明中的所有條款與條件，並想搭配應用程式使用卡巴斯基安全網路，請選擇 **我同意使用卡巴斯基安全網路**。
- 如果您不想使用卡巴斯基安全網路，請選擇 **我不同意使用卡巴斯基安全網路**，並在開啟的視窗中確認您的決定。

拒絕使用卡巴斯基安全網路不會中斷政策建立過程。您可以隨時在政策設定中啟用或停用卡巴斯基安全網路或變更受管理裝置的 KSN 模式。

繼續精靈的下一步。

8. 系統會提示您閱讀設定 Kaspersky Endpoint Security 的建議。檢閱允許應用程式最佳化系統資源使用的設定。

   繼續精靈的下一步。

9. 新政策設定視窗的**一般**索引標籤將會開啟。指定新政策的名稱。

   您也可以配置以下政策設定：

   - 政策狀態：
     - **作用中**。目前套用於裝置的政策。如果選擇了此選項，則下次裝置與管理伺服器同步時，此政策將在裝置上生效。預設情況下已勾選此選項。
     - **非作用中**。如果選擇此選項，政策將不會套用於裝置，而是保留在**政策**資料夾中。您可以稍後啟動未啟動的政策。
     - **漫遊**。如果選擇此選項，則當裝置離開組織網路時，政策將生效。

       在裝置上處於活動狀態的網路代理原則的**網路 → 連線設定檔**部分中，必須啟用**管理伺服器無法使用時啟用漫遊模式**設定。

   - 政策設定繼承：
     - **來自父政策的繼承**如果啟用此切換開關，則政策設定將從上級群組政策繼承。父政策中用帶有“掛鎖”（🔒）圖示的設定不可編輯。切換按鈕預設為開啟狀態。
     - **子政策的強制繼承**如果啟用此切換開關，政策設定將傳播至子政策。在子政策的內容中，“**來自父政策的繼承**“切換按鈕將自動開啟，且無法關閉。子政策的設定將從父政策繼承，但帶有開啟的“掛鎖”（🔓）圖示的設定例外。預設情況下，切換按鈕關閉。

   如需政策設定的一般資訊，請參閱 卡巴斯基安全管理中心說明。

10. 如果您想管理其他政策設定，請前往 **應用程式設定** 索引標籤，並視需要進行變更。

    您也可以稍後變更政策設定。

11. 點擊“**儲存**”按鈕。

如何在管理主控台中建立政策

1. 在管理主控台樹狀圖中的**受管理裝置**資料夾中，選擇包含應套用政策的裝置的管理群組。

   您可以在具有該管理群組名稱的資料夾的**裝置**索引標籤上檢視屬於該管理群組的裝置清單。

2. 在工作區選擇“**政策**”標籤。

3. 點擊**新政策**按鈕來啟動新政策精靈。

   您也可以透過點擊政策清單中內容功能表中的**建立→政策**項目來啟動精靈。

4. 在精靈的第一步中，在清單中選擇 Kaspersky Endpoint Security。

   繼續精靈的下一步。

5. 輸入新政策的名稱。

6. 若要在已建立的政策中使用先前版本的 Kaspersky Endpoint Security 政策的設定，請選取**使用早期應用程式版本的政策設定**核取方塊。

   繼續精靈的下一步。

7. 決定是否要使用卡巴斯基安全網路。仔細閱讀卡巴斯基安全網路聲明並執行以下操作之一：

   - 如果您同意本聲明的所有條款和條件，並希望應用程式使用卡巴斯基安全網路，請選擇**我確認我已完整閱讀、理解並接受卡巴斯基安全網路聲明的條款和條件**。

   - 如果您不想使用卡巴斯基安全網絡，請選擇 **我不接受卡巴斯基安全網路聲明的條款和條件**，並在開啟的視窗中確認您的決定。

   拒絕使用卡巴斯基安全網路不會中斷政策建立過程。您可以隨時在政策設定中啟用或停用卡巴斯基安全網路或變更受管理裝置的 KSN 模式。

   繼續精靈的下一步。

8. 指定 Kaspersky Endpoint Security 使用模式：

   - 在**標準模式或 Endpoint Detection and Response Agent 模式**下，該應用程式可作為獨立應用程式或支援 Kaspersky Detection and Response 解決方案和協力廠商病毒防護解決方案協同工作的應用程式，用於防護 Linux 裝置。

   - **用於防護虛擬環境的 Light Agent 模式**— 作為 Kaspersky Security for Virtualization Light Agent 解決方案的一部分，應用程式用於防護執行 Linux 來賓作業系統的虛擬機。

   繼續精靈的下一步。

9. 如果您在 Light Agent 模式下使用應用程式，請配置 SVM 偵測設定：

   a. 選擇 Light Agent 用於發現可連線的 SVM 的方法。

      - **使用 Integration Server**如果選擇此選項，Light Agent 將連線至 Integration Server 以獲取可用於連線的 SVM 清單和其詳情。

      - **使用 SVM 位址自訂清單**如果選擇此選項，您可以指定此政策管理的 Light Agent 可以連線到的 SVM 清單。Light Agent 將僅連線到清單中指定的 SVM。

      如果您選取 **使用 SVM 位址自訂清單** 選項，Light Agent 使用延伸 SVM 選擇演算法，且 SVM 已啟用大型基礎架構防護模式，則只有在忽略 SVM 路徑時，才能將 Light Agent 連線到此 SVM。在 **SVM 選擇演算法** 區段中，您需要將 **SVM 路徑** 設定設為 **略過**。如果設定了任何其他值，Light Agent 將無法連線到 SVM。如需更多詳細資訊，請參閱 Kaspersky Security for Virtualization Light Agent 說明。

   b. 如果選擇 Integration Server，精靈將顯示將 Light Agent 連線到 Integration Server 的目前設定：用於連線的位址和連接埠。如有必要，指定新的連線設定：

      a. 點擊**編輯**按鈕並在開啟的視窗中指定新的連線設定：

         - **位址**。安裝 Integration Server 的裝置的 IP 位址（IPv4 格式）或完全限定網域名稱 (FQDN)。如果將位址指定為 NetBIOS 名稱、localhost 或 127.0.0.1，與 Integration Server 的連線將完成並顯示錯誤。

         - **連接埠**。連線 Integration Server 的連接埠。預設情況下，指定連接埠為 7271。

如果您的基礎架構中部署了基於 Linux 的高可用性 Integration Server 叢集，則需要將負載均衡器的位址和連接埠指定為用於連線到 Integration Server 的位址和連接埠。如需更多詳細資訊，請參閱 Kaspersky Security for Virtualization Light Agent 說明。

b. 點擊**OK**。

c. 如果託管卡巴斯基安全管理中心管理主控台的主機不屬於網域，或者您的帳戶不屬於 KLAdmins 本機或網域群組或本機管理員群組，則 Integration Server 管理員帳號將用於在 Integration Server 上進行身分驗證。

在開啟的視窗中，輸入 Integration Server 管理員的密碼（`admin`帳號的密碼），點擊**OK**按鈕。

d. MMC 外掛程式檢查從 Integration Server 收到的 SSL 憑證。如果憑證包含錯誤或不受信任，將會開啟**驗證 Integration Server 憑證**視窗。您可以點擊視窗中的連結檢視已收到憑證的詳細資訊。

如果您遇到 SSL 憑證問題，我們建議您確保使用的資料傳輸通道是安全的。

若要繼續連線到 Integration Server，請點擊**略過**按鈕。接收的憑證將在安裝卡巴斯基安全管理中心管理主控台的裝置上，以受信任憑證進行安裝。

c. 如果您選擇手動定義的 SVM 位址清單，請建立此政策管理的 Light Agent 可以連線到的 SVM 清單。若要將 SVM 新增至清單，請按一下 **新增** 按鈕，並在開啟的視窗中指定 SVM 的 IPv4 格式 IP 位址或完整網域名稱 (FQDN)。您可從新行輸入多個 SVM IP 位址或完全限定網域名稱。

僅指定對應到單一 IP 位址的完全限定網域名稱 (FQDN)。使用與多個 IP 位址相對應的完全限定網域名稱可能會導致應用程式出現錯誤。

您可以透過點擊**刪除**按鈕來刪除清單中選擇的位址。

繼續精靈的下一步。

10. 如有必要，配置檔案威脅防護的一般設定。

繼續精靈的下一步。

11. 如有必要，請編輯已預設配置的檔案威脅防護設定。

繼續精靈的下一步。

12. 如有必要，配置檔案威脅防護的排除項目。

繼續精靈的下一步。

13. 如果有必要，修改感染物件的預設操作。

繼續精靈的下一步。

14. 選擇政策狀態：

- **已啟用的政策**。目前套用於裝置的政策。如果選擇了此選項，則下次裝置與管理伺服器同步時，此政策將在裝置上生效。預設情況下已勾選此選項。
- **非活動政策**。如果選擇此選項，政策將不會套用於裝置，而是保留在**政策**資料夾中。您可以稍後啟動未啟動的政策。

- **漫遊政策**。如果選擇此選項，則當裝置離開組織網路時，政策將生效。

> 在裝置上處於活動狀態的網路代理原則的**網路 → 連線設定檔**部分中，必須啟用**管理伺服器無法使用時啟用漫遊模式**設定。

15. 完成新政策精靈。

建立的政策顯示在**政策**索引標籤上的管理群組的政策清單中以及主控台樹的**政策**資料夾中。

如需管理政策的一般資訊，請參閱 卡巴斯基安全管理中心說明。

實用文章

如果工作未執行或政策未套用，該怎麼辦

如果裝置具有以下狀態，該怎麼辦：「政策設定無效。政策尚未套用。」

錯誤：「目前版本的卡巴斯基安全管理中心網頁主控台不支援應用程式，或未安裝應用程式 Web 外掛程式」

匯出和匯入政策設定

Kaspersky Endpoint Security 允許將政策及其設定和設定檔匯出到 KLP 檔案。然後，您可以使用政策匯出/匯入功能來備份政策、將政策移轉到另一台伺服器，或（例如）將政策從卡巴斯基安全管理中心 Windows 移轉到卡巴斯基安全管理中心 Linux。有關政策管理的詳細資訊，請參閱卡巴斯基安全管理中心說明。

如何在管理主控台 (MMC) 中匯出和匯入政策

1. 開啟卡巴斯基安全管理中心的管理主控台。
2. 在管理主控台樹狀目錄的“**受管理裝置**”資料夾中，開啟相關用戶端電腦所屬的管理群組名稱的資料夾。
3. 在工作區選取“**政策**”標籤。
4. 若要導出政策：
   a. 點擊要匯出的政策。
   b. 點選視窗右上部的“**匯出政策到檔案**”連接。
   c. 在開啟的視窗中，指定您要將政策匯出到的 KLP 檔案的名稱，然後選取要儲存此檔案的資料夾。
   d. 儲存檔案。
5. 若要導入政策：
   a. 點擊“**從檔案匯入政策**”。
   b. 在開啟的視窗中，選取要匯入的 KLP 政策。
   c. 開啟檔案。

這會新增一項政策，狀態為*停用政策*。

如何在網頁主控台中匯出和匯入政策

1. 在網頁主控台的主視窗中，選擇**資產管理 → 政策**。
2. 若要導出政策：
   a. 選中要匯出的政策旁邊的核取方塊。
   b. 點擊"**匯出**"按鈕。
   c. 在開啟的視窗中，指定您要將政策匯出到的 KLP 檔案的名稱，然後選取要儲存此檔案的資料夾。
   d. 儲存檔案。
3. 若要導入政策：
   a. 點擊"**匯入**"。
   b. 選擇要匯入的 KLP 政策檔案。
   c. 政策成功處理後，選擇要套用該政策的管理群組。
   d. 按一下**完成**按鈕以結束匯入政策。

   這會新增一項政策，狀態為*非作用中*。

在網頁主控台中匯出和匯入特定政策設定

在網頁主控台中，您可以將個別政策設定匯出到 JSON 檔案，並從檔案匯入這類設定。例如，您可以匯出 Web 控制規則清單或檔案威脅防護範圍清單。

以下設定可用於匯出和匯入：

- 檔案威脅防護範圍
- 郵件威脅防護的附件篩選器
- 網路封包規則
- Web 控制規則
- 應用程式控制規則
- 監控範圍和系統完整性監控排除範圍
- 遙測設定
- 受信任區域的特定排除項

若要在網頁主控台中匯出或匯入設定：

1. 在網頁主控台的主視窗中，選擇**資產管理 → 政策**。
2. 點擊 Kaspersky Endpoint Security 政策的名稱。
   政策內容視窗將開啟。
3. 選擇"**應用程式設定**"標籤。
4. 前往您要匯出或匯入設定的區段。
5. 點擊 按鈕。
6. 選擇操作：**匯入** 或 **匯出**。
7. 如果您要匯入設定，請選擇要從中匯入設定的檔案。

在卡巴斯基安全管理中心中建立的 Kaspersky EndpoinSecurity 工作

您可以在卡巴斯基安全管理中心中為 Kaspersky EndpoinSecurity 建立以下類型的工作：

- 在單個裝置上執行的本機工作；
- 在管理群組內的裝置上執行的群組工作；
- 針對裝置選取項的工作，可在多台裝置上執行，無論這些裝置是否包含在管理群組中。

您可以建立任意數量的工作。

有關在卡巴斯基安全管理中心中建立之工作的一般資訊，請參閱 卡巴斯基安全管理中心說明。

工作類型

卡巴斯基安全管理中心中提供了以下用於管理 Kaspersky Endpoint Security 的工作：

- *惡意軟體掃描*。在工作執行期間，應用程式會掃描工作設定中指定的裝置區域以尋找病毒和其他惡意軟體。
- *關鍵區域掃描*。在工作執行期間，應用程式會掃描引導磁區、啟動物件、處理程序記憶體和核心記憶體。
- *容器掃描*。在工作執行期間，應用程式會掃描容器和映像中是否有病毒和其他惡意軟體。
- *清查*。在工作執行期間，應用程式會接收關於裝置上儲存的所有可執行檔的資訊，並管理黃金映像。
- *系統完整性檢查*。在工作執行過程中，應用程式會透過比較被監控物件的目前狀態與先前作為基準建立的原始狀態來確定每個物件的變化。
- *新增金鑰*。在工作執行過程中，應用程式會新增一個金鑰（包括備用金鑰）來啟動應用程式。
- *更新*。在工作執行期間，應用程式根據配置的更新設定更新資料庫。
- *回溯*。在工作執行期間，應用程式會回溯最後的資料庫更新。

在網頁主控台中管理工作

如何在網頁主控台中為裝置群組或裝置選取項建立工作

1. 在網頁主控台主視窗中，選擇**資產（裝置）→工作**。
   工作清單開啟。

2. 點擊“**新增**”按鈕。
   啟動“工作精靈”。

3. 在精靈的第一步，執行下列操作：

   a. 在**應用程式**下拉清單中，選擇應用程式名稱：Kaspersky Endpoint Security。

   b. 在**工作類型**下拉清單中，選擇要建立的工作類型。

   c. 在**工作名稱**欄位中，輸入新工作的名稱。

   d. 在**將指派工作之裝置**部分中，選擇定義工作範圍的方法。工作範圍包括將在上面執行工作的裝置：

   - 如果要在特定管理群組中包含的所有裝置上執行該工作，請選擇**將工作指派給管理群組**選項。
   - 如果要在指定裝置上執行工作，請選擇**手動指定裝置位址，或從清單中匯入位址**選項。
   - 如果要根據預定義的標準在裝置選擇中包含的裝置上執行工作，請選擇**將工作指派給裝置分類**選項。有關如何建立裝置分類的資訊，請參閱卡巴斯基安全管理中心說明系統。

   繼續精靈的下一步。

4. 根據所選的定義工作範圍的方法，執行下列一項操作：

   - 在管理群組樹狀目錄中，選擇所需管理群組旁邊的核取方塊。
   - 在裝置清單中，選取所需裝置旁的核取方塊。如果未列出所需的裝置，您可以透過以下方式新增：
     - 使用**新增裝置**按鈕。您可以按名稱或 IP 位址新增裝置，從指定的 IP 範圍新增裝置，或從管理伺服器輪詢企業 LAN 時偵測到的裝置清單中選擇裝置。
     - 使用**從檔案匯入裝置**按鈕。對於匯入，使用包含裝置位址清單的 TXT 檔案，其中每個位址必須位於單獨的行上。
   - 從清單中，選擇包含所需裝置的選項名稱。

   繼續精靈的下一步。

5. 若要在建立工作後立即管理工作設定，請在精靈的最後一個步驟中選取 **建立完成後開啟工作詳細資料** 核取方塊。工作使用預設設定建立。

6. 完成精靈。

   在工作清單中將顯示一個新工作。

如何在網頁主控台中建立本機工作

1. 在網頁主控台主視窗中，選擇**資產（裝置）→受管理裝置**。

   受管理裝置的清單將開啟。

2. 選擇包含必要裝置的管理群組。為此，請按一下受管理裝置清單上方的 **顯示階層** 按鈕，並在開啟的視窗中選取管理群組。

   此清單僅顯示選定管理群組的受管理裝置。

3. 在清單中，找到要為其建立工作之裝置，然後點擊裝置名稱。

4. 這將開啟受管理裝置屬性視窗；在該視窗中，轉到**工作**索引標籤。

   為此裝置建立的工作清單得到顯示。

5. 點擊"**新增**"按鈕。

   啟動"工作精靈"。

6. 在精靈的第一步，執行下列操作：

   a. 在**應用程式**下拉清單中，選擇應用程式名稱：Kaspersky Endpoint Security。

   b. 在**工作類型**下拉清單中，選擇要建立的工作類型。

   c. 在**工作名稱**欄位中，輸入新工作的名稱。

7. 若要在建立工作後立即管理工作設定，請在精靈的最後一個步驟中選取 **建立完成後開啟工作詳細資料** 核取方塊。工作使用預設設定建立。

8. 完成精靈。

在工作清單中將顯示一個新工作。

如何在網頁主控台中啟動、停止、暫停或繼續工作

1. 在卡巴斯基安全管理中心網頁主控台主視窗中，選擇**資產（裝置）→工作**。

   工作清單開啟。

2. 執行下列操作之一：

   - 若要啟動或停止在特定管理群組中所包含之所有裝置上執行的工作，請按一下視窗上方的 **顯示階層** 按鈕，並在顯示的視窗中選取管理群組。

     此清單僅顯示為選定的管理群組所建立的工作。

   - 若要啟動或停止在一或多個裝置上執行的工作（針對裝置集合的工作），請按一下視窗上方的 **顯示階層** 按鈕，並在顯示的視窗中選取具有管理伺服器名稱的頂層節點。

     此清單顯示在管理伺服器上建立的所有工作。

3. 在工作清單中，選取所需工作名稱旁的核取方塊，然後點擊工作清單上方的操作按鈕。

> *更新*工作無法暫停或恢復，只能啟動或停止。

在管理主控台中管理工作

若要在管理主控台中為裝置群組或裝置選取項建立工作

1. 在管理主控台中，執行下列其中一項操作：

   - 若要建立將在所選管理群組中包含的裝置上執行的工作，請在**受管理裝置**資料夾中的主控台樹中選擇此管理群組，然後在工作區中選擇**工作**索引標籤並點擊**新工作**按鈕。

     新工作精靈將為選定管理群組的裝置啟動。

   - 若要建立將在一個或多個裝置上執行的工作（一組裝置的工作），請選擇主控台樹狀圖中的**工作**資料夾，然後點擊工作區中的**新工作**按鈕。

     新工作精靈為該組裝置啟動。

2. 在精靈的第一步中，選擇 Kaspersky Endpoint Security 和工作類型。

   繼續精靈的下一步。

3. 如果您正在為一組裝置建立工作，精靈會提示您定義工作範圍。工作範圍包括將運行該工作之裝置。

   a. 指定定義工作範圍的方法：從管理伺服器偵測到的裝置清單中選取裝置；手動設定裝置位址；從檔案匯入裝置清單，或指定先前設定的裝置選取項（如需詳細資訊，請參閱 卡巴斯基安全管理中心說明 ）。

   b. 根據您指定的定義工作範圍的方法，在開啟的視窗中執行下列操作之一：

      - 在偵測到的裝置清單中，指定將在其上執行工作的裝置。為此，請選取裝置名稱左側清單中的核取方塊。

      - 點擊**新增**或**新增 IP 範圍**按鈕並手動輸入裝置位址。

      - 點擊**匯入**按鈕，然後在開啟的視窗中選擇包含裝置位址清單的 TXT 檔案。

      - 點擊**瀏覽**按鈕，在開啟的視窗中指定包含將在其上執行工作的裝置分類的名稱。

   繼續精靈的下一步。

4. 依照精靈中的說明配置可用的工作設定。

5. 輸入新工作的名稱並繼續精靈的下一步。

6. 若要在精靈結束後立即啟動工作，請在最後一步中選取**精靈結束後執行工作**核取方塊。

7. 完成精靈。

   在工作清單中將顯示一個新工作。

如何在管理主控台中建立本機工作

1. 在管理主控台樹狀圖中的**管理裝置**資料夾中，選擇包含必要裝置的管理群組。

2. 在工作區選取“**裝置**”標籤。

3. 在受管理裝置清單中，選擇所需的裝置並雙擊它以開啟**屬性：<工作名稱>**視窗。

4. 在顯示的受管理裝置屬性視窗中，選擇**工作**部分。

   為此裝置建立的工作清單得到顯示。

5. 點擊“**新增**”按鈕。

   啟動“工作精靈”。

6. 在精靈的第一步中，選擇 Kaspersky Endpoint Security 和工作類型。

   繼續精靈的下一步。

7. 輸入新工作的名稱並按照精靈的說明配置可用的工作設定。

8. 完成精靈。

   在工作清單中將顯示一個新工作。

如何在管理主控台中啟動、停止、暫停或繼續工作

1. 在管理主控台中，執行下列其中一項操作：

   - 若要啟動或停止在指定管理群組中包含的裝置上執行的工作，請在主控台樹狀圖中選擇此管理群組，然後在工作區中選擇**工作**索引標籤。

     為選定管理群組建立的工作清單將開啟。

   - 若要啟動或停止在一台或多台裝置上執行的工作（一組裝置的工作），請選擇主控台樹中的**工作**資料夾。

     管理伺服器上建立的所有工作的清單將開啟。

2. 在工作清單中，選擇所需的工作，開啟該工作的內容功能表，然後選擇要執行的操作。

> *更新*工作無法暫停或恢復，只能啟動或停止。

在工作清單中，您可以監控工作執行結果：檢視工作狀態以及工作在裝置上的效能統計資訊。您也可以建立事件分類來監控工作的執行情況。有關事件選取的詳細資訊，請參閱 卡巴斯基安全管理中心說明。

工作執行結果也會保存在裝置本機和卡巴斯基安全管理中心報告中。

管理和執行工作時的特殊考量

- 針對裝置集合的工作僅在工作中指定的裝置上執行。如果將新裝置新增至已建立工作的裝置集合，該工作將不會在這些裝置上執行。在此情況下，您需要建立新工作或編輯現有工作。

- 工作僅當裝置上執行 Kaspersky Endpoint Security 時才會執行。

- 如果裝置受政策管理，則可能無法使用命令列或應用程式的圖形介面檢視和管理在卡巴斯基安全管理中心中建立的工作。

- 在卡巴斯基安全管理中心中，您可以為 Kaspersky Endpoint Security 應用程式建立所有類型的工作。是否在受保護裝置上套用和執行工作，取決於該裝置上的 應用程式模式。例如，如果應用程式以 Light Agent 模式執行，則 *新增金鑰*、*更新* 和 *回溯* 工作不會套用到裝置上。

登入和登出網頁主控台和雲端主控台

卡巴斯基安全管理中心網頁主控台

若要登入網頁主控台，您需要知道在網頁主控台安裝期間指定的管理伺服器的網址和連接埠號（預設使用連接埠 8080）。您的瀏覽器中也必須啟用 JavaScript。

您可以使用下列其中一種方法登入卡巴斯基安全管理中心網頁主控台：

- 網域身分驗證（單一登入）
- 網域使用者的使用者名稱和密碼
- 內部使用者的使用者名稱和密碼

有關登入和登出卡巴斯基安全管理中心網頁主控台的詳細資訊，請參閱卡巴斯基安全管理中心說明。

若要透過指定使用者名稱和密碼登入網頁主控台：

1. 在瀏覽器中，前往：

   ```
   https://<Kaspersky Security Center Web Console address>:<port number>
   ```

   這會開啟選取管理伺服器的頁面。

2. 如果您已新增多個受信任的管理伺服器，請從清單中選取您要連線的管理伺服器。
   如果您只新增了一台管理伺服器，則不會顯示管理伺服器清單。
   瀏覽器會重新導向至 `https://<Administration Server address>:4444`。

3. 輸入您帳戶的使用者名稱和密碼。

   > 建議確保密碼複雜度和反暴力破解機制，確保密碼在 6 個月內無法被猜到。

4. 點擊**登入**。
   如果管理伺服器沒有回應，或者您輸入的憑證不正確，則會顯示錯誤訊息。

5. 輸入您行動裝置上的身分驗證應用程式產生的一次性安全代碼。
   如果是首次登入，請為您的帳戶設定兩步驟身分驗證。

登入後，將顯示包含最後使用的語言和主題的儀表板。

有關網頁主控台介面的詳細資訊，請參閱卡巴斯基安全管理中心說明。

若要登出網頁主控台：

在螢幕左下角選擇**<帳戶名稱>** → **結束**。

網頁主控台關閉，登入頁面顯示。

卡巴斯基安全管理中心雲端主控台

對於卡巴斯基安全管理中心雲端主控台，使用網路權杖登入雲端主控台入口網站上的帳戶。

有關卡巴斯基安全管理中心雲端主控台的詳細資訊，請參閱卡巴斯基安全管理中心雲端主控台說明文件。

使用指令列管理應用程式

透過指令列，您可以在裝置上安裝、解除安裝、啟動和停止 Kaspersky Endpoint Security，也可以在本機管理應用程式。

元件和工作

應用程式的功能元件受在作業系統中執行的*Kaspersky Endpoint Security 本機工作*支援。若要啟用或停用裝置上的應用程式功能元件，您需要在指令列上啟動或停止對應的 Kaspersky Endpoint Security 工作。

若要對裝置進行一次掃描，您也需要啟動對應的 Kaspersky Endpoint Security 工作。

若要管理裝置上功能元件的設定或裝置掃描設定，您需要管理對應的 Kaspersky Endpoint Security 工作設定。

一般設定

除了個別 Kaspersky Endpoint Security 工作特有的設定外，還有一些一般設定：

- 一般容器掃描設定。用於即時掃描容器和命名空間（容器監控）。
- 網路流量掃描設定。由 Web 威脅防護、網路威脅防護、郵件威脅防護 和 Web 控制 元件使用。
- 一般應用程式設定。這些設定控管應用程式整體的運作以及個別功能的運作。

管理命令

您可以使用 *kesl-control 公用程式*，在指令列上管理 Kaspersky Endpoint Security 工作和設定。

只能建立或刪除使用者工作。預定義工作無法建立或刪除。

視應用程式的模式而定，您可以建立下列類型的使用者工作：

- 標準模式：*ODS*、*更新*、*回溯*、*ODFIM*、*ContainerScan*和*InventoryScan*；
- Light Agent 模式：*ODS*、*ODFIM*、*容器掃描*和 *清查掃描*。

您可以啟動和停止所有預定義工作和使用者工作，但 *產品授權* 類型的工作除外。

您可以暫停和恢復 *ODS*、*ODFIM* 和 *清查掃描* 工作。

Kaspersky Endpoint Security 本機工作

下表列出可用於在指令列上管理 Kaspersky Endpoint Security 的工作：

每個應用程式工作都有一個在指令列上使用的名稱、ID 和類型。

所有工作（包括已刪除的工作）的 ID 都是唯一的。應用程式不會重複使用已刪除工作的識別碼。新工作的識別碼是最新建立的工作的識別碼的下一個連續數字。

工作名稱不區分大小寫。

在應用程式安裝期間會建立*預定義工作*。這些工作無法被刪除。每個預定義工作都有一個名稱和 ID。

使用應用程式時所建立的工作稱為*使用者工作*。建立工作時，請指定其名稱。使用者工作 的 ID 由應用程式在建立工作時定義和指派。使用者工作 的 ID 從 100 開始。

在運行過程中，應用程式會建立*臨時掃描工作*。臨時工作名稱和 ID 由應用程式指派。臨時工作完成後會被自動刪除。

應用程式工作

工作	工作說明	指令列中的工作名稱	工作 ID	工作類型
檔案威脅防護	此工作可讓您即時啟用或停用檔案威脅防護並定義檔案威脅防護防護元件的設定。如果啟用檔案威脅防護，則工作會在應用程式啟動時自動執行	File_Threat_Protection	1	OAS
惡意軟體掃描	此工作可讓您根據需要掃描檔案系統物件中的惡意軟體並定義掃描的設定。您可以使用此工作執行完整或自訂掃描裝置。	Scan_My_Computer	2	ODS
惡意軟體掃描（使用者工作）		user-defined	從 100 開始	ODS
自訂掃描檔案	此工作用於設定及儲存使用 `kesl-control --scan-file` 指令掃描指定檔案和目錄時所使用的設定。指令執行的結果是，應用程式會建立並啟動臨時檔案掃描工作。	Scan_File	3	ODS
關鍵區域掃描	此工作可讓您根據需要執行作業系統的關鍵區域掃描並定義掃描的設定。	Critical_Areas_Scan	4	ODS
更新	您可以使用此工作執行排程和按需的應用程式資料庫和模組更新並編輯更新設定。	Update	6	Update
更新（使用者工作）		user-defined	從 100 開始	Update
回溯	您可以使用此工作來回復應用程式資料庫和模組的上次更新。	Rollback	7	Rollback
回溯（使用者工作）		user-defined	從 100 開始	Rollback

工作	工作說明	指令列中的工作名稱	工作 ID	工作類型
產品授權	此工作提供啟動裝置上安裝的應用程式的功能。此工作在應用程式啟動時自動啟動，駐留在裝置操作記憶體中。工作沒有設定；產品授權金鑰使用特殊的管理指令進行管理。無法啟動、停止或刪除該工作。	License	9	License
系統完整性檢查	此工作可讓您透過將監控物件的目前狀態與先前記錄的狀態進行比較來檢查已包含在監控範圍內的檔案和目錄的變更。	System_Integrity_Monitoring	11	OAFIM
系統完整性檢查（使用者工作）		user-defined	從 100 開始	ODFIM
防火牆管理	此工作可讓您啟用或停用防火牆管理並定義裝置上的網路連線控制設定。	Firewall_Management	12	Firewall
Anti-Cryptor	此工作可讓您啟用或停用對檔案進行遠端惡意加密的防護，並定義加密軟體防護元件的設定。	Anti_Cryptor	13	AntiCryptor
Web 威脅防護	此工作可讓您啟用或停用 Web 威脅防護，並定義 Web 威脅防護 元件的設定。如果啟用 Web 威脅防護，則工作會在應用程式啟動時自動執行	Web_Threat_Protection	14	WTP
裝置控制	此工作可讓您啟用或停用裝置控制並定義裝置控制元件的設定。如果啟用裝置控制，則工作會在應用程式啟動時自動執行。	Device_Control	15	DeviceControl
卸除式磁碟機掃描	此工作可讓您即時監控卸除式媒體與裝置的連線，並定義卸除式磁碟機掃描的設定及其引導磁區中的惡意軟體掃描。	Removable_Drives_Scan	16	RDS
網路威脅防護	此工作可讓您啟用或停用網路威脅防護並定義網路威脅防護防護元件的設定。	Network_Threat_Protection	17	NTP
容器掃描	此工作可讓您根據需要掃描容器和映像並定義掃描的設定。	Container_Scan	18	ContainerScan
容器掃描（使用者工作）		user-defined	從 100 開始	ContainerScan
自訂容器自訂掃描	此工作用於設定及儲存使用 `kesl-control [-T] --scan-container` 指令掃描指定容器和映像時所使用的設定。指令執行的結果是，應用程式會建立並啟動一個臨時的容器掃描工作。	Custom_Container_Scan	19	ContainerScan
行為偵測	此工作可讓您監控作業系統中應用程式的惡意活動。如果啟用行為偵測，則工作會在應用程式啟動時自動執行。	Behavior_Detection	20	BehaviorDetection
應用程式控制	此工作可讓您啟用或停用應用程式控制並定義應用程式控制元件的設定。	Application_Control	21	AppControl
清查	此工作可讓您取得裝置上應用程式所有可執行檔的資訊，並管理應用程式的 Golden Image 類別。	Inventory_Scan	22	InventoryScan
清查（使用者工作）		user-defined	從 100 開始	InventoryScan
Kaspersky Endpoint Detection and Response Expert (on-premises) 整合。	此工作可讓您啟用或停用與 Kaspersky Endpoint Detection and Response Expert (on-premises) 或 Kaspersky Endpoint Detection and Response (KATA) 的整合，並管理整合設定。	KATAEDR	24	KATAEDR
Web 控制	此工作可讓您啟用或停用Web 控制並定義 Web 控制元件的設定。	Web_Control	26	WebControl

工作	工作說明	指令列中的工作名稱	工作 ID	工作類型
Sandbox 整合	此工作可啟用和停用與 Sandbox 的整合並指定整合設定。	Standalone_Sandbox	29	StandaloneSandbox
物件執行防禦 (EDR Expert (on-premises))	此工作可讓您啟用和停用 Endpoint Detection and Response Expert (on-premises) 執行防禦規則的使用，並檢視這些規則的清單。	KATAEDR_Prevention	30	KATAEDRPrevention
Kaspersky Network Detection and Response (KATA) 整合	此工作可讓您啟用或停用與 Kaspersky Network Detection and Response (KATA) 的整合，並指定整合設定。	KATANDR	31	KATANDR
物件執行防禦（EDR Optimum）	此工作可讓您啟用和停用Endpoint Detection and Response Optimum執行防禦規則，也可以檢視這些規則的清單。	EDRO_Prevention	32	Prevention
KUMA 整合	此工作可啟用和停用與卡巴斯基統一監控和分析平台的整合並指定整合設定。	KUMA	33	KUMA
郵件威脅防護	此工作可讓您針對傳入和傳出電子郵件訊息的附件進行掃描，以偵測病毒和其他威脅性應用程式。如果啟用郵件威脅防護，則工作會在應用程式啟動時自動執行	Mail_Monitoring	35	MailMonitoring
BadUSB 攻擊防護	此工作可讓您防止偽裝成鍵盤的受感染 USB 裝置連線到用戶端裝置。	Bad_USB	37	BadUSB
Kaspersky Endpoint Detection and Response Expert (cloud) 整合	此工作可讓您啟用或停用與 Kaspersky Endpoint Detection and Response Expert (cloud) 的整合，並指定整合設定。	EDRExpertCloud	39	EDRExpertCloud

編輯工作設定

您可以編輯所有使用者工作和所有預定義工作的設定，但 *回溯* 和 *產品授權* 類型的工作除外（這些工作沒有設定）。如果應用程式在 Light Agent 模式下使用，則也無法編輯預定義*更新*工作的設定。

對於 *OAS*、*ODS*、*OAFIM*、*ODFIM* 和 *加密軟體防護* 類型的工作，您可以新增或移除掃描範圍和排除範圍。

您可以透過以下方式編輯工作設定：

- 使用設定檔。此方法可同時修改所有工作設定。您可以使用輸出工作設定的指令，取得要編輯的設定檔。
- 使用 <setting name>=<setting value> 格式的命令列選項。此方法可變更個別工作設定。您可以使用輸出工作設定的指令，檢視工作設定的目前值。

對於某些工作，還提供了單獨的管理指令，可讓您編輯工作設定。

如何輸出工作設定的目前值

您可以將工作設定的目前值輸出到主控台或設定檔。然後，您可以編輯此檔案來修改工作設定。

將工作設定的目前值輸出到主控台

```
kesl-control --get-settings <task ID|name>
```

其中：

- `<task ID|name>` 是任務建立時指派的 ID，或是命令列中的任務名稱。

將工作設定的目前值輸出到設定檔

```
kesl-control --get-settings <task ID/name> --file <path to configuration file> [--json]
```

其中：

- `--file <path to configuration file>` 是您要將工作設定輸出至其中的設定檔路徑。如果指定檔案的名稱而不指定其路徑，則檔案會在目前目錄中建立。如果指定路徑中已經存在檔案，則該檔案會被覆寫。如果指定的目錄不存在，則不會建立設定檔。

- `--json` 被指定以 JSON 格式輸出設定。如果沒有指定 `--json` 選項，則設定以 INI 格式輸出。

如何使用設定檔修改工作設定：

1. 使用以下指令將工作設定輸出到設定檔：

   ```
   kesl-control --get-settings --file <path to configuration file> [--json]
   ```

   其中：

   - `--file <path to configuration file>` 是您要從中匯入任務設定之設定檔的完整路徑。

   - 如果要將設定輸出到 JSON 設定檔，請指定 `--json` 選項。如果未指定 `--json` 選項，應用程式會將設定輸出到 INI 檔案。

2. 開啟產生的設定檔，視需要編輯設定，然後儲存變更。

   對於 *OAS*、*ODS*、*OAFIM*、*ODFIM* 和 *AntiCryptor* 類型的工作，您可以新增或刪除掃描範圍和排除範圍。

   如果要新增掃描範圍，請將包含下列設定的 `[ScanScope.item_#]` 區段新增至檔案：

   - `AreaDesc` 是掃描範圍的描述，其中包含關於此範圍的附加資訊。

   - `UseScanArea` 啟用指定範圍的掃描。

   - `Path` 是包含要掃描物件的目錄路徑。您可以指定本機目錄的路徑或啟用掃描用戶端裝置上安裝的遠端目錄。

   - `AreaMask.item_#` 是掃描範圍的限制。您可以為要掃描的檔案的名稱指定一個遮罩。預設情況下，對掃描範圍內的所有物件啟用掃描。您可以指定多個 `AreaMask.item_#` 項目。

   如果要新增排除範圍，請在檔案中新增具有下列設定的 `[ExcludedFromScanScope.item_#]` 部分：

   - `AreaDesc` – 排除範圍的描述，其中包含關於排除範圍的附加資訊。

   - `UseScanArea` 可啟用排除指定的範圍。

   - `Path` 是包含要排除物件的目錄路徑。您可以指定本機目錄的路徑或排除用戶端裝置上安裝的遠端目錄。設定的可能值取決於工作的類型。

- `AreaMask.item_#`是排除範圍的限制。您可以為想要從掃描範圍中排除的檔案的名稱指定一個遮罩。預設情況下，範圍內的所有物件都被排除。

  範例

  ```
  [ExcludedFromScanScope.item_0000]
  AreaDesc=
  UseScanArea=Yes
  Path=/tmp/notchecked
  AreaMask.item_0000=*
  ```

您可以指定多個`[ScanScope.item_#]`和`[ExcludedFromScanScope.item_#]`部分。應用程式按索引的升序處理範圍。

3. 執行以下指令：

```
kesl-control --set-settings <task ID/name> --file <path to configuration file> [--json]
```

其中：

- `<task ID/name>` 是任務建立時指派的 ID，或是命令列中的任務名稱。
- `--file <path to configuration file>` 是您要從中匯入任務設定之設定檔的完整路徑。
- 如果要從 JSON 設定檔匯入設定，請指定`--json`選項。如果未指定`--json`選項，應用程式將嘗試從 INI 檔案匯入。如果匯入失敗，則會顯示錯誤。

檔案中定義的所有工作設定值都將被匯入應用程式。

如果您變更允許清單，或在應用程式控制工作設定中禁止啟動所有應用程式或影響 Kaspersky Endpoint Security 運行的應用程式，請執行帶有`--set-settings`選項的`--accept`指令。

如何使用命令列選項變更個別工作設定

執行命令：

```
kesl-control --set-settings <task ID|name> <setting name >=<setting value> [<setting name >=<setting value>]
```

其中：

- `<task ID|name>` 是任務建立時指派的 ID，或是命令列中的任務名稱。
- `<setting name >=<setting value>` 是一項工作設定的名稱和值。您可以使用顯示工作設定的指令來取得工作設定的目前值。

指定工作設定的值將會被改變。

如果您變更允許清單，或在應用程式控制工作設定中禁止啟動所有應用程式或影響 Kaspersky Endpoint Security 運行的應用程式，請執行帶有`--set-settings`選項的`--accept`指令。

如何使用命令列選項新增或移除掃描範圍

使用命令列選項新增掃描範圍

```
kesl-control --set-settings <task ID|name> --add-path <path>
```

其中：

- `<task ID|name>` 是任務建立時指派的 ID，或是命令列中的任務名稱。
- `<path>` 是包含要掃描物件的目錄路徑。

此指令會將新的 `[ScanScope.item_#]` 區段新增至工作設定。應用程式掃描`Path`設定所指定的目錄中的物件。掃描範圍的其餘設定採用預設值。

如果工作設定中已包含具有`[ScanScope.item_#]`設定的指定值的`Path`部分，則不會新增重複部分。

如果將`UseScanArea`設定被設為`No`，則執行此指令後其值將變為`Yes`，位於此目錄中的物件將被掃描。

將 /home 目錄新增至 ID=100 的工作掃描範圍的範例

```
kesl-control --set-settings 100 ScanScope.item_0000.UseScanArea=Yes ScanScope.item_0000.Path=/home
```

以下掃描範圍設定將會被新增至工作：

```
[ScanScope.item_0001]
AreaDesc=
UseScanArea=Yes
Path=/home
AreaMask.item_0000=*
```

使用命令列選項移除掃描範圍

```
kesl-control --set-settings <task ID|name> --del-path <path>
```

此指令會從工作設定移除包含指定路徑的 `[ScanScope.item_#]` 區段。應用程式將不會掃描指定目錄中的物件。

如何使用命令列選項新增或移除排除範圍

使用命令列選項新增排除範圍

```
kesl-control --set-settings <task ID|name> --add-exclusion <path>
```

其中：

- `<task ID|name>` 是任務建立時指派的 ID，或是命令列中的任務名稱。
- `<path>` 是包含要排除物件的目錄路徑。

此指令會將新的 `[ExcludedFromScanScope.item_#]` 區段新增至工作設定。應用程式會將 `Path` 設定所指定目錄中的物件排除於掃描之外。排除範圍的其餘設定採用預設值。

如果工作設定中已包含具有`[ExcludedFromScanScope.item_#]`設定的指定值的`Path`部分，則不會新增重複部分。

如果將`UseScanArea`設定設為`No`，則執行此指令後其值將變更為`Yes`，且位於此目錄中的物件將被排除在掃描之外。

使用命令列選項移除排除範圍

```
kesl-control --set-settings <task ID|name> --del-exclusion <path>
```

此指令會從工作設定移除包含指定路徑的 `[ExcludedFromScanScope.item_#]` 區段。應用程式不會從掃描中排除指定目錄中的物件。

如何還原預設工作設定

執行命令：

```
kesl-control --set-settings <task ID|name> --set-to-default
```

其中，`<task ID|name>` 是任務建立時指派的 ID，或是命令列中的任務名稱。

應用程式將設定值變更為其預設值。

設定工作排程

根據應用程式的模式，您可以為下列類型的工作設定排程：

- 標準模式：*ODS*、*更新*、*回溯*、*ODFIM*、*ContainerScan*和*InventoryScan*；
- Light Agent 模式：*ODS*、*ODFIM*、*容器掃描*和 *清查掃描*。

您可以透過下列方式編輯工作排程：

- 使用設定檔。此方法可同時修改所有工作排程設定。您可以使用輸出排程設定的命令取得要編輯的設定檔。
- 使用 <setting name>=<setting value> 格式的命令列選項。此方法可修改個別工作排程設定。您可以使用輸出排程設定的命令檢視工作設定的目前值。

如何輸出目前的排程設定

您可以將工作執行排程設定的目前值輸出到主控台或設定檔。然後您可以編輯此檔案以修改設定。

將目前工作排程設定輸出至主控台

```
kesl-control --get-schedule <task ID|name> [--json]
```

其中：

- `<task ID|name>` 是任務建立時指派的 ID，或是命令列中的任務名稱。
- `--json` 被指定以 JSON 格式輸出設定。如果省略 --json 選項，則設定以 INI 格式輸出。

將目前工作排程設定輸出至設定檔

```
kesl-control --get-schedule <task ID|name> --file <path to configuration file> [--json]
```

其中 `--file <path to configuration file>` 是您要將工作排程設定輸出至其中的設定檔路徑。如果指定檔案的名稱而不指定其路徑，則檔案會在目前目錄中建立。如果指定路徑中已經存在檔案，則該檔案會被覆寫。如果指定的目錄不存在，則不會建立設定檔。

將更新工作排程設定輸出至名為 `update_schedule.ini` 的檔案，並將建立的檔案儲存至目前目錄的範例

```
kesl-control --get-schedule 6 --file update_schedule.ini
```

將更新工作排程寫入終端機的範例

```
kesl-control --get-schedule 6
```

如何使用設定檔設定工作排程

```
kesl-control --set-schedule <task ID|name> --file <path to configuration file> [--json]
```

其中：

- `<task ID|name>` 是任務建立時指派的 ID，或是命令列中的任務名稱。
- `--file <path to configuration file>` 是您要從中匯入工作排程設定的設定檔完整路徑。
- 如果要從 JSON 設定檔匯入設定，請指定 `--json` 選項。如果未指定 `--json` 選項，應用程式將嘗試從 INI 檔案匯入。如果匯入失敗，則會顯示錯誤。

將設定檔 `/home/test/on_demand_schedule.ini` 中的排程設定匯入 `ID=2` 的工作範例

```
kesl-control --set-schedule 2 --file /home/test/on_demand_schedule.ini
```

如何使用命令列選項修改工作排程設定：

```
kesl-control --set-schedule <task ID|name> <setting name>=<setting value> [<setting name>=<setting value>]
```

其中：

- `<task ID|name>` 是任務建立時指派的 ID，或是命令列中的任務名稱。
- `<setting name>=<setting value>` 是一項工作排程設定的名稱和值。

設定工作每 `10` 小時執行一次的範例

```
RuleType=Hourly
RunMissedStartRules=No
StartTime=2021/May/30 23:05:00;10
RandomInterval=0
```

設定工作每 `10` 分鐘執行一次的範例

```
RuleType=Minutely
RunMissedStartRules=No
StartTime=23:10:00;10
RandomInterval=0
```

設定工作於每月 `15` 日執行的範例

```
RuleType=Monthly
RunMissedStartRules=No
```

```
StartTime=23:25:00;15
RandomInterval=0
```

設定工作每週二執行的範例

```
RuleType=Weekly
StartTime=18:01:30;Tue
RandomInterval=99
RunMissedStartRules=No
```

設定工作每 11 天執行一次的範例

```
RuleType=Daily
RunMissedStartRules=No
StartTime=23:15:00;11
RandomInterval=0
```

管理一般應用程式設定

一般應用程式設定定義了應用程式整體的運作以及各個功能的操作。使用一般設定，您可以：

- 在應用程式中配置卡巴斯基安全網路的使用和惡意軟體防護資料庫的精簡版。
- 在應用程式中設定代理伺服器的使用。
- 選擇檔案操作攔截模式（掃描期間阻止/不阻止檔案）。
- 配置掛載點掃描的排除項目（全域排除項目）。
- 配置處理程序記憶體掃描的排除項目。
- 啟用或停用即時容器監控。
- 啟用或停用偵測入侵者可以用來破壞裝置或資料的合法應用程式。
- 啟用或停用與 Kaspersky Managed Detection and Response 的整合。
- 配置事件記錄的使用。
- 配置掃描工作（ODS 類型）的 CPU 資源使用限制。
- 限制非特權使用者可以同時啟動的使用者掃描工作的數量。

您可以透過以下方式使用特殊管理指令來管理一般應用程式設定：

- 使用設定檔。此方法可讓您同時變更所有一般設定。您可以使用一般設定輸出指令取得要編輯的設定檔。
- 使用 <setting name>=<setting value> 格式的命令列選項。此方法可讓您變更個別設定。您可以使用一般設定輸出指令取得設定的目前值。

如何輸出一般應用程式設定的目前值

您可以將一般應用程式設定的目前值輸出到主控台或設定檔。然後，您可以使用此檔案來編輯設定。

將應用程式一般設定的目前值輸出到主控台

```
kesl-control --get-app-settings [--json]
```

其中，指定 `--json` 以 JSON 格式輸出設定。如果沒有指定 `--json` 選項，則設定以 INI 格式輸出。

將應用程式一般設定的目前值輸出到設定檔

```
kesl-control --get-app-settings --file <path to configuration file> [--json]
```

其中 `--file <path to configuration file>` 是您要將應用程式一般設定輸出至其中的設定檔路徑。如果指定檔案的名稱而不指定其路徑，則檔案會在目前目錄中建立。如果指定路徑中已經存在檔案，則該檔案會被覆寫。如果指定的目錄不存在，則不會建立設定檔。

將一般應用程式設定寫入目前目錄中的 `kesl_config.ini` 檔案的範例

```
kesl-control --get-app-settings --file kesl_config.ini
```

如何使用設定檔編輯工作設定：

1. 使用 `kesl-control --get-app-settings` 指令將一般應用程式設定輸出到設定檔。
2. 開啟產生的設定檔，視需要編輯設定，然後儲存變更。
3. 執行以下指令：

   ```
   kesl-control --set-app-settings --file <path to configuration file> [--json]
   ```

   其中：

   - `--file <path to configuration file>` 是包含一般應用程式設定的設定檔完整路徑。如果刪除設定檔中的任意參數，則命令執行後將顯示該參數的預設值。
   - 如果要從 JSON 設定檔匯入設定，請指定 `--json` 選項。如果未指定 `--json` 選項，應用程式將嘗試從 INI 檔案匯入。如果匯入失敗，則會顯示錯誤。

   檔案中定義的所有一般設定的值將被匯入到應用程式中。

   從 `/home/test/kesl_config.ini` 設定檔將一般設定匯入應用程式的範例

   ```
   kesl-control --set-app-settings --file /home/test/kesl_config.ini
   ```

如何使用命令列選項變更一般設定

使用命令列選項變更一般設定

```
kesl-control --set-app-settings <setting name>=<setting value> [<setting name >=<setting value>]
```

其中 `<setting name>=<setting value>` 是一般應用程式設定的名稱和值。

指定的一般設定的值將被改變。

設定偵錯檔案詳細程度為低的範例

```
kesl-control --set-app-settings TraceLevel=NotDetailed
```

新增掛載點排除以使其不受檔案操作攔截的範例

```
kesl-control --set-app-settings ExcludedMountPoint.item_0000="/data"
```

使用篩選器來限制查詢結果

篩選器可讓您在執行應用程式管理指令時限制查詢結果。篩選條件使用一個或多個*邏輯表達式*指定，這些表達式使用邏輯運算子 and 進行組合。篩選條件必須用引號括起來：

您可以將篩選器用於下列目的：

顯示關於某些應用程式目前事件的資訊

```
kesl-control -W --query "<field> <comparison operator> '<value>'[ and <field> <comparison operator> '<value>']"
```

顯示事件記錄中關於某些應用程式事件的資訊

```
kesl-control -E --query "<field> <comparison operator> '<value>'[ and <field> <comparison operator> '<value>']"
```

顯示備份中某些物件的資訊

```
kesl-control -B --query "<field> <comparison operator> '<value>'[ and <field> <comparison operator> '<value>']"
```

從備份中刪除某些物件

```
kesl-control -B --mass-remove --query "<field> <comparison operator> '<value>'[ and <field> <comparison operator>
'<value>']"
```

其中：

- `<field>` 是資料庫欄位的名稱。
- `<comparison operator>` 是下列比較運算之一：
  - `>` 表示“大於”
  - `<` 表示「小於」
  - `like` 符合指定值。指定值時，您可以使用 % 遮罩：例如，邏輯運算式 `"FileName like '%etc%'"` 會設定「FileName 欄位中包含文字「etc」」限制

    > `like` 比較操作僅適用於資料庫中以文字形式儲存的欄位。`like` 操作不適用於包含日期、時間、數字或其他非文字資料類型的欄位。

  - `==` 表示“等於”

- != 表示“不等於”
- >= 表示“大於或等於”
- <= 表示「小於或等於」

- `<value>` 是欄位的值。值必須用單引號 (') 括起來。

  您可以指定日期值作為 UNIX™ 時間（自 1970 年 1 月 1 日 00:00:00 (UTC) 以來經過的秒數）或 YYYY-MM-DD hh:mm:ss 格式的日期值。使用者以使用者本機時區指定日期和時間，應用程式以同一時區顯示它們。

`FileName` 欄位中包含文字「`etc`」的事件資訊輸出範例

```
kesl-control -E --query "FileName like '%etc%'"
```

`ThreatDetected` 類型事件資訊輸出範例

```
kesl-control -E --query "EventType == 'ThreatDetected'"
```

由 `ODS` 類型的工作建立的 `ThreatDetected` 類型事件資訊輸出範例

```
kesl-control -E --query "EventType == 'ThreatDetected' and TaskType == 'ODS'"
```

`UNIX` 時間戳記系統（自 `1970` 年 `1` 月 `1` 日 `00:00:00 (UTC)` 以來經過的秒數）中指定日期之後產生的事件資訊輸出範例

```
kesl-control -E --query "Date > '1583425000'"
```

以 `YYYY-MM-DD hh:mm:ss` 格式指定的日期之後產生的事件資訊輸出範例

```
kesl-control -E --query "Date > '2022-12-22 18:52:45'"
```

備份儲存中具有高嚴重等級的檔案資訊輸出範例

```
kesl-control -B --query "DangerLevel == 'High'"
```

匯出和匯入應用程式設定

Kaspersky Endpoint Security 可讓您匯出和匯入所有應用程式設定，以便進行故障排除、驗證設定或簡化其他使用者裝置上的應用程式配置。

> 僅允許受信任的使用者存取設定檔。在將設定匯入應用程式之前，請先驗證目錄、設定檔、執行檔和隔離區的路徑。請勿從不受信任的來源匯入設定檔。設定檔遭到破壞可能會影響組織基礎架構及使用者資料的安全性、完整性或功能。

匯出設定

匯出設定時，所有應用程式設定（包括一般容器掃描設定、網路流量掃描設定、一般應用程式設定和工作設定）都儲存在一個設定檔中。之後，您可以使用此設定檔將設定匯入到應用程式中。

匯出應用程式設定

```
kesl-control --export-settings --file <configuration file path> [--json]
```

其中：

- `--file <configuration file path>` 是您要用來儲存應用程式設定之設定檔的完整路徑。
- 指定 `--json` 可將設定以 JSON 格式匯出至設定檔。如果未指定 `--json` 選項，則設定將被匯出到 INI 檔案。

匯入設定

1. 執行以下指令：

   ```
   kesl-control --import-settings --file <configuration file path> [--json]
   ```

   其中：

   - `--file <configuration file path>` 是您要從中匯入應用程式設定之設定檔的完整路徑。
   - 指定 `--json` 可從 JSON 格式的設定檔匯入設定。如果未指定 `--json` 選項，應用程式將嘗試從 INI 檔案匯入。如果匯入失敗，則會顯示錯誤。

2. 重啟應用程式。

匯出和匯入設定的特殊考量和限制

- 匯入或匯出設定時必須啟動應用程式。
- 如果 Kaspersky Endpoint Security 以 Light Agent 模式使用，則無法匯出或匯入 `Update` 類型的預定義工作設定。
- 如果政策禁止變更設定，則無法匯入設定。
- 如果您將從舊版應用程式匯出的設定匯入至新版應用程式，則舊版中不存在的設定會設為預設值。
- 您無法將設定從較新版本匯入至較舊版本。

- 部分政策和工作設定無法從應用程式 Web 外掛程式 12.3 和 12.4 版匯入至應用程式 12.5 版。此限制適用於下列政策和工作設定：
  - 檔案威脅防護和加密軟體防護的防護範圍和排除範圍
  - 行為分析掃描的程序排除項目
  - 裝置控制的受信任裝置
  - 系統完整性監控的掃描範圍和排除範圍
  - Web 控制規則
  - 代理伺服器設定
  - 程序記憶體掃描的排除項目
  - 全域排除（從掃描中排除掛載點）
  - *ODS*、*容器掃描*、*清查掃描*、*ODFIM* 工作的掃描範圍。
- 匯入設定後，以下項目會關閉：卡巴斯基安全網路 (`UseKSN=No`)、雲端模式 (`CloudMode=No`) 和 MDR 整合 (`UseMDR=No`)。如果您要使用此功能，請調整相關設定。
- 匯入應用程式設定後，內部工作 ID可能會變更。建議使用工作名稱來管理工作。
- 與 Kaspersky Endpoint Detection and Response Expert (cloud) 整合時，會匯出所有設定，包括從 Kaspersky Endpoint Detection and Response Expert (cloud) 接收的設定：
  - 遙測伺服器的位址和連接埠
  - 回應伺服器的位址和連接埠
  - 回應伺服器的連線逾時
  - 回應伺服器的回應逾時
  - 遙測伺服器的連線逾時
  - 遙測伺服器的回應逾時
  - 遙測伺服器的用戶端憑證
  - 遙測伺服器的伺服器憑證
  - 回應伺服器的用戶端憑證
  - 回應伺服器的伺服器憑證

  匯入時，上述設定不會匯入至裝置。

透過圖形介面管理應用程式

透過圖形介面管理應用程式需要 管理員 (admin) 角色的權限。

如果 Kaspersky Endpoint Security 是在 Light Agent 模式下使用，則不支援圖形介面。

在應用程式的 **標準模式**中，您可以使用圖形介面執行以下操作：

- 檢視裝置防護狀態的資訊。
- 配置應用程式元件。
  選取目錄
  - 檔案威脅防護。
  - 防火牆管理。
  - 加密軟體防護。
  - 卸除式磁碟機掃描。
  - Web 威脅防護。
  - 郵件威脅防護。
  - 裝置控制。
  - 網路威脅防護。
  - BadUSB 攻擊防護。
  - 行為偵測。
  - 弱點利用防禦。
  - 應用程式控制。
  - Web 控制。
  - 系統完整性監控。
- 掃描檔案和目錄，包括將檔案傳送至沙盒進行掃描。
- 啟動更新並復原資料庫更新。
- 為應用程式啟用或停用卡巴斯基安全網路。
- 向組織區域網路的管理員要求並取得對被封鎖裝置的暫時存取權限。

- 管理應用程式產品授權金鑰，並檢視目前使用的產品授權和金鑰資訊。
- 檢視關於放置在備份中的物件的資訊。
- 檢視應用程式報告。
- 建立應用程式偵錯檔案。

通知區域中的應用程式圖示

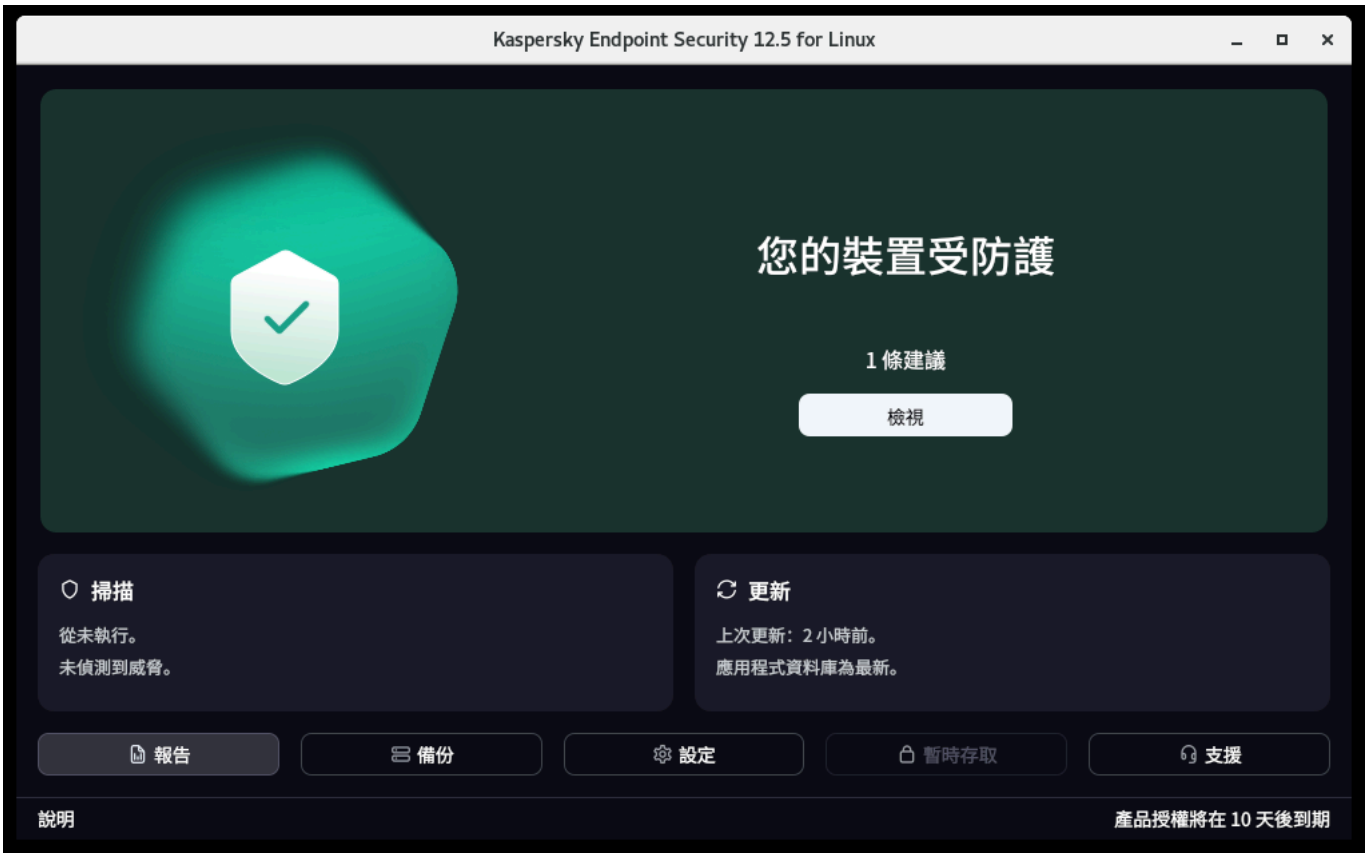
點擊托盤中的 Kaspersky Endpoint Security 圖示可以存取右鍵功能表和應用程式圖形介面的主視窗。

> 在某些作業系統中，安裝應用程式圖形介面套件後可能會遺失預設的應用程式圖示。

應用程式圖示的內容功能表包含下列項目：

- **Kaspersky Endpoint Security 12.5 for Linux**。開啟應用程式圖形介面的主視窗。
- **結束**。結束圖形介面。

應用程式圖形介面的主視窗



應用程式主視窗

防護狀態	裝置防護狀態的資訊。顯示在主視窗的上半部。 您可以點擊 **檢視** 按鈕以開啟 **防護中心** 視窗。此視窗會顯示針對修復防護問題（如有）所需執行操作的建議。
掃描	惡意軟體掃描工作狀態和偵測到的威脅數量的資訊。 您可以點擊此區段以開啟 **掃描** 視窗。在此視窗中，您可以啟動和停止 *惡意軟體掃描*、*關鍵區域掃描* 和 *容器掃描* 工作，並檢視這些工作的報告。
更新	資料庫更新工作狀態的資訊。 您可以點擊此區段以開啟 **更新** 視窗。在此視窗中，您可以啟動 *更新* 和 *回溯* 工作，並檢視這些工作的報告。
報告	檢視元件和工作的報告與統計資料。
備份	檢視 備份 中的物件詳細資訊。 如果按鈕處於非使用中狀態，該怎麼辦
設定	啟用或停用應用程式元件，配置 卡巴斯基安全網路。 如果按鈕處於非使用中狀態，該怎麼辦
暫時存取權限	請求並取得對被封鎖裝置的暫時存取權限。
支援	有關應用程式的資訊：Kaspersky Endpoint Security 的當前版本，資料庫發布日期，金鑰以及其他資訊。 您也可以造訪卡巴斯基資源以取得實用資訊，或聯絡技術支援。
產品授權期限	剩餘產品授權期限 您可以點擊此區域以開啟 **產品授權** 視窗。在此視窗中，您可以檢視產品授權的詳細資訊，或造訪卡巴斯基網站購買新的產品授權。

防護狀態監控

卡巴斯基安全管理中心用戶端裝置的防護狀態

您可以使用用戶端裝置的狀態，在卡巴斯基安全管理中心中取得裝置防護狀態的相關資訊。對於卡巴斯基安全管理中心，用戶端裝置是指已安裝卡巴斯基安全管理中心網路代理的裝置。

用戶端裝置的狀態可根據卡巴斯基安全管理中心中配置的規則變更為*嚴重*或*警告*。例如，如果裝置上未安裝防護應用程式、長時間未執行病毒掃描、應用程式資料庫已過期、產品授權已過期，或卡巴斯基安全管理中心已從受管理應用程式接收裝置狀態，狀態可能會變更。

有關狀態變更原因以及配置分配狀態條件的更多詳細資訊，請參閱卡巴斯基安全管理中心說明。

如何在網頁主控台中檢查裝置的防護狀態

1. 在網頁主控台的主視窗中，選取 **資產管理 → 資產 (裝置)**。

   受管理裝置的清單將開啟。

2. 選擇包含必要裝置的管理群組。若要選取巢狀群組，請按一下視窗上方的 **顯示階層結構** 按鈕。

   此清單僅顯示選定管理群組的受管理裝置。

3. 按一下裝置名稱。

4. 這會開啟受管理裝置的屬性視窗；在該視窗的 **一般** 索引標籤上，選取 **防護** 區段。

防護部分顯示關於裝置的以下資訊：

- **在網路中可見**是所選裝置在網路中的可見性：*Yes*或*No*。
- **裝置狀態**是根據管理員為選定裝置設定的防護狀態標準以及網路中的裝置活動所產生的用戶端裝置的狀態：*OK*、*緊急*或*警告*。
- **狀態描述**表示將裝置狀態變更為*緊急*或*警告*的原因。
- **防護狀態**表示所選裝置上檔案威脅防護的目前狀態，例如*正在執行*、*已停止*或*已暫停*。
- **上次完整檢查**表示在選定裝置上完成上次完整掃描工作的日期和時間。
- **偵測到病毒**表示自安裝 Kaspersky Endpoint Security 以來，在所選裝置上偵測到的惡意物件總數（偵測到的威脅計數器）。
- **解毒失敗的物件**表示 Kaspersky Endpoint Security 無法解毒的受感染物件的數量。

如何在管理主控台中檢查裝置的防護狀態

1. 在管理主控台樹狀圖中的**管理裝置**資料夾中，選擇包含必要裝置的管理群組。
2. 在工作區選取"**裝置**"標籤。
3. 在受管理裝置清單中，選擇所需的裝置並雙擊它以開啟**屬性：<工作名稱>**視窗。
4. 在開啟的受管理裝置屬性視窗中，選擇**防護**部分。

防護部分顯示關於裝置的以下資訊：

- **裝置狀態**：根據管理員為所選裝置的防護狀態和網路中的裝置活動所設定的標準所產生的用戶端裝置狀態。
- **所有問題**：所選裝置上安裝的受管理應用程式偵測到的問題的完整清單。每個問題都有一個應用程式提示分配給裝置的狀態。
- **即時防護狀態**：選定裝置上檔案威脅防護的目前狀態，例如*正在執行*或*已停止*。當防護狀態變更時，僅當裝置與管理伺服器同步後，新的狀態才會顯示在裝置屬性視窗中。
- **上次按需掃描**：上次在選定裝置上執行惡意軟體掃描的日期和時間。
- **偵測到的威脅總數**：自安裝應用程式（第一次掃描）或自上次重設威脅計數器以來，在選定裝置上偵測到的威脅總數。

  若要重設計數器，請點擊**重設**按鈕。
- **活動威脅**：選定裝置上未處理的檔案數量。

有關用戶端裝置狀態的詳細資訊，請參閱卡巴斯基安全管理中心說明。

裝置上應用程式運作的一般資訊

如何在網頁主控台中檢視應用程式的一般資訊

1. 在網頁主控台的主視窗中，選取 **資產管理 → 資產 (裝置)**。
   受管理裝置的清單將開啟。
2. 選擇包含必要裝置的管理群組。若要選取巢狀群組，請按一下視窗上方的 **顯示階層結構** 按鈕。
   此清單僅顯示選定管理群組的受管理裝置。
3. 按一下裝置名稱。
4. 這將開啟受管理裝置屬性視窗；在該視窗中，轉到**應用程式**索引標籤。
5. 在裝置上安裝的應用程式清單中，點擊 Kaspersky Endpoint Security。
   應用程式屬性視窗隨即開啟。
6. 在 **一般** 索引標籤的 **資訊** 區段中檢視應用程式的一般資訊：
   - **名稱**是應用程式的名稱。
   - **版本**是應用程式的版本號。
   - **已安裝**是應用程式在裝置上安裝的日期和時間。
   - **上次軟體更新**：Kaspersky Endpoint Security 軟體模組上次更新的日期和時間。
   - **上次同步**是裝置上次連線到卡巴斯基安全管理中心伺服器的日期和時間。
   - **目前狀態**是裝置上應用程式的狀態，例如 *執行中* 或 *已停止*。
   - **已安裝的更新**區塊包含關於已安裝的應用程式更新版本的資訊。
   - 在**應用程式資料庫**下，您可以找到關於應用程式資料庫更新發布的日期和時間以及上次更新的日期和時間的資訊。
7. 在 **一般** 索引標籤的 **元件** 區段中檢視應用程式功能元件的相關資訊。顯示每個元件的狀態（例如，*已停止*、*已暫停*、*未安裝*）和版本。
8. 在 **事件** 索引標籤上檢視裝置上的應用程式事件清單。

如何在管理主控台中檢視應用程式的一般資訊

1. 在卡巴斯基安全管理中心管理主控台樹中的**受管理裝置**資料夾中，選擇包含所需裝置的管理群組。
2. 在工作區選取“**裝置**”標籤。
3. 在受管理裝置清單中，選擇所需的裝置並雙擊它以開啟**屬性：<工作名稱>**視窗。
4. 在顯示的受管理裝置屬性視窗中，選取「**應用程式**」區段。
   視窗右側顯示裝置上安裝的卡巴斯基應用程式清單。

5. 選擇 Kaspersky Endpoint Security 並雙擊它以開啟應用程式屬性視窗。或者，您可以使用視窗下部的**屬性**按鈕。

   應用程式屬性視窗隨即開啟。

6. 在 **一般** 區段中檢視應用程式項目的一般資訊。

   - **版本號**：應用程式的版本號。
   - **已安裝**是應用程式在裝置上安裝的日期和時間。
   - **目前狀態**是應用程式 (kesl 服務) 的狀態。應用程式可以具有 *執行中* 或 *已暫停* 等狀態。
   - **上次軟體更新**：Kaspersky Endpoint Security 軟體模組上次更新的日期和時間。
   - **已安裝的更新**是關於已安裝的應用程式更新版本的資訊。
   - **應用程式資料庫**是應用程式資料庫更新發布的日期和時間。

7. 在 **元件** 區段中檢視應用程式功能元件的相關資訊。顯示每個元件的狀態（例如，*已停止*、*已暫停*、*未安裝*）和版本。

如何在命令列中檢視應用程式的一般資訊

執行以下指令：

```
kesl-control --app-info [--json] [--check-permissions]
```

其中：

`--json`：以 JSON 格式輸出資料。

`--check-permissions` 顯示權限設定不正確的應用程式目錄路徑。

指令執行的結果會在主控台中顯示以下資訊：

- **名稱**應用程式名稱。
- **版本**目前的應用程式版本。
- **政策**關於卡巴斯基安全管理中心安全政策是否在裝置上套用的資訊。
- 關於裝置上套用的政策的延伸資訊：
  - 政策名稱。
  - 政策上次在裝置上套用或更新時的日期和時間。
  - 裝置所屬的卡巴斯基安全管理中心管理群組。
  - 裝置上套用的政策設定檔清單（如果有）。

> 如果裝置上安裝的網路代理的**允許應用程式擷取裝置上的政策延伸資料**設定允許從 Kaspersky Endpoint Security 擷取延伸政策資料，則會顯示延伸政策資訊。預設情況下停用此設定。有關網路代理設定的詳細資訊，請參閱卡巴斯基安全管理中心說明。

- 有關應用程式使用之產品授權的資訊：
  - **應用程式產品授權資訊**應用程式產品授權資訊或應用程式產品授權金鑰狀態。
  - **Kaspersky Endpoint Security 產品授權到期日期**。應用程式產品授權到期日期和時間 (UTC)。
- Endpoint Detection and Response Optimum 元件和用於與卡巴斯基解決方案整合之元件的產品授權資訊。如果受防護裝置上已啟動下列元件，則會顯示這些欄位：
  - **EDR Optimum 許可資訊**。有關啟動 Endpoint Detection and Response Optimum 元件所用的的產品授權或 EDR Optimum 產品授權金鑰的狀態的資訊。
  - **EDR Optimum 產品授權到期日期。**產品授權到期日和時間（UTC）。
  - **KUMA 產品授權資訊**。關於使用卡巴斯基統一監控和分析平台功能的產品授權的資訊，或 KUMA 產品授權金鑰的狀態。
  - **KUMA 產品授權到期日期**。產品授權到期日和時間（UTC）。
  - **MDR 產品授權資訊**。有關啟動 Managed Detection and Response 元件所用的產品授權或 MDR 產品授權金鑰狀態的資訊。
  - **MDR 產品授權到期日期**。產品授權到期日和時間（UTC）。
  - **EDR Expert (on-premises) 產品授權資訊**。有關用於啟動 Endpoint Detection and Response Expert (on-premises) 元件的產品授權，或 EDR Expert (on-premises) 產品授權金鑰狀態的資訊。
  - **EDR Expert (on-premises) 的產品授權到期日期**。產品授權到期日和時間（UTC）。
  - **EDR Expert (cloud) 產品授權資訊**。有關用於啟動 Endpoint Detection and Response Expert (on-premise) 元件的產品授權，或 EDR Expert (cloud) 產品授權金鑰狀態的資訊。
  - **EDR Expert (cloud) 的產品授權到期日期**。產品授權到期日和時間（UTC）。
- **訂購狀態**訂購狀態。如果應用程式在訂購下啟動，則會顯示此欄位。
- **MDR BLOB 檔案狀態**用於與 Kaspersky Managed Detection and Response 整合的 MDR BLOB 檔案的狀態。
- **MDR BLOB 檔案的產品授權的到期日期**Kaspersky Managed Detection and Response產 品授權到期日期和時間（UTC）。如果已為 Kaspersky Managed Detection and Response 整合載入了BLOB設定檔，則會顯示此欄位。
- **備份狀態**有關備份狀態的資訊。
- **備份區使用**備份大小。
- **Scan_My_Computer 工作的上次執行日期**上次惡意軟體掃描工作的時間。
- **資料庫的上次發佈日期**應用程式資料庫上次發布的日期和時間。
- **應用程式資料庫已加載**關於應用程式資料庫是否已下載的資訊。
- **可更新的內核模組狀態**有關可更新的內核模組狀態的資訊。
- **卡巴斯基安全網路使用**關於使用卡巴斯基安全網路的資訊：延伸 KSN 模式、基本 KSN 模式或停用。

- **Light Agent 模式**。有關以 Light Agent 模式使用應用程式的資訊。如果應用程式以標準模式或 Endpoint Detection and Response Agent 模式使用，則不會顯示此行。
- **Endpoint Detection and Response Agent 模式**。有關以 EDR Agent 模式 使用應用程式的資訊。如果應用程式以基本模式或 Light Agent 模式使用，則不會顯示此行。
- **卡巴斯基安全網路基礎結構**關於與卡巴斯基信譽資料庫配合使用的基礎設施解決方案的資訊：`Kaspersky Security Network`或`Kaspersky Private Security Network`。
- **Kaspersky Managed Detection and Response 整合**。Kaspersky Managed Detection and Response 整合狀態。
- **Kaspersky Endpoint Detection and Response Optimum**。與 Kaspersky Endpoint Detection and Response Optimum 整合的狀態。
- **檔案威脅防護**。即時檔案威脅防護狀態。
- **容器監控**。即時掃描容器狀態。
- **系統完整性監控**。系統完整性監控元件狀態。
- **防火牆管理**。防火牆管理元件狀態。
- **加密軟體防護**。加密軟體防護元件狀態。
- **Web 威脅防護**。Web 威脅防護元件狀態。
- **裝置控制**。裝置控制元件狀態。
- **卸除式磁碟機掃描**。卸除式磁碟機掃描元件狀態。
- **BadUSB 攻擊防護**。BadUSB 攻擊防護元件狀態。
- **網路威脅防護**。網路威脅防護元件狀態。
- **行為偵測**。行為偵測元件狀態。
- **應用程式控制**。應用程式控制元件狀態。
- **Web 控制**。Web 控制元件狀態。
- **Kaspersky Endpoint Detection and Response Expert (on-premises) 整合**。與 Kaspersky Endpoint Detection and Response Expert (on-premises) 或 Kaspersky Endpoint Detection and Response (KATA) 整合的狀態。
- **Kaspersky Endpoint Detection and Response Expert (cloud) 整合**。Kaspersky Endpoint Detection and Response Expert (cloud) 整合狀態。
- **Sandbox 整合**。Sandbox 整合狀態。
- **卡巴斯基統一監控和分析平台整合**。卡巴斯基統一監控和分析平台整合狀態。
- **Kaspersky Network Detection and Response (KATA) 整合**Kaspersky Network Detection and Response (KATA) 整合狀態。
- **郵件威脅防護**。郵件威脅防護元件狀態。

- **更新後的動作**應用程式更新操作和使用者要執行的操作。
- **應用程式不穩定**有關應用程式當機時進行轉儲的資訊。如果在轉儲目錄中找到任何檔案，則會顯示此欄位。
- **應用程式狀態**有關網路代理連線狀態和系統目錄權限的資訊：
  - *OK*網路代理已連線，系統目錄權限已正確設定。
  - *緊急。無網路代理連線*
  - *緊急。系統目錄的權限配置不正確*
  - *緊急。無網路代理連線。系統目錄的權限配置不正確*

如何在圖形介面中檢視應用程式的一般資訊

1. 開啟應用程式圖形介面的主視窗。
2. 在主視窗下方，點擊**支援**按鈕。
   支援視窗開啟。
3. 檢視裝置和已安裝應用程式的一般資訊：
   - 應用程式版本。
   - **產品授權金鑰**顯示新增至應用程式的活動主產品授權金鑰，或一條提示未新增金鑰的訊息。點擊此欄位中的連結會開啟**產品授權**視窗，該視窗會顯示詳細的產品授權資訊。
   - **金鑰狀態**顯示關於活動主產品授權金鑰的狀態的資訊，或未新增金鑰的訊息。
   - **資料庫發佈日期**– 應用程式資料庫的狀態和發布日期。
   - **作業系統**– 關於裝置作業系統的資訊。
   - **應用程式管理** – 關於裝置是否受政策管理的資訊。

   如果在網路代理政策中啟用了**允許應用程式擷取裝置上的政策延伸資料**選項，則該視窗還會顯示關於在安裝了該應用程式的裝置上套用的政策的下列資訊。
   - **政策名稱**是安裝了應用程式的裝置上套用之政策的名稱。
   - **套用日期** – 在安裝了應用程式的裝置上最後套用或更新政策的日期和時間。
   - **管理員群組**是包含安裝了應用程式的裝置且受政策管理的管理群組的名稱。
   - **活動政策設定檔**是裝置上套用的活動政策設定檔清單（如果有）。

應用程式統計資料

您可以檢視最常掃描的檔案和已啟動處理程序的統計資料。

您可以在 kesl.ini 設定檔 的 `[ScannerImpactStats]` 區域中設定應用程式計算和顯示統計資料的方式。

如何在網頁主控台中檢視掃描統計資料

1. 在網頁主控台的主視窗中，選取 **資產管理 → 資產 (裝置)**。
   受管理裝置的清單將開啟。
2. 選擇包含必要裝置的管理群組。若要選取巢狀群組，請按一下視窗上方的 **顯示階層結構** 按鈕。
   此清單僅顯示選定管理群組的受管理裝置。
3. 按一下裝置名稱。
4. 這將開啟受管理裝置屬性視窗；在該視窗中，轉到**應用程式**索引標籤。
5. 在裝置上安裝的應用程式清單中，點擊 Kaspersky Endpoint Security。
6. 在開啟的應用程式屬性視窗中，在**應用程式設定**索引標籤上，選擇**統計資料→掃描統計資料**。
7. 在**掃描統計資料**視窗中檢視應用程式統計資料：
   - **最常掃描的應用程式（檔案威脅防護）**區塊會顯示檔案威脅防護元件最常掃描的應用程式的路徑，以及該元件存取這些應用程式的次數。檔案依存取次數的降序顯示。
   - 在**最常啟動的處理程序**下，您可以找到 Kaspersky Endpoint Security 最常偵測到的處理程序的路徑以及此類處理程序啟動的數量。處理程序路徑依處理程序啟動數量降序排列。

   您可以點擊每個區域上方的**匯出**按鈕，將對應的統計資料匯出到文字檔。

如何在管理主控台中檢視掃描統計資料

1. 在卡巴斯基安全管理中心管理主控台樹中的**受管理裝置**資料夾中，選擇包含所需裝置的管理群組。
2. 在工作區選取“**裝置**”標籤。
3. 在受管理裝置清單中，選擇所需的裝置並雙擊它以開啟**屬性：<工作名稱>**視窗。
4. 在顯示的受管理裝置屬性視窗中，選取「**應用程式**」區段。
   視窗右側顯示裝置上安裝的卡巴斯基應用程式清單。
5. 選擇 Kaspersky Endpoint Security 並雙擊它以開啟應用程式屬性視窗。或者，您可以使用視窗下部的**屬性**按鈕。
6. 在開啟的視窗中，選擇**統計資料→掃描統計資料**。
7. 檢視應用程式統計資料：
   - **最常掃描的應用程式（檔案威脅防護）**區塊會顯示檔案威脅防護元件最常掃描的應用程式的路徑，以及該元件存取這些應用程式的次數。檔案依存取次數的降序顯示。
   - 在**最常啟動的處理程序**下，您可以找到 Kaspersky Endpoint Security 最常偵測到的處理程序的路徑以及此類處理程序啟動的數量。處理程序路徑依處理程序啟動數量降序排列。

   您可以點擊每個區域下方的**匯出**按鈕，將對應的統計資料匯出到文字檔。

如何在命令列中檢視掃描統計資料

執行以下指令：

```
kesl-control [-S] --get-statistic [--files] [--processes]
```

其中：

- `--files`：檔案威脅防護元件掃描最頻繁的檔案的統計，以及元件存取這些檔案的次數。
- `--processes`: Kaspersky Endpoint Security 最常啟動的處理程序的統計資料，以及此類啟動的數量。

> 將處理程序從行為偵測元件的掃描中排除不會從統計資料中刪除這些處理程序，但可以提高 Kaspersky Endpoint Security 應用程式的效能。

如果您未指定任何選項，應用程式將顯示三個清單：最常掃描的檔案的統計資訊、最常啟動的處理程序的統計資訊以及在裝置上找到的掛載點清單。

> 在 CentOS 5.2、5.4、6.4 和 6.6 上，不會收集經常掃描檔案的統計資料。

發現的掛載點

您可以檢視在裝置上找到的掛載點清單。該清單會顯示資訊，指出掛載點是否已新增至掃描排除項目。

如何在網頁主控台中檢視掛載點清單

1. 在網頁主控台的主視窗中，選取 **資產管理 → 資產 (裝置)**。
   受管理裝置的清單將開啟。
2. 選擇包含必要裝置的管理群組。若要選取巢狀群組，請按一下視窗上方的 **顯示階層結構** 按鈕。
   此清單僅顯示選定管理群組的受管理裝置。
3. 按一下裝置名稱。
4. 這將開啟受管理裝置屬性視窗；在該視窗中，轉到**應用程式**索引標籤。
5. 在裝置上安裝的應用程式清單中，點擊 Kaspersky Endpoint Security。
6. 在開啟的應用程式屬性視窗中，在**應用程式設定**索引標籤上，選擇**統計資料→掛接點**。
   掛接點視窗將開啟。
7. 在表格中檢視掛載點的相關資訊：
   - **掛載點路徑**是裝置上偵測到的掛載點的路徑。
   - **命名空間**指示掛載點是否發現於命名空間中。
   - **已排除**指示掛載點是否已被新增至掃描排除項目。

掛載點路徑依下列方式排序：

- 靜態、系統、服務和其他掛載點
- 在其命名空間中安裝的 snap 套件和安裝點
- Docker 容器管理系統所建立的掛載點

透過點擊清單上方視窗頂端的**匯出**按鈕，您可以將掛載點清單匯出到文字檔。該檔案包含掛載點路徑清單，以及**[Namespace]**和**[Excluded]**標籤。

如何在管理主控台中檢視掛載點清單

1. 在卡巴斯基安全管理中心管理主控台樹中的**受管理裝置**資料夾中，選擇包含所需裝置的管理群組。
2. 在工作區選取"**裝置**"標籤。
3. 在受管理裝置清單中，選擇所需的裝置並雙擊它以開啟**屬性：<工作名稱>**視窗。
4. 在顯示的受管理裝置屬性視窗中，選取「**應用程式**」區段。
   視窗右側顯示裝置上安裝的卡巴斯基應用程式清單。
5. 選擇 Kaspersky Endpoint Security 並雙擊它以開啟應用程式屬性視窗。或者，您可以使用視窗下部的**屬性**按鈕。
6. 這會開啟應用程式屬性視窗；在該視窗中，選取**統計資料 → 掛載點**區段。
7. 在**掛載點清單**表格中檢視掛載點的相關資訊：
   - **掛載點路徑**是裝置上偵測到的掛載點的路徑。
   - **命名空間**指示掛載點是否發現於命名空間中。
   - **已排除**指示掛載點是否已被新增至掃描排除項目。

   掛載點路徑依下列方式排序：

   - 靜態、系統、服務和其他掛載點
   - 在其命名空間中安裝的 snap 套件和安裝點
   - Docker 容器管理系統所建立的掛載點

   透過點擊清單下方的**匯出**按鈕，您可以將掛載點清單匯出為文字格式的檔案。該檔案包含掛載點路徑清單，以及 `[Namespace]` 和 `[Excluded]` 標籤。

如何在命令列中檢視掛載點清單

執行以下指令：

```
kesl-control [-S] --get-statistic --mountpoints
```

輸出包含以下資訊：

- `[excluded]` 表示掛載點是否已新增至掃描排除項目。
- `[namespace]`，指示掛載點是否發現於命名空間中。
- 裝置上發現的掛載點的路徑。

掛載點路徑依下列方式排序：

- 靜態、系統、服務和其他掛載點
- 在其命名空間中安裝的 snap 套件和安裝點
- Docker 容器管理系統所建立的掛載點

功能和技術清單

在命令列中，您可以檢視應用程式功能清單，其中包含狀態資訊（已使用或未使用）以及用於實作這些應用程式功能的 Linux 技術。

檢視功能和技術清單

```
kesl-control --supported-tech-info
```

指令執行的結果會在主控台中顯示以下資訊：

檔案操作攔截：

狀態：使用中或未使用

技術：fanotify、檔案威脅防護內核模組、可更新的內核模組。

處理程序啟動攔截：

狀態：使用中或未使用

技術：eBPF、kprobe、netlink、未定義、可更新的內核模組。

掃描網路流量：

狀態：使用中或未使用

技術：eBPF、iptables、未定義。

iptables 公用程式：

狀態：使用中或未使用

技術：ipv6、未定義、逾時、支援規則中的多個標籤。

網路隔離：

狀態：使用中或未使用

技術：eBPF、iptables、未定義。

弱點利用防禦：

狀態：使用中或未使用

技術：未定義、可更新的內核模組。

即時保護狀態

即時電腦保護狀態決定檔案威脅防護元件的狀態。檔案威脅防護會為電腦提供最低限度的安全防護。該元件會與 Kaspersky Endpoint Security 一起啟動，並即時掃描檔案。

即時保護狀態

卡巴斯基安全管理中心中的狀態	指令列上的狀態	描述
執行中	已啟動	檔案威脅防護工作已啟動且正在執行。
正在啟動	正在啟動 或 正在還原	嘗試執行檔案威脅防護工作。請等待工作啟動。
已停止	已停止 或 正在停止	檔案威脅防護工作已手動停止。在卡巴斯基安全管理中心或電腦本機上執行該工作。 如果應用程式安裝在 Light Agent 模式下，當無法連線至 SVM 時，裝置會取得此狀態。
已暫停	正在暫停 或 已暫停	檔案威脅防護工作已手動暫停。在卡巴斯基安全管理中心或電腦本機上執行該工作。
未設定		應用程式以 EDR Agent 模式安裝。檔案威脅防護元件以通知模式運作。
未知		未知錯誤。

如何查看即時電腦保護狀態

您可以在卡巴斯基安全管理中心主控台的受管理裝置清單中，或在電腦本機上查看即時電腦保護狀態。

如何在網頁主控台中查看即時電腦保護狀態

在網頁主控台的主視窗中，選擇**資產管理 → 資產（裝置）**。

目前的保護狀態會顯示在裝置清單的 **即時防護狀態** 欄中。如果缺少 **即時防護狀態** 欄，請管理欄設定（ ⚙ ）。

如何在指令列上查看即時電腦保護狀態

執行以下指令：

```
kesl-control --get-task-state 1
```

因此，Kaspersky Endpoint Security 會以下列格式顯示檔案威脅防護運作的相關資訊：

名稱: File_Threat_Protection	
ID	: 1
類型	: OAS
狀態	: <protection status>

即時電腦保護狀態不是 執行中 時該怎麼辦

1. 確保在政策內容中已啟用檔案威脅防護。
2. 確保應用程式已啟動。
3. 請嘗試執行檔案威脅防護工作：

   如何在網頁主控台中執行檔案威脅防護工作

   1. 在網頁主控台的主視窗中，選擇**資產管理 → 資產（裝置）**。
      受管理裝置的清單將開啟。
   2. 在清單中找到您的裝置並點擊其名稱。
   3. 這將開啟受管理裝置屬性視窗；在該視窗中，轉到**工作**索引標籤。
      這會開啟裝置上所有工作的清單。
   4. 選取 **檔案威脅防護** 工作，然後點擊 **執行** 按鈕。

   如何在指令列上執行檔案威脅防護工作

   執行以下指令：

   ```
   kesl-control --start-task 1
   ```

事件和報告

當應用程式執行時，會發生各種*事件*。這些事件可能是資訊性的，也可能包含重要資料。例如，應用程式可以使用事件來通知應用程式資料庫更新成功，或通知應用程式程式元件出現錯誤，需要修復。

Kaspersky Endpoint Security 將關於應用程式事件的資訊儲存到以下記錄中：

- 應用程式事件記錄。預設情況下，應用程式會將事件資訊儲存在位於 /var/opt/kaspersky/kesl/private/storage 目錄中的事件記錄資料庫檔案中。您可以在指令列中設定應用程式事件記錄。
- 作業系統記錄 (syslog)。預設不使用作業系統記錄。您可以啟用將事件儲存到此記錄。

存取應用程式事件記錄和作業系統記錄需要 root 權限。

如果 Kaspersky EndpoinSecurity 由卡巴斯基安全管理中心管理，則關於事件的資訊可能會被傳送至卡巴斯基安全管理中心伺服器。聚合規則適用於某些事件。如果在應用程式執行時短時間內建立了大量相同類型的事件，應用程式將切換到事件聚合模式，並向卡巴斯基安全管理中心傳送聚合事件以及事件設定描述。對於不同的事件可能會採用不同的聚合規則。如需事件的詳細資訊，請參閱 卡巴斯基安全管理中心說明。

您可以透過以下方式接收關於應用程式事件的資訊：

- 在管理主控台和網頁主控台中
- 在指令列中
- 使用應用程式的圖形使用者介面時 — 如果已在政策屬性或應用程式的一般設定中啟用 顯示通知，則會在快顯通知中顯示

應用程式可以產生有關應用程式執行時發生的事件的各種類型的*報告*。報告包含關於每個 Kaspersky Endpoint Security 元件的運行、每個工作的結果以及應用程式的整體運行的資訊。

您可以透過以下方式檢視報告：

- 卡巴斯基安全管理中心報告可在管理主控台和網頁主控台中取得。您可以使用它們來獲取關於受感染檔案或金鑰和應用程式資料庫的使用情況等資訊。如需使用卡巴斯基安全管理中心報告的詳細資訊，請參閱 卡巴斯基安全管理中心說明。
- Kaspersky Endpoint Security 的圖形使用者介面會顯示應用程式、其元件和工作的報告。

報告和事件的內容

事件和報告可能包含以下個人資料：

- 作業系統使用者的使用者名稱和使用者 ID
- 使用者檔案路徑
- 加密軟體防護元件掃描的遠端裝置的 IP 位址
- 防火牆管理元件掃描的網路封包傳送者和接收者的 IP 位址
- 更新來源的網址
- 一般應用程式設定值
- 指令列工作名稱和設定
- 偵測到惡意、網路釣魚、廣告軟體網址以及包含入侵者可以用來入侵裝置或資料的合法應用程式的網址
- 容器和映像的名稱
- 容器和映像的路徑
- 裝置的名稱和 ID
- 應用程式類別的名稱

- 儲存庫的網址
- 應用程式可執行檔的檔案名稱、路徑和雜湊

檔案路徑中的字元轉義規則

某些事件可能包含檔案路徑。對於輸出，檔案路徑被視為 UTF-8 字串。如果路徑中的任何位元組不符合UTF-8編碼規則，則用 **?** 字元替換。任何對 Unicode 範圍之外的字元代碼（大於 0x10FFFF）進行編碼的四位元組序列也將被替換為 **?** 字元。特殊字元以某種方式逸出（替換）。

以下規則適用於`kesl-control -E --query`輸出中事件內檔案路徑中的逸出字元：

- '\a', '\b', '\t', '\n', '\v', '\f', '\r' 字符被替換為兩個字元，如下所示：

  '\a' -> "\\a"

  '\b' -> "\\b"

  '\t' -> "\\t"

  '\n' -> "\\n"

  '\v' -> "\\v"

  '\f' -> "\\f"

  '\r' -> "\\r"

- 所有其他特殊字元均不加修改地輸出。

以下規則適用於`kesl-control -E --query --json`輸出中事件內檔案路徑中的逸出字元：

- 根據 JSON 格式，'\b'，'\f'，'\n'，'\r'，'\t'，'"'，'\\'字元的逸出如下：

  '\b' -> "\\b"

  '\f' -> "\\f"

  '\n' -> "\\n"

  '\r' -> "\\r"

  '\t' -> "\\t"

  '"' -> "\\"

  '\\' -> "\\\\"

- 所有其他特殊字元均按照 JSON 中逸出特殊字元的一般規則進行逸出（'\a' -> '\u0007'）。

傳送到 syslog 時事件中檔案路徑中的字元逸出規則：

- 根據 JSON 格式，'\b'，'\f'，'\n'，'\r'，'\t'，'"'，'\\'字元的逸出如下：

  '\b' -> "\\b"

  '\f' -> "\\f"

  '\n' -> "\\n"

  '\r' -> "\\r"

  '\t' -> "\\t"

  '"' -> "\\"

  '\\' -> "\\\\"

- 所有其他特殊字元均按照 JSON 中逸出特殊字元的一般規則進行逸出（'\a' -> '\u0007'）。

描述規則時序列中的第一個反斜線是逸出字元。

例如：
`'\a'` 是一個字元（一個控製字元）。

`'\\a'` 是兩個字元（反斜線 +「a」字元）。

`'\\'` 是一個字元（反斜線），`'\\\\'` 是兩個字元（反斜線 + 反斜線）。

配置將事件記錄到作業系統日誌中

Kaspersky Endpoint Security 執行期間發生的事件可以記錄在作業系統日誌 (syslog) 中。您可以使用網頁主控台、管理主控台或指令列啟用或停用此日誌中的事件記錄。

依預設，將事件記錄到作業系統日誌的功能已停用。

如果 Kaspersky Endpoint Security 以標準模式或 EDR Agent 模式執行，並由卡巴斯基安全管理中心中的政策進行管理，則依預設，新增和移除產品授權金鑰以及產品授權到期的資訊會記錄在作業系統日誌中。您可以在套用於應用程式的政策的屬性中選擇想要記錄在作業系統日誌中的事件。

如何在網頁主控台中設定將事件記錄到 syslog

1. 在網頁主控台的主視窗中，選取 **資產管理** → **政策**。
2. 按一下 Kaspersky Endpoint Security for Linux 政策的名稱。
   政策內容視窗將開啟。
3. 轉到**應用程式設定**索引標籤。
4. 選取 **一般設定** → **事件設定**。
   事件類型會依嚴重性分組顯示。
5. 在含有與您要設定記錄到作業系統日誌之事件相對應的嚴重性等級名稱的區塊中，按一下 **設定** 按鈕。
   這會開啟一個視窗，其中列出所選嚴重性等級的所有事件。您可以針對每個事件個別啟用或停用記錄到作業系統日誌。
6. 在 **事件** 欄中，按一下您要設定記錄到作業系統日誌的事件名稱。
7. 前往 **通知** 標籤。
8. 選取或清除 **儲存在作業系統事件日誌中** 核取方塊。

事件通知設定

如何在管理主控台中設定將事件記錄到 syslog

1. 在卡巴斯基安全管理中心管理主控台樹中的**受管理裝置**資料夾中，開啟包含所需裝置的管理群組名稱的資料夾。

2. 在工作區選擇"**政策**"標籤。

3. 在政策清單中，選擇所需的政策並雙擊它以開啟**屬性：<政策名稱>**視窗。

4. 前往 **一般設定** → **介面** 區段。

5. 在 **通知** 下，按一下 **設定**。

   通知設定 視窗隨即開啟。

6. 使用核取方塊選擇應用程式在作業系統日誌中記錄的事件。

   您也可以選取特定嚴重性等級的所有事件：

   - *緊急事件*對裝置安全構成嚴重威脅（偵測到惡意物件、弱點、應用程式執行問題）。緊急事件需要您立即關注。我們建議不要停用緊急事件通知。

   - *功能性故障*是指應用程式發生故障（處理錯誤、工作配置錯誤）。此類事件不會對裝置安全構成直接威脅，但需要您採取措施使應用程式能正常運作。

   - *"警告"*不要求您立即採取行動，但可能表示裝置安全有潛在的未來威脅。

   - *資訊性訊息*對應於具有資訊性質的事件。

如何在命令列中設定將事件記錄到 syslog

您可以透過`UseSyslog`中的UseSyslog選項在指令列中啟用或停用將事件儲存到作業系統日誌。

您可以透過指令列開關或包含所有一般應用程式設定的設定檔來編輯該選項。

啟用或停用將事件記錄到 `syslog`

```
kesl-control --set-app-settings UseSyslog=<Yes|No>
```

其中：

- `Yes`：啟用將所有事件儲存到 syslog。
- `No`（預設）：禁止將事件儲存到 syslog。

配置應用程式事件記錄設定

預設情況下，關於事件的資訊會儲存到裝置上的應用程式事件記錄中。

事件記錄資料庫包含下列檔案：

- 多個包含事件的檔案。檔案數量取決於事件記錄中的當前事件數，以及設定應用程式儲存的最大事件數（`MaxEventsNumber` 設定）。

  事件檔案的名稱包含其序號（例如：events.db.0001）。當檔案存滿時，系統會自動建立新檔案。若所有事件檔案（不包含最早檔案）中的事件總數達到 `MaxEventsNumber` 設定值，系統會刪除最早的檔案。這表示應用程式儲存的事件數可能超過設定值。

- 用於管理事件檔案的資料庫的主檔案，其中儲存關於事件記錄檔案的資訊。此檔案無法刪除。

您可以透過一般應用程式設定在命令列中管理以下應用程式事件記錄選項：

- 透過 `EventsStoragePath` 設定變更應用程式事件記錄資料庫的路徑。預設值：/var/opt/kaspersky/kesl/private/storage/events.db。
- 透過`MaxEventsNumber`選項指定應用程式要儲存的最大事件數。預設值：500000。

您可以在命令列或設定檔中檢視目前的一般應用程式設定。

將應用程式一般設定的目前值輸出到主控台

```
kesl-control --get-app-settings [--json]
```

其中，指定 `--json` 以 JSON 格式輸出設定。

將應用程式一般設定的目前值輸出到設定檔

```
kesl-control --get-app-settings --file <path to configuration file> [--json]
```

其中 `--file <path to configuration file>` 是您要將應用程式一般設定輸出至其中的設定檔路徑。如果指定檔案的名稱而不指定其路徑，則檔案會在目前目錄中建立。如果指定路徑中已經存在檔案，則該檔案會被覆寫。如果指定的目錄不存在，則不會建立設定檔。

您可以藉助指令列開關或包含所有一般應用程式設定的設定檔來變更設定值。

使用命令列選項修改事件設定

```
kesl-control --set-app-settings <setting name>=<setting value> [<setting name>=<setting value>]
```

其中，<設定名稱>=<設定值> 是其中一項設定的名稱和值。

使用設定檔變更事件設定

```
kesl-control --set-app-settings --file <path to configuration file> [--json]
```

其中：

- `--file <path to configuration file>` 是包含一般應用程式設定的設定檔完整路徑。如果刪除設定檔中的任意參數，則命令執行後將顯示該參數的預設值。
- 如果要從 JSON 設定檔匯入設定，請指定 `--json` 選項。如果未指定 --json 選項，應用程式會嘗試從 INI 檔案匯入。如果匯入失敗，則會顯示錯誤。

檔案中定義的所有一般設定的值將被匯入到應用程式中。

檢視應用程式事件

在卡巴斯基安全管理中心檢視 Kaspersky Endpoint Security 應用程式的所有事件

Kaspersky Endpoint Security 安全應用程式的事件依嚴重程度分為以下幾種類型：

- *緊急事件*對裝置安全構成嚴重威脅（偵測到惡意物件、弱點、應用程式執行問題）。緊急事件需要您立即關注。我們建議不要停用緊急事件通知。
- *功能性故障*是指應用程式發生故障（處理錯誤、工作配置錯誤）。此類事件不會對裝置安全構成直接威脅，但需要您採取措施使應用程式能正常運作。
- *"警告"*不要求您立即採取行動，但可能表示裝置安全有潛在的未來威脅。
- *資訊性訊息*對應於具有資訊性質的事件。

所有 Kaspersky Endpoint Security 事件的清單顯示在網頁主控台和管理主控台中。

如何在網頁主控台中檢視所有事件清單

1. 在網頁主控台的主視窗中，選擇**資產管理 → 政策**。
2. 點擊 Kaspersky Endpoint Security 政策的名稱。

   政策內容視窗將開啟。
3. 前往 **事件設定** 索引標籤。

   顯示依嚴重性篩選的所有事件清單。
4. 使用左側功能表檢視其他嚴重性等級的所有事件。

如何在管理主控台中檢視所有事件清單

1. 在卡巴斯基安全管理中心管理主控台樹中的**受管理裝置**資料夾中，開啟包含所需裝置的管理群組名稱的資料夾。
2. 在工作區選擇“**政策**”標籤。
3. 在政策清單中，選擇所需的政策並雙擊它以開啟**屬性：<政策名稱>**視窗。
4. 前往 **一般設定** → **通知設定** 區段。
5. 在 **通知** 下，按一下 **設定**。

   通知設定 視窗隨即開啟。

您可以配置事件通知。通知會及時為您提供關於應用程式事件的資訊。您可以配置在從應用程式接收事件或透過電子郵件接收關於事件的通知時執行指令碼。如需使用卡巴斯基安全管理中心通知的詳細資訊，請參閱 卡巴斯基安全管理中心說明 。

在應用程式圖形介面中檢視事件

預設情況下，在應用程式的圖形介面中，事件資訊以彈出通知的形式顯示。

如何在網頁主控台中設定彈出式通知

1. 在網頁主控台的主視窗中，選取 **資產管理** → **政策**。
2. 按一下 Kaspersky Endpoint Security for Linux 政策的名稱。

   政策內容視窗將開啟。
3. 轉到**應用程式設定**索引標籤。
4. 選取 **一般設定** → **事件設定**。
5. 點擊 **其他設定** 連結。

   其他設定視窗隨即開啟。
6. 選取或清除 **在圖形使用者介面中顯示彈出式通知** 核取方塊。預設情況下已選擇此核取方塊。
7. 儲存變更。

如何在管理主控台中設定彈出式通知

1. 在卡巴斯基安全管理中心管理主控台樹中的**受管理裝置**資料夾中，開啟包含所需裝置的管理群組名稱的資料夾。
2. 在工作區選擇“**政策**”標籤。
3. 在政策清單中，選擇所需的政策並雙擊它以開啟**屬性：<政策名稱>**視窗。
4. 前往 **一般設定** → **通知設定** 區段。
5. 選取或清除 **在圖形使用者介面中顯示彈出式通知** 核取方塊。預設情況下已選擇此核取方塊。

如何在命令列中設定彈出式通知

在指令列中，您可以使用 `ShowPopUpNotifications` 中的ShowPopUpNotifications啟用或者停用圖形介面中的彈出通知。

您可以藉助命令列開關或包含所有一般應用程式設定的設定檔來變更設定的值。

啟用在圖形介面中顯示彈出式通知

```
kesl-control --set-app-settings ShowPopUpNotifications=<Yes|No>
```

其中：

- `Yes`（預設值）— 在圖形使用者介面中顯示彈出通知。
- `No`——不在圖形使用者介面中顯示彈出通知。

在命令列中檢視 Kaspersky Endpoint Security 應用程式的目前事件

在命令列中，您可以輸出應用程式中所有目前事件的資訊，或輸出與指定工作相關的事件資訊。您可以使用篩選器輸出某些目前事件，例如指定類型的事件。

在主控台中顯示所有目前應用程式事件的資訊

```
kesl-control -W
```

該命令可傳回事件的名稱以及關於該事件的附加資訊。

執行工作，並將與其相關聯的目前事件資訊輸出到主控台

```
kesl-control --start-task <task ID|name> -W
```

其中 `<<task ID|name>` 是建立工作時指派給工作的 ID，或是命令列中的工作名稱。

此命令會啟動具有指定 ID 或名稱的工作，並啟用與該工作相關聯之目前事件的輸出。事件會在此工作產生後立即輸出。

啟動 `ID=1` 的工作並啟用其事件輸出的範例

```
kesl-control --start-task 1 -W
```

在主控台中顯示符合篩選條件的目前事件資訊

```
kesl-control -W --query "<filter conditions>"
```

其中，`<filter conditions>` 是一個或多個採用 `<field> <comparison operation> '<value>'` 格式並由 `and` 邏輯運算子結合的 邏輯運算式。

TaskStateChanged 事件輸出的範例

```
kesl-control -W --query "EventType == 'TaskStateChanged'"
```

由 'User' 使用者啟動的 TaskSettingsChanged 事件輸出範例

```
kesl-control -W --query "EventType == 'TaskSettingsChanged' and Initiator == 'User'"
```

顯示應用程式事件記錄中的事件

您可以使用命令列，將應用程式事件記錄中的事件資訊輸出至主控台或檔案。若要輸出事件子集，請使用 篩選。

將應用程式事件記錄中所有事件的資訊輸出至主控台

```
kesl-control -E --query [--db <database file>]
```

其中，`<database file>` 是要從中輸出事件之事件記錄資料庫檔案的完整路徑。

預設情況下，應用程式會將事件資訊儲存在 `/var/opt/kaspersky/kesl/private/storage/events.db` 資料庫中。資料庫的位置由 `EventsStoragePath` 一般應用程式設定決定。

如果事件記錄位於預設資料庫中，請使用以下命令將事件輸出至主控台：

```
kesl-control -E
```

您可以使用`less`來導覽顯示的事件清單。預設情況下，應用程式最多儲存 500,000 個事件。應用程式儲存的最大事件數由`MaxEventsNumber`一般應用程式設定決定。

在主控台中顯示應用程式事件記錄中符合特定條件的事件資訊

```
kesl-control -E --query "<filter conditions>" [--db <database file>] [-n <number>] [--json] [--reverse]
```

其中：

- `<filter conditions>` 會指定一個或多個採用 `<field> <comparison operator> '<value>'` 格式並使用邏輯運算子 `and` 結合的 邏輯運算式，以限制查詢結果。
- `<number>` 是您要輸出的選取範圍中最新事件的數量（也就是從選取範圍末尾開始計算的記錄數）。
- `--json`：以 JSON 格式輸出事件。
- `--reverse`：以相反順序顯示事件（從最新事件在頂部到最舊事件在底部）。

將應用程式事件記錄中所有事件的資訊輸出至檔案

```
kesl-control -E --query "<>" [--db <database file>] [-n <number>] --file <path to file> [--json]
```

其中，`--file <path to file>` 是要將事件輸出至其中之檔案的完整路徑。

實用文章

如何處理誤報

檢視報告

檢視報告僅可在應用程式的圖形介面中進行。

有關每個 Kaspersky Endpoint Security 元件的操作、每個掃描工作的執行情況、更新工作和完整性檢查工作以及應用程式整體操作的資訊，均記錄在*報告*中。

報告中使用以下事件重要性等級：

- *緊急*— 具有緊急重要性等級的事件，需要您注意，因為它們表明應用程式運行中存在問題或裝置防護中存在弱點
- *高*
- *中等*
- *低等*
- *資訊*
- *錯誤*

應用程式中提供以下報告：

- **統計**。檔案威脅防護和掃描工作統計資訊。您可以透過點擊**重新加載**按鈕來更新顯示的報告。
- **系統稽核**。關於應用程式運作期間以及使用者與應用程式互動期間發生的事件資訊。
- **威脅防護**。關於以下應用程式元件執行時記錄之事件的資訊：
  - 檔案威脅防護
  - 卸除式磁碟機掃描
  - Anti-Cryptor
  - Web 威脅防護
  - 郵件威脅防護
  - 網路威脅防護
  - BadUSB 攻擊防護
  - 防火牆管理

- 應用程式控制
- 裝置控制
- 行為偵測
- 弱點利用防禦
- 系統完整性監控
- Web 控制

- **按需工作**。此報告包含關於掃描工作、更新工作和系統完整性檢查工作記錄的資訊事件。
- **執行防禦** 此報告包含 EDR Expert (on-premises) 和 EDR Optimum 元件在物件執行防禦期間記錄的事件資訊。

如何在應用程式介面中檢視報告

1. 開啟應用程式圖形介面的主視窗。
2. 在主應用程式視窗的下方，點擊**報告**按鈕。

   報告視窗將開啟。
3. 在**報告**視窗的左側，選擇所需的報告類型。

   報告會顯示在視窗右側。報告資料以包含事件清單的表格形式呈現。表中的每一行都包含關於單獨事件的資訊。事件屬性顯示在表格列中。各種元件和工作執行時記錄的事件具有不同的屬性集。

   預設情況下，事件會依 **日期和時間** 欄中的值以遞增順序排序。為便於處理報告，您可以透過以下幾種方法修改資料的顯示方式：

   - 按發生時間篩選事件清單。
   - 使用搜尋功能尋找特定的事件。
4. 要檢視事件的相關詳細資訊，請在報告中選擇事件。

   包含此事件屬性的部分將顯示在視窗底部。

獲取系統效能指標

Kaspersky Endpoint Security 會影響作業系統。為了幫助您分析影響，應用程式可以獲取與應用程式效能相關的指標。

您可以使用 Grafana 等資料視覺化工具分析指標。您可以將匯出的指標發佈到 Prometheus 和 Zabbix 等監控系統。

設定收集應用程式所使用之作業系統資源的指標

```
kesl-control [-J] --export-metrics [--period <interval in seconds between outputs>|--interactive]
```

其中：

`--period` 啟用將結果定期輸出至命令列（輸出間隔以秒為單位指定）。

`--interactive`啟用互動式輸出（按下**Enter**鍵時）。

此指令可將指標清單輸出到主控台。

指標清單

指標的內部名稱；指標的標籤和類型	描述和建議服閾值設定
lfs_system_descriptor_opened_count 量測計	kesl 處理程序目前開啟的描述符數量。 如果描述符數量每小時增加超過 250 個，建議聯絡技術支援。
lfs_system_uptime_milliseconds 計數器	自作業系統啟動迄今的毫秒數目。
lfs_system_memory_usage_bytes “type=virtual”標籤 量測計	kesl 處理程序目前使用的虛擬記憶體數量。 建議採取措施，依據系統資訊設定閾值。您可以手動或使用指令碼取得此資訊。如需範例指令碼，可以聯絡技術支援。
lfs_system_memory_usage_bytes “type=resident”標籤 量測計	kesl 處理程序目前使用的駐留記憶體數量。 建議採取措施，依據系統資訊設定閾值。您可以手動或使用指令碼取得此資訊。如需範例指令碼，可以聯絡技術支援。
lfs_system_memory_usage_bytes “type=swap”標籤 量測計	kesl 處理程序目前使用的交換空間量。 建議採取措施，依據系統資訊設定閾值。您可以手動或使用指令碼取得此資訊。如需範例指令碼，可以聯絡技術支援。
lfs_system_memory_wd_limits_bytes “type=virtual”標籤 量測計	限制 kesl 處理程序對虛擬記憶體的使用。
lfs_system_memory_wd_limits_bytes “type=resident”標籤 量測計	限制 kesl 處理程序對駐留記憶體的使用。
lfs_system_memory_wd_limits_bytes “type=swap”標籤 量測計	kesl 處理程序對交換空間的使用限制。
lfs_system_cpu_usage_milliseconds “type=user”標籤 計數器	自 kesl 處理程序啟動迄今，kesl 處理程序在使用者空間中佔用的 CPU 時間（毫秒）。 建議採取措施，依據系統資訊設定閾值。您可以手動或使用指令碼取得此資訊。如需範例指令碼，可以聯絡技術支援。
lfs_system_cpu_usage_milliseconds “type=kernel”標籤 計數器	自 kesl 處理程序啟動迄今，kesl 處理程序在內核空間中佔用的 CPU 時間（毫秒）。 建議採取措施，依據系統資訊設定閾值。您可以手動或使用指令碼取得此資訊。如需範例指令碼，可以聯絡技術支援。
lfs_system_cpu_usage_milliseconds “type=total”標籤 計數器	自 kesl 處理程序啟動迄今，kesl 處理程序在使用者空間和內核空間中佔用的 CPU 時間（毫秒）。 如果 kesl 處理程序佔用的 CPU 時間超出其餘工作負載，建議聯絡技術支援。
lfs_tcpSynInterceptor_connection_hanging_count 計數器	自 kesl 處理程序啟動迄今，伺服器與用戶端之間 TCP 網路中握手階段掛起的網路連線總數（若網路連線等待遠端伺服器允許連線的時間達 1 秒至 2 分鐘，則視為掛起，具體取決於 /proc/sys/net/ipv4/tcp_syn_retries 中的系統設定）。 此指標數值上升，可能是遠端伺服器無法存取或遺失所致。如果掛起的網路連線數量每分鐘增加超過 10 個，建議聯絡技術支援。
lfs_tcpSynInterceptor_connection_count 量測計	目前等待連線到遠端伺服器的網路連線數。
lfs_tcpSynInterceptor_verdict_count “verdict=allow”標籤 計數器	自 kesl 處理程序啟動迄今已建立的被攔截的連線總數。
lfs_tcpSynInterceptor_verdict_count “verdict=drop”標籤 計數器	自 kesl 處理程序啟動迄今，攔截的尚未建立連線總數。

指標的內部名稱；指標的標籤和類型	描述和建議服閾值設定
lfs_tcpSynInterceptor_verdict_count “verdict=unknown”標籤 計數器	自 kesl 處理程序啟動迄今，遠端伺服器解決方案無法處理的網路連線總數。
lfs_tcpSynInterceptor_verdict_latency_milliseconds 直方圖	自 SYN 封包被攔截至其判定發放之時，遠端伺服器對連線做出判定所用時間的直方圖。
lfs_tproxy_connection_count “direction=inbound”標籤 量測計	目前攔截的輸入網路連線數量。
lfs_tproxy_connection_count “direction=outbound”標籤 量測計	目前攔截的輸出網路連線數量。
lfs_tproxy_connection_processed_count “direction=inbound”標籤 計數器	已攔截的入站網路連線總數。
lfs_tproxy_connection_processed_count “direction=outbound”標籤 計數器	已攔截的出站網路連線總數。
lfs_tproxy_connection_orphaned_count 計數器	自 Web 威脅防護、網路威脅防護和 Web 控制防護元件啟動起，Kaspersky Endpoint Security 攔截的連線總數（但並非故意攔截，例如因 iptables 設定不相容，或應用程式沒有時間處理新攔截設定所致）。此類連線會被拒絕。 如果此類連線的總數超過 10，則可能表示應用程式或系統運作不正確，建議聯絡技術支援。
lfs_tproxy_threadPool_task_count 計數器	自 Web 威脅防護、網路威脅防護和 Web 控制防護元件啟動起，新增至執行緒池的工作總數（新連線、新一批資料、已傳送的資料等）。 如果已建立但是未完成的工作總數不斷增加，則需要新增資源、設定排除項目或聯絡技術支援。
lfs_tproxy_threadPool_thread_count 量測計	服務於網路攔截器 MITM 機制的執行緒數量。執行緒由執行緒管理器建立，用於處理連線。所有執行緒都會執行相同的程式碼，並在其中等候網路事件，例如新連線以及已建立連線上的傳入封包。
lfs_tproxy_threadPool_thread_waiting 量測計	lfs_tproxy_threadPool_thread_count 中的空閒執行緒數量。在網路攔截器的 MITM 機制中等候 poll 的執行緒。
lfs_tproxy_threadPool_task_duration_milliseconds 直方圖	攔截連線處理工作執行時間的直方圖。 如果 95% 的工作執行時間超過 1 秒，則需要新增資源、設定排除項目或聯絡技術支援。
lfs_tproxy_socket_count 量測計	目前通訊端（偵聽通訊端和連線通訊端）數量。攔截連線有 2 個連線通訊端。
lfs_trafficScanning_object_hanging_count 量測計	目前攔截流量中的掛起物件掃描數量（掃描持續時間超過 1 分鐘視為掛起）。 掛起物件掃描總數超過 35 表示應用程式資料庫有問題。如果遇到這種情況，建議聯絡技術支援。
lfs_trafficScanning_object_duration_milliseconds 直方圖	攔截流量物件掃描持續時間的直方圖。 如果 95% 的物件掃描時間超過 1 秒，則需要新增資源、更新應用程式資料庫或聯絡技術支援。 如果攔截流量中的封包掃描增長率為 0，且 lfs.tproxy.threadPool.task.count 指標的值不為 0，則需要更新應用程式資料庫或聯絡技術支援。
lfs_fileMonitor_cache_size 量測計	檔案監控（檔案修訂快取）的目前大小，用於監控檔案修改。 如果檔案監控快取的目前大小大於 50,000，建議聯絡技術支援。
lfs_fileMonitor_cache_hit_count 計數器	檔案監控快取（檔案修訂快取）的命中計數，用於監控檔案修改。
lfs_fileMonitor_cache_miss_count 計數器	檔案監控快取（檔案修訂快取）的未命中計數，用於監控檔案修改。

指標的內部名稱；指標的標籤和類型	描述和建議服閾值設定
lfs_faCache_file_count 量測計	免掃描 fanotify 攔截器檔案快取的目前大小。 如果檔案快取的目前大小大於 100,000，建議聯絡技術支援。
lfs_faCache_file_hit_count 計數器	免掃描 fanotify 攔截器檔案快取的命中計數。
lfs_faCache_file_miss_count 計數器	免掃描 fanotify 攔截器檔案快取的未命中計數。
lfs_faCache_volume_count 量測計	fanotify 攔截器掛載點快取的目前大小。
lfs_oas_cache_file_count 量測計	免掃描檔案威脅防護檔案快取的目前大小。 如果檔案快取的目前大小大於 100,000，建議聯絡技術支援。
lfs_oas_cache_file_hit_count 計數器	免掃描檔案威脅防護檔案快取的命中計數。
lfs_oas_cache_file_miss_count 計數器	免掃描檔案威脅防護檔案快取的未命中計數。
lfs_oas_cache_volume_count 量測計	檔案威脅防護掛載點快取的目前大小。
lfs_processManager_cache_size 量測計	系統中目前已快取的活動處理程序數量。
lfs_processManager_cache_hit_count 計數器	系統處理程序快取的命中計數。
lfs_processManager_cache_miss_count 計數器	系統處理程序快取的未命中計數。
lfs_blockingProcessInterceptor_cache_size 量測計	可用於啟動處理程序的解譯器快取的目前大小。 這個數字取決於指令碼在特定裝置上執行的強度。如果檔案快取的目前大小大於 10000，建議聯絡技術支援。
lfs_blockingProcessInterceptor_cache_hit_count 計數器	解譯器快取的命中計數。
lfs_blockingProcessInterceptor_cache_miss_count 計數器	解譯器快取的未命中計數。
lfs_doc_prevention_cache_file_count 量測計	開啟文件時，不需要掃描的物件的 *物件執行防禦* 工作檔案快取目前大小。
lfs_script_prevention_cache_file_count 量測計	執行指令碼時，不需要掃描的物件的 *物件執行防禦* 工作檔案快取目前大小。
lfs_doc_prevention_cache_file_hit_count 計數器	開啟文件時，不需要掃描的物件的 *物件執行防禦* 工作檔案快取命中次數。
lfs_script_prevention_cache_file_hit_count 計數器	執行指令碼時，不需要掃描的物件的 *物件執行防禦* 工作檔案快取命中次數。
lfs_doc_prevention_cache_file_miss_count 計數器	開啟文件時，不需要掃描的物件的 *物件執行防禦* 工作檔案快取未命中次數。
lfs_script_prevention_cache_file_miss_count 計數器	執行指令碼時，不需要掃描的物件的 *物件執行防禦* 工作檔案快取未命中次數。
lfs_doc_prevention_cache_volume_count 量測計	文件的「物件執行防禦」工作掛載點快取目前大小。
lfs_script_prevention_cache_volume_count 量測計	指令碼的「物件執行防禦」工作掛載點快取目前大小。
eka_telemetry_metrics_registry_callbacks_exec_duration_milliseconds 量測計	為登錄檔中所有已註冊用戶端執行目前指標更新之耗時（毫秒）。

指標的內部名稱；指標的標籤和類型	描述和建議服閾值設定
eka_telemetry_metrics_registry_registered_callbacks 量測計	MetricsRegistry 為所有已註冊用戶端執行指標更新回撥的目前次數。
eka_telemetry_metrics_registry_scrape_duration_milliseconds 量測計	獲取所有登錄檔指標之耗時（毫秒）。 如果該指標中 99% 的數值在 10 分鐘內超過 1 秒，建議聯絡技術支援。

應用程式穩定性監控

Kaspersky Endpoint Security 應用程式穩定性監控會追蹤應用程式異常停止的次數，並在應用程式效能不穩定時通知管理員。

如何在網頁主控台中設定應用程式穩定性監控

1. 在網頁主控台的主視窗中，選取 **資產管理** → **政策**。
2. 按一下 Kaspersky Endpoint Security for Linux 政策的名稱。
   政策內容視窗將開啟。
3. 轉到**應用程式設定**索引標籤。
4. 選擇“**一般設定** → **效能**”。
5. 選取或清除 **啟用應用程式穩定性監控** 核取方塊。預設情況下已清空此核取方塊。

如何在管理主控台中設定應用程式穩定性監控

1. 在卡巴斯基安全管理中心管理主控台樹中的**受管理裝置**資料夾中，開啟包含所需裝置的管理群組名稱的資料夾。
2. 在工作區選擇“**政策**”標籤。
3. 在政策清單中，選擇所需的政策並雙擊它以開啟**屬性：<政策名稱>**視窗。
4. 前往 **一般設定** → **應用程式設定** 區段。
5. 選取或清除 **啟用應用程式穩定性監控** 核取方塊。預設情況下已清空此核取方塊。

若要套用此設定，必須重新啟動應用程式和網路代理。

如果應用程式不穩定，則安裝了應用程式的裝置的屬性中會顯示下列訊息：*<次數>應用程式異常停止<日期和時間>*。

如何在命令列中設定應用程式穩定性監控

在命令列中，您可以使用 kesl.ini 設定檔中的 `TrackProductCrashes`、`ProductHealthLogFile`、`WarnThreshold`、`WarnAfter_#_crash` 和 `WarnRemovingThreshold` 設定來設定 Kaspersky Endpoint Security 穩定性監控。

`TrackProductCrashes` 允許在應用程式不穩定時將裝置狀態資訊從 Kaspersky Endpoint Security 傳送到卡巴斯基安全管理中心。此設定可以採用以下值：

- `Yes/true` 允許將裝置狀態資訊從 Kaspersky Endpoint Security 傳送到卡巴斯基安全管理中心。
- `No/false` 禁止將裝置狀態資訊從 Kaspersky Endpoint Security 傳送到卡巴斯基安全管理中心。

`ProductHealthLogFile`設定可讓您指定用於應用程式穩定性監控的檔案的路徑。預設值：/var/opt/kaspersky/kesl/private/kesl_health.log。

`WarnThreshold`設定可讓您設定時間間隔（以秒為單位），在此期間應用程式在顯示關於不穩定操作的通知之前必須經歷指定次數的異常停止。預設值：3600 秒。

`WarnRemovingThreshold`設定可讓您設定在此後清除應用程式不穩定狀態的時間間隔（以秒為單位）。預設值：86400 秒。

`WarnAfter_#_crash` 設定允許您設定應用程式異常停止的次數，超過此次數後會顯示關於應用程式不穩定的通知。此設定可採用 0 至 10 之間的值。預設值：10。如果值為 0，則不顯示不穩定的應用程式通知。

修改此檔案後，請重新啟動 Kaspersky Endpoint Security。

應用程式元件完整性檢查

Kaspersky Endpoint Security 包含許多不同的二進位模組，形式包括動態連結程式庫、可執行檔、設定檔和介面檔。駭客可以用包含惡意程式碼的其他檔案，取代應用程式的一個或多個可執行模組或檔案。為了防止這類模組和檔案遭到取代，Kaspersky Endpoint Security 可以檢查應用程式元件的完整性。該應用程式會檢查模組和檔案是否有未經授權的變更或損壞。如果應用程式模組或檔案的總和檢查碼不正確，則認為已損壞。

如果裝置上安裝了以下應用程式元件，則會執行完整性檢查：

- 應用程式套件
- 圖形使用者介面套件
- 卡巴斯基安全管理中心網路代理套件
- Kaspersky Endpoint Security 管理 Web 外掛程式
- Kaspersky Endpoint Security MMC 管理外掛程式

應用程式元件的完整性使用完整性檢查實用程式進行檢查。此實用程式檢查特殊清單（稱為*清單檔案*）中的檔案的完整性。每個應用程式元件都有自己的清單檔案，其中包含應用程式檔案清單，這些檔案的完整性對於該應用程式元件的正確運作至關重要。清單檔案經過數位簽章且其完整性也經過檢查。

若要在 Linux 裝置上執行完整性檢查公用程式，需要具有 root 權限的帳戶。

完整性檢查實用程式隨應用程式安裝，位於下列路徑：

- 作為應用程式套件（integrity_checker）的一部分：/opt/kaspersky/kesl/bin/integrity_checker。
- 作為 Kaspersky Endpoint Security 的 MMC 管理外掛程式 (integrity_checker.exe) 的一部分：
  - %ProgramFiles%\Kaspersky Lab\Kaspersky Security Center\Plugins\kesl_<版本號>.plg\integrity_checker.exe — 適用於 32 位元作業系統
  - %ProgramFiles(x86)%\Kaspersky Lab\Kaspersky Security Center\Plugins\kesl_<version number>.plg\integrity_checker.exe — 適用於 64 位元作業系統

清單檔案位於以下路徑：

- 若要檢查應用程式套件的完整性：/opt/kaspersky/kesl/bin/integrity_check.xml。
- 若要檢查圖形使用者介面套件的完整性：/opt/kaspersky/kesl/bin/gui_integrity_check.xml。
- 檢查網路代理：
  - /opt/kaspersky/klnagent/bin/kl_file_integrity_manifest.xml — 適用於 32 位元作業系統
  - /opt/kaspersky/klnagent64/bin/kl_file_integrity_manifest.xml — 適用於 64 位元作業系統
- 要檢查 Kaspersky Endpoint Security MMC 管理外掛程式
  - %ProgramFiles%\Kaspersky Lab\Kaspersky Security Center\Plugins\kesl_<plugin version>.plg\integrity_check.xml — 適用於 32 位元作業系統
  - %ProgramFiles(x86)%\Kaspersky Lab\Kaspersky Security Center\Plugins\kesl_<plugin version>.plg\integrity_check.xml — 適用於 64 位元作業系統

若要檢查解決方案元件的完整性，您需要從該元件工具的資料夾執行該工具。

檢查應用程式套件的完整性

```
integrity_checker [<path to manifest file>] --crl /var/opt/kaspersky/kesl/private/data/KDSCRL/ --signature-type kds-with-filename
```

檢查圖形介面套件的完整性

```
integrity_checker <path to manifest file> --crl /var/opt/kaspersky/kesl/private/data/KDSCRL/ --signature-type kds-with-filename
```

檢查 Kaspersky Endpoint Security MMC 管理外掛程式的完整性

```
integrity_checker.exe [<path to manifest file>]
```

檢查網路代理的完整性

```
integrity_checker <path to manifest file>
```

預設路徑用於位於與完整性檢查器實用程式相同目錄中的清單檔案。

您可以使用下列選用設定執行實用程式：

- `--crl <directory>` 是包含憑證撤銷清單的目錄路徑。
- `--verbose` — 顯示關於已執行操作及其結果的詳細資訊。如果不指定此設定，則只會顯示錯誤、未通過檢查的物件和掃描統計摘要。
- `--trace <file name>` 會將掃描期間發生的事件以 DEBUG 記錄等級寫入指定檔案。
- `--signature-type kds` 是要驗證的簽章類型（檢查 Kaspersky Endpoint Security 管理 Web 外掛程式時需要此選項）。
- `--signature-type kds-with-filename` 是要驗證的簽章類型（檢查應用程式套件和圖形介面套件時需要此設定）。
- `--single_file <file name>` 僅檢查資訊清單中的指定檔案，並忽略資訊清單中的所有其他物件。
- `--version` – 顯示實用程式的版本，但不執行完整性檢查。

檢視完整性檢查工具的所有可用選項

```
integrity_checker --help
```

清單檔案檢查結果顯示如下：

- `SUCCEEDED` — 已確認檔案的完整性（返回代碼 0）。
- `FAILED` — 尚未確認檔案的完整性（返回代碼不為 0）。

如果在應用程式啟動時偵測到違反應用程式或網路代理的完整性，Kaspersky Endpoint Security 會在事件記錄和卡巴斯基安全管理中心中產生相應的事件。

應用程式存取控制

Kaspersky Endpoint Security 中的存取控制以 Role Based Access Control (RBAC) 政策為基礎。若要授予使用者特定權限或資源存取權，您需要指派對應的角色。*角色*是用於管理應用程式的一組權利和特權。

使用者角色可讓日常存取權限管理變得更輕鬆、更快速。角色的存取權限會依據使用者的典型工作和職務說明進行設定。

應用程式需要作業系統中的提升權限才能保護裝置。應用程式需要 root 權限才能執行其部分基本安全功能。

應用程式的角色型存取模型包含 管理員 (admin) 角色。在某些情況下，具有管理員角色的使用者所執行的動作，可能會導致以作業系統超級使用者 (root) 的權限執行操作。

管理員角色應僅授予受信任的使用者。此管理員角色遭到入侵或濫用會導致整個裝置遭到入侵，並可能影響您組織基礎架構以及使用者資料的安全性、完整性或效能。

授予管理員角色是系統擁有者的責任，並應依照您組織的存取控制政策以及對相關使用者的信任程度來執行。

預先定義的角色

使用者可以根據其角色透過指令列存取Kaspersky Endpoint Security 功能。*角色*是用於管理應用程式的一組權利和特權。

在作業系統中建立四個系統使用者群組：

- kesladmin
- kesluser
- keslaudit
- nokesl

當您將應用程式角色指派給系統使用者時，該使用者會新增至對應的群組（請參閱下表）。當您撤銷使用者的角色時，該使用者會從對應的群組中移除。

指派或撤銷角色後，您必須重新啟動應用程式（kesl 處理程序）及其圖形介面（kesl-gui 處理程序）。

角色和使用者群組

角色名稱	應用程式中的角色	作業系統使用者群組	權限
管理員	admin	kesladmin	無需使用 sudo 命令即可在應用程式的圖形介面和命令列中管理應用程式設定和工作設定。 管理應用程式授權。 為使用者指派角色。 撤銷使用者的角色（管理員無法撤銷自己的 admin 角色）。 檢視和管理使用者的儲存。
使用者	user	kesluser	僅管理使用者檔案掃描工作。 啟動和停止更新工作。 將檔案傳送至沙盒進行掃描 檢視此使用者建立的工作的報告。 檢視對於所有應用程式使用者常見的特定事件。
稽核員	audit	keslaudit	檢視應用程式設定 檢視應用程式狀態。 檢視所有工作、其設定和啟動排程。 檢視所有事件。 檢視備份中的所有物件。
–	–	nokesl	應用程式中未分配任何角色，沒有權限。

如何指派或撤銷使用者角色

角色會定義使用者的權限，以及使用者可在系統中執行的動作。只有具有管理員 (kesladmin) 角色的使用者才能管理角色。建議在受保護裝置上至少建立一位具有管理員角色的使用者，以避免應用程式由具有 root 權限的使用者管理。

檢視使用者和角色清單

```
kesl-control --get-user-list
```

為使用者指派角色

```
kesl-control --grant-role <admin|user|audit> <user name>
```

為使用者 `test15` 指派 `audit` 角色的範例

```
kesl-control --grant-role audit test15
```

撤銷使用者的角色

```
kesl-control --revoke-role <role> <user name>
```

撤銷使用者 `test15` 的 `audit` 角色的範例

```
kesl-control --revoke-role audit test15
```

卡巴斯基安全管理中心中的 RBAC 功能區域

預設情況下，卡巴斯基安全管理中心管理系統中具有「Kaspersky Endpoint Security 管理員」角色的使用者可存取 Kaspersky Endpoint Security 的所有功能。

您可以為 Kaspersky Endpoint Security 使用者或群組選取以下預先定義的 Kaspersky Endpoint Security 功能存取等級之一：

- **讀取** 授予檢視 Kaspersky Endpoint Security 一般設定和 Kaspersky Endpoint Security 元件設定的能力。
- **編輯** 授予檢視和編輯 Kaspersky Endpoint Security 一般設定和 Kaspersky Endpoint Security 元件設定的能力。
- **執行** 授予啟動和停止 Kaspersky Endpoint Security 工作的能力。
- **對裝置選取項目執行操作** 授予針對裝置選取項目啟動和停止 Kaspersky Endpoint Security 工作的能力。

您也可以設定進階存取權限：允許或拒絕存取 Kaspersky Endpoint Security 功能。

如何在網頁主控台中設定應用程式功能的存取權限

1. 在網頁主控台的主視窗中，選擇**使用者和角色 → 角色**。
2. 選取要為其設定功能區域的角色。
   如有必要，您可以新增角色。請參閱 卡巴斯基安全管理中心說明 瞭解更多詳情。
3. 設定 Kaspersky Endpoint Security 應用程式的存取權限。
4. 點擊"**儲存**"按鈕。

Kaspersky Endpoint Security 功能的存取權限

功能區域	Kaspersky Endpoint Security 功能
基本功能	更新應用程式資料庫和模組 回溯 清查 BadUSB 攻擊防護 系統完整性監控 系統完整性檢查 偵測設定 卡巴斯基安全網路 使用者互動 效能 網路設定 容器掃描 技術支援 報告和儲存 與 KSC 整合 遙測來源和 auditd 模式（作業系統互動設定） 事件設定 Light Agent 模式 新增金鑰
應用程式控制	應用程式控制
裝置控制	裝置控制
資料加密	授予裝置暫時存取權（裝置控制）
信任區域	信任區域： • 指定受信任的網址 • 受信任 IP 位址 • 監控的連接埠 • 受信任的根憑證 • 受信任網域 • 受信任掛接點 • 流量攔截排除項目 • 受信任應用程式 • 惡意軟體掃描排除項目 • 受信任裝置

功能區域	Kaspersky Endpoint Security 功能
Detection and Response	內建代理程式： • Managed Detection and Response • Endpoint Detection and Response • Endpoint Detection and Response Expert (on-premises) • Endpoint Detection and Response Expert (cloud) • Network Detection and Response (KATA) • Sandbox • 與 KUMA 整合。 回應動作： • 終止處理程序 • 啟動處理程序 • IOC 掃描 • 從裝置接收檔案 • 移動檔案到隔離 • 從裝置中刪除檔案 • 網路隔離 • 物件的執行防禦 • 遙測設定
主機入侵防禦	行為偵測 弱點利用防禦 Anti-Cryptor 網路威脅防護 防火牆管理
防護元件	惡意軟體掃描 關鍵區域掃描 檔案威脅防護 郵件威脅防護 卸除式磁碟機掃描 Web 威脅防護
Web 控制	Web 控制

受防護裝置典型角色的建議

工作站

如果您要在工作站上安裝應用程式，建議也安裝應用程式的圖形介面。

安裝應用程式後：

- 啟用 Web 威脅防護。
- 如果裝置沒有直接連線至網際網路，請使用下列其中一個選項，在網路流量掃描設定中選取本機憑證驗證：
  - 在網頁主控台中，在 **加密連線掃描** 下，按一下 **設定** 按鈕，然後將 **憑證驗證政策** 設定為 **本機檢查**。
  - 在管理主控台中，在 **加密連線設定** 下，將 **憑證驗證政策** 設定為 **本機檢查**。
  - 在裝置本機使用命令列：

    ```
    kesl-control --set-net-settings CertificateVerificationPolicy=LocalCheck
    ```

  應用程式不會使用網際網路來驗證憑證。
- 針對使用 Samba 和 NFS 通訊協定掛載在裝置上的所有遠端目錄，設定 檔案操作攔截排除（全域排除）。

檔案伺服器

安裝應用程式後：

1. 請確定 檔案威脅防護 設定中已停用壓縮檔掃描。預設情況下已勾選此選項。
2. 建立具有下列設定的 *惡意軟體掃描* 工作：
   - 壓縮檔掃描：已啟用
   - 工作排程：在最低負載時段

Web 伺服器

Kaspersky Endpoint Security 不適用於 Web 伺服器防護。若要保護 Web 伺服器，建議使用 Kaspersky NGFW 和 Kaspersky Web Traffic Security 。

如果您在 Web 伺服器上使用 Kaspersky Endpoint Security，且該伺服器使用 HTTPS 通訊協定並具有高用戶端負載，Web 威脅防護 可能會大幅提高系統資源使用率。這是由於應用程式解密和 HTTPS 流量掃描造成的。

請分析在 Web 威脅防護運作時，Web 伺服器負載的變化。您可以設定排除以最佳化設定並消除相容性問題。

代理伺服器

安裝應用程式後，請在作為代理伺服器或負載平衡器的裝置上停用 Web 威脅防護 和 網路威脅防護 元件。

容器化伺服器

安裝應用程式後，請在用於容器化服務的伺服器上停用 Web 威脅防護、網路威脅防護 和 防火牆管理 元件。若要保護容器環境，可以使用 Kaspersky Container Security 應用程式。

資料庫伺服器

為資料庫管理系統的工作目錄設定全域排除。

請向您的 DBMS 管理員確認基礎架構中的工作目錄清單。

以下範例路徑適用於 Ubuntu 作業系統。在其他作業系統中，目錄可能有所不同。

常用 DBMS 的建議

PostgreSQL。完全消除資料檔案和預寫式記錄 (WAL 檔案) 的檔案作業延遲至關重要。我們也建議排除 PostgreSQL 處理程序和資料表空間的檔案作業（請參閱以下範例）。在典型的 PostgreSQL 安裝中，這些檔案位於以下目錄：

- 統計資訊和並行查詢：`/dev/shm`
- 資料：`/var/lib/postgresql/<PostgreSQL version>/main`
- WAL 檔案：`/var/lib/postgresql/<PostgreSQL version>/main/pg_wal`
- 可執行檔：`/usr/lib/postgresql/<PostgreSQL version>/bin/`。

Postgres Pro。請遵循 PostgreSQL 的指導方針。此外，請將 `/var/lib/pgpro/<Postgres Pro version>/data` 目錄新增至排除項目。

Oracle Database。您可以從 `/etc/oratab` 設定檔取得所有資料庫的工作目錄清單。

ScyllaDB。使用 Web 威脅防護和網路威脅防護元件時，請使用流量攔截的 eBPF 模式。若要管理 Detection and Response 解決方案的快取模式，請使用 kesl.ini 設定檔中 `UseIncreasedXdrEventsCache=yes` 設定的預設值。

設定 PostgreSQL 工作目錄全域排除的範例

如果您使用以*fanotify 技術*為基礎的機制來攔截系統事件，DBMS 檔案目錄必須是掛載點。如果您使用*可更新的內核模組*來攔截系統事件，則不需要建立掛載點。

若要建立掛載點：

1. 檢查包含資料庫檔案的目錄是否為掛載點：

   ```
   mount
   ```

   如果這些目錄未出現在 mount 指令的輸出中：

   a. 建立掛載點：

   ```
   mount --bind /var/lib/postgresql/<PostgreSQL version>/main/ /var/lib/postgresql/<PostgreSQL version>/main
   ```

   不需要為 WAL 檔案所在的目錄建立單獨的掛載點，因為該目錄巢狀在資料目錄內。

   b. 將以下行新增至 /etc/fstab 檔案，使新建立的掛載點在系統重新啟動後持續存在：

   ```
   /var/lib/postgresql/<PostgreSQL version>/main /var/lib/postgresql/<PostgreSQL version>/main none
   defaults,bind 0 0
   ```

2. 重新啟動 PostgreSQL 服務：

   ```
   systemctl restart postgresql
   ```

若要設定工作目錄的全域排除：

1. 將目錄新增至全域排除：

   ```
   kesl-control --set-app-settings ExcludedMountPoint.item_0000=/var/lib/postgresql/<PostgreSQL version>/main
   kesl-control --set-app-settings ExcludedMountPoint.item_0001=/var/lib/postgresql/<PostgreSQL
   version>/main/pg_wal
   kesl-control --set-app-settings ExcludedMountPoint.item_0002=/usr/lib/postgresql/<PostgreSQL version>/bin/
   kesl-control --set-app-settings ExcludedMountPoint.item_0003=/usr/lib/postgresql/<PostgreSQL version>
   ```

2. 如果使用表空間，也請將其新增至排除：

   ```
   kesl-control --set-app-settings ExcludedMountPoint.item_0000=<tablespace directory>
   ```

3. 重新啟動應用程式以套用全域排除：

```
systemctl restart kesl
```

更新應用程式資料庫和模組

更新 Kaspersky Endpoint Security 的資料庫和應用程式模組，可確保您的裝置獲得最新防護。新病毒和其他類型的惡意程式每天都在全世界出現。Kaspersky Endpoint Security 資料庫包含關於威脅的資訊和解毒的方法。為了快速偵測威脅，建議您定期更新應用程式資料庫和模組。

定期資料庫更新需要啟動的應用程式產品授權。如果沒有啟動的產品授權，您將只能執行一次更新。

如果 應用程式部署 成功，且您在初始設定階段選擇更新資料庫，則安裝應用程式後，資料庫即為最新狀態。您可以在卡巴斯基安全管理中心檢視裝置的防護狀態時，透過查看用戶端裝置的狀態取得資料庫狀態資訊；也可以在命令列使用 `kesl-control --app-info` 命令取得該資訊。如果資料庫不是最新狀態，您需要設定並啟動資料庫更新。

正在配置資料庫和模組更新

1. **選擇更新散佈方案和更新來源**

   *更新來源*是包含 Kaspersky Endpoint Security 資料庫和應用程式模組更新的資源。更新來源可以是以下其中一項：卡巴斯基更新伺服器；卡巴斯基安全管理中心管理伺服器儲存區；FTP、HTTP 或 HTTPS 伺服器；由使用者使用 Samba 或 NFS 通訊協定掛載的本機或網路目錄。

   如果 Kaspersky Endpoint Security 以 Light Agent 模式 使用，受防護的虛擬機上的資料庫會從 SVM 上的目錄更新。

2. **設定資料庫更新工作**

   更新 工作會下載更新套件，並在裝置上安裝資料庫和應用程式模組更新。

應用程式可能無法在美國境內提供更新功能（包括病毒防護簽章更新和程式碼庫更新）。

更新期間，將下載以下物件並安裝到您的裝置上：

- Kaspersky Endpoint Security 資料庫。應用程式資料庫包含惡意軟體偵測規則、網路攻擊描述、惡意和釣魚網址資料庫、橫幅廣告資料庫、垃圾郵件資料庫及其他資料。
- 程式模組。模組更新旨在消除應用程式中的弱點並改進防護裝置的方法。模組更新可能變更應用程式元件的行為和新增新功能。

您也可以接收自動安裝的應用程式更新（自動修補程式）。自動修補程式包含應用程式的修正和改善項目。

更新時，系統會將您電腦上的應用程式模組和資料庫，與 更新來源 中的最新版本進行比較。如果您目前的資料庫和應用程式模組與其各自的最新版本不同，則更新的缺失部分將安裝在您的裝置上。

如果資料庫過期，更新量可能會很大，這可能會花費更多的網際網路流量（最多達幾十 MB）。磁碟空間量最多可達 3 GB。

實用文章

應用程式資料庫和模組更新疑難排解

如果收到以下狀態，該怎麼辦：「已安裝應用程式更新或 cryptossl 模組更新。重新啟動應用程式。」

如何選擇更新來源和散佈方案

選擇 Kaspersky Endpoint Security 更新來源

*更新來源*是包含 Kaspersky Endpoint Security 資料庫和應用程式模組更新的資源。

更新來源可以是以下其中一項：卡巴斯基更新伺服器、卡巴斯基安全管理中心管理伺服器的儲存區、使用者掛載的本機或網路 (SMB/NFS) 目錄、FTP、HTTP 或 HTTPS 伺服器。選擇您自己的 HTTPS 伺服器作為更新來源時，您需要確保其具有正確的憑證鏈。自我簽署憑證只能作為憑證鏈中的根憑證使用。在此情況下，您需要將其新增至裝置上的受信任憑證清單。

如果 Kaspersky Endpoint Security 以 Light Agent 模式 使用，受防護的虛擬機上的資料庫會從 SVM 上的目錄更新。

如果選取多個資源作為更新來源，Kaspersky Endpoint Security 會從清單頂端開始逐一嘗試連線到這些來源，並透過從第一個可用來源擷取更新套件來執行更新工作。嘗試連線到所選更新來源時，您可以設定其回應逾時。如果更新來源在指定時間內沒有回應，應用程式將聯絡清單中的下一個更新來源。

選擇更新分發方案

Kaspersky Endpoint Security 支援下列資料庫和應用程式模組更新分發方案：

集中更新

如果您使用卡巴斯基安全管理中心集中管理組織中的裝置防護，建議您設定集中式資料庫更新。集中更新可減少外部網際網路流量，並提供方便的更新監控。

集中更新套件括以下步驟：

1. 將更新套件下載到組織網路內的儲存區。

   您可以使用卡巴斯基安全管理中心管理伺服器的儲存庫作為儲存庫。更新套件會透過管理伺服器的 *下載更新至管理伺服器儲存區* 工作下載至管理伺服器儲存區。

2. 將更新套件分發到用戶端裝置

   更新套件透過 Kaspersky Endpoint Security 的*更新*工作分發到用戶端裝置。在工作設定中，選擇卡巴斯基安全管理中心作為更新來源。

從卡巴斯基更新伺服器更新

卡巴斯基更新伺服器位於世界各地不同的國家，從而確保更新的高可靠性。如果無法從一台伺服器執行更新，則應用程式將切換到下一台伺服器。更新透過 HTTPS 協定下載。有關卡巴斯基更新伺服器的更多資訊，請參閱技術支援知識庫。

從使用者掛載的本機或網路目錄 (SMB/NFS)，或從 FTP、HTTP 或 HTTPS 伺服器進行更新

自訂更新來源必須包含預先下載的更新套件（例如，您可以使用 卡巴斯基更新公用程式 來完成）。選擇您自己的 HTTPS 伺服器作為更新來源時，您需要確保其具有正確的憑證鏈。自我簽署憑證只能作為憑證鏈中的根憑證使用。在此情況下，您需要將其新增至裝置上的受信任憑證清單。您可以在*更新*工作設定中指定自訂更新來源。如需有關建立自訂更新來源的詳細資訊，請參閱 卡巴斯基安全管理中心說明。

更新透過標準網路協定從卡巴斯基更新伺服器或其他 FTP、HTTP 或 HTTPS 伺服器下載。預設情況下，網際網路連線設定自動確定。如果您使用代理伺服器，請指定代理伺服器設定。

如何設定資料庫更新工作

更新 工作會下載更新套件，並在裝置上安裝資料庫和應用程式模組更新。

在卡巴斯基安全管理中心中更新資料庫

在卡巴斯基安全管理中心中，*更新*工作由管理伺服器快速啟動精靈自動建立。若要在執行精靈時建立*更新*工作，您需要安裝 Kaspersky Endpoint Security 管理外掛程式。

您可以使用自動建立的 *更新*群組工作，或使用網頁主控台或管理主控台建立並執行自訂群組更新工作和本機更新工作。

> 如果 Kaspersky Endpoint Security 是在 Light Agent 模式下使用，則受防護的虛擬機上的資料庫會使用特殊的 *更新*本機工作進行更新，其中 SVM 上的目錄指定為更新來源。更新工作自動開始。您不能刪除此工作或變更其設定。不支援使用在卡巴斯基安全管理中心建立的工作更新資料庫和應用程式模組。

如何在網頁主控台中設定並執行更新工作

1. 在網頁主控台的主視窗中，選擇**工作**。

   工作清單開啟。

2. 在工作清單中，選擇 Kaspersky Endpoint Security 更新工作，然後按一下該工作的名稱。

   工作內容視窗將開啟。

3. 選擇“**應用程式設定**”標籤。

4. 在 **更新來源** 區段中，根據所使用的更新方案，選擇應用程式將從中接收資料庫和模組更新的來源。

   更新來源清單包含兩個來源：卡巴斯基更新伺服器和卡巴斯基安全管理中心。**狀態**列指示應用程式在執行工作時是否正在使用此更新來源。您可以按一下**新增**按鈕將其他更新來源新增至清單。您可以指定 FTP、HTTP 和 HTTPS 伺服器上的目錄，或掛載在受防護用戶端裝置上的任何裝置中的目錄，包括透過 Samba 或 NFS 協定掛載的遠端裝置中的目錄，作為更新來源。如果無法從更新來源執行更新，Kaspersky Endpoint Security 將切換到下一個更新來源。應用程式會依照表中出現的順序存取更新來源。

5. 在工作內容視窗中，選取 **排程** 索引標籤，並設定執行更新工作的排程。預設會為工作選擇手動啟動模式。

   如果您已選擇**卡巴斯基安全管理中心**作為更新來源，請從**啟動工作**下拉清單中選擇**當下載更新至儲存庫時**。如需有關排程工作的詳細資訊，請參閱卡巴斯基安全管理中心說明。

6. 儲存變更。

工作將根據配置的排程啟動。您也可以手動執行工作。

如何在管理主控台中設定並執行更新工作

1. 在管理主控台中，執行下列其中一項操作：

   - 若要編輯在指定管理群組中包含的裝置上執行的工作的設定，請在主控台樹狀圖中選擇此管理群組，然後在工作區中選擇**工作**索引標籤。

   - 若要編輯在一台或多台裝置上執行的工作（一組裝置的工作）的設定，請選擇主控台樹中的**工作**資料夾。

2. 在工作清單中，選擇更新工作，然後按兩下該工作以開啟工作內容視窗。

3. 在工作屬性視窗中，選擇左側清單中的**更新來源**部分。

4. 根據所使用的更新方案，在表中選擇應用程式將從其接收資料庫和模組更新的更新來源。

   更新來源清單包含兩個來源：卡巴斯基更新伺服器和卡巴斯基安全管理中心。**狀態**列指示應用程式在執行工作時是否正在使用此更新來源。您可以按一下**新增**按鈕將其他更新來源新增至清單。您可以指定 FTP、HTTP 或 HTTPS 伺服器作為更新來源。如果無法從更新來源執行更新，Kaspersky Endpoint Security 將切換到下一個更新來源。應用程式會依照表中出現的順序存取更新來源。

5. 選擇**設定**部分並配置其他更新設定。

6. 選擇**排程**索引標籤並配置用於執行更新工作的排程。預設會為工作選擇手動啟動模式。

   如果您已選擇**卡巴斯基安全管理中心**作為更新來源，請從**排程的啟動**下拉清單中選擇**當下載更新至儲存庫時**。如需有關排程工作的詳細資訊，請參閱卡巴斯基安全管理中心說明。

7. 在**屬性：<工作名稱>**視窗中點擊**套用**或**確定**儲存所做的變更。

工作將根據配置的排程啟動。您也可以手動執行工作。

透過命令列更新資料庫

在命令列中，您可以使用 *Update* 預定義工作，或建立 Update 類型的 使用者工作，來更新資料庫和應用程式模組。

您可以透過變更工作設定來管理手動更新工作（啟動、停止、暫停和繼續）、設定工作排程，以及管理更新設定。

如何在命令列中建立並設定更新工作

在命令列中，您可以透過兩種方式建立並設定自訂更新工作：

- 透過在設定檔中指定工作的所有設定來建立工作。
- 建立含預設設定的工作，然後設定其設定。

使用取自設定檔的設定建立更新工作

```
kesl-control --create-task <task name> --type <task type> --file <path to file> [--json]
```

其中：

- `<path to file>` 是包含您要用於該工作之設定的設定檔完整路徑。
- 指定 `--json` 可從 JSON 格式的設定檔匯入設定。如果未指定 `--json` 選項，應用程式將嘗試從 INI 檔案匯入。如果匯入失敗，則會顯示錯誤。

設定檔範例

```
ConnectionTimeout=10
ApplicationUpdateMode=DownloadOnly
[Sources.item_0000]
Enabled=Yes
SourceType=Custom
URL=https://s00.upd.kaspersky.com
```

若要建立並設定具有預設設定的更新工作：

1. 執行以下指令建立工作：

   ```
   kesl-control --create-task <更新工作名稱> --type Update
   ```

   其中，`<update task name>` 是您要為新更新工作設定的名稱。

   此指令會建立具有預設設定的更新工作。

2. 如有需要，請執行以下指令管理更新工作設定：

   ```
   kesl-control --set-settings <update task ID|name> <setting name>=<setting value> [<setting name>=<setting value>]
   ```

3. 如有需要，請執行以下指令管理更新工作排程設定：

   ```
   kesl-control --set-schedule <update task ID|name> <setting name>=<setting value> [<setting name>=<setting value>]
   ```

4. 執行以下指令檢查工作設定的目前值：

   ```
   kesl-control --get-settings <update task ID|name>
   ```

在應用程式圖形介面中更新資料庫

如何在圖形介面中啟動或停止更新工作

1. 開啟應用程式圖形介面的主視窗。
2. 在主應用程式視窗中，點擊**更新**。
   將開啟**更新**視窗。
3. 執行下列操作之一：
   - 若要啟動一項工作，請點擊要啟動的工作下方的**啟動**按鈕。
     顯示正在執行的更新工作的進度。
   - 若要停止工作，請點擊要停止的掃描工作下的**停止**按鈕。
     更新工作停止。
4. 若要檢視工作報告，請點擊**顯示報告**按鈕。

如何使用 Kaspersky Update Utility 進行更新

為了減少網路流量，您可以使用 Kaspersky Update Utility 從共用目錄配置組織 LAN 裝置上的應用程式資料庫和模組的更新。為此，組織 LAN 中的一台裝置必須從卡巴斯基安全管理中心伺服器或卡巴斯基更新伺服器接收更新套件，並使用該實用程式將收到的更新套件複製到共用目錄。組織區域網路上的其他裝置將能夠從該共用目錄接收更新套件。

若要設定卡巴斯基安全管理中心使用 Kaspersky Update Utility 從共用目錄更新資料庫：

1. 在組織 LAN 的其中一台裝置上安裝 Kaspersky Update Utility。
   您可以從卡巴斯基技術支援網站下載 Kaspersky Update Utility 分發套件。
2. 在 Kaspersky Update Utility 設定中配置將更新套件複製到共用目錄。
   選擇更新來源（例如，管理伺服器儲存區）以及 Kaspersky Update Utility 將複製更新套件的共用目錄。有關使用卡巴斯基更新實用程式的詳細資訊，請參閱 卡巴斯基知識庫。
3. 配置組織本機網路中其他裝置上指定共用目錄的應用程式資料庫和模組的更新：
   a. 使用網頁主控台或管理主控台開啟將在所需裝置上執行的 **更新** 工作的屬性。
   b. 在工作屬性中，轉到**更新來源**部分。
   c. 在**更新來源**部分，選擇**區域或全域網路上的其他來源**選項。
   d. 在更新來源表中，點擊**新增**按鈕並指定共用目錄的路徑。

      更新來源的位址必須與 Kaspersky Update Utility 設定中指定的位址相符。

   e. 選取**使用此來源**核取方塊並點擊**確定**。

f. 在表中，使用**向上**和**向下**按鈕設定更新來源的順序。

g. 儲存對工作設定的變更。

若要設定卡巴斯基安全管理中心使用指令列從共用目錄更新資料庫：

1. 在組織 LAN 的其中一台裝置上安裝 Kaspersky Update Utility。
   您可以從卡巴斯基技術支援網站下載 Kaspersky Update Utility 分發套件。

2. 在 Kaspersky Update Utility 設定中配置將更新套件複製到共用目錄。
   選擇更新來源（例如，管理伺服器儲存區）以及 Kaspersky Update Utility 將複製更新套件的共用目錄。有關使用卡巴斯基更新實用程式的詳細資訊，請參閱 卡巴斯基知識庫。

3. 設定從組織本機網路中其他裝置上的指定共用目錄更新應用程式資料庫和模組：在 `Update` 工作設定中設定 `SourceType=Custom`，並在 `[Sources.item_#]` 區段中指定共用目錄的路徑。

   更新來源的位址必須與 Kaspersky Update Utility 設定中指定的位址相符。

如何回溯應用程式資料庫和模組更新

在資料庫和應用程式模組第二次更新之後，即可使用將資料庫和應用程式模組回溯至先前版本的功能。

每次使用者開始更新程式時，Kaspersky Endpoint Security 會為目前資料庫和程式模組建立一個備份副本。讓您能夠在必要時將資料庫和程式模組回溯至它們的前一版本。回溯至前一更新這個功能十分有用，例如，如果新資料庫版本引起誤報，導致 Kaspersky Endpoint Security 封鎖某個安全的應用程式，回溯操作就會十分有用。

如果 Kaspersky Endpoint Security 是以Light Agent 模式使用，則無法使用該工作來回溯資料庫更新。

在卡巴斯基安全管理中心中，您可以使用網頁主控台或管理主控台，為管理群組或個別裝置建立回溯工作。

在指令列中，您可以透過下列方式回溯資料庫更新：

- 執行*回溯*預定義工作。
- 建立並執行*回溯*自訂工作。

*回溯*工作沒有任何設定。

如何在網頁主控台中回溯應用程式資料庫和模組更新

1. 在網頁主控台的主視窗中，選擇**工作**。
   工作清單開啟。

2. 點擊“**新增**”。
   啟動“工作精靈”。

3. 配置工作設定：

   a. 在**應用程式**下拉式清單中，選取應用程式名稱。

   b. 在“**工作類型**”下拉式清單中，選取“**回溯**”。

   c. 在**工作名稱**欄位中，輸入新工作的名稱。

   d. 在**要將工作指派給的裝置**下，選擇您要如何定義工作範圍。

4. 根據您偏好的工作範圍定義方法選取裝置。

5. 完成精靈。

   在工作清單中將顯示一個新工作。

6. 選中工作旁邊的核取方塊，然後點擊“**開始**”按鈕。

如何在管理主控台中回溯應用程式資料庫和模組更新

1. 在管理主控台中，執行下列其中一項操作：

   - 若要建立將在所選管理群組中包含的裝置上執行的工作，請在**受管理裝置**資料夾中的主控台樹中選擇此管理群組，然後在工作區中選擇**工作**索引標籤並點擊**新工作**按鈕。

     新工作精靈將為選定管理群組的裝置啟動。

   - 若要建立將在一個或多個裝置上執行的工作（一組裝置的工作），請選擇主控台樹狀圖中的**工作**資料夾，然後點擊工作區中的**新工作**按鈕。

     新工作精靈為該組裝置啟動。

2. 在精靈的第一步中，於清單中選取 Kaspersky Endpoint Security 和 **回溯** 工作類型。

3. 如果您要為一組裝置建立工作，精靈會提示您選取要指派該工作的裝置。選擇您要如何定義工作範圍。

4. 根據您偏好的工作範圍定義方法選取裝置。

5. 設定工作的排程。

6. 輸入新工作的名稱。

7. 完成精靈。

   在工作清單中將顯示一個新工作。

8. 在工作清單中，選取該工作，開啟該工作的內容功能表，然後選取**啟動**。

如何在指令列中回溯應用程式資料庫和模組更新

執行命令：

回溯資料庫和模組更新

```
kesl-control --start-task 7
```

如何在圖形介面中回溯應用程式資料庫和模組更新

1. 開啟應用程式圖形介面的主視窗。
2. 在主應用程式視窗中，點擊**更新**。
   將開啟**更新**視窗。
3. 點擊**回溯更新**連結，以回溯資料庫更新。

主機威脅防護

檔案威脅防護

檔案威脅防護會為電腦提供最低限度的安全防護。該元件會與 Kaspersky Endpoint Security 一起啟動，並即時掃描檔案。

檔案威脅防護的運作方式

1. **應用程式會攔截檔案操作事件，並封鎖動作直到掃描完成。**

   應用程式會使用檔案操作攔截機制，並在掃描完成之前封鎖對該檔案的所有存取。

2. **應用程式會掃描檔案**

   檔案威脅防護會使用以下技術掃描檔案：

   - 病毒資料庫。
   - 卡巴斯基安全網路的雲端服務。
   - 啟發式分析技術可偵測卡巴斯基資料庫尚未涵蓋的威脅。

3. **掃描完成**

   掃描後，應用程式會允許該操作，或封鎖該操作並執行威脅偵測時指定的動作。

檔案威脅防護的初始設定

初始設定包括基本端點防護所需的步驟。

1. **選擇系統事件攔截機制**

   檔案威脅防護會攔截檔案操作事件，並封鎖動作直到掃描完成。

安裝應用程式時，您選擇了系統事件攔截機制：

- 基於可更新的內核模組的攔截機制
- 以 fanotify 為基礎的系統攔截機制
- 適用於沒有 fanotify 的作業系統的檔案威脅防護核心模組

系統事件攔截機制的選擇取決於電腦的組態。可提供最佳效能的攔截技術是可更新的內核模組。您可以在應用程式設定中啟用此機制。

2. **設定檔案威脅防護**

   預設情況下，檔案威脅防護已啟用，並依照卡巴斯基專家建議的設定執行。預設設定提供建議的防護等級和最佳資源使用。如果您對基礎架構安全性有特殊要求，您可以變更這些設定。

3. **設定防護範圍**

   預設情況下，應用程式會掃描受防護裝置上的所有檔案。如果您只需要掃描個別目錄（例如，檔案會從外部來源自動下載到其中的目錄），您可以僅將該目錄指定為防護範圍。在其他情況下，我們建議保留預設防護範圍，並使用排除項目來微調範圍。

4. **從掃描中排除掛載點**

   從掃描中排除掛載點可讓您避免攔截特定目錄中的檔案操作。例如，您可以從掃描中排除共用網路資源，並使用 Kaspersky Endpoint Security 在實際儲存這些資源的裝置上加以保護。您也可以參閱檔案威脅防護和掃描任務建議。

5. **新增排除項目**

   排除項目有助於平衡系統安全性與效能。為確保第三方軟體穩定運作，請將相應軟體說明文件中列出的檔案和目錄新增至排除項目。

   我們建議排除以下物件：

   - 資料庫。掃描大型資料庫需要大量資源。頻繁存取資料庫檔案會觸發頻繁掃描。
   - 資源密集型處理程序所使用的檔案。掃描此類檔案會降低電腦速度。
   - 包含記錄檔的目錄。作業系統會持續寫入記錄檔。因此，檔案威脅防護會浪費電腦資源掃描記錄檔。

> 如果某個物件已由檔案威脅防護元件排除在掃描範圍之外，我們建議使用*惡意軟體掃描*工作掃描此類物件。

高負載伺服器的額外設定

額外設定包括微調檔案威脅防護的步驟。完成初始設定後，如果遇到任何延遲，或是正在設定高負載伺服器，請執行以下步驟：

1. **停用掃描期間的檔案存取封鎖**

   預設情況下，檔案威脅防護會封鎖對正在掃描之檔案的所有存取，直到掃描完成。如果停用封鎖模式，檔案威脅防護會以通知模式運作。此檔案操作攔截模式在掃描期間對系統效能的影響較小，但檔案中的威脅可能無法被解毒或刪除。

   > 如果停用封鎖模式，裝置控制、物件執行防禦動作和卸除式磁碟機掃描工作也會以通知模式運作。

2. **收集檔案掃描統計資料**

   監控電腦的主要效能指標：CPU 負載、第三方軟體效能或其他指標。這將協助您確定如何降低系統負載。

   您可以使用應用程式效能分析工具取得檔案掃描統計資料。您也可以使用自己的監控工具。

3. **最佳化應用程式效能**

   分析收集到的資訊後，最佳化應用程式效能：

   - 新增全域排除項目
   - 新增排除項目
   - 最佳化應用程式設定

4. **啟用掃描期間的檔案存取封鎖**

   啟用掃描期間的檔案存取封鎖。偵測到受感染物件時，應用程式將執行所選動作。

特殊考量與限制

- 如果 root 使用者無法存取透過 NFS4 協定掛載到裝置上的遠端目錄中的檔案，應用程式會封鎖所有使用者對此類檔案的存取。
- 如果檔案威脅防護和容器監控均已啟用，應用程式也會掃描所有命名空間和容器。

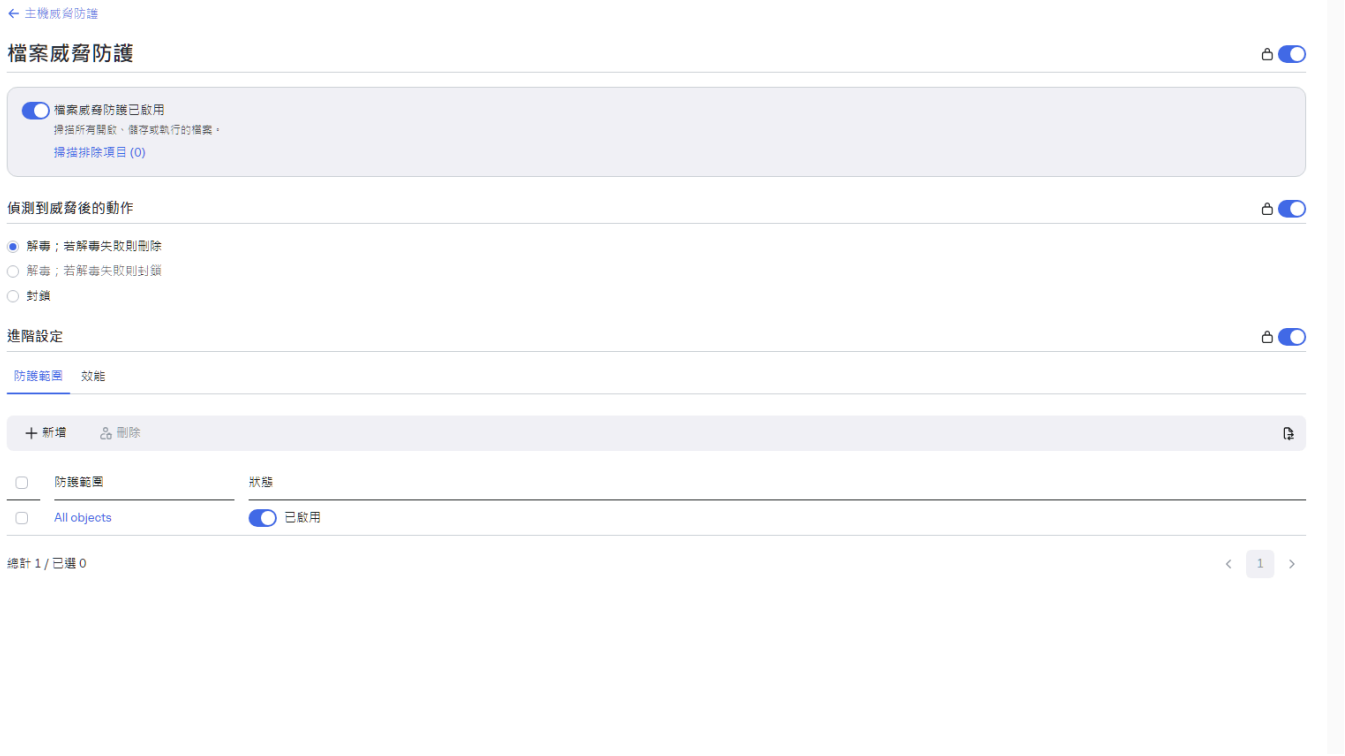
如何建立防護範圍

*防護範圍*是 Kaspersky Endpoint Security 掃描是否存在威脅的物件路徑清單。預設情況下，應用程式會掃描受防護裝置上的所有檔案。如果您只需要掃描個別目錄（例如，自動從外部來源下載檔案的目錄），則可以將此目錄指定為防護範圍。在其他情況下，我們建議保留預設防護範圍，並使用排除項目來微調範圍。

Kaspersky Endpoint Security 會依照物件在物件清單中出現的順序掃描物件。如果有必要，將子目錄放在清單中高於其父目錄的位置，以便為子目錄配置與父目錄的安全性設定不同的安全性設定。

如何在網頁主控台中建立防護範圍

1. 在網頁主控台的主視窗中，選擇**資產管理 → 政策**。
2. 點擊 Kaspersky Endpoint Security 政策的名稱。
   政策內容視窗將開啟。
3. 選擇“**應用程式設定**”標籤。
4. 轉到 **主機威脅防護 → 檔案威脅防護**。
5. 在“**防護範圍**”塊中， 點擊“**新增**”。
6. 這會開啟一個視窗；在該視窗中，選取檔案系統類型：
   - **本機**不需網路連線即可存取的硬碟目錄。
   - **已掛接**已掛載的遠端或本機目錄。
   - **已共用**可透過 Samba (SMB) 或 NFS 通訊協定存取的電腦目錄。
   - **所有遠端掛接**使用 Samba 和 NFS 協定掛載在裝置上的所有遠端目錄。
   - **所有共用**透過 Samba 和 NFS 通訊協定存取的所有電腦目錄。
7. 對於本機檔案系統，請指定目錄路徑（例如，`/path/to/folder`）。如有必要，選中“**包含子資料夾**”核取方塊。
8. 指定已掛載或共用檔案系統的存取協定。
9. 指定物件副檔名的遮罩（例如，`*.txt`）。使用逗號分隔遮罩。
10. 要將此政策套用到電腦，請關閉... 掛鎖圖示並儲存變更。



如何在命令列建立防護範圍

1. 執行以下指令：

```
kesl-control --set-settings 1 --add-path <path>
```

   新的`[ScanScope.item_#]`部分將被新增至工作設定中。應用程式掃描`Path`設定所指定的目錄中的物件。

2. 若要檢查元件設定的目前值，請執行以下命令：

```
kesl-control --get-settings 1
```

範例

```
kesl-control --set-settings 1 ScanScope.item_0001.UseScanArea=Yes ScanScope.item_0001.Path=/home
```

以下防護範圍設定會新增至工作：

```
[ScanScope.item_0001]
AreaDesc=All object
UseScanArea=Yes
Path=/home
AreaMask.item_0000=*
```

如何選擇偵測到檔案威脅時的動作

一旦偵測到惡意軟體，Kaspersky Endpoint Security 可能會刪除受感染的檔案並終止從該檔案啟動的惡意軟體處理程序。在檔案威脅防護設定中，您可以選取 Kaspersky Endpoint Security 在偵測到威脅時執行的動作。

如何在網頁主控台中設定偵測到威脅後的動作

1. 在網頁主控台的主視窗中，選擇**資產管理 → 政策**。

2. 點擊 Kaspersky Endpoint Security 政策的名稱。
   政策內容視窗將開啟。

3. 選擇“**應用程式設定**”標籤。

4. 轉到 **主機威脅防護 → 檔案威脅防護**。

5. 在 **偵測到威脅後的動作** 下，選擇偵測到威脅時應用程式將執行的動作：

   - **解毒；若解毒失敗則刪除**（預設）。如果選取該選項，應用程式將自動對偵測到的受感染檔案執行解毒操作。如果解毒失敗，應用程式將刪除檔案。

   - **解毒；若解毒失敗則封鎖**如果選取該選項，應用程式將自動對偵測到的受感染檔案執行解毒操作。如果解毒失敗，應用程式將封鎖此檔案。

   - **封鎖**如果選擇該選項，應用程式將自動封鎖受感染的檔案，而不對其進行解毒或者刪除。

6. 要將此政策套用到電腦，請關閉... 掛鎖圖示並儲存變更。

如何在命令列設定偵測到威脅後的動作

1. 執行以下指令：

```
kesl-control --set-settings 1 ActionOnThreat=<DisinfectDeleteIfNotPossible|DisinfectBlockIfNotPossible|Block>
```

2. 若要檢查元件設定的目前值，請執行以下命令：

```
kesl-control --get-settings 1
```

符號

命令選項

設定	描述
`ActionOnThreat`	偵測到威脅後的動作： • `DisinfectDeleteIfNotPossible`（預設）。如果選取該選項，應用程式將自動對偵測到的受感染檔案執行解毒操作。如果解毒失敗，應用程式將刪除檔案。 • `DisinfectBlockIfNotPossible`。如果選取該選項，應用程式將自動對偵測到的受感染檔案執行解毒操作。如果解毒失敗，應用程式將封鎖此檔案。 • `Block`。如果選擇該選項，應用程式將自動封鎖受感染的檔案，而不對其進行解毒或者刪除。

什麼是檔案掃描的智慧模式

檔案威脅防護會掃描所有已開啟、儲存或執行的檔案。預設情況下，檔案威脅防護會以智慧模式掃描檔案。在*智慧模式*下，檔案威脅防護會在嘗試開啟檔案時掃描該檔案。如果某個處理程序在一段時間內重複存取某個檔案並加以修改，檔案威脅防護只會在該處理程序關閉該檔案時重新掃描該檔案。這可將應用程式對系統效能的影響降至最低，同時提供高等級保護。

若要讓智慧模式運作，必須選取並啟動可更新的內核模組。

您無法在網頁主控台中變更檔案掃描模式。

如何在命令列中選取檔案掃描模式

1. 執行以下指令：

```
kesl-control --set-settings 1 ScanByAccessType=<SmartCheck|OpenAndModify|Open>
```

2. 若要檢查元件設定的目前值，請執行以下命令：

```
kesl-control --get-settings 1
```

符號

設定	描述
`ScanByAccessType`	檔案掃描模式： • `SmartCheck`（預設值）。檔案威脅防護會以智慧模式掃描檔案。Kaspersky Endpoint Security 會在檔案開啟時掃描該檔案，並且在檔案已修改的情況下，於檔案關閉時掃描該檔案。 如果智慧模式無法使用，應用程式會在檔案開啟時以及每次修改檔案時掃描檔案（`OpenAndModify`）。例如，如果可更新的內核模組已停止，智慧模式可能無法使用。 • `OpenAndModify`。Kaspersky Endpoint Security 會在檔案開啟時以及每次修改檔案時掃描檔案，而不僅是在檔案關閉時。 • `Open`。Kaspersky Endpoint Security 會在嘗試開啟檔案以進行讀取、執行或修改時掃描該檔案。

如何最佳化檔案掃描

設定檔案掃描以最佳化檔案威脅防護元件。這有助於降低受保護裝置的 CPU 使用率。您可以限制壓縮檔掃描、設定可掃描物件的大小上限，以及設定物件掃描持續時間上限。

如何在網頁主控台中設定檔案掃描

1. 在網頁主控台的主視窗中，選擇**資產管理 → 政策**。
2. 點擊 Kaspersky Endpoint Security 政策的名稱。

   政策內容視窗將開啟。
3. 選擇“**應用程式設定**”標籤。
4. 轉到 **主機威脅防護 → 檔案威脅防護**。
5. 在 **進階設定** 下，選取 **效能** 索引標籤並設定檔案掃描：
   - **掃描壓縮檔案**這包括對 ZIP、GZIP、BZIP、RAR、TAR、ARJ、CAB、LHA、JAR、ICE 和其他類型壓縮檔案的掃描。應用程式不僅透過副檔名，還透過格式來識別壓縮檔案。掃描壓縮檔案時，應用程式會執行遞歸解包。這樣做可以偵測嵌套壓縮檔案（壓縮檔案中的壓縮檔案）中的威脅。預設情況下，掃描處於停用狀態。
   - **掃描分發套件和自解壓縮檔案**掃描協力廠商應用程式的安裝套件和自解壓縮檔案。自解壓縮檔案是包含可執行解壓縮模組的檔案。預設情況下，掃描處於停用狀態。
   - **掃描郵件資料庫**掃描 Microsoft Outlook、Outlook Express、The Bat! 和其他郵件用戶端的電子郵件資料庫。預設情況下，掃描處於停用狀態。
   - **掃描電子郵件格式檔案**掃描純文字電子郵件。預設情況下，掃描處於停用狀態。
   - **不掃描大於該值的壓縮檔案 (MB)**要掃描的物件的最大大小（以兆位元組為單位）。如果要掃描的物件大於指定值，應用程式將跳過該物件。
   - **略過掃描時間超過以下時長的檔案（秒）**最大物件掃描持續時間（以秒為單位）。如果掃描時間超過此設定指定的時間，應用程式將停止掃描物件。預設情況下，應用程式會嘗試在一分鐘內掃描物件。
6. 要將此政策套用到電腦，請關閉... 掛鎖圖示並儲存變更。

如何在命令列中設定檔案掃描

1. 執行以下指令：

```
kesl-control --set-settings 1 ScanArchived=<Yes|No> ScanSfxArchived=<Yes|No> ScanMailBases=<Yes|No>
ScanPlainMail=<Yes|No> SkipPlainTextFiles=<Yes|No> SkipDatabaseJournals=<Yes|No> SizeLimit=<Object size (MB)>
TimeLimit=<Scan time (sec)>
```

2. 若要檢查元件設定的目前值，請執行以下命令：

```
kesl-control --get-settings 1
```

符號

命令選項

設定	描述
ScanArchived	這包括對 ZIP、GZIP、BZIP、RAR、TAR、ARJ、CAB、LHA、JAR、ICE 和其他類型壓縮檔案的掃描。應用程式不僅透過副檔名，還透過格式來識別壓縮檔案。掃描壓縮檔案時，應用程式會執行遞歸解包。這樣做可以偵測嵌套壓縮檔案（壓縮檔案中的壓縮檔案）中的威脅。預設情況下，掃描處於停用狀態。
ScanSfxArchived	掃描協力廠商應用程式的安裝套件和自解壓縮檔案。自解壓縮檔案是包含可執行解壓縮模組的檔案。預設情況下，掃描處於停用狀態。
ScanMailBases	掃描 Microsoft Outlook、Outlook Express、The Bat! 和其他郵件用戶端的電子郵件資料庫。預設情況下，掃描處於停用狀態。
ScanPlainMail	掃描純文字電子郵件。預設情況下，掃描處於停用狀態。
SkipPlainTextFiles	暫時將文字格式的檔案排除在掃描之外。如果文字檔案在最近一次掃描後的 10 分鐘內由同一處理程序重複使用，應用程式將不會掃描這些文字檔案。預設情況下，掃描排除處於停用狀態。 此設定適用於支援 fanotify 系統事件攔截機制的裝置。在具有可更新的內核模組的裝置上，應用程式會使用掃描結果快取來最佳化負載。
SkipDatabaseJournals	暫時將資料庫日誌檔案排除在掃描範圍之外。如果日誌檔案在最近一次掃描後的 10 分鐘內由同一處理程序重複使用，應用程式將不會掃描資料庫日誌檔案。預設情況下，掃描排除處於停用狀態。 此設定適用於支援 fanotify 系統事件攔截機制的裝置。在具有可更新的內核模組的裝置上，應用程式會使用掃描結果快取來最佳化負載。
SizeLimit	要掃描的物件的最大大小（以兆位元組為單位）。如果要掃描的物件大於指定值，應用程式將跳過該物件。（值 0）。
TimeLimit	最大物件掃描持續時間（以秒為單位）。如果掃描時間超過此設定指定的時間，應用程式將停止掃描物件。預設情況下，應用程式會嘗試在一分鐘內掃描物件。（值 60）。

掃描符號連結和硬連結的特殊注意事項

Kaspersky Endpoint Security 可讓您掃描檔案的符號連結和硬連結。

符號連結（也稱為 Soft link）是指向另一個檔案或目錄的檔案。符號連結及其指向的檔案可以位於不同的檔案系統上。此外，這類連結可能會指向不存在的檔案。當您刪除目標檔案時，連結不會被刪除，但會停止運作。

Hard link 本質上是檔案的替代名稱。硬連結會指向包含檔案中繼資料的檔案索引描述元 (inode)。只要仍有至少一個指向該檔案的硬連結，該檔案就會繼續存在於檔案系統中。

掃描符號連結

只有當符號連結所指向的檔案位於檔案威脅防護的防護範圍內時，應用程式才會掃描符號連結。

如果檔案位於防護範圍之外，應用程式不會跟隨符號連結來掃描檔案內容。但是，如果該檔案包含惡意程式碼，裝置的安全性會受到威脅。

掃描硬連結

如果在有多個硬連結指向的檔案中偵測到惡意程式碼，應用程式會解毒原始檔案。如果無法解毒，應用程式會刪除硬連結，並在備份中以已刪除連結的名稱建立來源檔案的副本。應用程式只會刪除正在處理的硬連結，可能指向相同資料的其餘硬連結會保持不變。

當您從備份還原硬連結時，應用程式會在原始位置建立原始檔案的副本，並使用正在還原之硬連結的名稱。還原後的連結不會成為指向原始檔案的硬連結，並會與指向同一檔案的其他硬連結保持獨立。

解析依處理程序排除項目中的符號連結

如果 `ExcludedForProgram` 區段中 `ProgramPath` 參數的路徑是指向二進位可執行檔的符號連結，應用程式會將排除套用至目標檔案的路徑。此規則適用於指向此檔案的所有連結，而不只是明確指定的連結。此參數使用程式映像檔的路徑，因此不會解析指向指令碼（例如 `.sh`）的符號連結。

執行工作並套用設定時，會判定目標檔案。如果連結指向不存在的檔案，連結本身的路徑會包含在排除中。如果連結之後被同名的一般可執行檔取代，排除將套用至該檔案。

含符號連結的排除範例

```
[ExcludedForProgram.item_0000]
ProgramPath=/usr/bin/md5sum
UseExcludedForProgram=Yes
Path=/root/s1
```

啟動工作時，`/usr/bin/md5sum` 連結指向 `/bin/coreutils`，因此 `/bin/coreutils` 將新增至排除中。如果連結之後重新導向至 `/bin/false`，排除仍會套用至 `/bin/coreutils`，直到工作重新啟動為止，而不會套用至 `/bin/false`。工作重新啟動後，排除將套用至 `/bin/false`，而非 `/bin/coreutils`。

惡意軟體掃描

惡意軟體掃描對於電腦安全至關重要。定期進行惡意軟體掃描有助於防止因安全等級設定過低或者其他原因導致防護元件未能偵測到惡意軟體進行傳播。

Kaspersky Endpoint Security 已預先定義 *惡意軟體掃描* 標準工作。您可以使用此工作對裝置執行完整掃描。在完整掃描期間，應用程式將掃描位於裝置本機磁碟機上的所有物件，以及使用建議的安全性設定透過 Samba 或 NFS 協定存取的所有已安裝和共用的物件。

管理伺服器初始設定精靈會自動建立 *惡意軟體掃描* 工作。要建立「*惡意軟體掃描*」工作，請在執行精靈時安裝 Kaspersky Endpoint Security for Linux 管理外掛程式。如有必要，您可以建立 *惡意軟體掃描* 類型的使用者工作。

惡意軟體掃描工作設定

1. **設定工作執行排程**

   在掃描期間，Kaspersky Endpoint Security 可能會使用比平常更多的電腦資源。建議您在電腦負載最低的時段排程掃描工作。

2. **最佳化掃描對系統造成的負載**

   執行惡意軟體掃描工作時，您可以限制 CPU 使用率。這可能會增加掃描電腦所需的時間。

   Kaspersky Endpoint Security 允許在筆記型電腦使用電池供電時取消排程工作。

3. **設定惡意軟體掃描工作的設定**

   預設情況下，惡意軟體掃描工作會使用卡巴斯基專家建議的設定。預設設定提供建議的防護等級和最佳資源使用。如果您對基礎架構安全有特殊要求，可以變更這些設定。

   > 預設情況下，應用程式會掃描壓縮檔。為此，應用程式會將壓縮檔解壓縮到 /tmp 目錄。請確保電腦上有足夠的可用空間來解壓縮壓縮檔。

4. **設定掃描範圍**

   預設情況下，應用程式會掃描受防護裝置上的所有檔案。如果您只需要掃描單一目錄（例如，從外部來源自動下載檔案的目錄），您可以僅將該目錄指定為掃描範圍。在其他情況下，建議保留預設掃描範圍，並使用排除項目來微調範圍。

   > 若要掃描伺服器，建議將掃描範圍分成數個子範圍，並為每個子範圍建立單獨的惡意軟體掃描工作。為了分散負載，請為每項工作排定不同的開始時間。

5. **新增掃描排除**

   設定排除範圍：

   - **掃描排除項目**。排除項目有助於平衡系統安全性與效能。為了確保第三方軟體穩定執行，請將相應軟體文件中列出的檔案和目錄新增至排除項目。

     如果您已為 檔案威脅防護 元件建立排除範圍，也可以將這些排除項目套用至惡意軟體掃描工作。

   - **全域排除項目**。排除掛載點（全域排除項目）可讓您避免攔截某些目錄中的檔案操作。將共用網路資源排除在掃描範圍之外。要防護共用網路資源，可在資源實體儲存的裝置上使用 Kaspersky Endpoint Security 應用程式。

6. **執行惡意軟體掃描工作**

   如何在網頁主控台中執行惡意軟體掃描工作

   1. 在網頁主控台的主視窗中，選擇**工作**。

      工作清單開啟。

   2. 點擊 Kaspersky Endpoint Security 的"*惡意軟體掃描*"工作。

      工作內容視窗將開啟。

      *惡意軟體掃描*工作由管理伺服器快速啟動精靈自動建立。要建立「*惡意軟體掃描*」工作，請在執行精靈時安裝 Kaspersky Endpoint Security for Linux 管理外掛程式。

      如有必要，您可以建立 *惡意軟體掃描* 類型的使用者工作。

3. 在 **設定** 索引標籤上管理工作設定。

4. 在 **應用程式設定** 索引標籤上設定應用程式的進階設定（請參閱下表）。

5. 在 **排程** 索引標籤上設定工作啟動方式。
   預設情況下，Kaspersky Endpoint Security 設定為手動執行工作。

6. 儲存變更。

7. 執行工作。

惡意軟體掃描 工作設定

設定	描述
掃描範圍	包含工作掃描範圍的表格。預設只有一個掃描範圍處於作用中；其中包含本機檔案系統的所有目錄。您可以手動新增掃描範圍。
偵測到威脅後的動作	• **解毒；若解毒失敗則刪除**（預設值）。如果選取此動作，應用程式會嘗試透過在備份中儲存物件副本對感染物件解毒。如果無法進行解毒（例如，如果無法對該類型的物件或該物件中的威脅類型解毒），則應用程式將刪除感染物件。 • **解毒；若解毒失敗則通知**如果選取此動作，應用程式會嘗試透過在備份中儲存物件副本對感染物件解毒。如果無法進行解毒（例如，如果無法解毒該類型的物件或該物件中的威脅類型），則應用程式會在日誌中建立記錄。 • **通知**如果選取此動作，應用程式會在記錄中建立關於感染物件的記錄。
掃描壓縮檔案	如果啟用此選項，應用程式會掃描壓縮檔。 應用程式掃描以下壓縮檔案：.zip；.7z*；.7-z；.rar；.iso；.cab；.bz；.bz2；.tbz；.tbz2；.gz；.tgz；.arj。支援的壓縮檔案格式清單取決於所使用的應用程式資料庫。 要掃描壓縮檔案，應用程式必須先將其解壓，這可能會減慢掃描速度。您可以透過指定 **略過掃描時間超過以下時長的檔案（秒）** 和 **不掃描大於該值的檔案 (MB)** 設定來縮短掃描壓縮檔所需的時間。 預設會停用此選項。
掃描分發套件和自解壓縮檔案	如果啟用此選項，應用程式會掃描自解壓縮檔案。自解壓縮檔案是包含可執行解壓縮模組的檔案。 預設會停用此選項。
掃描電子郵件格式檔案	如果啟用此選項，應用程式會掃描文字格式的電子郵件訊息。 預設情況下，此功能已停用。
掃描郵件資料庫	如果啟用此選項，應用程式會掃描 Microsoft Outlook、Outlook Express、The Bat! 及其他郵件應用程式的郵件資料庫。 預設情況下，此功能已停用。
不掃描大於該值的檔案 (MB)	您可以指定可掃描檔案的大小上限（以 MB 為單位）。 可用值：1–999999。預設會停用此限制。
略過掃描時間超過以下時長的檔案（秒）	您可以指定檔案的掃描時間上限（以秒為單位）。在指定時間之後，應用程式將停止掃描檔案。 可用值：1–9999。預設會停用此限制。
不要同時執行多個掃描工作	如果掃描已經在執行，延遲啟動掃描工作。如果目前掃描繼續，Kaspersky Endpoint Security 將加入佇列新的掃描工作。這將有助於最佳化電腦負載。例如，讓我們假設應用程式已根據排程啟動了一項完整掃描工作。如果使用者嘗試從應用程式介面啟動快速掃描，Kaspersky Endpoint Security 將加入佇列該快速掃描工作，然後在完整掃描工作結束後自動啟動該工作。 預設情況下，此功能已停用。
使用 iChecker 技術	如果啟用此選項，應用程式只會掃描新檔案以及上次掃描後修改過的檔案。 如果停用此選項，應用程式會掃描檔案，無論檔案的建立日期或修改日期為何。 預設會停用此選項。

如何在命令列中執行惡意軟體掃描工作

1. 預設情況下，應用程式具有 *惡意軟體掃描*（*掃描我的電腦*）工作。如果您想建立新的 *惡意軟體掃描* 工作，請執行以下命令：

```
kesl-control --create-task <task name> --type ODS
```

   其中 `<task name>` 是您要為新工作設定的名稱。

   此指令會傳回已建立工作的 ID。

2. 如有必要，請使用以下命令變更工作設定（請參閱下表）：

```
kesl-control --set-settings <task ID|name> <setting name>=<setting value> [<setting name>=<setting value>]
```

   變更工作設定的範例

```
kesl-control --set-settings 101 ScanFiles=No
```

   您也可以使用設定檔管理工作設定。

3. 如有必要，請設定工作排程。預設情況下，此工作會手動啟動。

4. 若要檢查工作設定的目前值，請執行以下命令：

```
kesl-control --get-settings <task ID|name>
```

5. 若要執行 *惡意軟體掃描* 工作，請執行以下命令：

```
kesl-control --start-task <task ID|name> [-W] [--progress]
```

   命令範例

```
kesl-control --start-task 2 -W
```

6. 若要停止 *惡意軟體掃描* 工作，請執行以下命令：

```
kesl-control --stop-task <task ID|name> [-W]
```

符號

惡意軟體掃描工作設定

設定	描述	參數值
ScanFiles	啟用檔案掃描。	Yes（預設值）— 掃描檔案。 No — 不掃描檔案。
ScanBootSectors	啟用引導磁區掃描。	Yes（預設值）— 掃描引導磁區。 No — 不掃描引導磁區。
ScanComputerMemory	啟用處理程序記憶體和核心記憶體掃描。	Yes（預設值）— 掃描處理程序記憶體和核心記憶體。 No — 不掃描處理程序記憶體和核心記憶體。

設定	描述	參數值
ScanStartupObjects	啟用啟動物件掃描。	Yes（預設值）— 掃描啟動物件。 No — 不掃描啟動物件。
ScanArchived	啟用壓縮檔案掃描（包括 SFX 自解壓縮檔案）。 應用程式掃描以下壓縮檔案：.zip；.7z*；.7-z；.rar；.iso；.cab；.bz；.bz2；.tbz；.tbz2；.gz；.tgz；.arj。支援的壓縮檔案格式清單取決於所使用的應用程式資料庫。	Yes（預設值）— 掃描壓縮檔案。 如果將 ActionOnThreat 設定為 DisinfectDeleteIfNotPossible，並且無法解毒，則應用程式會根據壓縮檔案類型，刪除感染物件或包含威脅的整個壓縮檔案。 No — 不掃描壓縮檔案。
ScanSfxArchived	僅啟用對 self-extracting archives 的掃描（包含可執行解壓縮模組的壓縮檔案）。	Yes（預設值）— 掃描自解壓縮檔案。 No — 不掃描自解壓縮檔案。
ScanMailBases	啟用掃描 Microsoft Outlook、Outlook Express、The Bat 和其他郵件用戶端的電子郵件資料庫。	Yes — 掃描電子郵件資料庫的檔案。 No（預設值）— 不掃描電子郵件資料庫的檔案。
ScanPlainMail	啟用對 plain text 電子郵件訊息的掃描。	Yes — 掃描純文字電子郵件。 No（預設值）— 不掃描純文字電子郵件。
SizeLimit	要掃描的物件的最大大小（以兆位元組為單位）。如果要掃描的物件大於指定值，應用程式將跳過該物件。	0 至 999999 0 — 應用程式可掃描任意大小的物件。 預設值：0。
TimeLimit	最大物件掃描持續時間（以秒為單位）。如果掃描時間超過此設定指定的時間，應用程式將停止掃描物件。	0 至 9999 0 — 物件掃描時間不受限制。 預設值：0。
QueueScanTasks	如果先前啟動的排程掃描仍在執行，則延遲排程掃描工作。如果目前的掃描持續執行，Kaspersky Endpoint Security 會將排程掃描工作加入佇列。這將有助於最佳化電腦負載。例如，掃描工作排定在 18:00 和 20:00 執行。如果 18:00 的掃描仍在執行，則排定在 20:00 執行的掃描工作會延遲。延遲的工作會在 18:00 的工作完成後執行。	Yes，可在目前的掃描仍在執行時，將排程掃描工作加入佇列。 No（預設值），即使目前的掃描仍在執行，也會執行排程掃描工作。
ActionOnThreat	選取應用程式對感染物件執行的動作。	DisinfectDeleteIfNotPossible（解毒；如果不能解毒則刪除）表示應用程式會先將物件副本儲存在備份中，隨後嘗試對感染物件解毒。如果無法進行解毒（例如，如果無法對該類型的物件或該物件中的威脅類型解毒），則應用程式將刪除感染物件。 DisinfectInformIfNotPossible（解毒；如果無法解毒則告知）表示應用程式會先將物件副本儲存在備份中，隨後嘗試對感染物件解毒。如果無法進行解毒（例如，如果無法解毒該類型的物件或該物件中的威脅類型），則應用程式會在日誌中建立記錄。 Inform 表示應用程式不會嘗試解毒或刪除感染物件。會記錄關於感染物件的資訊。 預設值：DisinfectDeleteIfNotPossible。
UseExcludeMasks	允許從掃描中排除由 ExcludeMasks.item_# 設定指定的物件。	Yes — 從掃描中排除 ExcludeMasks.item_# 設定指定的物件。 No（預設值）— 不從掃描中排除 ExcludeMasks.item_# 設定指定的物件。

設定	描述	參數值
ExcludeMasks.item_#	按名稱或遮罩排除掃描物件。您可以使用此設定按名稱從指定的掃描範圍中排除單一檔案，或使用 shell 格式的遮罩一次排除多個檔案。 在為此設定指定值之前，請確保UseExcludeMasks設定已啟用。	預設值未定義。 範例 UseExcludeMasks=Yes ExcludeMasks.item_0000=eicar1.* ExcludeMasks.item_0001=eicar2.*
UseExcludeThreats	啟用從掃描中排除包含 ExcludeThreats.item_# 設定所指定威脅的物件。	Yes — 從掃描中排除包含ExcludeThreats.item_#設定所指定的威脅的物件。 No（預設值）：不從掃描中排除包含ExcludeThreats.item_#設定指定的威脅的物件。
ExcludeThreats.item_#	根據偵測到的威脅名稱從掃描中排除物件。在為此設定指定值之前，請確保UseExcludeThreats設定已啟用。 為了從掃描中排除物件，請指定在此物件中偵測到的威脅的全名 — 包含應用程式判定物件被感染的字串。 例如，您可能正在使用公用程式來獲取關於網路的資訊。為了防止應用程式封鎖它，請將其中包含的威脅的全名新增至排除掃描的威脅清單。 您可以在應用程式記錄或網站https://threats.kaspersky.com中找到在物件中偵測到的威脅的全名。	設定值區分大小寫。 預設值未定義。 範例 UseExcludeThreats=Yes ExcludeThreats.item_0000=EICAR-Test-* ExcludeThreats.item_0001=?rojan.Linux
UseGlobalExclusions	啟用全域排除進行掃描。	Yes（預設值）— 使用全域排除。 No — 不使用全域排除。
UseOASExclusions	啟用檔案威脅防護排除項目進行掃描。	Yes（預設值）— 使用檔案威脅防護排除項目。 No — 不使用檔案威脅防護排除項目。
ReportCleanObjects	啟用記錄關於應用程式報告未被感染的掃描物件的資訊。 例如，您可以啟用此設定，以確保應用程式掃描了特定物件。	Yes — 記錄關於未感染物件的資訊。 No（預設值）— 不記錄關於未感染物件的資訊。
ReportPackedObjects	啟用記錄關於作為複合物件一部分的掃描物件的資訊。 例如，您可以啟用此設定來確保應用程式已掃描壓縮檔案內的物件。	Yes — 記錄關於壓縮檔案中已掃描物件的資訊。 No（預設值）— 不記錄關於檔案中掃描物件的資訊。
ReportUnprocessedObjects	啟用記錄關於由於某種原因尚未處理的物件的資訊。	Yes — 記錄關於未處理物件的資訊。 No（預設值）— 不記錄關於未處理物件的資訊。
UseAnalyzer	啟用啟發式分析。 啟發式分析可以幫助應用程式在病毒分析師發現威脅之前就偵測到威脅。	Yes（預設值）— 啟用啟發式分析器。 No — 停用啟發式分析器。
HeuristicLevel	指定啟發式分析級別。 您可以指定啟發式分析級別。啟發式分析級別可設定威脅搜尋的徹底性、作業系統資源的負載和掃描持續時間之間的平衡。啟發式分析級別越高，掃描所需的資源和時間就越多。	Light — 最不徹底的掃描，系統負載最小。 Medium — 中等啟發式分析級別，系統負載平衡。 Deep — 最徹底的掃描，系統負載最大。 Recommended（預設值）— 建議的值。
UseIChecker	啟用 iChecker 技術。	Yes（預設值）— 啟用 iChecker 技術。 No — 停用 iChecker 技術。
DeviceNameMasks.item_#	裝置名稱清單。應用程式將掃描這些裝置的引導磁區。 設定值不能為空。必須指定至少一個裝置名稱遮罩才能執行此工作。	AllObjects — 掃描所有裝置的引導磁區。 <device name mask> – 掃描名稱與指定遮罩相符的裝置的引導磁區。 預設值：/** — 裝置名稱中的任意一組字元，包括 / 字元。
[ScanScope.item_#]部分包含以下設定：		

設定	描述	參數值
AreaDesc	掃描範圍的描述，包含關於掃描範圍的附加資訊。使用此設定指定的字串的最大長度為 4096 個字元。	預設值：All objects。 範例 AreaDesc="Mail bases scan"
UseScanArea	啟用指定範圍的掃描。若要執行該工作，請啟用至少一個範圍的掃描。	Yes（預設值）— 掃描指定範圍。 No — 不掃描指定範圍。
AreaMask.item_#	掃描範圍限制。在掃描範圍內，應用程式僅掃描使用 shell 格式的遮罩指定的檔案。 如果未指定此設定，應用程式將掃描掃描範圍內的所有物件。您可以為此設定指定多個值。	預設值為 *（掃描所有物件）。 範例 AreaMask.item_0000=*doc
Path	包含要掃描的物件的目錄的路徑。	<path to local directory> – 掃描指定目錄中的物件。預設指定 / 路徑 — 應用程式掃描本機檔案系統的所有目錄。 Shared:NFS — 掃描可透過 NFS 協定存取的裝置檔案系統資源。 Shared:SMB — 掃描可透過 Samba 協定存取的裝置檔案系統資源。 Mounted:NFS — 使用 NFS 協定掃描裝置上安裝的遠端目錄。 Mounted:SMB — 使用 Samba 協定掃描裝置上安裝的遠端目錄。 AllRemoteMounted — 使用 Samba 和 NFS 協定掃描裝置上安裝的所有遠端目錄。 AllShared — 掃描所有可透過 Samba 和 NFS 協定存取的裝置檔案系統資源。 <file system type> – 掃描指定檔案系統裝置的所有資源。
[ExcludedFromScanScope.item_#]部分包含以下設定：		
AreaDesc	掃描排除範圍的描述，包含關於排除掃描範圍的附加資訊。	預設值未定義。
UseScanArea	從掃描中排除指定的掃描範圍。	Yes（預設值）— 排除指定範圍。 No — 不排除指定的範圍。
AreaMask.item_#	掃描排除項目範圍的限制。在排除範圍中，應用程式僅排除使用 shell 格式的遮罩指定的檔案。 如果未指定此設定，應用程式將排除排除範圍內的所有物件。您可以為此設定指定多個值。	預設值：*（排除所有物件）

設定	描述	參數值
`Path`	包含要排除的物件的目錄的路徑。	`<path to local directory>` – 從掃描中排除指定目錄（包括子目錄）中的物件。您可以使用遮罩來指定路徑。 為了最佳化掃描工作的運行，建議將系統以唯讀模式掛載的快照路徑新增至具有 btrfs 檔案系統且啟用活動快照的系統的排除項目中。例如，對於基於 SUSE/OpenSUSE 的系統，可以新增以下排除 `/.snapshots/*/snapshot/`。 預設會指定 `/` 路徑。應用程式將本機檔案系統的所有目錄排除在掃描之外。 `Mounted:NFS` — 從掃描中排除使用 NFS 協定掛載在裝置上的遠端目錄。 `Mounted:SMB` — 從掃描中排除使用 Samba 協定安裝在裝置上的遠端目錄。 `AllRemoteMounted` — 從掃描中排除使用 Samba 和 NFS 協定安裝在裝置上的所有遠端目錄。 `<file system type>` – 從掃描中排除指定檔案系統裝置的所有資源。 只有當遠端目錄在工作啟動前安裝時，應用程式才會將其排除在掃描範圍之外。工作啟動後裝載的遠端目錄不會被排除在掃描之外。

如何從圖形介面執行惡意軟體掃描工作

1. 開啟應用程式圖形介面的主視窗。
2. 點擊“**掃描**”。
   開啟“**掃描**”視窗。
3. 若要啟動掃描工作，請點擊要啟動的掃描工作下方的 **開始** 按鈕。
   正在執行的掃描工作的進度將顯示。
4. 若要停止掃描工作，請點擊要停止的掃描工作下方的 **停止** 按鈕。
   掃描工作停止，關於掃描物件和偵測到的威脅的資訊將顯示。
5. 若要檢視掃描工作報告，請點擊 **顯示報告** 按鈕。

當偵測到受感染物件或掃描工作完成時，會顯示相應的通知。

掃描 視窗也會顯示暫時性引導磁區掃描工作（*Scan_Boot_Sectors_{ID}*）和暫時性自訂檔案掃描工作（*Scan_File_{ID}*）的進度和結果。

7 收集電腦掃描統計資料

您可以使用報告來取得電腦的掃描統計資料。請確保掃描持續時間在可接受範圍內。檢查偵測到的物件，如果這些物件可信，請將它們新增至排除。

特殊考量與限制

- 如果 root 使用者沒有權限存取透過 NFSv4 協定掛載到裝置上的遠端目錄，應用程式將在掃描期間略過此檔案。
- 在執行掃描工作時，Kaspersky Endpoint Security 可以解毒並刪除被防止修改的檔案：具有“不可變”和“僅追加”屬性的檔案以及具有“不可變”和“僅追加”屬性的目錄中的檔案。備份可儲存在清除或刪除之前建立的這些檔案的副本。如果需要，您可以從備份副本中還原檔案。當掃描工作完成後，已解毒檔案的“不可變”和“僅追加”屬性不被保留。
- 如果使用者或監控服務在惡意軟體掃描期間重新啟動應用程式，或如果電腦在掃描期間重新啟動，掃描會停止。下次啟動惡意軟體掃描時，掃描會從頭開始。

實用文章

如果您的裝置可用磁碟空間不足，該怎麼辦

如何建立掃描範圍

*掃描範圍*是 Kaspersky Endpoint Security 要掃描是否存在威脅的物件路徑清單。預設情況下，應用程式會掃描受防護裝置上的所有檔案。如果您只需要掃描個別目錄（例如，自動從外部來源下載檔案的目錄），可以將此目錄指定為掃描範圍。

Kaspersky Endpoint Security 會依照物件在物件清單中出現的順序掃描物件。如果有必要，將子目錄放在清單中高於其父目錄的位置，以便為子目錄配置與父目錄的安全性設定不同的安全性設定。

在使用專用 parsecfs 檔案系統（Astra Linux Special Edition）的作業系統上執行時，我們建議將此檔案系統的掛載路徑新增至掃描排除項目。

如何在網頁主控台中建立掃描範圍

1. 在網頁主控台的主視窗中，選擇**工作**。

   工作清單開啟。

2. 點擊掃描工作。

   工作內容視窗將開啟。

3. 選擇“**應用程式設定**”標籤。

4. 在“**掃描範圍**”區域中點擊“**新增**”。

5. 在 **檔案系統、存取協定和路徑** 下拉清單中，選取檔案系統類型：

   - **本機**不需網路連線即可存取的硬碟目錄。
   - **已掛接**已掛載的遠端或本機目錄。

- **已共用**可透過 Samba (SMB) 或 NFS 通訊協定存取的電腦目錄。
- **所有遠端掛接**使用 Samba 和 NFS 協定掛載在裝置上的所有遠端目錄。
- **所有共用**透過 Samba 和 NFS 通訊協定存取的所有電腦目錄。

6. 對於 **已掛接** 和 **已共用** 檔案系統類型，請選取存取協定：
   - **NFS**。使用 NFS 協定掛載在裝置上的遠端目錄。
   - **Samba**。使用 Samba 協定掛載在裝置上的遠端目錄。
   - **自訂**。裝置上類型不是 NFS 或 Samba 的檔案系統資源（例如 `ext4` 或 `parsecfs`）。
7. 指定目錄路徑或路徑遮罩。
8. 如有必要，請指定物件名稱的遮罩（例如，`*.txt` 或 `report_*`）。使用逗號分隔遮罩。
9. 點擊“**新增**”。

   新物件已新增至掃描範圍。您可以從掃描範圍中排除物件，而不必將其從物件清單中移除。若要這樣做，請停用物件旁邊的切換開關。
10. 如有必要，請啟用或停用掃描範圍中的預先定義物件：
    - **內核記憶體**。**執行中的處理程序的記憶體**。
    - **正在執行的處理程序和啟動物件**
    - **磁碟開機磁區**
    - **所有硬碟磁碟機**
    - **所有網路磁碟機**
11. 要將此政策套用到電腦，請關閉... 掛鎖圖示並儲存變更。

如何在命令列中建立掃描範圍

1. 執行以下指令：

```
kesl-control --set-settings 2 --add-path <path>
```

新的 `[ScanScope.item_#]` 部分將被新增至工作設定中。應用程式將掃描指定目錄中的物件。

範例

```
kesl-control --set-settings 2 ScanScope.item_0001.UseScanArea=Yes ScanScope.item_0001.Path=/home
```

以下掃描範圍設定將會被新增至工作：

```
[ScanScope.item_0001]
AreaDesc=All objects
UseScanArea=Yes
Path=/home
AreaMask.item_0000=*
```

2. 如果您想要將來自 NFS 或 Samba 以外特定類型之已掛載檔案系統的資源（例如 `parsecfs` ）納入掃描範圍，請在 `Path` 參數中指定檔案系統類型：Path=<檔案系統類型>

   應用程式將掃描指定裝置檔案系統的所有資源。

   範例

   ```
   kesl-control --set-settings 2 ScanScope.item_0002.UseScanArea=Yes ScanScope.item_0002.Path=parsecfs
   ```

   以下掃描範圍設定將會被新增至工作：

   ```
   [ScanScope.item_0002]
   AreaDesc=All objects
   UseScanArea=Yes
   Path=parsecfs
   AreaMask.item_0000=*
   ```

3. 若要檢查工作設定的目前值，請執行以下命令：

   ```
   kesl-control --get-settings 2
   ```

如何設定掃描排程

執行 *惡意軟體掃描* 工作可能會增加電腦的資源使用率。為了在使用者主動使用電腦時，將 Kaspersky Endpoint Security 對其電腦效能的影響降至最低，您可以排程該工作在最適當的時間執行。

例如，如果貴組織員工按固定時間表工作，您可以設定掃描在夜間或週末執行。如果因任何原因無法執行掃描（例如電腦在該時間關閉），您可以設定錯過的工作在可行時立即自動執行。

如果您無法確定執行電腦掃描的最佳排程，則不僅可以在特定時間執行 *惡意軟體掃描* 任務，也可以根據特定條件執行，例如啟動應用程式時、將更新下載至儲存區時、偵測到病毒攻擊時，或其他任務完成時。您也可以使用 Wake-on-LAN 功能，在任務開始前不久開啟已關機的電腦。您只能在卡巴斯基安全管理中心中為“*惡意軟體掃描*”工作設定使用“Wake-on-LAN”執行掃描。您不能在應用程式介面中啟用“Wake-on-LAN”進行電腦掃描。

如何在網頁主控台中執行惡意軟體掃描工作

1. 在網頁主控台的主視窗中，選擇**工作**。

   工作清單開啟。

2. 點擊掃描工作。

   工作內容視窗將開啟。

3. 在工作內容視窗中，選取“**排程**”標籤。

4. 設定掃描工作排程。

5. 根據選定的頻率，配置指定工作執行排程的進階設定（請見下表）。

6. 儲存變更。

掃描排程設定

設定	描述
開始工作	**手動**執行模式，您可以在方便時手動開始掃描。 依排程。在該掃描工作執行模式下，應用程式將按照您建立的排程啟動掃描工作。如果選擇該掃描工作執行模式，您也可以手動啟動掃描工作。
執行錯過的工作	如果選中此核取方塊，Kaspersky Endpoint Security 將在可能的情況下儘快啟動已略過的工作。工作在某些情況下可能被略過，例如，電腦在排程的工作啟動時關閉。當應用程式有機會執行錯過的工作時，它會在一定的時間間隔內隨機執行工作，以分配電腦上的負載。 如果清除此核取方塊，Kaspersky Endpoint Security 不會執行已略過的工作。它將按照目前排程執行下一次工作。
使用工作啟動自動隨機化延遲	如果選擇該核取方塊，則工作不會嚴格按照排程執行，而是在某個間隔內隨機執行，即工作的開始時間分散開。隨機開始時間有助於避免當工作按照排程執行時，大量電腦同時存取管理伺服器。 隨機開始時間的範圍在建立工作時自動計算，取決於分配了工作的電腦數量。隨後，工作會始終在計算的開始時間執行。不過，只要工作設定被修改或者手動執行工作，計算的開始時間就會變更。 如果清除該核取方塊，則工作會準確在排程的時間執行。
對於在以下間隔內啟動的工作，使用工作啟動自動隨機化延遲	如果選取此核取方塊，則該工作將在特定時間範圍內的隨機時間在電腦上執行。隨機開始時間有助於避免當工作按照排程執行時，大量電腦同時存取管理伺服器。 如果清除該核取方塊，則工作會準確在排程的時間執行。
在啟動工作之前，使用 Wake-On-LAN 功能開啟裝置	如果選擇此核取方塊，則電腦的作業系統會被給與指定的前置重疊時間以在執行工作前完成啟動。預設前置重疊時間為 5 分鐘。 如果您希望在包括關機電腦在內的所有電腦上執行工作，請選擇此核取方塊。
完成工作後將裝置關機	如果選取此核取方塊，電腦將在工作完成後關機。例如，您可以啟用此功能以在周五下班後掃描電腦。工作完成後，應用程式會在週末關閉電腦。
停止工作，若執行時間超過	限制工作執行時間。超出指定時間後，Kaspersky Endpoint Security 將停止工作。工作未標記為已完成。下次 Kaspersky Endpoint Security 執行該工作時，它將從頭開始按排程執行。

如何在命令列中排程惡意軟體掃描工作

若要在特定時間執行工作一次，請執行下列命令：

```
kesl-control --set-schedule 2 RuleType=Once StartTime='<year>/<month>/<day of the month> <hh>:<mm>:<ss>'
```

若要每月執行工作，請執行下列命令：

```
kesl-control --set-schedule 2 RuleType=Monthly StartTime='<hh>:<mm>:<ss>;<day of the month>'
```

若要在一週中的特定日期執行工作，請執行下列命令：

```
kesl-control --set-schedule 2 RuleType=Weekly StartTime='<hh>:<mm>:<ss>;<day of the week>'
```

若要以天為間隔定期執行工作，請執行下列命令：

```
kesl-control --set-schedule 2 RuleType=Daily StartTime='<hh>:<mm>:<ss>;<interval between runs (in days)>'
```

若要從特定日期開始以小時為間隔定期執行工作，請執行下列命令：

```
kesl-control --set-schedule 2 RuleType=Hourly StartTime='<year>/<month>/<day of the month> <hh>:<mm>:<ss>;
<interval between runs (in hours)>'
```

若要從特定日期開始定期執行工作，請執行下列命令：

```
kesl-control --set-schedule 2 RuleType=Minutely StartTime='<hh>:<mm>:<ss>;<interval between runs (in minutes)>'
```

若要在應用程式啟動後立即執行工作，請執行下列命令：

```
kesl-control --set-schedule 2 RuleType=PS
```

若要在資料庫更新後立即執行工作，請執行下列命令：

```
kesl-control --set-schedule 2 RuleType=BR
```

若要停用工作的排程，請執行下列命令：

```
kesl-control --set-schedule 2 RuleType=Manual
```

若要管理其他工作排程設定，請執行下列命令：

```
kesl-control --set-schedule 2 RandomInterval=<time interval (minutes)> RunMissedStartRules=<Yes|No>
UseWorkingTimeout=<Yes|No> WorkingTimeout=<maximum task completion time (minutes)> QueueScanTasks=<Yes|No>
```

若要檢查工作設定的目前值，請執行以下指令：

```
kesl-control --get-schedule 2
```

符號

工作啟動排程設定

設定	描述
RuleType	工作啟動排程。 • Once：執行工作一次。 • Monthly：每月在指定的日期和時間執行工作。 • Weekly：每週在指定的日期和時間執行工作。 • Daily：依照指定的天數間隔定期執行工作。 • Hourly：從指定的日期和時間開始，按照指定的小時間隔定期執行工作。 • Minutely：從指定時間開始，按照指定的分鐘間隔定期執行工作。 • Manual — 手動啟動工作。 • PS — 啟動應用程式後啟動工作。 • BR — 應用程式資料庫更新後啟動工作。
StartTime	工作開始日期和時間。此設定的格式取決於 RuleType。 可能的值： • <year>:1970 至 2099 • <month>:JAN，FEB，MAR，APR，MAY，JUN，JUL，AUG，SEP，OCT，NOV，DEC。 • <day of the month>:1 至 31 • <day of the week>:Mon，Tue，Wed，Thu，Fri，Sat，Sun。 • <hh>:0 至 23 • <mm>:0 至 59 • <ss>:0 至 59 • <interval between runs (in days)>:0 至 364 • <interval between runs (in hours)>:0 至 23 • <interval between runs (in minutes)>:0 至 59
RandomInterval	在特定時間間隔內（從 0 到指定值）隨機在電腦上執行工作。這樣可避免多個工作同時啟動。 預設值：99分鐘。 可用值：0 – 999。
RunMissedStartRules	應用程式啟動後執行錯過的工作。 • Yes（預設值）表示已啟用執行錯過的工作。如果排程工作執行時應用程式停止或電腦關機，Kaspersky Endpoint Security 會在應用程式啟動後立即啟動該工作。這樣可確保不會錯過任何關鍵工作。 • No 表示已停用執行錯過的工作。如果排程工作執行時應用程式停止或電腦關機，應用程式將略過該工作。這樣可避免在啟動應用程式時產生額外負載。

設定	描述
UseWorkingTimeout	達到WorkingTimeout設定指定的最大工作執行時間時停止工作。即使未完成，工作也會停止。下次工作啟動將按照排程進行。 • Yes — 達到最大工作執行時間時停止工作。 • No（預設值）— 達到最大工作執行時間時不停止工作。
WorkingTimeout	如果UseWorkingTimeout=Yes，則應用程式停止執行工作後的最大工作執行時間（以分鐘為單位）。 預設值：120分鐘。 可用值：1 – 999。

每 10 小時執行掃描工作的範例

```
kesl-control --set-schedule 2 RuleType=Hourly StartTime='2030/May/28 12:00:00;10'
```

每月 15 日執行掃描工作的範例

```
kesl-control --set-schedule 2 RuleType=Monthly StartTime='12:00:00;15'
```

每週二執行工作的範例

```
kesl-control --set-schedule 2 RuleType=Weekly StartTime='12:00:00;Tue'
```

如何掃描單一檔案或目錄

Kaspersky Endpoint Security 可讓您使用命令列執行單個檔案掃描，以尋找病毒和其他惡意軟體。例如，您可以選擇性地掃描預設停用檔案威脅防護掃描的封存檔案。

預設情況下，應用程式會使用卡巴斯基專家建議的 *掃描檔案 (ID: 3) 工作設定*掃描檔案。預設設定提供建議的防護等級和最佳資源使用。預設情況下，應用程式會將受感染物件的副本儲存到備份，並嘗試解毒該物件。如果無法進行解毒（例如，如果無法對該類型的物件或該物件中的威脅類型解毒），則應用程式將刪除感染物件。您可以選擇在偵測到威脅時採取其他操作，並管理其他工作設定。

如何在命令列中開始掃描單一檔案或目錄

```
kesl-control --scan-file <path to the file or directory>
```

因此，Kaspersky Endpoint Security 會產生下列格式的報告：

掃描的物件：N

偵測到的物件總數：N

感染物件和其他物件：N

解毒的物件：N

移至備份：N

移除的物件：N

未解毒的物件：N

掃描錯誤：N

受密碼防護的物件：N

略過的物件：N

被 Cloud Sandbox 偵測到：N

如何最佳化自訂掃描任務

若要最佳化自訂掃描，您可以限制同時啟動多個任務。如果使用者嘗試同時執行過多自訂掃描任務，應用程式將不會執行超出限制的任務。這可讓您控制用戶端裝置的資源使用率，例如，避免伺服器負載過高。預設情況下，自訂掃描任務數量限制設定為 100。

Kaspersky Endpoint Security 僅會限制非特權使用者的任務。具有 root 權限的使用者可以不受限制地執行自訂掃描任務。

您可以在命令列中使用一般應用程式設定來設定自訂掃描任務限制。您無法在管理主控台或網頁主控台中設定任務限制。

如何在命令列中最佳化自訂掃描任務

```
kesl-control --set-app-settings LimitNumberOfScanFileTasks=<number of tasks>
```

關鍵區域掃描

特殊掃描工作可讓您僅掃描電腦的關鍵區域：*關鍵區域掃描*。*關鍵區域掃描* 會快速掃描電腦中最常發現惡意軟體的區域。此工作的掃描範圍包括開機磁區、啟動物件、核心記憶體和執行中的處理程序。

成功危害電腦關鍵區域的惡意軟體可在規避偵測的同時執行其功能。預設情況下，應用程式會使用卡巴斯基專家建議的設定執行工作。預設設定提供建議的防護等級和最佳資源使用。

卡巴斯基專家不建議變更 *關鍵區域掃描* 工作的預設設定。

如果 root 使用者沒有權限存取透過 NFSv4 協定掛載到裝置上的遠端目錄，應用程式將在掃描期間略過此檔案。

管理伺服器初始設定精靈會自動建立 *關鍵區域掃描* 工作。要建立「*關鍵區域掃描*」工作，請在執行精靈時安裝 Kaspersky Endpoint Security for Linux 管理外掛程式。如有必要，您可以建立 *關鍵區域掃描* 類型的使用者工作。

如何在網頁主控台中執行關鍵區域掃描

1. 在網頁主控台的主視窗中，選擇**工作**。

   工作清單開啟。

2. 點擊“**新增**”。

   啟動“工作精靈”。

3. 配置工作設定：

   a. 在 **應用程式** 下拉式清單中，選取 **Kaspersky Endpoint Security for Linux**。

   b. 在“**工作類型**”下拉式清單中，選取“**關鍵區域掃描**”。

   c. 在 **工作名稱** 欄位中，輸入簡要說明，例如 *電腦感染後的關鍵區域掃描*。

   d. 在“**要將工作指派給的裝置**”塊中，選取工作範圍。

4. 按照所選工作範圍選項選取裝置。繼續下一步。

5. 完成精靈。

6. 點擊掃描工作。
   工作內容視窗將開啟。

7. 選擇“**應用程式設定**”標籤。

8. 配置掃描工作（請參見下表）。

9. 如有必要，請在 **排程** 索引標籤上設定工作啟動排程設定。

10. 儲存變更。

11. 執行掃描工作。

關鍵區域掃描工作設定

設定	描述
掃描範圍	包含工作掃描範圍的表格。預設情況下，掃描範圍包括本機檔案系統的所有目錄、核心記憶體、執行中處理程序的記憶體、啟動物件和開機磁區。
偵測到威脅後的動作	• **解毒；若解毒失敗則刪除**（預設）。如果選取此動作，應用程式會嘗試透過在備份中儲存物件副本對感染物件解毒。如果無法進行解毒（例如，如果無法對該類型的物件或該物件中的威脅類型解毒），則應用程式將刪除感染物件。 • **解毒；若解毒失敗則通知**如果選取此動作，應用程式會嘗試透過在備份中儲存物件副本對感染物件解毒。如果無法進行解毒（例如，如果無法解毒該類型的物件或該物件中的威脅類型），則應用程式會在日誌中建立記錄。 • **通知**如果選取此動作，應用程式會在記錄中建立關於感染物件的記錄。
掃描壓縮檔案	如果啟用此選項，應用程式會掃描壓縮檔。 應用程式掃描以下壓縮檔案：.zip；.7z*；.7-z；.rar；.iso；.cab；.bz；.bz2；.tbz；.tbz2；.gz；.tgz；.arj。支援的壓縮檔案格式清單取決於所使用的應用程式資料庫。 要掃描壓縮檔案，應用程式必須先將其解壓，這可能會減慢掃描速度。您可以透過指定 **略過掃描時間超過以下時長的檔案（秒）** 和 **不掃描大於該值的檔案 (MB)** 設定來縮短掃描壓縮檔所需的時間。 預設會停用此選項。
掃描分發套件和自解壓縮檔案	如果啟用此選項，應用程式會掃描自解壓縮檔案。自解壓縮檔案是包含可執行解壓縮模組的檔案。 預設會停用此選項。
掃描電子郵件格式檔案	掃描純文字電子郵件。 預設情況下，此功能已停用。
掃描郵件資料庫	如果啟用此選項，應用程式會掃描 Microsoft Outlook、Outlook Express、The Bat! 及其他郵件應用程式的郵件資料庫。 預設情況下，此功能已停用。
不掃描大於該值的檔案 (MB)	您可以指定可掃描檔案的大小上限（以 MB 為單位）。 可用值：0–9999。如果該值設為 0，應用程式將掃描任意大小的檔案。 預設情況下，此功能已停用。
略過掃描時間超過以下時長的檔案（秒）	您可以指定檔案的掃描時間上限（以秒為單位）。在指定時間之後，應用程式將停止掃描檔案。 可用值：0–9999。如果該值設為 0，則掃描時間不受限制。 預設情況下，此功能已停用。

設定	描述
不要同時執行多個掃描工作	如果掃描已經在執行，延遲啟動掃描工作。如果目前掃描繼續，Kaspersky Endpoint Security 將加入佇列新的掃描工作。這將有助於最佳化電腦負載。例如，讓我們假設應用程式已根據排程啟動了一項完整掃描工作。如果使用者嘗試從應用程式介面啟動快速掃描，Kaspersky Endpoint Security 將加入佇列該快速掃描工作，然後在完整掃描工作結束後自動啟動該工作。 預設情況下，此功能已停用。
使用 iChecker 技術	如果啟用此選項，應用程式只會掃描新檔案以及上次掃描後修改過的檔案。 如果停用此選項，應用程式會掃描檔案，無論檔案的建立日期或修改日期為何。 預設會停用此選項。

如何在命令列執行關鍵區域掃描工作

1. 如有必要，請設定工作設定（請參閱下表）。

```
kesl-control --set-settings 4 <setting name>=<setting value>
```

2. 如有必要，設定工作排程。

3. 若要檢查工作設定的目前值，請執行以下命令：

```
kesl-control --get-settings 4 [--json]
```

其中`--json`表示以 JSON 格式輸出資料。

4. 若要執行工作，請執行以下命令：

```
kesl-control --start-task 4 [-W] [--progress]
```

其中：

- `[-W]`啟用與此工作相關的目前事件的輸出。
- `[--progress]`：顯示工作進度。

如有必要，您可以建立使用者工作，類型為 *關鍵區域掃描*。

關鍵區域掃描工作設定

設定	描述	參數值
`ScanFiles`	啟用檔案掃描。	`Yes` — 掃描檔案。 `No`（預設值）— 不掃描檔案。
`ScanBootSectors`	啟用引導磁區掃描。	`Yes`（預設值）— 掃描引導磁區。 `No` — 不掃描引導磁區。
`ScanComputerMemory`	啟用處理程序記憶體和核心記憶體掃描。	`Yes`（預設值）— 掃描處理程序記憶體和核心記憶體。 `No` — 不掃描處理程序記憶體和核心記憶體。
`ScanStartupObjects`	啟用啟動物件掃描。	`Yes`（預設值）— 掃描啟動物件。 `No` — 不掃描啟動物件。

設定	描述	參數值
ScanArchived	啟用壓縮檔案掃描（包括 SFX 自解壓縮檔案）。 應用程式掃描以下壓縮檔案：.zip；.7z*；.7-z；.rar；.iso；.cab；.bz；.bz2；.tbz；.tbz2；.gz；.tgz；.arj。支援的壓縮檔案格式清單取決於所使用的應用程式資料庫。	Yes（預設值）— 掃描壓縮檔案。 如果將 ActionOnThreat 設定為 DisinfectDeleteIfNotPossible，並且無法解毒，則應用程式會根據壓縮檔案類型，刪除感染物件或包含威脅的整個壓縮檔案。 No — 不掃描壓縮檔案。
ScanSfxArchived	僅啟用對 self-extracting archives 的掃描（包含可執行解壓縮模組的壓縮檔案）。	Yes（預設值）— 掃描自解壓縮檔案。 No — 不掃描自解壓縮檔案。
ScanMailBases	啟用掃描 Microsoft Outlook、Outlook Express、The Bat 和其他郵件用戶端的電子郵件資料庫。	Yes — 掃描電子郵件資料庫的檔案。 No（預設值）— 不掃描電子郵件資料庫的檔案。
ScanPlainMail	啟用對 plain text 電子郵件訊息的掃描。	Yes — 掃描純文字電子郵件。 No（預設值）— 不掃描純文字電子郵件。
SizeLimit	要掃描的物件的最大大小（以兆位元組為單位）。如果要掃描的物件大於指定值，應用程式將跳過該物件。	0 至 999999 0 — 應用程式可掃描任意大小的物件。 預設值：0。
TimeLimit	最大物件掃描持續時間（以秒為單位）。如果掃描時間超過此設定指定的時間，應用程式將停止掃描物件。	0 至 9999 0 — 物件掃描時間不受限制。 預設值：0。
QueueScanTasks	如果先前啟動的排程掃描仍在執行，則延遲排程掃描工作。如果目前的掃描持續執行，Kaspersky Endpoint Security 會將排程掃描工作加入佇列。這將有助於最佳化電腦負載。例如，掃描工作排定在 18:00 和 20:00 執行。如果 18:00 的掃描仍在執行，則排定在 20:00 執行的掃描工作會延遲。延遲的工作會在 18:00 的工作完成後執行。	Yes，可在目前的掃描仍在執行時，將排程掃描工作加入佇列。 No（預設值），即使目前的掃描仍在執行，也會執行排程掃描工作。
ActionOnThreat	選取應用程式對感染物件執行的動作。	DisinfectDeleteIfNotPossible（解毒；如果不能解毒則刪除）表示應用程式會先將物件副本儲存在備份中，隨後嘗試對感染物件解毒。如果無法進行解毒（例如，如果無法對該類型的物件或該物件中的威脅類型解毒），則應用程式將刪除感染物件。 DisinfectInformIfNotPossible（解毒；如果無法解毒則告知）表示應用程式會先將物件副本儲存在備份中，隨後嘗試對感染物件解毒。如果無法進行解毒（例如，如果無法解毒該類型的物件或該物件中的威脅類型），則應用程式會在日誌中建立記錄。 Inform 表示應用程式不會嘗試解毒或刪除感染物件。會記錄關於感染物件的資訊。 預設值：DisinfectDeleteIfNotPossible。
UseExcludeMasks	允許從掃描中排除由 ExcludeMasks.item_# 設定指定的物件。	Yes — 從掃描中排除 ExcludeMasks.item_# 設定指定的物件。 No（預設值）— 不從掃描中排除 ExcludeMasks.item_# 設定指定的物件。
ExcludeMasks.item_#	按名稱或遮罩排除掃描物件。您可以使用此設定按名稱從指定的掃描範圍中排除單一檔案，或使用 shell 格式的遮罩一次排除多個檔案。 在為此設定指定值之前，請確保 UseExcludeMasks 設定已啟用。	預設值未定義。 範例 UseExcludeMasks=Yes ExcludeMasks.item_0000=eicar1.* ExcludeMasks.item_0001=eicar2.*

設定	描述	參數值
UseExcludeThreats	啟用從掃描中排除包含 ExcludeThreats.item_# 設定所指定威脅的物件。	Yes — 從掃描中排除包含 ExcludeThreats.item_#設定所指定的威脅的物件。 No（預設值）：不從掃描中排除包含 ExcludeThreats.item_#設定指定的威脅的物件。
ExcludeThreats.item_#	根據偵測到的威脅名稱從掃描中排除物件。在為此設定指定值之前，請確保UseExcludeThreats設定已啟用。 為了從掃描中排除物件，請指定在此物件中偵測到的威脅的全名 — 包含應用程式判定物件被感染的字串。 例如，您可能正在使用公用程式來獲取關於網路的資訊。為了防止應用程式封鎖它，請將其中包含的威脅的全名新增至排除掃描的威脅清單。 您可以在應用程式記錄或網站https://threats.kaspersky.com 中找到在物件中偵測到的威脅的全名。	設定值區分大小寫。 預設值未定義。 範例 UseExcludeThreats=Yes ExcludeThreats.item_0000=EICAR-Test-* ExcludeThreats.item_0001=?rojan.Linux
UseGlobalExclusions	啟用全域排除進行掃描。	Yes（預設值）— 使用全域排除。 No — 不使用全域排除。
UseOASExclusions	啟用檔案威脅防護排除項目進行掃描。	Yes（預設值）— 使用檔案威脅防護排除項目。 No — 不使用檔案威脅防護排除項目。
ReportCleanObjects	啟用記錄關於應用程式報告未被感染的掃描物件的資訊。 例如，您可以啟用此設定，以確保應用程式掃描了特定物件。	Yes — 記錄關於未感染物件的資訊。 No（預設值）— 不記錄關於未感染物件的資訊。
ReportPackedObjects	啟用記錄關於作為複合物件一部分的掃描物件的資訊。 例如，您可以啟用此設定來確保應用程式已掃描壓縮檔案內的物件。	Yes — 記錄關於壓縮檔案中已掃描物件的資訊。 No（預設值）— 不記錄關於檔案中掃描物件的資訊。
ReportUnprocessedObjects	啟用記錄關於由於某種原因尚未處理的物件的資訊。	Yes — 記錄關於未處理物件的資訊。 No（預設值）— 不記錄關於未處理物件的資訊。
UseAnalyzer	啟用啟發式分析。 啟發式分析可以幫助應用程式在病毒分析師發現威脅之前就偵測到威脅。	Yes（預設值）— 啟用啟發式分析器。 No — 停用啟發式分析器。
HeuristicLevel	指定啟發式分析級別。 您可以指定啟發式分析級別。啟發式分析級別可設定威脅搜尋的徹底性、作業系統資源的負載和掃描持續時間之間的平衡。啟發式分析級別越高，掃描所需的資源和時間就越多。	Light — 最不徹底的掃描，系統負載最小。 Medium — 中等啟發式分析級別，系統負載平衡。 Deep — 最徹底的掃描，系統負載最大。 Recommended（預設值）— 建議的值。
UseIChecker	啟用 iChecker 技術。	Yes（預設值）— 啟用 iChecker 技術。 No — 停用 iChecker 技術。
DeviceNameMasks.item_#	裝置名稱清單。應用程式將掃描這些裝置的引導磁區。 設定值不能為空。必須指定至少一個裝置名稱遮罩才能執行此工作。	AllObjects — 掃描所有裝置的引導磁區。 <device name mask> – 掃描名稱與指定遮罩相符的裝置的引導磁區。 預設值：/** — 裝置名稱中的任意一組字元，包括 / 字元。
[ScanScope.item_#] 部分包含以下設定：		
AreaDesc	掃描範圍的描述，包含關於掃描範圍的附加資訊。使用此設定指定的字串的最大長度為 4096 個字元。	預設值：All objects。 範例 AreaDesc="Mail bases scan"
UseScanArea	啟用指定範圍的掃描。若要執行該工作，請啟用至少一個範圍的掃描。	Yes（預設值）— 掃描指定範圍。 No — 不掃描指定範圍。

設定	描述	參數值
AreaMask.item_#	掃描範圍限制。在掃描範圍內，應用程式僅掃描使用 shell 格式的遮罩指定的檔案。 如果未指定此設定，應用程式將掃描掃描範圍內的所有物件。您可以為此設定指定多個值。	預設值為 * （掃描所有物件）。 範例 AreaMask.item_<item number>=*doc
Path	包含要掃描的物件的目錄的路徑。	<path to local directory> – 掃描指定目錄中的物件。預設指定 / 路徑 — 應用程式掃描本機檔案系統的所有目錄。 Shared:NFS — 掃描可透過 NFS 協定存取的裝置檔案系統資源。 Shared:SMB — 掃描可透過 Samba 協定存取的裝置檔案系統資源。 Mounted:NFS — 使用 NFS 協定掃描裝置上安裝的遠端目錄。 Mounted:SMB — 使用 Samba 協定掃描裝置上安裝的遠端目錄。 AllRemoteMounted — 使用 Samba 和 NFS 協定掃描裝置上安裝的所有遠端目錄。 AllShared — 掃描所有可透過 Samba 和 NFS 協定存取的裝置檔案系統資源。 <file system type> – 掃描指定檔案系統裝置的所有資源。
[ExcludedFromScanScope.item_#] 部分包含以下設定：		
AreaDesc	掃描排除範圍的描述，包含關於排除掃描範圍的附加資訊。	預設值未定義。
UseScanArea	從掃描中排除指定的掃描範圍。	Yes （預設值）— 排除指定範圍。 No — 不排除指定的範圍。
AreaMask.item_#	掃描排除項目範圍的限制。在排除範圍中，應用程式僅排除使用 shell 格式的遮罩指定的檔案。 如果未指定此設定，應用程式將排除排除範圍內的所有物件。您可以為此設定指定多個值。	預設值： * （排除所有物件）
Path	包含要排除的物件的目錄的路徑。	<path to local directory> – 從掃描中排除指定目錄（包括子目錄）中的物件。您可以使用遮罩來指定路徑。 為了最佳化掃描工作的運行，建議將系統以唯讀模式掃載的快照路徑新增至具有 btrfs 檔案系統且啟用活動快照的系統的排除項目中。例如，對於基於 SUSE/OpenSUSE 的系統，可以新增以下排除 /.snapshots/*/snapshot/ 。 預設會指定 / 路徑。應用程式將本機檔案系統的所有目錄排除在掃描之外。 Mounted:NFS — 從掃描中排除使用 NFS 協定掃載在裝置上的遠端目錄。 Mounted:SMB — 從掃描中排除使用 Samba 協定安裝在裝置上的遠端目錄。 AllRemoteMounted — 從掃描中排除使用 Samba 和 NFS 協定安裝在裝置上的所有遠端目錄。 <file system type> – 從掃描中排除指定檔案系統裝置的所有資源。 只有當遠端目錄在工作啟動前安裝時，應用程式才會將其排除在掃描範圍之外。工作啟動後裝載的遠端目錄不會被排除在掃描之外。

實用文章

如何指定遮罩

您可以使用`*`（星號）字元來建立檔案或目錄名稱遮罩。

您可以指示單一`*`字元來表示檔案或目錄名稱中`/`字元前面的任意字元集（包括空集）。例如，`/dir/*/file` 或 `/dir/*/*/file`。

您可以用兩個連續的`*`字元來表示檔案或目錄名稱中的任意一組字元（包括空集和`/`字元）。例如，`/dir/**/file*/` 或 `/dir/file**/`。

`**`遮罩在目錄名稱中只能使用一次。例如，`/dir/**/**/file`是一個不正確的遮罩。

您可以使用單一`?`字元來表示檔案或目錄名稱中的任意一個字元。

容器掃描

Kaspersky Endpoint Security 可以即時或按需掃描容器和映像中是否存在惡意軟體。

要使用容器掃描功能，需要包含此功能的授權。

此元件不適用於搭載 Elbrus CPU 的裝置。

容器監控

*容器監控*元件會即時掃描正在執行的容器和命名空間。容器監控元件預設為啟用狀態。

為了使容器監控元件正常運作，必須啟用檔案威脅防護元件。掃描容器和命名空間時套用檔案威脅防護設定。

建議的容器監控設定情境包含以下步驟：

1. **設定應用程式與容器管理工具的整合**

   應用程式支援與Docker 容器管理系統、CRI-O 環境以及 Podman 和 runc 公用程式整合。

2. **建立防護範圍**

   確定您要在其上掃描容器和命名空間的裝置。

3. **在「容器監控」設定中，選取「略過容器」動作**

   當容器中偵測到受感染物件時，Kaspersky Endpoint Security 可以立即停止容器、不採取任何操作，或在證明無法對物件進行解毒或消除威脅時停止容器。選取 **略過容器** 操作以測試該元件。當偵測到受感染物件時，應用程式不會對容器執行任何動作，但會記錄偵測到的威脅相關資訊。

4. **收集容器監控統計資料**

   您可以使用報告取得容器監控統計資料。

5. **選取在偵測到受感染物件時要對容器執行的操作。**

   選擇應用程式偵測到受感染物件時對容器執行的操作。

容器的自訂掃描

應用程式可以隨需掃描容器和映像中的病毒及其他惡意軟體。此操作會使用預定義的*容器掃描 (Container_Scan)* 工作來完成。您可以透過命令列、在網頁主控台或管理主控台中設定預定義工作，或建立用於掃描容器的使用者工作。

應用程式可以同時執行多個容器掃描工作。

建議的容器掃描設定情境包含以下步驟：

1. **設定應用程式與容器管理工具的整合**

   應用程式支援與Docker 容器管理系統、CRI-O 環境以及 Podman 和 runc 公用程式整合。

2. **設定掃描範圍**

   預設情況下，應用程式會掃描受保護裝置上的所有容器。如果只需要掃描個別容器，您可以指定其名稱或名稱遮罩。

3. **在「容器掃描」設定中，選取「略過容器」和「略過映像」動作**

   當容器中偵測到受感染物件時，Kaspersky Endpoint Security 可以立即停止容器、不採取任何操作，或在證明無法對物件進行解毒或消除威脅時停止容器。如果在容器映像中偵測到受感染物件，Kaspersky Endpoint Security 可以刪除容器映像，或不對容器映像採取任何動作。選取 **略過容器** 和 **略過映像** 操作以測試該工作。當偵測到受感染物件時，應用程式不會對容器和映像執行任何動作，但會記錄偵測到的威脅相關資訊。

4. **收集容器掃描統計資料**

   您可以使用報告取得容器掃描統計資料。

5. **最佳化應用程式效能**

   分析收集到的資訊後，最佳化應用程式效能：

   - 新增全域排除項目
   - 新增掃描排除
   - 最佳化容器掃描

6. **選取偵測到受感染物件時要對容器及其映像執行的操作**

   選取應用程式在偵測到受感染物件時對容器及其映像執行的操作。

自訂容器自訂掃描

*自訂容器掃描*工作允許設定及儲存使用下列命令掃描指定容器和映像時使用的設定：

```
kesl-control --scan-container
```

自訂掃描使用預定義工作*Custom_Container_Scan* (ID:19) 中儲存的設定執行。您可以透過編輯此工作的設定來配置自訂容器掃描設定。預設情況下，*自訂容器掃描*工作具有與*容器掃描工作*（ID:18）相同的設定。

該命令會建立並執行暫時工作來掃描容器和映像，並在完成後自動刪除該工作。在這種情況下，掃描結果將輸出到主控台。

特殊考量與限制

- 除非作業系統中安裝了用於處理容器和命名空間的元件，否則應用程式不會掃描命名空間和容器。在這種情況下，命令列上的容器監控元件狀態會顯示為「工作可用但未執行」，而在卡巴斯基安全管理中心中則顯示為「已停止」。
- 只有在應用程式的產品授權包含此功能時，才能選取容器監控操作。

如何配置與容器管理工具的整合

該應用程式支援與 Docker 容器管理系統、CRI-O 環境以及 Podman 和 runc 實用程式進行整合。您可以設定與這些容器管理工具的整合。

如何在網頁主控台中設定與容器管理工具的整合

1. 在網頁主控台的主視窗中，選擇**資產管理** → **政策**。
2. 點擊 Kaspersky Endpoint Security 政策的名稱。

   政策內容視窗將開啟。
3. 選擇“**應用程式設定**”標籤。
4. 前往**一般設定** → **容器掃描設定**。
5. 請確保容器監控元件的切換開關位於 **“監控命名空間和容器”已啟用** 位置。
6. 在”**容器掃描設定**”塊中，點擊”**配置**”按鈕。
7. 這會開啟 **掃描設定** 視窗；在該視窗中，選取受保護裝置的作業系統中已安裝並使用的容器管理工具旁的核取方塊，然後視需要管理設定：
   - **使用 Docker** 核取方塊會啟用 Docker 容器管理系統。預設情況下已選擇此核取方塊。
     - **Docker 通訊端路徑**是用於輸入 Docker 通訊端路徑或 URI（統一資源識別碼）的輸入欄位。預設值：/var/run/docker.sock。

- **使用 CRI-O** 核取方塊會啟用 CRI-O 環境。預設情況下已選擇此核取方塊。
  - **檔案路徑**是用於輸入 CRI-O 設定檔路徑的輸入欄位。預設值：/etc/crio/crio.conf。
- **使用 Podman** 核取方塊會啟用 Podman 實用程式。預設情況下已選擇此核取方塊。
  - **檔案路徑**是用於輸入 Podman 實用程式可執行檔路徑的輸入欄位。預設值：/usr/bin/podman。
  - **根目錄**是用於輸入容器儲存根目錄路徑的輸入欄位。
- **使用 runc** 核取方塊會啟用 runc 實用程式。預設情況下已選擇此核取方塊。
  - **檔案路徑**是用於輸入 runc 實用程式可執行檔路徑的輸入欄位。預設值：/usr/bin/runc。
  - **根目錄**是用於輸入容器狀態儲存根目錄路徑的輸入欄位。預設值：/run/runc。

8. 儲存變更。

如何在命令列中設定與容器管理工具的整合

在命令列中，您可以使用 一般應用程式設定中的 `NamespaceMonitoring=<Yes|No>` 設定來啟用或停用命名空間和容器的即時監控。

您可以使用包含所有一般應用程式設定的設定檔或使用指令列選項編輯設定`NamespaceMonitoring`的值。

使用命令列選項啟用命名空間和容器的監控

```
kesl-control --set-app-settings NamespaceMonitoring=Yes
```

即時掃描命名空間和容器時，會套用 容器掃描設定。您可以使用 Kaspersky Endpoint Security 的特殊管理指令來檢視和編輯這些設定：

- 您可以將容器掃描設定的目前值輸出到主控台或設定檔。您可以使用此檔案來編輯設定。
- 您可以使用包含設定的設定檔編輯所有容器掃描設定。您可以使用用于顯示一般容器掃描設定的指令來取得設定檔。
- 您可以使用 `<setting name>=<setting value>` 格式的命令列選項管理個別設定。您可以使用輸出容器掃描設定的指令來取得設定的目前值。

將容器掃描設定的目前值輸出到主控台

```
kesl-control --get-container-settings [--json]
```

其中，指定 `--json` 以 JSON 格式輸出設定。如果沒有指定`--json`選項，則設定以 INI 格式輸出。

將容器掃描設定的目前值輸出到檔案

```
kesl-control --get-container-settings --file <path to configuration file> [--json]
```

其中：

- `--file <path to configuration file>` 是您要儲存容器掃描設定之檔案的路徑。如果指定檔案的名稱而不指定其路徑，則該檔案會在目前目錄中建立。如果指定路徑中已經存在指定名稱的檔案，則該檔案將被覆寫。如果在磁碟上找不到指定的目錄，則不會建立檔案。
- `--json`被指定以 JSON 格式輸出設定。如果沒有指定`--json`選項，則設定以 INI 格式輸出。

若要使用設定檔修改容器掃描設定的值：

1. 將容器掃描設定輸出到設定檔，如上所述。
2. 編輯檔案中必要參數的值並儲存變更。
3. 執行以下指令：

   ```
   kesl-control --set-container-settings --file <path to configuration file> [--json]
   ```

   其中：

   - `--file <path to configuration file>` 是包含容器掃描設定之設定檔的完整路徑。
   - 如果要從 JSON 設定檔匯入設定，請指定 `--json` 選項。如果未指定 `--json` 選項，應用程式將嘗試從 INI 檔案匯入。如果匯入失敗，則會顯示錯誤。

檔案中指定的所有容器掃描設定值都會匯入應用程式。

使用命令列選項修改容器掃描設定的值

```
kesl-control --set-container-settings <setting name>=<setting value> [<setting name>=<setting value>]
```

其中 `<setting name>=<setting value>` 是 容器掃描設定的名稱和值。

指定的容器掃描設定值已修改。

如何為容器和映像建立自訂掃描範圍

掃描範圍

*掃描範圍*是 Kaspersky Endpoint Security 在執行 *容器掃描* 工作時掃描的容器名稱清單。

預設情況下，*容器掃描* 工作會掃描受防護裝置上的所有容器。如果只需要掃描個別容器，您可以指定其名稱或名稱遮罩。

如何在網頁主控台中建立掃描範圍

1. 在網頁主控台的主視窗中，選擇**工作**。

   工作清單開啟。

2. 在任務清單中，選擇 Kaspersky Endpoint Security 容器掃描任務，然後按一下任務名稱。

   工作內容視窗將開啟。

3. 選擇"**應用程式設定**"標籤。
4. 在 **進階掃描設定** → **容器掃描設定** 下方，於 **名稱遮罩** 欄位中輸入您要掃描之容器的名稱或名稱遮罩。預設情況下，會掃描所有容器。

5. 在 **進階掃描設定 → 映像掃描設定** 下方，於 **名稱遮罩** 欄位中輸入您要掃描之容器映像的名稱或名稱遮罩。預設情況下，會掃描所有映像。

6. 儲存變更。

如何在命令列中建立掃描範圍

1. 使用以下命令設定掃描範圍：

```
kesl-control --set-settings <task ID|name> ScanContainers=Yes ContainerNameMask=<container name or mask>
ScanImages=Yes ImageNameMask=<image name or mask>
```

   其中：

   - `<task ID|name>` 是任務建立時指派的 ID，或是命令列中的任務名稱。
   - `<container name or mask>` 是您要掃描之容器的名稱或名稱遮罩。遮罩以指令 shell 格式指定。您可以使用 `?` 和 `*` 符號。預設情況下，會掃描所有容器。
   - `<image name or mask>` 是您要掃描之映像的名稱或名稱遮罩。遮罩以指令 shell 格式指定。您可以使用 `?` 和 `*` 符號。預設情況下，會掃描所有映像。

2. 您也可以使用設定檔來設定掃描範圍：

   a. 執行以下命令，將任務設定輸出至設定檔：

```
kesl-control --get-settings <task ID|name> [--json]
```

   b. 開啟設定檔進行編輯。

   c. 將以下設定新增至檔案：

   - `ScanContainers=Yes` 會啟用指定容器的掃描。
   - `ContainerNameMask=<container name or mask>` 是您要掃描之容器的名稱或名稱遮罩。遮罩以指令 shell 格式指定。您可以使用 `?` 和 `*` 符號。預設情況下，會掃描所有容器。

- `ScanImages=Yes` 會啟用指定映像的掃描。

- `ImageNameMask=<image name or mask>` 是您要掃描之映像的名稱或名稱遮罩。遮罩以指令 shell 格式指定。您可以使用 `?` 和 `*` 符號。預設情況下，會掃描所有映像。

對名為 `my_container` 的容器執行容器掃描的範例

```
ContainerNameMask=my_container
```

掃描名稱以 `my_container` 開頭之所有容器的範例

```
ContainerNameMask=my_container*
```

對名稱以 `my_` 開頭、接著包含任意五個字元、再接著是 `_container`，並以任意字元序列結尾的所有容器執行容器掃描的範例

```
ContainerNameMask=my_?????_container*
```

對名稱為 `"my_image"` 且標籤為 `"latest"` 的映像執行映像掃描的範例

```
ImageNameMask=my_image:latest
```

對名稱以 `my_image_` 開頭且具有任意標籤的所有映像執行映像掃描的範例

```
ImageNameMask=my_image*
```

d. 儲存設定檔中的變更。

e. 使用以下命令將設定從設定檔匯入至任務：

```
kesl- <task ID|name> --file <path> [--json]
```

其中：

- `<task ID|name>` 是任務建立時指派的 ID，或是命令列中的任務名稱。

- `--file <path>` 是您要從中匯入任務設定之設定檔的完整路徑。

- 如果要從 JSON 設定檔匯入設定，請指定 `--json` 選項。如果未指定 --json 選項，應用程式會嘗試從 INI 檔案匯入。如果匯入失敗，則會顯示錯誤。

檔案中定義的所有任務設定值都將匯入至應用程式。

掃描排除項目

*掃描排除項目*是一組必須符合的條件，以便 Kaspersky Endpoint Security 不會掃描特定物件是否有病毒和其他威脅。掃描排除項目可讓您使用入侵者可以利用來危害電腦或使用者資料的合法應用程式。此類應用程式不一定具有惡意目的，但可能會遭駭客利用。如需入侵者可以利用來危害電腦或使用者資料的合法應用程式詳細資訊，請造訪 卡巴斯基百科全書網站。

您也可以從掃描範圍中排除某些信任的目錄，以最佳化應用程式效能。

可以使用以下方法從掃描中排除物件：

- **依遮罩排除**。輸入含遮罩的檔案名稱。Kaspersky Endpoint Security 輸入遮罩時支援`*`和`?`字元。

  使用遮罩：

  - `*`（星號）字元，可取代任意字元組合，但`\`和`/`字元除外（檔案和目錄路徑中檔案與目錄名稱的分隔符號）。例如，遮罩 `/dir/*/*.txt` 將包含位於 dir 目錄內的目錄中、具有 TXT 副檔名之檔案的所有路徑，但不包含子目錄中的檔案。

  - 兩個連續的`*`字元可取代檔案或目錄名稱中的任意字元組合（包括空集合），包括`\`和`/`字元（檔案和目錄路徑中檔案與目錄名稱的分隔符號）。例如，遮罩 `/dir/**/*.txt` 將包含位於巢狀於 dir 目錄內的目錄中、具有 TXT 副檔名之檔案的所有路徑，但不包含 dir 目錄本身。

  - `?`（問號）字元，可取代任何單一字元，但`\`和`/`字元除外（檔案和目錄路徑中檔案與目錄名稱的分隔符號）。例如，`/dir/???.txt` 遮罩將包含位於 dir 目錄中，具有 TXT 副檔名且名稱由三個字元組成的所有檔案路徑。

- **依威脅名稱排除** 根據 卡巴斯基百科全書 的分類輸入物件類型的名稱（例如`Email-Worm`、`Rootkit`或`RemoteAdmin`）。您可以用`?`字元（替換任何單個字元）和`*`字元（替換任意數量的字元）來使用遮罩。例如，如果指定了`Client*`遮罩，則應用程式將從掃描中排除`Client-IRC`、`Client-P2P`和`Client-SMTP`物件。

Kaspersky Endpoint Security 也允許從掃描中排除特定格式的檔案：封存檔、電子郵件資料庫、文字檔、資料庫記錄檔。

如何在網頁主控台中新增掃描排除項目

1. 在網頁主控台的主視窗中，選擇**工作**。

   工作清單開啟。

2. 在任務清單中，選擇 Kaspersky Endpoint Security 容器掃描任務，然後按一下任務名稱。

   工作內容視窗將開啟。

3. 選擇"**應用程式設定**"標籤。

4. 轉到"**排除範圍**"區域。

5. 如有必要，依遮罩新增排除項目：

   a. 在"**按遮罩排除**"塊中，點擊"**新增**"按鈕。

   b. 這會開啟一個視窗；請在該視窗中指定您希望 Kaspersky Endpoint Security 從掃描中排除之檔案名稱的範本。

   c. 點擊"**新增**"。

   排除項目已新增至清單。

6. 如有必要，依威脅名稱新增排除項目：

   a. 在"**依照威脅名稱排序排除項目**"塊中，點擊"**新增**"按鈕。

   b. 這會開啟一個視窗；請在該視窗中指定威脅名稱的範本。該應用程式不會封鎖指定的威脅。

   例如，如果您使用工具掃描網路，請將該工具的威脅完整名稱新增到要從掃描中排除的威脅清單。

您可以在應用程式記錄或網站https://threats.kaspersky.com 中找到在物件中偵測到的威脅的全名。

7. 如有必要，您可以為每個清單匯入或匯出排除項目：

- 若要匯出排除項目清單，請點擊 **匯出** 按鈕。

  Kaspersky Endpoint Security 會將 export.json 檔案儲存在您的標準下載資料夾中。

- 若要匯入排除項目清單：

  a. 點擊“**匯入**”。

  b. 選取要從中匯入排除範圍的 JSON 檔案。

  c. 開啟檔案。

  d. 選取匯入方法：將排除項目新增至現有清單，或取代排除項目清單。

  e. 儲存變更。

  JSON 檔案中的規則會顯示在清單中。

8. 儲存變更。

如何在命令列新增掃描排除項目

1. 使用以下命令新增排除範圍：

```
kesl-control --set-settings <task ID|name> --add-exclusion <path>
```

其中：

- `<task ID|name>` 是任務建立時指派的 ID，或是命令列中的任務名稱。

- `--add-exclusion <path>` 會新增包含您要排除於掃描之外之物件的目錄路徑。

新的 `[ExcludedFromScanScope.item_#]` 部分將被新增至工作設定中。應用程式會將 `Path` 設定所指定目錄中的物件排除於掃描之外。排除範圍的其餘設定採用預設值。

如果工作設定中已包含具有 `[ExcludedFromScanScope.item_#]` 設定的指定值的 `Path` 部分，則不會新增重複部分。

如果將 `UseScanArea` 設定設為 `No`，則執行此指令後其值將變更為 `Yes`，且位於此目錄中的物件將被排除在掃描之外。

2. 您也可以使用設定檔新增排除範圍：

   a. 執行以下命令，將任務設定輸出至設定檔：

```
kesl-control --get-settings <task ID|name> [--json]
```

   b. 開啟設定檔進行編輯。

c. 將包含以下設定的 `[ExcludedFromScanScope.item_#]` 區段新增至檔案：

- `AreaDesc` – 排除範圍的描述，其中包含關於排除範圍的附加資訊。
- `UseScanArea` 可啟用排除指定的範圍。
- `Path` 是包含要排除物件的目錄路徑。您可以指定本機目錄的路徑或排除用戶端裝置上安裝的遠端目錄。設定的可能值取決於工作的類型。
- `AreaMask.item_#` 是排除範圍的限制。您可以為想要從掃描範圍中排除的檔案的名稱指定一個遮罩。預設情況下，範圍內的所有物件都被排除。

範例

```
[ExcludedFromScanScope.item_0000]
AreaDesc=
UseScanArea=Yes
Path=/tmp/notchecked
AreaMask.item_0000=*
```

d. 您可以指定多個 `[ExcludedFromScanScope.item_#]` 區段。

應用程式按索引的升序處理範圍。

e. 儲存設定檔中的變更。

f. 使用以下命令將設定從設定檔匯入至任務：

```
kesl-control --set-settings <task ID|name> --file <path>
```

3. 如有必要，您可以執行以下命令來刪除排除範圍：

```
kesl-control --set-settings <task ID|name> --del-exclusion <path>
```

其中：

- `<task ID|name>` 是任務建立時指派的 ID，或是命令列中的任務名稱。
- `--del-exclusion <path>` 會移除包含要排除於掃描之外之物件的目錄路徑。

包含指定路徑的 `[ExcludedFromScanScope.item_#]` 區段將從任務設定中刪除。應用程式不會從掃描中排除指定目錄中的物件。

如何最佳化容器掃描

設定檔案掃描，以最佳化任務效能。這有助於降低受保護裝置的 CPU 使用率。您可以限制壓縮檔掃描、設定可掃描物件的大小上限，以及設定物件掃描持續時間上限。Kaspersky Endpoint Security 也允許將特定格式的檔案排除在掃描之外：壓縮檔案、電子郵件資料庫、文字檔案和純文字電子郵件訊息。

如何在網頁主控台中設定檔案掃描

1. 在網頁主控台的主視窗中，選擇**工作**。

工作清單開啟。

2. 在任務清單中，選擇 Kaspersky Endpoint Security 容器掃描任務，然後按一下任務名稱。

   工作內容視窗將開啟。

3. 選擇“**應用程式設定**”標籤。

4. 在 **掃描設定** 下，設定檔案掃描：

   - **掃描壓縮檔案**這包括對 ZIP、GZIP、BZIP、RAR、TAR、ARJ、CAB、LHA、JAR、ICE 和其他類型壓縮檔案的掃描。應用程式不僅透過副檔名，還透過格式來識別壓縮檔案。掃描壓縮檔案時，應用程式會執行遞歸解包。這樣做可以偵測嵌套壓縮檔案（壓縮檔案中的壓縮檔案）中的威脅。預設情況下，掃描處於停用狀態。

   - **掃描 SFX 壓縮檔案**掃描包含可執行解壓縮模組的自解壓縮檔案。預設情況下，掃描處於停用狀態。

   - **掃描郵件資料庫**掃描 Microsoft Outlook、Outlook Express、The Bat! 和其他郵件用戶端的電子郵件資料庫。預設情況下，掃描處於停用狀態。

   - **掃描郵件格式檔案**掃描純文字電子郵件。預設情況下，掃描處於停用狀態。

   - **略過掃描時間超過以下時長的檔案（秒）**最大物件掃描持續時間（以秒為單位）。如果掃描時間超過此設定指定的時間，應用程式將停止掃描物件。預設情況下，應用程式會嘗試在一分鐘內掃描物件。

   - **略過大於以下大小的檔案 (MB)**要掃描的物件的最大大小（以兆位元組為單位）。如果要掃描的物件大於指定值，應用程式將跳過該物件。

   - **略過大於以下大小的檔案 (MB)**如果掃描已經在執行，延遲啟動掃描工作。如果目前掃描繼續，Kaspersky Endpoint Security 將加入佇列新的掃描工作。這將有助於最佳化電腦負載。例如，讓我們假設應用程式已根據排程啟動了一項完整掃描工作。如果使用者嘗試從應用程式介面啟動快速掃描，Kaspersky Endpoint Security 將加入佇列該快速掃描工作，然後在完整掃描工作結束後自動啟動該工作。

5. 儲存變更。

如何在命令列中設定檔案掃描

1. 執行以下指令：

```
kesl --set-settings <task ID|name> ScanArchived=<Yes|No> ScanSfxArchived=<Yes|No> ScanMailBases=<Yes|No>
ScanPlainMail=<Yes|No> SkipPlainTextFiles=<Yes|No> SkipDatabaseJournals=<Yes|No> SizeLimit=<object size (MB)>
TimeLimit=<scan time (sec)> QueueScanTasks=<Yes|No>
```

   其中：

   - `<task ID|name>` 是任務建立時指派的 ID，或是命令列中的任務名稱。

   - `<object size (MB)>` 是要掃描之物件的大小上限（以 MB 為單位）。如果要掃描的物件大於指定值，應用程式將跳過該物件。預設值：`0`。

   - `<scan time (sec)>` 是物件掃描的最長持續時間（以秒為單位）。如果掃描時間超過此設定指定的時間，應用程式將停止掃描物件。預設值：`0`。

2. 您也可以使用設定檔來進行設定：

   a. 執行以下命令，將任務設定輸出至設定檔：

```
kesl-control --get-settings <task ID|name> [--json]
```

b. 開啟設定檔進行編輯。

c. 將以下適用於容器和映像內物件的 *容器掃描* 任務設定新增至此檔案：`ScanArchived`、`ScanSfxArchived`、`ScanMailBases`、`ScanPlainMail`、`SizeLimit`、`TimeLimit`、`QueueScanTasks`。

d. 儲存設定檔中的變更。

e. 使用以下命令將設定從設定檔匯入至任務：

```
kesl-control --set-settings <task ID|name> --file <path> [--json]
```

其中：

- `<task ID|name>` 是任務建立時指派的 ID，或是命令列中的任務名稱。
- `--file <path>` 是您要從中匯入任務設定之設定檔的完整路徑。
- 如果要從 JSON 設定檔匯入設定，請指定`--json`選項。如果未指定`--json`選項，應用程式將嘗試從 INI 檔案匯入。如果匯入失敗，則會顯示錯誤。

檔案中定義的所有任務設定值都將匯入至應用程式。

如何選擇當偵測到受感染物件時要對容器執行的操作

當容器中偵測到受感染物件時，Kaspersky Endpoint Security 可以立即停止容器、不採取任何操作，或在證明無法對物件進行解毒或消除威脅時停止容器。您可以選擇當 *容器監控* 元件進行即時掃描期間，或執行依需求 *容器掃描* 工作期間偵測到受感染物件時，Kaspersky Endpoint Security 對容器執行的操作。

如果在容器映像中偵測到受感染物件，Kaspersky Endpoint Security 可能會刪除該映像，或不對該映像採取任何操作。您可以選擇當執行依需求 *容器掃描* 工作期間偵測到受感染物件時，Kaspersky Endpoint Security 對容器映像執行的操作。

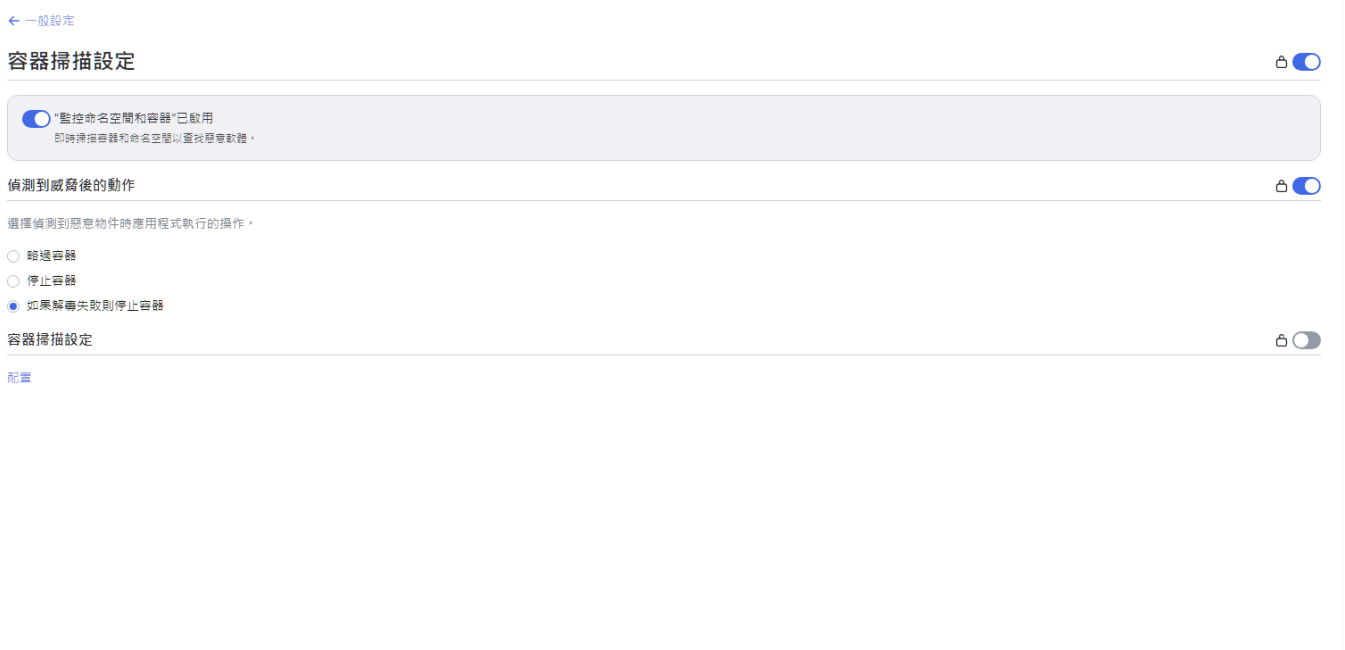
如何在網頁主控台中選擇容器監控的偵測到威脅後的動作

1. 在網頁主控台的主視窗中，選擇**資產管理 → 政策**。
2. 點擊 Kaspersky Endpoint Security 政策的名稱。
   政策內容視窗將開啟。
3. 選擇"**應用程式設定**"標籤。
4. 轉到"**一般設定**"→"**容器掃描設定**"。
5. 請確保容器監控元件的切換開關位於 **"監控命名空間和容器"已啟用** 位置。
6. 在 **偵測到威脅後的動作** 下，選擇當容器中偵測到受感染物件時應用程式將採取的操作：
   - **略過容器**當在容器中偵測到受感染物件時，應用程式不會對容器執行任何動作。
   - **停止容器**當在容器中偵測到受感染物件時，應用程式會停止容器。

- **如果解毒失敗則停止容器**（預設）。當在容器中偵測到受感染物件時，應用程式會嘗試解毒受感染物件。如果受感染物件無法被解毒，應用程式將停止該容器。

> 由於 CRI-O 環境的工作方式，感染物件不會在 CRI-O 環境中的容器中被解毒或刪除。建議選擇**停止容器**動作。

7. 儲存變更。



容器掃描設定

如何在命令列中選擇容器監控的偵測到威脅後的動作

1. 執行以下指令：

```
kesl-control --set-container-settings OnAccessContainerScanAction=<Skip|StopContainer|StopContainerIfFailed>
```

> 只有在使用具備支援此功能的產品授權執行應用程式時，才能配置此設定。

2. 若要檢查容器掃描設定的目前值，請執行下列指令：

```
kesl-control --get-settings container-settings
```

如何在網頁主控台中選擇容器掃描偵測到威脅後的動作

1. 在網頁主控台的主視窗中，選擇**工作**。

   工作清單開啟。

2. 在任務清單中，選擇 Kaspersky Endpoint Security 容器掃描任務，然後按一下任務名稱。

   工作內容視窗將開啟。

3. 選擇"**應用程式設定**"標籤。

4. 在 **進階掃描設定 → 容器掃描設定 → 偵測到威脅後的動作** 下，選擇當容器中偵測到受感染物件時應用程式將執行的動作：

   - **略過容器**當在容器中偵測到受感染物件時，應用程式不會對容器執行任何動作。
   - **停止容器**當在容器中偵測到受感染物件時，應用程式會停止容器。
   - **如果清除失敗則停止容器**（預設）。當在容器中偵測到受感染物件時，應用程式會嘗試解毒受感染物件。如果受感染物件無法被解毒，應用程式將停止該容器。

     > 由於 CRI-O 環境的工作方式，感染物件不會在 CRI-O 環境中的容器中被解毒或刪除。建議選擇**停止容器**動作。

5. 在 **進階掃描設定 → 映像掃描設定 → 偵測到威脅後的動作** 下，選擇當容器中偵測到受感染物件時應用程式將執行的動作：

   - **略過映像**（預設）。當在映像中偵測到受感染物件時，應用程式不會對映像執行任何動作。
   - **刪除映像**（不建議）。當在映像中偵測到受感染物件時，應用程式會刪除映像。所有相依性也將被刪除。正在執行的容器將被停止，然後被刪除。

6. 儲存變更。

如何在命令列中選擇容器掃描偵測到威脅後的動作

1. 執行以下指令：

   ```
   kesl-control --set-settings <task ID|name> ContainerScanAction=<Skip|StopContainer|StopContainerIfFailed>
   ImageAction=<Skip|Delete>
   ```

   其中，`<task ID|name>` 是任務建立時指派的 ID，或是命令列中的任務名稱。

   > 由於 CRI-O 環境的工作方式，感染物件不會在 CRI-O 環境中的容器中被解毒或刪除。建議選擇 `StopContainer` 動作。

2. 您也可以使用設定檔設定該動作：

   a. 執行以下命令，將任務設定輸出至設定檔：

   ```
   kesl-control --get-settings <task ID|name> [--json]
   ```

   b. 開啟設定檔進行編輯。

   c. 將*容器掃描*任務的以下設定新增至檔案：

      - `ContainerScanAction=<Skip|StopContainer|StopContainerIfFailed>` – 當偵測到受感染物件時對容器執行的動作。預設值：`StopContainerIfFailed`。
      - `ImageAction=<Skip|Delete>` – 當偵測到受感染物件時對容器映像執行的動作。預設值：`Skip`。

   d. 儲存設定檔中的變更。

e. 使用以下命令將設定從設定檔匯入至任務：

```
kesl-control --set-settings <task ID|name> --file <path> [--json]
```

其中：

- `<task ID|name>` 是任務建立時指派的 ID，或是命令列中的任務名稱。
- `--file <path>` 是您要從中匯入任務設定之設定檔的完整路徑。
- 如果要從 JSON 設定檔匯入設定，請指定 `--json` 選項。如果未指定 `--json` 選項，應用程式將嘗試從 INI 檔案匯入。如果匯入失敗，則會顯示錯誤。

檔案中定義的所有任務設定值都將匯入至應用程式。

如何對容器和映像執行自訂掃描

若要在命令列上啟動自訂容器掃描工作，請執行下列指令：

```
kesl-control --scan-container <id|name[:tag]>
```

其中 `<id|name[:tag]>` 是容器或映像的名稱或 ID。您可以使用遮罩來掃描多個物件。

如果有多個同名實體，應用程式將掃描所有實體。

執行該指令的結果是建立一個臨時的容器和映像掃描工作，完成後會自動刪除。在這種情況下，掃描結果將輸出到主控台。

對名為 `my_container` 的容器執行容器掃描的範例

```
kesl-control --scan-container my_container
```

對名為 `my_image` 的映像執行映像掃描的範例（所有標籤）

```
kesl-control --scan-container my_image*
```

實用文章

如何指定遮罩

您可以使用 `*`（星號）字元來建立檔案或目錄名稱遮罩。

您可以指示單一 `*` 字元來表示檔案或目錄名稱中 `/` 字元前面的任意字元集（包括空集）。例如，`/dir/*/file` 或 `/dir/*/*/file`。

您可以用兩個連續的 `*` 字元來表示檔案或目錄名稱中的任意一組字元（包括空集和 `/` 字元）。例如，`/dir/**/file*/` 或 `/dir/file**/`。

**遮罩在目錄名稱中只能使用一次。例如，`/dir/**/**/file`是一個不正確的遮罩。

您可以使用單一 ? 字元來表示檔案或目錄名稱中的任意一個字元。

卸除式磁碟機掃描

Kaspersky Endpoint Security 會掃描您執行或複製的所有檔案，即使檔案位於卸除式磁碟機上。應用程式會掃描 CD、DVD、藍光光碟、快閃磁碟機（包括 USB 數據機）、外部硬碟和軟碟片上的檔案。預設情況下，卸除式磁碟機掃描已停用。

卸除式磁碟機掃描的運作方式

連接卸除式磁碟機時，應用程式會自動建立並啟動下列採用預設設定的掃描工作：*關鍵區域掃描* 用於快速掃描，*惡意軟體掃描* 用於詳細掃描。這些工作無法停止。在卸除式磁碟機上偵測到威脅時，Kaspersky Endpoint Security 會嘗試對受感染的物件解毒。如果無法解毒，應用程式會刪除受感染的物件。掃描完成後，應用程式會自動刪除這些工作。

掃描類型

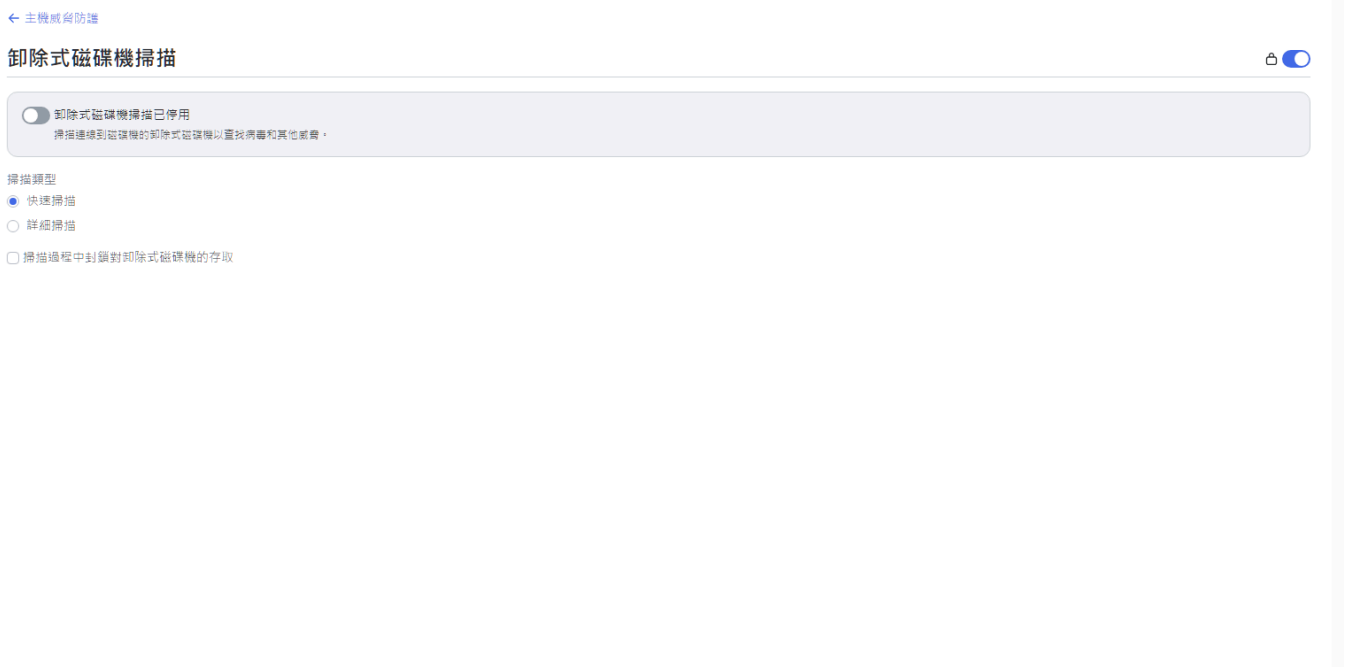
- **快速掃描**Kaspersky Endpoint Security 僅掃描 具有指定副檔名的檔案，且不會解壓縮複合物件。應用程式會使用 *關鍵區域掃描* 工作的預設設定執行快速掃描。
- **詳細掃描**Kaspersky Endpoint Security 會掃描卸除式磁碟機上的所有檔案。應用程式會使用 *惡意軟體掃描* 工作的預設設定執行詳細掃描。

如何在網頁主控台中選擇卸除式磁碟機掃描類型

1. 在網頁主控台的主視窗中，選擇**資產管理 → 政策**。
2. 點擊 Kaspersky Endpoint Security 政策的名稱。
   政策內容視窗將開啟。
3. 選擇“**應用程式設定**”標籤。
4. 轉到”**主機威脅防護**”→”**卸除式磁碟機掃描**”。
5. 確保該元件的切換開關處於 **卸除式磁碟機掃描已啟用** 位置。
6. 在 **掃描類型** 下，選擇卸除式磁碟機掃描的類型：**快速掃描** 或 **詳細掃描**。
7. 如有必要，選中“**掃描期間封鎖對檔案的存取**”核取方塊。
   封鎖對檔案的存取可防止使用者在掃描進行期間執行惡意軟體。

   掃描開機磁區時，應用程式不會封鎖任何檔案。

8. 要將此政策套用到電腦，請關閉... 掛鎖圖示並儲存變更。



卸除式磁碟機掃描

如何在命令列中選擇卸除式磁碟機掃描類型

1. 連接卸除式磁碟機時，選擇要執行的掃描類型：

```
kesl-control --set-settings 16 ScanRemovableDrives=<DetailedScan|QuickScan|NoScan> BlockDuringScan=<Yes|No>
```

2. 插入 CD/DVD 光碟機或藍光光碟時，選擇要執行的掃描類型：

```
kesl-control --set-settings 16 ScanOpticalDrives=<DetailedScan|QuickScan|NoScan> BlockDuringScan=<Yes|No>
```

3. 若要檢查元件設定的目前值，請執行以下命令：

```
kesl-control --get-settings 16
```

符號

命令選項

設定	描述
`ScanRemovableDrives`	連接卸除式磁碟機時的掃描類型： • `DetailedScan`。詳細掃描。 • `QuickScan`。快速掃描。 • `NoScan`（預設）。應用程式不會執行掃描。
`ScanOpticalDrives`	插入 CD/DVD 光碟機或藍光光碟時要執行的掃描類型： • `DetailedScan`。詳細掃描。 • `QuickScan`。快速掃描。 • `NoScan`（預設）。應用程式不會執行掃描。
`BlockDuringScan`	掃描期間封鎖對連接磁碟上檔案的存取。預設情況下，應用程式不會封鎖對檔案的存取。封鎖對檔案的存取可防止使用者在掃描進行期間執行惡意軟體。 掃描開機磁區時，應用程式不會封鎖任何檔案。

行為偵測

行為偵測元件可監控可能危害電腦或使用者資料的應用程式活動（開啟檔案、建立連線等）。該元件會監控應用程式行為，以尋找危險模式。如果應用程式活動符合其中一種模式，Kaspersky Endpoint Security 會執行選定的回應動作。Kaspersky Endpoint Security 的此功能可為電腦提供主動防護。

為了讓行為偵測元件實現最佳效能，建議啟用 Web 威脅防護元件。

行為偵測的運作方式

1. **應用程式會監控作業系統中的事件**

   應用程式會接收由事件組成的遙測串流：處理程序建立與終止、已開啟的檔案、已建立的連線等。應用程式也會為事件補充相關中繼資料（處理程序名稱、PID、IP 位址等）。

2. **應用程式會將遙測串流與危險行為模式進行比較**

   如果第三方應用程式的動作符合危險行為模式，Kaspersky Endpoint Security 會執行威脅回應動作（例如，可以停止第三方應用程式）。

3. **應用程式會將遙測資料傳送至 KSN**

   應用程式會篩選事件，並將這些事件傳送至 KSN 以供進一步分析。

設定行為偵測

1. **在行為偵測設定中，選取「通知」動作**

   預設情況下，行為偵測元件已啟用。在行為偵測設定中，建議選取 **通知** 作為偵測到威脅後的動作，並檢查已安裝的應用程式是否能正常運作。Kaspersky Endpoint Security 允許所有應用程式活動，並保留元件的執行記錄。

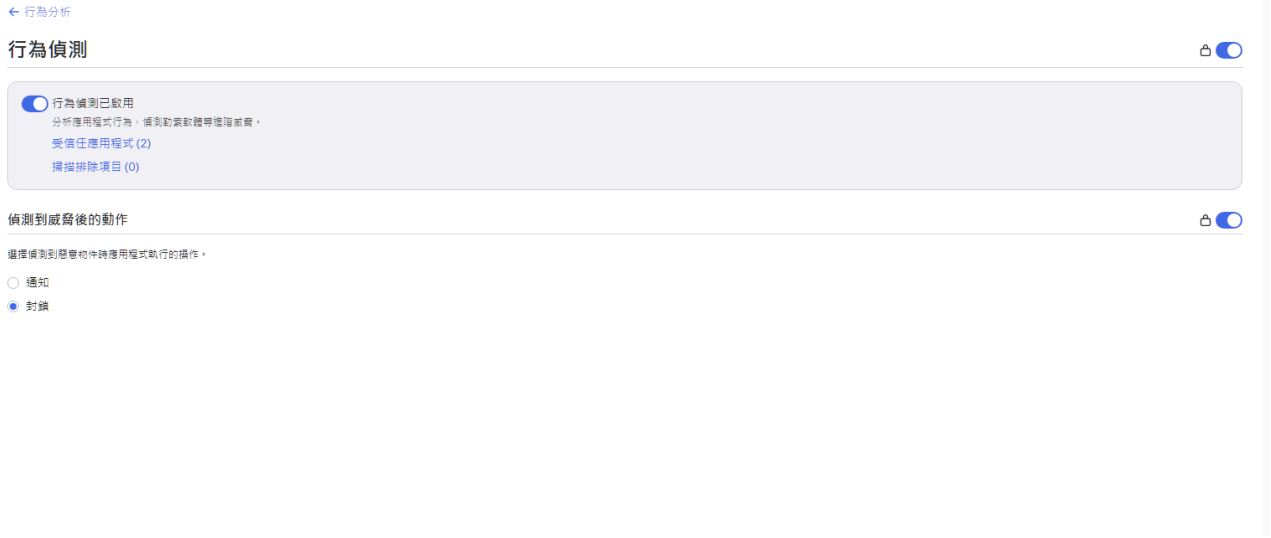
   如何在網頁主控台中選擇偵測到惡意軟體活動時要執行的動作

   1. 在網頁主控台的主視窗中，選擇**資產管理** → **政策**。
   2. 點擊 Kaspersky Endpoint Security 政策的名稱。
      政策內容視窗將開啟。
   3. 選擇"**應用程式設定**"標籤。
   4. 轉到"**主機威脅防護**" → "**行為分析**" → "**行為偵測**"。

5. 在“**偵測到威脅後的動作**”塊中選擇相關操作：

- **通知**如果偵測到惡意活動，Kaspersky Endpoint Security 不會停止此應用程式，而只會在事件記錄中記錄一個關於偵測到惡意活動的事件。
- **封鎖**如果偵測到惡意活動，Kaspersky Endpoint Security 會停止正在執行惡意活動的應用程式處理程序，並記錄有關偵測到的惡意活動的資訊。

6. 要將此政策套用到電腦，請關閉... 掛鎖圖示並儲存變更。



行為偵測

如何在命令列中選擇偵測到惡意軟體活動時要執行的動作

1. 執行以下指令：

```
kesl-control --set-settings 20 TaskMode=<Block|Notify>
```

2. 若要檢查元件設定的目前值，請執行以下命令：

```
kesl-control --get-settings 20
```

符號

命令選項

設定	描述
TaskMode	偵測到惡意軟體活動時要執行的動作： • Block（預設）。如果偵測到惡意活動，Kaspersky Endpoint Security 會停止正在執行惡意活動的應用程式處理程序，並記錄有關偵測到的惡意活動的資訊。 • Notify。如果偵測到惡意活動，Kaspersky Endpoint Security 不會停止此應用程式，而只會在事件記錄中記錄一個關於偵測到惡意活動的事件。

2 收集行為偵測統計資料

您可以使用 報告取得行為偵測統計資料。

3 最佳化應用程式效能

分析收集到的資訊後，最佳化應用程式效能並新增排除項目。

4. **在行為偵測設定中，選取「封鎖」動作**

   啟用對應用程式惡意活動的封鎖。之後，Kaspersky Endpoint Security 將停止正在執行惡意活動的應用程式處理程序。

特殊考量與限制

- 當 Kaspersky Endpoint Security 與 Kaspersky Managed Detection and Response 和 Kaspersky Anti Targeted Attack Platform 解決方案整合時，為了讓行為偵測元件正確運作，請確保在設定檔中將 auditd 設為無設定封鎖模式 `enabled 1`。

弱點利用防禦

弱點利用防禦會監控利用您裝置上的弱點來取得管理員權限或執行惡意動作的程式碼。

若要使弱點利用防禦元件正常運作，必須啟用下列元件：

- 行為偵測
- 可更新的內核模組

> 此元件不適用於搭載 Elbrus CPU 的裝置。

弱點利用防禦的運作方式

1. **應用程式會監控作業系統中的事件**

   應用程式會接收由事件組成的遙測串流：處理程序建立與終止、已開啟的檔案、已建立的連線等。應用程式也會為事件補充相關中繼資料（處理程序名稱、PID、IP 位址等）。

2. **應用程式會將遙測串流與危險行為模式進行比較**

   如果第三方應用程式的動作符合危險行為模式，Kaspersky Endpoint Security 會執行威脅回應動作（例如，可以停止第三方應用程式）。

設定弱點利用防禦

1. **在弱點利用防禦設定中，選取「通知」動作**

   預設情況下，弱點利用防禦元件已停用。在弱點利用防禦設定中，選取**通知**作為偵測到威脅後的動作，並檢查已安裝的應用程式是否能正常運作。Kaspersky Endpoint Security 允許所有應用程式活動，並記錄偵測到的威脅相關資訊。

如何在網頁主控台中選擇偵測到弱點利用後的動作

1. 在網頁主控台的主視窗中，選擇**資產管理** → **政策**。
2. 點擊 Kaspersky Endpoint Security 政策的名稱。
   政策內容視窗將開啟。
3. 選擇"**應用程式設定**"標籤。
4. 轉到"**主機威脅防護**" → "**行為分析**" → "**弱點利用防禦**"。
5. 使用"**弱點利用防禦**"切換開關可啟用或停用元件。
6. 在"**偵測到威脅後的動作**"塊中選擇相關操作：
   - **封鎖**如果選擇此項，在偵測到弱點時，Kaspersky Endpoint Security 會封鎖此弱點的操作，並生成一條包含此弱點相關資訊的日誌項目。
   - **通知**如果選擇此項目，當 Kaspersky Endpoint Security 偵測到弱點利用時，它將記錄一條包含弱點利用資訊的項目並將此弱點利用的相關資訊新增到活動威脅清單。
7. 要將此政策套用到電腦，請關閉... 掛鎖圖示並儲存變更。

如何在命令列中選擇偵測到威脅後的動作

1. 若要啟用弱點利用防禦，請執行下列指令：

```
kesl-control --set-settings 20 UseAEP=Yes
```

2. 選擇偵測到弱點利用後的動作：

```
kesl-control --set-settings 20 AEPMode=<Block|Notify>
```

3. 若要檢查元件設定的目前值，請執行以下命令：

```
kesl-control --get-settings 20
```

符號

命令選項

設定	描述
UseAEP	啟用元件： • Yes 會啟用弱點利用防禦。 • No（預設）會停用「漏洞攻擊防護」。
AEPMode	偵測到弱點利用後的動作： • Block（預設）。Kaspersky Endpoint Security 會封鎖此弱點利用的操作，並建立包含此弱點利用相關資訊的記錄項目。 • Notify。Kaspersky Endpoint Security 偵測到弱點利用時，會建立包含該弱點利用相關資訊的記錄項目，並將此弱點利用的相關資訊新增到活動威脅清單。

2 收集弱點利用防禦統計資料

您可以使用報告取得弱點利用防禦統計資料。

3. **最佳化應用程式效能**

   分析收集到的資訊後，最佳化應用程式效能：

   - 新增全域排除項目
   - 新增排除項目

4. **在弱點利用防禦設定中，選取「封鎖」動作**

   啟用封鎖作業系統中應用程式惡意活動的功能。

Anti-Cryptor

加密軟體防護元件會分析電腦共用網路目錄中遠端裝置的活動，提供遠端加密防護。加密軟體防護會分析透過 NFS 和 SMB 通訊協定傳輸到受防護電腦的檔案。

如果活動與外部加密典型的行為流簽章相符，Kaspersky Endpoint Security 會封鎖此活動或通知您。

加密軟體防護的運作方式

1. **應用程式會攔截 NFS 和 SMB 請求**

   應用程式會接收透過 NFS 和 SMB 通訊協定傳輸之檔案建立和修改相關的遙測資料流。

2. **應用程式會將遙測資料流與簽章資料庫進行比較。**

   如果第三方應用程式的動作與勒索軟體的動作相符，Kaspersky Endpoint Security 會執行所選的偵測到威脅後的動作（例如，封鎖與遠端電腦的連線）。

設定加密軟體防護

1. **設定防護範圍**

   預設情況下，應用程式會掃描所有共用目錄。如果您只需要掃描個別目錄（例如，檔案會從外部來源自動下載到其中的目錄），您可以僅將該目錄指定為防護範圍。在其他情況下，我們建議保留預設防護範圍，並使用排除項目來微調範圍。

2. **在加密軟體防護設定中，選取「通知」動作**

   預設情況下，加密軟體防護處於停用狀態。建議啟用加密軟體防護，並將偵測到威脅後的動作設為**通知**，然後檢查對所有公司資源的存取。Kaspersky Endpoint Security 允許存取共用目錄中的所有資源，並記錄偵測到的威脅相關資訊。

3. **收集加密軟體防護統計資料**

   您可以使用報告取得加密軟體防護統計資料。

4. **最佳化應用程式效能**

分析收集到的資訊後，最佳化應用程式效能：

- 新增全域排除項目。
- 新增排除項目。

5. **在加密軟體防護設定中，選取「封鎖連線」動作**

   啟用封鎖來自遠端攻擊裝置的網路流量。

特殊考量與限制

- 加密軟體防護元件可搭配 SMB1、SMB2、SMB3、NFS3、TCP/UDP 和 IP 通訊協定正常運作。不支援使用 NFS2 和 NFS4 協定。建議設定您的伺服器，使其無法使用 NFS2 和 NFS4 協定掛載資源。
- 若要讓加密軟體防護元件正常運作，必須在作業系統中安裝至少一種服務（Samba 或 NFS）。對於 NFS 服務，必須安裝 rpcbind 套件。
- Kaspersky Endpoint Security 不會阻止對網路檔案資源的存取，除非遠端裝置的活動被識別為惡意。因此，在應用程式偵測到惡意活動之前，至少會有一個檔案被加密。

如何選擇偵測到惡意加密時的操作

如果偵測到惡意加密，應用程式可以封鎖遠端攻擊裝置的網路流量，或僅通知偵測到惡意加密。

若要封鎖網路流量，Kaspersky Endpoint Security 會建立一個動態防火牆規則。防火牆會暫時封鎖攻擊裝置的網路流量。應用程式還會將攻擊裝置新增至已封鎖裝置清單。被封鎖的裝置無法存取共用網路目錄。

若要通知管理員偵測到惡意加密，應用程式會產生 *偵測到加密* 事件。

預設情況下，應用程式會封鎖攻擊裝置的網路流量 60 分鐘。當封鎖時間到期時，應用程式會將受感染的裝置從已封鎖裝置清單中移除，並自動還原該裝置對網路檔案資源的存取權。

您可以在使用者的電腦本機檢視已封鎖裝置清單，並手動解除封鎖這些裝置。除了 *偵測到加密* 事件外，卡巴斯基安全管理中心不提供監控和管理已封鎖裝置的工具。

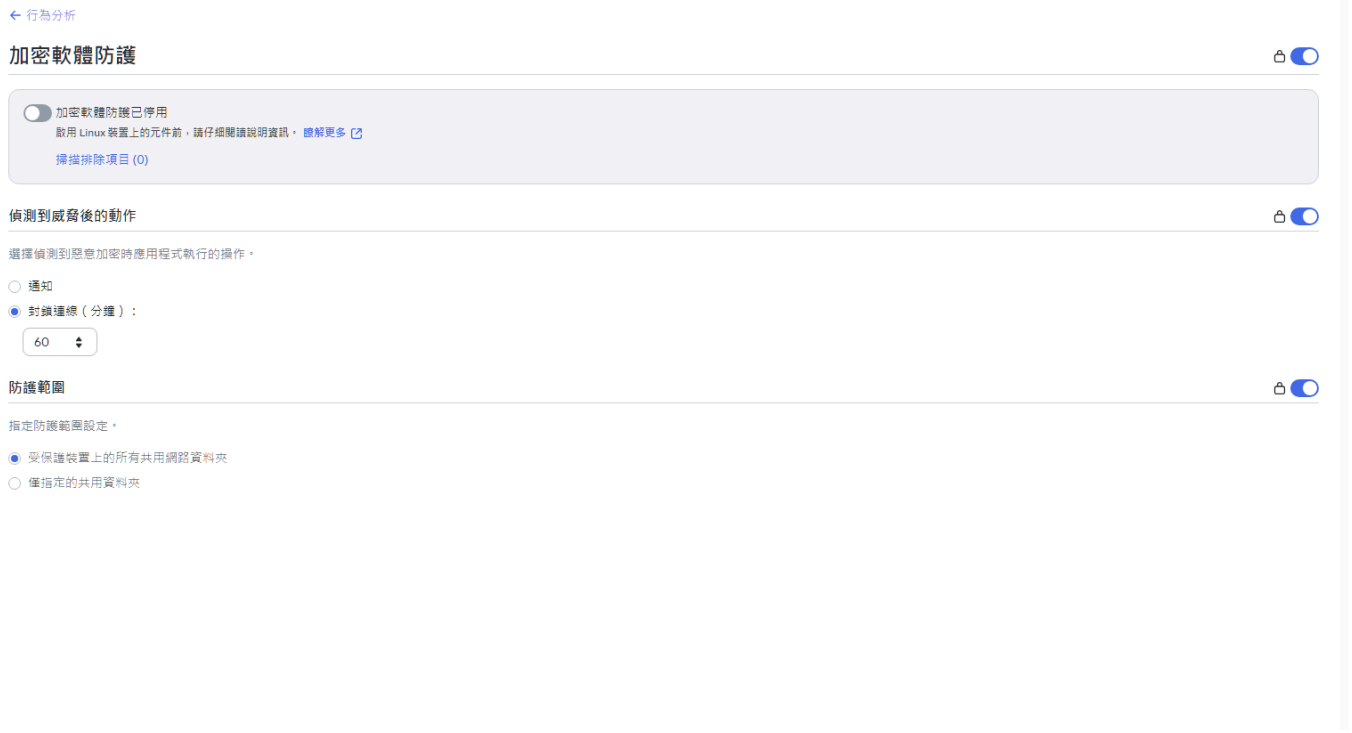
如何在網頁主控台中設定偵測到惡意加密時的動作

1. 在網頁主控台的主視窗中，選擇**資產管理 → 政策**。
2. 點擊 Kaspersky Endpoint Security 政策的名稱。

   政策內容視窗將開啟。
3. 選擇“**應用程式設定**”標籤。
4. 轉到”**主機威脅防護**” → ”**行為分析**” → ”**加密軟體防護**”。
5. 確保該元件的切換開關處於 **加密軟體防護已啟用** 位置。
6. 在 **偵測到威脅後的動作** 下，選取應用程式在偵測到威脅時將採取的動作：**通知** 或 **封鎖連線（分鐘）**。

7. 如果選取 **封鎖連線（分鐘）**，請設定攻擊裝置的封鎖期間（以分鐘為單位）。預設情況下，裝置會被封鎖 60 分鐘。

8. 要將此政策套用到電腦，請關閉... 掛鎖圖示並儲存變更。



Anti-Cryptor

如何在命令列設定偵測到惡意加密時的動作

1. 執行以下指令：

```
kesl-control --set-settings 13 ActionOnDetect=<Block|Notify>
```

2. 選取 `Block` 動作的封鎖期間。

```
kesl-control --set-settings 13 BlockTime=<Blocking period>
```

3. 若要檢查元件設定的目前值，請執行以下命令：

```
kesl-control --get-settings 13
```

符號

命令選項

設定	描述
`ActionOnDetect`	偵測到外部加密時的動作： • `Block`（預設）會封鎖攻擊裝置的網路流量，並建立 *偵測到加密* 事件。 • `Notify` 會建立 *偵測到加密* 事件，而不封鎖網路流量。
`BlockTime`	攻擊裝置的封鎖期間（以分鐘為單位）。

如何建立防護範圍

*防護範圍*是 Kaspersky Endpoint Security 監控檔案活動的共用網路目錄路徑清單。Kaspersky Endpoint Security 輸入遮罩時支援`*`和`?`字元。預設情況下，應用程式會自動識別共用網路目錄，並監控這些目錄中的檔案活動。

如有必要，您可以將惡意加密的檔案活動監控限制為部分目錄。Kaspersky Endpoint Security 依照範圍清單中出現的順序掃描指定範圍內的物件。如果有必要，將子目錄放在清單中高於其父目錄的位置，以便為子目錄配置與父目錄的安全性設定不同的安全性設定。

如果您的組織在透過共用網路目錄交換檔案時使用資料加密，從防護範圍中排除目錄可減少誤報數量。例如，當使用者在共用資料夾中處理具有 ENC 副檔名的檔案時，加密軟體防護可能會產生誤報。此類活動比對外部加密通常有的行為模式。如果您在共用網路目錄中有加密檔案以防護資料，請將該目錄新增到排除項目。

如何在網頁主控台中建立防護範圍

1. 在網頁主控台的主視窗中，選擇**資產管理 → 政策**。
2. 點擊 Kaspersky Endpoint Security 政策的名稱。
   政策內容視窗將開啟。
3. 選擇“**應用程式設定**”標籤。
4. 轉到”**主機威脅防護**” → ”**行為分析**” → ”**加密軟體防護**”。
5. 確保該元件的切換開關處於 **加密軟體防護已啟用** 位置。
6. 在**防護範圍**下面，選擇**僅指定的共用資料夾**。
7. 在目錄清單中，點擊 **新增**。
8. 這會開啟一個視窗；在該視窗中，選取檔案系統類型：
   - **本機**不需網路連線即可存取的硬碟目錄。
   - **已共用**可透過 Samba (SMB) 或 NFS 通訊協定存取的電腦目錄。
   - **所有共用**透過 Samba 和 NFS 通訊協定存取的所有電腦目錄。
9. 對於本機檔案系統，請指定目錄路徑（例如，`/path/to/folder`）。
10. 指定物件副檔名的遮罩（例如，`*.txt`）。使用逗號分隔遮罩。
11. 要將此政策套用到電腦，請關閉... 掛鎖圖示並儲存變更。

如何在命令列建立防護範圍

1. 執行以下指令：

```
kesl-control --set-settings 13 ScanScope.item_#.UseScanArea=Yes \
        [ScanScope.item_#.AreaDesc=<description of the area>] \
        [ScanScope.item_#.AreaMask.item_#=<mask in shell format>] \
        [ScanScope.item_#.Path=<path to the directory>]
```

2. 若要檢查元件設定的目前值，請執行以下命令：

```
kesl-control --get-settings 13
```

符號

命令選項

設定	描述
`ScanScope.item_#.UseScanArea=Yes`	啟用防護範圍編號 `#`。 您可以暫時排除防護範圍，而不是將其刪除。若要這麼做，請設定 `ScanScope.item_#.UseScanArea=No`。
`ScanScope.item_#.AreaDesc`	防護範圍的描述；包含關於 `#` 防護範圍的其他資訊。
`ScanScope.item_#.AreaMask.item_#`	防護範圍限制。在防護範圍內，應用程式僅防護使用 shell 格式的遮罩指定的物件。 範例 `ScanScope.item_0001.AreaMask.item_0001=*.exe ScanScope.item_0001.AreaMask.item_0002=*.txt.`
`ScanScope.item_#.Path`	要防護的物件所在的目錄的路徑。可能的值： • `AllShared`（預設）。透過 Samba 和 NFS 通訊協定存取的所有電腦目錄。 • `Shared:SMB`。可透過 Samba (SMB) 通訊協定存取的目錄。 • `Shared:NFS`。可透過 NFS 通訊協定存取的目錄。 • `<path to local directory>`。不需網路連線即可存取的硬碟目錄。Kaspersky Endpoint Security 輸入遮罩時支援 `*` 和 `?` 字元。

僅包含 `/home` 目錄的防護範圍範例

```
kesl-control --set-settings 13 ScanScope.item_0001.UseScanArea=Yes ScanScope.item_0001.Path=/home
```

BadUSB 攻擊防護

攻擊者可以利用 USB 裝置（例如隨身碟）韌體中的弱點，重新編寫該裝置的程式，使作業系統在連接時將此裝置辨識為鍵盤。因此，受感染的 USB 裝置可能會以您的使用者帳戶執行命令，例如下載惡意軟體。

BadUSB 攻擊防護元件可防止受感染的 USB 裝置連接。

> 此元件不適用於搭載 Elbrus CPU 的裝置。

BadUSB 攻擊防護的運作方式

1. **應用程式會提示您授權 USB 裝置**

   當 USB 裝置連接到裝置時，應用程式會提示使用者輸入應用程式產生的數字代碼。此程序稱為 *授權*。

2. **使用者輸入授權碼**

   使用者可以使用所連接的 USB 裝置本身（鍵盤或條碼掃描器）或螢幕小鍵盤（如果可用）輸入代碼。您無法使用已連接的 USB 裝置輸入代碼。

3. **應用程式允許已授權的 USB 裝置連接，並封鎖未授權的 USB 裝置**

   如果正確輸入數字代碼，應用程式會將識別參數，也就是 USB 裝置的 VID/PID 及其連接的連接埠號碼，儲存在已授權 USB 裝置清單中。如果重新連接此 USB 裝置或重新啟動作業系統，則無需再次授權此 USB 裝置。

   如果輸入的數字代碼錯誤，應用程式將產生一個新代碼。您可以設定輸入數字代碼的最大嘗試次數。如果多次輸入錯誤的數字代碼，應用程式會在一段時間內封鎖來自此 USB 裝置的輸入。等待 USB 裝置鎖定時間結束後，您可以再次嘗試授權 USB 裝置。您可以設定經過多久後可以繼續嘗試輸入授權碼。

當已授權的 USB 裝置連接到不同的 USB 連接埠時，應用程式會要求重新授權該裝置。

設定 BadUSB 攻擊防護

1. **啟用 BadUSB 攻擊防護**

   預設情況下， BadUSB 攻擊防護元件處於停用狀態。識別不受信任人士可實體存取且需要防範外部攻擊者的裝置，並在這些裝置上啟用 BadUSB 攻擊防護元件。啟用 BadUSB 攻擊防護後，應用程式將要求授權已連接的 USB 裝置，使用者在授權前將無法使用未授權的 USB 裝置。不過，在啟用 BadUSB 攻擊防護之前已連接的 USB 裝置預設會視為已授權，無需授權。

   在啟用並設定 BadUSB 攻擊防護之前，請勿將任何不受信任的 USB 裝置連接到該裝置。

2. **設定 BadUSB 攻擊防護**

   根據所連接的 USB 裝置類型（鍵盤或條碼掃描器），設定授權碼的顯示方式：以條碼或數字代碼（預設設定）顯示。

   如有必要，請設定 USB 裝置授權：

   - 輸入授權碼的最大嘗試次數
   - 達到最大嘗試次數時 USB 裝置的封鎖持續時間。

如何設定 USB 裝置授權

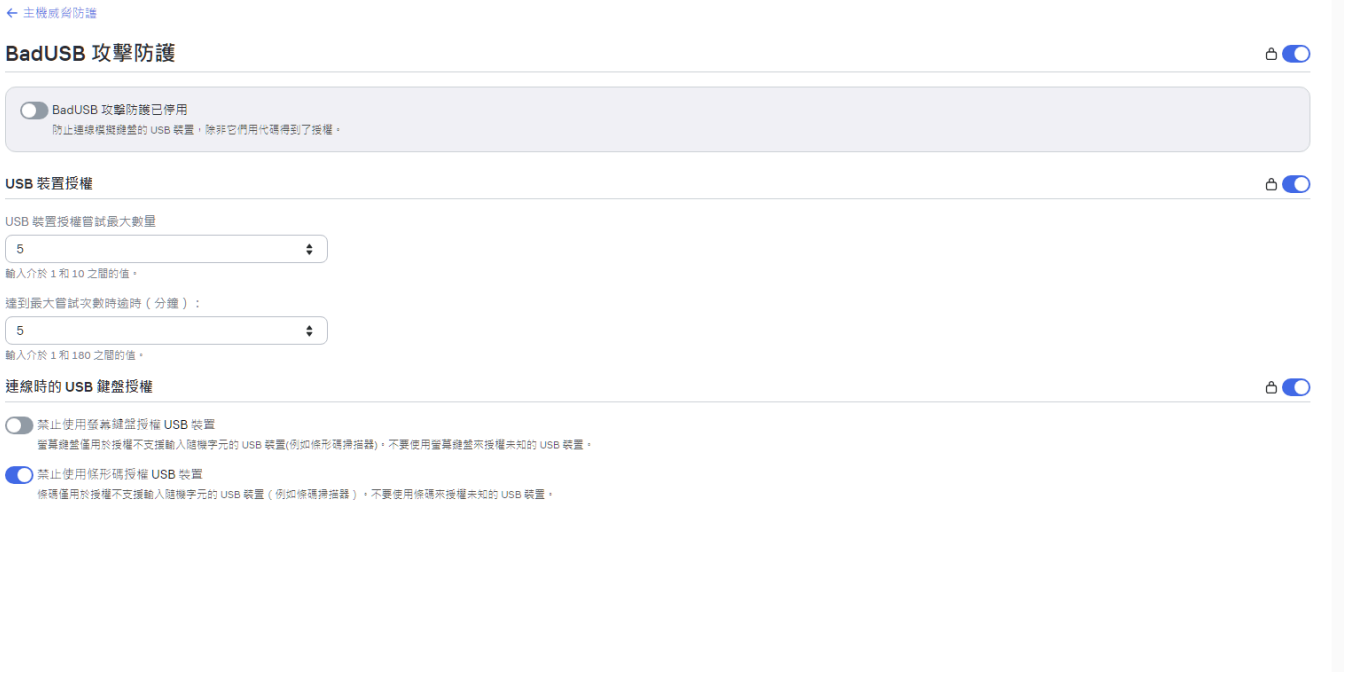
當作業系統識別為輸入裝置的 USB 裝置連線到受管理裝置時，應用程式會建議使用數字代碼或條碼授權該 USB 裝置。如果授權碼輸入錯誤，應用程式會產生新的代碼。如果授權碼多次輸入錯誤，或授權視窗遭關閉，應用程式會封鎖來自此 USB 裝置的輸入。當 USB 裝置封鎖時間到期或作業系統重新啟動時，應用程式會提示使用者再次執行授權。

Kaspersky Endpoint Security 可讓您設定 USB 裝置授權

- 最大授權嘗試次數。
- 達到最大嘗試次數時 USB 裝置的封鎖持續時間。

如何在網頁主控台中設定 USB 裝置授權

1. 在網頁主控台的主視窗中，選擇**資產管理 → 政策**。
2. 點擊 Kaspersky Endpoint Security 政策的名稱。
   政策內容視窗將開啟。
3. 選擇“**應用程式設定**”標籤。
4. 轉到”**主機威脅防護**”→”**BadUSB 攻擊防護**”。
5. 確保該元件的切換開關處於 **BadUSB 攻擊防護已啟用** 位置。
6. 在 **USB 裝置授權** 下，設定授權設定：
   - **USB 裝置授權嘗試最大數量**如果授權碼輸入錯誤達到指定次數，則自動封鎖 USB 裝置。有效值為 1 到 10。例如，如果您允許嘗試輸入授權碼五次，則應用程式會在第五次嘗試失敗後封鎖 USB 裝置。Kaspersky Endpoint Security 會顯示 USB 裝置被封鎖的時間。該時間經過後，您將再一次有 5 次嘗試輸入授權碼。
   - **達到最大嘗試次數時逾時（分鐘）**在指定次數的授權碼輸入失敗後，USB 裝置被封鎖的持續時間。可選值：1 到 180（分鐘）。
7. 要將此政策套用到電腦，請關閉... 掛鎖圖示並儲存變更。



BadUSB 攻擊防護

如何在命令列中設定 USB 裝置授權

1. 執行以下指令：

```
kesl-control --set-settings 37 MaxAuthAttempts=<number of attempts> TimeoutAfterAttempts=<timeout (minutes)>
```

2. 若要檢查元件設定的目前值，請執行以下命令：

```
kesl-control --get-settings 37
```

符號

命令選項

設定	描述
`MaxAuthAttempts`	如果授權碼輸入錯誤達到指定次數，則自動封鎖 USB 裝置。有效值為 1 到 10。例如，如果您允許嘗試輸入授權碼五次，則應用程式會在第五次嘗試失敗後封鎖 USB 裝置。Kaspersky Endpoint Security 會顯示 USB 裝置被封鎖的時間。該時間經過後，您將再一次有 5 次嘗試輸入授權碼。 預設值：5。
`TimeoutAfterAttempts`	在指定次數的授權碼輸入失敗後，USB 裝置被封鎖的持續時間。可選值：1 到 180（分鐘）。 預設值：5分鐘。

如何允許使用螢幕小鍵盤連接 USB 裝置

應當僅在 USB 裝置授權不支援輸入隨機字元時（例如條碼掃描器）使用螢幕鍵盤授權。不建議使用螢幕鍵盤授權未知的 USB 裝置。預設允許使用螢幕鍵盤。

建議僅使用螢幕鍵盤來授權使用者已知的 USB 裝置。

如何在網頁主控台中啟用使用螢幕鍵盤進行 USB 裝置授權

1. 在網頁主控台的主視窗中，選擇**資產管理 → 政策**。
2. 點擊 Kaspersky Endpoint Security 政策的名稱。
   政策內容視窗將開啟。
3. 選擇"**應用程式設定**"標籤。
4. 轉到"**主機威脅防護**"→"**BadUSB 攻擊防護**"。
5. 確保該元件的切換開關處於 **BadUSB 攻擊防護已啟用** 位置。
6. 請確保 **禁止使用螢幕鍵盤授權 USB 裝置** 切換開關已關閉。預設情況下，切換按鈕關閉。
7. 若要將政策套用到裝置，請關閉 掛鎖圖示並儲存變更。

如何在指令列中啟用使用螢幕鍵盤進行 USB 裝置授權

執行命令：

```
kesl-control --set-settings 37 ProhibitOnScreenKeyboard=No
```

如何允許使用條碼掃描器連接 USB 裝置

當將條碼掃描器連線到裝置時，BadUSB 攻擊防護元件會將此掃描器識別為輸入裝置，並提示您執行授權。若要授權條碼掃描器，您必須掃描螢幕上顯示的條碼。應用程式會產生 Code39 格式的條碼。大多數條碼掃描器和 QR 碼掃描器均支援此格式。

應用程式也支援另一種授權條碼掃描器的方式。如果您使用觸控螢幕裝置，則可以使用螢幕鍵盤輸入代碼。為此，您需要 允許使用螢幕鍵盤。例如，對於收銀機內建的固定條碼掃描器，這種方法很方便。禁止使用其他條碼掃描器授權方法。預設情況下，應用程式不會使用條碼來授權 USB 裝置。

如何在網頁主控台中使用條碼掃描器啟用 USB 裝置授權

1. 在網頁主控台的主視窗中，選擇**資產管理 → 政策**。
2. 點擊 Kaspersky Endpoint Security 政策的名稱。
   政策內容視窗將開啟。
3. 選擇"**應用程式設定**"標籤。
4. 轉到"**主機威脅防護**"→"**BadUSB 攻擊防護**"。
5. 確保該元件的切換開關處於 **BadUSB 攻擊防護已啟用** 位置。
6. 停用 **禁止使用條形碼授權 USB 裝置** 切換開關。
7. 若要將政策套用到裝置，請關閉 掛鎖圖示並儲存變更。

如何在命令列上使用條碼掃描器啟用 USB 裝置授權

執行命令：

```
kesl-control --set-settings 37 ProhibitBarcodeScanner=No
```

通訊與 Web 防護

郵件威脅防護

郵件威脅防護元件會掃描收發電子郵件的附件，以偵測病毒和其他威脅性應用程式。此元件使用病毒資料庫、卡巴斯基安全網路雲端服務和啟發式分析來保護裝置。

郵件威脅防護可以掃描收件和寄件。應用程式支援下列郵件用戶端中的 POP3、SMTP 和 IMAP：應用程式也支援延伸版本的通訊協定：POP3S、SMTPS 和 IMAPS。

如果在瀏覽器中開啟郵件用戶端，"郵件威脅防護"元件不會掃描郵件。

> 若要郵件威脅防護元件正常運作，必須在網路設定中監控網路連接埠 25、110、143、465、587、993 和 995。這些網路連接埠預設已被新增至受監控連接埠清單。從清單中移除這些連接埠可能會導致元件無法正常運作。

郵件威脅防護元件預設已啟用。

郵件威脅防護的運作方式

安裝 Kaspersky Endpoint Security 時，應用程式會新增自我簽署憑證 *卡巴斯基病毒防護個人根憑證*。應用程式會將此憑證放置在本機信任的憑證存放區 (`/etc/ssl/certs`)。每次應用程式啟動時，都會檢查該憑證是否存在。如果憑證已被刪除，應用程式會自動還原該憑證。

1. **應用程式攔截郵件流量**

   Kaspersky Endpoint Security 會透過 POP3、SMTP 和 IMAP 通訊協定檢查連線。

2. **應用程式會掃描傳入和傳出郵件**

   郵件威脅防護使用下列技術掃描流量：

   - 病毒資料庫。
   - 卡巴斯基安全網路的雲端服務。
   - 啟發式分析技術可偵測卡巴斯基資料庫尚未涵蓋的威脅。

3. **應用程式完成掃描**

   如果傳入郵件的附件或郵件本文包含威脅，Kaspersky Endpoint Security 會執行偵測到威脅後的動作。如果在傳出郵件中偵測到威脅，郵件威脅防護會封鎖此郵件的傳送。

設定郵件威脅防護

1. **定義用於元件測試部署的群組**

   劃分出一小組裝置，用於測試郵件威脅防護元件的設定。這可讓您確認元件設定正確，並確保郵件用戶端穩定運作，避免可能的故障。

2. **設定附件篩選器**

   預設情況下，由卡巴斯基設定的郵件威脅防護篩選器會提供建議的防護等級。如果您對郵件安全性有特殊需求，可以變更附件篩選器設定。

3. **設定郵件掃描**

   如有必要，請根據郵件伺服器的參數設定電子郵件掃描。例如，您可以限制掃描的封存檔大小，以降低郵件伺服器的負載。

4. **確認郵件威脅防護是否正常運作**

   產生一封含有惡意附件的測試郵件。將郵件傳送到您選取的裝置群組，並確認郵件中的惡意內容已依照元件設定進行處理。

   您也可以執行下列指令，確認應用程式已產生對應的 *偵測到威脅* 事件：

   ```
   kesl-control -E -q "TaskName == 'Mail_Monitoring'"
   ```

5. **將郵件威脅防護設定套用至組織中的所有裝置**

特殊考量與限制

- 如果受防護裝置上的郵件用戶端未使用受信任憑證的本機儲存區，請手動將 *卡巴斯基病毒防護個人根憑證* 憑證新增至郵件用戶端的受信任憑證儲存區。如需新增憑證的詳細資訊，請參閱郵件用戶端的官方文件。

- 郵件威脅防護不會嘗試解毒傳出郵件中的惡意附件。含有惡意附件的傳出郵件會被完全封鎖或允許通過。

偵測到郵件威脅時該怎麼辦

如果在*傳出郵件*的附件中偵測到受感染物件，應用程式會阻止該郵件傳送。

如果在*傳入郵件*中偵測到受感染物件，應用程式可以嘗試解毒該物件，然後刪除該物件或封鎖對該物件的存取。Kaspersky Endpoint Security 也會將關於已執行動作的資訊新增至郵件主旨，例如，*[郵件已處理] <郵件主旨>*。

設定郵件威脅防護時，您可以選取在電子郵件中偵測到威脅時 Kaspersky Endpoint Security 將執行的動作。

如何在網頁主控台中設定偵測到威脅時的動作

1. 在網頁主控台的主視窗中，選擇**資產管理 → 政策**。

2. 點擊 Kaspersky Endpoint Security 政策的名稱。

   政策內容視窗將開啟。

3. 選擇"**應用程式設定**"標籤。

4. 轉到"**通訊與 Web 防護**"→"**郵件威脅防護**"。

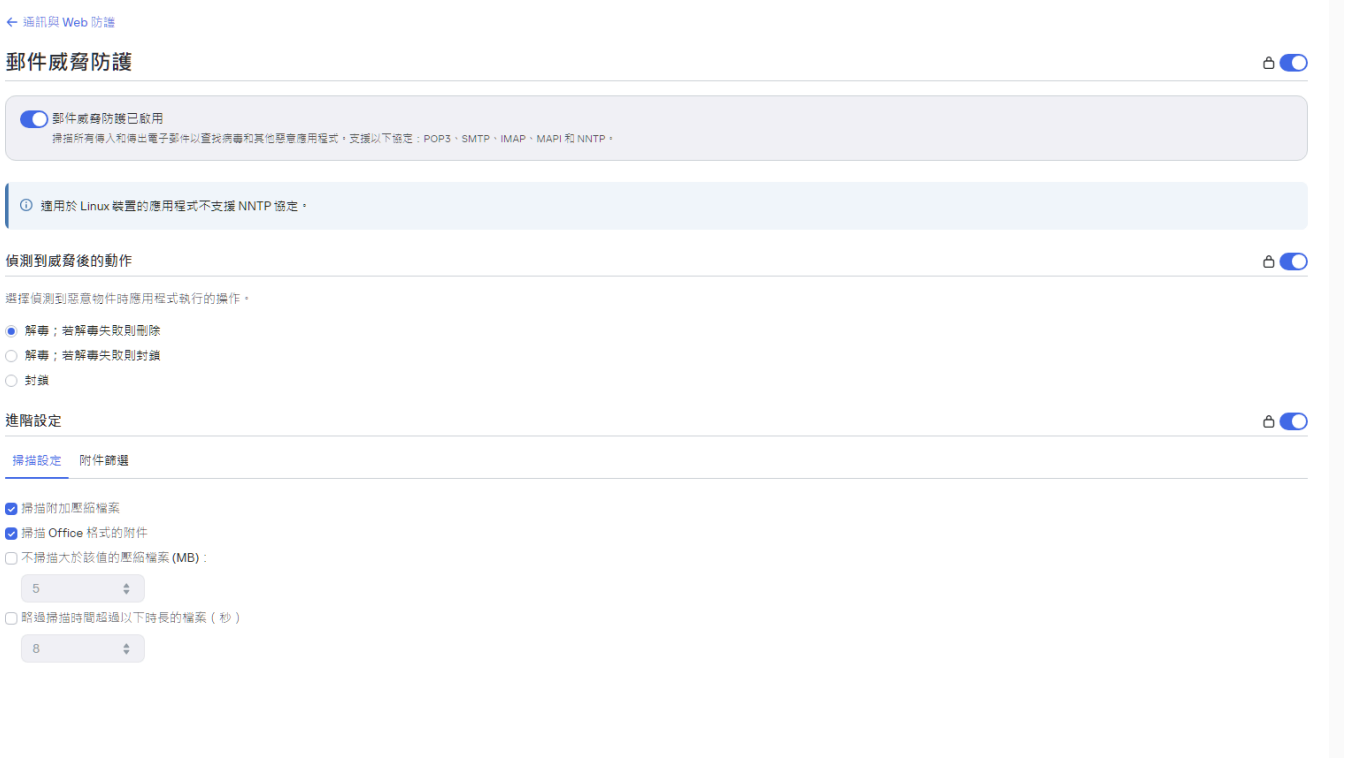
5. 在 **偵測到威脅後的動作** 下，選擇偵測到威脅時應用程式將執行的動作：

   - **解毒；若解毒失敗則刪除**當在傳入的郵件中偵測到感染物件時，應用程式會嘗試對偵測到的感染物件進行解毒。然後，帶有安全附件的郵件將被提供給使用者。如果解毒失敗，應用程式將刪除受感染的物件。應用程式會將有關已執行操作的資訊新增至郵件主旨中，例如：*[郵件已處理] <郵件主旨>*。如果在傳出郵件中偵測到感染物件，應用程式會封鎖該郵件，郵件用戶端將顯示錯誤。

   - **解毒；若解毒失敗則封鎖**當在傳入的郵件中偵測到感染物件時，應用程式會嘗試對偵測到的感染物件進行解毒。然後，帶有安全附件的郵件將被提供給使用者。如果解毒失敗，應用程式會在郵件主旨中新增警告。然後，帶有原始附件的郵件將被提供給使用者。如果在傳出郵件中偵測到感染物件，應用程式會封鎖該郵件，郵件用戶端將顯示錯誤。

   - **封鎖**如果在收到的郵件中偵測到受感染的對象，應用程式會在郵件主旨中新增警告。然後，帶有原始附件的郵件將被提供給使用者。如果在傳出郵件中偵測到感染物件，應用程式會封鎖該郵件，郵件用戶端將顯示錯誤。

6. 要將此政策套用到電腦，請關閉... 掛鎖圖示並儲存變更。



郵件威脅防護

如何在命令列中設定偵測到威脅時的動作

1. 請確定郵件威脅防護元件已啟用：

```
kesl-control --get-task-state 35
```

元件必須處於 **已啟動** 狀態。

2. 如果元件已停用，請執行下列命令：

```
kesl-control --start-task 35
```

3. 選取偵測到傳入郵件中的郵件威脅時要執行的動作：

```
kesl-control --set-settings 35 ActionOnThreat=<DisinfectDeleteIfNotPossible|DisinfectBlockIfNotPossible|Block>
```

4. 若要檢查元件設定的目前值，請執行以下命令：

```
kesl-control --get-settings 35
```

符號

設定	描述
`ActionOnThreat`	偵測到威脅後的動作： • `DisinfectDeleteIfNotPossible`（預設）。當在傳入的郵件中偵測到感染物件時，應用程式會嘗試對偵測到的感染物件進行解毒。然後，帶有安全附件的郵件將被提供給使用者。如果解毒失敗，應用程式將刪除受感染的物件。應用程式會將有關已執行操作的資訊新增至郵件主旨中，例如：*[郵件已處理]<郵件主旨>*。如果在傳出郵件中偵測到感染物件，應用程式會封鎖該郵件，郵件用戶端將顯示錯誤。 • `DisinfectBlockIfNotPossible`。當在傳入的郵件中偵測到感染物件時，應用程式會嘗試對偵測到的感染物件進行解毒。然後，帶有安全附件的郵件將被提供給使用者。如果解毒失敗，應用程式會在郵件主旨中新增警告。然後，帶有原始附件的郵件將被提供給使用者。如果在傳出郵件中偵測到感染物件，應用程式會封鎖該郵件，郵件用戶端將顯示錯誤。 • `Block`。如果在收到的郵件中偵測到受感染的對象，應用程式會在郵件主旨中新增警告。然後，帶有原始附件的郵件將被提供給使用者。如果在傳出郵件中偵測到感染物件，應用程式會封鎖該郵件，郵件用戶端將顯示錯誤。

如何最佳化電子郵件附件掃描

設定電子郵件附件掃描，以最佳化郵件威脅防護元件。這有助於降低受保護裝置的 CPU 使用率。您可以限制掃描附加的封存檔、設定可掃描附件的大小上限，以及設定物件掃描持續時間上限。

如何在網頁主控台中最佳化附件掃描

1. 在網頁主控台的主視窗中，選擇**資產管理 → 政策**。
2. 點擊 Kaspersky Endpoint Security 政策的名稱。
   政策內容視窗將開啟。
3. 選擇"**應用程式設定**"標籤。
4. 轉到"**通訊與 Web 防護**"→"**郵件威脅防護**"。
5. 在**進階設定**下，選擇**掃描設定**標籤。
6. 設定附件掃描：
   - **掃描附加壓縮檔案**這包括對 ZIP、GZIP、BZIP、RAR、TAR、ARJ、CAB、LHA、JAR、ICE 和其他類型壓縮檔案的掃描。應用程式不僅透過副檔名，還透過格式來識別壓縮檔案。掃描壓縮檔案時，應用程式會執行遞歸解包。這樣做可以偵測嵌套壓縮檔案（壓縮檔案中的壓縮檔案）中的威脅。
   - **掃描 Office 格式的附件**掃描 Microsoft Office 檔案（DOC，DOCX，XLS，PPT 和其他 Microsoft 副檔名）。Office 格式檔案也包含 OLE 物件。無論是否選取此核取方塊，應用程式都會掃描小於 1 MB 的 Office 格式附件。
   - **不掃描大於該值的壓縮檔案 (MB)**如果選取此核取方塊，郵件威脅防護將不會掃描任何大於指定限制的壓縮檔案附件。如果清除此核取方塊，郵件威脅防護將掃描任何大小的壓縮檔案附件。
   - **略過掃描時間超過以下時長的檔案（秒）**如果勾選此核取方塊，則會限制附加到電子郵件的壓縮檔案的掃描持續時間。
7. 要將此政策套用到電腦，請關閉... 掛鎖圖示並儲存變更。

如何在命令列中最佳化附件掃描

1. 請確定郵件威脅防護元件已啟用：

```
kesl-control --get-task-state 35
```

2. 元件必須具有 `Started` 狀態。

3. 如果元件已停用，請執行下列命令：

```
kesl-control --start-task 35
```

4. 選取偵測到傳入郵件中的郵件威脅時要執行的動作：

```
kesl-control --set-settings 35 [ScanFileArchive=<Yes|No>] [UseSizeLimit=<Yes|No>] [SizeLimit=<archive size
(MB)>] [UseTimeLimit=<Yes|No>] [TimeLimit=<scan time (sec)>] [ScanFileOffice=<Yes|No>]
```

5. 若要檢查元件設定的目前值，請執行以下命令：

```
kesl-control --get-settings 35
```

符號

命令選項

設定	描述
`ScanFileArchive`	這包括對 ZIP、GZIP、BZIP、RAR、TAR、ARJ、CAB、LHA、JAR、ICE 和其他類型壓縮檔案的掃描。應用程式不僅透過副檔名，還透過格式來識別壓縮檔案。掃描壓縮檔案時，應用程式會執行遞歸解包。這樣做可以偵測嵌套壓縮檔案（壓縮檔案中的壓縮檔案）中的威脅。預設情況下，應用程式會掃描附加的封存檔。
`UseSizeLimit` `SizeLimit`	限制可掃描之附加封存檔的大小。如果附加封存檔的大小超過指定值，郵件威脅防護在掃描時會跳過該封存檔。預設情況下，應用程式會掃描任意大小的封存檔。
`UseTimeLimit` `TimeLimit`	掃描附加封存檔的時間限制。預設情況下，附加封存檔的掃描時間不受限制。
`ScanFileOffice`	掃描 Microsoft Office 檔案（DOC，DOCX，XLS，PPT 和其他 Microsoft 副檔名）。Office 格式檔案也包含 OLE 物件。無論是否選取此核取方塊，應用程式都會掃描小於 1 MB 的 Office 格式附件。預設情況下，應用程式會掃描附加的 Office 格式檔案。

電子郵件附件篩選器的用途

附件篩選器不適用於發出的電子郵件。

惡意應用程式會以電子郵件附件的形式傳播。您可以根據郵件附件類型設定篩選，指定類型的檔案可以被自動重新命名或刪除。透過重新命名某種類型的附件，Kaspersky Endpoint Security 可以防護您的電腦，防禦惡意應用程式的自動執行。

例如，您可以為 HTML 檔案設定附件篩選。HTML 檔案可能包含惡意指令碼。如果應用程式重新命名此類檔案，使用者將無法在電子郵件訊息中按兩下 HTML 頁面來開啟它。若要開啟 HTML 檔案，使用者需要下載該檔案並重新命名。這可讓使用者有時間分析收到的訊息，並防止惡意指令碼啟動。

預設情況下，應用程式會重新命名副檔名為 CMD、COM、EXE、JS、JSE、MSI、SCR、VBE、VBS、SH 的檔案。應用程式會將指定檔案類型副檔名的最後一個字元取代為底線字元（例如 attachment.doc_）。

如何在網頁主控台中設定附件篩選器

1. 在網頁主控台的主視窗中，選擇**資產管理 → 政策**。
2. 點擊 Kaspersky Endpoint Security 政策的名稱。
   政策內容視窗將開啟。
3. 選擇“**應用程式設定**”標籤。
4. 轉到”**通訊與 Web 防護**”→”**郵件威脅防護**”。
5. 在**進階設定**下，選擇**附件篩選**標籤。
6. 選取應用程式將對電子郵件附件執行的動作：
   - **不修改附件**如果選擇此選項，郵件威脅防護將不會篩選電子郵件附件。
   - **重新命名選取類型的附件**如果選擇此選項， 郵件威脅防護會將指定檔案類型（例如 attachment.doc_）的副檔名最後一個字元替換為下劃線字元。因此，使用者需要重命名檔案才能開啟它。
   - **刪除選取類型的附件**如果選擇此選項， 郵件威脅防護會從電子郵件中刪除指定類型的附件。
7. 如果您在上一步驟選取了 **重新命名選取類型的附件** 或 **刪除選取類型的附件** 選項，請選取相關檔案類型的核取方塊。
8. 如果您需要的檔案類型未列出，請新增附件類型：
   a. 點擊“**新增**”。
      這會開啟用於新增附件類型的表單。
   b. 在 **附件類型** 欄位中，以 `*.<extension>`（例如 `*.doc`）格式指定副檔名遮罩。
      如果要指定多個檔案類型，請在新的一行輸入每個檔案類型。
9. 要將此政策套用到電腦，請關閉... 掛鎖圖示並儲存變更。

如何在命令列設定附件篩選器

1. 請確定郵件威脅防護元件已啟用：

```
kesl-control --get-task-state 35
```

2. 元件必須具有 `Started` 狀態。
3. 如果元件已停用，請執行下列命令：

```
kesl-control --start-task 35
```

4. 選取應用程式將對電子郵件附件執行的動作：

```
kesl-control --set-settings 35 ExtensionFilter=<Disable|Rename|Delete>
ExtensionMasks.item_#.UseExtensionMask=Yes\
[ExtensionMasks=*.<extention>]
```

5. 若要檢查元件設定的目前值，請執行以下命令：

```
kesl-control --get-settings 35
```

符號

命令選項

設定	描述
`ExtensionFilter`	應用程式將對電子郵件附件執行的動作： `Disable`。如果選擇此選項，郵件威脅防護將不會篩選電子郵件附件。 `Rename`（預設）。如果選擇此選項， 郵件威脅防護會將指定檔案類型（例如 attachment.doc_）的副檔名最後一個字元替換為下劃線字元。因此，使用者需要重命名檔案才能開啟它。 `Delete`。如果選擇此選項， 郵件威脅防護會從電子郵件中刪除指定類型的附件。
`UseExtensionMask=Yes`	將檔案類型新增至附件篩選器。 您可以暫時從附件篩選器中排除檔案類型，而不是移除該檔案類型。若要這麼做，請設定 `ExtensionMasks.item_#.UseExtensionMask=No`
`ExtensionMasks=*.<extention>`	您要重新命名或從電子郵件訊息中移除的附件類型副檔名。

Web 威脅防護

Web 威脅防護元件可防止從網際網路下載惡意檔案，並封鎖與惡意網站和釣魚網站的連線。此元件借助防毒資料庫、卡巴斯基安全網路雲端服務和啟發式分析提供電腦防護。

Web 威脅防護的運作方式

安裝 Kaspersky Endpoint Security 時，應用程式會新增自我簽署憑證 *卡巴斯基病毒防護個人根憑證*。應用程式會將此憑證放置在本機受信任的憑證存放區 (`/etc/ssl/certs`) 以及網頁瀏覽器的憑證存放區中。每次應用程式啟動時，都會檢查該憑證是否存在。如果憑證已被刪除，應用程式會自動還原該憑證。

1. **攔截傳出連線**

   第三方應用程式（例如瀏覽器）會起始與伺服器的連線。Kaspersky Endpoint Security 會將伺服器憑證取代為自己的憑證，該憑證使用卡巴斯基病毒防護個人根憑證簽署。接著，應用程式會攔截加密金鑰並解密通訊工作階段。Kaspersky Endpoint Security 會在不向使用者發出警示的情況下執行此操作，因為卡巴斯基病毒防護個人根憑證位於受信任的憑證存放區中。

2. **掃描網路流量**

   Web 威脅防護使用下列技術掃描流量：

   - 病毒資料庫。
   - 卡巴斯基安全網路的雲端服務。
   - 啟發式分析技術可偵測卡巴斯基資料庫尚未涵蓋的威脅。

3. **掃描完成**

   如果網站被分類為惡意網站或網路釣魚網站，Kaspersky Endpoint Security 會執行 Web 威脅防護元件設定中指定的操作：封鎖連線或顯示警告。

Web 威脅防護設定

1. **設定作業系統的防火牆規則**

   如果系統有自己的網路規則或 firewalld 規則，且這些規則包含 Drop 政策，則為確保應用程式正常運作，您需要新增規則，以允許來自本機裝置（回送）的傳入連線：

   iptables 的範例命令：

   ```
   iptables -A INPUT -i lo -j ACCEPT
   ```

2. **選取網路流量攔截模式**

   收到網路封包時，Web 威脅防護會擷取資料以掃描威脅。網路流量攔截可使用下列模式：

   - eBPF
   - iptables（預設）

   網路流量攔截模式的選擇取決於組織的基礎架構。在封閉邊界中，建議使用 eBPF。在其他情境下，請使用 iptables。

   > 我們建議根據網路流量攔截模式，將裝置分組到不同的管理群組。

3. **設定憑證驗證政策**

   預設情況下，Web 威脅防護會解密並掃描透過加密連線傳送的網路流量。在此期間，元件可以使用網際網路進行驗證，並下載驗證憑證所需的缺失鏈。如果裝置無法直接存取網際網路，則必須選取本機憑證驗證方法（不使用網際網路）或使用代理伺服器存取網際網路。

   憑證驗證政策還包括下列設定：

   - 存取含有不受信任憑證的網站
   - 存取發生憑證驗證錯誤的網站

   預設情況下，Kaspersky Endpoint Security 允許瀏覽含有不受信任憑證的網站，並將發生憑證驗證錯誤的網域新增至排除項目。例如，使用銀行應用程式或雲端儲存時，可能會發生憑證驗證錯誤。這些服務所屬的網域可能會拒絕卡巴斯基病毒防護個人根憑證。您可以設定自己的憑證驗證政策。

4. **新增受信任憑證**

   如果您的組織使用私人憑證授權單位為內部伺服器發行憑證，Kaspersky Endpoint Security 可能會因憑證驗證錯誤而封鎖 Web 資源的存取。將這些憑證新增至受信任清單，以將 Web 資源從加密連線掃描中排除。

5. **在 Web 威脅防護設定中，選取「通知」動作**

   預設情況下，Web 威脅防護工作被停用。建議啟用 Web 威脅防護，並將偵測到威脅後的動作設為**通知**，然後檢查對所有公司資源的存取。Kaspersky Endpoint Security 允許存取所有網站，並記錄偵測到的威脅相關資訊。

6. **收集 Web 威脅防護視為不安全之網站的統計資料**

   您可以使用報告取得 Web 威脅防護視為不安全的網站統計資料。

7 **新增受信任的網址**

檢閱 Web 威脅防護報告後，您需要將您信任的網址新增至受信任清單。如果受信任網址清單不足以解決 Kaspersky Endpoint Security 應用程式與第三方應用程式之間的衝突，則可以使用特殊的允許規則鏈 kesl_bypass。*kesl_bypass 鏈*是 Kaspersky Endpoint Security 在作業系統防火牆 (iptables/ip6tables) 的 mangle 表中建立的特殊規則清單。

8 **在 Web 威脅防護設定中，選取「封鎖」動作**

啟用封鎖網路流量中的受感染物件。

特殊考量與限制

- 應用程式會掃描 TCP 連接埠的傳入流量，並使用 localhost 上的連接埠 9879 攔截連線。如果連接埠 9879 正在使用中，應用程式會自動選擇可用的連接埠來攔截連線。
- 啟用或停用應用程式，以及啟用或停用 Web 威脅防護和網路威脅防護元件，會終止被攔截連接埠上的連線。
- Kaspersky Endpoint Security 會掃描 HTTP 和 HTTPS 流量。Kaspersky Endpoint Security 掃描 URL 和 IP 位址。
- 應用程式支援下列瀏覽器可執行檔，包括 snap 格式的可執行檔：
  - chrome
  - chromium
  - chromium-browser
  - firefox
  - firefox-esr
  - google-chrome
  - opera
  - yandex-browser
- 如果使用者嘗試造訪惡意網站，應用程式會執行下列操作：
  - **HTTP**。應用程式會封鎖存取並顯示警告。
  - **HTTPS**。應用程式會封鎖存取；瀏覽器會顯示錯誤頁面。
- 刪除應用程式憑證可能會導致 Web 威脅防護元件無法正常運作。

實用文章

收到「造訪具有不受信任憑證的網域」警告時該怎麼做

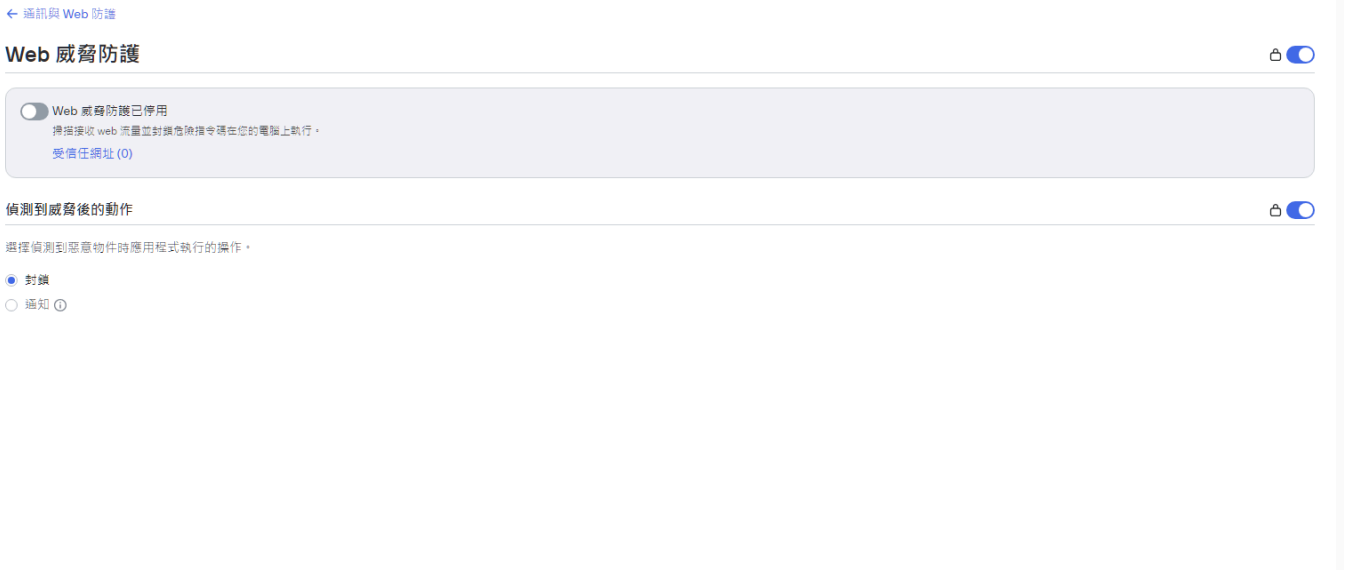
如何在偵測到 Web 威脅時選擇操作

偵測到 Web 威脅時，Kaspersky Endpoint Security 可以封鎖對危險物件的存取，或僅通知偵測到危險物件。

如何在網頁主控台中設定偵測到 Web 威脅時的動作

1. 在網頁主控台的主視窗中，選擇**資產管理 → 政策**。
2. 點擊 Kaspersky Endpoint Security 政策的名稱。

   政策內容視窗將開啟。
3. 選擇"**應用程式設定**"標籤。
4. 轉到"**通訊與 Web 防護**"→"**Web 威脅防護**"。
5. 在 **偵測到威脅後的動作** 下，選擇偵測到威脅時應用程式將執行的動作：
   - **封鎖**如果選擇此選項並且在 Web 流量中偵測到受感染物件，"Web 威脅防護"元件將封鎖存取物件並在瀏覽器中顯示一條訊息。
   - **通知**Kaspersky Endpoint Security 在 Web 流量中偵測到受感染物件時，會通知使用者。Web 威脅防護會允許將此物件下載到裝置。同時，應用程式會記錄受感染物件的相關資訊，並將其新增至活躍威脅清單。
6. 要將此政策套用到電腦，請關閉... 掛鎖圖示並儲存變更。



Web 威脅防護

如何在命令列中設定偵測到威脅時的動作

1. 執行以下指令：

```
kesl-control --set-settings 14 ActionOnDetect=<Block|Notify>
```

2. 選擇要用於掃描連結的資料庫：

```
kesl-control --set-settings 14 CheckMalicious=<Yes|No> CheckAdware=<Yes|No> CheckOther=<Yes|No>
```

3. 若要檢查元件設定的目前值，請執行以下命令：

```
kesl-control --get-settings 14
```

符號

命令選項

設定	描述
ActionOnDetect	偵測到威脅後的動作： • Block（預設）。如果選擇此選項並且在 Web 流量中偵測到受感染物件，“Web 威脅防護”元件將封鎖存取物件並在瀏覽器中顯示一條訊息。 • Notify。如果選擇此選項，且在 Web 流量中偵測到受感染物件，Kaspersky Endpoint Security 會允許將此物件下載到電腦，但會將受感染物件的相關資訊新增到活動威脅清單中。
CheckMalicious	掃描連接以確定它們是否包含在惡意網址資料庫中，可以讓您追蹤被新增到拒絕清單的網站。惡意網址資料庫由 Kaspersky 維護，包含在程式安裝套件中，並透過 Kaspersky Endpoint Security 資料庫更新進行補充。預設情況下啟用掃描（Yes）。
CheckAdware	根據廣告網址資料庫檢查連結。預設情況下停用掃描（No）。
CheckOther	根據包含入侵者可以利用的合法應用程式的網址資料庫檢查連結，這些應用程式可能會用來入侵裝置或資料。預設情況下停用掃描（No）。

什麼是釣魚防護

Web 威脅防護可檢查連接來查看他們是否屬於網路釣魚網址。這有助於防範“*釣魚攻擊*”。釣魚攻擊常常帶有偽裝，比如從您銀行發來的帶有銀行官方網站連結的電子郵件訊息。點擊此連結，您將進入銀行網站的完整複製網站，甚至可以在瀏覽器位址欄看到其真實位址，即使您在假網站上。從此刻起，您在網站上的所有操作都將被追蹤，進而用來竊取您的金錢。

由於釣魚網站的連結不僅能透過電子郵件訊息傳送，而且還可能來自其他來源（比如即時訊息軟體），因此“Web 威脅防護”元件將在 Web 流量掃描等級監視您存取釣魚網站的操作並封鎖您存取此類網站。Kaspersky Endpoint Security 分發套件中包含釣魚網址清單。

> 您只能透過命令列設定釣魚防護功能。您無法在網頁主控台中設定釣魚防護。預設啟用使用啟發式分析進行網路釣魚防護。

如何透過命令列啟用釣魚防護

1. 請確保 Web 威脅防護元件已啟用：

   ```
   kesl-control --get-task-state 14
   ```

   元件必須處於 **已啟動** 狀態。

2. 如果元件已停用，請執行下列命令：

   ```
   kesl-control --start-task 14
   ```

3. 啟用釣魚防護：

   ```
   kesl-control --set-settings 14 CheckPhishing=Yes
   ```

4. 設定用於掃描網頁中釣魚連結的啟發式分析：

```
kesl-control --set-settings 14 UseHeuristicForPhishing=<Yes|No>
```

此設定不適用於配備 Elbrus CPU 的裝置。

5. 若要檢查元件設定的目前值，請執行以下命令：

```
kesl-control --get-settings 14
```

網路威脅防護

*網路威脅防護*元件（也稱為Intrusion Detection System，IDS）會監控入站網路流量，以偵測具網路攻擊特徵的活動。當應用程式偵測到在使用者電腦上有網路攻擊企圖時，它將封鎖與攻擊電腦的連線。應用程式資料庫提供目前已知類型的網路攻擊以及應對方法。"網路威脅防護"元件偵測到的網路攻擊清單在資料庫和應用程式模組更新期間更新。

網路威脅防護的運作方式

1. **應用程式分析傳入封包**

   為掃描傳入流量，網路威脅防護元件會從應用程式資料庫接收連接埠號碼，並透過所有這些連接埠接受連線。在 iptables 流量攔截模式下進行網路掃描程序期間，裝置上的連接埠可能看似為開放狀態，即使系統上沒有任何應用程式正在監聽該連接埠。建議使用 防火牆關閉未使用的連接埠。

2. **應用程式掃描傳入流量**

   網路威脅防護使用以下技術掃描傳入流量：

   - 病毒資料庫。
   - 卡巴斯基安全網路的雲端服務。
   - 啟發式分析技術可偵測卡巴斯基資料庫尚未涵蓋的威脅。

3. **掃描完成**

   偵測到網路威脅時，應用程式會在指定時間內封鎖來自攻擊裝置的所有網路連線。

網路威脅防護設定

1. **設定作業系統的防火牆規則**

   若要確保 REDIRECT 規則（例如，從連接埠 443 重新導向到 8443）與網路威脅防護的攔截規則相容，您需要刪除 REDIRECT 規則並新增攔截規則。

   刪除 REDIRECT 規則的命令範例：

   ```
   iptables -t nat -D PREROUTING -p tcp -m tcp --dport 443 -j REDIRECT --to-ports 8443
   ```

   新增攔截規則的命令範例：

   ```
   iptables -t nat -A PREROUTING -p tcp -m tcp --dport 443 -m mark ! --mark 0x400/0x400 -j REDIRECT --to-ports 8443
   ```

   ```
   iptables -t nat -A OUTPUT -p tcp --dport 443 -m mark --mark 0x400/0x400 -m addrtype ! --src-type LOCAL -j DNAT -
   -to-destination :8443
   ```

2. **建立受監控網路連接埠的清單**

   預設情況下，應用程式會監控已知和已註冊的連接埠，例如 HTTPS 連線的連接埠 443，以及 IMAP 郵件協定的連接埠 143。預設設定提供建議的防護等級和最佳資源使用。如有必要，您可以變更受監控連接埠清單或啟用所有連接埠的監控。

3. **選擇流量攔截模式**

   收到網路封包時，網路威脅防護會擷取資料以掃描威脅。可使用以下模式攔截傳入流量：

   - eBPF
   - iptables（預設）

   流量攔截模式的選擇取決於組織的基礎架構。在封閉邊界中，建議使用 eBPF。在其他情境下，請使用 iptables。

   建議根據流量攔截模式將裝置分組到不同的管理群組。

4. **在通知模式下啟用 Web 威脅防護**

   預設情況下，網路威脅防護處於停用狀態。在以封鎖模式啟用網路威脅防護之前，建議以通知模式啟用該元件。這可讓 Kaspersky Endpoint Security 偵測可疑的網路活動，並記錄有關偵測到的網路攻擊的資訊，而不會中斷網路連線。檢查第三方企業應用程式對網路資源的存取權。確保網路連接埠控制不會降低這些應用程式的速度。

5. **收集網路威脅防護偵測到可疑網路活動來源 IP 位址的統計資訊**

   您可以檢閱 報告，以取得網路威脅防護認為不安全的 IP 位址統計資訊。應用程式會產生 *偵測到網路攻擊* 事件。

6. **新增受信任的 IP 位址**

   檢閱網路威脅防護報告後，您需要將您信任其網路連線的裝置 IP 位址新增至受信任清單。您可以將個別裝置或子網路的位址新增至排除清單。網路威脅防護不會攔截或掃描來自此類裝置的封包。

7 **以封鎖模式啟用網路威脅防護**

將受信任裝置的 IP 位址新增至排除清單後，以封鎖模式啟用該元件。不受信任裝置的網路活動會遭到封鎖，相關資訊會顯示在報告中。

特殊考量與限制

- 應用程式會掃描 TCP 連接埠的傳入流量。應用程式會使用 localhost 上的固定連接埠 9789 來攔截連線。
- 啟用或停用應用程式，以及啟用或停用 Web 威脅防護和網路威脅防護元件，會終止被攔截連接埠上的連線。
- 由於不支援 TProxy，網路威脅防護在執行 CentOS 5.2 和 5.4 的電腦上無法運作。

如何選擇偵測到網路威脅時的動作

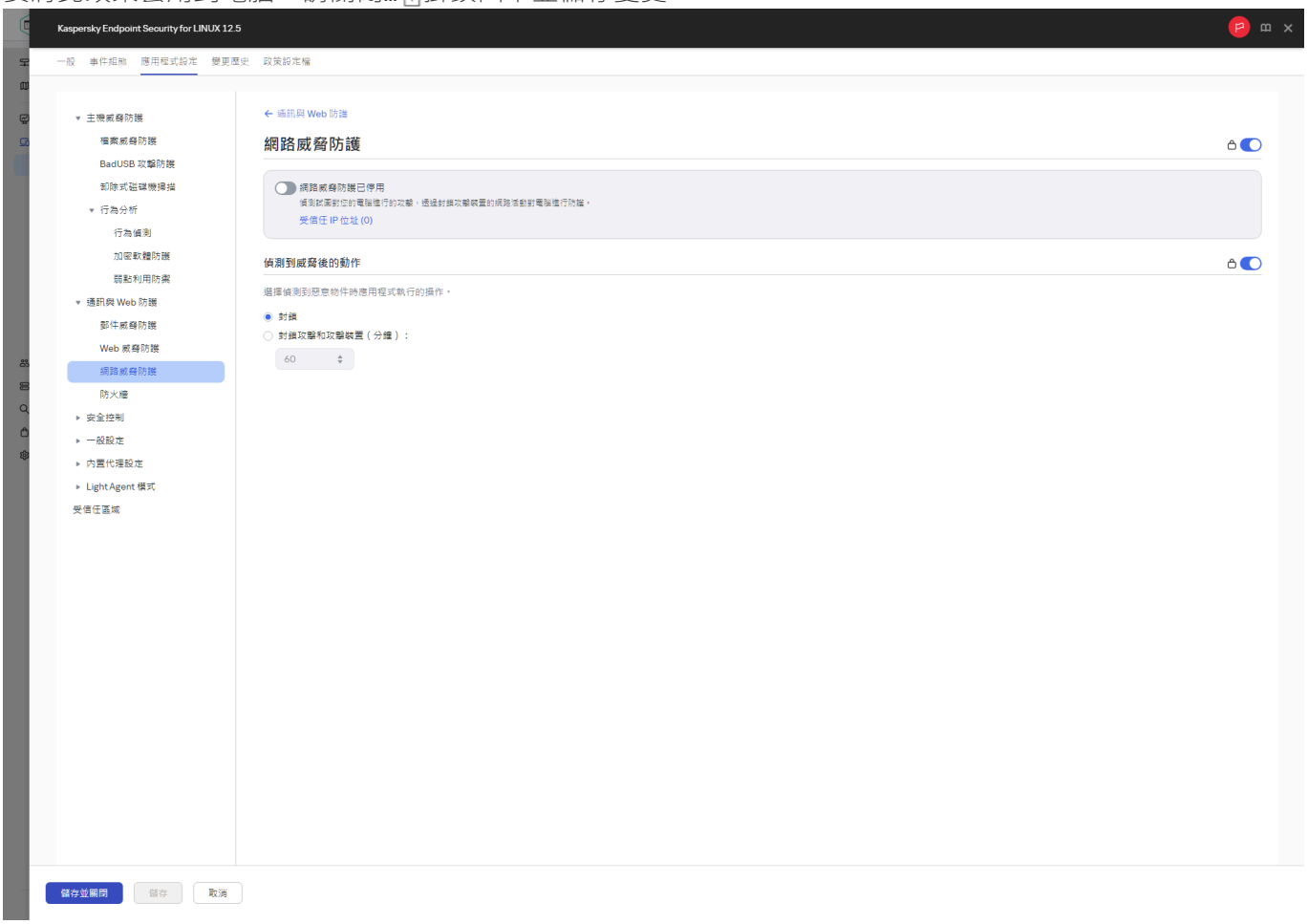
如果偵測到對受保護裝置的網路攻擊嘗試，應用程式會封鎖攻擊裝置的網路活動，並建立 *偵測到網路攻擊* 事件。

若要封鎖網路流量，Kaspersky Endpoint Security 會建立一個動態防火牆規則。防火牆會暫時封鎖攻擊裝置的網路流量。應用程式也會將遭入侵裝置新增至已封鎖裝置清單。被封鎖的裝置無法存取共用網路目錄。

如何在網頁主控台中設定偵測到網路攻擊時的動作

1. 在網頁主控台的主視窗中，選擇**資產管理 → 政策**。
2. 點擊 Kaspersky Endpoint Security 政策的名稱。
   政策內容視窗將開啟。
3. 選擇"**應用程式設定**"標籤。
4. 轉到"**通訊與 Web 防護**"→"**網路威脅防護**"。
5. 確保該元件的切換開關處於 **網路威脅防護已啟用** 位置。
6. 選擇"**為 Linux 裝置啟用網路威脅防護**"核取方塊。
7. 在 **偵測到威脅後的動作** 下，選取應用程式在偵測到威脅時將採取的動作：**封鎖** 或 **封鎖攻擊和攻擊裝置（分鐘）**。
8. 如果選取 **封鎖攻擊和攻擊裝置（分鐘）**，請設定遭入侵裝置的封鎖持續時間（分鐘）。預設情況下，裝置會被封鎖 60 分鐘。有效值為 1 到 999。

9. 要將此政策套用到電腦，請關閉... 掛鎖圖示並儲存變更。



網路威脅防護

如何在命令列中設定偵測到網路攻擊時的動作

1. 請確定已啟用網路威脅防護元件：

```
kesl-control --get-task-state 17
```

元件必須處於 **已啟動** 狀態。

2. 如果元件已停用，請執行下列命令：

```
kesl-control --start-task 17
```

3. 選擇偵測到網路威脅時的動作：

```
kesl-control --set-settings 17 ActionOnDetect=<Block|Notify>
```

4. 設定遭入侵裝置的封鎖：

```
kesl-control --set-settings 17 BlockAttackingHosts=<Yes|No>
```

5. 選擇 `BlockAttackingHosts=Yes` 動作的封鎖期間：

```
kesl-control --set-settings 17 BlockDurationMinutes=<Blocking period>
```

6. 若要檢查元件設定的目前值，請執行以下命令：

```
kesl-control --get-settings 17
```

符號

命令選項

設定	描述
`ActionOnDetect`	偵測到網路威脅時的動作： • `Block`（預設）會封鎖遭入侵裝置的網路流量，並建立 *偵測到網路攻擊* 事件。 • `Notify` 會建立 *偵測到網路攻擊* 事件，而不封鎖網路流量。
`BlockAttackingHosts`	封鎖攻擊裝置的網路活動。預設會啟用裝置封鎖。
`BlockDurationMinutes`	設定涉及惡意活動或惡意資料加密的遠端裝置的封鎖持續時間。

如何管理被封鎖的裝置

在防護裝置免受網路威脅和遠端惡意加密侵害時，Kaspersky Endpoint Security 可以封鎖其動作被視為惡意的遠端裝置。裝置會受到 加密軟體防護 和 網路威脅防護 元件保護，以防範這些類型的威脅。Kaspersky Endpoint Security 會在一段時間內封鎖網路流量。封鎖期間到期時，Kaspersky Endpoint Security 會允許網路流量恢復。預設情況下，應用程式會封鎖攻擊裝置的網路流量 60 分鐘。封鎖時間到期時，應用程式會將此裝置從被封鎖的裝置清單中移除。

如果 Kaspersky Endpoint Security 封鎖了受信任裝置，您需要將此裝置的 IP 位址新增至排除清單。

如何檢視被封鎖的裝置清單

```
kesl-control -H --get-blocked-hosts
```

指令執行的結果是，應用程式將被封鎖裝置的清單輸出到主控台。

被封鎖的裝置清單

```
Blocked devices: 1
Host                : 10.69.119.234
Block date          : 2026-04-29 15:44
Will be unblocked   : 2026-04-29 16:44
Task name           : Network_Threat_Protection
```

如何解除對裝置的封鎖

```
kesl-control -H --allow-hosts <address>
```

其中 `<address>` 是裝置或子網路的一個或多個 IP 位址（IPv4/IPv6，包括短格式位址）。您可以指定多個裝置或子網路的 IP 位址，以空格分隔。

防火牆管理

作業系統的防火牆會控制裝置的所有網路活動，無論是網際網路或本機網路上的活動。防火牆會保護裝置上的資料免於未經授權的存取，並封鎖大多數威脅，例如來自網路、針對裝置的攻擊。防火牆可偵測使用者裝置上的所有網路連線，並取得其 IP 位址清單。

應用程式會使用「防火牆管理」元件來管理作業系統的防火牆。此元件會將 網路封包規則 新增至作業系統的防火牆，以監控裝置的網路活動。您可以使用網路封包規則來指定所需的裝置防護級別，從完全阻止所有應用程式的網際網路存取到允許無限制存取。

防火牆管理元件預設停用。

啟用防火牆管理元件後，Kaspersky Endpoint Security 會使用作業系統提供的工具自動刪除所有為防火牆設定的自訂規則。元件停用後，這些規則不會還原。

如果已啟用「防火牆管理」，Kaspersky Endpoint Security 會每 60 秒檢查一次作業系統的防火牆。如果檢查發現第三方應用程式或公用程式已新增或移除網路封包規則，Kaspersky Endpoint Security 會還原使用應用程式建立的防火牆規則集。

當防火牆管理停用時，Kaspersky Endpoint Security 仍會掃描作業系統防火牆。這可讓應用程式還原動態規則。

啟用 Firewall 管理元件之前，請執行下列操作：

- 停用其他管理作業系統防火牆的工具。
- 啟用「防火牆管理」元件之前，請儲存並備份已設定的任何自訂防火牆規則。

如何建立網路封包規則

防火牆會根據 *網路封包規則*篩選受保護裝置上的所有網路活動。網路封包規則會限制網路封包或連線，而不論應用程式為何。規則會根據以下條件允許或拒絕網路活動：

- 連線協定和連接埠
- 流量方向
- 傳送或接收網路流量之裝置的 IP 位址

網路封包規則的優先順序

預設為所有傳出封包和連線。預設規則具有最低優先順序：如果沒有觸發其他網路封包規則，或沒有指定其他網路封包規則，則允許該活動。

防火牆會依照網路封包規則的優先順序套用這些規則。規則的優先順序是其在清單中的位置，從上到下。防火牆會依據清單中的第一個規則篩選網路連線，並允許或封鎖網路活動。如果規則不相符，防火牆會套用清單中的下一個規則，依此類推。接著，該元件會忽略符合連線的規則之後的所有網路封包規則。

建立網路封包規則的建議

若要在命令列中建立網路封包規則，您可以使用命令列選項或 設定檔。如果您想要新增多個規則，請使用設定檔加以新增。

使用命令列選項一次新增大量規則可能會導致 CPU 負載遽增。

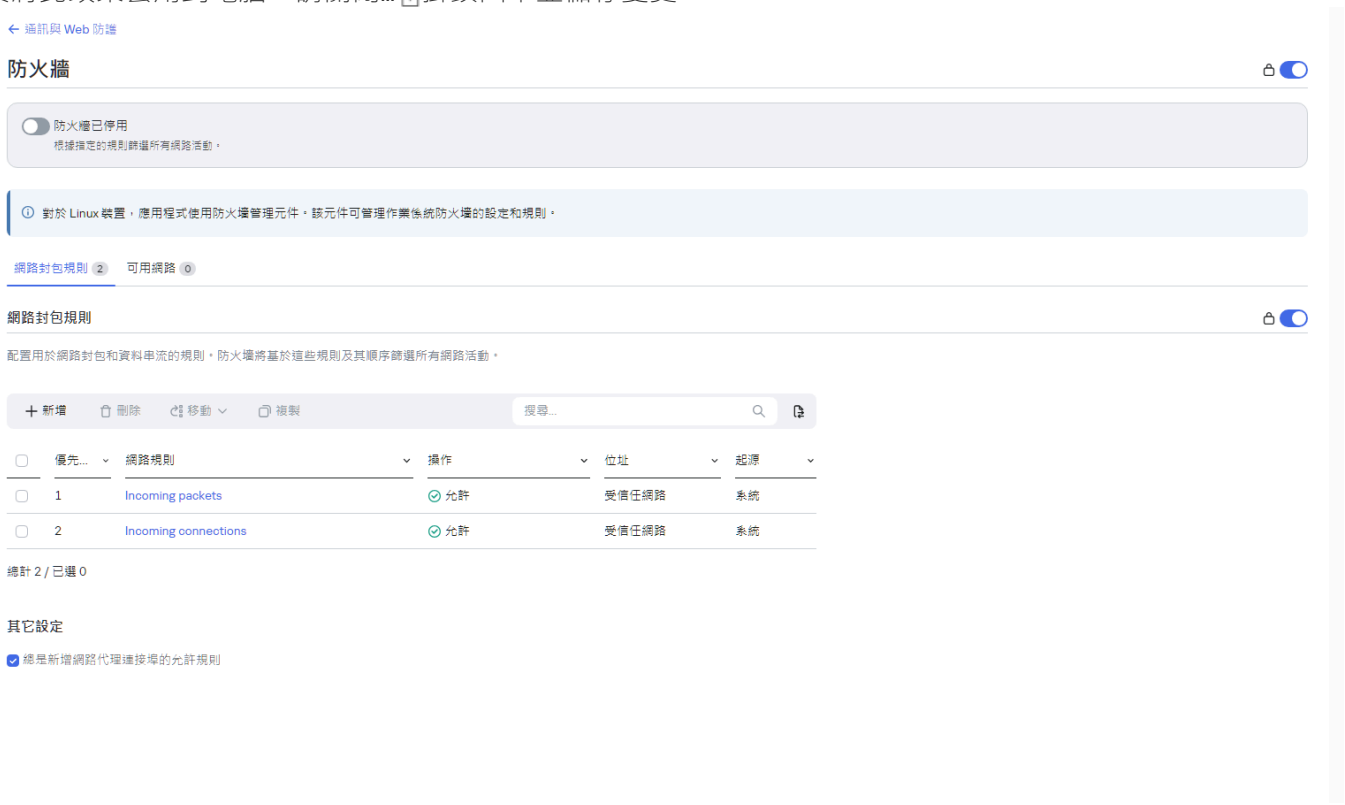
如何在網頁主控台中建立網路封包規則

1. 在網頁主控台的主視窗中，選擇**資產管理 → 政策**。
2. 點擊 Kaspersky Endpoint Security 政策的名稱。
   政策內容視窗將開啟。
3. 選擇"**應用程式設定**"標籤。
4. 選擇"**通訊與 Web 防護**" → "**防火牆**"。
5. 確保該元件的切換開關處於 **防火牆已啟用** 位置。
6. 在"**網路封包規則**"標籤上點擊"**新增**"按鈕 。
   這會開啟新的網路規則表單（請參見下圖）。
7. 在"**規則名稱**"欄位中輸入規則的名稱。
   您可以透過點擊"**選取規則範本**"連線來選擇預定義的規則範本。規則範本包含最常用網路連線的設定。
   除了優先順序以及防火墻套用至連線的操作之外，網路規則的所有設定都會自動填入。
8. 在「**優先順序**」欄位中，指定規則的優先順序。預設情況下，會以最高優先順序建立規則。
9. 在 **操作** 下，選取規則觸發時希望防火墻處理網路活動的方式：**允許** 或 **封鎖**。
10. 在「**方向**」欄位中，選取您希望規則套用到的網路活動：
    - **接收**防火牆將網路規則套用於所有接收網路封包。
    - **接收(封包)**防火牆將把網路規則套用到透過遠端電腦發起的連線傳送的所有網路封包。
    - **接收/傳送**防火牆將為接收和傳送的網路封包套用網路規則，與此網路連線的發起者是使用者電腦還是遠端電腦無關。
    - **傳送(封包)**防火牆將網路規則套用於所有傳送網路封包。
    - **傳送**防火牆將為透過使用者電腦發起的連線傳送的所有網路封包套用網路規則。
    - **接收/傳送（封包）**防火牆將網路規則套用於所有傳入和傳出網路封包。
11. 如果您希望將網路規則的操作反映在報告中，請選取「**記錄事件**」核取方塊。根據規則的操作，應用程式會建立 *網路活動已封鎖* 或 *網路活動已允許* 事件。
12. 在「**通信協定設定**」索引標籤上，選取您希望規則用來篩選網路活動的通訊協定。
13. 轉到"**遠端網路位址**"標籤。

14. 在「**遠端**」欄位中，指定可傳送和接收網路封包的遠端電腦網路位址：防火墙會將規則套用至指定的位址。

15. 在「**本機**」欄位中，指定已安裝 Kaspersky Endpoint Security 且可傳送和接收網路封包的電腦網路位址：防火墙會將規則套用至指定的位址。

16. 要將此政策套用到電腦，請關閉... 掛鎖圖示並儲存變更。



防火牆

如何在命令列中建立網路封包規則

1. 請確保防火墙管理已啟用：

```
kesl-control --get-task-state 12
```

元件必須處於 **已啟動** 狀態。

2. 如果元件已停用，請執行下列命令：

```
kesl-control --start-task 12
```

3. 新增新的網路封包規則：

```
kesl-control [-F] --add-rule [--name <rule name>] [--action <Allow|Block>] [--protocol <protocol>] [--direction
<direction>] [--remote <remote address>:<port>] [--local <local address>:<port>] [--at <index>]
```

如果您想要新增多個規則，請使用設定檔加以新增：

a. 將元件的設定輸出至設定檔：

```
kesl-control --get-settings 12 --file <path to file> [--json]
```

b. 開啟設定檔，並新增包含下列區段的網路封包規則：

```
[PacketRules.item_#]
Name=<rule name>
FirewallAction=<Allow|Block>
Protocol=<protocol>
Direction=<direction>
RemoteAddress=<remote address>
LocalAddress=<local address>
LogAttempts=<Yes|No>
```

c. 將設定從設定檔匯入至應用程式中：

```
kesl-control --set-settings 12 --file <path to file> [--json]
```

4. 若要檢視網路封包規則清單，請執行以下指令：

```
kesl-control -F --query
```

應用程式會以下列格式顯示所有網路封包規則的清單：`<IP protocol version> <table> <chain> <rule in the format of the iptables-save utility>`。

符號

命令選項

設定	描述
`--name <rule name>` `Name`	網路封包規則名稱。預設為 `Packet rule #<n>`。
`--action` `FirewallAction`	對此網路封包規則中指定的連線執行的操作。 • `Allow`（預設）表示允許連線。 • `Block` 表示封鎖連線。
`--protocol` `Protocol`	您要監控網路活動的協定類型。 • `Any`（預設）表示防火牆控制所有網路活動 • `TCP` • `UDP` • `ICMP` • `ICMPv6` • `IGMP` • `GRE`
`--direction` `Direction`	受監控網路活動的方向： • `IncomingOutgoing` 或 `InOut`（預設）。防火牆將網路規則套用於所有傳入和傳出網路封包。 • `Incoming` 或 `In`。防火牆將把網路規則套用到透過遠端電腦發起的連線傳送的所有網路封包。 • `Outgoing` 或 `Out`。防火牆將為透過使用者電腦發起的連線傳送的所有網路封包套用網路規則。 • `IncomingPacket` 或 `InPacket`。防火牆將網路規則套用於所有接收網路封包。 • `OutgoingPacket` 或 `OutPacket`。防火牆將網路規則套用於所有傳送網路封包。 • `IncomingOutgoingPacket` 或 `InOutPacket`。防火牆將為接收和傳送的網路封包套用網路規則，與此網路連線的發起者是使用者電腦還是遠端電腦無關。

設定	描述
`--remote <remote address[:<port>]>` `RemoteAddress=<remote address>`	遠端裝置的 IP 位址： • `Any`（預設）會啟用對具有任何 IP 位址的遠端裝置所傳送和/或接收之網路封包的監控。 • `Trusted` 是針對受信任網路設定的網路區域。 • `Local` 是針對本機網路設定的網路區域。 • `Public` 是針對公用網路設定的網路區域。 • `d.d.d.d` 是 IPv4 位址，其中 d 是 0 到 255 的十進位數。 • `d.d.d.d – d.d.d.d` 是 IPv4 位址範圍。 • `d.d.d.d/p` 是 IPv4 子網，其中 p 是 0 到 32 的數字。 • `x:x:x:x:x:x:x:x` 是 IPv6 位址，其中 x 是 0 到 ffff 的十六進位數。 • `x:x:x:x:x:x:x:x – x:x:x:x:x:x:x:x` 是 IPv6 位址範圍。 • `x:x:x:x:x:x:x:x/p` 是 IPv6 位址的子網，其中 p 是 0 到 128 的數字；為求簡潔，您可以使用 `::`。 您也可以指定遠端連接埠： • `Any`（預設）表示監控所有遠端連接埠 • `0 – 65535`。
`--local <local address[:<port>]>` `LocalAddress=<local address>`	已安裝 Kaspersky Endpoint Security 之裝置的網路位址： • `Any`（預設）表示監控具有任何 IP 位址的本機裝置所傳送和/或接收的網路封包。 • `Trusted` 是針對受信任網路設定的網路區域。 • `Local` 是針對本機網路設定的網路區域。 • `Public` 是針對公用網路設定的網路區域。 • `d.d.d.d` 是 IPv4 位址，其中 d 是 0 到 255 的十進位數。 • `d.d.d.d – d.d.d.d` 是 IPv4 位址範圍。 • `d.d.d.d/p` 是 IPv4 子網，其中 p 是 0 到 32 的數字。 • `x:x:x:x:x:x:x:x` 是 IPv6 位址，其中 x 是 0 到 ffff 的十六進位數。 • `x:x:x:x:x:x:x:x – x:x:x:x:x:x:x:x` 是 IPv6 位址範圍。 • `x:x:x:x:x:x:x:x/p` 是 IPv6 位址的子網，其中 p 是 0 到 128 的數字；為求簡潔，您可以使用 `::`。 您也可以指定本機連接埠： • `Any`（預設）表示監控所有本機連接埠 • `0 – 65535`。
`--at <index>`	網路封包規則清單中規則的索引。如果未指定 `--at` 選項或其值大於清單中的規則數，則新規則將會新增至清單的末端。
`LogAttempts`	在報告中包含網路規則操作的記錄。 • `Yes` — 在報告中記錄操作。 • `No`（預設值）- 不在報告中寫入操作。

封鎖所有傳入和已建立至 TCP 連接埠 23 的連線的規則範例

```
kesl-control -F --add-rule --name Block_Telnet --action Block --direction in --protocol TCP --local any:23 --
remote any
```

針對公用網路區域封鎖透過 TCP 連接埠 23 傳入和已建立連線的規則範例

```
kesl-control -F --add-rule --name Block_Telnet --action Block --direction in --protocol TCP --local any:23 --
remote Public
```

網路封包規則使用範例

1. **僅允許本機網路上的一台特定電腦存取網際網路，並封鎖所有其他電腦的存取**

   允許電腦 (192.168.2.22) 透過 TCP 協定存取網際網路的規則：

   ```
   kesl-control --add-rule --name InternetAccess --action Allow --protocol TCP --local 192.168.2.22
   ```

   封鎖其他電腦存取網際網路的規則：

   ```
   kesl-control --add-rule --name InternetBlock --action Block --protocol TCP --local 192.168.1.0/24
   ```

2. **僅封鎖本機網路上一台特定電腦的網際網路存取**

   封鎖電腦 (192.168.2.23) 存取網際網路的規則：

```
kesl-control --add-rule --name InternetBlock --action Block --protocol TCP --local 192.168.2.23
```

3. **封鎖從本機網路存取特定網站**

   拒絕本機網路上的電腦透過 HTTP 存取 example.com (91.198.174.192) 的規則：

```
kesl-control --add-rule --name ExampleHTTP --action Block --protocol TCP --remote 91.198.174.192:80
```

   拒絕本機網路上的電腦透過 HTTPS 存取 example.com (91.198.174.192) 的規則：

```
kesl-control --add-rule --name ExampleHTTPS --action Block --protocol TCP --remote 91.198.174.192:443
```

4. **僅允許本機網路上的特定電腦存取一個指定網站**

   允許電腦 (192.168.2.24) 透過 HTTP 存取 example.com (91.198.174.192) 的規則：

```
kesl-control --add-rule --name ExampleHTTP --action Allow --protocol TCP --remote 91.198.174.192:80 --local
192.168.2.24
```

   允許電腦 (192.168.2.25) 透過 HTTPS 存取 example.com (91.198.174.192) 的規則：

```
kesl-control --add-rule --name ExampleHTTPS --action Allow --protocol TCP --remote 91.198.174.192:443 --local
192.168.2.25
```

   封鎖電腦 (192.168.2.26) 存取網際網路的規則：

```
kesl-control --add-rule --name InternetBlock --action Block --protocol TCP --local 192.168.2.26
```

如何將 IP 位址新增至網路區域：公用、本機、受信任

防火牆允許監控*網路區域*的網路活動。網路區域是指在一種網路連線類型下群組在一起的一組 IP 位址或子網路。您可以使用預先定義的網路區域，對多個 IP 位址或子網路重複使用規則，而無需為每個 IP 位址或子網路建立單獨的規則。

Kaspersky Endpoint Security 區分三種網路區域：

- **公用網路**網路不受防毒應用程式、防火牆或篩檢程式防護（例如咖啡館中的 Wi-Fi）。當使用者操作連線到此類網路的電腦時，防火牆會封鎖對此電腦的檔案和印表機的存取。外部使用者也無法透過共用資料夾存取資料，以及遠端存取該電腦的桌面。

- **本機網路**為對此電腦上的檔案和印表機具有受限存取權限的使用者提供的網路（例如企業 LAN 或家庭網路）。

- **受信任網路**其中的電腦不會曝露於被攻擊或未經授權的資料存取嘗試的安全網路。防火牆允許在具有此狀態的網路中進行任何網路活動。

如何在網頁主控台中將 IP 位址新增至網路區域

1. 在網頁主控台的主視窗中，選擇**資產管理** → **政策**。
2. 點擊 Kaspersky Endpoint Security 政策的名稱。
   政策內容視窗將開啟。
3. 選擇“**應用程式設定**”標籤。
4. 選擇“**通訊與 Web 防護**” → “**防火牆**”。
5. 轉到“**可用網路**”標籤。
6. 點擊“**新增**”。
   這會開啟用於新增網路連線的表單。
7. 在 **名稱** 欄位中，輸入網路連線的名稱。
8. 在 **網路類型** 欄位中，選取網路連線所屬的網路區域：**公用網路**、**本機網路**、**受信任網路**。
9. 在 **IP 位址** 欄位中，指定將與網路連線建立關聯的 IP 位址或子網路。
10. 要將此政策套用到電腦，請關閉... 掛鎖圖示並儲存變更。

如何在命令列中將 IP 位址新增至網路區域

1. 請確保防火牆管理已啟用：

   ```
   kesl-control --get-task-state 12
   ```

   元件必須處於 **已啟動** 狀態。
2. 如果元件已停用，請執行下列命令：

   ```
   kesl-control --start-task 12
   ```

3. 將位址新增至網路區域：

   ```
   kesl-control -F --add-zone <Public|Local|Trusted> --address <IP address>
   ```

   若要檢視網路封包規則清單，請執行以下指令：

   ```
   kesl-control -F --query
   ```

符號

命令選項

設定	描述
`--add-zone`	預先定義的網路區域： • `Public`。公共網路。 • `Local`。本機網路。 • `Trusted`。受信任網路。
`--address`	網路位址或子網路。

範例

```
kesl-control -F --add-zone Local --address 10.28.0.0/24
```

什麼是動態規則

Kaspersky Endpoint Security 允許新增或移除應用程式正常運作所需的防火牆*動態規則*。範例：

- 網路代理會新增允許連線至卡巴斯基安全管理中心的動態規則。
- 加密軟體防護元件會新增動態規則，用於攔截透過 NFS 和 SMB 檔案傳輸與儲存通訊協定傳輸的流量。這可讓該元件封鎖其動作被應用程式判定為惡意加密之裝置的網路流量。
- 如果在 Light Agent 模式下使用 Kaspersky Endpoint Security，則動態規則會自動新增至防火牆，以允許連線至 SVM 和 Integration Server。

Kaspersky Endpoint Security 會自動建立動態規則，允許應用程式元件存取網路資源。動態規則不依賴防火牆管理元件狀態（已啟用/停用）或元件操作設定的變更。動態規則的執行優先順序高於網路封包規則的優先順序。如果任何動態規則被刪除，應用程式會還原一組動態規則，例如透過使用 iptables 公用程式。如果 kesl 程序被 Watchdog 伺服器終止，則應用程式在運作期間建立的所有規則鏈結（kesl-bypass 除外）都會從 iptables 中刪除。

您可以使用以下指令檢視動態規則集：

```
kesl-control -F --query
```

應用程式會以下列格式顯示所有網路封包規則的清單：`<IP protocol version> <table> <chain> <rule in the format of the iptables-save utility>`。動態規則會分隔到不同的鏈結中：`kesl_input`、`kesl_output`、`kesl_prerouting`、`kesl_postrouting`、`kesl_forward`。

您無法管理動態規則的設定。

範例

```
ipv4 mangle kesl_output -p tcp -m tcp --dport 80 -m mark ! --mark 0x400/0x400 -m conntrack --ctdir ORIGINAL -m
addrtype ! --dst-type LOCAL -j MARK --set-xmark 0x100/0x100 tag WebAv
```

如何建立連線至卡巴斯基安全管理中心的規則

網路代理用於與卡巴斯基安全管理中心進行交互。若要讓網路代理與卡巴斯基安全管理中心保持永久連線，您需要為網路代理的連接埠新增允許規則。在這種情況下，即使您錯誤地設定防火牆並意外封鎖所有連線，您仍能在卡巴斯基安全管理中心主控台中遠端設定防火牆。

連接埠組合取決於電腦的角色（例如，分發點）。要了解將在电脑上開啟的連接埠的更多資訊，請參閱 卡巴斯基安全管理中心說明。

如何在網頁主控台中為網路代理新增允許規則

1. 在網頁主控台的主視窗中，選擇**資產管理** → **政策**。
2. 點擊 Kaspersky Endpoint Security 政策的名稱。
   政策內容視窗將開啟。
3. 選擇“**應用程式設定**”標籤。
4. 選擇“**通訊與 Web 防護**” → “**防火牆**”。
5. 確保該元件的切換開關處於 **防火牆已啟用** 位置。
6. 選擇“**總是新增網路代理連接埠的允許規則**”核取方塊。
7. 要將此政策套用到電腦，請關閉... 掛鎖圖示並儲存變更。

如何在命令列上為網路代理新增允許規則

1. 請確保防火墻管理已啟用：

   ```
   kesl-control --get-task-state 12
   ```

   元件必須處於 **已啟動** 狀態。
2. 如果元件已停用，請執行下列命令：

   ```
   kesl-control --start-task 12
   ```
3. 執行以下指令：

   ```
   kesl-control --set-settings 12 OpenNagentPorts=Yes
   ```
4. 若要檢查元件設定的目前值，請執行以下命令：

   ```
   kesl-control --get-settings 12
   ```

安全控制

裝置控制

*裝置控制*會管理使用者對安裝在用戶端裝置上或連線至用戶端裝置的裝置（例如硬碟、相機或 Wi-Fi 模組）的存取。這使得您可以在連線外部裝置時防護用戶端裝置免受感染，並防止資料遺失或外洩。

裝置控制的運作方式

依預設，裝置控制元件會以預設設定啟用。

1. **使用者嘗試取得該裝置的存取權限**
2. **裝置控制在以下層級管理使用者存取：**
   - 由裝置控制分類的**裝置類型**，例如印表機、卸除式磁碟機或 CD/DVD 光碟機。每種裝置類型都可以套用下列其中一種*存取模式*：
     - *允許*，允許存取此類型的裝置。
     - *封鎖*：封鎖對此類型裝置的存取。
     - *取決於匯流排*：根據裝置所連線匯流排設定的存取模式允許或阻止對裝置的存取。
     - *自訂*：根據裝置存取規則允許或封鎖對裝置的存取。
     - *唯讀*：允許對所選類型的裝置進行唯讀存取，同時封鎖寫入存取。
   - **連接匯流排**。*連接匯流排*是裝置用來連線至用戶端裝置的介面，例如 USB 或 FireWire。下列一種存取模式可套用於連線匯流排：
     - *允許*：授予對透過此連線匯流排連線的裝置的存取權限。
     - *封鎖*：拒絕存取使用此連線匯流排連線的裝置。

   例如，可拒絕所有透過 USB 連線的裝置存取。
3. **掃描完成**

   如果使用者嘗試存取的裝置不是此使用者的受信任裝置，或使用者沒有依據存取模式取得該裝置的存取權限，應用程式會封鎖此使用者對該裝置的存取。

   如果使用者認為遭到誤封鎖，可以向組織的管理員傳送請求以申訴誤封鎖，或請求暫時存取該裝置。

當裝置控制被停用時，應用程式將解除封鎖對被封鎖裝置的存取。

設定裝置控制

1. **設定受信任裝置**

   *信任的裝置*是指在信任裝置設定中指定的使用者可隨時進行完全存取的裝置。您可以為個別使用者、使用者群組或組織的所有使用者授予受信任裝置的存取權限。例如，您可以限制對特定 USB 裝置的存取或僅限制對 USB 磁碟機的存取；拒絕存取其他 USB 裝置。
2. **設定存取模式**

   您可以為裝置類型和連接匯流排設定存取模式。依預設，所有裝置類型都會選取 *依匯流排而定* 存取模式。為連線匯流排選擇*允許*存取模式。相應的，裝置控制授予使用者對所有裝置的完全存取權限。
3. **設定存取規則**

   對於儲存裝置（硬碟、卸除式磁碟機、軟碟機和 CD/DVD 光碟機），您可以設定 *存取規則*。

4. **設定訊息範本**

   如有必要，您可以自訂訊息的範本文字，以通知使用者裝置存取遭到封鎖或裝置的某項操作遭到禁止。

5. **設定裝置的暫時存取權限**

   如有必要，允許使用者取得遭封鎖裝置的暫時存取權限。

特殊考量與限制

- 首次啟用裝置控制時，它會為所有具有已知裝置或匯流排類型的偵測到的裝置產生*DeviceAllowed*事件。除非這些裝置的控制設定發生變化，否則後續元件執行時不會產生重複事件。
- 裝置控制不會阻止系統磁碟機。如果應用程式無法自動偵測系統磁碟機，裝置控制元件將因錯誤而終止。
- 以下 Linux 核心上不支援透過系統裝置驅動程式依照裝置類型或連線匯流排封鎖裝置：3.10、5.14、5.15、5.17、6.1、6.8。在這些核心上，在*透過規則*存取模式下，僅阻止開啟檔案和讀取目錄（即獲取檔案和目錄的名稱）。在不支援 fanotify 的系統上，也不支援封鎖讀取目錄。
- 裝置控制可忽略安裝點排除項目。對安裝在排除點的裝置的存取可以透過裝置控制設定進行限制。
- 在一般應用程式設定中，如果停用在掃描期間封鎖對檔案的存取，則您無法使用裝置存取排程來封鎖對裝置的存取。

如何在指令列上管理受信任裝置清單

受信任裝置清單包含允許存取之裝置的相關資訊（針對特定使用者或群組）。

在命令列中，您可以檢視受信任裝置清單、新增和刪除裝置，以及從檔案匯入受信任裝置清單。

檢視受信任裝置清單

```
kesl-control --trusted-devices --list
```

將裝置新增到受信任裝置清單

```
kesl-control --trusted-devices --add <device id or mask>
```

其中 `<device id or mask>` 是裝置 ID 或裝置 ID 遮罩。

從受信任裝置清單中刪除裝置

```
kesl-control --trusted-devices --delete <device id or mask>
```

其中 `<device id or mask>` 是裝置 ID 或裝置 ID 遮罩。

從檔案匯入受信任裝置清單

```
kesl-control --trusted-devices --merge|--add|--replace --file <file>
```

其中：

- `--merge` 可合併受信任裝置清單。如果目前清單和匯入的清單中包含具有相同 ID 的裝置條目，則更新現有條目。對於目前清單中不存在的裝置，將會新增條目。
- `--add` 在匯入時新增目前受信任裝置清單。僅將先前不在裝置清單中的裝置項目新增至清單中。
- `--replace` 取代目前受信任裝置清單。現有受信任裝置清單將匯入的清單取代。
- `--file <file>` 是將從中匯入受信任裝置清單之 JSON 檔案的完整路徑。

如何設定裝置存取模式

對於每種裝置類型（根據裝置控制元件的分類，例如印表機、卸除式磁碟機、CD/DVD 光碟機），可以套用下列其中一種*存取模式*：

- *允許*，允許存取此類型的裝置。
- *封鎖*：封鎖對此類型裝置的存取。
- *取決於匯流排*：根據裝置所連線匯流排設定的存取模式允許或阻止對裝置的存取。
- *自訂*：根據裝置存取規則允許或封鎖對裝置的存取。*裝置存取規則*是一組選項，用於確定哪些使用者可以在何時存取安裝在用戶端裝置上或已連線到客戶端的裝置。此存取模式僅可針對儲存裝置（硬碟、卸除式磁碟機、軟碟機、CD/DVD 磁碟機）指定。
- *唯讀*：允許對所選類型的裝置進行唯讀存取，同時封鎖寫入存取。此存取模式僅可針對儲存裝置（硬碟、卸除式磁碟機、軟碟機、CD/DVD 磁碟機）指定。如果裝置具有「唯讀」存取類型，即使將受信任裝置指派給特定使用者，系統仍會忽略受指派的使用者，但會對所有使用者開放寫入權限。

如何在網頁主控台中為裝置類型設定裝置存取模式

1. 在網頁主控台的主視窗中，選擇**資產管理 → 政策**。
2. 點擊 Kaspersky Endpoint Security 政策的名稱。

   政策內容視窗將開啟。
3. 選擇“**應用程式設定**”標籤。
4. 轉到”**安全控制**”→”**裝置控制**”。
5. 確保該元件的切換開關處於 **裝置控制已啟用** 位置。
6. 在 **裝置存取規則** 下方，於表格中選取 **裝置和 Wi-Fi 網路** 標籤。
7. 在 **名稱** 欄中，選取您要設定存取模式的裝置類型。
8. 在 **存取** 下拉式清單中，選取以下存取模式之一：
   - **允許**：允許存取所選類型的裝置。
   - **封鎖**：禁止存取選定類型的裝置。

- **取決於匯流排**（預設值）：根據連線匯流排的存取模式允許或封鎖對裝置的存取。
- **自訂**：根據存取規則和排程允許或封鎖對裝置的存取。此選項僅適用於儲存裝置（硬碟、卸除式磁碟機、軟碟機、CD/DVD 光碟機）。
- **唯讀**：允許對所選類型的裝置進行唯讀存取。此選項僅適用於儲存裝置（硬碟、卸除式磁碟機、軟碟機、CD/DVD 光碟機）。

9. 在下方表格中，點擊 **新增** 按鈕。

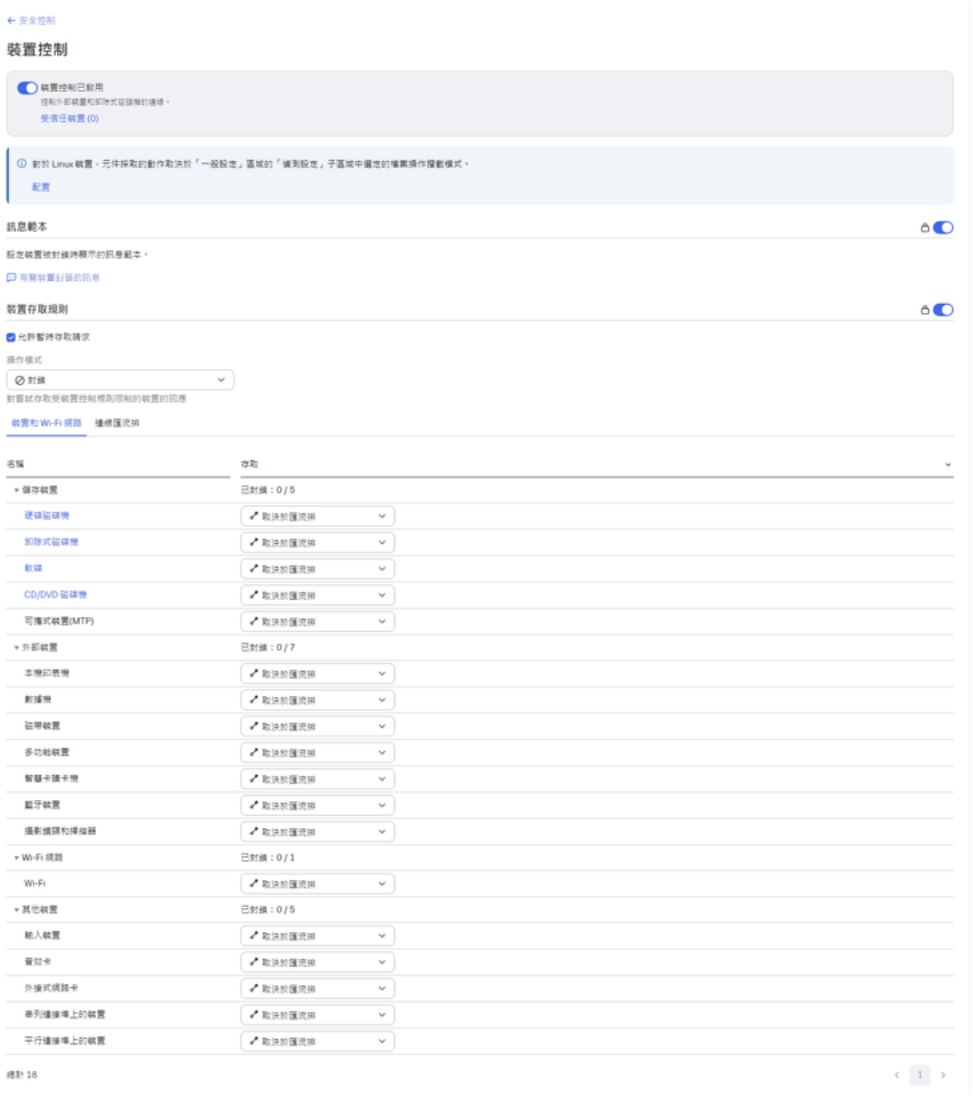
   這會開啟新增存取規則的視窗。

10. 在 **優先順序** 欄位中，設定存取規則優先順序。

11. 選取存取規則將套用的使用者或使用者群組。預設情況下，此規則適用於所有使用者。

12. 如有必要，請設定存取排程。預設情況下，此規則一律套用。

13. 要將此政策套用到電腦，請關閉... 掛鎖圖示並儲存變更。



裝置控制

如何在命令列中為裝置類型設定裝置存取模式

1. 確認裝置控制元件正在執行：

   ```
   kesl-control --get-task-list
   ```

   元件必須處於 **已啟動** 狀態。

2. 如果元件已停用，請執行下列命令：

   ```
   kesl-control --start-task 15
   ```

3. 選取在嘗試存取根據裝置控制規則受到限制的裝置時的操作模式：

   ```
   kesl-control --set-settings 15 OperationMode=<Notify|Block>
   ```

4. 指定其中一種裝置類型的存取模式：`HardDrive`、`RemovableDrive`、`FloppyDrive`、`OpticalDrive`、`SerialPortDevice`、`ParallelPortDevice`、`Printer`、`Modem`、`TapeDrive`、`MultifuncDevice`、`SmartCardReader`、`WiFiAdapter`、`NetworkAdapter`、`PortableDevice`、`PortableDevice`、`BluetoothDevice`、`ImagingDevice`、`SoundAdapter`、`InputDevice`

   ```
   kesl-control --set-settings 15 DeviceClass.<device type>=<Allow|Block>
   ```

5. 若要檢視 裝置控制設定，請執行以下指令：

   ```
   kesl-control --get-settings 15
   ```

如何在網頁主控台中設定連線匯流排存取模式

1. 在網頁主控台的主視窗中，選擇**資產管理 → 政策**。
2. 點擊 Kaspersky Endpoint Security 政策的名稱。
   政策內容視窗將開啟。
3. 選擇"**應用程式設定**"標籤。
4. 轉到"**安全控制**"→"**裝置控制**"。
5. 確保該元件的切換開關處於 **裝置控制已啟用** 位置。
6. 在 **裝置存取規則** 下方，於表格中選取 **連線匯流排** 標籤。
7. 在 **名稱** 欄中，選取您要為其設定存取模式的匯流排。
8. 在 **存取** 下拉式清單中，選取以下存取模式之一：
   - **允許**：授予對透過此連線匯流排連線的裝置的存取權限。
   - **封鎖**：拒絕存取使用此連線匯流排連線的裝置。
9. 要將此政策套用到電腦，請關閉... 掛鎖圖示並儲存變更。

如何在命令列中設定連線匯流排存取模式

1. 確認裝置控制元件正在執行：

```
kesl-control --get-task-list
```

   元件必須處於 **已啟動** 狀態。

2. 如果元件已停用，請執行下列命令：

```
kesl-control --start-task 15
```

3. 選取在嘗試存取根據裝置控制規則受到限制的裝置時的操作模式：

```
kesl-control --set-settings 15 OperationMode=<Notify|Block>
```

4. 指定連線匯流排的存取模式：

```
kesl-control --set-settings 15 DeviceBus.USB=<Allow|Block>
kesl-control --set-settings 15 DeviceBus.FireWire=<Allow|Block>
```

5. 若要檢視 裝置控制設定，請執行以下指令：

```
kesl-control --get-settings 15
```

如何設定裝置存取規則

對於儲存裝置（硬碟、卸除式磁碟機、軟碟機和 CD/DVD 光碟機），您可以設定存取規則。*裝置存取規則*是一組選項，用於決定哪些使用者可以在何時存取安裝在用戶端裝置上或連線到該用戶端裝置的裝置。此存取模式僅可針對儲存裝置（硬碟、卸除式磁碟機、軟碟機、CD/DVD 磁碟機）指定。當連線禁止的裝置時，應用程式將拒絕規則中指定的使用者存取該裝置並顯示通知。在嘗試在此裝置上進行讀寫期間，應用程式會默默阻止規則中指定的使用者進行讀寫。如果您嘗試對存取模式設定為*透過規則*的裝置執行操作，但在存取時未發現任何有效規則，則該操作將被封鎖。

如何在網頁主控台中設定裝置存取規則

1. 在網頁主控台的主視窗中，選擇**資產管理 → 政策**。

2. 點擊 Kaspersky Endpoint Security 政策的名稱。
   政策內容視窗將開啟。

3. 選擇"**應用程式設定**"標籤。

4. 轉到"**安全控制**"→"**裝置控制**"。

5. 確保該元件的切換開關處於 **裝置控制已啟用** 位置。

6. 在 **裝置存取規則** 下方，於表格中選取 **裝置和 Wi-Fi 網路** 標籤。

7. 在 **名稱** 欄中，選取您要新增存取規則的儲存裝置類型（硬碟機、卸除式磁碟機、軟碟機、CD/DVD 光碟機）。

8. 在開啟的視窗中，於 **裝置存取規則** 下方選取 **自訂**。

9. 在下方表格中，點擊 **新增** 按鈕。

   這會開啟新增存取規則的視窗。

10. 在 **優先順序** 欄位中，設定存取規則優先順序。

11. 選取存取規則將套用的使用者或使用者群組。預設情況下，此規則適用於所有使用者。

12. 如有必要，請設定存取排程。預設情況下，此規則一律套用。

13. 要將此政策套用到電腦，請關閉... 掛鎖圖示並儲存變更。

如何在命令列設定裝置存取規則

1. 確認裝置控制元件正在執行：

```
kesl-control --get-task-list
```

   元件必須處於 **已啟動** 狀態。

2. 如果元件已停用，請執行下列命令：

```
kesl-control --start-task 15
```

3. 若要檢視 裝置控制設定，請執行以下指令：

```
kesl-control --get-settings 15
```

4. 選取在嘗試存取根據裝置控制規則受到限制的裝置時的操作模式：

```
kesl-control --set-settings 15 OperationMode=<Notify|Block>
```

5. 為下列其中一種裝置類型新增存取規則：`HardDrivePrincipals.item_#.AccessRules.item_#`、`RemovableDrivePrincipals.item_#.AccessRules.item_#`、`FloppyDrivePrincipals.item_#.AccessRules.item_#` 或 `OpticalDrivePrincipals.item_#.AccessRules.item_#`。

   - 啟用規則並指定預設排程：

     ```
     kesl-control --set-settings 15
     <Hard|Removable|Floppy|Optical>DrivePrincipals.item_#.AccessRules.item_#.UseRule=Yes
     <Hard|Removable|Floppy|Optical>DrivePrincipals.item_#.AccessRules.item_#.ScheduleName=Default
     ```

     範例

     ```
     kesl-control --set-settings 15 RemovableDrivePrincipals.item_0001.AccessRules.item_0001.UseRule=Yes
     RemovableDrivePrincipals.item_0001.AccessRules.item_0001.ScheduleName=Default
     ```

   - 設定規則觸發時的裝置控制動作：

     ```
     kesl-control --set-settings 15
     <Hard|Removable|Floppy|Optical>DrivePrincipals.item_#.AccessRules.item_#.Access=Allow|Block
     ```

     範例

     ```
     kesl-control --set-settings 15 RemovableDrivePrincipals.item_0001.AccessRules.item_0001.UseRule=Yes
     RemovableDrivePrincipals.item_0001.AccessRules.item_0001.Access=Allow
     RemovableDrivePrincipals.item_0001.AccessRules.item_0001.ScheduleName=Default
     ```

   - 如有必要，請指定此規則將套用到的使用者：

     ```
     kesl-control --set-settings 15 <Hard|Removable|Floppy|Optical>DrivePrincipals.item_#.Principal=<Name>=
     <\Everyone|user name|@group name>
     ```

     範例

     ```
     kesl-control --set-settings 15 RemovableDrivePrincipals.item_0001.Principal=\Everyone
     ```

   - 如有必要，請編輯規則排程：

     ```
     kesl-control --set-settings 15 Schedules.item_#.ScheduleName=<Name> Schedules.item_#.DaysHours=<All|day of
     the week|hour>
     ```

     範例

     ```
     kesl-control --set-settings 15 Schedules.item_0001.ScheduleName=Default Schedules.item_0001.DaysHours=All
     ```

如何設定裝置控制訊息範本

當使用者嘗試存取被封鎖的裝置時，應用程式會顯示一條關於存取被拒絕或裝置操作被封鎖的訊息。

存取被拒絕訊息基於描述封鎖原因的範本。您可以在訊息範本中使用特殊變數（例如 %USER_NAME%）。這些變數允許您對不同的裝置使用相同的訊息範本。產生訊息時，應用程式會將與特定裝置、使用者和事件對應的變數值帶入訊息中。

您可以編輯訊息範本。

如何在網頁主控台中編輯訊息範本

1. 在網頁主控台的主視窗中，選擇**資產管理 → 政策**。
2. 點擊 Kaspersky Endpoint Security 政策的名稱。

   政策內容視窗將開啟。
3. 選擇“**應用程式設定**”標籤。
4. 轉到”**安全控制**”→”**裝置控制**”。
5. 在 **訊息範本** 下，點擊 **有關裝置封鎖的訊息** 連結。

   這將開啟訊息範本配置視窗。
6. 在 **給使用者的訊息** 索引標籤上配置裝置控制訊息範本。
7. 您可以點擊**新增變數**和**新增連結**按鈕，在使用者訊息本文中新增變數和連結。若要向範本新增變數，請將遊標放在文字中的所需位置，點擊**新增變數**按鈕，然後從下拉清單中選擇變數。若要向範本新增連接，請將遊標放在文字中的所需位置，然後點擊**新增連結**按鈕。

   如果您想還原訊息範本的文字，請點擊 **還原預設** 按鈕。
8. 點擊**OK**。
9. 點擊**儲存**按鈕儲存所做的變更。

如何在管理主控台中變更訊息範本

1. 在管理主控台樹狀圖中的**受管理裝置**資料夾中，開啟包含所需裝置所屬的管理群組名稱的資料夾。
2. 在工作區選擇“**政策**”標籤。
3. 在政策清單中，選擇所需的政策並雙擊它以開啟**屬性：<政策名稱>**視窗。

   您也可以透過使用政策右鍵功能表中的**屬性**項目或點擊位於政策設定部分中政策清單右側的**配置政策設定**連結來開啟政策屬性視窗。
4. 在政策視窗中，選擇**安全控制→ 裝置控制**。
5. 在**訊息範本**部分，點擊**配置**按鈕。
6. 這將開啟**訊息範本**視窗；在該視窗中，在**封鎖**頁簽上配置裝置控制訊息範本。

   您可以點擊**變數**和**連結**按鈕，向訊息正文中新增變數和連結。若要向範本新增變數，請將遊標放在文字中的所需位置，點選**變數**按鈕，然後從下拉清單中選擇變數。若要向範本新增連接，請將遊標放在文字中的所需位置，然後點擊**連結**按鈕。

   您還可以透過點擊**預設**按鈕來還原訊息範本的文字。
7. 點擊**OK**。
8. 點擊“**套用**”。

授予對裝置的臨時存取權限

配置設備控制時，管理員可能會錯誤阻止使用者存取其工作所需的裝置。如果使用者認為對裝置的存取或對裝置內容的操作被錯誤阻止，使用者可以向企業本地網路管理員申請對被阻止裝置的臨時存取權。

如果管理員允許使用者請求臨時存取權限，則使用者可以這樣做。管理員可以在網頁主控台、管理主控台中的政策屬性，或在裝置控制工作設定中設定此權限。

授予對被封鎖裝置的存取權限涉及以下步驟：

1. 使用者建立*存取請求檔案*並將其傳送給管理員，例如，透過電子郵件或任何可用的方式（管理員可以在封鎖訊息範本中配置此操作）。使用者可以在應用程式的圖形介面或命令列中請求對被封鎖裝置的暫時存取權限。

2. 管理員根據存取請求檔案建立*存取金鑰*，並將其傳遞給使用者，例如透過電子郵件或其他方式。在網頁主控台中授予對被封鎖裝置的存取權限。

3. 使用者上傳存取金鑰即可獲得對被封鎖裝置的臨時存取權限。使用者可以在應用程式的圖形使用者介面或命令列中上傳存取金鑰。

只有當組織中部署了卡巴斯基安全管理中心 16.1 且用戶端裝置能夠與管理伺服器建立連線時，才能授予對被封鎖裝置的存取權。

如何在網頁主控台中為被封鎖裝置建立存取金鑰

1. 在網頁主控台主視窗中，選擇**資產（裝置）→受管理裝置**。

   受管理裝置的清單將開啟。

2. 選擇包含相關裝置的管理群組，然後選取裝置名稱旁的核取方塊。

3. 在受管理裝置清單上方，點擊**授予裝置離線存取權限**按鈕。如果裝置清單上方未顯示此按鈕，請點擊三個點按鈕，然後從選單中選擇**授予裝置離線存取權限**指令。

4. 這將開啟**應用程式設定**視窗；在該視窗的**裝置控制**部分，按一下**瀏覽**按鈕並下載從使用者收到的存取請求檔案。

   此時將顯示使用者要求存取的被封鎖裝置的資訊。

5. 如有必要，請在**存取持續時間**欄位中變更以小時為單位的持續時間。

   預設情況下，**存取持續時間**設定為使用者在產生存取請求檔案時指定的值。

6. 如有必要，請變更**指定存取金鑰可在用戶端裝置上使用多長時間（以小時為單位）**欄位中的值。

   此欄位包含使用者可以上傳存取金鑰的時間段。

7. 點擊**建立金鑰**按鈕。

8. 使用 *.acode 副檔名儲存存取金鑰檔案。

如何在命令列請求並取得暫時存取權限

如果使用者認為裝置存取遭誤封鎖，或對裝置內容執行的操作遭誤禁止，則可以使用下列裝置控制管理命令，向組織本機網路管理員請求對被封鎖裝置的暫時存取權限：

請求被封鎖裝置的暫時存取權限

```
kesl-control --request-temporary-device-access --device-id <device identifier>  --access-duration <access duration> --path <path to the access request file>
```

其中：

`--device-id <device identifier>` 是您要取得存取權之被封鎖裝置的 ID。

`--access-duration <access duration>` 是您要存取裝置的期間（以小時為單位）。可選值：1 到 100

`--path <path to the access request file>` 是您要儲存副檔名為 .akey 的存取請求檔案所在目錄的路徑。

此命令會建立一個存取請求檔案，該檔案必須傳送給管理員，例如透過電子郵件或其他方式（管理員可以在封鎖訊息範本中描述首選方法）。

收到管理員提供的存取金鑰後，您必須輸入該存取金鑰，以取得裝置的暫時存取權限。

上傳被封鎖裝置的存取金鑰

```
kesl-control --upload-temporary-device-access-key --path <path to the file with the access key>
```

其中：

`--path <path to the file with the access key>` 是包含裝置存取金鑰之檔案（副檔名為 .acode 的檔案）的路徑。

此命令會輸出有關已授予的裝置存取權限和存取持續時間的資訊。

如何在圖形介面請求並取得暫時存取權限

當裝置連線後，如果裝置控制拒絕存取該裝置，則會顯示一個視窗，其中包含有關裝置存取被封鎖的訊息。

您可以使用圖形介面向組織的本機網路管理員要求對被封鎖裝置的臨時存取權限：

- 在顯示裝置存取被封鎖訊息的視窗中，點擊**確定**
- 在應用程式圖形介面的主視窗中

請求對被封鎖裝置的臨時存取權限：

1. 開啟應用程式圖形介面的主視窗。
2. 在主視窗下方，點擊**臨時存取權限**按鈕。
   這將開啟**臨時存取權限**視窗。
   您也可以在顯示裝置存取被封鎖訊息的視窗中點擊**確定**來開啟**臨時存取權限**視窗。
3. 在**請求存取被封鎖裝置**部分，在已連線裝置清單中選擇要存取的裝置。
4. 在**裝置存取持續時間（小時）**欄位中，指定您希望取得裝置存取權限的時間段（以小時為單位）。
5. 點擊**建立請求存取檔案**按鈕。

6. 在開啟的視窗中，指定要儲存副檔名為 .akey 的存取請求檔案的目錄路徑。

7. 將存取請求檔案傳送給管理員，例如，透過電子郵件或任何可用的方式（管理員可以在封鎖訊息範本中配置此操作）。

從管理員處取得存取金鑰後，您可以上傳該存取金鑰以獲得對被封鎖裝置的臨時存取權限。

獲取對被封鎖裝置的臨時存取權限：

1. 開啟應用程式圖形介面的主視窗。

2. 在主視窗下方，點擊**臨時存取權限**按鈕。

   這將開啟**臨時存取權限**視窗。

3. 在**獲取裝置存取權限**部分，點擊**上傳存取金鑰**按鈕。

4. 在開啟的視窗中，選擇從組織的本機網路管理員收到的裝置存取金鑰檔案（副檔名為 .acode 的檔案）。

5. 螢幕上會顯示一個視窗，其中包含關於已授予存取權限的裝置以及存取持續時間的資訊。

6. 點擊**OK**。

Web 控制

“Web 控制”管理使用者對 Web 資源的存取。這可讓您減少流量消耗，並減少工作時間的不當使用。如果使用者嘗試開啟受 Web 控制限制存取的網站，Kaspersky Endpoint Security 會阻止存取或顯示警告。

Web 控制允許依內容類別和資料類型限制對 Web 資源的存取，以及封鎖對個別網站的存取。您可以限制使用者存取（例如）“社群網路”內容類別或其他類別。應用程式按照檔案格式而不是副檔名來確定資料類型。

Web 控制的運作方式

1. **應用程式檢查對 Web 資源的請求**

   Web 控制使用以下技術確定網站的內容類別和資料類型：

   - 病毒資料庫。
   - 卡巴斯基安全網路的雲端服務。
   - 啟發式分析技術可偵測卡巴斯基資料庫尚未涵蓋的威脅。

2. **應用程式套用規則**

   應用程式按優先順序套用 Web 控制規則。優先順序編號越低，規則的優先順序越高。如果有多個規則適用於某個網站，Web 控制會套用優先順序最高的規則。

   例如，應用程式可以將企業入口網站識別為社群網路。要限制對社群網路的存取並提供對公司 Web 入口的存取權限，請建立兩條規則：一條針對“*社群網路*”網站類別的封鎖規則和一條針對公司 Web 入口網站的允許規則。企業入口網站存取規則的優先順序必須高於社群網路存取規則。

3. **掃描完成**

   如果規則封鎖對 Web 資源的存取，應用程式會在瀏覽器中顯示封鎖訊息。該資源將無法使用。

   如果使用者認為網頁遭到誤封鎖，可以向組織的管理員傳送誤封鎖請求。

設定 Web 控制

1. **設定 Web 控制規則**

   Web 控制會使用*存取規則*管理使用者對網站的存取。這些規則可限制個別使用者對網站的存取，以及設定存取排程。

   例如，您可以限制組織內除 IT 部門外的所有使用者存取 *網際網路通訊* 類別中的網站。

2. **設定訊息範本**

   根據存取規則的動作，Web 控制會向使用者顯示關於造訪不需要網站的訊息或封鎖訊息。當網站遭到封鎖時，使用者可以向本機網路管理員傳送關於誤封鎖的訊息。

   系統提供了用於此類訊息的範本。

   無法在命令列上編輯範本。

3. **啟用 Web 控制**

   預設情況下，Web 控制已停用。您可以在網頁主控台或管理主控台中使用切換開關啟用該元件，或在命令列上使用以下命令啟用該元件：

```
kesl-control --start-task 26
```

特殊考量與限制

- 該應用程式不會掃描壓縮檔案內的檔案。例如，如果映像檔案被存檔，應用程式會將資料類型偵測為壓縮檔案而不是映像檔案。
- Kaspersky Endpoint Security 僅監控 HTTP 和 HTTPS 流量。
- 當 Web 威脅防護和 Web 控制同時執行時，Web 威脅防護設定會套用至 Web 資源。這表示即使 Web 控制規則允許存取惡意網站或網路釣魚網站，該網站也會遭到封鎖。

如何建立網頁資源的存取規則

*網頁資源存取規則*是使用者造訪網頁資源時 Kaspersky Endpoint Security 套用的一個篩選器和動作集合。存取規則可以包括規則排程。

規則會依下列篩選器限制對網頁資源的存取：

- **內容類別**Web 控制會依內容和資料類型將網頁資源分類。這可讓您限制使用者存取具有特定內容類別（例如 *支付系統*）及/或特定資料類型（例如 *可執行檔*）的網站。
- **單個網站**Web 控制可限制使用者對網頁資源的個別網址或網址群組的存取。

  網址的網域不區分大小寫。如果規則包含 `examPLE.com` 這類網址，Web 控制將限制對 `example.com` 的存取。

  如果在存取規則中同時設定依內容類別篩選器和依個別網站篩選器，Web 控制不會限制對指定內容類別中所有網站的存取，而只會限制對指定網址的存取。
- **按使用者和使用者群組名稱進行篩選**。Web 控制可限制個別使用者或使用者群組對網頁資源的存取。例如，您可以限制組織中除 IT 部門以外的所有使用者存取社群媒體網站。
- **規則排程**。規則排程決定應用程式控制對規則中指定的 Web 資源的存取控制的時間。例如，您可以僅在工作時間限制對不需要的網站的存取。

> 如果沒有建立封鎖規則，則不會解密 HTTPS 流量。

如何在網頁主控台中建立存取規則

1. 在網頁主控台的主視窗中，選擇**資產管理 → 政策**。
2. 點擊 Kaspersky Endpoint Security 政策的名稱。

   政策內容視窗將開啟。
3. 選擇"**應用程式設定**"標籤。
4. 轉到"**安全控制**"→"**Web 控制**"。
5. 確保該元件的切換開關處於 **Web 控制已啟用** 位置。
6. 在 **規則清單** 下，選取預設的 Web 控制動作：
   - **允許除規則清單外的所有內容**
   - **封鎖除規則清單外的所有內容**
7. 點擊"**新增**"。

   這將開啟新增存取規則的表單。
8. 在 **規則名稱** 欄位中，輸入規則名稱。規則名稱必須唯一。
9. 在 **優先順序** 欄位中，設定存取規則優先順序。

10. 選取當規則觸發時，您希望 Web 控制套用至網頁資源的動作：

- **允許**Web 控制允許使用者存取 Web 資源。
- **封鎖**Web 控制將阻止使用者對 Web 資源的存取並顯示存取被封鎖的訊息。使用者可以透過點擊封鎖訊息中的連結，向本機網路管理員傳送訊息以回報封鎖錯誤。
- **通知**Web 控制會顯示有關造訪不需要的網頁資源的警告。如果使用者認為警告不正確，警告中的連結可讓使用者前往網頁或向組織的本機網路管理員傳送請求。

11. 選取存取規則篩選器：

- **內容類別**指定您希望存取規則控制的內容類別。您可以選取多個類別。
- **單個網站**指定網站位址或網站群組。

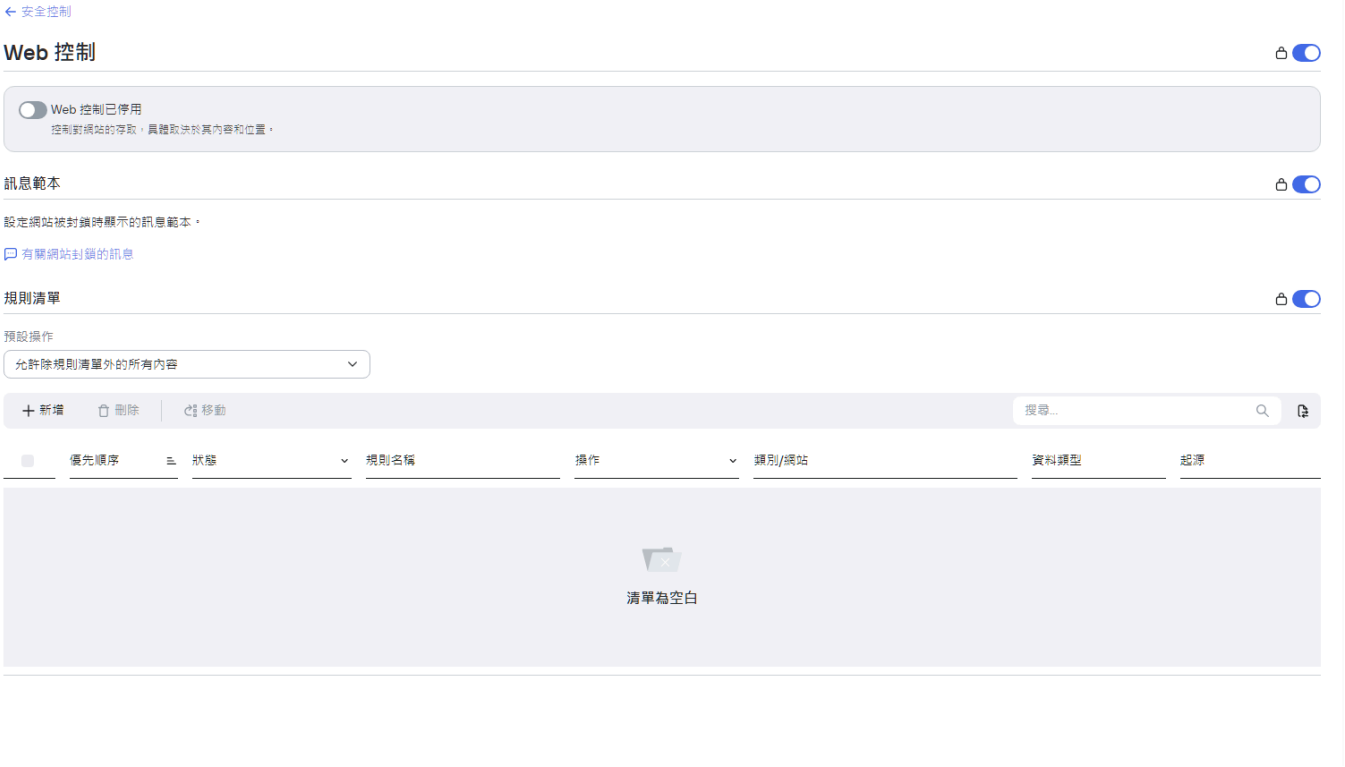
> 在網頁主控台中，您無法同時依內容類別和個別網站設定篩選器。

12. 如有必要，請指定您希望應用程式篩選的資料類型。

13. 選取存取規則將套用的使用者或使用者群組。預設情況下，此規則適用於所有使用者。

14. 如有必要，請設定存取排程。預設情況下，此規則一律套用。

15. 要將此政策套用到電腦，請關閉... 掛鎖圖示並儲存變更。



Web 控制

如何在命令列建立存取規則

1. 請確保 Web 控制元件已啟用：

```
kesl-control --get-settings 26
```

元件必須處於 **已啟動** 狀態。

2. 如果元件已停用，請執行下列命令：

```
kesl-control --start-task 26
```

3. 選取預設的 Web 控制動作：

```
kesl-control --set-settings 26 WebControlDefaultAction=<Allow|Block>
```

4. 新增 ID 為 `#` 的存取規則：

   a. 啟用規則：

   ```
   kesl-control --set-settings 26 Rules.item_#.Enabled=Yes
   ```

   b. 輸入規則名稱：

   ```
   kesl-control --set-settings 26 Rules.item_#.Name=<rule name>
   ```

   c. 指定當規則觸發時，您希望 Web 控制套用至網頁資源的動作：

   ```
   kesl-control --set-settings 26 Rules.item_#.WebControlAction=<Allow|Block|Notify>
   ```

   d. 如果您需要依內容類別篩選網頁資源：

   ```
   kesl-control --set-settings 26 Rules.item_#.UseCategories=<ContentOnly|FormatOnly|ContentAndFormat>
   kesl-control --set-settings 26 Rules.item_#.ContentCategories.item_#.ContentCategory=<category>
   [Rules.item_#.FormatCategories.item_#.FormatCategory=<format>]
   ```

   e. 如果您需要篩選個別網頁資源：

   ```
   kesl-control --set-settings 26 Rules.item_#.UseUrls=Yes
   kesl-control --set-settings 26 Rules.item_#.Urls.item_#=<web address>
   ```

   f. 如有必要，請指定規則將套用的使用者：

   ```
   kesl-control --set-settings 26 Rules.item_#.UsePrincipals=Yes
   kesl-control --set-settings 26 Rules.item_#.Principals.item_#.Name=<user name|@group name>
   ```

g. 如有必要，請指定規則的排程：

```
kesl-control --set-settings 26 Rules.item_#.Schedules.item_#.Id=<ID> Rules.item_#.Schedules.item_#.Name=
<schedule name> Rules.item_#.Schedules.item_#.DaysHours=<day of the week|hour>
```

5. 若要檢視 Web 控制規則清單，請執行以下命令：

```
kesl-control --get-settings 26
```

符號

命令選項

設定	描述
WebControlDefaultAction	Web 控制對未在任何存取規則中指定的 Web 資源套用的操作。
Enabled=Yes	啟用 ID 為 # 的存取規則。
Name	規則名稱。規則名稱必須唯一。
WebControlAction	Web 控制在規則觸發時對 Web 資源套用的操作： Allow(預設值) — 允許存取 Web 資源。 Block — 阻止存取 Web 資源。 Notify – 顯示造訪不需要的 Web 資源的警告。透過點擊警告訊息中的連接，使用者可以存取所請求的 Web 資源。
UseCategories	在規則中使用依內容類別和資料類型類別區分的篩選器： None（預設）— 不使用 Web 資源內容篩選器。 ContentOnly — 在規則中使用內容類別篩選器。 FormatOnly — 在規則中使用資料類型類別篩選器。 ContentAndFormat — 在規則中使用內容類別篩選器和資料類型類別篩選器。
ContentCategories.item_#.ContentCategory	內容類別。
FormatCategories.item_#.FormatCategory	資料類型類別： Video – 視訊檔案 Audio – 音訊檔案 OfficeDocument — Office 應用程式檔案 Executable — 可執行檔 Archives — 壓縮檔案 Images — 映像檔案 Scripts — 指令碼
UseUrls=Yes	在篩選規則中使用個別網站。
Urls.item_#	規則控制存取控制的 Web 資源的位址。您可以使用遮罩來指定 Web 資源位址。
UsePrincipals=Yes	使用受 Web 資源存取規則涵蓋的使用者篩選器。
Principals.item_#.Name	Web 資源存取規則涵蓋的使用者或使用者群組： <user name> 是規則適用的使用者名稱。 @<group name> 是規則適用的使用者群組名稱。
Schedules.item_#.Id	排程 ID。
Schedules.item_#.Name	指定排程名稱。
Schedules.item_#.DaysHours	指定排程的時間間隔： <day of week> 是星期幾。您可以使用星期的完整名稱或縮寫（例如，若為星期一，您可以指定 Mo、Mon 或 Monday）。對於星期幾，您可以指定間隔或特定日期。一周從週日開始。 <hour> – 小時 [0:24]。您只能指定小時的間隔。

如何修改 Web 控制訊息範本

根據存取規則中指定的操作，當使用者嘗試存取 Web 資源時，Web 控制會向使用者顯示訊息（透過將 HTTP 伺服器回應取代為包含訊息的 HTML 頁面）：

- **警告。**使用者嘗試造訪不需要的資源時，向使用者顯示的訊息。如果已為規則選擇 **通知** 動作，應用程式會顯示此訊息。

  如果使用者認為警告不正確，警告中的連結可讓使用者前往網頁或向組織的本機網路管理員傳送請求。

- **已封鎖的 Web 資源訊息** 封鎖不需要的 Web 資源時，向使用者顯示的訊息。如果已為規則選擇 **封鎖** 動作，應用程式會顯示此訊息。

  如果使用者認為 Web 資源遭到錯誤封鎖，Web 資源封鎖訊息中的連結可讓使用者向組織的區域網路管理員提交請求。

提供了警告訊息、Web 資源封鎖訊息以及向組織的區域網路管理員傳送的請求範本。提供了特殊變數來管理訊息範本（例如 `%USER_NAME%`）。變數可讓單一訊息範本套用至不同電腦。在產生訊息時，Kaspersky Endpoint Security 會從作業系統設定中擷取變數值，並將其插入與特定電腦、使用者及事件對應的訊息中。

無法在命令列上編輯範本。

如何在網頁主控台中編輯訊息範本

1. 在網頁主控台的主視窗中，選擇**資產管理 → 政策**。
2. 點擊 Kaspersky Endpoint Security 政策的名稱。

   政策內容視窗將開啟。
3. 選擇"**應用程式設定**"標籤。
4. 轉到"**安全控制**"→"**Web 控制**"。
5. 在 **訊息範本** 下，點擊 **有關網站封鎖的訊息** 連結。

   這會開啟包含訊息範本的視窗。
6. 配置 Web 控制訊息範本：

   - **警告**使用者嘗試造訪不需要的資源時，向使用者顯示的警告範本。
   - **有關封鎖的訊息**封鎖不需要的網頁或網站時顯示的訊息範本。
   - **傳送給管理員的郵件**傳送給管理員的訊息範本。在使用者認為網頁遭到錯誤封鎖時使用。使用者請求存取後，應用程式會將 *傳送給管理員的網頁存取封鎖訊息* 事件傳送至卡巴斯基安全管理中心。事件描述包含給管理員的訊息，其中變數被其值取代。如果您的組織中未部署卡巴斯基安全管理中心解決方案或沒有與管理伺服器連線，則應用程式將向管理員指定的電子郵件地址傳送訊息。

   如果您想還原訊息範本的文字，請點擊 **重設為預設文字** 按鈕。
7. 要將此政策套用到電腦，請關閉... 掛鎖圖示並儲存變更。

如何在管理主控台中變更訊息範本

1. 在管理主控台樹狀圖中的**受管理裝置**資料夾中，開啟包含所需裝置所屬的管理群組名稱的資料夾。

2. 在工作區選擇“**政策**”標籤。

3. 在政策清單中，選擇所需的政策，然後開啟**屬性：<政策名稱>**視窗。

   您也可以透過使用政策右鍵功能表中的**屬性**項目或點擊位於政策設定部分中政策清單右側的**配置政策設定**連結來開啟政策屬性視窗。

4. 在政策視窗中，選擇**安全控制→ Web 控制**。

5. 在**訊息範本**部分，點擊**配置**按鈕。

6. 這將開啟**訊息範本**視窗；在該視窗中，在以下索引標籤上配置 Web 控制訊息範本：

   - **警告**。輸入欄位包含觸發規則時出現的訊息模板，該訊息警告嘗試存取不良 Web 資源。

   - **封鎖訊息**。該項目欄位包含某個封鎖存取網頁資源的規則被觸發時要顯示的訊息的範本。

   - **向管理員投訴**。輸入欄位包含當使用者認為被封鎖的 Web 資源不應被封鎖時要傳送給企業區域網路管理員的投訴範本。在使用者請求存取後，Kaspersky Endpoint Security 會向卡巴斯基安全管理中心傳送一個*關於被拒絕存取網頁緻管理員的訊息*事件。事件描述包含給管理員的訊息，其中變數被其值取代。您可以使用**使用者要求**選擇在卡巴斯基安全管理中心主控台中檢視這些事件。如果您的組織中未部署卡巴斯基安全管理中心解決方案或沒有與管理伺服器連線，則應用程式將向管理員指定的電子郵件地址傳送訊息。

   在**警告**和**封鎖訊息**索引標籤上，您可以使用**變數**和**連結**按鈕為使用者訊息新增變數和連結。

   您可以透過點擊**預設**按鈕來還原訊息範本的文字。

7. 點擊**OK**。

8. 點擊“**套用**”。

用於建立 Web 資源位址遮罩的規則

當建立 Web 資源存取規則時必須輸入大量類似的 Web 資源位址時時，*Web 資源位址遮罩*（“位址遮罩”）會很方便。一個精心建構的位址遮罩可以取代大量的 Web 資源位址。

建立位址遮罩時需遵循以下規則：

1. `*`字元可替換零個或多個字元的任意序列。

   例如，如果您輸入位址遮罩`*abc*`，Web 資源存取規則將套用至所有包含序列`abc`的位址。範例：`http://www.example.com/page_0-9abcdef.html`。

2. 字元序列`*.`可讓您選擇一個位址的所有網域，即它代表一個*網域遮罩*。網域遮罩`*.`被解釋為任何網域、子網域或空字串。

   範例：以下位址與`*.example.com`遮罩相符：

   - `http://pictures.example.com` – 網域遮罩 `*.` 符合 `pictures.`。

   - `http://user.pictures.example.com` — 網域遮罩`*.`匹配`pictures.`和`user.`。

   - `http://example.com` — 網域遮罩`*.`被解釋為空字串。

3. 位址遮罩開頭的字元序列`www.`被解釋為序列`*.`。

   範例：位址遮罩`www.example.com`被解釋為`*.example.com`。此遮罩與位址`www2.example.com`和`www.pictures.example.com`相符。

4. 如果位址遮罩不以`*`字元開頭，則該位址遮罩相符的內容與以`*.`開頭時相符的內容相同。

5. 如果位址遮罩以`/`或`*`以外的字元結尾，則該位址遮罩相符的內容與以`/*`結尾時相符的內容相同。

   範例：位址遮罩`http://www.example.com`與`http://www.example.com/abc`形式的位址匹配，其中`a`、`b`、`c`是任意字元。

6. 如果位址遮罩以`/`字元結尾，則該位址遮罩相符的內容與以`/*`結尾時相符的內容相同。

7. 字元序列`/*`將被解釋為`/*`或空字串。

8. 當將 Web 資源位址與位址遮罩進行比較時，會考慮協定（http: 或 https:）。

   - 如果位址遮罩中沒有網路協定，則位址遮罩將匹配具有任何網路協定的位址。

     範例：位址遮罩`example.com`與位址`http://` `example.com`和`https://` `example.com`相符。

   - 如果位址遮罩中存在網路協定，則只有具有相同網路協定的位址才會與位址遮罩相符。

     範例：位址遮罩`http://*.example.com`與位址`http://www.example.com`匹配，但與位址`https://www.example.com`不符。

9. 用雙引號括起來的位址遮罩無需進行任何進一步的替換即可解釋，但如果`*`字元最初包含在位址遮罩中則為例外。對於用雙引號括起來的位址遮罩，不強制執行規則 5 和 7（請參閱下表中的範例 14–18）。

10. Web 資源位址遮罩的評估不考慮使用者名稱和密碼、連線連接埠或大小寫。

套用規則以建構位址遮罩的範例

編號	位址遮罩	Web 資源位址	位址是否與位址遮罩相符？	註解
1	*.example.com	http://www.123example.com	否	參閱規則 1。
2	*.example.com	http://www.123.example.com	是	參閱規則 2。
3	*example.com	http://www.123example.com	是	參閱規則 1。
4	*example.com	http://www.123.example.com	是	參閱規則 1。
5	http://www.*.example.com	http://www.123example.com	否	參閱規則 1。
6	www.example.com	http://www.example.com	是	請參閱規則 3、2 和 1。
7	www.example.com	https://www.example.com	是	請參閱規則 3、2 和 1。
8	http://www.*.example.com	http://123.example.com	是	請參閱規則 3、4 和 1。
9	www.example.com	http://www.example.com/abc	是	請參閱規則 3、5 和 1。
10	example.com	http://www.example.com	是	請參閱規則 3 和 1。
11	http://example.com/	http://example.com/abc	是	參閱規則 6。
12	http://example.com/*	http://example.com	是	參閱規則 7。
13	http://example.com	https://example.com	否	參閱規則 8。
14	"example.com"	http://www.example.com	否	參閱規則 9。
15	"http://www.example.com"	http://www.example.com/abc	否	參閱規則 9。
16	"*.example.com"	http://www.example.com	是	請參閱規則 1 和 9。

編號	位址遮罩	Web 資源位址	位址是否與位址遮罩相符？	註解
17	"http://www.example.com/*"	http://www.example.com/abc	是	請參閱規則 1 和 9。
18	"www.example.com"	http://www.example.com; https://www.example.com	是	請參閱規則 9 和 8。
19	www.example.com/abc/123	http://www.example.com/abc	否	位址遮罩比 Web 資源位址包含更多資訊。

應用程式控制

應用程式控制可管理使用者裝置上第三方應用程式的啟動。這可降低受保護裝置感染惡意軟體的風險。

要使用該元件，需要包含相應功能的產品授權。

應用程式控制的運作方式

1. **使用者嘗試執行第三方應用程式**
2. **應用程式控制套用規則**

   應用程式控制會依序將規則套用至正在啟動的應用程式。元件會根據所選規則模式*控制*正在啟動的應用程式或*測試*規則。封鎖規則的優先等級高於允許規則的優先等級。
3. **掃描完成**

   如果規則阻止應用程式執行，該元件會封鎖此應用程式的啟動並產生 *已禁止應用程式啟動* 事件。在測試模式下，該元件不會封鎖此應用程式的啟動，並會產生 *禁止應用程式在測試模式下啟動* 事件。

設定應用程式控制

1. **清查應用程式**

   使用 清查 工作取得受保護裝置上已安裝應用程式的清單。根據此資訊，建立您要阻止執行的應用程式清單。
2. **選取應用程式控制操作模式**

   應用程式元件可以在以下兩種模式之一下運行：

   - *允許除規則清單外的所有內容*應用程式控制允許使用者執行任何第三方應用程式，規則禁止的應用程式除外。
   - *封鎖除規則清單外的所有內容*應用程式控制允許使用者執行任何第三方應用程式，規則允許且未禁止的應用程式除外。

   應用程式控制模式的選擇取決於貴組織的安全政策，以及您要控制的應用程式數量。
3. **建立應用程式類別**

定義允許或拒絕之應用程式的類別。應用程式類別適用於公司網路中的所有裝置，與管理群組無關。應用程式類別可讓您針對一組應用程式設定規則，而不是根據包含與排除條件設定規則。

建議您建立涵蓋公司內所使用的標準應用程式集的"工作應用程式"類別。如果工作中不同的使用者群組使用不同的應用程式集，則可以為每個使用者群組建立單獨的應用程式類別。

建議您在卡巴斯基安全管理中心中設定應用程式類別。

4. **設定應用程式控制規則**

   此元件會根據*應用程式控制規則*控制應用程式啟動，這些規則定義了應用程式控制允許或拒絕為所選使用者群組啟動第三方應用程式的條件。

5. **測試應用程式控制規則**

   預設情況下，應用程式控制被停用。建議您在測試模式下啟用應用程式控制，並測試已建立的應用程式控制規則。應用程式不會封鎖第三方應用程式執行，但會將其啟動通知傳送至管理伺服器。

6. **瞭解應用程式控制規則的運作方式**

   檢視有關應用程式控制在測試模式下運作的報告。檢視資訊後，視需要調整您的應用程式控制規則。

7. **啟用應用程式控制規則**

   在此模式下，如果規則不允許執行第三方應用程式，Kaspersky Endpoint Security 會阻止這些應用程式執行。

   如何在網頁主控台中啟用應用程式控制規則

   1. 在網頁主控台的主視窗中，選擇**資產管理 → 政策**。
   2. 點擊 Kaspersky Endpoint Security 政策的名稱。
      政策內容視窗將開啟。
   3. 選擇"**應用程式設定**"標籤。
   4. 轉到"**安全控制**"→"**應用程式控制**"。
   5. 確保該元件的切換開關處於 **應用程式控制已啟用** 位置。
   6. 在 **啟動應用程式時的動作** 下，為應用程式控制選取 **套用規則** 操作。
   7. 要將此政策套用到電腦，請關閉... 掛鎖圖示並儲存變更。

   如何在命令列中啟用應用程式控制規則

   若要選取應用程式控制的測試模式，請執行以下命令：

```
kesl-control --set-settings 21 AppControlRulesAction=ApplyRules
```

卡巴斯基安全管理中心管理員或在應用程式中指派了管理員角色的本機使用者可以使用應用程式控制允許或拒絕在根帳戶下啟動處理程序。

特殊考量與限制

- 應用程式控制不控制 Snap、Flatpak 或 AppImage 應用程式的啟動。
- 應用程式控制工作不控制從 Kaspersky Endpoint Security 不支援的解釋器啟動指令碼，或啟動未透過指令列傳遞給解釋器的指令碼。Kaspersky Endpoint Security 支援以下解釋器：python、perl、bash、ssh。
- 如果規則允許解譯器執行，應用程式控制不會封鎖從該解譯器啟動的指令碼。如果規則禁止啟動解譯器命令列中指定的至少一個指令碼，Kaspersky Endpoint Security 會封鎖解譯器命令列中指定的所有指令碼。排除：cat script.py | Python。

應用程式清查

若要建立最佳的 應用程式控制規則，建議先瞭解公司 LAN 中受保護裝置上使用的應用程式。透過 *清查* 工作，您可以取得以下資訊：

- 第三方應用程式的名稱和版本
- 簡短描述

要使用該工作，需要包含相應功能的產品授權。

卡巴斯基安全管理中心資料庫可以儲存最多 150,000 條已處理檔案的資訊。達到限制後，將不再處理新檔案。若要恢復清查，您需要從受保護裝置中刪除先前清查期間新增至卡巴斯基安全管理中心資料庫的檔案。

設定並執行清查工作

1. **建立清查工作**

   如何在網頁主控台中建立清查工作

   1. 在網頁主控台的主視窗中，選擇**工作**。

      工作清單開啟。

   2. 點擊“**新增**”。

      啟動“工作精靈”。

   3. 配置工作設定：

      a. 在“**應用程式**”下拉式清單中，選取“**Kaspersky Endpoint Security for Linux 12.5**”。

      b. 在“**工作類型**”下拉式清單中，選取“**Inventory**”。

      c. 在 **工作名稱** 欄位中，輸入工作名稱。

      d. 在“**要將工作指派給的裝置**”塊中，選取工作範圍。

4. 按照所選工作範圍選項選取裝置。

5. 完成精靈。

如何在命令列中建立清查工作

若要建立工作，請執行以下指令：

```
kesl-control --create-task <task name> --type InventoryScan
```

其中 `<task name>` 是新工作名稱。

此指令會傳回已建立工作的 ID。

指令執行結果範例：

工作已建立（工作 ID：100）

2 **設定清查範圍**

若要啟動工作，必須指定至少一個清查範圍。預設會設定 *可執行指令* – `/usr/bin` 範圍。

Kaspersky Endpoint Security 依照物件在範圍清單中出現的順序掃描指定範圍內的物件。如果有必要，將子目錄放在清單中高於其父目錄的位置，以便為子目錄配置與父目錄的安全性設定不同的安全性設定。

如何在網頁主控台中設定清查範圍

1. 在網頁主控台的主視窗中，選擇**工作**。

   工作清單開啟。

2. 點擊已建立的清查工作。

   工作內容視窗將開啟。

3. 選擇"**應用程式設定**"標籤。

4. 轉到"**清查範圍**"區域。

5. 點擊"**新增**"。

   這會開啟用於新增清查範圍的視窗。

6. 在 **範圍名稱** 欄位中，輸入清查範圍的名稱，例如 *桌面上的檔案*。

7. 在 **路徑** 欄位中，指定個別檔案或目錄的路徑，例如 `/path/to/folder`。Kaspersky Endpoint Security 輸入遮罩時支援 `*` 和 `?` 字元。

8. 如有必要，請以命令 shell 格式指定物件名稱的遮罩，例如 `*.txt`、`file?.*`。一次新增一個遮罩。

9. 儲存變更。

如何在命令列中設定清查範圍

1. 執行以下指令：

```
kesl-control --set-settings <task name | task ID> ScanScope.item_#.UseScanArea=Yes
        [ScanScope.item_#.AreaDesc=<description of the area>\]
        [ScanScope.item_#.AreaMask.item_#=<mask in shell format>\]
        ScanScope.item_#.Path=<path to the directory>
```

2. 若要檢查目前設定，請執行以下指令：

```
kesl-control --get-settings <task name | task ID>
```

符號

清查工作設定

設定	描述
UseScanArea=Yes	啟用 ID 為 # 的清查範圍。 您可以暫時停用清查範圍掃描，而不是刪除該範圍。若要這麼做，請設定 ScanScope.item_#.UseScanArea=No。
AreaDesc	清查範圍的描述。使用此設定指定的字串的最大長度為 4096 個字元。
AreaMask.item_#	清查掃描範圍限制。在清查範圍內，應用程式僅掃描使用 shell 格式的遮罩指定的物件。 您可以以任意順序指定多個 ScanScope.item_#.AreaMask.item_# 項目。應用程式按索引的升序處理範圍。 例如，ScanScope.item_0001.AreaMask.item_0001=*.exe ScanScope.item_0001.AreaMask.item_0002=*.txt。
Path	包含要掃描的物件的目錄的路徑。Kaspersky Endpoint Security 輸入遮罩時支援 * 和 ? 字元。 預設值：/usr/bin

3. **如有必要，請編輯工作設定**

如何在網頁主控台中設定清查工作

1. 在網頁主控台的主視窗中，選擇**工作**。
   工作清單開啟。
2. 點擊已建立的清查工作。
   工作內容視窗將開啟。
3. 選擇“**應用程式設定**”標籤。
4. 轉到“**清查設定**”區域。
5. 選擇對「黃金映像」應用程式類別執行的動作：
   - **無變更** – 完成清查後，不變更「黃金映像」類別。這是預設選項。當您想要取得裝置上使用的第三方應用程式清單，但不將其新增至「黃金映像」類別時，可以使用此選項。
   - **更新或建立（如果不存在）** – 將清查工作在裝置上偵測到的應用程式新增至「黃金映像」類別。如果該類別不存在，則建立該類別。如果該類別存在，則更新該類別中的應用程式清單。
   - **移除** – 清除「黃金映像」應用程式類別。此類別會在工作啟動後立即清除，不會對裝置上的檔案執行清查。

6. 如有必要，請選取以下核取方塊：

   - **指令碼檔案清查**檢查清查範圍內是否有指令碼。應用程式會將此資訊傳送至卡巴斯基安全管理中心。
   - **掃描所有可執行檔**
   - **掃描二進位檔案**掃描二進位檔案（副檔名為 .elf、.java 和 .pyc 的檔案）。

7. 儲存變更。

如何在命令列中設定清查工作

執行命令：

```
kesl-control --set-settings <task name | task ID> ScanScripts=<Yes|No> ScanBinaries=<Yes|No>
ScanAllExecutable=<Yes|No> GoldenImageAction=<DoNothing|Create|Remove>
```

符號

清查工作設定

設定	描述
ScanScripts	檢查清查區域內是否有指令碼： Yes（預設值）— 掃描指令碼。 No — 不掃描指令碼。
ScanBinaries	掃描二進位檔案（副檔名為 .elf、.java 和 .pyc 的檔案）： Yes（預設值）— 掃描二進位。 No — 不掃描二進位檔案。
ScanAllExecutable	掃描可執行檔案： Yes（預設值）— 掃描具有可執行位元的檔案。 No — 不掃描具有可執行位的檔案。
GoldenImageAction	完成清查工作後，Kaspersky Endpoint Security 必須對「黃金映像」應用程式類別執行的動作： DoNothing（預設）– 不要變更「黃金映像」應用程式類別。 Create – 將偵測到的應用程式新增至「黃金映像」應用程式類別。如果該類別不存在，則建立該類別。如果該類別存在，則更新該類別中的應用程式清單。 Remove – 清除「黃金映像」應用程式類別。此類別會在工作啟動後立即清除，不會對裝置上的檔案執行清查。

4 設定排除範圍

排除的優先順序高於清查範圍。排除的物件即使位於清查範圍內，也不會被掃描。如果清查範圍定義的層級低於排除目錄，則應用程式會在執行工作時跳過此清查範圍。

如何在網頁主控台中設定排除範圍

1. 在網頁主控台的主視窗中，選擇**工作**。
2. 工作清單開啟。
3. 點擊已建立的清查工作。
   工作內容視窗將開啟。
4. 選擇“**應用程式設定**”標籤。
5. 轉到“**排除範圍**”區域。

6. 點擊“**新增**”。

   這將開啟用於新增排除範圍的視窗。

7. 在 **範圍名稱** 欄位中，指定排除範圍的名稱，例如 *系統檔案*。

8. 在 **路徑** 欄位中，指定個別檔案或目錄的路徑（例如 `/path/to/folder`）。Kaspersky Endpoint Security 輸入遮罩時支援`*`和`?`字元。

9. 請以命令 shell 格式指定物件名稱的遮罩（例如 `*.txt` 或 `file?.*`）。一次新增一個遮罩。

10. 儲存變更。

如何在命令列上設定排除範圍

1. 執行以下指令：

```
kesl-control --set-settings <task name | task ID>       ExcludedFromScanScope.item_#.UseScanArea=Yes
        [ExcludedFromScanScope.item_#.AreaDesc=<description of the area>\]
        [ExcludedFromScanScope.item_#.AreaMask.item_#=<mask in shell format>\]
        ExcludedFromScanScope.item_#.Path=<path to the directory>
```

2. 若要檢查目前設定，請執行以下指令：

```
kesl-control --get-settings <task name | task ID>
```

符號

清查工作設定

設定	描述
`UseScanArea`	從清查中排除指定的範圍。 您可以暫時停用排除範圍，而不是刪除該範圍。若要這麼做，請設定 `ExcludedFromScanScope.item_#.UseScanArea=No`。
`AreaDesc`	清查排除範圍的描述。
`AreaMask.item_#`	排除範圍的限制。在排除範圍中，應用程式僅會從掃描中排除使用 shell 格式的遮罩指定的物件。 您可以以任意順序指定多個`ExcludedFromScanScope.item_#.AreaMask.item_#`項目。應用程式按索引的升序處理範圍。 例如，`ExcludedFromScanScope.item_0001.AreaMask.item_0001=*.exe` `ScanScope.item_0001.AreaMask.item_0002=*.txt`。
`Path`	要從清查中排除的目錄路徑。Kaspersky Endpoint Security 輸入遮罩時支援`*`和`?`字元。

從清查中排除 `/tmp` 目錄的範例：

```
kesl-control --set-settings 100 ExcludedFromScanScope.item_0001.UseScanArea=Yes
ScanScope.item_0001.Path=/tmp
```

5 執行工作

如何在網頁主控台中執行清查工作

1. 在網頁主控台的主視窗中，選擇**工作**。

   工作清單開啟。

2. 選取已建立的工作旁邊的核取方塊。

3. 點擊“**開始**”。

如何在命令列中執行清查工作

若要執行工作，請執行以下指令：

```
kesl-control --start-task <task ID|name> [-W] [--progress]
```

其中：

- `<task ID|name>` 是任務建立時指派的 ID，或是命令列中的任務名稱。
- `[-W]` 啟用與此工作相關的目前事件的輸出。
- `[--progress]` 啟用工作進度顯示。

檢視偵測到的應用程式清單

若要在網頁主控台中檢視裝置上偵測到的應用程式清單：

1. 在網頁主控台的主視窗中，選擇**工作**。
   工作清單開啟。
2. 點擊已建立的清查工作。
   工作內容視窗將開啟。
3. 選擇“**結果**”標籤。

檢視用戶端裝置上偵測到的應用程式清單

```
kesl-control --get-app-list [--json]
```

Kaspersky Endpoint Security 可顯示關於偵測到的應用程式的以下資訊：

- 清查的日期和時間
- 應用程式數量
- 包含以下資訊的應用程式清單：
  - 應用程式的路徑。
  - 應用程式雜湊總和。
  - 應用程式類型。例如，`Script`，`Executable`。
  - 應用程式所屬的類別（如果先前已建立）。您可以使用以下指令檢視已建立的應用程式類別清單：

    ```
    kesl-control --get-categories
    ```

新增類別時，其資訊不會在應用程式清單中自動更新。若要更新應用程式清單，您必須再次執行清查工作。

如何設定應用程式控制操作模式

應用程式元件可以在以下兩種模式之一下運行：

- *允許除規則清單外的所有內容*應用程式控制允許使用者執行任何第三方應用程式，規則禁止的應用程式除外。
- *封鎖除規則清單外的所有內容*應用程式控制允許使用者執行任何第三方應用程式，規則允許且未禁止的應用程式除外。

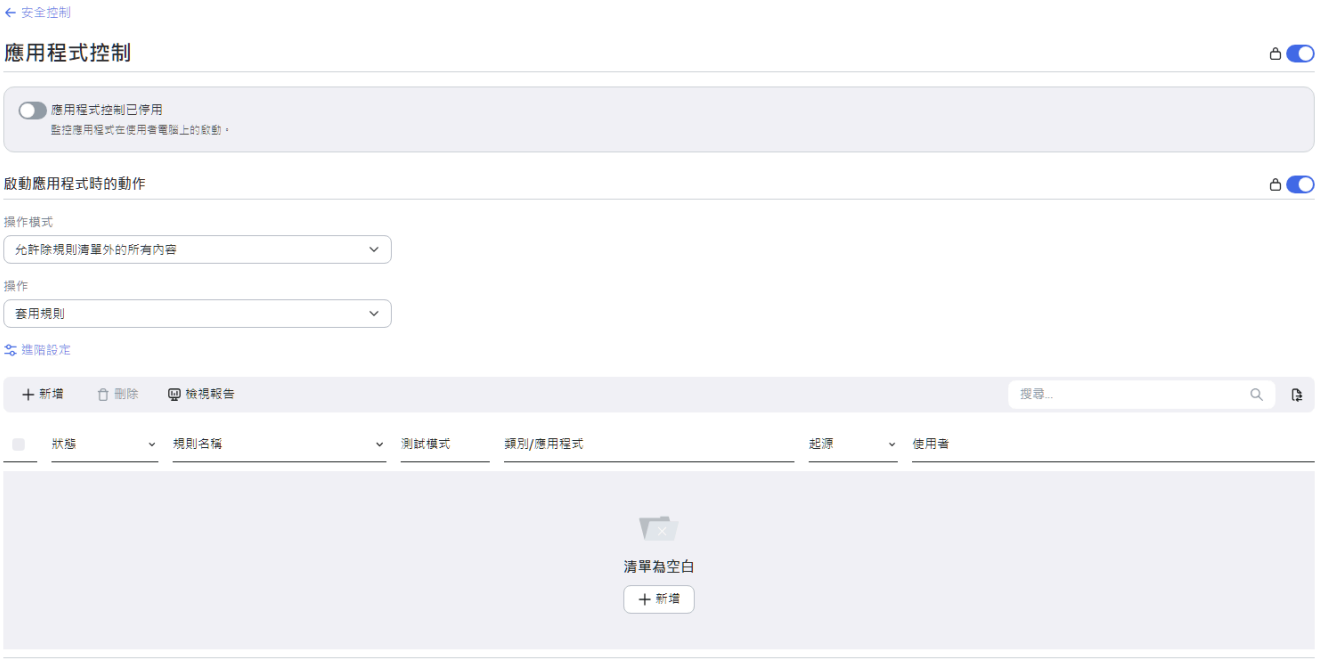
應用程式控制模式的選擇取決於貴組織的安全政策，以及您要控制的應用程式數量。

如何在網頁主控台中設定應用程式控制操作模式

1. 在網頁主控台的主視窗中，選擇**資產管理 → 政策**。
2. 點擊 Kaspersky Endpoint Security 政策的名稱。

   政策內容視窗將開啟。
3. 選擇"**應用程式設定**"標籤。
4. 轉到"**安全控制**"→"**應用程式控制**"。
5. 確保該元件的切換開關處於 **應用程式控制已啟用** 位置。
6. 在 **啟動應用程式時的動作** 下，選取應用程式控制操作模式：
   - **允許除規則清單外的所有內容**
   - **封鎖除規則清單外的所有內容**

7. 要將此政策套用到電腦，請關閉... 掛鎖圖示並儲存變更。



應用程式控制

如何在命令列中設定應用程式控制操作模式

執行命令：

```
kesl-control --set-settings 21 AppControlMode=<AllowList|DenyList>
```

符號

命令選項

設定	描述
AppControlMode	AllowList — Kaspersky Endpoint Security 阻止使用者啟動任何未在應用程式控制規則中指定的應用程式。 DenyList（預設值）— Kaspersky Endpoint Security 允許使用者啟動任何未在應用程式控制規則中指定的應用程式。

建立應用程式類別

為了在建立應用程式控制規則時更加方便，您可以建立*應用程式類別*。

Kaspersky Endpoint Security 使用下列技術判斷應用程式的類別：

- 病毒資料庫。
- 卡巴斯基安全網路的雲端服務。
- 啟發式分析技術可偵測卡巴斯基資料庫尚未涵蓋的威脅。

在 Kaspersky Endpoint Security for Linux 中，可以根據下列參數建立類別：

- 應用程式的可執行檔的名稱。
- 包含應用程式可執行檔的目錄的名稱。
- 應用程式可執行檔的雜湊。僅可使用 SHA256。

  您可以使用遮罩來指定檔案和目錄的名稱。

  指定遮罩的規則

  您可以使用 * 字元（任意字元序列）或 ？字元（任意一個字元）作為檔案或目錄名稱遮罩。

  您可以使用 * 字元來表示檔案或目錄名稱中包含 / 字元的任意字元集（包括空集）。例如，`/dir/*/file*/` 或 `/dir/file*/`。

  您可以用單個 ? 字元來表示檔案或目錄名稱中的任意一個字元（包括 / ）。

建議您建立涵蓋公司內所使用的標準應用程式集的"工作應用程式"類別。如果工作中不同的使用者群組使用不同的應用程式集，則可以為每個使用者群組建立單獨的應用程式類別。

Kaspersky Endpoint Security for Linux 不支援 KL 類別。

若要在卡巴斯基安全管理中心中建立應用程式類別：

1. 在網頁主控台的主視窗中，選擇**資產管理 → 第三方應用程式 → 應用程式類別**。
2. 點擊"**新增**"。

   使用者類別建立精靈將啟動。
3. 請按照使用者類別建立精靈的指示操作。

步驟 1.

在此步驟中，指定應用程式類別的名稱，並選擇下列應用程式類別類型之一：

- *含有手動新增內容的類別。可執行檔的資料被手動新增到該類別中*如果選擇此類型的類別，在 *條件*步驟和 *排除項目*步驟中，您將可以定義可執行檔據此被包括在類別中的標準。
- *包含指定資料夾內可執行檔的類別。複製至指定資料夾的應用程式可執行檔被自動處理，它們的計量被新增到類別中*如果選擇此類型的類別，在下一步中，您將能夠指定一個資料夾，系統會自動將該資料夾中的可執行檔納入類別。
- *包含所選裝置上可執行檔的類別。這些可執行檔被自動處理，它們的計量被新增到類別中*如果選擇此類型的類別，下一步您可以指定將自動包括在此類別中的可執行檔所屬的電腦。

步驟 2.

如果您選擇了以下類別類型：**含有手動新增內容的類別。可執行檔的資料被手動新增到該類別中**，則可以執行此步驟。

在此步驟中，請選擇將應用程式納入該類別的標準：

- **從 KL 類別**

  如果選擇此選項，您可以將卡巴斯基應用程式類別指定為將應用程式新增至自訂類別的條件。*KL 類別*是具有相同主旨內容的應用程式清單。該清單由 Kaspersky 專家維護。例如，"Office 應用程式"KL 類別就包含了 Microsoft Office 套裝的所有應用程式、Adobe Acrobat 和其他應用程式。

  您可以選擇所有 KL 類別來生成受信任應用程式的延伸清單。

- **從儲存區選取憑證**

  如果選擇此選項，您可以指定來自商店的憑證。此類別條件僅符合使用指定憑證簽署的可執行檔。

  如果您已選擇憑證作為規則觸發條件，請確保此憑證已新增至電腦上的受信任系統儲存，並檢查應用程式中的受信任系統儲存使用設定。

- **指定應用程式路徑（支援遮罩）**

  如果選擇此選項，您可以指定用戶端裝置上的檔案或資料夾，可執行檔將從中新增至自訂應用程式類別。您可以使用正規表示式，例如`C:\path_to_exe\*`。示例：`C:\Program Files\Internet Explorer\*`。

- **卸除式磁碟機**

  如果選擇此選項，您可以指定從其啟動應用程式的媒介的類型（任何媒介或卸除式磁碟機）。從選定類型的媒介啟動的應用程式將被新增到自訂應用程式類別中。

- **雜湊、檔案內容或憑證**：

  - **從可執行檔清單中選擇**

    如果選擇此選項，您可以從用戶端裝置上的可執行檔清單中選擇要新增至該類別的應用程式。

  - **從應用程式登錄檔中選擇**

    如果選擇此選項，則會顯示應用程式的登錄檔。從登錄檔中選擇應用程式後，一個視窗將開啟，其中的設定預先填入了所選應用程式的中繼資料：

    - 檔案名稱
    - 檔案版本 您可以指定確切的版本，或輸入條件，例如「大於 5.0」。
    - 應用程式名稱。
    - 應用程式版本。您可以指定確切的版本，或輸入條件，例如"大於 5.0"。
    - 供應商。

請注意，只會封鎖符合指定參數的可執行檔，但不會阻止所選應用程式本身的啟動。如果所選中繼資料與啟動應用程式時啟動的可執行檔的中繼資料匹配，則可以繼續執行下一步。否則，您需要手動編輯這些值，使它們與可執行檔的中繼資料相符。

- **手動設定**

  如果選擇此選項，則需要指定檔案雜湊值、中繼資料或憑證作為將應用程式新增至自訂類別的條件。

  檔案雜湊值

  根據網路中裝置上安裝的安全應用程式版本，您需要選擇 Kaspersky Endpoint Security 套用於該類別檔案的雜湊演算法。有關由雜湊函數計算出的雜湊值的資訊儲存在管理伺服器的資料庫中。

  SHA256 是一種加密雜湊函數，其演算法沒有已知弱點；它目前被認為是安全性最高的雜湊函數。Kaspersky Endpoint Security 10 及更高版本支援 SHA256。Kaspersky Endpoint Security 10 之前的版本支援 MD5 雜湊函數。

  選擇您希望 Kaspersky Endpoint Security 套用於類別中檔案的雜湊函數之一：

  - 如果您的網路中安裝的所有安全應用程式實例都是 Kaspersky Endpoint Security 10 或更高版本，請選擇 **SHA256** 核取方塊。我們不建議基於 Kaspersky Endpoint Security 10 或更早版本的可執行檔的 SHA256 雜湊值建立類別。這可能會導致安全應用程式發生故障。在這種情況下，您可以為該類別的檔案使用 MD5 加密雜湊函數。

  - 如果您的網路中安裝了早於 Kaspersky Endpoint Security 10 的版本，請選擇 **MD5 雜湊值** 核取方塊。對於 Kaspersky Endpoint Security 10 或更高版本，無法根據執行檔的 MD5 雜湊值新增類別。在這種情況下，您可以為該類別的檔案使用 SHA256 加密雜湊函數。

  - 如果您的網路中包含使用 Kaspersky Endpoint Security 10 及更高版本的裝置，請同時選擇 **SHA256** 核取方塊和 **MD5 雜湊值** 核取方塊。

  檔案內容

  如果選擇此選項，您可以指定檔案名稱、檔案版本和供應商等檔案中繼資料。類別條件僅符合中繼資料相同的可執行檔。

  憑證

  如果選擇此選項，您可以指定來自商店的憑證。此類別條件僅符合使用指定憑證簽署的可執行檔。

- **從 MSI 套件/壓縮檔案資料夾**

  如果選擇此選項，您可以將 MSI 安裝程式檔案指定為將應用程式新增至自訂類別的條件。應用程式安裝程式的中繼資料會被傳送到管理伺服器。安裝程式中繼資料與指定的 MSI 安裝程式相符的應用程式將被新增至自訂應用程式類別。

步驟 3.

如果您選擇了以下類別類型：**含有手動新增內容的類別。可執行檔的資料被手動新增到該類別中**，則可以執行此步驟。

在此步驟指定的應用程式將從類別中排除，即使在“配置將應用程式包括在類別中的條件”步驟指定了這些應用程式。

在此步驟中，請選擇將應用程式從類別中排除的標準：

- **從 KL 類別**

  如果選擇此選項，您可以將卡巴斯基應用程式類別指定為將應用程式新增至自訂類別的條件。*KL 類別*是具有相同主旨內容的應用程式清單。該清單由 Kaspersky 專家維護。例如，”Office 應用程式”KL 類別就包含了 Microsoft Office 套裝的所有應用程式、Adobe Acrobat 和其他應用程式。

  您可以選擇所有 KL 類別來生成受信任應用程式的延伸清單。

- **從儲存區選取憑證**

  如果選擇此選項，您可以指定來自商店的憑證。此類別條件僅符合使用指定憑證簽署的可執行檔。

  如果您已選擇憑證作為規則觸發條件，請確保此憑證已新增至電腦上的受信任系統儲存，並檢查應用程式中的受信任系統儲存使用設定。

- **指定應用程式路徑（支援遮罩）**

  如果選擇此選項，您可以指定用戶端裝置上的檔案或資料夾，可執行檔將從中新增至自訂應用程式類別。您可以使用正規表示式，例如`C:\path_to_exe\*`。示例：`C:\Program Files\Internet Explorer\*`。

- **卸除式磁碟機**

  如果選擇此選項，您可以指定從其啟動應用程式的媒介的類型（任何媒介或卸除式磁碟機）。從選定類型的媒介啟動的應用程式將被新增到自訂應用程式類別中。

- **雜湊、檔案內容或憑證**：

  - **從可執行檔清單中選擇**

    如果選擇此選項，您可以從用戶端裝置上的可執行檔清單中選擇要新增至該類別的應用程式。

  - **從應用程式登錄檔中選擇**

    如果選擇此選項，則會顯示應用程式的登錄檔。從登錄檔中選擇應用程式後，一個視窗將開啟，其中的設定預先填入了所選應用程式的中繼資料：

    - 檔案名稱

    - 檔案版本 您可以指定確切的版本，或輸入條件，例如「大於 5.0」。

    - 應用程式名稱。

- 應用程式版本。您可以指定確切的版本，或輸入條件，例如“大於 5.0”。

- 供應商。

請注意，只會封鎖符合指定參數的可執行檔，但不會阻止所選應用程式本身的啟動。如果所選中繼資料與啟動應用程式時啟動的可執行檔的中繼資料匹配，則可以繼續執行下一步。否則，您需要手動編輯這些值，使它們與可執行檔的中繼資料相符。

- **手動設定**

  如果選擇此選項，則需要指定檔案雜湊值、中繼資料或憑證作為將應用程式新增至自訂類別的條件。

  檔案雜湊值

  根據網路中裝置上安裝的安全應用程式版本，您需要選擇 Kaspersky Endpoint Security 套用於該類別檔案的雜湊演算法。有關由雜湊函數計算出的雜湊值的資訊儲存在管理伺服器的資料庫中。

  SHA256 是一種加密雜湊函數，其演算法沒有已知弱點；它目前被認為是安全性最高的雜湊函數。Kaspersky Endpoint Security 10 及更高版本支援 SHA256。Kaspersky Endpoint Security 10 之前的版本支援 MD5 雜湊函數。

  選擇您希望 Kaspersky Endpoint Security 套用於類別中檔案的雜湊函數之一：

  - 如果您的網路中安裝的所有安全應用程式實例都是 Kaspersky Endpoint Security 10 或更高版本，請選擇 **SHA256** 核取方塊。我們不建議基於 Kaspersky Endpoint Security 10 或更早版本的可執行檔的 SHA256 雜湊值建立類別。這可能會導致安全應用程式發生故障。在這種情況下，您可以為該類別的檔案使用 MD5 加密雜湊函數。

  - 如果您的網路中安裝了早於 Kaspersky Endpoint Security 10 的版本，請選擇 **MD5 雜湊值** 核取方塊。對於 Kaspersky Endpoint Security 10 或更高版本，無法根據執行檔的 MD5 雜湊值新增類別。在這種情況下，您可以為該類別的檔案使用 SHA256 加密雜湊函數。

  - 如果您的網路中包含使用 Kaspersky Endpoint Security 10 及更高版本的裝置，請同時選擇 **SHA256** 核取方塊和 **MD5 雜湊值** 核取方塊。

  檔案內容

  如果選擇此選項，您可以指定檔案名稱、檔案版本和供應商等檔案中繼資料。類別條件僅符合中繼資料相同的可執行檔。

  憑證

  如果選擇此選項，您可以指定來自商店的憑證。此類別條件僅符合使用指定憑證簽署的可執行檔。

- **從 MSI 套件/壓縮檔案資料夾**

  如果選擇此選項，您可以將 MSI 安裝程式檔案指定為將應用程式新增至自訂類別的條件。應用程式安裝程式的中繼資料會被傳送到管理伺服器。安裝程式中繼資料與指定的 MSI 安裝程式相符的應用程式將被新增至自訂應用程式類別。

步驟 4. 設定

> 如果您選擇了以下類別類型：**包含所選裝置上可執行檔的類別。這些可執行檔被自動處理，它們的計量被新增到類別中**，則可以執行此步驟。

在此步驟中，點擊“**新增**”按鈕，指定將由卡巴斯基安全管理中心新增到該應用程式類別的可執行檔所屬的電腦。

在此步驟中，配置以下設定：

- **雜湊函數計算的演算法**

  根據您網路中裝置上安裝的安全應用程式版本，您需要選擇卡巴斯基安全管理中心對該類別中的檔案套用的雜湊演算法。有關由雜湊函數計算出的雜湊值的資訊儲存在管理伺服器的資料庫中。

  *SHA256 是一種加密雜湊函數，其演算法沒有已知弱點；它目前被認為是安全性最高的雜湊函數。*Kaspersky Endpoint Security for Linux 支援 SHA256。

  選擇要套用於類別中檔案的一種雜湊演算法：

  - 如果您在受保護裝置上使用 Kaspersky Endpoint Security for Linux，請選取 **為該類別中的檔案計算 SHA256（在 Kaspersky Endpoint Security 10 Service Pack 2 for Windows 或更新版本中支援）** 核取方塊。

  - 如果您在受保護裝置上使用 Kaspersky Endpoint Security for Windows，請選取 **為該類別中的檔案計算 MD5（在早於 Kaspersky Endpoint Security 10 Service Pack 2 for Windows 的版本中支援）** 核取方塊。

  如果您在網路中同時使用適用於 Windows 和 Linux 的應用程式，請選取兩個核取方塊。

- **將資料與管理伺服器儲存同步**

  如果您希望管理伺服器定期檢查指定的資料夾（或多個資料夾）中的變更，請選擇此選項。

  預設情況下停用此設定。

  如果啟用此參數，請指定檢查指定資料夾（或多個資料夾）變更的時間段（以小時為單位）。預設情況下，期間設定為 24 個小時。

- **檔案類型**

  在此部分，您可以指定要用於建立應用程式類別的檔案類型。

  所有檔案該類別將匹配所有檔案。預設啟用此選項。

  僅應用程式類別之外的檔案該類別將僅匹配應用程式類別之外的檔案。

- **資料夾**

  在此部分，您可以指定選定電腦的資料夾，其中包含要用於建立應用程式類別的檔案。

  所有資料夾該類別將匹配所有資料夾。預設啟用此選項。

  指定資料夾此類別將僅與指定的資料夾相符。如果選擇此選項，則需要指定資料夾路徑。

步驟 5.

如果您選擇了以下類別類型：**包含指定資料夾內可執行檔的類別。複製至指定資料夾的應用程式可執行檔被自動處理，它們的計量被新增到類別中**，則可以執行此步驟。

在此步驟中，指定包含將用於建立類別之可執行檔的資料夾。

管理下列設定：

- **包含動態連結程式庫 (DLL) 到該類別**

  應用程式類別包含動態連結程式庫（DLL 格式的檔案），且應用程式控制元件會記錄此類程式庫在系統中執行的動作。在應用程式類別中包含 DLL 檔案可能降低卡巴斯基安全管理中心的效能。

  預設情況下已清空此核取方塊。

- **包含指令碼到該類別**

  應用程式類別包含指令碼資料，且指令碼不會遭到 Web 威脅防護封鎖。將指令碼資料包含在類別中可能會降低卡巴斯基安全管理中心的效能。

  預設情況下已清空此核取方塊。

- **雜湊函數計算的演算法**

  根據您網路中裝置上安裝的安全應用程式版本，您需要選擇卡巴斯基安全管理中心對該類別中的檔案套用的雜湊演算法。有關由雜湊函數計算出的雜湊值的資訊儲存在管理伺服器的資料庫中。

  *SHA256 是一種加密雜湊函數，其演算法沒有已知弱點；它目前被認為是安全性最高的雜湊函數。*Kaspersky Endpoint Security for Linux 支援 SHA256。

  選擇要套用於類別中檔案的一種雜湊演算法：

  - 如果您在受保護裝置上使用 Kaspersky Endpoint Security for Linux，請選取 **為該類別中的檔案計算 SHA256（在 Kaspersky Endpoint Security 10 Service Pack 2 for Windows 或更新版本中支援）** 核取方塊。

  - 如果您在受保護裝置上使用 Kaspersky Endpoint Security for Windows，請選取 **為該類別中的檔案計算 MD5（在早於 Kaspersky Endpoint Security 10 Service Pack 2 for Windows 的版本中支援）** 核取方塊。

  如果您在網路中同時使用適用於 Windows 和 Linux 的應用程式，請選取兩個核取方塊。

- **強制掃描資料夾以尋找變更**

  如果啟用此選項，應用程式會定期檢查類別內容新增資料夾是否有變更。您可以在核取方塊旁的輸入欄位中指定檢查頻率（以小時為單位）。預設情況下，強制檢查之間的時間間隔為 24 小時。

  如果停用此選項，應用程式不會強制對資料夾進行任何檢查。如果檔案已遭修改、新增或刪除，伺服器會嘗試存取這些檔案。

  預設情況下已清空此核取方塊。

步驟 6.

完成精靈。精靈完成後，新的應用程式類別即建立。您可以使用應用程式控制規則控制類別中的應用程式。

黃金映像

您可以使用清查新增 Golden Image 應用程式類別。此類別預設為空白。「黃金映像」類別包含隨作業系統一起交付到裝置的應用程式。此類別中的應用程式會視為受信任。如有必要，您可以將第三方應用程式新增至此類別。

清查工作完成後，應用程式可以透過以下方式修改「黃金映像」類別：

- **無變更** – 完成清查後，不變更「黃金映像」類別。這是預設選項。當您想要取得裝置上使用的第三方應用程式清單，但不將其新增至「黃金映像」類別時，可以使用此選項。
- **更新或建立（如果不存在）** – 將清查工作在裝置上偵測到的應用程式新增至「黃金映像」類別。如果該類別不存在，則建立該類別。如果該類別存在，則更新該類別中的應用程式清單。
- **移除** – 清除「黃金映像」應用程式類別。此類別會在工作啟動後立即清除，不會對裝置上的檔案執行清查。

  這在以下情境中可能很有用：

  - 如果您需要防止裝置上「黃金映像」類別中的應用程式啟動，但無法停用應用程式控制規則。
  - 如果您將包含與目前政策不同之應用程式控制規則的新政策套用至裝置，或將裝置移至子政策。在此情況下，我們建議清除「黃金映像」類別，以避免誤封鎖允許的應用程式。

根據基線電腦設定「黃金映像」類別

您可以使用基線電腦建立包含一組所需應用程式的「黃金映像」類別。然後，您可以使用此類別建立應用程式控制允許規則。

根據基線電腦設定「黃金映像」類別包括以下步驟：

1. **設定參考電腦**

   安裝並設定裝置在企業網路上運作所需的所有軟體，包括 Kaspersky Endpoint Security for Linux 和網路代理。

2. **建立清查工作**

   在網頁主控台或命令列中建立工作，並管理以下設定：

   - 「黃金映像」應用程式類別的操作：**更新或建立（如果不存在）**；

     ```
     GoldenImageAction=Create
     ```

   - 清查範圍為參考電腦。

3. **執行清查工作並等待其完成。**

   此工作會產生「黃金映像」應用程式類別。

4. **將類別清單匯出至檔案。**

> 您無法在網頁主控台中匯出類別清單。

執行命令：

```
kesl-control [-A] --get-categories --file <path to file> --json
```

其中 `<path to file>` 是您要將工作設定輸出至其中的設定檔路徑。

5. **如有必要，請調整「黃金映像」類別**

檢閱包含應用程式類別清單的設定檔。如有必要，請在「黃金映像」類別中調整應用程式清單。

6. **從設定檔匯入設定。**

如果您已修改包含應用程式類別清單的設定檔，請將其匯入應用程式：

```
kesl-control [-A] --set-categories --names GoldenImage [<category name 1> <category name 2> ... <name of category N>] --file <path to file>
```

其中 `<category name 1> <category name 2> ... <category name N>` 是「黃金映像」類別以外之其他類別的名稱，也就是您要變更其資訊的類別。

`<path to file>` 是您要將工作設定輸出至其中的設定檔路徑。

因此，您可以使用「黃金映像」類別建立應用程式控制規則。

關於應用程式控制規則

*應用程式控制規則*是一組條件，用於判斷應用程式控制是否允許或拒絕選取的使用者群組啟動第三方應用程式。

這些規則會根據下列條件限制第三方應用程式的啟動：

- **應用程式類別**。應用程式所屬的 應用程式類別。

> 每個類別只能在一條規則中使用。

- **使用者和使用者群組**。應用程式控制可限制個別使用者或使用者群組對第三方應用程式的存取。例如，您可以限制組織中除 IT 部門以外的所有使用者存取遠端管理應用程式。

應用程式控制規則可以具有以下*運行狀態*之一：

- **已啟用**。應用程式控制會套用該規則。
- **已停用**。應用程式控制不會套用該規則。
- **測試**。應用程式控制不會封鎖第三方應用程式執行，但會將其啟動的通知傳送至管理伺服器。

如何在網頁主控台中新增應用程式控制規則

1. 在網頁主控台的主視窗中，選擇**資產管理 → 政策**。
2. 點擊 Kaspersky Endpoint Security 政策的名稱。
   政策內容視窗將開啟。
3. 選擇“**應用程式設定**”標籤。
4. 轉到”**安全控制**”→”**應用程式控制**”。
5. 確保該元件的切換開關處於 **應用程式控制已啟用** 位置。
6. 在”**啟動應用程式時的動作**”塊中，點擊”**新增**”按鈕。
   這會開啟用於新增應用程式控制規則的表單。
7. 在 **狀態** 欄位中，設定規則的狀態。
8. 如果您要測試規則，請將此切換開關設為 **已啟用**，並選取 **測試模式** 核取方塊。
9. 在 **規則名稱** 欄位中，輸入規則名稱。規則名稱必須唯一。
10. 選取要套用規則的應用程式類別。若未指定類別，則無法儲存規則。
11. 選取使用者或使用者群組及其執行應用程式的權限。
12. 要將此政策套用到電腦，請關閉... 掛鎖圖示並儲存變更。

如何在命令列中新增應用程式控制規則

1. 將應用程式控制規則清單輸出至檔案：

   ```
   kesl-control --get-settings 21 --file <path to file> [--json]
   ```

2. 開啟設定檔，並根據應用程式控制模式，為 ID 為 `#` 的規則新增區段：

   a. 如果選取 `AppControlMode=AllowList`:

   ```
   [AllowListRules.item_#]
   Description=<rule name>
   AppControlRuleStatus=<On|Off|Test>
   Category=<category name>
   [AllowListRules.item_#.ACL.item_#]
   Access=<Allow|Block>
   Principal=<user>
   ```

   模式

b. 如果選取 `AppControlMode=DenyList`:

```
[DenyListRules.item_#]
Description=<rule name>
AppControlRuleStatus=<On|Off|Test>
Category=<category name>
[DenyListRules.item_#.ACL.item_#]
Access=<Allow|Block>
Principal=<user>
```

模式

3. 將設定從設定檔匯入至應用程式中：

```
kesl-control --set-settings 21 --file <path to file> [--json]
```

符號

命令選項

設定	描述
`[AllowListRules.item_#]` `[DenyListRules.item_#]`	ID 為 `#` 的應用程式控制規則。
`[AllowListRules.item_#.ACL.item_#]` `[DenyListRules.item_#.ACL.item_#]`	應用程式控制規則 (ID 為 `#`) 所適用的使用者清單。
`Description`	應用程式控制規則的描述。
`AppControlRuleStatus`	應用程式控制規則的運作狀態： `On`（預設值）：啟用此規則，Kaspersky Endpoint Security 將此規則套用至應用程式控制。 `Off`：該規則不用於應用程式控制。 `Test` — Kaspersky Endpoint Security 允許啟動規則涵蓋的應用程式，但在報告中記錄關於這些應用程式啟動的資訊。
`Category`	規則套用的應用程式類別的名稱。 您可以指定 `Golden Image` 類別。
`Access`	指派給使用者或使用者群組的存取類型： `Allow`（預設值）— 允許執行應用程式。 `Block` — 拒絕執行應用程式。
`Principal`	應用程式控制規則所適用的使用者或使用者群組： `\Everyone`（預設值）：此規則適用於所有使用者。 `<user>` 是規則適用的使用者名稱。 `@<group name>` 是規則適用的使用者群組名稱。

應用程式控制規則測試模式

為確保應用程式控制不會封鎖運作所需的應用程式，建議您測試應用程式控制規則。在測試模式下，Kaspersky Endpoint Security 會封鎖第三方應用程式執行，並將有關其啟動的通知傳送至管理伺服器。

除了規則禁止的應用程式以外，應用程式控制預設允許所有第三方應用程式執行。

測試應用程式控制規則

1. **建立應用程式控制規則**

   設定並啟用應用程式控制規則以進行測試。例如，您可以建立規則，以防止執行任何第三方應用程式，除了「黃金映像」和「工作應用程式」類別中的應用程式以外。

2. **在測試模式下啟用應用程式控制**

   如何在網頁主控台中啟用應用程式控制的測試模式

   1. 在網頁主控台的主視窗中，選擇**資產管理** → **政策**。
   2. 點擊 Kaspersky Endpoint Security 政策的名稱。
      政策內容視窗將開啟。
   3. 選擇"**應用程式設定**"標籤。
   4. 轉到"**安全控制**"→"**應用程式控制**"。
   5. 確保該元件的切換開關處於 **應用程式控制已啟用** 位置。
   6. 在 **啟動應用程式時的動作** 下，為應用程式控制選取 **通知** 操作。
   7. 要將此政策套用到電腦，請關閉... 掛鎖圖示並儲存變更。

   如何在命令列上啟用應用程式控制的測試模式

   若要選取應用程式控制的測試模式，請執行以下命令：

   ```
   kesl-control --set-settings 21 AppControlRulesAction=TestRules
   ```

3. **檢閱測試結果**

   檢閱傳送至卡巴斯基安全管理中心的應用程式控制報告及該元件的事件。

   如何在網頁主控台中檢視應用程式控制報告

   1. 在網頁主控台的主視窗中，選擇**資產管理** → **政策**。
   2. 點擊 Kaspersky Endpoint Security 政策的名稱。
      政策內容視窗將開啟。
   3. 選擇"**應用程式設定**"標籤。
   4. 轉到"**安全控制**"→"**應用程式控制**"。
   5. 確保該元件的切換開關處於 **應用程式控制已啟用** 位置。
   6. 在應用程式控制規則表格中，按一下 **檢視報告** 按鈕。
   7. 開啟"**測試模式中禁止的應用程式報告**"視窗。
   8. 檢閱測試模式下禁止的應用程式啟動相關資訊。

如何檢視應用程式控制測試執行產生的事件

1. 在網頁主控台的主視窗中，選擇**監控** → **事件分類**。
2. 點擊“**新增**”。
3. 在開啟的 **新事件分類** 視窗中，為選取項目指定名稱。例如：「應用程式控制規則測試」。
4. 前往 **事件** 區段，並管理以下設定：
   - **應用程式名稱** – Kaspersky Endpoint Security for Linux。
   - **嚴重等級** – **資訊**。
   - 請選擇**包含選定的一般事件**選項。
   - 選取 **禁止應用程式在測試模式下啟動** 和 **允許應用程式在測試模式下啟動** 事件旁的核取方塊。
5. 如有需要，請設定其餘設定。
6. 儲存變更。
7. 按一下選取項目的名稱，以檢視事件選取結果。

4 **調整規則**

如果對於電腦使用者工作所需的所有應用程式，測試模式都不會產生封鎖啟動事件，則說明建立了正確的規則。

否則，請編輯您已建立規則的設定、建立其他規則，或刪除現有規則。

系統完整性監控

系統完整性監控元件監視作業系統中可能表示電腦安全漏洞的變化。當偵測到此類變更時，Kaspersky Endpoint Security 會產生相應的事件並向管理員發出警報。

系統完整性監控的運作方式

系統完整性監控可以即時運作，也可以按需運作：

- *系統完整性監控*元件可讓您*即時*監控已納入監控範圍之檔案和目錄的變更。
- *系統完整性檢查*功能可讓您將已納入監控範圍之物件的目前狀態與其記錄的狀態進行比較，可*依排程或按需*進行。

系統完整性監控不會分享有關所做變更的具體資料。*系統完整性檢查*工作會傳送有關被修改屬性以及被移動的檔案和目錄的資料。

特殊考量與限制

- Linux 作業系統的技術限制使得應用程式無法識別對檔案進行了變更的使用者或處理程序。
- 當目錄被新增至監控或排除範圍時，應用程式不會檢查該目錄是否存在。

即時系統完整性監控

系統完整性監控允許即時偵測監控範圍中包含的物件變更。

系統完整性監控的運作方式

1. **應用程式會攔截檔案操作事件**

   應用程式會使用特殊的攔截機制，對正在掃描的檔案具有唯讀存取權限。

2. **應用程式會檢查檔案是否已被修改。**

   系統完整性監控會追蹤以下檔案屬性的變更：

   - 內容（`write ()`、`truncate ()` 及其他修改）
   - 中繼資料（使用 `chmod` 或 `chown` 命令變更存取權限）
   - 時間戳記（`utimensat`）
   - 延伸屬性（`setxattr`）及其他屬性

3. **掃描完成**

   如果檔案已被修改，應用程式會產生 *系統完整性檢查失敗* 事件。

設定系統完整性監控

1. **啟用系統完整性監控**

   預設情況下，系統完整性監控停用。選取您要即時監控檔案變更的裝置，並在這些裝置上啟用系統完整性監控元件。

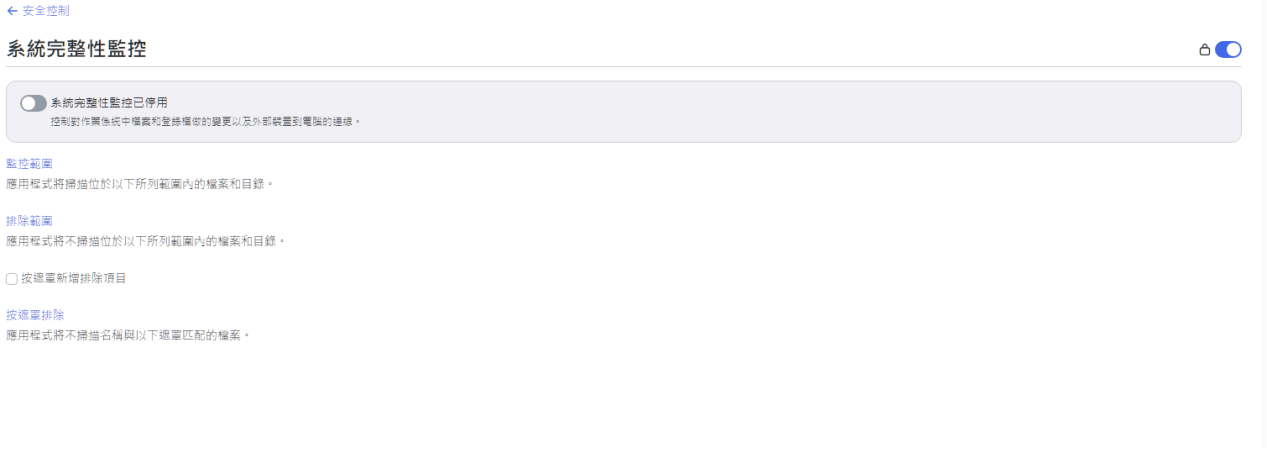
2. **設定監控範圍**

   若要使元件運作，必須至少指定一個監控範圍。預設會設定 *卡巴斯基內部物件*（`/opt/kaspersky/kesl/`）監控範圍。

   Kaspersky Endpoint Security 依照物件在範圍清單中出現的順序掃描指定範圍內的物件。如果有必要，將子目錄放在清單中高於其父目錄的位置，以便為子目錄配置與父目錄的安全性設定不同的安全性設定。

如何在網頁主控台中設定監控範圍

1. 在網頁主控台的主視窗中，選擇**資產管理 → 政策**。
2. 點擊 Kaspersky Endpoint Security 政策的名稱。
   政策內容視窗將開啟。
3. 選擇"**應用程式設定**"標籤。
4. 轉到"**安全控制**"→"**系統完整性監控**"。
5. 點擊"**監控範圍**"連接。
   這會開啟包含掃描範圍表格的視窗。
6. 點擊"**新增**"。
   這會開啟用於新增掃描範圍的視窗
7. 在 **名稱** 欄位中，指定監控範圍的名稱，例如 *關鍵物件*。
8. 在 **路徑** 欄位中，指定個別檔案或目錄的路徑（例如 `/path/to/folder`）。Kaspersky Endpoint Security 輸入遮罩時支援`*`和`?`字元。
9. 如有必要，請以命令 shell 格式指定物件名稱的遮罩（例如 `*.txt` 或 `file?.*`）。一次新增一個遮罩。
10. 要將此政策套用到電腦，請關閉... 掛鎖圖示並儲存變更。



系統完整性監控

如何在命令列中設定監控範圍

1. 執行以下指令：

```
kesl-control --set-settings 11  ScanScope.item_#.UseScanArea=Yes
        [ScanScope.item_#.AreaDesc=<description of the area>\]
        [ScanScope.item_#.AreaMask.item_#=<mask in shell format>\]
        ScanScope.item_#.Path=<path to the directory>
```

2. 若要檢查元件設定的目前值，請執行以下命令：

```
kesl-control --get-settings 11
```

符號

設定	描述
`UseScanArea=Yes`	啟用 ID 為 `#` 的監控範圍。 您可以暫時停用監控範圍的掃描，而不是刪除該範圍。若要這麼做，請設定 `ScanScope.item_#.UseScanArea=No`。
`AreaDesc`	監測範圍描述；包含關於監控範圍的附加資訊。
`AreaMask.item_#`	監控範圍限制。在監控範圍內，應用程式僅掃描使用 shell 格式的遮罩指定的物件。 例如，`ScanScope.item_0001.AreaMask.item_0001=*.exe` `ScanScope.item_0001.AreaMask.item_0002=*.txt`。
`Path`	監控目錄的路徑。Kaspersky Endpoint Security 輸入遮罩時支援`*`和`?`字元。

範例

僅包含 `/etc` 目錄的監控範圍：

```
kesl-control --set-settings 11 ScanScope.item_0000.UseScanArea=Yes ScanScope.item_0000.Path=/etc
```

3 設定排除範圍

排除的優先順序高於監控範圍。排除的物件即使位於監控範圍內，也不會被掃描。如果監控範圍定義的等級低於排除目錄，則應用程式在系統完整性監控期間將跳過該監控範圍。

如何在網頁主控台中設定排除範圍

1. 在網頁主控台的主視窗中，選擇**資產管理** → **政策**。
2. 點擊 Kaspersky Endpoint Security 政策的名稱。
   政策內容視窗將開啟。
3. 選擇"**應用程式設定**"標籤。
4. 轉到"**安全控制**"→"**系統完整性監控**"。

您可以依路徑或檔案名稱遮罩指定排除項目。應用程式可將整個目錄（或個別檔案）從掃描中排除，或在監控範圍中排除符合名稱遮罩的檔案。

若要依路徑新增排除項目：

1. 點擊"**排除範圍**"連接。
   這將開啟包含排除範圍表格的視窗。
2. 點擊"**新增**"。
   這將開啟用於新增排除範圍的視窗。
3. 在 **名稱** 欄位中，指定排除範圍的名稱，例如 *系統檔案*。
4. 在 **路徑** 欄位中，指定個別檔案或目錄的路徑（例如 `/path/to/folder`）。Kaspersky Endpoint Security 輸入遮罩時支援`*`和`?`字元。

5. 請以命令 shell 格式指定物件名稱的遮罩（例如 `*.txt` 或 `file?.*`）。一次新增一個遮罩。

6. 要將此政策套用到電腦，請關閉... 掛鎖圖示並儲存變更。

若要依檔案名稱遮罩新增排除項目：

1. 選擇"**按遮罩新增排除項目**"核取方塊。

2. 點擊"**按遮罩排除**"連接。
   這將開啟包含依遮罩設定之排除範圍的表格。

3. 點擊"**新增**"。
   這將開啟用於依遮罩新增排除範圍的視窗。

4. 請以命令 shell 格式指定檔案名稱遮罩（例如 `*.txt` 或 `file?.*`）。一次新增一個遮罩。

5. 要將此政策套用到電腦，請關閉... 掛鎖圖示並儲存變更。

如何在命令列上設定排除範圍

1. 執行以下指令：

```
kesl-control --set-settings 11  ExcludedFromScanScope.item_#.UseScanArea=Yes
        [ExcludedFromScanScope.item_#.AreaDesc=<description of the area>\]
        [ExcludedFromScanScope.item_#.AreaMask.item_#=<mask in shell format>\]
        ExcludedFromScanScope.item_#.Path=<path to the directory>
```

2. 若要檢查元件設定的目前值，請執行以下命令：

```
kesl-control --get-settings 11
```

符號

命令選項

設定	描述
`UseScanArea=Yes`	將具有 `#` ID 的指定範圍排除在監控之外。 您可以暫時停用排除範圍，而不是刪除該範圍。若要這麼做，請設定 `ExcludedFromScanScope.item_#.UseScanArea=No`。
`AreaDesc`	監控排除範圍描述，包含關於監控排除範圍的附加資訊。
`AreaMask.item_#`	排除範圍的限制。在排除範圍中，應用程式僅會從掃描中排除使用 shell 格式的遮罩指定的物件。 例如，`ExcludedFromScanScope.item_0001.AreaMask.item_0001=*.exe` `ScanScope.item_0001.AreaMask.item_0002=*.txt`。
`Path`	要從掃描中排除之目錄的路徑。Kaspersky Endpoint Security 輸入遮罩時支援 `*` 和 `?` 字元。

範例

僅包含 `/tmp` 目錄的排除範圍：

```
kesl-control --set-settings 11 ExcludedFromScanScope.item_0001.UseScanArea=Yes
```

```
ScanScope.item_0001.Path=/tmp
```

系統完整性檢查

執行 *系統完整性檢查* 工作時，應用程式會將每個物件的目前狀態與其原始狀態（即基準）進行比較。基線包含受監控物件的路徑及其中繼資料。這可讓您追蹤監控範圍內所包含檔案和目錄的變更。

基線可能還包含個人資料。

與 系統完整性監控 元件相比，*系統完整性檢查* 工作有助於限制事件數量，並可讓您產生作業系統變更的摘要報告。

系統完整性檢查的運作方式

1. **應用程式建立系統快照**

   系統基準會在工作首次執行期間建立。如果您建立了多個系統完整性檢查工作，則會為每個工作建立一個單獨的基線。對於 Linux 裝置，當工作設定變更時（例如新增監控範圍），以及在啟用 **每次工作啟動時重新構建基線** 設定的情況下啟動工作時，會重建基準。

   基準儲存區位於 `/var/opt/kaspersky/kesl/private/fim.db`。存取包含基線的資料庫需要 root 權限。基準會與相關聯的系統完整性檢查工作一併刪除。

2. **應用程式尋找系統狀態變更**

   應用程式會套用下列準則，比較監控範圍內所包含物件的相關資訊：

   - 檔案的 SHA256 雜湊值（用於完整檢查）
   - 檔案變更時間
   - 檔案大小

3. **掃描完成**

   如果系統目前狀態與基準不同，Kaspersky Endpoint Security 會產生系統完整性違規事件：*系統完整性檢查失敗*。

設定和執行系統完整性檢查工作

1. **建立系統完整性檢查工作**

   如何在網頁主控台中建立系統完整性檢查工作

   1. 在網頁主控台的主視窗中，選擇**工作**。

      工作清單開啟。

   2. 點擊“**新增**”。

      啟動“工作精靈”。

3. 配置工作設定：

   a. 在“**應用程式**”下拉式清單中，選取“**Kaspersky Endpoint Security for Linux 12.5**”。

   b. 在“**工作類型**”下拉式清單中，選取“**系統完整性檢查**”。

   c. 在“**工作名稱**”欄位中，輸入簡要說明，例如“*每週系統完整性檢查*”。

   d. 在“**要將工作指派給的裝置**”塊中，選取工作範圍。

4. 按照所選工作範圍選項選取裝置。

5. 完成精靈。

如何在命令列中建立系統完整性檢查工作

若要建立工作，請執行以下指令：

```
kesl-control --create-task <task name> --type ODFIM
```

其中 `<task name>` 是新工作名稱。

此指令會傳回已建立工作的 ID。

指令執行結果範例：

工作已建立（工作 ID：115）

2. **如有必要，請編輯工作設定**

如何在網頁主控台中設定系統完整性檢查工作

1. 在網頁主控台的主視窗中，選擇**工作**。
   工作清單開啟。

2. 點擊新建立的系統完整性檢查工作。
   工作內容視窗將開啟。

3. 選擇“**應用程式設定**”標籤。

4. 選擇掃描類型：

   - **完整掃描**應用程式會將檔案目前狀態的 SHA256 雜湊值與系統快照中的雜湊值進行比較。

   - **快速掃描**應用程式只會比較檔案大小。如果檔案大小未變更，修改時間不會被視為關鍵參數。

5. 在 **系統完整性檢查設定** 區段中，選取以下核取方塊：

- **每次工作啟動時重新構建基線**如果選取此核取方塊，應用程式會在每次工作啟動時重建基準。
- **追蹤監控範圍中的目錄**如果選取此核取方塊，應用程式會檢查使用者指定的目錄。如果清除此核取方塊，應用程式只會掃描預設掃描範圍 – *卡巴斯基內部物件*(/opt/kaspersky/kesl/)。
- **追蹤每次工作啟動時檔案上次被存取的情況**如果選取此核取方塊，應用程式會在每次工作執行時檢查檔案的上次存取時間（ noatime 參數）。

6. 儲存變更。

如何在命令列中設定系統完整性檢查工作

執行命令：

```
kesl-control --set-settings <task ID|name> RebuildBaseline=<Yes|No> [CheckFileHash=<Yes|No>]
[TrackDirectoryChanges=<Yes|No>] [TrackLastAccessTime=<Yes|No>] [UseExcludeMasks=<Yes|No>]
[ExcludeMasks.item_#=<object mask>]
```

符號

系統完整性檢查 工作設定

設定	描述
RebuildBaseline	在每次工作啟動時重建基準。
CheckFileHash	掃描檔案的 SHA256 雜湊值。如果停用此檢查，應用程式將僅比較檔案大小（如果檔案大小沒有改變，則修改時間不被視為關鍵參數）。
TrackDirectoryChanges	掃描使用者指定的目錄。如果停用此設定，應用程式只會掃描預設範圍 (/opt/kaspersky/kesl/)。
TrackLastAccessTime	檢查檔案的上次存取時間（ noatime 選項）。
UseExcludeMasks	監控排除項目。新的 [ExcludeMasks.item_#] 部分將被新增至工作設定中。應用程式將不會掃描此區段中指定的物件。 僅當指定了 ExcludeMasks.item_# 設定時，此設定才適用。
ExcludeMasks.item_#= <object mask>	從監控範圍排除物件。您可以使用此設定，依名稱從指定的掃描範圍中排除個別檔案，或使用命令 shell 格式的遮罩一次排除多個檔案。Kaspersky Endpoint Security 輸入遮罩時支援 * 和 ? 字元。 只有啟用 UseExcludeMasks 參數時，才能管理此設定。 您可以指定多個遮罩。每個遮罩必須在新行上用新索引指定。 範例：ExcludeMasks.item_0000=<eicar1.*>

3 設定監控範圍

若要啟動工作，必須指定至少一個監控範圍。預設會設定 *卡巴斯基內部物件*(/opt/kaspersky/kesl/) 監控範圍。

只有當基準包含屬於該工作監控範圍之物件的資訊時，才會執行工作。

Kaspersky Endpoint Security 依照物件在範圍清單中出現的順序掃描指定範圍內的物件。如果有必要，將子目錄放在清單中高於其父目錄的位置，以便為子目錄配置與父目錄的安全性設定不同的安全性設定。

如何在網頁主控台中設定監控範圍

1. 在網頁主控台的主視窗中，選擇**工作**。

   工作清單開啟。

2. 點擊新建立的系統完整性檢查工作。

   工作內容視窗將開啟。

3. 選擇“**應用程式設定**”標籤。

4. 請確保選中**追蹤監控範圍中的目錄**核取方塊。

5. 在”**監控和排除範圍**”塊中，點擊”**監控範圍**”連接。
   這會開啟包含掃描範圍表格的視窗。

6. 點擊“**新增**”。
   這會開啟用於新增掃描範圍的視窗

7. 在 **名稱** 欄位中，輸入監控範圍的名稱，例如 *桌面上的檔案*。

8. 在 **路徑** 欄位中，指定個別檔案或目錄的路徑（例如 `/path/to/folder`）。Kaspersky Endpoint Security 輸入遮罩時支援`*`和`?`字元。

9. 如有必要，請以命令 shell 格式指定物件名稱的遮罩（例如 `*.txt`、`file?.*`）。一次新增一個遮罩。

10. 儲存變更。

如何在命令列中設定監控範圍

1. 執行以下指令：

```
kesl-control --set-settings <task ID|name> TrackDirectoryChanges=Yes ScanScope.item_#.UseScanArea=Yes
        [ScanScope.item_#.AreaDesc=<description of the area>\]
        [ScanScope.item_#.AreaMask.item_#=<mask in shell format>\]
        ScanScope.item_#.Path=<path to the directory>
```

2. 若要檢查目前設定，請執行以下指令：

```
kesl-control --get-settings <task ID|name>
```

符號

系統完整性檢查 工作設定

設定	描述
`UseScanArea=Yes`	啟用 ID 為`#`的監控範圍。 您可以暫時停用監控範圍的掃描，而不是刪除該範圍。若要這麼做，請設定 `ScanScope.item_#.UseScanArea=No`。
`AreaDesc`	監測範圍描述；包含關於監控範圍的附加資訊。
`AreaMask.item_#`	監控範圍限制。在監控範圍內，應用程式僅掃描使用 shell 格式的遮罩指定的物件。 您可以以任意順序指定多個`ScanScope.item_#.AreaMask.item_#`項目。應用程式按索引的升序處理範圍。 例如，`ScanScope.item_0001.AreaMask.item_0001=*.exe` `ScanScope.item_0001.AreaMask.item_0002=*.txt`。
`Path`	監控目錄的路徑。Kaspersky Endpoint Security 輸入遮罩時支援`*`和`?`字元。

範例

僅包含 `/etc` 目錄的監控範圍：

```
kesl-control --set-settings 115 ScanScope.item_0000.UseScanArea=Yes ScanScope.item_0000.Path=/etc
```

4 設定排除範圍

排除的優先順序高於監控範圍。排除的物件即使位於監控範圍內，也不會被掃描。如果監控範圍定義的等級低於排除目錄，則應用程式在系統完整性監控期間將跳過該監控範圍。

如何在網頁主控台中設定排除範圍

1. 在網頁主控台的主視窗中，選擇**工作**。
2. 工作清單開啟。
3. 點擊新建立的系統完整性檢查工作。

   工作內容視窗將開啟。
4. 選擇"**應用程式設定**"標籤。

您可以依路徑或檔案名稱遮罩指定排除項目。應用程式可將整個目錄（或個別檔案）從掃描中排除，或在監控範圍中排除符合名稱遮罩的檔案。

若要依路徑新增排除項目：

1. 在"**監控和排除範圍**"塊中，點擊"**排除範圍**"連接。

   這將開啟包含排除範圍表格的視窗。
2. 點擊"**新增**"。

   這將開啟用於新增排除範圍的視窗。
3. 在 **名稱** 欄位中，指定排除範圍的名稱，例如 *系統檔案*。
4. 在 **路徑** 欄位中，指定個別檔案或目錄的路徑（例如 `/path/to/folder`）。Kaspersky Endpoint Security 輸入遮罩時支援`*` 和 `?`字元。
5. 請以命令 shell 格式指定物件名稱的遮罩（例如 `*.txt` 或 `file?.*`）。一次新增一個遮罩。
6. 要將此政策套用到電腦，請關閉... 掛鎖圖示並儲存變更。

若要依檔案名稱遮罩新增排除項目：

1. 在"**監控和排除範圍**"塊中，點擊"**按遮罩排除**"連接。

   這將開啟包含依遮罩設定之排除範圍的表格。
2. 點擊"**新增**"。

   這將開啟用於依遮罩新增排除範圍的視窗。
3. 請以命令 shell 格式指定檔案名稱遮罩（例如 `*.txt` 或 `file?.*`）。一次新增一個遮罩。
4. 要將此政策套用到電腦，請關閉... 掛鎖圖示並儲存變更。

如何在命令列上設定排除範圍

1. 執行以下指令：

```
kesl-control --set-settings <task ID|name>      ExcludedFromScanScope.item_#.UseScanArea=Yes
        [ExcludedFromScanScope.item_#.AreaDesc=<description of the area>\]
        [ExcludedFromScanScope.item_#.AreaMask.item_#=<mask in shell format>\]
        ExcludedFromScanScope.item_#.Path=<path to the directory>
```

2. 若要檢查目前設定，請執行以下指令：

```
kesl-control --get-settings <task ID|name>
```

符號

系統完整性檢查 工作設定

設定	描述
UseScanArea=Yes	將具有 # ID 的指定範圍排除在監控之外。 您可以暫時停用排除範圍，而不是刪除該範圍。若要這麼做，請設定 ExcludedFromScanScope.item_#.UseScanArea=No 。
AreaDesc	監控排除範圍描述，包含關於監控排除範圍的附加資訊。
AreaMask.item_#	排除範圍的限制。在排除範圍中，應用程式僅會從掃描中排除使用 shell 格式的遮罩指定的物件。 您可以以任意順序指定多個 ExcludedFromScanScope.item_#.AreaMask.item_# 項目。應用程式按索引的升序處理範圍。 例如， ExcludedFromScanScope.item_0001.AreaMask.item_0001=*.exe ScanScope.item_0001.AreaMask.item_0002=*.txt 。
Path	要從掃描中排除之目錄的路徑。Kaspersky Endpoint Security 輸入遮罩時支援 * 和 ? 字元。

範例

僅包含 /tmp 目錄的排除範圍：

```
kesl-control --set-settings 115 ExcludedFromScanScope.item_0001.UseScanArea=Yes
ScanScope.item_0001.Path=/tmp
```

5 執行工作

如何在網頁主控台中執行系統完整性檢查工作

1. 在網頁主控台的主視窗中，選擇**工作**。
   工作清單開啟。
2. 選取已建立的工作旁邊的核取方塊。
3. 點擊**“開始”**。

如何在命令列上執行系統完整性檢查工作

若要執行工作，請執行以下指令：

```
kesl-control --start-task <task ID|name> [-W] [--progress]
```

其中：

- `<task ID|name>` 是任務建立時指派的 ID，或是命令列中的任務名稱。
- `[-W]` 啟用與此工作相關的目前事件的輸出。
- `[--progress]` 啟用工作進度顯示。

信任區域

*信任區域*是在其有效時，管理員建立的 Kaspersky Endpoint Security 不進行監控的物件和應用程式的清單。

考慮到所處理物件的特點和安裝在電腦上的應用程式，管理員可以自主建立信任區域。當 Kaspersky Endpoint Security 封鎖存取特定物件或應用程式時，如果您確定此物件或應用程式是無害的，則有必要將其包含在信任區域中。

受信任區域設定

設定	描述
網址	Web 威脅防護元件認為受信任的網址。此元件不會掃描來自這些位址的傳入和傳出流量以查找威脅。例如，如果該元件干擾從已知網站下載檔案，則可以使用受信任位址清單。 如需更多資訊，請參閱 如何新增受信任的網址 一文
IP 位址	受信任裝置的 IP 位址。網路威脅防護元件不會封鎖來自這些位址的網路活動。 應用程式也不會記錄有關來自排除清單中的 IP 位址的網路攻擊的資訊。 如需更多資訊，請參閱 如何新增電腦的受信任 IP 位址 一文
網路連接埠	網路威脅防護元件從掃描中排除的網路連接埠清單。 如需更多資訊，請參閱 如何選擇受監控的網路連接埠 一文
根憑證	Kaspersky Endpoint Security 認為受信任的根憑證。當 Web 威脅防護、郵件威脅防護 和 Web 控制 元件掃描加密連線（HTTPS 連線）時，會使用受信任的根憑證清單。 如需更多資訊，請參閱 如何將憑證新增至受信任的根憑證清單 一文
網域	受信任網域清單。Web 威脅防護和 Web 控制 元件不會控制與這些網域的加密連線。 如需更多資訊，請參閱 如何新增受信任網域 一文
掛接點	受信任掛載點清單。檔案威脅防護、加密軟體防護和 容器掃描 元件會從掃描中排除指定的掛載點。 掛載點的指定方式必須與 `mount` 指令輸出中顯示的方式相同。 如需更多資訊，請參閱「如何排除掛載點」一文
應用程式	Kaspersky Endpoint Security 不會控制其檔案與網路活動或系統登錄存取的應用程式。例如 檔案威脅防護 或 行為偵測 等防護元件不會控制指定應用程式的活動。 如需更多資訊，請參閱 如何新增受信任的應用程式 一文
惡意軟體掃描排除項目	由所有或部分應用程式元件從掃描中排除的檔案或資料夾，以及物件類型（根據 病毒百科全書 ）。 如需更多資訊，請參閱 如何新增防護排除項目 一文
裝置	裝置控制 元件一律允許所選使用者或群組完整存取的裝置。 如需更多資訊，請參閱 如何新增受信任裝置 一文

如何新增防護排除項目

*防護排除*是一組條件，在這些條件下，Kaspersky Endpoint Security 不會掃描物件以查找病毒和其他惡意軟體。

可以使用以下方法從掃描中排除物件：

- **排除項目**。目錄路徑。Kaspersky Endpoint Security 輸入遮罩時支援`*`和`?`字元。範例：`/.snapshots/*/snapshot/`。

  若要指定容器或映像檔中的路徑，請使用標籤。

  如何使用標籤

  您可以使用特殊標籤來指定容器或映像：

  - `[container-id:<id>]/<path to local directory>`
  - `[container-name:<name>]/<path to local directory>`
  - `[image-id:<id>]/<path to local directory>`
  - `[image-name:<name>]/<path to local directory>`

  其中：

  `<id>` 是容器 ID。

  `<name>` 是容器名稱

  `<path to local directory>` 是本機目錄路徑。

  您也可以使用標籤的唯一組合：`[container-id:<id>]`、`[container-name:<name>]`、`[image-id:<id>]` 和 `[image-name:<name>]/path to local directory>`。

  允許在一個區域內任意組合 1 到 4 個唯一標籤。列出的順序不重要。

  範例：

  - `[container-name:<name>][image-name:<name>]/path to local directory>`
  - `[container-id:<id>][image-name:<name>]/<path to local directory>`
  - `[image-name:<name>][image-id:<id>]/<path to local directory>`
  - `[container-name:<name>][container-id:<id>][image-name:<name>]/<path to local directory>`
  - `[container-name:<name>][image-id:<id>][container-id:<id>][image-name:<name>]/path to local directory>`

  您可以在名稱和識別碼中使用遮罩（`?`和`*`字元）。

- **依遮罩排除**。使用遮罩指定的檔案名稱。Kaspersky Endpoint Security 輸入遮罩時支援`*`和`?`字元。例如：`*.txt` 遮罩會比對所有文字檔案。

使用遮罩：

- `*`（星號）字元，可取代任意字元組合，但 `\` 和 `/` 字元除外（檔案和目錄路徑中檔案與目錄名稱的分隔符號）。例如，遮罩 `/dir/*/*.txt` 將包含位於 dir 目錄內的目錄中、具有 TXT 副檔名之檔案的所有路徑，但不包含子目錄中的檔案。

- 兩個連續的 `*` 字元可取代檔案或目錄名稱中的任意字元組合（包括空集合），包括 `\` 和 `/` 字元（檔案和目錄路徑中檔案與目錄名稱的分隔符號）。例如，遮罩 `/dir/**/*.txt` 將包含位於巢狀於 dir 目錄內的目錄中、具有 TXT 副檔名之檔案的所有路徑，但不包含 dir 目錄本身。

- `?`（問號）字元，可取代任何單一字元，但 `\` 和 `/` 字元除外（檔案和目錄路徑中檔案與目錄名稱的分隔符號）。例如，`/dir/???.txt` 遮罩將包含位於 dir 目錄中，具有 TXT 副檔名且名稱由三個字元組成的所有檔案路徑。

- **依威脅名稱的排除項目** 根據 卡巴斯基百科全書 分類的物件類型名稱（例如，`Email-Worm`、`Rootkit` 或 `RemoteAdmin`）。您可以用`?`字元（替換任何單個字元）和`*`字元（替換任意數量的字元）來使用遮罩。例如，如果指定了`Client*`遮罩，則應用程式將從掃描中排除`Client-IRC`、`Client-P2P`和`Client-SMTP`物件。

- **依處理程序的排除項目** 處理程序路徑。

Kaspersky Endpoint Security 也允許 排除特定格式的檔案：封存檔、電子郵件資料庫、文字檔案、資料庫記錄檔。

如何在網頁主控台中新增防護排除項目

1. 在網頁主控台的主視窗中，選擇**資產管理 → 政策**。

2. 點擊 Kaspersky Endpoint Security 政策的名稱。

   政策內容視窗將開啟。

3. 選擇“**應用程式設定**”標籤。

4. 轉到 **主機威脅防護 → 檔案威脅防護**。

5. 點擊”**掃描排除項目**”連接。

6. 在開啟的視窗中，點擊“**新增**”按鈕。

7. 選取要用於防護排除項目的條件核取方塊：

   - **檔案或資料夾路徑**指定檔案或目錄路徑，或檔案名稱遮罩。若要指定容器或映像檔中的路徑，請使用標籤。

     對於本機檔案系統，請指定目錄路徑（例如，`/path/to/folder/`）。對於已掛載的檔案系統或所有遠端掛載的檔案系統，請輸入檔案名稱遮罩。對於已掛載的檔案系統，也請指定存取協定（NFS、Samba 或自訂）。

   - **物件類型**指定威脅名稱。

   - **物件雜湊**輸入物件的 SHA256 雜湊值。您也可以新增檔案，或指定要從中取得用於排除的 SHA256 雜湊值的事件。

8. 選取要套用排除的防護元件：

- **所有防護元件**此排除會套用至受 **惡意軟體掃描排除項目** 影響的所有防護元件。
- **選定防護元件**選取要套用排除的元件：檔案威脅防護、加密軟體防護、弱點利用防禦。

9. 要將此政策套用到電腦，請關閉... 掛鎖圖示並儲存變更。

如何在命令列中新增防護排除項目

1. 若要依路徑新增排除項目，請執行以下命令：

```
kesl-control --set-settings 1 --add-exclusion <path>
```

2. 若要依遮罩新增排除項目，請依照以下步驟操作：

   a. 啟用依遮罩進行檔案排除：

   ```
   kesl-control --set-settings 1 UseExcludeMasks=Yes
   ```

   b. 新增檔案遮罩：

   ```
   kesl-control --set-settings 1 ExcludeMasks.item_#=<file mask>
   ```

3. 若要依威脅名稱新增排除項目，請依照以下步驟操作：

   a. 啟用依威脅名稱進行檔案排除：

   ```
   kesl-control --set-settings 1 UseExcludeThreats=Yes
   ```

   b. 新增威脅名稱：

   ```
   kesl-control --set-settings 1 ExcludeThreats.item_#=<threat name>
   ```

4. 若要檢查元件設定的目前值，請執行以下命令：

```
kesl-control --get-settings 1
```

符號

命令選項

設定	描述
`--add-exclusion`	從掃描中排除目錄。新的 `[ExcludedFromScanScope.item_#]` 部分將被新增至工作設定中。應用程式會將 `path` 設定所指定目錄中的物件排除於掃描之外。
`ExcludeMasks.item_#`	按名稱或遮罩排除掃描物件。使用 shell 格式的遮罩輸入檔案名稱。範例：`ExcludeMasks.item_0000=*_my_file_??.html`。
`ExcludeThreats.item_#`	根據偵測到的威脅名稱從掃描中排除物件。為了從掃描中排除物件，請指定在此物件中偵測到的威脅的全名 — 包含應用程式判定物件被感染的字串。 例如，您可能正在使用公用程式來獲取關於網路的資訊。為了防止應用程式封鎖它，請將其中包含的威脅的全名新增至排除掃描的威脅清單。範例： `ExcludeThreats.item_0000=EICAR-Test-*`。

如何新增受信任的網址

Web 威脅防護除了封鎖惡意網站和釣魚網站外，還可以封鎖其它網站。例如，Web 威脅防護可以封鎖不符合 RFC 標準的 HTTP 流量。您可以為您信任其內容的網址建立一個清單。“Web 威脅防護”元件不會分析來自受信任網址的資訊，不會檢查它們中是否含有病毒或其他威脅。在一些情況下本選項十分有用，例如，當“Web 威脅防護”元件干擾您從一個已知網站上下載檔案時。

如何在網頁主控台中新增受信任的網址

1. 在網頁主控台的主視窗中，選擇**資產管理** → **政策**頁簽。
2. 點擊 Kaspersky Endpoint Security 政策的名稱。
   政策內容視窗將開啟。
3. 選擇“**應用程式設定**”標籤。
4. 轉到“**受信任區域**”區域。
5. 在開啟的視窗中，點擊“**網址**”連接。
   這會開啟包含受信任網址清單的視窗。
6. 為您信任其內容的網頁或網址建立清單。
   Kaspersky Endpoint Security 輸入遮罩時支援`*`和`?`字元。
   您也可以從 JSON 檔案匯入受信任的網址清單。
7. 要將此政策套用到電腦，請關閉... 掛鎖圖示並儲存變更。

如何在命令列上新增受信任的網址

1. 若要啟用受信任的網址清單，請執行以下指令：

```
kesl-control --set-settings 14 UseTrustedAddresses=Yes
```

2. 若要新增受信任的網址，請執行以下指令：

```
kesl-control --set-settings 14 TrustedAddresses.item_#=<trusted web address>
```

3. 若要檢查元件設定的目前值，請執行以下命令：

```
kesl-control --get-settings 14
```

範例

```
kesl-control --set-settings 14 TrustedAddresses.item_001=https://example.com/
```

如何新增電腦的受信任 IP 位址

Kaspersky Endpoint Security 可以識別網路攻擊並封鎖傳輸大量封包（例如，來自監視攝像機）的不安全網路連線。要使用受信任裝置，您可以將這些裝置的 IP 位址新增到排除項目清單中。受信任的網址會影響 網路威脅防護 元件。

如何在網頁主控台中設定排除封鎖的位址

1. 在網頁主控台的主視窗中，選擇**資產管理** → **政策**頁簽。
2. 點擊 Kaspersky Endpoint Security 政策的名稱。
   政策內容視窗將開啟。
3. 選擇“**應用程式設定**”標籤。
4. 轉到“**受信任區域**”區域。
5. 在開啟的視窗中，點擊“**IP 位址**”連接。
   這會開啟包含受信任 IP 位址清單的視窗。
6. 在開啟的視窗中，點擊“**新增**”按鈕。
7. 輸入不封鎖網路攻擊的電腦的 IP 位址。
   如有必要，請指定子網路。
8. 要將此政策套用到電腦，請關閉... 掛鎖圖示並儲存變更。

如何在命令列中設定排除封鎖的位址

1. 若要套用受信任的 IP 位址，請執行下列命令：

```
kesl-control --set-settings 17 UseExcludeIPs=Yes
```

2. 若要新增受信任的 IP 位址，請執行下列命令：

```
kesl-control --set-settings 17 ExcludeIPs.item_#=<IP address>
```

3. 若要掃描受信任 IP 位址清單，請執行下列命令：

```
kesl-control --get-settings 17 TrustedIPAddresses
```

範例

```
kesl-control --set-settings 17 ExcludeIPs.item_0000="192.168.2.0/24"
```

如何選取受監控的網路連接埠

Kaspersky Endpoint Security 會監控透過特定協定傳輸，並經由使用者電腦上特定開放 TCP 連接埠的資料流。預設情況下，應用程式會監控已知和已註冊的連接埠，例如 HTTPS 連線的連接埠 443，以及 IMAP 郵件協定的連接埠 143。

*受信任的網路連接埠*是 網路威脅防護 元件從掃描中排除的網路連接埠。這是為了設定 Kaspersky Endpoint Security，使其與受信任的第三方服務和應用程式相容，並最佳化效能。例如，您可以為內部備份服務指定網路連接埠，讓應用程式不會干擾備份副本的下載或上傳。

請務必記住，從掃描中排除網路連接埠會降低裝置的防護程度。請盡量將排除項目維持在最低限度。

如何在網頁主控台中從掃描中排除網路連接埠

1. 在網頁主控台的主視窗中，選擇**資產管理 → 政策**。
2. 點擊 Kaspersky Endpoint Security 政策的名稱。
   政策內容視窗將開啟。
3. 選擇"**應用程式設定**"標籤。
4. 轉到"**受信任區域**"→"**網路連接埠**"。
   這會開啟包含受監控網路連接埠清單的視窗。
5. 停用您要從掃描中排除之連接埠的切換開關。
   如果未列出您需要的連接埠，表示應用程式不會掃描該連接埠。
6. 要將此政策套用到電腦，請關閉... 🔒掛鎖圖示並儲存變更。

如何在命令列中從掃描中排除網路連接埠

1. 執行以下命令以取得受監控連接埠清單：

```
kesl-control --get-net-setting
```

2. 如果已啟用所有連接埠的監控 (`MonitorNetworkPorts=All`)，請執行以下命令：

```
kesl-control --set-net-settings MonitorNetworkPorts=Selected
```

   這會新增一個 `[NetworkPorts.item_#]` 區段，其中包含受監控的網路連接埠。

3. 如果該區段包含您想要從掃描中排除的連接埠，請執行以下步驟：

   a. 若要將網路流量掃描設定輸出到檔案，請執行以下命令：

```
kesl-control --get-net-setting --file <path to file>
```

   b. 在此檔案中，刪除包含您不想要監控之網路連接埠的 `[NetworkPorts.item_#]` 區段。

c. 若要套用您的設定，請執行以下命令：

```
kesl-control --set-net-settings --file <path to file>
```

修改後的設定會匯入應用程式。

如何將憑證新增至受信任的根憑證清單

如果（例如）您需要部署新認證中心，Kaspersky Endpoint Security 可讓您在使用者電腦上安裝受信任根憑證。該應用程式可讓您將憑證新增至一個特殊的 Kaspersky Endpoint Security 憑證商店。在此情況下，該憑證被認為僅對 Kaspersky Endpoint Security 應用程式受信任。換而言之，使用者可以用瀏覽器中的新憑證存取網站。如果其它應用程式嘗試存取網站，您會因為憑證問題得到一個連線錯誤。

以下元件會使用受信任根憑證：

- Web 威脅防護
- 郵件威脅防護
- Web 控制

支援 CER、CRT、PEM 和 DER 格式的受信任憑證。受信任憑證的最大檔案大小為 2 MB。

如何在網頁主控台中安裝受信任根憑證

1. 在網頁主控台的主視窗中，選擇**資產管理** → **政策**。
2. 點擊 Kaspersky Endpoint Security 政策的名稱。
   政策內容視窗將開啟。
3. 選擇“**應用程式設定**”標籤。
4. 轉到”**受信任區域**”→”**根憑證**”。
   這將開啟包含受信任根憑證清單的視窗。
5. 點擊“**新增**”。
   這將開啟用於新增憑證的表單。
6. 上傳憑證。
7. 如有必要，請在 **註釋** 欄位中輸入憑證的描述。
8. 儲存變更。

在受信任的憑證清單中，序號會用作憑證名稱。

如何在指令列上安裝受信任根憑證

1. 若要新增憑證，請執行以下指令：

```
kesl-control --add-certificate <path to certificate>
```

2. 若要檢視受信任根憑證清單，請執行以下指令：

```
kesl-control --list-certificates
```

每個憑證都會顯示以下資訊：

- 憑證主體
- 序號
- 憑證發佈者
- 憑證開始日期
- 憑證到期日期
- SHA256 憑證指紋

3. 若要從清單中移除憑證，請執行以下指令：

```
kesl-control --remove-certificate <certificate subject>
```

如何新增受信任網域

Kaspersky Endpoint Security 有一份受信任網域清單，對於這些網域不會掃描加密連線。受信任網域會影響 Web 威脅防護 和 Web 控制。將網域排除於掃描範圍外，可避免封鎖來自您所知來源的流量。

指定網域名稱。系統會忽略網址，例如 `example.com/*` 或 `https://example.com`。

如何在網頁主控台中指定受信任網域

1. 在網頁主控台的主視窗中，選擇**資產管理** → **政策**。
2. 點擊 Kaspersky Endpoint Security 政策的名稱。
   政策內容視窗將開啟。
3. 選擇"**應用程式設定**"標籤。
4. 轉到"**受信任區域**"→"**受信任網域**"。
   這將開啟包含受信任網域清單的視窗。
5. 點擊"**新增**"。
   這將開啟新增網域的表單。
6. 指定網域名稱或網域遮罩。例如，`*example.com`。
7. 儲存變更。

如何在命令列中指定受信任網域

1. 若要新增網域，請執行以下指令：

```
kesl-control --set-net-settings ManageExclusions=Yes Exclusions.item_#.DomainName=<domain name>
```

2. 若要測試您的設定，請執行以下指令：

```
kesl-control --get-net-settings
```

   受信任網域應列在 `[Exclusions.item_#]` 區段中。

範例

```
kesl-control --set-net-settings Exclusions.item_0000.DomainName=example.com
```

如何排除掛載點

若要將某個目錄中的檔案排除在掃描範圍以及攔截範圍之外，需要排除整個掛載點。此類排除稱為*全域排除*。應用程式會將掛載在裝置上的受信任本機或遠端目錄從掃描及檔案操作攔截中排除。例如，您可以排除包含暫存檔案的掛載點，以減少系統負載並讓掃描更快完成。

掛載點排除會影響下列元件：

- 檔案威脅防護
- Anti-Cryptor
- 容器掃描

受信任的掛載點也會由下列工作排除在掃描範圍之外：

- 惡意軟體掃描
- 關鍵區域掃描
- 容器掃描
- 卸除式磁碟機掃描

> 掛載點的指定方式必須與`mount`指令輸出中顯示的方式相同。

如何在網頁主控台中指定受信任的掛載點

1. 在網頁主控台的主視窗中，選擇**資產管理** → **政策**。
2. 點擊 Kaspersky Endpoint Security 政策的名稱。
   政策內容視窗將開啟。

3. 選擇“**應用程式設定**”標籤。

4. 轉到”**受信任區域**”→”**掛接點**”。
   這將開啟包含受信任掛載點清單的視窗。

5. 點擊“**新增**”。
   這將開啟新增掛載點的表單。

6. 在檔案系統下拉式清單中，選取要排除的目錄所在的檔案系統類型：**本機**、**已掛接**、**所有遠端掛接**。
   Kaspersky Endpoint Security 支援用於遠端目錄的 Samba 和 NFS 通訊協定。

   > 掛載點的指定方式必須與`mount`指令輸出中顯示的方式相同。

7. 輸入包含要排除目錄的檔案系統名稱。

8. 要將此政策套用到電腦，請關閉... 掛鎖圖示並儲存變更。

如何在命令列中指定受信任的掛載點

1. 如果目錄不是掛載點，請執行以下命令，從該目錄建立掛載點：

```
mount --bind <path to dir> <path to dir>
```

2. 若要在伺服器重新啟動後保留掛載點，請將下列行新增至 `/etc/fstab` 檔案：

```
<path to dir> <path to dir> none defaults,bind 0 0
```

3. 重新啟動 Kaspersky Endpoint Security：

```
systemctl restart kesl
```

4. 若要新增受信任的掛載點，請執行以下命令：

```
kesl-control --set-app-settings ExcludedMountPoint.item_#=<path to mount point>
```

5. 重新啟動應用程式以套用全域排除：

```
systemctl restart kesl
```

範例

```
kesl-control --set-app-settings ExcludedMountPoint.item_0000="/tmp"
```

如何新增受信任應用程式

*受信任應用程式清單*是一份應用程式清單，Kaspersky Endpoint Security 不會監控這些應用程式的檔案和處理程序活動（包括惡意活動）或處理程序記憶體。預設情況下，Kaspersky Endpoint Security 會監控由任何應用程式處理程序開啟、執行或儲存的物件，並控制所有應用程式的活動。

受信任應用程式會影響以下元件：

- 檔案威脅防護
- 行為偵測

以及處理程序記憶體掃描排除。

如何在網頁主控台中指定受信任應用程式

1. 在網頁主控台的主視窗中，選擇**資產管理 → 政策**。
2. 點擊 Kaspersky Endpoint Security 政策的名稱。

   政策內容視窗將開啟。
3. 選擇"**應用程式設定**"標籤。
4. 轉到"**受信任區域**"→"**受信任應用程式**"。

   這將開啟包含受信任應用程式清單的視窗。
5. 如果要為公司內的所有電腦建立受信任应用程式的綜合清單，請選取"**繼承時合併值**"核取方塊。將合併父政策和子政策中的受信任應用程式清單。父政策中的應用程式僅顯示在子政策中供檢視，無法修改或刪除。

   若要合併清單，必須啟用父政策設定的繼承。
6. 點擊"**新增**"。

   這會開啟新增應用程式的表單。
7. 指定應用程式路徑或路徑遮罩。
8. 配置受信任應用程式設定：

   - **不掃描該應用程式開啟的檔案**Kaspersky Endpoint Security 的掃描將排除應用程式開啟的所有檔案。
   - **不監控應用程式活動**Kaspersky Endpoint Security 不會監控作業系統內受信任應用程式的檔案和網路活動。

     您也可以選取 **不要為 Managed Detection and Response 和 Endpoint Detection and Response 監控** 核取方塊，分別為 MDR 和 EDR (KATA) 元件配置應用程式活動監控。
   - **不監控子應用程式活動**Kaspersky Endpoint Security 不會監控由受信任應用程式啟動之應用程式的檔案和網路活動。
   - **不掃描指定應用程式的記憶體**Kaspersky Endpoint Security 不會掃描由受信任應用程式產生之處理程序的記憶體。

在網頁主控台中，Kaspersky Endpoint Security for Linux 不提供 **註釋** 設定。

9. 儲存變更。

如何在命令列中指定受信任應用程式

1. 若要將受信任應用程式的檔案活動排除在掃描範圍之外，請執行以下命令：

```
kesl-control --set-settings 1 ExcludedForProgram.item_#.UseExcludedForProgram=Yes
ExcludedForProgram.item_#.ProgramPath=<path to app> ExcludedForProgram.item_#.AreaDesc=<trusted app name>
[ExcludedForProgram.item_#.ApplyToDescendants=Yes]
```

2. 若要將受信任應用程式的處理程序活動排除在掃描範圍之外，請執行以下命令：

```
kesl-control --set-set 20 UseTrustedPrograms=Yes TrustedPrograms.item_#.UseTrustedProgram=Yes
TrustedPrograms.item_#.ProgramPath=<path to app> TrustedPrograms.item_#.ProgramDesc=<trusted app name>
[TrustedPrograms.item_#.UseTrustedProgramForMDRAndEDR=Yes] [TrustedPrograms.item_#.ApplyToDescendants=Yes]
```

3. 若要將受信任應用程式處理程序的記憶體排除在掃描範圍之外，請執行以下命令：

```
kesl-control --set-app-settings MemScanExcludedProgramPath.item_#=<path to app>
```

符號

命令選項

設定	描述
`ExcludedForProgram.item_#.UseExcludedForProgram=Yes`	將受信任應用程式的檔案活動排除在檔案威脅防護元件的掃描範圍之外。
`ExcludedForProgram.item_#.ProgramPath`	ID 為 `#` 的受信任應用程式路徑。檔案威脅防護元件不會掃描指定應用程式的處理程序。 如果使用可更新內核模組進行系統事件攔截，則指定的處理程序將被排除在所有命名空間的攔截之外。
`ExcludedForProgram.item_#.AreaDesc`	ID 為 `#` 的受信任應用程式名稱。
`ExcludedForProgram.item_#.ApplyToDescendants=Yes`	將受信任應用程式的子處理程序排除在檔案威脅防護元件的掃描範圍之外。
`UseTrustedPrograms=Yes`	將受信任應用程式處理程序的活動排除在行為偵測元件的掃描範圍之外。
`TrustedPrograms.item_#.UseTrustedProgram=Yes`	將 ID 為 `#` 的受信任應用程式活動排除在掃描範圍之外。
`TrustedPrograms.item_#.ProgramPath`	ID 為 `#` 的受信任應用程式路徑。行為偵測元件不會掃描指定應用程式的處理程序。 Kaspersky Endpoint Security 輸入遮罩時支援 `*` 和 `?` 字元。
`TrustedPrograms.item_#.ProgramDesc`	ID 為 `#` 的受信任應用程式名稱。
`TrustedPrograms.item_#.UseTrustedProgramForMDRAndEDR=Yes`	將受信任應用程式的活動排除在 Managed Detection and Response 和 Endpoint Detection and Response Expert (on-premises) 元件的遙測資料收集範圍之外。
`TrustedPrograms.item_#.ApplyToDescendants=Yes`	將受信任應用程式的子處理程序排除在行為偵測元件的掃描範圍之外。
`MemScanExcludedProgramPath.item_#`	ID 為 `#` 的受信任應用程式路徑。應用程式不會檢查受信任應用程式處理程序的記憶體。

如何新增受信任裝置

*信任的裝置*是指在信任裝置設定中指定的使用者可隨時進行完全存取的裝置。

要使用受信任裝置，您可以為單一使用者、一組使用者或組織的所有使用者授予存取權限。例如，如果您的組織不允許使用卸除式磁碟機，但是管理員在工作中使用卸除式磁碟機，您可以僅允許一組管理員使用卸除式磁碟機。為此，請將卸除式磁碟機新增到受信任清單中，並配置使用者存取權限。

您可以根據以下資料新增受信任裝置：

- **ID**每個裝置都有唯一識別碼（Hardware ID，或 HWID）。您可以使用作業系統工具在裝置屬性中檢視該 ID。裝置 ID 範例：`SCSI\CDROM&VEN_NECVMWAR&PROD_VMWARE_SATA_CD00\5&354AE4D7&0&000000`。如果要新增多個特定裝置，則按 ID 新增裝置很方便。

- **按 ID 遮罩**。如果您使用具有相似 ID 的多個裝置，則可以使用遮罩將裝置新增至受信任清單。`*` 字元可替換任意一組字元。`?` 字元可替換任意單一字元。例如，`WDC_C*`。

如何在卡巴斯基安全管理中心網頁主控台中新增受信任裝置

1. 在網頁主控台的主視窗中，選擇**資產管理 → 政策**。

2. 點擊 Kaspersky Endpoint Security 政策的名稱。

   政策內容視窗將開啟。

3. 選擇“**應用程式設定**”標籤。

4. 轉到”**裝置控制**”→”**受信任裝置**”。

   這會開啟包含受信任裝置清單的視窗。

5. 點擊“**新增**”。

   這會開啟新增裝置的表單。

6. 在 **使用者或群組** 下，指定要將該裝置視為受信任裝置的使用者或使用者群組。

   您可以在卡巴斯基安全管理中心的帳戶清單中選擇使用者，或手動輸入本機使用者名稱。卡巴斯基建議僅在無法使用網域使用者帳戶的特殊情況下使用本機使用者帳戶。

   預設情況下，允許 Everyone 群組存取受信任裝置。

7. 在 **裝置類型** 下，從下拉式清單選取裝置類型（例如 **卸除式磁碟機**）。

8. 若要根據 ID 遮罩新增裝置，請選取 **使用遮罩** 核取方塊。

9. 在 **搜尋受信任的裝置** 欄位中，輸入裝置 ID 或 ID 遮罩。

   表格會顯示符合定義條件的裝置清單。

10. 選中您想要新增到受信任裝置清單中的裝置名稱旁邊的核取方塊。

11. 如有必要，請在 **註釋** 索引標籤上說明將裝置新增至受信任清單的原因。

12. 要將此政策套用到電腦，請關閉... 掛鎖圖示並儲存變更。

如何在命令列中新增受信任裝置

1. 若要新增受信任裝置，請執行下列指令：

```
kesl-control --trusted-devices --add <device ID>
```

2. 若要掃描元件的受信任裝置清單，請執行下列指令：

```
kesl-control --trusted-devices --list
```

範例

```
kesl-control --trusted-devices --add WDC_C*
```

一般設定

偵測設定

偵測其他類型的物件

不管應用程式設定的配置如何，Kaspersky Endpoint Security 始終會偵測並封鎖病毒、蠕蟲和木馬。它們可能會給電腦帶來巨大的損害。

您還可以啟用偵測入侵者可以利用來危害電腦或使用者資料的合法應用程式。此類應用程式不一定具有惡意目的，但可能會遭駭客利用。如需入侵者可以利用來危害電腦或使用者資料的合法應用程式詳細資訊，請造訪 卡巴斯基百科全書網站 。

如何在網頁主控台中設定偵測入侵者可以利用來危害裝置或資料的應用程式

1. 在網頁主控台的主視窗中，選擇**資產管理 → 政策**。
2. 點擊 Kaspersky Endpoint Security 政策的名稱。
   政策內容視窗將開啟。
3. 選擇“**應用程式設定**”標籤。
4. 轉到 **一般設定 → 偵測設定**。
5. 在“**偵測其他類型的物件**“塊中，選中“**可被入侵者利用以破壞您的電腦或個人資料的合法軟體**”核取方塊。

6. 儲存變更。

偵測設定

如何在命令列中設定偵測入侵者可以利用來危害裝置或資料的應用程式

1. 若要設定偵測攻擊者可以用來危害裝置或資料的應用程式，請針對應用程式防護元件執行下列指令：

```
kesl-control --set-app-settings DetectOtherObjects=<Yes|No>
```

2. 若要根據包含入侵者可以利用的合法應用程式（這些應用程式可用於危害裝置或資料）的網址資料庫檢查連結，請在 Web 威脅防護元件中執行下列指令：

```
kesl-control --set-settings 14 CheckOther=<Yes|No>
```

3. 若要檢查目前的應用程式設定，請執行下列指令：

```
kesl-control --get-app-settings
```

4. 若要檢查目前的 Web 威脅防護設定，請執行下列指令：

```
kesl-control --get-settings 14
```

事件記錄設定

預設情況下，Kaspersky Endpoint Security 不會記錄處理已封裝和未受感染物件的事件，也不會記錄未由檔案威脅防護元件處理之物件的事件。

您可以啟用此類事件的記錄，讓應用程式產生 *偵測到封裝物件*、*物件未處理*、*物件已處理* 事件。此類事件在設定元件時以及偵錯或疑難排解應用程式時非常有用。這可讓您確保此類物件已由應用程式掃描，且未因錯誤而被略過。

如何在網頁主控台中啟用物件處理事件記錄

1. 在網頁主控台的主視窗中，選擇**資產管理 → 政策**。
2. 點擊 Kaspersky Endpoint Security 政策的名稱。
   政策內容視窗將開啟。
3. 選擇“**應用程式設定**”標籤。
4. 轉到 **一般設定 → 偵測設定**。
5. 在**物件記錄設定**下，選取相關事件類型旁的核取方塊。
   - **記錄清潔物件**
   - **記錄未處理的物件**
   - **記錄封裝的物件**
6. 儲存變更。

如何在命令列中啟用記錄有關處理物件的事件

1. 若要記錄有關未感染物件的事件，請執行下列指令：

```
kesl-control --set-settings 1 ReportCleanObjects=Yes
```

2. 若要記錄有關未處理物件的事件，請執行下列指令：

```
kesl-control --set-settings 1 ReportUnprocessedObjects=Yes
```

3. 若要記錄有關已封裝物件的事件，請執行下列指令：

```
kesl-control --set-settings 1 ReportPackedObjects=Yes
```

4. 若要檢查檔案威脅防護設定的目前值，請執行下列指令：

```
kesl-control --get-settings 1
```

卡巴斯基安全網路

為了更有效地防護您的電腦，Kaspersky Endpoint Security 使用從全球使用者處接收的資料。卡巴斯基安全網路旨在獲取此資料。

應用程式可能無法在美國境內使用 KSN 功能。

卡巴斯基安全網路 (KSN) 是雲端服務的基礎架構，可讓您存取卡巴斯基線上知識庫，其中包含檔案、網頁資源和軟體信譽的相關資訊。使用卡巴斯基安全網路的資料可確保 Kaspersky Endpoint Security 能夠更快地對新型威脅作出回應，提高一些防護元件的效能，並減少誤報風險。如果您正在參與卡巴斯基安全網路，KSN 服務將為 Kaspersky Endpoint Security 提供有關所掃描網址的信譽的資訊，以及有關所掃描檔案的類別和信譽的資訊。有關 KSN 配置的詳細資訊，請參閱卡巴斯基安全管理中心說明。

卡巴斯基安全網路的使用是自願的。應用程式將在初始化設定期間提示您使用 KSN。使用者可以隨時開始或停止加入 KSN。

關於參與 KSN 期間產生的統計資訊的儲存、銷毀和/或提交給卡巴斯基的詳細資訊，請參閱《卡巴斯基安全網路聲明》和卡巴斯基網站。包含卡巴斯基安全網路聲明文字的 ksn_license.<language ID> 檔案隨附於應用程式發佈套件中，並可在 /opt/kaspersky/kesl/doc 目錄中找到。

卡巴斯基信譽資料庫的基礎結構

Kaspersky Endpoint Security 支援以下基礎設施解決方案與卡巴斯基信譽資料庫搭配使用：

- *卡巴斯基安全網路 (KSN)* 是大多數 Kaspersky 應用程式使用的解決方案。KSN 參與者從卡巴斯基接收資訊，並向 Kaspersky 傳送使用者電腦上偵測到的物件的資訊，以便 Kaspersky 分析人員進行額外分析，並包括在信譽和統計資料庫中。
- *卡巴斯基安全網路 (KSN)* 是讓承載 Kaspersky Endpoint Security 或其他 Kaspersky 應用程式的電腦的使用者獲得卡巴斯基信譽資料庫以及其他統計資料的存取權限的解決方案，無需從他們自己的電腦向卡巴斯基傳送資料。KPSN 專為因以下任一原因無法參與卡巴斯基安全網路的公司客戶所設計：
  - 本機工作站未連線網際網路。
  - 法律禁止或企業安全限制將任何資料傳送到國外或組織的本機網路

若要在使用新的產品授權啟動應用程式後使用 KPSN，請將新的產品授權金鑰告知服務提供者。否則，身分驗證錯誤將阻止與 KPSN 進行資料交換。

卡巴斯基私有安全網路的限制

卡巴斯基私有安全網路使您可以使用自己的本機信譽資料庫來檢查物件（檔案或網址）的信譽。與新增到 KSN / KPSN 中的物件相比，新增到本機信譽資料庫中的物件的信譽具有更高的優先級。例如，假設 Kaspersky Endpoint Security 正在掃描電腦並請求 KSN / KPSN中 檔案的信譽。如果檔案在本機信譽資料庫中具有“*不信任*”的信譽，但在 KSN / KPSN 中具有“*受信任*”的信譽，則 Kaspersky Endpoint Security 會將檔案偵測為“*不信任*”，並將採取針對偵測到的威脅而定義的操作。

但是，在某些情況下，Kaspersky Endpoint Security 可能不會請求 KSN / KPSN 中物件的信譽。在這種情況下，Kaspersky Endpoint Security 將不會從 KPSN 的本機信譽資料庫接收資料。由於以下原因，Kaspersky Endpoint Security 可能不會請求 KSN / KPSN 中物件的信譽：

- 卡巴斯基應用程式正在使用離線信譽資料庫。離線信譽資料庫旨在在卡巴斯基應用程式運行期間最佳化資源，並防護電腦上的重要物件。離線信譽資料庫由卡巴斯基專家根據卡巴斯基安全網路中的資料建立。卡巴斯基應用程式使用特定應用程式的病毒資料庫更新離線信譽資料庫。如果離線信譽資料庫包含有關被掃描物件的資訊，則應用程式不會從 KSN / KPSN 請求該物件的信譽。
- 在應用程式設定中配置掃描排除項目（受信任區域）。在這種情況下，應用程式不會考慮本機信譽資料庫中物件的信譽。
- 應用程式會使用掃描最佳化技術，例如 iChecker，或將傳送至 KSN / KPSN 的信譽請求快取。在這種情況下，應用程式不可請求先前掃描的物件的信譽。
- 為了最佳化其工作量，應用程式掃描特定格式和大小的檔案。有關格式和大小限制的清單由卡巴斯基專家確定。此清單已使用應用程式的病毒資料庫更新。您也可以在應用程式介面中配置掃描優化設定，例如，檔案威脅防護元件 。
- Kaspersky Endpoint Security 在 Light Agent 模式下透過 KSN 代理伺服器 與 KSN 伺服器通訊。不支援與 KSN 直接通訊。

如何啟用或停用卡巴斯基安全網路

預設情況下，Kaspersky Endpoint Security 使用延伸 KSN 模式。*延伸 KSN 模式*是 Kaspersky Endpoint Security 向 Kaspersky 傳送附加資料的一種模式。

> 不會獲取、處理或儲存任何個人資料。關於參與 KSN 期間產生的統計資訊的儲存、銷毀和/或提交給卡巴斯基的詳細資訊，請參閱《卡巴斯基安全網路聲明》和卡巴斯基網站。帶有卡巴斯基安全網路聲明文字的檔案包含在應用程式分發套裝中。

如何在網頁主控台中啟用或停用 KSN

1. 在網頁主控台的主視窗中，選擇**資產管理 → 政策**。
2. 點擊 Kaspersky Endpoint Security 政策的名稱。

   政策內容視窗將開啟。
3. 選擇“**應用程式設定**”標籤。
4. 轉到”**一般設定**”→”**卡巴斯基安全網路**”。
5. 使用 **卡巴斯基安全網路 (KSN) 使用** 切換開關來啟用或停用該元件。
6. 如果您已啟用 KSN 使用，**卡巴斯基安全網路聲明**視窗將會開啟。如果同意，請接受《卡巴斯基安全網路(KSN)聲明》的使用條款。
7. 如有需要，請選取或清除 **使用延伸 KSN 模式** 核取方塊。

8. 儲存變更。

卡巴斯基安全網路

如何在命令列中啟用或停用 KSN

1. 檢查卡巴斯基安全網路的狀態：

```
kesl-control --app-info
```

應用程式會在 **卡巴斯基安全網路使用** 行顯示 KSN 的狀態：

- **已停用**
- **基本 KSN 模式**
- **延伸 KSN 模式**

2. 若要啟用卡巴斯基安全網路的標準模式，請執行以下命令：

```
kesl-control --set-app-settings UseKSN=Basic --accept-ksn
```

3. 若要啟用卡巴斯基安全網路的延伸模式，請執行以下命令：

```
kesl-control --set-app-settings UseKSN=Extended --accept-ksn
```

4. 若要停用卡巴斯基安全網路，請執行以下命令:

```
kesl-control --set-app-settings UseKSN=No
```

如何在應用程式介面中啟用或停用 KSN 使用

1. 開啟應用程式主視窗。
2. 在應用程式主視窗下方，點擊 **設定** 按鈕。
3. 在開啟的視窗中，選取以下選項之一：
   - **延伸 KSN 模式**，如果您想要使用卡巴斯基安全網路、從知識庫取得資訊，以及傳送關於威脅類型和來源的匿名統計資料和資訊。
   - **基本 KSN 模式**，如果您想要使用卡巴斯基安全網路、從知識庫取得資訊，但不傳送關於威脅類型和來源的匿名統計資料和資訊。
4. 點擊"**啟用**"。
5. 在 **卡巴斯基安全網路使用** 視窗中，仔細閱讀卡巴斯基安全網路聲明，然後選取以下選項之一：
   - **我確認我已完整閱讀、理解並接受卡巴斯基安全網路聲明的條款和條件**
   - **我不接受卡巴斯基安全網路聲明的條款和條件**
6. 點擊"**OK**"。

因此，如果啟用了使用 KSN，則 Kaspersky Endpoint Security 會使用有關從卡巴斯基安全網路收到的檔案、網頁資源和應用程式信譽的資訊。

Kaspersky Endpoint Security 使用以下網路設定與外部服務互動：

位址	協定	連接埠
ds.kaspersky.com	HTTPS	443
ksn-a-stat-geo.kaspersky-labs.com	KSN	443, 1443
ksn-file-geo.kaspersky-labs.com	KSN	443, 1443
ksn-verdict-geo.kaspersky-labs.com	KSN	443, 1443
ksn-url-geo.kaspersky-labs.com	KSN	443, 1443
ksn-a-p2p-geo.kaspersky-labs.com	KSN	443, 1443
ksn-cinfo-geo.kaspersky-labs.com	KSN	443, 1443

應用程式的雲端模式是什麼

在 *雲端模式*中，Kaspersky Endpoint Security 會使用輕量版的病毒防護資料庫，這可將電腦 RAM 的負載大約減半。

只有在啟用卡巴斯基安全網路時，才能使用雲端模式。如果您未參與卡巴斯基安全網路或已停用雲端模式，Kaspersky Endpoint Security 會從 Kaspersky 伺服器下載完整版本的病毒資料庫。預設情況下已啟用雲端模式。

> 如果應用程式在 Light Agent 模式下執行，則無法使用雲端模式。

如何在網頁主控台中啟用或停用雲端模式

1. 在網頁主控台的主視窗中，選擇**資產管理 → 政策**。
2. 點擊 Kaspersky Endpoint Security 政策的名稱。
   政策內容視窗將開啟。
3. 選擇“**應用程式設定**”標籤。
4. 轉到”**一般設定**”→”**卡巴斯基安全網路**”。
5. 使用“**使用雲端模式**“切換開關可啟用或停用元件。
6. 要將此政策套用到電腦，請關閉... 掛鎖圖示並儲存變更。

如何在命令列中啟用或停用雲端模式

1. 若要瞭解應用程式的目前狀態，請執行命令以顯示應用程式的一般設定：

   ```
   kesl-control --get-app-settings
   ```

   應用程式會在 `CloudMode` 行中顯示其狀態。

2. 若要啟用或停用雲端模式，請執行以下命令：

   ```
   kesl-control --set-app-settings CloudMode=<Yes|No>
   ```

因此，Kaspersky Endpoint Security 在下一次更新期間將下載輕量級版本或完整版的病毒資料庫。

如果病毒資料庫的輕量級版本不可用，Kaspersky Endpoint Security 會自動轉換到病毒資料庫的進階版本。

KSN 代理的用途

受卡巴斯基安全管理中心管理伺服器管理的使用者電腦可以直接或者透過 KSN Proxy 服務與 KSN 互動。

> 如果應用程式在 Light Agent 模式下執行，則不支援與 KSN 直接通訊。Kaspersky Endpoint Security 使用 KSN 代理伺服器與 KSN 伺服器互動。

KSN Proxy 服務提供以下功能：

- 即使無法直接存取網際網路，使用者的電腦仍可查詢 KSN 並向 KSN 提交資訊。
- KSN Proxy 服務暫存處理過的資料，從而減少外部網路通訊信道上的負荷，並加快使用者接收資料的速度。

預設情況下，在 KSN 被啟用和 KSN 聲明被接受後，應用程式將使用代理伺服器連線到卡巴斯基安全網路。應用程式使用的代理伺服器是透過 TCP 連接埠 13111 的卡巴斯基安全管理中心管理伺服器。

您可以在管理伺服器內容中進行 KSN 代理伺服器設定。如需 KSN 代理伺服器的詳細資訊，請參閱 卡巴斯基安全管理中心說明。

無法使用命令列設定與 KSN 代理伺服器的連線設定。

如何在網頁主控台中透過代理伺服器設定 KSN 連線

1. 在網頁主控台的主視窗中，選擇**資產管理 → 政策**。
2. 點擊 Kaspersky Endpoint Security 政策的名稱。
   政策內容視窗將開啟。
3. 選擇"**應用程式設定**"標籤。
4. 轉到"**一般設定**"→"**卡巴斯基安全網路**"。
5. 使用 **使用管理伺服器為 KSN 代理伺服器** 核取方塊來啟用或停用 KSN 代理。
6. 如有必要，選取或清除 **當 KSN 代理伺服器不可用時使用卡巴斯基安全網路伺服器** 核取方塊。預設情況下已選擇此核取方塊。
   如果啟用此選項，當 KSN 代理服務無法使用時，Kaspersky Endpoint Security 會直接使用 KSN 伺服器。KSN 伺服器可以位於 Kaspersky 側，也可以位於協力廠商一側的伺服器（使用卡巴斯基私有安全網路時）。
7. 儲存變更。

配置資料傳輸到卡巴斯基安全管理中心儲存

在卡巴斯基安全管理中心中，您可以啟用或停用將備份中的檔案、隔離區的檔案、未處理的檔案和已連線的裝置相關的資料傳輸到卡巴斯基安全管理中心儲存。

如何檢視用戶端裝置上的已隔離檔案

卡巴斯基應用程式在用戶端裝置上隔離的檔案總清單會儲存在卡巴斯基安全管理中心中。

1. 在網頁主控台的主視窗中，選擇**操作 → 儲存區**。
2. 前往 **隔離** 資料夾。
3. 已隔離物件的資訊會顯示在主控台的右側窗格中。

如何檢視用戶端裝置上備份中的檔案

卡巴斯基應用程式在用戶端裝置上置於備份中的檔案總清單會儲存在卡巴斯基安全管理中心中。

1. 在網頁主控台的主視窗中，選擇**操作 → 儲存區**。
2. 前往 **檔案備份** 資料夾。
3. 置於備份中的物件資訊會顯示在主控台的右側窗格中。

如何檢視活動威脅清單中未處理檔案的資訊

1. 在網頁主控台的主視窗中，選擇**操作** → **儲存區**。
2. 前往 **活動威脅** 資料夾。
3. 活動威脅清單中未處理檔案的資訊會顯示在主控台的右側窗格中。

如何檢視連線至用戶端裝置的硬體資訊

1. 在網頁主控台的主視窗中，選擇**操作** → **儲存區**。
2. 前往 **硬體** 資料夾。
3. 裝置資訊會顯示在主控台的右側窗格中。

如果啟用了裝置控制，則會傳輸資料。

如何檢視用戶端裝置上的應用程式資訊

1. 在網頁主控台的主視窗中，選擇**操作** → **第三方應用程式**。
2. 前往 **應用程式登錄** 資料夾。
3. 應用程式資訊會顯示在主控台的右側窗格中。

如果啟用了應用程式控制，則會傳輸資料。

如何設定與管理伺服器的整合

若要在政策內容中設定管理伺服器整合：

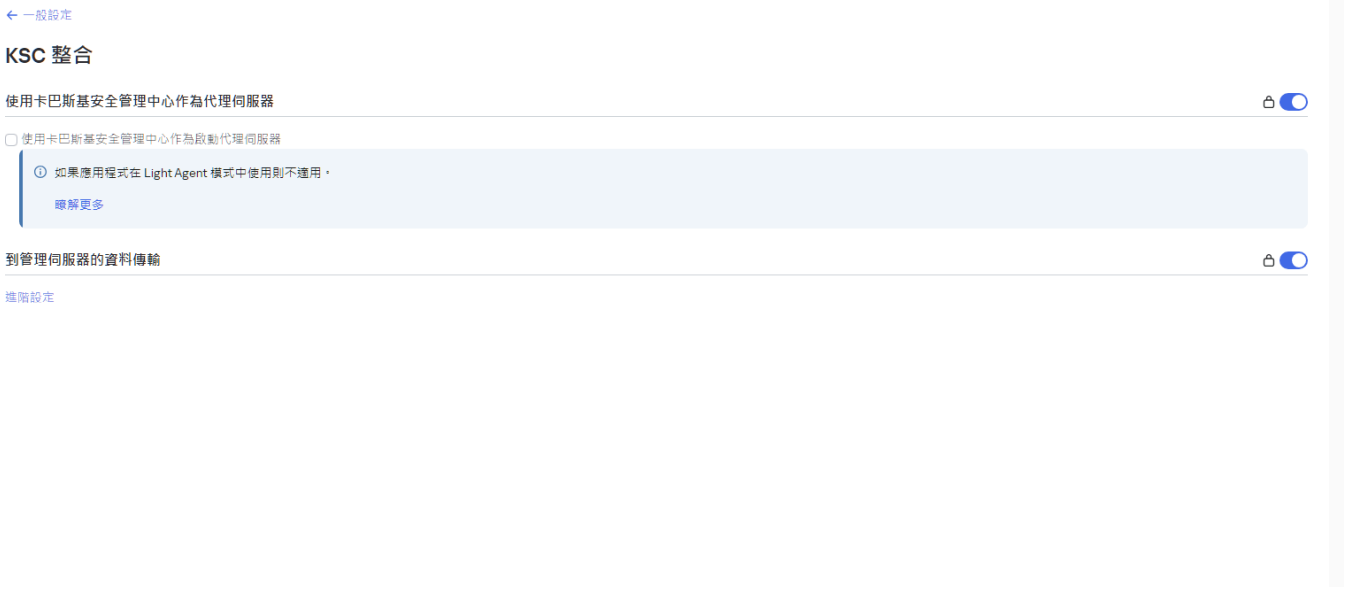
1. 在網頁主控台的主視窗中，選擇**資產管理** → **政策**。
2. 點擊 Kaspersky Endpoint Security 政策的名稱。
   政策內容視窗將開啟。
3. 選擇"**應用程式設定**"標籤。
4. 轉到"**一般設定**"→"**KSC 整合**"。
5. 點擊 **其他設定** 連結。
6. 選取要將其資訊轉送至管理伺服器的用戶端電腦事件類別：
   - **關於隔離區中的檔案** 此核取方塊可啟用或停用將隔離檔案的相關資料傳輸到管理伺服器。
   - **關於備份中的檔案**。此核取方塊可啟用或停用將關於備份中檔案的資料傳輸到管理伺服器。
   - **關於未處理的檔案**。此核取方塊可啟用或停用向管理伺服器傳送關於掃描期間未處理檔案的通知。

- **關於已安裝的裝置**。此核取方塊可啟用或停用向管理伺服器傳送關於安裝在用戶端裝置上或已連線到用戶端的裝置的資料。
- **關於已啟動的應用程式**。此核取方塊可啟用或停用將清查工作在用戶端裝置上發現的應用程式清單傳送至管理伺服器。

7. 要將此政策套用到電腦，請關閉... 掛鎖圖示並儲存變更。

若要在受管理裝置的內容中設定管理伺服器整合：

1. 在網頁主控台的主視窗中，選擇**資產管理 → 資產（裝置）→ 受管理裝置**。
2. 點擊 **<device name>** 連結。
3. 選取 **應用程式** 索引標籤，然後點擊 **Kaspersky Endpoint Security** 連結。
4. 在 **應用程式設定** 索引標籤上，前往 **儲存設定** 區段。
5. 在 **將資料傳輸至管理伺服器的設定** 下，點擊 **設定** 按鈕。
6. 在 **資料傳輸設定** 視窗中，您可以啟用或停用向管理伺服器傳送資訊：
   - **通知備份中的檔案**。此核取方塊可啟用或停用將關於備份中檔案的資料傳輸到管理伺服器。
   - **通知隔離區中的檔案**。此核取方塊可啟用或停用將關於被隔離檔案的資料傳輸到管理伺服器。
   - **通知未處理的檔案**。此核取方塊可啟用或停用向管理伺服器傳送關於掃描期間未處理檔案的通知。
   - **通知已安裝的裝置**。此核取方塊可啟用或停用向管理伺服器傳送關於安裝在用戶端裝置上或已連線到用戶端的裝置的資料。
   - **通知在裝置上發現的應用程式**。此核取方塊可啟用或停用將清查工作在用戶端裝置上發現的應用程式清單傳送至管理伺服器。
7. 儲存變更。



與卡巴斯基安全管理中心的整合

如何設定應用程式啟動

設定應用程式啟動

您可以設定 Kaspersky Endpoint Security 的啟動失敗嘗試次數上限和啟動逾時時間。如果應用程式長時間無法啟動，這可以減輕系統負載。預設情況下，連續嘗試啟動應用程式失敗的次數上限為 5 次，逾時時間上限為 3 分鐘。

如何在網頁主控台中設定應用程式啟動

1. 在網頁主控台的主視窗中，選擇**資產管理 → 政策**。
2. 點擊 Kaspersky Endpoint Security 政策的名稱。
   政策內容視窗將開啟。
3. 選擇"**應用程式設定**"標籤。
4. 轉到"**一般設定**"→"**使用者互動**"。
5. 在 **應用程式啟動設定** 下，輸入以下欄位中的值：
   - **應用程式啟動嘗試連續不成功最大次數**預設值：5。
   - **等待應用程式啟動的最長時間（分鐘）**預設值：3。
6. 要將此政策套用到電腦，請關閉... 掛鎖圖示並儲存變更。

如何在命令列中設定應用程式啟動

在指令列中，您可以使用`MaxRestartCount`中的`StartupTimeout`和StartupTimeout設定來配置應用程式啟動設定。

`MaxRestartCount`設定可讓您設定啟動應用程式連續嘗試失敗的最大次數。此設定可採用 1 至 10 之間的值。預設值：5。

`StartupTimeout`設定可讓您設定等待應用程式啟動的最大時間（以分鐘為單位），此後 kesl 處理程序將重新啟動。此設定可採用 1 至 60 之間的值。預設值：3。

套用關鍵更新

您可以設定應用程式，在安裝後的前 24 小時過後，收到關鍵更新時自動重新啟動。安裝後的前 24 小時內，應用程式收到關鍵更新時會自動重新啟動，無需其他設定。

如何在網頁主控台中設定應用程式自動重新啟動

1. 在網頁主控台的主視窗中，選擇**資產管理 → 政策**。
2. 點擊 Kaspersky Endpoint Security 政策的名稱。
   政策內容視窗將開啟。
3. 選擇“**應用程式設定**”標籤。
4. 轉到”**一般設定**”→”**使用者互動**”。
5. 在“**套用關鍵更新**“塊中，選中“**當收到關鍵更新時自動重啟應用程式**”核取方塊。
   Kaspersky Endpoint Security 應用程式會在安裝一天後收到關鍵更新時重新啟動。
6. 儲存變更。

如何在命令列中設定應用程式自動重新啟動

您可以使用 一般應用程式設定中的 `UrgentUpdateRestartEnabled` 設定，在命令列中設定應用程式自動重新啟動。

若要在安裝關鍵更新時自動重新啟動應用程式，請執行以下命令：

```
kesl-control --set-app-settings UrgentUpdateRestartEnabled=Yes
```

配置工作管理的權限

您可以在卡巴斯基安全管理中心中定義下列使用者權限：

- 使用在 Kaspersky Endpoint Security 中建立的本機工作。如果卡巴斯基安全管理中心政策阻止使用者檢視、編輯、建立及刪除本機工作，則無法取得關於 Scan_My_Computer、Critical_Areas_Scan、Container_Scan、Inventory_Scan、Update（在標準模式下）和 Rollback（在標準模式下）工作的資訊。
- 檢視和管理用戶端裝置上在卡巴斯基安全管理中心中建立的工作。

若要在網頁主控台中設定工作管理權限：

1. 在網頁主控台的主視窗中，選擇**資產管理 → 政策**。
2. 點擊 Kaspersky Endpoint Security 政策的名稱。
   政策內容視窗將開啟。
3. 選擇“**應用程式設定**”標籤。
4. 轉到”**一般設定**”→”**使用者互動**”。

5. 在 **允許的動作** 下，選取允許使用者在其裝置上執行的動作：

- **存取本機工作**如果選擇此核取方塊，本機工作將顯示在 Kaspersky Endpoint Security 的本機介面上。如果其他政策限制未阻止此操作，使用者可以在應用程式圖形介面或命令列中設定、執行、建立及刪除可用的本機工作。
- **管理小組任務**如果選取此核取方塊，使用者可以在用戶端裝置上管理卡巴斯基安全管理中心中設定的群組工作。可以從應用程式圖形介面或命令列執行工作。

6. 要將此政策套用到電腦，請關閉... 掛鎖圖示並儲存變更。

密碼防護

密碼防護可讓您根據授予的權限，限制使用者修改 Kaspersky Endpoint Security 的存取權限（例如，檢視應用程式報告的權限）。限制對應用程式設定的存取權限，可降低對應用程式進行未授權或非故意變更的風險。

密碼防護的運作方式

1. **使用者嘗試執行由該元件控制的操作**

   例如，停用防護元件或檢視 Kaspersky Endpoint Security 報告。

2. **Kaspersky Endpoint Security 檢查使用者權限**

   如果使用者擁有相應權限，則會成功執行該操作。如果使用者沒有相應權限，應用程式會封鎖該操作並顯示錯誤。

   在 Kaspersky Endpoint Security 的圖形介面中，無法檢視或編輯禁止的操作。

配置密碼防護

1. **啟用密碼防護**

   預設情況下，密碼防護處於停用狀態。在網頁主控台或管理主控台中啟用該元件，或使用以下命令在命令列中啟用該元件：

   ```
   kesl-control --set-permission-manager-settings Enabled=Yes
   ```

2. **配置使用者權限**

   預設情況下，應用程式已針對預先定義的使用者群組設定使用者權限：*kesladmin*、*kesluser*、*keslaudit*。

   為這些群組配置使用者權限，或建立新的使用者或使用者群組。

   為確保應用程式正常運作，建議您為至少一個群組配置權限。

如何在網頁主控台中配置自訂權限

1. 在網頁主控台的主視窗中，選擇**資產管理 → 政策**。
2. 點擊 Kaspersky Endpoint Security 政策的名稱。
   政策內容視窗將開啟。
3. 選擇"**應用程式設定**"標籤。
4. 轉到"**一般設定**"→"**自我防護**"。
5. 確保該元件的切換開關處於 **密碼防護已啟用** 位置。
6. 點擊"**使用者權限**"連接。
   這會開啟包含使用者及其權限的視窗。
7. 如果您要變更預先定義群組的權限，請按一下群組名稱。
   如果您要變更其他使用者或群組的權限：
   a. 點擊"**新增**"。
   b. 從 Active Directory 選取使用者或群組，或手動輸入名稱。
8. 選取您要授予使用者或群組之權限旁的核取方塊。
9. 要將此政策套用到電腦，請關閉... 🔒掛鎖圖示並儲存變更。

自我防護

如何在命令列上配置自訂權限

1. 若要檢視目前的密碼防護設定清單，請執行以下指令：

```
kesl-control --get-permission-manager-settings
```

2. 若要變更使用者或群組的權限，請執行以下指令：

```
kesl-control --set-permissions <principal> [--group] <permissions>=<Yes|No> [--file <file name>] [--
json]
```

3. 若要移除已配置權限的使用者或群組，請執行以下指令：

```
kesl-control --remove-permissions <principal> [--group]
```

符號

命令選項

設定	描述
`--group`	此設定適用於群組。如果未指定 `--group` 選項，則此設定適用於個別使用者。
`--file <file name>`	將參數輸出到檔案或從檔案匯入參數。輸入 `<file name>`。
`--json`	將參數輸出到 JSON 檔案或從 JSON 檔案匯入參數。 只有在指定 `--file <file name>` 選項時，才能指定此選項。
`principal`	使用者或使用者群組名稱。
`permissions`	自訂權限。指定 `Yes` 可允許使用者執行動作，或指定 `No` 可拒絕。 • `StopProtection`。停用防護元件。 • `StopSecurityControl`。停用控制元件 • `StartProtection`。啟用防護元件。 • `StartSecurityControl`。啟用控制元件 • `ApplicationSettings`。設定應用程式 • `ViewReports`。檢視報告 • `RestoreFromBackup`。從備份還原 • `RemoveLicenseKey`。移除金鑰 • `AddLicense`。新增金鑰 • `DisablePolicy`。停用卡巴斯基安全管理中心政策

範例

撤銷 *kesluser* 群組的檢視報告權限：

```
kesl-control --set-permissions kesluser --group ViewReports=No
```

允許 *new-user* 管理控制元件：

```
kesl-control --set-permissions new-user startSecurityControl=Yes StopSecurityControl=Yes
```

密碼防護的特殊考量事項

- 如果停用密碼防護，是否允許使用者管理應用程式由 使用者角色 決定。
- 如果使用者的存取層級同時受群組權限和個別權限控管，個別權限會覆寫群組權限。也就是說，即使使用者的個別權限比該使用者的群組權限更嚴格，也以更嚴格的權限為準。

  例如，如果 *kesluser* 群組不得管理應用程式，您仍可以允許該群組中的個別使用者管理應用程式。即使群組權限不允許，這類使用者仍可管理應用程式。
- 如果啟用密碼防護，且使用者既沒有個別權限也沒有群組權限，則會禁止所有動作。

關於自訂權限

如果啟用密碼防護，將使用 *使用者權限* 控制管理 Kaspersky Endpoint Security 的存取權。使用者權限定義使用者的權限（請參閱下表）。

自訂權限

權限	權限
設定應用程式	檢視和編輯應用程式設定。 無需使用 `sudo` 命令，即可在應用程式的 圖形介面 和命令列中管理工作設定。 為使用者指派角色。 撤銷使用者角色（管理員無權撤銷自己的管理員角色）。 管理 *回溯* 工作。 管理元件： • Managed Detection and Response • Endpoint Detection and Response Optimum
啟用防護元件。	管理元件： • 檔案威脅防護 • 卸除式磁碟機掃描 • 行為偵測 • Anti-Cryptor • BadUSB 攻擊防護 • 郵件威脅防護 • Web 威脅防護 • 網路威脅防護 • 防火牆管理 • 系統完整性監控 • 物件執行防禦 (EDR Optimum) (*EDRO_Prevention*) • Endpoint Detection and Response Expert (on-premises) • Endpoint Detection and Response Expert (cloud) • Network Detection and Response (KATA) • Sandbox • 與 KUMA 整合
停用防護元件	
啟用控制元件	管理元件： • 裝置控制 • 應用程式控制 • Web 控制
停用控制元件	
檢視報告	檢視工作報告 檢視事件
從備份還原	檢視和管理使用者的儲存。
刪除金鑰	管理應用程式授權。
新增金鑰	
停用卡巴斯基安全管理中心政策	在裝置上停用或啟用卡巴斯基安全管理中心政策。

自訂權限涉及的特殊注意事項

- 使用者權限不會影響檢視工作清單、檢視備份中的物件，以及檢視應用程式的設定和狀態。

  所有使用者均可管理以下工作：

  - 掃描工作（*自訂掃描*、*容器掃描*、*自訂容器掃描*、*關鍵區域掃描*、*惡意軟體掃描*）
  - *清查*

- *資料庫和應用程式模組更新*
- *系統完整性檢查*
- *IoC 搜尋*

- 如果裝置受卡巴斯基安全管理中心政策控制，則無法在圖形介面中新增或移除主產品授權金鑰。具有 *新增金鑰* 和 *移除金鑰* 權限的使用者可以新增備用金鑰，或新增用於啟動其他卡巴斯基解決方案（附加元件）的產品授權金鑰。

  如果裝置不受政策管理，使用者可以移除或新增主產品授權金鑰。

預設使用者權限

預設情況下，應用程式已針對預先定義的使用者群組設定使用者權限：*kesladmin*、*kesluser*、*keslaudit*。對於不屬於這些群組的使用者，禁止對應用程式執行所有操作。

預定義群組的使用者權限

權限	kesladmin	kesluser	keslaudit
設定應用程式	✓	–	–
啟用防護元件。	✓	–	–
停用防護元件	✓	–	–
啟用控制元件	✓	–	–
停用控制元件	✓	–	–
檢視報告	✓	–	✓
從備份還原	✓	–	–
刪除金鑰	✓	–	–
新增金鑰	✓	–	–
停用卡巴斯基安全管理中心政策	✓	–	–

效能設定

使用 Kaspersky Endpoint Security 應用程式掃描電腦可能會佔用大量系統資源。若要最佳化系統負載，您可以：

- 使用電池供電時延遲或者略過排程工作
- 限制掃描工作的 CPU 使用率 (%)
- 限制應用程式的駐留記憶體使用量
- 從掃描中排除某些處理程序的記憶體

使用電池供電時延遲或者略過排程工作

如果您的裝置正在使用電池供電，而您想要減少 Kaspersky Endpoint Security 的資源使用量，您可以跳過排程工作：

- 所有掃描工作（自訂掃描、容器掃描、自訂容器掃描、關鍵區域掃描、*惡意軟體掃描*）
- *Inventory*
- *資料庫和應用程式模組更新*
- *應用程式完整性檢查*
- *IOC 掃描*

您可以根據需要手動執行工作。

如何使用網頁主控台取消以電池供電執行時的排程工作

1. 在網頁主控台的主視窗中，選擇**資產管理 → 政策**。
2. 點擊 Kaspersky Endpoint Security 政策的名稱。
   政策內容視窗將開啟。
3. 選擇"**應用程式設定**"標籤。
4. 轉到"**一般設定**"→"**效能**"。
5. 啟用 **使用電池供電時延遲或者略過排程工作** 功能。
   Kaspersky Endpoint Security 會*取消*排程工作。
6. 儲存變更。

如何使用命令列取消以電池供電執行時的排程工作

您可以使用一般應用程式設定中的 `PowerSaveMode` 設定在命令列中設定已排程工作的取消。

若要在裝置以電池供電運作時取消排程工作，請執行以下命令：

```
kesl-control --set-app-settings PowerSaveMode=Yes
```

限制掃描工作的 CPU 使用率 (%)

您可以限制 *惡意軟體掃描*、*關鍵區域掃描*、*清查*和 *容器掃描*工作（屬於 ODS、ContainerScan 和 InventoryScan 類型）的 CPU 使用率和記憶體使用量。預設情況下，記憶體使用限制設定為 8192 MB。未設定 CPU 使用率限制。

建議您將掃描工作的記憶體使用限制設定為低於常駐記憶體使用限制，以免掃描工作耗盡所有可用 RAM 並導致應用程式重新啟動。

請注意，所有 CPU 核心的總容量視為 100%。

在 `top` 實用程式的輸出結果中，100% 代表單一核心的完整使用率。因此，對於 10 核心 CPU（`top` 實用程式報告為 1000% 總使用率），400% 的值表示整體 CPU（所有核心合計）的使用率為 40%。如果您希望相同 10 個核心上 `top` 公用程式輸出中的值永遠不超過 150%，請將 CPU 使用率限制設定為 `15%`。

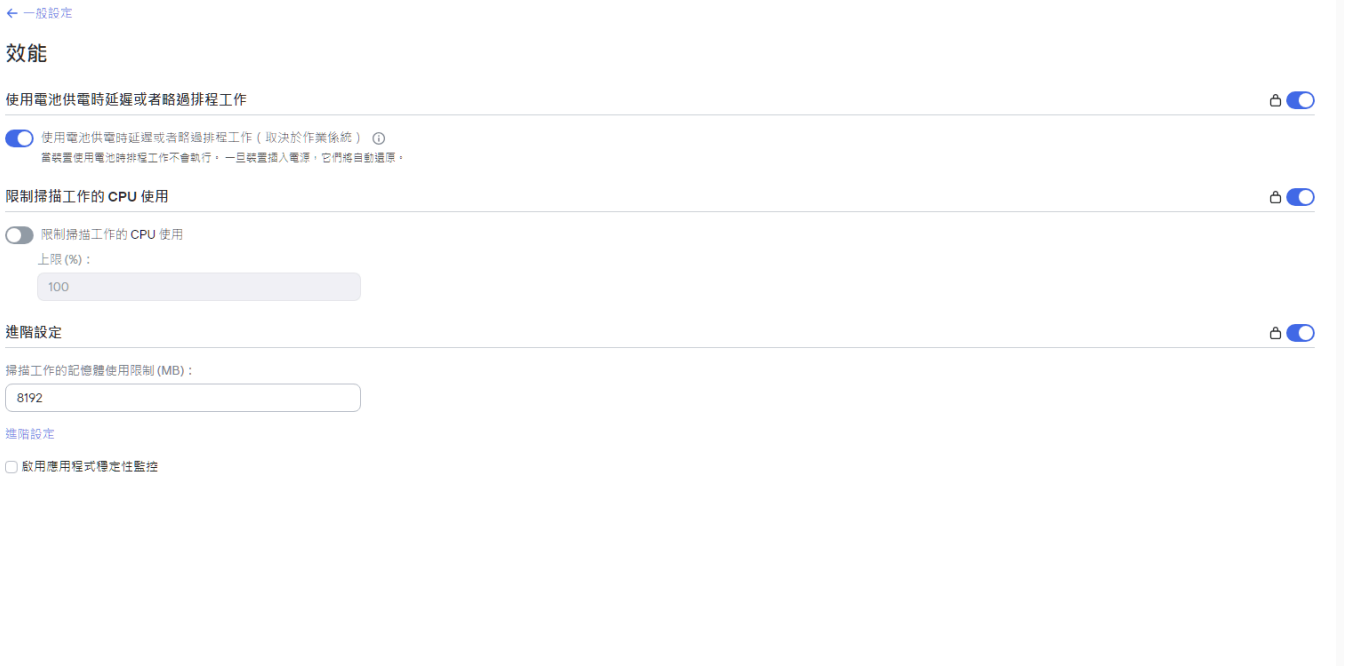
CPU 使用率限制會套用至 *惡意軟體掃描*、*關鍵區域掃描*、*清查*和 *容器掃描*工作，這表示 CPU 使用率可能會超過設定值。

在執行 CentOS 5.2 和 5.4 的裝置上無法限制 CPU 使用率。

如何在網頁主控台中限制記憶體和 CPU 資源使用量

1. 在網頁主控台的主視窗中，選擇**資產管理 → 政策**。
2. 點擊 Kaspersky Endpoint Security 政策的名稱。
   政策內容視窗將開啟。
3. 選擇"**應用程式設定**"標籤。
4. 轉到"**一般設定**"→"**效能**"。
5. 啟用 **限制掃描工作的 CPU 使用** 功能。
6. 在 **上限 (%)** 欄位中指定所有 CPU 核心的最大負載。值必須是 10 到 100 之間的整數。
7. 在 **進階設定** 下，於對應欄位中指定掃描工作的記憶體使用限制 (MB)。預設值：8192。

8. 要將此政策套用到電腦，請關閉... 掛鎖圖示並儲存變更。



效能

如何在命令列上限制記憶體和 CPU 資源使用量

在命令列上，您可以使用 一般應用程式設定中的 `UseOnDemandCPULimit` 和 `OnDemandCPULimit` 設定，為掃描工作設定 CPU 資源使用量限制。

1. 執行以下命令以啟用掃描工作的 CPU 限制：

```
kesl-control --set-app-settings UseOnDemandCPULimit = Yes
```

2. 執行以下命令以設定 CPU 限制：

```
kesl-control --set-app-settings OnDemandCPULimit =<value>
```

   限制以百分比設定；可用值為 10 到 100 之間的整數。

3. 透過管理 kesl.ini 設定檔中的 `ScanMemoryLimit` 設定，指定掃描工作的記憶體使用限制。

限制應用程式的駐留記憶體使用量

您可以限制應用程式的駐留記憶體使用量。預設情況下，限制設定為最多 50% 的記憶體，但不得少於 2 GB，且不得超過 16 GB。

如何在網頁主控台中限制常駐記憶體使用量

1. 在網頁主控台的主視窗中，選擇**資產管理 → 政策**。

2. 點擊 Kaspersky Endpoint Security 政策的名稱。

   政策內容視窗將開啟。

3. 選擇“**應用程式設定**”標籤。

4. 轉到"**一般設定**"→"**效能**"。

5. 在 **進階設定** 下，點擊 **進階設定** 連結，然後在顯示的視窗中，選取 **限制應用程式記憶體使用** 核取方塊。
   在下拉清單中，您可以選擇如何限制駐留記憶體使用：

   - **設定準確值 (%)**選擇此項後，**精確值 (%)** 欄位會變為可用，您可以在其中指定百分比值。預設值為 50%
   - **設定準確值 (MB)**選擇此項後，**精確值 (MB)** 欄位會變為可用，您可以在其中指定以 MB 為單位的值。預設值為 2000 MB。
   - **使用兩值之中最高者（% 或者 MB）**選擇此項後，**準確值 (%)** 和 **準確值 (MB)** 欄位會變為可用，您可以在其中指定必要值。
   - **使用兩值之中最低者（% 或者 MB）**選擇此項後，**準確值 (%)** 和 **準確值 (MB)** 欄位會變為可用，您可以在其中指定必要值。
   - **自動限制（建議）**選取此項目時，將自動限制駐留記憶體的使用量（預設值）。

6. 儲存變更。

若要套用變更，請在政策套用後，重新啟動受管理裝置上的 Kaspersky Endpoint Security 應用程式。

如何在命令列上限制常駐記憶體使用量

您無法在命令列上管理 `MaxMemory` 設定。使用 kesl.ini 設定檔設定常駐記憶體限制。

只有在技術支援專家的監督下並根據其指示，才建議變更預設值。

`MaxMemory` 參數可以採用下列值：

- `off` — 駐留集合大小不受限制。
- `<value>%` – RAM 的 1% 到 100% 之間的值。
- `<value>MB` – 以 MB 為單位的值。
- `lowest/<value>%/<value>MB` – 百分比值和以 MB 為單位的絕對值中較小的值。
- `highest/<value>%/<value>MB` – 百分比值和以 MB 為單位的絕對值中較大的值。
- `auto`（預設）– 自動限制。

從掃描中排除處理程序記憶體

您可以從掃描中排除所選處理程序的記憶體。

如何在網頁主控台中從掃描中排除處理程序記憶體

1. 在網頁主控台的主視窗中，選擇**資產管理 → 政策**。
2. 點擊 Kaspersky Endpoint Security 政策的名稱。
   政策內容視窗將開啟。
3. 選擇"**應用程式設定**"標籤。
4. 轉到"**一般設定**"→"**效能**"。
5. 在"**進階設定**"塊中，點擊"**設定從掃描中排除處理程序記憶體**"連接。
6. 這會開啟一個視窗；在該視窗中，點擊 **新增** 按鈕，並指定處理程序可執行檔的路徑。
   路徑要求：
7. 必須以 `/` 開頭（絕對路徑）
   a. 不得包含禁止使用的字元：
      - `\0`（空位元組）：作業系統禁止使用。
      - 檔案或目錄名稱中的斜線（`/`）：用作分隔符號。
8. 要將此政策套用到電腦，請關閉... 掛鎖圖示並儲存變更。

如何在命令列中從掃描中排除處理程序記憶體

您可以在指令列中使用`MemScanExcludedProgramPath.item_#`中的MemScanExcludedProgramPath.item_#選項配置從掃描中排除處理程序記憶體。

您可以藉助命令列開關或包含所有一般應用程式設定的設定檔來變更設定的值。

`MemScanExcludedProgramPath.item_#`包含本機目錄中處理程序的完整路徑。您可以使用遮罩來指定路徑。

您可以指定多個要排除在掃描之外的處理程序。

實用文章

如何指定遮罩

您可以使用`*`（星號）字元來建立檔案或目錄名稱遮罩。

您可以指示單一`*`字元來表示檔案或目錄名稱中`/`字元前面的任意字元集（包括空集）。例如，`/dir/*/file` 或 `/dir/*/*/file`。

您可以用兩個連續的`*`字元來表示檔案或目錄名稱中的任意一組字元（包括空集和`/`字元）。例如，`/dir/**/file*/` 或 `/dir/file**/`。

`**`遮罩在目錄名稱中只能使用一次。例如，`/dir/**/**/file`是一個不正確的遮罩。

您可以使用單一`?`字元來表示檔案或目錄名稱中的任意一個字元。

最佳化應用程式的資源消耗

網路設定

您可以設定用於互聯網連線的代理伺服器，選擇網路連接埠監控模式，並設定加密連線掃描。

如何管理代理伺服器設定

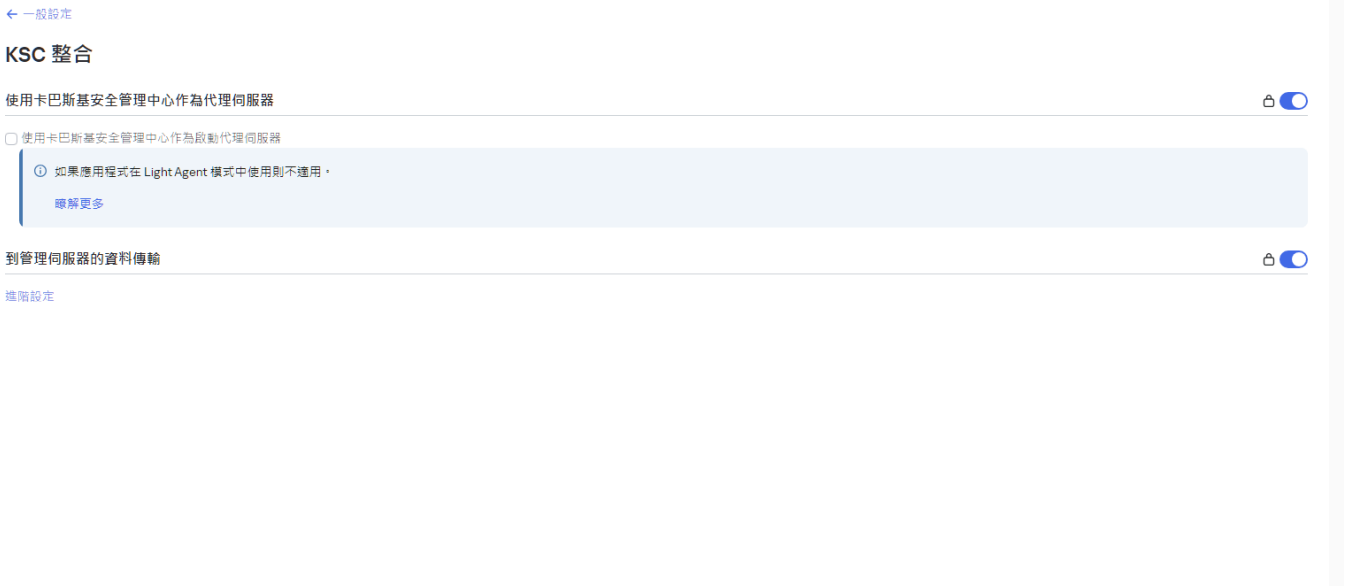
如果用戶端裝置的使用者使用代理伺服器連線到網際網路，您可以配置代理伺服器設定。Kaspersky Endpoint Security 應用程式可以使用代理伺服器連線到卡巴斯基啟動伺服器、資料庫和應用程式模組的更新來源、卡巴斯基安全網路，以及使用 Web 威脅防護元件驗證網站憑證。

預設情況下，不會使用代理伺服器。

如果您使用啟動碼在沒有網際網路存取的隔離網段中啟動裝置，則可以使用卡巴斯基安全管理中心管理伺服器作為代理伺服器，來存取卡巴斯基啟動伺服器。

如何在網頁主控台中將卡巴斯基安全管理中心設定為啟動應用程式的代理伺服器

1. 在網頁主控台的主視窗中，選擇 **資產管理** → **政策**。
2. 點擊 Kaspersky Endpoint Security 政策的名稱。
   政策內容視窗將開啟。
3. 選取“**應用程式設定**”標籤。
4. 前往 **一般設定** → **KSC 整合**區域。
5. 選擇 **使用卡巴斯基安全管理中心作為啟動用代理伺服器**核取方塊。
6. 點擊“**儲存**”按鈕。

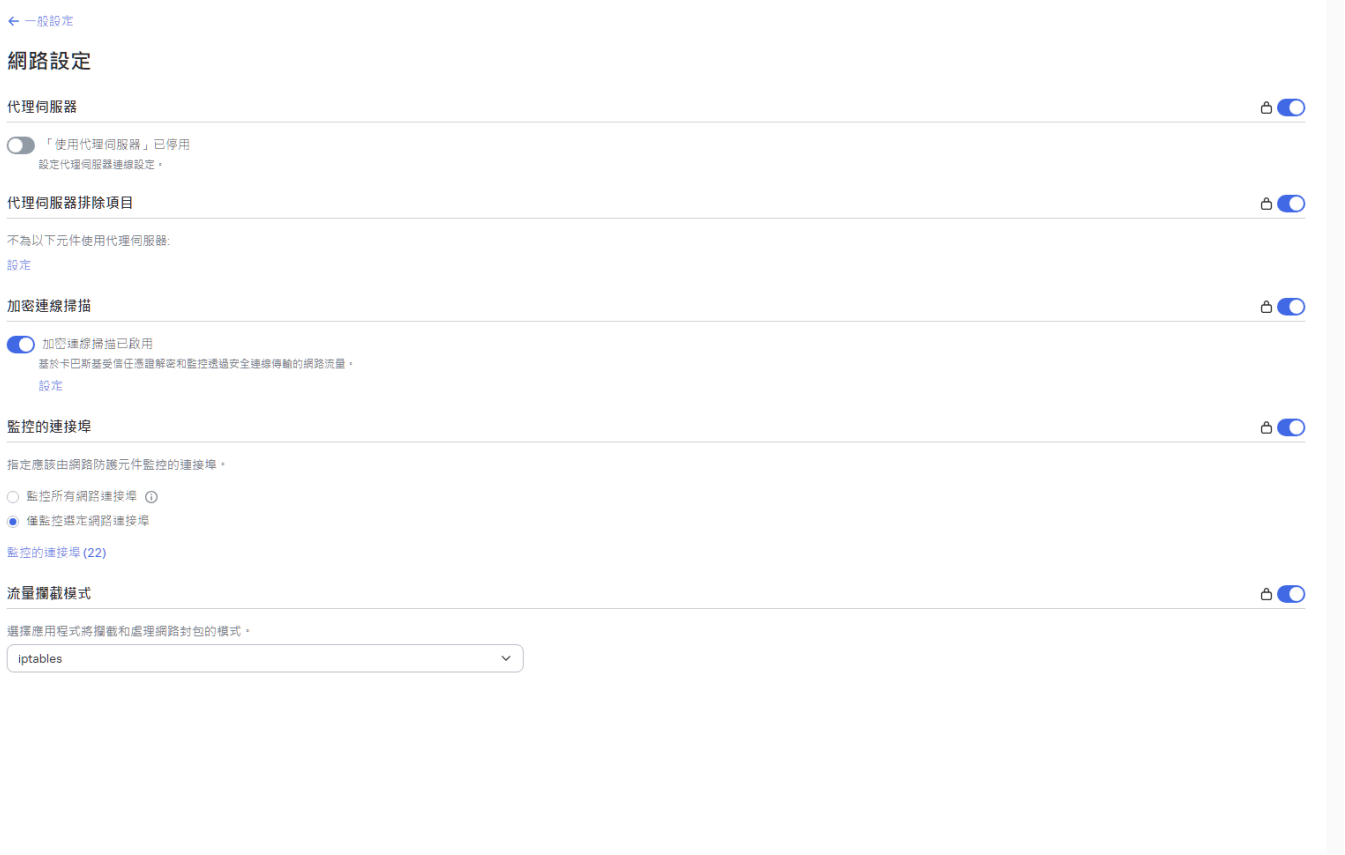


如果 Kaspersky Endpoint Security 是以 Light Agent 模式使用，則不支援使用代理伺服器連線至卡巴斯基安全網路、SVM 和 Integration Server。此外，在 Light Agent 模式下，不支援使用管理伺服器作為存取卡巴斯基啟動伺服器的代理伺服器。

如何在網頁主控台中管理代理伺服器設定

1. 在網頁主控台的主視窗中，選擇**資產管理 → 政策**。
2. 點擊 Kaspersky Endpoint Security 政策的名稱。
   政策內容視窗將開啟。
3. 選擇"**應用程式設定**"標籤。
4. 轉到 **一般設定 → 網路設定**。
5. 將切換開關設定為 **「使用代理伺服器」已啟用**。
6. 在顯示的視窗中，填寫以下欄位：
   - **代理伺服器位址**
   - **代理伺服器連接埠**
7. 如有必要，啟用代理伺服器身分驗證：
   a. 選擇"**使用代理伺服器身分驗證**"核取方塊。
   b. 填寫以下欄位：
      - **使用者名稱**
      - **密碼**

8. 儲存變更。



網路設定

如何在命令列中管理代理伺服器設定

1. 若要啟用代理伺服器的使用，請執行以下命令：

```
kesl-control --set-net-settings UseProxy=Yes ProxyServer=<proxy server address>
```

2. 若要檢查網路設定的目前值，請執行下列命令：

```
kesl-control --get-net-settings
```

符號

命令選項

設定	描述
ProxyServer	用於連線網際網路的代理伺服器位址。 代理伺服器位址採用以下格式之一： • [<connection protocol>://]<address of the proxy server>:<port>，如果連線到代理伺服器不需要身分驗證； • [<connection protocol>://][<user name>:[<password>]@]<address of the proxy server>:<port>，如果連線到代理伺服器需要身分驗證。指定 IPv6 位址時，請將其輸入方括號中。 不支援透過 HTTPS 連線到代理伺服器。 透過 HTTP 代理連線時，我們建議使用不用於登入其他系統的單獨帳戶。HTTP 代理程式使用不安全的連線，帳戶可能會受到損害。

代理伺服器排除

如果您不需要對某些位址的連線使用代理伺服器，可以將這些位址新增至排除項目。

您也可以針對 EDR Expert (on-premises)、NDR (KATA) 和沙盒元件停用代理伺服器使用，這些元件提供與 Detection and Response 解決方案整合。連線至這些元件的 Integration Server 時，將不會使用代理伺服器。

如何在網頁主控台中配置代理伺服器排除項目

1. 在網頁主控台的主視窗中，選擇**資產管理 → 政策**。
2. 點擊 Kaspersky Endpoint Security 政策的名稱。
   政策內容視窗將開啟。
3. 選擇"**應用程式設定**"標籤。
4. 轉到 **一般設定 → 網路設定**。
5. 在"**代理伺服器排除項目**"塊中，點擊"**設定**"連接。
   這會開啟代理伺服器排除視窗
6. 選取您不想使用代理伺服器的元件核取方塊：
   - **Endpoint Detection and Response Expert (on-premises)**
   - **KATA Sandbox**
   - **Network Detection and Response (KATA)**
7. 新增您不想使用代理伺服器的 IP 位址。範例：`1.2.3.4/24`、`1234::cdef/96`。
8. 儲存變更。

如何在命令列中配置代理伺服器排除項目

1. 若要新增您不想使用代理伺服器的位址，請執行以下命令：

```
kesl-control --set-net-settings ProxyBypass=<address:port>
```

2. 若要對與卡巴斯基 Detection and Response 解決方案的整合繞過代理伺服器，請執行以下命令：

```
kesl-control --set-net-settings [ProxyBypassEdr=<Yes|No>] [ProxyBypassNdr=<Yes|No>] [ProxyBypassSandbox=
<Yes|No>]
```

3. 若要檢查網路設定的目前值，請執行下列命令：

```
kesl-control --get-net-settings
```

符號

設定	描述
`ProxyBypass`	要繞過代理伺服器的位址清單。 位址以 `<address>[:<port>]` 格式指定。若要指定位址，您可以使用遮罩（`*` 符號）以及 `\` 符號後面的註釋。
`ProxyBypassEdr`	連線到 Kaspersky Endpoint Detection and Response Expert (on-premises) Integration Server 時是否使用代理伺服器。預設情況下，不會使用代理伺服器（`No`）。
`ProxyBypassNdr`	連線到 Kaspersky Network Detection and Response (KATA) Integration Server 時是否使用代理伺服器。預設情況下，不會使用代理伺服器（`No`）。
`ProxyBypassSandbox`	連線到提供與 Sandbox 互動的伺服器時是否使用代理伺服器。預設情況下，不會使用代理伺服器（`No`）。

應用程式如何攔截流量

應用程式可以採用以下兩種網路流量攔截模式之一：eBPF 或 iptables。預設選取 iptables 模式。

此設定不適用於配備 Elbrus CPU 的裝置。

關於 eBPF 網路流量攔截

在 eBPF 模式下，應用程式會建立自己獨立的網路命名空間（network linux namespace），在其中使用與本機網路介面的 `tc`（linux traffic control）佇列關聯的 eBPF 程式重新導向網路封包。重定向的網路流量然後會被根據活動的網路工作進行分析，然後被返回到原始網路介面。

為了在命名空間之間進行通訊，使用成對的 `veth` 虛擬網路介面（每對的每一端都在其自己的網路命名空間中）：

- `kesl_in - kesl_worm_in` 配對會傳輸入站連線的網路流量。
- `kesl_out - kesl_worm_out` 配對會傳輸出站連線的網路流量。

透過這些介面對，網路流量被從預設命名空間傳送到應用程式建立的命名空間進行掃描，並透過相同的接口，流量在分析後被返回。

只有當應用程式正在執行且網路攔截被啟用時，網路流量才能從系統中的其他網路介面到達這些介面。這些介面不能用於遠端裝置之間的網路資料傳輸。

關於 iptables 網路流量攔截

在 iptables 模式下，會使用 tproxy 核心機制執行攔截。

系統會在 mangle 表格的 PREROUTING 鏈中建立對應規則，將流量轉送到應用程式開啟的特殊連接埠。應用程式也會將額外規則新增至作業系統防火牆的各種表格，以便將封包轉送至 tproxy。應用程式的網路攔截器位於用戶端與伺服器之間，並分別與兩者建立個別連線，掃描並傳輸兩者之間的流量。

攔截到的入站與出站連線會以不同標籤標記，您可以在 kesl.ini 設定檔中變更這些標籤。

對於出站連線，系統會引入額外的路由規則，將攔截的連接埠的出站流量重新導向至 tproxy 中的回送介面。

選取流量攔截模式

如何在網頁主控台中選取網路流量攔截模式

1. 在網頁主控台的主視窗中，選擇**資產管理 → 政策**。
2. 點擊 Kaspersky Endpoint Security 政策的名稱。
   政策內容視窗將開啟。
3. 選擇"**應用程式設定**"標籤。
4. 轉到"**一般設定**"→"**網路設定**"。
5. 在 **流量攔截模式** 下，選取應用程式的流量攔截模式：
   - **iptables**預設選取。應用程式會使用 iptables 工具攔截流量。
   - **eBPF**應用程式會使用 eBPF 技術攔截流量。
6. 要將此政策套用到電腦，請關閉... 掛鎖圖示並儲存變更。

如何在命令列中選取網路流量攔截模式

1. 執行以下指令：

```
kesl-control --set-net-settings NetInterceptorMode=<UseEBPF|UseIPTables>
```

2. 若要檢查網路設定的目前值，請執行下列命令：

```
kesl-control --get-net-setting
```

特殊考量與限制

- 若要變更流量攔截模式，需要重新啟動應用程式。重新啟動會中斷已建立的網路連線。
- 如果應用程式無法使用 eBPF 模式攔截網路流量，則會改用 iptables 模式。

如何設定憑證驗證政策

網路流量掃描設定由 Web 威脅防護、網路威脅防護、郵件威脅防護和 Web 控制使用。

預設情況下，Web 威脅防護會解密並掃描透過加密連線傳送的網路流量。為了實現這一點，應用程式會驗證整個憑證鏈。

憑證驗證政策包含以下設定：

- 驗證方法（本機或透過網際網路）
- 存取含有不受信任憑證的網站
- 存取發生憑證驗證錯誤的網站

如果裝置沒有直接的網際網路連線，您可以選擇本機憑證驗證方法。

預設情況下，應用程式允許與具有不受信任憑證的網域建立網路連線。應用程式會顯示一個 HTML 頁面，上有警告以及不建議存取相關網域的原因資訊（請見下圖）。使用者可以點擊 HTML 警告頁面中的連結來獲取對所請求 Web 資源的存取權限。

如果協力廠商應用程式或服務與具有不受信任憑證的網域建立連線，應用程式將建立自己的憑證來掃描流量。新憑證的狀態為"*不受信任*"。這對於警告協力廠商應用程式關注不受信任的連線很有必要，因為在此情況下無法顯示 HTML 頁面，連線可以在背景模式中建立。

憑證驗證可能會以錯誤結束。例如，在使用雲端儲存或驗證自我簽署的憑證時。預設情況下，應用程式會將此類網站的網域名稱新增至排除項目，並且在存取此網域時不會控制加密的網路流量。應用程式還會為加密連線掃描錯誤產生一個事件。

> 您只能在應用程式的本機介面中檢視具有加密連線掃描錯誤的網域清單。

如何在網頁主控台中設定憑證驗證政策

1. 在網頁主控台的主視窗中，選擇**資產管理** → **政策**。
2. 點擊 Kaspersky Endpoint Security 政策的名稱。
   政策內容視窗將開啟。
3. 選擇"**應用程式設定**"標籤。
4. 轉到"**一般設定**"→"**網路設定**"。
5. 在 **加密連線掃描** 下，確保撥動開關位於 **加密連線掃描已啟用** 位置。
   如果撥動開關已停用，Kaspersky Endpoint Security 將無法存取位址以 `https://` 開頭的網站內容。
6. 點擊 **設定** 連結並設定憑證驗證政策：
   - **正在造訪具有不受信任憑證的網域**遇到不受信任的憑證時的操作
     - **允許連線**應用程式允許連線到具有不受信任憑證的網域。應用程式會顯示一個 HTML 頁面，上有警告以及不建議存取相關網域的原因資訊（請見下圖）。使用者可以點擊 HTML 警告頁面中的連結來獲取對所請求 Web 資源的存取權限。
     - **封鎖連線**存取具有不受信任憑證的網域時，Kaspersky Endpoint Security 會封鎖網路連線，並顯示一個 HTML 頁面，其中顯示該網域遭封鎖的原因。

- **造訪包含加密連線掃描錯誤的網域**發生加密連線掃描錯誤時的操作：
  - **允許並新增網域至排除項目**發生加密連線掃描錯誤時，應用程式會將導致錯誤的網域新增至排除清單，並且在存取此網域時不監控加密網路流量。
  - **封鎖連線**發生加密連線掃描錯誤時，Kaspersky Endpoint Security 會封鎖網路連線。
- **憑證驗證政策**應用程式驗證憑證的方式：
  - **完整檢查**應用程式使用網際網路來檢查並下載驗證憑證所需的缺少憑證鏈。
  - **本機檢查**應用程式會在電腦本機上驗證憑證。

7. 要將此政策套用到電腦，請關閉... 掛鎖圖示並儲存變更。

如何在命令列中設定憑證驗證政策

1. 若要啟用加密連線掃描，請執行下列命令：

```
kesl-control --set-net-settings EncryptedConnectionsScan=Yes
```

2. 若要選取憑證驗證方法，請執行下列命令：

```
kesl-control --set-net-settings CertificateVerificationPolicy=<FullCheck|LocalCheck>
```

3. 若要選取發現不受信任的憑證時要採取的操作，請執行下列命令：

```
kesl-control --set-net-settings UntrustedCertificateAction=<Allow|Block>
```

4. 若要選取加密連線掃描期間發生錯誤時要採取的操作，請執行下列命令：

```
kesl-control --set-net-setting EncryptedConnectionsScanErrorAction=<AddToAutoExclusions|Disconnect>
```

5. 若要檢查網路設定的目前值，請執行下列命令：

```
kesl-control --get-net-setting
```

符號

命令選項

設定	描述
`EncryptedConnectionsScan`	加密連線掃描模式： `Yes`（預設）。已啟用加密連線掃描。 `No`。加密連線掃描已停用。
`CertificateVerificationPolicy`	憑證驗證政策： `FullCheck`（預設）。應用程式使用網際網路來檢查並下載驗證憑證所需的缺少憑證鏈。 `LocalCheck`。應用程式會在電腦本機上驗證憑證。

設定	描述
`UntrustedCertificateAction`	遇到不受信任的憑證時的操作 `Allow`（預設）。應用程式允許連線到具有不受信任憑證的網域。應用程式會顯示一個 HTML 頁面，上有警告以及不建議存取相關網域的原因資訊（請見下圖）。使用者可以點擊 HTML 警告頁面中的連結來獲取對所請求 Web 資源的存取權限。 `Block`。如果選取此選項，當存取具有不受信任憑證的網域時，Kaspersky Endpoint Security 將封鎖網路連線。在瀏覽器中開啟具有未受信任憑證的網域時，Kaspersky Endpoint Security 會顯示一個 HTML 頁面，其中顯示封鎖該網域的原因。
`EncryptedConnectionsScanErrorAction`	發生加密連線掃描錯誤時的操作： `AddToAutoExclusions`（預設）。發生加密連線掃描錯誤時，應用程式會將導致錯誤的網域新增至排除清單，並且在存取此網域時不監控加密網路流量。 `Disconnect`。發生加密連線掃描錯誤時，Kaspersky Endpoint Security 會封鎖網路連線。

如何配置受監控的連接埠

Kaspersky Endpoint Security 執行時，網路威脅防護元件會監控透過某些網路連接埠傳輸的資料。應用程式監控的網路連接埠清單是根據卡巴斯基專家的建議進行配置。

行為偵測和 弱點利用防禦元件還會監控可能威脅電腦安全之應用程式處理程序的網路連接埠。應用程式透過病毒資料庫獲取有關此類處理程序的資訊。

您可以配置要讓應用程式監控的連接埠：

- **監控所有網路連接埠**在此網路連接埠監控模式下，應用程式會監控通過電腦任何開放網路連接埠的資料流。

  指定此值可能會顯著增加作業系統負載。

- **僅監控選定網路連接埠**在此網路連接埠監視模式下，防護元件將監控電腦的選定連接埠和選定應用程式的網路活動。

如果要攔截到 NFS 伺服器的網路連線，則需要確保 NFS 伺服器以 `insecure` 選項啟動（以便接受來自 1–1024 範圍之外的連接埠的連線），否則 NFS 伺服器可能會拒絕此類連線。

如何在網頁主控台中配置受監控的連接埠

1. 在網頁主控台的主視窗中，選擇**資產管理 → 政策**。
2. 點擊 Kaspersky Endpoint Security 政策的名稱。
   政策內容視窗將開啟。
3. 選擇“**應用程式設定**”標籤。
4. 轉到 **一般設定 → 網路設定**。
5. 在 **監控的連接埠** 下，選擇應用程式連接埠監控模式：
   - **監控所有網路連接埠**
   - **僅監控選定網路連接埠**（預設值）。

6. 如果您選擇 **僅監控選定網路連接埠** 選項，請配置要監控的連接埠清單：

   a. 點擊"**監控的連接埠**"連接。

   b. 編輯受監控連接埠清單。

   > 若要郵件威脅防護元件正常運作，必須在網路設定中監控網路連接埠 25、110、143、465、587、993 和 995。這些網路連接埠預設已被新增至受監控連接埠清單。從清單中移除這些連接埠可能會導致元件無法正常運作。

7. 儲存變更。

如何在命令列中配置受監控的連接埠

1. 若要選擇連接埠監控模式，請執行以下命令：

```
kesl-control --set-net-settings MonitorNetworkPorts=<All|Selected>
```

2. 如果您選擇僅監控選定的連接埠 (`MonitorNetworkPorts=Selected`)，請指定要監控的連接埠清單：

```
kesl-control --set-net-settings NetworkPorts.item_#.PortName=<port name> NetworkPorts.item_#.Port=<port number>
```

   若要從監控清單中移除連接埠，請使用設定檔編輯該清單。

3. 若要檢查網路設定的目前值，請執行下列命令：

```
kesl-control --get-net-settings
```

符號

命令選項

設定	描述
`MonitorNetworkPorts`	`Selected`（預設值）— 僅監控 `[NetworkPorts.item_#]` 部分中指定的網路連接埠（請參閱下方）。 `All` — 監控所有網路連接埠。 指定此值可能會顯著增加作業系統負載。
`PortName`	網路連接埠描述。
`Port`	應用程式要監控的網路連接埠號碼。可能的值：`1 – 65535`。 若要郵件威脅防護元件正常運作，必須在網路設定中監控網路連接埠 25、110、143、465、587、993 和 995。這些網路連接埠預設已被新增至受監控連接埠清單。從清單中移除這些連接埠可能會導致元件無法正常運作。

使用作業系統工具設定流量攔截排除項目

在 Kaspersky Endpoint Security 設定中，您可以依流量方向、目的地 IP 位址和連接埠設定流量攔截排除。如果這類排除不足以解決 Kaspersky Endpoint Security 應用程式與用戶端應用程式之間的衝突，您可以使用特殊的允許規則鏈 kesl_bypass。

kesl_bypass 鏈是 Kaspersky Endpoint Security 在作業系統防火牆 (iptables/ip6tables) 的 mangle 表中建立的特殊規則清單。kesl_bypass 鏈的規則可讓流量排除在 Kaspersky Endpoint Security 攔截之外。kesl_bypass 鏈會新增到網路封包處理程序的最前端，這表示 kesl_bypass 規則會在所有其他 iptables 規則之前處理。

與您可以在 Kaspersky Endpoint Security 設定中啟用的排除不同，kesl_bypass 鏈不僅允許依流量方向、目的地 IP 位址和連接埠設定排除，也可依連線的其他參數設定排除。

kesl_bypass 鏈中的規則可以透過作業系統方式變更。

例如，您可以執行以下命令，將規則新增至 kesl_bypass 鏈：

```
iptables -t mangle -I kesl_bypass -m tcp -p tcp --dport http -j ACCEPT
```

此規則可讓任何 IP 位址上連接埠 80 的傳入和傳出 HTTP 流量排除在 Kaspersky Endpoint Security 攔截之外。這有助於避免與您信任的 Web 服務發生潛在衝突。

如果在鏈中設定了流量排除規則，這些規則會影響 Web 威脅防護、網路威脅防護 和 Web 控制 元件。

移除應用程式時，只有在 kesl_bypass 規則鏈為空時，才會將其從 iptables 和 ip6tables 中移除。

攔截檔案操作

檔案操作攔截模式會影響 檔案威脅防護與 裝置控制元件、物件的執行防禦動作，以及 卸除式磁碟機掃描工作。

如果已啟用檔案操作攔截的封鎖模式

- 在掃描期間，應用程式可以阻止對檔案威脅防護元件正在掃描的檔案的存取。如果掃描未偵測到檔案中存在威脅，應用程式將允許存取該檔案。偵測到受感染的物件時，應用程式會執行檔案威脅防護元件的 **偵測到威脅後的動作** (`ActionOnThreat`) 設定中指定的動作。
- 當裝置控制元件決定是否可以授予對裝置的存取權限時，應用程式可以阻止對裝置上的檔案的存取。如果掃描後裝置控制允許存取包含檔案的裝置，則應用程式允許存取檔案。
- 在物件執行防護判斷是否可執行裝置上的檔案時，應用程式可能會封鎖這些檔案。如果掃描結果顯示物件執行防護允許執行這些檔案，應用程式便會允許其執行。
- 掃描期間，應用程式可能會封鎖對卸除式磁碟機上檔案的存取。如果掃描未偵測到檔案中存在威脅，應用程式將允許存取該檔案。偵測到受感染的物件時，應用程式會執行檔案威脅防護元件的 **偵測到威脅後的動作** (`ActionOnThreat`) 設定中指定的動作。

如果已停用檔案操作攔截的封鎖模式

- 無論選取哪種運作模式，檔案威脅防護元件均以通知模式運作，允許存取檔案並以非同步方式執行掃描。
- 無論選取哪種運作模式，裝置控制元件均以通知模式運作，且一律允許存取裝置。

- 無論選取哪種運作模式，物件執行防護動作均以通知模式運作，且一律允許執行物件。
- 應用程式一律允許存取卸除式磁碟機上的檔案，並以非同步方式執行掃描。

此檔案操作攔截模式在掃描期間對系統效能的影響較小，但檔案中的威脅可能無法被解毒或刪除。如果在掃描期間，與此檔案關聯的程序在應用程式判定此檔案狀態之前成功重新命名該檔案，則可能會發生這種情況。

預設會啟用檔案操作攔截封鎖模式。

如何在網頁主控台中設定檔案操作攔截模式

1. 在網頁主控台的主視窗中，選擇**資產管理** → **政策**。
2. 點擊 Kaspersky Endpoint Security 政策的名稱。
   政策內容視窗將開啟。
3. 選擇"**應用程式設定**"標籤。
4. 轉到 **一般設定** → **偵測設定**。
5. 在 **檔案操作攔截模式**下，清除或選取 **掃描期間封鎖對檔案的存取**核取方塊。預設情況下已選擇此核取方塊。
6. 儲存變更。

如何在命令列中設定檔案操作攔截模式

您可以使用`FileBlockDuringScan`中的FileBlockDuringScan設定在指令列中配置檔操作攔截模式。

若要選取檔案操作攔截模式，請執行以下命令：

```
kesl-control --set-app-settings FileBlockDuringScan=<Yes|No>
```

符號

命令選項

設定	描述
`FileBlockDuringScan`	`Yes`（預設值），用於在檔案正由 檔案威脅防護與 裝置控制元件、執行防禦動作，以及 卸除式磁碟機掃描工作掃描時，封鎖對檔案的存取。 `No`則允許在掃描期間存取檔案。允許對任何檔案的請求，掃描非同步完成。

設定系統事件攔截

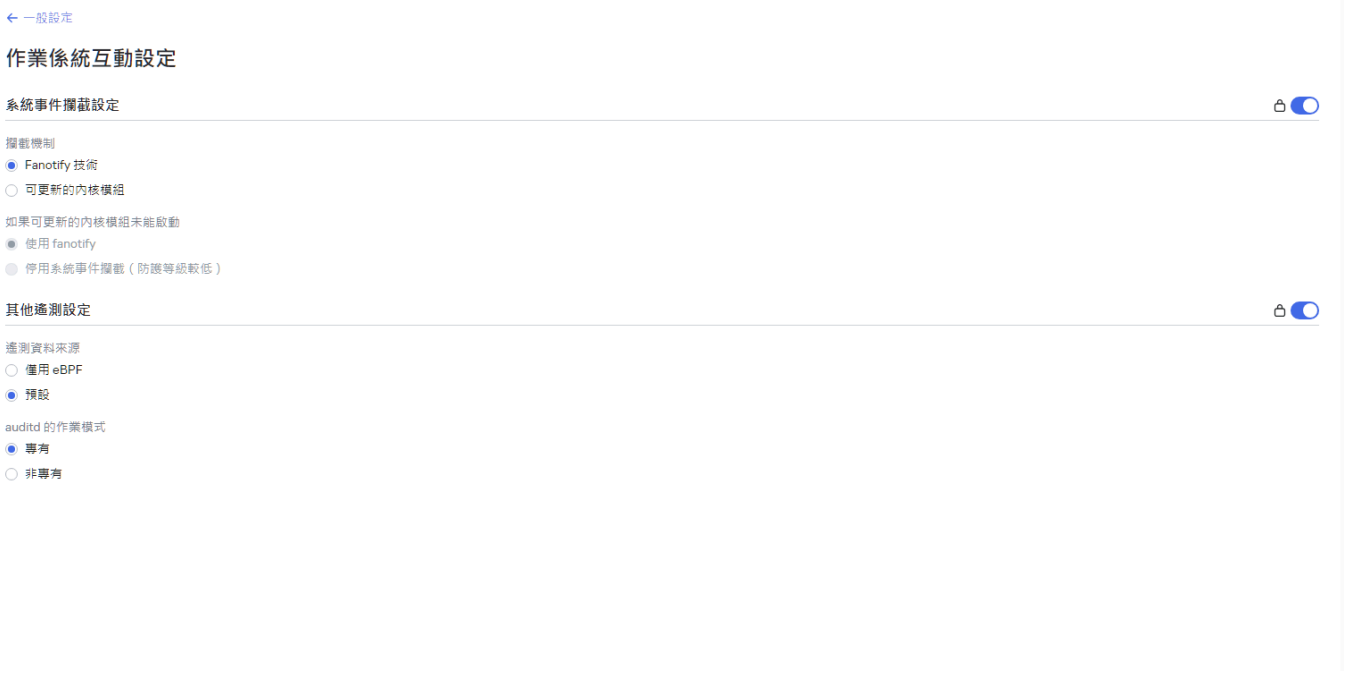
您可以在網頁主控台、命令列或管理主控台中選擇系統事件攔截機制。

只有在作業系統支援 fanotify 技術的裝置上，才能管理系統事件攔截的設定。

設定系統事件攔截不適用於配備 Elbrus CPU 的裝置。

如何在網頁主控台中設定系統事件攔截機制

1. 在網頁主控台的主視窗中，選擇**資產管理 → 政策**。
2. 點擊 Kaspersky Endpoint Security 政策的名稱。
   政策內容視窗將開啟。
3. 選擇“**應用程式設定**”標籤。
4. 前往**一般設定 → 作業系統互動設定**。
5. 在**系統事件攔截設定**下，選擇系統事件攔截機制：
   - **Fanotify 技術**
   - **可更新的內核模組**如果選取此選項，請選擇當可更新的內核模組無法啟動時應用程式將執行的動作：
     - **使用 fanotify**
     - **停用系統事件攔截（防護等級較低）**



作業系統互動設定

如何在命令列中設定系統事件攔截機制

1. 若要選擇系統事件攔截機制，請執行以下指令：

```
kesl-control --set-app-settings InterceptorMode=<UseFanotify|UseUpdatableKernelModule>
```

2. 若要設定當可更新的內核模組無法啟動時應用程式將執行的動作，請執行以下指令：

```
kesl-control --set-app-settings InterceptorFallbackStrategy=<FallbackToFanotify|FallbackToLimitedMode>
```

3. 若要讓應用程式在可更新的內核模組無法啟動時重新啟動，請執行以下指令：

```
kesl-control --set-app-settings InterceptorApplyStrategy=<RestartServiceAutomatically|RestartServiceManually>
```

4. 若要檢查目前的應用程式設定，請執行下列指令：

```
kesl-control --get-app-settings [--json]
```

符號

命令選項

設定	描述
`InterceptorMode`	`UseFanotify`（預設）– 使用 fanotify 技術攔截系統事件。 `UseUpdatableKernelModule` – 使用可更新內核模組攔截系統事件。
`InterceptorFallbackStrategy`	`FallbackToFanotify`（預設）– 切換到 fanotify 進行系統事件攔截。 `FallbackToLimitedMode` – 不使用系統事件攔截。如果應用程式不使用系統事件攔截，則不會執行即時檔案掃描，並且裝置的保護等級會降低。
`InterceptorApplyStrategy`	`RestartServiceAutomatically` 會自動重新啟動應用程式，以啟動可更新的內核模組。建議使用此設定。 `RestartServiceManually`（預設）會在使用者手動重新啟動應用程式後，啟動可更新的內核模組。

> 如果作業系統符合安裝可更新的內核模組的要求，則應用程式可以使用基於可更新的內核模組的攔截機制。

如果您選擇了基於可更新的內核模組的攔截機制，則可以配置在可更新的內核模組啟動而模組沒有啟動時時發生錯誤的應用程式的行為。在此情況下，應用程式可回退到 fanotify 或停用系統事件攔截。

如果在安裝應用程式期間無法安裝可更新的內核模組，您可以稍後在您的作業系統可獲得支援時安裝。為此，請執行以下操作：

1. 更新應用程式資料庫和模組。可更新的內核模組會作為常規更新過程的一部分進行安裝。
2. 根據可更新的內核模組選擇攔截機制。

應用程式可以在以下情況下切換到使用可更新的內核模組：

- 在應用程式設定中，您已將攔截系統事件的機制變更為可更新的內核模組。
- 在未啟動可更新內核模組的裝置上，資料庫和模組更新引入了支援可更新的內核模組的更新。

有關可更新的內核模組狀態的資訊

關於可更新的內核模組狀態和可用性的資訊以狀態形式顯示：

- **執行中** 表示模組已安裝並正在執行。
- **已停止** 表示模組已安裝但未執行。

- **不可用** 表示裝置不支援此模組。
- **故障** 表示啟動模組時發生錯誤，且模組未執行。

您可以在網頁主控台和命令列中檢視裝置上可更新的內核模組的狀態。

如何在網頁主控台中檢視可更新的內核模組的狀態

1. 在網頁主控台的主視窗中，選取 **資產管理 → 資產 (裝置)**。
   受管理裝置的清單將開啟。
2. 選擇包含必要裝置的管理群組。若要選取巢狀群組，請按一下視窗上方的 **顯示階層結構** 按鈕。
   此清單僅顯示選定管理群組的受管理裝置。
3. 按一下裝置名稱。
4. 這將開啟受管理裝置屬性視窗；在該視窗中，轉到**應用程式**索引標籤。
5. 在裝置上安裝的應用程式清單中，點擊 Kaspersky Endpoint Security。
6. 檢視 **可更新的內核模組** 功能元件的狀態。

如何在命令列中檢視可更新的內核模組的狀態

若要檢視可更新的內核模組的狀態，請執行以下命令：

```
kesl-control --app-info [--json]
```

其中 `--json` 表示以 JSON 格式輸出資料。如果不指定`--json`選項，設定將被輸出到主控台。

使用可更新的內核模組時的「安全」模式

若應用程式在使用可更新的內核模組時不穩定，在達到指定的異常停止次數上限後，應用程式會自動切換到「安全」模式（在 kesl.ini 設定檔中設定 `SafeMode=yes` ）。預設情況下，應用程式會在發生三次異常停止後進入「安全」模式。異常停止次數上限在 kesl.ini 設定檔的 `PanicThreshold` 設定中進行設定。

若應用程式在「安全」模式下執行，則不會啟動可更新的內核模組，並且應用程式會切換到 fanotify 來攔截系統事件。應用程式會將 `UpdatableKernelModule=Error` 標籤傳送到卡巴斯基安全管理中心。

若要在解決應用程式問題後繼續使用可更新的內核模組，需停用「安全」模式。

如何在命令列中停用應用程式的安全模式

1. 開啟 /var/opt/kaspersky/kesl/common/kesl.ini 檔案進行編輯。
2. 在 `[General]` 區域中，設定 `SafeMode=no`。
3. 重新啟動 Kaspersky Endpoint Security：

   ```
   systemctl restart kesl
   ```

安全模式已停用。

管理其他遙測設定

您可以管理與 Detection and Response 解決方案整合時，用於收集傳送到此類解決方案的遙測資料的進階設定：

- 遙測來源。您可以使用 eBPF 技術和 auditd 服務獲取遙測資料，也可以單獨使用 eBPF 技術。
- auditd 服務的模式。Kaspersky Endpoint Security 可以在獨佔模式或群播模式下使用 auditd 服務。

如何在網頁主控台中設定其他遙測設定

1. 在網頁主控台的主視窗中，選擇**資產管理 → 政策**。
2. 點擊 Kaspersky Endpoint Security 政策的名稱。
   政策內容視窗將開啟。
3. 選擇"**應用程式設定**"標籤。
4. 轉到"**一般設定**"→"**作業系統互動設定**"。
5. 在 **遙測設定** 下，指定 Kaspersky Endpoint Security 用來收集遙測資料的來源：
   - **僅使用 eBPF**表示僅使用 eBPF 技術獲取遙測資料。

     > 如果選取 **僅使用 eBPF** 選項，Detection and Response 解決方案的遙測可能會受到限制。

   - **預設**表示使用 eBPF 技術和 auditd 服務來取得遙測資料。
6. 另請指定 auditd 服務的模式：
   - **獨佔**表示 Kaspersky Endpoint Security 以獨佔模式使用 auditd 服務。
   - **非獨佔**表示 auditd 服務以非獨佔模式使用。

     > 只有在 **遙測來源** 設定為 **預設** 時，才會套用此設定。

7. 要將此政策套用到電腦，請關閉... 掛鎖圖示並儲存變更。

如何在命令列上設定其他遙測設定

在命令列上，您可以使用 行為偵測 預定義工作的 `TelemetrySource` 和 `UseTelemetryMonopolyMode` 設定來管理其他遙測設定。

1. 若要啟用遙測來源，請執行以下指令：

```
kesl-control --set-settings 20 TelemetrySource=<Default|OnlyEBPF>
```

2. 若要為 auditd 服務選取模式，請執行以下指令：

```
kesl-control --set-settings 20 UseTelemetryMonopolyMode=<True|False>
```

符號

命令選項

設定	描述
`TelemetrySource`	`Default`（預設）表示使用 eBPF 技術和 auditd 服務來獲取遙測資料。 `OnlyEBPF` 表示僅使用 eBPF 技術獲取遙測資料。
`UseTelemetryMonopolyMode`	`True`（預設值）表示 Kaspersky Endpoint Security 以獨佔模式使用 auditd 服務。 `False` 表示 auditd 服務以非獨佔模式使用。 僅當 `TelemetrySource` 被設定為 `Default` 時，`UseTelemetryMonopolyMode` 設定才會套用。

備份

如果 Kaspersky Endpoint Security 在掃描受防護裝置時偵測到檔案中的惡意程式碼，應用程式會封鎖該檔案、將其指派為*已感染*狀態、將副本放入備份副本並嘗試對檔案進行解毒。

*備份*會保留在解毒過程中被刪除或修改的檔案的備份副本。*備份副本*在解毒或刪除檔案之前建立。檔案的備份副本以特定格式儲存並且不會帶來威脅。

有時在解毒過程中無法保持檔案的完整性。如果在解毒病毒後，您部分或完全無法存取已解毒檔案中的重要資訊，則可以嘗試從備份副本中還原該檔案。

還原感染物件可能會導致裝置感染。

備份檔案備份副本可能包含個人資料。存取備份物件需要 root 權限。

配置備份設定

您可以在網頁主控台、管理主控台或使用命令列管理裝置上的備份設定。您可配置以下備份設定：

- **備份中物件的儲存時間。**預設情況下，物件保留 30 天。最長儲存期限超出後，Kaspersky Endpoint Security 將刪除備份區中最舊的檔案。
- **最大備份大小。**預設會配置以下最大備份大小：
  - 若未套用政策，則為 0 MB
  - 若套用政策，則為 1024 MB

為避免超過最大儲存大小，當達到最大儲存大小時，Kaspersky Endpoint Security 將自動刪除儲存中的最早檔案。

- **儲存備份和 隔離區物件的目錄路徑**（只能在命令列中配置）。預設情況下，/var/opt/kaspersky/kesl/common/objects-backup/ 目錄用於儲存檔案的備份副本和隔離的檔案。

如何在網頁主控台中配置備份設定

若要在政策屬性中管理備份設定：

1. 在網頁主控台的主視窗中，選擇**資產管理 → 政策**。
2. 點擊 Kaspersky Endpoint Security 政策的名稱。

   政策內容視窗將開啟。
3. 選擇"**應用程式設定**"標籤。
4. 前往 **一般設定 → 報告和儲存** 區域。
5. 在 **備份** 區域中，配置以下設定：
   - **以下時間後刪除物件 (天)**如果選中該核取方塊，則最大檔案儲存期限制為定義的時間間隔。預設情況下已選擇此核取方塊。

     有效值為 0 到 10000。
   - **備份大小限制為 (MB)**如果選中該核取方塊，則最大儲存大小限制為定義值。預設情況下已選擇此核取方塊。

     有效值為 1 到 4000。
6. 要將此政策套用到電腦，請關閉... 掛鎖圖示並儲存變更。

若要在受管理裝置的屬性中管理備份設定：

1. 在網頁主控台的主視窗中，選取 **資產管理 → 資產（裝置）**。

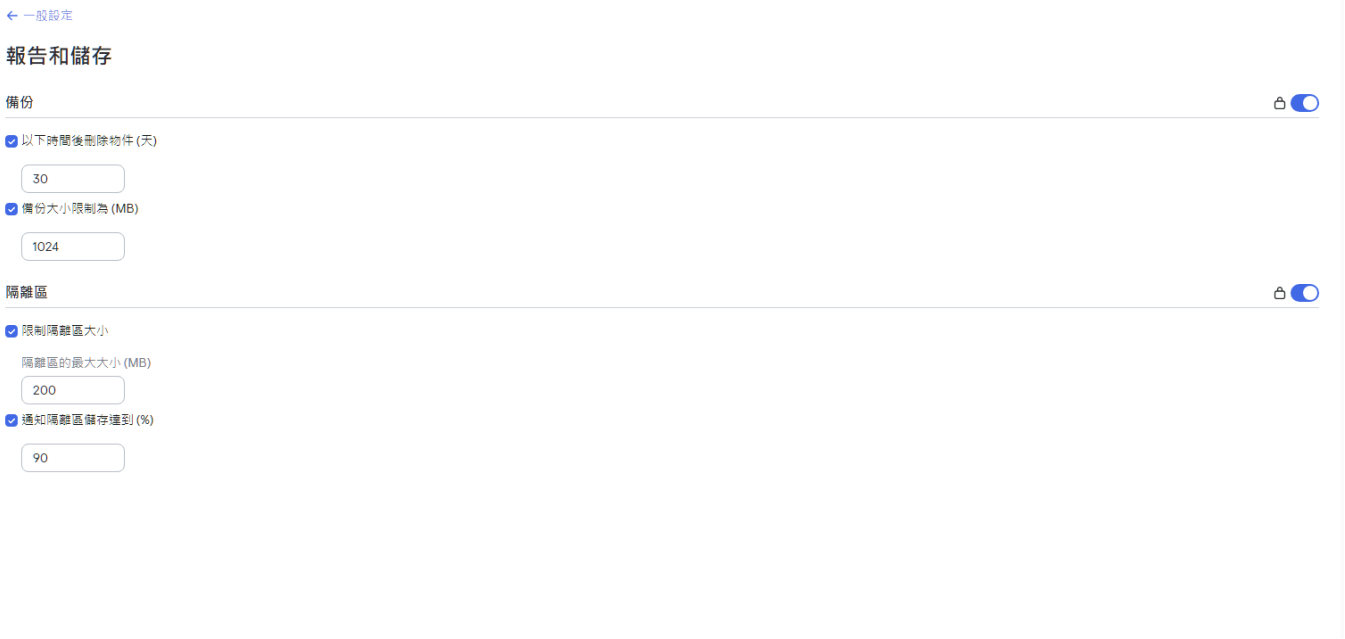
   受管理裝置的清單將開啟。
2. 選擇包含必要裝置的管理群組。若要選取巢狀群組，請按一下視窗上方的 **顯示階層結構** 按鈕。

   此清單僅顯示選定管理群組的受管理裝置。
3. 按一下裝置名稱。
4. 這將開啟受管理裝置屬性視窗；在該視窗中，轉到**應用程式**索引標籤。
5. 選取 Kaspersky Endpoint Security
6. 前往 **應用程式設定 → 儲存設定**。
   - **以下時間後刪除物件 (天)**如果選中該核取方塊，則最大檔案儲存期限制為定義的時間間隔。預設情況下已選擇此核取方塊。

     有效值為 1 到 10000。
   - **備份大小限制為 (MB)**如果選中該核取方塊，則最大儲存大小限制為定義值。預設情況下已選擇此核取方塊。

     有效值為 1 到 4000。

7. 儲存變更。



報告和儲存

如何在命令列中配置備份

在指令列中，您可以使用一般應用程式設定中的`BackupDaysToLive,`、`BackupSizeLimit`和`QuarantineBackupFolder`設定來配置備份設定。

1. 若要配置備份中物件的保留期間，請執行以下指令：

```
kesl-control --set-app-settings BackupDaysToLive=<days>
```

2. 若要配置備份的大小上限，請執行以下指令：

```
kesl-control --set-app-settings BackupSizeLimit=<Backup size>
```

3. 若要配置儲存備份和隔離區物件的目錄，請執行以下指令：

```
kesl-control --set-app-settings QuarantineBackupFolder=<path to folder>
```

4. 若要檢查目前的應用程式設定，請執行下列指令：

```
kesl-control --get-app-settings
```

命令選項

設定	描述
`BackupDaysToLive`	將物件儲存在備份儲存中的時間段（以天為單位）。指定時間過去後，應用程式將刪除最舊的檔案備份副本。 若要刪除物件保留限制，請設定 0。
`BackupSizeLimit`	最大備份大小（MB）。當達到最大備份儲存大小時，應用程式將刪除檔案的最舊備份副本。 若要刪除備份大小限制，請設定 0。

設定	描述
`QuarantineBackupFolder`	儲存備份和隔離物件的目錄的路徑。您可以指定與預設目錄不同的目錄。您可以使用任何裝置上的目錄作為儲存備份和隔離物件的目錄。不建議指派位於遠端裝置（例如透過 Samba 和 NFS 協定安裝的裝置）上的目錄。 如果指定的目錄不存在或不可用，應用程式將使用預設目錄。 預設值：`/var/opt/kaspersky/kesl/common/objects-backup/` 存取預設目錄需要 root 權限。

檢視備份物件

由用戶端裝置上的卡巴斯基應用程式放置到備份中的檔案一般清單會在卡巴斯基安全管理中心中產生，並可在網頁主控台和管理主控台（**進階** → **儲存庫** → **備份**）中取得。

卡巴斯基安全管理中心不會將檔案從備份複製到管理伺服器；所有檔案都儲存在受防護裝置上的備份中。

如何在網頁主控台中檢視備份中物件的資訊

1. 在主網頁主控台視窗中，選取 **儲存區** → **檔案備份**。

   這會開啟由用戶端裝置上的卡巴斯基應用程式放入備份的檔案清單。卡巴斯基安全管理中心不會將檔案從備份複製到管理伺服器；所有檔案都儲存在受防護裝置上的備份中。

2. 檢視受保護裝置上備份儲存區中檔案的屬性：

   - **檔案名稱**
   - **狀態**：
     - *警告*
     - *可能已感染*
     - *由使用者新增*
     - *誤報*
     - *已解毒*
     - *未感染*
     - *受密碼保護*
     - *已刪除*
     - *必須傳送給卡巴斯基*
   - **裝置名稱**

- **已執行的操作**：
  - *刪除*
  - *解毒*
  - *掃描*
  - *還原*
- **物件**
- **已放入儲存庫**
- **項目新增者**
- **大小（位元組）**
- **已還原資料夾**
- **使用者**
- **描述**
- **虛擬管理伺服器的名稱**

如何在命令列上檢視備份中物件的資訊

要檢視備份中物件的詳細資訊，請執行：

```
kesl-control -B --query ["<filter conditions>"] [-n <objects number>] [--json]
```

其中：

- `<filter conditions>` 會指定一個或多個採用 `<field> <comparison operator> '<value>'` 格式並使用邏輯運算子 `and` 結合的 邏輯運算式，以限制查詢結果。如果您不指定任何篩選條件，應用程式將顯示備份中所有物件的詳細資訊。
- `<objects number>` 會指定要顯示儲存區中多少個最新物件。如果您不指定`-n`選項，應用程式將顯示最近 30 個物件的資訊。如果要顯示所有物件的資訊，請指定`0`。
- `--json`：以 JSON 格式輸出資料。

`ObjectId`行顯示應用程式在將物件放入備份時指派給該物件的數字識別碼。此 ID用於對物件執行操作，例如從備份儲存中還原或刪除物件。

如何在圖形介面中檢視備份中物件的資訊

1. 開啟應用程式圖形介面的主視窗。
2. 在主應用程式視窗的下方，點擊**備份**按鈕。

   這將開啟**備份**視窗。

在此視窗中顯示關於備份儲存中的物件的以下資訊：

- 物件名稱。
- 物件的完整路徑。
- 物件被新增到備份的日期。
- 物件被從備份中刪除的日期（如果設定了備份保留期，則會顯示此欄位）。
- 物件大小。

從備份還原物件

檔案將根據指定的設定從備份還原到其原始位置。還原會保留 MAC 標籤（僅限 Astra Linux 裝置）和原始檔案的屬性（不可變屬性和僅追加屬性除外）。

在 Astra Linux 裝置上，從備份還原檔案在下列情況下會出錯：

- 檔案的 MAC 標籤高於要將檔案還原到的目錄的MAC 標籤。
- 檔案的 MAC 標籤低於要將檔案還原到的目錄的 MAC 標籤，且沒有為該目錄設定 ccnr 標誌。
- 在封閉軟體環境模式下的 Astra Linux 裝置上，您只能使用將檔案放入備份時所使用的相同帳戶來還原檔案。還原檔案時，應用程式會建立 MAC 標籤為 3（cnnr 旗標）的目錄。

要在卡巴斯基安全管理中心中管理備份中的檔案，您需要啟用將備份中的檔案資料傳輸到管理伺服器。

還原感染物件可能會導致裝置感染。

如何在網頁主控台中從備份還原物件

1. 在主網頁主控台視窗中，選取 **儲存區** → **檔案備份**。

   這會開啟由用戶端裝置上的卡巴斯基應用程式放入備份的檔案清單。卡巴斯基安全管理中心不會將檔案從備份複製到管理伺服器；所有檔案都儲存在受防護裝置上的備份中。

2. 選取您要還原之檔案旁邊的核取方塊。
3. 按一下 **還原**。

   用戶端裝置上的備份物件會被還原。

如何在命令列上從備份還原物件

若要將原始名稱下的物件還原到原始定位，請執行以下命令：

```
kesl-control -B --restore <object id>
```

其中 `<object id>` 是應用程式在將物件放入備份時指派給該物件的數字識別碼。

若要以新名稱將物件還原至指定目錄，請執行下列命令：

```
kesl-control -B --restore <object id> --file <path to file>
```

其中 `--file <path to file>` 是檔案的新名稱，以及您要將其儲存至其中的目錄路徑。如果指定目錄不存在，應用程式將建立該目錄。

> 在封閉軟體環境模式下的 Astra Linux 裝置上，您只能使用將檔案放入備份時所使用的相同帳戶來還原檔案。

如何在圖形介面中從備份還原物件

若要將物件從備份還原到其原始目錄：

1. 開啟應用程式圖形介面的主視窗。
2. 在主應用程式視窗的下方，點擊**備份**按鈕。

   這將開啟**備份**視窗。
3. 選取您要還原的物件。
4. 按一下 **還原**。

備份中的物件會被還原，並可在原始目錄中使用。

> 關於還原和刪除物件的資訊被保存到事件記錄中。

從備份中刪除物件

當指定的保留期到期或達到最大備份大小時，應用程式會自動刪除最舊的備份副本，無論其狀態為何。

您可以手動刪除已還原或未還原的檔案的備份副本。

如何在網頁主控台中刪除備份中的物件

1. 在主網頁主控台視窗中，選取 **儲存區 → 檔案備份**。

   這會開啟由用戶端裝置上的卡巴斯基應用程式放入備份的檔案清單。卡巴斯基安全管理中心不會將檔案從備份複製到管理伺服器；所有檔案都儲存在受防護裝置上的備份中。
2. 選取您要刪除之檔案旁邊的核取方塊。
3. 按一下 **刪除** 按鈕。

用戶端裝置上的備份物件會被刪除。

如何在命令列上從備份刪除物件

若要從備份中刪除選定的物件，請執行：

```
kesl-control -B --mass-remove --query "<filter conditions>"
```

其中 `<filter conditions>` 指定一個或多個採用 `<field> <comparison operator> '<value>'` 格式的邏輯運算式，這些運算式使用邏輯運算子 `and` 組合，以限制查詢結果。

範例：

```
刪除 ID=15 的物件
kesl-control -B --mass-remove --query "ObjectId == '15'"
```

```
刪除名稱或路徑中包含 "test" 的物件
kesl-control -B --mass-remove --query "FileName like '%test%'"
```

若要從備份中刪除所有物件，請執行：

```
kesl-control -B --mass-remove
```

如何在圖形介面中從備份刪除物件

1. 開啟應用程式圖形介面的主視窗。
2. 在主應用程式視窗的下方，點擊**備份**按鈕。
   這將開啟**備份**視窗。
3. 選取您要刪除的物件。
4. 按一下 **刪除** 按鈕。

備份物件將被刪除。已刪除的物件將來無法還原。

> 關於還原和刪除物件的資訊被保存到事件記錄中。

進階威脅和目標式攻擊防護

Kaspersky Detection and Response 解決方案是用於偵測進階威脅的安全系統，可指明對不同級別的組織基礎結構進行的攻擊。Detection and Response 解決方案提供有關偵測到的威脅的資訊，並讓您管理對偵測結果的回應。

Kaspersky Endpoint Security 可與下列 Kaspersky Detection and Response 解決方案互通：

- 開放式單一管理平台 (OSMP) 上的 Kaspersky Endpoint Detection and Response Expert (on-premises)。整合由 Kaspersky Endpoint Security 應用程式元件 Endpoint Detection and Response Expert (on-premises)（以下亦稱為 *EDR Expert (on-premises)*）提供。
- 開放式單一管理平台 (OSMP) 上的 Kaspersky Endpoint Detection and Response Expert (cloud)。整合由 Kaspersky Endpoint Security 應用程式元件 Endpoint Detection and Response Expert (cloud)（以下亦稱為 *EDR Expert (cloud)*）提供。

- Kaspersky Anti Targeted Attack Platform上的 Kaspersky Endpoint Detection and Response 和 Kaspersky Network Detection and Response 元件。整合由 Kaspersky Endpoint Security 應用程式的以下元件提供：
  - Endpoint Detection and Response Expert (on-premises)（以下亦稱為 *EDR Expert (on-premises)*）。
  - Network Detection and Response (KATA)（以下也稱為 *NDR (KATA)*）。
- 在開放式單一管理平台 (OSMP) 或 Kaspersky Anti Targeted Attack Platform 上的Sandbox。整合由以下 Kaspersky Endpoint Security 元件提供：*Sandbox*。
- 卡巴斯基統一監控與分析平台。
- Kaspersky Endpoint Detection and Response Optimum。Kaspersky Endpoint Security 元件 (Endpoint Detection and Response Optimum (*EDR Optimum*)) 可促進整合。
- Kaspersky Managed Detection and Response。Kaspersky Endpoint Security 元件：Managed Detection and Response (*MDR*) 可促進整合。

Detection and Response 解決方案整合功能

- 如果您在EDR Agent 模式下使用 Kaspersky Endpoint Security，則僅支援與開放式單一管理平台 (OSMP) 上的 Kaspersky Endpoint Detection and Response Expert (on-premises)，以及 Kaspersky Anti Targeted Attack Platform 上的 Kaspersky Endpoint Detection and Response 和 Kaspersky Network Detection and Response 元件進行整合。
- 當 Kaspersky Endpoint Security 與 Kaspersky Managed Detection and Response 和 Kaspersky Anti Targeted Attack Platform 整合時，內建代理程式可能會將大量事件記錄到 systemd-journald 記錄檔。如果您要停用將稽核事件記錄到 systemd-journald 記錄檔的功能，請停用 systemd-journald-audit 通訊端並重新啟動作業系統。

  停用 systemd-journald-audit 通訊端

  ```
  systemctl stop systemd-journald-audit.socket
  systemctl disable systemd-journald-audit.socket
  systemctl mask systemd-journald-audit.socket
  ```

- 預設情況下，在 SintezM-Client 作業系統中，auditd 服務設定受到修改防護，即處於 `enabled 2` 模式下。當 Kaspersky Endpoint Security 與 Kaspersky Managed Detection and Response 和 Kaspersky Anti Targeted Attack Platform 解決方案整合時，為了行為偵測元件能夠正確運行，請將設定檔中的 auditd 模式變更為 `enabled 1`（無配置封鎖）並重新啟動作業系統。
- Detection and Response 解決方案在由已安裝 Kaspersky Endpoint Security for Linux 的映像建立的虛擬機上可能無法正常運作。與 Detection and Response 解決方案整合時，會使用電腦的唯一 ID (Sensor ID)。應用程式會在初始安裝期間產生此 ID，即使解除安裝應用程式後，該 ID 也會保留。複製映像時，虛擬機會繼承 Sensor ID，這可能會導致 Detection and Response 解決方案將多個虛擬機識別為同一個裝置。

  建立參考映像以便與 MDR 正確整合的建議

  如何準備參考映像以便與 EDR Expert (on-premises) 正確整合

因應措施

與 Detection and Response 解決方案整合時，Kaspersky Endpoint Security 可以執行威脅回應操作以維護安全功能。若在 Detection and Response 解決方案設定中啟用了此功能，則威脅回應操作可以在 Detection and Response 解決方案端產生，並在 Kaspersky Endpoint Security 裝置上自動執行。您也可以手動設定和執行威脅回應操作。

威脅回應操作的設定具體取決於與 Kaspersky Endpoint Security 整合的 Detection and Response 解決方案。

Kaspersky Endpoint Security 可以執行下列威脅回應操作：

- 將裝置與網路隔離。

  與 Endpoint Detection and Response Expert (on-premises)、Kaspersky Endpoint Detection and Response Expert (cloud)、Kaspersky Endpoint Detection and Response (KATA) 或 Kaspersky Managed Detection and Response 整合時，網路隔離會在 Detection and Response 解決方案端啟用或停用。您可以手動停用裝置的網路隔離。

  與 Kaspersky Endpoint Detection and Response Optimum 整合時，可以自動或手動將裝置與網路隔離。您可以設定網路隔離或手動停用裝置的網路隔離。

- 隔離檔案。

  此操作透過*隔離檔案*工作執行。

  與 Endpoint Detection and Response Expert (on-premises)、Kaspersky Endpoint Detection and Response (KATA) 或 Kaspersky Managed Detection and Response 整合時，工作會在 Detection and Response 解決方案端建立並執行。

  與 Kaspersky Endpoint Detection and Response Optimum 整合時，可以根據偵測到的入侵指標自動隔離檔案。

  當與 Kaspersky Endpoint Detection and Response Optimum 或 Kaspersky Managed Detection and Response 整合時，您也可以手動隔離檔案。

- 從隔離區還原檔案。

  與 Endpoint Detection and Response Expert (on-premises)、Kaspersky Endpoint Detection and Response Expert (cloud)、Kaspersky Endpoint Detection and Response (KATA) 或 Kaspersky Managed Detection and Response 整合時，威脅回應動作會在 Detection and Response 解決方案端產生。您也可以透過卡巴斯基安全管理中心或命令列手動執行該動作。

  與 Kaspersky Endpoint Detection and Response Optimum 整合時，可以透過卡巴斯基安全管理中心或命令列手動執行該動作。

- 從隔離區刪除檔案。

  與 Endpoint Detection and Response Expert (on-premises)、Kaspersky Endpoint Detection and Response Expert (cloud)、Kaspersky Endpoint Detection and Response (KATA) 或 Kaspersky Managed Detection and Response 整合時，威脅回應動作會在 Detection and Response 解決方案端產生。您也可以透過卡巴斯基安全管理中心或命令列手動執行該動作。

  與 Kaspersky Endpoint Detection and Response Optimum 整合時，可以透過卡巴斯基安全管理中心或命令列手動執行該動作。

- 從隔離區取得檔案。

與 Kaspersky Endpoint Detection and Response Expert (on-premises)、Kaspersky Endpoint Detection and Response Expert (cloud) 或 Kaspersky Endpoint Detection and Response (KATA) 整合時，威脅回應動作會在 Detection and Response 解決方案端產生。

與 Kaspersky Endpoint Detection and Response Optimum 整合時，可以透過卡巴斯基安全管理中心手動執行該動作。

- 從裝置接收檔案。

  此操作透過*取得檔案*工作執行。例如，您可以設定應用程式以取得由第三方應用程式生成的事件記錄檔案。

  與 Endpoint Detection and Response Expert (on-premises)、Kaspersky Endpoint Detection and Response (KATA) 或 Kaspersky Managed Detection and Response 整合時，工作會在 Detection and Response 解決方案端建立並執行。

  與 Kaspersky Endpoint Detection and Response Optimum 解決方案整合時，可在網頁主控台中建立「取得檔案」工作。

- 從裝置刪除檔案。

  此操作透過*刪除檔案*工作執行。

  與 Kaspersky Endpoint Detection and Response Expert (on-premises)、Kaspersky Endpoint Detection and Response Expert (cloud) 或 Kaspersky Endpoint Detection and Response (KATA) 整合時，該工作會在 Detection and Response 解決方案端建立並執行。

  與 Kaspersky Endpoint Detection and Response Optimum 解決方案整合時，可在網頁主控台中建立「刪除檔案」工作。

- 遠端執行裝置中的處理程序。

  此操作使用*執行應用程式*工作執行。例如，您可以遠端執行建立裝置設定檔的實用程式，然後使用*獲取檔案*工作擷取已建立的檔案。

  與 Endpoint Detection and Response Expert (on-premises)、Kaspersky Endpoint Detection and Response (KATA) 或 Kaspersky Managed Detection and Response 整合時，工作會在 Detection and Response 解決方案端建立並執行。

  與 Kaspersky Endpoint Detection and Response Optimum 解決方案整合時，可在網頁主控台中建立並執行「執行處理程序」工作。

- 遠端終止裝置中的處理程序。

  此操作使用*Kill 處理程序*工作執行。例如，您可以遠端終止使用"執行處理程序"工作啟動的網際網路速度測試實用程式。

  與 Endpoint Detection and Response Expert (on-premises)、Kaspersky Endpoint Detection and Response (KATA) 或 Kaspersky Managed Detection and Response 整合時，工作會在 Detection and Response 解決方案端建立並執行。

  與 Kaspersky Endpoint Detection and Response Optimum 解決方案整合時，可在網頁主控台中建立並執行 Kill 處理程序工作。

- 偵測裝置上的入侵指標 (IOC)。

  *入侵指標 (IOC)*是關於物件或活動的一組資料，表示對裝置進行了未經授權的存取（洩漏資料）。例如，登入嘗試失敗的次數較多就可能是入侵指標。

- 啟動 *YARA 掃描*。

  在*YARA 掃描*期間， Kaspersky Endpoint Security 使用 YARA 檔案搜尋裝置上的惡意活動特徵。*YARA 檔案*是副檔名為 YARA 或 YAR 的檔案，其中包含 YARA 規則。*YARA 規則*描述針對企業 IT 基礎架構的定向攻擊和入侵特徵。Kaspersky Endpoint Security 使用這些規則掃描物件。如果滿足規則的條件，分析器會判定感染正在進行，將詳細資訊記錄在日誌中。掃描會在本機磁碟機上遞歸執行。不支援掃描網路、可移動和雲端資源。

在 Kaspersky Endpoint Security 裝置上執行 YARA 掃描的命令，會在 Kaspersky Endpoint Detection and Response Expert (on-premises) 和 Kaspersky Endpoint Detection and Response Expert (cloud) 解決方案端建立並執行。

- 執行防護

- 獲取取證資訊。

  與 Kaspersky Endpoint Detection and Response Expert (on-premises) 和 Kaspersky Endpoint Detection and Response Expert (cloud) 整合時，您可以收集數位資料，這些資料可能有助於調查與網路犯罪和資料外洩相關的事件。

  此操作可使用下列工作執行：

  - *獲取取證*工作，會收集以下類型的資訊：
    - 檔案清單
    - 處理程序清單
    - 自動執行點清單
  - *獲取記憶體傾印*工作
  - *獲取處理程序記憶體傾印*工作
  - *獲取磁碟映像*工作

  工作會在 Kaspersky Endpoint Detection and Response Expert (on-premises) 和 Kaspersky Endpoint Detection and Response Expert (cloud) 解決方案端建立並執行。

搜尋入侵指標

*洩露指示器 (IOC)*是一個物件或者活動的資料集合，表明對電腦的未經授權存取（資料洩露）。例如，登入嘗試失敗的次數較多就可能是入侵指標。"*IOC 掃描*"工作可發現電腦上的洩露指示器並採取威脅回應措施。

如果符合下列條件之一，則可在 Kaspersky Endpoint Security 應用程式中使用 IOC 掃描功能：

- Kaspersky Endpoint Security 與 Kaspersky Endpoint Detection and Response Optimum 解決方案的整合已啟用，並且 EDR Optimum 元件已啟動。

  在此情況下，IOC 搜尋是使用 *IOC 掃描* 工作執行的。

- 已啟用 Kaspersky Endpoint Security 應用程式與 Kaspersky Endpoint Detection and Response Expert (on-premises) 或 Kaspersky Endpoint Detection and Response (KATA) 元件 的整合，且 EDR Expert (on-premises) 元件已啟動。

  在此情況下，IOC 掃描是在對應解決方案端執行。

*IOC 掃描*工作僅在作業系統的主命名空間中檢查 IOC 術語（IOC 物件的屬性，例如檔案雜湊）。*IOC 掃描*工作不會計算大於 200 MB 的檔案雜湊值。

為了搜尋入侵指標，Kaspersky Endpoint Security 會使用為使用者準備的IOC 檔案。如果您想手動新增入侵指標，請參閱IOC 檔案要求。如果 IOC 檔案不符合要求，應用程式將無法使用它。

IOC 掃描工作中使用的所有 IOC 檔案的 ID必須是唯一的。如果載入具有相同 ID 的多個 IOC 檔案，則應用程式僅使用其中一個 IOC 檔案。其他 IOC 檔案將被自動排除。

建立一個 IOC 掃描工作

您可以手動建立 *IOC 掃描* 工作：

- 在偵測詳情中（僅適用於 EDR Optimum）。

  *偵測詳情*是一款用來檢視有關被偵測的威脅的整個收集資訊的工具。偵測詳情包括，例如，出現在電腦上的檔案的歷史。有關偵測詳情的詳細資訊，請參閱 Kaspersky Endpoint Detection and Response Optimum 說明 與 Kaspersky Endpoint Detection and Response Expert 說明 。

- 使用工作精靈。

- 在本機命令列上。

如何在網頁主控台中建立 IOC 掃描 工作

1. 在網頁主控台的主視窗中，選擇**工作**。

   工作清單開啟。

2. 點擊"**新增**"。

   啟動"工作精靈"。

3. 配置工作設定：

   a. 在"**應用程式**"下拉式清單中，選取"**Kaspersky Endpoint Security for Linux 12.5**"。

   b. 在"**工作類型**"下拉式清單中，選取"**IOC 掃描**"。

   c. 在**工作名稱**欄位中，輸入新工作的名稱。

   d. 在**要將工作指派給的裝置**下，選擇您要如何定義工作範圍。

4. 根據您偏好的工作範圍定義方法選取裝置。繼續下一步。

5. 完成精靈。

   在工作清單中將顯示一個新工作。

6. 點擊新工作。

   工作內容視窗將開啟。

7. 選擇"**應用程式設定**"標籤。

8. 轉到"**威脅掃描**"區域。

9. 上傳 IOC 檔案以搜尋入侵指標。

   上傳 IOC 檔案後，應用程式會顯示有關該檔案的摘要資訊，包括未通過檢查的指標清單。上傳 IOC 檔案後，您可以直接在工作屬性中手動在內建編輯器中編輯檔案。Kaspersky Endpoint Security 支援編輯符合 OpenIOC 1.1 標準的 IOC 檔案。無法修改符合 OpenIOC 1.0 版本的 IOC 檔案的內容。

   Kaspersky Endpoint Security 會將 IOC 檔案新增至 IOC 集合。如果有必要，您可以暫時將 IOC 檔案排除在工作範圍之外。

我們不建議在開始此工作後新增或刪除 IOC 檔案。這可能會導致該工作之前執行的 IOC 掃描結果顯示不正確。我們建議新增工作，以根據新的 IOC 檔案執行 IOC 掃描。

10. 轉到“**掃描設定**”區域。

11. 如有必要，請設定回溯 IOC 掃描。

    回顧 IOC 掃描 是 *IOC 掃描* 工作的一種模式，在此模式下 Kaspersky Endpoint Security 會使用特定時間段的資料掃描入侵指標。此模式旨在透過受防護電腦的遙測資料（例如網路活動、處理程序、檔案和其他遙測資料）來搜尋入侵指標。Kaspersky Endpoint Security 會分析電腦上的作業系統日誌和瀏覽器日誌中的資料。回顧 IOC 掃描可分析以下瀏覽器的日誌：Google Chrome、Mozilla Firefox、Microsoft Edge（版本 79 或更高版本）。

    a. 在 **追溯 IOC 掃描** 下，前往搜尋設定。

    b. 啟用 **追溯 IOC 掃描** 切換開關。

    c. 設定回溯 IOC 掃描的時間間隔。

12. 選擇必須作為工作的一部分進行分析的資料類型（IOC 文件）。

    Kaspersky Endpoint Security 根據載入的 IOC 檔案的內容自動選擇*IOC 掃描*工作的資料類型（IOC 文件）。不建議取消選擇資料類型。

    此外，您可以設定 **檔案 - FileItem** 資料類型的搜尋範圍。在使用預設範圍的電腦上設定 IOC 掃描範圍。

13. 轉到“**回應設定**”區域。

14. 選取工作的操作模式：**僅警示** 或 **警示並回應**。

15. 選取偵測到 IOC 時的回應操作：

    - **執行關鍵區域掃描**如果選擇該選項，Kaspersky Endpoint Security 將執行“*關鍵區域掃描*工作”。預設情況下，Kaspersky Endpoint Security 會掃描核心記憶體、執行中的處理程序和開機磁區。

      Kaspersky Endpoint Security 掃描的關鍵區域

      - /lib/systemd
      - /lib/udev
      - /lib/dbus-1.0
      - /usr/local/lib/systemd/user
      - /usr/share/dbus-1
      - /usr/share/gdm/autostart
      - /usr/share/gnome/autostart
      - /var/spool/at
      - /var/spool/在/spool

- /var/spool/anacron
- /var/spool/cron
- /boot
- /bin
- /sbin
- /lib
- /lib32
- /lib64
- /libx32
- /usr/lib
- /usr/lib32
- /usr/lib64
- /usr/libx32
- ~/.config/autostart
- ~/.config/autostart-scripts
- ~/.config/plasma-workspace/env
- ~/.config/plasma-workspace/shutdown
- ~/.config/lxsession
- ~/.fluxbox/startup
- ~/.kde/Autostart
- /etc

- **將副本移動到隔離區，刪除物件**如果選擇該選項，Kaspersky Endpoint Security 會刪除在電腦上發現的惡意物件。在刪除物件之前，Kaspersky Endpoint Security 會建立該物件的備份副本，以便您稍後需要時還原物件。Kaspersky Endpoint Security 會將備份副本移動到隔離。

  如果此核取方塊被清除，您可以在手動執行工作後手動隔離檔案。如果 *IOC 掃描* 工作偵測到可能危及資料的檔案，您可以直接從 IOC 掃描結果中隔離此檔案（**應用程式設定 → IOC 掃描結果**）。結果，Kaspersky Endpoint Security 將使用偵測到的檔案的預設資料啟動工作建立精靈。您只需要管理附加工作設定，例如設定工作排程。

- **從網路中隔離裝置**如果選擇該選項，Kaspersky Endpoint Security 會從網路隔離電腦以防止威脅傳播。您可以在 Endpoint Detection and Response 元件設定中設定隔離持續時間。

  如果此核取方塊被清除，您可以在手動執行工作後將電腦與網路隔離。如果 *IOC 掃描* 工作偵測到可能危及資料的檔案，您可以直接從 IOC 掃描結果中隔離此檔案（**應用程式設定 → IOC 掃描結果**）。結果，Kaspersky Endpoint Security 將使用偵測到的檔案的預設資料啟動工作建立精靈。您只需要管理附加工作設定，例如設定工作排程。

16. 在工作內容視窗中，選取"**排程**"標籤。

17. 設定工作排程。

    Wake-on-LAN對於該工作不可用。確保電腦已開啟以執行工作。

18. 儲存變更。

19. 選中該工作旁邊的核取方塊。

20. 點擊"**開始**"。

您可以在網頁主控台的 **IOC 掃描結果** 下，於工作內容中檢視 *IOC 掃描* 工作的結果。IOC 掃描結果保存 30 天。此時間過後，Kaspersky Endpoint Security 會自動刪除舊條目。

如何在命令列上建立 IOC 掃描 工作

執行命令：

```
kesl-control [-T] --scan-ioc --path <path to the directory or file> [--process on|off] [--hint <regular
expression>] [--arpentry on|off] [--ports on|off] [--system on|off] [--files on|off] [--drives
all|system|critical|custom] [--excludes <list of exclusions>] [--scope <list of directories>] [--action
Skip|QuarantineFile|IsolateHost|ScanCriticalAreas]
```

符號

惡意軟體掃描工作的設定

設定	描述
`--path`	用於執行掃描的 IOC 檔案路徑，或包含副檔名為 .IOC 或 .XML 之 IOC 檔案的目錄路徑。*IOC 檔案*是包含應用程式試圖匹配以計數偵測的指示器集合的檔案。IOC 檔案必須符合 OpenIOC 標準。 您可以指定多個路徑，以空格分隔。您也可以指定兩種類型的路徑（檔案路徑和目錄路徑）。
`--process`	執行 IOC 掃描時分析處理程序資料（ProcessItem 字詞）。 如果引數值為 `off`，則 Kaspersky Endpoint Security 執行掃描時不分析在電腦上執行的處理程序。如果 IOC 檔案包含 ProcessItem IOC 文件的 IOC 字詞，他們會被忽略（偵測為不匹配）。 如果未指定引數，則僅當 ProcessItem IOC 文件在供掃描的 IOC 檔案中得到說明時，Kaspersky Endpoint Security 才分析處理程序資料。
`--hint`	執行 IOC 掃描時分析檔案資料（(ProcessItem 和 FileItem 字詞）。 您可以採用以下方式之一選擇檔案： • `<full path to the executable file of the process>` – ProcessItem 字詞； • `<full path to the file>` – FileItem 字詞。
`--arpentry`	執行 IOC 掃描時分析本機 ARP 表格中的記錄相關資料（ArpEntryItem 字詞）。 如果引數值為 `off`，則 Kaspersky Endpoint Security 不掃描 ARP 表格。如果 IOC 檔案包含 ArpEntryItem IOC 文件字詞，則他們會被忽略（偵測為不匹配）。 如果未指定引數，則僅當 ArpEntryItem IOC 文件在供掃描的 IOC 檔案中得到說明時，Kaspersky Endpoint Security 才分析 ARP 表格。

設定	描述
`--ports`	執行 IOC 掃描時分析開啟用來監聽的連接埠相關資料（PortItem 字詞）。 如果引數值為 `off`，則 Kaspersky Endpoint Security 不掃描裝置上的活動連線表格。如果 IOC 檔案包含 PortItem IOC 文件字詞，則他們會被忽略（偵測為不匹配）。 如果未指定引數，則僅當 PortItem IOC 文件在供掃描的 IOC 檔案中得到說明時，Kaspersky Endpoint Security 才分析活動連線表格。
`--system`	執行 IOC 掃描時分析環境資料（SystemInfoItem 字詞）。 如果引數值為 `off`，則 Kaspersky Endpoint Security 不分析環境資料。如果 IOC 檔案包含 SystemInfoItem IOC 文件字詞，則他們會被忽略（偵測為不匹配）。 如果未指定引數，則僅當 SystemInfoItem IOC 文件在供掃描的 IOC 檔案中得到說明時，Kaspersky Endpoint Security 才分析環境資料。
`--files`	執行 IOC 掃描時分析檔案資料（FileItem 字詞）。 如果引數值為 `off`，則 Kaspersky Endpoint Security 不分析檔案資料。如果 IOC 檔案包含 FileItem IOC 文件字詞，則他們會被忽略（偵測為不匹配）。 如果未指定引數，則僅當 FileItem IOC 文件在供掃描的 IOC 檔案中得到說明時，Kaspersky Endpoint Security 才分析檔案資料。
`--drives`	設定分析 FileItem IOC 文件的資料時的 IOC 掃描範圍。 您可以為掃描範圍設定以下值： • `<all>`，對於所有可用的檔案範圍。 • `<system>`，對於安裝了作業系統的資料夾中的檔案。 • `<critical>`，對於使用者和系統資料夾中的臨時檔案。 • `<custom>`，對於使用者定義的範圍中的檔案（`/scope=<list of folders to scan>`）。 如果未指定引數，則為關鍵領域進行掃描。
`--excludes`	設定分析 FileItem IOC 文件的資料時的排除範圍。您可以指定多個路徑，之間由空格分開。
`--scope`	分析 FileItem IOC 文件的資料時的使用者定義 IOC 掃描範圍 (`/drives=custom`)。您可以指定多個路徑，之間由空格分開。
`--action`	偵測到入侵指標時執行的操作： • `Skip`。如果選擇此選項，Kaspersky Endpoint Security 只會偵測可能導致資料遭入侵的檔案。 • `QuarantineFile`。如果選擇該選項，Kaspersky Endpoint Security 會刪除在電腦上發現的惡意物件。在刪除物件之前，Kaspersky Endpoint Security 會建立該物件的備份副本，以便您稍後需要時還原物件。Kaspersky Endpoint Security 會將備份副本移動到隔離。 • `IsolateHost`。如果選擇該選項，Kaspersky Endpoint Security 會從網路隔離電腦以防止威脅傳播。 • `ScanCriticalAreas`。如果選擇該選項，Kaspersky Endpoint Security 將執行"*關鍵區域掃描*工作"。預設情況下，Kaspersky Endpoint Security 會掃描核心記憶體、執行中的處理程序和開機磁區。

網路隔離

與 Detection and Response 解決方案整合時，裝置可以作為威脅回應動作的一部分與網路隔離。

與網路隔離相關的特殊注意事項

啟用網路隔離後，應用程式將切斷裝置上的所有活動網路連線並阻止所有新的 TCP/IP 網路連線，但以下列出的連線例外：

- 網路隔離排除項目中指定的連線
- 由 Kaspersky Endpoint Security 服務發起的連線
- 由卡巴斯基安全管理中心網路代理發起的連線
- 與 SVM 和 Integration Server 的連線（如果應用程式是在 Light Agent 模式下使用）。
- KSN 連線（與 Kaspersky Managed Detection and Response 整合時）

滿足以下條件之一時，可以套用網路隔離：

- Kaspersky Endpoint Security 與 Kaspersky Endpoint Detection and Response Optimum 解決方案的整合已啟用，並且 EDR Optimum 元件已啟動。
- 已啟用 Kaspersky Endpoint Security 應用程式與 Kaspersky Endpoint Detection and Response Expert (on-premises) 或 Kaspersky Endpoint Detection and Response (KATA) 元件 的整合，且 EDR Expert (on-premises) 元件已啟動。
- Kaspersky Endpoint Security 與 Kaspersky Managed Detection and Response 解決方案的整合已啟用，並且 MDR 元件已啟動。

與 Kaspersky Endpoint Detection and Response Expert (on-premises)、Kaspersky Endpoint Detection and Response (KATA) 和 Kaspersky Managed Detection and Response 整合時，裝置的網路隔離會啟用或停用，並在 Detection and Response 解決方案端設定網路隔離排除項目。如需詳細資訊，請參閱Kaspersky Endpoint Detection and Response Expert (on-premises) 說明、Kaspersky Anti Targeted Attack Platform 說明或 Kaspersky Managed Detection and Response 說明。如果需要，您可以手動停用裝置的網路隔離：

- 在網頁主控台中的裝置內容中（僅在與 Kaspersky Endpoint Detection and Response Expert (on-premises) 或 Kaspersky Endpoint Detection and Response (KATA) 整合時）
- 在指令列上

無論與 Detection and Response 解決方案的整合是否已啟用，也無論是否將政策套用至裝置，都可以手動停用網路隔離。

與 Kaspersky Endpoint Detection and Response Optimum 整合時，可以採用下列模式之一來套用網路隔離：

- 自動網路隔離模式。透過偵測入侵指標，可以自動將裝置與網路隔離。在**偵測到 IOC 時的動作**區域中建立和設定 *IOC 掃描*工作設定時，如果選取**偵測到 IOC 時套用回應動作**和**將裝置與網路隔離**核取方塊，則當應用程式偵測到入侵指標時，會自動啟用網路隔離。

  您可以管理以下自動網路隔離設定：

  - 變更之後會自動停用網路隔離的時間段。
  - 為自動隔離的裝置設定網路隔離排除項目。

  > 如果被自動隔離的裝置符合某項政策，則會套用該政策中指定的設定。如果未套用政策，則會套用裝置內容中指定的設定。

- 手動網路隔離模式。在調查偵測到的威脅時，您可以將裝置與網路隔離。您可以在警示詳情視窗和 網頁主控台中的裝置內容中，手動啟用裝置的網路隔離。

  您可以管理以下手動網路隔離設定：

  - 變更之後會自動停用網路隔離的時間段。
  - 為手動隔離的裝置設定網路隔離排除項目。

與 Kaspersky Endpoint Detection and Response Optimum 整合時，您可以在網頁主控台中的裝置內容中和命令列上手動停用裝置的網路隔離。

您可以在命令列中檢查裝置的網路隔離狀態。

隔離裝置會被自動分配**被從網路隔離**標籤。當網路隔離停用時，此標籤會被自動刪除。

有關按標籤獲取隔離裝置清單的一般資訊，請參閱Kaspersky Endpoint Detection and Response Optimum 說明。

網路隔離限制

當您使用網路隔離時，我們強烈建議您熟悉相關的限制。

為了使網路隔離發揮作用，Kaspersky Endpoint Security 必須執行。如果 Kaspersky Endpoint Security 發生故障（且應用程式未執行），則當 Kaspersky Managed Detection and Response 啟用網路隔離時，流量可能無法被封鎖。

DHCP 和 DNS 不會被自動新增至網路隔離排除項目中，因此如果資源的網路位址在網路隔離期間變更，Kaspersky Endpoint Security 將無法存取它。容錯 KATA 伺服器的節點也是如此。我們建議不要變更他們的位址，以便 Kaspersky Endpoint Security 不會與他們失去聯絡。

代理伺服器不會自動新被增至網路隔離排除項目中，因此您需要手動將其新增至排除項目中，以便 Kaspersky Endpoint Security 不會與提供整合的伺服器失去聯絡。

在內核版本為 4.18 或更高版本且支援 eBPF 和 BTF、並啟用了內核偵錯的偵錯點和 kprobes 功能的裝置上，支援按名稱將處理程序從網路隔離中排除。

如果 Kaspersky Endpoint Security 是以標準模式或 EDR Agent 模式使用，則使用網路隔離時，建議執行以下操作：

- 使用 KSN 代理伺服器與卡巴斯基安全網路進行互動。
- 將卡巴斯基安全管理中心用作代理伺服器進行應用程式啟動。

  如果無法使用卡巴斯基安全管理中心作為代理伺服器，則必須設定要使用的代理伺服器並將其新增至排除項目。
- 指定卡巴斯基安全管理中心作為資料庫更新來源。

如果 Kaspersky Endpoint Security 是以 Light Agent 模式使用，則這些建議不適用。

在網頁主控台中手動啟用或停用裝置的網路隔離

只有與 Kaspersky Endpoint Detection and Response Optimum 整合後，您才可以使用網頁主控台為裝置啟用網路隔離。

與 Kaspersky Endpoint Detection and Response Optimum 整合時手動啟用和停用裝置的網路隔離

若要手動啟用或停用裝置的網路隔離：

1. 在網頁主控台主視窗中，選擇**資產（裝置）→受管理裝置**。

   受管理裝置的清單將開啟。

2. 如有需要，請選擇管理群組、尋找您的裝置，然後按一下其名稱。

3. 這將開啟受管理裝置屬性視窗；在該視窗中，轉到**應用程式**索引標籤。

4. 在裝置上安裝的應用程式清單中，點擊 Kaspersky Endpoint Security。

5. 在開啟的應用程式屬性視窗中，於**應用程式設定**索引標籤上，選擇**內建代理程式 → Endpoint Detection and Response**。

6. 這將開啟一個視窗；在該視窗的**網路隔離**下，執行下列操作之一：

   - 點擊 **將裝置與網路隔離** 按鈕，以啟用裝置的網路隔離。僅在 **Endpoint Detection and Response** 切換開關已啟用時，此按鈕才可用。

     當您按一下此按鈕時，裝置將在*您於 啟用網路隔離 (NetworkIsolationStart) 工作屬性中指定的期間*內受到隔離。

   - 點擊**解除封鎖被隔離的裝置**按鈕可停用裝置的網路隔離。無論 **Endpoint Detection and Response** 切換開關為啟用或停用，此按鈕皆可用。

7. 點擊**OK**。

如果您啟用了裝置的網路隔離，Kaspersky Endpoint Security 會為該裝置分配**ISOLATED FROM NETWORK**標籤。如果停用了裝置的網路隔離，Kaspersky Endpoint Security 將從該裝置中刪除此標籤。

與 Kaspersky Endpoint Detection and Response Expert (on-premises) 或 Kaspersky Endpoint Detection and Response (KATA) 整合時，手動停用裝置的網路隔離

手動停用裝置的網路隔離：

1. 在網頁主控台主視窗中，選擇**資產（裝置）→受管理裝置**。

   受管理裝置的清單將開啟。

2. 選擇包含必要裝置的管理群組。為此，請點擊受管理裝置清單上方的**目前路徑**欄位中的連接，然後在開啟的視窗中選擇管理群組。

   此清單僅顯示選定管理群組的受管理裝置。

3. 在清單中找到您的裝置並點擊其名稱。

4. 這將開啟受管理裝置屬性視窗；在該視窗中，轉到**應用程式**索引標籤。

5. 在裝置上安裝的應用程式清單中，點擊 Kaspersky Endpoint Security。

6. 在開啟的應用程式屬性視窗的**應用程式設定**索引標籤上，選擇**Detection and Response**部分。

7. 在 **網路隔離 (EDR Expert (on-premises))** 下，點擊 **解除封鎖已隔離的裝置** 按鈕以停用裝置的網路隔離。

停用裝置的網路隔離後，Kaspersky Endpoint Security 將從裝置中刪除 **ISOLATED FROM NETWORK** 標籤。

設定自動網路隔離的持續時間

只有與 Kaspersky Endpoint Detection and Response Optimum 整合後，您才可以設定自動網路隔離的持續時間：

*IOC 掃描*工作隔離的裝置的網路隔離會在一定時間後自動停用。您可以在網頁主控台中的裝置內容和政策內容中設定此逾時。關於網頁主控台政策屬性中網路隔離設定的描述，請參閱附錄 5。有關受管理裝置屬性中網路隔離設定的描述，請參閱下表。

如果政策套用至裝置，則會套用政策中指定的設定；無法在裝置內容中設定自動網路隔離逾時。如果政策未套用至裝置，則會套用裝置內容中指定的設定。

預設情況下，應用程式在啟用網路隔離 5 小時後會停用網路隔離。網路隔離已停用後，裝置可以不受限制地在網路上運作。

在裝置屬性中配置自動停用網路隔離

配置自動停用裝置網路隔離：

1. 在網頁主控台主視窗中，選擇**資產（裝置）→受管理裝置**。

   受管理裝置的清單將開啟。

2. 選擇包含必要裝置的管理群組。為此，請點擊受管理裝置清單上方的**目前路徑**欄位中的連接，然後在開啟的視窗中選擇管理群組。

   此清單僅顯示選定管理群組的受管理裝置。

3. 在清單中找到您的裝置並點擊其名稱。

4. 這將開啟受管理裝置屬性視窗；在該視窗中，轉到**應用程式**索引標籤。

5. 在裝置上安裝的應用程式清單中，點擊 Kaspersky Endpoint Security。

6. 在開啟的應用程式屬性視窗中，在**應用程式設定**索引標籤上，選擇**Detection and Response**，然後點擊**Endpoint Detection and Response Optimum**連結。

7. 在**網路隔離**下，點擊**設定裝置解除封鎖**。

8. 這將開啟**配置裝置解除封鎖**視窗；在該視窗中，選取**此後解除封鎖自動隔離的裝置：**核取方塊，並在其下方的輸入欄位中，指定在之後裝置必須被自動解除封鎖的時間段（以小時為單位）。

9. 儲存變更。

手動設定網路隔離

若要手動將裝置與網路隔離，則需要與 Kaspersky Endpoint Detection and Response Optimum 整合。

若手動為裝置啟用網路隔離，則可透過*啟用網路隔離* (*NetworkIsolationStart*) 本機工作預先設定網路隔離。您可以設定裝置的網路隔離排除項目和網路隔離持續時間。

*啟用網路隔離*是一項預定義工作，僅在以下情況下自動執行：

- 點擊裝置內容中的**將裝置與網路隔離**按鈕。
- 如果您在警示詳情視窗中啟用裝置的網路隔離。

您無法透過點擊**新增**按鈕來建立*啟用網路隔離*工作的新實例，也無法透過點擊**啟動**按鈕來執行該工作。該工作僅在裝置內容中可用，您可以在為裝置啟用網路隔離之前變更其設定。

> 無論裝置是否套用了政策，*啟用網路隔離*工作設定均會套用。

若要設定裝置的網路隔離參數：

1. 在網頁主控台主視窗中，選擇**資產（裝置）→受管理裝置**。

   受管理裝置的清單將開啟。

2. 選擇包含必要裝置的管理群組。為此，請點擊受管理裝置清單上方的**目前路徑**欄位中的連接，然後在開啟的視窗中選擇管理群組。

   此清單僅顯示選定管理群組的受管理裝置。

3. 在清單中找到您的裝置並點擊其名稱。

4. 這將開啟受管理裝置屬性視窗；在該視窗中，轉到**工作**索引標籤。

5. 在工作清單中，點擊*啟用網路隔離*工作。

   工作內容視窗將開啟。

6. 轉到**應用程式設定**索引標籤。

7. 點擊**配置排除項目**連結以開啟**排除項目**視窗。

8. 在開啟的視窗中，使用表格上方的按鈕執行必要的操作：

   - 如果要新增關於排除的網路連線的資訊，請按照以下方式之一進行操作：
     - 點擊**新增**按鈕，然後輸入網路連線的資訊。
     - 點擊**從設定檔新增**按鈕，然後從詞典中選擇網路設定檔。
   - 如果要刪除關於排除的網路連線的資訊，請選取要刪除的網路連線旁的核取方塊，然後點擊**移除**按鈕。

9. 點擊**OK**。

10. 在**隔離裝置**欄位中，輸入所需的裝置網路隔離持續時間（以小時為單位）。

    網路隔離預設時長為 5 小時。

    網路隔離最短時長為 1 小時。

11. 點擊**儲存**按鈕儲存所做的變更。

在網頁主控台中設定網路隔離排除項目

當 Kaspersky Endpoint Security 與 Endpoint Detection and Response Expert (on-premises)、Kaspersky Endpoint Detection and Response (KATA) 或 Kaspersky Managed Detection and Response 整合時，網路隔離排除項目會在 Detection and Response 解決方案端進行設定。如需詳細資訊，請參閱Kaspersky Endpoint Detection and Response Expert (on-premises) 說明、Kaspersky Anti Targeted Attack Platform 說明或Kaspersky Managed Detection and Response 說明。

Kaspersky Endpoint Security 與 Kaspersky Endpoint Detection and Response Optimum 整合時，您可以透過下列方式設定網路隔離排除項目：

- 在網頁主控台的政策內容中。系統為套用該政策的裝置自動啟用網路隔離後，將套用該政策中設定的排除項目。
- 在網頁主控台中的裝置內容中。系統為未套用該政策的裝置自動啟用網路隔離後，將套用裝置內容中設定的排除項目。
- *在啟用網路隔離 (NetworkIsolationStart) 本機工作的設定中*。如果手動為裝置啟用網路隔離，將套用此工作內容中設定的排除項目。無論裝置是否已套用政策，*啟用網路隔離*工作設定都會套用。

為設定網路隔離排除項目，應用程式提供*標準網路設定檔*清單。網路設定檔中包含的規則用於確保具有 DNS/DHCP 伺服器和 DNS/DHCP 用戶端角色的裝置不間斷運行。您可以管理標準網路設定檔的設定並手動設定排除項目。

> 如果已將政策套用至裝置，則無法在裝置屬性中新增或移除網路隔離排除項目。

如何在網頁主控台中新增網路隔離排除項目

1. 在網頁主控台的主視窗中，選擇**資產管理** → **政策**。
2. 點擊 Kaspersky Endpoint Security 政策的名稱。
   政策內容視窗將開啟。
3. 選擇"**應用程式設定**"標籤。
4. 轉到"**內置代理設定**"→"**Endpoint Detection and Response**"。
5. 在"**網路隔離**"塊中，點擊"**排除項目**"連接。
   這會開啟一個包含網路隔離排除項目清單的視窗。
6. 您可以透過以下方式排除網路連線：
   - 按一下 **新增**，然後輸入網路連線的資訊。

     > 您可以新增應用程式，讓該元件不封鎖其網路連線。此設定適用於核心版本為 4.18 或更新版本、支援 eBPF 和 BTF，且已啟用用於核心追蹤的 tracepoints 和 kprobes 功能的裝置。

   - 按一下 **從設定檔新增** 按鈕，然後從詞典中選取網路設定檔。
7. 儲存變更。

如何在網頁主控台中移除網路隔離排除項目

1. 在網頁主控台的主視窗中，選擇**資產管理** → **政策**。
2. 點擊 Kaspersky Endpoint Security 政策的名稱。
   政策內容視窗將開啟。
3. 選擇"**應用程式設定**"標籤。

4. 轉到"**內置代理設定**"→"**Endpoint Detection and Response**"。

5. 在"**網路隔離**"塊中，點擊"**排除項目**"連接。

   這會開啟一個包含網路隔離排除項目清單的視窗。

6. 選取網路連線旁的核取方塊，然後按一下 **刪除**。

7. 儲存變更。

隔離檔案

當回應威脅時，Kaspersky Endpoint Detection and Response 可以建立"*移動檔案到隔離區*"工作。這對於最小化威脅的後果是必需的。*隔離區*是電腦上的一個特別本機儲存區域。使用者可以隔離使用者認為對電腦有危險的檔案。隔離的檔案以加密形式儲存，不會威脅裝置的安全。

您可以用以下方式建立"*移動檔案到隔離區*"工作：

- 在偵測詳情中（僅適用於 EDR Optimum）。

  *偵測詳情*是一款用來檢視有關被偵測的威脅的整個收集資訊的工具。偵測詳情包括，例如，出現在電腦上的檔案的歷史。您可以直接從警示詳情中選取要刪除的檔案。結果，Kaspersky Endpoint Security 將使用偵測到的檔案的預設資料啟動工作建立精靈。您只需要管理附加工作設定，例如設定工作排程。

- 使用工作精靈。

  新工作精靈可讓您手動輸入要刪除的檔案或目錄的路徑，以及要刪除之檔案的雜湊值。您也可以管理附加工作設定，例如設定工作排程。

- 在 *IOC 掃描* 工作設定中。

  如果 *IOC 掃描* 工作偵測到可能危及資料的檔案，您可以直接從 IOC 掃描結果中隔離此檔案（**應用程式設定** → **IOC 掃描結果**）。結果，Kaspersky Endpoint Security 將使用偵測到的檔案的預設資料啟動工作建立精靈。您只需要管理附加工作設定，例如設定工作排程。

檔案大小不得超過 100 MB。

如何建立 移動檔案到隔離區 工作

1. 在網頁主控台的主視窗中，選擇**工作**。

   工作清單開啟。

2. 點擊"**新增**"。

   啟動"工作精靈"。

3. 配置工作設定：

   a. 在"**應用程式**"下拉式清單中，選取"**Kaspersky Endpoint Security for Linux**"。

   b. 在"**工作類型**"下拉式清單中，選取"**移動檔案到隔離區**"。

   c. 在"**工作名稱**"欄位中，輸入簡要說明。

   d. 在"**要將工作指派給的裝置**"塊中，選取工作範圍。

4. 按照所選工作範圍選項選取裝置。點擊“**下一步**”。

5. 點擊“**完成**”按鈕結束精靈。
   在工作清單中將顯示一個新工作。

6. 點擊新工作。

7. 工作內容視窗將開啟。

8. 選擇“**應用程式設定**”標籤。

9. 在檔案清單中，點擊“**新增**”。
   檔案新增精靈啟動。

10. 若要新增檔案，您需要輸入檔案路徑或目錄路徑以及檔案雜湊值。

11. 在工作內容視窗中，選取“**排程**”標籤。

12. 設定工作排程。

13. 儲存變更。

14. 選中該工作旁邊的核取方塊。

15. 點擊“**開始**”。

結果，Kaspersky Endpoint Security 會將檔案移動到隔離區。

如果檔案被其它處理程序鎖定，工作將顯示為“*已完成*”，但是檔案本身只有在電腦重啟後才會被隔離。重啟電腦後，請確認檔案已刪除。

如果您試圖隔離一個目前在執行的可執行檔，“*移動檔案到隔離區*”工作可能完成但有“*存取被拒絕*”錯誤。為該檔案建立終止處理程序工作，然後重試。

如果您試圖隔離一個太大的檔案，“*移動檔案到隔離區*”工作可能完成但有“*隔離區儲存空間不足*”錯誤。清除隔離區或增加隔離區的大小。然後再試。

從裝置接收檔案

您可以從使用者的電腦獲取檔案。例如，您可以設定應用程式以取得由第三方應用程式生成的事件記錄檔案。工作執行後，檔案副本會儲存在隔離區中。*隔離區*是電腦上的一個特別本機儲存區域。您可以使用網頁主控台（**操作 → 儲存區 → 隔離**）從隔離區將此檔案下載到電腦。使用者裝置上的原始檔案仍保留在其原始目錄中。

在卡巴斯基安全管理中心的隔離檔案清單中，無論檔案掃描結果如何，透過 *獲取檔案* 工作接收的所有檔案都將具有 *被感染* 狀態。

檔案大小不得超過 100 MB。

如何建立 獲取檔案 工作

1. 在網頁主控台的主視窗中，選擇**工作**。
   工作清單開啟。
2. 點擊“**新增**”。
   啟動“工作精靈”。
3. 配置工作設定：
   a. 在“**應用程式**”下拉式清單中，選取“**Kaspersky Endpoint Security for Linux**”。
   b. 在“**工作類型**”下拉式清單中，選取“**獲取檔案**”。
   c. 在“**工作名稱**”欄位中，輸入簡要說明。
   d. 在“**要將工作指派給的裝置**”塊中，選取工作範圍。
4. 按照所選工作範圍選項選取裝置。點擊“**下一步**”。
5. 點擊“**完成**”按鈕結束精靈。
   在工作清單中將顯示一個新工作。
6. 點擊新工作。
7. 工作內容視窗將開啟。
8. 選擇“**應用程式設定**”標籤。
9. 在檔案清單中，點擊“**新增**”。
   檔案新增精靈啟動。
10. 若要新增檔案，您需要輸入檔案路徑或目錄路徑以及檔案雜湊值。
11. 在工作內容視窗中，選取“**排程**”標籤。
12. 設定工作排程。
13. 儲存變更。
14. 選中該工作旁邊的核取方塊。
15. 點擊“**開始**”。

結果，Kaspersky Endpoint Security 將建立一個檔案副本並將此副本移動到隔離區。您可以在網頁主控台中從隔離區下載檔案。

如果發生以下情況，*獲取檔案* 工作將以錯誤結束：

- 未找到指定的檔案。
- 指定了不正確的檔案資訊（檔案名稱或總和檢查碼）。
- 權限不足，無法管理指定檔案。

- 指定檔案已被封鎖。
- 隔離區空間不足。
- 指定的檔案太大（超過 100 MB）。

從裝置中刪除檔案

您可以使用“*刪除檔案*”工作遠端刪除檔案。例如，您可以在回應威脅時遠端刪除檔案。

如何建立 刪除檔案 工作

1. 在網頁主控台的主視窗中，選擇**工作**。
   工作清單開啟。
2. 點擊“**新增**”。
   啟動“工作精靈”。
3. 配置工作設定：
   a. 在“**應用程式**”下拉式清單中，選取“**Kaspersky Endpoint Security for Linux**”。
   b. 在“**工作類型**”下拉式清單中，選取“**刪除檔案**”。
   c. 在“**工作名稱**”欄位中，輸入簡要說明。
   d. 在“**要將工作指派給的裝置**”塊中，選取工作範圍。
4. 按照所選工作範圍選項選取裝置。點擊“**下一步**”。
5. 點擊“**完成**”按鈕結束精靈。
   在工作清單中將顯示一個新工作。
6. 點擊新工作。
7. 工作內容視窗將開啟。
8. 選擇“**應用程式設定**”標籤。
9. 若要新增檔案，您需要輸入目錄路徑和檔案雜湊值。
10. 在工作內容視窗中，選取“**排程**”標籤。
11. 設定工作排程。
12. 儲存變更。
13. 選中該工作旁邊的核取方塊。
14. 點擊“**開始**”。

結果，Kaspersky Endpoint Security 會從電腦刪除檔案。如果檔案被其它處理程序鎖定，工作將顯示為“*已完成*”，但是檔案本身只有在電腦重啟後才會被刪除。重啟電腦後，請確認檔案已刪除。

啟動處理程序

您可以使用“*處理程序啟動*”工作遠端執行檔案。例如，您可以遠端執行建立電腦設定檔的公用程式。接下來，您可以使用 *獲取檔案* 工作在卡巴斯基安全管理中心網頁主控台中接收所建立的檔案。

> 如果作業系統中的 SELinux 處於 `Enforcing` 模式，若要啟動 *處理程序啟動* 工作，您需要對 SELinux 執行額外配置。

如何配置 SELinux 以執行“啟動處理程序”工作

如果您計劃在作業系統上以 `Enforcing` 模式使用 SELinux，則若要在與 Detection and Response 解決方案整合時執行回應操作，您需要另外管理 SELinux 設定。

> 此 SELinux 設定需要 root 權限。

若要設定 SELinux 以執行回應操作：

1. 將 SELinux 切換到權限模式：

   - 如果已啟用 SELinux，請執行以下指令：

     將 SELinux 切換為寬容模式

     ```
     setenforce Permissive
     ```

   - 如果已停用 SELinux，請在 /etc/selinux/config 設定檔中設定 `SELINUX=permissive`，然後重新啟動作業系統。

2. 確保系統上安裝了 semanage 實用程式。如果未安裝該實用程式，請根據套件管理器安裝 policycoreutils-python 或 policycoreutils-python-utils 套件。

3. 請執行所有工作，以執行您要在與 Detection and Response 解決方案整合時使用的回應操作。

4. 請確保 audit.log 檔案中沒有錯誤。

   檢視 audit.log 檔案

   ```
   grep kesl /var/log/audit/audit.log
   ```

5. 如果 audit.log 檔案中有任何錯誤，請根據封鎖記錄建立並載入新的規則模組以修復錯誤，然後再次執行回應操作工作。

   根據封鎖記錄建立並載入新的規則模組：

   ```
   grep kesl /var/log/audit/audit.log | audit2allow -M kesl
   semodule -i kesl.pp
   ```

6. 將 SELinux 切換為強制模式。

```
setenforce Enforcing
```

如何建立 處理程序啟動 工作

1. 在網頁主控台的主視窗中，選擇**工作**。
   工作清單開啟。

2. 點擊“**新增**”。
   啟動“工作精靈”。

3. 配置工作設定：

   a. 在“**應用程式**”下拉式清單中，選取“**Kaspersky Endpoint Security for Linux**”。

   b. 在“**工作類型**”下拉式清單中，選取“**處理程序啟動**”。

   c. 在“**工作名稱**”欄位中，輸入簡要說明。

   d. 在“**要將工作指派給的裝置**”塊中，選取工作範圍。

4. 按照所選工作範圍選項選取裝置。點擊“**下一步**”。

5. 點擊“**完成**”按鈕結束精靈。
   在工作清單中將顯示一個新工作。

6. 點擊新工作。

7. 工作內容視窗將開啟。

8. 選擇“**應用程式設定**”標籤。

9. 輸入處理程序啟動指令：

   - **可執行指令**用於輸入啟動處理程序的指令的欄位。
     例如，如果您想執行用於檢查與管理伺服器連線的 `klnagchk` 公用程式，請輸入 `/opt/kaspersky/klnagent/bin/klnagchk`。

   - **指令行參數(可選)**用於輸入指令列參數的欄位，以便在啟動時將附加輸入傳遞給指令碼、實用程式或應用程式。
     例如，您可以輸入 `-logfile /tmp/klnagchk.log`參數。此參數會告訴工具將結果儲存至 `/tmp` 中名為 `klnagchk.log` 的檔案。如果需要傳遞多個參數，請以空格分隔。

   - **工作資料夾路徑(可選)**用於輸入工作目錄路徑的欄位，處理程序會將檔案放置在該目錄中。
     例如，您可以輸入 `/tmp`，並使用以下參數執行 `klnagchk` 公用程式：`-logfile klnagchk.log -savecert certificate.cer`。在此情況下，兩個檔案均會在 `tmp` 中建立。

10. 在工作內容視窗中，選取“**排程**”標籤。

11. 設定工作排程。

12. 儲存變更。

13. 選中該工作旁邊的核取方塊。

14. 點擊“**開始**”。

    結果，Kaspersky Endpoint Security 將在靜默模式下執行指令和啟動處理程序。您可以在工作內容的“**執行結果**”區域中檢視工作結果。

終止處理程序

您可以使用“*終止處理程序*”工作遠端終止處理程序。例如，您可以遠端終止因惡意活動而啟動的程序。

如果想要禁止執行檔案，您可以配置“執行防護元件。您可以禁止執行可執行檔、指令碼、Office 格式的檔案。

如何建立 終止處理程序 工作

1. 在網頁主控台的主視窗中，選擇**工作**。
   工作清單開啟。

2. 點擊“**新增**”。
   啟動“工作精靈”。

3. 配置工作設定：

   a. 在“**應用程式**”下拉式清單中，選取“**Kaspersky Endpoint Security for Linux**”。

   b. 在“**工作類型**”下拉式清單中，選取“*終止處理程序*”。

   c. 在“**工作名稱**”欄位中，輸入簡要說明。

   d. 在“**要將工作指派給的裝置**”塊中，選取工作範圍。

4. 按照所選工作範圍選項選取裝置。點擊“**下一步**”。

5. 點擊“**完成**”按鈕結束精靈。
   在工作清單中將顯示一個新工作。

6. 點擊新工作。

7. 工作內容視窗將開啟。

8. 選擇“**應用程式設定**”標籤。

9. 若要終止程序，您必須選取要終止之程序的檔案。您可以採用以下方式之一選擇檔案：

   - 輸入檔案的完整名稱。

   - 輸入檔案的雜湊和檔案的路徑。

   - 輸入處理程序的 PID（僅限於本機工作）。

   - 如果檔案位於網路磁碟機上，則輸入以`\\`而不是磁碟機字母開始的檔案路徑。例如，`\\server\shared_folder\file.exe`。如果檔案路徑包含網路磁碟機字母，您可能獲得“*未找到檔案*”錯誤。

10. 在工作內容視窗中，選取“**排程**”標籤。

11. 設定工作排程。

12. 儲存變更。

13. 選中該工作旁邊的核取方塊。

14. 點擊“**開始**”。

    結果，Kaspersky Endpoint Security 會終止電腦上的處理程序。您可以在工作內容的“**結果**”區域中檢視工作結果。

物件的執行防禦

與卡巴斯基 Detection and Response 解決方案整合時，您可以套用此回應動作；Kaspersky Endpoint Security 會從這些解決方案接收執行防禦規則。

如果物件符合規則，Kaspersky Endpoint Security 會阻止執行該物件。

物件執行防禦 EDR Expert (on-premises)

與 Kaspersky Endpoint Detection and Response Expert (on-premise)、Kaspersky Endpoint Detection and Response Expert (cloud) 或 Kaspersky Endpoint Detection and Response (KATA) 整合時，您可以在相應解決方案的主控台中設定規則，以封鎖物件的執行。

如果已啟用與 Kaspersky Endpoint Detection and Response Expert (on-premises) 解決方案或 Kaspersky Endpoint Detection and Response (KATA) 元件的整合，您可以在政策屬性中啟用或停用物件執行防禦（**應用程式設定** → **內置代理設定** → **Endpoint Detection and Response Expert (on-premises)**）。

若要啟用物件執行防禦，請將切換開關設定為 **執行防止已啟用**。

物件執行防禦（EDR Optimum）

與 Kaspersky Endpoint Detection and Response Optimum 整合時，您可以在網頁主控台中設定物件執行防禦和執行防禦規則。

如何在卡巴斯基安全管理中心政策中啟用物件執行防禦

1. 在網頁主控台的主視窗中，選擇**資產管理** → **政策**。

2. 點擊 Kaspersky Endpoint Security 政策的名稱。

   政策內容視窗將開啟。

3. 選擇“**應用程式設定**”標籤。

4. 轉到”**內置代理設定**”→”**Endpoint Detection and Response**”。

5. 轉到“**執行防止**”標籤。

6. 將切換開關設定為 **執行防止已啟用**。

7. 選取啟動或開啟物件時的動作

   - **封鎖並新增至事件記錄**應用程式會封鎖符合防禦規則標準的物件執行或文件開啟，並在事件日誌中記錄嘗試執行物件或開啟文件的事件。

   - **新增至事件記錄**應用程式會記錄關於嘗試執行符合防禦規則標準的可執行物件或開啟符合防禦規則標準的文件的事件，但實際上不會封鎖其執行或開啟。

8. 儲存變更。

如何在受管理裝置屬性中啟用物件執行防禦

1. 在網頁主控台中，前往 **資產管理 → 資產（裝置）**。

2. 點擊所需裝置名稱的連結。

3. 這會開啟所選裝置的屬性視窗；在該視窗中，前往 **應用程式** 索引標籤，然後按一下 **<Kaspersky Endpoint Security** 應用程式名稱> 連結。

   1. 在網頁主控台的主視窗中，選擇**資產管理 → 政策**。

   2. 點擊 Kaspersky Endpoint Security 政策的名稱。

      政策內容視窗將開啟。

   3. 選擇“**應用程式設定**”標籤。

   4. 轉到”**內置代理設定**”→”**Endpoint Detection and Response**”。

   5. 轉到“**執行防止**”標籤。

   6. 將切換開關設定為 **執行防止已啟用**。

   7. 選取啟動或開啟物件時的動作

      - **封鎖並新增至事件記錄**應用程式會封鎖符合防禦規則標準的物件執行或文件開啟，並在事件日誌中記錄嘗試執行物件或開啟文件的事件。

      - **新增至事件記錄**應用程式會記錄關於嘗試執行符合防禦規則標準的可執行物件或開啟符合防禦規則標準的文件的事件，但實際上不會封鎖其執行或開啟。

   8. 儲存變更。

4. 選擇“**應用程式設定**”標籤。

5. 轉到”**內置代理設定**”→”**Endpoint Detection and Response**”。

6. 前往 **執行防止** 子區段。

7. 將切換開關設定為 **執行防止已啟用**。

8. 選取物件執行防禦模式：

   - **封鎖**。在此模式下，應用程式會阻止執行符合預防規則標準的物件或開啟符合預防規則標準的文件，並在事件日誌中記錄嘗試執行物件或開啟文件的事件。

   - **通知**。在這種模式下，應用程式會在事件日誌中記錄關於嘗試執行可執行物件或開啟符合預防規則標準的檔案的事件，但實際上並不會阻止它們的執行或開啟。預設情況下已選擇此模式。

9. 儲存變更。

如果將政策套用至裝置，則無法在裝置內容中啟用或停用物件執行防禦。

如何在網頁主控台中新增 EDR Optimum 元件的物件執行防禦規則

1. 在網頁主控台的主視窗中，選擇**資產管理 → 政策**。

2. 點擊 Kaspersky Endpoint Security 政策的名稱。

   政策內容視窗將開啟。

3. 選擇"**應用程式設定**"標籤。

4. 如有必要，選中"**使用大小寫路徑**"核取方塊。

5. 在政策或受管理裝置的屬性中，按一下物件執行防禦規則清單上方工具列中的 **新增** 按鈕。

6. 這將開啟一個視窗；在該視窗中，輸入執行防禦規則的名稱。

7. 透過將開關設定為適當的位置來指定執行防禦規則的狀態。

8. 在 **類型** 下拉式清單中，選取您要封鎖的物件類型：

   - **可執行檔**

   - **指令碼**

   - **Office 應用程式檔案**

   如果選擇了錯誤的物件類型，應用程式將無法封鎖該檔案或指令碼。

9. 若要新增物件，請在對應欄位中指定物件的路徑和/或物件的總和檢查碼（檔案的 SHA256 或 MD5 雜湊值）。

10. 儲存變更。

    建立的規則將會被新增到**物件執行防禦**設定區塊的規則清單中。

Kaspersky Endpoint Security 會控制裝置上可執行檔案和指令碼的執行，以及 Office 應用程式檔案的開啟。物件執行防禦支援特定的一組辦公室應用程式檔案副檔名和特定的一組指令碼解釋器。透過阻止物件啟動，您可以阻止威脅蔓延。

如果符合下列條件之一，則 Kaspersky Endpoint Security 應用程式中可使用執行防禦功能：

- 與 Kaspersky Endpoint Detection and Response Optimum 解決方案的整合已啟用，並且 EDR Optimum 元件已啟動。
- 與 Kaspersky Endpoint Detection and Response Expert (on-premises) 或 Kaspersky Endpoint Detection and Response (KATA) 元件 的整合已啟用，並且 EDR Expert (on-premises) 元件已啟動。
- 與 Kaspersky Endpoint Detection and Response Expert (cloud) 的整合已啟用，並且 EDR Expert (cloud) 元件已啟動。

如果未啟用檔案操作攔截的封鎖模式，則無論設定的運作模式為何，物件的執行防禦都會以通知模式運作。

預設停用物件執行防禦。啟用物件執行防禦可能會影響作業系統中應用程式的啟動速度。

為了使物件執行防禦起作用，您需要啟用執行防禦規則。

物件執行防禦的限制和特殊注意事項

物件執行防禦限制

物件執行防禦規則有以下限制：

- 在應用程式啟動之前，Kaspersky Endpoint Security 應用程式不會阻止執行防禦規則中指定的物件。
- Kaspersky Endpoint Security 應用程式不會阻止在建立或修改預防規則之前開啟的檔案。
- Kaspersky Endpoint Security 應用程式不會阻止在建立或修改執行防禦規則以覆寫這些物件之前執行的執行防禦規則所涵蓋的物件。
- 某些檔案對於作業系統和應用程式的運作至關重要。阻止此類檔案的執行可能會擾亂系統運作。

我們不建議建立超過 50000 條執行防禦規則，因為這可能會導致系統不穩定。

與 Kaspersky Endpoint Detection and Response Expert (on-premises) 和 Kaspersky Endpoint Detection and Response (KATA) 整合時，物件執行防禦的特殊注意事項

當 Kaspersky Endpoint Security 應用程式與 Kaspersky Endpoint Detection and Response Expert (on-premises) 或 Kaspersky Endpoint Detection and Response (KATA) 整合時，應用程式會使用 *EDR Expert (on-premises) 元件的執行防禦規則*。應用程式會從 Kaspersky Endpoint Detection and Response Expert (on-premises) 或 Kaspersky Endpoint Detection and Response (KATA) 取得這些規則。

與 Kaspersky Endpoint Detection and Response Expert (on-premises) 或 Kaspersky Endpoint Detection and Response (KATA) 整合時，您可以：

- 在網頁主控台或管理主控台中，啟用或停用 EDR Expert (on-premises) 元件之物件執行防禦規則的套用。

  當執行防禦規則被觸發時，Kaspersky Endpoint Security 會將報告傳送至 Endpoint Detection and Response Expert (on-premises) 或 Kaspersky Anti Targeted Attack Platform。詳情請參閱相關解決方案的說明。
- 在指令列中檢視 EDR Expert (on-premises) 元件的物件執行防禦規則清單。

與 Kaspersky Endpoint Detection and Response Optimum 整合時，物件執行防禦的特殊注意事項

Kaspersky Endpoint Security 與 Kaspersky Endpoint Detection and Response Optimum 解決方案整合時，應用程式使用 *EDR Optimum 元件的物件執行防禦規則*。您可以在網頁主控台中手動建立這些規則。您也可以在警示詳情視窗中自動建立執行防禦規則。

與 Kaspersky Endpoint Detection and Response Optimum 整合時，您可以：

- 在網頁主控台中，啟用或停用 EDR Optimum 元件之物件執行防禦規則的套用。
- 在網頁主控台中建立和設定 EDR Optimum 的物件執行防禦規則。

  您也可以透過在警示詳情視窗中防止檔案執行，自動為物件建立執行防禦規則。執行防禦規則新增到裝置所屬的管理群組的政策中。

  > 只有當政策套用至裝置時，您才可以在「警示詳情」視窗中預防檔案的執行。

- 在命令列上檢視 EDR Optimum 元件的物件執行防禦規則清單。

與 Kaspersky Endpoint Detection and Response Optimum 整合時，物件執行防禦可以採用以下兩種模式之一工作：

- **封鎖**。在此模式下，應用程式會阻止執行符合預防規則標準的物件或開啟符合預防規則標準的文件，並記錄關於嘗試執行物件或開啟文件的事件。

  > Kaspersky Endpoint Security 應用程式會阻止執行被執行防禦規則禁止的指令碼，即使該指令碼是由允許的指令碼匯入的。

- **通知**。在這種模式下，應用程式會記錄關於嘗試執行可執行物件或開啟符合預防規則標準的文件的事件，但實際上並不會阻止它們的執行或開啟。預設情況下已選擇此模式。

管理隔離區

*隔離區*是裝置上的一個特殊儲存位置，用於儲存可能感染病毒或在偵測時無法解毒的檔案。隔離區允許隔離檔案以進行進一步調查。隔離的檔案以加密形式儲存，不會威脅裝置的安全。與隔離區相反，備份區儲存在解毒過程中偵測到惡意程式碼並被刪除或修改的檔案的備份副本。

該應用程式僅在與 Detection and Response 解決方案整合時使用隔離區來執行建議的威脅回應動作。該應用程式與 Kaspersky Endpoint Detection and Response Optimum 或 Kaspersky Managed Detection and Response 整合時，您還可以手動隔離您認為對您的裝置有危險的檔案。

預設情況下，/var/opt/kaspersky/kesl/common/objects-backup/ 目錄用於儲存隔離檔案。該目錄還包含備份物件。您可以使用命令列變更用於儲存備份和隔離物件的目錄。

隔離的檔案可能包含個人資料。存取隔離檔案需要 root 權限。

您可以在網頁主控台或管理主控台中使用政策，或使用指令列，在裝置上配置隔離區設定。您可以配置以下隔離區設定：

- 必須已滿才能產生關於隔離區已滿的事件的隔離區百分比。預設情況下，當隔離區已滿 90% 時會產生事件。
- 隔離區的最大容量（以兆位元組為單位）。當達到最大隔離區大小時，應用程式會自動刪除最舊的被隔離的檔案。預設情況下，如果應用程式在標準模式或 EDR Agent 模式下使用，則隔離區大小上限為 200 MB；如果應用程式在 Light Agent 模式下使用，則隔離區大小上限為 100 MB。
- 儲存備份和隔離物件的目錄路徑（只能在命令列上配置）。

如何在網頁主控台中管理隔離區設定

1. 在網頁主控台的主視窗中，選擇**資產管理 → 政策**。
2. 點擊 Kaspersky Endpoint Security 政策的名稱。
   政策內容視窗將開啟。
3. 選擇"**應用程式設定**"標籤。
4. 轉到"**一般設定**"→"**報告和儲存**"。
5. 在 **隔離區** 區域中，配置以下設定：
   - **限制隔離區大小**將隔離區限制為以 MB 為單位指定的大小。預設情況下已選擇此核取方塊。
   - **隔離區的最大大小 (MB)**如果啟用 **限制隔離區大小** 設定，您可以指定隔離區的大小上限，以 MB 為單位（預設為 200 MB）。隔離區大小不得超過 999,999 MB。
   - **隔離區容滿時通知**隔離區使用量達到此百分比時的通知。預設情況下已選擇此核取方塊。
     您可以指定達到後即傳送通知的百分比（預設為 90%）。
6. 要將此政策套用到電腦，請關閉... 掛鎖圖示並儲存變更。

隔離檔案

某些檔案對於作業系統和應用程式的運作至關重要。隔離此類檔案可能會擾亂系統的運作。

只有在滿足下列條件之一時，才可以將檔案置於隔離區：

- Kaspersky Endpoint Security 與 Kaspersky Endpoint Detection and Response Optimum 的整合已啟用，且 EDR Optimum 元件已啟動。
- 已啟用 Kaspersky Endpoint Security 應用程式與 Kaspersky Endpoint Detection and Response Expert (on-premises) 或 Kaspersky Endpoint Detection and Response (KATA) 元件 的整合，且 EDR Expert (on-premises) 元件已啟動。
- Kaspersky Endpoint Security 與 Kaspersky Managed Detection and Response 的整合已啟用，且 MDR 元件已啟動。

用於儲存隔離物件的目錄必須可寫入。

與 Kaspersky Endpoint Detection and Response (on-premises) 或 Kaspersky Endpoint Detection and Response (KATA) 整合時，可透過下列其中一種方式將檔案隔離：

- 透過 Detection and Response 解決方案側配置的工作。如需詳細資訊，請參閱 Kaspersky Endpoint Detection and Response Expert (on-premises) 說明 或 Kaspersky Anti Targeted Attack Platform 說明 。
- 因對處理程序記憶體執行 IOC 掃描工作 而產生。

與 Kaspersky Managed Detection and Response 整合時，檔案將透過以下方式之一被隔離：

- 由於執行了在 Kaspersky Managed Detection and Response 端配置的工作。
- 由於在裝置上執行了管理隔離區的命令。

有關與 Kaspersky Endpoint Detection and Response 整合時使用隔離區的更多資訊，請參閱 Kaspersky Endpoint Detection and Response 說明 。

與 Kaspersky Endpoint Detection and Response 整合時，檔案將透過以下方式之一被隔離：

- 由於偵測到入侵指標自動進行。
- 作為*隔離*工作的結果，您可以在Web 主控台中建立該工作。
- 由於在裝置上執行了管理隔離區的命令。
- 因遵循警示詳情中的建議而產生。

有關與 Kaspersky Endpoint Detection and Response Optimum 整合時管理隔離區的更多信息，請參閱 Kaspersky Endpoint Detection and Response Optimum 說明。

管理隔離檔案

您可以管理隔離檔案：

- 卡巴斯基安全管理中心，卡巴斯基應用程式所隔離的檔案通用清單內。

  若要在卡巴斯基安全管理中心中管理被隔離的檔案，您需要啟用將被隔離的檔案的資料傳輸到管理伺服器。

- 在裝置上本機使用命令列。

您可以檢視關於隔離檔案的資訊，以及刪除和還原隔離區中的檔案。

無論是否啟用與 Detection and Response 解決方案的整合，也無論是否將政策套用至裝置，都可以從隔離區還原、刪除和擷取檔案。

用戶端裝置上被卡巴斯基應用程式隔離的檔案的一般清單儲存在卡巴斯基安全管理中心中，可在管理主控台（**進階 → 儲存庫 → 隔離區**）和網頁主控台（**操作 → 儲存庫 → 隔離區**）中存取。卡巴斯基安全管理中心不會將檔案從隔離區儲存複製到管理伺服器；所有檔案都儲存在用戶端裝置上的隔離儲存中。如需有關在卡巴斯基安全管理中心中管理已隔離檔案的詳細資訊，請參閱卡巴斯基安全管理中心說明。

隔離的檔案將被根據指定設定還原到其原始位置。還原會保留 MAC 標籤（僅限 Astra Linux 裝置）和原始檔案的屬性（包括不可變屬性和僅追加屬性）。具有不可變和僅追加屬性的檔案，只有在原始檔案不存在時才能還原到該位置，或還原到原始位置，但使用不同的名稱。要將檔案從隔離區還原到不同目錄或使用不同的名稱還原到原始位置，需要 root 權限。

還原過程完成後，應用程式將刪除還原檔案的隔離副本。

在以下情況下，從隔離區還原檔案會失敗：

- 隔離區儲存中未找到要還原的檔案。
- 正在被還原的檔案的名稱指定不正確或大小寫錯誤。
- 檔案 ID 指定不正確。
- 目標目錄已被刪除、移動、重新命名，或者您沒有對該資料夾的存取權限。

  在這種情況下，應用程式會將檔案移至 /var/opt/kaspersky/kesl/common/restored/ 目錄。您可以手動將檔案從該目錄移至您選擇的目錄。

- 指定路徑下已存在同名檔案。
- 裝置沒有足夠的空間。
- 僅限 Astra Linux 裝置：檔案的 MAC 標籤高於要將檔案還原到的目錄的 MAC 標籤。
- 僅限 Astra Linux 裝置：檔案的 MAC 標籤低於要將檔案還原到的目錄的 MAC 標籤，且沒有為該目錄設定 ccnr 標誌。

在下列情況下，從隔離區刪除檔案會失敗：

- 隔離儲存中未找到要刪除的檔案。
- 被刪除的檔案的名稱指定不正確或大小寫錯誤。
- 檔案 ID 指定不正確。

Endpoint Detection and Response Optimum

Kaspersky Endpoint Detection and Response Optimum 是一個解決方案，用於防護組織的 IT 基礎設施免受漏洞利用、勒索軟體、無檔案攻擊以及攻擊者用來破壞裝置或資料的合法系統工具等的威脅。

Kaspersky Endpoint Security 12.5 for Linux 與 Kaspersky Endpoint Detection and Response Optimum 版本 3.1 相容。

Kaspersky Endpoint Security 與 Kaspersky Endpoint Detection and Response Optimum 的整合由 Kaspersky Endpoint Security 元件促進：Endpoint Detection and Response Optimum (*EDR Optimum*)。

若要使用 EDR Optimum 元件集中管理 Kaspersky Endpoint Security 應用程式，請使用卡巴斯基安全管理中心 Windows 15.1 或卡巴斯基安全管理中心 Linux 15.3、15.4、16.0、16.1、16.2。

此元件不適用於搭載 Elbrus CPU 的裝置。

Kaspersky Endpoint Detection and Response Optimum 的運作方式

Kaspersky Endpoint Detection and Response Optimum 會監控並分析威脅的演化，並向安全人員或管理員提供有關潛在攻擊的資訊，協助他們及時執行威脅回應動作。

Kaspersky Endpoint Detection and Response Optimum 使用下列威脅情報工具：

- 卡巴斯基安全網路（以下也稱為 KSN）雲端服務基礎設施，提供對卡巴斯基檔案、網站和軟體信譽線上知識庫的存取。
- 與卡巴斯基威脅情報入口網站整合，其中包含並顯示關於檔案和網站信譽的資訊。
- Kaspersky 威脅資料庫。

與 Kaspersky Endpoint Detection and Response Optimum 互動時，Kaspersky Endpoint Security 可以：

- 將關於裝置事件的資料傳送到卡巴斯基安全管理中心。Kaspersky Endpoint Security 會將有關處理程序、開啟的網路連線和修改的檔案的監控資料以及應用程式偵測到的威脅資料和針對這些威脅的處理結果資料傳送到卡巴斯基安全管理中心。
- 在接收來自卡巴斯基安全管理中心的指令時執行威脅回應操作以維護安全。

設定 Kaspersky Endpoint Detection and Response Optimum 整合

先決條件

在設定 Kaspersky Endpoint Detection and Response Optimum 整合之前：

- 新增 EDR Optimum 產品授權金鑰至應用程式，如果您已購買單獨的產品授權以使用此功能。

  如果您使用 Kaspersky Endpoint Security，且其產品授權包含 Kaspersky Endpoint Detection and Response Optimum，則不需要執行任何操作。

  > 如果在 Light Agent 模式下使用 Kaspersky Endpoint Security，則產品授權金鑰會新增至 SVM。

- 確保已啟用以下項目且運作正常：
  - 標準模式或延伸模式下的 卡巴斯基安全網路：

    > 為了最有效地運行 Kaspersky Endpoint Detection and Response Optimum，我們建議使用延伸的卡巴斯基安全網路模式。

  - Kaspersky Endpoint Security 應用程式的以下元件：
    - 檔案威脅防護。
    - 行為偵測。

  若要確保遙測資料完整，並在卡巴斯基安全管理中心中建立威脅發展鏈，您還需要啟用 Web 威脅防護。

  您也可以啟用物件執行防禦功能。

必要設定步驟

1. **安裝 Kaspersky Endpoint Detection and Response Optimum 管理外掛程式**

   Kaspersky Endpoint Detection and Response Optimum 管理外掛程式是用於管理 Windows、Mac 和 Linux 作業系統上的代理程式的統一外掛程式，是顯示警示和檢視警示詳情所必需的。如需安裝程序的說明，請參閱 Kaspersky Endpoint Detection and Response Optimum 說明。

   如果您的基礎設施使用 卡巴斯基安全管理中心雲端主控台來管理 Kaspersky Endpoint Detection and Response Optimum，則預設會安裝此外掛程式。

2. **設定 Kaspersky Endpoint Detection and Response Optimum 整合設定**

   您可以透過以下方式進行設定：

   - 使用網頁主控台（卡巴斯基安全管理中心主控台和/或 OSMP 主控台）。
   - 使用指令列。

     > 使用卡巴斯基安全管理中心管理主控台管理 EDR Optimum 元件不受支援。

3. **啟用將資料傳輸至管理伺服器**

若要使用 Kaspersky Endpoint Detection and Response Optimum 的所有功能，您必須配置以下內容：

- 啟用將備份和隔離區中的檔案相關資訊傳送到卡巴斯基安全管理中心儲存。為此，您需要在政策屬性中選取以下核取方塊：
  - **關於備份中的檔案**
  - **關於隔離區中的檔案**
- 允許顯示警示清單 為此，您可以在卡巴斯基安全管理中心網頁主控台主視窗的**設定→介面設定**下啟用**顯示 EDR 警示**切換開關。

  顯示 EDR 警示設定在 15.1 之前的網頁主控台版本中不提供。在卡巴斯基安全管理中心主控台中，您可以從威脅報告導覽至 EDR 警示。

- 啟用傳輸受管理裝置上協力廠商應用程式事件的相關資訊。若要這麼做，請在受管理裝置上執行以下命令：

  ```
  kesl-control --set-app-settings SystemEventsTransmission=Yes
  ```

  啟用此設定可能會顯著增加作業系統負載。

4. **請確保已成功建立與 Kaspersky Endpoint Detection and Response Optimum 的連線**

以任何方便的方式檢查 Kaspersky Endpoint Detection and Response Optimum 的狀態。
已設定 Kaspersky Endpoint Detection and Response Optimum 整合。偵測到威脅時，系統會產生警示。在警示詳情視窗中，您可以檢視關於威脅的資訊並執行回應動作。

如何啟用 EDR Optimum 整合

在網頁主控台中，您可以在政策內容中啟用或停用 EDR Optimum 元件，並設定與 Kaspersky Endpoint Detection and Response Optimum 的整合。

如何在網頁主控台中啟用 Kaspersky Endpoint Detection and Response Optimum 整合

1. 在網頁主控台的主視窗中，選擇**資產管理 → 政策**頁簽。
2. 點擊 Kaspersky Endpoint Security 政策的名稱。

   政策內容視窗將開啟。
3. 選擇"**應用程式設定**"標籤。
4. 轉到"**內置代理設定**"→"**Endpoint Detection and Response**"。
5. 啟用 **Endpoint Detection and Response 已啟用** 切換開關。
6. 要將此政策套用到電腦，請關閉... 掛鎖圖示並儲存變更。

如何在指令列上啟用 Kaspersky Endpoint Detection and Response Optimum 整合

若要啟用 EDR Optimum 元件，請執行以下命令：

```
kesl-control --set-app-settings UseEdrOptimum=Yes
```

1. 在網頁主控台的主視窗中，選取 **資產管理** → **資產（裝置）** 區域。
2. 點擊所需裝置名稱的連結。
3. 這會開啟所選裝置的內容視窗；在該視窗中，前往 **應用程式** 索引標籤，然後點擊 <Kaspersky Endpoint Security application name> 連結。
4. 前往 **應用程式設定** 索引標籤，點擊 **Detection and Response** 區域，然後點擊 **Endpoint Detection and Response Optimum** 連結。
5. 這會開啟一個視窗；在該視窗中，將切換開關設定為 **已啟用 Endpoint Detection and Response Optimum**，以啟用整合。
6. 如有必要，請管理以下設定：
   - 作為自動網路隔離的一部分，裝置封鎖持續時間。

     點擊 **設定裝置解除封鎖** 連結，並指定封鎖時間。
   - 自動網路隔離排除
7. 儲存變更。

受管理裝置已設定與 Kaspersky Endpoint Detection and Response Optimum 整合。

如何確認 EDR Optimum 整合正常運作

請閱讀可能的整合狀態及其顯示時機的相關資訊。

您可以透過以下方式測試 EDR Optimum 元件：

- 在命令列上使用以下命令：

  ```
  kesl-control --app-info
  ```

  EDR Optimum 整合顯示為 **執行中** 狀態。
- 在網頁主控台中：
  - 使用*應用程式元件狀態報告*。關於報告的詳細資訊，請參閱卡巴斯基安全管理中心說明。
  - 前往 **資產管理** → **資產** 區段 → <裝置名稱> 連結 → **應用程式** 索引標籤 → <Kaspersky Endpoint Security 應用程式名稱> 連結 → **一般** 索引標籤 → **元件**。

    Endpoint Detection and Response Optimum 元件顯示為 **執行中** 狀態。

Cloud Sandbox

Cloud Sandbox 技術可讓您偵測電腦上的進階威脅。Kaspersky Endpoint Security 自動將被偵測檔案轉寄到 Cloud Sandbox 進行分析。Cloud Sandbox 在隔離環境中執行這些檔案以偵測惡意活動並確定這些檔案的信譽。有關這些檔案的資料然後被傳送到卡巴斯基安全網路。因此，如果 Cloud Sandbox 偵測到一個惡意檔案，Kaspersky Endpoint Security 將執行適當操作在偵測到該檔案的所有電腦上消除該威脅。

若要 Cloud Sandbox 作業，您必須啟用使用卡巴斯基安全網路。

如果您使用卡巴斯基私人安全網路，則 Cloud Sandbox 技術不可用。

Cloud Sandbox 技術一律啟用，且可供卡巴斯基安全網路的所有使用者使用，無論產品授權類型為何。如果您已經部署 Endpoint Detection and Response Optimum 解決方案，可以針對 Cloud Sandbox 偵測到的威脅啟用獨立計數器。在分析偵測到的威脅時，您可以使用此計數器來編制統計資料。Kaspersky Endpoint Security 會在卡巴斯基安全管理中心主控台的 *威脅報告* 中指明 Cloud Sandbox 威脅偵測技術。

如何在網頁主控台中啟用 Cloud Sandbox 計數器

1. 在網頁主控台的主視窗中，選擇**資產管理 → 政策**。
2. 點擊 Kaspersky Endpoint Security 政策的名稱。
   政策內容視窗將開啟。
3. 選擇"**應用程式設定**"標籤。
4. 轉到"**內置代理設定**"→"**Endpoint Detection and Response**"。
5. 選擇"**Cloud Sandbox**"標籤。
6. 啟用 **Cloud Sandbox 已啟用** 切換開關。
7. 要將此政策套用到電腦，請關閉... 掛鎖圖示並儲存變更。

Endpoint Detection and Response Expert (on-premises)

卡巴斯基 Endpoint Detection and Response Expert (on-premises) 是一款企業網路安全解決方案，可防禦大多數網路安全風險，並涵蓋威脅傳播的主要情境。卡巴斯基 Endpoint Detection and Response Expert (on-premises) 的元件部署在開放式單一管理平台 (OSMP) 上。如需此解決方案與平台的詳細資訊，請參閱卡巴斯基 Endpoint Detection and Response Expert (on-premises) 說明。

與卡巴斯基 Endpoint Detection and Response Expert (on-premises) 解決方案的整合由 Kaspersky Endpoint Security 應用程式元件 Endpoint Detection and Response Expert (on-premises)（以下亦稱為 *EDR Expert (on-premises)*）提供。

此元件不適用於搭載 Elbrus CPU 的裝置。

Endpoint Detection and Response Expert (on-premises) 的運作方式

1. **安裝 Kaspersky Endpoint Security 的裝置會與 OSMP 威脅回應操作伺服器和 OSMP 遙測收集伺服器建立安全連線**
2. **Kaspersky Endpoint Security 會將資料傳送至 OSMP 平台上的遙測收集伺服器**

   會傳輸以下資訊：

   - 裝置上事件的資訊
   - 應用程式偵測到的威脅資訊
   - 處理這些威脅之結果的資訊
   - 處理程序、開啟的網路連線和已修改檔案的監控資料
3. **Kaspersky Endpoint Security 執行威脅回應操作**

   回應操作會根據 OSMP 平台上的威脅回應操作伺服器命令執行。

設定 Kaspersky Endpoint Detection and Response Expert (on-premises) 整合

先決條件

設定與卡巴斯基 Endpoint Detection and Response Expert (on-premises) 的整合之前：

- 允許透過連接埠 443 和 8443 進行連線。
- 啟用 行為偵測 元件，以傳輸必要的遙測資料。

  如果您想取得其他防護元件所偵測威脅的相關資訊，請啟用這些元件：

  - 檔案威脅防護。
  - 網路威脅防護。
  - Web 威脅防護。
  - 加密軟體防護。
  - 應用程式控制。
  - 裝置控制。
  - 系統完整性監控。

  > 如果行為偵測使用 eBPF 機制取得系統遙測資料（在內核版本 4.18 及更高版本，且具有 eBPF 支援的 64 位元作業系統上可用），則遙測資料將更加全面。

- 如果您已購買單獨的產品授權來使用此功能，請將 EDR Expert (on-premises) 產品授權金鑰新增至應用程式。

如果您是依據包含卡巴斯基 Endpoint Detection and Response Expert (on-premises) 的產品授權使用 Kaspersky Endpoint Security，則無須執行任何操作。

如果應用程式是在 Light Agent 模式下使用，EDR Expert (on-premises) 產品授權金鑰會新增至 SVM。

- 此外，您還需要在 OSMP 平台上設定 收集器、關聯器和 儲存體。

必要設定步驟

1. **取得並處理 OSMP 伺服器所核發的憑證**

   與卡巴斯基 Endpoint Detection and Response Expert (on-premises) 整合時，執行 Kaspersky Endpoint Security 的裝置會與 OSMP 威脅回應伺服器和 OSMP 遙測伺服器建立加密的 HTTPS 連線。

   > 如果在 Kaspersky Endpoint Security 應用程式的一般設定中配置了代理伺服器，則將使用代理伺服器連線到 OSMP 伺服器。

   用於防護與 OSMP 伺服器連線的憑證必須由 OSMP 平台管理員提供。

   若要處理憑證，請依照 將 PFX 憑證轉換為 PEM 格式一文中說明的步驟操作。

   您可以使用伺服器憑證和/或用戶端憑證。選擇取決於貴組織的安全政策。

2. **設定 Kaspersky Endpoint Detection and Response Expert (on-premises) 整合設定**

   您可以透過以下方式進行設定：

   - 使用網頁主控台（卡巴斯基安全管理中心主控台和/或 OSMP 主控台）。
   - 使用指令列。

   如果您想要使用物件執行防禦，可以啟用 EDR Expert (on-premises) 元件的物件執行防禦規則。

3. **確認已成功建立與 Endpoint Detection and Response Expert (on-premises) 平台的連線**

   以任何方便的方式檢查 EDR Expert (on-premises) 的狀態。

4. **必要時管理其他設定**

   - 如果您的作業系統上將 SELinux 設定為 Enforcing 模式，則還需要額外設定 SELinux以執行回應操作。
   - 若要執行**記憶體傾印**或**程序傾印**回應操作，請解除封鎖 ptrace。
   - 檢閱網路隔離的限制。
   - 啟用傳輸受管理裝置上協力廠商應用程式事件的相關資訊。若要這麼做，請在受管理裝置上執行以下命令：

     ```
     kesl-control --set-app-settings SystemEventsTransmission=Yes
     ```

     > 啟用此設定可能會顯著增加作業系統負載。

如何準備參考映像以便與 EDR Expert (on-premises) 正確整合

準備映像前，請確定參考裝置上不存在 `/var/opt/kaspersky/.ids_generated` 檔案。

若要準備參考映像以便與卡巴斯基 Endpoint Detection and Response Expert（內部部署）正確整合：

遵循這些指示操作時，請勿重新啟動參考裝置或 Kaspersky Endpoint Security 應用程式。

1. 以 root 身分執行下列指令：

```
systemctl stop kesl
systemctl edit kesl
```

2. 在編輯器中，於 `### Anything between here and the comment below will become the contents of the drop-in file` 與 `### Edits below this comment will be discarded` 兩行之間新增下列其中一個設定：

   - 每次在暫時虛擬機上啟動應用程式時，更新 SensorID

```
[Service]
ExecStartPre=-/usr/bin/uuid-regen.sh -a
```

   - 在持久性虛擬機上僅更新 SensorID 一次

```
[Service]
ExecStartPre=-/usr/bin/uuid-regen.sh -b
```

3. 儲存變更並關閉編輯器。

   已建立 `/etc/systemd/system/kesl.d/override.conf` 檔案。檢閱其內容，確保其符合新增的設定。

4. 執行下列指令以重新載入 systemd 服務：

```
systemctl daemon-reload
```

5. 建立包含下列內容的 `/usr/bin/uuid-regen.sh` 檔案：

```
#!/usr/bin/env bash
# ------------------------------------------------------------
#  Kaspersky IDs updater
#  Modes:
#    -a   Always regenerate the IDs (default)
#    -b   Generate them only once – subsequent runs do nothing
#  Exit code: always 0
# ------------------------------------------------------------
set -euo pipefail
# ----- configuration ------------------------------------------------
PCID_FILE="/var/opt/kaspersky/kesl/common/pcid"
INSTALL_ID_FILE="/var/opt/kaspersky/epagent/install_id"
KESL_INI="/var/opt/kaspersky/kesl/common/kesl.ini"
# Marker that shows the script has already been executed in mode b
MARKER="/var/opt/kaspersky/.ids_generated"
# ----- default mode -------------------------------------------------
MODE="a"
# ----- parse command-line arguments ---------------------------------
while getopts ":ab" opt; do
   case $opt in
       a) MODE="a" ;;
       b) MODE="b" ;;
       \?) echo "Invalid option: -$OPTARG" >&2; exit 0 ;;
   esac
done
shift $((OPTIND-1))
# ----- helper: generate a new UUID and write to a file ---------------
write_uuid() {
   local target=$1
   /usr/bin/uuidgen > "$target"
}
# ----- helper: replace MachineId in kesl.ini -------------------------
replace_machine_id() {
   local new_id
   new_id=$(/usr/bin/uuidgen)
   /usr/bin/sed -i "s/^MachineId=.*/MachineId=${new_id}/" "$KESL_INI"
}
# ----- main logic ----------------------------------------------------
if [[ "$MODE" == "b" && -f "$MARKER" ]]; then
   # Mode b – already ran once → do nothing
   :
else
   # (re)generate all required values
   write_uuid "$PCID_FILE"
   write_uuid "$INSTALL_ID_FILE"
   replace_machine_id
   # In mode b remember that we have already executed
   if [[ "$MODE" == "b" ]]; then
       /usr/bin/touch "$MARKER"
   fi
fi
exit 0
```

6. 使用下列指令變更 `/usr/bin/uuid-regen.sh` 檔案的權限：

```
chmod 700 /usr/bin/uuid-regen.sh
```

參考裝置現在已準備好建立作業系統映像。

如何設定 EDR Expert (on-premises) 整合

在網頁主控台中，您可以啟用或停用 EDR Expert (on-premises) 元件，並在 Kaspersky Endpoint Security 政策內容中設定 Kaspersky Endpoint Security 與 Kaspersky Endpoint Detection and Response Expert (on-premises) 的整合。

如何在網頁主控台中設定 Kaspersky Endpoint Detection and Response Expert (on-premises) 整合

1. 在網頁主控台的主視窗中，選擇**資產管理** → **政策**。
2. 點擊 Kaspersky Endpoint Security 政策的名稱。

   政策內容視窗將開啟。
3. 選擇"**應用程式設定**"標籤。
4. 前往 **內置代理設定** → **Endpoint Detection and Response Expert (on-premises)**。
5. 選取 **Endpoint Detection and Response Expert 版本 8.0 或更新版本** 選項。
6. 新增遙測資料收集伺服器和回應伺服器。

   若要執行此操作，請在 **連線到遙測資料收集伺服器** 和 **連線到威脅回應伺服器** 區段中，點擊 **新增** 按鈕。在開啟的視窗中，指定伺服器位址 (IPv4、IPv6) 以及用於連線到伺服器的連接埠。
7. 若要新增憑證，請在 **連線到遙測資料收集伺服器** 和 **連線到威脅回應伺服器** 區段中點擊 **連線設定** 連結；然後在顯示的窗格中執行下列操作：

   a. 在對應區段中點擊 **上傳** 按鈕，新增伺服器憑證。

   b. 如果您需要額外保護，請建立加密容器。

      若要執行此操作，請在 **額外連線保護** 區段中：

      1. 選取 **使用雙向身分驗證** 核取方塊。
      2. 點擊 **上傳** 按鈕，然後新增您完成 主要整合情境 時收到的用戶端憑證。
      3. 在對應欄位中輸入加密容器的密碼。

         > **加密容器密碼** 欄位為必填。若未輸入用戶端憑證（加密容器）的密碼，您無法儲存設定。
8. 要將此政策套用到電腦，請關閉... 掛鎖圖示並儲存變更。

如何在指令列中設定 Kaspersky Endpoint Detection and Response Expert (on-premises) 整合

1. 若要新增回應伺服器憑證，請執行下列指令：

```
kesl-control [-R] --add-kataedr-server-certificate <file> --server-type response
```

2. 若要新增遙測伺服器憑證，請執行下列指令：

```
kesl-control [-R] --add-kataedr-server-certificate <file> --server-type telemetry
```

3. 若要設定整合設定，請執行下列指令：

```
kesl-control --set-settings 24 [<setting name>=<setting value>]
```

   設定及其可能值列於下表。

4. 若要新增用於連線至回應伺服器的用戶端憑證，請執行下列指令：

```
kesl-control [-R] --add-kataedr-client-certificate <file> --server-type response
```

5. 若要新增用於連線到遙測伺服器的用戶端憑證，請執行下列指令：

```
kesl-control [-R] --add-kataedr-client-certificate <file> --server-type telemetry
```

6. 若要啟用與 EDR Expert (on-premises) 的整合，請執行下列指令：

```
kesl-control --start-task 24
```

Kaspersky Endpoint Detection and Response Expert (on-premises) 整合設定

設定	描述	值
Mode	整合模式。 對於 Kaspersky Endpoint Detection and Response Expert (on-premises) 整合，Kaspersky Endpoint Security 應用程式會與 OSMP 平台上的伺服器互動。 對於 Kaspersky Endpoint Detection and Response (KATA) 整合，Kaspersky Endpoint Security 安全應用程式與 Kaspersky Anti Targeted Attack Platform 上的伺服器進行互動。	EDRKATA（預設）是 EDR (KATA) 整合模式。允許啟用與 Kaspersky Endpoint Detection and Response (KATA) 整合，Kaspersky Endpoint Detection and Response (KATA) 是 Kaspersky Anti Targeted Attack Platform 的元件。 EDRExpertOnPrem 是 EDR Expert (on-premises) 整合模式。啟用 Kaspersky Endpoint Detection and Response Expert (on-premises) 整合
UseClientPinnedCertificate	啟用或停用雙向身分驗證，以增強與 OSMP 威脅回應操作伺服器連線的安全性。 如果 OSMP 威脅回應伺服器端已啟用雙向身分驗證，您需要在 *Kaspersky Endpoint Detection and Response Expert (on-premises) 整合*工作的設定中啟用雙向身分驗證，並在啟動工作前新增用戶端憑證。	Yes 會啟用雙向身分驗證，以提高與 OSMP 威脅回應動作伺服器連線的安全性。 No（預設值）— 不使用雙向身分驗證。
SynchronizationPeriod	向 OSMP 威脅回應操作伺服器發送同步請求的週期（以分鐘為單位）。	預設值：5。
ConnectionTimeout	等待連接到 OSMP 威脅回應操作伺服器的最長時間（以秒鐘為單位）。	預設值：10。
RequestTimeout	等待 OSMP 威脅回應操作伺服器回應的最長時間（以秒鐘為單位）。	預設值：10。
EnableTelemetry	將裝置上事件的相關資料（遙測資料）傳送到 OSMP 遙測資料收集伺服器。	Yes（預設值）啟用向 OSMP 遙測伺服器傳送遙測資料。 No 停用傳送遙測資料。
[Endpoints.item_#]部分包含 OSMP 威脅回應伺服器的位址和連接埠。您可以新增多個伺服器。		
Address	OSMP 威脅回應操作伺服器位址。 可指定 Integration Server 的 IP 位址（IPv4 或 IPv6）或完全限定網域名稱 (FQDN)。 為確保在裝置上啟用網路隔離的情況下應用程式發生故障時與伺服器的通訊不會中斷，我們建議指定伺服器的 IP 位址。	預設值：127.0.0.1。
Port	用於連線到 OSMP 威脅回應伺服器的連接埠。	預設值：443。
[TelemetrySettings]部分包含用於連線到 OSMP 遙測伺服器的一般設定。		
UseClientPinnedCertificate	啟用或停用雙向身分驗證，以增強與 OSMP 遙測伺服器連線的安全性。 如果 OSMP 遙測伺服器端已啟用雙向身分驗證，您需要在 *Kaspersky Endpoint Detection and Response Expert (on-premises) 整合*工作的設定中啟用雙向身分驗證，並在啟動工作前新增用戶端憑證。	Yes 會啟用雙向身分驗證，以提高與 OSMP 遙測伺服器連線的安全性。 No（預設值）— 不使用雙向身分驗證。

設定	描述	值
ConnectionTimeout	等待連接到 OSMP 遙測伺服器的最長時間（以秒鐘為單位）。	預設值：10。
RequestTimeout	等待 OSMP 遙測伺服器回應的最長時間（以秒鐘為單位）。	預設值：10。
OnlyTaggedEvents	僅傳送含 IOA 的遙測資料。*攻擊指標 (IOA)* 是指包含系統中可疑行為（指示可能存在針對性攻擊）描述的規則。應用程式會將系統中正在進行的行為與這些規則進行比較，並記錄下指示存在針對性攻擊的事件。應用程式使用*串流掃描*技術，該技術允許即時追蹤此類事件。	Yes — 僅在偵測到攻擊指標 (IOA) 時傳送遙測資料。 No（預設值）— 傳送所有遙測資料。
[TelemetrySettings.Endpoints.item_#]部分包含 OSMP 遙測伺服器的位址和連接埠。您可以新增多個伺服器。		
Address	OSMP 遙測伺服器憑證位址 可指定 Integration Server 的 IP 位址（IPv4 或 IPv6）或完全限定網域名稱 (FQDN)。 為確保在裝置上啟用網路隔離的情況下應用程式發生故障時與伺服器的通訊不會中斷，我們建議指定伺服器的 IP 位址。	預設值：127.0.0.1。
Port	用於連線 OSMP 遙測伺服器的連線埠。	預設值：443。
[TelemetrySettings.EventTransferSettings]部分包含資料傳輸到 OSMP 遙測伺服器的設定。		
MaximumDataTransferTime	向 OSMP 遙測伺服器傳送事件的最大延遲時間（以秒鐘為單位）。	預設值：30。
UseRequestCountLimits	限制請求數量。該功能有助於最佳化伺服器負載。如果啟用此功能，應用程式會限制傳輸的事件。如果事件數量超過配置的限制，Kaspersky Endpoint Security 將停止傳送事件。	Yes（預設值）— 調節傳送的事件數量。 No — 不調節事件的數量。
MaximumNumberOfEventsInHour	每小時的最大事件數量	預設值：3000。
MaximumNumberOfEventsInPackage	一個套件中的最大事件數量。	預設值：1024。
EventLimitExceededPercentage	事件數量超過限制（百分比）。如果某種類型的事件佔事件總數的比例超過配置的閾值（百分比），則傳送事件會受到限制。	預設值：15。

對於 Kaspersky Endpoint Detection and Response Expert (on-premises) 整合的設定，階層中的巢狀政策允許指定獨立值，即使所有其他政策設定均已繼承。

如果在父政策中啟用了 Kaspersky Endpoint Detection and Response Expert (on-premises) 整合，且在子政策中啟用了設定繼承，則依預設，子政策的整合設定也會被繼承，且無法變更。如果您想要設定獨立的整合設定，請從下拉式清單中選取 **使用自訂連線設定**。這會使 Kaspersky Endpoint Detection and Response Expert (on-premises) 整合設定可供編輯。

如果您使用網頁主控台或命令列，若要與 Kaspersky Endpoint Detection and Response (on-premises) 整合，您需要在 EDR Expert (on-premises) 元件的設定中選取 EDR (on-premises) 整合模式：

- 如果使用網頁主控台，請在政策設定中選擇**Endpoint Detection and Response Expert（版本 8.0 或更高版本）**。若要在裝置上設定與 Kaspersky Endpoint Detection and Response (on-premises) 的整合，您需要在網頁主控台中針對任一版本（8.0 版及更新版本，或 7.1 版及更早版本）管理「掛鎖」。
- 如果您使用命令列，請在工作設定中設定`Mode=EDRExpertOnPrem`。

如何驗證 EDR Expert (on-premises) 整合已啟動並正常執行

如何測試 EDR Expert (on-premises) 元件：

- 在命令列上使用以下命令：

```
kesl-control --app-info
```

- 在網頁主控台中。
  - 在卡巴斯基安全管理中心主控台中：
    使用*應用程式元件狀態報告*。關於報告的詳細資訊，請參閱卡巴斯基安全管理中心說明。
  - 在 OSMP 主控台中：
    - 使用*應用程式元件狀態報告*。
    - 前往**資產管理** → **資產**區段，然後選取**分析與回應**索引標籤。
      裝置會以**正常活動**遙測狀態顯示在清單中。
    - 前往**威脅搜尋**區段。
      來自該裝置的遙測事件會顯示在事件清單中。

Endpoint Detection and Response Expert (cloud)

Kaspersky Endpoint Security for Linux 與 Kaspersky Endpoint Detection and Response Expert (cloud) 的整合暫時無法使用。此功能計劃於 2026 年底前獲得支援。請持續關注我們的版本說明，以瞭解應用程式升級與新功能。

Kaspersky Endpoint Security for Linux 支援與 Kaspersky Endpoint Detection and Response Expert (cloud) 解決方案整合。*Kaspersky Endpoint Detection and Response Expert (cloud)* 是一款基於雲端的企業網路安全解決方案，其中包含卡巴斯基應用程式，可協助組織防禦大多數類型的網路風險並涵蓋最重要的威脅傳播場景。EDR Expert (cloud) 元件部署在開放式單一管理平台 (OSMP) 上。該平台可在單一介面中運行跨平台場景，並允許將卡巴斯基應用程式與協力廠商應用程式整合到一個綜合安全系統中。

解決方案的核心要素之一是 *SIEM)*。SIEM 可追蹤來自所有元件的事件，並使用供應商和使用者定義的規則將這些事件相互關聯起來。EDR Expert (cloud) 會查看從企業基礎設施接收的日誌和遙測資料，以自動偵測攻擊，並允許使用統一調查圖來調查事件，該調查圖結合了 EDR Expert (cloud) 中收集的所有事件，包括來自卡巴斯基應用程式和協力廠商資訊安全產品的事件。

對於進階事件的回應，EDR Expert (cloud) 使用預設場景和使用者自訂場景。您還可以使用來自協力廠商應用程式的回應操作以及涉及多個應用程式的回應場景。

威脅情報工具

Kaspersky Endpoint Detection and Response 使用以下 Threat Intelligence 工具：

- 與 Kaspersky Threat Intelligence Portal 的整合，包含和顯示有關檔案和網址信譽的資訊。
- Kaspersky 威脅資料庫。
- 卡巴斯基安全網路（以下也稱為 "KSN"）雲端服務基礎架構，提供對即時檔案、網站、和來自卡巴斯基知識庫的軟體信譽資訊的存取。使用卡巴斯基安全網路的資料可確保 Kaspersky Endpoint Security 能夠更快地對威脅作出回應，提高一些防護元件的效能，並減少誤報風險。

解決方案的工作原理

Kaspersky Endpoint Security 應用程式安裝在公司 IT 基礎結構上的單個電腦上，持續監控處理程序、開啟的網路連線和被修改的檔案。

有關電腦上的事件的資訊（遙測資料）被傳送到 EDR Expert (cloud) 伺服器。在此情況下，Kaspersky Endpoint Security 也會將應用程式發現的威脅相關資訊以及這些威脅的處理結果相關資訊傳送到遙測資料收集伺服器。

EDR Expert (cloud) 整合在卡巴斯基安全管理中心主控台中配置。內建代理然後被使用開放單一管理平台 (OSMP) 進行管理，包括執行工作、管理隔離物件、檢視報告和其他操作。

EDR Expert (cloud) 的限制

- Kaspersky Endpoint Security 在 Light Agent 模式下不支援與 EDR Expert (cloud) 整合。
- EDR Expert (cloud) 不適用於搭載 Elbrus CPU 的裝置。
- EDR Expert (cloud) 不支援以 Arm 架構為基礎的裝置。
- EDR Expert (cloud) 不適用於執行 64 位元作業系統的電腦。

如何設定內建代理與 EDR Expert (cloud) 的整合

若要與卡巴斯基 Endpoint Detection and Response Expert (cloud) 解決方案整合，您需要啟用 Endpoint Detection and Response Expert (cloud) 元件，並設定與遙測資料收集伺服器及回應伺服器的連線。

遙測資料收集伺服器 是 SIEM 解決方案的一部分，用於收集、正規化、關聯、分析和儲存有關電腦上發生的事件的資訊。

回應伺服器 是一台用於接收和掃描資料、研究物件行為並發布此類研究結果的伺服器。

Endpoint Detection and Response (cloud) 與 *Endpoint Detection and Response Expert (on-premises)* 元件彼此不相容。

EDR Expert (cloud) 運作條件

若要 EDR Expert (cloud) 正常運行，必須滿足以下條件：

- Kaspersky Endpoint Detection and Response Expert (cloud) 基礎結構在您所在的地區可用。如需瞭解您所在地區是否提供 EDR Expert (cloud) 基礎架構，請聯絡技術支援。
- OSMP（Open Single Management Platform已安裝。
- Kaspersky Endpoint Security 已在 標準模式 下安裝。
- Kaspersky Endpoint Security 應用程式已啟動，功能受產品授權覆蓋。
- 您已接受 Kaspersky Endpoint Detection and Response Expert (cloud) 資料處理協議的條款。
- Endpoint Detection and Response Expert (cloud)元件已啟用。
- 已啟用用於傳輸必要遙測資料的 行為偵測 元件。
  如果您想取得其他防護元件所偵測威脅的相關資訊，請啟用這些元件：
  - 檔案威脅防護。
  - 網路威脅防護。
  - Web 威脅防護。
  - 加密軟體防護。
  - 應用程式控制。
  - 裝置控制。
  - 系統完整性監控。

與 EDR Expert (cloud) 整合的步驟

設定 EDR Expert (cloud) 整合涉及以下步驟：

1. **選擇 EDR Expert 模式**

   Kaspersky Endpoint Security 支援兩種 EDR Expert 模式：內部部署和雲端。若要與卡巴斯基 Endpoint Detection and Response Expert (cloud) 整合，您需要在 安裝應用程式 期間啟用對應的模式。預設情況下，應用程式使用 Endpoint Detection and Response Expert (on-premises) 整合。

2. **啟動 Kaspersky Endpoint Detection and Response Expert (cloud)**

   您需要單獨購買 Kaspersky Endpoint Detection and Response Expert (cloud) 的產品授權。

   為 Kaspersky Endpoint Detection and Response Expert (cloud) 新增單獨的金鑰後，該功能將可用。因此，電腦上將新增兩個金鑰：一個金鑰用於 Kaspersky Endpoint Security，一個金鑰用於 Kaspersky Endpoint Detection and Response Expert (cloud)。

   獨立 Endpoint Detection and Response Expert (cloud) 功能的授權和 Kaspersky Endpoint Security 的授權一樣。

請確定您的產品授權涵蓋 EDR Expert (cloud) 功能，且可在 卡巴斯基安全管理中心中或受防護裝置上 運作。

3 設定與遙測資料收集伺服器及回應伺服器的連線

卡巴斯基 Endpoint Detection and Response Expert (cloud) 需要在 Kaspersky Endpoint Security 與兩台伺服器之間建立受信任連線：遙測資料收集伺服器和回應伺服器。應用程式會在您接受卡巴斯基 Endpoint Detection and Response Expert (cloud) 資料處理協議的條款與條件後，自動接收用於建立受信任連線的伺服器位址和憑證。因此，您只需管理用於連線到伺服器的進階設定：是否要使用 TCP 隧道，以及向伺服器傳送同步請求的週期。

如何在網頁主控台中設定 Kaspersky Endpoint Security 連線至 EDR Expert (cloud) 的其他設定

1. 在網頁主控台的主視窗中，選擇**資產管理** → **政策**頁簽。
2. 點擊 Kaspersky Endpoint Security 政策的名稱。

   政策內容視窗將開啟。
3. 選擇"**應用程式設定**"標籤。
4. 轉到"**內置代理設定**"→"**Endpoint Detection and Response Expert (cloud)**"。
5. 使用 **Endpoint Detection and Response Expert (cloud) 已停用** 撥動開關啟用元件。
6. 如果目前政策是子政策，且父政策禁止變更 EDR Expert (cloud) 整合設定（閉合的"掛鎖"），則您可以在 **繼承** 部分配置設定繼承：
   - **繼承政策的連線設定**（預設值）。連線設定將繼承自父政策。您將無法編輯這些設定。
   - **使用自訂連線設定**您可以手動配置連線設定。
7. **回應伺服器** 索引標籤顯示回應伺服器的完全限定網域名稱和連接埠，這些資訊會得到自動檢索。如果您的基礎結構中的安全性政策不允許您直接連線到 EDR Expert (cloud) 伺服器，則可以透過 TCP 通道建立連線：
   a. 選擇"**使用 TCP 通道進行回應**"核取方塊。
   b. 請指定伺服器位址（IPv4、IPv6）和連線到通道的連接埠。
8. 如有必要，請在 **傳送同步請求到伺服器的時間間隔 (分)** 欄位中設定向伺服器傳送同步請求的頻率。在同步過程中，Kaspersky Endpoint Security 會接收威脅回應工作並傳送工作結果。
9. 轉到"**遙測資料收集伺服器**"標籤。
10. 設定遙測資料收集伺服器的連線設定：
    a. 點擊"**編輯**"連接。
    b. 這會開啟一個視窗；在該視窗中，從清單中選取遙測資料收集伺服器。KUMA 收集器在 EDR Expert (cloud) 中充當遙測資料收集伺服器。有關詳細資訊，請參閱 Kaspersky Unified Monitoring and Analysis Platform 說明。

       如果連線到遙測資料收集伺服器時發生錯誤，請選取其他伺服器。如果您無法連線到遙測資料收集伺服器，請聯絡技術支援。
    c. 如有必要，您可以透過 TCP 隧道設定與遙測資料收集伺服器的連線，就像設定回應伺服器一樣。
11. 要將此政策套用到電腦，請關閉... 掛鎖圖示並儲存變更。

如何在命令列中檢視憑證資訊

1. 若要檢視用戶端憑證的相關資訊，請執行以下命令：

```
kesl-control --query-cloudxdr-client-certificate --server-type telemetry
```

```
kesl-control --query-cloudxdr-client-certificate --server-type response
```

2. 若要檢視伺服器憑證的相關資訊，請執行以下命令：

```
kesl-control --query-cloudxdr-server-certificate --server-type telemetry
```

```
kesl-control --query-cloudxdr-server-certificate --server-type response
```

因此，Kaspersky Endpoint Security 將會以下列方式顯示憑證資訊：

```
Serial number: 12 34 56 78 AB CD EF GH
Subject: C=EN, ST=Moscow, L=Moscow, O=AO Kaspersky Lab, OU=Future Technologies, CN=epp
Issuer: C=EN, ST=Moscow, L=Moscow, O=AO Kaspersky Lab, OU=Future Technologies, CN=epp
Valid from: 2022-07-27 13:25:35
Expires on: 2072-07-14 13:25:35
SHA1 fingerprint: a14f12df23fg3465bgh6345g567df
```

透過檢視"*應用程式元件狀態報告*"來檢查元件的運行狀態。您也可以檢視受保護裝置上元件的狀態。

如何最佳化 EDR Expert (cloud) 遙測傳輸

遙測 是受防護電腦上發生的事件的清單。Kaspersky Endpoint Security 會在同步期間分析遙測資料並將其傳送至遙測資料收集伺服器。遙測事件幾乎連續不斷地到達伺服器。當滿足以下任一條件時，Kaspersky Endpoint Security 啟動與伺服器的同步：

- 同步間隔已用完。
- 緩衝區中的事件數超過上限。

因此，預設情況下，應用程式每 30 秒或每當緩衝區包含 1024 個事件時同步一次。您可以在 Kaspersky Endpoint Security 政策中配置同步行為並選擇最佳值以匹配您的網路負載（請參閱下面的說明）。

如果 Kaspersky Endpoint Security 與伺服器之間沒有連線，應用程式將對新事件進行佇列。當連線還原時，Kaspersky Endpoint Security 將以正確順序將佇列事件傳送到伺服器。為避免伺服器過載，Kaspersky Endpoint Security 可能會略過一些事件。要啟用此功能，您可以最佳化事件傳輸設定，例如，設定每小時最大事件數值（請參閱下面的說明）。

如何在網頁主控台中最佳化遙測資料傳輸

1. 在網頁主控台的主視窗中，選擇**資產管理 → 政策**頁簽。
2. 點擊 Kaspersky Endpoint Security 政策的名稱。

   政策內容視窗將開啟。
3. 選擇"**應用程式設定**"標籤。

4. 轉到"**內置代理設定**"→"**Endpoint Detection and Response Expert (cloud)**"。

5. 在開啟的視窗中選擇"**資料傳輸設定**"標籤。

6. 請確保選中**"傳送遙測資料"已啟用**核取方塊。

7. 如有需要，請停用 **僅傳送具有 IOA 的遙測** 功能。*攻擊指標 (IOA)* 是指包含系統中可疑行為（指示可能存在針對性攻擊）描述的規則。應用程式會將系統中正在進行的行為與這些規則進行比較，並記錄下指示存在針對性攻擊的事件。應用程式使用*串流掃描*技術，該技術允許即時追蹤此類事件。預設情況下，此功能已停用。

8. 如有必要，請配置伺服器同步設定：

   - **最大事件傳輸延遲時間（秒）**應用程式在同步間隔到期後與伺服器同步以傳送事件。預設設定是 30 秒。

   - **事件套件的最大數量**當緩衝區充滿事件時，應用程式會與伺服器同步。預設設定為 1024 個事件。

9. 轉到"**請求節流**"標籤。

10. 如有必要，請使用 **請求節流已啟用** 切換開關停用請求節流。

    該功能有助於最佳化伺服器負載。如果啟用此功能，應用程式會限制傳輸的事件。如果事件數量超過配置的限制，Kaspersky Endpoint Security 將停止傳送事件。預設會停用此選項。

11. 配置用於將事件傳送到伺服器的最佳化設定：

    - **每個小時的最大事件數量**如果事件流超過配置的每小時事件數限制，應用程式會分析遙測數據流並限制事件的傳送。Kaspersky Endpoint Security 在一小時後還原傳送事件。預設設定是每小時 3000 個事件。如果應用程式安裝在伺服器上，則遙測資料流會更高。對於伺服器，建議將該值增加到每小時 60,000 個事件。

    - **事件限制超過百分比 (%)**該應用程式按類型對事件進行排序（例如，"登錄檔中的變更"事件），如果相同類型的事件佔事件總數的比率超過配置的百分比限制，則限制事件的傳輸。當其他事件與事件總數的比率再次變得足夠大時，Kaspersky Endpoint Security 會還原傳送事件。預設設定為 15%。

12. 要將此政策套用到電腦，請關閉... 掛鎖圖示並儲存變更。

如何在命令列中最佳化遙測資料傳輸

1. 若要啟用傳送遙測資料，請執行以下命令：

```
kesl-control --set-settings 39 [EnableTelemetry=<Yes|No>] [TelemetrySettings.OnlyTaggedEvents=<Yes|No>]
```

2. 若要設定與伺服器的同步設定，請執行以下命令：

```
kesl-control --set-settings 39 [TelemetrySettings.EventTransferSettings.UseRequestCountLimits=<Yes|No>]
[TelemetrySettings.EventTransferSettings.MaximumDataTransferTime=<delay in sending events in seconds>]
[TelemetrySettings.EventTransferSettings.MaximumNumberOfEventsInHour=<number of events>]
[TelemetrySettings.EventTransferSettings.MaximumNumberOfEventsInPackage=<number of event packages>]
[TelemetrySettings.EventTransferSettings.EventLimitExceededPercentage=<percentage of exceeding the event
limit>]
```

設定	描述
`EnableTelemetry`	將裝置上事件的相關資料（遙測資料）傳送到 OSMP 遙測資料收集伺服器。 預設會啟用遙測傳送 (`Yes`)。
`TelemetrySettings.OnlyTaggedEvents`	僅傳送含 IOA 的遙測資料。*攻擊指標 (IOA)* 是指包含系統中可疑行為（指示可能存在針對性攻擊）描述的規則。應用程式會將系統中正在進行的行為與這些規則進行比較，並記錄下指示存在針對性攻擊的事件。應用程式使用*串流掃描*技術，該技術允許即時追蹤此類事件。 預設會停用僅傳送含 IOA 的遙測資料 (`No`)。
`[TelemetrySettings.EventTransferSettings]` 區段包含用於連線至 OSMP 遙測伺服器的一般設定。	
`UseRequestCountLimits`	請求節流。該功能有助於最佳化伺服器負載。如果啟用此功能，應用程式會限制傳輸的事件。如果事件數量超過配置的限制，Kaspersky Endpoint Security 將停止傳送事件。 預設會停用此選項。
`MaximumDataTransferTime`	最大事件傳輸延遲時間（秒）。應用程式在同步間隔到期後與伺服器同步以傳送事件。預設設定是 30 秒。
`MaximumNumberOfEventsInHour`	每個小時的最大事件數量。如果事件流超過配置的每小時事件數限制，應用程式會分析遙測數據流並限制事件的傳送。Kaspersky Endpoint Security 在一小時後還原傳送事件。預設設定是每小時 3000 個事件。如果應用程式安裝在伺服器上，則遙測資料流會更高。對於伺服器，建議將該值增加到每小時 60,000 個事件。
`MaximumNumberOfEventsInPackage`	套件中的事件數量上限。當緩衝區充滿事件時，應用程式會與伺服器同步。預設設定為 1024 個事件。
`EventLimitExceededPercentage`	事件限制超過百分比 (%)。該應用程式按類型對事件進行排序（例如，“登錄檔中的變更”事件），如果相同類型的事件佔事件總數的比率超過配置的百分比限制，則限制事件的傳輸。當其他事件與事件總數的比率再次變得足夠大時，Kaspersky Endpoint Security 會還原傳送事件。預設設定為 15%。

如何設定 EDR Expert (cloud) 遙測資料排除項目

為了提高效能並最佳化到遙測資料收集伺服器的資料傳輸，您可以新增遙測排除項目。例如，您可以選擇不傳送單個應用程式的網路通訊資料。

> 使用過多規則可能會增加遙測資料收集伺服器的負載，並降低電腦效能。我們建議只新增必要的規則。

若要在網頁主控台中建立遙測資料排除項目：

1. 在網頁主控台的主視窗中，選擇**資產管理 → 政策**頁簽。
2. 點擊 Kaspersky Endpoint Security 政策的名稱。
   政策內容視窗將開啟。
3. 選擇“**應用程式設定**”標籤。
4. 轉到”**一般設定**”→”**遙測設定**”。
5. 選擇“**EDR Expert（雲端）遙測**”標籤。
6. 在”**一般排除項目**”塊中，點擊”**新增**”按鈕。
   這將開啟用於新增遙測資料排除規則的視窗。

7. 設定遙測資料排除規則：

   a. 如有必要，可變更規則的狀態。預設情況下規則已啟用。

   b. 輸入規則的名稱。

   c. 選擇觸發規則時要執行的操作：

      - **不收集**篩選的事件將被從傳送的遙測資料中排除。

      - **排除 IOA**IOA 規則觸發事件將被從傳送的遙測資料中排除。*攻擊指標 (IOA)* 是指包含系統中可疑行為（指示可能存在針對性攻擊）描述的規則。應用程式會將系統中正在進行的行為與這些規則進行比較，並記錄下指示存在針對性攻擊的事件。應用程式使用*串流掃描*技術，該技術允許即時追蹤此類事件。

   d. 如果選擇 **排除 IOA** 選項，請指定要新增至排除項目的 IOA 規則：

      - **全部排除**當滿足指定條件時，應用程式將從遙測資料中排除基於所有 IOA 規則產生的事件。

      - **依照 GUID 排除**指定 IOA 規則的 GUID。您可以使用 `,` 指定多個 GUID。有關 IOA 規則的更多詳細資訊，請參閱... EDR Expert (cloud) 說明。

   e. 指定篩選條件：

   如有必要，您可以使用 **AND**、**OR** 和 **NOT** 運算子，新增多個篩選條件和條件群組，以建立複雜的篩選準則。您也可以向條件群組中新增嵌套條件和條件群組。

8. 如有必要，在**所有事件類型**下，依事件類型新增遙測排除項目。

   a. 點擊事件類型名稱。

   b. 在開啟的視窗中，點擊"**手動設定**"按鈕。

   c. 在"**排除規則**"塊中，點擊"**新增**"按鈕。

      這將開啟用於新增遙測資料排除規則的視窗。在遙測資料排除規則中，已預先設定與事件類型相對應的 `EventType` 篩選條件。

   d. 指定篩選條件：

9. 若要將政策套用至電腦，請確保掛鎖已關閉 (🔒)，然後儲存變更。

如何匯出或匯入 EDR Expert (cloud) 事件篩選器

您可以將排除項目清單匯出到 JSON 檔案。然後，您可以修改檔案，例如，新增大量事件 ID。您還可以使用匯出/匯入功能來備份事件篩選器，或將清單遷移到其他伺服器。

> 使用過多規則可能會增加遙測資料收集伺服器的負載，並降低電腦效能。我們建議只新增必要的規則。

在網頁主控台中匯出和匯入事件篩選器：

1. 在網頁主控台的主視窗中，選擇**資產管理 → 政策**頁簽。
2. 點擊 Kaspersky Endpoint Security 政策的名稱。
   政策內容視窗將開啟。
3. 選擇“**應用程式設定**”標籤。
4. 轉到”**一般設定**”→”**遙測設定**”。
5. 選擇“**EDR Expert（雲端）遙測**”標籤。
6. 若要匯出事件篩選器：
   a. 點擊“**匯出**”。
   b. 在開啟的視窗中，指定您要將事件篩選器匯出到的 JSON 檔案的名稱，然後選取要儲存此檔案的資料夾。
   c. 儲存檔案。
      Kaspersky Endpoint Security 會將事件篩選器匯出到 JSON 檔案。
7. 若要匯入事件篩選器：
   a. 點擊“**匯入**”。
   b. 在開啟的視窗中，選取要從中匯入事件篩選器的 JSON 檔案。
   c. 選擇您希望如何匯入事件篩選規則：新增至現有規則或丟棄現有規則並以新規則取代。
   d. 開啟檔案。
8. 若要將政策套用至電腦，請確保掛鎖已關閉 (🔒)，然後儲存變更。
   1. 在網頁主控台的主視窗中，選擇**資產管理 → 政策**頁簽。
   2. 點擊 Kaspersky Endpoint Security 政策的名稱。
      政策內容視窗將開啟。
   3. 選擇“**應用程式設定**”標籤。
   4. 轉到”**一般設定**”→”**遙測設定**”。
   5. 選擇“**EDR Expert（雲端）遙測**”標籤。
   6. 若要匯出事件篩選器：
      a. 點擊“**匯出**”。
      b. 在開啟的視窗中，指定您要將事件篩選器匯出到的 JSON 檔案的名稱，然後選取要儲存此檔案的資料夾。
      c. 儲存檔案。
         Kaspersky Endpoint Security 會將事件篩選器匯出到 JSON 檔案。

7. 若要匯入事件篩選器：

   a. 點擊“**匯入**”。

   b. 在開啟的視窗中，選取要從中匯入事件篩選器的 JSON 檔案。

   c. 選擇您希望如何匯入事件篩選規則：新增至現有規則或丟棄現有規則並以新規則取代。

   d. 開啟檔案。

8. 若要將政策套用至電腦，請確保掛鎖已關閉 (🔒)，然後儲存變更。

Kaspersky Anti Targeted Attack Platform

Kaspersky Anti Targeted Attack Platform 是一種解決方案，用於保護組織的 IT 基礎架構，並及早偵測零時差攻擊、針對性攻擊和進階持續性威脅（以下亦稱為 APT）等威脅。有關解決方案的詳細資訊，請參閱 Kaspersky Anti Targeted Attack Platform 說明。

Kaspersky Endpoint Security 應用程式可以與 Kaspersky Anti Targeted Attack Platform 上的以下元件整合：

Kaspersky Endpoint Detection and Response (KATA)

此元件可防護組織本機網路中的裝置。與 Kaspersky Endpoint Detection and Response (KATA) 整合時，Kaspersky Endpoint Security 會執行以下功能：

- 將裝置上事件的資訊（遙測）傳送到提供與 Kaspersky Endpoint Detection and Response (KATA) 互動的中央節點伺服器（以下亦稱為 *KATA 伺服器*）。

  Kaspersky Endpoint Security 會將處理程序、開啟的網路連線和已修改檔案的監控資料傳送到中央節點元件，以及應用程式偵測到的威脅資料和處理這些威脅的結果資料。

- 收到 Kaspersky Anti Targeted Attack Platform 的指令時，執行 威脅回應操作 以確保安全。

支援與 Kaspersky Endpoint Detection and Response (KATA) 7.1 及更早版本整合。

Network Detection and Response (KATA)

此元件可防護組織的內部網路。與 Kaspersky Network Detection and Response (KATA) 整合時，Kaspersky Endpoint Security 可以將有關裝置事件的資訊（遙測）傳送到提供與 Kaspersky Network Detection and Response (KATA) 互動的 Central Node 伺服器（以下也稱為 *NDR 伺服器*）。

Sandbox

Kaspersky Endpoint Security 應用程式會將檔案傳送到處理與 沙盒 互動的中央節點伺服器以進行掃描。

Kaspersky Endpoint Security 的以下元件可實現與 Kaspersky Anti Targeted Attack Platform 整合：

- Endpoint Detection and Response Expert (on-premises)，以下亦稱為 *EDR Expert (on-premises)*。

  從 Kaspersky Endpoint Security 12.4 for Linux 開始，Endpoint Detection and Response (KATA) 元件已重新命名為 Endpoint Detection and Response Expert (on-premises)。現在，此元件不僅可與 Kaspersky Anti Targeted Attack Platform 的元件 Kaspersky Endpoint Detection and Response (KATA) 整合，還可與 Kaspersky Endpoint Detection and Response Expert (on-premises) 解決方案整合。

- Network Detection and Response (KATA)，以下亦稱為 *NDR (KATA)*。
- 沙盒。

您可以配置 Kaspersky Endpoint Security 與 Kaspersky Anti Targeted Attack Platform 解決方案的所有元件的整合，也可以單獨配置與每個元件的整合。

此元件不適用於搭載 Elbrus CPU 的裝置。

配置 Kaspersky Anti Targeted Attack Platform 整合

先決條件

在配置 Kaspersky Network Detection and Response (KATA) 整合之前，請允許連接埠 8085 上的連線。

在配置與 Kaspersky Endpoint Detection and Response (KATA) 元件的整合之前：

- 允許透過連接埠 443、8443 進行連線。
- 啟用 行為偵測 元件，以傳輸必要的遙測資料。

  行為分析元件可用於核心版本 3.13 及更新版本的裝置。

  如果您想取得其他防護元件所偵測威脅的相關資訊，請啟用這些元件：

  - 檔案威脅防護。
  - 網路威脅防護。
  - Web 威脅防護。
  - 加密軟體防護。
  - 應用程式控制。
  - 裝置控制。
  - 系統完整性監控。

啟用 eBPF 網路流量攔截模式可使遙測資料更全面。eBPF 技術可用於執行支援 eBPF、核心版本 4.18 或更新版本之 64 位元作業系統的電腦。

建議您檢查電腦是否支援傳送遙測資料所需的元件。

- 如果您已購買單獨的產品授權來使用此功能，請將 EDR Expert (on-premises) 產品授權金鑰新增至應用程式。

  如果您是依據包含卡巴斯基 Endpoint Detection and Response Expert (on-premises) 的產品授權使用 Kaspersky Endpoint Security，則無須執行任何操作。

  如果您在 Light Agent 模式下使用 Kaspersky Endpoint Security，則需要將用於啟動附加功能的產品授權金鑰新增至 SVM。

必要設定步驟

1. **取得並處理由中央節點伺服器簽發的憑證**

   與 Kaspersky Anti Targeted Attack Platform 整合時，執行 Kaspersky Endpoint Security 的裝置會與提供整合的 Central Node 伺服器建立加密的 HTTPS 連線。

   如果 Kaspersky Endpoint Security 的一般設定規定必須使用代理伺服器，則與處理Kaspersky Anti Targeted Attack Platform 元件互動的伺服器的連線將透過代理伺服器建立。

   用於保護處理與 Kaspersky Anti Targeted Attack Platform 解決方案的元件進行互動的伺服器連線的憑證必須由 Kaspersky Anti Targeted Attack Platform 管理員提供。

   若要處理憑證，請依照 將 PFX 憑證轉換為 PEM 格式一文中說明的步驟操作。

   您可以使用伺服器憑證和/或用戶端憑證。選擇取決於貴組織的安全政策。

2. **配置 Kaspersky Anti Targeted Attack Platform 整合設定**

   您可以透過以下方式進行設定：

   - 使用網頁主控台（卡巴斯基安全管理中心主控台和/或 OSMP 主控台 中的 EDR (KATA) 和 NDR (KATA)）。
   - 使用卡巴斯基安全管理中心管理主控台（EDR (KATA) 和 NDR (KATA)）。
   - 使用命令列（EDR (KATA) 和 NDR (KATA)）。

3. **確認已成功建立與 Kaspersky Anti Targeted Attack Platform 的連線。**

   請以任何方便的方式檢查 Kaspersky Anti Targeted Attack Platform 元件的狀態。

4. **必要時管理其他設定**

   - 如果您的作業系統上將 SELinux 設定為 Enforcing 模式，則還需要額外設定 SELinux 以執行回應操作。
   - 檢閱網路隔離的限制。

如何配置 EDR (KATA) 整合

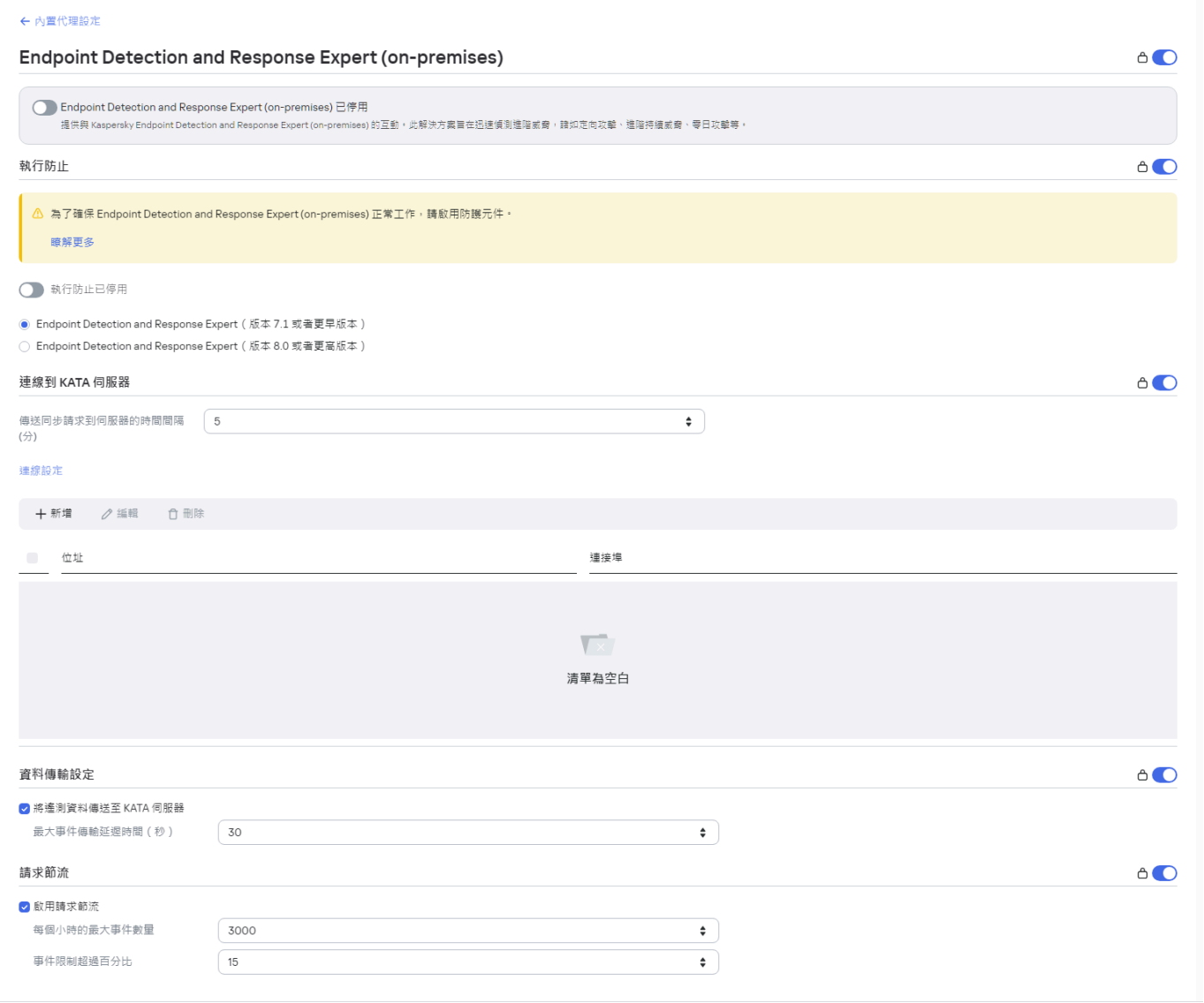
在網頁主控台中，您可以啟用或停用 Kaspersky Endpoint Detection and Response (KATA) 元件，並設定 Kaspersky Endpoint Security 應用程式與此元件的整合。

如何在網頁主控台中設定 Kaspersky Endpoint Detection and Response (KATA) 整合

1. 在網頁主控台的主視窗中，選擇**資產管理 → 政策**。
2. 點擊 Kaspersky Endpoint Security 政策的名稱。
   政策內容視窗將開啟。
3. 選擇“**應用程式設定**”標籤。
4. 在開啟的政策內容視窗中，選取 **應用程式設定** 標籤。
5. 前往 **內置代理設定 → Endpoint Detection and Response Expert (on-premises)**。
6. 在畫面右側：
   a. 選取 **Endpoint Detection and Response Expert 7.1 或更早版本** 選項。
   b. 在 **與遙測資料收集伺服器的連線** 區段中，按一下工具列中的 **新增** 按鈕，然後按一下 **選取伺服器**，以選取遙測資料收集伺服器。
   c. 在 **與回應伺服器的連線** 區段中，按一下工具列中的 **新增** 按鈕，然後按一下 **選取伺服器**，以選取回應伺服器。
   d. 按一下 **與遙測資料收集伺服器的連線** 和 **與威脅回應伺服器的連線** 區段中的 **連線設定** 連結，然後在顯示的窗格中：
      1. 按一下 **上傳** 按鈕，以新增伺服器憑證。
      2. 如果您需要額外保護，請建立加密容器。
         若要執行此操作，請在 **額外連線保護** 區段中：
         - 選取 **使用雙向身分驗證** 核取方塊。
         - 按一下 **上傳** 按鈕，並新增您在主要情境步驟 1 中取得的用戶端憑證。
         - 在對應欄位中輸入加密容器的密碼。

         加密容器密碼 欄位為必填。若未輸入用戶端憑證（加密容器）的密碼，您無法儲存設定。

7. 要將此政策套用到電腦，請關閉... 🔒掛鎖圖示並儲存變更。



Endpoint Detection and Response Expert (on-premises)

如何透過指令列設定 Kaspersky Endpoint Detection and Response (KATA) 整合

1. 若要選取 EDR (KATA) 整合模式，請執行下列指令：

```
kesl-control --set-settings 24 Mode=EDRKATA
```

2. 若要新增 Central Node 伺服器，請執行下列指令：

```
kesl-control --set-settings 24 Endpoints.item_001.Address=<central node server address>
Endpoints.item_001.Port=<central node server port>
```

3. 若要新增回應伺服器憑證，請執行下列指令：

```
kesl-control [-R] --add-kataedr-server-certificate <file>
```

4. 若要設定整合設定，請執行下列指令：

```
kesl-control --set-settings 24 [<setting name>=<setting value>]
```

設定及其可能值列於下表。

5. 若要新增用於連線至回應伺服器的用戶端憑證，請執行下列指令：

```
kesl-control [-R] --add-kataedr-server-certificate <file>
```

6. 若要啟用與 EDR (KATA) 的整合，請執行下列指令：

```
kesl-control --start-task 24
```

Kaspersky Endpoint Detection and Response (KATA) 整合設定

設定	描述	值
Mode	整合模式。 對於 Kaspersky Endpoint Detection and Response Expert (on-premises) 整合，Kaspersky Endpoint Security 應用程式會與 OSMP 平台上的伺服器互動。 對於 Kaspersky Endpoint Detection and Response (KATA) 整合，Kaspersky Endpoint Security 安全應用程式與 Kaspersky Anti Targeted Attack Platform 上的伺服器進行互動。	EDRKATA（預設）是 EDR (KATA) 整合模式。允許啟用與 Kaspersky Endpoint Detection and Response (KATA) 整合，Kaspersky Endpoint Detection and Response (KATA) 是 Kaspersky Anti Targeted Attack Platform 的元件。 EDRExpertOnPrem 是 EDR Expert (on-premises) 整合模式。啟用 Kaspersky Endpoint Detection and Response Expert (on-premises) 整合
UseClientPinnedCertificate	啟用和停用雙向身分驗證以進一步防護與 KATA 伺服器的連線。 如果在 KATA 伺服器端啟用了雙向身分驗證，您需要在 *Kaspersky Endpoint Detection and Response Expert (on-premises) 整合* 工作的設定中啟用雙向身分驗證，並在啟動工作之前新增用戶端憑證。	Yes – 使用雙向身分驗證進一步防護與 KATA 伺服器的連線。 No（預設值）— 不使用雙向身分驗證。
SynchronizationPeriod	向 KATA 伺服器傳送同步請求的頻率（以分鐘為單位）。	預設值：5。
ConnectionTimeout	等待連線到 KATA 伺服器的最長時間（秒）。	預設值：10。
RequestTimeout	等待 KATA 伺服器回應的最長時間（秒）。	預設值：10。
EnableTelemetry	將事件資料（遙測）傳送至 KATA。	Yes（預設值）– 將遙測資料傳送到 KATA 伺服器。 No 停用傳送遙測資料。
[Endpoints.item_#]部分包含 KATA 伺服器的位址和連接埠。您可以新增多個伺服器。		
Address	KATA 伺服器位址 可指定 Integration Server 的 IP 位址（IPv4 或 IPv6）或完全限定網域名稱 (FQDN)。 為確保在裝置上啟用網路隔離的情況下應用程式發生故障時與伺服器的通訊不會中斷，我們建議指定伺服器的 IP 位址。	預設值：127.0.0.1。
Port	連線 KATA 伺服器的連線埠。	預設值：443。
[EventTransferSettings]部分包含將資料傳送到 KATA 伺服器的設定。		
MaximumDataTransferTime	向 KATA 伺服器傳送事件的最大延遲（以秒為單位）。	預設值：30。
UseRequestCountLimits	啟用和停用調節傳送到 KATA 伺服器的事件數量。	Yes（預設值）— 調節傳送的事件數量。 No — 不調節事件的數量。

設定	描述	值
MaximumNumberOfEventsInHour	每小時的最大事件數量	預設值：3000。
MaximumNumberOfEventsInPackage	一個套件中的最大事件數量。	預設值：1024。
EventLimitExceededPercentage	事件數量超過限制（百分比）。如果某種類型的事件佔事件總數的比例超過配置的閾值（百分比），則傳送事件會受到限制。	預設值：15。

如果您使用網頁主控台或命令列，若要與 Kaspersky Endpoint Detection and Response (KATA) 整合，您需要在 EDR Expert (on-premises) 元件的設定中選取 *EDR (KATA)* 整合模式：

- 如果您使用網頁主控台，請在政策設定中選取 **Endpoint Detection and Response Expert（版本 7.1 或者更早版本）** 選項。若要在裝置上設定與 Kaspersky Endpoint Detection and Response (KATA) 的整合，您需要在網頁主控台中針對任一版本（版本 8.0 及更新版本，以及版本 7.1 及更舊版本）管理「掛鎖」。
- 如果您使用命令列，請在工作設定中設定`Mode=EDRKATA`。

如何配置 NDR (KATA) 整合

在網頁主控台中，您可以啟用或停用 Kaspersky Network Detection and Response (KATA) 元件，並設定 Kaspersky Endpoint Security 應用程式與此元件的整合。

如何在網頁主控台中設定 Kaspersky Network Detection and Response (KATA) 整合

1. 在網頁主控台的主視窗中，選擇**資產管理** → **政策**。
2. 點擊 Kaspersky Endpoint Security 政策的名稱。
   政策內容視窗將開啟。
3. 選擇“**應用程式設定**”標籤。
4. 前往 **內置代理設定** → **Network Detection and Response (KATA)**。
5. 啟用 **Network Detection and Response (KATA)** 切換開關。
6. 點擊“**連線設定**”。
7. 配置伺服器連線：
   - **逾時（秒）**中央節點伺服器響應最大超時。當超時用完時，Kaspersky Endpoint Security 會嘗試連線到不同的中央節點伺服器。
   - **伺服器憑證**用於與中央節點伺服器建立可信連線的 TLS 憑證。您可以在 Kaspersky Anti Targeted Attack Platform 主控台中獲取 TLS 憑證（請參閱 Kaspersky Anti Targeted Attack Platform 說明）。

- **使用雙向身分驗證**在 Kaspersky Endpoint Security 和中央節點伺服器之間建立安全連線時進行雙向身分驗證。要使用雙向身分驗證，您需要在中央節點伺服器設定中啟用雙向身分驗證，然後獲取加密容器並設定密碼以防護加密容器。*加密容器*是一個帶有憑證和私鑰的 PFX 存檔。您可以在 Kaspersky Anti Targeted Attack Platform 主控台中獲得一個加密容器（請參閱 Kaspersky Anti Targeted Attack Platform 說明）。配置中央節點設定後，您還需要在 Kaspersky Endpoint Security 設定中啟用雙向身分驗證並加載受密碼防護的加密容器。

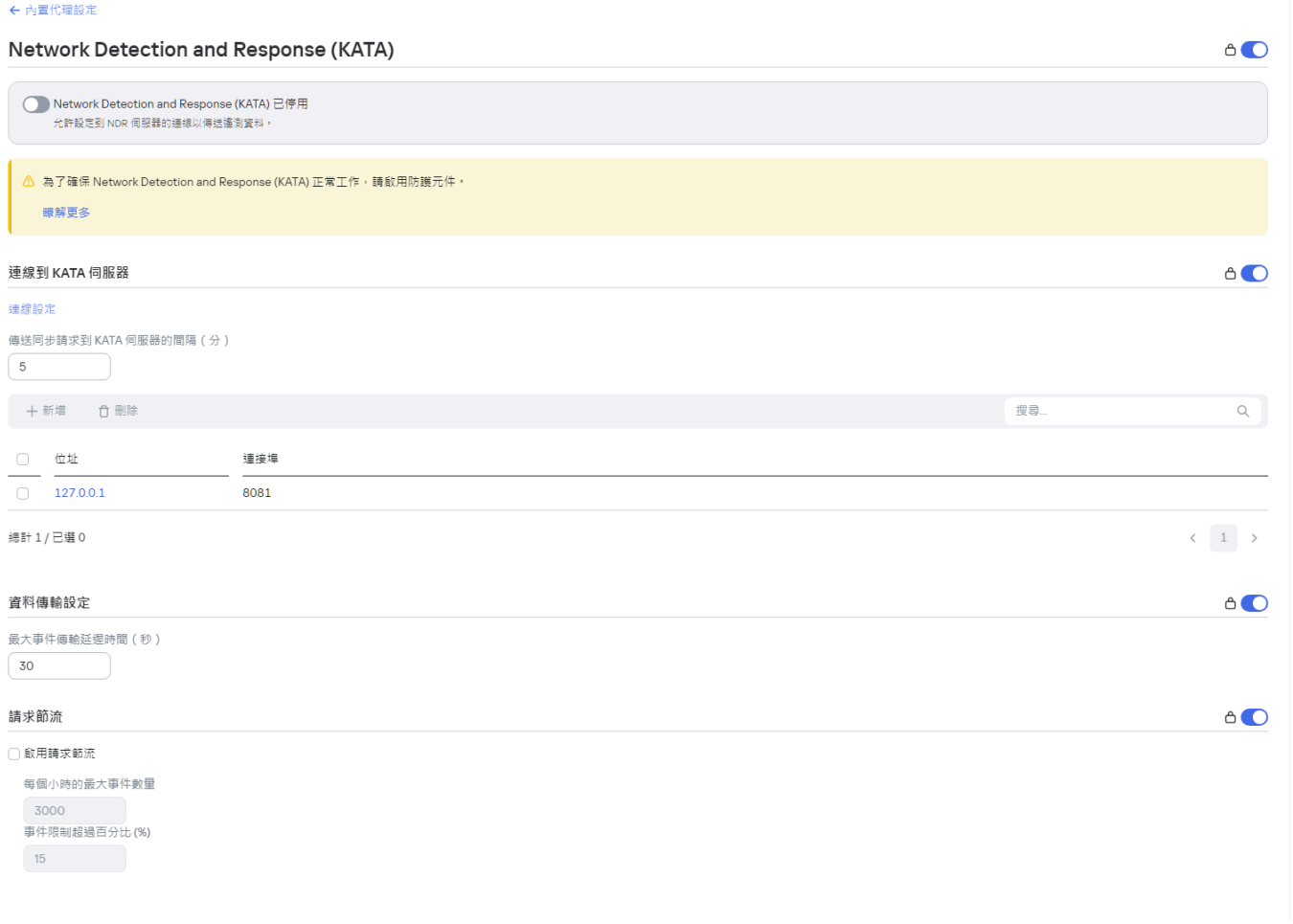
> 加密容器必須受密碼防護。無法新增密碼為空的加密容器。

8. 點擊"**確定**"。

9. 新增中央節點伺服器。為此，請指定伺服器位址（IPv4、IPv6）和連線到伺服器的連接埠。

10. 您可以新增多個中央節點伺服器位址。Kaspersky Endpoint Security 嘗試使用第一個 IP 位址連線到伺服器。如果無法建立連線，Kaspersky Endpoint Security 將嘗試使用清單中的第二個 IP 位址進行連線，依此類推。

11. 要將此政策套用到電腦，請關閉... 掛鎖圖示並儲存變更。



Network Detection and Response (KATA)

如何透過指令列設定 Kaspersky Network Detection and Response (KATA) 整合

1. 若要新增 Central Node 伺服器，請執行下列指令：

```
kesl-control --set-settings 31 Endpoints.item_001.Address=<cenral node server address> Endpoints.item_001.Port=
<central node server port>
```

2. 若要新增回應伺服器憑證，請執行下列指令：

```
kesl-control [-R] --add-katandr-server-certificate <file>
```

3. 若要設定整合設定，請執行下列指令：

```
kesl-control --set-settings 31 [<setting name>=<setting value>]
```

設定及其可能值列於下表。

4. 若要新增用於連線至回應伺服器的用戶端憑證，請執行下列指令：

```
kesl-control [-R] --add-katandr-server-certificate <file>
```

5. 若要啟用與 NDR (KATA) 的整合，請執行下列指令：

```
kesl-control --start-task 31
```

Kaspersky Network Detection and Response (KATA) 整合工作設定

設定	描述	值
UseClientPinnedCertificate	啟用和停用雙向身分驗證以進一步防護與 NDR 伺服器的連線。 如果在 NDR 伺服器端啟用了用戶端憑證驗證，請在啟動*Kaspersky NetworkDetection and Response (KATA) 整合*工作之前啟用用戶端憑證使用並新增用戶端憑證。	Yes – 使用雙向身分驗證進一步防護與 NDR 伺服器的連線。 No（預設值）— 不使用雙向身分驗證。
SynchronizationPeriod	向 NDR 伺服器傳送同步請求的頻率（以分鐘為單位）。	預設值：5。
ConnectionTimeout	等待連線到 NDR 伺服器的最長時間（秒）。	預設值：10。
RequestTimeout	等待 NDR 伺服器回應的最長時間（秒）。	預設值：10。
[Endpoints.item_#]部分包含 NDR 伺服器的位址和連接埠。		
Address	NDR 伺服器位址 可指定 Integration Server 的 IP 位址（IPv4 或 IPv6）或完全限定網域名稱 (FQDN)。	預設值：127.0.0.1。
Port	連線 NDR 伺服器的連線埠。	預設值：8081。
[EventTransferSettings]部分包含將事件傳送到 NDR 伺服器的設定。		
MaximumDataTransferTime	向 NDR 伺服器傳送事件的最大延遲（以秒為單位）。	預設值：30。
MaximumNumberOfEventsInPackage	一個套件中的最大事件數量。	預設值：1024。
UseRequestCountLimits	啟用和停用調節傳送到 NDR 伺服器的事件數量。	Yes（預設值）— 調節傳送的事件數量。 No — 不調節事件的數量。
MaximumNumberOfEventsInHour	每小時的最大事件數量	預設值：3000。
EventLimitExceededPercentage	事件節流閾（百分比）。如果某種類型的事件佔事件總數的比例超過配置的閾值（百分比），則傳送事件會受到限制。	預設值：15。
PingPeriod	NDR 伺服器輪詢週期（秒）。	預設值：450。

如何驗證 KATA 整合已啟動並正在執行

您可以透過以下方式測試 Kaspersky Anti Targeted Attack Platform 元件：

- 在命令列上使用以下命令：

  ```
  kesl-control --app-info
  ```

  針對與 EDR (on-premises) 和 NDR (KATA) 元件的整合，會顯示**可用且正在執行**狀態。

- 在網頁主控台中：
  - 在卡巴斯基安全管理中心主控台中，使用*應用程式元件狀態報告*。關於報告的詳細資訊，請參閱卡巴斯基安全管理中心說明。
  - 在 OSMP 主控台中：
    - 使用*應用程式元件狀態報告*。
    - 前往**資產管理** → **資產**區段，選取 **分析與回應**索引標籤。

      該裝置會在清單中顯示，其遙測狀態為 **正常活動**。
    - 前往 **威脅搜尋**區段。

      來自該裝置的遙測事件會顯示在事件清單中。
- 在 Kaspersky Anti Targeted Attack Platform 中：

  前往**資產** → **裝置**區段。裝置會顯示在表格中。如有需要，您可以依**EPP 應用程式**、**EPP 連線**、**上次連線至 EPP**篩選表格。

  按一下裝置名稱會開啟窗格。在**端點代理程式**區段中，連線狀態為**作用中**。

Sandbox

Sandbox 技術能夠分析和掃描部署了作業系統虛擬映像的特殊伺服器上的物件，以偵測惡意活動和針對企業 IT 基礎架構的定向攻擊指標。

Kaspersky Endpoint Security 應用程式可以透過開放單一管理平台 (OSMP) 或 Kaspersky Anti Targeted Attack Platform 與沙盒進行互動。

> 此元件不適用於搭載 Elbrus CPU 的裝置。

如何設定 Sandbox 整合

開始設定 Sandbox 整合之前：

- 允許下列入站和出站連線：
  - 入站（管理介面）：
    - TCP 22
    - TCP 443
    - TCP 8443
  - 出站（管理介面）：
    - TCP 80 或 TCP 443
  - 出站及對應的入站方向（用於存取已處理物件的介面）：
    任何連接埠。
- 如果您想從檔案或目錄的快顯功能表手動將檔案傳送至沙盒，請安裝圖形介面（kesl-gui 套件）。

必要設定步驟

1. **在平台中建立沙盒伺服器連線請求，然後在沙盒管理主控台中確認連線**

   如需詳細資訊，請參閱各解決方案的說明：

   - Kaspersky Anti Targeted Attack Platform
   - Open Single Management Platform

   以任何方便的方式儲存沙盒伺服器的 IP 位址。後續設定整合時將會需要用到此位址。

2. **取得並處理由 OSMP 伺服器或 中央節點 伺服器簽發的憑證**

   與 Sandbox 整合時，執行 Kaspersky Endpoint Security 的裝置會與 Integration Server 建立加密的 HTTPS 連線。

   > 如果在 Kaspersky Endpoint Security 應用程式的一般設定中配置了代理伺服器，則將使用代理伺服器連線到處理與 Sandbox 活動的伺服器。

   用於防護與處理 Sandbox 互動的伺服器連線的憑證必須由 OSMP 平台或 Kaspersky Anti Targeted Attack Platform 的管理員提供。

   若要處理憑證，請依照 將 PFX 憑證轉換為 PEM 格式一文中說明的步驟操作。

   您可以使用伺服器憑證和/或用戶端憑證。選擇取決於貴組織的安全政策。

3. **管理 Sandbox 整合設定**

   若要傳送檔案進行掃描，您必須啟用與 KATA Sandbox 的整合並新增部署在解決方案內的中央節點伺服器。

如何在網頁主控台中設定 Sandbox 整合

1. 在網頁主控台的主視窗中，選擇**資產管理 → 政策**。
2. 點擊 Kaspersky Endpoint Security 政策的名稱。
   政策內容視窗將開啟。
3. 選擇"**應用程式設定**"標籤。
4. 轉到"**內置代理設定**"→"**Sandbox**"。
5. 在 **用於掃描的檔案提交類型** 下拉式清單中，選取所需的方法：
   - **手動**在此模式下，您可以使用命令手動或從 **在 Sandbox 中掃描** 內容功能表，將物件傳送至 Sandbox 進行掃描。

     > 如果您的 Sandbox 版本低於 8.0，建議選取此類型。

   - **自動**應用程式會自動傳送物件進行掃描，無法手動傳送物件到 Sandbox 進行掃描。
   - **組合**應用程式會自動傳送物件進行掃描，但您也可以使用命令或圖形介面手動將物件傳送到 Sandbox。
6. 在 **連線到 Sandbox 伺服器** 區段中：
   - 按一下工具列中的 **新增** 按鈕，以新增 Integration Server。
     您可以指定 KATA / OSMP 平台的 IP 位址或其 FQDN 作為位址。

     > 如果沙盒伺服器已連線至 OSMP，則只能指定代理程式伺服器的 FQDN。

   - 新增您在主要案例第 2 步收到的 Kaspersky Anti Targeted Attack Platform 或 OSMP 的伺服器憑證。
     若要執行此操作，請按一下 **伺服器連線設定** 連結，然後在顯示的窗格中，於 **伺服器 TLS 憑證** 區段中，按一下 **上傳** 按鈕。
   - 如果您需要額外保護，請建立加密容器。
     若要執行此操作，請在 **附加連線安全** 區段中：
     - 選擇"**使用雙向身分驗證**"核取方塊。
     - 按一下 **上傳** 按鈕並新增用戶端憑證。
     - 在對應欄位中輸入加密容器的密碼。

     > **加密容器密碼** 欄位為必填欄位。若未輸入用戶端憑證（加密容器）的密碼，您無法儲存設定。

7. 在“**偵測到威脅後的動作**”塊中選擇相關操作：

- **將副本移動到隔離區，刪除物件**如果選擇該選項，Kaspersky Endpoint Security 會刪除在電腦上發現的惡意物件。在刪除物件之前，Kaspersky Endpoint Security 會建立該物件的備份副本，以便您稍後需要時還原物件。Kaspersky Endpoint Security 會將備份副本移動到隔離。

- **執行關鍵區域掃描**如果選擇該選項，Kaspersky Endpoint Security 將執行“*關鍵區域掃描*工作”。預設情況下，Kaspersky Endpoint Security 會掃描核心記憶體、執行中的處理程序和開機磁區。

- **建立 IOC 掃描工作**如果選擇該選項，Kaspersky Endpoint Security 會自動建立 *IOC 掃描（IOC 自動掃描工作）*。對於此工作，您可以配置執行模式、掃描範圍，以及偵測到 IOC 時的動作（*將副本移動到隔離區，刪除物件* 或 *執行關鍵區域掃描*）。若要修改 “*IOC 掃描*”工作的其它設定，請前往工作設定。

8. 如有必要，在**IOC 掃描範圍**塊中配置*IOC 掃描*工作設定。

- **關鍵檔案區域**如果選取此選項，Kaspersky Endpoint Security 只會在使用者和系統目錄中掃描 IOC。

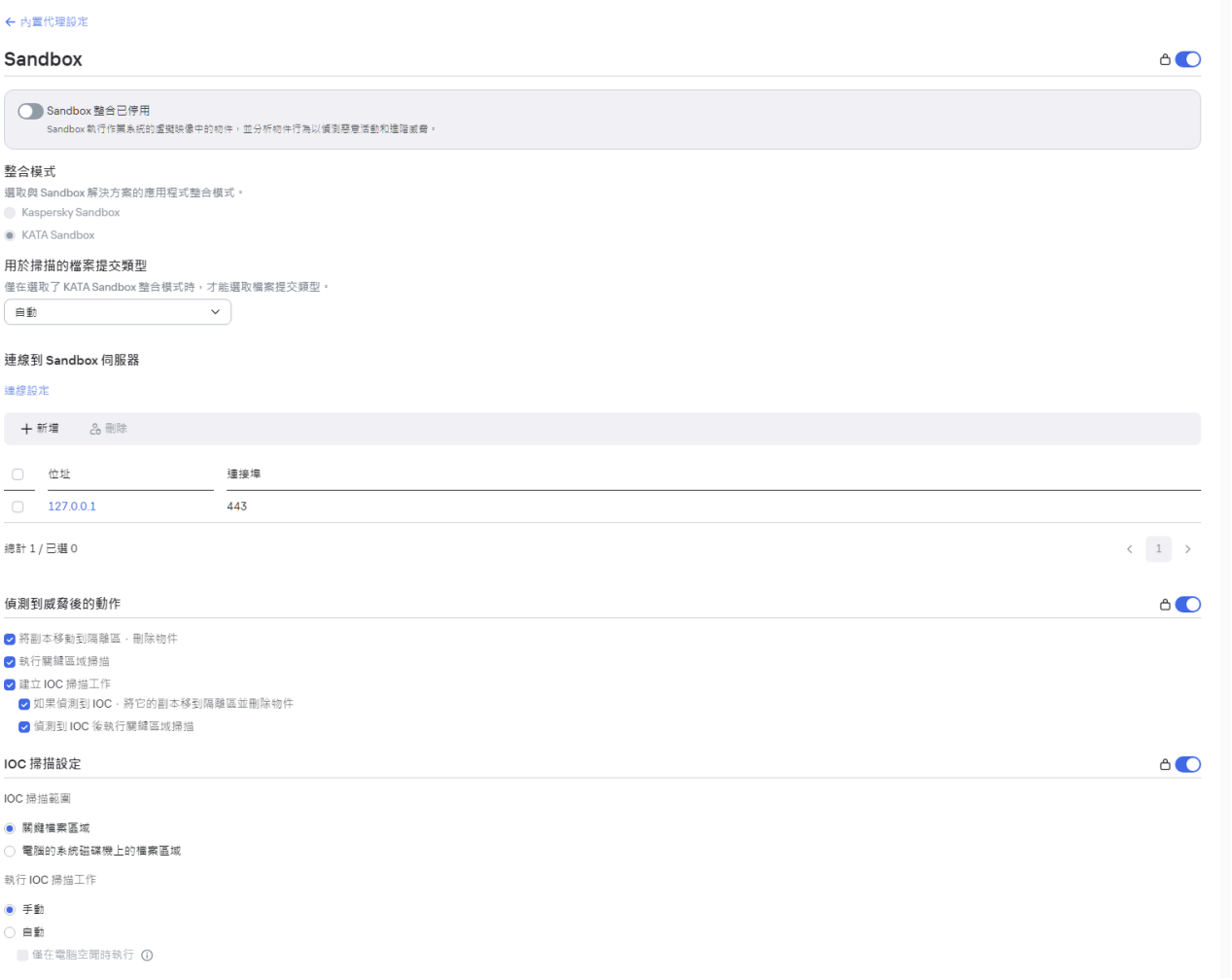
- **電腦的系統磁碟機上的檔案區域**如果選取此選項，Kaspersky Endpoint Security 會掃描根檔案系統中的所有檔案是否存在 IOC。

9. 如有必要，在**執行 IOC 掃描工作**塊中配置*IOC 掃描*工作設定。

- **手動**執行您可以在其中在方便時手動開始*IOC 掃描*工作的模式。

- **自動**在此執行模式下，Kaspersky Endpoint Security 會在偵測到威脅後自動執行 *IOC 掃描* 工作。

10. 要將此政策套用到電腦，請關閉... 掛鎖圖示並儲存變更。



Sandbox

如何在指令列上配置 Sandbox 整合

1. 若要新增伺服器憑證，請執行下列指令：

```
kesl-control [-X] --add-sandbox-server-certificate <file>
```

2. 若要新增中央節點或 OSMP 伺服器，請執行下列指令：

```
kesl-control --set-settings 29 Servers.item_0000.Address=<server> Servers.item_0000.Port=<port>
```

3. 若要設定整合設定，請執行下列指令：

```
kesl-control --set-settings 29 [<setting name>=<setting value>]
```

設定及其可能值列於下表。

4. 若要新增用戶端憑證，請執行下列指令：

```
kesl-control [-X] --add-sandbox-client-certificate <file>
```

5. 若要啟用 Sandbox 整合，請執行下列指令：

```
kesl-control --start-task 29
```

Sandbox 整合工作設定

設定	描述	值
UseClientCertificate	啟用和停用雙向身分驗證以進一步防護與 Sandbox 伺服器的連線。 如果在 Sandbox 伺服器端啟用了用戶端憑證驗證，請在啟動*Sandbox 整合*工作之前啟用用戶端憑證的使用並新增用戶端憑證。	Yes – 使用雙向身分驗證進一步防護與沙盒伺服器的連線。 No（預設值）— 不使用雙向身分驗證。
ConnectionTimeout	等待與伺服器連線的最長時間（以秒為單位）。	預設值：10。
RequestTimeout	等待伺服器回應的最長時間（以秒為單位）。	預設值：10。
SendingMode	將物件傳送到 Sandbox 進行掃描的模式	AutoOnly（預設值）— 當嘗試存取檔案時，自動傳送檔案進行掃描. Manual — 手動傳送檔案進行掃描。 AutoAndManual — 自動和手動傳送檔案進行掃描。
QuarantineFile	偵測到威脅時隔離區檔案。	Yes（預設值）– 如果偵測到威脅，則刪除原始檔案，並將檔案副本放入隔離區。 No — 偵測到威脅時不隔離檔案。
ScanCriticalAreas	偵測到威脅時，執行關鍵區域掃描。	Yes（預設值）– 偵測到威脅時啟動關鍵區域掃描。 No – 偵測到威脅時不啟動關鍵區域掃描。
CreateIocScanTask	偵測到威脅時建立IOC 掃描工作。	Yes（預設值）– 偵測到威脅時建立 IOC 掃描工作。 No – 偵測到威脅時不建立 IOC 掃描工作。
QuarantineFileOnIocDetected	偵測到入侵指標時隔離物件。	Yes（預設值）– 如果偵測到入侵指標，則刪除原始物件，並將物件的副本置於隔離區。 No – 偵測到入侵指標時，不隔離物件。
ScanCriticalAreasOnIocDetected	偵測到入侵指標時，執行關鍵區域掃描。	Yes（預設值）– 偵測到入侵指標時啟動關鍵區域掃描。 No – 偵測到入侵指標時不啟動關鍵區域掃描。
Drives	IoC 掃描範圍。	Critical（預設）— 掃描使用者和系統目錄中的檔案。 System — 掃描根檔案系統中的所有檔案。
ScheduleMode	IOC 掃描工作啟動模式。	Manually（預設）– 手動啟動 IOC 掃描工作。 AfterTreatDetected – 偵測到威脅後啟動 IOC 掃描工作。
[Servers.item_#]部分包含 Sandbox 伺服器的設定。		
Address	伺服器的位址。 可指定 Integration Server 的 IP 位址（IPv4 或 IPv6）或完全限定網域名稱 (FQDN)。	預設值：127.0.0.1。
Port	用於連線至伺服器的連接埠。	預設值：443。
[SandboxTransferSettings]部分包含在 Sandbox 中傳送檔案進行掃描的設定。		
SandboxQueue	掃描請求佇列的最大大小（以兆位元組為單位）。	預設值：1024。

4 **確認已成功建立與沙盒的連線**

以任何方便的方式檢查沙盒的狀態 。

如何確認 Sandbox 整合已啟動並正常執行

您可以透過以下方式測試沙盒元件：

- 在命令列上使用以下命令：

  ```
  kesl-control --app-info
  ```

  Sandbox 整合會顯示為 **可用且執行中** 狀態。

- 在網頁主控台中：
  - 在卡巴斯基安全管理中心主控台中：
    使用*應用程式元件狀態報告*。關於報告的詳細資訊，請參閱卡巴斯基安全管理中心說明。
  - 在 OSMP 主控台中：
    - 使用*應用程式元件狀態報告*。
    - 前往 **威脅搜尋**區段。
      成功的沙盒連線事件會顯示在事件清單中。
- 在 Kaspersky Anti Targeted Attack Platform 中：
  前往**資產** → **裝置**區段。裝置會顯示在表格中。如有需要，您可以依**EPP 應用程式**、**EPP 連線**、**上次連線至 EPP**篩選表格。
  按一下裝置名稱會開啟窗格。在 Endpoint Agent 區段中，連線狀態為 **作用中**。

如何手動將檔案傳送到沙盒

Kaspersky Endpoint Security 可讓使用者從內容功能表手動傳送檔案或目錄，以便在沙盒中掃描。

若要將檔案傳送到沙盒中進行掃描，必須符合下列條件：

- 必須安裝 Kaspersky Endpoint Security 的圖形介面。
- Kaspersky Endpoint Security 必須與沙盒整合。
- 傳送檔案進行掃描的模式必須設定為 **手動** 或 **組合**。

若要將檔案或目錄傳送到沙盒中進行掃描：

1. 開啟您要掃描之檔案或目錄的內容功能表。
2. 選取 **Kaspersky Endpoint Security 12.5 for Linux** 作為開啟檔案或目錄的應用程式。

   根據桌面環境的不同，右鍵功能表指令的名稱可能會有所不同。

3. 然後，在內容功能表中選取 **在 Sandbox 中掃描**。

Kaspersky Managed Detection and Response

Kaspersky Endpoint Security 包含一個內建代理程式，可與 Kaspersky Managed Detection and Response 解決方案整合。*Kaspersky Managed Detection and Response (MDR)* 解決方案會自動偵測並分析您基礎架構中的安全事件。為此，MDR 會使用從端點接收的遙測資料和機器學習技術。MDR 會將事件資料傳送給卡巴斯基專家。接著，專家可以處理事件，例如，將新項目新增至病毒防護資料庫。或者，專家可以針對處理事件提出建議，例如，建議將電腦與網路隔離。如需有關解決方案運作方式的詳細資訊，請參閱 Kaspersky Managed Detection and Response 說明。

此整合由 Kaspersky Endpoint Security 元件實現：Managed Detection and Response (MDR)。必須使用整合情境中所述的其中一種方式啟動元件。

此元件不適用於搭載 Elbrus CPU 的裝置。

用於與 MDR 整合的 Kaspersky Endpoint Security 組態

下列組態可用於與 MDR 搭配使用：

- **[KES+內建代理程式]**。在此組態中，Kaspersky Endpoint Security 同時作為確保電腦安全性的應用程式，以及用於與 MDR 搭配運作的應用程式。
- **[第三方 EPP+EDR Agent]**。在此組態中，IT 基礎架構的安全性由第三方 Endpoint Protection Platform (EPP) 提供。與 MDR 的互動由 Endpoint Detection and Response Agent (EDR Agent) 組態中的 Kaspersky Endpoint Security 提供。在此組態中，EDR Agent 與第三方 EPP 應用程式相容。

建立參考映像以便與 MDR 正確整合的建議

我們不建議在參考映像中包含 Kaspersky Endpoint Security for Linux 應用程式。

如果參考映像中包含 Kaspersky Endpoint Security for Linux，請在基於此映像的每部裝置上執行下列步驟：

1. 若要建立新的 UUID，請執行下列指令：

```
uuidgen > /var/opt/kaspersky/kesl/common/pcid
uuidgen > /var/opt/kaspersky/epagent/install_id
```

2. 解除安裝 Kaspersky Endpoint Security for Linux，然後重新安裝。

如果您未遵循這些步驟，裝置可能無法正確識別。

上傳 KPSN 設定檔

如果您的配置不符合無需 KPSN 設定檔即可運行的要求，則若要與 Kaspersky Managed Detection and Response 進行整合，您需要將*KPSN 設定檔*上傳到卡巴斯基安全管理中心管理伺服器。該檔案包含必要的遙測設定。帶有 .pkcs7 副檔名的 KPSN 設定檔位於 MDR 設定檔的 ZIP 壓縮檔案中。有關詳細資訊，請參閱 Kaspersky Managed Detection and Response 說明。

您可以在網頁主控台或管理主控台中上傳 KPSN 設定檔。

上傳 KPSN 設定檔即表示您同意安裝有 Kaspersky Endpoint Security 的裝置的資料將被自動傳送至卡巴斯基進行處理。如果您不同意處理傳輸的資料，請不要載入設定檔。有關被傳輸資料的詳細描述，請參閱 Kaspersky Managed Detection and Response 文件。

如何在網頁主控台中上傳 KPSN 設定檔

1. 在主網頁主控台視窗中，開啟管理伺服器屬性視窗。
2. 在左側清單中，選擇**KSN 代理伺服器設定**部分。
3. 開啟**在管理伺服器上啟用 KSN 代理伺服器作為代理伺服器**切換開關，以啟用 KSN 代理伺服器服務。
4. 開啟**使用卡巴斯基私人安全網路**切換開關。
5. 在開啟的視窗中顯示關於在安裝了先前版本的網路代理的分發點上使用 KSN 代理伺服器的具體方面的警告，點擊**確定**。
6. 點擊**帶有 KSN 代理伺服器設定的檔案**按鈕。
7. 選取 KSN 設定檔（帶有 pkcs7 副檔名）並點擊**開啟**。
8. 接受 KPSN 聲明的條款和條件，然後點擊**儲存**按鈕。

如何在管理主控台 (MMC) 中上傳 KPSN 設定檔

1. 在管理主控台樹中，開啟管理伺服器屬性視窗。
2. 選擇**KSN 代理伺服器→ KSN 代理伺服器設定**。
3. 選取**使用管理伺服器作為代理伺服器**核取方塊以啟用 KSN 代理伺服器服務。
4. 選取 **設定 KPSN** 核取方塊。

5. 在開啟的視窗中顯示關於在安裝了先前版本的網路代理的分發點上使用 KSN 代理伺服器的具體方面的警告，點擊**確定**。

6. 點擊**帶有 KSN 代理伺服器設定的檔案**按鈕。

7. 選取 KSN 設定檔（帶有 pkcs7 副檔名）並點擊**開啟**。

8. 接受 KPSN 聲明的條款和條件，然後點擊**套用**按鈕。

如何在命令列上傳 KPSN 設定檔

執行命令：

```
kesl-control --load-mdr-blob <path to the MDR BLOB>
```

如何設定 MDR 整合

在設定 Kaspersky Managed Detection and Response 整合之前：

- 允許透過連接埠 443 和 1443 進行連線。
- 允許連線到以下位址：
  - *.ksn.kaspersky-labs.com
  - ksn-*.kaspersky-labs.com
  - ds.kaspersky.com

  位址清單可能會變更。若要取得確切位址，您可以聯絡技術支援。

- 確保已啟用以下項目且運作正常：
  - 卡巴斯基安全網路（延伸模式）：
  - 行為偵測。

    為確保遙測資料完整，您也可以啟用以下元件：Web 威脅防護、網路威脅防護、檔案威脅防護和 郵件威脅防護。

必要設定步驟

1. **透過以下方式之一啟動 MDR 元件**

   - 使用產品授權金鑰。

     如果您已購買單獨的產品授權來使用此功能，請將 MDR 產品授權金鑰新增至應用程式。

     如果您使用 Kaspersky Endpoint Security 時採用的產品授權包含 Kaspersky Managed Detection and Response，則不需要執行任何動作。

     如果 Kaspersky Endpoint Security 是以 Light Agent 模式使用，MDR 產品授權金鑰會新增至 SVM。

- 使用 MDR BLOB 檔案。

  在 MDR 主控台中，下載 MDR 設定檔。此檔案是 ZIP 壓縮檔，包含 MDR BLOB 檔案和 KPSN 設定檔。

  然後在 網頁主控台、管理主控台或命令列中上傳 BLOB 檔案。

Kaspersky Endpoint Security 應用程式的版本會決定 MDR 元件的啟動方法，以及您是否需要使用 KPSN 設定檔。有關詳細資訊，請參閱 Kaspersky Managed Detection and Response 說明。

> 如果卡巴斯基安全管理中心管理伺服器以階層方式組織，且次要伺服器沒有直接網際網路存取權，即使主要管理伺服器可存取網際網路，Kaspersky Managed Detection and Response 仍無法運作。

2 上傳 KPSN 設定檔

如果您的組織有多個租戶，或您已使用 MDR BLOB 啟動 MDR 元件，請將 KPSN 檔案上傳至卡巴斯基安全管理中心管理伺服器。此檔案包含傳送遙測資料所需的設定；您可以在包含 MDR 設定檔的 ZIP 壓縮檔中找到此檔案。

3 設定 Kaspersky Managed Detection and Response 的整合設定

如何在網頁主控台中啟用 Kaspersky Managed Detection and Response 整合

1. 在網頁主控台的主視窗中，選擇 **資產管理** → **政策** 區段。
2. 點擊所需的 Kaspersky Endpoint Security 政策。
3. 在開啟的政策內容視窗中，選擇 **應用程式設定** 索引標籤。
4. 在 **內置代理設定** 區段中，選擇 **Managed Detection and Response**，然後在畫面右側管理以下設定：
   - 將切換開關設定為 **已啟用 Managed Detection and Response**。
   - 如果您有租戶，或已使用 MDR BLOB 檔案啟動 MDR 元件，請按一下 **上傳** 按鈕以新增 MDR BLOB 檔案。
5. 儲存設定。

Managed Detection and Response

如何從命令列啟用 Kaspersky Managed Detection and Response 整合

1. 若要啟用 MDR 元件，請執行以下命令：

```
kesl-control --set-app-settings UseMDR=Yes
```

2. 若要新增 BLOB 檔案，請執行以下命令：

```
kesl-control --load-mdr-blob <path to the MDR BLOB>
```

4. **設定 KSN 政策**

如何在網頁主控台中管理 KSN 設定

1. 在 Kaspersky Endpoint Security 政策的 **應用程式設定** 索引標籤上，前往 **一般設定** 區段。
2. 選擇 **卡巴斯基安全網路**，然後在畫面右側指定以下設定：
   a. 將切換開關設定為 **「使用卡巴斯基安全網路 (KSN)」已啟用**。
   b. 在 **KSN 設定** 子區段中，選取 **啟用延伸 KSN 模式** 核取方塊。
   c. 在 **KSN 代理伺服器** 子區段中，選取以下核取方塊：
      - **使用管理伺服器為 KSN 代理伺服器**
      - **當 KSN 代理伺服器不可用時使用卡巴斯基安全網路伺服器**

      遙測資料將從管理伺服器或裝置收集，具體取決於已設定的選項是否可用。
3. 儲存設定。

如何從命令列設定 KSN 的設定

若要以擴充模式啟用 KSN，請執行以下命令：

```
kesl-control --set-app-settings UseKSN=Extended --accept-ksn
```

5. **啟用 KSN**

如何在網頁主控台中啟用 KSN

1. 在主選單中，按一下管理伺服器的名稱。
2. 在開啟的視窗中，於 **一般** 索引標籤上，選擇 **KSN 代理** 區段。
3. 將切換開關設定為 **在管理伺服器上啟用 KSN 代理 已啟用**。

4. 根據您使用的 KSN 基礎架構解決方案 啟用切換開關：
   - **使用卡巴斯基安全網路 已啟用**
   - **使用卡巴斯基私人安全網路 已啟用**，然後上傳 KPSN 設定檔。
5. 儲存設定。

6. **請確保已成功建立與 Kaspersky Managed Detection and Response 的連線**

   以任何方便的方式檢查 Kaspersky Managed Detection and Response 的狀態。

如何驗證 MDR 整合是否已啟用

您可以透過以下方式檢查 Kaspersky Managed Detection and Response 元件的運作狀況：

- 在命令列上使用以下命令：

  ```
  kesl-control --app-info
  ```

  Kaspersky Managed Detection and Response 整合會顯示為**可用且正在執行**狀態。

- 在 MDR Console 中，前往**資產**區段。裝置會顯示為**正常**（綠色）狀態。

如果元件已停用：

1. 更新應用程式的病毒防護資料庫。
2. 請確保卡巴斯基安全網路已啟用，且正在延伸模式下執行。
3. 檢查 Kaspersky Endpoint Security 和 MDR 的產品授權金鑰。
4. 請確保 BLOB 檔案已新增至政策。
5. 確認 MDR 所需的元件是否正常運作。

Kaspersky Unified Monitoring and Analysis Platform

Kaspersky Endpoint Security for Linux 支援 Kaspersky Unified Monitoring and Analysis Platform 解決方案。*Kaspersky Unified Monitoring and Analysis Platform (KUMA)* 是適用於組織 IT 基礎結構的安全資訊和事件管理 (SIEM) 解決方案。KUMA 可讓您在安全威脅造成損害之前進行偵測、分析和緩解。

關於該解決方案的更多資訊，請參閱卡巴斯基統一監控和分析平台說明。

Kaspersky Endpoint Security 應用程式安裝在公司 IT 基礎結構上的單個電腦上，持續監控處理程序、開啟的網路連線和被修改的檔案。有關電腦上的事件的資訊（遙測資料）被傳送到 Kaspersky Unified Monitoring and Analysis Platform (KUMA) 伺服器。

此元件不適用於搭載 Elbrus CPU 的裝置。

如何設定 KUMA 整合

設定 Kaspersky Unified Monitoring and Analysis Platform 整合之前：

- 允許透過連接埠 443 和 1443，或 KUMA 收集器端設定的連接埠進行連線。
- 如果您已購買單獨的產品授權來使用此功能，請將 KUMA 產品授權金鑰新增至應用程式。

  如果您使用 Kaspersky Endpoint Security 的產品授權包含 Kaspersky Unified Monitoring and Analysis Platform，則不需要執行任何動作。

  如果應用程式以 Light Agent 模式 使用，KUMA 產品授權金鑰會新增至 SVM。

必要設定步驟

1. **在 KUMA 中設定收集器和正規化器。**

   如果您想使用用戶端憑證，請在設定收集器時，於 **傳輸** 索引標籤上選取 tcp 連接器類型。接著，在 **進階設定** 索引標籤上，在 **TLS 模式** 下拉式清單中，選取 **具有用戶端身分驗證的自訂 PFX**。

2. **複製要連線的收集器位址**

   在 **資源** → **活動服務** 區段中的服務表格內，以任何方便的方式複製並儲存 **FQDN / IP 位址** 和 **連接埠** 欄中的值。

   如果您使用 TLS 進行連線，請僅指定完整網域名稱 (FQDN)。設定值區分大小寫。

3. **取得並處理由 KUMA 伺服器核發的憑證**

   KUMA 伺服器的 UDP 連線不支援使用憑證來保護連線安全。

   如果在 Kaspersky Endpoint Security 的一般應用程式設定中配置了使用代理伺服器，則使用代理伺服器連線到 KUMA 伺服器。

   取得 伺服器憑證（微服務 CA 憑證），請參閱下載 CA 憑證。若要處理憑證，請依照 將 PFX 憑證轉換為 PEM 格式一文中的步驟，將其轉換為 DER 或 PEM 格式。

   為了加強保護，您也可以使用在設定收集器時取得的 用戶端憑證，請參閱步驟 1。

4. **設定 Kaspersky Unified Monitoring and Analysis Platform 的整合設定**

   如何在卡巴斯基安全管理中心網頁主控台中設定 KUMA 整合

   1. 在網頁主控台的主視窗中，選擇**資產管理** → **政策**。
   2. 點擊 Kaspersky Endpoint Security 政策的名稱。

      政策內容視窗將開啟。
   3. 選擇“**應用程式設定**”標籤。

4. 轉到"**內置代理設定**"→"**KUMA 整合**"。

5. 啟用 **KUMA 整合已啟用** 切換開關。

6. 新增 KUMA 伺服器：

   a. 點擊"**新增**"。

   這將開啟一個表單，您可以在其中新增 KUMA 伺服器。

   b. 選取用於連線至 KUMA 伺服器的協定：**HTTP/HTTPS**、**TCP**、**UDP**。

   Kaspersky Endpoint Security 中用於連線至收集器的協定必須與 KUMA 中的連接器類型相符：**http**、**tcp** 或 **udp**。

   如果您選取 **HTTP/HTTPS** 協定，預設情況下，應用程式會使用 HTTPS 連線至 KUMA 伺服器。若要使用 HTTP，您需要在伺服器位址中手動指定此協定（例如，`http://server.com`）。

   c. 請輸入伺服器位址（IPv4、IPv6）和用於連線至伺服器的連接埠（預設指定連接埠 443）。

   您可以在 KUMA 主控台的連接器屬性中檢視伺服器位址。如需 KUMA 連接器的詳細資訊，請參閱 Kaspersky Unified Monitoring and Analysis Platform 說明。

   d. 點擊"**確定**"。

   Kaspersky Endpoint Security 將連線到清單中的第一台 KUMA 伺服器。如果連線失敗，Kaspersky Endpoint Security 將連線到清單中的第二台 KUMA 伺服器，依此類推。

7. 如有必要，在**伺服器連線設定**塊中配置**傳送事件時的最大延遲（秒）**設定。當指定的時間結束時，Kaspersky Endpoint Security 會嘗試連線至相同的收集器；如果有多個收集器，則會連線至清單中的下一個收集器。預設設定是 30 秒。

8. 儲存變更。

如何在指令列上設定 KUMA 整合

1. 若要新增 KUMA 伺服器，請執行下列指令：

```
kesl-control --set-settings 33 Servers.item_001.ServerAddress=<kuma server address>
Servers.item_001.Port=<kuma server port> Servers.item_001.ServerProtocol=<tcp|HTTPWithCompression|udp>
```

2. 若要新增 KUMA 伺服器憑證，請執行下列指令：

```
kesl-control [-M] --add-kuma-server-certificate <path to the file>
```

3. 若要設定整合設定，請執行下列指令：

```
kesl-control --set-settings 33 [<setting name>=<setting value>]
```

   設定及其可能值列於下表。

4. 若要新增用於連線至回應伺服器的用戶端憑證，請執行下列指令：

```
kesl-control [-M] --add-kuma-client-certificate <path to the file>
```

5. 若要啟用與 EDR (KATA) 的整合，請執行下列指令：

```
kesl-control --start-task 33
```

卡巴斯基統一監控與分析平台整合工作設定

設定	描述	值
`UseTls`	啟用或停用伺服器憑證驗證，以對與 KUMA 伺服器的連線提供額外防護。	`Yes` — 使用憑證進一步防護與 KUMA 伺服器的連線。 `No`（預設）— 不使用憑證來防護與 KUMA 伺服器的連線。
`UseClientCertificate`	啟用和停用雙向身分驗證以進一步防護與 KUMA 伺服器的連線。 如果在 KUMA 伺服器端啟用了用戶端憑證驗證，請在啟動卡巴斯基統一監控和分析平台整合工作之前啟用用戶端憑證的使用並新增用戶端憑證。	`Yes` – 使用雙向身分驗證進一步防護與 KUMA 伺服器的連線。 `No`（預設值）— 不使用雙向身分驗證。
`ConnectionTimeout`	等待連線到 KUMA 伺服器的最長時間（秒）。	預設值：`5`。
[Servers.item_#]部分包含 KUMA 伺服器的設定。		
`ServerAddress`	KUMA 伺服器位址 可指定 Integration Server 的 IP 位址（IPv4 或 IPv6）或完全限定網域名稱 (FQDN)。 如果設定`UseTls=Yes`，則必須從購買授權時收到的憑證指定伺服器的完全限定網域名稱 (FQDN) 才能使用 KUMA。	預設值：`127.0.0.1`。
`ServerPort`	連線 KUMA 伺服器的連線埠。	預設值：`443`。
`ServerProtocol`	用於連線到 KUMA 伺服器的協定。	`tcp`（預設值）— 使用 TCP 協定連線到 KUMA 伺服器。 `HTTPWithCompression` — 使用 HTTP 協定及事件壓縮連線至 KUMA 伺服器。 `udp` — 使用 UDP 協定連線到 KUMA 伺服器。 當選取 UDP 協定時，不支援使用憑證來提供連線保護（系統會忽略 `UseTls`、`UseClientCertificate` 和 `ConnectionTimeout` 設定的值），且不會產生與 KUMA 伺服器連線相關的事件。
[KumaTransferSettings] 區段包含將事件傳送至 KUMA 伺服器的設定。		
`EventTransferTimeMax`	向 KUMA 伺服器傳送事件的最大延遲（以秒為單位）。	預設值：`30`。

5. **請確定已成功建立與 Kaspersky Unified Monitoring and Analysis Platform 的連線**

   使用任何方便的方式檢查 KUMA 的狀態。

如何驗證 KUMA 整合已啟動並正在執行

您可以透過以下方式測試 KUMA 元件：

- 在命令列上使用以下命令：

```
kesl-control --app-info
```

KUMA 整合會顯示為 **可用且正在執行** 狀態。

- 在網頁主控台（OSMP 主控台）中：

  前往 **威脅搜尋** 區段：事件清單中會顯示相關裝置狀態為「已建立與 KUMA 的連線」的遙測事件。

- 在 Kaspersky Unified Monitoring and Analysis Platform 中：

  在 KUMA 主控台的主功能表中，前往 **事件** 區段：清單中會顯示 Kaspersky Endpoint Security 遙測事件。

虛擬環境防護

Kaspersky Endpoint Security 支援 Light Agent 模式，可作為 Kaspersky Security for Virtualization Light Agent 的一部分運作。*Kaspersky Security for Virtualization Light Agent* 是一個整合的解決方案，可為虛擬機提供全面防護，抵禦各種類型的資訊安全威脅、網路攻擊和網路釣魚攻擊。若要使用此解決方案，您必須以 Light Agent 模式安裝應用程式。

當您啟動 Light Agent 時，它會建立並維護與虛擬機 SVM (Secure Virtual Machine）的連線。SVM 上部署了 Protection Server。*Protection Server* 是一個 Kaspersky Security for Virtualization Light Agent 解決方案元件，用於掃描檔案中是否存在病毒和其他惡意軟體、更新防毒資料庫並管理產品授權金鑰。Light Agent 會將需要掃描的檔案或其片段傳送到 SVM。掃描結果適用於所有安裝了 Light Agent 的虛擬機（SharedCache技術）。此技術可提高解決方案效率，並加快對威脅的回應。

組織的基礎結構可能包含許多安裝了 Light Agent 的虛擬機和許多 SVM。Integration Server 處理虛擬機與 SVM 之間的互動。*Integration Server* 是 Kaspersky Security for Virtualization Light Agent 解決方案的一個元件，可產生可用 SVM 清單並將此資料傳輸至 Light Agent、參與 Light Agent 探索 SVM、保護 Light Agent 與 SVM 之間的連線，並執行其他功能。

將 Light Agent 連線到 SVM

1. **取得可用 SVM 清單**

   Light Agent 取得可用 SVM 的清單。

2. **選取最佳 Protection Server（SVM）**

   Light Agent 根據 VM 選取演算法 確定最適合連線的可用 Protection Server (SVM)。

3. **檢查其他連線設定**

   Light Agent 會檢查其他 SVM 連線設定：標籤、連線防護狀態、產品授權涵蓋的應用程式功能。

4. **將 Light Agent 連線到 SVM**

   Light Agent 會與選取的 SVM 建立並維持連線。

如何設定 SVM 探索

您可以為 Light Agent 選擇一種 SVM 發現方法：

- 使用 Integration Server (VIIS)。

  Integration Server 是一種解決方案元件，可讓 Kaspersky Security for Virtualization Light Agent 與虛擬基礎架構互動，並產生可供連線的 SVM 清單。Light Agent 與 Integration Server 建立連線並取得 SVM 位址清單。

Integration Server 在大型虛擬基礎架構中最為實用，因為它會自動平衡 SVM 之間的負載，取得可用 SVM 的相關資訊，分析此資訊，並向 Light Agent 提供最適合連線的 Protection Server (SVM) 清單。

為了 Light Agent 能夠取得 SVM 清單，您只需輸入Integration Server 的位址。

- 使用 Integration Server 的高可用性叢集。

  Kaspersky Security for Virtualization Light Agent 6.4 支援部署 Integration Server 的高可用性叢集。每當主要 Integration Server 發生故障時，SVM 和 Light Agent 都會容錯移轉至備用 Integration Server，因此 Integration Server 的高可用性叢集可為虛擬環境提供不間斷的防護。特殊的叢集元件 *負載平衡器*負責伺服器容錯移轉。如需 Integration Server 高可用性叢集的詳細資訊，請參閱Kaspersky Security for Virtualization Light Agent 說明。

  若要讓 Light Agent 取得 SVM 清單，您需要輸入安裝負載平衡器之裝置的位址。

- 使用 SVM 位址清單。

  如果需要指定想要 Light Agent 連線到的單個 SVM，您可以手動準備一個清單。

  您需要列出 Light Agent 可連線的可用 SVM 的位址。

如何在 Web 主控台中透過 Light Agent 配置 SVM 發現

1. 在網頁主控台的主視窗中，選擇**資產管理 → 政策**。
2. 點擊 Kaspersky Endpoint Security 政策的名稱。

   政策內容視窗將開啟。
3. 選擇"**應用程式設定**"標籤。
4. 轉到"**Light Agent 模式**"→"**SVM 發現設定**"。
5. 選擇 SVM 發現方法。
   - **使用 Integration Server**請根據您的基礎架構，輸入 Integration Server 的連線設定：
     - **單一 Integration Server**。輸入 Integration Server 連線設定：裝置的 IPv4 位址或完整網域名稱 (FQDN)。
     - **Integration Server 的高可用性叢集**。輸入叢集中負載平衡器的 IP 位址和連接埠。
   - **使用 SVM 位址自訂清單**建立 Light Agent 可連線的 SVM 清單。指定 IPv4 格式的 IP 位址或 SVM 的完全限定網域名稱 (FQDN)。每個清單項目必須另起一行，或用分號 (`;`) 字元與前一項分隔開。

     > 在 SVM 位址清單中，僅指定與單一 IP 位址相符的完整限定網域名稱 (FQDN)。使用與多個 IP 位址相對應的完全限定網域名稱可能會導致解決方案出現錯誤。
6. 要將此政策套用到電腦，請關閉... 掛鎖圖示並儲存變更。

若要在命令列中檢視有關將 Light Agent 連線到 Integration Server 的資訊：

1. 請確定應用程式是以 Light Agent 模式安裝：

   ```
   kesl-control -V --ksvla-info
   ```

   元件狀態必須為 **開啟**。

2. 輸出有關 Light Agent 與 Integration Server 連線的資訊：

```
kesl-control -V --viis-info
```

此命令向主控台輸出以下資訊：

- Light Agent 已連線的 Integration Server 的位址和連線埠。
- 與 Integration Server 的連線狀態。
- Light Agent 和 Integration Server 之間上次連線的日期和時間。

如何在命令列中檢視 Light Agent 與 Integration Server 連線的相關資訊

1. 請確定應用程式是以 Light Agent 模式安裝：

   ```
   kesl-control -V --ksvla-info
   ```

   元件狀態必須為 **開啟**。

2. 輸出有關 Light Agent 與 Integration Server 連線的資訊：

   ```
   kesl-control -V --svm-info
   ```

此命令向主控台輸出以下資訊：

- Light Agent 連線到的 SVM 的位址，以及虛擬基礎架構中 SVM 相對於 Light Agent 的定位：本機或非本機。
- Light Agent 使用的 SVM 發現方法：使用 Integration Server 或使用 SVM 位址的自訂清單。
- SVM 位址清單（如果選取的 SVM 發現方法是 SVM 位址清單）。
- 用於將 Light Agent 連線到 SVM 的標籤。
- SVM 選擇演算法：標準或進階。如果使用延伸 SVM 選擇演算法，則也會顯示 SVM 在虛擬基礎架構中的定位類型。
- Light Agent 和 Protection Server 之間的連線。

Light Agent 如何選擇 SVM

組織的基礎結構可能有多個已部署的 SVM，Light Agent 可以連線到這些 SVM。為了平衡網路負載和虛擬基礎結構的資源，您需要在 SVM 之間分發 Light Agent。

SVM 選擇演算法

Light Agent 可以套用下列 SVM 選擇演算法進行連線：標準演算法（預設）和延伸演算法。

標準演算法	延伸演算法
如果使用此演算法，安裝和啟動後，虛擬機上的 Light Agent 會選擇連線到對於 Light Agent 是本機的 SVM。 如果找不到適合連線的本機 SVM，則 Light Agent 會選擇連線 Light Agent 數量最少的 SVM，與 SVM 在虛擬基礎架構中的位置無關。 如果已為 SVM 上的 Protection Server 啟用大型基礎架構防護模式，應用程式不會判定 SVM 相對於 Light Agent 是否為本機。在此情況下，建議使用延伸 SVM 選擇演算法，並選擇 Integration Server 作為 SVM 探索方法。 SVM 是否被視為 Light Agent 的本機 SVM 取決於虛擬基礎架構的類型。	如果套用此演算法，您可以定義下列 SVM 選擇設定： • 選擇用於連線的 SVM 時，要考量還是忽略 SVM 在基礎架構中的位置 • 如果考量 SVM 位置，則判定 SVM 相對於 Light Agent 是否為本機的方法 如果 Light Agent 忽略 SVM 在基礎架構中的位置，Light Agent 將能夠連線到任何可供連線的 SVM。 如果 Light Agent 必須考量 SVM 在基礎架構中的位置，您需要選擇在判定 SVM 相對於 Light Agent 是否為本機時要考量的 SVM 路徑類型。SVM 是否被視為 Light Agent 的本機 SVM 取決於虛擬基礎架構的類型。 如果 Light Agent 在選擇要連線的 SVM 時考量 SVM 在基礎架構中的位置，Light Agent 只能連線到本機 SVM。 例如，如果您指定 Hypervisor 叢集作為 SVM 路徑類型，則部署在此 Hypervisor 叢集上的所有 SVM 都會被視為 Light Agent 的本機 SVM，且 Light Agent 只能連線到其中一個 SVM。如果 Light Agent 執行所在的同一叢集中沒有可供連線的 SVM，Light Agent 不會連線到 SVM。 選擇 SVM 時，Light Agent 也會考量已連線的 Light Agent 數量，以確保 Light Agent 在可供連線的 SVM 之間平均分配。 如果 Light Agent 使用延伸 SVM 選擇演算法，且 SVM 探索方法設定為 SVM 位址清單，並且已在 SVM 上啟用大型基礎架構防護模式，則只有在忽略 SVM 路徑的情況下，才能將 Light Agent 連線到此 SVM。
Basis Dynamix Enterprise	
在以 Basis Dynamix Enterprise 為基礎的虛擬基礎架構中，被視為 Light Agent 本機 SVM 的 SVM，是部署在與安裝 Light Agent 的虛擬機相同節點上的 SVM。	在以 Basis Dynamix Enterprise 為基礎的虛擬基礎架構中，在下列任一情況下，SVM 可被視為 Light Agent 的本機 SVM： • SVM 部署在與安裝 Light Agent 的虛擬機相同的節點上。 • SVM 部署在與安裝 Light Agent 的虛擬機相同的區域中。 • SVM 部署在與安裝 Light Agent 的虛擬機相同的資料中心中。
Microsoft Hyper-V、XenServer、VMware vSphere、KVM、Proxmox VE、Basis、HUAWEI FusionSphere、Nutanix Acropolis、ALT Virtualization Server、Astra Linux、Numa vServer 和 Basis Dynamix Standard	
在以 Microsoft Hyper-V、XenServer、VMware vSphere、KVM、Proxmox VE、Basis、HUAWEI FusionSphere、Nutanix Acropolis、ALT Virtualization Server、Astra Linux、Numa vServer 或 Basis Dynamix Standard 為基礎的虛擬基礎架構中，被視為 Light Agent 本機 SVM 的 SVM，是部署在與安裝 Light Agent 的虛擬機相同 Hypervisor 上的 SVM。	在以 Microsoft Hyper-V、XenServer、VMware vSphere、KVM、Proxmox VE、Basis、HUAWEI FusionSphere、Nutanix Acropolis、ALT Virtualization Server、Astra Linux、Numa vServer 或 Basis Dynamix Standard 為基礎的虛擬基礎架構中，在下列任一情況下，SVM 可被視為 Light Agent 的本機 SVM： • SVM 部署在與安裝 Light Agent 的虛擬機相同的 Hypervisor 上。 • SVM 部署在與安裝 Light Agent 的虛擬機相同的 Hypervisor 叢集上。 • SVM 部署在與安裝 Light Agent 的虛擬機相同的資料中心中。
OpenStack 和 VK Private Cloud SVM	

標準演算法	延伸演算法
在執行於 OpenStack 或 VK Private Cloud 平台上的虛擬基礎架構中，您可以使用 Integration Server 設定檔 appsettings.json 的 `HypervisorSpecificSettings:Openstack` 區段中的 `StandardAlgorithmSvmLocality` 參數，指定如何判定 SVM 相對於 Light Agent 是否為本機。依據 Integration Server 的版本，此檔案位於下列其中一個路徑： • /var/opt/kaspersky/viis/common/：適用於以 Linux 為基礎的 Integration Server • %ProgramFiles(x86)%\Kaspersky Lab\Kaspersky VIISLA\：適用於以 Windows 為基礎的 Integration Server `StandardAlgorithmSvmLocality` 參數可以採用下列值： • `ServerGroup` – 如果選取此值，則當 SVM 位於與安裝 Light Agent 的虛擬機相同的伺服器群組中時，SVM 會被視為 Light Agent 的本機 SVM。預設情況下會使用此數值。 • `Project` – 如果選取此值，則當 SVM 部署在與安裝 Light Agent 的虛擬機相同的 OpenStack 專案中時，SVM 會被視為 Light Agent 的本機 SVM。 • `AvailabilityZone` – 如果選取此值，則當 SVM 位於與安裝 Light Agent 的虛擬機相同的可用區域中時，SVM 會被視為 Light Agent 的本機 SVM。	在執行於 OpenStack 或 VK Private Cloud 平台上的虛擬基礎架構中，在下列任一情況下，SVM 可被視為 Light Agent 的本機 SVM： • SVM 位於與安裝 Light Agent 的虛擬機相同的伺服器群組中。 • SVM 部署在與安裝 Light Agent 的虛擬機相同的 OpenStack 專案中。 • SVM 位於與安裝 Light Agent 的虛擬機相同的可用區域中。

除了 SVM 線演算法之外，您還可以 使用標籤調節 Light Agent 與 SVM 的連線。

如何在 Web 主控台中配置 Light Agent 的 SVM 選取演算法

1. 在網頁主控台的主視窗中，選擇**資產管理** → **政策**。
2. 點擊 Kaspersky Endpoint Security 政策的名稱。
   政策內容視窗將開啟。
3. 選擇"**應用程式設定**"標籤。
4. 轉到"**Light Agent 模式**"→"**SVM 選擇演算法**"。
5. 選取演算法：
   - **使用標準 SVM 選擇演算法**Light Agent 會選擇部署在相同 Hypervisor 中的 SVM。
   - **使用延伸 SVM 選擇演算法**Light Agent 選擇部署在所選 SVM 路徑類型（預設情況下， **Hypervisor** ）中的 SVM。
6. 如果需要，請為延伸 SVM 選取演算法選擇 SVM 路徑：
   - **Hypervisor**Light Agent 會選擇要連線的符合下列條件的 SVM（取決於虛擬基礎架構的類型）：
     - SVM 部署在與安裝了 Light Agent 的虛擬機相同的 Hypervisor 上（在基於 Microsoft Hyper-V、XenServer、VMware vSphere、KVM、Proxmox VE、Basis、華為 FusionSphere、Nutanix Acropolis、ALT Virtualization Server、Astra Linux、Numa vServer 或 Basis Dynamix Standard 的虛擬基礎架構中）。
     - SVM 位於與安裝 Light Agent 的虛擬機相同的伺服器群組中（在執行於 OpenStack 或 VK Private Cloud 平台上的虛擬基礎架構中）。
     - SVM 位於與安裝 Light Agent 的虛擬機相同的節點上（在 Basis Dynamix Enterprise 虛擬基礎架構中）。

   如果在裝有 Light Agent 的虛擬機所在的相同Hypervisor 或相同伺服器群組中沒有可供連線的 SVM，則 Light Agent 不會連線到 SVM。

- **叢集**Light Agent 會選擇要連線的符合下列條件的 SVM（取決於虛擬基礎架構的類型）：

  - SVM 部署在與安裝 Light Agent 的虛擬機相同的 Hypervisor 叢集上（在以 Microsoft Hyper-V、XenServer、VMware vSphere、KVM、Proxmox VE、Basis、HUAWEI FusionSphere、Nutanix Acropolis、ALT Virtualization Server、Astra Linux、Numa vServer 或 Basis Dynamix Standard 為基礎的虛擬基礎架構中）。

  - SVM 部署在與安裝 Light Agent 的虛擬機相同的 OpenStack 專案中（在執行於 OpenStack 或 VK Private Cloud 平台上的虛擬基礎架構中）。

  - SVM 位於與安裝 Light Agent 的虛擬機相同的區域中（在 Basis Dynamix Enterprise 虛擬基礎架構中）。

  如果在裝有 Light Agent 的虛擬機所在的相同 Hypervisor 叢集或相同 OpenStack 專案中沒有可供連線的 SVM，則 Light Agent 不會連線到 SVM。

- **資料中心**Light Agent 會選擇要連線的符合下列條件的 SVM（取決於虛擬基礎架構的類型）：

  - SVM 部署在與安裝 Light Agent 的虛擬機相同的資料中心中（在以 Microsoft Hyper-V、XenServer、VMware vSphere、KVM、Proxmox VE、Basis、HUAWEI FusionSphere、Nutanix Acropolis、ALT Virtualization Server、Astra Linux、Numa vServer 或 Basis Dynamix Standard 為基礎的虛擬基礎架構中）。

  - SVM 位於與安裝 Light Agent 的虛擬機相同的可用區域中（在執行於 OpenStack 或 VK Private Cloud 平台上的虛擬基礎架構中）。

  - SVM 位於與安裝 Light Agent 的虛擬機相同的資料中心中（在 Basis Dynamix Enterprise 虛擬基礎架構中）。

  如果帶有 Light Agent 的虛擬機所在的相同資料中心或可用性區域中沒有可用於連線的 SVM，則 Light Agent 不會連線到 SVM。

- **略過**Light Agent 會略過用於連線到 Protection Server 的 SVM 路徑。Light Agent 會考慮其他標準：標籤、連線到 SVM 的 Light Agent 數量等。

7. 要將此政策套用到電腦，請關閉... 掛鎖圖示並儲存變更。

如何在 SVM 之間平衡 Light Agent 的連線

多個 Light Agent 可以連線到一個 SVM。若要平衡 Light Agent 連線，您可以指定單獨的 SVM 清單。如果您使用 Integration Server 用於 SVM 發現，則可以使用 *標籤* 平衡 Light Agent 與 SVM 的連線。也就是說，對於 Light Agent，您可以使用標籤來指派用於連線的 SVM 清單。為此，您必須為 Light Agent 指派一個標籤，並在 SVM 設定中指定該標籤。有關在 SVM 設定中指定標籤的詳細資訊，請參閱 Kaspersky Security for Virtualization Light Agent 說明。

範例：Kaspersky Endpoint Detection and Response Optimum 解決方案部署在您的指定虛擬機主機的基礎結構中。在這種情況下，您可以指派 `[EDROptimum]` 標記到 Light Agent，使其連線到新增了 EDR Optimum（EDR Optimum Add-on）產品授權金鑰的 SVM。結果，您可以在具有 Light Agent 的虛擬機上使用 EDR Optimum 功能。在沒有 EDR Optimum 產品授權金鑰的情況下將 Light Agent 連線到 SVM 時，Kaspersky Endpoint Detection and Response Optimum 功能不可用。

如何在 Web 主控台中將 SVM 連線標籤指派給 Light Agent

1. 在網頁主控台的主視窗中，選擇**資產管理 → 政策**。
2. 點擊 Kaspersky Endpoint Security 政策的名稱。
   政策內容視窗將開啟。
3. 選擇"**應用程式設定**"標籤。
4. 轉到"**Light Agent 模式**"→"**SVM 連線標記**"。
5. 選擇 **使用連線標記** 核取方塊並輸入 SVM 連線標籤。
   對於標籤，您可以輸入最長 255 個字元的文字字串。您可使用除 `;` 字元外的任何字元。
6. 要將此政策套用到電腦，請關閉... 掛鎖圖示並儲存變更。

保護 Light Agent 與 SVM 之間的連線

您可以設定 Light Agent 和 Protection Server 之間的連線加密。為此，您需要在 SVM 上的 Protection Server 設定和 Light Agent 設定中啟用 Light Agent 和 Protection Server 之間的資料管道加密。

啟用了連線防護的 Light Agent 只能連線到啟用了 Light Agent 與 Protection Server 之間資料管道加密的 SVM。停用連線防護的 Light Agent 只能連線到停用管道加密或允許 Protection Server 與 Light Agent 之間有不安全連線的 SVM。

有關在 Protection Server 上配置連線防護的詳細資訊，請參閱 Kaspersky Security for Virtualization Light Agent 說明。

使用加密保護連線可能會降低 Kaspersky Security for Virtualization Light Agent 的效能。

如何在 Web 主控台中配置 Light Agent 中的連線防護

1. 在網頁主控台的主視窗中，選擇**資產管理 → 政策**。
2. 點擊 Kaspersky Endpoint Security 政策的名稱。
   政策內容視窗將開啟。
3. 選擇"**應用程式設定**"標籤。
4. 轉到"**Light Agent 模式**"→"**連線防護**"。
5. 選擇"**加密 Light Agent 和 Protection Server 之間的資料渠道**"核取方塊。
6. 要將此政策套用到電腦，請關閉... 掛鎖圖示並儲存變更。

如何查看 Light Agent 的狀態

在命令列中，您可以檢視關於在 Light Agent 模式下使用的應用程式的以下資訊：

- 在 Light Agent 模式下使用應用程式的設定
- 將 Light Agent 連線到 Integration Server
- 將 Light Agent 連線到 SVM

檢視在 Light Agent 模式下使用應用程式的設定資訊

```
kesl-control [-V] --ksvla-info
```

此命令向主控台輸出以下資訊：

- 用於防護虛擬環境的 Light Agent 模式：開啟 或 關閉。

  如果啟用 Light Agent 模式，該應用程式將用作 Kaspersky Security for Virtualization Light Agent 解決方案的一部分。

- VDI 防護模式：開啟 或 關閉。

  VDI 防護模式最佳化了 Kaspersky Endpoint Security 在暫時虛擬機上的運作。如果啟用了 VDI 防護模式，則需要重新啟動受防護的虛擬機的更新不會安裝在暫時虛擬機上。當收到需要重新啟動的更新時，安裝在暫時虛擬機上的 Light Agent 會向卡巴斯基安全管理中心傳送一則訊息，提示需要更新受防護的虛擬機範本。

- 虛擬機類型：持續性或非持續性。
- 虛擬機角色：伺服器 或 工作站。
- 虛擬機 ID – UUID。

檢視 Light Agent 與 Integration Server 連線的資訊

```
kesl-control [-V] --viis-info
```

此命令向主控台輸出以下資訊：

- Light Agent 已連線的 Integration Server 的位址和連線埠。
- 與 Integration Server 的連線狀態。
- Light Agent 和 Integration Server 之間上次連線的日期和時間。

如果您的基礎架構具有基於 Linux 的高可用性叢集，則會顯示負載平衡器的位址和連接埠。如需更多詳細資訊，請參閱 Kaspersky Security for Virtualization Light Agent 說明。

檢視 Light Agent 與 SVM 連線的資訊

```
kesl-control [-V] --svm-info
```

此命令向主控台輸出以下資訊：

- Light Agent 連線到的 SVM 的位址，以及虛擬基礎架構中 SVM 相對於 Light Agent 的定位：本機或非本機。
- Light Agent 使用的 SVM 發現方法：使用 Integration Server 或使用 SVM 位址的自訂清單。
- SVM 位址清單（如果選取的 SVM 發現方法是 SVM 位址清單）。
- 用於將 Light Agent 連線到 SVM 的標籤。
- SVM 選擇演算法：標準或進階。如果使用延伸 SVM 選擇演算法，則也會顯示 SVM 在虛擬基礎架構中的定位類型。
- Light Agent 和 Protection Server 之間的連線。

關於將 Light Agent 連線到 Integration Server 和 SVM 的設定的資訊，請參閱Kaspersky Security for Virtualization Light Agent 說明。

最佳做法

部署 Kaspersky Endpoint Security for Linux 時，您可以使用本節所述建議來設定電腦防護並最佳化效能。有關處理電腦效能問題的更多資訊，請參閱技術支援知識庫。

最佳化應用程式的資源消耗

使用預設設定執行的應用程式可能會影響某些裝置上的系統效能，因為應用程式和 Kaspersky Endpoint Security 所使用的資源相同。

最佳化應用程式系統資源消耗的建議設定案例：

1. **依據基礎架構中每個裝置的角色，將裝置放入管理群組中。**

   對裝置及其執行的功能進行清查，並依據這些功能將其放入不同的管理群組中。例如，可以有一個包含網頁伺服器的管理群組、一個包含資料庫伺服器的管理群組以及一個包含使用者工作站的管理群組等等。

2. **為常見的伺服器角色設定應用程式。**

   依照建議，根據裝置在基礎架構中的角色設定應用程式。

3. **分析試點裝置上的效能。**

   在每個管理群組中挑選一或兩個試點裝置。對於每台裝置，需分析 Kaspersky Endpoint Security 的系統資源使用情況及其對已安裝應用程式的效能影響。

4. **依據效能分析結果在試點裝置上設定應用程式。**

   如果應用程式的效能顯著下降，或者 Kaspersky Endpoint Security 所消耗的系統資源量將對作業系統和應用程式的運作產生重要影響，請依照建議設定檔案威脅防護和掃描工作。

   若要降低 Web 威脅防護、網路威脅防護和 行為偵測 元件對您應用程式效能的影響，請最佳化這些元件的效能。

5. **在所有裝置上設定應用程式。**

   如果上述步驟有助於提升試點裝置的效能，可在其他同類型裝置上進行相同的變更。

裝置上的應用程式效能分析

掃描物件時，Kaspersky Endpoint Security 使用 CPU 資源、磁碟子系統輸入/輸出和 RAM。

檢視應用程式資源消耗的資訊

```
top -bn1|grep kesl
```

該命令必須在系統處於負載狀態下執行。

指令輸出顯示已使用的記憶體量和處理器時間：

```
651 root        20      0 3014172 2.302g 154360 S 120.0 30.0    0:32.80 kesl
```

第 6 欄顯示駐留記憶體量：2.302g。

第 9 列顯示處理器核心使用的百分比 - 120.0，其中每個核心佔 100%。因此，120% 意味著一個核心被充分利用，而另一個核心使用了 20%。

若要取得應用程式效能的相關資訊，您也可以配置應用程式使用的作業系統資源指標收集。

如果 Kaspersky Endpoint Security 嚴重降低系統速度，您需要找出哪些應用程式元件和工作正在佔用系統資源。

為此，請在裝置上執行以下實驗：

1. **分析「檔案威脅防護」工作（OAS 類型的工作）的資源消耗**

   這樣一來，您可以瞭解效能問題是否與「檔案威脅防護」工作或掃描工作（ODS 和 ContainerScan 類型的工作）有關，並遵循相關工作的建議。

   如何分析「檔案威脅防護」工作的資源消耗

   1. 停止所有掃描和監控工作。
   2. 請確認在調查期間不排定執行自訂掃描工作（ODS 和 ContainerScan 類型的工作）：

      a. 取得所有應用程式工作的清單：

      ```
      kesl-control --get-task-list
      ```

      b. 取得所有 ODS 和 ContainerScan 類型工作的排程設定：

      ```
      kesl-control --get-schedule <task ID |name>
      ```

      如果指令輸出為 `RuleType=Manual`，則表示只能手動啟動工作。

      c. 對於所有 `RuleType` 不是 `Manual` 的工作，變更排程：

      ```
      kesl-control --set-schedule <task ID |name> RuleType=Manual
      ```

   3. 啟用產生高詳細程度的應用程式偵錯檔案：

      ```
      kesl-control --set-app-settings TraceLevel=Detailed
      ```

   4. 如果「檔案威脅防護」工作未執行，請啟動它：

      ```
      kesl-control --start-task 1
      ```

   5. 以導致效能問題的相同模式對系統施加負載。數小時即可。
   6. 分析生成的偵錯檔案。預設情況下，偵錯檔案將保存在 /var/log/kaspersky/kesl/ 目錄中。

應用程式會在負載狀態下將大量資訊寫入偵錯檔案；但是僅會保留 10 個檔案（每個檔案大小為 500 MB），這意味著舊資訊將被覆蓋。

如果效能和資源消耗問題仍然存在，可能需要最佳化檔案威脅防護。

如果效能和資源消耗問題不再發生，則這些問題的最可能原因是自訂掃描工作（ODS 和 ContainerScan 類型的工作）或「行為偵測」工作。您需要最佳化掃描工作，或分析「行為偵測」工作的效能。

7. 停用建立應用程式偵錯檔案：

```
kesl-control --set-app-settings TraceLevel=None
```

2. **分析「行為偵測」工作（Behavior_Detection 類型的工作）的資源使用量。**

這樣一來，您可以瞭解效能問題是否與「行為偵測」工作或掃描工作（ODS 和 ContainerScan 類型的工作）有關，並遵循相關工作的建議。

如何分析「行為偵測」工作的資源使用量

1. 停止所有掃描和監控工作。
2. 請確認在調查期間不排定執行自訂掃描工作（ODS 和 ContainerScan 類型的工作）：
   a. 取得所有應用程式工作的清單：

   ```
   kesl-control --get-task-list
   ```

   b. 取得所有 ODS 和 ContainerScan 類型工作的排程設定：

   ```
   kesl-control --get-schedule <task ID|name>
   ```

   如果指令輸出為 `RuleType=Manual`，則表示只能手動啟動工作。

   c. 對於所有 `RuleType` 不是 `Manual` 的工作，變更排程：

   ```
   kesl-control --set-schedule <task ID|name> RuleType=Manual
   ```

3. 啟用產生高詳細程度的應用程式偵錯檔案：

```
kesl-control --set-app-settings TraceLevel=Detailed
```

4. 如果「行為偵測」工作未執行，請啟動它：

```
kesl-control --start-task 20
```

5. 以導致效能問題的相同模式對系統施加負載。數小時即可。
6. 分析生成的偵錯檔案。預設情況下，偵錯檔案將保存在 /var/log/kaspersky/kesl/ 目錄中。

應用程式會在負載狀態下將大量資訊寫入偵錯檔案；但是僅會保留 10 個檔案（每個檔案大小為 500 MB），這意味著舊資訊將被覆蓋。

如果效能和資源消耗問題仍然存在，您可能需要最佳化「行為偵測」。

如果效能和資源消耗問題不再發生，則這些問題的最可能原因是自訂掃描工作（ODS 和 ContainerScan 類型的工作）。這意味著您需要最佳化這些工作。

7. 停用建立應用程式偵錯檔案：

```
kesl-control --set-app-settings TraceLevel=None
```

3 識別最常掃描的物件

您可以從掃描中排除無危險性且經常掃描的物件和檔案，以最佳化檔案威脅防護和掃描工作的效能。

判斷掃描次數最多的物件是否危險。例如，如果寫入操作由受信任處理程序執行，則資料庫檔案、目錄和記錄檔案均可被視為安全。如果遇到任何困難，請聯絡技術支援。

如何識別最常掃描的物件

1. 取得掃描次數最多的物件清單：

```
fgrep 'AVP ENTER' /var/log/kaspersky/kesl/kesl.* | awk '{print $8}' | sort | uniq -c | sort -k1 -n -
r|less
```

結果會載入到 less 文字檢視器公用程式中，其中會先顯示掃描次數最多的物件。

若需要從根目錄 / 開始，將子目錄中的物件掃描統計資料彙整至特定深度，您可以將 `cut -d/ -f 1-X` 新增至命令，其中 X 為巢狀深度。範例：

```
fgrep 'AVP ENTER' /var/log/kaspersky/kesl/kesl.* | awk '{print $8}' | cut -d/ -f 1-4 | sort | uniq -c |
sort -k1 -n -r|less
```

2. 如果各類服務經常將資料寫入系統中的檔案，則此類檔案會在待處理佇列中被再次掃描。取得待處理佇列中掃描次數最多的路徑清單：

```
fgrep 'SYSCALL' /var/log/kaspersky/kesl/kesl.* | fgrep 'KLIF_ACTION_CLOSE_MODIFY' | awk '{print $10}' |
sort | uniq -c | sort -k1 -n -r
```

被掃描次數最多的檔案將出現在清單的開頭。

若需要從根目錄 / 開始，將子目錄中的物件掃描統計資料彙整至特定深度，您可以將 `cut -d/ -f 1-X` 新增至命令，其中 X 為巢狀深度。範例：

```
fgrep 'SYSCALL' /var/log/kaspersky/kesl/kesl.* | fgrep 'KLIF_ACTION_CLOSE_MODIFY' | awk '{print $10}' |
tr -d ',' |  cut -d/ -f 1-3 | sort | uniq -c | sort -k1 -n -r
```

4 識別 Kaspersky Endpoint Security 最常偵測到啟動的程序

您可以從掃描中排除無危險性且經常啟動的程序，以最佳化「行為偵測」的效能。

如何識別最常啟動的程序

執行命令：

```
kesl-control --get-statistic --processes
```

此命令會輸出 Kaspersky Endpoint Security 最常偵測到其啟動的處理程序清單，以及這些處理程序的啟動次數。

5 **識別檔案操作攔截發生次數最多的路徑**

您可以從檔案操作攔截中排除目錄，以最佳化檔案威脅防護和掃描工作的效能。

如何取得檔案操作攔截相關資訊

您可以透過以下方式取得檔案操作攔截相關資訊：

- 取得檔案威脅防護元件最常掃描的檔案統計資料：

  ```
  kesl-control --get-statistic --files
  ```

  此命令可顯示過去 24 小時內的檔案操作攔截統計資料。

- 使用應用程式偵錯檔案進行更詳細的分析。透過分析偵錯檔案，可以取得應用程式攔截的檔案清單，並識別與大量檔案操作攔截關聯的路徑。

  預設情況下，應用程式不會生成偵錯檔案。

  啟用偵錯檔案建立

  ```
  kesl-control --set-app-settings TraceLevel=Detailed
  ```

  啟用偵錯可能會影響整體系統效能。如果不再需要偵錯檔案，建議停用偵錯。

  停用偵錯檔案建立

  ```
  kesl-control --set-app-settings TraceLevel=None
  ```

- 取得已攔截檔案清單：

  ```
  grep 'FACACHE.*needs' /var/log/kaspersky/kesl/kesl.* | awk '{print $9}' | tr -d '}'|awk -F':' '{print
  $2}'|sort | uniq -c | sort -k1 -n -r
  ```

  若需要從根目錄 / 開始，將子目錄中的檔案操作攔截統計資料彙整至特定深度，您可以將 `cut -d/ -f 1-X` 新增至命令，其中 X 為巢狀深度。範例：

  ```
  grep 'FACACHE.*needs' /var/log/kaspersky/kesl/kesl.* | awk '{print $9}' | tr -d '}'|awk -F':' '{print
  $2}'| cut -d/ -f 1-3|sort | uniq -c | sort -k1 -n -r|less
  ```

您可以在命令列上分析應用程式效能。如果裝置受卡巴斯基安全管理中心政策管理，請在調查期間允許本機工作管理。

檔案威脅防護和掃描工作建議

一般建議

掃描排除項目

掃描排除項目可協助均衡系統安全性與效能。

建議將以下項目排除在掃描範圍之外：

- 資料庫的資料檔案和索引檔案。根據卡巴斯基病毒專家的說法，病毒不會透過此類檔案傳播。
- 來自最常掃描的物件清單的安全物件。

可透過檔案路徑（也可以指定掛載類型）、檔案遮罩、威脅類型和執行檔案操作的處理程序路徑設定排除項目。

> 應用程式不會掃描排除在掃描範圍之外的物件，但檔案操作仍會產生輕微延遲，因為應用程式仍會對檔案操作執行攔截和封鎖。如果您需要避免哪怕是極短暫的延遲，建議設定檔案操作攔截的排除項目。

如何設定排除項目：

- 您可透過網頁主控台或管理主控台在政策中設定檔案威脅防護排除項目，或透過命令列在本機裝置上設定檔案威脅防護排除項目。
- 您可以在卡巴斯基安全管理中心的工作設定中，或使用命令列在裝置本機，設定 ODS 和容器掃描類型掃描工作的排除項目。

  > 為一個掃描工作設定的排除項目不會影響其他掃描工作。必須為每個掃描工作單獨配置排除項目。

在命令列中設定檔案威脅防護排除項目的範例

以遞迴方式排除 `/tmp/logs` 目錄及其所有子目錄和檔案

```
kesl-control --set-settings 1 --add-exclusion /tmp/logs
```

透過遮罩排除 `/tmp/logs` 目錄中的特定檔案或檔案群組

```
kesl-control --set-settings 1 --add-exclusion /tmp/logs/*.log
```

使用遞迴遮罩排除 `/tmp` 目錄及子目錄中所有副檔名為 `.log` 的檔案

```
kesl-control --set-settings 1 --add-exclusion /tmp/**/*.log
```

檔案操作攔截的排除項目

在檔案威脅防護和掃描工作期間，應用程式仍可能會攔截排除在掃描之外的檔案。應用程式會在對事件進行處理之前，攔截檔案操作事件並封鎖動作。掃描後，應用程式可以：

- 解鎖並允許操作。
- 封鎖操作並執行防護或驗證設定中指定的動作。

攔截事件需要一些時間，這會影響其他應用程式和作業系統的效能。

> 如果您的作業系統支援 fanotify 技術並符合要求，請為應用程式設定可更新的內核模組。可更新的內核模組包含在應用程式分發套裝中。可更新的內核模組可最佳化檔案操作攔截。

若要將特定目錄中的檔案不僅排除在掃描之外，也排除在攔截之外，請設定掛載點排除（全域排除項目）。排除掛載點可讓您排除裝置上掛載的本機或遠端目錄以阻止檔案操作的攔截。

您可以使用網頁主控台、管理主控台或命令列，檢視在裝置上偵測到的掛載點清單。該清單會顯示資訊，指出掛載點是否已新增至掃描排除項目。

卡巴斯基專家建議在以下情況下使用全域排除：

- 與已掛載遠端資源（例如 NFS 或 SMB）的連線速度緩慢。
- 即使輕微延遲也無法接受。

您可以指定掛載點類型（Local、AllRemoteMounted、Mounted:NFS、Mounted:SMB 或 Mounted:Custom）或特定掛載點。應用程式不會監控已排除的範圍。

> 要防護共用網路資源，可在資源實體儲存的裝置上使用 Kaspersky Endpoint Security 應用程式。

如果您使用可更新的內核模組進行系統事件攔截，則可以將裝置上掛載的個別本機或遠端目錄排除在攔截之外，而不僅限於整個掛載點。

> 如果您使用 fanotify 進行系統事件攔截，則全域排除項目不適用於不是掛載點的路徑。

您可以使用網頁主控台或管理主控台在政策中設定全域排除項目，或使用命令列在裝置本機設定。

使用命令列為 /tmp 目錄設定全域排除項目的範例

要將 /tmp 目錄中的所有檔案排除在攔截之外，請執行以下操作：

1. 如果您使用 fanotify 進行系統事件攔截，請檢查 /tmp 目錄是否為掛載點：

```
mount
```

如果 mount 指令的輸出中沒有該目錄：

a. 建立掛載點：

```
mount --bind /tmp/ /tmp
```

b. 將以下行新增至 /etc/fstab 檔案，使新建立的掛載點在系統重新啟動後持續存在：

```
/tmp /tmp none defaults,bind 0 0
```

如果您使用可更新的內核模組進行系統事件攔截，請跳過此步驟。

2. 將 /tmp 目錄新增至全域排除項目：

```
kesl-control --set-app-settings ExcludedMountPoint.item_0000=/tmp
```

3. 重新啟動應用程式以套用全域排除：

```
systemctl restart kesl
```

限制應用程式的 RAM 使用量

您可以限制 Kaspersky Endpoint Security 使用檔案威脅防護元件掃描檔案以及執行 ODS 和 ContainerScan 類型的掃描工作時使用的 RAM 量。

對於具有大量 RAM（超過 5 GB）的系統，限制記憶體使用量非常有用。

預設情況下，應用程式最多可使用 8192 MB 的 RAM。您可以調整應用程式使用的 RAM 量：

- 在政策中，使用**掃描工作的記憶體使用限制 (MB)** 設定。
- 在裝置本機使用 kesl.ini 設定檔中的 `ScanMemoryLimit` 設定。

如果指定的值小於 2 MB，應用程式將使用最小值 (2 MB)。如果指定的值大於裝置上可用的 RAM 量，則應用程式最多會使用 25% 的 RAM。此值無法變更。

> 此設定僅限制掃描檔案時使用的記憶體量。這意味著應用程式所需的記憶體總量可能超過此設定的值。

檔案威脅防護的其他建議

僅在開啟檔案時掃描

將檔案掃描模式變更為僅在開啟檔案時掃描檔案。預設情況下，如果嘗試開啟檔案，應用程式會掃描該檔案；若檔案已被修改，則在嘗試關閉該檔案後，應用程式會再次掃描該檔案。

可在檔案威脅防護設定中變更檔案掃描模式：

- 透過網頁主控台或管理主控台在政策中：將**檔案威脅防護模式**設定為**開啟時**。
- 在裝置本機：

```
kesl-control --set-set 1 ScanByAccessType=Open
```

檔案開啟後對其所做的變更不會被掃描，直到下次開啟檔案時才會被掃描。

掃描壓縮檔案

確保壓縮檔案掃描已停用（預設設定）。掃描壓縮檔案會影響效能，因為在將壓縮檔案解壓縮到 /tmp 暫存目錄並進行掃描時，會封鎖對壓縮檔案的存取。壓縮檔案的定義範圍包括傳統的壓縮檔案以及 .jar 等封裝物件。

既可透過網頁主控台或管理主控台（**掃描壓縮檔案**設定）啟用或停用壓縮檔案掃描，也可透過命令列（`ScanArchived` 設定）在本機裝置上啟用或停用壓縮檔案掃描。

掃描從網路目錄複製的檔案

為從網路目錄複製的檔案設定掃描排除。僅當複製到本機目錄的過程完成後才會掃描檔案。

若要從掃描中排除位於網路目錄中的檔案，請根據用於從網路目錄複製的實用程式（例如，`cp` 實用程式）的處理程序配置排除項目。

如果使用卡巴斯基安全管理中心管理應用程式，您可以根據網頁主控台或管理主控台中的處理程序配置排除項目。如果您使用命令列管理應用程式，則可以透過將 `[ExcludedForProgram.item_#]` 區段新增至 OAS 工作的設定，來設定按處理程序排除。

掃描工作的其他建議

工作啟動排程

排定掃描工作，避免工作重疊。該應用程式允許同時執行多個掃描工作，但這可能會顯著增加資源消耗。在本機裝置上或在卡巴斯基安全管理中心中檢查所有 ODS 和 ContainerScan 工作的排程。

在伺服器負載最低時執行掃描。

掃描遠端目錄

確保掃描工作範圍不包括透過 SMB 或 NFS 掛載在裝置上的任何遠端目錄。

建議直接在提供資源的裝置上掃描此類目錄。如果無法實現，請勿在執行關鍵服務的伺服器上執行掃描，因為此類工作可能耗時較長（取決於連線速度與檔案數量）。

使用全域排除項目和檔案威脅防護排除項目

確保已為惡意軟體掃描工作啟用以下設定：

- **使用全域排除項目** (`UseGlobalExclusions`) 以從掃描中排除全域排除項目中指定的掛載點。
- **使用檔案威脅防護排除項目** (`UseOASExclusions`) 以在掃描期間使用已設定的檔案威脅防護排除項目。

預設情況下，這兩個設定均已啟用。

> 為了最佳化掃描工作的運行，建議將系統以唯讀模式掛載的快照路徑新增至具有 btrfs 檔案系統且啟用活動快照的系統的排除項目中。例如，對於基於 SUSE/OpenSUSE 的系統，您可以為路徑新增以下排除：`/.snapshots/*/snapshot/`。

關於 Web 威脅防護和網路威脅防護工作的建議

一般建議

作業系統的防火牆

如果系統自帶包含丟棄政策的網路規則（或 firewalld 規則），為確保應用程式正常運作，請新增一條接受規則，以允許來自本機裝置（回送）的傳入連線：

iptables 的範例命令

```
iptables -A INPUT -i lo -j ACCEPT
```

受監控網路連接埠清單

限制應用程式監控的網路連接埠清單。預設情況下，應用程式將僅監控已選取的網路連接埠。如果裝置使用 SMB 連線，請確保使用預設值：

- 透過網頁主控台或管理主控台在政策中：於網路流量掃描設定內，選取**僅監控選定的網路連接埠**選項。
- 在本機裝置上：`MonitorNetworkPort` 網路流量掃描設定設為 `Selected`。

將應用程式與 HAProxy 搭配使用

將應用程式與 HAProxy 負載平衡器搭配使用時：

1. 開啟 /var/opt/kaspersky/kesl/common/kesl.ini 設定檔，建立 `[Environment]` 區域並向其新增 `TcpSynInterceptDisabled=1` 設定。
2. 重新啟動應用程式：

   ```
   systemctl restart kesl
   ```

將應用程式與 Kubernetes 搭配使用

若要讓 Web 威脅防護和網路威脅防護元件與使用 Calico 和 Cilium 網路外掛程式的 Kubernetes 叢集搭配運作，請在 kesl.ini 設定檔中管理 `WtpFwMark`、`NtpFwMark`、`BypassFwMark` 和 `BypassNflogMark` 設定。

收到「應用程式模組完整性檢查失敗」錯誤時該怎麼辦

Web 威脅防護的建議

憑證驗證政策

預設情況下，Web 威脅防護元件會解密並掃描透過加密連線傳送的網路流量。在此期間，元件可以使用網際網路進行驗證，並下載驗證憑證所需的缺失鏈。

如果裝置無法直接存取網際網路，請執行以下其中一項操作：

- 在網路流量掃描設定中選取本機憑證驗證方法：
  - 透過網頁主控台或管理主控台在政策中：將**憑證驗證政策**設定為**本機檢查**。
  - 在裝置本機使用命令列：

    ```
    kesl-control --set-net-settings CertificateVerificationPolicy=LocalCheck
    ```

  應用程式不會使用網際網路來驗證憑證。

- 透過代理伺服器設定網際網路存取：
  - 在政策中，使用網頁主控台或 管理主控台：設定代理伺服器設定。
  - 在裝置本機使用命令列：

    啟用使用需要身分驗證的代理伺服器

    ```
    kesl-control --set-app-settings UseProxy=Yes ProxyServer=<connection protocol>://<user name>:<password>@<IP address of the proxy server>:<port number>
    ```

    啟用使用不需要身分驗證的代理伺服器

    ```
    kesl-control --set-app-settings UseProxy=Yes ProxyServer=<connection protocol>://<IP address of the proxy server>:<port number>
    ```

網路威脅防護的建議

與 REDIRECT 規則的相容性

為確保網路威脅防護元件的攔截規則與 REDIRECT 規則相容（例如，從連接埠 443 重新導向至 8443）：

1. 刪除規則：

   ```
   iptables -t nat -A PREROUTING -p tcp -m tcp --dport 443 -j REDIRECT --to-ports 8443
   ```

2. 將其取代為以下規則：

```
iptables -t nat -A PREROUTING -p tcp -m tcp --dport 443 -m mark ! --mark 0x400/0x400 -j REDIRECT --to-ports
8443
iptables -t nat -A OUTPUT -p tcp --dport 443 -m mark --mark 0x400/0x400 -m addrtype ! --src-type LOCAL -j DNAT
--to-destination :8443
```

行為偵測建議

我們建議將行為偵測元件最常掃描的處理程序活動排除在掃描之外。

若要找出最常啟動的處理程序，請執行以下命令：

```
kesl-control --get-statistic --processes
```

此命令會輸出 Kaspersky Endpoint Security 最常偵測到其啟動的處理程序清單，以及這些處理程序的啟動次數。

您可以使用網頁主控台或管理主控台在政策中設定排除，或使用命令列在裝置本機上設定。

預設情況下，只有指定的處理程序會排除在掃描之外；行為偵測會繼續掃描已排除處理程序的子處理程序。

在命令列上設定排除的範例

將 my_program1 和 my_program2 的活動排除在掃描之外

```
kesl-control --set-settings 20 UseTrustedPrograms=Yes TrustedPrograms.item_0000.ProgramPath=/bin/my_program1
TrustedPrograms.item_0001.ProgramPath=/bin/my_program2
```

將 my_program1 及其子處理程序的活動排除在掃描之外

```
kesl-control --set-settings 20 UseTrustedPrograms=Yes TrustedPrograms.item_0000.ProgramPath=/bin/my_program1
TrustedPrograms.item_0000.ApplyToDescendants=Yes
```

與卡巴斯基解決方案的互通性

Kaspersky Endpoint Security 應用程式支援與部分卡巴斯基解決方案的互通性。為了實現應用程式的最佳互通性，請遵循本節中的指南。

卡巴斯基安全管理中心 Linux

將 Kaspersky Endpoint Security for Linux 與卡巴斯基安全管理中心 Linux 搭配使用時，建議使用本文所述設定。

應用程式元件	建議的元件狀態	建議
檔案威脅防護	已啟用	新增防護排除項目： • /opt/kaspersky/klnagent/sbin/klnagent • /opt/kaspersky/klnagent64/sbin/klnagent • /var/lib/postgresql/<PostgreSQL version>
惡意軟體掃描	已啟用	
卸除式磁碟機掃描	已停用	–
行為偵測	已啟用	使用預設設定。
網路威脅防護	已啟用	選取 eBPF 網路流量攔截模式 NetInterceptorMode=UseEBPF
Web 威脅防護	已啟用	使用預設設定。
Anti-Cryptor	已停用	–
容器掃描	已停用	–
清查	已停用	–
裝置控制	已停用	–
應用程式控制	已停用	–
防火牆	已停用	–
Web 控制	已停用	–
系統完整性監控	已啟用	新增掃描範圍： • /etc • /opt/kaspersky/kesl/ • /opt/kaspersky/ksc64
系統完整性檢查	已停用	–
Endpoint Detection and Response Expert (on-premises)	已啟用	使用預設設定。
Endpoint Detection and Response Expert (cloud)	已停用	–
Managed Detection and Response	已啟用	使用預設設定。
Network Detection and Response (KATA)	已停用	–
與 KUMA 整合	已停用	–
Sandbox	已停用	–
回應動作	存在一些限制	針對回應動作，您無法排除 Kaspersky Endpoint Security for Linux 所需的物件以及關鍵系統物件。啟動回應動作時，請確保這些動作不會干擾系統和您使用的應用程式。
圖形介面	未設定	–
Kaspersky Endpoint Security for Linux 管理 Web 外掛程式	已安裝	使用預設設定。
Kaspersky Endpoint Security for Linux MMC 管理外掛程式	已安裝	使用預設設定。
網路代理	已安裝	使用預設設定。
檔案操作攔截機制	基於 fanotify 的系統攔截機制	使用預設設定。
系統事件遙測來源	eBPF+auditd	TelemetrySource=Default
弱點利用防禦	已停用	–
使用卡巴斯基安全網路	已啟用	使用預設設定。
郵件威脅防護	已啟用	使用預設設定。

應用程式元件	建議的元件狀態	建議
BadUSB 攻擊防護	已停用	–
全域排除項目	已設定	如果您使用快速安裝指令碼 安裝卡巴斯基安全管理中心，請將掛載點新增至排除項目： `/var/lib/postgresql/<PostgreSQL version>/main` 其中 `<PostgreSQL version>` 是您使用的 PostgreSQL DBMS 版本號碼。

Network Detection and Response (KATA)

搭配 Network Detection and Response (KATA) 使用 Kaspersky Endpoint Security for Linux 時，建議使用本文所述的設定。

另請參閱 卡巴斯基 Anti Targeted Attack (KATA) Platform 解決方案說明文件 。

具有 Sensor 元件的伺服器上 Kaspersky Endpoint Security for Linux 的設定

Sensor 伺服器的建議設定

應用程式元件	建議的元件狀態	建議
檔案威脅防護	已啟用	新增防護排除項目： • `[container-name:*kata_scanner*]/var/opt/kaspersky/apt-collector/spool` • `[container-name:*kata_scanner*]/data/var/opt/kaspersky/apt-collector/spool` • `[container-name:*kata_scanner*]/storage/data/var/opt/kaspersky/apt-collector/spool` • `[container-name:*preprocessor_icap*]/tmp/content` • `[container-name:*preprocessor_span*]/tmp/suricata` • `[container-name:*preprocessor_span*]/mnt/kaspersky/nta` • `[container-name:*preprocessor_smtp*]/tmp/` • `[container-name:*preprocessor_pop*]/tmp/` • `[container-name:*sandbox_scan*]/tmp/` • `[container-name:*]/var/log/kaspersky`
惡意軟體掃描	已停用	–
卸除式磁碟機掃描	已停用	–
行為偵測	已啟用	使用預設設定。
網路威脅防護	已停用	–
Web 威脅防護	已停用	–
Anti-Cryptor	已停用	–
容器掃描	已啟用	啟用容器監控，以即時掃描執行中的容器和命名空間 `NamespaceMonitoring=Yes`
清查	已停用	–
裝置控制	已停用	–
應用程式控制	已停用	–
防火牆	已停用	–
Web 控制	已停用	–
系統完整性監控	已停用	–
系統完整性檢查	已停用	–

應用程式元件	建議的元件狀態	建議
Endpoint Detection and Response Expert (on-premises)	已停用	–
Endpoint Detection and Response Expert (cloud)	已停用	–
Managed Detection and Response	已停用	–
Network Detection and Response (KATA)	已停用	–
與 KUMA 整合	已停用	–
Sandbox	已停用	–
回應動作	已停用	–
圖形介面	未設定	–
網路代理	已安裝	使用預設設定。
檔案操作攔截機制	基於 fanotify 的系統攔截機制	使用預設設定。
系統事件遙測來源	eBPF+auditd	`TelemetrySource=Default`
弱點利用防禦	已停用	–
使用卡巴斯基安全網路	已啟用	使用預設設定。
郵件威脅防護	已停用	–
BadUSB 攻擊防護	已停用	–
偵錯檔案	–	將偵錯檔案的目錄變更為 `/var/log/kaspersky` 目錄以外的目錄。例如，使用 `/var/log/kesl` 目錄。
全域排除項目	已設定	排除下列掛載點： • `/apt_spool` • `/storage` • `/var/lib/postgresql` • `/var/lib/clickhouse` • `/tmp/apttmp/*` • `/tmp/suricata/*` • `/tmp/traffic/*` • `/tmp/apt_certs/*` tmp/apttmp/*、/tmp/suricata/*、/tmp/traffic/* 和 /tmp/apt_certs/* 掛載點的排除適用於 8.0 版和更早版本的 NDR (KATA) 伺服器。 • `/varog/kaspersky` • `/var/opt/kaspersky` • `/data` • `/data/volumes/dumps`

具有 Central Node 元件的伺服器上 Kaspersky Endpoint Security for Linux 的設定

Central Node 伺服器的建議設定

應用程式元件	建議的元件狀態	建議
檔案威脅防護	已啟用	新增防護排除項目： • [container-name:*edr_synchronizer*]/tmp/ • [container-name:*ids_alert_syncer*]/tmp/ • [container-name:kata_product_main_1_kata_scanner]/storage • [container-name:kata_product_main_1_postgresql_server]/var/lib/postgresql • [container-name:kata_product_main_1_clickhouse]/var/lib/clickhouse • [container-name:*kata_scanner*]/storage/data/var/opt/kaspersky/apt-collector/spool • [container-name:*kata_scanner*]/var/opt/kaspersky/apt-agents • [container-name:*kata_scanner*]/var/lib/nginx/body • [container-name:*kata_scanner*]/apt_spool • [container-name:*kata_scanner*]/tmp/ • [container-name:*kafka*]/tmp/ • [container-name:*ksn_proxy*]/tmp/ • [container-name:*preprocessor_smtp*]/tmp/ • [container-name:*preprocessor_pop*]/tmp/ • [container-name:*preprocessor_icap*]/tmp/ • [container-name:*preprocessor_span*]/tmp/ • [container-name:*sandbox_scan*]/tmp/ • [container-name:*statistics_clickhouse_importer*]/tmp/ • [container-name:*updates_consistency_checker*]/tmp/ • [container-name:*web_backend*]/tmp/ • [container-name:*]/var/opt/kaspersky • /tmp/ • /var/log/kaspersky
惡意軟體掃描	已停用	–
卸除式磁碟機掃描	已停用	–
行為偵測	已啟用	使用預設設定。
網路威脅防護	已停用	–
Web 威脅防護	已停用	–
Anti-Cryptor	已停用	–
容器掃描	已啟用	啟用容器監控，以即時掃描執行中的容器和命名空間 NamespaceMonitoring=Yes
清查	已停用	–
裝置控制	已停用	–
應用程式控制	已停用	–
防火牆	已停用	–
Web 控制	已停用	–
系統完整性監控	已停用	–
系統完整性檢查	已停用	–
Endpoint Detection and Response Expert (on-premises)	已停用	–
Endpoint Detection and Response Expert (cloud)	已停用	–
Managed Detection and Response	已停用	–
Network Detection and Response (KATA)	已停用	–

應用程式元件	建議的元件狀態	建議
與 KUMA 整合	已停用	–
Sandbox	已停用	–
回應動作	已停用	–
圖形介面	未設定	–
網路代理	已安裝	使用預設設定。
檔案操作攔截機制	基於 fanotify 的系統攔截機制	使用預設設定。
系統事件遙測來源	eBPF+auditd	`TelemetrySource=Default`
弱點利用防禦	已停用	–
使用卡巴斯基安全網路	已啟用	使用預設設定。
郵件威脅防護	已停用	–
BadUSB 攻擊防護	已停用	–
偵錯檔案	–	將偵錯檔案的目錄變更為 `/var/log/kaspersky` 目錄以外的目錄。例如，使用 `/var/log/kesl` 目錄。
全域排除項目	已設定	將掛載點新增至排除項目： • `/apt_spool` • `/storage` • `/var/lib/postgresql` • `/var/lib/clickhouse` • `/tmp/apttmp/*` • `/tmp/suricata/*` • `/tmp/traffic/*` • `/tmp/apt_certs/*` tmp/apttmp/*、/tmp/suricata/*、/tmp/traffic/* 和 /tmp/apt_certs/* 掛載點的排除適用於 8.0 版和更早版本的 NDR (KATA) 伺服器。 • `/var/log/kaspersky` • `/var/opt/kaspersky` • `/data`

Kaspersky Unified Monitoring and Analysis Platform

將 Kaspersky Endpoint Security for Linux 與 Kaspersky Unified Monitoring and Analysis Platform 搭配使用時，建議使用本文所述的設定。

建議設定

應用程式元件	建議的元件狀態	建議
檔案威脅防護	已啟用	新增防護排除項目： • `/opt/kaspersky/kuma` • `/opt/kaspersky/klnagent/sbin/klnagent` • `/opt/kaspersky/klnagent64/sbin/klnagent`
惡意軟體掃描	已停用	–
卸除式磁碟機掃描	已停用	–
行為偵測	已啟用	將處理程序排除於掃描之外 `/opt/kaspersky/kuma`
網路威脅防護	已啟用	停用封鎖已遭入侵的裝置 `BlockAttackingHosts=No`

應用程式元件	建議的元件狀態	建議
Web 威脅防護	已停用	–
Anti-Cryptor	已停用	–
容器掃描	已停用	–
清查	已停用	–
裝置控制	已停用	–
應用程式控制	已停用	–
防火牆	已停用	–
Web 控制	已停用	–
系統完整性監控	已停用	–
系統完整性檢查	已停用	–
Endpoint Detection and Response Expert (on-premises)	已停用	–
Endpoint Detection and Response Expert (cloud)	已停用	–
Managed Detection and Response	已停用	–
Network Detection and Response (KATA)	已停用	–
與 KUMA 整合	已停用	–
Sandbox	已停用	–
回應動作	已停用	–
圖形介面	未設定	–
網路代理	已安裝	使用預設設定。
檔案操作攔截機制	基於 fanotify 的系統攔截機制	使用預設設定。
系統事件遙測來源	eBPF+auditd	`TelemetrySource=Default`
弱點利用防禦	已停用	–
使用卡巴斯基安全網路	已啟用	使用預設設定。
郵件威脅防護	已停用	–
BadUSB 攻擊防護	已停用	–

應用程式元件參考

用於管理 Kaspersky Endpoint Security 的指令

在指令列中，Kaspersky Endpoint Security 使用 Kaspersky Endpoint Security 管理指令來管理。

您可以透過執行以下指令檢視管理指令說明：

```
kesl-control --help <prefix of command group>
```

其中 `<prefix of command group>` 可採用以下值：

- `-A`：用於管理應用程式控制的指令
- `-B`：用於管理備份的指令
- `-C`：用於管理一般容器掃描設定的指令
- `-D`：用於管理裝置控制的指令
- `-E`：用於檢視目前應用程式事件的指令
- `-F`：用於防火牆管理的指令
- `-H`：用於管理被加密軟體防護和網路威脅防護封鎖的裝置的指令
- `-J`：用於管理系統效能指標取得的指令
- `-L`：用於管理產品授權金鑰的指令
- `-M`：用於管理 Kaspersky Endpoint Security 應用程式與 Kaspersky Unified Monitoring and Analysis Platform 整合設定的指令
- `-N`：用於管理加密連線掃描設定的指令
- `-Q`：用於管理隔離區的指令
- `-R`：用於管理 Kaspersky Endpoint Security 與 Kaspersky Endpoint Detection and Response (KATA)、Kaspersky Network Detection and Response (KATA)、Kaspersky Endpoint Detection and Response Expert (cloud) 和 Kaspersky Endpoint Detection and Response Optimum 整合設定的指令
- `-S`:統計指令。
- `-T`：用於管理應用程式工作和設定的指令
- `-U`：用於管理使用者和角色的指令
- `-V`：Light Agent 模式下的應用程式指令

- `-W`：用於顯示應用程式事件記錄中的事件的指令
- `-X`：用於管理 Kaspersky Endpoint Security 應用程式與 沙盒 整合設定的指令

在 bash shell 中，您可以為 kesl-control 指令啟用自動完成功能。

在目前的 bash 工作階段中，為 kesl-control 指令啟用自動完成功能

```
source /opt/kaspersky/kesl/shared/bash_completion.sh
```

為所有新的 bash 工作階段啟用自動完成功能

```
echo "source /opt/kaspersky/kesl/shared/bash_completion.sh" >> ~/.bashrc
```

用於管理產品授權金鑰的指令

`-L` 前綴表示該指令屬於用於管理產品授權金鑰的指令群組。

> 如果應用程式以標準模式或 EDR Agent 模式執行，則可以使用新增或移除產品授權金鑰的指令。如果在 Light Agent 模式下使用應用程式，金鑰管理指令會傳回錯誤。

kesl-control --add-active-key

此指令可讓您使用金鑰檔案或啟動碼，將作用中產品授權金鑰新增至應用程式。

您可以使用此指令新增用於啟動應用程式的金鑰，以及用於啟動產品授權未涵蓋之元件的金鑰。您不需要在指令中指定金鑰的類型。

使用金鑰檔案新增產品授權金鑰

```
kesl-control [-L] --add-active-key <key file path>
```

使用啟動碼新增產品授權金鑰

```
kesl-control [-L] --add-active-key <activation code>
```

其中：

`<key file path>` 是金鑰檔案的路徑。如果金鑰檔案位於目前目錄中，則僅指定檔案名稱就足夠了。

`<activation code>` 是啟動碼。

使用 /home/test/00000001.key 檔案作為啟動金鑰來新增金鑰的範例

```
kesl-control --add-active-key /home/test/00000001.key
```

kesl-control --add-reserve-key

此指令可讓您使用金鑰檔案或啟動碼，將備用產品授權金鑰新增至應用程式。

您可以使用此指令新增用於啟動應用程式的金鑰，以及用於啟動產品授權未涵蓋之元件的金鑰。您不需要在指令中指定金鑰的類型。

> 如果尚未將活動金鑰新增至裝置上的應用程式，則指令失敗。

使用金鑰檔案新增備用產品授權金鑰

```
kesl-control [-L] --add-reserve-key <key file path>
```

使用啟動碼新增備用產品授權金鑰

```
kesl-control [-L] --add-reserve-key <activation code>
```

其中：

`<key file path>` 是金鑰檔案的路徑。如果金鑰檔案位於目前目錄中，則僅指定檔案名稱就足夠了。

`<activation code>` 是啟動碼。

使用 `/home/test/00000002.key` 檔案新增備用金鑰的範例

```
kesl-control --add-reserve-key /home/test/00000002.key
```

kesl-control --remove-active-key

此指令可讓您刪除活動的產品授權金鑰。

```
刪除作用中 EDR Optimum 產品授權金鑰
kesl-control [-L] --remove-active-key [--edr-optimum]
```

```
刪除作用中 KUMA 產品授權金鑰
kesl-control [-L] --remove-active-key [--kuma]
```

```
刪除作用中 MDR 產品授權金鑰
kesl-control [-L] --remove-active-key [--mdr]
```

```
刪除作用中 EDR Expert (on-premises) 產品授權金鑰
kesl-control [-L] --remove-active-key [--edr-kata]
```

```
刪除作用中 EDR Expert (cloud) 產品授權金鑰
kesl-control [-L] --remove-active-key [--cxdr]
```

```
刪除作用中 KWSM 產品授權金鑰
kesl-control [-L] --remove-active-key [--khcs]
```

其中：

`--edr-optimum`— 刪除活動的 EDR Optimum 產品授權金鑰。

`--kuma` – 移除作用中 KUMA 產品授權金鑰。

`--mdr` – 移除作用中 MDR 產品授權金鑰。

`--edr-kata` – 移除作用中 EDR Expert (on-premises) 產品授權金鑰。

`--cxdr` – 移除作用中 EDR Expert (cloud) 產品授權金鑰。

`--khcs` – 移除作用中 KWSM 產品授權金鑰。

如果您未在命令列中指定 `--edr-optimum`、`--kuma`、`--mdr`、`--edr-kata`、`--cxdr` 或 `--khcs` 選項，此指令會刪除用來啟動應用程式的啟動金鑰。

kesl-control --remove-reserve-key

此指令可讓您刪除備用產品授權金鑰。

```
刪除備用 EDR Optimum 產品授權金鑰
kesl-control [-L] --remove-reserve-key [--edr-optimum]
```

```
刪除備用 KUMA 產品授權金鑰
kesl-control [-L] --remove-reserve-key [--kuma]
```

```
刪除備用 MDR 產品授權金鑰
kesl-control [-L] --remove-reserve-key [--mdr]
```

```
刪除備用 EDR Expert (on-premises) 產品授權金鑰
kesl-control [-L] --remove-reserve-key [--edr-kata]
```

```
刪除備用 EDR Expert (cloud) 產品授權金鑰
kesl-control [-L] --remove-reserve-key [--cxdr]
```

```
刪除備用 KWSM 產品授權金鑰
kesl-control [-L] --remove-reserve-key [--khcs]
```

其中：

`--edr-optimum`— 刪除備用 EDR Optimum 授權金鑰。

`--kuma` – 移除備用 KUMA 產品授權金鑰。

`--mdr` – 移除備用 MDR 產品授權金鑰。

`--edr-kata` – 移除備用 EDR Expert (on-premises) 產品授權金鑰。

`--cxdr` – 移除備用 EDR Expert (cloud) 產品授權金鑰。

`--khcs` – 移除備用 KWSM 產品授權金鑰。

如果您未在命令列中指定 `--edr-optimum`、`--kuma`、`--mdr`、`--edr-kata`、`--cxdr` 或 `--` 選項，此指令會從應用程式中移除備用金鑰。

kesl-control -L --query

此指令會輸出用於啟動應用程式的產品授權以及目前正在使用的產品授權金鑰的資訊。

```
kesl-control -L --query [--json]
```

其中：

`--json`：以 JSON 格式輸出資料。

kesl-control --load-mdr-blob

此指令可讓您將 BLOB 檔案上傳到裝置，該檔案可用於與 Kaspersky Managed Detection and Response 整合。您可以在 MDR 設定檔的 ZIP 壓縮檔案中找到 BLOB 檔案。

```
kesl-control [-L] --load-mdr-blob <path to MDR BLOB file>
```

kesl-control --remove-mdr-blob

此指令可讓您從裝置中移除用於與 Kaspersky Managed Detection and Response 整合的 BLOB 檔案。

```
kesl-control [-L] --remove-mdr-blob
```

用於管理使用者和角色的指令

-U 前綴表示該指令屬於管理使用者和角色的指令群組。

管理使用者角色

顯示使用者和角色清單

```
kesl-control [-U] --get-user-list
```

為指定使用者指派角色

```
kesl-control [-U] --grant-role <role> <user>
```

撤銷使用者角色

```
kesl-control [-U] --revoke-role <role> <user>
```

其中：

`<user>` 是使用者或使用者群組名稱。

`<role>` 是使用者或使用者群組的角色。

密碼防護設定

您可以使用命令來管理密碼防護。

啟用或停用密碼防護

```
kesl-control --set-permission-manager-settings Enabled=<Yes|No>
```

檢視目前的密碼防護設定

```
kesl-control --get-permission-manager-settings
```

編輯使用者或群組的權限

```
kesl-control --set-permissions <user> [--group] <permissions>=<Yes|No> [--file <file name>] [--json]
```

檢視使用者或群組的目前權限

```
kesl-control --get-permissions <user> [--group] [--file <file name>] [--json]
```

移除已設定權限的使用者或使用者群組

```
kesl-control --remove-permissions <user> [--group]
```

其中：

`<user>` 是使用者或使用者群組名稱。

`<permissions>` 用於自訂權限。

`--group` 會將設定套用至使用者群組。如果未指定此選項，則會將設定套用至個別使用者。

`--file <path to file>` 會將設定儲存或匯出至設定檔。如果未指定此選項，則會將命令結果寫入標準輸出。

`--json` 被指定以 JSON 格式輸出設定。

管理裝置上的政策

> 若要停用裝置上的政策，使用者需要停用卡巴斯基安全管理中心政策權限。

如果使用者已停用裝置上的政策，則在裝置或 Kaspersky Endpoint Security 重新啟動後，該政策會再次變為作用中。

停用裝置上的政策

```
kesl-control --disable-policy
```

將政策套用至裝置

```
kesl-control --enable-policy
```

管理應用程式工作和設定

`-T` 前置詞表示該指令屬於用於管理應用程式設定和工作的指令群組。

`-C` 前置詞表示該指令屬於用於管理容器掃描設定的指令群組。

`-N` 前綴表示該指令屬於用於管理網路流量掃描設定的指令群組。

kesl-control --export-settings

此指令可將所有應用程式設定輸出到主控台或匯出到設定檔。這些包括一般容器掃描設定、加密連線掃描設定、一般應用程式設定和工作設定。

```
kesl-control [-T] --export-settings [--file <path to file>] [--json]
```

其中：

`--file <path to file>` 是您要用來儲存應用程式設定之設定檔的完整路徑。

`--json` 被指定以 JSON 格式輸出設定。

kesl-control --import-settings

> 僅允許受信任的使用者存取設定檔。在將設定匯入應用程式之前，請先驗證目錄、設定檔、執行檔和隔離區的路徑。請勿從不受信任的來源匯入設定檔。設定檔遭到破壞可能會影響組織基礎架構及使用者資料的安全性、完整性或功能。

此指令從設定檔匯入所有應用程式設定，包括一般容器掃描設定、加密連線掃描設定、一般應用程式設定和工作設定。

```
kesl-control [-T] --import-settings --file <path to configuration file> [--json]
```

其中：

`--file <path to file>` 是您要從中匯入應用程式設定之設定檔的完整路徑。

指定 `--json` 可從 JSON 格式的設定檔匯入設定。如果未指定 `--json` 選項，應用程式將嘗試從 INI 檔案匯入。如果匯入失敗，則會顯示錯誤。

kesl-control --update-application

此指令可安裝下載的應用程式模組更新。

> 如果應用程式正在以 Light Agent 模式使用，則此指令無法執行。

```
kesl-control [-T] --update-application
```

用於管理一般應用程式設定的指令

kesl-control --get-app-settings

此指令可將一般應用程式設定的目前值輸出到主控台或設定檔。

```
kesl-control [-T] --get-app-settings [--file <path to file>] [--json]
```

其中：

`--file <path to file>` 是要將應用程式的一般設定輸出至其中的設定檔路徑。如果不指定 `--file` 選項，設定將被輸出到主控台。

如果指定檔案的名稱而不指定其路徑，則檔案會在目前目錄中建立。如果指定路徑中已經存在檔案，則該檔案會被覆寫。如果指定的目錄不存在，則不會產生設定檔。

`--json`被指定以 JSON 格式輸出設定。

kesl-control --set-app-settings

此指令透過指令選項或從設定檔匯入設定來配置一般應用程式設定。

使用指令列選項指定設定：

```
kesl-control [-T] --set-app-settings <setting name>=<setting value> [<setting name>=<setting value>]
```

使用設定檔指定設定：

```
kesl-control [-T] --set-app-settings --file <path to file> [--json]
```

其中：

`<setting name>=<setting value>` 是一般應用程式設定的名稱和值。

`--file <path to file>` 是您要從中匯入應用程式設定之設定檔的完整路徑。

`--json` 用於以 JSON 格式將設定從設定檔匯入應用程式。如果未指定`--json`選項，應用程式將嘗試從 INI 檔案匯入。如果匯入失敗，則會顯示錯誤。

用於管理工作設定的指令

kesl-control --get-settings

此指令可將指定工作的目前設定輸出到主控台或設定檔。

```
kesl-control [-T] --get-settings <task ID|name> [--file <path to file>] [--json]
```

其中：

`<task ID|name>` 是任務建立時指派的 ID，或是命令列中的任務名稱。

`--file <path to file>` 是您要將工作設定輸出至其中的設定檔路徑。如果不指定`--file`選項，設定將被輸出到主控台。

如果指定檔案的名稱而不指定其路徑，則檔案會在目前目錄中建立。如果指定路徑中已經存在檔案，則該檔案會被覆寫。如果指定的目錄不存在，則不會產生設定檔。

`--json`被指定以 JSON 格式輸出設定。

kesl-control --set-settings

此指令可透過指令選項或從設定檔匯入設定來定義指定工作的設定。

使用指令列選項指定設定：

```
kesl-control [-T] --set-settings <task ID|name> <setting name>=<setting value> [<setting name>=<setting value>] [--add-path <path>] [--del-path <path>] [--add-exclusion <path>] [--del-exclusion <path>]
```

使用設定檔指定設定：

```
kesl-control [-T] --set-settings <task ID/name> --file <path to file> [--json]
```

其中：

`<task ID|name>` 是任務建立時指派的 ID，或是命令列中的任務名稱。

`<setting name>=<setting value>` 是一項工作設定的名稱和值。

`--add-path <path>` 會新增包含要掃描物件的目錄路徑。

`--del-path <path>` 會移除包含要掃描物件的目錄路徑。

`--add-exclusion <path>` 會新增包含要從掃描中排除之物件的目錄路徑。

`--del-exclusion <path>` 會移除包含要排除於掃描之外之物件的目錄路徑。

`--file <path to file>` 是您要從中匯入任務設定之設定檔的完整路徑。

指定 `--json` 可從 JSON 格式的設定檔匯入設定。如果未指定`--json`選項，應用程式將嘗試從 INI 檔案匯入。如果匯入失敗，則會顯示錯誤。

kesl-control --set-to-default

此指令可還原指定工作的預設設定。

```
kesl-control [-T] --set-settings <task ID|name> --set-to-default
```

其中：

`<task ID|name>` 是任務建立時指派的 ID，或是命令列中的任務名稱。

kesl-control --get-schedule

此指令可將指定工作的目前排程輸出到主控台或設定檔。

```
kesl-control [-T] --get-schedule <task ID|name> [--file <path to file>] [--json]
```

其中：

`<task ID|name>` 是任務建立時指派的 ID，或是命令列中的任務名稱。

`--file <path to file>` 是您要將工作排程設定輸出至其中的設定檔路徑。如果不指定`--file`選項，設定將被輸出到主控台。

如果指定檔案的名稱而不指定其路徑，則檔案會在目前目錄中建立。如果指定路徑中已經存在檔案，則該檔案會被覆寫。如果指定的目錄不存在，則不會產生設定檔。

`--json`被指定以 JSON 格式輸出設定。

kesl-control --set-schedule

該指令可透過指令選項或從設定檔匯入設定來定義指定工作的排程。

使用指令列選項指定設定：

```
kesl-control [-T] --set-schedule <task ID|name> <setting name>=<setting value> [<setting name>=<setting value>]
```

使用設定檔指定設定：

```
kesl-control [-T] --set-schedule <task ID|name> --file <path to file> [--json]
```

其中：

`<task ID|name>` 是任務建立時指派的 ID，或是命令列中的任務名稱。

`<setting name>=<setting value>` 是一項工作排程設定的名稱和值。

`--file <path to file>` 是您要從中匯入工作排程設定的設定檔完整路徑。

指定 `--json` 可從 JSON 格式的設定檔匯入設定。如果未指定`--json`選項，應用程式將嘗試從 INI 檔案匯入。如果匯入失敗，則會顯示錯誤。

用於管理工作的命令

kesl-control --get-task-list

此命令會輸出現有工作的清單。

```
kesl-control [-T] --get-task-list [--json]
```

其中：

`--json` 被指定以 JSON 格式輸出設定。

將為每個工作顯示以下資訊：

- `Name`：工作名稱
- `ID`：工作 ID
- `Type`：工作類型
- `State`：工作的目前狀態

> 如果卡巴斯基安全管理中心政策禁止使用者檢視和編輯本機工作，則無法取得 `Scan_My_Computer`、`Critical_Areas_Scan`、`Container_Scan`、`Inventory_Scan`、`Update` 和 `Rollback` 工作的相關資訊。

kesl-control --get-task-state

此命令會輸出指定工作的狀態。

```
kesl-control [-T] --get-task-state <task ID|name> [--json]
```

其中：

`<task ID|name>` 是任務建立時指派的 ID，或是命令列中的任務名稱。

`--json` 被指定以 JSON 格式輸出設定。

應用程式工作可處於以下狀態：

- `Started` – 工作正在執行。
- `Starting` – 工作正在啟動。

- `Stopped` – 工作已停止。
- `Stopping` – 工作正在停止。

`ODS`、`ODFIM` 和 `InventoryScan` 類型的工作也可能處於以下狀態之一：

- `Pausing` – 工作正在暫停。
- `Suspended` – 工作已暫停。
- `Resuming` – 工作正在恢復。

kesl-control --create-task

此命令會使用預設設定或設定檔中指定的設定，建立指定類型的工作。

只能建立使用者工作。預定義工作無法建立。

視應用程式的模式而定，您可以建立下列類型的使用者工作：

- 標準模式：`ODS`、`Update`、`Rollback`、`ODFIM`、`ContainerScan` 和 `InventoryScan`。
- Light Agent 模式：`ODS`、`ODFIM`、`ContainerScan` 和 `InventoryScan`。

使用預設設定建立工作

```
kesl-control [-T] --create-task <task name> --type <task type>
```

使用設定檔中的設定建立工作

```
kesl-control [-T] --create-task <task name> --type <task type> [--file <path to file>] [--json]
```

其中：

`<task name>` 是您為新工作指定的名稱。

`<task type>` 會指定您要建立的工作類型。

`--file <path to file>` 是包含用於建立工作之設定的設定檔完整路徑。

指定 `--json` 可從 JSON 格式的設定檔匯入設定。如果未指定`--json`選項，應用程式將嘗試從 INI 檔案匯入。如果匯入失敗，則會顯示錯誤。

kesl-control --delete-task

此命令會刪除工作。

只能刪除使用者工作。預定義工作不能被刪除。

```
kesl-control [-T] --delete-task <task ID|name>
```

其中：

`<task ID|name>` 是任務建立時指派的 ID，或是命令列中的任務名稱。

kesl-control --start-task

此命令會啟動工作。

您可以啟動和停止所有預定義工作和使用者工作，但 `License` 類型的工作除外。

```
kesl-control [-T] --start-task <task ID|name> [-W] [--progress]
```

其中：

`<task ID|name>` 是任務建立時指派的 ID，或是命令列中的任務名稱。

`-W`：啟用目前事件輸出。

`--progress`：顯示工作進度。

執行 ID 為 1 的工作，並啟用與該工作相關的目前事件顯示的範例

```
kesl-control --start-task 1 -W
```

如果啟動工作時發生錯誤，導致工作無法啟動，則在重新啟動應用程式後，嘗試再次啟動工作。

kesl-control --stop-task

此命令會停止工作。

您可以啟動和停止所有預定義工作和使用者工作，但 `License` 類型的工作除外。

```
kesl-control [-T] --stop-task <task ID|name> [-W]
```

其中：

`<task ID|name>` 是任務建立時指派的 ID，或是命令列中的任務名稱。

`-W`：啟用目前事件輸出。

kesl-control --suspend-task

此命令會暫停工作。

您只能暫停 ODS、ODFIM 和 InventoryScan 工作。

```
kesl-control [-T] --suspend-task <task ID|name>
```

其中：

`<task ID|name>` 是任務建立時指派的 ID，或是命令列中的任務名稱。

kesl-control --resume-task

此命令會恢復工作。

您只能恢復 ODS、ODFIM 和 InventoryScan 工作。

```
kesl-control [-T] --resume-task <task ID|name>
```

其中：

`<task ID|name>` 是任務建立時指派的 ID，或是命令列中的任務名稱。

kesl-control --scan-file

此命令會建立並執行自訂掃描工作。

```
kesl-control [-T] --scan-file <path> [--action <action>]
```

其中：

`<path>` 是您要掃描的檔案或目錄路徑。您可以指定多個路徑，以空格分隔。

`--action <action>` 是您希望應用程式對受感染物件執行的動作。如果您未指定 `--action` 選項，應用程式會執行建議的動作。

kesl-control --scan-container

此命令會建立並執行容器或映像的自訂掃描工作。

```
kesl-control [-T] --scan-container <ID|name[:tag]>
```

其中：

`<ID|name[:tag]>` 是容器或映像的名稱或 ID。您可以使用遮罩來掃描多個物件。

實用文章

如何指定遮罩

您可以使用`*`（星號）字元來建立檔案或目錄名稱遮罩。

您可以指示單一`*`字元來表示檔案或目錄名稱中`/`字元前面的任意字元集（包括空集）。例如，`/dir/*/file` 或 `/dir/*/*/file`。

您可以用兩個連續的`*`字元來表示檔案或目錄名稱中的任意一組字元（包括空集和`/`字元）。例如，`/dir/**/file*/` 或 `/dir/file**/`。

`**`遮罩在目錄名稱中只能使用一次。例如，`/dir/**/**/file`是一個不正確的遮罩。

您可以使用單一`?`字元來表示檔案或目錄名稱中的任意一個字元。

用於管理一般容器掃描設定的指令

kesl-control --get-container-settings

此指令可將目前的一般容器掃描設定輸出到主控台或設定檔。

```
kesl-control [-C] --get-container-settings [--file <path to file>] [--json]
```

其中：

`--file <path to file>` 是您要將容器掃描一般設定輸出至其中的設定檔路徑。如果不指定`--file`選項，設定將被輸出到主控台。

如果指定檔案的名稱而不指定其路徑，則檔案會在目前目錄中建立。如果指定路徑中已經存在檔案，則該檔案會被覆寫。如果指定的目錄不存在，則不會產生設定檔。

`--json`被指定以 JSON 格式輸出設定。

kesl-control --set-container-settings

此指令可使用指令選項或透過從設定檔匯入設定來配置一般容器掃描設定。

使用指令列選項指定設定：

```
kesl-control [-C] --set-container-settings <setting name>=<setting value> [<setting name>=<setting value>]
```

使用設定檔指定設定：

```
kesl-control [-C] --set-container-settings --file <path to file> [--json]
```

其中：

`<setting name>=<setting value>` 是 容器掃描一般設定的名稱和值。

`--file <path to file>` 是您要從中匯入容器掃描一般設定的設定檔完整路徑。

`--json` 用於以 JSON 格式將設定從設定檔匯入應用程式。如果未指定`--json`選項，應用程式將嘗試從 INI 檔案匯入。如果匯入失敗，則會顯示錯誤。

用於管理網路流量掃描設定的指令

`-N` 前綴表示該指令屬於用於管理網路流量掃描設定的指令群組。

kesl-control -N --query

此指令可輸出加密連線掃描的排除項目清單：

- 使用者新增的排除項目清單；
- 應用程式新增的排除項目清單；
- 從應用程式資料庫收到的排除項目清單。

顯示使用者新增的排除項目清單

```
kesl-control -N --query user
```

顯示應用程式新增的排除項目清單

```
kesl-control -N --query auto
```

顯示從應用程式資料庫收到的排除項目清單

```
kesl-control -N --query kl
```

kesl-control --clear-web-auto-excluded

此指令可清除應用程式自動排除在掃描範圍之外的網域清單。

```
kesl-control -N --clear-web-auto-excluded
```

kesl-control --get-net-settings

此指令可將目前網路流量掃描設定輸出到主控台或設定檔。

```
kesl-control [-N] --get-net-settings [--file <path to file>] [--json]
```

其中：

`--file <path to file>` 是您要將網路流量掃描設定輸出到其中的設定檔路徑。如果不指定`--file`選項，設定將被輸出到主控台。

如果指定檔案的名稱而不指定其路徑，則檔案會在目前目錄中建立。如果指定路徑中已經存在檔案，則該檔案會被覆寫。如果指定的目錄不存在，則不會產生設定檔。

`--json`被指定以 JSON 格式輸出設定。

kesl-control --set-net-settings

此指令可使用指令選項或透過從設定檔匯入設定來配置網路流量掃描設定。

使用指令列選項指定設定：

```
kesl-control [-N] --set-net-settings <setting name>=<setting value> [<setting name>=<setting value>]
```

使用設定檔指定設定：

```
kesl-control [-N] --set-net-settings --file <path to file> [--json]
```

其中：

`<setting name>=<setting value>` 是網路流量掃描設定的名稱和值。

`--file <path to file>` 是您要從中匯入網路流量掃描設定的設定檔完整路徑。

`--json` 用於以 JSON 格式將設定從設定檔匯入應用程式。如果未指定`--json`選項，應用程式將嘗試從 INI 檔案匯入。如果匯入失敗，則會顯示錯誤。

kesl-control --list-certificates

此命令可輸出受信任根憑證的清單。

```
kesl-control [-N] --list-certificates
```

kesl-control --add-certificate

此命令可將憑證新增至受信任根憑證清單。

```
kesl-control [-N] --add-certificate <path to certificate>
```

其中：

`<path to certificate>` 是您要新增之憑證檔案的路徑（PEM 或 DER 格式）。

kesl-control --remove-certificate

此命令可從受信任根憑證清單中刪除憑證。

```
kesl-control [-N] --remove-certificate <certificate subject>
```

kesl-control --add-bypass-endpoints

您可以使用此指令新增流量攔截排除。

```
kesl-control [-N] --add-bypass-endpoints --direction <in|out> --remote-ip <remote IP address> --dst-port
<destination port>
```

其中：

`<in|out>` 是排除連線中的流量方向：傳出或傳入。

`<remote IP address>` 是遠端裝置的 IPv4 或 IPv6 位址。如果將輸入流量排除於攔截範圍外，則會排除來自指定 IP 位址的流量。如果將輸出流量排除於攔截範圍外，則會排除傳送至指定 IP 位址的流量。

`<destination port>` 是受保護裝置上的連接埠（傳入流量的排除）或遠端裝置上的連接埠（傳出流量的排除）。傳送至該連接埠的流量將被排除於攔截範圍外。

kesl-control --list-bypass-endpoints

您可以使用此指令檢視已設定的流量攔截排除項目清單。

```
kesl-control [-N] --list-bypass-endpoints
```

kesl-control --remove-bypass-endpoints

您可以使用此指令拆除流量攔截排除項目。

```
kesl-control [-N] --remove-bypass-endpoints --direction <in|out> --remote-ip <remote IP address> --dst-port
<destination port>
```

其中：

`<in|out>` 是排除連線中的流量方向：傳出或傳入。

`<remote IP address>` 是遠端裝置的 IPv4 或 IPv6 位址，其流量會排除在攔截之外（視流量方向而定）。

`<destination port>` 是受保護裝置上的連接埠（傳入流量的排除）或遠端裝置上的連接埠（傳出流量的排除）。

狀態和防護監控

統計指令

-S 前置詞表示該命令屬於 statistics 命令群組。

kesl-control --app-info

此指令可輸出關於應用程式的資訊。

```
kesl-control [-S] --app-info [--json] [--check-permissions]
```

其中：

`--json` 被指定以 JSON 格式輸出設定。

`--check-permissions` 顯示權限設定不正確的應用程式目錄路徑。

kesl-control --supported-tech-info

此指令會顯示應用程式功能清單、其狀態資訊（已使用或未使用），以及用來實作這些應用程式功能的 Linux 技術。

```
kesl-control [-S] --supported-tech-info [--json]
```

其中：

`--json`：以 JSON 格式輸出功能。

kesl-control --get-statistic

此指令可讓您顯示關於應用程式操作的統計資訊和在裝置上找到的掛載點清單。

```
kesl-control [-S] --get-statistic [--files] [--processes] [--mountpoints]
```

其中：

`--files`：檔案威脅防護元件掃描最頻繁的檔案的統計，以及元件存取這些檔案的次數。

`--processes`: Kaspersky Endpoint Security 最常啟動的處理程序的統計資料，以及此類啟動的數量。

> 將處理程序從行為偵測元件的掃描中排除不會從統計資料中刪除這些處理程序，但可以提高 Kaspersky Endpoint Security 應用程式的效能。

`--mountpoints`：掛載點清單。在輸出中，掛載點路徑按以下方式排序：

- 靜態、系統、服務和其他掛載點
- 在其命名空間中安裝的 snap 套件和安裝點
- Docker 容器管理系統所建立的掛載點

您可以以任意組合指定一個或多個選項，或者不指定任何選項。如果您未指定任何選項，應用程式將顯示三個清單：最常掃描的檔案的統計資訊、最常啟動的處理程序的統計資訊以及在裝置上找到的掛載點清單。

kesl-control --omsinfo

此指令會建立 JSON 檔案以便與 Microsoft Operations Management Suite 整合。

```
kesl-control [-S] --omsinfo --file <path to file>
```

用於顯示事件的指令

`-W` 前置詞表示用於顯示應用程式事件記錄中的事件的指令。

kesl-control -W

此命令可以顯示目前應用程式事件。該命令可傳回事件的名稱以及關於該事件的附加資訊。您可以使用該指令顯示所有目前應用程式事件或僅顯示與目前正在執行的工作相關的事件。

```
kesl-control -W [--query "<filter conditions>"]
```

其中：

`<filter conditions>` 指定一個或多個 邏輯運算式，其格式為 `<field> <comparison operation> '<value>'`，並使用邏輯運算子 `and` 組合，以輸出特定目前事件。

用於管理應用程式事件的指令

-E 前置詞表示該指令屬於用於管理應用程式事件的指令群組。

kesl-control -E

此指令可輸出關於應用程式事件記錄中所有事件的資訊。您可以使用`less`指令導覽顯示的事件清單。

```
kesl-control -E
```

kesl-control -E --query

此指令可輸出關於應用程式事件記錄中的事件的資訊。您可以使用`less`指令導覽顯示的事件清單。您可以使用篩選器輸出特定事件或將事件清單輸出到檔案。

```
kesl-control -E --query "<filter conditions>" [--db <database file>] [-n <number>] [--file <path to file>] [--
json] [--reverse]
```

其中：

`<database file>` 是要從中輸出事件的事件記錄資料庫檔案完整路徑。預設情況下，應用程式將關於事件的資訊儲存到資料庫 var/opt/kaspersky/kesl/private/storage/events.db。資料庫的位置由 `EventsStoragePath` 一般應用程式設定決定。

`<filter conditions>` 會指定一個或多個採用 `<field> <comparison operator> '<value>'` 格式並使用邏輯運算子 `and` 結合的 邏輯運算式，以限制查詢結果。

`<number>` 是您要輸出的選取範圍中最新事件的數量（也就是從選取範圍末尾開始計算的記錄數）。

`--file <path to file>` 是要將事件輸出至其中的檔案完整路徑。如果指定檔案的名稱而不指定其路徑，則該檔案會在目前目錄中建立。如果指定路徑中已經存在指定名稱的檔案，則該檔案將被覆寫。如果在磁碟上找不到指定的目錄，則不會建立檔案。

如果不指定`--file`選項，事件清單將被輸出到主控台。

`--json`：以 JSON 格式輸出事件。

`--reverse`：以相反順序顯示事件（從最新事件在頂部到最舊事件在底部）。

用於管理系統效能指標的指令

kesl-control --export-metrics

此指令允許設定作業系統效能指標的獲取。

```
kesl-control [-J] --export-metrics [--period <interval in seconds between exports>|--interactive]
```

其中：

`--period`可啟用定期輸出結果。

`<interval in seconds between exports>` 指定命令結果輸出至命令列主控台的頻率（以秒為單位）

`--interactive`啟用互動式輸出（按下**Enter**鍵時）。

安全控制

用於管理裝置控制的指令

-D 前置詞表示該指令屬於用於管理 裝置控制 的指令群組。

管理裝置控制設定

檢視目前的裝置控制設定

```
kesl-control --get-settings 15 [--file <path to file>] [--json]
```

修改應用程式控制設定

```
kesl-control --set-settings 15 [<setting>=<value>] [--file <path to file>] [--json]
```

其中：

`<setting>=<value>` 指定裝置控制的設定及其值。

--file <path to file> 會將設定儲存或匯出到設定檔中。如果未指定此選項，則會將命令結果寫入標準輸出。

`--json`：以 JSON 格式輸出資料。

管理裝置

檢視已連線裝置清單

```
kesl-control [-D] --get-device-list [--all] [--json] [--export <file>]
```

其中：

`--all` 會列出所有已連線裝置。

`--json` 會以 JSON 格式列出已連線裝置。

`--export <file>` 會將已連線裝置清單匯出至 JSON 檔案。已連線裝置清單已匯出。

Kaspersky Endpoint Security 會顯示下列已連線裝置相關資訊：

- **裝置類型**。已連線裝置的類型。例如，`OpticalDrive` 或 `HardDrive`。
- **識別碼**。已連線裝置的 ID。
- **名稱**。已連線裝置的名稱。
- **路徑**。sysfs 虛擬作業系統中裝置的路徑。
- **系統磁碟機**。此設定表示已連線裝置是否為系統磁碟機（是或否）。
- **匯流排**。連線匯流排。可能的值：`UnknownBus`、`USB`、`FireWire`。
- **驅動程式**。sysfs 虛擬作業系統讀取的驅動程式名稱。

受信任裝置

此指令可讓您檢視受信任裝置清單、從清單中新增和刪除裝置，以及從檔案匯入受信任裝置清單。

```
kesl-control [-D] --trusted-devices [--list] [--add <ID>] [--delete <ID>] [--merge|--add|--replace --file <file>]
```

其中：

`--list` – 顯示受信任裝置清單。

`--add <ID>` 會依裝置 ID 或裝置 ID 遮罩將裝置新增至受信任裝置清單。

`--delete <ID>` 會依裝置 ID 或裝置 ID 遮罩將裝置從受信任裝置清單中移除。

`--merge` 可合併受信任裝置清單。如果目前清單和匯入的清單中包含具有相同 ID 的裝置條目，則更新現有條目。對於目前清單中不存在的裝置，將會新增條目。

`--add` 在匯入時新增目前受信任裝置清單。僅將先前不在裝置清單中的裝置項目新增至清單中。

`--replace` 取代目前受信任裝置清單。現有受信任裝置清單將匯入的清單取代。

`--file <file>` 會從指定的檔案匯入受信任裝置清單。您需要指定 JSON 檔案的完整路徑。

暫時存取被封鎖的裝置

這些指令可讓您建立存取請求檔案並上傳存取金鑰，以取得遭封鎖裝置的暫時存取權：

建立存取請求檔案

```
kesl-control [-D] --request-temporary-device-access --device-id <device ID> --access-duration <access duration> --
path <path to access request file>
```

上傳存取金鑰

```
kesl-control [-D] --upload-temporary-device-access-key --path <access key>
```

其中：

`--device-id <device ID>` 是您要取得存取權之被封鎖裝置的 ID。

`--access-duration <access duration>` 是您要取得裝置存取權的時間長度（以小時為單位）。可選值：1 到 100

`--path <path to access request file>` 是您要儲存副檔名為 .akey 的存取請求檔案所在目錄的路徑。

`--path <access key>` 是包含裝置存取金鑰之檔案（副檔名為 .acode 的檔案）的路徑。

用於管理應用程式控制的指令

-A 前置詞表示該指令屬於用於管理應用程式控制的指令群組。

管理清查工作

檢視用戶端裝置上偵測到的應用程式清單

```
kesl-control [-A] --get-app-list [--json]
```

其中：

`--json`：以 JSON 格式輸出資料。

檢視應用程式類別

檢視已建立的應用程式控制類別清單

```
kesl-control [-A] --get-categories [--names <name of category 1> <name of category 2> ... <name of category N>] [--file <path to file>] [--json]
```

其中：

`<category name 1> <category name 2> ... <category name N>` 是類別名稱。如果要檢視關於多個類別的資訊，請指定類別的名稱，並以空格分隔。

`--file <path to file>` 會將設定儲存或匯出至設定檔。如果未指定此選項，則會將命令結果寫入標準輸出。

`--json`：以 JSON 格式輸出資料。

管理應用程式類別

若要建立應用程式類別：

1. 將應用程式類別清單寫入設定檔：

   ```
   kesl-control --set-categories --file <path to file>
   ```

2. 依下列方式新增應用程式類別：

```
[
   {
      "Exclude" : [ "(FilePath like <application>)", "(FileHash == <hash>)" ],
      "GUID" : "<category ID>",
      "Include" : [ "(FilePath like <application>)", "(FileHash == <hash>)" ],
      "Name" : "<category name 1>"
   },
 {
      "Exclude" : [ "(FilePath like <application>)", "(FileHash == <hash>)" ],
      "GUID" : "<category ID>",
      "Include" : [ "(FilePath like <application>)", "(FileHash == <hash>)" ],
      "Name" : "<category name 2>"
   }
]
```

若要在 `Exclude` 和 `Include` 欄位中指定檔案路徑，可以使用遮罩。

3. 將類別清單匯入應用程式：

```
kesl-control [-A] --set-categories [--names <category name 1> <category name 2> ... <name of category N>] --
file <path to file>
```

編輯應用程式控制類別清單

```
kesl-control [-A] --set-categories [--names <category name 1> <category name 2> ... <name of category N>] --file
<path to file>
```

其中：

`FilePath like <application>` 是應用程式可執行檔的完整路徑。

`FileHash == <hash>` 是應用程式可執行檔的 SHA256 雜湊值。

`<category ID>` 是唯一的類別 ID。必須設定。輸入不含連字號的 `GUID`。

`<category name 1> <category name 2> ... <category name N>` 是類別名稱。必須設定。

如果要變更多個類別的資訊，請指定類別的名稱，並以空格分隔。如果您未指定類別名稱，則不會建立該類別，或會將該類別從現有類別清單中刪除。

`--file <path to file>` 會將設定儲存或匯出到 JSON 設定檔中。

管理應用程式控制設定

檢視目前的應用程式控制設定

```
kesl-control --get-settings 21 [--file <path to file>] [--json]
```

修改應用程式控制設定

```
kesl-control --set-settings 21 [<setting>=<value>] [--file <path to file>] [--json]
```

其中：

`<setting>=<value>` 會指定應用程式控制設定及其值。

`--file <path to file>` 會將設定儲存或匯出至設定檔。如果未指定此選項，則會將命令結果寫入標準輸出。

`--json`：以 JSON 格式輸出資料。

將設定重設為預設值

```
刪除應用程式類別與應用程式控制規則清單，並還原預設設定
kesl-control --set-settings 21 --set-to-default
```

實用文章

如何指定遮罩

您可以使用 * 字元（任意字元序列）或 ? 字元（任意一個字元）作為檔案或目錄名稱遮罩。

您可以使用 * 字元來表示檔案或目錄名稱中包含 / 字元的任意字元集（包括空集）。例如，`/dir/*/file*/` 或 `/dir/file*/`。

您可以用單個 ? 字元來表示檔案或目錄名稱中的任意一個字元（包括 / ）。

Web 控制管理指令

管理 Web 控制設定

```
檢視目前的 Web 控制設定
kesl-control --get-settings 26 [--file <path to file>] [--json]
```

```
修改 Web 控制設定
kesl-control --set-settings 26 [<setting>=<value>] [--file <path to file>] [--json]
```

其中：

`<setting>=<value>` 是 Web 控制的設定及其值。您可以修改任意數量的設定。

`--file <path to file>` 會將設定儲存或匯出至設定檔。如果未指定此選項，則會將命令結果寫入標準輸出。

`--json`：以 JSON 格式輸出資料。

將設定重設為預設值

```
刪除已配置的設定並還原預設的 Web 控制設定
kesl-control --set-settings 26 --set-to-default
```

網路連線防護

用於管理被封鎖裝置的指令

-H 前綴表示該命令屬於用於管理遭 加密軟體防護 和 網路威脅防護 封鎖之裝置的命令群組。

kesl-control --get-blocked-hosts

該指令允許您將被封鎖的裝置清單輸出到主控台。

```
kesl-control [-H] --get-blocked-hosts
```

kesl-control --allow-hosts

該指令允許您解除對被封鎖裝置的阻止。

```
kesl-control [-H] --allow-hosts <address>
```

其中：

`<address>` 是裝置或子網路的 IP 位址（IPv4/IPv6，包括短形式的位址）。您可以指定多個裝置或子網路的 IP 位址，以空格分隔。

防火牆管理指令

-F 前綴表示該指令屬於防火牆管理指令。

kesl-control --add-rule

此指令可新增一個新的網路封包規則。

```
kesl-control [-F] --add-rule [--name <rule name>] [--action <Allow|Block>] [--protocol <protocol>] [--direction
<direction>] [--remote <remote address>:<port>] [--local <local address>:<port>] [--at <index>]
```

其中：

`--name <rule name>` 是網路封包規則的名稱。

`--action <Allow|Block>` 是將對此網路封包規則中指定的連線執行的操作。

`--protocol <protocol>` 是您要監控其網路活動的協定。

`--direction <direction>` 是受監控網路活動的方向。

`--remote <remote address>:<port>` 是遠端裝置的網路位址。

`--local <local address>:<port>` 是已安裝 Kaspersky Endpoint Security 之裝置的網路位址。

`--at <index>` 是網路封包規則清單中該規則的編號。如果未指定 `--at` 選項或其值大於清單中的規則數，則新規則將會新增至清單的末端。

指令中未指定值的參數將被設定為其預設值。

kesl-control --del-rule

此指令可刪除規則清單中具有指定名稱或索引的網路封包規則。

依規則名稱刪除網路封包規則

```
kesl-control [-F] --del-rule --name <rule name>
```

依規則編號刪除網路封包規則

```
kesl-control [-F] --del-rule --index <index>
```

其中：

`--name <rule name>` 是網路封包規則的名稱。

`--index <index>` 是網路封包規則清單中該規則的編號。

kesl-control --move-rule

此指令會改變網路封包規則的執行優先順序。

依規則名稱變更網路封包規則的優先順序

```
kesl-control [-F] --move-rule --name <rule name> --at <index>
```

依規則編號變更網路封包規則的優先順序

```
kesl-control [-F] --move-rule --index <index> --at <index>
```

其中：

`--name <rule name>` 是網路封包規則的名稱。

`--index <index>` 是網路封包規則清單中該規則的目前編號。

`--at <index>` 是網路封包規則清單中該規則的新編號。

kesl-control --add-zone

此指令可將位址新增至網路區域。

```
kesl-control [-F] --add-zone --zone <zone> --address <address>
```

其中：

`--zone <zone>` 是網路區域的預定義名稱。

`--address <address>` 是網路位址或子網路。

kesl-control --del-zone

此指令可從網路區域中刪除一個位址。

依位址或子網路從網路區域移除位址

```
kesl-control [-F] --del-zone --zone <zone> --address <address>
```

依規則編號從網路區域移除位址

```
kesl-control [-F] --del-zone --zone <zone> --index <address index>
```

其中：

`--zone <zone>` 是網路區域的預定義名稱。

`--address <address>` 是網路位址或子網路。

`--index <address index>` 是網路區域中位址的編號。

kesl-control -F --query

此指令可顯示使用 Kaspersky Endpoint Security 建立的防火牆規則。

```
kesl-control -F --query
```

進階威脅和目標式攻擊防護

用於管理隔離區的指令

-Q 前綴表示該指令屬於用於管理 隔離區 的指令群組。

kesl-control -Q --mass-remove

該指令將從隔離區中刪除部分或全部檔案。

刪除所有檔案

```
kesl-control -Q --mass-remove
```

刪除符合篩選條件的檔案

```
kesl-control -Q --mass-remove --query "<filter conditions>"
```

其中：

`<filter conditions>` 會指定一個或多個採用 `<field> <comparison operator> '<value>'` 格式並使用邏輯運算子 `and` 結合的 邏輯運算式，以限制查詢結果。

kesl-control --put

> 此指令僅當 Kaspersky Endpoint Security 與 Kaspersky Endpoint Detection and Response Optimum 或 Kaspersky Managed Detection and Response 整合時可用。

該指令允許隔離檔案。

```
kesl-control [-Q] --put <file path> [--md5] [--sha256] [--save-original-file]
```

其中：

`<file path>` 是您要隔離的檔案路徑。

`--md5` 是您要隔離的檔案的 MD5 雜湊值。

`--sha256` 是您要隔離的檔案的 SHA256 雜湊值。

`--save-original-file` 保留原始檔案。如果不指定此選項，則原始檔案將被刪除。

kesl-control -Q --query

此指令可輸出關於被隔離的檔案的資訊。

輸出所有已隔離檔案的資訊

```
kesl-control -Q --query [-n <number>] [--json]
```

顯示符合篩選條件的已隔離檔案資訊

```
kesl-control -Q --query ["<filter conditions>"] [-n <number>]
```

其中：

`<filter conditions>` 會指定一個或多個採用 `<field> <comparison operator> '<value>'` 格式並使用邏輯運算子 `and` 結合的 邏輯運算式，以限制查詢結果。如果您不指定任何篩選條件，應用程式將顯示所有被被隔離檔案的詳細資訊。

`<number>` 是您要顯示之最近隔離檔案的數量。如果不指定 `-n` 選項，則顯示最後 30 個檔案。若要顯示所有檔案，請指定 0。

`--json`：以 JSON 格式輸出資料。

kesl-control -Q --restore

該指令可讓您從隔離區還原檔案。

```
kesl-control -Q --restore <file ID> [--file <file path>]
```

其中：

`<file ID>` 是已隔離檔案的 ID。

`--file <file path>` 是檔案的新名稱，以及用於儲存該檔案的目錄路徑。如果不指定`--file`選項，則檔案將以其原始名稱和原始位置還原。如果目錄被刪除或使用者沒有存取權限，應用程式會將檔案放在 /var/opt/kaspersky/kesl/common/restored/ 目錄中。您可以手動將檔案從該目錄移至您選擇的目錄。

用於管理 EDR Expert (on-premises) 元件的指令

-R 前綴表示該指令屬於用於管理與卡巴斯基 Detection and Response 解決方案之整合設定的指令群組。

kesl-control --add-kataedr-server-certificate

此命令可讓您新增或取代先前新增的KATA 伺服器、OSMP 威脅回應伺服器或 OSMP 遙測伺服器的憑證（取決於整合模式）。

```
kesl-control [-R] --add-kataedr-server-certificate <file> [--server-type <response|telemetry>]
```

其中：

`<file>` 是包含伺服器憑證的檔案路徑。

`--server-type <response|telemetry>` 可讓您在 EDR Expert (on-premises) 整合模式下，選擇要為其新增或取代憑證的伺服器類型：

- `response` — OSMP 威脅回應操作伺服器
- `telemetry` — OSMP 遙測伺服器

如果您要新增或取代 KATA 伺服器憑證，請省略`--server-type`選項。

kesl-control --remove-kataedr-server-certificate

此命令可讓您移除先前新增的KATA 伺服器、OSMP 威脅回應伺服器或 OSMP 遙測伺服器的憑證（取決於整合模式）。

```
kesl-control [-R] --remove-kataedr-server-certificate [--server-type <response|telemetry>]
```

其中：

`--server-type <response|telemetry>` 可讓您在 EDR Expert (on-premises) 整合模式下，選擇要移除其憑證的伺服器類型：

- `response` — OSMP 威脅回應操作伺服器
- `telemetry` — OSMP 遙測伺服器

如果要移除 KATA 伺服器憑證，請省略`--server-type`選項。

kesl-control --query-kataedr-server-certificate

此命令可讓您檢視先前新增的KATA 伺服器、OSMP威脅回應伺服器或 OSMP 遙測伺服器（取決於整合模式）的憑證資訊。

```
kesl-control [-R] --query-kataedr-server-certificate [--server-type <response|telemetry>]
```

其中：

`--server-type <response|telemetry>` 可讓您在 EDR Expert (on-premises) 整合模式下，選擇要檢視其憑證資訊的伺服器類型：

- `response` — OSMP 威脅回應操作伺服器
- `telemetry` — OSMP 遙測伺服器

如果要檢視 KATA 伺服器憑證的資訊，請省略`--server-type`選項。

kesl-control --add-kataedr-client-certificate

此命令可讓您新增或者取代先前新增的用於防護與KATA 伺服器、OSMP威脅回應伺服器或 OSMP 遙測伺服器（取決於整合模式）連線的用戶端憑證的資訊。

```
kesl-control [-R] --add-kataedr-client-certificate <file>  [--server-type <response|telemetry>]
```

其中：

`<file>` 是加密容器（PFX 封存檔）的路徑，其中包含用戶端憑證和私密金鑰。

> 您必須指定加密容器的密碼。否則，當您按一下**輸入**時，會顯示 `Certificate password is required and cannot be empty` 錯誤。

`--server-type <response|telemetry>` 可讓您在 EDR Expert (on-premises) 整合模式下，選擇要為其新增用戶端憑證的伺服器類型：

- `response` — OSMP 威脅回應操作伺服器
- `telemetry` — OSMP 遙測伺服器

如果您要新增或取代用於 KATA 伺服器連線的用戶端憑證，請省略`--server-type`選項。

kesl-control --remove-kataedr-client-certificate

此命令可讓您刪除先前新增的用於防護與KATA 伺服器、OSMP威脅回應伺服器或 OSMP 遙測伺服器（取決於整合模式）連線的用戶端憑證。

```
kesl-control [-R] --remove-kataedr-client-certificate [--server-type <response|telemetry>]
```

其中：

`--server-type <response|telemetry>` 可讓您在 EDR Expert (on-premises) 整合模式下，選擇要移除其用戶端憑證的伺服器類型：

- `response` — OSMP 威脅回應操作伺服器
- `telemetry` — OSMP 遙測伺服器

如果您要移除用於 KATA 伺服器連線的用戶端憑證，請省略`--server-type`選項。

kesl-control --query-kataedr-client-certificate

此命令可讓您檢視先前新增的用於防護與KATA 伺服器、OSMP威脅回應伺服器或 OSMP 遙測伺服器（取決於整合模式）連線的用戶端憑證的資訊。

```
kesl-control [-R] --query-kataedr-client-certificate [--server-type <response|telemetry>]
```

其中：

`--server-type <response|telemetry>` 可讓您在 EDR Expert (on-premises) 整合模式下，選擇要檢視其用戶端憑證資訊的伺服器類型：

- `response` — OSMP 威脅回應操作伺服器
- `telemetry` — OSMP 遙測伺服器

如果要檢視與 KATA 伺服器連線的用戶端憑證訊息，請省略`--server-type`選項。

用於管理 EDR Expert (cloud) 元件的指令

-R 前綴表示該指令屬於用於管理與卡巴斯基 Detection and Response 解決方案之整合設定的指令群組。

kesl-control --query-cloudxdr-server-certificate

此指令可讓您檢視OSMP 威脅回應伺服器或 OSMP 遙測收集伺服器的憑證資訊。

```
kesl-control [-R] --query-cloudxdr-server-certificate --server-type <response|telemetry>
```

其中：

`--server-type <response|telemetry>` 可讓您在 EDR Expert (cloud) 整合模式下，選取要檢視其憑證資訊的伺服器類型：

- `response` — OSMP 威脅回應操作伺服器
- `telemetry` — OSMP 遙測伺服器

kesl-control --query-cloudxdr-client-certificate

此指令可讓您檢視先前新增的用戶端憑證資訊，該憑證用於保護與OSMP 威脅回應伺服器或 OSMP 遙測伺服器的連線。

```
kesl-control [-R] --query-cloudxdr-client-certificate --server-type <response|telemetry>
```

其中：

`--server-type <response|telemetry>` 可讓您在 EDR Expert (cloud) 整合模式下，選取要檢視其用戶端憑證資訊的伺服器類型：

- `response` — OSMP 威脅回應操作伺服器
- `telemetry` — OSMP 遙測伺服器

用於管理 NDR (KATA) 元件的命令

-R 前綴表示該指令屬於用於管理與卡巴斯基 Detection and Response 解決方案之整合設定的指令群組。

kesl-control --add-katandr-server-certificate

此指令可新增或取代先前新增的 NDR 伺服器憑證。

```
kesl-control [-R] --add-katandr-server-certificate <file>
```

其中：

`<file>` 是包含伺服器憑證的檔案路徑。

kesl-control --remove-katandr-server-certificate

此指令可移除 NDR 伺服器憑證。

```
kesl-control [-R] --remove-katandr-server-certificate
```

kesl-control --query-katandr-server-certificate

此指令可輸出關於 NDR 伺服器憑證的資訊。

```
kesl-control [-R] --query-katandr-server-certificate
```

kesl-control --add-katandr-client-certificate

此指令可新增或取代用於防護與 NDR 伺服器連線的先前新增的用戶端憑證。

```
kesl-control [-R] --add-katandr-client-certificate <file>
```

其中：

`<file>` 是加密容器（PFX 封存檔）的路徑，其中包含用戶端憑證和私密金鑰。

> 您必須指定加密容器的密碼。否則，當您按一下**輸入**時，會顯示 `Certificate password is required and cannot be empty` 錯誤。

kesl-control --remove-katandr-client-certificate

此指令可刪除用於防護與 NDR 伺服器連線的用戶端憑證。

```
kesl-control [-R] --remove-katandr-client-certificate
```

kesl-control --query-katandr-client-certificate

此指令可輸出關於用戶端憑證的資訊。

```
kesl-control [-R] --query-katandr-client-certificate
```

用於管理裝置網路隔離的命令

-R 前綴表示該指令屬於用於管理與卡巴斯基 Detection and Response 解決方案之整合設定的指令群組。與指定的 Detection and Response 解決方案整合後，裝置的網路隔離將會套用為偵測到威脅後的威脅回應操作。

kesl-control --isolation-stat

此命令可將網路隔離的目前狀態輸出到主控台：已啟用或已停用。

```
kesl-control [-R] --isolation-stat
```

kesl-control --isolation-off

此指令可讓您停用裝置的網路隔離。

```
kesl-control [-R] --isolation-off
```

用於管理 KUMA 整合設定的指令

-M 前綴表示該指令屬於用於管理 Kaspersky Unified Monitoring and Analysis Platform 設定的指令群組。

kesl-control --add-kuma-server-certificate

此指令可新增或取代先前新增的 KUMA 伺服器憑證。

```
kesl-control [-M] --add-kuma-server-certificate <path to file>
```

其中：

`<path to file>` 是包含 DER 或 PEM 格式伺服器憑證的檔案路徑。

kesl-control --remove-kuma-server-certificate

此指令可刪除 KUMA 伺服器憑證。

```
kesl-control [-M] --remove-kuma-server-certificate
```

kesl-control --query-kuma-server-certificate

此指令可輸出關於 KUMA 伺服器憑證的資訊。

```
kesl-control [-M] --query-kuma-server-certificate
```

kesl-control --add-kuma-client-certificate

此指令可新增或取代用於防護與 KUMA 伺服器連線的先前新增的用戶端憑證。

```
kesl-control [-M] --add-kuma-client-certificate <path to file>
```

其中：

`<path to file>` 是加密容器（PFX 封存檔）的路徑，其中包含用戶端憑證和私密金鑰。

> 您必須指定加密容器的密碼。否則，當您按一下**輸入**時，會顯示 `Certificate password is required and cannot be empty` 錯誤。

kesl-control --remove-kuma-client-certificate

此指令可刪除用於防護與 KUMA 伺服器連線的用戶端憑證。

```
kesl-control [-M] --remove-kuma-client-certificate
```

kesl-control --query-kuma-client-certificate

此指令可輸出關於用戶端憑證的資訊。

```
kesl-control [-M] --query-kuma-client-certificate
```

用於管理 Sandbox 整合設定的指令

-X 前置詞表示該指令屬於用於管理Sandbox 整合設定的指令群組。

kesl-control --add-sandbox-server-certificate

此命令會新增或取代負責與 Sandbox 互動的伺服器的先前新增的憑證。

```
kesl-control [-X] --add-sandbox-server-certificate <file>
```

其中：

`<file>` 是包含 DER 或 PEM 格式伺服器憑證的檔案路徑。

kesl-control --remove-sandbox-server-certificate

此命令會刪除負責與 Sandbox 互動的伺服器的憑證。

```
kesl-control [-X] --remove-sandbox-server-certificate
```

kesl-control --query-sandbox-server-certificate

此命令顯示關於負責與 Sandbox 互動的伺服器的憑證的資訊。

```
kesl-control [-X] --query-sandbox-server-certificate
```

kesl-control --add-sandbox-client-certificate

此命令會新增或取代先前新增的用戶端憑證，該憑證用於對負責與 Sandbox 互動的伺服器的連線提供防護。

```
kesl-control [-X] --add-sandbox-client-certificate <file>
```

其中：

`<file>` 是加密容器（PFX 封存檔）的路徑，其中包含用戶端憑證和私密金鑰。

> 您必須指定加密容器的密碼。否則，當您按一下**輸入**時，會顯示 `Certificate password is required and cannot be empty` 錯誤。

kesl-control --remove-sandbox-client-certificate

此命令會刪除用於對負責與 Sandbox 互動的伺服器的連線提供防護的用戶端憑證。

```
kesl-control [-X] --remove-sandbox-client-certificate
```

kesl-control --query-sandbox-client-certificate

此指令可輸出關於用戶端憑證的資訊。

```
kesl-control [-X] --query-sandbox-client-certificate
```

kesl-control --sandbox

此指令可將要掃描的檔案傳送至 Sandbox。

```
kesl-control [-X] --sandbox <path 1> <path 2>
```

其中：

`<path>` 是您要掃描的檔案或目錄路徑。您可以指定多個路徑，以空格分隔。

用於管理 IOC 掃描的指令

`-T` 前置詞表示該指令屬於用於管理應用程式設定和工作的指令群組。

kesl-control --scan-ioc

此指令可啟動搜尋裝置上的入侵指標 (IOC)。

```
kesl-control [-T] --scan-ioc --path <path to directory or file> [--process on|off] [--hint <regular expression>]
[--arpentry on|off] [--ports on|off] [--system on|off] [--files on|off] [--drives all|system|critical|custom] [--
excludes <list of exclusions>] [--scope <list of directories>] [--action
Skip|QuarantineFile|IsolateHost|ScanCriticalAreas]
```

其中：

`--path <path to directory or file>` 是 IOC 檔案的路徑，或包含副檔名為 .IOC 或 .XML 之 IOC 檔案的目錄路徑，應用於執行掃描。

> 您可以指定多個路徑，以空格分隔。您也可以指定兩種類型的路徑（檔案路徑和目錄路徑）。

`--process` — 啟用對裝置上執行的處理程序的分析。

可能的參數：

- on — 啟用對裝置上執行的處理程序的分析（預設值）。
- `off` — 停用對裝置上執行的處理程序的分析。

如果不指定`--process`選項，則僅當使用的 IOC 檔案指定了這些處理程序的詳細資訊（`ProcessItem`）時，應用程式才會分析處理程序。

`--hint <regular expression>` 是與要分析的檔案 (`FileItem`) 或處理程序可執行檔 (`ProcessItem`) 的完整路徑相符的正規運算式。

您可以使用以下正規表達式元素：

- 中繼字元：`.` `^` `$` `|`
- 字元類別：`digit`、`alpha`、`lower`、`upper`、`cntrl`
- 量詞：`*` `+` `?` `{n}` `{n,}` `{n, m}`
- 否定：`[^a-c]`
- 逸出字元：`\a` `\e` `\f`，`\n` `\r` `\t` `\v` `\b`

`--arpentry` — 啟用分析 ARP 表 (`ArpEntryItem`) 中的條目。

可能的參數：

- `on` — 啟用分析 ARP 表中的條目（預設值）。
- `off` — 停用分析 ARP 表中的條目。

如果不指定`--arpentry`選項，則僅當使用的 IOC 檔案指定了 ARP 表 (`ArpEntryItem`) 的詳細資訊時，應用程式才會分析 ARP 表。

`--ports` — 啟用分析用於連線的開放連接埠。

可能的參數：

- `on` — 啟用分析用於連線的開放連接埠並掃描裝置上的活動連線（預設值）。
- `off` — 停用分析用於連線的開放連接埠並且不掃描裝置上的活動連線。

如果不指定`--ports`選項，則僅當使用的 IOC 檔案指定了這些連接埠的詳細資訊（`PortItem`）時，應用程式才會分析連接埠。

`--system` — 啟用系統環境分析。

可能的參數：

- `on` — 啟用系統環境分析（預設值）。
- `off` — 停用系統環境分析。

如果不指定`--system`選項，則僅當使用的 IOC 檔案指定了系統環境 (`SystemInfoItem`) 的詳細資訊時，應用程式才會分析系統環境。

`--files` — 啟用檔案分析。

可能的參數：

- `on` — 啟用檔案分析（預設值）。
- `off` — 停用檔案分析。

如果沒有指定`--files`選項，則僅當使用的 IOC 檔案指定了這些檔案的詳細資訊 (`FileItem`) 時，應用程式才會分析檔案。

`--drives` — 要掃描的區域。

可能的參數：

- `all`— 檢查所有可用的檔案區域。
- `system` — 掃描根檔案系統中的所有檔案。
- `critical` — 掃描使用者和系統目錄中的檔案（預設值）。
- `custom` — 僅掃描您指定區域中的檔案。

如果您未指定`--drives`選項，應用程式將分析使用者和系統目錄中的檔案。

`--excludes <list of exclusions>` 是排除在掃描範圍外的路徑清單。

此選項指定的排除項目是全域的，並且無論範圍類型或目錄清單如何均有效。這些排除項目優先於其他指令列選項，包括`--hint`和`--scope`。

> 排除項目被指定為路徑，但不能包含遞歸元素或通配符（例如`*`）。

如果不指定`--excludes`選項，則掃描執行時將不進行排除。

您可以指定多個排除項目，以空格分隔。

`--scope <list of directories>` 是要掃描的其他目錄清單。

> 如果您為 `custom` 選項指定了 `--drives` 參數，則需要此選項。

`--action` — 當偵測到入侵指標時執行的操作。

可能的參數：

- `Skip` — 應用程式不會對偵測到的物件執行任何操作，但關於它的資訊將保存在工作執行結果中（預設值）。
- `QuarantineFile` — 應用程式將隔離偵測到的物件。
- `IsolateHost` — 應用程式對偵測到物件的裝置實施網路隔離。
- `ScanCriticalAreas` – 應用程式將執行關鍵區域掃描。

Kaspersky Endpoint Security 掃描的關鍵區域

- /lib/systemd
- /lib/udev
- /lib/dbus-1.0
- /usr/local/lib/systemd/user
- /usr/share/dbus-1
- /usr/share/gdm/autostart
- /usr/share/gnome/autostart
- /var/spool/at
- /var/spool/在/spool
- /var/spool/anacron
- /var/spool/cron
- /boot

- /bin
- /sbin
- /lib
- /lib32
- /lib64
- /libx32
- /usr/lib
- /usr/lib32
- /usr/lib64
- /usr/libx32
- ~/.config/autostart
- ~/.config/autostart-scripts
- ~/.config/plasma-workspace/env
- ~/.config/plasma-workspace/shutdown
- ~/.config/lxsession
- ~/.fluxbox/startup
- ~/.kde/Autostart
- /etc

您可以用逗號分隔來指定多個操作。

> 如果指定`Skip`參數，請不要新增任何其他參數。`Skip`參數只能單獨使用。

kesl-control --get-response-task-list

此指令顯示裝置上正在執行的 *IOC 掃描* 工作的相關資訊。

```
kesl-control [-T] --get-response-task-list
```

因此，應用程式會以下列格式顯示正在執行工作的相關資訊：

工作 ID：<工作 ID>
回應操作：locScan

建立日期：<工作建立日期和時間>

啟動工作：<工作啟動排程>

狀態：<工作狀態>

Kaspersky Endpoint Security 會在每次與伺服器同步時，更新正在執行的 *IOC 掃描* 工作的相關資訊。您可以在與卡巴斯基 Detection and Response 解決方案整合的設定中設定同步週期（ `SynchronizationPeriod` ）。預設情況下，應用程式每 5 分鐘與伺服器同步一次。

kesl-control --delete-response-task <工作 ID>

此指令會依 ID 刪除 *IOC 掃描* 工作。應用程式會在電腦本機刪除該工作。如果您尚未在網頁主控台或 OSMP Console 中刪除該工作，應用程式會在下次與伺服器同步時還原該工作。

```
kesl-control [-T] --delete-response-task-list <task ID>
```

Light Agent 模式下的應用程式指令

-V 前置字元表示此指令屬於 Kaspersky Endpoint Security 在 Light Agent 模式下使用的指令群組。

> 只有在 Kaspersky Endpoint Security 以 Light Agent 模式使用時，才可以執行這些指令。

kesl-control --ksvla-info

此指令會輸出資訊，說明如何在 Light Agent 模式下使用應用程式。

```
kesl-control --ksvla-info
```

kesl-control --viis-info

此指令會輸出資訊，內容是關於將 Light Agent 模式下的應用程式連線到 Integration Server。

```
kesl-control --viis-info
```

kesl-control --svm-info

此指令會輸出資訊，內容是關於將 Light Agent 模式下的應用程式連線到 SVM。

```
kesl-control --svm-info
```

應用程式命令列選項

更新工作

下表說明您可以為 Update 工作指定之所有設定的所有可用值和預設值。

更新工作設定

設定	描述	參數值
ConnectionTimeout	嘗試連線更新來源時的回應逾時（以秒為單位）。如果更新來源在指定的時間間隔內沒有回應，應用程式將聯絡清單中的下一個更新來源。	只能使用 0 至 120 範圍內的整數。 預設值：10。
ApplicationUpdateMode	如何下載並安裝自動安裝的應用程式更新（自動修補程式）。	Disabled — 不下載或安裝自動修補程式。 DownloadOnly（預設值）— 下載自動修補程式，但不安裝它們。 DownloadAndInstall：自動下載並安裝自動修補程式。自動修補程式安裝後，應用程式將自動重新啟動。
[Sources.item_#]部分包含以下設定：		
Enabled	使用SourceType 設定中指定的更新來源。 要執行該工作，至少需要啟用一個更新來源。	Yes（預設）— 應用程式正在使用更新來源。 No — 應用程式未使用更新來源。
SourceType	應用程式從其接收更新的來源。	KLServers（預設值）— 應用程式從其中一個卡巴斯基更新伺服器接收更新。更新透過 HTTPS 協定下載。 SCServer。應用程式從安裝在本機網路上的管理伺服器下載更新到受防護的裝置。如果您使用卡巴斯基安全管理中心集中管理組織中的裝置防護，則可以選擇此更新來源。 Custom。應用程式從URL 設定中指定的自訂來源下載更新。您可以指定 FTP、HTTP 和 HTTPS 伺服器上的目錄或受防護用戶端裝置上掛載的任何裝置上的目錄，包括透過 Samba 或 NFS 協定掛載的遠端裝置上的目錄。
URL	區域網路或網際網路上的自訂更新來源的位址。	預設值未定義。 例如： URL=http://example.com/bases/ — 包含更新目錄的 HTTP 伺服器位址。 URL=/home/bases/ — 受防護電腦上包含應用程式資料庫的目錄。

主機威脅防護

檔案威脅防護工作

在指令列中，您可以使用檔案威脅防護預定義工作 (`File_Threat_Protection`) 來管理檔案威脅防護。

檔案威脅防護工作預設啟動。您可以手動啟動和停止此工作。

> 從指令列啟動和停止檔案威脅防護工作需要管理員角色權限。

您可以透過編輯檔案威脅防護預定義工作的設定來配置檔威脅防護設定。

下表說明您可以為檔案威脅防護工作指定的所有設定的所有可能值和預設值。

檔案威脅防護工作設定

設定	描述	參數值
`ScanArchived`	啟用壓縮檔案掃描（包括 SFX 自解壓縮檔案）。 應用程式掃描以下壓縮檔案：.zip；.7z*；.7-z；.rar；.iso；.cab；.bz；.bz2；.tbz；.tbz2；.gz；.tgz；.arj。支援的壓縮檔案格式清單取決於所使用的應用程式資料庫。 我們不建議啟用此設定，因為掃描壓縮檔案會影響效能，因為在將壓縮檔案解壓縮到臨時目錄並進行掃描時，對壓縮檔案的存取會被封鎖。	`Yes` — 掃描壓縮檔案。 如果將 `ActionOnThreat` 設定為 `DisinfectDeleteIfNotPossible`，並且無法解毒，則應用程式會根據壓縮檔案類型，刪除感染物件或包含威脅的整個壓縮檔案。 `No`（預設值）— 不掃描壓縮檔案。
`ScanSfxArchived`	僅啟用對自解壓縮檔案（包含可執行解壓縮模組的壓縮檔案）的掃描。	`Yes` — 掃描自解壓縮檔案。 `No`（預設值）— 不掃描自解壓縮檔案。
`ScanMailBases`	啟用掃描 Microsoft Outlook、Outlook Express、The Bat 和其他郵件用戶端的電子郵件資料庫。	`Yes` — 掃描電子郵件資料庫的檔案。 `No`（預設值）— 不掃描電子郵件資料庫的檔案。
`ScanPlainMail`	啟用純文字電子郵件訊息的掃描。	`Yes` — 掃描純文字電子郵件。 `No`（預設值）— 不掃描純文字電子郵件。
`SkipPlainTextFiles`	暫時將文字格式的檔案排除在掃描之外。此設定可以最佳化應用程式記錄的掃描。 如果您使用基於 fanotify 的系統事件攔截機制，則會套用此設定。使用可更新的內核模組時，系統會利用掃描結果快取來最佳化掃描。	`Yes` – 如果文字檔案在最近一次掃描後的 10 分鐘內被同一處理程序重複使用，則不要掃描這些文字檔案。 `No`（預設值）– 以純文字格式掃描檔案。
`SkipDatabaseJournals`	暫時將資料庫日誌檔案排除在掃描範圍之外。此設定可以最佳化資料庫日誌檔案的掃描。 如果您使用基於 fanotify 的系統事件攔截機制，則會套用此設定。使用可更新的內核模組時，系統會利用掃描結果快取來最佳化掃描。	`Yes` – 如果資料庫日誌檔案在最近一次掃描後 10 分鐘內由同一處理程序重複使用，則不會掃描這些日誌檔案。 `No`（預設）– 掃描資料庫日誌檔案。

設定	描述	參數值
SizeLimit	要掃描的物件的最大大小（以兆位元組為單位）。如果要掃描的物件大於指定值，應用程式將跳過該物件。	0 至 999999 0 — 應用程式可掃描任意大小的物件。 預設值：0。
TimeLimit	最大物件掃描持續時間（以秒為單位）。 如果掃描時間超過此設定指定的時間，應用程式將停止掃描物件。	0 至 9999 0 — 物件掃描時間不受限制。 預設值：60。
ActionOnThreat	選取應用程式對感染物件執行的動作。	DisinfectDeleteIfNotPossible（解毒；如果不能解毒則刪除）表示應用程式會先將物件副本儲存在備份中，隨後嘗試對感染物件解毒。如果無法進行解毒（例如，如果無法對該類型的物件或該物件中的威脅類型解毒），則應用程式將刪除感染物件。 DisinfectBlockIfNotPossible（解毒；如果無法解毒則封鎖）表示應用程式會先將物件副本儲存在備份中，隨後嘗試對感染物件解毒。如果無法進行解毒（例如，如果無法對該類型的物件或該物件中的威脅類型解毒），則應用程式將封鎖對感染物件的存取。 Block — 應用程式封鎖對受感染物件的存取。 預設值：DisinfectDeleteIfNotPossible。
UseExcludeMasks	允許從掃描中排除由ExcludeMasks.item_#設定指定的物件。	Yes — 從掃描中排除ExcludeMasks.item_#設定指定的物件。 No（預設值）— 不從掃描中排除ExcludeMasks.item_#設定指定的物件。
ExcludeMasks.item_#	按名稱或遮罩排除掃描物件。 您可以使用此設定按名稱從指定的掃描範圍中排除單一檔案，或使用 shell 格式的遮罩一次排除多個檔案。	預設值未定義。 範例 UseExcludeMasks=Yes ExcludeMasks.item_0000=eicar1.* ExcludeMasks.item_0001=eicar2.*
UseExcludeThreats	啟用從掃描中排除包含 ExcludeThreats.item_# 設定所指定威脅的物件。	Yes — 從掃描中排除包含ExcludeThreats.item_#設定所指定的威脅的物件。 No（預設值）：不從掃描中排除包含ExcludeThreats.item_#設定指定的威脅的物件。
ExcludeThreats.item_#	根據偵測到的威脅名稱從掃描中排除物件。在為此設定指定值之前，請確保UseExcludeThreats設定已啟用。 為了從掃描中排除物件，請指定在此物件中偵測到的威脅的全名 — 包含應用程式判定物件被感染的字串。 例如，您可能正在使用公用程式來獲取關於網路的資訊。為了防止應用程式封鎖它，請將其中包含的威脅的全名新增至排除掃描的威脅清單。 您可以在應用程式記錄或網站https://threats.kaspersky.com 中找到在物件中偵測到的威脅的全名。	設定值區分大小寫。 預設值未定義。 範例 UseExcludeThreats=Yes ExcludeThreats.item_0000=EICAR-Test-* ExcludeThreats.item_0001=?rojan.Linux
ReportCleanObjects	啟用記錄關於應用程式報告未被感染的掃描物件的資訊。 例如，您可以啟用此設定，以確保應用程式掃描了特定物件。	Yes — 記錄關於未感染物件的資訊。 No（預設值）— 不記錄關於未感染物件的資訊。
ReportPackedObjects	啟用記錄關於作為複合物件一部分的掃描物件的資訊。 例如，您可以啟用此設定來確保應用程式已掃描壓縮檔案內的物件。	Yes — 記錄關於壓縮檔案中已掃描物件的資訊。 No（預設值）— 不記錄關於檔案中掃描物件的資訊。
ReportUnprocessedObjects	啟用記錄關於由於某種原因尚未處理的物件的資訊。	Yes — 記錄關於未處理物件的資訊。 No（預設值）— 不記錄關於未處理物件的資訊。

設定	描述	參數值
UseAnalyzer	啟用啟發式分析。 啟發式分析可以幫助應用程式在病毒分析師發現威脅之前就偵測到威脅。 此設定不適用於配備 Elbrus CPU 的裝置。	Yes（預設值）— 啟用啟發式分析器。 No — 停用啟發式分析器。
HeuristicLevel	指定啟發式分析級別。 啟發式分析級別可設定威脅搜尋的徹底性、作業系統資源的負載和掃描持續時間之間的平衡。啟發式分析級別越高，掃描所需的資源和時間就越多。 此設定不適用於配備 Elbrus CPU 的裝置。	Light — 最不徹底的掃描，系統負載最小。 Medium — 中等啟發式分析級別，系統負載平衡。 Deep — 最徹底的掃描，系統負載最大。 Recommended（預設值）— 建議的值。
UseIChecker	啟用 iChecker 技術。	Yes（預設值）— 啟用 iChecker 技術。 No — 停用 iChecker 技術。
ScanByAccessType	檔案威脅防護工作運作模式。ScanByAccessType 設定僅適用於「檔案威脅防護」工作。	SmartCheck（預設值）— 在嘗試開啟檔案時掃描檔案，如果檔案已修改，則在嘗試關閉檔案時再次掃描檔案。如果處理程序在執行過程中多次存取某個物件並對其進行修改，則應用程式僅在該處理程序最後一次關閉該物件時才會再次掃描該物件。 OpenAndModify — 在嘗試開啟檔案時掃描檔案，如果檔案已被修改，則在嘗試關閉檔案時再次掃描檔案。 Open — 掃描檔案，檢查是否嘗試開啟它以進行讀取、執行或修改。
[ScanScope.item_#]部分包含以下設定：		
AreaDesc	掃描範圍的描述，包含關於掃描範圍的附加資訊。 使用此設定指定的字串的最大長度為 4096 個字元。	預設值：All objects。 範例 AreaDesc="Scanning of email databases"
UseScanArea	啟用指定範圍的掃描。若要執行該工作，請啟用至少一個範圍的掃描。	Yes（預設值）— 掃描指定範圍。 No — 不掃描指定範圍。
AreaMask.item_#	掃描範圍限制。在此掃描範圍下，應用程式僅掃描使用 shell 格式的遮罩指定的檔案。 如果未指定此設定，應用程式將掃描掃描範圍內的所有物件。您可以為此設定指定多個值。	預設值為 *（掃描所有物件）。 範例 AreaMask_item_<item number>=*doc
Path	包含要掃描的物件的目錄的路徑。	<path to local folder> – 掃描指定目錄中的物件。您可以使用遮罩和標籤來指定路徑。 Shared:NFS — 掃描可透過 NFS 協定存取的裝置檔案系統資源。 Shared:SMB — 掃描可透過 Samba 協定存取的裝置檔案系統資源。 Mounted:NFS — 使用 NFS 協定掃描裝置上安裝的遠端目錄。 Mounted:SMB — 使用 Samba 協定掃描裝置上安裝的遠端目錄。 AllRemoteMounted — 使用 Samba 和 NFS 協定掃描裝置上安裝的所有遠端目錄。 AllShared — 掃描所有可透過 Samba 和 NFS 協定存取的裝置檔案系統資源。 <file system type> – 掃描指定檔案系統裝置的所有資源。
[ExcludedFromScanScope.item_#]部分包含以下設定：		
AreaDesc	掃描排除範圍的描述，包含關於排除掃描範圍的附加資訊。	預設值未定義。

設定	描述	參數值
UseScanArea	從掃描中排除指定的掃描範圍。	Yes（預設值）— 排除指定範圍。 No — 不排除指定的範圍。
AreaMask.item_#	掃描排除項目範圍的限制。在排除範圍內，應用程式僅從掃描中排除使用 shell 格式的遮罩指定的檔案。 如果未指定此設定，應用程式將不會掃描排除範圍內的任何物件。您可以為此設定指定多個值。	預設值：*（從掃描中排除所有物件）
Path	包含要排除的物件的目錄的路徑。	<path to local folder> – 從掃描中排除指定目錄（包括子目錄）中的物件。您可以使用遮罩和標籤來指定路徑。 Mounted:NFS — 從掃描中排除使用 NFS 協定掛載在裝置上的遠端目錄。 Mounted:SMB — 從掃描中排除使用 Samba 協定安裝在裝置上的遠端目錄。 AllRemoteMounted — 從掃描中排除使用 Samba 和 NFS 協定安裝在裝置上的所有遠端目錄。 <file system> – 從掃描中排除指定檔案系統裝置的所有資源。
[ExcludedForProgram.item_#]部分包含以下設定：		
ProgramPath	被排除的處理程序的路徑。 如果使用可更新內核模組進行系統事件攔截，則指定的處理程序將被排除在所有命名空間的攔截之外。	<path to process> — 從掃描中排除指定目錄中的物件。
ApplyToDescendants	從掃描中排除 ProgramPath 設定指定的排除處理程序的子處理程序。	Yes – 從掃描中排除指定處理程序及其所有子處理程序。 No（預設值）- 僅從掃描中排除指定的處理程序，不從掃描中排除其子處理程序。
AreaDesc	處理程序排除範圍的描述。	預設值：All objects。
UseExcludedForProgram	從掃描中排除指定的掃描範圍。	Yes（預設值）— 排除指定範圍。 No — 不排除指定的範圍。
AreaMask.item_#	處理程序排除範圍的限制。在處理程序排除範圍內，應用程式僅從掃描中排除使用 shell 格式的遮罩指定的檔案。 如果未指定此設定，應用程式將從掃描中排除處理程序排除範圍內的所有物件。您可以為此設定指定多個值。	預設值：*（從掃描中排除所有物件）
Path	包含被處理程序修改的檔案的目錄的路徑。	<path to local folder> — 從掃描中排除指定目錄中的物件。您可以使用遮罩來指定路徑。 Shared:NFS — 從掃描中排除可透過 NFS 協定存取的裝置檔案系統資源。 Shared:SMB — 從掃描中排除可透過 Samba 協定存取的裝置檔案系統資源。 Mounted:NFS — 從掃描中排除使用 NFS 協定掛載在裝置上的遠端目錄。 Mounted:SMB — 從掃描中排除使用 Samba 協定安裝在裝置上的遠端目錄。 AllRemoteMounted — 從掃描中排除使用 Samba 和 NFS 協定安裝在裝置上的所有遠端目錄。 AllShared — 從掃描中排除所有可使用 Samba 和 NFS 協定存取的裝置檔案系統資源。 <file system type> – 從掃描中排除指定檔案系統裝置的所有資源。

實用文章

如何指定遮罩

您可以使用*（星號）字元來建立檔案或目錄名稱遮罩。

您可以指示單一*字元來表示檔案或目錄名稱中/字元前面的任意字元集（包括空集）。例如，/dir/*/file 或 /dir/*/*/file。

您可以用兩個連續的*字元來表示檔案或目錄名稱中的任意一組字元（包括空集和/字元）。例如，/dir/**/file*/ 或 /dir/file**/。

遮罩在目錄名稱中只能使用一次。例如，/dir//**/file是一個不正確的遮罩。

您可以使用單一?字元來表示檔案或目錄名稱中的任意一個字元。

如何使用標籤

您可以使用特殊標籤來指定容器或映像：

- [container-id:<id>]/<path to local directory>
- [container-name:<name>]/<path to local directory>
- [image-id:<id>]/<path to local directory>
- [image-name:<name>]/<path to local directory>

其中：

<id> 是容器 ID。

<name> 是容器名稱

<path to local directory> 是本機目錄路徑。

您也可以使用標籤的唯一組合：[container-id:<id>]、[container-name:<name>]、[image-id:<id>] 和 [image-name:<name>]/path to local directory>。

允許在一個區域內任意組合1到 4 個唯一標籤。列出的順序不重要。

範例：

- [container-name:<name>][image-name:<name>]/path to local directory>
- [container-id:<id>][image-name:<name>]/<path to local directory>
- [image-name:<name>][image-id:<id>]/<path to local directory>

- [container-name:<name>][container-id:<id>][image-name:<name>]/<path to local directory>
- [container-name:<name>][image-id:<id>][container-id:<id>][image-name:<name>]/path to local directory>

您可以在名稱和識別碼中使用遮罩（`?`和`*`字元）。

最佳化網路目錄掃描

為了最佳化檔案威脅防護工作，您可以從掃描中排除從網路目錄複製到本機目錄的任何檔案。為此，請根據用於從網路目錄複製的實用程式（例如，`cp`實用程式）的處理程序配置排除。

若要設定從掃描中排除網路目錄：

1. 使用下列指令將檔案威脅防護工作設定（`File_Threat_Protection`，ID:1）輸出至設定檔：

```
kesl-control --get-settings 1 --file <full path to the configuration file> [--json]
```

2. 開啟設定檔並新增 `[ExcludedForProgram.item_#]` 區段，其設定如下：

   - `ProgramPath`— 要排除的處理程序的路徑或包含要排除的處理程序的目錄的路徑。
   - `ApplyToDescendants`是一個參數，指示掃描是否應該排除被排除處理程序的子處理程序（可能的值：`Yes`或`No`）。
   - `AreaDesc`— 處理程序排除範圍的描述，包含關於排除範圍的附加資訊。
   - `UseExcludedForProgram`可啟用在工作運行期間排除指定範圍（可能的值：`Yes`或`No`）。
   - `Path`— 包含處理程序修改的檔案或目錄的路徑。
   - `AreaMask.item_#`是要從掃描中排除的檔案的檔案名稱遮罩。您也可以指定檔案的完整路徑。

   範例

```
[ExcludedForProgram.item_0000]
ProgramPath=/usr/bin/cp
ApplyToDescendants=No
AreaDesc=
UseExcludedForProgram=Yes
Path=AllRemoteMounted
AreaMask.item_0000=*
```

3. 執行以下指令：

```
kesl-control --set-settings 1 --file <full path to the configuration file> [--json]
```

   如果要從 JSON 格式的設定檔匯入設定，請指定`--json`選項。如果未指定該選項，應用程式將嘗試從 INI 檔案匯入設定。如果匯入失敗，則會顯示錯誤。

應用程式不會掃描網路目錄中的檔案，而是掃描`cp`指令本身（對於上面給出的範例）和本機檔案。

惡意軟體掃描

在指令列中，您可以透過以下方式掃描惡意軟體：

- 使用惡意軟體掃描預定義工作（`Scan_My_Computer`）。您可以手動啟動、停止、暫停或繼續此工作，以及設定工作排程。您可以透過編輯此工作的設定來配置掃描設定。
- 使用惡意軟體掃描自訂工作（`ODS` 類型的工作）。您可以手動啟動、停止、暫停或繼續使用者工作，並設定工作排程。

您可以使用以下命令對指定的檔案和目錄執行*自訂掃描*：

```
kesl-control --scan-file
```

惡意軟體掃描工作

此表說明您可以為惡意軟體掃描工作（`Scan_My_Computer`）指定的所有設定及其所有可能值和預設值。

惡意軟體掃描工作設定

設定	描述	參數值
`ScanFiles`	啟用檔案掃描。	`Yes`（預設值）— 掃描檔案。 `No` — 不掃描檔案。
`ScanBootSectors`	啟用引導磁區掃描。	`Yes`（預設值）— 掃描引導磁區。 `No` — 不掃描引導磁區。
`ScanComputerMemory`	啟用處理程序記憶體和核心記憶體掃描。	`Yes`（預設值）— 掃描處理程序記憶體和核心記憶體。 `No` — 不掃描處理程序記憶體和核心記憶體。
`ScanStartupObjects`	啟用啟動物件掃描。	`Yes`（預設值）— 掃描啟動物件。 `No` — 不掃描啟動物件。
`ScanArchived`	啟用壓縮檔案掃描（包括 SFX 自解壓縮檔案）。 應用程式掃描以下壓縮檔案：.zip；.7z*；.7-z；.rar；.iso；.cab；.bz；.bz2；.tbz；.tbz2；.gz；.tgz；.arj。支援的壓縮檔案格式清單取決於所使用的應用程式資料庫。	`Yes`（預設值）— 掃描壓縮檔案。 如果將 `ActionOnThreat` 設定為 `DisinfectDeleteIfNotPossible`，並且無法解毒，則應用程式會根據壓縮檔案類型，刪除感染物件或包含威脅的整個壓縮檔案。 `No` — 不掃描壓縮檔案。
`ScanSfxArchived`	僅啟用對自解壓縮檔案（包含可執行解壓縮模組的壓縮檔案）的掃描。	`Yes`（預設值）— 掃描自解壓縮檔案。 `No` — 不掃描自解壓縮檔案。
`ScanMailBases`	啟用掃描 Microsoft Outlook、Outlook Express、The Bat 和其他郵件用戶端的電子郵件資料庫。	`Yes` — 掃描電子郵件資料庫的檔案。 `No`（預設值）— 不掃描電子郵件資料庫的檔案。
`ScanPlainMail`	啟用純文字電子郵件訊息的掃描。	`Yes` — 掃描純文字電子郵件。 `No`（預設值）— 不掃描純文字電子郵件。
`SizeLimit`	要掃描的物件的最大大小（以兆位元組為單位）。如果要掃描的物件大於指定值，應用程式將跳過該物件。	0 至 999999 0 — 應用程式可掃描任意大小的物件。 預設值：0。

設定	描述	參數值
TimeLimit	最大物件掃描持續時間（以秒為單位）。如果掃描時間超過此設定指定的時間，應用程式將停止掃描物件。	0 至 9999 0 — 物件掃描時間不受限制。 預設值：0。
QueueScanTasks	如果先前啟動的排程掃描仍在執行，則延遲排程掃描工作。如果目前的掃描持續執行，Kaspersky Endpoint Security 會將排程掃描工作加入佇列。這將有助於最佳化電腦負載。例如，掃描工作排定在 18:00 和 20:00 執行。如果 18:00 的掃描仍在執行，則排定在 20:00 執行的掃描工作會延遲。延遲的工作會在 18:00 的工作完成後執行。	Yes，可在目前的掃描仍在執行時，將排程掃描工作加入佇列。 No（預設值），即使目前的掃描仍在執行，也會執行排程掃描工作。
ActionOnThreat	選取應用程式對感染物件執行的動作。	DisinfectDeleteIfNotPossible（解毒；如果不能解毒則刪除）表示應用程式會先將物件副本儲存在備份中，隨後嘗試對感染物件解毒。如果無法進行解毒（例如，如果無法對該類型的物件或該物件中的威脅類型解毒），則應用程式將刪除感染物件。 DisinfectInformIfNotPossible（解毒；如果無法解毒則告知）表示應用程式會先將物件副本儲存在備份中，隨後嘗試對感染物件解毒。如果無法進行解毒（例如，如果無法解毒該類型的物件或該物件中的威脅類型），則應用程式會在日誌中建立記錄。 Inform 表示應用程式不會嘗試解毒或刪除感染物件。會記錄關於感染物件的資訊。 預設值：DisinfectDeleteIfNotPossible。
UseExcludeMasks	允許從掃描中排除由 ExcludeMasks.item_# 設定指定的物件。	Yes — 從掃描中排除 ExcludeMasks.item_# 設定指定的物件。 No（預設值）— 不從掃描中排除 ExcludeMasks.item_# 設定指定的物件。
ExcludeMasks.item_#	按名稱或遮罩排除掃描物件。您可以使用此設定按名稱從指定的掃描範圍中排除單一檔案，或使用 shell 格式的遮罩一次排除多個檔案。 在為此設定指定值之前，請確保 UseExcludeMasks 設定已啟用。	預設值未定義。 範例 UseExcludeMasks=Yes ExcludeMasks.item_0000=eicar1.* ExcludeMasks.item_0001=eicar2.*
UseExcludeThreats	啟用從掃描中排除包含 ExcludeThreats.item_# 設定所指定威脅的物件。	Yes — 從掃描中排除包含 ExcludeThreats.item_# 設定所指定的威脅的物件。 No（預設值）：不從掃描中排除包含 ExcludeThreats.item_# 設定指定的威脅的物件。
ExcludeThreats.item_#	根據偵測到的威脅名稱從掃描中排除物件。在為此設定指定值之前，請確保 UseExcludeThreats 設定已啟用。 為了從掃描中排除物件，請指定在此物件中偵測到的威脅的全名 — 包含應用程式判定物件被感染的字串。 例如，您可能正在使用公用程式來獲取關於網路的資訊。為了防止應用程式封鎖它，請將其中包含的威脅的全名新增至排除掃描的威脅清單。 您可以在應用程式記錄或網站https://threats.kaspersky.com 中找到在物件中偵測到的威脅的全名。	設定值區分大小寫。 預設值未定義。 範例 UseExcludeThreats=Yes ExcludeThreats.item_0000=EICAR-Test-* ExcludeThreats.item_0001=?rojan.Linux
UseGlobalExclusions	啟用全域排除進行掃描。	Yes（預設值）— 使用全域排除。 No — 不使用全域排除。
UseOASExclusions	啟用檔案威脅防護排除項目進行掃描。	Yes（預設值）— 使用檔案威脅防護排除項目。 No — 不使用檔案威脅防護排除項目。

設定	描述	參數值
ReportCleanObjects	啟用記錄關於應用程式報告未被感染的掃描物件的資訊。 例如，您可以啟用此設定，以確保應用程式掃描了特定物件。	Yes — 記錄關於未感染物件的資訊。 No（預設值）— 不記錄關於未感染物件的資訊。
ReportPackedObjects	啟用記錄關於作為複合物件一部分的掃描物件的資訊。 例如，您可以啟用此設定來確保應用程式已掃描壓縮檔案內的物件。	Yes — 記錄關於壓縮檔案中已掃描物件的資訊。 No（預設值）— 不記錄關於檔案中掃描物件的資訊。
ReportUnprocessedObjects	啟用記錄關於由於某種原因尚未處理的物件的資訊。	Yes — 記錄關於未處理物件的資訊。 No（預設值）— 不記錄關於未處理物件的資訊。
UseAnalyzer	啟用啟發式分析。 啟發式分析可以幫助應用程式在病毒分析師發現威脅之前就偵測到威脅。	Yes（預設值）— 啟用啟發式分析器。 No — 停用啟發式分析器。
HeuristicLevel	指定啟發式分析級別。 您可以指定啟發式分析級別。啟發式分析級別可設定威脅搜尋的徹底性、作業系統資源的負載和掃描持續時間之間的平衡。啟發式分析級別越高，掃描所需的資源和時間就越多。	Light — 最不徹底的掃描，系統負載最小。 Medium — 中等啟發式分析級別，系統負載平衡。 Deep — 最徹底的掃描，系統負載最大。 Recommended（預設值）— 建議的值。
UseIChecker	啟用 iChecker 技術。	Yes（預設值）— 啟用 iChecker 技術。 No — 停用 iChecker 技術。
DeviceNameMasks.item_#	裝置名稱清單。應用程式將掃描這些裝置的引導磁區。 設定值不能為空。必須指定至少一個裝置名稱遮罩才能執行此工作。	AllObjects — 掃描所有裝置的引導磁區。 <device name mask> – 掃描名稱與指定遮罩相符的裝置的引導磁區。 預設值：/** — 裝置名稱中的任意一組字元，包括 / 字元。
[ScanScope.item_#]部分包含以下設定：		
AreaDesc	掃描範圍的描述，包含關於掃描範圍的附加資訊。使用此設定指定的字串的最大長度為 4096 個字元。	預設值：All objects。 範例 AreaDesc="Mail bases scan"
UseScanArea	啟用指定範圍的掃描。若要執行該工作，請啟用至少一個範圍的掃描。	Yes（預設值）— 掃描指定範圍。 No — 不掃描指定範圍。
AreaMask.item_#	掃描範圍限制。在掃描範圍內，應用程式僅掃描使用 shell 格式的遮罩指定的檔案。 如果未指定此設定，應用程式將掃描掃描範圍內的所有物件。您可以為此設定指定多個值。	預設值為 *（掃描所有物件）。 範例 AreaMask.item_0000=*doc
Path	包含要掃描的物件的目錄的路徑。	<path to local directory> – 掃描指定目錄中的物件。 Shared:NFS — 掃描可透過 NFS 協定存取的裝置檔案系統資源。 Shared:SMB — 掃描可透過 Samba 協定存取的裝置檔案系統資源。 Mounted:NFS — 使用 NFS 協定掃描裝置上安裝的遠端目錄。 Mounted:SMB — 使用 Samba 協定掃描裝置上安裝的遠端目錄。 AllRemoteMounted — 使用 Samba 和 NFS 協定掃描裝置上安裝的所有遠端目錄。 AllShared — 掃描所有可透過 Samba 和 NFS 協定存取的裝置檔案系統資源。 <file system type> – 掃描指定檔案系統裝置的所有資源。
[ExcludedFromScanScope.item_#]部分包含以下設定：		

設定	描述	參數值
AreaDesc	掃描排除範圍的描述，包含關於排除掃描範圍的附加資訊。	預設值未定義。
UseScanArea	從掃描中排除指定的掃描範圍。	Yes（預設值）— 排除指定範圍。 No — 不排除指定的範圍。
AreaMask.item_#	掃描排除項目範圍的限制。在排除範圍中，應用程式僅排除使用 shell 格式的遮罩指定的檔案。 如果未指定此設定，應用程式將排除排除範圍內的所有物件。您可以為此設定指定多個值。	預設值：*（排除所有物件）
Path	包含要排除的物件的目錄的路徑。	<path to local directory> – 從掃描中排除指定目錄（包括子目錄）中的物件。您可以使用遮罩來指定路徑。 為了最佳化掃描工作的運行，建議將系統以唯讀模式掛載的快照路徑新增至具有 btrfs 檔案系統且啟用活動快照的系統的排除項目中。例如，對於基於 SUSE/OpenSUSE 的系統，可以新增以下排除 /.snapshots/*/snapshot/ 。 預設會指定 / 路徑。應用程式將本機檔案系統的所有目錄排除在掃描之外。 Mounted:NFS — 從掃描中排除使用 NFS 協定掛載在裝置上的遠端目錄。 Mounted:SMB — 從掃描中排除使用 Samba 協定安裝在裝置上的遠端目錄。 AllRemoteMounted — 從掃描中排除使用 Samba 和 NFS 協定安裝在裝置上的所有遠端目錄。 <file system type> – 從掃描中排除指定檔案系統裝置的所有資源。 只有當遠端目錄在工作啟動前安裝時，應用程式才會將其排除在掃描範圍之外。工作啟動後裝載的遠端目錄不會被排除在掃描之外。

實用文章

如何指定遮罩

您可以使用*（星號）字元來建立檔案或目錄名稱遮罩。

您可以指示單一*字元來表示檔案或目錄名稱中/字元前面的任意字元集（包括空集）。例如，/dir/*/file 或 /dir/*/*/file。

您可以用兩個連續的*字元來表示檔案或目錄名稱中的任意一組字元（包括空集和/字元）。例如，/dir/**/file*/ 或 /dir/file**/。

遮罩在目錄名稱中只能使用一次。例如，/dir//**/file是一個不正確的遮罩。

您可以使用單一?字元來表示檔案或目錄名稱中的任意一個字元。

自訂掃描工作

此表說明您可為自訂掃描工作（Scan_File）指定之所有設定的所有可用值和預設值。

設定	描述	參數值
ScanFiles	啟用檔案掃描。	Yes（預設值）— 掃描檔案。 No — 不掃描檔案。
ScanBootSectors	啟用引導磁區掃描。	Yes — 掃描引導磁區。 No（預設值）— 不掃描開機磁區。
ScanComputerMemory	啟用處理程序記憶體和核心記憶體掃描。	Yes — 掃描處理程序記憶體和核心記憶體。 No（預設值）— 不掃描處理程序記憶體和核心記憶體。
ScanStartupObjects	啟用啟動物件掃描。	Yes — 掃描啟動物件。 No（預設值）— 不掃描啟動物件。
ScanArchived	啟用壓縮檔案掃描（包括 SFX 自解壓縮檔案）。 應用程式掃描以下壓縮檔案：.zip；.7z*；.7-z；.rar；.iso；.cab；.bz；.bz2；.tbz；.tbz2；.gz；.tgz；.arj。支援的壓縮檔案格式清單取決於所使用的應用程式資料庫。	Yes（預設值）— 掃描壓縮檔案。 如果將 ActionOnThreat 設定為 DisinfectDeleteIfNotPossible，並且無法解毒，則應用程式會根據壓縮檔案類型，刪除感染物件或包含威脅的整個壓縮檔案。 No — 不掃描壓縮檔案。
ScanSfxArchived	僅啟用對自解壓縮檔案（包含可執行解壓縮模組的壓縮檔案）的掃描。	Yes（預設值）— 掃描自解壓縮檔案。 No — 不掃描自解壓縮檔案。
ScanMailBases	啟用掃描 Microsoft Outlook、Outlook Express、The Bat! 和其他郵件用戶端的電子郵件資料庫。	Yes — 掃描電子郵件資料庫的檔案。 No（預設值）— 不掃描電子郵件資料庫的檔案。
ScanPlainMail	啟用純文字電子郵件訊息的掃描。	Yes — 掃描純文字電子郵件。 No（預設值）— 不掃描純文字電子郵件。
SizeLimit	要掃描的物件的最大大小（以兆位元組為單位）。如果要掃描的物件大於指定值，應用程式將跳過該物件。	0 至 999999 0 — 應用程式可掃描任意大小的物件。 預設值：0。
TimeLimit	最大物件掃描持續時間（以秒為單位）。如果掃描時間超過此設定指定的時間，應用程式將停止掃描物件。	0 至 9999 0 — 物件掃描時間不受限制。 預設值：0。
QueueScanTasks	如果先前啟動的排程掃描仍在執行，則延遲排程掃描工作。如果目前的掃描持續執行，Kaspersky Endpoint Security 會將排程掃描工作加入佇列。這將有助於最佳化電腦負載。例如，掃描工作排定在 18:00 和 20:00 執行。如果 18:00 的掃描仍在執行，則排定在 20:00 執行的掃描工作會延遲。延遲的工作會在 18:00 的工作完成後執行。	Yes，可在目前的掃描仍在執行時，將排程掃描工作加入佇列。 No（預設值），即使目前的掃描仍在執行，也會執行排程掃描工作。
ActionOnThreat	選取應用程式對感染物件執行的動作。	DisinfectDeleteIfNotPossible（解毒；如果不能解毒則刪除）表示應用程式會先將物件副本儲存在備份中，隨後嘗試對感染物件解毒。如果無法進行解毒（例如，如果無法對該類型的物件或該物件中的威脅類型解毒），則應用程式將刪除感染物件。 DisinfectInformIfNotPossible（解毒；如果無法解毒則告知）表示應用程式會先將物件副本儲存在備份中，隨後嘗試對感染物件解毒。如果無法進行解毒（例如，如果無法解毒該類型的物件或該物件中的威脅類型），則應用程式會在日誌中建立記錄。 Inform 表示應用程式不會嘗試解毒或刪除感染物件。會記錄關於感染物件的資訊。 預設值：DisinfectDeleteIfNotPossible。

設定	描述	參數值
UseExcludeMasks	允許從掃描中排除由ExcludeMasks.item_#設定指定的物件。	Yes — 從掃描中排除ExcludeMasks.item_#設定指定的物件。 No（預設值）不從掃描中排除ExcludeMasks.item_# 設定所指定的物件。
ExcludeMasks.item_#	按名稱或遮罩排除掃描物件。您可以使用此設定按名稱從指定的掃描範圍中排除單一檔案，或使用 shell 格式的遮罩一次排除多個檔案。	預設值未定義。 範例 UseExcludeMasks=Yes ExcludeMasks.item_0000=eicar1.* ExcludeMasks.item_0001=eicar2.*
UseExcludeThreats	啟用從掃描中排除包含 ExcludeThreats.item_# 設定所指定威脅的物件。	Yes — 從掃描中排除包含ExcludeThreats.item_#設定所指定的威脅的物件。 No（預設值）：不從掃描中排除包含ExcludeThreats.item_#設定指定的威脅的物件。
ExcludeThreats.item_#	根據偵測到的威脅名稱從掃描中排除物件。在為此設定指定值之前，請確保UseExcludeThreats設定已啟用。 為了從掃描中排除物件，請指定在此物件中偵測到的威脅的全名 — 包含應用程式判定物件被感染的字串。 例如，您可能正在使用公用程式來獲取關於網路的資訊。為了防止應用程式封鎖它，請將其中包含的威脅的全名新增至排除掃描的威脅清單。 您可以在應用程式記錄或網站https://threats.kaspersky.com 中找到在物件中偵測到的威脅的全名。	設定值區分大小寫。 預設值未定義。 範例 UseExcludeThreats=Yes ExcludeThreats.item_0000=EICAR-Test-* ExcludeThreats.item_0001=?rojan.Linux
UseGlobalExclusions	啟用全域排除進行掃描。	Yes（預設值）使用全域排除。 No — 不使用全域排除。
UseOASExclusions	啟用檔案威脅防護排除項目進行掃描。	Yes（預設值）使用檔案威脅防護排除。 No — 不使用檔案威脅防護排除項目。
ReportCleanObjects	啟用記錄關於應用程式報告未被感染的掃描物件的資訊。 例如，您可以啟用此設定，以確保應用程式掃描了特定物件。	Yes — 記錄關於未感染物件的資訊。 No（預設值）不記錄未感染物件的資訊。
ReportPackedObjects	啟用記錄關於作為複合物件一部分的掃描物件的資訊。 例如，您可以啟用此設定來確保應用程式已掃描壓縮檔案內的物件。	Yes — 記錄關於壓縮檔案中已掃描物件的資訊。 No（預設值）不記錄壓縮檔內已掃描物件的資訊。
ReportUnprocessedObjects	啟用記錄關於由於某種原因尚未處理的物件的資訊。	Yes — 記錄關於未處理物件的資訊。 No（預設值）不記錄未處理物件的資訊。
UseAnalyzer	啟用啟發式分析。 啟發式分析可以幫助應用程式在病毒分析師發現威脅之前就偵測到威脅。	Yes（預設值）啟用啟發式分析器。 No — 停用啟發式分析器。
HeuristicLevel	指定啟發式分析級別。 您可以指定啟發式分析級別。啟發式分析級別可設定威脅搜尋的徹底性、作業系統資源的負載和掃描持續時間之間的平衡。啟發式分析級別越高，掃描所需的資源和時間就越多。	Light — 最不徹底的掃描，系統負載最小。 Medium — 中等啟發式分析級別，系統負載平衡。 Deep — 最徹底的掃描，系統負載最大。 Recommended（預設值）– 建議的值。
UseIChecker	啟用 iChecker 技術。	Yes（預設值）啟用 iChecker 技術。 No — 停用 iChecker 技術。
DeviceNameMasks.item_#	裝置名稱清單。應用程式將掃描這些裝置的引導磁區。 設定值不能為空。必須指定至少一個裝置名稱遮罩才能執行此工作。	AllObjects — 掃描所有裝置的引導磁區。 <device name mask> – 掃描名稱與指定遮罩相符的裝置的引導磁區。 預設值：/** — 裝置名稱中的任意一組字元，包括 / 字元。

關鍵區域掃描工作

下表說明您可以為關鍵區域掃描工作（`Critical_Areas_Scan`）指定的所有設定及其所有可用值和預設值。

關鍵區域掃描工作設定

設定	描述	參數值
`ScanFiles`	啟用檔案掃描。	`Yes` — 掃描檔案。 `No`（預設值）— 不掃描檔案。
`ScanBootSectors`	啟用引導磁區掃描。	`Yes`（預設值）— 掃描引導磁區。 `No` — 不掃描引導磁區。
`ScanComputerMemory`	啟用處理程序記憶體和核心記憶體掃描。	`Yes`（預設值）— 掃描處理程序記憶體和核心記憶體。 `No` — 不掃描處理程序記憶體和核心記憶體。
`ScanStartupObjects`	啟用啟動物件掃描。	`Yes`（預設值）— 掃描啟動物件。 `No` — 不掃描啟動物件。
`ScanArchived`	啟用壓縮檔案掃描（包括 SFX 自解壓縮檔案）。 應用程式掃描以下壓縮檔案：.zip；.7z*；.7-z；.rar；.iso；.cab；.bz；.bz2；.tbz；.tbz2；.gz；.tgz；.arj。支援的壓縮檔案格式清單取決於所使用的應用程式資料庫。	`Yes`（預設值）— 掃描壓縮檔案。 如果將 `ActionOnThreat` 設定為 `DisinfectDeleteIfNotPossible`，並且無法解毒，則應用程式會根據壓縮檔案類型，刪除感染物件或包含威脅的整個壓縮檔案。 `No` — 不掃描壓縮檔案。
`ScanSfxArchived`	僅啟用對自解壓縮檔案（包含可執行解壓縮模組的壓縮檔案）的掃描。	`Yes`（預設值）— 掃描自解壓縮檔案。 `No` — 不掃描自解壓縮檔案。
`ScanMailBases`	啟用掃描 Microsoft Outlook、Outlook Express、The Bat 和其他郵件用戶端的電子郵件資料庫。	`Yes` — 掃描電子郵件資料庫的檔案。 `No`（預設值）— 不掃描電子郵件資料庫的檔案。
`ScanPlainMail`	啟用純文字電子郵件訊息的掃描。	`Yes` — 掃描純文字電子郵件。 `No`（預設值）— 不掃描純文字電子郵件。
`SizeLimit`	要掃描的物件的最大大小（以兆位元組為單位）。如果要掃描的物件大於指定值，應用程式將跳過該物件。	0 至 999999 0 — 應用程式可掃描任意大小的物件。 預設值：0。
`TimeLimit`	最大物件掃描持續時間（以秒為單位）。如果掃描時間超過此設定指定的時間，應用程式將停止掃描物件。	0 至 9999 0 — 物件掃描時間不受限制。 預設值：0。
`QueueScanTasks`	如果先前啟動的排程掃描仍在執行，則延遲排程掃描工作。如果目前的掃描持續執行，Kaspersky Endpoint Security 會將排程掃描工作加入佇列。這將有助於最佳化電腦負載。例如，掃描工作排定在 18:00 和 20:00 執行。如果 18:00 的掃描仍在執行，則排定在 20:00 執行的掃描工作會延遲。延遲的工作會在 18:00 的工作完成後執行。	`Yes`，可在目前的掃描仍在執行時，將排程掃描工作加入佇列。 `No`（預設值），即使目前的掃描仍在執行，也會執行排程掃描工作。

設定	描述	參數值
ActionOnThreat	選取應用程式對感染物件執行的動作。	DisinfectDeleteIfNotPossible（解毒；如果不能解毒則刪除）表示應用程式會先將物件副本儲存在備份中，隨後嘗試對感染物件解毒。如果無法進行解毒（例如，如果無法對該類型的物件或該物件中的威脅類型解毒），則應用程式將刪除感染物件。 DisinfectInformIfNotPossible（解毒；如果無法解毒則告知）表示應用程式會先將物件副本儲存在備份中，隨後嘗試對感染物件解毒。如果無法進行解毒（例如，如果無法解毒該類型的物件或該物件中的威脅類型），則應用程式會在日誌中建立記錄。 Inform 表示應用程式不會嘗試解毒或刪除感染物件。會記錄關於感染物件的資訊。 預設值：DisinfectDeleteIfNotPossible。
UseExcludeMasks	允許從掃描中排除由ExcludeMasks.item_#設定指定的物件。	Yes — 從掃描中排除ExcludeMasks.item_#設定指定的物件。 No（預設值）— 不從掃描中排除ExcludeMasks.item_#設定指定的物件。
ExcludeMasks.item_#	按名稱或遮罩排除掃描物件。您可以使用此設定按名稱從指定的掃描範圍中排除單一檔案，或使用 shell 格式的遮罩一次排除多個檔案。 在為此設定指定值之前，請確保UseExcludeMasks設定已啟用。	預設值未定義。 範例 UseExcludeMasks=Yes ExcludeMasks.item_0000=eicar1.* ExcludeMasks.item_0001=eicar2.*
UseExcludeThreats	啟用從掃描中排除包含 ExcludeThreats.item_# 設定所指定威脅的物件。	Yes — 從掃描中排除包含ExcludeThreats.item_#設定所指定的威脅的物件。 No（預設值）：不從掃描中排除包含ExcludeThreats.item_#設定指定的威脅的物件。
ExcludeThreats.item_#	根據偵測到的威脅名稱從掃描中排除物件。在為此設定指定值之前，請確保UseExcludeThreats設定已啟用。 為了從掃描中排除物件，請指定在此物件中偵測到的威脅的全名 — 包含應用程式判定物件被感染的字串。 例如，您可能正在使用公用程式來獲取關於網路的資訊。為了防止應用程式封鎖它，請將其中包含的威脅的全名新增至排除掃描的威脅清單。 您可以在應用程式記錄或網站https://threats.kaspersky.com 中找到在物件中偵測到的威脅的全名。	設定值區分大小寫。 預設值未定義。 範例 UseExcludeThreats=Yes ExcludeThreats.item_0000=EICAR-Test-* ExcludeThreats.item_0001=?rojan.Linux
UseGlobalExclusions	啟用全域排除進行掃描。	Yes（預設值）— 使用全域排除。 No — 不使用全域排除。
UseOASExclusions	啟用檔案威脅防護排除項目進行掃描。	Yes（預設值）— 使用檔案威脅防護排除項目。 No — 不使用檔案威脅防護排除項目。
ReportCleanObjects	啟用記錄關於應用程式報告未被感染的掃描物件的資訊。 例如，您可以啟用此設定，以確保應用程式掃描了特定物件。	Yes — 記錄關於未感染物件的資訊。 No（預設值）— 不記錄關於未感染物件的資訊。
ReportPackedObjects	啟用記錄關於作為複合物件一部分的掃描物件的資訊。 例如，您可以啟用此設定來確保應用程式已掃描壓縮檔案內的物件。	Yes — 記錄關於壓縮檔案中已掃描物件的資訊。 No（預設值）— 不記錄關於檔案中掃描物件的資訊。
ReportUnprocessedObjects	啟用記錄關於由於某種原因尚未處理的物件的資訊。	Yes — 記錄關於未處理物件的資訊。 No（預設值）— 不記錄關於未處理物件的資訊。

設定	描述	參數值
UseAnalyzer	啟用啟發式分析。 啟發式分析可以幫助應用程式在病毒分析師發現威脅之前就偵測到威脅。	Yes（預設值）— 啟用啟發式分析器。 No — 停用啟發式分析器。
HeuristicLevel	指定啟發式分析級別。 您可以指定啟發式分析級別。啟發式分析級別可設定威脅搜尋的徹底性、作業系統資源的負載和掃描持續時間之間的平衡。啟發式分析級別越高，掃描所需的資源和時間就越多。	Light — 最不徹底的掃描，系統負載最小。 Medium — 中等啟發式分析級別，系統負載平衡。 Deep — 最徹底的掃描，系統負載最大。 Recommended（預設值）— 建議的值。
UseIChecker	啟用 iChecker 技術。	Yes（預設值）— 啟用 iChecker 技術。 No — 停用 iChecker 技術。
DeviceNameMasks.item_#	裝置名稱清單。應用程式將掃描這些裝置的引導磁區。 設定值不能為空。必須指定至少一個裝置名稱遮罩才能執行此工作。	AllObjects — 掃描所有裝置的引導磁區。 <device name mask> – 掃描名稱與指定遮罩相符的裝置的引導磁區。 預設值：/** — 裝置名稱中的任意一組字元，包括 / 字元。
[ScanScope.item_#]部分包含以下設定：		
AreaDesc	掃描範圍的描述，包含關於掃描範圍的附加資訊。使用此設定指定的字串的最大長度為 4096 個字元。	預設值：All objects。 範例 AreaDesc="Mail bases scan"
UseScanArea	啟用指定範圍的掃描。若要執行該工作，請啟用至少一個範圍的掃描。	Yes（預設值）— 掃描指定範圍。 No — 不掃描指定範圍。
AreaMask.item_#	掃描範圍限制。在掃描範圍內，應用程式僅掃描使用 shell 格式的遮罩指定的檔案。 如果未指定此設定，應用程式將掃描掃描範圍內的所有物件。您可以為此設定指定多個值。	預設值為 *（掃描所有物件）。 範例 AreaMask.item_0000=*doc
Path	包含要掃描的物件的目錄的路徑。	<path to local directory> – 掃描指定目錄中的物件。 Shared:NFS — 掃描可透過 NFS 協定存取的裝置檔案系統資源。 Shared:SMB — 掃描可透過 Samba 協定存取的裝置檔案系統資源。 Mounted:NFS — 使用 NFS 協定掃描裝置上安裝的遠端目錄。 Mounted:SMB — 使用 Samba 協定掃描裝置上安裝的遠端目錄。 AllRemoteMounted — 使用 Samba 和 NFS 協定掃描裝置上安裝的所有遠端目錄。 AllShared — 掃描所有可透過 Samba 和 NFS 協定存取的裝置檔案系統資源。 <file system type> – 掃描指定檔案系統裝置的所有資源。
[ExcludedFromScanScope.item_#]部分包含以下設定：		
AreaDesc	掃描排除範圍的描述，包含關於排除掃描範圍的附加資訊。	預設值未定義。
UseScanArea	從掃描中排除指定的掃描範圍。	Yes（預設值）— 排除指定範圍。 No — 不排除指定的範圍。
AreaMask.item_#	掃描排除項目範圍的限制。在排除範圍中，應用程式僅排除使用 shell 格式的遮罩指定的檔案。 如果未指定此設定，應用程式將排除排除範圍內的所有物件。您可以為此設定指定多個值。	預設值：*（排除所有物件）

設定	描述	參數值
Path	包含要排除的物件的目錄的路徑。	`<path to local directory>` – 從掃描中排除指定目錄（包括子目錄）中的物件。您可以使用遮罩來指定路徑。 為了最佳化掃描工作的運行，建議將系統以唯讀模式掛載的快照路徑新增至具有 btrfs 檔案系統且啟用活動快照的系統的排除項目中。例如，對於基於 SUSE/OpenSUSE 的系統，可以新增以下排除 `/.snapshots/*/snapshot/` 。 預設會指定 `/` 路徑。應用程式將本機檔案系統的所有目錄排除在掃描之外。 `Mounted:NFS` — 從掃描中排除使用 NFS 協定掛載在裝置上的遠端目錄。 `Mounted:SMB` — 從掃描中排除使用 Samba 協定安裝在裝置上的遠端目錄。 `AllRemoteMounted` — 從掃描中排除使用 Samba 和 NFS 協定安裝在裝置上的所有遠端目錄。 `<file system type>` – 從掃描中排除指定檔案系統裝置的所有資源。 只有當遠端目錄在工作啟動前安裝時，應用程式才會將其排除在掃描範圍之外。工作啟動後裝載的遠端目錄不會被排除在掃描之外。

實用文章

如何指定遮罩

您可以使用`*`（星號）字元來建立檔案或目錄名稱遮罩。

您可以指示單一`*`字元來表示檔案或目錄名稱中`/`字元前面的任意字元集（包括空集）。例如，`/dir/*/file` 或 `/dir/*/*/file`。

您可以用兩個連續的`*`字元來表示檔案或目錄名稱中的任意一組字元（包括空集和`/`字元）。例如，`/dir/**/file*/` 或 `/dir/file**/`。

`**`遮罩在目錄名稱中只能使用一次。例如，`/dir/**/**/file`是一個不正確的遮罩。

您可以使用單一`?`字元來表示檔案或目錄名稱中的任意一個字元。

卸除式磁碟機掃描工作

在指令列中，您可以使用`Removable_Drives_Scan`磁碟機掃描。

預設情況下，*卸除式磁碟機掃描*不執行。您可以手動啟動和停止此工作。您可以透過編輯此工作的設定來配置掃描設定。

如果工作正在執行，應用程式將監視卸除式磁碟機與裝置的連線，並且當卸除式磁碟機連線時，它會建立並啟動臨時引導磁區掃描工作（`ODS`類型的工作）。此工作無法停止。工作執行完成後，應用程式會自動刪除該工作。

如果您在*卸除式磁碟機掃描*工作設定中啟用了檔案掃描，應用程式也會啟動一個或多個臨時自訂檔案掃描工作（ODS類型的工作）。如有必要，具有管理員權限的使用者可以停止這些工作。

如果修改*卸除式磁碟機掃描*工作設定，新值將不會套用於已在執行的臨時工作。停止*卸除式磁碟機掃描*工作不會停止已在執行的臨時工作。

卸除式磁碟機掃描工作設定

設定	描述	參數值
ScanRemovableDrives	當卸除式媒體連線到裝置時，啟用卸除式媒體的掃描。 此設定不適用於 CD/DVD 光碟機和藍光光碟（請參閱 ScanOpticalDrives 設定）。	DetailedScan。掃描卸除式媒體上的所有檔案（CD/DVD 和藍光光碟除外）。 詳細掃描使用Scan_File工作 (ID: 3) 的 Scan_File 設定執行。 QuickScan。僅掃描卸除式媒體上**特定類型**的檔案（CD/DVD 和藍光光碟除外）。 在卸除式媒體上掃描下列檔案格式：com、exe、sys、prg、bin、bat、cmd、dpl、dll、scr、cpl、ocx、tsp、drv、vxd、pif、lnk、reg、ini、cia、vbs、vbe、js、jse、htm、htt、hhip、aspx、ig、cx、fpm、rtf、shs、dwg、msi、otm、pdf、swf、jpeg、emf、ico、ov?、xl*、xlsb、pp*、md*、sldx、sldm、thmx。 快速掃描使用Critical_Areas_Scan工作 (ID:4) 的 Critical_Areas_Scan 設定執行。 NoScan（預設值）— 當卸除式媒體連線到裝置時不掃描該媒體。
ScanOpticalDrives	當 CD/DVD 光碟機和藍光光碟連線到裝置時，啟用掃描它們。	DetailedScan。掃描 CD/DVD 光碟機和藍光光碟上的所有檔案。 詳細掃描使用Scan_File工作 (ID: 3) 的 Scan_File 設定執行。 QuickScan。僅掃描 CD/DVD 光碟機和藍光光碟上**特定類型**的檔案。 在卸除式媒體上掃描下列檔案格式：com、exe、sys、prg、bin、bat、cmd、dpl、dll、scr、cpl、ocx、tsp、drv、vxd、pif、lnk、reg、ini、cia、vbs、vbe、js、jse、htm、htt、hhip、aspx、ig、cx、fpm、rtf、shs、dwg、msi、otm、pdf、swf、jpeg、emf、ico、ov?、xl*、xlsb、pp*、md*、sldx、sldm、thmx。 快速掃描使用Critical_Areas_Scan工作 (ID:4) 的 Critical_Areas_Scan 設定執行。 NoScan（預設值）。連接時不掃描 CD/DVD 光碟機和藍光光碟。
BlockDuringScan	啟用掃描期間封鎖連線磁碟上的檔案。掃描引導磁區時，檔案不會被封鎖。	Yes — 掃描期間封鎖檔案。 No（預設值）— 掃描期間不封鎖檔案。

容器掃描

在指令列上，您可以透過以下方式掃描容器和映像：

- 使用容器掃描預定義工作（Container_Scan）。您可以手動啟動或停止此工作，以及設定工作排程。您可以透過編輯此工作的設定來配置掃描設定。
- 使用容器掃描使用者工作（ContainerScan 類型的工作）。您可以手動啟動和停止使用者工作，以及設定工作排程。
- 使用以下指令，您可以對指定的容器和映像執行*自訂掃描*：

```
kesl-control --scan-container
```

容器掃描設定

下表說明在即時掃描命名空間和容器時使用的容器掃描設定。

一般容器和命名空間掃描設定

設定	描述	參數值
OnAccessContainerScanAction	當偵測到受感染物件時對容器執行的操作。 在支援此功能的產品授權下使用應用程式時，此設定可用。 掃描容器內的物件時使用檔案威脅防護工作設定。	StopContainerIfFailed（預設值）— 如果無法解毒或刪除受感染的物件，則停止容器。若指定了此值，則對容器執行的動作也取決於檔案威脅防護工作的 ActionOnThreat 設定。如果將 ActionOnThreat 設定為 DisinfectDeleteIfNotPossible，且應用程式在執行動作時無法解毒或刪除感染物件，則容器將停止。 StopContainer — 當偵測到感染物件時停止容器。 Skip — 當偵測到感染物件時，不對容器執行任何操作。
UseDocker	使用 Docker 容器管理系統。	Yes（預設）啟用 Docker 容器管理系統。 No 停用 Docker 容器管理系統。
DockerSocket	Docker 通訊端路徑或 URI（通用資源識別碼）。	預設值：/var/run/docker.sock。
UseCrio	使用 CRI-O 環境。	Yes（預設值）— 使用 CRI-O 環境。 No — 不使用 CRI-O 環境。
CrioConfigFilePath	CRI-O 設定檔的路徑。	預設值：/etc/crio/crio.conf。
UsePodman	使用 Podman 實用程式。	Yes（預設值）— 使用 Podman 實用程式。 No — 不使用 Podman 實用程式。
PodmanBinaryPath	Podman 實用程式可執行檔的路徑。	預設值：/usr/bin/podman。
PodmanRootFolder	容器儲存的根目錄路徑。	預設值：/var/lib/containers/storage。
UseRunc	使用 runc 實用程式。	Yes（預設值）— 使用 runc 實用程式。 No ：不使用 runc 實用程式。
RuncBinaryPath	runc 實用程式可執行檔的路徑。	預設值：/usr/bin/runc。
RuncRootFolder	容器狀態儲存的根目錄路徑。	預設值：/run/runc。

容器掃描工作

此表格說明您可以為容器掃描工作 (Container_Scan) 指定的所有設定之可用值和預設值。

容器掃描工作設定

設定	描述	參數值
ScanContainers	透過遮罩指定的容器掃描 您可以使用 ContainerNameMask 設定指定遮罩。	Yes（預設值）— 掃描由遮罩定義的容器。 No — 不掃描遮罩定義的容器。
ContainerNameMask	指定定義要掃描的容器的名稱或名稱遮罩。 遮罩以指令 shell 格式指定。您可以使用 ? 和 * 符號。 指定此設定之前，請確保 ScanContainers=Yes 。	預設值：*（掃描所有容器）。 對名為 my_container 的容器執行容器掃描的範例 ContainerNameMask=my_container 掃描名稱以 my_container 開頭之所有容器的範例 ContainerNameMask=my_container* 對名稱以 my_ 開頭、接著包含任意五個字元、再接著是 _container，並以任意字元序列結尾的所有容器執行容器掃描的範例 ContainerNameMask=my_?????_container*

設定	描述	參數值
ScanImages	透過遮罩指定的映像掃描 您可以使用 ImageNameMask 設定指定遮罩。	Yes (預設值) — 掃描由遮罩定義的映像。 No — 不掃描遮罩定義的映像。
ImageNameMask	指定定義要掃描的映像的名稱或名稱遮罩。 指定此設定之前，請確保 ScanImages 設定已設為 Yes 。 遮罩以指令 shell 格式指定。 如果要指定多個遮罩，則每個遮罩必須在新行上使用新索引指定。	預設值：*（掃描所有映像）。 對名稱為 "my_image" 且標籤為 "latest" 的映像執行映像掃描的範例 ImageNameMask=my_image:latest 對名稱以 my_image_ 開頭且具有任意標籤的所有映像執行映像掃描的範例 ImageNameMask=my_image*
DeepScan	檢查所有映像層和正在執行的容器。	Yes — 掃描所有層。 No（預設值）— 不掃描任何層。
ContainerScanAction	當偵測到受感染物件時對容器執行的操作。下面描述了對容器內受感染物件的操作。	StopContainerIfFailed（預設值）— 如果無法解毒或刪除受感染的物件，應用程式將停止容器。如果選取此值，則對容器執行的動作還取決於 ActionOnThreat 設定，該設定適用於容器和映像內的物件（請參閱下表）。如果將 ActionOnThreat 設定為 DisinfectDeleteIfNotPossible，且應用程式在執行動作時無法解毒或刪除感染物件，則容器將停止。 由於 CRI-O 環境的工作方式，感染物件不會在 CRI-O 環境中的容器中被解毒或刪除。建議選擇 StopContainer 動作。 StopContainer — 當偵測到感染物件時，應用程式將停止容器。 Skip — 當偵測到感染物件時，應用程式不對容器執行任何操作。
ImageAction	指定偵測到受感染物件時對映像執行的操作。下面描述了對映像內受感染物件的操作。	Skip（預設值）— 當偵測到感染物件時，應用程式不會對映像執行任何操作。 Delete — 當偵測到感染物件時，應用程式將刪除映像（不建議）。 所有相依性也將被刪除。正在執行的容器將被停止，然後被刪除。

下面所述的設定適用於容器和映像內的物件。

容器掃描工作設定

設定	描述	參數值
ScanArchived	啟用壓縮檔案掃描（包括 SFX 自解壓縮檔案）。 應用程式掃描以下壓縮檔案：.zip；.7z*；.7-z；.rar；.iso；.cab；.bz；.bz2；.tbz；.tbz2；.gz；.tgz；.arj。支援的壓縮檔案格式清單取決於所使用的應用程式資料庫。	Yes（預設值）— 掃描壓縮檔案。 如果將 ActionOnThreat 設定為 DisinfectDeleteIfNotPossible，並且無法解毒，則應用程式會根據壓縮檔案類型，刪除感染物件或包含威脅的整個壓縮檔案。 No — 不掃描壓縮檔案。
ScanSfxArchived	僅啟用對自解壓縮檔案（包含可執行解壓縮模組的壓縮檔案）的掃描。	Yes（預設值）— 掃描自解壓縮檔案。 No — 不掃描自解壓縮檔案。
ScanMailBases	啟用掃描 Microsoft Outlook、Outlook Express、The Bat 和其他郵件用戶端的電子郵件資料庫。	Yes — 掃描電子郵件資料庫的檔案。 No（預設值）— 不掃描電子郵件資料庫的檔案。
ScanPlainMail	啟用純文字電子郵件訊息的掃描。	Yes — 掃描純文字電子郵件。 No（預設值）— 不掃描純文字電子郵件。
TimeLimit	最大物件掃描持續時間（以秒為單位）。如果掃描時間超過此設定指定的時間，應用程式將停止掃描物件。	0 至 9999 0 — 物件掃描時間不受限制。 預設值：0。

設定	描述	參數值
SizeLimit	要掃描的物件的最大大小（以兆位元組為單位）。如果要掃描的物件大於指定值，應用程式將跳過該物件。	0 至 999999 0 — 應用程式可掃描任意大小的物件。 預設值：0。
ActionOnThreat	選取應用程式對感染物件執行的動作。	DisinfectDeleteIfNotPossible（解毒；如果不能解毒則刪除）表示應用程式會先將物件副本儲存在備份中，隨後嘗試對感染物件解毒。如果無法進行解毒（例如，如果無法對該類型的物件或該物件中的威脅類型解毒），則應用程式將刪除感染物件。 DisinfectInformIfNotPossible（解毒；如果無法解毒則告知）表示應用程式會先將物件副本儲存在備份中，隨後嘗試對感染物件解毒。如果無法進行解毒（例如，如果無法解毒該類型的物件或該物件中的威脅類型），則應用程式會在日誌中建立記錄。 Inform 表示應用程式不會嘗試解毒或刪除感染物件。會記錄關於感染物件的資訊。 預設值：DisinfectDeleteIfNotPossible。
UseExcludeMasks	對 ExcludeMasks.item_# 設定指定的物件使用掃描排除項目。	Yes — 從掃描中排除 ExcludeMasks.item_# 設定指定的物件。 No（預設值）— 不從掃描中排除 ExcludeMasks.item_# 設定指定的物件。
ExcludeMasks.item_#	按名稱或遮罩排除掃描物件。您可以使用此設定按名稱從指定的掃描範圍中排除單一檔案，或使用 shell 格式的遮罩一次排除多個檔案。	預設值未定義。 範例 UseExcludeMasks=Yes ExcludeMasks.item_0000=eicar1.* ExcludeMasks.item_0001=eicar2.*
UseExcludeThreats	對包含 ExcludeThreats.item_# 設定所指定的威脅的物件使用掃描排除項目。	Yes — 從掃描中排除包含 ExcludeThreats.item_# 設定所指定的威脅的物件。 No（預設值）：不從掃描中排除包含 ExcludeThreats.item_# 設定指定的威脅的物件。
ExcludeThreats.item_#	根據偵測到的威脅名稱從掃描中排除物件。在為此設定指定值之前，請確保 UseExcludeThreats 設定已啟用。 為了從掃描中排除物件，請指定在此物件中偵測到的威脅的全名 — 包含應用程式判定物件被感染的字串。 例如，您可能正在使用公用程式來獲取關於網路的資訊。為了防止應用程式封鎖它，請將其中包含的威脅的全名新增至排除掃描的威脅清單。 您可以在應用程式記錄或網站https://threats.kaspersky.com 中找到在物件中偵測到的威脅的全名。	設定值區分大小寫。 預設值未定義。 範例 UseExcludeThreats=Yes ExcludeThreats.item_0000=EICAR-Test-* ExcludeThreats.item_0001=?rojan.Linux
UseGlobalExclusions	啟用全域排除進行掃描。	Yes（預設值）— 使用全域排除。 No — 不使用全域排除。
ReportCleanObjects	啟用記錄關於應用程式報告未被感染的掃描物件的資訊。 例如，您可以啟用此設定，以確保應用程式掃描了特定物件。	Yes — 記錄關於未感染物件的資訊。 No（預設值）— 不記錄關於未感染物件的資訊。
ReportPackedObjects	啟用記錄關於作為複合物件一部分的掃描物件的資訊。 例如，您可以啟用此設定來確保應用程式已掃描壓縮檔案內的物件。	Yes — 記錄關於壓縮檔案中已掃描物件的資訊。 No（預設值）— 不記錄關於檔案中掃描物件的資訊。
ReportUnprocessedObjects	啟用記錄關於由於某種原因尚未處理的物件的資訊。	Yes — 記錄關於未處理物件的資訊。 No（預設值）— 不記錄關於未處理物件的資訊。

設定	描述	參數值
`UseAnalyzer`	啟用啟發式分析。 啟發式分析可以幫助應用程式在病毒分析師發現威脅之前就偵測到威脅。	`Yes`（預設值）— 啟用啟發式分析器。 `No` — 停用啟發式分析器。
`HeuristicLevel`	指定啟發式分析級別。 您可以指定啟發式分析級別。啟發式分析級別可設定威脅搜尋的徹底性、作業系統資源的負載和掃描持續時間之間的平衡。啟發式分析級別越高，掃描所需的資源和時間就越多。	`Light` — 最不徹底的掃描，系統負載最小。 `Medium` — 中等啟發式分析級別，系統負載平衡。 `Deep` — 最徹底的掃描，系統負載最大。 `Recommended`（預設值）— 建議的值。
`UseIChecker`	啟用 iChecker 技術。	`Yes`（預設值）— 啟用 iChecker 技術。 `No` — 停用 iChecker 技術。
`QueueScanTasks`	如果先前啟動的排程掃描仍在執行，則延遲排程掃描工作。如果目前的掃描持續執行，Kaspersky Endpoint Security 會將排程掃描工作加入佇列。這將有助於最佳化電腦負載。例如，掃描工作排定在 18:00 和 20:00 執行。如果 18:00 的掃描仍在執行，則排定在 20:00 執行的掃描工作會延遲。延遲的工作會在 18:00 的工作完成後執行。	`Yes`，可在目前的掃描仍在執行時，將排程掃描工作加入佇列。 `No`（預設值），即使目前的掃描仍在執行，也會執行排程掃描工作。

與 Jenkins 整合

Kaspersky Endpoint Security 支援與 Jenkins 整合。Jenkins Pipeline外掛程式可用於掃描不同階段的Docker映像。例如，您可以在開發過程中或發布之前掃描儲存庫中的 Docker 映像。

若要將 Kaspersky Endpoint Security 與 Jenkins 整合：

1. 在 Jenkins 節點上安裝 Kaspersky Endpoint Security。
2. 在 Jenkins 節點上安裝 Docker Engine。
   有關詳細資訊，請參閱Docker Engine 文件。
3. 向 Jenkins 使用者授予 Kaspersky Endpoint Security 管理員權限：

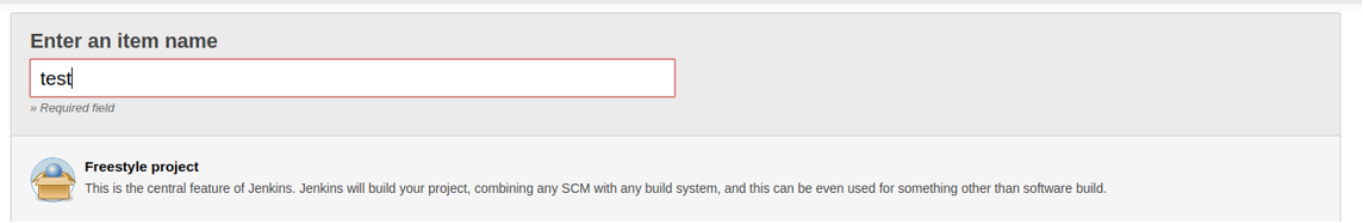
   ```
   kesl-control --grant-role admin <Jenkins user name>
   ```

4. 將 Jenkins 使用者加入 docker 群組：

   ```
   sudo usermod -aG docker <Jenkins user name>
   ```

   通常使用 jenkins 名稱。

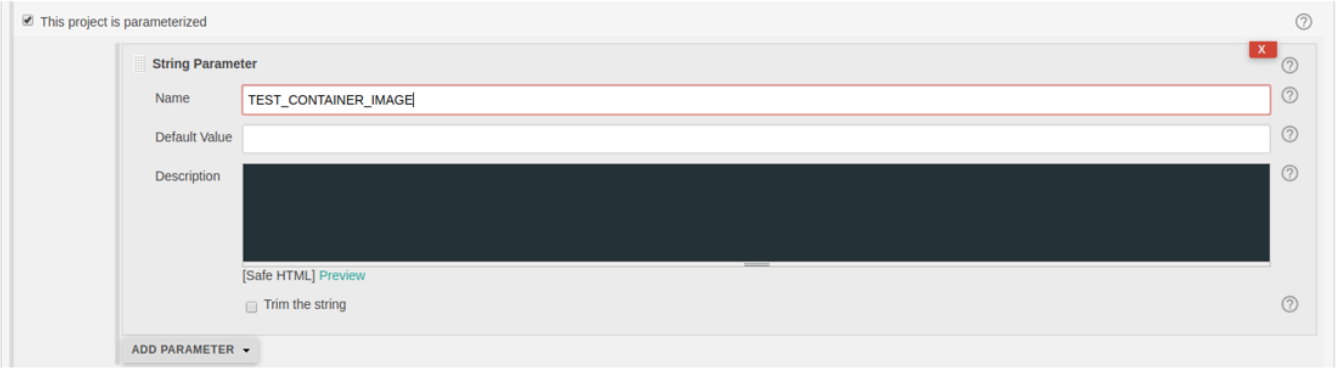
5. 在 Jenkins 中，建立以`test` 名稱命名的新建置作業（**新項目→輸入項目名稱**）。



6. 根據您的需求配置您的專案。假設結果為您有一個需要掃描的映像或已啟動的容器。

7. 若要啟動 Docker 容器，請將下列指令碼新增至 Jenkins 建置處理程序。如果您使用 Jenkins 外掛程式或其他方式啟動 Docker 容器，請將執行中 Docker 容器的 ID 儲存至 /tmp/kesl_cs_info 檔案，以供進一步掃描：

```
TMP_FILE="/tmp/kesl_cs_info"
EXIT_CODE=0
echo "Start container from image: '${TEST_CONTAINER_IMAGE}'"
CONTAINER_ID=$(docker run -d -v /storage:/storage ${TEST_CONTAINER_IMAGE} /storage/docker_process.sh)
if [ -z "${CONTAINER_ID}" ] ; then
echo "Cannot start container from image ${TEST_CONTAINER_IMAGE}"
exit 1
fi
echo "${CONTAINER_ID}" > ${TMP_FILE}
exit ${EXIT_CODE}
```



8. 建置工件後，將以下指令碼新增至建置 jenkins 的步驟中。

   該指令碼支援一個容器進行掃描。如果有必要，請根據您的需求修改指令碼。

```
TMP_FILE="/tmp/kesl_cs_info"
EXIT_CODE=0
if [ ! -f "${TMP_FILE}" ] ; then
echo "Cannot find temporary file with container ID: '${TMP_FILE}'"
exit 1
fi
CONTAINER_ID=$(cat ${TMP_FILE})
if [ -z "${CONTAINER_ID}" ] ; then
echo "Cannot find container ID in the temporary file: '${TMP_FILE}'"
exit 1
fi
echo "Start anti-virus scan for: '${CONTAINER_ID}'"
THREATS_AMOUNT=$(kesl-control --scan-container ${CONTAINER_ID}|grep 'Total detected objects'|awk '{print $5}')
if [ "${THREATS_AMOUNT}" != "0" ] ; then
echo "ATTENTION! ${THREATS_AMOUNT} threats detected at: '${CONTAINER_ID}'"
EXIT_CODE=1
else
echo "Not threats found"
fi
echo "Remove container: {${CONTAINER_ID}}"
docker kill ${CONTAINER_ID}
docker rm -f ${CONTAINER_ID}
rm -f ${TMP_FILE}
```

9. 若要掃描儲存庫中的 Docker 映像，請使用下列指令碼：

```
DOCKER_FILE=https://raw.githubusercontent.com/ianmiell/simple-dockerfile/master/Dockerfile
DOCKER_FILE_FETCHED=$$.Dockerfile
TEST_IMAGE_NAME=test_image
echo "Build image from ${DOCKER_FILE}"
curl ${DOCKER_FILE} -o ${DOCKER_FILE_FETCHED}
if [ -f ${DOCKER_FILE_FETCHED} ] ; then
echo "Dockerfile fetched: ${DOCKER_FILE_FETCHED}"
else
echo "Dockerfile not fetched"
exit 1
fi
docker build -f ${DOCKER_FILE_FETCHED} -t ${TEST_IMAGE_NAME}
echo "Scan docker image"
SCAN_RESULT=$(/opt/kaspersky/kesl/bin/kesl-control --scan-container ${TEST_IMAGE_NAME}*)
echo "Scan done: "
echo $SCAN_RESULT
```

10. 儲存建置作業。

加密軟體防護工作

在指令列中，您可以使用加密軟體防護工作 (`Anti_Cryptor`) 來管理加密軟體防護。

預設情況下，加密軟體防護工作不執行。您可以手動啟動和停止此工作。

您可以透過編輯加密軟體防護預定義工作的設定來配置加密軟體防護設定。

加密軟體防護工作設定

設定	描述	參數值
`ActionOnDetect`	啟用不受信任的主機封鎖。	`Block`（預設值）— 啟用不受信任的主機封鎖。 `Notify`：停用不受信任的主機封鎖。
`BlockTime`	阻止不受信任的裝置的時間（分鐘）。 如果受感染的主機被阻止，並且您變更 `BlockTime` 設定的值，則該主機的封鎖時間將不會改變。封鎖時間不是動態值，是在封鎖的那一刻計算出來的。	從 1 到 4294967295 的整數。 預設值：30。
`UseExcludeMasks`	啟用從防護範圍中排除 `ExcludeMasks.item_#` 設定指定的物件。 僅當指定了 `ExcludeMasks.item_#` 設定時，此設定才適用。	`Yes` — 從防護範圍中排除 `ExcludeMasks.item_#` 設定指定的物件。 `No`（預設值）— 不將 `ExcludeMasks.item_#` 設定指定的物件排除在防護範圍之外。
`ExcludeMasks.item_#`	按名稱或遮罩將物件排除在防護範圍之外。您可以使用此設定按名稱從指定的防護範圍中排除單個檔案，或使用 shell 格式的遮罩同時排除多個檔案。 在為此設定指定值之前，請確保 `UseExcludeMasks` 設定已啟用。 如果要指定多個遮罩，請在新行上使用新索引指定每個遮罩。	預設值未定義。
[ScanScope.item_#]部分包含應用程式防護範圍。對於加密軟體防護工作，您需要指定至少一個防護範圍；您只能指定共用目錄。 您可以以任何順序指定多個 [ScanScope.item_#] 部分。應用程式按索引的升序處理範圍。 [ScanScope.item_#] 部分包含以下設定：		
`AreaDesc`	防護範圍的描述；包含關於防護範圍的附加資訊。	預設值：`All shared directories`。
`UseScanArea`	啟用指定範圍的防護。若要執行該工作，請啟用至少一個範圍的防護。	`Yes`（預設值）— 防護指定範圍。 `No` — 不防護指定範圍。
`AreaMask.item_#`	防護範圍限制。在防護範圍內，應用程式僅防護使用 shell 格式的遮罩指定的物件。 您可以以任意順序指定多個 `AreaMask.item_#` 項目。應用程式按索引的升序處理範圍。	預設值：`*`（防護所有物件）。

設定	描述	參數值
Path	要防護的物件所在的目錄的路徑。	< 本機目錄路徑 > – 防護可透過 SMB/NFS 存取的本機目錄。您可以使用遮罩來指定路徑。 AllShared（預設值）— 防護所有可透過 SMB/NFS 存取的資源。 Shared:SMB – 防護可透過 SMB 存取的資源。 Shared:NFS – 防護可透過 NFS 存取的資源。
[ExcludedFromScanScope.item_#]部分包含要從所有 [ScanScope.item_#] 部分排除的物件。符合任何 [ExcludedFromScanScope.item_#] 部分規則的物件不會被掃描。[ExcludedFromScanScope.item_#] 部分的格式與 [ScanScope.item_#] 部分的格式類似。您可以按任意順序指定多個 [ExcludedFromScanScope.item_#] 部分。應用程式按索引的升序處理範圍。 [ExcludedFromScanScope.item_#] 部分包含以下設定：		
AreaDesc	防護排除範圍的描述，包含關於排除範圍的附加資訊。	預設值：All objects。
UseScanArea	將指定的範圍排除在防護範圍之外。	Yes（預設值）— 將指定範圍排除在防護範圍之外。 No — 不將指定範圍排除在防護範圍之外。
AreaMask.item_#	防護排除範圍的限制。在排除範圍中，應用程式僅排除使用 shell 格式的遮罩指定的物件。 您可以以任意順序指定多個AreaMask.item_#項目。應用程式按索引的升序處理範圍。	預設值：*（排除所有物件）
Path	包含被從防護中排除的物件的目錄路徑。	< 本機目錄路徑 > — 將指定目錄中的物件排除在防護之外。您可以使用遮罩來指定路徑。 Mounted:NFS — 將使用 NFS 協定安裝在用戶端裝置上的遠端目錄排除在防護之外。 Mounted:SMB — 將使用 Samba 協定安裝在用戶端裝置上的遠端目錄排除在防護之外。 AllRemoteMounted — 將使用 Samba 和 NFS 協定安裝在用戶端裝置上的所有遠端目錄排除在防護之外。

實用文章

如何指定遮罩

您可以使用*（星號）字元來建立檔案或目錄名稱遮罩。

您可以指示單一*字元來表示檔案或目錄名稱中/字元前面的任意字元集（包括空集）。例如，/dir/*/file 或 /dir/*/*/file。

您可以用兩個連續的*字元來表示檔案或目錄名稱中的任意一組字元（包括空集和/字元）。例如，/dir/**/file*/ 或 /dir/file**/。

遮罩在目錄名稱中只能使用一次。例如，/dir//**/file是一個不正確的遮罩。

您可以使用單一?字元來表示檔案或目錄名稱中的任意一個字元。

行為偵測工作

您可以使用行為偵測預定義工作（Behavior_Detection），透過指令列管理作業系統中的應用程式行為偵測。

行為偵測工作預設執行。您可以手動啟動和停止工作。

您可以透過編輯行為偵測預定義工作的設定來配置行為偵測。

設定	描述	參數值
UseTrustedPrograms	從掃描中排除處理程序。	Yes – 不掃描所指示處理程序的活動。 No（預設值）– 掃描所有處理程序。
TaskMode	在作業系統中偵測到惡意活動時應用程式執行的操作。	Block（預設值）- 終止執行惡意活動的應用程式的處理程序。 Notify – 不終止執行惡意活動的處理程序；僅在事件日誌中記錄偵測到的惡意活動。
TelemetrySource	與 Detection and Response 解決方案整合時，用於收集發送到此類解決方案的遙測資料的其他設定。 僅當 TelemetrySource 被設定為 Default 時，UseTelemetryMonopolyMode 設定才會套用。	Default（預設）表示使用 eBPF 技術和 auditd 服務來獲取遙測資料。 OnlyEBPF 表示僅使用 eBPF 技術獲取遙測資料。
UseTelemetryMonopolyMode	此設定不適用於配備 Elbrus CPU 的裝置。	True（預設值）表示 Kaspersky Endpoint Security 以獨佔模式使用 auditd 服務。 False 表示 auditd 服務以非獨佔模式使用。
[TrustedPrograms.item_#]部分包含從行為偵測掃描中排除的處理程序。Kaspersky Endpoint Security 不監控指定處理程序的活動。		
ProgramPath	被排除的處理程序的路徑。	< 處理程序的完整路徑 > – 不掃描指定本機目錄中的處理程序。您可以使用遮罩來指定路徑。
ApplyToDescendants	從掃描中排除 ProgramPath 設定指定的排除處理程序的子處理程序。	Yes – 從掃描中排除指定處理程序及其所有子處理程序。 No（預設值）- 僅從掃描中排除指定的處理程序，不從掃描中排除其子處理程序。
ProgramDesc	被排除的處理程序的描述。	
UseTrustedProgram	將指定處理程序的活動排除在掃描之外。	Yes（預設值）– 將指定處理程序的活動排除在掃描之外。 No – 不將指定處理程序的活動排除在掃描之外。
UseTrustedProgramForDetects	將某個處理程序的活動排除在行為偵測掃描之外。	如果設定為 Yes，則指定處理程序的活動會被排除在行為偵測的掃描範圍之外。 如果設定為 No（預設），則指定處理程序的活動不會被排除在行為偵測的掃描範圍之外。
UseTrustedProgramForMDRAndEDR	將此處理程序從 MDR 和 EDR Expert (on-premises) 元件收集的遙測資料中排除。 此設定不適用於配備 Elbrus CPU 的裝置。	Yes – 將此處理程序的活動從 MDR 和 EDR Expert (on-premises) 元件收集的遙測資料中排除。 No（預設值）— 不將此處理程序的活動從遙測資料中排除。

實用文章

如何指定遮罩

您可以使用 * （星號）字元來建立檔案或目錄名稱遮罩。

您可以指示單一 * 字元來表示檔案或目錄名稱中 / 字元前面的任意字元集（包括空集）。例如，/dir/*/file 或 /dir/*/*/file。

您可以用兩個連續的*字元來表示檔案或目錄名稱中的任意一組字元（包括空集和/字元）。例如，/dir/**/file*/ 或 /dir/file**/。

遮罩在目錄名稱中只能使用一次。例如，/dir//**/file是一個不正確的遮罩。

您可以使用單一?字元來表示檔案或目錄名稱中的任意一個字元。

弱點利用防禦

在命令列上，您可以使用行為偵測預定義工作（Behavior_Detection）的設定來管理弱點利用防禦。

您可以透過編輯行為偵測預定義工作的設定來配置弱點利用防禦（請見下表）。

弱點利用防禦設定

設定	描述	參數值
UseAEP	啟用漏洞攻擊防護元件。	Yes 會啟用弱點利用防禦。 No（預設）會停用「漏洞攻擊防護」。
AEPMode	偵測到漏洞攻擊時要採取的動作。	如果設定為 Block（預設），則會封鎖漏洞攻擊惡意活動並記錄事件。 如果設定為 Notify，則不會封鎖漏洞攻擊活動，且只會在事件記錄中記錄關於偵測到的漏洞攻擊的資訊。
[AEPExclusions.item_#]部分包含弱點利用防禦元件的掃描排除項目。		
Enabled	啟用從弱點利用防禦元件的掃描中排除。	Yes（預設值）– 使用弱點利用防禦排除。 No — 不使用弱點利用防禦排除。
DetectName	根據在物件中偵測到的威脅名稱從掃描中排除物件。在為此設定指定值之前，請確保UseDetectName設定已啟用。	為了從掃描中排除物件，請指定在此物件中偵測到的威脅的全名 — 包含應用程式判定物件被感染的字串。 您可以在應用程式記錄或網站https://threats.kaspersky.com 中找到在物件中偵測到的威脅的全名。
Hash	排除在其中透過其雜湊值偵測到威脅的物件。在為此設定指定值之前，請確保UseHash設定已啟用。	
HashType	您想要使用Hash參數來將檔案從掃描中排除的檔案雜湊類型。	Md5 – MD5 雜湊 Sha256 – SHA256 雜湊
Path	排除路徑中偵測到威脅的物件。在為此設定指定值之前，請確保UsePath設定已啟用。	< 檔案或本機目錄的完整路徑 > – 從掃描中排除檔案或指定目錄（包括子目錄）中的物件。您可以在路徑中使用*和?字元。
UseDetectName	啟用從掃描中排除包含 DetectName 設定所指定威脅的物件。	Yes（預設值）— 從掃描中排除包含DetectName 設定所指定的威脅的物件。 No — 不從掃描中排除包含使用DetectName設定指定的威脅的物件
UseHash	透過雜湊值排除偵測到威脅的檔案。檔案雜湊在Hash參數中指定。	Yes（預設值）— 透過雜湊值排除偵測到威脅的檔案。 No — 不透過雜湊值排除偵測到威脅的檔案。
UsePath	依照路徑排除偵測到威脅的檔案。文件路徑使用Path參數指定。	Yes（預設值）— 依照徑排除偵測到威脅的檔案。 No — 不依照路徑排除偵測到威脅的檔案。

使用卡巴斯基安全網路

您可以使用UseKSN中的UseKSN選項在指令列中啟用或停用卡巴斯基安全網路的使用。

您可以使用指令列選項或包含所有一般應用程式設定的設定檔，變更 UseKSN 設定的值。

若要使用指令列開關啟用卡巴斯基安全網路，請執行：

```
kesl-control --set-app-settings UseKSN=<Extended/Basic> --accept-ksn
```

其中：

`<Extended/Basic>`：卡巴斯基安全網路模式。

`--accept-ksn`：一個表示您同意卡巴斯基安全網路聲明條款的選項。您確認已完全閱讀、理解並接受卡巴斯基安全網路聲明的條款和條件。

檔案 ksn_license.<語言 ID> 包含卡巴斯基安全網路聲明文字，位於目錄 /opt/kaspersky/kesl/doc/ 中。

若要使用指令列開關停用卡巴斯基安全網路，請執行：

```
kesl-control --set-app-settings UseKSN=No
```

若要使用設定檔啟用或停用卡巴斯基安全網路，請執行以下命令：

```
kesl-control --set-app-settings --file <path to the configuration file> [--json] [--accept-ksn]
```

其中：

`--file <path to the configuration file>` 是包含一般應用程式設定的設定檔完整路徑，其中已設定所需的 `UseKSN` 值。

如果要從 JSON 設定檔匯入設定，請指定`--json`選項。如果未指定`--json`選項，應用程式將嘗試從 INI 檔案匯入。如果匯入失敗，則會顯示錯誤。

`--accept-ksn`：一個表示您同意卡巴斯基安全網路聲明條款的選項。如果您要啟用卡巴斯基安全網路，則必須指定該選項。

如果用戶端裝置上安裝的 Kaspersky Endpoint Security 依照卡巴斯基安全管理中心政策執行，則只能使用卡巴斯基安全管理中心修改 `UseKSN` 設定的值。當用戶端裝置上安裝的 Kaspersky Endpoint Security 依照政策停止執行時，將為該設定指派以下值：`UseKSN=No`。

連線到卡巴斯基安全網路

若要檢查與卡巴斯基安全網路的連線，請執行以下命令：

```
kesl-control --app-info
```

使用卡巴斯基安全網路行顯示與卡巴斯基安全網路的連線狀態：

- 如果顯示 *延伸 KSN 模式* 狀態，Kaspersky Endpoint Security 將使用卡巴斯基安全網路，可從知識庫取得資訊，並傳送匿名統計資訊以及關於威脅類型和來源的資訊。
- 如果顯示 *基本 KSN 模式* 狀態，Kaspersky Endpoint Security 將使用卡巴斯基安全網路，且可從知識庫取得資訊，但不會傳送匿名統計資訊以及關於威脅類型和來源的資訊。
- 如果顯示 *KSN 未使用* 狀態，Kaspersky Endpoint Security 不使用卡巴斯基安全網路。

卡巴斯基安全網路基礎設施 列會顯示關於用於與卡巴斯基信譽資料庫搭配使用的基礎設施解決方案的資訊：*KSN* 或 *KPSN*。

由於以下原因，可能無法連線卡巴斯基安全網路：

- 使用者裝置未連線至網際網路。
- 卡巴斯基安全網路的使用已被停用。
- 應用程式尚未啟動或產品授權已過期。
- 偵測到與產品授權金鑰相關的問題。例如，金鑰在拒絕清單中。

啟用或停用雲端模式

*雲端模式*是Kaspersky Endpoint Security的操作模式，使用輕量級版本的惡意軟體資料庫。

> 如果在用於防護虛擬環境的 Light Agent 模式下使用 Kaspersky Endpoint Security，則不支援使用輕量型惡意軟體資料庫。應用程式從 Protection Server 接收 Light Agent 操作所需的特殊資料庫。

您可以在一般應用程式設定中借助`CloudMode=Yes/No`選項在指令列中啟用或停用雲端模式。

您可以使用包含所有一般應用程式設定的設定檔，或使用命令列選項來變更 `CloudMode` 設定。

> 如果卡巴斯基安全網路已啟用，則可以使用雲端模式。

BadUSB 攻擊防護工作

在命令列中，您也可以使用 BadUSB 攻擊防護預先定義工作 (`Bad_USB`) 來管理 BadUSB 攻擊防護。

BadUSB 攻擊防護工作預設不啟動。您可以手動啟動和停止此工作。

> 從指令列啟動和停止 BadUSB 攻擊防護工作需要管理員角色權限。

您可以透過編輯BadUSB 攻擊防護預定義工作的設定來管理 BadUSB 攻擊防護設定。

下表描述了您可以為 BadUSB 攻擊防護工作指定的設定的可用值和預設值。

BadUSB 攻擊防護工作設定

設定	描述	參數值
`MaxAuthAttempts`	USB 裝置授權嘗試的最多次數，此後應用程式將封鎖 USB 裝置和對 USB 裝置繼續進行的授權嘗試，封鎖時長在 `TimeoutAfterAttempts` 參數中指定。	可選值：1 到 10 預設值：5。
`TimeoutAfterAttempts`	嘗試輸入授權碼失敗達到`MaxAuthAttempts` 次後封鎖 USB 裝置的持續時間。	可選值：1 到 180 分鐘。預設值：5分鐘。

設定	描述	參數值
ProhibitOnScreenKeyboard	禁止或允許使用螢幕鍵盤授權 USB 裝置。	如果設定為 Yes，則應用程式不允許使用螢幕鍵盤對無法用來輸入授權碼的 USB 裝置進行鍵盤授權。 如果設定為 No，則應用程式允許使用螢幕鍵盤對無法用來輸入授權碼的 USB 裝置進行鍵盤授權。
ProhibitBarcodeScanner	啟用或停用將授權碼顯示為條碼，以便授權無法輸入授權碼的 USB 裝置。	Yes（預設）禁止將授權碼顯示為條碼。 No 允許將授權碼顯示為條碼。

通訊與 Web 防護

Web 威脅防護工作

在指令列中，您可以使用 Web 威脅防護預先定義工作（Web_Threat_Protection）來管理 Web 威脅防護。

如果在系統中偵測到其中一個受支援的瀏覽器並且允許在裝置上本機管理 Web 威脅防護設定（未套用政策或未在政策屬性中設定"鎖定"），則該工作會自動啟動。您可以手動啟動和停止工作。

您可以透過編輯Web 威脅防護預定義工作的設定來配置 Web 威脅防護設定。

Web 威脅防護工作設定

設定	描述	參數值
ActionOnDetect	指定在 Web 流量中偵測到受感染物件時要執行的操作。	Notify — 允許下載偵測到的物件、顯示封鎖存取嘗試的通知並記錄關於受感染物件的資訊。 Block（預設值）— 阻止對偵測到的物件進行存取、顯示關於被阻止存取嘗試的通知並記錄關於受感染物件的資訊。
CheckMalicious	針對惡意網址資料庫檢查連結。	Yes（預設值）— 檢查連結是否列在惡意連結資料庫中。 No — 不檢查連結是否列在惡意連結資料庫中。
CheckPhishing	針對網路釣魚網址資料庫檢查連結。	Yes（預設值）— 檢查連結是否列在網路釣魚連結資料庫中。 No — 不檢查連結是否列在網路釣魚連結資料庫中。
UseHeuristicForPhishing	使用啟發式分析掃描網頁中的釣魚連結。 此設定不適用於配備 Elbrus CPU 的裝置。	Yes（預設值）— 使用啟發式分析來偵測釣魚連結。如果指定了此值，則啟發式分析的等級為 Light（最不徹底的掃描，系統負載最小）。您無法變更 Web 威脅防護工作的啟發式分析等級。 No — 不要使用啟發式分析來偵測釣魚連結。
CheckAdware	根據廣告網址資料庫檢查連結。	Yes — 檢查連結是否列在廣告軟體連結資料庫中。 No（預設值）— 不檢查連結是否列在廣告軟體連結資料庫中。
CheckOther	根據包含入侵者可以利用的合法應用程式的網址資料庫檢查連結，這些應用程式可能會用來入侵裝置或資料。	Yes — 檢查這些連結是否列在包含合法應用程式的網址資料庫中，這些應用程式可能會被入侵者用來損壞您的裝置或資料。 No（預設值）— 不檢查連結是否列在包含會被入侵者用來損壞您的裝置或資料的合法應用程式的網址資料庫中。
UseTrustedAddresses	使用受信任網址清單。應用程式不掃描受信任的網址以查找病毒或其他惡意物件。您可以使用 TrustedAddresses.item_# 設定指定受信任的網址。	Yes（預設值）— 使用受信任的網址清單。 No — 不使用受信任網址清單。

設定	描述	參數值
`TrustedAddresses.item_#`	指定受信任的網址。	預設值未定義。 您可以使用遮罩來指定網址。 不支援使用遮罩指定 IP 位址。

實用文章

如何指定遮罩

建立位址遮罩時，使用星號 (*) 作為一個或多個字元的佔位符。如果輸入 *abc* 位址遮罩，它將套用於所有包含 “abc”序列的 Web 資源（例如，www.virus.com/download_virus/page_0-9abcdef.html）。若要將星號作為字元包含在位址遮罩中，但不作為遮罩，請輸入兩次 * 字元（例如，www.virus.com/**/page_0-9abcdef.html 表示 www.virus.com/*/page_0-9abcdef.html）。

掃描網路流量

在命令列上，您可以使用特殊的管理命令來管理網路流量掃描設定。您可以使用網路流量掃描設定管理命令來執行下列操作：

- 管理網路流量掃描設定。
- 檢視加密連線掃描的排除項目。
- 清除應用程式自動從掃描中排除的網域清單。
- 配置應用程式在掃描加密連線時使用的受信任根憑證清單。
- 設定與檢視流量攔截排除項目。

檢視和編輯網路流量掃描設定

您可以使用特殊的網路流量掃描設定管理指令來：

- 將網路流量掃描設定的目前值輸出到主控台或設定檔。您可以使用此檔案來編輯設定。
- 使用設定檔管理所有網路流量掃描設定。您可以獲取一個設定檔，可以使用顯示網路流量掃描設定輸出命令對其進行編輯。
- 使用格式為 < 設定名稱 >=< 設定值 > 的命令列選項編輯個別設定。您可以使用用於顯示網路流量掃描設定的指令來取得設定的目前值。

若要將目前的網路流量掃描設定輸出到主控台，請執行下列指令：

```
kesl-control --get-net-settings [--json]
```

其中，指定 `--json` 以 JSON 格式輸出設定。如果沒有指定 `--json` 選項，則設定以 INI 格式輸出。

若要將目前網路流量掃描設定輸出到檔案，請執行以下命令：

```
kesl-control --get-net-settings --file <path to configuration file> [--json]
```

其中：

- `--file <path to the configuration file>` 是將儲存網路流量掃描設定的檔案路徑。如果指定檔案的名稱而不指定其路徑，則該檔案會在目前目錄中建立。如果指定路徑中已經存在指定名稱的檔案，則該檔案將被覆寫。如果在磁碟上找不到指定的目錄，則不會建立檔案。
- `--json` 被指定以 JSON 格式輸出設定。如果沒有指定 `--json` 選項，則設定以 INI 格式輸出。

若要使用設定檔管理網路掃描設定：

1. 將網路流量掃描設定輸出到設定檔，如上所述。
2. 編輯檔案中必要參數的值並儲存變更。
3. 執行以下指令：

   ```
   kesl-control --set-net-settings --file <path to the configuration file> [--json]
   ```

   其中：

   - `--file <path to the configuration file>` 是包含網路流量掃描設定之設定檔的完整路徑。
   - `--json` 用於以 JSON 格式將設定從設定檔匯入應用程式。如果未指定 `--json` 選項，應用程式將嘗試從 INI 檔案匯入。如果匯入失敗，則會顯示錯誤。

   檔案中配置的所有網路流量掃描設定都會被匯入應用程式。

若要在命令列上編輯網路流量掃描設定，請執行以下命令：

```
kesl-control --set-net-settings <parameter name>=<parameter value> [<parameter name>=<parameter value>]
```

其中 `<parameter name>=<parameter value>` 是 網路流量掃描設定的名稱和值。

指定設定的值已被修改。

檢視加密連線掃描的排除項目

您可以檢視加密連線掃描的以下排除項目清單：

- 使用者新增的排除項目清單；
- 應用程式新增的排除項目清單；
- 從應用程式資料庫收到的排除項目清單。

若要檢視使用者新增的加密連線掃描排除項目清單，請執行下列指令：

```
kesl-control -N --query user
```

若要檢視使用者新增的加密連線掃描排除項目清單，請執行下列指令：

```
kesl-control -N --query auto
```

若要檢視從應用程式資料庫收到的加密連線掃描排除項目清單，請執行下列指令：

```
kesl-control -N --query kl
```

若要清除應用程式自動排除在掃描之外的網域清單，請執行下列指令：

```
kesl-control [-N] --clear-web-auto-excluded
```

管理受信任的根憑證清單

若要將憑證新增至受信任的根憑證清單，請執行以下指令：

```
kesl-control --add-certificate <path to the certificate>
```

其中：

`<path to the certificate>` 是您要新增之憑證檔案的路徑（PEM 或 DER 格式）。

若要從受信任的根憑證清單中刪除憑證，請執行以下指令：

```
kesl-control --remove-certificate <subject of the certificate>
```

若要檢視受信任的根憑證清單，請執行下列指令：

```
kesl-control --list-certificates
```

每個憑證都會顯示以下資訊：

- 憑證主體
- 序號
- 憑證發佈者
- 憑證開始日期

- 憑證到期日期
- SHA256 憑證指紋

設定與檢視流量攔截排除項目

若要新增流量攔截排除項目，請執行以下命令：

```
kesl-control --add-bypass-endpoints --direction <in|out> --remote-ip <remote IP address> --dst-port <destination port>
```

其中：

- `<in|out>` 是排除連線中的流量方向。您可以為輸入流量或輸出流量設定排除項目。
- `<remote IP address>` 是遠端裝置的 IPv4 或 IPv6 位址。依流量方向而定，來自指定 IP 位址的流量（輸入流量排除）或傳送至指定 IP 位址的流量（輸出流量排除）將被排除。
- `<destination port>` 視流量方向而定：
  - 受防護裝置上的連接埠（輸入流量排除）。從遠端裝置傳送至該連接埠的流量將排除於攔截範圍外。
  - 遠端裝置上的連接埠（輸出流量排除）。從受防護裝置傳送至該連接埠的流量將排除於攔截範圍外。

在排除項目中，您可以指定不含連接埠的遠端裝置 IP 位址或不含 IP 位址的目的地連接埠。

> 如果在輸入流量排除規則中僅指定遠端裝置的 IP 位址（未指定受防護裝置上的連接埠），則來自遠端裝置的所有流量都將排除於攔截範圍外。建議僅為受信任裝置的流量設定此排除規則。

若要檢視已設定的流量攔截排除項目清單，請執行以下命令：

```
kesl-control --list-bypass-endpoints
```

每個排除項目都會顯示以下資訊：

- 排除項目序號
- 流量方向
- 遠端裝置的 IP 位址
- 連接埠編號

若要刪除流量攔截排除項目，請執行以下命令：

```
kesl-control --remove-bypass-endpoints --direction <in|out> --remote-ip <remote IP address> --dst-port <destination port>
```

其中：

- `<in|out>` 是排除連線中的流量方向。
- `<remote IP address` 是遠端裝置的 IPv4 或 IPv6 位址，其流量會排除在攔截之外（視流量方向而定）。
- `<destination port>` 是受保護裝置上的連接埠（傳入流量的排除）或遠端裝置上的連接埠（傳出流量的排除）。

網路威脅防護工作

在指令列中，您可以使用網路威脅防護預定義工作 (`Network_Threat_Protection`) 來管理網路威脅防護。

預設情況下，網路威脅防護工作不執行。您可以手動啟動和停止工作。

您可以透過編輯網路威脅防護預定義工作的設定來配置網路威脅防護設定。

網路威脅防護工作設定

設定	描述	參數值
`ActionOnDetect`	偵測到典型的網路攻擊型網路活動時執行的動作。 將此設定的值從 `Block` 變更為 `Notify` 將清除被封鎖裝置的清單。	`Notify` — 允許網路活動，記錄關於偵測到的網路活動的資訊。如果指定了此值，則會忽略 `BlockAttackingHosts` 參數的值。 `Block`（預設值）— 阻止網路活動並記錄關於它的資訊。
`BlockAttackingHosts`	封鎖攻擊者裝置的網路活動。	`Yes`（預設值）— 封鎖攻擊者裝置的網路活動。 `No` — 不封鎖攻擊者裝置的網路活動。如果指定此值並將 `ActionOnDetect` 參數設為 `Block`，則應用程式將封鎖來自攻擊者裝置的網路活動，但不會將該裝置新增至被封鎖裝置的清單。
`BlockDurationMinutes`	指定封鎖攻擊裝置的時長（以分鐘為單位）。	1 至 32768 預設值：60。
`UseExcludeIPs`	使用 IP 位址清單，當偵測到網路攻擊時，其網路活動不會被封鎖。應用程式將僅記錄關於這些裝置的危險活動的資訊。 您可以使用 `ExcludeIPs.item_#` 設定將 IP 位址新增至排除項目清單。	`Yes` — 使用排除的 IP 位址清單。 `No`（預設值）— 不使用排除的 IP 位址清單。
`ExcludeIPs.item_#`	指定應用程式不會封鎖其網路活動的 IP 位址。此清單預設會空白。	`d.d.d.d` — IPv4 位址，其中 d 是 0 至 255 之間的十進位數。 `d.d.d.d/p` — IPv4 位址的子網路，其中 p 是 0 到 32 之間的數字。 `x:x:x:x:x:x:x:x` — IPv6 位址，其中 x 是 0 到 ffff 的十六進位數。 `x:x:x:x::0/p` — IPv6 位址的子網路，其中 p 是 0 到 64 之間的數字。 預設值未定義。

防火牆管理

在指令列中，您可以使用防火牆管理預定義工作（`Firewall_Management`）設定防火牆管理。

預設情況下，防火牆管理工作不執行。您可以手動啟動和停止此工作。

您可以透過編輯防火牆管理預定義工作的設定來配置防火牆管理設定。

您也可以使用防火牆管理指令配置防火牆管理設定：

- 建立和刪除網路封包規則並更改其執行優先順序。
- 建立網路區域中的 IP 位址或子網路清單。
- 使用以下指令檢視在應用程式中建立的防火牆規則：

```
kesl-control -F --query
```

防火牆管理工作設定

設定	描述	參數值
DefaultIncomingAction	如果沒有網路規則適用於此連線類型，則對入站連線執行的預設操作。	Allow（預設值）— 允許入站連線。 Block — 封鎖入站連線。
DefaultIncomingPacketAction	如果沒有網路封包規則適用於此連線類型，則對傳入封包執行的預設操作。	Allow（預設值）— 允許傳入封包。 Block — 封鎖傳入封包。
OpenNagentPorts	將網路代理動態規則新增至網路封包規則。	Yes（預設值）– 將網路代理動態規則新增到網路封包規則中。 No – 不將網路代理動態規則新增至網路封包規則。
[PacketRules.item_#]部分包含防火牆管理工作的網路封包規則。您可以以任意順序指定多個 [PacketRules.item_#] 部分。應用程式按索引的升序處理範圍。 每個 [PacketRules.item_#] 部分包含以下設定：		
Name	網路封包規則名稱。	預設值：Packet rule #<n>，其中 n 是索引。
FirewallAction	對此網路封包規則中指定的連線執行的操作。	Allow（預設值）— 允許網路連線。 Block — 封鎖網路連線。
Protocol	需要監控網路活動的協定類型。	Any（預設值）— 防火牆管理工作監控所有網路活動。 TCP UDP ICMP ICMPv6 IGMP GRE
RemotePorts	受監控的遠端裝置的連線埠號。可以為此值指定一個整數或間隔。 僅當 Protocol 設定被設為 TCP 或 UDP 時才指定此設定。	Any（預設值）— 監控所有遠端連接埠。 0 – 65535.
LocalPorts	連線受監控的本機裝置的連接埠號。可以為此值指定一個整數或間隔。 僅當 Protocol 設定被設為 TCP 或 UDP 時才指定此設定。	Any（預設值）— 監控所有本機連接埠。 0 – 65535.
ICMPType	ICMP 封包類型。 僅當 Protocol 設定被設為 ICMP 或 ICMPv6 時才指定此設定。	Any（預設值）— 監控所有 ICMP 封包類型。 符合資料傳輸協定規範的整數。
ICMPCode	ICMP 封包代碼。 僅當 Protocol 設定被設為 ICMP 或 ICMPv6 時才指定此設定。	Any（預設值）— 監控所有 ICMP 封包代碼。 符合資料傳輸協定規範的整數。

設定	描述	參數值
Direction	受監控網路活動的指引。	IncomingOutgoing 或 InOut（預設值）— 監控入站與出站連線。 Incoming 或 In — 僅監控入站連線。 Outgoing 或 Out — 僅監控出站連線。 IncomingPacket 或 InPacket — 僅監控傳入封包。 OutgoingPacket 或 OutPacket — 僅監控傳出的封包。 IncomingOutgoingPacket 或 InOutPacket — 監控傳入和傳出的封包。
RemoteAddress	可以傳送和接收網路封包的遠端裝置的網路位址。	Any（預設值）— 監控具有任意 IP 位址的遠端裝置傳送和/或接收的網路封包。 Trusted — 可信任網路的預定義網路區域。 Local — 本機網路的預定義網路區域。 Public — 公共網路的預定義網路區域。 d.d.d.d — IPv4 位址，其中 d 是 0 至 255 之間的十進位數。 d.d.d.d – d.d.d.d — IPv4 位址範圍。 d.d.d.d/p — IPv4 位址的子網路，其中 p 是 0 到 32 之間的數字。 x:x:x:x:x:x:x:x — IPv6 位址，其中 x 是 0 到 ffff 的十六進位數。 x:x:x:x:x:x:x:x – x:x:x:x:x:x:x:x — IPv6 位址範圍。 x:x:x:x:x:x:x:x/p — IPv6 位址子網路，其中 p 是 0 到 128 之間的數字；為簡潔起見，您可以使用::。
LocalAddress	安裝了 Kaspersky Endpoint Security 並可以傳送和/或接收網路封包的裝置的網路位址。	Any（預設值）— 監控具有任意 IP 位址的本機裝置所傳送和/或接收的網路封包。 d.d.d.d — IPv4 位址，其中 d 是 0 至 255 之間的十進位數。 d.d.d.d – d.d.d.d — IPv4 位址範圍。 d.d.d.d/p — IPv4 位址的子網路，其中 p 是 0 到 32 之間的數字。 x:x:x:x:x:x:x:x — IPv6 位址，其中 x 是 0 到 ffff 的十六進位數。 x:x:x:x:x:x:x:x – x:x:x:x:x:x:x:x — IPv6 位址範圍。 x:x:x:x:x:x:x:x/p — IPv6 位址子網路，其中 p 是 0 到 128 之間的數字；為簡潔起見，您可以使用::。
LogAttempts	在報告中包含網路規則操作的記錄。	Yes — 在報告中記錄操作。 No（預設值）- 不在報告中寫入操作。
[NetworkZonesPublic]部分包含與公共網路相關的網路位址。您可以指定多個 IP 位址或 IP 位址子網路。		
Address.item_#	指定 IP 位址或 IP 位址的子網路。	d.d.d.d — IPv4 位址，其中 d 是 0 至 255 之間的十進位數。 d.d.d.d/p — IPv4 位址的子網路，其中 p 是 0 到 32 之間的數字。 x:x:x:x:x:x:x:x — IPv6 位址，其中 x 是 0 到 ffff 的十六進位數。 x:x:x:x::0/p — IPv6 位址的子網路，其中 p 是 0 到 64 之間的數字。 預設值：""（此區域中沒有網路位址）
[NetworkZonesLocal]部分包含與本機網路相關的網路位址。您可以指定多個 IP 位址或 IP 位址子網路。		

設定	描述	參數值
`Address.item_#`	指定 IP 位址或 IP 位址的子網路。	`d.d.d.d` — IPv4 位址，其中 d 是 0 至 255 之間的十進位數。 `d.d.d.d/p` — IPv4 位址的子網路，其中 p 是 0 到 32 之間的數字。 `x:x:x:x:x:x:x:x` — IPv6 位址，其中 x 是 0 到 ffff 的十六進位數。 `x:x:x:x::0/p` — IPv6 位址的子網路，其中 p 是 0 到 64 之間的數字。 預設值：`""`（此區域中沒有網路位址）
[NetworkZonesTrusted]部分包含與受信任網路關聯的網路位址。您可以指定多個 IP 位址或 IP 位址子網路。		
`Address.item_#`	指定 IP 位址或 IP 位址的子網路。	`d.d.d.d` — IPv4 位址，其中 d 是 0 至 255 之間的十進位數。 `d.d.d.d/p` — IPv4 位址的子網路，其中 p 是 0 到 32 之間的數字。 `x:x:x:x:x:x:x:x` — IPv6 位址，其中 x 是 0 到 ffff 的十六進位數。 `x:x:x:x::0/p` — IPv6 位址的子網路，其中 p 是 0 到 64 之間的數字。 預設值：`""`（此區域中沒有網路位址）

設定網路封包規則清單

若要新增網路封包規則，請執行下列指令：

```
kesl-control [-F] --add-rule [--name <rule name>] [--action <Allow|Block>] [--protocol <protocol>] [--direction
<direction>] [--remote <remote address>:<port>] [--local <local address>:<port>] [--at <index>]
```

其中：

- `--name <rule name>` 是網路封包規則的名稱。
- `--action <Allow|Block>` 是將對此網路封包規則中指定的連線執行的操作。
- `--protocol <protocol>` 是您要監控其網路活動的協定。
- `--direction <direction>` 是受監控網路活動的方向。
- `--remote <remote address>:<port>` 是遠端裝置的網路位址。您可以指定預定義網路區域的名稱作為遠端位址。
- `--local <local address>:<port>` 是已安裝 Kaspersky Endpoint Security 之裝置的網路位址。
- `--at <index>` 是規則在網路封包規則清單中的索引。如果未指定 `--at` 選項或其值大於清單中的規則數，則新規則將會新增至清單的末端。

指令中未指定值的參數將被設定為其預設值。

建立封鎖所有連至 TCP 連接埠 23 的傳入和已建立連線之規則範例

```
kesl-control --add-rule --name Block_Telnet --action Block --direction in --protocol TCP --local any:23 --remote any
```

建立針對公共網路區域封鎖透過 TCP 連接埠 23 的傳入和已建立連線之規則範例

```
kesl-control --add-rule --name Block_Telnet --action Block --direction in --protocol TCP --local any:23 --remote Public
```

若要刪除網路封包規則，請執行下列指令之一：

```
kesl-control --del-rule --name <rule name>
```

或

```
kesl-control --del-rule --index <current index>
```

其中：

- `--name <rule name>` 是網路封包規則的名稱。
- `--index <current index>` 是網路封包規則清單中規則的目前索引。

如果網路封包規則清單包含多個同名規則，或不包含指定名稱或索引的規則，則會發生錯誤。

若要變更網路封包規則的執行優先級，請執行下列指令之一：

```
kesl-control --move-rule --name <rule name> --at < new index>
```

或

```
kesl-control --move-rule --index <current index> --at <new index>
```

其中：

- `--name <rule name>` 是網路封包規則的名稱。
- `--index <current index>` 是網路封包規則清單中規則的目前索引。
- `--at <new index>` 是網路封包規則清單中規則的新索引。

設定網路區域

若要將網路位址新增至區域，請執行下列指令：

```
kesl-control --add-zone <zone> --address <address>
```

其中：

- `<zone>` 是網路區域的預定義名稱。可能的值：`Public`、`Local`、`Trusted`。
- `<address>` 是網路位址或子網路。

若要從區域中刪除網路位址，請執行下列指令之一：

```
kesl-control --del-zone <zone> --address <address>
```

或

```
kesl-control --del-zone <zone> --index <address index in the zone>
```

如果一個區域包含多個具有相同網路位址的項目，則不會執行`--del-zone`指令。

如果指定的網路位址或索引不存在，則會產生錯誤訊息。

安全控制

裝置控制工作

此表說明您可以為裝置控制工作（`Device_Control`）指定的所有設定及其所有可能值和預設值。

裝置控制工作設定

設定	描述	參數值
`OperationMode`	對嘗試存取根據裝置控制規則受到限制的裝置做出的回應	`Block`（預設值）- 應用程式套用程式為裝置或匯流排定義的存取模式。 `Notify` - 應用程式測試所選的存取模式並產生關於偵測到存取裝置的嘗試的事件。
`AllowToRequestTemporaryAccess`	允許請求對被封鎖裝置的臨時存取權限。 只有當組織中部署了卡巴斯基安全管理中心 16.1 且用戶端裝置能夠與管理伺服器建立連線時，才能授予對被封鎖裝置的存取權。	`Yes` – 允許使用者在應用程式的圖形介面或命令列中請求對被封鎖裝置的臨時存取權。 `No`（預設）— 不允許使用者請求對被封鎖裝置的臨時存取權限。
[DeviceClass]部分包含根據裝置類型決定的存取模式。		
`HardDrive`	連線到用戶端裝置的硬碟的存取模式。	`Allow` — 允許使用者存取硬碟。 `DependsOnBus`（預設）：對硬碟的存取取決於其所連線匯流排定義的存取模式。 `Block` — 對使用者封鎖存取所有硬碟（系統硬碟例外，永遠不會被裝置控制封鎖）。 `ByRule` — 對硬碟的存取取決於存取規則。 `ReadOnly` – 使用者只能對硬碟進行唯讀存取，寫入將被封鎖。

設定	描述	參數值
RemovableDrive	連線到用戶端裝置的卸除式磁碟機的存取模式。	Allow — 允許使用者存取卸除式磁碟機。 DependsOnBus（預設）：對卸除式磁碟機的存取取決於其所連線匯流排定義的存取模式。 Block — 封鎖使用者存取卸除式磁碟機。 ByRule — 卸除式磁碟機的存取取決於存取規則。 ReadOnly – 使用者只能對卸除式磁碟機進行唯讀存取，寫入將被封鎖。
FloppyDrive	連線到用戶端裝置的軟碟機的存取模式。 應用程式不會封鎖使用 ISA 匯流排連線到用戶端裝置的軟碟機。	Allow — 允許使用者存取軟碟機。 DependsOnBus（預設）：對軟碟機的存取取決於其所連線匯流排定義的存取模式。 Block — 封鎖使用者存取軟碟機。 ByRule — 對軟碟機的存取取決於存取規則。 ReadOnly — 使用者只能對軟碟機進行唯讀存取，寫入將被封鎖。
OpticalDrive	連線到用戶端裝置的 CD/DVD 光碟機的存取模式。	Allow — 允許使用者存取 CD/DVD 光碟機。 DependsOnBus（預設）：對 CD/DVD 光碟機的存取取決於其所連線匯流排定義的存取模式。 Block — 封鎖使用者存取 CD/DVD 光碟機。 ByRule — 對 CD/DVD 光碟機的存取取決於存取規則。 ReadOnly – 使用者只能對 CD/DVD 磁碟機進行唯讀存取，寫入將被封鎖。
SerialPortDevice	透過序列埠連線到用戶端裝置的裝置的存取模式。 應用程式不會封鎖使用 ISA 匯流排透過序列埠連線到用戶端裝置的裝置。	Allow — 允許使用者存取透過序列埠連線的裝置。 DependsOnBus（預設）：透過串列連線的裝置的存取依賴於匯流排存取模式。 Block — 封鎖使用者存取透過序列埠連線的裝置。
ParallelPortDevice	透過並行連接埠連線到用戶端裝置的裝置的存取模式。	Allow — 允許使用者存取透過並行連接埠連線的裝置。 DependsOnBus（預設）：對透過並行連接埠連線的裝置的存取取決於匯流排存取模式。 Block — 封鎖使用者存取透過並行連接埠連線的裝置。
Printer	連線到用戶端裝置的印表機的存取模式。	Allow — 允許使用者存取印表機。 DependsOnBus（預設）：對印表機的存取取決於其所連線匯流排定義的存取模式。 Block — 封鎖使用者存取印表機。
Modem	連接到用戶端裝置的數據機的存取模式。	Allow — 允許使用者存取數據機。 DependsOnBus（預設）：對數據機的存取取決於其所已連線的匯流排定義的存取模式。 Block — 封鎖使用者存取數據機。
TapeDrive	連線到用戶端裝置的磁帶裝置的存取模式。	Allow — 允許使用者存取磁帶裝置。 DependsOnBus（預設）：對磁帶裝置的存取取決於為其所連線的匯流排定義的存取模式 Block — 封鎖使用者存取磁帶裝置。
MultifuncDevice	連線到用戶端裝置的多功能裝置的存取模式。	Allow — 允許使用者存取多功能裝置。 DependsOnBus（預設）：對多功能裝置的存取取決於其所連線的匯流排定義的存取模式。 Block — 封鎖使用者存取多功能裝置。
SmartCardReader	連線到用戶端裝置的智慧卡讀卡器的存取模式。	Allow — 允許使用者存取智慧卡讀卡器。 DependsOnBus（預設）：對智慧卡讀卡器的存取取決於其所已連線的匯流排定義的存取模式。 Block — 封鎖使用者存取智慧卡讀卡器。
WiFiAdapter	連線到用戶端裝置的 Wi-Fi 介面卡的存取模式。	Allow — 允許使用者存取 Wi-Fi 介面卡。 DependsOnBus（預設）：對 Wi-Fi 介面卡的存取取決於連線匯流排存取模式。 Block — 封鎖使用者存取 Wi-Fi 介面卡。

設定	描述	參數值
NetworkAdapter	連線到用戶端裝置的外部網路介面卡的存取模式。	Allow — 允許使用者存取外部網路介面卡。 DependsOnBus（預設）：對外部網路介面卡的存取取決於其所連線的匯流排定義的存取模式。 裝置控制不允許拒絕存取外部網路介面卡，以避免斷開用戶端裝置與網路的連線。
PortableDevice	連線到用戶端裝置的可攜式裝置的存取模式。	Allow — 允許使用者存取可攜式裝置。 DependsOnBus（預設）：對可攜式裝置的存取取決於其所已連線的匯流排定義的存取模式。 Block — 封鎖使用者存取可攜式裝置。
BluetoothDevice	連線到用戶端裝置的藍牙裝置的存取模式。	Allow — 允許使用者存取藍牙裝置。 DependsOnBus（預設）：對藍牙裝置的存取取決於其所連線匯流排定義的存取模式。 Block — 封鎖使用者存取藍牙裝置。
ImagingDevice	連線到用戶端裝置的映像裝置的存取模式。	Allow — 允許使用者存取所有映像裝置。 DependsOnBus（預設）：對映像裝置的存取取決於其所連線匯流排定義的存取模式。 Block—封鎖使用者存取所有映像裝置。
SoundAdapter	連線到用戶端裝置的聲音介面卡的存取模式。	Allow—允許使用者存取所有聲音介面卡。 DependsOnBus（預設）：對聲音介面卡的存取取決於其所連線的匯流排定義的存取模式。 Block—封鎖使用者存取所有聲音介面卡。
InputDevice	連線到用戶端裝置的輸入裝置（鍵盤、滑鼠、觸控板等）的存取模式。	Allow — 允許使用者存取輸入裝置。 DependsOnBus（預設）：對輸入裝置的存取取決於其所連線的匯流排定義的存取模式。 Block — 封鎖使用者存取輸入裝置。
[DeviceBus]部分包含連線匯流排的存取模式。		
USB	透過 USB 連線到用戶端裝置的裝置的存取模式。	Allow（預設值）— 允許使用者存取 USB 裝置。 Block — 封鎖使用者存取 USB 裝置。
FireWire	透過 FireWire 連線到用戶端裝置的裝置的存取模式。	Allow（預設值）— 允許使用者存取透過 FireWire 介面連線的裝置。 Block — 封鎖使用者存取透過 FireWire 介面連線的裝置。
[TrustedDevices.item_ #]部分包含受信任裝置。		
DeviceId	指定受信任裝置的 ID或 ID 遮罩。	您可以使用遮罩 *（任意字元序列）或？（任意單一字元）表示裝置 ID。 例如： *若要拒絕存取指定裝置以外的所有 USB 裝置，請指定以下設定：* 在 [DeviceBus] 部分中，指定 USB=Block 在 [TrustedDevices.item_#] 部分中，指定 DeviceId=<device ID> *若要拒絕存取所有 USB 裝置，但允許存取所有 USB 磁碟機，請指定以下設定：* 在 [DeviceBus] 部分中，指定 USB=Block 在 [TrustedDevices.item_#] 部分中，指定 DeviceId=USBSTOR*
Comment	對指定的受信任裝置的註解。	—
[TrustedDevices.item_#.Principals.item_#] 區域包含存取受信任裝置的規則。		

設定	描述	參數值
Principal	其裝置受信任的使用者或群組。 如果裝置具有「唯讀」存取類型，即使將受信任裝置指派給特定使用者，系統仍會忽略受指派的使用者，但會對所有使用者開放寫入權限。	\Everyone（預設）：該裝置對所有使用者而言都是受信任的。 <user name> 是裝置所信任的本機或網域使用者名稱（如果系統允許以此格式輸入使用者名稱，則不必指定包含網域的完整名稱；也可以採用 <網域名稱>\<user name> 或 <user name>@<網域名稱> 格式）。 @<group name> 是裝置所信任的（本機或網域）使用者群組名稱。
[Schedules.item_#]部分包含裝置存取排程。您僅可以為硬碟、卸除式磁碟機、軟碟機和 CD/DVD 光碟機設定排程。		
ScheduleName	指定排程名稱。 排程名稱必須唯一。	預設值：Default。 如果允許連線匯流排存取對應的裝置類型，則Default排程可讓使用者隨時完全存取裝置。 您無法刪除Default排程。
DaysHours	指定排程的時間間隔。	All（預設值）— 此排程全天候有效（沒有時間限制）。 <weekday> – 星期幾。您可以使用星期的完整名稱或縮寫（例如，若為星期一，您可以指定 Mo 、 Mon 或 Monday ）。對於星期幾，您可以指定間隔或特定日期。一周從週日開始。 <hour> – 小時 [0:24]。對於小時，您只能指定間隔。 schedule_1 的範例，其有效時間為週日至週六的上午 0 點至上午 11 點、中午 12 點至下午 3 點，以及下午 4 點至凌晨 12 點。 [Schedules.item_0001] ScheduleName=schedule_1 DaysHours=Su-Sa:0..11,12..15,16..24 schedule_2 的範例，適用於下列時間間隔：星期四中午 12 點至下午 2 點，以及星期五凌晨 2 點至下午 3 點和下午 4 點至凌晨 12 點。 [Schedules.item_0002] ScheduleName=schedule_2 DaysHours=Th:12..14;Fr:2..15,16..24 schedule_3 的範例，其每週 7 天、每天 24 小時有效。 [Schedules.item_0003] ScheduleName=schedule_3 DaysHours=All
[HardDrivePrincipals.item_#]部分包含硬碟存取規則。 對於硬碟磁碟機，必須始終啟用至少一個排程。您可以為一個硬碟指派多個存取規則。此外，可以為一個使用者或一組使用者指定多個排程。如果使用者或群組的存取規則發生衝突，則授予最低存取權限。		
Principal	指定為其套用存取規則的使用者或使用者群組。	\Everyone（預設值）— 存取規則套用於所有使用者。 <user name> 是存取規則適用的本機使用者名稱。 @<group name> 是存取規則適用的使用者群組名稱。
[HardDrivePrincipals.item_#.AccessRules.item_#] 包含存取規則設定。		
UseRule	指定規則是啟用還是停用。	Yes（預設值）— 存取規則已啟用。 No — 存取規則已停用。
ScheduleName	[Schedules.item_#] 部分中指定的排程。	預設值：Default。
Access	指定存取類型。	Allow（預設值）— 允許存取硬碟磁碟機。 Block — 封鎖對硬碟的存取。
[RemovableDrivePrincipals.item_#]部分包含卸除式磁碟機的存取規則。 對於卸除式磁碟機，必須始終啟用至少一個排程。您可以為卸除式磁碟機指派多個存取規則。此外，可以為一個使用者或一組使用者指定多個排程。如果使用者或群組的存取規則發生衝突，則授予最低存取權限。		
Principal	指定為其套用存取規則的使用者或使用者群組。	\Everyone（預設值）— 存取規則套用於所有使用者。 <user name> 是存取規則適用的本機使用者名稱。 @<group name> 是存取規則適用的使用者群組名稱。
[RemovableDrivePrincipals.item_#.AccessRules.item_#] 包含存取規則設定。		
UseRule	指定規則是啟用還是停用。	Yes（預設值）— 存取規則已啟用。 No — 存取規則已停用。

設定	描述	參數值
ScheduleName	[Schedules.item_#] 部分中指定的排程。	預設值：Default。
Access	指定存取類型。	Allow（預設值）— 允許存取卸除式磁碟機。 Block — 封鎖存取卸除式磁碟機。
[FloppyDrivePrincipals.item_#]部分包含軟碟機的存取規則。 對於軟碟機，必須始終啟用至少一個排程。您可以為軟碟機指派多個存取規則。此外，可以為一個使用者或一組使用者指定多個排程。如果使用者或群組的存取規則發生衝突，則授予最低存取權限。		
Principal	指定為其套用存取規則的使用者或使用者群組。	\Everyone（預設值）— 存取規則套用於所有使用者。 <user name> 是存取規則適用的本機使用者名稱。 @<group name> 是存取規則適用的使用者群組名稱。
[FloppyDrivePrincipals.item_#.AccessRules.item_#] 包含存取規則設定。		
UseRule	指定規則是啟用還是停用。	Yes（預設值）— 存取規則已啟用。 No — 存取規則已停用。
ScheduleName	[Schedules.item_#] 部分中指定的排程。	預設值：Default。
Access	指定存取類型。	Allow（預設值）— 允許存取軟碟機。 Block —封鎖對軟碟機的存取。
[OpticalDrivePrincipals.item_#]部分包含 CD/DVD 光碟機的存取規則。 對於 CD/DVD 磁碟機，必須始終啟用至少一個排程。您可以為 CD/DVD 光碟機指派多個存取規則。此外，可以為一個使用者或一組使用者指定多個排程。如果使用者或群組的存取規則發生衝突，則授予最低存取權限。		
Principal	指定為其套用存取規則的使用者或使用者群組。	\Everyone（預設值）— 存取規則套用於所有使用者。 <user name> 是存取規則適用的本機使用者名稱。 @<group name> 是存取規則適用的使用者群組名稱。
[OpticalDrivePrincipals.item_#.AccessRules.item_#] 包含存取規則設定。		
UseRule	指定規則是啟用還是停用。	Yes（預設值）— 存取規則已啟用。 No — 存取規則已停用。
ScheduleName	[Schedules.item_#] 部分中指定的排程。	預設值：Default。
Access	指定存取類型。	Allow（預設值）— 允許存取 CD/DVD 磁碟機。 Block — 封鎖存取 CD/DVD 光碟機。

Web 控制

在指令列上，您可以使用 Web 控制預定義工作 (Web_Control) 來管理 Web 控制。

預設情況下，Web 控制工作處於停止狀態。您可以手動啟動和停止工作。

您可以透過變更Web 控制預定義工作的設定來編輯 Web 控制設定。

您也可以使用 Web 控制管理指令檢視和編輯 Web 控制設定。

Web 控制工作

下表說明可為 Web 控制工作 (Web_Control) 指定之所有設定的所有可用值及預設值。

設定	描述	參數值
WebControlDefaultAction	預設規則，即當 Web 控制偵測到嘗試存取其他規則未涵蓋的 Web 資源時所執行的操作。	Allow（預設值）— 允許存取 Web 資源。 Block — 阻止存取 Web 資源。
ComplaintRecipient	管理員的電子郵件位址，用於接收關於錯誤封鎖網頁資源的訊息。	
[Rules.item_#]部分包含以下設定：		
Name	Web 資源存取規則名稱。規則名稱必須唯一。	
WebControlAction	當 Web 控制偵測到嘗試存取與規則相符的 Web 資源時將執行的該規則的操作。	Allow(預設值) — 允許存取 Web 資源。 Block — 阻止存取 Web 資源。 Notify — 顯示警告，表示該 Web 資源不受歡迎。透過點擊警告訊息中的連接，使用者可以存取所請求的 Web 資源。
Enabled	Web資源存取規則的狀態。	Yes — 規則已啟用，Web 控制在運作期間套用此規則。 No（預設值）— 規則已停用，在 Web 控制執行時不被使用。
ScheduleId	[Schedules.item_#] 部分中使用的排程 ID。	
UseUrls	在規則中使用 Web 資源位址篩選器。	Yes — 在規則中使用 Web 資源位址篩選器。 No（預設值）— 不使用網頁網址篩選器，將規則套用至所有 Web 資源位址。
Urls.item_#	規則控制存取控制的 Web 資源的位址。	您可以使用遮罩來指定 Web 資源位址。
UseCategories	在規則中使用按內容類別和資料類型類別的篩選器。	None（預設）— 不使用 Web 資源內容篩選器。 ContentOnly — 在規則中使用內容類別篩選器。 FormatOnly — 在規則中使用資料類型類別篩選器。 ContentAndFormat — 在規則中使用內容類別篩選器和資料類型類別篩選器。
[Rules.item_#.ContentCategories.item_#]	用於指定內容類別的部分。	–
ContentCategory	內容類別。	AdultContent, AlcoholTobaccoNarcotics, Violence, Profanity, Weapons, ChatForum, WebMail, OnlineShops, SocialNets, Recruitment, HttpQueryRedirection, CreditCards, PoliceDecision, SoftwareAudioVideo, TechnologyElectronics, GamblingLotteriesSweepstakes, InternetCommunicationMedia, CryptocurAndMining, LegislationBE, ECommerce, ComputerGames, Religions, News, Torrents, FileSharing, AudioAndVideo, BankSites, Blogs, DatingSites, LegislationRF, LegislationGlobal, SexuallyExplicit, Sexuality, AITools
[Rules.item_#.FormatCategories.item_#]	用於指定資料類型類別的部分。	–

設定	描述	參數值
FormatCategory	資料類型類別。	Video — 視訊 Audio — 音訊資料 OfficeDocument — Office 應用程式檔案 Executable — 可執行檔 Archives — 壓縮檔案 Images — 映像檔案 Scripts — 指令碼
UsePrincipals	使用受 Web 資源存取規則涵蓋的使用者篩選器。	Yes — 使用規則中的使用者篩選器。 No（預設值）— 不使用使用者篩選器，將規則套用至所有使用者。
[Rules.item_#.Principals.item_#]	用於指定受 Web 資源存取規則涵蓋的使用者的部分。	
Name	Web 資源存取規則涵蓋的使用者或使用者群組。	<username> 是規則適用的使用者名稱。 @<groupname> 是規則適用的使用者群組名稱。 預設值：Web 資源存取規則適用於所有使用者。
[UrlCategories.item_#]部分包含以下設定：		
Name	規則控制所存取的 Web 資源位址群組的名稱。	
Urls.item_#	屬於該群組的 Web 資源的位址。	您可以使用遮罩來指定 Web 資源位址。
[Schedules.item_#]部分包含規則排程。		
Id	[Rules.item_#] 部分中使用的排程 ID。	1 - 999999 0是Default 排程的 ID，它允許規則不受任何時間限制地運行，即在任何時候運行。
Name	指定排程名稱。	
DaysHours	指定排程的時間間隔。	<weekday> – 星期幾。您可以使用星期的完整名稱或縮寫（例如，若為星期一，您可以指定 Mo、Mon 或 Monday）。對於星期幾，您可以指定間隔或特定日期。—周從週日開始。 <hour> – 小時 [0:24]。您只能指定小時的間隔。

檢視和編輯 Web 控制設定

若要檢視 Web 控制設定，請執行以下指令：

```
kesl-control --get-settings 26 [--file <path to the configuration file>] [--json]
```

其中：

`--file <path to the configuration file>` 是您要將設定輸出到其中的設定檔完整路徑。

`--json`：以 JSON 格式輸出資料。

若要編輯 Web 控制設定，請執行以下指令：

```
kesl-control --set-settings 26 [--file <path to the configuration file>] [--json]
```

其中：

`--file <path to the configuration file>` 是您要從中匯入設定的設定檔完整路徑。

`--json` — 從 JSON 檔案匯入資料。

若要刪除已配置的設定並將 Web 控制設定重設為預設規則，請執行以下指令：

```
kesl-control --set-settings 26 --set-to-default
```

應用程式控制

在指令列中，您可以使用應用程式控制預定義工作（`Application_Control`）來管理應用程式控制。

預設情況下，應用程式控制工作不執行。您可以手動啟動和停止工作。

您可以透過編輯應用程式控制預定義工作的設定來配置裝置上的應用程式控制。

如果您變更允許的應用程式清單，或禁止啟動所有應用程式或影響 Kaspersky Endpoint Security 運作的應用程式，則在使用設定檔或指令列選項修改工作設定時，請執行以下指令：

```
kesl-control --set-settings --accept
```

您也可以使用應用程式控制指令來設定應用程式控制：

- 建立和編輯類別清單。
- 檢視在應用程式中建立的類別清單。
- 配置應用程式控制規則清單。

應用程式控制工作

此表說明可為應用程式控制工作 (`Application_Control`) 指定之所有設定的所有可能值及預設值。

應用程式控制工作設定

設定	描述	參數值
`AppControlMode`	應用程式控制工作運作模式。	`AllowList` — Kaspersky Endpoint Security 阻止使用者啟動任何未在應用程式控制規則中指定的應用程式。 `DenyList`（預設值）— Kaspersky Endpoint Security 允許使用者啟動任何未在應用程式控制規則中指定的應用程式。
`AppControlRulesAction`	Kaspersky Endpoint Security 在偵測到嘗試啟動與配置的規則相符的應用程式時執行的操作。	`ApplyRules`（預設值）— Kaspersky Endpoint Security 套用應用程式控制規則並執行規則中指定的操作。 `TestRules` — Kaspersky Endpoint Security 測試規則並產生關於偵測滿足規則的應用程式的事件。
[Categories.item_#]部分包含以下設定：		
`Name`	規則套用的應用程式類別的名稱。	
`UseIncludes`	使用包容性條件來觸發規則。	`Yes` — 如果應用程式至少滿足一個包容性條件，則將該規則套用於該應用程式。 `No`（預設值）— 即使應用程式滿足包容性條件，也不將規則套用於應用程式。

設定	描述	參數值
IncludeFileNames.item_#	觸發規則的可執行檔的名稱。	您可以使用遮罩來指定檔案名稱。
IncludeFolders.item_#	包含觸發規則的應用程式可執行檔的目錄的名稱。	您可以使用遮罩來指定目錄名稱。
IncludeHashes.item_#	觸發規則的可執行檔的 SHA256 雜湊。	僅可使用 SHA256。
UseExcludes	使用排除條件來觸發規則。	Yes — 如果應用程式至少符合一個排他性條件或不符合任何包容性條件，則不將該規則套用於該應用程式。 No（預設值）— 將規則套用於應用程式，即使應用程式至少符合一個排除條件。
ExcludeFileNames.item_#	觸發規則的可執行檔的名稱。	您可以使用遮罩來指定檔案名稱。
ExcludeFolders.item_#	包含觸發規則的應用程式可執行檔的目錄的名稱。	您可以使用遮罩來指定目錄名稱。
ExcludeHashes.item_#	觸發規則的可執行檔的 SHA256 雜湊。	僅可使用 SHA256。
[AllowListRules.item_#]部分包含用於*AllowList*操作模式的應用程式控制規則清單。 每個 [AllowListRules.item_#] 部分包含以下設定：		
Description	應用程式控制規則的描述。	
AppControlRuleStatus	應用程式控制規則的運作狀態：	On（預設值）：啟用此規則，Kaspersky Endpoint Security 將此規則套用至應用程式控制。 Off：該規則不用於應用程式控制。 Test — Kaspersky Endpoint Security 允許啟動規則涵蓋的應用程式，但在報告中記錄關於這些應用程式啟動的資訊。
Category	規則套用的應用程式類別的名稱。 您可以指定"黃金映像"類別。	
[AllowListRules.item_#.ACL.item_#] 部分包含被允許或拒絕執行應用程式的使用者清單。		
Access	指派給使用者或使用者群組的存取類型。	Allow（預設值）— 允許執行應用程式。 Block — 拒絕執行應用程式。
Principal	應用程式控制規則套用的使用者或使用者群組。	\Everyone（預設值）：此規則適用於所有使用者。 < 使用者名稱 > 是適用該規則的使用者名稱。 @< 群組名稱 > 是適用該規則的使用者群組名稱。
[DenyListRules.item_#]部分包含用於*DenyList*操作模式的應用程式控制規則清單。 每個 [DenyListRules.item_#] 部分包含以下設定：		
Description	應用程式控制規則的描述。	
AppControlRuleStatus	應用程式控制規則的運作狀態：	On（預設值）：啟用此規則，Kaspersky Endpoint Security 將此規則套用至應用程式控制。 Off：該規則不用於應用程式控制。 Test — Kaspersky Endpoint Security 允許啟動規則涵蓋的應用程式，但在報告中記錄關於這些應用程式啟動的資訊。
Category	規則套用的已建立應用程式類別的名稱。 您可以將應用程式的"黃金映像"清單指定為一個類別。	
[DenyListRules.item_#.ACL.item_#]部分包含允許或拒絕執行應用程式的使用者清單。		
Access	指派給使用者或使用者群組的存取類型。	Allow — 允許應用程式啟動。 Block（預設值）– 不允許應用程式啟動。
Principal	應用程式控制規則套用的使用者或使用者群組。	\Everyone（預設值）：此規則適用於所有使用者。 < 使用者名稱 > 是適用該規則的使用者名稱。 @< 群組名稱 > 是適用該規則的使用者群組名稱。

實用文章

如何指定遮罩

您可以使用 * 字元（任意字元序列）或 ? 字元（任意一個字元）作為檔案或目錄名稱遮罩。

您可以使用 * 字元來表示檔案或目錄名稱中包含 / 字元的任意字元集（包括空集）。例如，`/dir/*/file*/` 或 `/dir/file*/`。

您可以用單個 ? 字元來表示檔案或目錄名稱中的任意一個字元（包括 / ）。

建立和編輯類別清單

您可以透過兩種方式建立新類別：

- 使用「kesl --set-settings」指令和應用程式控制工作設定設定檔 (`Application_Control`)。
- 使用 kesl --set-categories 指令和類別設定檔。

若要建立應用程式類別，請執行以下指令：

```
kesl-control --set-categories --file <path to the configuration file>
```

其中：

`--file <path to the configuration file>` 是包含類別設定的設定檔路徑。

具有類別設定的檔案必須具有以下結構：

```
[
   {
      "Exclude" : [ "(FilePath like <full path to the application's executable file>)", "(FileHash == <hash of the executable file>)" ],
      "GUID" : "<unique category identifier>",
      "Include" : [ "(FilePath like <full path to the application's executable file>)", "(FileHash == <hash of the executable file>)" ],
      "Name" : "<category name 1>"
   },
 {
      "Exclude" : [ "(FilePath like <full path to the application's executable file>)", "(FileHash == <hash of the executable file>)" ],
      "GUID" : "<unique category identifier>",
      "Include" : [ "(FilePath like <full path to the application's executable file>)", "(FileHash == <hash of the executable file>)" ],
      "Name" : "<category name 2>"
   }
]
```

若要在 `Exclude` 和 `Include` 欄位中指定檔案名稱，您可以使用遮罩。

> `Name` 設定必需有。如果不指定類別的名稱，則不會建立或刪除該類別。`GUID` 設定也必須有。如果不指定它，則會顯示錯誤訊息並且不會建立類別。指定的 `GUID` 設定必須不帶連字號。

若要編輯已建立的應用程式類別清單，請執行以下指令：

```
kesl-control --set-categories [--names <category name 1> <category name 2> ... <category name N>] --file <path to the configuration file>
```

其中：

- `<category name 1> <category name 2> ... <category name N>` 是您要編輯其資訊的類別名稱。如果要變更多個類別的資訊，請指定類別的名稱，並以空格分隔。如果不指定類別名稱，則會刪除現有類別並從指定檔案建立新類別。
- `--file <path to the configuration file>` 是包含類別設定的設定檔路徑。

實用文章

如何指定遮罩

您可以使用 * 字元（任意字元序列）或 ？字元（任意一個字元）作為檔案或目錄名稱遮罩。

您可以使用 * 字元來表示檔案或目錄名稱中包含 / 字元的任意字元集（包括空集）。例如，`/dir/*/file*/` 或 `/dir/file*/`。

您可以用單個 ? 字元來表示檔案或目錄名稱中的任意一個字元（包括 / ）。

檢視類別清單

在指令列中，您可以使用應用程式控制指令 `kesl-control --get-categories` 來檢視已建立的應用程式類別清單。

建立的類別清單包含以下類別：

- 在卡巴斯基安全管理中心中建立的類別。
- 使用指令列在應用程式控制工作設定中新增的類別。
- 使用清查工作（在卡巴斯基安全管理中心中或使用指令列）建立的“GoldenImage”類別。

若要檢視所有已建立的應用程式類別的清單，請執行以下指令：

```
kesl-control --get-categories [--file <path to the configuration file>] [--json]
```

其中：

- `--file <path to the configuration file>` 是您要將設定輸出到其中的設定檔完整路徑。
- `--json` 被指定以 JSON 格式輸出設定。

Kaspersky Endpoint Security 顯示關於每個應用程式類別的以下資訊：

- 類別的唯一識別碼 (GUID)
- 類別名稱
- 觸發規則的條件清單
- 觸發規則的專屬條件清單

若要檢視單獨應用程式類別清單，請執行下列指令：

```
kesl-control --get-categories [--names <category name 1> <category name 2> ... <category name N>] [--file <path to the configuration file>] [--json]
```

其中：

- `<category name 1> <category name 2> ... <category name N>` 是您要檢視其資訊的類別名稱。如果要檢視關於多個類別的資訊，請指定類別的名稱，並以空格分隔。
- `--file <path to the configuration file>` – 類別清單將匯出到的 JSON 設定檔的完整路徑。
- `--json` 被指定以 JSON 格式輸出設定。

如果在應用程式控制工作設定中，在觸發規則的包容或排他性條件的 `[Categories.item_#]` 部分中指定指向包含可執行檔的應用程式檔案或目錄的符號連接，則在檢視這些條件的類別清單時，將顯示符號連結指向的來源路徑。

配置應用程式控制規則清單

若要檢視應用程式控制規則清單，請執行以下指令：

```
kesl-control --get-settings 21 [--file <path to the configuration file>] [--json]
```

其中：

- `--file <path to the configuration file>` 是您要將設定輸出到其中的設定檔完整路徑。
- `--json`：以 JSON 格式輸出資料。

Kaspersky Endpoint Security 顯示關於應用程式控制規則的以下資訊：

- 應用程式控制工作運作模式。
- 應用程式控制在偵測到嘗試啟動與設定的規則相符的應用程式時所採取的操作。
- 應用程式控制規則的描述（如果有）。
- 應用程式控制規則的運作狀態。
- 規則套用的應用程式類別名稱。
- 指派給使用者或使用者群組的存取類型。
- 應用程式控制規則套用的使用者或使用者群組。

若要編輯應用程式類別和應用程式控制規則的清單，請執行以下指令：

```
kesl-control --set-settings 21 [--file <path to the configuration file>] [--json]
```

其中：

- `--file <path to the configuration file>` 是您要從中匯入設定的設定檔完整路徑。
- `--json` — 從 JSON 檔案匯入資料。

若要刪除應用程式類別和應用程式控制規則的清單，請執行以下指令：

```
kesl-control --set-settings 21 --set-to-default
```

設定清查

您可以使用指令列來清查受防護裝置上的應用程式，如下所示：

- 透過清查預定義工作 (`Inventory_Scan`)。您可以手動啟動或停止此工作，以及設定工作排程。您可以透過編輯此工作的設定來配置掃描設定。
- 透過使用者清查工作（`InventoryScan` 類型的工作）。您可以手動啟動、停止、暫停或繼續使用者工作，並設定工作排程。

您可以使用應用程式控制管理指令檢視由於清查工作中在裝置上偵測到的應用程式清單。

清查工作

此表說明您可以為清查工作（`Inventory_Scan`）指定的所有設定及其所有可能值和預設值。

清查工作設定

設定	描述	參數值
`ScanScripts`	啟用指令碼掃描。	`Yes`（預設值）— 掃描指令碼。 `No` — 不掃描指令碼。
`ScanBinaries`	啟用二進位檔案掃描（elf、java 和 pyc）。	`Yes`（預設值）— 掃描二進位。 `No` — 不掃描二進位檔案。
`ScanAllExecutable`	啟用對具有可執行位的檔案的掃描。	`Yes`（預設值）— 掃描具有可執行位元的檔案。 `No` — 不掃描具有可執行位的檔案。
`GoldenImageAction`	完成清查工作後，Kaspersky Endpoint Security 必須對「黃金映像」應用程式類別執行的動作： 您可以使用應用程式控制規則中的「黃金映像」類別。	`DoNothing`（預設）– 完成清查後不變更黃金映像應用程式類別。 `Create` – 將偵測到的應用程式新增至黃金映像應用程式類別。如果該類別不存在，則建立該類別。如果該類別存在，則更新該類別中的應用程式清單。 `Remove` – 清除「黃金映像」應用程式類別。此類別會在工作啟動後立即清除，不會對裝置上的檔案執行清查。
[ScanScope.item_#]部分包含以下設定：		
`AreaDesc`	清查範圍的描述。使用此設定指定的字串的最大長度為 4096 個字元。	預設值：`All objects`。
`UseScanArea`	啟用指定清查範圍的掃描。若要執行該工作，請啟用至少一個清查範圍的掃描。	`Yes`（預設值）— 掃描指定的清查範圍。 `No` — 不掃描指定的清查範圍。

設定	描述	參數值
AreaMask.item_#	清查掃描範圍限制。在清查掃描範圍中，應用程式僅掃描使用 shell 格式的遮罩指定的檔案。 如果未指定此設定，應用程式將掃描清查範圍內的所有物件。您可以為此設定指定多個值。	預設值為 * （掃描所有物件）。
Path	包含要掃描的物件的目錄的路徑。	< 本機目錄路徑 > — 掃描指定目錄中的物件。 預設值： /usr/bin
[ExcludedFromScanScope.item_#]部分包含以下設定：		
AreaDesc	清查排除範圍的描述。	預設值未定義。
UseScanArea	從清查中排除指定的範圍。	Yes （預設值）— 排除指定範圍。 No — 不排除指定的範圍。
AreaMask.item_#	使用外殼遮罩限制清查排除範圍。 如果未指定此設定，應用程式將排除清查範圍內的所有物件。您可以為此設定指定多個值。	預設值： * （排除所有物件）
Path	包含要排除的物件的目錄的路徑。	< 本機目錄路徑 > 從掃描中排除指定目錄中的物件。您可以使用遮罩來指定路徑。

實用文章

如何指定遮罩

您可以使用 * （星號）字元來建立檔案或目錄名稱遮罩。

您可以指示單一 * 字元來表示檔案或目錄名稱中 / 字元前面的任意字元集（包括空集）。例如， /dir/*/file 或 /dir/*/*/file 。

您可以用兩個連續的 * 字元來表示檔案或目錄名稱中的任意一組字元（包括空集和 / 字元）。例如， /dir/**/file*/ 或 /dir/file**/ 。

** 遮罩在目錄名稱中只能使用一次。例如， /dir/**/**/file 是一個不正確的遮罩。

您可以使用單一 ? 字元來表示檔案或目錄名稱中的任意一個字元。

檢視偵測到的應用程式清單

若要檢視裝置上偵測到的應用程式清單，請執行以下指令：

```
kesl-control --get-app-list [--json]
```

其中 --json 表示以 JSON 格式輸出資料。

Kaspersky Endpoint Security 可顯示關於偵測到的應用程式的以下資訊：

- **清查的日期和時間**。執行清查工作的日期和時間
- **應用程式數量**。裝置上偵測到的應用程式數量

- 包含以下資訊的應用程式清單：
  - **路徑**。應用程式的路徑。
  - **雜湊**。應用程式雜湊總和。
  - **類型**。應用程式類型。例如，`Script`，`Executable`。
  - **類別**。應用程式所屬的類別（如果先前已建立）。您可以使用以下命令檢視已建立的應用程式類別清單：

    ```
    kesl-control --get-categories
    ```

> 新增類別時，其資訊不會在應用程式清單中自動更新。若要更新應用程式清單，您需要重新啟動清查工作。

系統完整性監控工作

您可以使用系統完整性監控預定義工作（`System_Integrity_Monitoring`）在指令列中即時管理系統完整性監控。`OAFIM` 工作類型。

系統完整性監控工作預設不執行。您可以手動啟動和停止工作。

您可以透過編輯系統完整性監控預定義工作的設定來在裝置上設定系統完整性監控。

按存取系統完整性監控工作設定

設定	描述	參數值
`UseExcludeMasks`	對 `ExcludeThreats.item_#` 設定指定的物件啟用監控範圍排除。 僅當指定了 `ExcludeMasks.item_#` 設定時，此設定才適用。	`Yes` — 從監控範圍中排除 `ExcludeMasks.item_#` 設定指定的物件。 `No`（預設值）— 不從監控範圍中排除 `ExcludeMasks.item_#` 設定指定的物件。
`ExcludeMasks.item_#`	按名稱或遮罩排除監控中的物件。您可以使用此設定按名稱從指定的掃描範圍中排除單一檔案，或使用 shell 格式的遮罩一次排除多個檔案。 在為此設定指定值之前，請確保 `UseExcludeMasks` 設定已啟用。 您可以指定多個遮罩。每個遮罩必須在新行上用新索引指定。	預設值未定義。
[ScanScope.item_#] 區段包含系統完整性監控工作的監控範圍。必須為該工作指定至少一個監控範圍。您可以以任何順序指定多個 [ScanScope.item_#] 部分。應用程式按索引的升序處理範圍。 [ScanScope.item_#] 部分包含以下設定：		
`AreaDesc`	監測範圍描述；包含關於監控範圍的附加資訊。	預設值未定義。
`UseScanArea`	啟用指定範圍的監控。	`Yes`（預設值）— 監控指定範圍。 `No` — 不監控指定範圍。
`Path`	監控目錄的路徑。	您可以使用遮罩來指定路徑。 預設值：/opt/kaspersky/kesl/
`AreaMask.item_#`	監控範圍限制。在監控範圍內，應用程式僅掃描使用 shell 格式的遮罩指定的物件。 您可以以任意順序指定多個 `AreaMask.item_#` 項目。應用程式按索引的升序處理範圍。	預設值：`*`（監控所有物件）
[ExcludedFromScanScope.item_#] 包含要從所有 [ScanScope.item_#] 部分排除的物件。您可以以任意順序指定多個 [ExcludedFromScanScope.item_#] 部分。應用程式按索引的升序處理範圍。 [ExcludedFromScanScope.item_#] 部分包含以下設定：		

設定	描述	參數值
AreaDesc	監控排除範圍描述，包含關於監控排除範圍的附加資訊。	預設值未定義。
UseScanArea	將指定範圍排除在監控之外。	Yes（預設值）— 從監控中排除指定範圍。 No — 不將指定範圍排除在監控之外。
Path	包含被從監控中排除的物件的目錄路徑。	您可以使用遮罩來指定路徑。 預設值未定義。
AreaMask.item_#	監控排除範圍的限制。在監控排除範圍中，應用程式僅排除使用 shell 格式的遮罩指定的物件。 您可以以任意順序指定多個 AreaMask.item_# 項目。應用程式按索引的升序處理範圍。	預設值：*（從監控中排除所有物件）。

實用文章

如何指定遮罩

您可以使用 *（星號）字元來建立檔案或目錄名稱遮罩。

您可以指示單一 * 字元來表示檔案或目錄名稱中 / 字元前面的任意字元集（包括空集）。例如，/dir/*/file 或 /dir/*/*/file。

您可以用兩個連續的 * 字元來表示檔案或目錄名稱中的任意一組字元（包括空集和 / 字元）。例如，/dir/**/file*/ 或 /dir/file**/。

** 遮罩在目錄名稱中只能使用一次。例如，/dir/**/**/file 是一個不正確的遮罩。

您可以使用單一 ? 字元來表示檔案或目錄名稱中的任意一個字元。

系統完整性檢查工作

您可以使用自訂系統完整性檢查工作（System_Integrity_Monitoring），在指令列中對裝置執行系統完整性檢查。ODFIM 工作類型。

您可以手動啟動、停止、暫停或繼續使用者工作，並設定工作排程。您可以透過編輯這些工作的設定來配置系統完整性檢查。

系統完整性檢查工作設定

設定	描述	參數值
RebuildBaseline	在*系統完整性檢查*工作完成後啟用基線重建。	Yes：每次*系統完整性檢查*工作完成時重建基線。 No（預設）：每次*系統完整性檢查*工作完成時不重建基線。
CheckFileHash	將受監控檔案的目前狀態與原始狀態進行比較時，使用檔案雜湊（SHA256）作為標準。	Yes：檢查雜湊。 No（預設值）— 停用雜湊檢查。如果停用此檢查，應用程式將僅比較檔案大小（如果檔案大小沒有改變，則修改時間不被視為關鍵參數）。
TrackDirectoryChanges	啟用目錄監控。	Yes：檢查系統完整性時監控目錄。 No（預設值）— 不監控目錄。
TrackLastAccessTime	啟用追蹤上次檔案存取時間。在 Linux 作業系統中，它是 noatime 設定。	Yes — 追蹤上次檔案存取時間。 No（預設值）— 不追蹤上次檔案存取時間。

設定	描述	參數值
UseExcludeMasks	對 ExcludeMasks.item_# 設定指定的物件啟用監控範圍排除。 僅當指定了 ExcludeMasks.item_# 設定時，此設定才適用。	Yes — 從監控範圍中排除 ExcludeMasks.item_# 設定指定的物件。 No（預設值）— 不從監控範圍中排除 ExcludeMasks.item_# 設定指定的物件。
ExcludeMasks.item_#	按名稱或遮罩排除監控中的物件。您可以使用此設定按名稱從指定的掃描範圍中排除單一檔案，或使用 shell 格式的遮罩一次排除多個檔案。 在為此設定指定值之前，請確保 UseExcludeMasks 設定已啟用。 您可以指定多個遮罩。每個遮罩必須在新行上用新索引指定。	預設值未定義。
[ScanScope.item_#] 區段包含 *系統完整性檢查* 的監控範圍。必須為該工作指定至少一個監控範圍。您可以以任何順序指定多個 [ScanScope.item_#] 部分。應用程式按索引的升序處理範圍。 [ScanScope.item_#] 部分包含以下設定：		
AreaDesc	監測範圍描述；包含關於監控範圍的附加資訊。	預設值未定義。
UseScanArea	啟用指定範圍的監控。	Yes（預設值）— 監控指定範圍。 No — 不監控指定範圍。
Path	監控目錄的路徑。	您可以使用遮罩來指定路徑。 預設值：/opt/kaspersky/kesl/
AreaMask.item_#	監控範圍限制。在監控範圍內，應用程式僅掃描使用 shell 格式的遮罩指定的物件。 您可以以任意順序指定多個 AreaMask.item_# 項目。應用程式按索引的升序處理範圍。	預設值：*（監控所有物件）
[ExcludedFromScanScope.item_#]部分包含要從所有 [ScanScope.item_#] 部分排除的物件。您可以按任意順序指定多個 [ExcludedFromScanScope.item_#] 部分。應用程式按索引的升序處理範圍。 [ExcludedFromScanScope.item_#] 部分包含以下設定：		
AreaDesc	監控排除範圍描述，包含關於監控排除範圍的附加資訊。	預設值未定義。
UseScanArea	將指定範圍排除在監控之外。	Yes（預設值）— 從監控中排除指定範圍。 No — 不將指定範圍排除在監控之外。
Path	包含被從監控中排除的物件的目錄路徑。	您可以使用遮罩來指定路徑。 預設值未定義。
AreaMask.item_#	監控排除範圍的限制。在監控排除範圍中，應用程式僅排除使用 shell 格式的遮罩指定的物件。 您可以以任意順序指定多個 AreaMask.item_# 項目。應用程式按索引的升序處理範圍。	預設值：*（從監控中排除所有物件）。

實用文章

如何指定遮罩

您可以使用 *（星號）字元來建立檔案或目錄名稱遮罩。

您可以指示單一 * 字元來表示檔案或目錄名稱中 / 字元前面的任意字元集（包括空集）。例如，/dir/*/file 或 /dir/*/*/file。

您可以用兩個連續的 * 字元來表示檔案或目錄名稱中的任意一組字元（包括空集和 / 字元）。例如，/dir/**/file*/ 或 /dir/file**/。

** 遮罩在目錄名稱中只能使用一次。例如，/dir/**/**/file 是一個不正確的遮罩。

您可以使用單一 ? 字元來表示檔案或目錄名稱中的任意一個字元。

進階威脅和目標式攻擊防護

Kaspersky Endpoint Detection and Response Expert (on-premises) 整合

您可以透過命令列上的 *Kaspersky Endpoint Detection and Response Expert (on-premises)*（`KATAEDR`）預定義工作，管理 Kaspersky Endpoint Security 與 Kaspersky Endpoint Detection and Response Expert (on-premises) 解決方案之間的整合。

> 此工作還可讓您管理 Kaspersky Endpoint Detection and Response (KATA) 整合設定。對於 Kaspersky Endpoint Detection and Response Expert (on-premises) 整合，您需要選取 *EDR Expert (on-premises)* 整合模式，並視需要管理整合設定。

您可以透過編輯預定義工作的設定來管理 Kaspersky Endpoint Detection and Response Expert (on-premises) 整合設定。

*Kaspersky Endpoint Detection and Response Expert (on-premises) 整合*工作預設不會執行。您可以手動啟動和停止工作。

您可以使用 EDR Expert (on-premises) 元件管理指令管理憑證，這些憑證用於連線到 OSMP 伺服器。

Kaspersky Endpoint Detection and Response Expert (on-premises) 整合設定

下表說明 Kaspersky Endpoint Detection and Response Expert (on-premises) (`KATAEDR`) 整合預定義工作的設定，您可以在與 Kaspersky Endpoint Detection and Response Expert (on-premises) 整合時管理這些設定。

> 此工作還可讓您管理 Kaspersky Endpoint Detection and Response (KATA) 整合設定。若要整合 Kaspersky Endpoint Detection and Response Expert (on-premises)，您需要在工作設定中選取 *EDR Expert (on-premises)* 整合模式（`Mode=EDRExpertOnPrem`）。

Kaspersky Endpoint Detection and Response Expert (on-premises) 整合設定

設定	描述	值
`Mode`	整合模式。 對於 Kaspersky Endpoint Detection and Response Expert (on-premises) 整合，Kaspersky Endpoint Security 應用程式會與 OSMP 平台上的伺服器互動。 對於 Kaspersky Endpoint Detection and Response (KATA) 整合，Kaspersky Endpoint Security 安全應用程式與 Kaspersky Anti Targeted Attack Platform 上的伺服器進行互動。	`EDRKATA`（預設）是 EDR (KATA) 整合模式。允許啟用與 Kaspersky Endpoint Detection and Response (KATA) 整合，Kaspersky Endpoint Detection and Response (KATA) 是 Kaspersky Anti Targeted Attack Platform 的元件。 `EDRExpertOnPrem` 是 EDR Expert (on-premises) 整合模式。啟用 Kaspersky Endpoint Detection and Response Expert (on-premises) 整合

設定	描述	值
UseClientPinnedCertificate	啟用或停用雙向身分驗證，以增強與 OSMP 威脅回應操作伺服器連線的安全性。 如果 OSMP 威脅回應伺服器端已啟用雙向身分驗證，您需要在 *Kaspersky Endpoint Detection and Response Expert (on-premises) 整合*工作的設定中啟用雙向身分驗證，並在啟動工作前新增用戶端憑證。	Yes 會啟用雙向身分驗證，以提高與 OSMP 威脅回應動作伺服器連線的安全性。 No（預設值）— 不使用雙向身分驗證。
SynchronizationPeriod	向 OSMP 威脅回應操作伺服器發送同步請求的週期（以分鐘為單位）。	預設值：5。
ConnectionTimeout	等待連接到 OSMP 威脅回應操作伺服器的最長時間（以秒鐘為單位）。	預設值：10。
RequestTimeout	等待 OSMP 威脅回應操作伺服器回應的最長時間（以秒鐘為單位）。	預設值：10。
EnableTelemetry	將裝置上事件的相關資料（遙測資料）傳送到 OSMP 遙測資料收集伺服器。	Yes（預設值）啟用向 OSMP 遙測伺服器傳送遙測資料。 No 停用傳送遙測資料。
[Endpoints.item_#]部分包含 OSMP 威脅回應伺服器的位址和連接埠。您可以新增多個伺服器。		
Address	OSMP 威脅回應操作伺服器位址。 可指定 Integration Server 的 IP 位址（IPv4 或 IPv6）或完全限定網域名稱 (FQDN)。 為確保在裝置上啟用網路隔離的情況下應用程式發生故障時與伺服器的通訊不會中斷，我們建議指定伺服器的 IP 位址。	預設值：127.0.0.1。
Port	用於連線到 OSMP 威脅回應伺服器的連接埠。	預設值：443。
[TelemetrySettings]部分包含用於連線到 OSMP 遙測伺服器的一般設定。		
UseClientPinnedCertificate	啟用或停用雙向身分驗證，以增強與 OSMP 遙測伺服器連線的安全性。 如果 OSMP 遙測伺服器端已啟用雙向身分驗證，您需要在 *Kaspersky Endpoint Detection and Response Expert (on-premises) 整合*工作的設定中啟用雙向身分驗證，並在啟動工作前新增用戶端憑證。	Yes 會啟用雙向身分驗證，以提高與 OSMP 遙測伺服器連線的安全性。 No（預設值）— 不使用雙向身分驗證。
ConnectionTimeout	等待連接到 OSMP 遙測伺服器的最長時間（以秒鐘為單位）。	預設值：10。
RequestTimeout	等待 OSMP 遙測伺服器回應的最長時間（以秒鐘為單位）。	預設值：10。
OnlyTaggedEvents	僅傳送含 IOA 的遙測資料。*攻擊指標 (IOA)* 是指包含系統中可疑行為（指示可能存在針對性攻擊）描述的規則。應用程式會將系統中正在進行的行為與這些規則進行比較，並記錄下指示存在針對性攻擊的事件。應用程式使用*串流掃描*技術，該技術允許即時追蹤此類事件。	Yes — 僅在偵測到攻擊指標 (IOA) 時傳送遙測資料。 No（預設值）— 傳送所有遙測資料。
[TelemetrySettings.Endpoints.item_#]部分包含 OSMP 遙測伺服器的位址和連接埠。您可以新增多個伺服器。		
Address	OSMP 遙測伺服器憑證位址 可指定 Integration Server 的 IP 位址（IPv4 或 IPv6）或完全限定網域名稱 (FQDN)。 為確保在裝置上啟用網路隔離的情況下應用程式發生故障時與伺服器的通訊不會中斷，我們建議指定伺服器的 IP 位址。	預設值：127.0.0.1。
Port	用於連線 OSMP 遙測伺服器的連線埠。	預設值：443。
[TelemetrySettings.EventTransferSettings]部分包含資料傳輸到 OSMP 遙測伺服器的設定。		
MaximumDataTransferTime	向 OSMP 遙測伺服器傳送事件的最大延遲時間（以秒鐘為單位）。	預設值：30。
UseRequestCountLimits	限制請求數量。該功能有助於最佳化伺服器負載。如果啟用此功能，應用程式會限制傳輸的事件。如果事件數量超過配置的限制，Kaspersky Endpoint Security 將停止傳送事件。	Yes（預設值）— 調節傳送的事件數量。 No — 不調節事件的數量。

設定	描述	值
MaximumNumberOfEventsInHour	每小時的最大事件數量	預設值：3000。
MaximumNumberOfEventsInPackage	一個套件中的最大事件數量。	預設值：1024。
EventLimitExceededPercentage	事件數量超過限制（百分比）。如果某種類型的事件佔事件總數的比例超過配置的閾值（百分比），則傳送事件會受到限制。	預設值：15。

管理用於連線到 OSMP EDR Expert (on-premises) 伺服器的憑證

管理憑證需要具有管理員(admin) 角色的使用者的權限。

您可以使用指令來管理用於連線到 OSMP 伺服器的憑證。您可以使用憑證執行以下操作：

- 新增或取代 OSMP 伺服器的憑證：威脅回應伺服器和遙測伺服器
- 顯示關於伺服器憑證的資訊
- 刪除伺服器憑證
- 新增或取代用於防護與 OSMP 伺服器（威脅回應伺服器和遙測伺服器）連線的用戶端憑證。
- 顯示有關於用戶端憑證的資訊
- 刪除客戶端憑證

管理用於與 OSMP威脅回應伺服器連線的憑證

若要新增或者取代威脅回應操作伺服器憑證，請執行以下命令：

```
kesl-control [-R] --add-kataedr-server-certificate <file> --server-type response
```

其中 `<file>` 是包含伺服器憑證的檔案路徑。

若要新增或取代用於威脅回應伺服器連線的用戶端憑證：

1. 執行以下指令：

   ```
   kesl-control [-R] --add-kataedr-client-certificate <file> --server-type response
   ```

   其中 `<file>` 是包含用戶端憑證和私密金鑰的加密容器（PFX 封存檔）的路徑。

2. 輸入加密容器密碼

如果已在 OSMP 伺服器設定中啟用用戶端憑證驗證，並且在 *Kaspersky Endpoint Detection and Response Expert (on-premises) 整合* 工作設定 中，`[KATAEDR]` 區段內的 `UseClientPinnedCertificate` 設定值為 `yes`，則用戶端憑證會用於為與 OSMP 伺服器的連線提供額外防護。

若要顯示有關威脅回應操作伺服器憑證的資訊，請執行以下命令：

```
kesl-control [-R] --query-kataedr-server-certificate --server-type response
```

若要顯示用於防護與威脅回應操作伺服器連線的用戶端憑證訊息，請執行下列命令：

```
kesl-control [-R] --query-kataedr-client-certificate --server-type response
```

執行該指令將顯示以下憑證資訊：

- 憑證序號
- 憑證主體
- 憑證發佈者
- 憑證開始日期
- 憑證到期日期
- SHA1 和 SHA256 憑證指紋

若要刪除威脅回應操作伺服器憑證，請執行以下命令：

```
kesl-control [-R] --remove-kataedr-server-certificate --server-type response
```

若要刪除用於防護與威脅回應操作伺服器連線的用戶端憑證，請執行下列命令：

```
kesl-control [-R] --remove-kataedr-client-certificate --server-type response
```

管理用於連線 OSMP 遙測伺服器的憑證

若要新增或取代遙測伺服器的憑證，請執行以下命令：

```
kesl-control [-R] --add-kataedr-server-certificate <file> --server-type telemetry
```

其中 `<file>` 是包含伺服器憑證的檔案路徑。

若要新增或替換用於遙測伺服器連線的用戶端憑證：

1. 執行以下指令：

```
kesl-control [-R] --add-kataedr-client-certificate <file> --server-type telemetry
```

   其中 `<file>` 是包含用戶端憑證和私密金鑰的加密容器（PFX 封存檔）的路徑。

2. 如果加密容器受密碼防護，請在提示時輸入密碼。

> 如果已在 OSMP 伺服器設定中啟用用戶端憑證驗證，並且在 *Kaspersky Endpoint Detection and Response Expert (on-premises) 整合* 工作設定 中，`[TelemetrySettings]` 區段內的 `UseClientPinnedCertificate` 設定值為 `yes`，則用戶端憑證會用於為與 OSMP 伺服器的連線提供額外防護。

若要顯示有關遙測伺服器憑證的資訊，請執行以下命令：

```
kesl-control [-R] --query-kataedr-server-certificate --server-type telemetry
```

若要顯示用於防護與遙測伺服器連線的用戶端憑證資訊，請執行下列命令：

```
kesl-control [-R] --query-kataedr-client-certificate --server-type telemetry
```

執行該指令將顯示以下憑證資訊：

- 憑證序號
- 憑證主體
- 憑證發佈者
- 憑證開始日期
- 憑證到期日期
- SHA1 和 SHA256 憑證指紋

若要刪除遙測伺服器憑證，請執行以下指令：

```
kesl-control [-R] --remove-kataedr-server-certificate --server-type telemetry
```

若要刪除用於防護與遙測伺服器連線的用戶端憑證，請執行下列命令：

```
kesl-control [-R] --remove-kataedr-client-certificate --server-type telemetry
```

卡巴斯基 Endpoint Detection and Response Expert (cloud) 整合

您可以透過命令列上的 *卡巴斯基 Endpoint Detection and Response Expert (cloud) 整合* 預定義工作，管理 Kaspersky Endpoint Security 與卡巴斯基 Endpoint Detection and Response Expert (cloud) 解決方案之間的整合。

您可以透過編輯預定義工作的設定，管理卡巴斯基 Endpoint Detection and Response Expert (cloud) 整合設定。

*卡巴斯基 Endpoint Detection and Response Expert (cloud) 整合*工作預設不會執行。您可以手動啟動和停止工作。

卡巴斯基 Endpoint Detection and Response Expert (cloud) 整合設定

下表說明 Kaspersky Endpoint Detection and Response Expert (cloud) 整合預定義工作 (`EDRExpertCloud`) 的設定。

如何取得工作的目前設定值

```
kesl-control --get-settings 39
```

如何設定工作設定

```
kesl-control --set-settings 39 <parameter>=<value>
```

卡巴斯基 Endpoint Detection and Response Expert (cloud) 整合設定

設定	描述
回應伺服器整合設定	
`UseTunnel`	使用 TCP 隧道連線至回應伺服器。如果您基礎架構中的安全性政策不允許您直接連線至伺服器，則會使用 TCP 隧道連線至伺服器。 預設為停用使用 TCP 隧道 (`No`)。
`TunnelAddress`	用於連線至隧道的伺服器位址 (IPv4 或 IPv6)。
`TunnelPort`	用於連線至隧道的伺服器連接埠。
`SynchronizationPeriod`	向 OSMP 威脅回應操作伺服器發送同步請求的週期（以分鐘為單位）。 預設值：`5`。
遙測資料收集伺服器整合設定 `[TelemetrySettings]` 區段包含用於連線至 OSMP 遙測伺服器的一般設定。	
`EnableTelemetry`	將裝置上事件的相關資料（遙測資料）傳送到 OSMP 遙測資料收集伺服器。 預設會啟用遙測傳送 (`Yes`)。
`OnlyTaggedEvents`	僅傳送含 IOA 的遙測資料。*攻擊指標 (IOA)* 是指包含系統中可疑行為（指示可能存在針對性攻擊）描述的規則。應用程式會將系統中正在進行的行為與這些規則進行比較，並記錄下指示存在針對性攻擊的事件。應用程式使用*串流掃描*技術，該技術允許即時追蹤此類事件。 預設會停用僅傳送含 IOA 的遙測資料 (`No`)。
`UseTunnel`	使用 TCP 隧道連線至遙測資料收集伺服器。如果您基礎架構中的安全性政策不允許您直接連線至伺服器，則會使用 TCP 隧道連線至伺服器。 預設為停用使用 TCP 隧道 (`No`)。
`TunnelAddress`	用於連線至隧道的伺服器位址 (IPv4 或 IPv6)。
`TunnelPort`	用於連線至隧道的伺服器連接埠。
`[TelemetrySettings.EventTransferSettings]` 區段包含用於連線至 OSMP 遙測伺服器的一般設定。	

設定	描述
`UseRequestCountLimits`	限制請求數量。該功能有助於最佳化伺服器負載。如果啟用此功能，應用程式會限制傳輸的事件。如果事件數量超過配置的限制，Kaspersky Endpoint Security 將停止傳送事件。 預設會停用此選項。
`MaximumDataTransferTime`	傳送事件時的最大延遲。應用程式在同步間隔到期後與伺服器同步以傳送事件。預設設定是 30 秒。
`MaximumNumberOfEventsInHour`	每小時事件數量上限。應用程式會分析遙測資料流，如果事件流超過設定的每小時事件數限制，則限制事件的傳送。Kaspersky Endpoint Security 在一小時後還原傳送事件。預設設定是每小時 3000 個事件。如果應用程式安裝在伺服器上，則遙測資料流會更高。對於伺服器，建議將該值增加到每小時 60,000 個事件。
`MaximumNumberOfEventsInPackage`	套件中事件的最大數量。當緩衝區充滿事件時，應用程式會與伺服器同步。預設設定為 1024 個事件。
`EventLimitExceededPercentage`	事件節流閾（百分比）。該應用程式按類型對事件進行排序（例如，“登錄檔中的變更”事件），如果相同類型的事件佔事件總數的比率超過配置的百分比限制，則限制事件的傳輸。當其他事件與事件總數的比率再次變得足夠大時，Kaspersky Endpoint Security 會還原傳送事件。預設設定為 15%。

管理 OSMP EDR Expert 伺服器 (cloud) 連線憑證

管理憑證需要具有管理員(admin) 角色的使用者的權限。

應用程式會在您接受卡巴斯基 Endpoint Detection and Response Expert (cloud) 資料處理協議的條款與條件後，自動接收用於建立受信任連線的伺服器位址和憑證。因此，您無法使用命令新增或移除憑證。您只能在命令列中顯示憑證相關資訊。

管理用於與 OSMP威脅回應伺服器連線的憑證

若要顯示威脅回應伺服器憑證的相關資訊

```
kesl-control [-R] --query-cloudxdr-server-certificate --server-type response
```

若要顯示用於威脅回應伺服器連線的用戶端憑證相關資訊

```
kesl-control [-R] --query-cloudxdr-client-certificate --server-type response
```

執行該指令將顯示以下憑證資訊：

- 憑證序號
- 憑證主體
- 憑證發佈者
- 憑證開始日期
- 憑證到期日期
- SHA1 和 SHA256 憑證指紋

管理用於連線 OSMP 遙測伺服器的憑證

顯示遙測收集伺服器憑證的相關資訊

```
kesl-control [-R] --query-cloudxdr-server-certificate --server-type telemetry
```

若要顯示用於遙測伺服器連線的用戶端憑證相關資訊

```
kesl-control [-R] --query-cloudxdr-client-certificate --server-type telemetry
```

執行該指令將顯示以下憑證資訊：

- 憑證序號
- 憑證主體
- 憑證發佈者
- 憑證開始日期
- 憑證到期日期
- SHA1 和 SHA256 憑證指紋

Kaspersky Endpoint Detection and Response (KATA) 整合

您可以透過命令列上的 *Kaspersky Endpoint Detection and Response Expert (on-premises) 整合*（ `KATAEDR` ）預定義工作，管理 Kaspersky Endpoint Security 與 Kaspersky Endpoint Detection and Response (KATA) 元件之間的整合。

> 此工作也可讓您管理 Kaspersky Endpoint Detection and Response Expert (on-premises) 整合設定。若要與 Kaspersky Endpoint Detection and Response (KATA) 整合，您需要在工作設定中選擇 EDR (KATA) 整合模式，並視需要管理整合設定。

您可以透過編輯預定義工作設定來配置Kaspersky Endpoint Detection and Response (KATA) 整合設定。

*Kaspersky Endpoint Detection and Response Expert (on-premises) 整合*工作預設不會執行。您可以手動啟動和停止工作。

您可以使用 EDR Expert (on-premises) 元件管理指令管理憑證，這些憑證用於連線到 KATA 伺服器。

Kaspersky Endpoint Detection and Response (KATA) 整合設定

下表說明 Kaspersky Endpoint Detection and Response Expert (on-premises)（ `KATAEDR` ）整合預定義工作的設定，您可以在與 Kaspersky Endpoint Detection and Response (KATA) 整合時管理這些設定。

> 此工作也可讓您管理 Kaspersky Endpoint Detection and Response Expert (on-premises) 整合設定。要與 Kaspersky Endpoint Detection and Response (KATA) 整合，您需要在工作設定中選擇 *EDR (KATA)* 整合模式（ `Mode=EDRKATA` ）。

設定	描述	值
Mode	整合模式。 對於 Kaspersky Endpoint Detection and Response Expert (on-premises) 整合，Kaspersky Endpoint Security 應用程式會與 OSMP 平台上的伺服器互動。 對於 Kaspersky Endpoint Detection and Response (KATA) 整合，Kaspersky Endpoint Security 安全應用程式與 Kaspersky Anti Targeted Attack Platform 上的伺服器進行互動。	EDRKATA（預設）是 EDR (KATA) 整合模式。允許啟用與 Kaspersky Endpoint Detection and Response (KATA) 整合，Kaspersky Endpoint Detection and Response (KATA) 是 Kaspersky Anti Targeted Attack Platform 的元件。 EDRExpertOnPrem 是 EDR Expert (on-premises) 整合模式。啟用 Kaspersky Endpoint Detection and Response Expert (on-premises) 整合
UseClientPinnedCertificate	啟用和停用雙向身分驗證以進一步防護與 KATA 伺服器的連線。 如果在 KATA 伺服器端啟用了雙向身分驗證，您需要在 *Kaspersky Endpoint Detection and Response Expert (on-premises) 整合* 工作的設定中啟用雙向身分驗證，並在啟動工作之前新增用戶端憑證。	Yes – 使用雙向身分驗證進一步防護與 KATA 伺服器的連線。 No（預設值）— 不使用雙向身分驗證。
SynchronizationPeriod	向 KATA 伺服器傳送同步請求的頻率（以分鐘為單位）。	預設值：5。
ConnectionTimeout	等待連線到 KATA 伺服器的最長時間（秒）。	預設值：10。
RequestTimeout	等待 KATA 伺服器回應的最長時間（秒）。	預設值：10。
EnableTelemetry	將事件資料（遙測）傳送至 KATA。	Yes（預設值）– 將遙測資料傳送到 KATA 伺服器。 No 停用傳送遙測資料。
[Endpoints.item_#]部分包含 KATA 伺服器的位址和連接埠。您可以新增多個伺服器。		
Address	KATA 伺服器位址 可指定 Integration Server 的 IP 位址（IPv4 或 IPv6）或完全限定網域名稱 (FQDN)。 為確保在裝置上啟用網路隔離的情況下應用程式發生故障時與伺服器的通訊不會中斷，我們建議指定伺服器的 IP 位址。	預設值：127.0.0.1。
Port	連線 KATA 伺服器的連線埠。	預設值：443。
[EventTransferSettings]部分包含將資料傳送到 KATA 伺服器的設定。		
MaximumDataTransferTime	向 KATA 伺服器傳送事件的最大延遲（以秒為單位）。	預設值：30。
UseRequestCountLimits	啟用和停用調節傳送到 KATA 伺服器的事件數量。	Yes（預設值）— 調節傳送的事件數量。 No — 不調節事件的數量。
MaximumNumberOfEventsInHour	每小時的最大事件數量	預設值：3000。
MaximumNumberOfEventsInPackage	一個套件中的最大事件數量。	預設值：1024。
EventLimitExceededPercentage	事件數量超過限制（百分比）。如果某種類型的事件佔事件總數的比例超過配置的閾值（百分比），則傳送事件會受到限制。	預設值：15。

管理用於連線 KATA 伺服器的憑證

管理憑證需要具有管理員(admin) 角色的使用者的權限。

您可以使用指令來管理用於連線至 KATA 伺服器的憑證。您可以使用憑證執行以下操作：

- 新增或替換 KATA 伺服器憑證
- 顯示關於伺服器憑證的資訊
- 刪除伺服器憑證
- 刪除或替換用於防護與 KATA 伺服器連線的用戶端憑證
- 顯示有關於用戶端憑證的資訊
- 刪除用戶端憑證

若要新增或取代伺服器憑證，請執行下列指令：

```
kesl-control [-R] --add-kataedr-server-certificate <file>
```

其中 `<file>` 是包含伺服器憑證的檔案路徑。

若要新增或變更用戶端憑證：

1. 執行以下指令：

   ```
   kesl-control [-R] --add-kataedr-client-certificate <file>
   ```

   其中 `<file>` 是包含用戶端憑證和私密金鑰的加密容器（PFX 封存檔）的路徑。

2. 輸入加密容器密碼

> 如果 KATA 伺服器設定中已啟用用戶端憑證驗證，且在 *Kaspersky Endpoint Detection and Response Expert (on-premises) 整合* 工作設定中，`UseClientPinnedCertificate` 設為 `yes`，則會使用用戶端憑證為與 KATA 伺服器的連線提供額外防護。

若要顯示伺服器憑證資訊，請執行以下指令：

```
kesl-control [-R] --query-kataedr-server-certificate
```

若要顯示用戶端憑證資訊，請執行以下指令：

```
kesl-control [-R] --query-kataedr-client-certificate
```

執行該指令將顯示以下憑證資訊：

- 憑證序號
- 憑證主體
- 憑證發佈者

- 憑證開始日期
- 憑證到期日期
- SHA1 和 SHA256 憑證指紋

若要刪除伺服器憑證資訊，請執行以下指令：

```
kesl-control [-R] --remove-kataedr-server-certificate
```

若要刪除用戶端憑證資訊，請執行以下指令：

```
kesl-control [-R] --remove-kataedr-client-certificate
```

Kaspersky Network Detection and Response (KATA) 整合

您可以在命令列上透過 *Kaspersky Network Detection and Response (KATA) 整合*（ `KATANDR` ）預定義工作，管理卡巴斯基安全網路與 Kaspersky Endpoint Detection and Response (KATA) 之間的整合：

*Kaspersky Network Detection and Response (KATA) 整合*預設不執行。您可以手動啟動和停止工作。

您可以透過編輯預定義工作設定來配置Kaspersky Network Detection and Response (KATA) 整合設定。

您可以使用NDR (KATA) 元件管理指令來管理用於連線到 NDR 伺服器的憑證。

Kaspersky Network Detection and Response (KATA) 整合設定

此表說明您可以為 Kaspersky Network Detection and Response (KATA) 整合工作（ `KATANDR` ）指定的所有可用設定，以及所有設定的預設值。

Kaspersky Network Detection and Response (KATA) 整合工作設定

設定	描述	值
`UseClientPinnedCertificate`	啟用和停用雙向身分驗證以進一步防護與 NDR 伺服器的連線。 如果在 NDR 伺服器端啟用了用戶端憑證驗證，請在啟動*Kaspersky NetworkDetection and Response (KATA) 整合*工作之前啟用用戶端憑證使用並新增用戶端憑證。	`Yes` – 使用雙向身分驗證進一步防護與 NDR 伺服器的連線。 `No`（預設值）– 不使用雙向身分驗證。
`SynchronizationPeriod`	向 NDR 伺服器傳送同步請求的頻率（以分鐘為單位）。	預設值：`5`。
`ConnectionTimeout`	等待連線到 NDR 伺服器的最長時間（秒）。	預設值：`10`。
`RequestTimeout`	等待 NDR 伺服器回應的最長時間（秒）。	預設值：`10`。
[Endpoints.item_#]部分包含 NDR 伺服器的位址和連接埠。		
`Address`	NDR 伺服器位址 可指定 Integration Server 的 IP 位址（IPv4 或 IPv6）或完全限定網域名稱 (FQDN)。	預設值：`127.0.0.1`。
`Port`	連線 NDR 伺服器的連線埠。	預設值：`8081`。
[EventTransferSettings]部分包含將事件傳送到 NDR 伺服器的設定。		
`MaximumDataTransferTime`	向 NDR 伺服器傳送事件的最大延遲（以秒為單位）。	預設值：`30`。
`MaximumNumberOfEventsInPackage`	一個套件中的最大事件數量。	預設值：`1024`。

設定	描述	值
UseRequestCountLimits	啟用和停用調節傳送到 NDR 伺服器的事件數量。	Yes（預設值）— 調節傳送的事件數量。 No — 不調節事件的數量。
MaximumNumberOfEventsInHour	每小時的最大事件數量	預設值：3000。
EventLimitExceededPercentage	事件節流閾（百分比）。如果某種類型的事件佔事件總數的比例超過配置的閾值（百分比），則傳送事件會受到限制。	預設值：15。
PingPeriod	NDR 伺服器輪詢週期（秒）。	預設值：450。

管理用於連線 NDR 伺服器的憑證

管理憑證需要具有管理員(admin) 角色的使用者的權限。

您可以使用指令來管理用於連線至 NDR 伺服器的憑證。您可以使用憑證執行以下操作：

- 新增或替換 NDR 伺服器憑證
- 顯示關於伺服器憑證的資訊
- 刪除伺服器憑證
- 刪除或替換用於保護與 NDR 伺服器連線的用戶端憑證
- 顯示有關於用戶端憑證的資訊
- 刪除用戶端憑證

若要新增或取代伺服器憑證，請執行下列指令：

```
kesl-control [-R] --add-katandr-server-certificate <file>
```

其中 `<file>` 是包含伺服器憑證的檔案路徑。

若要新增或變更用戶端憑證：

1. 執行以下指令：

   ```
   kesl-control [-R] --add-katandr-client-certificate <file>
   ```

   其中 `<file>` 是包含用戶端憑證和私密金鑰的加密容器（PFX 封存檔）的路徑。

2. 輸入加密容器密碼

如果在 NDR 伺服器設定中啟用了用戶端憑證驗證，且在 *Kaspersky Network Detection and Response (KATA) 整合* 工作設定中將 `UseClientPinnedCertificate` 設定設為 `yes`，則會使用用戶端憑證為與 NDR 伺服器的連線提供額外防護。

若要顯示伺服器憑證資訊，請執行以下指令：

```
kesl-control [-R] --query-katandr-server-certificate
```

若要顯示用戶端憑證資訊，請執行以下指令：

```
kesl-control [-R] --query-katandr-client-certificate
```

執行該指令將顯示以下憑證資訊：

- 憑證序號
- 憑證主體
- 憑證發佈者
- 憑證開始日期
- 憑證到期日期
- SHA1 和 SHA256 憑證指紋

若要刪除伺服器憑證資訊，請執行以下指令：

```
kesl-control [-R] --remove-katandr-server-certificate
```

若要刪除用戶端憑證資訊，請執行以下指令：

```
kesl-control [-R] --remove-katandr-client-certificate
```

Sandbox 整合

在指令列上，您可以使用*Sandbox 整合*預定義工作來管理 Kaspersky Endpoint Security 應用程式與 Sandbox 的整合。

預設情況下，*Sandbox 整合*工作未執行。您可以手動啟動和停止此工作。

若要啟動 Sandbox 整合 工作，請執行下列指令：

```
kesl-control --start-task 29
```

> 如果尚未新增伺服器憑證，則無法啟動*與 Sandbox 整合*工作。

如果 *Sandbox 整合* 工作已啟動，且 其選取的模式允許手動傳送檔案以進行掃描（ Manual 或 AutoAndManual ），您可以從命令列將要掃描的檔案傳送至沙盒。

如何將檔案傳送至沙盒進行掃描

```
kesl-control [-X] --sandbox <path>
```

其中 <path> 是您要掃描的檔案或目錄路徑。您可以指定多個路徑，以空格分隔。

您可以透過編輯預定義工作的設定來配置 Sandbox 整合設定。

透過使用KATA Sandbox 整合設定管理命令，您可以管理用於連線至負責與 Sandbox 伺服器互動的伺服器的憑證。

Sandbox 整合設定

下表說明您可以為 Sandbox 整合工作（ Standalone_Sandbox ）指定的所有可用設定，以及所有設定的預設值。

如何設定 Sandbox 整合設定

```
kesl-control --set-settings 29 Servers.item_0000.Address=<server> Servers.item_0000.Port=<port> [<setting name>=
<setting value>]
```

Sandbox 整合工作設定

設定	描述	值
UseClientCertificate	啟用和停用雙向身分驗證以進一步防護與 Sandbox 伺服器的連線。 如果在 Sandbox 伺服器端啟用了用戶端憑證驗證，請在啟動 *Sandbox 整合*工作之前啟用用戶端憑證的使用並新增用戶端憑證。	Yes – 使用雙向身分驗證進一步防護與沙盒伺服器的連線。 No（預設值）— 不使用雙向身分驗證。
ConnectionTimeout	等待與伺服器連線的最長時間（以秒為單位）。	預設值：10。
RequestTimeout	等待伺服器回應的最長時間（以秒為單位）。	預設值：10。
SendingMode	將物件傳送到 Sandbox 進行掃描的模式	AutoOnly（預設值）— 當嘗試存取檔案時，自動傳送檔案進行掃描. Manual — 手動傳送檔案進行掃描。 AutoAndManual — 自動和手動傳送檔案進行掃描。
QuarantineFile	偵測到威脅時隔離區檔案。	Yes（預設值）– 如果偵測到威脅，則刪除原始檔案，並將檔案副本放入隔離區。 No— 偵測到威脅時不隔離檔案。
ScanCriticalAreas	偵測到威脅時，執行關鍵區域掃描。	Yes（預設值）– 偵測到威脅時啟動關鍵區域掃描。 No – 偵測到威脅時不啟動關鍵區域掃描。
CreateIocScanTask	偵測到威脅時建立IOC 掃描工作。	Yes（預設值）– 偵測到威脅時建立 IOC 掃描工作。 No – 偵測到威脅時不建立 IOC 掃描工作。
QuarantineFileOnIocDetected	偵測到入侵指標時隔離物件。	Yes（預設值）– 如果偵測到入侵指標，則刪除原始物件，並將物件的副本置於隔離區。 No – 偵測到入侵指標時，不隔離物件。
ScanCriticalAreasOnIocDetected	偵測到入侵指標時，執行關鍵區域掃描。	Yes（預設值）– 偵測到入侵指標時啟動關鍵區域掃描。 No – 偵測到入侵指標時不啟動關鍵區域掃描。

設定	描述	值
`Drives`	IoC 掃描範圍。	`Critical`（預設）— 掃描使用者和系統目錄中的檔案。 `System` — 掃描根檔案系統中的所有檔案。
`ScheduleMode`	IOC 掃描工作啟動模式。	`Manually`（預設）– 手動啟動 IOC 掃描工作。 `AfterTreatDetected` – 偵測到威脅後啟動 IOC 掃描工作。
[Servers.item_#]部分包含 Sandbox 伺服器的設定。		
`Address`	伺服器的位址。 可指定 Integration Server 的 IP 位址（IPv4 或 IPv6）或完全限定網域名稱 (FQDN)。	預設值：`127.0.0.1`。
`Port`	用於連線至伺服器的連接埠。	預設值：`443`。
[SandboxTransferSettings]部分包含在 Sandbox 中傳送檔案進行掃描的設定。		
`SandboxQueue`	掃描請求佇列的最大大小（以兆位元組為單位）。	預設值：`1024`。

管理用於連線 Sandbox 伺服器的憑證

管理憑證需要具有管理員(admin) 角色的使用者的權限。

您可以使用指令管理用於連線到 OSMP 伺服器或負責與沙盒互動的 Central Node 伺服器（以下也稱為沙盒伺服器）的憑證。您可以使用憑證執行以下操作：

- 新增或替換伺服器憑證
- 顯示關於伺服器憑證的資訊
- 刪除伺服器憑證
- 新增或替換用戶端憑證
- 顯示有關於用戶端憑證的資訊
- 刪除用戶端憑證

若要新增或取代伺服器憑證，請執行下列指令：

```
kesl-control [-X] --add-sandbox-server-certificate <file>
```

其中 `<file>` 是包含伺服器憑證的檔案路徑。

若要新增或變更用戶端憑證：

1. 執行以下指令：

```
kesl-control [-X] --add-sandbox-client-certificate <file>
```

   其中 `<file>` 是包含用戶端憑證和私密金鑰的加密容器（PFX 封存檔）的路徑。

2. 輸入加密容器密碼

> 如果在沙盒伺服器設定中啟用了用戶端憑證驗證，且在 *Sandbox 整合* 工作的 設定 中，`UseClientCertificate` 設為 `yes`，則用戶端憑證會用於為與沙盒伺服器的連線提供額外防護。

若要顯示憑證訊息，請執行以下指令：

- 對於伺服器憑證：

```
kesl-control [-X] --query-sandbox-server-certificate
```

- 對於用戶端憑證：

```
kesl-control [-X] --query-sandbox-client-certificate
```

  執行該指令將顯示以下憑證資訊：

- 憑證序號
- 憑證主體
- 憑證發佈者
- 憑證開始日期
- 憑證到期日期
- SHA1 和 SHA256 憑證指紋

若要刪除伺服器憑證資訊，請執行以下指令：

```
kesl-control [-X] --remove-sandbox-server-certificate
```

若要刪除用戶端憑證資訊，請執行以下指令：

```
kesl-control [-X] --remove-sandbox-client-certificate
```

啟用或停用 Kaspersky Endpoint Detection and Response Optimum 整合

您可以使用一般應用程式設定中的 `UseEdrOptimum` 設定來啟用或停用 EDR Optimum 元件。

您可以藉助命令列開關或包含所有一般應用程式設定的設定檔來變更設定的值。

使用命令列選項啟用 EDR Optimum 元件：

```
kesl-control --set-app-settings UseEdrOptimum=Yes
```

使用命令列選項停用 EDR Optimum 元件：

```
kesl-control --set-app-settings UseEdrOptimum=No
```

配置 Kaspersky Managed Detection and Response 整合

在指令列中，您可以執行以下操作：

- 啟用或停用 MDR 元件。
- 上傳或刪除包含 Kaspersky Managed Detection and Response 產品授權資訊的 MDR BLOB 檔案。

  如果使用產品授權金鑰啟動 MDR 元件，則無需上傳 MDR BLOB 檔案。

我們建議在管理主控台或網頁主控台中配置 Kaspersky Endpoint Security 與 Kaspersky Managed Detection and Response 之間的整合。

您可以編輯一般應用程式設定中的 `UseMDR` 選項來啟用或停用 MDR 元件。您可以藉助命令列開關或包含所有一般應用程式設定的設定檔來變更設定的值。

`UseMDR` 參數可以採用下列值：

- `Yes` 表示啟用 MDR 元件。
- `No` 表示停用 MDR 元件。

如果您啟用 MDR 元件，且卡巴斯基安全網路已停用或在基礎模式下使用，則系統會顯示錯誤訊息並且不會啟用 MDR 元件。若要啟用 MDR 元件，您必須在延伸模式下啟用 KSN。

您可以使用產品授權金鑰管理命令上傳或刪除 MDR BLOB 檔案。您可以在 MDR 設定檔的 ZIP 壓縮檔案中找到 BLOB 檔案。

若要上傳 BLOB 設定檔，請執行以下命令：

```
kesl-control --load-mdr-blob <path to the MDR BLOB>
```

若要刪除 BLOB 檔案，請執行以下命令：

```
kesl-control --remove-mdr-blob
```

啟用整合可建立每天執行一次的`Mdr_Autostart_Scan`服務工作。

管理裝置網路隔離

與 Detection and Response 解決方案整合時，在命令列中，您可以：

- 檢查裝置的網路隔離狀態並檢視網路隔離排除項目清單。
- 停用裝置的網路隔離。

若要停用裝置的網路隔離，請執行以下命令：

```
kesl-control [-R] --isolation-off
```

若要檢查網路隔離狀態並檢視網路隔離排除項目清單，請執行以下命令：

```
kesl-control [-R] --isolation-stat
```

系統會顯示下列網路隔離狀態之一：

- *網路隔離已啟用*。
- *網路隔離已停用*。

管理隔離區設定

在指令列中，您可以使用一般應用程式設定中的`QuarantineSizeLimit`、`QuarantineFillingNotification`和`QuarantineBackupFolder`設定來配置隔離區。

您可以藉助指令列開關或包含所有一般應用程式設定的設定檔來變更設定值。

隔離設定

設定	描述	值
`QuarantineFillingNotification`	必須已滿才能產生關於隔離區已滿的事件的隔離區百分比。 若要停用產生關於隔離區已滿的事件，請輸入 0。	0 至 100 0 — 產生關於隔離區已滿的事件被停用。 預設值：90。

設定	描述	值
`QuarantineSizeLimit`	隔離區的最大大小（以兆位元組為單位）。當達到最大隔離區大小時，應用程式將刪除最舊的檔案。 若要使隔離區的大小不受限制，請輸入 0。	0 至 4000 0 表示隔離區大小不受限制。 如果應用程式在標準模式或 EDR Agent 模式下使用，則預設值為 200；如果應用程式在 Light Agent 模式下使用，則預設值為 100。
`QuarantineBackupFolder`	儲存備份和隔離物件的目錄的路徑。您可以指定與預設目錄不同的目錄。您可以使用任何裝置上的目錄作為儲存備份和隔離物件的目錄。不建議指派位於遠端裝置（例如透過 Samba 和 NFS 協定安裝的裝置）上的目錄。 如果指定的目錄不存在或不可用，應用程式將使用預設目錄。	預設值：/var/opt/kaspersky/kesl/common/objects-backup/ 存取預設目錄需要 root 權限。

透過指令列管理被隔離的檔案

與 Detection and Response 解決方案整合時，您可以在命令列上使用隔離區管理命令來執行以下操作：

- 將檔案放入隔離區（僅與Kaspersky Endpoint Detection and Response Optimum或Kaspersky Managed Detection and Response整合時）。
- 檢視關於被隔離的檔案的資訊。
- 從隔離區中刪除所有檔案或指定的檔案。
- 從隔離區還原檔案。

還原感染檔案可能會導致裝置感染。

隔離檔案

若要隔離檔案，請執行以下指令：

```
kesl-control [-Q] --put <path to the file> [--md5] [--sha256] [--save-original-file]
```

其中：

- `<path to the file>` 是您要隔離的檔案路徑。
- `--md5` 是您要隔離的檔案的 MD5 雜湊值。
- `--sha256` 是您要隔離的檔案的 SHA256 雜湊值。
- `--save-original-file` 保留原始檔案。如果不指定此選項，則原始檔案將被刪除。

  只有當使用者帳戶具有刪除物件的權限時，才會刪除原始檔案。如果權限不足，則會顯示檔案刪除錯誤訊息。

只有與Kaspersky Endpoint Detection and Response Optimum或Kaspersky Managed Detection and Response整合時，您才可以使用此命令。

檢視關於被隔離檔案的資訊

要檢視關於被隔離檔案的資訊，請執行以下指令：

```
kesl-control -Q --query ["<filter conditions>"] [-n <number of files>] [--json]
```

其中：

- `<filter conditions>` 指定一個或多個 邏輯運算式，格式為 `< 欄位 > < 比較運算 > '< 值 >'`，並使用 `and` 邏輯運算子組合，以限制查詢結果。如果您不指定任何篩選條件，應用程式將顯示所有被被隔離檔案的詳細資訊。
- `<number of files>` 是您要顯示之最近隔離檔案的數量。如果不指定 `-n` 選項，則顯示最後 30 個檔案。指定 0 則顯示所有檔案。
- `--json`：以 JSON 格式輸出資料。

`ObjectId` 行顯示應用程式在隔離檔案時指派給該檔案的數字 ID。此 ID 用於對檔案執行操作，例如還原檔案或將其從隔離區中刪除。

從隔離區還原檔案

若要將隔離區中的檔案以其原始名稱還原到原始位置，請執行下列命令：

```
kesl-control -Q --restore <object identifier>
```

其中 `<object identifier>` 是應用程式在檔案被隔離時指派給該檔案的數字 ID。

若要將隔離區中的檔案以新名稱還原到指定目錄，請執行下列命令：

```
kesl-control -Q --restore <object identifier> --file <path to the file>
```

其中 --file `<path to the file>` 是檔案的新名稱，以及您要儲存檔案的目錄路徑。

只有當您的使用者擁有 root 權限時，您才可以將檔案從隔離區還原到其他目錄。如果您的使用者權限不足，則只能將檔案還原到原始位置。

在封閉軟體環境模式下的 Astra Linux 裝置上，您只能使用將檔案放入備份時所使用的相同帳戶來還原檔案。還原檔案時，應用程式會建立 MAC 標籤為 3（cnnr 旗標）的目錄。

從隔離區刪除檔案

若要從隔離區刪除選定的檔案，請執行下列指令：

```
kesl-control -Q --mass-remove --query "<filter conditions>"
```

其中 `<filter conditions>` 指定一個或多個 邏輯運算式，格式為 <field><comparison operation>'<value>'，並使用 "and" 邏輯運算子組合，以限制查詢結果。

刪除名稱或路徑中包含「`test`」的檔案範例

```
kesl-control -Q --mass-remove --query "FileName like '%test%'"
```

若要從隔離區中刪除所有檔案，請執行以下指令：

```
kesl-control -Q --mass-remove
```

搜尋入侵指標

只有在與 Kaspersky Endpoint Detection and Response Optimum 整合時，您才可以使用命令列中的 IOC 掃描工作掃描入侵指標。與 Kaspersky Endpoint Detection and Response (on-premises) 或 Kaspersky Endpoint Detection and Response (KATA) 整合時，IOC 掃描將在相關的 Detection and Response 解決方案端執行。

若要從指令列建立、設定和執行IOC 掃描工作，請執行以下指令：

```
kesl-control [-T] --scan-ioc --path <path to the directory or file> [--process on|off] [--hint <regular
expression>] [--arpentry on|off] [--ports on|off] [--system on|off] [--files on|off] [--drives
all|system|critical|custom] [--excludes <list of exclusions>] [--scope <list of directories>] [--action
Skip|QuarantineFile|IsolateHost|ScanCriticalAreas]
```

其中：

- `--path <path to the directory or file>` 是 IOC 檔案的路徑，或包含副檔名為 .IOC 或 .XML 之 IOC 檔案的目錄路徑，應用於執行掃描。

  您可以指定多個路徑，以空格分隔。您也可以指定兩種類型的路徑（檔案路徑和目錄路徑）。

- `--process` — 啟用對裝置上執行的處理程序的分析。

  可能的參數：

  - on — 啟用對裝置上執行的處理程序的分析（預設值）。
  - `off` — 停用對裝置上執行的處理程序的分析。

  如果不指定`--process`選項，則僅當使用的 IOC 檔案指定了這些處理程序的詳細資訊（`ProcessItem`）時，應用程式才會分析處理程序。

- `--hint <regular expression>` 是與要分析的檔案 (`FileItem`) 或處理程序可執行檔 (`ProcessItem`) 的完整路徑相符的正規運算式。

  您可以使用以下正規表達式元素：

  - 元字元：`. ^ $ |`
  - 字元類別：數字、字母、小寫、大寫、cntrl
  - 量詞：`* + ? {n} {n,} {n, m}`
  - 否定：`[^a-c]`
  - 逸出字元：`\a \e \f`，`\n \r \t \v \b`

- `--arpentry` — 啟用分析 ARP 表 (`ArpEntryItem`) 中的條目。

  可能的參數：

  - on — 啟用分析 ARP 表中的條目（預設值）。
  - off — 停用分析 ARP 表中的條目。

  如果不指定 `--arpentry` 選項，則僅當使用的 IOC 檔案指定了 ARP 表 (`ArpEntryItem`) 的詳細資訊時，應用程式才會分析 ARP 表。

  `--ports` — 啟用分析用於連線的開放連接埠。

  可能的參數：

  - on — 啟用分析用於連線的開放連接埠並掃描裝置上的活動連線（預設值）。
  - off — 停用分析用於連線的開放連接埠並且不掃描裝置上的活動連線。

  如果不指定 `--ports` 選項，則僅當使用的 IOC 檔案指定了這些連接埠的詳細資訊（`PortItem`）時，應用程式才會分析連接埠。

- `--system` — 啟用系統環境分析。

  可能的參數：

  - on — 啟用系統環境分析（預設值）。
  - off — 停用系統環境分析。

  如果不指定 `--system` 選項，則僅當使用的 IOC 檔案指定了系統環境 (`SystemInfoItem`) 的詳細資訊時，應用程式才會分析系統環境。

- `--files` — 啟用檔案分析。

  可能的參數：

  - on — 啟用檔案分析（預設值）。
  - off — 停用檔案分析。

  如果沒有指定 `--files` 選項，則僅當使用的 IOC 檔案指定了這些檔案的詳細資訊 (`FileItem`) 時，應用程式才會分析檔案。

- `--drives` — 要掃描的區域。

  可能的參數：

  - `all` — 檢查所有可用的檔案區域。
  - `system` — 掃描根檔案系統中的所有檔案。
  - `critical` — 掃描使用者和系統目錄中的檔案（預設值）。
  - `custom` — 僅掃描您指定區域中的檔案。

  如果您未指定`--drives`選項，應用程式將分析使用者和系統目錄中的檔案。

- `--excludes <list of exclusions>` 是排除在掃描範圍外的路徑清單。

  此選項指定的排除項目是全域的，並且無論範圍類型或目錄清單如何均有效。這些排除項目優先於其他指令列選項，包括`--hint`和`--scope`。

  > 排除項目被指定為路徑，但不能包含遞歸元素或通配符（例如`*`）。

  如果不指定`--excludes`選項，則掃描執行時將不進行排除。

  您可以指定多個排除項目，以空格分隔。

- `--scope <list of directories>` 是要掃描的其他目錄清單。

  > 如果您為 `custom` 選項指定了 `--drives` 參數，則需要此選項。

- `--action` — 當偵測到入侵指標時執行的操作。

  可能的參數：

  - `Skip` — 應用程式不會對偵測到的物件執行任何操作，但關於它的資訊將保存在工作執行結果中（預設值）。
  - `QuarantineFile` — 應用程式將隔離偵測到的物件。
  - `IsolateHost` — 應用程式對偵測到物件的裝置實施網路隔離。
  - `ScanCriticalAreas` – 應用程式將執行關鍵區域掃描。

    Kaspersky Endpoint Security 掃描的關鍵區域

    - /lib/systemd
    - /lib/udev
    - /lib/dbus-1.0
    - /usr/local/lib/systemd/user
    - /usr/share/dbus-1
    - /usr/share/gdm/autostart

- /usr/share/gnome/autostart
- /var/spool/at
- /var/spool/在/spool
- /var/spool/anacron
- /var/spool/cron
- /boot
- /bin
- /sbin
- /lib
- /lib32
- /lib64
- /libx32
- /usr/lib
- /usr/lib32
- /usr/lib64
- /usr/libx32
- ~/.config/autostart
- ~/.config/autostart-scripts
- ~/.config/plasma-workspace/env
- ~/.config/plasma-workspace/shutdown
- ~/.config/lxsession
- ~/.fluxbox/startup
- ~/.kde/Autostart
- /etc

您可以用逗號分隔來指定多個操作。

> 如果指定`Skip`參數，請不要新增任何其他參數。`Skip`參數只能單獨使用。

管理執行防護

執行防護可讓人管理可執行檔和指令碼的執行，以及開啟 Office 格式的檔案。執行防護使用執行防護規則管理使用者對檔案的存取。

物件執行防禦包含以下工作：

- *物件執行防禦（EDR Expert（on-premises））*（ `KATAEDR_Prevention` ）
- *物件執行防禦（EDR Expert (cloud)）*（ `EDRExpertCloud_Prevention` ）
- *物件執行防禦 (EDR Optimum)*（ `EDRO_Prevention` ）

預設情況下，不會啟動*物件執行防禦*工作。如果您已新增至少一個執行防禦規則，應用程式會啟動該工作。

若要檢視執行防禦規則清單，請執行以下指令：

```
kesl-control [-T] --get-prevention-state [--kata|cxdr|edro]
```

其中：

`--kata`：EDR Expert (on-premises) 元件的執行防禦規則清單
`--cxdr`：EDR Expert (cloud) 元件的執行防禦規則清單
`--edro`：EDR Optimum 元件的執行防禦規則清單

配置 KUMA 整合

在指令列中，您可以使用預定義工作：*卡巴斯基統一監控和分析平台整合*管理 Kaspersky Endpoint Security 與卡巴斯基統一監控和分析平台的整合。

預設情況下，*卡巴斯基統一監控和分析平台整合*工作未執行。您可以手動啟動和停止此工作。

您可以透過編輯預定義工作設定來配置卡巴斯基統一監控和分析平台整合設定。

透過使用用於管理卡巴斯基統一監控和分析平台整合設定的指令，您可以管理用於連線 KUMA 伺服器的憑證。

Kaspersky Unified Monitoring and Analysis Platform 整合工作

此表說明您可以為 Kaspersky Unified Monitoring and Analysis Platform（ `KUMA` ）整合工作指定的所有可用設定，以及所有設定的預設值。

設定	描述	值
UseTls	啟用或停用伺服器憑證驗證，以對與 KUMA 伺服器的連線提供額外防護。	Yes — 使用憑證進一步防護與 KUMA 伺服器的連線。 No（預設）— 不使用憑證來防護與 KUMA 伺服器的連線。
UseClientCertificate	啟用和停用雙向身分驗證以進一步防護與 KUMA 伺服器的連線。 如果在 KUMA 伺服器端啟用了用戶端憑證驗證，請在啟動卡巴斯基統一監控和分析平台整合工作之前啟用用戶端憑證的使用並新增用戶端憑證。	Yes – 使用雙向身分驗證進一步防護與 KUMA 伺服器的連線。 No（預設值）— 不使用雙向身分驗證。
ConnectionTimeout	等待連線到 KUMA 伺服器的最長時間（秒）。	預設值：5。
[Servers.item_#]部分包含 KUMA 伺服器的設定。		
ServerAddress	KUMA 伺服器位址 可指定 Integration Server 的 IP 位址（IPv4 或 IPv6）或完全限定網域名稱 (FQDN)。 如果設定 UseTls=Yes，則必須從購買授權時收到的憑證指定伺服器的完全限定網域名稱 (FQDN) 才能使用 KUMA。	預設值：127.0.0.1。
ServerPort	連線 KUMA 伺服器的連線埠。	預設值：443。
ServerProtocol	用於連線到 KUMA 伺服器的協定。	tcp（預設值）— 使用 TCP 協定連線到 KUMA 伺服器。 HTTPWithCompression — 使用 HTTP 協定及事件壓縮連線至 KUMA 伺服器。 udp — 使用 UDP 協定連線到 KUMA 伺服器。 當選取 UDP 協定時，不支援使用憑證來提供連線保護（系統會忽略 UseTls、UseClientCertificate 和 ConnectionTimeout 設定的值），且不會產生與 KUMA 伺服器連線相關的事件。
[KumaTransferSettings] 區段包含將事件傳送至 KUMA 伺服器的設定。		
EventTransferTimeMax	向 KUMA 伺服器傳送事件的最大延遲（以秒為單位）。	預設值：30。

管理用於連線 KUMA 伺服器的憑證

選擇 UDP 協定時，不支援使用憑證提供連線防護。

管理憑證需要具有管理員(admin) 角色的使用者的權限。

您可以使用指令來管理用於連線至 KUMA 伺服器的憑證。您可以使用憑證執行以下操作：

- 新增或替換伺服器憑證
- 顯示關於伺服器憑證的資訊
- 刪除伺服器憑證
- 新增或替換用戶端憑證

- 顯示有關於用戶端憑證的資訊
- 刪除用戶端憑證

若要新增或取代伺服器憑證，請執行下列指令：

```
kesl-control [-M] --add-kuma-server-certificate <path to the file>
```

其中 `<path to the file>` 是檔案路徑，該檔案包含 DER 或 PEM 格式的伺服器憑證。

若要新增或變更用戶端憑證：

1. 執行以下指令：

   ```
   kesl-control [-M] --add-kuma-client-certificate <path to the file>
   ```

   其中 `<path to the file>` 是包含用戶端憑證和私密金鑰的加密容器（PFX 封存檔）的路徑。

2. 輸入加密容器密碼

> 如果在 KUMA 伺服器設定中啟用了用戶端憑證驗證，且在 *與 Kaspersky Unified Monitoring and Analysis Platform 整合*的工作設定中將 `UseClientCertificate` 設定設為 `yes`，則會使用用戶端憑證，為與 KUMA 伺服器的連線提供額外防護。

若要顯示憑證訊息，請執行以下指令：

- 對於伺服器憑證：

  ```
  kesl-control [-M] --query-kuma-server-certificate
  ```

- 對於用戶端憑證：

  ```
  kesl-control [-M] --query-kuma-client-certificate
  ```

  執行該指令將顯示以下憑證資訊：

- 憑證序號
- 憑證主體
- 憑證發佈者
- 憑證開始日期
- 憑證到期日期
- SHA1 和 SHA256 憑證指紋

若要刪除伺服器憑證資訊，請執行以下指令：

```
kesl-control [-M] --remove-kuma-server-certificate
```

若要刪除用戶端憑證資訊，請執行以下指令：

```
kesl-control [-M] --remove-kuma-client-certificate
```

一般設定

在管理主控台中，您可以在政策內容（**一般設定**）中管理定義應用程式整體運作和個別功能運作的一般應用程式設定。

一般應用程式設定

下表說明一般應用程式設定，這些設定會控管整個應用程式的運作以及各個功能的運作。

一般應用程式設定

設定	描述	參數值
`SambaConfigPath`	儲存 Samba 設定檔的目錄。需要 Samba 設定檔來確保 `AllShared` 或 `Shared:SMB` 值可用於 `Path` 設定。 變更此設定後必須重新啟動應用程式。	電腦上 SAMBA 設定檔的標準目錄已預設指定。 預設值：/etc/samba/smb.conf。
`NfsExportPath`	儲存 NFS 設定檔的目錄。需要 NFS 設定檔來確保 `AllShared` 或 `Shared:NFS` 值可用於 `Path` 設定。 變更此設定後必須重新啟動應用程式。	電腦上 NFS 設定檔的標準目錄已預設指定。 預設值：/etc/exports。
`TraceFolder`	儲存應用程式偵錯檔案的目錄。 變更此設定後必須重新啟動應用程式。	預設值：/var/log/kaspersky/kesl。 存取預設的偵錯檔案目錄需要 root 權限。如果您指目錄，請確保只有 root 對此目錄具有讀取和寫入權或 `rwx-------` 權限）。
`TraceLevel`	啟用應用程式偵錯以及偵錯檔案中的詳細程度。 此設定僅啟用應用程式偵錯檔案的產生。若要為圖形介面和 kesl-control 命令列公用程式產生偵錯檔案，您需要設定 LFS_ENABLE_ALL_COMPONENTS_LOGGING 環境變數。	`Detailed` – 產生詳細的應用程式偵錯檔案。 `MediumDetailed` – 產生包含資訊訊息和錯誤訊息偵錯檔案。 `NotDetailed` – 產生包含錯誤訊息的應用程式偵錯 `None`（預設值）– 不產生應用程式偵錯檔案。
`TraceMaxFileCount`	應用程式偵錯檔案的最大數量。 變更此設定後必須重新啟動應用程式。	1–10000 預設值：10。

設定	描述	參數值
TraceMaxFileSize	指定應用程式偵錯檔案的最大大小（以兆位元組為單位）。 變更此設定後必須重新啟動應用程式。	1–1000 預設值：500。
WdTraceLevel	啟用Watchdog 伺服器偵錯並設定偵錯檔案中的詳細程度。	Detailed – 產生詳細的 Watchdog 伺服器偵錯檔案 MediumDetailed – 產生包含資訊訊息和錯誤訊息 Watchdog 伺服器偵錯檔案。 NotDetailed – 產生包含錯誤訊息的 Watchdog 伺 檔案。 None – 不產生 Watchdog 伺服器偵錯檔案。 Product（預設值）– 將此值設為與 TraceLevel
BlockFilesGreaterMaxFileNamePath	阻止存取完整路徑長度超出以位元組為單位指定的定義設定值的檔案。如果被掃描檔案的完整路徑長度超出此設定的值，掃描工作將在掃描過程中跳過此檔案。 此設定僅適用於不支援 fanotify 的作業系統。 變更此設定的值後，需要重新啟動檔案威脅防護工作。	4096–33554432 預設值：16384。
DetectOtherObjects	啟用偵測入侵者可以用來破壞裝置或資料的合法應用程式。	Yes：啟用偵測入侵者可以用來破壞裝置或資料的 式。 No（預設）：停用偵測入侵者可以用來破壞裝置或 法應用程式。
NamespaceMonitoring	啟用命名空間和容器的掃描。 除非作業系統中安裝了用於處理容器和命名空間的元件，否則應用程式不會掃描命名空間和容器。	Yes（預設值）啟用命名空間和容器的掃描。 No 停用命名空間和容器的掃描。
FileBlockDuringScan	啟用檔案操作攔截模式，在掃描期間阻止對檔案的存取。檔案操作攔截模式會影響 檔案威脅防護與 裝置控制元件、物件的執行防禦動作，以及 卸除式磁碟機掃描工作。	Yes（預設值）— 在掃描期間封鎖對檔案的存取。 No 則允許在掃描期間存取檔案。允許對任何檔案的 描非同步完成。此檔案操作攔截模式在掃描期間對 影響較小，但檔案中的威脅可能無法被解毒或刪除 描期間，與此檔案關聯的程序在應用程式判定此檔 成功重新命名該檔案，則可能會發生這種情況。然 脅防護、裝置控制、執行防禦元件，以及卸除式磁 作，無論選取何種操作模式，都會以通知模式運作
UseKSN	為應用程式設定卡巴斯基安全網路。	Basic — 允許在標準模式下使用卡巴斯基安全網路 Extended — 允許在延伸模式下使用卡巴斯基安全 No（預設值）— 不使用卡巴斯基安全網路。
CloudMode	啟用雲端模式。如果啟用 KSN，則可以使用雲端模式。 如果打算使用雲端模式，請確保您的裝置上可使用 KSN。 此設定僅當應用程式在標準模式下使用時才適用。	Yes（預設值）— 啟用 Kaspersky Endpoint Securit 級版本的惡意軟體資料庫的操作模式。 No（預設值）— 使用惡意軟體資料庫的完整版本。 如果停用 KSN，雲端模式也會自動停用。

設定	描述	參數值
UseMDR	啟用 Managed Detection and Response 元件以便與 Kaspersky Managed Detection and Response整合。 如果您啟用 MDR 元件，且卡巴斯基安全網路已停用或在基礎模式下使用，則系統會顯示錯誤訊息並且不會啟用 MDR 元件。若要啟用 MDR 元件，您必須在延伸模式下啟用 KSN。 此設定不適用於配備 Elbrus CPU 的裝置。	Yes — 啟用 Managed Detection and Response 元件 No（預設值）— 停用 Managed Detection and Resp 件。
UseEdrOptimum	啟用 EDR Optimum 元件以便與 Kaspersky Endpoint Detection and Response Optimum整合。 此設定不適用於配備 Elbrus CPU 的裝置。	Yes — 啟用 EDR Optimum 元件。 No（預設）— 停用 EDR Optimum 元件。
UseProxy	允許 Kaspersky Endpoint Security 元件使用代理伺服器。代理伺服器可用於存取卡巴斯基啟動伺服器、資料庫和應用程式模組的更新來源、卡巴斯基安全網路，以及使用 Web 威脅防護元件驗證網站憑證。 如果 Kaspersky Endpoint Security 是以 Light Agent 模式使用，則不支援使用代理伺服器連線至卡巴斯基安全網路、SVM 和 Integration Server。	Yes：啟用代理伺服器的使用。 No（預設）— 停用代理伺服器的使用。
ProxyServer	用於連線網際網路的代理伺服器位址。 透過 HTTP 代理連線時，我們建議使用不用於登入其他系統的單獨帳戶。HTTP 代理程式使用不安全的連線，帳戶可能會受到損害。	代理伺服器位址採用以下格式之一： • [<connection protocol>://]<address o proxy server>:<port>，如果連線到代理伺 身分驗證； • [<connection protocol>://][<user name [<password>]@]<address of the proxy s <port>，如果連線到代理伺服器需要身分驗證 IPv6 位址時，請將其輸入方括號中。 不支援透過 HTTPS 連線到代理伺服器。
ProxyBypass	要繞過代理伺服器的位址清單。	位址以 <address>[:<port>] 格式指定。若要指定 可以使用遮罩（* 符號）以及 \ 符號後面的註釋。
ProxyBypassEdr	連線到 Kaspersky Endpoint Detection and Response Expert (on-premises) Integration Server 時是否使用代理伺服器。 此設定不適用於配備 Elbrus CPU 的裝置。	Yes 以在連線到 Kaspersky Endpoint Detection and Expert (on-premise) 整合伺服器時不使用代理伺服 No（預設值）以在連線到 Kaspersky Endpoint Det Response Expert (on-premise) 整合伺服器時使用代 器。

設定	描述	參數值
ProxyBypassNdr	連線到 Kaspersky Network Detection and Response (KATA) Integration Server 時是否使用代理伺服器。 此設定不適用於配備 Elbrus CPU 的裝置。	Yes — 連線到 Kaspersky Endpoint Detection and R (KATA) Integration Server 時不使用代理伺服器。 No（預設值）— 連線到 Kaspersky Endpoint Detec Response (KATA) Integration Server 時使用代理伺
ProxyBypassSandbox	連線到提供與 Sandbox 互動的伺服器時是否使用代理伺服器。 此設定不適用於配備 Elbrus CPU 的裝置。	Yes，在連線到提供與 Sandbox 互動的伺服器時續 器。 No（預設值），在連線到提供與 Sandbox 互動的 用代理伺服器。
MaxEventsNumber	應用程式儲存的最大事件數。當超過指定的事件數時，應用程式將刪除最早的事件。	預設值：500000。 如果值為 0，則不儲存新事件，但會刪除較早的事
LimitNumberOfScanFileTasks	非特權使用者可以在裝置上同時啟動的自訂掃描工作的最大數量。此設定不會限制具有 root 權限或 kesladmin 角色的使用者可啟動的工作數量。	0–100000 0 表示非特權使用者不能啟動自訂掃描工作。 預設值：100。
UseSyslog	啟用將應用程式事件記錄到 syslog。 存取 syslog 需要 root 權限。	Yes：啟用將事件儲存到 syslog。 No（預設）：禁止將事件儲存到 syslog。
EventsStoragePath	事件記錄資料庫主要檔案的路徑。 存取預設事件資料庫需要 root 權限。	預設值： /var/opt/kaspersky/kesl/private/storage/
ExcludedMountPoint.item_#	從掃描範圍中排除的掛載點。排除適用於檔案威脅防護、加密軟體防護和容器監控元件以及卸除式磁碟機掃描工作的操作，並且還在 ODS 和 ContainerScan 掃描工作的操作中進行了配置。 您可以指定多個要從掃描中排除的掛載點。 掛載點的指定方式必須與 mount 指令輸出中顯示的方式相同。 預設情況下，ExcludedMountPoint.item_# 設定未指定。	AllRemoteMounted — 將使用 SMB 和 NFS 協定安 的所有遠端目錄從檔案操作攔截中排除。 Mounted:NFS — 將使用 NFS 協定安裝在裝置上的 錄從檔案操作攔截中排除。 Mounted:SMB — 將使用 SMB 協定安裝在裝置上的 錄從檔案操作攔截中排除。 Mounted:<file system type>：將所有具有指 類型的已掛載目錄從檔案操作攔截中排除。 /mnt — 將 /mnt 掛載點（包括子目錄）中的物件排 操作攔截之外。此目錄用作卸除式磁碟機的臨時掛 <path that contains the /mnt/user*|/mnt/**/user_share>：將掛載點 指定遮罩的物件從檔案操作攔截中排除。
MemScanExcludedProgramPath.item_#	從掃描中排除處理程序記憶體。 應用程式不會掃描指示處理程序的記憶體。	<full path to process> — 從掃描中排除指定 件。您可以使用遮罩來指定路徑。
PowerSaveMode	取消使用電池供電的裝置上的排程工作。	Yes（預設值）會在裝置使用電池供電時跳過已排 No 會執行已排程工作，無論裝置是否使用電池供
UseOnDemandCPULimit	啟用 *ODS*、*容器掃描* 和 *清查掃描*-類型工作的 CPU 使用率限制。	Yes：為 *ODS*、*ContainerScan* 和 *InventoryScan* 工 使用率限制。 No（預設）：停用工作的 CPU 使用率限制。
OnDemandCPULimit	執行 *ODS*、*容器掃描* 和 *清查掃描*-類型工作時，所有處理器核心的最高使用率（百分比）。	10 到 100 的整數值。 預設值：100。
BackupSizeLimit	最大備份大小（MB）。當達到最大備份儲存大小時，應用程式將刪除檔案的最舊備份副本。 若要刪除備份大小限制，請設定 0。	0 至 4000 0–無限大小。 預設值：0。

設定	描述	參數值
`BackupDaysToLive`	將物件儲存在備份儲存中的時間段（以天為單位）。指定時間過去後，應用程式將刪除最舊的檔案備份副本。 若要刪除物件保留限制，請設定 0。	0 至 10000 0–無限制保留。 預設值：30。
`QuarantineSizeLimit`	隔離區的最大大小（以兆位元組為單位）。當達到最大隔離區大小時，應用程式將刪除最舊的檔案。 若要使隔離區的大小不受限制，請輸入 0。 此設定不適用於配備 Elbrus CPU 的裝置。	0 至 999999 0 表示隔離區大小不受限制。 如果應用程式在標準模式下使用，則預設值為 200 程式在 Light Agent 模式下使用，則預設值為 100。
`QuarantineFillingNotification`	必須已滿才能產生關於隔離區已滿的事件的隔離區百分比。 若要停用產生關於隔離區已滿的事件，請輸入 0。 此設定不適用於配備 Elbrus CPU 的裝置。	0 至 100 0 — 產生關於隔離區已滿的事件被停用。 預設值：90。
`QuarantineBackupFolder`	儲存檔案備份副本和隔離檔案的目錄的路徑。 您可以變更預設目錄。如果指定的目錄不存在或不可用，應用程式將使用預設目錄。 此設定不適用於配備 Elbrus CPU 的裝置。使用 `BackupFolder` 設定。	預設值： `/var/opt/kaspersky/kesl/common/objects-b` 存取預設目錄需要 root 權限。
`BackupFolder`	備份目錄的路徑。 您可以變更預設目錄。如果指定的目錄不存在或不可用，應用程式將使用預設目錄。	預設值：`/var/opt/kaspersky/kesl/common/ob` `backup/` 存取預設備份儲存目錄需要 root 權限。
`ShowPopUpNotifications`	啟用在圖形使用者介面中顯示彈出通知。	`Yes`（預設值）— 在圖形使用者介面中顯示彈出通 `No`——不在圖形使用者介面中顯示彈出通知。
`InterceptorMode`	Kaspersky Endpoint Security 所使用的系統事件攔截機制： 此設定僅適用於執行支援 fanotify 技術的作業系統的裝置。 此設定不適用於配備 Elbrus CPU 的裝置。	`UseFanotify`（預設）– 使用 fanotify 技術攔截系 `UseUpdatableKernelModule` – 使用可更新內核模 統事件。
`InterceptorFallbackStrategy`	如果可更新的內核模組未能啟動，應用程式會採取的動作。 此設定僅適用於執行支援 fanotify 技術的作業系統的裝置。	`FallbackToFanotify`（預設）– 切換到 fanotify 件攔截。 `FallbackToLimitedMode` – 不使用系統事件攔截 程式不使用系統事件攔截，則不會執行即時檔案掃 置的保護等級會降低。

設定	描述	參數值
`InterceptorApplyStrategy`	如果應用程式切換到使用可更新的內核模組，則必須重新啟動應用程式才能啟動該模組。此設定可讓您指定是希望自動重新啟動應用程式還是希望手動重新啟動應用程式。 此設定僅適用於執行支援 fanotify 技術的作業系統的裝置。	`RestartServiceAutomatically` 會自動重新啟動式，以啟動可更新的內核模組。建議使用此設定。 `RestartServiceManually`（預設）會在使用者手動應用程式後，啟動可更新的內核模組。
`SystemEventsTransmission`	啟用傳輸來自第三方應用程式（非卡巴斯基解決方案）的事件資訊。如果啟用此設定，除了本身的事件之外，Kaspersky Endpoint Security 也會將第三方應用程式的 systemd-journald 事件傳送到應用程式事件記錄。 存取 systemd-journald 需要 root 權限。	`Yes` 會啟用將第三方應用程式的 systemd-journald 輸到應用程式事件記錄。 `No`（預設）會停用將第三方應用程式的 systemd-j件資訊傳輸到應用程式事件記錄。
`UrgentUpdateRestartEnabled`	在安裝應用程式後的前 24 小時之後，收到關鍵更新時自動重新啟動應用程式。	`Yes` 以在收到關鍵更新時自動重新啟動應用程式。 `No`（預設值）以在收到關鍵更新時不重新啟動應用
`CoreDumps`	當應用程式發生故障時啟用傾印檔案的建立。	`Yes` 以在應用程式當機時建立傾印檔案。 `No`（預設值）以在應用程式當機時不建立傾印檔案
`CoreDumpsPath`	儲存傾印檔案的目錄路徑。	預設值： `/var/opt/kaspersky/kesl/common/dumps` 存取預設傾印檔案目錄需要 root 權限。

實用文章

如何指定遮罩

您可以使用 `*`（星號）字元來建立檔案或目錄名稱遮罩。

您可以指示單一 `*` 字元來表示檔案或目錄名稱中 `/` 字元前面的任意字元集（包括空集）。例如，`/dir/*/file` 或 `/dir/*/*/file`。

您可以用兩個連續的 `*` 字元來表示檔案或目錄名稱中的任意一組字元（包括空集和 `/` 字元）。例如，`/dir/**/file*/` 或 `/dir/file**/`。

`**` 遮罩在目錄名稱中只能使用一次。例如，`/dir/**/**/file` 是一個不正確的遮罩。

您可以使用單一 `?` 字元來表示檔案或目錄名稱中的任意一個字元。

工作排程

下表說明您可針對所有應用程式工作管理的工作排程設定。

設定	描述
RuleType	工作啟動排程。 • Once：執行工作一次。 • Monthly：每月在指定的日期和時間執行工作。 • Weekly：每週在指定的日期和時間執行工作。 • Daily：依照指定的天數間隔定期執行工作。 • Hourly：從指定的日期和時間開始，按照指定的小時間隔定期執行工作。 • Minutely：從指定時間開始，按照指定的分鐘間隔定期執行工作。 • Manual — 手動啟動工作。 • PS — 啟動應用程式後啟動工作。 • BR — 應用程式資料庫更新後啟動工作。
StartTime	工作開始日期和時間。此設定的格式取決於 RuleType。 可能的值： • <year>:1970 至 2099 • <month>:JAN，FEB，MAR，APR，MAY，JUN，JUL，AUG，SEP，OCT，NOV，DEC。 • <day of the month>:1 至 31 • <day of the week>:Mon，Tue，Wed，Thu，Fri，Sat，Sun。 • <hh>:0 至 23 • <mm>:0 至 59 • <ss>:0 至 59 • <interval between runs (in days)>:0 至 364 • <interval between runs (in hours)>:0 至 23 • <interval between runs (in minutes)>:0 至 59
RandomInterval	在特定時間間隔內（從 0 到指定值）隨機在電腦上執行工作。這樣可避免多個工作同時啟動。 預設值：99分鐘。 可用值：0 – 999。
RunMissedStartRules	應用程式啟動後執行錯過的工作。 • Yes（預設值）表示已啟用執行錯過的工作。如果排程工作執行時應用程式停止或電腦關機，Kaspersky Endpoint Security 會在應用程式啟動後立即啟動該工作。這樣可確保不會錯過任何關鍵工作。 • No 表示已停用執行錯過的工作。如果排程工作執行時應用程式停止或電腦關機，應用程式將略過該工作。這樣可避免在啟動應用程式時產生額外負載。
UseWorkingTimeout	達到 WorkingTimeout 設定指定的最大工作執行時間時停止工作。即使未完成，工作也會停止。下次工作啟動將按照排程進行。 • Yes — 達到最大工作執行時間時停止工作。 • No（預設值）— 達到最大工作執行時間時不停止工作。
WorkingTimeout	如果 UseWorkingTimeout=Yes，則應用程式停止執行工作後的最大工作執行時間（以分鐘為單位）。 預設值：120分鐘。 可用值：1 – 999。

配置代理伺服器設定

在命令列中，您可以使用 UseProxy、ProxyServer、ProxyBypass、ProxyBypassEdr、ProxyBypassNdr 及 ProxyBypassSandbox 一般應用程式設定來管理應用程式元件的代理伺服器設定。

您可以藉助指令列開關或包含所有一般應用程式設定的設定檔來變更設定值。

UseProxy 參數可以採用下列值：

- Yes 會啟用代理伺服器的使用。
- No 會停用代理伺服器。

ProxyServer 設定可讓您以 `<connection protocol>://[<user>[:<password>]@]<proxy server address>:<port number>` 格式指定代理伺服器設定，其中：

- `<user>` 是在代理伺服器上進行身分驗證的使用者名稱。
- `<password>` 是在代理伺服器上進行身分驗證的使用者密碼。
- `<proxy server address>` 是代理伺服器的 IP 位址或網域名稱。
- `<port number>` 是代理伺服器的連接埠號碼。

不支援透過 HTTPS 連線到代理伺服器。

透過 HTTP 代理連線時，我們建議使用不用於登入其他系統的單獨帳戶。HTTP 代理程式使用不安全的連線，帳戶可能會受到損害。

借助 `ProxyBypass` 設定，您可以指定無需代理伺服器即可連線的位址清單。位址以 `<address>[:<port number>]` 格式指定。要指定位址，您可以使用遮罩（`*`符號）和註釋（在 \ 符號之後）。

以下設定可讓您設定 EDR Expert (on-premises)、NDR (KATA) 和沙盒元件使用代理伺服器，這些元件可與 Detection and Response 解決方案整合：

- `ProxyBypassEdr` 設定會在連線至提供與 Kaspersky Endpoint Detection and Response Expert (on-premises) 或 Kaspersky Endpoint Detection and Response (KATA) 整合的伺服器時，啟用或停用代理伺服器的使用。
- `ProxyBypassNdr`設定用於啟用或停用當連線到提供與 Kaspersky Network Detection and Response (KATA) 整合的伺服器時使用代理伺服器。
- `ProxyBypassSandbox` 設定可以啟用或停用當連線到提供與 Sandbox 互動的伺服器時使用代理伺服器。

此設定可以採用以下值：

- `Yes` 會啟用代理伺服器的使用。
- `No` 會停用代理伺服器。

配置備份設定

在指令列中，您可以使用一般應用程式設定中的`BackupDaysToLive,`、`BackupSizeLimit`和`QuarantineBackupFolder`設定來配置備份設定。

您可以藉助指令列開關或包含所有一般應用程式設定的設定檔來變更設定值。

備份設定

設定	描述	值
`BackupDaysToLive`	將物件儲存在備份儲存中的時間段（以天為單位）。指定時間過去後，應用程式將刪除最舊的檔案備份副本。 若要刪除物件保留限制，請設定 0。	0 至 10000 0–無限制保留。 預設值：30。

設定	描述	值
BackupSizeLimit	最大備份大小（MB）。當達到最大備份儲存大小時，應用程式將刪除檔案的最舊備份副本。 若要刪除備份大小限制，請設定 0。	0 至 4000 0–無限大小。 預設值：0。
QuarantineBackupFolder	儲存檔案備份副本和隔離檔案的目錄的路徑。 您可以變更預設目錄。如果指定的目錄不存在或不可用，應用程式將使用預設目錄。 此設定不適用於配備 Elbrus CPU 的裝置。使用 BackupFolder 設定。	預設值：/var/opt/kaspersky/kesl/common/objects-backup/ 存取預設目錄需要 root 權限。
BackupFolder	備份目錄的路徑。 您可以變更預設目錄。如果指定的目錄不存在或不可用，應用程式將使用預設目錄。	預設值：/var/opt/kaspersky/kesl/common/objects-backup/ 存取預設備份儲存目錄需要 root 權限。

網路流量掃描設定

網路流量掃描設定

設定	描述	參數值
EncryptedConnectionsScan	啟用或停用加密連線掃描。 對於 FTP 協定，加密連線掃描預設被停用。	Yes（預設值）— 啟用加密連線掃描。 No — 停用加密連線掃描。應用程式不會解密加密的流量。
EncryptedConnectionsScanErrorAction	指定當網站上發生加密連線掃描錯誤時要執行的操作。	AddToAutoExclusions（預設值）— 將發生錯誤的網域加入包含掃描錯誤的網域清單。當造訪此網域時，應用程式將不會監控加密的 Web 流量。 Disconnect — 封鎖網路連線。
CertificateVerificationPolicy	指定 Kaspersky Endpoint Security 檢查憑證的方式。 如果憑證是自簽署的，則應用程式不會執行額外驗證。	FullCheck（預設值）— 應用程式使用網際網路檢查並下載驗證憑證所需的缺失鏈。 LocalCheck — 應用程式不會使用網際網路來驗證憑證。
UntrustedCertificateAction	偵測到未確認的憑證時所採取的操作。	Allow（預設值）— 允許在存取具有不受信任憑證的網域時建立網路連線。 Block — 封鎖在存取具有不受信任憑證的網域時建立的網路連線。
ManageExclusions	掃描加密流量時使用排除項目。	Yes – 不掃描 [Exclusions.item_#] 下指定的網站（請參閱下方）。 No（預設值）— 掃描所有網站。
MonitorNetworkPorts	指定 Kaspersky Endpoint Security 監控網路連接埠的方式。	Selected（預設值）— 僅監控 [NetworkPorts.item_#] 部分中指定的網路連接埠（請參閱下方）。 All — 監控所有網路連接埠。 指定此值可能會顯著增加作業系統負載。

設定	描述	參數值
NetInterceptorMode	Kaspersky Endpoint Security 應用程式的流量攔截模式。 此設定不適用於配備 Elbrus CPU 的裝置。	UseEBPF — 使用 eBPF 技術攔截流量。 UseIPTables（預設值）— 使用 iptables 實用程式攔截流量。 若要變更流量攔截模式，需要重新啟動應用程式。重新啟動會中斷已建立的網路連線。
[Exclusions.item_#]部分包含從掃描中排除的網域。應用程式不會掃描造訪指定網域時建立的連線。		
DomainName	指定網域名稱。	您可以在指定網域時使用遮罩。
[IncomingEndpointsExclusions.item_#]部分包含入站流量的排除項目。		
RemoteIp	遠端裝置的 IP 位址，其流量將被排除在攔截範圍之外。	
DestinationPort	受防護裝置上的連接埠，來自遠端裝置的流量將被排除在攔截範圍之外。	
[OutgoingEndpointsExclusions.item_#]部分包含出站流量的排除項目。		
RemoteIp	遠端裝置的 IP 位址，其流量將被排除在攔截範圍之外。	
DestinationPort	受防護裝置上的連接埠，來自受防護裝置的流量將被排除在攔截範圍之外。	
[NetworkPorts.item_#]部分包含應用程式監控的網路連接埠。		
PortName	網路連接埠描述。	
Port	應用程式要監控的網路連接埠號碼。	1 – 65535. 預設值未定義。

配置全域排除

您可以透過 ExcludedMountPoint.item_# 中的ExcludedMountPoint.item_#選項在指令列中定義掛載點排除。

您可以藉助命令列開關或包含所有一般應用程式設定的設定檔來變更設定的值。

ExcludedMountPoint.item_# 參數可以採用下列值：

- AllRemoteMounted — 將使用 SMB 和 NFS 協定安裝在裝置上的所有遠端目錄從檔案操作攔截中排除。
- Mounted:NFS — 將使用 NFS 協定安裝在裝置上的所有遠端目錄從檔案操作攔截中排除。
- Mounted:SMB — 將使用 SMB 協定安裝在裝置上的所有遠端目錄從檔案操作攔截中排除。
- Mounted:<file system type>：將所有具有指定檔案系統類型的已掛載目錄從檔案操作攔截中排除。
- /mnt — 將 /mnt 掛載點（包括子目錄）中的物件排除在檔案操作攔截之外。此目錄用作卸除式磁碟機的臨時掛載點。
- <path containing the mask /mnt/user* or /mnt/**/user_share>：將掛載點中名稱包含指定遮罩的物件從檔案操作攔截中排除。

掛載點的指定方式必須與mount指令輸出中顯示的方式相同。

您可以指定多個要排除在掃描之外的掛載點。

實用文章

如何指定遮罩

您可以使用*（星號）字元來建立檔案或目錄名稱遮罩。

您可以指示單一*字元來表示檔案或目錄名稱中/字元前面的任意字元集（包括空集）。例如，/dir/*/file 或 /dir/*/*/file。

您可以用兩個連續的*字元來表示檔案或目錄名稱中的任意一組字元（包括空集和/字元）。例如，/dir/**/file*/ 或 /dir/file**/。

遮罩在目錄名稱中只能使用一次。例如，/dir//**/file是一個不正確的遮罩。

您可以使用單一?字元來表示檔案或目錄名稱中的任意一個字元。

密碼防護設定

您可以透過使用命令列選項或編輯設定檔來變更設定，授予或撤銷管理應用程式的權限。

密碼防護設定

設定	描述	值
StopProtection	停用防護元件。	Yes 允許使用者執行動作。 No 禁止使用者執行動作。
StopSecurityControl	停用控制元件	
StartProtection	啟用防護元件	
StartSecurityControl	啟用控制元件	
ApplicationSettings	設定應用程式	
ViewReports	檢視報告	
RestoreFromBackup	從備份還原	
RemoveLicenseKey	移除金鑰	
AddLicense	新增金鑰	
DisablePolicy	停用卡巴斯基安全管理中心政策	

管理主控台中的應用程式設定

您可以使用政策來設定 Kaspersky Endpoint Security。有關應用程式元件的詳細資訊，請參見相應章節。

資料庫更新

在管理主控台中，您可以使用更新工作來更新資料庫。

您可以建立並執行更新使用者工作。您可以透過編輯工作的設定來管理更新設定。

在更新工作的屬性中，於**更新來源**和**設定**區段中，您可以管理下表列出的設定。

更新工作部分的更新來源

設定	描述

更新來源	此表包含資料庫更新來源清單。在更新過程中，應用程式會依照表中出現的順序存取更新來源。
	該表包含以下列：
	• **來源位址**是更新來源的位址：
	  • **卡巴斯基更新伺服器**，卡巴斯基應用程式的資料庫更新在此發布（預設值）。
	  • **卡巴斯基安全管理中心**— 卡巴斯基安全管理中心管理伺服器。
	  • 由使用者新增的來自本機或全域網路上的其他來源：HTTP、HTTPS 或 FTP 伺服器或本機網路伺服器上的目錄。
	• **狀態**指示更新來源是否在工作中使用（**使用中**或**未使用**）。您可以在點擊**編輯**按鈕時開啟的**更新來源**視窗中，選取或清除**使用此來源**核取方塊來變更狀態。
	您可以在表格中新增、編輯、刪除、上移或下移更新來源。

更新工作設定部分

設定	描述
更新來源回應逾時（秒）。	應用程式等待所選更新來源回應的最長時間（以秒為單位）。如果此時仍未收到任何回應，則會在工作記錄中記錄與更新來源失去通訊的事件。 可用值：0–120。如果指定 0，則應用程式等待所選來源的回應的時間段不受限制。 預設值：10 秒。
應用程式更新下載模式	在下拉清單中，您可以選擇自動安裝的更新（自動修補程式）的下載方式： • **不下載**。選擇此項目時，不會自動下載自動修補程式。 • **僅下載**。選擇此清單項目時，自動修補程式會自動下載，但不安裝在用戶端裝置上（預設設定）。 • **下載並安裝**。選擇此清單項目時，自動修補程式會自動下載並安裝在用戶端裝置上。自動修補程式安裝後，應用程式將自動重新啟動。

主機威脅防護

檔案威脅防護

在管理主控台中，您可以在政策屬性（**關鍵威脅防護 → 檔案威脅防護**）中管理檔案威脅防護。

檔案威脅防護元件設定

設定	描述
啟用檔案威脅防護	此核取方塊可啟用或停用所有受管理裝置上的檔案威脅防護元件。 預設情況下已選擇此核取方塊。
檔案威脅防護模式	在此下拉清單中，您可以選擇檔案威脅防護元件模式： • **智慧檢查**（預設值）— 當嘗試開啟檔案時掃描檔案；如果檔案已被修改，則嘗試關閉檔案時再次掃描。如果某個處理程序在一定時間內多次存取並修改某個檔案，則僅當該處理程序最後一次關閉該檔案時，應用程式才會再次掃描該檔案。 • **開啟時**— 在嘗試開啟檔案進行讀取、執行或修改時掃描檔案。 • **開啟和修改時**— 嘗試開啟檔案時掃描檔案，如果檔案已被修改，則嘗試關閉檔案時再次掃描。

設定	描述
掃描	這組設定包含開啟視窗的按鈕，您可以在其中配置掃描範圍和掃描設定。
偵測到威脅後的動作	這組設定包含**配置**按鈕。點擊此按鈕將開啟**偵測到威脅後的動作**視窗，您可以在其中設定應用程式對偵測到的感染物件執行的操作。

掃描範圍視窗

此表包含掃描範圍。該應用程式將掃描表中指定路徑中的檔案和目錄。預設情況下，該表包含一個掃描範圍，其中包括本機檔案系統的所有目錄。

掃描範圍設定

設定	描述
範圍名稱	掃描範圍名稱。
路徑	應用程式掃描的目錄的路徑。
狀態	狀態表示應用程式是否掃描此範圍。

您可以**新增**、**編輯**、**刪除**、**上移**和**下移**表項。

點擊"**向下移動**"按鈕可將選定的項目在表格中向下移動。

Kaspersky Endpoint Security 依照掃描範圍表中所列的順序掃描指定範圍內的物件。如果要為子目錄配置與父目錄的安全性設定不同的安全性設定，則必須在表中將子目錄置於高於其父目錄的位置。

如果在表中選擇了範圍，則此按鈕可用。

點擊"**向上移動**"按鈕可將選定的項目在表中上移。

Kaspersky Endpoint Security 依照掃描範圍表中所列的順序掃描指定範圍內的物件。如果要為子目錄配置與父目錄的安全性設定不同的安全性設定，則必須在表中將子目錄置於高於其父目錄的位置。

如果在表中選擇了範圍，則此按鈕可用。

點擊"**刪除**"按鈕可將選定的範圍從掃描中排除。

如果表中至少選擇了一個掃描範圍，則此按鈕可用。

所選元素的設定在單獨的視窗中變更。

點擊**"新增"**按鈕將開啟一個視窗，您可以在其中指定新的項目設定。

Kaspersky Endpoint Security 依照範圍清單中出現的順序掃描指定範圍內的物件。如果有必要，將子目錄放在清單中高於其父目錄的位置，以便為子目錄配置與父目錄的安全性設定不同的安全性設定。

「新增掃描範圍」視窗

在此視窗中，您可以新增和設定掃描範圍。

設定	描述
掃描範圍名稱	用於輸入掃描範圍名稱的欄位。該名稱將顯示在**掃描範圍**視窗的表中。 輸入欄位不能為空。
使用此範圍	此核取方塊可啟用或停用應用程式對此範圍的掃描。 如果選取此核取方塊，應用程式將處理此掃描範圍。 如果清除此核取方塊，應用程式將不處理此掃描範圍。您稍後可以透過選取核取方塊將此範圍包含在元件設定中。 預設情況下已選擇此核取方塊。
檔案系統、存取協定和路徑	設定區塊可讓您設定掃描範圍。 您可以在檔案系統下拉清單中選擇檔案系統類型： • **Local**（預設值）— 本機目錄。若選擇此項，則需要指明本機目錄的路徑。 • **已掛接**— 已掛載遠端或本機目錄。若選擇此項，則需要指明檔案系統的協定或名稱。 • **共用**— Protection Server 的檔案系統資源可透過 Samba 或 NFS 協定存取。 • **所有遠端掛載**— 使用 Samba 和 NFS 協定掛載在裝置上的所有遠端目錄。 • **所有共用**— Protection Server 的所有檔案系統資源都可以透過 Samba 和 NFS 協定存取。
	如果在檔案系統下拉清單中選擇了**已共用**或**已掛接**，則可以在右側的下拉清單中選擇遠端存取協定： • **NFS**：使用 NFS 協定掛載在裝置上的遠端目錄。 • **Samba**：使用 Samba 協定安裝在裝置上的遠端目錄。 • **自訂**— 在下方欄位中指定的裝置檔案系統的資源。
	如果在檔案系統下拉清單中選擇了**本機**，那麼您可以在輸入欄位中輸入要新增至掃描範圍的目錄的路徑。您可以使用遮罩和標籤來指定路徑。 預設指定**/**路徑 — 應用程式掃描本機檔案系統的所有目錄。 如果在檔案系統下拉清單中選擇了**本機**類型，且未指定路徑，則應用程式將掃描本機檔案系統的所有目錄。
檔案系統名稱	此欄位用於輸入要新增至掃描範圍的目錄所在的檔案系統的名稱。 如果在檔案系統下拉清單中選擇了"**已掛接**"類型，並且在右側的下拉清單中選擇了"**自訂**"項目，則該欄位可用。
遮罩	此清單包含應用程式掃描的物件的名稱遮罩。 預設情況下，清單包含*遮罩（所有物件）。 您可以新增、編輯或刪除遮罩。

實用文章

如何指定遮罩

您可以使用*（星號）字元來建立檔案或目錄名稱遮罩。

您可以指示單一*字元來表示檔案或目錄名稱中/字元前面的任意字元集（包括空集）。例如，`/dir/*/file` 或 `/dir/*/*/file`。

您可以用兩個連續的*字元來表示檔案或目錄名稱中的任意一組字元（包括空集和/字元）。例如，`/dir/**/file*/` 或 `/dir/file**/`。

**遮罩在目錄名稱中只能使用一次。例如，`/dir/**/**/file`是一個不正確的遮罩。

您可以使用單一?字元來表示檔案或目錄名稱中的任意一個字元。

如何使用標籤

您可以使用特殊標籤來指定容器或映像：

- `[container-id:<id>]/<path to local directory>`
- `[container-name:<name>]/<path to local directory>`

- [image-id:<id>]/<path to local directory>
- [image-name:<name>]/<path to local directory>

其中：

<id> 是容器 ID。

<name> 是容器名稱

<path to local directory> 是本機目錄路徑。

您也可以使用標籤的唯一組合：[container-id:<id>]、[container-name:<name>]、[image-id:<id>] 和 [image-name:<name>]/path to local directory>。

允許在一個區域內任意組合 1 到 4 個唯一標籤。列出的順序不重要。

範例：

- [container-name:<name>][image-name:<name>]/path to local directory>
- [container-id:<id>][image-name:<name>]/<path to local directory>
- [image-name:<name>][image-id:<id>]/<path to local directory>
- [container-name:<name>][container-id:<id>][image-name:<name>]/<path to local directory>
- [container-name:<name>][image-id:<id>][container-id:<id>][image-name:<name>]/path to local directory>

您可以在名稱和識別碼中使用遮罩（?和*字元）。

掃描設定視窗

在此視窗中，您可以在啟用檔案威脅防護的情況下設定檔掃描設定。

檔案威脅防護設定

設定	描述
掃描壓縮檔案	此核取方塊可啟用或停用壓縮檔案掃描。 如果勾選此核取方塊，Kaspersky Endpoint Security 將掃描壓縮檔案。 要掃描壓縮檔案，應用程式必須先將其解壓，這可能會減慢掃描速度。您可以透過在**一般掃描設定**部分中啟用和設定**略過掃描時間超過以下時長的檔案（秒）**和**略過大於以下大小的檔案 (MB)**設定來減少壓縮檔案掃描的持續時間。 如果清除此核取方塊，Kaspersky Endpoint Security 將不掃描壓縮檔案。 預設情況下已清空此核取方塊。
掃描 SFX 壓縮檔案	此核取方塊可啟用或停用*自解壓縮壓縮檔案*掃描。自解壓縮檔案是包含可執行解壓縮模組的檔案。 如果勾選此核取方塊，Kaspersky Endpoint Security 將掃描自解壓縮檔案。 若清除此核取方塊，Kaspersky Endpoint Security 將不掃描自解壓縮檔案。 如果取消選取**掃描壓縮檔案**核取方塊，則此核取方塊可用。 預設情況下已清空此核取方塊。

設定	描述
掃描郵件資料庫	此核取方塊可啟用或停用對 Microsoft Outlook、Outlook Express、The Bat! 和其他郵件應用程式的郵件資料庫的掃描。 如果勾選此核取方塊，Kaspersky Endpoint Security 將掃描郵件資料庫檔案。 如果清除此核取方塊，Kaspersky Endpoint Security 將不掃描郵件資料庫檔案。 預設情況下已清空此核取方塊。
掃描郵件格式檔案	此核取方塊可啟用或停用對純文字電子郵件檔案的掃描。 如果勾選此核取方塊，Kaspersky Endpoint Security 將掃描純文字訊息。 如果清除此核取方塊，Kaspersky Endpoint Security 將不掃描純文字訊息。 預設情況下已清空此核取方塊。
略過文字檔案	暫時將文字格式的檔案排除在掃描之外。 如果勾選該核取方塊，Kaspersky Endpoint Security 將不會掃描在最近一次掃描後 10 分鐘內被同一處理程序使用的文字檔案。此設定可以最佳化應用程式記錄的掃描。 如果未選取此核取方塊，Kaspersky Endpoint Security 將掃描文字檔案。 預設情況下已清空此核取方塊。 如果您使用基於 fanotify 的系統事件攔截機制，則會套用此設定。使用可更新的內核模組時，系統會利用掃描結果快取來最佳化掃描。
跳過資料庫記錄檔案	暫時將資料庫日誌檔案排除在掃描範圍之外。 如果勾選該核取方塊，且日誌檔案在最近一次掃描後 10 分鐘內由同一處理程序重複使用，應用程式將不會掃描資料庫日誌檔案。此設定可以最佳化資料庫日誌檔案的掃描。 如果清除此核取方塊，應用程式將掃描資料庫日誌檔案。 預設情況下已清空此核取方塊。 如果您使用基於 fanotify 的系統事件攔截機制，則會套用此設定。使用可更新的內核模組時，系統會利用掃描結果快取來最佳化掃描。
略過掃描時間超過以下時長的檔案（秒）	在此欄位中，您可以指定掃描檔案的最大時間（以秒為單位）。在指定時間之後，Kaspersky Endpoint Security 將停止掃描檔案。 可用值：0–9999。如果該值設為 0，則掃描時間不受限制。 預設值：60。
跳過檔案，如果大於 (MB)	在此欄位中，您可以指定要掃描檔案的最大大小（以兆位元組為單位）。 可用值：0–999999。如果值設定為 0，Kaspersky Endpoint Security 將掃描任意大小的檔案。 預設值：0。
記錄清潔物件	此核取方塊可啟用或停用*ObjectProcessed*類型事件的記錄。 如果選取此核取方塊，Kaspersky Endpoint Security 將記錄所有掃描物件的*ObjectProcessed*類型事件。 如果清除此核取方塊，Kaspersky Endpoint Security 將不會記錄*ObjectProcessed*類型事件。 預設情況下已清空此核取方塊。
記錄未處理的物件	如果在掃描期間無法處理檔案，則此核取方塊將啟用或停用記錄*ObjectNotProcessed*類型事件。 如果選取此核取方塊，Kaspersky Endpoint Security 將記錄*ObjectNotProcessed*類型的事件。 如果清除此核取方塊，Kaspersky Endpoint Security 將不會記錄*ObjectNotProcessed*類型的事件。 預設情況下已清空此核取方塊。
記錄封裝的物件	此核取方塊可啟用或停用對偵測到的所有打包物件的*PackedObjectDetected*類型事件的記錄。 如果選取此核取方塊，Kaspersky Endpoint Security 將記錄*PackedObjectDetected*類型事件。 如果清除此核取方塊，Kaspersky Endpoint Security 將不會記錄*PackedObjectDetected*類型的事件。 預設情況下已清空此核取方塊。
使用 iChecker 技術	此核取方塊可啟用或停用僅掃描新的和自上次掃描以來修改的檔案。 如果選取該核取方塊，Kaspersky Endpoint Security 將僅掃描新的或自上次掃描以來修改的檔案。 如果清除該核取方塊，Kaspersky Endpoint Security 將掃描檔案，無論其建立或修改日期為何。 預設情況下已選擇此核取方塊。

設定	描述
使用啟發式分析	此核取方塊可啟用或停用檔案掃描期間的啟發式分析。 預設情況下已選擇此核取方塊。
啟發式分析等級	如果選取**使用啟發式分析**核取方塊，則可以在下拉式清單中選擇啟發式分析等級： • **淺度**是最不詳細且系統負載最小的掃描。 • **中度**是具有平衡系統負載的中等掃描。 • **深度**是最詳細的掃描，具有最大的系統負載。 • **建議**（預設值）是卡巴斯基專家推薦的最佳等級。它確保防護品質和對受防護裝置效能的影響達到最佳組合。

偵測到威脅後的動作視窗

在此視窗中，您可以配置 Kaspersky Endpoint Security 對偵測到的感染物件執行的操作：

檔案威脅防護設定

設定	描述
偵測到威脅後的動作	您可以選取應用程式對偵測到的感染物件執行的動作： • **解毒；如果不能解毒則刪除**（預設）。如果選取此動作，應用程式會嘗試透過在備份中儲存物件副本對感染物件解毒。如果無法進行解毒（例如，如果無法對該類型的物件或該物件中的威脅類型解毒），則應用程式將刪除感染物件。 • **解毒；如果解毒失敗則封鎖**。如果選取此動作，應用程式會嘗試透過在備份中儲存物件副本對感染物件解毒。如果無法進行解毒（例如，如果無法對該類型的物件或該物件中的威脅類型解毒），則應用程式將封鎖對感染物件的存取。 • **封鎖**。如果選取此動作，應用程式將封鎖對感染物件的存取。 感染物件被解毒或刪除後，感染物件副本將放置在備份中。

檔案威脅防護排除項目

*防護排除*是一組條件，在這些條件下，Kaspersky Endpoint Security 不會掃描物件以查找病毒和其他惡意軟體。您也可以透過遮罩和威脅名稱排除物件，並為處理程序配置排除項目。

在管理主控台中，您可以在政策內容（**關鍵威脅防護 → 檔案威脅防護排除項目**）中設定檔案威脅防護排除項目。

掃描排除設定

設定組	描述
排除項目	這組設定包含**配置**按鈕。按一下此按鈕會開啟**排除範圍**視窗。在此視窗中，您可以定義要從掃描中排除的範圍清單。
依照遮罩排序排除項目	這組設定包含**設定**按鈕，該按鈕會開啟**依遮罩排除項目**視窗。在此視窗中，您可以按照名稱遮罩配置從掃描中排除的物件。
依照威脅名稱排序排除項目	這組設定包含**設定**按鈕，該按鈕會開啟**依威脅名稱排除項目**視窗。在此視窗中，您可以根據威脅名稱配置從掃描中排除物件。
依照處理程序使用排除項目	這組設定包含**設定**按鈕，該按鈕會開啟**依處理程序排除項目**視窗。在此視窗中，您可以排除處理程序的活動。

排除範圍視窗

此視窗包含掃描排除範圍。該應用程式不會掃描位於表中指定路徑的檔案和目錄。

排除範圍設定

設定	描述
排除範圍名稱	排除範圍名稱。
路徑	被排除掃描的目錄的路徑。
狀態	狀態表明應用程式是否使用此排除。

預設情況下，排除範圍表為空。您可以新增、編輯和刪除表中的項目。

您也可以透過點擊**進階->匯入**從檔案中匯入排除項目清單，透過點擊**進階->匯出選定**或**進階->全部匯出**將新增的排除項目清單匯出到檔案。

新排除範圍視窗

在此視窗中，您可以新增和設定掃描排除掃描範圍。

排除範圍設定

設定	描述
排除範圍名稱	用於輸入排除範圍名稱的欄位。該名稱將顯示在**排除範圍**視窗的表中。 輸入欄位不能為空。
使用此範圍	此核取方塊可以啟用或停用應用程式執行時排除掃描範圍。 如果選取此核取方塊，應用程式將在掃描期間排除該區域。 如果清除此核取方塊，應用程式會將此區域納入掃描範圍。您可以稍後透過選取核取方塊來排除該範圍。 預設情況下已選擇此核取方塊。
檔案系統、存取協定和路徑	設定區塊可讓您設定排除範圍。 在檔案系統下拉清單中，您可以選擇要從掃描中排除的目錄的檔案系統類型： • **Local**，用於本機目錄。 • **已掛接**— 已掛載的目錄。 • **所有遠端掛載**— 使用 Samba 和 NFS 協定掛載在裝置上的所有遠端目錄。
	如果檔案系統下拉清單選擇的是**已掛接**，則可以在右側的下拉清單中選擇遠端存取協定： • **NFS**：使用 NFS 協定掛載在裝置上的遠端目錄。 • **Samba**：使用 Samba 協定安裝在裝置上的遠端目錄。 • **自訂**— 在下方欄位中指定的裝置檔案系統的資源。
	如果在檔案系統下拉清單中選擇了**本機**，那麼您可以在輸入欄位中輸入要新增至排除範圍的目錄的路徑。您可以使用遮罩和標籤來指定路徑。 預設指定**/**路徑。應用程式將本機檔案系統的所有目錄排除在掃描之外。
檔案系統名稱	此欄位用於輸入要新增至排除範圍的目錄所在的檔案系統的名稱。 如果在檔案系統下拉清單中選擇了"**已掛接**"類型，並且在右側的下拉清單中選擇了"**自訂**"項目，則該欄位可用。
遮罩	此清單包含應用程式從掃描中排除的物件的名稱遮罩。遮罩僅適用於路徑欄位中指定的目錄中的物件。 預設情況下，清單包含*遮罩（所有物件）。 您可以新增、編輯或刪除遮罩。

實用文章

如何指定遮罩

您可以使用`*`（星號）字元來建立檔案或目錄名稱遮罩。

您可以指示單一`*`字元來表示檔案或目錄名稱中`/`字元前面的任意字元集（包括空集）。例如，`/dir/*/file` 或 `/dir/*/*/file`。

您可以用兩個連續的`*`字元來表示檔案或目錄名稱中的任意一組字元（包括空集和`/`字元）。例如，`/dir/**/file*/` 或 `/dir/file**/`。

`**`遮罩在目錄名稱中只能使用一次。例如，`/dir/**/**/file`是一個不正確的遮罩。

您可以使用單一`?`字元來表示檔案或目錄名稱中的任意一個字元。

如何使用標籤

您可以使用特殊標籤來指定容器或映像：

- [container-id:<id>]/<path to local directory>
- [container-name:<name>]/<path to local directory>
- [image-id:<id>]/<path to local directory>
- [image-name:<name>]/<path to local directory>

其中：

<id> 是容器 ID。

<name> 是容器名稱

<path to local directory> 是本機目錄路徑。

您也可以使用標籤的唯一組合：[container-id:<id>]、[container-name:<name>]、[image-id:<id>] 和 [image-name:<name>]/path to local directory>。

允許在一個區域內任意組合 1 到 4 個唯一標籤。列出的順序不重要。

範例：

- [container-name:<name>][image-name:<name>]/path to local directory>
- [container-id:<id>][image-name:<name>]/<path to local directory>
- [image-name:<name>][image-id:<id>]/<path to local directory>
- [container-name:<name>][container-id:<id>][image-name:<name>]/<path to local directory>
- [container-name:<name>][image-id:<id>][container-id:<id>][image-name:<name>]/path to local directory>

您可以在名稱和識別碼中使用遮罩（? 和 * 字元）。

依照遮罩排序排除項目視窗

您可以按名稱遮罩配置物件的掃描排除項目。應用程式不會掃描名稱包含指定遮罩的檔案。預設情況下，遮罩清單為空。

您可以新增、編輯或刪除遮罩。

點擊**新增**按鈕將開啟**物件遮罩**視窗。在此視窗的**定義物件遮罩**欄位中，您可以指定 Kaspersky Endpoint Security 從掃描中排除的檔案的名稱範本。

例如：
*.txt 遮罩指所有文字檔案。
*_my_file_??.html 遮罩指的是以任意字元開頭，以 _my_file_ 後面跟著任意兩個字元結尾的 html 檔案（例如，2020_my_file_09.html）。

您可以啟用在繼承子政策設定時合併排除項目清單。如果要合併清單項目，請選中**合併繼承的值**核取方塊。如果選取該核取方塊，則父政策清單中的項目將顯示在子政策中，並且可以將項目新增至子原則清單。如果取消選中此核取方塊，則在繼承政策設定時不會合併清單項目。預設情況下已清空此核取方塊。

依照威脅名稱排序排除項目視窗

您可以根據威脅名稱配置從掃描中排除物件。該應用程式不會封鎖指定的威脅。預設情況下，威脅名稱清單為空。

您可以新增、編輯和刪除威脅名稱。

您可以啟用在繼承子政策設定時合併排除項目清單。如果要合併清單項目，請選中**合併繼承的值**核取方塊。如果選取該核取方塊，則父政策清單中的項目將顯示在子政策中，並且可以將項目新增至子原則清單。如果取消選中此核取方塊，則在繼承政策設定時不會合併清單項目。預設情況下已清空此核取方塊。

依照處理程序使用排除項目視窗

此視窗包含每個處理程序的排除範圍。透過「依照處理程序排序排除項目」的排除範圍，您可以從掃描中排除指定處理程序的活動以及該指定處理程序修改的檔案。預設情況下，該清單包含兩個排除範圍，其中涵蓋網路代理的路徑。如果有必要，您可以刪除這些排除項目。

依照處理程序使用排除項目的排除範圍設定

設定	描述
合併繼承的值	此核取方塊可啟用或停用在繼承子政策設定時合併清單。 如果選取該核取方塊，則父政策清單中的項目將顯示在子政策中，並且可以將項目新增至子原則清單。 如果取消選中此核取方塊，則在繼承政策設定時不會合併清單項目。 預設情況下已清空此核取方塊。
排除範圍名稱	排除範圍名稱。
路徑	被排除的處理程序的完整路徑。
狀態	狀態表明應用程式是否使用此排除。

您可以新增、編輯或刪除表中的項目。

您也可以透過點擊**進階->匯入**從檔案中匯入排除項目清單，透過點擊**進階->匯出選定**或**進階->全部匯出**將新增的排除項目清單匯出到檔案。

受信任處理程序視窗

在此視窗中，您可以新增和設定按處理程序排除的排除範圍。

依照處理程序使用排除項目的排除範圍設定

設定	描述
排除範圍名稱	用於輸入排除範圍名稱的欄位。此名稱將顯示在**依照處理程序排序排除項目**視窗的表格中。 輸入欄位不能為空。
被排除的處理程序的路徑	您想要從掃描中排除的處理程序的完整路徑。 如果使用可更新內核模組進行系統事件攔截，則指定的處理程序將被排除在所有命名空間的攔截之外。
套用於子處理程序	排除**被排除的處理程序的路徑**設定所指示的被排除處理程序的子處理程序。 預設情況下已清空此核取方塊。
使用此範圍	此核取方塊可啟用或停用此排除範圍。 如果選取此核取方塊，應用程式將在掃描期間排除該區域。 如果清除此核取方塊，應用程式會將此區域納入掃描範圍。您可以稍後透過選取核取方塊來排除該範圍。 預設情況下已選擇此核取方塊。

設定	描述
被修改的檔案的路徑	這組設定可讓您為該處理程序修改的檔案設定掃描排除項目。 在檔案系統下拉清單中，您可以選擇要從掃描中排除的目錄的檔案系統類型： • **Local**，用於本機目錄。若選擇此項，則需要指明本機目錄的路徑。 • **已掛接**— 已掛載遠端或本機目錄。若選擇此項，則需要指明檔案系統的協定或名稱。 • **共用**— Protection Server 的檔案系統資源可透過 Samba 或 NFS 協定存取。 • **所有遠端掛載**— 使用 Samba 和 NFS 協定掛載在裝置上的所有遠端目錄。 • **所有共用**— Protection Server 的所有檔案系統資源都可以透過 Samba 和 NFS 協定存取。
	如果在檔案系統下拉清單中選擇了**已掛載**或**已共用**，則您可以在存取協定下拉清單中選擇遠端存取協定： • **NFS**：使用 NFS 協定掛載在裝置上的遠端目錄。 • **Samba**：使用 Samba 協定安裝在裝置上的遠端目錄。 • **自訂**— 在下方欄位中指定的裝置檔案系統的資源。
	如果在檔案系統下拉清單中選擇了**本機**，那麼您可以在輸入欄位中輸入要新增至排除範圍的目錄的路徑。您可以使用遮罩來指定路徑。輸入欄位不能為空。
檔案系統名稱	此欄位用於輸入要新增至排除範圍的目錄所在的檔案系統的名稱。 如果在檔案系統下拉清單中選擇了"**已掛接**"類型，並且在右側的下拉清單中選擇了"**自訂**"項目，則該欄位可用。
遮罩	此清單包含應用程式從掃描中排除的物件的名稱遮罩。遮罩僅適用於**被修改的檔案的路徑**欄位中指定的目錄中的物件。 您可以新增、編輯或刪除遮罩。

實用文章

如何指定遮罩

您可以使用`*`（星號）字元來建立檔案或目錄名稱遮罩。

您可以指示單一`*`字元來表示檔案或目錄名稱中`/`字元前面的任意字元集（包括空集）。例如，`/dir/*/file` 或 `/dir/*/*/file`。

您可以用兩個連續的`*`字元來表示檔案或目錄名稱中的任意一組字元（包括空集和`/`字元）。例如，`/dir/**/file*/` 或 `/dir/file**/`。

`**`遮罩在目錄名稱中只能使用一次。例如，`/dir/**/**/file`是一個不正確的遮罩。

您可以使用單一`?`字元來表示檔案或目錄名稱中的任意一個字元。

惡意軟體掃描

在管理主控台中，您可以使用*惡意軟體掃描*工作來掃描惡意軟體。

您可以執行自動建立的群組工作，也可以建立並執行使用者工作以進行掃描。您可以透過編輯工作的設定來管理掃描設定。

在 *搜尋惡意軟體* 工作的內容中，您可以在 **設定** 區段管理下表列出的設定。

惡意軟體掃描工作設定

設定	描述
掃描	這組設定包含可開啟視窗的按鈕，您可以在這些視窗中配置掃描範圍、掃描範圍設定和掃描設定。
偵測到威脅後的動作	這組設定包含**配置**按鈕。點擊此按鈕將開啟**偵測到威脅後的動作**視窗，您可以在其中設定應用程式對偵測到的感染物件執行的操作。

在 *搜尋惡意軟體* 工作的內容中，您可以在 **排除** 區段自訂排除範圍、依遮罩和依威脅名稱的排除。

掃描範圍視窗

此表包含掃描範圍。該應用程式將掃描表中指定路徑中的檔案和目錄。預設情況下，該表包含一個掃描範圍，其中包括本機檔案系統的所有目錄。

掃描範圍設定

設定	描述
範圍名稱	掃描範圍名稱。
路徑	應用程式掃描的目錄的路徑。
狀態	狀態表示應用程式是否掃描此範圍。

您可以**新增**、**編輯**、**刪除**、**上移**和**下移**表項。

點擊“**向下移動**”按鈕可將選定的項目在表格中向下移動。

Kaspersky Endpoint Security 依照掃描範圍表中所列的順序掃描指定範圍內的物件。如果要為子目錄配置與父目錄的安全性設定不同的安全性設定，則必須在表中將子目錄置於高於其父目錄的位置。

如果在表中選擇了範圍，則此按鈕可用。

點擊“**向上移動**”按鈕可將選定的項目在表中上移。

Kaspersky Endpoint Security 依照掃描範圍表中所列的順序掃描指定範圍內的物件。如果要為子目錄配置與父目錄的安全性設定不同的安全性設定，則必須在表中將子目錄置於高於其父目錄的位置。

如果在表中選擇了範圍，則此按鈕可用。

點擊“**刪除**”按鈕可將選定的範圍從掃描中排除。

如果表中至少選擇了一個掃描範圍，則此按鈕可用。

所選元素的設定在單獨的視窗中變更。

點擊**“新增”**按鈕將開啟一個視窗，您可以在其中指定新的項目設定。

Kaspersky Endpoint Security 依照範圍清單中出現的順序掃描指定範圍內的物件。如果有必要，將子目錄放在清單中高於其父目錄的位置，以便為子目錄配置與父目錄的安全性設定不同的安全性設定。

<新掃描範圍>視窗

在此視窗中，您可以新增和設定掃描範圍。

掃描範圍設定

設定	描述
掃描範圍名稱	用於輸入掃描範圍名稱的欄位。該名稱將顯示在**掃描範圍**視窗的表中。 輸入欄位不能為空。
使用此範圍	此核取方塊可啟用或停用應用程式對此範圍的掃描。 如果選取此核取方塊，應用程式將處理此掃描範圍。 如果清除此核取方塊，應用程式將不處理此掃描範圍。您稍後可以透過選取核取方塊將此範圍包含在元件設定中。 預設情況下已選擇此核取方塊。

設定	描述
檔案系統、存取協定和路徑	設定區塊可讓您設定掃描範圍。 您可以在檔案系統下拉清單中選擇檔案系統類型： • **Local**（預設值）— 本機目錄。若選擇此項，則需要指明本機目錄的路徑。 • **已掛接**— 已掛載遠端或本機目錄。若選擇此項，則需要指明檔案系統的協定或名稱。 • **共用**— Protection Server 的檔案系統資源可透過 Samba 或 NFS 協定存取。 • **所有遠端掛載**— 使用 Samba 和 NFS 協定掛載在裝置上的所有遠端目錄。 • **所有共用**— Protection Server 的所有檔案系統資源都可以透過 Samba 和 NFS 協定存取。
	如果在檔案系統下拉清單中選擇了**已共用**或**已掛接**，則可以在右側的下拉清單中選擇遠端存取協定： • **NFS**：使用 NFS 協定掛載在裝置上的遠端目錄。 • **Samba**：使用 Samba 協定安裝在裝置上的遠端目錄。 • **自訂**— 在下方欄位中指定的裝置檔案系統的資源。
	如果在檔案系統下拉清單中選擇了**本機**，那麼您可以在輸入欄位中輸入要新增至掃描範圍的目錄的路徑。您可以使用遮罩和標籤來指定路徑。 預設指定**/**路徑 — 應用程式掃描本機檔案系統的所有目錄。 如果在檔案系統下拉清單中選擇了**本機**類型，且未指定路徑，則應用程式將掃描本機檔案系統的所有目錄。
檔案系統名稱	此欄位用於輸入要新增至掃描範圍的目錄所在的檔案系統的名稱。 如果在檔案系統下拉清單中選擇了"**已掛接**"類型，並且在右側的下拉清單中選擇了"**自訂**"項目，則該欄位可用。
遮罩	此清單包含應用程式掃描的物件的名稱遮罩。 預設情況下，清單包含*遮罩（所有物件）。 您可以新增、編輯或刪除遮罩。

實用文章

如何指定遮罩

您可以使用*（星號）字元來建立檔案或目錄名稱遮罩。

您可以指示單一*字元來表示檔案或目錄名稱中/字元前面的任意字元集（包括空集）。例如，`/dir/*/file` 或 `/dir/*/*/file`。

您可以用兩個連續的*字元來表示檔案或目錄名稱中的任意一組字元（包括空集和/字元）。例如，`/dir/**/file*/` 或 `/dir/file**/`。

**遮罩在目錄名稱中只能使用一次。例如，`/dir/**/**/file`是一個不正確的遮罩。

您可以使用單一?字元來表示檔案或目錄名稱中的任意一個字元。

如何使用標籤

您可以使用特殊標籤來指定容器或映像：

- `[container-id:<id>]/<path to local directory>`
- `[container-name:<name>]/<path to local directory>`
- `[image-id:<id>]/<path to local directory>`
- `[image-name:<name>]/<path to local directory>`

其中：

`<id>` 是容器 ID。

`<name>` 是容器名稱

`<path to local directory>` 是本機目錄路徑。

您也可以使用標籤的唯一組合：`[container-id:<id>]`、`[container-name:<name>]`、`[image-id:<id>]` 和 `[image-name:<name>]/path to local directory>`。

允許在一個區域內任意組合1到 4 個唯一標籤。列出的順序不重要。

範例：

- `[container-name:<name>][image-name:<name>]/path to local directory>`
- `[container-id:<id>][image-name:<name>]/<path to local directory>`
- `[image-name:<name>][image-id:<id>]/<path to local directory>`
- `[container-name:<name>][container-id:<id>][image-name:<name>]/<path to local directory>`
- `[container-name:<name>][image-id:<id>][container-id:<id>][image-name:<name>]/path to local directory>`

您可以在名稱和識別碼中使用遮罩（`?` 和 `*` 字元）。

掃描範圍設定視窗

在此視窗中，您可以配置惡意軟體掃描工作的掃描設定。該應用程式可讓您掃描檔案、引導磁區、裝置記憶體和啟動物件。

掃描範圍設定

設定	描述
掃描檔案	此核取方塊可啟用或停用檔案掃描。 如果選取該核取方塊，應用程式將掃描檔案。 如果清除該核取方塊，應用程式將不會掃描檔案。 預設情況下已選擇此核取方塊。
掃描引導磁區	此核取方塊可啟用或停用引導磁區掃描。 如果選取該核取方塊，應用程式將掃描引導磁區。 如果清除該核取方塊，應用程式將不會掃描引導磁區。 預設情況下已清空此核取方塊。
掃描內核記憶體和正在執行的處理程序	此核取方塊可啟用或停用裝置記憶體掃描。 如果選取該核取方塊，應用程式將掃描內核記憶體和正在執行的處理程序。 如果清除該核取方塊，應用程式將不會掃描內核記憶體和正在執行的處理程序。 預設情況下已清空此核取方塊。
掃描啟動物件	此核取方塊可啟用或停用啟動物件掃描。 如果選取該核取方塊，應用程式將掃描啟動物件。 如果清除該核取方塊，應用程式將不會掃描啟動物件。 預設情況下已清空此核取方塊。
要掃描的裝置	這組設定包含**配置**按鈕。按一下此按鈕會開啟 **掃描範圍** 視窗，您可以在此指定必須掃描其開機磁區的裝置。
使用全域排除項目	此核取方塊可啟用或停用在應用程式執行時排除全域例外中指定的掛載點。 如果選取此核取方塊，應用程式將從掃描中排除配置的掛載點。 預設情況下已選擇此核取方塊。

設定	描述
使用檔案威脅防護排除項目	此核取方塊可啟用或停用應用程式執行時使用配置的檔案威脅防護排除項目。 如果選取該核取方塊，應用程式將不會掃描檔案威脅防護元件的排除項目中指定的物件。 預設情況下已選擇此核取方塊。

掃描範圍視窗

此表包含應用程式必須掃描其引導磁區的裝置的名稱遮罩。預設情況下，該表包含**/****裝置名稱遮罩（所有裝置）。

您可以新增、編輯和刪除表中的項目。

掃描設定視窗

在此視窗中，您可以配置工作的檔案掃描設定。

掃描設定

設定	描述
掃描壓縮檔案	此核取方塊可啟用或停用壓縮檔案掃描。 如果選取該核取方塊，應用程式將掃描壓縮檔案。 要掃描壓縮檔案，應用程式必須先將其解壓，這可能會減慢掃描速度。您可以透過在 **一般掃描設定** 區段中設定 **略過掃描時間超過以下時長的檔案（秒）** 和 **略過大於以下大小的檔案 (MB)** 設定，縮短壓縮檔案掃描的時間。 如果清除該核取方塊，應用程式將不會掃描壓縮檔案。 預設情況下已選擇此核取方塊。
掃描 SFX 壓縮檔案	此核取方塊可啟用或停用*自解壓縮壓縮檔案*掃描。自解壓縮檔案是包含可執行解壓縮模組的檔案。 如果選取該核取方塊，應用程式將掃描自解壓縮檔案。 如果清除該核取方塊，應用程式將不會掃描自解壓縮檔案。 如果清除 **掃描壓縮檔案** 核取方塊，則可使用此核取方塊。 預設情況下已選擇此核取方塊。
掃描郵件資料庫	此核取方塊可啟用或停用對 Microsoft Outlook、Outlook Express、The Bat! 和其他郵件應用程式的郵件資料庫的掃描。 如果選取該核取方塊，應用程式將掃描郵件資料庫檔案。 如果清除該核取方塊，應用程式將不會掃描郵件資料庫檔案。 預設情況下已清空此核取方塊。
掃描郵件格式檔案	此核取方塊可啟用或停用對純文字電子郵件檔案的掃描。 如果選取此核取方塊，應用程式將掃描純文字訊息。 如果清除此核取方塊，應用程式將不會掃描純文字訊息。 預設情況下已清空此核取方塊。
略過掃描時間超過以下時長的檔案（秒）	在此欄位中，您可以指定掃描檔案的最大時間（以秒為單位）。在指定時間之後，應用程式將停止掃描檔案。 可用值：0–9999。如果該值設為 0，則掃描時間不受限制。 預設值：0。
略過大於以下大小的檔案 (MB)	在此欄位中，您可以指定要掃描檔案的最大大小（以兆位元組為單位）。 可用值：0–999999。如果該值設為 0，應用程式將掃描任意大小的檔案。 預設值：0。
記錄清潔物件	此核取方塊可啟用或停用*ObjectProcessed*類型事件的記錄。 如果選取此核取方塊，應用程式將記錄所有掃描物件的*ObjectProcessed*類型的事件。 如果清除此核取方塊，應用程式將不會記錄任何掃描物件的*ObjectProcessed*類型的事件。 預設情況下已清空此核取方塊。
記錄未處理的物件	如果在掃描期間無法處理檔案，則此核取方塊將啟用或停用記錄*ObjectNotProcessed*類型事件。 如果選取此核取方塊，應用程式將記錄*ObjectNotProcessed*類型的事件。 如果清除此核取方塊，應用程式將不會記錄*ObjectNotProcessed*類型的事件。 預設情況下已清空此核取方塊。

設定	描述
記錄封裝的物件	此核取方塊可啟用或停用對偵測到的所有打包物件的*PackedObjectDetected*類型事件的記錄。 如果選取此核取方塊，應用程式將記錄*PackedObjectDetected*類型的事件。 如果清除此核取方塊，應用程式將不會記錄*PackedObjectDetected*類型的事件。 預設情況下已清空此核取方塊。
使用 iChecker 技術	此核取方塊可啟用或停用僅掃描新的和自上次掃描以來修改的檔案。 如果選取該核取方塊，應用程式將僅掃描新檔案或自上次掃描以來修改的檔案。 如果清除該核取方塊，應用程式將掃描檔案，無論其建立或修改日期如何。 預設情況下已選擇此核取方塊。
使用啟發式分析	此核取方塊可啟用或停用檔案掃描期間的啟發式分析。 預設情況下已選擇此核取方塊。
啟發式分析等級	如果選取 **使用啟發式分析** 核取方塊，您可以在下拉式清單中選取啟發式分析等級： • **淺度** 是詳細程度最低的掃描，系統負載最小。 • **中度** 是中等程度的掃描，系統負載均衡。 • **深度** 是最詳細的掃描，系統負載最大。 • **建議**（預設）是卡巴斯基專家建議的最佳等級。它確保防護品質和對受防護裝置效能的影響達到最佳組合。
不要同時執行多個掃描工作	如果掃描已經在執行，延遲啟動掃描工作。如果目前掃描繼續，Kaspersky Endpoint Security 將加入佇列新的掃描工作。這將有助於最佳化電腦負載。例如，讓我們假設應用程式已根據排程啟動了一項完整掃描工作。如果使用者嘗試從應用程式介面啟動快速掃描，Kaspersky Endpoint Security 將加入佇列該快速掃描工作，然後在完整掃描工作結束後自動啟動該工作。 預設情況下已清空此核取方塊。

偵測到威脅後的動作視窗

在此視窗中，您可以配置 Kaspersky Endpoint Security 對偵測到的感染物件執行的操作：

偵測到威脅後的動作

設定	描述
偵測到威脅後的動作	您可以選取應用程式對偵測到的感染物件執行的操作： • **解毒；如果不能解毒則刪除**（預設）。如果選取此動作，應用程式會嘗試透過在備份中儲存物件副本對感染物件解毒。如果無法進行解毒（例如，如果無法對該類型的物件或該物件中的威脅類型解毒），則應用程式將刪除感染物件。 • **解毒；如果解毒失敗則通知**。如果選取此動作，應用程式會嘗試透過在備份中儲存物件副本對感染物件解毒。如果無法進行解毒（例如，如果無法解毒該類型的物件或該物件中的威脅類型），則應用程式會在日誌中建立記錄。 • **通知**。如果選取此動作，應用程式會在記錄中建立關於感染物件的記錄。

排除項目部分

*掃描排除*是一組條件。當滿足這些條件時，Kaspersky Endpoint Security 不會掃描物件中是否有病毒和其他惡意軟體。您也可以按遮罩和威脅名稱從掃描中排除物件。

掃描排除設定

設定組	描述
排除範圍	這組設定包含**配置**按鈕。點擊此按鈕會開啟 **排除範圍** 視窗。在此視窗中，您可以定義要從掃描中排除的範圍清單。
依照遮罩排序排除項目	這組設定包含**設定**按鈕，該按鈕會開啟**依遮罩排除項目**視窗。在此視窗中，您可以按照名稱遮罩配置從掃描中排除的物件。
依照威脅名稱排序排除項目	這組設定包含**設定**按鈕，該按鈕會開啟**依威脅名稱排除項目**視窗。在此視窗中，您可以根據威脅名稱配置從掃描中排除物件。

排除範圍視窗

此視窗包含掃描排除範圍。該應用程式不會掃描位於表中指定路徑的檔案和目錄。

排除範圍設定

設定	描述
排除範圍名稱	排除範圍名稱。
路徑	被排除掃描的目錄的路徑。
狀態	狀態表明應用程式是否使用此排除。

預設情況下，排除範圍表為空。您可以新增、編輯和刪除表中的項目。

您也可以透過點擊**進階->匯入**從檔案中匯入排除項目清單，透過點擊**進階->匯出選定**或**進階->全部匯出**將新增的排除項目清單匯出到檔案。

新排除範圍視窗

在此視窗中，您可以新增和設定掃描排除掃描範圍。

排除範圍設定

設定	描述
排除範圍名稱	用於輸入排除範圍名稱的欄位。該名稱將顯示在**排除範圍**視窗的表中。 輸入欄位不能為空。
使用此範圍	此核取方塊可以啟用或停用應用程式執行時排除掃描範圍。 如果選取此核取方塊，應用程式將在掃描期間排除該區域。 如果清除此核取方塊，應用程式會將此區域納入掃描範圍。您可以稍後透過選取核取方塊來排除該範圍。 預設情況下已選擇此核取方塊。
檔案系統、存取協定和路徑	設定區塊可讓您設定排除範圍。 在檔案系統下拉清單中，您可以選擇要從掃描中排除的目錄的檔案系統類型： • **Local**，用於本機目錄。 • **已掛接**— 已掛載的目錄。 • **所有遠端掛載**— 使用 Samba 和 NFS 協定掛載在裝置上的所有遠端目錄。
	如果檔案系統下拉清單選擇的是**已掛接**，則可以在右側的下拉清單中選擇遠端存取協定： • **NFS**：使用 NFS 協定掛載在裝置上的遠端目錄。 • **Samba**：使用 Samba 協定安裝在裝置上的遠端目錄。 • **自訂**— 在下方欄位中指定的裝置檔案系統的資源。
	如果在檔案系統下拉清單中選擇了**本機**，那麼您可以在輸入欄位中輸入要新增至排除範圍的目錄的路徑。您可以使用遮罩和標籤來指定路徑。 預設指定**/**路徑。應用程式將本機檔案系統的所有目錄排除在掃描之外。
檔案系統名稱	此欄位用於輸入要新增至排除範圍的目錄所在的檔案系統的名稱。 如果在檔案系統下拉清單中選擇了"**已掛接**"類型，並且在右側的下拉清單中選擇了"**自訂**"項目，則該欄位可用。
遮罩	此清單包含應用程式從掃描中排除的物件的名稱遮罩。遮罩僅適用於路徑欄位中指定的目錄中的物件。 預設情況下，清單包含*遮罩（所有物件）。 您可以新增、編輯或刪除遮罩。

實用文章

如何指定遮罩

您可以使用*（星號）字元來建立檔案或目錄名稱遮罩。

您可以指示單一*字元來表示檔案或目錄名稱中/字元前面的任意字元集（包括空集）。例如，`/dir/*/file` 或 `/dir/*/*/file`。

您可以用兩個連續的*字元來表示檔案或目錄名稱中的任意一組字元（包括空集和/字元）。例如，`/dir/**/file*/` 或 `/dir/file**/`。

遮罩在目錄名稱中只能使用一次。例如，/dir//**/file是一個不正確的遮罩。

您可以使用單一?字元來表示檔案或目錄名稱中的任意一個字元。

如何使用標籤

您可以使用特殊標籤來指定容器或映像：

- [container-id:<id>]/<path to local directory>
- [container-name:<name>]/<path to local directory>
- [image-id:<id>]/<path to local directory>
- [image-name:<name>]/<path to local directory>

其中：

<id> 是容器 ID。

<name> 是容器名稱

<path to local directory> 是本機目錄路徑。

您也可以使用標籤的唯一組合：[container-id:<id>]、[container-name:<name>]、[image-id:<id>] 和 [image-name:<name>]/path to local directory>。

允許在一個區域內任意組合 1 到 4 個唯一標籤。列出的順序不重要。

範例：

- [container-name:<name>][image-name:<name>]/path to local directory>
- [container-id:<id>][image-name:<name>]/<path to local directory>
- [image-name:<name>][image-id:<id>]/<path to local directory>
- [container-name:<name>][container-id:<id>][image-name:<name>]/<path to local directory>
- [container-name:<name>][image-id:<id>][container-id:<id>][image-name:<name>]/path to local directory>

您可以在名稱和識別碼中使用遮罩（?和*字元）。

依照遮罩排序排除項目視窗

您可以按名稱遮罩配置物件的掃描排除項目。應用程式不會掃描名稱包含指定遮罩的檔案。預設情況下，遮罩清單為空。

您可以新增、編輯或刪除遮罩。

點擊**新增**按鈕將開啟**物件遮罩**視窗。在此視窗的**定義物件遮罩**欄位中，您可以指定 Kaspersky Endpoint Security 從掃描中排除的檔案的名稱範本。

例如：
`*.txt` 遮罩指所有文字檔案。
`*_my_file_??.html` 遮罩指的是以任意字元開頭，以 `_my_file_` 後面跟著任意兩個字元結尾的 html 檔案（例如，2020_my_file_09.html）。

依照威脅名稱排序排除項目視窗

您可以根據威脅名稱配置從掃描中排除物件。該應用程式不會封鎖指定的威脅。預設情況下，威脅名稱清單為空。

您可以新增、編輯和刪除威脅名稱。

關鍵區域掃描

在管理主控台中，您可以使用*關鍵區域掃描*工作對受防護裝置的作業系統執行關鍵區域掃描。

您可以建立並執行自訂的關鍵區域掃描工作。您可以透過編輯工作的設定來管理掃描設定。

在「*關鍵區域掃描*」工作的內容中，於「**設定**」區段，您可以管理下表列出的設定。

關鍵區域掃描工作設定

設定	描述
掃描	這組設定包含可開啟視窗的按鈕，您可以在這些視窗中配置掃描範圍、掃描範圍設定和掃描設定。
偵測到威脅後的動作	這組設定包含**配置**按鈕。點擊此按鈕將開啟**偵測到威脅後的動作**視窗，您可以在其中設定應用程式對偵測到的感染物件執行的操作。

在「*關鍵區域掃描*」工作的內容中，於「**排除**」區段，您可以自訂 排除範圍、依遮罩排除和 依威脅名稱排除。

掃描範圍視窗

此表包含掃描範圍。該應用程式將掃描表中指定路徑中的檔案和目錄。預設情況下，該表包含一個掃描範圍，其中包括本機檔案系統的所有目錄。

掃描範圍設定

設定	描述
範圍名稱	掃描範圍名稱。
路徑	應用程式掃描的目錄的路徑。
狀態	狀態表示應用程式是否掃描此範圍。

您可以**新增**、**編輯**、**刪除**、**上移**和**下移**表項。

點擊“**向下移動**”按鈕可將選定的項目在表格中向下移動。

Kaspersky Endpoint Security 依照掃描範圍表中所列的順序掃描指定範圍內的物件。如果要為子目錄配置與父目錄的安全性設定不同的安全性設定，則必須在表中將子目錄置於高於其父目錄的位置。

如果在表中選擇了範圍，則此按鈕可用。

點擊“**向上移動**”按鈕可將選定的項目在表中上移。

Kaspersky Endpoint Security 依照掃描範圍表中所列的順序掃描指定範圍內的物件。如果要為子目錄配置與父目錄的安全性設定不同的安全性設定，則必須在表中將子目錄置於高於其父目錄的位置。

如果在表中選擇了範圍，則此按鈕可用。

點擊“**刪除**”按鈕可將選定的範圍從掃描中排除。

如果表中至少選擇了一個掃描範圍，則此按鈕可用。

所選元素的設定在單獨的視窗中變更。

點擊**“新增”**按鈕將開啟一個視窗，您可以在其中指定新的項目設定。

Kaspersky Endpoint Security 依照範圍清單中出現的順序掃描指定範圍內的物件。如果有必要，將子目錄放在清單中高於其父目錄的位置，以便為子目錄配置與父目錄的安全性設定不同的安全性設定。

「新增掃描範圍」視窗

在此視窗中，您可以新增和設定掃描範圍。

掃描範圍設定

設定	描述
掃描範圍名稱	用於輸入掃描範圍名稱的欄位。該名稱將顯示在**掃描範圍**視窗的表中。 輸入欄位不能為空。
使用此範圍	此核取方塊可啟用或停用應用程式對此範圍的掃描。 如果選取此核取方塊，應用程式將處理此掃描範圍。 如果清除此核取方塊，應用程式將不處理此掃描範圍。您稍後可以透過選取核取方塊將此範圍包含在元件設定中。 預設情況下已選擇此核取方塊。
檔案系統、存取協定和路徑	設定區塊可讓您設定掃描範圍。 您可以在檔案系統下拉清單中選擇檔案系統類型： • **Local**（預設值）— 本機目錄。若選擇此項，則需要指明本機目錄的路徑。 • **已掛接**— 已掛載遠端或本機目錄。若選擇此項，則需要指明檔案系統的協定或名稱。 • **共用**— Protection Server 的檔案系統資源可透過 Samba 或 NFS 協定存取。 • **所有遠端掛載**— 使用 Samba 和 NFS 協定掛載在裝置上的所有遠端目錄。 • **所有共用**— Protection Server 的所有檔案系統資源都可以透過 Samba 和 NFS 協定存取。
	如果在檔案系統下拉清單中選擇了**已共用**或**已掛接**，則可以在右側的下拉清單中選擇遠端存取協定： • **NFS**：使用 NFS 協定掛載在裝置上的遠端目錄。 • **Samba**：使用 Samba 協定安裝在裝置上的遠端目錄。 • **自訂**— 在下方欄位中指定的裝置檔案系統的資源。
	如果在檔案系統下拉清單中選擇了**本機**，那麼您可以在輸入欄位中輸入要新增至掃描範圍的目錄的路徑。您可以使用遮罩和標籤來指定路徑。 預設指定**/**路徑 — 應用程式掃描本機檔案系統的所有目錄。 如果在檔案系統下拉清單中選擇了**本機**類型，且未指定路徑，則應用程式將掃描本機檔案系統的所有目錄。
檔案系統名稱	此欄位用於輸入要新增至掃描範圍的目錄所在的檔案系統的名稱。 如果在檔案系統下拉清單中選擇了“**已掛接**”類型，並且在右側的下拉清單中選擇了“**自訂**”項目，則該欄位可用。
遮罩	此清單包含應用程式掃描的物件的名稱遮罩。 預設情況下，清單包含*遮罩（所有物件）。 您可以新增、編輯或刪除遮罩。

實用文章

如何指定遮罩

您可以使用*（星號）字元來建立檔案或目錄名稱遮罩。

您可以指示單一*字元來表示檔案或目錄名稱中/字元前面的任意字元集（包括空集）。例如，`/dir/*/file` 或 `/dir/*/*/file`。

您可以用兩個連續的*字元來表示檔案或目錄名稱中的任意一組字元（包括空集和/字元）。例如，/dir/**/file*/ 或 /dir/file**/。

遮罩在目錄名稱中只能使用一次。例如，/dir//**/file是一個不正確的遮罩。

您可以使用單一?字元來表示檔案或目錄名稱中的任意一個字元。

如何使用標籤

您可以使用特殊標籤來指定容器或映像：

- [container-id:<id>]/<path to local directory>
- [container-name:<name>]/<path to local directory>
- [image-id:<id>]/<path to local directory>
- [image-name:<name>]/<path to local directory>

其中：

<id> 是容器 ID。

<name> 是容器名稱

<path to local directory> 是本機目錄路徑。

您也可以使用標籤的唯一組合：[container-id:<id>]、[container-name:<name>]、[image-id:<id>] 和 [image-name:<name>]/path to local directory>。

允許在一個區域內任意組合1到 4 個唯一標籤。列出的順序不重要。

範例：

- [container-name:<name>][image-name:<name>]/path to local directory>
- [container-id:<id>][image-name:<name>]/<path to local directory>
- [image-name:<name>][image-id:<id>]/<path to local directory>
- [container-name:<name>][container-id:<id>][image-name:<name>]/<path to local directory>
- [container-name:<name>][image-id:<id>][container-id:<id>][image-name:<name>]/path to local directory>

您可以在名稱和識別碼中使用遮罩（`?`和`*`字元）。

掃描範圍設定視窗

在此視窗中，您可以配置關鍵區域掃描工作的掃描設定。該應用程式可讓您掃描檔案、引導磁區、啟動物件、處理程序記憶體和內核記憶體。

掃描範圍設定

設定	描述
掃描檔案	此核取方塊可啟用或停用檔案掃描。 如果勾選此核取方塊，Kaspersky Endpoint Security 將掃描檔案。 如果未選取此核取方塊，Kaspersky Endpoint Security 將不會掃描檔案。 預設情況下已清空此核取方塊。
掃描引導磁區	此核取方塊可啟用或停用引導磁區掃描。 如果勾選此核取方塊，Kaspersky Endpoint Security 將掃描引導磁區。 如果未選取此核取方塊，Kaspersky Endpoint Security 將不掃描引導磁區。 預設情況下已選擇此核取方塊。
掃描內核記憶體和正在執行的處理程序	此核取方塊可啟用或停用裝置記憶體掃描。 如果選取該核取方塊，Kaspersky Endpoint Security 將掃描內核記憶體和正在執行的處理程序。 如果清除該核取方塊，Kaspersky Endpoint Security 將不會掃描內核記憶體和正在執行的處理程序。 預設情況下已選擇此核取方塊。
掃描啟動物件	此核取方塊可啟用或停用啟動物件掃描。 如果勾選此核取方塊，Kaspersky Endpoint Security 將掃描啟動物件。 如果取消選取此核取方塊，Kaspersky Endpoint Security 將不會掃描啟動物件。 預設情況下已選擇此核取方塊。
要掃描的裝置	這組設定包含**配置**按鈕。按一下此按鈕會開啟 **掃描範圍** 視窗，您可以在此指定必須掃描其開機磁區的裝置。
使用全域排除項目	此核取方塊可啟用或停用在應用程式執行時排除全域例外中指定的掛載點。 如果選取此核取方塊，應用程式將從掃描中排除配置的掛載點。 預設情況下已選擇此核取方塊。
使用檔案威脅防護排除項目	此核取方塊可啟用或停用應用程式執行時使用配置的檔案威脅防護排除項目。 如果選取該核取方塊，應用程式將不會掃描檔案威脅防護元件的排除項目中指定的物件。 預設情況下已選擇此核取方塊。

掃描範圍視窗

此表包含應用程式必須掃描其引導磁區的裝置的名稱遮罩。預設情況下，該表包含**/****裝置名稱遮罩（所有裝置）。

您可以新增、編輯和刪除表中的項目。

掃描設定視窗

在此視窗中，您可以配置工作的檔案掃描設定。

掃描設定

設定	描述
掃描壓縮檔案	此核取方塊可啟用或停用壓縮檔案掃描。 如果選取該核取方塊，應用程式將掃描壓縮檔案。 要掃描壓縮檔案，應用程式必須先將其解壓，這可能會減慢掃描速度。您可以透過在 **一般掃描設定** 區段中設定 **略過掃描時間超過以下時長的檔案（秒）** 和 **略過大於以下大小的檔案 (MB)** 設定，縮短壓縮檔案掃描的時間。 如果清除該核取方塊，應用程式將不會掃描壓縮檔案。 預設情況下已選擇此核取方塊。
掃描 SFX 壓縮檔案	此核取方塊可啟用或停用*自解壓縮壓縮檔案*掃描。自解壓縮檔案是包含可執行解壓縮模組的檔案。 如果選取該核取方塊，應用程式將掃描自解壓縮檔案。 如果清除該核取方塊，應用程式將不會掃描自解壓縮檔案。 如果清除 **掃描壓縮檔案** 核取方塊，則可使用此核取方塊。 預設情況下已選擇此核取方塊。

設定	描述
掃描郵件資料庫	此核取方塊可啟用或停用對 Microsoft Outlook、Outlook Express、The Bat! 和其他郵件應用程式的郵件資料庫的掃描。 如果選取該核取方塊，應用程式將掃描郵件資料庫檔案。 如果清除該核取方塊，應用程式將不會掃描郵件資料庫檔案。 預設情況下已清空此核取方塊。
掃描郵件格式檔案	此核取方塊可啟用或停用對純文字電子郵件檔案的掃描。 如果選取此核取方塊，應用程式將掃描純文字訊息。 如果清除此核取方塊，應用程式將不會掃描純文字訊息。 預設情況下已清空此核取方塊。
略過掃描時間超過以下時長的檔案（秒）	在此欄位中，您可以指定掃描檔案的最大時間（以秒為單位）。在指定時間之後，應用程式將停止掃描檔案。 可用值：0–9999。如果該值設為 0，則掃描時間不受限制。 預設值：0。
略過大於以下大小的檔案 (MB)	在此欄位中，您可以指定要掃描檔案的最大大小（以兆位元組為單位）。 可用值：0–999999。如果該值設為 0，應用程式將掃描任意大小的檔案。 預設值：0。
記錄清潔物件	此核取方塊可啟用或停用*ObjectProcessed*類型事件的記錄。 如果選取此核取方塊，應用程式將記錄所有掃描物件的*ObjectProcessed*類型的事件。 如果清除此核取方塊，應用程式將不會記錄任何掃描物件的*ObjectProcessed*類型的事件。 預設情況下已清空此核取方塊。
記錄未處理的物件	如果在掃描期間無法處理檔案，則此核取方塊將啟用或停用記錄*ObjectNotProcessed*類型事件。 如果選取此核取方塊，應用程式將記錄*ObjectNotProcessed*類型的事件。 如果清除此核取方塊，應用程式將不會記錄*ObjectNotProcessed*類型的事件。 預設情況下已清空此核取方塊。
記錄封裝的物件	此核取方塊可啟用或停用對偵測到的所有打包物件的*PackedObjectDetected*類型事件的記錄。 如果選取此核取方塊，應用程式將記錄*PackedObjectDetected*類型的事件。 如果清除此核取方塊，應用程式將不會記錄*PackedObjectDetected*類型的事件。 預設情況下已清空此核取方塊。
使用 iChecker 技術	此核取方塊可啟用或停用僅掃描新的和自上次掃描以來修改的檔案。 如果選取該核取方塊，應用程式將僅掃描新檔案或自上次掃描以來修改的檔案。 如果清除該核取方塊，應用程式將掃描檔案，無論其建立或修改日期如何。 預設情況下已選擇此核取方塊。
使用啟發式分析	此核取方塊可啟用或停用檔案掃描期間的啟發式分析。 預設情況下已選擇此核取方塊。
啟發式分析等級	如果選取 **使用啟發式分析** 核取方塊，您可以在下拉式清單中選取啟發式分析等級： • **淺度** 是詳細程度最低的掃描，系統負載最小。 • **中度** 是中等程度的掃描，系統負載均衡。 • **深度** 是最詳細的掃描，系統負載最大。 • **建議**（預設）是卡巴斯基專家建議的最佳等級。它確保防護品質和對受防護裝置效能的影響達到最佳組合。
不要同時執行多個掃描工作	如果掃描已經在執行，延遲啟動掃描工作。如果目前掃描繼續，Kaspersky Endpoint Security 將加入佇列新的掃描工作。這將有助於最佳化電腦負載。例如，讓我們假設應用程式已根據排程啟動了一項完整掃描工作。如果使用者嘗試從應用程式介面啟動快速掃描，Kaspersky Endpoint Security 將加入佇列該快速掃描工作，然後在完整掃描工作結束後自動啟動該工作。 預設情況下已清空此核取方塊。

偵測到威脅後的動作視窗

在此視窗中，您可以配置 Kaspersky Endpoint Security 對偵測到的感染物件執行的操作：

偵測到威脅後的動作

設定	描述
偵測到威脅後的動作	您可以選取應用程式對偵測到的感染物件執行的操作： • **解毒；如果不能解毒則刪除**（預設）。如果選取此動作，應用程式會嘗試透過在備份中儲存物件副本對感染物件解毒。如果無法進行解毒（例如，如果無法對該類型的物件或該物件中的威脅類型解毒），則應用程式將刪除感染物件。 • **解毒；如果解毒失敗則通知**。如果選取此動作，應用程式會嘗試透過在備份中儲存物件副本對感染物件解毒。如果無法進行解毒（例如，如果無法解毒該類型的物件或該物件中的威脅類型），則應用程式會在日誌中建立記錄。 • **通知**。如果選取此動作，應用程式會在記錄中建立關於感染物件的記錄。

排除項目部分

*掃描排除*是一組條件。當滿足這些條件時，Kaspersky Endpoint Security 不會掃描物件中是否有病毒和其他惡意軟體。您也可以按遮罩和威脅名稱從掃描中排除物件。

掃描排除設定

設定組	描述
排除範圍	這組設定包含**配置**按鈕。按一下此按鈕會開啟**排除範圍**視窗。在此視窗中，您可以定義要從掃描中排除的範圍清單。
依照遮罩排序排除項目	這組設定包含**設定**按鈕，該按鈕會開啟**依遮罩排除項目**視窗。在此視窗中，您可以按照名稱遮罩配置從掃描中排除的物件。
依照威脅名稱排序排除項目	這組設定包含**設定**按鈕，該按鈕會開啟**依威脅名稱排除項目**視窗。在此視窗中，您可以根據威脅名稱配置從掃描中排除物件。

排除範圍視窗

此視窗包含掃描排除範圍。該應用程式不會掃描位於表中指定路徑的檔案和目錄。

排除範圍設定

設定	描述
排除範圍名稱	排除範圍名稱。
路徑	被排除掃描的目錄的路徑。
狀態	狀態表明應用程式是否使用此排除。

預設情況下，排除範圍表為空。您可以新增、編輯和刪除表中的項目。

您也可以透過點擊**進階->匯入**從檔案中匯入排除項目清單，透過點擊**進階->匯出選定**或**進階->全部匯出**將新增的排除項目清單匯出到檔案。

新排除範圍視窗

在此視窗中，您可以新增和設定掃描排除掃描範圍。

排除範圍設定

設定	描述
排除範圍名稱	用於輸入排除範圍名稱的欄位。該名稱將顯示在**排除範圍**視窗的表中。 輸入欄位不能為空。
使用此範圍	此核取方塊可以啟用或停用應用程式執行時排除掃描範圍。 如果選取此核取方塊，應用程式將在掃描期間排除該區域。 如果清除此核取方塊，應用程式會將此區域納入掃描範圍。您可以稍後透過選取核取方塊來排除該範圍。 預設情況下已選擇此核取方塊。

設定	描述
檔案系統、存取協定和路徑	設定區塊可讓您設定排除範圍。 在檔案系統下拉清單中，您可以選擇要從掃描中排除的目錄的檔案系統類型： • **Local**，用於本機目錄。 • **已掛接**— 已掛載的目錄。 • **所有遠端掛載**— 使用 Samba 和 NFS 協定掛載在裝置上的所有遠端目錄。
	如果檔案系統下拉清單選擇的是**已掛接**，則可以在右側的下拉清單中選擇遠端存取協定： • **NFS**：使用 NFS 協定掛載在裝置上的遠端目錄。 • **Samba**：使用 Samba 協定安裝在裝置上的遠端目錄。 • **自訂**— 在下方欄位中指定的裝置檔案系統的資源。
	如果在檔案系統下拉清單中選擇了**本機**，那麼您可以在輸入欄位中輸入要新增至排除範圍的目錄的路徑。您可以使用遮罩和標籤來指定路徑。 預設指定**/**路徑。應用程式將本機檔案系統的所有目錄排除在掃描之外。
檔案系統名稱	此欄位用於輸入要新增至排除範圍的目錄所在的檔案系統的名稱。 如果在檔案系統下拉清單中選擇了"**已掛接**"類型，並且在右側的下拉清單中選擇了"**自訂**"項目，則該欄位可用。
遮罩	此清單包含應用程式從掃描中排除的物件的名稱遮罩。遮罩僅適用於路徑欄位中指定的目錄中的物件。 預設情況下，清單包含*遮罩（所有物件）。 您可以新增、編輯或刪除遮罩。

實用文章

如何指定遮罩

您可以使用*（星號）字元來建立檔案或目錄名稱遮罩。

您可以指示單一*字元來表示檔案或目錄名稱中/字元前面的任意字元集（包括空集）。例如，`/dir/*/file` 或 `/dir/*/*/file`。

您可以用兩個連續的*字元來表示檔案或目錄名稱中的任意一組字元（包括空集和/字元）。例如，`/dir/**/file*/` 或 `/dir/file**/`。

**遮罩在目錄名稱中只能使用一次。例如，`/dir/**/**/file`是一個不正確的遮罩。

您可以使用單一?字元來表示檔案或目錄名稱中的任意一個字元。

如何使用標籤

您可以使用特殊標籤來指定容器或映像：

- `[container-id:<id>]/<path to local directory>`
- `[container-name:<name>]/<path to local directory>`
- `[image-id:<id>]/<path to local directory>`
- `[image-name:<name>]/<path to local directory>`

其中：

`<id>` 是容器 ID。

`<name>` 是容器名稱

`<path to local directory>` 是本機目錄路徑。

您也可以使用標籤的唯一組合：`[container-id:<id>]`、`[container-name:<name>]`、`[image-id:<id>]` 和 `[image-name:<name>]/path to local directory>`。

允許在一個區域內任意組合 1 到 4 個唯一標籤。列出的順序不重要。

範例：

- `[container-name:<name>][image-name:<name>]/path to local directory>`
- `[container-id:<id>][image-name:<name>]/<path to local directory>`
- `[image-name:<name>][image-id:<id>]/<path to local directory>`
- `[container-name:<name>][container-id:<id>][image-name:<name>]/<path to local directory>`
- `[container-name:<name>][image-id:<id>][container-id:<id>][image-name:<name>]/path to local directory>`

您可以在名稱和識別碼中使用遮罩（`?` 和 `*` 字元）。

依照遮罩排序排除項目視窗

您可以按名稱遮罩配置物件的掃描排除項目。應用程式不會掃描名稱包含指定遮罩的檔案。預設情況下，遮罩清單為空。

您可以新增、編輯或刪除遮罩。

點擊**新增**按鈕將開啟**物件遮罩**視窗。在此視窗的**定義物件遮罩**欄位中，您可以指定 Kaspersky Endpoint Security 從掃描中排除的檔案的名稱範本。

例如：
`*.txt` 遮罩指所有文字檔案。
`*_my_file_??.html` 遮罩指的是以任意字元開頭，以 `_my_file_` 後面跟著任意兩個字元結尾的 html 檔案（例如，2020_my_file_09.html）。

依照威脅名稱排序排除項目視窗

您可以根據威脅名稱配置從掃描中排除物件。該應用程式不會封鎖指定的威脅。預設情況下，威脅名稱清單為空。

您可以新增、編輯和刪除威脅名稱。

容器監控

在管理主控台中，您可以在政策內容（**一般設定** → **容器掃描設定**）中設定容器監控元件。

容器監控設定

設定	描述
啟用命名空間和容器掃描	此核取方塊可啟用或停用命名空間和容器的即時掃描。 預設情況下已選擇此核取方塊。
偵測到威脅時對容器的動作	在下拉清單中，您可以選擇偵測到感染物件時對容器執行的操作： • **略過容器**：如果偵測到感染物件，應用程式不會對該容器執行任何操作。 • **停止容器**：如果偵測到感染物件，應用程式將停止該容器。 • **如果解毒失敗則停止容器**（預設值）— 如果對受感染物件的解毒失敗，應用程式將停止容器。 在支援此功能的產品授權下使用應用程式時，此設定可用。
容器掃描設定	設定組包含**配置**按鈕。點擊此按鈕將開啟**容器掃描設定**視窗。

容器掃描設定視窗

在此視窗中，您可以編輯將 Kaspersky Endpoint Security 與 Docker 容器管理系統、CRI-O 環境以及 Podman 和 runc 實用程式進行整合的設定。

容器掃描設定

設定	描述
使用 Docker	此核取方塊可啟用或停用 Docker 容器管理系統的使用。 預設情況下已選擇此核取方塊。
Docker 通訊端路徑	Docker 通訊端的路徑或 URI（統一資源識別碼）的輸入欄位。 預設值：/var/run/docker.sock。
使用 CRI-O	此核取方塊可啟用或停用 CRI-O 環境的使用。 預設情況下已選擇此核取方塊。
檔案路徑	CRI-O 設定檔路徑的輸入欄位。 預設值：/etc/crio/crio.conf。
使用 Podman	此核取方塊可啟用或停用 Podman 實用程式的使用。 預設情況下已選擇此核取方塊。
檔案路徑	Podman 實用程式可執行檔路徑的輸入欄位。 預設值：/usr/bin/podman。
根目錄	容器儲存根目錄路徑的輸入欄位。 預設值：/var/lib/containers/storage
使用 runc	此核取方塊可啟用或停用 runc 實用程式的使用。 預設情況下已選擇此核取方塊。
檔案路徑	runc 實用程式可執行檔路徑的輸入欄位。 預設值：/usr/bin/runc。
根目錄	容器狀態儲存的根目錄路徑的輸入欄位。 預設值：/run/runc。

容器掃描

在管理主控台中，您可以使用*容器掃描*工作掃描容器和映像。

您可以建立並執行自訂容器掃描工作。您可以透過編輯工作的設定來管理掃描設定。

在 *容器掃描* 工作的屬性中，您可以在 **設定** 區段管理下表所列的設定。

容器掃描工作設定

設定	描述
掃描	這組設定包含視窗開啟按鈕，您可以在其中配置容器掃描設定和一般掃描設定。
偵測到威脅後的動作	這組設定包含**配置**按鈕。點擊此按鈕將開啟**偵測到威脅後的動作**視窗，您可以在其中設定應用程式對偵測到的感染物件執行的操作。

在 *容器掃描* 工作的屬性中，您也可以在 **排除** 區段設定依遮罩和依威脅名稱的排除項目。

容器掃描設定視窗

在此視窗中，您可以配置容器和映像掃描設定。

容器和映像掃描設定

設定	描述
掃描容器	此核取方塊可啟用或停用容器掃描。如果選取該核取方塊，您可以指定要掃描的容器的名稱或名稱遮罩。 預設情況下已選擇此核取方塊。
名稱遮罩	需要掃描的容器的名稱或名稱遮罩的輸入欄位。 預設情況下，指定*遮罩 – 所有容器都將掃描。
偵測到威脅後的動作	在下拉清單中，您可以選擇偵測到感染物件時對容器執行的操作： • **略過容器** - 偵測到受感染的感染物件時，不對容器執行任何操作。 • **停止容器** – 偵測到感染物件時停止容器。 • **如果解毒失敗則停止容器**（預設值） – 如果感染物件解毒或威脅消除失敗，則停止容器。 由於 CRI-O 環境的工作方式，感染物件不會在 CRI-O 環境中的容器中被解毒或刪除。建議選取 **停止容器** 操作。
掃描映像	此核取方塊可啟用或停用映像掃描。如果選取該核取方塊，您可以指定要掃描映像的名稱或名稱遮罩。 預設情況下已選擇此核取方塊。
名稱遮罩	待掃描映像的名稱或名稱遮罩的輸入欄位。 預設情況下，指定*遮罩（掃描所有映像）。
偵測到威脅後的動作	在下拉清單中，您可以選擇當偵測到受感染物件時對映像執行的操作： • **略過映像**（預設值） - 偵測到受感染物件時，不對映像執行任何操作。 • 當偵測到受感染物件時**刪除映像**（不建議）。所有相依性也將被刪除。正在執行的容器將被停止，然後被刪除。
掃描每層	此核取方塊可啟用或停用對所有層的映像和正在執行的容器的掃描。 預設情況下已清空此核取方塊。

掃描設定視窗

在此視窗中，您可以配置工作的檔案掃描設定。

掃描設定

設定	描述
掃描壓縮檔案	此核取方塊可啟用或停用壓縮檔案掃描。 如果選取該核取方塊，應用程式將掃描壓縮檔案。 要掃描壓縮檔案，應用程式必須先將其解壓，這可能會減慢掃描速度。您可以透過在 **一般掃描設定** 區段中設定 **略過掃描時間超過以下時長的檔案（秒）** 和 **略過大於以下大小的檔案 (MB)** 設定，縮短壓縮檔案掃描的時間。 如果清除該核取方塊，應用程式將不會掃描壓縮檔案。 預設情況下已選擇此核取方塊。

設定	描述
掃描 SFX 壓縮檔案	此核取方塊可啟用或停用*自解壓縮壓縮檔案*掃描。自解壓縮檔案是包含可執行解壓縮模組的檔案。 如果選取該核取方塊，應用程式將掃描自解壓縮檔案。 如果清除該核取方塊，應用程式將不會掃描自解壓縮檔案。 如果清除 **掃描壓縮檔案** 核取方塊，則可使用此核取方塊。 預設情況下已選擇此核取方塊。
掃描郵件資料庫	此核取方塊可啟用或停用對 Microsoft Outlook、Outlook Express、The Bat! 和其他郵件應用程式的郵件資料庫的掃描。 如果選取該核取方塊，應用程式將掃描郵件資料庫檔案。 如果清除該核取方塊，應用程式將不會掃描郵件資料庫檔案。 預設情況下已清空此核取方塊。
掃描郵件格式檔案	此核取方塊可啟用或停用對純文字電子郵件檔案的掃描。 如果選取此核取方塊，應用程式將掃描純文字訊息。 如果清除此核取方塊，應用程式將不會掃描純文字訊息。 預設情況下已清空此核取方塊。
略過掃描時間超過以下時長的檔案（秒）	在此欄位中，您可以指定掃描檔案的最大時間（以秒為單位）。在指定時間之後，應用程式將停止掃描檔案。 可用值：0–9999。如果該值設為 0，則掃描時間不受限制。 預設值：0。
略過大於以下大小的檔案 (MB)	在此欄位中，您可以指定要掃描檔案的最大大小（以兆位元組為單位）。 可用值：0–999999。如果該值設為 0，應用程式將掃描任意大小的檔案。 預設值：0。
記錄清潔物件	此核取方塊可啟用或停用*ObjectProcessed*類型事件的記錄。 如果選取此核取方塊，應用程式將記錄所有掃描物件的*ObjectProcessed*類型的事件。 如果清除此核取方塊，應用程式將不會記錄任何掃描物件的*ObjectProcessed*類型的事件。 預設情況下已清空此核取方塊。
記錄未處理的物件	如果在掃描期間無法處理檔案，則此核取方塊將啟用或停用記錄*ObjectNotProcessed*類型事件。 如果選取此核取方塊，應用程式將記錄*ObjectNotProcessed*類型的事件。 如果清除此核取方塊，應用程式將不會記錄*ObjectNotProcessed*類型的事件。 預設情況下已清空此核取方塊。
記錄封裝的物件	此核取方塊可啟用或停用對偵測到的所有打包物件的*PackedObjectDetected*類型事件的記錄。 如果選取此核取方塊，應用程式將記錄*PackedObjectDetected*類型的事件。 如果清除此核取方塊，應用程式將不會記錄*PackedObjectDetected*類型的事件。 預設情況下已清空此核取方塊。
使用 iChecker 技術	此核取方塊可啟用或停用僅掃描新的和自上次掃描以來修改的檔案。 如果選取該核取方塊，應用程式將僅掃描新檔案或自上次掃描以來修改的檔案。 如果清除該核取方塊，應用程式將掃描檔案，無論其建立或修改日期如何。 預設情況下已選擇此核取方塊。
使用啟發式分析	此核取方塊可啟用或停用檔案掃描期間的啟發式分析。 預設情況下已選擇此核取方塊。
啟發式分析等級	如果選取 **使用啟發式分析** 核取方塊，您可以在下拉式清單中選取啟發式分析等級： • **淺度** 是詳細程度最低的掃描，系統負載最小。 • **中度** 是中等程度的掃描，系統負載均衡。 • **深度** 是最詳細的掃描，系統負載最大。 • **建議**（預設）是卡巴斯基專家建議的最佳等級。它確保防護品質和對受防護裝置效能的影響達到最佳組合。
不要同時執行多個掃描工作	如果掃描已經在執行，延遲啟動掃描工作。如果目前掃描繼續，Kaspersky Endpoint Security 將加入佇列新的掃描工作。這將有助於最佳化電腦負載。例如，讓我們假設應用程式已根據排程啟動了一項完整掃描工作。如果使用者嘗試從應用程式介面啟動快速掃描，Kaspersky Endpoint Security 將加入佇列該快速掃描工作，然後在完整掃描工作結束後自動啟動該工作。 預設情況下已清空此核取方塊。

偵測到威脅後的動作視窗

在此視窗中，您可以配置 Kaspersky Endpoint Security 對偵測到的感染物件執行的操作：

偵測到威脅後的動作

設定	描述
偵測到威脅後的動作	您可以選取應用程式對偵測到的感染物件執行的操作： • **解毒；如果不能解毒則刪除**（預設）。如果選取此動作，應用程式會嘗試透過在備份中儲存物件副本對感染物件解毒。如果無法進行解毒（例如，如果無法對該類型的物件或該物件中的威脅類型解毒），則應用程式將刪除感染物件。 • **解毒；如果解毒失敗則通知**。如果選取此動作，應用程式會嘗試透過在備份中儲存物件副本對感染物件解毒。如果無法進行解毒（例如，如果無法解毒該類型的物件或該物件中的威脅類型），則應用程式會在日誌中建立記錄。 • **通知**。如果選取此動作，應用程式會在記錄中建立關於感染物件的記錄。

排除項目部分

掃描排除設定

設定組	描述
依照遮罩排序排除項目	這組設定包含**設定**按鈕，該按鈕會開啟**依遮罩排除項目**視窗。在此視窗中，您可以按照名稱遮罩配置從掃描中排除的物件。
依照威脅名稱排序排除項目	這組設定包含**設定**按鈕，該按鈕會開啟**依威脅名稱排除項目**視窗。在此視窗中，您可以根據威脅名稱配置從掃描中排除物件。
使用全域排除項目	此核取方塊可啟用或停用在應用程式執行時排除全域例外中指定的掛載點。 如果選取此核取方塊，應用程式將從掃描中排除配置的掛載點。 預設情況下已選擇此核取方塊。

依照遮罩排序排除項目視窗

您可以按名稱遮罩配置物件的掃描排除項目。應用程式不會掃描名稱包含指定遮罩的檔案。預設情況下，遮罩清單為空。

您可以新增、編輯或刪除遮罩。

點擊**新增**按鈕將開啟**物件遮罩**視窗。在此視窗的**定義物件遮罩**欄位中，您可以指定 Kaspersky Endpoint Security 從掃描中排除的檔案的名稱範本。

例如：
`*.txt` 遮罩指所有文字檔案。
`*_my_file_??.html` 遮罩指的是以任意字元開頭，以 `_my_file_` 後面跟著任意兩個字元結尾的 html 檔案（例如，2020_my_file_09.html）。

依照威脅名稱排序排除項目視窗

您可以根據威脅名稱配置從掃描中排除物件。該應用程式不會封鎖指定的威脅。預設情況下，威脅名稱清單為空。

您可以新增、編輯和刪除威脅名稱。

卸除式磁碟機掃描

在管理主控台中，您可以在政策內容（**本機工作 → 卸除式磁碟機掃描**）中設定卸除式磁碟機掃描的設定。

卸除式磁碟機掃描元件設定

設定	描述
連線到裝置時啟用卸除式磁碟機掃描	此核取方塊可啟用或停用當卸除式磁碟機連線到使用者裝置時對其進行掃描。 預設情況下已清空此核取方塊。
卸除式磁碟機連線時的動作	在下拉清單中，您可以選擇卸除式磁碟機連線到使用者裝置時應用程式要執行的操作： • 連線時**不掃描**卸除式磁碟機（預設值）。 • **快速掃描**：僅掃描卸除式磁碟機（CD/DVD 光碟機和藍光光碟除外）中特定類型的檔案，且不解壓縮複合物件。快速掃描使用*關鍵區域掃描*工作的預設設定執行。 • **詳細掃描**：掃描卸除式磁碟機上的所有檔案（CD/DVD 光碟機和藍光光碟除外）。詳細掃描使用*惡意軟體掃描*工作的預設設定執行。
CD / DVD 磁碟機連線時的動作	在下拉清單中，您可以選擇在 CD/DVD 光碟機和藍光光碟連線到使用者裝置時應用程式要執行的操作： • 連線時**不掃描**CD/DVD 光碟機和藍光光碟（預設值）。 • **快速掃描**：僅掃描 CD/DVD 光碟機和藍光光碟中特定類型的檔案。快速掃描使用*關鍵區域掃描*工作的預設設定執行。 • **詳細掃描**：掃描 CD/DVD 光碟機和藍光光碟上的所有檔案。詳細掃描使用*惡意軟體掃描*工作的預設設定執行。
掃描過程中封鎖對卸除式磁碟機的存取	此核取方塊可啟用或停用在執行掃描期間封鎖已連線磁碟機上的檔案。 預設情況下已清空此核取方塊。

實用文章

快速掃描的檔案類型

在卸除式媒體上掃描下列檔案格式：com、exe、sys、prg、bin、bat、cmd、dpl、dll、scr、cpl、ocx、tsp、drv、vxd、pif、lnk、reg、ini、cia、vbs、vbe、js、jse、htm、htt、hhip、aspx、ig、cx、fpm、rtf、shs、dwg、msi、otm、pdf、swf、jpeg、emf、ico、ov?、xl*、xlsb、pp*、md*、sldx、sldm、thmx。

行為偵測

在管理主控台中，您可以在政策內容（**進階威脅防護 → 行為偵測**）中管理行為偵測設定。

行為偵測元件設定

設定	描述
啟用行為偵測	此核取方塊可啟用或停用行為偵測元件。 預設情況下已選擇此核取方塊。
偵測到惡意軟體活動後的動作	在作業系統中偵測到惡意活動時，Kaspersky Endpoint Security 將執行的操作： • **封鎖**執行惡意活動的應用程式（預設值）。Kaspersky Endpoint Security 終止執行惡意活動的處理程序並記錄關於偵測到的惡意活動的資訊。 • **通知**使用者。Kaspersky Endpoint Security 不會終止執行惡意活動的處理程序；它僅在事件日誌中記錄偵測到的惡意活動。
依照處理程序使用排除項目	此核取方塊可按行為偵測元件運行中的處理程序來啟用或停用排除項目。 預設情況下已清空此核取方塊。 **配置**按鈕可開啟**依照處理程序排序排除項目**視窗。在此視窗中，您可以排除處理程序的活動。

依照處理程序使用排除項目視窗

此視窗包含每個處理程序的排除範圍。透過「依照處理程序排序排除項目」的排除範圍，您可以排除指定處理程序的活動。

依照處理程序使用排除項目的排除範圍設定

設定	描述
合併繼承的值	此核取方塊可啟用或停用在繼承子政策設定時合併清單。 如果選取該核取方塊，則父政策清單中的項目將顯示在子政策中，並且可以將項目新增至子原則清單。 如果取消選中此核取方塊，則在繼承政策設定時不會合併清單項目。 預設情況下已清空此核取方塊。
排除範圍名稱	排除範圍名稱。
路徑	被排除的處理程序的完整路徑。
狀態	狀態表明應用程式是否使用此排除。

預設情況下，排除範圍表為空。您可以新增、編輯或刪除表中的項目。

您也可以透過點擊**進階->匯入**從檔案中匯入排除項目清單，透過點擊**進階->匯出選定**或**進階->全部匯出**將新增的排除項目清單匯出到檔案。

受信任處理程序視窗

在此視窗中，您可以新增和設定按處理程序排除的排除範圍。

依照處理程序使用排除項目的排除範圍設定

設定	描述
排除範圍名稱	用於輸入排除範圍名稱的欄位。此名稱將顯示在**依照處理程序排序排除項目**視窗的表格中。
被排除的處理程序的路徑	您想要從掃描中排除的處理程序的完整路徑。您可以使用遮罩來指定路徑。 輸入欄位不能為空。
套用於子處理程序	排除**被排除的處理程序的路徑**設定所指示的被排除處理程序的子處理程序。 預設情況下已清空此核取方塊。
使用此範圍	此核取方塊可啟用或停用此排除範圍。 如果選取此核取方塊，應用程式將排除此範圍。 如果清除此核取方塊，則應用程式將包括此範圍。您可以稍後透過選取核取方塊來排除該範圍。 預設情況下已選擇此核取方塊。
將處理程序從行為偵測掃描中排除	此核取方塊可啟用或停用行為偵測掃描的處理程序排除項目。 預設情況下已清空此核取方塊。
從 MDR 和 EDR Expert (on-premises) 遙測資料中排除處理程序	此核取方塊可啟用或停用將處理程序從 MDR 和 EDR Expert (on-premises) 元件收集的遙測資料中排除。 預設情況下已清空此核取方塊。

實用文章

如何指定遮罩

您可以使用*（星號）字元來建立檔案或目錄名稱遮罩。

您可以指示單一*字元來表示檔案或目錄名稱中/字元前面的任意字元集（包括空集）。例如，`/dir/*/file` 或 `/dir/*/*/file`。

您可以用兩個連續的*字元來表示檔案或目錄名稱中的任意一組字元（包括空集和/字元）。例如，`/dir/**/file*/` 或 `/dir/file**/`。

**遮罩在目錄名稱中只能使用一次。例如，`/dir/**/**/file`是一個不正確的遮罩。

您可以使用單一?字元來表示檔案或目錄名稱中的任意一個字元。

弱點利用防禦

在管理主控台中，您可以在政策內容（**進階威脅防護 → 行為偵測**）中設定弱點利用防禦。

弱點利用防禦元件設定

設定	描述
啟用弱點利用防禦	此核取方塊可啟用或停用弱點利用防護。 預設情況下已清空此核取方塊。
弱點利用防禦	按一下 **設定** 按鈕會開啟 **弱點利用防禦排除項目** 視窗，您可以在其中設定弱點利用防禦元件的掃描排除項目。
偵測到弱點利用後的動作	偵測到弱點利用時應用程式將執行的動作： • **封鎖**（預設值）。應用程式可阻止弱點利用的惡意活動，並在事件記錄中記錄相關資訊。 • **通知**應用程式不會阻止弱點利用活動，而只會在事件記錄中記錄關於弱點利用偵測的資訊。

弱點利用防禦排除項目視窗

在此視窗中，您可以配置從弱點利用防禦掃描中排除的物件。該應用程式將不會掃描指定物件。預設情況下，物件清單為空。

弱點利用防禦排除設定

設定	描述
合併繼承的值	此核取方塊可啟用或停用在繼承子政策設定時合併清單。 如果選取該核取方塊，則父政策清單中的項目將顯示在子政策中，並且可以將項目新增至子原則清單。 如果取消選中此核取方塊，則在繼承政策設定時不會合併清單項目。 預設情況下已清空此核取方塊。
狀態	狀態表明應用程式是否使用此排除。
威脅名稱。	要從掃描中排除的威脅的名稱。
檔案或目錄路徑	要從掃描範圍中排除的檔案或目錄的完整路徑。
檔案雜湊值	排除在掃描範圍之外的檔案的雜湊值。
備註	掃描排除注釋。

預設情況下，排除項目表為空。您可以新增、編輯或刪除表中的項目。

弱點利用防禦排除視窗

在此視窗中，您可以新增或配置從弱點利用防禦掃描中排除的物件。

弱點利用防禦排除設定

設定	描述
使用威脅名稱	此核取方塊可啟用或停用按物件中偵測到的威脅名稱排除掃描。 預設情況下已選擇此核取方塊。
威脅名稱。	在此欄位中，您可以輸入在物件中偵測到的威脅的名稱。為了從掃描中排除物件，請指定在此物件中偵測到的威脅的全名 — 包含應用程式判定物件被感染的字串。您可以在應用程式記錄或網站https://threats.kaspersky.com 中找到在物件中偵測到的威脅的全名。 如果選取**使用威脅名稱**核取方塊，則此欄位可用。
使用檔案雜湊	此核取方塊可啟用或停用按檔案雜湊值排除掃描。 預設情況下已選擇此核取方塊。
檔案雜湊總和類型	在此下拉清單中，您可以選擇要用於將檔案從掃描中排除的檔案雜湊類型： • MD5。 • SHA256。 如果選取**使用檔案雜湊**核取方塊，則此下拉清單可用。
檔案雜湊總和	在此欄位中，您可以輸入要根據其將檔案從掃描中排除的檔案的雜湊值。 如果選取**使用檔案雜湊**核取方塊，則此欄位可用。
使用檔案或目錄路徑	此核取方塊可啟用或停用按照路徑排除在路徑中偵測到威脅的檔案。 預設情況下已選擇此核取方塊。
檔案或目錄路徑	用於指定您想要從掃描中排除的檔案或者目錄的路徑的輸入欄位。路徑中可以使用 * 和 ? 字元。 如果選取**使用檔案或目錄路徑**核取方塊，則此欄位可用。
備註	註解的輸入欄位（可選）。
使用該排除項目	此核取方塊可在應用程式執行時啟用或停用此排除項目的使用。 預設情況下已選擇此核取方塊。

Anti-Cryptor

在管理主控台中，您可以在政策屬性中管理加密軟體防護設定（**進階威脅防護 → 加密軟體防護**）。

Anti-Cryptor 元件設定

設定	描述
啟用加密軟體防護	此核取方塊可啟用或停用透過 SMB/NFS 協定進行網路存取的本機目錄中檔案的防護，以防止遠端惡意加密。 預設情況下已清空此核取方塊。
防護範圍	這組設定包含開啟視窗的按鈕，您可以在其中配置掃描範圍和防護設定。
排除項目	這組設定包含**配置**按鈕。按一下此按鈕會開啟**排除範圍**視窗。在此視窗中，您可以定義要從掃描中排除的範圍清單。
依照遮罩排序排除項目	這組設定包含**設定**按鈕，該按鈕會開啟**依遮罩排除項目**視窗。在此視窗中，您可以按照名稱遮罩配置從掃描中排除的物件。

掃描範圍視窗

此表包含掃描範圍。該應用程式將掃描表中指定路徑中的檔案和目錄。預設情況下，該表包含一個掃描範圍，其中包括本機檔案系統的所有目錄。

掃描範圍設定

設定	描述
範圍名稱	掃描範圍名稱。
路徑	應用程式掃描的目錄的路徑。
狀態	狀態表示應用程式是否掃描此範圍。

您可以**新增**、**編輯**、**刪除**、**上移**和**下移**表項。

點擊“**向下移動**”按鈕可將選定的項目在表格中向下移動。

Kaspersky Endpoint Security 依照掃描範圍表中所列的順序掃描指定範圍內的物件。如果要為子目錄配置與父目錄的安全性設定不同的安全性設定，則必須在表中將子目錄置於高於其父目錄的位置。

如果在表中選擇了範圍，則此按鈕可用。

點擊“**向上移動**”按鈕可將選定的項目在表中上移。

Kaspersky Endpoint Security 依照掃描範圍表中所列的順序掃描指定範圍內的物件。如果要為子目錄配置與父目錄的安全性設定不同的安全性設定，則必須在表中將子目錄置於高於其父目錄的位置。

如果在表中選擇了範圍，則此按鈕可用。

點擊“**刪除**”按鈕可將選定的範圍從掃描中排除。

如果表中至少選擇了一個掃描範圍，則此按鈕可用。

所選元素的設定在單獨的視窗中變更。

點擊**“新增”**按鈕將開啟一個視窗，您可以在其中指定新的項目設定。

Kaspersky Endpoint Security 依照範圍清單中出現的順序掃描指定範圍內的物件。如果有必要，將子目錄放在清單中高於其父目錄的位置，以便為子目錄配置與父目錄的安全性設定不同的安全性設定。

「新增掃描範圍」視窗

在此視窗中，您可以新增或配置加密軟體防護元件的防護範圍。

防護範圍設定

設定	描述
範圍名稱	用於輸入防護範圍名稱的欄位。該名稱將顯示在**掃描範圍**視窗的表中。 輸入欄位不能為空。
使用此範圍	此核取方塊可啟用或停用應用程式對此範圍的掃描。 如果選取此核取方塊，應用程式將在元件運行期間處理此防護範圍。 如果清除此核取方塊，應用程式在元件操作期間不會處理此防護範圍。您稍後可以透過選取核取方塊將此範圍包含在元件操作設定中。 預設情況下已選擇此核取方塊。
檔案系統、存取協定和路徑	設定區塊可讓您設定掃描範圍。 您可以在檔案系統下拉清單中選擇檔案系統類型： • **Local**，用於本機目錄。 • **共用**顯示可透過 Samba 或 NFS 協定存取的伺服器檔案系統資源。 • **所有共用**（預設值）顯示所有可透過 Samba 和 NFS 協定存取的伺服器檔案系統資源。
	如果在檔案系統下拉清單中選擇了**共用**，則可以在右側的下拉清單中選擇遠端存取協定： • **NFS**：使用 NFS 協定掛載在裝置上的遠端目錄。 • **Samba**：使用 Samba 協定安裝在裝置上的遠端目錄。
	如果在檔案系統下拉清單中選擇了**本機**，那麼您可以在輸入欄位中輸入要新增至防護範圍的目錄的路徑。您可以使用遮罩來指定路徑。 該欄位不能為空。
遮罩	此清單包含應用程式在加密軟體防護元件運作期間掃描的物件的名稱遮罩。 預設情況下，清單包含*遮罩（所有物件）。 您可以新增、編輯或刪除遮罩。

實用文章

如何指定遮罩

您可以使用*（星號）字元來建立檔案或目錄名稱遮罩。

您可以指示單一*字元來表示檔案或目錄名稱中/字元前面的任意字元集（包括空集）。例如，`/dir/*/file` 或 `/dir/*/*/file`。

您可以用兩個連續的*字元來表示檔案或目錄名稱中的任意一組字元（包括空集和/字元）。例如，`/dir/**/file*/` 或 `/dir/file**/`。

**遮罩在目錄名稱中只能使用一次。例如，`/dir/**/**/file`是一個不正確的遮罩。

您可以使用單一?字元來表示檔案或目錄名稱中的任意一個字元。

防護設定視窗

防護設定

設定	描述
偵測到加密後的動作	偵測到惡意加密後 Kaspersky Endpoint Security 將執行的操作： • **通知**使用者。Kaspersky Endpoint Security 不會阻止執行加密的裝置；它僅在事件日誌中記錄關於偵測到惡意加密的事件。 • **封鎖**執行加密的裝置（預設值）。
不受信任的主機封鎖時長（分鐘）	您可以在此欄位中指定不受信任主機的封鎖持續時間（以分鐘為單位）。在指定時間之後，Kaspersky Endpoint Security 會將不受信任的裝置從封鎖裝置清單中刪除。當主機被從不受信任主機清單中刪除後，該主機對網路檔案資源的存取權將自動還原。 如果受感染的主機被封鎖並且您變更此設定值，則該主機的封鎖時間將不會改變。封鎖時間不是動態值，是在封鎖的那一刻計算出來的。 可能的值：從 1 到 2147483647 的整數。 預設值：30。

排除範圍視窗

此視窗包含掃描排除範圍。該應用程式不會掃描位於表中指定路徑的檔案和目錄。

排除範圍設定

設定	描述
排除範圍名稱	排除範圍名稱。
路徑	被排除掃描的目錄的路徑。
狀態	狀態表明應用程式是否使用此排除。

預設情況下，排除範圍表為空。您可以新增、編輯和刪除表中的項目。

您也可以透過點擊**進階->匯入**從檔案中匯入排除項目清單，透過點擊**進階->匯出選定**或**進階->全部匯出**將新增的排除項目清單匯出到檔案。

新排除範圍視窗

- 在此視窗中，您可以新增和設定掃描排除掃描範圍。

設定	描述
排除範圍名稱	用於輸入排除範圍名稱的欄位。該名稱將顯示在**排除範圍**視窗的表中。 輸入欄位不能為空。
使用此範圍	此核取方塊可以啟用或停用應用程式執行時排除掃描範圍。 如果選取此核取方塊，應用程式將在掃描期間排除該區域。 如果清除此核取方塊，應用程式會將此區域納入掃描範圍。您可以稍後透過選取核取方塊來排除該範圍。 預設情況下已選擇此核取方塊。
檔案系統、存取協定和路徑	設定區塊可讓您設定排除範圍。 在檔案系統下拉清單中，您可以選擇要從掃描中排除的目錄的檔案系統類型： • **本機** 適用於本機目錄。 • **已掛接** 適用於已掛載的目錄。 • **所有遠端掛接** 適用於使用 Samba 和 NFS 協定掛載在裝置上的所有遠端目錄。
	如果在檔案系統下拉式清單中選取 **已掛接**，您可以在右側的下拉式清單中選取遠端存取協定： • **NFS** 適用於使用 NFS 協定掛載在裝置上的遠端目錄。 • **Samba** 適用於使用 Samba 協定掛載在裝置上的遠端目錄。 • **自訂** 適用於下方欄位中指定的裝置檔案系統資源。
	如果在檔案系統下拉式清單中選取 **本機**，您可以在輸入欄位中輸入要新增至排除範圍之目錄的路徑。您可以使用遮罩和標籤來指定路徑。 預設指定**/**路徑。應用程式將本機檔案系統的所有目錄排除在掃描之外。
檔案系統名稱	此欄位用於輸入要新增至排除範圍的目錄所在的檔案系統的名稱。 如果在檔案系統下拉式清單中選取 **已掛接** 類型，並且在右側下拉式清單中選取 **自訂** 項目，則該欄位可用。
遮罩	此清單包含應用程式從掃描中排除的物件的名稱遮罩。遮罩僅適用於路徑欄位中指定的目錄中的物件。 預設情況下，清單包含*****遮罩（所有物件）。 您可以新增、編輯或刪除遮罩。

實用文章

如何指定遮罩

您可以使用`*`（星號）字元來建立檔案或目錄名稱遮罩。

您可以指示單一`*`字元來表示檔案或目錄名稱中`/`字元前面的任意字元集（包括空集）。例如，`/dir/*/file` 或 `/dir/*/*/file`。

您可以用兩個連續的`*`字元來表示檔案或目錄名稱中的任意一組字元（包括空集和`/`字元）。例如，`/dir/**/file*/` 或 `/dir/file**/`。

`**`遮罩在目錄名稱中只能使用一次。例如，`/dir/**/**/file`是一個不正確的遮罩。

您可以使用單一`?`字元來表示檔案或目錄名稱中的任意一個字元。

如何使用標籤

您可以使用特殊標籤來指定容器或映像：

- `[container-id:<id>]/<path to local directory>`
- `[container-name:<name>]/<path to local directory>`
- `[image-id:<id>]/<path to local directory>`
- `[image-name:<name>]/<path to local directory>`

其中：

`<id>` 是容器 ID。

`<name>` 是容器名稱

`<path to local directory>` 是本機目錄路徑。

您也可以使用標籤的唯一組合：`[container-id:<id>]`、`[container-name:<name>]`、`[image-id:<id>]` 和 `[image-name:<name>]/path to local directory>`。

允許在一個區域內任意組合 1 到 4 個唯一標籤。列出的順序不重要。

範例：

- `[container-name:<name>][image-name:<name>]/path to local directory>`
- `[container-id:<id>][image-name:<name>]/<path to local directory>`
- `[image-name:<name>][image-id:<id>]/<path to local directory>`
- `[container-name:<name>][container-id:<id>][image-name:<name>]/<path to local directory>`
- `[container-name:<name>][image-id:<id>][container-id:<id>][image-name:<name>]/path to local directory>`

您可以在名稱和識別碼中使用遮罩（`?` 和 `*` 字元）。

依照遮罩排序排除項目視窗

您可以按名稱遮罩配置物件的掃描排除項目。應用程式不會掃描名稱包含指定遮罩的檔案。預設情況下，遮罩清單為空。

您可以新增、編輯或刪除遮罩。

點擊**新增**按鈕將開啟**物件遮罩**視窗。在此視窗的**定義物件遮罩**欄位中，您可以指定 Kaspersky Endpoint Security 從掃描中排除的檔案的名稱範本。

例如：
`*.txt` 遮罩指所有文字檔案。
`*_my_file_??.html` 遮罩指的是以任意字元開頭，以 `_my_file_` 後面跟著任意兩個字元結尾的 html 檔案（例如，2020_my_file_09.html）。

您可以啟用在繼承子政策設定時合併排除項目清單。如果要合併清單項目，請選中**合併繼承的值**核取方塊。如果選取該核取方塊，則父政策清單中的項目將顯示在子政策中，並且可以將項目新增至子原則清單。如果取消選中此核取方塊，則在繼承政策設定時不會合併清單項目。預設情況下已清空此核取方塊。

卡巴斯基安全網路

在管理主控台中，您可以在政策屬性（**進階威脅防護** → **卡巴斯基安全網路**）中設定 Kaspersky Endpoint Security 使用卡巴斯基安全網路。

您可以在卡巴斯基安全網路聲明視窗中閱讀**卡巴斯基安全網路聲明**的文字，點擊**卡巴斯基安全網路聲明**連結即可開啟該視窗。

卡巴斯基安全管理中心透過*裝置*索引標籤上受管理裝置清單中的用戶端裝置狀態（**正常**、**緊急**、**警告**）顯示關於 KSN 可用性的資訊。

卡巴斯基安全網路設定

設定	描述
卡巴斯基安全網路聲明	點擊此連結會開啟 **卡巴斯基安全網路聲明**視窗。在此視窗中，您可以閱讀卡巴斯基安全網路聲明的文字。
卡巴斯基安全網路 (KSN)	此區塊顯示關於 KSN 模式的資訊或表示 Kaspersky Endpoint Security 未使用 KSN。 **編輯**按鈕可開啟一個視窗，您可以在其中配置卡巴斯基安全網路的使用。
啟用雲端模式	在 *雲端模式*中，Kaspersky Endpoint Security 會使用輕量版的病毒防護資料庫，這可將電腦 RAM 的負載大約減半。 如果啟用了 KSN，則此核取方塊可用。 如果您在建立政策時接受了卡巴斯基安全網路聲明的條款並在延伸 KSN 模式下使用 KSN，則該核取方塊會被選取。 下次應用程式資料庫更新後，該模式將已啟用或已停用。 此設定僅當應用程式在標準模式下使用時才適用。
使用管理伺服器作為 KSN 代理伺服器	如果選取此核取方塊，Kaspersky Endpoint Security 會使用管理伺服器上的 KSN 代理服務與 KSN 伺服器進行通訊。 預設情況下已選擇此核取方塊。 此設定僅當應用程式在標準模式下使用時才適用。在 Light Agent 模式下，此應用程式只能透過 KSN 代理伺服器與 KSN 基礎架構進行通訊。
當 KSN Proxy 無法使用時使用 KSN 伺服器	如果選取此核取方塊，當 KSN 代理服務不可用時，Kaspersky Endpoint Security 會直接與 KSN 伺服器進行通訊。 預設情況下已選擇此核取方塊。 選取**使用管理伺服器作為 KSN 代理伺服器**核取方塊後，則此核取方塊才可用。 此設定僅當應用程式在標準模式下使用時才適用。

卡巴斯基安全網路設定

在此視窗中，您可以設定卡巴斯基安全網路參與設定。

卡巴斯基安全網路設定

設定	描述
更多資訊	點擊此連結將開啟卡巴斯基網站。
不使用卡巴斯基安全網路	選擇此選項即表示您拒絕使用卡巴斯基安全網路。
基本 KSN 模式	選擇此選項幾表示您接受使用卡巴斯基安全網路的條款。您將能夠從卡巴斯基的線上知識庫獲得關於檔案、Web 資源和軟體信譽的資訊。
延伸 KSN 模式	選擇此選項幾表示您接受使用卡巴斯基安全網路的條款。您將能夠從卡巴斯基的線上知識庫獲得關於檔案、Web 資源和軟體信譽的資訊。此外，關於各種威脅的類型和來源的匿名統計資料和資訊將被傳送給卡巴斯基，以改善卡巴斯基安全網路。
卡巴斯基安全網路聲明	此連結可開啟**卡巴斯基安全網路聲明**視窗，您可以在其中閱讀卡巴斯基安全網路聲明的文字。

卡巴斯基安全網路聲明

在此視窗中，您可以閱讀卡巴斯基安全網路聲明的文字並接受其條款和條件。

卡巴斯基安全網路設定

設定	描述
我確認我已完整閱讀、理解並接受卡巴斯基安全網路聲明的條款和條件	選擇此選項幾表示，您確認您想要使用卡巴斯基安全網路，並且您已完全閱讀、理解並接受所顯示的卡巴斯基安全網路聲明的條款和條件。 如果您在卡巴斯基安全網路設定視窗中選擇了**基本 KSN 模式**或**延伸 KSN 模式**選項，則此選項可用。
我不接受卡巴斯基安全網路聲明的條款和條件	選擇此選項幾表示，您確認不想使用卡巴斯基安全網路。 如果您在卡巴斯基安全網路設定視窗中選擇了**基本 KSN 模式**或**延伸 KSN 模式**選項，則此選項可用。

卡巴斯基私人安全網路聲明

在此視窗中，您可以閱讀卡巴斯基私人安全網路聲明的文字並接受其條款和條件。

卡巴斯基安全網路設定

設定	描述
我確認我已完整閱讀、理解並接受卡巴斯基安全網路聲明的條款和條件	選擇此選項即表示您確認想要參與卡巴斯基安全網路，並且您已完全閱讀、理解並接受所顯示的卡巴斯基私人安全網路聲明的條款和條件。
我不接受卡巴斯基安全網路聲明的條款和條件	選擇此選項幾表示，您確認不想使用卡巴斯基安全網路。

BadUSB 攻擊防護

在管理主控台中，您可以在政策屬性中管理 Web 威脅防護設定（**關鍵威脅防護 → BadUSB 攻擊防護**）。

BadUSB 攻擊防護元件設定

設定	描述
啟用 BadUSB 攻擊防護	此核取方塊可啟用或停用 BadUSB 攻擊防護元件。 該元件預設為停用。
USB 裝置授權最大嘗試次數	如果授權碼輸入錯誤達到指定次數，則自動封鎖 USB 裝置。有效值為 1 到 10。例如，如果您允許嘗試輸入授權碼五次，則應用程式會在第五次嘗試失敗後封鎖 USB 裝置。Kaspersky Endpoint Security 會顯示 USB 裝置被封鎖的時間。該時間經過後，您將再一次有 5 次嘗試輸入授權碼。
當達到最大的授權嘗試次數時的封鎖持續時間（分鐘）	在指定次數的授權碼輸入失敗後，USB 裝置被封鎖的持續時間。可選值：1 到 180（分鐘）。
授權 USB 裝置時不要允許使用螢幕鍵盤	如果開啟此撥動按鈕，應用程式將封鎖使用螢幕鍵盤認證無法輸入認證碼的 USB 裝置。
禁止使用條碼授權 USB 裝置	如果啟用此切換開關，則應用程式不允許使用條碼對無法用於輸入授權碼的 USB 裝置進行授權。

通訊與 Web 防護

郵件威脅防護

在管理主控台中，您可以在政策屬性中管理 Web 威脅防護設定（**關鍵威脅防護 → 郵件威脅防護**）。

郵件威脅防護元件設定

設定	描述
郵件威脅防護	此核取方塊可啟用或停用郵件威脅防護。 此元件預設為啟用。
設定 (防護設定)	點擊此按鈕將開啟**Web 威脅防護設定**視窗，您可以在其中配置郵件威脅防護範圍和複合檔案的掃描設定。
設定 (附件篩選)	點擊此按鈕將開啟**附件篩選**視窗，您可以在其中配置電子郵件附件的篩選條件。
使用啟發式分析器 **啟發式分析等級**	此核取方塊可啟用或停用啟發式分析器。 在掃描檔案查找惡意代碼時，啟發式分析器會執行可執行檔中的指令。啟發式分析器執行的指令數量取決於指定的啟發式分析級別。啟發式分析級別可設定威脅搜尋的徹底性、作業系統資源的負載和啟發式分析持續時間之間的平衡。 預設啟發式分析器已啟用，並選擇了中等啟發式分析級別。
偵測到威脅後的動作	郵件威脅防護在電子郵件中偵測到威脅時執行的動作： • **解毒；如果不能解毒則刪除** 當在傳入的郵件中偵測到感染物件時，應用程式會嘗試對偵測到的感染物件進行解毒。然後，帶有安全附件的郵件將被提供給使用者。如果解毒失敗，應用程式將刪除受感染的物件。應用程式會將有關已執行操作的資訊新增至郵件主旨中，例如：*[郵件已處理] <郵件主旨>*。預設情況下已選擇此操作。 • **解毒；如果解毒失敗則封鎖**當在傳入的郵件中偵測到感染物件時，應用程式會嘗試對偵測到的感染物件進行解毒。然後，帶有安全附件的郵件將被提供給使用者。如果解毒失敗，應用程式會在郵件主旨中新增警告。然後，帶有原始附件的郵件將被提供給使用者。 • **封鎖**如果在收到的郵件中偵測到受感染的對象，應用程式會在郵件主旨中新增警告。然後，帶有原始附件的郵件將被提供給使用者。 此設定不適用於傳出郵件。如果在傳送的訊息中偵測到受感染物件，應用程式將阻止該訊息的傳送。

郵件威脅防護設定視窗

在此視窗中，您可以設定郵件威脅防護範圍和複合檔案掃描設定。

郵件威脅防護設定

設定	描述
防護範圍	*防護範圍*可指定元件必須掃描的物件：傳入和傳出郵件，或僅傳入郵件。 預設情況下，**傳入和傳出的訊息**選項處於選取狀態。
掃描壓縮檔案附件	啟用或停用掃描壓縮檔案附件。 這包括對 ZIP、GZIP、BZIP、RAR、TAR、ARJ、CAB、LHA、JAR、ICE 和其他類型壓縮檔案的掃描。應用程式不僅透過副檔名，還透過格式來識別壓縮檔案。掃描壓縮檔案時，應用程式會執行遞歸解包。這樣做可以偵測嵌套壓縮檔案（壓縮檔案中的壓縮檔案）中的威脅。 預設情況下已選擇此核取方塊。
掃描附加的辦公室應用程式檔案	啟用或停用掃描 Office 格式的附件。無論是否選取此核取方塊，應用程式都會掃描小於 1MB 的 Office 格式附件。 預設情況下已選擇此核取方塊。
不掃描大於以下大小的壓縮檔案 (MB)	如果選取此核取方塊，郵件威脅防護將不會掃描任何大於指定限制的壓縮檔案附件。如果清除此核取方塊，郵件威脅防護將掃描任何大小的壓縮檔案附件。 預設情況下已清空此核取方塊。
限制壓縮檔案掃描持續時長為（秒鐘）	如果勾選此核取方塊，則會限制附加到電子郵件的壓縮檔案的掃描持續時間。 預設情況下已清空此核取方塊。

附件篩選視窗

在此視窗中，您可以配置電子郵件附件篩選。

附件篩選設定

設定	描述
不套用篩選器	如果選擇此選項，郵件威脅防護將不會篩選電子郵件附件。
重命名指定類型的附件	如果選擇此選項， 郵件威脅防護會將指定檔案類型（例如 attachment.doc_）的副檔名最後一個字元替換為下劃線字元。因此，使用者需要重命名檔案才能開啟它。 預設選取。
刪除指定類型的附件	如果選擇此選項， 郵件威脅防護會從電子郵件中刪除指定類型的附件。 您可以在檔案遮罩清單中指定要重新命名或從電子郵件中刪除的附件類型。
合併繼承的值	此核取方塊可啟用或停用在繼承子政策設定時合併清單。 如果選取該核取方塊，則父政策清單中的項目將顯示在子政策中，並且可以將項目新增至子原則清單。 如果取消選中此核取方塊，則在繼承政策設定時不會合併清單項目。 預設情況下已清空此核取方塊。
附件類型表	此表列出了您要從電子郵件中刪除的附件類型。 您可以使用對應的按鈕新增、編輯或刪除附件類型。

Web 威脅防護

在管理主控台中，您可以在政策屬性（**關鍵威脅防護** → **Web 威脅防護**）中配置 Web 威脅防護設定。

Web 威脅防護元件設定

設定	描述
啟用 Web 威脅防護	此核取方塊可用或停用 Web 威脅防護。 預設情況下已清空此核取方塊。
受信任網址	這組設定包含**配置**按鈕，該按鈕可開啟**受信任的網址**視窗，您可以在其中指定受信任的網址清單。應用程式不會掃描此清單中包含的網站的內容。
偵測到威脅後的動作	應用程式對在其中偵測到危險物件的網路資源執行的操作： • **封鎖**存取在網路流量中偵測到的所有危險對象，顯示關於被封鎖的存取嘗試的通知，並記錄關於危險對象的資訊（預設值）。 • 當在 Web 流量中偵測到危險物體時**通知**使用者。Web 威脅防護會允許將此物件下載到裝置。同時，應用程式會記錄關於危險物件的資訊並將其新增至活動威脅清單。
掃描設定	這組設定包含**配置**按鈕，該按鈕可開啟**掃描設定**視窗，您可以在其中配置掃描傳入流量的設定。

受信任網址視窗

在此視窗中，您可以新增您認為內容可信任的網址和網頁。

您只能將 HTTP/HTTPS 網址新增至受信任網址清單。您可以使用遮罩來指定網址。不支援使用遮罩指定 IP 位址。此清單預設會空白。您可以新增、編輯和刪除清單中的網址。

實用文章

如何指定遮罩

建立位址遮罩時，使用星號 (*) 作為一個或多個字元的佔位符。如果輸入 *abc* 位址遮罩，它將套用於所有包含“abc”序列的 Web 資源（例如，www.virus.com/download_virus/page_0-9abcdef.html）。若要將星號作為字元包含在位址遮罩中，但不作為遮罩，請輸入兩次 * 字元（例如，www.virus.com/**/page_0-9abcdef.html 表示 www.virus.com/*/page_0-9abcdef.html）。

掃描設定視窗

在此視窗中，您可以設定 Web 威脅防護元件運作期間掃描傳入流量的設定。

Web 威脅防護設定

設定	描述
偵測惡意物件	此核取方塊可啟用或停用針對惡意網址資料庫的連結檢查。 預設情況下已選擇此核取方塊。
偵測釣魚連結	此核取方塊可啟用或停用針對網路釣魚網址資料庫的連結檢查。 預設情況下已選擇此核取方塊。
使用啟發式分析偵測釣魚連結	此核取方塊可啟用或停用啟發式分析偵測釣魚連結。 如果選取**偵測釣魚連結**核取方塊，則此核取方塊可用，並且預設為選取。
偵測廣告軟體	此核取方塊可啟用或停用針對廣告軟體網址資料庫的連結檢查。 預設情況下已清空此核取方塊。
偵測入侵者可以用來損害裝置或資料的合法應用程式	此核取方塊可啟用或停用檢查入侵者可以來損害裝置或資料的合法應用程式資料庫的連接。 預設情況下已清空此核取方塊。

網路威脅防護

在管理主控台中，您可以在政策屬性（**關鍵威脅防護 → 網路威脅防護**）中管理網路威脅防護設定。

網路威脅防護元件設定

設定	描述
啟用網路威脅防護	此核取方塊可啟用或停用網路威脅防護。 預設情況下已清空此核取方塊。
偵測到威脅後的動作	在偵測到典型的網路攻擊的網路活動時執行的操作。 • **通知**使用者。應用程式允許網路活動並記錄關於偵測到的網路活動的資訊。 • **封鎖**來自攻擊者裝置的網路活動並記錄關於偵測到的網路活動的資訊（預設值）。
封鎖攻擊裝置	此核取方塊可啟用或停用在偵測到網路攻擊嘗試時封鎖網路活動。 預設情況下已選擇此核取方塊。
攻擊裝置封鎖時長（分鐘）	您可以在此欄位中指定封鎖攻擊裝置的持續時間（分鐘）。在指定時間之後，Kaspersky Endpoint Security 將允許來自該裝置的網路活動。 可能的值：從 1 到 32768 的整數。 預設值：60。
排除項目	這組設定包含**配置**按鈕，它可開啟**排除項目**視窗，您可以在其中指定 IP 位址清單。來自這些 IP 位址的網路攻擊將不會被封鎖。

排除視窗

在此視窗中，您可以新增不會封鎖網路攻擊的 IP 位址。

此清單預設會空白。

您可以新增、編輯和刪除清單中的 IP 位址。您可以指定 IPv4 和 IPv6 格式的 IP 位址。

防火牆管理

在管理主控台中，您可以在政策屬性（**關鍵威脅防護 → 防火牆管理**）中設定防火牆管理設定。

防火牆管理設定

設定	描述
啟用防火牆管理	此核取方塊可啟用或停用防火牆管理。 預設情況下已清空此核取方塊。
網路封包規則	這組設定包含**配置**按鈕。點擊此按鈕將開啟**網路封包規則**視窗。在此視窗中，您可以設定防火牆管理元件在偵測到網路連線嘗試時套用的網路封包規則。
可用網路	這組設定包含**配置**按鈕。點擊此按鈕將開啟**可用網路**視窗。在此視窗中，您可以設定防火牆管理元件將監控的網路清單。
傳入連線	在此下拉清單中，您可以選擇對傳入網路連線執行的操作： • **允許**網路連線（預設值）。 • **封鎖**網路連線。
傳入封包	在此下拉清單中，您可以選擇對傳入封包執行的操作： • **允許**傳入封包（預設值）。 • **封鎖**傳入封包。
總是新增網路代理連接埠的允許規則	此核取方塊可啟用或停用自動新增網路代理連接埠的允許規則。 預設情況下已選擇此核取方塊。

網路封包規則視窗

網路封包規則表包含防火牆管理元件用於網路活動監控的網路封包規則。您可以設定下表中所述的網路封包規則的設定。

網路封包規則設定

設定	描述
名稱	網路封包規則名稱。
操作	防火牆管理偵測到網路活動時要執行的操作。
本機位址	安裝了 Kaspersky Endpoint Security 並可以傳送和/或接收網路封包的裝置的網路位址。
遠端位址	可以傳送和/或接收網路封包的遠端裝置的網路位址。
Logging	此列顯示應用程式是否記錄網路封包規則的操作。 如果值為**Yes**，則應用程式將記錄網路封包規則的操作。 如果值為**No**，則應用程式不會記錄網路封包規則的操作。

預設情況下，網路封包規則表是空的。

您可以在表中新增、編輯、刪除、上移和下移網路封包規則。

增加了網路封包規則視窗

在這個視窗中，您可以配置新增的網路封包規則設定。

設定	描述
協定	您可以選擇要監控網路活動的資料傳輸協定的類型： • **任何**（預設值） • **GRE** • **ICMP** • **ICMPv6** • **IGMP** • **TCP** • **UDP**
方向	您可以指定被監控的網路活動的方向： • **傳入封包**。如果選擇此選項，防火牆管理元件將僅監控傳入的封包。 • **傳入**。如果選擇此選項，防火牆管理元件將僅監控傳入的連線。 • **傳入/傳出**（預設設定）。如果選擇此選項，防火牆管理元件將監控傳入和傳出的連線。 • **傳入/傳出封包**。如果選擇此選項，防火牆管理元件將監控傳入和傳出的封包。 • **傳出封包**。如果選擇此選項，防火牆管理元件將僅監控傳出的封包。 • **傳出**。如果選擇此選項，防火牆管理元件將僅監控傳出的連線。
ICMP 類型	您可以指定 ICMP 類型。防火牆管理元件監控主機或閘道傳送的指定類型的訊息。 如果選擇了**指定**選項，則會顯示用於輸入 ICMP 類型的欄位。 如果在**協議**下拉清單中選擇了**ICMP**或**ICMPv6**資料傳輸協定，則會顯示此視窗。
ICMP 代碼	您可以指定 ICMP 代碼。防火牆管理元件可監控主機或閘道傳送的 **ICMP 類型**欄位中指定的類型、**ICMP 代碼**欄位中指定的代碼的訊息。 如果選擇了**指定**選項，則會顯示用於輸入 ICMP 代碼的欄位。 如果在**協議**下拉清單中選擇了**ICMP**或**ICMPv6**資料傳輸協定，則會顯示此視窗。
遠端連接埠	您可以指定要監控連線的遠端裝置的連接埠號碼或連接埠範圍。 如果選擇了**已指定**選項，則會顯示用於輸入連接埠號的欄位。 只有在**協定**下拉清單中選擇了**TCP**或**UDP**資料傳輸協定時，才會顯示此視窗。
本機連接埠	您可以指定要監控連線的本機裝置的連接埠號碼或連接埠範圍。 如果選擇了**已指定**選項，則會顯示用於輸入連接埠號的欄位。 只有在**協定**下拉清單中選擇了**TCP**或**UDP**資料傳輸協定時，才會顯示此視窗。
遠端位址	您可以指定能夠傳送和接收網路封包的遠端裝置的網路位址： • **任何位址**（預設值）。如果選擇此項，網路規則將控制具有任何 IP 位址的遠端裝置傳送和/或接收的網路封包。 • **指定的位址或位址範圍**。如果選擇此選項，網路規則將控制下表中指定的 IP 位址的遠端裝置傳送和接收網路封包。點擊表格上方的**新增**按鈕將開啟**新增 IP 位址**視窗，您可以在其中指定裝置的 IP 位址、網路位址或 IP 位址範圍。 • **依照網路類型**。如果選擇此項，網路規則將控制具有與所選網路類型關聯的 IP 位址的遠端裝置傳送和接收的網路封包：**公用網路**、**區域網路**或**受信任網路**。
本機位址	您可以指定安裝了 Kaspersky Endpoint Security 且可以傳送和接收網路封包的裝置的網路位址： • **任何位址**（預設值）。如果選擇此選項，網路規則將控制安裝了 Kaspersky Endpoint Security 的裝置傳送和/或接收的網路封包，而不管它們的 IP 位址如何。 • **指定的位址或位址範圍**。如果選擇此選項，網路規則將控制安裝了 Kaspersky Endpoint Security 的裝置的網路位址，這些裝置可以傳送和接收網路封包。這些網路位址在下表中指定。點擊表格上方的**新增**按鈕將開啟**新增 IP 位址**視窗，您可以在其中指定裝置的 IP 位址、網路位址或 IP 位址範圍。
操作	您可以選擇防火牆管理元件偵測到網路活動時要執行的操作： • **封鎖**網路活動。 • **允許**網路活動（預設值）。
Logging	您可以指定網路規則的操作是否記錄在報告中。
規則名稱	輸入網路封包規則名稱的欄位。

新增 IP 位址視窗

在此視窗中，您可以指定裝置的 IP 位址、網路位址或 IP 位址範圍。

您可以指定多個位址；每個位址輸入在新的一行上，以方便複製。

可用網路視窗

可用網路表包含由防火牆管理元件控制的網路。預設情況下，可用網頁表是空的。

可用網路設定

設定	描述
IP 位址	網路 IP 位址。
網路類型	網路類型（**公用網路**、**區域網路**或**受信任網路**）。

您可以新增、編輯和刪除可用網路。

網路連線視窗

在此視窗中，您可以設定防火牆管理元件將監控的網路連線。

網路連線

設定	描述
IP 位址	用於輸入網路 IP 位址的欄位。
網路類型	您可以選擇網路類型： • **公用** • **本機** • **受信任**

安全控制

裝置控制

在管理主控台中，您可以在政策屬性（**安全控制 → 裝置控制**）中管理裝置控制設定。

裝置控制設定

設定	描述
啟用裝置控制	此核取方塊可啟用或停用裝置控制。 預設情況下已選擇此核取方塊。
受信任裝置	這組設定包含**配置**按鈕。點擊此按鈕將開啟"**受信任裝置**"視窗。在此視窗中，您可以將裝置新增至受信任裝置清單。
裝置控制操作模式	對嘗試存取根據裝置控制規則受到限制的裝置做出的回應： • **通知**。如果您選取此選項，Kaspersky Endpoint Security 會測試所選的存取模式，並針對偵測到的裝置存取嘗試產生事件。 • **封鎖**（預設值）。如果選擇此選項，Kaspersky Endpoint Security 將套用為裝置或匯流排設定的存取模式。
裝置控制設定	這組設定包含開啟視窗的按鈕，您可以在其中按類型和連線匯流排配置裝置的存取模式。
允許請求臨時存取權限	如果選取此核取方塊，使用者可以在應用程式的圖形介面或命令列中請求暫時存取被封鎖的裝置。
訊息範本	這組設定包含**配置**按鈕。點擊此按鈕將開啟**訊息範本**視窗。

受信任裝置視窗

此表包含受信任裝置的清單。預設情況下，該表是空的。

受信任裝置設定

設定	描述
裝置 ID	受信任裝置的 ID。
裝置名稱	受信任裝置名稱。
裝置類型	受信任裝置類型（例如，硬碟或智慧卡讀卡器）。
主機名稱	受信任裝置所連線的用戶端裝置的名稱。
使用者或群組名稱	裝置受信任的使用者或群組的名稱。
備註	與受信任裝置相關的註解。

您可以使用**新增**按鈕將裝置新增至受信任裝置清單，具體操作如下：

- 指定裝置 ID 或裝置 ID 遮罩（**新增→ 按 ID 或遮罩新增裝置**）。
- 從受管理裝置上偵測到的裝置清單中選擇所需裝置（**新增→ 從主機上偵測到的裝置清單中選擇裝置**）。
- 從卡巴斯基安全管理中心中的裝置控制事件中偵測到的裝置清單中選擇所需裝置（**新增 → 基於事件新增裝置**）。

您可以在表格中編輯和刪除受信任裝置。

您也可以透過點擊**進階 → 匯出所選**或**進階 → 匯出全部**按鈕將已新增的裝置清單匯出到檔案，並透過點擊**進階 → 匯入**按鈕從 JSON 檔案匯入裝置清單。

有三種匯入模式：

- **與現有清單合併**：匯入時合併受信任裝置清單。如果檔案中已存在此裝置 ID 的項目，則會更新現有項目的設定。對於先前不在清單中的裝置，將會新增項目。
- **新增至現有清單**：匯入時將受信任裝置新增至清單。僅將先前不在裝置清單中的裝置項目新增至清單中。
- **取代現有清單**：取代受信任裝置清單。現有受信任裝置清單將被檔案中的清單取代。

受信任裝置（裝置 ID）視窗

在此視窗中，您可以透過裝置識別碼將其新增至受信任裝置清單。

按 ID 新增裝置

設定	描述
裝置 ID	用於輸入要新增至受信任裝置清單的裝置的識別碼或識別碼遮罩的欄位。 若要指定識別碼，您可以使用下列通配符：*（任意字元序列）或？（任意單一字元）。例如，您可以指定 USBSTOR* 遮罩以允許存取所有 USB 磁碟機。
在主機上尋找	點擊該按鈕將顯示使用指定 ID 或遮罩在連線的用戶端裝置上發現的裝置。如果**裝置 ID** 欄位不為空，則按鈕可用。

設定	描述
發現裝置	該表包含以下列： • **裝置類型** - 發現的裝置類型（例如，硬碟或智慧卡讀卡器）。 • **裝置 ID** - 發現的裝置的 ID。 • **裝置名稱** - 發現的裝置的名稱。 • **主機名稱** - 發現的裝置所連線的用戶端裝置的名稱。
備註	用於輸入要新增至受信任裝置清單的裝置的註解的欄位（選用）。
允許使用者和/或使用者群組進行存取	此欄位顯示其裝置受信任的使用者和/或群組的名稱。預設值為 **\Everyone**（所有使用者）。
設定	點擊此按鈕將開啟**存取受信任裝置**視窗。

用戶端裝置上的裝置視窗

在此視窗中，您可以透過在現有受管理裝置清單中選擇裝置，將其新增至受信任裝置清單。

只有活動政策已建立且與網路代理的同步已執行時，才可取得現有裝置的資訊（同步間隔在網路代理政策中指定；預設為 15 分鐘）。

如果您新建立了不活動的政策，則清單為空。

從受管理用戶端裝置上偵測到的裝置清單中新增裝置

設定	描述
主機名稱	用於輸入要尋找其連線裝置的受管理裝置的名稱或名稱遮罩的欄位。預設遮罩為 * – 所有受管理裝置。
裝置類型	在此下拉清單中，您可以選擇要搜尋的連線裝置的類型（例如，硬碟或智慧卡讀卡器）。預設選擇**所有裝置**選項。
裝置 ID	用於輸入要尋找的裝置的識別碼或識別碼遮罩的欄位。預設遮罩為 * – 所有裝置。
在主機上尋找	點擊此按鈕時，應用程式將搜尋具有指定參數的裝置。搜尋結果顯示在下表中。
偵測到的裝置清單	該表包含以下列： • **主機名稱** - 發現的裝置所連線的用戶端裝置的名稱。 • **裝置類型** - 發現的裝置類型（例如，硬碟或智慧卡讀卡器）。 • **裝置名稱** - 發現的裝置的名稱。 • **裝置 ID** - 發現的裝置的 ID。

基於裝置控制事件視窗的裝置清單

在此視窗中，您可以建立在卡巴斯基安全管理中心裝置控制事件中偵測到的裝置清單。然後，您可以將此清單中的裝置新增至受信任裝置清單。

您可以選擇一個或多個裝置新增至受信任裝置清單。

如果已啟用裝置控制、存在活動政策且已與網路代理執行同步（同步頻率由網路代理政策指定；預設為每 15 分鐘一次），則提供有關裝置的資訊。

如果您新建立了不活動的政策，則清單為空。

從卡巴斯基安全管理中心事件中偵測到的裝置清單新增裝置

設定	描述
事件類型	您可以使用核取方塊選擇傳送到卡巴斯基安全管理中心的裝置控制事件類型。清單包含在指定類型事件中偵測到的裝置。 預設情況下選擇所有核取方塊。
管理員群組	此欄位用於輸入包含偵測到的裝置所連線的用戶端裝置的管理群組名稱。清單中僅包含已連線到指定管理群組中用戶端裝置的裝置。 您可以指定部分群組名稱。 預設情況下，清單包含連線到任何管理群組中用戶端裝置的裝置。
事件時間段	在下拉清單中，您可以選擇事件發生的時間段。清單包含在指定時間內傳送到卡巴斯基安全管理中心的事件中偵測到的裝置。 預設情況下，清單包含過去一個月內事件中偵測到的裝置。
搜尋裝置	點擊此按鈕時，應用程式將搜尋具有指定參數的裝置。搜尋結果顯示在下表中。
發現裝置	該表包含以下列： • **裝置類型** - 發現的裝置類型（例如，硬碟或智慧卡讀卡器）。 • **裝置 ID** - 發現的裝置的 ID。 • **裝置名稱** - 發現的裝置的名稱。 • **主機名稱** - 發現的裝置所連線的用戶端裝置的名稱。 • **連線日期**是被發現裝置連線的日期。 • **管理群組**是包含偵測到的裝置所連線的用戶端裝置的管理群組的名稱。
備註	用於輸入要新增至受信任裝置清單的裝置的註解的欄位（選用）。
允許使用者和/或使用者群組進行存取	此欄位顯示其裝置受信任的使用者和/或群組的名稱。預設值為 **\Everyone**（所有使用者）。
設定	點擊此按鈕將開啟**存取受信任裝置**視窗。

存取受信任裝置的視窗

在此視窗中，您可以設定使用者或使用者群組對選定受信任裝置的存取。

存取受信任裝置

設定	描述
使用者和/或使用者群組	要信任新增裝置的使用者和群組清單。 預設情況下，該表包含**\Everyone**項目（所有使用者）。 您可以新增、編輯或刪除使用者或使用者群組。

使用者或群組視窗

在此視窗中，您可以指定要信任裝置的使用者或使用者群組。

受信任裝置設定

設定	描述
類型	要信任裝置的**使用者**或**群組**。
使用者或群組名稱	本機使用者或網域使用者的名稱（如果系統允許以此格式輸入使用者名稱，則不指定帶網域的全名，或採用 <網域名稱>\<使用者名稱> 或 <使用者名稱>@<網域名稱> 格式），或要信任裝置的使用者群組名稱。

裝置類型視窗

在這個視窗中，您可以設定各類裝置的存取模式。

裝置類型的存取模式

設定	描述
裝置類型	裝置類型（例如，硬碟、印表機）。
存取模式	裝置存取模式。右鍵點擊滑鼠將開啟一個右鍵功能表，您可以在其中選擇以下項目之一： • **允許**：允許存取所選類型的裝置。 • **封鎖**：禁止存取選定類型的裝置。 • **取決於匯流排**（預設值）：根據連線匯流排的存取模式允許或封鎖對裝置的存取。 • **透過規則**：根據存取規則和排程允許或封鎖裝置存取。此選單指令僅適用於儲存裝置（硬碟、卸除式磁碟機、軟碟機、CD/DVD 磁碟機）。 • **唯讀**：允許對所選類型的裝置進行唯讀存取。此選單指令僅適用於儲存裝置（硬碟、卸除式磁碟機、軟碟機、CD/DVD 磁碟機）。

您可以在雙擊裝置類型時開啟的**設定裝置存取規則**視窗中配置存取規則和排程。

設定裝置存取規則視窗

在此視窗中，您可以為所選的裝置類型設定存取規則和排程。

雙擊**裝置類型**視窗中的裝置類型即可開啟此視窗。

裝置存取規則和排程

設定	描述
使用者和/或使用者群組	此清單包含您可以設定存取排程的使用者和群組。 預設情況下，該表包含**\Everyone**項目（所有使用者）。 您可以新增、編輯或刪除使用者或使用者群組。
裝置存取規則	此表包含使用者和使用者群組的存取排程。它由以下列組成： • **存取排程**– 現有存取排程的名稱。排程旁邊的核取方塊表示該排程是否已被元件使用。 • **存取**– 排程的存取類型：**允許**（授予所選類型的裝置存取權限）或**封鎖**（拒絕所選類型的裝置存取）。 您只能為硬碟、卸除式磁碟機、軟碟機和 CD/DVD 光碟機配置排程。預設情況下，該表包含**預設**存取排程，如果允許透過**連線匯流排**存取此類裝置，則該排程隨時為所有使用者提供對裝置的完全存取權（在**使用者和/或使用者群組**清單中選擇了\Everyone項目）。 您可以新增、編輯或刪除選定使用者的存取排程。**預設**排程不能被修改或刪除。

使用者或群組視窗

在此視窗中，您可以指定應用裝置存取規則的使用者或使用者群組。

設定裝置存取規則

設定	描述
類型	應用程式控制規則套用的**使用者**或**群組**。
使用者或群組名稱	規則適用的本機使用者名稱或使用者群組名稱。

存取排程視窗

在此視窗中，您可以設定裝置存取排程。

裝置存取排程

設定	描述
名稱	存取排程名稱的輸入欄位。
時間間隔	您可以在此表中選擇排程的時間間隔（天數和小時數）。 以綠色突出顯示的間隔包含在排程中。 若要從排程中排除某個間隔，請點擊對應的儲存格。被從排程中排除的間隔以灰色突出顯示。 預設情況下，所有間隔（24/7）被包含在排程中。

連線匯流排視窗

在此視窗中，您可以設定連線匯流排的存取模式。

連線匯流排的存取模式

設定	描述
連線匯流排	被裝置用於連線用戶端裝置的連線匯流排： • **FireWire** • **USB**
存取模式	連線匯流排存取模式。右鍵點擊滑鼠將開啟一個右鍵功能表，您可以在其中選擇以下項目之一： • **允許**（預設）：提供透過此匯流排連線的裝置的存取。 • **封鎖**：拒絕存取使用此連線匯流排連線的裝置。

Web 控制

在管理主控台中，您可以在政策屬性（**安全控制 → Web 控制**）中管理 Web 控制設定。

Web 控制元件設定

設定	描述
啟用 Web 控制	此核取方塊可啟用 Web 控制元件。 預設情況下已清空此核取方塊。

Web 控制設定	此表包含 Web 資源存取規則的清單。Web 控制會依照表中所列的順序套用規則。
	該表包含以下列：
	• **狀態**。Web 資源存取規則的狀態：
	  • *已啟用* — 此規則已啟用，Web 控制在運行期間套用此規則。
	  • *已停用* — 此規則已停用，在 Web 控制執行時不使用。
	  您可以選擇或清除表中的核取方塊，您也可以在**Web 控制規則**視窗中選取或清除**使用此規則**核取方塊。
	• **操作**。當應用程式偵測到嘗試存取符合規則的 Web 資源時要採取的操作。
	• **名稱**。Web資源存取規則名稱。
	您可以新增、編輯、刪除、上移和下移表格中的項目。
	您也可以透過點擊**進階 -> 匯入**從檔案匯入規則清單，透過點擊**其他 -> 匯出選定項目**或**其他 -> 匯出全部**將新增的規則清單匯出到檔案。匯入時，您將被提示取代規則清單或將規則新增至現有清單。

預設規則	在下拉清單中，您可以選擇預設規則來控制應用程式如何管理對其他規則未涵蓋的 Web 資源的存取： • **Allow**（預設值）— 允許存取 Web 資源。 • **Block**— 阻止存取 Web 資源。
訊息範本	這組設定包含**配置**按鈕。點擊此按鈕將開啟**訊息範本**視窗。

Web 控制規則視窗

在此視窗中，您可以配置 Web 資源存取規則的設定。

設定	描述
規則名稱	用於輸入 Web 資源存取規則名稱的欄位。規則名稱必須唯一。
使用此規則	此核取方塊可在應用程式執行時啟用或停用此規則的使用。 如果選取該核取方塊，則啟用該規則，Web 控制會在執行時套用此規則。 如果清除該核取方塊，則規則將被停用，不會在 Web 控制執行時使用。稍後您可以透過選取核取方塊來啟用此 Web 控制規則。 預設情況下已選擇此核取方塊。
過濾內容	在下拉清單中，您可以選擇 Web 資源的內容篩選器： • **不過濾** (預設值).如果選擇此項，則不使用 Web 資源內容篩選器。 • **按內容類別**。當選擇此項時，**選擇**按鈕變為可用。點擊此按鈕將開啟**內容類別選取**視窗。 • **依據資料類型類別**。當選擇此項時，**選擇**按鈕變為可用。點擊此按鈕將開啟**資料類型類別選取**視窗。 • **依據內容類別和資料類型類別**。當選擇此項時，**選擇**按鈕變為可用。點擊這些按鈕將開啟視窗，您可以在其中選擇必要的類別。
過濾位址	在下拉清單中，您可以選擇 Web 資源位址的篩選器： • **任何位址**（預設值）。若選取此項，則不使用網頁網址篩選；Web 控制規則套用於所有 Web 資源位址。 • **指定的位址**。當選擇此項時，**選取位址**按鈕變為可用。點擊此按鈕將開啟**選取位址**視窗，您可以在其中選擇必要的 Web 資源位址。
套用到使用者	在下拉清單中，您可以選擇 Web 資源存取規則套用的使用者： • **所有使用者** (預設值).若選擇此項，則不使用使用者篩選器； Web 控制規則套用於所有使用者。 • **所選使用者**。當選擇此項時，**選取使用者**按鈕將變為可用。點擊此按鈕將開啟**選取使用者**視窗。
規則排程	在下拉清單中，您可以設定 Web 資源存取規則的排程： • **總是**（預設值）。選取此項目時，Web 資源存取規則的套用將不受時間限制，即在任何時候都適用。 • **<排程名稱>**。當選擇此項目時，**刪除**和**編輯**按鈕將變為可用，您可以點擊這些按鈕來刪除或配置排程。 • **新增排程**。選擇此項目將開啟**存取排程**視窗，您可以在其中為 Web 資源存取規則配置新的排程。
規則動作	在下拉清單中，您可以選擇當 Web 控制偵測到嘗試存取與規則相符的 Web 資源時將執行的操作： • **允許**(預設值) — 允許存取 Web 資源。 • **封鎖** — 阻止對 Web 資源的存取並顯示存取被阻止的訊息。 • **通知**— 顯示警告，告知您該 Web 資源不受歡迎。透過點擊警告訊息中的連接，使用者可以存取所請求的 Web 資源。

內容類別選取視窗

在此視窗中，您可以選擇想要為其存取控制的內容類別。

為此，請選取類別旁的核取方塊。

預設情況下所有核取方塊均已清除。

> 選取所有巢狀內容類別的核取方塊不會自動選取父內容類別的核取方塊。

資料類型類別選取視窗

在此視窗中，您可以選擇想要存取控制的類型類別。

為此，請選取類別旁的核取方塊。

預設情況下所有核取方塊均已清除。

選擇位址視窗

在此視窗中，您可以指定想要控制使用者存取權限的 Web 資源的網址。您可以指定多個位址；每個位址輸入在新的一行上，以方便複製。您可以使用遮罩來指定位址。

如果要指定一組位址，請點擊 **新增位址群組** 按鈕來開啟 **選取位址群組** 視窗。

選擇位址群組視窗

此表包含 Web 資源位址群組，這些資源的使用者存取受 Web 控制元件控制。

如果要將一組位址新增至**選取位址**視窗的群組清單中，請選取表中群組名稱旁的核取方塊，然後點擊表格下方的**新增**按鈕。

您可以新增、編輯或刪除表中的項目。

如果要在此視窗的群組清單中新增一組新位址，請點擊表格上方的**新增**按鈕開啟**新增位址**群組視窗。

預設情況下，該表是空的。

新增位址群組視窗

在此視窗中，您可以指定想要控制使用者存取權限的 Web 資源位址群組。您可以在位址群組中指定多個位址；每個位址都輸入在新的一行上，以方便複製。您可以使用遮罩來指定位址。

選擇使用者視窗

此表包含根據規則控制其對 Web 資源的存取的使用者和使用者群組的名稱。

您可以在表格中新增、編輯或刪除項目

如果您要在此視窗的使用者清單中新增使用者和/或使用者群組，請點擊表格上方的**新增**按鈕以開啟**使用者或群組**視窗。

預設情況下，該表是空的。

使用者或群組視窗

在此視窗中，您可以指定套用 Web 資源存取規則的使用者或使用者群組。

設定 Web 資源存取規則

設定	描述
類型	應用程式控制規則套用的**使用者**或**群組**。
使用者或群組名稱	適用該規則的使用者或使用者群組的名稱。

存取排程視窗

在此視窗中，您可以設定 Web 資源存取排程。

Web資源存取排程

設定	描述
名稱	存取排程名稱的輸入欄位。
時間間隔	您可以在此表中選擇排程的時間間隔（天數和小時數）。 以綠色突出顯示的間隔包含在排程中。 若要從排程中排除某個間隔，請點擊對應的儲存格。被從排程中排除的間隔以灰色突出顯示。 預設情況下，所有間隔（24/7）被包含在排程中。

應用程式控制

在管理主控台中，您可以在政策屬性（**安全控制 → 應用程式控制**）中管理應用程式控制設定。

應用程式控制元件設定

設定	描述
啟用應用程式控制	此核取方塊可啟用應用程式控制元件。 預設情況下已清空此核取方塊。
應用程式啟動嘗試時的動作	在偵測到嘗試啟動與配置的規則相符的應用程式時，Kaspersky Endpoint Security 執行的操作： • **套用規則**（預設值）。如果您選擇此選項，Kaspersky Endpoint Security 將套用應用程式控制規則並執行規則中指定的操作。 • **測試規則**。如果您選擇此選項，Kaspersky Endpoint Security 將測試規則並產生關於嘗試啟動符合規則的應用程式的事件。
應用程式控制模式	應用程式控制工作運作模式： • **允許清單**。如果選擇此選項，Kaspersky Endpoint Security 將阻止所有使用者啟動應用程式控制規則中指定的應用程式之外的任何應用程式。 • **拒絕清單**（預設值）。如果選擇此選項，Kaspersky Endpoint Security 將允許所有使用者啟動應用程式控制規則中指定的應用程式以外的任何應用程式。
應用程式 控制規則	這組設定包含**配置**按鈕。點擊此按鈕將開啟**應用程式控制規則**視窗。
套用規則	在下拉清單中，您可以選擇新增規則的方式： • **用政策規則取代本機規則**。當您選擇此項目時，應用程式僅套用政策中指定的規則。 • **新增政策規則到本機規則**（預設值）。如果選擇此項目，應用程式將會將政策中配置的規則與受防護裝置上配置的本機規則一起套用。

應用程式控制規則視窗

應用程式控制規則表包含應用程式控制應用程式元件使用的規則。應用程式控制規則表預設為空。

應用程式控制規則設定

設定	描述
類別名稱	規則使用的應用程式類別的名稱。
狀態	應用程式控制規則的運作狀態： • *已啟用*– 規則已啟用，應用程式控制在運行期間套用此規則。 • *已停用*– 規則已停用，在應用程式控制執行時不使用。 • *測試*– 應用程式控制允許啟動符合規則標準的應用程式，但在報告中記錄關於這些應用程式啟動的資訊。 您可以在**新增規則**視窗中變更規則狀態。

您可以新增、修改或刪除應用程式控制規則。

新增規則視窗

在此視窗中，您可以配置應用程式控制規則的設定。

新增應用程式控制規則

設定	描述
描述	應用程式控制規則的描述。
規則狀態	在下拉清單中，您可以選擇應用程式控制規則的狀態： • *已啟用*– 規則已啟用，應用程式控制在運行期間套用此規則。 • *已停用*– 規則已停用，在應用程式控制執行時不使用。 • *測試*– 應用程式控制允許啟動符合規則標準的應用程式，但在報告中記錄關於這些應用程式啟動的資訊。
類別	設定組包含**配置**按鈕。點擊此按鈕將開啟**應用程式類別**視窗。
使用者及其權限	此表包含適用應用程式控制規則的使用者或使用者群組清單以及指派給他們的存取類型，包含以下列： • **使用者或群組名稱**– 應用程式控制規則適用的使用者的名稱或使用者群組的名稱。 • **存取**– 存取類型：**允許**啟動應用程式或**封鎖**啟動應用程式。 您可以新增、編輯或刪除使用者或使用者群組。

應用程式類別視窗

在此視窗中，您可以新增類別或設定應用程式控制規則的類別設定。

Kaspersky Endpoint Security 不支援使用卡巴斯基安全管理中心的 KL 類別。

應用程式控制類別

設定	描述
類別名稱	新增的應用程式控制類別的清單。
新增	點擊該按鈕即可啟動類別建立精靈。按照精靈的說明進行操作。 有關建立類別的詳細資訊，請參閱卡巴斯基安全管理中心說明。
編輯	點擊此按鈕將開啟類別屬性視窗，您可以在其中變更類別設定。無法編輯**黃金映像 (local)**類別。

使用者或群組視窗

在此視窗中，您可以指定要為其設定規則的本機或網域使用者或使用者群組。

新增應用程式控制規則

設定	描述
類型	應用程式控制規則套用的**使用者**或**群組**。
使用者或群組名稱	應用程式控制規則套用的使用者或使用者群組的名稱。
存取	存取類型：**允許**啟動應用程式或**封鎖**啟動應用程式。

清查

在卡巴斯基安全管理中心管理主控台中，您可以使用*清查*工作對受防護裝置的應用程式執行清查。

您可以建立並執行清查使用者工作。您可以透過編輯工作的設定來管理掃描設定。

卡巴斯基安全管理中心資料庫可以儲存最多 150,000 條已處理檔案的資訊。當達到此記錄數時，將不再處理新檔案。若要復原清查工作，請從安裝了 Kaspersky Endpoint Security 的裝置中刪除卡巴斯基安全管理中心資料庫中根據先前的清查註冊的檔案。

清查工作設定

設定	描述
工作完成後對"黃金映像"類別執行的操作	在下拉清單中，您可以選取清查工作完成後 Kaspersky Endpoint Security 必須對「黃金映像」應用程式類別執行的動作： • **無變更** – 完成清查後，不變更「黃金映像」應用程式類別。這是預設設定。 • **更新或建立（如果不存在）** – 將清查工作在裝置上發現的應用程式新增至「黃金映像」類別。如果該類別不存在，則建立該類別。如果該類別存在，則更新該類別中的應用程式清單。 • **刪除** – 清除「黃金映像」類別的應用程式。此類別會在工作啟動後立即清除，不會對裝置上的檔案執行清查。 您可以在應用程式控制規則中使用「黃金映像」類別。
掃描所有可執行檔	此核取方塊可啟用或停用可執行檔掃描。 預設情況下已選擇此核取方塊。
掃描二進位檔案	此核取方塊可啟用或停用二進位檔案（副檔名為 .elf、.java 和 .pyc 的檔案）的掃描。 預設情況下已選擇此核取方塊。
掃描指令碼	此核取方塊可啟用或停用指令碼掃描。 預設情況下已選擇此核取方塊。
清查範圍	設定組包含**配置**按鈕。點擊此按鈕將開啟**掃描範圍**視窗。

在清查工作的**排除項目**區域，您也可以設定要從掃描中排除的範圍。

掃描範圍視窗

此表包含掃描範圍。該應用程式將掃描表中指定路徑中的檔案和目錄。預設情況下，該表包含一個掃描範圍 - /usr/bin。

清查工作的掃描範圍設定

設定	描述
範圍名稱	掃描範圍名稱。
路徑	應用程式掃描的目錄的路徑。
狀態	狀態表示應用程式是否掃描此範圍。

您可以新增、編輯、刪除、上移和下移表項。

Kaspersky Endpoint Security 依照範圍清單中出現的順序掃描指定範圍內的物件。如果有必要，將子目錄放在清單中高於其父目錄的位置，以便為子目錄配置與父目錄的安全性設定不同的安全性設定。

「新增掃描範圍」視窗

在此視窗中，您可以新增和配置清查工作的掃描範圍。

清查範圍設定

設定	描述
掃描範圍名稱	用於輸入掃描範圍名稱的欄位。該名稱將顯示在**掃描範圍**視窗的表中。 輸入欄位不能為空。
使用此範圍	此核取方塊可啟用或停用執行工作時對此範圍的掃描。 如果選取此核取方塊，應用程式將在執行工作時處理此掃描範圍。 如果清除此核取方塊，應用程式在執行工作時不會處理此掃描範圍。您稍後可以透過選取核取方塊將此範圍包含在工作設定中。 預設情況下已選擇此核取方塊。

設定	描述
檔案系統、存取協定和路徑	您想要包含在掃描範圍中的本機目錄的路徑的輸入欄位。您可以使用遮罩來指定路徑。 該欄位不能為空。
遮罩	此清單包含應用程式在執行工作時掃描的物件的名稱遮罩。 預設情況下，清單包含*遮罩（所有物件）。 您可以新增、編輯或刪除遮罩。

實用文章

如何指定遮罩

您可以使用*（星號）字元來建立檔案或目錄名稱遮罩。

您可以指示單一*字元來表示檔案或目錄名稱中/字元前面的任意字元集（包括空集）。例如，`/dir/*/file` 或 `/dir/*/*/file`。

您可以用兩個連續的*字元來表示檔案或目錄名稱中的任意一組字元（包括空集和/字元）。例如，`/dir/**/file*/` 或 `/dir/file**/`。

**遮罩在目錄名稱中只能使用一次。例如，`/dir/**/**/file`是一個不正確的遮罩。

您可以使用單一?字元來表示檔案或目錄名稱中的任意一個字元。

排除項目部分

掃描排除設定

設定組	描述
排除範圍	這組設定包含**配置**按鈕。按一下此按鈕會開啟**排除範圍**視窗。在此視窗中，您可以定義要排除在監控之外的範圍清單。

排除範圍視窗

此視窗包含掃描排除範圍。該應用程式不會掃描位於表中指定路徑的檔案和目錄。

排除範圍設定

設定	描述
排除範圍名稱	排除範圍名稱。
路徑	被排除掃描的目錄的路徑。
狀態	狀態表明應用程式是否使用此排除。

預設情況下，排除範圍表為空。您可以新增、編輯和刪除表中的項目。

您也可以透過點擊**進階->匯入**從檔案中匯入排除項目清單，透過點擊**進階->匯出選定**或**進階->全部匯出**將新增的排除項目清單匯出到檔案。

新排除範圍視窗

在此視窗中，您可以新增和配置清查工作掃描排除範圍。

排除範圍設定

設定	描述
排除範圍名稱	用於輸入排除範圍名稱的欄位。該名稱將顯示在**排除範圍**視窗的表中。 輸入欄位不能為空。
使用此範圍	此核取方塊可啟用或停用執行工作時的範圍排除。 如果選取此核取方塊，應用程式將在執行工作時排除此範圍。 如果清除此核取方塊，應用程式將在工作執行期間包含此範圍。您稍後可以透過選取核取方塊將該範圍排除在掃描範圍之外。 預設情況下已選擇此核取方塊。
檔案系統、存取協定和路徑	您想要從清查中排除的本機目錄的路徑的輸入欄位。您可以使用遮罩來指定路徑。該欄位不能為空。
遮罩	此清單包含應用程式從掃描中排除的物件的名稱遮罩。 您可以新增、編輯或刪除遮罩。

實用文章

如何指定遮罩

您可以使用 * （星號）字元來建立檔案或目錄名稱遮罩。

您可以指示單一 * 字元來表示檔案或目錄名稱中 / 字元前面的任意字元集（包括空集）。例如，`/dir/*/file` 或 `/dir/*/*/file`。

您可以用兩個連續的 * 字元來表示檔案或目錄名稱中的任意一組字元（包括空集和 / 字元）。例如，`/dir/**/file*/` 或 `/dir/file**/`。

** 遮罩在目錄名稱中只能使用一次。例如，`/dir/**/**/file` 是一個不正確的遮罩。

您可以使用單一 ? 字元來表示檔案或目錄名稱中的任意一個字元。

系統完整性監控

在管理主控台中，您可以在政策屬性（**安全控制 → 系統完整性監控**）中設定系統完整性監控設定。

系統完整性監控設定

設定	描述
啟用系統完整性監控	此核取方塊可啟用或停用系統完整性監控。 預設情況下已清空此核取方塊。
監控範圍	設定組包含**配置**按鈕。按一下此按鈕會開啟**掃描範圍**視窗。
監控排除項目	這組設定包含**配置**按鈕。按一下此按鈕會開啟**排除範圍**視窗。
依照遮罩排序排除項目	這組設定包含**設定**按鈕，該按鈕會開啟**依遮罩排除項目**視窗。

掃描範圍視窗

此表包含系統完整性監控元件的監控範圍。該應用程式監視位於表中指定路徑中的檔案和目錄。預設情況下，表格包含一個監控範圍，**卡巴斯基內部物件**（/opt/kaspersky/kesl/）。

監控範圍設定

設定	描述
合併繼承的值	此核取方塊可啟用或停用在繼承子政策設定時合併清單。 如果選取該核取方塊，則父政策清單中的項目將顯示在子政策中，並且可以將項目新增至子原則清單。 如果取消選中此核取方塊，則在繼承政策設定時不會合併清單項目。 預設情況下已清空此核取方塊。
範圍名稱	監控範圍名稱。
路徑	應用程式防護的目錄的路徑。
狀態	狀態表示應用程式是否掃描此範圍。

您可以新增、編輯、刪除、上移和下移表項。

Kaspersky Endpoint Security 依照物件在範圍清單中出現的順序掃描指定範圍內的物件。如果有必要，將子目錄放在清單中高於其父目錄的位置，以便為子目錄配置與父目錄的安全性設定不同的安全性設定。

「新增掃描範圍」視窗

在此視窗中，您可以新增和設定係統完整性監控元件的監控範圍。

監控範圍設定

設定	描述
掃描範圍名稱	用於輸入監控範圍名稱的欄位。該名稱將顯示在**掃描範圍**視窗的表中。 輸入欄位不能為空。
使用此範圍	此核取方塊可啟用或停用應用程式對此範圍的掃描。 如果選取此核取方塊，則應用程式將在運行過程中控制此監控範圍。 如果清除此核取方塊，應用程式在操作期間不會控制此監控範圍。您稍後可以透過選取核取方塊將此範圍包含在元件設定中。 預設情況下已選擇此核取方塊。
檔案系統、存取協定和路徑	想要包含在監控範圍中的本機目錄的路徑的輸入欄位。 該欄位不能為空。預設路徑是 /opt/kaspersky/kesl。
遮罩	此清單包含應用程式掃描的物件的名稱遮罩。 預設情況下，清單包含*遮罩（所有物件）。 您可以新增、編輯或刪除遮罩。

排除範圍視窗

此視窗包含系統完整性監控元件的監控排除範圍。該應用程式不會掃描位於表中指定路徑的檔案和目錄。

監控排除範圍設定

設定	描述
合併繼承的值	此核取方塊可啟用或停用在繼承子政策設定時合併清單。 如果選取該核取方塊，則父政策清單中的項目將顯示在子政策中，並且可以將項目新增至子原則清單。 如果取消選中此核取方塊，則在繼承政策設定時不會合併清單項目。 預設情況下已清空此核取方塊。
排除範圍名稱	排除範圍名稱。
路徑	排除在監控之外的目錄的路徑。
狀態	指示應用程式在元件運行期間是否將此範圍排除在監控之外。

預設情況下，排除範圍表為空。您可以新增、編輯或刪除表中的項目。

您也可以透過點擊**匯入**從檔案匯入排除範圍清單，透過點擊**匯出**將排除範圍清單匯出到 JSON 格式的檔案。匯入時，系統會提示您取代排除範圍清單或將排除範圍新增至現有清單。

新排除範圍視窗

在此視窗中，您可以新增或配置係統完整性監控元件的監控排除範圍。

監控排除範圍設定

設定	描述
排除範圍名稱	用於輸入排除範圍名稱的欄位。該名稱將顯示在**排除範圍**視窗的表中。輸入欄位不能為空。
使用此範圍	此核取方塊可以啟用或停用應用程式執行時排除監控範圍的功能。 如果選取此核取方塊，應用程式將在元件運行期間將此範圍排除在監控之外。 如果清除此核取方塊，應用程式將在元件操作期間監視此範圍。您稍後可以透過選取核取方塊將該範圍排除在監控之外。 預設情況下已選擇此核取方塊。
檔案系統、存取協定和路徑	您想要新增至排除範圍的本機目錄的路徑的輸入欄位。該欄位不能為空。 預設指定**/**路徑。應用程式將本機檔案系統的所有目錄排除在掃描之外。
遮罩	此清單包含應用程式從監控中排除的物件的名稱遮罩。 預設情況下，清單包含*遮罩（所有物件）。 您可以新增、編輯或刪除遮罩。 點擊**新增**按鈕將開啟**物件遮罩**視窗。在此視窗的**定義物件遮罩**欄位中，您可以指定 Kaspersky Endpoint Security 從監控中排除的檔案的名稱範本。 例如： `*.txt` 遮罩指所有文字檔案。 `*_my_file_??.html` 遮罩指的是以任意字元開頭，以 `_my_file_` 後面跟著任意兩個字元結尾的 html 檔案（例如，2020_my_file_09.html）。

依照遮罩排序排除項目視窗

您可以根據名稱遮罩配置從監控中排除物件。應用程式不會掃描名稱包含指定遮罩的檔案。預設情況下，遮罩清單為空。

您可以新增、編輯或刪除遮罩。

點擊**新增**按鈕將開啟**物件遮罩**視窗。在此視窗的**定義物件遮罩**欄位中，您可以指定 Kaspersky Endpoint Security 從監控中排除的檔案的名稱範本。

例如：
`*.txt` 遮罩指所有文字檔案。
`*_my_file_??.html` 遮罩指的是以任意字元開頭，以 `_my_file_` 後面跟著任意兩個字元結尾的 html 檔案（例如，2020_my_file_09.html）。

您也可以使用 **匯入** 按鈕從檔案匯入排除清單，並使用 **匯出** 按鈕將排除清單匯出至 JSON 檔案。匯入時，您將被提示取代排除項目清單或將排除項目新增至現有清單。

您可以啟用在繼承子政策設定時合併排除項目清單。如果要合併清單項目，請選中**合併繼承的值**核取方塊。如果選取該核取方塊，則父政策清單中的項目將顯示在子政策中，並且可以將項目新增至子原則清單。如果取消選中此核取方塊，則在繼承政策設定時不會合併清單項目。預設情況下已清空此核取方塊。

系統完整性檢查

您可以在管理主控台中藉助*系統完整性檢查*工作執行系統完整性檢查。

您可以建立並執行自訂系統完整性檢查工作。您可以透過編輯工作的設定來管理掃描設定。

在系統完整性檢查工作屬性的**設定**部分中，您可以編輯下表中所列的設定。

系統完整性檢查工作設定

設定	描述
每次工作開始時重建基線	此核取方塊可啟用或停用每次啟動系統完整性檢查工作時重建系統基線。 預設情況下已清空此核取方塊。
檢查 SHA256 雜湊	此核取方塊可啟用或停用在比較檔案的目前狀態與原始狀態時使用檔案雜湊作為標準。 如果清除此核取方塊，應用程式將僅比較檔案大小（如果檔案大小沒有改變，則修改時間不被視為關鍵參數）。 預設情況下已清空此核取方塊。
追蹤監控範圍中的目錄	此核取方塊可啟用或停用系統完整性檢查期間對指定監控範圍內的目錄進行掃描。 預設情況下已清空此核取方塊。
追蹤上次存取檔案的時間	此核取方塊可啟用或停用在系統完整性檢查執行時追蹤檔案存取時間。 預設情況下已清空此核取方塊。
監控範圍	設定組包含**配置**按鈕。按一下此按鈕會開啟**掃描範圍**視窗。

在系統完整性檢查屬性的 **排除範圍** 區段中，您可以定義監控排除項目和依遮罩排除項目。

掃描範圍視窗

此表包含系統完整性檢查工作的監控範圍。該應用程式監視位於表中指定路徑中的檔案和目錄。預設情況下，表格包含一個監控範圍，**卡巴斯基內部物件**（/opt/kaspersky/kesl/）。

監控範圍設定

設定	描述
範圍名稱	監控範圍名稱。
路徑	應用程式防護的目錄的路徑。
狀態	狀態表示應用程式是否掃描此範圍。

您可以新增、編輯、刪除、上移和下移表項。

Kaspersky Endpoint Security 依照物件在範圍清單中出現的順序掃描指定範圍內的物件。如果有必要，將子目錄放在清單中高於其父目錄的位置，以便為子目錄配置與父目錄的安全性設定不同的安全性設定。

「新增掃描範圍」視窗

在此視窗中，您可以新增和設定系統完整性檢查工作的監控範圍。

監控範圍設定

設定	描述
掃描範圍名稱	用於輸入監控範圍名稱的欄位。該名稱將顯示在**掃描範圍**視窗的表中。 輸入欄位不能為空。
使用此範圍	此核取方塊可啟用或停用應用程式對此範圍的掃描。 如果選取此核取方塊，則應用程式將在運行過程中控制此監控範圍。 如果清除此核取方塊，應用程式在操作期間不會控制此監控範圍。您稍後可以透過選取核取方塊將此範圍包含在元件設定中。 預設情況下已選擇此核取方塊。
檔案系統、存取協定和路徑	想要包含在監控範圍中的本機目錄的路徑的輸入欄位。您可以使用遮罩來指定路徑。 該欄位不能為空。 預設路徑是 /opt/kaspersky/kesl。
遮罩	此清單包含應用程式掃描的物件的名稱遮罩。 預設情況下，清單包含*遮罩（所有物件）。 您可以新增、編輯或刪除遮罩。

如何指定遮罩

您可以使用*（星號）字元來建立檔案或目錄名稱遮罩。

您可以指示單一*字元來表示檔案或目錄名稱中/字元前面的任意字元集（包括空集）。例如，`/dir/*/file` 或 `/dir/*/*/file`。

您可以用兩個連續的*字元來表示檔案或目錄名稱中的任意一組字元（包括空集和/字元）。例如，`/dir/**/file*/` 或 `/dir/file**/`。

**遮罩在目錄名稱中只能使用一次。例如，`/dir/**/**/file`是一個不正確的遮罩。

您可以使用單一?字元來表示檔案或目錄名稱中的任意一個字元。

排除項目部分

掃描排除設定

設定組	描述
監控排除項目	這組設定包含**配置**按鈕。按一下此按鈕會開啟**排除範圍**視窗。在此視窗中，您可以定義要排除在監控之外的範圍清單。
依照遮罩排序排除項目	這組設定包含**設定**按鈕，該按鈕會開啟**依遮罩排除項目**視窗。在此視窗中，您可以透過名稱遮罩配置從監控中排除的物件。

排除範圍視窗

此表包含系統完整性檢查元件的掃描排除範圍。該應用程式不會掃描位於表中指定路徑的檔案和目錄。預設情況下，該表為空。

系統完整性檢查工作的掃描排除範圍設定

設定	描述
排除範圍名稱	排除範圍名稱。
路徑	被排除掃描的目錄的路徑。
狀態	指示應用程式在元件運行期間是否將此範圍排除在監控之外。

您可以新增、編輯或刪除表中的項目。

新排除範圍視窗

在此視窗中，您可以新增和設定系統完整性檢查工作的監控排除範圍。

監控排除範圍設定

設定	描述
排除範圍名稱	用於輸入排除範圍名稱的欄位。該名稱將顯示在**排除範圍**視窗的表中。輸入欄位不能為空。
使用此範圍	此核取方塊可以啟用或停用應用程式執行時排除監控範圍的功能。 如果選取此核取方塊，應用程式將在工作操作期間將此範圍排除在監控之外。 如果清除此核取方塊，應用程式將在工作期間監視此範圍。您稍後可以透過選取核取方塊將該範圍排除在監控之外。 預設情況下已選擇此核取方塊。
檔案系統、存取協定和路徑	您想要新增至排除範圍的本機目錄的路徑的輸入欄位。您可以使用遮罩來指定路徑。 該欄位不能為空。 預設指定/路徑。應用程式將本機檔案系統的所有目錄排除在掃描之外。

設定	描述
遮罩	此清單包含應用程式從監控中排除的物件的名稱遮罩。 預設情況下，清單包含*遮罩（所有物件）。 您可以新增、編輯或刪除遮罩。 點擊**新增**按鈕將開啟**物件遮罩**視窗。在此視窗的**定義物件遮罩**欄位中，您可以指定 Kaspersky Endpoint Security 從掃描中排除的檔案的名稱範本。 例如： `*.txt` 遮罩指所有文字檔案。 `*_my_file_??.html` 遮罩指的是以任意字元開頭，以 `_my_file_` 後面跟著任意兩個字元結尾的 html 檔案（例如，2020_my_file_09.html）。

實用文章

如何指定遮罩

您可以使用*（星號）字元來建立檔案或目錄名稱遮罩。

您可以指示單一*字元來表示檔案或目錄名稱中/字元前面的任意字元集（包括空集）。例如，`/dir/*/file` 或 `/dir/*/*/file`。

您可以用兩個連續的*字元來表示檔案或目錄名稱中的任意一組字元（包括空集和/字元）。例如，`/dir/**/file*/` 或 `/dir/file**/`。

**遮罩在目錄名稱中只能使用一次。例如，`/dir/**/**/file`是一個不正確的遮罩。

您可以使用單一?字元來表示檔案或目錄名稱中的任意一個字元。

依照遮罩排序排除項目視窗

您可以根據名稱遮罩配置從監控中排除物件。應用程式不會掃描名稱包含指定遮罩的檔案。預設情況下，遮罩清單為空。

您可以新增、編輯或刪除遮罩。

點擊**新增**按鈕將開啟**物件遮罩**視窗。在此視窗的**定義物件遮罩**欄位中，您可以指定 Kaspersky Endpoint Security 從掃描中排除的檔案的名稱範本。

例如：
`*.txt` 遮罩指所有文字檔案。
`*_my_file_??.html` 遮罩指的是以任意字元開頭，以 `_my_file_` 後面跟著任意兩個字元結尾的 html 檔案（例如，2020_my_file_09.html）。

本機工作

工作管理

在管理主控台中，您可以在政策內容（**本機工作 → 工作管理**）中設定檢視和管理工作的權限。

工作管理設定

設定	描述
允許本機工作	此核取方塊可允許或阻止使用者檢視在 Kaspersky Endpoint Security 中建立的本機工作以及在受管理用戶端裝置上控制這些工作。 如果選取此核取方塊，使用者可以在應用程式圖形介面和命令列中設定和執行工作。 如果取消選取此核取方塊，則不會使用本機工作。排期的本機工作不會執行。無法在應用程式圖形介面或命令列中執行或設定工作。 預設情況下已清空此核取方塊。
允許檢視和管理透過 KSC 建立的工作	此核取方塊可允許或禁止使用者檢視在卡巴斯基安全管理中心中建立的工作以及在用戶端裝置上管理這些工作。 如果選取此核取方塊，則在卡巴斯基安全管理中心中建立的工作將顯示在應用程式圖形介面中。使用者可以在應用程式圖形介面和命令列中啟動和停止這些工作。 如果取消選取此核取方塊，則無法在應用程式圖形介面或命令列中檢視或管理在卡巴斯基安全管理中心中建立的工作。 預設情況下已清空此核取方塊。

進階威脅和目標式攻擊防護

與 Kaspersky Managed Detection and Response 整合

在管理主控台中，您可以在政策內容（**Detection and Response → Managed Detection and Response**）中啟用或停用 MDR 元件，並上傳 MDR BLOB 檔案。

MDR 整合設定

設定	描述
啟用 Managed Detection and Response	此核取方塊可啟用或停用 MDR 元件，這對 Kaspersky Endpoint Security 與 Kaspersky Managed Detection and Response 解決方案的整合是必要操作。 該元件預設為停用。 如果您啟用 MDR 元件且卡巴斯基安全網路已停用或在標準模式下使用，系統將提示您接受卡巴斯基安全網路聲明以允許在延伸模式下使用卡巴斯基安全網路。 如果父政策禁止變更 KSN 設定，則系統會顯示錯誤訊息，且不會啟用 MDR 元件。
上傳	點擊此按鈕將開啟一個標準的 Microsoft Windows 視窗，您可以在其中選取要上傳的 MDR BLOB 檔案。 如果您有租戶，或已使用 MDR BLOB 檔案啟動 MDR 元件，則必須執行此動作。

BLOB 檔案可以在 Kaspersky Managed Detection and Response 分發套件中包含的 MDR 設定檔的 ZIP 壓縮檔案中找到。

上傳 BLOB 檔案，即表示您同意安裝有 Kaspersky Endpoint Security 的裝置的資料將被自動傳送至卡巴斯基進行處理。如果您不同意處理傳輸的資料，請不要上傳該檔案。有關傳輸資料的詳細說明，請參閱 Kaspersky Managed Detection and Response 說明部分。

Kaspersky Endpoint Detection and Response (on-premises) 整合

在管理主控台中，您可以啟用或停用 EDR Expert (on-premises) 元件，並在政策屬性（**Detection and Response → EDR Expert (on-premises)**）中管理將 Kaspersky Endpoint Security 應用程式與 Kaspersky Endpoint Detection and Response (KATA) 元件整合的設定。

如果在網頁主控台中為 EDR Expert (on-premises) 元件選取 **Endpoint Detection and Response Expert（版本 8.0 及更高版本）**，亦即選取 EDR Expert (on-premises) 整合模式，則管理主控台會顯示警告，且 Kaspersky Endpoint Detection and Response (KATA) 整合設定無法使用。您可以在網頁主控台中變更整合模式。

Kaspersky Endpoint Detection and Response (on-premises) 整合設定

設定	描述
啟用 Endpoint Detection and Response Expert（on-premises）	此核取方塊會啟用或停用 EDR Expert (on-premises) 元件，該元件提供與 Kaspersky Endpoint Detection and Response (KATA) 的整合。 該元件預設為停用。
啟用物件執行防禦	此核取方塊會啟用或停用 物件執行防禦 的 EDR Expert (on-premises) 規則。
KATA 伺服器	**配置**按鈕可開啟一個視窗，您可以在其中配置與 KATA 伺服器的連線，以及檢視已配置連線的伺服器清單。
伺服器連線設定	點擊**配置**按鈕將開啟一個視窗，您可以在其中配置連線到 KATA 伺服器的一般設定、新增伺服器憑證以及設定連線到 KATA 伺服器時的雙向身分驗證。
資料傳輸設定	點擊**配置**按鈕將開啟一個視窗，您可以在其中配置將資料傳輸到 KATA 伺服器的設定。

配置 KATA 伺服器連線

表格列出了 KATA 伺服器的連線設定。對於配置了連線的每台伺服器，該表都指示一個 IP 位址（IPv4 或 IPv6）或伺服器的完全限定網域名稱 (FQDN) 和連接埠。

您可以使用表格上方的按鈕和功能表執行以下操作：

- 新增KATA 伺服器連線設定
- 編輯或刪除先前配置的連線設定
- 匯出或匯入已配置的連線設定清單

伺服器連線設定

設定	描述
位址	KATA 伺服器位址 可指定 IP 位址（IPv4 或 IPv6）或完全限定網域名稱 (FQDN)。 為確保在裝置上啟用網路隔離的情況下應用程式發生故障時與伺服器的通訊不會中斷，我們建議指定伺服器的 IP 位址。 預設值：`127.0.0.1`。
連接埠	連線 KATA 伺服器的連線埠。 預設值：`443`。

管理一般 KATA 伺服器連線設定

在此視窗中，您可以配置連線到 KATA 伺服器的一般設定。

KATA 伺服器連線設定

設定	描述
每隔 (分鐘) 向 KATA 伺服器傳送一次同步請求	向 KATA 伺服器傳送同步請求的頻率（以分鐘為單位）。 預設值：`5`。
等待伺服器連線的最長時間（秒鐘）	等待連線到 KATA 伺服器的最長時間（秒）。 預設值：`10`。
等待伺服器回應的最長時間（秒鐘）	等待 KATA 伺服器回應的最長時間（秒）。 預設值：`10`。
允許傳送遙測	此核取方塊可啟用或停用將關於裝置事件（遙測）的資料傳送至 KATA 伺服器。 預設啟用遙測傳送。

伺服器憑證	此部分包含用於新增或刪除伺服器憑證的按鈕：
	• **新增**將開啟一個視窗，您可以在其中新增伺服器憑證。如果尚未新增伺服器憑證，則會顯示該按鈕。
	在用於新增憑證的視窗中，您可以透過以下方式之一新增 KATA 伺服器憑證：
	  • 在**從檔案新增**欄位中，指定包含 DER 或 PEM 格式憑證的憑證檔案的路徑。**瀏覽**按鈕可開啟標準檔案選擇視窗。
	  • 將憑證檔案的內容複製到**輸入憑證詳情**欄位中。
	如果已新增伺服器憑證，則會在 Kaspersky Endpoint Security 端驗證伺服器憑證。這提高了連線的安全性。
	• **刪除**將刪除之前新增的伺服器憑證。該按鈕僅在新增了伺服器憑證後才會顯示。

其他連線防護	本節包含使用雙向身分驗證設定連線的額外安全性的控制：
	• **使用雙向身分驗證**可啟用或停用雙向身分驗證以進一步防護與 KATA 伺服器的連線。若要使用雙向身分驗證，您需要新增用戶端憑證。
	  雙向身分驗證必須在 KATA 伺服器端啟用。
	• **新增**將開啟用於新增用戶端憑證的視窗以增強與 KATA 伺服器連線的安全性。如果選取**使用雙向身分驗證**核取方塊且尚未新增用戶端憑證，則會顯示此按鈕。
	若要新增用戶端憑證，請在憑證新增視窗中指定包含用戶端憑證和私密金鑰的加密容器（PFX 壓縮檔案）的路徑。**瀏覽**按鈕可開啟標準檔案選擇視窗。接下來，在 **加密容器密碼** 欄位中輸入用戶端憑證密碼。
	  此欄位為必填。如果您嘗試在未輸入密碼的情況下儲存設定，則會顯示錯誤訊息。
	如果密碼正確，**確定**按鈕會變為可用。您可以儲存設定。
	• **刪除**會刪除先前新增的客戶端憑證。如果已新增用戶端憑證，則會顯示該按鈕。

配置到 KATA 伺服器的資料傳輸

在此視窗中，您可以配置將資料傳送到 KATA 伺服器的設定。

將資料傳送到 KATA伺服器的設定

設定	描述
傳送事件時的最大延遲（秒鐘）	向 KATA 伺服器傳送事件的最大延遲（以秒為單位）。 預設值：`30`。
啟用事件節流	啟用或停用對傳送至 KATA 伺服器的事件數量進行調整。
每小時的最大事件數量	每小時的最大事件數量 預設值：`3000`。
事件數量超過限制（百分比）	事件數量超過限制（百分比）。如果某一類型的事件（例如，關於登錄檔變更的事件）與總事件數的比例超過設定的閾值（百分比），則傳送事件會受到限制。 預設值：`15`。

Kaspersky Network Detection and Response (KATA) 整合

在管理主控台中，您可以啟用或停用 NDR (KATA) 元件，並在政策屬性（**Detection and Response → Network Detection and Response (KATA)**）中，管理將 Kaspersky Endpoint Security 應用程式與 Kaspersky Network Detection and Response (KATA) 元件整合的設定。

Kaspersky Network Detection and Response (KATA) 整合設定

設定	描述
啟用 Network Detection and Response (KATA)	此核取方塊可啟用或停用 NDR (KATA) 元件。 該元件預設為停用。
NDR 伺服器	**配置**按鈕可開啟一個視窗，您可以在其中配置與 NDR 伺服器的連線，以及檢視已配置連線的伺服器清單。
伺服器連線設定	點擊**配置**按鈕將開啟一個視窗，您可以在其中配置連線到 NDR 伺服器的一般設定、新增伺服器憑證以及設定連線到 NDR 伺服器時的雙向身分驗證。
資料傳輸設定	點擊**配置**按鈕將開啟一個視窗，您可以在其中配置將資料傳輸到 NDR 伺服器的設定。

配置 NDR 伺服器連線

表格列出了 NDR 伺服器的連線設定。對於配置了連線的每台伺服器，該表都指示一個 IP 位址（IPv4 或 IPv6）或伺服器的完全限定網域名稱 (FQDN) 和連接埠。

您可以使用表格上方的按鈕和功能表執行以下操作：

- 新增NDR 伺服器連線設定
- 編輯或刪除先前配置的連線設定
- 匯出或匯入已配置的連線設定清單

伺服器連線設定

設定	描述
位址	NDR 伺服器位址 可指定 IP 位址（IPv4 或 IPv6）或完全限定網域名稱 (FQDN)。 預設值：`127.0.0.1`。
連接埠	連線 NDR 伺服器的連線埠。 預設值：`443`。

管理一般 NDR 伺服器連線設定

在此視窗中，您可以配置連線到 NDR 伺服器的一般設定。

NDR 伺服器連線設定

設定	描述
每隔 (分鐘) 向 NDR 伺服器傳送一次同步請求	向 NDR 伺服器傳送同步請求的頻率（以分鐘為單位）。 預設值：`5`。
等待伺服器連線的最長時間（秒鐘）	等待連線到 NDR 伺服器的最長時間（秒）。 預設值：`10`。

設定	描述
等待伺服器回應的最長時間（秒鐘）	等待 NDR 伺服器回應的最長時間（秒）。 預設值：`10`。

伺服器憑證	此部分包含用於新增或刪除伺服器憑證的按鈕：
	• **新增**將開啟一個視窗，您可以在其中新增伺服器憑證。如果尚未新增伺服器憑證，則會顯示該按鈕。
	在用於新增憑證的視窗中，您可以透過以下方式之一新增 NDR 伺服器憑證：
	  • 在**從檔案新增**欄位中，指定包含 DER 或 PEM 格式憑證的憑證檔案的路徑。**瀏覽**按鈕可開啟標準檔案選擇視窗。
	  • 將憑證檔案的內容複製到**輸入憑證詳情**欄位中。
	如果已新增伺服器憑證，則會在 Kaspersky Endpoint Security 端驗證伺服器憑證。這提高了連線的安全性。
	• **刪除**將刪除之前新增的伺服器憑證。該按鈕僅在新增了伺服器憑證後才會顯示。

其他連線防護	本節包含使用雙向身分驗證設定連線的額外安全性的控制：
	• **使用雙向身分驗證**可啟用或停用雙向身分驗證以進一步防護與 NDR 伺服器的連線。若要使用雙向身分驗證，您需要新增用戶端憑證。
	  雙向身分驗證必須在 NDR 伺服器端啟用。
	• **新增**將開啟用於新增用戶端憑證的視窗以增強與 NDR 伺服器連線的安全性。如果選取**使用雙向身分驗證**核取方塊且尚未新增用戶端憑證，則會顯示此按鈕。
	若要新增用戶端憑證，請在憑證新增視窗中指定包含用戶端憑證和私密金鑰的加密容器（PFX 壓縮檔案）的路徑。**瀏覽**按鈕可開啟標準檔案選擇視窗。接下來，在 **加密容器密碼** 欄位中輸入用戶端憑證密碼。
	  此欄位為必填。如果您嘗試在未輸入密碼的情況下儲存設定，則會顯示錯誤訊息。
	如果密碼正確，**確定**按鈕會變為可用。您可以儲存設定。
	• **刪除**會刪除先前新增的客戶端憑證。如果已新增用戶端憑證，則會顯示該按鈕。

配置到 NDR 伺服器的資料傳輸

在此視窗中，您可以配置將資料傳送到 NDR 伺服器的設定。

將資料傳送到 NDR伺服器的設定

設定	描述
傳送事件時的最大延遲（秒鐘）	向 NDR 伺服器傳送事件的最大延遲（以秒為單位）。 預設值：`30`。
套件中事件的最大數量	一個套件中的最大事件數量。 預設值：`1024`。
伺服器輪詢頻次	向 NDR 伺服器傳送同步請求的頻次（以秒為單位）。 預設值：`450`。
啟用事件節流	啟用或停用對傳送至 NDR 伺服器的事件數量進行調整。
每小時的最大事件數量	每小時的最大事件數量 預設值：`3000`。
事件數量超過限制（百分比）	事件數量超過限制（百分比）。如果某一類型的事件（例如，關於登錄檔變更的事件）與總事件數的比例超過設定的閾值（百分比），則傳送事件會受到限制。 預設值：`15`。

與 KUMA 整合

在管理主控台中，您可以啟用或停用 Kaspersky Endpoint Security 與 Kaspersky Unified Monitoring and Analysis Platform 的整合，並在政策屬性（**KUMA 整合** → **KUMA 整合**）中管理整合設定。

設定	描述
啟用 KUMA 整合	啟用或停用 Kaspersky Endpoint Security 應用程式與 Kaspersky Unified Monitoring and Analysis Platform 解決方案的整合。 預設情況下，KUMA 整合停用。
使用加密連線	此核取方塊可啟用或停用伺服器憑證驗證，以對與 KUMA 伺服器的連線提供額外防護。 若要驗證伺服器憑證，您需要選取此核取方塊並在**KUMA 伺服器**視窗中新增伺服器憑證。 預設情況下已清空此核取方塊。
KUMA 伺服器	**配置**按鈕可開啟**KUMA 伺服器**視窗。在此視窗中，您可以配置與 KUMA 伺服器的連線，並檢視已配置連線的伺服器清單。
KUMA 伺服器連線設定	點擊**配置**按鈕可開啟**伺服器連線設定**視窗，您可以在其中配置連線到 KUMA 伺服器的一般設定、新增伺服器憑證以及設定連線到 KUMA 伺服器時的雙向身分驗證。
傳送事件時的最大延遲（秒鐘）	向 KUMA 伺服器傳送事件的最大延遲（以秒為單位）。 預設值：`30`。

KUMA 伺服器視窗

視窗中的表格顯示了連線到 KUMA 伺服器的設定清單。對於配置了連線的每台伺服器，該表指示：

- 伺服器的 IP 位址（IPv4 或 IPv6）或完全限定網域名稱 (FQDN)。如果您在KUMA 整合設定視窗中選取了**使用加密連線**核取方塊，則必須從購買產品授權時收到的憑證指定伺服器的完全限定網域名稱 (FQDN) 才能使用 KUMA。
- 連線 KUMA 伺服器的連線埠。
- 用於連線 KUMA 伺服器的協定。

您可以使用表格上方的按鈕和功能表執行以下操作：

- 新增 KUMA 伺服器連線設定
- 編輯或刪除先前配置的連線設定
- 匯出或匯入已配置的連線設定清單

KUMA 伺服器視窗

在此視窗中您可以指定 KUMA 伺服器連線設定。

KUMA 伺服器連線設定

設定	描述
位址	KUMA 伺服器位址 可指定 IP 位址（IPv4 或 IPv6）或完全限定網域名稱 (FQDN)。如果您在KUMA 整合設定視窗中選取了**使用加密連線**核取方塊，則必須從購買產品授權時收到的憑證指定伺服器的完全限定網域名稱 (FQDN) 才能使用 KUMA。
連接埠	連線 KUMA 伺服器的連線埠。 預設值：`443`。
協定	用於連線到 KUMA 伺服器的協定：TCP、UDP 或使用壓縮的 HTTP/HTTPS。 選擇 UDP 協定時，不支援使用憑證提供連線防護，且沒有關於與 KUMA 伺服器連線的事件。 預設為 TCP。

KUMA 伺服器連線設定視窗

在此視窗中，您可以配置連線到 KUMA 伺服器的一般設定。

KUMA 伺服器連線設定

設定	描述
等待伺服器連線的最長時間（秒鐘）	等待連線到 KUMA 伺服器的最長時間（秒）。 預設值：5。
伺服器憑證	此部分包含用於新增或刪除伺服器憑證的按鈕。
新增（伺服器憑證）	開啟新增伺服器憑證視窗。 如果尚未新增伺服器憑證，則會顯示該按鈕。
刪除（伺服器憑證）	移除伺服器憑證。 該按鈕僅在新增了伺服器憑證後才會顯示。
其他連線防護	本節包含使用雙向身分驗證設定連線的額外安全性的控制。
使用雙向身分驗證	此核取方塊可啟用或停用雙向身分驗證，以對與 KUMA 伺服器的連線提供額外防護。 若要使用雙向身分驗證，您需要新增用戶端憑證。 雙向身分驗證必須在 KUMA 伺服器端啟用。
新增（用戶端憑證）	開啟用戶端憑證新增視窗以確保與 KUMA 伺服器連線的安全。 如果尚未新增用戶端憑證，則會顯示該按鈕。 如果要為連線配置額外防護，請在 KUMA 伺服器端啟用用戶端憑證驗證，並在此視窗中選取**使用雙向身分驗證**核取方塊。
移除（用戶端憑證）	移除用戶端憑證。 如果已新增用戶端憑證，則會顯示該按鈕。

新增伺服器憑證視窗

在此視窗中，您可以透過以下方式之一新增 KUMA 伺服器憑證：

- 在**從檔案新增**欄位中指定憑證檔案的路徑。**瀏覽**按鈕可開啟標準檔案選擇視窗。指定包含 DER 或 PEM 格式的憑證的檔案的路徑。
- 將憑證檔案的內容複製到**輸入憑證詳情**欄位。

如果已新增伺服器憑證，則會在 Kaspersky Endpoint Security 端驗證伺服器憑證。這提高了連線的安全性。

新增用戶端憑證視窗

在此視窗中，您可以新增用戶端憑證以進一步防護與 KUMA 伺服器的連線。

如果要為連線配置額外的防護，請在 KUMA 伺服器端啟用用戶端憑證驗證，並在**KUMA 伺服器連線設定**視窗中選取**使用雙向身分驗證**核取方塊。

若要新增用戶端憑證，請指定包含用戶端憑證和私密金鑰的加密容器（PFX 壓縮檔案）的路徑。**瀏覽**按鈕可開啟標準檔案選擇視窗。接下來，在 **加密容器密碼** 欄位中輸入用戶端憑證密碼。

此欄位為必填。如果您嘗試在未輸入密碼的情況下儲存設定，則會顯示錯誤訊息。

如果密碼正確，**確定**按鈕會變為可用。您可以儲存設定。

隔離

在管理主控台中，您可以在政策屬性（**一般設定** → **儲存設定**）和受管理裝置屬性（**受管理裝置** → **裝置**索引標籤 → 裝置屬性視窗 → **應用程式**區段 → 應用程式屬性視窗 → **儲存設定**）中管理隔離區設定。

隔離設定

設定	描述
限制隔離區的大小為 (MB)：	此核取方塊可啟用或停用將隔離區的最大大小限制為指定值（以兆位元組為單位）。如果清除該核取方塊，則隔離區容量不受限制。 可用值：1–999999。 如果應用程式在標準模式或 EDR Agent 模式下使用，則預設值為 200；如果應用程式在 Light Agent 模式下使用，則預設值為 100。
隔離區容量達到 (%) 時通知：	此核取方塊可啟用或停用隔離區已滿以產生關於隔離區已滿的事件的百分比限制。如果清除該核取方塊，則不會產生關於隔離區已滿的事件。 可用值：1–100。 預設值：90。

物件的執行防禦

只有在啟用與 Kaspersky Endpoint Detection and Response Expert (on-premises) 或與 Kaspersky Endpoint Detection and Response (KATA) 的整合時，才能在管理主控台中啟用或停用物件的執行防禦。

您可以在政策內容（**應用程式設定** → **Detection and Response** → **EDR Expert (on-premises)**）中啟用或停用物件執行防禦。

位於 **物件執行防禦** 下的 **啟用物件執行防禦** 核取方塊會啟用或停用 EDR Expert (on-premises) 的物件執行防禦規則。

一般設定

在管理主控台中，您可以在政策內容（**一般設定**）中管理定義應用程式整體運作和個別功能運作的一般應用程式設定。

代理伺服器

在管理主控台中，您可以在政策屬性（**一般設定** → **代理伺服器設定**）中管理代理伺服器設定。

代理伺服器設定

設定	描述
不使用代理伺服器	如果選擇此選項，應用程式將不使用代理伺服器。
使用指定的代理伺服器設定	如果選取此選項，應用程式會使用指定的代理伺服器設定連線到卡巴斯基啟動伺服器、資料庫和應用程式模組的更新來源、卡巴斯基安全網路，以及使用 Web 威脅防護元件驗證網站憑證。
位址和連接埠	用於輸入代理伺服器的 IP 位址或網域名稱及其連接埠的欄位。 預設連接埠：3128。 如果選擇了**使用指定的代理伺服器設定**選項，則這些欄位可用。
使用代理伺服器身分驗證	此核取方塊可啟用或停用使用使用者名稱和密碼進行代理伺服器身分驗證。 如果選擇了**使用指定的代理伺服器設定**選項，則此核取方塊可用。 預設情況下已清空此核取方塊。 透過 HTTP 代理連線時，我們建議使用不用於登入其他系統的單獨帳戶。HTTP 代理程式使用不安全的連線，帳戶可能會受到損害。
使用者名稱	用於進行代理伺服器身分驗證的使用者名稱的輸入欄位。 如果選取**使用代理伺服器身分驗證**核取方塊，則此輸入欄位可用。
密碼	用於輸入進行代理伺服器身分驗證的使用者密碼的輸入欄位。 建議確保密碼複雜度和反暴力破解機制，確保密碼在 6 個月內無法被猜到。 點擊**顯示**按鈕將使使用者密碼以明文顯示在**密碼**欄位中。預設情況下，使用者密碼是隱藏的，顯示為星號。 如果選取**使用代理伺服器身分驗證**核取方塊，則文字方塊和按鈕可用。
將卡巴斯基安全管理中心用作代理伺服器進行應用程式啟動	啟用或停用卡巴斯基安全管理中心管理伺服器作為存取卡巴斯基啟動伺服器的代理伺服器。使用啟動碼在沒有網際網路存取的隔離網段中啟動應用程式時，這是必要操作。 如果選取此核取方塊，應用程式會透過具有網際網路存取權限的管理伺服器存取啟動伺服器。 預設情況下已清空此核取方塊。 此設定僅當應用程式在標準模式下使用時才適用。如果應用程式在 Light Agent 模式下使用，則產品授權資訊由 Protection Server 提供。
代理伺服器排除	這組設定包含**設定**按鈕，它可開啟**代理伺服器排除項目**視窗。

代理伺服器排除項目視窗

在此視窗中，您可以設定與 Kaspersky Anti Targeted Attack Platform 解決方案元件整合時代理伺服器的使用，以及您想要繞過代理伺服器的位址清單。

代理伺服器排除

設定	描述
不要為元件使用代理伺服器	選取您不想使用代理伺服器的應用程式元件旁的核取方塊： • **Endpoint Detection and Response Expert (on-premises)** – 連線至提供與 Kaspersky Endpoint Detection and Response Expert (on-premises) 或 Kaspersky Endpoint Detection and Response (KATA) 整合的伺服器時，不要使用代理伺服器。 • **Sandbox** — 在連線到提供與 Sandbox 互動的伺服器時不使用代理伺服器。 • **Network Detection and Response (KATA)** — 連線到 Kaspersky Endpoint Detection and Response (KATA) Integration Server 時不使用代理伺服器。
不要為位址使用代理伺服器	此表包含繞過代理伺服器連線的位址清單。 • **IP 位址/DNS 名稱**是您想要在不使用代理伺服器的情況下連線的 IP 位址或 DNS 名稱。您可以使用遮罩（ * 和 ? 字元）來指定位址。 • 您可以選擇在**備註**欄位中輸入評論。 您可以新增、編輯或刪除表中的位址。

掃描工作的 CPU 使用率

在管理主控台中，您可以在政策屬性（**一般設定 → 應用程式設定**，**效能**區段）中啟用或停用 CPU 使用率限制，並設定掃描工作的記憶體使用量限制。

按一下 **效能** 下的 **設定** 會開啟 **掃描工作的效能設定** 視窗，您可以在其中的 **CPU 和記憶體使用** 區段設定限制（請參閱下表）。

CPU 和記憶體使用量設定

設定	描述
限制掃描工作的 CPU 使用率 (%)	此核取方塊可啟用或停用*惡意軟體掃描*、*關鍵區域掃描*、*清查*和*容器掃描*工作的 CPU 使用率限制。 如果選取該核取方塊，則所有處理器核心的最大利用率將不會超過右側欄位中指定的百分比。此欄位數值必須是 10 到 100 之間的整數。 預設情況下已清空此核取方塊。
掃描工作的記憶體使用限制 (MB)	掃描工作的記憶體使用限制的輸入欄位（以兆位元組為單位）。 預設值：8192。

使用電池電源執行工作

在管理主控台中，您可以在政策內容（**一般設定 → 應用程式設定**，**效能**區域）中設定取消已排程工作。

使用電池供電時的工作設定

設定	描述
使用電池供電時略過已排程工作	此核取方塊可啟用或停用取消已排程工作。 預設情況下已選擇此核取方塊。 如果清除此核取方塊，則無論裝置是否使用電池供電，所有工作都會按排程執行。

啟動應用程式

在管理主控台中，您可以在政策屬性（**一般設定 → 應用程式設定**，**應用程式啟動設定**區段）中管理應用程式啟動設定。

在**應用程式啟動設定**下，點擊**配置**按鈕將開啟**應用程式啟動設定**視窗，您可以在其中編輯應用程式啟動設定（請參閱下表）。

應用程式啟動設定

設定	描述
應用程式啟動嘗試連續不成功最大次數	啟動應用程式的最大連續嘗試失敗次數的輸入欄位。 預設值：5。
等待應用程式啟動的最長時間（分鐘）	等待應用程式啟動的最長時間（以分鐘為單位）的輸入欄位，此後 kesl 處理程序將重新啟動。 預設值：3。

收到關鍵更新時自動重新啟動

在管理主控台中，您可以在政策屬性（**一般設定 → 應用程式設定**）中配置安裝關鍵更新時自動重新啟動應用程式。

在**進階應用程式設定**區段中，點擊**配置**按鈕會開啟**其他設定**視窗，您可以在其中配置應用程式在收到關鍵更新時重新啟動（請參閱下表）。

用於套用關鍵更新的設定

設定	描述
收到關鍵更新時自動重新啟動應用程式	此核取方塊會啟用或停用在安裝應用程式後超過 24 小時收到關鍵更新時自動重新啟動應用程式。 預設情況下已清空此核取方塊。 如果選取此核取方塊，則在安裝後經過 24 小時的情況下，應用程式會在收到關鍵更新後重新啟動。

密碼防護

在管理主控台中，您可以在政策內容（**一般設定 → 介面**，**密碼防護** 區段）中配置密碼防護設定。

在 **密碼防護** 下，按一下 **設定** 按鈕會開啟 **密碼防護設定** 視窗，您可在其中編輯密碼防護設定（請參閱下表）。

應用程式啟動設定

設定	描述
啟用密碼防護	此核取方塊會啟用或停用應用程式設定的密碼防護。 預設情況下已清空此核取方塊。
權限	此表包含使用者和群組，您可以為其設定變更應用程式設定的權限。此表包含以下欄位： • **使用者 / 群組** 是本機或網域使用者的名稱，或是已為其設定權限的使用者群組名稱。 • **類型** 是為其設定權限的 **使用者** 或 **群組**。 • **權限** 是允許使用者或群組執行的操作清單。 您可以新增、編輯和刪除使用者或使用者群組。 您可以按一下 **新增** 按鈕來開啟 **使用者/群組的權限** 視窗，您可在其中新增使用者或群組，並設定變更應用程式設定的權限。

追蹤與傾印設定

在管理主控台中，您可以在政策內容（**一般設定 → 應用程式設定**，**偵錯和傾印設定**區段）中管理偵錯和傾印設定。

在**偵錯和傾印設定**下，點擊**配置**會開啟**偵錯和傾印設定**視窗，您可在其中編輯偵錯傾印設定（請參閱下表）。

追蹤與傾印設定

設定	描述
偵錯檔案目錄的路徑	儲存偵錯檔案的目錄路徑的輸入欄位。 預設值：/var/log/kaspersky/kesl。 如果指定其他目錄，請確保執行 Kaspersky Endpoint Security 的使用者對該目錄具有讀取和寫入權限。存取預設的偵錯檔案目錄需要 root 權限。
偵錯檔案最大大小 (MB)	在此欄位中，您可以輸入應用程式偵錯檔案的最大大小（以兆位元組為單位）。 預設值：500。

設定	描述
偵錯檔案最大數量	在此欄位中，您可以輸入應用程式偵錯檔案的最大數量。 預設值：10。
應用程式崩潰時建立傾印檔案	此核取方塊可啟用或停用應用程式崩潰時建立傾印檔案。 預設情況下已清空此核取方塊。
傾印檔案目錄的路徑	輸入欄位，用於輸入儲存傾印檔案的目錄的路徑。輸入欄位限制為 128 個字元。 預設值：/var/opt/kaspersky/kesl/common/dumps。

應用程式的駐留記憶體使用率

在管理主控台中，您可以在政策屬性（**一般設定** → **應用程式設定**）中設定駐留記憶體使用量限制。

在**進階應用程式設定**部分，點擊**配置**按鈕將開啟**其他設定**視窗，您可以在其中配置駐留記憶體使用限制（請參閱下表）。

若要套用變更，請在政策套用後，重新啟動受管理裝置上的 Kaspersky Endpoint Security 應用程式。

應用程式的駐留記憶體使用量設定

設定	描述
應用程式記憶體使用	在下拉清單中，您可以選擇如何限制駐留記憶體使用： • **無限制**。如果選擇此選項，駐留記憶體的使用不受限制。 • **自動受限制（建議）**。選取此項目時，將自動限制駐留記憶體的使用量（預設值）。 • **限制為總量的百分比**。選擇此項後，**記憶體使用限制 (%)**欄位將可用，您可以在其中以百分比形式指定必要值。 • **限制為值 (MB)**。選擇此項後，**記憶體使用限制 (MB)**欄位將可用，您可以在其中指定所需的值（以兆位元組為單位）。 • **限製為其中最低 (%, MB)**。選擇此項目時，**記憶體使用限制 (%)**和**記憶體使用限制 (MB)**欄位將變為可用，您可以在其中指定必要的值。 • **限製為其中最高 (%, MB)**。選擇此項目時，**記憶體使用限制 (%)**和**記憶體使用限制 (MB)**欄位將變為可用，您可以在其中指定必要的值。
記憶體使用限制 (%)	記憶體使用限制的輸入欄位（以百分比表示）。 預設值：50。
記憶體使用限制 (MB)	記憶體使用限制的輸入欄位（以兆位元組為單位）。 預設值：2000。

加密連線掃描

在管理主控台中，您可以在政策屬性（**一般設定** → **網路設定**）中管理網路流量掃描設定。

設定	描述
啟用加密連線掃描	此核取方塊可啟用或停用加密連線掃描。 預設情況下已選擇此核取方塊。

加密連線設定	此區域包含加密連線掃描設定：
	• **造訪具有不受信任憑證的網域**可指定應用程式在遇到憑證不受信任的網域時必須執行的動作：
	  • **允許**（預設值）— 允許連線到包含不受信任憑證的網域。
	  • **封鎖**— 阻止連線到包含不受信任憑證的網域。
	• **造訪包含網路流量掃描錯誤的網域**可指定應用程式在遇到有網路流量掃描錯誤的網域時必須執行的動作：
	  • **允許並將網域新增至排除項目**（預設值）– 將導致錯誤的網域新增至具有掃描錯誤的網域清單中，並且在存取此網域時不掃描加密的網路流量。
	  • **封鎖**— 阻止與出現掃描錯誤的網域連線。
	• **憑證驗證政策**是應用程式用來驗證憑證是否有效的方法：
	  • **本機檢查**：應用程式不使用網際網路來驗證憑證。
	  • **完整檢查**（預設值）：應用程式使用網際網路來檢查並下載驗證憑證所需的缺失憑證鏈。

受信任網域	這組設定包含**配置**按鈕，它可開啟**受信任網域**視窗，您可以在其中配置受信任網域清單。
受信任的根憑證	這組設定包含**配置**按鈕。點擊此按鈕將開啟"**受信任的根憑證**"視窗。在此視窗中，您可以配置 Kaspersky Endpoint Security 在掃描加密連線時必須視為受信任的根憑證清單。
流量攔截排除項目	此設定群組包含**設定**按鈕，點擊即可開啟**流量攔截排除項目**視窗。在此視窗中，您可以管理應用程式排除於攔截範圍外的連線設定。
網路連接埠設定	這組設定包含**配置**按鈕。點擊此按鈕將開啟**監控的連接埠**視窗。
進階設定	此設定群組包含**配置**按鈕，點擊即可開啟**流量攔截模式**視窗。在此視窗中，您可以配置流量攔截模式： • **使用 eBPF**。如果選擇此選項，應用程式將使用 eBPF 技術攔截流量。 • **使用 iptables**（預設）。如果選擇此選項，應用程式將使用 iptables 技術攔截流量。 若要變更流量攔截模式，需要重新啟動應用程式。重新啟動會中斷已建立的網路連線。

受信任網域視窗

此清單包含將從掃描中排除的網域名稱和網域遮罩。應用程式不會掃描造訪指定網域時建立的連線。

範例： `*example.com`。例如，`*example.com/*`不正確，因為需要指定網域位址而不是網頁。

此清單預設會空白。您可以從受信任網域清單中新增、編輯或刪除網域。

受信任憑證視窗

您可以設定 Kaspersky Endpoint Security 認為受信任的根憑證清單。受信任的根憑證清單在掃描加密連線時使用。

每個憑證都會顯示以下資訊：

- 憑證主體
- 憑證序號
- 憑證發佈者

- 憑證開始日期
- 憑證到期日期
- SHA256 憑證指紋

預設情況下，憑證清單為空。

您可以新增或刪除憑證。

點擊**新增**按鈕會開啟一個視窗，您可以在其中透過以下方式之一將憑證新增至受信任憑證清單：

- 指明憑證檔案的路徑。**瀏覽**按鈕可開啟標準檔案選擇視窗。指示包含憑證的檔案的路徑，採用 DER 或 PEM 格式。
- 將憑證檔案的內容複製到**輸入憑證詳情**欄位。

流量攔截排除項目視窗

該表包含應用程式從流量攔截範圍中排除的連線設定：

- **遠端 IP 位址**是被排除於攔截範圍外的流量往來的 IP 位址（依流量方向而定）。
- **目的端連接埠**是受防護裝置上的連接埠（入站流量攔截排除）或遠端裝置上的連接埠（出站流量攔截排除）。
- **流量方向**是連線中的流量方向：輸入或輸出。

您可以新增、編輯或刪除排除項目。

流量攔截排除項目視窗

在此視窗中，您可以新增流量攔截排除項目。為此，您需要指定以下連線設定：

- **遠端 IP 位址**是遠端裝置的 IPv4 或 IPv6 位址。依流量方向而定，來自指定 IP 位址的流量（輸入流量排除）或傳送至指定 IP 位址的流量（輸出流量排除）將被排除。
- **目的地連接埠**，依流量方向而定：
  - 受防護裝置上的連接埠（輸入流量排除）。從遠端裝置傳送至該連接埠的流量將排除於攔截範圍外。
  - 遠端裝置上的連接埠（輸出流量排除）。從受防護裝置傳送至該連接埠的流量將排除於攔截範圍外。
- **流量方向**是排除連線中的流量方向。您可以為輸入流量或輸出流量設定排除項目。

在排除項目中，您可以指定不含連接埠的遠端裝置 IP 位址或不含 IP 位址的目的地連接埠。

> 如果在輸入流量排除規則中僅指定遠端裝置的 IP 位址（未指定受防護裝置上的連接埠），則來自遠端裝置的所有流量都將排除於攔截範圍外。建議僅為受信任裝置的流量設定此排除規則。

監控的連接埠

網路連接埠設定

設定	描述
監控所有網路連接埠	如果選擇此選項，應用程式將監控所有網路連接埠。
僅監控選定的網路連接埠	如果選擇此選項，應用程式將僅監控表中指定的網路連接埠。 預設情況下已勾選此選項。
網路連接埠設定	如果選擇**僅監控選定的網路連接埠**選項，此表包含應用程式監控的網路連接埠。該表包含兩列： • **連接埠**— 監控的連接埠。 • **描述**— 監控的連接埠的描述。 預設情況下，此表顯示通常用於傳輸郵件和網路流量的網路連接埠清單。網路連接埠清單包含在應用程式套件中。 您可以新增、編輯和刪除表中的項目。

全域排除項目

在管理主控台中，您可以在政策屬性（**一般設定 → 全域排除項目**）中設定全域排除項目。

排除的掛接點設定群組包含一個**配置**按鈕。點擊此按鈕將開啟**排除的掛接點**視窗。

視窗中的清單包含排除的掛載點的路徑。此清單預設會空白。

您可以新增、編輯和刪除清單中的項目。

掛載點路徑視窗

掛載點設定

設定	描述
檔案系統、存取協定和路徑	設定區塊可讓您設定掛載點的定位。 在檔案系統下拉清單中，您可以選擇要新增至掃描排除的目錄所在的檔案系統類型： • **Local**：本機掛載點。 • **已掛接**：使用 Samba 或 NFS 協定掛載到裝置上的遠端目錄。 • **所有遠端掛載**— 使用 Samba 和 NFS 協定掛載在裝置上的所有遠端目錄。
	如果檔案系統下拉清單選擇的是**已掛接**，則可以在右側的下拉清單中選擇遠端存取協定： • **NFS**：使用 NFS 協定掛載在裝置上的遠端目錄。 • **Samba**：使用 Samba 協定安裝在裝置上的遠端目錄。 • **自訂**：下面欄位中指定的裝置檔案系統的所有資源。
	如果在檔案系統下拉清單中選擇**本機**，則您可以在輸入欄位中輸入要從檔案操作攔截中排除的掛載點的路徑。您可以使用遮罩來指定路徑。 掛載點的指定方式必須與 `mount` 指令輸出中顯示的方式相同。
檔案系統名稱	此欄位用於輸入要從檔案操作攔截中排除的目錄所在的檔案系統的名稱。 如果在檔案系統下拉清單中選擇了“**已掛接**”類型，並且在右側的下拉清單中選擇了“**自訂**”項目，則該欄位可用。

實用文章

如何指定遮罩

您可以使用*（星號）字元來建立檔案或目錄名稱遮罩。

您可以指示單一*字元來表示檔案或目錄名稱中/字元前面的任意字元集（包括空集）。例如，`/dir/*/file` 或 `/dir/*/*/file`。

您可以用兩個連續的*字元來表示檔案或目錄名稱中的任意一組字元（包括空集和/字元）。例如，`/dir/**/file*/` 或 `/dir/file**/`。

**遮罩在目錄名稱中只能使用一次。例如，`/dir/**/**/file`是一個不正確的遮罩。

您可以使用單一?字元來表示檔案或目錄名稱中的任意一個字元。

從掃描中排除處理程序記憶體

在管理主控台中，您可以在政策屬性（**一般設定** → **排除處理程序記憶體**）中設定將處理程序記憶體排除於掃描之外。

點擊**從掃描中排除處理程序記憶體**下的**配置**將開啟一個視窗，您可以在其中建立排除項目清單。

從掃描中排除處理程序記憶體視窗中的清單包含應用程式從處理程序記憶體掃描中排除的處理程序的路徑。您可以使用遮罩來指定路徑。此清單預設會空白。

您可以啟用在繼承子政策設定時合併排除項目清單。若要合併清單項，請在**從掃描中排除處理程序記憶體**視窗中選取**合併繼承的值**核取方塊。如果選取該核取方塊，則父政策清單中的項目將顯示在子政策中，並且可以將項目新增至子原則清單。如果取消選中此核取方塊，則在繼承政策設定時不會合併清單項目。預設情況下已清空此核取方塊。

實用文章

如何指定遮罩

您可以使用*（星號）字元來建立檔案或目錄名稱遮罩。

您可以指示單一*字元來表示檔案或目錄名稱中/字元前面的任意字元集（包括空集）。例如，`/dir/*/file` 或 `/dir/*/*/file`。

您可以用兩個連續的*字元來表示檔案或目錄名稱中的任意一組字元（包括空集和/字元）。例如，`/dir/**/file*/` 或 `/dir/file**/`。

**遮罩在目錄名稱中只能使用一次。例如，`/dir/**/**/file`是一個不正確的遮罩。

您可以使用單一?字元來表示檔案或目錄名稱中的任意一個字元。

備份

在管理主控台中，您可以在政策屬性（**一般設定** → **儲存設定**）和受管理裝置屬性（**受管理裝置** → **裝置**頁籤 → 裝置屬性視窗 → **應用程式**區段 → 應用程式屬性視窗 → **儲存設定**）中管理備份設定。

備份設定

設定	描述
儲存物件不超過以下時間（天）	此核取方塊可啟用或停用備份儲存中物件的儲存期限限制（以天為單位）。 可用值：0–10000。 如果指定 0，則在備份儲存中儲存物件的期限不受限制。 預設值：30。
限制備份的大小為 (MB)	此核取方塊可啟用或停用最大備份儲存大小（以兆位元組為單位）。 可用值：1–4000。如果清除該核取方塊，則備份的大小將不受限制。 預設情況下已清空此核取方塊。

偵測駭客可用來造成危害的應用程式

在管理主控台中，您可以在政策屬性（**一般設定** → **應用程式設定**，**掃描設定**區段）中設定對入侵者可用於危害裝置或資料的合法應用程式的偵測。

入侵者可用於危害裝置或資料的應用程式偵測設定

設定	描述
偵測入侵者可以用來損害裝置或資料的合法應用程式	此核取方塊會啟用或停用對可能被駭客用來危害使用者電腦或資料的合法應用程式的偵測。 預設情況下已清空此核取方塊。

攔截檔案操作

在管理主控台中，您可以在政策內容（**一般設定** → **應用程式設定**，**檔案操作攔截模式**區域）中設定檔案操作攔截模式。

檔案操作攔截設定

設定	描述
掃描期間封鎖對檔案的存取	此核取方塊可啟用或停用在 檔案威脅防護 和 裝置控制 元件、執行防禦動作及 卸除式磁碟機掃描 工作掃描檔案期間封鎖對檔案的存取。 預設情況下已選擇此核取方塊。 如果清除該核取方塊，則允許在掃描持續期間存取任何檔案，並且掃描以非同步模式執行。

傳送資訊至卡巴斯基安全管理中心儲存區

在卡巴斯基安全管理中心中，您可以啟用或停用將備份中的檔案、隔離區的檔案、未處理的檔案和已連線的裝置相關的資料傳輸到卡巴斯基安全管理中心儲存。

用戶端裝置上由卡巴斯基應用程式隔離的檔案一般清單會保存在卡巴斯基安全管理中心中，也可在管理主控台（**進階** → **儲存庫** → **隔離區**）中取得。

卡巴斯基安全管理中心會產生用戶端裝置上由卡巴斯基應用程式置於備份中的檔案一般清單，並可在管理主控台（**進階** → **儲存庫** → **備份**）中取得。

未處理檔案的資訊會顯示在管理主控台的活動威脅清單中（**進階** → **儲存庫** → **活動威脅**）。

安裝在用戶端裝置上或連接至用戶端裝置的裝置資訊會顯示在管理主控台的設備清單中（**進階** → **儲存庫** → **硬體**）。如果啟用了裝置控制，則會傳輸資料。

在用戶端裝置上偵測到的應用程式資訊也會顯示在管理主控台的應用程式清單中（**進階** → **應用程式管理** → **應用程式登錄**）。如果啟用了應用程式控制，則會傳輸資料。

在管理主控台中啟用和停用資料傳輸

在管理主控台中，您可以在政策屬性（**一般設定** → **儲存設定**、**將資料傳輸至管理伺服器**）或受管理裝置的屬性（**受管理裝置** → **裝置**頁籤 → 裝置屬性視窗 → **應用程式**區段 → 應用程式屬性視窗 → **儲存設定**、**將資料傳輸至管理伺服器**區段）中，啟用或停用將資料傳輸至管理伺服器。

點擊**將資料傳輸到管理伺服器**區域中的**配置**將開啟**資料傳輸設定**視窗，您可以在其中啟用或停用將資料傳輸到管理伺服器。

向管理伺服器傳輸資料的設定

設定	描述
關於隔離區中的檔案	此核取方塊可啟用或停用將關於被隔離檔案的資料傳輸到管理伺服器。 預設情況下已選擇此核取方塊。
關於備份中的檔案	此核取方塊可啟用或停用將關於備份中檔案的資料傳輸到管理伺服器。 預設情況下已選擇此核取方塊。
關於未處理的檔案	此核取方塊可啟用或停用向管理伺服器傳送關於掃描期間未處理檔案的通知。 預設情況下已選擇此核取方塊。
關於安裝的裝置	此核取方塊可啟用或停用向管理伺服器傳送關於安裝在用戶端裝置上或已連線到用戶端的裝置的資料。 預設情況下已選擇此核取方塊。
關於在裝置上發現的應用程式	此核取方塊可啟用或停用將清查工作在用戶端裝置上發現的應用程式清單傳送至管理伺服器。 預設情況下已選擇此核取方塊。

系統事件攔截

在管理主控台中，您可以在政策內容（**一般設定** → **作業系統互動設定**，**系統事件攔截設定**區段）中設定系統事件攔截。

> 這些設定僅適用於執行支援 fanotify 技術的作業系統的裝置。

系統事件攔截設定

設定	描述
攔截機制	應用程式使用的系統事件攔截機制： • **Fanotify 技術**（預設）。如果選取此選項，應用程式將使用 fanotify 技術進行系統事件攔截。 • **可更新的內核模組**。如果選取此選項，應用程式將使用可更新的內核模組進行系統事件攔截。
如果可更新的內核模組未能啟動	如果可更新的內核模組未能啟動，應用程式會採取的動作： • **使用 fanotify**（預設）。如果選取此選項，應用程式將切換到 fanotify 技術進行系統事件攔截。 • **停用系統事件攔截**如果應用程式不使用系統事件攔截，則不會執行即時檔案掃描，並且裝置的防護等級會降低。 如果選取了**可更新的內核模組**攔截機制，則此選項可用。

其他遙測設定

在管理主控台中，您可以在政策屬性（**一般設定 → 作業系統互動設定**，**其他遙測設定**區段）中管理其他遙測設定。

其他遙測設定

設定	描述
遙測來源	Kaspersky Endpoint Security 用於收集遙測資料的來源： • **僅使用 eBPF**表示僅使用 eBPF 技術獲取遙測資料。 • **使用 eBPF 和 auditd**（預設）表示使用 eBPF 技術和 auditd 服務獲取遙測資料。
使用 auditd	auditd 服務的模式： • **以獨佔模式使用 auditd**（預設）表示Kaspersky Endpoint Security 以獨佔模式使用 auditd 服務。 • **非獨佔模式**是指 auditd 服務以非獨佔模式使用。 此設定僅在**遙測來源**被設定為**使用 eBPF 和 auditd**時套用。

Light Agent 模式

在管理主控台中，您可以在政策屬性（**Light Agent 模式**）中管理將 Light Agent 連線到 SVM 的設定。

連線至 Integration Server

本節所述的設定僅適用於使用 Kaspersky Endpoint Security 以 Light Agent 模式防護虛擬環境的情況。

如果您希望 Light Agent 透過 Integration Server 接收關於 SVM 的資訊，或希望防護 Protection Server 和 Light Agent 之間的連線，則需要連線到 Integration Server。

此視窗顯示連線 Light Agent 到 Integration Server 的目前設定：伺服器位址和連接埠。**編輯**按鈕可開啟**與 Integration Server 的連線**視窗，您可以在其中配置與 Integration Server 的連線。

連線至 Integration Server 視窗

在此視窗中，您可以指定或變更連線 Light Agent 和 Integration Server 的設定。

設定	描述
位址	安裝 Integration Server 的裝置的 IP 位址（IPv4 格式）或完全限定網域名稱 (FQDN)。 如果安裝了卡巴斯基安全管理中心管理主控台的裝置是網域的一部分，則該欄位預設指示該裝置的網域名稱。 如果安裝了卡巴斯基安全管理中心管理主控台的裝置不屬於網域的一部分，或 Integration Server 安裝在另一台裝置上，則必須手動填寫該欄位。 如果將位址指定為 NetBIOS 名稱、localhost 或 127.0.0.1，與 Integration Server 的連線將完成並顯示錯誤。
連接埠	連線 Integration Server 的連接埠。 預設情況下，指定連接埠為 7271。

如果您的基礎架構中部署了基於 Linux 的高可用性 Integration Server 叢集，則需要將負載均衡器的位址和連接埠指定為用於連線到 Integration Server 的位址和連接埠。如需更多詳細資訊，請參閱 Kaspersky Security for Virtualization Light Agent 說明。

驗證 Integration Server 憑證視窗

如果從 Integration Server 收到的 SSL 憑證包含錯誤或不受信任，則會出現此視窗。

您可以點擊視窗中的連結檢視已收到憑證的詳細資訊。

如果您遇到 SSL 憑證問題，我們建議您確保使用的資料傳輸通道是安全的。

若要繼續連線到 Integration Server，請點擊**略過**按鈕。接收的憑證將在安裝卡巴斯基安全管理中心管理主控台的裝置上，以受信任憑證進行安裝。

Integration Server 視窗中的身分驗證

如果託管卡巴斯基安全管理中心管理主控台的主機不屬於網域，或者您的帳戶不屬於 KLAdmins 本機或網域群組或本機管理員群組，則會出現此視窗。

指定 Integration Server 管理員的密碼（`admin` 帳戶的密碼），點擊**確定**按鈕。

建議確保密碼複雜度和反暴力破解機制，確保密碼在 6 個月內無法被猜到。

以管理員權限連線到 Integration Server 後，政策會自動收到 `agent` 帳戶的密碼，該密碼用於將 Light Agent 連線到 Integration Server。

SVM 發現設定

本節所述的設定僅適用於在 Light Agent 模式下使用 Kaspersky Endpoint Security 的情況。

在此視窗中，您可以選擇 Light Agent 用於發現可連線的 SVM 的方法。

SVM 發現設定

設定	描述
使用 Integration Server	如果選擇此選項，Light Agent 將連線至 Integration Server 以獲取可用於連線的 SVM 清單和其詳情。 如果您想要使用 Integration Server，則需要配置將 Light Agent 連線到 Integration Server 的設定。
使用自訂的 SVM 位址清單	如果選擇此選項，您可以指定此政策管理的 Light Agent 可以連線到的 SVM 清單。Light Agent 將僅連線到清單中指定的 SVM。
SVM 清單	此政策涵蓋的 Light Agent 可以連線到的 SVM 的 IP 位址清單（採用 IPv4 位址格式）或完全限定網域名稱 (FQDN)。 點擊 **新增** 以開啟一個視窗，您可以在其中指定 SVM 的 IPv4 格式 IP 位址或完全限定網域名稱 (FQDN)。您可從新行輸入多個 SVM IP 位址或完全限定網域名稱。 僅指定對應到單一 IP 位址的完全限定網域名稱 (FQDN)。使用與多個 IP 位址相對應的完全限定網域名稱可能會導致應用程式出現錯誤。 您可以透過點擊**刪除**按鈕來刪除清單中選擇的位址。 如果選擇了**使用自訂的 SVM 位址清單**選項，則會顯示 SVM 位址清單。

如果您選擇**使用自訂的 SVM 位址清單**選項，則Light Agent 將使用延伸 SVM 選擇演算法，並在 SVM 上啟用大型基礎設施防護模式（有關更多資訊，請參閱 Kaspersky Security for Virtualization Light Agent 說明），則僅當忽略 SVM 路徑時才可以將 Light Agent 連線到此 SVM。在**SVM 選擇演算法**部分，您需要將**SVM 路徑**設定設為**略過**。如果設定了任何其他值，Light Agent 將無法連線到 SVM。

SVM 連線標籤

在此視窗中，您可以啟用 Light Agent 使用標籤，並指派 Light Agent 將用於連線的標籤。

確保在 Protection Server 設定中也配置了連線標籤的使用：有關更多資訊，請參閱Kaspersky Security for Virtualization Light Agent 的說明。指派了標籤的 Light Agent 只能連線到允許連線到具有該標籤的 Light Agent 的 SVM。

用於使用連線標籤的設定

設定	描述
使用連線標籤	此核取方塊可啟用或停用 Light Agent 使用 SVM 連線標籤。
標籤	分配給 Light Agent 的標籤。 對於一個標籤，可以輸入最長 255 個字元的文字字串。您可使用除 **;** 字元外的任何字元。 如果選取**使用連線標籤**核取方塊，則此欄位可用。

SVM 選擇演算法

在此視窗中，您可以指定 Light Agent 必須使用的 SVM 選擇演算法，並配置使用延伸 SVM 選擇演算法的設定。

設定	描述
使用標準 SVM 選擇演算法	如果選擇此選項，則在虛擬機上安裝並執行後，Light Agent 將選擇連線到 Light Agent 本機的 SVM。有關更多詳細資訊，請參閱Kaspersky Hybrid Cloud Security for Virtualization Light Agent 的說明 。 如果找不到適合連線的本機 SVM，則 Light Agent 會選擇連線 Light Agent 數量最少的 SVM，與 SVM 在虛擬基礎架構中的位置無關。 預設情況下已勾選此選項。
使用延伸 SVM 選擇演算法	如果選擇了此選項，您可以使用**SVM 路徑**滑桿來指定在確定 SVM 相對於 Light Agent 是否為本機時，如何考慮 SVM 在虛擬基礎架構中的位置。Light Agent 只能連線到本機的 SVM。 您也可以指定選擇要連線的 SVM 時不應考慮虛擬基礎架構中的 SVM 路徑。 在選擇 SVM 時，Light Agent 會考慮連線到 SVM 的 Light Agent 的數量，以確保 Light Agent 在可連線的 SVM 之間均勻分佈。

SVM 路徑	可讓您指定虛擬基礎架構中的 SVM 路徑類型，在選擇要連線的 SVM 時會考慮該類型：
	• **Hypervisor**。Light Agent 會選擇要連線的符合下列條件的 SVM（取決於虛擬基礎架構的類型）：
	  • SVM 部署在與已安裝 Light Agent 的虛擬機相同的 Hypervisor 上（在 Microsoft Hyper-V 平台、XenServer、VMware vSphere、KVM、Proxmox VE、Basis、HUAWEI FusionSphere、Nutanix Acropolis、ALT Virtualization Server、Astra Linux、Numa vServer 或 Basis Dynamix Standard 上的虛擬基礎架構中）。
	  • SVM 位於與安裝 Light Agent 的虛擬機相同的伺服器群組中（在執行於 OpenStack 或 VK Private Cloud 平台上的虛擬基礎架構中）。
	  • SVM 位於與安裝 Light Agent 的虛擬機相同的節點上（在 Basis Dynamix Enterprise 虛擬基礎架構中）。
	  如果在裝有 Light Agent 的虛擬機所在的相同Hypervisor 或相同伺服器群組中沒有可供連線的 SVM，則 Light Agent 不會連線到 SVM。
	• **叢集**。Light Agent 會選擇要連線的符合下列條件的 SVM（取決於虛擬基礎架構的類型）：
	  • SVM 部署在與已安裝 Light Agent 的虛擬機相同的 Hypervisor 叢集中（在 Microsoft Hyper-V 平台、XenServer、VMware vSphere、KVM、Proxmox VE、Basis、HUAWEI FusionSphere、Nutanix Acropolis、ALT Virtualization Server、Astra Linux、Numa vServer 或 Basis Dynamix Standard 上的虛擬基礎架構中）。
	  • SVM 部署在與已安裝 Light Agent 的虛擬機相同的 OpenStack 專案中（在 OpenStack 平台或 VK Private Cloud 上執行的虛擬基礎架構中）。
	  • SVM 位於與安裝 Light Agent 的虛擬機相同的區域中（在 Basis Dynamix Enterprise 虛擬基礎架構中）。
	  如果在裝有 Light Agent 的虛擬機所在的相同 Hypervisor 叢集或相同 OpenStack 專案中沒有可供連線的 SVM，則 Light Agent 不會連線到 SVM。
	• **資料中心**。Light Agent 會選擇要連線的符合下列條件的 SVM（取決於虛擬基礎架構的類型）：
	  • SVM 部署在與已安裝 Light Agent 的虛擬機相同的資料中心中（在 Microsoft Hyper-V 平台、XenServer、VMware vSphere、KVM、Proxmox VE、Basis、HUAWEI FusionSphere、Nutanix Acropolis、ALT Virtualization Server、Astra Linux、Numa vServer 或 Basis Dynamix Standard 上的虛擬基礎架構中）。
	  • SVM 位於與已安裝 Light Agent 的虛擬機相同的可用區域中（在 OpenStack 平台或 VK Private Cloud 上執行的虛擬基礎架構中）。
	  • SVM 位於與安裝 Light Agent 的虛擬機相同的資料中心中（在 Basis Dynamix Enterprise 虛擬基礎架構中）。
	  如果帶有 Light Agent 的虛擬機所在的相同資料中心或可用性區域中沒有可用於連線的 SVM，則 Light Agent 不會連線到 SVM。
	• **略過**。在選擇 SVM 時，Light Agent 不會考慮其位置。
	預設選擇**Hypervisor**選項。
	如果選擇了**使用延伸 SVM 選擇演算法**選項，則此選項可用。

如果 Light Agent 使用延伸 SVM 選擇演算法，並且選擇 SVM 位址清單作為SVM 發現方法，並且在 SVM 上啟用了大型基礎設施防護模式（有關更多資訊，請參閱 Kaspersky Security for Virtualization Light Agent 說明），則僅當略過 SVM 路徑時才可以將 Light Agent 連線到此 SVM。您必須將**SVM 路徑**設定設為**略過**。如果設定了任何其他值，Light Agent 將無法連線到 SVM。

防護連線

在此視窗中，您可以啟用加密 Light Agent 和 Protection Server 之間的資料傳輸通道

確保在 SVM 上的 Protection Server 設定中啟用了 Light Agent 和 Protection Server 之間的資料傳輸通道加密。有關更多詳細資訊，請參閱Kaspersky Hybrid Cloud Security for Virtualization Light Agent 的說明。

連線防護設定

設定	描述
加密 Light Agent 和 Protection Server 之間的資料通道	使用加密來防護 Light Agent 和 Protection Server 之間的連線。 如果選取該核取方塊，則會在由政策管理的 Light Agent 與其所連線的 SVM 上的 Protection Server 之間建立加密連線。為其啟用了連線防護的 Light Agent 只能連線到在其上啟用了連線防護的 SVM，或允許與 Protection Server 建立不受防護的連線。 如果清除該核取方塊，則會在 Light Agent 和 Light Agent 所連線的 SVM 上的 Protection Server 之間建立不受防護的連線。 預設情況下已清空此核取方塊。

已知問題和限制

應用程式限制

Kaspersky Endpoint Security 在以下情況下不受支援：

- 在 OSnova 作業系統的封閉軟體環境模式和強化核心模式下。
- 在基於 Red Hat Enterprise Linux 的作業系統上使用 IMA 子系統時。
- 在基於 Red Hat Enterprise Linux 的作業系統上使用 FIPS 模式時。
- 在 Ubuntu 作業系統和基於 SUSE Linux Enterprise Server 的作業系統上使用 AppArmor 強制存取控制系統時。
- 使用 Grsecurity 安全系統時（在所有作業系統上）。
- 使用 seccomp 機制時（在所有作業系統上）。
- 使用 WSL1 和 WSL2 技術時（在所有作業系統上）。
- 使用某些檔案系統掛載選項時（例如 noexec、nosuid）。
- 當 Kaspersky Endpoint Security 安裝在容器內時。

Detection and Response 解決方案在由已安裝 Kaspersky Endpoint Security for Linux 的映像建立的虛擬機上可能無法正常運作。與 Detection and Response 解決方案整合時，會使用電腦的唯一 ID (Sensor ID)。應用程式會在初始安裝期間產生此 ID，即使解除安裝應用程式後，該 ID 也會保留。複製映像時，虛擬機會繼承 Sensor ID，這可能會導致 Detection and Response 解決方案將多個虛擬機識別為同一個裝置。

應用程式在某些架構上的限制

應用程式在以下處理器架構上執行時存在限制：

Elbrus

- Light Agent 模式：不受支援。
- EDR 代理程式模式：不受支援。
- BadUSB 攻擊防護：無法運作。
- 弱點利用防禦：無法運作。
- Web 威脅防護：掃描網頁是否含有網路釣魚連結時，無法使用啟發式分析。
- Kaspersky Endpoint Detection and Response Optimum 整合：無法運作。

- Kaspersky Endpoint Detection and Response Expert (cloud) 整合：無法運作。
- Kaspersky Endpoint Detection and Response (KATA) 整合：無法運作。
- Kaspersky Managed Detection and Response 整合：無法運作。
- 沙盒：無法運作。
- KUMA 整合：無法運作。
- 容器掃描：無法運作。
- 可更新的內核模組：不支援。
- 管理圖形使用者介面：由於不支援沙盒元件，使用者無法在沙盒中提交檔案進行掃描。

應用程式在某些作業系統上的限制

應用程式在以下作業系統上執行時存在限制：

Astra Linux Special Edition RUSB.10015-01 (operational update 1.5)

- BadUSB 攻擊防護：無法運作，因為作業系統中缺少 systemd-logind 服務。
- 惡意軟體掃描、關鍵區域掃描、清查和容器掃描工作的 CPU 資源使用量限制，在「4.2.0-23-generic」核心上無法運作。

CentOS 5.2 和 5.4

- 行為偵測:無法保證該元件能正常運作，因為同步處理程序啟動攔截不可用。
- 郵件威脅防護：無法運作。
- Web 威脅防護：無法運作，因為不支援 TProxy 機制。
- 網路威脅防護：無法運作，因為不支援 TProxy 機制。
- 加密軟體防護：無法運作，因為不支援 TProxy 機制。
- BadUSB 攻擊防護：無法運作，因為作業系統中缺少 systemd-logind 服務。
- 容器掃描：無法運作，因為作業系統不支援容器。
- 裝置控制：裝置的 ReadOnly 模式只有在應用程式中啟用該模式後連接裝置時才會生效。對於在啟用此模式之前已連接的裝置，存取模式會保持不變。
- 應用程式控制：無法運作，因為不支援同步攔截程序啟動所需的 fanotify 技術。
- 防火牆管理：無法運作，因為不支援在 iptables 中新增鏈。
- Web 控制：無法運作，因為不支援 TProxy 機制。

- 可更新的內核模組：不支援。
- 網路隔離：無法運作，因為不支援 TProxy 機制。
- 執行防禦無法對物件運作，因為無法同步攔截程序啟動。
- Kaspersky Endpoint Detection and Response Optimum 整合：無法運作。
- Kaspersky Endpoint Detection and Response Expert (cloud) 整合：無法運作。
- Kaspersky Endpoint Detection and Response (KATA) 整合：eBPF 遙測來源無法使用。
- Kaspersky Managed Detection and Response 整合：auditd 遙測來源無法使用。
- 圖形使用者介面：無法運作，因為作業系統中缺少 libxcb 函式庫。
- 卡巴斯基安全管理中心網路代理：需要額外的裝置設定。請參閱卡巴斯基安全管理中心說明。
- 安裝/移除：此應用程式與這些作業系統版本中的 SELinux 不相容。可能的解決方案：將 SELinux 置於非封鎖模式（寬容模式）、停用 SELinux，或手動設定 SELinux。
- 惡意軟體掃描：在 glibc 版本早於 2.11 的作業系統中，位於路徑長度超過 4096 個字元的目錄中的檔案不會被解毒或刪除。
- 惡意軟體掃描、關鍵區域掃描、清查和容器掃描工作的 CPU 資源使用限制無法運作。
- 不支援 Light Agent 模式，因此安裝應用程式時不適用 KSVLA_MODE、SERVER_MODE、VDI_MODE 設定。
- 不支援應用程式在 EDR Agent 模式下運作。
- 此應用程式在卡巴斯基安全管理中心雲端主控台中不受支援。
- 應用程式不支援以 FUSE 技術為基礎的檔案系統。
- 最常掃描檔案的統計資料不會被收集。
- 在某些情況下，作為與 Kaspersky Endpoint Detection and Response (KATA) 整合的一部分傳輸的遙測資料，可能包含來自系統事件記錄之事件的不完整資訊。

CentOS 6.4 和 6.6

- 行為偵測:無法保證該元件能正常運作，因為同步處理程序啟動攔截不可用。
- Web 威脅防護：IPv6 流量攔截無法運作。
- 網路威脅防護：IPv6 流量攔截無法運作。
- 加密軟體防護：IPv6 流量攔截無法運作。
- BadUSB 攻擊防護：無法運作，因為作業系統中缺少 systemd-logind 服務。
- 容器掃描：無法運作，因為作業系統不支援容器。
- 應用程式控制：無法運作，因為不支援同步攔截程序啟動所需的 fanotify 技術。
- 防火牆管理：防火牆的 IPv6 規則無法運作。

- Web 控制：IPv6 流量攔截無法運作。
- 可更新的內核模組：不支援。
- 執行防禦無法對物件運作，因為無法同步攔截程序啟動。
- Kaspersky Endpoint Detection and Response Optimum：威脅發展鏈未顯示網路活動，因為不支援 TProxy。僅提供有關檔案操作的遙測事件。物件執行防禦無法運作，因為無法同步攔截程序啟動。
- Kaspersky Endpoint Detection and Response Expert (cloud) 整合：無法運作。
- Kaspersky Endpoint Detection and Response (KATA) 整合：eBPF 遙測來源無法使用。
- Kaspersky Managed Detection and Response 整合：auditd 遙測來源無法使用。
- 卡巴斯基安全管理中心網路代理：需要額外的裝置設定。請參閱卡巴斯基安全管理中心說明。
- 安裝/移除：此應用程式與這些作業系統版本中的 SELinux 不相容。可能的解決方案：將 SELinux 置於非封鎖模式（寬容模式）、停用 SELinux，或手動設定 SELinux。
- 惡意軟體掃描：在 glibc 版本早於 2.11 的作業系統中，位於路徑長度超過 4096 個字元的目錄中的檔案不會被解毒或刪除。
- 不支援應用程式在 Light Agent 模式和 EDR Agent 模式下運作。
- 此應用程式在卡巴斯基安全管理中心雲端主控台中不受支援。
- 最常掃描檔案的統計資料不會被收集。
- 在某些情況下，作為與 Kaspersky Endpoint Detection and Response (KATA) 整合的一部分傳輸的遙測資料，可能包含來自系統事件記錄之事件的不完整資訊。

與 ptrace 設定值相關的限制

作業系統的 `kernel.yama.ptrace_scope` 設定值可能會影響 Kaspersky Endpoint Security：

- 1（受限 ptrace）。程序只能連線至由其啟動的程序。需要特殊權限才能連線至其他程序。應用程式的功能受到以下限制：
  - 行為偵測元件無法取得程序的環境參數。
  - 在內核版本高於 5.7 的作業系統上，應用程式控制元件無法讀取程序的命令列參數和環境變數，因為禁止讀取 /proc/<pid>/syscall 和 /proc/<pid>/mem。在內核版本為 5.0 的作業系統上，應用程式控制元件無法正常運作。
  - 程序記憶體和內核記憶體掃描無法在掃描工作中運作，因為禁止讀取 /proc/<pid>/mem。
  - 由於不允許讀取 /proc/<pid>/mem，因此無法保證 YARA 對程序記憶體的掃描。
- 2（管理 ptrace）。只有具備 CAP_SYS_PTRACE 權限的程序（通常為 root）才能使用 ptrace，或存取 /proc 中的程序（/proc/<pid>/mem）。故障排除受到限制，因為當機傾印不適用於使用者程序（例如 kesl-control 和 kesl-gui），但傾印適用於 kesl 程序本身。

- 3（禁止 ptrace）：在作業系統層級完全禁止 ptrace。應用程式的功能受到以下限制：
  - 當機傾印不適用於 kesl 程序或使用者程序（例如 kesl-control 和 kesl-gui）。
  - 行為偵測元件無法取得程序的環境參數。
  - 不支援應用程式控制元件。
  - 因為無法讀取 /proc/<pid>/mem 目錄：
    - 程序記憶體和內核記憶體掃描無法在掃描工作中運作。
    - 與 Detection and Response 解決方案整合時，「取得記憶體傾印」和「取得程序記憶體傾印」工作無法運作。
    - 在與卡巴斯基 Endpoint Detection and Response Expert (on-premises) 整合時，無法保證程序記憶體的 YARA 掃描在強制存取控制模式下運作。

可更新的內核模組的限制

可更新的內核模組不支援以下內核類型和版本：

Ubuntu

- `*-kvm`
- `*-gkeop 5.15.0-100[1234] (bionic/jammy)`
- `focal 5.10.0-1002-oem`
- `noble 6.8.0-1014-ibm`
- `*-realtime`
- `*-uc-*`
- `kinetic 5.18.0-100(1|2)-(ibm|gcp|oracle)`

Astra

- `6.1.90-1-generic-*, 6.6.28-1-generic-*`
- `*-hardened`

Debian

- `*-rt`
- `5.14.0-1-(cloud-amd64|amd64)-5.14.6-2`
- `6.1.0-36-(cloud-amd64|amd64)-6.1.139-1`

- `6.5.0-5-*amd64-6.5.13-1`
- `6.6.*`

RED OS 7.3

- `kernel-ml-5.14.9-1.el7`

RED OS 8.0

- `6.6.26-1.red80`
- `6.6.34-1.red80`
- `6.6.51-1.red80`
- `6.6.76-1.red80`
- `6.6.6-1.red80`

使用 eBPF 技術的限制

若要使用 eBPF 技術攔截網路流量，您需要使用下列選項編譯的 Linux 核心 4.18 或更新版本：

- `CONFIG_DEBUG_INFO_BTF=y` 或 `m`（支援具備 BTF 的 eBPF）
- `CONFIG_KPROBES= y`
- `CONFIG_TRACEPOINTS=y`
- `CONFIG_FSNOTIFY=y`

若要在與 Detection and Response 解決方案整合時使用 eBPF 傳送遙測資料，您需要使用下列選項編譯的 Linux 核心 4.18 或更新版本：

- `CONFIG_BPF=y`
- `CONFIG_BPF_SYSCALL=y`
- `CONFIG_TRACEPOINTS=y`
- `CONFIG_KPROBES=y`
- `CONFIG_KPROBES_ON_FTRACE=y`
- `CONFIG_KRETPROBES=y`
- `CONFIG_HAVE_SYSCALL_TRACEPOINTS=y`
- `CONFIG_FTRACE=y`

- `CONFIG_FUNCTION_TRACER=y`
- `CONFIG_DYNAMIC_FTRACE=y`
- `CONFIG_DYNAMIC_FTRACE_WITH_REGS=y`
- `CONFIG_FTRACE_SYSCALLS=y`
- `CONFIG_KPROBE_EVENTS=y`
- `CONFIG_FSNOTIFY=y`

特殊考量事項

- 此應用程式不能同時在 Light Agent 模式和 EDR Agent 模式下使用。
- 在使用 auditd 3.0.7 和 Linux 核心 4.18 的作業系統中，使用行為偵測元件可能會導致應用程式和 ssh 連線凍結。
- 在 Kylin Desktop V10 SP1 2303 作業系統上，行為偵測元件可能會使作業系統凍結。若要解決此問題，建議更新作業系統核心。

Light Agent 模式的特殊注意事項

如果在 Light Agent 模式下使用 Kaspersky Endpoint Security：

- 無法使用卡巴斯基安全管理中心雲端主控台和圖形使用者介面進行應用程式管理。
- 不支援使用雲端資料庫。
- Kaspersky Endpoint Security 使用 KSN 代理伺服器與 KSN伺服器互動。不支援與 KSN 直接通訊。
- 連線到 Integration Server、SVM 或 KSN 伺服器時，不支援使用應用程式的代理伺服器。

EDR Agent 模式的特殊注意事項

如果 Kaspersky Endpoint Security 正在 EDR Agent 模式下使用，則僅有有限的應用程式元件和工作子集可用。安裝後，應用程式設定如下：

- 不支援卡巴斯基 Endpoint Detection and Response Expert (cloud) 整合。
- 以下元件提供與 Detection and Response 解決方案的整合，完全可管理：
  - EDR Expert (on-premises)
  - NDR (KATA)

  這些元件預設為停用狀態，您需要啟用它們，才能使應用程式在 EDR Agent 模式下運作。您可以管理整合設定，包括物件執行防禦功能。
- 掃描期間不會封鎖對檔案的存取： **掃描期間封鎖對檔案的存取**核取方塊已清除 (`FileBlockDuringScan=No`)。可以修改此設定，但不會套用到受保護的裝置上。
- 檔案威脅防護和加密軟體防護防護元件以功能受限模式運行：當偵測到威脅時，這些元件不會嘗試解毒或刪除惡意物件，也不會阻止存取或應用程式活動，而只會將威脅偵測訊息傳送到提供與 Detection and Response 解決方案進行整合的Integration Server。

  您可以啟用或停用檔案威脅防護和加密軟體防護功能，並管理元件設置，但“偵測到威脅後的動作”例外。以下設定不會套用到受保護的裝置上：
  - 檔案威脅防護：**偵測到威脅後的動作**為**跳過**（ `ActionOnThreat=Skip` ）。
  - 加密軟體防護：**偵測到加密時的動作**為**通知**（ `ActionOnDetect=Notify` ）。
- 行為偵測元件完全可管理。
- 所有其他防護和控制元件均已停用，且無法管理。

當與卡巴斯基 Endpoint Detection and Response Expert (on-premises) 或 Kaspersky Endpoint Detection and Response (KATA) 整合時，作為威脅回應動作的一部分，Kaspersky Endpoint Security 可以控制裝置上執行檔和指令碼的啟動。物件執行防禦功能可用，但是有以下限制：

- 如果指令碼是從解釋器啟動的，則應用程式不控制指令碼的啟動。
- 應用程式不控制裝置上辦公室軟體檔案的開啟。

聯絡技術支援

如果您在應用程式檔案或關於應用程式的其他資訊來源中找不到問題的解決方案，建議聯絡技術支援。技術支援專家將回答您關於安裝和使用 Kaspersky Endpoint Security 的任何問題。

卡巴斯基會在 Kaspersky Endpoint Security 每個版本的生命週期內提供支援（請參閱應用程式生命週期頁面）。與技術支援部門聯絡之前，請閱讀支援規則。

您可以透過以下方式取得技術支援：

- 造訪技術支援網站。
- 從Kaspersky CompanyAccount 入口網站向卡巴斯基技術支援提交請求。

透過 Kaspersky CompanyAccount 取得技術支援

Kaspersky CompanyAccount 是一項針對使用 Kaspersky 應用程式的公司入口網站。卡巴斯基 CompanyAccount 讓使用卡巴斯基應用程式的組織能夠透過電子郵件請求聯絡卡巴斯基技術支援。您可以在入口網站上建立新的請求、監控請求進度，並保留請求處理歷史記錄。

在卡巴斯基 CompanyAccount 的單一帳戶下註冊您組織的所有員工。這可讓您集中管理向卡巴斯基提交的電子請求，並控制使用者對卡巴斯基 CompanyAccount 的存取權限。

Kaspersky CompanyAccount 入口採用以下語言提供：

- 英語
- 西班牙語
- 意大利語
- 德語
- 波蘭語
- 葡萄牙語
- 俄語
- 法語
- 日語

若要瞭解有關卡巴斯基 CompanyAccount 的更多資訊，請造訪卡巴斯基 CompanyAccount 技術支援網站。

獲取技術支援資訊

當您將問題告知卡巴斯基技術支援專家後，他們可能會要求您傳送*偵錯檔案*或*傾印檔案*。

技術支援專家可能還需要有關裝置上的作業系統和正在運行的處理程序的其他資訊，以及有關應用程式元件運行的詳細報告。

在診斷問題時，技術支援專家可能會要求您將應用程式設定變更為：

- 啟動功能以接收進階診斷資訊；
- 對無法透過標準使用者介面執行的各個應用程式元件進行更詳細的配置；
- 變更用於儲存接收到的診斷資訊的設定；
- 以配置在檔案中擷取和儲存網路流量。

技術支援專家將告訴您執行這些操作所需的所有資訊（步驟順序、要變更的設定、設定檔、指令碼、進階指令列功能、Debug 模組、特殊實用程式等），以及為診斷目的收到的資訊主體。接收到的進階診斷資訊儲存在使用者裝置上。該訊息不會被自動傳送給卡巴斯基。

上述步驟應僅在技術支援專家提供的說明的指導下執行。使用應用程式檔案中未描述或技術支援專家未推薦的方法自行變更應用程式檔案可能會導致應用程式和作業系統效能不佳和出現故障、防護性降低以及資料無法存取和損壞。

如何啟用和設定偵錯檔案的建立

*偵錯檔案*可偵錯應用程式指令的逐步執行，並偵測應用程式運行的哪個階段發生錯誤。

預設不會產生應用程式偵錯檔案。您可以在命令列、一般應用程式設定或圖形使用者介面中啟用或停用偵錯檔案建立，並選取偵錯層級。

如果您透過卡巴斯基安全管理中心管理 Kaspersky EndpoinSecurity 應用程式，則可以使用網頁主控台或管理主控台在 Kaspersky EndpoinSecurity 安全政策設定中管理應用程式的偵錯設定。

如何在網頁主控台中管理偵錯設定

1. 在網頁主控台的主視窗中，選擇 **資產管理** → **政策**。
2. 點擊 Kaspersky Endpoint Security 政策的名稱。

   政策內容視窗將開啟。
3. 選擇“**應用程式設定**”標籤。
4. 前往 **一般設定** → **技術支援** 區段，並查看 **偵錯設定** 下的內容。

5. 如果您要變更預設儲存應用程式偵錯檔案的目錄，請在 **偵錯資料夾路徑** 欄位中指定用於儲存偵錯檔案的目錄。預設值：/var/log/kaspersky/kesl。存取預設的偵錯檔案目錄需要 root 權限。如果您指定不同的目錄，請確保只有 root 對此目錄具有讀取和寫入權限（ `700` 或 `rwx--------` 權限）。

6. 如有必要，請在 **最大偵錯檔案大小 (MB)** 欄位中指定應用程式偵錯檔案的大小上限（以 MB 為單位）。預設值：500。

7. 如有必要，請在 **偵錯檔案最大數量** 欄位中指定應用程式偵錯檔案的數量上限。預設值：10。

8. 儲存變更。

9. 重新啟動應用程式以套用偵錯設定。

如何在管理主控台中管理偵錯設定

1. 在卡巴斯基安全管理中心管理主控台樹中的**受管理裝置**資料夾中，開啟包含所需裝置的管理群組名稱的資料夾。

2. 在工作區選擇“**政策**”標籤。

3. 在政策清單中，選擇所需的政策並雙擊它以開啟**屬性：<政策名稱>**視窗。

   您也可以透過使用政策右鍵功能表中的**屬性**項目或點擊位於政策設定部分中政策清單右側的**配置政策設定**連結來開啟政策屬性視窗。

4. 前往 **一般設定** → **應用程式設定** 區段。

5. 在 **追蹤和傾印設定** 下，點擊 **設定**。

6. 這會開啟 **追蹤和傾印設定** 視窗。

7. 如果您要變更預設儲存應用程式偵錯檔案的目錄，請在 **偵錯檔案目錄路徑** 欄位中指定用於儲存偵錯檔案的目錄。預設值：/var/log/kaspersky/kesl。存取預設的偵錯檔案目錄需要 root 權限。如果您指定不同的目錄，請確保只有 root 對此目錄具有讀取和寫入權限（ `700` 或 `rwx--------` 權限）。

8. 如有必要，請在 **偵錯檔案大小上限 (MB)** 欄位中指定應用程式偵錯檔案的大小上限（以 MB 為單位）。預設值：500。

9. 如有必要，請在 **偵錯檔案數量上限** 欄位中指定應用程式可以建立的偵錯檔案數量上限。預設值：10。

10. 在 **追蹤和傾印設定** 視窗中，點擊 **確定**。

11. 點擊“**套用**”。

12. 重新啟動應用程式以套用偵錯設定。

如何在命令列啟用偵錯並管理偵錯設定

在命令列中，您可以使用 一般應用程式設定 中的 `TraceLevel`、`TraceFolder`、`TraceMaxFileCount` 和 `TraceMaxFileSize` 設定來設定偵錯。您可以藉助指令列開關或包含所有一般應用程式設定的設定檔來變更設定值。

若要在命令列建立偵錯檔案並設定偵錯設定：

1. 啟用偵錯檔案建立並選取偵錯層級：

   ```
   kesl-control --set-app-settings TraceLevel=Detailed | MediumDetailed | NotDetailed
   ```

   其中：

   - `Detailed`— 產生詳細的偵錯檔案。
   - `MediumDetailed`— 產生一個包含資訊訊息和錯誤訊息的偵錯檔案。
   - `NotDetailed`— 產生一個包含錯誤訊息的偵錯檔案。

2. 如果您要變更預設儲存應用程式偵錯檔案的目錄，請指定用於儲存偵錯檔案的目錄：

   ```
   kesl-control --set-app-settings TraceFolder=<path to trace files directory>
   ```

   其中 `<path to trace files directory>` 是儲存偵錯檔案的目錄路徑。預設值：/var/log/kaspersky/kesl。存取預設的偵錯檔案目錄需要 root 權限。如果您指定不同的目錄，請確保只有 root 對此目錄具有讀取和寫入權限（`700` 或 `rwx--------` 權限）。

3. 如有必要，請指定偵錯檔案數量上限：

   ```
   kesl-control --set-app-settings TraceMaxFileCount=<number of application trace files>
   ```

   其中 `<number of application trace files>` 是應用程式偵錯檔案的數量上限。可能的值：1 到 10000。預設值：10。

4. 如有必要，請指定應用程式偵錯檔案的大小上限（以 MB 為單位）：

   ```
   kesl-control --set-app-settings TraceMaxFileSize=<size of an application trace file>
   ```

   其中 `<size of an application trace file>` 是偵錯檔案的大小上限（以 MB 為單位）。可能的值：1 到 1000。預設值：500。

變更`TraceFolder`、`TraceMaxFileCount`或`TraceMaxFileSize`設定的值後，需要重新啟動應用程式。

若要停用建立偵錯檔案，請執行以下命令：

```
kesl-control --set-app-settings TraceLevel=None
```

如何在圖形介面中啟用偵錯並管理偵錯設定

若要建立偵錯檔案並配置其詳細程度，您需要具有管理員角色(admin) 的使用者。

1. 開啟應用程式圖形介面的主視窗。
2. 在主應用程式視窗的下方，點擊**支援**按鈕。

   支援視窗開啟。

3. 點擊**偵錯**連結以開啟**偵錯**視窗

4. 在 **層級** 下拉式清單中，選取偵錯檔案的詳細程度：

   - **診斷 (300)** – 僅錯誤訊息。
   - **資訊 (700)** – 資訊和錯誤訊息。
   - **偵錯 (800)** – 詳細偵錯檔案。

   建議您向卡巴斯基技術支援專家確認所需的詳細程度。預設設定為 **診斷 (300)**。

5. 點擊**啟用**按鈕開始偵錯。

6. 重現導致問題的情況。

7. 點擊**停用**按鈕可停止偵錯。

建立的偵錯檔案儲存在 /var/log/kaspersky/kesl/ 目錄中。

您也可以啟用並設定 Watchdog 伺服器偵錯檔案的建立。

如何在命令列中啟用偵錯並管理 Watchdog 伺服器偵錯設定

在命令列中，您可以使用 一般應用程式設定中的 `WdTraceLevel` 設定來設定 Watchdog 伺服器偵錯。您可以使用命令列選項或包含所有一般應用程式設定的設定檔來變更設定值。

建立 `Watchdog` 伺服器偵錯檔案，並從命令列設定偵錯設定

```
kesl-control --set-app-settings WdTraceLevel=Detailed | MediumDetailed | NotDetailed | Product
```

其中：

- `Detailed`— 產生詳細的偵錯檔案。
- `MediumDetailed`— 產生一個包含資訊訊息和錯誤訊息的偵錯檔案。
- `NotDetailed`— 產生一個包含錯誤訊息的偵錯檔案。
- `Product` – 將值設定為等於 一般應用程式設定中 `TraceLevel` 設定的值。如果 `TraceLevel=None`，則不會產生偵錯檔案。

停用建立 `Watchdog` 伺服器偵錯檔案，並從命令列設定偵錯設定

```
kesl-control --set-app-settings WdTraceLevel=None
```

預設情況下，建立的偵錯檔案會儲存在 /var/log/kaspersky/kesl/ 目錄中。存取此目錄需要 root 權限。您可以指定其他目錄來儲存偵錯檔案。如果您指定不同的目錄，請確保只有 root 對此目錄具有讀取和寫入權限（ `700` 或 `rwx--------` 權限）。

圖形介面和 kesl-control 命令列公用程式的偵錯檔案會儲存在 /var/log/kaspersky/kesl-user 目錄中。若要啟用這些偵錯檔案的建立，您需要設定 LFS_ENABLE_ALL_COMPONENTS_LOGGING 環境變數。

為了儲存偵錯檔案，除了最低硬體需求所列的磁碟空間之外，應用程式還需要額外的磁碟空間。

只要應用程式正在使用，偵錯檔案就會儲存在裝置上，並且當應用程式被刪除時，偵錯檔案會被永久刪除。偵錯檔案不會被自動傳送給卡巴斯基。

偵錯檔案以人類可讀的格式保存。建議在將資訊傳送給卡巴斯基之前防護其免受未經授權的存取。

MMC 管理外掛程式偵錯檔案

如果您使用管理主控台管理 Kaspersky Endpoint Security，則管理 MMC 外掛程式執行時發生的事件的資訊可以儲存到安裝了管理伺服器的裝置上的 Kaspersky Endpoint Security MMC 外掛程式偵錯檔案中。檔案名稱包含應用程式版本號、檔案建立日期和時間以及處理程序識別碼 (PID)。該檔案包含關於 MMC 外掛程式運行期間發生的事件的資訊，特別是有關政策和工作運行的資訊。

預設不產生 MMC 外掛程式偵錯檔案。您可以使用登錄機碼來建立 MMC 外掛程式偵錯檔案。聯絡技術支援代表，獲得如何建立追蹤檔案的詳細資訊。

MMC 外掛程式所建立的所有偵錯檔案位於使用者在登錄機碼配置期間指定的資料夾中。

管理 Web 外掛程式偵錯檔案

如果您使用網頁主控台管理 Kaspersky Endpoint Security，則關於管理 Web 外掛程式執行時發生的事件的資訊可寫入 Web 外掛程式偵錯檔案。

如果在網頁主控台安裝精靈中啟用網頁主控台活動記錄，則會自動建立 Web 外掛程式的偵錯檔案（如需詳細資訊，請參閱 卡巴斯基安全管理中心說明 ）。

Web 外掛程式的偵錯檔案儲存在網頁主控台安裝資料夾的"logs"子資料夾中。

應用程式偵錯檔案內容

偵錯檔案包含以下一般資料：

- 事件時間。
- 執行線程編號。
- 引起該事件的應用程式元件。
- 事件嚴重程度（通知性事件、警告、緊急事件、錯誤）。
- 關於應用程式元件命令執行和命令執行結果的事件說明。

除了一般資料之外，偵錯檔案還可儲存以下資訊：

- 應用程式元件的狀態及其操作資料。
- 應用程式中的使用者活動資料。
- 有關裝置上安裝的硬體的資料。
- 關於所有作業系統物件和事件的資料，包括關於使用者活動的資訊。
- 作業系統物件中包含的資料（例如，可能包含任何使用者個人資料的檔案內容）。
- 網路流量資料（例如，網站上輸入欄位的內容，其中可能包括銀行卡資訊或任何其他敏感資料）。

- 從卡巴斯基伺服器接收的資料（例如應用程式資料庫的版本）。
- 從 KATA 伺服器、OSMP 伺服器以及提供與 Sandbox 互動的伺服器接收的資料。
- 有關消耗的 CPU 資源的資料。
- 有關消耗的 RAM 資源的資料。
- 關於應用程式讀取和寫入檔案操作的資料。
- 有關應用程式運行所需的快取資訊量的資料。

管理外掛程式偵錯檔案的內容

管理外掛程式的偵錯檔案包含以下一般資料：

- 事件時間。
- 執行線程編號。
- 引起該事件的應用程式元件。
- 事件嚴重程度（通知性事件、警告、緊急事件、錯誤）。
- 關於應用程式元件命令執行和命令執行結果的事件說明。

除了一般資料之外，管理外掛程式的偵錯檔案可能包含以下資訊：

- 個人資料，包括姓氏、名字（如果此類資料是檔案路徑的一部分）。
- 用於登入作業系統的帳戶名（如果使用者帳戶名稱是檔案名稱一部分）。

如何啟用和設定傾印

*傾印檔案*包含建立傾印時 Kaspersky Endpoint Security 處理程序的工作記憶體的所有資訊

> 傾印檔案可能包含個人資料。建議在將資訊傳送給卡巴斯基之前防護其免受未經授權的存取。

預設不產生傾印檔案。您可以啟用或停用應用程式故障時的傾印。

如果您透過卡巴斯基安全管理中心管理 Kaspersky Endpoint Security 應用程式，則可以使用網頁主控台或管理主控台，在 Kaspersky Endpoint Security 政策設定中啟用或停用並設定傾印。

如果您使用指令列來管理應用程式，則可以透過一般應用程式設定啟用或停用傾印。

傾印檔案的最大數量有限。

> 根據作業系統設定，可能不會建立使用者傾印檔案。確保使用`sysctl kernel.yama.ptrace_scope=0`配置系統核心。

如何在網頁主控台中啟用和設定傾印

若要在網頁主控台中啟用和設定傾印：

1. 在網頁主控台的主視窗中，選擇 **資產管理** → **政策**。
2. 點擊 Kaspersky Endpoint Security 政策的名稱。

   政策內容視窗將開啟。
3. 選擇"**應用程式設定**"標籤。
4. 前往 **一般設定** → **技術支援** 區段中的 **偵錯資訊**。
5. 如果您希望在應用程式當機時產生傾印檔案，請啟用 **傾印寫入已啟用** 切換開關。
6. 如果您要變更預設儲存 kesl 程序傾印檔案的目錄，請在 **代碼傾印路徑** 欄位中指定用於儲存傾印檔案的目錄。預設值：/var/opt/kaspersky/kesl/common/dumps。存取預設傾印檔案目錄需要 root 權限。如果您指定不同的目錄，請確保只有 root 對此目錄具有讀取和寫入權限（`700` 或 `rwx--------` 權限）。
7. 儲存變更。

如何在管理主控台中啟用和設定傾印

若要在管理主控台中啟用和設定傾印：

1. 在卡巴斯基安全管理中心管理主控台樹中的**受管理裝置**資料夾中，開啟包含所需裝置的管理群組名稱的資料夾。
2. 在工作區選擇"**政策**"標籤。
3. 在政策清單中，選擇所需的政策並雙擊它以開啟**屬性：<政策名稱>**視窗。

   您也可以透過使用政策右鍵功能表中的**屬性**項目或點擊位於政策設定部分中政策清單右側的**配置政策設定**連結來開啟政策屬性視窗。
4. 前往 **一般設定** → **應用程式設定** 區段。
5. 在 **追蹤和傾印設定** 下，點擊 **設定**。
6. 這會開啟 **追蹤和傾印設定** 視窗。
7. 如果您希望在應用程式當機時產生傾印檔案，請選取 **應用程式當機時建立傾印檔案** 核取方塊。
8. 如果您要變更預設儲存 kesl 程序傾印檔案的目錄，請在 **傾印檔案目錄的路徑** 欄位中指定用於儲存傾印檔案的目錄。預設值：/var/opt/kaspersky/kesl/common/dumps。存取預設傾印檔案目錄需要 root 權限（`700` 或 `rwx--------` 權限）。如果您指定不同的目錄，請確保只有 root 對此目錄具有讀取和寫入權限。
9. 在 **追蹤和傾印設定** 視窗中，點擊 **確定**。
10. 點擊"**套用**"。

如何在指令列中啟用和設定傾印

在指令列中，您可以使用一般應用程式設定中的 `CoreDumps` 和 `CoreDumpsPath` 設定來啟用、停用和設定傾印。

若要啟用和設定傾印：

1. 執行下列命令以啟用傾印：

```
kesl --set-app-settings CoreDumps=Yes
```

2. 如果您要變更儲存傾印檔案的目錄，請在 `CoreDumpsPath` 設定中指定目錄路徑。

```
kesl --set-app-settings CoreDumpsPath=<path to directory with dump files>
```

   其中 `<path to directory with dump files>` 是儲存傾印檔案的目錄路徑。預設值：/var/opt/kaspersky/kesl/common/dumps。存取預設傾印檔案目錄需要 root 權限（ `700` 或 `rwx--------` 權限）。如果您指定不同的目錄，請確保只有 root 對此目錄具有讀取和寫入權限。

若要停用傾印，請執行下列命令：

```
kesl --set-app-settings CoreDumps=No
```

如果您已啟用傾印，預設情況下，傾印檔案會儲存在下列目錄中：

- /var/opt/kaspersky/kesl/common/dumps（kesl 處理程序的傾印檔案）
- /var/opt/kaspersky/kesl/common/dumps-user （使用者處理程序的傾印檔案）

存取預設傾印檔案目錄需要 root 權限。您可以指定不同的目錄來儲存 kesl 程序的傾印檔案。如果您指定不同的目錄，請確保只有 root 對此目錄具有讀取和寫入權限（ `700` 或 `rwx--------` 權限）。

若要儲存傾印檔案，除了最低硬體需求中列出的磁碟空間之外，應用程式還需要額外的磁碟空間。

只要應用程式在使用中，就會在電腦中儲存傾印檔案，當應用程式被移除後，傾印檔案將被永久移除。傾印檔案不會被自動傳輸給卡巴斯基。

使用卡巴斯基安全管理中心進行遠端裝置診斷

在卡巴斯基安全管理中心中，您可以對用戶端裝置執行遠端診斷。遠端診斷程序可讓您遠端執行以下操作：

- 啟用或停用追蹤。
- 變更偵錯等級。
- 下載偵錯檔案。
- 下載遠端應用程式安裝記錄。
- 下載系統事件（syslog）記錄。
- 啟動、停止和重新啟動應用程式。

網頁主控台中的遠端診斷

如果您使用網頁主控台管理 Kaspersky Endpoint Security，則用戶端裝置的遠端診斷將在遠端診斷視窗中完成。

若要開啟裝置的遠端裝置診斷視窗：

1. 在網頁主控台主視窗中，選擇**資產（裝置）→受管理裝置**。
   受管理裝置的清單將開啟。
2. 選擇您想要遠端診斷的裝置並點擊其<裝置名稱>連接。
   裝置內容視窗開啟。
3. 在**進階**索引標籤上，選擇**遠端診斷**部分。

在裝置遠端診斷視窗中，您可以檢視遠端安裝記錄。

若要檢視裝置上的遠端安裝記錄，請執行下列操作：

1. 開啟遠端裝置診斷視窗。
2. 在**事件記錄**索引標籤上的**偵錯檔案**區塊下，點擊**遠端安裝記錄**。
   裝置偵錯事件記錄視窗開啟。

有關遠端診斷的更多資訊，請參閱卡巴斯基安全管理中心說明。

使用管理主控台進行遠端診斷

如果您使用管理主控台來管理 Kaspersky Endpoint Security，則遠端診斷將使用與管理主控台一起自動安裝在裝置上的特殊卡巴斯基安全管理中心遠端診斷實用程式進行。

若要開啟遠端診斷實用程式的主視窗，請執行以下操作：

1. 在管理主控台樹狀圖中的**管理裝置**資料夾中，選擇包含必要裝置的管理群組。
2. 在工作區選取“**裝置**”標籤。
3. 在受管理裝置清單中，選擇要連線遠端診斷實用程式的裝置，然後在裝置內容功能表中選擇**外部工具→遠端診斷**。
   卡巴斯基安全管理中心遠端診斷實用程式的主視窗開啟。

您可以使用遠端裝置診斷實用程式來檢視遠端安裝記錄。

若要檢視裝置上的遠端安裝記錄，請執行下列操作：

1. 開啟遠端診斷實用程式的主視窗。
2. 如果需要，請配置將實用程式連線到裝置的選項。在遠端診斷實用程式的主視窗中，點擊**登入**按鈕。
3. 在開啟的視窗中，在物件樹中，選擇**遠端安裝記錄**資料夾。

有關遠端診斷實用程式的更多資訊，請參閱卡巴斯基安全管理中心說明部分。

附錄

本節提供的資訊是主要說明文字的補充。

附錄 1。設定檔和預設應用程式設定

以下設定檔用於管理 Kaspersky Endpoint Security：

- 包含應用程式初始設定的設定檔：
- 應用程式初始配置時自動產生的預設設定檔，包含初始配置時設定的選項。這些設定在執行時套用。
- 您可以使用 Kaspersky Endpoint Security 管理指令建立的設定檔。這些設定檔可能包含工作設定和其他應用程式設定。您可以修改這些檔案並匯入到應用程式中來修改相應的選項。

用於編輯工作設定檔的規則

編輯設定檔時，請遵守以下規則：

- 在設定檔中指定所有必需的設定。您可以使用指令列指定無需檔案的單個工作設定。
- 如果某個設定屬於某個部分，則僅在本部分內容中指定它。您可以在一個部分內以任意順序指定設定。
- 將各部分的名稱括在方括號 [ ] 中。
- 以 < 設定名稱 >=< 設定值 > 格式指定設定值（設定名稱與其值之間的空格不予處理）。

  範例:
  ```
  [ScanScope.item_0000]
  AreaDesc=Home
  AreaMask.item_0000=*doc
  Path=/home
  ```

  將忽略字串值的第一個引號之前和最後一個引號之後以及未用引號括起來的字串值的開頭和結尾處的空格和索引標籤字元。

- 如需為某項設定指定多個值，請重複該設定的次數，次數應與要指定的值的數量相同。

  範例:
  ```
  AreaMask.item_0000=*xml
  AreaMask.item_0001=*doc
  ```

- 輸入以下類型的設定的值時要區分大小寫：
  - 掃描物件和排除物件的名稱（遮罩）。
  - 威脅的名稱（遮罩）。

  其餘設定值不區分大小寫。

- 指定布林設定值如下：`Yes` / `No`。

- 使用引號將包含空格字元的字串值括起來（例如，檔案和目錄的名稱及其路徑、包含「YYYY-MM-DD HH:MM:SS」格式的日期和時間的表達式）。

  您可以輸入帶引號或不帶引號的其餘值。

  範例:
  `AreaDesc=" 掃描電子郵件資料庫 "`

  字串開頭或結尾的單引號視為錯誤。

初始設定檔

您可以使用設定檔指定應用程式的初始設定：

- 如果您使用卡巴斯基安全管理中心安裝應用程式，您可以在 用於遠端應用程式安裝的封存檔中找到 autoinstall.ini 設定檔。建立安裝套件之前，您可以在此檔案中指定設定。卡巴斯基安全管理中心會在應用程式安裝期間套用這些設定。

- 如果您使用命令列安裝應用程式，則需要建立設定檔，並在啟動初始設定精靈時指定該檔案的路徑。您可以從 autoinstall.ini 設定檔複製此檔案的結構。

在安裝後的設定檔中，您可以指定下表中顯示的設定。適用的設定集合取決於應用程式使用模式。已為 autoinstall.ini 檔案指定預設值。

某些設定的有效值取決於您是透過卡巴斯基安全管理中心進行遠端安裝，還是透過命令列安裝。

若要變更設定檔中的設定，請以 <setting name>=<value> 格式指定其值。

範例

```
UPDATER_SOURCE=KLServers
```

設定	描述	參數值

[CustomSettings] 區段	在遠端安裝期間對應用程式進行微調。可讓您變更 kesl.ini 檔案中的部分設定以及 追蹤等級。
	
	只有在初始安裝期間，您才能使用此區段配置應用程式。
	
	如果 `[CustomSettings]` 區段中的設定與 autoinstall.ini 檔案中的設定重複，則會將 autoinstall.ini 設定套用至應用程式。
		• 以 <setting section>.<setting name>=<value> 格式表示的 kesl.ini 設定檔中的任何設定
		範例
		`[CustomSettings]`
		`General.Locale=ru_RU.utf8`
		`Network.ProxyRouteTable=202`
		`Watchdog.MaxMemory=20MB`
		• `TraceLevel`，應用程式偵錯檔案的詳細程度：
		  • `Detailed` – 產生詳細的應用程式偵錯檔案。
		  • `MediumDetailed` – 產生包含資訊訊息和錯誤訊息的應用程式偵錯檔案。
		  • `NotDetailed` – 產生包含錯誤訊息的應用程式偵錯檔案。
		  • `None`（預設值）– 不產生應用程式偵錯檔案。
		• `WdTraceLevel`，Watchdog 伺服器偵錯檔案的詳細程度：
		  • `Detailed`，以產生詳細的 Watchdog 伺服器偵錯檔案。
		  • `MediumDetailed`，以產生包含資訊訊息和錯誤訊息的 Watchdog 伺服器偵錯檔案。
		  • `NotDetailed`，以產生包含錯誤訊息的 Watchdog 伺服器偵錯檔案。
		  • `None`，不產生 Watchdog 伺服器偵錯檔案。
		  • `Product`（預設值），將此值設為與 `TraceLevel` 值相同。

EULA_AGREED	必須設定。 接受最終使用者產品授權協議的條款。	`Yes`（預設）– 接受《最終使用者產品授權協議》的條款和條件。 `No` – 不接受《最終使用者產品授權協議》的條款和條件。應用程式安裝將被終止。
PRIVACY_POLICY_AGREED	必須設定。 接受隱私政策條款。	`Yes`（預設）– 接受《隱私權政策》的條款和條件。 `No` – 不接受《隱私權政策》的條款和條件。應用程式安裝將被終止。
USE_KSN	必須設定。 啟用卡巴斯基安全網路使用：要啟用 KSN，必須接受卡巴斯基安全網路聲明的條款。 如果在標準模式下使用 Kaspersky Endpoint Security，且您已啟用 KSN，則應用程式的雲端模式將自動啟用。在這種模式下，Kaspersky Endpoint Security 使用惡意軟體資料庫的輕量級版本。	`Yes` – 接受卡巴斯基安全網路聲明的條款並允許使用 KSN。 `No` –（預設值）不接受《卡巴斯基安全網路聲明》的條款和條件。退出 KSN 不會中止應用程式安裝處理程序。

設定	描述	參數值
區域設定	傳送至卡巴斯基安全管理中心的應用程式事件所使用的區域設定。 圖形介面和應用程式指令列的區域設定取自 `LANG` 環境變數。如果應用程式不支援此本地化，則預設為英語本地化。	RFC 3066 格式的區域設定。可能的值： • `de_DE.UTF-8` – 德文 • `en_US.UTF-8` – 英語（美國） • `es_MX.UTF-8` – 西班牙語（墨西哥） • `fr_FR.UTF-8` – 法文 • `ja_JP.UTF-8` – 日文 • `pt_BR.UTF-8` – 葡萄牙語（巴西） • `ru_RU.UTF-8` – 俄文 • `zh_TW.UTF-8` – 繁體中文 • `zh_CN.UTF-8` – 簡體中文 如果未指定 `LOCALE` 設定，則使用作業系統區域設定。 如果應用程式無法偵測作業系統的區域設定或不支援該區域設定，則使用英文（RFC 3066 格式的 en_US.UTF-8）對事件進行本地化。
INSTALL_LICENSE	在 autoinstall.ini 設定檔中：用於將產品授權金鑰新增至應用程式的啟動碼。 在命令列設定檔中，您也可以指定金鑰檔案的路徑，以便將產品授權金鑰新增至應用程式。 此設定僅當應用程式在標準模式下使用時才適用。	`<activation code>`，如果您想在透過卡巴斯基安全管理中心或命令列安裝時使用啟動碼啟動應用程式。 `<full path to key file>`，如果您想在命令列安裝期間使用金鑰檔案啟動應用程式。 `None`：如果不想在安裝期間啟動該應用程式（例如：在無網際網路連線的隔離網段中安裝應用程式時）。
UPDATER_SOURCE	資料庫和應用程式模組的更新來源。 僅當應用程式以標準模式或 EDR 代理程式模式使用時，才會套用此參數。	`SCServer` – 使用卡巴斯基安全管理中心伺服器作為更新來源。 `KLServers`（預設）– 使用卡巴斯基伺服器作為更新來源。 `<update source address>`，可以是本機目錄（例如 /home/bases）或遠端 HTTP 或 HTTPS 伺服器（例如 http://example.com/bases/）。
PROXY_SERVER	用於連線網際網路的代理伺服器位址。 僅當應用程式以標準模式或 EDR 代理程式模式使用時，才會套用此參數。	代理伺服器位址採用以下格式之一： • `[<connection protocol>://]<address of the proxy server>:<port>`，如果連線到代理伺服器不需要身分驗證； • `[<connection protocol>://][<user name>:[<password>]@]<address of the proxy server>:<port>`，如果連線到代理伺服器需要身分驗證。指定 IPv6 位址時，請將其輸入方括號中。 不支援透過 HTTPS 連線到代理伺服器。

設定	描述	參數值
UPDATE_EXECUTE	在初始設定期間啟動應用程式資料庫更新工作。 僅當應用程式以標準模式或 EDR 代理程式模式使用時，才會套用此參數。	`Yes`（預設值）— 啟動更新工作。 `No` — 不啟動更新工作。
KERNEL_SRCS_INSTALL	啟動檔案威脅防護時，自動編譯核心模組。 此設定僅適用於不支援 fanotify 的作業系統。	`Yes`（預設）– 檔案威脅防護啟動時，編譯內核模組。 `No` – 不編譯內核模組。
USE_GUI	安裝和使用應用程式的圖形介面。 僅當應用程式以標準模式或 EDR 代理程式模式使用時，才會套用此參數。	`Yes` – 安裝並使用應用程式的圖形介面（必須將安裝圖形介面的檔案新增至安裝套件）。 `No`（預設）– 不使用圖形介面。
GROUP_CLEAN	必須設定。 在安裝應用程式之前，自動從 kesladmin 和 keslaudit 特權群組中刪除使用者。	`Yes` — 從特權群組中刪除使用者。如果值為 `Yes`，且沒有 nogroup 群組，則安裝會失敗，您將被提示手動從特權群組中刪除特權使用者。 `No`（預設）– 不從特權群組中移除使用者。
ADMIN_USER	被指派了管理員角色(admin) 的使用者。 管理員角色允許在應用程式的圖形介面和命令列中管理應用程式設定和工作設定，而無需使用 `sudo` 命令。	
CONFIGURE_SELINUX	自動設定 SELinux 以與 Kaspersky Endpoint Security 搭配使用。	`Yes`（預設值）— 自動設定 SELinux 以與 Kaspersky Endpoint Security 搭配使用。 `No` – 不執行自動 SELinux 設定。
DISABLE_PROTECTION	安裝後停用應用程式的功能元件。 停用了元件的安裝會很方便，例如，如果您需要重現應用程式的問題並建立偵錯檔案。 如果在安裝應用程式後使用 `DISABLE_PROTECTION=Yes` 啟用必要的元件，則啟用的元件將在應用程式重新啟動後繼續運作。	`Yes` — 安裝後啟動應用程式時停用防護元件和掃描工作。 `No` – 安裝後啟動應用程式時不停用防護元件和掃描工作。
ENDPOINT_AGENT_MODE	在 EDR 代理程式模式下使用 Kaspersky Endpoint Security。 此設定不適用於配備 Elbrus CPU 的裝置。	`Yes` – Kaspersky Endpoint Security 正在 EDR 代理程式模式下使用，以支援卡巴斯基 Detection and Response 解決方案與受防護裝置上的協力廠商病毒防護解決方案協同工作。 `No`（預設值）– Kaspersky Endpoint Security 以標準模式或 Light Agent 模式運作（請參閱 KSVLA_MODE 設定）。

設定	描述	參數值
EDR_EXPERT_CLOUD_MODE	選擇 Endpoint Detection and Response Expert 元件的模式。 此設定僅當應用程式在標準模式下使用時才適用。 此設定不適用於配備 Elbrus CPU 的裝置。	`Yes` 表示應用程式使用 Kaspersky Endpoint Detection and Response Expert (cloud) 整合。 `No`（預設值）表示應用程式使用 Kaspersky Endpoint Detection and Response Expert (on-premises) 整合。
KSVLA_MODE	在 Light Agent 模式下使用 Kaspersky Endpoint Security。 此設定不適用於配備 Elbrus CPU 的裝置。	`Yes` - Kaspersky Endpoint Security 以 Light Agent 模式使用（作為 Kaspersky Hybrid Cloud Security for Virtualization Light Agent 的一部分）。 `No`（預設值）– Kaspersky Endpoint Security 以標準模式或 EDR 代理程式模式使用（請參閱 ENDPOINT_AGENT_MODE 設定）。
SERVER_MODE	受防護的虛擬機的角色（伺服器或工作站）。 此設定僅當應用程式在 Light Agent 模式下使用時才套用。 此設定不適用於配備 Elbrus CPU 的裝置。	`Yes` - 受防護的虛擬機用作伺服器。 `No` - 受防護的虛擬機用作工作站。
VDI_MODE	啟用 VDI 防護模式以最佳化暫時虛擬機上的應用程式效能。 此設定僅當應用程式在 Light Agent 模式下使用時才套用。 此設定不適用於配備 Elbrus CPU 的裝置。	`Yes` - 啟用 VDI 防護模式。如果您要在用於建立暫時虛擬機的虛擬機範本上安裝 Kaspersky Endpoint Security，則建議這樣做。 `No` – 不啟用 VDI 防護模式。
INTERCEPTOR_MODE	Kaspersky Endpoint Security 所使用的系統事件攔截機制： 此設定僅適用於執行支援 fanotify 技術的作業系統的裝置。 此設定不適用於配備 Elbrus CPU 的裝置。	`UseFanotify`（預設）– 使用 fanotify 技術攔截系統事件。 `UseUpdatableKernelModule` – 使用可更新內核模組攔截系統事件。

設定	描述	參數值
INTERCEPTOR_FALLBACK_STRATEGY	如果可更新的內核模組未能啟動，應用程式會採取的動作。 此設定僅適用於執行支援 fanotify 技術的作業系統的裝置。 此設定不適用於配備 Elbrus CPU 的裝置。	`FallbackToFanotify`（預設）– 切換到 fanotify 進行系統事件攔截。 `FallbackToLimitedMode` – 不使用系統事件攔截。結果，無法執行即時檔案掃描，這會導致裝置的防護等級降低。
INTERCEPTOR_APPLY_STRATEGY	如果應用程式切換到使用可更新的內核模組，則必須重新啟動應用程式才能啟動該模組。此設定可讓您指定是希望自動重新啟動應用程式還是希望手動重新啟動應用程式。 此設定僅適用於透過卡巴斯基安全管理中心安裝的情況。 此設定僅適用於執行支援 fanotify 技術的作業系統的裝置。 此設定不適用於配備 Elbrus CPU 的裝置。	`RestartServiceAutomatically`（預設值）會自動重新啟動應用程式，以啟動可更新內核模組。 `RestartServiceManually` 會在使用者手動重新啟動應用程式後，啟動可更新的內核模組。 我們建議自動重新啟動應用程式以切換到使用可更新的內核模組。重新啟動應用程式後手動啟動可更新的內核模組可能會導致應用程式錯誤。
ENABLE_TRACES_ON_FIRST_STARTUP	在安裝後首次啟動應用程式時建立偵錯檔案。 為了建立偵錯檔案，系統會在 /var/log/kaspersky/kesl/ 目錄中自動建立一個名為 kesl_startup.log 的檔案。常規應用程式偵錯檔案的大小限制不適用於此檔案。偵錯在五分鐘後或檔案威脅防護工作啟動後停止。	`Yes` — 在安裝後首次啟動應用程式時建立偵錯檔案。 `No`（預設值）– 首次啟動應用程式時不建立偵錯檔案。
AK_FORCED_PACKAGE_MANAGER_OPERATIONS_AS_FALLBACK	使用忽略套件管理器錯誤的應用程式安裝模式。 如果無法正常安裝應用程式，可以使用此模式。 此設定僅適用於透過卡巴斯基安全管理中心安裝的情況。 只有在技術支援專家的監督下並根據其指示，才建議變更預設值。	`No`（預設值），以正常安裝應用程式。 `Yes`，以在忽略系統錯誤的情況下安裝應用程式。

設定	描述	參數值
AK_REMOVE_PARTIALLY_INSTALLED_PACKAGE	如果應用程式安裝套件僅部分安裝，則自動將其移除。 如果無法正常安裝應用程式，請停用此設定。 此設定僅適用於透過卡巴斯基安全管理中心安裝的情況。 只有在技術支援專家的監督下並根據其指示，才建議變更預設值。	`Yes`（預設值），以移除部分安裝的應用程式安裝套件。 `No`，以在忽略部分安裝套件的情況下安裝應用程式。
AK_PACKAGE_MANAGER_DEBUG_LOG_OUTPUT	啟用套件管理器的偵錯記錄。 如果無法正常安裝應用程式，可以使用此設定。 此設定僅適用於透過卡巴斯基安全管理中心安裝的情況。 只有在技術支援專家的監督下並根據其指示，才建議變更預設值。	`Yes`，以啟用套件管理器的偵錯記錄。 `No`（預設值），以不啟用套件管理器的偵錯記錄。

安裝套件中的初始設定

您可以在用於透過卡巴斯基安全管理中心安裝應用程式的安裝套件中，指定應用程式的初始設定。

在卡巴斯基安全管理中心網頁主控台中，您可以在安裝套件內容的**設定**索引標籤中指定 Kaspersky Endpoint Security 的初始設定。建立的安裝套件可在網頁主控台主視窗的以下區域之一中找到：

- **裝置發現和部署→部署和分配→安裝套件**。
- **操作→儲存庫→安裝套件**。

在卡巴斯基安全管理中心管理主控台中，您可以在建立安裝套件時或在安裝套件內容的**設定**區域中指定 Kaspersky Endpoint Security 的初始設定。建立的安裝套件位於管理主控台樹中的**附加 → 遠端安裝 → 安裝套件**資料夾中。

適用的設定集合取決於應用程式使用模式。

網頁主控台中的初始設定

設定	描述
使用模式	• **標準模式以防護工作站和伺服器**（預設值）。如果選擇此選項，應用程式將作為獨立應用程式來防護 Linux 工作站和伺服器。 • **Endpoint Detection and Response Agent**如果選擇此選項，應用程式將用於支援 Kaspersky Detection and Response 解決方案與受防護裝置上的協力廠商病毒防護解決方案協同工作。 • **用於防護虛擬環境的 Light Agent**如果選擇此選項，應用程式將在 Light Agent 模式下使用（作為 Kaspersky Security for Virtualization Light Agent 的一部分）。 EDR Agent 模式和 Light Agent 模式不適用於配備 Elbrus CPU 的裝置。
啟用 Endpoint Detection and Response Expert (cloud)	選取此核取方塊，以使用 Endpoint Detection and Response Expert (cloud) 整合。 在標準模式下，應用程式支援與 Endpoint Detection and Response Expert (cloud) 和 Endpoint Detection and Response Expert (on-premises) 整合。如果取消選取此核取方塊，則會使用與 Endpoint Detection and Response Expert (on-premises) 的整合。 此設定僅在應用程式以標準模式使用時適用 此設定不適用於配備 Elbrus CPU 的裝置。
啟用 VDI 防護模式	選取此核取方塊可啟用 VDI 防護模式。如果您要在用於建立暫時虛擬機的虛擬機範本上安裝該應用程式，則建議這樣做。預設情況下已清空此核取方塊。 此設定僅當應用程式在 Light Agent 模式下使用時才套用。 此設定不適用於配備 Elbrus CPU 的裝置。
受防護的虛擬機被用作伺服器	將安裝應用程式的虛擬機的角色：伺服器或工作站。預設情況下，此核取方塊處於選取狀態（虛擬機在虛擬基礎架構中用作伺服器）。 此設定僅當應用程式在 Light Agent 模式下使用時才套用。 此設定不適用於配備 Elbrus CPU 的裝置。
KSC 中的事件的語言	傳送至卡巴斯基安全管理中心的應用程式事件所使用的區域語言： • **系統**（預設），以使用作業系統區域設定。 如果應用程式無法偵測到作業系統的區域設定或不支援該區域設定，則使用英語來本地化事件。 • Kaspersky Endpoint Security 支援的語言之一：英文（美國）、西班牙文（墨西哥）、繁體中文、簡體中文、德文、葡萄牙文（巴西）、俄文、法文、日文。 圖形介面和應用程式指令列的區域設定取自 `LANG` 環境變數。如果應用程式不支援此本地化，則預設為英語本地化。
啟動應用程式	如果您想在安裝期間啟動應用程式，請選取此核取方塊。在顯示的欄位中輸入啟動碼。預設情況下已清空此核取方塊。 此設定僅當應用程式在標準模式下使用時才適用。

設定	描述
更新來源	資料庫和應用程式模組的更新來源。 • **卡巴斯基更新伺服器**（預設）。 • **卡巴斯基安全管理中心**。 • **本機或全球網路中的其他來源**。如果選取此選項，請在開啟的欄位中輸入更新來源的位址。 僅當應用程式以標準模式或 EDR 代理程式模式使用時，才會套用此參數。
安裝後執行資料庫更新工作	如果選取此核取方塊，則應用程式安裝後，資料庫和應用程式模組更新工作將啟動。預設情況下已選擇此核取方塊。 如果您已將預先下載的應用程式資料庫新增至安裝套件，請取消選取此核取方塊。 僅當應用程式以標準模式或 EDR 代理程式模式使用時，才會套用此參數。
指定代理伺服器設定	如果您使用代理伺服器存取網際網路，請選取此核取方塊。在顯示的欄位中，採用以下格式之一輸入代理伺服器位址： • `[<connection protocol>://]<address of the proxy server>:<port>`，如果連線到代理伺服器不需要身分驗證； • `[<connection protocol>://][<user name>:[<password>]@]<address of the proxy server>:<port>`，如果連線到代理伺服器需要身分驗證。指定 IPv6 位址時，請將其輸入方括號中。 不支援透過 HTTPS 連線到代理伺服器。 僅當應用程式以標準模式或 EDR 代理程式模式使用時，才會套用此參數。
安裝內核來源代碼	如果選取此核取方塊，啟動檔案威脅防護會自動在不支援 fanotify 的作業系統上啟動內核模組的編譯。預設情況下已選擇此核取方塊。 此設定僅適用於不支援 fanotify 的作業系統。 此設定不適用於配備 Elbrus CPU 的裝置。
使用圖形使用者介面	如果您打算安裝並使用應用程式圖形介面，請選取此核取方塊。必須將用於安裝圖形介面的檔案新增至安裝套件。預設情況下已清空此核取方塊。 僅當應用程式以標準模式或 EDR 代理程式模式使用時，才會套用此參數。
指定具有管理員角色的使用者	選取此核取方塊可以指定要向其指派管理員角色的使用者。管理員角色允許在應用程式的圖形介面和命令列中管理應用程式設定和工作設定，而無需使用 `sudo` 命令。 在顯示的欄位中輸入使用者名稱。
自動設定 SELinux	如果選取此核取方塊，SELinux 會在應用程式的初始設定期間自動設定為與 Kaspersky Endpoint Security 協同工作。預設情況下已選擇此核取方塊。
將使用者從特權群組中移除	選取此核取方塊可以在安裝應用程式之前從「kesladmin」和「keslaudit」特權群組中刪除使用者。預設情況下已清空此核取方塊。 如果選取該核取方塊且“nogroup”群組不存在，安裝失敗，您會被提示手動從特權群組中移除使用者。
停用防護元件和安裝後應用程式首次啟動的掃描工作	如果您在完成安裝過程後想要在停用防護元件和掃描工作的情況下執行應用程式，請選取此核取方塊。 停用了防護元件的安裝會很方便，例如，為了重現應用程式運行中的問題並建立偵錯檔案。 如果啟用了必要的元件和工作，則應用程式重新啟動後，啟用的元件和工作將繼續運作。
啟用當應用程式在安裝後首次啟動時進行跟蹤	如果您希望在安裝後首次啟動應用程式時建立偵錯檔案，請選取此核取方塊。 為了建立偵錯檔案，系統會在 /var/log/kaspersky/kesl/ 目錄中自動建立一個名為 kesl_startup.log 的檔案。常規應用程式偵錯檔案的大小限制不適用於此檔案。偵錯在五分鐘後或檔案威脅防護工作啟動後停止。

設定	描述
攔截機制	應用程式使用的系統事件攔截機制： • **Fanotify 技術**（預設）。如果選取此選項，應用程式將使用 fanotify 技術進行系統事件攔截。 • **可更新的內核模組**。如果選取此選項，則會在應用程式安裝期間安裝可更新的內核模組。應用程式使用此模組來攔截系統事件。 此設定僅適用於執行支援 fanotify 技術的作業系統的裝置。 此設定不適用於配備 Elbrus CPU 的裝置。
如果可更新的內核模組未能啟動	可更新的內核模組無法啟動時，應用程式會執行的動作： • **使用 fanotify**（預設）。如果選取此選項，應用程式將切換到 fanotify 技術進行系統事件攔截。 • **停用系統事件攔截**如果應用程式不使用系統事件攔截，則不會執行即時檔案掃描，並且裝置的防護等級會降低。 如果選取了**可更新的內核模組**攔截機制，則此選項可用。 此設定僅適用於執行支援 fanotify 技術的作業系統的裝置。 此設定不適用於配備 Elbrus CPU 的裝置。
啟用套件管理器錯誤忽略模式	選取此核取方塊，以在安裝應用程式時忽略套件管理器錯誤。預設情況下已清空此核取方塊。 如果無法正常安裝應用程式，可以使用此設定。 我們建議僅在技術支援人員的監督下啟用此設定。

管理主控台中的初始設定

初始設定

設定	描述
KSC 中的事件的語言	傳送至卡巴斯基安全管理中心的應用程式事件所使用的區域語言： • **系統**（預設），以使用作業系統區域設定。 如果應用程式無法偵測到作業系統的區域設定或不支援該區域設定，則使用英語來本地化事件。 • Kaspersky Endpoint Security 支援的語言之一：英文（美國）、西班牙文（墨西哥）、繁體中文、簡體中文、德文、葡萄牙文（巴西）、俄文、法文、日文。 圖形介面和應用程式指令列的區域設定取自 `LANG` 環境變數。如果應用程式不支援此本地化，則預設為英語本地化。
啟動碼	如果您想在安裝期間啟動應用程式，請輸入啟動碼。 此設定僅當應用程式在標準模式下使用時才適用。
選取更新來源	按一下 **設定** 按鈕會開啟一個視窗，您可以在其中選取資料庫和應用程式模組更新來源： • **卡巴斯基更新伺服器**（預設值）。 • **卡巴斯基安全管理中心** • **區域或全域網路上的其他來源**如果選取此選項，請在 **位址** 欄位中輸入更新來源的位址。 僅當應用程式以標準模式或 EDR 代理程式模式使用時，才會套用此參數。

設定	描述
安裝後執行資料庫更新工作	如果選取此核取方塊，則應用程式安裝後，資料庫和應用程式模組更新工作將啟動。預設情況下已選擇此核取方塊。 如果您已將預先下載的應用程式資料庫新增至安裝套件，請取消選取此核取方塊。 僅當應用程式以標準模式或 EDR 代理程式模式使用時，才會套用此參數。
代理伺服器位址	如果您使用代理伺服器存取網際網路，請使用下列格式之一輸入代理伺服器的位址： • `[<connection protocol>://]<address of the proxy server>:<port>`，如果連線到代理伺服器不需要身分驗證； • `[<connection protocol>://][<user name>:[<password>]@]<address of the proxy server>:<port>`，如果連線到代理伺服器需要身分驗證。指定 IPv6 位址時，請將其輸入方括號中。 不支援透過 HTTPS 連線到代理伺服器。 僅當應用程式以標準模式或 EDR 代理程式模式使用時，才會套用此參數。
安裝內核來源代碼	如果選取此核取方塊，啟動檔案威脅防護會自動在不支援 fanotify 的作業系統上啟動內核模組的編譯。預設情況下已選擇此核取方塊。 此設定僅適用於不支援 fanotify 的作業系統。 此設定不適用於配備 Elbrus CPU 的裝置。
使用圖形使用者介面	如果您打算安裝並使用應用程式圖形介面，請選取此核取方塊。必須將用於安裝圖形介面的檔案新增至安裝套件。預設情況下已清空此核取方塊。 僅當應用程式以標準模式或 EDR 代理程式模式使用時，才會套用此參數。
具有管理員角色的使用者	您想要向其指派管理員角色的使用者名稱。管理員角色允許在應用程式的圖形介面和命令列中管理應用程式設定和工作設定，而無需使用 `sudo` 命令。
自動設定 SELinux	如果選取此核取方塊，SELinux 會在應用程式的初始設定期間自動設定為與 Kaspersky Endpoint Security 協同工作。預設情況下已選擇此核取方塊。
將使用者從特權群組中移除	選取此核取方塊可以在安裝應用程式之前從「kesladmin」和「keslaudit」特權群組中刪除使用者。預設情況下已清空此核取方塊。 如果選取該核取方塊且“nogroup”群組不存在，安裝失敗，您會被提示手動從特權群組中移除使用者。
安裝後第一次啟動應用程式時，請停用防護元件和掃描工作	如果您在完成安裝過程後想要在停用防護元件和掃描工作的情況下執行應用程式，請選取此核取方塊。 停用了防護元件的安裝會很方便，例如，為了重現應用程式運行中的問題並建立偵錯檔案。 如果啟用了必要的元件和工作，則應用程式重新啟動後，啟用的元件和工作將繼續運作。
當應用程式在安裝後首次啟動時啟用偵錯	如果您希望在安裝後首次啟動應用程式時建立偵錯檔案，請選取此核取方塊。 為了建立偵錯檔案，系統會在 /var/log/kaspersky/kesl/ 目錄中自動建立一個名為 kesl_startup.log 的檔案。常規應用程式偵錯檔案的大小限制不適用於此檔案。偵錯在五分鐘後或檔案威脅防護工作啟動後停止。
應用程式模式	這組設定包含 **設定** 按鈕。按一下此按鈕會開啟 **應用程式模式** 視窗。在此視窗中，您可以選擇應用程式的模式。 • **標準模式以防護工作站和伺服器**（預設值）。如果選擇此選項，應用程式將作為獨立應用程式來防護 Linux 工作站和伺服器。 • **Endpoint Detection and Response Agent**如果選擇此選項，應用程式將用於支援 Kaspersky Detection and Response 解決方案與受防護裝置上的協力廠商病毒防護解決方案協同工作。 • **用於防護虛擬環境的 Light Agent**如果選擇此選項，應用程式將在 Light Agent 模式下使用（作為 Kaspersky Security for Virtualization Light Agent 的一部分）。 EDR Agent 模式和 Light Agent 模式不適用於配備 Elbrus CPU 的裝置。

設定	描述
啟用 Endpoint Detection and Response Expert (cloud)	選取此核取方塊，以使用 Endpoint Detection and Response Expert (cloud) 整合。 在標準模式下，應用程式支援與 Endpoint Detection and Response Expert (cloud) 和 Endpoint Detection and Response Expert (on-premises) 整合。如果取消選取此核取方塊，則會使用與 Endpoint Detection and Response Expert (on-premises) 的整合。 此設定僅當應用程式在標準模式下使用時才適用。 此設定不適用於配備 Elbrus CPU 的裝置。
受防護的虛擬機被用作伺服器	將安裝應用程式的虛擬機的角色：伺服器或工作站。預設情況下，此核取方塊處於選取狀態（虛擬機在虛擬基礎架構中用作伺服器）。 此設定僅當應用程式在 Light Agent 模式下使用時才套用。 此設定不適用於配備 Elbrus CPU 的裝置。
啟用 VDI 防護模式	選取此核取方塊可啟用 VDI 防護模式。如果您要在用於建立暫時虛擬機的虛擬機範本上安裝該應用程式，則建議這樣做。預設情況下已清空此核取方塊。 此設定僅當應用程式在 Light Agent 模式下使用時才套用。 此設定不適用於配備 Elbrus CPU 的裝置。
系統事件攔截	這組設定包含 **設定** 按鈕。按一下此按鈕會開啟 **系統事件攔截設定** 視窗。在此視窗中，您可以選擇應用程式要使用的系統事件攔截模式： • **Fanotify 技術**（預設值）。如果選取此選項，應用程式將使用 fanotify 技術進行系統事件攔截。 • **可更新的內核模組**如果選取此選項，則會在應用程式安裝期間安裝可更新的內核模組。應用程式使用此模組來攔截系統事件。 此設定僅適用於執行支援 fanotify 技術的作業系統的裝置。 此設定不適用於配備 Elbrus CPU 的裝置。
如果可更新的內核模組未能啟動 （**系統事件攔截設定**視窗）。	可更新的內核模組無法啟動時，應用程式會執行的動作： • **使用 fanotify**（預設）。如果選取此選項，應用程式將切換到 fanotify 技術進行系統事件攔截。 • **停用系統事件攔截**如果應用程式不使用系統事件攔截，則不會執行即時檔案掃描，並且裝置的防護等級會降低。 如果選取了**可更新的內核模組**攔截機制，則此選項可用。 此設定僅適用於執行支援 fanotify 技術的作業系統的裝置。 此設定不適用於配備 Elbrus CPU 的裝置。
啟用套件管理器錯誤忽略模式	選取此核取方塊，以在安裝應用程式時忽略套件管理器錯誤。預設情況下已清空此核取方塊。 如果無法正常安裝應用程式，可以使用此設定。 我們建議僅在技術支援人員的監督下啟用此設定。

預設設定檔

初始配置後，應用程式將建立以下設定檔：

- /var/opt/kaspersky/kesl/common/agreements.ini
  Agreements.ini 設定檔包含與產品授權協議、隱私權政策和卡巴斯基安全網路聲明相關的設定。
- /var/opt/kaspersky/kesl/common/kesl.ini
  kesl.ini 設定檔包含下表中描述的設定。

如有必要，您可以在 kesl.ini 檔案中編輯設定值。

這些檔案中的預設值只能在技術支援專家的監督下並按照他們的指示進行變更。

若要套用對設定檔所做的變更，請重新啟動 Kaspersky Endpoint Security 應用程式。

如果檔案中缺少參數或指定了錯誤的參數值，應用程式將使用預設值。

kesl.ini 設定檔的設定

設定	描述	參數值
[General]部分包含以下設定：		
`Locale`	Kaspersky Endpoint Security 傳送到卡巴斯基安全管理中心的應用程式事件所使用的區域設定。 圖形介面和應用程式指令列的區域設定取自 `LANG` 環境變數。如果應用程式不支援此本地化，則預設為英語本地化。	採用 RFC 3066 指定格式的區域設定。 如果未指定 `Locale` 設定，則使用作業系統區域設定。 如果應用程式無法偵測作業系統的區域設定或不支援該區域設定，則使用英文（RFC 3066 格式的 en_US.UTF-8）對事件進行本地化。
`PackageType`	已安裝的應用程式套件格式。 不建議手動更改此設定的值，該值會在應用程式初始設定期間自動填入。	`rpm` — 安裝了 RPM 套件。 `deb` — 安裝了 DEB 套件。
`UseFanotify`	使用 fanotify 技術攔截檔案操作。 不建議手動更改此設定的值，此設定會在應用程式初始設定期間指定。 此設定不適用於配備 Elbrus CPU 的裝置。	`true/yes` – 應用程式使用 fanotify 技術攔截檔案操作。 `false/no` – 應用程式不使用 fanotify 技術攔截檔案操作。

設定	描述	參數值
`KsvlaMode`	在 Light Agent 模式下使用 Kaspersky Endpoint Security。 不建議手動更改此設定的值，此設定會在應用程式初始設定期間指定。 此設定不適用於配備 Elbrus CPU 的裝置。	`true/yes` 表示應用程式是以 Light Agent 模式使用。 `false/no` – 應用程式在標準模式下使用。
`EndpointAgentMode`	在 EDR 代理程式模式下使用 Kaspersky Endpoint Security。 此設定不適用於配備 Elbrus CPU 的裝置。	`true/yes` 表示應用程式處於 EDR Agent 模式。 `false/no` – 應用程式在標準模式下使用。
`KcsMode`	將 Kaspersky Endpoint Security 用作 Kaspersky Container Security 解決方案中的檔案威脅防護元件。 不建議手動更改此設定的值，此設定僅供 Kaspersky Container Security 解決方案使用。 此設定不適用於配備 Elbrus CPU 的裝置。	`true/yes` 表示該應用程式用作 Kaspersky Container Security 解決方案中的檔案威脅防護元件。 `false/no`（預設）表示應用程式是以其中一種 Kaspersky Endpoint Security 模式使用（標準模式、EDR Agent 模式或 Light Agent 模式）。
`StartupTraces`	在應用程式啟動時啟用產生偵錯檔案。	`true/yes` – 在應用程式啟動時建立偵錯檔案。 `false/no`（預設值）– 在應用程式啟動時不建立偵錯檔案。
`RevealSensitiveInfoInTraces`	顯示偵錯檔案中可能包含個人資料（例如密碼）的資訊。	`true/yes`（預設值）— 顯示應用程式偵錯檔案中可能包含個人資料的資訊。 `false/no`（預設值）— 不顯示偵錯檔案中可能包含個人資料的資訊。
`AsyncTraces`	啟用非同步偵錯，其中資訊以非同步方式記錄到偵錯檔案中。	`true/yes` – 啟用非同步偵錯。 `false/no`（預設值）– 不啟用非同步偵錯。
`MinFreeDiskSpace`	寫入傾印檔案後剩餘的最小磁碟記憶體量（以兆位元組為單位）。	預設值：300。
`ScanMemoryLimit`	應用程式使用 RAM 的限制（以兆位元組為單位）。	預設值：8192。 我們建議將 `ScanMemoryLimit` 設定為低於 `MaxMemory` 設定，以避免掃描工作耗盡所有可用記憶體並導致應用程式重新啟動。
`MachineId`	使用者的唯一裝置 ID。	此設定的值在應用程式安裝期間自動填入。
`SocketPath`	用於遠端連線的通訊端路徑，例如，圖形介面和 kesl-control 實用程式。	預設值：/var/run/bl4control。
`MaxInotifyWatches`	/proc/sys/fs/inotify/max_user_watches 中對檔案和目錄變更 (使用者監視) 的訂購數量的限制。 如果作業系統中的設定值小於 `MaxInotifyWatches` 設定值，應用程式會將作業系統設定值變更為 `MaxInotifyWatches` 值。	預設值：299987。

設定	描述	參數值
`MaxInotifyInstances`	/proc/sys/fs/inotify/max_user_instances 中設定了一個使用者對檔案和目錄變更的訂購數量上限。 如果作業系統中的設定值小於 `MaxInotifyInstances` 設定值，應用程式會將作業系統設定值變更為 `MaxInotifyInstances` 值。	預設值：4047。
`ExecEnvMax`	應用程式從指令調用中捕獲的環境變數的數量。	預設值：50。
`ExecArgMax`	應用程式從 exec 調用中捕獲的參數數量。	預設值：20。
`AdditionalDNSLookup`	表示使用公共 DNS。 如果透過系統 DNS 存取伺服器時發生錯誤，應用程式將使用公共 DNS。這對於更新應用程式資料庫和維護裝置安全是必要的。應用程式將按以下順序使用以下公共 DNS： 1. Google Public DNS™ (8.8.8.8)。 2. Cloudflare® DNS (1.1.1.1)。 3. Alibaba Cloud® DNS (223.6.6.6)。 4. Quad9® DNS (9.9.9.9)。 5. CleanBrowsing (185.228.168.168)。	`true/yes` – 使用公共 DNS 存取卡巴斯基伺服器。 `false/no`（預設值）– 不使用公共 DNS 存取卡巴斯基伺服器。 由於應用程式與 DNS 伺服器建立了 TCP/UDP 連線，因此應用程式的請求可能包含網域位址和使用者的外部 IP 位址。例如，透過 HTTPS 互動時檢查 Web 資源的憑證時需要此資訊。如果應用程式使用公共 DNS 伺服器，則資料處理規則受對應服務的隱私權政策管轄。
`PanicThreshold`	使用可更新的內核模組時的異常停止次數上限。達到指定值時，應用程式會進入「安全」模式，該模式下不會啟動可更新的內核模組。 此設定不適用於配備 Elbrus CPU 的裝置。	預設值：3。
`SafeMode`	使用可更新的內核模組時啟用「安全」模式。在此模式下，應用程式不會啟動可更新的內核模組。 如果應用程式達到 `PanicThreshold` 設定中指定的異常停止次數上限，則會自動啟動「安全」模式。 此設定不適用於配備 Elbrus CPU 的裝置。	`true/yes` 表示應用程式已啟用「安全」模式。 `false/no`（預設）表示應用程式已停用「安全」模式，應用程式將正常運作。
`GetContainerName`	與 Kaspersky Managed Detection and Response 整合時，遙測中包含以下容器資訊： • 容器中發生的事件指示 • 容器命名空間 ID • 容器名稱 只有當您擁有使用容器掃描工作的產品授權且容器具有足夠的生命週期時，才會傳輸容器名稱。 此設定不適用於配備 Elbrus CPU 的裝置。	`true/yes` 表示在與 Kaspersky Managed Detection and Response 整合時，遙測中包含有關容器的延伸資訊。 `false/no` 表示在與 Kaspersky Managed Detection and Response 整合時，遙測中不包含有關容器的延伸資訊。

設定	描述	參數值
`UseIncreasedXdrEventsCache`	與 Detection and Response 解決方案整合時管理事件快取。高效能與 RAM 佔用量之間需要取捨。	`true/yes`（預設值）會將磁碟 I/O 降至最低，但會使用更多 RAM（100 MB）。 `false/no` 使用較少記憶體（約 5 MB），代價是增加磁碟讀取和寫入作業。
`FastShutdown`	應用程式停止或重新啟動時快速關閉 kesl 處理程序。	`true/yes` 可在應用程式停止時快速關閉 kesl 處理程序。 `false/no`（預設值）會停用應用程式停止時快速關閉 kesl 處理程序。
[網路]部分包含以下設定：		
`WtpFwMark`	iptables 規則中的標記，用於將流量轉送至應用程式以供Web 威脅防護元件處理。 如果裝有該應用程式的裝置執行其他使用 TCP 封包遮罩第九位元的其他軟體，並且發生衝突，則可能需要變更此標記。	帶有前綴 0x 的十進制值或十六進制數。 預設值：0x100。 為避免應用程式在作為分散式系統（例如 Kubernetes）一部分的節點上執行時出現循環流量掃描，您需要使用較高位元來變更網路封包標記的值。例如：0x1000 或 0x10000（標記限為 32 位元整數）。
`NtpFwMark`	iptables 規則中的標記，用於將流量轉送到應用程式以供網路威脅防護元件處理。 如果裝有該應用程式的裝置執行其他使用 TCP 封包遮罩第九位元的其他軟體，並且發生衝突，則可能需要變更此標記。	帶有前綴 0x 的十進制值或十六進制數。 預設值：0x200。 為避免應用程式在作為分散式系統（例如 Kubernetes）一部分的節點上執行時出現循環流量掃描，您需要使用較高位元來變更網路封包標記的值。例如：0x2000 或 0x20000（標記限為 32 位元整數）。
`BypassFwMark`	用來標明由應用程式建立或掃描的封包的標記，以便應用程式不再掃描它們。	帶有前綴 0x 的十進制值或十六進制數。 預設值：0x400。 為避免應用程式在作為分散式系統（例如 Kubernetes）一部分的節點上執行時出現循環流量掃描，您需要使用較高位元來變更網路封包標記的值。例如：0x4000 或 0x40000（標記限為 32 位元整數）。

`BypassNFlogMark`	應用程式在掃描時將忽略的封包標記。	帶有前綴 0x 的十進制值或十六進制數。
		預設值：0x800。
		範例：
		忽略指定裝置的所有 TCP 流量：
		`iptables -t mangle -A PREROUTING -s <IP address (CIDR)> -p tcp -j MARK --set-xmark 0x800/0x800`
		`iptables -t mangle -A OUTPUT -d <IP address (CIDR)> -p tcp -j MARK --set-xmark 0x800/0x800`
		忽略 HTTPS 伺服器流量：
		`iptables -t mangle -A PREROUTING -p tcp -m tcp --dport 443 -j MARK --set-xmark 0x800/0x800`
		`iptables -t mangle -A OUTPUT -p tcp -m tcp --sport 443 -j MARK --set-xmark 0x800/0x800`
		為避免應用程式在作為分散式系統（例如 Kubernetes）一部分的節點上執行時出現循環流量掃描，您需要使用較高位元來變更網路封包標記的值。例如：0x8000 或 0x80000（標記限為 32 位元整數）。

`ProxyRouteTable`	路由表的編號。	預設值：101。

設定	描述	參數值
[ScannerImpactStats]部分包含以下設定：		
`CollectFileScanStatistics`	啟用應用程式對檔案和處理程序掃描統計資料的計數。	`true/yes`（預設值）啟用檔案和處理程序掃描統計的統計。 `false/no` 停用檔案和處理程序掃描統計的統計。
`StatCollectionPeriod`	時間段，在此期間應用程式在將統計資料儲存到偵錯檔案和報告之前收集已掃描檔案和偵測到的處理程序的統計資料。	預設值：10分鐘。
`StatCollectionCount`	應用程式在 `StatCollectionPeriod` 參數指定的時間間隔內計數的已掃描檔案和偵測到的處理程序的數量，這些數量包含在報告和偵錯檔案中。	預設值：10。
`ReportStatAmount`	當天最常掃描的檔案和處理程序的報告中要寫入的記錄數。	預設值：20。
[虛擬化]部分包含以下設定：		
`ServerMode`	Kaspersky Endpoint Security 以 Light Agent 模式使用之受防護的虛擬機角色：伺服器或工作站。 不建議手動更改此設定的值，此設定會在應用程式初始設定期間指定。 此設定不適用於配備 Elbrus CPU 的裝置。	`true/yes` – 受防護的虛擬機用作伺服器。 `false/no` – 受防護的虛擬機用作工作站。
`VdiMode`	在以 Light Agent 模式使用應用程式時啟用 VDI 防護模式。 不建議手動更改此設定的值，此設定會在應用程式初始設定期間指定。 此設定不適用於配備 Elbrus CPU 的裝置。	`true/yes` – VDI 防護模式已啟用。 `false/no` – VDI 防護模式已停用。
[Watchdog]部分包含以下設定：		
`TimeoutAfterHeadshot`	從 Watchdog 伺服器向 kesl 處理程序傳送 HEADSHOT 訊號開始，等待 kesl 處理程序完成的最長時間。	預設值：2分鐘。
`StartupTimeout`	等待應用程式啟動的最長時間（以分鐘為單位），此後 Watchdog 伺服器將啟動重新啟動 kesl 處理程序的程式。	預設值：3分鐘。
`TimeoutAfterKill`	從 Watchdog 伺服器向 kesl 處理程序傳送 SIGKILL 訊號開始，等待受控 kesl 處理程序完成的最長時間。 如果 kesl 程序在此時間結束之前未完成，則執行 --failed-kill 設定指定的操作。	預設值：2天。
`PingInterval`	應用程式回應收到的 PING 訊息並嘗試向 Watchdog 伺服器傳送 PONG 訊息的間隔。	預設值：2000 毫秒。
`MaxRestartCount`	啟動應用程式的最大連續嘗試失敗次數。	預設值：5。
`ActivityTimeout`	應用程式向 Watchdog 伺服器傳送訊息的最大時間間隔。 如果在此時間間隔內未從應用程式收到訊息，Watchdog 伺服器將開始重新啟動 kesl 處理程序的程式。	預設值：2分鐘。

設定	描述	參數值
ConnectTimeout	自 kesl 處理程序啟動起算，應用程式連線到 Watchdog 伺服器的最大逾時時間。 如果應用程式在此時間間隔內未建立連線，Watchdog 伺服器將開始重新啟動 kesl 處理程序的程式。	預設值：3分鐘。
RegisterTimeout	從應用程式連線到 Watchdog 伺服器到伺服器收到 REGISTER 訊息的最長時間。	預設值：500 毫秒。
TimeoutAfterShutdown	從 Watchdog 伺服器向 kesl 處理程序傳送 SHUTDOWN 訊號開始，等待 kesl 處理程序完成的最長時間。	預設值：2分鐘。
MaxMemory	限制 kesl 處理程序對駐留記憶體的使用。 如果 kesl 處理程序使用的駐留記憶體超過此限制，Watchdog 伺服器將開始重新啟動 kesl 處理程序的過程。	off — 駐留集合大小不受限制。 <value>% – RAM 的 1% 到 100% 之間的值。 <value>MB – 以 MB 為單位的值。 lowest/<value>%/<value>MB – 百分比值和以 MB 為單位的絕對值中較小的值。 highest/<value>%/<value>MB – 百分比值和以 MB 為單位的絕對值中較大的值。 auto – 最多佔可用記憶體的 50%，但不少於 2 GB，也不多於 16 GB。 預設值：auto。
MaxVirtualMemory	限制 kesl 處理程序對虛擬記憶體的使用。 如果 kesl 處理程序使用的虛擬記憶體超過此限制，Watchdog 伺服器將開始重新啟動 kesl 處理程序的過程。	off（預設值）– 虛擬記憶體大小不受限制。 <value>MB – 以 MB 為單位的值。
MaxSwapMemory	對 kesl 處理程序的交換檔案大小的限制。 如果 kesl 處理程序的交換檔案超出此限制，Watchdog 伺服器將開始重新啟動 kesl 處理程序的過程。	off（預設值）– 交換檔案的大小不受限制。 <value>% – RAM 的 0% 到 100% 之間的值。 <value>MB – 以 MB 為單位的值。 lowest/<value>%/<value>MB – 百分比值和以 MB 為單位的絕對值中較小的值。 highest/<value>%/<value>MB – 百分比值和以 MB 為單位的絕對值中較大的值。
TrackProductCrashes	如果應用程式不穩定，則啟用將裝置狀態從 Kaspersky Endpoint Security 傳送到卡巴斯基安全管理中心的功能。	true/yes 允許將裝置狀態資訊從 Kaspersky Endpoint Security 傳送到卡巴斯基安全管理中心。 false/no（預設）禁止將裝置狀態從 Kaspersky Endpoint Security 傳送到卡巴斯基安全管理中心。
ProductHealthLogFile	用於應用程式穩定性監控的檔案路徑。	預設值：/var/opt/kaspersky/kesl/private/kesl_health.log。
WarnThreshold	應用程式在顯示不穩定操作的通知之前必須經歷指定次數的異常停止的時間間隔（以秒為單位）。	預設值：3600 秒。
WarnAfter_#_crash	應用程式異常停止次數上限，超過該次數後會顯示關於應用程式執行不穩定的通知。	預設值：10。 如果值為 0，則不顯示不穩定的應用程式通知。
WarnRemovingThreshold	應用程式不穩定狀態被清除後的時間間隔（以秒為單位）。	預設值：86400 秒。
SyscallHangProbePeriod	Watchdog 伺服器呼叫 open 和 execve 系統功能並增加這些功能的成功計數器的週期。	預設值：3 秒。
SyscallHangCheckPeriod	Watchdog 伺服器檢查 open 和 execve 功能的成功計數器的週期。 如果此時間之後計數器的值沒有變化，Watchdog 伺服器將啟動重新啟動 kesl 處理程序的程式。	預設值：32 秒。
DumpSuspendPeriod	等待創建應用程式傾印檔案的最長時間，在此期間 Watchdog 伺服器會暫停檢查應用程式活動。 如果此時間之後轉儲創建仍未完成，Watchdog 伺服器將啟動重新啟動 kesl 處理程序的程式。	可能的值：1-30 分鐘。 預設值：2分鐘。

設定	描述	參數值
`TimeoutAfterCoredump`	Watchdog 伺服器在將 SIGTRAP 訊號作為異常處理程序終止程序的一部分進行傳送後，暫停向 kesl 處理程序傳送其他訊號的最大持續時間。	預設值：2分鐘。 我們建議將 `TimeoutAfterCoredump` 設定為大於或等於 `DumpSuspendPeriod`。 您可以使用下列單位來指定此設定： • `<n> day|days|d` 表示天 • `<n> hour|hours|hr|h` 表示小時 • `<n> minute|minutes|min|m` 表示分鐘 • `<n> second|seconds|sec|s` 表示秒 • `<n> [msec|ms]` 表示毫秒 如果沒有指定單位，應用程式會將該值解釋為毫秒。
`TimeoutMaxCleanPeriod`	清除作業系統防火牆規則的處理程序所允許執行的最長時間。如果處理程序未在此時間內發出完成訊號，Watchdog 伺服器會將該處理程序視為凍結。	預設值：10 秒。
`TimeoutAfterClean`	在 Watchdog 伺服器向清理處理程序傳送 SIGTERM 訊號後，清除作業系統防火牆規則的處理程序可完成工作的最長時間。	預設值：10 秒。
預設情況下，設定檔中不存在**[Environment]**部分。		
`ExperimentalContainerdSupport`	在執行容器監控元件時啟用對 containerd 環境的支援。 預設情況下，設定檔中不存在此部分。如果要在容器監控元件執行時使用 containerd 環境，則需要在設定檔中手動新增 `[Environment]` 部分 以及其中的 `ExperimentalContainerdSupport` 設定。 此設定不適用於配備 Elbrus CPU 的裝置。	`true/yes` – 在容器監控元件的運作中啟用對 containerd 環境的支援。 `false/no` – 在容器監控元件的運作中不啟用對 containerd 環境的支援。
`ReduceSWMemoryConsumption`	限制行為偵測元件處理事件佇列時的記憶體消耗。 設定記憶體限制會對威脅偵測造成負面影響，包括作為與 Detection and Response 解決方案整合一部分傳輸的遙測資料品質。如果沒有其他方法可解決記憶體消耗過高的問題，我們建議僅在高負載系統上設定限制，並在設定前聯絡技術支援以取得具體指示。	1 – 限制行為偵測元件處理事件佇列時的記憶體使用量。 0（預設值）– 不限制記憶體使用量。 變更此設定後必須重新啟動應用程式。

指令列工作的預設設定

本節包含透過指令列管理 Kaspersky Endpoint Security 所提供的所有預定義工作的預設選項。

`Rollback` 和 `License` 工作沒有設定。

File_Threat_Protection 工作 (ID:1) 的預設設定

```
ScanArchived=No

ScanSfxArchived=No

ScanMailBases=No

ScanPlainMail=No

SkipPlainTextFiles=No

SkipDatabaseJournals=No

TimeLimit=60

SizeLimit=0

ActionOnThreat=DisinfectDeleteIfNotPossible

UseExcludeMasks=No

UseExcludeThreats=No

ReportCleanObjects=No

ReportPackedObjects=No

ReportUnprocessedObjects=No

UseAnalyzer=Yes

HeuristicLevel=Recommended

UseIChecker=Yes

ScanByAccessType=SmartCheck

[ScanScope.item_0000]

AreaDesc=All objects

UseScanArea=Yes

Path=/

AreaMask.item_0000=*
```

Scan_My_Computer 工作 (ID:2) 的預設設定

```
ScanFiles=Yes

ScanBootSectors=Yes

ScanComputerMemory=Yes

ScanStartupObjects=Yes

ScanArchived=Yes

ScanSfxArchived=Yes

ScanMailBases=No

ScanPlainMail=No

TimeLimit=0

SizeLimit=0

QueueScanTasks=0

ActionOnThreat=DisinfectDeleteIfNotPossible

UseExcludeMasks=No

UseExcludeThreats=No

ReportCleanObjects=No

ReportPackedObjects=No

ReportUnprocessedObjects=No

UseAnalyzer=Yes

HeuristicLevel=Recommended

UseIChecker=Yes

UseGlobalExclusions=Yes

UseOASExclusions=Yes

DeviceNameMasks.item_0000=/**

[ScanScope.item_0000]

AreaDesc=All objects
```

UseScanArea=Yes

Path=/

AreaMask.item_0000=*

Scan_File 工作 (ID:3) 的預設設定

ScanFiles=Yes

ScanBootSectors=No

ScanComputerMemory=No

ScanStartupObjects=No

ScanArchived=Yes

ScanSfxArchived=Yes

ScanMailBases=No

ScanPlainMail=No

TimeLimit=0

SizeLimit=0

QueueScanTasks=0

ActionOnThreat=DisinfectDeleteIfNotPossible

UseExcludeMasks=No

UseExcludeThreats=No

ReportCleanObjects=No

ReportPackedObjects=No

ReportUnprocessedObjects=No

UseAnalyzer=Yes

HeuristicLevel=Recommended

UseIChecker=Yes

UseGlobalExclusions=Yes

UseOASExclusions=Yes

DeviceNameMasks.item_0000=/**

```
[ScanScope.item_0000]

AreaDesc=All objects

UseScanArea=Yes

Path=/

AreaMask.item_0000=*
```

Critical_Areas_Scan 工作 (ID:4) 的預設設定

```
ScanFiles=No

ScanBootSectors=Yes

ScanComputerMemory=Yes

ScanStartupObjects=Yes

ScanArchived=Yes

ScanSfxArchived=Yes

ScanMailBases=No

ScanPlainMail=No

TimeLimit=0

SizeLimit=0

QueueScanTasks=No

ActionOnThreat=DisinfectDeleteIfNotPossible

UseExcludeMasks=No

UseExcludeThreats=No

ReportCleanObjects=No

ReportPackedObjects=No

ReportUnprocessedObjects=No

UseAnalyzer=Yes

HeuristicLevel=Recommended

UseIChecker=Yes

UseGlobalExclusions=Yes
```

```
UseOASExclusions=Yes

DeviceNameMasks.item_0000=/**

[ScanScope.item_0000]

AreaDesc=All objects

UseScanArea=Yes

Path=/

AreaMask.item_0000=*
```

更新工作 (ID:6) 的預設設定

```
ConnectionTimeout=10

ApplicationUpdateMode=DownloadOnly

[Sources.item_0000]

Enabled=Yes

SourceType=KLServers

URL=
```

System_Integrity_Monitoring 工作 (ID:11) 的預設設定

```
UseExcludeMasks=No

[ScanScope.item_0000]

AreaDesc=Kaspersky internal objects

UseScanArea=Yes

Path=/opt/kaspersky/kesl/

AreaMask.item_0000=*
```

Firewall_Management 工作 (ID:12) 的預設設定

```
DefaultIncomingAction=Allow

DefaultIncomingPacketAction=Allow

OpenNagentPorts=Yes
```

```
[NetworkZonesTrusted]

[NetworkZonesLocal]

[NetworkZonesPublic]
```

Anti_Cryptor 工作的預設設定 (ID:13)

```
ActionOnDetect=Block

BlockTime=30

UseExcludeMasks=No

[ScanScope.item_0000]

AreaDesc=All shared directories

UseScanArea=Yes

Path=AllShared

AreaMask.item_0000=*
```

Web_Threat_Protection 工作（ID:14）的預設設定

```
UseTrustedAddresses=Yes

ActionOnDetect=Block

CheckMalicious=Yes

CheckPhishing=Yes

UseHeuristicForPhishing=Yes

CheckAdware=No

CheckOther=No
```

Device_Control 工作 (ID:15) 的預設設定

```
OperationMode=Block

AllowToRequestTemporaryAccess=No

[DeviceClass]

HardDrive=DependsOnBus
```

```
RemovableDrive=DependsOnBus

Printer=DependsOnBus

FloppyDrive=DependsOnBus

OpticalDrive=DependsOnBus

Modem=DependsOnBus

TapeDrive=DependsOnBus

MultifuncDevice=DependsOnBus

SmartCardReader=DependsOnBus

PortableDevice=DependsOnBus

WiFiAdapter=DependsOnBus

NetworkAdapter=DependsOnBus

BluetoothDevice=DependsOnBus

ImagingDevice=DependsOnBus

SerialPortDevice=DependsOnBus

ParallelPortDevice=DependsOnBus

InputDevice=DependsOnBus

SoundAdapter=DependsOnBus

[DeviceBus]

USB=Allow

FireWire=Allow

[Schedules.item_0000]

ScheduleName=Default

DaysHours=All

[HardDrivePrincipals.item_0000]

Principal=\Everyone

[HardDrivePrincipals.item_0000.AccessRules.item_0000]

UseRule=Yes
```

```
ScheduleName=Default

Access=Allow

[RemovableDrivePrincipals.item_0000]

Principal=\Everyone

[RemovableDrivePrincipals.item_0000.AccessRules.item_0000]

UseRule=Yes

ScheduleName=Default

Access=Allow

[FloppyDrivePrincipals.item_0000]

Principal=\Everyone

[FloppyDrivePrincipals.item_0000.AccessRules.item_0000]

UseRule=Yes

ScheduleName=Default

Access=Allow

[OpticalDrivePrincipals.item_0000]

Principal=\Everyone

[OpticalDrivePrincipals.item_0000.AccessRules.item_0000]

UseRule=Yes

ScheduleName=Default

Access=Allow
```

Removable_Drives_Scan（ID:16）工作的預設設定

```
ScanRemovableDrives=NoScan

ScanOpticalDrives=NoScan

BlockDuringScan=No
```

Network_Threat_Protection 工作（ID:17）的預設值

```
ActionOnDetect=Block
```

```
BlockAttackingHosts=Yes

BlockDurationMinutes=60

UseExcludeIPs=No
```

Container_Scan (ID:18) 和 Custom_Container_Scan (ID:19) 工作的預設設定

```
ScanArchived=Yes

ScanSfxArchived=Yes

ScanMailBases=No

ScanPlainMail=No

TimeLimit=0

SizeLimit=0

ActionOnThreat=DisinfectDeleteIfNotPossible

UseExcludeMasks=No

UseExcludeThreats=No

ReportCleanObjects=No

ReportPackedObjects=No

ReportUnprocessedObjects=No

UseAnalyzer=Yes

HeuristicLevel=Recommended

UseIChecker=Yes

ScanContainers=Yes

ContainerNameMask=*

ScanImages=Yes

ImageNameMask=*

DeepScan=No

ContainerScanAction=StopContainerIfFailed

ImageAction=Skip

UseGlobalExclusions=Yes
```

```
QueueScanTasks=No
```

您也可以使用此設定檔中的選項執行自訂容器掃描工作。

Behavior_Detection 工作的預設設定（ID:20）

```
UseTrustedPrograms=No

TaskMode=Block

UseAEP=No

AEPMode=Block

UseTelemetryMonopolyMode=Yes

TelemetrySource=Default
```

Application_Control 工作的預設設定 (ID:21)

```
AppControlMode=DenyList

AppControlRulesAction=ApplyRules
```

Inventory_Scan 工作的預設設定 (ID:22)

```
ScanScripts=Yes

ScanBinaries=Yes

ScanAllExecutable=Yes

GoldenImageAction=DoNothing

[ScanScope.item_0000]

AreaDesc=All objects

UseScanArea=Yes

Path=/usr/bin

AreaMask.item_0000=*
```

KATAEDR 工作的預設設定（ID:24）

```
Mode=EDRKATA
```

```
UseClientPinnedCertificate=No

SynchronizationPeriod=5

ConnectionTimeout=10

RequestTimeout=10

EnableTelemetry=Yes

[Endpoints.item_0000]

Address=127.0.0.1

Port=443

[EventTransferSettings]

MaximumDataTransferTime=30

UseRequestCountLimits=Yes

MaximumNumberOfEventsInHour=3000

EventLimitExceededPercentage=15

[TelemetrySettings]

UseClientPinnedCertificate=No

ConnectionTimeout=10

RequestTimeout=10

OnlyTaggedEvents=No

[TelemetrySettings.Endpoints.item_#]

Address=

Port=443

[TelemetrySettings.EventTransferSettings]

MaximumDataTransferTime=30

UseRequestCountLimits=Yes

MaximumNumberOfEventsInHour=3000

EventLimitExceededPercentage=15
```

Web_Control 工作（ID:26）的預設設定

```
WebControlDefaultAction=Allow

ComplaintRecipient=
```

Standalone_Sandbox 工作（ID:29）的預設設定

```
ConnectionTimeout=10

RequestTimeout=10

UseClientCertificate=No

SendingMode=AutoOnly

QuarantineFile=Yes

ScanCriticalAreas=Yes

CreateIocScanTask=Yes

QuarantineFileOnIocDetected=Yes

ScanCriticalAreasOnIocDetected=Yes

Drives=Critical

ScheduleMode=Manually

[Servers.item_0000]

Address=127.0.0.1

Port=443

[SandboxTransferSettings]

SandboxQueue=1024
```

KATANDR 工作（ID:31）的預設設定

```
UseClientPinnedCertificate=No

SynchronizationPeriod=5

ConnectionTimeout=10

RequestTimeout=10
```

```
[Endpoints.item_0000]

Address=127.0.0.1

Port=8081

[EventTransferSettings]

MaximumDataTransferTime=30

MaximumNumberOfEventsInPackage=1024

UseRequestCountLimits=Yes

MaximumNumberOfEventsInHour=3000

EventLimitExceededPercentage=15

PingPeriod=450
```

KUMA 工作（ID:33）的預設設定

```
UseClientCertificate=No

UseTls=No

ConnectionTimeout=5

[Servers.item_0000]

Address=127.0.0.1

Port=443

Protocol=TCP

[SiemTransferSettings]

EventTransferTimeMax=30
```

郵件威脅防護工作（ID：35）的預設設定；

```
CheckIncomingMessagesOnly=No

ActionOnThreat=DisinfectDeleteIfNotPossible

ScanFileArchive=Yes

ScanFileOffice=Yes

UseTimeLimit=No
```

```
TimeLimit=8

UseSizeLimit=No

SizeLimit=5

ExtensionFilter=Rename

UseAnalyzer=Yes

AnalyzerLevel=Medium

[ExtensionMasks.item_0000]

UseExtensionMask=Yes

ExtensionMask=*.txt

[ExtensionMasks.item_0001]

UseExtensionMask=Yes

ExtensionMask=*.run

[ExtensionMasks.item_0002]

UseExtensionMask=Yes

ExtensionMask=*.exe

[ExtensionMasks.item_0003]

UseExtensionMask=Yes

ExtensionMask=*.js

[ExtensionMasks.item_0004]

UseExtensionMask=Yes

ExtensionMask=*.jse

[ExtensionMasks.item_0005]

UseExtensionMask=Yes

ExtensionMask=*.msi

[ExtensionMasks.item_0006]

UseExtensionMask=Yes

ExtensionMask=*.scr
```

```
[ExtensionMasks.item_0007]

UseExtensionMask=Yes

ExtensionMask=*.vbe

[ExtensionMasks.item_0008]

UseExtensionMask=Yes

ExtensionMask=*.vbs

[ExtensionMasks.item_0009]

UseExtensionMask=Yes

ExtensionMask=*.sh
```

BadUSB 攻擊防護工作（ID：37）的預設設定；

```
MaxAuthAttempts=5

TimeoutAfterAttempts=5

ProhibitOnScreenKeyboard=No

ProhibitBarcodeScanner=Yes
```

KATANDR 工作（ID:31）的預設設定

```
ConnectionTimeout=10

RequestTimeout=10

SynchronizationPeriod=5

UseTunnel=No

TunnelAddress=127.0.0.1

TunnelPort=443

[Endpoints.item_0000]

Address=127.0.0.1
Port=443
EnableTelemetry=Yes
[TelemetrySettings]

ConnectionTimeout=10
```

```
RequestTimeout=10
OnlyTaggedEvents=No
UseTunnel=No
TunnelAddress=127.0.0.1
TunnelPort=443
[TelemetrySettings.Endpoints.item_0000]

Address=127.0.0.1
Port=443
[TelemetrySettings.EventTransferSettings]

MaximumDataTransferTime=30
UseRequestCountLimits=Yes
MaximumNumberOfEventsInHour=3000
EventLimitExceededPercentage=15
MaximumNumberOfEventsInPackage=1024
```

附錄 2。配置與 Linux 版卡巴斯基防毒軟體郵件伺服器的互動

若要設定 Kaspersky Endpoint Security 和 Linux 版卡巴斯基防毒軟體郵件伺服器的聯合操作：

1. 使用以下命令將「檔案威脅防護」工作設定保存在設定檔中：

   `kesl-control --get-settings 1 --file <` 檔案的完整路徑 `>`

2. 開啟已建立的設定檔進行編輯。

3. 將以下部分新增至已建立的檔案：

   `[ExcludedFromScanScope.item_<` 項目編號 `>]`

   `Path=/var/opt/kaspersky/klms`

4. 為與 Linux 版卡巴斯基防毒軟體郵件伺服器整合的所有郵件代理重複上述指定的部分。

5. 若要將 Linux 版卡巴斯基防毒軟體郵件伺服器的篩選器和服務的臨時目錄排除在掃描範圍之外，請將以下部分新增至已建立的檔案：

   `[ExcludedFromScanScope.item_<` 項目編號 `>]`

   `Path=/tmp/klmstmp`

6. 儲存設定檔中的變更。

7. 使用以下命令將設定從設定檔匯入到「檔案威脅防護」工作：

   `kesl-control --set-settings 1 --file <` 檔案的完整路徑 `>`

附錄 3。與外部服務互動的設定

Kaspersky Endpoint Security 使用以下網路設定和加密設定與外部服務進行互動。

與外部服務互動的設定

服務和協定的網路位址	描述
activation-v2.kaspersky.com/activationservice/activationservice.svc 協定：HTTPS 連接埠：443	應用程式啟動。
s00.upd.kaspersky.com s01.upd.kaspersky.com s02.upd.kaspersky.com s03.upd.kaspersky.com s04.upd.kaspersky.com s05.upd.kaspersky.com s06.upd.kaspersky.com s07.upd.kaspersky.com s08.upd.kaspersky.com s09.upd.kaspersky.com s10.upd.kaspersky.com s11.upd.kaspersky.com s12.upd.kaspersky.com s13.upd.kaspersky.com s14.upd.kaspersky.com s15.upd.kaspersky.com s16.upd.kaspersky.com s17.upd.kaspersky.com s18.upd.kaspersky.com s19.upd.kaspersky.com 協定：HTTPS 連接埠：443	更新應用程式資料庫和模組。

服務和協定的網路位址	描述
p00.upd.kaspersky.com p01.upd.kaspersky.com p02.upd.kaspersky.com p03.upd.kaspersky.com p04.upd.kaspersky.com p05.upd.kaspersky.com p06.upd.kaspersky.com p07.upd.kaspersky.com p08.upd.kaspersky.com p09.upd.kaspersky.com p10.upd.kaspersky.com p11.upd.kaspersky.com p12.upd.kaspersky.com p13.upd.kaspersky.com p14.upd.kaspersky.com p15.upd.kaspersky.com p16.upd.kaspersky.com p17.upd.kaspersky.com p18.upd.kaspersky.com p19.upd.kaspersky.com downloads.kaspersky-labs.com 協定：HTTP 連接埠：80	更新應用程式資料庫和模組。
downloads.upd.kaspersky.com 協定：HTTPS 連接埠：443	• 更新應用程式資料庫和模組。 • 正在檢查對卡巴斯基伺服器的存取權限。如果透過系統 DNS 存取伺服器時發生錯誤，應用程式將使用公共 DNS。這對於更新應用程式資料庫和維護裝置安全是必要的。應用程式將按以下順序使用以下公共 DNS： 1. Google Public DNS (8.8.8.8)。 2. Cloudflare DNS (1.1.1.1)。 3. Alibaba Cloud DNS (223.6.6.6)。 4. Quad9 DNS (9.9.9.9)。 5. CleanBrowsing (185.228.168.168)。 由於應用程式與 DNS 伺服器建立了 TCP/UDP 連線，因此應用程式的請求可能包含網域位址和使用者的外部 IP 位址。例如，透過 HTTPS 互動時檢查 Web 資源的憑證時需要此資訊。如果應用程式使用公共 DNS 伺服器，則資料處理規則受對應服務的隱私權政策管轄。
ds.kaspersky.com 協定：HTTPS 連接埠：443	使用卡巴斯基安全網路。
ksn-a-stat-geo.kaspersky-labs.com ksn-file-geo.kaspersky-labs.com ksn-verdict-geo.kaspersky-labs.com ksn-url-geo.kaspersky-labs.com ksn-a-p2p-geo.kaspersky-labs.com ksn-cinfo-geo.kaspersky-labs.com 協定：KSN 連接埠：443，1443	使用卡巴斯基安全網路。

服務和協定的網路位址	描述
click.kaspersky.com 協定：HTTPS 連接埠：443	點擊使用者介面上的連結。
crl.kaspersky.com ocsp.kaspersky.com 協定：HTTP 連接埠：80	公鑰基礎結構（PKI）。 這些伺服器（crl.kaspersky.com）是公鑰基礎設施（PKI）的一部分，是驗證卡巴斯基基數位簽章憑證有效狀態所必需的。CRL 伺服器提供已撤銷憑證的清單。OCSP 服務允許即時查詢特定憑證的狀態。這些元件維護與數位憑證互動的安全性，並提供針對可能攻擊的防護。

附錄 4。檔案延伸程式，用於快速掃描卸除式磁碟機

com – 大小不超過 64 KB 的應用程式的可執行檔

exe – 可執行檔或自解壓存檔

sys – Microsoft Windows 系統檔案

prg – dBase™ 程式文字、Clipper 或 Microsoft Visual FoxPro®，或 WAVmaker 程式

bin – 二進位檔案

bat – 批次檔案

cmd – Microsoft Windows NT 的指令檔案（相似於 DOS 的 bat 檔案）、OS/2

dpl – 壓縮的 Borland Delphi 庫

dll – 動態連結程式庫

scr – Microsoft Windows 屏保

cpl – Microsoft Windows 控制台模組

ocx – Microsoft OLE（物件連結和嵌入）物件

tsp – 以分時模式執行的程式

drv – 裝置驅動程式

vxd – Microsoft Windows 虛擬裝置驅動程式

pif – 程式資訊檔案

lnk – Microsoft Windows 連結檔案

reg – Microsoft Windows 系統登錄機碼檔案

ini – 包含 Microsoft Windows、Windows NT 和某些應用程式配置資料的設定檔

cla – Java 類

vbs – Visual Basic® 指令碼

vbe – BIOS 影片延伸程式

js, jse – JavaScript source text

htm – 超文字文件

htt – Microsoft Windows 超文字標頭

hta – Microsoft Internet Explorer® 超文字程式

asp – Active Server Pages 指令碼

chm – 編譯的 HTML 檔案

pht – 帶有 PHP 指令碼的 HTML 檔案

php – 集成到 HTML 檔案的指令碼

wsh – Microsoft Windows Script Host 檔案

wsf – Microsoft Windows 指令碼

the – Microsoft Windows 95 桌面壁紙檔案

hlp – Win 說明檔案

msg – Microsoft Mail 郵件

plg – 郵件

mbx – 已儲存的 Microsoft Office Outlook 郵件

doc* – Microsoft Office Word 文件，例如：doc（Microsoft Office Word 文件）、docx（帶 XML 支援的 Microsoft Office Word 2007 文件）、docm（帶巨集支援的 Microsoft Office Word 2007 文件）

dot* – Microsoft Office Word 文件模組，例如 dot（Microsoft Office Word 文件範本）、dotx（Microsoft Office Word 2007 文件範本）、dotm（帶巨集支援的 Microsoft Office Word 2007 文件範本）

fpm – 資料庫程式、Microsoft Visual FoxPro 開機檔案

rtf – 富文字格式文件

shs – Windows Shell Scrap Object Handler 片段

dwg – AutoCAD® 圖紙資料庫

msi – Microsoft Windows Installer 安裝套件

otm – 適用於 Microsoft Office Outlook 的 VBA 項目

pdf – Adobe Acrobat 文件

swf – Shockwave® Flash 封包文件

jpg, jpeg – 壓縮影像格式

emf – 增強元檔案格式檔案；

ico – 物件圖示檔案

ov? – Microsoft Office Word 可執行檔

xl* – Microsoft Office Excel 文件和檔案，例如：xla 對應 Microsoft Office Excel、xlc 對應圖表、xlt 對應文件範本、xlsx 對應 Microsoft Office Excel 2007 工作簿、xltm 對應支援巨集的 Microsoft Office Excel 2007 工作簿、xlsb 對應二進位格式（非 XML）的 Microsoft Office Excel 2007 工作簿、xltx 對應於 Microsoft Office Excel 2007 範本、xlsm 對應於支援巨集的 Microsoft Office Excel 2007 範本、xlam 對應於支援巨集的 Microsoft Office Excel 2007 外掛程式

pp* – Microsoft Office PowerPoint® 文件和檔案，例如：pps 代表 Microsoft Office PowerPoint 幻燈片、ppt 代表幻燈片、pptx 代表 Microsoft Office PowerPoint 2007 幻燈片、pptm 代表支援巨集的 Microsoft Office PowerPoint 2007 幻燈片、potx 代表 Microsoft Office PowerPoint 2007 幻燈片範本、potm 代表支援巨集的 Microsoft Office PowerPoint 2007 幻燈片、ppsx 代表 Microsoft Office PowerPoint 2007 幻燈片、ppsm 代表支援巨集的 Microsoft Office PowerPoint 2007 幻燈片、ppam 代表支援巨集的 Microsoft Office PowerPoint 2007 外掛程式

md* – Microsoft Office Access® 文件和檔案，例如：mda 代表 Microsoft Office Access 工作群組，mdb 代表資料庫

sldx – Microsoft PowerPoint 2007 幻燈片

sldm – 支援巨集的 Microsoft PowerPoint 2007 幻燈片

thmx – Microsoft Office 2007 主旨

附錄 5。訊息模板中的變數

裝置控制和 Web 控制元件可讓您設定 Kaspersky Endpoint Security 向嘗試存取被封鎖的裝置、應用程式或資源，或嘗試執行潛在危險操作的使用者顯示的訊息範本。

提供了特殊變數來管理訊息範本（例如 `%USER_NAME%`）。變數可讓單一訊息範本套用至不同電腦。在產生訊息時，Kaspersky Endpoint Security 會從作業系統設定中擷取變數值，並將其插入與特定電腦、使用者及事件對應的訊息中。

裝置控制訊息範本中的變數

您可以在使用者訊息範本或管理員訊息範本中使用以下變數：

- **使用者** – `%USER_NAME%`。

  郵件產生所在電腦上的目前使用者帳戶名稱，格式為 `<device name>\<user alias>`（例如，`DESKTOP-123\John.Smith`）。

- **電腦名稱** – `%COMPUTER_NAME%`。

  裝置在其上被封鎖的電腦的名稱。

- **規則名稱** – `%RULE%`。

  封鎖裝置的規則的名稱。

- **規則觸發日期** – `%DATE%`。

  裝置被封鎖的日期，格式為 DD.MM.YYYY。

- **規則觸發時間** – `%TIME%`。

  裝置封鎖的時間，格式為 HH:MM。

- **裝置名稱** – `%DEVICE_NAME%`。

  被封鎖裝置的名稱。

- **裝置類型** – `%DEVICE_TYPE%`。

  被封鎖裝置的類型（例如，印表機、卸除式磁碟機、CD/DVD 磁碟機）。

- **裝置型號** – `%DEVICE_VIDPID%`。

  被封鎖裝置的型號（例如，VID_1234&PID_5678）。

- **裝置 ID** – `%DEVICE_ID%`。

  被封鎖裝置的 ID（例如，`SCSI\CDROM&VEN_NECVMWAR&PROD_VMWARE_SATA_CD00\5&354AE4D7&0&000000`）。

- **裝置作業** – `%OPERATION%`。

  禁止對該裝置進行的操作類型。

Web 控制訊息範本中的變數

您可以在使用者訊息範本或管理員訊息範本中使用以下變數：

- **使用者** – `%USER_NAME%`。

  郵件產生所在電腦上的目前使用者帳戶名稱，格式為 `<device name>\<user alias>`（例如，`DESKTOP-123\John.Smith`）。

- **網路資源位址** – `%CANONIC_REQUEST_URL%`。

  被封鎖 Web 資源的位址。

- **規則名稱** – `%RULE%`。

  封鎖 Web 資源的規則的名稱。

- **用於傳送訊息的電子郵件** – `%COMPLAIN_EMAIL%`。

  用於接收關於 Web 資源封鎖回饋的電子郵件地址。點擊電子郵件地址會開啟一個視窗，使用者可以在該視窗中向管理員寫訊息。

- **內容類別的名稱** – `%CONTENT_CATEGORY_LIST%`。

  被封鎖資源所屬的網站類別（例如，*支付系統*）。

- **資料類型類別的名稱** – %TYPE_CATEGORY_LIST%。

  被封鎖 Web 資源的資料類型類別（例如，*圖形檔案*）。

- **到所需網路資源的連結** – %CONTINUE_PAGE%。

  指向所請求網頁的連結（例如，http://www.example.com/pagename.html）。

- **網站連結** – %CONTINUE_SITE%。

  指向包含所請求網頁的網站的連結（例如，http://www.example.com/）。

- **用於存取網域的連結** – %CONTINUE_DOMAIN%。

  點擊此連結即可造訪該網域名稱的所有現有網頁。例如，如果被封鎖網頁的位址是 http://www.example.com，%CONTINUE_DOMAIN% 變數將被替換為 http://*.example.com 連接。點擊此連結即可存取基本網域名稱 http://www.example.com/ 的所有網址，包括子網域名稱，例如 http://start.example.com/* 或者 http://domain.domain.example.com/*，其中 * 字元代表任意字元序列（包括空字串）。

附錄 6。應用程式事件

有關每個 Kaspersky Endpoint Security 元件的操作、資料加密事件、每個惡意軟體掃描工作的完成、更新工作和完整性檢查工作以及應用程式的整體操作的資訊，都會記錄在卡巴斯基安全管理中心事件日誌和作業系統事件日誌 (syslog) 中。

緊急

系統完整性違規

狀態	!
元件	系統完整性監控
Linux 事件 ID	0
卡巴斯基安全管理中心事件 ID	GNRL_EV_FIM_ALARM
日誌 (syslog) (預設)	–
卡巴斯基安全管理中心事件日誌（預設）	✓

應用程式啟動遭拒

狀態	!
元件	應用程式控制
Linux 事件 ID	122
卡巴斯基安全管理中心事件 ID	GNRL_EV_APPLICATION_LAUNCH_DENIED
日誌 (syslog) (預設)	–
卡巴斯基安全管理中心事件日誌（預設）	✓

偵測到惡意物件（本機資料庫）

狀態	!
元件	檔案威脅防護 郵件威脅防護 行為偵測 弱點利用防禦 Sandbox
Linux 事件 ID	6
卡巴斯基安全管理中心事件 ID	`GNRL_EV_VIRUS_FOUND`
日誌 (syslog) (預設)	–
卡巴斯基安全管理中心事件日誌（預設）	✓

已超過系統完整性監控事件限制

狀態	!
元件	系統完整性監控
Linux 事件 ID	70
卡巴斯基安全管理中心事件 ID	`GNRL_EV_FIM_ALARM_OVERFLOW`
日誌 (syslog) (預設)	–
卡巴斯基安全管理中心事件日誌（預設）	✓

禁止對裝置執行操作

狀態	!
元件	裝置控制
Linux 事件 ID	94
卡巴斯基安全管理中心事件 ID	`GNRL_EV_DEVCTRL_DEV_PLUG_DENIED`
日誌 (syslog) (預設)	–
卡巴斯基安全管理中心事件日誌（預設）	✓

偵測到網路攻擊

狀態	!
元件	網路威脅防護
Linux 事件 ID	102
卡巴斯基安全管理中心事件 ID	`GNRL_EV_ATTACK_DETECTED`
日誌 (syslog) (預設)	–
卡巴斯基安全管理中心事件日誌（預設）	✓

存取遭拒（本機資料庫）

狀態	!
元件	Web 控制
Linux 事件 ID	190
卡巴斯基安全管理中心事件 ID	`GNRL_EV_WEB_URL_BLOCKED`
日誌 (syslog) (預設)	–
卡巴斯基安全管理中心事件日誌（預設）	✓

警告

無法解毒

狀態	⚠
元件	檔案威脅防護 郵件威脅防護
Linux 事件 ID	10
卡巴斯基安全管理中心事件 ID	`GNRL_EV_OBJECT_NOTCURED`
日誌 (syslog) (預設)	–
卡巴斯基安全管理中心事件日誌（預設）	✓

關於不良內容的警告 (本機資料庫)

狀態	⚠
元件	Web 控制
Linux 事件 ID	192
卡巴斯基安全管理中心事件 ID	`GNRL_EV_WEB_URL_WARNING`
日誌 (syslog) (預設)	–
卡巴斯基安全管理中心事件日誌（預設）	✓

關於封鎖網頁存取的管理員訊息

狀態	⚠
元件	Web 控制
Linux 事件 ID	196
卡巴斯基安全管理中心事件 ID	`GNRL_EV_WC_USER_REQUEST`
日誌 (syslog) (預設)	–
卡巴斯基安全管理中心事件日誌（預設）	✓

資訊訊息

物件已解毒

狀態	ⓘ
元件	檔案威脅防護 郵件威脅防護
Linux 事件 ID	9
卡巴斯基安全管理中心事件 ID	`GNRL_EV_OBJECT_CURED`
日誌 (syslog) (預設)	–
卡巴斯基安全管理中心事件日誌（預設）	✓

物件已刪除

狀態	ⓘ
元件	檔案威脅防護 郵件威脅防護
Linux 事件 ID	8
卡巴斯基安全管理中心事件 ID	GNRL_EV_OBJECT_DELETED
日誌 (syslog) (預設)	–
卡巴斯基安全管理中心事件日誌（預設）	✓

已允許啟動應用程式

狀態	ⓘ
元件	應用程式控制
Linux 事件 ID	120
卡巴斯基安全管理中心事件 ID	GNRL_EV_APPLICATION_LAUNCHED
日誌 (syslog) (預設)	–
卡巴斯基安全管理中心事件記錄	未設定

已在測試模式中允許啟動應用程式

狀態	ⓘ
元件	應用程式控制
Linux 事件 ID	121
卡巴斯基安全管理中心事件 ID	GNRL_EV_APP_LAUNCH_TESTED_ALLOW
日誌 (syslog) (預設)	–
卡巴斯基安全管理中心事件日誌（預設）	✓

已在測試模式中拒絕啟動應用程式

狀態	ⓘ
元件	應用程式控制
Linux 事件 ID	123
卡巴斯基安全管理中心事件 ID	GNRL_EV_APP_LAUNCH_TESTED_DENIED
日誌 (syslog) (預設)	–
卡巴斯基安全管理中心事件日誌（預設）	✓

裝置已連線

狀態	ⓘ
元件	裝置控制
Linux 事件 ID	90
卡巴斯基安全管理中心事件 ID	GNRL_EV_DEVCTRL_DEV_PLUGGED
日誌 (syslog) (預設)	–
卡巴斯基安全管理中心事件日誌（預設）	✓

裝置已中斷連線

狀態	ⓘ
元件	裝置控制
Linux 事件 ID	91
卡巴斯基安全管理中心事件 ID	GNRL_EV_DEVCTRL_DEV_UNPLUGGED
日誌 (syslog) (預設)	–
卡巴斯基安全管理中心事件日誌（預設）	✓

附錄 7。傳回碼

初始設定精靈的傳回碼

0 – 安裝已成功完成。

嚴重錯誤

1 – 未知錯誤（除下列列出的錯誤之外的所有其他嚴重錯誤，例如：系統錯誤、記憶體不足、檔案開啟錯誤等）。

2 – 初始設定檔包含無效參數。

3 – 安裝或更新應用程式失敗。

4 – 無法移除應用程式。

5 – 無法啟動應用程式。可能原因：存取權限設定不正確。確認只有 Root 帳戶具有下列目錄的寫入權限：/、/opt、/opt/kaspersky、/var、/var/opt、/var/opt/kaspersky、/usr 和 /usr/lib64。

6 – 安裝前尚未執行必要動作。

7 – 更新應用程式失敗。不支援安裝較早版本的應用程式。

8 – 從特權群組移除使用者失敗。

9 – 無法為應用程式安裝建立唯一的 MachineID。

10 – 啟動或重新啟動應用程式失敗。

11 – 尚未接受最終使用者產品授權協議（EULA）和隱私權政策的條款與條件。

12 – 應用程式不能同時在 Light Agent 模式和 EDR Agent 模式下使用。

13 – 找不到 Astra Linux 中用於封閉式軟體環境模式的 astra-digsig-oldkeys 套件。

14 – 初始設定已經開始。

15 – 必須移除作為卡巴斯基 Security for Virtualization 5.2 Light Agent 解決方案一部分安裝的 Light Agent for Linux 元件。

16 – 必須安裝卡巴斯基安全管理中心網路代理。

17 – 由於應用程式處理程序已在執行，因此啟動初始設定精靈失敗。

18 – 不支援 fanotify。為檔案威脅防護編譯核心模組失敗。

19 – 安裝需要管理員權限。

20 – 應用程式服務尚未啟動。

21 – 應用程式更新已復原。

22 – 不支援應用程式在 EDR Agent 模式或 Light Agent 模式下與卡巴斯基 Endpoint Detection and Response Expert (cloud) 整合。

警告

71 – 安裝期間出現多個警告。如需更多詳細資訊，請參閱安裝記錄。

72 – 更新應用程式資料庫失敗。

75 – 需要重新啟動作業系統。

76 – 套用 KSN 設定失敗，或尚未接受 KSN 聲明的條款與條件。

77 – 啟動可更新的內核模組失敗。

79 – 安裝或更新應用程式的圖形介面套件失敗。

80 – 下載應用程式資料庫失敗。

81 – 應用程式啟動因網路問題而以錯誤結束。

82 – 應用程式由政策管理。

83 – 應用程式 GUI 未啟動。

84 – 指派管理員角色失敗。找不到指定的使用者。

85 – 只能在套件管理器的忽略錯誤模式下安裝或更新應用程式套件。

86 – 移除應用程式的圖形介面套件失敗。

87 – 只能在套件管理器的忽略錯誤模式下移除應用程式套件。

88 – 將管理員角色指派給使用者失敗。

89 – 產品授權金鑰無效。

90 – 設定更新工作排程失敗。

kesl-control 命令列公用程式的回傳碼

0 – 指令/工作成功完成。

1 – 指令語法中存在一般錯誤。

2 – 傳遞的應用程式設定中有錯誤。

64 – Kaspersky Endpoint Security 未執行。

66 – 應用程式資料庫未載入（僅由 `kesl-control --app-info` 指令使用）。

67 – 應用程式啟動因網路問題而以錯誤結束。

68 – 由於應用程式由政策管理，因此無法執行該指令。

69 – 應用程式位於 Amazon Paid Ami 基礎設施中。

70 – 嘗試啟動已在執行的工作、刪除正在執行的工作、變更正在執行的工作的設定、停止已停止的工作、暫停已暫停的工作，或恢復正在執行的工作。

71 – 卡巴斯基安全網路聲明尚未被接受。

72 – 在執行自訂掃描或自訂容器掃描工作期間偵測到威脅。

73 – 嘗試設定會影響應用程式運作的應用程式控制工作設定，但未使用 `--accept` 選項進行確認。

74 – 更新後必須重新啟動 Kaspersky Endpoint Security。

75 – 必須重新啟動裝置。

76 – 禁止連線，因為只有具有 root 權限的使用者才應該對指定路徑有寫入權限。

77 – 指定的產品授權金鑰已在裝置上使用。

78 – 由於應用程式正在 Light Agent 模式下使用，因此無法執行指令/工作。

79 – 由於應用程式正在標準模式下使用，因此無法執行該指令。

80 – 由於網路問題，更新下載操作失敗。

81 – 裝置上安裝的作業系統版本不支援此元件。

128 – 未知錯誤。

65 – 所有其他錯誤。

附錄 8。準備包含應用程式資料庫的壓縮檔

在手動建立 Kaspersky Endpoint Security 安裝套件時，您可以將先前下載的應用程式資料庫新增至其中。如果您使用的是含有整合資料庫的安裝套件，則應用程式已與資料庫一起安裝；在這種情況下，您不需要在安裝後立即更新資料庫。

將應用程式資料庫新增至安裝套件會增加套件大小。

您需要為受防護裝置上作業系統的每種架構和位元數組合準備一組個別的應用程式資料庫。您可以將包含一組或多組應用程式資料庫的壓縮檔新增至安裝套件。若要準備每組應用程式資料庫，您需要在具有相符架構和位元數作業系統的裝置上，預先安裝 Kaspersky Endpoint Security 應用程式執行個體。

若要準備包含資料庫的壓縮檔：

1. 在裝置上使用卡巴斯基安全管理中心或使用指令列安裝 Kaspersky Endpoint Security 並執行初始設定。
2. 更新裝置上的應用程式資料庫。您可以在應用程式初始設定期間更新資料庫，或在安裝後透過在指令列執行*更新*工作，或在卡巴斯基安全管理中心執行*更新*工作來更新資料庫。
3. 根據受防護裝置上作業系統的架構和位元數，為資料庫建立目錄：
   - 如果應用程式安裝在 64 位元作業系統上，則為 x86_64
   - 如果應用程式安裝在 32 位元作業系統上，則為 i386
   - 如果應用程式安裝在適用於 Arm 架構的 64 位元作業系統上，則為 arm64
   - 如果應用程式安裝在適用於 Elbrus 架構的 64 位元作業系統上，則為 e2k
4. 將 /var/opt/kaspersky/kesl/private/updates 目錄的內容複製到建立的資料庫目錄。
5. 將建立的資料庫目錄新增至 kesl-bases.tgz 壓縮檔。

   如果您想要建立安裝套件，以便在具有不同架構和位元數的多個作業系統上安裝，則需要準備數個包含資料庫的目錄，並將它們全部新增至 kesl-bases.tgz 壓縮檔。

預設情況下，資料庫更新工作會在安裝 Kaspersky Endpoint Security 應用程式後啟動。如果您從具有整合資料庫的安裝套件安裝應用程式，請在安裝應用程式後停用資料庫更新工作。您可以在已建立的安裝套件的內容中，或在autoinstall.ini 設定檔中設定此設定 (`UPDATE_EXECUTE=No`)。

附錄 9。IOC 檔案的要求

建立 IOC 掃描工作時，請考慮以下IOC 檔案要求和限制：

- 應用程式支援 OpenIOC 格式版本 1.0 和 1.1 中帶有 .IOC 或 .XML 副檔名的 IOC 檔案，這是一種描述入侵指標的開放標準。
- IOC 檔案中的語義錯誤和不受支援的 IOC 術語和標籤不會導致工作失敗。對於 IOC 檔案的此類部分，應用程式會記錄不存在符合項目。

- IOC 掃描工作中使用的所有 IOC 檔案的 ID 必須是唯一的。如果有識別符一樣的 IOC 檔案，它可能會影響工作執行結果。
- 我們建議為每個威脅建立一個 IOC 檔案。這會使*IOC 掃描*工作結果更容易閱讀。

點擊下面的連結可以下載的檔案包含一個表格，其中列出了 OpenIOC 標準的 IOC 術語的完整清單。

下載 IOC TERMS.XLSX 檔案

下表列出了應用程式支援 OpenIOC 標準方式的特殊考量和限制。

OpenIOC 標準版本 1.0 和 1.1 的功能和限制

支援的條件	OpenIOC 1.0: • `is` • `isnot`（作為集合的排除項目） • `contains` • `containsnot`（作為集合的排除項目） OpenIOC 1.1: • `is` • `contains` • `starts-with` • `ends-with` • `matches` • `greater-than` • `less-than`
支援的條件屬性	OpenIOC 1.1: • `preserve-case` • `negate`
受支援的操作	`AND` `OR`
受支援的資料類型	`"date"`:日期（適用條件：`is`, `greater-than`, `less-than`） `"int"`：整數（適用條件：`is`、`greater-than`、`less-than`） `"string"`：string（適用條件：`is`、`contains`、`matches`、`starts-with`、`ends-with`） `"duration"`：持續時間（以秒為單位）（適用術語：`is`、`greater-than`、`less-than`）

對於解釋資料類型的特殊注意事項	`"boolean string"`、`"restricted string"`、`"md5"`、`"IP"`、`"sha256"`、`"base64Binary"`資料類型被解釋為字串。
	應用程式支援將`Content`參數解釋為以間隔指定的`int`和`date`資料類型：
	• OpenIOC 1.0:
	在`TO`欄位中使用`Content`操作：
	`<Content type="int">49600 TO 50700</Content>`
	`<Content type="date">2009-04-28T10:00:00Z TO 2009-04-28T16:00:00Z</Content>`
	`<Content type="int">[154192 TO 154192]</Content>`
	• OpenIOC 1.1:
	  • 使用 `greater-than`和 `less-than` 條件
	  • 使用“`TO`”欄位中的“`Content`”運算子
	
	如果指標以 `ISO 8601, Zulu time zone, UTC`格式指定，則應用程式支援`date`和`duration`資料類型的解釋。

法律聲明

資料提供

本節介紹 Kaspersky Endpoint Security 可能儲存在裝置上並在運行過程中自動傳送給卡巴斯基的資訊。

卡巴斯基根據法律和卡巴斯基的適用規則防護由此收到的任何資訊。資料透過加密通道傳輸。

有關在使用應用程式期間取得並傳送給卡巴斯基之資訊的處理、儲存和銷毀的詳細資訊，請閱讀最終使用者產品授權協議、卡巴斯基安全網路聲明，以及卡巴斯基網站上的隱私權政策。license.<language ID> 和 ksn_license.<language ID> 檔案包含最終使用者產品授權協議和卡巴斯基安全網路聲明，包括在應用程式分發套件中。

當使用啟動碼時提供的資料

如果 Kaspersky Endpoint Security 在標準模式或 EDR Agent 模式下使用並使用啟動碼啟動，為了驗證應用程式是否被合法使用並取得有關應用程式分發和使用的統計資訊，您同意自動向卡巴斯基提供以下資訊：

- 已安裝應用程式的類型、版本和當地語係化；
- 已安裝應用程式更新的版本；
- 裝置 ID 和裝置上的應用程式安裝 ID；
- 用於啟動應用程式的啟動碼；
- 目前產品授權的 ID；
- 應用程式產品授權金鑰建立日期和時間；
- 使用者裝置上的日期和時間；
- 應用程式產品授權期限到期日期和時間；
- 作業系統的類型、版本和位元大小。

從卡巴斯基更新伺服器下載更新時提供的資料

如果 Kaspersky Endpoint Security 正在標準模式或 EDR Agent 模式下使用，且您使用卡巴斯基更新伺服器下載更新，為了提高更新程序的效率並提供有關應用程式分發和使用情況的統計資訊，您同意自動向卡巴斯基提供以下資訊：

- 從產品授權中派生出的應用程式 ID；
- 應用程式的完整版本；
- 應用程式產品授權 ID；

- 使用的應用程式產品授權類型；
- 應用程式安裝 ID (PCID)；
- 應用程式更新開始的 ID；
- 目前處理的網址。

在 Light Agent 模式下使用應用程式時傳輸的資料

如果 Kaspersky Endpoint Security 以 Light Agent 模式作為 Kaspersky Security for Virtualization Light Agent 的一部分使用，應用程式會儲存以下可能包含個人和機密資料的資訊，並在應用程式執行期間將其傳送給其他解決方案元件。

- 為了啟動，Kaspersky Endpoint Security 會向 Protection Server 傳送以下資料：產品授權金鑰狀態確認的有效期限、受防護的虛擬機的 BIOS ID 以及 Light Agent 工作所需產品授權的資訊。
- 為了更新 Light Agent 資料庫，Kaspersky Endpoint Security 會向 Protection Server 傳送以下資料：從產品授權取得的軟體識別碼；軟體的完整版本；軟體產品授權識別碼；軟體安裝識別碼（PCID）；處理的網址；產品授權類型；更新開始的識別碼。
- 為了提供防護，Kaspersky Endpoint Security 會在掃描工作執行時向 Protection Server 傳送掃描物件所需的資訊。傳輸的資訊可能包含檔案名稱和其在檔案系統中的路徑、檔案校驗、網址和掃描的物件或其片段。
- 在由 VMware vCenter Server 和 VMware NSX Manager 管理的基礎結構中，Kaspersky Endpoint Security 可能會在偵測到病毒、惡意軟體或典型的網路攻擊活動時向 Integration Server 傳送關於指派給受防護的虛擬機的安全標籤的資訊。另外也會傳送受防護的虛擬機 ID。
- 為了取得選擇連線 SVM 時所使用的資訊，Kaspersky Endpoint Security 會將受防護的虛擬機的識別碼傳送到 Integration Server 和 Protection Server。
- 在多組織用戶模式下使用 Kaspersky Security for Virtualization Light Agent 解決方案時，產生租用戶防護報告所需的資訊可能會從 Kaspersky Endpoint Security Protection Server 傳送到 SVM。可能傳送以下資料：受防護的虛擬機的識別碼；受防護的虛擬機上安裝的來賓作業系統的類型和版本； Kaspersky Endpoint Security 連線到 SVM 的時間間隔。
- 為了取得統計資料，Kaspersky Endpoint Security 會向 Protection Server 傳送以下資訊：關於受防護的虛擬機的作業系統版本的資訊；Kaspersky Endpoint Security 的當地語係化；啟動的 Kaspersky Endpoint Security 元件的名稱；受防護的虛擬機的識別碼（BIOS ID）。

指定的資訊透過加密資料通道傳輸（除了掃描物件所需資訊和選擇 SVM 時使用的資訊）。預設情況下，Kaspersky Endpoint Security 和 Protection Server 之間的連線不加密。您可以在 Kaspersky Endpoint Security 設定中啟用 Light Agent 和 Protection Server 之間的資料通道加密。

傳送至卡巴斯基安全管理中心的資料

在運行過程中，Kaspersky Endpoint Security 會保存並向卡巴斯基安全管理中心提交以下資訊，其中可能包含個人和機密資料：

- 關於應用程式使用的資料庫的資訊：
  - 應用程式所需的資料庫類別清單
  - 資料庫發布並載入到應用程式的日期和時間
  - 下載的應用程式資料庫更新的發布日期
  - 上次應用程式資料庫更新的時間
  - 目前使用的應用程式資料庫中的記錄數
- 應用程式產品授權資訊：
  - 產品授權序號和類型
  - 產品授權有效期限（天）
  - 產品授權覆蓋的裝置數量
  - 產品授權期限的開始和結束日期
  - 產品授權金鑰狀態
  - 如果應用程式是使用啟動碼啟動的，則上次與啟動伺服器成功同步的日期和時間
  - 產品授權套用的應用程式識別碼
  - 產品授權下可用的功能
  - 為其提供產品授權的組織的名稱
  - 如果應用程式在訂購下使用，則提供附加資訊（訂購標誌、訂購到期日期和可續約訂購的天數、訂購提供者網址、目前訂購狀態和此狀態的原因）、應用程式在裝置上啟用的日期和時間
  - 裝置上應用程式產品授權的到期日期和時間
- 關於應用程式更新的資訊：
  - 要安裝或刪除的更新清單
  - 更新發布日期和*嚴重*狀態標誌
  - 更新的名稱、版本和簡短描述
  - 更新詳細描述連接

    - 應用程式更新的最終使用者產品授權協議和隱私權政策的識別碼和文字
    - 應用程式更新的卡巴斯基安全網路聲明識別碼和文字
    - 顯示是否可以刪除更新的指示器
    - 應用程式政策和管理外掛程式的版本
    - 應用程式管理外掛程式下載網址
    - 已安裝應用程式更新的名稱、版本和安裝日期
    - 如果更新安裝或刪除完成但有錯誤，則出現錯誤代碼和描述
    - 由於應用程式更新而需要重新啟動裝置或應用程式的標誌和原因
- 使用者同意或不同意卡巴斯基安全網路聲明、最終使用者產品授權協議和隱私權政策的條款和條件
- 分配給裝置的標籤清單
- 裝置狀態及其分配原因的清單。
- 應用程式的整體狀態及其所有元件的狀態；政策合規性資訊、裝置即時防護狀態、應用程式穩定性狀態、應用程式停止資訊。
- 上次裝置掃描的日期和時間；掃描物件的數量；檢測到的惡意物件的數量；被阻止、被刪除和被解毒的物件的數量；無法解毒的物件數量；掃描錯誤次數；偵測到的網路攻擊數量
- 有關應用程式設定的當前套用值的資料
- 群組工作和本機工作的目前狀態、執行結果以及工作的設定。
- 關於連線到用戶端裝置的外部裝置的資訊（ID、名稱、類型、製造商、描述、序號、VID/PID）
- 關於備份儲存中檔案備份副本的資訊（物件的名稱、路徑、大小和類型、物件的描述、偵測到的威脅的名稱、用於偵測威脅的應用程式資料庫的版本、物件被移動到備份儲存的日期和時間）、對備份儲存中的物件執行的操作（已刪除、已還原）以及管理員請求的檔案。
- 關於每個應用程式元件的運行以及以事件形式表示的每個工作執行的資訊：
    - 事件日期和時間
    - 事件名稱和類型
    - 事件嚴重等級
    - 事件發生時執行的工作或應用程式元件的名稱
    - 觸發事件的應用程式資訊：應用程式名稱、磁碟上檔案的路徑、處理程序識別碼、設定值（如果觸發了應用程式啟動或設定修改事件）
    - 使用者 ID
    - 觸發事件的操作發起者（工作排程程式、應用程式、卡巴斯基安全管理中心或使用者）的名稱

- 發起檔案存取的使用者的姓名和識別碼
- 物件或操作處理結果（描述、類型、名稱、威脅等級及準確性、檔案名稱及裝置上的操作類型、應用程式對操作的決策）
- 關於物件的資訊（物件名稱和類型、磁碟上物件的路徑、物件版本、大小、關於執行的操作的資訊、事件觸發器描述、不處理和跳過物件的原因描述）
- 裝置資訊（製造商名稱、裝置名稱、路徑、裝置類型、匯流排類型、識別碼、VID/PID、系統裝置標誌、裝置存取規則排程的名稱）
- 關於封鎖和解除封鎖裝置的資訊；關於被封鎖的連線的資訊（名稱、描述、裝置名稱、協定、遠端位址和連接埠、本機位址和連接埠、封包規則、操作）
- 關於所請求網址的資訊
- 關於偵測到的物件的資訊
- 偵測的類型、方法和 ID
- 關於已執行操作的資訊
- 關於應用程式資料庫的資訊（下載的資料庫更新發布日期、資料庫使用情況資訊、資料庫使用錯誤、關於取消已安裝資料庫更新的資訊）
- 關於加密偵測的資訊（勒索軟體名稱；偵測到加密的裝置名稱；關於封鎖和解除封鎖裝置的資訊）
- 應用程式設定和網路設定
- 關於觸發的應用程式控制規則（名稱和類型）以及套用該規則的結果的資訊
- 關於容器和容器鏡像的資訊（容器或容器映像的名稱、容器或容器映像的路徑、儲存庫 URL）
- 關於活動連線和被封鎖連線的資訊（名稱、描述和類型）
- 關於阻止和取消阻止存取不受信任裝置的資訊
- 關於使用 KSN 的資訊（KSN 連線狀態、KSN 基礎設施、延伸模式下 KSN 聲明的識別碼、延伸模式下對 KSN 聲明的接受、KSN 聲明的識別碼、對 KSN 聲明的接受）
- 關於憑證的資訊（網域名稱、主旨名稱、頒發者名稱、到期日期、憑證狀態、憑證類型、新增憑證的日期、頒發日期、序號、SHA256 指紋）
- 關於作為企業軟體解決方案一部分的外部系統的資訊（Integration Server 位址）
- 關於啟用和停用裝置網路隔離的資訊
- 關於在 Light Agent 模式下工作的資訊：虛擬機範本的名稱、Integration Server 的位址
- 為其啟用或停用網路隔離的裝置的名稱
- 掃描工作統計：掃描物件數量；發現的威脅數量；受感染物件的數量；疑似感染物件的數量；被解毒物件的數量；新增到備份的物件數量；已刪除物件的數量；未解毒物件的數量；掃描錯誤次數；受密碼防護的物件的數量；被跳過的物件的數量；掃描的容器和映像的數量

    - 關於應用程式中使用的 EDR Optimum 元件版本的資訊
    - 威脅發展鏈資訊：威脅開發鍊線上清單名稱、威脅發展鏈 ID
- 關於系統完整性掃描工作的操作的資訊（名稱、類型、路徑）以及關於系統基線的資訊
- 關於網路活動、封包規則和網路攻擊的資訊
- 使用者角色資訊：
    - 發起變更使用者角色的使用者的姓名和識別碼
    - 使用者角色
    - 已被指派或撤銷角色的使用者的名稱
- 關於在用戶端裝置上偵測到的受信任應用程式可執行檔的資訊（檔案的名稱、路徑、類型和雜湊值；應用程式所屬的類別清單；應用程式所屬的 KL 類別；應用程式所屬的信任群組；首次啟動檔案的時間；應用程式的名稱和版本；應用程式供應商的名稱；用於簽署應用程式的憑證資訊；序號，指紋，發行者，主旨，發佈日期，到期日期，公開金鑰）。
- 威脅發展鍊線上清單資訊：威脅發展鏈 ID；威脅發展鏈的建立時間戳記；威脅發展鏈的格式（文字或壓縮檔案）；威脅發展鏈的主體大小（以位元組為單位）。

在應用程式介面中點擊連結時提供的資料

當點擊 Kaspersky Endpoint Security 介面中的連結時，您同意自動向卡巴斯基提供以下資訊：

- 應用程式的完整版本；
- 應用程式區域設定；
- 應用程式 ID (PID)；
- 連結名稱。

使用卡巴斯基安全網路時提供的資料

卡巴斯基安全網路向卡巴斯基提供的資料集取決於卡巴斯基安全網路模式。

含有卡巴斯基安全網路聲明文字的 ksn_license.<語言 ID> 檔案包括在應用程式分發套裝中。

基本 KSN 模式下的資料提供

如果您在基本 KSN 模式下使用卡巴斯基安全網路（在網頁主控台中啟用 **使用卡巴斯基安全網路 (KSN)** 切換開關並清除 **使用延伸 KSN 模式** 核取方塊，在管理主控台中選取 **基本 KSN 模式** 選項），接受 卡巴斯基安全網路聲明的條款與條件，即表示您同意自動向卡巴斯基提供以下資訊。

延伸 KSN 模式下的資料提供

如果您在延伸 KSN 模式下使用卡巴斯基安全網路（在網頁主控台中啟用 **使用卡巴斯基安全網路 (KSN)** 切換開關並勾選 **使用延伸 KSN 模式** 核取方塊，在管理主控台中選取 **延伸 KSN 模式** 選項），接受 卡巴斯基安全網路聲明 的條款與條件，即表示除上述資訊外，您同意自動向卡巴斯基提供以下資訊。

在延伸 KSN 模式下使用 Kaspersky Endpoint Detection and Response Expert (on-premises) 整合時的資料提供

如果您將 Kaspersky Endpoint Security 作為 Kaspersky Endpoint Detection and Response Expert (on-premises) 的一部分使用，以及在延伸模式下使用卡巴斯基安全網路，則接受 卡巴斯基安全網路聲明 的條款即表示，除上述資訊外，您同意自動向卡巴斯基提供以下資訊。

在基本模式或 Endpoint Detection and Response Agent 模式下使用 Kaspersky Endpoint Security 時的資料提供

如果您在標準模式或 Endpoint Detection and Response Agent 模式下使用 Kaspersky Endpoint Security，並在延伸模式下使用卡巴斯基安全網路，接受卡巴斯基安全網路聲明的條款即表示您同意自動向卡巴斯基提供除上述所列資訊外的以下資訊：

與 Kaspersky Endpoint Detection and Response Optimum 整合時提供的資料

與*IOC 掃描*工作結果一起傳輸的資料

Kaspersky Endpoint Security 會自動將*IOC 掃描*工作結果的資料傳送至卡巴斯基安全管理中心。

*IOC 掃描*工作結果資料可能包含以下資訊：

- 網路資訊：
  - 位址解析協定 (ARP) 表中的 IP 位址
  - 位址解析協定表中的 MAC 位址
  - DNS 記錄的類型和名稱
  - 受防護裝置的 IP 位址
  - 受防護裝置的 MAC 位址
  - 遠端連線的IP位址和連線埠

    - 本機網路介面卡的 IP 位址
    - 本機介面卡上的開放連接埠號
    - 根據網際網路號碼分配機構 (IANA) 標準的協定編號
- 關於處理程序的資訊：
    - 處理程序名稱
    - 處理程序引數
    - 處理程序的可執行檔路徑
    - 處理程序 ID (PID)
    - 父處理程序 ID
    - 啟動該處理程序的使用者的名稱
    - 處理程序開始的日期和時間
- 服務資訊：
    - 服務名稱
    - 服務說明
    - 服務可執行檔的路徑和名稱
    - 服務 ID
    - 服務類型（內核驅動程式、介面卡等）
    - 服務狀態
    - 服務啟動模式
    - 啟動服務的使用者的名稱
- 關於檔案系統的資訊：
    - 磁碟區名稱
    - 磁碟區字母
    - 磁碟區類型
- 關於作業系統的資訊：
    - 作業系統的名稱和版本
    - 受防護裝置的網路名稱
    - 裝置所屬的網域或群組

- 關於 Web 活動的資訊：
  - 瀏覽器名稱
  - 瀏覽器版本
  - 上次存取 Web 資源的時間
  - HTTP 請求的網址
  - 發出 HTTP 請求的使用者的姓名
  - 發出 HTTP 請求的處理程序的名稱
  - 發出 HTTP 請求的處理程序的可執行檔的路徑
  - 發出 HTTP 請求的處理程序的 ID
  - HTTP referer（HTTP 請求來源的網址）
  - 所請求資源的網址
  - 已處理的 Web 請求的使用者代理程式 (HTTP User-Agent)
  - HTTP 請求執行時間
  - 發出 HTTP 請求的處理程序的唯一 ID

用於建立威脅發展鏈的資料

用於建立威脅發展鏈的資料可能包含以下資訊：

- 關於警示的一般資訊：
  - 警示日期和時間
  - 物件名稱
  - 掃描模式
  - 與警示相關的最後一個操作的狀態
  - 警示處理失敗的原因
- 被處理物件的相關資訊：
  - 處理程序識別碼
  - 父處理程序 ID
  - 處理程序檔 ID

- 處理程序的指令列
- 啟動該處理程序的使用者的名稱
- 在其中啟動處理程序的工作階段的 ID
- 在其中啟動處理程序的工作階段類型
- 所處理物件的完整性等級
- 使用者是否屬於特權群組
- 被處理物件的 ID
- 被處理物件的全名
- 受防護裝置的 ID
- 物件的完整名稱（本機檔案或網址）
- 被處理物件的 MD5 和 SHA256 總和檢查碼
- 被處理物件的類型
- 物件建立和最後修改的日期
- 所處理的物件大小；
- 目前處理中物件的檔案屬性；
- 關於簽署該物件的組織的資訊
- 物件數位憑證驗證結果
- 物件的安全識別碼 (SID)
- 物件的時區 ID
- 從其下載物件的網址（僅適用於檔案）
- 下載檔案的應用程式的名稱
- 下載檔案的應用程式的 MD5 和 SHA256 總和檢查碼
- 最後修改檔案的應用程式的名稱
- 上次修改檔案的應用程式的 MD5 和 SHA256 總和檢查碼
- 已處理物件的啟動次數
- 被處理物件首次啟動的日期和時間
- 檔案的唯一 ID
- 檔案全名（本機檔案或網址）

- 被處理的 Web 請求的網址
- 已處理的 Web 請求的連結來源（HTTP referer）
- 被處理的 Web 請求的使用者代理
- 已處理的 Web 請求的類型（GET 或 POST）
- 被處理的 Web 請求的本機 IP 連接埠
- 被處理的 Web 請求的遠端 IP 連接埠
- 被處理的 Web 請求的連線方向（傳入或傳出）
- 被注入惡意程式碼的處理程序的 ID

與 Kaspersky Endpoint Detection and Response (KATA) 元件整合時提供的資料

在將 Kaspersky Endpoint Security 與 Kaspersky Anti Targeted Attack Platform 解決方案的元件 Kaspersky Endpoint Detection and Response (KATA) 整合時，Kaspersky Endpoint Security 會儲存以下資訊，其中可能包含個人和機密資料：

- 提供與 Kaspersky Endpoint Detection and Response (KATA) 互動的中央節點伺服器（以下簡稱*KATA 伺服器*）的位址。
- 用於與 Kaspersky Endpoint Detection and Response (KATA) Integration Server 整合的伺服器憑證的公開金鑰
- 用於與 Kaspersky Endpoint Detection and Response (KATA) 整合的用戶端憑證
- 用於在代理伺服器上進行身分驗證的認證資料。
- 與 KATA 伺服器同步的頻率設定以及向 KATA 伺服器傳送資料的設定
- 與 KATA 伺服器的連線狀態以及關於用戶端憑證和伺服器憑證錯誤的訊息
- 從 KATA 伺服器接收的工作的設定：
  - 工作啟動排程設定
  - 啟動工作必須使用的帳戶名稱和密碼
  - 設定版本
  - 服務啟動類型
  - 服務名稱
  - 用於啟動處理程序的指令列（包括參數）
  - 物件的 MD5 和 SHA256 雜湊值

    - 物件路徑
    - IOC 檔案
- 隔離設定，根據該設定，裝置將被阻止連線到除排除項目中指定的裝置以外的其他裝置

將 Kaspersky Endpoint Security 與 Kaspersky Endpoint Detection and Response (KATA) 整合時，Kaspersky Endpoint Security 會儲存下列資訊並可能將其傳送至 KATA 伺服器：

- 向 EDR Expert (on-premise) 元件傳送同步請求的資訊：
    - 唯一識別碼
    - 伺服器位址的基礎部分
    - 裝置名稱
    - 裝置的 IP 位址
    - 裝置的 MAC 位址
    - 裝置上的本機時間
    - 安裝在裝置上的作業系統的名稱和版本
    - Kaspersky Endpoint Security 的版本
    - 正在使用的應用程式資料庫的發布日期
    - 產品授權金鑰狀態
- 工作執行報告中對 EDR Expert (on-premise) 元件的請求資訊：
    - 裝置的 IP 位址
    - 唯一識別碼
    - 伺服器位址的基礎部分
    - 裝置的 MAC 位址
    - 工作執行錯誤和返回代碼
    - 工作完成狀態
    - 工作完成時間
    - 使用的工作設定版本
    - 關於根據伺服器請求在裝置上啟動或停止的處理程序的資訊：PID 和 UniquePID、錯誤代碼、物件的 MD5 和 SHA256 總和檢查碼
    - 伺服器請求的檔案
    - 取得物件資訊時的錯誤訊息：處理錯誤的物件的全名；錯誤代碼

- 網路隔離狀態
- 對於 IOC，會傳回掃描結果（是否偵測到每個指示器、是否找到物件以及關於偵測到指示器哪個分支的資訊）。
- 對於在其中偵測到 IOC 的物件，根據指示器的類型傳回不同的值：
  - ArpEntry：來自 ARP 表的 IP 位址（包括 ipv6），來自 ARP 表的實體位址。
  - 檔案：檔案的 MD5 檔案雜湊值、檔案的 SHA256 檔案雜湊值、完整檔案名稱（包括路徑）、檔案大小。
  - 連接埠：掃描時用於建立連線的遠端 IP 位址和連接埠；本機介面卡的 IPS 位址和連接埠；協定類型（TCP、UDP、IP、RAWIP）。
  - 處理程序：處理程序名稱；處理程序參數；處理程序檔案的路徑；處理程序的系統 PID；父處理程序的系統 PID；啟動該處理程序的使用者的名稱；處理程序啟動的日期和時間。
  - SystemInfo：作業系統名稱；作業系統版本；沒有網域的裝置的網路名稱；網域或工作群組。
  - 使用者：使用者名稱。
- 對於隔離物件：
  - 檔案路徑
  - 檔案大小
  - 隔離時被分配的檔案 ID
  - 原始檔案刪除標誌
- 對於從隔離區取得的檔案：
  - 隔離時被分配的檔案 ID
- 對於阻止執行可執行檔或指令碼的情況：
  - 處理程序 ID
  - 父處理程序 ID
  - 系統 ID
  - 登入工作階段 ID
  - 處理程序狀態
  - 執行攔截的日期和時間

    - 對於辦公室應用程式禁止開啟的檔案：
        - 處理程序 ID
        - 檔案 ID
        - 執行攔截的日期和時間
- 關於檔案的資訊：
    - 檔案的唯一 ID
    - 物件的 MD5 雜湊
    - 檔案內容
- 遙測封包中的資料：
    - 關於檔案的資訊：
        - 檔案的唯一 ID
        - 檔案路徑
        - 檔案名稱
        - 檔案大小
        - 檔案屬性
        - 檔案的建立日期和時間
        - 檔案的最後修改日期和時間
        - 物件的 MD5 和 SHA256 雜湊
        - 擁有該檔案的使用者和群組的資訊（名稱和 ID）
    - 關於正在執行的處理程序的資訊：
        - 處理程序檔 ID
        - 處理程序 ID
        - 啟動該處理程序的指令列選項
        - 工作階段 ID
        - 處理程序開始的日期和時間
        - 啟動該處理程序的使用者和群組的資訊（名稱和 ID）

- 有關取得對另一個處理程序記憶體的存取權限的處理程序的資訊：
  - 處理程序 ID
  - 注入方法和位址。
  - 用於修改處理程序的指令列（包括參數）。
  - 處理程序的系統呼叫參數
- 關於偵測到並處理的威脅的資訊：
  - 根據卡巴斯基分類，偵測到的威脅的名稱以及偵測到威脅的技術
  - 應用程式資料庫版本
  - 从其下載受感染物件的網址
  - 威脅處理狀態
  - 威脅無法消除的原因
  - 威脅檔案的唯一 ID
- 檔案修改資料：
  - 被修改檔案的唯一 ID
  - 進行變更的處理程序的唯一 ID
  - 修改訊息
- 關於系統变更的資料：
  - 進行變更的處理程序的唯一 ID
  - 關於發生的變化的資訊
- 使用者登入資訊：
  - 工作階段 ID
  - 使用者資訊（姓名和 ID）
  - 從其建立工作階段的裝置的 IP 位址
- 關於正在被終止的處理程序的資料：處理程序的唯一 ID
- 關於將庫載入到處理程序位址空間的資訊：已載入庫的 ID
- 關於已建立網路連線的資訊：
  - 本機 IP 位址
  - 遠端 IP 位址

    - 連線方向
    - 協定
- 关于在某個連接埠上監聽外部網路連線的處理程序的資訊：
    - 本機位址（連接埠和 IP 位址）
    - 協定
- DNS 伺服器查詢資訊：
    - 查詢資源的域名
    - 查詢資源的 IP 位址
    - DNS 伺服器 IP 位址
    - 查詢類型

此處列出的資訊也可以儲存在偵錯檔案和傾印檔案中。

與 Kaspersky Endpoint Detection and Response Expert (on-premises) 元件整合時提供的資料

將 Kaspersky Endpoint Security 與 Kaspersky Endpoint Detection and Response Expert (on-premises) 整合時，Kaspersky Endpoint Security 會儲存以下資訊，其中可能包含個人和機密資料：

- 用於與 Kaspersky Endpoint Detection and Response Expert (on-premises) 整合的伺服器清單。
- 提供與 Kaspersky Endpoint Detection and Response Expert (on-premises) 整合的伺服器憑證公開金鑰。
- 用於與 Kaspersky Endpoint Detection and Response Expert (on-premises) 整合的用戶端憑證。
- 用於在代理伺服器上進行身分驗證的認證資料。
- 負責與 Kaspersky Endpoint Detection and Response Expert (on-premises) 整合的伺服器之同步頻率設定，以及此伺服器的資料傳輸設定。
- 處理與 Kaspersky Endpoint Detection and Response Expert (on-premises) 整合的伺服器連線狀態，以及有關用戶端和伺服器憑證錯誤的資訊。
- 來自用於與 Kaspersky Endpoint Detection and Response Expert (on-premises) 整合的伺服器的工作參數：
    - 工作啟動排程設定
    - 啟動工作必須使用的帳戶名稱和密碼
    - 設定版本
    - 服務啟動類型

    - 服務名稱
    - 用於啟動處理程序的指令列（包括參數）
    - 物件的 MD5 和 SHA256 雜湊值
    - 物件路徑
    - IOC 檔案
- 隔離設定，根據該設定，裝置將被阻止連線到除排除項目中指定的裝置以外的其他裝置

當 Kaspersky Endpoint Security 應用程式與 Kaspersky Endpoint Detection and Response Expert (on-premises) 整合時，應用程式會儲存並可將以下資料傳輸至 Integration Server：

- 向 EDR Expert (on-premises) 元件傳送同步請求的資訊：
    - 唯一識別碼
    - 伺服器位址的基礎部分
    - 裝置名稱
    - 裝置的 IP 位址
    - 裝置的 MAC 位址
    - 裝置上的本機時間
    - 安裝在裝置上的作業系統的名稱和版本
    - Kaspersky Endpoint Security 的版本
    - 正在使用的應用程式資料庫的發布日期
    - 產品授權金鑰狀態
- 工作執行報告中對 EDR Expert (on-premises) 元件的請求資訊：
    - 裝置的 IP 位址
    - 唯一識別碼
    - 伺服器位址的基礎部分
    - 裝置的 MAC 位址
    - 工作執行錯誤和返回代碼
    - 工作完成狀態
    - 工作完成時間
    - 使用的工作設定版本

- 關於根據伺服器請求在裝置上啟動或停止的處理程序的資訊：PID 和 UniquePID、錯誤代碼、物件的 MD5 和 SHA256 總和檢查碼
- 伺服器請求的檔案
- 取得物件資訊時的錯誤訊息：處理錯誤的物件的全名；錯誤代碼
- 網路隔離狀態
- 對於 IOC，會傳回掃描結果（是否偵測到每個指示器、是否找到物件以及關於偵測到指示器哪個分支的資訊）。
- 對於 YARA 規則，將傳回搜尋結果（規則是否被觸發、找到的物件以及有關觸發規則的資訊）。
- 對於在其中偵測到 IOC 的物件和 YARA 規則，根據類型傳回不同的值：
  - ArpEntry：來自 ARP 表的 IP 位址（包括 ipv6），來自 ARP 表的實體位址。
  - 檔案：檔案的 MD5 檔案雜湊值、檔案的 SHA256 檔案雜湊值、完整檔案名稱（包括路徑）、檔案大小。
  - 連接埠：掃描時用於建立連線的遠端 IP 位址和連接埠；本機介面卡的 IPS 位址和連接埠；協定類型（TCP、UDP、IP、RAWIP）。
  - 處理程序：處理程序名稱；處理程序參數；處理程序檔案的路徑；處理程序的系統 PID；父處理程序的系統 PID；啟動該處理程序的使用者的名稱；處理程序啟動的日期和時間。
  - SystemInfo：作業系統名稱；作業系統版本；沒有網域的裝置的網路名稱；網域或工作群組。
  - 使用者：使用者名稱。
- 對於隔離物件：
  - 檔案路徑
  - 檔案大小
  - 隔離時被分配的檔案 ID
  - 原始檔案刪除標誌
- 對於從隔離區接收、還原或刪除的檔案：
  - 隔離時被分配的檔案 ID
- 對於阻止執行可執行檔或指令碼的情況：
  - 處理程序 ID
  - 父處理程序 ID
  - 系統 ID
  - 登入工作階段 ID

    - 處理程序狀態
    - 執行攔截的日期和時間
- 對於辦公室應用程式禁止開啟的檔案：
    - 處理程序 ID
    - 檔案 ID
    - 執行攔截的日期和時間
- 所指定目錄中的檔案清單：
    - 檔案名稱
    - 檔案的絕對路徑
    - 檔案大小
    - 檔案類型
    - 擁有者使用者和擁有者群組的名稱和 ID
    - 檔案存取權限
    - 套用於每個檔案的特殊檔案系統標誌
    - 檔案中繼資料
    - 指向檔案的硬連結數量
    - 檔案建立、修改和最後存取時間
- 裝置上正在執行的處理程序清單：
    - 處理程序名稱
    - 處理程序開始時間
    - 處理程序狀態
    - 處理程序 ID (PID) 和父處理程序 ID
    - 處理程序的目前工作目錄
    - 啟動該處理程序的指令列選項
    - 環境變數
    - 處理程序的可執行檔路徑
    - 啟動處理程序的使用者的工作階段 ID

    - 啟動該處理程序的使用者的 ID
    - 處理程序可用使用其權限存取系統檔案和資源的使用者和群組的 ID
  - 自動執行點清單：
    - 自動執行點類型
    - 檔案名稱
    - 檔案的絕對路徑
    - 檔案存取權限
    - 套用於每個檔案的特殊檔案系統標誌
    - 擁有者使用者和擁有者群組的名稱和 ID
    - 檔案建立、修改和最後存取時間
  - 處理程序記憶體映像：
    - 處理程序名稱
    - 處理程序檔案的完整路徑
    - 處理程序傾印檔案
    - 處理程序傾印檔案的大小
  - 裝置記憶體映像：裝置 RAM 的傾印檔案
  - 裝置磁碟映像
- 關於檔案的資訊：
  - 檔案的唯一 ID
  - 物件的 MD5 雜湊
  - 檔案內容
- 遙測封包中的資料：
  - 遙測事件的資料：
    - 事件 ID。
    - 事件在被傳送的遙測封包序列中的編號。
    - 事件類型。
    - 事件時間。

- 關於受防護裝置的資訊：
  - 受防護裝置的名稱。
  - 卡巴斯基安全管理中心中受防護裝置的 ID。
  - 卡巴斯基 Endpoint Detection and Response Expert (on-premises) 中受防護裝置的 ID。
  - 安裝在受防護裝置上的作業系統的名稱、版本和系列。
  - 受防護裝置上安裝的作業系統的啟動和關閉時間。
- 關於檔案的資訊：
  - 檔案的唯一 ID
  - 檔案路徑
  - 檔案名稱
  - 檔案大小
  - 檔案屬性
  - 檔案的建立日期和時間
  - 檔案的最後修改日期和時間
  - 物件的 MD5 和 SHA256 雜湊
  - 擁有該檔案的使用者和群組的資訊（名稱和 ID）
- 關於正在執行的處理程序的資訊：
  - 處理程序檔 ID
  - 處理程序 ID
  - 啟動該處理程序的指令列選項
  - 工作階段 ID
  - 處理程序開始的日期和時間
  - 啟動該處理程序的使用者和群組的資訊（名稱和 ID）
- 有關取得對另一個處理程序記憶體的存取權限的處理程序的資訊：
  - 處理程序 ID
  - 注入方法和位址。
  - 用於修改處理程序的指令列（包括參數）。
  - 處理程序的系統呼叫參數

- 關於偵測到並處理的威脅的資訊：
  - 根據卡巴斯基分類，偵測到的威脅的名稱以及偵測到威脅的技術
  - 應用程式資料庫的發佈日期與版本
  - 从其下載受感染物件的網址
  - 威脅處理狀態
  - 威脅無法消除的原因
  - 威脅檔案的唯一 ID
- 檔案修改資料：
  - 被修改檔案的唯一 ID
  - 進行變更的處理程序的唯一 ID
  - 修改訊息
- 關於系統变更的資料：
  - 進行變更的處理程序的唯一 ID
  - 關於發生的變化的資訊
- 使用者登入資訊：
  - 工作階段 ID
  - 使用者資訊（姓名和 ID）
  - 從其建立工作階段的裝置的 IP 位址
- 關於正在被終止的處理程序的資料：處理程序的唯一 ID
- 關於將庫載入到處理程序位址空間的資訊：已載入庫的 ID
- 建立與終止網路連線的相關資訊：
  - 本機 IP 位址
  - 遠端 IP 位址
  - 連線方向
  - 協定
  - 連線建立時間
  - 連線終止時間
  - 連線持續時間

    - 連線期間傳送的位元組
    - 連線期間接收的位元組
- 关于在某個連接埠上監聽外部網路連線的處理程序的資訊：
    - 本機位址（連接埠和 IP 位址）
    - 協定
- DNS 伺服器查詢資訊：
    - 查詢資源的域名
    - 查詢資源的 IP 位址
    - DNS 伺服器 IP 位址
    - 查詢類型
- 已連線外部裝置的資訊：
    - 操作類型（裝置連線）
    - 裝置類型
    - 唯一裝置 ID
    - 裝置名稱
    - 裝置路徑
- 應用程式及其模組的相關資訊：
    - 應用程式版本。
    - 應用程式的安裝、啟動、停止或解除安裝時間。
    - 應用程式操作發起人。
    - 應用程式異常停止時的停止原因。
    - 異常停止時的返回代碼。
- 有關與工作排程器互動（工作建立和刪除）的資訊：
    - 工作名稱。
    - 已排程命令的路徑。
    - 工作啟動排程。
    - 建立工作的使用者的名稱。

    - 啟動工作的使用者的名稱。
    - 刪除工作的使用者的名稱。
- 有關服務建立、刪除和修改的資訊：
    - 服務名稱（如已變更，則包括先前的名稱）
    - 服務類型（如已變更，則包括先前的類型）
    - 可執行檔的路徑（如果已變更，則包括先前的路徑）
    - 服務依賴項（如已變更，則包括先前的依賴項）
    - 啟動服務的使用者的名稱（如果已變更，則包括先前的使用者名稱）
    - 服務的顯示名稱（如果已變更，則包括先前的顯示名稱）
    - 建立、刪除或修改服務的使用者的名稱
    - 延遲的刪除標誌
- 主控台輸入相關資訊：
    - 發起主控台輸入的處理程序的 ID 和類型
    - 主控台輸入的內容
- 關於已安裝裝置的資訊：
    - 磁區的系統名稱
    - 掛載點
- 有關處理程序記憶體變更的資訊：
    - 處理程序的系統呼叫參數
    - 執行程式碼注入的處理程序及其父處理程序的相關資訊
        - 處理程序 ID 和處理程序及其父處理程序的唯一 ID
        - 用於啟動該處理程序及其父處理程序的命令列
        - 處理程序的環境變數
        - 啟動處理程序及其父處理程序所使用的使用者帳戶類型
        - 用於啟動處理程序的系統呼叫
        - 啟動該處理程序的使用者的 ID
        - 處理程序以及父處理程序的名稱及全名
        - 處理程序和父處理程序的完整路徑

    - 處理程序及其父處理程序的 MD5 和 SHA256 雜湊值
    - 工作階段 ID
    - 啟動處理程序及其父處理程序的的使用者的名稱、網域名稱和 ID。
  - 關於透過其載入執行程式碼注入之處理程序的處理程序的資訊
    - 透過其載入處理程序的處理程序的唯一 ID
    - 透過其載入處理程序的檔案的名稱和全名
    - 透過其載入處理程序的處理程序的完整路徑
    - 透過其載入處理程序的處理程序的 MD5 雜湊
  - 關於作為處理程序發起者的處理程序的資訊
    - 處理程序 ID 和作為處理程序發起者的處理程序的唯一 ID
    - 作為處理程序發起者的處理程序的命令列
    - 啟動作為處理程序發起者的處理程序的使用者的名稱和網域名稱
    - 處理程序 ID 和作為處理程序發起者的處理程序的名稱和全面
    - 作為處理程序發起者的處理程序的完整路徑
    - 作為處理程序發起者的處理程序的 MD5 和 SHA256 雜湊

此處列出的資訊也可以儲存在偵錯檔案和傾印檔案中。

與 Kaspersky Endpoint Detection and Response Expert (cloud) 元件整合時提供的資料

將 Kaspersky Endpoint Security 與 Kaspersky Endpoint Detection and Response Expert (cloud) 整合時，Kaspersky Endpoint Security 會儲存以下資訊，其中可能包含個人和機密資料：

- 用於與 Kaspersky Endpoint Detection and Response Expert (cloud) 整合的伺服器清單。
- Kaspersky Endpoint Detection and Response Expert (cloud) 遙測和回應伺服器通道的位址。
- 用於與 Kaspersky Endpoint Detection and Response Expert (cloud) 整合的伺服器憑證。
- 用於與 Kaspersky Endpoint Detection and Response Expert (cloud) 整合的用戶端憑證。
- 負責與 Kaspersky Endpoint Detection and Response Expert (cloud) 整合的伺服器的同步頻率設定，以及該伺服器的資料傳輸設定。
- 處理 Kaspersky Endpoint Detection and Response Expert (cloud) 整合的伺服器的連線狀態，以及用戶端和伺服器憑證錯誤的相關資訊。

- 來自用於與 Kaspersky Endpoint Detection and Response Expert (cloud) 整合的伺服器的工作參數：
  - 工作啟動排程設定
  - 啟動工作必須使用的帳戶名稱和密碼
  - 設定版本
  - 服務啟動類型
  - 服務名稱
  - 用於啟動處理程序的指令列（包括參數）
  - 物件的 MD5 和 SHA256 雜湊值
  - 物件路徑
  - IOC 檔案
- 隔離設定，根據該設定，裝置將被阻止連線到除排除項目中指定的裝置以外的其他裝置

當 Kaspersky Endpoint Security 應用程式與 Kaspersky Endpoint Detection and Response Expert (cloud) 整合時，該應用程式會儲存下列資料，並可將其傳輸到 Integration Server：

- 傳送至 EDR Expert (cloud) 元件的同步請求資訊：
  - 唯一識別碼
  - 伺服器位址的基礎部分
  - 裝置名稱
  - 裝置的 IP 位址
  - 裝置的 MAC 位址
  - 裝置上的本機時間
  - 安裝在裝置上的作業系統的名稱和版本
  - Kaspersky Endpoint Security 的版本
  - 正在使用的應用程式資料庫的發布日期
  - 產品授權金鑰狀態
- 工作執行報告中對 EDR Expert (cloud) 元件的請求資訊：
  - 裝置的 IP 位址
  - 唯一識別碼
  - 伺服器位址的基礎部分
  - 裝置的 MAC 位址

- 工作執行錯誤和返回代碼
- 工作完成狀態
- 工作完成時間
- 使用的工作設定版本
- 伺服器要求在裝置上啟動的處理程序相關資訊：
  - 處理程序終止程式碼
  - 處理程序標準輸出檔案的唯一 ID。
  - 處理程序標準錯誤檔案的唯一 ID。
- 伺服器要求在裝置上啟動或停止的處理程序相關資訊：
  - PID（系統處理程序 ID）。
  - UniquePID（處理程序的唯一識別符）
  - 錯誤代碼
- 伺服器要求的檔案副本，以及該檔案的路徑和 ID。
- 作業系統重新啟動後刪除檔案的旗標。
- 取得物件資訊時的錯誤訊息：處理錯誤的物件的全名；錯誤代碼
- 網路隔離狀態
- 對於 IOC，會傳回掃描結果（是否偵測到每個指示器、是否找到物件以及關於偵測到指示器哪個分支的資訊）。
- 對於偵測到 IoC 的物件，會根據指標類型傳回不同的值：
  - ArpEntry：來自 ARP 表的 IP 位址（包括 ipv6），來自 ARP 表的實體位址。
  - 檔案：檔案的 MD5 檔案雜湊值、檔案的 SHA256 檔案雜湊值、完整檔案名稱（包括路徑）、檔案大小。
  - 連接埠：掃描時用於建立連線的遠端 IP 位址和連接埠；本機介面卡的 IPS 位址和連接埠；協定類型（TCP、UDP、IP、RAWIP）。
  - 處理程序：處理程序名稱；處理程序參數；處理程序檔案的路徑；處理程序的系統 PID；父處理程序的系統 PID；啟動該處理程序的使用者的名稱；處理程序啟動的日期和時間。
  - SystemInfo：作業系統名稱；作業系統版本；沒有網域的裝置的網路名稱；網域或工作群組。
  - 使用者：使用者名稱。

- 對於隔離物件：
  - 檔案路徑
  - 檔案大小
  - 隔離時被分配的檔案 ID
  - 原始檔案刪除標誌
- 對於從隔離區接收、還原或刪除的檔案：
  - 隔離時被分配的檔案 ID
- 對於阻止執行可執行檔或指令碼的情況：
  - 處理程序 ID
  - 父處理程序 ID
  - 系統 ID
  - 登入工作階段 ID
  - 處理程序狀態
  - 執行攔截的日期和時間
- 對於辦公室應用程式禁止開啟的檔案：
  - 處理程序 ID
  - 檔案 ID
  - 執行攔截的日期和時間
- 所指定目錄中的檔案清單：
  - 檔案名稱
  - 檔案的絕對路徑
  - 檔案大小
  - 檔案類型
  - 擁有者使用者和擁有者群組的名稱和 ID
  - 檔案存取權限
  - 套用於每個檔案的特殊檔案系統標誌
  - 檔案中繼資料

    - 指向檔案的硬連結數量
    - 檔案建立、修改和最後存取時間
- 裝置上正在執行的處理程序清單：
    - 處理程序名稱
    - 處理程序開始時間
    - 處理程序狀態
    - 處理程序 ID (PID) 和父處理程序 ID
    - 處理程序的目前工作目錄
    - 啟動該處理程序的指令列選項
    - 環境變數
    - 處理程序的可執行檔路徑
    - 啟動處理程序的使用者的工作階段 ID
    - 啟動該處理程序的使用者的 ID
    - 處理程序可用使用其權限存取系統檔案和資源的使用者和群組的 ID
- 自動執行點清單：
    - 自動執行點類型
    - 檔案名稱
    - 檔案的絕對路徑
    - 檔案存取權限
    - 套用於每個檔案的特殊檔案系統標誌
    - 擁有者使用者和擁有者群組的名稱和 ID
    - 檔案建立、修改和最後存取時間
    - 可執行檔案或可載入模組的 MD5 雜湊值和 SHA-256 雜湊值。
- 處理程序記憶體映像：
    - 處理程序記憶體映像檔案的名稱。
    - 處理程序檔案的完整路徑
    - 處理程序記憶體映像檔案的唯一 ID。
    - 處理程序記憶體映像檔案的大小。

- 裝置記憶體映像：
  - 開始傾印的日期和時間。
  - 傾印檔案的完整路徑
  - 裝置記憶體映像檔案的大小。
- 裝置磁碟映像：
  - 開始傾印的日期和時間。
  - 傾印檔案的完整路徑陣列
  - 裝置磁碟映像檔案的大小。
  - 邏輯磁碟。
  - 實體磁碟。
- 遙測封包中的資料：
  - 遙測事件的資料：
    - 事件 ID。
    - 事件在被傳送的遙測封包序列中的編號。
    - 事件類型。
    - 事件時間。
  - 關於受防護裝置的資訊：
    - 受防護裝置的名稱。
    - 卡巴斯基安全管理中心中受防護裝置的 ID。
    - 卡巴斯基 Endpoint Detection and Response Expert (on-premises) 中受防護裝置的 ID。
    - 安裝在受防護裝置上的作業系統的名稱、版本和系列。
    - 受防護裝置上安裝的作業系統的啟動和關閉時間。
  - 關於檔案的資訊：
    - 檔案的唯一 ID
    - 檔案路徑
    - 檔案名稱
    - 檔案大小
    - 檔案屬性

    - 檔案的建立日期和時間
    - 檔案的最後修改日期和時間
    - 物件的 MD5 和 SHA256 雜湊
    - 擁有該檔案的使用者和群組的資訊（名稱和 ID）
- 關於正在執行的處理程序的資訊：
    - 處理程序檔 ID
    - 處理程序 ID
    - 啟動該處理程序的指令列選項
    - 工作階段 ID
    - 處理程序開始的日期和時間
    - 啟動該處理程序的使用者和群組的資訊（名稱和 ID）
- 有關取得對另一個處理程序記憶體的存取權限的處理程序的資訊：
    - 處理程序 ID
    - 注入方法和位址。
    - 用於修改處理程序的指令列（包括參數）。
    - 處理程序的系統呼叫參數
- 關於偵測到並處理的威脅的資訊：
    - 根據卡巴斯基分類，偵測到的威脅的名稱以及偵測到威脅的技術
    - 應用程式資料庫的發佈日期與版本
    - 从其下載受感染物件的網址
    - 威脅處理狀態
    - 威脅無法消除的原因
    - 威脅檔案的唯一 ID
- 檔案修改資料：
    - 被修改檔案的唯一 ID
    - 進行變更的處理程序的唯一 ID
    - 修改訊息

- 關於系統变更的資料：
  - 進行變更的處理程序的唯一 ID
  - 關於發生的變化的資訊
- 使用者登入資訊：
  - 工作階段 ID
  - 使用者資訊（姓名和 ID）
  - 從其建立工作階段的裝置的 IP 位址
- 關於正在被終止的處理程序的資料：處理程序的唯一 ID
- 關於將庫載入到處理程序位址空間的資訊：已載入庫的 ID
- 建立與終止網路連線的相關資訊：
  - 本機 IP 位址
  - 遠端 IP 位址
  - 連線方向
  - 協定
  - 連線建立時間
  - 連線終止時間
  - 連線持續時間
  - 連線期間傳送的位元組
  - 連線期間接收的位元組
- 关于在某個連接埠上監聽外部網路連線的處理程序的資訊：
  - 本機位址（連接埠和 IP 位址）
  - 協定
- DNS 伺服器查詢資訊：
  - 查詢資源的域名
  - 查詢資源的 IP 位址
  - DNS 伺服器 IP 位址
  - 查詢類型

- 已連線外部裝置的資訊：
  - 操作類型（裝置連線）
  - 裝置類型
  - 唯一裝置 ID
  - 裝置名稱
  - 裝置路徑
- 應用程式及其模組的相關資訊：
  - 應用程式版本。
  - 應用程式的安裝、啟動、停止或解除安裝時間。
  - 應用程式操作發起人。
  - 應用程式異常停止時的停止原因。
  - 異常停止時的返回代碼。
- 有關與工作排程器互動（工作建立和刪除）的資訊：
  - 工作名稱。
  - 已排程命令的路徑。
  - 工作啟動排程。
  - 建立工作的使用者的名稱。
  - 啟動工作的使用者的名稱。
  - 刪除工作的使用者的名稱。
- 有關服務建立、刪除和修改的資訊：
  - 服務名稱（如已變更，則包括先前的名稱）
  - 服務類型（如已變更，則包括先前的類型）
  - 可執行檔的路徑（如果已變更，則包括先前的路徑）
  - 服務依賴項（如已變更，則包括先前的依賴項）
  - 啟動服務的使用者的名稱（如果已變更，則包括先前的使用者名稱）
  - 服務的顯示名稱（如果已變更，則包括先前的顯示名稱）
  - 建立、刪除或修改服務的使用者的名稱
  - 延遲的刪除標誌

- 主控台輸入相關資訊：
  - 發起主控台輸入的處理程序的 ID 和類型
  - 主控台輸入的內容
- 關於已安裝裝置的資訊：
  - 磁區的系統名稱
  - 掛載點
- 有關處理程序記憶體變更的資訊：
  - 處理程序的系統呼叫參數
  - 執行程式碼注入的處理程序及其父處理程序的相關資訊
    - 處理程序 ID 和處理程序及其父處理程序的唯一 ID
    - 用於啟動該處理程序及其父處理程序的命令列
    - 處理程序的環境變數
    - 啟動處理程序及其父處理程序所使用的使用者帳戶類型
    - 用於啟動處理程序的系統呼叫
    - 啟動該處理程序的使用者的 ID
    - 處理程序以及父處理程序的名稱及全名
    - 處理程序和父處理程序的完整路徑
    - 處理程序及其父處理程序的 MD5 和 SHA256 雜湊值
    - 工作階段 ID
    - 啟動處理程序及其父處理程序的的使用者的名稱、網域名稱和 ID。
  - 關於透過其載入執行程式碼注入之處理程序的處理程序的資訊
    - 透過其載入處理程序的處理程序的唯一 ID
    - 透過其載入處理程序的檔案的名稱和全名
    - 透過其載入處理程序的處理程序的完整路徑
    - 透過其載入處理程序的處理程序的 MD5 雜湊
  - 關於作為處理程序發起者的處理程序的資訊
    - 處理程序 ID 和作為處理程序發起者的處理程序的唯一 ID
    - 作為處理程序發起者的處理程序的命令列

- 啟動作為處理程序發起者的處理程序的使用者的名稱和網域名稱
- 處理程序 ID 和作為處理程序發起者的處理程序的名稱和全面
- 作為處理程序發起者的處理程序的完整路徑
- 作為處理程序發起者的處理程序的 MD5 和 SHA256 雜湊

此處列出的資訊也可以儲存在偵錯檔案和傾印檔案中。

與 Kaspersky Network Detection and Response (KATA) 元件整合時提供的資料

在將 Kaspersky Endpoint Security 與 Kaspersky Anti Targeted Attack Platform 解決方案的元件 Detection and Response (KATA) 整合時，Kaspersky Endpoint Security 會儲存以下資訊，其中可能包含個人和機密資料：

- NDR 伺服器位址
- 用於與 Kaspersky NetworkDetection and Response (KATA) 整合的伺服器憑證的公開金鑰
- 與 Kaspersky Network Detection and Response (KATA) 整合的用戶端憑證
- 用於在代理伺服器上進行身分驗證的認證資料。
- 與 NDR 伺服器同步的頻率設定以及向 NDR 伺服器傳送資料的設定
- NDR 伺服器連線狀態以及與用戶端憑證和伺服器憑證相關的錯誤資訊

當 Kaspersky Endpoint Security 與Kaspersky Network Detection and Response (KATA) 元件整合時，Kaspersky Endpoint Security 應用程式會儲存下列資料並將其傳送至 NDR 伺服器：

- 來自同步請求到 NDR 伺服器的資料：
  - 唯一識別碼
  - 伺服器位址的基礎部分
  - 裝置名稱
  - 裝置的 IP 位址
  - 裝置的 MAC 位址
  - 裝置上的本機時間
  - 裝置上安裝的作業系統的名稱、系列和版本
  - Kaspersky Endpoint Security 的版本
  - 正在使用的應用程式資料庫的發布日期

    - 產品授權金鑰狀態
    - 使用者裝置的型號和製造商
- 遙測封包中的資料：
    - 關於裝置和使用者的資訊：
        - 裝置名稱和裝置上的時間
        - 作業系統的系列、名稱和版本
        - 關於網路介面的資訊（描述、帶有子網路遮罩的 IP 位址清單、MAC 位址、度量數字、DNS 網域名稱、路由資訊、監聽連接埠號）
        - 裝置內部唯一 ID
        - 使用者名稱和 ID
        - 使用者群組名稱和 ID
    - 關於 Kaspersky Endpoint Security 應用程式的資訊：
        - 應用程式的名稱和版本
        - 上次更新應用程式的日期
        - 關於產品授權金鑰的資訊（序號、類型、產品授權有效期、金鑰狀態）
        - 應用程式資料庫版本
        - 支援的 API 版本清單
    - 關於已建立連線的資訊：
        - 本機 IP 位址、連接埠和 MAC 位址
        - 遠端 IP 位址、連接埠和 MAC 位址
        - 閘道 IP 位址。
        - 協定類型（根據 IANA）、協定編號和 EtherType
        - 接收和傳送的套件數量
    - 關於已處理檔案的資訊：
        - 檔案名稱和唯一 ID
        - 檔案類型和大小
        - 檔案映像的完整路徑
        - 檔案系統屬性遮罩

    - 檔案建立和修改的時間
    - 總和檢查碼（MD5 和 SHA256）
    - 檔案特權，包括繼承的和有效的
- 關於正在執行和終止處理程序的資訊：
    - 處理程序 UID 和 PID
    - 處理程序類型。
    - 工作階段 ID
    - 執行的命令
    - 環境變數
- 關於偵測到並處理的威脅的資訊：
    - 根據卡巴斯基分類，偵測到的威脅的名稱以及偵測到威脅的技術
    - 應用程式資料庫版本
    - 从其下載受感染物件的網址
    - 威脅處理狀態
    - 威脅無法消除的原因

此處列出的資訊也可以儲存在偵錯檔案和傾印檔案中。

與卡巴斯基統一監控和分析平台整合時提供的資料

將 Kaspersky Endpoint Security 與 Kaspersky Unified Monitoring and Analysis Platform 整合時，Kaspersky Endpoint Security 會儲存以下資訊，其中可能包含個人和機密資料：

- KUMA 伺服器位址
- 用於與卡巴斯基統一監控和分析平台整合的伺服器憑證的公開金鑰（使用 UDP 協定連線 KUMA 伺服器時例外）
- 用於與卡巴斯基統一監控和分析平台整合的用戶端憑證
- 用於在代理伺服器上進行身分驗證的認證資料。
- 與 KUMA 伺服器同步的頻率設定以及向 KUMA 伺服器傳送資料的設定
- KUMA 伺服器連線狀態以及與用戶端憑證和伺服器憑證相關的錯誤資訊

將 Kaspersky Endpoint Security 與 Kaspersky Unified Monitoring and Analysis Platform 整合時，Kaspersky Endpoint Security 應用程式會將下列資料儲存並透過遙測封包傳輸到 KUMA 伺服器：

- 關於檔案修改的資訊：
  - 修改前檔案的唯一 ID
  - 被修改檔案的唯一 ID
  - 進行變更的處理程序的唯一 ID
  - 檔案操作類型及標誌
  - 修改檔案的日期和時間
- 關於正在執行和終止處理程序的資訊：
  - 處理程序檔 ID
  - 處理程序 UID 和 PID
  - 啟動該處理程序的指令列選項
  - 工作階段 ID
  - 處理程序開始的日期和時間
  - 啟動該處理程序的使用者和群組的資訊（名稱和 ID）
- 事件記錄中關於事件的資訊：
  - 事件日期和時間
  - 與事件關聯的處理程序的 UID
  - 事件的類型和描述
  - 執行操作的結果

有關協力廠商代碼的資訊

關於協力廠商代碼資訊包含在應用程式安裝資料夾中的 legal_notices.txt 檔案中。

商標聲明

註冊商標及服務標誌均為其各自所有人的財產。

Adobe、Acrobat、Flash 和 Shockwave 是 Adobe 在美國和/或其他國家/地區的註冊商標或商標。

AMD64 是 Advanced Micro Devices, Inc. 的商標或註冊商標。

Amazon 是 Amazon.com, Inc. 或其附屬公司的商標。

Arm 是 Arm Limited（或子公司）在美國和/或其他國家的註冊商標。

AutoCAD 是 Autodesk, Inc. 和/或其子公司/附屬公司在美國和/或其他國家/地區的商標或註冊商標。

Borland 是 Borland Software Corporation 的商標或註冊商標。

dBase 是 dataBased Intelligence, Inc. 的商標

FireWire 是 Apple Inc. 的商標。

Bluetooth 文字、標誌和商標歸 Bluetooth SIG, Inc. 所有。

Ubuntu 和 LTS 是 Canonical Ltd 的註冊商標。

XenServer 是 Cloud Software Group, Inc. 和/或其子公司在美國和/或其他國家的註冊商標或商標。

Cloudflare、Cloudflare 標誌和 Cloudflare Workers 是 Cloudflare, Inc. 在美國和其他司法管轄區的商標和/或註冊商標。

Grafana 文字商標與 Grafana 標誌均為 Coding Instinct AB 在美國及其他國家/地區的註冊商標/服務標誌或商標/服務標誌，並經 Coding Instinct 授權使用。本公司與 Coding Instinct 或 Grafana 社群無任何從屬關係，亦未獲得其背書或贊助。

Docker 和 Docker 標誌是 Docker, Inc. 在美國和/或其國家的商標或註冊商標。Docker, Inc. 和其他各方也可能擁有此處使用的其他條款中的商標權。

Chrome、Chromium、Google Chrome、Google Public DNS 是 Google LLC 的商標。

華為、EulerOS、FusionSphere 是華為技術有限公司的商標。

Linux 是 Linus Torvalds 在美國和其他國家/地區的註冊商標。

Microsoft、Microsoft Edge、Active Directory、Hyper-V、Outlook、Visual Basic、Visual FoxPro、Visual C++、PowerPoint、Excel、Internet Explorer、Windows 和 Windows Server 是 Microsoft 集團旗下公司的商標。

OpenStack 是 OpenStack 基金會在美國和其他國家（地區）的商標。

Oracle、Java 和 JavaScript 是 Oracle 和/或其附屬公司的註冊商標。

Python 是 Python Software Foundation 的商標或註冊商標。

Red Hat Enterprise Linux、CentOS 和 Fedora 是 Red Hat, Inc. 或其子公司在美國和其他國家/地區的商標或註冊商標。

Debian 是 Public Interest, Inc. 公司的軟體的註冊商標。

Kubernetes 是 The Linux Foundation 在美國及其他國家/地區的註冊商標。

Rocky Linux 是 Rocky Enterprise Software Foundation 的商標。

UNIX 是在美國和其他國家/地區的註冊商標，透過 X/Open Company Limited 授權。

Zabbix 是 Zabbix SIA 的註冊商標。