kaspersky

# Kaspersky Endpoint Security 12.12 for Windows

© 2026 AO Kaspersky Lab

# 目錄


Kaspersky Endpoint Security for Windows 說明
- 新增功能
- 常見問題

Kaspersky Endpoint Security for Windows
- 應用程式的模式：標準、EDR Agent、Light Agent
- 分發套件
- 硬體和軟體需求
- 取決於作業系統類型的可用應用程式功能比較
- 根據管理工具比較應用程式功能
- 與其他應用程式的相容性

安裝和移除應用程式
- 透過卡巴斯基安全管理中心佈署
  - 應用程式的標準安裝
  - 建立安裝套件
  - 更新安裝套件中的資料庫
  - 建立遠端安裝工作
- 使用精靈在本機安裝應用程式
- 使用系統中心設定管理器遠端安裝應用程式
- setup.ini 檔案安裝設定說明
- 變更程式元件
- 升級先前版本的應用程式
  - 升級應用程式而無需重新啟動
  - 應用程式的 SMU 更新
- 移除應用程式

應用程式授權
- 關於最終使用者產品授權協議
- 關於授權
- 關於產品授權憑證
- 關於訂購
- 關於產品授權金鑰
- 關於啟動碼
- 關於金鑰檔案
- 依據工作站的產品授權類型比對應用程式功能
- 依據伺服器的產品授權類型比對應用程式功能
- 啟動應用程式
- 移除產品授權金鑰
- 檢視產品授權資訊
- 購買產品授權
- 續約訂購

資料提供
- 在最終使用者產品授權協議下的資料提供
- 使用卡巴斯基安全網路時的資料提供

使用 Detection and Response 解決方案時的資料提供
Kaspersky Endpoint Detection and Response
Kaspersky Sandbox
Kaspersky Anti Targeted Attack Platform (EDR)
符合歐洲聯盟法規（GDPR）
準備開始
關於 Kaspersky Endpoint Security for Windows 管理外掛程式
使用不同版本的管理外掛程式時的特別考慮
使用加密協定與外部服務進行交互時的特殊考量
程式介面
工作列通知區域中的程式圖示
簡化的應用程式介面
設定應用程式介面的顯示
準備應用程式以供使用
管理政策
建立政策
安全等級指示器
工作管理
配置本機應用程式設定
啟動和停止 Kaspersky Endpoint Security
暫停和還原電腦防護和控制
建立和使用設定檔
還原應用程式預設設定
Kaspersky Endpoint Security 的效能以及與其他應用程式的相容性
啟用或停用省電模式
啟用或停用允許其他應用程式使用資源
最佳化 Kaspersky Endpoint Security 效能的最佳實踐
惡意軟體掃描
掃描電腦
掃描連線到電腦的卸除式磁碟
背景掃描
從內容功能表掃描
應用程式完整性檢查
編輯掃描範圍
執行排程的掃描
作為不同使用者執行掃描
掃描最佳化
更新資料庫和程式模組
資料庫和應用程式模組更新方案
從伺服器儲存區更新
從共用資料夾更新
使用 Kaspersky 更新實用程式更新
在行動模式下更新
開始和停止更新工作
在不同使用者帳戶權限下開始更新工作
選取更新工作執行模式
新增更新來源

- 更新應用程式模組
- 使用代理伺服器進行更新
- 最近更新還原

進階解毒技術

- 在工作站上解毒活動威脅
- 在伺服器上解毒活動威脅

消除未處理的威脅

電腦防護

- 檔案威脅防護
  - 啟用和停用檔案威脅防護
  - 自動暫停檔案威脅防護
  - 變更"檔案威脅防護"元件對受感染檔案執行的操作
  - 構成"檔案威脅防護"元件的防護範圍
  - 選擇掃描方式
  - 在"檔案威脅防護"元件的執行中使用掃描技術
  - 最佳化檔案掃描
  - 掃描複合檔案
  - 變更掃描模式
  - 容器掃描
- 主機入侵防禦
  - 啟用和停用主機入侵防禦
  - 管理應用程式信任群組
    - 變更應用程式的信任群組
    - 配置信任群組權限
    - 選取在 Kaspersky Endpoint Security 啟動之前啟動的應用程式信任群組
    - 選擇未知應用程式的信任群組
    - 為數位簽章應用程式選擇信任群組
  - 管理應用程式權限
  - 防護作業系統資源和个人資料
  - 刪除有關未使用之應用程式的資訊
  - 監控主機入侵防禦
  - 防護對音訊和視訊的存取
- BadUSB 攻擊防護
  - 啟用和停用 BadUSB 攻擊防護
  - 使用螢幕鍵盤授權 USB 裝置
  - 條碼掃描器授權
- AMSI 防護
  - 啟用和停用 AMSI 防護
  - 透過 AMSI 防護最佳化檔案掃描
- Web 威脅防護
  - 啟用和停用 Web 威脅防護
  - 設定惡意網址偵測方法
  - 釣魚網站防護
  - 建立受信任網址清單
  - 匯出和匯入受信任網址的清單

郵件威脅防護
- 啟用和停用郵件威脅防護
- 變更對受感染電子郵件採取的操作
- 構成"郵件威脅防護"元件的防護範圍
- 掃描附加於電子郵件中的複合檔案
- 電子郵件訊息附件篩選
- 匯出和匯入附件篩選延伸程式
- 掃描 Microsoft Office Outlook 中的電子郵件
- 掃描 Thunderbird、MyOffice和 R7-Office 中的電子郵件

網路威脅防護
- 啟用和停用網路威脅防護
- 封鎖發動攻擊的電腦
- 設定排除在封鎖外的位址
- 匯出和匯入封鎖排除項目清單
- 按類型配置網路威脅防護

防火牆
- 啟用或停用防火牆
- 變更網路連線類型
- 管理網路封包規則
  - 建立網路封包規則
  - 啟動或停用網路封包規則
  - 變更網路封包規則的防火牆操作
  - 變更網路封包規則的優先順序
  - 匯出和匯入網路封包規則
  - 以 XML 格式定義網路封包規則
- 管理應用程式網路規則
  - 建立應用程式網路規則
  - 啟用和停用應用程式網路規則
  - 變更應用程式網路規則的防火牆操作
  - 變更應用程式網路規則的優先順序
- 網路監控

弱點利用防禦
- 啟用和停用弱點利用防禦
- 系統處理程序記憶體防護

行為偵測

Anti-Cryptor
- 啟用和停用共用資料夾對外部加密的防護
- 配置不受信任電腦的封鎖時間
- 編輯防護範圍
- 新增受信任電腦以進行外部資料加密
- 匯出和匯入防止共用資料夾被外部加密的排除項目清單

修復引擎

卡巴斯基安全網路
- 啟用和停用卡巴斯基安全網路的使用
- 卡巴斯基私有安全網路的限制
- 為防護元件啟用和停用雲端模式

KSN 代理設定
在卡巴斯基安全網路中檢查檔案信譽
加密連線掃描
啟用加密連線掃描
安裝受信任根憑證
掃描具有不受信任憑證的加密連線
將卡巴斯基憑證新增到自己的憑證儲存中
從掃描中排除加密連線
抹除資料
電腦控制
Web 控制
新增網路資源存取規則
按網頁資源位址篩選
按網頁資源內容篩選
測試網頁存取規則
匯出和匯入 Web 控制規則
匯出和匯入 Web 控制規則的網頁資源位址
監控使用者網際網路活動
編輯 Web 控制訊息範本
編輯網頁資源位址的遮罩
虛擬機器的 Web 控制
Web 控制訊息範本中的變數
裝置控制
關於存取規則
按類型管理對裝置的存取
透過連線匯流排管理對裝置的存取
區分使用者對裝置的存取權限
管理存取行動裝置的權限
管理存取藍牙裝置的權限
列印控制
Wi-Fi 連線控制
監視卸除式磁碟機的使用
變更快取持續時間
對信任裝置的操作
在應用程式介面中向信任清單新增裝置
在卡巴斯基安全管理中心中向受信任清單新增裝置
匯出和匯入受信任裝置的清單
獲得存取被封鎖裝置的權限
授予存取權限的線上模式
授予存取權限的離線模式
編輯裝置控制訊息範本
橋接防護
啟用橋接防護
變更連線規則的狀態
變更連線規則的優先順序

適應性異常控制
訓練“自適應異常控制”
啟用和停用適應性異常控制規則
在適應性異常控制規則觸發時變更執行的操作
建立適應性異常控制規則的排除項目
匯出和匯入適應性異常控制規則排除項目
更新適應性異常控制規則
編輯適應性異常控制訊息範本
監控適應性異常控制操作
應用程式控制
應用程式控制功能限制
接收有關安裝在使用者電腦上的應用程式的資訊
如何啟用被封鎖的應用程式模式
基於基線電腦的應用程式控制
管理應用程式控制規則
為應用程式控制規則新增觸發條件
將“可執行檔”資料夾中的可執行檔新增到應用程式類別
將事件相關的可執行檔新增到應用程式類別
新增應用程式控制規則
透過卡巴斯基安全管理中心變更應用程式控制規則的狀態
匯出和匯入應用程式控制規則
檢視“應用程式控制”元件的執行所產生的事件
檢視有關封鎖的應用程式的報告
測試應用程式控制規則
啟用和停用應用程式控制規則測試
檢視有關測試模式下封鎖的應用程式的報告
檢視“應用程式控制”元件的測試執行所產生的事件
應用程式活動監控
為檔案或資料夾建立名稱遮罩的規則
編輯應用程式控制訊息範本
應用程式控制訊息範本中的變數
實施允許的應用程式清單的最佳實踐
配置應用程式的允許清單模式
測試允許清單模式
支援允許清單模式
網路連接埠監控
啟動對所有網路連接埠的監控
建立受監控網路連接埠的清單
建立所有網路連接埠受監控的應用程式清單
匯出和匯入受監控的連接埠的清單
記錄檢查
配置預定義規則
新增自訂規則
系統完整性監控
關於系統完整性監控規則
即時系統完整性監控
按需系統完整性檢查

匯出和匯入系統完整性監控規則
檢視系統完整性監控報告
系統完整性狀態重置
Cloud Discovery
應用程式掃描排除項目
建立掃描排除項目
依偵測到的物件類型建立排除項目
編輯信任應用程式清單
建立本機信任區域
匯出和匯入受信任區域
使用受信任數位簽章處理應用程式
附錄。預先定義的掃描排除項目和受信任的應用程式
SQL 伺服器
Microsoft Exchange 伺服器
系統中心配置管理器
Citrix
VMware
管理備份
配置備份區中的檔案的最長儲存期
設定備份區的最大容量
從備份區中還原檔案
從備份區中刪除檔案備份副本
通知服務
設定事件日誌設定
設定通知的顯示和傳送
設定應用程式狀態警告在通知區域的顯示
使用者和管理員之間的訊息傳遞
管理報告
檢視報告
設定最大報告儲存時間
設定報告檔案的最大容量
將報告儲存到檔案
清理報告
Kaspersky Endpoint Security 自我防護
啟用和停用自我防護
啟用和停用 AM-PPL 支援
防護應用程式服務抵禦外部管理
支援遠端管理應用程式
密碼防護
啟用密碼防護
為單個使用者或群組授予權限
使用暫時密碼授予權限
撤銷暫時密碼
密碼防護權限的特殊方面
重設 KLAdmin 密碼
管理員伺服器連線防護

資料加密
- 加密功能限制
- 變更加密金鑰的長度 (AES56 / AES256)
- 卡巴斯基磁碟加密
  - SSD 磁碟機加密的特殊功能
  - 啟動卡巴斯基磁碟加密
  - 建立硬碟磁碟機加密排除清單
  - 匯出和匯入從加密範圍中排除的硬碟磁碟機清單
  - 啟用單點登入 (SSO) 技術
  - 管理身分驗證代理帳戶
  - 配合身分驗證代理使用令牌和智慧卡
  - 硬碟磁碟機解密
  - 還原對受卡巴斯基磁碟加密技術防護的磁碟機的存取權限
  - 使用身分驗證代理服務帳戶登入
  - 更新作業系統
  - 消除加密功能更新的錯誤
  - 身分驗證代理偵錯
  - 編輯身分驗證代理說明文字
  - 測試執行身分驗證代理後，刪除剩餘物件與資料
- BitLocker 管理
  - 啟動 BitLocker 磁碟機加密
  - 解密受 BitLocker 防護的硬碟磁碟機
  - 還原對 BitLocker 防護的磁碟機的存取權限
  - 暫停 BitLocker 防護以更新軟體
- 本機電腦磁碟機上檔案級加密
  - 加密本機電腦磁碟中的檔案
  - 為應用程式建立加密檔案存取規則
  - 加密特定應用程式建立或修改的檔案
  - 生成解密規則
  - 在本機電腦磁碟機上解密檔案
  - 建立加密資料
  - 還原對加密檔案的存取權限
  - 作業系統故障後還原對加密檔案的存取
  - 編輯加密檔案存取訊息範本
- 卸除式磁碟機加密
  - 啟動卸除式磁碟機加密
  - 新增卸除式磁碟機加密規則
  - 匯出和匯入卸除式磁碟機的加密規則清單
  - 用於存取卸除式磁碟機上加密檔案的攜帶模式
  - 卸除式磁碟機解密
- 檢視資料加密詳細資訊
  - 檢視加密狀態
  - 在卡巴斯基安全管理中心的資訊顯示器上檢視加密統計資訊
  - 檢視本機電腦磁碟機上檔案加密錯誤
  - 檢視資料加密報告

無法存取加密裝置時的裝置使用
使用 FDERT 還原實用程式還原資料
建立作業系統緊急修復光碟
Detection and Response 解決方案
MDR 和 EDR Optimum 許可
Kaspersky Endpoint Agent
將 [KES+KEA] 配置遷移到 [KES+內建代理] 配置
Kaspersky Endpoint Agent 的政策和工作遷移
Endpoint Detection and Response Agent (EDR Agent)
安裝 EDR Agent
將 EDR Agent 與 MDR 整合
將 EDR Agent 與 EDR (KATA) 整合
將 EDR Agent 與 NDR (KATA) 整合
EDR Agent 與 EDR Expert (on-premise) 整合
與協力廠商 EPP 應用程式的相容性
Managed Detection and Response
內建代理與 MDR 整合
MDR 的 KEA 到 KES 遷移指南
Endpoint Detection and Response
內建代理與 EDR Optimum / EDR Expert 整合
掃描洩露指示器（標準工作）
IOC 掃描的延伸遙測
移動檔案到隔離
獲取檔案
刪除檔案
處理程序啟動
終止處理程序
執行防護
電腦網路隔離
Cloud Sandbox
EDR Optimum 的 KEA 到 KES 遷移指南
Kaspersky Sandbox
內建代理與 Kaspersky Sandbox 整合
掃描洩露指示器（獨立工作）
Kaspersky Sandbox 的 KEA 到 KES 遷移指南
Kaspersky Anti Targeted Attack Platform
內建代理與 EDR / NDR (KATA) 整合
配置 EDR (KATA) 遙測
EDR (KATA) 遙測排除項目
例 1。被排除的處理程序
例 2。被排除的網路通訊
例 3。被排除的檔案操作
例 4。被排除的登錄檔修改
KATA Sandbox
內建代理與 KATA Sandbox 整合
配置威脅回應操作
EDR (KATA) 的 KEA 到 KES 遷移指南

- Endpoint Detection and Response Expert（本地部署）
  - 內建代理與 EDR Expert (on-premise) 整合
  - 配置 EDR Expert (on-premise) 遙測設定
  - EDR Expert (on-premise) 遙測排除項目
  - 匯出和匯入 EDR Expert (on-premise) 事件篩選器
- 管理隔離
  - 配置最大隔離大小
  - 將有關隔離檔案的資料傳送到卡巴斯基安全管理中心
  - 從隔離區中還原檔案
- 監控 EDR 操作

Kaspersky Unified Monitoring and Analysis Platform (KUMA)
- Kaspersky Endpoint Security 與 KUMA 整合
- 篩選要傳送到 KUMA 的事件
- 匯出和匯入 KUMA 事件篩選器

KSWS 到 KES 遷移指南
- KSWS 和 KES 元件的對應關係
- KSWS 和 KES 設定的對應關係
- 遷移 KSWS 元件
- 遷移 KSWS 工作和政策
- 遷移 KSWS 受信任區域
- 遷移 KSWS 應用程式啟動控制規則
- 安裝 KES 而不是 KSWS
- 將 [KSWS+KEA] 配置遷移到 [KES+內建代理] 配置
- 確保已成功刪除 Kaspersky Security for Windows Server
- 使用 KSWS 金鑰啟動 KES
- 遷移高負載伺服器的特殊注意事項
- 在 Server Core 模式下管理伺服器上的應用程式
- 將 [KSWS+KEA] 遷移到 [KES+內建代理]

用來防護虛擬機的 Light Agent 模式
- Light Agent 模式的特殊注意事項
- 虛擬機的初步配置
  - 與 Citrix App Layering 技術的相容性
  - 與 Citrix Provisioning (Citrix Provisioning Services) 技術的相容性
  - 與 Omnissa App Volumes 技術的相容性
- 安裝 Light Agent
- 將 Light Agent 連線到 SVM
  - SVM 發現
  - 配置 Light Agent 的 SVM 選取演算法
  - 將 Light Agent 的連線分發到 SVM（標籤）
  - 防護 Light Agent 和 SVM 之間的連線
- 啟動 Light Agent
- KSVLA Light Agent 到 KES Light Agent 遷移指南
  - 安裝 KES Light Agent 而不是 KSVLA Light Agent
  - KSVLA Light Agent 和 KES Light Agent 元件的對應關係
  - 遷移 KSVLA Light Agent 工作和政策
  - 將 [KSVLA Light Agent+KEA] 配置遷移到 [KES Light Agent+內建代理] 配置

從命令列管理應用程式
- Setup。安裝應用程式
- Setup /x。移除應用程式
- msiexec /i.還原應用程式
- AVP 命令
  - SCAN。惡意軟體掃描
  - UPDATE。更新資料庫和程式模組
  - ROLLBACK。最近更新還原
  - TRACES。偵錯
  - START。啟動設定檔
  - STOP。停止設定檔
  - STATUS。設定檔狀態
  - STATISTICS。設定檔操作統計
  - RESTORE。從備份區中還原檔案
  - EXPORT。匯出應用程式設定
  - IMPORT。匯入應用程式設定
  - ADDKEY。套用金鑰檔案
  - LICENSE。產品授權
  - RENEW。購買產品授權
  - PBATESTRESET。在加密磁碟之前重設磁碟檢查結果
  - EXIT。結束應用程式
  - EXITPOLICY。停用政策
  - STARTPOLICY。啟用政策
  - DISABLE。停用防護
  - SPYWARE。間諜軟體偵測
  - KSN。在 KSN / KPSN 之間切換
  - SERVERBINDINGDISABLE。停用伺服器連線防護
- KESCLI 命令
  - Scan。惡意軟體掃描
  - GetScanState。掃描完成狀態
  - GetLastScanTime。確定掃描完成時間
  - GetThreats。獲取偵測到的威脅的資料
  - UpdateDefinitions。更新資料庫和程式模組
  - GetDefinitionState。確定資料庫的上次更新日期和時間
  - EnableRTP。啟用防護
  - GetRealTimeProtectionState。"檔案威脅防護"狀態
  - GetEncryptionState。瓷碟加密狀態
  - Version。識別應用程式版本
- Detection and Response 管理指令
  - SANDBOX。管理 Sandbox
  - PREVENTION。管理執行防護
  - ISOLATION。管理網路隔離
  - RESTORE。從隔離區中還原檔案
  - IOCSCAN。掃描查找洩露指示器 (IOC)
  - MDRLICENSE.MDR 啟動
  - EDRKATA。與 EDR (KATA) 進行整合
  - KUMA。與 KUMA 整合

YARA。執行 YARA 掃描
遙測篩選器。篩選要傳送到 KUMA 的事件
Light Agent 管理指令
KSVLAINFO。確定 Light Agent 模式
VllSINFO。Light Agent 與 Integration Server 的連線狀態
SVMINFO。Light Agent 與 Protection Server 的連線狀態
錯誤代碼
附錄。應用程式設定檔
透過 REST API 管理應用程式
使用 REST API 安裝應用程式
使用 API
關於應用程式的資訊源
聯絡技術支援服務
偵錯檔案的內容和儲存
應用程式操作追蹤
應用程式效能追蹤
傾印寫入
防護傾印檔案和偵錯檔案
取得作業系統資料 (Kaspersky Get System Info)
限制和警告
詞彙表
Cloud Discovery
Integration Server
IOC
IOC 檔案
Kerberos 身分驗證
Light Agent
OLE 物件
OpenIOC
SVM
受信任平台模組
受感染的檔案
可疑網頁位址資料庫
存檔
工作
已感染檔案
憑證發佈者
掃描範圍
授權憑證
攜帶式檔案管理器
啟動金鑰
病毒資料庫
管理群組
網路代理
網頁資源位址的正規表示式
解毒
誤報

身分驗證代理
遮罩
釣魚網頁位址資料庫
防護範圍
附錄
附錄 1。應用程式設定
檔案威脅防護
Web 威脅防護
郵件威脅防護
網路威脅防護
防火牆
BadUSB 攻擊防護
AMSI 防護
弱點利用防禦
行為偵測
主機入侵防禦
修復引擎
卡巴斯基安全網路
記錄檢查
Anti-Cryptor
Web 控制
裝置控制
應用程式控制
適應性異常控制
系統完整性監控
Endpoint Sensor
Sandbox
Managed Detection and Response
Endpoint Detection and Response
Endpoint Detection and Response Expert（本地部署）
Network Detection and Response (KATA)
與 KUMA 整合
完整磁碟加密
檔案級加密
卸除式磁碟機加密
模組（資料加密）
排除
應用程式設定
報告和儲存
網路設定
介面
監控設定
更新資料庫和程式模組
附錄 2。應用程式信任群組
附錄 3。檔案延伸程式，用於快速掃描卸除式磁碟機
附錄 4。郵件威脅防護附件篩選器的檔案類型
附錄 5。與外部服務交互的網路設定

- 附錄 6。應用程式事件
  - 緊急
  - 功能失敗
  - 警告
  - 資訊訊息
- 附錄 7。受支援的執行防護的檔案副檔名
- 附錄 8。支援執行防止的指令碼解譯器
- 附錄 9。登錄檔中的IOC 掃描範圍 (RegistryItem)
- 附錄 10。IOC 檔案要求
- 附錄 11。應用程式元件規則中的使用者帳戶
- 附錄 12。EDR 威脅回應的 API

有關協力廠商代碼的資訊

商標聲明

# Kaspersky Endpoint Security for Windows 說明

## 版本 12.12 新增功能

- 共用資料夾保護現在是一個獨立元件，Anti-Cryptor。
- 向*IOC掃描*工作新增了回顧掃描功能。
- 每個版本 Kaspersky Endpoint Security for Windows 中的新增功能

## 準備開始

- Kaspersky Endpoint Security for Windows 部署
- Kaspersky Endpoint Security for Windows 初始設定
- 最佳化應用程式效能
- Kaspersky Endpoint Security for Windows 授權

## 消除威脅

- 工作站上
- 伺服器上
- 回應偵測到洩露指示（網路隔離 → 隔離 → 執行防護）

### 將 KES 用作其它解決方案的一部分

- Kaspersky EDR
- Kaspersky Sandbox
- Kaspersky MDR

### 資料提供

- 根據最終使用者產品授權協議
- 當使用 KSN 時
- GDPR

# 新增功能

更新 12.12

Kaspersky Endpoint Security 12.12 for Windows 引入了以下功能和改進：

1. 先前作為行為偵測元件一部分的共用資料夾外部加密防護功能，現在成為一個獨立元件。 Anti-Cryptor。
2. 已新增對 Kerberos 協定的支持，以便透過用於網際網路存取的代理伺服器對應用程式進行身分驗證。
3. 現在，您可以為 受信任的應用程式指定檔案雜湊，而不僅是完整路徑。
4. Endpoint Detection and Response (EDR) 解決方案使用者可以使用更多的 *IOC掃描* 工作功能。回顧 IOC 掃描功能現已可用。*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。此模式旨在偵測電腦網路活動資料中的入侵指標。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。
5. Kaspersky Endpoint Detection and Response (EDR) 的使用者可以移除 隔離區規模限制。這對於 YARA 掃描來說可能很有必要，因為該應用程式可能會保存大型記憶體傾印檔案。現在，您可以將所有可用磁碟空間用於隔離。

6. 現在支援 HTTPS 壓縮，以最佳化將事件匯出到 Kaspersky Unified Monitoring and Analysis Platform（KUMA）。這有助於減少傳出的流量。

7. 在開發此版本的 Kaspersky Endpoint Security for Windows 時，我們納入了以下專用修補程式中包含的變更：PF13115、PF13118、PF13119、PF13120、PF13123、PF13124、PF14061、PF14062、PF14064、PF14065、PF14069、PF14070、PF15054、PF15056、PF15058、PF15062、PF15063、PF15064、PF16052、PF16053、PF16055、PF16056、PF16057、PF16060、PF16061、PF16062、PF17027、PF17029、PF17039、PF17041、PF17043、PF17048、PF17050、PF17051、PF17053、PF17054、PF18010、PF18011、PF18014、PF18015、PF18020、PF18021、PF18022、PF18023、PF18024、PF18028、PF18031、PF18032、PF18043、PF18050、PF18051、PF18053、PF19003、PF19016、PF19018、PF19017、PF19032、PF19034、PF19036、PF19037、PF19041、PF19043、PF19049、PF19051 、PF19055、PF19056、PF20011、PF20016、PF20017、PF20020、PF20021、PF20033、PF20036、PF20038、PF20039、PF20049、PF20052、PF20055、PF20060、PF20065、PF21007、PF21010、PF21019、PF21021、PF21024、PF21026、PF22004、PF22008、PF22014。

## 更新 12.11

Kaspersky Endpoint Security 12.11 for Windows 提供了以下功能和改進：

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

2. 新增了對自動提交到 KATA Sandbox 的檔案進行審查的支援。*KATA Sandbox* 是 Kaspersky Anti Targeted Attack Platform 的元件，可在作業系統的虛擬映像上執行檔案。Sandbox 會分析物件行為以偵測惡意行動和組織的 IT 基礎架構上的針對性攻擊所特有的活動。Sandbox 會分析和掃描部署了 Microsoft Windows 作業系統的虛擬影像的特殊伺服器（Sandbox 伺服器）上的物件。若要讓 KATA Sandbox 在自動模式下運行，必須部署 Kaspersky Anti Targeted Attack Platform 8.0 或更高版本。

3. 最佳化了 EDR 遙測資料傳送。現在您可以指定最大封包長度。

4. 改進了與卡巴斯基安全網路的連線診斷功能。擴充了卡巴斯基安全網路的連線錯誤詳細資訊，以解決潛在問題。

5. 新增了對設定要傳送到 Kaspersky Unified Monitoring and Analysis Platform (KUMA) 的事件清單的支援。現在，除 KUMA 中的預定義事件清單外，您還可以手動將事件新增到遙測資料中，或依據其在 Windows 事件記錄中的 ID 排除事件。

6. 更新了網頁主控台中的政策介面。政策區域的佈局已經過變更，以便加快基本功能存取速度。

7. 支援 Windows 11 25H2。

8. 在開發此版本的 Kaspersky Endpoint Security for Windows 時，我們納入了以下專用修補程式中包含的變更：PF13115、PF13118、PF13119、PF13120、PF13123、PF13124、PF14061、PF14062、PF14064、PF14065、PF14069、PF14070、PF15054、PF15056、PF15058、PF15062、PF15063、PF15064、PF16052、PF16053、PF16055、PF16056、PF16057、PF16060、PF16061、PF16062、PF17027、PF17029、PF17039、PF17041、PF17043、PF17048、PF17050、PF17051、PF17053、PF17054、PF18010、PF18011、PF18014、PF18015、PF18020、PF18021、PF18022、PF18023、PF18024、PF18028、PF18031、PF18032、PF18043、PF18050、PF18051、PF18053、PF19003、PF19016、PF19018、PF19017、PF19032、PF19034、PF19036、PF19037、PF19041、PF19043、PF19049、PF19051 、PF19055、PF19056、PF20011、PF20016、PF20017、PF20020、PF20021、PF20033、PF20036、PF20038、PF20039、PF20049、PF20052、PF20055、PF20060、PF20065、PF21007、PF21010、PF21019、PF21021、PF21024、PF21026、PF22004、PF22008、PF22014。

更新 12.10

Kaspersky Endpoint Security 12.10 for Windows 提供了以下功能和改進：

1. 對於 BadUSB 攻擊防護元件，已新增透過從螢幕上讀取條碼來授權條碼掃描器的選項。現在您無需使用螢幕鍵盤輸入代碼來授權條碼掃描器。

2. Endpoint Detection and Response (EDR) 解決方案的使用者可以使用以下功能和改進：

   - 現在您可以在警示詳細資訊中管理電腦的網路隔離。此外，您可以在警示詳細資料中指定電腦網路隔離時間段和新增排除項目。

   - 使用新資料填寫警示詳細資訊。現在，警示詳細資訊包含有關威脅的更多資訊，包括應用程式在回應 EDR 威脅時的行為。

   - IOC 檔案處理得到了改進。現在，您可以在卡巴斯基安全管理中心網頁主控台介面中檢視和編輯 IOC 檔案的內容。載入 IOC 檔案後，應用程式將顯示有關 IOC 術語套用的報告。

   - 改進了對偵測到的 IOC 的回應。現在，您可以直接在工作屬性的 IOC偵測結果中隔離 *IOC掃描* 工作偵測到的檔案。您也可以在工作屬性中將電腦與網路隔離。

   - 現在您可以直接在 *IOC掃描* 工作中根據 TXT 檔案中產生的檔案雜湊、IP 位址或 DNS 名稱清單建立 IOC 檔案。

   - 擴大了 *IOC掃描* 工作的掃描範圍。現在，您可以為登錄檔的 IOC 掃描定義一個範圍（**Windows Registry – RegistryItem**）。在應用程式的早期版本中，您只能使用登錄檔中預先定義的 IOC 掃描範圍。

3. 新增了新的密碼防護權限，*匯出設定*。預設情況下，只有 KLAdmin 使用者可以在應用程式介面中使用 Kaspersky Endpoint Security 設定建立設定檔。要授予其他使用者存取權限，您需要授予他們相應的權限。

4. 在開發此版本的 Kaspersky Endpoint Security for Windows 時，我們納入了以下專用修補程式中包含的變更：PF12120、PF12121、PF12122、PF13115、PF13118、PF13119、PF13120、PF13123、PF14061、PF14062、PF14064、PF14065、PF15054、PF15056, PF15058、PF15062, PF16052、PF16053、PF16055、PF16056、PF16057, PF17027、PF17029、PF17039、PF17041、PF17043、PF17048、PF17050、PF18010、PF18011, PF18014, PF18015、PF18020、PF18021、PF18022、PF18023、PF18024、PF18028、PF18031、PF18032、PF18043、PF19003、PF19016、PF19018、PF19017、PF19032、PF19034、PF19036、PF19037, PF19041、PF19043、PF19049、PF20011、PF20016、PF20017、PF20020、PF20021、PF20033、PF20036、PF20038、PF20039、PF20049、PF21007。

## 更新 12.9

Kaspersky Endpoint Security 12.9 for Windows 提供了以下功能和改進：

1. 新增了*管理暫時密碼*的新功能 。暫時密碼可讓您為單獨的電腦提供啟用了密碼防護的 Kaspersky Endpoint Security 的存取權限。暫時密碼管理允許保存密碼歷史記錄（最多 30 天）、監控暫時密碼狀態（*啟動*，*已到期*，*已吊銷*）並撤銷暫時密碼。

2. 新增了在套用程式政策後立即終止與 Web 控制規則禁止的 Web 資源的連線的選項。在該應用程式的先前版本中，Web 控制僅限制與禁止的 Web 資源的新連線。

3. 對於 Kaspersky Anti Targeted Attack Platform 使用者，新增了在電腦上本機執行 YARA 檢查選項。為此，您需要下載一個包含 YARA 規則的檔案並在 CMD 中執行命令。

4. 修正了在磁碟機已使用第三方工具受 BitLocker 防護的電腦上啟用 BitLocker 時應用程式的行為。Kaspersky Endpoint Security 啟動還原程序，將還原金鑰傳送至卡巴斯基安全管理中心。因此，BitLocker 管理被轉移到卡巴斯基安全管理中心主控台。

5. 一個新的部分，**回應歷史**，可供卡巴斯基的 Detection and Response 解決方案的使用者使用。此部分包含有關在電腦上執行的威脅回應操作的資訊。例如，這些操作包括執行 *停止處理程序* 工作或將電腦與網路隔離。回應歷史記錄僅適用於以下卡巴斯基解決方案的使用者：MDR、EDR、KATA。

6. 對於卡巴斯基統一監控和分析平台使用者，現在可以使用支援 EDR 威脅回應操作。在應對威脅時，KUMA 會執行建立對應 EDR 工作的指令碼。若要執行 EDR 工作，您需要在 KUMA 主控台中為自訂指令碼建立回應規則並選擇事件。

7. 在開發此版本的 Kaspersky Endpoint Security for Windows 時，我們納入了以下專用修補程式中包含的變更：PF10360、PF10362、PF10363、PF12120、PF12121、PF12122、PF13115、PF13118、PF13119、PF14061、PF14062、PF14064、PF14065、PF15054、PF15056、PF15058、PF16052、PF16053、PF16055、PF16056、PF17027、PF17029、PF17039、PF17041、PF17043、PF18010、PF18011、PF18014、PF18015、PF18020、PF18021、PF18022、PF18023、PF18024、PF18028、PF19003、PF19016、PF19018、PF19017、PF19032、PF19034、PF19036、PF19037、PF19041、PF20011、PF20016、PF20017、PF20020、PF20021。

## 更新 12.8

Kaspersky Endpoint Security 12.8 for Windows 提供了以下功能和改進：

1. 該應用程式現在支援 用於防護虛擬環境的 Light Agent 模式。現在，您可以將該應用程式部署為 Light Agent，作為 Kaspersky Security for Virtualization Light Agent 6.2 解決方案的一部分。

2. 攔截伺服器上 Docker 容器中的檔案操作現在受支援。一個 *容器* 是一個隔離環境，應用程式可以在其中執行而無需直接與作業系統交互。Kaspersky Endpoint Security 掃描使用者有權存取的容器內的檔案。當偵測到威脅時，應用程式會封鎖該惡意活動並嘗試清除容器內的檔案。如果無法清除檔案，應用程式將停止容器。

3. 現在，您可以定義防護範圍，以防護共用資料夾免受外部加密（行為偵測元件）。現在，您可以指定應用程式必須監視其檔案活動的共用資料夾。您也可以將文件排除在防護範圍之外。在應用程式的先前版本中，行為偵測元件監視所有共用資料夾的檔案活動。

4. 現在，您可以在安裝套件中為不同類型的作業系統配置不同的元件集合。也就是說，您可以使用相同的安裝套件將應用程式部署到工作站和伺服器。對於某些作業系統類型不可用的元件會自動在安裝套件屬性中排除。

5. 可選擇的選項 預定義掃描排除項目和受信任應用程式 已新增。預定義掃描排除項目和受信任應用程式允許在虛擬環境（Citrix、VMware）中快速配置應用程式的受信任區域。此類排除項目包括（例如）VHD 和 VHDX 虛擬機檔案。當建立應用程式安裝套件、建立政策或安裝 Kaspersky Endpoint Security 時可以新增排除項目。

6. EDR 遙測現在包括使用 USB 連線裝置進行操作的事件。您也可以將這些事件新增至 EDR 遙測的排除項目中。

7. 封鎖透過過時的 TLS 1.0 協定建立網路連線的選項已新增。TLS 1.0 的安全等級較低，因此建議停用該協定並使用較新的 TLS 1.2 或 TLS 1.3 版本。預設情況下，Kaspersky Endpoint Security 封鎖 TLS 1.0 連線。更新應用程式版本後，使用 TLS 1.0 協定的協力廠商服務運行可能會失敗。為了避免協力廠商服務運行出現問題，您可以在更新應用程式版本之前 允許在群組政策中使用 TLS 1.0 協定。

8. 在開發此版本的 Kaspersky Endpoint Security for Windows 時，我们納入了以下專用修補程式中包含的變更：PF10053、PF10054、PF10360、PF10362、PF10363、PF12120、PF12121、PF12122、PF13115、PF13118、PF13119、PF14061、PF14062、PF14064、PF14065、PF15054、PF15056、PF15058、PF16052、PF16053、PF16055、PF16056、PF17027、PF17029、PF17039、PF17041、PF17043、PF18010、PF18011、PF18014、PF18015、PF18020、PF18021、PF18022、PF18023、PF18024、PF18028、PF19003、PF19016、PF19018。

## 更新 12.7

Kaspersky Endpoint Security 12.7 for Windows 提供了以下功能和改進：

1. 現在，您可以限制 *惡意軟體掃描* 工作的 CPU 資源使用。為此，在應用程式設定中，指定掃描電腦時可利用的所有核心的最大 CPU 負載百分比。

2. 現在您可以手動 傳送檔案以供在 KATA Sandbox 中掃描。*KATA Sandbox* 是 Kaspersky Anti Targeted Attack Platform 的元件，可在作業系統的虛擬映像上執行檔案。Sandbox 會分析物件行為以偵測惡意行動和組織的 IT 基礎架構上的針對性攻擊所特有的活動。Sandbox 會分析和掃描部署了 Microsoft Windows 作業系統的虛擬影像的特殊伺服器（Sandbox 伺服器）上的物件。若要將檔案傳送至 KATA Sandbox 進行掃描，請在檔案的上下文選單中選擇相關指令。

3. 現在您可以設定與防護企業 LAN 的解決方案 *Kaspersky Network Detection and Response* 的整合。Kaspersky Network Detection and Response (NDR) 是 Kaspersky Anti Targeted Attack Platform 的一部分。您可以在標準模式以及 EDR Agent 模式下配置與 NDR 的互動。

4. 在郵件威脅防護延伸程式中新增了對 Microsoft Office Outlook 電子郵件用戶端版本 2021 的支援。該延伸程式允許在郵件用戶端級別而不是協定級別掃描郵件。除了郵件之外，該延伸程式還允許您掃描透過 MAPI 接口從 Microsoft Exchange 儲存庫接收到的物件（例如，日曆中的物件）。此掃描在郵件用戶端中進行。

5. 在開發此版本的 Kaspersky Endpoint Security for Windows 時，我们納入了以下專用修補程式中包含的變更：PF10049、PF10355、PF12114、PF13109、PF14056、PF15038、PF15045、PF16037、PF16042、PF16047、PF17014、PF17018、PF17021、PF17024、PF18006、PF18007。

## 更新 12.6

Kaspersky Endpoint Security 12.6 for Windows 提供了以下功能和改進：

1. 與卡巴斯基 SIEM 解決方案整合的功能（*Kaspersky Unified Monitoring and Analysis Platform; KUMA*）已新增。現在可以將事件從 Windows 事件記錄傳送到 KUMA 收集器。這可讓 KUMA 從安裝了 Kaspersky Endpoint Security 的所有電腦接收 Windows 事件（支援一組有限的 EventID），而無需在這些電腦上安裝 KUMA 代理程式。

2. 新增了 *系統完整性監控* 元件來取代檔案完整性監控元件。系統完整性監控元件包括檔案完整性監控的所有功能，此外還允許監控登錄機碼變更和外部裝置的連線。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示。檔案完整性監控不再是應用程式的一部分。當您更新應用程式時，檔案完整性監控設定會自動遷移到系統完整性監控。為確保系統完整性監控正確運行，Kaspersky Endpoint Security 應用程式和管理外掛程式都應被更新至版本 12.6。

3. 已安裝的內建 EDR Agent (KATA) 的狀態已新增至卡巴斯基安全管理中心主控台的電腦內容中。現在，如果您安裝了內建 EDR Agent (KATA)，**Endpoint Sensor 狀態**列將顯示元件的目前狀態（例如，*正在執行*、*已停止*、*不受產品許可支援*，等等）。

4. 可選擇的選項 預定義掃描排除項目和受信任應用程式 已新增。預定義掃描排除項目和受信任應用程式有助於在 SQL 伺服器、Microsoft Exchange 伺服器和 System Center Configuration Manager 上使用應用程式時快速設定受信任區域。此類排除項目包括（例如）MDF 和 LDF 資料庫檔案。建立新政策、修改現有政策或安裝 Kaspersky Endpoint Security 時可以新增排除項目。

5. Kaspersky Endpoint Detection and Response Optimum 的警示詳細資訊顯示已被從 Kaspersky Endpoint Security 管理外掛程式移至單獨的 Kaspersky Endpoint Detection and Response 管理外掛程式。EDR 管理外掛程式是一個單一外掛程式，可與 Windows、Mac 和 Linux 作業系統上的代理程式一起使用。現在，當使用 EDR Optimum 時，您將需要 Kaspersky Endpoint Security 管理外掛程式來建立威脅回應工作，並需要 EDR 管理外掛程式來檢視警示詳細資訊。

6. 支援 Windows 11 24H2。

7. 在開發此版本的 Kaspersky Endpoint Security for Windows 時，我们納入了以下專用修補程式中包含的變更：pf10048、pf10353、pf12106、pf12107、pf12108、pf13090、pf13100、pf15031、pf15034、pf15036、pf16021、pf16023、pf16029、pf17002。

## 更新 12.5

Kaspersky Endpoint Security 12.5 for Windows 提供了以下功能和改進：

1. 新增了配置遙測排除項目的選項。*遙測*是受防護電腦上發生的事件的清單。遙測資料由 Kaspersky Anti Targeted Attack Platform (EDR) 用來監控和防護組織的 IT 基礎結構。配置遙測排除項目有助於提高電腦效能並最佳化到遙測資料收集伺服器的資料傳輸。

2. 應用程式信任區域的介面已得到改進。如果管理員禁止使用者新增自己的（本機）掃描排除項目和可信應用程式，Kaspersky Endpoint Security 現在會對使用者隱藏可信區域物件。這可以防止入侵者對受信任區域進行未經授權的存取，從而提高電腦安全等級。

3. 新增了掃描 MyOffice Mail 和 R7-Office Organizer 郵件用戶端流量的選項。郵件威脅防護元件現在不僅掃描下載時的郵件附件，而且掃描傳送和接收的郵件。

4. 網路資源的新類別 *生成式人工智能工具* 已新增。您可以使用 Web 控制配置對新類別網站的存取。

5. 現在您可以在防火牆清單中選擇網路封包規則的位置。網路封包規則在清單中的位置決定其優先順序。在該應用程式的早期版本中，新規則只能新增到清單末尾，之後您必須在清單中手動移動規則以確定其優先順序。現在，新增規則時，您可以選擇是否將該規則放置在清單的開頭、末尾或所選規則的旁邊。

6. 在 Kaspersky Endpoint Security 元件的規則中，您現在不僅可以從 Active Directory 選擇使用者，还可以從卡巴斯基安全管理中心的使用者清單中選擇使用者。您還可以手動輸入本機使用者帳戶資料。已為以下元件的規則新增了這種可能性：應用程式控制、裝置控制、Web 控制、適應性異常控制和記錄檢查。

7. 網路攻擊偵測報告現在包含一個列，其中包含攻擊電腦的 MAC 位址（網路威脅防護元件）。現在，除了攻擊電腦的 IP 位址之外，您還可以在報告中看到其 MAC 位址。這對於事件調查很有幫助。包含攻擊電腦 MAC 位址的報告也將在卡巴斯基安全管理中心 Linux 主控台版本 15.1 及更高版本中提供。

8. 電腦防護等級要求得到了提高。高防護等級現在需要啟用防護應用程式服務抵禦外部管理。在政策視窗的上部檢查安全等級指示器。如果您的安全等級為中低，您可以在安全等級指示器建議視窗中啟用防護應用程式服務抵禦外部管理。

9. 已新增當應用程式在Endpoint Detection and Response Agent (EDR Agent) 配置中執行時的物件偵測新事件支援。這些事件已在 [KES+內建代理] 配置中受支援。

10. 在開發此版本的 Kaspersky Endpoint Security for Windows 時，我们納入了以下專用修補程式中包含的變更：pf9640、pf9830、pf9831、pf10047、pf10351、pf12102、pf12105、pf13084、pf13089、pf14040、pf14047、pf15026、pf15028、pf16013。

## 更新 12.4

Kaspersky Endpoint Security 12.4 for Windows 提供了以下功能和改進：

1. 新增了新功能以防護電腦到卡巴斯基安全管理中心的連線。新的"*管理伺服器連線防護*"工作允許設定用於連線到受信任伺服器的密碼。這意味著沒有此密碼則無法重新連線電腦和執行來自另一台伺服器的指令。

2. 對於密碼防護元件，新增了不只從 Active Directory 選擇使用者的能力。即，您可以手動指定使用者名稱和密碼並為此帳戶指派存取權限給 Kaspersky Endpoint Security。這樣，您就無需與其他使用者共用您的 KLAdmin 密碼或建立新的 Active Directory 帳戶以控制對應用程式的存取。

3. 支援 Windows 11 23H2。

## 更新 12.3

Kaspersky Endpoint Security 12.3 for Windows 提供了以下功能和改進：

1. 現在您可以將應用程式安裝在 Endpoint Detection and Response Agent 配置中。此配置可讓人安裝具有卡巴斯基 Detection and Response 解決方案要求的元件集合的應用程式：Kaspersky Managed Detection and Response 和 Kaspersky Anti Targeted Attack Platform (EDR)。您可以在此配置中與協力廠商解決方案（例如 Dr.Web、Dallas Lock、ESET）一起安裝應用程式。這使您可以將協力廠商基礎結構安全工具與卡巴斯基的 Detection and Response 一起使用。

2. Kaspersky Endpoint Security 對藍牙裝置的操作得到了改進。現在，您可以配置排除項目並限制對除輸入裝置（無線鍵盤、滑鼠等）之外的所有藍牙裝置的存取。

3. 應用程式控制元件對可執行檔的資料庫的操作得到了最佳化。現在，如果某個檔案被從電腦中刪除，Kaspersky Endpoint Security 可以從資料庫中自動刪除該檔案。這可以使資料庫保持最新並節省卡巴斯基安全管理中心資源。

4. 電腦防護等級要求得到了提高。現在高防護等級要求啟用密碼防護。在政策視窗的上部檢查防護等級指示器。如果防護等級為中或低，您可以在安全等級指示器建議視窗中啟用密碼防護。

5. 新增了 HTTPS 協定支援以使應用程式能夠與卡巴斯基安全網路一起使用。在 KSN 代理伺服器設定中的管理伺服器屬性中啟用 HTTPS 使用。

## 更新 12.2

Kaspersky Endpoint Security 12.2 for Windows 提供了以下功能和改進：

1. 向控制與 Wi-Fi 網路的連線新增了 WPA3 協定支援。現在您可以在受信任的 Wi-Fi 網路設定中選擇 WPA3 協定，並拒絕連線到使用不太安全的協定的網路。

2. 現在您可以為網路威脅防護排除項目選擇協定和連接埠。現在除了指定受信任裝置的 IP 位址外，您還可以選擇連接埠和協定。這使您可以排除個別資料流並防止來自受信任 IP 位址的網路攻擊。

3. 如果政策被套用於電腦，本機*資料庫和應用程式模組更新 task*的不同更新來源順序。卡巴斯基安全管理中心伺服器，而不是卡巴斯基伺服器，現在被預設用作第一個更新來源。這有助於在使用者執行本機*資料庫和應用程式模組更新*工作時節省流量。

## 更新 12.1

Kaspersky Endpoint Security 12.1 for Windows 提供了以下功能和改進：

1. 新增了 Kaspersky Anti Targeted Attack Platform 解決方案的內建代理。您不再需要 Kaspersky Endpoint Agent 來使用 EDR (KATA)。Kaspersky Endpoint Agent 的所有功能將由 Kaspersky Endpoint Security 執行。若要遷移 Kaspersky Endpoint Agent 政策，請使用遷移精靈。更新應用程式後，Kaspersky Endpoint Security 將切換到使用內建代理並刪除 Kaspersky Endpoint Agent。Kaspersky Endpoint Agent 已新增至不相容的軟體清單中。Kaspersky Endpoint Security 具有適用於所有 Detection and Response 解決方案的內建代理，因此不再需要安裝 Kaspersky Endpoint Agent 來與這些解決方案整合。

2. 現在支援 Azure WVD 相容模式。此功能可確保在 Kaspersky Anti Targeted Attack Platform 主控台中正確顯示 Azure 虛擬機狀態。Azure WVD 相容模式允許為這些虛擬機分配永久唯一的感應器 ID。

3. 現在，您可以在 iTunes 或類似應用程式中設定行動裝置的使用者存取權限。例如，您可以允許行動裝置只在 iTunes 中使用並阻止將行動裝置作為卸除式磁碟機使用。該應用程式還支援 Android 偵錯橋接器 (ADB) 應用程式的這些規則。

4. 不再支援卡巴斯基安全管理中心版本 11。將卡巴斯基安全管理中心升級到最新版本。

## 更新 12.0

Kaspersky Endpoint Security 12.0 for Windows 提供了以下功能和改進：

1. Kaspersky Endpoint Security 在伺服器上的操作得到了改進。現在您可以從 Kaspersky Security for Windows Server 遷移到 Kaspersky Endpoint Security for Windows，並使用單一解決方案來防護工作站和伺服器。若要遷移應用程式設定，請執行政策和工作批轉換精靈。KSWS 產品授權金鑰可用於啟動 KES。遷移到 KES 後，您甚至不需要重新啟動伺服器。有關遷移到 KES 的更多資訊，請參閱遷移指南。

2. 屬於 Amazon Machine Image (AMI) 中付費虛擬機映像的應用程式的許可得到了改進。無需單獨啟動應用程式。在這種情況下，卡巴斯基安全管理中心使用已新增到應用程式的雲端環境的產品授權金鑰。

3. 裝置控制得到了改進：

   - 對於攜帶式裝置 (MTP)，您可以設定存取規則（閱讀/寫入），選擇具有裝置存取權限的使用者或者使用者群組，或者設定裝置存取排程。現在，您可以用和針對卸除式磁碟機一樣的方式建立攜帶式裝置存取規則。
   - 現在，您可以在 Android Debug Bridge (ADB) 或類似應用程式中設定行動裝置的使用者存取權限。例如，您可以允許行動裝置只在 ADB 中使用並阻止將行動裝置作為卸除式磁碟機使用。
   - 現在，即使行動裝置存取被封鎖，您也可以透過將行動裝置連線到電腦的 USB 連接埠來為其充電。
   - 對於印表機，您現在可以為使用者設定列印權限。Kaspersky Endpoint Security 支援控制對本機和網路印表機的存取。現在，您可以允許或者阻止單個使用者在本機或者網路印表機上列印。
   - 新增了 WPA3 協定支援以控制與 Wi-Fi 網路的連線。現在您可以在受信任的 Wi-Fi 網路設定中選擇使用 WPA3 協定，並拒絕連線到使用不太安全的協定的網路。

## 更新 11.11.0

1. 已新增的伺服器的記錄檢查元件。記錄檢查會基於 Windows 事件記錄分析結果監控受防護環境的完整性。如果應用程式在系統中偵測到有非典型行為的跡象，它會通知管理員，因為該行為可能表明有人嘗試網路攻擊。

2. 已新增伺服器的檔案完整性監控元件。檔案完整性監控會偵測給定監控區域中的物件（檔案和資料夾）變更。這些變更可能表明有電腦安全入侵。當偵測到物件變更時，應用程式會通知管理員。

3. Kaspersky Endpoint Detection and Response Optimum (EDR Optimum) 的警示詳細資訊介面得到了改進。威脅發展鏈的元素得到了統一，鏈條中程序之間的連接不再重疊。這使得分析威脅的演化更容易。

4. 改進了應用程式效能。為此目的，網路威脅防護元件的網路流量處理得到了最佳化。

5. 新增了"升級 Kaspersky Endpoint Security 而無需重新啟動"的選項。這可讓您確保升級應用程式時伺服器的作業不中斷。從版本 11.10.0 開始您可以升級應用程式而無需重新啟動。從版本 11.11.0 開始您可以安裝修補程式而無需重新啟動。

6. "*病毒掃描*"工作在卡巴斯基安全管理中心主控台中進行了重命名。該工作現在稱為"*惡意軟體掃描*"。

## 更新 11.10.0

Kaspersky Endpoint Security 11.10.0 for Windows 提供了以下功能和改進：

1. 新增了對使用卡巴斯基完整磁碟加密進行單點登入的協力廠商憑據提供者的支援。Kaspersky Endpoint Security 監控 ADSelfService Plus 的使用者密碼並在使用者變更密碼（例如）時更新身分驗證代理的資料。

2. 新增了啟用顯示 Cloud Sandbox 技術偵測到的威脅的選項。這項技術對 Endpoint Detection and Response 解決方案（EDR Optimum 或 EDR Expert）的使用者可用。*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識別惡意活動和決定其信譽。

3. 向 EDR Optimum 使用者的警示詳情新增了有關檔案的其它資訊。警示詳情現在包括有關信任群組、數位簽名和檔案發佈的資訊，以及其它資訊。您也可以從警示詳情直接跳到 Kaspersky Threat Intelligence Portal (KL TIP) 上的詳細檔案描述。

4. 改進了應用程式效能。為此，我們最佳化了背景掃描操作並新增了如果掃描已經在執行時佇列掃描工作的能力。

## 更新 11.9.0

Kaspersky Endpoint Security 11.9.0 for Windows 提供了以下功能和改進：

1. 現在，您可以在使用卡巴斯基磁碟加密時建立一個身分驗證代理服務帳戶。獲取電腦的存取權限時（例如，當使用者忘記密碼時）需要該服務帳戶。您也可以將服務帳戶作為備用帳戶。

2. Kaspersky Endpoint Agent 分發套件不再是應用程式分發套件的一部分。若要支援 Detection and Response 解決方案，您可以使用 Kaspersky Endpoint Security 內建代理。必要的話，您可以從 Kaspersky Anti Targeted Attack Platform 分發套件下載 Kaspersky Endpoint Agent 分發套件。

3. Kaspersky Endpoint Detection and Response Optimum (EDR Optimum) 的警示詳細資訊介面得到了改進。威脅響應功能現在具有工具提示。當偵測到洩露指示時，系統還會顯示確保公司基礎結構安全的逐步操作指示。

4. 現在，您可以用 Kaspersky Hybrid Cloud Security 產品授權金鑰啟動 Kaspersky Endpoint Security for Windows。

5. 新增了關於與憑證不受信任的網域建立連線和加密連線掃描錯誤的新事件。

## 更新 11.8.0

Kaspersky Endpoint Security 11.8.0 for Windows 提供了以下功能和改進：

1. 新增了內建代理以支援 Kaspersky Endpoint Detection and Response Expert 解決方案的操作。*Kaspersky Endpoint Detection and Response Expert* 是用於防護公司 IT 基礎結構抵禦進階網路威脅的解決方案。該解決方案的功能結合了自動偵測威脅和回應這些威脅的能力，以抵消包括新漏洞、勒索軟體、無檔案攻擊以及使用合法系統工具的方法。EDR Expert 比 EDR Optimum 提供更多的威脅監控和回應功能。有關解決方案的更多資訊，請參見Kaspersky Endpoint Detection and Response Expert 說明。

2. 網路監控介面現已改進。除了 TCP 之外，網路監控現在還顯示 UDP 通訊協定。

3. *病毒掃描*工作得到了改進。如果您在掃描期間重新啟動了電腦，Kaspersky Endpoint Security 將自動執行工作，從掃描被中斷的地方繼續。

4. 現在您可以設定工作執行時間限制。您可以限制*病毒掃描*和*IOC 掃描*工作的執行時間。超出指定時間後，Kaspersky Endpoint Security 將停止工作。例如，為了減少*病毒掃描*工作執行時間，您可以配置掃描範圍或者最佳化掃描。

5. 為 Windows 10 Enterprise 多工作階段上安裝的應用程式解除了伺服器平台的限制。Kaspersky Endpoint Security 限制將 Windows 10 Enterprise 多工作階段視為工作站作業系統而不是伺服器作業系統。相應的，伺服器平台限制不再套用於 Windows 10 Enterprise 多工作階段上的應用程式。此外，應用程式使用工作站產品授權金鑰進行啟動，而不是伺服器產品授權金鑰。

## 更新 11.7.0

Kaspersky Endpoint Security for Windows 11.7.0 提供以下新功能和改進：

1. Kaspersky Endpoint Security for Windows 介面得到更新。

2. 支援 Windows 11、Windows 10 21H2 和 Windows Server 2022。

3. 新增了新元件：

   - 已新增用於和 Kaspersky Sandbox 進行整合的內建代理。*Kaspersky Sandbox 解決方案*可偵測和自動封鎖電腦上的進階威脅。Kaspersky Sandbox 會分析物件行為以偵測惡意行動和組織的 IT 基礎結構上的針對性攻擊所特有的活動。Kaspersky Sandbox 會分析和掃描部署了 Microsoft Windows 作業系統的虛擬映像的特殊伺服器（Kaspersky Sandbox 伺服器）上的物件。有關解決方案的詳情，請參閱 Kaspersky Sandbox 說明。

     您不再需要 Kaspersky Endpoint Agent 來使用 Kaspersky Sandbox。Kaspersky Endpoint Agent 的所有功能將由 Kaspersky Endpoint Security 執行。若要遷移 Kaspersky Endpoint Agent 政策，請使用遷移精靈。您需要卡巴斯基安全管理中心 13.2 以便 Kaspersky Sandbox 的所有功能工作。若要瞭解從 Kaspersky Endpoint Agent 遷移到 Kaspersky Endpoint Security for Windows 的詳細資訊，請參閱“應用程式說明”。

   - 新增了內建代理以支援 Kaspersky Endpoint Detection and Response Optimum 解決方案的操作。*Kaspersky Endpoint Detection and Response Optimum* 是用於防護組織的 IT 基礎結構抵禦進階網路威脅的解決方案。該解決方案的功能結合了自動偵測威脅和回應這些威脅的能力，以抵消包括新漏洞、勒索軟體、無檔案攻擊以及使用合法系統工具的方法。有關解決方案的更多資訊，請參見Kaspersky Endpoint Detection and Response Optimum 說明。

     您不再需要 Kaspersky Endpoint Agent 來使用 Kaspersky Endpoint Detection and Response。Kaspersky Endpoint Agent 的所有功能將由 Kaspersky Endpoint Security 執行。若要遷移 Kaspersky Endpoint Agent 政策和工作，請使用遷移精靈。若要使用所有功能，Kaspersky Endpoint Detection and Response Optimum 需要卡巴斯基安全管理中心 13.2。若要瞭解從 Kaspersky Endpoint Agent 遷移到 Kaspersky Endpoint Security for Windows 的詳細資訊，請參閱“應用程式說明”。

4. 以新增適用於 Kaspersky Endpoint Agent 政策和工作的遷移精靈。遷移精靈將為 Kaspersky Endpoint Security for Windows 建立新的合併政策和工作。該精靈可允許 Detection and Response 解決方案從 Kaspersky Endpoint Agent 轉換到 Kaspersky Endpoint Security。Detection and Response 解決方案包括 Kaspersky Sandbox、 Kaspersky Endpoint Detection and Response Optimum (EDR Optimum)、和 Kaspersky Managed Detection and Response (MDR)。

5. 分發套件中包含的 Kaspersky Endpoint Agent 已更新至版本 3.11。

   當升級 Kaspersky Endpoint Security 時，應用程式會偵測版本和指定 Kaspersky Endpoint Agent 的目的。如果 Kaspersky Endpoint Agent 被指定用於操作 Kaspersky Sandbox、Kaspersky Managed Detection and Response (MDR) 和 Kaspersky Endpoint Detection and Response Optimum (EDR Optimum)，Kaspersky Endpoint Security 將把這些解決方案的操作轉換到應用程式的內建代理。對於 Kaspersky Sandbox 和 EDR Optimum，應用程式會自動解除安裝 Kaspersky Endpoint Agent。對於 MDR，您可以手動解除安裝 Kaspersky Endpoint Agent。如果 Kaspersky Endpoint Agent 被指定用於操作 Kaspersky Endpoint Detection and Response Expert (EDR Expert)，Kaspersky Endpoint Security 將升級 Kaspersky Endpoint Agent 的版本。有關該應用程式的更多詳細資訊，請參閱支援 Kaspersky Endpoint Agent 的 Kaspersky 解決方案的文件。

6. BitLocker 加密功能得到改進：

   - 增強 PIN 現在可以和"BitLocker 磁碟機加密"使用。*增強 PIN* 允許使用除了數字字元的其它字元：大寫和小寫拉丁字母，特殊字元，和空格。

   - 新增了停用用於升級作業系統或者安裝更新套件的 BitLocker 身分驗證的功能。安裝更新可能需要多次重啟電腦。為了正確安裝更新，您可以暫時關閉 BitLocker 身分驗證並在安裝更新後重新啟用身分驗證。

   - 現在您可以為 BitLocker 加密密碼或者 PIN 設定一個到期時間。當密碼或者 PIN 到期時，Kaspersky Endpoint Security 會提示使用者設定新密碼。

7. 現在您可以設定 BadUSB 攻擊防護的鍵盤授權嘗試最大數量。當達到設定的授權碼輸入失敗嘗試數量時，USB 裝置會被暫時鎖定。

8. 防火牆功能得到改進：

   - 現在您可以設定一個用於防火牆封包規則的 IP 位址範圍。您可以輸入 IPv4 或者 IPv6 格式的位址範圍。例如，`192.168.1.1-192.168.1.100` 或 `12:34::2-12:34::99`。

   - 現在您可以為防火牆封包規則輸入 DNS 名稱而不是 IP 位址。您應該將 DNS 名稱僅用於 LAN 電腦後者內部服務。與雲端服務（例如 Microsoft Azure）和其他網際網路資源的交互應該由 Web 控制元件進行處理。

9. Web 控制規則搜尋得到改進。若要搜尋網頁資源存取規則，除了規則名稱外，您可以使用網站的 URL、使用者名稱、內容類別、或者資料類型。

10. *病毒掃描*工作得到了改進：

    - 空閒模式中的*病毒掃描*工作得到了改進。如果您在掃描期間重新啟動了電腦，Kaspersky Endpoint Security 將自動執行工作，從掃描被中斷的地方繼續。

    - *病毒掃描*工作得到了最佳化。預設 Kaspersky Endpoint Security 只在電腦空閒時執行掃描。您可以在工作內容中設定何時執行電腦掃描。

11. 現在您可以限制對應用程式活動監控提供的資料的使用者存取權限。*應用程式活動監控*是一個用於即時檢視使用者電腦上的應用程式活動資訊的工具。管理員可以在應用程式政策內容中向使用者隱藏應用程式活動監控。

12. 改進了透過 REST API 管理應用程式的安全性。現在 Kaspersky Endpoint Security 可驗證透過 REST API 傳送的要求的簽章。若要管理程序，您需要安裝請求識別憑證。

## 更新 11.6.0

Kaspersky Endpoint Security 11.6.0 for Windows 提供了以下功能和改進：

1. 支援 Windows 10 21H1。有關對 Microsoft Windows 10 作業系統的支援的詳細資訊，請參閱技術支援知識庫。

2. Managed Detection and Response 元件已新增。該元件有助於與稱為 Kaspersky Managed Detection and Response 的解決方案進行交互。Kaspersky Managed Detection and Response（MDR）提供全天候的防護，以免受越來越多的威脅侵害，這些威脅能夠繞過一些組織的自動防護機制，這些組織難以找到高素質專家或內部資源有限。如欲瞭解該解決方案如何工作的詳細資訊，請參閱 Kaspersky Managed Detection and Response 說明。

3. 分發套件中包含的 Kaspersky Endpoint Agent 已更新至版本 3.10。Kaspersky Endpoint Agent 3.10 提供了新功能，解決了一些以前的問題，並提高了穩定性。有關該應用程式的更多詳細資訊，請參閱支援 Kaspersky Endpoint Agent 的 Kaspersky 解決方案的文件。

4. 現在，它在"網路威脅防護設定"中提供的功能可管理防護以抵禦諸如網路泛洪和連接埠掃描之類的攻擊。

5. 新增了為防火牆建立網路規則的新方法。您可以為"網路監控"視窗中顯示的連線新增"封包規則"和"應用程式規則"。但是，網路規則連線設定將自動配置。

6. 網路監控介面現已改進。新增了有關網路活動的資訊：處理程序 ID，用於啟動網路活動；網路類型（本機網路或網際網路）；本機連接埠。預設隱藏有關網路類型的資訊。

7. 現在，可以為新的 Windows 使用者自動建立身分驗證代理帳戶。該代理允許使用者完成身分驗證，以存取使用卡巴斯基磁碟加密技術加密的磁碟機，並加載作業系統。該應用程式可檢查有關電腦上 Windows 使用者帳戶的資訊。如果 Kaspersky Endpoint Security 偵測到沒有身分驗證代理帳戶的 Windows 使用者帳戶，則應用程式將建立一個新帳戶來存取加密的磁碟機。這意味著您不需要為具有已加密磁碟機的電腦手動新增身分驗證代理帳戶。

8. 現在可以監視使用者電腦上的應用程式介面中的磁碟加密處理程序（卡巴斯基磁碟加密和 BitLocker）。您可以從"主應用程式視窗"執行加密監控工具。

## 更新 11.5.0

Kaspersky Endpoint Security 11.5.0 for Windows 提供了以下功能和改進：

1. 支援 Windows 10 20H2。有關對 Microsoft Windows 10 作業系統的支援的詳細資訊，請參閱技術支援知識庫。

2. 更新的應用程式介面。還更新了通知區域、應用程式通知和對話框中的應用程式圖示。

3. 改進了用於應用程式控制、裝置控制和適應性異常控制元件的 Kaspersky Endpoint Security 網頁外掛程式的介面。

4. 新增了以 XML 格式匯入和匯出規則和排除項目清單的功能。XML 格式允許您在清單匯出後對其進行編輯。您只能在卡巴斯基安全管理中心主控台中管理清單。以下清單可用於匯出/匯入：

   - 行為偵測（排除項目清單）。
   - Web 威脅防護（受信任的網址清單）。
   - 郵件威脅防護（附件篩選延伸程式清單）。
   - 網路威脅防護（排除項目清單）。
   - 防火牆（網路封包規則清單）。
   - 應用程式控制（規則清單）。
   - Web 控制（規則清單）。
   - 網路連接埠監控（Kaspersky Endpoint Security 監控的連接埠和應用程式清單）。

- 卡巴斯基磁碟加密（排除項目清單）。
- 卸除式磁碟機加密（規則清單）。

5. 物件 MD5 資訊已新增到威脅偵測報告中。在應用程式的早期版本中，Kaspersky Endpoint Security 僅顯示物件的 SHA256。

6. 在"裝置控制"設定中新增了為裝置存取規則分配優先順序的功能。優先順序分配可讓使用者對裝置存取的設定更加靈活。如果已將使用者新增到多個群組，則 Kaspersky Endpoint Security 會根據具有最高優先順序的規則來管理裝置存取。例如，您可以向 Everyone 群組授予只讀權限，向管理員群組授予讀/寫權限。為此，請為管理員群組分配優先順序 0，為 Everyone 群組分配優先順序 1。您只能為具有檔案系統的裝置配置優先順序。這包括硬碟磁碟機、卸除式磁碟機、軟碟、CD / DVD 磁碟機和可攜式裝置（MTP）。

7. 新增了新功能：
   - 管理音頻通知。
   - 如果網際網路連線受到限制（例如，透過行動連線），則網路數據流量控制 Kaspersky Endpoint Security 會限制其自身的網路流量。
   - 透過受信任的遠端管理應用程式（例如 TeamViewer、LogMeIn Pro 和 Remotely Anywhere）來管理 Kaspersky Endpoint Security 設定。您可以使用遠端管理應用程式來啟動 Kaspersky Endpoint Security 並在應用程式介面中管理設定。
   - 管理在 Firefox 和 Thunderbird 中的安全流量掃描設定。您可以選擇 Mozilla 將使用的憑證儲存：Windows 憑證儲存或 Mozilla 憑證儲存。此功能僅適用於沒有套用政策的電腦。如果將政策套用於電腦，Kaspersky Endpoint Security 會自動啟用在 Firefox 和 Thunderbird 中使用 Windows 憑證儲存。

8. 新增了配置安全流量掃描模式的功能：即使停用防護元件也始終掃描流量，或者在防護元件請求時掃描流量。

9. 修改了從報告中刪除資訊的處理程序。使用者只能刪除所有報告。在應用程式的先前版本中，使用者可以選擇特定的應用程式元件，這些元件的資訊將被從報告中刪除。

10. 修改了用於匯入包含 Kaspersky Endpoint Security 設定的設定檔的處理程序，以及修改了用於還原應用程式設定的處理程序。匯入或還原之前，Kaspersky Endpoint Security 僅顯示警告。在該應用程式的早期版本中，您可以在套用新設定之前檢視它們的值。

11. 簡化恢復對由 BitLocker 加密的磁碟機存取的程序。完成存取恢復程序後，Kaspersky Endpoint Security 會提示使用者設定新密碼或 PIN 代碼。設定新密碼後，BitLocker 將加密磁碟機。在應用程式的早期版本中，使用者必須在 BitLocker 設定中手動重置密碼。

12. 使用者現在可以為特定電腦建立自己的本機受信任區域。這樣，除了政策中的一般受信任區域之外，使用者還可以建立自己的"排除項目"和"受信任應用程式"的本機清單。管理員可以允許或封鎖使用本機排除項目或本機受信任的應用程式。管理員可以使用卡巴斯基安全管理中心檢視、新增、編輯或刪除電腦屬性中的清單項目。

13. 新增了在受信任應用程式的屬性中輸入註解的功能。註解有助於簡化對受信任應用程式的搜尋和排序。

14. 透過 REST API 管理應用程式：
   - 現在可以配置 Outlook 的郵件威脅防護延伸程式的設定。
   - 禁止停用病毒、蠕蟲和特洛伊木馬偵測。

## 更新 11.4.0

Kaspersky Endpoint Security 11.4.0 for Windows 提供了以下功能和改進：

1. 全新設計的工作列通知區域中的程式圖示。現在將顯示全新的 圖示，以取代原來的 圖示。如果需要使用者執行操作（例如，在更新應用程式後重新啟動電腦），則圖示將變更為 。如果應用程式的防護元件被停用或發生故障，則圖示將變更為 或 。如果將滑鼠懸停在該圖示上方，Kaspersky Endpoint Security 將顯示有關電腦防護問題的敘述。

2. 分發套件中包含的 Kaspersky Endpoint Agent 已更新至版本 3.9。Kaspersky Endpoint Agent 3.9 支援與新的卡巴斯基解決方案整合。有關該應用程式的更多詳細資訊，請參閱支援 Kaspersky Endpoint Agent 的 Kaspersky 解決方案的文件。

3. 為 Kaspersky Endpoint Security 元件新增了"*產品授權不支援*"狀態。您可以在"主應用程式視窗"中的元件清單中檢視元件的狀態。

4. 來自弱點利用防禦的新事件已新增到報告中。

5. 現在，在啟動磁碟機加密時，會自動將卡巴斯基磁碟加密技術的驅動程式新增到 Windows 還原環境 (WinRE) 中。安裝該應用程式時，會向 Kaspersky Endpoint Security 的早期版本新增驅動程式。在受到卡巴斯基磁碟加密技術防護的電腦上還原作業系統時，向 WinRE 新增驅動程式可以提高應用程式的穩定性。

Endpoint Sensor 元件已從 Kaspersky Endpoint Security 中刪除。如果電腦上已安裝 Kaspersky Endpoint Security 版本 11.0.0 至 11.3.0，您仍然可以在政策中設定 Endpoint Sensor 設定。

# 常見問題


### 一般

Kaspersky Endpoint Security 可以在哪些電腦上執行？
自上個版本以來有哪些變更？
Kaspersky Endpoint Security 可以與其他哪些 Kaspersky 應用程式一起執行？
如何在 Kaspersky Endpoint Security 執行期間節省電腦資源？

### 佈署

如何將 Kaspersky Endpoint Security 安裝到組織的所有電腦上？
哪些安裝設定可以在命令列中配置？
如何遠端移除 Kaspersky Endpoint Security？

### 更新

有哪些方法可以更新資料庫？
如果更新後出現問題應該怎麼辦？
如何更新公司網路外部的資料庫？
是否能使用代理伺服器進行更新？

### 安全

Kaspersky Endpoint Security 如何掃描電子郵件？
如何從掃描中排除受信任的檔案？
如何防護電腦免受快閃記憶體磁碟機中的病毒的侵害？
如何執行對使用者隱藏的惡意軟體掃描？
如何暫時暫停 Kaspersky Endpoint Security 的防護？
如何還原 Kaspersky Endpoint Security 錯誤刪除的檔案？
如何防護 Kaspersky Endpoint Security 不被使用者移除？

### 網際網路

Kaspersky Endpoint Security 是否掃描加密連線 (HTTPS)？
如何允許使用者只連線到受信任的 Wi-Fi 網路？
如何封鎖社群網路？

### 應用程式

如何找出使用者電腦上安裝了哪些應用程式（資產）？
如何防止執行電腦遊戲？
如何驗證"應用程式控制"是否已正確配置？
如何將應用程式新增到受信任清單？

### 裝置

如何封鎖使用快閃記憶體磁碟機？
如何將裝置新增至受信任清單？
是否能獲取對封鎖的裝置的存取權限？

### 加密

在哪些條件下無法進行加密？
如何使用密碼限制對壓縮檔案的存取？
是否能使用加密的智慧卡和權杖？
如果未與卡巴斯基安全管理中心連線，是否能存取加密資料？
如果電腦作業系統出現故障但資料仍然加密，應該怎麼辦？

### 支援

報告檔案儲存在何處？
如何建立偵錯檔案？
如何啟用傾印寫入？

# Kaspersky Endpoint Security for Windows

Kaspersky Endpoint Security for Windows（以下簡稱 Kaspersky Endpoint Security）為電腦提供全面防護，封鎖各種類型的威脅、網路攻擊和釣魚攻擊。

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

## 威脅偵測技術



**機器 學習**

Kaspersky Endpoint Security 使用基於機器學習的模型。該模型由 Kaspersky 專家開發。隨後，模型被不斷灌輸以 KSN 的威脅資料（模型訓練）。



**雲端 分析**

Kaspersky Endpoint Security 接收來自卡巴斯基安全網路的威脅資料。*卡巴斯基安全網路（KSN）*是雲端服務的基礎結構，可提供對線上卡巴斯基知識庫的存取，該知識庫包含有關檔案、網頁資源和軟體信譽的資訊。



**專家分析**

Kaspersky Endpoint Security 使用 Kaspersky 病毒分析師新增的威脅資料。如果物件的信譽無法自動確定，則病毒分析師將評估物件。



**行為 分析**

Kaspersky Endpoint Security 會及時分析物件的活動。



**自動 分析**

Kaspersky Endpoint Security 接收來自物件自動分析系統的資料。系統處理傳送到 Kaspersky 的所有物件。系統然後確定物件的信譽，並將資料新增至病毒資料庫。如果系統無法確定物件的信譽，則系統會查詢 Kaspersky 病毒分析。



**Sandbox**

Kaspersky Endpoint Security 會處理虛擬機中的物件。Kaspersky Sandbox 會分析物件的行為並就其信譽做出決定。該技術只有在您使用 Kaspersky Sandbox 解決方案時才可使用。



**Cloud Sandbox**

Kaspersky Endpoint Security 在卡巴斯基提供的隔離環境中掃描物件。Cloud Sandbox 技術永久啟用，對所有卡巴斯基安全網路使用者可用，與他們使用的產品授權類型無關。如果您已經部署 Endpoint Detection and Response 解決方案，可以為 Cloud Sandbox 偵測到的威脅啟用單獨的計數器。

## 選取目錄

每種類型的威脅是由專門的元件處理。各個元件均可獨立啟用或停用，並可以配置其設定。

| 區域 | 元件 |
| --- | --- |
| **關鍵威脅防護**  | **檔案威脅防護**<br>"檔案威脅防護"元件允許您防止電腦的檔案系統受到感染。預設情況下，檔案威脅防護元件會永久駐留在電腦的 RAM 中，並即時掃描所有開啟、儲存或執行的檔案。該元件會掃描所有電腦磁碟機（包括已連線的磁碟機）上的檔案。該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來提供電腦防護。<br><br>**Web 威脅防護**<br>"Web 威脅防護"元件可防止從網際網路下載惡意檔案，同時封鎖惡意網站和釣魚網站。該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來提供電腦防護。<br><br>**郵件威脅防護**<br>"郵件威脅防護"元件掃描傳送和接收電子郵件的附件是否有病毒和其他威脅。該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來提供電腦防護。<br><br>郵件威脅防護可以掃描傳入和傳出的郵件。該應用程式在以下郵件用戶端中支援 POP3、SMTP、IMAP 和 NNTP：<br><br>• Microsoft Office Outlook<br>• Mozilla Thunderbird<br>• Windows Mail<br>• MyOffice Mail<br>• R7-Office Organizer<br><br>若要掃描 Mozilla Thunderbird、MyOffice Mail 及 R7-Office Organizer 郵件用戶端的流量，您需要將卡巴斯基憑證新增至專屬憑證儲存區，並選擇該專屬憑證儲存區。<br><br>郵件威脅防護不支援其他協定和郵件用戶端。<br><br>郵件威脅防護並不總是能夠獲得*協定級別*的郵件存取權限（例如，當使用 Microsoft Exchange 解決方案時）。為此，郵件威脅防護包括 Microsoft Office Outlook 延伸程式。該延伸程式允許在*郵件用戶端級別*掃描郵件。郵件威脅防護延伸支援 Outlook 2010、2013、2016、2019 和 2021 的操作。<br><br>**網路威脅防護**<br>*網路威脅防護*元件（也稱為入侵偵測系統，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。<br><br>**防火牆**<br>在網際網路或區域網路上工作時，防火牆會封鎖未經授權的電腦連線。防火牆還控制腦上應用程式的網路活動。這允許您防護公司區域網路免受身分竊盜和其他攻擊。該元件借助防毒資料庫、卡巴斯基安全網路雲端服務和預先定義的*網路規則*來提供電腦防護。<br>**BadUSB 攻擊防護**<br>BadUSB 攻擊防護元件可以防止受感染的模擬鍵盤的 USB 裝置連線至電腦。<br><br>**AMSI 防護**<br>AMSI 防護元件設計用於支援 Microsoft 的反惡意軟件掃描接口。*惡意軟體防護掃描介面 (AMSI)* 允許具有 AMSI 支援的協力廠商應用程式將物件（例如，PowerShell 指令碼）傳送到 Kaspersky Endpoint Security 進行附加掃描，然後接收這些物件的掃描結果。 |

| 區域 | 元件 |
| --- | --- |
| **進階威脅防護**  | **卡巴斯基安全網路**<br>*卡巴斯基安全網路（KSN）*是雲端服務的基礎結構，可提供對線上卡巴斯基知識庫的存取，該知識庫包含有關檔案、網頁資源和軟體信譽的資訊。使用卡巴斯基安全網路的資料可確保 Kaspersky 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 提供有關所掃描檔案的類別和信譽的資訊，以及有關所掃描網址的信譽的資訊。<br>**行為偵測**<br>"行為偵測"元件接收您電腦上的應用程式操作的資料，並將此資訊提供給其他防護元件以提高效能。"行為偵測"元件將行為流簽章 (BSS) 用於應用程式。如果應用程式操作比對危險活動行為流簽章，Kaspersky Endpoint Security 將執行選定的回應操作。Kaspersky Endpoint Security 基於行為特徵碼，可為電腦提供主動防禦。<br><br>行為偵測元件也會監控網路連接埠，以查找可能威脅電腦安全的應用程式處理程序。應用程式透過病毒資料庫獲取有關此類處理程序的資訊。<br>**Anti-Cryptor**<br>Anti-Cryptor 元件可分析共用資料夾中的活動。如果該活動與外部加密的典型行為流簽章比對，Kaspersky Endpoint Security 將執行選定操作。<br><br>**弱點利用防禦**<br>"弱點利用防禦"元件可偵測利用電腦弱點來利用管理員權限或執行惡意活動的程式程式碼。例如，弱點利用程式可以利用緩衝區溢位攻擊。為此，弱點利用程式會向易受攻擊的應用程式傳送大量資料。處理此資料時，易受攻擊的應用程式會執行惡意程式碼。此攻擊的結果是，弱點利用程式可啟動未經授權的惡意軟體安裝。當存在從易於感染的應用程式執行可執行檔的嘗試，並且該嘗試並非由使用者執行時，Kaspersky Endpoint Security 將封鎖該檔案執行或通知使用者。<br><br>漏洞利用防護元件也會監控網路連接埠，以查找可能威脅電腦安全的應用程式處理程序。應用程式透過病毒資料庫獲取有關此類處理程序的資訊。<br>**主機入侵防禦**<br>"主機入侵防禦"元件可避免應用程式執行可能給作業系統帶來危險的操作，並確保控制對作業系統資源和個人資料的存取。該元件借助防毒資料庫和卡巴斯基安全網路雲端服務來提供電腦防護。<br>**修復引擎**<br>修復引擎允許 Kaspersky Endpoint Security 復原惡意軟體在作業系統中執行的操作。 |
| **安全控制**  | **應用程式控制**<br>"應用程式控制"管理使用者電腦上的應用程式啟動。這允許您在使用應用程式時實行公司安全政策。"應用程式控制"還透過限制對應用程式的存取來降低電腦感染的風險。<br>**裝置控制**<br>"裝置控制"管理使用者對安裝在電腦上或連線到電腦的裝置（例如，硬碟磁碟機、相機或 Wi-Fi 模組）的存取。這樣可以在連線此類裝置時防護電腦免受感染，並防止資料遺失或洩漏。<br>**Web 控制**<br>"Web 控制"管理使用者對 Web 資源的存取。這有助於減少流量和工作時間的不當使用。當使用者嘗試開啟受"Web 控制"限制的網站時，Kaspersky Endpoint Security 會封鎖存取或顯示警告。<br>**自適應異常控制**<br>自適應異常控制元件會監視並封鎖不是公司網路內電腦典型操作的相關操作。自適應異常控制使用一組規則來偵錯非典型行為（例如，*從 Office 應用程式啟動 Microsoft PowerShell* 規則）。規則由 Kaspersky 專家根據惡意活動的典型情景建立。您可以配置"自適應異常控制"處理每條規則的方式，例如，允許執行使某些工作流工作自動化的 PowerShell 指令碼。Kaspersky Endpoint Security 會同時更新規則集和應用程式資料庫。<br>**記錄審查**<br>記錄檢查會基於 Windows 事件記錄分析監控受防護環境的完整性。如果應用程式在系統中偵測到有非典型行為的跡象，它會通知管理員，因為該行為可能表明有人嘗試網路攻擊。<br>**系統完整性監控**<br>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示。 |
| **工作**  | **惡意軟體掃描**<br>Kaspersky Endpoint Security 掃描電腦查找病毒和其它威脅。惡意軟體掃描有助於排除傳播未被防護元件偵測到（例如，由於安全等級低）的惡意軟體的可能性。<br>**資料庫和應用程式模組更新**<br>Kaspersky Endpoint Security 下載更新應用程式資料庫和模組。更新可以確保電腦防護最新的病毒和其他威脅。在預設設定下，應用程式將會自動更新，但視情況所需，您亦可手動更新資料庫和應用程式模組。<br>**上次更新回溯**<br><br>Kaspersky Endpoint Security 將回溯最新更新的資料庫和模組。這允許您在必要時將資料庫和應用程式模組回溯到以前的版本，例如，當新資料庫版本包含無效簽章而導致 Kaspersky Endpoint Security 封鎖了安全的應用程式時。<br>**應用程式完整性檢查**<br><br>Kaspersky Endpoint Security 將檢查應用程式安裝資料夾內的應用程式模組以檢查任何損壞或修改。如果應用程式模組擁有錯誤的數位簽章，則此模組被認定為損壞。 |

| 區域 | 元件 |
| --- | --- |
| 資料加密  | **檔案級加密**<br>該元件允許建立檔案加密規則。您可以選擇預定義資料夾進行加密，手動選擇資料夾，或者根據副檔名選取單個檔案。<br>**完整磁碟加密**<br>該元件允許使用卡巴斯基磁碟加密或者 BitLocker 磁碟機加密來加密硬碟。<br>**卸除式磁碟機加密**<br>該元件允許防護卸除式磁碟機上的資料。您可以使用完整磁碟加密 (FDE) 或者檔案級加密 (FLE)。 |
| Detection and Response  | **Endpoint Detection and Response Optimum**<br>Kaspersky Endpoint Detection and Response Optimum 解決方案的內建代理（以下也稱為 "EDR Optimum"）。*Kaspersky Endpoint Detection and Response* 是用於防護組織的 IT 基礎結構抵禦進階網路威脅的解決方案。該解決方案的功能結合了自動偵測威脅和回應這些威脅的能力，以抵消包括新漏洞、勒索軟體、無檔案攻擊以及使用合法系統工具的方法。有關解決方案的更多資訊，請參見Kaspersky Endpoint Detection and Response Optimum 說明。<br>**Endpoint Detection and Response Expert**<br>Kaspersky Endpoint Detection and Response Expert 解決方案的內建代理（以下也稱為 "EDR Expert"）。EDR Expert 比 EDR Optimum 提供更多的威脅監控和回應功能。有關解決方案的更多資訊，請參見Kaspersky Endpoint Detection and Response Expert 說明。<br>**Endpoint Detection and Response Expert (on-premise)** 和**Network Detection and Response (KATA)**<br>用於管理 Endpoint Detection and Response 和 Network Detection and Response 元件的內建代理，元件屬於 Kaspersky Anti Targeted Attack Platform 解決方案。*Kaspersky Anti Targeted Attack Platform* 是旨在及時偵測複雜威脅（如針對性攻擊、進階持久性威脅 (APT)、零日攻擊等）的解決方案。Kaspersky Anti Targeted Attack Platform 包括三個功能單元：<br>• Kaspersky Anti Targeted Attack Platform (*KATA*)<br>• Kaspersky Endpoint Detection and Response (*EDR (KATA)*)<br>• Network Detection and Response (*NDR (KATA)*)<br>您可以單獨購買所有功能單元或單獨的功能單元。有關解決方案的詳細資訊，請參閱 Kaspersky Anti Targeted Attack Platform 說明。<br>**Sandbox**<br>Sandbox 的內建代理。*Sandbox*元件可偵測和自動封鎖電腦上的進階威脅。Sandbox 會分析物件行為以偵測惡意行動和組織的 IT 基礎架構上的針對性攻擊所特有的活動。Sandbox 會分析和掃描部署了 Microsoft Windows 作業系統的虛擬影像的特殊伺服器（Sandbox 伺服器）上的物件。有關解決方案的詳細資訊，請參閱 Kaspersky Sandbox 說明 和 Kaspersky Anti Targeted Attack Platform 說明。<br>**Managed Detection and Response**<br>支援 Kaspersky Endpoint Detection and Response Optimum 解決方案操作的內建代理。*Kaspersky Managed Detection and Response (MDR)* 解決方案可自動偵測和分析您的基礎架構中的安全事件。為此，MDR 會使用從端點和機學習收到的遙測資料。MDR 會將事件資料傳送給卡巴斯基專家。專家然後可以處理事件，並且，例如，新增新項目至病毒資料庫。或者，專家可以簽發事件處理建議，並且，例如，建議從網路中隔離電腦。如欲瞭解該解決方案如何工作的詳細資訊，請參閱 Kaspersky Managed Detection and Response 說明。 |

# 應用程式的模式：標準、EDR Agent、Light Agent

Kaspersky Endpoint Security for Windows 是許多卡巴斯基解決方案的一部分。根據解決方案，您需要為應用程式選擇一種模式。

| | |
| --- | --- |
|  | 標準模式<br>這是應用程式的主要和預設模式。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 為工作站和伺服器提供全面防護，使其免受各種威脅、網路攻擊和詐騙。 |



EDR Agent

此模式允許將 Kaspersky Detection and Response 解決方案與協力廠商 EPP 解決方案一起部署。Detection and Response 解決方案包括 Kaspersky Managed Detection and Response (MDR) 和 Kaspersky Anti Targeted Attack Platform (KATA)。EDR Agent 也支援 Kaspersky SIEM 解決方案、Kaspersky Unified Monitoring and Analysis Platform (KUMA)。

在此模式下，檔案威脅防護或 Web 威脅防護等標準防護元件無法使用。協力廠商 EPP 解決方案提供對電腦的標準防護。EDR Agent 持續監視在這些電腦上執行的處理程序、開啟的網路連線以及正在修改的檔案。並與 Detection and Response 解決方案互動。



Light Agent

此模式用於防護虛擬環境。Light Agent 模式下的 Kaspersky Endpoint Security 是 Kaspersky Hybrid Cloud Security 決方案的一部分。Light Agent 可為工作站和伺服器防護裝有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，物件透過安裝在單獨虛擬機 SVM （Secure Virtual Machine）上的特殊解決方案元件來掃描是否存在病毒和其他惡意軟體。因此，Light Agent 使用 SVM 的資源而不是虛擬機的資源來確保基礎結構的安全。

# 分發套件

分發套裝包括以下分發套件：

- **強加密 (AES256)**
  此分發套件包含用於實施有效金鑰長度為 256 位元的 AES（進階加密標準）加密演算法的加密工具。
- **簡單加密 (AES56)**
  此分發套件包含用於實施有效金鑰長度為 56 位元的 AES 加密演算法的加密工具。

每個分發套件都包含以下檔案：

| | |
|---|---|
| `kes_win.msi` | Kaspersky Endpoint Security 安裝套件。 |
| `setup_kes.exe` | 透過任一可用方法安裝應用程式所需的檔案。 |
| `kes_win.kud` | 用於建立 Kaspersky Endpoint Security 安裝套件的檔案。 |
| `klcfginst.msi` | 卡巴斯基安全管理中心管理主控台中應用程式管理外掛程式的安裝套件。 |
| `bases.cab` | 安裝過程中使用的更新套件檔案。 |
| `cleaner_v2.cab`<br>`cleanerapi_v2.cab` | 用於刪除不相容軟體的檔案。 |
| `incompatible.txt` | 包含可能導致 Kaspersky Endpoint Security 相容性問題的軟體清單的檔案。卡巴斯基不保證 Kaspersky Endpoint Security 與清單中的軟體相容。 |
| `ksn_<language ID>.txt` | 包含參與卡巴斯基安全網路的條款的檔案。 |
| `license.txt` | 包含最終使用者產品授權協議和隱私政策的檔案。 |
| `installer.ini` | 包含分發套裝內部設定的檔案。 |
| `kes.cab` | 應用程式圖形介面檔案。 |

| | |
|---|---|
| aes256.cab / aes56.cab | AES 加密演算法檔案。 |
| package.kcat | 帶有應用程式分發套件的簽章的檔案。數位簽章可保證應用程式分發套件的真實性和完整性。 |

不建議變更這些設定的值。如果您希望變更安裝選項，請使用 setup.ini 檔案。

# 硬體和軟體需求

為確保 Kaspersky Endpoint Security 的正常執行，您的電腦必須符合以下需求：

最低一般要求：

- 2 GB 磁碟可使用空間
- CPU:
  - 工作站：1 GHz
  - 伺服器：1.4 GHz
  - SSE2 指示支援。

  不支援 Arm 架構。
- RAM:
  - 工作站（x86）：1 GB
  - 工作站（x64）：2 GB
  - 伺服器：2 GB
  - 用來安裝包含用於 Kaspersky Anti Targeted Attack Platform (EDR) 整合的內建代理的應用程式的伺服器：8 GB
- Microsoft .NET Framework 4 或更高版本
- 若要安裝應用程式，您需要擁有電腦的管理員權限。

## 工作站

支援的工作站作業系統：

- Windows 7 Home / Professional / Ultimate / Enterprise Service Pack 1 或更高版本
- Windows 8 Professional / Enterprise

- Windows 8.1 Professional / Enterprise
- Windows 10 Home / Pro / Pro for Workstations / Education / Enterprise / Enterprise 多工作階段
- Windows 11 Home / Pro / Pro for Workstations / Education / Enterprise

Windows 作業系統從版本 11 24H2 開始支援 UDP Receive Segment Coalescing Offload （URO）技術。如果電腦上安裝了相容的網路卡和驅動程式，則預設啟用該技術。在使用者的電腦上停用 URO 會顯著降低應用程式的效能。

為確保 Kaspersky Endpoint Security 正常運作，Windows Security Center (wscsvc) 服務必須在使用者的電腦上執行。

如果未安裝作業係統更新 KB4490628（2019 年 3 月 12 日）和 KB4474419（2019 年 9 月 23 日），Kaspersky Endpoint Security 將無法安裝在 Microsoft Windows 7 上。有關詳細資訊，請參閱卡巴斯基知識庫。

有關對 Microsoft Windows 10 作業系統的支援的詳細資訊，請參閱技術支援知識庫。

有關對 Microsoft Windows 11 作業系統的支援的詳細資訊，請參閱技術支援知識庫。

伺服器

Kaspersky Endpoint Security 支援執行伺服器 Windows 作業系統的電腦上的應用程式的核心元件。您可以在組織的伺服器和叢集上使用 Kaspersky Endpoint Security for Windows 而不是 Kaspersky Security for Windows Server（Cluster Mode）。應用程式也支援Server Core Mode（請見已知問題）。

支援的伺服器作業系統：

- Windows Small Business Server 2011 Essentials / Standard（64 位元）

  Microsoft Small Business Server 2011 Standard（64 位元）僅在安裝了 Service Pack 1 for Microsoft Windows Server 2008 R2 時才受支援。

- Windows MultiPoint Server 2011（64 位元）
- Windows Server 2008 R2 Foundation / Standard / Enterprise / Datacenter Service Pack 1 或更高版本
- Windows Web Server 2008 R2 Service Pack 1 或更高版本
- Windows Server 2012 Foundation / Essentials / Standard / Datacenter （包括 Server Core 模式）
- Windows Server 2012 R2 Foundation / Essentials / Standard / Datacenter（包括 Server Core 模式）
- Windows Server 2016 Essentials / Standard / Datacenter（包括 Server Core 模式）

- Windows Server 2019 Essentials / Standard / Datacenter（包括 Server Core 模式）
- Windows Server 2022 Standard / Datacenter / Datacenter: Azure Edition（包括 Server Core 模式）
- Windows Server 2025 Standard / Datacenter

如果未安裝作業係統更新 KB4490628（2019 年 3 月 12 日）和 KB4474419（2019 年 9 月 23 日），Kaspersky Endpoint Security 將無法安裝在 Microsoft Windows 2008 R2 上。

有關對 Microsoft Windows Server 2016 和 Microsoft Windows Server 2019 作業系統的支援的詳細資訊，請參閱技術支援知識庫。

有關對 Microsoft Windows Server 2022 作業系統的支援的詳細資訊，請參閱技術支援知識庫。

不受支援的伺服器作業系統：

- Windows Server 2003 Standard / Enterprise / Datacenter SP2 或更高版本
- Windows Server 2003 R2 Foundation / Standard / Enterprise / Datacenter SP2 或更高版本
- Windows Server 2008 Standard / Enterprise / Datacenter SP2 或更高版本
- Windows Server 2008 Core Standard / Enterprise / Datacenter SP2 或更高版本
- Microsoft Small Business Server 2008 Standard / Premium SP2 或更高版本

### 虛擬平台

標準模式下應用程式運行所支援的虛擬平台：

- VMware Workstation Pro 17.6.4
- VMware ESXi 8.0 Update 3g
- Windows Server 2025
- Citrix Virtual Apps and Desktops 7 2507 LTSR
- Citrix Provisioning 2507 LTSR
- XenServer 8.4

### 用於安裝 Light Agent 的虛擬機

虛擬機上的 BIOS 必須支援 SMBIOS 規範版本 2.1 或更高版本。

虛擬機上必須安裝以下套件和實用程式：

- 使用 Microsoft Hyper-V 時 – Integration Services 套件。
- 使用 VMware vSphere 時 – VMware Tools 套件。
- 使用 XenServer 時 – XenTools 套件。
- 使用 HUAWEI FusionSphere 時 – 華為工具包。
- 使用以 KVM 為基礎的 Hypervisor 時 – QEMU Guest Agent。

參閱Kaspersky Security for Virtualization Light Agent 說明瞭解在 Light Agent 模式下執行應用程式的虛擬基礎架構要求。

為了使應用程式正常運作，請使用頻寬至少為 100 Mbit/s 的虛擬網路介面。

### 終端伺服器

受支援的終端伺服器類型：

- Microsoft Remote Desktop Services based on Windows Server 2008 R2 SP1
- 基於 Windows Server 2012 的 Microsoft Remote Desktop Services
- 基於 Windows Server 2012 R2 的 Microsoft Remote Desktop Services
- 基於 Windows Server 2016 的 Microsoft Remote Desktop Services
- 基於 Windows Server 2019 的 Microsoft Remote Desktop Services
- 基於 Windows Server 2022 的 Microsoft Remote Desktop Services
- 基於 Windows Server 2025 的 Microsoft Remote Desktop Services
- 來自 Citrix Virtual Apps 和 Desktops 7 2507 LTSR 的 Citrix RDSH

### 卡巴斯基安全管理中心支援

Kaspersky Endpoint Security 支援以下版本的卡巴斯基安全管理中心的操作：

- 卡巴斯基安全管理中心 14
- 卡巴斯基安全管理中心 14.1
- 卡巴斯基安全管理中心 14.2
- 卡巴斯基安全管理中心 Linux 14.2

- 卡巴斯基安全管理中心 Linux 15
- 卡巴斯基安全管理中心 Windows 15.1
- 卡巴斯基安全管理中心 Linux 15.1
- 卡巴斯基安全管理中心 Linux 15.2
- 卡巴斯基安全管理中心 Linux 15.3
- 卡巴斯基安全管理中心 Linux 15.4
- 卡巴斯基安全管理中心 Linux 16
- 卡巴斯基安全管理中心 Linux 16.1

# 取決於作業系統類型的可用應用程式功能比較

可用的 Kaspersky Endpoint Security 功能集取決於作業系統的類型：工作站或伺服器（請參見下表）。

從 Kaspersky Endpoint Security 12.8 for Windows 開始，您可以在安裝套件中為不同的作業系統類型配置不同的元件集合。也就是說，您可以使用相同的 安裝套件將應用程式部署到工作站和伺服器。

Kaspersky Endpoint Security 功能比較

| 功能 | 工作站 | 伺服器 | Server Core 模式 |
|---|---|---|---|
| **進階威脅防護** | | | |
| 卡巴斯基安全網路 | ✓ | ✓ | ✓ |
| 行為偵測 | ✓ | ✓ | ✓ |
| 加密軟體防護 | ✓ | ✓ | ✓ |
| 弱點利用防禦 | ✓ | ✓ | ✓ |
| 主機入侵防禦 | ✓ | – | – |
| 修復引擎 | ✓ | ✓ | ✓ |
| **關鍵威脅防護** | | | |
| 檔案威脅防護 | ✓ | ✓ | ✓ |
| Web 威脅防護 | ✓ | ✓ | – |
| 郵件威脅防護 | ✓ | ✓ | – |
| 防火牆 | ✓ | ✓ | ✓ |
| 網路威脅防護 | ✓ | ✓ | ✓ |
| BadUSB 攻擊防護 | ✓ | ✓ | – |
| AMSI 防護 | ✓ | ✓ | ✓ |
| **安全控制** | | | |
| 記錄審查 | – | ✓ | – |
| 應用程式控制 | ✓ | ✓ | ✓ |
| 裝置控制 | ✓ | ✓ | ✓ |
| Web 控制 | ✓ | ✓ | – |

| 功能 | 工作站 | 伺服器 | Server Core 模式 |
|---|---|---|---|
| 自適應異常控制 | ✓ | – | – |
| 系統完整性監控 | – | ✓ | – |
| Cloud Discovery | ✓ | – | – |
| **資料加密** | | | |
| 卡巴斯基磁碟加密 | ✓ | – | – |
| BitLocker 磁碟機加密 | ✓ | ✓ | ✓ |
| 檔案級加密 | ✓ | – | – |
| 卸除式磁碟機加密 | ✓ | – | – |
| **Detection and Response** | | | |
| Endpoint Detection and Response Optimum | ✓ | ✓ | ✓ |
| Endpoint Detection and Response Expert | ✓ | ✓ | ✓ |
| Endpoint Detection and Response (KATA) | ✓ | ✓ | ✓ |
| Network Detection and Response (KATA) | ✓ | ✓ | ✓ |
| Sandbox | ✓ | ✓ | ✓ |
| Managed Detection and Response (MDR) | ✓ | ✓ | ✓ |
| KUMA 整合 | ✓ | ✓ | ✓ |

# 根據管理工具比較應用程式功能

Kaspersky Endpoint Security 中提供的功能集取決於管理工具（請參見下表）。

您可以使用卡巴斯基安全管理中心的以下主控台管理應用程式：

- 管理主控台。管理員工作站上安裝的 Microsoft 管理主控台 (MMC) 管理單元。
- 網頁主控台。管理伺服器上安裝的卡巴斯基安全管理中心元件。您可以在任何可存取管理伺服器的電腦上透過瀏覽器在網頁主控台中工作。

您也可以使用卡巴斯基安全管理中心雲端主控台管理應用程式。*卡巴斯基安全管理中心雲端主控台*是卡巴斯基安全管理中心的雲端版本。這意味著卡巴斯基安全管理中心的管理伺服器和其他元件安裝在卡巴斯基雲端基礎結構中。有關使用卡巴斯基安全管理中心雲端主控台管理應用程式的詳細資訊，請參閱卡巴斯基安全管理中心雲端主控台說明。

Kaspersky Endpoint Security 是 Kaspersky Next Pro View 解決方案的一部分。有關作為此解決方案的一部分時可用的應用程式功能的更多資訊，請參閱 Kaspersky Next 說明。

Kaspersky Endpoint Security 功能比較

| 功能 | 卡巴斯基安全管理中心 | | 卡巴斯基安全管理中心 |
|---|---|---|---|
| | 管理主控台 | 網頁主控台 | 雲端主控台 |
| **進階威脅防護** | | | |
| 卡巴斯基安全網路 | ✓ | ✓ | ✓ |
| 卡巴斯基私有安全網路 | ✓ | ✓ | – |
| 行為偵測 | ✓ | ✓ | ✓ |
| 加密軟體防護 | | | |

| 功能 | 卡巴斯基安全管理中心 | | 卡巴斯基安全管理中心 |
|---|---|---|---|
| | 管理主控台 | 網頁主控台 | 雲端主控台 |
| 弱點利用防禦 | ✓ | ✓ | ✓ |
| 主機入侵防禦 | ✓ | ✓ | ✓ |
| 修復引擎 | ✓ | ✓ | ✓ |
| **關鍵威脅防護** | | | |
| 檔案威脅防護 | ✓ | ✓ | ✓ |
| Web 威脅防護 | ✓ | ✓ | ✓ |
| 郵件威脅防護 | ✓ | ✓ | ✓ |
| 防火牆 | ✓ | ✓ | ✓ |
| 網路威脅防護 | ✓ | ✓ | ✓ |
| BadUSB 攻擊防護 | ✓ | ✓ | ✓ |
| AMSI 防護 | ✓ | ✓ | ✓ |
| **安全控制** | | | |
| 記錄審查 | ✓ | ✓ | ✓ |
| 應用程式控制 | ✓ | ✓ | ✓ |
| 裝置控制 | ✓ | ✓ | ✓ |
| Web 控制 | ✓ | ✓ | ✓ |
| 自適應異常控制 | ✓ | ✓ | ✓ |
| 系統完整性監控 | ✓ | ✓ | ✓ |
| Cloud Discovery | – | – | ✓ |
| **資料加密** | | | |
| 卡巴斯基磁碟加密 | ✓ | ✓ | – |
| BitLocker 磁碟機加密 | ✓ | ✓ | ✓ |
| 檔案級加密 | ✓ | ✓ | – |
| 卸除式磁碟機加密 | ✓ | ✓ | – |
| **Detection and Response** | | | |
| Endpoint Detection and Response Optimum | – | ✓ | ✓ |
| Endpoint Detection and Response Expert | – | – | ✓ |
| Endpoint Detection and Response (KATA) | ✓ | ✓ | – |
| Network Detection and Response (KATA) | ✓ | ✓ | – |
| Sandbox | – | ✓ | – |
| Managed Detection and Response (MDR) | ✓ | ✓ | ✓ |
| **KUMA 整合** | ✓ | ✓ | ✓ |
| **工作** | | | |
| 新增金鑰 | ✓ | ✓ | ✓ |
| 變更應用程式元件 | ✓ | ✓ | ✓ |
| 清查 | ✓ | ✓ | ✓ |
| 更新 | ✓ | ✓ | ✓ |
| 更新回溯 | ✓ | ✓ | ✓ |
| 惡意軟體掃描 | ✓ | ✓ | ✓ |
| 應用程式完整性檢查 | ✓ | ✓ | – |

| 功能 | 卡巴斯基安全管理中心 | | 卡巴斯基安全管理中心 |
|---|---|---|---|
| | 管理主控台 | 網頁主控台 | 雲端主控台 |
| 抹除資料 | ✓ | ✓ | ✓ |
| 管理身分驗證代理帳戶（卡巴斯基磁碟加密） | ✓ | ✓ | – |
| IOC 掃描 (EDR) | – | ✓ | ✓ |
| 移動檔案到隔離區 (EDR) | – | ✓ | ✓ |
| 獲取檔案 (EDR) | – | ✓ | ✓ |
| 刪除檔案 (EDR) | – | ✓ | ✓ |
| 啟動處理程序 (EDR) | – | ✓ | ✓ |
| 終止處理程序 (EDR) | – | ✓ | ✓ |

# 與其他應用程式的相容性

Kaspersky Endpoint Security 與某些 Kaspersky 應用程式以及某些協力廠商應用程式不相容。因此，在安裝、更新應用程式版本和變更應用程式元件之前，Kaspersky Endpoint Security 會掃描電腦，查看是否有此類應用程式。

## 與協力廠商應用程式的相容性

Kaspersky Endpoint Security 與屬於協力廠商端點防護系統 (Endpoint Protection Platform, EPP) 的應用程式不相容。Kaspersky Endpoint Security 也可能會遇到與其他應用程式的相容性問題。為了確定相容性，Kaspersky Endpoint Security 會查閱卡巴斯基準備的軟體清單。該清單包含在incompatible.txt檔案中。該檔案包括在分發套件中。

卡巴斯基不保證 Kaspersky Endpoint Security 與清單中的軟體相容。如果發現清單中的應用程式，安裝程式將停止 Kaspersky Endpoint Security 的部署。安裝程式可能會自動從清單中刪除某些應用程式。如果您願意無視風險並希望在同一台電腦上安裝 Kaspersky Endpoint Security 和清單中的某個軟體，則可以跳過電腦檢查（請參閱下面的說明）。

**下載 INCOMPATIBLE.TXT 檔案**

## 與卡巴斯基應用程式的相容性

Kaspersky Endpoint Security 與以下 Kaspersky 應用程式不相容：

- 卡巴斯基標準版 | 進階版| 專業版。
- Kaspersky Small Office Security。
- 卡巴斯基安全軟體。
- Kaspersky Anti-Virus。

- Kaspersky Total Security。
- Kaspersky Safe Kids。
- Kaspersky Free。
- Kaspersky Anti-Ransomware Tool。
- Endpoint Sensor 作為 Kaspersky Anti Targeted Attack Platform 和 Kaspersky Endpoint Detection and Response 解決方案的一部分。
- Kaspersky Endpoint Agent 作為 Detection and Response 解決方案的一部分。

  卡巴斯基正在將所有 Detection and Response 切換為使用 Kaspersky Endpoint Security 內建代理，而不是 Kaspersky Endpoint Agent。從版本 12.1 開始，該應用程式支援所有 Detection and Response 解決方案。

- Kaspersky Security for Virtualization Light Agent。
- Kaspersky Fraud Prevention for Endpoint。
- Kaspersky Security for Windows Server

  從 Kaspersky Endpoint Security 12.0 開始，您可以從 Kaspersky Security for Windows Server 遷移到 Kaspersky Endpoint Security for Windows，並使用同一個解決方案來防護工作站和伺服器。

- Kaspersky Embedded Systems Security。

如果電腦安裝了該清單中的 Kaspersky 應用程式，Kaspersky Endpoint Security 會移除這些應用程式。請等待此過程結束，然後再繼續安裝 Kaspersky Endpoint Security。

### 跳過檢查可能導致相容性問題的軟體

如果 Kaspersky Endpoint Security 偵測到incompatible.txt清單中的軟體，應用程式安裝將會被終止。要繼續安裝，您必須刪除該應用程式。不過，如果協力廠商軟體的廠商在檔案中指明其軟體與 Endpoint Protection Platform (EPP) 相容，您可以將 Kaspersky Endpoint Security 安裝到包含該廠商的應用程式的電腦上。例如，Endpoint Detection and Response (EDR) 解決方案提供者可能宣佈他們與協力廠商 EPP 系統相容。如果是這種情況，您需要啟動安裝 Kaspersky Endpoint Security 而不執行不已安裝的軟體檢查。為此，將以下參數傳遞給安裝程式：

- `SKIPPRODUCTCHECK=1`。停用已安裝軟體檢查。分發套件中包含的 incompatible.txt 檔案提供了可能引起相容性問題的軟體清單。如果沒有為此參數設定任何值，並且偵測到清單中的軟體，則將終止 Kaspersky Endpoint Security 的安裝。
- `SKIPPRODUCTUNINSTALL=1`。停用從incompatible.txt清單中自動移除偵測到的軟體。如果沒有為此參數設定任何值，則 Kaspersky Endpoint Security 將嘗試移除可能引起相容性問題的軟體。
- `CLEANERSIGNCHECK=0`。停用對檢查發現的應用程式進行數位簽章驗證。如果未設定此參數，當透過卡巴斯基安全管理中心部署應用程式時，數位簽章驗證將被停用。本機安裝應用程式時將預設啟用數位簽章驗證。

您可以在本機安裝應用程式時在指令列中傳遞參數。

如果在安裝過程中您跳過了可能導致相容性問題的軟體掃描，Kaspersky Endpoint Security 可以在應用程式元件變更時再次執行此檢查。若要跳過對已安裝軟體的掃描，您需要配置 *變更應用程式元件* 工作。

範例:

```
C:\KES\setup_kes.exe /pEULA=1 /pPRIVACYPOLICY=1 /pKSN=0 /pSKIPPRODUCTCHECK=1 /pSKIPPRODUCTUNINSTALL=1
/pCLEANERSIGNCHECK=0 /s
```

若要遠端安裝 Kaspersky Endpoint Security，您需要將適當的參數新增到安裝套件產生檔案，它的名稱為 `kes_win.kud`，位於 `[Setup]` 中（詳情見下）。`kes_win.kud` 檔案包括在分發套件中。

kes_win.kud

```
[Setup]
UseWrapper=1
ExecutableRelPath=EXEC
Params=/s /pAKINSTALL=1 /pEULA=1 /pPRIVACYPOLICY=1 /pKSN=0 /pSKIPPRODUCTCHECK=1 /pSKIPPRODUCTUNINSTALL=1
/pCLEANERSIGNCHECK=0
Executable=setup_kes.exe
RebootDelegated = 1
RebootAllowed=1
ConfigFile=installer.ini
RelPathsToExclude=klcfginst.msi
```

# 安裝和移除應用程式

可以透過以下方式在電腦上安裝 Kaspersky Endpoint Security：

- 本機使用安裝精靈。
- 本機使用命令列。
- 遠端使用卡巴斯基安全管理中心。
- 遠端透過 Microsoft Windows 群組政策管理編輯器（有關詳細資訊，請造訪 Microsoft 技術支援網站）。
- 遠端使用系統中心配置管理器。

您可以透過多種方式配置應用程式安裝設定。如果同時使用多種方法配置設定，Kaspersky Endpoint Security 將套用具有最高優先順序的設定。Kaspersky Endpoint Security 使用以下優先順序順序：

1. 從 setup.ini 檔案收到的設定。
2. 從 installer.ini 檔案收到的設定。
3. 從命令列收到的設定。
4. 從 設定檔（install.cfg）接收到的設定。

我們建議您在啟動 Kaspersky Endpoint Security 安裝（包括遠端安裝）之前關閉所有活動的應用程式。

安裝 Kaspersky Endpoint Security 時，作業系統可能會顯示自己的訊息。安裝應用程式時，網路和網際網路連線也可能會中斷。

安裝、更新或解除安裝 Kaspersky Endpoint Security 時，可能會出現錯誤。有關解決這些錯誤的更多資訊，請參閱技術支援知識庫。

# 透過卡巴斯基安全管理中心佈署

Kaspersky Endpoint Security 可以透過多種方式佈署在企業網路內的電腦上。您可以為您的組織選取最合適的佈署方案，或同時組合多個佈署方案。在安裝應用程式之前，您必須確保電腦上安裝了卡巴斯基安全管理中心網路代理。*網路代理*可促進管理伺服器與用戶端電腦之間的互動。

卡巴斯基安全管理中心支援以下主要佈署方法：

- 使用防護佈署精靈安裝應用程式。

  如果您滿意 Kaspersky Endpoint Security for Windows 的預設設定，並且的您組織的基礎結構很簡單，不需要特殊配置，則標準安裝方法很方便。

- 使用遠端安裝工作安裝應用程式。

通用安裝方法允許您配置 Kaspersky Endpoint Security 設定並靈活管理遠端安裝工作。Kaspersky Endpoint Security 的安裝套件括以下步驟：

1. 建立安裝套件。
2. 建立遠端安裝工作。

卡巴斯基安全管理中心還支援使用其他方法來安裝 Kaspersky Endpoint Security，例如在作業系統映射內佈署。有關其他佈署方法的詳細資訊，請參閱卡巴斯基安全管理中心說明。

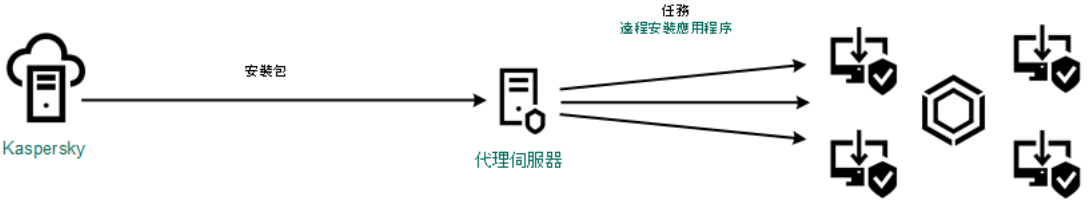
# 應用程式的標準安裝

卡巴斯基安全管理中心提供了防護佈署精靈，以便在企業電腦上安裝應用程式。防護佈署精靈包括以下主要操作：

1. 選擇 Kaspersky Endpoint Security 安裝套件。

   *安裝套件*是為透過卡巴斯基安全管理中心遠端安裝 Kaspersky 應用程式而建立的一組檔案。安裝套件中包含安裝應用程式以及安裝後立即執行應用程式所需的一系列設定。安裝套件透過應用程式分發套件中包括的副檔名為 .kpd 和 .kud 的檔案建立。Kaspersky Endpoint Security 安裝套件通用於所有受支援的 Windows 版本和處理器架構類型。

2. 建立卡巴斯基安全管理中心管理伺服器的*遠端安裝應用程式*工作。




Kaspersky Endpoint Security 佈署

**如何在管理主控台 (MMC) 中執行防護佈署精靈**

1. 開啟卡巴斯基安全管理中心管理主控台。
2. 在主控台樹狀目錄中，選擇"**進階 → 遠端安裝**"。
3. 點擊"**在受管理裝置上佈署安裝套件（工作站）**"連接。

這將啟動防護佈署精靈。按照精靈的說明進行操作。

用戶端電腦上的 TCP 連接埠 139 和 445 以及 UDP 連接埠 137 和 138 必須開放。

步驟 1. 選取安裝套件

從清單中選取 Kaspersky Endpoint Security 安裝套件。如果清單不包含 Kaspersky Endpoint Security 安裝套件，可以在精靈中建立安裝套件。

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

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

步驟 2. 選取安裝套件來源

選擇 **部署卡巴斯基安全管理中心套件** 來源。

步驟 3. 選取要進行安裝的裝置

選取要安裝 Kaspersky Endpoint Security 的電腦。下列選項可用：

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

步驟 4. 定義遠端安裝工作設定

配置以下其他應用程式設定：

- **強制下載安裝套件**選取應用程式安裝方法：
  - **使用網路代理**如果電腦上未安裝網路代理，將首先使用作業系統的工具安裝網路代理。然後透過網路代理的工具安裝 Kaspersky Endpoint Security。
  - **透過發佈點使用作業系統資源**透過發佈點使用作業系統資源將安裝套件傳輸到用戶端電腦。如果網路中有至少一個發佈點，則可以選取此選項。有關發佈點的詳細資訊，請參閱卡巴斯基安全管理中心說明。
  - **透過管理伺服器使用作業系統資源**檔案將透過管理伺服器使用作業系統資源傳送到用戶端電腦。如果用戶端電腦上未安裝網路代理，但用戶端電腦與管理伺服器在同一網路中，可以選取此選項。
- **透過其他管理伺服器管理的裝置的行為**。選取 Kaspersky Endpoint Security 安裝方法。如果網路中安裝了多個管理伺服器，這些管理伺服器可能看到相同的用戶端電腦。例如，這可能導致透過不同的管理伺服器在同一用戶端電腦上多次遠端安裝同一應用程式，或產生其他衝突。
- **如果已經安裝應用程式則不再重新安裝**例如，如果要安裝較早版本的應用程式，則清除此核取方塊。
- **在 Active Directory 群組政策中指定安裝網路代理程式**。使用 Active Directory 資源手動安裝網路代理。要安裝網路代理，必須以網域管理員權限執行遠端安裝工作。

步驟 5. 選取產品授權金鑰

向安裝套件新增用於啟動應用程式的金鑰。此步驟為可選項。如果管理伺服器包含帶自動分發功能的產品授權金鑰，則該金鑰稍後將自動新增。您還可以稍後透過使用"*新增金鑰*"工作來啟動應用程式。

步驟 6. 選取作業系統重新啟動設定

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

步驟 7. 在安裝應用程式前刪除不相容的應用程式

請仔細閱讀不相容應用程式清單並允許移除這些應用程式。如果電腦上安裝了不相容的應用程式，安裝 Kaspersky Endpoint Security 將以出錯結束。

步驟 8. 選取用於存取裝置的帳戶

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

步驟 9. 開始安裝

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

**如何在網頁主控台和雲端主控台中啟動防護佈署精靈**

在網頁主控台的主視窗中，選擇**發現和佈署 → 佈署和指派 → 防護佈署精靈**。

這將啟動防護佈署精靈。按照精靈的說明進行操作。

用戶端電腦上的 TCP 連接埠 139 和 445 以及 UDP 連接埠 137 和 138 必須開放。

步驟 1. 選取安裝套件

從清單中選取 Kaspersky Endpoint Security 安裝套件。如果清單不包含 Kaspersky Endpoint Security 安裝套件，可以在精靈中建立安裝套件。要建立安裝套件，您無需搜尋分發套件並將其儲存到電腦記憶體中。在卡巴斯基安全管理中心中，可以檢視位於 Kaspersky 伺服器中的分發套件清單，安裝套件會自動建立。Kaspersky 在發佈新版本的應用程式後會更新該清單。

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

步驟 2. 選取產品授權金鑰

向安裝套件新增用於啟動應用程式的金鑰。此步驟為可選項。如果管理伺服器包含帶自動分發功能的產品授權金鑰，則該金鑰稍後將自動新增。您還可以稍後透過使用"*新增金鑰*"工作來啟動應用程式。

步驟 3. 選取網路代理

選取將與 Kaspersky Endpoint Security 一起安裝的網路代理的版本。*網路代理*可促進管理伺服器與用戶端電腦之間的互動。如果電腦上已安裝網路代理，則不會再次安裝。

步驟 4. 選取要進行安裝的裝置

選取要安裝 Kaspersky Endpoint Security 的電腦。下列選項可用：

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

步驟 5. 配置進階設定

配置以下其他應用程式設定：

- **強制下載安裝套件**。選取應用程式安裝方法：
  - **使用網路代理**如果電腦上未安裝網路代理，將首先使用作業系統的工具安裝網路代理。然後透過網路代理的工具安裝 Kaspersky Endpoint Security。
  - **透過發佈點使用作業系統資源**透過發佈點使用作業系統資源將安裝套件傳輸到用戶端電腦。如果網路中有至少一個發佈點，則可以選取此選項。有關發佈點的詳細資訊，請參閱卡巴斯基安全管理中心說明。
  - **透過管理伺服器使用作業系統資源**檔案將透過管理伺服器使用作業系統資源傳送到用戶端電腦。如果用戶端電腦上未安裝網路代理，但用戶端電腦與管理伺服器在同一網路中，可以選取此選項。
- **如果已經安裝應用程式則不再重新安裝**。例如，如果要安裝較早版本的應用程式，則清除此核取方塊。
- **在 Active Directory 群組政策中指派安裝套件的安裝**Kaspersky Endpoint Security 透過網路代理安裝或透過 Active Directory 手動安裝。要安裝網路代理，必須以網域管理員權限執行遠端安裝工作。

步驟 6. 選取作業系統重新啟動設定

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

步驟 7. 在安裝應用程式前刪除不相容的應用程式

請仔細閱讀不相容應用程式清單並允許移除這些應用程式。如果電腦上安裝了不相容的應用程式，安裝 Kaspersky Endpoint Security 將以出錯結束。

步驟 8. 分配到管理群組

選取安裝網路代理後，電腦將被移動到其中的管理群組。需要將電腦移至管理群組，以便套用政策和群組工作。如果電腦已在任意管理群組中，則該電腦不會被重新移動。如果不選取管理群組，電腦將被新增到**未指派的裝置**群組。

步驟 9. 選取用於存取裝置的帳戶

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

步驟 10.開始安裝

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

# 建立安裝套件

*安裝套件*是為透過卡巴斯基安全管理中心遠端安裝 Kaspersky 應用程式而建立的一組檔案。安裝套件中包含安裝應用程式以及安裝後立即執行應用程式所需的一系列設定。安裝套件透過應用程式分發套件中包括的副檔名為 .kpd 和 .kud 的檔案建立。Kaspersky Endpoint Security 安裝套件通用於所有受支援的 Windows 版本和處理器架構類型。

**如何在管理主控台 (MMC) 中建立安裝套件**

1. 在管理主控台中，轉到資料夾**"管理伺服器 → 進階 → 遠端安裝 → 安裝套件"**。
   這將開啟已下載到卡巴斯基安全管理中心的安裝套件清單。
2. 點擊**"建立安裝套件"**。

新安裝套件精靈啟動。按照精靈的說明進行操作。

步驟 1. 選取安裝套件類型

請選擇**為卡巴斯基應用程式建立安裝套件**選項。

步驟 2. 定義安裝套件名稱

輸入安裝套件的名稱，例如，*Kaspersky Endpoint Security for Windows 12.12*。

步驟 3. 選取用於安裝的分發套件

點擊**"瀏覽"**按鈕，然後選擇分發套件中包含的`kes_win.kud`檔案。

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

步驟 4. 最終使用者產品授權協議和隱私政策

閱讀並接受最終使用者產品授權協議的條款。

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

在安裝套件設定中，您可以選擇適合不同作業系統類型的應用程式元件。即，安裝套件包括兩套元件：用於工作站的元件和用於伺服器的元件。在部署安裝套件之前，安裝程式會偵測作業系統的類型，並僅安裝您為該作業系統類型選擇的應用程式元件。這樣，您可以為工作站和伺服器使用同一個安裝套件。

安裝套件包含來自管理伺服器儲存區的病毒資料庫。您可以更新安裝套件中的資料庫，以減少在安裝 Kaspersky Endpoint Security 之後更新資料庫時的流量消耗。

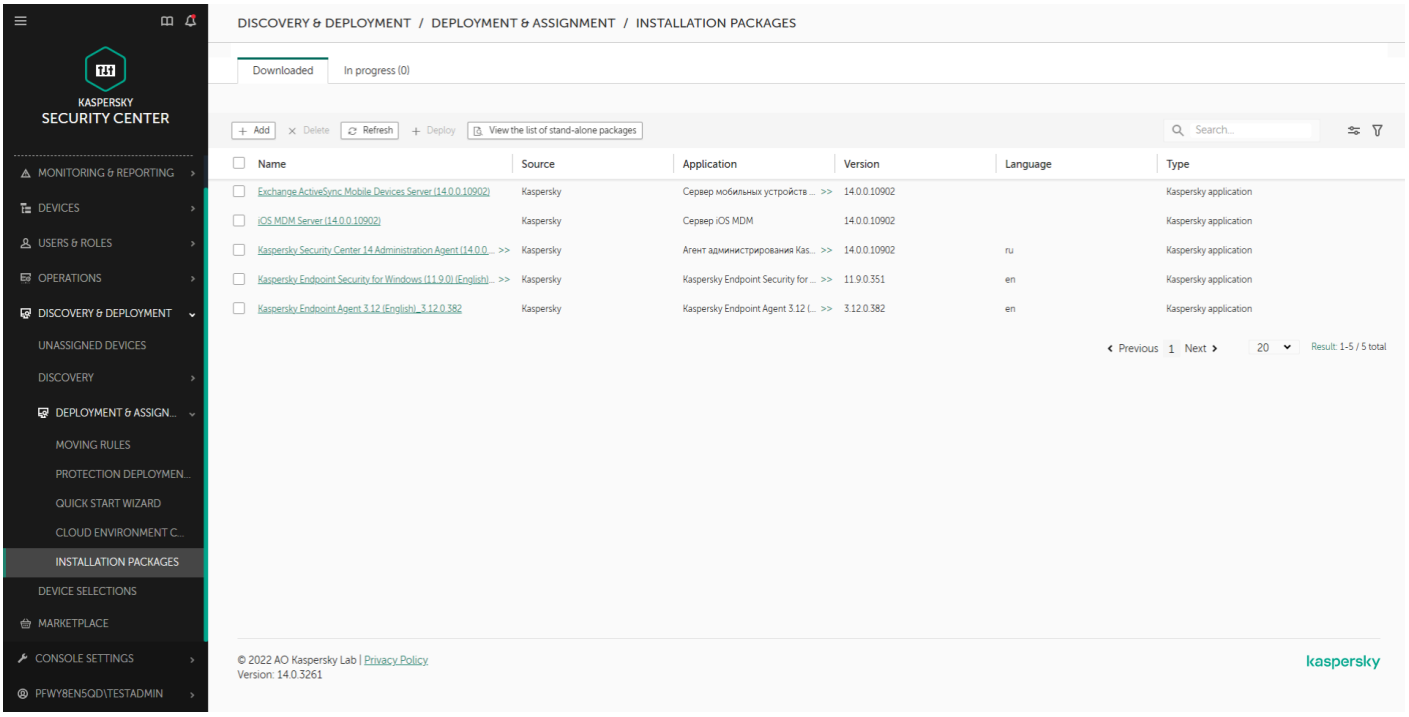
**如何在網頁主控台和雲端主控台中建立安裝套件**

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

   這將開啟已下載到卡巴斯基安全管理中心的安裝套件清單。

2. 點擊**"新增"**。

新安裝套件精靈啟動。按照精靈的說明進行操作。




安裝套件清單

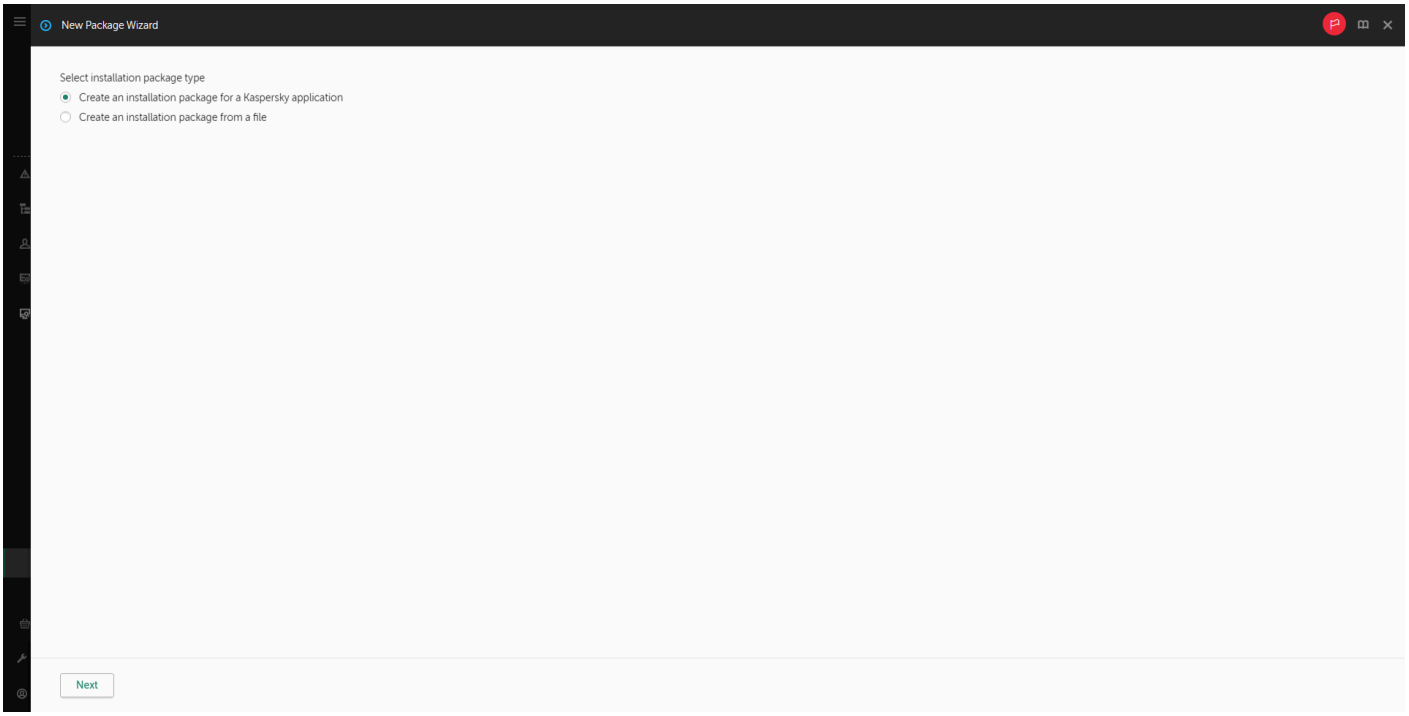
步驟 1. 選取安裝套件類型

請選擇**為卡巴斯基應用程式建立安裝套件**選項。

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

您還可以從檔案建立安裝套件。

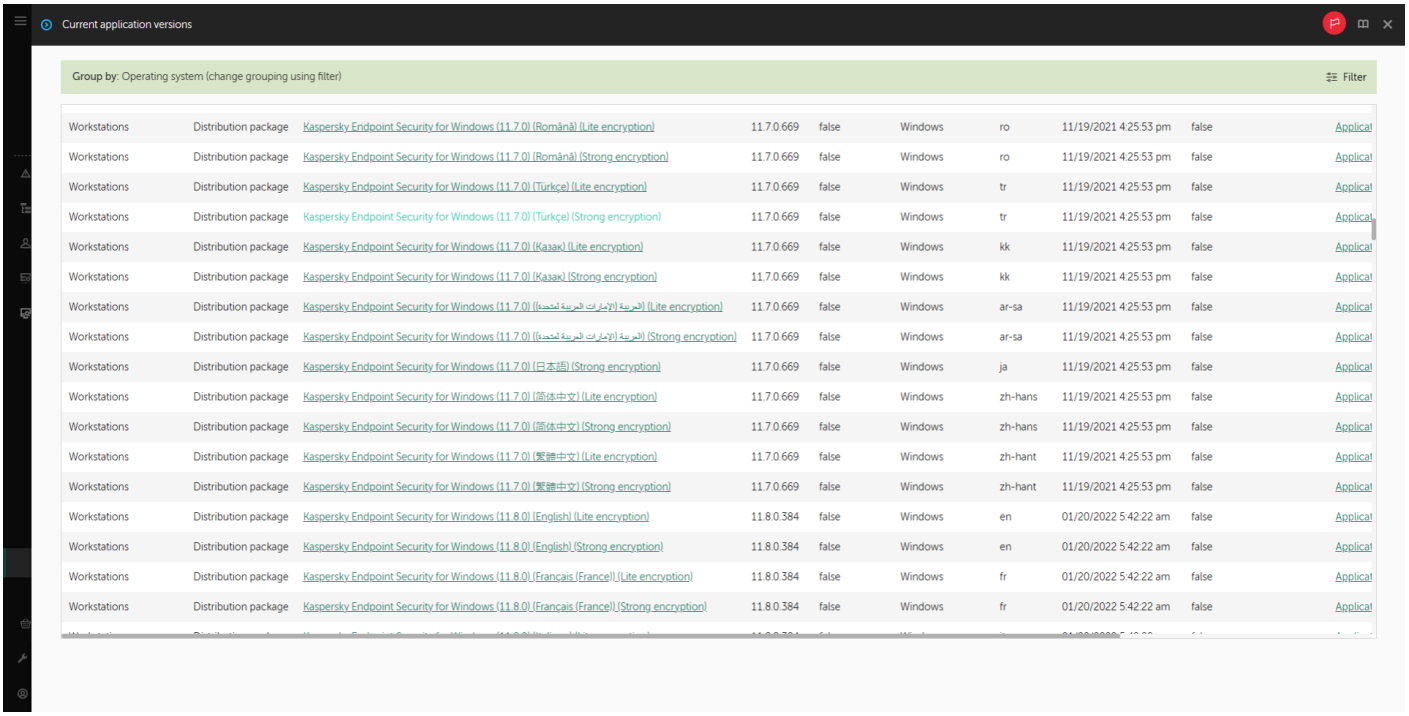
只有在卡巴斯基安全管理中心網頁主控台中才能從檔案建立 Kaspersky Endpoint Security 的安裝套件。




安裝套件類型

## 步驟 2. 安裝套件

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

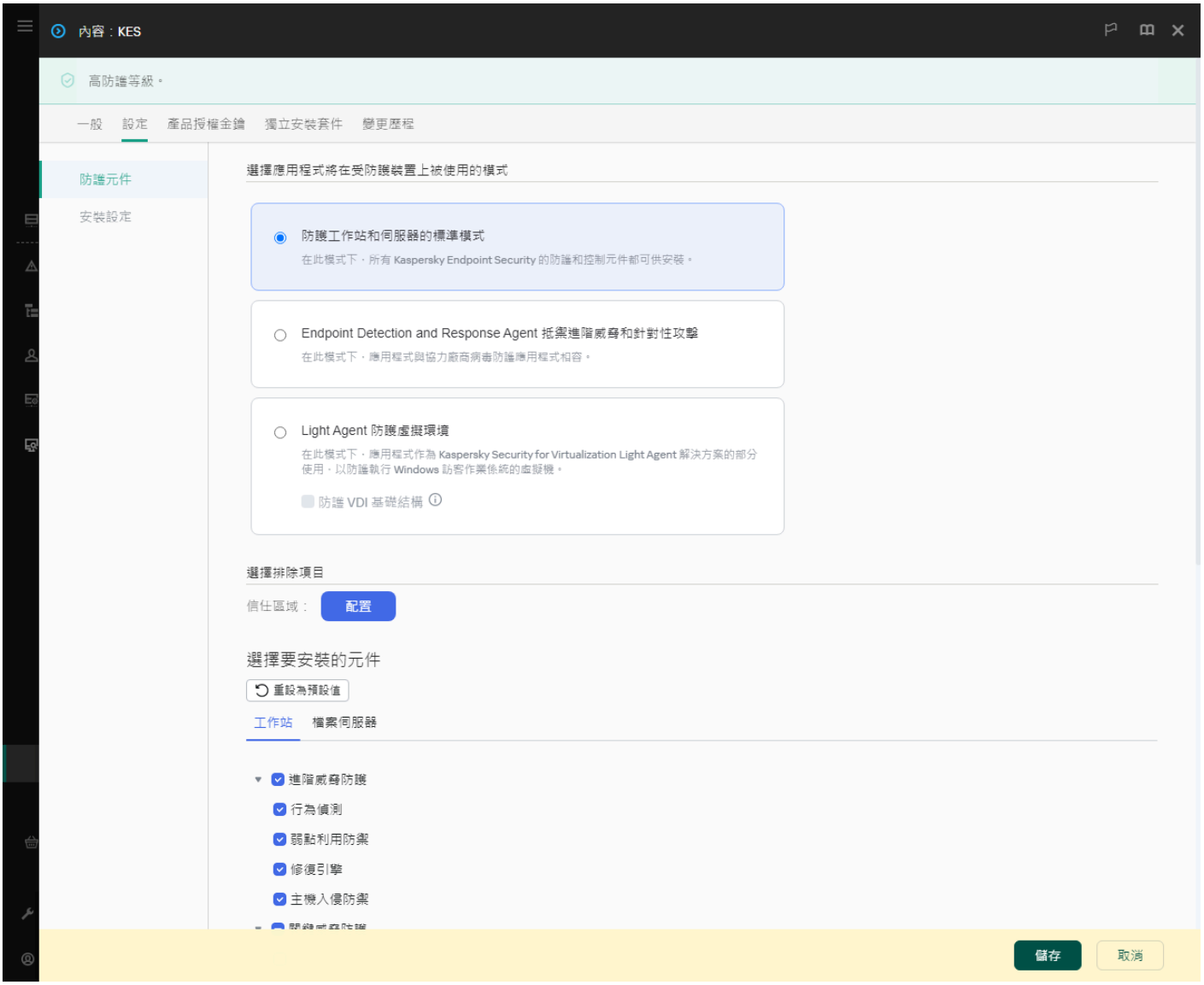



卡巴斯基伺服器上的安裝套件清單

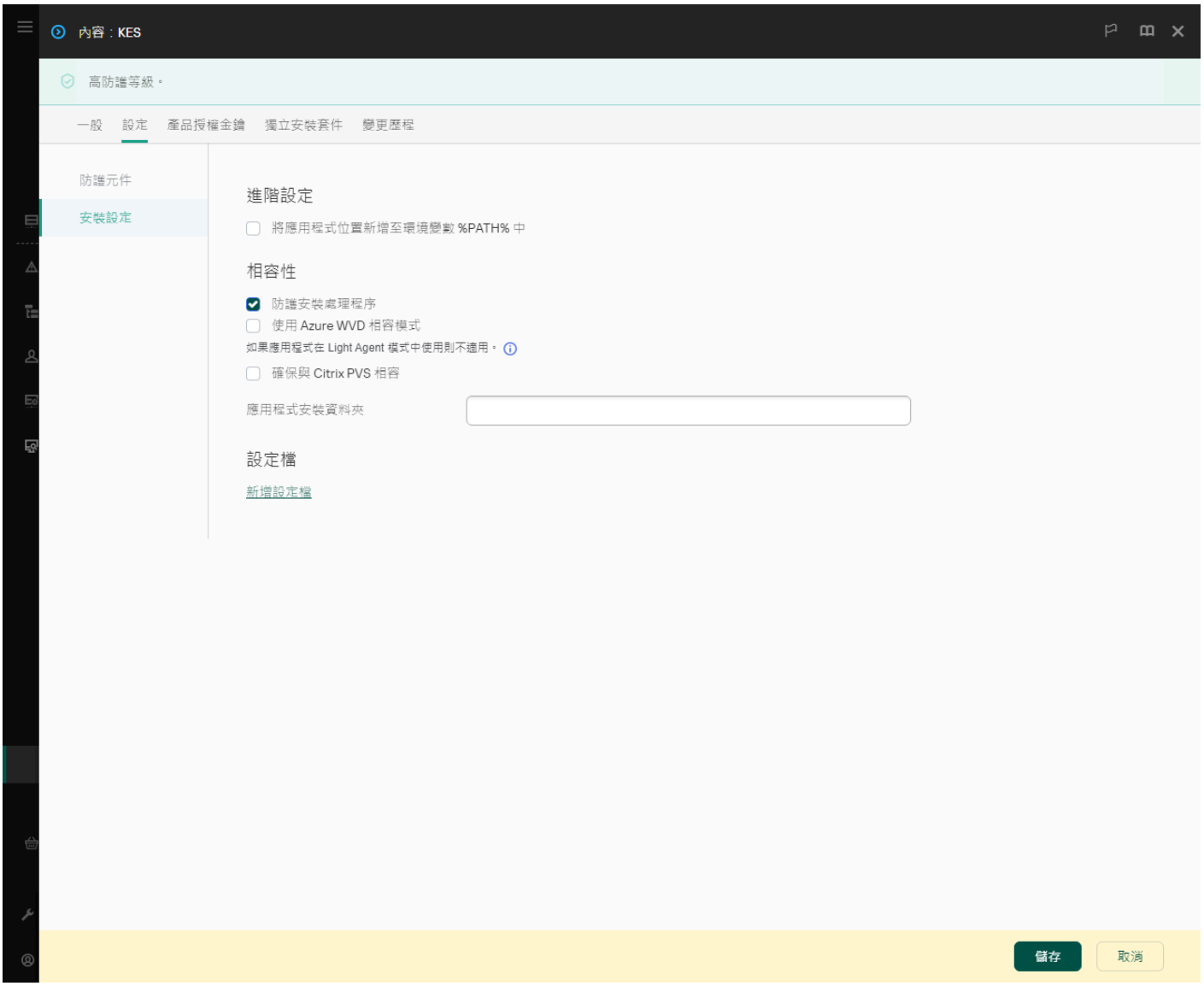
安裝套件將被建立並新增到卡巴斯基安全管理中心中。使用安裝套件，您可以在企業網路電腦上安裝 Kaspersky Endpoint Security 或更新應用程式版本。

在安裝套件設定中，您可以選擇適合不同作業系統類型的應用程式元件。即，安裝套件包括兩套元件：用於工作站的元件和用於伺服器的元件。在部署安裝套件之前，安裝程式會偵測作業系統的類型，並僅安裝您為該作業系統類型選擇的應用程式元件。這樣，您可以為工作站和伺服器使用同一個安裝套件。

安裝套件包含來自管理伺服器儲存區的病毒資料庫。您可以更新安裝套件中的資料庫，以減少在安裝 Kaspersky Endpoint Security 之後更新資料庫時的流量消耗。




安裝套件中包含的元件




安裝套件的安裝設定

安裝套件設定

| 區域 | 描述 |
| --- | --- |
| **防護元件** | **標準模式**預設配置。此配置允許您使用應用程式的所有元件，包括為 Detection and Response 解決方案提供支援的元件。此配置用於全面防護電腦免受各種威脅、網路攻擊和欺詐。<br>**Endpoint Detection and Response Agent**在此配置中，您只能安裝為 Detection and Response 解決方案提供支援的元件： MDR，EDR (KATA)， NDR (KATA)， EDR Expert (on-premise) 以及 KUMA。如果您的組織中與 Kaspersky Detection and Response 解決方案一起部署了協力廠商Endpoint Protection Platform (EPP)，則需要此配置。這使得 Endpoint Detection and Response Agent 配置中的 Kaspersky Endpoint Security 與協力廠商 EPP 應用程式相容。<br>**Light Agent 防護虛擬環境**此配置適用於用作 Kaspersky Security for Virtualization Light Agent 解決方案一部分的應用程式。Light Agent 必須安裝在需要使用此解決方案防護的每台虛擬機上。在此配置中，您無法使用資料加密元件或自適應異常控制。如果您要在將用於建立的虛擬機範本上安裝 Light Agent *非持久虛擬機*，選擇 **防護 VDI 基礎結構** 核取方塊（VDI 代表 Virtual Desktop Infrastructure）。VDI 防護模式有助於最佳化 Kaspersky Endpoint Security 在非持久虛擬機上的效能。在此模式下，Light Agent 會拒絕需要重新啟動虛擬機的應用程式更新。當收到需要重新啟動的應用程式更新時，Light Agent 會產生一個有關需要更新受防護虛擬機範本的事件。 |
| **排除項目** | 從 Kaspersky Endpoint Security 12.6 for Windows 開始，掃描排除項目和受信任應用程式被新增到受信任區域。預先定義的掃描排除項目和受信任應用程式有助於在 SQL 伺服器、Microsoft Exchange 伺服器和 System Center Configuration Manager 上快速設定 Kaspersky Endpoint Security。這意味著您無需在伺服器上為應用程式手動設定受信任區域。<br>從 Kaspersky Endpoint Security 12.8 for Windows 開始，您可以在 Light Agent 模式下安裝應用程式以防護虛擬環境。預定義掃描排除項目和受信任的應用程式可以幫助您在Citrix 和 VMware虛擬環境中快速設定 Kaspersky Endpoint Security。<br>您也可以稍後在政策屬性中配置受信任區域：掃描排除項目和受信任應用程式。 |

| 區域 | 描述 |
| --- | --- |
| **選擇要安裝的元件** | 在此區域中，可以選取將可用的應用程式元件。您可以透過使用*變更應用程式元件*工作在以後變更應用程式元件集合。<br>您可以為工作站和伺服器建立單獨的元件集合。在部署安裝套件之前，安裝程式會偵測作業系統的類型，並僅安裝您為該作業系統類型選擇的應用程式元件。這樣，您可以為工作站和伺服器使用同一個安裝套件。<br>可用元件集合取決於應用程式的配置：<br>**標準模式**<br>預設情況下不安裝"BadUSB 攻擊防護"元件、Detection and Response 元件和資料加密元件。這些元件可在安裝套件設定中新增。<br>**Endpoint Detection and Response Agent**<br>在此配置中，僅 Kaspersky Detection and Response 解決方案的內建代理可用。<br>**Light Agent 防護虛擬環境**<br>在此配置中，您可以使用**標準模式**配置中幾乎所有可用的應用程式元件，資料加密元件和適應性異常控制除外。 |
| **產品授權金鑰** | 在此區段中，您可以啟動應用程式。要啟動應用程式，您必須選擇一個產品授權金鑰。在此之前，您必須將金鑰新增到管理伺服器。有關將金鑰新增到卡巴斯基安全管理中心管理伺服器的詳細資訊，請參閱卡巴斯基安全管理中心說明。 |
| **不相容的應用程式** | 請仔細閱讀不相容應用程式清單並允許移除這些應用程式。如果電腦上安裝了不相容的應用程式，安裝 Kaspersky Endpoint Security 將以出錯結束。 |
| **安裝設定** | **將 avp.com 檔案路徑新增至系統變數 %PATH%**您可以將安裝路徑新增到%PATH%變數中，以方便使用命令列介面。<br>**防護安裝處理程序**安裝防護包括防止分發套件被更換為惡意應用程式、封鎖對 Kaspersky Endpoint Security 安裝資料夾的存取，以及封鎖對包含應用程式金鑰的系統登錄檔部分的存取。但是，如果無法安裝應用程式（例如，藉助 Windows Remote Desktop 執行遠端安裝），我們建議您停用安裝過程的防護。<br>**確保與 Citrix PVS 相容**您可以啟用Citrix Provisioning Services支援以將 Kaspersky Endpoint Security 安裝到虛擬機。<br>**使用 Azure WVD 相容模式**此功能可確保在 Kaspersky Anti Targeted Attack Platform 主控台中正確顯示 Azure 虛擬機狀態。為了監控電腦的效能，Kaspersky Endpoint Security 將遙測資料傳送到 KATA 伺服器。遙測包括電腦的 ID（Sensor ID）。Azure WVD 相容模式允許為這些虛擬機分配永久唯一的Sensor ID。如果關閉相容模式，由於 Azure 虛擬機的工作方式，Sensor ID 可能會在電腦重新啟動後發生變化。這可能會導致主控台上出現重複的虛擬機。<br>**應用程式安裝資料夾**您可以變更用戶端電腦上的 Kaspersky Endpoint Security 安裝路徑。預設情況下，應用程式安裝在 `%ProgramFiles(x86)%\Kaspersky Lab\KES.12.12` 資料夾中。<br>**設定檔**使用預定義設定安裝應用程式。為此，您需要上傳定義 Kaspersky Endpoint Security 設定的檔案。您可以在應用程式的本機介面中建立設定檔。 |

# 更新安裝套件中的資料庫

安裝套件包含來自管理伺服器儲存區的病毒資料庫，這些資料庫在建立安裝套件時是最新的。建立安裝套件後，可以更新安裝套件中的病毒資料庫。這樣可以減少在安裝 Kaspersky Endpoint Security 後更新病毒資料庫時的流量消耗。

要更新管理伺服器儲存區中的病毒資料庫，請使用管理伺服器的"*將更新下載至管理伺服器儲存區*"工作。有關更新管理伺服器儲存區中的病毒資料庫的詳細資訊，請參閱卡巴斯基安全管理中心說明。

您只能在管理主控台和卡巴斯基安全管理中心網頁主控台中更新安裝套件中的資料庫。無法在卡巴斯基安全管理中心雲端主控台中更新安裝套件中的資料庫。

### 如何透過管理主控台 (MMC) 更新安裝套件中的病毒資料庫

1. 開啟卡巴斯基安全管理中心管理主控台。
2. 在主控台樹狀目錄中，選擇**進階 → 遠端安裝 → 安裝套件**資料夾。

   這將開啟已下載到卡巴斯基安全管理中心的安裝套件清單。
3. 開啟安裝套件的內容。
4. 在"**一般**"區域中點擊"**更新資料庫**"。

結果，將從管理伺服器儲存區更新安裝套件中的病毒資料庫。分發套件中包含的bases.cab檔案將被bases資料夾替換。更新套件檔案將位於該資料夾中。

**如何透過網頁主控台更新安裝套件中的病毒資料庫**

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

   這將開啟已下載到網頁主控台的安裝套件清單。

2. 點擊要更新其中的病毒資料庫的 Kaspersky Endpoint Security 安裝套件的名稱。

   安裝套件內容視窗將開啟。

3. 在"**一般資訊**"標籤上，點擊"**更新資料庫**"連結。

結果，將從管理伺服器儲存區更新安裝套件中的病毒資料庫。分發套件中包含的bases.cab檔案將被bases資料夾替換。更新套件檔案將位於該資料夾中。

# 建立遠端安裝工作

*遠端安裝應用程式*工作旨在遠端安裝 Kaspersky Endpoint Security。*遠端安裝應用程式*工作允許您將應用程式的安裝套件佈署到組織中的所有電腦裡。在佈署安裝軟體套件之前，您可以更新安裝套件內的防毒資料庫，並在安裝套件的內容中選取可用的應用程式元件。

**如何在管理主控台 (MMC) 中建立遠端安裝工作**

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

   工作清單開啟。

3. 點擊"**新工作**"。

啟動"工作精靈"。按照精靈的說明進行操作。

步驟 1. 選取工作類型

選擇"**卡巴斯基安全管理中心管理伺服器 → 遠端安裝應用程式**"。

步驟 2. 選取安裝套件

從清單中選取 Kaspersky Endpoint Security 安裝套件。如果清單不包含 Kaspersky Endpoint Security 安裝套件，可以在精靈中建立安裝套件。

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

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

步驟 3. 其他

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

步驟 4. 設定

配置以下其他應用程式設定：

- **強制下載安裝套件**選取應用程式安裝方法：
  - **使用網路代理**如果電腦上未安裝網路代理，將首先使用作業系統的工具安裝網路代理。然後透過網路代理的工具安裝 Kaspersky Endpoint Security。
  - **透過發佈點使用作業系統資源**透過發佈點使用作業系統資源將安裝套件傳輸到用戶端電腦。如果網路中有至少一個發佈點，則可以選取此選項。有關發佈點的詳細資訊，請參閱卡巴斯基安全管理中心說明。
  - **透過管理伺服器使用作業系統資源**檔案將透過管理伺服器使用作業系統資源傳送到用戶端電腦。如果用戶端電腦上未安裝網路代理，但用戶端電腦與管理伺服器在同一網路中，可以選取此選項。
- **透過其他管理伺服器管理的裝置的行為**選取 Kaspersky Endpoint Security 安裝方法。如果網路中安裝了多個管理伺服器，這些管理伺服器可能看到相同的用戶端電腦。例如，這可能導致透過不同的管理伺服器在同一用戶端電腦上多次遠端安裝同一應用程式，或產生其他衝突。
- **如果已經安裝應用程式則不再重新安裝**例如，如果要安裝較早版本的應用程式，則清除此核取方塊。

步驟 5. 選取作業系統重新啟動設定

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

步驟 6. 選取將要對其分配工作的裝置

選取要安裝 Kaspersky Endpoint Security 的電腦。下列選項可用：

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

步驟 7. 選取要執行工作的帳戶

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

步驟 8. 設定工作啟動排程

配置啟動工作的排程，例如，手動或在電腦空閒時。

步驟 9. 定義工作名稱

輸入工作的名稱，例如“*安裝 Kaspersky Endpoint Security for Windows 12.12*”。

步驟 10.完成工作建立

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

**如何在網頁主控台和雲端主控台中建立遠端安裝工作**

1. 在網頁主控台的主視窗中，選擇**資產（裝置）→工作**。
   工作清單開啟。
2. 點擊“**新增**”。

啟動“工作精靈”。按照精靈的說明進行操作。

步驟 1. 配置一般工作設定

配置一般工作設定：

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

步驟 2. 選取要進行安裝的電腦

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

步驟 3. 配置安裝套件

在此步驟中，配置安裝套件：

1. 選取 Kaspersky Endpoint Security for Windows (12.12) 安裝套件。
2. 選取網路代理安裝套件。

   所選版本的網路代理將與 Kaspersky Endpoint Security 一起安裝。*網路代理*可促進管理伺服器與用戶端電腦之間的互動。如果電腦上已安裝網路代理，則不會再次安裝。
3. 在**強制下載安裝套件**區塊中，選擇應用程式安裝方法：
   - **使用網路代理**如果電腦上未安裝網路代理，將首先使用作業系統的工具安裝網路代理。然後透過網路代理的工具安裝 Kaspersky Endpoint Security。
   - **透過發佈點使用作業系統資源**透過發佈點使用作業系統資源將安裝套件傳輸到用戶端電腦。如果網路中有至少一個發佈點，則可以選取此選項。有關發佈點的詳細資訊，請參閱卡巴斯基安全管理中心說明。
   - **透過管理伺服器使用作業系統資源**檔案將透過管理伺服器使用作業系統資源傳送到用戶端電腦。如果用戶端電腦上未安裝網路代理，但用戶端電腦與管理伺服器在同一網路中，可以選取此選項。
4. 在**同時下載的最大數量**欄位中，設定傳送到管理伺服器的安裝套件下載請求數量限制。限制請求數有助於防止網路超載。
5. 在"**安裝嘗試次數上限**"欄位中，設定安裝應用程式嘗試次數限制。如果安裝 Kaspersky Endpoint Security 以出錯結束，工作將自動再次啟動安裝。
6. 如有必要，清除"**如果已經安裝應用程式則不再重新安裝**"核取方塊。例如，這樣可以安裝應用程式的一個先前版本。
7. 如有必要，清除"**下載之前驗證作業系統類型**"核取方塊。這樣可避免在電腦的作業系統不符合軟體需求時下載應用程式分發套件。如果您確定電腦的作業系統符合軟體需求，可以略過此驗證。
8. 如有必要，選中"**在 Active Directory 群組政策中指派安裝套件的安裝**"核取方塊。Kaspersky Endpoint Security 透過網路代理安裝或透過 Active Directory 手動安裝。要安裝網路代理，必須以網域管理員權限執行遠端安裝工作。
9. 如有必要，選中"**提示使用者關閉執行中的應用程式**"核取方塊。安裝 Kaspersky Endpoint Security 會佔用電腦資源。為方便使用者，應用程式安裝精靈會在開始安裝前提示您關閉正在執行的應用程式。這有助於防止其他應用程式執行中端，並防止可能的電腦故障。
10. 在"**透過其他管理伺服器管理的裝置的行為**"塊中，選取 Kaspersky Endpoint Security 安裝方法。如果網路中安裝了多個管理伺服器，這些管理伺服器可能看到相同的用戶端電腦。例如，這可能導致透過不同的管理伺服器在同一用戶端電腦上多次遠端安裝同一應用程式，或產生其他衝突。

步驟 4. 選取要執行工作的帳戶

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

步驟 5. 完成工作建立

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

# 使用精靈在本機安裝應用程式

應用程式安裝精靈的介面包含了對應於應用程式安裝步驟的一系列視窗。請確認您用以執行安裝精靈的使用者帳戶位於管理員群組中。

*使用安裝精靈來安裝應用程式或從上一版本升級應用程式：*

1. 複製"分發套件"資料夾到使用者的電腦。
2. 執行 setup_kes.exe。

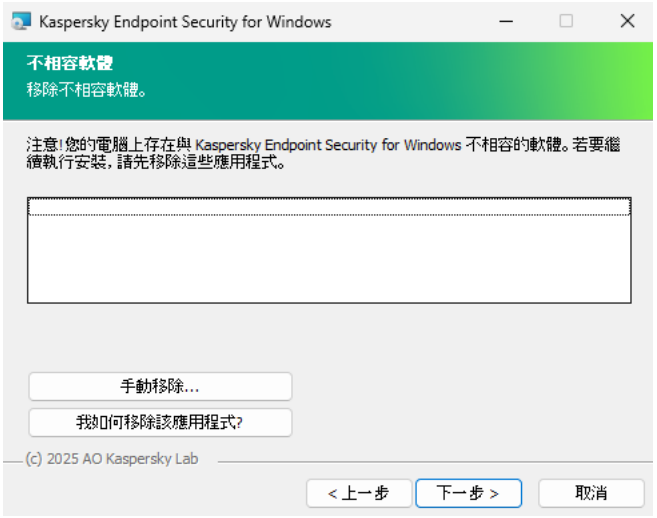
   啟動"安裝精靈"。

準備安裝

在電腦上安裝 Kaspersky Endpoint Security 或從先前版本升級之前，將檢查以下條件：

- 是否存在 Kaspersky Endpoint Security 可能有相容性問題的軟體（軟體清單可在包含在 分發套件中的 incompatible.txt檔案中找到）。
- 無論是否符合軟硬體要求。
- 是否存在 Microsoft .NET Framework
- 確認使用者是否有權限進行安裝。

如果不符合以上任何需求，系統將在電腦螢幕上顯示相關通知。例如，關於不相容軟體的通知（請見下圖）。



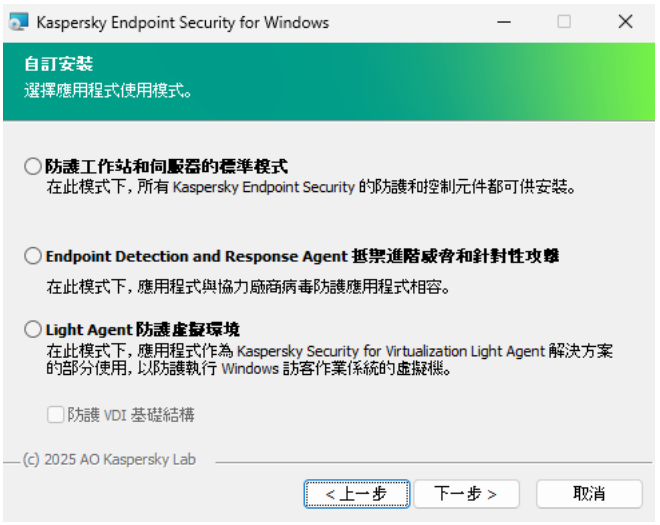

移除不相容軟體

如果電腦符合列出的需求，“安裝精靈”將搜尋應用程式安裝期間可能導致衝突的 Kaspersky 應用程式。如果發現衝突的程式，系統將提示您手動移除它們。

如果偵測到的應用包括以前版本的 Kaspersky Endpoint Security，所有可以被移轉的資料（如啟動資料和應用程式設定）會在安裝 Kaspersky Endpoint Security 12.12 for Windows 時被保留和使用，以前版本的應用程式將被自動刪除。這適用於以下應用程式版本:

- Kaspersky Endpoint Security 11.10.0 for Windows（版本 11.10.0.399）。
- Kaspersky Endpoint Security 11.11.0 for Windows（版本 11.11.0.452）。
- Kaspersky Endpoint Security 12.0 for Windows（版本 12.0.0.465）。
- Kaspersky Endpoint Security 12.1 for Windows（版本 12.1.0.506）。
- Kaspersky Endpoint Security 12.2 for Windows（版本 12.2.0.462）。
- Kaspersky Endpoint Security 12.3 for Windows（版本 12.3.0.493）。
- Kaspersky Endpoint Security 12.4 for Windows（版本 12.4.0.467）。
- Kaspersky Endpoint Security 12.5 for Windows（版本 12.5.0.539）。
- Kaspersky Endpoint Security 12.6 for Windows（版本 12.6.0.438）。
- Kaspersky Endpoint Security 12.7 for Windows（版本 12.7.0.533）。
- Kaspersky Endpoint Security 12.8 for Windows（版本 12.8.0.505）。
- Kaspersky Endpoint Security 12.9 for Windows（版本 12.9.0.384）。
- Kaspersky Endpoint Security 12.10 for Windows（版本 12.10.0.466）。
- Kaspersky Endpoint Security 12.11 for Windows（版本 12.11.0.637）。

Kaspersky Endpoint Security 的配置




選擇應用程式的配置

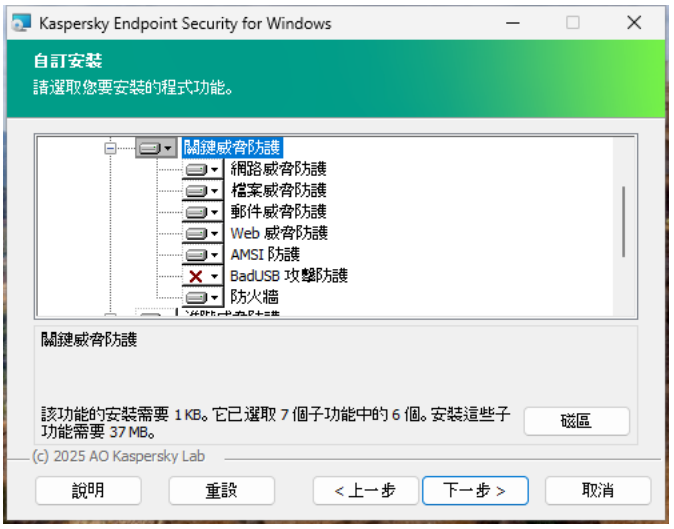
**標準模式**預設配置。此配置允許您使用應用程式的所有元件，包括為 Detection and Response 解決方案提供支援的元件。此配置用於全面防護電腦免受各種威脅、網路攻擊和欺詐。

**Endpoint Detection and Response Agent**在此配置中，您只能安裝為 Detection and Response 解決方案提供支援的元件： MDR，EDR (KATA)， NDR (KATA)， EDR Expert (on-premise) 以及 KUMA。如果您的組織中與 Kaspersky Detection and Response 解決方案一起部署了協力廠商Endpoint Protection Platform (EPP)，則需要此配置。這使得 Endpoint Detection and Response Agent 配置中的 Kaspersky Endpoint Security 與協力廠商 EPP 應用程式相容。

**Light Agent 防護虛擬環境**此配置適用於用作 Kaspersky Security for Virtualization Light Agent 解決方案一部分的應用程式。Light Agent 必須安裝在需要使用此解決方案防護的每台虛擬機上。在此配置中，您無法使用資料加密元件或自適應異常控制。如果您要在將用於建立的虛擬機範本上安裝 Light Agent *非持久虛擬機*，選擇 **防護 VDI 基礎結構** 核取方塊（VDI 代表 Virtual Desktop Infrastructure）。VDI 防護模式有助於最佳化 Kaspersky Endpoint Security 在非持久虛擬機上的效能。在此模式下，Light Agent 會拒絕需要重新啟動虛擬機的應用程式更新。當收到需要重新啟動的應用程式更新時，Light Agent 會產生一個有關需要更新受防護虛擬機範本的事件。

## Kaspersky Endpoint Security 元件

在安裝過程中，您可以選取想要安裝的 Kaspersky Endpoint Security 元件（請見下圖）。“檔案威脅防護”元件是必須安裝的必備元件。您無法取消其安裝。




選擇要安裝的應用程式元件

預設情況下，除了以下元件之外選定安裝所有應用程式元件：

- BadUSB 攻擊防護。
- 資料加密元件。
- Detection and Response 元件。

安裝應用程式後，您可以變更可用的應用程式元件。為此，您需要再次執行安裝精靈，然後選擇變更可用元件。

如果需要安裝 Detection and Response 元件，Kaspersky Endpoint Security 支援以下設定：

- 僅 Endpoint Detection and Response Optimum
- 僅 Endpoint Detection and Response Expert
- 僅 Endpoint Detection and Response (KATA)
- 僅 Network Detection and Response (KATA)
- 僅 Sandbox
- Endpoint Detection and Response Optimum 和 Sandbox
- Endpoint Detection and Response Expert 和 Sandbox
- Endpoint Detection and Response (KATA) 和 Sandbox
- Network Detection and Response (KATA) 和 Endpoint Detection and Response (KATA)
- Network Detection and Response (KATA) 和 Managed Detection and Response

Kaspersky Endpoint Security 在安裝應用程式之前會驗證所選的元件。如果 Detection and Response 元件的選取設定不受支援，則無法安裝 Kaspersky Endpoint Security。

## 選擇安裝應用程式的資料夾

您可以變更用戶端電腦上的 Kaspersky Endpoint Security 安裝路徑。預設情況下，應用程式安裝在 `%ProgramFiles(x86)%\Kaspersky Lab\KES.12.12` 資料夾中。

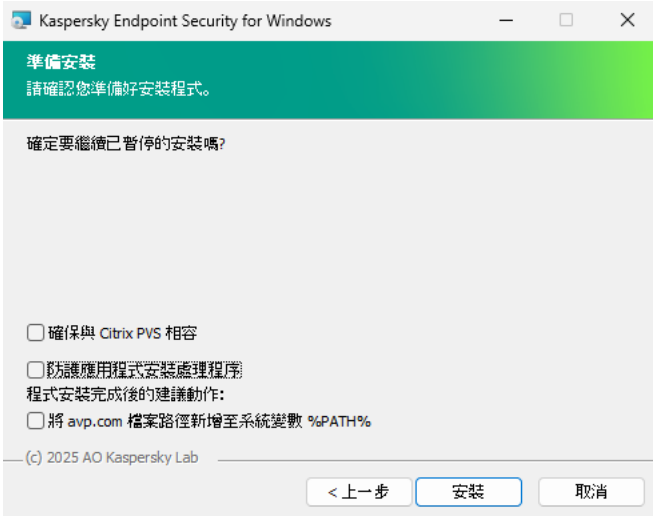
## 配置受信任區域

從 Kaspersky Endpoint Security 12.6 for Windows 開始，掃描排除項目和受信任應用程式被新增到受信任區域。預先定義的掃描排除項目和受信任應用程式有助於在 SQL 伺服器、Microsoft Exchange 伺服器和 System Center Configuration Manager 上快速設定 Kaspersky Endpoint Security。這意味著您無需在伺服器上為應用程式手動設定受信任區域。

從 Kaspersky Endpoint Security 12.8 for Windows 開始，您可以在 Light Agent 模式下安裝應用程式以防護虛擬環境。預定義掃描排除項目和受信任的應用程式可以幫助您在Citrix 和 VMware虛擬環境中快速設定 Kaspersky Endpoint Security。

您也可以稍後在政策屬性中配置受信任區域：掃描排除項目和受信任應用程式。

## 進階設定




*進階應用程式安裝設定*

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

**確保與 Citrix PVS 相容**您可以啟用Citrix Provisioning Services支援以將 Kaspersky Endpoint Security 安裝到虛擬機。

**將 avp.com 檔案路徑新增至系統變數 %PATH%**您可以將安裝路徑新增到%PATH%變數中，以方便使用命令列介面。

# 使用系統中心設定管理器遠端安裝應用程式

這些手冊適用於 System Center Configuration Manager 2012 R2。

*若要使用系統中心設定管理器遠端安裝應用程式：*

1. 開啟設定管理器主控台。
2. 在主控台右側，在"**應用程式管理**"塊中選取"**軟體套件**"。
3. 在控制面板中的主控台右上部分，點擊"**建立軟體套件**"按鈕。
   這會啟動"*新建軟體套件和應用程式精靈*"。
4. 在新建軟體套件和應用程式精靈中：
   a. 在"**軟體套件**"區域中：
      - 在"**名稱**"欄位中輸入安裝套件名稱。
      - 在"**來源資料夾**"欄位中指定包含 Kaspersky Endpoint Security 分發套件的資料夾的路徑。
   b. 在"**應用程式類型**"區域中選取"**標準程式**"選項。
   c. 在"**標準程式**"區域中：
      - 在"**名稱**"欄位中，輸入安裝套件的唯一名稱（例如包含版本的應用程式名稱）。
      - 在"**命令列**"欄位中從命令列中指定 Kaspersky Endpoint Security 安裝選項。
      - 點擊"**瀏覽**"按鈕指定應用程式可執行檔的路徑。
      - 確保**執行模式**清單選擇了**以管理員權限執行**項目。
   d. 在"**要求**"區域中：
      - 如果您希望在安裝 Kaspersky Endpoint Security 之前啟用其他應用程式，則選取"**首先執行其他程式**"核取方塊。
        從"**應用程式**"下拉清單中選取此應用程式，或者點擊"**瀏覽**"按鈕指定此應用程式可執行檔的路徑。
      - 如果希望僅在指定的作業系統中安裝應用程式，請在"**平台要求**"塊中選擇"**此程式只能在指定的平台上執行**"選項。
        在此清單中選取要安裝 Kaspersky Endpoint Security 的作業系統旁的核取方塊。

      此步驟為可選項。
   e. 在"**摘要**"區域中選中所有輸入的設定值，點擊"**下一步**"。

建立的安裝套件將顯示在可用安裝套件清單的"**軟體套件**"區域中。

5. 在安裝套件內容功能表中，選取"**佈署**"。
   這將啟動"*佈署手冊*"。

6. 在佈署精靈中：

   a. 在"**一般**"區域中：

      - 在"**軟體**"欄位中輸入安裝套件的唯一名稱或者點擊"**瀏覽**"按鈕從清單中選取安裝套件。
      - 在"**集合**"欄位中輸入要安裝應用程式的電腦集合的名稱，或者點擊"**瀏覽**"按鈕選取集合。

   b. 在"**包括**"區域中，新增發佈點（有關詳情，請參閱系統中心設定管理器的說明文件）。

   c. 如有必要，在佈署精靈中指定其他設定的值。這些設定是 Kaspersky Endpoint Security 遠端安裝的可選項。

   d. 在"**摘要**"區域中選中所有輸入的設定值，點擊"**下一步**"。

   佈署精靈完成後將建立遠端安裝 Kaspersky Endpoint Security 的工作。

# setup.ini 檔案安裝設定說明

從命令列安裝應用程式或使用 Microsoft Windows 的群組政策編輯器時使用 setup.ini 檔案。要應用 setup.ini 檔案中的設定，請將該檔案放入包含 Kaspersky Endpoint Security 分發套件的資料夾。

僅當在靜默模式下安裝應用程式時使用 setup.ini 檔案。

您無法將路徑新增至 setup.ini 檔案中的 install.cfg 設定檔。如果您只是將此檔案放在包含 Kaspersky Endpoint Security 分發套件的資料夾中，則應用程式還會跳過 install.cfg。如果要套用 install.cfg 設定檔的設定，您需要在以下應用程式安裝指令中指定檔案的路徑：`CONFIGPATH=<path to the configuration file>`。

下載 SETUP.INI 檔案

setup.ini檔案包含以下部分：

- `[Setup]` – 應用程式安裝的一般設定。
- `[Components]` – 選取要以獨立模式安裝的應用程式元件。至少需選取一個元件進行安裝，未選取的元件將不會進行安裝。"檔案威脅防護"是強制性元件，無論此區域中表明的是哪種設定都會安裝在電腦上。
- `[Tasks]` – 選取要包含在 Kaspersky Endpoint Security 工作清單中的工作。如果沒有指定工作，所有工作都包含在Kaspersky Endpoint Security的工作清單中。

`1` 值的替代值為 `yes`、`on`、`enable`、`enabled` 和 `true`。`0` 值的替代值為 `no`、`off`、`disable`、`disabled` 和 `false`。

| 區域 | 參數 | 描述 |
|---|---|---|
| [Setup] | InstallDir | 應用程式安裝資料夾的路徑。 |
| | ActivationCode | Kaspersky Endpoint Security 啟動碼。 |
| | EULA=1 | 接受最終使用者產品授權協議的條款。授權協議的內容包括在 Kaspersky Endpoint Security 分發套件中。<br>必須接受最終使用者產品授權協議才能安裝應用程式或升級應用程式版本。 |
| | PrivacyPolicy=1 | 接受隱私政策。隱私政策的文字包含在 Kaspersky Endpoint Security 分發套件中。<br>要安裝應用程式或升級應用程式版本，您必須接受隱私政策。 |
| | KSN | 接受或拒絕參與卡巴斯基安全網路 (KSN)。如果沒有為此參數設定任何值，在首次啟動 Kaspersky Endpoint Security 時，Kaspersky Endpoint Security 將提示您確認同意或拒絕加入 KSN。可用值：<br>• 1 – 同意加入 KSN。<br>• 0 – 拒絕加入 KSN（預設值）。<br>Kaspersky Endpoint Security 分發套件已針對與卡巴斯基安全網路配合使用進行最佳化。如果您選擇不加入卡巴斯基安全網路，則應該在安裝完成後立即更新 Kaspersky Endpoint Security。 |
| | Login | 設定用於存取 Kaspersky Endpoint Security 功能和設定的使用者名稱（"密碼防護"元件）。該使用者名稱與"Password"和"PasswordArea"設定一起進行設定。預設使用使用者名稱 KLAdmin。 |
| | Password | 指定用於存取 Kaspersky Endpoint Security 功能和設定的密碼（該密碼與"Login"和"PasswordArea"參數一起指定）。<br>如果您指定了口令，但沒有指定帶有 Login 參數的使用者名稱，將預設使用 KLAdmin 使用者名稱。 |
| | PasswordArea | 指定用於存取 Kaspersky Endpoint Security 的密碼範圍。當使用者嘗試執行包含在此範圍中的操作時，Kaspersky Endpoint Security 將提示使用者輸入帳戶憑證（"Login"和"Password"參數）。使用";"字元以指定多個值。<br>可用值：<br>• SET – 修改應用程式設定。<br>• EXIT – 結束應用程式。<br>• DISPROTECT – 停用防護元件並停止掃描工作。<br>• DISPOLICY – 停用卡巴斯基安全管理中心政策。<br>• UNINST – 從電腦中移除應用程式。<br>• DISCTRL – 停用控制元件。<br>• REMOVELIC – 刪除金鑰。<br>• REPORTS – 檢視報告。<br>• EXPORT – 匯出應用程式設定。<br>例如，PasswordArea=SET;PasswordArea=UNINST;PasswordArea=EXIT。 |
| | SelfProtection | 啟用或停用應用程式安裝防護機制。可用值：<br>• 1 – 啟用程式安裝防護機制（預設值）。<br>• 0 – 停用程式安裝防護機制。<br>安裝防護包括防止分發套件被更換為惡意應用程式、封鎖對 Kaspersky Endpoint Security 安裝資料夾的存取，以及封鎖對包含應用程式金鑰的系統登錄檔部分的存取。但是，如果無法安裝應用程式（例如，藉助 Windows Remote Desktop 執行遠端安裝），我們建議您停用安裝過程的防護。 |
| | PROTECTOSSERVICES | 作業係統防護服務功能。作業係統服務防護可防止協力廠商應用程式干擾作業係統服務的運作。此類服務（例如）包括應用程式自動啟動服務。<br>• 1 表示作業係統服務防護已啟用（預設值）。<br>• 0 表示作業係統服務防護已停用。 |

| 區域 | 參數 | 描述 |
| --- | --- | --- |
| | EnableAzureSupport | 啟用或停用 Azure WVD 相容模式。可用值：<br>• 1 – Azure WVD 相容模式被啟用。<br>• 0 – Azure WVD 相容模式被停用（預設值）。<br>此功能可確保在 Kaspersky Anti Targeted Attack Platform 主控台中正確顯示 Azure 虛擬機狀態。為了監控電腦的效能，Kaspersky Endpoint Security 將遙測資料傳送到 KATA 伺服器。遙測包括電腦的 ID（Sensor ID）。Azure WVD 相容模式允許為這些虛擬機分配永久唯一的 Sensor ID。如果關閉相容模式，由於 Azure 虛擬機的工作方式，Sensor ID 可能會在電腦重新啟動後發生變化。這可能會導致主控台上出現重複的虛擬機。 |
| | Reboot=1 | 自動重新啟動電腦（如果安裝或升級應用程式後需要重新啟動）。如果未為此參數設定任何值，則阻止電腦自動重新啟動。<br><br>安裝 Kaspersky Endpoint Security 時，不需要重新啟動。僅當在安裝前必須移除不相容的應用程式時，才需要重新啟動。更新應用程式版本時也可能需要重新啟動。 |
| | AddEnvironment | 在 %PATH% 系統變數中，新增位於 Kaspersky Endpoint Security 安裝資料夾的可執行檔的路徑。可用值：<br>• 1 – 以位於 Kaspersky Endpoint Security 安裝資料夾的可執行檔的路徑補充 %PATH% 系統變數。<br>• 0 – 不以位於 Kaspersky Endpoint Security 安裝資料夾的可執行檔的路徑補充 %PATH% 系統變數。 |
| | AMPPL | 啟用或停用 Kaspersky Endpoint Security 處理程序使用 AM-PPL 技術（Antimalware Protected Process Light）提供的防護。有關 AM-PPL 技術的詳細資訊，請存取 Microsoft 網站。<br>AM-PPL 技術適用於 Windows 10 版本 1703 (RS2) 或更高版本以及 Windows Server 2019 作業系統。<br>可用值：<br>• 1 – 啟用 Kaspersky Endpoint Security 處理程序使用 AM-PPL 技術提供的防護。<br>• 0 – 停用 Kaspersky Endpoint Security 處理程序使用 AM-PPL 技術提供的防護。 |
| | UPGRADEMODE | 應用程式升級模式：<br>• Seamless 意味著用電腦重新啟動升級應用程式（預設值）。<br>• Force 意味著升級應用程式而無需重新啟動。<br>從版本 11.10.0 開始您可以升級應用程式而無需重新啟動。若要升級更早版本的應用程式，您必須重新啟動電腦。從版本 11.11.0 開始您可以安裝修補程式而無需重新啟動。<br>安裝 Kaspersky Endpoint Security 時，不需要重新啟動。因此，應用程式的升級模式將在應用程式設定中指定。您可以在應用程式設定中或政策中變更該參數。<br>當升級已安裝的應用程式時，在 setup.ini 檔案中指定的參數的優先順序比在應用程式設定中或者在命令行指定的參數的優先順序高。例如，如果在 setup.ini 檔案中指定"Force"升級模式，在應用程式設定中指定"Seamless"模式，升級將安裝而不重新啟動（Force）。如果您使用的是 setup.ini 檔案，其中 UPGRADEMODE 參數未指定，安裝程式將使用預設值（Seamless），將安裝升級並重新啟動電腦。 |
| | SetupReg | 啟用將 setup.reg 檔案中的登錄機碼寫入登錄檔。SetupReg: setup.reg 參數值。 |
| | EnableTraces | 啟用或停用應用程式跟蹤。Kaspersky Endpoint Security 在啟動後將偵錯檔案儲存在資料夾 %ProgramData%\Kaspersky Lab\KES.12.12\Traces 中。可用值：<br>• 1 – 跟蹤已啟用。<br>• 0 – 跟蹤已停用（預設值）。 |
| | TracesLevel | 偵錯詳細等級。可用值：<br>• 100（關鍵）。僅包含有關致命錯誤的訊息。<br>• 200（高）。有關所有錯誤的訊息，包括致命錯誤。<br>• 300（診斷）。有關所有錯誤的訊息以及警告。<br>• 400（重要）。所有錯誤訊息、警告和其他資訊。<br>• 500（一般）。有關所有錯誤的訊息和警告，以及有關正常模式下應用程式操作的詳細資訊（預設）。<br>• 600（低）。所有訊息。 |
| | RESTAPI | 透過 REST API 管理應用程式。要透過 REST API 管理應用程式，必須指定使用者名稱（RESTAPI_User 參數）。<br>可用值：<br>• 1 –允許透過 REST API 進行管理。<br>• 0 –封鎖透過 REST API 進行管理（預設值）。<br>要透過 REST API 管理應用程式，必須允許使用管理系統進行管理。要執行此操作，請設定 AdminKitConnector=1 參數。如果透過 REST API 管理應用程式，則無法使用 Kaspersky 的管理系統來管理應用程式。 |

| 區域 | 參數 | 描述 |
| --- | --- | --- |
| | `RESTAPI_User` | 用於透過 REST API 管理應用程式的 Windows 網域帳戶的使用者名稱。只有此使用者可以透過 REST API 管理應用程式。輸入格式為 `<DOMAIN>\<UserName>` 的使用者名稱（例如，`RESTAPI_User=COMPANY\Administrator`）。您只能選擇一個使用者來使用 REST API。<br>新增使用者名稱是透過 REST API 管理應用程式的先決條件。 |
| | `RESTAPI_Port` | 用於透過 REST API 管理應用程式的連接埠。預設情況下使用 6782 連接埠。確保連接埠空閒。 |
| | `RESTAPI_Certificate` | 用於識別請求的憑證（例如，`RESTAPI_Certificate=C:\cert.pem`）。Kaspersky Endpoint Security 與 REST 用戶端進行安全交互需要設定請求識別。為此，您必須安裝憑證並隨後簽署每個請求的承載。 |
| | `StandaloneMode` | 在 Endpoint Detection and Response Agent（EDR Agent）模式下安裝應用程式。*Endpoint Detection and Response Agent* 是一個應用程式，安裝在組織 IT 基礎結構中的各個工作站和伺服器上，用於支援 Kaspersky Managed Detection and Response 和 Kaspersky Anti Targeted Attack Platform 解決方案。EDR Agent 與協力廠商 EPP應用程式相容。這使您可以將協力廠商基礎結構安全工具與卡巴斯基的 Detection and Response 一起使用。<br>若要安裝 EDR Agent，請在 `[Components]` 部分中選擇 `StandaloneKATA`、`StandaloneNDR` 或者 `StandaloneMDR` 元件。EDR Agent 不支援其他應用程式元件。<br>可用值：<br>• `1` 以 EDR Agent 模式安裝應用程式。<br>• `0` 以標準模式（預設）安裝應用程式。 |
| | `KSVLAMode` | 以Light Agent 模式.安裝應用程式。此配置適用於用作 Kaspersky Security for Virtualization Light Agent 解決方案一部分的應用程式。Light Agent 必須安裝在需要使用此解決方案防護的每台虛擬機上。<br>可用值：<br>• `1` 以 Light Agent 模式安裝應用程式。<br>• `0` 以標準模式（預設）安裝應用程式。 |
| | `InstallOnVDI` | 在 Light Agent 模式下安裝應用程式時啟用 VDI 防護模式（`KSVLAMode=1`）。VDI 防護模式有助於最佳化 Kaspersky Endpoint Security 在非持久虛擬機上的效能。在此模式下，Light Agent 會拒絕需要重新啟動虛擬機的應用程式更新。當收到需要重新啟動的應用程式更新時，Light Agent 會產生一個有關需要更新受防護虛擬機範本的事件。<br>可用值：<br>• `1` 啟用 VDI 防護模式。<br>• `0` 停用 VDI 防護模式（預設）。 |
| | `KESExclusions` | 在伺服器上安裝應用程式時新增預定義 掃描排除項 和 受信任應用程式。預先定義的掃描排除項目和受信任應用程式有助於在 SQL 伺服器、Microsoft Exchange 伺服器和 System Center Configuration Manager 上快速設定 Kaspersky Endpoint Security。例如，SQL 伺服器的預定義掃描排除項目包括 MDF 和 LDF 資料庫檔案。這意味著您無需在伺服器上為應用程式手動設定受信任區域。<br>可用值：<br>• `1` 啟用預先定義的掃描排除項目和受信任的應用程式。<br>• `0`停用預先定義的掃描排除項目和受信任的應用程式。 |
| | `LAExclusions` | 在虛擬機上安裝應用程式（Light Agent 模式）時新增預定義 掃描排除項目 和 受信任應用程式。預定義掃描排除項目和受信任的應用程式可以幫助您在Citrix 和 VMware虛擬環境中快速設定 Kaspersky Endpoint Security。<br>可用值：<br>• `1` 啟用預先定義的掃描排除項目和受信任的應用程式。<br>• `0`停用預先定義的掃描排除項目和受信任的應用程式。 |
| | `EnableUniqueSensorID` | 在安裝或更新應用程式期間建立唯一的電腦識別符 (Sensor ID)。Sensor ID 在 Kaspersky Anti Targeted Attack Platform 解決方案中用於識別向伺服器傳送遙測資料的電腦。建立 Sensor ID 時，應用程式使用的演算法會考慮電腦的配置，例如主機板序號。在某些情況下，例如，在虛擬環境中使用應用程式時，Sensor ID 可能會重複。因此， Kaspersky Anti Targeted Attack Platform 無法辨識傳送遙測資料的電腦。要建立唯一的 Sensor ID，需要設定參數 `EnableUniqueSensorID=1`。結果，應用程式將使用不同的演算法來建立 Sensor ID，該演算法會考慮有關電腦的其他資料。這可確保唯一的 Sensor ID。<br>預設情況下，未設定此參數。應用程式在以下情況下繼承 Sensor ID：<br>• 更新應用程式版本；<br>• 將 [KES+KEA] 配置遷移到 [KES+內建代理] 配置。<br>作為應用程式修復的一部分，安裝程式会嘗試繼承Sensor ID。如果 Sensor ID 無法還原，應用程式會建立一個新的 Sensor ID。 |

| 區域 | 參數 | 描述 |
| --- | --- | --- |
| [Components] | ALL | 安裝所有元件。如果指定了參數值 1，所有元件都將安裝，與單個元件的安裝設定無關。<br>因為 Detection and Response 解決方案受支援的方式，Endpoint Detection and Response Optimum 以及 Kaspersky Sandbox 元件安裝在電腦上。Endpoint Detection and Response Expert 和與該配置不相容。 |
| | MailThreatProtection | 郵件威脅防護。 |
| | WebThreatProtection | Web 威脅防護。 |
| | AMSI | AMSI 防護。 |
| | HostIntrusionPrevention | 主機入侵防禦。 |
| | BehaviorDetection | 行為偵測。 |
| | ExploitPrevention | 弱點利用防禦。 |
| | RemediationEngine | 修復引擎。 |
| | Firewall | 防火牆。 |
| | NetworkThreatProtection | 網路威脅防護。 |
| | WebControl | Web 控制。 |
| | DeviceControl | 裝置控制。 |
| | ApplicationControl | 應用程式控制。 |
| | AdaptiveAnomaliesControl | 適應性異常控制。 |
| | CloudDiscovery | Cloud Discovery。 |
| | LogInspector | 記錄檢查 |
| | AntiCryptor | Anti-Cryptor |
| | SystemIntegrityMonitor | 系統完整性監控。 |
| | FileEncryption | "檔案級加密"庫。 |
| | DiskEncryption | "完整磁碟加密"庫。 |
| | BadUSBAttackPrevention | BadUSB 攻擊防護。 |
| | EDR | Endpoint Detection and Response Optimum (EDR Optimum).<br>該元件與 EDR Expert ( EDRCloud ) 和 EDR KATA ( EDRKATA ) 元件不相容。 |
| | EDRCloud | Endpoint Detection and Response Expert (EDR Expert)。<br>元件與 EDR Optimum ( EDR ) 和 EDR KATA ( EDRKATA ) 元件不相容。 |
| | AntiAPT | Endpoint Detection and Response (KATA).<br>該元件與 EDR Expert ( EDRCloud ) 和 EDR Optimum ( EDR ) 元件不相容。 |
| | SB | Kaspersky Sandbox 或 KATA Sandbox。<br>*Kaspersky Sandbox* 是卡巴斯基的獨立 Detection and Response 解決方案。*KATA Sandbox* 是 Kaspersky Anti Targeted Attack Platform 解決方案的一個元件。 |
| | MDR | Managed Detection and Response。 |

| 區域 | 參數 | 描述 |
| --- | --- | --- |
| | NDR | Network Detection and Response (KATA)。<br>該元件與 EDR Expert (EDRCloud) 和 EDR Optimum (EDR) 元件不相容。 |
| | AdminKitConnector | 使用管理系統管理應用程式。例如，管理系統包括卡巴斯基安全管理中心。除了 Kaspersky 管理系統，您還可以使用協力廠商解決方案。Kaspersky Endpoint Security 為此提供了一個 API。<br>可用值：<br>• 1 - 允許在管理系統的幫助下管理應用程式（預設值）。<br>• 0 - 僅允許透過本機介面管理應用程式。 |
| | KUMAIntegration | 與 KUMA 整合。 |
| | StandaloneKATA | 在 Endpoint Detection and Response Agent (EDR Agent) 模式中安裝應用程式以與 Kaspersky Anti Targeted Attack Platform (EDR).解決方案進行整合。 |
| | StandaloneMDR | 在 Endpoint Detection and Response Agent (EDR Agent) 模式中安裝應用程式以與 Kaspersky Managed Detection and Response.進行整合。 |
| | StandaloneNDR | 在 Endpoint Detection and Response Agent (EDR Agent) 模式中安裝應用程式以與 Kaspersky Anti Targeted Attack Platform (NDR).解決方案進行整合。 |
| [Tasks] | ScanMyComputer | 完整掃描工作。可用值：<br>• 1 – 該工作將包含在 Kaspersky Endpoint Security 工作清單中。<br>• 0 – 該工作不會包含在 Kaspersky Endpoint Security 工作清單中。 |
| | ScanCritical | 關鍵區域掃描工作。可用值：<br>• 1 – 該工作將包含在 Kaspersky Endpoint Security 工作清單中。<br>• 0 – 該工作不會包含在 Kaspersky Endpoint Security 工作清單中。 |
| | Updater | 更新工作。可用值：<br>• 1 – 該工作將包含在 Kaspersky Endpoint Security 工作清單中。<br>• 0 – 該工作不會包含在 Kaspersky Endpoint Security 工作清單中。 |

# 變更程式元件

在安裝應用程式期間，您可以選擇變更可用的元件。您可以透過以下方式變更可用的應用程式元件：

- 本機使用安裝精靈。

  使用 Windows 作業系統的一般方法（透過“主控台”）變更應用程式元件。執行應用程式安裝精靈，然後選取用於變更可用應用程式元件的選項。按照螢幕上的說明進行操作。

  如果應用程式是透過卡巴斯基安全管理中心安裝的，則此方法不可用。您只能在本機安裝應用程式之後在控制面板中變更應用程式元件的選擇。

- 遠端使用卡巴斯基安全管理中心。

  “*變更應用程式元件*”工作允許您在安裝應用程式後變更 Kaspersky Endpoint Security 元件。

變更應用程式元件時，請考慮以下特殊注意事項：

- 在執行 Windows Server 的電腦上，無法安裝 Kaspersky Endpoint Security 的所有元件（例如，“適應性異常控制”元件無法使用）。

- 如果電腦上的硬碟受“完整磁碟加密 (FDE)”防護，則無法刪除“完整磁碟加密”元件。要刪除“完整磁碟加密”元件，請解密電腦的所有硬碟。

- 如果電腦具有加密的檔案 (FLE) 或使用者使用加密的卸除式磁碟機（FDE 或 FLE），則在刪除資料加密元件之後將無法存取檔案和卸除式磁碟機。您可以透過重新安裝資料加密元件來存取這些檔案和卸除式磁碟機。

- 如果應用程式在 VDI 基礎結構中以 Light Agent 模式安裝，不支援變更設定元件。

**如何在管理主控台 (MMC) 中新增或刪除應用程式元件**

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

2. 點擊**"新工作"**。

啟動"工作精靈"。按照精靈的說明進行操作。

步驟 1. 選取工作類型

選取**"Kaspersky Endpoint Security for Windows (12.12)"→"選擇要安裝的元件"**。

步驟 2. 變更應用程式元件的工作設定

選擇應用程式配置：

- **防護工作站和伺服器的標準模式**預設配置。此配置允許您使用應用程式的所有元件，包括為 Detection and Response 解決方案提供支援的元件。此配置用於全面防護電腦免受各種威脅、網路攻擊和欺詐。

- **Endpoint Detection and Response Agent 抵禦進階威脅和針對性攻擊**在此配置中，您只能安裝為 Detection and Response 解決方案提供支援的元件： MDR，EDR (KATA)， NDR (KATA)， EDR Expert (on-premise) 以及 KUMA。如果您的組織中與 Kaspersky Detection and Response 解決方案一起部署了協力廠商Endpoint Protection Platform (EPP)，則需要此配置。這使得 Endpoint Detection and Response Agent 配置中的 Kaspersky Endpoint Security 與協力廠商 EPP 應用程式相容。

  當變更 EDR 代理的應用程式配置以使其與 MDR 協同工作時，請確保已啟用負責接收遙測資料的元件。

- **Light Agent 防護虛擬環境**此配置適用於用作 Kaspersky Security for Virtualization Light Agent 解決方案一部分的應用程式。Light Agent 必須安裝在需要使用此解決方案防護的每台虛擬機上。在此配置中，您無法使用資料加密元件或自適應異常控制。如果您要在將用於建立的虛擬機範本上安裝 Light Agent *非持久虛擬機*，選擇 **防護 VDI 基礎結構** 核取方塊（VDI 代表 Virtual Desktop Infrastructure）。VDI 防護模式有助於最佳化 Kaspersky Endpoint Security 在非持久虛擬機上的效能。在此模式下，Light Agent 會拒絕需要重新啟動虛擬機的應用程式更新。當收到需要重新啟動的應用程式更新時，Light Agent 會產生一個有關需要更新受防護虛擬機範本的事件。

選取將在使用者電腦上可用的應用程式元件。

### 步驟 3. 進階設定

為工作配置進階設定（請參閱下表）。

### 步驟 4. 選取將要對其分配工作的裝置

選取將要執行工作的電腦。下列選項可用：

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

### 步驟 5. 設定工作啟動排程

配置啟動工作的排程，例如，手動或在電腦空閒時。

### 步驟 6. 定義工作名稱

輸入工作的名稱，例如，“*新增應用程式控制元件*”。

### 步驟 7. 完成工作建立

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

**如何在網頁主控台和雲端主控台中新增或刪除應用程式元件**

1. 在網頁主控台的主視窗中，選擇**資產（裝置）→ 工作**。
   工作清單開啟。
2. 點擊“**新增**”。

啟動“工作精靈”。按照精靈的說明進行操作。

### 步驟 1. 配置一般工作設定

配置一般工作設定：

1. 在"**應用程式**"下拉式清單中，選取"**Kaspersky Endpoint Security for Windows 12.12.0**"。
2. 在"**工作類型**"下拉式清單中，選取"**變更應用程式元件**"。
3. 在"**工作名稱**"欄位中，輸入簡要說明，例如，"*新增應用程式控制元件*"。
4. 在"**要將工作指派給的裝置**"塊中，選取工作範圍。

### 步驟 2. 選取將要對其分配工作的裝置

選取將要執行工作的電腦。例如，選取單獨的管理群組或構建一個選項。

### 步驟 3. 完成工作建立

選擇 **建立完成時開啟工作詳情** 核取方塊並完成精靈。

在工作內容中，選取"**應用程式設定**"區域。接下來，選擇應用程式的配置：

- **防護工作站和伺服器的標準模式**預設配置。此配置允許您使用應用程式的所有元件，包括為 Detection and Response 解決方案提供支援的元件。此配置用於全面防護電腦免受各種威脅、網路攻擊和欺詐。
- **Endpoint Detection and Response Agent 抵禦進階威脅和針對性攻擊**在此配置中，您只能安裝為 Detection and Response 解決方案提供支援的元件： MDR，EDR (KATA)， NDR (KATA)， EDR Expert (on-premise) 以及 KUMA。如果您的組織中與 Kaspersky Detection and Response 解決方案一起部署了協力廠商Endpoint Protection Platform (EPP)，則需要此配置。這使得 Endpoint Detection and Response Agent 配置中的 Kaspersky Endpoint Security 與協力廠商 EPP 應用程式相容。

  當變更 EDR 代理的應用程式配置以使其與 MDR 協同工作時，請確保已啟用負責接收遙測資料的元件。

- **Light Agent 防護虛擬環境**此配置適用於用作 Kaspersky Security for Virtualization Light Agent 解決方案一部分的應用程式。Light Agent 必須安裝在需要使用此解決方案防護的每台虛擬機上。在此配置中，您無法使用資料加密元件或自適應異常控制。如果您要在將用於建立的虛擬機範本上安裝 Light Agent *非持久虛擬機*，選擇 **防護 VDI 基礎結構** 核取方塊（VDI 代表 Virtual Desktop Infrastructure）。VDI 防護模式有助於最佳化 Kaspersky Endpoint Security 在非持久虛擬機上的效能。在此模式下，Light Agent 會拒絕需要重新啟動虛擬機的應用程式更新。當收到需要重新啟動的應用程式更新時，Light Agent 會產生一個有關需要更新受防護虛擬機範本的事件。

選取將在使用者電腦上可用的應用程式元件。為工作配置進階設定（請參閱下表）。

結果，使用者電腦上的 Kaspersky Endpoint Security 元件集將在靜默模式下變更。可用元件的設定將顯示在應用程式的本機介面中。應用程式中未包括的元件將被停用，並且這些元件的設定無法使用。

安裝、更新或解除安裝 Kaspersky Endpoint Security 時，可能會出現錯誤。有關解決這些錯誤的更多資訊，請參閱技術支援知識庫。

工作的進階設定

| 參數 | 描述 |
| --- | --- |
| **工作設定** | **檢查不相容的協力廠商應用程式**預設情況下，Kaspersky Endpoint Security 檢查已安裝應用程式的相容性。incompatible.txt 檔案提供可能引起相容性問題的軟體清單。檔案包括在分發套件中。如果啟用了掃描已安裝的軟體，當偵測到清單中的應用程式時，Kaspersky Endpoint Security 會停止該工作。如果協力廠商軟體的供應商文件聲稱與Endpoint Protection Platform（EPP）相容，您可以停用掃描已安裝的軟體。<br>**移除不相容的協力廠商應用程式**變更元件集之前，自動移除incompatible.txt檔案中所列的應用程式。如果啟用此功能，Kaspersky Endpoint Security 會嘗試移除可能導致相容性問題的應用程式，以便繼續工作。<br>**使用 Azure WVD 相容模式**此功能可確保在 Kaspersky Anti Targeted Attack Platform 主控台中正確顯示 Azure 虛擬機狀態。為了監控電腦的效能，Kaspersky Endpoint Security 將遙測資料傳送到 KATA 伺服器。遙測包括電腦的 ID（Sensor ID）。Azure WVD 相容模式允許為這些虛擬機分配永久唯一的Sensor ID。如果關閉相容模式，由於 Azure 虛擬機的工作方式，Sensor ID 可能會在電腦重新啟動後發生變化。這可能會導致主控台上出現重複的虛擬機。 |
| **排除項目** | 從 Kaspersky Endpoint Security 12.6 for Windows 開始，掃描排除項目和受信任應用程式被新增到受信任區域。預先定義的掃描排除項目和受信任應用程式有助於在 SQL 伺服器、Microsoft Exchange 伺服器和 System Center Configuration Manager 上快速設定 Kaspersky Endpoint Security。這意味著您無需在伺服器上為應用程式手動設定受信任區域。<br>從 Kaspersky Endpoint Security 12.8 for Windows 開始，您可以在 Light Agent 模式下安裝應用程式以防護虛擬環境。預定義掃描排除項目和受信任的應用程式可以幫助您在Citrix 和 VMware虛擬環境中快速設定 Kaspersky Endpoint Security。<br>您也可以稍後在政策屬性中配置受信任區域：掃描排除項目和受信任應用程式。 |
| **單獨模式/組合模式** | 您可以為工作站和伺服器建立單獨的元件集合 – **單獨模式**。在部署安裝套件之前，安裝程式會偵測作業系統的類型，並僅安裝您為該作業系統類型選擇的應用程式元件。這樣，您可以為工作站和伺服器使用同一個安裝套件。<br>**組合模式** 提供工作站和伺服器的常用元件清單。單個元件的可用性取決於作業系統類型。在這種模式下，我們建議為工作站建立單獨的安裝套件，為伺服器建立單獨的安裝套件。僅在標準模式下可配置安裝套件中的常用元件清單。 |
| **設定用於修改應用程式元件集的密碼** | 管理員通常啟用密碼防護以限制對 Kaspersky Endpoint Security 的存取。也就是說，要修改應用程式元件的選擇，您必須輸入具有**移除/修改/還原應用程式**權限的使用者認證。例如，您可以使用 KLAdmin 帳戶。 |
| **使用密碼解除安裝 Kaspersky Endpoint Agent 和 Kaspersky Security for Windows Server** | 管理員通常在這些工作的設定中啟用密碼防護以限制對 Kaspersky Endpoint Agent (KEA) 和 Kaspersky Security for Windows Server (KSWS) 的存取。也就是說，如果您從 [KES+KEA] 配置遷移到 [KES+built-in agent]，或者如果您從 KSWS 遷移到 KES，則必須輸入密碼才能刪除這些應用程式。 |

# 升級先前版本的應用程式

將以前版本的應用程式更新為較新版本時，請考慮以下事項：

- 當地語係化新版本的 Kaspersky Endpoint Security 必須比對已安裝版本的應用程式的當地語係化。如果應用程式的當地語係化不比對，則應用程式升級會完成但有錯誤。
- 建議在開始更新之前結束所有活動的應用程式。
- 在更新之前，Kaspersky Endpoint Security 會封鎖完整磁碟加密功能。如果無法鎖定完整磁碟加密，升級安裝將不會啟動。更新應用程式後，將還原完整磁碟加密功能。

Kaspersky Endpoint Security 支援以下應用程式版本的更新：

- Kaspersky Endpoint Security 11.10.0 for Windows（版本 11.10.0.399）。
- Kaspersky Endpoint Security 11.11.0 for Windows（版本 11.11.0.452）。

- Kaspersky Endpoint Security 12.0 for Windows（版本 12.0.0.465）。
- Kaspersky Endpoint Security 12.1 for Windows（版本 12.1.0.506）。
- Kaspersky Endpoint Security 12.2 for Windows（版本 12.2.0.462）。
- Kaspersky Endpoint Security 12.3 for Windows（版本 12.3.0.493）。
- Kaspersky Endpoint Security 12.4 for Windows（版本 12.4.0.467）。
- Kaspersky Endpoint Security 12.5 for Windows（版本 12.5.0.539）。
- Kaspersky Endpoint Security 12.6 for Windows（版本 12.6.0.438）。
- Kaspersky Endpoint Security 12.7 for Windows（版本 12.7.0.533）。
- Kaspersky Endpoint Security 12.8 for Windows（版本 12.8.0.505）。
- Kaspersky Endpoint Security 12.9 for Windows（版本 12.9.0.384）。
- Kaspersky Endpoint Security 12.10 for Windows（版本 12.10.0.466）。
- Kaspersky Endpoint Security 12.11 for Windows（版本 12.11.0.637）。

安裝、更新或解除安裝 Kaspersky Endpoint Security 時，可能會出現錯誤。有關解決這些錯誤的更多資訊，請參閱技術支援知識庫。

## 應用程式升級方法

可以透過以下方式在電腦上更新 Kaspersky Endpoint Security：

- 使用卡巴斯基更新服務 (Seamless Update – SMU)。
- 本機使用安裝精靈。
- 本機使用命令列。
- 遠端使用卡巴斯基安全管理中心。
- 遠端透過 Microsoft Windows 群組政策管理編輯器（有關詳細資訊，請造訪 Microsoft 技術支援網站）。
- 遠端使用系統中心配置管理器。

如果公司網路中部署的應用程式所包含的元件集與預設元件集不同，則透過管理主控台 (MMC) 更新應用程式與透過網頁主控台和雲端主控台更新應用程式也有所差異。在更新 Kaspersky Endpoint Security 時，應考慮以下事項：

- 卡巴斯基安全管理中心網頁主控台或卡巴斯基安全管理中心雲端主控台。

  如果使用預設元件集為新版本的應用程式建立安裝套件，則將不會變更使用者電腦上的元件集。要為 Kaspersky Endpoint Security 使用預設元件集，您需要開啟安裝套件內容，變更元件集，然後還原為原始元件集並儲存變更。

- 卡巴斯基安全管理中心管理主控台。

  更新後的應用程式元件集將與安裝套件中的元件集相符。也就是說，例如，如果新版本的應用程式採用預設元件集，則將從電腦中刪除 BadUSB 攻擊防護元件，因為此元件已從預設元件集中排除。要繼續為應用程式使用與更新之前相同的元件集，請在安裝套件設定中選擇所需的元件。

# 升級應用程式而無需重新啟動

升級應用程式而無需重新啟動可以在更新應用程式版本時提供不受中斷的伺服器作業。

升級應用程式而無需重新啟動有以下限制：

- 從版本 11.10.0 開始您可以升級應用程式而無需重新啟動。若要升級更早版本的應用程式，您必須重新啟動電腦。
- 從版本 11.11.0 開始您也可以升級應用程式而無需重新啟動。為較早版本的應用程式安裝修補可能需要重新啟動電腦。
- 升級應用程式而無需重新啟動不可在啟用了資料加密（卡巴斯基加密 (FDE)，BitLocker，檔案級加密 (FLE)）的電腦上使用。若要在啟用了資料加密的電腦上升級應用程式，必須重新啟動電腦。
- 如果不重新啟動，則無法在虛擬機上升級應用程式。要升級虛擬機上的應用程式，您必須重新啟動虛擬機。

升級應用程式、安裝修補程式、變更應用程式元件集或還原後，Kaspersky Endpoint Security 將重新啟動以開始使用新版本。重新啟動 Kaspersky Endpoint Security 可能需要最多一分鐘。在該期間電腦防護等級降低。重新啟動應用程式後，電腦的防護等級將會還原。

**如何在管理主控台 (MMC) 中選擇應用程式升級模式**

1. 在網頁主控台的主視窗中，選擇**資產（裝置）→政策和設定檔**。
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**應用程式更新設定**塊中，選擇或清空**安裝應用程式更新而不重新啟動**核取方塊以配置應用程式升級模式。
6. 儲存變更。

1. 在卡巴斯基安全管理中心管理主控台樹狀目錄中，選取**政策**。
2. 選擇必要的政策並點擊以開啟政策內容。
3. 在政策視窗中，選擇"**一般設定 → 應用程式設定**"。
4. 在**進階設定**塊中，選擇或清空**安裝應用程式更新而不重新啟動**核取方塊以配置應用程式升級模式。
5. 儲存變更。

**如何在應用程式介面中選擇應用程式升級模式**

1. 在"應用程式主視窗"中，點擊⚙按鈕。
2. 在應用程式設定視窗中，選取"**一般設定**"→"**應用程式設定**"。




Kaspersky Endpoint Security for Windows 設定

3. 在**一般**塊中，選擇或清空**安裝更新而不重新啟動電腦**核取方塊以配置應用程式升級模式。
4. 儲存變更。

結果，在升級應用程式而無需重新啟動後，電腦上將安裝兩個版本的應用程式。安裝程式將安裝新版本的應用程式以分開 Program Files 和 Program Data 資料夾中的子資料夾。安裝程式也會為新版本的應用程式建立一個單獨的登錄機碼。您不必手動移除先前版本的應用程式。電腦重新啟動時，先前版本將被自動移除。

您可以在卡巴斯基安全管理中心主控台中使用卡巴斯基應用程式版本報告檢查 Kaspersky Endpoint Security 升級狀況。

# 應用程式的 SMU 更新

若要使用卡巴斯基更新服務更新應用程式 (Seamless Update; SMU)，您不需要執行安裝程式，這與 其他更新方法相反。Kaspersky Endpoint Security 獲得新版本應用程式的 來源與病毒資料庫一樣。

SMU 更新可讓將組織中所有電腦上的應用程式更新至最新版本。在套用 SMU 更新之前，我們建議先在幾台電腦上測試新版本的應用程式。為此，您必須手動更新這些電腦上的應用程式（例如，在本機上使用 設定精靈）。執行 SMU 更新時無法選擇單獨的電腦。

應用程式的更新時間表由卡巴斯基工作人員確定。為了確保新版本的應用程式順利執行，卡巴斯基逐步提供更新。這意味著您可能會在新版本發布後兩個月後獲得 SMU 更新。

您可以使用 *資料庫和應用程式模組更新* 工作管理應用程式的 SMU 更新。要將應用程式的新版本包含在與病毒資料庫相同的套件中，您必須允許更新 *應用程式模組* 在 *資料庫和應用程式模組更新* 工作設定。此外在 *資料庫和應用程式模組更新* 工作設定中，您可以 允許更新應用程式而無需重新啟動。

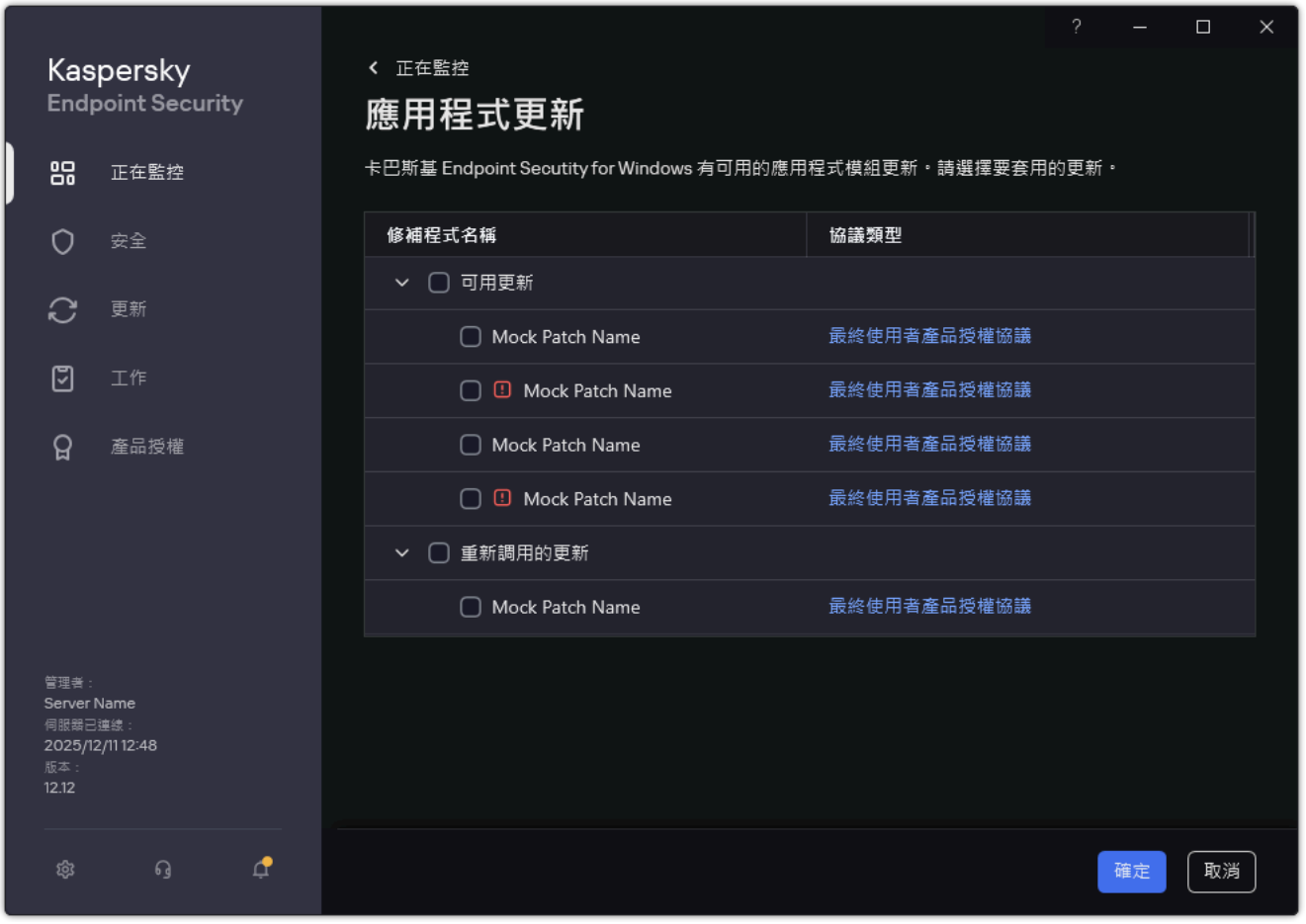
應用程式 SMU 更新的步驟

1. **應用程式的新版本發布後，卡巴斯基會分發更新。**
2. **使用者批准應用程式的更新。**

   如果電腦已連線至卡巴斯基安全管理中心，則更新可以在卡巴斯基安全管理中的心**卡巴斯基資料庫和應用程式模組更新** 部分中找到。有關批准更新的詳細資訊，請參閱卡巴斯基安全管理中心說明。

   如果電腦未連線到卡巴斯基安全管理中心，則可以在應用程式介面的通知部分中找到更新： 。若要批准更新，請選擇應用程式的版本並接受協議的條款和條件（請參閱下圖）。
3. **Kaspersky Endpoint Security 按照配置的時間表執行 *資料庫和應用程式模組更新* 工作。**

結果，Kaspersky Endpoint Security 會以"靜默"模式更新應用程式。




可用的應用程式更新

# 移除應用程式

移除 Kaspersky Endpoint Security 將導致電腦和使用者資訊失去對威脅的防護。

安裝、更新或解除安裝 Kaspersky Endpoint Security 時，可能會出現錯誤。有關解決這些錯誤的更多資訊，請參閱技術支援知識庫。

## 用卡巴斯基安全管理中心移除應用程式

您可以使用“*遠端解除安裝應用程式*”工作遠端移除應用程式。執行該工作時，Kaspersky Endpoint Security 會將應用程式移除實用程式下載到使用者的電腦。完成應用程式的移除後，將自動刪除該實用程式。

**如何透過管理主控台 (MMC) 刪除應用程式**

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

   啟動“工作精靈”。按照精靈的說明進行操作。

### 步驟 1. 選取工作類型

選擇“**卡巴斯基安全管理中心管理伺服器 → 進階 → 遠端解除安裝應用程式**”。

### 步驟 2. 選取要刪除的應用程式

選擇“**移除卡巴斯基安全管理中心支援的應用程式**”。

### 步驟 3. 應用程式移除的工作設定

選取“**Kaspersky Endpoint Security for Windows (12.12)**”。

### 步驟 4. 移除實用程式設定

配置以下其他應用程式設定：

- **強制下載解除安裝實用程式**選取實用程式傳送方式：
  - **使用網路代理**如果電腦上未安裝網路代理，將首先使用作業系統的工具安裝網路代理。然後透過網路代理的工具移除 Kaspersky Endpoint Security。
  - **透過管理伺服器使用作業系統資源**實用程式將透過管理伺服器使用作業系統資源傳送到用戶端電腦。如果用戶端電腦上未安裝網路代理，但用戶端電腦與管理伺服器在同一網路中，可以選取此選項。
  - **透過發佈點使用作業系統資源**透過發佈點使用作業系統資源將實用程式傳輸到用戶端裝置。如果網路中有至少一個發佈點，則可以選取此選項。有關發佈點的詳細資訊，請參閱卡巴斯基安全管理中心說明。
- **下載之前驗證作業系統類型**如有必要，清除此核取方塊。這樣可避免在電腦的作業系統不符合軟體需求時下載移除實用程式。如果您確定電腦的作業系統符合軟體需求，可以略過此驗證。

如果應用程式移除操作受密碼防護，請執行以下操作：

1. 選擇"**使用解除安裝密碼**"核取方塊。
2. 點擊"**編輯**"按鈕。
3. 輸入 KLAdmin 帳戶密碼。

### 步驟 5. 選取作業系統重新啟動設定

移除應用程式後，需要重新啟動。選取將要執行之用於重新啟動電腦的操作。

### 步驟 6. 選取將要對其分配工作的裝置

選取將要執行工作的電腦。下列選項可用：

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

步驟 7. 選取要執行工作的帳戶

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

步驟 8. 設定工作啟動排程

配置啟動工作的排程，例如，手動或在電腦空閒時。

步驟 9. 定義工作名稱

輸入工作的名稱，例如"*移除 Kaspersky Endpoint Security 12.12*"。

步驟 10.完成工作建立

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

應用程式將以靜默模式移除。

**如何透過網頁主控台和雲端主控台刪除應用程式**

1. 在網頁主控台的主視窗中，選擇**資產（裝置）→ 工作**。
   工作清單開啟。
2. 點擊**"新增"**。

啟動"工作精靈"。按照精靈的說明進行操作。

步驟 1. 配置一般工作設定

配置一般工作設定：

1. 在**"應用程式"**下拉清單中，選取**"卡巴斯基安全管理中心"**。
2. 在**"工作類型"**下拉式清單中，選取**"遠端解除安裝應用程式"**。
3. 在**"工作名稱"**欄位中，輸入簡要說明，例如，"*移除技術支援電腦中的 Kaspersky Endpoint Security*"。
4. 在**"要將工作指派給的裝置"**塊中，選取工作範圍。

### 步驟 2. 選取將要對其分配工作的裝置

選取將要執行工作的電腦。例如，選取單獨的管理群組或構建一個選項。

### 步驟 3. 配置應用程式移除設定

在此步驟中，配置應用程式移除設定：

1. 選擇**解除安裝受管理應用程式**類型。
2. 選擇"**Kaspersky Endpoint Security for Windows**"。
3. **強制下載解除安裝實用程式**選取實用程式傳送方式：
   - **使用網路代理**如果電腦上未安裝網路代理，將首先使用作業系統的工具安裝網路代理。然後透過網路代理的工具移除 Kaspersky Endpoint Security。
   - **透過管理伺服器使用作業系統資源**實用程式將透過管理伺服器使用作業系統資源傳送到用戶端電腦。如果用戶端電腦上未安裝網路代理，但用戶端電腦與管理伺服器在同一網路中，可以選取此選項。
   - **透過發佈點使用作業系統資源**透過發佈點使用作業系統資源將實用程式傳輸到用戶端裝置。如果網路中有至少一個發佈點，則可以選取此選項。有關發佈點的詳細資訊，請參閱卡巴斯基安全管理中心說明。
4. 在"**同時下載的最大數量**"欄位中，設定傳送到管理伺服器的下載應用程式移除實用程式請求數量限制。限制請求數有助於防止網路超載。
5. 在"**解除安裝嘗試次數上限**"欄位中，設定移除應用程式嘗試次數限制。如果移除 Kaspersky Endpoint Security 以出錯結束，工作將自動再次啟動移除。
6. 如有必要，清除"**下載之前驗證作業系統類型**"核取方塊。這樣可避免在電腦的作業系統不符合軟體需求時下載移除實用程式。如果您確定電腦的作業系統符合軟體需求，可以略過此驗證。

### 步驟 4. 選取要執行工作的帳戶

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

### 步驟 5. 完成工作建立

點擊"**完成**"按鈕結束精靈。在工作清單中將顯示一個新工作。

要執行工作，請選中與工作對應的核取方塊，然後點擊**"開始"**按鈕。應用程式將以靜默模式移除。移除完成後，Kaspersky Endpoint Security 會顯示重新啟動電腦的提示。

如果應用程式移除操作受密碼防護，請在*"遠端解除安裝應用程式"*工作的內容中輸入 KLAdmin 帳戶密碼。如果沒有密碼，工作不會執行。

*要在"遠端解除安裝應用程式"工作中使用 KLAdmin 帳戶密碼：*

1. 在網頁主控台的主視窗中，選擇**資產（裝置）→工作**。
   工作清單開啟。
2. 點擊卡巴斯基安全管理中心的**"遠端解除安裝應用程式"**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**"使用解除安裝密碼"**核取方塊。
5. 輸入 KLAdmin 帳戶密碼。
6. 儲存變更。

重新啟動應用程式以完成移除。為此，網路代理會顯示一個快顯視窗。

## 使用 Active Directory 遠端移除應用程式

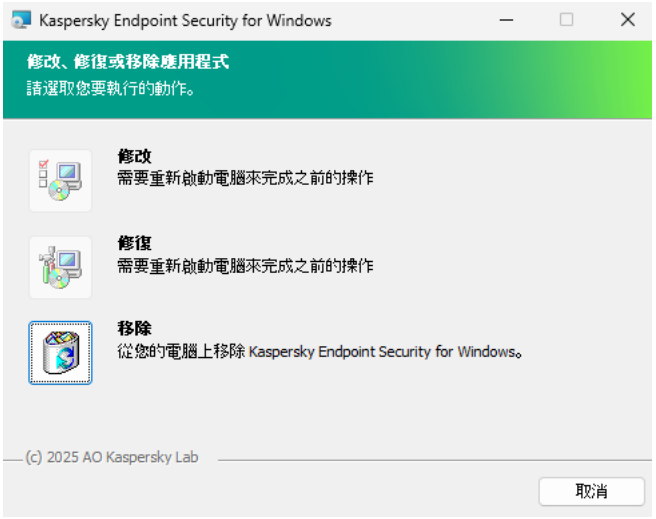
您可以使用 Microsoft Windows 群組政策遠端解除安裝應用程式。若要解除安裝應用程式，您需要開啟群組政策管理主控台 (gpmc.msc) 然後使用群組政策編輯器建立一個應用程式移除工作（要了解更多詳情，請造訪 Microsoft 技術支援網站）。

如果應用程式移除操作受密碼防護，則您需要執行以下操作：

1. 建立一個包含以下內容的 BAT 檔案：
   ```
   msiexec.exe /x<GUID> KLLOGIN=<user name> KLPASSWD=<password> /qn
   ```
   <GUID> 是應用程式的唯一 ID。您可以在技術支援知識庫中或者使用以下命令找到應用程式的 GUID：
   ```
   wmic product where "Name like '%Kaspersky Endpoint Security%'" get Name,
   IdentifyingNumber
   ```
   範例：
   ```
   msiexec.exe /x{6BB76C8F-365E-4345-83ED-6D7AD612AF76} KLLOGIN=KLAdmin KLPASSWD=samplePassword /qn
   ```
2. 在群組政策管理主控台 (gpmc.msc) 中為電腦建立一個新的 Microsoft Windows 政策。
3. 使用新政策執行在電腦上建立的 BAT 檔案。

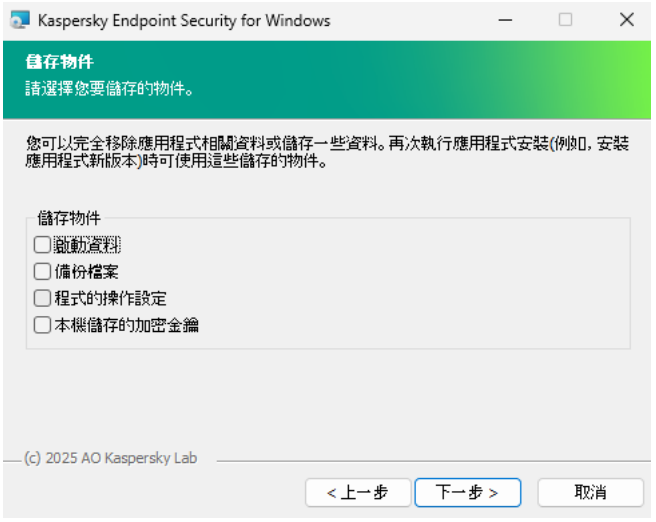
本機移除應用程式

您也可以使用安裝精靈本機移除應用程式。使用 Windows 作業系統的一般方法（透過"主控台"）移除 Kaspersky Endpoint Security。啟動"安裝精靈"。按照螢幕上的說明進行操作。




選擇應用程式移除操作

您可以指定要儲存應用程式使用的哪些資料，以供在下次安裝應用程式（例如升級到較新版本的應用程式）時使用。如果您並未指定任何資料，應用程式將被完全刪除（請見下圖）。




移除後儲存資料

您可以儲存以下資料：

- **啟動資料**，讓您避免再次啟動應用程式。如果產品授權期限在安裝之前未到期，Kaspersky Endpoint Security 會自動新增產品授權金鑰。
- **備份檔案** – 程式要掃描的置於"備份區"中的物件。

> 在移除應用程式之後儲存的備份檔案只能在用於儲存這些檔案的同一版本應用程式中存取。

如果您排程在移除應用程式之後使用備份物件，必須在移除應用程式之前還原這些物件。但是，Kaspersky 專家不建議從備份區中還原物件，因為這可能會損害電腦。

- **程式的操作設定** – 應用程式配置過程中選取的應用程式設定值。
- **本機儲存的加密金鑰** – 該資料提供對在移除程式之前加密的檔案和磁碟機的存取權限。為保證對加密檔案和磁碟機的存取權限，請確保在重新安裝 Kaspersky Endpoint Security 時選擇了資料加密功能。存取以前加密的檔案和磁碟機不需要進一步操作。

Kaspersky Endpoint Security 將資料儲存在 `C:\ProgramData\Kaspersky Lab\KES.12.12\QB` 資料夾中。

您也可以使用命令列本機刪除應用程式。

# 應用程式授權

本部分提供了 Kaspersky Endpoint Security 產品授權相關一般概念的資訊。

## 關於最終使用者產品授權協議

*最終使用者產品授權協議*是您與 AO Kaspersky Lab 之間達成的法律協議，它規定了您在使用所購買的應用程式時須遵循的條款。

建議您在使用應用程式前認真閱讀《產品授權協議》條款。

您可透過下列方式檢視此授權協議的條款：

- 以互動模式安裝 Kaspersky Endpoint Security 時。
- 透過閱讀 license.txt 檔案。該檔案包括在應用程式分發套件中，還位於應用程式安裝資料夾 `%ProgramFiles(x86)%\Kaspersky Lab\KES\Doc\<locale>\KES` 中。

安裝程式時確認您同意最終使用者產品授權協議即表示您同意最終使用者產品授權協議中的條款。如果您不同意最終使用者產品授權協議的條款，將會中止安裝。

## 關於授權

*產品授權*是根據最終使用者產品授權協議授予的在有限時間內使用本應用程式的權限。

該產品授權可讓您根據最終使用者授權許可協議的條款使用該應用程式，並獲得技術支援。可以使用的功能清單和應用程式使用期限取決於啟動應用程式的產品授權類型。

我們提供下列授權類型：

- *試用版* – 目的在於讓使用者熟悉該應用程式的免費授權。

  試用版產品授權通常擁有較短的有效期。當試用版授權到期，所有 Kaspersky Endpoint Security 功能將轉為停用。要繼續使用此應用程式，您必須購買一個正式授權。

  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，便無法再使用試用產品授權進行啟動。

- *正式版* – 購買 Kaspersky Endpoint Security 的付費授權。

  正式產品授權中所能使用的應用程式功能取決於所選產品。所選的產品指定在產品授權憑證中。可用產品的資訊可以在 Kaspersky 網站 上找到。

  當正式版產品授權到期時，應用程式的關鍵功能將被停用。要繼續使用此應用程式，您必須續約正式產品授權。如果不打算續約產品授權，您必須從電腦移除應用程式。

# 關於產品授權憑證

*產品授權憑證*是傳送給使用者的一個帶有金鑰檔案或啟動碼的檔案。

產品授權憑證包含以下產品授權資訊：

- 產品授權 ID 或訂單號。
- 被授予產品授權的使用者詳情。
- 可以使用產品授權啟動的應用程式詳情。
- 授權單元的數量限制（例如，可以在此產品授權下使用應用程式的裝置數量）。
- 產品授權期限開始日期。
- 產品授權到期日期或產品授權期限。
- 產品授權類型。

# 關於訂購

*Kaspersky Endpoint Security 訂購*是一項帶有特定參數（如訂購到期日期和受防護裝置數量）的應用程式購買訂單。您可以從服務供應商（範例您的 ISP）處訂購 Kaspersky Endpoint Security 訂購。您可以手動或自動對訂購進行續約，也可以取消訂購。您可以在服務供應商網站上管理您的訂購。

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）。有限訂購期到期後，要使 Kaspersky Endpoint Security 繼續工作，您必須續約訂購。如果按時預支付供應商服務，則可以自動續約無限訂購。

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。寬限期的可用性和期限由服務提供者決定。

要在訂購下使用 Kaspersky Endpoint Security，您需要套用從服務供應商處接收到的啟動碼。套用啟動碼之後，將新增啟動金鑰。啟動金鑰確認在訂購下使用應用程式的產品授權。您不能使用金鑰檔案啟動訂購下的應用程式。服務提供商只能提供一個啟動碼。無法在訂購下新增備用金鑰。

在訂購下購買的啟動碼可能無法用於啟動先前版本的 Kaspersky Endpoint Security。

# 關於產品授權金鑰

*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。

對於訂購中新增的金鑰，不提供產品授權憑證。

您可以透過套用金鑰檔案或輸入啟動碼來向應用程式新增產品授權金鑰。

若違反了最終使用者授權協議的條款，則 Kaspersky 可以封鎖此金鑰。如果金鑰被封鎖，則您必須新增其他金鑰才繼續使用應用程式。

有兩種類型的金鑰：啟動金鑰和備用金鑰。

*啟動金鑰*是程式目前正在使用的金鑰。試用版產品授權或正式版產品授權金鑰可以被新增為啟動金鑰。本應用程式不能擁有兩個及以上啟動金鑰。

*備用金鑰*使用者可新增一組目前尚未使用的金鑰。啟動金鑰到期後，備用金鑰將自動生效。在目前已有金鑰啟用下才能新增備用金鑰。

只能將試用版產品授權的金鑰以啟動金鑰的形式進行新增。無法將其新增為備用金鑰。試用版產品授權金鑰無法替換正式版產品授權的啟動金鑰。

如果金鑰被新增到禁止金鑰清單中，則用於啟動應用程式的產品授權定義的應用程式功能將保持八天可用。應用程式將通知使用者該金鑰已新增到禁止金鑰清單中。八天後，應用程式功能將限制為產品授權到期後可用的功能級別。您可以使用防護和控制元件並使用產品授權到期之前安裝的應用程式資料庫執行掃描。此應用程式也會繼續加密在產品授權到期前經過修改或加密過的檔案，但是不會加密新檔案。卡巴斯基安全網路無法使用。

# 關於啟動碼

*啟動碼*是由 20 個字母數字字元組成的唯一序號。輸入啟動碼以新增用於啟動 Kaspersky Endpoint Security 的產品授權金鑰。在您購買 Kaspersky Endpoint Security 之後，您指定的電子郵件地址會收到啟動碼。

要用啟動碼啟動應用程式，需要網際網路接入連線到 Kaspersky 的啟動伺服器。

當應用程式使用啟動碼啟動時，將新增啟動金鑰。備用金鑰只能使用啟動碼新增，而不能使用金鑰檔案新增。

如果啟動應用程式後遺失了啟動碼，則您可以還原啟動碼。您可能會需要啟動碼，例如用於註冊 Kaspersky CompanyAccount。如果啟動碼在應用程式啟動後丟失，請聯絡您從其購買產品授權的 Kaspersky 合作廠商。

# 關於金鑰檔案

*金鑰檔案*是您從 Kaspersky 接收到的 .key 副檔名的檔案。金鑰檔案的目的是新增能夠啟動應用程式的產品授權金鑰。

在購買 Kaspersky Endpoint Security 或訂購 Kaspersky Endpoint Security 試用版後，您會在您提供的電子郵件地址收到金鑰檔案。

使用金鑰檔案無需連線至 Kaspersky 啟動伺服器以啟動應用程式。

如果金鑰檔案被意外刪除，則您可以還原它。您可能需要金鑰檔案註冊諸如卡巴斯基公司帳戶之類的服務。

若要還原金鑰檔案，請執行以下操作：

- 聯絡產品授權銷售商。
- 基於您現有的啟動碼在 Kaspersky 網站上獲得金鑰檔案。
- 從另一個管理伺服器取得金鑰檔案。

當使用金鑰檔案啟動應用程式時，將新增啟動金鑰。備用金鑰只能使用金鑰檔案新增，而不能使用啟動碼新增。

# 依據工作站的產品授權類型比對應用程式功能

工作站上可用的 Kaspersky Endpoint Security 功能集合取決於產品授權類型（請見下表）。

也請參見伺服器的應用程式功能比對

根據 Kaspersky Next 產品授權類型進行應用程式功能比較，請參見 Kaspersky Next 說明。

Kaspersky Endpoint Security 功能比較

| 功能 | Kaspersky Endpoint Security for Business Select | Kaspersky Endpoint Security for Business Advanced | Kaspersky Total Security | Kaspersky Endpoint Detection and Response Optimum | Kaspersky Optimum Security | Kaspersky Endpoint Detection and Response Expert | Kaspersky Hybrid Cloud Security 標準版 | Kaspersky Hybrid Cloud Security 企業版 |
|---|---|---|---|---|---|---|---|---|
| **進階威脅防護** | | | | | | | | |
| 卡巴斯基安全網路 | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| 行為偵測 | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| 加密軟體防護 | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| 弱點利用防禦 | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| 主機入侵防禦 | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| 修復引擎 | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| **關鍵威脅防護** | | | | | | | | |
| 檔案威脅防護 | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| Web 威脅防護 | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| 郵件威脅防護 | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| 防火牆 | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| 網路威脅防護 | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| BadUSB 攻擊防護 | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| AMSI 防護 | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| **安全控制** | | | | | | | | |
| 記錄檢查 | – | – | – | – | – | – | – | – |
| 應用程式控制 | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| 裝置控制 | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |

| 功能 | Kaspersky Endpoint Security for Business Select | Kaspersky Endpoint Security for Business Advanced | Kaspersky Total Security | Kaspersky Endpoint Detection and Response Optimum | Kaspersky Optimum Security | Kaspersky Endpoint Detection and Response Expert | Kaspersky Hybrid Cloud Security 標準版 | Kaspersky Hybrid Cloud Security 企業版 |
|---|---|---|---|---|---|---|---|---|
| Web 控制 | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| 自適應異常控制 | – | ✓ | ✓ | ✓ | ✓ | ✓ | – | ✓ |
| 系統完整性監控 | – | – | – | – | – | – | – | – |
| **資料加密** | | | | | | | | |
| 卡巴斯基磁碟加密 | – | ✓ | ✓ | ✓ | ✓ | ✓ | – | ✓ |
| BitLocker 磁碟機加密 | – | ✓ | ✓ | ✓ | ✓ | ✓ | – | ✓ |
| 檔案級加密 | – | ✓ | ✓ | ✓ | ✓ | ✓ | – | ✓ |
| 卸除式磁碟機加密 | – | ✓ | ✓ | ✓ | ✓ | ✓ | – | ✓ |
| **Detection and Response** | | | | | | | | |
| Endpoint Detection and Response Optimum | – | – | – | ✓ | ✓ | – | – | – |
| Endpoint Detection and Response Expert | – | – | – | – | – | ✓ | – | – |
| Kaspersky Sandbox *（Kaspersky Sandbox 產品授權必須單獨購買）* | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| **與 KUMA 整合** *（KUMA 整合的產品授權必須單獨購買）* | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| **Light Agent 模式** *（若要啟動應用程式，您必須將產品授權金鑰新增至 Light Agent 連線的 SVM）* | – | – | – | – | – | – | ✓ | ✓ |

# 依據伺服器的產品授權類型比對應用程式功能

伺服器上可用的 Kaspersky Endpoint Security 功能集合取決於產品授權類型（請見下表）。

也請參見工作站的應用程式功能比對

根據 Kaspersky Next 產品授權類型進行應用程式功能比較，請參見 Kaspersky Next 說明。

| 功能 | Kaspersky Endpoint Security for Business Select | Kaspersky Endpoint Security for Business Advanced | Kaspersky Total Security | Kaspersky Endpoint Detection and Response Optimum | Kaspersky Optimum Security | Kaspersky Endpoint Detection and Response Expert | Kaspersky Hybrid Cloud Security 標準版 | Kaspersky Hybrid Cloud Security 企業版 |
|---|---|---|---|---|---|---|---|---|
| **進階威脅防護** | | | | | | | | |
| 卡巴斯基安全網路 | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| 行為偵測 | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| 加密軟體防護 | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| 弱點利用防禦 | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| 主機入侵防禦 | – | – | – | – | – | – | – | – |
| 修復引擎 | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| **關鍵威脅防護** | | | | | | | | |
| 檔案威脅防護 | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| Web 威脅防護 | – | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| 郵件威脅防護 | – | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| 防火牆 | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| 網路威脅防護 | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| BadUSB 攻擊防護 | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| AMSI 防護 | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| **安全控制** | | | | | | | | |
| 記錄檢查 | – | – | – | – | – | – | – | ✓ |
| 應用程式控制 | – | ✓ | ✓ | ✓ | ✓ | ✓ | – | ✓ |
| 裝置控制 | – | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| Web 控制 | – | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| 自適應異常控制 | – | – | – | – | – | – | – | – |
| 系統完整性監控 | – | – | – | – | – | – | – | ✓ |
| **資料加密** | | | | | | | | |
| 卡巴斯基磁碟加密 | – | – | – | – | – | – | – | – |
| BitLocker 磁碟機加密 | – | ✓ | ✓ | ✓ | ✓ | ✓ | – | ✓ |
| 檔案級加密 | – | – | – | – | – | – | – | – |
| 卸除式磁碟機加密 | – | – | – | – | – | – | – | – |
| **Detection and Response** | | | | | | | | |
| Endpoint Detection and Response Optimum | – | – | – | ✓ | ✓ | – | – | – |
| Endpoint Detection and Response Expert | – | – | – | – | – | ✓ | – | – |

| 功能 | Kaspersky Endpoint Security for Business Select | Kaspersky Endpoint Security for Business Advanced | Kaspersky Total Security | Kaspersky Endpoint Detection and Response Optimum | Kaspersky Optimum Security | Kaspersky Endpoint Detection and Response Expert | Kaspersky Hybrid Cloud Security 標準版 | Kaspersky Hybrid Cloud Security 企業版 |
|---|---|---|---|---|---|---|---|---|
| Kaspersky Sandbox<br>*（Kaspersky Sandbox 產品授權必須單獨購買）* | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| **與 KUMA 整合**<br>*（KUMA 整合的產品授權必須單獨購買）* | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| **Light Agent 模式**<br>*（若要啟動應用程式，您必須將產品授權金鑰新增至 Light Agent 連線的 SVM）* | – | – | – | – | – | – | ✓ | ✓ |

# 啟動應用程式

*啟動*是一種啟動產品授權的過程，允許您在產品授權過期之前使用該應用程式全部的功能。應用程式啟動涉及新增產品授權金鑰。

您可以採用以下方式啟動應用程式：

- 使用啟動精靈從應用程式介面本機進行。您可使用此方式同時新增啟動金鑰與備用金鑰。
- 遠端使用卡巴斯基安全管理中心軟體套裝。
  - 使用"*新增金鑰*"工作。

    此方法允許您向特定電腦或屬於管理群組的電腦新增金鑰。您可使用此方式同時新增啟動金鑰與備用金鑰。
  - 透過將儲存在卡巴斯基安全管理中心管理伺服器中的金鑰分發到電腦。

    使用此方法可以自動將金鑰新增到已連線到卡巴斯基安全管理中心的電腦和新電腦。要使用此方法，需要先將金鑰新增到卡巴斯基安全管理中心管理伺服器。有關將金鑰新增到卡巴斯基安全管理中心管理伺服器的詳細資訊，請參閱卡巴斯基安全管理中心說明。

    在訂購下購買的啟動碼位於第一位。

- 透過將金鑰新增到 Kaspersky Endpoint Security 安裝套件。

  此方法可讓您在 Kaspersky Endpoint Security 部署期間將金鑰新增到安裝套件內容。安裝後應用程式會被自動啟動。

- 使用命令列。

根據 Kaspersky 的啟動伺服器的負載分佈情況，（在遠端安裝或非互動安裝失）程式用啟動碼啟動可能會花一定時間。若您需要立即啟動應用程式，您可能需要中斷正在進行的啟動過程，並使用啟動精靈進行啟動。

如果在 Light Agent 模式 下使用 Kaspersky Endpoint Security 來防護虛擬環境，則不不需要單獨啟動應用程式。

## 啟動應用程式

**如何在管理主控台 (MMC) 中啟動應用程式**

1. 在卡巴斯基安全管理中心管理主控台樹狀目錄中，選取**工作**。

   工作清單開啟。

2. 點擊**"新工作"**。

啟動"工作精靈"。按照精靈的說明進行操作。

### 步驟 1. 選取工作類型

選取**"Kaspersky Endpoint Security for Windows (12.12)"→"新增金鑰"**。

### 步驟 2. 新增金鑰

輸入啟動碼或選取金鑰檔案。

有關將金鑰新增到卡巴斯基安全管理中心儲存區的詳細資訊，請參閱卡巴斯基安全管理中心說明。

步驟 3. 選取將要對其分配工作的裝置

選取將要執行工作的電腦。下列選項可用：

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

步驟 4. 設定工作啟動排程

配置啟動工作的排程，例如，手動或在電腦空閒時。

步驟 5. 定義工作名稱

輸入工作的名稱，例如"*啟動 Kaspersky Endpoint Security for Windows*"。

步驟 6. 完成工作建立

結束精靈。如有必要，選中"**精靈完成時執行工作**"核取方塊。您可以在工作內容中監控工作進度。結果，Kaspersky Endpoint Security 將以靜默模式在使用者電腦上啟動。

**如何在網頁主控台和雲端主控台中啟動應用程式**

1. 在網頁主控台的主視窗中，選擇**資產（裝置）→工作**。

   工作清單開啟。

2. 點擊"**新增**"。

啟動"工作精靈"。按照精靈的說明進行操作。

步驟 1. 配置一般工作設定

配置一般工作設定：

1. 在"**應用程式**"下拉式清單中，選取"**Kaspersky Endpoint Security for Windows 12.12.0**"。
2. 在"**工作類型**"下拉式清單中，選取"**新增金鑰**"。

3. 在**"工作名稱"**欄位中，輸入簡要說明，例如，"*啟動 Kaspersky Endpoint Security for Windows*"。

4. 在**"要將工作指派給的裝置"**塊中，選取工作範圍。前往下一步。

### 步驟 2. 選取將要對其分配工作的裝置

選取將要執行工作的電腦。下列選項可用：

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

### 步驟3. 選取產品授權

選取要用於啟動應用程式的產品授權。前往下一步。

您可以向網頁主控台新增金鑰（**"操作 → 產品授權"**）。

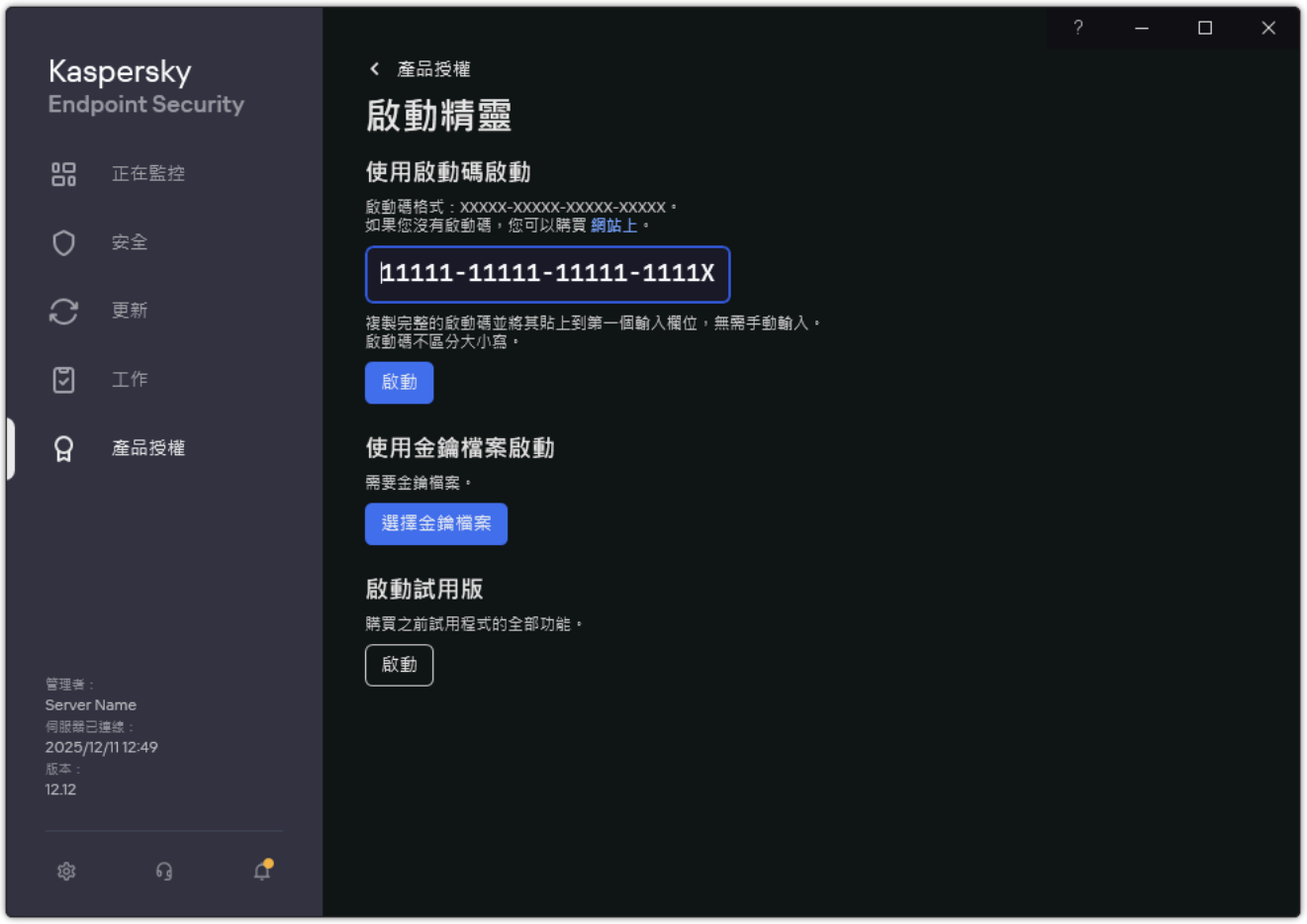
### 步驟 4. 完成工作建立

點擊**"完成"**按鈕結束精靈。在工作清單中將顯示一個新工作。要執行工作，請選中與工作對應的核取方塊，然後點擊**"開始"**按鈕。結果，Kaspersky Endpoint Security 將以靜默模式在使用者電腦上啟動。

**如何在應用程式介面中啟動應用程式**

1. 在應用程式主視窗中，轉至**"產品授權"**區域。
2. 點擊**"使用新產品授權啟動應用程式"**。

應用程式啟動精靈將啟動。按照啟動精靈的指示操作。




啟動應用程式

在“*新增金鑰*”工作的內容中，可以將備用金鑰新增到電腦。當啟動金鑰到期或被刪除時，*備用金鑰*會成為啟動金鑰。使用備用金鑰可避免當產品授權到期時應用程式功能受限。

### 如何透過管理主控台 (MMC) 自動向電腦新增產品授權金鑰

1. 在管理主控台中，轉到資料夾“**卡巴斯基產品授權**”。

   隨即開啟產品授權金鑰清單。

2. 開啟產品授權金鑰內容。

3. 在“**一般**”區域中選擇“**自動分發產品授權金鑰到受管理裝置**”核取方塊。

4. 儲存變更。

結果是金鑰將自動分發到相應電腦。在將金鑰作為啟動金鑰或備用金鑰進行自動分發的過程中，會考慮產品授權對電腦數量的限制（在金鑰內容中設定）。如果達到產品授權限制，會自動停止將該金鑰分發到電腦。您可以在“**裝置**”區域的金鑰內容中檢視已新增金鑰的電腦數量以及其他資料。

### 如何透過網頁主控台和雲端主控台自動向電腦新增產品授權金鑰

1. 在網頁主控台的主視窗中，選擇**操作 → 產品授權 → 卡巴斯基產品授權**。

   隨即開啟產品授權金鑰清單。

2. 開啟產品授權金鑰內容。

3. 在**一般**頁簽上，啟用 **自動分發產品授權金鑰到受管理裝置**切換開關。

4. 儲存變更。

結果是金鑰將自動分發到相應電腦。在將金鑰作為啟動金鑰或備用金鑰進行自動分發的過程中，會考慮產品授權對電腦數量的限制（在金鑰內容中設定）。如果達到產品授權限制，會自動停止將該金鑰分發到電腦。您可以在**"裝置"**標籤上的金鑰內容中檢視已新增金鑰的電腦數量以及其他資料。

如果您在使用*啟動碼*啟動應用程式，需要網際網路接入連線到 Kaspersky 的啟動伺服器。如果您使用*金鑰檔案*啟動應用程式，則无需存取網際網路。如果電腦位於無法存取網際網路的隔離網段中，若要使用代碼啟動應用程式，您必須允許使用卡巴斯基安全管理中心管理伺服器作為代理伺服器。也就是說，應用程式可以透過具有網際網路存取權限的管理伺服器來存取啟動伺服器。

**如何允許使用管理伺服器作為代理伺服器來啟動管理主控台 (MMC) 中的應用程式**

1. 在卡巴斯基安全管理中心管理主控台樹狀目錄中，選取**政策**。

2. 選擇必要的政策並點擊以開啟政策內容。

3. 在政策視窗中，選擇**"一般設定 → 應用程式設定"**。

4. 選擇**"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。

5. 儲存變更。

**如何允許使用管理伺服器作為代理伺服器在網頁主控台和雲端主控台中啟動應用程式**

1. 在網頁主控台的主視窗中，選擇**資產（裝置）→ 政策和設定檔**。

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. 選擇**"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。

6. 儲存變更。

如果您無法使用*啟動碼*啟動應用程式，您可以嘗試使用卡巴斯基解決方案獲取一個*金鑰檔案*，並嘗試使用不同方法再次啟動應用程式。

## 產品授權使用監控

您可以透過以下方式監控產品授權的使用：

- 檢視組織的基礎結構的 *產品授權金鑰使用報告*（**監控和報告 → 報告**）。
- 在**"受管理裝置 → 裝置"**標籤上檢視電腦的狀態。如果應用程式未啟動，電腦將具有 ⚠ *"應用程式未啟動"*狀態。

- 檢視電腦內容中的產品授權資訊。
- 檢視金鑰屬性（**操作 → 產品授權**）。

### 作為卡巴斯基安全網路中心雲端主控台的一部分啟動應用程式的細節

卡巴斯基安全管理中心雲端主控台提供了試用版。*試用版*是卡巴斯基安全管理中心雲端主控台的特殊版本，旨在使使用者熟悉該應用程式的功能。在此版本中，您可以在 30 天內在工作區中執行操作。所有託管的應用程式都自動在卡巴斯基安全管理中心雲端主控台的試用授權許可下執行，包括 Kaspersky Endpoint Security。但是，當卡巴斯基安全管理中心雲端主控台的試用授權許可到期時，您無法使用 Kaspersky Endpoint Security 自身的試用授權許可啟動該應用程式。有關卡巴斯基安全管理中心產品授權的詳細資訊，請參閱卡巴斯基安全管理中心雲端主控台說明。

卡巴斯基安全管理中心雲端主控台試用版不允許以後切換到商業版本。30 天期限到期後，所有試用工作區及其所有內容都將被自動刪除。

# 移除產品授權金鑰

若要移除產品授權金鑰，您需要在電腦上執行特殊工作。例如，您可以移除產品授權金鑰以重新排列許可單元。此外，當產品授權到期時，Kaspersky Endpoint Security 會通知您。如果您新增了短期產品授權金鑰來試用應用程式（例如 EDR Optimum Add-on），則可以刪除此授權金鑰以消除通知並修復電腦的狀態。

*移除金鑰*工作允許從電腦中刪除任何產品授權金鑰。您可以刪除活動產品授權金鑰以及備用產品授權金鑰。除了 Kaspersky Endpoint Security 啟動產品授權金鑰之外，您還可以刪除Kaspersky Detection and Response 解決方案（例如，EDR Optimum Add-on）的單獨產品授權金鑰。

**如何在管理主控台 (MMC) 中移除產品授權金鑰**

1. 在卡巴斯基安全管理中心管理主控台樹狀目錄中，選取**工作**。

   工作清單開啟。

2. 點擊**"新工作"**。

啟動"工作精靈"。按照精靈的說明進行操作。

### 步驟 1. 選取工作類型

選取**"Kaspersky Endpoint Security for Windows (12.12)"→"移除金鑰"**。

### 步驟2. 選取產品授權

選擇您要移除的產品授權金鑰。您可以從卡巴斯基安全管理中心金鑰儲存中選擇產品授權金鑰或選擇金鑰檔案。

步驟 3. 選取將要對其分配工作的裝置

選取將要執行工作的電腦。下列選項可用：

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

步驟 4. 設定工作啟動排程

配置啟動工作的排程，例如，手動或在電腦空閒時。

步驟 5. 定義工作名稱

輸入工作的名稱，例如"*移除 Beta 版金鑰*"。

步驟 6. 完成工作建立

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

**如何在網頁主控台中移除產品授權金鑰**

1. 在網頁主控台的主視窗中，選擇**資產（裝置）→工作**。
   工作清單開啟。
2. 點擊"**新增**"。

啟動"工作精靈"。按照精靈的說明進行操作。

步驟 1. 配置一般工作設定

配置一般工作設定：

1. 在"**應用程式**"下拉式清單中，選取"**Kaspersky Endpoint Security for Windows 12.12.0**"。
2. 在"**工作類型**"下拉式清單中，選取"**移除金鑰**"。

3. 在**"工作名稱"**欄位中，輸入簡要說明，例如*"移除 Beta 版金鑰"*。

4. 在**"要將工作指派給的裝置"**塊中，選取工作範圍。前往下一步。

### 步驟 2. 選取將要對其分配工作的裝置

選取將要執行工作的電腦。下列選項可用：

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

### 步驟3. 選取產品授權

選擇您要移除的產品授權金鑰。您可以從卡巴斯基安全管理中心金鑰儲存中選擇產品授權金鑰或選擇金鑰檔案。前往下一步。

### 步驟 4. 完成工作建立

點擊**"完成"**按鈕結束精靈。在工作清單中將顯示一個新工作。要執行工作，請選中與工作對應的核取方塊，然後點擊**"開始"**按鈕。

### 如何在應用程式介面中移除產品授權金鑰

1. 在應用程式主視窗中，轉至**"產品授權"**區域。
2. 選擇您要取消刪除的金鑰，然後點擊**刪除**。



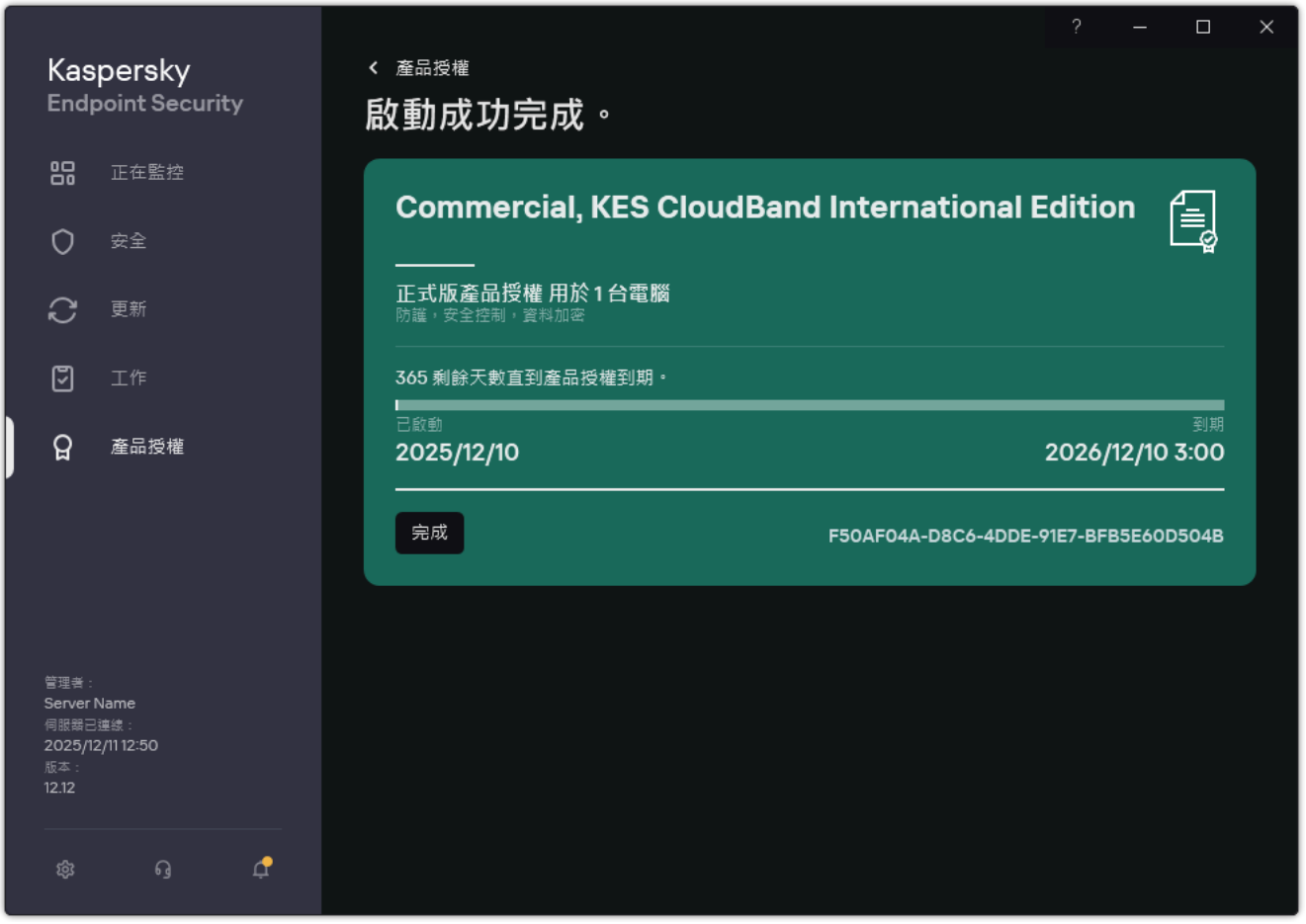

"產品授權管理"視窗

您還可以 在命令列上移除產品授權金鑰。

# 檢視產品授權資訊

*要檢視產品授權的相關資訊：*

在應用程式主視窗中，轉至**"產品授權"**區域（請見下圖）。




"產品授權管理"視窗

該區域會顯示以下詳情：

- *金鑰狀態*。一台電腦上可以儲存多個金鑰。有兩種類型的金鑰：啟動金鑰和備用金鑰。本應用程式不能擁有兩個及以上啟動金鑰。只有啟動金鑰到期或透過點擊**"刪除"**刪除啟動金鑰後，備用金鑰才變為啟動金鑰。
- *應用程式名稱*。已購買的 Kaspersky 應用程式的全名。
- *產品授權類型*。以下產品授權類型可用：試用和正式。
- *功能*。在您的產品授權下提供的應用程式功能。功能可能包括防護、安全控制、資料加密等。授權憑證中還提供了可用功能的清單。

- *有關產品授權的附加資訊*。產品授權期限的開始日期和結束日期（僅適用於啟動金鑰），產品授權期限的剩餘時長。

  產品授權到期日期根據作業系統中配置的時區進行顯示。

- *金鑰*。金鑰是從啟動碼或金鑰檔案生成的唯一字母數字序列。

在"產品授權管理"視窗中，還可以執行下列操作之一：

- **購買產品授權 / 續約產品授權**。開啟受防護裝置線上商店網站，在其中可以購買或續約產品授權。為此，請輸入您的公司資訊並支付訂單。
- **使用新產品授權啟動應用程式**啟動應用程式啟動精靈。在此精靈中可以使用啟動碼或金鑰檔案新增金鑰。應用程式啟動精靈允許您新增一個啟動金鑰和一個（且僅有一個）備用金鑰。

# 購買產品授權

您可以在安裝程式後購買授權。購買產品授權後，您將收到用於啟動應用程式的啟動碼或金鑰檔案。

*要購買產品授權：*

1. 在應用程式主視窗中，轉至**"產品授權"**區域。
2. 請執行以下操作之一：
   - 如果未新增任何金鑰，或新增了試用版產品授權的金鑰，請點擊**"購買產品授權"**按鈕。
   - 如果安裝了正式版產品授權的金鑰，請點擊**"續約產品授權"**按鈕。

   這時瀏覽器將開啟 Kaspersky 線上商店的視窗，您可以在此網站中購買產品授權。

# 續約訂購

當您在訂購下使用程式時，Kaspersky Endpoint Security 將按照指定間隔自動聯絡啟動伺服器，直至您的訂購到期。

如果您在無限訂購下使用應用程式，Kaspersky Endpoint Security 將自動檢查啟動伺服器，以背景模式獲取續約的金鑰。如果啟動伺服器上有可用金鑰，應用程式會替換先前產品授權繼而新增此產品授權。透過這種方式，使用無限訂購的 Kaspersky Endpoint Security 無需使用者介入進行更新。

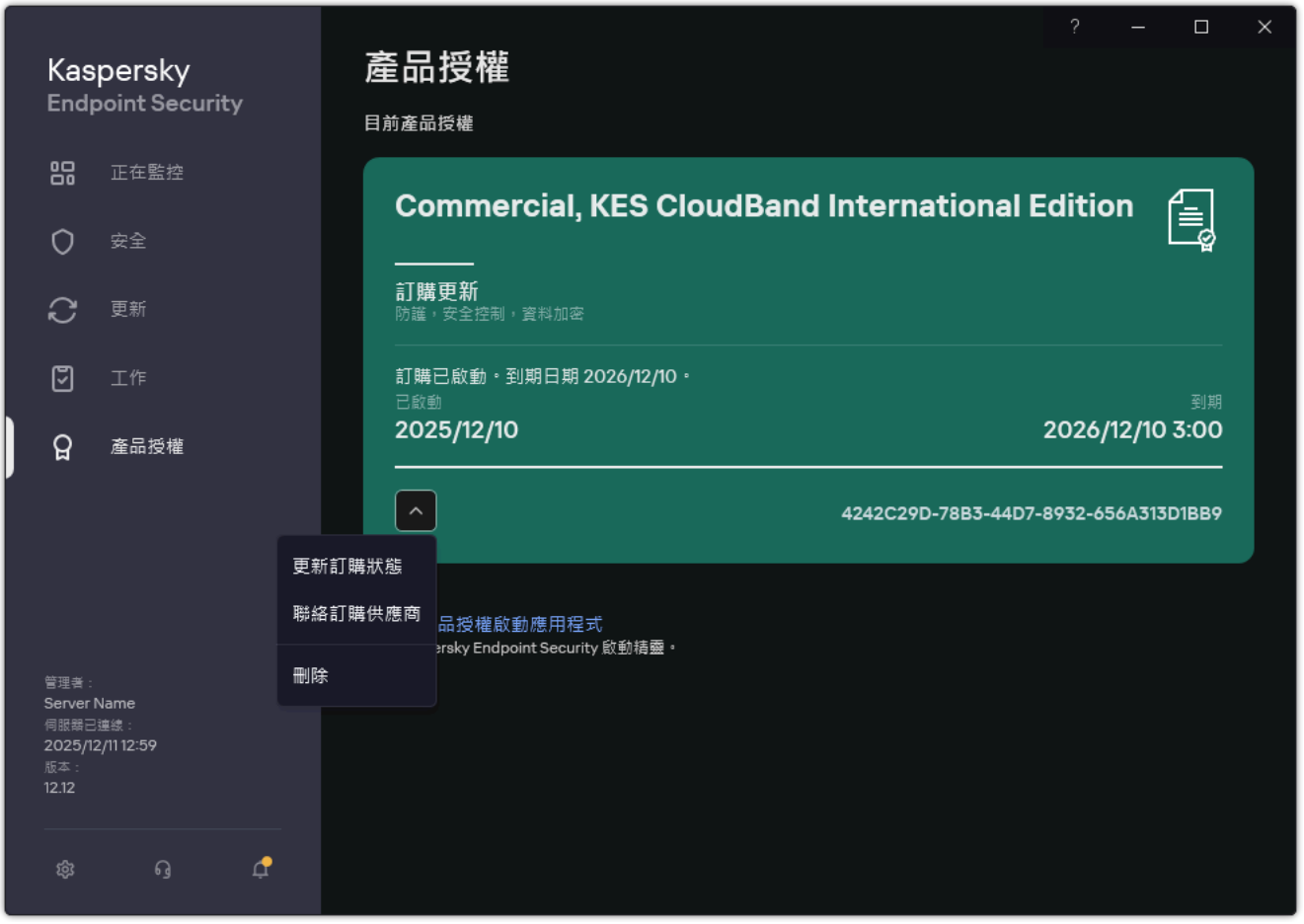
如果您在有限訂購下使用本應用程式，在訂購到期之日（或訂購續約寬限期到期之日），Kaspersky Endpoint Security 將通知您，並停止嘗試自動續約訂購。在這種情況下，Kaspersky Endpoint Security 將與正式版應用程式到期一樣的方式執行：應用程式執行但是沒有更新且卡巴斯基安全網路不可用。

您可以在服務提供者的網站上續約訂購。

*若要從程式介面中存取服務供應商網站，請執行以下操作：*

1. 在應用程式主視窗中，轉至**"產品授權"**區域。
2. 點擊**"聯絡訂購供應商"**。

您可以手動更新訂購狀態。如果在寬限期後對訂購進行續約並且訂購狀態未自動更新時，您可能需要執行此操作。




續約訂購

# 資料提供

## 在最終使用者產品授權協議下的資料提供

如果套用啟動碼來啟動 Kaspersky Endpoint Security，則您同意為驗證應用程式的正確使用而自動定期向 Kaspersky 傳送以下資訊：

- Kaspersky Endpoint Security 的類型、版本和中文化；
- Kaspersky Endpoint Security 已安裝更新的版本；
- 電腦 ID 和該電腦上的特定 Kaspersky Endpoint Security 安裝的 ID；
- 序號和啟動金鑰識別符；
- 作業系統的類型、版本和比特率，以及虛擬環境的名稱（如果 Kaspersky Endpoint Security 安裝在虛擬環境中）；
- 權利持有者服務的唯一請求 ID；
- 傳送資訊時活動的 Kaspersky Endpoint Security 元件的 ID。

Kaspersky 也可以使用這些資訊來生成關於 Kaspersky 軟體傳播和使用的統計資訊。

使用啟動碼，即表明您同意自動傳送以上列出的資料。如果您不同意傳送這些資訊至 Kaspersky，則應該使用金鑰檔案來啟動 Kaspersky Endpoint Security。

同意最終使用者產品授權協議的條款，表示您同意自動傳送以下資訊：

- 升級 Kaspersky Endpoint Security 時：
  - Kaspersky Endpoint Security 的版本；
  - Kaspersky Endpoint Security 的 ID；
  - 啟動金鑰；
  - 升級工作啟動的唯一 ID；
  - Kaspersky Endpoint Security 安裝的唯一 ID。
- 點擊 Kaspersky Endpoint Security 介面中的連結時：
  - Kaspersky Endpoint Security 的版本；
  - 作業系統版本；
  - Kaspersky Endpoint Security 啟動日期；
  - 產品授權到期日期；
  - 金鑰建立日期；

- Kaspersky Endpoint Security 安裝日期；
- Kaspersky Endpoint Security 的 ID；
- 作業系統中偵測到的弱點的 ID；
- 為 Kaspersky Endpoint Security 安裝的最新更新的 ID；
- 偵測到的帶威脅的檔案的雜湊值，以及按照 Kaspersky 分類確定的威脅名稱；
- Kaspersky Endpoint Security 啟動錯誤類別；
- Kaspersky Endpoint Security 啟動錯誤代碼；
- 金鑰到期前的天數；
- 新增金鑰後經過的天數；
- 產品授權到期後經過的天數；
- 套用目前產品授權的電腦數量；
- 啟動金鑰；
- Kaspersky Endpoint Security 產品授權條款；
- 產品授權目前狀態；
- 目前產品授權的類型；
- 應用程式類型；
- 升級工作啟動的唯一 ID；
- 電腦上 Kaspersky Endpoint Security 安裝的唯一 ID；
- Kaspersky Endpoint Security 介面語言。

Kaspersky 將根據法律和 Kaspersky 應用程式管理規定防護收到的資訊。資料透過加密的通訊通道傳輸。

請閱讀最終使用者產品授權協議並存取 Kaspersky 網站瞭解當您接受《最終使用者產品授權協議》和同意《卡巴斯基安全網路聲明》之後我們如何接收、儲存和銷毀有關程式使用的資訊。license.txt 和 ksn_<語言 ID>.txt 檔案包含最終使用者產品授權協議的文字，卡巴斯基安全網路聲明包含在應用程式分發套件中。

# 使用卡巴斯基安全網路時的資料提供

Kaspersky Endpoint Security 傳送到 Kaspersky 的資料集合取決於產品授權的類型和卡巴斯基安全網路使用設定。

### 經產品授權在不超過 4 台電腦上使用 KSN

同意卡巴斯基安全網路聲明，表示您同意自動傳送以下資訊：

- 有關 KSN 配置更新的資訊：活動配置的識別碼、收到的配置的識別碼、配置更新的錯誤代碼；
- 有關要掃描的檔案和 URL 位址的資訊：所掃描檔案的核對總和 (MD5、SHA2-256、SHA1) 和檔案模式 (MD5)，模式大小，偵測到的威脅的類型及其在權利所有人分類中的名稱，病毒資料庫的識別碼，其信譽被請求的 URL 位址，以及引用頁 URL 位址，連線協定的識別碼和使用的連接埠號；
- 偵測到威脅的掃描工作的 ID；
- 有關需要用來驗證真實性的數位憑證的資訊：用於對掃描的物件進行簽章的憑證的核對總和 (SHA256) 以及憑證的公開金鑰；
- 執行掃描的軟體元件的識別碼；
- 病毒資料庫的 ID 以及這些病毒資料庫中的記錄的 ID；
- 有關電腦上的軟體啟動的資訊：來自啟動服務的已簽章票證頭（區域啟動中心的識別碼、啟動碼的核對總和、票證的核對總和、票證建立日期、票證的唯一識別碼、票證版本、產品授權狀態、票證有效期的開始/結束日期和時間、產品授權的唯一識別碼、產品授權版本），用於對票證頭簽章的憑證的識別碼，金鑰檔案的核對總和 (MD5)；
- 有關權利所有人的軟體的資訊：完整版本，類型，用於連線到 Kaspersky 服務的協定的版本。

### 經產品授權在 5 台或更多電腦上使用 KSN

同意卡巴斯基安全網路聲明，表示您同意自動傳送以下資訊：

如果選中“**卡巴斯基安全網路**”核取方塊並且清除“**啟用延伸 KSN 模式**”核取方塊，則應用程式會傳送以下資訊：

- 有關 KSN 配置更新的資訊：活動配置的識別碼、收到的配置的識別碼、配置更新的錯誤代碼；
- 有關要掃描的檔案和 URL 位址的資訊：所掃描檔案的核對總和 (MD5、SHA2-256、SHA1) 和檔案模式 (MD5)，模式大小，偵測到的威脅的類型及其在權利所有人分類中的名稱，病毒資料庫的識別碼，其信譽被請求的 URL 位址，以及引用頁 URL 位址，連線協定的識別碼和使用的連接埠號；
- 偵測到威脅的掃描工作的 ID；
- 有關需要用來驗證真實性的數位憑證的資訊：用於對掃描的物件進行簽章的憑證的核對總和 (SHA256) 以及憑證的公開金鑰；
- 執行掃描的軟體元件的識別碼；
- 病毒資料庫的 ID 以及這些病毒資料庫中的記錄的 ID；

- 有關電腦上的軟體啟動的資訊：來自啟動服務的已簽章票證頭（區域啟動中心的識別碼、啟動碼的核對總和、票證的核對總和、票證建立日期、票證的唯一識別碼、票證版本、產品授權狀態、票證有效期的開始/結束日期和時間、產品授權的唯一識別碼、產品授權版本），用於對票證頭簽章的憑證的識別碼，金鑰檔案的核對總和 (MD5)；

- 有關權利所有人的軟體的資訊：完整版本，類型，用於連線到 Kaspersky 服務的協定的版本。

如果除了**"卡巴斯基安全網路"**核取方塊之外，還選擇了**"啟用延伸 KSN 模式"**核取方塊，則除了上面列出的資訊之外，應用程式還會傳送以下資訊：

- 有關對請求的包含主機的被處理 URL 和 IP 位址的 Web 資源進行分類的結果的資訊，執行分類的軟體元件的版本，分類方法，以及針對 Web 資源定義的類別集；

- 有關電腦上安裝的軟體的資訊：軟體應用程式和軟體供應商的名稱，登錄機碼及其值，已安裝的軟體元件的檔案資訊（核對總和（MD5、SHA2-256、SHA1）、名稱、檔案在電腦上的路徑、大小、版本和數位簽章）；

- 有關電腦的病毒防護狀態的資訊：正在使用的病毒資料庫的版本和發行時間戳記，工作的 ID 和執行掃描的軟體的 ID；

- 有關最終使用者正在下載的檔案的資訊：下載的檔案和下載頁的 URL 和 IP 位址，下載協議識別符和連線連接埠號，表示 URL 是否為惡意的狀態，檔案的屬性、大小和核對總和（MD5、SHA2-256、SHA1），下載檔案的處理程序的相關資訊（核對總和（MD5、SHA2-256、SHA1）、建立/構建日期和時間、自動執行狀態、內容、封裝程式的名稱、簽章資訊、可執行檔標誌、格式識別符和熵），檔案名稱及其在電腦上的路徑，檔案的數位簽章及其產生時的時間戳記，發生偵測的 URL 位址，頁面上看上去可疑或有害的指令碼的編號，有關產生的 HTTP 請求以及對它們的回應的資訊；

- 有關正在執行的應用程式及其模組的資訊：系統中正在執行的處理程序的資料（處理程序 ID (PID)，處理程序名稱，有關啟動處理程序的帳戶的資訊，啟動處理程序的應用程式和指令，受信任程式或處理程序的標誌，處理程序檔案的完整路徑及其核對總和（MD5、SHA2-256、SHA1），啟動命令列，處理程序完整性等級，處理程序所屬產品的敘述（產品名稱和發佈者詳細資訊），以及所使用的數位憑證和驗證它們的真實性所需的資訊或者關於是否缺少檔案數位簽章的資訊），以及有關載入到處理程序中的模組的資訊（模組的名稱、大小、類型、建立日期、內容、核對總和（MD5、SHA2-256、SHA1）以及在電腦上的路徑），PE 檔案頭資訊，封裝程式的名稱（如果檔案已封裝）；

- 有關所有潛在惡意物件和活動的資訊：偵測到的物件的名稱，電腦上物件的完整路徑，所處理檔案的核對總和（MD5、SHA2-256、SHA1），偵測日期和時間，感染檔案的名稱、大小和路徑，路徑範本代碼，可執行檔標誌，表示物件是否為容器的指示器，封裝程式名稱（如果檔案已封裝），檔案類型代碼，檔案格式 ID，惡意軟體執行的操作清單以及軟體和使用者針對其做出的回應決策，病毒資料庫的 ID 和這些病毒資料庫中用於制定決策的記錄的 ID，潛在惡意物件的指示器，偵測到的威脅在權利所有人分類中的名稱，危險等級，偵測狀態和偵測方法，包含在已分析上下文中的原因及上下文中檔案的序號，核對總和（MD5、SHA2-256、SHA1），用於傳送感染訊息或連結的應用程式的可執行檔的名稱和內容，被封鎖物件的主機的去個性化 IP 位址（IPv4 和 IPv6），檔案熵，檔案自動執行指示器，在系統中首次偵測到檔案的時間，上次傳送統計資訊後檔案被執行的次數，透過其收到惡意物件的郵件用戶端的名稱、核對總和（MD5、SHA2-256、SHA1）和大小，執行掃描的軟體工作的 ID，表示檔案信譽或簽章是否經過檢查的指示器，檔案處理結果，為物件收集的模式的核對總和 (MD5)，模式大小（以位元組為單位），以及使用的偵測技術的技術規格；

- 有關掃描的物件的資訊：檔案移入或移出的指定信任群組，將檔案移入該類別的理由，類別識別符，有關類別源的資訊和類別資料庫版本，檔案的受信任憑證標誌，檔案的供應商名稱，檔案版本，包含該檔案的軟體應用程式的名稱和版本；

- 有關偵測到的弱點的資訊：弱點資料庫中的弱點 ID，弱點危險等級；

- 有關可執行檔類比的資訊：檔案大小及其核對總和（MD5、SHA2-256、SHA1），模擬元件的版本，模擬深度，類比過程中獲得的邏輯塊內的一系列內容和函數，可執行檔的 PE 頭中的資料；

- 發起攻擊的電腦的 IP 位址（IPv4 和 IPv6），被當作網路攻擊目的的電腦連接埠號，包含攻擊的 IP 封包的協定的識別符，攻擊目的（組織名稱、網站），攻擊響應標記，攻擊的權重，信任等級；

- 有關與欺詐網路資源相關的攻擊的資訊，所存取網站的 DNS 和 IP 位址（IPv4 和 IPv6）；

- 請求的 Web 資源的 DNS 和 IP 位址（IPv4 或 IPv6），有關存取該 Web 資源的檔案和 Web 用戶端的資訊，檔案的名稱、大小和核對總和（MD5、SHA2-256、SHA1），檔案的完整路徑和路徑範本代碼，檢查其數位簽章的結果，及其在 KSN 中的狀態；

- 有關惡意軟體操作回溯的資訊：有關其活動被回溯的檔案的資料（檔案名稱、檔案的完整路徑、檔案的大小和核對總和（MD5、SHA2-256、SHA1）），有關刪除、重命名和複製檔案以及還原登錄檔中的值（登錄機碼的指令和值）的成功和失敗操作的資料，有關惡意軟體修改的系統檔案的資訊（回溯前後）；

- 有關為適應性異常控制元件設定的排除項目的資訊：觸發的規則的 ID 和狀態，觸發規則時軟體執行的操作，處理程序或執行緒執行可疑活動時所用的使用者帳戶的類型，有關執行可疑活動或受可疑活動支配的處理程序的資訊（指令碼 ID 或處理程序檔案名稱，處理程序檔案的完整路徑，路徑範本代碼，處理程序檔案的總和檢查碼（MD5、SHA2-256、SHA1））；有關執行了可疑操作的物件的資訊以及受可疑活動支配的物件的資訊（登錄機碼名稱或檔案名稱，檔案的完整路徑，路徑範本代碼和檔案的總和檢查碼（MD5、SHA2-256、SHA1））。

- 有關載入的軟體模組的資訊：模組檔案的名稱、大小和核對總和（MD5、SHA2-256、SHA1），模組檔案的完整路徑和路徑範本代碼，模組檔案的數位簽章設定，簽章建立資料和時間，為模組檔案簽章的主體和組織的名稱，載入模組的處理程序的 ID，模組供應商的名稱，以及載入佇列中模組的序號；

- 有關軟體與 KSN 服務的互動品質的資訊：產生統計資訊的時間段的開始和結束日期及時間，有關對所用的每個 KSN 服務的請求和連線的品質的資訊（KSN 服務 ID，成功請求數量，含有來自快取的回應的請求數量，不成功請求數量（網路問題、軟體設定中停用 KSN、路由不正確），成功請求的時間分佈，取消的請求的時間分佈，超出時間限制的請求的時間分佈，與取自快取的 KSN 的連線數，與 KSN 的成功連線數，與 KSN 的不成功連線數，成功事務數，不成功事務數，與 KSN 的成功連線的時間分佈，與 KSN 的不成功連線的時間分佈，成功事務的時間分佈，不成功事務的時間分佈）；

- 如果偵測到潛在惡意物件，將提供處理程序的記憶體中的資料的相關資訊：系統物件階層架構 (ObjectManager) 的元素、UEFI BIOS 記憶體中的資料、登錄機碼的名稱及其值；

- 有關系統記錄中的事件的資訊：事件的時間戳記，在其中發現事件的記錄的名稱，事件的類型和類別，事件來源的名稱和事件的敘述；

- 有關網路連線的資訊：啟動了開啟連接埠的處理程序的檔案的版本和核對總和（MD5、SHA2-256、SHA1），處理程序檔案的路徑和數位簽章，本機和遠程 IP 位址，本機和遠程連線連接埠號，連線狀態，連接埠開啟時間戳記；

- 有關在電腦上安裝和啟動軟體的日期的資訊：出售產品授權的合作夥伴的 ID，產品授權的序列號，來自啟動服務的票證的簽章標頭（區域啟動中心的 ID，啟動碼的總和檢查碼，票證的總和檢查碼，票證的建立日期，票證的唯一 ID，票證版本，產品授權狀態，票證的開始/結束日期和時間，產品授權的唯一 ID，產品授權版本），用於簽署票頭的憑證的 ID，金鑰檔案的總和檢查碼（MD5），電腦上軟體安裝的唯一ID，要更新的應用程式的類型和 Id，更新工作的 ID；

- 有關所有已安裝的更新集的資訊以及最近安裝/刪除的更新集的資訊，導致傳送更新資訊的事件的類型，上次安裝更新後經過的時間，有關任何目前已安裝的病毒資料庫的資訊；

- 有關電腦上的軟體執行的資訊：CPU 使用率資料，記憶體使用率資料（專用位元組，未分頁緩衝集區，分頁緩衝集區），軟體處理程序中的活動執行緒數和掛起執行緒數，以及錯誤發生前的軟體執行時間；

- 自軟體安裝以來和上次更新以來軟體轉儲和系統轉儲 (BSOD) 的次數，當機的軟體模組的識別符和版本，軟體處理程序中的記憶體堆疊，以及當機時的病毒資料庫的相關資訊；

- 有關系統轉儲 (BSOD) 的資料：指示電腦上發生 BSOD 的標誌，導致 BSOD 的驅動程式的名稱，驅動程式中的位址和記憶體堆疊，指示發生 BSOD 之前作業系統連線持續時間的標誌，當機的驅動程式的記憶體堆疊、儲存的記憶體傾印的類型，指示 BSOD 之前作業系統連線持續 10 分鐘以上的標誌、轉儲的唯一識別符，BSOD 的時間戳記；

- 有關軟體元件執行期間出現的錯誤或效能問題的資訊：軟體的狀態 ID，錯誤類型，代碼和原因以及發生錯誤的時間，元件的 ID，出現錯誤的產品的元件、模組和處理程序的 ID，出現錯誤的工作或更新類別的 ID，軟體使用的驅動程式的記錄（錯誤代碼、模組名稱、原始檔案的名稱和出現錯誤的列）；

- 有關病毒資料庫和軟體元件更新的資訊：在上次更新過程中下載以及目前更新過程中正在下載的索引檔案的名稱、日期和時間；

- 有關軟體操作異常終止的資訊：轉儲的建立時間戳記、類型，導致軟體操作異常終止的事件的類型（意外斷電、協力廠商應用程式當機），意外斷電的日期和時間；

- 有關軟體驅動程式與硬體和軟體的相容性的資訊：有關限制軟體元件功能的作業系統內容的資訊（安全啟動、KPTI、WHQL 強制、BitLocker、區分大小寫），安裝的下載軟體的類型（UEFI、BIOS），受信任平台模組 (TPM) 識別符，TPM 規範版本，有關電腦上安裝的 CPU 的資訊，代碼完整性和 Device Guard 的執行模式和參數，驅動程式的執行模式和使用目前模式的原因，軟體驅動程式的版本，電腦的軟體和硬體虛擬化支援狀態；

- 有關導致出錯的協力廠商應用程式的資訊：應用程式名稱、版本和中文化，系統應用程式記錄中關於該錯誤的錯誤代碼和資訊，發生錯誤的位址和協力廠商應用程式的記憶體堆疊，指示軟體元件中出現錯誤的標誌，出錯之前協力廠商應用程式的執行時長，出錯的應用程式處理程序映射的核對總和（MD5、SHA2-256、SHA1），應用程式處理程序映射的路徑和路徑範本代碼，系統記錄中與該應用程式相關的錯誤說明資訊，發生錯誤的應用程式模組的相關資訊（異常識別符，應用程式模組中偏移量形式的當機記憶體位址，模組的名稱和版本，權利所有人外掛程式中的應用程式當機識別符以及當機的記憶體堆疊，當機之前應用程式工作階段的持續時間）；

- 軟體更新程式元件的版本，在元件的生命週期內執行更新工作時更新程式元件當機的次數，更新工作類型的 ID，更新程式元件完成更新工作的失敗嘗試次數；

- 有關軟體系統監控元件執行的資訊：元件的完整版本，啟動元件時的日期和時間，溢出事件佇列的事件的代碼及此類事件的數量，佇列溢出事件的總數，有關事件的發起程式的處理程序的檔案的資訊（檔案名稱及其在電腦上的路徑、檔案路徑的範本代碼、與檔案關聯的處理程序的核對總和（MD5、SHA2-256、SHA1）、檔案版本），發生的事件攔截的識別符，攔截篩選器的完整版本，攔截的事件的類型的識別符，事件佇列的大小和佇列中第一個事件與目前事件之間的事件數量，佇列中過期事件的數量，有關目前事件的發起程式處理程序的檔案的資訊（檔案名稱及其在電腦上的路徑，檔案路徑的範本代碼，與檔案關聯的處理程序的核對總和（MD5、SHA2-256、SHA1）），事件處理持續時間，事件處理最大持續時間，傳送統計資訊的概率，有關超過處理時間限制的作業系統事件的資訊（事件的日期和時間，病毒資料庫的重複初始化次數，病毒資料庫更新後最近一次重複初始化的日期和時間，每個系統監控元件的事件處理延遲時間，排隊的事件數量，已處理的事件數量，目前類型的延遲事件數量，目前類型的事件的總延遲時間，所有事件的總延遲時間）；

- 發生軟體效能問題時來自 Windows 事件追蹤工具（Event Tracing for Windows，ETW）的資訊，來自 Microsoft 的 SysConfig / SysConfigEx / WinSATAssesssment 事件的提供者：有關電腦的資訊（型號，製造商，外殼的外形規格，版本），有關 Windows 效能指標的資訊（WinSAT 評估，Windows 效能指標），網域名稱，有關物理和邏輯處理器的資訊（物理和邏輯處理器的數量，製造商，型號，步進級別，核心數量，時鐘頻率，CPUID，快取）特性，邏輯處理器特性，支援的模式和指令的指示），有關 RAM 模組的資訊（類型，表單係數，製造商，型號，容量，記憶體分配的規模），有關網路介面的資訊（IP 和 MAC 位址，名稱，描述，網路介面的配置，按類型對網路套件的數量和大小進行的細分，網路交換速度，按類型對網路錯誤的數量進行的細分），IDE 控制器的配置，DNS 伺服器的 IP 位址，有關視訊卡的資訊（型號，描述，製造商，相容性，視訊記憶體容量，熒幕權限，每像素位元數，BIOS 版本），有關即插即用裝置的資訊（名稱，描述，裝置識別符 [PnP，ACPI]，有關磁碟和儲存裝置的資訊（磁碟或快閃磁碟機的數量，製造商，型號，磁碟容量，磁柱數，每個磁柱的磁道，每個磁道的磁區數，磁區容量，快取特性，序列號，分割數，SCSI 控制器的配置），有關邏輯磁碟的資訊（序列號，分割容量，磁碟區容量，磁碟區字母，分割類型，檔案系統類型，叢集數目，叢集大小，每個叢集的磁區數，空叢集和已佔用叢集的數目，可開機磁碟區的字母，與磁碟啟動相關的分割偏移位址），有關 BIOS 主機板的資訊（製造商，發布日期，版本），有關主機板的資訊（製造商，型號，類型），有關物理記憶體的資訊（共用和可用容量），有關作業系統服務的資訊（名稱，描述，狀態，標籤，有關處理程序的資訊 [名稱和 PID]，電腦的能耗參數，中斷控制器的配置，Windows 系統資料夾的路徑（Windows 和 System32），有關作業系統的資訊（版本，內部版本，發行日期，名稱），類型，安裝日期），頁面檔案的大小，有關監視器的資訊（數量，製造商，熒幕權限，分辨率容量，類型），有關視訊卡驅動的資訊（製造商，發布日期，版本）；

- 來自 ETW 的資訊，Microsoft 的 EventTrace/EventMetadata 事件的提供方：有關系統事件序列的資訊（類型、時間、日期、時區），帶追蹤結果的檔案中繼資料（名稱、結構、追蹤參數、按類型細分的偵錯運算元），有關作業系統的資訊（名稱、類型、版本、內部版本號、發佈日期、啟動時間）；

- 來自 ETW 的資訊，Microsoft 的處理程序/Microsoft Windows 核心處理程序/Microsoft Windows 核心處理器電源事件的提供方：有關已啟動和已完成處理程序的資訊（名稱、PID、啟動參數、命令列、返回代碼、電源管理參數、啟動和完成時間、存取權杖類型、SID、SessionID、已安裝的敘述符數），有關執行緒優先順序變化的資訊（TID、優先順序、時間），有關處理程序的磁碟操作的資訊（類型、時間、容量、編號），可用記憶體處理程序的結構和容量的變更歷程記錄；

- 來自 ETW 的資訊，Microsoft 的 StackWalk/Perfinfo 事件的提供方：有關效能計數器的資訊（單個程式碼片段的效能、函式呼叫的序列、PID、TID、ISR 和 DPC 的位址和內容）；

- 來自 ETW 的資訊，Microsoft 的 KernelTraceControl-Image ID 事件的提供方：有關可執行檔和動態庫的資訊（名稱、映射大小、完整路徑），有關 PDB 檔案的資訊（名稱、識別符），可執行檔的 VERSIONINFO 資來源資料（名稱、敘述、建立者、當地語係化、應用程式版本和識別符、檔案版本和識別符）；

- 來自 ETW 的資訊，Microsoft 的 FileIo/DiskIo/映射/Windows 核心磁碟事件的提供方：有關檔案和磁碟操作的資訊（類型、容量、開始時間、完成時間、持續時間、完成狀態、PID、TID、驅動程式函式呼叫位址、I/O 請求封包 (IRP)、Windows 檔案物件內容），有關檔案和磁碟操作所涉及的檔案的資訊（名稱、版本、大小、完整路徑、內容、偏移、映射核對總和、開啟和存取選項）；

- 來自 ETW 的資訊，Microsoft 的 PageFault 事件的提供方：有關記憶體頁面存取錯誤的資訊（位址、時間、容量、PID、TID、Windows 檔案物件內容、記憶體分配參數）；

- 來自 ETW 的資訊，Microsoft 的執行緒事件的提供方：有關執行緒建立/完成的資訊，有關已啟動的執行緒的資訊（PID、TID、堆疊大小、CPU 資源的優先順序和分配、I/O 資源、執行緒間的記憶體頁面、堆疊位址、初始函數位址、執行緒環境塊 (TEB) 的位址、Windows 服務標籤）；

- 來自 ETW 的資訊，Microsoft 的 Windows 核心記憶體事件的提供方：有關記憶體管理操作的資訊（完成狀態、時間、數量、PID），記憶體分配結構（類型、容量、SessionID、PID）；

- 有關發生效能問題時軟體操作的資訊：軟體安裝識別符，效能下降的類型和值，有關軟體內的事件序列的資訊（時間、時區、類型、完成狀態、軟體元件識別符、軟體執行場景識別符、TID、PID、函式呼叫位址），有關要檢查的網路連線的資訊（URL、連線方向、網路封包大小），有關 PDB 檔案的資訊（名稱、識別符、可執行檔的映射大小），有關要檢查的檔案的資訊（名稱、完整路徑、核對總和），軟體效能監控參數；

- 有關作業系統上次重新啟動失敗的資訊：作業系統安裝以來重新啟動失敗的次數，系統轉儲資料（錯誤的代碼和參數，導致作業系統執行出錯的模組的名稱、版本和核對總和 (CRC32)，模組內偏移量形式的錯誤位址，系統轉儲的核對總和（MD5、SHA2-256、SHA1））；

- 驗證用於對檔案簽章的數位憑證的真實性所需的資訊：憑證的指紋，核對總和演算法，憑證的公開金鑰和序號，憑證頒發者的名稱，憑證驗證的結果和憑證的資料庫識別符；

- 有關對軟體的自我防護執行攻擊的處理程序的資訊：處理程序檔案的名稱和大小，其核對總和（MD5、SHA2-256、SHA1），處理程序檔案的完整路徑和檔案路徑的範本代碼，建立/構建時間戳記，可執行檔標誌，處理程序檔案的內容，用於對處理程序檔案簽章的憑證的相關資訊，用於啟動處理程序的帳戶的代碼，為存取處理程序所執行的操作的 ID，用於執行操作的資源的類型（處理程序，檔案，登錄檔物件，FindWindow 搜尋函數），用於執行操作的資源的名稱，表示操作成功的標誌，處理程序檔案的狀態及其在 KSN 中的簽章；

- 權利所有人軟體的資訊：使用的軟體的完整版本、類型、當地語係化和操作狀態，已安裝的軟體元件的版本及其操作狀態，有關已安裝的軟體更新的資訊，TARGET 篩選器的值，用於連線到權利所有人的服務所使用協定的版本；

- 有關電腦上安裝的硬體的資訊：類型、名稱、型號名稱、固件版本、內建和所連線裝置的參數、帶有已安裝軟體的電腦的唯一識別符；

- 有關作業系統和已安裝更新的版本的資訊，作業系統執行模式的字體大小、版本和參數，作業系統核心檔案的版本和總和檢查碼（MD5、SHA2-256、SHA1），以及作業系統啟動日期和時間；
- 可執行檔和非可執行檔，全部或部分；
- 電腦 RAM 的一部分；
- 作業系統引導過程中涉及的磁區；
- 網路流量封包；
- 包含可疑物件和惡意物件的網頁和電子郵件；
- WMI 儲存區的類別和類別執行個體的描述；
- 應用程式活動報告：
  - 傳送的檔案的名稱、大小和版本，其描述和總和檢查碼（MD5，SHA2-256，SHA1），檔案格式識別符，檔案廠商的名稱，檔案所屬產品的名稱，到電腦上的檔案的完整路徑，路徑的範本代碼，檔案的建立和修改時間戳記；
  - 憑證有效期的開始和結束日期/時間（如果檔案具有數位簽章），簽章的日期和時間，憑證頒發者的名稱，有關憑證持有者的資訊，指紋，憑證的公鑰和適當算法，以及憑證序列號；
  - 執行處理程序的帳戶的名稱；
  - 執行處理程序的電腦名稱的總和檢查碼（MD5，SHA2-256，SHA1）；
  - 處理程序視窗的標題；
  - 病毒資料庫的識別符，根據權利擁有人分類偵測到的威脅的名稱；
  - 有關已安裝的產品授權的資料，其識別符、類型和到期日期；
  - 提供資訊時電腦的本機時間；
  - 處理程序存取的檔案的名稱和路徑；
  - 處理程序存取的登錄機碼的名稱及其值；
  - 處理程序存取的 URL 和 IP 位址；
  - 從中下載執行檔案的 URL 和 IP 位址。

# 使用 Detection and Response 解決方案時的資料提供

在安裝了 Kaspersky Endpoint Security 的電腦上會儲存準備自動傳送到 Kaspersky Endpoint Detection and Response、Kaspersky Sandbox 和 Kaspersky Anti Targeted Attack Platform 伺服器的資料。檔案以普通未加密的形式儲存在電腦上。

具體的資料集合取決於使用 Kaspersky Endpoint Security 的解決方案。

# Kaspersky Endpoint Detection and Response

若 Kaspersky Endpoint Security 被解除安裝，則應用程式本機儲存在電腦上的所有資料將被從電腦中刪除。

由於 IOC 掃描 工作執行（標準工作）收到的資料

Kaspersky Endpoint Security 會自動提交 *IOC 掃描* 工作執行結果的資料到卡巴斯基安全管理中心。

*IOC 掃描*工作執行結果中的資料可能包含以下資訊：

- 來自 ARP 表的 IP 位址
- 來自 ARP 表的實體地址
- DNS 記錄類型和名稱
- 受防護電腦的 IP 位址
- 受防護電腦的實體地址（MAC 位址）
- 事件日誌項目中的識別碼
- 記錄中的資料來源名稱
- 記錄名稱
- 事件時間
- 檔案的 MD5 和 SHA256 雜湊
- 檔案的完整名稱（包括路徑）
- 檔案大小
- 掃描期間建立連線的遠端 IP 位址和連接埠
- 本機介面卡 IP 位址
- 本機介面卡上開啟的連接埠
- 數字形式的通訊協定（符合 IANA 標準）
- 處理程序名稱
- 處理程序引數
- 處理程序檔案的路徑

- 處理程序的 Windows 識別碼 (PID)
- 父處理程序的 Windows 識別碼 (PID)
- 啟動處理程序的使用者帳戶
- 處理程序開始的日期和時間
- 服務名稱
- 服務說明
- DLL 服務的路徑和名稱（對於 svchost）
- 服務可執行檔的路徑和名稱
- 服務的 Windows 識別碼 (PID)
- 服務類型（例如，內核驅動程式或介面卡）
- 服務狀態
- 服務啟動模式
- 使用者帳戶名稱。
- 磁碟區名稱
- 磁碟區字母
- 磁碟區類型
- Windows 登錄值
- 登錄區值
- 登錄機碼路徑（沒有登錄區和值名稱）
- 登錄設定
- 系統（環境）
- 電腦上安裝的作業係統的名稱和版本
- 受防護電腦的網路名稱
- 受防護電腦所屬的網域或群組
- 瀏覽器名稱
- 瀏覽器版本
- 上次存取 Web 資源的時間
- 來自 HTTP 請求的 URL

- 用於 HTTP 請求的帳戶名稱
- 發出 HTTP 請求的處理程序的檔案名稱
- 發出 HTTP 請求的處理程序的檔案的完整路徑
- 發出 HTTP 請求的處理程序的 Windows 識別碼 (PID)
- HTTP 推薦者（HTTP 請求來源 URL）
- 透過 HTTP 請求的資源的 URI
- 有關 HTTP 使用者代理（發出 HTTP 請求的應用程式）的資訊
- HTTP 請求執行時間
- 發出 HTTP 請求的處理程序的唯一識別碼

用於建立威脅發展鏈的資料

用於建立威脅發展鏈的資料預設儲存 7 天。資料會自動傳送到卡巴斯基安全管理中心。

用於建立威脅發展鏈的資料可能包含以下資訊：

- 事件日期和時間
- 偵測名稱
- 掃描模式
- 與偵測相關的最後一個動作的狀態
- 偵測處理失敗的原因
- 偵測到的物件類型
- 偵測到的物件名稱
- 物件被處理後的威脅狀態
- 對物件執行操作失敗的原因
- 為回溯惡意操作而執行的操作
- 被處理物件的相關資訊：
  - 處理程序的唯一識別符
  - 父處理程序的唯一識別符
  - 處理程序檔案的唯一識別符

- Windows 處理程序識別符 (PID)
- 處理程序指令行
- 啟動處理程序的使用者帳戶
- 執行處理程序的登錄工作階段的代碼
- 執行處理程序的工作階段的類型
- 被處理的處理程序的完整性級別
- 在特權本機和網域群組中啟動處理程序的使用者帳戶的成員身分
- 被處理物件的識別符
- 被處理物件的全名
- 受防護裝置的識別符
- 物件全名（本機檔案名稱或下載的檔案網址）
- 被處理物件的 MD5 或 SHA256 雜湊
- 被處理物件的類型
- 被處理物件的建立日期
- 最後修改被處理物件的日期
- 被處理物件的大小
- 被處理物件的屬性
- 簽署被處理物件的組織
- 被處理物件數位憑證校驗結果
- 被處理物件的安全識別符 (SID)
- 被處理物件的時區識別符
- 被處理物件下載網址（僅適用於磁碟上的檔案）
- 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 雜湊
- 最後修改檔案的應用程式的名稱
- 最後修改檔案的應用程式的 MD5 和 SHA256 雜湊
- 被處理物件啟動的數目
- 首次啟動被處理物件的日期和時間

- 檔案的唯一識別符
- 檔案全名（本機檔案名稱或下載的檔案網址）
- 被處理的 Windows 登錄變數的路徑
- 被處理的 Windows 登錄變數的名稱
- 被處理的 Windows 登錄變數的值
- 被處理的 Windows 登錄變數的類型
- 自動執行點中被處理登錄機碼成員資格指示器
- 被處理的 Web 請求的網址
- 被處理的 Web 請求的連接來源
- 被處理的 Web 請求的使用者代理
- 被處理的 Web 請求的類型（`GET` or `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）
- 嵌入惡意代碼的處理程序的識別符

# Kaspersky Sandbox

若 Kaspersky Endpoint Security 被解除安裝，則應用程式本機儲存在電腦上的所有資料將被從電腦中刪除。

服務資料

Kaspersky Endpoint Security 儲存自動響應期間處理的以下資料：

- 在配置 Kaspersky Endpoint Security 的內建代理期間由使用者輸入的被處理檔案和資料：
  - 已隔離的檔案
  - 用於與 Kaspersky Sandbox 整合的憑證的公開金鑰
- Kaspersky Endpoint Security 內建代理的快取：
  - 掃描結果寫入快取的時間
  - 掃描工作的 MD5 雜湊

    - 掃描工作識別碼
    - 物件的掃描結果
- 物件掃描請求佇列：
    - 佇列中物件的 ID
    - 物件放入佇列的時間
    - 佇列中物件的處理狀態
    - 使用者工作階段在建立物件掃描工作的作業係統中的 ID
    - 其帳戶被用於建立工作的作業係統使用者的系統識別碼 (SID)
    - 物件掃描工作的 MD5 雜湊
- 有關 Kaspersky Endpoint Security 內建代理正在等待來自 Kaspersky Sandbox 的掃描結果的工作的資訊：
    - 收到物件掃描工作的時間
    - 物件處理狀態
    - 使用者工作階段在建立物件掃描工作的作業係統中的 ID
    - 物件掃描工作的識別符
    - 物件掃描工作的 MD5 雜湊
    - 其帳戶被用於建立工作的作業係統使用者的系統識別碼 (SID)
    - 自動建立的 IOC 的 XML 架構
    - 被掃描物件的 MD5 或 SHA256 雜湊
    - 處理錯誤
    - 為其建立工作的物件的名稱
    - 物件的掃描結果

Kaspersky Sandbox 請求中的資料

來自 Kaspersky Endpoint Security 內置代理對 Kaspersky Sandbox 的請求的以下資料儲存在本機電腦上：

- 掃描工作的 MD5 雜湊
- 掃描工作識別碼
- 被掃描物件和所有相關檔案

由於 IOC 掃描 工作執行（獨立工作）收到的資料

Kaspersky Endpoint Security 會自動提交 *IOC 掃描* 工作執行結果的資料到卡巴斯基安全管理中心。

*IOC 掃描*工作執行結果中的資料可能包含以下資訊：

- 來自 ARP 表的 IP 位址
- 來自 ARP 表的實體地址
- DNS 記錄類型和名稱
- 受防護電腦的 IP 位址
- 受防護電腦的實體地址（MAC 位址）
- 事件日誌項目中的識別碼
- 記錄中的資料來源名稱
- 記錄名稱
- 事件時間
- 檔案的 MD5 和 SHA256 雜湊
- 檔案的完整名稱（包括路徑）
- 檔案大小
- 掃描期間建立連線的遠端 IP 位址和連接埠
- 本機介面卡 IP 位址
- 本機介面卡上開啟的連接埠
- 數字形式的通訊協定（符合 IANA 標準）
- 處理程序名稱
- 處理程序引數
- 處理程序檔案的路徑
- 處理程序的 Windows 識別碼 (PID)
- 父處理程序的 Windows 識別碼 (PID)
- 啟動處理程序的使用者帳戶
- 處理程序開始的日期和時間
- 服務名稱

- 服務說明
- DLL 服務的路徑和名稱（對於 svchost）
- 服務可執行檔的路徑和名稱
- 服務的 Windows 識別碼 (PID)
- 服務類型（例如，內核驅動程式或介面卡）
- 服務狀態
- 服務啟動模式
- 使用者帳戶名稱。
- 磁碟區名稱
- 磁碟區字母
- 磁碟區類型
- Windows 登錄值
- 登錄區值
- 登錄機碼路徑（沒有登錄區和值名稱）
- 登錄設定
- 系統（環境）
- 電腦上安裝的作業係統的名稱和版本
- 受防護電腦的網路名稱
- 受防護電腦所屬的網域或群組
- 瀏覽器名稱
- 瀏覽器版本
- 上次存取 Web 資源的時間
- 來自 HTTP 請求的 URL
- 用於 HTTP 請求的帳戶名稱
- 發出 HTTP 請求的處理程序的檔案名稱
- 發出 HTTP 請求的處理程序的檔案的完整路徑
- 發出 HTTP 請求的處理程序的 Windows 識別碼 (PID)
- HTTP 推薦者（HTTP 請求來源 URL）

- 透過 HTTP 請求的資源的 URI
- 有關 HTTP 使用者代理（發出 HTTP 請求的應用程式）的資訊
- HTTP 請求執行時間
- 發出 HTTP 請求的處理程序的唯一識別碼

# Kaspersky Anti Targeted Attack Platform (EDR)

若 Kaspersky Endpoint Security 被解除安裝，則應用程式本機儲存在電腦上的所有資料將被從電腦中刪除。

服務資料

Kaspersky Endpoint Security 的內建代理在本機儲存以下資料：

- 在配置 Kaspersky Endpoint Security 的內建代理期間由使用者輸入的被處理檔案和資料：
  - 已隔離的檔案
  - Kaspersky Endpoint Security 內建代理設定：
    - 用於與 Central Node 整合的憑證的公開金鑰
    - 產品授權資料
- 與 Central Node 整合所需的資料：
  - 遙測事件封包佇列
  - 從 Central Node 接收到的 IOC 檔案識別符的快取
  - 要在 *Get 檔案*工作中傳遞到伺服器的物件
  - *Get 鑒定*工作結果報告

KATA (EDR) 請求中的資料

與 Kaspersky Anti Targeted Attack Platform 整合時，以下資料儲存在本機電腦上：

來自 Kaspersky Endpoint Security 的內建代理請求 Central Node 元件的資料：

- 在同步請求中：
  - 唯一 ID
  - 伺服器網址的基本部分
  - 電腦名稱
  - 電腦 IP 位址
  - 電腦 MAC 位址
  - 電腦上的本機時間
  - Kaspersky Endpoint Security 的自我防御狀態
  - 電腦上安裝的作業係統的名稱和版本
  - Kaspersky Endpoint Security 的版本
  - 應用程式設定和工作設定的版本
  - 工作狀態：工作的識別符、執行狀態、錯誤代碼
- 在從伺服器獲取檔案的請求中：
  - 檔案的唯一識別符
  - 唯一的 Kaspersky Endpoint Security 識別符
  - 憑證的唯一識別符
  - 安裝了 Central Node 元件的伺服器網址的基本部分
  - 主機 IP 位址
- 在工作執行結果的報告中：
  - 主機 IP 位址
  - 有關在 IOC 掃描或 YARA 掃描期間偵測到的物件的資訊
  - 完成工作後執行的附加操作的標誌
  - 工作執行錯誤和返回代碼
  - 工作完成狀態
  - 工作完成時間
  - 用於執行工作的設定的版本

- 有關提交到伺服器的物件、隔離物件和從隔離區還原的物件的資訊：物件路徑、MD5 和 SHA256 雜湊、隔離物件的識別符
- 有關根據伺服器請求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 雜湊
- 有關應伺服器請求在電腦上啟動或停止的服務的資訊：服務名稱、啟動類型、錯誤代碼、服務檔案映像的 MD5 和 SHA256 雜湊
- 有關為 YARA 掃描建立記憶體傾印的物件的資訊（路徑、傾印檔案識別符）
- 伺服器請求的檔案
- 遙測封包
- 關於正在執行的處理程序的資料：
  - 可執行檔案名稱，包括完整路徑和副檔名
  - 處理程序自動執行參數
  - 處理程序 ID
  - 登入工作階段 ID
  - 登入工作階段名稱
  - 處理程序開始的日期和時間
  - 物件的 MD5 和 SHA256 雜湊
- 檔案資料：
  - 檔案路徑
  - 檔案名稱
  - 檔案大小
  - 檔案屬性
  - 檔案建立的日期和時間
  - 上次修改檔案的日期和時間
  - 檔案描述
  - 公司名稱
  - 物件的 MD5 和 SHA256 雜湊
  - 登錄機碼（適用於自動執行點）

- 抓取物件資訊時發生的錯誤資料：
  - 發生錯誤時被處理的物件的全名
  - 錯誤代碼
- 遙測資料：
  - 主機 IP 位址
  - 確認的更新操作之前登錄中的資料類型
  - 確認的變更操作之前登錄機碼中的資料
  - 被處理指令碼的文字或其中的一部分
  - 被處理物件的類型
  - 將指令傳遞給指令解釋器的方式

從 Central Node 元件的請求到 Kaspersky Endpoint Security 的內建代理的資料：

- 工作設定：
  - 工作類型
  - 工作排程設定
  - 可以執行工作的帳戶的名稱和密碼
  - 設定版本
  - 隔離物件的識別符
  - 物件路徑
  - 物件的 MD5 和 SHA256 雜湊
  - 使用引數啟動處理程序的指令行
  - 完成工作後執行的附加操作的標誌
  - 要從伺服器抓取的 IOC 檔案識別符
  - IOC 檔案
  - 服務名稱
  - 服務啟動類型
  - 必須為其接收 *Get 鑒定*工作結果的資料夾
  - *Get 鑒定*工作的物件名稱和副檔名的遮罩

- 網路隔離設定：
  - 設定類型
  - 設定版本
  - 網路隔離排除項目和排除項目設定清單：流量方向、IP 位址、連接埠、通訊協定和可執行檔的完整路徑
  - 附加操作的旗標
  - 自動隔離停用時間
- 執行防護設定：
  - 設定類型
  - 設定版本
  - 執行預防規則和規則設定的清單：物件路徑、物件類型、物件的 MD5 和 SHA256 雜湊
  - 附加操作的旗標
- 事件篩選設定：
  - 模組名稱
  - 物件的完整路徑
  - 物件的 MD5 和 SHA256 雜湊
  - Windows 事件記錄中項目的識別符
  - 數位憑證設定
  - 流量方向、IP 位址、連接埠、通訊協定、可執行檔的完整路徑
  - 使用者名稱
  - 使用者登入名類型
  - 套用篩選器的遙測事件類型

### YARA 掃描結果中的資料

Kaspersky Endpoint Security 內建代理會自動將 YARA 掃描結果傳輸至 Kaspersky Anti Targeted Attack Platform 以構建威脅發展鏈。

資料臨時儲存在本機佇列中，用於向 Kaspersky Anti Targeted Attack Platform 伺服器傳送工作執行結果。資料將在傳送後被從臨時儲存中刪除。

YARA 掃描結果包含以下資料：

- 檔案的 MD5 和 SHA256 雜湊
- 檔案完整名稱
- 檔案路徑
- 檔案大小
- 處理程序名稱
- 處理程序引數
- 處理程序檔案的路徑
- 處理程序的 Windows 識別碼 (PID)
- 父處理程序的 Windows 識別碼 (PID)
- 啟動處理程序的使用者帳戶
- 處理程序開始的日期和時間

# 符合歐洲聯盟法規（GDPR）

在以下情況下，Kaspersky Endpoint Security 可能會將資料傳輸到卡巴斯基：

- 使用卡巴斯基安全網路。
- 用啟動碼啟動應用程式。
- 更新應用程式模組和病毒資料庫。
- 跟隨應用程式介面中的連接。

無論資料分類和接收資料的地區如何，卡巴斯基都遵守高標準的資料安全性，並採取各種法律、組織和技術措施來防護使用者資料，確保資料安全性和機密性，並確保實現適用法律保證的使用者權利。隱私政策的文本包含在應用程式分發套件中，可以在卡巴斯基網站上找到。

在使用 Kaspersky Endpoint Security 之前，請仔細閱讀最終使用者產品授權協議和卡巴斯基安全網路聲明中傳輸資料的描述。如果根據您當地的法規或標準，在所述任何情況下從 Kaspersky Endpoint Security 傳輸的特定資料都可以歸類為個人資料，則您必須確保對這些資料進行合法處理並獲得最終使用者的同意，以收集和傳輸這樣的資料。

請閱讀最終使用者產品授權協議並存取 Kaspersky 網站瞭解當您接受《最終使用者產品授權協議》和同意《卡巴斯基安全網路聲明》之後我們如何接收、儲存和銷毀有關程式使用的資訊。license.txt 和 ksn_<語言 ID>.txt 檔案包含最終使用者產品授權協議的文字，卡巴斯基安全網路聲明包含在應用程式分發套件中。

如果您不想將資料傳輸到卡巴斯基，可以停用資料供應。

## 使用卡巴斯基安全網路

使用卡巴斯基安全網路即表明您同意自動提供卡巴斯基安全網路聲明中列出的資料。如果您不同意向卡巴斯基提供此資料，請使用卡巴斯基私有安全網路 (KPSN) 或停用 KSN。有關 KPSN 的詳細資訊，請參閱卡巴斯基私有安全網路的文件。

## 用啟動碼啟動應用程式

使用啟動碼即表明您同意自動提供最終使用者產品授權協議中列出的資料。如果您不同意提供此資料給 Kaspersky，請使用使用金鑰檔案來啟動 Kaspersky Endpoint Security。

## 更新應用程式模組和病毒資料庫

使用 Kaspersky 伺服器即表明您同意自動提供最終使用者產品授權協議中列出的資料。卡巴斯基需要此資訊以驗證 Kaspersky Endpoint Security 正在被合法使用。如果您不同意將這些資訊提供給 Kaspersky，請使用卡巴斯基安全管理中心進行資料庫更新或使用Kaspersky Update Utility。

## 跟隨應用程式介面中的連接

使用應用程式介面中的連接即表明您同意自動提供最終使用者產品授權協議中列出的資料。在每個特定連接中傳輸的資料的精確清單取決於該連接在應用程式介面中的位置以及它要解決的問題。如果您不同意向卡巴斯基提供此資料，請使用簡化的應用程式介面或隱藏應用程式介面。

## 傾印寫入

如果啟用了轉儲寫入，Kaspersky Endpoint Security 將建立一個傾印檔案，該檔案將包含建立該傾印檔案時來自應用程式處理程序的所有記憶體資料。

# 準備開始

安裝 Kaspersky Endpoint Security 後，您可以使用以下介面管理應用程式：

- 本機應用程式介面。
- 卡巴斯基安全管理中心管理主控台。
- 卡巴斯基安全管理中心網頁主控台。
- 卡巴斯基安全管理中心雲端主控台。

## 卡巴斯基安全管理中心管理主控台

卡巴斯基安全管理中心允許您遠端安裝和移除、啟動和停止 Kaspersky Endpoint Security，配置應用程式設定，變更可用應用程式元件的集合，新增金鑰以及啟動和停止更新和掃描工作。

可以使用卡巴斯基安全管理中心管理外掛程式透過 Kaspersky Endpoint Security 管理應用程式。

有關透過卡巴斯基安全管理中心管理應用程式的詳細資訊，請參閱卡巴斯基安全管理中心說明。

## 卡巴斯基安全管理中心網頁主控台或卡巴斯基安全管理中心雲端主控台

卡巴斯基安全管理中心網頁主控台（以下簡稱"*網頁主控台*"）是用於集中執行主要工作來管理和維護組織網路的安全系統的 Web 應用程式。網頁主控台是提供使用者介面的卡巴斯基安全管理中心元件。有關卡巴斯基安全管理中心網頁主控台的詳細資訊，請參閱卡巴斯基安全管理中心說明。

卡巴斯基安全管理中心雲端主控台（以下簡稱"*雲端主控台*"）是用於防護和管理組織網路的基於雲端的解決方案。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。

網頁主控台和雲端主控台允許您執行以下操作：

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

透過網頁主控台、雲端主控台和卡巴斯基安全管理中心管理主控台管理 Kaspersky Endpoint Security 都提供不同的管理功能。對於不同的主控台，可用的元件和工作也有所不同。

# 關於 Kaspersky Endpoint Security for Windows 管理外掛程式

Kaspersky Endpoint Security for Windows 管理外掛程式允許在 Kaspersky Endpoint Security 和卡巴斯基安全管理中心之間進行互動。透過管理外掛程式，您可以使用政策、工作和本機應用程式設定來管理 Kaspersky Endpoint Security。該 Web 外掛程式提供了與卡巴斯基安全管理中心網頁主控台進行互動的功能。

管理外掛程式的版本會根據用戶端電腦上所安裝 Kaspersky Endpoint Security 應用程式版本的不同而有所不同。如果已安裝的管理外掛程式版本的功能少於已安裝的 Kaspersky Endpoint Security 版本，則缺少的功能的設定不受管理外掛程式的約束。這些設定可以由使用者在 Kaspersky Endpoint Security 的本機介面中修改。

預設情況下，卡巴斯基安全管理中心網頁主控台中不安裝 Web 外掛程式。 必須在安裝了卡巴斯基安全管理中心網頁主控台的電腦上安裝 Web 外掛程式。有權在瀏覽器中存取網頁主控台的所有管理員都可以使用該 Web 外掛程式的功能。您可以在網頁主控台介面中檢視已安裝的 Web 外掛程式清單（**主控台設定 → Web 外掛程式**）。有關 Web 外掛程式版本與網頁主控台的相容性的詳細資訊，請參閱卡巴斯基安全管理中心說明。

如果您將 Kaspersky Endpoint Security 作為 Kaspersky Endpoint Detection and Response Optimum 解決方案的一部分使用，則必須安裝 Kaspersky Endpoint Detection and Response 管理外掛程式。您需要管理外掛程式來顯示警示詳細資訊。*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。因此，要建立威脅回應工作，您需要 Kaspersky Endpoint Security 管理外掛程式；要檢視警示詳細資訊，您需要 EDR 管理外掛程式。

## 安裝 Web 外掛程式

您可以按如下方式安裝該 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"安裝 Web 外掛程式。

  第一次將網頁主控台連線到管理伺服器時，網頁主控台會自動提示您執行快速啟動精靈。您也可以在網頁主控台介面中執行快速啟動精靈（**發現和佈署 → 佈署和指派 → 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。有關卡巴斯基安全管理中心網頁主控台的"快速啟動精靈"的更多詳細資訊，請參閱 卡巴斯基安全管理中心說明 。

- 從網頁主控台中的可用分發套件清單安裝 Web 外掛程式。

  要安裝 Web 外掛程式，請在網頁主控台介面中選取 Kaspersky Endpoint Security Web 外掛程式的分發套件（**主控台設定 → Web 外掛程式**）。在新版本的 Kaspersky 應用程式發佈後，可用分發套件清單會自動更新。

- 將分發套件從外部來源下載到網頁主控台。

  要安裝 Web 外掛程式，請在網頁主控台介面中新增 Kaspersky Endpoint Security Web 外掛程式分發套件的 ZIP 存檔（**主控台設定 → Web 外掛程式**）。例如，可以在 Kaspersky 網站下載 Web 外掛程式的分發套件。

從 Kaspersky Endpoint Security 12.11 for Windows 開始，Web 外掛程式的安裝過程改變了。分發套件現在包含兩個 Web 外掛程式：*Kaspersky Endpoint Security for Windows 12.12.0* 和 *Unified Protection and Management Plug-in*。這是由於卡巴斯基應用程式的管理過渡到使用單一的統一 Web 外掛程式所致。統一的 Web 外掛程式允許建立單一政策來管理多個卡巴斯基應用程式（例如，Kaspersky Endpoint Security for Windows、macOS和 Linux）。過渡到統一的 Web 外掛程式可能需要多個版本。過渡完成後，分發套件將僅包含 *Unified Protection and Management Plug-in*。

### 更新管理外掛程式

要更新 Kaspersky Endpoint Security for Windows 管理外掛程式，請下載該外掛程式的最新版本（包含在分發套件中），並執行外掛程式安裝精靈。

如果有新版本的 Web 外掛程式可用，網頁主控台將顯示通知"*所用外掛程式有更新*"。您可以繼續從該網頁主控台通知更新 Web 外掛程式版本。您可以在網頁主控台介面中手動檢查新 Web 外掛程式更新（"**主控台設定**"→"**Web 外掛程式**"）。更新過程中將自動刪除以前版本的 Web 外掛程式。

Web 外掛程式更新後，將儲存已有項目（例如，政策或工作）。用於實現 Kaspersky Endpoint Security 新功能的新項目設定將顯示在現有項目中，並採用預設值。

您可以按如下方式更新 Web 外掛程式：

- 在線上模式下，在 Web 外掛程式清單中更新 Web 外掛程式。

  要更新 Web 外掛程式，必須在網頁主控台介面中選取 Kaspersky Endpoint Security Web 外掛程式的分發套件（"**主控台設定**"→"**Web 外掛程式**"）。網頁主控台將在 Kaspersky 伺服器中檢查可用更新，並下載相關更新。

- 從檔案更新 Web 外掛程式。

  要更新 Web 外掛程式，必須在網頁主控台介面中選取 Kaspersky Endpoint Security for Windows Web 外掛程式的分發套件的 ZIP 存檔（**主控台設定 → Web 外掛程式**）。例如，可以在 Kaspersky 網站下載 Web 外掛程式的分發套件。您只能將 Kaspersky Endpoint Security Web 外掛程式更新到最新版本。Web 外掛程式不能更新到較舊版本。

如果開啟了任何項目（如政策或工作），則 Web 外掛程式將檢查其相容性資訊。如果 Web 外掛程式的版本等於或晚於相容性資訊中指定的版本，則您可變更此項目的設定。否則您無法使用 Web 外掛程式變更所選項目的設定。建議更新 Web 外掛程式。

# 使用不同版本的管理外掛程式時的特別考慮

只有當您的管理外掛程式的版本等於或者晚於 Kaspersky Endpoint Security 與管理外掛程式相容性資訊中指定的版本時，您才可以透過卡巴斯基安全管理中心管理 Kaspersky Endpoint Security。您可以在包括在分發套件中的 installer.ini 檔案中檢視管理外掛程式的最低要求版本。

如果開啟了任何項目（如政策或工作），則管理外掛程式將檢查其相容性資訊。如果管理外掛程式的版本等於或晚於相容性資訊中指定的版本，則您可變更此項目的設定。否則您無法使用管理外掛程式變更所選項目的設定。建議升級管理外掛程式。

如果在管理主控台中安裝了 Kaspersky Endpoint Security 管理外掛程式，在安裝新版本的管理外掛程式時請考慮以下事項：

- 以前版本的 Kaspersky Endpoint Security 管理外掛程式將被移除。
- 新版本的 Kaspersky Endpoint Security 管理外掛程式支援管理使用者電腦上的 Kaspersky Endpoint Security for Windows。
- 您可以使用新版本的管理外掛程式變更由以前版本的管理外掛程式建立的政策、工作和其他項目中的設定。
- 對於新設定，新版本的管理外掛程式會在第一次儲存政策、政策設定檔或工作時分配預設值。

  升級管理外掛程式後，建議檢查新設定的值並將其儲存在政策和政策設定檔中。如果不執行此操作，使用者電腦上的新 Kaspersky Endpoint Security 設定群組將採用預設值並可以編輯（ 內容）。建議從頂級層級的政策和政策設定檔開始檢查設定。還建議使用有權存取所有卡巴斯基安全管理中心功能區域的使用者帳戶。

  要瞭解應用程式的新功能，請參閱版本說明或應用程式說明。

- 如果新版本的管理外掛程式的一組設定中新增了新參數，先前為該群組設定的 / 內容定義的狀態不會變更。

# 使用加密協定與外部服務進行交互時的特殊考量

Kaspersky Endpoint Security 和卡巴斯基安全管理中心使用帶有 TLS（Transport Layer Security）的加密通訊通道來與 Kaspersky 的外部服務一起使用。Kaspersky Endpoint Security 使用外部服務來實現以下功能：

- 更新資料庫和應用程式軟體模組；
- 用啟動碼啟動應用程式（啟動 2.0）；
- 使用卡巴斯基安全網路。

TLS 的使用透過提供以下功能來保護應用程式的安全：

- 加密。訊息的內容是機密的，不會透露給第三方使用者。
- 完整性郵件接收者確定自傳送者轉發郵件以來，郵件內容尚未修改。
- 身分驗證。收件人確定僅與受信任的卡巴斯基伺服器建立通訊。

Kaspersky Endpoint Security 使用公開金鑰憑證進行伺服器身分驗證。使用憑證需要Public Key Infrastructure（PKI）。憑證授權是 PKI 的一部分。卡巴斯基使用自己的憑證授權，因為卡巴斯基的服務具有高度技術性且不公開。在這種情況下，如果撤銷了 Thawte、VeriSign、GlobalTrust 和其他憑證的根憑證，則卡巴斯基 PKI 仍可正常運行而不會中斷。

Kaspersky Endpoint Security 認為具有 MITM（支援 HTTPS 協定解析的軟體和硬體工具）的環境是不安全的。使用卡巴斯基服務時可能會遇到錯誤。例如，可能會出現關於使用Self-Signed Certificate的錯誤。由於您環境中的 HTTPS 檢查工具無法識別 Kaspersky PKI，因此可能會出現這些錯誤。要糾正這些問題，必須設定排除項目以與外部服務進行交互。

# 程式介面




應用程式主視窗

| | |
|---|---|
| **正在監控** | • **報告**檢視應用程式運行期間發生的事件、單個元件和工作。<br>• **備份**檢視應用程式已刪除的感染檔案的已儲存副本的清單。<br>• **威脅偵測技術**檢視有關威脅偵測技術以及這些技術偵測到的威脅數量的資訊。<br>• **卡巴斯基安全網路**Kaspersky Endpoint Security 和卡巴斯基安全網路之間的連線狀態以及全球 KSN 統計資訊。*卡巴斯基安全網路（KSN）*是雲端服務的基礎結構，可提供對線上卡巴斯基知識庫的存取，該知識庫包含有關檔案、網頁資源和軟體信譽的資訊。使用卡巴斯基安全網路的資料可確保 Kaspersky 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 提供有關所掃描檔案的類別和信譽的資訊，以及有關所掃描網址的信譽的資訊。<br>• **應用程式活動監控**檢視有關已安裝應用程式操作的資訊。應用程式活動監控將保持對檔案、登錄檔以及與應用程式關聯的作業系統事件的偵錯。<br>• **網路監控**。即時檢視有關電腦網路活動的資訊。<br>• **加密監控器**及時監控磁碟加密或解密過程。如果安裝了 Kaspersky Disk Encryption 元件或 BitLocker 磁碟機加密元件，則加密監控可用。 |
| **安全** | 已安裝元件的運行狀態。您也可以繼續配置元件或者檢視報告。 |
| **更新** | 管理 Kaspersky Endpoint Security 更新工作。您可以更新病毒資料庫和應用程式模組並回溯上一次更新。管理員可以對使用者隱藏該區域或者限制工作管理。 |
| **工作** | 管理 Kaspersky Endpoint Security 掃描工作。您可以執行惡意軟體掃描和應用程式完整性檢查。管理員可以向使用者隱藏工作或限制工作管理。 |
| **產品授權** | 應用程式產品授權。您可以購買產品授權，啟動應用程式或續約訂購。您還可以檢視有關當前產品授權的資訊。 |
| ⚙ | 配置應用程式設定。管理員可以禁止變更卡巴斯基安全管理中心中的設定。 |
| ? | 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。您也可以前往 Kaspersky 資訊資源，其提供實用的資訊、建議以及有關如何購買、安裝和使用應用程式的常見問題解答。 |
| 🔔 | 包含有關可用更新以及對加密檔案和裝置的存取請求的資訊的訊息。 |

# 工作列通知區域中的程式圖示

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

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

本圖示有以下功能：

- 顯示應用程式的活動。
- 是存取內容功能表和應用程式主視窗的快速方式。

提供以下應用程式圖示狀態以顯示應用程式執行資訊：

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

應用程式圖示的內容功能表包含下列項目：

- **Kaspersky Endpoint Security for Windows**開啟主應用程式視窗。在此視窗中，您可以調節應用程式元件和工作的執行，並檢視已處理的檔案和偵測到的威脅的統計資料。
- **暫停防護 / 還原防護**。暫停政策中不帶鎖標記 () 的所有防護和控制元件的執行。在執行此操作之前，建議停用卡巴斯基安全管理中心政策。

  在暫停防護和控制元件的執行之前，應用程式會請求 Kaspersky Endpoint Security 的存取密碼（帳戶密碼或暫時密碼）。您隨後可以選擇暫停時間段：特定一段時間、直至重新啟動或使用者請求後。

  如果已啟用密碼防護，則此內容功能表項可用。要還原防護和控制元件執行，請在應用程式的內容功能表中點擊**"還原防護"**。

  暫停防護和控制元件的執行不會影響更新和惡意軟體掃描工作的效能。應用程式也繼續使用卡巴斯基安全網路。

- **停用政策 / 啟用政策**。在電腦上停用卡巴斯基安全管理中心政策。所有 Kaspersky Endpoint Security 設定均可進行配置，包括政策中已上鎖的設定 ()。如果停用政策，應用程式將請求存取 Kaspersky Endpoint Security 的密碼（帳戶密碼或暫時密碼）。如果已啟用密碼防護，則此內容功能表項可用。要啟用政策，請在應用程式的內容功能表中選擇**"啟用政策"**。
- **設定**開啟應用程式設定視窗。
- **支援**這將開啟包含聯絡 Kaspersky 技術支援所需資訊的視窗。
- **關於**此項目可開啟一個包含應用程式詳細資訊的視窗。

- **結束**本項目可結束 Kaspersky Endpoint Security。點擊內容功能表中的"結束"項目會導致應用程式結束記憶體。




應用程式圖示的右鍵選單

# 簡化的應用程式介面

如果將配置了"顯示簡化應用程式介面"的卡巴斯基安全管理中心政策應用於已安裝 Kaspersky Endpoint Security 的用戶端電腦，則在此用戶端電腦上不能使用應用程式主視窗。右鍵點擊 Kaspersky Endpoint Security 圖示可開啟內容功能表（如下圖），其中包含以下項目：

- **停用政策 / 啟用政策**。在電腦上停用卡巴斯基安全管理中心政策。所有 Kaspersky Endpoint Security 設定均可進行配置，包括政策中已上鎖的設定 (🔒)。如果停用政策，應用程式將請求存取 Kaspersky Endpoint Security 的密碼（帳戶密碼或暫時密碼）。如果已啟用密碼防護，則此內容功能表項可用。要啟用政策，請在應用程式的內容功能表中選擇"**啟用政策**"。

- **工作**包含以下項的下拉清單：

  - **應用程式完整性檢查**
  - **回溯資料庫到先前的版本**
  - **完整掃描**
  - **自訂掃描**
  - **關鍵區域掃描**
  - **更新**

- **支援**這將開啟包含聯絡 Kaspersky 技術支援所需資訊的視窗。

- **結束**本項目可結束 Kaspersky Endpoint Security。點擊內容功能表中的"結束"項目會導致應用程式結束記憶體。




顯示簡化介面時應用程式圖示的內容功能表

# 設定應用程式介面的顯示

您可以為使用者設定應用程式介面的顯示模式。使用者可以透過以下方式與應用程式進行互動：

- **顯示簡化介面**在用戶端電腦上，主應用程式視窗不可存取，只有 Windows 通知區域中的圖示可用。在該圖示的內容功能表中，使用者可以使用 Kaspersky Endpoint Security 執行有限數量的操作。Kaspersky Endpoint Security 還會在應用程式圖示上方顯示通知。

- **顯示使用者介面**在用戶端電腦上，Kaspersky Endpoint Security 的主視窗和 Windows 通知區域中的圖示均可用。在該圖示的內容功能表中，使用者可以使用 Kaspersky Endpoint Security 執行操作。Kaspersky Endpoint Security 還會在應用程式圖示上方顯示通知。

- **不顯示使用者介面**在用戶端電腦上，不顯示 Kaspersky Endpoint Security 操作的跡象。Windows 通知區域中的圖示和通知不可用。

**如何在管理主控台 (MMC) 中設定應用程式介面的顯示模式**

1. 在卡巴斯基安全管理中心管理主控台樹狀目錄中，選取**政策**。
2. 選擇必要的政策並點擊以開啟政策內容。
3. 在政策視窗中，選擇"**一般設定 → 介面**"。
4. 在"**使用者互動**"塊中執行以下操作之一：
   - 如果您要在用戶端電腦上顯示以下介面元素，請選擇"**顯示使用者介面**"核取方塊：
     - 包含"**開始**"功能表中的應用程式名稱的資料夾
     - Microsoft Windows 工作通知區域中的 Kaspersky Endpoint Security 圖示
     - 彈出通知

     如果選中此核取方塊，使用者可以從應用程式介面檢視應用程式設定，並可以根據可用權限變更應用程式設定。
   - 如果您希望在用戶端電腦上隱藏 Kaspersky Endpoint Security 的所有跡象，請清除"**顯示使用者介面**"核取方塊。
5. 如果您想要簡化的應用程式介面顯示在已安裝 Kaspersky Endpoint Security 的用戶端電腦上，請在"**使用者互動**"塊中選中"**顯示簡化介面**"核取方塊。

**如何在網頁主控台和雲端主控台中設定應用程式介面的顯示模式**

1. 在網頁主控台的主視窗中，選擇**資產（裝置）→ 政策和設定檔**。
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“**使用者可見性**”塊中，設定應用程式介面的顯示方式：

   - **顯示應用程式圖示**用戶端電腦在通知區域顯示應用程式圖示。在該圖示的內容功能表中，使用者可以使用 Kaspersky Endpoint Security 執行操作。Kaspersky Endpoint Security 還會在應用程式圖示上方顯示通知。

   - **不為使用者顯示應用程式介面**用戶端電腦上不會顯示 Kaspersky Endpoint Security 的主視窗，只能使用通知區域的圖示。使用者可透過圖示的右鍵選單執行 Kaspersky Endpoint Security 的部分操作。Kaspersky Endpoint Security 還會在應用程式圖示上方顯示通知。

6. 儲存變更。

# 準備應用程式以供使用

在用戶端電腦上佈署應用程式後，要從卡巴斯基安全管理中心網頁主控台使用 Kaspersky Endpoint Security，需要執行以下操作：

- 建立並配置政策。

  您可以使用政策讓同一 Kaspersky Endpoint Security 設定應用於一個管理群組的所有用戶端電腦中。卡巴斯基安全管理中心的快速啟動精靈會自動為 Kaspersky Endpoint Security 建立政策。

- 建立“*資料庫和應用程式模組更新*”和“*惡意軟體掃描*”工作。

  使電腦安全性保持最新需要“*資料庫和應用程式模組更新*”工作。執行該工作時，Kaspersky Endpoint Security 將更新病毒資料庫和應用程式模組。*資料庫和應用程式模組更新*工作由管理伺服器快速啟動精靈自動建立。要建立“*資料庫和應用程式模組更新*”工作，請在執行精靈時安裝 Kaspersky Endpoint Security for Windows 管理外掛程式。

  及時偵測威脅和其他惡意軟體需要“*惡意軟體掃描*”工作。您需要手動建立“*惡意軟體掃描*”工作。

  **如何在管理主控台 (MMC) 中建立“惡意軟體掃描”工作**

  1. 在卡巴斯基安全管理中心管理主控台樹狀目錄中，選取**工作**。

     工作清單開啟。

  2. 點擊**“新工作”**。

  啟動“工作精靈”。按照精靈的說明進行操作。

### 步驟 1. 選取工作類型

選取“**Kaspersky Endpoint Security for Windows (12.12)**”→“**惡意軟體掃描**”。

### 步驟 2. 掃描範圍

建立 Kaspersky Endpoint Security 在執行掃描工作時要掃描的物件清單。

### 步驟 3. Kaspersky Endpoint Security 操作

選擇偵測到威脅後的動作：

- **解毒；若解毒失敗則刪除**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；若解毒失敗則通知**如果選擇該選項，Kaspersky Endpoint Security 將自動對已經偵測到的所有受感染的檔案執行解毒操作。如果解毒失敗，Kaspersky Endpoint Security 會將偵測到的受感染檔案的相關資訊新增到活動威脅清單。
- **通知**如果選擇此選項，Kaspersky Endpoint Security 會在偵測到受感染檔案時將這些檔案的相關資訊新增到活動威脅清單。
- **立即執行進階解毒技術**如果選取該核取方塊，則 Kaspersky Endpoint Security 在掃描過程中將使用進階解毒技術來處理活動威脅。

  *進階解毒技術*致力於清除 RAM 中已啟動處理程序，以及封鎖 Kaspersky Endpoint Security 使用其他方式移除它們的惡意應用程式。這些威脅將從電腦中清除。執行進階解毒過程時，我們建議您不要開啟新的程式或者編輯作業系統登錄檔。進階解毒技術會佔用相當多的作業系統資源，這可能會降低其他應用程式的執行速度。完成進階解毒後，Kaspersky Endpoint Security 將重啟電腦，且不提示使用者進行確認。
- **僅在電腦空閒時執行**電腦資源繁忙時，推遲工作的啟動。如果電腦已鎖定或熒幕保護程式已開啟，Kaspersky Endpoint Security 會啟動掃描工作。如果您中斷了執行工作（例如，透過解鎖電腦），Kaspersky Endpoint Security 會自動執行工作，從被中斷的地方繼續。此排程選項可讓您在使用電腦時節省電腦資源。

### 步驟 4. 選取將要對其分配工作的裝置

選取將要執行工作的電腦。下列選項可用：

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

### 步驟 5. 選取要執行工作的帳戶

選取要執行*惡意軟體掃描*工作的帳戶。預設情況下，Kaspersky Endpoint Security 將使用本機使用者帳戶的權限啟動工作。如果掃描範圍包括網路磁碟機或存取受限的其他物件，請選擇具有足夠存取權限的使用者帳戶。

步驟 6. 設定工作啟動排程

設定工作啟動排程，例如，手動或在將防毒資料庫下載到儲存庫之後。

步驟 7. 定義工作名稱

輸入工作的名稱，例如“*每日完整掃描*”。

步驟 8. 完成工作建立

結束精靈。如有必要，選中“**精靈完成時執行工作**”核取方塊。您可以在工作內容中監控工作進度。結果，將按照指定排程在使用者電腦上執行“惡意軟體掃描”工作。

**如何在網頁主控台中建立“惡意軟體掃描”工作**

1. 在網頁主控台的主視窗中，選擇**資產（裝置）→ 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 Windows 12.12.0**”。

   b. 在“**工作類型**”下拉式清單中，選取“**惡意軟體掃描**”。

   c. 在“**工作名稱**”欄位中，輸入簡要說明，例如“*每週掃描*”。

   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。前往下一步。

5. 選取要執行工作的帳戶。預設情況下，Kaspersky Endpoint Security 將使用本機使用者帳戶的權限啟動工作。

6. 結束精靈。

   在工作清單中將顯示一個新工作。

7. 要配置工作排程，請轉到工作內容。

   建議至少一周一次排程執行工作。

8. 選中該工作旁邊的核取方塊。

9. 點擊“**開始**”。

   您可以監控工作的狀態，以及成功完成工作或完成工作時發生錯誤的裝置數量。

結果，將按照指定排程在使用者電腦上執行"惡意軟體掃描"工作。

- 最佳化 Kaspersky Endpoint Security 效能.

# 管理政策

*政策*是為管理群組定義的一系列應用程式設定。您可以為一個應用程式配置多個具有不同值的政策。對於不同的管理群組，應用程式可以在不同的設定下執行。每個管理群組都有自己的應用程式政策。

每個政策設定都有（"掛鎖"）屬性。此屬性的狀態決定了該設定是否會傳遞給管理群組中的受管理裝置：

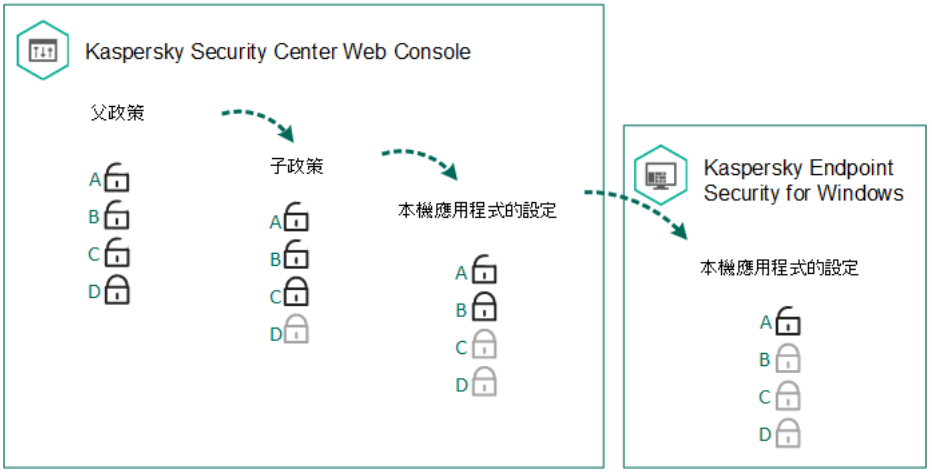
- 如果"掛鎖"是打開的（），此設定的值將不會傳遞給受管理裝置。此設定可在應用程式的本機介面中進行修改。此類設定被稱為 *已解鎖*。
- 如果"掛鎖"已關閉（），該設定的值將被傳遞並套用於受管理裝置。此類設定被稱為 *已鎖定*。被封鎖的設定無法在應用程式的本機介面中進行修改。

在*同步*期間，政策設定由網路代理傳送到用戶端電腦。預設情況下，管理伺服器在政策設定發生變化後立刻執行同步。使用用戶端電腦上的 UDP 連接埠 15000 進行同步。預設情況下，管理伺服器每 15 分鐘執行一次同步。如果在政策設定發生變化後同步失敗，將按照配置的排程執行下一次同步嘗試。

## 設定繼承

像管理群組一樣，政策按層次結構排列。*子政策*是用於嵌套階層架構等級的政策，即用於嵌套管理群組和輔助管理伺服器的政策。

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具有（關閉的"掛鎖"）屬性，則在子政策和 本機應用程式設定中，設定的值將根據父政策被覆蓋，並且該設定將被鎖定。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。




設定繼承

為每個擁有卡巴斯基安全管理中心管理伺服器存取權限的使用者指定存取政策設定的權限（讀取、寫入、執行），並為 Kaspersky Endpoint Security 的每個功能範圍單獨指定政策設定。要配置政策設定的存取權限，請轉至卡巴斯基安全管理中心管理伺服器屬性視窗的**安全性**部分（預設情況下，此部分在主控台介面中被隱藏）。

# 建立政策

建立政策時，精靈會建議與所選模式相關的設定。例如，對於 Light Agent 模式，您必須新增 Protection Server (SVM)。使用應用程式防護 SQL 伺服器時，必須新增預定義掃描排除項目，以確保伺服器的運作不會受到干擾。選擇模式後，精靈會建議相關的政策設定。然後，您可以在政策屬性中編輯這些設定。

**如何在管理主控台 (MMC) 中建立政策**

1. 開啟卡巴斯基安全管理中心管理主控台。
2. 在管理主控台樹狀目錄的**"受管理裝置"**資料夾中，選取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. 點擊**"新政策"**。
   啟動"政策精靈"。
5. 按照"政策精靈"的說明進行操作。

步驟 1. 選取要建立群組政策的應用程式

選取 **Kaspersky Endpoint Security for Windows (12.12)**應用程式。

步驟 2. 命名群組政策

輸入群組政策的名稱，例如，*辦公室政策*。

您也可以使用政策精靈基於現有政策建立新政策。為此，在指定群組政策名稱時，選擇 **使用早期版本應用程式的政策設定** 核取方塊。此精靈還允許基於不同解決方案的政策建立 Kaspersky Endpoint Security (KES) 政策，例如 Kaspersky Security for Windows Server (KSWS) 或 Kaspersky Security for Virtualization Light Agent for Windows

步驟 3. 參與卡巴斯基安全網絡

請閱讀並接受卡巴斯基安全網路 (KSN) 聲明的條款。

步驟 4.選擇電腦上的應用程式使用模式

根據使用 Kaspersky Endpoint Security 的目的，您可以以不同的模式部署 Kaspersky Endpoint Security 應用程式：

- 標準模式。

  如果選擇此模式，您可以在精靈執行時指定基本政策設定。您也可以從設定檔匯入基本政策設定。

- Endpoint Detection and Response Agent

  如果選擇此模式，則只能使用預設設定建立政策。若要配置 EDR Agent 設定，您必須在精靈完成後導覽至政策屬性。

- Light Agent 防護虛擬環境

  如果選擇此模式，則在下一步，您必須設定與 Protection Server (SVM) 的連線。應用程式需要這些設定才能在 Light Agent 模式下運作。

Kaspersky Endpoint Security 為所有應用程式模式和作業係統類型提供通用政策。這意味著該政策涵蓋整套設定。但是，應用程式可能會忽略某些政策設定，因為 Kaspersky Endpoint Security 是在某些功能不可用的模式下部署的。例如，在 Endpoint Detection and Response Agent 模式下使用應用程式時，只有與 Kaspersky Detection and Response 解決方案整合以及與 KUMA 整合相關的設定可用。

我們建議針對不同模式和作業系統類型使用不同的政策。

步驟 5. 配置受信任區域

配置受信任區域。您可以新增預定義的 掃描排除項目 和 受信任應用程式。預先定義的掃描排除項目和受信任應用程式有助於在 SQL 伺服器、Microsoft Exchange 伺服器和 System Center Configuration Manager 上快速設定 Kaspersky Endpoint Security。這意味著您無需在伺服器上為應用程式手動設定受信任區域。預定義掃描排除項目和受信任應用程式還可以幫助您在Citrix 和 Vmware虛擬環境中以虛擬環境中以 Light Agent 模式快速設定 Kaspersky Endpoint Security。

步驟 6. 選擇政策狀態

- **作用中**下次同步後，該政策將用作電腦上的活動政策。

  活動政策的設定在同步期間儲存到用戶端電腦上。您無法同時將多個政策套用到一台電腦，因此每個群組只能有一個政策處於活動狀態。

- **非作用中**備份政策。如有必要，不活動政策可切換為活動狀態。

  您可以建立無限數量的不活動政策。不活動政策不影響網路中電腦的應用程式設定。不活動政策用作緊急情況（如病毒攻擊）的後備。如果存在透過快閃記憶體磁碟機進行的攻擊，您可以啟動用於封鎖存取快閃記憶體磁碟機的政策。在這種情況下，活動政策會自動變為不活動。

- **漫遊**當電腦離開組織網路周界時，將啟動該政策。

結束精靈。

### 如何在網頁主控台和雲端主控台中建立政策

1. 在網頁主控台的主視窗中，選擇**資產（裝置）→政策和設定檔**。
2. 點擊**"新增"**。

   啟動"政策精靈"。
3. 選取 Kaspersky Endpoint Security 並點擊**"下一步"**。
4. 請閱讀並接受卡巴斯基安全網路 (KSN) 聲明的條款，然後點擊**"下一步"**。
5. 選擇應用程式的模式：

   - 防護工作站和伺服器的標準模式。
   - Endpoint Detection and Response Agent 抵禦進階威脅和針對性攻擊

     如果選擇此模式，您可以建立政策以將電腦與 Kaspersky Detection and Response 解決方案整合。精靈會提示您設定 Kaspersky Managed Detection and Response 以及 Kaspersky Anti Targeted Attack Platform (EDR) 的整合。
   - Light Agent 防護虛擬環境

     如果選擇此模式，則在下一步，您必須設定與 Protection Server (SVM) 的連線。應用程式需要這些設定才能在 Light Agent 模式下運作。

   Kaspersky Endpoint Security 為所有應用程式模式和作業系統類型提供通用政策。這意味著該政策涵蓋整套設定。但是，應用程式可能會忽略某些政策設定，因為 Kaspersky Endpoint Security 是在某些功能不可用的模式下部署的。例如，在 Endpoint Detection and Response Agent 模式下使用應用程式時，只有與 Kaspersky Detection and Response 解決方案整合以及與 KUMA 整合相關的設定可用。

   > 我們建議針對不同模式和作業系統類型使用不同的政策。
6. 配置受信任區域。您可以新增預定義的 掃描排除項目 和 受信任應用程式。預先定義的掃描排除項目和受信任應用程式有助於在 SQL 伺服器、Microsoft Exchange 伺服器和 System Center Configuration Manager 上快速設定 Kaspersky Endpoint Security。這意味著您無需在伺服器上為應用程式手動設定受信任區域。預定義掃描排除項目和受信任應用程式還可以幫助您在Citrix 和 Vmware虛擬環境中以虛擬環境中以 Light Agent 模式快速設定 Kaspersky Endpoint Security。
7. 在**"一般"**標籤上，可以執行以下操作：

   - 變更政策名稱。
   - 選取政策狀態：

     - **作用中**下次同步後，該政策將用作電腦上的活動政策。

       活動政策的設定在同步期間儲存到用戶端電腦上。您無法同時將多個政策套用到一台電腦，因此每個群組只能有一個政策處於活動狀態。
     - **非作用中**備份政策。如有必要，不活動政策可切換為活動狀態。

       您可以建立無限數量的不活動政策。不活動政策不影響網路中電腦的應用程式設定。不活動政策用作緊急情況（如病毒攻擊）的後備。如果存在透過快閃記憶體磁碟機進行的攻擊，您可以啟動用於封鎖存取快閃記憶體磁碟機的政策。在這種情況下，活動政策會自動變為不活動。
     - **漫遊**當電腦離開組織網路周界時，將啟動該政策。

- 配置設定繼承：
  - **從父政策繼承設定**如果開啟此開關，則政策設定值將從頂級政策繼承。如果為父政策設定了，則無法編輯政策設定。
  - **在子政策中強制繼承設定**如果開啟該切換按鈕，政策設定的值將傳播到子政策。在子政策的內容中，**"從父政策繼承設定"**切換按鈕將自動開啟，且無法關閉。子政策設定繼承自父政策，除了標記有 的設定外。如果為父政策設定了，則無法編輯子政策設定。

8. 在**"應用程式設定"**標籤上，可以配置 Kaspersky Endpoint Security 政策設定。

9. 結束精靈。

結果，在下次同步期間，將在用戶端電腦上配置 Kaspersky Endpoint Security 設定。透過點擊主螢幕上的按鈕，可以在 Kaspersky Endpoint Security 介面中檢視有關應用於電腦的政策資訊（例如，政策名稱）。為此，在網路代理政策的設定中，需要啟用接收延伸政策資料。有關網路代理政策的詳細資訊，請參閱卡巴斯基安全管理中心說明。

# 安全等級指示器

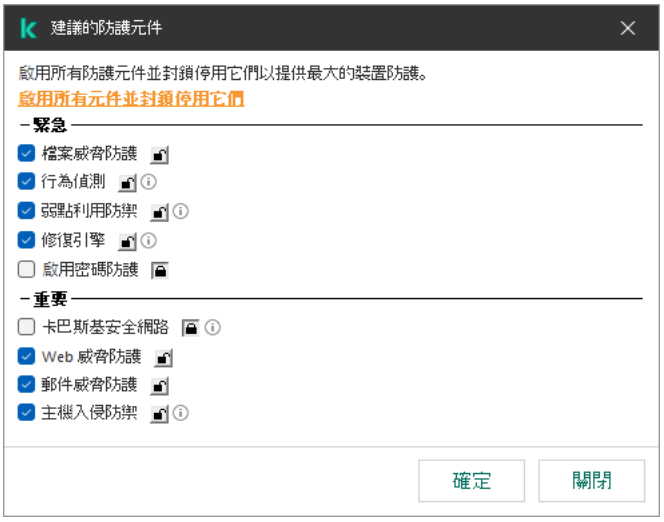
安全等級指示器顯示在政策內容視窗的上部。此指示器的值可能如下：

- **高防護等級**如果啟用以下類別的所有元件，指示器為此值並變為綠色：
  - **緊急**此類別包含以下元件：
    - 檔案威脅防護
    - 行為偵測
    - 弱點利用防禦
    - 修復引擎
    - 防護應用程式服務抵禦外部管理
  - **重要**此類別包含以下元件：
    - 卡巴斯基安全網路
    - Web 威脅防護
    - 郵件威脅防護
    - 主機入侵防禦
    - 密碼防護
- **中度防護等級**如果停用了一個重要元件，指示器為此值並變為黃色。

- **低度防護等級**在以下任意一種情況下，指示器為此值並變為紅色：
  - 一個或多個關鍵元件被停用。
  - 兩個或更多重要元件被停用。

如果指示器的值為**"中度防護等級"**或**"低度防護等級"**，則指示器的右側將顯示一個連結，點擊該連結可開啟**"建議的防護元件"**視窗。在此視窗中，可以啟用任一建議的防護元件。

升級應用程式後，保護等級指示器所顯示的等級可能會低於升級前的等級。這是因為新版本的應用程式引入了對保障電腦安全十分重要的新元件或功能。升級應用程式後，您需要管理新的設定以確保保護等級維持在較高水平。




政策的安全等級指示器

# 工作管理

您可以建立以下類型的工作來透過卡巴斯基安全管理中心管理 Kaspersky Endpoint Security。

- 為單獨的用戶端電腦設定的本機工作。
- 為一個或多個管理群組中的用戶端電腦設定的群組工作。
- 面向一組所選電腦的工作。

您可以建立任意數量的群組工作、面向一組所選電腦的工作或本機工作。有關使用管理群組和電腦選取的詳細資訊，請參閱卡巴斯基安全管理中心說明。

Kaspersky Endpoint Security 支援以下工作：

- **惡意軟體掃描**。Kaspersky Endpoint Security 將對工作設定中指定的電腦區域執行病毒掃描。Kaspersky Endpoint Security 執行需要*"惡意軟體掃描"*工作，該工作在快速啟動精靈期間建立。建議至少一周一次排程執行工作。
- **新增金鑰**。Kaspersky Endpoint Security 新增用於啟動應用程式的金鑰，包括備用金鑰。在執行該工作前，請確保將執行該工作的電腦數量不超過產品授權允許的電腦數。

- **變更應用程式元件**。Kaspersky Endpoint Security 將根據工作設定中指定元件清單在用戶端電腦上安裝和刪除元件。"檔案威脅防護"元件無法刪除。Kaspersky Endpoint Security 元件的最佳化集合有助於節省電腦資源。

- **清查**。Kaspersky Endpoint Security 將接收電腦上儲存的所有應用程式可執行檔的相關資訊。"*清查*"工作由"應用程式控制"元件執行。如果未安裝"應用程式控制"元件，該工作將以錯誤結束。

- **資料庫和應用程式模組更新**。Kaspersky Endpoint Security 更新資料庫和應用程式模組。Kaspersky Endpoint Security 執行需要"*資料庫和應用程式模組更新*"工作，該工作在快速啟動精靈期間建立。建議配置每天至少執行一次該工作的排程。

- **抹除資料**。Kaspersky Endpoint Security 立即或與卡巴斯基安全管理中心長時間沒有連線後刪除使用者電腦中的檔案和資料夾。

- **更新回溯**。Kaspersky Endpoint Security 回溯最近的資料庫和應用程式模組更新。例如，如果新資料庫包含可能導致 Kaspersky Endpoint Security 封鎖安全應用程式的錯誤資料，可能需要執行此工作。

- **應用程式完整性檢查**。Kaspersky Endpoint Security 分析應用程式檔案，檢查檔案是否損壞或被修改，並驗證應用程式檔案的數位簽章。

- **管理身分驗證代理帳戶**。Kaspersky Endpoint Security 會設定身分驗證代理帳戶設定。使用加密磁碟機需要身分驗證代理。載入作業系統之前，使用者需要使用代理完成身分驗證。

如果應用程式作為卡巴斯基的 Endpoint Detection and Response 解決方案 一部分工作，您可以執行其他工作作為偵測回應操作（responses）。例如，您可以使用"*停止處理程序*"工作遠端終止處理程序。

僅當 Kaspersky Endpoint Security 正在執行時，才會在電腦上執行工作。

## 建立工作

### 如何在管理主控台 (MMC) 中建立工作

1. 開啟卡巴斯基安全管理中心管理主控台。
2. 選取管理主控台樹狀目錄中的"**工作**"資料夾。
3. 點擊"**新工作**"。

   啟動"工作精靈"。
4. 請按照工作精靈的指示操作。

### 如何在網頁主控台和雲端主控台中建立工作

1. 在網頁主控台的主視窗中，選擇**資產（裝置）→ 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 Windows 12.12.0**”。

   b. 在“**工作類型**”下拉清單中，選取要在使用者電腦上執行的工作。

   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。前往下一步。

5. 選取要執行工作的帳戶。預設情況下，Kaspersky Endpoint Security 將使用本機使用者帳戶的權限啟動工作。

6. 結束精靈。

在工作清單中將顯示一個新工作。該工作將具有預設設定。要配置工作設定，需要轉到工作內容。要執行工作，需要選中與工作對應的核取方塊，然後點擊“**開始**”按鈕。啟動工作後，您可以暫停工作並稍後還原。

在工作清單中，您可以監視工作結果，其中包括工作狀態和電腦上的工作效能統計。您還可以建立一組用於監控工作完成的事件（“**監控和報告 → 事件分類**”）。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。工作執行結果還本機儲存在 Windows 事件記錄和 Kaspersky Endpoint Security 報告中。

## 管理工作存取權限

透過設定 Kaspersky Endpoint Security 的功能區存取權限，為每個擁有卡巴斯基安全管理中心管理伺服器存取權的使用者定義 Kaspersky Endpoint Security 工作的存取權限（讀取、寫入、執行）。若要配置存取 Kaspersky Endpoint Security 功能區的權限，請轉至卡巴斯基安全管理中心管理伺服器內容視窗“**安全性**”區域中。有關透過卡巴斯基安全管理中心進行工作管理的詳細資訊，請參閱卡巴斯基安全管理中心說明。

您可以使用政策設定使用者存取工作的權限（*工作管理模式*）。例如，您可以在 Kaspersky Endpoint Security 介面中隱藏群組工作。

**如何透過管理主控台 (MMC) 在 Kaspersky Endpoint Security 介面中設定工作管理模式**

1. 在卡巴斯基安全管理中心管理主控台樹狀目錄中，選取**政策**。

2. 選擇必要的政策並點擊以開啟政策內容。

3. 在政策視窗中，選擇“**本機工作 → 工作管理**”。

4. 設定工作管理模式（參見下表）。

5. 儲存變更。

**如何透過網頁主控台在 Kaspersky Endpoint Security 介面中設定工作管理模式**

1. 在網頁主控台的主視窗中，選擇**資產（裝置）→ 政策和設定檔**。

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**允許的操作**下方，設定工作管理模式（參見下表）。

6. 儲存變更。

工作管理設定

| 參數 | 描述 |
| --- | --- |
| **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。當沒有其他政策限制時，使用者可以配置並執行工作。不過，配置工作執行排程對於使用者仍然不可用。使用者只能手動執行工作。<br>如果此核取方塊被清空，則停止使用本機工作。在此模式中，本機工作不根據排程執行。工作無法在 Kaspersky Endpoint Security 本機介面中啟動或編輯，使用命令列工作時也無法進行。<br>使用者仍可以透過在檔案或資料夾的內容功能表中選取"**掃描病毒**"選項開始檔案或資料夾掃描。掃描工作將使用自訂掃描工作的預設設定值啟動。 |
| **查看小組任務** | 如果選擇此核取方塊，群組工作將顯示在 Kaspersky Endpoint Security 的本機介面上。使用者可以在應用程式介面中查看所有工作的清單。<br>如果清除該核取方塊，則 Kaspersky Endpoint Security 將顯示空的工作清單。 |
| **管理小組任務** | 如果選取該核取方塊，則使用者可以啟動和停止在卡巴斯基安全管理中心主控台中指定的群組工作。使用者可以在應用程式介面或簡化的應用程式介面中啟動和停止工作。<br>如果清除該核取方塊，則 Kaspersky Endpoint Security 將自動啟動排程工作，或者由管理員在卡巴斯基安全管理中心主控台中手動啟動工作。 |

# 配置本機應用程式設定

在卡巴斯基安全管理中心中，您可以配置特定電腦上的 Kaspersky Endpoint Security 設定。這些設定是*本機應用程式設定*。某些設定可能無法存取進行編輯。這些設定被政策屬性中的屬性鎖定 。

### 如何在管理主控台 (MMC) 中配置本機應用程式設定

1. 開啟卡巴斯基安全管理中心管理主控台。

2. 在管理主控台樹狀目錄的"**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"**裝置**"標籤。

4. 點擊以開啟電腦內容視窗。

5. 在電腦內容視窗中，選取"**應用程式**"區域。

6. 在電腦上安裝的 Kaspersky 應用程式清單中，選取 **Kaspersky Endpoint Security for Windows (12.12)** 並點擊以開啟應用程式內容。

7. 在"**一般設定**"區域中，配置 Kaspersky Endpoint Security 以及報告和儲存。

   應用程式屬性視窗中的其餘部分是卡巴斯基安全管理中心的標準。《卡巴斯基安全管理中心說明》提供了這些區域的說明。

   如果某個應用程式受到禁止變更特定設定的政策的限制，則在"**一般設定**"區域中配置應用程式設定時，您將無法編輯它們。

8. 儲存變更。

**如何在網頁主控台和雲端主控台中配置本機應用程式設定**

1. 在網頁主控台的主視窗中，選擇**資產（裝置）→受管理裝置**。
2. 選取要為其配置本機應用程式設定的電腦。
   這將開啟電腦內容。
3. 選擇"**應用程式**"標籤。
4. 點擊"**Kaspersky Endpoint Security for Windows**"。
   這將開啟本機應用程式設定。
5. 選擇"**應用程式設定**"標籤。
6. 配置本機應用程式設定。
7. 儲存變更。

本機應用程式設定與政策設定相同，但加密設定除外。

# 啟動和停止 Kaspersky Endpoint Security

將 Kaspersky Endpoint Security 安裝到使用者的電腦後，該應用程式會自動啟動。預設情況下，Kaspersky Endpoint Security 在作業系統啟動後啟動。在作業系統設定中無法設定應用程式的自動啟動。

在作業系統啟動後下載 Kaspersky Endpoint Security 病毒資料庫最多可能需要兩分鐘，具體取決於電腦的功能。在該期間電腦防護等級降低。在已啟動的作業系統上啟動 Kaspersky Endpoint Security 時，下載病毒資料庫不會導致電腦防護等級降低。

**如何在管理主控台 (MMC) 中設定 Kaspersky Endpoint Security 的啟動**

1. 在卡巴斯基安全管理中心管理主控台樹狀目錄中，選取**政策**。
2. 選擇必要的政策並點擊以開啟政策內容。
3. 在政策視窗中，選擇"**一般設定 → 應用程式設定**"。
4. 使用"**在電腦啟動時啟動應用程式（建議）**"核取方塊配置應用程式啟動。
5. 儲存變更。

**如何在網頁主控台中設定 Kaspersky Endpoint Security 的啟動**

1. 在網頁主控台的主視窗中，選擇**資產（裝置）→政策和設定檔**。
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. 使用“**電腦啟動時啟動 Kaspersky Endpoint Security （建議）**”核取方塊配置應用程式啟動。

6. 儲存變更。

**如何在應用程式介面中設定 Kaspersky Endpoint Security 的啟動**

1. 在“應用程式主視窗”中，點擊⚙按鈕。

2. 在應用程式設定視窗中，選取“**一般設定**”→“**應用程式設定**”。




Kaspersky Endpoint Security for Windows 設定

3. 使用“**在電腦啟動時啟動應用程式（建議）**”核取方塊配置應用程式啟動。

4. 儲存變更。

Kaspersky 專家建議您不要手動停止 Kaspersky Endpoint Security，因為這樣做會使電腦和您的個人資料曝露於威脅之中。如有必要，您可以根據需要暫停電腦防護而無需停止應用程式。

您可以使用**防護狀態**小元件來監控應用程式狀態。

**如何在管理主控台 (MMC) 中啟動或停止 Kaspersky Endpoint Security**

1. 開啟卡巴斯基安全管理中心管理主控台。

2. 在管理主控台樹狀目錄的“**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“**裝置**”標籤。

4. 點擊以開啟電腦內容視窗。

5. 在電腦內容視窗中，選取“**應用程式**”區域。

6. 在電腦上安裝的 Kaspersky 應用程式清單中，選取 **Kaspersky Endpoint Security for Windows (12.12)** 並點擊以開啟應用程式內容。

7. 請執行以下操作之一：

   - 要啟動應用程式，請點擊 Kaspersky 應用程式清單右側的 按鈕。
   - 要停止應用程式，請點擊 Kaspersky 應用程式清單右側的 按鈕。

**如何在網頁主控台中啟動或停止 Kaspersky Endpoint Security**

1. 在網頁主控台的主視窗中，選擇**資產（裝置）→受管理裝置**。

2. 點擊您要在其上啟動或停止 Kaspersky Endpoint Security 的電腦的名稱。
   電腦內容視窗將開啟。

3. 選擇“**應用程式**”標籤。

4. 選中與 **Kaspersky Endpoint Security for Windows** 對應的核取方塊。

5. 點擊“**開始**”或“**停止**”按鈕。

**如何從命令列啟動或停止 Kaspersky Endpoint Security**

1. 以管理員身分執行命令列解譯器 (cmd.exe)。

2. 轉到可執行檔 klpsm.exe 所在的資料夾。

3. 要從命令列啟動應用程式，請輸入 `klpsm.exe start_avp_service`。

4. 要從命令列停止應用程式，請輸入 `klpsm.exe stop_avp_service`。

> 要從命令列停止應用程式，必須啟用系統服務的外部管理。




透過命令列啟動和停止應用程式

# 暫停和還原電腦防護和控制

暫停電腦防護和控制表示停用 Kaspersky Endpoint Security 的所有防護和控制元件一段時間。

應用程式狀態使用工作列通知區域中應用程式圖示進行顯示。

- 圖示表示電腦防護和控制已暫停。
- 圖示表示電腦防護和控制已啟用。

暫停或還原電腦防護和控制不影響掃描工作或程式更新工作。

如果在暫停或還原電腦防護和控制時已建立任何網路連線，系統會顯示關於終止這些網路連線的通知。

*暫停電腦防護和控制：*

1. 在工作列通知區域按右鍵程式圖示，開啟內容功能表中。
2. 在內容功能表中，選取**"暫停防護"**（參見下圖）。
   如果已啟用密碼防護，則此內容功能表項可用。
3. 從以下選項中選取一個選項：
   - **暫停時間 <時間段>** – 經過下面的下拉清單中所指定的時間後將還原電腦防護和控制。
   - **暫停至應用程式重新啟動** – 重新啟動應用程式或重新啟動作業系統後還原電腦防護和控制。若要使用此選項，必須啟用應用程式的自動啟動。
   - **暫停** – 在您決定重新啟用時將還原電腦防護和控制。
4. 點擊**"暫停防護"**。

Kaspersky Endpoint Security 將暫停政策中不帶鎖標記 () 的所有防護和控制元件的執行。在執行此操作之前，建議停用卡巴斯基安全管理中心政策。




應用程式圖示的右鍵選單

*還原電腦防護和控制：*

1. 在工作列通知區域按右鍵程式圖示，開啟內容功能表中。
2. 在內容功能表中，選取**"還原防護"**。

如果您決定還原電腦防護和控制，可以隨時進行該操作，這與您之前選取的防護暫停選項無關。

# 建立和使用設定檔

帶有 Kaspersky Endpoint Security 設定的設定檔允許您完成以下工作：

- 透過命令列使用自訂的設定本機安裝 Kaspersky Endpoint Security。
- 透過卡巴斯基安全管理中心使用自訂的設定遠端安裝 Kaspersky Endpoint Security。
- 從一台電腦上將 Kaspersky Endpoint Security 設定遷移至其他電腦上（請參閱以下說明）。

## 匯出設定檔

*若要建立設定檔，請執行以下操作：*

1. 在"應用程式主視窗"中，點擊 按鈕。
2. 在應用程式設定視窗中，選取"**一般設定**"→"**變更設定**"。
3. 點擊"**匯出**"。
4. 在開啟的視窗中，指定您要儲存設定檔的路徑並輸入其名稱。

   若要使用設定檔本機或遠端安裝 Kaspersky Endpoint Security，您必須將其命名為install.cfg。

5. 如有必要，請輸入將應用程式設定匯出到檔案的密碼。

   若要儲存設定檔， 必須啟用密碼保護。。使用者必須具有"**設定匯出**"權限。

6. 儲存檔案。

結果，應用程式會建立一個設定檔。設定檔可能包含使用者帳戶詳細資訊，因此 Kaspersky Endpoint Security 會對該檔案進行加密。您無法編輯設定檔。任何修改設定檔的嘗試都會導致檔案損壞。

## 匯入設定檔

設定檔可能包含新增至應用程式中的使用者帳戶的詳細資訊。如果您在建立檔案的同一台電腦上匯入該檔案，Kaspersky Endpoint Security 會匯入使用者帳戶的密碼。如果您在另一台電腦上匯入檔案，則需要手動輸入密碼。

*若要從設定檔匯入 Kaspersky Endpoint Security 設定：*

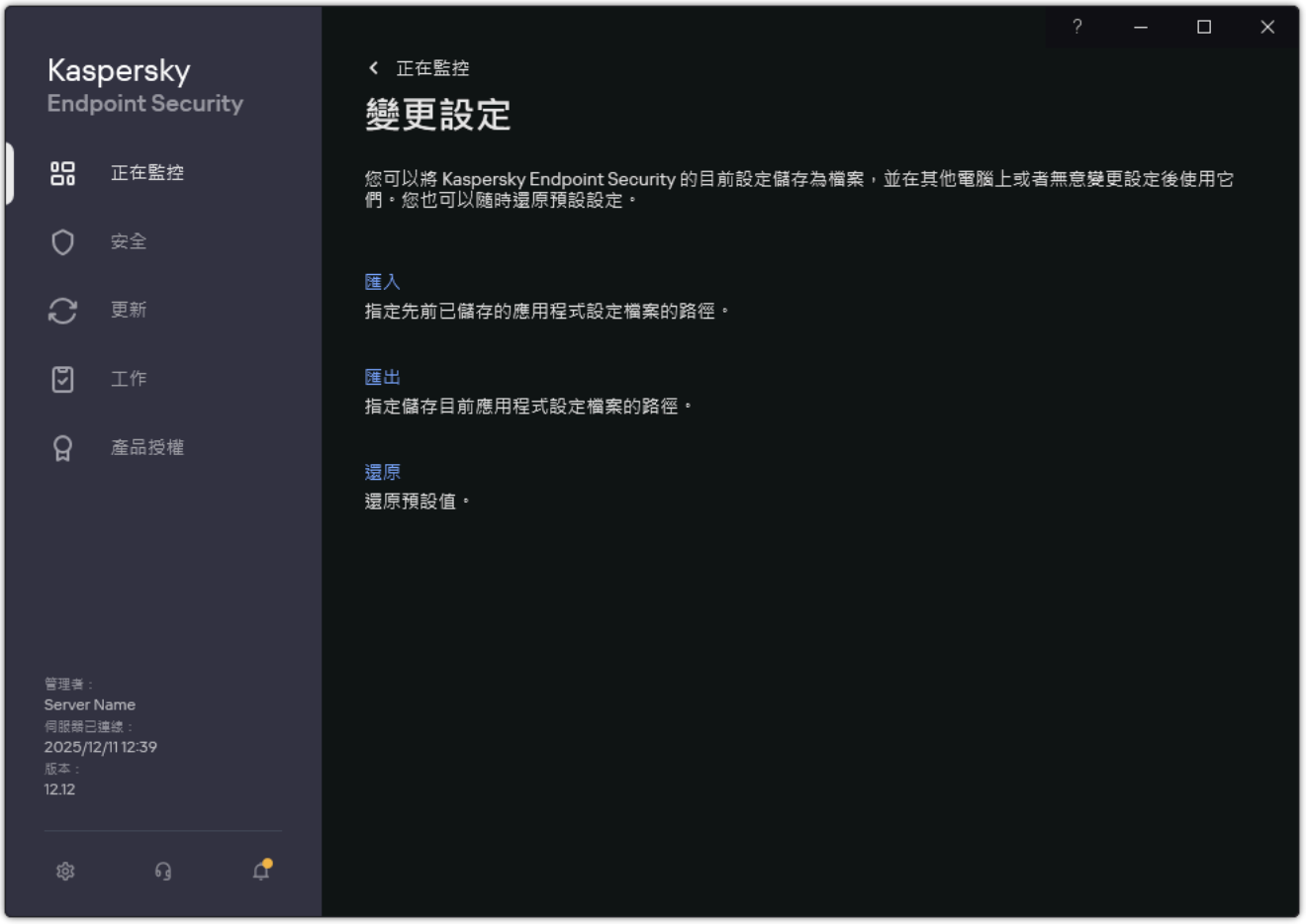
1. 在"應用程式主視窗"中，點擊 按鈕。
2. 在應用程式設定視窗中，選取"**一般設定**"→"**變更設定**"。

3. 點擊“**匯入**”。

4. 在開啟的視窗中，輸入設定檔的路徑。

5. 開啟檔案。

Kaspersky Endpoint Security 設定的所有值都將根據選定設定檔進行設定。




管理應用程式設定

# 還原應用程式預設設定

您可以隨時還原卡巴斯基建議的應用程式設定 。還原設定之後，應用程式將為所有防護元件設定“**建議**”安全等級。

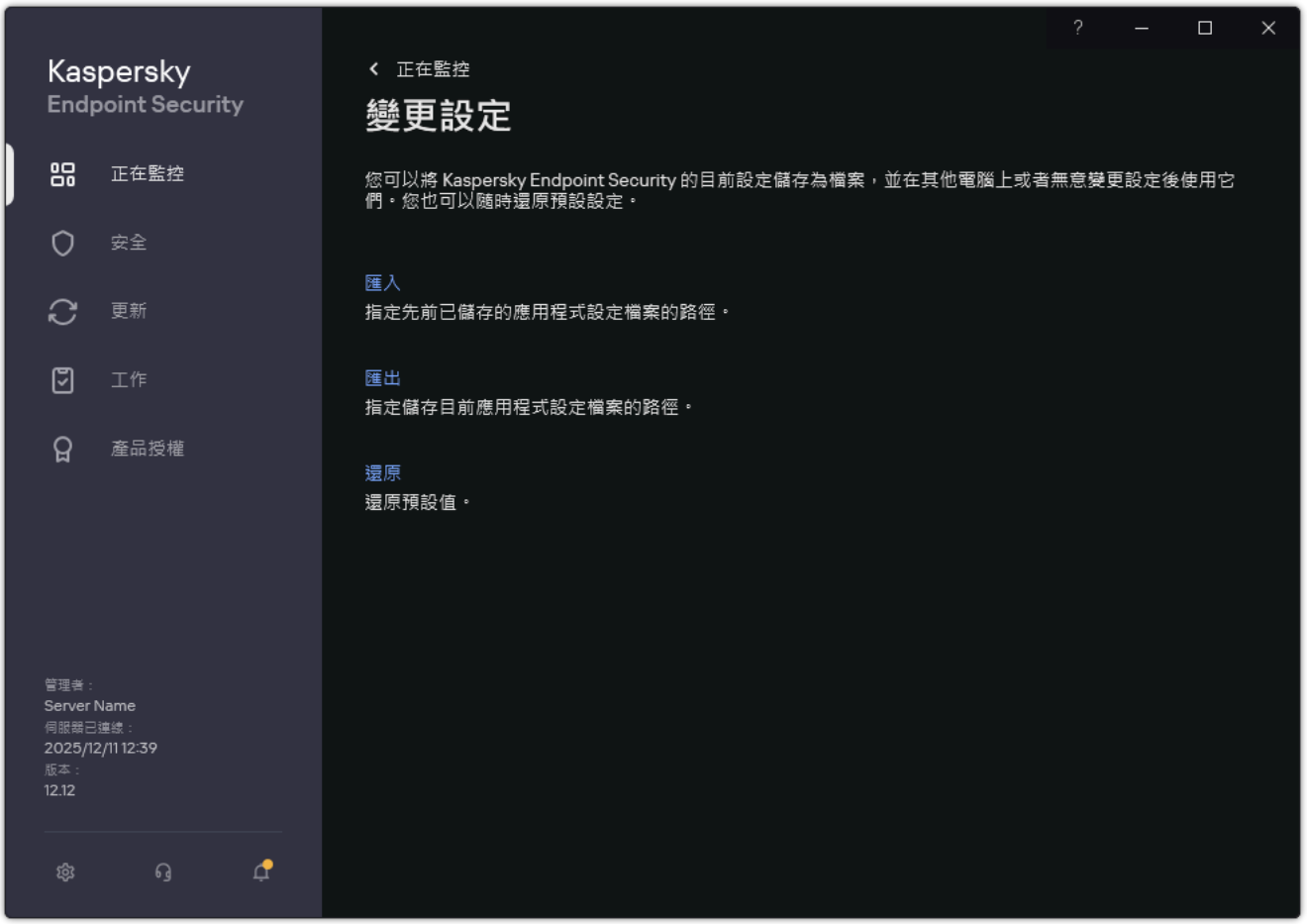
*要還原應用程式預設設定，請：*

1. 在“應用程式主視窗”中，點擊⚙ 按鈕。

2. 在應用程式設定視窗中，選取”**一般設定**“→“**變更設定**”。

3. 點擊“**還原**”。

4. 儲存變更。




管理應用程式設定

# Kaspersky Endpoint Security 的效能以及與其他應用程式的相容性

Kaspersky Endpoint Security 效能指可偵測的威脅類型、電量消耗以及電腦資源使用。

## 選擇可偵測的威脅類型

Kaspersky Endpoint Security 將讓您精調電腦防護並選取執行期間應用程式偵測的物件類型。Kaspersky Endpoint Security 將持續掃描作業系統中的病毒、蠕蟲和木馬。您不能停用對這些威脅類型的掃描。此類惡意程式可能會給電腦帶來巨大的損害。為了更好地防護您的電腦，您可以透過啟動對合法應用程式的監控來擴大可偵測的威脅類型範圍，因為入侵者可能侵入這些應用程式損害電腦或使用者資料。

## 使用省電模式

對於行動式電腦來說，應用程式的電量消耗是一個關鍵的考慮因素。Kaspersky Endpoint Security 的排程工作通常會消耗可觀的資源。當電腦使用電池執行時，您可以使用省電模式，更加節省電量。

在省電模式下，以下排程工作將自動延遲：

- 更新工作；
- 完整掃描工作；
- 關鍵區域掃描工作；
- 自訂掃描工作；
- 完整性檢查工作。

無論是否啟用省電模式，Kaspersky Endpoint Security 將在筆記型電腦切換到電池電源時暫停加密工作。及當筆記型電腦從電池電源切換到主電源還原應用程式的加密工作。

## 允許其他應用程式使用電腦資源

掃描電腦時消耗的電腦資源可能會增加 CPU 和硬碟磁碟機子系統的負載。為了解決在 CPU 和硬碟磁碟機子系統上的負載新增的條件下發生的同步執行的問題，Kaspersky Endpoint Security 可以將資源讓給其他應用程式。

## 使用進階解毒技術

如今的惡意應用程式能夠入侵作業系統的最底層，繼而無法順利清除。在作業系統中偵測到惡意活動之後，Kaspersky Endpoint Security 將使用特殊的進階解毒技術執行廣泛的清除步驟。*進階解毒技術*致力於清除 RAM 中已啟動處理程序，以及封鎖 Kaspersky Endpoint Security 使用其他方式移除它們的惡意應用程式。這些威脅將從電腦中清除。執行進階解毒過程時，我們建議您不要開啟新的程式或者編輯作業系統登錄檔。進階解毒技術會佔用相當多的作業系統資源，這可能會降低其他應用程式的執行速度。

在執行 Microsoft Windows for workstations 的電腦上執行完進階解毒過程後，Kaspersky Endpoint Security 將請求使用者授權，重新啟動電腦。系統重新啟動後 Kaspersky Endpoint Security 將刪除惡意軟體檔案並啟動“快速”電腦完整掃描。

由於 Kaspersky Endpoint Security 的特性，在執行 Microsoft Windows for servers 的電腦上將不會提示重新啟動。排程外檔案伺務器的重新啟動，可能會導致檔案伺務器未儲存的資料遺失或暫時不可使用的情況。我們建議您在電腦重新啟動後開始一次尋找病毒和其他威脅的完整掃描工作。這就是為什麼預設情況下檔案伺服器關進階解毒技術的原因。

如果偵測到檔案伺服器上有病毒感染，事件通知將傳遞到卡巴斯基安全管理中心，採取進階消毒。要清除伺服器的活動感染，請對伺服器啟用進階解毒技術，並在伺服器使用者合適的時間啟動“*惡意軟體掃描*”群組工作。

# 啟用或停用省電模式

*若要啟用或停用省電模式，請執行以下操作：*

1. 在“應用程式主視窗”中，點擊⚙按鈕。
2. 在應用程式設定視窗中，選取”**一般設定**“→“**應用程式設定**”。




Kaspersky Endpoint Security for Windows 設定

3. 在“**效能**“塊中，使用“**使用電池供電時延遲排程工作**”核取方塊來啟用或停用省電模式。
   啟用節能模式且電腦使用電池執行時，即使排程了以下工作，以下工作也不會執行：
   - *資料庫和應用程式模組更新*
   - *完整掃描*
   - *關鍵區域掃描*
   - *自訂掃描*
   - *應用程式完整性檢查*
   - *IOC 掃描*
4. 儲存變更。

# 啟用或停用允許其他應用程式使用資源

Kaspersky Endpoint Security 在掃描電腦時對電腦資源的使用，可能會增加 CPU 和硬碟子系統的負載。這可能減緩其他應用程式的速度。為了最佳化效能，Kaspersky Endpoint Security 提供了一種*將資源傳輸到其他應用程式的模式*。在此模式中，當 CPU 負載過高時，作業係統可降低 Kaspersky Endpoint Security 掃描工作執行緒的優先順序。這可允許重新分配作業係統資源到其他應用程式。因此，掃描工作將收到更少的 CPU 時間。結果，Kaspersky Endpoint Security 將花更多時間來掃描電腦。預設情況下，應用程式已設定為允許其他應用程式使用資源。

**如何在管理主控台（MMC）中啟用或停用允許其他應用程式使用資源**

1. 在卡巴斯基安全管理中心管理主控台樹狀目錄中，選取**政策**。
2. 選擇必要的政策並點擊以開啟政策內容。
3. 在政策視窗中，選擇“**一般設定 → 應用程式設定**”。
4. 在“**效能**“塊中，使用“將”**將資源讓給其他應用程式**“核取方塊來啟用或停用允許其他應用程式使用資源。
5. 儲存變更。

**如何在網頁主控台和雲端主控台中啟用或停用允許其他應用程式使用資源**

1. 在網頁主控台的主視窗中，選擇**資產（裝置）→ 政策和設定檔**。
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“**將資源讓給其他應用程式**“塊中，使用”**將資源讓給其他應用程式**“切換開關來啟用或停用允許其他應用程式使用資源。
6. 儲存變更。

**如何在應用程式介面中啟用或停用允許其他應用程式使用資源**

1. 在"應用程式主視窗"中，點擊⚙按鈕。
2. 在應用程式設定視窗中，選取"**一般設定**"→"**應用程式設定**"。




Kaspersky Endpoint Security for Windows 設定

3. 在"**效能**"塊中，使用"將"**將資源讓給其他應用程式**"核取方塊來啟用或停用允許其他應用程式使用資源。
4. 儲存變更。

# 最佳化 Kaspersky Endpoint Security 效能的最佳實踐

在部署 Kaspersky Endpoint Security for Windows 時，您可以使用以下建議來配置電腦防護和最佳化效能。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。

## 一般

根據以下建議配置應用程式的一般設定：

1. 將 Kaspersky Endpoint Security 升級到最新版本。
   較新版本的應用程式修復了錯誤，提高了穩定性並最佳化了效能。

2. 使用預設設定啟用防護元件。

   預設設定被認為最佳。此設定由 Kaspersky 專家建議。預設設定提供建議的防護等級和最佳資源使用。如有需要，您可以還原應用程式預設設定。

3. 啟用應用程式效能最佳化功能。

   應用程式具有效能最佳化功能：節能模式和將資源讓給其他應用程式。確保啟用這些選項。

## 工作站上的惡意軟體掃描

對工作站上的惡意軟體掃描建議啟用背景掃描。*背景掃描* 是 Kaspersky Endpoint Security 的一種掃描模式，不會向使用者顯示通知。背景掃描比其他類型的掃描（如完整掃描）需要更少的電腦資來源。在此模式下，Kaspersky Endpoint Security 掃描啟動物件、開啟磁區、系統記憶體和系統磁碟分割。背景掃描設定被認為最佳。此設定由 Kaspersky 專家建議。因此，要對電腦執行惡意軟體掃描，您可以僅使用背景掃描模式，而無需使用其他掃描工作。

如果背景掃描不適合您的需要，請根據以下建議配置*惡意軟體掃描*工作：

1. 設定掃描電腦時 CPU 資源消耗的限制。

   您可以限制*惡意軟體掃描* 工作時的 CPU 使用率。為此，在應用程式設定中，指定掃描電腦時可利用的所有核心的最大 CPU 負載百分比。這可能會增加掃描電腦所需的時間。

2. 配置最佳電腦掃描排程。

   您可以配置當電腦在最小負載下運行時要執行的工作。例如，您可以將工作配置為在晚上或週末執行。

   如果使用者在工作時間之外關閉電腦，您可以 啟用網路喚醒功能。“Wake-on-LAN”功能允許透過區域網路遠端傳送特殊信號來開機電腦。要使用此功能，您必須在 BIOS 設定中啟用“Wake-on-LAN”。您還可以在掃描完成後自動關閉電腦。

   如果您無法配置最佳掃描排程，請將工作設定為僅在電腦空閒時執行。如果電腦已鎖定或熒幕保護程式已開啟，Kaspersky Endpoint Security 會啟動掃描工作。如果您中斷了執行工作（例如，透過解鎖電腦），Kaspersky Endpoint Security 會自動執行工作，從被中斷的地方繼續。

3. 定義掃描範圍。

   選擇以下物件進行掃描（最小掃描範圍集）：

   - 內核記憶體
   - 正在執行的處理程序和啟動物件
   - 開機磁區
   - %systemroot%（不包括子資料夾）
   - %systemroot%\System（不包括子資料夾）
   - %systemroot%\System32（不包括子資料夾）
   - %systemroot%\System32\drivers（不包括子資料夾）
   - %systemroot%\SysWOW64（不包括子資料夾）
   - %systemroot%\SysWOW64\drivers（不包括子資料夾）

4. 開啟 iSwift 和 iChecker 技術。

   - iSwift 技術。

     該技術允許透過排除特定檔案不掃描的方式提高掃描速度。該技術將使用特殊演算法將檔案排除在掃描範圍之外，該演算法會考慮 Kaspersky Endpoint Security 資料庫的發佈日期、檔案的上次掃描日期以及對掃描設定的任何修改。iSwift 技術是對用於 NTFS 檔案系統的 iChecker 技術的增強版。

   - iChecker 技術.

     該技術允許透過排除特定檔案不掃描的方式提高掃描速度。該技術將使用特殊演算法將檔案排除在掃描範圍之外，該演算法會考慮 Kaspersky Endpoint Security 資料庫的發佈日期、檔案的上次掃描日期以及對掃描設定的任何修改。iChecker 技術受到幾個限制：它無法操作大檔案，並且僅能套用至擁有程式可辨識結構的檔案 (例如：.exe、.dll、.lnk、.ttf、.inf、.sys、.com、.chm、.zip 和 .rar)。

   您只能在管理主控台 (MMC) 和 Kaspersky Endpoint Security 介面中開啟 iSwift 和 iChecker 技術。您無法在卡巴斯基安全管理中心網頁主控台中啟用這些技術。

5. 停用掃描受密碼防護的壓縮檔案。

   如果啟用了對受密碼防護的壓縮檔案的掃描，則會在掃描壓縮檔案之前顯示密碼提示。由於工作被建議安排在非辦公時間，使用者無法輸入密碼。您可以 手動掃描受密碼防護的壓縮檔案.

6. 停用同時啟動多個掃描工作。

   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。

伺服器上的惡意軟體掃描

根據以下建議配置*惡意軟體掃描*工作：

1. 設定掃描電腦時 CPU 資源消耗的限制。

   您可以限制*惡意軟體掃描* 工作時的 CPU 使用率。為此，在應用程式設定中，指定掃描電腦時可利用的所有核心的最大 CPU 負載百分比。這可能會增加掃描電腦所需的時間。

2. 配置最佳電腦掃描排程。

   您可以配置當電腦在最小負載下運行時要執行的工作。例如，您可以將工作配置為在晚上或週末執行。

3. 開啟 iSwift 和 iChecker 技術。

   - iSwift 技術。

     該技術允許透過排除特定檔案不掃描的方式提高掃描速度。該技術將使用特殊演算法將檔案排除在掃描範圍之外，該演算法會考慮 Kaspersky Endpoint Security 資料庫的發佈日期、檔案的上次掃描日期以及對掃描設定的任何修改。iSwift 技術是對用於 NTFS 檔案系統的 iChecker 技術的增強版。

   - iChecker 技術.

     該技術允許透過排除特定檔案不掃描的方式提高掃描速度。該技術將使用特殊演算法將檔案排除在掃描範圍之外，該演算法會考慮 Kaspersky Endpoint Security 資料庫的發佈日期、檔案的上次掃描日期以及對掃描設定的任何修改。iChecker 技術受到幾個限制：它無法操作大檔案，並且僅能套用至擁有程式可辨識結構的檔案 (例如：.exe、.dll、.lnk、.ttf、.inf、.sys、.com、.chm、.zip 和 .rar)。

您只能在管理主控台 (MMC) 和 Kaspersky Endpoint Security 介面中開啟 iSwift 和 iChecker 技術。您無法在卡巴斯基安全管理中心網頁主控台中啟用這些技術。

4. 停用掃描受密碼防護的壓縮檔案。

   如果啟用了對受密碼防護的壓縮檔案的掃描，則會在掃描壓縮檔案之前顯示密碼提示。由於工作被建議安排在非辦公時間，使用者無法輸入密碼。您可以 手動掃描受密碼防護的壓縮檔案.

5. 停用同時啟動多個掃描工作。

   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。

## 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。

*卡巴斯基安全網路（KSN）*是雲端服務的基礎結構，可提供對線上卡巴斯基知識庫的存取，該知識庫包含有關檔案、網頁資源和軟體信譽的資訊。使用卡巴斯基安全網路的資料可確保 Kaspersky 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。

根據以下建議編輯卡巴斯基安全網路設定：

1. 停用延伸 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。

2. 配置卡巴斯基私有安全網路。

   *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。

3. 啟用雲端模式。

   *雲端模式* 是指 Kaspersky Endpoint Security 使用輕量級版本的病毒資料庫的應用程式執行模式。當使用輕量級病毒資料庫時，卡巴斯基安全網路支援應用程式執行。與通常的資料庫相比，輕量級版本的病毒資料庫僅需要大約一半的電腦 RAM。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。

# 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 不會掃描其內容位於 OneDrive 雲端儲存中的檔案，但會建立記錄項目來說明尚未掃描這些檔案。

## 完整掃描

徹底地掃描整個電腦。Kaspersky Endpoint Security 掃描以下物件：

- 內核記憶體
- 作業系統啟動時載入的物件
- 開機磁區
- 作業系統備份儲存區
- 所有硬碟磁碟機和卸除式磁碟機

卡巴斯基專家建議不要變更"*完整掃描*"工作的掃描範圍。

為節省電腦資源，建議使用背景掃描工作而不是完整掃描工作。這不會影響電腦的安全等級。

## 關鍵區域掃描

預設情況下，Kaspersky Endpoint Security 會掃描內核記憶體、執行處理序和磁碟的開啟磁區。

卡巴斯基專家建議不要變更"*關鍵區域掃描*"工作的掃描範圍。

### 自訂掃描

Kaspersky Endpoint Security 將掃描使用者選擇的物件。您可以掃描下表中的任意物件：

- 系統記憶體
- 作業系統啟動時載入的物件
- 作業系統備份儲存區
- 硬碟、卸除式和網路磁碟機
- 任何選取的檔案

### 背景掃描

*背景掃描* 是 Kaspersky Endpoint Security 的一種掃描模式，不會向使用者顯示通知。背景掃描比其他類型的掃描（如完整掃描）需要更少的電腦資來源。在此模式下，Kaspersky Endpoint Security 掃描啟動物件、開啟磁區、系統記憶體和系統磁碟分割。

### 應用程式完整性檢查

Kaspersky Endpoint Security 將檢查程式的模組是否損壞或者被修改，

# 掃描電腦

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。該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來提供電腦防護。

Kaspersky Endpoint Security 預定義了以下標準工作： *完整掃描*，*關鍵區域掃描*，*自訂掃描*。如果您的組織部署了卡巴斯基安全管理中心管理系統，您可以建立一個*惡意軟體掃描*工作並配置掃描。

**如何在管理主控台 (MMC) 中執行掃描工作**

1. 開啟卡巴斯基安全管理中心管理主控台。
2. 在主控台樹狀目錄中，選擇“**工作**”。
3. 選擇掃描工作並雙擊以開啟工作內容。
   需要的話建立 *惡意軟體掃描* 工作。
4. 在工作內容視窗中，選取“**設定**”區域。

5. 配置掃描工作（請參見下表）。

   如有必要，設定掃描工作排程。

6. 儲存變更。

7. 執行掃描工作。

Kaspersky Endpoint Security 將開始掃描電腦。如果使用者中斷了執行工作（例如，透過關閉電腦），Kaspersky Endpoint Security 會自動執行工作，從掃描被中斷的地方繼續。

**如何在網頁主控台和雲端主控台中執行掃描工作**

1. 在網頁主控台的主視窗中，選擇**資產（裝置）→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. 配置掃描工作（請參見下表）。

   如有必要，設定掃描工作排程。

5. 儲存變更。

6. 執行掃描工作。

Kaspersky Endpoint Security 將開始掃描電腦。如果使用者中斷了執行工作（例如，透過關閉電腦），Kaspersky Endpoint Security 會自動執行工作，從掃描被中斷的地方繼續。

**如何在應用程式介面中執行掃描工作**

1. 在應用程式主視窗中，轉至"**工作**"區域。

2. 在工作清單中，選擇掃描工作，然後點擊⚙。

3. 配置掃描工作（請參見下表）。

   如有必要，設定掃描工作排程。

4. 儲存變更。

5. 執行掃描工作。

Kaspersky Endpoint Security 將開始掃描電腦。應用程式將顯示掃描進度、已掃描檔案的數目以及剩餘的掃描時間。您可以隨時點擊"**停止**"按鈕來停止工作。如果掃描工作未顯示，則意味著管理員已在政策中禁止使用本機工作。

為了在掃描電腦時最佳化 Kaspersky Endpoint Security 效能，您可以管理 *完整掃描* 工作的進階設定並限制 CPU 資源的使用。

在卡巴斯基安全管理中心中，您也可以使用 *背景掃描* 工作而不是 *完整掃描* 工作來最佳化應用程式效能。這不會影響電腦的安全等級。背景掃描不可配置。

結果，Kaspersky Endpoint Security 將掃描電腦，如果偵測到威脅，將執行在應用程式設定中設定的動作。通常來說，應用程式會嘗試解毒受感染的檔案。結果，受感染的檔案會收到以下狀態：

- **稍後處理**感染的檔案無法被解毒。應用程式將在電腦重新啟動後刪除受感染的檔案。
- **記錄**感染的檔案無法被解毒。應用程式會將偵測到的受感染檔案的相關資訊新增到活動威脅清單。
- **不支援寫入**或者**寫入錯誤**。感染的檔案無法被解毒。應用程式沒有寫入存取權限。
- **已處理**應用程式較早偵測到一個受感染的檔案。應用程式將在電腦重新啟動後解毒或者刪除受感染的檔案。

掃描設定

| 參數 | 描述 |
| --- | --- |
| **安全等級** | Kaspersky Endpoint Security 可以使用不同的設定群組來執行掃描。這些儲存在應用程式中的設定群組稱為"*安全防護等級*"：<br>• **高**Kaspersky Endpoint Security 將掃描所有類型的檔案。掃描複合檔案時，應用程式會掃描壓縮檔案、分發套件、辦公室格式的檔案，但不會掃描受密碼防護的壓縮檔案。當設定此安全性等級時，應用程式將使用啟發式分析 **深度掃描** 詳細等級。<br>• **建議**Kaspersky Endpoint Security 將掃描所有類型的檔案。掃描複合檔案時，應用程式會掃描壓縮檔案、分發套件、辦公室格式的檔案，但不會掃描受密碼防護的壓縮檔案。當設定此安全性等級時，應用程式將使用啟發式分析 **中度掃描** 詳細等級。<br>• **低**Kaspersky Endpoint Security 僅掃描指定的檔案格式。掃描複合檔案時，應用程式會掃描壓縮檔案、分發套件、辦公室格式的檔案，但不會掃描受密碼防護的壓縮檔案。當設定此安全性等級時，應用程式將使用啟發式分析 **輕度掃描** 詳細等級。<br>您可以選擇某種預設的安全防護等級或手動配置安全性等級的設定。如果您改變了檔案安全防護等級設定，仍可隨時還原到建議的檔案安全防護等級設定。 |
| **偵測到威脅後的動作** | **解毒；若解毒失敗則刪除**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。<br>**解毒；若解毒失敗則通知**如果選擇該選項，Kaspersky Endpoint Security 將自動對已經偵測到的所有受感染的檔案執行解毒操作。如果解毒失敗，Kaspersky Endpoint Security 會將偵測到的受感染檔案的相關資訊新增到活動威脅清單。<br>**通知**如果選擇此選項，Kaspersky Endpoint Security 會在偵測到受感染檔案時將這些檔案的相關資訊新增到活動威脅清單。<br>在嘗試解毒或刪除受感染的檔案之前，應用程式會建立該檔案的備份副本，以防您需要還原該檔案或將來可以對其進行解毒。<br>在偵測到屬於 Windows Store 應用程式一部分的受感染檔案時，Kaspersky Endpoint Security 將嘗試刪除檔案。 |
| **立即執行進階解毒技術**<br>*（僅在卡巴斯基安全管理中心主控台中可用）* | 僅當在套用於電腦的政策的內容中啟用"進階解毒"功能後，才會在此電腦上執行病毒掃描工作期間執行進階解毒。<br>如果選擇該核取方塊，Kaspersky Endpoint Security 會在執行病毒掃描工作期間偵測到活躍感染後立即解毒。活躍感染被解毒後，Kaspersky Endpoint Security 會不提示使用者即重新啟動電腦。<br>如果清空該核取方塊，則 Kaspersky Endpoint Security 不會在執行病毒掃描工作期間偵測到活躍感染後立即解毒。卡巴斯基安全管理中心會在本機應用程式報告中和卡巴斯基安全管理中心端產生活躍感染事件。當開啟進階解毒功能再次執行病毒掃描工作時，活躍感染會被解毒。按此方式，系統管理員可以選擇合適的時間執行進階解毒並隨後自動重新啟動電腦。 |
| **掃描範圍** | Kaspersky Endpoint Security 在執行掃描工作時掃描的物件清單。掃描範圍內的物件可以包括內核記憶體、執行的處理程序、開機磁區、系統備份儲存、硬碟磁碟機、卸除式磁碟機或網路磁碟、資料夾或檔案。<br>在 Kaspersky Endpoint Security for Windows 12.12 中，電子郵件被排除在應用程式掃描範圍之外。傳入和傳出電子郵件的掃描由 郵件威脅防護元件執行。如果您使用的是較早版本的管理外掛程式，即使政策中包含電子郵件，該應用程式也會將電子郵件排除在掃描範圍之外。 |

| 參數 | 描述 |
| --- | --- |
| **掃描排程** | **手動**執行模式，您可以在方便時手動開始掃描。<br>**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。 |
| **應用程式啟動後延遲執行時間 N 分鐘** | 在應用程式啟動後延遲的掃描啟動。作業系統啟動時有許多處理程序在執行，因此延遲執行掃描工作而不是在 Kaspersky Endpoint Security 啟動後立刻執行更有利。 |
| **執行略過的工作** | 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。<br>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。 |
| **僅在電腦空閒時執行** | 電腦資源繁忙時，推遲工作的啟動。如果電腦已鎖定或熒幕保護程式已開啟，Kaspersky Endpoint Security 會啟動掃描工作。如果您中斷了執行工作（例如，透過解鎖電腦），Kaspersky Endpoint Security 會自動執行工作，從被中斷的地方繼續。此排程選項可讓您在使用電腦時節省電腦資源。 |
| **執行掃描為** | 預設情況下，掃描工作以您在作業系統中註冊了其權限的使用者的名稱執行。防護範圍可能包括網路磁碟或其他需要特殊存取權限的物件。您可以在應用程式設定中指定一個擁有所需權限的使用者，然後使用此使用者帳戶執行掃描工作。 |
| **檔案類型** | Kaspersky Endpoint Security 將沒有副檔名的檔案視為可執行檔。應用程式總是掃描可執行檔，而與所選的要掃描的檔案類型無關。<br>**所有檔案**如果啟用該設定，Kaspersky Endpoint Security 將毫無例外地掃描所有檔案（所有格式和副檔名）。<br>**按格式掃描檔案**如果啟用該設定，則應用程式僅掃描被感染的檔案。在掃描檔案以尋找惡意程式碼之前，系統將分析檔案的內部頭以確定檔案的格式（例如，.txt、.doc 或 .exe）。掃描還會查找具有特定副檔名的檔案。<br>**按副檔名掃描檔案**如果啟用該設定，則應用程式僅掃描被感染的檔案。此時，系統將根據檔案的副檔名確定檔案格式。<br>預設情況下，Kaspersky Endpoint Security 根據其格式掃描檔案。根據副檔名掃描檔案不太安全，因為惡意檔案可以有不在潛在感染清單上的副檔名（例如 `.123`）。 |
| **只掃描新增及修改的檔案** | 僅掃描新檔案和自上次掃描以來已被修改的檔案。這有助於縮短掃描的持續時間。此模式適用於簡單檔案和複合檔案。 |
| **略過掃描時間超過以下值的檔案 N 秒** | 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。 |
| **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。<br>不過，即使以下掃描工作之一在執行，Kaspersky Endpoint Security 也會立即啟動掃描工作：<br>• 連線時掃描卸除式磁碟機。<br>• 從內容功能表掃描。<br>• 偵測到洩露指示器 (IoC) 時啟動的關鍵區域掃描。<br>如果清除此核取方塊，Kaspersky Endpoint Security 可讓您同時執行多個掃描工作。執行多個掃描工作需要更多電腦資源。 |
| **掃描壓縮檔案** | 掃描 ZIP、GZIP、BZIP、RAR、TAR、ARJ、CAB、LHA、JAR、ICE 和其它存檔。應用程式不僅依照副檔名而且依照格式掃描存檔。當檢查封存時，應用程式會執行巡迴解壓縮。這可讓人偵測多層封存（封存內的封存）內的威脅。 |
| **掃描分發套件** | 掃描協力廠商應用程式的分發套件。 |
| **掃描 Microsoft Office 格式的檔案** | 掃描 Microsoft Office 檔案（DOC、DOCX、XLS、PPT 和其他 Microsoft 副檔名）。Office 格式檔案也包含 OLE 物件。應用程式掃描小於 1 MB 的 office 格式檔案，無論該核取方塊是否被選中。 |

| 參數 | 描述 |
| --- | --- |
| **掃描電子郵件格式檔案** | 掃描電子郵件格式檔案和電子郵件資料庫。應用程式掃描 MS Outlook 和 Windows Mail 郵件用戶端使用的 PST 和 OST 檔案以及 EML 檔案。<br>Kaspersky Endpoint Security 不支援 64 位元版本的 MS Outlook 電子郵件用戶端。這意味著如果電腦上安裝了 64 位元版本的 MS Outlook，則即使郵件包含在掃描範圍內，Kaspersky Endpoint Security 也不掃描 MS Outlook 檔案（PST 和 OST 檔案）。<br>如果選取此方塊，Kaspersky Endpoint Security 將把郵件格式檔案的各個部分分解（標題、正文、附件）後掃描威脅。<br>如果清空此方塊，Kaspersky Endpoint Security 將把郵件格式的檔案作為一個單獨的檔案掃描。<br>當在 PST 或 OST 檔案中發現惡意物件時，Kaspersky Endpoint Security 會根據所選操作（例如，對檔案進行解毒或刪除）使其無害。<br>當在其他郵件用戶端（例如 Mozilla Thunderbird）的檔案中偵測到惡意檔案時，Kaspersky Endpoint Security 只會標記受感染的郵件。您需要手動刪除帶有受感染附件的郵件。 |
| **掃描受密碼防護的壓縮檔案** | 如果選擇此方塊，應用程式將掃描密碼防護的存檔。在掃描存檔中的檔案前，系統將提示您輸入密碼。<br>如果清空此方塊，應用程式將略過掃描密碼防護的存檔。 |
| **不解壓縮大型複合檔案** | 如果選中該核取方塊，應用程式不會掃描其大小超過指定值的複合檔案。<br>如果清除該核取方塊，應用程式將掃描所有大小的複合檔案。<br>應用程式會掃描從存檔中提取的大檔案，而不管是否選中該核取方塊。 |
| **機器學習和簽章分析** | 機器學習和簽章分析使用 Kaspersky Endpoint Security 資料庫，其中包含已知威脅的敘述以及消除它們的方法。使用此方法的防護提供了可接受的最低安全等級。<br>根據 Kaspersky 專家的建議，機器學習和簽章分析始終啟用。 |
| **啟發式分析** | 開發該技術的目的是偵測使用 Kaspersky 應用程式資料庫無法偵測到的威脅。它可以偵測受未知病毒或已知病毒新變種感染的可疑檔案。<br>掃描檔案中的惡意代碼時，啟發式分析器將執行可執行檔案中的指令。啟發式分析器執行的指令數取決於為啟發式分析器指定的級別。啟發式分析等級可在全面搜尋新威脅、載入作業系統資源和啟發式分析持續時間之間進行平衡。 |
| **iSwift 技術**<br>*（僅在管理主控台（MMC）和 Kaspersky Endpoint Security 介面中可用）* | 該技術允許透過排除特定檔案不掃描的方式提高掃描速度。該技術將使用特殊演算法將檔案排除在掃描範圍之外，該演算法會考慮 Kaspersky Endpoint Security 資料庫的發佈日期、檔案的上次掃描日期以及對掃描設定的任何修改。iSwift 技術是對用於 NTFS 檔案系統的 iChecker 技術的增強版。 |
| **iChecker 技術**<br>*（僅在管理主控台（MMC）和 Kaspersky Endpoint Security 介面中可用）* | 該技術允許透過排除特定檔案不掃描的方式提高掃描速度。該技術將使用特殊演算法將檔案排除在掃描範圍之外，該演算法會考慮 Kaspersky Endpoint Security 資料庫的發佈日期、檔案的上次掃描日期以及對掃描設定的任何修改。iChecker 技術受到幾個限制：它無法操作大檔案，並且僅能套用至擁有程式可辨識結構的檔案 (例如：.exe、.dll、.lnk、.ttf、.inf、.sys、.com、.chm、.zip 和 .rar)。 |

# 掃描連線到電腦的卸除式磁碟

Kaspersky Endpoint Security 會掃描您執行或複製的所有檔案，包括位於卸除式儲存裝置的檔案（“檔案威脅防護”元件）。若要防止病毒和其它惡意軟體的傳播，您可以配置當卸除式磁碟機連線到電腦時對其自動掃描。Kaspersky Endpoint Security 將自動對已經偵測到的所有受感染的檔案執行解毒操作。如果解毒失敗，Kaspersky Endpoint Security 將刪除檔案。該元件透過執行實作機器學習、啟發式分析（高等級）和特征碼分析的掃描來保持電腦安全。Kaspersky Endpoint Security 還使用 iSwift 和 iChecker 掃描最佳化技術。這些技術總是開啟，無法停用。

### 如何在管理主控台 (MMC) 中配置執行卸除式磁碟機掃描

1. 在卡巴斯基安全管理中心管理主控台樹狀目錄中，選取**政策**。
2. 選擇必要的政策並點擊以開啟政策內容。

3. 在政策視窗中，選擇**"本機工作 → 卸除式磁碟機掃描"**。

4. 在**"連接到卸除式磁碟機的操作"**下拉式清單中，選擇**"最大防護"**或者**"建議防護"**。

5. 配置卸除式磁碟機掃描的進階選項（請參見下表）。

6. 儲存變更。

**如何在網頁主控台和雲端主控台中配置執行卸除式磁碟機掃描**

1. 在網頁主控台的主視窗中，選擇**資產（裝置）→ 政策和設定檔**。

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. 使用**"卸除式磁碟機掃描已啟用"**切換開關可啟用或停用元件。

6. 在**掃描類型**塊中，選擇**詳細掃描** or **快速掃描**。

7. 配置卸除式磁碟機掃描的進階選項（請參見下表）。

8. 儲存變更。

**如何在應用程式介面中配置執行卸除式磁碟機掃描**

1. 在應用程式主視窗中，轉至**"工作"**區域。

2. 在工作清單中，選擇掃描工作，然後點擊⚙。

3. 使用**"卸除式磁碟機掃描"**開關可以啟用或停用在連線到電腦時對卸除式磁碟機執行掃描。

4. 配置卸除式磁碟機掃描的進階選項（請參見下表）。

5. 儲存變更。

因此，Kaspersky Endpoint Security 會對不大於指定最大的大小的卸除式磁碟機執行卸除式磁碟機掃描。如果*卸除式磁碟機掃描*工作未顯示，則意味著管理員已在政策中禁止使用本機工作。

"卸除式磁碟機掃描"工作設定

| 參數 | 描述 |
| --- | --- |
| **掃描類型** | **詳細掃描**如果選擇此選項，當連接卸除式磁碟機時，Kaspersky Endpoint Security 會掃描所有檔案，包括複合物件、壓縮檔案、分發套件內的檔案，以及 Office 格式檔案。Kaspersky Endpoint Security 不掃描郵件格式的檔案或者密碼防護的壓縮檔案。<br>**快速掃描**如果選取此選項，Kaspersky Endpoint Security 將在連線卸除式磁碟機後只掃描最容易被感染的特定格式的檔案，並且不會解壓縮複合物件。 |
| **最大磁碟機容量 (MB)** | 如果選中此核取方塊，Kaspersky Endpoint Security 將對大小不超過指定最大磁碟大小的卸除式磁碟機執行選定操作。如果卸除式磁碟機的大小超出配置的值，Kaspersky Endpoint Security 將跳過掃描。<br>如果清除該核取方塊，Kaspersky Endpoint Security 將對任意大小的卸除式磁碟機執行選定的操作。 |
| **隱藏掃描進度列** | 如果選中此核取方塊，Kaspersky Endpoint Security 將在單獨的視窗和**"工作"**區域中顯示卸除式磁碟機掃描進度。<br>如果清除該核取方塊，Kaspersky Endpoint Security 將在背景啟動卸除式磁碟機掃描。 |
| **防止使用者停止掃描** | 如果選擇了該核取方塊，則對於 Kaspersky Endpoint Security 的本機介面中的卸除式磁碟機掃描工作，**"工作"**區域中的**"停止"**按鈕和卸除式磁碟機掃描視窗中的**"停止"**按鈕將不可使用。 |

# 背景掃描

*背景掃描* 是 Kaspersky Endpoint Security 的一種掃描模式，不會向使用者顯示通知。背景掃描比其他類型的掃描（如完整掃描）需要更少的電腦資來源。在此模式下，Kaspersky Endpoint Security 掃描啟動物件、開啟磁區、系統記憶體和系統磁碟分割。

為節省電腦資源，建議使用背景掃描工作而不是完整掃描工作。這不會影響電腦的安全等級。這些工作的掃描範圍一樣。為了最佳化電腦負載，應用程式不會同時執行完整掃描工作和背景掃描工作。如果您已經執行了完整掃描工作，在完整掃描工作完成後幾天 Kaspersky Endpoint Security 不會啟動背景掃描工作。

在以下情況下，啟動背景掃描：

- 病毒資料庫更新後。
- Kaspersky Endpoint Security 啟動 30 分鐘後。
- 每六個小時一次。
- 當電腦空閒五分鐘或更長時間（電腦被鎖定或熒幕保護程式開啟）時。

當滿足以下任一條件時，電腦空閒時進行的背景掃描會中斷：

- 電腦進入活動模式。

  > 如果背景掃描超過十天未執行，則掃描不會中斷。

- 電腦（筆記型電腦）轉換到電池模式。

> 執行背景掃描時，Kaspersky Endpoint Security 不掃描其內容位於 OneDrive 雲端儲存中的檔案。

**如何在管理主控台 (MMC) 中啟用背景掃描**

1. 在卡巴斯基安全管理中心管理主控台樹狀目錄中，選取**政策**。
2. 選擇必要的政策並點擊以開啟政策內容。
3. 在政策視窗中，選擇“**本機工作 → 背景掃描**”。
4. 使用“**啟用背景掃描**”核取方塊可啟用或停用背景掃描。
5. 儲存變更。

**如何在網頁主控台和雲端主控台中啟用背景掃描**

1. 在網頁主控台的主視窗中，選擇**資產（裝置）→ 政策和設定檔**。
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**背景掃描**下面，使用“**背景掃描已啟用**“切換開關啟用或停用背景掃描。

6. 儲存變更。

**如何在應用程式介面中啟用背景掃描**

1. 在應用程式主視窗中，轉至“**工作**”區域。

2. 在工作清單中，選擇掃描工作，然後點擊⚙。

3. 使用**背景掃描**開關可啟用或停用背景掃描。

4. 儲存變更。

如果“*背景掃描*”未顯示，則意味著管理員已在政策中禁止使用本機工作。

# 從內容功能表掃描

Kaspersky Endpoint Security 允許您從內容功能表執行單個檔案掃描來尋找病毒和其他惡意軟體（請參見下圖）。

從內容功能表執行掃描時，Kaspersky Endpoint Security 不掃描其內容位於 OneDrive 雲端儲存中的檔案。




從內容功能表掃描

**如何在管理主控台 (MMC) 中配置從內容功能表掃描**

1. 在卡巴斯基安全管理中心管理主控台樹狀目錄中，選取**政策**。

2. 選擇必要的政策並點擊以開啟政策內容。

3. 在政策視窗中，選擇“**本機工作 → 從內容功能表掃描**”。

4. 配置從內容功能表掃描（請參見下表）。

5. 儲存變更。

### 如何在網頁主控台和雲端主控台中配置從內容功能表掃描

1. 在網頁主控台的主視窗中，選擇**資產（裝置）→政策和設定檔**。
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**從內容功能表掃描**下，配置從內容功能表掃描（請參見下表）。
6. 儲存變更。

### 如何在應用程式介面中配置從內容功能表掃描

1. 在應用程式主視窗中，轉至"**工作**"區域。
2. 在工作清單中，選擇掃描工作，然後點擊⚙。
3. 配置從內容功能表掃描（請參見下表）。
4. 儲存變更。

如果*從內容功能表掃描*工作未顯示，則意味著管理員已在政策中禁止使用本機工作。

"從內容功能表掃描"工作設定

| 參數 | 描述 |
| --- | --- |
| **安全等級** | Kaspersky Endpoint Security 可以使用不同的設定群組來執行掃描。這些儲存在應用程式中的設定群組稱為"*安全防護等級*"：<br>• **高**Kaspersky Endpoint Security 將掃描所有類型的檔案。掃描複合檔案時，應用程式會掃描壓縮檔案、分發套件、辦公室格式的檔案，但不會掃描受密碼防護的壓縮檔案。當設定此安全性等級時，應用程式將使用啟發式分析 **深度掃描** 詳細等級。<br>• **建議**Kaspersky Endpoint Security 將掃描所有類型的檔案。掃描複合檔案時，應用程式會掃描壓縮檔案、分發套件、辦公室格式的檔案，但不會掃描受密碼防護的壓縮檔案。當設定此安全性等級時，應用程式將使用啟發式分析 **中度掃描** 詳細等級。<br>• **低**Kaspersky Endpoint Security 僅掃描指定的檔案格式。掃描複合檔案時，應用程式會掃描壓縮檔案、分發套件、辦公室格式的檔案，但不會掃描受密碼防護的壓縮檔案。當設定此安全性等級時，應用程式將使用啟發式分析 **輕度掃描** 詳細等級。 |
| **偵測到威脅後的動作** | **解毒；若解毒失敗則刪除**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。<br>**解毒；若解毒失敗則通知**如果選擇該選項，Kaspersky Endpoint Security 將自動對已經偵測到的所有受感染的檔案執行解毒操作。如果解毒失敗，Kaspersky Endpoint Security 會將偵測到的受感染檔案的相關資訊新增到活動威脅清單。<br>**通知**如果選擇此選項，Kaspersky Endpoint Security 會在偵測到受感染檔案時將這些檔案的相關資訊新增到活動威脅清單。 |
| **檔案類型** | Kaspersky Endpoint Security 將沒有副檔名的檔案視為可執行檔。應用程式總是掃描可執行檔，而與所選的要掃描的檔案類型無關。<br>**所有檔案**如果啟用該設定，Kaspersky Endpoint Security 將毫無例外地掃描所有檔案（所有格式和副檔名）。<br>**按格式掃描檔案**如果啟用該設定，則應用程式僅掃描被感染的檔案。在掃描檔案以尋找惡意程式碼之前，系統將分析檔案的內部頭以確定檔案的格式（例如，.txt、.doc 或 .exe）。掃描還會查找具有特定副檔名的檔案。<br>**按副檔名掃描檔案**如果啟用該設定，則應用程式僅掃描被感染的檔案。此時，系統將根據檔案的副檔名確定檔案格式。<br>預設情況下，Kaspersky Endpoint Security 根據其格式掃描檔案。根據副檔名掃描檔案不太安全，因為惡意檔案可以有不在潛在感染清單上的副檔名（例如 `.123`）。 |
| **只掃描新增及修改的檔案** | 僅掃描新檔案和自上次掃描以來已被修改的檔案。這有助於縮短掃描的持續時間。此模式適用於簡單檔案和複合檔案。 |

| 參數 | 描述 |
| --- | --- |
| **略過掃描時間超過以下值的檔案 N 秒** | 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。 |
| **掃描壓縮檔案** | 掃描 ZIP、GZIP、BZIP、RAR、TAR、ARJ、CAB、LHA、JAR、ICE 和其它存檔。應用程式不僅依照副檔名而且依照格式掃描存檔。當檢查封存時，應用程式會執行巡迴解壓縮。這可讓人偵測多層封存（封存內的封存）內的威脅。 |
| **掃描分發套件** | 此方塊將啟用或停用對分發套件的掃描。 |
| **掃描 Microsoft Office 格式的檔案** | 掃描 Microsoft Office 檔案（DOC，DOCX，XLS，PPT 和其他 Microsoft 副檔名）。Office 格式檔案也包含 OLE 物件。應用程式掃描小於 1 MB 的 office 格式檔案，無論該核取方塊是否被選中。 |
| **掃描電子郵件格式檔案** | 掃描電子郵件格式檔案和電子郵件資料庫。應用程式掃描 MS Outlook 和 Windows Mail 郵件用戶端使用的 PST 和 OST 檔案以及 EML 檔案。<br><br>Kaspersky Endpoint Security 不支援 64 位元版本的 MS Outlook 電子郵件用戶端。這意味著如果電腦上安裝了 64 位元版本的 MS Outlook，則即使郵件包含在掃描範圍內，Kaspersky Endpoint Security 也不掃描 MS Outlook 檔案（PST 和 OST 檔案）。<br><br>如果選取此方塊，Kaspersky Endpoint Security 將把郵件格式檔案的各個部分分解（標題、正文、附件）後掃描威脅。<br>如果清空此方塊，Kaspersky Endpoint Security 將把郵件格式的檔案作為一個單獨的檔案掃描。<br>當在 PST 或 OST 檔案中發現惡意物件時，Kaspersky Endpoint Security 會根據所選操作（例如，對檔案進行解毒或刪除）使其無害。<br>當在其他郵件用戶端（例如 Mozilla Thunderbird）的檔案中偵測到惡意檔案時，Kaspersky Endpoint Security 只會標記受感染的郵件。您需要手動刪除帶有受感染附件的郵件。 |
| **掃描受密碼防護的壓縮檔案** | 如果選擇此方塊，應用程式將掃描密碼防護的存檔。在掃描存檔中的檔案前，系統將提示您輸入密碼。<br>如果清空此方塊，應用程式將略過掃描密碼防護的存檔。 |
| **不解壓縮大型複合檔案** | 如果選中該核取方塊，應用程式不會掃描其大小超過指定值的複合檔案。<br>如果清除該核取方塊，應用程式將掃描所有大小的複合檔案。<br>應用程式會掃描從存檔中提取的大檔案，而不管是否選中該核取方塊。 |
| **機器學習和簽章分析** | 機器學習和簽章分析使用 Kaspersky Endpoint Security 資料庫，其中包含已知威脅的敘述以及消除它們的方法。使用此方法的防護提供了可接受的最低安全等級。<br>根據 Kaspersky 專家的建議，機器學習和簽章分析始終啟用。 |
| **啟發式分析** | 開發該技術的目的是偵測使用 Kaspersky 應用程式資料庫無法偵測到的威脅。它可以偵測受未知病毒或已知病毒新變種感染的可疑檔案。<br><br>掃描檔案中的惡意代碼時，啟發式分析器將執行可執行檔案中的指令。啟發式分析器執行的指令數取決於為啟發式分析器指定的級別。啟發式分析等級可在全面搜尋新威脅、載入作業系統資源和啟發式分析持續時間之間進行平衡。 |
| **iSwift 技術** | 該技術允許透過排除特定檔案不掃描的方式提高掃描速度。該技術將使用特殊演算法將檔案排除在掃描範圍之外，該演算法會考慮 Kaspersky Endpoint Security 資料庫的發佈日期、檔案的上次掃描日期以及對掃描設定的任何修改。iSwift 技術是對用於 NTFS 檔案系統的 iChecker 技術的增強版。 |
| **iChecker 技術** | 該技術允許透過排除特定檔案不掃描的方式提高掃描速度。該技術將使用特殊演算法將檔案排除在掃描範圍之外，該演算法會考慮 Kaspersky Endpoint Security 資料庫的發佈日期、檔案的上次掃描日期以及對掃描設定的任何修改。iChecker 技術受到幾個限制：它無法操作大檔案，並且僅能套用至擁有程式可辨識結構的檔案 (例如：.exe、.dll、.lnk、.ttf、.inf、.sys、.com、.chm、.zip 和 .rar)。 |

# 應用程式完整性檢查

Kaspersky Endpoint Security 將檢查程式的模組是否損壞或者被修改，例如，如果套用庫的數位簽章錯誤，則該庫被視為損壞。“*應用程式完整性檢查*”工作用於檢查應用程式檔案。如果 Kaspersky Endpoint Security 偵測到惡意物件但未清除它，請執行“*應用程式完整性檢查*工作。

您可以在卡巴斯基安全管理中心網頁主控台和管理主控台中建立“*應用程式完整性檢查*”工作。無法在卡巴斯基安全管理中心雲端主控台中建立工作。

在以下情況下，應用程式完整性可能會被破壞：

- 惡意物件修改了 Kaspersky Endpoint Security 的檔案。在這種情況下，使用作業系統的工具執行還原 Kaspersky Endpoint Security 的步驟。還原後，執行電腦完整掃描並重複完整性檢查。
- 數位簽章已過期。在這種情況下，請更新 Kaspersky Endpoint Security。

**如何透過管理主控台 (MMC) 執行應用程式完整性檢查**

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

啟動"工作精靈"。按照精靈的說明進行操作。

步驟 1. 選取工作類型

選取**"Kaspersky Endpoint Security for Windows (12.12)"→"應用程式完整性檢查"**。

步驟 2. 選取將要對其分配工作的裝置

選取將要執行工作的電腦。下列選項可用：

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

步驟 3. 設定工作啟動排程

設定工作啟動排程，例如，手動或當偵測到病毒爆發時。

步驟 4. 定義工作名稱

輸入工作的名稱，例如*"在電腦感染後執行完整性檢查"*。

步驟 5. 完成工作建立

結束精靈。如有必要，選中**"精靈完成時執行工作"**核取方塊。您可以在工作內容中監控工作進度。結果，Kaspersky Endpoint Security 將檢查應用程式的完整性。您還可以在工作內容中配置應用程式完整性檢查排程（請參見下表）。

**如何透過網頁主控台執行應用程式完整性檢查**

1. 在網頁主控台的主視窗中，選擇**資產（裝置）→ 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 Windows 12.12.0"**。

   b. 在**"工作類型"**下拉式清單中，選取**"應用程式完整性檢查"**。

   c. 在**"工作名稱"**欄位中，輸入簡要說明，例如，"*在電腦感染後檢查應用程式的完整性*"。

   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。前往下一步。

5. 選取要執行工作的帳戶。預設情況下，Kaspersky Endpoint Security 將使用本機使用者帳戶的權限啟動工作。

6. 結束精靈。

   在工作清單中將顯示一個新工作。

7. 選中該工作旁邊的核取方塊。

結果，Kaspersky Endpoint Security 將檢查應用程式的完整性。您還可以在工作內容中配置應用程式完整性檢查排程（請參見下表）。

**如何在應用程式介面中執行完整性檢查**

1. 在應用程式主視窗中，轉至**"工作"**區域。

2. 這將開啟工作清單；選擇*應用程式完整性檢查*工作，然後點擊**執行**。

結果，Kaspersky Endpoint Security 將檢查應用程式的完整性。您還可以在工作內容中配置應用程式完整性檢查排程（請參見下表）。如果*應用程式完整性檢查*工作未顯示，則意味著管理員已在政策中禁止使用本機工作。

| 參數 | 描述 |
| --- | --- |
| **掃描排程** | **手動**執行模式，您可以在方便時手動開始掃描。<br>**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。 |
| **執行略過的工作** | 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。<br>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。 |
| **僅在電腦空閒時執行** | 電腦資源繁忙時，推遲工作的啟動。如果電腦已鎖定或熒幕保護程式已開啟，Kaspersky Endpoint Security 會啟動掃描工作。如果您中斷了執行工作（例如，透過解鎖電腦），Kaspersky Endpoint Security 會自動執行工作，從被中斷的地方繼續。此排程選項可讓您在使用電腦時節省電腦資源。 |

# 編輯掃描範圍

"*掃描範圍*"是一個 Kaspersky Endpoint Security 執行工作時掃描的資料夾和路徑的路徑清單。Kaspersky Endpoint Security 輸入遮罩時支援環境變量以及`*`和`?`字元。

若要編輯掃描範圍，我們建議使用"*自訂掃描*"工作。卡巴斯基專家建議不要變更"*完整掃描*"和"*關鍵區域掃描*"工作的掃描範圍。

Kaspersky Endpoint Security 有以下預定義物件屬於掃描範圍：

- **系統記憶體**
- **啟動物件**

  處理程序和系統啟動時執行的應用程式可執行檔所佔用的記憶體。
- **磁碟開機磁區**

  硬碟和卸除式磁碟開機磁區。
- **系統備份**

  "系統磁碟區內容資訊"資料夾。
- **所有外部裝置**
- **所有硬碟磁碟機**
- **所有網路磁碟機**

在 Kaspersky Endpoint Security for Windows 12.12 中，電子郵件被排除在應用程式掃描範圍之外。傳入和傳出電子郵件的掃描由 郵件威脅防護元件執行。如果您使用的是較早版本的管理外掛程式，即使政策中包含電子郵件，該應用程式也會將電子郵件排除在掃描範圍之外。

我們建議建立單獨的掃描工作來掃描網路磁碟機或共用資料夾。在*惡意軟體掃描*工作的設定中，指定對此磁碟機具有寫入權限的使用者；這對於減輕偵測到的威脅很有必要。如果網路磁碟機所在的伺服器有自己的安全工具，請不要對該磁碟機執行掃描工作。這樣就可以避免兩次檢查物件，提高伺服器的效能。

要從掃描範圍中排除資料夾或檔案，請將資料夾或者檔案新增至受信任區域。

**如何在管理主控台 (MMC) 中編輯掃描排除項目**

1. 開啟卡巴斯基安全管理中心管理主控台。
2. 在主控台樹狀目錄中，選擇**"工作"**。
3. 選擇掃描工作並雙擊以開啟工作內容。
   需要的話建立 *惡意軟體掃描* 工作。
4. 在工作內容視窗中，選取**"設定"**區域。
5. 在**"掃描範圍"**區域中點擊**"設定"**。
6. 在開啟的視窗中，選擇要新增到掃描範圍或從中排除的物件。
7. 如果您希望將新物件新增至掃描範圍：
   a. 點擊**"新增"**。
   b. 在**"物件"**欄位中，輸入資料夾或者檔案路徑。
      使用遮罩：
      - `*`（星號）字元代表任意一組字元，但 `\` 和 `/` 字元除外（這兩個字元是檔案和資料夾路徑中的檔案和資料夾名稱的分隔符號）。例如，遮罩"`C:\*\*.txt`"將包括位於 C: 磁碟機但是不在子資料夾中所有帶 TXT 副檔名的檔案的路徑。
      - 兩個連續 `*` 字元在檔案或資料夾名稱中代表任意一組字元（包括空集），包括 `\` 和 `/` 字元（這兩個字元是檔案和資料夾路徑中的檔案和資料夾名稱的分隔符號）。例如，遮罩 `C:\Folder\**\*.txt` 將包括位於巢嵌在 `Folder` 內的資料夾（`Folder`自身除外）中所有帶 TXT 副檔名的檔案的路徑。遮罩必須包含至少一個嵌套等級。遮罩 `C:\**\*.txt` 不是有效遮罩。
      - `?`（問號）字元代表任意單個字元，但 `\` 和 `/` 字元除外（這兩個字元是檔案和資料夾路徑中的檔案和資料夾名稱的分隔符號）。例如，遮罩 `C:\Folder\???.txt` 將包括位於 `Folder` 資料夾中所有帶 TXT 副檔名且名稱由三個字元構成的檔案的路徑。

      您可以在檔案或者資料夾路徑的任何地方使用遮罩。例如，如果您想要掃描範圍包括電腦上的所有使用者帳戶的"下載"資料夾，請輸入 `C:\Users\*\Downloads\` 遮罩。
      電腦檔案資源清單中的**此 PC**物件包含以下物件：**所有硬碟磁碟機**、**所有網路磁碟機**及**所有卸除式磁碟機**。

   您可以從掃描中排除物件，而無需將其從掃描範圍內的物件清單中刪除。為此，請清除物件旁邊的核取方塊。
8. 儲存變更。若要在電腦上套用該政策，請關閉掛鎖。

**如何在網頁主控台和雲端主控台中編輯掃描範圍**

1. 在網頁主控台的主視窗中，選擇**資產（裝置）→ 工作**。
   工作清單開啟。
2. 點擊掃描工作。
   工作內容視窗將開啟。需要的話建立 *惡意軟體掃描* 工作。

3. 選擇“**應用程式設定**”標籤。

4. 在“**掃描範圍**”中，選擇要新增到掃描範圍或從中排除的物件。

5. 如果您希望將新物件新增至掃描範圍：

   a. 點擊“**新增**”。

   b. 輸入資料夾或者檔案路徑。

   使用遮罩：

   - `*`（星號）字元代表任意一組字元，但 `\` 和 `/` 字元除外（這兩個字元是檔案和資料夾路徑中的檔案和資料夾名稱的分隔符號）。例如，遮罩“`C:\*\*.txt`”將包括位於 C: 磁碟機但是不在子資料夾中所有帶 TXT 副檔名的檔案的路徑。

   - 兩個連續 `*` 字元在檔案或資料夾名稱中代表任意一組字元（包括空集），包括 `\` 和 `/` 字元（這兩個字元是檔案和資料夾路徑中的檔案和資料夾名稱的分隔符號）。例如，遮罩 `C:\Folder\**\*.txt` 將包括位於巢嵌在 `Folder` 內的資料夾（`Folder`自身除外）中所有帶 TXT 副檔名的檔案的路徑。遮罩必須包含至少一個嵌套等級。遮罩 `C:\**\*.txt` 不是有效遮罩。

   - `?`（問號）字元代表任意單個字元，但 `\` 和 `/` 字元除外（這兩個字元是檔案和資料夾路徑中的檔案和資料夾名稱的分隔符號）。例如，遮罩 `C:\Folder\???.txt` 將包括位於 `Folder` 資料夾中所有帶 TXT 副檔名且名稱由三個字元構成的檔案的路徑。

   您可以在檔案或者資料夾路徑的任何地方使用遮罩。例如，如果您想要掃描範圍包括電腦上的所有使用者帳戶的“下載”資料夾，請輸入 `C:\Users\*\Downloads\` 遮罩。

   您可以從掃描中排除物件，而無需將其從掃描範圍內的物件清單中刪除。為此，將它旁邊的切換開關設為關閉位置。

6. 儲存變更。

**如何在應用程式介面中編輯掃描範圍**

1. 在應用程式主視窗中，轉至“**工作**”區域。

2. 這將開啟工作清單；選擇*自訂掃描*工作，然後點擊**選擇**。

   您也可以編輯其它工作的掃描範圍。卡巴斯基專家建議不要變更“*完整掃描*”和“*關鍵區域掃描*”工作的掃描範圍。

3. 在開啟的視窗中，選擇要新增到掃描範圍的物件。

4. 儲存變更。

如果掃描工作未顯示，則意味著管理員已在政策中禁止使用本機工作。

# 執行排程的掃描

完整掃描電腦會花費一些時間和電腦的資源。您應該選擇最佳時間來執行電腦掃描，以避免負面影響其它軟體的效能。Kaspersky Endpoint Security 可讓您設定正常的電腦掃描排程。如果您所在的組織有工作排程的話，這會很方便。您可以設定在晚上或者週末執行電腦掃描。如果由於任何原因無法執行掃描工作（例如，當時電腦處於關機狀態），則可以設定錯過的工作，使其在電腦可用時儘快自動執行。

如果不可能設定最佳掃描排程，Kaspersky Endpoint Security 可讓您在滿足以下特殊情況時執行電腦掃描：

- 在資料庫更新後。

  Kaspersky Endpoint Security 可用更新的簽章資料庫執行電腦掃描。

- 在應用程式啟動後。

  Kaspersky Endpoint Security 可在應用程式啟動經過指定時間時執行電腦掃描。作業系統啟動時有許多處理程序在執行，因此延遲執行掃描工作而不是在 Kaspersky Endpoint Security 啟動後立刻執行更有利。

- Wake-on-LAN 功能。

  即使電腦關閉，Kaspersky Endpoint Security 也可以根據排程執行電腦掃描。為此，應用程式會使用作業系統的"Wake-on-LAN"功能。"Wake-on-LAN"功能允許透過區域網路遠端傳送特殊信號來開機電腦。要使用此功能，您必須在 BIOS 設定中啟用"Wake-on-LAN"。

  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。

- 在電腦空閒時

  當熒幕保護程式處於活躍狀態或者熒幕被鎖定時，Kaspersky Endpoint Security 會根據排程執行電腦掃描。如果使用者解鎖了電腦，Kaspersky Endpoint Security 會暫停掃描。這意味著應用程式可能需要花好幾天來完成一次完整的電腦掃描。

**如何在管理主控台 (MMC) 中設定掃描排程**

1. 開啟卡巴斯基安全管理中心管理主控台。
2. 在主控台樹狀目錄中，選擇"**工作**"。
3. 選擇掃描工作並雙擊以開啟工作內容。

   需要的話建立 *惡意軟體掃描* 工作。
4. 在工作內容視窗中，選取"**排程**"區域。
5. 設定掃描工作排程。
6. 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）。
7. 儲存變更。

**如何在網頁主控台和雲端主控台中配置掃描排程**

1. 在網頁主控台的主視窗中，選擇**資產（裝置）→ 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。

## 如何在應用程式介面中設定掃描排程

僅當政策沒有套用到電腦時，您才可以設定掃描排程。對於政策下的電腦，您可以在卡巴斯基安全管理中心中設定“*惡意軟體掃描*”工作。

1. 在應用程式主視窗中，轉至“**工作**”區域。
2. 在工作清單中，選擇掃描工作，然後點擊⚙。

   您可以設定執行完整掃描、關鍵區域掃描、或者完整性檢查的排程。您只能手動執行“自訂掃描”。
3. 點擊“**掃描排程**”。
4. 在開啟的視窗中，設定掃描工作執行排程。
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

| 參數 | 描述 |
| --- | --- |
| **掃描排程** | **手動**執行模式，您可以在方便時手動開始掃描。<br>**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。 |
| **應用程式啟動後延遲執行時間 N 分鐘** | 在應用程式啟動後延遲的掃描啟動。作業系統啟動時有許多處理程序在執行，因此延遲執行掃描工作而不是在 Kaspersky Endpoint Security 啟動後立刻執行更有利。 |
| **執行略過的工作** | 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。<br>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。 |
| **僅在電腦空閒時執行** | 電腦資源繁忙時，推遲工作的啟動。如果電腦已鎖定或熒幕保護程式已開啟，Kaspersky Endpoint Security 會啟動掃描工作。如果您中斷了執行工作（例如，透過解鎖電腦），Kaspersky Endpoint Security 會自動執行工作，從被中斷的地方繼續。此排程選項可讓您在使用電腦時節省電腦資源。 |
| **使用工作啟動自動隨機化延遲**<br>*（僅在卡巴斯基安全管理中心主控台中可用）* | 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。<br>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。<br>如果清除該核取方塊，則工作會準確在排程的時間執行。 |
| **使用工作啟動隨機延遲間隔（分鐘）** | 如果選取此核取方塊，則該工作將在特定時間範圍內的隨機時間在電腦上執行。隨機開始時間有助於避免當工作按照排程執行時，大量電腦同時存取管理伺服器。<br>如果清除該核取方塊，則工作會準確在排程的時間執行。 |
| **停止工作，若執行時間超過（分鐘）**<br>*（僅在卡巴斯基安全管理中心主控台中可用）* | 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。<br>例如，為了減少工作執行時間，您可以配置掃描範圍或者最佳化掃描。 |
| **透過使用 Wake-On-LAN 功能在啟動工作之前開啟裝置（分鐘）**<br>*（僅在卡巴斯基安全管理中心主控台中可用）* | 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。<br>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**<br>*（僅在卡巴斯基安全管理中心主控台中可用）* | 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。 |

# 作為不同使用者執行掃描

預設情況下，掃描工作以您在作業系統中註冊了其權限的使用者的名稱執行。防護範圍可能包括網路磁碟或其他需要特殊存取權限的物件。您可以在應用程式設定中指定一個擁有所需權限的使用者，然後使用此使用者帳戶執行掃描工作。

您可以作為不同使用者執行以下掃描：

- 關鍵區域掃描。
- 完整掃描。
- 自訂掃描。
- 從內容功能表掃描。

您無法設定執行"卸除式磁碟機掃描"、"背景掃描"、或者"完整性檢查"的使用者權限。

**如何在管理主控台 (MMC) 中作為不同使用者執行掃描**

1. 開啟卡巴斯基安全管理中心管理主控台。
2. 在管理主控台樹狀目錄的"**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"**工作**"標籤。
4. 選擇掃描工作並雙擊以開啟工作內容。
5. 在工作內容視窗中，選取"**帳戶**"區域。
6. 輸入您希望用其權限執行掃描工作的使用者的帳戶認證。
7. 儲存變更。

**如何在網頁主控台或雲端主控台中作為不同使用者執行掃描**

1. 在網頁主控台的主視窗中，選擇**資產（裝置）→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"**設定**"標籤。
4. 在"**帳戶**"塊中，點擊"**設定**"按鈕。
5. 輸入您希望用其權限執行掃描工作的使用者的帳戶認證。
6. 儲存變更。

**如何在應用程式介面中作為不同使用者執行掃描**

1. 在應用程式主視窗中，轉至**"工作"**區域。
2. 在工作清單中，選擇掃描工作，然後點擊⚙。
3. 在工作內容中，選擇**"進階設定" → "執行掃描為"**。
4. 在開啟的視窗中，輸入您希望用其權限執行掃描工作的使用者的帳戶認證。
5. 儲存變更。

如果掃描工作未顯示，則意味著管理員已在政策中禁止使用本機工作。

# 掃描最佳化

## 掃描電腦時限制 CPU 使用率

您可以限制*惡意軟體掃描*工作時的 CPU 使用率。這可能會增加掃描電腦所需的時間。

**如何在管理主控台 (MMC) 中掃描電腦時限制 CPU 使用率**

1. 在卡巴斯基安全管理中心管理主控台樹狀目錄中，選取**政策**。
2. 選擇必要的政策並點擊以開啟政策內容。
3. 在政策視窗中，選擇**"一般設定 → 應用程式設定"**。
4. 在**效能**下面，選擇 **限制掃描工作的 CPU 使用** 核取方塊並輸入 CPU 資源消耗的平均值（百分比）。
5. 儲存變更。

**如何在 Web 主控台和雲端主控台中掃描電腦時限制 CPU 使用率**

1. 在網頁主控台的主視窗中，選擇**資產（裝置）→ 政策和設定檔**。
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**限制掃描工作的 CPU 使用**下面，將切換開關設為 **限制掃描工作的 CPU 使用** 並輸入 CPU 資源消耗的平均值（百分比）。
6. 儲存變更。

**如何在應用程式介面掃描電腦時限制 CPU 使用率**

1. 在“應用程式主視窗”中，點擊⚙按鈕。
2. 在應用程式設定視窗中，選取”**一般設定**“→“**應用程式設定**”。




Kaspersky Endpoint Security for Windows 設定

3. 在**效能**下面，選擇 **限制掃描工作的 CPU 使用** 核取方塊並輸入 CPU 資源消耗的平均值（百分比）。
4. 儲存變更。

配置惡意軟體掃描的進階工作設定。

您可以最佳化檔案掃描：縮短掃描時間並提高 Kaspersky Endpoint Security 的執行速度。這可以透過僅掃描新檔案和上次掃描後經過修改的檔案來實現。此模式適用於簡單檔案和複合檔案。您還可以設定單個檔案的掃描限制。當指定的時間間隔到期時，Kaspersky Endpoint Security 將從目前掃描中排除該檔案（除包含多個檔案的存檔和物件之外）。

隱藏病毒和其他惡意程式的一種常用方法就是將其植入複合檔案中，例如存檔案或資料庫中。為了偵測以這種方式隱藏的病毒和其他惡意軟體，必須將複合檔案解壓縮，但是這可能會降低掃描速度。您可以限制要掃描的複合檔案類型，從而加快掃描速度。

您也可以啟用 iChecker 和 iSwift 技術。iChecker 和 iSwift 技術可以透過排除上次掃描後未修改的檔案來最佳化檔案掃描速度。

### 如何在管理主控台 (MMC) 中最佳化掃描

1. 開啟卡巴斯基安全管理中心管理主控台。
2. 在主控台樹狀目錄中，選擇**"工作"**。
3. 選擇掃描工作並雙擊以開啟工作內容。

   需要的話建立 *惡意軟體掃描* 工作。
4. 在工作內容視窗中，選取**"設定"**區域。
5. 在**"安全等級"**塊中，點擊**"設定"**按鈕。

   這將開啟掃描工作設定視窗。
6. 在**"最佳化"**塊中，配置掃描設定：

   - **只掃描新增及修改的檔案**僅掃描新檔案和自上次掃描以來已被修改的檔案。這有助於縮短掃描的持續時間。此模式適用於簡單檔案和複合檔案。

     您也可以設定依類型掃描新檔案。例如，您可以掃描所有分發套件和只掃描新壓縮檔案和 Office 格式的檔案。

   - **略過掃描時間超過以下值的檔案 N 秒**。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。

   - **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。
7. 點擊**"附加"**。

   這會開啟複合檔案掃描設定視窗。
8. 在**"容量限制"**塊中，選中**"複合檔案大於指定值時不解壓縮"**核取方塊。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。

   無論是否選中**"複合檔案大於指定值時不解壓縮"**核取方塊，Kaspersky Endpoint Security 均會掃描從存檔中提取的大型檔案。
9. 點擊**"確定"**。
10. 轉到**"附加"**標籤。

11. 在“**掃描技術**”塊中，選取您要在掃描期間使用的技術名稱旁邊的核取方塊。

    - **iSwift 技術**該技術允許透過排除特定檔案不掃描的方式提高掃描速度。該技術將使用特殊演算法將檔案排除在掃描範圍之外，該演算法會考慮 Kaspersky Endpoint Security 資料庫的發佈日期、檔案的上次掃描日期以及對掃描設定的任何修改。iSwift 技術是對用於 NTFS 檔案系統的 iChecker 技術的增強版。

    - **iChecker 技術**該技術允許透過排除特定檔案不掃描的方式提高掃描速度。該技術將使用特殊演算法將檔案排除在掃描範圍之外，該演算法會考慮 Kaspersky Endpoint Security 資料庫的發佈日期、檔案的上次掃描日期以及對掃描設定的任何修改。iChecker 技術受到幾個限制：它無法操作大檔案，並且僅能套用至擁有程式可辨識結構的檔案 (例如：.exe、.dll、.lnk、.ttf、.inf、.sys、.com、.chm、.zip 和 .rar)。

12. 儲存變更。

**如何在網頁主控台和 Cloud Console 中最佳化掃描**

1. 在網頁主控台的主視窗中，選擇**資產（裝置）→工作**。

   工作清單開啟。

2. 點擊掃描工作。

   工作內容視窗將開啟。需要的話建立 *惡意軟體掃描* 工作。

3. 選擇“**應用程式設定**”標籤。

4. 在“**偵測到威脅後的動作**“塊中，選中“**只掃描新增及修改的檔案**”核取方塊。僅掃描新檔案和自上次掃描以來已被修改的檔案。這有助於縮短掃描的持續時間。此模式適用於簡單檔案和複合檔案。

   您也可以設定依類型掃描新檔案。例如，您可以掃描所有分發套件和只掃描新壓縮檔案和 Office 格式的檔案。

5. 在“**掃描最佳化**“塊中，選中“**複合檔案大於指定值時不解壓縮**”核取方塊。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。

   無論是否選中“**複合檔案大於指定值時不解壓縮**”核取方塊，Kaspersky Endpoint Security 均會掃描從存檔中提取的大型檔案。

6. 選擇“**不要同時執行多個掃描工作**”核取方塊。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。

7. 在“**進階設定**“塊中，選中“**略過掃描時間超過以下時長的檔案（秒）**”核取方塊。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。

8. 儲存變更。

**如何在應用程式介面中最佳化掃描**

1. 在應用程式主視窗中，轉至“**工作**”區域。

2. 在工作清單中，選擇掃描工作，然後點擊⚙。

3. 點擊“**進階設定**”。

4. 在“**最佳化**“塊中，配置掃描設定：

   - **只掃描新增及修改的檔案**僅掃描新檔案和自上次掃描以來已被修改的檔案。這有助於縮短掃描的持續時間。此模式適用於簡單檔案和複合檔案。

     您也可以設定依類型掃描新檔案。例如，您可以掃描所有分發套件和只掃描新壓縮檔案和 Office 格式的檔案。

   - **略過掃描時間超過以下值的檔案 N 秒**。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。

   - **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。

5. 在“**大小限制**“塊中，選中“**不解壓縮大型複合檔案**”核取方塊。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。

   無論是否選中“**不解壓縮大型複合檔案**”核取方塊，Kaspersky Endpoint Security 均會掃描從存檔中提取的大型檔案。

6. 在“**掃描技術**”塊中，選取您要在掃描期間使用的技術名稱旁邊的核取方塊。

   - **iSwift 技術**該技術允許透過排除特定檔案不掃描的方式提高掃描速度。該技術將使用特殊演算法將檔案排除在掃描範圍之外，該演算法會考慮 Kaspersky Endpoint Security 資料庫的發佈日期、檔案的上次掃描日期以及對掃描設定的任何修改。iSwift 技術是對用於 NTFS 檔案系統的 iChecker 技術的增強版。

   - **iChecker 技術**該技術允許透過排除特定檔案不掃描的方式提高掃描速度。該技術將使用特殊演算法將檔案排除在掃描範圍之外，該演算法會考慮 Kaspersky Endpoint Security 資料庫的發佈日期、檔案的上次掃描日期以及對掃描設定的任何修改。iChecker 技術受到幾個限制：它無法操作大檔案，並且僅能套用至擁有程式可辨識結構的檔案 (例如：.exe、.dll、.lnk、.ttf、.inf、.sys、.com、.chm、.zip 和 .rar)。

7. 儲存變更。

如果掃描工作未顯示，則意味著管理員已在政策中禁止使用本機工作。

# 更新資料庫和程式模組

更新 Kaspersky Endpoint Security 的資料庫和程式模組可為您的電腦提供最新防護。新病毒和其他類型的惡意程式每天都在全世界出現。Kaspersky Endpoint Security 資料庫包含關於威脅的資訊和解毒的方法。要快速偵測到威脅，建議您定期更新資料庫和應用程式模組。

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

定期更新需要一份程式要使用的活動授權檔案。如果目前沒有產品授權，您將只能執行一次更新。

您的電腦必須連線到網際網路才能成功下載來自卡巴斯基更新伺服器的更新資料。預設情況下，系統將自動確定網際網路連線設定。如果您使用代理伺服器，則需要設定代理伺服器設定。

透過 HTTPS 協定下載更新。當無法透過 HTTPS 協定下載更新時，也可以透過 HTTP 協定下載。

當執行更新時，以下物件將下載並安裝到您的電腦中：

- Kaspersky Endpoint Security 資料庫。由於資料庫包含了威脅簽章和關於如何刪除威脅的資訊，電腦因此而獲得防護。當搜尋並為受感染檔案解毒時，防護元件將使用此資訊。資料庫將不斷更新應對它們的方法和新威脅記錄。因此，我們建議您定期更新資料庫。

  除了 Kaspersky Endpoint Security 資料庫之外，系統也會更新已啟用程式元件以攔截網路流量的網路驅動程式。

- 程式模組。除了 Kaspersky Endpoint Security 資料庫，您也可以更新程式模組。更新程式模組可以修復 Kaspersky Endpoint Security 中的弱點、新增新功能或強化現有功能。

更新時，您的電腦上的程式模組和資料庫將與最新版本更新來源進行對比。如果您目前資料庫和程式模組與對應的最新版本不同，缺少的更新部分將安裝在您的電腦上。

如果資料庫過期，更新量可能會很大，這可能會花費更多的網際網路流量（最多達幾十 MB）。

Kaspersky Endpoint Security 資料庫的目前狀態相關資訊顯示在應用程式主視窗中，或者通知區域中當您將游標懸浮在應用程式圖示上看到的工具提示中。

有關更新工作執行期間更新結果和所有發生事件的資訊將記錄在 Kaspersky Endpoint Security 報告中。

如果應用程式正在 Light Agent 模式下運作，更新應用程式資料庫和模組時將涉及特別考慮 。

# 資料庫和應用程式模組更新方案

更新 Kaspersky Endpoint Security 的資料庫和程式模組可為您的電腦提供最新防護。新病毒和其他類型的惡意程式每天都在全世界出現。Kaspersky Endpoint Security 資料庫包含關於威脅的資訊和解毒的方法。要快速偵測到威脅，建議您定期更新資料庫和應用程式模組。

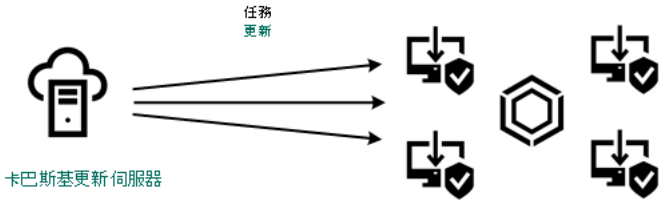
以下物件在使用者的電腦上更新：

- 病毒資料庫。病毒資料庫包括惡意軟體簽章資料庫、網路攻擊敘述、惡意和釣魚網址資料庫、廣告欄資料庫、垃圾郵件資料庫以及其他資料。
- 程式模組。模組更新旨在消除應用程式中的弱點和改進電腦防護方法。模組更新可能變更應用程式元件的行為和新增新功能。

Kaspersky Endpoint Security 支援下列資料庫和應用程式模組更新方案：

- 從 Kaspersky 伺服器更新。

  卡巴斯基更新伺服器位於全球多個國家。這可確保更新的高可靠性。如果無法從一台伺服器執行更新，Kaspersky Endpoint Security 會切換到下一台伺服器。




從 Kaspersky 伺服器更新

- 集中更新。

  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。

     更新套件由名為“*將更新下載至管理伺服器儲存區*”的管理伺服器工作下載到儲存區。

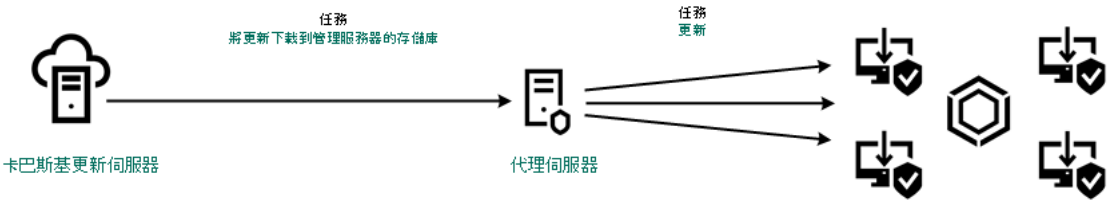
  2. 將更新套件下載到共用資料夾（可選）。

     您可以使用以下方法將更新套件下載到共用資料夾：

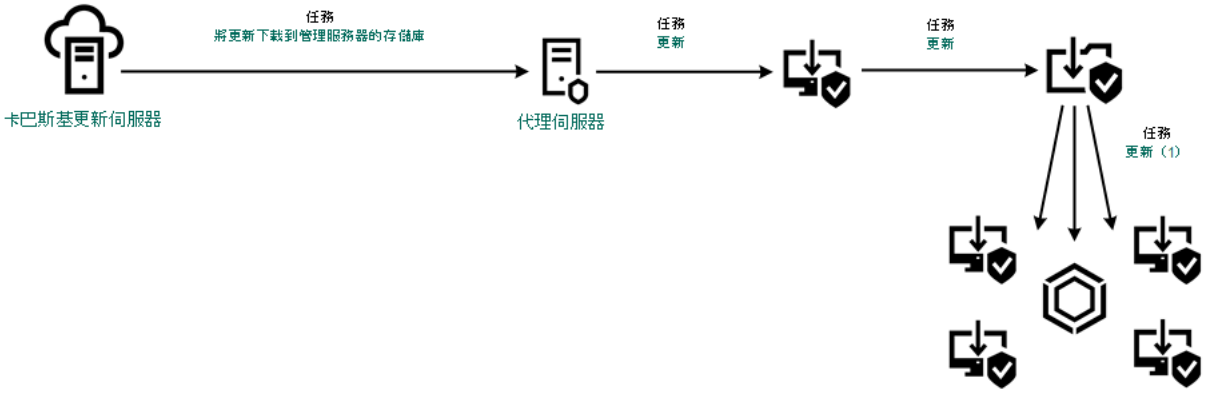
     - 使用 Kaspersky Endpoint Security 的“*資料庫和應用程式模組更新*”工作。該工作用於公司區域網路中的一台電腦。
     - 使用 Kaspersky 更新實用程式。有關使用 Kaspersky 更新實用程式的詳細資訊，請參閱 卡巴斯基知識庫。

3. 將更新套件分發到用戶端電腦。

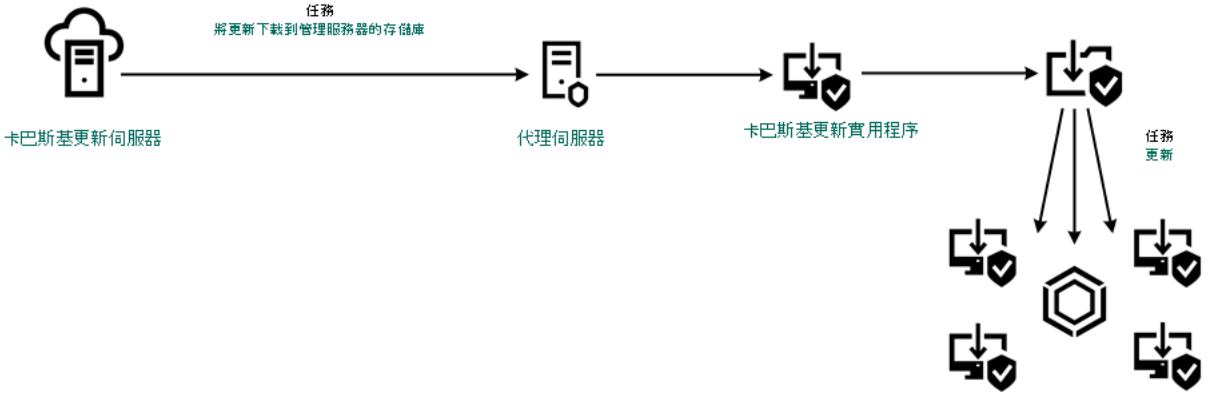
   更新套件由 Kaspersky Endpoint Security 的"*資料庫和應用程式模組更新*"工作分發到用戶端電腦。您可以為每個管理群組建立無限數量的更新工作。




從伺服器儲存區更新




從共用資料夾更新




使用 Kaspersky 更新實用程式更新

對於卡巴斯基安全管理中心，預設更新來源清單包含卡巴斯基安全管理中心管理伺服器和卡巴斯基更新伺服器。對於卡巴斯基安全管理中心雲端主控台，預設更新來源清單包含發佈點和卡巴斯基更新伺服器。有關發佈點的詳細資訊，請參閱卡巴斯基安全管理中心雲端主控台說明。您可以在清單中新增其他更新來源。您可以指定 HTTP/FTP 伺服器和共用資料夾作為更新來源。如果無法從一個更新來源執行更新，Kaspersky Endpoint Security 會轉換到下一個更新來源。

更新透過標準網路通訊協定從卡巴斯基更新伺服器或其他 FTP 或 HTTP 伺服器下載。如果存取更新來源需要連線代理伺服器，則在 Kaspersky Endpoint Security 政策設定中指定代理伺服器設定。

# 從伺服器儲存區更新

為了節省網際網路流量，您可以配置組織的 LAN 中的電腦從伺服器儲存區更新資料庫和應用程式模組。為此，卡巴斯基安全管理中心必須將更新套件從卡巴斯基更新伺服器下載到儲存區（FTP 或 HTTP 伺服器、網路或本機資料夾）。組織的 LAN 中的其他電腦將能夠從伺服器儲存區接收更新套件。

配置從伺服器儲存區更新資料庫和應用程式模組包括以下步驟：

1. 配置將更新套件下載到管理伺服器儲存區（“*將更新下載至管理伺服器儲存區*”工作）。

   *將更新下載至管理伺服器儲存區*工作將由管理伺服器快速啟動精靈自動建立，該工作只能有一個實例。預設情況下，卡巴斯基安全管理中心將更新套件複製到資料夾 `\\<server name>\KLSHARE\Updates`。有關下載更新到管理伺服器儲存區的詳細資訊，請參閱卡巴斯基安全管理中心說明。

2. 配置組織的 LAN 中的其餘電腦從指定伺服器儲存區更新資料庫和應用程式模組（“*資料庫和應用程式模組更新*”工作）。

   **如何在管理主控台 (MMC) 中配置指定伺服器儲存中的 Kaspersky Endpoint Security 更新**

   1. 開啟卡巴斯基安全管理中心管理主控台。

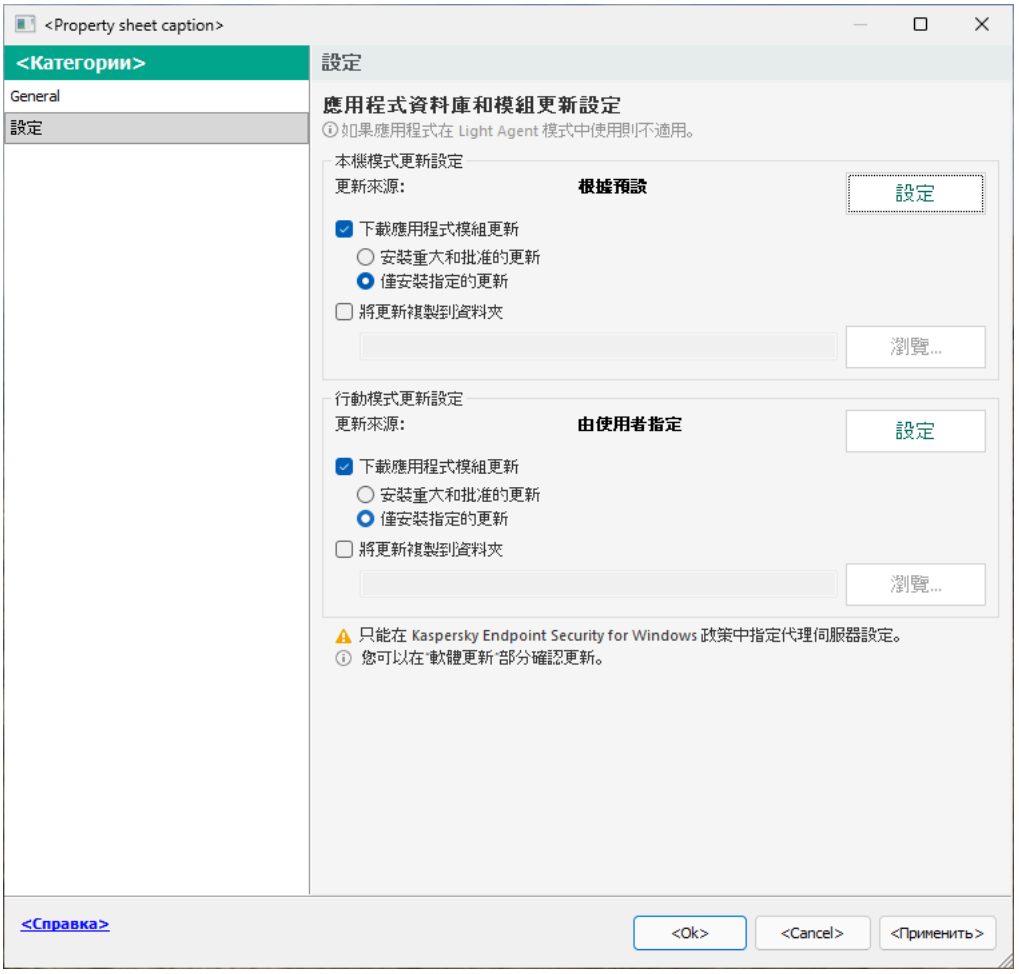
      在主控台樹狀目錄中，選擇“**工作**”。

   2. 點擊 Kaspersky Endpoint Security 的“**資料庫和應用程式模組更新**”工作。

      工作內容視窗將開啟。

      *資料庫和應用程式模組更新*工作由管理伺服器快速啟動精靈自動建立。要建立“*資料庫和應用程式模組更新*”工作，請在執行精靈時安裝 Kaspersky Endpoint Security for Windows 管理外掛程式。

   3. 在工作內容視窗中，選取“**設定**”區域。




資料庫和應用程式模組更新工作設定

4. 在”**本機模式更新設定**”塊中，點擊”**設定**”按鈕。

5. 在更新來源清單中，確保啟用來自**卡巴斯基安全管理中心**來源的更新。此外，**卡巴斯基安全管理中心**來源必須具有最高優先順序。

6. 如有必要，新增更新來源：

   a. 在更新來源清單中，點擊**"新增"**按鈕。

   b. 在**"更新來源"**欄位中，指定卡巴斯基安全管理中心會將接收自 Kaspersky 伺服器的更新套件複製到的 FTP 或 HTTP 伺服器、網路資料夾或者本機資料夾的位址。

   > 當設定將更新下載到伺服器儲存時，更新來源的位址必須與您在**"更新儲存資料夾"**欄位中指定的位址相符（*將更新下載至管理伺服器儲存區*工作）。

   c. 點擊**"確定"**。

   您可以排除更新來源而不將其從更新來源清單中刪除。為此，請清除物件旁邊的核取方塊。




更新來源

7. 使用**"上移"**和**"下移"**按鈕配置更新來源的優先順序。

   如果無法從第一個更新來源執行更新，Kaspersky Endpoint Security 會轉換到下一個更新來源。

8. 在工作內容視窗中，選取**"排程"**區域並配置工作執行模式。

9. 預設情況下，Kaspersky Endpoint Security 以手動模式執行工作。

10. 儲存變更。

**如何在 Web 主控台中配置指定伺服器儲存中的 Kaspersky Endpoint Security 更新**

1. 在網頁主控台的主視窗中，選擇**資產（裝置）→工作**。

   工作清單開啟。

2. 點擊 Kaspersky Endpoint Security 的**"更新"**工作。

   工作內容視窗將開啟。

   *更新*工作由管理伺服器快速啟動精靈自動建立。要建立*"更新"*工作，請在執行精靈時安裝 Kaspersky Endpoint Security for Windows 管理外掛程式。

3. 選擇**"應用程式設定 → 本機模式"**標籤。

4. 在更新來源清單中，確保啟用來自**卡巴斯基安全管理中心**來源的更新。此外，**卡巴斯基安全管理中心**來源必須具有最高優先順序。

5. 如有必要，新增更新來源：

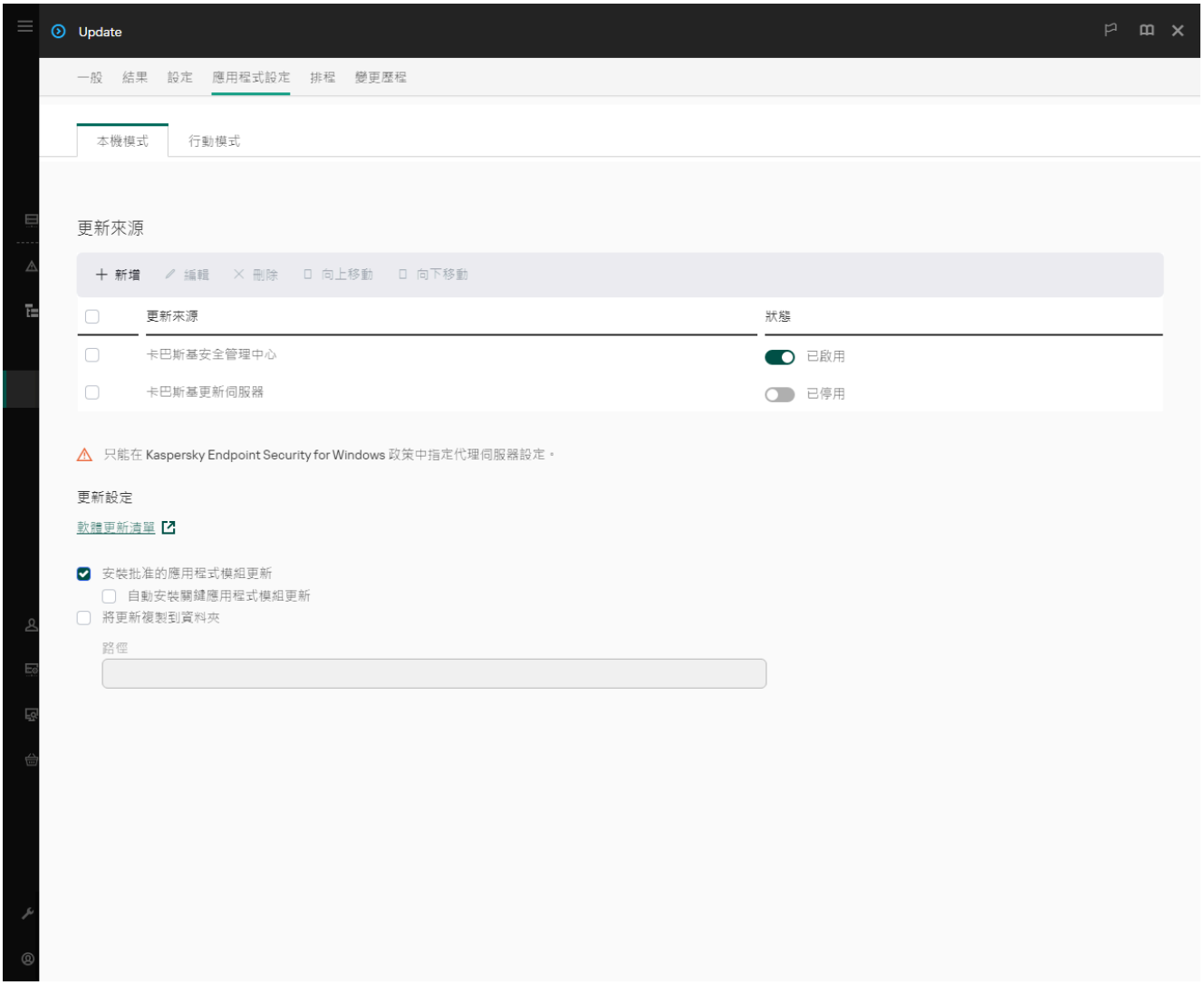
   a. 在更新來源清單中，點擊**"新增"**按鈕。

   b. 在**"更新來源"**欄位中，指定卡巴斯基安全管理中心會將接收自 Kaspersky 伺服器的更新套件複製到的 FTP 或 HTTP 伺服器、網路資料夾或者本機資料夾的位址。

      當設定將更新下載到伺服器儲存時，更新來源的位址必須與您在**"更新儲存資料夾"**欄位中指定的位址相符（*將更新下載至管理伺服器儲存區*工作）。

   c. 點擊**"儲存"**。

   您可以排除更新來源而不將其從更新來源清單中刪除。為此，將它旁邊的切換開關設為關閉位置。




更新來源

6. 使用**"上"**和**"下"**按鈕配置更新來源的優先順序。

   如果無法從第一個更新來源執行更新，Kaspersky Endpoint Security 會轉換到下一個更新來源。

7. 在工作內容視窗中，選取**"排程"**區域並配置工作執行模式。

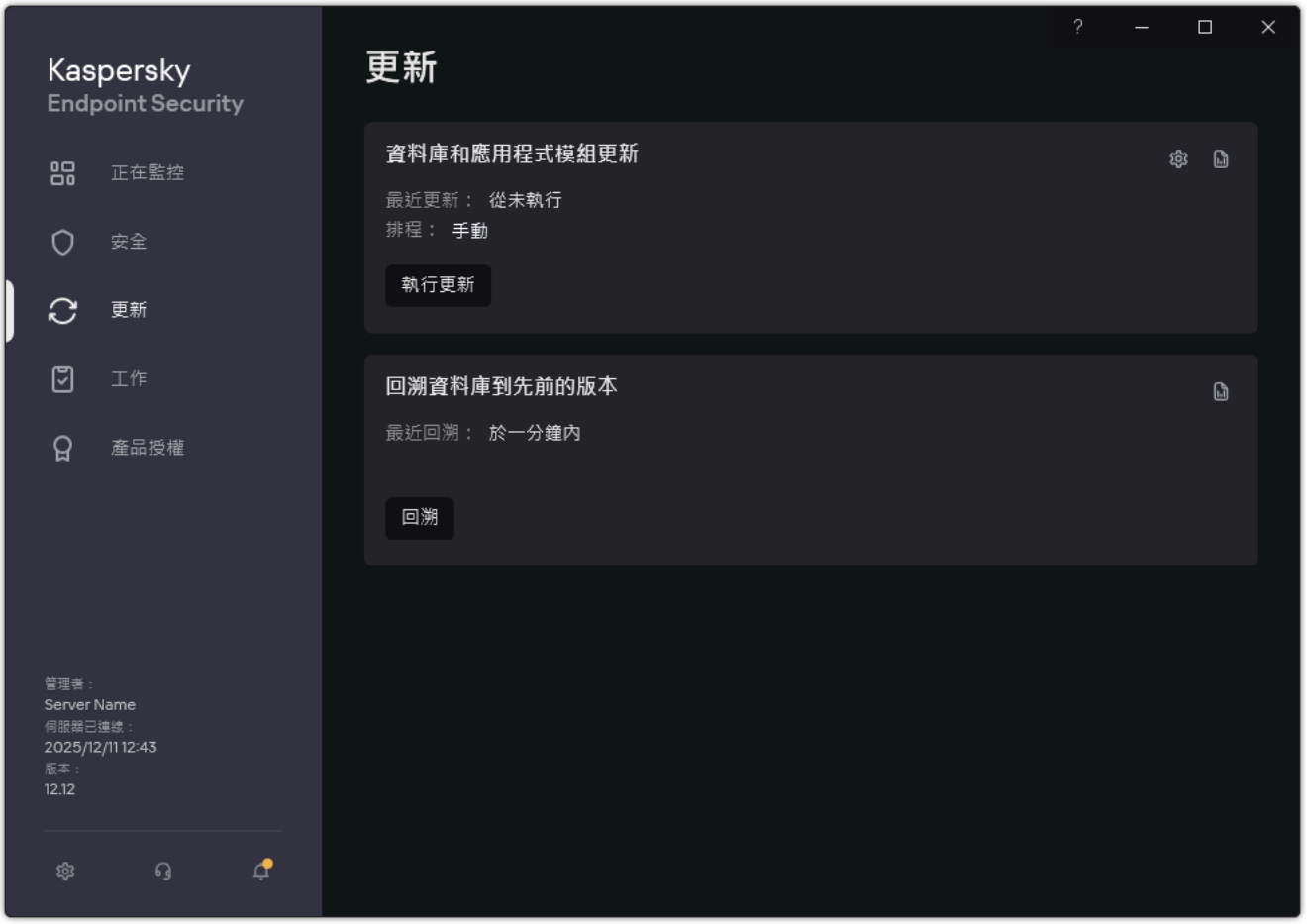
8. 預設情況下，Kaspersky Endpoint Security 以手動模式執行工作。

9. 儲存變更。

**如何在應用程式介面中配置指定伺服器儲存中的 Kaspersky Endpoint Security 更新**

您不能在應用程式介面中配置*資料庫和應用程式模組更新*群組工作。只有一個本機更新工作，*資料庫和應用程式模組更新*，可供使用者使用。如果*資料庫和應用程式模組更新*工作未顯示，則意味著管理員已在政策中禁止使用本機工作。

1. 在應用程式主視窗中，轉至**"更新"**區域。




本機更新工作

2. 這將開啟工作清單；選擇*資料庫和應用程式模組更新*工作，然後點擊⚙。

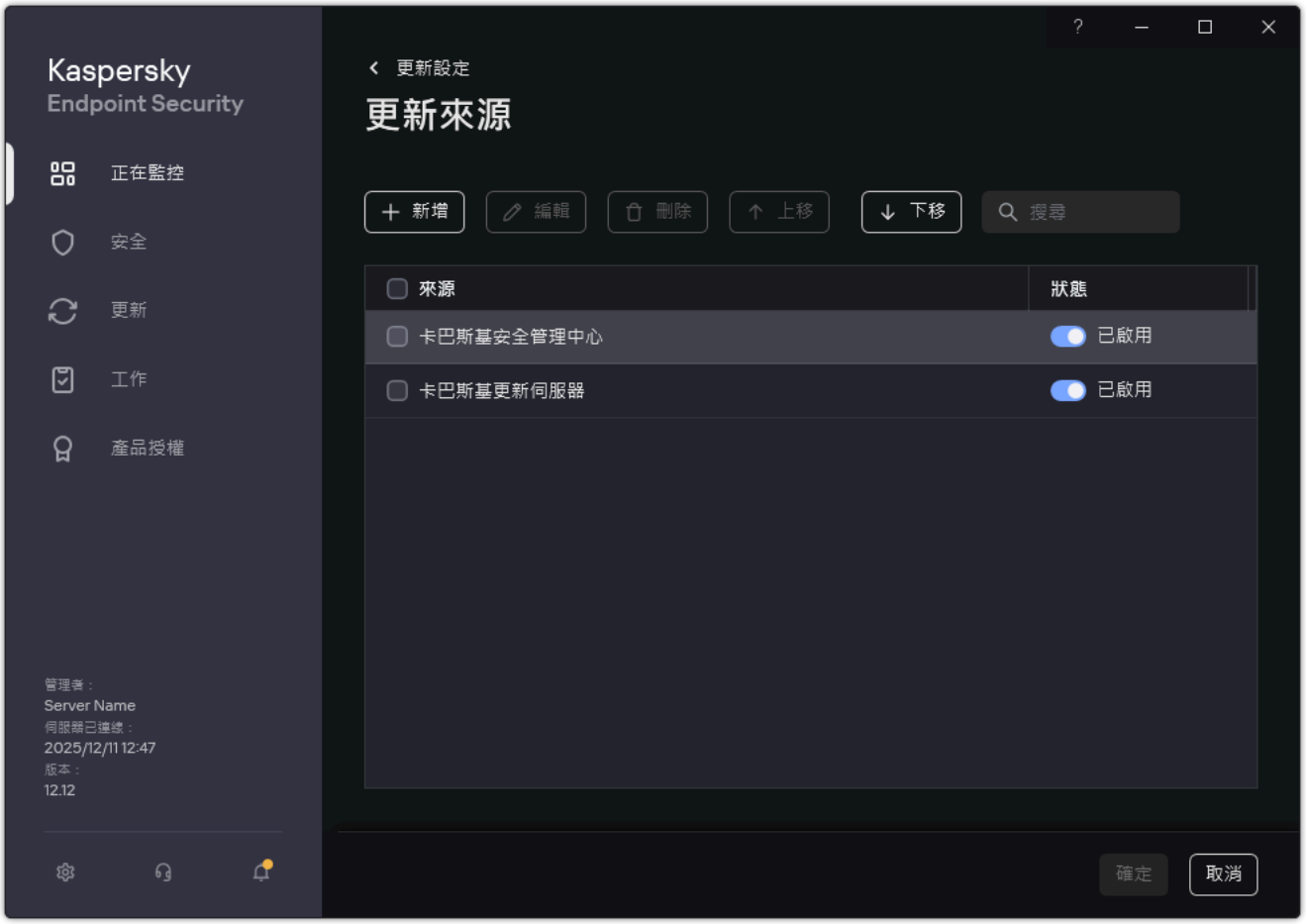
   工作內容視窗將開啟。

3. 在工作內容視窗中，點擊**選擇更新來源**。

4. 在更新來源清單中，確保啟用來自**卡巴斯基安全管理中心**來源的更新。此外，**卡巴斯基安全管理中心**來源必須具有最高優先順序。

5. 如有必要，新增更新來源：

a. 在更新來源清單中，點擊**"新增"**按鈕。




更新來源

a. 指定卡巴斯基安全管理中心會將接收自 Kaspersky 伺服器的更新套件複製到的 FTP 或 HTTP 伺服器、網路資料夾或者本機資料夾的位址。

> 當設定將更新下載到伺服器儲存時，更新來源的位址必須與您在**"更新儲存資料夾"**欄位中指定的位址相符（*將更新下載至管理伺服器儲存區*工作）。

b. 點擊**"選擇"**。

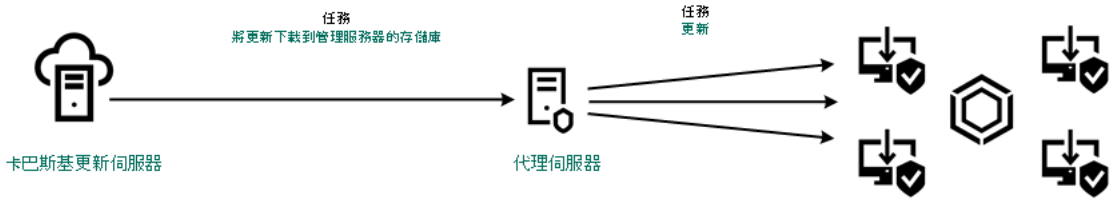
您可以排除更新來源而不將其從更新來源清單中刪除。為此，將它旁邊的切換開關設為關閉位置。

6. 使用**"上移"**和**"下移"**按鈕配置更新來源的優先順序。

如果無法從第一個更新來源執行更新，Kaspersky Endpoint Security 會轉換到下一個更新來源。

> 如果電腦由卡巴斯基安全管理中心管理，則無法配置*資料庫和應用程式模組更新*工作的執行模式。您只能手動執行工作。

7. 儲存變更。




從伺服器儲存區更新

# 從共用資料夾更新

為了節省流量，您可以配置組織的 LAN 中的電腦從共用資料夾更新資料庫和應用程式模組。為此，組織的 LAN 中的一台電腦必須從卡巴斯基安全管理中心管理伺服器或從卡巴斯基更新伺服器接收更新套件，然後將收到的更新套件複製到共用資料夾。組織的 LAN 中的其他電腦將能夠從該共用資料夾接收更新套件。

將更新套件複製到共用資料夾的 Kaspersky Endpoint Security 應用程式的版本和當地語係化必須比對從共用資料夾更新資料庫的應用程式的版本和當地語係化。如果應用程式的版本或者當地語係化不比對，資料庫更新可能會以錯誤結束。

配置從共用資料夾更新資料庫和應用程式模組包括以下步驟：

1. 設定從伺服器儲存區更新資料庫和應用程式模組。
2. 啟用將更新資料複製到位於區域網路上的一台電腦的共用資料夾中。

   **如何啟用在管理主控台 (MMC) 中將更新套件複製到共用資料夾**

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

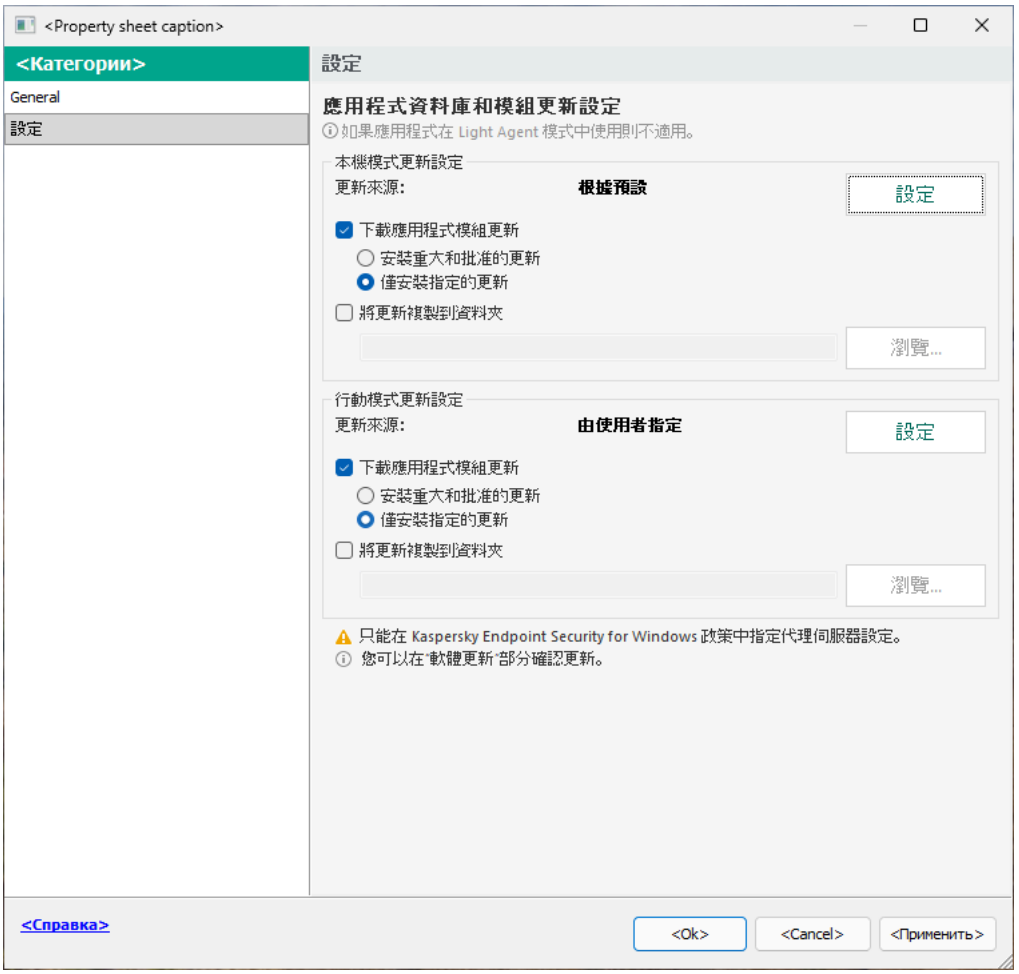
      必須為將用作更新來源的電腦分配*"資料庫和應用程式模組更新"*工作。

   3. 點擊 Kaspersky Endpoint Security 的**"資料庫和應用程式模組更新"**工作。

      工作內容視窗將開啟。

      *資料庫和應用程式模組更新*工作由管理伺服器快速啟動精靈自動建立。要建立*"資料庫和應用程式模組更新"*工作，請在執行精靈時安裝 Kaspersky Endpoint Security for Windows 管理外掛程式。

4. 在工作內容視窗中，選取**"設定"**區域。




資料庫和應用程式模組更新工作設定

5. 在**"本機模式更新設定"**塊中，點擊**"設定"**按鈕。

6. 配置更新來源。

   更新來源可以是卡巴斯基更新伺服器、卡巴斯基安全管理中心管理伺服器、其他 FTP 或 HTTP 伺服器、本機資料夾或網路資料夾。

7. 選擇**"將更新複製到資料夾"**核取方塊。

8. 在**"資料夾路徑"**欄位中，輸入共用資料夾的 UNC 路徑（例如 `\\<server name>\KLSHARE\Updates`）。

   如果將該欄位留空，Kaspersky Endpoint Security 會將更新套件複製到 `C:\Documents and Settings\All Users\Application Data\Kaspersky Lab\AVP12\Update distribution\`。

9. 儲存變更。

**如何啟用在網頁主控台和雲端主控台中將更新套件複製到共用資料夾**

1. 在網頁主控台的主視窗中，選擇**資產（裝置）→工作**。

   工作清單開啟。

   > 必須為將用作更新來源的電腦分配*"更新"*工作。

2. 點擊 Kaspersky Endpoint Security 的**"更新"**工作。

   工作內容視窗將開啟。

*更新*工作由管理伺服器快速啟動精靈自動建立。要建立"*更新*"工作，請在執行精靈時安裝 Kaspersky Endpoint Security for Windows 管理外掛程式。

3. 選擇"**應用程式設定 → 本機模式**"標籤。
4. 配置更新來源。

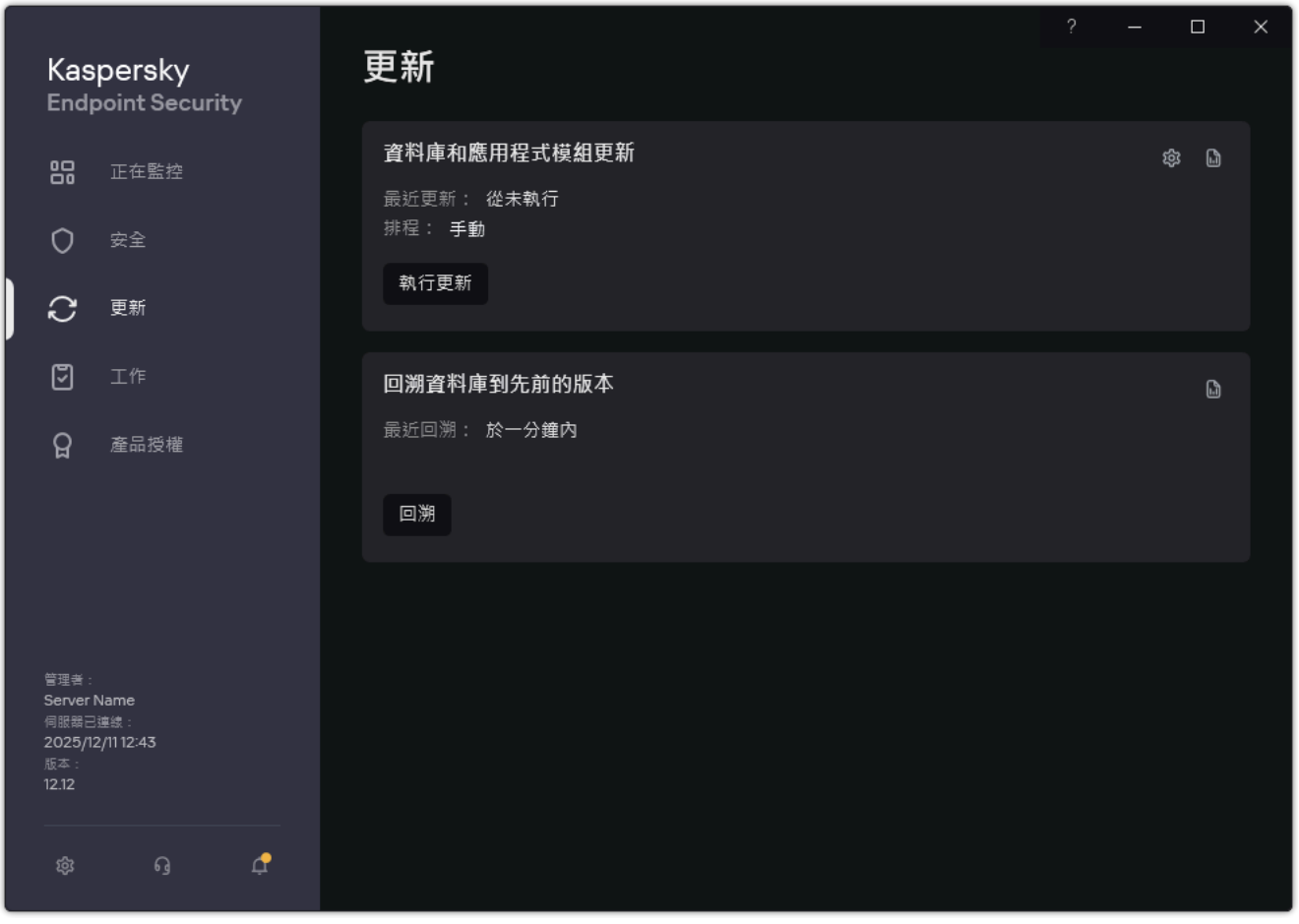
   更新來源可以是卡巴斯基更新伺服器、卡巴斯基安全管理中心管理伺服器、其他 FTP 或 HTTP 伺服器、本機資料夾或網路資料夾。
5. 選擇"**將更新複製到資料夾**"核取方塊。
6. 在"**路徑**"欄位中，輸入共用資料夾的 UNC 路徑（例如 `\\<server name>\KLSHARE\Updates`）。

   如果將該欄位留空，Kaspersky Endpoint Security 會將更新套件複製到 `C:\Documents and Settings\All Users\Application Data\Kaspersky Lab\AVP12\Update distribution\`。
7. 儲存變更。

**如何啟用在應用程式介面中將更新套件複製到共用資料夾**

您不能在應用程式介面中配置*資料庫和應用程式模組更新*群組工作。只有一個本機更新工作，*資料庫和應用程式模組更新*，可供使用者使用。如果*資料庫和應用程式模組更新*工作未顯示，則意味著管理員已在政策中禁止使用本機工作。

1. 在應用程式主視窗中，轉至"**更新**"區域。




本機更新工作

2. 這將開啟工作清單；選擇*資料庫和應用程式模組更新*工作，然後點擊⚙。

   工作內容視窗將開啟。

3. 在“**正在發佈更新**“塊中，選中“**將更新複製到資料夾**”核取方塊。

4. 輸入共用資料夾的 UNC 路徑（例如 `\\<server name>\KLSHARE\Updates`）。

5. 儲存變更。

3. 配置組織的 LAN 中的其餘電腦從指定共用資料夾更新資料庫和應用程式模組。

**如何在管理主控台 (MMC) 中設定共用資料夾更新**

1. 在網頁主控台的主視窗中，選擇**資產（裝置）→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 Windows 12.12.0**”。

   b. 在“**工作類型**”下拉式清單中，選取“**資料庫和應用程式模組更新**”。

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

5. 點擊**“新工作”**。

啟動“工作精靈”。按照精靈的說明進行操作。

步驟 1. 選取工作類型

選取“**Kaspersky Endpoint Security for Windows (12.12)**”→“**資料庫和應用程式模組更新**”。

步驟 2. 選擇更新來源

新增新的更新來源：共用資料夾。來源位址必須與您之前配置將更新套件複製到共用資料夾時在“**資料夾路徑**”欄位中指定的位址相比對。使用“**上移**”和“**下移**”按鈕配置更新來源的優先順序。

步驟 3. 選取將要對其分配工作的裝置

選取將要執行工作的電腦。下列選項可用：

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

必須為組織的 LAN 中除用作更新來源的電腦之外的電腦分配"*資料庫和應用程式模組更新*"工作。

步驟 4. 選取要執行工作的帳戶

選取要執行*資料庫和應用程式模組更新*工作的帳戶。預設情況下，Kaspersky Endpoint Security 將使用本機使用者帳戶的權限啟動工作。

步驟 5. 設定工作啟動排程

設定工作啟動排程，例如，手動或在將防毒資料庫下載到儲存庫之後。

步驟 6. 定義工作名稱

輸入工作名稱，例如 *從共用資料夾更新*。

步驟 7. 完成工作建立

結束精靈。如有必要，選中"**精靈完成時執行工作**"核取方塊。您可以在工作內容中監控工作進度。結果，將按照指定排程在使用者電腦上執行更新工作。

**如何在網頁主控台和雲端主控台中配置共用資料夾更新**

1. 在網頁主控台的主視窗中，選擇**資產（裝置）→ 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 Windows 12.12.0**”。

   b. 在“**工作類型**”下拉式清單中，選取“**更新**”。

   c. 在“**工作名稱**”欄位中，輸入簡要說明，例如，“*從共用資料夾更新*”。

   d. 在“**要將工作指派給的裝置**”塊中，選取工作範圍。

   > 必須為組織的 LAN 中除用作更新來源的電腦之外的電腦分配“*更新*”工作。

4. 按照所選工作範圍選項選取裝置，然後前往下一步。

5. 結束精靈。
   在工作表中將顯示一個新工作。

6. 點擊新建立的“*更新*”工作。
   工作內容視窗將開啟。

7. 選擇“**應用程式設定 → 本機模式**”標籤。

8. 在”**更新來源**”塊中，點擊”**新增**”按鈕。

9. 在開啟的視窗中，輸入共用資料夾的路徑。

   > 來源位址必須與您之前配置將更新套件複製到共用資料夾時在“**路徑**”欄位中指定的位址相比對（請參見上述說明）。

10. 點擊“**確定**”。

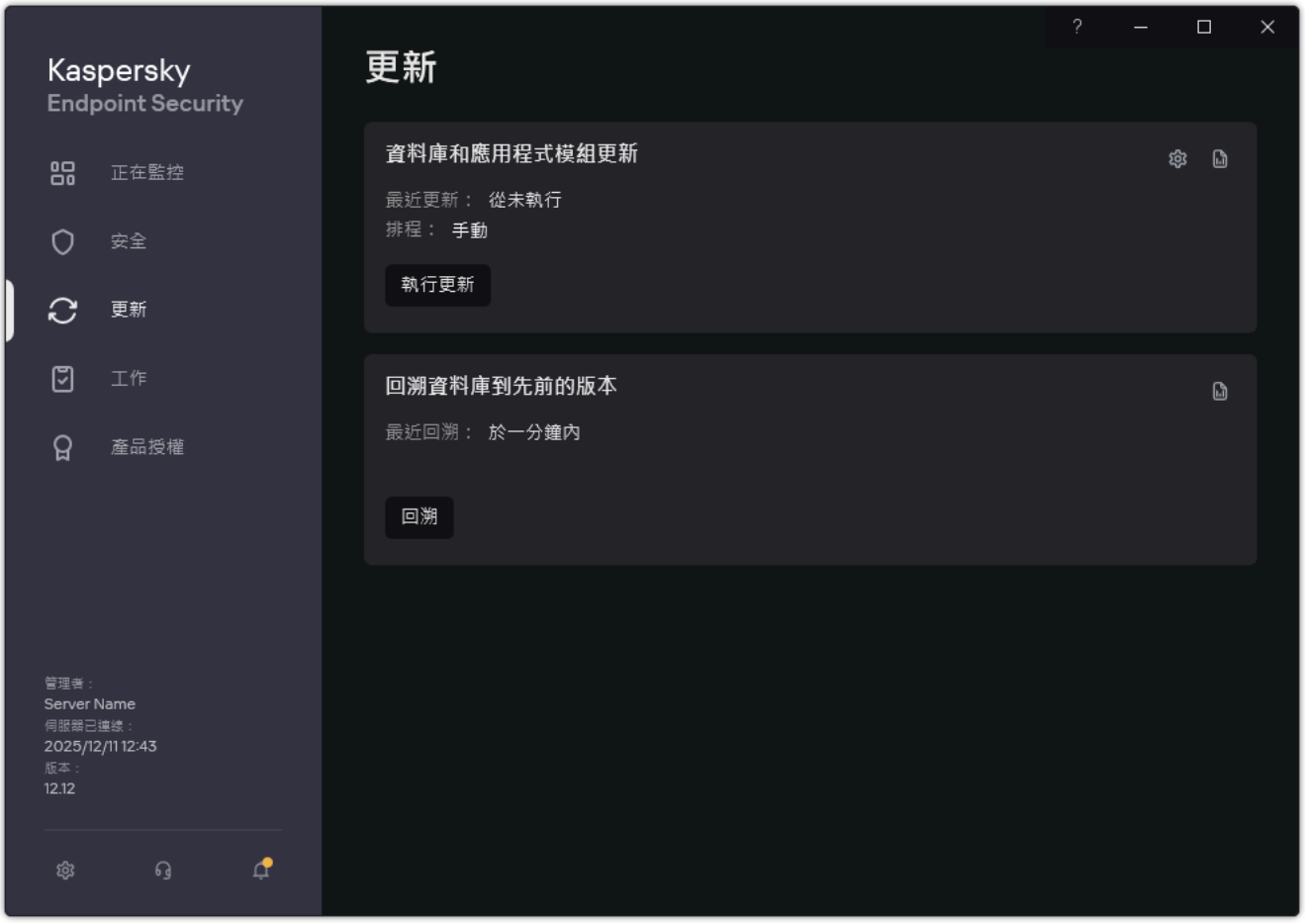
11. 使用“**上**”和“**下**”按鈕配置更新來源的優先順序。

12. 儲存變更。

### 如何在應用程式介面中設定共用資料夾更新

您不能在應用程式介面中配置*資料庫和應用程式模組更新*群組工作。只有一個本機更新工作，*資料庫和應用程式模組更新*，可供使用者使用。如果*資料庫和應用程式模組更新*工作未顯示，則意味著管理員已在政策中禁止使用本機工作。

1. 在應用程式主視窗中，轉至**"更新"**區域。




本機更新工作

2. 這將開啟工作清單；選擇*資料庫和應用程式模組更新*工作，然後點擊⚙。
   工作內容視窗將開啟。
3. 點擊**"選擇更新來源"**。
4. 在開啟的視窗中，點擊**"新增"**按鈕。
5. 在開啟的視窗中，輸入共用資料夾的路徑。

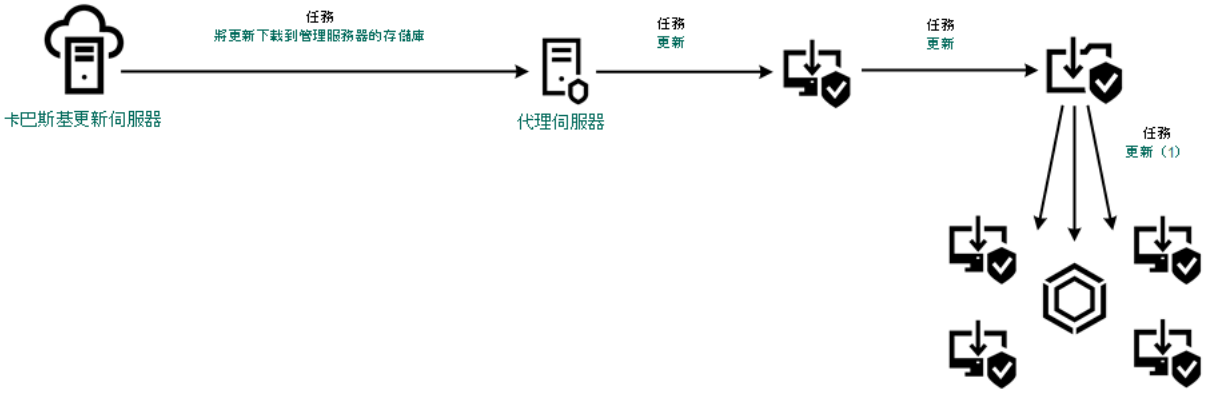
   來源位址必須與您之前設定將更新套件複製到共用資料夾時指定的位址相符（請參見上述說明）。

6. 點擊**"選擇"**。

7. 使用“**上移**”和“**下移**”按鈕配置更新來源的優先順序。

   如果無法從第一個更新來源執行更新，Kaspersky Endpoint Security 會轉換到下一個更新來源。

8. 儲存變更。




從共用資料夾更新

# 使用 Kaspersky 更新實用程式更新

為了節省網際網路流量，您可以使用 Kaspersky 更新實用程式配置從共用資料夾更新組織 LAN 中的電腦上的資料庫和應用程式模組。為此，組織的 LAN 中的一台電腦必須從卡巴斯基安全管理中心管理伺服器或從卡巴斯基更新伺服器接收更新套件，然後使用實用程式將收到的更新套件複製到共用資料夾。組織的 LAN 中的其他電腦將能夠從該共用資料夾接收更新套件。

將更新套件複製到共用資料夾的 Kaspersky Endpoint Security 應用程式的版本和當地語係化必須比對從共用資料夾更新資料庫的應用程式的版本和當地語係化。如果應用程式的版本或者當地語係化不比對，資料庫更新可能會以錯誤結束。

配置從共用資料夾更新資料庫和應用程式模組包括以下步驟：

1. 設定從伺服器儲存區更新資料庫和應用程式模組。

2. 在組織的 LAN 的一台電腦上安裝 Kaspersky 更新實用程式。

3. 在 Kaspersky 更新實用程式設定中配置將更新套件複製到共用資料夾。

   您可以從 Kaspersky 技術支援網站 下載 Kaspersky 更新實用程式分發套件。安裝該實用程式後，選擇更新來源（例如，管理伺服器儲存區）和 Kaspersky 更新實用程式將更新套件複製到的共用資料夾。有關使用 Kaspersky 更新實用程式的詳細資訊，請參閱 卡巴斯基知識庫 。

4. 配置組織的 LAN 中的其餘電腦從指定共用資料夾更新資料庫和應用程式模組。

   **如何在管理主控台 (MMC) 中設定共用資料夾更新**

   1. 開啟卡巴斯基安全管理中心管理主控台。

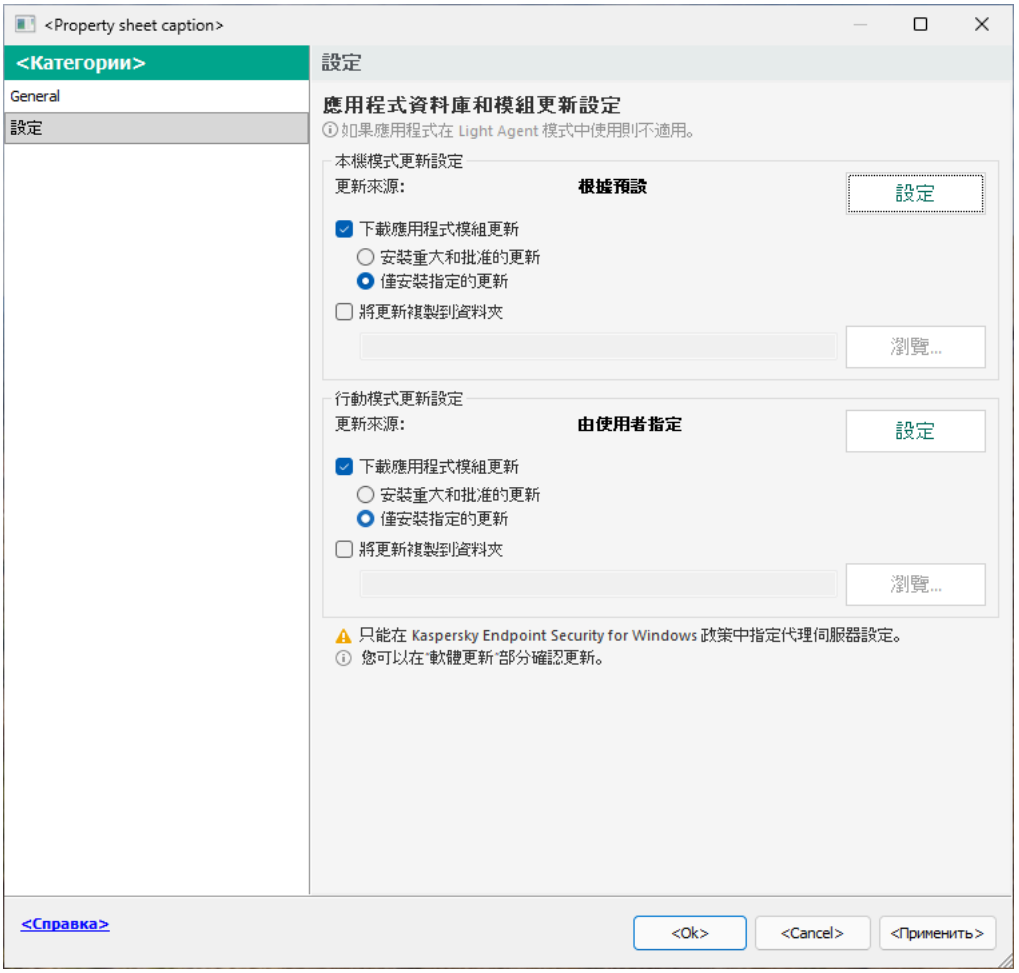
   2. 在主控台樹狀目錄中，選擇“**工作**”。

   3. 點擊 Kaspersky Endpoint Security 的“**資料庫和應用程式模組更新**”工作。

      工作內容視窗將開啟。

*資料庫和應用程式模組更新*工作由管理伺服器快速啟動精靈自動建立。要建立"*資料庫和應用程式模組更新*"工作，請在執行精靈時安裝 Kaspersky Endpoint Security for Windows 管理外掛程式。

4. 在工作內容視窗中，選取"**設定**"區域。




資料庫和應用程式模組更新工作設定

5. 在"**本機模式更新設定**"塊中，點擊"**設定**"按鈕。

6. 在更新來源清單中，點擊"**新增**"按鈕。

7. 在開啟的視窗中，輸入共用資料夾的 UNC 路徑（例如 `\\<server name>\KLSHARE\Updates`）。

   來源位址必須與 Kaspersky 更新實用程式設定中指示的位址比對。

8. 點擊"**確定**"。

9. 使用"**上移**"和"**下移**"按鈕配置更新來源的優先順序。

   如果無法從第一個更新來源執行更新，Kaspersky Endpoint Security 會轉換到下一個更新來源。

10. 儲存變更。

**如何在網頁主控台和雲端主控台中配置共用資料夾更新**

1. 在網頁主控台的主視窗中，選擇**資產（裝置）→工作**。

   工作清單開啟。

2. 點擊 Kaspersky Endpoint Security 的"**更新**"工作。

工作內容視窗將開啟。

*更新*工作由管理伺服器快速啟動精靈自動建立。要建立"*更新*"工作，請在執行精靈時安裝 Kaspersky Endpoint Security for Windows 管理外掛程式。

3. 選擇"**應用程式設定 → 本機模式**"標籤。
4. 在更新來源清單中，點擊"**新增**"按鈕。
5. 在開啟的視窗中，輸入共用資料夾的 UNC 路徑（例如 `\\<server name>\KLSHARE\Updates`）。

   來源位址必須與 Kaspersky 更新實用程式設定中指示的位址比對。

6. 點擊"**確定**"。
7. 使用"**上移**"和"**下移**"按鈕配置更新來源的優先順序。

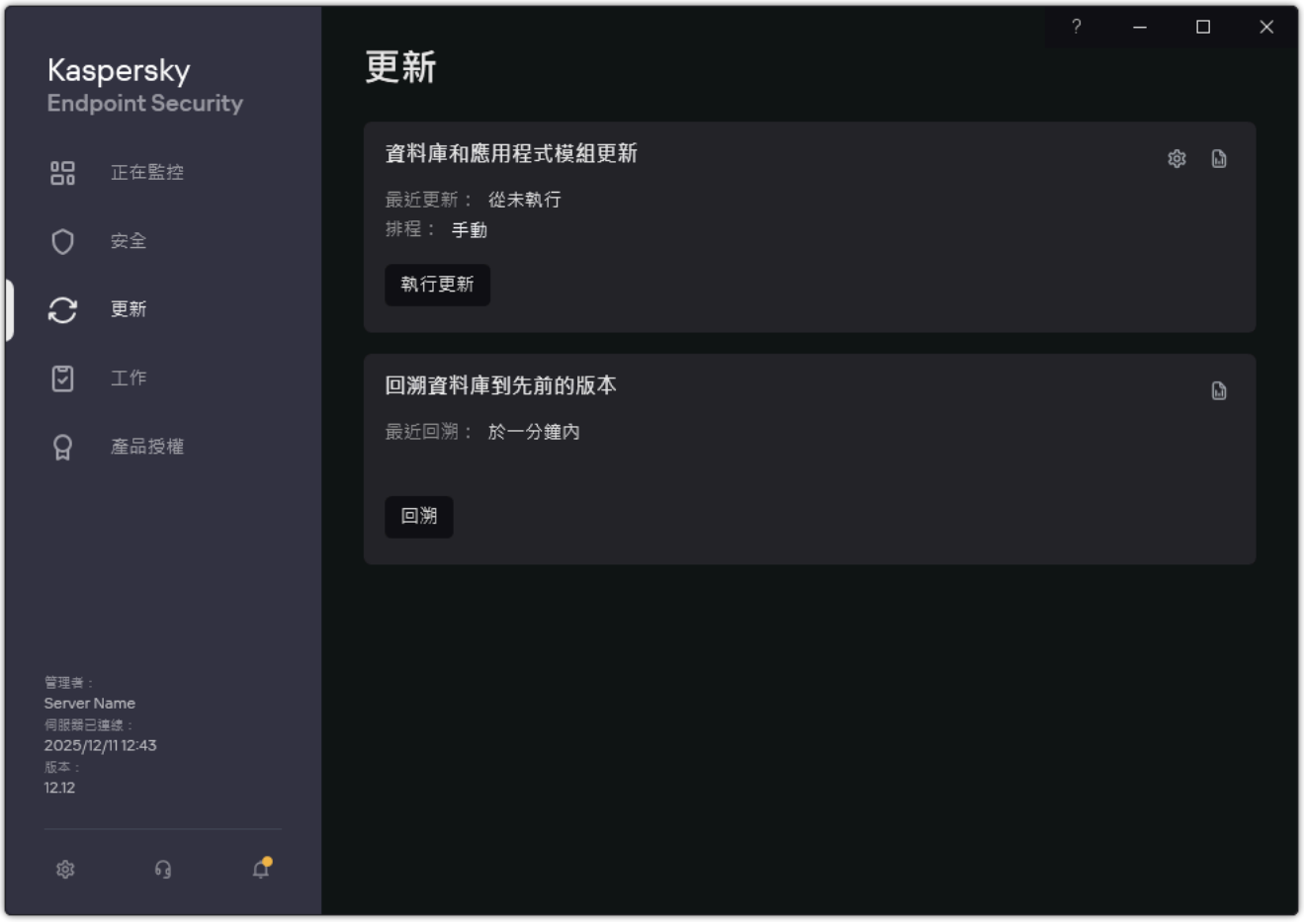
   如果無法從第一個更新來源執行更新，Kaspersky Endpoint Security 會轉換到下一個更新來源。

8. 儲存變更。

**如何在應用程式介面中設定共用資料夾更新**

您不能在應用程式介面中配置*資料庫和應用程式模組更新*群組工作。只有一個本機更新工作，*資料庫和應用程式模組更新*，可供使用者使用。如果*資料庫和應用程式模組更新*工作未顯示，則意味著管理員已在政策中禁止使用本機工作。

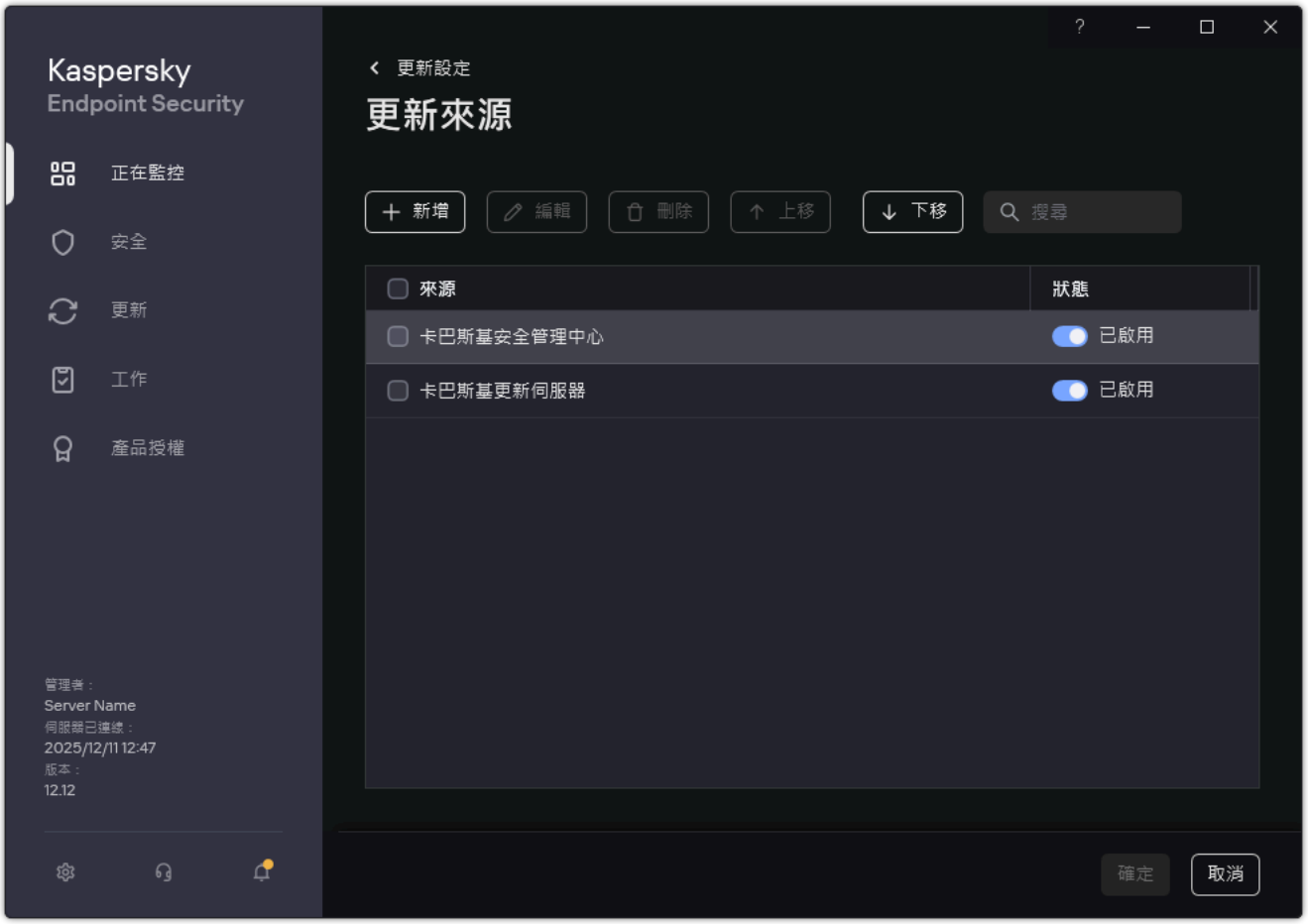
1. 在應用程式主視窗中，轉至"**更新**"區域。



2. 這將開啟工作清單；選擇*資料庫和應用程式模組更新*工作，然後點擊⚙。
   工作內容視窗將開啟。

3. 在工作內容視窗中，點擊**選擇更新來源**。

4. 在更新來源清單中，點擊**"新增"**按鈕。




更新來源

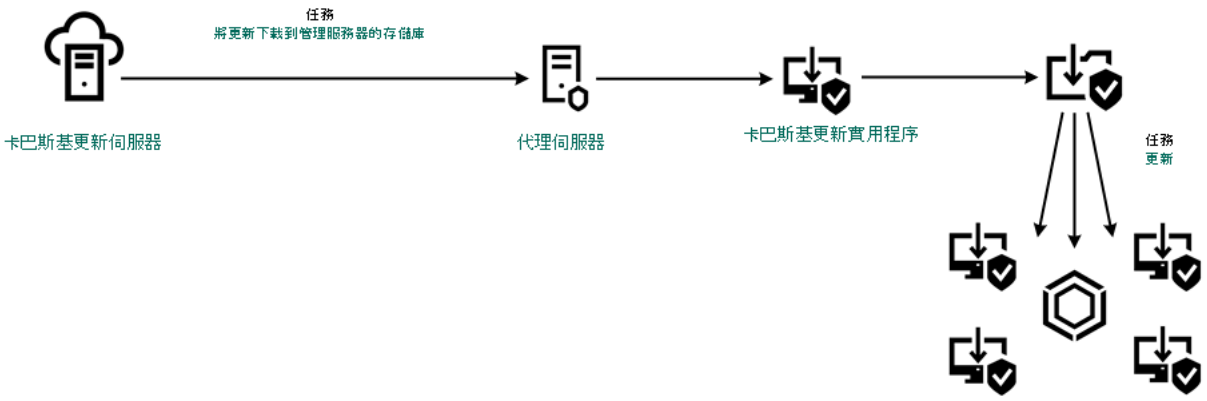
5. 輸入共用資料夾的 UNC 路徑（例如 `\\<server name>\KLSHARE\Updates`）。

   來源位址必須與 Kaspersky 更新實用程式設定中指示的位址比對。

6. 點擊**"選擇"**。

7. 使用**"上移"**和**"下移"**按鈕配置更新來源的優先順序。
   如果無法從第一個更新來源執行更新，Kaspersky Endpoint Security 會轉換到下一個更新來源。

8. 儲存變更。




使用 Kaspersky 更新實用程式更新

# 在行動模式下更新

*行動模式*是電腦離開組織網路周界（*離線電腦*）時 Kaspersky Endpoint Security 的執行模式。有關使用離線電腦以及與漫遊使用者一起工作的詳細資訊，請參閱卡巴斯基安全管理中心說明。

組織網路外部的離線電腦無法連線到管理伺服器來更新資料庫和應用程式模組。預設情況下，只有卡巴斯基更新伺服器用作行動模式下更新資料庫和應用程式模組的更新來源。是否使用代理伺服器連線到網際網路由特殊漫遊政策確定。漫遊政策必須單獨建立。當 Kaspersky Endpoint Security 切換到行動模式後，更新工作每兩小時啟動一次。

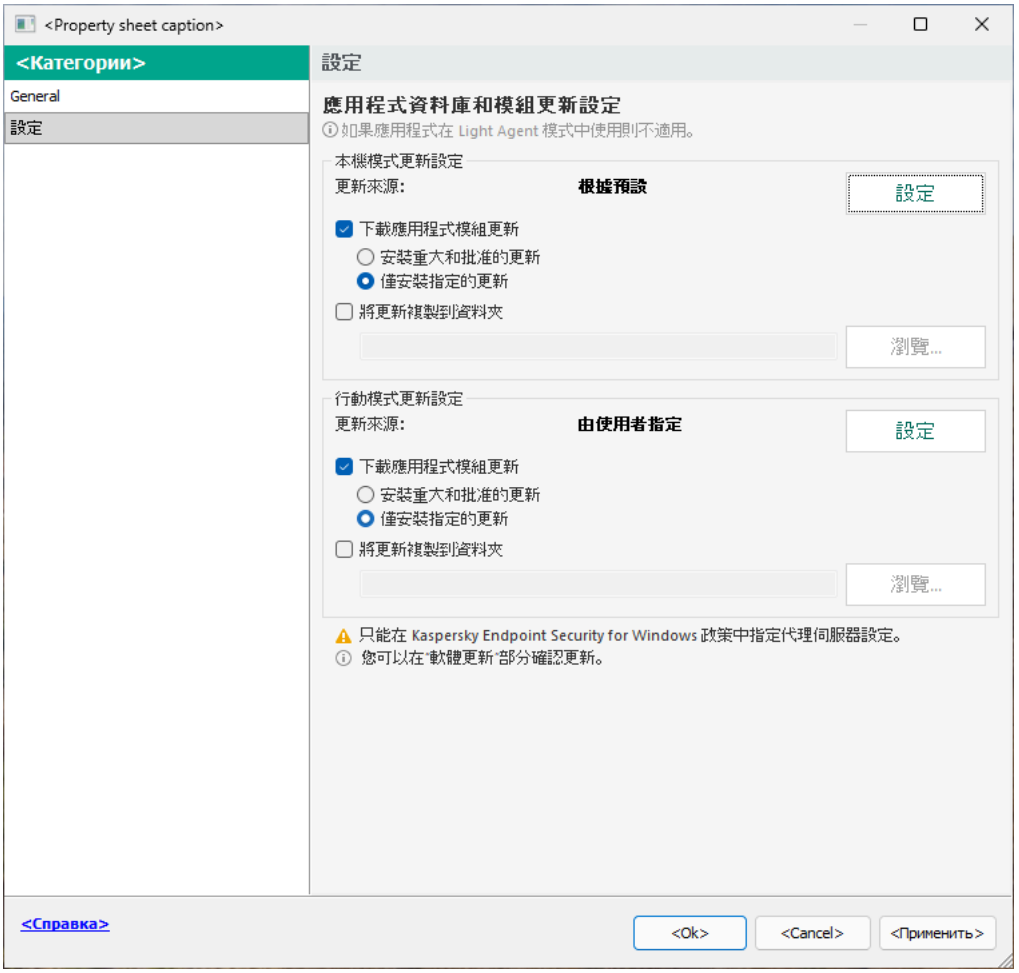
**如何在管理主控台 (MMC) 中設定行動模式的更新設定**

1. 開啟卡巴斯基安全管理中心管理主控台。
2. 在主控台樹狀目錄中，選擇“**工作**”。
3. 點擊 Kaspersky Endpoint Security 的“**資料庫和應用程式模組更新**”工作。

   工作內容視窗將開啟。

   *資料庫和應用程式模組更新*工作由管理伺服器快速啟動精靈自動建立。要建立“*資料庫和應用程式模組更新*”工作，請在執行精靈時安裝 Kaspersky Endpoint Security for Windows 管理外掛程式。

4. 在工作內容視窗中，選取“**設定**”區域。




資料庫和應用程式模組更新工作設定

5. 在”**行動模式更新設定**”塊中，點擊”**設定**”按鈕。

6. 配置更新來源。更新來源可以是卡巴斯基更新伺服器、其他 FTP 和 HTTP 伺服器、本機資料夾或網路資料夾。

7. 儲存變更。

### 如何在網頁主控台和雲端主控台中配置行動模式的更新設定

1. 在網頁主控台的主視窗中，選擇**資產（裝置）→工作**。

   工作清單開啟。

2. 點擊 Kaspersky Endpoint Security 的“**更新**”工作。

   工作內容視窗將開啟。

   *更新*工作由管理伺服器快速啟動精靈自動建立。要建立“*更新*”工作，請在執行精靈時安裝 Kaspersky Endpoint Security for Windows 管理外掛程式。

3. 選擇“**應用程式設定 → 行動模式**”標籤。

4. 配置更新來源。更新來源可以是卡巴斯基更新伺服器、其他 FTP 和 HTTP 伺服器、本機資料夾或網路資料夾。

5. 儲存變更。

結果，當使用者電腦切換到行動模式時，資料庫和應用程式模組將獲得更新。

# 開始和停止更新工作

無論選取的何種更新工作執行模式，您都可以隨時啟動或停止 Kaspersky Endpoint Security 更新工作。

*若要啟動或停止更新工作，請執行以下操作：*

1. 在應用程式主視窗中，轉至**"更新"**區域。
2. 如果要啟動更新工作，請在**"資料庫和應用程式模組更新"**塊中，點擊**"更新"**按鈕。

Kaspersky Endpoint Security 將啟動應用程式模組和資料庫的更新。該應用程式將顯示工作進度、下載檔案的大小以及更新來源。您可以隨時點擊**"停止更新"**按鈕來停止工作。

*要在顯示簡化的應用程式介面時啟動或停止更新工作：*

1. 在工作列通知區域按右鍵程式圖示，開啟內容功能表中。
2. 在內容功能表中的**"工作"**下拉清單中，執行以下操作之一：
   - 選擇未執行的更新工作以將其啟動
   - 選擇正在執行的更新工作以將其停止
   - 選擇暫停的更新工作以將其還原或重新啟動

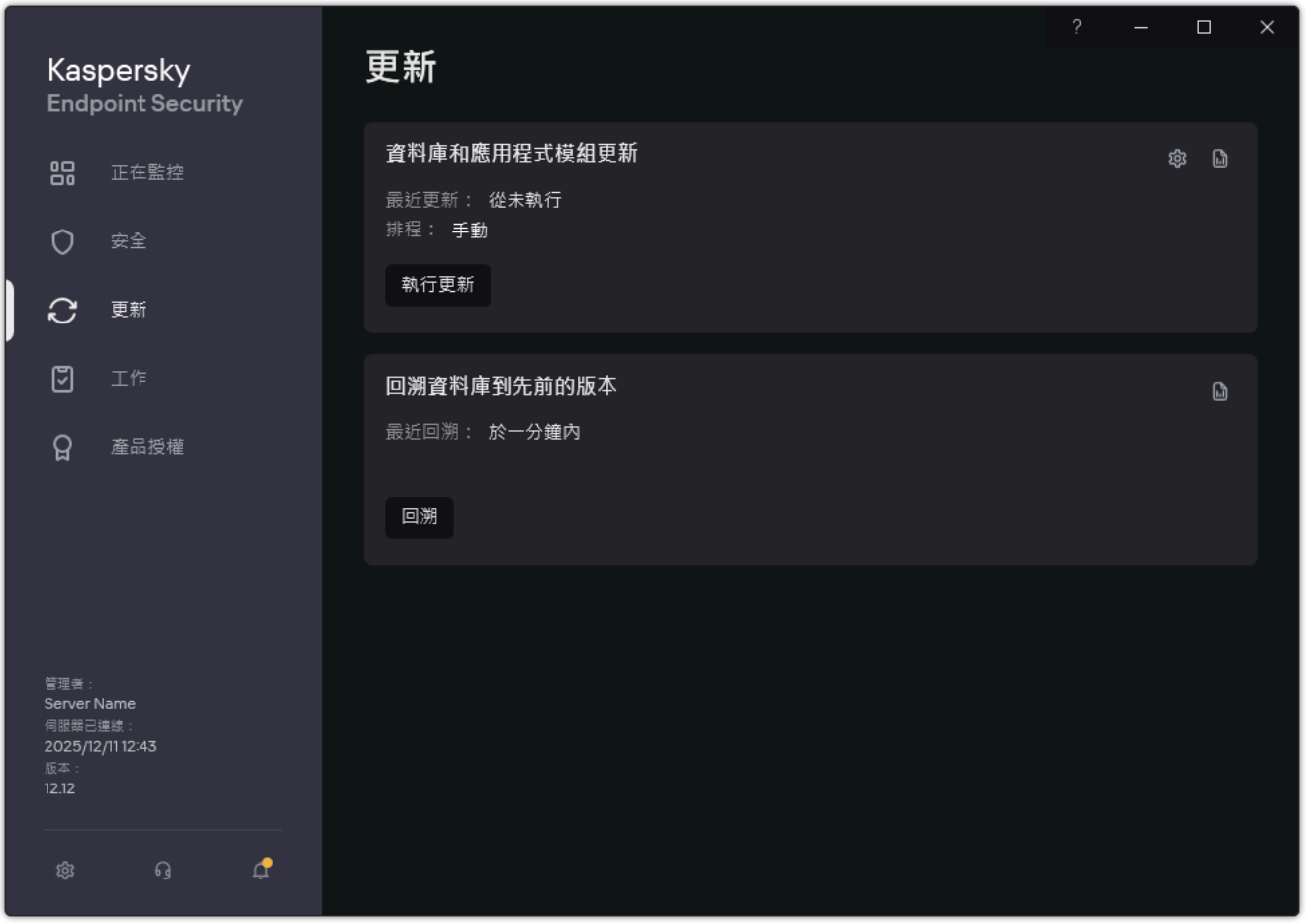
# 在不同使用者帳戶權限下開始更新工作

預設情況下，Kaspersky Endpoint Security 使用您用來登入作業系統的帳戶執行更新工作。但是，Kaspersky Endpoint Security 可以從使用者沒有存取權限的更新來源（例如，含有更新資料的共用資料夾）進行更新，或者從沒有設定過代理伺服器身分驗證的更新來源進行更新。在應用程式設定中，您可以指定一個擁有以上權限的使用者，然後使用此使用者帳戶開始 Kaspersky Endpoint Security 更新工作。

*若要使用不同的使用者帳戶開始更新工作，請執行以下操作：*

您不能在應用程式介面中配置*資料庫和應用程式模組更新*群組工作。只有一個本機更新工作，*資料庫和應用程式模組更新*，可供使用者使用。如果*資料庫和應用程式模組更新*工作未顯示，則意味著管理員已在政策中禁止使用本機工作。

1. 在應用程式主視窗中，轉至**"更新"**區域。




本機更新工作

2. 這將開啟工作清單；選擇*資料庫和應用程式模組更新*工作，然後點擊⚙。
   工作內容視窗將開啟。
3. 點擊**"以使用者權限執行資料庫更新"**。
4. 在開啟的視窗中選擇**"其他使用者"**。
5. 輸入具有存取更新來源所需權限的使用者的帳戶憑據。
6. 儲存變更。

# 選取更新工作執行模式

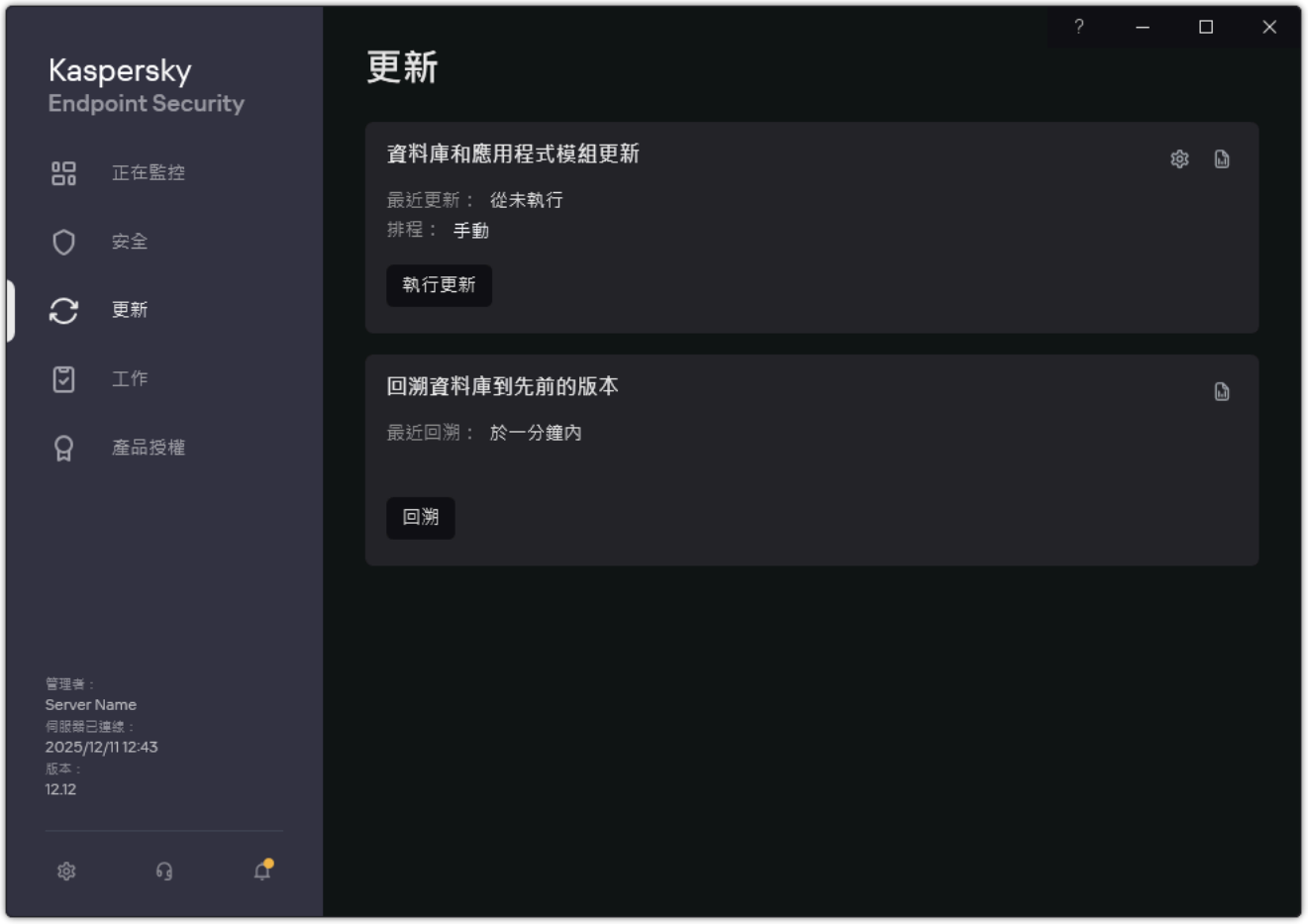
如果出於任何原因無法執行更新工作（例如，電腦當時沒有開啟），您可以設定錯過的工作在可能執行時立即自動開始。

如果您選取了**"依排程"**更新工作執行模式，而且 Kaspersky Endpoint Security 的啟動時間與更新工作啟動排程相符，您可以在程式啟動後延遲更新工作的執行。更新工作只能在 Kaspersky Endpoint Security 啟動後經過特定時間間隔後執行。

*若要選取更新工作執行模式，請執行以下操作：*

您不能在應用程式介面中配置*資料庫和應用程式模組更新*群組工作。只有一個本機更新工作，*資料庫和應用程式模組更新*，可供使用者使用。如果*資料庫和應用程式模組更新*工作未顯示，則意味著管理員已在政策中禁止使用本機工作。

1. 在應用程式主視窗中，轉至**"更新"**區域。




本機更新工作

2. 這將開啟工作清單；選擇*資料庫和應用程式模組更新*工作，然後點擊⚙。

   工作內容視窗將開啟。

3. 點擊**"執行模式"**。

4. 在開啟的視窗中，選擇更新工作執行模式：

   - 如果您希望 Kaspersky Endpoint Security 根據是否能夠從更新來源獲得更新資料來執行更新工作，請選取**"自動"**。Kaspersky Endpoint Security 檢查更新資料的頻率在病毒爆發時會新增，在其他時候會減少。
   - 如果您希望手動開始更新工作，請選取**"手動"**。

- 如果您希望為執行更新工作設定一個排程，請選取其它選項。設定用於啟動更新工作的進階設定：
  - 在"**應用程式啟動後延遲執行時間 N 分鐘**"欄位中，輸入您希望在 Kaspersky Endpoint Security 啟動後延遲啟動更新工作的時間間隔。
  - 如果您希望 Kaspersky Endpoint Security 在第一機會執行錯過的更新工作，請選擇"**電腦關閉時，在隔天執行排程掃描**"。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。

5. 儲存變更。

# 新增更新來源

*更新來源*是包含 Kaspersky Endpoint Security 的資料庫和程式模組更新的資源。

更新來源包括卡巴斯基安全管理中心、卡巴斯基更新伺服器、以及網路或本機資料夾。

更新來源的預設清單包括了卡巴斯基安全管理中心和卡巴斯基更新伺服器。您可以在清單中新增其他更新來源。您可以指定 HTTP/FTP 伺服器和共用資料夾作為更新來源。

除非它們是卡巴斯基的更新伺服器，否則 Kaspersky Endpoint Security 不支援來自 HTTPS 伺服器的更新。

如果選取了多個來源作為更新來源，Kaspersky Endpoint Security 將嘗試從清單頂端開始依次連接，使用從第一個可用源檢索到的更新資料執行更新工作。

預設情況下，Kaspersky Endpoint Security 使用卡巴斯基安全管理中心伺服器作為第一個更新來源。這有助於在更新時節省流量。如果政策未被套用到電腦，卡巴斯基伺服器將被選為*資料庫和應用程式模組更新*本機工作設定中的第一個更新來源，因為應用程式可能無法存取卡巴斯基安全管理中心伺服器。

如果應用程式在 Light Agent 模式下執行， SVM 上的一個資料夾將被選為更新來源。

### 如何在管理主控台 (MMC) 中新增更新來源

1. 開啟卡巴斯基安全管理中心管理主控台。

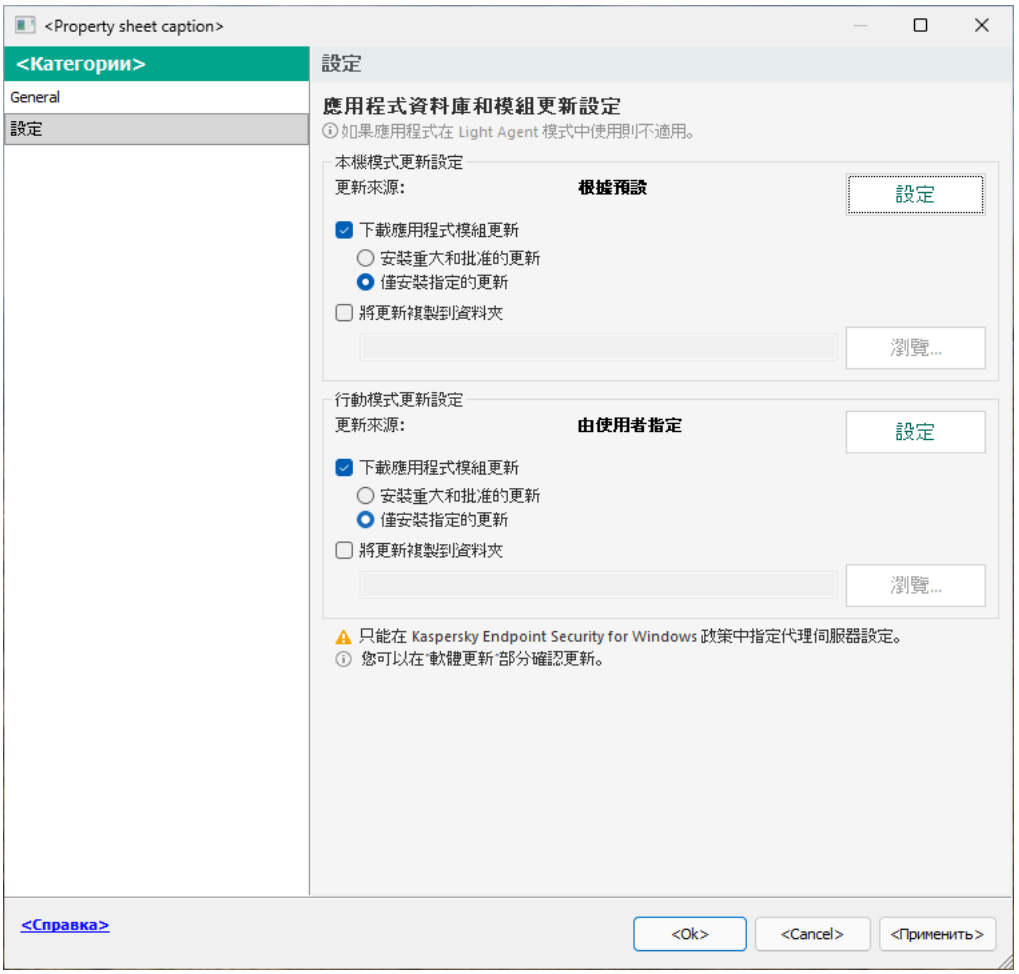
   在主控台樹狀目錄中，選擇"**工作**"。

2. 點擊 Kaspersky Endpoint Security 的"**資料庫和應用程式模組更新**"工作。

   工作內容視窗將開啟。

   *資料庫和應用程式模組更新*工作由管理伺服器快速啟動精靈自動建立。要建立"*資料庫和應用程式模組更新*"工作，請在執行精靈時安裝 Kaspersky Endpoint Security for Windows 管理外掛程式。

3. 在工作內容視窗中，選取“**設定**”區域。




資料庫和應用程式模組更新工作設定

4. 在”**本機模式更新設定**”塊中，點擊”**設定**”按鈕。




更新來源

5. 在更新來源清單中，點擊“**新增**”按鈕。

6. 在**更新來源**欄位中，指定包含更新套件的 FTP 或 HTTP 伺服器、網路資料夾或本機資料夾的位址。

   更新來源使用以下路徑格式：

   - 對於 FTP 或 HTTP 伺服器，請輸入它的網址或 IP 位址。

例如，`http://dnl-01.geo.kaspersky.com/` 或 `93.191.13.103`。

對於 FTP 伺服器，可以用以下格式在位址內指定身分驗證設定：`ftp://<user name>:<password>@<node>:<port>`。

- 對於網路資料夾，輸入 UNC 路徑。

  例如，`\\Server\Share\Update distribution`。

- 對於本機資料夾，輸入此資料夾的完整路徑。

  例如，`C:\Documents and Settings\All Users\Application Data\Kaspersky Lab\AVP12\Update distribution\`。

您可以排除更新來源而不將其從更新來源清單中刪除。為此，請清除物件旁邊的核取方塊。

7. 點擊**"確定"**。
8. 使用**"上移"**和**"下移"**按鈕配置更新來源的優先順序。

   如果無法從第一個更新來源執行更新，Kaspersky Endpoint Security 會轉換到下一個更新來源。
9. 如有需要，為行動模式新增更新來源。*行動模式*是電腦離開組織網路周界（*離線電腦*）時 Kaspersky Endpoint Security 的執行模式。
10. 儲存變更。

**如何在網頁主控台和雲端主控台中新增更新來源**

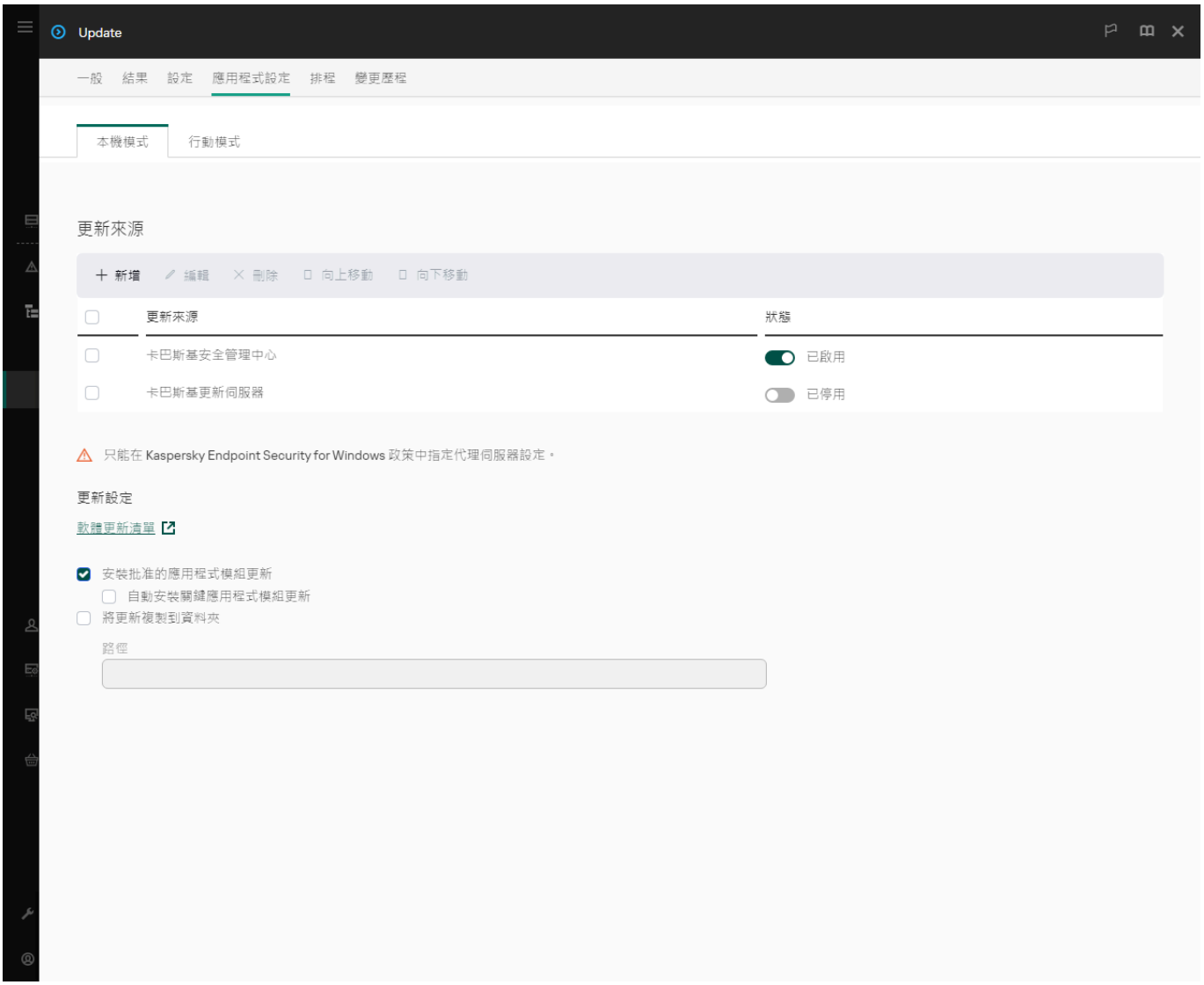
1. 在網頁主控台的主視窗中，選擇**資產（裝置）→工作**。

   工作清單開啟。
2. 點擊 Kaspersky Endpoint Security 的**"更新"**工作。

   工作內容視窗將開啟。

   *更新*工作由管理伺服器快速啟動精靈自動建立。要建立*"更新"*工作，請在執行精靈時安裝 Kaspersky Endpoint Security for Windows 管理外掛程式。

3. 選擇“**應用程式設定 → 本機模式**”標籤。




更新來源

4. 在更新來源清單中，點擊“**新增**”按鈕。

5. 在開啟的視窗中，指定包含更新套件的 FTP 或 HTTP 伺服器、網路資料夾或本機資料夾的位址。
   更新來源使用以下路徑格式：

   - 對於 FTP 或 HTTP 伺服器，請輸入它的網址或 IP 位址。
     例如，`http://dnl-01.geo.kaspersky.com/` 或 `93.191.13.103`。
     對於 FTP 伺服器，可以用以下格式在位址內指定身分驗證設定：`ftp://<user name>:<password>@<node>:<port>`。
   - 對於網路資料夾，輸入 UNC 路徑。
     例如，`\\Server\Share\Update distribution`。
   - 對於本機資料夾，輸入此資料夾的完整路徑。
     例如，`C:\Documents and Settings\All Users\Application Data\Kaspersky Lab\AVP12\Update distribution\`。

   您可以排除更新來源而不將其從更新來源清單中刪除。為此，將它旁邊的切換開關設為關閉位置。

6. 點擊“**確定**”。

7. 使用“**上**”和“**下**”按鈕配置更新來源的優先順序。

   如果無法從第一個更新來源執行更新，Kaspersky Endpoint Security 會轉換到下一個更新來源。

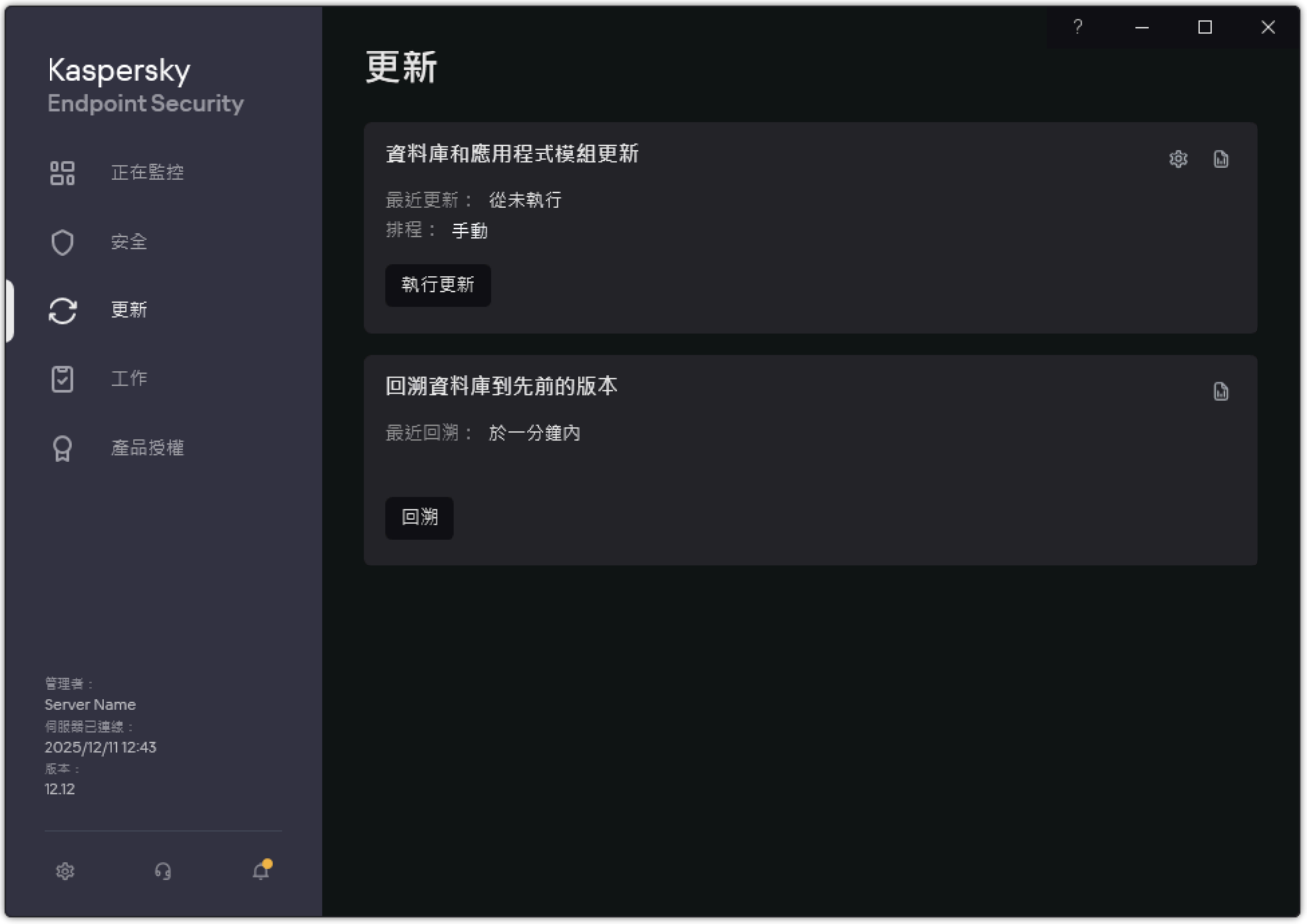
8. 如有需要，為行動模式新增更新來源。*行動模式*是電腦離開組織網路周界（*離線電腦*）時 Kaspersky Endpoint Security 的執行模式。

9. 儲存變更。

**如何在應用程式介面中新增更新來源**

您不能在應用程式介面中配置*資料庫和應用程式模組更新*群組工作。只有一個本機更新工作，*資料庫和應用程式模組更新*，可供使用者使用。如果*資料庫和應用程式模組更新*工作未顯示，則意味著管理員已在政策中禁止使用本機工作。

1. 在應用程式主視窗中，轉至“**更新**”區域。



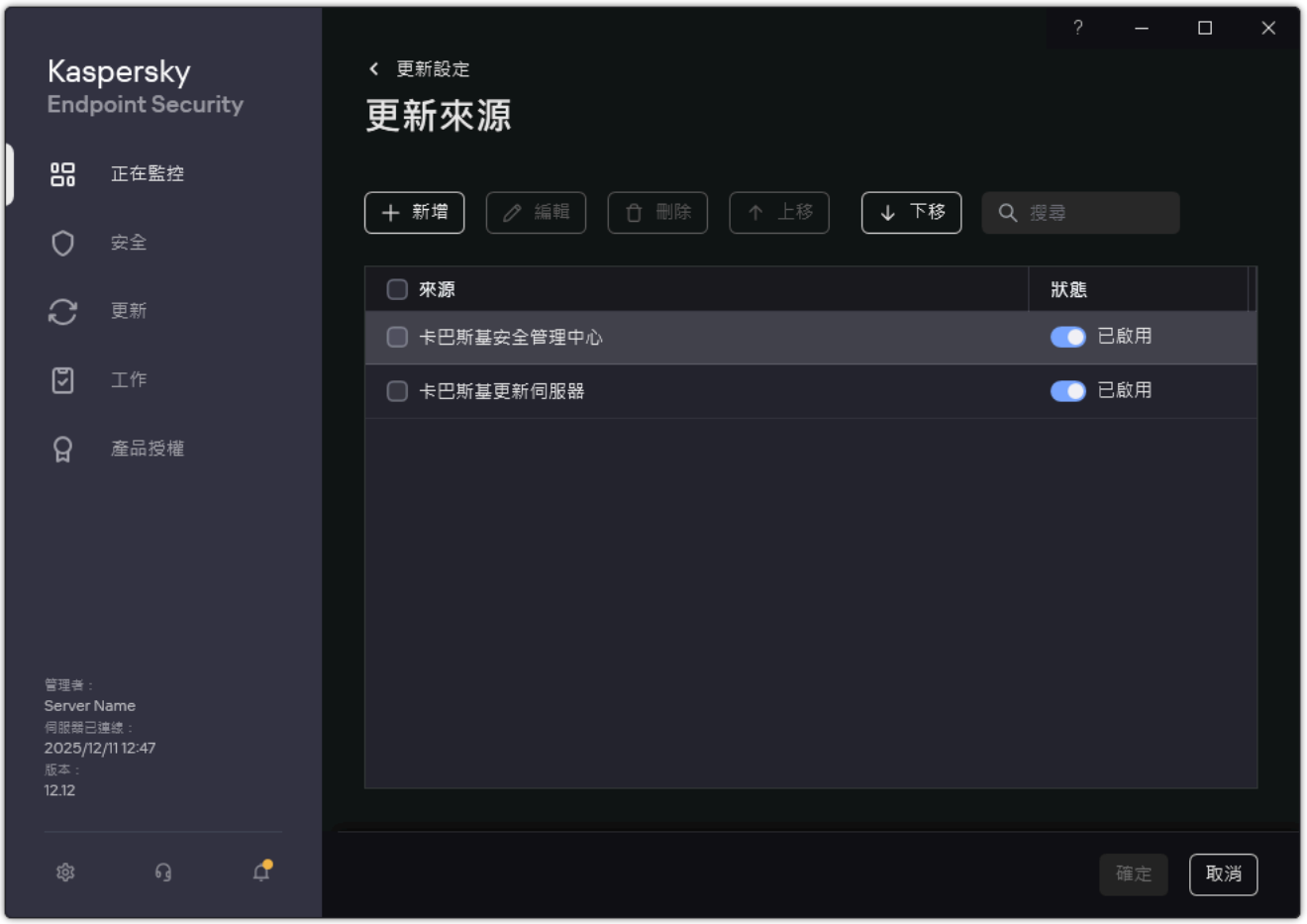

本機更新工作

2. 這將開啟工作清單；選擇*資料庫和應用程式模組更新*工作，然後點擊⚙。

   工作內容視窗將開啟。

3. 點擊“**選擇更新來源**”。

4. 在開啟的視窗中，點擊“**新增**”按鈕。




更新來源

5. 在開啟的視窗中，指定包含更新套件的 FTP 或 HTTP 伺服器、網路資料夾或本機資料夾的位址。

   更新來源使用以下路徑格式：

   - 對於 FTP 或 HTTP 伺服器，請輸入它的網址或 IP 位址。

     例如，`http://dnl-01.geo.kaspersky.com/` 或 `93.191.13.103`。

     對於 FTP 伺服器，可以用以下格式在位址內指定身分驗證設定：`ftp://<user name>:<password>@<node>:<port>`。

   - 對於網路資料夾，輸入 UNC 路徑。

     例如，`\\Server\Share\Update distribution`。

   - 對於本機資料夾，輸入此資料夾的完整路徑。

     例如，`C:\Documents and Settings\All Users\Application Data\Kaspersky Lab\AVP12\Update distribution\`。

6. 點擊“**選擇**”。

7. 使用“**上移**”和“**下移**”按鈕配置更新來源的優先順序。

8. 儲存變更。

# 更新應用程式模組

應用程式模組更新可修復錯誤、提高效能並新增新功能。當有新的應用程式模組更新可用時，您需要確認更新的安裝。您可以在應用程式介面或卡巴斯基安全管理中心中確認安裝了應用程式模組更新。每當有更新可以使用時，應用程式就會在 Kaspersky Endpoint Security 的主視窗中顯示通知：。如果應用程式模組更新需要檢視和接受最終使用者產品授權協議，應用程式將在最終使用者產品授權協議被接受後，安裝更新。

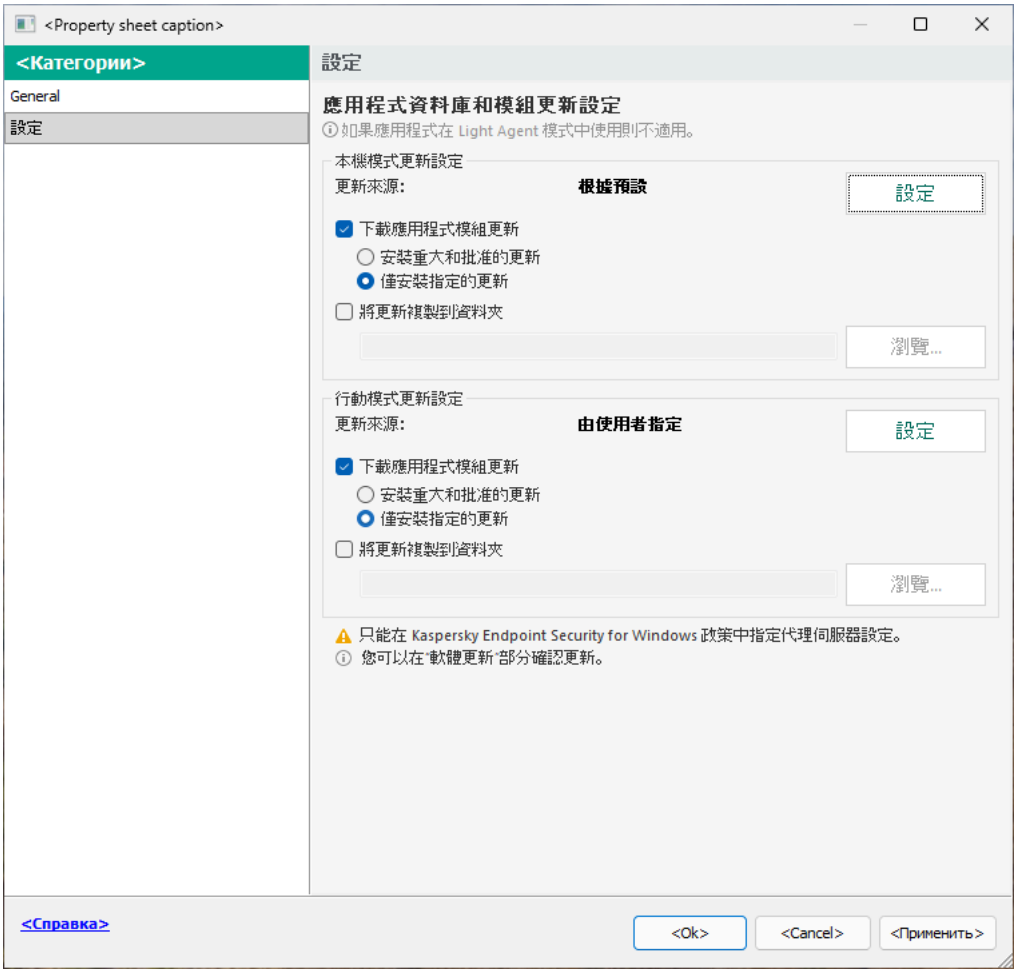
安裝應用程式更新後，您可能需要重新啟動電腦。

### 如何在管理主控台 (MMC) 中設定應用程式模組更新

1. 開啟卡巴斯基安全管理中心管理主控台。
2. 在主控台樹狀目錄中，選擇“**工作**”。
3. 點擊 Kaspersky Endpoint Security 的“**資料庫和應用程式模組更新**”工作。

   工作內容視窗將開啟。

   *資料庫和應用程式模組更新*工作由管理伺服器快速啟動精靈自動建立。要建立“*資料庫和應用程式模組更新*”工作，請在執行精靈時安裝 Kaspersky Endpoint Security for Windows 管理外掛程式。
4. 在工作內容視窗中，選取“**設定**”區域。




資料庫和應用程式模組更新工作設定

5. 在“**本機模式更新設定**“塊中，選中“**下載應用程式模組更新**”核取方塊。

   如果您想阻止下載應用程式模組更新，請清除 **下載應用程式模組更新** 核取方塊並禁止使用者使用本機工作。

6. 請選取您要安裝的應用程式模組更新。

   - **安裝重大和批准的更新**如果選擇此選項，當有應用程式模組更新可用時，僅在這些更新透過應用程式介面或在卡巴斯基安全管理中心一側被本機批准後，Kaspersky Endpoint Security 才會自動安裝關鍵更新和所有其他應用程式模組更新。

   - **僅安裝指定的更新**如果選擇此選項，當有應用程式模組更新可用時，僅在這些更新透過應用程式介面或在卡巴斯基安全管理中心一側被本機批准後，Kaspersky Endpoint Security 才會安裝它們。預設情況下已勾選此選項。

7. 如果有需要的話，配置行動模式的應用程式模組更新。*行動模式*是電腦離開組織網路周界（*離線電腦*）時 Kaspersky Endpoint Security 的執行模式。

8. 儲存變更。

**如何在網頁主控台和雲端主控台中配置應用程式模組更新**

1. 在網頁主控台的主視窗中，選擇**資產（裝置）→ 工作**。

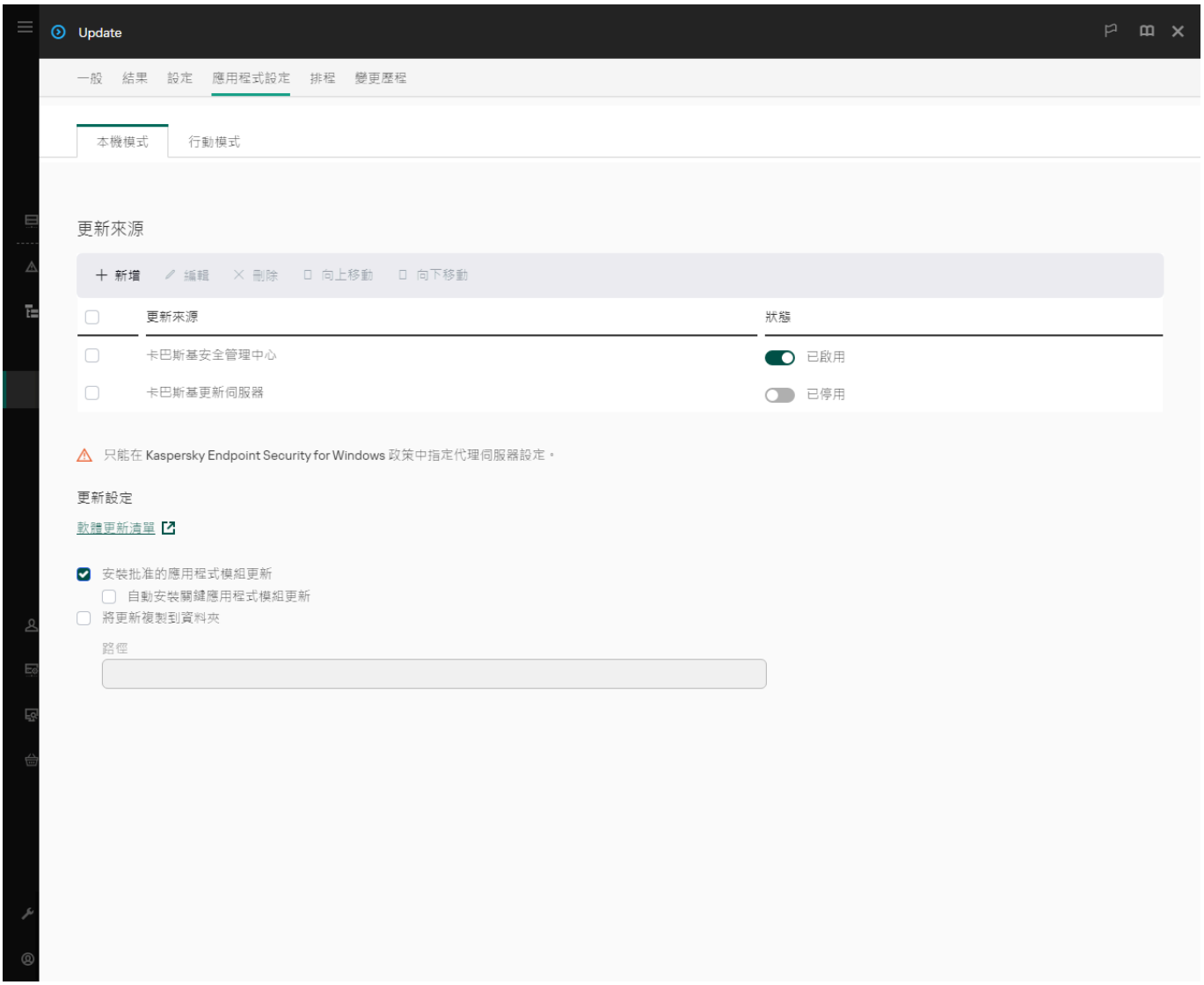
   工作清單開啟。

2. 點擊 Kaspersky Endpoint Security 的“**資料庫和應用程式模組更新**”工作。

   工作內容視窗將開啟。

   *資料庫和應用程式模組更新*工作由管理伺服器快速啟動精靈自動建立。要建立“*資料庫和應用程式模組更新*”工作，請在執行精靈時安裝 Kaspersky Endpoint Security for Windows 管理外掛程式。

3. 選擇"**應用程式設定 → 本機模式**"標籤。




更新工作設定

4. 在**更新設定**下面，選取您要安裝的應用程式模組更新：

   - **安裝批准的應用程式模組更新**如果選擇此選項，當有應用程式模組更新可用時，僅在這些更新透過應用程式介面或在卡巴斯基安全管理中心一側被本機批准後，Kaspersky Endpoint Security 才會安裝它們。預設情況下已勾選此選項。

   - **自動安裝關鍵應用程式模組更新**如果選擇此選項，當有應用程式模組更新可用時，僅在這些更新透過應用程式介面或在卡巴斯基安全管理中心一側被本機批准後，Kaspersky Endpoint Security 才會自動安裝關鍵更新和所有其他應用程式模組更新。

   如果您想阻止下載應用程式模組更新，請清除**安裝批准的應用程式模組更新**和**自動安裝關鍵應用程式模組更新**核取方塊並禁止使用者使用本機工作。

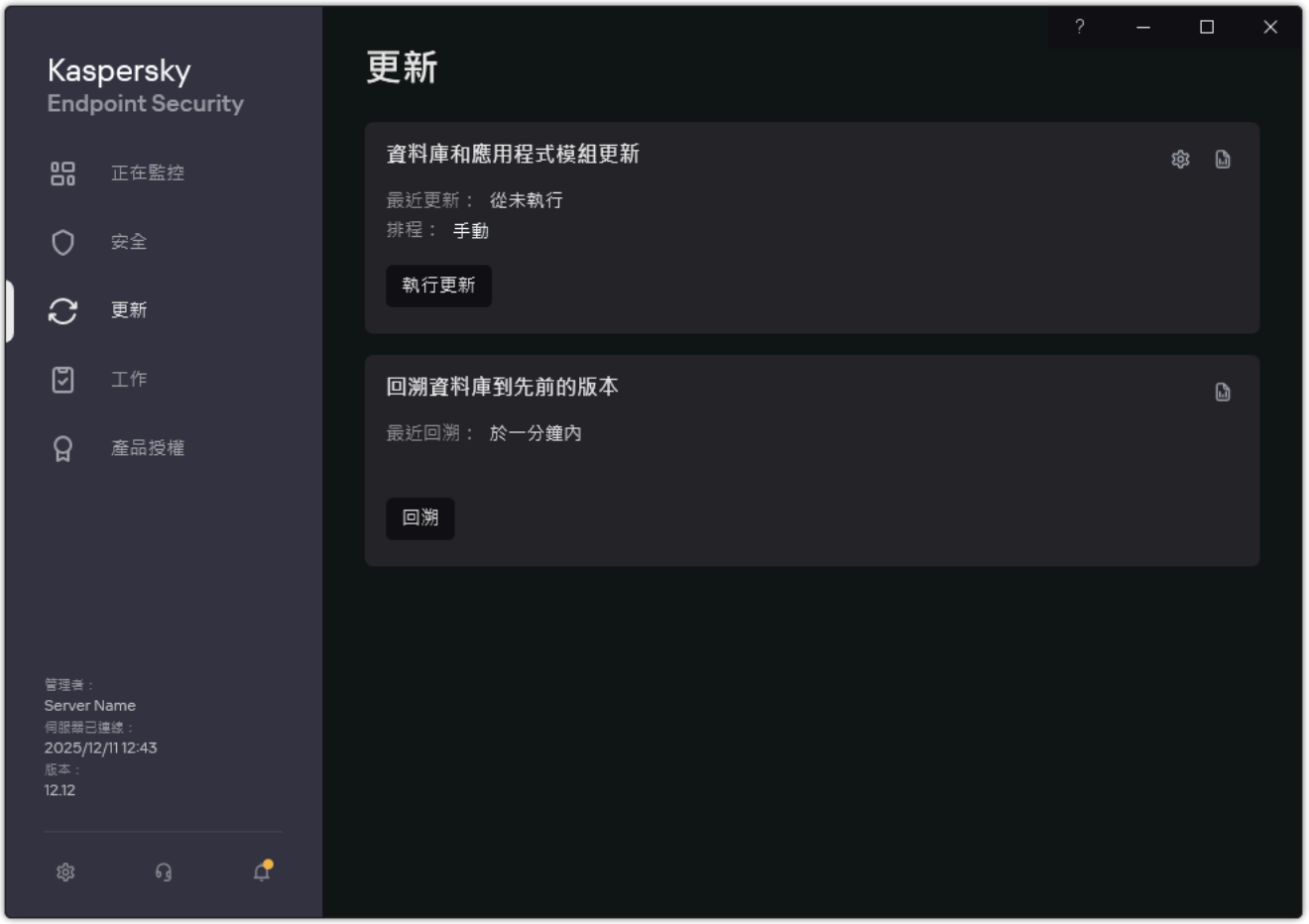
5. 如果有需要的話，配置行動模式的應用程式模組更新。*行動模式*是電腦離開組織網路周界（*離線電腦*）時 Kaspersky Endpoint Security 的執行模式。

6. 儲存變更。

### 如何在應用程式介面中設定應用程式模組更新

您不能在應用程式介面中配置*資料庫和應用程式模組更新*群組工作。只有一個本機更新工作，*資料庫和應用程式模組更新*，可供使用者使用。如果*資料庫和應用程式模組更新*工作未顯示，則意味著管理員已在政策中禁止使用本機工作。

1. 在應用程式主視窗中，轉至**"更新"**區域。




本機更新工作

2. 這將開啟工作清單；選擇*資料庫和應用程式模組更新*工作，然後點擊⚙。

   工作內容視窗將開啟。

3. 在**"下載和安裝應用程式模組更新"**塊中，選中**"下載應用程式模組更新"**核取方塊。

4. 請選取您要安裝的應用程式模組更新。

   - **安裝重大和指定的更新**如果選擇此選項，當有應用程式模組更新可用時，僅在這些更新透過應用程式介面或在卡巴斯基安全管理中心一側被本機批准後，Kaspersky Endpoint Security 才會自動安裝關鍵更新和所有其他應用程式模組更新。

   - **僅安裝指定的更新**如果選擇此選項，當有應用程式模組更新可用時，僅在這些更新透過應用程式介面或在卡巴斯基安全管理中心一側被本機批准後，Kaspersky Endpoint Security 才會安裝它們。預設情況下已勾選此選項。

5. 儲存變更。

# 使用代理伺服器進行更新

您可能需要指定代理伺服器設定才能從更新來源下載資料庫和應用程式模組更新。如果有多個更新來源，代理伺服器設定將適用於所有來源。如果某些更新來源不需要代理伺服器，可以在政策內容中停用代理伺服器。Kaspersky Endpoint Security 還將使用代理伺服器存取卡巴斯基安全網路和啟動伺服器。

*要配置透過代理伺服器連線到更新來源：*

1. 在網頁主控台的主視窗中點擊 ⚙。
   "管理伺服器"內容視窗將開啟。
2. 轉到"**設定網際網路存取**"區域。
3. 選擇"**使用代理伺服器**"核取方塊。
4. 配置代理伺服器連線設定：代理伺服器位址、連接埠和身分驗證設定（使用者名稱和密碼）。
5. 儲存變更。

*要對特定管理群組禁止使用代理伺服器：*

1. 在網頁主控台的主視窗中，選擇**資產（裝置）→政策和設定檔**。
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**"塊中，點擊"**設定**"按鈕。
6. 在開啟的視窗中，選中"**本機位址略過代理伺服器**"核取方塊。
7. 儲存變更。

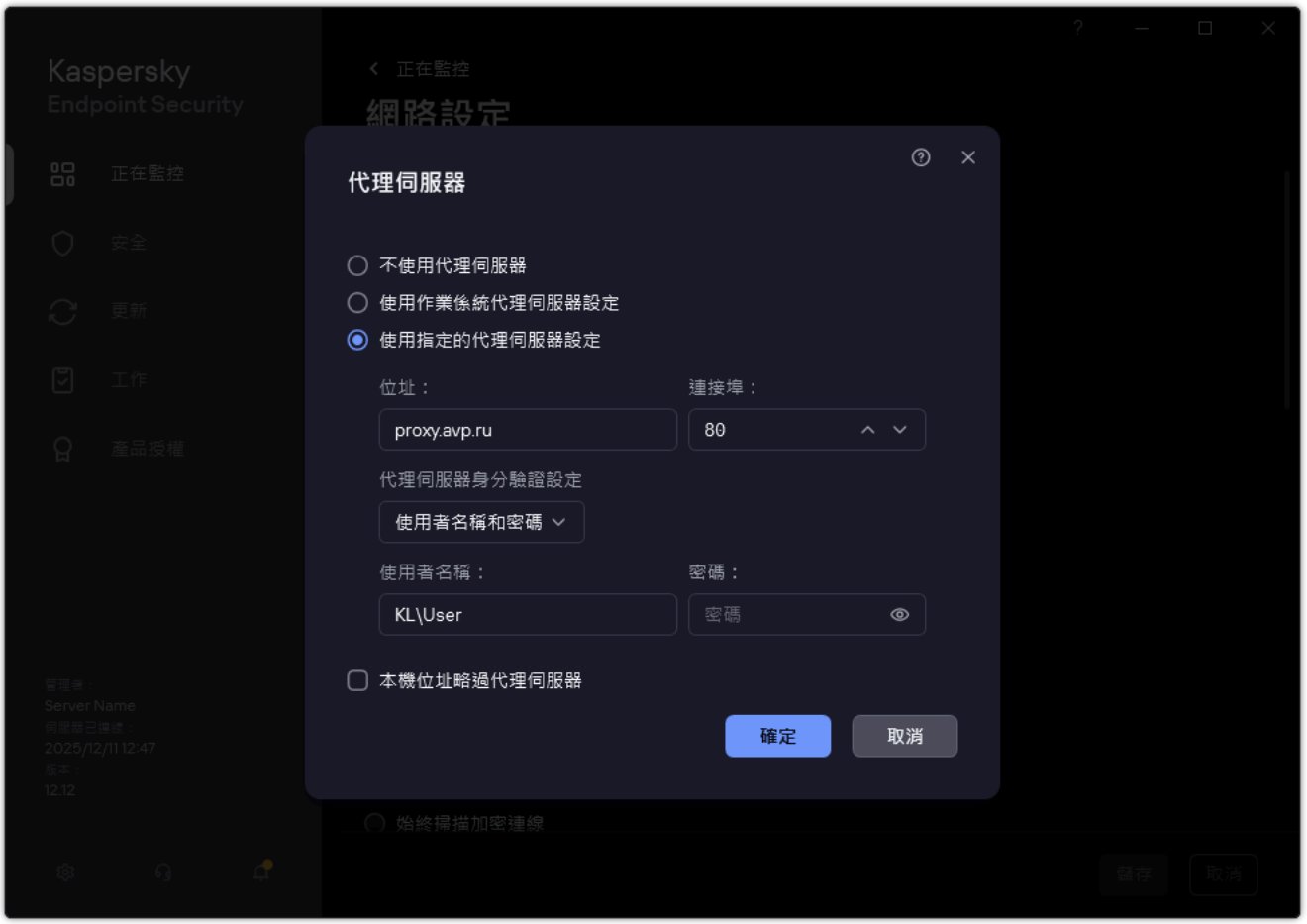
*要在應用程式介面中配置代理伺服器設定，請：*

1. 在“應用程式主視窗”中，點擊⚙按鈕。
2. 在應用程式設定視窗中，選取”**一般設定**“→“**網路設定**”。




應用程式網路設定

3. 在"**代理伺服器**"塊中，點擊"**代理伺服器設定**"連接。




代理伺服器連線設定

4. 在開啟的視窗中，選擇以下選項之一以確定代理伺服器位址：

   - **使用作業係統代理伺服器設定**

     預設情況下已勾選此選項。Kaspersky Endpoint Security 使用作業系統設定中定義的代理伺服器設定。

   - **使用指定的代理伺服器設定**

     如果選擇此選項，請配置用於連線到代理伺服器的設定：代理伺服器位址和連接埠。

5. 選擇您希望應用程式如何在代理伺服器上進行身分驗證。預設情況下，應用程式使用目前使用者的網域 NTLM 身分驗證。

6. 如果您希望在從共用資料夾更新資料庫和應用程式模組時停用代理伺服器，請選中"**本機位址略過代理伺服器**"核取方塊。

7. 儲存變更。

因此，Kaspersky Endpoint Security 將使用代理伺服器下載應用程式模組和資料庫更新。Kaspersky Endpoint Security 還將使用代理伺服器存取 KSN 伺服器和卡巴斯基啟動伺服器。如果代理伺服器上要求進行身分驗證，但未提供使用者帳戶憑據或憑據不正確，Kaspersky Endpoint Security 將提示您輸入使用者名稱和密碼。

# 最近更新還原

在資料庫和程式模組進行第一次更新以後，就能夠將資料庫和程式模組回溯至前一版本的功能。

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，當新資料庫版本包含一個無效的簽章而導致 Kaspersky Endpoint Security 封鎖某個安全的應用程式時，回溯操作就會十分有用。

Light Agent 模式下的 Kaspersky Endpoint Security 不支援 *更新回溯* 工作。

**如何在管理主控台 (MMC) 中回溯上次更新**

1. 在卡巴斯基安全管理中心管理主控台樹狀目錄中，選取**工作**。

   工作清單開啟。

2. 點擊**"新工作"**。

啟動"工作精靈"。按照精靈的說明進行操作。

步驟 1. 選取工作類型

1. 選取**"Kaspersky Endpoint Security for Windows (12.12)"→"更新回溯"**。

步驟 2. 選取將要對其分配工作的裝置

選取將要執行工作的電腦。下列選項可用：

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

步驟 3. 設定工作啟動排程

設定工作排程，例如手動。

步驟 4. 定義工作名稱

輸入工作的名稱。

步驟 7. 完成工作建立

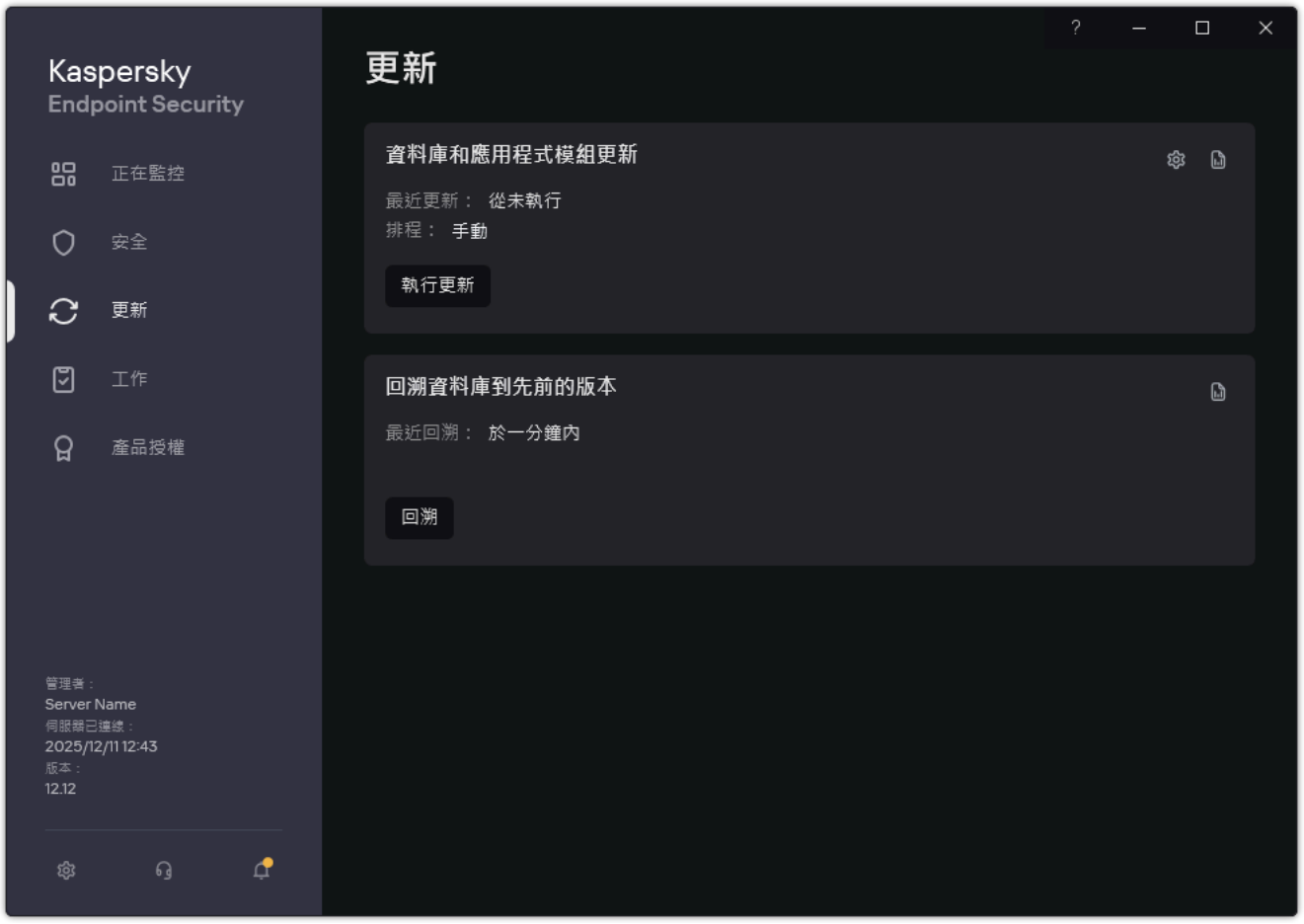
結束精靈。如有必要，選中**"精靈完成時執行工作"**核取方塊。您可以在工作內容中監控工作進度。

**如何在網頁主控台中回溯上次更新**

1. 在網頁主控台的主視窗中，選擇**資產（裝置）→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 Windows 12.12.0"**。
   b. 在**"工作類型"**下拉式清單中，選取**"更新回溯"**。
   c. 在**"工作名稱"**欄位中，輸入簡要說明，例如"*更新回溯*"。
   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。前往下一步。
5. 選取要執行工作的帳戶。預設情況下，Kaspersky Endpoint Security 將使用本機使用者帳戶的權限啟動工作。
6. 結束精靈。
7. 在工作清單中將顯示一個新工作。
8. 選中該工作旁邊的核取方塊。
9. 點擊**"開始"**。

### 如何在應用程式介面中回溯上次更新

1. 在應用程式主視窗中，轉至“**更新**”區域。




本機更新工作

2. 在“**回溯資料庫到先前的版本**“塊中，點擊“**回溯**”按鈕。

Kaspersky Endpoint Security 將開始回溯上一次資料庫更新。應用程式將顯示回溯進度、下載檔案的大小以及更新來源。您可以隨時點擊“**停止更新**“按鈕來停止工作。

# 進階解毒技術

為了處理活動威脅，Kaspersky Endpoint Security 使用了進階解毒技術。進階解毒的工作方式對工作站和伺服器不同。您可以在*惡意軟體掃描*工作設定和應用程式設定中配置進階解毒。

如果 Kaspersky Endpoint Security 無法停止惡意軟體的執行，您可以使用進階解毒技術。對於受政策約束的電腦，預設情況下會停用進階解毒，因為該技術會使用大量電腦資源。 對於不受政策約束的電腦，預設情況下會啟用進階解毒。

進階解毒的工作方式對工作站和伺服器不同。若要在伺服器上使用該技術，您必須在"*惡意軟體掃描*"工作的屬性中啟用立即使用進階解毒。在工作站上使用該技術不需要此先決條件。

**如何在管理主控台（MMC）中啟用或停用進階解毒技術**

1. 在卡巴斯基安全管理中心管理主控台樹狀目錄中，選取**政策**。
2. 選擇必要的政策並點擊以開啟政策內容。
3. 在政策視窗中，選擇"**一般設定 → 應用程式設定**"。
4. 在"**一般**"塊中，選擇或者清除"**啟用進階解毒技術**"核取方塊來啟用或停用進階解毒技術。
5. 儲存變更。

**如何在網頁主控台和雲端主控台中啟用或停用進階解毒技術**

1. 在網頁主控台的主視窗中，選擇**資產（裝置）→ 政策和設定檔**。
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"**一般設定 → 偵測設定**"。
5. 在"**進階解毒技術**"塊中，開啟或者關閉"**進階解毒技術已啟用**"切換開關來啟用或停用進階解毒技術。
6. 儲存變更。

**如何在應用程式介面中啟用或停用進階解毒技術**

1. 在“應用程式主視窗”中，點擊⚙按鈕。
2. 在應用程式設定視窗中，選取”**一般設定**“→“**應用程式設定**”。




Kaspersky Endpoint Security for Windows 設定

3. 在“**一般**”塊中，選擇或者清除“**使用進階解毒技術（需要大量電腦資源）**“核取方塊來啟用或停用進階解毒技術。
4. 儲存變更。

結果，進階解毒進行時使用者不能使用大多數作業系統功能。解毒完成時，電腦將重啟。

# 在工作站上解毒活動威脅

若要在工作站上處理活動威脅，請在應用程式設定中啟用進階解毒技術。接下來，請在"*惡意軟體掃描*"工作屬性中配置使用者經驗。工作內容中有一個"**立即執行進階解毒技術**"核取方塊。如果設定了該標記，Kaspersky Endpoint Security 將不通知使用者就執行解毒。解毒完成時，電腦將重啟。如果未設定該標記，Kaspersky Endpoint Security 將顯示活動威脅通知（請參見下圖）。未處理檔案，不可關閉此通知。

僅當在套用於電腦的政策的內容中啟用"進階解毒"功能後，才會在此電腦上執行病毒掃描工作期間執行進階解毒。




活動威脅通知

# 在伺服器上解毒活動威脅

若要在伺服器上處理活動威脅，您需要執行以下操作：

- 在應用程式設定中啟用進階解毒技術；
- 在"*惡意軟體掃描*"工作屬性中啟用立即使用進階解毒。

如果 Kaspersky Endpoint Security 安裝在執行 Windows for Servers 的電腦上，則 Kaspersky Endpoint Security 不顯示通知。因此，您無法選擇解毒活動威脅的動作。若要解毒威脅，您需要在應用程式設定中啟用進階解毒技術，在"*惡意軟體掃描*"工作設定中啟用立即執行進階解毒。然後您需要啟動"*惡意軟體掃描*"工作。

# 消除未處理的威脅

Kaspersky Endpoint Security 將記錄偵測到威活動脅但未處理的檔案的相關資訊。此資訊在活動威脅清單中以事件的形式記錄（請參見下圖）。




活動威脅清單

如果 Kaspersky Endpoint Security 在掃描電腦查找病毒和其他惡意軟體的過程中對檔案進行了解毒或刪除了威脅，則受感染的檔案被認為*已處理*。

如果 Kaspersky Endpoint Security 在掃描電腦中的病毒和其他威脅時由於某種原因未能按照指定的應用程式設定對某個檔案執行操作，Kaspersky Endpoint Security 會將該檔案移至活動威脅清單。

在下列情況中可能出現此狀況：

- 掃描的檔案無法使用（例如，檔案位於網路磁碟或沒有讀寫權限的卸除式磁碟機上）。
- 在*惡意軟體掃描*工作設定中，偵測到威脅後的動作被設定為**"通知"**。然後，當受感染的檔案通知顯示在熒幕上時，使用者選擇**"略過"**。

如果存在任何未處理的威脅，Kaspersky Endpoint Security 會將圖示變更為 。在應用程式主視窗中，將顯示威脅通知（請見下圖）。在卡巴斯基安全管理中心主控台中，電腦的狀態變更為緊急 – 。

**如何在管理主控台 (MMC) 中處理威脅**

1. 在管理主控台中，轉到資料夾**"管理伺服器 → 進階 → 儲存區 → 活動威脅"**。

   活動威脅清單開啟。

2. 選擇您要處理的物件。

3. 選擇您要如何處理威脅：

   - **解毒**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。

   - **刪除**如果選取該選項，應用程式會刪除活動威脅儲存庫中偵測到的受感染檔案。在這種情況下，應用程式會將偵測到的檔案保留在電腦記憶體中。若要消除電腦中的威脅，請選取**解毒**。

**如何在網頁主控台和雲端主控台中處理威脅**

1. 在網頁主控台的主視窗中，選擇**操作** → **儲存區** → **活動威脅**。

   活動威脅清單開啟。

2. 選擇您要處理的物件。

3. 選擇您要如何處理威脅：

   - **解毒**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。

   - **刪除**如果選取該選項，應用程式會刪除活動威脅儲存庫中偵測到的受感染檔案。在這種情況下，應用程式會將偵測到的檔案保留在電腦記憶體中。若要消除電腦中的威脅，請選取**解毒**。

**如何在應用程式介面中處理威脅**

1. 在應用程式主視窗的**"正在監控"**區域中，點擊**"防護存在風險"**圖標。

   活動威脅清單開啟。

2. 選擇您要處理的物件。

3. 選擇您要如何處理威脅：

   - **處理**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。

   - **新增至排除項目**如果選擇此操作，Kaspersky Endpoint Security 會建議 將檔案新增到掃描排除項目清單中。排除設定自動配置。如果新增排除項目不可用，則表示管理員已停用在政策設定中新增排除項目。

   - **略過**如果選擇此選項，Kaspersky Endpoint Security 將從活動威脅清單中刪除該條目。如果清單上沒有剩餘活動威脅，則電腦狀態將變更為*"確定"*。如果再次偵測到該物件，Kaspersky Endpoint Security 會將新條目新增到活動威脅清單中。

   - **開啟所在資料夾**如果選擇此選項，Kaspersky Endpoint Security 將在檔案總管中開啟包含物件的資料夾。然後，您可以手動刪除物件或將物件移動到防護範圍之外的資料夾中。

   - **瞭解更多**如果選取該選項，Kaspersky Endpoint Security 會開啟卡巴斯基弱點與威脅資料庫網站。

要在卡巴斯基安全管理中心主控台中處理活動威脅，您必須啟用將有關未處理檔案的資訊傳輸到管理伺服器。預設情況下啟用資料傳輸。

### 如何啟用在管理主控台 (MMC) 中傳輸未處理的檔案資料

1. 在卡巴斯基安全管理中心管理主控台樹狀目錄中，選取**政策**。
2. 選擇必要的政策並點擊以開啟政策內容。
3. 在政策視窗中，選擇**"一般設定 → 報告和儲存"**。
4. 在**"到管理伺服器的資料傳輸"**塊中，點擊**"設定"**按鈕。
5. 選擇**"未處理的檔案"**核取方塊。
6. 儲存變更。

### 如何啟用在網頁主控台中傳輸未處理的檔案資料

1. 在網頁主控台的主視窗中，選擇**資產（裝置）→ 政策和設定檔**。
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. 在**"到管理伺服器的資料傳輸"**塊中，選中**"關於未處理的檔案"**核取方塊。
6. 儲存變更。




偵測到威脅時的主應用程式視窗

# 電腦防護

## 檔案威脅防護

“檔案威脅防護”元件允許您防止電腦的檔案系統受到感染。預設情況下，檔案威脅防護元件會永久駐留在電腦的 RAM 中，並即時掃描所有開啟、儲存或執行的檔案。該元件會掃描所有電腦磁碟機（包括已連線的磁碟機）上的檔案。該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來提供電腦防護。

該元件將掃描使用者或應用程式存取的檔案。如果偵測到惡意檔案，Kaspersky Endpoint Security 將封鎖檔案操作。應用程式隨後將根據“檔案威脅防護”元件的設定來清除或刪除惡意檔案。

當嘗試存取其內容位於 OneDrive 雲端儲存中的檔案時，Kaspersky Endpoint Security 會下載並掃描檔案內容。

## 啟用和停用檔案威脅防護

預設情況下，“檔案威脅防護”元件已啟用並在 Kaspersky 專家建議的模式下執行。對於檔案威脅防護，Kaspersky Endpoint Security 可以套用不同的設定群組。這些儲存在應用程式中的設定群組稱為*安全防護等級*：**高**、**建議**、**低**。**建議**安全防護等級設定將被視為 Kaspersky 專家建議的最佳設定（請見下表）。您可以選擇某種預設的安全防護等級或手動配置安全性等級的設定。如果您改變了檔案安全防護等級設定，仍可隨時還原到建議的檔案安全防護等級設定。

檔案威脅防護元件使用從其他應用程式元件接收的資料。可選擇啟用這些元件。提供其他資料的元件包括：

- 卡巴斯基安全網路。
- 主機入侵防禦。
- 行為偵測。

**如何在管理主控台（MMC）中啟用或停用“檔案威脅防護”元件**

1. 在卡巴斯基安全管理中心管理主控台樹狀目錄中，選取**政策**。
2. 選擇必要的政策並點擊以開啟政策內容。
3. 在政策視窗中，選擇“**關鍵威脅防護 → 檔案威脅防護**”。
4. 使用“**檔案威脅防護**“核取方塊來啟用或停用元件。

5. 如果啟用了該元件，請在**"安全等級"**塊中執行下列操作之一：

   - 如果您希望套用一種預設的安全防護等級，請使用移動滑桿選取：

     - **高**選擇此檔案安全等級後，"檔案威脅防護"元件將對開啟、儲存和執行的所有檔案實施最嚴格的控制。"檔案威脅防護"元件會掃描電腦的所有硬碟磁碟機、卸除式磁碟機和網路磁碟機上的所有檔案類型。它還掃描存檔、安裝套件和嵌入式 OLE 物件。

     - **建議防護**Kaspersky Lab 專家建議此檔案安全等級。"檔案威脅防護"元件僅掃描電腦的所有硬碟磁碟機、卸除式磁碟機和網路磁碟機上的指定檔案格式，以及嵌入式 OLE 物件。"檔案威脅防護"元件不掃描壓縮套件或安裝套件。

     - **低**此檔案安全等級的設定可確保最大掃描速度。"檔案威脅防護"元件僅掃描電腦的所有硬碟磁碟機、卸除式磁碟機以及網路磁碟機上擁有指定副檔名的檔案。"檔案威脅防護"元件不掃描複合檔案。

   - 如果要設定自訂安全防護等級，請點擊**"設定"**按鈕然後定義您自己的元件設定。

     您可以透過點擊**"根據預設"**按鈕來還原預設安全等級的值。.

6. 在**偵測到威脅後的動作**塊中，選取 Kaspersky Endpoint Security 對惡意物件所採取的操作：

   - **解毒；若解毒失敗則刪除**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**如果選擇該選項，Kaspersky Endpoint Security 將自動對已經偵測到的所有受感染的檔案執行解毒操作。如果解毒失敗，Kaspersky Endpoint Security 將阻止檔案（讀取/寫入）。

   - **封鎖**如果選擇該選項，"檔案威脅防護"元件將自動封鎖所有受感染的檔案，而不對其進行解毒處理。

   - **通知**如果選擇此選項，Kaspersky Endpoint Security 會在偵測到受感染檔案時將這些檔案的相關資訊新增到活動威脅清單。

   在嘗試解毒或刪除受感染的檔案之前，應用程式會建立該檔案的備份副本，以防您需要還原該檔案或將來可以對其進行解毒。

7. 儲存變更。

**如何在網頁主控台和雲端主控台中啟用或停用"檔案威脅防護"元件**

1. 在網頁主控台的主視窗中，選擇**資產（裝置）→政策和設定檔**。

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. 使用**"檔案威脅防護已啟用"**切換開關可啟用或停用元件。

6. 如果您希望將新物件新增至防護範圍：

   a. 在**進階設定**下，選擇**防護範圍**標籤。

   b. 點擊**"新增"**。

c. 這會開啟一個視窗；在此視窗中，選擇要新增到防護範圍的物件。

使用遮罩：

- `*`（星號）字元代表任意一組字元，但 `\` 和 `/` 字元除外（這兩個字元是檔案和資料夾路徑中的檔案和資料夾名稱的分隔符號）。例如，遮罩"`C:\*\*.txt`"將包括位於 C: 磁碟機但是不在子資料夾中所有帶 TXT 副檔名的檔案的路徑。

- 兩個連續 `*` 字元在檔案或資料夾名稱中代表任意一組字元（包括空集），包括 `\` 和 `/` 字元（這兩個字元是檔案和資料夾路徑中的檔案和資料夾名稱的分隔符號）。例如，遮罩 `C:\Folder\**\*.txt` 將包括位於巢嵌在 `Folder` 內的資料夾（`Folder`自身除外）中所有帶 TXT 副檔名的檔案的路徑。遮罩必須包含至少一個嵌套等級。遮罩 `C:\**\*.txt` 不是有效遮罩。

- `?`（問號）字元代表任意單個字元，但 `\` 和 `/` 字元除外（這兩個字元是檔案和資料夾路徑中的檔案和資料夾名稱的分隔符號）。例如，遮罩 `C:\Folder\???.txt` 將包括位於 `Folder` 資料夾中所有帶 TXT 副檔名且名稱由三個字元構成的檔案的路徑。

您可以在檔案或者資料夾路徑的任何地方使用遮罩。例如，如果您想要掃描範圍包括電腦上的所有使用者帳戶的"下載"資料夾，請輸入 `C:\Users\*\Downloads\` 遮罩。

您可以從防護中排除物件，而無需將其從防護範圍內的物件清單中刪除。為此，將它旁邊的切換開關設為關閉位置。

d. 儲存變更。

7. 在**偵測到威脅後的動作**塊中，選取 Kaspersky Endpoint Security 對惡意物件所採取的操作：

- **解毒；若解毒失敗則刪除**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**如果選擇該選項，Kaspersky Endpoint Security 將自動對已經偵測到的所有受感染的檔案執行解毒操作。如果解毒失敗，Kaspersky Endpoint Security 將阻止檔案（讀取/寫入）。

- **封鎖**如果選擇該選項，"檔案威脅防護"元件將自動封鎖所有受感染的檔案，而不對其進行解毒處理。

在嘗試解毒或刪除受感染的檔案之前，應用程式會建立該檔案的備份副本，以防您需要還原該檔案或將來可以對其進行解毒。

8. 如有必要，請編輯檔案威脅防護的進階設定。

9. 儲存變更。

**如何在應用程式介面中啟用或停用檔案威脅防護元件**

1. 在"應用程式主視窗"中，點擊⚙按鈕。

2. 在應用程式設定視窗中，選取"**關鍵威脅防護**"→"**檔案威脅防護**"。

3. 使用"**檔案威脅防護**"切換開關可啟用或停用元件。

4. 如果啟用了該元件，請在“**安全等級**“塊中執行下列操作之一：

- 如果您希望套用一種預設的安全防護等級，請使用移動滑桿選取：
  - **高**選擇此檔案安全等級後，“檔案威脅防護”元件將對開啟、儲存和執行的所有檔案實施最嚴格的控制。“檔案威脅防護”元件會掃描電腦的所有硬碟磁碟機、卸除式磁碟機和網路磁碟機上的所有檔案類型。它還掃描存檔、安裝套件和嵌入式 OLE 物件。
  - **建議**Kaspersky Lab 專家建議此檔案安全等級。“檔案威脅防護”元件僅掃描電腦的所有硬碟磁碟機、卸除式磁碟機和網路磁碟機上的指定檔案格式，以及嵌入式 OLE 物件。“檔案威脅防護”元件不掃描壓縮套件或安裝套件。
  - **低**此檔案安全等級的設定可確保最大掃描速度。“檔案威脅防護”元件僅掃描電腦的所有硬碟磁碟機、卸除式磁碟機以及網路磁碟機上擁有指定副檔名的檔案。“檔案威脅防護”元件不掃描複合檔案。
- 如果要設定自訂安全防護等級，請點擊“**進階設定**“按鈕然後定義您自己的元件設定。

  您可以透過點擊“**還原建議的安全等級**”按鈕來還原預設安全等級的值。.

5. 在**偵測到威脅後的動作**塊中，選取 Kaspersky Endpoint Security 對惡意物件所採取的操作：

- **解毒；若解毒失敗則刪除**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**如果選擇該選項，Kaspersky Endpoint Security 將自動對已經偵測到的所有受感染的檔案執行解毒操作。如果解毒失敗，Kaspersky Endpoint Security 將阻止檔案（讀取/寫入）。
- **封鎖**如果選擇該選項，“檔案威脅防護”元件將自動封鎖所有受感染的檔案，而不對其進行解毒處理。
- **通知**如果選擇此選項，Kaspersky Endpoint Security 會在偵測到受感染檔案時將這些檔案的相關資訊新增到活動威脅清單。

在嘗試解毒或刪除受感染的檔案之前，應用程式會建立該檔案的備份副本，以防您需要還原該檔案或將來可以對其進行解毒。

6. 儲存變更。

卡巴斯基專家建議的檔案威脅防護設定（建議的安全防護等級）

| 參數 | 值 | 描述 |
|---|---|---|
| **檔案類型** | **按格式掃描檔案** | 如果啟用該設定，則應用程式僅掃描被感染的檔案。在掃描檔案以尋找惡意程式碼之前，系統將分析檔案的內部頭以確定檔案的格式（例如，.txt、.doc 或 .exe）。掃描還會查找具有特定副檔名的檔案。 |
| **啟發式分析** | **輕度掃描** | 開發該技術的目的是偵測使用 Kaspersky 應用程式資料庫無法偵測到的威脅。它可以偵測受未知病毒或已知病毒新變種感染的可疑檔案。<br>掃描檔案中的惡意代碼時，啟發式分析器將執行可執行檔案中的指令。啟發式分析器執行的指令數取決於為啟發式分析器指定的級別。啟發式分析等級可在全面搜尋新威脅、載入作業系統資源和啟發式分析持續時間之間進行平衡。 |
| **只掃描新增及修改的檔案** | **開** | 僅掃描新檔案和自上次掃描以來已被修改的檔案。這有助於縮短掃描的持續時間。此模式適用於簡單檔案和複合檔案。 |
| **使用 iSwift 技術** | **開** | 該技術允許透過排除特定檔案不掃描的方式提高掃描速度。該技術將使用特殊演算法將檔案排除在掃描範圍之外，該演算法會考慮 Kaspersky Endpoint Security 資料庫的發佈日期、檔案的上次掃描日期以及對掃描設定的任何修改。iSwift 技術是對用於 NTFS 檔案系統的 iChecker 技術的增強版。 |
| **使用 iChecker 技術** | **開** | 該技術允許透過排除特定檔案不掃描的方式提高掃描速度。該技術將使用特殊演算法將檔案排除在掃描範圍之外，該演算法會考慮 Kaspersky Endpoint Security 資料庫的發佈日期、檔案的上次掃描日期以及對掃描設定的任何修改。iChecker 技術受到幾個限制：它無法操作大檔案，並且僅能套用至擁有程式可辨識結構的檔案 (例如：.exe、.dll、.lnk、.ttf、.inf、.sys、.com、.chm、.zip 和 .rar)。 |

| 參數 | 值 | 描述 |
| --- | --- | --- |
| **掃描 Microsoft Office 格式的檔案** | **開** | 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。應用程式掃描小於 1 MB 的 office 格式檔案，無論該核取方塊是否被選中。 |
| **掃描電子郵件格式檔案** | **開** | 掃描電子郵件格式的檔案。應用程式掃描 MSG 和 EML 檔案。電子郵件格式檔案也包含 OLE 物件和 MHT 檔案。Kaspersky Endpoint Security 掃描小於 1 MB 的電子郵件格式檔案，無論該核取方塊是否被選中。 |
| **掃描模式** | **智慧模式** | 在此模式中，檔案威脅防護將基於對物件所做操作進行分析以掃描物件。例如，當操作某個 Microsoft Office 手冊時，Kaspersky Endpoint Security 將在其首次開啟和最後一次關閉時掃描該檔案。覆蓋檔案的操作過程不會掃描檔案。 |
| **偵測到威脅後的動作** | **解毒；若解毒失敗則刪除** | 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。 |

# 自動暫停檔案威脅防護

您可以設定“檔案威脅防護”在指定時間或處理特定應用程式時自動暫停。

只有“檔案威脅防護”與某些應用程式衝突時，才應將其暫停作為最後手段。如果在元件執行時發生任何衝突，建議您聯繫Kaspersky 技術支援。支援專家將幫助您設定“檔案威脅防護”元件以便與您的電腦上的其他應用程式同時執行。

*要設定“檔案威脅防護”的自動暫停：*

1. 在“應用程式主視窗”中，點擊 按鈕。
2. 在應用程式設定視窗中，選取”**關鍵威脅防護**“→“**檔案威脅防護**”。
3. 點擊“**進階設定**”。
4. 在”**暫停檔案威脅防護**”塊中，點擊”**暫停檔案威脅防護**”連接。
5. 在開啟的視窗中，配置用於暫停檔案威脅防護'的設定：
   a. 配置自動暫停檔案威脅防護排程。
   b. 建立一個其操作應導致檔案威脅防護暫停其活動的應用程式清單。
6. 儲存變更。

# 變更“檔案威脅防護”元件對受感染檔案執行的操作

預設情況下，“檔案威脅防護”元件將自動嘗試對已經偵測到的所有受感染檔案執行解毒操作。如果解毒失敗，“檔案威脅防護”元件將刪除這些檔案。

*要變更"檔案威脅防護"元件對受感染檔案執行的操作：*

1. 在"應用程式主視窗"中，點擊⚙按鈕。
2. 在應用程式設定視窗中，選取"**關鍵威脅防護**"→"**檔案威脅防護**"。
3. 在"**偵測到威脅後的動作**"塊，選取相關選項：
   - **解毒；若解毒失敗則刪除**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**如果選擇該選項，Kaspersky Endpoint Security 將自動對已經偵測到的所有受感染的檔案執行解毒操作。如果解毒失敗，Kaspersky Endpoint Security 將阻止檔案（讀取/寫入）。
   - **封鎖**如果選擇該選項，"檔案威脅防護"元件將自動封鎖所有受感染的檔案，而不對其進行解毒處理。

   在嘗試解毒或刪除受感染的檔案之前，應用程式會建立該檔案的備份副本，以防您需要還原該檔案或將來可以對其進行解毒。
4. 儲存變更。

# 構成"檔案威脅防護"元件的防護範圍

防護範圍是指元件啟用時的掃描物件。不同元件的防護範圍有不同的參數。要掃描的檔案的位置和類型是"檔案威脅防護"元件防護範圍的內容。預設情況下，"檔案威脅防護"元件僅掃描從硬碟、抽取式磁碟機和網路磁碟機執行的潛在受感染檔案。

選取需要掃描的檔案類型時，請考慮以下資訊：

1. 將惡意程式碼引入某些格式的檔案並隨後將其啟動的可能性很低（例如 TXT 格式）。同時，部分檔案格式會包含可幸執行檔代碼（如 .exe、.dll）。可執行代碼還可能包含在並非用於此用途的格式（例如 DOC 格式）的檔案中。這些檔案中，惡意程式碼入侵並執行的可能性高。
2. 入侵者可能會把可執行檔的副檔名重新命名為 .txt，然後將其中的病毒或其他惡意應用程式傳送到您的電腦中。如果您按照副檔名選取掃描檔案，程式將在掃描期間略過此檔案。如果選擇按格式掃描檔案，則 Kaspersky Endpoint Security 會分析檔案標頭，和副檔名無關。如果此分析顯示檔案具有可執行檔的格式（例如，EXE），則應用程式將對其進行掃描。

*要建立防護範圍，請執行以下操作：*

1. 在"應用程式主視窗"中，點擊⚙按鈕。
2. 在應用程式設定視窗中，選取"**關鍵威脅防護**"→"**檔案威脅防護**"。
3. 點擊"**進階設定**"。

4. 在“**檔案類型**”塊中，指定您希望“檔案威脅防護”元件掃描的檔案類型：

   - **所有檔案**如果啟用該設定，Kaspersky Endpoint Security 將毫無例外地掃描所有檔案（所有格式和副檔名）。
   - **按格式掃描檔案**如果啟用該設定，則應用程式僅掃描被感染的檔案。在掃描檔案以尋找惡意程式碼之前，系統將分析檔案的內部頭以確定檔案的格式（例如，.txt、.doc 或 .exe）。掃描還會查找具有特定副檔名的檔案。
   - **按副檔名掃描檔案**如果啟用該設定，則應用程式僅掃描被感染的檔案。此時，系統將根據檔案的副檔名確定檔案格式。

5. 點擊“**編輯防護範圍**”連接。

6. 在開啟的視窗中，選擇要新增到防護範圍或從中排除的物件。

   您無法刪除或編輯包括在預設防護範圍中的物件。

7. 如果您希望將新物件新增至防護範圍：

   a. 點擊“**新增**”。

   資料夾樹開啟。

   b. 在“**路徑**”欄位中，輸入資料夾或者檔案路徑。

   使用遮罩：

   - `*`（星號）字元代表任意一組字元，但 `\` 和 `/` 字元除外（這兩個字元是檔案和資料夾路徑中的檔案和資料夾名稱的分隔符號）。例如，遮罩“`C:\*\*.txt`”將包括位於 C: 磁碟機但是不在子資料夾中所有帶 TXT 副檔名的檔案的路徑。
   - 兩個連續 `*` 字元在檔案或資料夾名稱中代表任意一組字元（包括空集），包括 `\` 和 `/` 字元（這兩個字元是檔案和資料夾路徑中的檔案和資料夾名稱的分隔符號）。例如，遮罩 `C:\Folder\**\*.txt` 將包括位於巢嵌在 `Folder` 內的資料夾（`Folder`自身除外）中所有帶 TXT 副檔名的檔案的路徑。遮罩必須包含至少一個嵌套等級。遮罩 `C:\**\*.txt` 不是有效遮罩。
   - `?`（問號）字元代表任意單個字元，但 `\` 和 `/` 字元除外（這兩個字元是檔案和資料夾路徑中的檔案和資料夾名稱的分隔符號）。例如，遮罩 `C:\Folder\???.txt` 將包括位於 `Folder` 資料夾中所有帶 TXT 副檔名且名稱由三個字元構成的檔案的路徑。

   您可以在檔案或者資料夾路徑的任何地方使用遮罩。例如，如果您想要掃描範圍包括電腦上的所有使用者帳戶的“下載”資料夾，請輸入 `C:\Users\*\Downloads\` 遮罩。

   電腦檔案資源清單中的**此 PC**物件包含以下物件：**所有硬碟磁碟機**、**所有網路磁碟機**及**所有卸除式磁碟機**。

   您可以從掃描中排除物件，而無需將其從掃描範圍內的物件清單中刪除。為此，請清除物件旁邊的核取方塊。

8. 儲存變更。

# 選擇掃描方式

Kaspersky Endpoint Security 使用一種稱為機器學習和特徵碼分析的掃描技術。在特徵碼分析中，Kaspersky Endpoint Security 會將偵測物件與其資料庫中的記錄進行比對。根據 Kaspersky 專家的建議，機器學習和簽章分析始終啟用。

您可以使用啟發式分析提高防護效率。掃描檔案中的惡意代碼時，啟發式分析器將執行可執行檔案中的指令。啟發式分析器執行的指令數取決於為啟發式分析器指定的級別。啟發式分析等級可在全面搜尋新威脅、載入作業系統資源和啟發式分析持續時間之間進行平衡。

*要設定"檔案威脅防護"元件執行中啟發式分析的使用：*

1. 在"應用程式主視窗"中，點擊⚙按鈕。
2. 在應用程式設定視窗中，選取"**關鍵威脅防護**"→"**檔案威脅防護**"。
3. 點擊"**進階設定**"。
4. 如果希望應用程式使用啟發式分析來防禦檔案威脅，請選中"**掃描方式**"塊中的"**啟發式分析**"核取方塊。然後使用捲軸設定啟發式分析等級：**輕度掃描**、**中度掃描**或**深度掃描**。
5. 儲存變更。

# 在"檔案威脅防護"元件的執行中使用掃描技術

*要設定"檔案威脅防護"元件執行中掃描技術的使用：*

1. 在"應用程式主視窗"中，點擊⚙按鈕。
2. 在應用程式設定視窗中，選取"**關鍵威脅防護**"→"**檔案威脅防護**"。
3. 點擊"**進階設定**"。
4. 在"**掃描技術**"塊中，選取您要用於檔案威脅防護的技術名稱旁邊的核取方塊。

   - **使用 iSwift 技術**該技術允許透過排除特定檔案不掃描的方式提高掃描速度。該技術將使用特殊演算法將檔案排除在掃描範圍之外，該演算法會考慮 Kaspersky Endpoint Security 資料庫的發佈日期、檔案的上次掃描日期以及對掃描設定的任何修改。iSwift 技術是對用於 NTFS 檔案系統的 iChecker 技術的增強版。
   - **使用 iChecker 技術**該技術允許透過排除特定檔案不掃描的方式提高掃描速度。該技術將使用特殊演算法將檔案排除在掃描範圍之外，該演算法會考慮 Kaspersky Endpoint Security 資料庫的發佈日期、檔案的上次掃描日期以及對掃描設定的任何修改。iChecker 技術受到幾個限制：它無法操作大檔案，並且僅能套用至擁有程式可辨識結構的檔案 (例如：.exe、.dll、.lnk、.ttf、.inf、.sys、.com、.chm、.zip 和 .rar)。

5. 儲存變更。

# 最佳化檔案掃描

您可以透過減少掃描時間和提高 Kaspersky Endpoint Security 的執行速度來最佳化"檔案威脅防護"元件執行的檔案掃描。這可以透過僅掃描新檔案和上次掃描後經過修改的檔案來實現。此模式適用於簡單檔案和複合檔案。

您也可以啟用 iChecker 和 iSwift 技術，在掃描中排除最近一次掃描後未修改的檔案，從而最佳化檔案掃描速度。

*要最佳化檔案掃描，請執行以下操作：*

1. 在"應用程式主視窗"中，點擊⚙ 按鈕。
2. 在應用程式設定視窗中，選取"**關鍵威脅防護**"→"**檔案威脅防護**"。
3. 點擊"**進階設定**"。
4. 在"**最佳化**"塊中，選中"**只掃描新增及修改的檔案**"核取方塊。
5. 儲存變更。

# 掃描複合檔案

隱藏病毒和其他惡意程式的一種常用方法就是將其植入複合檔案中，例如存檔案或資料庫中。為了偵測以這種方式隱藏的病毒和其他惡意軟體，必須將複合檔案解壓縮，但是這可能會降低掃描速度。您可以限制要掃描的複合檔案類型，從而加快掃描速度。

用於處理受感染複合檔案（解毒或刪除）的方法取決於檔案類型。

"檔案威脅防護"元件會解毒 ZIP、GZIP、BZIP、RAR、TAR、ARJ、CAB、LHA、JAR 和 ICE 格式的複合檔案並刪除所有其他格式的檔案（郵件資料庫除外）。

*若要設定複合檔案的掃描，請執行以下操作：*

1. 在"應用程式主視窗"中，點擊⚙ 按鈕。
2. 在應用程式設定視窗中，選取"**關鍵威脅防護**"→"**檔案威脅防護**"。
3. 點擊"**進階設定**"。
4. 在"**掃描複合檔案**"塊中，指定您希望掃描的複合檔案類型：存檔、分發套件、郵件或 Office 格式檔案。
5. 如果停用了僅掃描新檔案和修改的檔案，請配置用於掃描每種類型的複合檔案的設定：掃描所有此類檔案或僅掃描新檔案。

   如果啟用僅掃描新檔案和修改的檔案，則 Kaspersky Endpoint Security 將僅掃描所有類型的複合檔案中的新檔案和修改的檔案。

6. 配置用於掃描複合檔案的進階設定。

- **不解壓縮大型複合檔案**

  如果選中該核取方塊，Kaspersky Endpoint Security 不會掃描其大小超過指定值的複合檔案。

  如果清除該核取方塊，Kaspersky Endpoint Security 將掃描所有大小的複合檔案。

  > 無論是否選中"**不解壓縮大型複合檔案**"核取方塊，Kaspersky Endpoint Security 均會掃描從存檔中提取的大型檔案。

- **在背景解壓縮複合檔案**

  如果選中該核取方塊，Kaspersky Endpoint Security 會提供對大於指定值的複合檔案的存取權限，然後再掃描這些檔案。在這種情況下，Kaspersky Endpoint Security 在背景解壓並掃描複合檔案。

  對於小於該值的複合檔案，只有在解壓和掃描這些檔案後，Kaspersky Endpoint Security 才會提供對這些檔案的存取權限。

  如果未選中該核取方塊，則只有在解壓和掃描任何大小的複合檔案後，Kaspersky Endpoint Security 才會提供對這些檔案的存取權限。

7. 儲存變更。

# 變更掃描模式

*掃描模式*是指觸發"檔案威脅防護"元件進行檔案掃描的條件。預設情況下，Kaspersky Endpoint Security 以智慧模式掃描檔案。在此檔案掃描模式下，"檔案威脅防護"元件將確定是否在使用者、應用程式（以使用者身分在登入的帳戶下或用不同帳戶）或作業系統對檔案執行分析操作後掃描檔案。例如，當操作某個 Microsoft Office Word 手冊時，Kaspersky Endpoint Security 將在其首次開啟和最後一次關閉時掃描該檔案。覆蓋檔案的操作過程不會掃描檔案。

*若要變更檔案掃描模式，請執行以下操作：*

1. 在"應用程式主視窗"中，點擊⚙按鈕。
2. 在應用程式設定視窗中，選取"**關鍵威脅防護**"→"**檔案威脅防護**"。
3. 點擊"**進階設定**"。
4. 在"**掃描模式**"塊中，選取所需的模式：

- **智慧模式**在此模式中，檔案威脅防護將基於對物件所做操作進行分析以掃描物件。例如，當操作某個 Microsoft Office 手冊時，Kaspersky Endpoint Security 將在其首次開啟和最後一次關閉時掃描該檔案。覆蓋檔案的操作過程不會掃描檔案。
- **在存取及修改時**在該模式中，檔案威脅防護將在出現開啟/修改檔案的嘗試時掃描物件。
- **存取時**在此模式中，檔案威脅防護將在出現開啟/修改檔案的嘗試時掃描物件。
- **執行時**在該模式中，檔案威脅防護僅在出現執行檔案的嘗試時掃描物件。

5. 儲存變更。

# 容器掃描

一個 *容器* 是一個隔離環境，應用程式可以在其中執行而無需直接與作業系統交互。使用容器涉及以下風險：

- 駭客可能能夠利用容器化弱點來損害容器內的應用程式。
- 駭客可能會利用容器環境的不安全配置來獲得對電腦上資料未經授權的存取或損害系統的完整性。
- 對容器的成功攻擊可以讓駭客獲得對電腦上資料的存取權限。
- 駭客可能會利用網路弱點來攔截網路流量。

Kaspersky Endpoint Security 不僅掃描磁碟上的檔案，還掃描容器內的檔案。也就是說，Kaspersky Endpoint Security 是用於偵測容器內惡意活動的外部工具。這可以維持容器的效能並防止與容器內的其他應用程式發生衝突。不支援在容器內安裝 Kaspersky Endpoint Security。

除了提供容器安全性之外，Kaspersky Endpoint Security 還允許使用應用程式控制管理容器內的應用程式。為容器配置應用程式控制的方式與為電腦上安裝的應用程式配置的方式相同。系統完整性監控 也支援容器。

## 容器要求

- 容器必須是 Docker 容器。其他容器化工具不受支援。
- 容器必須在處理程序隔離模式下執行。Hyper-V 隔離模式不受支援。
- 容器必須放置在 Windows Server 2016、2019 或 2022 伺服器上（Docker Host）。
- 容器必須包含 Windows 映像 (Docker Image）。不支援 Windows 10 和 11。不支援 Linux 映像。

## 偵測到威脅後的動作

如果在容器內偵測到威脅，應用程式將套用 為檔案威脅防護元件所選擇的操作。容器掃描具有其他設定（請參閱下方的說明）。如果偵測到威脅，應用程式會封鎖惡意活動並執行選定的操作（例如，嘗試解毒物件）。如果偵測到的物件無法被解毒，Kaspersky Endpoint Security 可以停止容器。預設情況下，容器停止功能處於停用狀態。

**如何在管理主控台 (MMC) 中設定容器掃描**

1. 在卡巴斯基安全管理中心管理主控台樹狀目錄中，選取**政策**。
2. 選擇必要的政策並點擊以開啟政策內容。
3. 在政策視窗中，選擇**"關鍵威脅防護 → 檔案威脅防護"**。
4. 點擊**"設定"**。
5. 在開啟的視窗中選擇**"附加"**標籤。

6. 在“**掃描在 Windows 容器中排除的檔案操作**“塊中，配置容器掃描設定：

   - **如果清除失敗則停止容器**應用程式對於偵測到的物件可能沒有足夠的讀寫權限。在這種情況下，不可能對檢測到的物件進行解毒或刪除。如果選取此核取方塊，應用程式將封鎖偵測到的物件並停止容器。如果清除此核取方塊，應用程式將僅封鎖偵測到的物件。

   - **不掃描在 Windows 容器中排除的檔案操作**如果選取該核取方塊，則應用程式僅在容器啟動時掃描容器。如果清除該核取方塊，應用程式將即時連續掃描容器。

7. 儲存變更。

**如何在網頁主控台和雲端主控台中配置容器掃描**

1. 在網頁主控台的主視窗中，選擇**資產（裝置）→政策和設定檔**。

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，選擇**效能**標籤。

6. 在“**掃描最佳化**“塊中，配置容器掃描設定：

   - **如果解毒失敗則停止容器**應用程式對於偵測到的物件可能沒有足夠的讀寫權限。在這種情況下，不可能對檢測到的物件進行解毒或刪除。如果選取此核取方塊，應用程式將封鎖偵測到的物件並停止容器。如果清除此核取方塊，應用程式將僅封鎖偵測到的物件。

   - **不掃描在 Windows 容器中排除的檔案操作**如果選取該核取方塊，則應用程式僅在容器啟動時掃描容器。如果清除該核取方塊，應用程式將即時連續掃描容器。

7. 儲存變更。

**如何在應用程式介面中配置容器掃描**

1. 在“應用程式主視窗”中，點擊⚙ 按鈕。

2. 在應用程式設定視窗中，選取”**關鍵威脅防護**“→“**檔案威脅防護**”。

3. 在“**掃描在 Windows 容器中排除的檔案操作**“塊中，配置容器掃描設定：

   - **如果清除失敗則停止容器**應用程式對於偵測到的物件可能沒有足夠的讀寫權限。在這種情況下，不可能對檢測到的物件進行解毒或刪除。如果選取此核取方塊，應用程式將封鎖偵測到的物件並停止容器。如果清除此核取方塊，應用程式將僅封鎖偵測到的物件。

   - **不掃描在 Windows 容器中排除的檔案操作**如果選取該核取方塊，則應用程式僅在容器啟動時掃描容器。如果清除該核取方塊，應用程式將即時連續掃描容器。

4. 儲存變更。

# 主機入侵防禦

如果 Kaspersky Endpoint Security 安裝在執行 Windows for Workstations 的電腦上，則該元件可用。如果 Kaspersky Endpoint Security 安裝在執行 Windows for Servers 的電腦上，則該元件不可用。

“主機入侵防禦”元件可避免應用程式執行可能給作業系統帶來危險的操作，並確保控制對作業系統資源和個人資料的存取。該元件借助防毒資料庫和卡巴斯基安全網路雲端服務來提供電腦防護。

該元件透過*應用程式權限*來控制應用程式的操作。應用程式權限包括以下存取參數：

- 對作業系統資源（例如，自動啟動選項、登錄機碼）的存取權限
- 對個人資料（例如，檔案和應用程式）的存取權限

防火牆元件使用*網絡規則*控制應用程式的網絡活動。

在應用程式首次啟動期間，“主機入侵防禦”元件會執行以下操作：

1. 使用下載的防毒資料庫檢查應用程式的安全性。
2. 在卡巴斯基安全網路中檢查應用程式安全性。

   建議您加入卡巴斯基安全網路以幫助“主機入侵防禦”元件更有效地工作。

3. 將應用程式放置在其中一個受信任群組中：*受信任*，*低限制*，*高限制*，*不信任*。

   信任群組定義了在控制應用程式活動時 Kaspersky Endpoint Security 所引用的權限。Kaspersky Endpoint Security 會將應用程式放置在某個信任群組中，實際取決於該應用程式可能對電腦造成的危險等級而定。

   Kaspersky Endpoint Security 將應用程式放置在“防火牆”和“主機入侵防禦”元件的信任群組中。您不能僅變更“防火牆”或“主機入侵防禦”的信任群組。

   如果您拒絕加入 KSN 或沒有網路，Kaspersky Endpoint Security 會根據“主機入侵防禦”元件的設定將應用程式放置在某個信任群組中。從 KSN 收到應用程式的信譽後，可以自動變更信任群組。

4. 根據信任群組封鎖應用程式操作。例如，“*高限制*”信任群組中的應用程式會被拒絕存取作業系統模組。

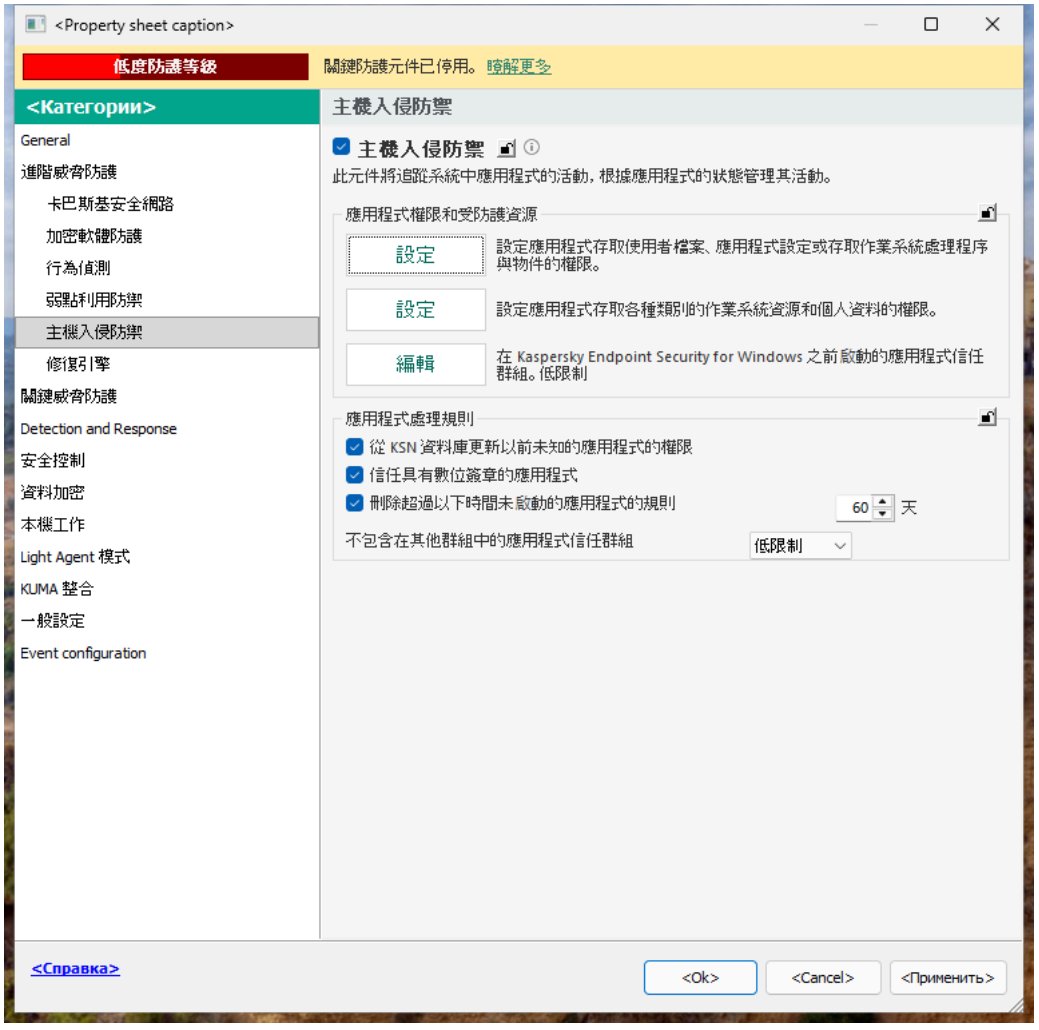
下次啟動應用程式時，Kaspersky Endpoint Security 會檢查該應用程式的完整性。如果應用程式未變更，則該元件對其應用目前應用程式權限。如果應用程式已經過修改，Kaspersky Endpoint Security 會分析應用程式，就像它初次開機時一樣。

# 啟用和停用主機入侵防禦

預設情況下，“主機入侵防禦”元件已啟用並在 Kaspersky 專家建議的模式下執行。

### 如何在管理主控台（MMC）中啟用或停用主機入侵防禦元件

1. 在卡巴斯基安全管理中心管理主控台樹狀目錄中，選取**政策**。
2. 選擇必要的政策並點擊以開啟政策內容。
3. 在政策視窗中，選擇“**進階威脅防護 → 主機入侵防禦**”。




入侵防禦設定

4. 使用“**主機入侵防禦**”核取方塊來啟用或停用元件。
5. 儲存變更。若要在電腦上套用該政策，請關閉掛鎖。

### 如何在網頁主控台和雲端主控台中啟用或停用主機入侵防禦元件

1. 在網頁主控台的主視窗中，選擇**資產（裝置）→ 政策和設定檔**。
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**"→"**主機入侵防禦**"。

5. 使用"**主機入侵防禦已啟用**"切換開關可啟用或停用元件。

6. 儲存變更。

**如何在應用程式介面中啟用或停用主機入侵防禦元件**

1. 在"應用程式主視窗"中，點擊⚙按鈕。

2. 在應用程式設定視窗中，選取"**進階威脅防護**"→"**主機入侵防禦**"。

3. 使用"**主機入侵防禦**"切換開關可啟用或停用元件。

4. 儲存變更。

如果啟用了主機入侵防禦元件，Kaspersky Endpoint Security 會將應用程式放置在某個信任群組中，實際取決於該應用程式可能對電腦造成的危險等級而定。然後，Kaspersky Endpoint Security 將根據信任群組封鎖應用程式的操作。

# 管理應用程式信任群組

每個應用程式首次啟動時，"主機入侵防禦"元件都會檢查此應用程式的安全性並將其置於某個信任群組中。

在應用程式掃描的第一階段，Kaspersky Endpoint Security 將搜尋已知應用程式的內部資料庫檢視是否存在比對的項目，同時向卡巴斯基安全網路資料庫傳送請求（如果網際網路連線可用）。根據內部資料庫和卡巴斯基安全網路資料庫中的搜尋結果，應用程式將被放入信任群組。隨後每次啟動應用程式時，如果應用程式在 KSN 資料庫中的信譽已變更，則 Kaspersky Endpoint Security 會向 KSN 資料庫傳送一個新查詢，並將該應用程式放入另一個信任群組。

您可以選擇想要 Kaspersky Endpoint Security 自動將所有未知應用程式放置到的信任群組。在 Kaspersky Endpoint Security 啟動之前一直在執行的應用程式會被自動放置到信任群組 在主機入侵防禦設定中設定。

對於先于 Kaspersky Endpoint Security 啟動的應用程式，只有網路活動受到控制。根據防火牆設定中定義的網路規則執行控制。

# 變更應用程式的信任群組

每個應用程式首次啟動時，"主機入侵防禦"元件都會檢查此應用程式的安全性並將其置於某個信任群組中。

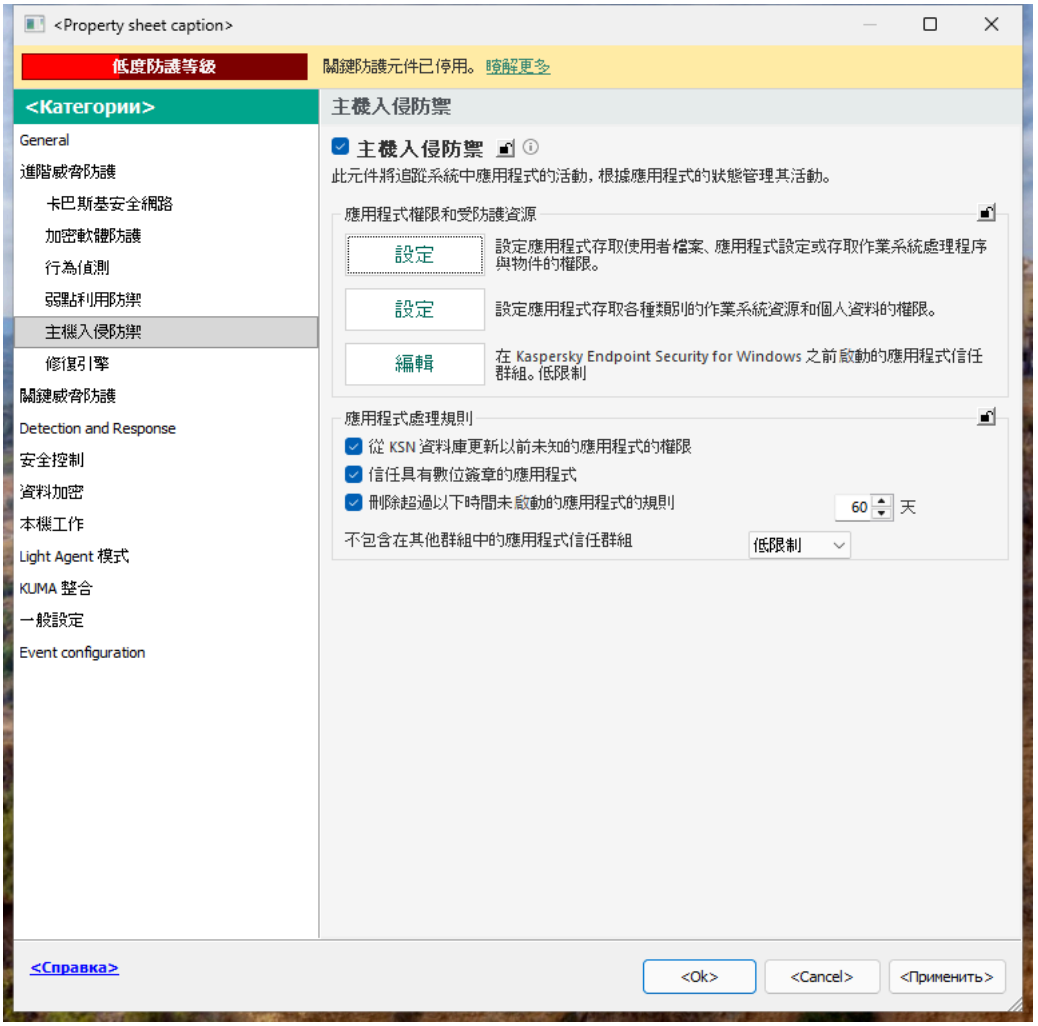
Kaspersky 專家建議您不要將應用程式從自動分配的信任群組移動到不同的信任群組。作為替代，如有必要，您可以修改單個應用程式的權限。

**如何在管理主控台 (MMC) 中變更應用程式的信任群組**

1. 在卡巴斯基安全管理中心管理主控台樹狀目錄中，選取**政策**。

2. 選擇必要的政策並點擊以開啟政策內容。

3. 在政策視窗中，選擇“**進階威脅防護 → 主機入侵防禦**”。




入侵防禦設定

4. 在”**應用程式權限和受防護資源**”塊中，點擊”**設定**”按鈕。

   這將開啟應用程式權限配置視窗和受防護資源的清單。

5. 選擇“**應用程式權限**”標籤。

6. 點擊“**新增**”。

7. 在開啟的視窗中，輸入條件搜尋要變更其信任群組的應用程式。

   您可以輸入應用程式名稱或供應商名稱。Kaspersky Endpoint Security 輸入遮罩時支援環境變量以及`*`和`?`字元。

8. 點擊“**重新整理**”。

   Kaspersky Endpoint Security 將在受管電腦上安裝的應用程式的合併清單中搜尋該應用程式。Kaspersky Endpoint Security 將顯示滿足您搜尋條件的應用程式清單。

9. 選取需要的應用程式。

10. 在“**將選擇應用程式新增至信任群組**”下拉清單中，為應用程式選擇必要的信任群組。

11. 儲存變更。若要在電腦上套用該政策，請關閉掛鎖。

**如何在網頁主控台和雲端主控台中變更應用程式的信任群組**

1. 在網頁主控台的主視窗中，選擇**資產（裝置）→政策和設定檔**。
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"→"主機入侵防禦"**。
5. 在**"應用程式權限和受防護資源"**塊中，點擊**"應用程式權限和受防護資源"**連接。
   這將開啟應用程式權限配置視窗和受防護資源的清單。
6. 選擇**"應用程式權限"**標籤。
   您將在視窗左側看到信任群組清單，並在右側看到它們的屬性。
7. 點擊**"新增"**。
   這將啟動用於將應用程式新增到信任群組的精靈。
8. 選擇相關應用程式信任群組。
9. 選擇**應用程式**類型。前往下一步。
   如果要變更多個應用程式的信任群組，請選擇**群組**類型並定義應用程式組的名稱。
10. 在開啟的應用程式清單中，選擇要變更其信任群組的應用程式。
    使用篩選器。您可以輸入應用程式名稱或供應商名稱。Kaspersky Endpoint Security 輸入遮罩時支援環境變量以及`*`和`?`字元。
11. 結束精靈。
    該應用程式將被新增到信任群組。
12. 儲存變更。

**如何在應用程式介面中變更應用程式的信任群組**

1. 在"應用程式主視窗"中，點擊⚙按鈕。
2. 在應用程式設定視窗中，選取**"進階威脅防護"→"主機入侵防禦"**。
3. 點擊**"管理應用程式"**。
   這將開啟已安裝的應用程式的清單。
4. 選取需要的應用程式。
5. 在應用程式的內容功能表中，點擊**"限制"→ <信任群組>**。
6. 儲存變更。

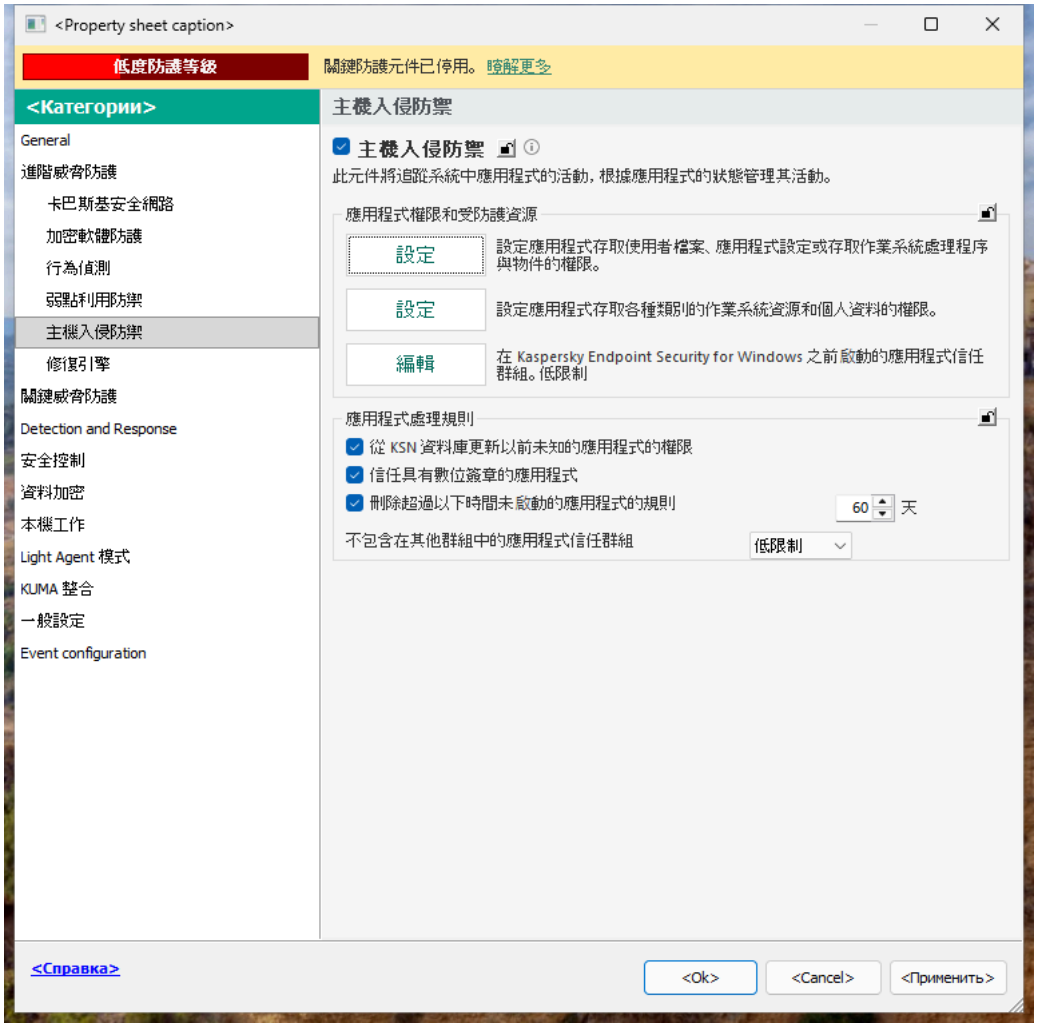
結果，該應用程式將被放入另一個信任群組。然後，Kaspersky Endpoint Security 將根據信任群組封鎖應用程式的操作。*(使用者定義)*狀態將被分配給該應用程式。如果在卡巴斯基安全網路中變更了應用程式的信譽，則主機入侵防禦元件將使該應用程式的信任群組保持不變。

# 配置信任群組權限

預設情況下，將為不同的信任群組建立最佳應用程式權限。信任群組中的應用程式群組的權限設定會繼承信任群組權限設定的值。

### 如何在管理主控台（MMC）中變更信任群組權限

1. 在卡巴斯基安全管理中心管理主控台樹狀目錄中，選取**政策**。
2. 選擇必要的政策並點擊以開啟政策內容。
3. 在政策視窗中，選擇**"進階威脅防護 → 主機入侵防禦"**。




入侵防禦設定

4. 在**"應用程式權限和受防護資源"**塊中，點擊**"設定"**按鈕。

   這將開啟應用程式權限配置視窗和受防護資源的清單。

5. 選擇**"應用程式權限"**標籤。
6. 選擇必要的信任群組。
7. 在信任群組的內容功能表中，選取**"群組權限"**。

   這將開啟信任群組屬性。

8. 請執行以下操作之一：

   - 如果要編輯用作業系統登錄檔、使用者檔案和應用程式設定來管理操作的的信任群組權限，請選取**"檔案和系統登錄檔"**標籤。
   - 如果要編輯管理對作業系統處理程序和物件存取權限的信任群組權限，請選擇**"權限"**標籤。

   防火牆元件使用*網絡規則*控制應用程式的網絡活動。

9. 對於相關資源，在相應操作的列中，右鍵點擊以開啟內容功能表，然後選擇必要的選項：**繼承**，**允許**（ ）或**封鎖**（ ）。

10. 如果要監視電腦資源的使用，請選擇**"記錄事件"**（ / ）。

    Kaspersky Endpoint Security 將記錄有關主機入侵防禦元件操作的資訊。報告包含有關應用程式執行的電腦資源操作的資訊（允許或禁止）。報告還包含有關利用每種資源的應用程式的資訊。

11. 儲存變更。若要在電腦上套用該政策，請關閉掛鎖。

**如何在網頁主控台和雲端主控台中變更信任群組權限**

1. 在網頁主控台的主視窗中，選擇**資產（裝置）→政策和設定檔**。
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"→"主機入侵防禦"**。
5. 在**"應用程式權限和受防護資源"**塊中，點擊**"應用程式權限和受防護資源"**連接。

   這將開啟應用程式權限配置視窗和受防護資源的清單。

6. 選擇**"應用程式權限"**標籤。

   您將在視窗左側看到信任群組清單，並在右側看到它們的屬性。

7. 在視窗的左側，選擇相關的信任群組。
8. 在視窗右側的下拉清單中，執行下列操作之一：

   - 要編輯管理應用程式存取作業系統登錄檔、使用者檔案和應用程式設定的權限的信任群組權限，請選取**"檔案和系統登錄檔"**標籤。
   - 如果要編輯用於管理對作業系統處理程序和物件存取權限的信任群組權限，請選擇**"權限"**。

   防火牆元件使用*網絡規則*控制應用程式的網絡活動。

9. 對於相關資源，在相應操作的列中，選擇必要的選項：**繼承**，**允許**（ ），**封鎖**（ ）。

10. 如果要監視電腦資源的使用，請選擇**"記錄事件"**（ / ）。

    Kaspersky Endpoint Security 將記錄有關主機入侵防禦元件操作的資訊。報告包含有關應用程式執行的電腦資源操作的資訊（允許或禁止）。報告還包含有關利用每種資源的應用程式的資訊。

11. 儲存變更。

**如何在應用程式介面中變更信任群組權限**

1. 在"應用程式主視窗"中，點擊 按鈕。
2. 在應用程式設定視窗中，選取**"進階威脅防護"→"主機入侵防禦"**。
3. 點擊**"管理應用程式"**。

   這將開啟已安裝的應用程式的清單。

4. 選擇必要的信任群組。
5. 在信任群組的內容功能表中，選取**"細節和規則"**。

   這將開啟信任群組屬性。

6. 請執行以下操作之一：

   - 如果要編輯用作業系統登錄檔、使用者檔案和應用程式設定來管理操作的的信任群組權限，請選取**"檔案和系統登錄檔"**標籤。
   - 如果要編輯管理對作業系統處理程序和物件存取權限的信任群組權限，請選擇**"權限"**標籤。

   防火牆元件使用*網絡規則*控制應用程式的網絡活動。

7. 對於相關資源，在相應操作的列中，右鍵點擊以開啟內容功能表，然後選擇必要的選項：**繼承**，**允許**（ ）或**拒絕**（ ）。
8. 如果要監視電腦資源的使用，請選擇**"記錄事件"**（ ）。

   Kaspersky Endpoint Security 將記錄有關主機入侵防禦元件操作的資訊。報告包含有關應用程式執行的電腦資源操作的資訊（允許或禁止）。報告還包含有關利用每種資源的應用程式的資訊。

9. 儲存變更。

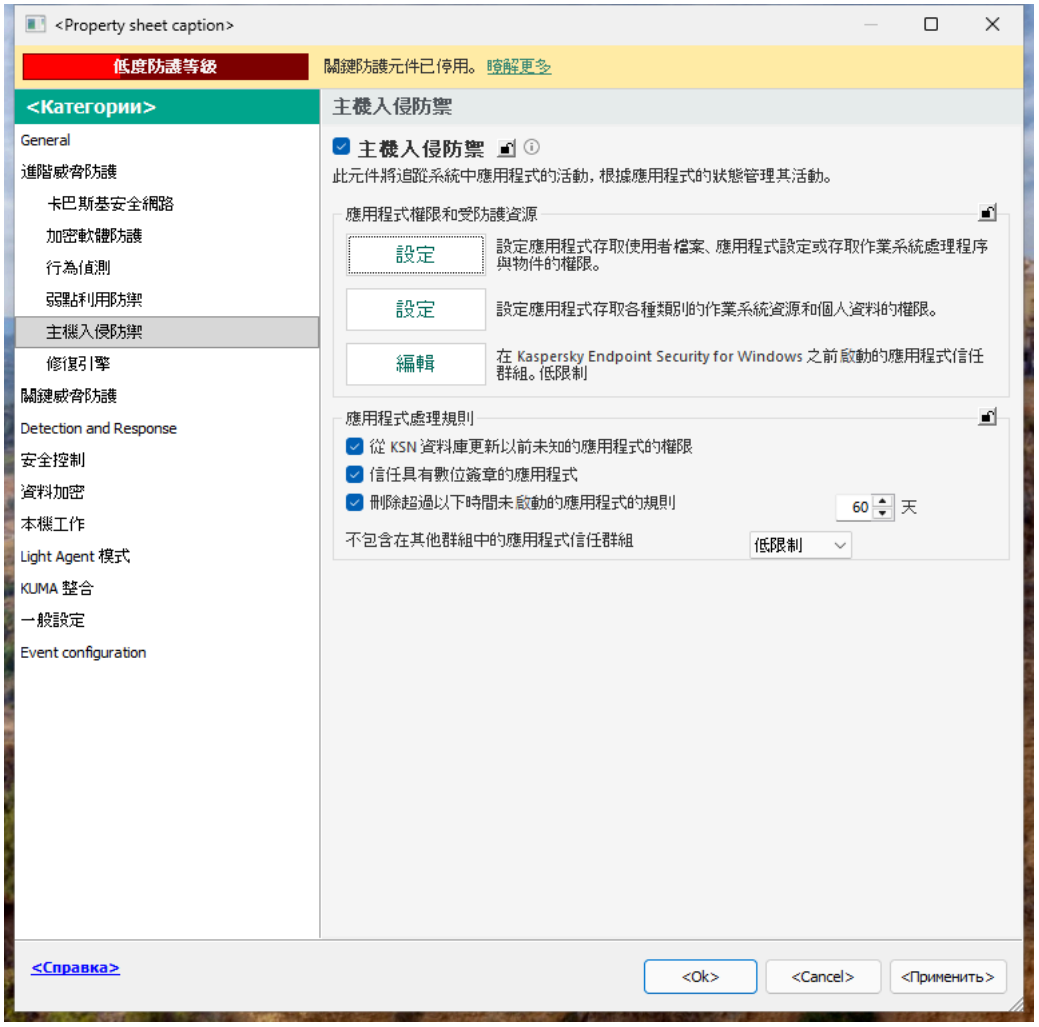
信任群組權限將被變更。然後，Kaspersky Endpoint Security 將根據信任群組封鎖應用程式的操作。狀態（*自訂設定*）將分配給信任群組。

# 選取在 Kaspersky Endpoint Security 啟動之前啟動的應用程式信任群組

對於先于 Kaspersky Endpoint Security 啟動的應用程式，只有網路活動受到控制。根據防火牆設定中定義的網路規則執行控制。若要指定必須為此類應用程式的網路活動應用哪些網路規則，您必須選取信任群組。

### 如何在管理主控台（MMC）中為在 Kaspersky Endpoint Security 之前啟動的應用程式選擇信任群組

1. 在卡巴斯基安全管理中心管理主控台樹狀目錄中，選取**政策**。
2. 選擇必要的政策並點擊以開啟政策內容。
3. 在政策視窗中，選擇"**進階威脅防護 → 主機入侵防禦**"。




入侵防禦設定

4. 在"**應用程式權限和受防護資源**"塊中，點擊"**編輯**"按鈕。
5. 對於"**在 Kaspersky Endpoint Security 前啟動的應用程式信任群組**"設定，選擇合適的"信任群組"。
6. 儲存變更。若要在電腦上套用該政策，請關閉掛鎖。

### 如何在網頁主控台和雲端主控台中為 Kaspersky Endpoint Security 之前啟動的應用程式選擇信任群組

1. 在網頁主控台的主視窗中，選擇**資產（裝置）→ 政策和設定檔**。
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**"→"**主機入侵防禦**"。

5. 對於“**在 Kaspersky Endpoint Security 前啟動的應用程式信任群組**”設定，選擇合適的“信任群組”。

6. 儲存變更。

**如何選取在 Kaspersky Endpoint Security 啟動之前啟動的應用程式信任群組**

1. 在“應用程式主視窗”中，點擊⚙ 按鈕。

2. 在應用程式設定視窗中，選取”**進階威脅防護**“→“**主機入侵防禦**”。

3. 在「**在 Kaspersky Endpoint Security 之前啟動的應用程式信任群組**」區塊中，選擇合適的信任群組。

4. 儲存變更。

結果，在 Kaspersky Endpoint Security 之前啟動的應用程式將被放入另一個信任群組。然後，Kaspersky Endpoint Security 將根據信任群組封鎖應用程式的操作。

## 選擇未知應用程式的信任群組

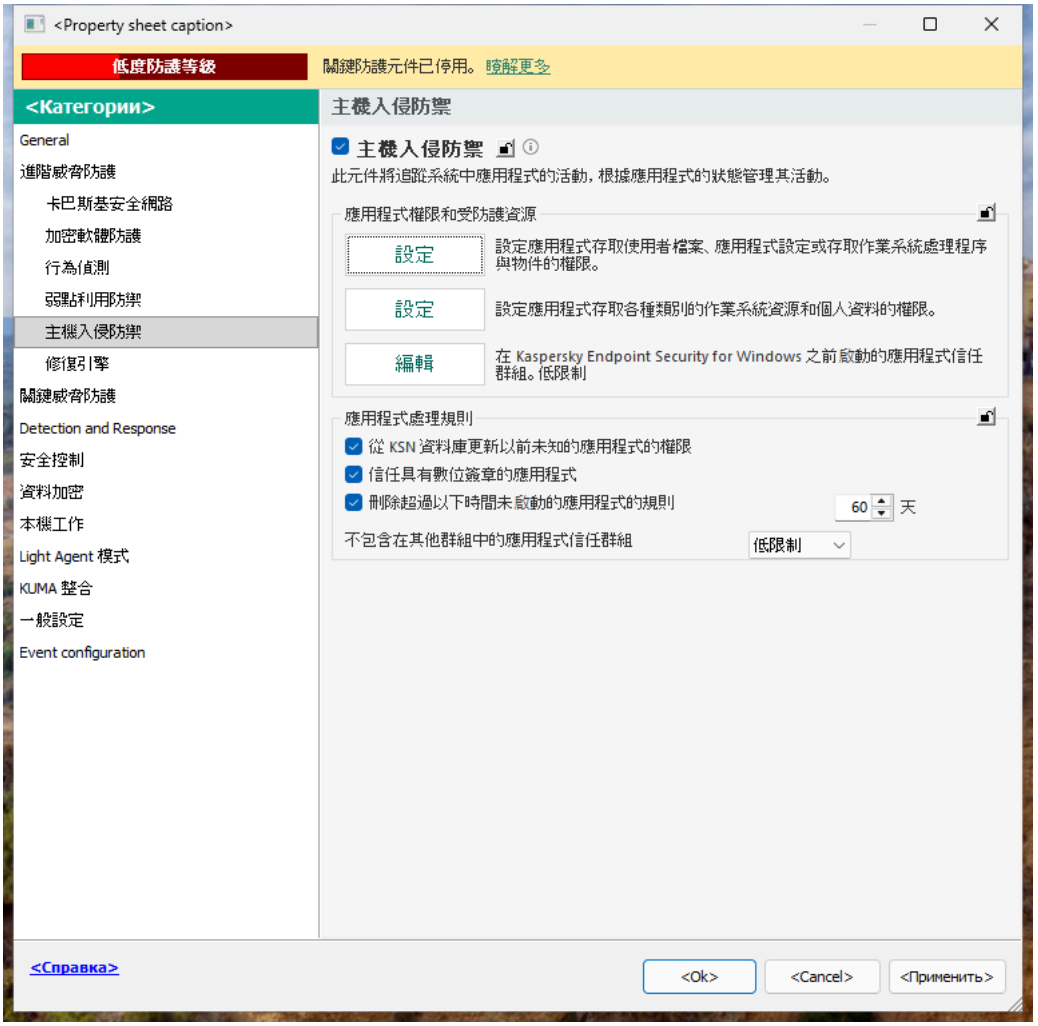
在首次啟動應用程式期間，主機入侵防禦元件將確定該應用程式的信任群組。如果您沒有網際網路存取權限，或者如果卡巴斯基安全網路沒有有關此應用程式的資訊，則預設情況下，Kaspersky Endpoint Security 會將應用程式放入“*低限制*”組。當在 KSN 中偵測到有關先前未知應用程式的資訊時，Kaspersky Endpoint Security 將更新該應用程式的權限。隨後您可以手動編輯應用程式權限。

**如何在管理主控台（MMC）中為未知應用程式選擇信任群組**

1. 在卡巴斯基安全管理中心管理主控台樹狀目錄中，選取**政策**。

2. 選擇必要的政策並點擊以開啟政策內容。

3. 在政策視窗中，選擇“**進階威脅防護 → 主機入侵防禦**”。




入侵防禦設定

4. 在“**應用程式處理規則**“塊中，使用“**不包含在其他群組中的應用程式信任群組**”下拉清單選擇必要的信任群組。

   如果啟用了參與卡巴斯基安全網路，Kaspersky Endpoint Security 會在每次應用程式啟動時向 KSN 傳送有關應用程式信譽的請求。根據收到的回應，應用程式可能會被移動至與“主機入侵防禦”元件設定中指定的信任群組不同的信任群組中。

5. 使用“**從 KSN 資料庫更新以前未知的應用程式的權限**“核取方塊來配置未知應用程式的權限的自動更新。

6. 儲存變更。若要在電腦上套用該政策，請關閉掛鎖。

**如何在網頁主控台和雲端主控台中為未知應用程式選擇信任群組**

1. 在網頁主控台的主視窗中，選擇**資產（裝置）→ 政策和設定檔**。

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**”→”**主機入侵防禦**”。

5. 在“**應用程式處理規則**“塊中，使用“**不包含在其他群組中的應用程式信任群組**”下拉清單選擇必要的信任群組。

   如果啟用了參與卡巴斯基安全網路，Kaspersky Endpoint Security 會在每次應用程式啟動時向 KSN 傳送有關應用程式信譽的請求。根據收到的回應，應用程式可能會被移動至與“主機入侵防禦”元件設定中指定的信任群組不同的信任群組中。

6. 使用“**從 KSN 資料庫更新以前未知的應用程式的權限**”核取方塊來配置未知應用程式的權限的自動更新。

7. 儲存變更。

**如何在應用程式介面中為未知應用程式選擇信任群組**

1. 在“應用程式主視窗”中，點擊⚙按鈕。

2. 在應用程式設定視窗中，選取”**進階威脅防護**“→“**主機入侵防禦**”。

3. 在「**應用程式處理規則**」區塊中，選擇合適的信任群組。

   如果啟用了參與卡巴斯基安全網路，Kaspersky Endpoint Security 會在每次應用程式啟動時向 KSN 傳送有關應用程式信譽的請求。根據收到的回應，應用程式可能會被移動至與“主機入侵防禦”元件設定中指定的信任群組不同的信任群組中。

4. 使用“**從 KSN 為之前未知應用程式更新規則**”核取方塊來配置未知應用程式的權限的自動更新。

5. 儲存變更。

## 為數位簽章應用程式選擇信任群組

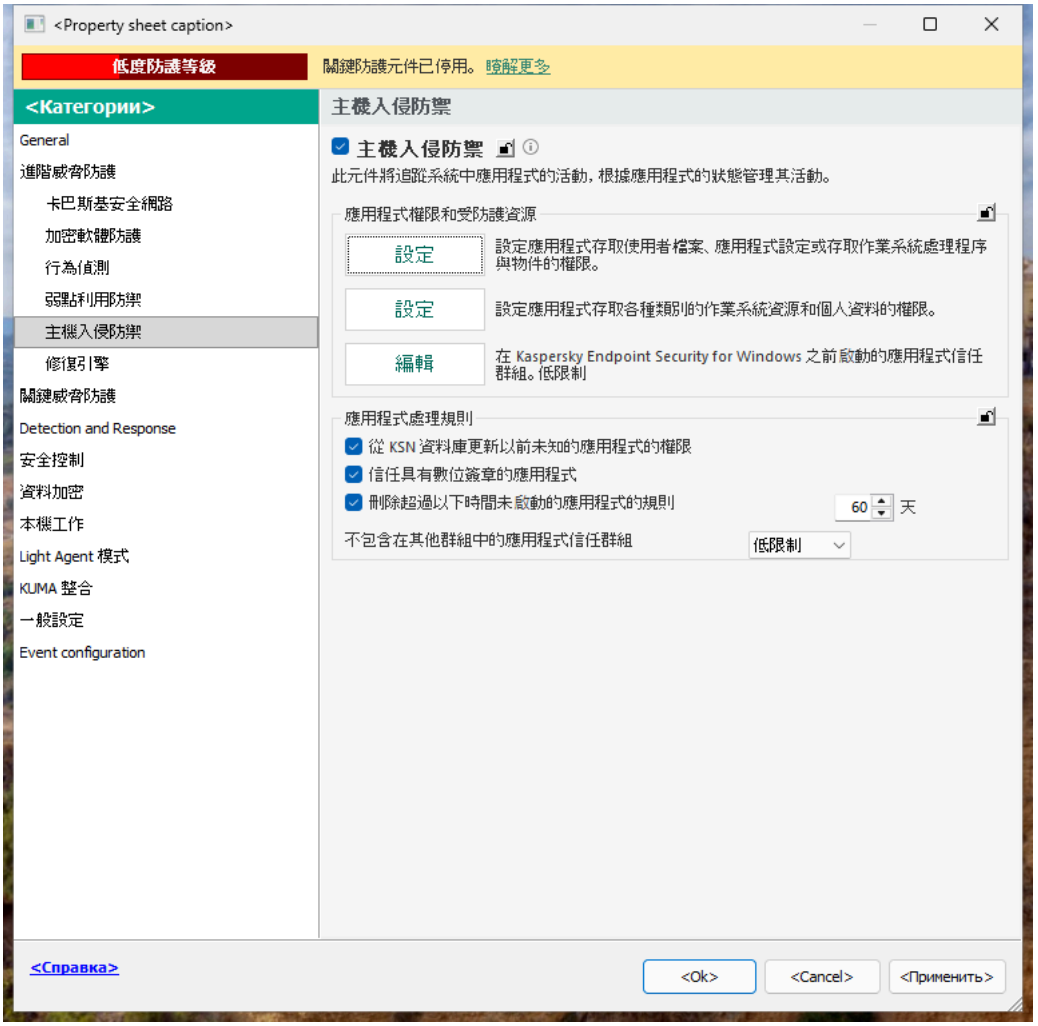
Kaspersky Endpoint Security 總是將帶有 Microsoft 憑證簽章或 Kaspersky 憑證簽章的應用程式放入*受信任*群組。

**如何在管理主控台（MMC）中為數位簽章的應用程式選擇信任群組**

1. 在卡巴斯基安全管理中心管理主控台樹狀目錄中，選取**政策**。

2. 選擇必要的政策並點擊以開啟政策內容。

3. 在政策視窗中，選擇“**進階威脅防護 → 主機入侵防禦**”。




入侵防禦設定

4. 在“**應用程式處理規則**”塊中，使用“**信任具有數位簽章的應用程式**核取方塊來為包含受信任供應商的數位簽章的應用程式啟用或停用自動分配給受信任群組信任群組。

   *受信任供應商*是卡巴斯基包含在受信任群組中的那些软体供應商。您還可以手動將供應商憑證新增到受信任系統憑證儲存中。

   如果清空此核取方塊，“主機入侵防禦”將不再信任經過數位簽章的應用程式，並使用其他參數以確定它們的信任群組。

5. 儲存變更。若要在電腦上套用該政策，請關閉掛鎖。

**如何在網頁主控台和雲端主控台中為數位簽章的應用程式選擇信任群組**

1. 在網頁主控台的主視窗中，選擇**資產（裝置）→ 政策和設定檔**。

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**”→”**主機入侵防禦**”。

5. 在“**應用程式處理規則**”塊中，使用“**信任具有數位簽章的應用程式**核取方塊來為包含受信任供應商的數位簽章的應用程式啟用或停用自動分配給受信任群組信任群組。

   *受信任供應商*是卡巴斯基包含在受信任群組中的那些软体供應商。您還可以手動將供應商憑證新增到受信任系統憑證儲存中。

如果清空此核取方塊，“主機入侵防禦”將不再信任經過數位簽章的應用程式，並使用其他參數以確定它們的信任群組。

6. 儲存變更。

**如何在應用程式介面中為數位簽章的應用程式選擇信任群組**

1. 在“應用程式主視窗”中，點擊⚙按鈕。
2. 在應用程式設定視窗中，選取”**進階威脅防護**“→“**主機入侵防禦**”。
3. 在“**應用程式處理規則**”塊中，使用“**信任具有數位簽章的應用程式**核取方塊來為包含受信任供應商的數位簽章的應用程式啟用或停用自動分配給受信任群組信任群組。

   *受信任供應商*是卡巴斯基包含在受信任群組中的那些软体供應商。您還可以手動將供應商憑證新增到受信任系統憑證儲存中。

   如果清空此核取方塊，“主機入侵防禦”將不再信任經過數位簽章的應用程式，並使用其他參數以確定它們的信任群組。

4. 儲存變更。

# 管理應用程式權限

預設情況下，應用程式活動是根據為 Kaspersky Endpoint Security 首次啟動時分配給該應用程式的特定信任群組定義的應用程式權限來控制的。如有必要，您可以為整個信任群組、單個應用程式或信任群組內的一組應用程式編輯應用程式權限。

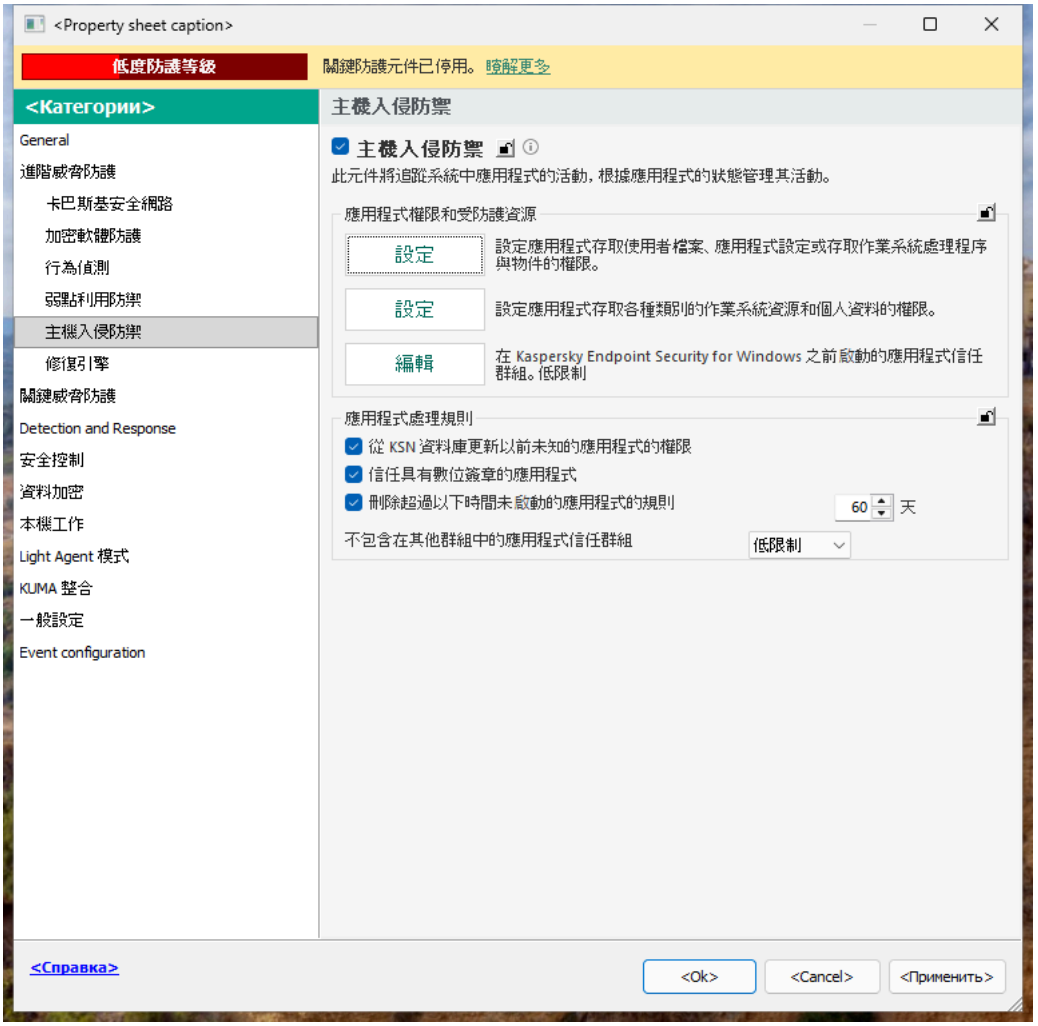
手動定義的應用程式權限比為信任群組定義的應用程式權限具有更高的優先級。換句話說，如果手動定義的應用程式權限與為信任群組定義的應用程式權限不同，則主機入侵防禦元件將根據手動定義的應用程式權限來控制應用程式活動。

您為應用程式建立的規則被子應用程式繼承。例如，如果您拒絕cmd.exe的所有網路活動，則如果使用cmd.exe啟動notepad.exe，則所有網路活動也將被拒絕。當應用程式不是另一個應用程式的子應用程式時，規則不被繼承。

**如何在管理主控台 (MMC) 中變更應用程式權限**

1. 在卡巴斯基安全管理中心管理主控台樹狀目錄中，選取**政策**。
2. 選擇必要的政策並點擊以開啟政策內容。

3. 在政策視窗中，選擇“**進階威脅防護 → 主機入侵防禦**”。




入侵防禦設定

4. 在”**應用程式權限和受防護資源**”塊中，點擊”**設定**”按鈕。

   這將開啟應用程式權限配置視窗和受防護資源的清單。

5. 選擇“**應用程式權限**”標籤。

6. 點擊“**新增**”。

7. 在開啟的視窗中，輸入條件以搜尋要變更其應用程式權限的應用程式。

   您可以輸入應用程式名稱或供應商名稱。Kaspersky Endpoint Security 輸入遮罩時支援環境變量以及`*`和`?`字元。

8. 點擊“**重新整理**”。

   Kaspersky Endpoint Security 將在受管電腦上安裝的應用程式的合併清單中搜尋該應用程式。Kaspersky Endpoint Security 將顯示滿足您搜尋條件的應用程式清單。

9. 選取需要的應用程式。

10. 在“**將選擇應用程式新增至信任群組**”下拉清單中，選擇“**預設群組**”，然後點擊“**確定**”。

    該應用程式將被新增到預設群組。

11. 選擇相關的應用程式，然後從應用程式的內容功能表中選擇“**應用程式權限**”。

    這將開啟應用程式屬性。

12. 請執行以下操作之一：

    - 如果要編輯用作業系統登錄檔、使用者檔案和應用程式設定來管理操作的的信任群組權限，請選取**"檔案和系統登錄檔"**標籤。
    - 如果要編輯管理對作業系統處理程序和物件存取權限的信任群組權限，請選擇**"權限"**標籤。

    防火牆元件使用*網絡規則*控制應用程式的網絡活動。

13. 對於相關資源，在相應操作的列中，右鍵點擊以開啟內容功能表，然後選擇必要的選項：**繼承**，**允許**（ ）或**封鎖**（ ）。

14. 如果要監視電腦資源的使用，請選擇**"記錄事件"**（ / ）。

    Kaspersky Endpoint Security 將記錄有關主機入侵防禦元件操作的資訊。報告包含有關應用程式執行的電腦資源操作的資訊（允許或禁止）。報告還包含有關利用每種資源的應用程式的資訊。

15. 儲存變更。若要在電腦上套用該政策，請關閉掛鎖。

**如何在網頁主控台和雲端主控台中變更程序權限**

1. 在網頁主控台的主視窗中，選擇**資產（裝置）→政策和設定檔**。
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"→"主機入侵防禦"**。
5. 在**"應用程式權限和受防護資源"**塊中，點擊**"應用程式權限和受防護資源"**連接。

   這將開啟應用程式權限配置視窗和受防護資源的清單。

6. 選擇**"應用程式權限"**標籤。

   您將在視窗左側看到信任群組清單，並在右側看到它們的屬性。

7. 點擊**"新增"**。

   這將啟動用於將應用程式新增到信任群組的精靈。

8. 選擇相關應用程式信任群組。
9. 選擇**應用程式**類型。前往下一步。

   如果要變更多個應用程式的信任群組，請選擇**群組**類型並定義應用程式組的名稱。

10. 在開啟的應用程式清單中，選擇要變更其應用程式權限的應用程式。

    使用篩選器。您可以輸入應用程式名稱或供應商名稱。Kaspersky Endpoint Security 輸入遮罩時支援環境變量以及*和?字元。

11. 結束精靈。

    該應用程式將被新增到信任群組。

12. 在視窗左側，選取相關應用程式。

13. 在視窗右側的下拉清單中，執行下列操作之一：

    - 要編輯管理應用程式存取作業系統登錄檔、使用者檔案和應用程式設定的權限的信任群組權限，請選取**"檔案和系統登錄檔"**標籤。
    - 如果要編輯用於管理對作業系統處理程序和物件存取權限的信任群組權限，請選擇**"權限"**。

    防火牆元件使用*網絡規則*控制應用程式的網絡活動。

14. 對於相關資源，在相應操作的列中，選擇必要的選項：**繼承**，**允許**（）、**封鎖**（）。

15. 如果要監視電腦資源的使用，請選擇**"記錄事件"**（ / ）。

    Kaspersky Endpoint Security 將記錄有關主機入侵防禦元件操作的資訊。報告包含有關應用程式執行的電腦資源操作的資訊（允許或禁止）。報告還包含有關利用每種資源的應用程式的資訊。

16. 儲存變更。

**如何在應用程式介面中變更應用程式權限**

1. 在"應用程式主視窗"中，點擊 按鈕。
2. 在應用程式設定視窗中，選取**"進階威脅防護"→"主機入侵防禦"**。
3. 點擊**"管理應用程式"**。

   這將開啟已安裝的應用程式的清單。

4. 選取需要的應用程式。
5. 在應用程式的內容功能表中，選取**"細節和規則"**。

   這將開啟應用程式屬性。

6. 請執行以下操作之一：

    - 如果要編輯用作業系統登錄檔、使用者檔案和應用程式設定來管理操作的的信任群組權限，請選取**"檔案和系統登錄檔"**標籤。
    - 如果要編輯管理對作業系統處理程序和物件存取權限的信任群組權限，請選擇**"權限"**標籤。

7. 對於相關資源，在相應操作的列中，右鍵點擊以開啟內容功能表，然後選擇必要的選項：**繼承**，**允許**（）或**拒絕**（）。
8. 如果要監視電腦資源的使用，請選擇**"記錄事件"**（）。

   Kaspersky Endpoint Security 將記錄有關主機入侵防禦元件操作的資訊。報告包含有關應用程式執行的電腦資源操作的資訊（允許或禁止）。報告還包含有關利用每種資源的應用程式的資訊。

9. 選擇**"排除項目"**標籤並配置應用程式的高級設定（請參閱下表）。
10. 儲存變更。

| 參數 | 描述 |
| --- | --- |
| **開啟前不掃描檔案** | Kaspersky Endpoint Security 的掃描將排除應用程式開啟的所有檔案。例如，如果您正在使用應用程式備份檔案，則此功能有助於減少 Kaspersky Endpoint Security 的資源消耗。 |
| **不監控應用程式活動** | Kaspersky Endpoint Security 將不會監控作業系統中應用程式的檔案和網路活動。您可以為 Kaspersky Endpoint Security 的不同元件設定應用程式活動監控：<br>• **不要為防護和控制元件監控**應用程式活動由以下元件監控：行為偵測，弱點利用防禦，主機入侵防禦，修復引擎和防火牆。<br>• **不要為 Managed Detection and Response 和 Endpoint Detection and Response 監控**應用程式活動由內建 MDR 代理 和 內建 EDR (KATA) 代理監控。<br>• **不要為 Endpoint Detection and Response 攔截主控台互動輸入**Kaspersky Endpoint Security 不會傳送有關在主控台上管理應用程式的遙測資料。遙測資料由 Kaspersky Anti Targeted Attack Platform (EDR) 使用。 |
| **不繼承父處理程序(應用程式)的限制** | Kaspersky Endpoint Security 不會將為父程序配置的限制套用於子程序。父程序由配置了應用程式權限（主機入侵防禦）和應用程式網路規則（防火牆）的應用程式啟動。 |
| **不監控子應用程式活動** | Kaspersky Endpoint Security 將不會監控該應用程式啟動的應用程式的檔案活動或網路活動。您可以遞歸套用排除項目。這樣應用程式就不會監視整個子應用程式鏈的活動。 |
| **允許與 Kaspersky Endpoint Security 的應用程式介面進行互動** | Kaspersky Endpoint Security 自我防護可封鎖從遠端電腦管理應用程式服務的所有嘗試。如果選擇該核取方塊，則允許遠端存取應用程式透過 Kaspersky Endpoint Security 介面管理 Kaspersky Endpoint Security 設定。 |
| **不掃描加密流量/不掃描所有流量** | Kaspersky Endpoint Security 將從掃描中排除由應用程式啟動的網路流量。您可以從掃描中排除所有流量或僅排除加密流量。您也可以從掃描中排除單個 IP 位址和連接埠號。 |

# 防護作業系統資源和个人資料

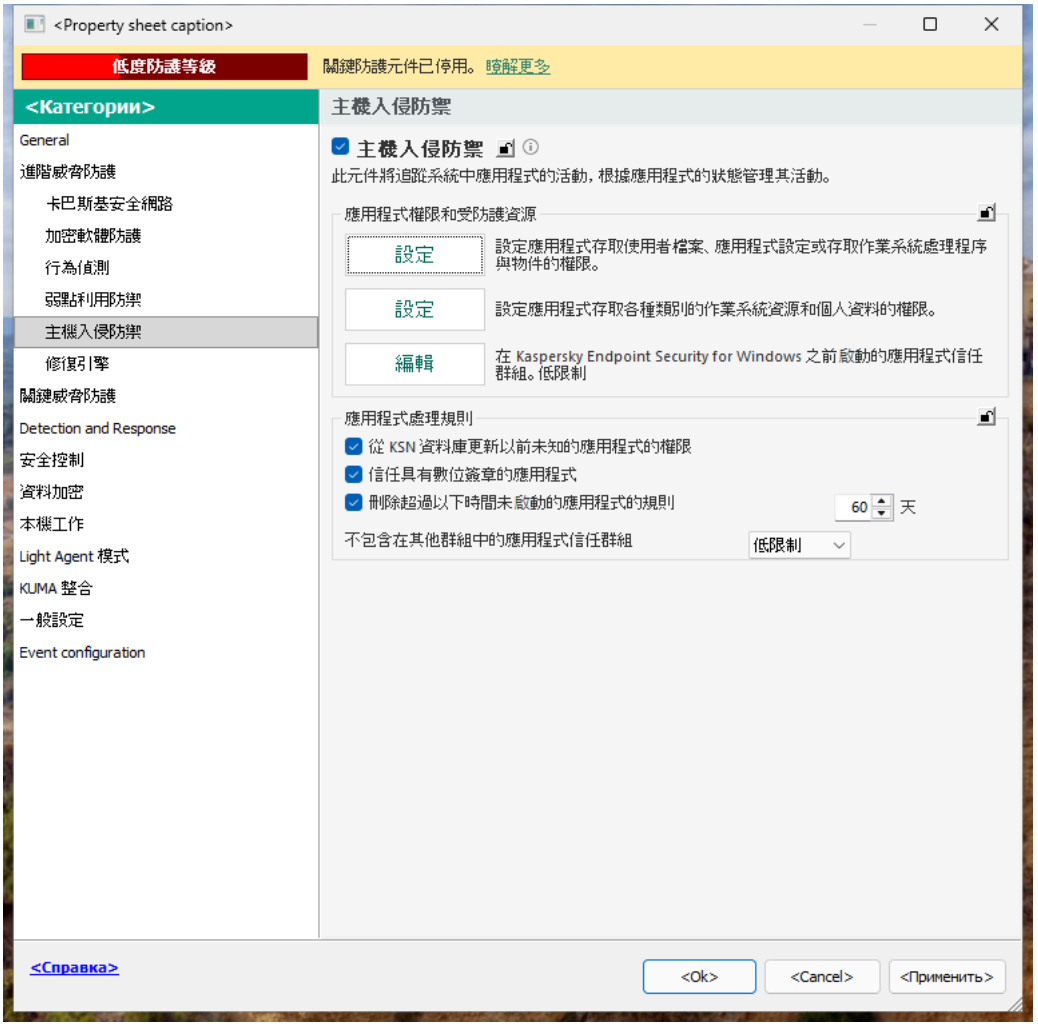
"主機入侵防禦"元件管理應用程式處理各種不同類別作業系統資源和個人資料的權限。Kaspersky 專家已建立受防護資源的預設類別。例如，"*作業系統*"類別具有"*啟動設定*"子類別，該子類別列出了與應用程式自動執行相關的所有登錄機碼。您無法編輯或刪除受防護資源的預設類別，或這些類別中的受防護資源。

### 如何在管理主控台 (MMC) 中新增受防護資源

1. 在卡巴斯基安全管理中心管理主控台樹狀目錄中，選取**政策**。

2. 選擇必要的政策並點擊以開啟政策內容。

3. 在政策視窗中，選擇“**進階威脅防護 → 主機入侵防禦**”。




入侵防禦設定

4. 在”**應用程式權限和受防護資源**”塊中，點擊”**設定**”按鈕。

   這將開啟應用程式權限配置視窗和受防護資源的清單。

5. 選擇“**受防護資源**”標籤。

   您將在視窗左側看到受防護資源的清單，以及根據特定信任群組存取這些資源的相應權限。

6. 選擇要向其新增受防護資源的受防護資源類別。

   如果要新增子類別，請點擊**新增→類別**。

7. 點擊”**新增**“按鈕。在下拉清單中，選擇要新增的資源類型：**檔案或資料夾**或**登錄機碼**。

8. 在開啟的視窗中，選擇檔案、資料夾或登錄機碼。

   您可以檢視應用程式的權限以存取新增的資源。為此，請在視窗的左側選擇新增的資源，Kaspersky Endpoint Security 將顯示每個信任群組的存取權限。您還可以透過使用新資源旁邊的核取方塊來停用對包含資源的應用程式活動的控制。

9. 儲存變更。若要在電腦上套用該政策，請關閉掛鎖。

**如何在網頁主控台和雲端主控台中新增受防護資源**

1. 在網頁主控台的主視窗中，選擇**資產（裝置）→政策和設定檔**。
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"→"主機入侵防禦"**。
5. 在**"應用程式權限和受防護資源"**塊中，點擊**"應用程式權限和受防護資源"**連接。
   這將開啟應用程式權限配置視窗和受防護資源的清單。
6. 選擇**"受防護資源"**標籤。
   您將在視窗左側看到受防護資源的清單，以及根據特定信任群組存取這些資源的相應權限。
7. 點擊**"新增"**。
   新資源精靈啟動。
8. 點擊**群組名稱**區塊，選擇要向其新增受防護資源的受防護資源類別。
   如果要新增子類別，請選擇**受防護資源的類別**選項。
9. 選擇要新增的資源類型：**檔案或資料夾**或**登錄機碼**。
10. 選擇一個檔案、資料夾或登錄機碼。
11. 結束精靈。
    您可以檢視應用程式的權限以存取新增的資源。為此，請在視窗的左側選擇新增的資源，Kaspersky Endpoint Security 將顯示每個信任群組的存取權限。您還可以使用**"狀態"**列中的核取方塊停用控制有資源的應用程式活動。
12. 儲存變更。

**如何在應用程式介面中新增受防護資源**

1. 在"應用程式主視窗"中，點擊⚙ 按鈕。
2. 在應用程式設定視窗中，選取**"進階威脅防護"→"主機入侵防禦"**。
3. 點擊**"管理資源"**。
   受防護資源清單開啟。
4. 選擇要向其新增受防護資源的受防護資源類別。
   如果要新增子類別，請點擊**新增→類別**。
5. 點擊**"新增"**按鈕。在下拉清單中，選擇要新增的資源類型：**檔案或資料夾**或**登錄機碼**。

6. 在開啟的視窗中，選擇檔案、資料夾或登錄機碼。

   您可以檢視應用程式的權限以存取新增的資源。為此，請在視窗的左側選擇新增的資源，Kaspersky Endpoint Security 將顯示應用程式清單以及每個應用程式的存取權限。您還可以透過使用**狀態**列中的**啟用控制**按鈕來停用對有資源的應用程式活動的控制。

7. 儲存變更。

Kaspersky Endpoint Security 將控制對新增的作業系統資源和個人資料的存取。Kaspersky Endpoint Security根據分配給該應用程式的信任群組控制應用程式對資源的存取。您可以手動變更應用程式的信任群組。

# 刪除有關未使用之應用程式的資訊

Kaspersky Endpoint Security 使用應用程式權限來控制應用程式的活動。應用程式權限由其信任群組確定。首次啟動應用程式時，Kaspersky Endpoint Security 會將應用程式放入信任群組。您可以手動變更應用程式的信任群組。您還可以手動配置單一應用程式的權限。Kaspersky Endpoint Security 儲存有關應用程式的以下資訊：應用程式的信任群組和應用程式的權限。

Kaspersky Endpoint Security 會自動刪除有關未使用的應用程式資訊以節省電腦資源。Kaspersky Endpoint Security 根據以下規則刪除應用程式資訊：

- 如果應用程式的信任組和權限已自動確認，Kaspersky Endpoint Security 將在 30 天後刪除有關此應用程式的訊息。不能變更應用程式訊息的儲存期限或關閉自動刪除。
- 如果您手動將應用程式放入信任群組或配置其存取權限，Kaspersky Endpoint Security 將在 60 天（預設儲存期限）後刪除有關此應用程式的資訊。您可以變更應用程式資訊的儲存期限，或關閉自動刪除（請參見下面說明）。

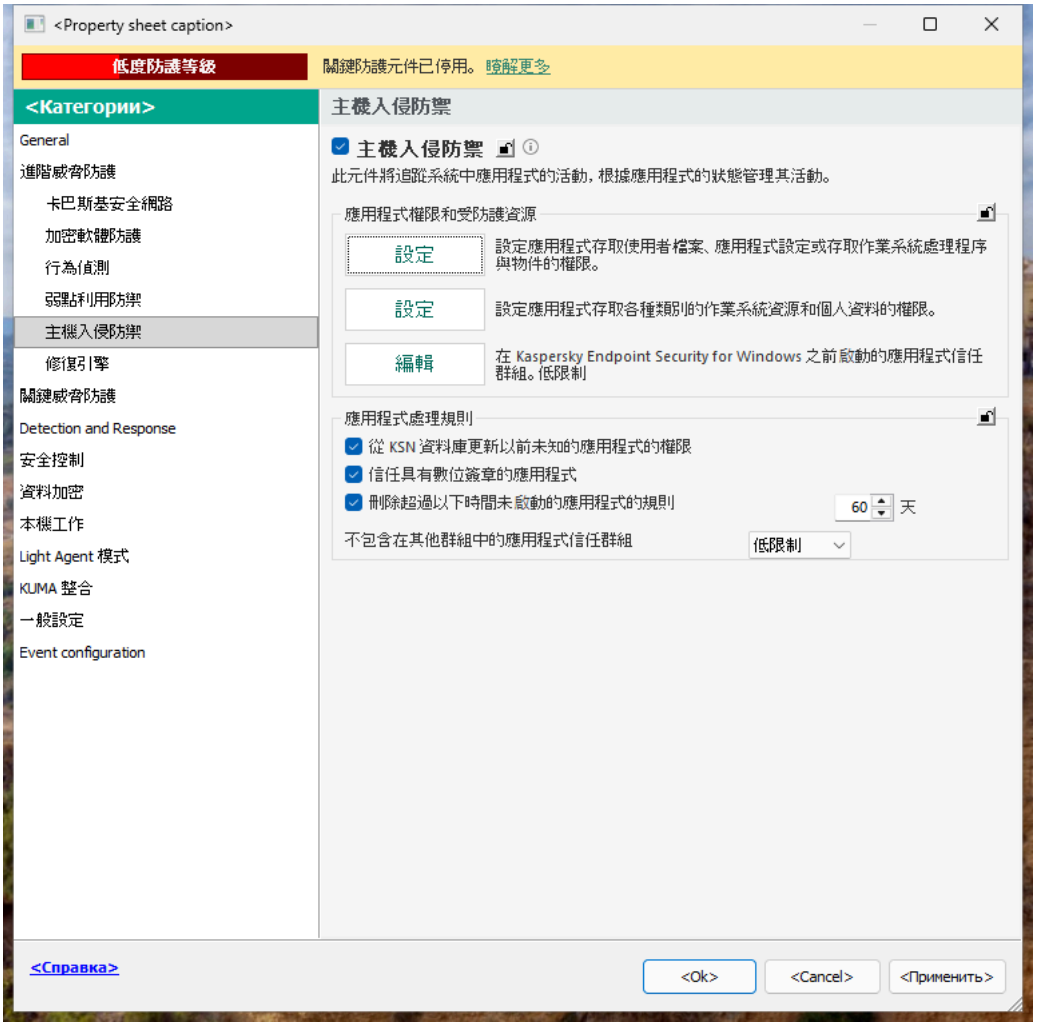
當啟動資訊已被刪除的應用程式時，Kaspersky Endpoint Security 會像首次啟動該應用程式一樣對其進行分析。

**如何在管理主控台（MMC）中配置自動刪除有關未使用的應用程式的資訊**

1. 在卡巴斯基安全管理中心管理主控台樹狀目錄中，選取**政策**。

2. 選擇必要的政策並點擊以開啟政策內容。

3. 在政策視窗中，選擇“**進階威脅防護 → 主機入侵防禦**”。




入侵防禦設定

4. 在“**應用程式處理規則**”塊中執行以下操作之一：

   - 如果要配置自動刪除，請選擇**刪除超過以下時間未啟動的應用程式的規則 N 天**核取方塊並輸入天數。

     您手動放入信任群組或手動設定其存取權限的應用程式相關資訊在定義的天數後將被 Kaspersky Endpoint Security 刪除。有關已自動確定其信任群組和應用程式權限的應用程式資訊也將在 30 天後被 Kaspersky Endpoint Security 刪除。

   - 如果要關閉自動刪除，請清除“**刪除超過以下時間未啟動的應用程式的規則 N 天**”核取方塊。

     您手動放入信任群組或手動設定其存取權限的應用程式相關資訊將被 Kaspersky Endpoint Security 無限期儲存，且沒有任何儲存期限。Kaspersky Endpoint Security 在 30 天後將只刪除已自動確定其信任群組和應用程式權限之應用程式的相關資訊。

5. 儲存變更。若要在電腦上套用該政策，請關閉掛鎖。

**如何在網頁主控台和雲端主控台中配置有關未使用應用程式的資訊的自動刪除**

1. 在網頁主控台的主視窗中，選擇**資產（裝置） → 政策和設定檔**。

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**”→”**主機入侵防禦**”。

5. 在“**應用程式處理規則**”塊中執行以下操作之一：

   - 如果要配置自動刪除，請選擇 **刪除超過 (天，1 至 90) 天未啟動的應用程式的規則**核取方塊並輸入天數。

     您手動放入信任群組或手動設定其存取權限的應用程式相關資訊在定義的天數後將被 Kaspersky Endpoint Security 刪除。有關已自動確定其信任群組和應用程式權限的應用程式資訊也將在 30 天後被 Kaspersky Endpoint Security 刪除。

   - 如果要關閉自動刪除，請清除“**刪除超過 (天，1 至 90) 天未啟動的應用程式的規則**”核取方塊。

     您手動放入信任群組或手動設定其存取權限的應用程式相關資訊將被 Kaspersky Endpoint Security 無限期儲存，且沒有任何儲存期限。Kaspersky Endpoint Security 在 30 天後將只刪除已自動確定其信任群組和應用程式權限之應用程式的相關資訊。

6. 儲存變更。

**如何在應用程式介面中配置有關未使用的應用程式的資訊的自動刪除**

1. 在“應用程式主視窗”中，點擊⚙ 按鈕。

2. 在應用程式設定視窗中，選取”**進階威脅防護**“→“**主機入侵防禦**”。

3. 在“**應用程式處理規則**”塊中執行以下操作之一：

   - 如果要配置自動刪除，請選擇**刪除超過以下時間未啟動的應用程式的規則 N 天 (從 1 到 90)**核取方塊並輸入天數。

     您手動放入信任群組或手動設定其存取權限的應用程式相關資訊在定義的天數後將被 Kaspersky Endpoint Security 刪除。有關已自動確定其信任群組和應用程式權限的應用程式資訊也將在 30 天後被 Kaspersky Endpoint Security 刪除。

   - 如果要關閉自動刪除，請清除“**刪除超過以下時間未啟動的應用程式的規則 N 天 (從 1 到 90)**”核取方塊。

     您手動放入信任群組或手動設定其存取權限的應用程式相關資訊將被 Kaspersky Endpoint Security 無限期儲存，且沒有任何儲存期限。Kaspersky Endpoint Security 在 30 天後將只刪除已自動確定其信任群組和應用程式權限之應用程式的相關資訊。

4. 儲存變更。

# 監控主機入侵防禦

您可以收到有關主機入侵防禦元件操作的報告。報告包含有關應用程式執行的電腦資源操作的資訊（允許或禁止）。報告還包含有關利用每種資源的應用程式的資訊。

要監視主機入侵防禦操作，您需要啟用報告寫作功能。例如，您可以在主機入侵防禦元件設定中為單個應用程式啟用報告轉發。

在配置主機入侵防禦監視時，將事件轉發到卡巴斯基安全管理中心時請考慮潛在的網路負載。您還可以僅在 Kaspersky Endpoint Security 的本機記錄中啟用報告儲存。

# 防護對音訊和視訊的存取

網路罪犯可以使用特殊程式來嘗試存取記錄音訊和視訊的裝置（例如麥克風或網路攝影機）。Kaspersky Endpoint Security 可控制應用程式何時接收音訊資料流或視訊資料流，並防護資料免遭未經授權的攔截。

預設情況下，Kaspersky Endpoint Security 僅允許從*受信任*群組接收應用程式的音訊和視訊串流。來自 *低限制*, *高限制* 和 *不信任* 群組的應用程式不被允許接收來自裝置的音訊串流和視訊串流。您可以手動允許應用程式接收音訊資料流和視訊資料流。

## 音訊資料流防護的特殊功能

音訊資料流防護有以下特性：

- 必須啟用"主機入侵防禦"元件，此功能才有效。
- 如果在"主機入侵防禦"元件啟動之前該應用程式開始接受音訊資料流，則 Kaspersky Endpoint Security 允許該應用程式接收音訊資料流且不顯示任何通知。
- 如果您在應用程式開始接收音訊資料流之後將該應用程式移動至"*不信任*"群組或"*高限制*"群組，Kaspersky Endpoint Security 將允許應用程式接收音訊資料流且不顯示任何通知。
- 應用程式存取錄音裝置的設定被變更後（例如，如果封鎖了應用程式接收音訊資料流），則必須重新啟動該應用程式才能封鎖其繼續接收音訊資料流。
- 控制對錄音裝置音訊資料流的存取不取決於應用程式的鏡頭存取設定。
- Kaspersky Endpoint Security 僅防護對內建麥克風和外建麥克風的存取。不支援其他音訊資料流裝置。
- Kaspersky Endpoint Security 無法防護對其他諸如單反相機、攜帶式錄影機和動作捕捉相機中音訊資料流的防護。
- 當您在安裝 Kaspersky Endpoint Security 之後首次執行音訊和視訊錄製或播放應用程式時，音訊和視訊播放或錄製可能會被中斷。為了確保該功能能夠控制應用程式對錄音裝置的存取，這是必要的。Kaspersky Endpoint Security 首次執行時控制音訊硬體的系統裝置將重新開機。

## 應用程式網路攝影機存取防護的特殊功能

網路攝影機存取防護功能擁有以下特別考慮和限制：

- 應用程式將控制從處理鏡頭資料而來的視訊和靜止影像。
- 應用程式將控制視訊流，如果其作為鏡頭接收視訊流的一部分。
- 應用程式僅控制在 Windows 裝置管理員中顯示為"影像裝置"透過 USB 或 IEEE1394 連線的鏡頭。

- Kaspersky Endpoint Security 支援以下鏡頭：
  - Logitech HD Webcam C270
  - Logitech HD Webcam C310
  - Logitech Webcam C210
  - Logitech Webcam Pro 9000
  - Logitech HD Webcam C525
  - Microsoft LifeCam VX-1000
  - Microsoft LifeCam VX-2000
  - Microsoft LifeCam VX-3000
  - Microsoft LifeCam VX-800
  - Microsoft LifeCam Cinema。

Kaspersky 不保證支援不在清單中的鏡頭。

# BadUSB 攻擊防護

某些病毒會修改 USB 裝置的固件以欺騙作業系統，將 USB 偽裝為鍵盤。結果，該病毒可能在您的使用者帳戶下執行命令以下載惡意軟體（例如）。

BadUSB 攻擊防護元件可以防止受感染的模擬鍵盤的 USB 裝置連線至電腦。

當 USB 裝置連線到電腦並被作業系統識別為鍵盤時，應用程式會提示使用者用該鍵盤或螢幕鍵盤（如適用）輸入由應用程式產生的數字代碼（請參閱下圖）。這個步驟稱為鍵盤授權。

如果輸入的代碼正確，應用程式會將識別參數（鍵盤的 VID/PID 及其所連接的連接埠號碼）儲存在授權鍵盤清單之中。重新啟動作業系統後重新連線鍵盤時無需重複鍵盤授權。

經授權的鍵盤連接至該電腦不同 USB 連接埠時，程式將再次提示為該鍵盤授權。

如果錯誤輸入數位代碼，則程式將生成新的代碼。您可以設定輸入數位代碼的嘗試次數。如果數位代碼多次輸入不正確，或者鍵盤授權視窗被關閉（請見下圖），則應用程式封鎖來自此鍵盤的輸入。當 USB 裝置封鎖時間經過或者作業系統重新啟動後，程式將再次提示使用者重新執行鍵盤授權。

程式將允許使用經過授權的鍵盤並封鎖未經授權的鍵盤。

預設情況下，未安裝"BadUSB 攻擊防護"元件。如果需要"BadUSB 攻擊防護"元件，可以在安裝應用程式前在安裝套件的內容中新增該元件，或者在安裝應用程式後變更可用的應用程式元件。




*鍵盤授權*

# 啟用和停用 BadUSB 攻擊防護

在 BadUSB 攻擊防護元件安裝前被電腦識別為鍵盤的 USB 裝置在該元件安裝後仍將被認定為經過授權。

**如何在管理主控台（MMC）中啟用或停用 BadUSB 攻擊防護**

1. 在卡巴斯基安全管理中心管理主控台樹狀目錄中，選取**政策**。
2. 選擇必要的政策並點擊以開啟政策內容。
3. 在政策視窗中，選擇"**關鍵威脅防護 → BadUSB 攻擊防護**"。
4. 使用"**BadUSB 攻擊防護**"核取方塊來啟用或停用元件。
5. 在"**連線時的 USB 裝置授權**"塊中，調節授權碼輸入安全設定：
   - **USB 裝置授權嘗試最大次數**在授權碼不正確輸入達到指定次數時自動封鎖 USB 裝置。有效值為 1 到 10。例如，如果您允許嘗試輸入授權碼五次，則應用程式會在第五次嘗試失敗後封鎖 USB 裝置。Kaspersky Endpoint Security 會顯示 USB 裝置的封鎖時長。該時間經過後，您可以有 5 次嘗試輸入授權碼。
   - **達到嘗試的最大次數時的逾時（分鐘）**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。有效值為 1 到 180（分鐘）。
6. 儲存變更。若要在電腦上套用該政策，請關閉掛鎖。

**如何在網頁主控台和雲端主控台中啟用或停用 BadUSB 攻擊防護**

1. 在網頁主控台的主視窗中，選擇**資產（裝置）→ 政策和設定檔**。
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. 使用“**BadUSB 攻擊防護已啟用**“切換開關可啟用或停用元件。

6. 在“**USB 裝置授權**”塊中，調節授權碼輸入安全設定：

   - **USB 裝置授權嘗試最大數量**在授權碼不正確輸入達到指定次數時自動封鎖 USB 裝置。有效值為 1 到 10。例如，如果您允許嘗試輸入授權碼五次，則應用程式會在第五次嘗試失敗後封鎖 USB 裝置。Kaspersky Endpoint Security 會顯示 USB 裝置的封鎖時長。該時間經過後，您可以有 5 次嘗試輸入授權碼。

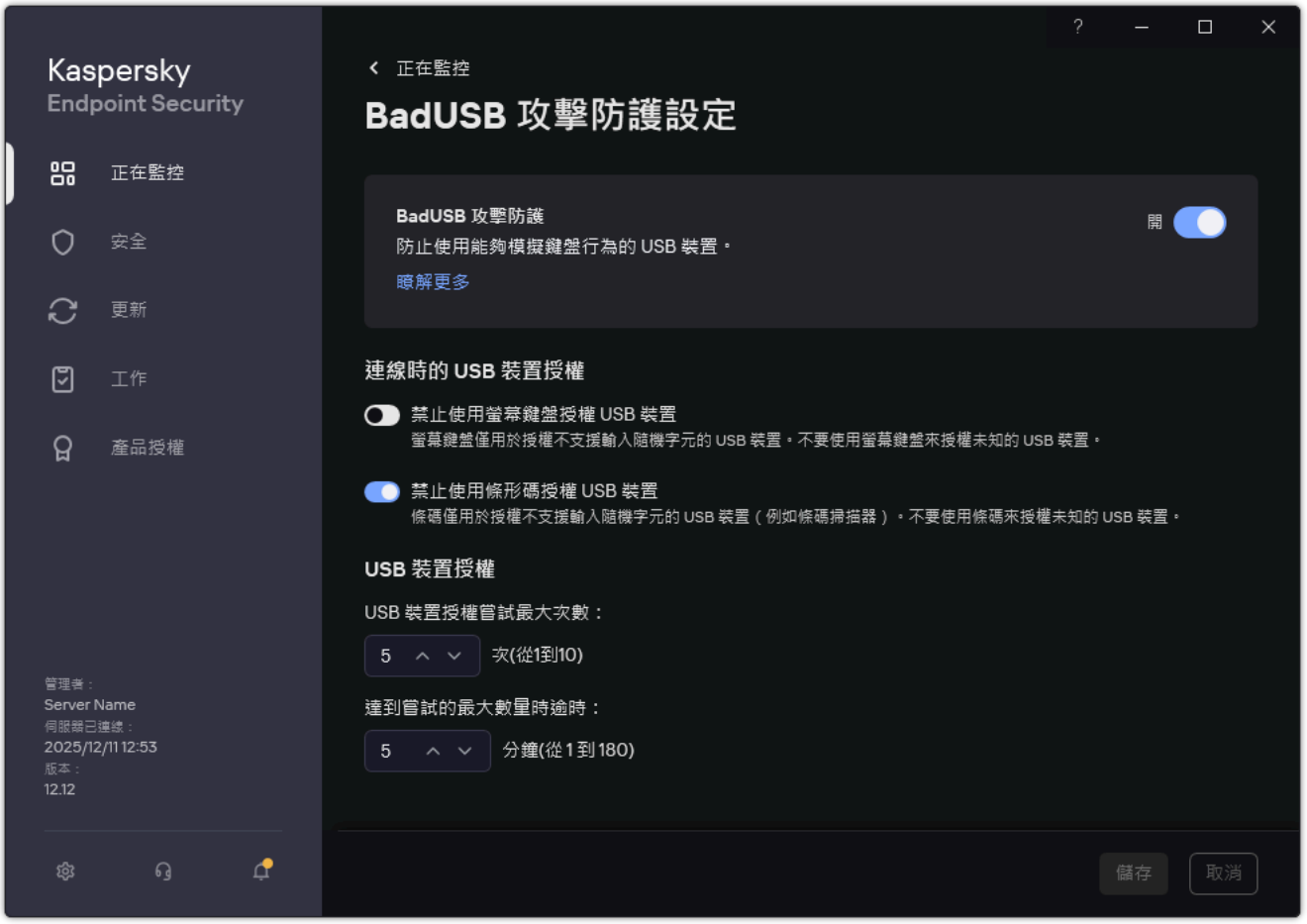
   - **達到最大嘗試次數時逾時（分鐘）**在指定次數的授權碼輸入失敗後，USB 裝置被封鎖的持續時間。有效值為 1 到 180（分鐘）。

7. 儲存變更。

### 如何在應用程式介面中啟用或停用 BadUSB 攻擊防護

1. 在“應用程式主視窗”中，點擊⚙ 按鈕。

2. 在應用程式設定視窗中，選取”**關鍵威脅防護**“→“**BadUSB 攻擊防護**”。




BadUSB 攻擊防護元件設定

3. 使用“**BadUSB 攻擊防護**“切換開關可啟用或停用元件。

4. 在**"連線時的 USB 裝置授權"**塊中，調節授權碼輸入安全設定：

   - **USB 裝置授權嘗試最大次數**在授權碼不正確輸入達到指定次數時自動封鎖 USB 裝置。有效值為 1 到 10。例如，如果您允許嘗試輸入授權碼五次，則應用程式會在第五次嘗試失敗後封鎖 USB 裝置。Kaspersky Endpoint Security 會顯示 USB 裝置的封鎖時長。該時間經過後，您可以有 5 次嘗試輸入授權碼。

   - **達到嘗試的最大數量時逾時**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。有效值為 1 到 180（分鐘）。

5. 儲存變更。

因此，如果啟用了 BadUSB 攻擊防護，則 Kaspersky Endpoint Security 要求對作業系統識別為鍵盤的已連線USB 裝置進行授權。鍵盤經過授權前使用者無法使用該鍵盤。

# 使用螢幕鍵盤授權 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。

**如何在管理主控台 (MMC) 中允許或禁止使用螢幕鍵盤進行授權**

1. 在卡巴斯基安全管理中心管理主控台樹狀目錄中，選取**政策**。

2. 選擇必要的政策並點擊以開啟政策內容。

3. 在政策視窗中，選擇**"關鍵威脅防護 → BadUSB 攻擊防護"**。

4. 請使用**"禁止使用螢幕鍵盤授權 USB 裝置"**核取方塊來封鎖或允許使用螢幕鍵盤進行授權。

5. 儲存變更。

**如何在網頁主控台和雲端主控台中允許或禁止使用螢幕鍵盤進行授權**

1. 在網頁主控台的主視窗中，選擇**資產（裝置）→ 政策和設定檔**。

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。

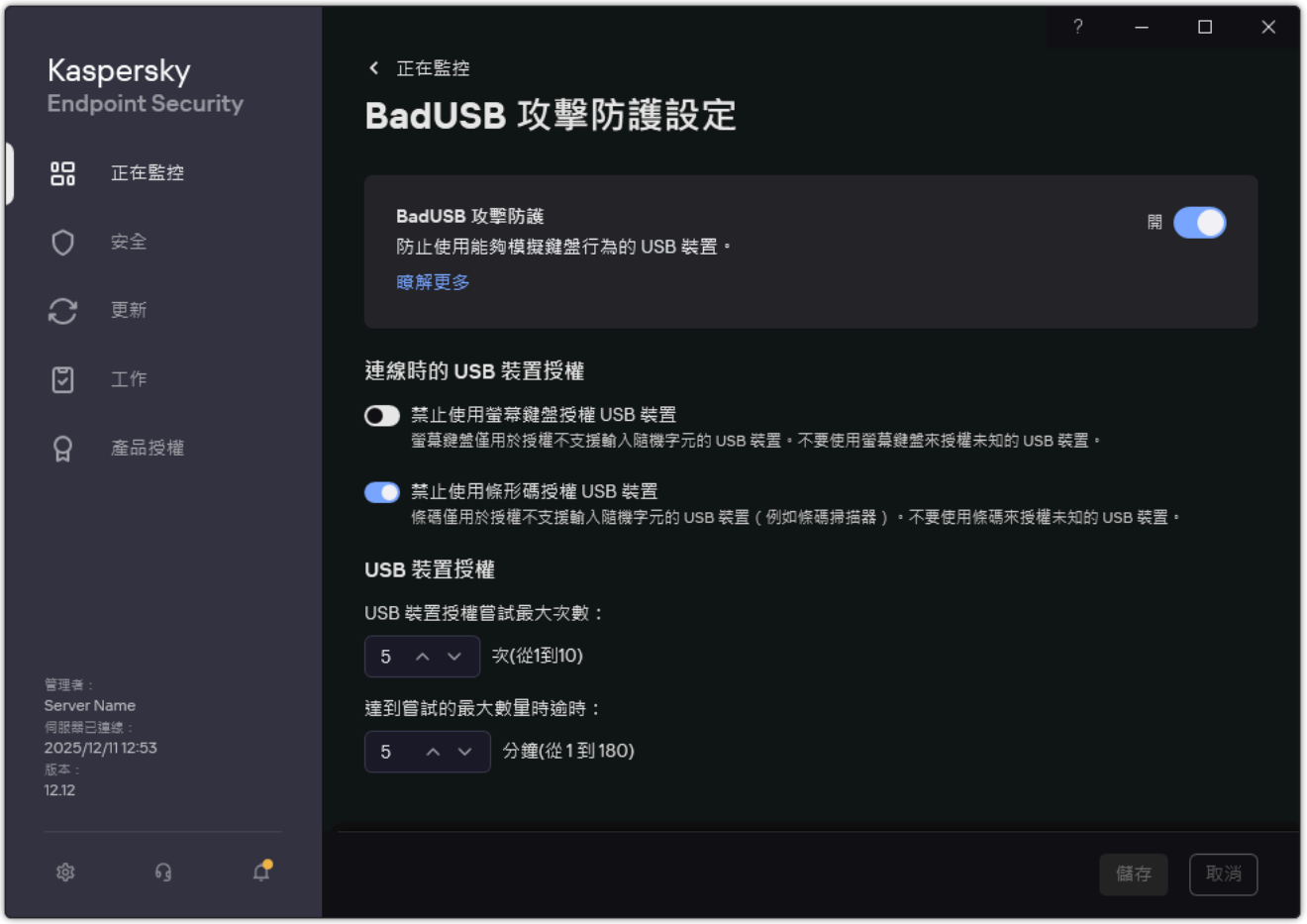
4. 轉到**"主機威脅防護"→"BadUSB 攻擊防護"**。

5. 請使用**"禁止使用螢幕鍵盤授權 USB 裝置"**開關來封鎖或允許使用螢幕鍵盤進行授權。

6. 儲存變更。

### 如何在應用程式介面中允許或禁止使用螢幕鍵盤進行授權

1. 在“應用程式主視窗”中，點擊⚙按鈕。
2. 在應用程式設定視窗中，選取”**關鍵威脅防護**“→“**BadUSB 攻擊防護**”。




BadUSB 攻擊防護元件設定

3. 請使用"**禁止使用螢幕鍵盤授權 USB 裝置**"開關來封鎖或允許使用螢幕鍵盤進行授權。

4. 儲存變更。




USB 裝置授權

# 條碼掃描器授權

當將條碼掃描器連線到電腦時，BadUSB 攻擊防護元件會將此裝置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，大多數條碼和 QR 代碼掃描器支援此格式。

Kaspersky Endpoint Security 也支援另一種條碼掃描器授權方法。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。

**如何在管理主控台（mmc）中透過條碼啟用 USB 裝置授權**

1. 開啟卡巴斯基安全管理中心管理主控台。

2. 在主控台樹狀目錄中，選擇"**政策**"。

3. 選擇必要的政策並點擊以開啟政策內容。

4. 在政策視窗中，選擇"**關鍵威脅防護 → BadUSB 攻擊防護**"。

5. 請使用"**禁止使用條形碼授權 USB 裝置**"核取方塊來封鎖或允許使用條碼進行授權。

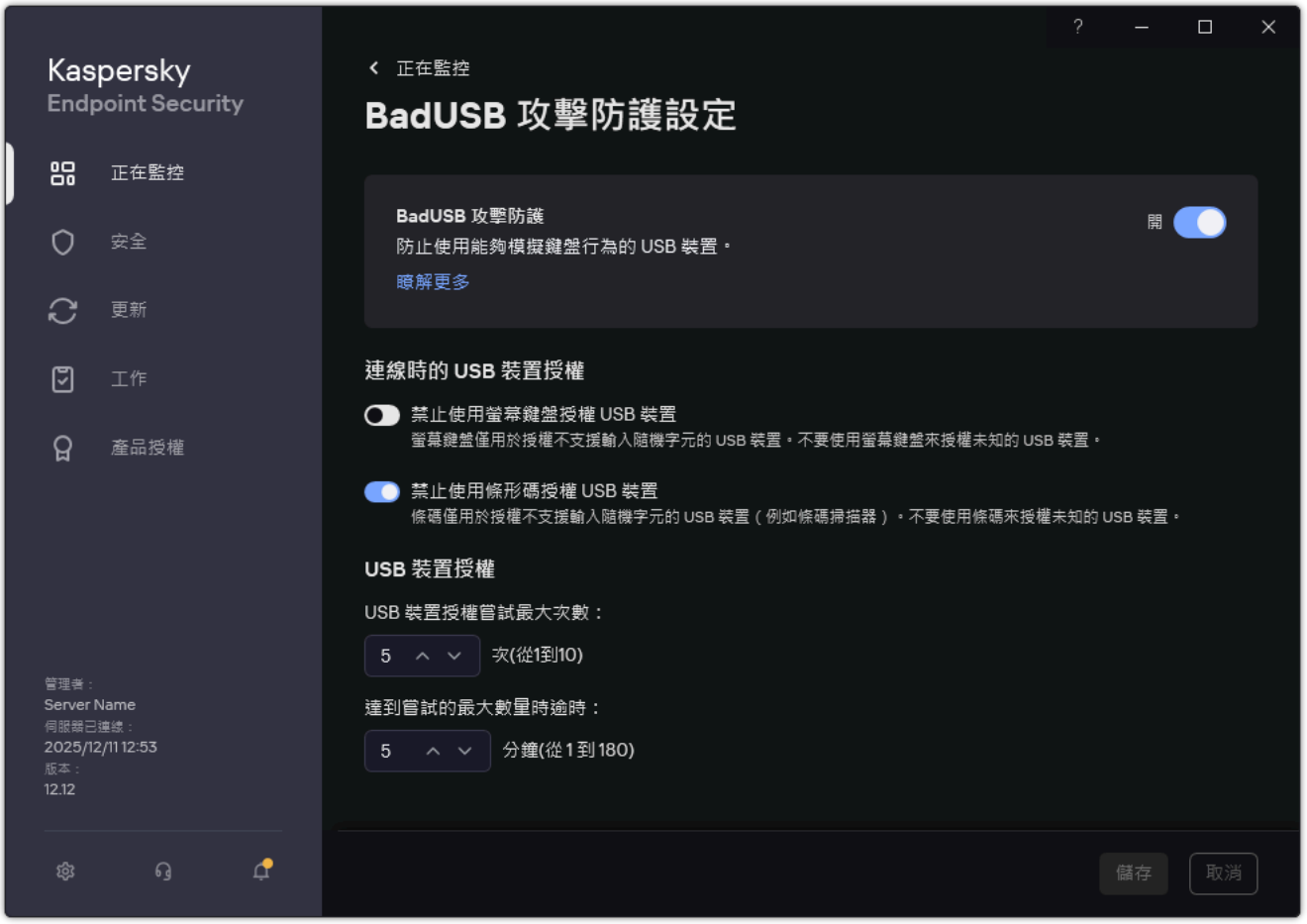
6. 儲存變更。若要在電腦上套用該政策，請關閉掛鎖。

### 如何在網頁主控台和雲端主控台中啟用透過條碼進行 USB 裝置授權

1. 在網頁主控台的主視窗中，選擇**資產（裝置）** → **政策和設定檔**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"**主機威脅防護**"→"**BadUSB 攻擊防護**"。
5. 請使用"**禁止使用條形碼授權 USB 裝置**"開關來封鎖或允許使用條碼進行授權。
6. 儲存變更。若要在電腦上套用該政策，請關閉掛鎖。

### 如何在應用程式介面中透過條碼啟用 USB 裝置授權

1. 在"應用程式主視窗"中，點擊 按鈕。
2. 在應用程式設定視窗中，選取"**關鍵威脅防護**"→"**BadUSB 攻擊防護**"。




BadUSB 攻擊防護元件設定

3. 請使用"**禁止使用條形碼授權 USB 裝置**"開關來封鎖或允許使用條碼進行授權。

4. 儲存變更。

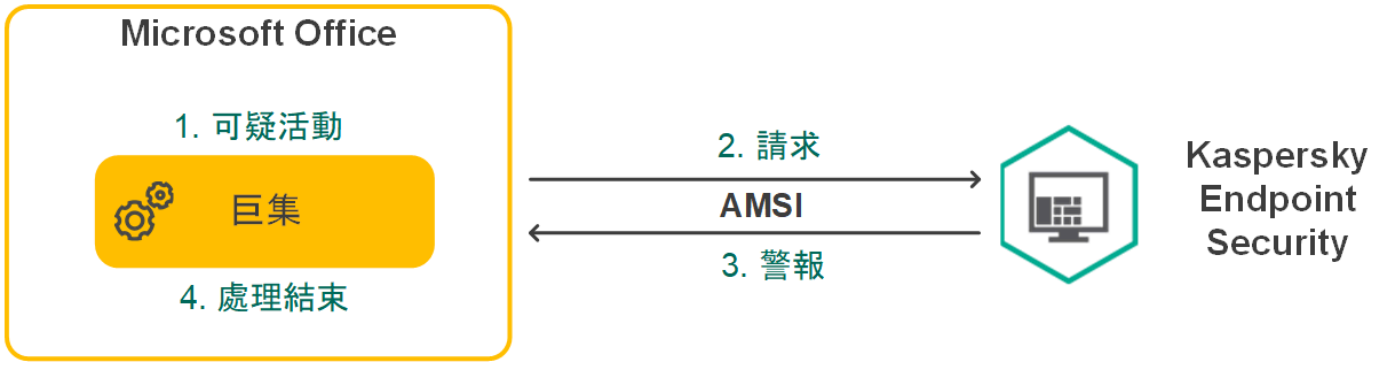



條碼掃描器授權

# AMSI 防護

AMSI 防護元件設計用於支援 Microsoft 的反惡意軟件掃描接口。*惡意軟體防護掃描介面 (AMSI)* 允許具有 AMSI 支援的協力廠商應用程式將物件（例如，PowerShell 指令碼）傳送到 Kaspersky Endpoint Security 進行附加掃描，然後接收這些物件的掃描結果。例如，協力廠商應用程式可能包括 Microsoft Office 應用程式（請參見下圖）。有關 AMSI 的詳細資訊，請參閱 Microsoft 文件。

AMSI 防護元件只能偵測威脅並將偵測到的威脅通知給協力廠商應用程式。在收到威脅通知後，協力廠商應用程式將不允許惡意操作（例如，終止操作）。




AMSI 操作示範

AMSI 防護元件可能會拒絕協力廠商應用程式的請求，例如，如果該應用程式超出了指定間隔內的最大請求數。Kaspersky Endpoint Security 將有關來自協力廠商應用程式的被拒絕請求的資訊傳送至管理伺服器。AMSI 防護元件不會拒絕來自對其啟用了與 AMSI 防護元件的持續整合的協力廠商應用程式的請求。

AMSI 防護元件可用於以下適用於工作站和伺服器的作業系統：

- Windows 10 Home / Pro / Pro for Workstations / Education / Enterprise / Enterprise 多工作階段
- Windows 11 Home / Pro / Pro for Workstations / Education / Enterprise
- Windows Server 2016 Essentials / Standard / Datacenter（包括 Server Core 模式）

- Windows Server 2019 Essentials / Standard / Datacenter（包括 Server Core 模式）
- Windows Server 2022 Standard / Datacenter / Datacenter: Azure Edition（包括 Server Core 模式）
- Windows Server 2025 Standard / Datacenter

# 啟用和停用 AMSI 防護

預設情況下，AMSI 防護已啟用並以卡巴斯基建議的模式運作（請參閱下表）。

**如何在管理主控台（MMC）中啟用或停用 AMSI 防護**

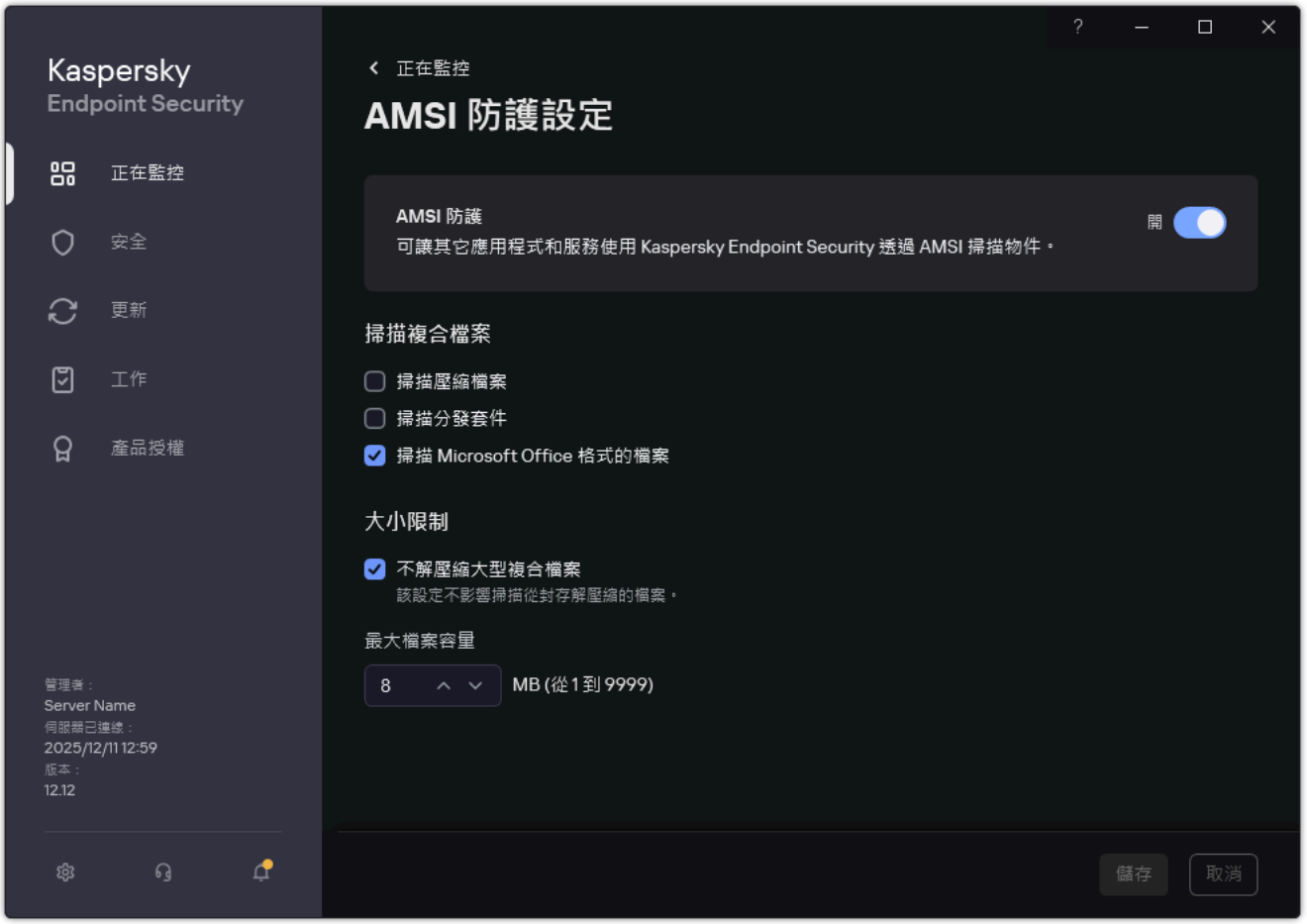
1. 在卡巴斯基安全管理中心管理主控台樹狀目錄中，選取**政策**。
2. 選擇必要的政策並點擊以開啟政策內容。
3. 在政策視窗中，選擇**"關鍵威脅防護 → AMSI 掃描程式"**。
4. 使用**"AMSI 掃描程式"**核取方塊來啟用或停用元件。
5. 儲存變更。若要在電腦上套用該政策，請關閉掛鎖。

**如何在網頁主控台和雲端主控台中啟用或停用 AMSI 防護**

1. 在網頁主控台的主視窗中，選擇**資產（裝置）→ 政策和設定檔**。
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"→"AMSI 防護"**。
5. 使用**"AMSI 防護已啟用"**切換開關可啟用或停用元件。
6. 儲存變更。若要在電腦上套用該政策，請關閉掛鎖。

### 如何在應用程式介面中啟用或停用 AMSI 防護

1. 在“應用程式主視窗”中，點擊⚙按鈕。
2. 在應用程式設定視窗中，選取”**關鍵威脅防護**“→“**AMSI 防護**”。




“AMSI 防護”設定

3. 使用“**AMSI 防護**“切換開關可啟用或停用元件。
4. 儲存變更。

卡巴斯基專家建議的 AMSI 防護設定

| 參數 | 值 | 描述 |
|---|---|---|
| **掃描壓縮檔案** | **關** | 掃描 ZIP、GZIP、BZIP、RAR、TAR、ARJ、CAB、LHA、JAR、ICE 和其它存檔。應用程式不僅依照副檔名而且依照格式掃描存檔。當檢查封存時，應用程式會執行巡迴解壓縮。這可讓人偵測多層封存（封存內的封存）內的威脅。 |
| **掃描分發套件** | **關** | 掃描協力廠商應用程式的分發套件。 |
| **掃描 Microsoft Office 格式的檔案** | **開** | 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。應用程式掃描小於 1 MB 的 office 格式檔案，無論該核取方塊是否被選中。 |
| **不解壓縮大型複合檔案** | **最大檔案容量 8 MB** | 如果選中該核取方塊，應用程式不會掃描其大小超過指定值的複合檔案。<br>如果清除該核取方塊，應用程式將掃描所有大小的複合檔案。<br>應用程式會掃描從存檔中提取的大檔案，而不管是否選中該核取方塊。 |

# 透過 AMSI 防護最佳化檔案掃描

您可以最佳化檔案掃描：縮短掃描時間並提高 Kaspersky Endpoint Security 的執行速度。您可以選擇需要掃描的複合檔案：壓縮檔案，分發套件或辦公室格式的檔案。您也可以限制要掃描的複合檔案的大小。“AMSI 防護”元件不會解壓縮大於指定大小的複合檔案。

隱藏病毒和其他惡意軟體的一種常用方法就是將其植入複合檔案中，例如存檔。為了偵測以這種方式隱藏的病毒和其他惡意軟體，必須將複合檔案解壓縮，但是這可能會降低掃描速度。您可以限制要掃描的複合檔案類型，從而加快掃描速度。

**如何在管理主控台 (MMC) 中最佳化 AMSI 防護的檔案掃描**

1. 在卡巴斯基安全管理中心管理主控台樹狀目錄中，選取**政策**。
2. 選擇必要的政策並點擊以開啟政策內容。
3. 在政策視窗中，選擇**"關鍵威脅防護 → AMSI 掃描程式"**。
4. 在**"掃描複合檔案"**塊中，指定您希望掃描的複合檔案類型：存檔、分發套件或 Office 格式檔案。
5. 在**"容量限制"**塊中執行以下操作之一：
   - 要封鎖"AMSI 防護"元件解壓縮大型複合檔案，請選中**"複合檔案大於指定值時不解壓縮"**核取方塊，並指定所需值。"AMSI 防護"元件不會解壓縮大於指定大小的複合檔案。
   - 要允許"AMSI 防護"元件解壓縮大型複合檔案，請取消選中**"複合檔案大於指定值時不解壓縮"**核取方塊。

   無論是否選中**"複合檔案大於指定值時不解壓縮"**核取方塊，"AMSI 防護"元件均會掃描從存檔中提取的大型檔案。
6. 儲存變更。若要在電腦上套用該政策，請關閉掛鎖。

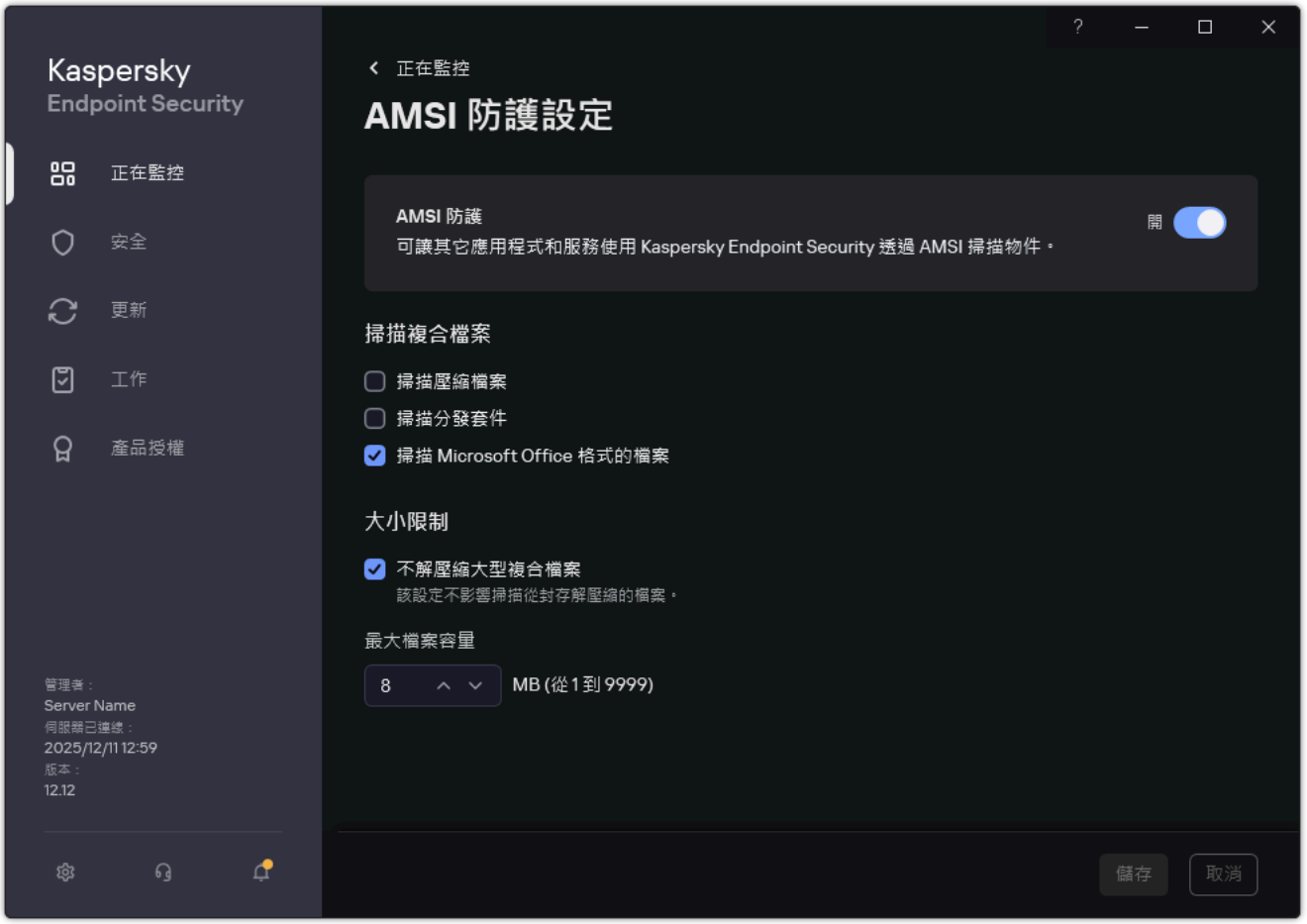
**如何在網頁主控台和雲端主控台中最佳化 AMSI 的檔案掃描**

1. 在網頁主控台的主視窗中，選擇**資產（裝置） → 政策和設定檔**。
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"→"AMSI 防護"**。
5. 在**"掃描複合檔案"**塊中，指定您希望掃描的複合檔案類型：存檔、分發套件或 Office 格式檔案。
6. 在**"掃描最佳化"**塊中執行以下操作之一：
   - 要封鎖"AMSI 防護"元件解壓縮大型複合檔案，請選中**"大小限制已啟用"**核取方塊，並指定所需值。"AMSI 防護"元件不會解壓縮大於指定大小的複合檔案。
   - 要允許"AMSI 防護"元件解壓縮大型複合檔案，請取消選中**"大小限制已啟用"**核取方塊。

   無論是否選中**"大小限制已啟用"**核取方塊，"AMSI 防護"元件均會掃描從存檔中提取的大型檔案。
7. 儲存變更。若要在電腦上套用該政策，請關閉掛鎖。

**如何在應用程式介面中最佳化 AMSI 防護的檔案掃描**

1. 在“應用程式主視窗”中，點擊⚙按鈕。
2. 在應用程式設定視窗中，選取”**關鍵威脅防護**“→“**AMSI 防護**”。




“AMSI 防護”設定

3. 在“**掃描複合檔案**”塊中，指定您希望掃描的複合檔案類型：存檔、分發套件或 Office 格式檔案。
4. 在“**大小限制**”塊中執行以下操作之一：
   - 要封鎖“AMSI 防護”元件解壓縮大型複合檔案，請選中“**不解壓縮大型複合檔案**”核取方塊，並指定所需值。“AMSI 防護”元件不會解壓縮大於指定大小的複合檔案。
   - 要允許“AMSI 防護”元件解壓縮大型複合檔案，請取消選中“**不解壓縮大型複合檔案**”核取方塊。

   無論是否選中“**不解壓縮大型複合檔案**”核取方塊，“AMSI 防護”元件均會掃描從存檔中提取的大型檔案。
5. 儲存變更。

# 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，同時封鎖惡意網站和釣魚網站。該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來提供電腦防護。

Kaspersky Endpoint Security 掃描 HTTP、HTTPS 和 FTP 流量。Kaspersky Endpoint Security 掃描 URL 和 IP 位址。

若要使用 Web 威脅防護，您必須完成應用程式的初始設定：

- 對於 HTTPS 流量監控，啟用加密連線掃描（預設為啟用）。
- 選擇 Kaspersky Endpoint Security 必須監控的連接埠（預設情況下，應用程式監控所有連接埠）。
- 選擇您希望 Kaspersky Endpoint Security 監控其流量的應用程式。大多數瀏覽器已出現在卡巴斯基推薦的應用程式清單中。如果清單中缺少您的瀏覽器，請手動新增。
- 我們建議將網頁交互指令碼注入到 Web 流量中（預設情況下，指令碼注入被停用）。此指令碼可啟用為應用程式事件日誌、OS 事件日誌和報告註冊 Web 威脅防護事件。

當使用者嘗試開啟惡意網站或釣魚網站時，Kaspersky Endpoint Security 將封鎖其存取並顯示警告（請參見下圖）。




網站存取被拒絕的訊息

# 啟用和停用 Web 威脅防護

預設情況下，“Web 威脅防護”元件已啟用並在 Kaspersky 專家建議的模式下執行。對於 Web 威脅防護，應用程式可以套用不同的設定群組。這些儲存在應用程式中的設定群組稱為*安全防護等級*：**高**、**建議**、**低**。**建議**Web 流量安全防護等級設定將被視為 Kaspersky 專家建議的最佳設定（請見下表）。您可以為透過 HTTP 和 FTP 協定接收或傳送的網頁流量選取一個預先設定的安全等級，或者也可以設定一個自訂網頁流量安全等級。如果您對網頁流量安全等級進行了變更，以後隨時可以還原至建議的網頁流量安全等級設定。

您只能在管理主控台 (MMC) 或者應用程式的本機介面中選擇或者設定安全等級。您不能在網頁主控台或者雲端主控台中選擇或者設定安全等級。

**如何在管理主控台（MMC）中啟用或停用“Web 威脅防護”元件**

1. 在卡巴斯基安全管理中心管理主控台樹狀目錄中，選取**政策**。
2. 選擇必要的政策並點擊以開啟政策內容。

3. 在政策視窗中，選擇“**關鍵威脅防護 → Web 威脅防護**”。

4. 使用“**Web 威脅防護**“核取方塊來啟用或停用元件。

5. 如果啟用了該元件，請在“**安全等級**“塊中執行下列操作之一：

   - 如果您希望套用一種預設的安全防護等級，請使用移動滑桿選取：

     - **高**在此安全等級下，“Web 威脅防護”元件對電腦透過 HTTP 和 FTP 收到的 Web 流量執行最大限度的掃描。“Web 威脅防護”使用整個程式應用資料庫詳細掃描所有 Web 流量物件，並盡可能執行最深度的啟發式分析。

     - **建議防護**該安全等級在應用程式的效能和 Web 流量的安全之間提供最佳平衡。“Web 威脅防護”元件執行中度掃描等級的啟發式分析。Kaspersky 專家建議使用此 Web 流量安全等級。下表提供了建議的安全防護等級的設定值。

     - **低**此 Web 流量安全等級的設定可確保最快的 Web 流量掃描速度。“Web 威脅防護”元件執行輕度掃描等級的啟發式分析。

   - 如果要設定自訂安全防護等級，請點擊“**設定**“按鈕然後定義您自己的元件設定。

     您可以透過點擊“**根據預設**”按鈕來還原預設安全等級的值。.

6. 在**偵測到威脅後的動作**塊中，選取 Kaspersky Endpoint Security 對惡意網頁流量物件所採取的操作：

   - **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**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”元件將允許此物件下載到電腦，但會將受感染物件的相關資訊新增到活動威脅清單中。

7. 儲存變更。

**如何在網頁主控台和雲端主控台中啟用或停用“Web 威脅防護”元件**

1. 在網頁主控台的主視窗中，選擇**資產（裝置）→ 政策和設定檔**。

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. 使用“**Web 威脅防護已啟用**“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，選取 Kaspersky Endpoint Security 對惡意網頁流量物件所採取的操作：

   - **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。

   - **允許、通知或者提示採取操作（取決於作業係統）**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”元件將允許此物件下載到電腦，但會將受感染物件的相關資訊新增到活動威脅清單中。

7. 如果有需要的話，列出受信任的網址清單。

8. 儲存變更。

**如何啟用或停用"Web 威脅防護"元件**

1. 在"應用程式主視窗"中，點擊⚙按鈕。

2. 在應用程式設定視窗中，選取"**關鍵威脅防護**"→"**Web 威脅防護**"。

3. 使用"**Web 威脅防護**"切換開關可啟用或停用元件。

4. 如果啟用了該元件，請在"**安全等級**"塊中執行下列操作之一：

   - 如果您希望套用一種預設的安全防護等級，請使用移動滑桿選取：

     - **高**在此安全等級下，"Web 威脅防護"元件對電腦透過 HTTP 和 FTP 收到的 Web 流量執行最大限度的掃描。"Web 威脅防護"使用整個程式應用資料庫詳細掃描所有 Web 流量物件，並盡可能執行最深度的啟發式分析。

     - **建議**該安全等級在應用程式的效能和 Web 流量的安全之間提供最佳平衡。"Web 威脅防護"元件執行中度掃描等級的啟發式分析。Kaspersky 專家建議使用此 Web 流量安全等級。下表提供了建議的安全防護等級的設定值。

     - **低**此 Web 流量安全等級的設定可確保最快的 Web 流量掃描速度。"Web 威脅防護"元件執行輕度掃描等級的啟發式分析。

   - 如果要設定自訂安全防護等級，請點擊"**進階設定**"按鈕然後定義您自己的元件設定。

     您可以透過點擊"**還原建議的安全等級**"按鈕來還原預設安全等級的值。.

5. 在**偵測到威脅後的動作**塊中，選取 Kaspersky Endpoint Security 對惡意網頁流量物件所採取的操作：

   - **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**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"元件將允許此物件下載到電腦，但會將受感染物件的相關資訊新增到活動威脅清單中。

6. 儲存變更。

卡巴斯基專家建議的 Web 威脅防護設定（建議的安全防護等級）

| 參數 | 值 | 描述 |
|---|---|---|
| **檢查網址是否在惡意網址資料庫中** | **開** | 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。 |
| **檢查網址是否在釣魚網址資料庫中** | **開** | 釣魚網址資料庫包含目前用於啟動釣魚攻擊的已知網站的位址。卡巴斯基使用從名為"釣魚防護工作組"的國際組織獲得的位址來補充網路釣魚連線資料庫。釣魚位址資料庫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。 |
| **使用啟發式分析**（Web 威脅防護） | **中度掃描** | 開發該技術的目的是偵測使用 Kaspersky 應用程式資料庫無法偵測到的威脅。它可以偵測受未知病毒或已知病毒新變種感染的可疑檔案。<br>當掃描網路流量中的病毒和其他構成威脅的應用程式時，啟發式分析將在可執行檔案中執行指令。啟發式分析器執行的指令數取決於為啟發式分析器指定的級別。啟發式分析等級可在全面搜尋新威脅、載入作業系統資源和啟發式分析持續時間之間進行平衡。 |
| **使用啟發式分析**（反網路釣魚） | **開** | 開發該技術的目的是偵測使用 Kaspersky 應用程式資料庫無法偵測到的威脅。它可以偵測受未知病毒或已知病毒新變種感染的可疑檔案。 |
| **偵測到威脅後的動作** | **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。 |

# 設定惡意網址偵測方法

Web 威脅防護使用病毒資料庫、卡巴斯基安全網路雲端服務和啟發式分析偵測惡意網址。

您只能在管理主控台 (MMC) 或者應用程式的本機介面中選擇惡意網址偵測方法。您不能在網頁主控台或者雲端主控台中選擇惡意網址偵測方法。預設選項是使用啟發式分析（中度掃描）根據惡意位址資料庫檢查網址。

## 使用惡意位址資料庫掃描

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。

Kaspersky Endpoint Security 將掃描所有連接，以確定它們是否在惡意網址資料庫中。應用程式的安全連線掃描設定不會影響連接掃描功能。換句話說，如果停用了加密連線掃描，即使網路流量是透過加密連線傳輸的，Kaspersky Endpoint Security 也會根據惡意網址資料庫檢查連接。

**如何啟用或者停用使用管理主控台 (MMC) 根據惡意網址資料庫檢查網址**

1. 在卡巴斯基安全管理中心管理主控台樹狀目錄中，選取**政策**。
2. 選擇必要的政策並點擊以開啟政策內容。
3. 在政策視窗中，選擇**"關鍵威脅防護 → Web 威脅防護"**。
4. 在**"安全等級"**塊中，點擊**"設定"**按鈕。
5. 在開啟的視窗中，在**"掃描方式"**塊中，選擇或者清除**"檢查網址是否在惡意網址資料庫中"**核取方塊來啟用或者停用檢查網址是否在惡意網址資料庫中。
6. 儲存變更。

**如何在應用程式介面中啟用或者停用檢查網址是否在惡意網址資料庫中。**

1. 在"應用程式主視窗"中，點擊 按鈕。
2. 在應用程式設定視窗中，選取**"關鍵威脅防護"→"Web 威脅防護"**。
3. 點擊**"進階設定"**。
4. 在**"掃描方式"**塊中，選擇或者清除**"檢查網址是否在惡意網址資料庫中"**核取方塊來啟用或者停用檢查網址是否在惡意網址資料庫中。
5. 儲存變更。

## 啟發式分析

在啟發式分析中，Kaspersky Endpoint Security 將分析應用程式在作業系統中的活動。啟發式分析可以偵測 Kaspersky Endpoint Security 資料庫中尚無記錄的安全威脅。

當掃描網路流量中的病毒和其他構成威脅的應用程式時，啟發式分析將在可執行檔案中執行指令。啟發式分析器執行的指令數取決於為啟發式分析器指定的級別。啟發式分析等級可在全面搜尋新威脅、載入作業系統資源和啟發式分析持續時間之間進行平衡。

### 如何在管理主控台（MMC）中啟用或停用啟發式分析

1. 在卡巴斯基安全管理中心管理主控台樹狀目錄中，選取**政策**。
2. 選擇必要的政策並點擊以開啟政策內容。
3. 在政策視窗中，選擇**"關鍵威脅防護 → Web 威脅防護"**。
4. 在**"安全等級"**塊中，點擊**"設定"**按鈕。
5. 在開啟的視窗中，如果您希望應用程式在掃描 Web 流量中的病毒和其他惡意軟體時使用啟發式分析，請在**"掃描方式"**塊中，選中**"使用啟發式分析"**核取方塊。
6. 使用捲軸設定啟發式分析等級：**輕度掃描**、**中度掃描**或**深度掃描**。

   當掃描網路流量中的病毒和其他構成威脅的應用程式時，啟發式分析將在可執行檔案中執行指令。啟發式分析器執行的指令數取決於為啟發式分析器指定的級別。啟發式分析等級可在全面搜尋新威脅、載入作業系統資源和啟發式分析持續時間之間進行平衡。
7. 儲存變更。

### 如何在應用程式介面中啟用或停用啟發式分析

1. 在"應用程式主視窗"中，點擊⚙按鈕。
2. 在應用程式設定視窗中，選取**"關鍵威脅防護"→"Web 威脅防護"**。
3. 點擊**"進階設定"**。
4. 如果希望應用程式在掃描 Web 流量中的病毒和其他惡意軟體時使用啟發式分析，請在**"掃描方式"**塊中，選中**"使用啟發式分析"**核取方塊。

   當掃描網路流量中的病毒和其他構成威脅的應用程式時，啟發式分析將在可執行檔案中執行指令。啟發式分析器執行的指令數取決於為啟發式分析器指定的級別。啟發式分析等級可在全面搜尋新威脅、載入作業系統資源和啟發式分析持續時間之間進行平衡。
5. 儲存變更。

# 釣魚網站防護

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。

您只能在管理主控台 (MMC) 或者應用程式的本機介面中設定網路釣魚防護。您不能在網頁主控台或者雲端主控台中設定網路釣魚防護。預設啟用使用啟發式分析進行網路釣魚防護。

**如何在管理主控台（MMC）中啟用或停用網路釣魚防護**

1. 在卡巴斯基安全管理中心管理主控台樹狀目錄中，選取**政策**。
2. 選擇必要的政策並點擊以開啟政策內容。
3. 在政策視窗中，選擇"**關鍵威脅防護 → Web 威脅防護**"。
4. 在"**安全等級**"塊中，點擊"**設定**"按鈕。
5. 在開啟的視窗中，在**網路釣魚防護設定**塊中，選擇或者清除**檢查網址是否在釣魚網址資料庫中**核取方塊以啟用或停用反網路釣魚。

   釣魚網址資料庫包含目前用於啟動釣魚攻擊的已知網站的位址。卡巴斯基使用從名為"釣魚防護工作組"的國際組織獲得的位址來補充網路釣魚連線資料庫。釣魚位址資料庫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。
6. 如果希望應用程式在掃描網頁中的釣魚連結時使用啟發式分析，請選中"**使用啟發式分析**"核取方塊。

   在啟發式分析中，Kaspersky Endpoint Security 將分析應用程式在作業系統中的活動。啟發式分析可以偵測 Kaspersky Endpoint Security 資料庫中尚無記錄的安全威脅。

   若要掃描連接，除了病毒資料庫和啟發式分析外，您還可以使用卡巴斯基安全網路信譽資料庫。
7. 儲存變更。

**如何在應用程式介面中啟用或停用網路釣魚防護**

1. 在"應用程式主視窗"中，點擊 按鈕。
2. 在應用程式設定視窗中，選取"**關鍵威脅防護**"→"**Web 威脅防護**"。
3. 點擊"**進階設定**"。
4. 如果您希望 Web 威脅防護元件根據網路釣魚網址資料庫檢查連結，請選中"**釣魚防護**"塊中的"**檢查網址是否在釣魚網址資料庫中**"核取方塊。釣魚網址資料庫包含目前用於啟動釣魚攻擊的已知網站的位址。卡巴斯基使用從名為"釣魚防護工作組"的國際組織獲得的位址來補充網路釣魚連線資料庫。釣魚位址資料庫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。
5. 如果希望應用程式在掃描網頁中的釣魚連結時使用啟發式分析，請選中"**使用啟發式分析**"核取方塊。

在啟發式分析中，Kaspersky Endpoint Security 將分析應用程式在作業系統中的活動。啟發式分析可以偵測 Kaspersky Endpoint Security 資料庫中尚無記錄的安全威脅。

若要掃描連接，除了病毒資料庫和啟發式分析外，您還可以使用卡巴斯基安全網路信譽資料庫。

6. 儲存變更。

# 建立受信任網址清單

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。

網址可以是某特定網頁的位址，也可以是某網站的位址。

管理主控台 (MMC) 和網頁主控台中受信任區域的分組方式不同。同樣，防止受信任區域參數變更的方式也不同（不同的“掛鎖”）。我們建議僅使用網頁主控台來管理應用程式。如果在不同主控台中配置受信任區域，管理外掛程式可能會將“掛鎖”重設為其預設狀態。

**如何使用管理主控台 (MMC) 新增受信任網址**

1. 在卡巴斯基安全管理中心管理主控台樹狀目錄中，選取**政策**。
2. 選擇必要的政策並點擊以開啟政策內容。
3. 在政策視窗中，選擇“**關鍵威脅防護 → Web 威脅防護**”。
4. 在”**安全等級**”塊中，點擊”**設定**”按鈕。
5. 在開啟的視窗中選擇“**受信任網址**”標籤。
6. 選擇“**不掃描受信任網址的 Web 流量**”核取方塊。

   如果選擇此選項，“Web 威脅防護”元件將不再掃描其網址包含在受信任網址清單中的網頁或網站的內容。您可以將網頁/網站的特定位址和位址遮罩新增至受信任網址清單。
7. 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。

   您還可以從 XML 檔案匯入受信任網址清單。
8. 儲存變更。

**如何在網頁主控台和雲端主控台中新增受信任網址**

1. 在網頁主控台的主視窗中，選擇**資產（裝置）→ 政策和設定檔**。
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. 點擊"**受信任網址**"。

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。

   您還可以從 XML 檔案匯入受信任網址清單。

7. 儲存變更。

**如何在應用程式介面中新增受信任網址**

1. 在"應用程式主視窗"中，點擊⚙按鈕。

2. 在應用程式設定視窗中，選取"**關鍵威脅防護**"→"**Web 威脅防護**"。

3. 點擊"**進階設定**"。

4. 選取"**不掃描來自以下的 Web 流量受信任網址**"核取方塊。

   如果選擇此選項，"Web 威脅防護"元件將不再掃描其網址包含在受信任網址清單中的網頁或網站的內容。您可以將網頁/網站的特定位址和位址遮罩新增至受信任網址清單。

5. 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。

   您還可以從 XML 檔案匯入受信任網址清單。

6. 儲存變更。

因此，Web 威脅防護不掃描受信任網址的流量。使用者總是可以從該網站開啟受信任網站並下載檔案。如果無法獲得網站的存取權限，請檢查加密連線掃描、Web 控制和網路連接埠監控元件。如果 Kaspersky Endpoint Security 偵測到從受信任網站下載的檔案為惡意檔案，您可以"將該檔案新增到排除項目"。

您也可以建立一個通用加密連線排除項目清單。在此情況下，當 Web 威脅防護、郵件威脅防護、Web 控制元件執行工作時，Kaspersky Endpoint Security 不掃描受信任網址的 HTTPS 流量。

# 匯出和匯入受信任網址的清單

您可以將受信任網址清單匯出到 XML 檔案。然後，您可以修改檔案，例如，新增大量相同類型的網址。您還可以使用匯出/匯入功能來備份受信任的網址清單，或將清單遷移到其他伺服器。

**如何在管理主控台 (MMC) 中匯出和匯入受信任的網址清單**

1. 在卡巴斯基安全管理中心管理主控台樹狀目錄中，選取**政策**。

2. 選擇必要的政策並點擊以開啟政策內容。

3. 在政策視窗中，選擇"**關鍵威脅防護 → Web 威脅防護**"。

4. 在"**安全等級**"塊中，點擊"**設定**"按鈕。

5. 在開啟的視窗中選擇"**受信任網址**"標籤。

6. 要匯出受信任網址清單：

   a. 選擇您要匯出的受信任網址。要選擇多個連接埠，請使用**CTRL**或**SHIFT**鍵。

   如果未選擇任何受信任網址，則 Kaspersky Endpoint Security 將匯出所有網址。

   b. 點擊"**匯出**"連接。

   c. 在開啟的視窗中，指定您要將受信任網址清單匯出到的 XML 檔案的名稱，然後選取要儲存此檔案的資料夾。

   d. 儲存檔案。

   Kaspersky Endpoint Security 會將整個受信任網址清單匯出到 XML 檔案。

7. 要匯入受信任網址的清單：

   a. 點擊"**匯入**"連接。

   在開啟的視窗中，選取要從中匯入受信任網址清單的 XML 檔案。

   b. 開啟檔案。

   如果電腦已經具有受信任網址清單，則 Kaspersky Endpoint Security 將提示您刪除現有清單或從 XML 檔案向其中新增新項目。

8. 儲存變更。

**如何在網頁主控台和雲端主控台中匯出和匯入受信任的網址清單**

1. 在網頁主控台的主視窗中，選擇**資產（裝置）→政策和設定檔**。

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. 要匯出"**規則清單**"塊中的排除項目清單：

   a. 選擇您要匯出的受信任網址。

   b. 點擊 → **匯出** 按鈕。

   Kaspersky Endpoint Security 會將受信任網址清單匯出到預設下載資料夾中的 JSON 檔案。

6. 要匯入"**規則清單**"塊中的排除項目清單：

   a. 點擊 → **匯入** 按鈕。

   在開啟的視窗中，選取要從中匯入受信任網址清單的 JSON 檔案。

   b. 開啟檔案。

   如果電腦已經具有受信任網址清單，則 Kaspersky Endpoint Security 將提示您刪除現有清單或從 JSON 檔案向其中新增新項目。

7. 儲存變更。

# 郵件威脅防護

"郵件威脅防護"元件掃描傳送和接收電子郵件的附件是否有病毒和其他威脅。該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來提供電腦防護。

郵件威脅防護可以掃描傳入和傳出的郵件。該應用程式在以下郵件用戶端中支援 POP3、SMTP、IMAP 和 NNTP：

- Microsoft Office Outlook
- Mozilla Thunderbird
- Windows Mail
- MyOffice Mail
- R7-Office Organizer

若要掃描 Mozilla Thunderbird、MyOffice Mail 及 R7-Office Organizer 郵件用戶端的流量，您需要將卡巴斯基憑證新增至專屬憑證儲存區，並選擇該專屬憑證儲存區。

郵件威脅防護不支援其他協定和郵件用戶端。

郵件威脅防護並不總是能夠獲得*協定級別*的郵件存取權限（例如，當使用 Microsoft Exchange 解決方案時）。為此，郵件威脅防護包括 Microsoft Office Outlook 延伸程式。該延伸程式允許在*郵件用戶端級別*掃描郵件。郵件威脅防護延伸支援 Outlook 2010、2013、2016、2019 和 2021 的操作。

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。

如果在附件中偵測到惡意檔案，Kaspersky Endpoint Security 會將有關已執行操作的資訊新增到郵件主旨，例如，*[郵件已處理]* <*郵件主旨*>。

# 啟用和停用郵件威脅防護

預設情況下，"郵件威脅防護"元件已啟用並在 Kaspersky 專家建議的模式下執行。對於郵件威脅防護，應用程式可以套用不同的設定群組。這些儲存在應用程式中的設定群組稱為*安全防護等級*：**高**、**建議**、**低**。**建議**郵件安全防護等級設定將被視為 Kaspersky 專家建議的最佳設定（請見下文）。您可以選取某個預設的電子郵件安全防護等級，也可以設定自訂電子郵件安全防護等級。如果您變更了電子郵件安全防護等級，您可以隨時還原為建議的電子郵件安全防護等級設定。

使用 Mozilla Thunderbird 郵件用戶端時，如果使用篩檢程式將訊息移出"收件箱"資料夾，"郵件威脅防護"元件將不能掃描病毒、其他惡意程式或經由 IMAP 協定傳送的電子郵件。

**如何在管理主控台（MMC）中啟用或停用"郵件威脅防護"元件**

1. 在卡巴斯基安全管理中心管理主控台樹狀目錄中，選取**政策**。
2. 選擇必要的政策並點擊以開啟政策內容。
3. 在政策視窗中，選擇"**關鍵威脅防護 → 郵件威脅防護**"。
4. 使用"**郵件威脅防護**"核取方塊來啟用或停用元件。
5. 如果啟用了該元件，請在"**安全等級**"塊中執行下列操作之一：
   - 如果您希望套用一種預設的安全防護等級，請使用移動滑桿選取：
     - **高**選擇此電子郵件安全等級時，"郵件威脅防護"元件會最徹底地掃描電子郵件。"郵件威脅防護"元件將掃描傳送和接收的電子郵件訊息，並執行深度啟發式分析。對於高風險環境，建議使用"高"郵件安全防護等級。這種情況的一個例子就是，未獲得集中式電子郵件防護的家用網路連線免費的電子郵件服務。
     - **建議防護**此電子郵件安全等級在應用程式的效能和電子郵件安全性之間提供最佳平衡。"郵件威脅防護"元件將掃描傳送和接收的電子郵件，並執行中度啟發式分析。Kaspersky 專家建議採用這一郵件流量安全等級。下表提供了建議的安全防護等級的設定值。
     - **低**選擇此電子郵件安全等級時，"郵件威脅防護"元件只掃描接收的電子郵件訊息，執行輕度啟發式分析，不掃描電子郵件的壓縮套件附件。在這一郵件安全等級中，"郵件威脅防護"元件將使用最少的作業系統資源，以最大速度掃描電子郵件。在防護良好的環境中工作時，建議使用"低"郵件安全等級。這類環境的一個例子是具有集中式電子郵件防護的企業區域網路。
   - 如果要設定自訂安全防護等級，請點擊"**設定**"按鈕然後定義您自己的元件設定。

     您可以透過點擊"**根據預設**"按鈕來還原預設安全等級的值。.
6. 在**偵測到威脅後的動作**塊中，選取 Kaspersky Endpoint Security 對惡意物件所採取的操作：
   - **解毒；若解毒失敗則刪除**在入站或出站郵件中偵測到受感染的物件時，應用程式會嘗試對偵測到的物件進行解毒。使用者將能夠存取帶安全附件的郵件。如果無法解毒物件，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到郵件主旨，例如，*[郵件已處理]<郵件主旨>*。
   - **解毒；若解毒失敗則封鎖**在入站郵件中偵測到受感染的物件時，應用程式會嘗試對偵測到的物件進行解毒。使用者將能夠存取帶安全附件的郵件。如果無法解毒物件，應用程式會將警告新增到郵件主旨。使用者將能夠存取帶原始附件的郵件。在出站郵件中偵測到受感染的物件時，應用程式會嘗試對偵測到的物件進行解毒。如果無法解毒物件，應用程式會封鎖郵件的傳輸，郵件使用者端會顯示錯誤。
   - **封鎖**如果在入站郵件中偵測到受感染的物件，應用程式會將警告新增到郵件主旨。使用者將能夠存取帶原始附件的郵件。如果在出站郵件中偵測到受感染的物件，應用程式會封鎖郵件的傳輸，郵件使用者端會顯示錯誤。
7. 儲存變更。若要在電腦上套用該政策，請關閉掛鎖。

**如何在網頁主控台和雲端主控台中啟用或停用"郵件威脅防護"元件**

1. 在網頁主控台的主視窗中，選擇**資產（裝置）→ 政策和設定檔**。
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. 使用"**郵件威脅防護已啟用**"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，選取 Kaspersky Endpoint Security 對惡意物件所採取的操作：

   - **解毒；若解毒失敗則刪除**在入站或出站郵件中偵測到受感染的物件時，應用程式會嘗試對偵測到的物件進行解毒。使用者將能夠存取帶安全附件的郵件。如果無法解毒物件，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到郵件主旨，例如，*[郵件已處理]<郵件主旨>*。

   - **解毒；若解毒失敗則封鎖**在入站郵件中偵測到受感染的物件時，應用程式會嘗試對偵測到的物件進行解毒。使用者將能夠存取帶安全附件的郵件。如果無法解毒物件，應用程式會將警告新增到郵件主旨。使用者將能夠存取帶原始附件的郵件。在出站郵件中偵測到受感染的物件時，應用程式會嘗試對偵測到的物件進行解毒。如果無法解毒物件，應用程式會封鎖郵件的傳輸，郵件使用者端會顯示錯誤。

   - **封鎖**如果在入站郵件中偵測到受感染的物件，應用程式會將警告新增到郵件主旨。使用者將能夠存取帶原始附件的郵件。如果在出站郵件中偵測到受感染的物件，應用程式會封鎖郵件的傳輸，郵件使用者端會顯示錯誤。

7. 如有必要，請編輯郵件威脅防護的進階設定。

8. 儲存變更。

**如何在應用程式介面中啟用或停用郵件威脅防護元件**

1. 在"應用程式主視窗"中，點擊⚙按鈕。

2. 在應用程式設定視窗中，選取"**關鍵威脅防護**"→"**郵件威脅防護**"。

3. 使用"**郵件威脅防護**"切換開關可啟用或停用元件。

4. 如果啟用了該元件，請在"**安全等級**"塊中執行下列操作之一：

   - 如果您希望套用一種預設的安全防護等級，請使用移動滑桿選取：

     - **高**選擇此電子郵件安全等級時，"郵件威脅防護"元件會最徹底地掃描電子郵件。"郵件威脅防護"元件將掃描傳送和接收的電子郵件訊息，並執行深度啟發式分析。對於高風險環境，建議使用"高"郵件安全防護等級。這種情況的一個例子就是，未獲得集中式電子郵件防護的家用網路連線免費的電子郵件服務。

     - **建議**此電子郵件安全等級在應用程式的效能和電子郵件安全性之間提供最佳平衡。"郵件威脅防護"元件將掃描傳送和接收的電子郵件，並執行中度啟發式分析。Kaspersky 專家建議採用這一郵件流量安全等級。下表提供了建議的安全防護等級的設定值。

     - **低**選擇此電子郵件安全等級時，"郵件威脅防護"元件只掃描接收的電子郵件訊息，執行輕度啟發式分析，不掃描電子郵件的壓縮套件附件。在這一郵件安全等級中，"郵件威脅防護"元件將使用最少的作業系統資源，以最大速度掃描電子郵件。在防護良好的環境中工作時，建議使用"低"郵件安全等級。這類環境的一個例子是具有集中式電子郵件防護的企業區域網路。

   - 如果要設定自訂安全防護等級，請點擊"**進階設定**"按鈕然後定義您自己的元件設定。

     您可以透過點擊"**還原建議的安全等級**"按鈕來還原預設安全等級的值。.

5. 在**偵測到威脅後的動作**塊中，選取 Kaspersky Endpoint Security 對惡意物件所採取的操作：

- **解毒；若解毒失敗則刪除**在入站或出站郵件中偵測到受感染的物件時，應用程式會嘗試對偵測到的物件進行解毒。使用者將能夠存取帶安全附件的郵件。如果無法解毒物件，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到郵件主旨，例如，*[郵件已處理]<郵件主旨>*。

- **解毒；若解毒失敗則封鎖**在入站郵件中偵測到受感染的物件時，應用程式會嘗試對偵測到的物件進行解毒。使用者將能夠存取帶安全附件的郵件。如果無法解毒物件，應用程式會將警告新增到郵件主旨。使用者將能夠存取帶原始附件的郵件。在出站郵件中偵測到受感染的物件時，應用程式會嘗試對偵測到的物件進行解毒。如果無法解毒物件，應用程式會封鎖郵件的傳輸，郵件使用者端會顯示錯誤。

- **封鎖**如果在入站郵件中偵測到受感染的物件，應用程式會將警告新增到郵件主旨。使用者將能夠存取帶原始附件的郵件。如果在出站郵件中偵測到受感染的物件，應用程式會封鎖郵件的傳輸，郵件使用者端會顯示錯誤。

6. 儲存變更。

卡巴斯基專家建議的郵件威脅防護設定（建議的安全防護等級）

| 參數 | 值 | 描述 |
|---|---|---|
| **防護範圍** | **接收和傳送的郵件** | *防護範圍*包括元件執行時檢查的物件： 接收和傳送的郵件或僅接收的訊息 。<br>為了防護您的電腦，您只需要掃描傳入的郵件。您可以開啟對傳出郵件的掃描功能，以防止受感染的檔案在存檔中傳送。如果要防止傳送特定格式的檔案（例如音訊和視訊檔案），您也可以開啟傳出郵件的掃描功能。 |
| **連線 Microsoft Outlook 延伸程式** | **開** | 如果選中該核取方塊，則在 Microsoft Outlook 中集成的延伸程式一側啟用對透過 POP3、SMTP、NNTP、IMAP 協定傳輸的電子郵件的掃描。<br>如果使用 Microsoft Outlook 的延伸程式掃描郵件，建議使用Cached Exchange Mode。有關 Cached Exchange 模式的詳細資訊和對其用途的建議，請參閱 Microsoft 知識庫。 |
| **掃描附件中的壓縮檔案** | **開** | 掃描 ZIP、GZIP、BZIP、RAR、TAR、ARJ、CAB、LHA、JAR、ICE 和其它存檔。應用程式不僅依照副檔名而且依照格式掃描存檔。當檢查封存時，應用程式會執行巡迴解壓縮。這可讓人偵測多層封存（封存內的封存）內的威脅。 |
| **掃描 Microsoft Office 格式的附加檔案** | **開** | 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。應用程式掃描小於 1 MB 的 office 格式檔案，無論該核取方塊是否被選中。 |
| **附件篩選** | **重新命名選取類型的附件** | 如果選擇此選項，郵件威脅防護元件將用下劃線字符（例如，attachment.doc__）替換在指定類型的附件檔案中找到的最後一個延伸字符。因此，為了開啟檔案，使用者必須重命名檔案。 |
| **啟發式分析** | **中度掃描** | 開發該技術的目的是偵測使用 Kaspersky 應用程式資料庫無法偵測到的威脅。它可以偵測受未知病毒或已知病毒新變種感染的可疑檔案。<br>掃描檔案中的惡意代碼時，啟發式分析器將執行可執行檔案中的指令。啟發式分析器執行的指令數取決於為啟發式分析器指定的級別。啟發式分析等級可在全面搜尋新威脅、載入作業系統資源和啟發式分析持續時間之間進行平衡。 |
| **偵測到威脅後的動作** | **解毒；若解毒失敗則刪除** | 在入站或出站郵件中偵測到受感染的物件時，應用程式會嘗試對偵測到的物件進行解毒。使用者將能夠存取帶安全附件的郵件。如果無法解毒物件，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到郵件主旨，例如，*[郵件已處理]<郵件主旨>*。 |

# 變更對受感染電子郵件採取的操作

預設情況下，“郵件威脅防護”元件將自動嘗試對已經偵測到的所有受感染電子郵件執行解毒操作。如果解毒失敗，“郵件威脅防護”元件會刪除感染的電子郵件。

*若變更對受感染電子郵件執行的操作，請執行以下操作：*

1. 在"應用程式主視窗"中，點擊⚙按鈕。
2. 在應用程式設定視窗中，選取"**關鍵威脅防護**"→"**郵件威脅防護**"。
3. 在"**偵測到威脅後的動作**"塊中選取 Kaspersky Endpoint Security 對偵測到受感染郵件執行的操作：
   - **解毒；若解毒失敗則刪除**在入站或出站郵件中偵測到受感染的物件時，應用程式會嘗試對偵測到的物件進行解毒。使用者將能夠存取帶安全附件的郵件。如果無法解毒物件，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到郵件主旨，例如，*[郵件已處理]* <*郵件主旨*>。
   - **解毒；若解毒失敗則封鎖**在入站郵件中偵測到受感染的物件時，應用程式會嘗試對偵測到的物件進行解毒。使用者將能夠存取帶安全附件的郵件。如果無法解毒物件，應用程式會將警告新增到郵件主旨。使用者將能夠存取帶原始附件的郵件。在出站郵件中偵測到受感染的物件時，應用程式會嘗試對偵測到的物件進行解毒。如果無法解毒物件，應用程式會封鎖郵件的傳輸，郵件使用者端會顯示錯誤。
   - **封鎖**如果在入站郵件中偵測到受感染的物件，應用程式會將警告新增到郵件主旨。使用者將能夠存取帶原始附件的郵件。如果在出站郵件中偵測到受感染的物件，應用程式會封鎖郵件的傳輸，郵件使用者端會顯示錯誤。
4. 儲存變更。

# 構成"郵件威脅防護"元件的防護範圍

*防護範圍*是指活動時被該元件掃描的物件。不同元件的防護範圍有不同的參數。"郵件威脅防護"元件的防護範圍內容包括將"郵件威脅防護"元件整合至郵件用戶端的設定，以及被"郵件威脅防護"元件掃描流量的電子郵件類型和電子郵件協定。預設情況下，Kaspersky Endpoint Security 將掃描透過 POP3、SMTP、NNTP 和 IMAP 協定進出的電子郵件和流量，並且該掃描與 Microsoft Office Outlook 電子郵件用戶端相整合。

*要構成"郵件威脅防護"元件的防護範圍：*

1. 在"應用程式主視窗"中，點擊⚙按鈕。
2. 在應用程式設定視窗中，選取"**關鍵威脅防護**"→"**郵件威脅防護**"。
3. 點擊"**進階設定**"。
4. 在"**防護範圍**"塊中，選擇要掃描的訊息：
   - **接收和傳送的郵件**
   - **僅接收訊息**

   為了防護您的電腦，您只需要掃描傳入的郵件。您可以開啟對傳出郵件的掃描功能，以防止受感染的檔案在存檔中傳送。如果要防止傳送特定格式的檔案（例如音訊和視訊檔案），您也可以開啟傳出郵件的掃描功能。

   如果您選取僅掃描接收的郵件，建議為所有傳送的郵件執行一次性掃描，因為有可能您的電腦存有郵件蠕蟲病毒並且會透過郵件傳播。這有助於避免因未監控電腦大量電子郵件散播而造成的問題。

5. 在“**連線**”塊中執行下列操作：

- 如果您希望“郵件威脅防護”元件在經由 POP3、SMTP、NNTP 和 IMAP 協議傳送的電子郵件被使用者的電腦收到之前進行掃描，請選取“**掃描 POP3、SMTP、NNTP 和 IMAP 流量**”核取方塊。

  如果您不希望“郵件威脅防護”元件在經由 POP3、SMTP、NNTP 和 IMAP 協議傳送的電子郵件到達使用者的電腦之前進行掃描，請清除“**掃描 POP3、SMTP、NNTP 和 IMAP 流量**”核取方塊。在這種情況下，如果選定了“**連線 Microsoft Outlook 延伸程式**”核取方塊，使用者電腦上接收到郵件時，郵件將經過 Microsoft Office Outlook 郵件用戶端中嵌入的“郵件威脅防護”延伸外掛程式的掃描。

  如果您使用的郵件用戶端不是 Microsoft Office Outlook，則如果清理了“**掃描 POP3、SMTP、NNTP 和 IMAP 流量**”核取方塊，郵件威脅防護元件不會掃描經由 POP3、SMTP、NNTP 和 IMAP 通訊協定傳輸的電子郵件。

- 如果您希望允許從 Microsoft Office Outlook 存取“郵件威脅防護”設定並且希望經由 POP3、SMTP、NNTP、IMAP 和 MAPI 協議傳送的郵件在到達電腦後由嵌入在 Microsoft Office Outlook 的延伸外掛程式進行掃描，請選取“**連線 Microsoft Outlook 延伸程式**”核取方塊。

  如果您希望封鎖從 Microsoft Office Outlook 存取“郵件威脅防護”設定並且禁止經由 POP3、SMTP、NNTP、IMAP 和 MAPI 協議傳送的郵件在到達電腦後由嵌入在 Microsoft Office Outlook 的延伸外掛程式進行掃描，請清除“**連線 Microsoft Outlook 延伸程式**”核取方塊。

  “郵件威脅防護”延伸程式在安裝 Kaspersky Endpoint Security 時嵌入在 Microsoft Office Outlook 郵件用戶端中。

6. 儲存變更。

# 掃描附加於電子郵件中的複合檔案

您可以啟用或停用掃描郵件附件，限制要掃描的郵件附件的最大大小並限制郵件附件最大掃描時長。

*若要設定對附加於電子郵件中的複合檔案掃描：*

1. 在“應用程式主視窗”中，點擊⚙ 按鈕。
2. 在應用程式設定視窗中，選取”**關鍵威脅防護**“→“**郵件威脅防護**”。
3. 點擊“**進階設定**”。

4. 在“**掃描複合檔案**“塊中，配置掃描設定：

- **掃描 Microsoft Office 格式的附加檔案**掃描 Microsoft Office 檔案（DOC，DOCX，XLS，PPT 和其他 Microsoft 副檔名）。Office 格式檔案也包含 OLE 物件。應用程式掃描小於 1 MB 的 office 格式檔案，無論該核取方塊是否被選中。
- **掃描附件中的壓縮檔案**掃描 ZIP、GZIP、BZIP、RAR、TAR、ARJ、CAB、LHA、JAR、ICE 和其它存檔。應用程式不僅依照副檔名而且依照格式掃描存檔。當檢查封存時，應用程式會執行巡迴解壓縮。這可讓人偵測多層封存（封存內的封存）內的威脅。

  如果在掃描期間應用程式在郵件的文字中偵測到存檔的密碼，該密碼將被用來掃描惡意應用程式的存檔的內容。在此情況下不儲存密碼。存檔在掃描期間被解壓縮。如果在解壓縮過程中發生應用程式錯誤，您可以手動刪除儲存到以下路徑的解壓縮檔案： %systemroot%\temp。這些檔案有 PR 前綴。

- **不掃描大於該值的存檔 N MB（從 1 到 9999）**。如果選擇此方塊，“郵件威脅防護”元件將在掃描中排除大小超過指定值的電子郵件附件。如果清空此方塊，則“郵件威脅防護”元件可以掃描任意尺寸的電子郵件附件。
- **限制壓縮檔案的檢查時間為 N 秒（從 1 到 9999）**。如果選擇此方塊，則分配的用於掃描電子郵件壓縮檔案附件的時間將被限制為指定的長度。

5. 儲存變更。

# 電子郵件訊息附件篩選

附件篩選功能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。

*若要設定附件的篩選，請執行以下操作：*

1. 在“應用程式主視窗”中，點擊⚙ 按鈕。
2. 在應用程式設定視窗中，選取”**關鍵威脅防護**“→“**郵件威脅防護**”。
3. 點擊“**進階設定**”。
4. 在“**附件篩選**”塊中執行以下操作之一：

- **停用篩選功能**如果選擇此選項，“郵件威脅防護”元件將不篩選屬於電子郵件附件的檔案。
- **重新命名選取類型的附件**如果選擇此選項，郵件威脅防護元件將用下劃線字符（例如，attachment.doc__）替換在指定類型的附件檔案中找到的最後一個延伸字符。因此，為了開啟檔案，使用者必須重命名檔案。
- **刪除選取類型的附件**如果選擇此選項，“郵件威脅防護”元件將從電子郵件中刪除指定的附件類型。

5. 如果您在上個步驟中選取了**"重新命名選取類型的附件"**選項或者**"刪除選取類型的附件"**選項，則選取相應類型檔案旁的核取方塊。

6. 儲存變更。

# 匯出和匯入附件篩選延伸程式

您可以將附件篩選延伸程式清單匯出到 XML 檔案。您可以使用匯出/匯入功能來備份延伸程式清單，或將清單遷移到其他伺服器。

**如何在管理主控台 (MMC) 中匯出和匯入附件篩選延伸程式清單**

1. 在網頁主控台的主視窗中，選擇**資產（裝置）→政策和設定檔**。

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. 要匯出**"附件篩選"**塊中的延伸程式清單：

   a. 選擇您要匯出的延伸程式。

   b. 點擊**"匯出"**連接。

   c. 在開啟的視窗中，指定您要將延伸程式清單匯出到的 XML 檔案的名稱，然後選取要儲存此檔案的資料夾。

   d. 儲存檔案。

      Kaspersky Endpoint Security 會將整個延伸程式清單匯出到 XML 檔案。

6. 要匯入**"附件篩選"**塊中的延伸程式清單：

   a. 點擊**"匯入"**連接。

   b. 在開啟的視窗中，選取要從中匯入延伸程式清單的 XML 檔案。

   c. 開啟檔案。

      如果電腦已經具有延伸程式清單，則 Kaspersky Endpoint Security 將提示您刪除現有清單或從 XML 檔案向其中新增新項目。

7. 儲存變更。

1. 在卡巴斯基安全管理中心管理主控台樹狀目錄中，選取**政策**。

2. 選擇必要的政策並點擊以開啟政策內容。

3. 在政策視窗中，選擇**"關鍵威脅防護 → 郵件威脅防護"**。

4. 在**"安全等級"**塊中，點擊**"設定"**按鈕。

5. 在開啟的視窗中選擇“**附件篩選**”標籤。

6. 要匯出延伸程式清單：

   a. 選擇您要匯出的延伸程式。要選擇多個連接埠，請使用**CTRL**或**SHIFT**鍵。

   b. 點擊”**匯出**”連接。

   c. 在開啟的視窗中，指定您要將延伸程式清單匯出到的 XML 檔案的名稱，然後選取要儲存此檔案的資料夾。

   d. 儲存檔案。

      Kaspersky Endpoint Security 會將整個延伸程式清單匯出到 XML 檔案。

7. 要匯入延伸程式清單：

   a. 點擊”**匯入**”連接。

   b. 在開啟的視窗中，選取要從中匯入延伸程式清單的 XML 檔案。

   c. 開啟檔案。

      如果電腦已經具有延伸程式清單，則 Kaspersky Endpoint Security 將提示您刪除現有清單或從 XML 檔案向其中新增新項目。

8. 儲存變更。

# 掃描 Microsoft Office Outlook 中的電子郵件

在 Kaspersky Endpoint Security 安裝期間，“郵件威脅防護”延伸程式嵌入到 Microsoft Office Outlook（以下簡稱 Outlook）中。該延伸程式允許在郵件用戶端級別而不是協定級別掃描郵件。除了郵件之外，該延伸程式還允許您掃描透過 MAPI 接口從 Microsoft Exchange 儲存庫接收到的物件（例如，日曆中的物件）。此掃描在郵件用戶端中進行。

您可從 Outlook 內部快速開啟“郵件威脅防護”元件設定，指定在何時掃描電子郵件以尋找掃描病毒和其他威脅。

> 郵件威脅防護延伸支援 Outlook 2010、2013、2016、2019 和 2021 的操作。

在 Outlook 中，接收的電子郵件首先由“郵件威脅防護”元件進行掃描（如果在 Kaspersky Endpoint Security 介面中選定了“掃描 POP3、SMTP、NNTP 和 IMAP 流量”核取方塊），然後由 Outlook 的“郵件威脅防護”延伸程式進行掃描。如果“郵件威脅防護”元件在郵件中偵測到惡意物件，會就此事件向您發出警訊。

如果在 Kaspersky Endpoint Security 介面中選定了“Microsoft Outlook 延伸程式已連線”，則可以直接在 Outlook 中配置“郵件威脅防護”元件設定（請見下圖）。




Outlook 中的郵件威脅防護元件設定

傳送的電子郵件首先由 Outlook 的“郵件威脅防護”延伸程式進行掃描，然後由“郵件威脅防護”元件進行掃描。

如果使用 Outlook 的“郵件威脅防護”延伸程式掃描郵件，建議使用緩衝區的交換模式。有關 Cached Exchange 模式的詳細資訊和對其用途的建議，請參閱 Microsoft 知識庫。

*要設定 Outlook 的“郵件威脅防護”延伸程式的作業模式：*

1. 在卡巴斯基安全管理中心管理主控台樹狀目錄中，選取**政策**。
2. 選擇必要的政策並點擊以開啟政策內容。
3. 在政策視窗中，選擇“**關鍵威脅防護 → 郵件威脅防護**”。
4. 在”**安全等級**”塊中，點擊”**設定**”按鈕。
5. 在開啟的視窗中的 **連線**塊中，點擊 **設定** 按鈕。
6. 在“**電子郵件防護**”視窗中執行下列操作之一：
   - 如果您希望 Outlook 的“郵件威脅防護”延伸程式在郵件到達信箱時進行掃描，選取“**接收時掃描**”核取方塊。
   - 如果您希望 Outlook 的“郵件威脅防護”延伸程式在使用者開啟郵件時進行掃描，請選中“**讀取時掃描**”核取方塊。
   - 如果您希望 Outlook 的“郵件威脅防護”延伸程式在傳送郵件時掃描郵件，請選中“**傳送時掃描**”核取方塊。
7. 儲存變更。

# 掃描 Thunderbird、MyOffice和 R7-Office 中的電子郵件

“郵件威脅防護”元件掃描傳送和接收電子郵件的附件是否有病毒和其他威脅。對於 Mozilla Thunderbird、MyOffice Mail 和 R7-Office Organizer 郵件用戶端，應用程式只能在 *協定級別*（POP3、SMTP、IMAP、NNTP）存取郵件。

若要掃描 Mozilla Thunderbird、MyOffice Mail 及 R7-Office Organizer 郵件用戶端的流量，您需要將卡巴斯基憑證新增至專屬憑證儲存區，並選擇該專屬憑證儲存區。

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。

## 即時郵件威脅防護

郵件威脅防護可以掃描傳入和傳出的郵件。預設情況下，“郵件威脅防護”元件將自動嘗試對已經偵測到的所有受感染電子郵件執行解毒操作。如果解毒失敗，“郵件威脅防護”元件會刪除感染的電子郵件。如果在附件中偵測到惡意檔案，Kaspersky Endpoint Security 會將有關已執行操作的資訊新增到郵件主旨，例如，*[郵件已處理] <郵件主旨>*。

使用 Mozilla Thunderbird 郵件用戶端時，如果使用篩檢程式將訊息移出“收件箱”資料夾，“郵件威脅防護”元件將不能掃描病毒、其他惡意程式或經由 IMAP 協定傳送的電子郵件。

## 郵件資料庫中的惡意軟體掃描

*惡意軟體掃描* 工作可以 掃描郵件格式檔案。如果在這些郵件用戶端的檔案中偵測到惡意物件，Kaspersky Endpoint Security 只會將偵測到的物件的資訊加入活動威脅清單。無論工作設定如何，應用程式都不會對郵件資料庫中的已感染檔案進行解毒或刪除。

## 消除活動威脅

郵件威脅防護可在協定層級防止電腦感染，但如果電腦在安裝 Kaspersky Endpoint Security 之前已被感染，則應用程式可能只能在郵件資料庫中偵測威脅。郵件威脅防護不包含專門用於將郵件拆分成各個部分（郵件頭、主體、附件）的元件，就像對 Microsoft Office Outlook那樣。因此，該應用程式無法刪除或解毒偵測到的物件。Kaspersky Endpoint Security 只會將偵測到的物件的相關資訊新增到活動威脅清單。

消除活動威脅：

1. 在郵件用戶端介面中手動尋找並刪除包含偵測到的物件的訊息。

   應用程式會將偵測到的物件的相關資訊新增到活動威脅清單。

   偵測到的物件卡片範例：

| | |
|---|---|
| | **HEUR:Trojan.PDF.Phish.gen**<br>物件：`C:\Users\admin\AppData\Roaming\Thunderbird\Profiles\ov56jpz0.default-release\Mail\mail.company.ru\Inbox// [From USER NAME <company@mail.com>][Date 25 Sep 2025 20:05:36] [Subj Mail title X] Object.pdf` |

2. 執行資料庫壓縮操作。

   當郵件被在使用者介面中刪除時，郵件用戶端只會新增一個刪除標記。郵件用戶端只有在資料庫壓縮後才會真正刪除郵件。有關資料庫壓縮的詳細資訊，請參閱郵件用戶端的說明（例如，Mozilla Thunderbird）。

3. 再一次執行 *惡意軟體掃描* 工作，確保*威脅*已不存在。

# 網路威脅防護

*網路威脅防護*元件（也稱為入侵偵測系統，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。

# 啟用和停用網路威脅防護

預設情況下，"網路威脅防護"已啟用並在最佳化模式下執行。Kaspersky Endpoint Security 會監控入站網路流量以了解網路攻擊的活動特徵並封鎖攻擊。

**如何在管理主控台（MMC）中啟用或停用網路威脅防護元件**

1. 在卡巴斯基安全管理中心管理主控台樹狀目錄中，選取**政策**。
2. 選擇必要的政策並點擊以開啟政策內容。
3. 在政策視窗中，選擇"**關鍵威脅防護 → 網路威脅防護**"。
4. 使用"**網路威脅防護**"核取方塊來啟用或停用元件。
5. 儲存變更。若要在電腦上套用該政策，請關閉掛鎖。

**如何在網頁主控台和雲端主控台中啟用或停用"網路威脅防護"元件**

1. 在網頁主控台的主視窗中，選擇**資產（裝置）→ 政策和設定檔**。
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. 使用"**網路威脅防護已啟用**"切換開關可啟用或停用元件。
6. 儲存變更。

**如何在應用程式介面中啟用或停用網路威脅防護**

1. 在“應用程式主視窗”中，點擊⚙按鈕。
2. 在應用程式設定視窗中，選取”**關鍵威脅防護**“→“**網路威脅防護**”。




網路威脅防護設定

3. 使用“**網路威脅防護**“切換開關可啟用或停用元件。
4. 儲存變更。

# 封鎖發動攻擊的電腦

如果啟用網路威脅防護元件，Kaspersky Endpoint Security 會自動封鎖網路威脅。此外，該應用程式可以封鎖發動攻擊的電腦並在一定時間內限製傳送網路封包。預設情況下，Kaspersky Endpoint Security 會封鎖電腦一小時。

**如何在管理主控台 (MMC) 中封鎖發動攻擊的電腦**

1. 在卡巴斯基安全管理中心管理主控台樹狀目錄中，選取**政策**。
2. 選擇必要的政策並點擊以開啟政策內容。
3. 在政策視窗中，選擇“**關鍵威脅防護 → 網路威脅防護**”。

4. 在**網路威脅防護設定**下面，選擇 **封鎖攻擊裝置 氮 分** 核取方塊。

   如果啟用此選項，“網路威脅防護”元件將把發動攻擊的電腦新增至封鎖清單。這意味著，“網路威脅防護”元件將會在該攻擊電腦的首次網路攻擊嘗試後的指定時間段內，封鎖與該電腦的網路連線。此封鎖操作將會自動防護電腦避免以後來自同一位址的攻擊。攻擊電腦必須待在封鎖清單中的最短時間為一分鐘。最長時間為 999 分鐘。

5. 在“**封鎖攻擊裝置 N 分**”核取方塊右側的欄位中，為發動攻擊的電腦設定不同的封鎖時長。

6. 儲存變更。

**如何在網頁主控台和雲端主控台中封鎖發動攻擊的電腦**

1. 在網頁主控台的主視窗中，選擇**資產（裝置）→ 政策和設定檔**。

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. 在“**偵測到威脅後的動作**“塊中，選中“**封鎖攻擊和攻擊裝置（分鐘）**”核取方塊。

   如果啟用此選項，“網路威脅防護”元件將把發動攻擊的電腦新增至封鎖清單。這意味著，“網路威脅防護”元件將會在該攻擊電腦的首次網路攻擊嘗試後的指定時間段內，封鎖與該電腦的網路連線。此封鎖操作將會自動防護電腦避免以後來自同一位址的攻擊。攻擊電腦必須待在封鎖清單中的最短時間為一分鐘。最長時間為 999 分鐘。

6. 變更攻擊電腦的封鎖持續時間。

7. 儲存變更。

### 如何在應用程式的使用者介面中封鎖發動攻擊的電腦

1. 在“應用程式主視窗”中，點擊⚙按鈕。
2. 在應用程式設定視窗中，選取“**關鍵威脅防護**”→“**網路威脅防護**”。




網路威脅防護設定

3. 開啟 **封鎖攻擊裝置 氮 分鐘** 開關。

   如果啟用此選項，“網路威脅防護”元件將把發動攻擊的電腦新增至封鎖清單。這意味著，“網路威脅防護”元件將會在該攻擊電腦的首次網路攻擊嘗試後的指定時間段內，封鎖與該電腦的網路連線。此封鎖操作將會自動防護電腦避免以後來自同一位址的攻擊。攻擊電腦必須待在封鎖清單中的最短時間為一分鐘。最長時間為 999 分鐘。

4. 在“**封鎖攻擊裝置 N 分鐘**”切換開關下的欄位中，為發動攻擊的電腦設定不同的封鎖時長。
5. 儲存變更。

結果，當 Kaspersky Endpoint Security 偵測到在使用者電腦上有網路攻擊企圖時，它將封鎖與發動攻擊的電腦的所有連線。Kaspersky Endpoint Security 可建立 *偵測到網路攻擊* 事件。事件包含有關攻擊電腦的資訊：IP 和 MAC 位址。

您可以在應用程式的使用者介面或卡巴斯基安全管理中心主控台 15.1 或更高版本中檢視攻擊電腦的 MAC 位址。




關於網路攻擊偵測的通知

當指定時間用完時，Kaspersky Endpoint Security 會解除對電腦的封鎖。除了報告中的 *偵測到網路攻擊* 事件之外，卡巴斯基安全管理中心主控台不提供用於監控被封鎖電腦的其他工具。您只能在應用程式介面中檢視被封鎖電腦的清單。此功能由*網路監控*工具提供。您還可以使用網路監控工具來解鎖電腦。

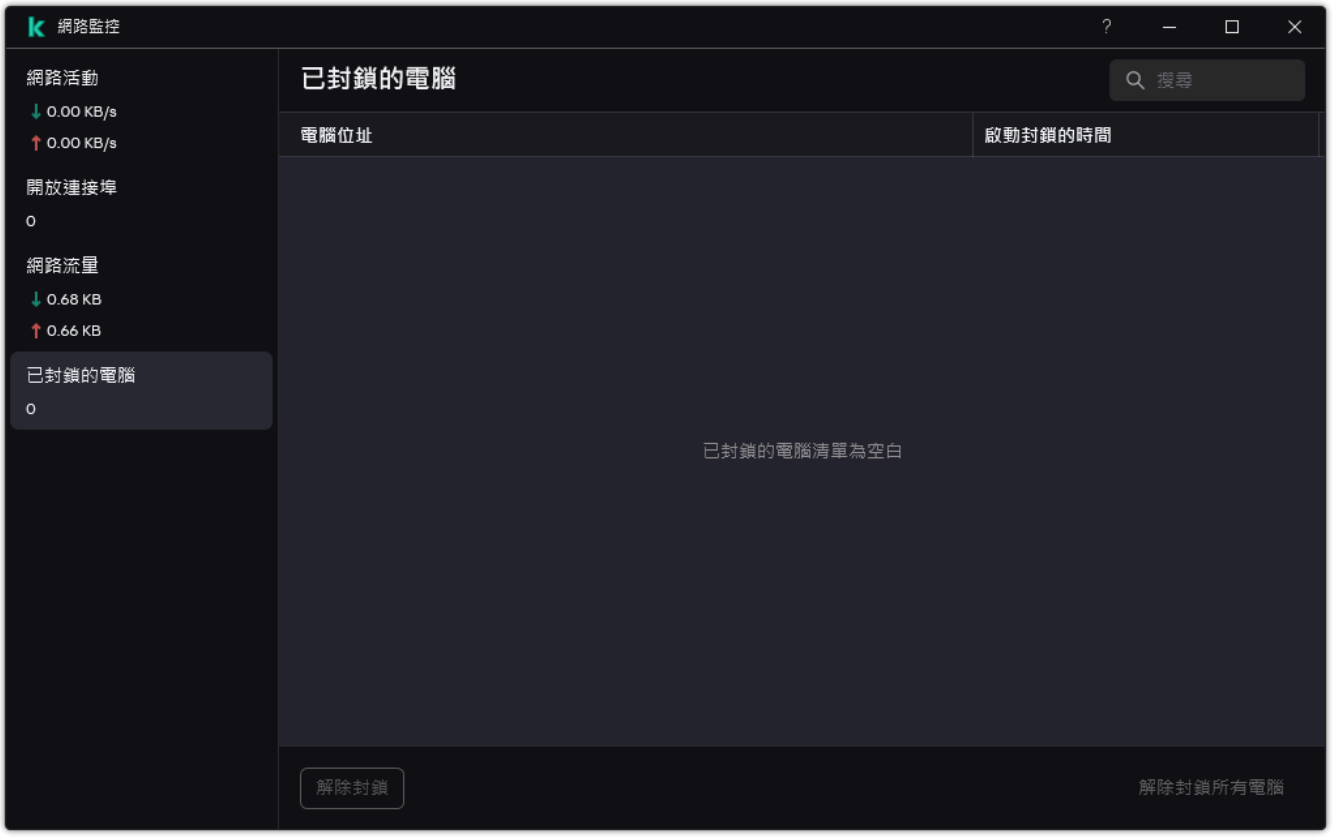
*要解鎖電腦：*

1. 在應用程式主視窗的**"正在監控"**區域中，點擊**"網路監控"**圖標。
2. 選擇**"已封鎖的電腦"**標籤。

   這將開啟被封鎖電腦清單（見下圖）。

   重新啟動應用程式以及變更網路威脅防護設定時，Kaspersky Endpoint Security 會清除封鎖清單。

3. 選擇您要取消封鎖的電腦，然後點擊**解除封鎖**。




被封鎖的電腦清單

# 設定排除在封鎖外的位址

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。您還可以選擇用於通信並允許特定網路活動的協定和連接埠。

Kaspersky Endpoint Security 12.2 中新增了選擇排除哪些協定和連接埠的功能。確保應用程式和管理外掛程式已更新至版本 12.2 或更高版本。如果您使用的是早期版本的應用程式或管理外掛程式，Kaspersky Endpoint Security 只能依據 IP 位址允許網路活動。

### 如何在管理主控台 (MMC) 中設定排除在封鎖外的位址

1. 在卡巴斯基安全管理中心管理主控台樹狀目錄中，選取**政策**。
2. 選擇必要的政策並點擊以開啟政策內容。
3. 在政策視窗中，選擇**"關鍵威脅防護 → 網路威脅防護"**。
4. 在**"網路威脅防護設定"**塊中，點擊**"排除項目"**按鈕。
5. 在開啟的視窗中，點擊**"新增"**按鈕。

6. 輸入不封鎖網路攻擊的電腦的 IP 位址。
   如果需要，選擇透過其傳輸資料的協定和連接埠。

7. 儲存變更。

**如何在網頁主控台和雲端主控台中配置排除在封鎖外的位址**

1. 在網頁主控台的主視窗中，選擇**資產（裝置）→ 政策和設定檔**。

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. 在視窗上方，點擊**"受信任 IP 位址"**連接。

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。
   如果需要，選擇透過其傳輸資料的協定和連接埠。

8. 儲存變更。

### 如何在應用程式的使用者介面中設定排除在封鎖外的位址

1. 在“應用程式主視窗”中，點擊 按鈕。
2. 在應用程式設定視窗中，選取”**關鍵威脅防護**“→“**網路威脅防護**”。




網路威脅防護設定

3. 點擊”**管理排除項目**”連接。
4. 在開啟的視窗中，點擊“**新增**”按鈕。
5. 輸入不封鎖網路攻擊的電腦的 IP 位址。

   如果需要，選擇透過其傳輸資料的協定和連接埠。
6. 儲存變更。

# 匯出和匯入封鎖排除項目清單

您可以將排除項目清單匯出到 XML 檔案。然後，您可以修改檔案，例如，新增大量相同類型的位址。您還可以使用匯出/匯入功能來備份排除項目清單，或將清單遷移到其他伺服器。

### 如何在管理主控台 (MMC) 中匯出和匯入排除項目清單

1. 在卡巴斯基安全管理中心管理主控台樹狀目錄中，選取**政策**。
2. 選擇必要的政策並點擊以開啟政策內容。

3. 在政策視窗中，選擇**"關鍵威脅防護 → 網路威脅防護"**。

4. 在**"網路威脅防護設定"**塊中，點擊**"排除項目"**按鈕。

5. 要匯出規則清單：

   a. 選取您想要匯出的排除項目。要選擇多個連接埠，請使用**CTRL**或**SHIFT**鍵。
   如果您未選擇任何排除項目，則 Kaspersky Endpoint Security 將匯出所有排除項目。

   b. 點擊 → **匯出** 按鈕。

   c. 在開啟的視窗中，指定您要將排除項目清單匯出到的 XML 檔案的名稱，然後選取要儲存此檔案的資料夾。

   d. 儲存檔案。
   Kaspersky Endpoint Security 會將整個排除項目清單匯出到 XML 檔案。

6. 若要匯入排除項目清單：

   a. 點擊 → **匯入** 按鈕。

   b. 在開啟的視窗中，選取要從中匯入排除項目清單的 XML 檔案。

   c. 開啟檔案。
   如果電腦已經具有排除項目清單，則 Kaspersky Endpoint Security 將提示您刪除現有清單或從 XML 檔案向其中新增新項目。

7. 儲存變更。

**如何在網頁主控台和 Cloud Console 中匯出和匯入排除項目清單**

1. 在網頁主控台的主視窗中，選擇**資產（裝置）→ 政策和設定檔**。

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. 在視窗上方，點擊**"受信任 IP 位址"**連接。
排除項目清單開啟。

6. 要匯出規則清單：

   a. 選取您想要匯出的排除項目。

   b. 點擊 → **匯出** 按鈕。
   Kaspersky Endpoint Security 會將排除項目清單匯出到預設下載資料夾中的 JSON 檔案。

7. 若要匯入排除項目清單：

   a. 點擊 → **匯入** 按鈕。

      在開啟的視窗中，選取要從中匯入排除項目清單的 JSON 檔案。

   b. 開啟檔案。

      如果電腦已經具有排除項目清單，則 Kaspersky Endpoint Security 將提示您刪除現有清單或從 JSON 檔案向其中新增新項目。

8. 儲存變更。

# 按類型配置網路威脅防護

Kaspersky Endpoint Security 使您可以管理針對以下類型網路攻擊的防護：

- *網路泛洪*是對組織的網路資源（例如 Web 伺服器）的攻擊。這種攻擊包括傳送大量請求以超載網路資源的帶寬。發生這種情況時，使用者將無法存取組織的網路資源。
- *連接埠掃描*攻擊包括掃描電腦上的 UDP 連接埠、TCP 連接埠和網路服務。此攻擊使攻擊者可以在進行更危險類型的網路攻擊之前確定電腦的漏洞程度。連接埠掃描還使攻擊者能夠識別電腦上的作業系統，並為該作業系統選擇適當的網路攻擊。
- *MAC 欺騙攻擊*包括變更網路裝置（網卡）的 MAC 位址。結果，攻擊者可以將傳送到某台裝置的資料重新導向到另一台裝置，並獲得對該資料的存取權限。Kaspersky Endpoint Security 允許您封鎖 MAC 欺騙攻擊並接收關於攻擊的通知。

如果某些允許的應用程式執行這些類型攻擊的典型操作，您可以停用對這些類型攻擊的偵測。這將有助於避免誤報。

預設情況下，Kaspersky Endpoint Security 不監視網路泛洪、連接埠掃描和 MAC 欺騙攻擊。

我們不建議在 Microsoft Hyper-V 基礎架構中的虛擬機上啟用 MAC 欺騙防護。由於 Microsoft Hyper-V 平台的特殊性，Kaspersky Industrial CyberSecurity for Nodes 可能會因誤報結果而封鎖 Hypervisor。

**如何在管理主控台 (MMC) 中按類型配置網路威脅防護**

1. 在卡巴斯基安全管理中心管理主控台樹狀目錄中，選取**政策**。
2. 選擇必要的政策並點擊以開啟政策內容。
3. 在政策視窗中，選擇“**關鍵威脅防護 → 網路威脅防護**”。
4. 使用“**將連接埠掃描和網路洪水當做攻擊處理**”核取方塊來啟用或停用對這些攻擊的偵測。

   如果啟用此功能，Kaspersky Endpoint Security 會監控網路流量以進行連接埠掃描和網路泛洪。如果偵測到此類行為，應用程式會通知使用者並將相應事件傳送到卡巴斯基安全管理中心。該應用程式提供有關發出請求的電腦的資訊。此資訊對於及時回應很有必要。但是，Kaspersky Endpoint Security 不會封鎖發出請求的電腦，因為此類流量可能在公司網路上很常見。

5. 在“**MAC 欺騙防護模式**”區域，選取以下選項之一：

   - **不跟蹤 MAC 欺騙**
   - **通知**
   - **封鎖**

6. 儲存變更。

**如何在網頁主控台和雲端主控台中配置網路威脅防護**

1. 在網頁主控台的主視窗中，選擇**資產（裝置）→ 政策和設定檔**。
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. 使用“**將連接埠掃描和網路洪水當做攻擊處理**”核取方塊來啟用或停用對這些攻擊的偵測。

   如果啟用此功能，Kaspersky Endpoint Security 會監控網路流量以進行連接埠掃描和網路泛洪。如果偵測到此類行為，應用程式會通知使用者並將相應事件傳送到卡巴斯基安全管理中心。該應用程式提供有關發出請求的電腦的資訊。此資訊對於及時回應很有必要。但是，Kaspersky Endpoint Security 不會封鎖發出請求的電腦，因為此類流量可能在公司網路上很常見。

6. 使用 **網路威脅防護已啟用** 切換開關來啟用對這些攻擊的偵測。
7. 儲存變更。

### 如何在應用程式介面中按類型配置網路威脅防護

1. 在“應用程式主視窗”中，點擊⚙按鈕。
2. 在應用程式設定視窗中，選取“**關鍵威脅防護**”→“**網路威脅防護**”。




網路威脅防護設定

3. 使用切換“**將連接埠掃描和網路洪水當做攻擊處理**”來啟用或停用對這些攻擊的偵測。

   如果啟用此功能，Kaspersky Endpoint Security 會監控網路流量以進行連接埠掃描和網路泛洪。如果偵測到此類行為，應用程式會通知使用者並將相應事件傳送到卡巴斯基安全管理中心。該應用程式提供有關發出請求的電腦的資訊。此資訊對於及時回應很有必要。但是，Kaspersky Endpoint Security 不會封鎖發出請求的電腦，因為此類流量可能在公司網路上很常見。

4. 使用切換“**MAC 欺騙防護**”來啟用或停用對這些攻擊的偵測。
5. 在“**偵測到 MAC 欺騙攻擊時的操作**”區域，選取以下選項之一：
   - **通知**
   - **封鎖**
6. 儲存變更。

# 防火牆

在網際網路或區域網路上工作時，防火牆會封鎖未經授權的電腦連線。防火牆還控制腦上應用程式的網路活動。這允許您防護公司區域網路免受身分竊盜和其他攻擊。該元件借助防毒資料庫、卡巴斯基安全網路雲端服務和預先定義的*網路規則*來提供電腦防護。

網路代理用於與卡巴斯基安全管理中心進行交互。防火牆會自動建立應用程式和網路代理正常工作所需的網路規則。結果，防火牆在电脑上開啟了多個連接埠。哪個連接埠開啟取決於电脑的角色（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 。

## 網路規則

您可以在以下等級配置網路規則：

- *網路封包規則*。網路封包規則將對網路封包進行限制，與應用程式無關。此類規則將限制透過特定連接埠的選定資料協定傳送和接收的網路流量。Kaspersky Endpoint Security 具有預先定義的網路封包規則，其中的權限由 Kaspersky 專家推薦。
- *應用程式網路規則*。應用程式網路規則將對特定應用程式的網路活動進行限制。它們不僅將網路封包的特徵列入重要參考因素，還把接收或傳送此網路封包的應用程式列入重要參考因素中。

應用程式對作業系統資源、處理程序和個人資料的控制存取由"主機入侵防禦"元件透過*應用程式權限*提供。

在應用程式首次啟動期間，"防火牆"會執行以下操作：

1. 使用下載的防毒資料庫檢查應用程式的安全性。
2. 在卡巴斯基安全網路中檢查應用程式安全性。

   建議您加入卡巴斯基安全網路以幫助"防火牆"元件更有效地工作。
3. 將應用程式放置在其中一個信任群組中：*受信任*，*低限制*，*高限制*，*不信任*。

   信任群組定義了在控制應用程式活動時 Kaspersky Endpoint Security 所引用的權限。Kaspersky Endpoint Security 會將應用程式放置在某個信任群組中，實際取決於該應用程式可能對電腦造成的危險等級而定。

   Kaspersky Endpoint Security 將應用程式放置在"防火牆"和"主機入侵防禦"元件的信任群組中。您不能僅變更"防火牆"或"主機入侵防禦"的信任群組。

   如果您拒絕加入 KSN 或沒有網路，Kaspersky Endpoint Security 會根據"主機入侵防禦"元件的設定將應用程式放置在某個信任群組中。從 KSN 收到應用程式的信譽後，可以自動變更信任群組。
4. 它是根據信任群組封鎖應用程式的網路活動。例如，不允許"*高限制*"信任群組中的應用程式使用任何網路連線。

下次啟動應用程式時，Kaspersky Endpoint Security 會檢查該應用程式的完整性。如果應用程式未變更，則該元件將對其套用目前的網路權限。如果應用程式已經過修改，Kaspersky Endpoint Security 會分析應用程式，就像它初次開機時一樣。

### 網路規則優先順序

每條規則都有優先順序。規則在清單中的位置越高，優先順序越高。如果將網路活動新增到多條規則中，"防火牆"會根據優先等級最高的規則來管理網路活動。

網路封包規則的優先順序比應用程式網路規則高。如果網路封包規則和應用程式網路規則指定了同一類別的網路活動，則該網路活動將根據網路封包規則進行處理。

應用程式的網路規則以特定方式工作。應用程式的網路規則包括基於網路狀態的存取規則：*公用網路*，*本機網路*，*受信任網路*。例如，預設情況下，"*高限制*"信任群組中的應用程式在所有狀態的網路中均不允許進行任何網路活動。如果為單個應用程式（父應用程式）指定了網路規則，則其他應用程式的子處理程序將依據父應用程式的網路規則執行。如果應用程式沒有網路規則，則子程序將根據應用程式信任組的網路存取規則執行。

例如，對於瀏覽器 X 以外的所有應用程式，您已禁止所有狀態的網路中的任何網路活動。如果從瀏覽器 X（父應用程式）開始安裝瀏覽器 Y（子處理程序），則瀏覽器 Y 安裝程式將存取網路並下載必要的檔案。安裝後，根據防火牆設定，瀏覽器 Y 將被拒絕執行任何網路連線。要禁止作為子處理程序的瀏覽器 Y 安裝程式的網路活動，必須為瀏覽器 Y 的安裝程式新增網路規則。

### 網路連線類型

"防火牆"允許您根據網路連線類型來控制網路活動。Kaspersky Endpoint Security 從電腦的作業系統接收網路連線類型。作業系統中的網路連線類型由使用者在設定連線時設定。您可以在 Kaspersky Endpoint Security 設定中變更網路連線的類型。"防火牆"將根據 Kaspersky Endpoint Security 設定中指定的而不是作業系統中的網路類型來監控網路活動。

下列網路連線類型可以使用：

- **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）。當使用者操作連接到此類網路的電腦時，防火牆可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。防火牆根據為每一個應用程式設定的網路規則，篩選應用程式的網路活動。

  防火牆預設為網際網路分配*公用網路*類型。您無法變更網際網路的類型。

- **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。

## 啟用或停用防火牆

預設情況下，防火牆為啟動狀態，各種功能均設定為最佳化。

**如何在管理主控台（MMC）中啟用或停用防火墙**

1. 在卡巴斯基安全管理中心管理主控台樹狀目錄中，選取**政策**。
2. 選擇必要的政策並點擊以開啟政策內容。
3. 在政策視窗中，選取**"關鍵威脅防護"→"防火牆"**。
4. 使用**"防火牆"**核取方塊來啟用或停用元件。
5. 儲存變更。

**如何在網頁主控台和雲端主控台中啟用或停用防火墙**

1. 在網頁主控台的主視窗中，選擇**資產（裝置）→ 政策和設定檔**。
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. 使用**"防火牆已啟用"**切換開關可啟用或停用元件。
6. 儲存變更。

**如何在應用程式介面中啟用或停用防火墙**

1. 在"應用程式主視窗"中，點擊⚙按鈕。
2. 在應用程式設定視窗中，選取**"關鍵威脅防護"→"防火牆"**。
3. 使用**"防火牆"**切換開關可啟用或停用元件。
4. 儲存變更。

結果，如果防火墙被啟用，Kaspersky Endpoint Security 將控制網路活動和封鎖未經授權的網路連線到您的電腦，以及封鎖您的電腦上未經授權的應用程式的網路活動。網路活動也被網路威脅防護元件所控制。網路威脅防護元件（也稱為入侵偵測系統）可監控入站網路流量以了解網路攻擊的活動特徵。

Kaspersky Endpoint Security 會在報告中記錄網路攻擊事件，與防火墙設定無關。即使防火墙使用規則封鎖了網路連線，因此防止了網路攻擊，網路威脅防護元件也會記錄網路攻擊事件。要求就您的組織內的電腦上的網路攻擊產生統計資訊。

# 變更網路連線類型

防火牆預設為網際網路分配*公用網路*類型。您無法變更網際網路的類型。

*若要變更網路連線類型，請執行以下操作：*

1. 在"應用程式主視窗"中，點擊⚙按鈕。
2. 在應用程式設定視窗中，選取"**關鍵威脅防護**"→"**防火牆**"。
3. 點擊"**可用網路**"。
4. 選取您想要變更其類型的網路連線。
5. 在"**網路類型**"列中，選擇網路連線的類型：
   - **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）。當使用者操作連接到此類網路的電腦時，防火牆可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。防火牆根據為每一個應用程式設定的網路規則，篩選應用程式的網路活動。
   - **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。
6. 儲存變更。

# 管理網路封包規則

您在管理網路封包規則時可執行以下操作：

- 建立新的網路封包規則。

  您可以透過建立一個可應用於網路封包和資料流的條件集和操作集來建立新的網路封包規則。

- 啟用或停用網路封包規則。

  預設情況下，由防火牆建立的所有網路封包規則處於"*開*"狀態。當啟用網路封包規則時，防火牆套用此規則。

  您可以停用網路封包規則清單中選取的任何網路封包規則。當停用網路封包規則時，防火牆將暫時不套用此規則。

  > 預設情況下，新增到網路封包規則清單中的自訂網路封包規則處於"*開*"狀態。

- 編輯現有網路封包規則的設定。

  當您建立新的網路封包規則之後，您始終可以重新編輯其設定並根據需要進行修改。

- 變更網路封包規則的防火牆操作。

  在網路封包規則清單中，您可以編輯防火牆在偵測到與特定網路封包規則相符的網路活動時的操作。

- 變更網路封包規則的優先順序。

  您可以提高或降低清單中選取的網路封包規則的優先順序。

- 刪除網路封包規則。

您可以刪除網路封包規則以停止防火牆將此規則應用於偵測網路活動，並停止將此規則顯示在"*關*"狀態的網路封包規則清單中。

# 建立網路封包規則

防火牆根據網路封包規則篩選電腦上的所有網路活動。網路封包規則包含防火牆套用於控制電腦網路連線的條件（例如方向、協定）。網路封包規則也指定防火牆對符合規則的連線執行的操作（允許或封鎖連線）。

## 建立網路封包規則的建議

您可以指定一個 IP 位址或一個 IP 位址範圍來篩選網路活動。您也可以指定 DNS 名稱，但我們建議使用 IP 位址和 IP 位址範圍。在網路封包名稱中使用 DNS 名稱可能不安全，因為 DNS 伺服器的擁有者可以修改 DNS 記錄的參數。惡意行為者還可以偽造 DNS 訊息並繞過防火牆規則。

您可以使用 網頁控制規則 按 DNS 名稱控製網路連線。如果需要在防火牆規則中指定 DNS 名稱：

- 確保企業區域網路的安全。
- 確保快取和權威 DNS 伺服器的安全。
- 啟用 DNS 記錄防修改保護。

在建立網路封包規則時，請記得，它們的優先順序比應用程式網路規則高。

## 建立網路封包規則的方法

您可以透過以下方式建立網路封包規則：

- 使用網路監控工具。

  *網路監控*是一個用於即時檢視網路活動資訊的工具。這很方便，因為您不需要配置所有規則設定。某些防火牆設定將從網路監控資料中自動插入。網路監控僅在應用程式介面中可用。

- 配置防火墻設定。

  這使您可以微調防火牆設定。您可以為任何網路活動建立規則，即使當前沒有網路活動也是如此。

**如何使用網路監控工具在應用程式介面中建立網路封包規則**

1. 在應用程式主視窗的"**正在監控**"區域中，點擊"**網路監控**"圖標。
2. 選擇"**網路活動**"標籤。

   "**網路活動**"標籤顯示電腦目前所有活動的網路連線。接收和傳送的網路連線都將同時顯示。
3. 在網路連線的內容功能表中，選擇"**建立網路封包規則**"。

   這將開啟網路規則屬性。

4. 設置封包規則的“**啟動**“狀態。
5. 在“**名稱**“欄位中手動輸入網路服務的名稱。
6. 設定網路規則設定（參見下表）。
   您可以透過點擊“**網路規則範本**“連線來選擇預定義的規則範本。規則範本描述了最常用的網路連線。
   所有網路規則設定將自動填寫。
7. 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。
8. 點擊“**儲存**”。
   新的網路規則將新增到清單中。
9. 使用“**上移**” / “**下移**”按鈕設定網路規則的優先順序。
10. 儲存變更。

**如何使用防火牆設定在應用程式介面中建立網路封包規則**

1. 在“應用程式主視窗”中，點擊⚙ 按鈕。
2. 在應用程式設定視窗中，選取”**關鍵威脅防護**“→“**防火牆**”。
3. 點擊“**封包規則**”。
   這將開啟防火牆設定的預設網路規則清單。
4. 使用 **新增** 下拉清單，選擇規則在清單中的位置：清單頂部、清單底部或所選規則的旁邊。
   規則在清單中的位置決定了規則的優先順序。清單頂部的規則具有最高優先順序。
5. 設置封包規則的“**啟動**“狀態。
6. 在“**名稱**“欄位中手動輸入網路服務的名稱。
7. 設定網路規則設定（參見下表）。
   您可以透過點擊“**網路規則範本**“連線來選擇預定義的規則範本。規則範本描述了最常用的網路連線。
   所有網路規則設定將自動填寫。
8. 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。
9. 點擊“**儲存**”。
   新的網路規則將新增到清單中。
10. 使用“**上移**” / “**下移**”按鈕設定網路規則的優先順序。
11. 儲存變更。

**如何在管理主控台 (MMC) 中建立網路封包規則**

1. 在卡巴斯基安全管理中心管理主控台樹狀目錄中，選取**政策**。
2. 選擇必要的政策並點擊以開啟政策內容。
3. 在政策視窗中，選取“**關鍵威脅防護**”→“**防火牆**”。

4. 在"**防火牆設定**"塊中，點擊"**設定**"按鈕。
   這將開啟網路封包規則清單和應用程式網路規則清單。

5. 選擇"**網路封包規則**"標籤。
   這將開啟防火牆設定的預設網路規則清單。

6. 使用 **新增** 下拉清單，選擇規則在清單中的位置：清單顶部、清單底部或所選規則的旁邊。
   規則在清單中的位置決定了規則的優先順序。清單顶部的規則具有最高優先順序。

7. 在"**名稱**"欄位中手動輸入網路服務的名稱。

8. 設定網路規則設定（參見下表）。
   您可以透過點擊按鈕來選擇預定義的規則範本。規則範本描述了最常用的網路連線。
   所有網路規則設定將自動填寫。

9. 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。

10. 儲存新網路規則。

11. 使用"**上移**" / "**下移**"按鈕設定網路規則的優先順序。

12. 儲存變更。

防火牆將根據規則控製網路封包。您可以從防火牆操作中停用封包規則，而無需將其從清單中刪除。為此，請清除物件旁邊的核取方塊。

**如何在網頁主控台和雲端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（裝置）→ 政策和設定檔**。

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. 選擇"**網路封包規則**"標籤。
   這將開啟防火牆設定的預設網路規則清單。

6. 點擊"**新增**"。
   這將開啟新網路規則的表單。

7. 在"**規則名稱**"欄位中手動輸入網路服務的名稱。

8. 設定網路規則設定（參見下表）。
   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。規則範本描述了最常用的網路連線。
   所有網路規則設定將自動填寫。

9. 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。

10. 儲存網路規則。

    新的網路規則將新增到清單中。

11. 使用**移動**按鈕設定網路規則的優先順序。

12. 儲存變更。

防火牆將根據規則控製網路封包。您可以從防火牆操作中停用封包規則，而無需將其從清單中刪除。使用**"狀態"**列中的開關來啟用或停用封包規則。

"網路封包規則"設定

| 參數 | 描述 |
| --- | --- |
| **操作** | **允許**<br>**封鎖**<br>**按應用程式規則**如果選擇此選項，則防火牆將應用程式網路規則套用於網路連線。 |
| **協定** | 透過所選協定控製網路活動：TCP，UDP，ICMP，ICMPv6，IGMP 和 GRE。<br>如果選取的是 ICMP 或 ICMPv6 埠，您可以定義 ICMP 封包類型和代碼：<br>如果選取的是 TCP 或 UDP 協定類型，您可以指定其連線受監控的本機和遠端電腦逗號分隔的連接埠。 |
| **方向** | **接收(封包)**防火牆將網路規則套用於所有接收網路封包。<br>**接收**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。<br>**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。<br>**傳送(封包)**防火牆將網路規則套用於所有傳送網路封包。<br>**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。 |
| **網路介面卡** | 可以傳送和/或接收網路封包的網路介面卡。指定網路介面卡的設定可以區分相同 IP 位址傳送或接收的網路封包。 |
| **生存時間 (TTL)** | 透過網路資料包的生命週期（生存時間，TTL）來限制對網路資料包的控制。 |
| **遠端位址** | 可以傳送和接收網路封包的遠端電腦的網路位址。防火牆將網路規則套用於指定範圍的遠端網路位址。您可以將所有 IP 位址包括在網路規則中，建立單獨的 IP 位址清單，指定 IP 位址範圍，或選擇一個子網（信任網路，本機網路，公用網路）。您也可以指定電腦的 DNS 名稱而不是它的 IP 位址。您應該將 DNS 名稱僅用於 LAN 電腦後者內部服務。與雲端服務（例如 Microsoft Azure）和其他網際網路資源的交互應該由 Web 控制元件進行處理。<br>如果在網路封包規則中新增了無法確定 IP 位址的 DNS 名稱，Kaspersky Endpoint Security 將顯示警告。在 Web 主控台的網路封包規則清單中，新增了包含錯誤描述的欄。在管理主控台 (MMC) 中，錯誤描述不可用。此類封包規則用顏色突出顯示。 |
| **本機位址** | 可以傳送和接收網路封包的電腦的網路位址。防火牆將網路規則套用於指定範圍的區域網路位址。您可以在網路規則中包括所有 IP 位址，建立一個單獨的 IP 位址清單，或指定一個 IP 位址範圍。<br>僅當指定了遠端位址清單時，應用程式才會儲存本機位址。也就是說，**來自清單的位址** 值已為 **遠端位址** 選取並且至少已新增一個位址。<br>有時候無法獲得應用程式的本機位址。在這種情況下，此參數將被忽略。 |

# 啟動或停用網路封包規則

*若要啟用或停用網路封包規則，請執行以下操作：*

1. 在"應用程式主視窗"中，點擊⚙按鈕。

2. 在應用程式設定視窗中，選取"**關鍵威脅防護**"→"**防火牆**"。

3. 點擊**"封包規則"**。
   這將開啟防火牆設定的預設網路封包規則清單。
4. 在清單中選取所需的網路封包規則。
5. 使用**"狀態"**列中的開關來啟用或停用規則。
6. 儲存變更。

## 變更網路封包規則的防火牆操作

*若要變更應用於網路封包規則的防火牆操作，請執行以下操作：*

1. 在"應用程式主視窗"中，點擊⚙按鈕。
2. 在應用程式設定視窗中，選取**"關鍵威脅防護"→"防火牆"**。
3. 點擊**"封包規則"**。
   這將開啟防火牆設定的預設網路封包規則清單。
4. 請在網路封包規則清單中選取並點擊**"編輯"**按鈕。
5. 在**"操作"**下拉清單中選取防火牆在偵測到此類網路活動後的操作：
   - **允許**
   - **封鎖**
   - **按應用程式規則**如果選擇此選項，則防火牆將應用程式網路規則套用於網路連線。
6. 儲存變更。

## 變更網路封包規則的優先順序

網路封包規則的優先順序取決於其在網路包規則清單中的位置。封包規則清單中位於最上方的優先等級最高。

每個手動建立的網路封包規則都將被新增到封包規則清單尾部，擁有最低的優先等級。

防火牆將按照網路封包規則清單中規則的顯示順序自上而下執行規則。根據套用於特定網路連線的每個已處理網路封包規則，防火牆會允許或封鎖對該網路連線設定中指定的位址和通訊埠的網路存取。

*若要變更網路封包規則優先順序，請執行以下操作：*

1. 在"應用程式主視窗"中，點擊⚙按鈕。
2. 在應用程式設定視窗中，選取**"關鍵威脅防護"→"防火牆"**。
3. 點擊**"封包規則"**。
   這將開啟防火牆設定的預設網路封包規則清單。

4. 在清單中選取您希望變更其優先順序的網路封包規則。

5. 使用"**上移**" / "**下移**"按鈕設定網路規則的優先順序。

6. 儲存變更。

## 匯出和匯入網路封包規則

您可以將網路封包規則清單匯出到 XML 檔案。然後，您可以修改檔案，例如，新增大量相同類型的規則。您可以使用匯出/匯入功能來備份網路封包規則清單，或將清單遷移到其他伺服器。

**如何在管理主控台 (MMC) 中匯出和匯入網路封包規則清單**

1. 在卡巴斯基安全管理中心管理主控台樹狀目錄中，選取**政策**。

2. 選擇必要的政策並點擊以開啟政策內容。

3. 在政策視窗中，選取"**關鍵威脅防護**"→"**防火牆**"。

4. 在"**防火牆設定**"塊中，點擊"**設定**"按鈕。

   這將開啟網路封包規則清單和應用程式網路規則清單。

5. 選擇"**網路封包規則**"標籤。

6. 要匯出網路封包規則清單：

   a. 選取您想要匯出的規則。要選擇多個連接埠，請使用**CTRL**或**SHIFT**鍵。

      如果您未選擇任何規則，則 Kaspersky Endpoint Security 將匯出所有規則。

   b. 點擊"**匯出**"連接。

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

   d. 儲存檔案。

      Kaspersky Endpoint Security 會將規則清單匯出到 XML 檔案。

7. 要匯入網路封包規則清單，請：

   a. 點擊"**匯入**"連接。

      在開啟的視窗中，選取要從中匯入規則清單的 XML 檔案。

   b. 開啟檔案。

      如果電腦已經具有規則清單，則 Kaspersky Endpoint Security 將提示您刪除現有清單或從 XML 檔案向其中新增新項目。

8. 儲存變更。

**如何在網頁主控台和雲端主控台中匯出和匯入網路封包規則清單**

1. 在網頁主控台的主視窗中，選擇**資產（裝置）→政策和設定檔**。
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. 要匯出"規則清單，請在**"網路封包規則"**塊中：
   a. 選取您想要匯出的規則。
   b. 點擊 → **匯出** 按鈕。
      Kaspersky Endpoint Security 會將規則清單匯出到預設下載資料夾中的 JSON 檔案。
6. 要匯入規則清單，請在**"網路封包規則"**塊中：
   a. 點擊 → **匯入** 按鈕。
      在開啟的視窗中，選取要從中匯入規則清單的 JSON 檔案。
   b. 開啟檔案。
      如果電腦已經具有規則清單，則 Kaspersky Endpoint Security 將提示您刪除現有清單或從 JSON 檔案向其中新增新項目。
7. 儲存變更。

# 以 XML 格式定義網路封包規則

防火牆允許以 XML 格式匯出網路封包規則。然後，您可以修改檔案，例如，新增大量相同類型的規則。

XML 文件包含兩個主要節點：`Rules`和`Resources`。`Rules`節點列出網路封包規則。此節點包含預設配置的規則（*預定義規則*）以及使用者新增的規則（*自訂規則*）。

"網路封包規則"標記

```
<key name="0000">
        <tDWORD name="RuleId">100</tDWORD>
        <tDWORD name="RuleState">1</tDWORD>
        <tDWORD name="RuleTypeId">4</tDWORD>
        <tQWORD name="AppIdEx">0</tQWORD>
        <tDWORD name="ResIdEx">812</tDWORD>
        <tDWORD name="ResIdEx2">0</tDWORD>
        <tDWORD name="AccessFlag">2</tDWORD>
</key>
```

XML 格式的網路封包規則"設定

| 參數 | 描述 | 值 |
| --- | --- | --- |
| `<key name="0000">` | 規則的優先順序。值越低，優先順序越高。 | 整數<br><br>優先順序值必須由 4 個數字組成。XML 檔案中的節點必須按優先順序值排列，以 `0000` 開始。 |
| `RuleId` | 規則的 ID。 | **預定義規則**<br>`100` – **透過 TCP 存取 DNS 伺服器服務**。<br>`101` – **透過 UDP 存取 DNS 伺服器服務**。<br>`102` – **傳送電子郵件訊息**。<br>`110` – **任何網路活動**（信任網路）。<br>`125` – **任何網路活動**（本機網路）。<br>`130` – **遠端桌面網路活動**。<br>`131` – **透過本機連接埠的 TCP 連線**。<br>`132` – **透過本機連接埠的 UDP 連線**。<br>`133` – **接收的 TCP 串流資料**。<br>`134` – **接收的 UDP 串流資料**。<br>`137` – **ICMP 目的地無法接通接收封包**。<br>`138` – **接收 ICMP Echo 回應封包**。<br>`140` – **ICMP 接收回應逾時**。<br>`142` – **接收的 ICMP 串流資料**。<br>`266` – **接收 ICMPv6 Echo 請求封包**。 |
| `RuleState` | 規則的狀態。 | `0` – 預定義規則已停用<br>`1` – 預定義規則已啟用<br>`2` – 自訂規則已停用<br>`3` – 自訂規則已啟用 |
| `RuleTypeId` | 規則類型的 ID。 | `4` – 網路封包規則。 |
| `AppIdEx` | 網路封包規則所屬的應用程式的 ID。 | 如果規則不屬於任何應用程式，則值為 `0`。 |
| `ResIdEx` | 具有規則設定的資源的主 ID。您可以使用此識別符尋找 `Resources` 節點中具有規則設定的塊。 | 整數 |
| `ResIdEx2` | 網路類型的 ID。 | `0` – **任何位址**。<br>`50` – **信任網路**。<br>`51` – **本機網路**。<br>`52` – **公用網路**。<br>`<Network Identifier>` – **來自清單的位址**（位址手動定義）。 |
| `AccessFlag` | **動作** 參數的值。 | `0` – **允許**。<br>`2` – **按應用程式規則**。<br>`3` – **封鎖**。<br>`4` – **允許** 和 **記錄事件**。<br>`6` – **按應用程式規則** 和 **記錄事件**。<br>`7` – **封鎖** 和 **記錄事件**。 |
| `</key>` | | |

`Resources` 節點包含網路封包規則設定。自訂網路封包規則設定列出在 `<key name="0004">` 塊中。

"自訂網路封包規則"標記

```
<key name="0026">
        <key name="Data">
                <key name="RemotePorts"> </key>
                <key name="LocalPorts"> </key>
                <key name="AdapterBindings">
```

```
                        <key name="0000">
                                <key name="IpAddresses">
                                        <key name="0000">
                                                <key name="IP">
                                                        <key name="V6">
                                                                <tQWORD name="Hi">0</tQWORD>
                                                                <tQWORD name="Lo">0</tQWORD>
                                                                <tDWORD name="Zone">0</tDWORD>
                                                                <tSTRING name="ZoneStr"/>
                                                        </key>
                                                        <tBYTE name="Version">4</tBYTE>
                                                        <tDWORD name="V4">16909060</tDWORD>
                                                        <tBYTE name="Mask">32</tBYTE>
                                                </key>
                                                <key name="AddressIP"> </key>
                                                <tSTRING name="Address"/>
                                        </key>
                                </key>
                                <key name="MacAddresses">
                                        <key name="0000">
                                                <tDWORD name="Type">0</tDWORD>
                                                <tQWORD name="AddressData0">1108152157446</tQWORD>
                                                <tQWORD name="AddressData1">0</tQWORD>
                                        </key>
                                </key>
                                <tSTRING name="AdapterName">ADAPTER TEST 123</tSTRING>
                                <tDWORD name="InterfaceType">3</tDWORD>
                        </key>
                </key>
                <tTYPE_ID name="unique">3213697024</tTYPE_ID>
                <tBYTE name="Proto">2</tBYTE>
                <tBYTE name="Direction">2</tBYTE>
                <tBYTE name="IcmpType">0</tBYTE>
                <tBYTE name="IcmpCode">0</tBYTE>
                <tDWORD name="Flags">1</tDWORD>
                <tBYTE name="TTL">255</tBYTE>
        </key>
        <key name="Childs"> </key>
        <tDWORD name="Id">1073747214</tDWORD>
        <tDWORD name="ParentID">7</tDWORD>
        <tDWORD name="Flags">38</tDWORD>
        <tSTRING name="Name">TEST1</tSTRING>
</key>
```

"自訂網路封包規則"設定

| 參數 | 描述 | 值 |
| --- | --- | --- |
| `<key name="Data">` | 參數塊的 ID。 | 整數 |
| RemotePorts | **遠端連接埠** 參數的值。 | 遠端連接埠範圍清單。 |
| LocalPorts | **本機連接埠** 參數的值。 | 本機連接埠範圍清單。 |
| AdapterBindings | **網路介面卡** 參數的值。 | IpAddresses – **IP 位址** 參數的值。<br>MacAddresses – **MAC 位址** 參數的值。<br>AdapterName – 網路介面卡名稱。<br>InterfaceType – **介面類型** 參數的值：<br>• 0 – **其他**。<br>• 1 – **LoopBack**。<br>• 2 – **有線網路(乙太網路)**。<br>• 3 – **無線網路(Wi-Fi)**。<br>• 4 – **通道**。<br>• 5 – **PPP 連線**。<br>• 6 – **PPPoE 連線**。<br>• 7 – **VPN 連線**。<br>• 8 – **Modem 連線**。 |
| unique | 結構的內部 ID。 | 整數<br>建議不變更此參數。 |

| 參數 | 描述 | 值 |
| --- | --- | --- |
| Proto | **協定** 參數的值。 | `0` – 已停用。<br>`1` – **ICMP**。<br>`2` – **IGMP**。<br>`6` – **TCP**。<br>`17` – **UDP**。<br>`47` – **GRE**。<br>`58` – **ICMPv6**。 |
| Direction | **方向** 參數的值。 | `1` – **接收(封包)**。<br>`2` – **傳送(封包)**。<br>`3` – **接收/傳送**。<br>`4` – **接收**。<br>`5` – **傳送**。 |

| 參數 | 描述 | 值 |
| --- | --- | --- |
| IcmpType | **ICMP 類型** 參數的值。 | **ICMP 協定**<br>0 – **Echo 回應** (ICMP) 或已停用。<br>3 – **無回應** (ICMP)。<br>4 – **來源抑制**。<br>5 – **重新導向**。<br>6 – **備用主機位址**。<br>8 – **Echo 請求**。<br>9 – **路由器公告**。<br>10 – **路由器請求**。<br>11 – **逾時**。<br>12 – **參數問題**。<br>13 – **時間戳記**。<br>14 – **時間戳記回應**。<br>15 – **資訊請求**。<br>16 – **資訊回應**。<br>17 – **位址遮罩請求**。<br>18 – **位址遮罩回應**。<br>30 – **追蹤路由**。<br>31 – **資料報轉換錯誤**。<br>32 – **行動主機重新導向**。<br>33 – **IPv6 位置請求**。<br>34 – **IPv6 位置應答**。<br>35 – **行動註冊請求**。<br>36 – **行動註冊回應**。<br>37 – **網域名稱請求**。<br>38 – **網域名稱回應**。<br>40 – **Photuris**。<br>**ICMPv6 協定**<br>1 – **無回應**。<br>2 – **封包太大**。<br>3 – **逾時**。<br>4 – **參數問題**。<br>128 – **Echo 請求**。<br>129 – **Echo 回應**。<br>130 – **多點廣播監聽查詢**。<br>131 – **多點廣播監聽報告**。<br>132 – **多點廣播監聽完成**。<br>133 – **路由器請求**。<br>134 – **路由器公告**。<br>135 – **網路芳鄰請求**。<br>136 – **網路芳鄰公告**。<br>137 – **重新導向訊息**。<br>138 – **路由器重新編號**。<br>139 – **ICMP 節點資訊查詢**。<br>141 – **反向的網芳邀請封包**。<br>142 – **反向的網芳公告封包**。<br>143 – **多點廣播監聽報告第二版**。 |

| 參數 | 描述 | 值 |
| --- | --- | --- |
| | | 144 – **歸屬代理位址發現請求訊息**。<br>145 – **歸屬代理位址發現應答訊息**。<br>146 – **行動式前置請求**。<br>147 – **行動式前置公告**。<br>148 – **憑證路徑邀請訊息**。<br>149 – **憑證路徑公告訊息**。<br>151 – **多路廣播路由公告**。<br>152 – **多路廣播路由邀請**。<br>153 – **多路廣播路由終端**。 |
| `IcmpCode` | **ICMP 代碼** 參數的值。 | `0` – **代碼 0** 或已停用。<br>`1` – **代碼 1**。<br>`2` – **代碼 2**。 |
| `Flags` | 結構屬性指標。 | 整數<br>建議不變更此參數。 |
| `TTL` | **生存時間（TTL)** 參數的值。 | 值（秒鐘）。若已停用，則值為 `0`。 |
| `</key>` | | |
| `Id` | 資源的主 ID（參見 `Rules` 節點）。 | 整數 |
| `ParentID` | 父群組的 ID。 | 整數<br>建議不變更此參數。 |
| `Flags` | 規則的狀態。 | `6` – 規則已停用。<br>`38` – 規則已啟用。 |
| `Name` | 網路封包規則的名稱。 | 字串 |

# 管理應用程式網路規則

預設情況下，Kaspersky Endpoint Security 將按照其所監控的檔案或網路活動所對應的軟體的供應商名稱對安裝在電腦上的所有應用程式進行群組分配。應用程式群組將依次被歸類到"信任群組"中。所有應用程式和應用程式群組都將繼承來自其父群組的內容：應用程式控制規則、應用程式網路規則及其執行優先順序。

像"主機入侵防禦"元件一樣，預設情況下，"防火牆"元件在篩選應用程式群組內所有應用程式的網路活動時將套用應用程式群組的網路規則。應用程式群組網路規則將定義群組中應用程式存取不同網路連線的權限。

預設情況下，防火牆將為電腦上的 Kaspersky Endpoint Security 偵測到的每個應用程式群組建立網路規則集。您可以變更套用於預設建立的應用程式群組網路規則的防火牆操作。您不能編輯、刪除、停用或變更預設情況下建立的應用程式群組網路規則的優先等級。

您也可以為單個應用程式建立網路規則。此類規則將擁有比該應用程式所屬網路規則群組高的優先順序。

# 建立應用程式網路規則

預設情況下，應用程式活動由針對 Kaspersky Endpoint Security 在此應用程式第一次啟動時將其分配到的信任群組定義的網路規則來控制。如有必要，您可以為整個信任群組、單個應用程式或信任群組內的一組應用程式建立網路規則。

手動定義的網路規則比為信任群組確定的網路規則具有更高的優先順序。換句話說，如果手動定義的應用程式規則與為信任群組確定的應用程式規則不同，則防火牆將根據手動定義的應用程式規則控制應用程式活動。

預設情況下，防火牆為每個應用程式建立以下網路規則：

- 信任網路中的任何網路活動。
- 本機網路中的任何網路活動。
- 公用網路中的任何網路活動。

Kaspersky Endpoint Security 根據預定義的網路規則控制應用程式的網路活動，如下所示：

- 受信任和低限制：允許所有網路活動。
- 高限制和不受信任：所有網路活動被封鎖。

預定義的應用程式規則無法編輯或刪除。

您可以透過以下方式建立應用程式網路規則：

- 使用網路監控工具。

  *網路監控*是一個用於即時檢視網路活動資訊的工具。這很方便，因為您不需要配置所有規則設定。某些防火牆設定將從網路監控資料中自動插入。網路監控僅在應用程式介面中可用。

- 配置防火墻設定。

  這使您可以微調防火牆設定。您可以為任何網路活動建立規則，即使當前沒有網路活動也是如此。

為應用程式建立網路規則時，請記住，網路封包規則的優先順序高於應用程式網路規則。

**如何使用網路監控工具在應用程式介面中建立應用程式網路規則**

1. 在應用程式主視窗的**"正在監控"**區域中，點擊**"網路監控"**圖標。
2. 選擇**"網路活動"**或**"開放連接埠"**標籤。

   **"網路活動"**標籤顯示電腦目前所有活動的網路連線。接收和傳送的網路連線都將同時顯示。

   **"開放連接埠"**標籤列出電腦所有開啟的網路連接埠。
3. 在網路連線的內容功能表中，選擇**"建立應用程式網路規則"**。

   "應用程式規則和屬性"視窗將開啟。
4. 選擇**"網路規則"**標籤。

   這將開啟防火牆設定的預設網路規則清單。

5. 點擊**"新增"**。
   這將開啟網路規則屬性。
6. 在**"名稱"**欄位中手動輸入網路服務的名稱。
7. 設定網路規則設定（參見下表）。
   您可以透過點擊**"網路規則範本"**連線來選擇預定義的規則範本。規則範本描述了最常用的網路連線。
   所有網路規則設定將自動填寫。
8. 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。
9. 點擊**"儲存"**。
   新的網路規則將新增到清單中。
10. 使用**"上移"** / **"下移"**按鈕設定網路規則的優先順序。
11. 儲存變更。

**如何使用防火牆設定在應用程式介面中建立應用程式網路規則**

1. 在"應用程式主視窗"中，點擊⚙按鈕。
2. 在應用程式設定視窗中，選取**"關鍵威脅防護"→"防火牆"**。
3. 點擊**"應用程式規則"**。
   這將開啟防火牆設定的預設網路規則清單。
4. 在應用程式清單中，選取您想為其建立網路規則的應用程式或應用程式群組。
5. 右鍵點擊以開啟內容功能表並選取**"細節和規則"**。
   "應用程式規則和屬性"視窗將開啟。
6. 選擇**"網路規則"**標籤。
7. 點擊**"新增"**。
   這將開啟網路規則屬性。
8. 在**"名稱"**欄位中手動輸入網路服務的名稱。
9. 設定網路規則設定（參見下表）。
   您可以透過點擊**"網路規則範本"**連線來選擇預定義的規則範本。規則範本描述了最常用的網路連線。
   所有網路規則設定將自動填寫。
10. 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。
11. 點擊**"儲存"**。
    新的網路規則將新增到清單中。
12. 使用**"上移"** / **"下移"**按鈕設定網路規則的優先順序。
13. 儲存變更。

### 如何在管理主控台 (MMC) 中建立應用程式網路規則

1. 在卡巴斯基安全管理中心管理主控台樹狀目錄中，選取**政策**。
2. 選擇必要的政策並點擊以開啟政策內容。
3. 在政策視窗中，選取**"關鍵威脅防護"→"防火牆"**。
4. 在**"防火牆設定"**塊中，點擊**"設定"**按鈕。
   這將開啟網路封包規則清單和應用程式網路規則清單。
5. 選擇**"應用程式網路規則"**標籤。
6. 點擊**"新增"**。
7. 在開啟的視窗中，輸入條件搜尋您想為其建立網路規則的應用程式。
   您可以輸入應用程式名稱或供應商名稱。Kaspersky Endpoint Security 輸入遮罩時支援環境變量以及 * 和 ? 字元。
8. 點擊**"重新整理"**。
   Kaspersky Endpoint Security 將在受管電腦上安裝的應用程式的合併清單中搜尋該應用程式。Kaspersky Endpoint Security 將顯示滿足您搜尋條件的應用程式清單。
9. 選取需要的應用程式。
10. 在**"將選擇應用程式新增至信任群組"**下拉清單中，選擇**"預設群組"**，然後點擊**"確定"**。
    該應用程式將被新增到預設群組。
11. 選擇相關的應用程式，然後從應用程式的內容功能表中選擇**"應用程式權限"**。
    "應用程式規則和屬性"視窗將開啟。
12. 選擇**"網路規則"**標籤。
    這將開啟防火牆設定的預設網路規則清單。
13. 點擊**"新增"**。
    這將開啟網路規則屬性。
14. 在**"名稱"**欄位中手動輸入網路服務的名稱。
15. 設定網路規則設定（參見下表）。
    您可以透過點擊按鈕來選擇預定義的規則範本。規則範本描述了最常用的網路連線。
    所有網路規則設定將自動填寫。
16. 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。
17. 儲存新網路規則。
18. 使用**"上移"** / **"下移"**按鈕設定網路規則的優先順序。
19. 儲存變更。

### 如何在網頁主控台和雲端主控台中建立應用程式網路規則

1. 在網頁主控台的主視窗中，選擇**資產（裝置）→政策和設定檔**。
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. 在**"應用程式權限和受防護資源"**塊中，點擊**"應用程式權限"**連接。
   這將開啟應用程式權限配置視窗和受防護資源的清單。
6. 選擇**"應用程式權限"**標籤。
   您將在視窗左側看到信任群組清單，並在右側看到它們的屬性。
7. 在**"應用程式"**塊中，點擊**"新增"**按鈕。
   這將啟動用於將應用程式新增到信任群組的精靈。
8. 選擇相關應用程式信任群組。
9. 選擇**應用程式**類型。前往下一步。
   如果要為多個應用程式建立網路規則，請選擇**"群組"**類型並為應用程式組定義一個名稱。
10. 在開啟的應用程式清單中，選取您想為其建立網路規則的應用程式。
    使用篩選器。您可以輸入應用程式名稱或供應商名稱。Kaspersky Endpoint Security 輸入遮罩時支援環境變量以及 * 和 ? 字元。
11. 結束精靈。
    該應用程式將被新增到信任群組。
12. 在視窗左側，選取相關應用程式。
13. 在視窗的右側，從下拉清單中選擇**網路規則**。
    這將開啟防火牆設定的預設網路規則清單。
14. 點擊**"新增"**。
    這將開啟應用程式規則屬性。
15. 在**"規則名稱"**欄位中手動輸入網路服務的名稱。
16. 設定網路規則設定（參見下表）。
    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。規則範本描述了最常用的網路連線。
    所有網路規則設定將自動填寫。
17. 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。
18. 儲存網路規則。
    新的網路規則將新增到清單中。

19. 使用**移動**按鈕設定網路規則的優先順序。

20. 儲存變更。

"應用程式網路規則"設定

| 參數 | 描述 |
| --- | --- |
| **操作** | **允許**<br>**封鎖** |
| **協定** | 透過所選協定控製網路活動：TCP，UDP，ICMP，ICMPv6，IGMP 和 GRE。<br>如果選取的是 ICMP 或 ICMPv6 埠，您可以定義 ICMP 封包類型和代碼：<br>如果選取的是 TCP 或 UDP 協定類型，您可以指定其連線受監控的本機和遠端電腦逗號分隔的連接埠。 |
| **方向** | **接收**<br>**接收/傳送**<br>**傳送** |
| **遠端位址** | 可以傳送和接收網路封包的遠端電腦的網路位址。防火牆將網路規則套用於指定範圍的遠端網路位址。您可以將所有 IP 位址包括在網路規則中，建立單獨的 IP 位址清單，指定 IP 位址範圍，或選擇一個子網（信任網路，本機網路，公用網路）。您也可以指定電腦的 DNS 名稱而不是它的 IP 位址。您應該將 DNS 名稱僅用於 LAN 電腦後者內部服務。與雲端服務（例如 Microsoft Azure）和其他網際網路資源的交互應該由 Web 控制元件進行處理。<br><br>如果在網路封包規則中新增了無法確定 IP 位址的 DNS 名稱，Kaspersky Endpoint Security 將顯示警告。在 Web 主控台的網路封包規則清單中，新增了包含錯誤描述的欄。在管理主控台 (MMC) 中，錯誤描述不可用。此類封包規則用顏色突出顯示。 |
| **本機位址** | 可以傳送和接收網路封包的電腦的網路位址。防火牆將網路規則套用於指定範圍的區域網路位址。您可以在網路規則中包括所有 IP 位址，建立一個單獨的 IP 位址清單，或指定一個 IP 位址範圍。<br><br>僅當指定了遠端位址清單時，應用程式才會儲存本機位址。也就是說，**來自清單的位址** 值已為 **遠端位址** 選取並且至少已新增一個位址。<br><br>有時候無法獲得應用程式的本機位址。在這種情況下，此參數將被忽略。 |

# 啟用和停用應用程式網路規則

*若要啟用或停用應用程式網路規則，請執行以下操作：*

1. 在"應用程式主視窗"中，點擊⚙ 按鈕。

2. 在應用程式設定視窗中，選取"**關鍵威脅防護**"→"**防火牆**"。

3. 點擊"**應用程式規則**"。

   這將開啟應用程式規則清單。

4. 在應用程式清單中，選取您想為其建立或編輯網路規則的應用程式或應用程式群組。

5. 右鍵點擊以開啟內容功能表並選取"**細節和規則**"。

   "應用程式規則和屬性"視窗將開啟。

6. 選擇"**網路規則**"標籤。

7. 在應用程式群組的網路規則清單中，選取相關的網路規則。

   "網路規則"視窗將開啟。

8. 設定網路規則的“**啟動**“或“**未啟動**”狀態。

   您不能停用預設情況下由防火牆建立的應用程式群組網路規則。

9. 儲存變更。

## 變更應用程式網路規則的防火牆操作

您可以變更應用於應用程式或應用程式群組的網路規則的預設建立的防火牆操作，也可以為應用程式或應用程式群組變更單個自訂網路規則的防火牆操作。

*若要為應用程式或應用程式群組變更所有網路規則的防火牆操作：*

1. 在“應用程式主視窗”中，點擊⚙按鈕。
2. 在應用程式設定視窗中，選取”**關鍵威脅防護**“→“**防火牆**”。
3. 點擊“**應用程式規則**”。

   這將開啟應用程式規則清單。

4. 如果您希望變更預設建立的應用至所有網路規則的防火牆操作，則選取清單中應用程式或應用程式群組。手動建立的網路規則將保持不變。
5. 右鍵點擊以開啟內容功能表，選擇“**網路規則**“，然後選擇要分配的操作：

   - **繼承**
   - **允許**
   - **封鎖**

6. 儲存變更。

*若要變更一個應用程式或應用程式群組網路規則的防火牆操作，請執行以下操作：*

1. 在“應用程式主視窗”中，點擊⚙按鈕。
2. 在應用程式設定視窗中，選取”**關鍵威脅防護**“→“**防火牆**”。
3. 點擊“**應用程式規則**”。

   這將開啟應用程式規則清單。

4. 在清單中選取您想為其變更一個網路規則操作的應用程式或應用程式群組。
5. 右鍵點擊以開啟內容功能表並選取“**細節和規則**”。

   “應用程式規則和屬性”視窗將開啟。

6. 選擇“**網路規則**”標籤。
7. 選取您要為其變更防火牆操作的網路規則。

8. 在“**動作**”列中，點擊右鍵顯示內容功能表，然後選擇您要分配的操作：
   - **繼承**
   - **允許**
   - **拒絕**
   - **記錄事件**
9. 儲存變更。

## 變更應用程式網路規則的優先順序

網路規則的優先順序取決於其在網路規則清單中的位置。防火牆執行按照網路規則清單中規則的顯示順序自上而下執行規則。根據套用於特定網路連線的每個已處理網路規則，防火牆會允許或封鎖對該網路連線設定中指定的位址和連接埠的網路存取。

手動建立的網路規則擁有比預設網路規則高的優先順序。

您不能變更預設應用程式群組網路規則的優先順序。

*要變更網路規則的優先順序，請執行以下操作：*

1. 在“應用程式主視窗”中，點擊⚙按鈕。
2. 在應用程式設定視窗中，選取”**關鍵威脅防護**“→“**防火牆**”。
3. 點擊“**應用程式規則**”。
   這將開啟應用程式規則清單。
4. 在應用程式群組網路規則清單中，選取您要變更網路規則優先順序的應用程式或應用程式群組。
5. 右鍵點擊以開啟內容功能表並選取“**細節和規則**”。
   “應用程式規則和屬性”視窗將開啟。
6. 選擇“**網路規則**”標籤。
7. 選取您想要變更其優先順序的網路規則。
8. 使用“**上移**” / “**下移**”按鈕設定網路規則的優先順序。
9. 儲存變更。

# 網路監控

*網路監控*是一個用於即時檢視網路活動資訊的工具。

*若要啟動網路監控，請執行以下操作：*

在應用程式主視窗的“**正在監控**”區域中，點擊“**網路監控**”圖標。

開啟“網路監控”視窗。在該視窗中，將以四個標籤顯示電腦網路活動的相關資訊：

- “**網路活動**”標籤顯示電腦目前所有活動的網路連線。接收和傳送的網路連線都將同時顯示。在此標籤上，您還可以為防火牆操作建立網路封包規則。
- “**開放連接埠**”標籤列出電腦所有開啟的網路連接埠。在此標籤上，您還可以為防火牆操作建立網路封包規則和應用程式規則。
- “**網路流量**”標籤顯示使用者電腦目前連線其他電腦之間傳送和接收的網路流量。
- “**已封鎖的電腦**”標籤列出“網路威脅防護”元件在偵測到網路攻擊後封鎖該網路活動的遠端電腦 IP 位址。

# 弱點利用防禦

“弱點利用防禦”元件可偵測利用電腦弱點來利用管理員權限或執行惡意活動的程式程式碼。例如，弱點利用程式可以利用緩衝區溢位攻擊。為此，弱點利用程式會向易受攻擊的應用程式傳送大量資料。處理此資料時，易受攻擊的應用程式會執行惡意程式碼。此攻擊的結果是，弱點利用程式可啟動未經授權的惡意軟體安裝。當存在從易於感染的應用程式執行可執行檔的嘗試，並且該嘗試並非由使用者執行時，Kaspersky Endpoint Security 將封鎖該檔案執行或通知使用者。

漏洞利用防護元件也會監控網路連接埠，以查找可能威脅電腦安全的應用程式處理程序。應用程式透過病毒資料庫獲取有關此類處理程序的資訊。

# 啟用和停用弱點利用防禦

預設情況下，弱點利用防禦為啟動狀態，各種功能均設定為最佳化。Kaspersky Endpoint Security 可監控易受攻擊的應用程式執行的可執行檔。如果 Kaspersky Endpoint Security 偵測到某個易於感染的應用程式的可執行檔被除使用者以外的事物執行，Kaspersky Endpoint Security 將執行選擇的操作（例如，封鎖運行）。

**如何在管理主控台（MMC）中啟用或停用弱點利用防禦**

1. 在卡巴斯基安全管理中心管理主控台樹狀目錄中，選取**政策**。
2. 選擇必要的政策並點擊以開啟政策內容。
3. 在政策視窗中，選擇“**進階威脅防護 → 弱點利用防禦**”。
4. 使用“**弱點利用防禦**”核取方塊來啟用或停用元件。

5. 在“**偵測到弱點時**”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，Kaspersky Endpoint Security 將在偵測到弱點時記錄包含弱點相關資訊的項目，並將此弱點的相關資訊新增至活動威脅清單。




活動威脅通知

6. 儲存變更。若要在電腦上套用該政策，請關閉掛鎖。

**如何在網頁主控台和雲端主控台中啟用或停用弱點利用防禦**

1. 在網頁主控台的主視窗中，選擇**資產（裝置）** → **政策和設定檔**。
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“**弱點利用防禦已啟用**“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。
- **通知或提示操作**如果選擇此項目，Kaspersky Endpoint Security 將在偵測到弱點時記錄包含弱點相關資訊的項目，並將此弱點的相關資訊新增至活動威脅清單。




活動威脅通知

7. 儲存變更。

**如何在應用程式介面中啟用或停用弱點利用防禦**

1. 在"應用程式主視窗"中，點擊⚙按鈕。
2. 在應用程式設定視窗中，選取"**進階威脅防護**"→"**弱點利用防禦**"。




弱點利用防禦設定

3. 使用"**弱點利用防禦**"切換開關可啟用或停用元件。
4. 在"**偵測到弱點時**"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，Kaspersky Endpoint Security 將在偵測到弱點時記錄包含弱點相關資訊的項目，並將此弱點的相關資訊新增至活動威脅清單。
5. 儲存變更。

# 系統處理程序記憶體防護

預設情況下，啟用系統處理程序記憶體防護。Kaspersky Endpoint Security 會封鎖嘗試存取系統處理程序的外部處理程序。

**如何在管理主控台（MMC）中啟用或停用系統處理程序記憶體防護**

1. 在卡巴斯基安全管理中心管理主控台樹狀目錄中，選取**政策**。
2. 選擇必要的政策並點擊以開啟政策內容。
3. 在政策視窗中，選擇**"進階威脅防護 → 弱點利用防禦"**。
4. 使用**"啟用系統處理程序記憶體防護"**核取方塊來啟用或停用選項。
5. 儲存變更。

**如何在網頁主控台和雲端主控台中啟用或停用系統處理程序記憶體防護**

1. 在網頁主控台的主視窗中，選擇**資產（裝置）→ 政策和設定檔**。
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**"系統處理程序記憶體防護已啟用"**開關來啟用或停用此功能。
6. 儲存變更。

**如何在應用程式介面中啟用或停用系統處理程序記憶體防護**

1. 在"應用程式主視窗"中，點擊⚙按鈕。
2. 在應用程式設定視窗中，選取"**進階威脅防護**"→"**弱點利用防禦**"。




弱點利用防禦設定

3. 使用"**啟用系統處理程序記憶體防護**"開關來啟用或停用此功能。
4. 儲存變更。

# 行為偵測

"行為偵測"元件接收您電腦上的應用程式操作的資料，並將此資訊提供給其他防護元件以提高效能。"行為偵測"元件將行為流簽章 (BSS) 用於應用程式。如果應用程式操作比對危險活動行為流簽章，Kaspersky Endpoint Security 將執行選定的回應操作。Kaspersky Endpoint Security 基於行為特徵碼，可為電腦提供主動防禦。

行為偵測元件也會監控網路連接埠，以查找可能威脅電腦安全的應用程式處理程序。應用程式透過病毒資料庫獲取有關此類處理程序的資訊。

預設情況下，行為偵測已啟用並在 Kaspersky 專家建議的模式下執行。當偵測到惡意活動時，Kaspersky Endpoint Security 會刪除惡意應用程式的可執行檔。

除非絕對必要，否則不建議停用行為偵測，因為這樣做會降低防護元件的有效性。防護元件可請求"行為偵測"元件收集的資料以偵測威脅。

**如何在管理主控台（MMC）中啟用或停用行為偵測**

1. 開啟卡巴斯基安全管理中心管理主控台。
2. 在主控台樹狀目錄中，選擇**"政策"**。
3. 選擇必要的政策並點擊以開啟政策內容。
4. 在政策視窗中，選擇**"進階威脅防護 → 行為偵測"**。
5. 使用**"行為偵測"**核取方塊來啟用或停用元件。
6. 在**"偵測到惡意軟體活動時的動作"**塊中選擇相關操作：
   - **刪除**如果選擇此項目，在偵測到惡意活動時，Kaspersky Endpoint Security 會刪除惡意應用程式的可執行檔，同時在備份區建立該檔案的備份副本。
   - **封鎖**如果選擇此項目，在偵測到惡意活動時，Kaspersky Endpoint Security 會終止該應用程式。
   - **通知**如果選擇此項目並且偵測到應用程式的惡意軟體活動，Kaspersky Endpoint Security 將應用程式惡意軟體活動的相關資訊新增至活動威脅清單。
7. 儲存變更。若要在電腦上套用該政策，請關閉掛鎖。

**如何在網頁主控台和雲端主控台中啟用或停用行為偵測**

1. 在網頁主控台的主視窗中，選擇**資產（裝置）→ 政策和設定檔**。
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**"行為分析"→"行為偵測"**。
5. 使用**"行為偵測已啟用"**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：
   - **刪除**如果選擇此項目，在偵測到惡意活動時，Kaspersky Endpoint Security 會刪除惡意應用程式的可執行檔，同時在備份區建立該檔案的備份副本。
   - **封鎖**如果選擇此項目，在偵測到惡意活動時，Kaspersky Endpoint Security 會終止該應用程式。
   - **通知**如果選擇此項目並且偵測到應用程式的惡意軟體活動，Kaspersky Endpoint Security 將應用程式惡意軟體活動的相關資訊新增至活動威脅清單。
7. 儲存變更。若要在電腦上套用該政策，請關閉掛鎖。

### 如何在應用程式介面中啟用或停用行為偵測

1. 在“應用程式主視窗”中，點擊⚙按鈕。
2. 在應用程式設定視窗中，選取”**進階威脅防護**“→“**行為偵測**”。




行為偵測設定

3. 使用“**行為偵測**“切換開關可啟用或停用元件。
4. 在“**偵測到惡意軟體活動時的動作**”塊中選擇相關操作：
   - **刪除**如果選擇此項目，在偵測到惡意活動時，Kaspersky Endpoint Security 會刪除惡意應用程式的可執行檔，同時在備份區建立該檔案的備份副本。
   - **封鎖**如果選擇此項目，在偵測到惡意活動時，Kaspersky Endpoint Security 會終止該應用程式。
   - **通知**如果選擇此項目並且偵測到應用程式的惡意軟體活動，Kaspersky Endpoint Security 將應用程式惡意軟體活動的相關資訊新增至活動威脅清單。
5. 儲存變更。

因此，如果啟用了“行為偵測”，Kaspersky Endpoint Security 將使用行為流簽章來分析作業系統中應用程式的活動。

# Anti-Cryptor

從 Kaspersky Endpoint Security 12.12 for Windows 開始，先前作為行為偵測元件一部分的共用資料夾外部加密防護功能成為一個獨立元件，Anti-Cryptor。

此元件只能監控針對儲存在檔案系統為 NTFS 的大型儲存裝置上並且未使用 EFS 加密的檔案所進行的操作。

Anti-Cryptor 元件可分析共用資料夾中的活動。如果該活動與外部加密的典型行為流簽章比對，Kaspersky Endpoint Security 將執行選定操作。

要讓 Anti-Cryptor 元件正常運作，您必須 啟用行為偵測元件。

如果卡巴斯基安全管理中心偵測到修改共用資料夾中的檔案的嘗試，則會採取以下操作：

- 封鎖存取啟動惡意活動的工作階段的檔案修改（檔案將為只讀）。
- 建立被修改的檔案的備份副本。
- 新增一個項目到 本機應用程式介面報告 並將有關檢測到的惡意活動的資訊傳送至卡巴斯基安全管理中心。
- 此外，如果啟用了"修復引擎"元件，被修改的檔案將從備份副本還原。

# 啟用和停用共用資料夾對外部加密的防護

預設情況下，共用資料夾對外部加密的防護已啟用，並按照卡巴斯基專家的建議運行。若要設定此功能，您可以建立防護範圍並配置排除項目（如有必要）。預設情況下，應用程式會自動識別共用資料夾並監視所有資料夾中的檔案活動。當偵測到對共用資料夾中的檔案進行外部加密的嘗試時，Kaspersky Endpoint Security 會封鎖遠端使用者的工作階段一小時（預設）。

安裝 Kaspersky Endpoint Security 後，共用資料夾對外部加密的防護將受到限制，直到電腦重新啟動為止。

**如何在管理主控台 (MMC) 中啟用或停用共用資料夾對外部加密的防護**

1. 在卡巴斯基安全管理中心管理主控台樹狀目錄中，選取**政策**。
2. 選擇必要的政策並點擊以開啟政策內容。
3. 在政策視窗中，選擇"**進階威脅防護 → 加密軟體防護**"。
4. 使用"**加密軟體防護**"核取方塊可啟用或停用對外部加密典型活動的偵測。

5. 選擇當偵測到嘗試修改共用資料夾中的檔案時應用程式將採取的相關操作：

   - **封鎖連線時間 N 分鐘**。如果選擇了該選項，則當 Kaspersky Endpoint Security 偵測到嘗試修改共用資料夾中的檔案時，它會封鎖啟動了惡意活動的工作階段的檔案修改存取權限，並建立修改檔案的備份副本。

     如果啟用了"修復引擎"元件，並且選擇"**封鎖連線時間 N 分鐘**"選項，被修改的檔案會被從備份副本還原。

   - **通知**如果選擇此選項，則在偵測到修改共用資料夾中的檔案的嘗試時，Kaspersky Endpoint Security 會將有關此嘗試的資訊新增至活動威脅清單中，並將項目新增至 本機應用程式介面報告 並將有關偵測到的惡意活動的資訊傳送至卡巴斯基安全管理中心。

6. 如果有需要的話， 編輯防護範圍並定義排除項目。

7. 儲存變更。若要在電腦上套用該政策，請關閉掛鎖。

**如何在網頁主控台和雲端主控台中啟用或停用共用資料夾對外部加密的防護**

1. 在網頁主控台的主視窗中，選擇**資產（裝置）→ 政策和設定檔**。

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. 使用"**加密軟體防護已啟用**"開關可啟用或停用對外部加密典型活動的偵測。

6. 選擇當偵測到嘗試修改共用資料夾中的檔案時應用程式將採取的相關操作：

   - **封鎖連線（分鐘）N 分鐘**。如果選擇了該選項，則當 Kaspersky Endpoint Security 偵測到嘗試修改共用資料夾中的檔案時，它會封鎖啟動了惡意活動的工作階段的檔案修改存取權限，並建立修改檔案的備份副本。

     如果啟用了"修復引擎"元件，並且選擇"**封鎖連線（分鐘）N 分鐘**"選項，被修改的檔案會被從備份副本還原。

   - **通知**如果選擇此選項，則在偵測到修改共用資料夾中的檔案的嘗試時，Kaspersky Endpoint Security 會將有關此嘗試的資訊新增至活動威脅清單中，並將項目新增至 本機應用程式介面報告 並將有關偵測到的惡意活動的資訊傳送至卡巴斯基安全管理中心。

7. 如果有需要的話， 編輯防護範圍並定義排除項目。

8. 儲存變更。若要在電腦上套用該政策，請關閉掛鎖。

**如何在應用程式介面中啟用或停用共用資料夾對外部加密的防護**

1. 在"應用程式主視窗"中，點擊 按鈕。

2. 在應用程式設定視窗中，選取"**進階威脅防護**"→"**加密軟體防護**"。

3. 使用"**共用資料夾對外部加密的防護**"核取方塊可啟用或停用對外部加密典型活動的偵測。

4. 使用"**共用資料夾對外部加密的防護**"核取方塊可啟用或停用對外部加密典型活動的偵測。

5. 選擇當偵測到嘗試修改共用資料夾中的檔案時應用程式將採取的相關操作：

   - **封鎖連線（分鐘）N 分鐘**。如果選擇了該選項，則當 Kaspersky Endpoint Security 偵測到嘗試修改共用資料夾中的檔案時，它會封鎖啟動了惡意活動的工作階段的檔案修改存取權限，並建立修改檔案的備份副本。

     如果啟用了"修復引擎"元件，並且選擇"**封鎖連線（分鐘）N 分鐘**"選項，被修改的檔案會被從備份副本還原。

   - **通知**如果選擇此選項，則在偵測到修改共用資料夾中的檔案的嘗試時，Kaspersky Endpoint Security 會將有關此嘗試的資訊新增至活動威脅清單中，並將項目新增至 本機應用程式介面報告 並將有關偵測到的惡意活動的資訊傳送至卡巴斯基安全管理中心。

6. 如果有需要的話， 編輯防護範圍並定義排除項目。

7. 儲存變更。

# 配置不受信任電腦的封鎖時間

*不受信任的電腦*是參與惡意活動或資料加密的遠端電腦。預設情況下，Kaspersky Endpoint Security 會封鎖遠端使用者的工作階段一小時。當封鎖期限到期時，Kaspersky Endpoint Security 將從封鎖清單中刪除電腦並還原對共用資料夾的存取。

**如何在管理主控台 (MMC) 中設定不受信任電腦的封鎖期限**

1. 在卡巴斯基安全管理中心管理主控台樹狀目錄中，選取**政策**。

2. 選擇必要的政策並點擊以開啟政策內容。

3. 在政策視窗中，選擇"**進階威脅防護 → 加密軟體防護**"。

4. 在 **偵測到威脅後的動作** 塊中，選擇 **封鎖連線時間 N 分鐘**。

5. 配置對從事惡意活動或資料加密的不受信任電腦的封鎖期限。

6. 儲存變更。

**如何在網頁主控台和雲端主控台中設定不受信任電腦的封鎖期限**

1. 在網頁主控台的主視窗中，選擇**資產（裝置）→ 政策和設定檔**。

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. 在**偵測到威脅後的動作**下面，配置對從事惡意活動或資料加密的不受信任電腦的封鎖期限。

6. 儲存變更。

**如何在應用程式介面中設定不受信任電腦的封鎖期限**

1. 在"應用程式主視窗"中，點擊⚙按鈕。

2. 在應用程式設定視窗中，選取"**進階威脅防護**"→"**加密軟體防護**"。

3. 在"**偵測到威脅後的動作**"塊中，選取"**封鎖連線（分鐘）**"。

4. 配置對從事惡意活動或資料加密的不受信任電腦的封鎖期限。

5. 儲存變更。

結果，遠端電腦將被鎖定。若要解鎖遠端電腦，您可以重新啟動 Kaspersky Endpoint Security。

# 編輯防護範圍

*防護範圍* 是 Kaspersky Endpoint Security 監控檔案活動的共用資料夾的路徑清單。Kaspersky Endpoint Security 輸入遮罩時支援環境變量以及`*`和`?`字元。預設情況下，應用程式會自動識別共用資料夾並監視所有資料夾中的檔案活動。

如果您的組織在使用共用資料夾交換檔案時使用資料加密，從防護範圍中排除資料夾可減少誤報的數量。例如，當使用者在共用資料夾中處理具有 ENC 副檔名的檔案時，行為偵測可能提高誤判數量。此類活動比對外部加密通常有的行為模式。如果您加密了共用資料夾中的檔案以防護資料，請將該資料夾新增到排除項目。

> 您還可以 排除不得處理外部加密嘗試的電腦。

**如何在管理主控台 (MMC) 中編輯防護範圍**

1. 在卡巴斯基安全管理中心管理主控台樹狀目錄中，選取**政策**。

2. 選擇必要的政策並點擊以開啟政策內容。

3. 在政策視窗中，選擇"**進階威脅防護 → 加密軟體防護**"。

4. 在"**防護範圍**"塊中，選取"**僅指定的共用資料夾**"。

5. 在資料夾清單中，點擊"**新增**"。

6. 這將開啟一個視窗；在該視窗中，輸入要包含在防護範圍中的共用資料夾的路徑（例如，`C:\Share`）。

   > 若要將共用資料夾新增至防護範圍，請使用本機路徑。

7. 點擊"**確定**"。

8. 如有必要，定義防護範圍排除項目：

   a. 在"**掃描排除項目**"塊中，點擊"**根據遮罩**"按鈕。

   b. 在開啟的視窗中，點擊"**新增**"按鈕。

   c. 在顯示的視窗中，指定`*.<file extension>`格式的檔案副檔名或資料夾路徑。Kaspersky Endpoint Security 輸入遮罩時支援`*`和`?`字元。

      該應用程式不支援某些排除項目檔案副檔名。因此，您可以將排除項目指定為`*.docx`或者`**\Folder\**`。

   您可以從掃描中排除物件，而無需將其從防護範圍內的物件清單中刪除。為此，請清除物件旁邊的核取方塊。

9. 儲存變更。

**如何在網頁主控台和雲端主控台中編輯防護範圍**

1. 在網頁主控台的主視窗中，選擇**資產（裝置）→政策和設定檔**。

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. 在"**防護範圍**"塊中，選取"**僅指定的共用資料夾**"。

6. 在資料夾清單中，點擊"**新增**"。

7. 這將開啟一個視窗；在該視窗中，輸入要包含在防護範圍中的共用資料夾的路徑（例如，`C:\Share`）。

   若要將共用資料夾新增至防護範圍，請使用本機路徑。

8. 點擊"**確定**"。

9. 如有必要，定義防護範圍排除項目：

   a. 在視窗上方，點擊"**掃描排除項目**"連接。

   b. 在開啟的視窗中，點擊"**新增**"按鈕。

   c. 在顯示的視窗中，指定`*.<file extension>`格式的檔案副檔名或資料夾路徑。Kaspersky Endpoint Security 輸入遮罩時支援`*`和`?`字元。

      該應用程式不支援某些排除項目檔案副檔名。因此，您可以將排除項目指定為`*.docx`或者`**\Folder\**`。

   您可以從掃描中排除物件，而無需將其從防護範圍內的物件清單中刪除。為此，請清除物件旁邊的核取方塊。

10. 儲存變更。

**如何在應用程式介面中編輯防護範圍**

1. 在“應用程式主視窗”中，點擊⚙按鈕。
2. 在應用程式設定視窗中，選取”**進階威脅防護**“→“**加密軟體防護**”。
3. 在“**防護範圍**”塊中，選取“**僅指定的共用資料夾**”。
4. 在資料夾清單中，點擊“**新增**”。
5. 這將開啟一個視窗；在該視窗中，輸入要包含在防護範圍中的共用資料夾的路徑（例如， `C:\Share` ）。

   若要將共用資料夾新增至防護範圍，請使用本機路徑。

6. 點擊“**確定**”。
7. 如有必要，定義防護範圍排除項目：

   a. 在視窗上方，點擊“**按遮罩排除**”連接。

   b. 在開啟的視窗中，點擊“**新增**”按鈕。

   c. 在顯示的視窗中，指定`*.<file extension>`格式的檔案副檔名或資料夾路徑。Kaspersky Endpoint Security 輸入遮罩時支援`*`和`?`字元。

   該應用程式不支援某些排除項目檔案副檔名。因此，您可以將排除項目指定為`*.docx`或者`**\Folder\**`。

   您可以從掃描中排除物件，而無需將其從防護範圍內的物件清單中刪除。為此，請清除物件旁邊的核取方塊。

8. 儲存變更。

1. 在“應用程式主視窗”中，點擊⚙按鈕。
2. 在應用程式設定視窗中，選取”**一般設定**“→“**排除項目和偵測到的物件類型**”。
3. 在”**排除項目**”塊中，點擊”**管理排除項目**”連接。
4. 點擊“**新增**”。
5. 點擊**瀏覽**並選擇共用資料夾。

您也可以手動輸入路徑。Kaspersky Endpoint Security 輸入遮罩時支援* 和 ?字元：

- `*`（星號）字元代表任意一組字元，但 `\` 和 `/` 字元除外（這兩個字元是檔案和資料夾路徑中的檔案和資料夾名稱的分隔符號）。例如，遮罩“`C:\*\*.txt`”將包括位於 C: 磁碟機但是不在子資料夾中所有帶 TXT 副檔名的檔案的路徑。

- 兩個連續 `*` 字元在檔案或資料夾名稱中代表任意一組字元（包括空集），包括 `\` 和 `/` 字元（這兩個字元是檔案和資料夾路徑中的檔案和資料夾名稱的分隔符號）。例如，遮罩 `C:\Folder\**\*.txt` 將包括位於巢嵌在 `Folder` 內的資料夾（`Folder`自身除外）中所有帶 TXT 副檔名的檔案的路徑。遮罩必須包含至少一個嵌套等級。遮罩 `C:\**\*.txt` 不是有效遮罩。

- `?`（問號）字元代表任意單個字元，但 `\` 和 `/` 字元除外（這兩個字元是檔案和資料夾路徑中的檔案和資料夾名稱的分隔符號）。例如，遮罩 `C:\Folder\???.txt` 將包括位於 `Folder` 資料夾中所有帶 TXT 副檔名且名稱由三個字元構成的檔案的路徑。

您可以在路徑的開始、中間或者結尾使用遮罩。例如，如果您想要將一個針對所有使用者的資料夾新增到排除項目，請輸入 `?:\Users\*\Folder\` 遮罩。

6. 在“**防護元件**“塊中，選中“**行為偵測**”元件。

7. 如有必要，在“**註釋**”欄位，輸入您建立的掃描排除項目的簡要說明。

8. 選擇排除項目的“**啟動**”狀態。

   您可以隨時使用開關停止排除。

9. 儲存變更。

1. 在網頁主控台的主視窗中，選擇**資產（裝置）→ 政策和設定檔**。

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“**惡意軟體掃描排除項目**”連接。

6. 如果要為公司內的所有電腦建立排除項目的綜合清單，請選取“**繼承時合併值**”核取方塊。將合併父政策和子政策中的排除項目清單。如果啟用繼承時合併值，則將合併清單。父政策中的排除項目以唯讀視圖的形式顯示在子政策中。無法變更或刪除父政策的排除項目。

7. 如果想要使用者能夠建立本機排除項目清單，請選中“**允許使用本機排除項目**“核取方塊。這樣，除了在政策中產生的排除項目的一般清單外，使用者还可以建立自己的排除項目本機清單。管理員可以使用卡巴斯基安全管理中心檢視、新增、編輯或刪除電腦屬性中的清單項目。

   如果核取方塊被清理，使用者只能存取政策中產生的排除項目的一般清單。此外，如果清除此核取方塊，Kaspersky Endpoint Security 會在應用程式的使用者介面中隱藏掃描排除項目的合併清單。

8. 點擊**新增** 並選擇一個操作：

   - **類別**您可以將掃描排除項目分組到不同的類別。若要建立新類別，請輸入類別名稱並在該類別中新增至少一個掃描排除項目。

   - **新排除項目**Kaspersky Endpoint Security 會將新的掃描排除項目新增至清單的根目錄。

   - **從清單中選取排除項目**為了在 SQL 伺服器、Microsoft Exchange 伺服器和 System Center Configuration Manager 上快速設定 Kaspersky Endpoint Security，應用程式包括*預定義的掃描排除項目*。另外還新增了預先定義的掃描排除項目，以支援 Citrix 和 VMware 虛擬環境中的應用程式安裝。您必須根據受防護伺服器的用途選擇預先定義的掃描排除項目。

9. 選擇要如何新增排除項目**檔案或資料夾路徑**。

10. 輸入共用資料夾的路徑。

    您也可以手動輸入路徑。Kaspersky Endpoint Security 輸入遮罩時支援`*` 和 `?`字元：

    - `*`（星號）字元代表任意一組字元，但 `\` 和 `/` 字元除外（這兩個字元是檔案和資料夾路徑中的檔案和資料夾名稱的分隔符號）。例如，遮罩"`C:\*\*.txt`"將包括位於 C: 磁碟機但是不在子資料夾中所有帶 TXT 副檔名的檔案的路徑。

    - 兩個連續 `*` 字元在檔案或資料夾名稱中代表任意一組字元（包括空集），包括 `\` 和 `/` 字元（這兩個字元是檔案和資料夾路徑中的檔案和資料夾名稱的分隔符號）。例如，遮罩 `C:\Folder\**\*.txt` 將包括位於巢嵌在 `Folder` 內的資料夾（`Folder`自身除外）中所有帶 TXT 副檔名的檔案的路徑。遮罩必須包含至少一個嵌套等級。遮罩 `C:\**\*.txt` 不是有效遮罩。

    - `?`（問號）字元代表任意單個字元，但 `\` 和 `/` 字元除外（這兩個字元是檔案和資料夾路徑中的檔案和資料夾名稱的分隔符號）。例如，遮罩 `C:\Folder\???.txt` 將包括位於 `Folder` 資料夾中所有帶 TXT 副檔名且名稱由三個字元構成的檔案的路徑。

    您可以在路徑的開始、中間或者結尾使用遮罩。例如，如果您想要將一個針對所有使用者的資料夾新增到排除項目，請輸入 `C:\Users\*\Folder\` 遮罩。

11. 在"**套用排除項目到**"塊中，選中"**行為偵測**"元件。

12. 如有必要，在"**註釋**"欄位，輸入您建立的掃描排除項目的簡要說明。

13. 選擇排除項目的"**新增至排除項目**"狀態。

    您可以隨時使用開關停止排除。

14. 儲存變更。

1. 在卡巴斯基安全管理中心管理主控台樹狀目錄中，選取**政策**。

2. 選擇必要的政策並點擊以開啟政策內容。

3. 在政策視窗中，選擇"**一般設定 → 排除項目和物件類型**"。

4. 在"**掃描排除項目和受信任應用程式 → 掃描排除項目**"塊中，點擊"**設定**"按鈕。

   這將開啟包含排除項目清單的視窗。

5. 如果要為公司內的所有電腦建立排除項目的綜合清單，請選取"**繼承時合併值**"核取方塊。將合併父政策和子政策中的排除項目清單。如果啟用繼承時合併值，則將合併清單。父政策中的排除項目以唯讀視圖的形式顯示在子政策中。無法變更或刪除父政策的排除項目。

6. 如果想要使用者能夠建立本機排除項目清單，請選中**"允許使用本機排除項目"**核取方塊。這樣，除了在政策中產生的排除項目的一般清單外，使用者还可以建立自己的排除項目本機清單。管理員可以使用卡巴斯基安全管理中心檢視、新增、編輯或刪除電腦屬性中的清單項目。

   如果核取方塊被清理，使用者只能存取政策中產生的排除項目的一般清單。此外，如果清除此核取方塊，Kaspersky Endpoint Security 會在應用程式的使用者介面中隱藏掃描排除項目的合併清單。

7. 點擊**新增** 並選擇一個操作：

   - **類別**您可以將掃描排除項目分組到不同的類別。若要建立新類別，請輸入類別名稱並在該類別中新增至少一個掃描排除項目。
   - **新排除項目**Kaspersky Endpoint Security 會將新的掃描排除項目新增至清單的根目錄。
   - **從清單中選取排除項目**為了在 SQL 伺服器、Microsoft Exchange 伺服器和 System Center Configuration Manager 上快速設定 Kaspersky Endpoint Security，應用程式包括*預定義的掃描排除項目*。另外還新增了預先定義的掃描排除項目，以支援 Citrix 和 VMware 虛擬環境中的應用程式安裝。您必須根據受防護伺服器的用途選擇預先定義的掃描排除項目。

8. 點擊**"新增"**。

9. 在**"內容"**塊中，選中**"檔案或資料夾"**核取方塊。

10. 點擊「**掃描排除項目說明(點擊下劃線項目進行編輯)**」區塊中的「**選擇檔案或資料夾。**」連結以開啟「**檔案或資料夾名稱**」視窗。

11. 點擊**瀏覽**並選擇共用資料夾。

    您也可以手動輸入路徑。Kaspersky Endpoint Security 輸入遮罩時支援* 和 ?字元：

    - `*`（星號）字元代表任意一組字元，但 `\` 和 `/` 字元除外（這兩個字元是檔案和資料夾路徑中的檔案和資料夾名稱的分隔符號）。例如，遮罩**"**`C:\*\*.txt`**"**將包括位於 C: 磁碟機但是不在子資料夾中所有帶 TXT 副檔名的檔案的路徑。
    - 兩個連續 `*` 字元在檔案或資料夾名稱中代表任意一組字元（包括空集），包括 `\` 和 `/` 字元（這兩個字元是檔案和資料夾路徑中的檔案和資料夾名稱的分隔符號）。例如，遮罩 `C:\Folder\**\*.txt` 將包括位於巢嵌在 `Folder` 內的資料夾（`Folder`自身除外）中所有帶 TXT 副檔名的檔案的路徑。遮罩必須包含至少一個嵌套等級。遮罩 `C:\**\*.txt` 不是有效遮罩。
    - `?`（問號）字元代表任意單個字元，但 `\` 和 `/` 字元除外（這兩個字元是檔案和資料夾路徑中的檔案和資料夾名稱的分隔符號）。例如，遮罩 `C:\Folder\???.txt` 將包括位於 `Folder` 資料夾中所有帶 TXT 副檔名且名稱由三個字元構成的檔案的路徑。

    您可以在路徑的開始、中間或者結尾使用遮罩。例如，如果您想要將一個針對所有使用者的資料夾新增到排除項目，請輸入 `?:\Users\*\Folder\` 遮罩。

12. 如有必要，在**"註解"**欄位，輸入您建立的掃描排除項目的簡要說明。

13. 點擊**掃描排除項目說明(點擊下劃線項目進行編輯)**區塊中的連結以開啟**防護元件**視窗。

14. 選中**行為偵測**元件旁邊的核取方塊。

15. 儲存變更。

# 新增受信任電腦以進行外部資料加密

如果您的組織在檔案交換工作流程中使用外部資料加密，則您必須建立受信任電腦清單。Kaspersky Endpoint Security 不監控受信任電腦的資料加密。

必須啟用稽核登入服務，才能從共用資料夾對外部加密的防護中排除位址。預設情況下，稽核登入服務已停用（有關啟用稽核登入服務的詳細資訊，請存取 Microsoft 網站）。

如果遠端電腦在 Kaspersky Endpoint Security 啟動前啟動，從共用資料夾防護中排除位址的功能將不適用於該遠端電腦。您可以在 Kaspersky Endpoint Security 啟動後重啟該遠端電腦，確保從共用資料夾防護中排除位址的功能在此遠端電腦上有效。

**如何在管理主控台 (MMC) 中新增受信任電腦以進行外部資料加密**

1. 在卡巴斯基安全管理中心管理主控台樹狀目錄中，選取**政策**。
2. 選擇必要的政策並點擊以開啟政策內容。
3. 在政策視窗中，選擇"**進階威脅防護 → 加密軟體防護**"。
4. 在"**掃描排除項目**"塊中，點擊"**按名稱或 IP 位址**"按鈕。
5. 在開啟的視窗中，點擊"**按名稱或 IP 位址**"按鈕。
6. 輸入不得處理其外部加密嘗試的電腦的 IP 位址、IP 位址範圍或名稱。
   例如：
   - `192.168.0.0 - 192.168.255.255`
   - `192.168.0.0/24`
   - `192.168.2-3.0-128`
   - `2001:db8:fd0c::/64`
   - `2001:db8:fd0c:: - 2001:db8:fd0c:ffff:ffff:ffff:ffff:ffff`
7. 儲存變更。

**如何在網頁主控台和雲端主控台中新增受信任電腦以進行外部資料加密**

1. 在網頁主控台的主視窗中，選擇**資產（裝置）→ 政策和設定檔**。
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. 在視窗上方，點擊“**按照名稱或 IP 位址 ({0}) 的排除項目**”連接。
6. 在開啟的視窗中，點擊“**新增**”按鈕。
7. 輸入不得處理其外部加密嘗試的電腦的 IP 位址、IP 位址範圍或名稱。
   例如：
   - `192.168.0.0 - 192.168.255.255`
   - `192.168.0.0/24`
   - `192.168.2-3.0-128`
   - `2001:db8:fd0c::/64`
   - `2001:db8:fd0c:: - 2001:db8:fd0c:ffff:ffff:ffff:ffff:ffff`
8. 儲存變更。

**如何在應用程式介面中新增受信任電腦進行外部資料加密**

1. 在“應用程式主視窗”中，點擊⚙ 按鈕。
2. 在應用程式設定視窗中，選取”**進階威脅防護**“→“**加密軟體防護**”。
3. 在視窗上方，點擊“**按照名稱或 IP 位址的排除項目**”連接。
4. 在開啟的視窗中，點擊“**新增**”按鈕。
5. 輸入不得處理其外部加密嘗試的電腦的 IP 位址、IP 位址範圍或名稱。
   例如：
   - `192.168.0.0 - 192.168.255.255`
   - `192.168.0.0/24`
   - `192.168.2-3.0-128`
   - `2001:db8:fd0c::/64`
   - `2001:db8:fd0c:: - 2001:db8:fd0c:ffff:ffff:ffff:ffff:ffff`
6. 儲存變更。

# 匯出和匯入防止共用資料夾被外部加密的排除項目清單

您可以將排除項目清單匯出到 XML 檔案。然後，您可以修改檔案，例如，新增大量相同類型的位址。您還可以使用匯出/匯入功能來備份排除項目清單，或將清單遷移到其他伺服器。

**如何在管理主控台 (MMC) 中匯出和匯入排除項目清單**

1. 在卡巴斯基安全管理中心管理主控台樹狀目錄中，選取**政策**。
2. 選擇必要的政策並點擊以開啟政策內容。
3. 在政策視窗中，選擇"**進階威脅防護 → 加密軟體防護**"。
4. 在"**掃描排除項目**"塊中，點擊"**按名稱或 IP 位址**"按鈕。
5. 要匯出規則清單：
   a. 選取您想要匯出的排除項目。要選擇多個連接埠，請使用**CTRL**或**SHIFT**鍵。
      如果您未選擇任何排除項目，則 Kaspersky Endpoint Security 將匯出所有排除項目。
   b. 點擊 → **匯出** 按鈕。
   c. 在開啟的視窗中，指定您要將排除項目清單匯出到的 XML 檔案的名稱，然後選取要儲存此檔案的資料夾。
   d. 儲存檔案。
      Kaspersky Endpoint Security 會將整個排除項目清單匯出到 XML 檔案。
6. 若要匯入排除項目清單：
   a. 點擊 → **匯入** 按鈕。
   b. 在開啟的視窗中，選取要從中匯入排除項目清單的 XML 檔案。
   c. 開啟檔案。
      如果電腦已經具有排除項目清單，則 Kaspersky Endpoint Security 將提示您刪除現有清單或從 XML 檔案向其中新增新項目。
7. 儲存變更。

**如何在網頁主控台和 Cloud Console 中匯出和匯入排除項目清單**

1. 在網頁主控台的主視窗中，選擇**資產（裝置）→ 政策和設定檔**。
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. 點擊"**按照名稱或 IP 位址 ({0}) 的排除項目**"連接。
6. 要匯出規則清單：
   a. 選取您想要匯出的排除項目。
   b. 點擊 → **匯出** 按鈕。
      Kaspersky Endpoint Security 會將排除項目清單匯出到預設下載資料夾中的 JSON 檔案。

7. 若要匯入排除項目清單：

   a. 點擊 → **匯入** 按鈕。

      在開啟的視窗中，選取要從中匯入排除項目清單的 JSON 檔案。

   b. 開啟檔案。

      如果電腦已經具有排除項目清單，則 Kaspersky Endpoint Security 將提示您刪除現有清單或從 JSON 檔案向其中新增新項目。

8. 儲存變更。

# 修復引擎

修復引擎允許 Kaspersky Endpoint Security 復原惡意軟體在作業系統中執行的操作。

回溯作業系統中的惡意軟體活動時，Kaspersky Endpoint Security 將處理以下類型的惡意軟體活動：

- **檔案活動**

  Kaspersky Endpoint Security 執行以下操作：

  - 移除惡意軟體（在除網路磁碟外的所有介質上）建立的可執行檔。
  - 移除已被惡意軟體入侵的程式所建立的可執行檔。
  - 還原被惡意軟體修改或刪除的檔案。

  檔案還原功能有一些限制。

- **登錄檔活動**

  Kaspersky Endpoint Security 執行以下操作：

  - 刪除由惡意軟體建立的登錄機碼。
  - 不會還原被惡意軟體修改或刪除的登錄機碼。

- **系統活動**

  Kaspersky Endpoint Security 執行以下操作：

  - 終止由惡意軟體啟動的處理程序。
  - 終止被惡意應用程式滲透的處理程序。
  - 不會還原被惡意程式掛起的處理程序。

- **網絡活動**

  Kaspersky Endpoint Security 執行以下操作：

  - 封鎖惡意軟體的網路活動。
  - 封鎖被惡意軟體入侵的處理程序的網路活動。

"檔案威脅防護"或"行為偵測"元件或在惡意軟體掃描過程中可以啟動惡意軟體操作回溯。

回溯惡意程式操作的過程將會影響一組嚴格限定的資料。回溯對於作業系統或您的電腦中資料的完整性不會產生負面影響。

**如何在管理主控台（MMC）中啟用或停用修復引擎元件**

1. 在卡巴斯基安全管理中心管理主控台樹狀目錄中，選取**政策**。
2. 選擇必要的政策並點擊以開啟政策內容。
3. 在政策視窗中，選擇"**進階威脅防護 → 修復引擎**"。
4. 使用"**修復引擎**"核取方塊來啟用或停用元件。
5. 儲存變更。

**如何在網頁主控台和雲端主控台中啟用或停用修復引擎元件**

1. 在網頁主控台的主視窗中，選擇**資產（裝置）→ 政策和設定檔**。
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**" → "**修復引擎**"。
5. 使用"**修復引擎已啟用**"切換開關可啟用或停用元件。
6. 儲存變更。

**如何在應用程式介面中啟用或停用修復引擎元件**

1. 在"應用程式主視窗"中，點擊⚙按鈕。
2. 在應用程式設定視窗中，選取"**進階威脅防護**"→"**修復引擎**"。
3. 使用"**修復引擎**"切換開關可啟用或停用元件。
4. 儲存變更。

因此，如果啟用了修復引擎，則 Kaspersky Endpoint Security 將復原由作業系統中的惡意應用程式執行的操作。

# 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。

KSN 功能可能無法在美國的應用程式中使用。

*卡巴斯基安全網路（KSN）*是雲端服務的基礎結構，可提供對線上卡巴斯基知識庫的存取，該知識庫包含有關檔案、網頁資源和軟體信譽的資訊。使用卡巴斯基安全網路的資料可確保 Kaspersky 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 提供有關所掃描檔案的類別和信譽的資訊，以及有關所掃描網址的信譽的資訊。

卡巴斯基安全網路的使用是自願的。應用程式將在初始化設定期間提示您使用 KSN。使用者可以隨時開始或停止加入 KSN。

有關在參與 KSN 期間生成的 Kaspersky 統計資訊的傳送詳情，以及有關此類資訊的儲存和銷毀，請參閱卡巴斯基安全網路聲明和 Kaspersky 網站。含有卡巴斯基安全網路聲明文字的 ksn_<語言 ID>.txt 檔案包括在應用程式分發套件中。

### 卡巴斯基信譽資料庫的基礎結構

Kaspersky Endpoint Security 支援以下用於使用 Kaspersky 信譽資料庫的基礎結構解決方案：

- *卡巴斯基安全網路 (KSN)* 是大多數 Kaspersky 應用程式使用的解決方案。KSN 參與者從卡巴斯基接收資訊，並向 Kaspersky 傳送使用者電腦上偵測到的物件的資訊，以便 Kaspersky 分析人員進行額外分析，並包括在信譽和統計資料庫中。
- *卡巴斯基安全網路 (KSN)* 是讓承載 Kaspersky 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。
  - 法律禁止或公司安全政策限制將任何資料傳輸到國家/地區外部或公司 LAN 外部。

# 啟用和停用卡巴斯基安全網路的使用

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。

**如何在管理主控台（MMC）中啟用或停用 KSN 使用**

1. 在卡巴斯基安全管理中心管理主控台樹狀目錄中，選取**政策**。
2. 選擇必要的政策並點擊以開啟政策內容。
3. 在政策視窗中，選擇"**進階威脅防護 → 卡巴斯基安全網路**"。
4. 使用"**卡巴斯基安全網路**"切換開關可啟用或停用元件。

   如果啟用了使用 KSN，Kaspersky Endpoint Security 將顯示卡巴斯基安全網路聲明。如果同意，請接受《卡巴斯基安全網路(KSN)聲明》的使用條款。
5. 如有必要，清除"**啟用延伸 KSN 模式**"核取方塊。
6. 儲存變更。若要在電腦上套用該政策，請關閉掛鎖。

**如何在網頁主控台和雲端主控台中啟用或停用 KSN 使用**

1. 在網頁主控台的主視窗中，選擇**資產（裝置）→政策和設定檔**。
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"**「使用卡巴斯基安全網路 (KSN)」已啟用**"切換開關可啟用或停用元件。

   如果啟用了使用 KSN，Kaspersky Endpoint Security 將顯示卡巴斯基安全網路聲明。如果同意，請接受《卡巴斯基安全網路(KSN)聲明》的使用條款。
6. 如果需要，請關閉"**啟用延伸 KSN 模式**"開關。
7. 儲存變更。若要在電腦上套用該政策，請關閉掛鎖。

**如何在應用程式介面中啟用或停用 KSN 使用**

1. 在"應用程式主視窗"中，點擊 按鈕。
2. 在應用程式設定視窗中，選取"**進階威脅防護**"→"**卡巴斯基安全網路**"。
3. 使用"**卡巴斯基安全網路**"切換開關可啟用或停用元件。

   如果啟用了使用 KSN，Kaspersky Endpoint Security 將顯示卡巴斯基安全網路聲明。如果同意，請接受《卡巴斯基安全網路(KSN)聲明》的使用條款。
4. 如果需要，請關閉"**啟用延伸 KSN 模式**"開關。
5. 儲存變更。

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。

# 卡巴斯基私有安全網路的限制

*卡巴斯基安全網路 (KSN)* 是讓承載 Kaspersky 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。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。
- 該應用程式使用掃描最佳化技術（例如 iSwift 或 iChecker），或者正在將信譽請求快取到 KSN / KPSN。在這種情況下，應用程式不可請求先前掃描的物件的信譽。
- 為了最佳化其工作量，應用程式掃描特定格式和大小的檔案。有關格式和大小限制的清單由卡巴斯基專家確定。此清單已使用應用程式的病毒資料庫更新。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。
- Light Agent 模式下的 Kaspersky Endpoint Security 透過 KSN 代理伺服器與 KSN 伺服器通訊。不支援與 KSN 直接通訊。

# 為防護元件啟用和停用雲端模式

*雲端模式* 是指 Kaspersky Endpoint Security 使用輕量級版本的病毒資料庫的應用程式執行模式。當使用輕量級病毒資料庫時，卡巴斯基安全網路支援應用程式執行。與通常的資料庫相比，輕量級版本的病毒資料庫僅需要大約一半的電腦 RAM。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。

從卡巴斯基專屬安全網路版本 3.0 開始，在使用卡巴斯基專屬安全網路時，雲端模式功能可用。

如果應用程式在 Light Agent 模式下工作，雲端模式不可用。

**如何在管理主控台（MMC）中啟用或停用防護元件的雲端模式**

1. 在卡巴斯基安全管理中心管理主控台樹狀目錄中，選取**政策**。
2. 選擇必要的政策並點擊以開啟政策內容。
3. 在政策視窗中，選擇“**進階威脅防護 → 卡巴斯基安全網路**”。
4. 使用“**啟用雲端模式**“核取方塊來啟用或停用元件。
5. 儲存變更。若要在電腦上套用該政策，請關閉掛鎖。

**如何在網頁主控台和雲端主控台中啟用或停用防護元件的雲端模式**

1. 在網頁主控台的主視窗中，選擇**資產（裝置）→ 政策和設定檔**。
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. 儲存變更。若要在電腦上套用該政策，請關閉掛鎖。

**如何在應用程式介面中啟用或停用防護元件的雲端模式**

1. 在“應用程式主視窗”中，點擊按鈕。

2. 在應用程式設定視窗中，選取”**進階威脅防護**“→“**卡巴斯基安全網路**”。

3. 使用“**啟用雲端模式**“切換開關可啟用或停用元件。

4. 儲存變更。

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 代理設定

受卡巴斯基安全管理中心管理伺服器管理的使用者電腦可以透過 KSN 代理服務與 KSN 互動。

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 透過 KSN 代理伺服器與 KSN 伺服器進行通訊。

KSN 代理服務提供以下功能：

- 使用者的電腦可以查詢的 KSN 和將資訊送交 KSN，即使沒有直接連線網際網路。
- KSN 代理服務暫存處理過的資料，從而減少外部網路通訊信道上的負荷，並加快使用者接收資料的速度。

預設情況下，在 KSN 被啟用和 KSN 聲明被接受後，應用程式將使用代理伺服器連線到卡巴斯基安全網路。應用程式使用的代理伺服器是透過 TCP 連接埠 13111 的卡巴斯基安全管理中心管理伺服器。因此，如果 KSN 代理不可用，您需要驗證以下資訊：

- *Ksnproxy* 服務正在管理伺服器上執行。
- 電腦上的防火墙沒有封鎖連接埠 13111。

您可以如下配置KSN 代理：啟用或停用 KSN 代理，然後配置用於連線的連接埠。為此，您需要開啟管理伺服器內容。有關 KSN 代理配置的詳細資訊，請參閱卡巴斯基安全管理中心說明。您也可以在 Kaspersky Endpoint Security 政策中為單台電腦啟用或停用 KSN 代理。

**如何在管理主控台（MMC）中啟用或停用 KSN 代理**

1. 在卡巴斯基安全管理中心管理主控台樹狀目錄中，選取**政策**。
2. 選擇必要的政策並點擊以開啟政策內容。
3. 在政策視窗中，選擇**"進階威脅防護 → 卡巴斯基安全網路"**。
4. 在**"KSN 代理設定"**塊中，使用**"使用管理伺服器為 KSN 代理伺服器"**核取方塊來啟用或停用 KSN 代理。
5. 如有必要，選中**"當 KSN 代理伺服器不可用時使用卡巴斯基安全網路伺服器"**核取方塊。

   如果選中該核取方塊，當 KSN 代理服務不可用時，Kaspersky Endpoint Security 將使用 KSN 伺服器。KSN 伺服器可以位於 Kaspersky 側，也可以位於協力廠商一側的伺服器（使用卡巴斯基私有安全網路時）。
6. 儲存變更。

**如何在 Web 主控台中啟用或停用 KSN 代理**

1. 在網頁主控台的主視窗中，選擇**資產（裝置）→ 政策和設定檔**。
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"**核取方塊可啟用或停用 KSN 代理。
6. 如有必要，選中**"當 KSN 代理伺服器不可用時使用卡巴斯基安全網路伺服器"**核取方塊。

   如果選中該核取方塊，當 KSN 代理服務不可用時，Kaspersky Endpoint Security 將使用 KSN 伺服器。KSN 伺服器可以位於 Kaspersky 側，也可以位於協力廠商一側的伺服器（使用卡巴斯基私有安全網路時）。
7. 儲存變更。

KSN 代理位址與管理伺服器位址比對。如果管理伺服器網域名稱被變更，則您需要手動更新 KSN 代理位址。

*若要配置 KSN 代理位址：*

1. 開啟卡巴斯基安全管理中心管理主控台。
2. 在主控台樹狀目錄中，選擇**進階 → 遠端安裝 → 安裝套件**資料夾。
3. 在**"安裝套件"**資料夾的內容功能表中，選取**"內容"**。
4. 在開啟視窗的**"一般"**標籤上，指定 KSN 代理伺服器的新位址。
5. 儲存變更。

# 在卡巴斯基安全網路中檢查檔案信譽

如果您懷疑某個檔案的安全性，可以在卡巴斯基安全網路中檢查其信譽。

如果您已接受"卡巴斯基安全網路聲明"的條款，則可以檢查檔案的信譽。

*若要在卡巴斯基安全網路中檢查檔案信譽：*

開啟檔案內容功能表，然後選取"**檢查 KSN 中的信譽**"選項（請參見下圖）。




檔案內容功能表

Kaspersky Endpoint Security 會顯示檔案信譽：

**受信任(卡巴斯基安全網路)**。如果滿足以下一個或多個條件，檔案將被應用程式視為可信：

- 檔案由受信任的供應商進行數位簽章；
- 檔案在卡巴斯基安全網路中具有受信任的聲譽；
- 使用者將此應用程式歸類在信任群組。

**可被入侵者利用以破壞您的電腦或個人資料的合法軟體**。有關可被犯罪分子用來破壞電腦或使用者個人資料的合法軟體的詳細資訊，請造訪 Kaspersky IT 百科全書網站。您可以將這些應用程式新增到受信任清單。

**不受信任(卡巴斯基安全網路)**。造成威脅的病毒或其他應用程式。

**未知(卡巴斯基安全網路)**。卡巴斯基安全網路沒有任何有關此檔案的資訊。您可以使用防毒資料庫掃描檔案（內容功能表中的"**掃描病毒**"選項）。

Kaspersky Endpoint Security 會顯示用來確認檔案信譽的 KSN 解決方案：*卡巴斯基安全網路* or *卡巴斯基私有安全網路*。

Kaspersky Endpoint Security 還會顯示有關檔案的其他資訊（請參見下圖）。




卡巴斯基安全網路中的檔案信譽

# 加密連線掃描

安裝後，Kaspersky Endpoint Security 會將 Kaspersky 憑證新增到受信任憑證的系統儲存（Windows 憑證儲存）。Kaspersky Endpoint Security 使用該憑證掃描加密連線。Kaspersky Endpoint Security 還包括使用 Firefox 和 Thunderbird 中的受信任憑證系統儲存來掃描這些應用程式的流量。

Web 控制、 郵件威脅防護、Web 威脅防護、行為偵測和 弱點利用防禦元件可以解密和掃描透過使用以下協定建立的加密連線傳輸的網路流量：

- SSL 3.0。
- TLS 1.0、TLS 1.1、TLS 1.2、TLS 1.3。

# 啟用加密連線掃描

預設情況下，Kaspersky Endpoint Security 並不總是掃描加密連線，而僅在防護元件請求時才掃描。

**如何在管理主控台 (MMC) 中啟用加密連線**

1. 開啟卡巴斯基安全管理中心管理主控台。
2. 在主控台樹狀目錄中，選擇“**政策**”。
3. 選擇必要的政策並點擊以開啟政策內容。
4. 在政策視窗中，選擇“**一般設定 → 網路設定**”。

5. 在“**加密連線掃描**”塊中，選擇加密連線掃描模式：

   - **掃描加密連線**Kaspersky Endpoint Security 將無法存取其位址以`https://`開頭的網站的內容。
   - **根據防護元件的請求掃描加密連線**僅在 Web 威脅防護、郵件威脅防護和 Web 控制元件要求時，Kaspersky Endpoint Security 才會掃描加密流量。
   - **始終掃描加密連線**即使防護元件被停用，Kaspersky Endpoint Security 也會掃描加密的網路流量。

   Kaspersky Endpoint Security 不會掃描由停用了流量掃描的受信任應用程式建立的加密連線。Kaspersky Endpoint Security 不會掃描預定義的受信任網站清單中的加密連線。預定義的受信任網站清單由卡巴斯基專家建立。此清單已使用應用程式的病毒資料庫更新。您只能在 Kaspersky Endpoint Security 介面中檢視預定義的受信任網站清單。您只能在卡巴斯基安全管理中心主控台中檢視清單。

6. 如有必要，新增掃描排除項目：受信任位址和應用程式。
7. 設定用於掃描加密連線的設定（參見下表）。
8. 儲存變更。若要在電腦上套用該政策，請關閉掛鎖。

**如何在網頁主控台和雲端主控台中啟用加密連線**

1. 在網頁主控台的主視窗中，選擇**資產（裝置）** → **政策和設定檔**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**”→”**網路設定**”。
5. 在“**加密連線掃描**”下方，開啟“**加密連線掃描已啟用**”開關。
   如果此撥動按鈕被關閉，Kaspersky Endpoint Security 將無法存取其位址以`https://`開頭的網站的內容。
6. 點擊“**設定**”然後選擇加密連線掃描模式：

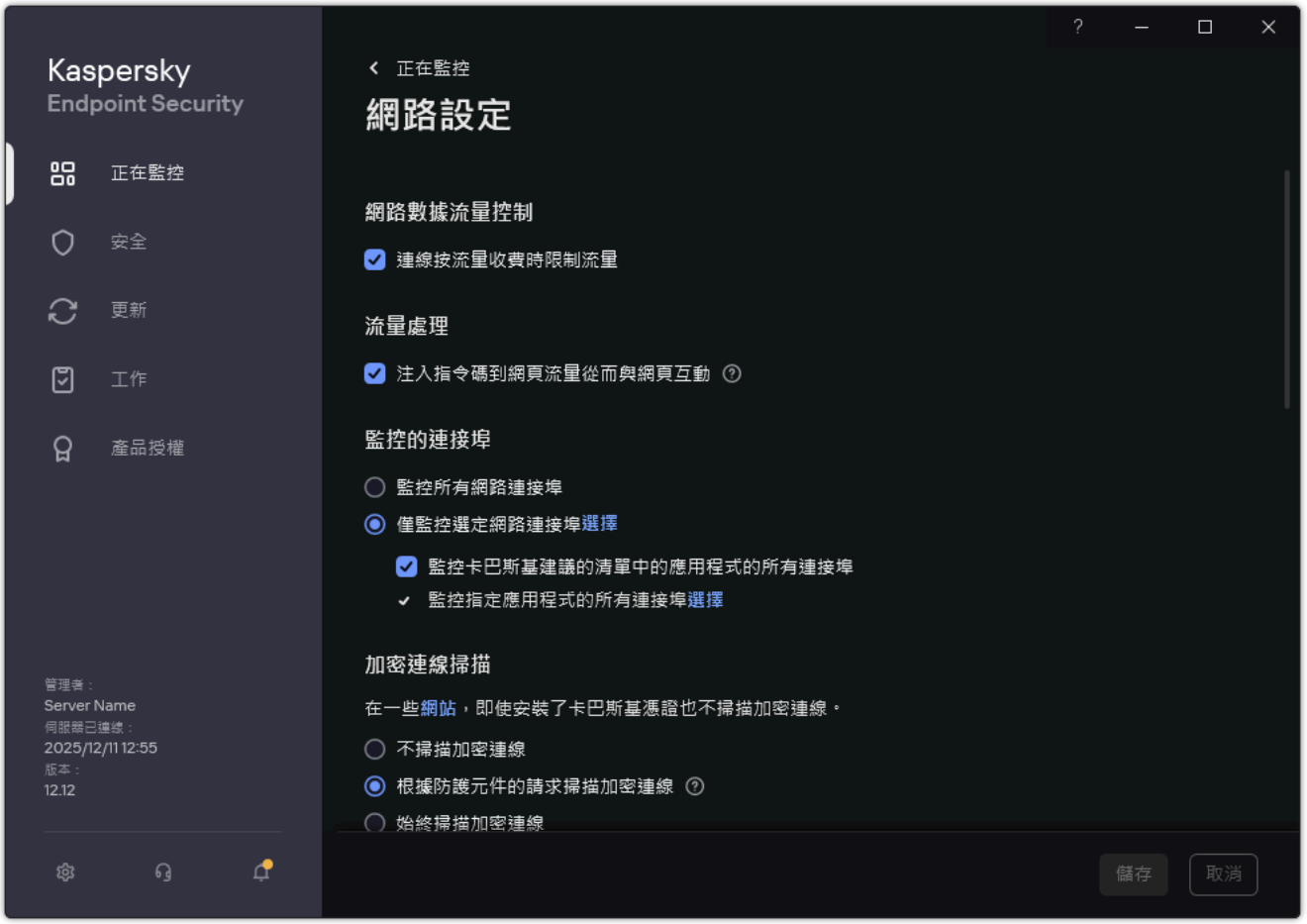
   - **根據防護元件的請求掃描加密連線**僅在 Web 威脅防護、郵件威脅防護和 Web 控制元件要求時，Kaspersky Endpoint Security 才會掃描加密流量。
   - **始終掃描加密連線**即使防護元件被停用，Kaspersky Endpoint Security 也會掃描加密的網路流量。

   Kaspersky Endpoint Security 不會掃描由停用了流量掃描的受信任應用程式建立的加密連線。Kaspersky Endpoint Security 不會掃描預定義的受信任網站清單中的加密連線。預定義的受信任網站清單由卡巴斯基專家建立。此清單已使用應用程式的病毒資料庫更新。您只能在 Kaspersky Endpoint Security 介面中檢視預定義的受信任網站清單。您只能在卡巴斯基安全管理中心主控台中檢視清單。

7. 如有必要，新增掃描排除項目：受信任位址和應用程式。
8. 設定用於掃描加密連線的設定（參見下表）。
9. 儲存變更。若要在電腦上套用該政策，請關閉掛鎖。

### 如何在應用程式介面中啟用加密連線

1. 在“應用程式主視窗”中，點擊⚙按鈕。
2. 在應用程式設定視窗中，選取”**一般設定**“→“**網路設定**”。




加密連線掃描設定

3. 在“**加密連線掃描**”塊中，選擇加密連線掃描模式：
   - **不掃描加密連線**Kaspersky Endpoint Security 將無法存取其位址以`https://`開頭的網站的內容。
   - **根據防護元件的請求掃描加密連線**僅在 Web 威脅防護、郵件威脅防護和 Web 控制元件要求時，Kaspersky Endpoint Security 才會掃描加密流量。
   - **始終掃描加密連線**即使防護元件被停用，Kaspersky Endpoint Security 也會掃描加密的網路流量。

   Kaspersky Endpoint Security 不會掃描由停用了流量掃描的受信任應用程式建立的加密連線。Kaspersky Endpoint Security 不會掃描預定義的受信任網站清單中的加密連線。預定義的受信任網站清單由卡巴斯基專家建立。此清單已使用應用程式的病毒資料庫更新。您只能在 Kaspersky Endpoint Security 介面中檢視預定義的受信任網站清單。您只能在卡巴斯基安全管理中心主控台中檢視清單。
4. 如有必要，新增掃描排除項目：受信任位址和應用程式。

5. 設定用於掃描加密連線的設定（參見下表）。




掃描加密連線的附加設定

6. 儲存變更。

加密連線掃描設定

| 參數 | 描述 |
| --- | --- |
| **信任根憑證** | 信任根憑證清單。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，你會因為憑證問題得到一個連線錯誤。若要新增至系統憑證商店，您可以使用 Active Directory 群組政策。 |
| **正在造訪具有不受信任憑證的網域** | • **允許**當存取具有不受信任憑證的網域時，Kaspersky Endpoint Security 將允許網路連線。<br>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，其中顯示警告和不建議存取該網域的原因。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。<br>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，Kaspersky Endpoint Security 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。<br>• **封鎖**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。 |
| **造訪包含加密連線掃描錯誤的網域** | • **封鎖**如果選取此項，在發生加密連線掃描錯誤時，Kaspersky Endpoint Security 會封鎖網路連線。<br>• **允許並新增網域至排除項目**如果選取此項，在發生加密連線掃描錯誤時，Kaspersky Endpoint Security 將導致錯誤的網域新增到具有掃描錯誤的網域清單中，並且在存取此網域時不監控加密網路流量。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。要清除清單內容，您需要選擇“**封鎖**”。Kaspersky Endpoint Security 還會為加密連線掃描錯誤產生一個事件。 |
| **封鎖 SSL 2.0 連線** | 如果選中該核取方塊，應用程式將監控和封鎖透過 SSL 2.0 協定建立的網路連線。<br>如果取消剔選此方格，應用程式不會封鎖透過 SSL 2.0 協定建立的網絡連線。不過，該應用程式不會監控通過該協定的網路流量。 |
| **封鎖 SSL 3.0 連線** | 如果選中該核取方塊，應用程式將封鎖透過 SSL 3.0 協定建立的網路連線。<br>如果取消剔選此方格，應用程式不會封鎖透過 SSL 3.0 協定建立的網絡連線。應用程式將監控透過該協定的網路流量。應用程式的所有組件均不受限制地運作。 |
| **封鎖 TLS 1.0 連線** | 如果選中該核取方塊，應用程式將封鎖透過 TLS 1.0 協定建立的網路連線。<br>如果清除該核取方塊，應用程式將不封鎖透過 TLS 1.0 協定建立的網路連線。應用程式將監控透過該協定的網路流量。應用程式的所有組件均不受限制地運作。 |

| 參數 | 描述 |
| --- | --- |
| **解密與使用 EV 憑證的網站之間的加密連線** | EV 憑證（Extended Validation Certificate）確認網站的真實性並增強連線的安全性。瀏覽器在網址列中使用鎖定圖示來指示網站具有 EV 憑證。瀏覽器也可能用綠色部分或完全渲染網址列。<br>如果選中該核取方塊，應用程式將解密並監控具有 EV 憑證的網站的加密連線。<br>如果清除該核取方塊，應用程式無權存取 HTTPS 流量的內容。為此，應用程式僅基於網址（例如 `https://bing.com`）監控 HTTPS 流量。<br>如果您第一次開啟具有 EV 憑證的網站，則無論是否選中該核取方塊，加密連線都將被解密。 |

# 安裝受信任根憑證

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，你會因為憑證問題得到一個連線錯誤。若要新增至系統憑證商店，您可以使用 Active Directory 群組政策。

### 如何在管理主控台 (MMC) 中安裝受信任根憑證

1. 在卡巴斯基安全管理中心管理主控台樹狀目錄中，選取**政策**。
2. 選擇必要的政策並點擊以開啟政策內容。
3. 在政策視窗中，選擇**"一般設定 → 網路設定"**。
4. 在**"信任根憑證"**塊中，點擊**"新增"**按鈕。
5. 這會開啟一個視窗，在視窗中選擇一個受信任根憑證。
   Kaspersky Endpoint Security 支援具有 PEM、DER 和 CRT 副檔名的憑證。
6. 儲存變更。

### 如何在網頁主控台和雲端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（裝置）→ 政策和設定檔**。
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. 點擊**"受信任根憑證"**連接。
6. 這會開啟一個視窗，點擊**"新增"**然後選擇一個受信任根憑證。
   Kaspersky Endpoint Security 支援具有 PEM、DER 和 CRT 副檔名的憑證。
7. 儲存變更。

**如何在應用程式介面中安裝受信任根憑證**

1. 在"應用程式主視窗"中，點擊⚙按鈕。
2. 在應用程式設定視窗中，選取"**一般設定**"→"**網路設定**"。
3. 在"**加密連線掃描**"塊中，點擊"**顯示憑證**"按鈕。
4. 這會開啟一個視窗，點擊"**新增**"然後選擇一個受信任根憑證。

   Kaspersky Endpoint Security 支援具有 PEM、DER 和 CRT 副檔名的憑證。
5. 儲存變更。

結果，當掃描流量時，除了系統憑證商店外，Kaspersky Endpoint Security 還使用自己的憑證商店。

# 掃描具有不受信任憑證的加密連線

安裝後，Kaspersky Endpoint Security 會將 Kaspersky 憑證新增到受信任憑證的系統儲存（Windows 憑證儲存）。Kaspersky Endpoint Security 使用該憑證掃描加密連線。在存取具有不受信任憑證的網域時，您可以允許或者拒絕使用者存取該網域（請參見以下操作指示）。

如果您允許使用者存取具有不受信任憑證的網域，Kaspersky Endpoint Security 將執行以下操作：

- 當在*瀏覽器*中存取具有不受信任憑證的網域時，Kaspersky Endpoint Security 會使用卡巴斯基憑證掃描流量。Kaspersky Endpoint Security 會顯示一個 HTML 頁面，上有不建議存取相關網域的警告和原因資訊（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。點擊此連結後，在隨後一個小時內存取同一網域中的其他資源時，Kaspersky Endpoint Security 不會顯示關於不受信任憑證的警告。Kaspersky Endpoint Security 還會就與不受信任憑證建立加密連線產生一個事件。

  在某些情況下，Kaspersky Endpoint Security 從技術上講無法在瀏覽器中顯示帶有警告的 HTML 頁面（見下圖）。例如，如果 Web 資源使用過時版本的網路協定和非標準連接埠。在這些情況下，Kaspersky Endpoint Security 會封鎖對此網域的存取，瀏覽器將顯示標準 `ERR_CONNECTION_RESET` 視窗。若要存取 Web 資源，您可以 將網域新增至排除項目 或使用受信任的憑證。

- 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，Kaspersky Endpoint Security 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。因此，如果協力廠商應用程式有內建憑證驗證工具，連線可能被終止。在此情況下，您必須聯絡網域擁有者然後設定受信任連線。如果無法設定受信任連線，您可以將該協力廠商應用程式新增至受信任應用程式清單。Kaspersky Endpoint Security 還會就與不受信任憑證建立加密連線產生一個事件。

**如何在管理主控台 (MMC) 中設定掃描具有不受信任憑證的加密連線**

1. 在卡巴斯基安全管理中心管理主控台樹狀目錄中，選取**政策**。
2. 選擇必要的政策並點擊以開啟政策內容。
3. 在政策視窗中，選擇"**一般設定 → 網路設定**"。
4. 在"**加密連線掃描**"塊中，點擊"**進階設定**"按鈕。

5. 在開啟的視窗中，選擇在存取具有不受信任憑證的網域時的應用程式操作模式：**允許** 或者 **封鎖**。

6. 儲存變更。

**如何在網頁主控台 (MMC) 和雲端主控台中設定掃描具有不受信任憑證的加密連線**

1. 在網頁主控台的主視窗中，選擇**資產（裝置）→政策和設定檔**。

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**"塊中，點擊"**設定**"連接。

6. 在開啟的視窗中，選擇在存取具有不受信任憑證的網域時的應用程式操作模式：**允許連線** 或者 **封鎖連線**。

7. 儲存變更。

**如何在應用程式介面中設定掃描具有不受信任憑證的加密連線**

1. 在"應用程式主視窗"中，點擊⚙按鈕。

2. 在應用程式設定視窗中，選取"**一般設定**"→"**網路設定**"。

3. 在**加密連線掃描**塊中，選擇存取具有不受信任憑證的網域時的應用程式操作模式：**允許** 或者 **封鎖**。

4. 儲存變更。




警告存取具有不受信任憑證的網域

# 將卡巴斯基憑證新增到自己的憑證儲存中

瀏覽器和郵件用戶端使用憑證來驗證 Web 資源的安全性和真實性。憑證還提供 Web 資源和使用者之間的資料加密。大多數瀏覽器和郵件用戶端使用受信任的憑證儲存空間（Windows 憑證儲存）。例如，Google Chrome。某些瀏覽器和郵件用戶端預設使用自己的憑證儲存，而不是 Windows 憑證儲存。例如，Firefox 和 Thunderbird。

安裝後，Kaspersky Endpoint Security 會將 Kaspersky 憑證新增到受信任憑證的系統儲存（Windows 憑證儲存）。如果在您的組織中部署了卡巴斯基安全管理中心，並且正在將政策套用於電腦，則 Kaspersky Endpoint Security 會自動啟用在瀏覽器和郵件用戶端中使用 Windows 憑證儲存，以掃描這些應用程式的流量。如果未將政策套用到電腦，則可以選擇瀏覽器和郵件用戶端將使用的憑證儲存。如果您選擇了自己的憑證儲存，請手動將卡巴斯基憑證新增至該儲存。這將有助於在使用 HTTPS 流量時避免錯誤。

若要掃描 Mozilla Firefox 瀏覽器和 Thunderbird 郵件用戶端中的流量，您必須啟用加密連線掃描。如果停用加密連線掃描，則應用程式不會掃描 Mozilla Firefox 瀏覽器和 Thunderbird 郵件用戶端中的流量。加密連線掃描也應被啟用以掃描 MyOffice Mail 和 R7-Office Organizer 郵件用戶端中的流量。

在將憑證新增至瀏覽器或郵件代理程式自己的憑證儲存區之前，請從 Windows 主控台（網際網路屬性）匯出卡巴斯基憑證。有關匯出 Kaspersky 憑證的詳細資訊，請參閱技術支援知識庫。您可以（例如）在 Mozilla 技術支援網站上了解有關將憑證新增到儲存的更多資訊。

您只能在應用程式的本機介面中選擇憑證儲存。

*要選擇憑證儲存來掃描瀏覽器和郵件用戶端中的加密連線，請：*

1. 在“應用程式主視窗”中，點擊⚙按鈕。
2. 在應用程式設定視窗中，選取”**一般設定**“→“**網路設定**”。
3. 在“**加密連線掃描**“塊中，選中“**若要使用其自己的憑證儲存來掃描應用程式中的加密連線，請使用**”核取方塊。
4. 選擇一個憑證儲存：
   - **Windows 憑證儲存(建議)**在安裝 Kaspersky Endpoint Security 期間，會將 Kaspersky 根憑證新增到此儲存中。
   - **自有憑證儲存**Mozilla Firefox 和 Thunderbird 使用它們自己的憑證儲存。如果選擇了 Mozilla 憑證儲存，則需要通過瀏覽器屬性手動將 Kaspersky 根憑證新增到該儲存中。

     MyOffice Mail 和 R7-Office Organizer 郵件用戶端也使用自己的憑證儲存。
5. 儲存變更。

# 從掃描中排除加密連線

大多數網路資源使用加密連線。卡巴斯基專家建議您啟用“加密連線掃描”。如果加密連線掃描會干擾與工作相關的活動，您可以將網站新增到被稱為“*受信任位址*”的排除項目中。在此情況下，當 Web 威脅防護、郵件威脅防護、Web 控制元件執行工作時，Kaspersky Endpoint Security 不掃描受信任網址的 HTTPS 流量。

如果受信任應用程式使用加密連線，您可以對此應用程式停用加密連線掃描。例如，您可以對使用自己的憑證執行雙因素身分驗證的雲端儲存應用程式停用加密連線掃描。

**如何從管理主控台 (MMC) 中的加密連線掃描中排除網址**

1. 在卡巴斯基安全管理中心管理主控台樹狀目錄中，選取**政策**。
2. 選擇必要的政策並點擊以開啟政策內容。
3. 在政策視窗中，選擇“**一般設定 → 網路設定**”。

4. 在"**加密連線掃描**"塊中，點擊"**設定受信任位址**"按鈕。

5. 點擊"**新增**"。

6. 如果您不希望 Kaspersky Endpoint Security 掃描在存取該網域時建立的加密連線，請輸入該網域名稱或 IP 位址。

   Kaspersky Endpoint Security 支援`*`字元用於在網域名稱中輸入遮罩。

   > Kaspersky Endpoint Security 不支援 IP 位址的`*`符號。您可以使用子網路遮罩（例如，198.51.100.0/24）選擇一個 IP 位址範圍。

   例如：

   - `domain.com` – 該記錄包括以下位址：`https://domain.com`，`https://www.domain.com`，`https://domain.com/page123`。該記錄排除子網域（例如，`subdomain.domain.com`）。
   - `subdomain.domain.com` – 該記錄包括以下位址：`https://subdomain.domain.com`，`https://subdomain.domain.com/page123`。該記錄排除 `domain.com` 子網域。
   - `*.domain.com` – 該記錄包括以下位址：`https://movies.domain.com`，`https://images.domain.com/page123`。該記錄排除 `domain.com` 子網域。

7. 儲存變更。

**如何從網頁主控台和 Cloud Console 中的加密連線掃描中排除網址**

1. 在網頁主控台的主視窗中，選擇**資產（裝置）→政策和設定檔**。

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**"塊中，點擊"**受信任網域**"按鈕。

6. 點擊"**新增**"。

7. 如果您不希望 Kaspersky Endpoint Security 掃描在存取該網域時建立的加密連線，請輸入該網域名稱或 IP 位址。

   Kaspersky Endpoint Security 支援`*`字元用於在網域名稱中輸入遮罩。

   > Kaspersky Endpoint Security 不支援 IP 位址的`*`符號。您可以使用子網路遮罩（例如，198.51.100.0/24）選擇一個 IP 位址範圍。

例如：

- `domain.com` – 該記錄包括以下位址：`https://domain.com`，`https://www.domain.com`，`https://domain.com/page123`。該記錄排除子網域（例如，`subdomain.domain.com`）。
- `subdomain.domain.com` – 該記錄包括以下位址：`https://subdomain.domain.com`，`https://subdomain.domain.com/page123`。該記錄排除 `domain.com` 子網域。
- `*.domain.com` – 該記錄包括以下位址：`https://movies.domain.com`，`https://images.domain.com/page123`。該記錄排除 `domain.com` 子網域。

8. 儲存變更。

**如何從應用程式介面中的加密連線掃描中排除網址**

1. 在“應用程式主視窗”中，點擊⚙按鈕。
2. 在應用程式設定視窗中，選取”**一般設定**“→“**網路設定**”。




應用程式網路設定

3. 在”**加密連線掃描**”塊中，點擊”**設定受信任位址**”按鈕。
4. 點擊“**新增**”。
5. 如果您不希望 Kaspersky Endpoint Security 掃描在存取該網域時建立的加密連線，請輸入該網域名稱或 IP 位址。

   Kaspersky Endpoint Security 支援`*`字元用於在網域名稱中輸入遮罩。

Kaspersky Endpoint Security 不支援 IP 位址的 * 符號。您可以使用子網路遮罩（例如，198.51.100.0/24）選擇一個 IP 位址範圍。

例如：

- domain.com – 該記錄包括以下位址：https://domain.com，https://www.domain.com，https://domain.com/page123。該記錄排除子網域（例如，subdomain.domain.com）。
- subdomain.domain.com – 該記錄包括以下位址：https://subdomain.domain.com，https://subdomain.domain.com/page123。該記錄排除 domain.com 子網域。
- *.domain.com – 該記錄包括以下位址：https://movies.domain.com，https://images.domain.com/page123。該記錄排除 domain.com 子網域。

6. 儲存變更。

預設情況下，當發生錯誤時，Kaspersky Endpoint Security 將不掃描加密連線，並將該網站新增到專門設定的"*有掃描錯誤的網域*"清單中。Kaspersky Endpoint Security 會為每個使用者編制單獨的清單，並且不會將資料傳送到卡巴斯基安全管理中心。您可以啟用當發生掃描錯誤時封鎖連線。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。

*要檢視有掃描錯誤的網域清單：*

1. 在"應用程式主視窗"中，點擊⚙按鈕。
2. 在應用程式設定視窗中，選取"**一般設定**"→"**網路設定**"。
3. 在"**加密連線掃描**"塊中，點擊"**有掃描錯誤的網域**"按鈕。

將開啟有掃描錯誤的網域清單。要重設該清單，請在政策中啟用當發生掃描錯誤時封鎖連線、套用政策，然後將參數重設為其初始值，並再次套用政策。

卡巴斯基專家會列出一系列*全域例外情況*，無論應用程式設定如何，Kaspersky Endpoint Security 都不會檢查這些受信任網站。

*要檢視加密流量掃描的全域排除項目：*

1. 在"應用程式主視窗"中，點擊⚙按鈕。
2. 在應用程式設定視窗中，選取"**一般設定**"→"**網路設定**"。
3. 在"**加密連線掃描**"塊中，點擊受信任網站連結清單。

這將開啟由卡巴斯基專家編譯的網站清單。Kaspersky Endpoint Security 不會掃描清單中網站的受防護連線。當更新 Kaspersky Endpoint Security 資料庫和模組時，該清單可能也更新。

# 抹除資料

Kaspersky Endpoint Security 允許您使用工作來遠端刪除使用者電腦中的資料。

Kaspersky Endpoint Security 刪除資料的方式如下：

- 在靜默模式下；
- 在硬碟和卸除式磁碟機上；
- 對於電腦上的所有使用者帳戶。

即使產品授權到期後，Kaspersky Endpoint Security 也會執行“*抹除資料*”工作，無論使用哪種產品授權類型。

### “資料抹除”模式

透過該工作可在以下模式中刪除資料：

- 立即刪除資料。

  例如，您可以在此模式下刪除過期資料以釋放磁碟空間。

- 延遲刪除資料。

  例如，此模式可用於防護筆記型電腦上的資料，以防其遺失或被竊。您可以配置成當筆記型電腦超出公司網路邊界並且長時間未與卡巴斯基安全管理中心同步時自動刪除資料。

無法在工作內容中設定刪除資料的排程。您只能在手動啟動工作後立即刪除資料，或者配置延遲的資料刪除（如果未與卡巴斯基安全管理中心連線）。

### 限制

資料抹除具有以下限制：

- 只有卡巴斯基安全管理中心管理員可以管理“*抹除資料*”工作。您無法在 Kaspersky Endpoint Security 的本機介面中配置或啟動工作。
- 對於 NTFS 檔案系統，Kaspersky Endpoint Security 僅刪除主資料流的名稱。交換資料流名稱不能刪除。
- 刪除符號連結檔案時，Kaspersky Endpoint Security 還會刪除在符號連結中指定了路徑的檔案。

### 建立抹除資料工作

*要刪除使用者電腦上的資料：*

1. 在網頁主控台的主視窗中，選擇**資產（裝置）→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 Windows 12.12.0**”。

   b. 在“**工作類型**”下拉式清單中，選取“**抹除資料**”。

   c. 在“**工作名稱**”欄位中，輸入簡要說明，例如“*抹除資料（竊盜防護）*”。

   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。前往下一步。

   如果將新電腦新增到工作範圍內的管理群組，則只有在新增新電腦後的 5 分鐘內完成工作，才會在新電腦上執行立即刪除資料工作。

5. 結束精靈。

   在工作清單中將顯示一個新工作。

6. 點擊 Kaspersky Endpoint Security 的“**抹除資料**”工作。

   工作內容視窗將開啟。

7. 選擇“**應用程式設定**”標籤。

8. 選擇資料刪除方法：：

   - **透過作業系統刪除**Kaspersky Endpoint Security 使用作業系統資源刪除檔案，而不將檔案傳送到回收筒。
   - **完全刪除，無法還原**Kaspersky Endpoint Security 使用隨機資料覆寫檔案。刪除資料後，幾乎不可能還原資料。

9. 如果要延遲刪除資料，請選中“**與卡巴斯基安全管理中心無連線超過以下時間時自動抹除資料 N 天**”核取方塊。定義天數。

   每次在定義的時間段內與卡巴斯基安全管理中心無連線時，將執行延遲刪除資料工作。

   配置延遲資料刪除時，請記住員工可能有不同的工作排程。還要考慮離線使用者的工作排程。有關使用離線電腦以及與漫遊使用者一起工作的詳細資訊，請參閱卡巴斯基安全管理中心說明。

   如果電腦關閉且連線中斷的時間超過配置的持續時間，則電腦啟動後，Kaspersky Endpoint Security 不會立即刪除資料。應用程式會等待與卡巴斯基安全管理中心同步一小時。這對於防止未經授權刪除關閉了電腦的使用者（例如，在外出度假前）的電腦上的資料很有必要。

   如果清除該核取方塊，則在與卡巴斯基安全管理中心同步後將立即執行該工作。

10. 建立要刪除的物件清單：

    - **資料夾**Kaspersky Endpoint Security 會刪除資料夾及其子資料夾中的所有檔案。Kaspersky Endpoint Security 不支援用來輸入資料夾路徑的遮罩和環境變數。
    - **根據副檔名選取檔案**Kaspersky Endpoint Security 將搜尋所有電腦磁碟機（包括卸除式磁碟機）中具有指定副檔名的檔案。使用“`;`”或“`,`”字元可指定多個副檔名。
    - **預定義範圍**Kaspersky Endpoint Security 將從以下區域刪除檔案：
        - **文件**作業系統的“*檔案*”資料夾及其子資料夾中的檔案。
        - **Cookies**瀏覽器在其中儲存使用者存取過的網站的資料（如使用者授權資料）的檔案。
        - **桌面**作業系統的“*桌面*”資料夾及其子資料夾中的檔案。
        - **暫時 Internet Explorer 檔案**與 Internet Explorer 操作有關的暫存檔案，如網頁副本、映像和媒體檔案。
        - **暫存檔**與電腦上安裝的應用程式的操作有關的暫存檔案。例如，Microsoft Office 應用程式會建立包含文件備份副本的暫存檔案。
        - **Outlook 檔案**與 Outlook 郵件用戶端操作有關的檔案：資料檔案 (PST)、離線資料檔案 (OST)、離線通訊錄檔案 (OAB) 和個人通訊錄檔案 (PAB)。
        - **使用者設定檔**儲存本機使用者帳戶的作業系統設定的檔案和資料夾集。

    您可以在每個標籤上建立要刪除的物件清單。Kaspersky Endpoint Security 將建立一個綜合清單，並在工作完成後刪除此清單中的檔案。

    > 您無法刪除 Kaspersky Endpoint Security 執行所需的檔案。

11. 儲存變更。

12. 選中該工作旁邊的核取方塊。

13. 點擊“**開始**”。

    結果，將根據所選模式刪除使用者電腦上的資料：立即刪除或無連線時刪除。如果 Kaspersky Endpoint Security 無法刪除檔案，例如使用者當前正在使用檔案時，應用程式不會嘗試再次刪除該檔案。要完成資料刪除，請再次執行該工作。

# 電腦控制

## Web 控制

“Web 控制”管理使用者對 Web 資源的存取。這有助於減少流量和工作時間的不當使用。當使用者嘗試開啟受“Web 控制”限制的網站時，Kaspersky Endpoint Security 將封鎖存取或顯示警告（請參見下圖）。

若要使用 Web Control，您必須完成應用程式的初始設定：

- 對於 HTTPS 流量監控， 啟用加密連線掃描 （預設為啟用）。
- 選擇 Kaspersky Endpoint Security 必須監控的連接埠（預設情況下，應用程式監控所有連接埠）。
- 選擇您希望 Kaspersky Endpoint Security 監控其流量的應用程式。大多數瀏覽器已出現在卡巴斯基推薦的應用程式清單中。如果清單中缺少您的瀏覽器，請手動新增。
- 我們建議 將網頁交互指令碼注入到 Web 流量中 （預設情況下，指令碼注入被停用）。此指令碼可啟用為應用程式事件日誌、OS 事件日誌和報告註冊 Web 控制事件。

### 管理對網站的存取的方法

“Web 控制”允許您使用以下方法配置對網站的存取：

- **網站類別**。網站按照卡巴斯基安全網路雲端服務、啟發式分析和已知網站資料庫（包含在應用程式資料庫中）進行分類。例如，您可以限制使用者存取“*社群網路*”類別或“其它類別”。
- **資料類型**。例如，您可以限制使用者存取網站上的資料，並隱藏影像。Kaspersky Endpoint Security 根據檔案格式確定資料類型，而不是基於其副檔名。

  Kaspersky Endpoint Security 不掃描壓縮檔案內的檔案。例如，如果影像檔案放在壓縮檔案中，Kaspersky Endpoint Security 會辨識“*壓縮檔案*”資料類型而不是“*圖形*”。

- **單個位址**。您可以輸入網址或使用遮罩。

可以同時使用多種方法來管理對網站的存取。例如，您可以僅針對“*網頁式電子郵件*”網站類別限制對“*Office 應用程式檔案*”資料類型的存取。

### 網站存取規則

“Web 控制”透過使用*存取規則*管理使用者對網站的存取。您可以為網站存取規則配置以下進階設定：

- 規則適用的使用者。

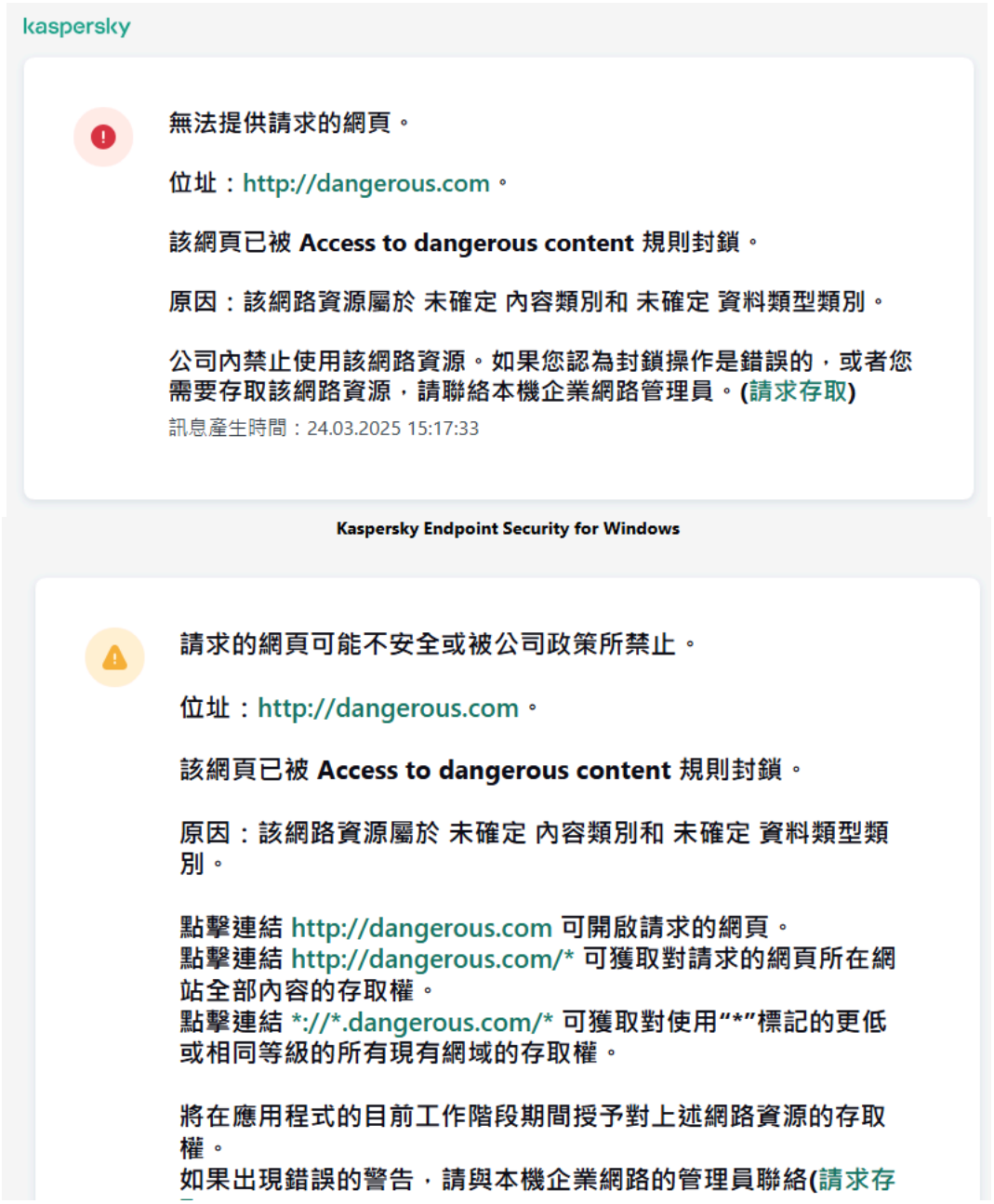
  例如，您可以限制公司內除 IT 部門以外的所有使用者透過瀏覽器存取網際網路。

- 規則排程。

  例如，您可以限制只能在工作時間透過瀏覽器存取網際網路。

## 存取規則優先順序

每條規則都有優先順序。規則在清單中的位置越高，優先順序越高。如果某個網站已新增到多條規則，“Web 控制”會基於優先順序最高的規則來管理對該網站的存取。例如，Kaspersky Endpoint Security 可能將公司入口辨識為社群網路。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。公司 Web 入口存取規則的優先順序必須高於社群網路存取規則的優先順序。




“Web 控制”訊息

# 新增網路資源存取規則

*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。

不建議建立超過 1000 條的 Web 資源存取規則，因為這可能導致系統變得不穩定。

網路資源存取規則是使用者在規則排程中指明的時間範圍內存取規則中描述的網頁資源時，Kaspersky Endpoint Security 執行的一組篩選和操作。透過篩選，您可以精確指定由 Web 控制元件控制其存取權限的網頁資源集區。

系統提供以下篩選功能選項：

- **按內容篩選**。Web 控制將按照內容和資料類型分類網頁資源。對於內容和資料屬於按這些類別定義的類型的網頁資源，您可以控制使用者對它們的存取權限。使用者存取屬於選取內容類別和/或資料類型類別的網頁資源時，Kaspersky Endpoint Security 會執行規則中指定的操作。

- **按網頁資源位址篩選**。您可以控制使用者對所有網頁資源位址或單個網頁資源位址和/或網頁資源位址群組的存取權限。

  如果指定按內容篩選和按網頁資源位址篩選，而指定的網頁資源位址和/或網頁資源位址群組屬於選取的內容類別或資料類型類別，Kaspersky Endpoint Security 不會控制對選取內容類別和/或資料類型類別中所有網頁資源的存取權限。相反，應用程式僅控制對指定網頁資源位址和/或網頁資源位址群組的存取權限。

- **按名稱篩選**。您可以指定可存取根據規則控制的網頁資源使用者和/或使用者群組的名稱。

- **規則排程**。您可以指定下列規則排程。規則排程為 Kaspersky Endpoint Security 監控對該規則涵蓋網路資源的存取時間範圍。

安裝 Kaspersky Endpoint Security 後，Web 控制元件的規則清單將不為空。*預設規則* 已預設。此規則套用於未被其他規則覆寫的任何 Web 資源，並允許或封鎖所有使用者存取這些 Web 資源。

每條規則都有優先順序。規則在清單中的位置越高，優先順序越高。如果某個網站已新增到多條規則，"Web 控制"會基於優先順序最高的規則來管理對該網站的存取。例如，Kaspersky Endpoint Security 可能將公司入口辨識為社群網路。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。公司 Web 入口存取規則的優先順序必須高於社群網路存取規則的優先順序。

### 如何在管理主控台 (MMC) 中新增網頁資源存取規則

1. 在卡巴斯基安全管理中心管理主控台樹狀目錄中，選取**政策**。
2. 選擇必要的政策並點擊以開啟政策內容。
3. 在政策視窗中，選擇"**安全控制 → Web 控制**"。
4. 選擇"**Web 控制**"核取方塊。
5. 在"**Web 控制設定**"塊中，點擊"**新增**"按鈕。

   開啟"**網路資源存取規則**"視窗。
6. 設定網路資源存取規則（請見下表）。

7. 如果您希望 Web 控制在應用程式政策後立即終止與禁止的 Web 資源的連接，請選擇 **套用規則後終止活動的使用者瀏覽器工作階段** 核取方塊。

   Web 控制僅允許在 Web 瀏覽器中立即中斷 Web 資源。對於其他應用程式，Web 控制僅限制新連線。

   如果清除該核取方塊，Web 控制將僅限制與禁止的 Web 資源的新連線。Web 控制不會終止活動連線。

8. 儲存變更。

**如何在網頁主控台和雲端主控台中新增網頁資源存取規則**

1. 在網頁主控台的主視窗中，選擇**資產（裝置）→ 政策和設定檔**。
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. 開啟“**Web 控制已啟用**“開關。
6. 在”**規則清單**”塊中，點擊”**新增**”按鈕。
7. 設定網路資源存取規則（請見下表）。
8. 如果您希望 Web 控制在應用程式政策後立即終止與禁止的 Web 資源的連接，請選擇 **套用規則後終止活動的使用者瀏覽器工作階段** 核取方塊。

   Web 控制僅允許在 Web 瀏覽器中立即中斷 Web 資源。對於其他應用程式，Web 控制僅限制新連線。

   如果清除該核取方塊，Web 控制將僅限制與禁止的 Web 資源的新連線。Web 控制不會終止活動連線。

9. 儲存變更。

**如何在應用程式介面中新增網頁資源存取規則**

1. 在“應用程式主視窗”中，點擊⚙按鈕。
2. 在應用程式設定視窗中，選取”**安全控制**“→“**Web 控制**”。




Web 控制設定

3. 開啟“**Web 控制**“開關。
4. 在”**設定**”塊中，點擊”**網路資源存取規則**”按鈕。
5. 在開啟的視窗中，點擊“**新增**”按鈕。

   開啟“**網路資源存取規則**”視窗。
6. 設定網路資源存取規則（請見下表）。
7. 如果您希望 Web 控制在應用程式政策後立即終止與禁止的 Web 資源的連接，請選擇 **套用規則後終止活動的使用者瀏覽器工作階段** 核取方塊。

   Web 控制僅允許在 Web 瀏覽器中立即中斷 Web 資源。對於其他應用程式，Web 控制僅限制新連線。

   如果清除該核取方塊，Web 控制將僅限制與禁止的 Web 資源的新連線。Web 控制不會終止活動連線。
8. 儲存變更。

結果，新的 Web 控制規則被新增到清單。必要的話，請變更 Web 控制規則的優先順序。您也可以使用切換開關隨時停用網頁資源存取規則而無需將其從清單中移除。

| 參數 | 描述 |
| --- | --- |
| **規則名稱** | Web 控制規則的名稱。 |
| **狀況** | • **開**<br>• **關**<br>您可以隨時使用開關停用網路資源存取規則。 |
| **操作** | • **允許**Web 控制可允許存取比對規則參數的網頁資源。<br>• **封鎖**Web 控制可封鎖存取比對規則參數的網頁資源並顯示網站存取被拒絕的訊息。<br>• **警告**當使用者嘗試存取比對規則的網頁資源時，Web 控制會顯示警告，不建議造訪該網頁資源。透過警告訊息連結，使用者可獲取對所請求的網路資源的存取權限。 |
| **篩選內容** | • **根據內容類別**您可以按"類別"（例如，"*社群網路*"類別）控制使用者對網路資源的存取。<br>• **根據資料類型**您可以根據發布的資料的特定資料類型（例如，*圖形*）來控制使用者對網路資源的存取。 |
| **位址** | • **套用於所有位址**Web 控制不會按位址篩選網路資源。<br>• **套用於單個位址**Web 控制將僅篩選清單中的網路資源位址。您可以輸入網址或使用遮罩。您還可以從 TXT 檔案匯出網路資源位址清單。您可以在 Active Directory 中、在卡巴斯基安全管理中心的账户清單中或透過手動輸入本機使用者名稱來選擇使用者。卡巴斯基建議僅在無法使用網域使用者帳戶的特殊情況下使用本機使用者帳戶。<br>如果停用加密連線掃描，則對於 HTTPS 協定只能按伺服器名稱篩選。 |
| **使用者** | • **所有使用者**Web 控制不會為特定使用者篩選網路資源。<br>• **個人使用者和/或使用者群組**Web 控制將僅針對特定使用者篩選網路資源。您可以在 Active Directory 中、在卡巴斯基安全管理中心的账户清單中或透過手動輸入本機使用者名稱來選擇使用者。卡巴斯基建議僅在無法使用網域使用者帳戶的特殊情況下使用本機使用者帳戶。 |
| **規則排程** | 規則排程為 Kaspersky Endpoint Security 監控對該規則涵蓋網路資源的存取時間範圍。例如，您可以限制只能在工作時間透過瀏覽器存取網際網路。 |

# 按網頁資源位址篩選

若要控制對單個網頁資源的存取，您必須建立一個 Web 控制規則，建立一個網址清單，並選擇一個 Web 控制動作。當建立網址清單時，您可以輸入 URL 位址或使用遮罩。

規則可包括規則排程和一個規則對其套用的使用者的清單。例如，您可以僅在工作時間內限制對網站的存取，或允許某群組中的使用者造訪網站。

### 如何在管理主控台 (MMC) 中啟用網頁資源篩選器

1. 在卡巴斯基安全管理中心管理主控台樹狀目錄中，選取**政策**。
2. 選擇必要的政策並點擊以開啟政策內容。
3. 在政策視窗中，選擇"**安全控制 → Web 控制**"。
4. 選擇"**Web 控制**"核取方塊。
5. 在"**Web 控制設定**"塊中，點擊"**新增**"按鈕。
   開啟"**網路資源存取規則**"視窗。
6. 設定網路資源存取規則：
   a. 在"**名稱**"欄位中輸入規則的名稱。
   b. 在"**套用於位址**"下拉式清單中，選取"**套用於單個位址**"。

c. 建立網頁資源位址清單。您可以輸入網址或使用遮罩。您還可以從 TXT 檔案匯出網路資源位址清單。

> 如果停用加密連線掃描，則對於 HTTPS 協定只能按伺服器名稱篩選。

d. 在**"套用於使用者"**下拉清單中，為使用者選取相關篩選器：

- **所有使用者**Web 控制不會按位址篩選網路資源。
- **所有個人使用者或使用者群組**Web 控制將僅篩選清單中的網路資源位址。您可以輸入網址或使用遮罩。您還可以從 TXT 檔案匯出網路資源位址清單。您可以在 Active Directory 中、在卡巴斯基安全管理中心的账户清單中或透過手動輸入本機使用者名稱來選擇使用者。卡巴斯基建議僅在無法使用網域使用者帳戶的特殊情況下使用本機使用者帳戶。

e. 在**"動作"**下拉式清單中，選取一個選項：

- **允許**Web 控制可允許存取比對規則參數的網頁資源。
- **封鎖**Web 控制可封鎖存取比對規則參數的網頁資源並顯示網站存取被拒絕的訊息。
- **警告**當使用者嘗試存取比對規則的網頁資源時，Web 控制會顯示警告，不建議造訪該網頁資源。透過警告訊息連結，使用者可獲取對所請求的網路資源的存取權限。

f. 在**規則排程**下拉式清單中，選取一個排程或建立一個新排程。

7. 如果您希望 Web 控制在應用程式政策後立即終止與禁止的 Web 資源的連接，請選擇 **套用規則後終止活動的使用者瀏覽器工作階段** 核取方塊。

> Web 控制僅允許在 Web 瀏覽器中立即中斷 Web 資源。對於其他應用程式，Web 控制僅限制新連線。

如果清除該核取方塊，Web 控制將僅限制與禁止的 Web 資源的新連線。Web 控制不會終止活動連線。

8. 儲存變更。

**如何透過網頁主控台和雲端主控台啟用網頁資源位址篩選器**

1. 在網頁主控台的主視窗中，選擇**資產（裝置）→政策和設定檔**。
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. 開啟**"Web 控制已啟用"**開關。
6. 在**"規則清單"**塊中，點擊**"新增"**按鈕。

7. 設定網路資源存取規則：

   a. 在**"規則名稱"**欄位中輸入規則的名稱。

   b. 選擇網路資源存取規則的**"已啟用"**狀態。

   您可以使用切換開關隨時停用網頁資源存取規則而無需將其從清單中移除。

   c. 在**"操作"**塊，選取相關選項：

   - **允許**Web 控制可允許存取比對規則參數的網頁資源。
   - **封鎖**Web 控制可封鎖存取比對規則參數的網頁資源並顯示網站存取被拒絕的訊息。
   - **通知**當使用者嘗試存取比對規則的網頁資源時，Web 控制會顯示警告，不建議造訪該網頁資源。透過警告訊息連結，使用者可獲取對所請求的網路資源的存取權限。

   d. 在**範圍**下面，選擇**單個網站**。

   e. 配置內容篩選器：

   - **單個位址**建立網頁資源位址清單。您可以輸入網址或使用遮罩。您還可以從 TXT 檔案匯出網路資源位址清單。

     如果停用加密連線掃描，則對於 HTTPS 協定只能按伺服器名稱篩選。

   - **資料類型**您可以根據發布的資料的特定資料類型（例如，*圖形*）來控制使用者對網路資源的存取。

   f. 在**使用者或群組**下面，選擇要將規則套用至 Web Control 的使用者。

   Web 控制將僅篩選清單中的網路資源位址。您可以輸入網址或使用遮罩。您還可以從 TXT 檔案匯出網路資源位址清單。您可以在 Active Directory 中、在卡巴斯基安全管理中心的账户清單中或透過手動輸入本機使用者名稱來選擇使用者。卡巴斯基建議僅在無法使用網域使用者帳戶的特殊情況下使用本機使用者帳戶。

   g. 在**存取排程**區塊中，選取一個排程或建立一個新排程。

8. 儲存變更。

### 如何在應用程式介面中啟用網頁資源位址篩選器

1. 在“應用程式主視窗”中，點擊⚙按鈕。
2. 在應用程式設定視窗中，選取”**安全控制**“→“**Web 控制**”。




Web 控制設定

3. 在”**設定**”塊中，點擊”**網路資源存取規則**”按鈕。
4. 在開啟的視窗中，點擊“**新增**”按鈕。
   開啟“**網路資源存取規則**”視窗。
5. 在“**規則名稱**”欄位中輸入規則的名稱。
6. 選擇網路資源存取規則的“**開**“狀態。
   您可以隨時使用開關停用網路資源存取規則。
7. 在“**操作**”塊，選取相關選項：
   - **允許**Web 控制可允許存取比對規則參數的網頁資源。
   - **封鎖**Web 控制可封鎖存取比對規則參數的網頁資源並顯示網站存取被拒絕的訊息。
   - **警告**當使用者嘗試存取比對規則的網頁資源時，Web 控制會顯示警告，不建議造訪該網頁資源。透過警告訊息連結，使用者可獲取對所請求的網路資源的存取權限。
8. 在**位址**下面，選擇**套用於單個位址**。
   建立網頁資源位址清單。您可以輸入網址或使用遮罩。您還可以從 TXT 檔案匯出網路資源位址清單。

如果停用加密連線掃描，則對於 HTTPS 協定只能按伺服器名稱篩選。

9. 在“**使用者**“塊中，為使用者選擇相關的過濾器：

   - **所有使用者**Web 控制不會為特定使用者篩選網路資源。
   - **個人使用者和/或使用者群組**Web 控制將僅篩選清單中的網路資源位址。您可以輸入網址或使用遮罩。您還可以從 TXT 檔案匯出網路資源位址清單。您可以在 Active Directory 中、在卡巴斯基安全管理中心的账户清單中或透過手動輸入本機使用者名稱來選擇使用者。卡巴斯基建議僅在無法使用網域使用者帳戶的特殊情況下使用本機使用者帳戶。

10. 在**規則排程**下拉式清單中，選取一個排程或建立一個新排程。

11. 如果您希望 Web 控制在應用程式政策後立即終止與禁止的 Web 資源的連接，請選擇 **套用規則後終止活動的使用者瀏覽器工作階段** 核取方塊。

    Web 控制僅允許在 Web 瀏覽器中立即中斷 Web 資源。對於其他應用程式，Web 控制僅限制新連線。

    如果清除該核取方塊，Web 控制將僅限制與禁止的 Web 資源的新連線。Web 控制不會終止活動連線。

12. 儲存變更。

結果，新的 Web 控制規則被新增到清單。必要的話，請變更 Web 控制規則的優先順序。您也可以使用切換開關隨時停用網頁資源存取規則而無需將其從清單中移除。

# 按網頁資源內容篩選

為了控制網頁資源內容的存取，Web 控制提供了類別篩選器和資料類型篩選器。

網站按照卡巴斯基安全網路雲端服務、啟發式分析和已知網站資料庫（包含在應用程式資料庫中）進行分類。例如，您可以限制使用者存取“*社群網路*”類別或“其它類別”。

例如，您可以根據資料類型限制使用者對網站的存取以隱藏映像。Kaspersky Endpoint Security 根據檔案格式確定資料類型，而不是基於其副檔名。Web 控制可區分以下資料類型：

- 視訊
- 音訊
- Office 應用程式檔案
- 可執行檔
- 壓縮檔案

- 圖形
- 日本。

Kaspersky Endpoint Security 不掃描壓縮檔案內的檔案。例如，如果影像檔案放在壓縮檔案中，Kaspersky Endpoint Security 會辨識“*壓縮檔案*”資料類型而不是“*圖形*”。

規則可包括規則排程和一個規則對其套用的使用者的清單。例如，您可以僅在工作時間內限制對網站的存取，或允許某群組中的使用者造訪網站。

**如何在管理主控台 (MMC) 中啟用網頁資源內容篩選器**

1. 在卡巴斯基安全管理中心管理主控台樹狀目錄中，選取**政策**。
2. 選擇必要的政策並點擊以開啟政策內容。
3. 在政策視窗中，選擇“**安全控制 → Web 控制**”。
4. 選擇“**Web 控制**”核取方塊。
5. 在”**Web 控制設定**”塊中，點擊”**新增**”按鈕。
   開啟“**網路資源存取規則**”視窗。
6. 設定網路資源存取規則：
   a. 在“**名稱**”欄位中輸入規則的名稱。
   b. 在“**篩選內容**”下拉清單中，選取相關內容篩選器：
      - **根據內容類別**您可以按“類別”（例如，“*社群網路*”類別）控制使用者對網路資源的存取。
      - **根據資料類型**您可以根據發布的資料的特定資料類型（例如，*圖形*）來控制使用者對網路資源的存取。
      - **根據內容類別和資料類型**按內容類別和資料類型篩選已啟用。

      選擇篩選器後，設定篩選器參數。
   c. 在“**套用於使用者**”下拉清單中，為使用者選取相關篩選器：
      - **所有使用者**Web 控制不會按位址篩選網路資源。
      - **所有個人使用者或使用者群組**Web 控制將僅篩選清單中的網路資源位址。您可以輸入網址或使用遮罩。您還可以從 TXT 檔案匯出網路資源位址清單。您可以在 Active Directory 中、在卡巴斯基安全管理中心的账户清單中或透過手動輸入本機使用者名稱來選擇使用者。卡巴斯基建議僅在無法使用網域使用者帳戶的特殊情況下使用本機使用者帳戶。

d. 在**"動作"**下拉式清單中，選取一個選項：

- **允許**Web 控制可允許存取比對規則參數的網頁資源。
- **封鎖**Web 控制可封鎖存取比對規則參數的網頁資源並顯示網站存取被拒絕的訊息。
- **警告**當使用者嘗試存取比對規則的網頁資源時，Web 控制會顯示警告，不建議造訪該網頁資源。透過警告訊息連結，使用者可獲取對所請求的網路資源的存取權限。

e. 在**規則排程**下拉式清單中，選取一個排程或建立一個新排程。

7. 如果您希望 Web 控制在應用程式政策後立即終止與禁止的 Web 資源的連接，請選擇 **套用規則後終止活動的使用者瀏覽器工作階段** 核取方塊。

> Web 控制僅允許在 Web 瀏覽器中立即中斷 Web 資源。對於其他應用程式，Web 控制僅限制新連線。

如果清除該核取方塊，Web 控制將僅限制與禁止的 Web 資源的新連線。Web 控制不會終止活動連線。

8. 儲存變更。

**如何透過網頁主控台和雲端主控台啟用網頁資源內容篩選器**

1. 在網頁主控台的主視窗中，選擇**資產（裝置）→政策和設定檔**。
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. 開啟**"Web 控制已啟用"**開關。
6. 在**"規則清單"**塊中，點擊**"新增"**按鈕。
7. 設定網路資源存取規則：

a. 在**"規則名稱"**欄位中輸入規則的名稱。

b. 選擇網路資源存取規則的**"已啟用"**狀態。
   您可以隨時使用開關停用網路資源存取規則。

c. 在**"操作"**塊，選取相關選項：

- **允許**Web 控制可允許存取比對規則參數的網頁資源。
- **封鎖**Web 控制可封鎖存取比對規則參數的網頁資源並顯示網站存取被拒絕的訊息。
- **通知**當使用者嘗試存取比對規則的網頁資源時，Web 控制會顯示警告，不建議造訪該網頁資源。透過警告訊息連結，使用者可獲取對所請求的網路資源的存取權限。

d. 在**範圍**下面，選擇**內容類別**。

e. 配置內容篩選器：

- **內容類別**您可以按“類別”（例如，“*社群網路*”類別）控制使用者對網路資源的存取。
- **資料類型**您可以根據發布的資料的特定資料類型（例如，*圖形*）來控制使用者對網路資源的存取。

f. 在**使用者或群組**下面，選擇要將規則套用至 Web Control 的使用者。

Web 控制將僅篩選清單中的網路資源位址。您可以輸入網址或使用遮罩。您還可以從 TXT 檔案匯出網路資源位址清單。您可以在 Active Directory 中、在卡巴斯基安全管理中心的账户清單中或透過手動輸入本機使用者名稱來選擇使用者。卡巴斯基建議僅在無法使用網域使用者帳戶的特殊情況下使用本機使用者帳戶。

g. 在**存取排程**區塊中，選取一個排程或建立一個新排程。

8. 儲存變更。

### 如何在應用程式介面中啟用網頁資源內容篩選器

1. 在“應用程式主視窗”中，點擊⚙按鈕。
2. 在應用程式設定視窗中，選取”**安全控制**“→“**Web 控制**”。




Web 控制設定

3. 在”**設定**”塊中，點擊”**網路資源存取規則**”按鈕。
4. 在開啟的視窗中，點擊“**新增**”按鈕。

開啟“**網路資源存取規則**”視窗。

5. 在“**規則名稱**”欄位中輸入規則的名稱。

6. 選擇網路資源存取規則的“**開**“狀態。

   您可以隨時使用開關停用網路資源存取規則。

7. 在“**操作**”塊，選取相關選項：

   - **允許**Web 控制可允許存取比對規則參數的網頁資源。
   - **封鎖**Web 控制可封鎖存取比對規則參數的網頁資源並顯示網站存取被拒絕的訊息。
   - **警告**當使用者嘗試存取比對規則的網頁資源時，Web 控制會顯示警告，不建議造訪該網頁資源。透過警告訊息連結，使用者可獲取對所請求的網路資源的存取權限。

8. 在“**篩選內容**“塊中，選擇相關的內容篩選器：

   - **根據內容類別**您可以按“類別”（例如，“*社群網路*”類別）控制使用者對網路資源的存取。
   - **根據資料類型**您可以根據發布的資料的特定資料類型（例如，*圖形*）來控制使用者對網路資源的存取。

   要配置內容篩選器，請：

   a. 點擊”**設定**”連接。

   b. 選取所需內容類別和/或資料類型名稱旁邊的核取方塊。

   選取某個內容類別和/或資料類型類別旁的核取方塊則表示 Kaspersky Endpoint Security 將套用規則以控制對屬於選取的內容類別和/或資料類型類別的網路資源存取。

   c. 返回用於配置網路資源存取規則的視窗。

9. 在“**使用者**“塊中，為使用者選擇相關的過濾器：

   - **所有使用者**Web 控制不會按位址篩選網路資源。
   - **個人使用者和/或使用者群組**Web 控制將僅篩選清單中的網路資源位址。您可以輸入網址或使用遮罩。您還可以從 TXT 檔案匯出網路資源位址清單。您可以在 Active Directory 中、在卡巴斯基安全管理中心的账户清單中或透過手動輸入本機使用者名稱來選擇使用者。卡巴斯基建議僅在無法使用網域使用者帳戶的特殊情況下使用本機使用者帳戶。要建立要對其套用規則的使用者清單：

     a. 點擊“**新增**”。

     b. 在開啟的視窗中，選擇要對其套用網路資源存取規則的使用者或使用者群組。

     c. 返回用於配置網路資源存取規則的視窗。

10. 在“**規則排程**”下拉清單中，選取所需排程的名稱，或根據選取的規則排程產生新排程。為此，請執行以下操作：

    a. 點擊“**編輯或新增**”。

    b. 在開啟的視窗中，點擊“**新增**”按鈕。

    c. 在開啟的視窗中，輸入規則排程名稱。

    d. 配置使用者的網路資源存取排程。

    e. 返回用於配置網路資源存取規則的視窗。

11. 如果您希望 Web 控制在應用程式政策後立即終止與禁止的 Web 資源的連接，請選擇 **套用規則後終止活動的使用者瀏覽器工作階段** 核取方塊。

    Web 控制僅允許在 Web 瀏覽器中立即中斷 Web 資源。對於其他應用程式，Web 控制僅限制新連線。

    如果清除該核取方塊，Web 控制將僅限制與禁止的 Web 資源的新連線。Web 控制不會終止活動連線。

12. 儲存變更。

結果，新的 Web 控制規則被新增到清單。必要的話，請變更 Web 控制規則的優先順序。您也可以使用切換開關隨時停用網頁資源存取規則而無需將其從清單中移除。

# 測試網頁存取規則

當設定 Web 控制時，您可能會無意中封鎖對使用者工作所需的網頁資源的存取。若要瞭解哪條 Web 控制規則在封鎖對網頁資源的存取，您可以使用 *Web 控制規則分析*工具。Web 控制規則分析僅可在 Kaspersky Endpoint Security 的介面中使用。在卡巴斯基安全管理中心主控台中，您無法找出哪條 Web 控制規則包括給定的資源。

如果使用者相信該網頁被封鎖是錯誤的，可以點選網頁資源封鎖通知中的連結，開啟預先產生的訊息並將其傳送給公司區域網路管理員。

*要測試網路資源存取規則，請執行下列操作：*

1. 在“應用程式主視窗”中，點擊⚙按鈕。
2. 在應用程式設定視窗中，選取”**安全控制**“→“**Web 控制**”。




Web 控制設定

3. 在"**設定**"塊中，點擊"**規則診斷**"連接。

   開啟"**規則診斷**"視窗。

4. 如果您想要測試 Kaspersky Endpoint Security 用於控制特定網頁資源存取權限的規則，請選取"**指定的網址**"核取方塊。然後在下面的欄位中輸入網頁資源的位址。

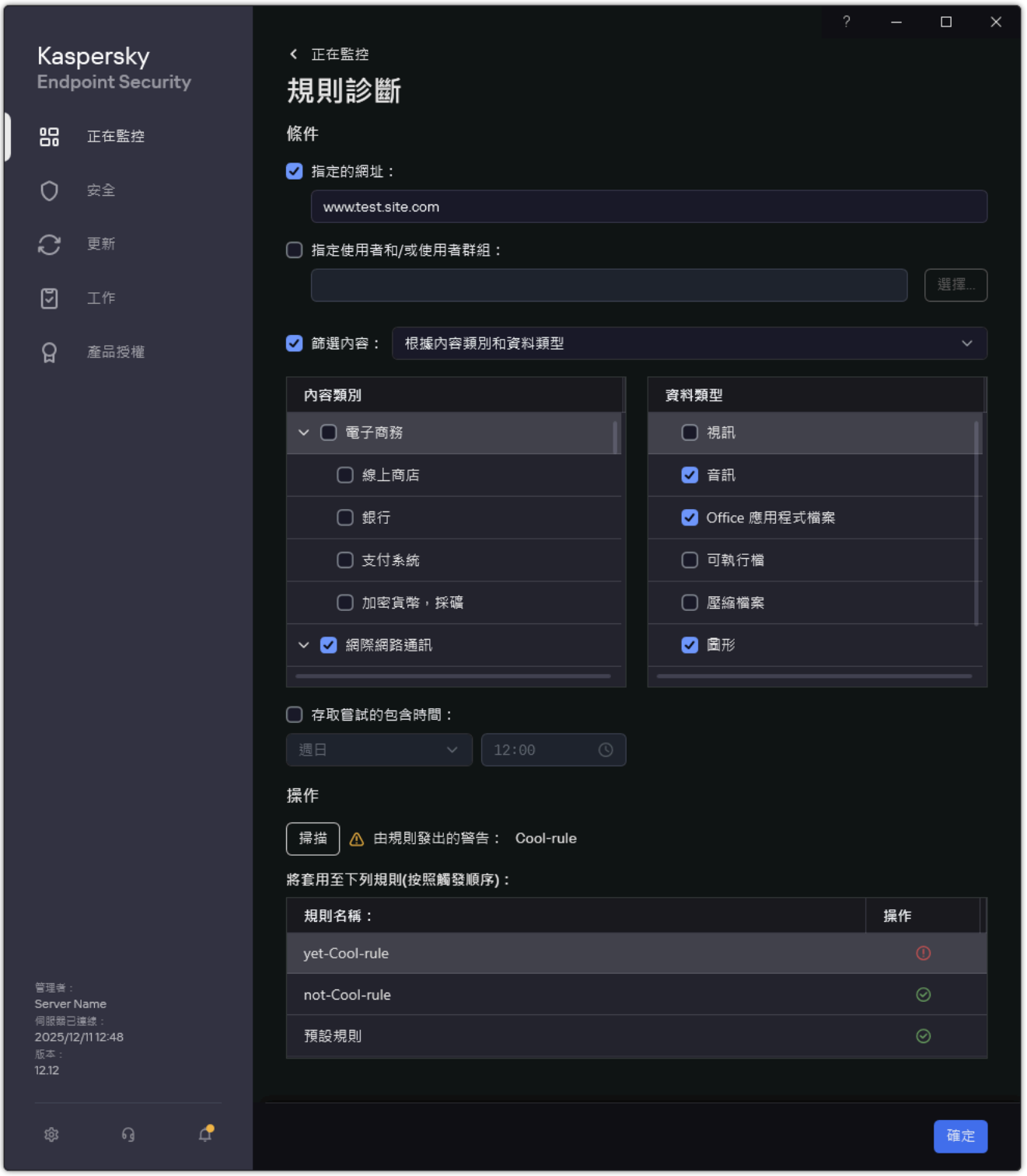
5. 如果您想要測試 Kaspersky Endpoint Security 用於為指定使用者和/或使用者群組控制網頁資源存取權限的規則，請指定使用者和/或使用者群組清單。

6. 如果您想要測試 Kaspersky Endpoint Security 用於控制某些內容類別和/或資料類型類別的網頁資源存取權限的規則，請選擇"**篩選內容**"核取方塊，然後從下拉式清單中選取有關選項（"**根據內容類別**"，"**根據資料類型**"，或"**根據內容類別和資料類型**"）。

7. 如果您要在測試規則時考慮嘗試存取規則診斷條件中指定的網頁資源的時間和星期幾，請選取"**存取嘗試的包含時間**"核取方塊。然後，請指定星期幾和時間。

8. 點擊"**掃描**"。

測試完成後將顯示一條訊息，其中包含關於 Kaspersky Endpoint Security 採取的操作（允許、封鎖或警告）的資訊，該操作是程式根據存取指定網路資源的嘗試所觸發的第一個規則而採取的。要觸發的第一個規則是在 Web 控制規則清單中具有比其他滿足診斷條件的規則更高排名的規則。該訊息顯示在"**掃描**"按鈕的右側。下表包含 Kaspersky Endpoint Security 根據其優先順序低於所觸發的第一個規則的規則而採取的操作的相關資訊。規則點擊降優先順序列出。




網頁資源存取測試結果

# 匯出和匯入 Web 控制規則

您可以將網頁控制規則清單匯出到 XML 或者 JSON 檔案。然後，您可以修改檔案，例如，新增大量相同類型的位址。您可以使用匯出/匯入功能來備份網頁控制規則清單，或將清單遷移到其他伺服器。

### 如何在管理主控台 (MMC) 中匯出和匯入網頁控制規則清單

1. 在卡巴斯基安全管理中心管理主控台樹狀目錄中，選取**政策**。

2. 選擇必要的政策並點擊以開啟政策內容。

3. 在政策視窗中，選擇“**安全控制 → Web 控制**”。

4. 要匯出網頁控制規則清單：

   a. 選取您想要匯出的規則。要選擇多個連接埠，請使用**CTRL**或**SHIFT**鍵。

   如果您未選擇任何規則，則 Kaspersky Endpoint Security 將匯出所有規則。

   b. 點擊”**匯出**”連接。

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

   d. 儲存檔案。

   Kaspersky Endpoint Security 會將規則清單匯出到 XML 檔案。

5. 要匯入網頁控制規則清單，請：

   a. 點擊”**匯入**”連接。

   在開啟的視窗中，選取要從中匯入規則清單的 XML 檔案。

   b. 開啟檔案。

   如果電腦已經具有規則清單，則 Kaspersky Endpoint Security 將提示您刪除現有清單或從 XML 檔案向其中新增新項目。

6. 儲存變更。

**如何在網頁主控台和雲端主控台中匯出和匯入網頁控制規則清單**

1. 在網頁主控台的主視窗中，選擇**資產（裝置）→ 政策和設定檔**。

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. 要匯出”規則清單，請在“**規則清單**“塊中：

   a. 選取您想要匯出的規則。

   b. 點擊 → **匯出** 按鈕。

   Kaspersky Endpoint Security 會將規則清單匯出到預設下載資料夾中的 JSON 檔案。

6. 要匯入規則清單，請在“**規則清單**“塊中：

   a. 點擊 → **匯入** 按鈕。

   在開啟的視窗中，選取要從中匯入規則清單的 JSON 檔案。

   b. 開啟檔案。

   如果電腦已經具有規則清單，則 Kaspersky Endpoint Security 將提示您刪除現有清單或從 JSON 檔案向其中新增新項目。

7. 儲存變更。

# 匯出和匯入 Web 控制規則的網頁資源位址

如果您在網路資源存取規則中建立了網路資源位址清單，則可將其匯出到檔案：

- TXT 格式，在管理主控台 (MMC) 中
- CSV 格式，在應用程式介面中

隨後，您可以從該檔案匯入清單，從而不必在設定存取規則時建立新的網頁位址清單。例如，在建立具有相似參數的存取規則時，用於匯出和匯入網頁位址清單的選項會非常有用。

您也可以匯出/匯入所有 Web 控制規則而不只是單個規則的網頁資源位址。

> 您不可以透過網頁主控台或 Cloud Console 匯出/匯入 Web 控制規則的網頁資源位址。

**如何在管理主控台 (MMC) 中匯出/匯入網頁控制規則的網頁資源位址**

1. 在卡巴斯基安全管理中心管理主控台樹狀目錄中，選取**政策**。
2. 選擇必要的政策並點擊以開啟政策內容。
3. 在政策視窗中，選擇"**安全控制 → Web 控制**"。
4. 在 **Web 控制設定** 塊中，選取您要將其網頁位址清單匯出或匯入到檔案的規則。

   Web 控制規則內容得到顯示。
5. 要匯出網頁資源清單，請在位址清單中執行以下操作：
   a. 選擇您要匯出的位址。

      如果您沒有選擇任何位址，Kaspersky Endpoint Security 將匯出所有位址。

   b. 點擊 按鈕。

   c. 在開啟的視窗中，輸入您要將網頁資源位址清單匯出到的 TXT 檔案的名稱，然後選取要儲存此檔案的資料夾。

   d. 儲存檔案。

      Kaspersky Endpoint Security 會將網頁資源位址清單匯出到 TXT 檔案。
6. 要匯入網頁資源清單，請在位址清單中執行以下操作：
   a. 點擊 按鈕。

      在開啟的視窗中，選取要從中匯入網頁資源清單的 TXT 檔案。

   b. 開啟檔案。

      如果電腦已經具有位址清單，則 Kaspersky Endpoint Security 將提示您刪除現有清單或從 TXT 檔案向其中新增新項目。
7. 儲存變更。

### 如何在應用程式介面中匯出/匯入網頁控制規則的網頁資源位址

1. 在“應用程式主視窗”中，點擊⚙按鈕。
2. 在應用程式設定視窗中，選取”**安全控制**“→“**Web 控制**”。




Web 控制設定

3. 在”**設定**”塊中，點擊”**網路資源存取規則**”按鈕。
4. 選取您要將其網頁位址清單匯出或匯入到檔案的規則。
5. 要匯出受信任網址清單，請在“**位址**“塊中執行以下操作：
   a. 選擇您要匯出的位址。
      如果您沒有選擇任何位址，Kaspersky Endpoint Security 將匯出所有位址。
   b. 點擊“**匯出**”。
   c. 在開啟的視窗中，輸入您要將網頁資源位址清單匯出到的 CSV 檔案的名稱，然後選取要儲存此檔案的資料夾。
   d. 儲存檔案。
      Kaspersky Endpoint Security 會將網頁資源位址清單匯出到 CSV 檔案。
6. 要匯入網頁資源清單，請在“**位址**“塊中執行以下操作：
   a. 點擊“**匯入**”。
      在開啟的視窗中，選取要從中匯入網頁資源清單的 CSV 檔案。

b. 開啟檔案。

如果電腦已經具有位址清單，則 Kaspersky Endpoint Security 將提示您刪除現有清單或從 CSV 檔案向其中新增新項目。

7. 儲存變更。

# 監控使用者網際網路活動

Kaspersky Endpoint Security 允許您記錄使用者對所有網站（包括允許的網站）的存取資料。這使您可以獲取完整的瀏覽器歷史記錄視圖。Kaspersky Endpoint Security 將使用者活動事件傳送到卡巴斯基安全管理中心、Kaspersky Endpoint Security 本機記錄和 Windows 事件記錄。要在卡巴斯基安全管理中心中接收事件，您需要在管理主控台或網頁主控台中配置政策中的事件設定。您還可以配置透過電子郵件傳輸 Web 控制事件以及在使用者電腦上顯示螢幕通知。

支援監控功能的瀏覽器：Microsoft Edge，Microsoft Internet Explorer，Google Chrome，Yandex Browser，Mozilla Firefox。使用者活動監控在其他瀏覽器中不工作。

Kaspersky Endpoint Security 會建立以下使用者網際網路活動事件：

- 鎖該網站（*緊急*狀態）。
- 存取非建議網站（*警告*狀態）。
- 存取允許的網站（*資訊*狀態）。

在啟用使用者網際網路活動監控之前，您必須執行以下操作：

- 將網頁交互指令碼注入 Web 流量中（請參閱以下說明）。指令碼將啟用 Web 控制事件的註冊。
- 對於 HTTPS 流量監控，需要啟用加密連線掃描。

## 注入網頁交互指令碼

**如何在管理主控台 (MMC) 中將網頁交互指令碼注入到 Web 流量中**

1. 在卡巴斯基安全管理中心管理主控台樹狀目錄中，選取**政策**。
2. 選擇必要的政策並點擊以開啟政策內容。
3. 在政策視窗中，選擇“**一般設定 → 網路設定**”。
4. 在“**加密連線掃描**“塊中，選中“**注入指令碼到網頁流量從而與網頁互動**”核取方塊。
5. 儲存變更。

**如何在網頁主控台和雲端主控台中將網頁交互指令碼注入到 Web 流量中**

1. 在網頁主控台的主視窗中，選擇**資產（裝置）→政策和設定檔**。
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. 在政策視窗中，選擇“**一般設定 → 網路設定**”。
5. 在“**監控網際網路連線**”下方，開啟“**「監控網際網路連線」已啟用**”開關。
6. 儲存變更。

**如何在應用程式介面中將網頁交互指令碼注入到 Web 流量中**

1. 在“應用程式主視窗”中，點擊⚙按鈕。
2. 在應用程式設定視窗中，選取”**一般設定**“→“**網路設定**”。




應用程式網路設定

3. 在“**流量處理**“塊中，選中“**注入指令碼到網頁流量從而與網頁互動**”核取方塊。
4. 儲存變更。

結果，Kaspersky Endpoint Security 會將網頁交互指令碼注入到 Web 流量中。此指令碼可啟用為應用程式事件日誌、OS 事件日誌和報告註冊 Web 控制事件。

配置 Web 控制事件的記錄

*要設定使用者電腦上的 Web 控制事件的記錄：*

1. 在"應用程式主視窗"中，點擊⚙按鈕。
2. 在應用程式設定視窗中，選取"**一般設定**"→"**介面**"。
3. 在"**通知**"塊中，點擊"**設定通知**"按鈕。
4. 在開啟的視窗中，選擇"**Web 控制**"區域。

   這將開啟 Web 控制事件和通知方法的表。
5. 為每個事件設定通知方法："**儲存在本機報告中**"或"**儲存於 Windows 事件記錄中**"。

   要記錄允許的網站存取事件，您還需要設定 Web 控制（請參見下面的說明）。

   在事件表中，您還可以啟用螢幕通知和電子郵件通知。要透過電子郵件傳送通知，您需要設定 SMTP 伺服器設定。有關透過電子郵件傳送通知的詳細資訊，請參閱卡巴斯基安全管理中心說明。
6. 儲存變更。

結果，Kaspersky Endpoint Security 開始記錄使用者網際網路活動事件。

"Web 控制"將使用者活動事件傳送到卡巴斯基安全管理中心，如下所示：

- 如果您使用卡巴斯基安全管理中心，"Web 控制"會針對構成網頁的所有物件傳送事件。因此，當一個網頁被封鎖時，可能會建立多個事件。例如，在封鎖網頁 http://www.example.com 時，Kaspersky Endpoint Security 可能會傳送以下物件的事件：http://www.example.com，http://www.example.com/icon.ico，http://www.example.com/file.js 等。
- 如果您使用卡巴斯基安全管理中心雲端主控台，"Web 控制"會對事件進行分組並僅傳送網站的協定和網域。例如，如果使用者存取非推薦網頁 http://www.example.com/main、http://www.example.com/contact、http://www.example.com/gallery，Kaspersky Endpoint Security 將只傳送一個包含 http://www.example.com 物件的事件。

造訪允許網站時記錄事件

*要啟用存取允許網站時記錄事件：*

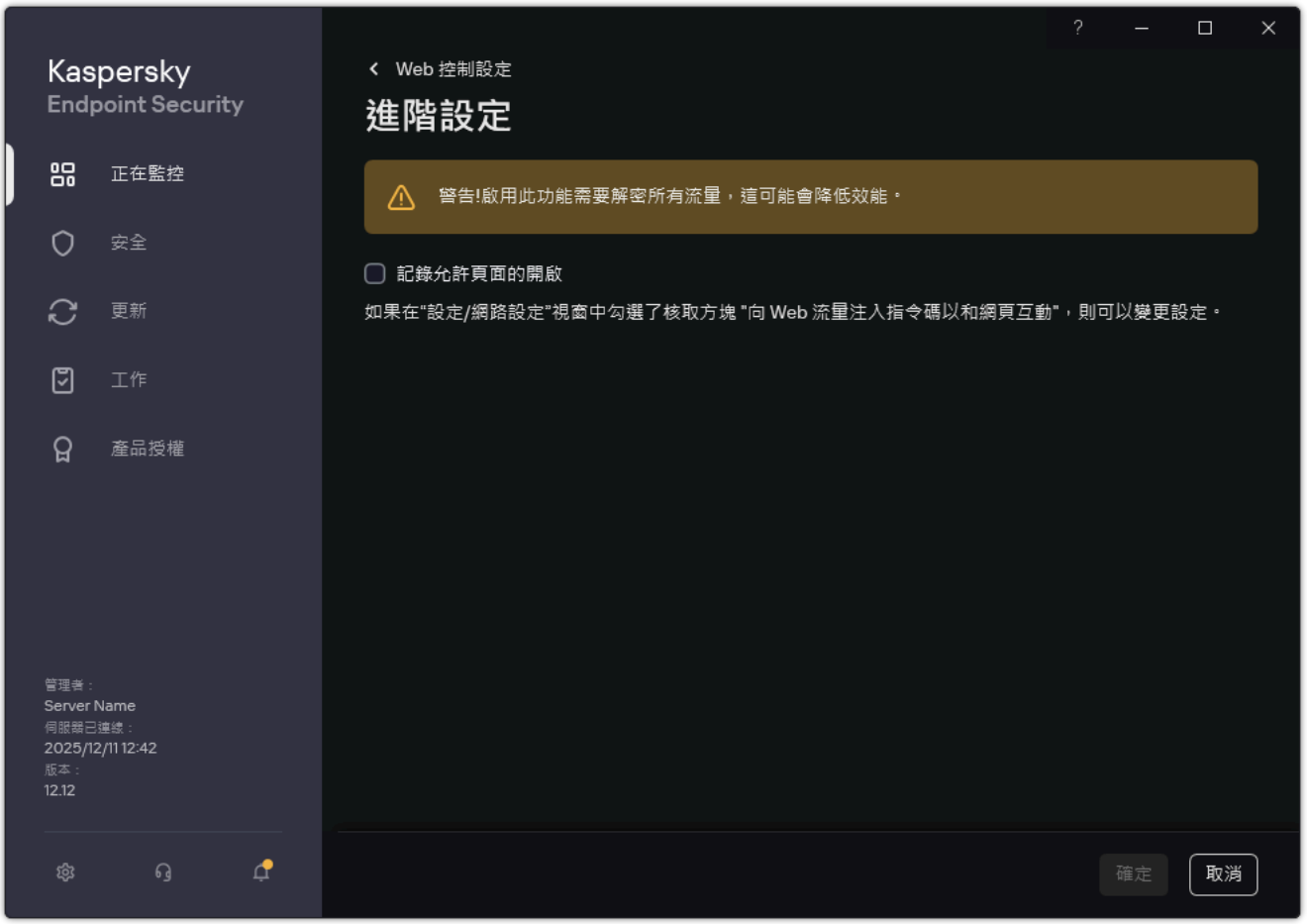
1. 在“應用程式主視窗”中，點擊⚙按鈕。
2. 在應用程式設定視窗中，選取”**安全控制**“→“**Web 控制**”。




Web 控制設定

3. 在”**附加**”塊中，點擊”**進階設定**”按鈕。

4. 在開啟的視窗中，選中“**記錄允許頁面的開啟**”核取方塊。




Web 控制進階設定

5. 儲存變更。

結果，您將能夠檢視完整的瀏覽器歷史記錄。

# 編輯 Web 控制訊息範本

根據在 Web 控制規則內容中指定的操作的類型，當使用者嘗試存取網際網路資源時，Kaspersky Endpoint Security 顯示下列類型之一的訊息（應用程式用 HTTP 伺服器回應訊息替換 HTML 頁面）：

- 警告訊息。該訊息將警告存取該網頁資源的使用者該網頁資源不受歡迎並且/或者違反公司安全政策。如果從描述該網頁資源的規則設定中選擇了“**警告**“選項，Kaspersky Endpoint Security 會顯示一條警告訊息。

  如果使用者認為該警告是錯誤的，使用者可以點擊警告訊息中的連結，開啟預先產生的回報訊息並將其傳送給公司區域網路管理員。

- 通知封鎖網頁資源的訊息。如果從描述該網頁資源的規則設定中選擇了“**封鎖**“選項，Kaspersky Endpoint Security 會顯示一條訊息，通知網頁資源被封鎖（請見下圖）。

如果使用者相信該網頁被封鎖是錯誤的，可以點選網頁資源封鎖通知中的連結，開啟預先產生的訊息並將其傳送給公司區域網路管理員。




關於 Web 資源封鎖的訊息

我們為警告訊息、通知網頁資源被封鎖的訊息以及要傳送給管理員的訊息提供了專用範本。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。

### 如何在管理主控台 (MMC) 中變更 Web 控制訊息範本

1. 在卡巴斯基安全管理中心管理主控台樹狀目錄中，選取**政策**。
2. 選擇必要的政策並點擊以開啟政策內容。
3. 在政策視窗中，選擇"**安全控制 → Web 控制**"。
4. 在"**訊息範本設定**"塊中，點擊"**範本**"按鈕。
5. 配置 Web 控制訊息範本：

   - **警告**該項目欄位包含一個訊息範本，嘗試存取不需要的網頁資源觸發警告訊息規則時就會顯示警告訊息。
   - **有關封鎖的訊息**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。
   - **傳送郵件給管理員**如果使用者認為封鎖是錯誤時要傳送給區域網路管理員的訊息範本。在使用者請求提供存取權限後，Kaspersky Endpoint Security 會向卡巴斯基安全管理中心傳送一個事件：**傳送給管理員的網頁存取封鎖訊息**。事件描述包含一條給管理員的訊息，其中包含被替換的變數。您可以使用預定義事件選擇**使用者請求**在卡巴斯基安全管理中心主控台中檢視這些事件。如果您的組織沒有部署卡巴斯基安全管理中心或者沒有連線到管理伺服器，應用程式將向管理員傳送一條訊息到指定的電子郵件信箱。

   若要將變數新增至範本文字，請將游標置於所需位置，點擊**變數**，然後從可用選項清單中選取所需變數。

   此外，您也可使用**根據預設**按鈕，還原預設範本文字。

6. 儲存變更。

### 如何在 Web 主控台和雲端主控台中變更 Web 控制訊息

1. 在網頁主控台的主視窗中，選擇**資產（裝置）→政策和設定檔**。
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** 區塊中，點擊 **有關網站封鎖的訊息** 連結和配置 Web 控制訊息的範本：

   - **警告**該項目欄位包含一個訊息範本，嘗試存取不需要的網頁資源觸發警告訊息規則時就會顯示警告訊息。
   - **有關封鎖的訊息**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。
   - **傳送給管理員的郵件**如果使用者認為封鎖是錯誤時要傳送給區域網路管理員的訊息範本。在使用者請求提供存取權限後，Kaspersky Endpoint Security 會向卡巴斯基安全管理中心傳送一個事件：**傳送給管理員的網頁存取封鎖訊息**。事件描述包含一條給管理員的訊息，其中包含被替換的變數。您可以使用預定義事件選擇**使用者請求**在卡巴斯基安全管理中心主控台中檢視這些事件。如果您的組織沒有部署卡巴斯基安全管理中心或者沒有連線到管理伺服器，應用程式將向管理員傳送一條訊息到指定的電子郵件信箱。

   若要將變數新增至範本文字，請將游標置於所需位置，點擊**新增變數**，然後從可用選項清單中選取所需變數。

   此外，您也可使用**重設為預設值**按鈕，還原預設範本文字。
6. 儲存變更。

### 如何在應用程式介面中變更 Web 控制訊息範本

1. 在“應用程式主視窗”中，點擊⚙按鈕。
2. 在應用程式設定視窗中，選取”**安全控制**“→“**Web 控制**”。




Web 控制設定

3. 在“**範本**“塊中，設定 Web 控制訊息範本：
   - **警告**該項目欄位包含一個訊息範本，嘗試存取不需要的網頁資源觸發警告訊息規則時就會顯示警告訊息。
   - **有關封鎖的訊息**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。
   - **傳送郵件給管理員**如果使用者認為封鎖是錯誤時要傳送給區域網路管理員的訊息範本。在使用者請求提供存取權限後，Kaspersky Endpoint Security 會向卡巴斯基安全管理中心傳送一個事件：**傳送給管理員的網頁存取封鎖訊息**。事件描述包含一條給管理員的訊息，其中包含被替換的變數。您可以使用預定義事件選擇**使用者請求**在卡巴斯基安全管理中心主控台中檢視這些事件。如果您的組織沒有部署卡巴斯基安全管理中心或者沒有連線到管理伺服器，應用程式將向管理員傳送一條訊息到指定的電子郵件信箱。

   若要將變數新增至範本文字，請將游標置於所需位置，點擊**新增變數**，然後從可用選項清單中選取所需變數。

   此外，您也可使用**重設**按鈕，還原預設範本文字。
4. 儲存變更。

# 編輯網頁資源位址的遮罩

如果您在建立網路資源存取規則時需要輸入多個相似的網頁位址，則使用*網路資源位址遮罩*（也稱為"位址遮罩"）會較為便利。如果建立得當，一個位址遮罩可以替換多項的網頁位址。

建立位址遮罩時遵循以下規則：

1. `*` 字元將替換包含零或任意個字元的任何序列。

   例如，如果輸入 `*abc*` 位址遮罩，則存取規則將套用於包含序列 `abc` 的所有網路資源。範例：`http://www.example.com/page_0-9abcdef.html`。

2. 一個序列的`*.`字符（稱為*網域遮罩*）可讓您選擇位址的所有網域。`*.`網域遮罩可表示任何網域名稱、子網域名稱或空白行。

   示例： `*.example.com`遮罩表示以下位址：

   - `http://pictures.example.com`。域遮罩`*.`代表`pictures.`
   - `http://user.pictures.example.com`。網域遮罩 `*.`代表`pictures.`和`user.`
   - `http://example.com`。網域遮罩`*.`被解釋為空白行

3. 位於位址遮罩開頭的`www.` 字元序列被解釋為 `*.` 序列。

   範例：位址遮罩 `www.example.com` 將被解釋為 `*.example.com`。此遮罩涵蓋位址`www2.example.com`和`www.pictures.example.com`。

4. 如果位址遮罩不以 `*` 字元開頭，則位址遮罩的內容等同於以`*.` 為首碼的內容。

5. 如果位址遮罩以 `/` 或 `*`，之外的字元結尾，則位址遮罩的內容等同於以`/*` 為尾碼的內容。

   範例：位址遮罩 `http://www.example.com` 涵蓋像 `http://www.example.com/abc` 這樣的位址，其中 `a`、`b` 和 `c` 為任意字元。

6. 如果位址遮罩以 `/` 字元結尾，則位址遮罩的內容等同於以 `/*` 為尾碼的內容。

7. 字元序列 `/*` 將被解釋為`/*` 或空字串。

8. 網頁資源位址根據位址遮罩進行驗證，同時會考慮使用的協定（http 或 https）：

   - 如果位址遮罩不含網路通訊協定，該位址遮罩將涵蓋使用任意網路通訊協定的位址。

     範例：地址掩碼 `example.com` 覆蓋地址 `http://`example.com 和 `https://`example.com。

   - 如果位址遮罩包含網路通訊協定，該位址僅涵蓋使用位址遮罩中網路通訊協定的位址。

     範例：位址遮罩 `http://*.example.com` 涵蓋位址 `http://www.example.com`，但不涵蓋 `https://www.example.com`。

9. 用雙引號引起來的位址遮罩表示除 `*` 字元（如果初始包含在位址遮罩中）外，不考慮其他任何替代項目。規則 5 和 7 不會應用至雙引號中的位址遮罩（請參閱下表中的範例 14-18）。

10. 在比較網頁資源的位址遮罩時，不會考慮使用者名稱和密碼、連接埠以及字元大小寫。

| 編號 | 位址遮罩 | 要驗證的網頁資源位址 | 是位址遮罩涵蓋的位址 | 註解 |
|---|---|---|---|---|
| 1 | *.example.com | http://www.123example.com | 否 | 參見規則 1。 |
| 2 | *.example.com | http://www.123.example.com | 是 | 參見規則 2。 |
| 3 | *example.com | http://www.123example.com | 是 | 參見規則 1。 |
| 4 | *example.com | http://www.123.example.com | 是 | 參見規則 1。 |
| 5 | http://www.*.example.com | http://www.123example.com | 否 | 參見規則 1。 |
| 6 | www.example.com | http://www.example.com | 是 | 參見規則 3、2、1。 |
| 7 | www.example.com | https://www.example.com | 是 | 參見規則 3、2、1。 |
| 8 | http://www.*.example.com | http://123.example.com | 是 | 參見規則 3、4、1。 |
| 9 | www.example.com | http://www.example.com/abc | 是 | 參見規則 3、5、1。 |
| 10 | example.com | http://www.example.com | 是 | 參見規則 3、1。 |
| 11 | http://example.com/ | http://example.com/abc | 是 | 參見規則 6。 |
| 12 | http://example.com/* | http://example.com | 是 | 參見規則 7。 |
| 13 | http://example.com | https://example.com | 否 | 參見規則 8。 |
| 14 | "example.com" | http://www.example.com | 否 | 參見規則 9。 |
| 15 | "http://www.example.com" | http://www.example.com/abc | 否 | 參見規則 9。 |
| 16 | "*.example.com" | http://www.example.com | 是 | 參見規則 1、9。 |
| 17 | "http://www.example.com/*" | http://www.example.com/abc | 是 | 參見規則 1、9。 |
| 18 | "www.example.com" | http://www.example.com;<br>https://www.example.com | 是 | 參見規則 9、8。 |
| 19 | www.example.com/abc/123 | http://www.example.com/abc | 否 | 位址遮罩包含的資訊量多於網頁位址。 |

# 虛擬機器的 Web 控制

Web 控制可控制電腦以及電腦上本機部署的虛擬機上的流量。此操作無需在本機虛擬機上安裝 Kaspersky Endpoint Security 應用程式即可實現。這意味著，如果使用者嘗試在*虛擬機*上的瀏覽器中開啟被 Web 控制規則封鎖的網站，安裝在 *電腦*主機作業系統上的應用程式將拒絕存取該網站。

Web 控制在不同虛擬機上的運作方式不同。

## Oracle VM VirtualBox

Kaspersky Endpoint Security 無限制地支援 Oracle VM VirtualBox 虛擬機上的 Web 控制規則。應用程式可以控制虛擬機的所有流量。如果在 Web 控制規則中配置了按使用者過濾，應用程式可以正常工作，因為虛擬機的所有處理程序都是由本機使用者啟動的。

### VMware工作站

Kaspersky Endpoint Security 支援 VMware Workstation 虛擬機上的 Web 控制規則，但有限制。應用程式不支援由使用者配置篩選器的規則。虛擬機處理程序在系統使用者（SYSTEM）下執行。這使得無法識別嘗試在虛擬機上開啟網站的使用者。

### Microsoft Hyper-V

Kaspersky Endpoint Security 不支援 Microsoft Hyper-V 虛擬機上的 Web 控制規則。

## 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）。

# 裝置控制

"裝置控制"管理使用者對安裝在電腦上或連線到電腦的裝置（例如，硬碟磁碟機、相機或 Wi-Fi 模組）的存取。這樣可以在連線此類裝置時防護電腦免受感染，並防止資料遺失或洩漏。

如果啟用了裝置控制，則應用程式會將有關已連線裝置的資訊轉送到卡巴斯基安全管理中心。您可以在卡巴斯基安全管理中心的"**進階** → **儲存區** → **硬體**"資料夾中檢視已連線裝置的清單。

## 裝置存取等級

"裝置控制"控制以下等級的存取權限：

- **裝置類型**。例如，印表機、卸除式磁碟機和 CD/DVD 磁碟機。

  您可以按如下方式配置裝置存取權限：

  - 允許 – ✓。
  - 封鎖 – ⊘。
  - 按規則（僅限印表機和攜帶式裝置） –。
  - 取決於連線匯流排（Wi-Fi 除外） –。
  - 封鎖但帶有例外（僅限 Wi-Fi） –。

- **連線匯流排**。*連線匯流排*是用於將裝置連線至電腦的介面（範例 USB 或 FireWire）。如果為裝置類型選擇 **取決於連線匯流排** 模式後，應用程式會根據連線介面（例如 USB）允許或拒絕對裝置的存取。

  您可以按如下方式配置裝置存取權限：

  - 允許 – ✓。
  - 封鎖 – ⊘。

- **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。

您可以根據以下資料新增受信任裝置：

- **透過裝置 ID**每個裝置都有一個唯一識別碼（硬體 ID 或 HWID）。您可以使用作業系統工具在裝置內容中檢視 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。

- **透過裝置型號**每個裝置都有一個供應商 ID (VID) 和一個產品 ID (PID)。您可以使用作業系統工具在裝置內容中檢視 ID。用於輸入 VID 和 PID 的範本：`VID_1234&PID_5678`。如果在組織中使用特定型號的裝置，則按型號新增裝置很方便。這樣，您可以新增該型號的所有裝置。

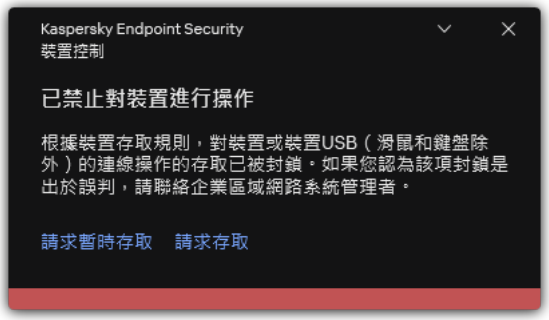
- **透過裝置 ID 遮罩**如果您使用具有相似 ID 的多個裝置，則可以使用遮罩將裝置新增到受信任清單。`*` 字元可替換任意一組字元。輸入遮罩時，Kaspersky Endpoint Security 不支援 `?` 字元。例如，`WDC_C*`。

- **依型號遮罩列出的裝置**如果您使用具有相似 VID 或 PID 的多個裝置（例如，同一製造商的裝置），則可以使用遮罩將裝置新增到受信任清單。`*` 字元可替換任意一組字元。輸入遮罩時，Kaspersky Endpoint Security 不支援 `?` 字元。例如，`VID_05AC&PID_*`。

“裝置控制”透過使用*存取規則*來管理使用者對裝置的存取。“裝置控制”還允許您儲存裝置連線/斷開連線事件。要儲存事件，您需要在政策中配置事件註冊。

如果對裝置的存取權限取決於連線介面（ 狀態），Kaspersky Endpoint Security 不會儲存裝置連線/斷開連線事件。要使 Kaspersky Endpoint Security 儲存裝置連線/斷開連線事件，請允許存取相應的裝置類型（ 狀態）或將裝置新增到信任清單。

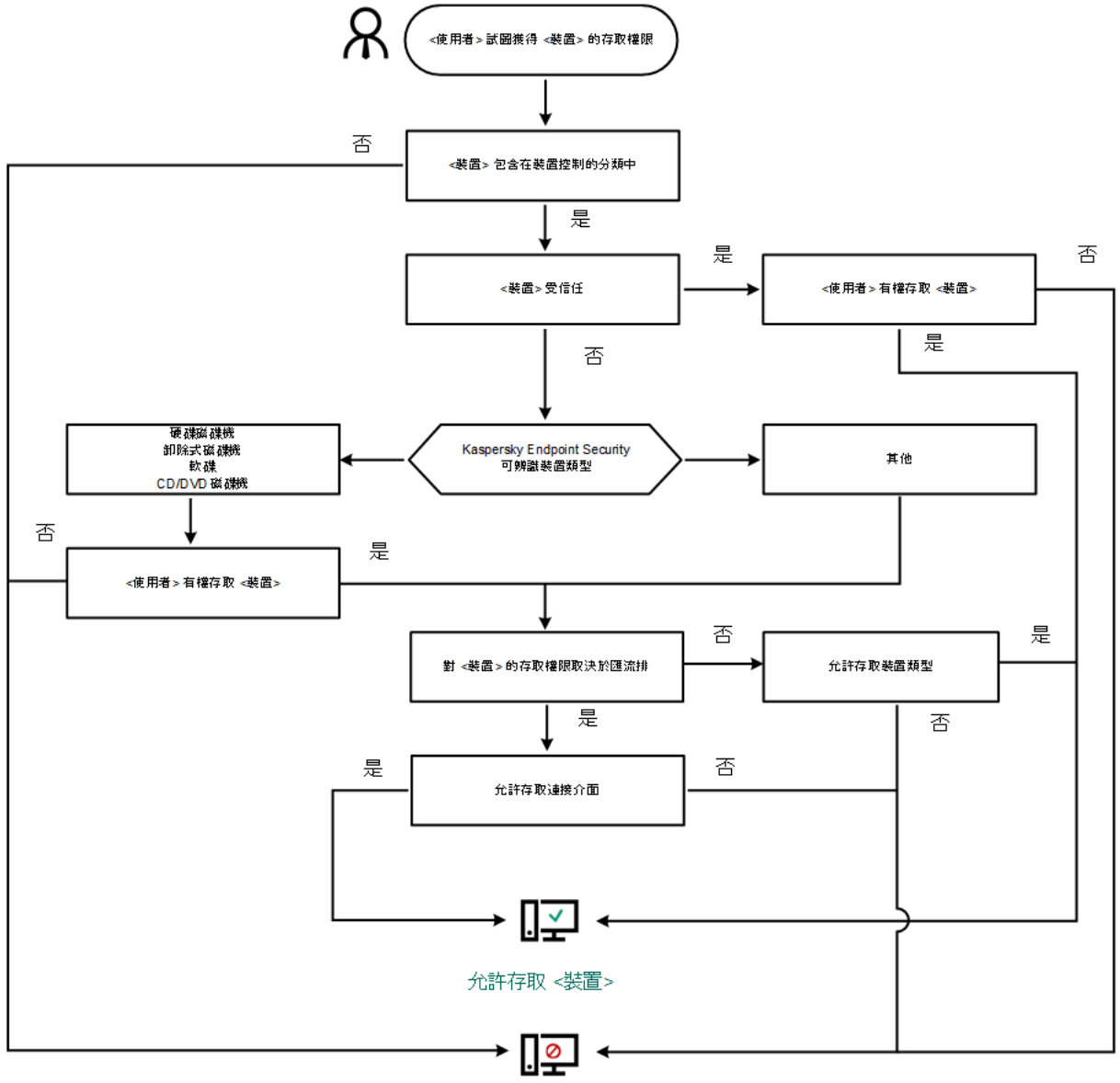
當被“裝置控制”封鎖的裝置連線到電腦時，Kaspersky Endpoint Security 將封鎖存取並顯示通知（請參見下圖）。




“裝置控制”通知

## 裝置控制執行演算法

Kaspersky Endpoint Security 在使用者將裝置連線到電腦之後做出是否允許存取該裝置的決定（請參見下圖）。




裝置控制執行演算法

如果已連線裝置並允許存取，您可以編輯存取規則並封鎖存取。在這種情況下，下次有人嘗試存取該裝置（例如檢視資料夾樹或執行讀取或寫入操作）時，Kaspersky Endpoint Security 會封鎖存取。沒有檔案系統的裝置僅在該裝置下一次連接時被封鎖。

如果已安裝有 Kaspersky Endpoint Security 的電腦上的使用者需要請求被錯誤封鎖的裝置的存取權限，則向該使用者傳送請求存取說明。

# 關於存取規則

*裝置存取規則*是一組設定，用於確定使用者如何可以存取安裝到或連線到電腦的裝置。這些設定包括對特定裝置的存取、存取排程以及讀取或寫入權限。您不能新增在裝置控制分類之外的裝置。此類裝置允許所有使用者存取。

## 裝置存取規則

存取規則的設定群組根據裝置類型的不同而不同（請參見下表）。

存取規則設定

| 裝置 | 存取控制 | 裝置存取排程 | 使用者和/或使用者群組的分配 | 優先順序 | 讀/寫權限 |
|---|---|---|---|---|---|
| 硬碟磁碟機 | ✓ | ✓ | ✓ | ✓ | ✓ |
| 卸除式磁碟機（包括 USB 快閃磁碟機） | ✓ | ✓ | ✓ | ✓ | ✓ |
| 軟碟 | ✓ | ✓ | ✓ | ✓ | ✓ |
| CD/DVD 磁碟機 | ✓ | ✓ | ✓ | ✓ | ✓ |
| 可攜式裝置(MTP) | ✓ | ✓ | ✓ | ✓ | ✓ |
| 本機印表機 | ✓ | – | ✓ | ✓ | – |
| 網路印表機 | ✓ | – | ✓ | ✓ | – |
| 數據機 | ✓ | – | – | – | – |
| 磁帶裝置 | ✓ | – | – | – | – |
| 多功能裝置 | ✓ | – | – | – | – |
| 智慧卡讀卡機 | ✓ | – | – | – | – |
| Windows CE USB ActiveSync 裝置 | ✓ | – | – | – | – |
| 外接式網路卡 | ✓ | – | – | – | – |
| 藍芽 | ✓ | – | – | – | – |
| 攝影鏡頭和掃描器 | ✓ | – | – | – | – |

## Wi-Fi 網路的存取規則

Wi-Fi 網路存取規則確定允許（✓ 狀態）還是禁止（⊘ 狀態）使用 Wi-Fi 網路。您可以將*受信任的 Wi-Fi 網路*（ 狀態）新增到規則中。允許無限制使用受信任的 Wi-Fi 網路。預設情況下，Wi-Fi 網路存取規則允許存取任何 Wi-Fi 網路。

## 連線匯流排存取規則

如果為裝置類型的存取規則選擇 **取決於連線匯流排** 模式，應用程式會根據連線介面允許或拒絕對裝置的存取。預設情況下，程式將為裝置控制元件分類中存在的所有連線匯流排建立允許存取的規則。

連線匯流排存取規則確定允許（ 狀態）還是禁止（ 狀態）連線裝置。裝置類型存取規則的優先權高於連線匯流排存取規則的優先權。

鍵盤和滑鼠無法使用"裝置控制"鎖定。如果禁止存取 USB 連線匯流排，使用者將繼續使用透過 USB 連線的鍵盤和滑鼠進行工作。BadUSB 攻擊防護元件旨在防止模擬鍵盤的、受感染的 USB 裝置連線至電腦。

# 按類型管理對裝置的存取

裝置控制允許按類型管理對裝置的存取。裝置類型由作業系統在裝置連線時決定。您可以使用作業系統內建的裝置管理器工具來尋找裝置類型。若要管理對裝置的存取，您必須配置規則。*裝置存取規則*是一組設定，用於確定使用者如何可以存取安裝到或連線到電腦的裝置。這些設定包括對特定裝置的存取、存取排程以及讀取或寫入權限。您不能新增在裝置控制分類之外的裝置。此類裝置允許所有使用者存取。

預設情況下，裝置控制允許所有使用者存取所有裝置。

您可以如下設定對裝置的存取：

- **允許**

  Kaspersky Endpoint Security 授予所有使用者對裝置的完全存取權。

- **封鎖**

  Kaspersky Endpoint Security 可封鎖裝置連線。該應用程式允許 僅連線受信任裝置。

- **取決於連線匯流排**

  Kaspersky Endpoint Security 可確定裝置的連線介面並根據裝置的匯流排連線狀態限制對裝置的存取。該應用程式還允許 連線受信任裝置。

- **按規則**

  對於某些裝置類型，您可以指定允許使用裝置的單個使用者或一組使用者，設定裝置存取排程，並配置讀寫權限。該應用程式還允許 連線受信任裝置。

配置對**硬碟磁碟機**類型裝置的存取時要小心。如果封鎖對系統磁碟的存取，應用程式可能會在引導作業系統時導致崩潰 (BSOD)。

如果裝置不符合裝置控制分類方案，則無法限制對該裝置的存取。

### 如何在管理主控台 (MMC) 中按類型管理對裝置的存取

1. 開啟卡巴斯基安全管理中心管理主控台。
2. 在主控台樹狀目錄中，選擇"**政策**"。
3. 選擇必要的政策並點擊以開啟政策內容。
4. 在政策視窗中，選擇"**安全控制 → 裝置控制**"。
5. 在**裝置控制設定**下，選擇**裝置類型**標籤。

   **裝置類型** 頁簽顯示裝置控制類別中包括的所有裝置的存取規則。

6. 配置裝置的存取規則：

   a. 選擇存取模式：**允許**、**封鎖**、**取決於連線匯流排**、**按規則**。

      要選取「**按規則**」存取模式，您必須雙擊開啟存取規則內容。

   b. 如果您選擇了 **取決於連線匯流排** 存取模式，請轉到 **連線匯流排** 頁簽並配置連線介面的存取規則。

   c. 對於儲存裝置（例如，卸除式媒體），您可以為單個使用者設定存取權限。您也可以設定裝置存取排程並配置讀寫權限。

      您可以將裝置新增到受信任清單。*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。

   d. 如有需要，配置列印規則。

   e. 如有需要，配置藍牙裝置存取規則。

   f. 如有需要，設定電腦 Wi-Fi 連線規則。

7. 儲存變更。若要在電腦上套用該政策，請關閉掛鎖。

**如何在網頁主控台和雲端主控台中按類型管理對裝置的存取**

1. 在網頁主控台的主視窗中，選擇**資產（裝置）→政策和設定檔**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**"安全控制"→"裝置控制"**。

5. 在**裝置存取規則**下，選擇**裝置和 Wi-Fi 網路**標籤。

   表格列出了"裝置控制"元件分類中存在的所有裝置的存取規則。

6. 配置裝置的存取規則：

   a. 選擇存取模式：**允許**、**封鎖**、**取決於匯流排**、**自訂**。

      如果下拉式選單中缺少存取模式，請雙擊裝置類型開啟存取規則屬性。

   b. 如果您選擇了 **取決於匯流排** 存取模式，請轉到 **連線匯流排** 頁簽並配置連線介面的存取規則。

   c. 對於儲存裝置（例如，卸除式媒體），您可以為單個使用者設定存取權限。您也可以設定裝置存取排程並配置讀寫權限。

      您可以將裝置新增到受信任清單。*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。

   d. 如有需要，配置列印規則。

   e. 如有需要，配置藍牙裝置存取規則。

   f. 如有需要，設定電腦 Wi-Fi 連線規則。

7. 儲存變更。若要在電腦上套用該政策，請關閉掛鎖。

**如何在應用程式介面中管理對裝置的存取**

1. 在"應用程式主視窗"中，點擊⚙按鈕。
2. 在應用程式設定視窗中，選取"**安全控制**"→"**裝置控制**"。
3. 在"**存取設定**"塊中，點擊"**裝置和 Wi-Fi 網路**"連接。
   表格列出了"裝置控制"元件分類中存在的所有裝置的存取規則。
4. 配置裝置的存取規則：
   a. 選擇存取模式：**允許**， **封鎖**，**取決於連線匯流排**，**按規則**。
      如果下拉式選單中缺少存取模式，請雙擊裝置類型開啟存取規則屬性。
   b. 如果您選擇了 **取決於連線匯流排** 存取模式，請轉到 **連線匯流排** 頁簽並配置連線介面的存取規則。
   c. 對於儲存裝置（例如，卸除式媒體），您可以為單個使用者設定存取權限。您也可以設定裝置存取排程並配置讀寫權限。
      您可以將裝置新增到受信任清單。*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。
   d. 如有需要， 配置列印規則。
   e. 如有需要， 配置藍牙裝置存取規則。
   f. 如有需要， 設定電腦 Wi-Fi 連線規則。
5. 儲存變更。

結果，當使用者嘗試存取裝置時，應用程式會根據規則阻止存取。Kaspersky Endpoint Security 也記錄相應事件。如果想授予單個裝置存取權限，您可以 將這些裝置新增至受信任裝置清單。

# 透過連線匯流排管理對裝置的存取

*若要編輯連線匯流排存取規則，請執行以下操作：*

1. 在"應用程式主視窗"中，點擊⚙按鈕。
2. 在應用程式設定視窗中，選取"**安全控制**"→"**裝置控制**"。
3. 在"**存取設定**"塊中，點擊"**連線匯流排**"按鈕。
   開啟的視窗顯示了裝置控制元件類別中包括的所有連線匯流排的存取規則。
4. 選取您想要編輯的存取規則。
5. 在"**存取**"列中，選擇是否允許存取連線匯流排：**允許**或**封鎖**。

   如果變更了連線匯流排的存取權限**串列埠(COM)** (COM) 或者 **並列埠(LPT)** (LPT)，必須重新啟動電腦以啟動存取規則。

6. 儲存變更。

# 區分使用者對裝置的存取權限

您可以按裝置類型或受信任裝置設定使用者存取權限。

## 按裝置類型區分使用者存取權限

裝置控制允許配置使用者對 *儲存裝置*上資料的存取權限。對於此類裝置，您可以配置寫入和讀取權限。裝置控制支援以下類型的 *儲存裝置*：

- 硬碟磁碟機。
- 卸除式磁碟機（包括 USB 快閃磁碟機）。
- 軟碟。
- CD/DVD 磁碟機。
- 可攜式裝置(MTP)。可攜式裝置 (MTP) 包括（例如）行動裝置、相機、媒體播放器等。

例如，透過這種方式，您可以僅允許管理員群組使用卸除式媒體。對於其他裝置類型，您可以拒絕或允許所有使用者存取。您還可以 設定使用者使用印表機的存取權限。

**如何在管理主控台 (MMC) 中設定使用者對儲存裝置上的資料的存取權限**

1. 開啟卡巴斯基安全管理中心管理主控台。
2. 在主控台樹狀目錄中，選擇**"政策"**。
3. 選擇必要的政策並點擊以開啟政策內容。
4. 在政策視窗中，選擇**"安全控制 → 裝置控制"**。
5. 在**裝置控制設定**下，選擇**裝置類型**標籤。
   **裝置類型** 頁簽顯示裝置控制類別中包括的所有裝置的存取規則。
6. 若要配置儲存裝置存取規則，請點擊兩下開啟規則清單。
7. 配置儲存裝置存取規則：
   a. 在**"存取規則"**塊中，點擊**"新增"**按鈕。
      這將開啟一個用於新增新儲存裝置存取規則的視窗。
   b. 在**規則的優先順序**欄位中，設定*規則寫入*優先順序。規則包括以下屬性：使用者帳戶，排程，權限（讀取/寫入）和優先順序。
      規則具有特定的優先順序。如果已將使用者新增到多個群組，則 Kaspersky Endpoint Security 會根據具有最高優先順序的規則來管理裝置存取。Kaspersky Endpoint Security 允許您分配從 0 到 10,000 的優先順序。值越高，優先順序越高。換言之，值為 0 的項目具有最低的優先順序。

例如，您可以向 Everyone 群組授予只讀權限，向管理員群組授予讀/寫權限。為此，請為管理員群組分配優先順序 1，為 Everyone 群組分配優先順序 0。

封鎖規則的優先等級高於允許規則的優先等級。換句話說，如果已將使用者新增到多個群組，並且所有規則的優先順序都相同，則 Kaspersky Endpoint Security 會根據任何現有的封鎖規則來管理裝置存取。

c. 在**"使用者和/或使用者群組規則"**，選擇使用者或使用者群組。您可以在 Active Directory 中、在卡巴斯基安全管理中心的账户清單中或透過手動輸入本機使用者名稱來選擇使用者。卡巴斯基建議僅在無法使用網域使用者帳戶的特殊情況下使用本機使用者帳戶。

d. 點擊**"確定"**。

8. 在**"所選存取規則的排程"**下方，設定使用者的儲存裝置存取排程。

例如，您可以允許使用者僅在工作時間使用儲存裝置。

9. 在檔案管理器中配置使用者對儲存裝置的存取權限（**讀取 / 寫入**）。

10. 儲存變更。若要在電腦上套用該政策，請關閉掛鎖。

**如何在網頁主控台和雲端主控台中設定使用者對儲存裝置上資料的存取權限**

1. 在網頁主控台的主視窗中，選擇**資產（裝置）→ 政策和設定檔**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**"安全控制"→"裝置控制"**。

5. 在 **裝置存取規則** 塊中，在存取規則表中，開啟儲存裝置的存取規則的屬性。

6. 在**"裝置存取規則"**塊中，選取**"自訂"**。

7. 配置儲存裝置存取規則：

a. 在**"使用者及其權限"**塊中，點擊**"新增"**按鈕。

這將開啟一個用於新增新儲存裝置存取規則的視窗。

b. 在**優先順序**欄位中，設定*規則寫入*優先順序。規則包括以下屬性：使用者帳戶，排程，權限（讀取/寫入）和優先順序。

規則具有特定的優先順序。如果已將使用者新增到多個群組，則 Kaspersky Endpoint Security 會根據具有最高優先順序的規則來管理裝置存取。Kaspersky Endpoint Security 允許您分配從 0 到 10,000 的優先順序。值越高，優先順序越高。換言之，值為 0 的項目具有最低的優先順序。

例如，您可以向 Everyone 群組授予只讀權限，向管理員群組授予讀/寫權限。為此，請為管理員群組分配優先順序 1，為 Everyone 群組分配優先順序 0。

封鎖規則的優先等級高於允許規則的優先等級。換句話說，如果已將使用者新增到多個群組，並且所有規則的優先順序都相同，則 Kaspersky Endpoint Security 會根據任何現有的封鎖規則來管理裝置存取。

c. 在**"使用者或群組"**，選擇使用者或使用者群組。您可以在 Active Directory 中、在卡巴斯基安全管理中心的账户清單中或透過手動輸入本機使用者名稱來選擇使用者。卡巴斯基建議僅在無法使用網域使用者帳戶的特殊情況下使用本機使用者帳戶。

d. 在**"存取排程"**下方，設定使用者的儲存裝置存取排程。

例如，您可以允許使用者僅在工作時間使用儲存裝置。

e. 在檔案管理器中配置使用者對儲存裝置的存取權限（**讀取 / 寫入**）。

f. 點擊**"儲存"**。

8. 儲存變更。若要在電腦上套用該政策，請關閉掛鎖。

**如何在應用程式介面中設定使用者對儲存裝置上資料的存取權限**

1. 在"應用程式主視窗"中，點擊 按鈕。

2. 在應用程式設定視窗中，選取**"安全控制"→"裝置控制"**。

3. 在**"存取設定"**塊中，點擊**"裝置和 Wi-Fi 網路"**連接。

表格列出了"裝置控制"元件分類中存在的所有裝置的存取規則。

4. 若要配置行動裝置存取規則，請右鍵點擊滑鼠開啟規則清單。

5. 配置儲存裝置存取規則：

a. 在**"使用者權限"**塊中，點擊**"新增"**按鈕。

這將開啟一個用於新增新儲存裝置存取規則的視窗。

b. 在**優先**欄位中，設定*規則寫入*優先順序。規則包括以下屬性：使用者帳戶，排程，權限（讀取/寫入）和優先順序。

規則具有特定的優先順序。如果已將使用者新增到多個群組，則 Kaspersky Endpoint Security 會根據具有最高優先順序的規則來管理裝置存取。Kaspersky Endpoint Security 允許您分配從 0 到 10,000 的優先順序。值越高，優先順序越高。換言之，值為 0 的項目具有最低的優先順序。

例如，您可以向 Everyone 群組授予只讀權限，向管理員群組授予讀/寫權限。為此，請為管理員群組分配優先順序 1，為 Everyone 群組分配優先順序 0。

封鎖規則的優先等級高於允許規則的優先等級。換句話說，如果已將使用者新增到多個群組，並且所有規則的優先順序都相同，則 Kaspersky Endpoint Security 會根據任何現有的封鎖規則來管理裝置存取。

c. 在**"使用者"**，選擇使用者或使用者群組。您可以在 Active Directory 中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。

d. 點擊**"確定"**。

6. 在**"裝置存取排程"**下方，設定使用者的儲存裝置存取排程。

例如，您可以允許使用者僅在工作時間使用儲存裝置。

7. 在檔案管理器中配置使用者對儲存裝置的存取權限（**讀取 / 寫入**）。

8. 儲存變更。

## 區分使用者對可信任裝置的存取權限

*信任的裝置*是指在信任裝置設定中指定的使用者可隨時進行完全存取的裝置。要使用受信任裝置，您可以為單一使用者、一組使用者或組織的所有使用者授予存取權限。您可以配置 受信任裝置屬性中的使用者存取權限。

# 管理存取行動裝置的權限

Kaspersky Endpoint Security 允許您控制對執行 Android 和 iOS 的行動裝置上的資料的存取。行動裝置屬於攜帶式裝置 (MTP) 類別。因此，若要配置對行動裝置上的資料的存取，您需要編輯攜帶式裝置 (MTP) 的存取設定。

當某個行動裝置連線到電腦時，作業系統會確定裝置類型。如果電腦上安裝了Android Debug Bridge (ADB)、iTunes 或其等效應用程式，作業系統會將行動裝置辨識為 ADB 或 iTunes 裝置。在所有其他情況下，作業系統可能將行動裝置類型辨識為用於檔案傳輸的可攜式裝置 (MTP)、用於影像傳輸的 PTP 裝置（相機）或其他裝置。裝置類型取決於行動裝置的型號和所選的 USB 連線模式。Kaspersky Endpoint Security 可讓您在 ADB 應用程式、iTunes 或檔案管理器中為行動裝置上的資料配置單獨的存取權限。在所有其他情況下，裝置控制允許根據攜帶式裝置 (MTP) 存取規則存取行動裝置。

## 存取行動裝置的權限

行動裝置屬於攜帶式裝置 (MTP) 類別，因此它們的設定相同。您可以選擇以下行動裝置存取模式之一：

- **允許**。Kaspersky Endpoint Security 允許完整存取行動裝置。您可以使用檔案管理器或 ADB 和 iTunes 應用程式在行動裝置上開啟、建立、修改、複製或刪除檔案。您還可以通過將行動裝置連線到電腦的 USB 連接埠來為裝置的電池充電。
- **封鎖**。Kaspersky Endpoint Security 限制檔案管理器以及 ADB 和 iTunes 應用程式中對行動裝置的存取。該應用程式只允許存取"受信任行動裝置"。您還可以通過將行動裝置連線到電腦的 USB 連接埠來為裝置的電池充電。
- **取決於連線匯流排**。Kaspersky Endpoint Security 允許根據 USB 連線狀態（**允許**或 **封鎖**）連線到行動裝置。
- **按規則**。Kaspersky Endpoint Security 根據規則限制對行動裝置的存取。在規則中，您可以配置存取權限（讀/寫），選擇可以存取行動裝置 的使用者或使用者群組，並配置行動裝置的存取排程。您還可以透過 ADB 和 iTunes 應用程式限制對行動裝置上的資料的存取。

## 配置行動裝置存取規則

攜帶式裝置 (MTP)、ADB 裝置和 iTunes 裝置的存取規則配置不同。對於攜帶式裝置 (MTP) 和 ADB 裝置，您可以為單個使用者或使用者群組配置規則，並為何時套用規則建立排程。對於 iTunes 裝置，您不能這樣做。您只能允許或拒絕所有使用者透過 iTunes 應用程式存取資料。

### 如何在管理主控台 (MMC) 中配置行動裝置存取規則

1. 在卡巴斯基安全管理中心管理主控台樹狀目錄中，選取**政策**。
2. 選擇必要的政策並點擊以開啟政策內容。
3. 在政策視窗中，選擇"**安全控制 → 裝置控制**"。
4. 在**裝置控制設定**下，選擇**裝置類型**標籤。

   表格列出了"裝置控制"元件分類中存在的所有裝置的存取規則。

5. 在"**可攜式裝置(MTP)**"裝置類型的內容功能表中，配置行動裝置存取模式：**允許**，**封鎖**，或者**取決於連線匯流排**。

6. 若要配置行動裝置存取規則，請點擊兩下開啟規則清單。

7. 配置行動裝置存取規則：

   a. 在"**存取規則**"塊中，點擊"**新增**"按鈕。

   這將開啟一個用於新增新行動裝置存取規則的視窗。

   b. 在**優先**欄位中，設定規則寫入優先順序。規則包括以下屬性：使用者帳戶，排程，權限（讀取/寫入/ADB 存取）和優先順序。

   規則具有特定的優先順序。如果已將使用者新增到多個群組，則 Kaspersky Endpoint Security 會根據具有最高優先順序的規則來管理裝置存取。Kaspersky Endpoint Security 允許您分配從 0 到 10,000 的優先順序。值越高，優先順序越高。換言之，值為 0 的項目具有最低的優先順序。

   例如，您可以向 Everyone 群組授予只讀權限，向管理員群組授予讀/寫權限。為此，請為管理員群組分配優先順序 1，為 Everyone 群組分配優先順序 0。

   封鎖規則的優先等級高於允許規則的優先等級。換句話說，如果已將使用者新增到多個群組，並且所有規則的優先順序都相同，則 Kaspersky Endpoint Security 會根據任何現有的封鎖規則來管理裝置存取。

   c. 在"**使用者和/或使用者群組規則**"，選擇使用者或使用者群組。您可以在 Active Directory 中、在卡巴斯基安全管理中心的账户清單中或透過手動輸入本機使用者名稱來選擇使用者。卡巴斯基建議僅在無法使用網域使用者帳戶的特殊情況下使用本機使用者帳戶。

   d. 點擊"**確定**"。

8. 在"**所選存取規則的排程**"下方，設定使用者的行動裝置存取排程。

   無法為 ADB 裝置配置單獨的存取排程。您可以為 ADB 裝置和攜帶式裝置 (MTP) 配置通用存取排程。

9. 在檔案管理器中配置使用者對行動裝置的存取權限（**讀取 / 寫入**）。

10. 使用**透過 ADB 存取**核取方塊配置透過 ADB 應用程式對行動裝置上資料進行存取 。

    如果清除該核取方塊，當連線行動裝置時，ADB 應用程式將被阻止偵測該裝置。

11. 在**透過 iTunes 存取**下，配置透過 iTunes 應用程式對行動裝置上的資料進行存取。

    Kaspersky Endpoint Security 透過 iTunes 應用程式為所有使用者套用行動裝置存取設定。無法為 iTunes 裝置配置單獨的存取排程。

12. 儲存變更。

**如何在網頁主控台和雲端主控台中配置行動裝置存取規則**

1. 在網頁主控台的主視窗中，選擇**資產（裝置）→ 政策和設定檔**。

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"**裝置存取規則**"塊中，點擊"**裝置和 Wi-Fi 網路**"連接。

   表格列出了"裝置控制"元件分類中存在的所有裝置的存取規則。

6. 選取"**可攜式裝置(MTP)**"裝置類型。

   這將開啟攜帶式裝置 (MTP) 存取權限。

7. 配置行動裝置存取模式：**允許**, **封鎖**, **取決於匯流排**, or **自訂**。

8. 使用**「所有使用者透過 iTunes 存取」已啟用**切換開關配置透過 iTunes 應用程式對行動裝置上的資料進行存取。

   Kaspersky Endpoint Security 透過 iTunes 應用程式為所有使用者套用行動裝置存取設定。無法為 iTunes 裝置配置單獨的存取排程。

9. 如果選擇"**自訂**"模式，必須為裝置新增存取規則。為此，在"**使用者及其權限**"下方，點擊"**新增**"按鈕並配置行動裝置存取規則：

   a. 在**優先順序**欄位中，設定規則寫入優先順序。規則包括以下屬性：使用者帳戶，排程，權限（讀取/寫入/ADB 存取）和優先順序。

      規則具有特定的優先順序。如果已將使用者新增到多個群組，則 Kaspersky Endpoint Security 會根據具有最高優先順序的規則來管理裝置存取。Kaspersky Endpoint Security 允許您分配從 0 到 10,000 的優先順序。值越高，優先順序越高。換言之，值為 0 的項目具有最低的優先順序。

      例如，您可以向 Everyone 群組授予只讀權限，向管理員群組授予讀/寫權限。為此，請為管理員群組分配優先順序 1，為 Everyone 群組分配優先順序 0。

      封鎖規則的優先等級高於允許規則的優先等級。換句話說，如果已將使用者新增到多個群組，並且所有規則的優先順序都相同，則 Kaspersky Endpoint Security 會根據任何現有的封鎖規則來管理裝置存取。

   b. 在"**使用者或群組**"下方，選擇存取行動裝置的使用者或者使用者群組。您可以在 Active Directory 中、在卡巴斯基安全管理中心的账户清單中或透過手動輸入本機使用者名稱來選擇使用者。卡巴斯基建議僅在無法使用網域使用者帳戶的特殊情況下使用本機使用者帳戶。

   c. 在"**存取排程**"下方，設定使用者的行動裝置存取排程。

      無法為 ADB 裝置配置單獨的存取排程。您可以為 ADB 裝置和攜帶式裝置 (MTP) 配置通用存取排程。

   d. 在檔案管理器中配置使用者對行動裝置的存取權限（**讀取 / 寫入**）。

   e. 使用**透過 ADB 存取**核取方塊配置透過 ADB 應用程式對行動裝置上資料進行存取 。

      如果清除該核取方塊，當連線行動裝置時，ADB 應用程式將被阻止偵測該裝置。

10. 儲存變更。

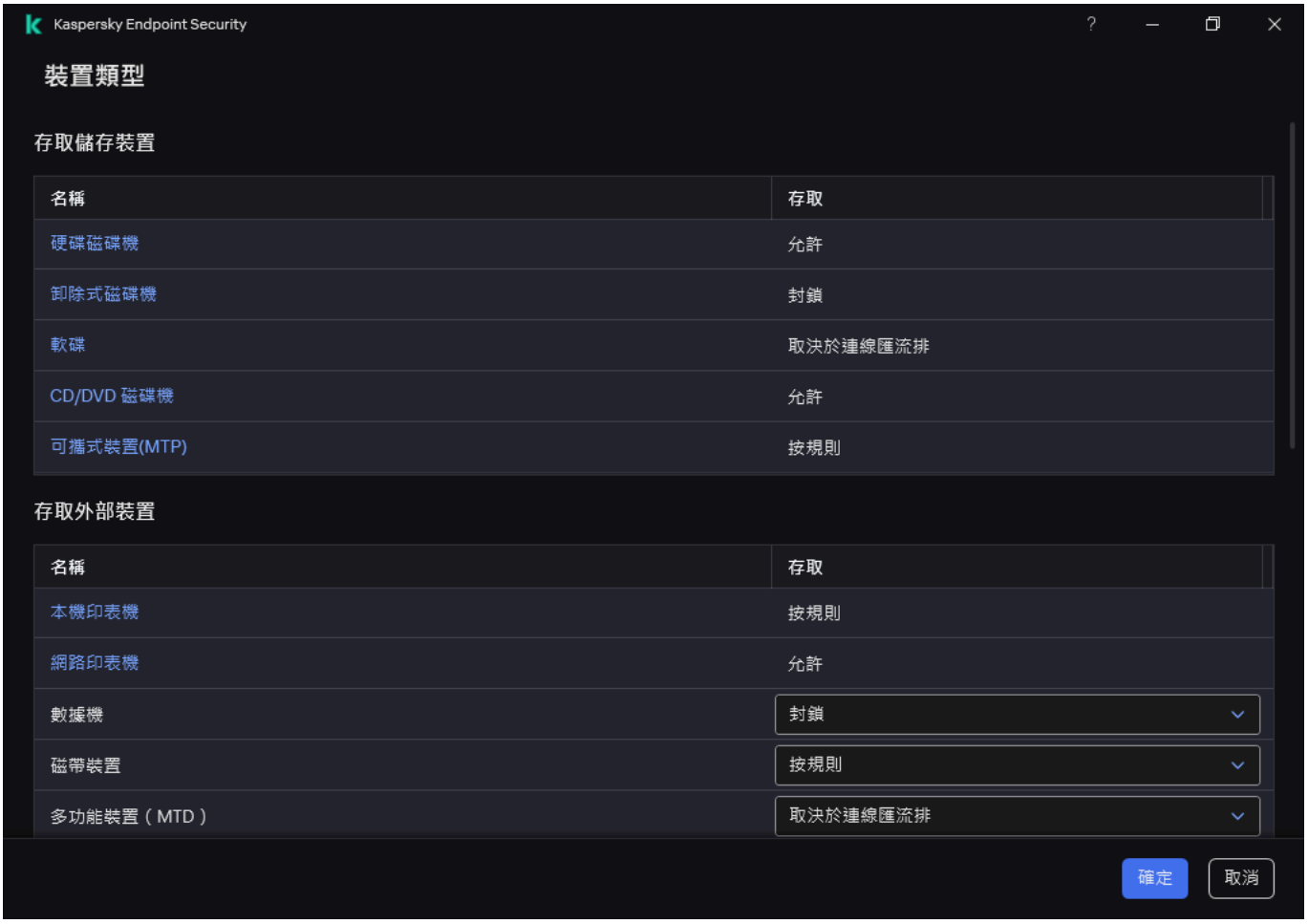
**如何在應用程式介面中配置行動裝置存取規則**

1. 在"應用程式主視窗"中，點擊⚙ 按鈕。

2. 在應用程式設定視窗中，選取"**安全控制**"→"**裝置控制**"。

3. 在"**存取設定**"塊中，點擊"**裝置和 Wi-Fi 網路**"按鈕。

開啟的視窗顯示了裝置控制元件類別中包括的所有裝置的存取規則。




裝置控制元件中的裝置類型

4. 在"**存取儲存裝置**"塊中，點擊"**可攜式裝置(MTP)**"連接。

   這將開啟一個包含攜帶式裝置 (MTP) 存取規則的視窗。

5. 在"**存取**"下方，配置行動裝置存取模式：**允許**，**封鎖**，**取決於連線匯流排**，或者**按規則**。

6. 如果選擇"**按規則**"模式，必須為裝置新增存取規則：

   a. 在"**使用者權限**"塊中，點擊"**新增**"按鈕。

      這將開啟一個用於新增新行動裝置存取規則的視窗。

   b. 在**優先**欄位中，設定規則寫入優先順序。規則包括以下屬性：使用者帳戶，排程，權限（讀取/寫入/ADB 存取）和優先順序。

      規則具有特定的優先順序。如果已將使用者新增到多個群組，則 Kaspersky Endpoint Security 會根據具有最高優先順序的規則來管理裝置存取。Kaspersky Endpoint Security 允許您分配從 0 到 10,000 的優先順序。值越高，優先順序越高。換言之，值為 0 的項目具有最低的優先順序。

      例如，您可以向 Everyone 群組授予只讀權限，向管理員群組授予讀/寫權限。為此，請為管理員群組分配優先順序 1，為 Everyone 群組分配優先順序 0。

      封鎖規則的優先等級高於允許規則的優先等級。換句話說，如果已將使用者新增到多個群組，並且所有規則的優先順序都相同，則 Kaspersky Endpoint Security 會根據任何現有的封鎖規則來管理裝置存取。

   c. 在"**狀況**"下方，開啟行動裝置存取規則。

d. 在“**存取規則**”下方，為使用者配置行動裝置存取權限。

- 在檔案管理器中配置使用者對行動裝置的存取權限（**讀取 / 寫入**）。
- 使用**透過 ADB 存取**核取方塊配置透過 ADB 應用程式對行動裝置上資料進行存取 。

  如果清除該核取方塊，當連線行動裝置時，ADB 應用程式將被阻止偵測該裝置。

e. 在“**使用者**”下方，選擇存取行動裝置的使用者或者使用者群組。您可以在 Active Directory 中、在卡巴斯基安全管理中心的账户清單中或透過手動輸入本機使用者名稱來選擇使用者。卡巴斯基建議僅在無法使用網域使用者帳戶的特殊情況下使用本機使用者帳戶。

f. 在“**裝置存取排程**”下方，設定使用者的裝置存取排程。

> 無法為 ADB 裝置配置單獨的存取排程。您可以為 ADB 裝置和攜帶式裝置 (MTP) 配置通用存取排程。

g. 在**透過 iTunes 存取**下，配置透過 iTunes 應用程式對行動裝置上的資料進行存取。

> Kaspersky Endpoint Security 透過 iTunes 應用程式為所有使用者套用行動裝置存取設定。無法為 iTunes 裝置配置單獨的存取排程。

7. 儲存變更。

結果，使用者對行動裝置的存取會根據規則受到限制。如果您在 ADB 和 iTunes 應用程式中禁止存取行動裝置，當您連線行動裝置時，ADB 和 iTunes 應用程式將被禁止偵測該行動裝置。

## 受信任行動裝置

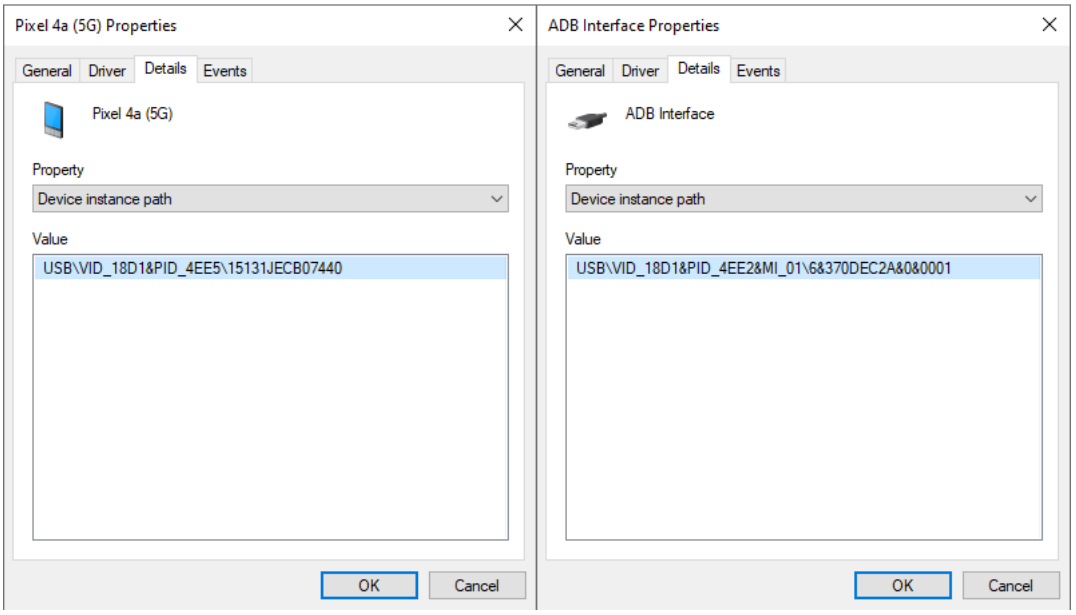
*信任的裝置*是指在信任裝置設定中指定的使用者可隨時進行完全存取的裝置。

新增受信任行動裝置的過程和新增其它類型受信任裝置的過程一模一樣。您可以依據 ID 或者裝置型號新增行動裝置。

若要依據 ID 新增受信任行動裝置，您將需要一個唯一 ID（Hardware ID – HWID）。您可以使用作業系統工具在裝置內容中找到 ID（請見下圖）。裝置管理器工具可讓您做到這點。攜帶式裝置（MTP）和 ADB、iTunes 裝置的 ID 即使對於同一個行動裝置也不同。攜帶式裝置 (MTP) 的 ID 可能如下所示：`15131JECB07440`。ADB 裝置的 ID 可能如下所示：`6&370DEC2A&0&0001`。如果要新增多個特定裝置，則按 ID 新增裝置很方便。您也可以使用遮罩。

> 如果在將裝置連線到電腦後安裝了 ADB 或 iTunes 應用程式，則該裝置的唯一 ID 可能會重設。這意味著 Kaspersky Endpoint Security 會將此裝置識別為新裝置。如果該裝置受信任，請再次將其新增至受信任清單。

若要按裝置型號新增受信任行動裝置，您將需要其Vendor ID (VID) 和 Product ID (PID)。您可以使用作業系統工具在裝置內容中找到 ID（請見下圖）。用於輸入 VID 和 PID 的範本：`VID_18D1&PID_4EE5`。如果在組織中使用特定型號的裝置，則按型號新增裝置很方便。這樣，您可以新增該型號的所有裝置。




裝置管理器中的裝置 ID

# 管理存取藍牙裝置的權限

Kaspersky Endpoint Security 允許管理對藍牙裝置的存取。藍牙裝置包括無線鍵盤、滑鼠、耳機、印表機等。您還可以使用藍牙進行通信，例如與行動裝置通信。

當藍牙裝置連線或斷開連線時，應用程式可能會建立有關該裝置的多個事件。原因是作業系統可能會將一個藍牙裝置偵測為多個不同類型的裝置。Kaspersky Endpoint Security 還管理藍牙適配器，通過該適配器將裝置作為單獨的裝置進行連線。這就是應用程式為每個偵測到的裝置建立一個事件的原因。

您可以選擇以下藍牙裝置存取模式之一：

- **允許且不記錄**。Kaspersky Endpoint Security 允許連線任何藍牙裝置，不會在事件日誌中儲存有關連線的資訊。您可以連線藍牙輸入裝置（鍵盤、滑鼠等）、通過藍牙傳送資料、管理其他藍牙裝置（耳機等）。
- **允許**。Kaspersky Endpoint Security 允許連線任何藍牙裝置。您可以連線藍牙輸入裝置（鍵盤、滑鼠等）、通過藍牙傳送資料、管理其他藍牙裝置（耳機等）。
- **封鎖**Kaspersky Endpoint Security 將限制對藍牙裝置的存取。您可以僅允許連線藍牙輸入裝置 Human Interface Devices 類別）。這些裝置包括鍵盤、滑鼠裝置、操縱桿等。

無法建立受信任的藍牙裝置清單。如果您限制了對藍牙裝置的存取，則只能連線藍牙輸入裝置。

### 如何在管理主控台 (MMC) 中配置藍牙裝置存取規則

1. 在卡巴斯基安全管理中心管理主控台樹狀目錄中，選取**政策**。
2. 選擇必要的政策並點擊以開啟政策內容。

3. 在政策視窗中，選擇“**安全控制 → 裝置控制**”。

4. 在**裝置控制設定**下，選擇**裝置類型**標籤。
   表格列出了“裝置控制”元件分類中存在的所有裝置的存取規則。

5. 在“**藍芽**”裝置類型的內容功能表中，配置藍牙裝置存取模式：**允許**，**封鎖**，**允許且不記錄**。

6. 儲存變更。

**如何在網頁主控台和雲端主控台中配置藍牙裝置存取規則**

1. 在網頁主控台的主視窗中，選擇**資產（裝置）→ 政策和設定檔**。

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”**裝置存取規則**”塊中，點擊”**裝置和 Wi-Fi 網路**”連接。
   表格列出了“裝置控制”元件分類中存在的所有裝置的存取規則。

6. 選取“**藍牙裝置**”裝置類型。
   這將開啟藍牙裝置存取設定。

7. 配置藍牙裝置存取模式：**允許**，**封鎖**，**允許且不記錄**。

8. 如果選擇**封鎖**模式，您可以允許只連線藍牙輸入裝置（鍵盤、滑鼠等）。為此，在 **排除項目** 下面，選擇 **輸入裝置（滑鼠和鍵盤）** 核取方塊。

9. 儲存變更。

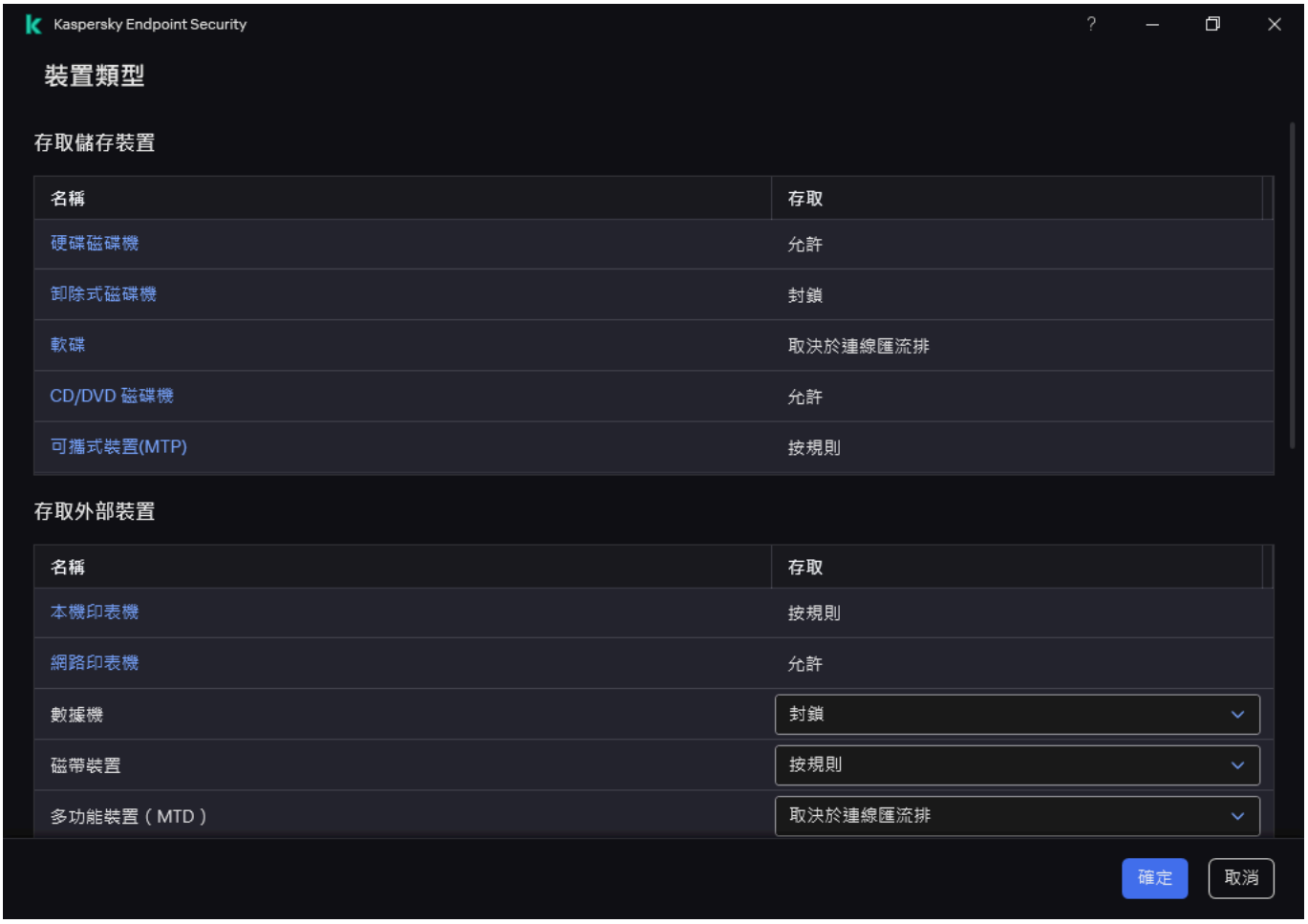
**如何在應用程式介面中配置藍牙裝置存取規則**

1. 在“應用程式主視窗”中，點擊 按鈕。

2. 在應用程式設定視窗中，選取”**安全控制**“→“**裝置控制**”。

3. 在”**存取設定**”塊中，點擊”**裝置和 Wi-Fi 網路**”按鈕。

開啟的視窗顯示了裝置控制元件類別中包括的所有裝置的存取規則。




裝置控制元件中的裝置類型

4. 在"**存取外部裝置**"塊中，點擊"**藍芽**"連接。
   這將開啟藍牙裝置存取設定。

5. 在**存取**下配置藍牙裝置存取模式：**允許**，**封鎖**，**允許且不記錄**。

6. 如果選擇**封鎖**模式，您可以允許只連線藍牙輸入裝置（鍵盤、滑鼠等）。為此，在 **排除項目** 下面，選擇 **輸入裝置（滑鼠和鍵盤）** 核取方塊。

7. 儲存變更。

# 列印控制

您可以使用列印控制來設定使用者對本機和網路印表機的存取。

## 本機印表機控制

Kaspersky Endpoint Security 允許在兩個級別設定對本機印表機的存取：*連線*和*列印*。

Kaspersky Endpoint Security 透過以下匯流排控制本機印表機連線：USB，序列連接埠 (COM)，平行連接埠 (LPT)。

Kaspersky Endpoint Security 僅在匯流排級別控製本機印表機與 COM 和 LPT 連接埠的連線。因此，要防止透過 COM 和 LPT 連接埠連接印表機，您需要 選擇 取決於連線匯流排 本機印表機的存取模式 和 禁止連線到 COM 和 LPT 匯流排。

對於連線到 USB 的印表機，應用程式會在兩個級別上進行控制：裝置類型（本機印表機）和連線匯流排（USB）。

您可以選擇以下方式之一透過 USB 存取本機印表機：

- **允許**。Kaspersky Endpoint Security 向所有使用者授予對本機印表機的完整存取權限。使用者可以使用作業系統提供的方式連線印表機和列印文件。
- **封鎖**。Kaspersky Endpoint Security 封鎖連線本機印表機。應用程式僅允許連線受信任印表機。
- **取決於連線匯流排**。Kaspersky Endpoint Security 允許根據 USB 連線狀態（**允許**或 **封鎖**）連線到本機印表機。
- **按規則**。若要控制列印，您必須新增*列印規則*。在規則中，您可以選擇要允許或封鎖其存取在本機印表機上列印文件的使用者或使用者群組。

網路印表機控制

Kaspersky Endpoint Security 允許設定在網路印表機上列印的存取權限。您可以選擇以下一種網路印表機存取模式：

- **允許且不記錄**。Kaspersky Endpoint Security 不控製網路印表機上的列印。該應用程式向所有使用者授予列印存取權限，不會將列印資訊儲存到事件日誌中。
- **允許**。Kaspersky Endpoint Security 向所有使用者授予在網路印表機上列印的存取權限。
- **封鎖**。Kaspersky Endpoint Security 向所有使用者限制對網路印表機的存取權限。應用程式僅允許存取受信任印表機。
- **按規則**。Kaspersky Endpoint Security 根據列印規則授予列印存取權限。在規則中，您可以選擇被允許或者防止在網路印表機上列印文件的使用者或者使用者群組。

為印表機新增列印規則

**如何在管理主控台 (MMC) 中新增列印規則**

1. 在卡巴斯基安全管理中心管理主控台樹狀目錄中，選取**政策**。
2. 選擇必要的政策並點擊以開啟政策內容。
3. 在政策視窗中，選擇“**安全控制 → 裝置控制**”。

4. 在**裝置控制設定**下，選擇**裝置類型**標籤。

   表格列出了"裝置控制"元件分類中存在的所有裝置的存取規則。

5. 在"**本機印表機**"和"**網路印表機**"裝置類型的內容功能表中，為相關印表機設定存取模式：**允許**，**封鎖**，**允許且不記錄**（僅適用於網路印表機）或 **取決於連線匯流排**（僅適用於本機印表機）。

6. 若要設定本機和網路印表機上的列印規則，點擊兩下規則清單開啟它們。

7. 選擇"**按規則**"作為印表機存取模式。

8. 選擇要對其套用列印規則的使用者或使用者群組。

   a. 點擊"**新增**"。

      這將開啟一個用於新增新列印規則的視窗。

   b. 將優先順序分配到規則項目。一個規則項目包括以下屬性：使用者帳戶，動作（允許/封鎖）和優先順序。

      規則具有特定的優先順序。如果已將使用者新增到多個群組，則 Kaspersky Endpoint Security 會根據具有最高優先順序的規則來管理裝置存取。Kaspersky Endpoint Security 允許您分配從 0 到 10,000 的優先順序。值越高，優先順序越高。換言之，值為 0 的項目具有最低的優先順序。

      例如，您可以向 Everyone 群組授予只讀權限，向管理員群組授予讀/寫權限。為此，請為管理員群組分配優先順序 1，為 Everyone 群組分配優先順序 0。

      封鎖規則的優先等級高於允許規則的優先等級。換句話說，如果已將使用者新增到多個群組，並且所有規則的優先順序都相同，則 Kaspersky Endpoint Security 會根據任何現有的封鎖規則來管理裝置存取。

   c. 在"**動作**"下方，設定使用者在印表機上列印的存取權限。

   d. 點擊"**使用者和群組**"然後選擇存取列印的使用者或者使用者群組。您可以在 Active Directory 中、在卡巴斯基安全管理中心的账户清單中或透過手動輸入本機使用者名稱來選擇使用者。卡巴斯基建議僅在無法使用網域使用者帳戶的特殊情況下使用本機使用者帳戶。

   e. 點擊"**確定**"。

9. 儲存變更。

**如何在網頁主控台和雲端主控台中新增列印規則**

1. 在網頁主控台的主視窗中，選擇**資產（裝置）→政策和設定檔**。

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"**裝置存取規則**"塊中，點擊"**裝置和 Wi-Fi 網路**"連接。

   表格列出了"裝置控制"元件分類中存在的所有裝置的存取規則。

6. 選擇"**本機印表機**"或者"**網路印表機**"裝置類型。

   這將開啟印表機存取規則。

7. 配置相關印表機的存取模式：**允許**，**封鎖**，**允許且不記錄**（僅適用於網路印表機），**取決於匯流排**（僅適用於本機印表機）或 **自訂**。

8. 如果選擇“**自訂**”模式，您必須為本機或者網路印表機新增列印規則。為此，請點擊列印規則表中的“**新增**”按鈕。

   這將開啟新列印規則的設定。

9. 將優先順序分配到規則項目。一個規則項目包括以下屬性：使用者帳戶，動作（允許/封鎖）和優先順序。

   規則具有特定的優先順序。如果已將使用者新增到多個群組，則 Kaspersky Endpoint Security 會根據具有最高優先順序的規則來管理裝置存取。Kaspersky Endpoint Security 允許您分配從 0 到 10,000 的優先順序。值越高，優先順序越高。換言之，值為 0 的項目具有最低的優先順序。

   例如，您可以向 Everyone 群組授予只讀權限，向管理員群組授予讀/寫權限。為此，請為管理員群組分配優先順序 1，為 Everyone 群組分配優先順序 0。

   封鎖規則的優先等級高於允許規則的優先等級。換句話說，如果已將使用者新增到多個群組，並且所有規則的優先順序都相同，則 Kaspersky Endpoint Security 會根據任何現有的封鎖規則來管理裝置存取。

10. 在“**操作**”下方，設定使用者在印表機上列印的存取權限。

11. 在“**使用者或群組**”下方，選擇存取列印的使用者或者使用者群組。您可以在 Active Directory 中、在卡巴斯基安全管理中心的账户清單中或透過手動輸入本機使用者名稱來選擇使用者。卡巴斯基建議僅在無法使用網域使用者帳戶的特殊情況下使用本機使用者帳戶。

12. 儲存變更。

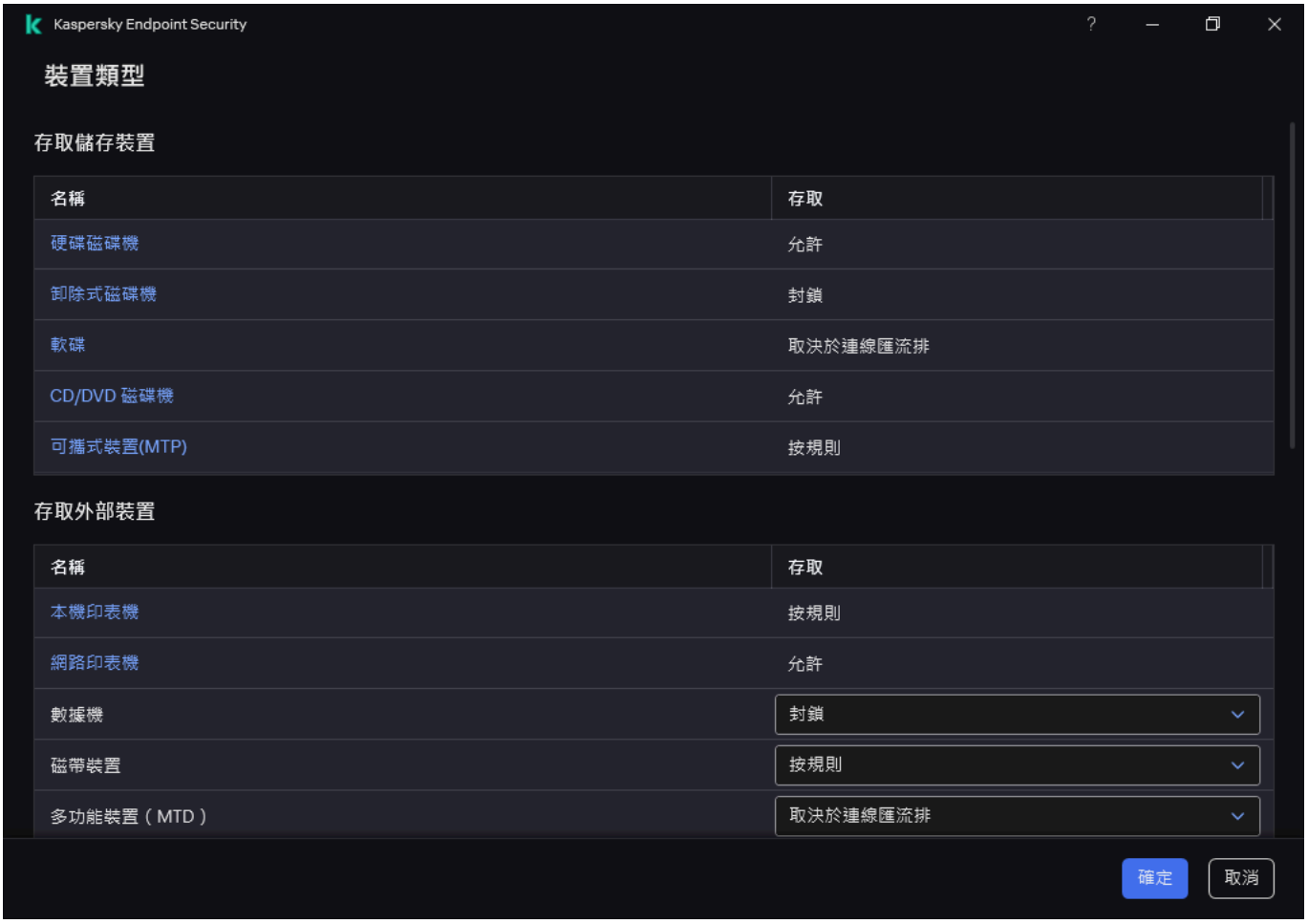
**如何在應用程式介面中新增列印規則**

1. 在“應用程式主視窗”中，點擊⚙ 按鈕。

2. 在應用程式設定視窗中，選取”**安全控制**“→“**裝置控制**”。

3. 在”**存取設定**”塊中，點擊”**裝置和 Wi-Fi 網路**”按鈕。

開啟的視窗顯示了裝置控制元件類別中包括的所有裝置的存取規則。




裝置控制元件中的裝置類型

4. 在“**存取外部裝置**”下方，點擊**本機印表機**或者**網路印表機**。

   這將開啟一個視窗，其中包含印表機存取規則。

5. 在**本機印表機存取** 或 **網路印表機存取**下面配置相關印表機的存取模式：**允許**，**封鎖**，**允許且不記錄**（僅適用於網路印表機），**取決於連線匯流排**（僅適用於本機印表機）或 **按規則**。

6. 如果選擇“**按規則**”模式，必須為印表機新增列印規則。選擇要對其套用列印規則的使用者或使用者群組。

   a. 點擊“**新增**”。

      這將開啟一個用於新增新列印規則的視窗。

   b. 將優先順序分配到規則項目。規則包括以下屬性：使用者帳戶，權限（允許/封鎖）和優先順序。

      規則具有特定的優先順序。如果已將使用者新增到多個群組，則 Kaspersky Endpoint Security 會根據具有最高優先順序的規則來管理裝置存取。Kaspersky Endpoint Security 允許您分配從 0 到 10,000 的優先順序。值越高，優先順序越高。換言之，值為 0 的項目具有最低的優先順序。

      例如，您可以向 Everyone 群組授予只讀權限，向管理員群組授予讀/寫權限。為此，請為管理員群組分配優先順序 1，為 Everyone 群組分配優先順序 0。

      封鎖規則的優先等級高於允許規則的優先等級。換句話說，如果已將使用者新增到多個群組，並且所有規則的優先順序都相同，則 Kaspersky Endpoint Security 會根據任何現有的封鎖規則來管理裝置存取。

c. 在“**操作**”下方，設定存取列印的使用者權限。

d. 在“**使用者和群組**”下方，選擇存取列印的使用者或者使用者群組。您可以在 Active Directory 中、在卡巴斯基安全管理中心的账户清單中或透過手動輸入本機使用者名稱來選擇使用者。卡巴斯基建議僅在無法使用網域使用者帳戶的特殊情況下使用本機使用者帳戶。

7. 儲存變更。

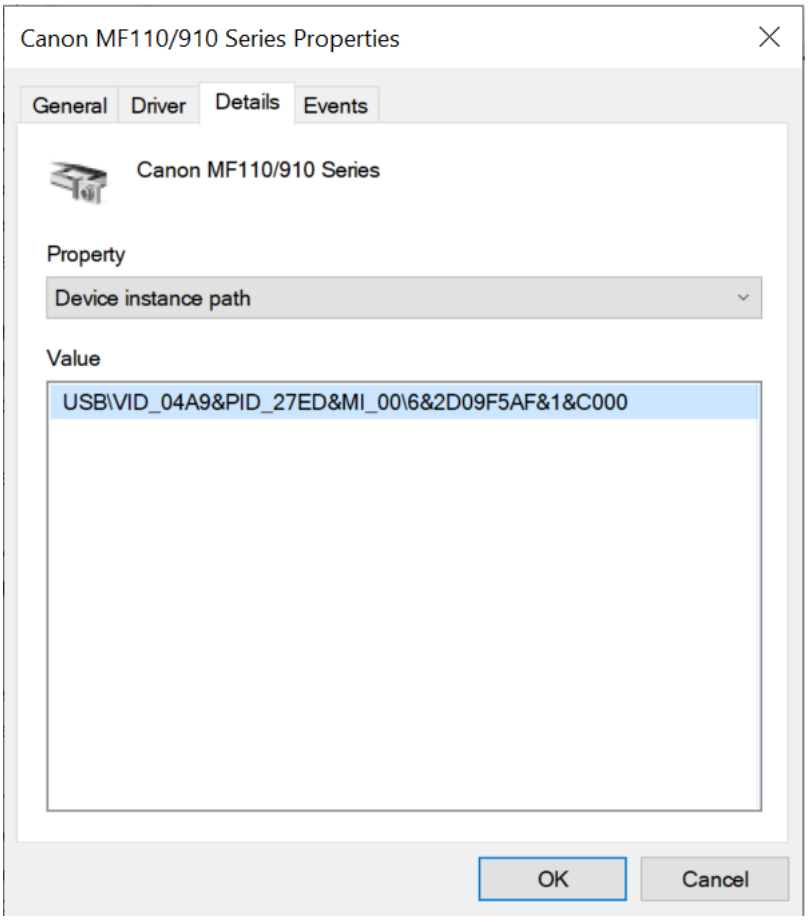
## 受信任印表機

*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。

新增受信任印表機的過程和新增其它類型受信任裝置的過程一模一樣。您可以依據 ID 或者裝置型號新增本機印表機。您只能依據裝置 ID 新增網路印表機。

若要依據 ID 新增受信任本機印表機，您將需要一個唯一 ID（Hardware ID – HWID）。您可以使用作業系統工具在裝置內容中找到 ID（請見下圖）。Device Manager工具可讓您做到這點。本機印表機的 ID 看起來可能是這樣：`6&2D09F5AF&1&C000`。如果要新增多個特定裝置，則按 ID 新增裝置很方便。您也可以使用遮罩。

若要按裝置型號新增受信任本機印表機，您將需要其Vendor ID (VID) 和 Product ID (PID)。您可以使用作業系統工具在裝置內容中找到 ID（請見下圖）。用於輸入 VID 和 PID 的範本：`VID_04A9&PID_27FD`。如果在組織中使用特定型號的裝置，則按型號新增裝置很方便。這樣，您可以新增該型號的所有裝置。




裝置管理器中的裝置 ID

若要新增受信任網路印表機，您將需要其裝置 ID。對於網路印表機，裝置 ID 可以是印表機的網路名稱（共用印表機的名稱），印表機的 IP 位址，或者印表機的 URL。

# Wi-Fi 連線控制

裝置控制可讓您管理電腦（膝上型電腦）的 Wi-Fi 連線。公共 Wi-Fi 網路可能不安全，使用此類網路可能導致資料損失。裝置控制可讓您封鎖使用者連線到 Wi-Fi 或者只允許連線到受信任網路。例如，您可以允許只連線到足夠安全的公司 Wi-Fi 網路。裝置控制將封鎖存取除受信任清單中指定的 Wi-Fi 網路之外的所有網路。

在執行 Windows 11 的電腦上，您需要啟用位置服務才能控制 Wi-Fi 連線。為此，您需要在作業系統設定中啟用**定位服務**開關（**設定 → 隱私權 → 位置的**）。如果位置服務被停用，Kaspersky Endpoint Security 不會控制與 Wi-Fi 網路的連線。

**如何在管理主控台 (MMC) 中限制 Wi-Fi 連線**

1. 在卡巴斯基安全管理中心管理主控台樹狀目錄中，選取**政策**。
2. 選擇必要的政策並點擊以開啟政策內容。
3. 在政策視窗中，選擇"**安全控制 → 裝置控制**"。
4. 在**裝置控制設定**下，選擇**裝置類型**標籤。

   表格列出了"裝置控制"元件分類中存在的所有裝置的存取規則。
5. 在 **Wi-Fi** 裝置類型的內容功能表中，選擇連線到 Wi-Fi 時採取的裝置控制動作：**允許** ()，**封鎖** ()，或者**封鎖但帶有例外** ()。
6. 如果選擇了"**封鎖但帶有例外**"選項，請建立一個受信任 Wi-Fi 網路的清單：

   a. 點擊兩下開啟受信任 Wi-Fi 網路列表。

   b. 在"**受信任的 Wi-Fi 網路**"塊中，點擊"**新增**"按鈕。

   c. 這會開啟一個視窗；在此視窗中設定受信任的 Wi-Fi 網路（請見下圖）：

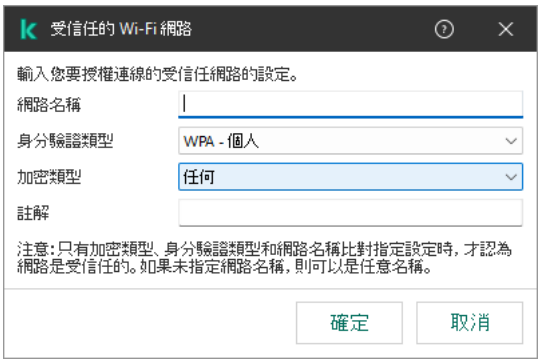
   - **網路名稱**Wi-Fi 的名稱或者 SSID（Service Set Identifier）。
   - **身分驗證類型**連線到 Wi-Fi 網路時使用的身分驗證類型。

     從 Kaspersky Endpoint Security for Windows 版本 12.0 開始，WPA3 協定支援已新增到應用程式中。如果在電腦上套用 Kaspersky Endpoint Security 12.2 政策，則在電腦上對於 Kaspersky Endpoint Security 11.11.0 及更早版本選擇 WPA2 協定；對於 12.0 到 12.1 版本選擇 WPA2 / WPA3；對於 12.2 及更高版本選擇 WPA3。
   - **加密類型**用於防護 Wi-Fi 流量的加密類型。
   - **註解**有關新增 Wi-Fi 網路的更多資訊。

   您可以在路由器設定中檢視受信任 Wi-Fi 網路的設定。

   如果某個 Wi-Fi 網路的設定比對規則中指定的所有設定則其被認定為受信任。

7. 儲存變更。




受信任 Wi-Fi 網路設定

### 如何在網頁主控台和雲端主控台中限制 Wi-Fi 連線

1. 在網頁主控台的主視窗中，選擇**資產（裝置）→政策和設定檔**。
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**裝置存取規則**下，選擇**裝置和 Wi-Fi 網路**標籤。
   表格列出了"裝置控制"元件分類中存在的所有裝置的存取規則。
6. 在"**Wi-Fi 網路**"塊中，點擊"**Wi-Fi**"連接。
7. 在開啟的視窗中，選擇連線到 Wi-Fi 時採取的裝置控制動作：**允許**，**封鎖**，或者 **封鎖但帶有例外**。
8. 如果選擇了"**封鎖但帶有例外**"選項，請建立一個受信任 Wi-Fi 網路的清單：
   a. 點擊兩下開啟受信任 Wi-Fi 網路列表。
   b. 在"**受信任的 Wi-Fi 網路**"塊中，點擊"**新增**"按鈕。
   c. 這會開啟一個視窗；在此視窗中設定受信任的 Wi-Fi 網路（請見下圖）：
      - **名稱**Wi-Fi 的名稱或者 SSID（Service Set Identifier）。
      - **身分驗證類型**連線到 Wi-Fi 網路時使用的身分驗證類型。

        從 Kaspersky Endpoint Security for Windows 版本 12.0 開始，WPA3 協定支援已新增到應用程式中。如果在電腦上套用 Kaspersky Endpoint Security 12.2 政策，則在電腦上對於 Kaspersky Endpoint Security 11.11.0 及更早版本選擇 WPA2 協定；對於 12.0 到 12.1 版本選擇 WPA2 / WPA3；對於 12.2 及更高版本選擇 WPA3。

      - **加密類型**用於防護 Wi-Fi 流量的加密類型。
      - **註釋**有關新增 Wi-Fi 網路的更多資訊。

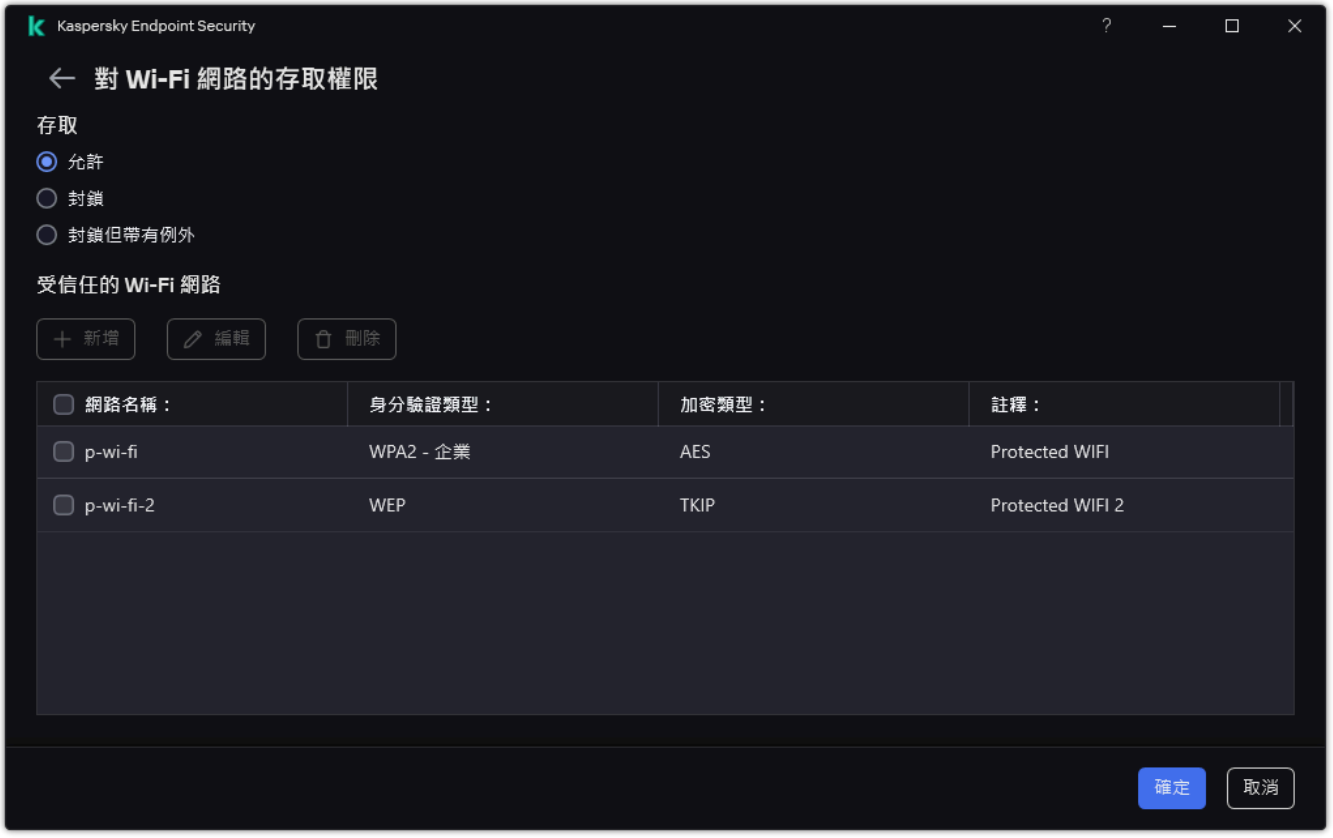
   您可以在路由器設定中檢視受信任 Wi-Fi 網路的設定。

如果某個 Wi-Fi 網路的設定比對規則中指定的所有設定則其被認定為受信任。

9. 儲存變更。

**如何在應用程式介面中限制 Wi-Fi 連線**

1. 在“應用程式主視窗”中，點擊⚙ 按鈕。
2. 在應用程式設定視窗中，選取”**安全控制**“→“**裝置控制**”。
3. 在”**存取設定**”塊中，點擊”**裝置和 Wi-Fi 網路**”按鈕。
   開啟的視窗顯示了裝置控制元件類別中包括的所有裝置的存取規則。
4. 在”**對 Wi-Fi 網路的存取權限**”塊中，點擊”**Wi-Fi**”連接。
   開啟的視窗將顯示 Wi-Fi 網路存取規則。




Wi-Fi 存取設定

5. 在“**存取**”下面，選擇連線到 Wi-Fi 時採取的裝置控制動作：**允許**，**封鎖**，或者 **封鎖但帶有例外**。

6. 如果選擇了**"封鎖但帶有例外"**選項，請建立一個受信任 Wi-Fi 網路的清單：

   a. 在**"受信任的 Wi-Fi 網路"**塊中，點擊**"新增"**按鈕。

   b. 這會開啟一個視窗；在此視窗中設定受信任的 Wi-Fi 網路（請見下圖）：

   - **網路名稱**Wi-Fi 的名稱或者 SSID（Service Set Identifier）。
   - **身分驗證類型**連線到 Wi-Fi 網路時使用的身分驗證類型。

     從 Kaspersky Endpoint Security for Windows 版本 12.0 開始，WPA3 協定支援已新增到應用程式中。如果在電腦上套用 Kaspersky Endpoint Security 12.2 政策，則在電腦上對於 Kaspersky Endpoint Security 11.11.0 及更早版本選擇 WPA2 協定；對於 12.0 到 12.1 版本選擇 WPA2 / WPA3；對於 12.2 及更高版本選擇 WPA3。

   - **加密類型**用於防護 Wi-Fi 流量的加密類型。
   - **註釋**有關新增 Wi-Fi 網路的更多資訊。

   您可以在路由器設定中檢視受信任 Wi-Fi 網路的設定。

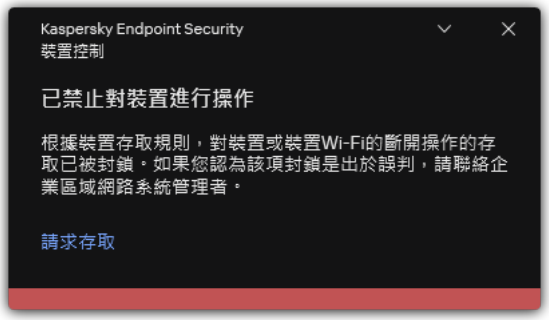
   如果某個 Wi-Fi 網路的設定比對規則中指定的所有設定則其被認定為受信任。

7. 儲存變更。




受信任 Wi-Fi 網路設定

結果，當使用者嘗試連線到未被列為受信任的 Wi-Fi 網路時，應用程式將封鎖連線並顯示通知（請見下圖）。




"裝置控制"通知

# 監視卸除式磁碟機的使用

監視卸除式磁碟機的使用包括：

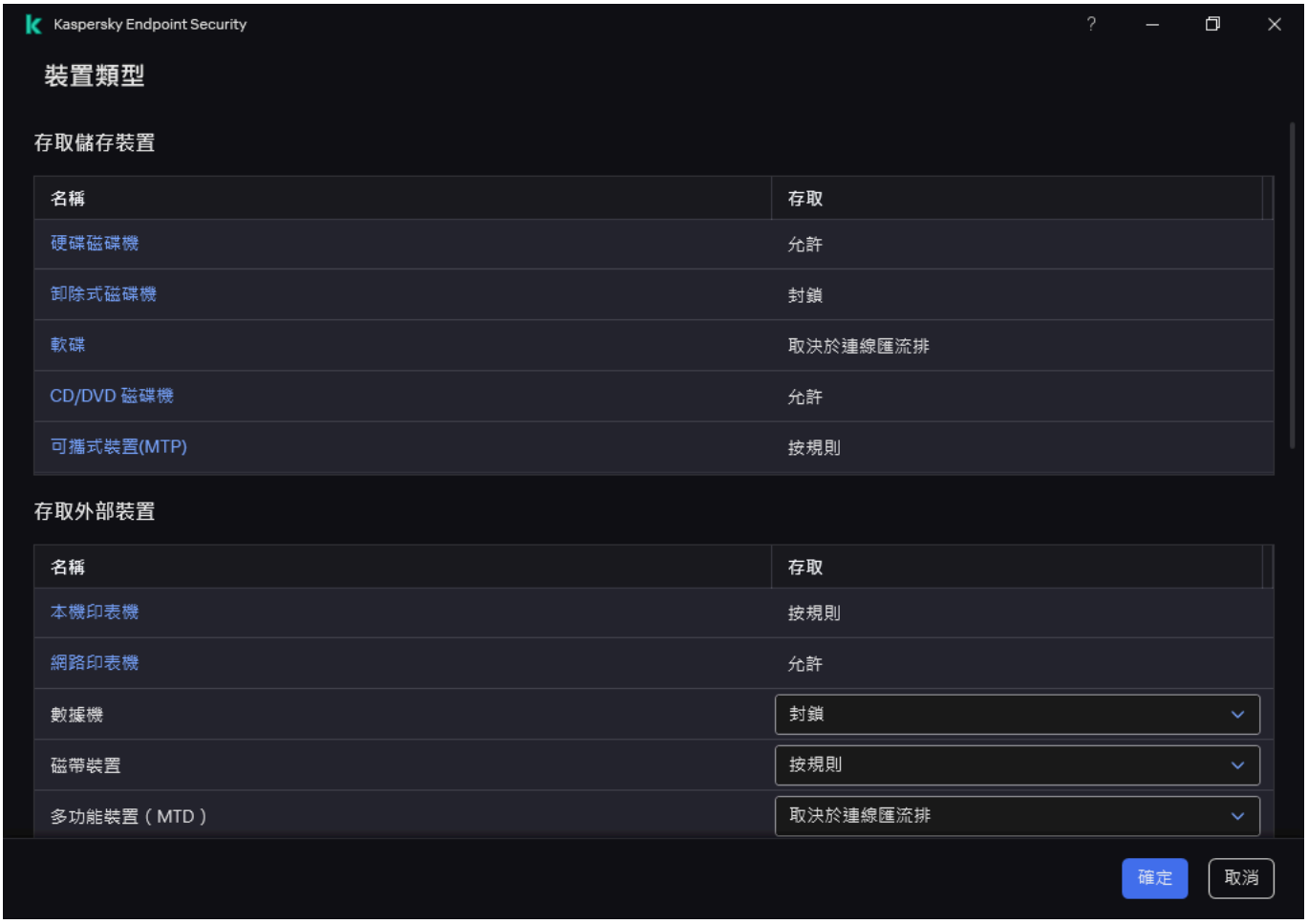
- 檢視卸除式磁碟機上的檔案的操作。
- 檢視受信任卸除式磁碟機的連線和斷開連線。

  Kaspersky Endpoint Security 允許檢視所有受信任裝置、而不只是卸除式磁碟機的連線和斷開連線您可以為"裝置控制"元件在"通知設定"中開啟事件記錄。事件有"*資訊訊息*"嚴重性等級。

*要啟用對卸除式磁碟機使用的監視，請：*

1. 在"應用程式主視窗"中，點擊⚙按鈕。
2. 在應用程式設定視窗中，選取"**安全控制**"→"**裝置控制**"。
3. 在"**存取設定**"塊中，點擊"**裝置和 Wi-Fi 網路**"按鈕。

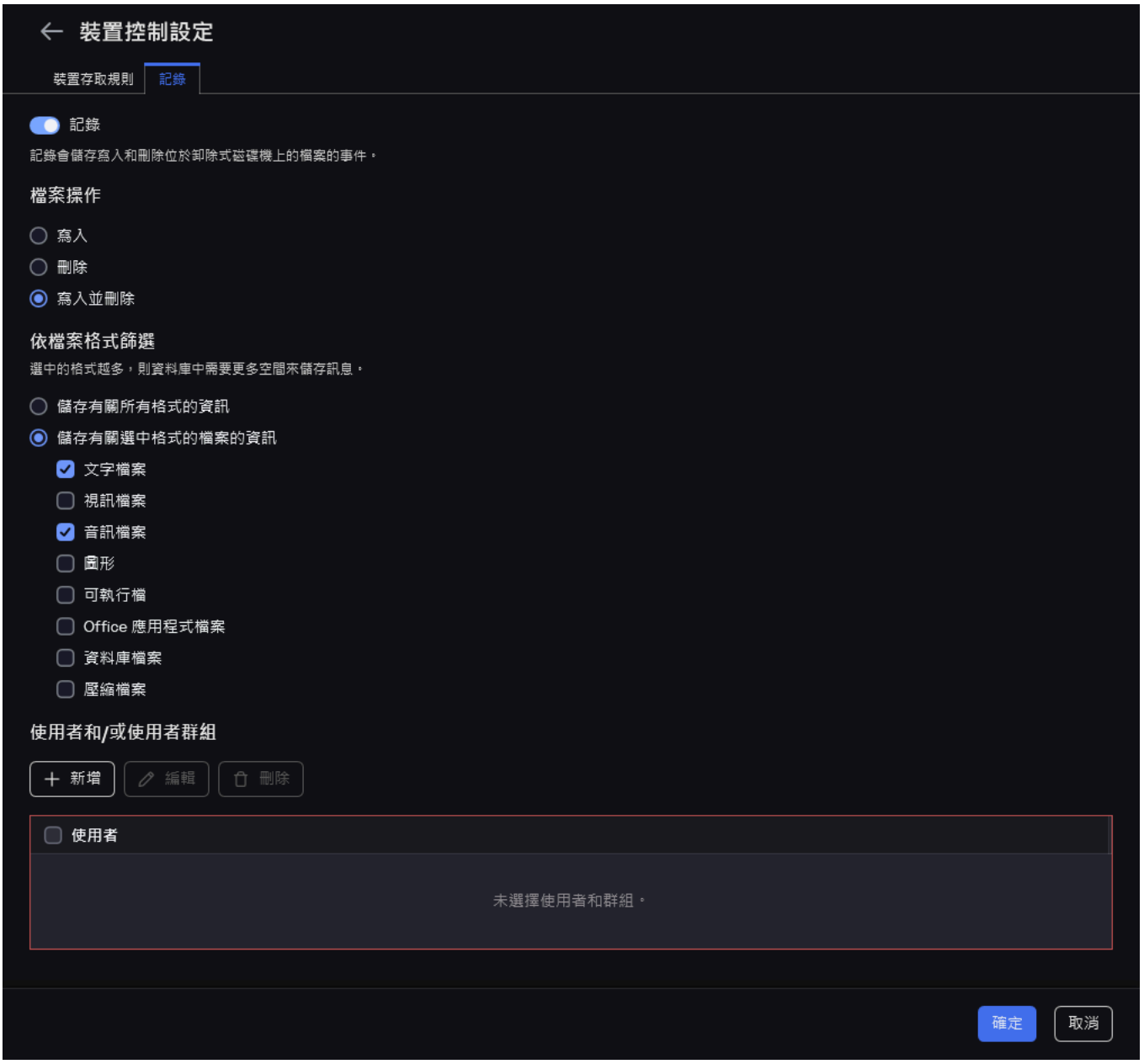
開啟的視窗顯示了裝置控制元件類別中包括的所有裝置的存取規則。




裝置控制元件中的裝置類型

4. 在“**存取儲存裝置**”塊中，選取“**卸除式磁碟機**”。

5. 在開啟的視窗中選擇“**記錄**”標籤。




卸除式磁碟機使用監控的設定

6. 開啟“**記錄**”開關。

7. 在“**檔案操作**”塊中，選擇要監視的操作：**寫入**，**刪除**。

8. 在“**依檔案格式篩選**”塊中，選擇其相關操作應由裝置控制進行記錄的檔案格式。

9. 選擇要監視其卸除式磁碟機使用情況的使用者或使用者群組。

10. 儲存變更。

因此，當使用者在卸除式磁碟機上寫入檔案或刪除檔案時，Kaspersky Endpoint Security 會將此類操作的資訊寫入事件記錄並將事件傳送至卡巴斯基安全管理中心。您可以在“**事件**”索引標籤上“**管理伺服器**”節點的工作區中的 卡巴斯基安全管理中心管理主控台中檢視與卸除式磁碟機上的檔案關聯的事件。要使事件顯示在本機 Kaspersky Endpoint Security 事件日誌中，您必須在“裝置控制”元件的通知設定中選擇“**檔案操作已執行**”核取方塊。

# 變更快取持續時間

裝置控制元件登錄與受監視裝置有關的事件，例如裝置的連線和斷開連線，從裝置讀取檔案，將檔案寫入裝置以及其他事件。然後，裝置控制將根據 Kaspersky Endpoint Security 設定允許或封鎖操作。

裝置控制在特定期間（稱為*快取期間*）內儲存有關事件的資訊。如果有關事件的資訊被快取並且該事件重複發生，則無需將其通知給 Kaspersky Endpoint Security 或顯示另一個提示以授予對相應操作的存取權限，例如連線裝置。這使得使用裝置更加方便。

如果以下所有事件設定與快取中的記錄匹配，則該事件被視為重複事件：

- 裝置 ID
- 嘗試存取的使用者帳戶的 SID
- 裝置類別
- 裝置採取的操作
- 此操作的應用程式權限：允許或拒絕
- 採取操作的處理程序路徑
- 正在被存取的檔案

在變更快取期間之前，請停用 Kaspersky Endpoint Security 自我防護。變更快取期間後，啟用自我防護。

*要變更快取期間，請：*

1. 在電腦上開啟登錄檔編輯器。
2. 在登錄檔編輯器中，轉到以下部分：
   - 對於 64 位元作業系統：
     `[HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\KasperskyLab\protected\KES\environment]`
   - 對於 32 位元作業系統：
     `[HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\protected\KES\environment]`
3. 開啟 `DeviceControlEventsCachePeriod` 進行編輯。
4. 定義裝置控制在刪除此資訊之前必須儲存有關事件的資訊的分鐘數。

# 對信任裝置的操作

*信任的裝置*是指在信任裝置設定中指定的使用者可隨時進行完全存取的裝置。

要使用受信任裝置，您可以為單一使用者、一組使用者或組織的所有使用者授予存取權限。

例如，如果您的組織不允許使用卸除式磁碟機，但是管理員在工作中使用卸除式磁碟機，您可以僅允許一組管理員使用卸除式磁碟機。為此，請將卸除式磁碟機新增到受信任清單中，並配置使用者存取權限。

不建議新增超過 1000 個受信任裝置，因為這可能造成系統不穩定。

Kaspersky Endpoint Security 允許您透過以下方式將裝置新增到受信任清單中：

- 如果您的組織中未佈署卡巴斯基安全管理中心，您可以將裝置連線到電腦，然後在應用程式設定中將其新增到受信任清單中。要將受信任裝置的清單分發到組織內的所有電腦，您可以在政策中啟用合併受信任裝置清單，也可以使用匯出/匯入程序。
- 如果您的組織中佈署了卡巴斯基安全管理中心，您可以遠端偵測所有已連線的裝置，並在政策中建立受信任裝置的清單。受信任裝置清單將在套用該政策的所有電腦上可用。

Kaspersky Endpoint Security 允許控制對受信任裝置的使用（連線和斷開連線）。您可以為“裝置控制”元件在“通知設定”中開啟事件記錄。事件有“*資訊*”嚴重性等級。

## 在應用程式介面中向信任清單新增裝置

預設情況下，在將裝置新增到信任裝置清單中後，所有用戶端（“Everyone”使用者群組）都被授權存取該裝置的權限。

*若要在應用程式介面中向信任清單新增裝置，請執行以下操作：*

1. 在“應用程式主視窗”中，點擊⚙按鈕。
2. 在應用程式設定視窗中，選取”**安全控制**“→“**裝置控制**”。
3. 在”**存取設定**”塊中，點擊”**受信任裝置**”按鈕。

   這將開啟受信任裝置的清單。
4. 點擊“**選擇**”。

   這將開啟連線裝置的清單。裝置清單項目取決於在“**顯示已連接的裝置**”下拉清單中選取的值。
5. 在裝置清單中，選擇要新增到受信任清單的裝置。

   Kaspersky Endpoint Security 不支援將**軟碟**類型的裝置新增到受信任清單。
6. 在“**註釋**”欄位中，您可以提供有關受信任裝置的任何相關資訊。
7. 選擇要允許其存取受信任裝置的使用者或使用者群組。

   您可以在 Active Directory 中、在卡巴斯基安全管理中心的账户清單中或透過手動輸入本機使用者名稱來選擇使用者。卡巴斯基建議僅在無法使用網域使用者帳戶的特殊情況下使用本機使用者帳戶。
8. 儲存變更。

# 在卡巴斯基安全管理中心中向受信任清單新增裝置

如果電腦上已安裝 Kaspersky Endpoint Security 並且已啟用"裝置控制"，則卡巴斯基安全管理中心會收到有關裝置的資訊。無法將裝置新增到受信任清單，除非卡巴斯基安全管理中心有該裝置的資訊。

您可以根據以下資料將裝置新增到受信任清單中：

- **透過裝置 ID**每個裝置都有一個唯一識別碼（硬體 ID 或 HWID）。您可以使用作業系統工具在裝置內容中檢視 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。

- **透過裝置型號**每個裝置都有一個供應商 ID (VID) 和一個產品 ID (PID)。您可以使用作業系統工具在裝置內容中檢視 ID。用於輸入 VID 和 PID 的範本：`VID_1234&PID_5678`。如果在組織中使用特定型號的裝置，則按型號新增裝置很方便。這樣，您可以新增該型號的所有裝置。

- **透過裝置 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到受信任清單。`*` 字元可替換任意一組字元。輸入遮罩時，Kaspersky Endpoint Security 不支援 `?` 字元。例如，`WDC_C*`。

- **依型號遮罩列出的裝置**如果您使用具有相似 VID 或 PID 的多個裝置（例如，同一製造商的裝置），則可以使用遮罩將裝置新增到受信任清單。`*` 字元可替換任意一組字元。輸入遮罩時，Kaspersky Endpoint Security 不支援 `?` 字元。例如，`VID_05AC&PID_*`。

管理主控台 (MMC) 和網頁主控台中受信任區域的分組方式不同。同樣，防止受信任區域參數變更的方式也不同（不同的"掛鎖"）。我們建議僅使用網頁主控台來管理應用程式。如果在不同主控台中配置受信任區域，管理外掛程式可能會將"掛鎖"重設為其預設狀態。

*要將裝置新增到受信任裝置清單：*

1. 在卡巴斯基安全管理中心管理主控台樹狀目錄中，選取**政策**。
2. 選擇必要的政策並點擊以開啟政策內容。
3. 在政策視窗中，選擇"**安全控制 → 裝置控制**"。
4. 在視窗右側，選取"**受信任裝置**"標籤。
5. 如果要為公司內的所有電腦建立受信任裝置的綜合清單，請選取"**繼承時合併值**"核取方塊。

   將合併父政策和子政策中的受信任裝置清單。如果啟用繼承時合併值，則將合併清單。父政策中的受信任裝置以唯讀視圖的形式顯示在子政策中。無法變更或刪除父政策的受信任裝置。
6. 點擊"**新增**"按鈕，然後選取將裝置新增到受信任清單的方法。
7. 要篩選裝置，請從"**裝置類型**"下拉清單中選取一種裝置類型（例如，"**卸除式磁碟機**"）。

   Kaspersky Endpoint Security 不支援將**軟碟**類型的裝置新增到受信任清單。

8. 在“**名稱/型號**”欄位中，輸入裝置 ID（VID 和 PID）或遮罩，具體取決於所選的新增方法。

   按型號遮罩（VID 和PID）新增裝置的操作方式如下：如果輸入的型號遮罩與任何型號都不相符，則 Kaspersky Endpoint Security 會檢查裝置 ID (HWID) 是否與該遮罩相符。Kaspersky Endpoint Security 只檢查裝置 ID 中決定了裝置的製造商和類型的部分 (`SCSI\CDROM&VEN_NECVMWAR&PROD_VMWARE_SATA_CD00\5&354AE4D7&0&000000`)。如果型號遮罩與裝置 ID 的此部分相符，則與該遮罩相符的裝置將被新增到電腦上的受信任裝置清單中。同時，當點擊“ **重新整理** ”按鈕時，卡巴斯基安全管理中心中的裝置清單將保持空白。要正確顯示裝置清單，可以按裝置 ID 遮罩新增裝置。

9. 要篩選裝置，請在“**電腦**”欄位中輸入裝置所連線之電腦的名稱或名稱遮罩。

   `*` 字元可替換任意一組字元。`?` 字元可替換任意單一字元。

10. 點擊 **重新整理**按鈕。

    該表顯示滿足定義的篩選條件的裝置清單。

11. 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。

12. 在“**註解**”欄位中，輸入將裝置新增到受信任清單的原因說明。

13. 點擊“**允許使用者和/或使用者群組**“欄位右側的“**選取**”按鈕。

14. 您可以在 Active Directory 中、在卡巴斯基安全管理中心的账户清單中或透過手動輸入本機使用者名稱來選擇使用者。卡巴斯基建議僅在無法使用網域使用者帳戶的特殊情況下使用本機使用者帳戶。

    預設情況下，允許 Everyone 群組存取受信任裝置。

15. 儲存變更。

連接裝置後，Kaspersky Endpoint Security 會檢查授權使用者的受信任裝置清單。如果裝置受信任，即使對裝置類型或連接介面的存取被拒，Kaspersky Endpoint Security 也會允許以所有權限存取該裝置。如果裝置不受信任並且存取被拒，您可以請求存取鎖定的裝置。

## 匯出和匯入受信任裝置的清單

要將受信任裝置的清單分發到組織中所有的電腦，可以使用匯出/匯入程序。

例如，如果您需要分發受信任的卸除式磁碟機的清單，需要執行以下操作：

1. 按順序將卸除式磁碟機連線到電腦。
2. 在 Kaspersky Endpoint Security 設定中，將卸除式磁碟機新增到受信任清單中。如有需要，設定使用者存取權限。例如，僅允許管理員存取卸除式磁碟機。
3. 在 Kaspersky Endpoint Security 設定中，匯出受信任裝置的清單（請參見以下說明）。
4. 將受信任裝置清單檔案分發到組織中的其他電腦。例如，將檔案放置在共用資料夾中。
5. 在組織的其他電腦上的 Kaspersky Endpoint Security 設定中匯入受信任裝置的清單（請參見以下說明）。

*要匯入或匯出受信任裝置的清單：*

1. 在"應用程式主視窗"中，點擊⚙按鈕。
2. 在應用程式設定視窗中，選取"**安全控制**"→"**裝置控制**"。
3. 在"**存取設定**"塊中，點擊"**受信任裝置**"按鈕。
   這將開啟受信任裝置的清單。
4. 要匯出信任裝置的清單：
   a. 選擇您要匯出的受信任裝置。
   b. 點擊"**匯出**"。
   c. 在開啟的視窗中，指定您要將受信任裝置清單匯出到的 XML 檔案的名稱，然後選取要儲存此檔案的資料夾。
   d. 儲存檔案。
      Kaspersky Endpoint Security 會將整個受信任裝置清單匯出到 XML 檔案。
5. 要匯入信任裝置的清單：
   a. 在"**匯入**"下拉清單中，選取相關操作：**匯入並新增至現有的**或**匯入並取代現有的**。
   b. 在開啟的視窗中，選取要從中匯入受信任裝置清單的 XML 檔案。
   c. 開啟檔案。
6. 儲存變更。

連接裝置後，Kaspersky Endpoint Security 會檢查授權使用者的受信任裝置清單。如果裝置受信任，即使對裝置類型或連接介面的存取被拒，Kaspersky Endpoint Security 也會允許以所有權限存取該裝置。

# 獲得存取被封鎖裝置的權限

配置"裝置控制"時，可能會意外封鎖對工作所需裝置的存取。

如果未在組織中佈署卡巴斯基安全管理中心，可以在 Kaspersky Endpoint Security 的設定中提供對裝置的存取權限。例如，可以將裝置新增到受信任清單或暫時停用"裝置控制"。

如果組織中已佈署卡巴斯基安全管理中心並且已將某個政策套用於電腦，則可以在管理主控台中提供對裝置的存取權限。

授予存取權限的線上模式

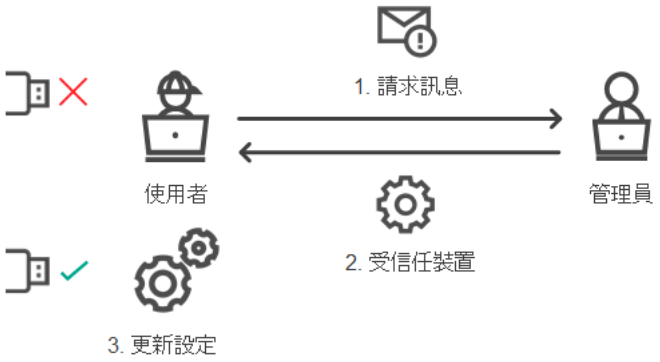
只有在組織中佈署了卡巴斯基安全管理中心且已將某個政策套用於電腦時，才能以線上模式授予對封鎖的裝置的存取權限。電腦必須能夠與管理伺服器建立連線。

線上模式下授予存取權限包括以下步驟：

1. 使用者向管理員傳送包含存取請求的訊息。
2. 管理員在卡巴斯基安全管理中心主控台中收到一條請求訊息。

   卡巴斯基安全管理中心主控台有預設的事件選擇*使用者請求*以便於跟踪來自使用者的訊息。
3. 管理員將裝置新增到受信任清單。

   您可以在管理群組的政策中或單個電腦的本機應用程式設定中新增受信任裝置。
4. 管理員在使用者的電腦上更新 Kaspersky Endpoint Security 的設定。




線上模式下授予裝置存取權限的示意圖

授予存取權限的離線模式

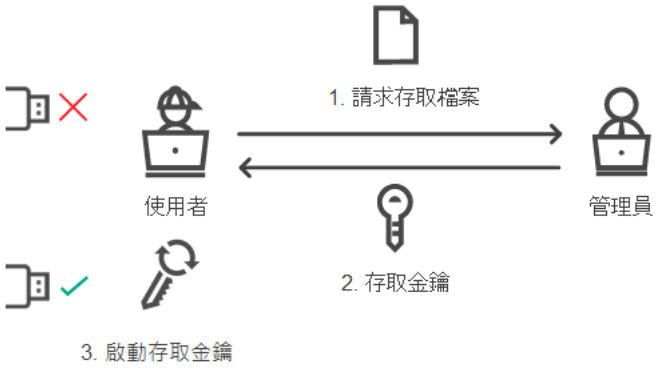
只有在組織中佈署了卡巴斯基安全管理中心且已將某個政策套用於電腦時，才能以離線模式授予對封鎖的裝置的存取權限。在政策設定的**"裝置控制"**部分中，必須選中**"允許暫時存取請求"**核取方塊。

如果需要授予對封鎖的裝置的暫時存取權限，但無法將裝置新增到受信任清單，則可以在離線模式下授予對裝置的存取權限。這樣，即使電腦沒有網路存取權限，或者電腦位於公司網路外部，您也可以授予對封鎖的裝置的存取權限。

離線模式下授予存取權限包括以下步驟：

1. 使用者建立請求存取檔案並將其傳送給管理員。
2. 管理員根據請求存取檔案建立存取金鑰並將其傳送給使用者。

3. 使用者啟動存取金鑰。




離線模式下授予裝置存取權限的示意圖

## 授予存取權限的線上模式

只有在組織中佈署了卡巴斯基安全管理中心且已將某個政策套用於電腦時，才能以線上模式授予對封鎖的裝置的存取權限。電腦必須能夠與管理伺服器建立連線。

*某使用者請求存取封鎖的裝置，如下所示：*

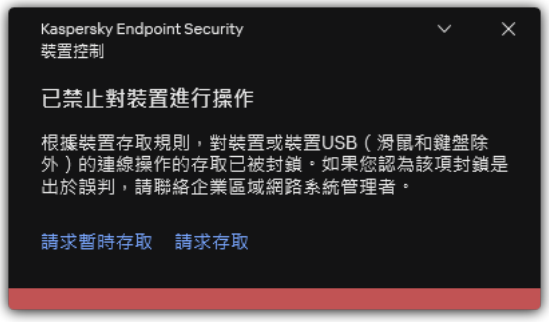
1. 將裝置連線到電腦。

   Kaspersky Endpoint Security 將顯示一條通知，指示對裝置的存取被封鎖（請參見下圖）。

2. 點擊"**請求存取**"連接。

   這將開啟一個視窗，其中包含給管理員的訊息。此訊息包含有關封鎖的裝置的資訊。

3. 點擊"**傳送**"。




"裝置控制"通知

下一步，卡巴斯基安全管理中心主控台中的管理員會收到*傳送給管理員的裝置存取封鎖訊息*事件。該事件包括使用者名稱、電腦名稱、使用者嘗試存取的裝置的詳情以及其他資料。您可以設定管理員被通知此類事件的方式並（例如）選擇電子郵件通知。卡巴斯基安全管理中心主控台有預設的事件選擇*使用者請求*以便於跟踪來自使用者的訊息。

若要允許存取，您必須新增裝置到信任清單。在電腦上更新 Kaspersky Endpoint Security 設定後，使用者可以獲得對裝置的存取權限。

# 授予存取權限的離線模式

只有在組織中佈署了卡巴斯基安全管理中心且已將某個政策套用於電腦時，才能以離線模式授予對封鎖的裝置的存取權限。在政策設定的**"裝置控制"**部分中，必須選中**"允許暫時存取請求"**核取方塊。

*某使用者請求存取封鎖的裝置，如下所示：*

1. 將裝置連線到電腦。

   Kaspersky Endpoint Security 將顯示一條通知，指示對裝置的存取被封鎖（請參見下圖）。

2. 點擊**"請求暫時存取"**連接。

   這將開啟包含已連線裝置清單的視窗。

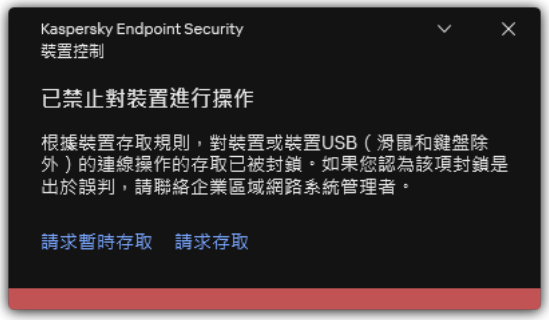
3. 在已連線裝置清單中，選取您想要取得其存取權限的裝置。

4. 點擊**"產生請求存取檔案"**。

5. 在**"存取持續時間"**欄位中，指定您想要存取裝置的時長。

6. 將檔案儲存到電腦記憶體中。

結果，帶 *.akey 副檔名的請求存取檔案將下載到電腦記憶體中。使用任何可用方法將裝置請求存取檔案傳送給公司 LAN 管理員。




"裝置控制"通知

**管理員如何在管理主控台 (MMC) 中為被封鎖的裝置建立存取金鑰**

1. 開啟卡巴斯基安全管理中心管理主控台。

2. 在管理主控台樹狀目錄的**"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**"裝置"**標籤。

4. 在用戶端電腦清單中，選取其使用者需要取得被封鎖裝置臨時存取權限的電腦。

5. 在用戶端電腦的內容功能表中選取在**"授予離線模式下的存取權限"**項目。

6. 在開啟的視窗中選擇**"裝置控制"**標籤。

7. 點擊**"瀏覽"**按鈕並下載從使用者處收到的請求存取檔案。
   您將看到有關使用者請求存取的封鎖的裝置的資訊。

8. 如果必要，變更**"存取持續時間"**設定的值。
   預設情況下，**"存取持續時間"**設定採用使用者在建立存取請求檔案時指示的值。

9. 指定**"啟用截止日期"**設定的值。
   定義使用者可透過使用提供的存取金鑰啟動被封鎖裝置存取權限的時間範圍。

10. 將存取金鑰檔案儲存到電腦記憶體中。

**管理員如何在 Web 主控台和 Cloud Console 中為被封鎖的裝置建立存取金鑰**

1. 在網頁主控台的主視窗中，選擇**資產（裝置）→受管理裝置**。

2. 在用戶端電腦清單中，選取其使用者需要取得被封鎖裝置臨時存取權限的電腦。

3. 點選位於電腦清單上方的省略號按鈕（ **...** ），然後點擊 **同意存取離線模式下的裝置** 按鈕。

4. 在開啟的視窗中，選擇**"裝置控制"**區域。

5. 點擊**"瀏覽"**按鈕並下載從使用者處收到的請求存取檔案。
   您將看到有關使用者請求存取的封鎖的裝置的資訊。

6. 如果必要，變更**"存取持續時間 (小時)"**設定的值。
   預設情況下，**"存取持續時間 (小時)"**設定採用使用者在建立存取請求檔案時指示的值。

7. 指定可以在裝置上啟動存取金鑰的時間段。
   定義使用者可透過使用提供的存取金鑰啟動被封鎖裝置存取權限的時間範圍。

8. 將存取金鑰檔案儲存到電腦記憶體中。

結果，封鎖的裝置的存取金鑰將下載到電腦記憶體中。存取金鑰檔案的副檔名為 *.acode。使用任何可用方法將封鎖的裝置的存取金鑰傳送給使用者。

*使用者啟動存取金鑰，如下所示：*

1. 在"應用程式主視窗"中，點擊⚙ 按鈕。

2. 在應用程式設定視窗中，選取**"安全控制"→"裝置控制"**。

3. 在**"存取請求"**塊中，點擊**"請求存取裝置"**按鈕。

4. 在開啟的視窗中，點擊**"啟動存取金鑰"**按鈕。

5. 在開啟的視窗中，選擇包含從公司 LAN 管理員處收到的裝置存取金鑰的檔案。
   這將開啟一個視窗，其中包含有關存取條款的資訊。

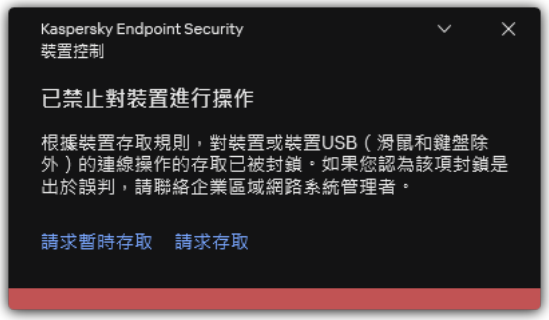
6. 點擊**"確定"**。

結果，使用者在管理員設定的時間段內獲得對裝置的存取權限。使用者獲得存取裝置的全套權限（讀取和寫入）。金鑰到期後，對裝置的存取將被封鎖。如果使用者需要永久存取裝置，請將裝置新增到受信任清單中。

# 編輯裝置控制訊息範本

當使用者嘗試存取被封鎖的裝置時，Kaspersky Endpoint Security 會顯示一條訊息，說明對該裝置的存取被封鎖，或封鎖對該裝置內容的操作。卡巴斯基專家向使用者提供訊息範本，描述裝置存取被封鎖的原因（見下圖）。

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"通知

如果使用者相信對裝置的存取被錯誤地封鎖了，或者對裝置內容的操作被錯誤封鎖了，使用者可以透過點擊被封鎖操作顯示訊息中的連結向公司區域網路管理員傳送訊息。為此，使用者必須點擊 **請求存取** 或者 **請求暫時存取** 按鈕並向管理員傳送一條訊息描述情況。您也可以準備一個傳送給管理員的訊息範本，向其中新增資料，以便您決定允許或封鎖對裝置的存取。在使用者請求提供存取權限後，Kaspersky Endpoint Security 會向卡巴斯基安全管理中心傳送一個事件：**傳送給管理員的裝置存取封鎖訊息**。事件描述包含一條給管理員的訊息，其中包含被替換的變數。您可以使用預定義事件選擇**使用者請求**在卡巴斯基安全管理中心主控台中檢視這些事件。如果您的組織沒有部署卡巴斯基安全管理中心或者沒有連線到管理伺服器，應用程式將向管理員傳送一條訊息到指定的電子郵件信箱。

### 如何在管理主控台 (MMC) 中變更裝置控制訊息範本

1. 在卡巴斯基安全管理中心管理主控台樹狀目錄中，選取**政策**。
2. 選擇必要的政策並點擊以開啟政策內容。
3. 在政策視窗中，選擇"**安全控制 → 裝置控制**"。
4. 在"**訊息範本設定**"塊中，點擊"**範本**"按鈕。
5. 這會開啟一個視窗；在該視窗中，配置應用程式控制範本：

   - **有關封鎖的訊息**當使用者嘗試存取封鎖的裝置時所顯示的訊息的範本。當使用者嘗試對被封鎖使用的裝置內容執行操作時，也會顯示此訊息。
   - **傳送郵件給管理員**當使用者確信裝置的存取權限或裝置內容操作被錯誤地禁止時，傳送給 LAN 管理員的訊息的範本。

   若要將變數新增至範本文字，請將游標置於所需位置，點擊**變數**，然後從可用選項清單中選取所需變數。

   您也可以還原預設範本文字。

6. 儲存變更。

**如何在 Web 主控台和雲端主控台中變更裝置控制訊息範本**

1. 在網頁主控台的主視窗中，選擇**資產（裝置）→政策和設定檔**。
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**"塊中，設定"應用程式控制"訊息的範本：

   - **傳送給使用者的郵件**當使用者嘗試存取封鎖的裝置時所顯示的訊息的範本。當使用者嘗試對被封鎖使用的裝置內容執行操作時，也會顯示此訊息。
   - **傳送給管理員的郵件**當使用者確信裝置的存取權限或裝置內容操作被錯誤地禁止時，傳送給 LAN 管理員的訊息的範本。

   若要將變數新增至範本文字，請將游標置於所需位置，點擊**新增變數**，然後從可用選項清單中選取所需變數。

   您也可以還原預設範本文字。
6. 儲存變更。

**如何在應用程式介面中變更裝置控制訊息範本**

1. 在"應用程式主視窗"中，點擊⚙按鈕。
2. 在應用程式設定視窗中，選取"**安全控制**"→"**應用程式控制**"。
3. 在"**訊息範本**"塊中，設定"應用程式控制"訊息的範本：

   - **有關封鎖的訊息**當使用者嘗試存取封鎖的裝置時所顯示的訊息的範本。當使用者嘗試對被封鎖使用的裝置內容執行操作時，也會顯示此訊息。
   - **傳送郵件給管理員**當使用者確信裝置的存取權限或裝置內容操作被錯誤地禁止時，傳送給 LAN 管理員的訊息的範本。

   若要將變數新增至範本文字，請將游標置於所需位置，點擊**新增變數**，然後從可用選項清單中選取所需變數。

   您也可以還原預設範本文字。
4. 儲存變更。

# 橋接防護

橋接防護透過封鎖為一台電腦同時建立多個網路連線來禁止建立橋接器。這樣可以防護公司網路避免未受防護和未經授權的網路上的攻擊。

橋接防護透過使用*連線規則*管理網路連線的建立。

已針對以下預定義的裝置類型建立連線規則：

- 網路介面卡；
- Wi-Fi 介面卡；
- 數據機。

如果啟用連線規則，Kaspersky Endpoint Security 將：

- 在建立新連線時封鎖活動連線（如果規則中指定的裝置類型同時用於這兩個連線）；
- 封鎖透過使用了較低優先順序規則的裝置類型建立的連線。

## 啟用橋接防護

預設情況下停用橋接防護。

*要啟用橋接防護，請：*

1. 在“應用程式主視窗”中，點擊 按鈕。
2. 在應用程式設定視窗中，選取”**安全控制**“→“**裝置控制**”。
3. 在”**存取設定**”塊中，點擊”**橋接防護**”按鈕。
4. 使用“**啟用橋接防護**”開關來啟用或停用此功能。
5. 儲存變更。

啟用橋接防護後，Kaspersky Endpoint Security 會按照連線規則封鎖已建立的連線。

## 變更連線規則的狀態

*要變更連線規則的狀態：*

1. 在“應用程式主視窗”中，點擊 按鈕。
2. 在應用程式設定視窗中，選取”**安全控制**“→“**裝置控制**”。
3. 在”**存取設定**”塊中，點擊”**橋接防護**”按鈕。
4. 在“**裝置的規則**”塊中，選擇要變更其狀態的規則。
5. 使用“**控制**“列中的開關來啟用或停用規則。
6. 儲存變更。

## 變更連線規則的優先順序

*要變更連線規則的優先順序：*

1. 在"應用程式主視窗"中，點擊⚙按鈕。
2. 在應用程式設定視窗中，選取"**安全控制**"→"**裝置控制**"。
3. 在"**存取設定**"塊中，點擊"**橋接防護**"按鈕。
4. 在"**裝置的規則**"塊中，選擇要變更其優先順序的規則。
5. 使用"**上移**" / "**下移**"按鈕設定連線規則的優先順序。

   規則在規則表中所處位置越高，其優先順序就越高。除了透過使用最高級規則的裝置類型所建立的連線外，橋接防護將封鎖所有連線。
6. 儲存變更。

# 適應性異常控制

如果 Kaspersky Endpoint Security 安裝在執行 Windows for Workstations 的電腦上，則該元件可用。如果 Kaspersky Endpoint Security 安裝在執行 Windows for Servers 的電腦上，則該元件不可用。

自適應異常控制元件會監視並封鎖不是公司網路內電腦典型操作的相關操作。自適應異常控制使用一組規則來偵錯非典型行為（例如，*從 Office 應用程式啟動 Microsoft PowerShell* 規則）。規則由 Kaspersky 專家根據惡意活動的典型情景建立。您可以配置"自適應異常控制"處理每條規則的方式，例如，允許執行使某些工作流工作自動化的 PowerShell 指令碼。Kaspersky Endpoint Security 會同時更新規則集和應用程式資料庫。規則集的更新必須手動確認。

### "自適應異常控制"設定

配置"自適應異常控制"包括以下步驟：

1. 訓練"自適應異常控制"。

   啟用"自適應異常控制"後，其規則在*訓練模式*下工作。在訓練期間，"自適應異常控制"監控規則觸發並將觸發事件傳送到卡巴斯基安全管理中心。每條規則都有自己的訓練模式持續時間。訓練模式持續時間由 Kaspersky 專家設定。通常，訓練模式保持活動兩周。

   如果在訓練期間某條規則完全未觸發，"自適應異常控制"會將與此規則關聯的操作視為非典型操作。Kaspersky Endpoint Security 將封鎖與該規則相關的所有操作。

   如果在訓練期間觸發了某條規則，Kaspersky Endpoint Security 會將事件記錄在規則觸發報告和**智慧培訓狀態中的規則觸發器**儲存區中。

2. 分析規則觸發報告。

   管理員分析 規則觸發報告 或內容 **智慧培訓狀態中的規則觸發器** 儲存區。然後管理員可以選取在觸發規則時“自適應異常控制”的行為：封鎖或允許。管理員還可以繼續監控規則的工作方式並延長訓練模式的持續時間。如果管理員未採取任何操作，應用程式也將繼續在訓練模式下工作。訓練模式期限重新開始。

“自適應異常控制”透過以下通道即時配置：

- “自適應異常控制”自動開始封鎖與從未在訓練模式中觸發的規則相關聯的操作。
- Kaspersky Endpoint Security 新增新規則或刪除過時規則。
- 管理員在檢視規則觸發報告和“**智慧培訓狀態中的規則觸發器**”儲存區的內容後配置“適應性異常控制”的操作。我們建議檢查有關規則觸發的報告以及 **智慧培訓狀態中的規則觸發器** 儲存區的內容。

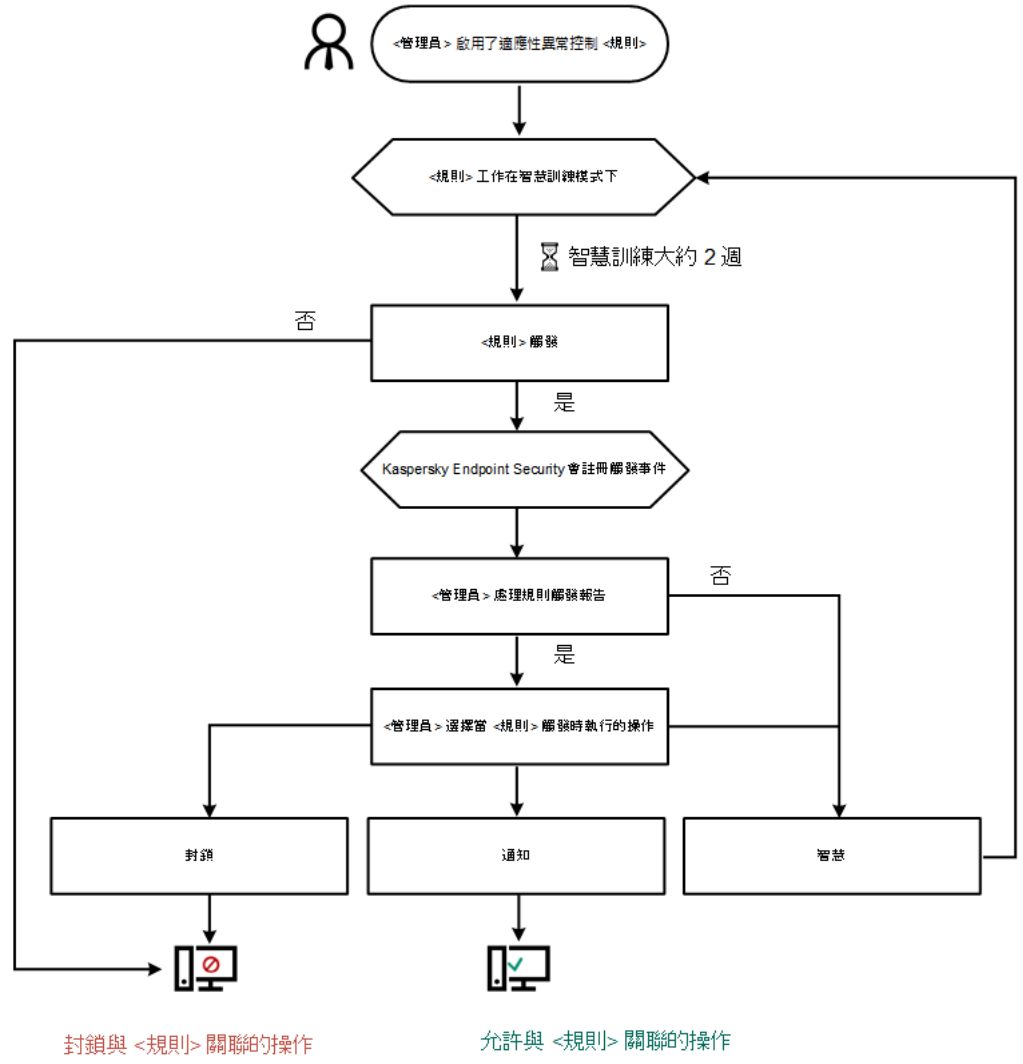
當惡意應用程式嘗試執行操作時，Kaspersky Endpoint Security 將封鎖該操作並顯示通知（請參見下圖）。




“自適應異常控制”通知

“自適應異常控制”操作演算法

Kaspersky Endpoint Security 根據以下演算法決定是允許還是封鎖與某條規則關聯的操作（請參見下圖）。




“自適應異常控制”操作演算法

# 訓練“自適應異常控制”

適應性異常控制包括一組規則（行為模式）。啟用“自適應異常控制”後，其規則在*訓練模式*下工作。在訓練期間，“自適應異常控制”監控規則觸發並將觸發事件傳送到卡巴斯基安全管理中心。適應性異常控制不會阻止電腦上的應用程式活動，而只會通知管理員。您也可以手動選擇觸發適應性異常控制規則時執行的操作。

**如何在管理主控台 (MMC) 中檢視適應性異常控制規則清單**

1. 開啟卡巴斯基安全管理中心管理主控台。
2. 在主控台樹狀目錄中，選擇“**政策**”。
3. 選擇必要的政策並點擊以開啟政策內容。
4. 在政策視窗中，選擇“**安全控制 → 自適應異常控制**”。

5. 選擇"**自適應異常控制**"核取方塊。

6. 在 **自適應異常控制規則設定**下面，查看規則清單。

   預設情況下，所有規則都在 **智慧** 模式下工作。

7. 如有必要，確認適應性異常控制規則的更新。

8. 如有必要，選擇適應性異常控制規則觸發時執行的操作：

   - **封鎖**如果選取此操作，當觸發適應性異常控制規則時，Kaspersky Endpoint Security 將封鎖規則覆蓋的活動，並記錄包含活動資訊的項目。
   - **通知**如果選取此操作，當觸發適應性異常控制規則時，Kaspersky Endpoint Security 將允許規則覆蓋的活動，並記錄包含活動資訊的項目。

9. 如果有必要，請停用您不想使用的規則。

10. 儲存變更。若要在電腦上套用該政策，請關閉掛鎖。

**如何在網頁主控台和雲端主控台中檢視適應性異常控制規則**

1. 在網頁主控台的主視窗中，選擇**資產（裝置）→政策和設定檔**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"**安全控制**"→"**自適應異常控制**"。

5. 開啟"**自適應異常控制已啟用**"開關。

6. 在 **規則**下面，查看規則清單。

   預設情況下，所有規則都在 **智慧** 模式下工作。

7. 如有必要，確認適應性異常控制規則的更新。

8. 如有必要，選擇適應性異常控制規則觸發時執行的操作：

   - **封鎖**如果選取此操作，當觸發適應性異常控制規則時，Kaspersky Endpoint Security 將封鎖規則覆蓋的活動，並記錄包含活動資訊的項目。
   - **通知**如果選取此操作，當觸發適應性異常控制規則時，Kaspersky Endpoint Security 將允許規則覆蓋的活動，並記錄包含活動資訊的項目。

9. 如果有必要，請停用您不想使用的規則。

10. 儲存變更。若要在電腦上套用該政策，請關閉掛鎖。

**如何在應用程式介面中檢視適應性異常控制規則清單**

1. 在"應用程式主視窗"中，點擊 按鈕。

2. 在應用程式設定視窗中，選取"**安全控制**"→"**自適應異常控制**"。

3. 開啟“**自適應異常控制**“開關。

4. 在”**規則**”塊中，點擊”**編輯規則**”連接。

   “適應性異常控制規則”清單將開啟。預設情況下，所有規則都在 **智慧** 模式下工作。

5. 如有必要，確認適應性異常控制規則的更新。

6. 如有必要，選擇適應性異常控制規則觸發時執行的操作：

   - **封鎖**如果選取此操作，當觸發適應性異常控制規則時，Kaspersky Endpoint Security 將封鎖規則覆蓋的活動，並記錄包含活動資訊的項目。

   - **通知**如果選取此操作，當觸發適應性異常控制規則時，Kaspersky Endpoint Security 將允許規則覆蓋的活動，並記錄包含活動資訊的項目。

7. 如果有必要，請停用您不想使用的規則。

8. 儲存變更。

每條規則都有自己的訓練模式持續時間。訓練模式持續時間由 Kaspersky 專家設定。通常，訓練模式保持活動兩周。

如果在訓練過程中，某條規則從未觸發，適應性異常控制會認為這種行為不正常，並將規則狀態改為 **智慧封鎖**。隨後，應用程式會阻止任何符合該規則的活動。

如果規則在訓練期間觸發，則需要手動設定應用程式對與該規則相符的偵測到的活動套用的操作。如果您未選擇規則觸發時的操作，適應性異常控制將繼續處於訓練模式。

# 啟用和停用適應性異常控制規則

*要停用或啟用適應性異常控制規則：*

1. 在“應用程式主視窗”中，點擊⚙ 按鈕。

2. 在應用程式設定視窗中，選取”**安全控制**“→“**自適應異常控制**”。

3. 在”**規則**”塊中，點擊”**編輯規則**”按鈕。

   “適應性異常控制規則”清單將開啟。

4. 在表中，選擇一組規則（例如*Office 應用程式的活動*）並展開。

5. 選擇一個規則（例如 *從 Office 應用程式啟動 Microsoft PowerShell*）。

6. 使用“**狀況**“列中的切換開關來啟用或停用適應性異常控制規則。

7. 儲存變更。

# 在適應性異常控制規則觸發時變更執行的操作

*要編輯觸發適應性異常控制規則時執行的操作：*

1. 在"應用程式主視窗"中，點擊⚙按鈕。
2. 在應用程式設定視窗中，選取"**安全控制**"→"**自適應異常控制**"。
3. 在"**規則**"塊中，點擊"**編輯規則**"按鈕。

   "適應性異常控制規則"清單將開啟。
4. 在表中選擇一個規則。
5. 點擊"**編輯**"。

   "適應性異常控制規則屬性"視窗將開啟。
6. 在"**操作**"區域，選取以下選項之一：

   - **智慧**如果選取此選項，自適應異常控制規則在 Kaspersky 專家定義的時間段內以智慧訓練狀態工作。在此模式下，當觸發自適應異常控制規則時，Kaspersky Endpoint Security 允許規則涵蓋的活動，並在卡巴斯基安全管理中心管理伺服器的**智慧培訓狀態中的規則觸發器**儲存中記錄項目。當為智慧訓練狀態下的工作設定的時間段結束後，Kaspersky Endpoint Security 將封鎖自適應異常控制規則覆蓋的活動，並記錄包含活動相關資訊的項目。
   - **封鎖**如果選取此操作，當觸發適應性異常控制規則時，Kaspersky Endpoint Security 將封鎖規則覆蓋的活動，並記錄包含活動資訊的項目。
   - **通知**如果選取此操作，當觸發適應性異常控制規則時，Kaspersky Endpoint Security 將允許規則覆蓋的活動，並記錄包含活動資訊的項目。
7. 儲存變更。

# 建立適應性異常控制規則的排除項目

您無法為適應性異常控制規則建立超過 1000 個排除項目。不建議建立超過 200 個排除項目。要減少使用的排除項目數量，建議在排除項目設定中使用遮罩。

適應性異常控制規則的排除項目包括來源物件和目的物件的說明。*來源物件*是執行操作的物件。*目的物件*是被執行操作的物件。例如，您開啟了一個名為 `file.xlsx` 的檔案。結果，一個帶 DLL 副檔名的庫檔案載入到電腦記憶體中。該庫被瀏覽器（名為 `browser.exe` 的可執行檔）使用。在此示例中，`file.xlsx` 是來源物件，Excel 是來源處理程序，`browser.exe` 是目的物件，Browser 是目的處理程序。

*要為適應性異常控制規則建立排除項目：*

1. 在"應用程式主視窗"中，點擊⚙按鈕。
2. 在應用程式設定視窗中，選取"**安全控制**"→"**自適應異常控制**"。

3. 在"**規則**"塊中，點擊"**編輯規則**"按鈕。

   "適應性異常控制規則"清單將開啟。

4. 在表中選擇一個規則。

5. 點擊"**編輯**"。

   "適應性異常控制規則屬性"視窗將開啟。

6. 在"**排除項目**"塊中，點擊"**新增**"按鈕。

   排除項目屬性視窗將開啟。

7. 選取要為其配置排除項目的使用者。

   您可以在 Active Directory 中、在卡巴斯基安全管理中心的账户清單中或透過手動輸入本機使用者名稱來選擇使用者。卡巴斯基建議僅在無法使用網域使用者帳戶的特殊情況下使用本機使用者帳戶。

   > "適應性異常控制"不支援使用者群組的排除項目。如果選擇了使用者群組，Kaspersky Endpoint Security 不會套用排除項目。

8. 在"**描述**"欄位中輸入排除項目的描述。

9. 定義來源物件的設定或該物件啟動的來源處理程序的設定：

   - **來源處理程序**檔案或包含檔案的資料夾的路徑或遮罩（例如，`C:\Dir\File.exe` 或 `Dir\*.exe`）。
   - **來源處理程序雜湊**檔案雜湊碼。
   - **來源物件**檔案或包含檔案的資料夾的路徑或遮罩（例如，`C:\Dir\File.exe` 或 `Dir\*.exe`）。例如，檔案路徑 `document.docm`，它使用指令碼或巨集來啟動目的處理程序。

     您還可以指定要排除的其他物件，如 Web 位址、巨集、命令列中的指令、登錄檔路徑等等。按照以下範本指定物件：`object://<object>`，其中 `<object>` 指物件的名稱，例如 `object://web.site.example.com`、`object://VBA`、`object://ipconfig`、`object://HKEY_USERS`。您也可以使用遮罩，例如，`object://*C:\Windows\temp\*`。
   - **來源物件雜湊**檔案雜湊碼。

   適應性異常控制規則不適用於該物件執行的操作或該物件啟動的處理程序。

10. 指定目的物件的設定或對該物件啟動的目的處理程序的設定。

    - **目標處理程序**檔案或包含檔案的資料夾的路徑或遮罩（例如，`C:\Dir\File.exe` 或 `Dir\*.exe`）。
    - **目標處理程序雜湊**檔案雜湊碼。
    - **目標物件**用於啟動目的處理程序的指令。使用模式 `object://<command>` 指定指令，例如，`object://cmdline:powershell -Command "$result = 'C:\Windows\temp\result_local_users_pwdage.txt'"`。您也可以使用遮罩，例如，`object://*C:\Windows\temp\*`。
    - **目標物件雜湊**檔案雜湊碼。

適應性異常控制規則不適用於對該物件執行的操作或對該物件啟動的處理程序。

11. 儲存變更。

# 匯出和匯入適應性異常控制規則排除項目

*要匯出或匯入所選規則的排除項目清單：*

1. 在"應用程式主視窗"中，點擊 按鈕。
2. 在應用程式設定視窗中，選取"**安全控制**"→"**自適應異常控制**"。
3. 在"**規則**"塊中，點擊"**編輯規則**"按鈕。
   "適應性異常控制規則"清單將開啟。
4. 要匯出規則清單：
   a. 選取您想要匯出其例外的規則。
   b. 點擊"**匯出**"。
   c. 在開啟的視窗中，指定您要將排除項目清單匯出到的 XML 檔案的名稱，然後選取要儲存此檔案的資料夾。
   d. 確認您只想匯出選定的排除項目，或匯出整個排除項目清單。
   e. 儲存檔案。
5. 要匯入規則清單：
   a. 點擊"**匯入**"。
   b. 在開啟的視窗中，選取要從中匯入排除項目清單的 XML 檔案。
   c. 開啟檔案。
      如果電腦已經具有排除項目清單，則 Kaspersky Endpoint Security 將提示您刪除現有清單或從 XML 檔案向其中新增新項目。
6. 儲存變更。

# 更新適應性異常控制規則

可以將新的適應性異常控制規則新增到規則表中，並且可以在更新病毒資料庫時從規則表中刪除現有適應性異常控制規則。如果尚未應用這些規則的更新，Kaspersky Endpoint Security 會區分要刪除或新增到表中的適應性異常控制規則。

在應用更新之前，Kaspersky Endpoint Security 會顯示要由規則表中的更新刪除的適應性異常控制規則集，並為其分配"*已停用*"狀態。不能變更這些規則的設定。

*要更新適應性異常控制規則：*

1. 在"應用程式主視窗"中，點擊 按鈕。
2. 在應用程式設定視窗中，選取"**安全控制**"→"**自適應異常控制**"。
3. 在"**規則**"塊中，點擊"**編輯規則**"按鈕。
   "適應性異常控制規則"清單將開啟。
4. 在開啟的視窗中，點擊"**批准更新**"按鈕。
   如果適應性異常控制規則的更新可用，則"**批准更新**"按鈕可用。
5. 儲存變更。

# 編輯適應性異常控制訊息範本

當使用者嘗試執行被適應性異常控制規則封鎖的操作時，Kaspersky Endpoint Security 會顯示一條訊息，提示封鎖了可能有害的操作。如果使用者認為該應用程式被錯誤地封鎖，使用者可使用訊息文字中的連結向公司區域網路管理員傳送訊息。

針對向管理員傳送有關封鎖潛在有害行為的訊息，系統提供了專用範本。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。

*若要編輯訊息範本，請執行下列操作：*

1. 在"應用程式主視窗"中，點擊 按鈕。
2. 在應用程式設定視窗中，選取"**安全控制**"→"**自適應異常控制**"。
3. 在"**範本**"塊中，設定適應性異常控制訊息範本：
   - **有關封鎖的訊息**當封鎖非典型操作的自適應異常控制規則觸發時，顯示給使用者的訊息的範本。
   - **傳送郵件給管理員**當使用者認為封鎖是錯誤的時可以傳送給本機公司網路系統管理員的訊息的範本。在使用者請求提供存取權限後，Kaspersky Endpoint Security 會向卡巴斯基安全管理中心傳送一個事件：**傳送給管理員的應用程式活動封鎖訊息**。事件描述包含一條給管理員的訊息，其中包含被替換的變數。您可以使用預定義事件選擇**使用者請求**在卡巴斯基安全管理中心主控台中檢視這些事件。如果您的組織沒有部署卡巴斯基安全管理中心或者沒有連線到管理伺服器，應用程式將向管理員傳送一條訊息到指定的電子郵件信箱。

   若要將變數新增至範本文字，請將游標置於所需位置，點擊**新增變數**，然後從可用選項清單中選取所需變數。

   此外，您也可使用**重設**按鈕，還原預設範本文字。
4. 儲存變更。

# 監控適應性異常控制操作

適應性異常控制包括幾種監控工具。監控適應性異常控制的主要目的是在訓練時配置元件。

適應性異常控制報告

適應性異常控制使用以下報告：

- **自適應異常控制規則狀態報告**該報告包含有關適應性異常控制規則狀態的資訊（*關閉*，*智慧培訓*，*智慧封鎖*，*通知*，*封鎖*）。該報告允許分析適應性異常控制的訓練水平，並評估從 *智慧培訓* 模式切換至正常運作模式（例如，*智慧封鎖*）的規則數目。

- **自適應異常控制規則觸發報告**此報告包含有關規則觸發的資訊。報告也展示規則觸發模式：*封鎖*（包括 *智慧封鎖*）或者 *通知*。該報告可以評估使用者電腦上適應性異常控制的活動。

**如何在管理主控台 (MMC) 中檢視適應性異常控制報告**

1. 在卡巴斯基安全管理中心管理主控台樹狀目錄中，選取**政策**。

2. 選擇必要的政策並點擊以開啟政策內容。

3. 在政策視窗中，選擇"**安全控制 → 自適應異常控制**"。

4. 請執行以下操作之一：

   - 如果您想檢視有關適應性異常控制規則狀態的報告，請點擊 **自適應異常控制規則狀態報告**連接。

   - 如果您想檢視有關被觸發的適應性異常控制規則的報告，請點擊 **自適應異常控制規則觸發報告**連接。

5. 報告建立過程將開始。

   此報告將顯示在新視窗中。

**如何在網頁主控台中檢視適應性異常控制報告**

1. 在網頁主控台的主視窗中，選擇**資產（裝置）→ 政策和設定檔**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"**安全控制**"→"**自適應異常控制**"。

5. 在"**規則**"塊中執行以下操作之一：

   - 如果您想檢視有關適應性異常控制規則狀態的報告，請選取**檢視報告 → 規則狀態**。

   - 如果您想檢視有關被觸發的適應性異常控制規則的報告，請點擊**檢視報告 → 偵測**。

6. 報告建立過程將開始。

   此報告將顯示在新視窗中。

若要在卡巴斯基安全管理中心主控台中產生報告，您必須啟用至管理伺服器的資料傳輸。預設情況下啟用資料傳輸。

**如何在管理主控台 (MMC) 中啟用為適應性異常控制進行資料傳輸**

1. 在卡巴斯基安全管理中心管理主控台樹狀目錄中，選取**政策**。
2. 選擇必要的政策並點擊以開啟政策內容。
3. 在政策視窗中，選擇"**一般設定 → 報告和儲存**"。
4. 在"**到管理伺服器的資料傳輸**"塊中，點擊"**設定**"按鈕。
5. 勾選以下核取方塊：
   - **自適應異常控制規則狀態報告**
   - **自適應異常控制規則觸發報告**
6. 儲存變更。

**如何在網頁主控台中啟用為適應性異常控制進行資料傳輸**

1. 在網頁主控台的主視窗中，選擇**資產（裝置）→ 政策和設定檔**。
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. 在**到管理伺服器的資料傳輸**下面，選擇以下核取方塊：
   - **自適應異常控制規則觸發報告**
   - **關於觸發的自適應異常控制規則的報告**
6. 儲存變更。

智慧培訓狀態中的規則觸發器 儲存

在訓練模式下，適應性異常控制會將有關已觸發規則的資訊傳送到單獨的存儲，**智慧培訓狀態中的規則觸發器**。有關已觸發規則的資訊在儲存中以事件清單的形式表示。若要調整適應性異常控制，您可以確認電腦上的異常行為，或者 新增規則排除項目。

"適應性異常控制"事件

適應性異常控制可記錄*封鎖*（包括 *智慧封鎖*）和 *通知*模式下的規則觸發事件。為此目的提供了以下事件：

**處理程序操作已封鎖**

**已略過處理程序操作**

事件包含有關可疑活動的資訊，包括檔案總和檢查碼、涉及的使用者、規則觸發時間和電腦名稱。分析事件後，如果您發現該活動合法，則可以立即從規則中新增排除項目。

# 應用程式控制

"應用程式控制"管理使用者電腦上的應用程式啟動。這允許您在使用應用程式時實行公司安全政策。"應用程式控制"還透過限制對應用程式的存取來降低電腦感染的風險。

設定"應用程式控制"包括以下步驟：

1. 建立應用程式類別。

   管理員建立管理員想要管理的應用程式類別。應用程式類別適用於公司網路中的所有電腦，與管理群組無關。要建立類別，您可以使用以下條件：KL 類別（例如，*瀏覽器*）、檔案雜湊、應用程式供應商和其他條件。

2. 建立應用程式控制規則。

   管理員在管理群組的政策中建立應用程式控制規則。該規則包括應用程式類別和這些類別中的應用程式啟動狀態：已封鎖或已允許。管理員可以建立許多規則。一個應用程式可能符合多個規則的條件。封鎖規則的優先等級高於允許規則的優先等級。Kaspersky Endpoint Security 每次啟動時都會檢查應用程式是否符合規則。Kaspersky Endpoint Security 會依序將應用程式與所有應用程式控制規則進行比對。

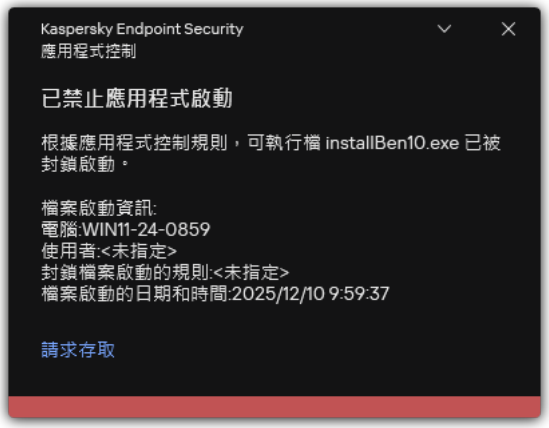
3. 選取應用程式控制模式。

   管理員選取對未包含在以下任何規則中之應用程式的處理模式（應用程式拒絕清單和允許清單）。

當使用者嘗試啟動已禁止的應用程式時，Kaspersky Endpoint Security 將封鎖該應用程式啟動並顯示通知（請參見下圖）。

系統提供了一種*測試模式*來檢查"應用程式控制"的設定。在此模式下，Kaspersky Endpoint Security 會執行以下操作：

- 允許啟動應用程式，包括已禁止的應用程式。
- 顯示有關已禁止之應用程式啟動的通知，並將資訊新增到使用者電腦上的報告中。
- 將有關已禁止之應用程式啟動的資料傳送到卡巴斯基安全管理中心。




"應用程式控制"通知

## “應用程式控制”執行模式

“應用程式控制”元件可在兩種模式下執行：

- **拒絕清單**在此模式下，“應用程式控制”允許使用者啟動除了應用程式控制規則中禁止的應用程式以外的所有應用程式。

  預設情況下，會啟用“應用程式控制”此一模式。

- **允許清單**在此模式下，“應用程式控制”會封鎖使用者啟動除了應用程式控制規則中允許和未禁止的應用程式以外的所有應用程式。

  如果完整設定了“應用程式控制”的允許規則，則該元件將封鎖啟動所有未經區域網路管理員驗證的新應用程式，同時允許執行使用者在工作中依賴的作業系統和受信任應用程式。

  您可以閱讀有關在允許清單模式下設定應用程式控制規則的建議。

可以使用 Kaspersky Endpoint Security 本機介面和卡巴斯基安全管理中心將“應用程式控制”設定為在這些模式下執行。

但是，卡巴斯基安全管理中心提供了在 Kaspersky Endpoint Security 本機介面中不可使用的工具，例如以下工作所需的工具：

- 建立應用程式類別。

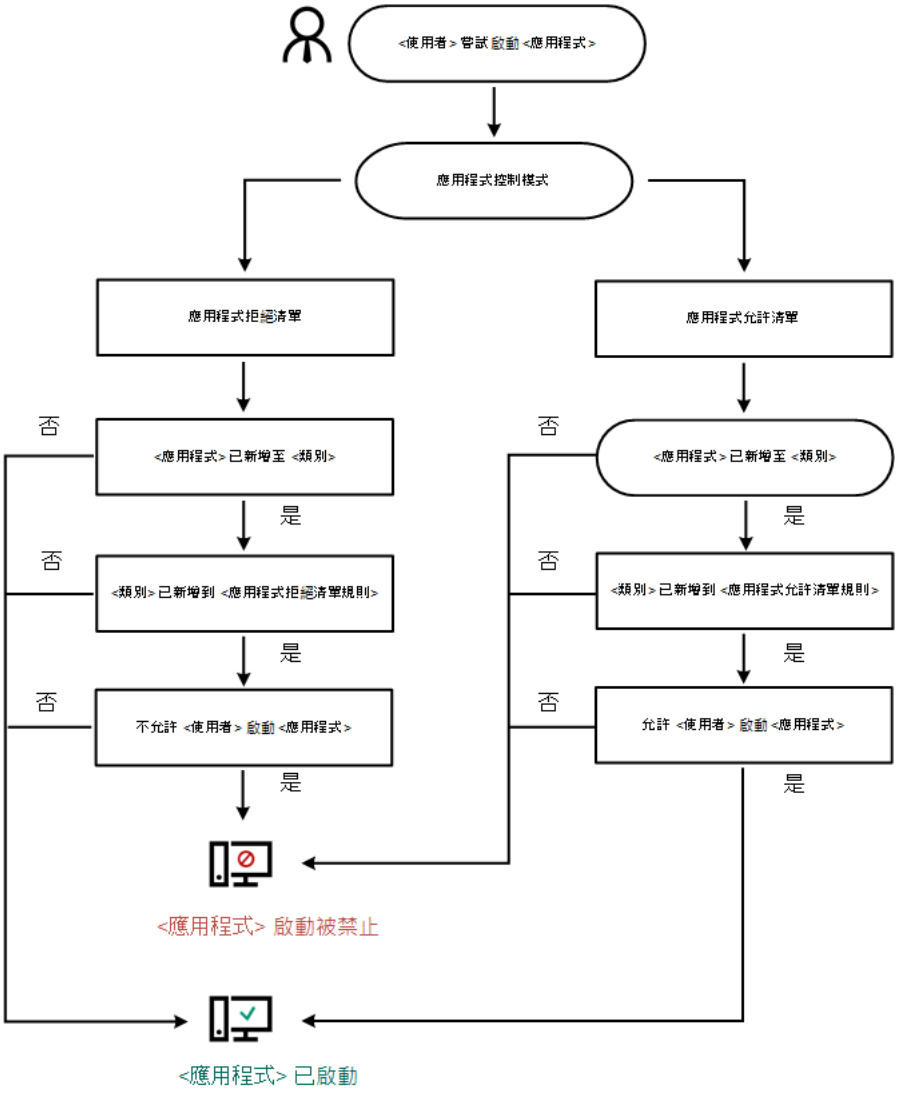
  在卡巴斯基安全管理中心管理主控台中建的應用程式控制規則，以您的自訂的應用程式類別為主，而不是以像 Kaspersky Endpoint Security 本機介面中的包含和排除條件為主。

- 接收有關安裝在公司區域網路電腦上的應用程式資訊。

因此，建議使用卡巴斯基安全管理中心設定“應用程式控制”元件的執行。

“應用程式控制”執行演算法

Kaspersky Endpoint Security 使用算法來決定是否啟動應用程式（請參見下圖）。




“應用程式控制”執行演算法

# 應用程式控制功能限制

在以下情況中“應用程式控制”元件的執行受到限制：

- 應用程式版本升級時，不支援匯入“應用程式控制”元件設定。
- 如果沒有與 KSN 伺服器連線，則 Kaspersky Endpoint Security 將僅從本機資料庫中接收關於應用程式及其模組信譽的資訊。

  Kaspersky Endpoint Security 指定為 KL 類別“**其他軟體\根據 KSN 信譽受信任的其他軟體**/根據是否可連線到 KSN 伺服器而不同。

- 在卡巴斯基安全管理中心資料庫中可以儲存 150,000 份已處理檔案的資訊。一旦達到這一數量的記錄，新的檔案將不會被處理。要還原清單操作，您必須從安裝了 Kaspersky Endpoint Security 的電腦上刪除之前存在卡巴斯基安全管理中心資料庫中的檔案。
- 此元件不會控制指令碼的啟動，除非透過命令列將指令碼傳送給解譯器。

  如果應用程式控制規則允許解譯器的啟動，則此元件將不會封鎖從此解譯器啟動指令碼。

  如果應用程式控制規則從一開始就封鎖解譯器命令列中指定的至少一個指令碼，該元件將封鎖解譯器命令列中指定的所有指令碼。
- 此元件不會封鎖從不受 Kaspersky Endpoint Security 支援的解譯器啟動指令碼。

  Kaspersky Endpoint Security 支援以下解譯器：

  - Java
  - PowerShell

  支援以下類型的解譯器：

  - %ComSpec%;
  - %SystemRoot%\system32\regedit.exe
  - %SystemRoot%\regedit.exe
  - %SystemRoot%\system32\regedt32.exe
  - %SystemRoot%\system32\cscript.exe
  - %SystemRoot%\system32\wscript.exe
  - %SystemRoot%\system32\msiexec.exe
  - %SystemRoot%\system32\mshta.exe
  - %SystemRoot%\system32\rundll32.exe
  - %SystemRoot%\system32\wwahost.exe
  - %SystemRoot%\syswow64\cmd.exe
  - %SystemRoot%\syswow64\regedit.exe
  - %SystemRoot%\syswow64\regedt32.exe
  - %SystemRoot%\syswow64\cscript.exe
  - %SystemRoot%\syswow64\wscript.exe
  - %SystemRoot%\syswow64\msiexec.exe

- %SystemRoot%\syswow64\mshta.exe
- %SystemRoot%\syswow64\rundll32.exe
- %SystemRoot%\syswow64\wwahost.exe

# 接收有關安裝在使用者電腦上的應用程式的資訊

要建立最佳化的應用程式控制規則，建議首先思考一下公司 LAN 中電腦上使用的應用程式。若要執行操作，您可以獲得以下資訊：

- 格式區域網路電腦上使用的應用程式供應商、版本和中文化語言。
- 程式更新頻率。
- 公司中所使用的應用程式使用政策（這可能是安全性政策或管理政策）。
- 應用程式分發套件的儲存位置。

## 檢視應用程式資訊

已安裝應用程式的資訊由卡巴斯基安全管理中心網路代理提供。已安裝應用程式的資訊由卡巴斯基安全管理中心網路代理在**應用程式登錄資料**資料夾中提供。網路代理每次與卡巴斯基安全管理中心同步時都會更新資訊。有關網路代理傳送的資訊詳情，請參閱卡巴斯基安全管理中心說明。

*要在"應用程式登錄資料"資料夾中開啟應用程式內容視窗：*

1. 開啟卡巴斯基安全管理中心管理主控台。
2. 在管理主控台樹狀目錄中，選擇**進階 → 應用程式管理 → 應用程式登錄資料**。
3. 選取應用程式。
4. 在應用程式的內容功能表中，選取"**內容**"。

## 檢視有關可執行檔的資訊

您可以在查詢可執行檔資訊時減少資料庫的負載。為了實現這一點，我們建議在安裝了標準軟體集的幾台參考電腦上執行 *清查* 工作。

您可以使用 Kaspersky Endpoint Security 的*清查*工作獲取可執行檔清單。您可以在卡巴斯基安全管理中心主控台的"**可執行檔**"資料夾中檢視正在執行的可執行檔的清單。

在執行 *清查* 工作之前，請確保資料庫符合卡巴斯基安全管理中心的建議。有關資料庫限制的詳細資訊，請參閱卡巴斯基安全管理中心說明。

**如何在管理主控台 (MMC) 中執行清查工作**

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

啟動"工作精靈"。按照精靈的說明進行操作。

步驟 1. 選取工作類型

選取**"Kaspersky Endpoint Security for Windows (12.12)"→"清查"**。

步驟 2. 清查範圍

建立您希望 Kaspersky Endpoint Security 在其中尋找可執行檔的資料夾清單。配置清查設定（參見下表）。

步驟 3. 選取將要對其分配工作的裝置

選取將要執行工作的電腦。下列選項可用：

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

步驟 4. 選取要執行工作的帳戶

選取要執行*清查*工作的帳戶。預設情況下，Kaspersky Endpoint Security 將使用本機使用者帳戶的權限啟動工作。如果清查範圍包括網路磁碟機或存取受限的其他物件，請選擇具有足夠存取權限的使用者帳戶。

步驟 5. 設定工作啟動排程

設定工作排程，例如手動。

步驟 6. 定義工作名稱

輸入工作的名稱，例如“*基線清查*”。

步驟 7. 完成工作建立

結束精靈。如有必要，選中“**精靈完成時執行工作**”核取方塊。您可以在工作內容中監控工作進度。結果，根據配置排程在使用者的電腦上執行可執行檔的搜尋。

**如何在網頁主控台和雲端主控台中執行清查工作**

1. 在網頁主控台的主視窗中，選擇**資產（裝置）→ 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 Windows 12.12.0**”。

   b. 在“**工作類型**”下拉式清單中，選取“**Inventory**”。

   c. 在“**工作名稱**”欄位中，輸入簡要說明，例如“*基線清查*”。

   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。前往下一步。

5. 選取要執行工作的帳戶。預設情況下，Kaspersky Endpoint Security 將使用本機使用者帳戶的權限啟動工作。

6. 結束精靈。

   在工作清單中將顯示一個新工作。

7. 若要配置工作，請前往工作屬性（請參閱下表）。

8. 選中該工作旁邊的核取方塊。

9. 點擊“**開始**”。

   您可以監控工作的狀態，以及成功完成工作或完成工作時發生錯誤的裝置數量。結果，將按照指定排程在使用者電腦上搜尋可執行檔。

| 參數 | 描述 |
| --- | --- |
| **清查範圍** | 構成清查範圍的物件清單。 |
| **DLL 模組清查** | Kaspersky Endpoint Security 在清查範圍內尋找 DLL 模組並將資訊傳送到 卡巴斯基安全管理中心。<br>啟用 DLL 模組清查會顯著增加完成清查工作所需的時間和資料庫的大小。 |
| **指令碼檔案清查** | Kaspersky Endpoint Security 在清查範圍內尋找指令碼並將資訊傳送到 卡巴斯基安全管理中心。<br>啟用指令碼檔案清查會顯著增加完成清查工作所需的時間和資料庫的大小。 |
| **當螢幕防護程式處於非作用中狀態且電腦未鎖定時暫停排程掃描** | 電腦資源繁忙時，推遲工作的啟動。如果電腦已鎖定或熒幕保護程式已開啟，Kaspersky Endpoint Security 會啟動掃描工作。如果您中斷了執行工作（例如，透過解鎖電腦），Kaspersky Endpoint Security 會自動執行工作，從被中斷的地方繼續。此排程選項可讓您在使用電腦時節省電腦資源。 |
| **只掃描新增及修改的檔案** | 僅掃描新檔案和自上次掃描以來已被修改的檔案。這有助於縮短掃描的持續時間。此模式適用於簡單檔案和複合檔案。 |
| **略過掃描時間超過以下時長的檔案（秒）N 秒** | 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。 |
| **掃描壓縮檔案** | 掃描 ZIP、GZIP、BZIP、RAR、TAR、ARJ、CAB、LHA、JAR、ICE 和其它存檔。應用程式不僅依照副檔名而且依照格式掃描存檔。當檢查封存時，應用程式會執行巡迴解壓縮。這可讓人偵測多層封存（封存內的封存）內的威脅。 |
| **掃描分發套件** | 掃描協力廠商應用程式的分發套件。 |
| **複合檔案大於指定值時不解壓縮** | 如果選中該核取方塊，應用程式不會掃描其大小超過指定值的複合檔案。<br>如果清除該核取方塊，應用程式將掃描所有大小的複合檔案。<br>應用程式會掃描從存檔中提取的大檔案，而不管是否選中該核取方塊。 |

*要開啟"可執行檔"資料夾中的可執行檔的內容視窗：*

1. 開啟卡巴斯基安全管理中心管理主控台。
2. 在管理主控台樹狀目錄中，選擇**進階 → 應用程式管理 → 可執行檔**。
3. 選取可執行檔。
4. 在可執行檔的內容功能表中，選擇"**內容**"。

要檢視該應用程式及其可執行檔的一般資訊以及安裝了該應用程式的電腦的清單，請開啟在"**應用程式登錄資料**"資料夾或"**可執行檔**"資料夾中選取的應用程式的內容視窗。

## 更新有關已安裝的應用程式和可執行檔案的資訊

從 Kaspersky Endpoint Security 12.3 for Windows 開始，應用程式控制元件對執行檔資料庫的操作得到了最佳化。檔案被從電腦中刪除後，Kaspersky Endpoint Security 12.3 for Windows 會自動更新資料庫。這可以使資料庫保持最新並節省卡巴斯基安全管理中心資源。

為了使已安裝應用程式的資料庫保持最新，必須啟用向管理伺服器傳送應用程式資訊（預設情況下啟用）。

**如何在管理主控台 (MMC) 中啟用應用程式資訊提交**

1. 在卡巴斯基安全管理中心管理主控台樹狀目錄中，選取**政策**。
2. 選擇必要的政策並點擊以開啟政策內容。
3. 在政策視窗中，選擇**"一般設定 → 報告和儲存"**。
4. 在**"到管理伺服器的資料傳輸"**塊中，點擊**"設定"**按鈕。
5. 選擇**"已啟動的應用程式"**核取方塊。
6. 儲存變更。

**如何透過網頁主控台和雲端主控台啟用應用程式資訊提交**

1. 在網頁主控台的主視窗中，選擇**資產（裝置）→ 政策和設定檔**。
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. 在**"到管理伺服器的資料傳輸"**塊中，點擊**"進階設定"**按鈕。
6. 在開啟的視窗中，選中**"關於已啟動的應用程式"**核取方塊。
7. 儲存變更。

# 如何啟用被封鎖的應用程式模式

在*已封鎖的應用程式*模式下，"應用程式控制"允許使用者啟動除了應用程式控制規則中禁止的應用程式以外的所有應用程式。也就是說，如果不存在拒絕規則，應用程式控制將允許啟動該應用程式。預設情況下，會啟用**"**應用程式控制"此一模式。

> 在啟用 *已封鎖的應用程式* 模式之前，我們建議測試您的應用程式控制規則。為此，您可以 啟用測試模式。

**如何在管理主控台 (MMC) 中選擇被封鎖的應用程式模式**

1. 開啟卡巴斯基安全管理中心管理主控台。
2. 在主控台樹狀目錄中，選擇**"政策"**。
3. 選擇必要的政策並點擊以開啟政策內容。
4. 在政策視窗中，選擇**"安全控制 → 應用程式控制"**。
5. 選擇**"應用程式控制"**核取方塊。
6. 在**"應用程式控制設定"**塊中，使用**"控制模式"**下拉清單選擇**拒絕清單**。

7. 在“**動作**”下拉清單中，選取應用程式的操作：

   - **測試規則**應用程式控制不會封鎖被規則阻止執行的應用程式，但會產生有關原本會被阻止的應用程式執行的事件。
   - **套用規則**應用程式控制可封鎖被封鎖的應用程式並產生相應的事件。

8. 選擇應用程式控制規則的狀態：

   - **啟用**此狀態表示在“應用程式控制”元件執行時使用該規則。
   - **關閉**此狀態表示在“應用程式控制”元件執行時略過該規則。
   - **測試**此狀態表示 Kaspersky Endpoint Security 總是允許啟動套用了規則的應用程式，但會在報告中記錄與啟動此類別應用程式有關的資訊。

   如有需要，新增應用程式控制規則。

9. 配置應用程式控制的進階設定：

   - **監控 DLL 模組的載入（顯著增加系統負載）**如果選定此核取方塊，Kaspersky Endpoint Security 將在使用者啟動應用程式時控制 DLL 模組的載入。有關 DLL 模組和載入此 DLL 模組的應用程式的資訊將記錄在此報告中。

     當啟用對載入 DLL 模組和驅動程式的控制時，請確保在“應用程式控制”設定中已啟用以下規則之一：預設**黃金映像**規則或其他包含"**黃金映像\受信任憑證**" KL 類別的規則，並確保在啟動 Kaspersky Endpoint Security 之前載入受信任的 DLL 模組和驅動程式。如果在停用“**黃金映像**”規則時啟用對載入 DLL 模組和驅動程式的控制，可能導致作業系統不穩定。

     Kaspersky Endpoint Security 僅監控自選中核取方塊後載入的 DLL 模組和驅動程式。選中核取方塊後，建議重新啟動電腦以確保應用程式監控所有 DLL 模組和驅動，包括在啟動 Kaspersky Endpoint Security 之前加載的模組和驅動。

   - **使用嚴格的數位簽章驗證**您可以選擇憑證作為應用程式控制規則的觸發條件。如果選取此核取方塊，Kaspersky Endpoint Security 會將規則套用於僅使用來自受信任的系統憑證存儲的憑證簽署的應用程式。使用此類憑證簽署的應用程式也被視為受防護元件信任，例如 *惡意軟體掃描* 工作。但是，如果您在應用程式控制規則中指定來自不同儲存空間的憑證，Kaspersky Endpoint Security 不會套用此類規則。

     如果清除該核取方塊，Kaspersky Endpoint Security 會將規則套用於由 Windows Trusted Root Certificate Store 中的憑證簽署的應用程式。此類應用程式不屬於受信任區域。防護元件監視此類應用程式的活動。

   - **有關封鎖的訊息**當觸發了某個封鎖應用程式啟動的應用程式控制規則時所顯示的訊息範本。
   - **傳送郵件給管理員**當使用者相信某個應用程式被錯誤地封鎖時，可以傳送給公司區域網路管理員的訊息模組。

10. 儲存變更。若要在電腦上套用該政策，請關閉掛鎖。

**如何在網頁主控台和雲端主控台中配置被封鎖的應用程式模式**

1. 在網頁主控台的主視窗中，選擇**資產（裝置）→政策和設定檔**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"**安全控制**"→"**應用程式控制**"。

5. 開啟"**應用程式控制已啟用**"開關。

6. 在"**操作模式**"塊中，選取"**封鎖除規則清單外的所有內容**"。

7. 在 **操作** 塊中，選擇應用程式控制的操作：

   - **通知**應用程式控制不會封鎖被規則阻止執行的應用程式，但會產生有關原本會被阻止的應用程式執行的事件。
   - **套用規則**應用程式控制可封鎖被封鎖的應用程式並產生相應的事件。

8. 選擇應用程式控制規則的狀態：

   - **已啟用**此狀態表示在"應用程式控制"元件執行時使用該規則。
   - **已停用**此狀態表示在"應用程式控制"元件執行時略過該規則。
   - **測試模式**此狀態表示 Kaspersky Endpoint Security 總是允許啟動套用了規則的應用程式，但會在報告中記錄與啟動此類別應用程式有關的資訊。

   如有需要，新增應用程式控制規則。

9. 配置應用程式控制的進階設定：

   - **監控 DLL 模組的載入**如果選定此核取方塊，Kaspersky Endpoint Security 將在使用者啟動應用程式時控制 DLL 模組的載入。有關 DLL 模組和載入此 DLL 模組的應用程式的資訊將記錄在此報告中。

     當啟用對載入 DLL 模組和驅動程式的控制時，請確保在"應用程式控制"設定中已啟用以下規則之一：預設**黃金映像**規則或其他包含"**黃金映像\受信任憑證**" KL 類別的規則，並確保在啟動 Kaspersky Endpoint Security 之前載入受信任的 DLL 模組和驅動程式。如果在停用"**黃金映像**"規則時啟用對載入 DLL 模組和驅動程式的控制，可能導致作業系統不穩定。

     Kaspersky Endpoint Security 僅監控自選中核取方塊後載入的 DLL 模組和驅動程式。選中核取方塊後，建議重新啟動電腦以確保應用程式監控所有 DLL 模組和驅動，包括在啟動 Kaspersky Endpoint Security 之前加載的模組和驅動。

   - **使用嚴格的數位簽章驗證**您可以選擇憑證作為應用程式控制規則的觸發條件。如果選取此核取方塊，Kaspersky Endpoint Security 會將規則套用於僅使用來自受信任的系統憑證存儲的憑證簽署的應用程式。使用此類憑證簽署的應用程式也被視為受防護元件信任，例如 *惡意軟體掃描* 工作。但是，如果您在應用程式控制規則中指定來自不同儲存空間的憑證，Kaspersky Endpoint Security 不會套用此類規則。

     如果清除該核取方塊，Kaspersky Endpoint Security 會將規則套用於由 Windows Trusted Root Certificate Store 中的憑證簽署的應用程式。此類應用程式不屬於受信任區域。防護元件監視此類應用程式的活動。

   - **傳送給使用者的郵件**當觸發了某個封鎖應用程式啟動的應用程式控制規則時所顯示的訊息範本。
   - **傳送給管理員的郵件**當使用者相信某個應用程式被錯誤地封鎖時，可以傳送給公司區域網路管理員的訊息模組。

10. 儲存變更。若要在電腦上套用該政策，請關閉掛鎖。

**如何在應用程式介面中選擇被封鎖的應用程式模式**

1. 在"應用程式主視窗"中，點擊⚙按鈕。
2. 在應用程式設定視窗中，選取"**安全控制**"→"**應用程式控制**"。
3. 開啟"**應用程式控制**"開關。
4. 在"**應用程式啟動控制模式**"塊中，選取"**拒絕清單。允許除了規則清單中的應用程式以外的所有應用程式**"。
5. 在 **啟動被規則封鎖的應用程式時的動作** 塊中，選擇應用程式控制的操作：
   - **告知（測試模式）並將事件記錄在 報告**。應用程式控制不會封鎖被規則阻止執行的應用程式，但會產生有關原本會被阻止的應用程式執行的事件。
   - **封鎖**應用程式控制可封鎖被封鎖的應用程式並產生相應的事件。
6. 選擇應用程式控制規則的狀態：
   - **已啟用**此狀態表示在"應用程式控制"元件執行時使用該規則。
   - **已停用**此狀態表示在"應用程式控制"元件執行時略過該規則。
   - **測試模式**此狀態表示 Kaspersky Endpoint Security 總是允許啟動套用了規則的應用程式，但會在報告中記錄與啟動此類別應用程式有關的資訊。

   如有需要，新增應用程式控制規則。
7. 配置應用程式控制的進階設定：
   - **監控 DLL 模組載入**如果選定此核取方塊，Kaspersky Endpoint Security 將在使用者啟動應用程式時控制 DLL 模組的載入。有關 DLL 模組和載入此 DLL 模組的應用程式的資訊將記錄在此報告中。

     當啟用對載入 DLL 模組和驅動程式的控制時，請確保在"應用程式控制"設定中已啟用以下規則之一：預設**黃金映像**規則或其他包含"**黃金映像\受信任憑證**" KL 類別的規則，並確保在啟動 Kaspersky Endpoint Security 之前載入受信任的 DLL 模組和驅動程式。如果在停用"**黃金映像**"規則時啟用對載入 DLL 模組和驅動程式的控制，可能導致作業系統不穩定。

     Kaspersky Endpoint Security 僅監控自選中核取方塊後載入的 DLL 模組和驅動程式。選中核取方塊後，建議重新啟動電腦以確保應用程式監控所有 DLL 模組和驅動，包括在啟動 Kaspersky Endpoint Security 之前加載的模組和驅動。
   - **使用嚴格的數位簽章驗證**您可以選擇憑證作為應用程式控制規則的觸發條件。如果選取此核取方塊，Kaspersky Endpoint Security 會將規則套用於僅使用來自受信任的系統憑證存儲的憑證簽署的應用程式。使用此類憑證簽署的應用程式也被視為受防護元件信任，例如 *惡意軟體掃描* 工作。但是，如果您在應用程式控制規則中指定來自不同儲存空間的憑證，Kaspersky Endpoint Security 不會套用此類規則。

     如果清除該核取方塊，Kaspersky Endpoint Security 會將規則套用於由 Windows Trusted Root Certificate Store 中的憑證簽署的應用程式。此類應用程式不屬於受信任區域。防護元件監視此類應用程式的活動。

- **有關應用程式封鎖的訊息範本**當觸發了某個封鎖應用程式啟動的應用程式控制規則時所顯示的訊息範本。
- **當應用程式被封鎖啟動時顯示的通知範本。**當使用者相信某個應用程式被錯誤地封鎖時，可以傳送給公司區域網路管理員的訊息模組。

8. 儲存變更。

結果，應用程式控制會封鎖被封鎖的應用程式。Kaspersky Endpoint Security 會產生 *已禁止應用程式啟動* 事件。您可以使用這些事件在卡巴斯基安全管理中心主控台中產生 *禁止的應用程式報告* 報告。在報告摘要中，您可以檢視觸發應用程式控制規則的應用程式和電腦的清單。

# 基於基線電腦的應用程式控制

您可以使用基線電腦來建立包含一組所需應用程式的映像。然後，您可以使用該映像在其他電腦上部署作業系統和應用程式。保持映像始終處於最新狀態並不總是可行。應用程式控制可讓您根據基線電腦維護允許的應用程式清單。應用程式控制會自動確定基線電腦上安裝了哪些應用程式並更新類別。這樣，電腦就獲得了最新的允許應用程式清單。

配置基於基線電腦的應用程式控制涉及以下步驟：

1. 建立自動更新類別。建立新類別時，選擇 **包括特定資料夾中的可執行檔的類別** 類別並選擇您的基線電腦。

   **如何在管理主控台 (MMC) 中建立自動更新類別**

   1. 開啟卡巴斯基安全管理中心管理主控台。
   2. 在管理主控台樹狀目錄中，選擇**進階 → 應用程式管理 → 應用程式類別**。
   3. 在工作區中點擊**新類別**按鈕。
      這將啟動應用程式類別建立精靈。
   4. 請按照應用程式類別建立精靈的指示操作。

步驟 1. 選擇類別類型

選擇 **包含選定裝置的可執行檔的類別** 作為類別類型。

步驟 2. 輸入使用者類別名稱

在此步驟中，為應用程式類別指定一個名稱。

步驟 3. 設定

如果您選取“**包含選定裝置的可執行檔的類別**”類別類型，此步驟可用。

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。**"可執行檔"**資料夾中指定電腦的所有可執行檔都將由卡巴斯基安全管理中心新增到此應用程式類別。

在此步驟還可以配置以下設定：

- 雜湊函數計算的演算法。要選擇演算法，您必須選中以下至少一個核取方塊：
  - **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）**
  - **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）**
- **"與管理伺服器儲存區同步資料"**核取方塊。如果您希望卡巴斯基安全管理中心定期清除應用程式類別並將**"可執行檔"**資料夾中指定電腦的所有可執行檔新增到該類別，請選取該核取方塊。

  如果清除**"與管理伺服器儲存區同步資料"**核取方塊，卡巴斯基安全管理中心在應用程式類別建立後不會對其進行任何修改。

步驟 4. 篩選

在此步驟中，配置檔案的篩選器。

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。預設情況下已勾選此選項。
- **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。

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。預設情況下已勾選此選項。
- **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. 建立自訂類別

結束精靈。

**如何在網頁主控台和 Cloud Console 中建立自動新增內容的類別**

1. 在網頁主控台的主視窗中，選擇**操作 → 第三方應用程式 → 應用程式類別**。

   這將開啟應用程式規則清單。

2. 點擊**"新增"**。

   這將啟動應用程式類別建立精靈。

3. 配置應用程式類別的一般設定：

   - 類別名稱。
   - 類別建立方法。選擇 **包含選定裝置的可執行檔的類別** 作為類別類型。

   前往下一步。

4. 配置應用程式類別的進階設定：

   - 指定卡巴斯基安全管理中心將為其將執行檔新增至應用程式類別的電腦。**"可執行檔"**資料夾中指定電腦的所有可執行檔都將由卡巴斯基安全管理中心新增到此應用程式類別。
   - 雜湊函數計算的演算法。
   - 配置與管理伺服器儲存同步資料的間隔。
   - 配置檔案的篩選器。

5. 結束精靈。

建立自動更新的類別時，將檔案細分為多個類別可能會很方便。例如，作業系統檔案和來自 Program Files 資料夾的檔案。為此，您可以在類別設定中使用篩選器並選擇單個資料夾。

2. 選取應用程式控制模式。您需要阻止所有未明確允許的應用程式的執行。為此，請選擇 *已封鎖的應用程式* 模式。

3. 建立應用程式控制規則。在規則設定中，選擇基線電腦的可執行檔所屬的類別。

   **如何在管理主控台 (MMC) 中配置基於基線電腦的應用程式控制**

   1. 開啟卡巴斯基安全管理中心管理主控台。
   2. 在主控台樹狀目錄中，選擇**"政策"**。
   3. 選擇必要的政策並點擊以開啟政策內容。
   4. 在政策視窗中，選擇**"安全控制 → 應用程式控制"**。
   5. 選擇**"應用程式控制"**核取方塊。
   6. 在**"應用程式控制設定"**塊中，使用**"控制模式"**下拉清單選擇**拒絕清單**。
   7. 在**"動作"**下拉清單中，選取應用程式的操作：
      - **測試規則**應用程式控制不會封鎖被規則阻止執行的應用程式，但會產生有關原本會被阻止的應用程式執行的事件。
      - **套用規則**應用程式控制可封鎖被封鎖的應用程式並產生相應的事件。
   8. 在應用程式控制規則清單中，點擊**"新增"**按鈕。

      這將啟動應用程式規則新增精靈。
   9. 在 **類別** 下拉清單中，選擇基於基線電腦的自動更新類別。
   10. 選擇要對其套用應用程式控制規則的使用者或使用者群組。

11. 配置應用程式控制規則的進階設定：

    - **拒絕其他使用者**應用程式會阻止所有不在清單中的使用者啟動屬於所選類別的應用程式。
    - **信任的更新程式**Kaspersky Endpoint Security 會將選定類別中包括的應用程式視為受信任更新程式，允許其建立將被允許隨後執行的其他可執行檔。

12. 儲存變更。若要在電腦上套用該政策，請關閉掛鎖。

**如何在網頁主控台和雲端主控台中配置基於基線電腦的應用程式控制**

1. 在網頁主控台的主視窗中，選擇**資產（裝置）→政策和設定檔**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**"安全控制"→"應用程式控制"**。
5. 開啟**"應用程式控制已啟用"**開關。
6. 在**"操作模式"**塊中，選取**"封鎖除規則清單外的所有內容"**。
7. 在 **操作** 塊中，選擇應用程式控制的操作：

    - **通知**應用程式控制不會封鎖被規則阻止執行的應用程式，但會產生有關原本會被阻止的應用程式執行的事件。
    - **套用規則**應用程式控制可封鎖被封鎖的應用程式並產生相應的事件。

8. 在應用程式控制規則清單中，點擊**"新增"**按鈕。

   這將啟動應用程式規則新增精靈。
9. 在 **類別/應用程式** 下面，選擇基於基線電腦的自動更新類別。
10. 選擇要對其套用應用程式控制規則的使用者或使用者群組。
11. 配置應用程式控制規則的進階設定：

    - **使用者**應用程式會阻止所有不在清單中的使用者啟動屬於所選類別的應用程式。
    - **信任的更新程式**Kaspersky Endpoint Security 會將選定類別中包括的應用程式視為受信任更新程式，允許其建立將被允許隨後執行的其他可執行檔。

12. 儲存變更。若要在電腦上套用該政策，請關閉掛鎖。

**如何在應用程式介面中配置基於基線電腦的應用程式控制**

1. 在**"**應用程式主視窗**"**中，點擊 按鈕。
2. 在應用程式設定視窗中，選取**"安全控制"→"應用程式控制"**。
3. 開啟**"應用程式控制"**開關。

4. 在**"應用程式啟動控制模式"**塊中，選取**"拒絕清單。允許除了規則清單中的應用程式以外的所有應用程式"**。

5. 在 **啟動被規則封鎖的應用程式時的動作** 塊中，選擇應用程式控制的操作：

   - **告知（測試模式）並將事件記錄在 報告**。應用程式控制不會封鎖被規則阻止執行的應用程式，但會產生有關原本會被阻止的應用程式執行的事件。
   - **封鎖**應用程式控制可封鎖被封鎖的應用程式並產生相應的事件。

6. 在應用程式控制規則清單中，點擊**"新增"**按鈕。

   這將啟動應用程式規則新增精靈。

7. 在 **類別** 下面，選擇基於基線電腦的自動更新類別。

8. 選擇要對其套用應用程式控制規則的使用者或使用者群組。

9. 配置應用程式控制規則的進階設定：

   - **拒絕其他使用者**應用程式會阻止所有不在清單中的使用者啟動屬於所選類別的應用程式。
   - **信任的更新程式**Kaspersky Endpoint Security 會將選定類別中包括的應用程式視為受信任更新程式，允許其建立將被允許隨後執行的其他可執行檔。

10. 儲存變更。

# 管理應用程式控制規則

Kaspersky Endpoint Security 透過規則控制使用者對應用程式的啟動。應用程式控制規則指定觸發條件以及條件被觸發時"應用程式控制"元件指定的操作（使用者允許或封鎖應用程式啟動）。

## 規則觸發條件

觸發規則的條件具有以下相關性："條件類型 - 條件標準 - 條件值"。根據規則觸發條件，Kaspersky Endpoint Security 將對應用程式應用（或不應用）規則。

規則中使用以下類型的條件：

- *包含條件*。如果應用程式比對至少一個包括條件，Kaspersky Endpoint Security 會將規則應用至此應用程式。
- *排除條件*。如果應用程式比對至少一個排除條件並且不比對任何包括條件，Kaspersky Endpoint Security 不會將規則套用至此應用程式。

規則觸發條件使用標準進行建立。Kaspersky Endpoint Security 中使用以下標準建立規則：

- 應用程式可執行檔所在資料夾的路徑。
- 檔案內容（應用程式可執行檔名稱、磁碟上應用程式的可執行檔名稱、應用程式可執行檔的版本、應用程式名稱以及應用程式供應商）。
- 應用程式可執行檔的雜湊值 。

- 憑證：發佈者、主題、指紋。
- 應用程式是否屬於某 KL 類別。
- 卸除式磁碟機上應用程式可執行檔的位置。

必須為條件中使用的每個標準制定標準值。如果要啟動的應用程式參數符合包括條件中指定的標準值，則觸發規則。在這種情況下，“應用程式控制”將執行規則中指定的操作。如果應用程式參數比對排除條件中指定的值，“應用程式控制”不會控制應用程式的啟動。

如果您選擇了一個憑證作為規則觸發條件，則需要確保該憑證已被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。

觸發規則後由“應用程式控制”元件作出決定。

觸發操作後，“應用程式控制”將允許使用者（或使用者群組）啟動應用程式或封鎖啟動。您可以選取允許或不允許比對規則的應用程式啟動的使用者或使用者群組。

如果一個規則未指定那些被允許啟動符合此規則的應用程式使用者，則此規則稱為“*封鎖*”規則。

如果一個規則未指定任何不允許啟動符合此規則的應用程式使用者，則此規則稱為“*允許*”規則。

封鎖規則的優先等級高於允許規則的優先等級。例如，如果已經為一個使用者群組指定應用程式控制允許規則，但也為此使用者群組中的使用者指定一個應用程式控制封鎖規則，則此使用者將被封鎖啟動應用程式。

規則的執行狀態

應用程式控制規則可為以下兩個狀態值之一：

- **已啟用**此狀態表示在“應用程式控制”元件執行時使用該規則。
- **已停用**此狀態表示在“應用程式控制”元件執行時略過該規則。
- **測試模式**此狀態表示 Kaspersky Endpoint Security 允許啟動套用了規則的應用程式，但會在報告中記錄與啟動此類別應用程式有關的資訊。

## 為應用程式控制規則新增觸發條件

您可以建立應用程式類別，以便建立應用程式控制規則。

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。

*要在管理主控台中建立應用程式類別：*

1. 開啟卡巴斯基安全管理中心管理主控台。
2. 在管理主控台樹狀目錄中，選擇**進階 → 應用程式管理 → 應用程式類別**。
3. 在工作區中點擊**新類別**按鈕。
   使用者類別建立精靈將啟動。
4. 請按照使用者類別建立精靈的指示操作。

步驟 1. 選擇類別類型

在此步驟中，選擇以下應用程式類別之一：

- 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*設定在類別中納入應用程式的條件*步驟和 *設定從類別排除應用程式的條件*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，您可以在*設定*步驟中指定將自動包括在此類別中的可執行檔所屬的電腦。
- 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，您可以在*儲存區資料夾*步驟中指定將自動包括在類別中的可執行檔所來自的資料夾。

建立包含自動新增內容的類別時，卡巴斯基安全管理中心對以下格式的檔案執行清查：EXE, COM, DLL, SYS, BAT, PS1, CMD, JS, VBS, REG, MSI, MSC, CPL, HTML, HTM, DRV, OCX 和 SCR。

步驟 2. 輸入使用者類別名稱

在此步驟中，為應用程式類別指定一個名稱。

步驟 3. 配置將應用程式包括在類別中的條件

當新增大量條件到應用程式控制規則（例如檔案雜湊值）時，電腦資源的消耗會增加。當條件總數達到 50,000 時，可能會出現效能問題。為了最佳化效能，建議審查並減少條件數量。

如果您選擇"**包含手動新增內容的類別**"類別類型，此步驟可用。

在此步驟中，在"**新增**"下拉清單中選取用於將應用程式包括到類別中的條件：

- **從可執行檔清單**將用戶端裝置上的可執行檔清單中的應用程式新增到自訂類別。
- **從檔案內容**指定可執行檔的詳細資料，作為將應用程式新增到自訂類別的條件。
- **資料夾內檔案數位簽章**選擇用戶端裝置上包含可執行檔的資料夾。卡巴斯基安全管理中心會將這些可執行檔的中繼資料作為將應用程式新增到自訂類別的條件。
- **資料夾內檔案的總和檢查碼**選擇用戶端裝置上包含可執行檔的資料夾。卡巴斯基安全管理中心會將這些可執行檔的雜湊值作為將應用程式新增到自訂類別的條件。
- **資料夾中的檔案憑證**選擇用戶端裝置上包含帶憑證簽章的可執行檔的資料夾。卡巴斯基安全管理中心會將這些可執行檔的憑證作為將應用程式新增到自訂類別的條件。

  不建議使用其內容中未指定**憑證指紋**參數的條件。

- **MSI 安裝檔案的檔案內容**選取 MSI 套件。卡巴斯基安全管理中心會將 MSI 套件內封裝的可執行檔的中繼資料作為將應用程式新增到自訂類別的條件。
- **應用程式 MSI 安裝檔案的核對總和**選取 MSI 套件。卡巴斯基安全管理中心會將此 MSI 套件內封裝的可執行檔的雜湊值作為將應用程式新增到自訂類別的條件。
- **從 KL 類別**指定 KL 類別作為將應用程式新增到自訂類別的條件。*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。
- **指定應用程式路徑（支援遮罩）**選擇用戶端裝置上的資料夾。卡巴斯基安全管理中心會將此資料夾下的可執行檔新增到自訂類別。
- **從儲存區選取憑證**選取用來對可執行檔簽章的憑證作為將應用程式新增到自訂類別的條件。

  不建議使用其內容中未指定**憑證指紋**參數的條件。

  您可以選擇憑證儲存。預設情況下，應用程式控制僅對使用受信任系統憑證儲存中的憑證簽署的應用程式套用規則。這透過 **使用嚴格的數位簽章驗證** 核取方塊啟用。

- **磁碟機類型**指定儲存裝置類型（所有硬碟磁碟機和卸除式磁碟機，或者僅限卸除式磁碟機）作為將應用程式新增到自訂類別的條件。

步驟 4. 配置將應用程式從類別中排除的條件

如果您選擇“**包含手動新增內容的類別**”類別類型，此步驟可用。

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，在“**新增**”下拉清單中選取用於將應用程式從類別中排除的條件：

- **從可執行檔清單**將用戶端裝置上的可執行檔清單中的應用程式新增到自訂類別。
- **從檔案內容**指定可執行檔的詳細資料，作為將應用程式新增到自訂類別的條件。
- **資料夾內檔案數位簽章**選擇用戶端裝置上包含可執行檔的資料夾。卡巴斯基安全管理中心會將這些可執行檔的中繼資料作為將應用程式新增到自訂類別的條件。
- **資料夾內檔案的總和檢查碼**選擇用戶端裝置上包含可執行檔的資料夾。卡巴斯基安全管理中心會將這些可執行檔的雜湊值作為將應用程式新增到自訂類別的條件。
- **資料夾中的檔案憑證**選擇用戶端裝置上包含帶憑證簽章的可執行檔的資料夾。卡巴斯基安全管理中心會將這些可執行檔的憑證作為將應用程式新增到自訂類別的條件。
- **MSI 安裝檔案的檔案內容**選取 MSI 套件。卡巴斯基安全管理中心會將 MSI 套件內封裝的可執行檔的中繼資料作為將應用程式新增到自訂類別的條件。
- **應用程式 MSI 安裝檔案的核對總和**選取 MSI 套件。卡巴斯基安全管理中心會將此 MSI 套件內封裝的可執行檔的雜湊值作為將應用程式新增到自訂類別的條件。
- **從 KL 類別**指定 KL 類別作為將應用程式新增到自訂類別的條件。*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。
- **指定應用程式路徑（支援遮罩）**選擇用戶端裝置上的資料夾。卡巴斯基安全管理中心會將此資料夾下的可執行檔新增到自訂類別。
- **從儲存區選取憑證**選取用來對可執行檔簽章的憑證作為將應用程式新增到自訂類別的條件。
- **磁碟機類型**指定儲存裝置類型（所有硬碟磁碟機和卸除式磁碟機，或者僅限卸除式磁碟機）作為將應用程式新增到自訂類別的條件。

步驟 5. 設定

如果您選取“**包含選定裝置的可執行檔的類別**”類別類型，此步驟可用。

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。**"可執行檔"**資料夾中指定電腦的所有可執行檔都將由卡巴斯基安全管理中心新增到此應用程式類別。

在此步驟還可以配置以下設定：

- 雜湊函數計算的演算法。要選擇演算法，您必須選中以下至少一個核取方塊：
  - **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）**
  - **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）**
- **"與管理伺服器儲存區同步資料"**核取方塊。如果您希望卡巴斯基安全管理中心定期清除應用程式類別並將**"可執行檔"**資料夾中指定電腦的所有可執行檔新增到該類別，請選取該核取方塊。

  如果清除**"與管理伺服器儲存區同步資料"**核取方塊，卡巴斯基安全管理中心在應用程式類別建立後不會對其進行任何修改。

步驟 6. 儲存庫資料夾

如果您選取**"包括來自指定資料夾的可執行檔的類別"**類別類型，此步驟可用。

在此步驟中，指定卡巴斯基安全管理中心將在其中搜尋可執行檔的資料夾，以便自動將應用程式新增到該應用程式類別。

在此步驟還可以配置以下設定：

- **"包含動態連結程式庫 (DLL) 到該類別"**核取方塊。如果您希望將動態連結程式庫（DLL 檔案）包含在應用程式類別中，請選中此核取方塊。

  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。

- **"包含指令碼到該類別"**核取方塊。如果您希望將指令碼包含在應用程式類別中，請選中此核取方塊。

  在應用程式類別中包含指令碼可能降低卡巴斯基安全管理中心的效能。

- 雜湊函數計算的演算法。要選擇演算法，您必須選中以下至少一個核取方塊：
  - **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）**
  - **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）**
- **"強制掃描資料夾以尋找變更"**核取方塊。如果您希望卡巴斯基安全管理中心在用於自動新增到應用程式類別的資料夾中定期搜尋可執行檔，請選擇此核取方塊。

  如果清除**"強制掃描資料夾以尋找變更"**核取方塊，卡巴斯基安全管理中心僅在用於自動新增到應用程式類別的資料夾有變更、該資料夾內新增或刪除了檔案時才在該資料夾中搜尋可執行檔。

- **掃描間隔（1–168 小時）**欄位。在此欄位中，您可以指定卡巴斯基安全管理中心在用於自動新增到應用程式類別的資料夾中搜尋可執行檔的時間間隔（以小時為單位）。

  如果選取了**強制掃描資料夾以尋找變更**核取方塊，則此欄位可用。

步驟 7. 建立自訂類別

結束精靈。

*要在應用程式介面中為應用程式控制規則新增觸發條件：*

1. 在"應用程式主視窗"中，點擊⚙按鈕。
2. 在應用程式設定視窗中，選取"**安全控制**"→"**應用程式控制**"。
3. 點擊"**已封鎖的應用程式**"或"**允許的應用程式**"按鈕。

   這將開啟應用程式控制規則清單。
4. 選取要為其配置觸發條件的規則。

   應用程式控制規則屬性將開啟。
5. 選擇"**條件：N**"標籤或"**排除項目：N**"標籤，然後點擊"**新增**"按鈕。
6. 選擇應用程式控制規則的觸發條件：

   - **根據已執行過的應用程式內容建立條件**在正執行應用程式的清單中，您可以選擇將套用應用程式控制規則的應用程式。Kaspersky Endpoint Security 還列出了之前在電腦上執行的應用程式。您需要選擇要用於建立一個或多個規則觸發條件的條件：**檔案雜湊**、**憑證**、**KL 類別**、**檔案內容**或**檔案或資料夾路徑**。
   - **條件"KL 類別"**。*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。
   - **自訂條件**您可以選擇應用程式檔案並選擇規則觸發條件之一：**檔案雜湊**、**憑證**、**檔案內容**或**檔案或資料夾路徑**。
   - **按照檔案磁碟機的條件（卸除式磁碟機）**應用程式控制規則僅適用於在卸除式磁碟機上執行的檔案。
   - **來自指定資料夾中檔案內容的條件**應用程式控制規則僅適用於指定資料夾中的檔案。您還可以在子資料夾中包含或排除檔案。您需要選擇要用於建立一個或多個規則觸發條件的條件：**檔案雜湊**、**憑證**、**KL 類別**、**檔案內容**或**檔案或資料夾路徑**。
7. 儲存變更。

新增條件時，請考慮應用程式控制的以下特殊注意事項：

- Kaspersky Endpoint Security 支援 `*` 和 `?` 字元用於在元資料中輸入遮罩：**檔案名稱**、**應用程式名稱**、**供應商**。
- Kaspersky Endpoint Security 不支援擁有雜湊代碼的 MD5 檔案並且不會基於 MD5 雜湊控制應用程式的啟動。規則觸發條件使用了 SHA256 雜湊代碼。

- 不建議僅將**發佈者**和**憑證主旨**標準設定為規則觸發條件。使用這些標準不可靠。
- 如果您在"**檔案或資料夾路徑**"欄位中使用符號連結，建議您解析符號連結以正確操作應用程式控制規則。要執行此操作，請點擊"**解析符號連結**"按鈕。

## 將"可執行檔"資料夾中的可執行檔新增到應用程式類別

在"**可執行檔**"資料夾中，將顯示在電腦上的偵測到的可執行檔清單。Kaspersky Endpoint Security 在執行清查工作後生成可執行檔清單。

*要將"可執行檔"資料夾中的可執行檔新增到應用程式類別：*

1. 開啟卡巴斯基安全管理中心管理主控台。
2. 在管理主控台樹狀目錄中，選擇**進階 → 應用程式管理 → 可執行檔**。
3. 在工作區中，選擇要新增到應用程式類別的可執行檔。
4. 右鍵點擊以開啟選定可執行檔的內容功能表，然後選取"**新增到類別**"。
5. 在開啟的視窗中，執行以下操作：
   - 在視窗上部，選擇下列選項之一：
     - **新增到新的應用程式類別**如果您要建立新的應用程式類別並向其中新增可執行檔，則選擇此選項。
     - **新增到現有應用程式類別**如果您要選取現有應用程式類別並向其中新增可執行檔，則選擇此選項。
   - 在"**規則類型**"塊中，選取以下選項之一：
     - **新增到包含的規則**如果您要建立將可執行檔新增到應用程式類別的條件，則選擇此選項。
     - **新增到排除的規則**如果您要建立將可執行檔從應用程式類別排除的條件，則選擇此選項。
   - 在"**用作條件的參數**"塊，選取以下選項之一：
     - **憑證詳情（如果檔案沒有憑證，則為 SHA256 雜湊）**
     - **憑證詳情（沒有憑證的檔案將被略過）**
     - **僅 SHA256（沒有雜湊的檔案將被略過）**
     - **僅 MD5（停產模式，僅適用於 Kaspersky Endpoint Security 10 Service Pack 1 版本）**
6. 儲存變更。

## 將事件相關的可執行檔新增到應用程式類別

*要將與應用程式控制事件相關聯的可執行檔新增到應用程式類別中：*

1. 開啟卡巴斯基安全管理中心管理主控台。
2. 在管理主控台樹狀目錄的**管理伺服器**節點中選取**事件**標籤。
3. 在**"事件分類"**下拉式清單中，選擇與應用程式控制元件的操作相關的事件（檢視"應用程式控制"元件的執行所產生的事件，檢視"應用程式控制"元件的測試執行所產生的事件）。
4. 點擊**"執行分類"**按鈕。
5. 選擇您要將其相關可執行檔新增到應用程式類別的事件。
6. 右鍵點擊以開啟選定事件的內容功能表，然後選取**"新增到類別"**。
7. 在開啟的視窗中，配置應用程式類別的設定：
   - 在視窗上部，選擇下列選項之一：
     - **新增到新的應用程式類別**。如果您要建立新的應用程式類別並向其中新增可執行檔，則選擇此選項。
     - **新增到現有應用程式類別**。如果您要選取現有應用程式類別並向其中新增可執行檔，則選擇此選項。
   - 在**"規則類型"**塊中，選取以下選項之一：
     - **新增到包含的規則**。如果您要建立將可執行檔新增到應用程式類別的條件，則選擇此選項。
     - **新增到排除的規則**。如果您要建立將可執行檔從應用程式類別排除的條件，則選擇此選項。
   - 在**"用作條件的參數"**塊，選取以下選項之一：
     - **憑證詳情（或沒有憑證的檔案的 SHA-256 雜湊）**。
     - **憑證詳情（沒有憑證的檔案將被略過）**。
     - **僅 SHA-256（沒有雜湊的檔案將被略過）**。
     - **僅 MD5（停產模式，僅適用 Kaspersky Endpoint Security 10 Service Pack 1 版本）**。
8. 儲存變更。

## 新增應用程式控制規則

*要使用卡巴斯基安全管理中心新增應用程式控制規則：*

1. 在卡巴斯基安全管理中心管理主控台樹狀目錄中，選取**政策**。
2. 選擇必要的政策並點擊以開啟政策內容。

3. 在政策視窗中，選擇“**安全控制 → 應用程式控制**”。

   在視窗右側，顯示了“應用程式控制”元件的設定。

4. 點擊“**新增**”。

   開啟“**應用程式控制規則**”視窗。

5. 請執行以下操作之一：

   - 如果要建立新類別：

     a. 點擊“**建立類別**”。

     使用者類別建立精靈將啟動。

     b. 請按照使用者類別建立精靈的指示操作。

     c. 在“**類別**”下拉清單中，選取所建立的應用程式類別。

   - 如果要編輯現有類別：

     a. 在“**類別**”下拉清單中，選取要編輯的已建立的應用程式類別。

     b. 點擊“**內容**”。

     c. 修改所選應用程式類別的設定。

     d. 儲存變更。

     e. 在“**類別**”下拉清單中，選取您要依據其建立規則的應用程式類別。

6. 在“**使用者及其權限**”表中，點擊“**新增**”按鈕。

   您可以在 Active Directory 中、在卡巴斯基安全管理中心的账户清單中或透過手動輸入本機使用者名稱來選擇使用者。卡巴斯基建議僅在無法使用網域使用者帳戶的特殊情況下使用本機使用者帳戶。

7. 在“**使用者及其權限**”表中，執行以下操作：

   - 如果您希望允許使用者和/或使用者群組啟動屬於選定類別的應用程式，則選取相關行中的“**允許**”核取方塊。

   - 如果您希望封鎖使用者和/或使用者群組啟動屬於選定類別的應用程式，則選取相關行中的“**封鎖**”核取方塊。

8. 如果您想要沒有出現在“**使用者或群組**”列中且不屬於“**使用者或群組**”列指定的使用者群組的使用者被封鎖啟動屬於所選類別的應用程式，請選擇“**拒絕其他使用者**”核取方塊。

9. 如果您希望 Kaspersky Endpoint Security 將選定應用程式類別中包括的應用程式視為信任更新程式，並且希望允許它們建立將被允許隨後執行的其它可執行檔，請選取“**信任的更新程式**”核取方塊。

   在轉移 Kaspersky Endpoint Security 設定時，也會轉移信任更新程式建立的可執行檔清單。

10. 儲存變更。

*要新增應用程式控制規則：*

1. 在"應用程式主視窗"中，點擊⚙按鈕。
2. 在應用程式設定視窗中，選取"**安全控制**"→"**應用程式控制**"。
3. 點擊"**已封鎖的應用程式**"或"**允許的應用程式**"按鈕。

   這將開啟應用程式控制規則清單。
4. 點擊"**新增**"。

   這會開啟"應用程式控制規則"設定視窗。
5. 在"**一般設定**"標籤上，定義規則的主要設定：

   a. 在"**規則名稱**"欄位中輸入規則的名稱。

   b. 在"**描述**"欄位中輸入規則的描述。

   c. 在"**使用者及其權限**"表中，點擊"**新增**"按鈕。

   您可以在 Active Directory 中、在卡巴斯基安全管理中心的账户清單中或透過手動輸入本機使用者名稱來選擇使用者。卡巴斯基建議僅在無法使用網域使用者帳戶的特殊情況下使用本機使用者帳戶。

   該規則預設適用於所有使用者。

   > 如果該表中沒有指定使用者，則無法儲存該規則。

   d. 在"**使用者及其權限**"表中，使用開關定義使用者啟動應用程式的權限。

   e. 如果您想要應用程式防止滿足規則觸發條件的應用程式為未列在"**使用者及其權限**"表中和未列在"**使用者及其權限**"表中的使用者群組成員的使用者執行，請選擇"**拒絕其他使用者**"核取方塊。

   > 如果清空了"**拒絕其他使用者**"核取方塊，則 Kaspersky Endpoint Security 不會控制"**使用者及其權限**"表中未指定的使用者以及不屬於"**使用者及其權限**"表中指定使用者群組的使用者啟動應用程式。

   f. 如果您想要 Kaspersky Endpoint Security 將符合規則觸發條件的應用程式視為信任的更新程式，請選擇"**信任的更新程式**"核取方塊。*信任的更新程式*是被允許建立其它可執行檔的應用程式，這些可執行檔將被允許隨後執行。

   如果一個應用程式觸發了多個規則，Kaspersky Endpoint Security 將在滿足以下條件的情況下設定"*信任的更新程式*"旗標：

   - 所有規則允許應用程式執行。
   - 至少一個規則選擇了"**信任的更新程式**"核取方塊。
6. 在"**條件：N**"標籤上，建立或編輯用於觸發規則的包含條件清單。
7. 在"**排除項目：N** "標籤上，建立或編輯用於觸發規則的排除條件清單。

   在轉移 Kaspersky Endpoint Security 設定時，也會轉移信任更新程式建立的可執行檔清單。
8. 儲存變更。

## 透過卡巴斯基安全管理中心變更應用程式控制規則的狀態

*要在管理主控台中變更應用程式控制規則的狀態：*

1. 在卡巴斯基安全管理中心管理主控台樹狀目錄中，選取**政策**。
2. 選擇必要的政策並點擊以開啟政策內容。
3. 在政策視窗中，選擇**"安全控制 → 應用程式控制"**。
   在視窗右側，顯示了"應用程式控制"元件的設定。
4. 在**"狀態"**列中，點擊左鍵顯示內容功能表，並選擇以下選項之一：
   - **啟用**此狀態表示在"應用程式控制"元件執行時使用該規則。
   - **關閉**此狀態表示在"應用程式控制"元件執行時略過該規則。
   - **測試**此狀態表示 Kaspersky Endpoint Security 總是允許啟動套用了規則的應用程式，但會在報告中記錄與啟動此類別應用程式有關的資訊。
5. 儲存變更。

*要在應用程式介面中變更應用程式控制規則的狀態：*

1. 在"應用程式主視窗"中，點擊⚙ 按鈕。
2. 在應用程式設定視窗中，選取**"安全控制"→"應用程式控制"**。
3. 點擊**"已封鎖的應用程式"**或**"允許的應用程式"**按鈕。
   這將開啟應用程式控制規則清單。
4. 在**"狀態"**列中，開啟內容功能表，並選取以下選項之一：
   - **已啟用**此狀態表示在"應用程式控制"元件執行時使用該規則。
   - **已停用**此狀態表示在"應用程式控制"元件執行時略過該規則。
   - **測試模式**此狀態表示 Kaspersky Endpoint Security 總是允許啟動套用了該規則的應用程式，但會在報告中記錄與啟動此類別應用程式有關的資訊。
5. 儲存變更。

## 匯出和匯入應用程式控制規則

您可以將應用程式控制規則清單匯出到 XML 檔案。您可以使用匯出/匯入功能來備份應用程式控制規則清單，或將清單遷移到其他伺服器。

匯出和匯入應用程式控制規則時，請記住以下特殊注意事項：

- Kaspersky Endpoint Security 僅匯出活動應用程式控制模式的規則清單。換句話說，如果應用程式控制在拒絕清單模式下運行，則 Kaspersky Endpoint Security 將只會匯出此模式的規則。要匯出允許清單模式的規則清單，您需要切換模式並再次執行匯出操作。
- Kaspersky Endpoint Security 使用應用程式類別來使應用程式控制規則起作用。將應用程式控制規則清單轉換到其他伺服器時，還需要轉換應用程式類別清單。有關匯出或匯入應用程式類別的更多詳細資訊，請參閱卡巴斯基安全管理中心說明。

**如何在管理主控台 (MMC) 中匯出和匯入應用程式控制規則清單**

1. 在卡巴斯基安全管理中心管理主控台樹狀目錄中，選取**政策**。
2. 選擇必要的政策並點擊以開啟政策內容。
3. 在政策視窗中，選擇"**安全控制 → 應用程式控制**"。
4. 要匯出應用程式控制規則清單：
   a. 選取您想要匯出的規則。要選擇多個連接埠，請使用**CTRL**或**SHIFT**鍵。
      如果您未選擇任何規則，則 Kaspersky Endpoint Security 將匯出所有規則。
   b. 點擊"**匯出**"連接。
   c. 在開啟的視窗中，指定您要將規則清單匯出到的 XML 檔案的名稱，然後選取要儲存此檔案的資料夾。
   d. 儲存檔案。
      Kaspersky Endpoint Security 會將規則清單匯出到 XML 檔案。
5. 要匯入應用程式控制規則清單：
   a. 點擊"**匯入**"連接。
      在開啟的視窗中，選取要從中匯入規則清單的 XML 檔案。
   b. 開啟檔案。
      如果電腦已經具有規則清單，則 Kaspersky Endpoint Security 將提示您刪除現有清單或從 XML 檔案向其中新增新項目。
6. 儲存變更。

**如何在網頁主控台和雲端主控台中匯出和匯入應用程式控制規則清單**

1. 在網頁主控台的主視窗中，選擇**資產（裝置） → 政策和設定檔**。
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. 在**操作模式**下面，選擇規則清單：應用程式拒絕清單或允許清單。

6. 要匯出規則清單：

   a. 選取您想要匯出的規則。

   b. 點擊 → **匯出** 按鈕。

      Kaspersky Endpoint Security 會將規則清單匯出到預設下載資料夾中的 JSON 檔案。

7. 要匯入規則清單：

   a. 點擊 → **匯入** 按鈕。

      在開啟的視窗中，選取要從中匯入規則清單的 JSON 檔案。

   b. 開啟檔案。

      如果電腦已經具有規則清單，則 Kaspersky Endpoint Security 將提示您刪除現有清單或從 JSON 檔案向其中新增新項目。

8. 儲存變更。

## 檢視"應用程式控制"元件的執行所產生的事件

*要檢視卡巴斯基安全管理中心收到的由"應用程式控制"元件的執行所產生的事件：*

1. 開啟卡巴斯基安全管理中心管理主控台。
2. 在管理主控台樹狀目錄的**管理伺服器**節點中選取**事件**標籤。
3. 點擊"**建立新分類**"按鈕。
4. 在開啟的視窗中，轉到"**事件**"區域。
5. 點擊"**全部清除**"按鈕。
6. 在"**事件**"表中選擇"**已禁止應用程式啟動**"核取方塊。
7. 儲存變更。
8. 在"**事件分類**"下拉清單中選擇建立的集合。
9. 點擊"**執行分類**"按鈕。

## 檢視有關封鎖的應用程式的報告

*要檢視有關封鎖的應用程式的報告：*

1. 開啟卡巴斯基安全管理中心管理主控台。
2. 在管理主控台樹狀目錄的**管理伺服器**節點中選取"**報告**"標籤。

3. 點擊**"新增報告範本"**。

   "新報告範本精靈"將啟動。

4. 按照"報告範本精靈"的說明進行操作。在 **選取報告範本類型** 步驟選擇 **其他 → 禁止的應用程式報告**。

   完成新報告範本精靈之後，新報告範本將出現在**"報告"**標籤上。

5. 點擊報告將其開啟。

報告建立過程將開始。此報告將顯示在新視窗中。

# 測試應用程式控制規則

要確保應用程式控制規則不會封鎖工作所需的應用程式，建議啟用應用程式控制規則的測試並在建立新規則後分析其執行。啟用應用程式控制規則的測試後，Kaspersky Endpoint Security 不會封鎖被"應用程式控制"封鎖啟動的應用程式，但是會將有關它們啟動的通知傳送給管理伺服器。

分析應用程式控制規則的執行需要檢視報告給卡巴斯基安全管理中心的已發生的應用程式控制事件。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，建議您更新已建立的規則的設定，建立附加規則或刪除現有規則。

預設情況下，Kaspersky Endpoint Security 允許啟動所有應用程式，但規則禁止的應用程式除外。

## 啟用和停用應用程式控制規則測試

*要在卡巴斯基安全管理中心中啟用或停用應用程式控制規則的測試：*

1. 在卡巴斯基安全管理中心管理主控台樹狀目錄中，選取**政策**。

2. 選擇必要的政策並點擊以開啟政策內容。

3. 在政策視窗中，選擇**"安全控制 → 應用程式控制"**。

   在視窗右側，顯示了"應用程式控制"元件的設定。

4. 在**"控制模式"**下拉清單中選取以下項之一：

   - **拒絕清單**如果選擇此選項，應用程式控制將允許所有使用者啟動所有應用程式，符合應用程式控制封鎖規則的應用程式除外。

   - **允許清單**如果選擇此選項，應用程式控制將封鎖所有使用者啟動任何應用程式，符合應用程式控制允許規則的應用程式除外。

5. 請執行以下操作之一：

   - 如果要啟用應用程式控制規則的測試，請在**"動作"**下拉式清單中選擇**"測試規則"**選項。

   - 如果您想要啟用應用程式控制以管理使用者電腦上的應用程式的啟動，請在下拉式清單中選擇**"套用規則"**。

6. 儲存變更。

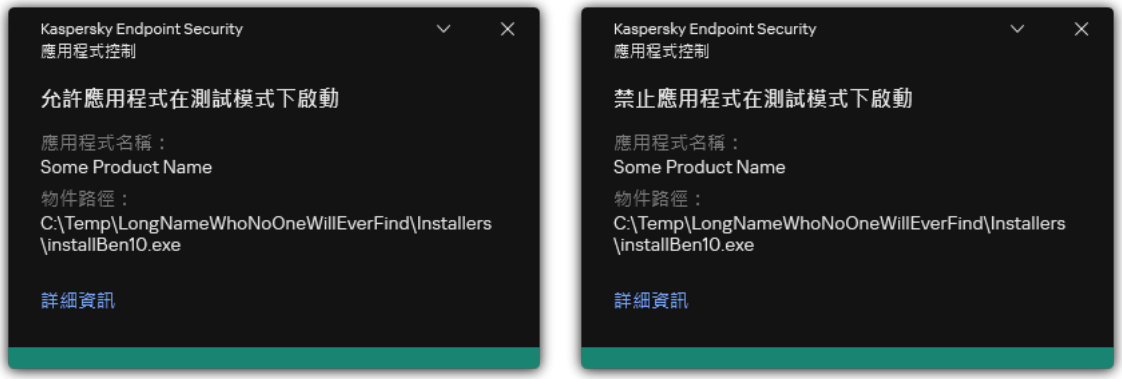
*要啟用應用程式控制規則的測試或為"應用程式控制"選擇封鎖操作：*

1. 在"應用程式主視窗"中，點擊⚙按鈕。
2. 在應用程式設定視窗中，選取"**安全控制**"→"**應用程式控制**"。
3. 點擊"**已封鎖的應用程式**"或"**允許的應用程式**"按鈕。

   這將開啟應用程式控制規則清單。
4. 在"**狀態**"列中，選取"**測試模式**"。

   此狀態表示 Kaspersky Endpoint Security 總是允許啟動套用了該規則的應用程式，但會在報告中記錄與啟動此類別應用程式有關的資訊。
5. 儲存變更。

Kaspersky Endpoint Security 不會封鎖被"應用程式控制"規則封鎖啟動的應用程式，但是會將它們的啟動報告給管理伺服器。您也可以就在使用者的電腦上進行規則測試設定通知顯示（請見下圖）。




測試模式中的"應用程式控制"通知

## 檢視有關測試模式下封鎖的應用程式的報告

*要檢視有關測試模式下封鎖的應用程式的報告：*

1. 開啟卡巴斯基安全管理中心管理主控台。
2. 在管理主控台樹狀目錄的**管理伺服器**節點中選取"**報告**"標籤。
3. 點擊"**新增報告範本**"。

   "新報告範本精靈"將啟動。
4. 按照"報告範本精靈"的說明進行操作。在 **選取報告範本類型** 步驟，選擇 **其他 → 測試模式中禁止的應用程式報告**。

   完成新報告範本精靈之後，新報告範本將出現在"**報告**"標籤上。
5. 點擊報告將其開啟。

報告建立過程將開始。此報告將顯示在新視窗中。

## 檢視"應用程式控制"元件的測試執行所產生的事件

*要檢視卡巴斯基安全管理中心收到的應用程式控制測試事件：*

1. 開啟卡巴斯基安全管理中心管理主控台。
2. 在管理主控台樹狀目錄的**管理伺服器**節點中選取**事件**標籤。
3. 點擊**"建立新分類"**按鈕。
4. 在開啟的視窗中，轉到**"事件"**區域。
5. 點擊**"全部清除"**按鈕。
6. 在**"事件"**表中選擇**"禁止應用程式在測試模式下啟動"**以及**"允許應用程式在測試模式下啟動"**核取方塊。
7. 儲存變更。
8. 在**"事件分類"**下拉清單中選擇建立的集合。
9. 點擊**"執行分類"**按鈕。

# 應用程式活動監控

如果 Kaspersky Endpoint Security 安裝在執行 Windows for Workstations 的電腦上，則該元件可用。如果 Kaspersky Endpoint Security 安裝在執行 Windows for Servers 的電腦上，則該元件不可用。

*應用程式活動監控*是一個用於即時檢視使用者電腦上的應用程式活動資訊的工具。

使用應用程式活動監控需要安裝應用程式控制和主機入侵防禦元件。如果未安裝這些元件，則應用程式活動監控區域會在應用程式主視窗中被隱藏。

*要啟動應用程式活動監控：*

在應用程式主視窗的**"正在監控"**區域中，點擊**"應用程式活動監控"**圖標。

在此視窗中，有關使用者的電腦上的應用程式活動的資訊將呈現在三個標籤上：

- **"所有應用程式"**標籤顯示有關電腦上安裝的所有應用程式的資訊。
- **"正在執行"**標籤即時顯示有關每個應用程式消耗的電腦資源的資訊。在此標籤中，您還可以繼續配置單個應用程式的權限。
- **"系統啟動時執行"**標籤顯示作業系統啟動時啟動的應用程式的清單。

如果您想要隱藏使用者電腦上的應用程式活動資訊，您可以限制使用者對"應用程式活動監控"工具的存取權限。

**如何使用管理主控台 (MMC) 在應用程式介面中隱藏應用程式活動監控**

1. 在卡巴斯基安全管理中心管理主控台樹狀目錄中，選取**政策**。
2. 選擇必要的政策並點擊以開啟政策內容。
3. 在政策視窗中，選擇"**一般設定 → 介面**"。
4. 使用"**隱藏應用程式活動監控區域**"核取方塊授予或者撤銷對工具的存取。
5. 儲存變更。

**如何使用網頁主控台和雲端主控台在應用程式介面中隱藏應用程式活動監控**

1. 在網頁主控台的主視窗中，選擇**資產（裝置）→ 政策和設定檔**。
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. 使用"**隱藏應用程式活動監控區域**"核取方塊授予或者撤銷對工具的存取。
6. 儲存變更。

# 為檔案或資料夾建立名稱遮罩的規則

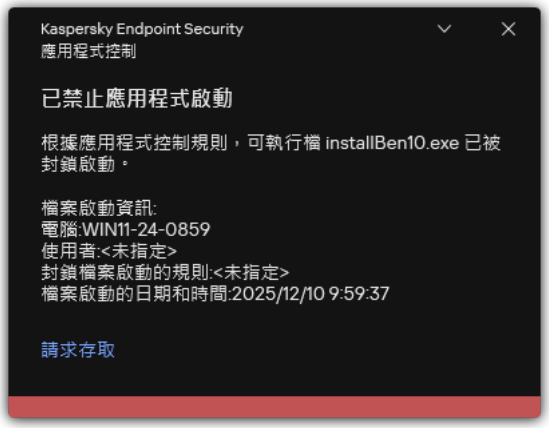
*檔案或資料夾名稱的遮罩*是使用通用字元對資料夾名稱或檔案名稱和副檔名的表示。

您可以使用以下一般字元建立檔案或資料夾名稱遮罩：

- `*`（星號）字元，可替換任何字元集合（包括空集合）。例如，`C:\*.txt`遮罩將包括位於 (C:) 磁碟機上資料夾和子資料夾中所有帶 `txt` 副檔名的檔案的路徑。
- `?`（問號）字元代表任意單個字元，但 `\` 和 `/` 字元除外（這兩個字元是檔案和資料夾路徑中的檔案和資料夾名稱的分隔符號）。例如，遮罩 `C:\Folder\???.txt` 將包括位於 `Folder` 資料夾中所有帶 TXT 副檔名且名稱由三個字元構成的檔案的路徑。

# 編輯應用程式控制訊息範本

使用者嘗試啟動被應用程式控制規則封鎖的應用程式時，Kaspersky Endpoint Security 會顯示訊息，指明該應用程式被封鎖啟動。卡巴斯基專家向使用者提供訊息範本，描述應用程式被封鎖的原因（見下圖）。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。




"應用程式控制"通知

如果您認為該應用程式被錯誤地封鎖啟動，可使用訊息內容中的連結向公司區域網路管理員傳送訊息。為此，使用者必須點擊 **請求存取** 按鈕並向管理員傳送一條訊息描述情況。您也可以準備一個傳送給管理員的訊息範本，向其中新增資料，以便您決定允許或封鎖對應用程式的存取。在使用者請求提供存取權限後，Kaspersky Endpoint Security 會向卡巴斯基安全管理中心傳送一個事件：**傳送給管理員的應用程式啟動封鎖訊息**。事件描述包含一條給管理員的訊息，其中包含被替換的變數。您可以使用預定義事件選擇**使用者請求**在卡巴斯基安全管理中心主控台中檢視這些事件。如果您的組織沒有部署卡巴斯基安全管理中心或者沒有連線到管理伺服器，應用程式將向管理員傳送一條訊息到指定的電子郵件信箱。

### 如何在管理主控台 (MMC) 中編輯應用程式控制訊息範本

1. 在卡巴斯基安全管理中心管理主控台樹狀目錄中，選取**政策**。
2. 選擇必要的政策並點擊以開啟政策內容。
3. 在政策視窗中，選擇"**安全控制 → 應用程式控制**"。
4. 在"**訊息範本設定**"塊中，點擊"**範本**"按鈕。
5. 這會開啟一個視窗；在該視窗中，配置應用程式控制範本：

   - **有關封鎖的訊息**當觸發了某個封鎖應用程式啟動的應用程式控制規則時所顯示的訊息範本。

     您無法在"測試模式"中設定應用程式控制的訊息範本。測試模式中的應用程式控制會顯示預設通知。

   - **傳送郵件給管理員**當使用者相信某個應用程式被錯誤地封鎖時，可以傳送給公司區域網路管理員的訊息模組。

   若要將變數新增至範本文字，請將游標置於所需位置，點擊**變數**，然後從可用選項清單中選取所需變數。

   此外，您也可使用**根據預設**按鈕，還原預設範本文字。

6. 儲存變更。

**如何在 Web 主控台和雲端主控台中編輯應用程式控制訊息**

1. 在網頁主控台的主視窗中，選擇**資產（裝置）→政策和設定檔**。
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. 在 **訊息範本** 區塊中，點擊 **有關應用程式啟動封鎖的訊息** 連結和配置應用程式控制訊息的範本：
   - **傳送給使用者的郵件**當觸發了某個封鎖應用程式啟動的應用程式控制規則時所顯示的訊息範本。
     您無法在"測試模式"中設定應用程式控制的訊息範本。測試模式中的應用程式控制會顯示預設通知。
   - **傳送給管理員的郵件**當使用者相信某個應用程式被錯誤地封鎖時，可以傳送給公司區域網路管理員的訊息模組。

   若要將變數新增至範本文字，請將游標置於所需位置，點擊**新增變數**，然後從可用選項清單中選取所需變數。
   此外，您也可使用**重設為預設值**按鈕，還原預設範本文字。
6. 儲存變更。

**如何在應用程式介面中編輯應用程式控制訊息範本**

1. 在"應用程式主視窗"中，點擊⚙按鈕。
2. 在應用程式設定視窗中，選取"**安全控制**"→"**應用程式控制**"。
3. 在"**有關應用程式封鎖的訊息範本**"塊中，設定"應用程式控制"訊息的範本：
   - **有關封鎖的訊息**當觸發了某個封鎖應用程式啟動的應用程式控制規則時所顯示的訊息範本。
     您無法在"測試模式"中設定應用程式控制的訊息範本。測試模式中的應用程式控制會顯示預設通知。
   - **傳送郵件給管理員**當使用者相信某個應用程式被錯誤地封鎖時，可以傳送給公司區域網路管理員的訊息模組。

   若要將變數新增至範本文字，請將游標置於所需位置，點擊**新增變數**，然後從可用選項清單中選取所需變數。
   此外，您也可使用**重設**按鈕，還原預設範本文字。
4. 儲存變更。

# 應用程式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：

- **已觸發的規則的名稱 – %RULE%**。
  封鎖檔案執行的規則的名稱。

- **目前日期** – %DATE%。

  檔案執行被封鎖的日期，格式為 DD.HH.YYYY。

- **目前時間** – %TIME%。

  檔案執行被封鎖的時間，格式為 HH:MM。

- **使用者名稱** – %USER_NAME%。

  檔案執行被封鎖的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%。

  執行在其上被封鎖的電腦的名稱。

- **可執行檔名稱** – %FILE_NAME%。

  被封鎖應用程式的可執行檔的名稱。

- **可執行檔的 KL 類別** – %KL_CAT%。

  被封鎖的應用程式所屬的 KL 類別（例如，*瀏覽器*）。

- **可執行檔的路徑** – %FILE_PATH%。

  被封鎖應用程式的可執行檔的完整路徑。

- **可執行檔版本** – %FILE_VERSION%。

  被封鎖應用程式的可執行檔的版本。

- **可執行檔的原始名稱** – %ORIGINAL_FILE_NAME%。

  被封鎖應用程式的可執行檔的原始名稱。檔案名稱在應用程式可執行檔的屬性中指定。

- **供應商** – %FILE_PUBLISHER%。

  被封鎖應用程式的供應商。

- **應用程式名稱** – %FILE_PRODUCT_NAME%。

  被封鎖應用程式的名稱。

- **應用程式版本** – %PRODUCT_VERSION%。

  被封鎖應用程式的版本。

- **可執行檔的雜湊** – %FILE_HASH%。

  被封鎖應用程式可執行檔的雜湊值 。

- **憑證發放者** – %CERT_ISSUER%。

  可執行檔簽章所用的憑證的核發者。

- **憑證主旨** – %CERT_SUBJECT%。

  可執行檔簽章所用的憑證的主旨。

- **憑證指紋** – %CERT_THUMBPRINT%。

  可執行檔簽章所用的憑證的指紋。

# 實施允許的應用程式清單的最佳實踐

計畫實施允許的應用程式清單時，建議執行以下操作：

1. 形成以下類型的群組：

   - 使用者群組。需要設定為允許使用各種應用程式集的使用者群組。
   - 管理群組。卡巴斯基安全管理中心將允許的應用程式清單套用於的一個或多個電腦群組。如果為這些群組使用不同的允許清單設定，則有必要建立多個電腦群組。

2. 建立必須允許啟動的應用程式清單。

   在建立清單前，建議執行以下操作：

   a. 執行清查工作。

      清查工作的建立、重新配置和啟動的相關資訊可在“工作管理”區域檢視。

   b. 檢視可執行檔清單。

## 配置應用程式的允許清單模式

設定允許清單模式時，建議執行以下操作：

1. 建立包含必須允許啟動的應用程式的應用程式類別。

   您可以選擇以下用於建立應用程式類別的方法之一：

   - **包含手動新增內容的類別**。您可以透過使用以下條件手動新增到此類別：
     - 檔案中繼資料。卡巴斯基安全管理中心會將所有附帶指定檔案內容的可執行檔新增到此應用程式類別。
     - 檔案雜湊碼。卡巴斯基安全管理中心會將所有具有指定雜湊值的可執行檔新增到此應用程式類別。

       使用此條件將排除自動安裝更新的功能，因為不同版本的檔案雜湊值也不同。

     - 檔案憑證。卡巴斯基安全管理中心會將所有具有指定憑證簽章的可執行檔新增到此應用程式類別。
     - KL 類別。卡巴斯基安全管理中心會將所有屬於指定 KL 類別的應用程式新增到此應用程式類別。
     - 應用程式資料夾。卡巴斯基安全管理中心會將此資料夾中的所有可執行檔新增到該應用程式類別。

       使用“**應用程式資料夾**”條件可能不安全，因為指定資料夾中的任何應用程式都將被允許啟動。建議只將使用具有“ **應用程式資料夾**”條件的應用程式類別的規則套用於那些必須允許為其自動安裝更新的使用者。

   - **包括特定資料夾中的可執行檔的類別**。您可以指定將自動分配到已建立的應用程式類別的可執行檔所來自的資料夾。

- **包含選定裝置的可執行檔的類別**。您可以指定其所有可執行檔都將自動分配到已建立的應用程式類別的電腦。

  使用這種方法建立應用程式類別時，卡巴斯基安全管理中心從**可執行檔**資料夾接收電腦上的應用程式的相關資訊。

2. 為"應用程式控制"元件選擇允許清單模式。

3. 使用已建立的應用程式類別建立應用程式控制規則。

   最初為"允許清單"模式定義了"**黃金映像**"規則和"**信任的更新程式**"規則。這些應用程式控制規則對應於 KL 類別。"黃金映像"KL 類別包含確保作業系統正常執行的程式。"信任的更新程式"KL類別包含最具信譽的軟體廠商的更新程式。您無法刪除這些規則。這些規則的設定無法編輯。預設情況下，啟用"**黃金映像**"規則，停用"**信任的更新程式**"規則。所有使用者允許啟動比對這些規則的觸發條件的應用程式。

4. 確定必須允許為其自動安裝更新的應用程式。

   您可以透過以下任意一種方式允許自動安裝更新：

   - 透過允許屬於任何 KL 類別的所有應用程式啟動來指定允許的應用程式的延伸清單。
   - 透過允許有憑證簽章的所有應用程式啟動來指定允許的應用程式的延伸清單。

     要允許有憑證簽章的所有應用程式啟動，您可以建立一個包含基於憑證的條件的類別，此條件只使用值為"*.*"的"**主旨**"參數。

   - 對於應用程式控制規則，選擇"**信任的更新程式**"參數。如果選中此核取方塊，Kaspersky Endpoint Security 會將規則中包含的應用程式視為信任更新程式。Kaspersky Endpoint Security 允許啟動已由規則中包含的應用程式安裝或更新的應用程式，條件是不會對這些應用程式套用封鎖規則。

     在轉移 Kaspersky Endpoint Security 設定時，也會轉移信任更新程式建立的可執行檔清單。

   - 建立一個資料夾，並在其中放置想要允許自動安裝更新的應用程式的可執行檔。然後使用"**應用程式資料夾**"條件建立應用程式類別，並指定該資料夾的路徑。隨後建立一個允許規則並選取此類型。

     使用"**應用程式資料夾**"條件可能不安全，因為指定資料夾中的任何應用程式都將被允許啟動。建議只將使用具有" **應用程式資料夾**"條件的應用程式類別的規則套用於那些必須允許為其自動安裝更新的使用者。

## 測試允許清單模式

要確保應用程式控制規則不會封鎖工作所需的應用程式，建議啟用應用程式控制規則的測試並在建立新規則後分析其執行。啟用測試模式後，Kaspersky Endpoint Security 不會封鎖被應用程式控制規則封鎖啟動的應用程式，但是會將有關它們啟動的通知傳送給管理伺服器。

測試允許清單模式時，建議執行以下操作：

1. 確定測試週期（從幾天到兩個月）。

2. 啟用應用程式控制規則的測試。

3. 檢查"應用程式控制"的執行測試所產生的事件和有關測試模式下封鎖的應用程式的報告來分析測試結果。

4. 根據分析結果，變更允許清單模式設定。

   特別是，根據測試結果，您可以將與事件相關的可執行檔新增到應用程式類別。

## 支援允許清單模式

為"應用程式控制"選擇封鎖操作後，建議執行以下操作以繼續支援允許清單模式：

- 檢查"應用程式控制"的執行所產生的事件和被封鎖執行的報告來分析"應用程式控制"的效果。
- 分析使用者的應用程式存取請求。
- 透過檢查其在卡巴斯基安全網路中的的信譽來分析不熟悉的可執行檔。
- 在安裝作業系統或軟體的更新前，請在電腦測試群組中安裝這些更新，以檢查應用程式控制規則將如何處理它們。
- 將必要的應用程式新增到應用程式控制規則中使用的類別。

# 網路連接埠監控

在 Kaspersky Endpoint Security 運行期間， Web 控制、郵件威脅防護、Web 威脅防護、行為偵測和 弱點利用防禦 元件將監控透過特定協定傳輸並經過使用者電腦上開放的特定 TCP 和 UDP 連接埠的資料流程。例如，"郵件威脅防護"元件分析透過 SMTP 傳輸的資訊，而"Web 威脅防護"元件分析透過 HTTP 和 FTP 傳輸的資訊。

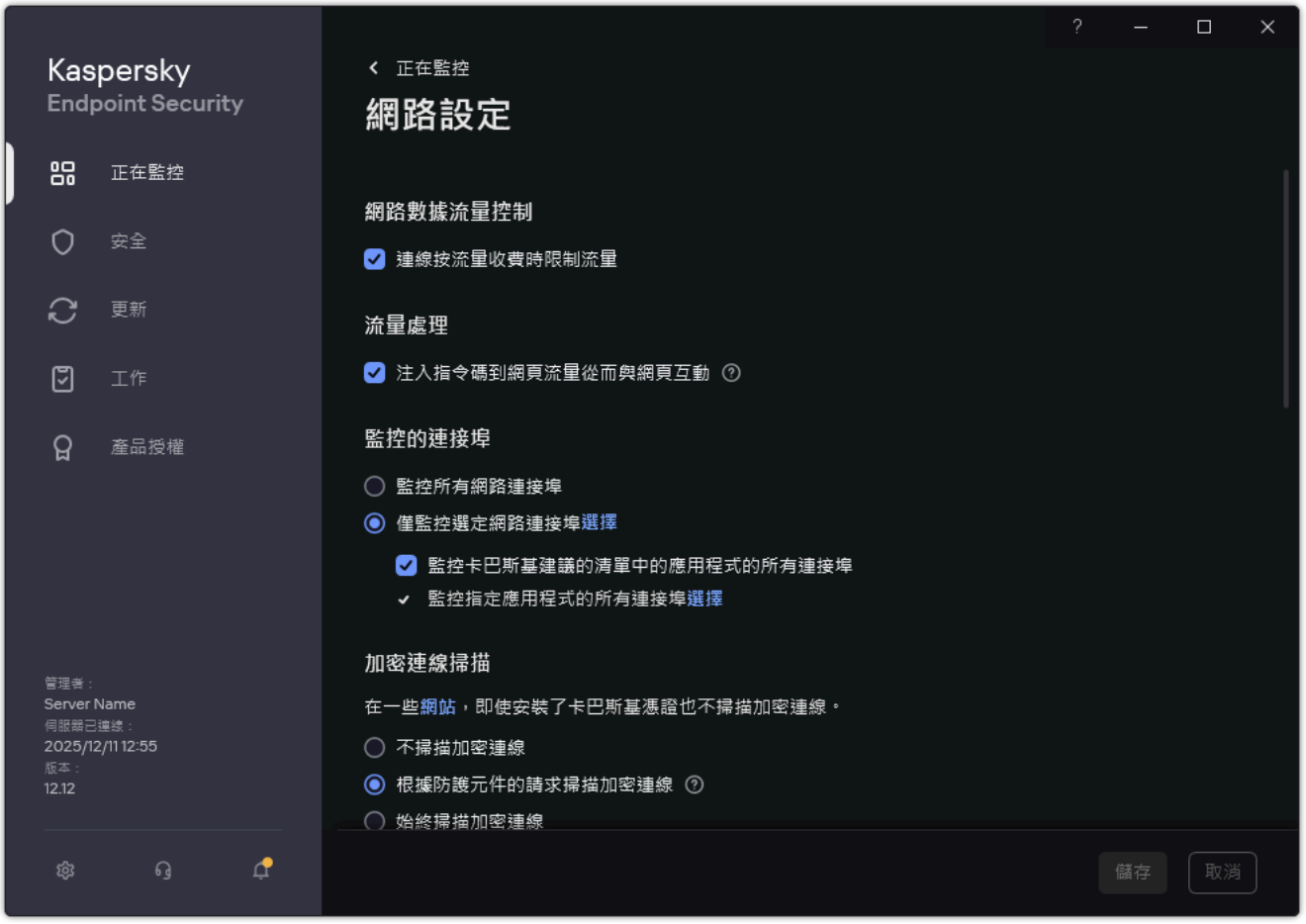
Kaspersky Endpoint Security 將使用者電腦的 TCP 和 UDP 通訊埠根據其組成方式分成多個群組。某些網路連接埠保留用於易受攻擊的服務。建議您更全面地監控這些連接埠，因為它們更有可能成為網路攻擊的目的。如果使用非標準網路連接埠的非標準服務，這些網路連接埠也可能成為攻擊電腦的目標。您可以指定網路連接埠清單和請求網路存取的應用程式清單。這樣在網路流量監控期間，這些連接埠和應用程式會受到"郵件威脅防護"和"Web 威脅防護"元件的特別關注。

為了確保電腦的安全， 行為偵測 和 弱點利用防禦 元件還監控通過網路連接埠的資料流。這些元件會持續監控網路流量，以發現可能造成威脅的單個處理程序。

# 啟動對所有網路連接埠的監控

*若要啟用對所有網路連接埠的監控，請執行以下操作：*

1. 在“應用程式主視窗”中，點擊⚙按鈕。
2. 在應用程式設定視窗中，選取”**一般設定**“→“**網路設定**”。




網路連接埠監控設定

3. 在“**監控的連接埠**”塊中，選取“**監控所有網路連接埠**”。
4. 儲存變更。

# 建立受監控網路連接埠的清單

*建立受監控的網路連接埠清單*

1. 在“應用程式主視窗”中，點擊⚙按鈕。
2. 在應用程式設定視窗中，選取”**一般設定**“→“**網路設定**”。
3. 在“**監控的連接埠**”塊中，選取“**僅監控選定網路連接埠**”。

4. 點擊**"選擇"**。

   這將顯示一個常用於傳送電子郵件和網路流量的網路連接埠清單。該網路連接埠清單包含在 Kaspersky Endpoint Security 安裝套件中。

5. 使用**"狀態"**列中的開關來啟用或停用網路連接埠監控。

6. 如果某網路連接埠未在網路連接埠清單中，請按照以下步驟新增：

   a. 點擊**"新增"**。

   b. 在開啟的視窗中，輸入網路連接埠編號和簡要說明。

   c. 設定網路連接埠監控的**"啟動"**或**"未啟動"**狀態。

7. 儲存變更。

若是 FTP 協定執行被動模式，透過隨機建立的網路連接埠，不會被新增到監控連接埠清單中。為了防護此類連線，請"啟用對所有網路連接埠的監控"或"為建立 FTP 連線的應用程式配置網路連接埠控制"。

# 建立所有網路連接埠受監控的應用程式清單

您可以使用 Kaspersky Endpoint Security 建立監控全部的連接埠的應用程式清單。

建議您在 Kaspersky Endpoint Security 建立監控全部的連接埠的應用程式清單中包含 FTP 協定接收或傳送資料的應用程式。

*若要建立所有網路連接埠受監控的應用程式清單，請執行以下操作：*

1. 在"應用程式主視窗"中，點擊⚙ 按鈕。

2. 在應用程式設定視窗中，選取**"一般設定"→"網路設定"**。

3. 在**"監控的連接埠"**塊中，選取**"僅監控選定網路連接埠"**。

4. 選擇**"監控卡巴斯基建議的清單中的應用程式的所有連接埠"**核取方塊。

   若選中此核取方塊，則 Kaspersky Endpoint Security 將監控以下應用程式的所有連接埠：

   - Adobe Acrobat Reader。
   - Apple Application Support。
   - Google Chrome。
   - Microsoft Edge。
   - Mozilla Firefox。
   - Internet Explorer。
   - Java。

- mIRC。
- Opera。
- Pidgin。
- Safari。
- Mail.ru Agent。
- Yandex Browser。

5. 選擇"**監控指定應用程式的所有連接埠**"核取方塊。
6. 點擊"**選擇**"。
   這將開啟一個 Kaspersky Endpoint Security 監控其網路連接埠的應用程式清單。
7. 使用"**狀態**"列中的開關來啟用或停用網路連接埠監控。
8. 如果清單中未包含某應用程式，請按照以下步驟新增：
   a. 點擊"**新增**"。
   b. 在開啟的視窗中，輸入應用程式的可執行檔的路徑和簡要說明。
   c. 設定網路連接埠監控的"**啟動**"或"**未啟動**"狀態。
9. 儲存變更。

# 匯出和匯入受監控的連接埠的清單

Kaspersky Endpoint Security 使用以下清單來監控網路連接埠：網路連接埠清單和由 Kaspersky Endpoint Security 監控其連接埠的應用程式清單。您可以將受監控連接埠的清單匯出到 XML 檔案。然後，您可以修改檔案，例如，新增大量具有相同描述的連接埠。您還可以使用匯出/匯入功能來備份受監控連接埠的清單，或將清單遷移到其他伺服器。

**如何在管理主控台（MMC）中匯出和匯入受監控連接埠的清單**

1. 在網頁主控台的主視窗中，選擇**資產（裝置）→政策和設定檔**。
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. 要匯出網路連接埠清單：

   a. 在**"監控的連接埠"**塊中，選取**"僅監控選定網路連接埠"**。

   b. 點擊**"選定 N 連接埠"**連接。

   開啟**"網路連接埠"**視窗。**網路連接埠** 視窗中將顯示一個常用於傳送電子郵件和網路流量的網路連接埠清單。該網路連接埠清單包含在 Kaspersky Endpoint Security 安裝套件中。

   c. 在网路連接埠清單中，選擇要匯出的連接埠。

   d. 點擊**"匯出"**。

   e. 在開啟的視窗中，輸入您要將網路連接埠清單匯出到的 XML 檔案的名稱，然後選取要儲存此檔案的資料夾。

   f. 儲存檔案。

   Kaspersky Endpoint Security 會將整個網路連接埠清單匯出到 XML 檔案。

6. 要匯出其連接埠受 Kaspersky Endpoint Security 監控的應用程式清單，請執行以下操作：

   a. 在**"監控的連接埠"**塊中，選中**"監控指定應用程式的所有連接埠"**核取方塊。

   b. 點擊**"選定 N 應用程式"**連接。

   c. 在應用程式清單中，選擇要匯出的應用程式。

   d. 點擊**"匯出"**。

   e. 在開啟的視窗中，指定您要將應用程式清單匯出到的 XML 檔案的名稱，然後選取要儲存此檔案的資料夾。

   f. 儲存檔案。

   Kaspersky Endpoint Security 會將整個應用程式清單匯出到 XML 檔案。

7. 要匯入網路連接埠清單：

   a. 在網路連接埠清單中，點擊**"匯入"**按鈕。

   在開啟的視窗中，選取要從中匯入網路連接埠清單的 XML 檔案。

   b. 開啟檔案。

   如果電腦已經具有網路連接埠清單，則 Kaspersky Endpoint Security 將提示您刪除現有清單或從 XML 檔案向其中新增新項目。

8. 要匯入其連接埠受 Kaspersky Endpoint Security 監控的應用程式清單，請執行以下操作：

   a. 在應用程式清單中，點擊**"匯入"**按鈕。

   在開啟的視窗中，選取要從中匯入應用程式清單的 XML 檔案。

   b. 開啟檔案。

   如果電腦已經具有應用程式清單，則 Kaspersky Endpoint Security 將提示您刪除現有清單或從 XML 檔案向其中新增新項目。

9. 儲存變更。

1. 在卡巴斯基安全管理中心管理主控台樹狀目錄中，選取**政策**。

2. 選擇必要的政策並點擊以開啟政策內容。

3. 在政策視窗中，選擇**"一般設定 → 網路設定"**。

4. 在**"監控的連接埠"**塊中，選取**"僅監控選定網路連接埠"**。

5. 點擊**"設定"**。

   開啟**"網路連接埠"**視窗。**網路連接埠** 視窗中將顯示一個常用於傳送電子郵件和網路流量的網路連接埠清單。該網路連接埠清單包含在 Kaspersky Endpoint Security 安裝套件中。

6. 要匯出網路連接埠清單：

   a. 在网路連接埠清單中，選擇要匯出的連接埠。要選擇多個連接埠，請使用**CTRL**或**SHIFT**鍵。

      如果未選擇任何連接埠，則 Kaspersky Endpoint Security 將匯出所有連接埠。

   b. 點擊**"匯出"**。

   c. 在開啟的視窗中，輸入您要將網路連接埠清單匯出到的 XML 檔案的名稱，然後選取要儲存此檔案的資料夾。

   d. 儲存檔案。

      Kaspersky Endpoint Security 會將整個網路連接埠清單匯出到 XML 檔案。

7. 要匯出其連接埠受 Kaspersky Endpoint Security 監控的應用程式清單，請執行以下操作：

   a. 選擇**"監控指定應用程式的所有連接埠"**核取方塊。

   b. 在應用程式清單中，選擇要匯出的應用程式。要選擇多個連接埠，請使用**CTRL**或**SHIFT**鍵。

      如果您沒有選擇任何應用程式，Kaspersky Endpoint Security 將匯出所有應用程式。

   c. 點擊**"匯出"**。

   d. 在開啟的視窗中，指定您要將應用程式清單匯出到的 XML 檔案的名稱，然後選取要儲存此檔案的資料夾。

   e. 儲存檔案。

      Kaspersky Endpoint Security 會將整個應用程式清單匯出到 XML 檔案。

8. 要匯入網路連接埠清單：

   a. 在網路連接埠清單中，點擊**"匯入"**按鈕。

      在開啟的視窗中，選取要從中匯入網路連接埠清單的 XML 檔案。

   b. 開啟檔案。

      如果電腦已經具有網路連接埠清單，則 Kaspersky Endpoint Security 將提示您刪除現有清單或從 XML 檔案向其中新增新項目。

9. 要匯入其連接埠受 Kaspersky Endpoint Security 監控的應用程式清單，請執行以下操作：

   a. 在應用程式清單中，點擊**"匯入"**按鈕。

      在開啟的視窗中，選取要從中匯入應用程式清單的 XML 檔案。

b. 開啟檔案。

如果電腦已經具有應用程式清單，則 Kaspersky Endpoint Security 將提示您刪除現有清單或從 XML 檔案向其中新增新項目。

10. 儲存變更。

# 記錄檢查

如果 Kaspersky Endpoint Security 安裝在執行 Windows for Servers 的電腦上，則該元件可用。如果 Kaspersky Endpoint Security 安裝在執行 Windows for Workstations 的電腦上，則該元件不可用。

從 11.11.0 版本開始，Kaspersky Endpoint Security for Windows 包括記錄檢查元件。記錄檢查會基於 Windows 事件記錄分析監控受防護環境的完整性。如果應用程式在系統中偵測到有非典型行為的跡象，它會通知管理員，因為該行為可能表明有人嘗試網路攻擊。

Kaspersky Endpoint Security 根據規則分析 Windows 事件記錄和偵測違規。元件包括預定義規則。預定義規則由啟發式分析提供支援。您也可以新增您自己的規則（自訂規則）。當規則觸發時，應用程式會建立一個狀態為“*緊急*”的事件（請見下圖）。

如果您想要使用記錄檢查，請確保稽核政策安全設定已配置且系統正在記錄相關事件（詳情請見 Microsoft 技術支援網站）。




記錄檢查通知

# 配置預定義規則

預定義規則包括受防護電腦上異常活動的範本。異常活動可能表明有人嘗試攻擊。預定義規則由啟發式分析提供支援。記錄檢查有七項預定義規則可用。您可以啟用或停用任何這些規則。預定義規則無法被刪除。

您可以為以下操作配置監控事件的規則觸發條件：

- 密碼暴力破解偵測
- 網路登入偵測

### 如何在管理主控台 (MMC) 中配置預定義規則

1. 在卡巴斯基安全管理中心管理主控台樹狀目錄中，選取**政策**。
2. 選擇必要的政策並點擊以開啟政策內容。
3. 在政策視窗中，選擇**"安全控制 → 記錄審查"**。
4. 請確保選中**記錄審查**核取方塊。
5. 在**"預定義規則"**塊中，點擊**"設定"**按鈕。
6. 選擇或清除核取方塊以配置預定義規則：
   - **系統中存在疑似暴力破解攻擊模式**
   - **網路登入工作階段中偵測到一個非典型活動**
   - **存在可能的 Windows 事件記錄濫用模式**
   - **代替安裝的新服務偵測到了非典型操作**
   - **偵測到使用明顯憑據的非典型登入名稱**
   - **系統中存在疑似 Kerberos 偽造 PAC (MS14-068) 攻擊模式**
   - **在有權限的內建管理員群組中偵測到可疑變更**
7. 必要的話配置**系統中存在疑似暴力破解攻擊模式**規則：
   a. 點擊規則下的**"設定"**按鈕。
   b. 在開啟的視窗中，指定嘗試次數和在此期間必須執行密碼輸入嘗試以觸發規則的時間段。
   c. 點擊**"確定"**。
8. 如果選定**網路登入工作階段中偵測到一個非典型活動**規則，您需要配置其設定：
   a. 點擊規則下的**"設定"**按鈕。
   b. 在**網路登入偵測**塊中，指定時間間隔的開始和結束時間。
      Kaspersky Endpoint Security 將在定義的間隔期間執行的登入嘗試視為異常活動。
      預設情況下不設定間隔期間，應用程式不監控登入嘗試。若要應用程式持續監控登入嘗試，請將間隔期間設為 12:00 AM - 11:59 PM。間隔期間的開始和結束不得重合。如果它們一樣，應用程式將不監控登入嘗試。
   c. 建立一個受信任使用者和受信任 IP 位址（IPv4 和 IPv6）清單。
      您可以在 Active Directory 中、在卡巴斯基安全管理中心的账户清單中或透過手動輸入本機使用者名稱來選擇使用者。卡巴斯基建議僅在無法使用網域使用者帳戶的特殊情況下使用本機使用者帳戶。Kaspersky Endpoint Security 不監控這些使用者和電腦的登入嘗試。
   d. 點擊**"確定"**。
9. 儲存變更。

**如何在網頁主控台和雲端主控台中配置預定義規則**

1. 在網頁主控台的主視窗中，選擇**資產（裝置）→政策和設定檔**。
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**"→"**記錄審查**"。
5. 請確保**記錄審查已啟用**開關已開啟。
6. 在**預定義規則**塊中，使用開關啟用或停用預定義規則：
   - **系統中存在疑似暴力破解攻擊模式**
   - **網路登入工作階段中偵測到一個非典型活動**
   - **存在可能的 Windows 事件記錄濫用模式**
   - **代替安裝的新服務偵測到了非典型操作**
   - **偵測到使用明顯憑據的非典型登入名稱**
   - **系統中存在疑似 Kerberos 偽造 PAC (MS14-068) 攻擊模式**
   a. **在有權限的內建管理員群組中偵測到可疑變更**
7. 必要的話配置**系統中存在疑似暴力破解攻擊模式**規則：
   a. 點擊規則下的**設定**。
   b. 在開啟的視窗中，指定嘗試次數和在此期間必須執行密碼輸入嘗試以觸發規則的時間段。
   c. 點擊"**確定**"。
8. 如果選定**網路登入工作階段中偵測到一個非典型活動**規則，您需要配置其設定：
   a. 點擊規則下的**設定**。
   b. 在**網路登入偵測**塊中，指定時間間隔的開始和結束時間。
      Kaspersky Endpoint Security 將在定義的間隔期間執行的登入嘗試視為異常活動。
      預設情況下不設定間隔期間，應用程式不監控登入嘗試。若要應用程式持續監控登入嘗試，請將間隔期間設為 12:00 AM - 11:59 PM。間隔期間的開始和結束不得重合。如果它們一樣，應用程式將不監控登入嘗試。
   c. 在**排除項目**塊中，新增受信任使用者和受信任 IP 位址（IPv4 和 IPv6）。
      您可以在 Active Directory 中、在卡巴斯基安全管理中心的账户清單中或透過手動輸入本機使用者名稱來選擇使用者。卡巴斯基建議僅在無法使用網域使用者帳戶的特殊情況下使用本機使用者帳戶。Kaspersky Endpoint Security 不監控這些使用者和電腦的登入嘗試。
   d. 點擊"**確定**"。
9. 儲存變更。

**如何在應用程式介面中配置預定義規則**

1. 在"應用程式主視窗"中，點擊 按鈕。
2. 在應用程式設定視窗中，選取"**安全控制**"→"**記錄審查**"。
3. 請確保**記錄審查**開關已開啟。
4. 在"**預定義規則**"塊中，點擊"**配置**"按鈕。
5. 選擇或清除核取方塊以配置預定義規則：
   - **系統中存在疑似暴力破解攻擊模式**
   - **網路登入工作階段中偵測到一個非典型活動**
   - **存在可能的 Windows 事件記錄濫用模式**
   - **代替安裝的新服務偵測到了非典型操作**
   - **偵測到使用明顯憑據的非典型登入名稱**
   - **系統中存在疑似 Kerberos 偽造 PAC (MS14-068) 攻擊模式**
   a. **在有權限的內建管理員群組中偵測到可疑變更**
6. 必要的話配置**系統中存在疑似暴力破解攻擊模式**規則：
   a. 點擊規則下的**設定**。
   b. 在開啟的視窗中，指定嘗試次數和在此期間必須執行密碼輸入嘗試以觸發規則的時間段。
7. 如果選定**網路登入工作階段中偵測到一個非典型活動**規則，您需要配置其設定：
   a. 點擊規則下的**設定**。
   b. 在**網路登入偵測**塊中，指定時間間隔的開始和結束時間。
      Kaspersky Endpoint Security 將在定義的間隔期間執行的登入嘗試視為異常活動。
      預設情況下不設定間隔期間，應用程式不監控登入嘗試。若要應用程式持續監控登入嘗試，請將間隔期間設為 12:00 AM - 11:59 PM。間隔期間的開始和結束不得重合。如果它們一樣，應用程式將不監控登入嘗試。
   c. 在**排除項目**塊中，新增受信任使用者和受信任 IP 位址（IPv4 和 IPv6）。
      您可以在 Active Directory 中、在卡巴斯基安全管理中心的账户清單中或透過手動輸入本機使用者名稱來選擇使用者。卡巴斯基建議僅在無法使用網域使用者帳戶的特殊情況下使用本機使用者帳戶。Kaspersky Endpoint Security 不監控這些使用者和電腦的登入嘗試。
8. 儲存變更。

結果，當規則觸發時，Kaspersky Endpoint Security 將建立"*緊急事件*"事件。

# 新增自訂規則

您可以設定自己的記錄檢查規則觸發條件。為此，您必須輸入一個事件 ID 並選擇一個事件來源。您可以在 Microsoft 技術支援網站 上查找事件 ID。您可以從標準記錄中選擇一個事件來源：*Application*、*Security*或 *System*。您也可以指定協力廠商應用程式的記錄。您可以使用"事件檢視程式"工具查找協力廠商應用程式記錄的名稱。協力廠商應用程式記錄保留在"應用程式和服務記錄"資料夾（例如，*Windows PowerShell* 記錄）中。

應用程式不檢查指定記錄是否真的存在於 Windows 事件記錄中。如果記錄名稱中有錯誤，則應用程式不監控該記錄的事件。

自訂規則清單已包括卡巴斯基專家建立的三個規則。

**如何在管理主控台 (MMC) 中新增自訂規則**

1. 在卡巴斯基安全管理中心管理主控台樹狀目錄中，選取**政策**。
2. 選擇必要的政策並點擊以開啟政策內容。
3. 在政策視窗中，選擇"**安全控制 → 記錄審查**"。
4. 請確保選中**記錄審查**核取方塊。
5. 在"**自訂規則**"塊中，點擊"**設定**"按鈕。
6. 在開啟的視窗中，選中您想要啟用的自訂規則旁邊的核取方塊。
7. 必要的話點擊**新增**建立您自己的自訂規則。
8. 這會開啟一個視窗；在該視窗中，配置自訂規則：
   - **規則名稱**
   - **記錄名稱**Windows 事件記錄。以下記錄可以使用： *Application*、*Security*、*System*。
   - **來源**協力廠商應用程式記錄。您可以使用"事件檢視程式"工具查找協力廠商應用程式記錄的名稱。協力廠商應用程式記錄保留在"應用程式和服務記錄"資料夾（例如，*Windows PowerShell* 記錄）中。
   - **事件識別符**Windows 事件記錄中的事件 ID。您可以在 Microsoft 技術文件 中查找事件 ID。
9. 儲存變更。

**如何在網頁主控台和雲端主控台中新增自訂規則**

1. 在網頁主控台的主視窗中，選擇**資產（裝置）→ 政策和設定檔**。
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**"→"**記錄審查**"。

5. 請確保**記錄審查已啟用**開關已開啟。

6. 在"**自訂規則**"塊中，選擇要啟用的自訂規則。

7. 必要的話點擊**新增**建立您自己的自訂規則。

8. 這會開啟一個視窗；在該視窗中，配置自訂規則：

   - **規則名稱**
   - **自訂記錄名稱**Windows 事件記錄。以下記錄可以使用： *Application*、*Security*、*System*。
   - **起源**協力廠商應用程式記錄。您可以使用"事件檢視程式"工具查找協力廠商應用程式記錄的名稱。協力廠商應用程式記錄保留在"應用程式和服務記錄"資料夾（例如，*Windows PowerShell* 記錄）中。
   - **事件識別符**Windows 事件記錄中的事件 ID。您可以在 Microsoft 技術文件 中查找事件 ID。

9. 儲存變更。

**如何在應用程式介面中新增自訂規則**

1. 在"應用程式主視窗"中，點擊 按鈕。

2. 在應用程式設定視窗中，選取"**安全控制**"→"**記錄審查**"。

3. 請確保**記錄審查**開關已開啟。

4. 在"**自訂規則**"塊中，點擊"**配置**"按鈕。

5. 在開啟的視窗中，選中您想要啟用的自訂規則旁邊的核取方塊。

6. 必要的話點擊**新增**建立您自己的自訂規則。

7. 這會開啟一個視窗；在該視窗中，配置自訂規則：

   - **規則名稱**
   - **記錄名稱**Windows 事件記錄。以下記錄可以使用： *Application*、*Security*、*System*。
   - **來源**協力廠商應用程式記錄。您可以使用"事件檢視程式"工具查找協力廠商應用程式記錄的名稱。協力廠商應用程式記錄保留在"應用程式和服務記錄"資料夾（例如，*Windows PowerShell* 記錄）中。
   - **事件識別符**Windows 事件記錄中的事件 ID。您可以在 Microsoft 技術文件 中查找事件 ID。

8. 儲存變更。

結果，當規則觸發時，Kaspersky Endpoint Security 將建立"*緊急*"事件。

# 系統完整性監控

如果 Kaspersky Endpoint Security 安裝在執行 Windows for Servers 的電腦上，則該元件可用。如果 Kaspersky Endpoint Security 安裝在執行 Windows for Workstations 的電腦上，則該元件不可用。

從版本 12.6 開始，Kaspersky Endpoint Security for Windows 包含系統完整性監控元件，而不是檔案完整性監控元件。系統完整性監控元件包括檔案完整性監控的所有功能，此外還允許監控登錄機碼變更和外部裝置的連線。

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示。系統完整性監控可以即時模式運行，也可以按需執行系統完整性檢查。

### 即時系統完整性監控

在即時模式下，系統完整性監控追蹤您包含在元件範圍（*監控範圍*）中的物件的變更。系統完整性監控還可以即時封鎖對此類物件的未經授權的存取。

### 按需系統完整性檢查

按需系統完整性檢查是一項可以手動或按排程執行的工作。若要執行*系統完整性檢查*工作，您必須配置元件的範圍（*監控範圍*）並建立基線。*基線*是系統中物件的記錄狀態，應用程式在與目前狀態進行比較時將其用作參考。

### 遷移檔案完整性監控設定

當您將 Kaspersky Endpoint Security 更新至版本 12.6 時，檔案完整性監視器設定會得到自動遷移。作為遷移的一部分，應用程式將監控規則移至系統完整性監控。當從 KSWS 遷移到 KES時，檔案完整性監控規則也會被遷移到系統完整性監控。

為確保系統完整性監控正確運行，Kaspersky Endpoint Security 應用程式和管理外掛程式都應被更新至版本 12.6。如果您安裝了早期版本的管理外掛程式，則無法設定係統完整性監控，因為管理外掛程式缺少 **系統完整性監控** 部分。

## 關於系統完整性監控規則

為了使系統完整性監控正常運作，您必須新增至少一個規則。*系統完整性監控規則*是定義使用者對檔案和登錄檔的存取權限的一組標準。系統完整性監控可偵測指定*監控範圍*內檔案和登錄檔的變更。監控範圍是系統完整性監控規則的標準之一。

系統完整性監控允許監控以下物件：

- 檔案
- 登錄檔
- 外部裝置

### 檔案監控涉及的特殊注意事項

系統完整性監控監控檔案和資料夾的變更以及被新增至監控範圍或從監控範圍中刪除的檔案。這些變更可能表明有電腦安全入侵。我們建議新增很少修改的物件或者只有管理員有權存取的物件。這有助於減少系統完整性監控事件數量。

系統完整性監控不會監控伺服器共用資料夾中檔案的變更。系統完整性監控只能在本機使用。

Kaspersky Endpoint Security 僅監控即時系統完整性監控開始運行時連線的磁碟上的檔案和資料夾的變更。如果即時系統完整性監控開始運行時未連線磁碟，則即使檔案和資料夾已新增至監控範圍，應用程式也不會監控該磁碟上的檔案和資料夾的變更。

### 登錄檔監控涉及的特殊注意事項

系統完整性監控監控登錄檔。這些變更可能表明有電腦安全入侵。

系統完整性監控監控登錄的以下根鍵：

- HKCR
- HKLM
- HKU
- HKCC
- HKEY_CLASSES_ROOT
- HKEY_LOCAL_MACHINE
- HKEY_USERS
- HKEY_CURRENT_CONFIG（僅在即時系統完整性監控中可用）
- HKEY_CURRENT_USER（僅在即時系統完整性監控中可用）

*系統完整性檢查*工作不支援 HKEY_CURRENT_USER 金鑰。您可以在下面指定 HKEY_USERS 下面的一個鍵作為 HKEY_USERS\<user profile ID>\<key>。

### 外部裝置監控涉及的特殊注意事項

系統完整性監控監控外部裝置的連線和斷開連線。為了防護電腦免受因與此類裝置交換檔案而導致的安全威脅，這樣很有必要。系統完整性監控不會監控對外部裝置的存取，也不會封鎖檔案交換。您可以使用不同的應用程式元件裝置控制配置對裝置的存取。

> 執行*基線系統完整性監控*工作時，如果外部裝置在作業系統中具有相同的磁碟機字母，應用程式將忽略其重新連線。若要進行記錄，重新連線的裝置必須具有不同的磁碟機字母。

系統完整性監控監控以下類型外部裝置的連線：

- 卸除式磁碟機（包括 USB 快閃磁碟機）。
- 硬碟磁碟機。
- 外接式網路卡。
- CD/DVD/藍光磁碟機。
- 掃描器/攝影機。

## 即時系統完整性監控

系統完整性監控允許即時追蹤作業系統中的變化。您可以追蹤可能表明電腦上存在安全漏洞的變更。此元件可封鎖這些變更或僅記錄變更事件。

為了使系統完整性監控正常運作，您必須新增至少一個規則。*系統完整性監控規則*是定義使用者對檔案和登錄檔的存取權限的一組標準。系統完整性監控可偵測指定*監控範圍*內檔案和登錄檔的變更。監控範圍是系統完整性監控規則的標準之一。

### 即時系統完整性監控模式

為了確保系統完整性監控規則不會封鎖對作業系統或其他服務的運作至關重要的資源的任何操作，我們建議啟用測試模式並分析元件如何影響系統。開啟測試模式後，Kaspersky Endpoint Security 不會封鎖規則禁止的使用者活動，而是產生 *警告* ⚠ 事件。

即時系統完整性監控元件有兩種模式：

- 封鎖。

  在此模式下，系統完整性監控追蹤系統中的變化並根據規則執行操作： **允許** 或者 **封鎖**。系統完整性監控也會產生對應的事件並變更在卡巴斯基安全管理中心主控台中的裝置狀態。

- 通知。

  在此模式下，系統完整性監控允許對監控範圍內的檔案和登錄機碼進行操作。如果禁止對檔案或登錄檔進行操作，則應用程式會產生一個事件：*測試模式中允許被禁止的操作*。要分析規則如何影響系統，您可以查看報告。

啟用即時系統完整性監控

**如何在管理主控台 (MMC) 中啟用即時系統完整性監控**

1. 在卡巴斯基安全管理中心管理主控台樹狀目錄中，選取**政策**。
2. 選擇必要的政策並點擊以開啟政策內容。
3. 在政策視窗中，選擇"**安全控制 → 系統完整性監控**"。
4. 選擇"**系統完整性監控**"核取方塊。
5. 在**用於封鎖規則的操作模式**下面，選擇即時系統完整性監控模式：
   - **封鎖**在此模式下，系統完整性監控會封鎖監控範圍內的檔案和登錄機碼的操作，並產生對應的事件。
   - **通知**在此模式下，系統完整性監控允許對監控範圍內的檔案和登錄機碼進行操作，並產生相應的事件。
6. 在"**即時系統完整性監控**"塊中，選中"**即時系統完整性監控**"核取方塊。
7. 配置外部裝置監控：
   a. 選擇"**監控裝置**"核取方塊。
   b. 在**事件嚴重性級別**下拉式清單中，選擇外部裝置監控事件的重要性等級：*資訊*, *警告*, *緊急*。

   系統完整性監控記錄外部裝置的目前連線情況。在應用程式設定中啟用該元件後，應用程式開始監控外部裝置的連線和中斷連線。隨後，當外部裝置連線或斷開連線時，應用程式會產生相應的事件。
8. 配置檔案和登錄檔監控：
   a. 選擇"**監控檔案和登錄檔**"核取方塊。
   b. 點擊"**設定**"。
   這將開啟系統完整性監控規則清單。
   c. 點擊"**新增**"。
   您也可以 **從其他來源匯入規則**。

   您可以將系統完整性監控規則清單匯出到 XML 檔案。然後，您可以修改檔案，例如，新增大量相同類型的記錄。您可以使用匯出/匯入功能來備份系統完整性監控規則清單，或將清單遷移到其他伺服器。

   > 系統完整性監控不支援為*系統完整性檢查*工作匯入 HKEY_CURRENT_USER 和 HKEY_CURRENT_CONFIG 金鑰。如果工作的監控範圍包含這些金鑰，應用程式會產生*監控範圍包括不正確的物件*事件。

   **如何在管理主控台 (MMC) 中匯出和匯入系統完整性監控規則清單**

   1. 在卡巴斯基安全管理中心管理主控台樹狀目錄中，選取**政策**。
   2. 選擇必要的政策並點擊以開啟政策內容。

3. 在政策視窗中，選擇**"安全控制 → 系統完整性監控"**。

4. 要匯出或匯入 *即時系統完整性監控* 規則：

   a. 在**"即時系統完整性監控"**塊中，點擊**"設定"**按鈕。

   b. 若要匯出即時系統完整性監控規則清單：

      1. 選取您想要匯出的規則。要選擇多個連接埠，請使用**CTRL**或**SHIFT**鍵。

         如果您未選擇任何規則，則 Kaspersky Endpoint Security 將匯出所有規則。

      2. 點擊**"匯出"**連接。

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

      4. 儲存檔案。

         Kaspersky Endpoint Security 會將規則清單匯出到 XML 檔案。

   c. 若要匯入即時系統完整性監控規則清單：

      1. 點擊**"匯入"**連接。

         在開啟的視窗中，選取要從中匯入規則清單的 XML 檔案。

      2. 開啟檔案。

         如果電腦已經具有規則清單，則 Kaspersky Endpoint Security 將提示您刪除現有清單或從 XML 檔案向其中新增新項目。

5. 若要匯出或匯入 *系統完整性檢查* 規則：

   a. 在**"系統完整性檢查"**塊中，選取**"自訂設定"**。

   b. 點擊**"設定"**。

   c. 若要匯出系統完整性檢查規則清單：

      1. 選取您想要匯出的規則。要選擇多個連接埠，請使用**CTRL**或**SHIFT**鍵。

         如果您未選擇任何規則，則 Kaspersky Endpoint Security 將匯出所有規則。

      2. 點擊**"匯出"**連接。

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

      4. 儲存檔案。

   Kaspersky Endpoint Security 會將規則清單匯出到 XML 檔案。

d. 若要匯入系統完整性檢查規則清單：

1. 點擊**"匯入"**連接。

   在開啟的視窗中，選取要從中匯入規則清單的 XML 檔案。

2. 開啟檔案。

如果電腦已經具有規則清單，則 Kaspersky Endpoint Security 將提示您刪除現有清單或從 XML 檔案向其中新增新項目。

6. 儲存變更。

**如何在網頁主控台中匯出和匯入系統完整性監控規則清單**

1. 在網頁主控台的主視窗中，選擇**資產（裝置）→ 政策和設定檔**。
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. 選擇**"Windows"**標籤。
6. 要匯出或匯入 *即時系統完整性監控* 規則：

   a. 在**"即時系統完整性監控"**塊中，點擊**"規則"**連接。

   b. 若要匯出即時系統完整性監控規則清單：

      1. 選取您想要匯出的規則。
      2. 點擊 → **匯出** 按鈕。

         Kaspersky Endpoint Security 會將規則清單匯出到預設下載資料夾中的 JSON 檔案。

   c. 若要匯入即時系統完整性監控規則清單：

      1. 點擊 → **匯入** 按鈕。

         在開啟的視窗中，選取要從中匯入受信任網址清單的 JSON 檔案。

      2. 開啟檔案。

         如果電腦已經具有規則清單，則 Kaspersky Endpoint Security 將提示您刪除現有清單或從 JSON 檔案向其中新增新項目。
7. 若要匯出或匯入 *系統完整性檢查* 規則：

   a. 在**"按需系統完整性檢查"**塊中，選取**"自訂設定"**。

   b. 點擊**"規則"**連接。

c. 若要匯出系統完整性檢查規則清單：

1. 選取您想要匯出的規則。

2. 點擊 → **匯出** 按鈕。

   Kaspersky Endpoint Security 會將規則清單匯出到預設下載資料夾中的 JSON 檔案。

d. 若要匯入系統完整性檢查規則清單：

1. 點擊 → **匯入** 按鈕。

   在開啟的視窗中，選取要從中匯入受信任網址清單的 JSON 檔案。

2. 開啟檔案。

   如果電腦已經具有規則清單，則 Kaspersky Endpoint Security 將提示您刪除現有清單或從 JSON 檔案向其中新增新項目。

8. 儲存變更。

d. 設定系統完整性監控規則（請參閱下表）。

9. 儲存變更。

**如何在網頁主控台中啟用即時系統完整性監控**

1. 在網頁主控台的主視窗中，選擇**資產（裝置）→ 政策和設定檔**。

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. 開啟**"系統完整性監控已啟用"**開關。

6. 選擇**"Windows"**標籤。

7. 在**即時系統完整性監控**下面，選擇即時系統完整性監控模式：

   - **套用規則**在此模式下，系統完整性監控會封鎖監控範圍內的檔案和登錄機碼的操作，並產生對應的事件。
   - **測試規則（通知）**在此模式下，系統完整性監控允許對監控範圍內的檔案和登錄機碼進行操作，並產生相應的事件。

8. 配置檔案和登錄檔監控：

a. 選擇**"監控檔案和登錄檔"**核取方塊。

b. 點擊**"規則"**。

   這將開啟系統完整性監控規則清單。

c. 點擊**"新增"**。

   您也可以 **從其他來源匯入規則**。

您可以將系統完整性監控規則清單匯出到 XML 檔案。然後，您可以修改檔案，例如，新增大量相同類型的記錄。您可以使用匯出/匯入功能來備份系統完整性監控規則清單，或將清單遷移到其他伺服器。

系統完整性監控不支援為*系統完整性檢查*工作匯入 `HKEY_CURRENT_USER` 和 `HKEY_CURRENT_CONFIG` 金鑰。如果工作的監控範圍包含這些金鑰，應用程式會產生*監控範圍包括不正確的物件*事件。

**如何在管理主控台 (MMC) 中匯出和匯入系統完整性監控規則清單**

1. 在卡巴斯基安全管理中心管理主控台樹狀目錄中，選取**政策**。
2. 選擇必要的政策並點擊以開啟政策內容。
3. 在政策視窗中，選擇"**安全控制 → 系統完整性監控**"。
4. 要匯出或匯入 *即時系統完整性監控* 規則：
   a. 在"**即時系統完整性監控**"塊中，點擊"**設定**"按鈕。
   b. 若要匯出即時系統完整性監控規則清單：
      1. 選取您想要匯出的規則。要選擇多個連接埠，請使用**CTRL**或**SHIFT**鍵。
         如果您未選擇任何規則，則 Kaspersky Endpoint Security 將匯出所有規則。
      2. 點擊"**匯出**"連接。
      3. 在開啟的視窗中，指定您要將規則清單匯出到的 XML 檔案的名稱，然後選取要儲存此檔案的資料夾。
      4. 儲存檔案。
         Kaspersky Endpoint Security 會將規則清單匯出到 XML 檔案。
   c. 若要匯入即時系統完整性監控規則清單：
      1. 點擊"**匯入**"連接。
         在開啟的視窗中，選取要從中匯入規則清單的 XML 檔案。
      2. 開啟檔案。
         如果電腦已經具有規則清單，則 Kaspersky Endpoint Security 將提示您刪除現有清單或從 XML 檔案向其中新增新項目。
5. 若要匯出或匯入 *系統完整性檢查* 規則：
   a. 在"**系統完整性檢查**"塊中，選取"**自訂設定**"。
   b. 點擊"**設定**"。
   c. 若要匯出系統完整性檢查規則清單：
      1. 選取您想要匯出的規則。要選擇多個連接埠，請使用**CTRL**或**SHIFT**鍵。
         如果您未選擇任何規則，則 Kaspersky Endpoint Security 將匯出所有規則。
      2. 點擊"**匯出**"連接。

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

4. 儲存檔案。

Kaspersky Endpoint Security 會將規則清單匯出到 XML 檔案。

d. 若要匯入系統完整性檢查規則清單：

1. 點擊**"匯入"**連接。

在開啟的視窗中，選取要從中匯入規則清單的 XML 檔案。

2. 開啟檔案。

如果電腦已經具有規則清單，則 Kaspersky Endpoint Security 將提示您刪除現有清單或從 XML 檔案向其中新增新項目。

6. 儲存變更。

**如何在網頁主控台中匯出和匯入系統完整性監控規則清單**

1. 在網頁主控台的主視窗中，選擇**資產（裝置）→政策和設定檔**。

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. 選擇**"Windows"**標籤。

6. 要匯出或匯入 *即時系統完整性監控* 規則：

a. 在**"即時系統完整性監控"**塊中，點擊**"規則"**連接。

b. 若要匯出即時系統完整性監控規則清單：

1. 選取您想要匯出的規則。

2. 點擊 → **匯出** 按鈕。

Kaspersky Endpoint Security 會將規則清單匯出到預設下載資料夾中的 JSON 檔案。

c. 若要匯入即時系統完整性監控規則清單：

1. 點擊 → **匯入** 按鈕。

在開啟的視窗中，選取要從中匯入受信任網址清單的 JSON 檔案。

2. 開啟檔案。

如果電腦已經具有規則清單，則 Kaspersky Endpoint Security 將提示您刪除現有清單或從 JSON 檔案向其中新增新項目。

7. 若要匯出或匯入 *系統完整性檢查* 規則：

   a. 在“**按需系統完整性檢查**”塊中，選取“**自訂設定**”。

   b. 點擊”**規則**”連接。

   c. 若要匯出系統完整性檢查規則清單：

      1. 選取您想要匯出的規則。

      2. 點擊 → **匯出** 按鈕。

         Kaspersky Endpoint Security 會將規則清單匯出到預設下載資料夾中的 JSON 檔案。

   d. 若要匯入系統完整性檢查規則清單：

      1. 點擊 → **匯入** 按鈕。

         在開啟的視窗中，選取要從中匯入受信任網址清單的 JSON 檔案。

      2. 開啟檔案。

         如果電腦已經具有規則清單，則 Kaspersky Endpoint Security 將提示您刪除現有清單或從 JSON 檔案向其中新增新項目。

8. 儲存變更。

d. 設定系統完整性監控規則（請參閱下表）。

9. 配置外部裝置監控：

   a. 選擇“**監控裝置**”核取方塊。

   b. 在**事件嚴重性級別**下拉式清單中，選擇外部裝置監控事件的重要性等級：*資訊*, *警告*, *緊急*。

系統完整性監控記錄外部裝置的目前連線情況。在應用程式設定中啟用該元件後，應用程式開始監控外部裝置的連線和中斷連線。隨後，當外部裝置連線或斷開連線時，應用程式會產生相應的事件。

10. 儲存變更。

**如何在應用程式介面中啟用即時系統完整性監控**

1. 在“應用程式主視窗”中，點擊 按鈕。

2. 在應用程式設定視窗中，選取”**安全控制**“→“**系統完整性監控**”。

3. 開啟 **系統完整性監控** 切換開關。

4. 在**用於封鎖規則的操作模式**下面，選擇即時系統完整性監控模式：

   - **封鎖**在此模式下，系統完整性監控會封鎖監控範圍內的檔案和登錄機碼的操作，並產生對應的事件。
   - **通知**在此模式下，系統完整性監控允許對監控範圍內的檔案和登錄機碼進行操作，並產生相應的事件。

5. 在“**即時系統完整性監控**“塊中，選中“**即時系統完整性監控**”核取方塊。

6. 配置外部裝置監控：

   a. 選擇**"監控裝置"**核取方塊。

   b. 在**事件嚴重性級別**下拉式清單中，選擇外部裝置監控事件的重要性等級：*資訊*, *警告*, *緊急*。

系統完整性監控記錄外部裝置的目前連線情況。在應用程式設定中啟用該元件後，應用程式開始監控外部裝置的連線和中斷連線。隨後，當外部裝置連線或斷開連線時，應用程式會產生相應的事件。

7. 配置檔案和登錄檔監控：

   a. 選擇**"監控檔案和登錄檔"**核取方塊。

   b. 點擊**"設定"**。

   這將開啟系統完整性監控規則清單。

   c. 點擊**"新增"**。

   您也可以 **從其他來源匯入規則**。

   您可以將系統完整性監控規則清單匯出到 XML 檔案。然後，您可以修改檔案，例如，新增大量相同類型的記錄。您可以使用匯出/匯入功能來備份系統完整性監控規則清單，或將清單遷移到其他伺服器。

> 系統完整性監控不支援為*系統完整性檢查*工作匯入 `HKEY_CURRENT_USER` 和 `HKEY_CURRENT_CONFIG` 金鑰。如果工作的監控範圍包含這些金鑰，應用程式會產生*監控範圍包括不正確的物件*事件。

**如何在管理主控台 (MMC) 中匯出和匯入系統完整性監控規則清單**

1. 在卡巴斯基安全管理中心管理主控台樹狀目錄中，選取**政策**。
2. 選擇必要的政策並點擊以開啟政策內容。
3. 在政策視窗中，選擇**"安全控制 → 系統完整性監控"**。
4. 要匯出或匯入 *即時系統完整性監控* 規則：

   a. 在**"即時系統完整性監控"**塊中，點擊**"設定"**按鈕。

   b. 若要匯出即時系統完整性監控規則清單：

      1. 選取您想要匯出的規則。要選擇多個連接埠，請使用**CTRL**或**SHIFT**鍵。

         如果您未選擇任何規則，則 Kaspersky Endpoint Security 將匯出所有規則。

      2. 點擊**"匯出"**連接。
      3. 在開啟的視窗中，指定您要將規則清單匯出到的 XML 檔案的名稱，然後選取要儲存此檔案的資料夾。
      4. 儲存檔案。

         Kaspersky Endpoint Security 會將規則清單匯出到 XML 檔案。

c. 若要匯入即時系統完整性監控規則清單：

1. 點擊"**匯入**"連接。

   在開啟的視窗中，選取要從中匯入規則清單的 XML 檔案。

2. 開啟檔案。

   如果電腦已經具有規則清單，則 Kaspersky Endpoint Security 將提示您刪除現有清單或從 XML 檔案向其中新增新項目。

5. 若要匯出或匯入 *系統完整性檢查* 規則：

a. 在"**系統完整性檢查**"塊中，選取"**自訂設定**"。

b. 點擊"**設定**"。

c. 若要匯出系統完整性檢查規則清單：

1. 選取您想要匯出的規則。要選擇多個連接埠，請使用**CTRL**或**SHIFT**鍵。

   如果您未選擇任何規則，則 Kaspersky Endpoint Security 將匯出所有規則。

2. 點擊"**匯出**"連接。

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

4. 儲存檔案。

Kaspersky Endpoint Security 會將規則清單匯出到 XML 檔案。

d. 若要匯入系統完整性檢查規則清單：

1. 點擊"**匯入**"連接。

   在開啟的視窗中，選取要從中匯入規則清單的 XML 檔案。

2. 開啟檔案。

如果電腦已經具有規則清單，則 Kaspersky Endpoint Security 將提示您刪除現有清單或從 XML 檔案向其中新增新項目。

6. 儲存變更。

**如何在網頁主控台中匯出和匯入系統完整性監控規則清單**

1. 在網頁主控台的主視窗中，選擇**資產（裝置）→政策和設定檔**。

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. 選擇"**Windows**"標籤。

6. 要匯出或匯入 *即時系統完整性監控* 規則：

a. 在"**即時系統完整性監控**"塊中，點擊"**規則**"連接。

b. 若要匯出即時系統完整性監控規則清單：

1. 選取您想要匯出的規則。

2. 點擊 → **匯出** 按鈕。

Kaspersky Endpoint Security 會將規則清單匯出到預設下載資料夾中的 JSON 檔案。

c. 若要匯入即時系統完整性監控規則清單：

1. 點擊 → **匯入** 按鈕。

在開啟的視窗中，選取要從中匯入受信任網址清單的 JSON 檔案。

2. 開啟檔案。

如果電腦已經具有規則清單，則 Kaspersky Endpoint Security 將提示您刪除現有清單或從 JSON 檔案向其中新增新項目。

7. 若要匯出或匯入 *系統完整性檢查* 規則：

a. 在"**按需系統完整性檢查**"塊中，選取"**自訂設定**"。

b. 點擊"**規則**"連接。

c. 若要匯出系統完整性檢查規則清單：

1. 選取您想要匯出的規則。

2. 點擊 → **匯出** 按鈕。

Kaspersky Endpoint Security 會將規則清單匯出到預設下載資料夾中的 JSON 檔案。

d. 若要匯入系統完整性檢查規則清單：

1. 點擊 → **匯入** 按鈕。

在開啟的視窗中，選取要從中匯入受信任網址清單的 JSON 檔案。

2. 開啟檔案。

如果電腦已經具有規則清單，則 Kaspersky Endpoint Security 將提示您刪除現有清單或從 JSON 檔案向其中新增新項目。

8. 儲存變更。

8. 設定系統完整性監控規則（請參閱下表）。

9. 儲存變更。

| 參數 | 描述 |
| --- | --- |
| **規則名稱** | 即時系統完整性監控規則的名稱 |
| **檔案和登錄檔操作** | • **允許**系統完整性監控允許對監控範圍內的檔案和登錄機碼進行操作。<br>• **封鎖**系統完整性監控行為取決於所選模式。如果您選擇了*系統防護模式*，系統完整性監控會封鎖監控範圍內的檔案和登錄機碼操作，產生對應的事件，並在在卡巴斯基安全管理中心主控台中變更裝置的狀態。如果您選擇了*測試模式*，系統完整性監控將允許對監控範圍內的檔案和登錄機碼進行操作。 |
| **事件嚴重性級別** | 只要監控範圍中的檔案或登錄機碼被修改，Kaspersky Endpoint Security 就會記錄檔案修改事件。以下事件嚴重程度級別可用：*資訊*, *警告*, *緊急*。 |
| **監控範圍** | • **檔案**元件監視的檔案和資料夾的清單。Kaspersky Endpoint Security 輸入遮罩時支援環境變量以及`*`和`?`字元。<br>使用遮罩：<br>  • `*`（星號）字元代表任意一組字元，但`\`和`/`字元除外（這兩個字元是檔案和資料夾路徑中的檔案和資料夾名稱的分隔符號）。例如，遮罩"`C:\*\*.txt`"將包括位於 C: 磁碟機但是不在子資料夾中所有帶 TXT 副檔名的檔案的路徑。<br>  • 兩個連續`*`字元在檔案或資料夾名稱中代表任意一組字元（包括空集），包括`\`和`/`字元（這兩個字元是檔案和資料夾路徑中的檔案和資料夾名稱的分隔符號）。例如，遮罩`C:\Folder\**\*.txt`將包括位於巢嵌在`Folder`內的資料夾（`Folder`自身除外）中所有帶 TXT 副檔名的檔案的路徑。遮罩必須包含至少一個嵌套等級。遮罩`C:\**\*.txt`不是有效遮罩。<br>  • `?`（問號）字元代表任意單個字元，但`\`和`/`字元除外（這兩個字元是檔案和資料夾路徑中的檔案和資料夾名稱的分隔符號）。例如，遮罩`C:\Folder\???.txt`將包括位於`Folder`資料夾中所有帶 TXT 副檔名且名稱由三個字元構成的檔案的路徑。<br>• **登錄檔**元件監視的登錄機碼和值的清單。Kaspersky Endpoint Security 輸入遮罩時支援`*`和`?`字元。 |
| **排除項目** | • **檔案**來自監控範圍的排除項目清單。Kaspersky Endpoint Security 輸入遮罩時支援環境變量以及`*`和`?`字元。例如，`C:\Folder\Application\*.log`。排除項目比監控範圍項目具有更高的優先順序。<br>使用遮罩：<br>  • `*`（星號）字元代表任意一組字元，但`\`和`/`字元除外（這兩個字元是檔案和資料夾路徑中的檔案和資料夾名稱的分隔符號）。例如，遮罩"`C:\*\*.txt`"將包括位於 C: 磁碟機但是不在子資料夾中所有帶 TXT 副檔名的檔案的路徑。<br>  • 兩個連續`*`字元在檔案或資料夾名稱中代表任意一組字元（包括空集），包括`\`和`/`字元（這兩個字元是檔案和資料夾路徑中的檔案和資料夾名稱的分隔符號）。例如，遮罩`C:\Folder\**\*.txt`將包括位於巢嵌在`Folder`內的資料夾（`Folder`自身除外）中所有帶 TXT 副檔名的檔案的路徑。遮罩必須包含至少一個嵌套等級。遮罩`C:\**\*.txt`不是有效遮罩。<br>  • `?`（問號）字元代表任意單個字元，但`\`和`/`字元除外（這兩個字元是檔案和資料夾路徑中的檔案和資料夾名稱的分隔符號）。例如，遮罩`C:\Folder\???.txt`將包括位於`Folder`資料夾中所有帶 TXT 副檔名且名稱由三個字元構成的檔案的路徑。<br>• **登錄檔**來自監控範圍的排除項目清單。Kaspersky Endpoint Security 輸入遮罩時支援`*`和`?`字元。排除項目比監控範圍項目具有更高的優先順序。 |
| **受信任的使用者和/或使用者群組** | *受信任使用者*是被允許對監視範圍內的檔案和登錄機碼執行操作的使用者。如果 Kaspersky Endpoint Security 偵測到受信任使用者執行的操作，系統完整性監控會產生一個*資訊*事件。<br>您可以在 Active Directory 中、在卡巴斯基安全管理中心的账户清單中或透過手動輸入本機使用者名稱來選擇使用者。卡巴斯基建議僅在無法使用網域使用者帳戶的特殊情況下使用本機使用者帳戶。 |
| **檔案作業標誌/被監控的作業** | 標記，標誌對應用程式將監視的檔案或登錄機碼採取的操作。 |
| **散列** | 計算修改時的檔案雜湊值。Kaspersky Endpoint Security 在產生事件時會加入有關檔案雜湊的資訊。 |

# 按需系統完整性檢查

按需系統完整性檢查是一項可以手動或按排程執行的工作。當執行*系統完整性檢查*工作時，應用程式將監控範圍內包含的物件的目前狀態與它們的*基線*狀態進行比較 。與即時系統完整性監控相比，*系統完整性檢查*工作有助於限制事件數量，讓您產生作業系統變更的總體報告。

為了使系統完整性監控正常運作，您必須新增至少一個規則。*系統完整性監控規則*是定義使用者對檔案和登錄檔的存取權限的一組標準。系統完整性監控可偵測指定*監控範圍*內檔案和登錄檔的變更。監控範圍是系統完整性監控規則的標準之一。您可以配置由即時系統完整性監控和 *系統完整性檢查* 工作共用的規則或為工作建立單獨規則。為了建立基線，Kaspersky Endpoint Security 會將*系統完整性檢查* 工作的監控範圍套用到*基線更新*工作。

建立和更新基線

*系統完整性檢查*工作需要基準才能工作。*基線*是系統中物件的記錄狀態，應用程式在與目前狀態進行比較時將其用作參考。如果系統的目前狀態與基準中記錄的系統狀態不同，Kaspersky Endpoint Security 會產生對應的事件。您可以使用*基線更新*工作建立或更新基線。

您可以透過以下方式更新基線：

- 完整更新。

  應用程式更新監控範圍內的所有物件。

- 增量更新。

  應用程式僅偵測和更新已修改或新的物件。

**如何在管理主控台 (MMC) 中建立或更新基線**

1. 在卡巴斯基安全管理中心管理主控台樹狀目錄中，選取**工作**。

   工作清單開啟。

2. 點擊**"新工作"**。

啟動"工作精靈"。按照精靈的說明進行操作。

步驟 1. 選取工作類型

選取**"Kaspersky Endpoint Security for Windows (12.12)"→"基線更新"**。

步驟 2.選擇基準更新模式

選擇基線更新模式：

- **完整更新**應用程式更新監控範圍內的所有物件。
- **遞增更新**應用程式僅偵測和更新已修改或新的物件。

步驟 3. 選取將要對其分配工作的裝置

選取將要執行工作的電腦。下列選項可用：

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

步驟 4. 定義工作名稱

輸入工作名稱，例如 *基線 2024*。

步驟 5. 完成工作建立

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

**如何在網頁主控台中建立或更新基線**

1. 在網頁主控台的主視窗中，選擇**資產（裝置）→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 Windows 12.12.0"**。
   b. 在**"工作類型"**下拉式清單中，選取**"基線更新"**。
   c. 在**"工作名稱"**欄位中，輸入簡要說明，例如"*基線 2024*"。
   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。前往下一步。
5. 選取要執行工作的帳戶。預設情況下，Kaspersky Endpoint Security 將使用本機使用者帳戶的權限啟動工作。
6. 結束精靈。
   在工作清單中將顯示一個新工作。
7. 點擊新工作。
   工作內容視窗將開啟。

8. 選擇**"應用程式設定"**標籤。
9. 選擇基線更新模式：
   - **完整更新**應用程式更新監控範圍內的所有物件。
   - **遞增更新**應用程式僅偵測和更新已修改或新的物件。
10. 儲存變更。
11. 選中該工作旁邊的核取方塊。
12. 點擊**"開始"**。

### 配置系統完整性檢查工作的監控範圍

預設情況下，*系統完整性檢查*工作的監控範圍與即時系統完整性監控的監控範圍相同。您可以為工作配置不同的監控範圍。

系統完整性監控不支援為*系統完整性檢查*工作匯入 HKEY_CURRENT_USER 和 HKEY_CURRENT_CONFIG 金鑰。如果工作的監控範圍包含這些金鑰，應用程式會產生*監控範圍包括不正確的物件*事件。

#### 如何在管理主控台 (MMC) 中為系統完整性檢查工作配置不同的監控範圍

1. 在卡巴斯基安全管理中心管理主控台樹狀目錄中，選取**政策**。
2. 選擇必要的政策並點擊以開啟政策內容。
3. 在政策視窗中，選擇**"安全控制 → 系統完整性監控"**。
4. 選擇**"系統完整性監控"**核取方塊。
5. 在**系統完整性檢查**下面，選擇工作配置模式：**自訂設定**。
6. 配置外部裝置監控：
   a. 選擇**"監控裝置"**核取方塊。
   b. 在**事件嚴重性級別**下拉式清單中，選擇外部裝置監控事件的重要性等級：*資訊*, *警告*, *緊急*。

   系統完整性監控記錄在建立基線時已連線外部裝置的資訊。隨後，當連線外部裝置時，應用程式會產生相應的事件。當執行*系統完整性檢查*工作時，應用程式不會監控外部裝置的中斷連線。
7. 配置檔案和登錄檔監控：
   a. 選擇**"監控檔案和登錄檔"**核取方塊。
   b. 點擊**"設定"**。

      這將開啟系統完整性監控規則清單。
   c. 點擊**"新增"**。

您也可以 **從其他來源匯入規則**。

您可以將系統完整性監控規則清單匯出到 XML 檔案。然後，您可以修改檔案，例如，新增大量相同類型的記錄。您可以使用匯出/匯入功能來備份系統完整性監控規則清單，或將清單遷移到其他伺服器。

系統完整性監控不支援為*系統完整性檢查*工作匯入 HKEY_CURRENT_USER 和 HKEY_CURRENT_CONFIG 金鑰。如果工作的監控範圍包含這些金鑰，應用程式會產生*監控範圍包括不正確的物件*事件。

**如何在管理主控台 (MMC) 中匯出和匯入系統完整性監控規則清單**

1. 在卡巴斯基安全管理中心管理主控台樹狀目錄中，選取**政策**。
2. 選擇必要的政策並點擊以開啟政策內容。
3. 在政策視窗中，選擇**"安全控制 → 系統完整性監控"**。
4. 要匯出或匯入 *即時系統完整性監控* 規則：
   a. 在**"即時系統完整性監控"**塊中，點擊**"設定"**按鈕。
   b. 若要匯出即時系統完整性監控規則清單：
      1. 選取您想要匯出的規則。要選擇多個連接埠，請使用**CTRL**或**SHIFT**鍵。
         如果您未選擇任何規則，則 Kaspersky Endpoint Security 將匯出所有規則。
      2. 點擊**"匯出"**連接。
      3. 在開啟的視窗中，指定您要將規則清單匯出到的 XML 檔案的名稱，然後選取要儲存此檔案的資料夾。
      4. 儲存檔案。
         Kaspersky Endpoint Security 會將規則清單匯出到 XML 檔案。
   c. 若要匯入即時系統完整性監控規則清單：
      1. 點擊**"匯入"**連接。
         在開啟的視窗中，選取要從中匯入規則清單的 XML 檔案。
      2. 開啟檔案。
         如果電腦已經具有規則清單，則 Kaspersky Endpoint Security 將提示您刪除現有清單或從 XML 檔案向其中新增新項目。
5. 若要匯出或匯入 *系統完整性檢查* 規則：
   a. 在**"系統完整性檢查"**塊中，選取**"自訂設定"**。
   b. 點擊**"設定"**。
   c. 若要匯出系統完整性檢查規則清單：
      1. 選取您想要匯出的規則。要選擇多個連接埠，請使用**CTRL**或**SHIFT**鍵。
         如果您未選擇任何規則，則 Kaspersky Endpoint Security 將匯出所有規則。

2. 點擊"**匯出**"連接。

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

4. 儲存檔案。

Kaspersky Endpoint Security 會將規則清單匯出到 XML 檔案。

d. 若要匯入系統完整性檢查規則清單：

1. 點擊"**匯入**"連接。

在開啟的視窗中，選取要從中匯入規則清單的 XML 檔案。

2. 開啟檔案。

如果電腦已經具有規則清單，則 Kaspersky Endpoint Security 將提示您刪除現有清單或從 XML 檔案向其中新增新項目。

6. 儲存變更。

**如何在網頁主控台中匯出和匯入系統完整性監控規則清單**

1. 在網頁主控台的主視窗中，選擇**資產（裝置）→ 政策和設定檔**。

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. 選擇"**Windows**"標籤。

6. 要匯出或匯入 *即時系統完整性監控* 規則：

a. 在"**即時系統完整性監控**"塊中，點擊"**規則**"連接。

b. 若要匯出即時系統完整性監控規則清單：

1. 選取您想要匯出的規則。

2. 點擊 → **匯出** 按鈕。

Kaspersky Endpoint Security 會將規則清單匯出到預設下載資料夾中的 JSON 檔案。

c. 若要匯入即時系統完整性監控規則清單：

1. 點擊 → **匯入** 按鈕。

在開啟的視窗中，選取要從中匯入受信任網址清單的 JSON 檔案。

2. 開啟檔案。

如果電腦已經具有規則清單，則 Kaspersky Endpoint Security 將提示您刪除現有清單或從 JSON 檔案向其中新增新項目。

7. 若要匯出或匯入 *系統完整性檢查* 規則：

a. 在“**按需系統完整性檢查**”塊中，選取“**自訂設定**”。

b. 點擊”**規則**”連接。

c. 若要匯出系統完整性檢查規則清單：

1. 選取您想要匯出的規則。

2. 點擊 → **匯出** 按鈕。

Kaspersky Endpoint Security 會將規則清單匯出到預設下載資料夾中的 JSON 檔案。

d. 若要匯入系統完整性檢查規則清單：

1. 點擊 → **匯入** 按鈕。

在開啟的視窗中，選取要從中匯入受信任網址清單的 JSON 檔案。

2. 開啟檔案。

如果電腦已經具有規則清單，則 Kaspersky Endpoint Security 將提示您刪除現有清單或從 JSON 檔案向其中新增新項目。

8. 儲存變更。

d. 設定系統完整性監控規則（請參閱下表）。

8. 儲存變更。

**如何在網頁主控台中為系統完整性檢查工作配置不同的監控範圍**

1. 在網頁主控台的主視窗中，選擇**資產（裝置）→ 政策和設定檔**。

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. 選擇“**Windows**”標籤。

6. 開啟“**系統完整性監控已啟用**“開關。

7. 在**系統完整性檢查**下面，選擇工作配置模式：**自訂設定**。

8. 配置外部裝置監控：

a. 選擇**“監控裝置”**核取方塊。

b. 在**事件嚴重性級別**下拉式清單中，選擇外部裝置監控事件的重要性等級：*資訊*, *警告*, *緊急*。

系統完整性監控記錄在建立基線時已連線外部裝置的資訊。隨後，當連線外部裝置時，應用程式會產生相應的事件。當執行 *系統完整性檢查* 工作時，應用程式不會監控外部裝置的中斷連線。

9. 配置檔案和登錄檔監控：

a. 選擇**"監控檔案和登錄檔"**核取方塊。

b. 點擊**"規則"**。

這將開啟系統完整性監控規則清單。

c. 點擊**"新增"**。

您也可以 **從其他來源匯入規則**。

您可以將系統完整性監控規則清單匯出到 XML 檔案。然後，您可以修改檔案，例如，新增大量相同類型的記錄。您可以使用匯出/匯入功能來備份系統完整性監控規則清單，或將清單遷移到其他伺服器。

系統完整性監控不支援為*系統完整性檢查*工作匯入 `HKEY_CURRENT_USER` 和 `HKEY_CURRENT_CONFIG` 金鑰。如果工作的監控範圍包含這些金鑰，應用程式會產生*監控範圍包括不正確的物件*事件。

**如何在管理主控台 (MMC) 中匯出和匯入系統完整性監控規則清單**

1. 在卡巴斯基安全管理中心管理主控台樹狀目錄中，選取**政策**。

2. 選擇必要的政策並點擊以開啟政策內容。

3. 在政策視窗中，選擇**"安全控制 → 系統完整性監控"**。

4. 要匯出或匯入 *即時系統完整性監控* 規則：

a. 在**"即時系統完整性監控"**塊中，點擊**"設定"**按鈕。

b. 若要匯出即時系統完整性監控規則清單：

1. 選取您想要匯出的規則。要選擇多個連接埠，請使用**CTRL**或**SHIFT**鍵。

如果您未選擇任何規則，則 Kaspersky Endpoint Security 將匯出所有規則。

2. 點擊**"匯出"**連接。

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

4. 儲存檔案。

Kaspersky Endpoint Security 會將規則清單匯出到 XML 檔案。

c. 若要匯入即時系統完整性監控規則清單：

1. 點擊**"匯入"**連接。

在開啟的視窗中，選取要從中匯入規則清單的 XML 檔案。

2. 開啟檔案。

如果電腦已經具有規則清單，則 Kaspersky Endpoint Security 將提示您刪除現有清單或從 XML 檔案向其中新增新項目。

5. 若要匯出或匯入 *系統完整性檢查* 規則：

   a. 在**"系統完整性檢查"**塊中，選取**"自訂設定"**。

   b. 點擊**"設定"**。

   c. 若要匯出系統完整性檢查規則清單：

      1. 選取您想要匯出的規則。要選擇多個連接埠，請使用**CTRL**或**SHIFT**鍵。

         如果您未選擇任何規則，則 Kaspersky Endpoint Security 將匯出所有規則。

      2. 點擊**"匯出"**連接。

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

      4. 儲存檔案。

      Kaspersky Endpoint Security 會將規則清單匯出到 XML 檔案。

   d. 若要匯入系統完整性檢查規則清單：

      1. 點擊**"匯入"**連接。

         在開啟的視窗中，選取要從中匯入規則清單的 XML 檔案。

      2. 開啟檔案。

      如果電腦已經具有規則清單，則 Kaspersky Endpoint Security 將提示您刪除現有清單或從 XML 檔案向其中新增新項目。

6. 儲存變更。

**如何在網頁主控台中匯出和匯入系統完整性監控規則清單**

1. 在網頁主控台的主視窗中，選擇**資產（裝置）→ 政策和設定檔**。

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. 選擇**"Windows"**標籤。

6. 要匯出或匯入 *即時系統完整性監控* 規則：

a. 在"**即時系統完整性監控**"塊中，點擊"**規則**"連接。

b. 若要匯出即時系統完整性監控規則清單：

1. 選取您想要匯出的規則。

2. 點擊 → **匯出** 按鈕。

Kaspersky Endpoint Security 會將規則清單匯出到預設下載資料夾中的 JSON 檔案。

c. 若要匯入即時系統完整性監控規則清單：

1. 點擊 → **匯入** 按鈕。

在開啟的視窗中，選取要從中匯入受信任網址清單的 JSON 檔案。

2. 開啟檔案。

如果電腦已經具有規則清單，則 Kaspersky Endpoint Security 將提示您刪除現有清單或從 JSON 檔案向其中新增新項目。

7. 若要匯出或匯入 *系統完整性檢查* 規則：

a. 在"**按需系統完整性檢查**"塊中，選取"**自訂設定**"。

b. 點擊"**規則**"連接。

c. 若要匯出系統完整性檢查規則清單：

1. 選取您想要匯出的規則。

2. 點擊 → **匯出** 按鈕。

Kaspersky Endpoint Security 會將規則清單匯出到預設下載資料夾中的 JSON 檔案。

d. 若要匯入系統完整性檢查規則清單：

1. 點擊 → **匯入** 按鈕。

在開啟的視窗中，選取要從中匯入受信任網址清單的 JSON 檔案。

2. 開啟檔案。

如果電腦已經具有規則清單，則 Kaspersky Endpoint Security 將提示您刪除現有清單或從 JSON 檔案向其中新增新項目。

8. 儲存變更。

d. 設定系統完整性監控規則（請參閱下表）。

10. 儲存變更。

**如何配置不同的監控範圍 系統完整性檢查 應用程式介面中的工作**

1. 在"應用程式主視窗"中，點擊 按鈕。

2. 在應用程式設定視窗中，選取"**安全控制**"→"**系統完整性監控**"。

3. 開啟 **系統完整性監控** 切換開關。

4. 在**系統完整性檢查**下面，選擇工作配置模式：**自訂設定**。

5. 配置外部裝置監控：

   a. 選擇**"監控裝置"**核取方塊。

   b. 在**事件嚴重性級別**下拉式清單中，選擇外部裝置監控事件的重要性等級：*資訊*, *警告*, *緊急*。

   系統完整性監控記錄在建立基線時已連線外部裝置的資訊。隨後，當連線外部裝置時，應用程式會產生相應的事件。當執行*系統完整性檢查*工作時，應用程式不會監控外部裝置的中斷連線。

6. 配置檔案和登錄檔監控：

   a. 選擇**"監控檔案和登錄檔"**核取方塊。

   b. 點擊**"設定"**。

   這將開啟系統完整性監控規則清單。

   c. 點擊**"新增"**。

   您也可以 **從其他來源匯入規則**。

   您可以將系統完整性監控規則清單匯出到 XML 檔案。然後，您可以修改檔案，例如，新增大量相同類型的記錄。您可以使用匯出/匯入功能來備份系統完整性監控規則清單，或將清單遷移到其他伺服器。

   > 系統完整性監控不支援為*系統完整性檢查*工作匯入 `HKEY_CURRENT_USER` 和 `HKEY_CURRENT_CONFIG` 金鑰。如果工作的監控範圍包含這些金鑰，應用程式會產生*監控範圍包括不正確的物件*事件。

   **如何在管理主控台 (MMC) 中匯出和匯入系統完整性監控規則清單**

   1. 在卡巴斯基安全管理中心管理主控台樹狀目錄中，選取**政策**。

   2. 選擇必要的政策並點擊以開啟政策內容。

   3. 在政策視窗中，選擇**"安全控制 → 系統完整性監控"**。

   4. 要匯出或匯入 *即時系統完整性監控* 規則：

      a. 在**"即時系統完整性監控"**塊中，點擊**"設定"**按鈕。

      b. 若要匯出即時系統完整性監控規則清單：

         1. 選取您想要匯出的規則。要選擇多個連接埠，請使用**CTRL**或**SHIFT**鍵。

            如果您未選擇任何規則，則 Kaspersky Endpoint Security 將匯出所有規則。

         2. 點擊**"匯出"**連接。

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

         4. 儲存檔案。

            Kaspersky Endpoint Security 會將規則清單匯出到 XML 檔案。

c. 若要匯入即時系統完整性監控規則清單：

1. 點擊"**匯入**"連接。

   在開啟的視窗中，選取要從中匯入規則清單的 XML 檔案。

2. 開啟檔案。

   如果電腦已經具有規則清單，則 Kaspersky Endpoint Security 將提示您刪除現有清單或從 XML 檔案向其中新增新項目。

5. 若要匯出或匯入 *系統完整性檢查* 規則：

a. 在"**系統完整性檢查**"塊中，選取"**自訂設定**"。

b. 點擊"**設定**"。

c. 若要匯出系統完整性檢查規則清單：

1. 選取您想要匯出的規則。要選擇多個連接埠，請使用**CTRL**或**SHIFT**鍵。

   如果您未選擇任何規則，則 Kaspersky Endpoint Security 將匯出所有規則。

2. 點擊"**匯出**"連接。

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

4. 儲存檔案。

Kaspersky Endpoint Security 會將規則清單匯出到 XML 檔案。

d. 若要匯入系統完整性檢查規則清單：

1. 點擊"**匯入**"連接。

   在開啟的視窗中，選取要從中匯入規則清單的 XML 檔案。

2. 開啟檔案。

如果電腦已經具有規則清單，則 Kaspersky Endpoint Security 將提示您刪除現有清單或從 XML 檔案向其中新增新項目。

6. 儲存變更。

**如何在網頁主控台中匯出和匯入系統完整性監控規則清單**

1. 在網頁主控台的主視窗中，選擇**資產（裝置）→政策和設定檔**。

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. 選擇"**Windows**"標籤。

6. 要匯出或匯入 *即時系統完整性監控* 規則：

a. 在"**即時系統完整性監控**"塊中，點擊"**規則**"連接。

b. 若要匯出即時系統完整性監控規則清單：

1. 選取您想要匯出的規則。

2. 點擊 → **匯出** 按鈕。

Kaspersky Endpoint Security 會將規則清單匯出到預設下載資料夾中的 JSON 檔案。

c. 若要匯入即時系統完整性監控規則清單：

1. 點擊 → **匯入** 按鈕。

在開啟的視窗中，選取要從中匯入受信任網址清單的 JSON 檔案。

2. 開啟檔案。

如果電腦已經具有規則清單，則 Kaspersky Endpoint Security 將提示您刪除現有清單或從 JSON 檔案向其中新增新項目。

7. 若要匯出或匯入 *系統完整性檢查* 規則：

a. 在"**按需系統完整性檢查**"塊中，選取"**自訂設定**"。

b. 點擊"**規則**"連接。

c. 若要匯出系統完整性檢查規則清單：

1. 選取您想要匯出的規則。

2. 點擊 → **匯出** 按鈕。

Kaspersky Endpoint Security 會將規則清單匯出到預設下載資料夾中的 JSON 檔案。

d. 若要匯入系統完整性檢查規則清單：

1. 點擊 → **匯入** 按鈕。

在開啟的視窗中，選取要從中匯入受信任網址清單的 JSON 檔案。

2. 開啟檔案。

如果電腦已經具有規則清單，則 Kaspersky Endpoint Security 將提示您刪除現有清單或從 JSON 檔案向其中新增新項目。

8. 儲存變更。

d. 設定系統完整性監控規則（請參閱下表）。

7. 儲存變更。

| 參數 | 描述 |
| --- | --- |
| **規則名稱** | *系統完整性檢查* 工作規則的名稱。 |
| **事件嚴重性級別** | 只要監控範圍中的檔案或登錄機碼被修改，Kaspersky Endpoint Security 就會記錄檔案修改事件。以下事件嚴重程度級別可用：*資訊*, *警告*, *緊急*。 |
| **監控範圍** | • **檔案**元件監視的檔案和資料夾的清單。Kaspersky Endpoint Security 輸入遮罩時支援環境變量以及`*`和`?`字元。<br>使用遮罩：<br>  • `*`（星號）字元代表任意一組字元，但`\`和`/`字元除外（這兩個字元是檔案和資料夾路徑中的檔案和資料夾名稱的分隔符號）。例如，遮罩"`C:\*\*.txt`"將包括位於 C: 磁碟機但是不在子資料夾中所有帶 TXT 副檔名的檔案的路徑。<br>  • 兩個連續`*`字元在檔案或資料夾名稱中代表任意一組字元（包括空集），包括`\`和`/`字元（這兩個字元是檔案和資料夾路徑中的檔案和資料夾名稱的分隔符號）。例如，遮罩`C:\Folder\**\*.txt`將包括位於巢嵌在`Folder`內的資料夾（`Folder`自身除外）中所有帶 TXT 副檔名的檔案的路徑。遮罩必須包含至少一個嵌套等級。遮罩`C:\**\*.txt`不是有效遮罩。<br>  • `?`（問號）字元代表任意單個字元，但`\`和`/`字元除外（這兩個字元是檔案和資料夾路徑中的檔案和資料夾名稱的分隔符號）。例如，遮罩`C:\Folder\???.txt`將包括位於`Folder`資料夾中所有帶 TXT 副檔名且名稱由三個字元構成的檔案的路徑。<br>• **登錄檔**元件監視的登錄機碼和值的清單。Kaspersky Endpoint Security 輸入遮罩時支援`*`和`?`字元。 |
| **排除項目** | • **檔案**來自監控範圍的排除項目清單。Kaspersky Endpoint Security 輸入遮罩時支援環境變量以及`*`和`?`字元。例如，`C:\Folder\Application\*.log`。排除項目比監控範圍項目具有更高的優先順序。<br>使用遮罩：<br>  • `*`（星號）字元代表任意一組字元，但`\`和`/`字元除外（這兩個字元是檔案和資料夾路徑中的檔案和資料夾名稱的分隔符號）。例如，遮罩"`C:\*\*.txt`"將包括位於 C: 磁碟機但是不在子資料夾中所有帶 TXT 副檔名的檔案的路徑。<br>  • 兩個連續`*`字元在檔案或資料夾名稱中代表任意一組字元（包括空集），包括`\`和`/`字元（這兩個字元是檔案和資料夾路徑中的檔案和資料夾名稱的分隔符號）。例如，遮罩`C:\Folder\**\*.txt`將包括位於巢嵌在`Folder`內的資料夾（`Folder`自身除外）中所有帶 TXT 副檔名的檔案的路徑。遮罩必須包含至少一個嵌套等級。遮罩`C:\**\*.txt`不是有效遮罩。<br>  • `?`（問號）字元代表任意單個字元，但`\`和`/`字元除外（這兩個字元是檔案和資料夾路徑中的檔案和資料夾名稱的分隔符號）。例如，遮罩`C:\Folder\???.txt`將包括位於`Folder`資料夾中所有帶 TXT 副檔名且名稱由三個字元構成的檔案的路徑。<br>• **登錄檔**來自監控範圍的排除項目清單。Kaspersky Endpoint Security 輸入遮罩時支援`*`和`?`字元。排除項目比監控範圍項目具有更高的優先順序。 |

## 執行"系統完整性檢查"工作

*系統完整性檢查* 工作允許檢查檔案或登錄機碼是否有變更以及檢查外部裝置的連線。要檢查檔案是否發生變更，您可以用以下模式執行*系統完整性檢查*工作：

- 快速掃描。

  檢查檔案是否發生變更時，應用程式僅檢查檔案屬性。該應用程式不檢查檔案的內容。

- 完整掃描。

  檢查檔案是否發生變更時，應用程式會檢查所有檔案屬性和檔案內容。

工作執行的模式不影響對登錄檔或外部裝置的檢查。

### 如何在管理主控台 (MMC) 中執行系統完整性檢查工作

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

   工作清單開啟。

3. 點擊**"新工作"**。

   啟動"工作精靈"。按照精靈的說明進行操作。

4. 選取 **Kaspersky Endpoint Security → 基線系統完整性監控**。選擇系統完整性監控模式：

   - **完整掃描**在此模式下，應用程式檢查檔案的所有屬性和雜湊。
   - **快速掃描**在此模式下，應用程式僅檢查檔案的屬性。

5. 選取將要執行工作的電腦。下列選項可用：

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

6. 選取要執行工作的帳戶。預設情況下，Kaspersky Endpoint Security 將使用本機使用者帳戶的權限啟動工作。

7. 設定工作啟動排程，例如，手動或在一周中指定的一天。

8. 輸入工作的名稱。

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

**如何在網頁主控台中執行"系統完整性檢查"工作**

1. 在網頁主控台的主視窗中，選擇**資產（裝置）→ 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 Windows 12.12.0"**。

   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。前往下一步。

5. 選取要執行工作的帳戶。預設情況下，Kaspersky Endpoint Security 將使用本機使用者帳戶的權限啟動工作。

6. 結束精靈。

   在工作清單中將顯示一個新工作。

7. 點擊新工作。
   工作內容視窗將開啟。
8. 選擇"**應用程式設定**"標籤。
9. 選擇系統完整性檢查模式：
   - **快速掃描**應用程式僅檢查檔案屬性。該應用程式不檢查檔案的內容。
   - **完整掃描**應用程式檢查檔案的所有屬性及其內容。
10. 儲存變更。
11. 選中該工作旁邊的核取方塊。
12. 點擊"**開始**"。

為了*系統完整性檢查*工作順利完成，*系統完整性檢查*工作的監控範圍必須完全匹配基線。如果監視範圍不同，工作結束時會出現錯誤。若要同步監控範圍，請執行具有新監控範圍的*基線更新*工作。

# 匯出和匯入系統完整性監控規則

您可以將系統完整性監控規則清單匯出到 XML 檔案。然後，您可以修改檔案，例如，新增大量相同類型的記錄。您可以使用匯出/匯入功能來備份系統完整性監控規則清單，或將清單遷移到其他伺服器。

系統完整性監控不支援為*系統完整性檢查*工作匯入 `HKEY_CURRENT_USER` 和 `HKEY_CURRENT_CONFIG` 金鑰。如果工作的監控範圍包含這些金鑰，應用程式會產生*監控範圍包括不正確的物件*事件。

**如何在管理主控台 (MMC) 中匯出和匯入系統完整性監控規則清單**

1. 在卡巴斯基安全管理中心管理主控台樹狀目錄中，選取**政策**。
2. 選擇必要的政策並點擊以開啟政策內容。
3. 在政策視窗中，選擇"**安全控制 → 系統完整性監控**"。
4. 要匯出或匯入 *即時系統完整性監控* 規則：
   a. 在"**即時系統完整性監控**"塊中，點擊"**設定**"按鈕。
   b. 若要匯出即時系統完整性監控規則清單：
      1. 選取您想要匯出的規則。要選擇多個連接埠，請使用**CTRL**或**SHIFT**鍵。
         如果您未選擇任何規則，則 Kaspersky Endpoint Security 將匯出所有規則。
      2. 點擊"**匯出**"連接。
      3. 在開啟的視窗中，指定您要將規則清單匯出到的 XML 檔案的名稱，然後選取要儲存此檔案的資料夾。
      4. 儲存檔案。
         Kaspersky Endpoint Security 會將規則清單匯出到 XML 檔案。

c. 若要匯入即時系統完整性監控規則清單：

1. 點擊**"匯入"**連接。

   在開啟的視窗中，選取要從中匯入規則清單的 XML 檔案。

2. 開啟檔案。

   如果電腦已經具有規則清單，則 Kaspersky Endpoint Security 將提示您刪除現有清單或從 XML 檔案向其中新增新項目。

5. 若要匯出或匯入 *系統完整性檢查* 規則：

a. 在**"系統完整性檢查"**塊中，選取**"自訂設定"**。

b. 點擊**"設定"**。

c. 若要匯出系統完整性檢查規則清單：

1. 選取您想要匯出的規則。要選擇多個連接埠，請使用**CTRL**或**SHIFT**鍵。

   如果您未選擇任何規則，則 Kaspersky Endpoint Security 將匯出所有規則。

2. 點擊**"匯出"**連接。

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

4. 儲存檔案。

Kaspersky Endpoint Security 會將規則清單匯出到 XML 檔案。

d. 若要匯入系統完整性檢查規則清單：

1. 點擊**"匯入"**連接。

   在開啟的視窗中，選取要從中匯入規則清單的 XML 檔案。

2. 開啟檔案。

如果電腦已經具有規則清單，則 Kaspersky Endpoint Security 將提示您刪除現有清單或從 XML 檔案向其中新增新項目。

6. 儲存變更。

**如何在網頁主控台中匯出和匯入系統完整性監控規則清單**

1. 在網頁主控台的主視窗中，選擇**資產（裝置）→政策和設定檔**。

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. 選擇**"Windows"**標籤。

6. 要匯出或匯入 *即時系統完整性監控* 規則：

   a. 在"**即時系統完整性監控**"塊中，點擊"**規則**"連接。

   b. 若要匯出即時系統完整性監控規則清單：

      1. 選取您想要匯出的規則。

      2. 點擊 → **匯出** 按鈕。

         Kaspersky Endpoint Security 會將規則清單匯出到預設下載資料夾中的 JSON 檔案。

   c. 若要匯入即時系統完整性監控規則清單：

      1. 點擊 → **匯入** 按鈕。

         在開啟的視窗中，選取要從中匯入受信任網址清單的 JSON 檔案。

      2. 開啟檔案。

         如果電腦已經具有規則清單，則 Kaspersky Endpoint Security 將提示您刪除現有清單或從 JSON 檔案向其中新增新項目。

7. 若要匯出或匯入 *系統完整性檢查* 規則：

   a. 在"**按需系統完整性檢查**"塊中，選取"**自訂設定**"。

   b. 點擊"**規則**"連接。

   c. 若要匯出系統完整性檢查規則清單：

      1. 選取您想要匯出的規則。

      2. 點擊 → **匯出** 按鈕。

         Kaspersky Endpoint Security 會將規則清單匯出到預設下載資料夾中的 JSON 檔案。

   d. 若要匯入系統完整性檢查規則清單：

      1. 點擊 → **匯入** 按鈕。

         在開啟的視窗中，選取要從中匯入受信任網址清單的 JSON 檔案。

      2. 開啟檔案。

         如果電腦已經具有規則清單，則 Kaspersky Endpoint Security 將提示您刪除現有清單或從 JSON 檔案向其中新增新項目。

8. 儲存變更。

# 檢視系統完整性監控報告

若要分析系統完整性監控規則的效能，您可以查看應用程式產生的報告和事件。Kaspersky Endpoint Security 產生以下有關該元件的報告：

- 在應用程式介面中:
  - 系統完整性監控報告
  - 系統完整性檢查報告
  - 基線更新報告

  報告包含系統完整性監控事件。
- 在卡巴斯基安全管理中心主控台中：
  - 報告觸發監控規則次數最多的電腦
  - 報告最常觸發的監控規則

  預設情況下，會建立過去 30 天的報告，包括建立報告的日期。

  **如何在管理主控台 (MMC) 中檢視系統完整性監控報告**

  1. 開啟卡巴斯基安全管理中心管理主控台。
  2. 在管理主控台樹狀目錄的**管理伺服器**節點中選取"**報告**"標籤。
  3. 點擊"**新增報告範本**"。

     "新報告範本精靈"將啟動。
  4. 按照"報告範本精靈"的說明進行操作。在**選取報告範本類型**步驟，選擇系統完整性監控報告（**其他** 部分）：
     - **檔案完整性監控/系統完整性監控規則最常觸發的前 10 台裝置**
     - **在裝置上觸發頻率最高的檔案完整性監控器/系統完整性監控的前 10 條規則**

     完成新報告範本精靈之後，新報告範本將出現在"**報告**"標籤上。
  5. 點擊報告將其開啟。

  報告建立過程將開始。此報告將顯示在新視窗中。

  **如何在網頁主控台中檢視系統完整性監控報告**

  1. 在網頁主控台的主視窗中，選擇**監控和報告 → 報告**。
  2. 點擊"**新增**"。

     "新報告範本精靈"將啟動。

3. 在**範本類型**下面的**其他**部分中，選擇系統完整性監控報告：

   - **檔案完整性監控/系統完整性監控規則最常觸發的前 10 台裝置**
   - **在裝置上觸發頻率最高的檔案完整性監控器/系統完整性監控的前 10 條規則**

   完成新報告範本精靈之後，新報告範本將出現在表格中。

4. 選擇並執行報告。

   報告建立過程將開始。此報告將顯示在新視窗中。

若要檢視應用程式產生的事件，您也可以使用在卡巴斯基安全管理中心主控台中的事件分類。

# 系統完整性狀態重置

在卡巴斯基安全管理中心主控台中的電腦具有以下狀態之一：*確定*，*警告*或者*緊急*。如果系統完整性監控偵測到監控範圍內的檔案或登錄機碼被修改，則電腦的狀態變更為*警告* 或者 *緊急*。系統完整性監控分配的狀態稱為 *系統完整性狀態*。例如，如果分析使您確信偵測到的物件修改不會影響電腦的安全性，您可以重設系統完整性狀態。

**如何在管理主控台 (MMC) 中重置系統完整性狀態**

1. 在卡巴斯基安全管理中心管理主控台樹狀目錄中，選取**工作**。

   工作清單開啟。

2. 點擊**"新工作"**。

啟動"工作精靈"。按照精靈的說明進行操作。

步驟 1. 選取工作類型

選取"**Kaspersky Endpoint Security for Windows (12.12)**"→"**系統完整性狀態重設**"。

步驟 2. 選取將要對其分配工作的裝置

選取將要執行工作的電腦。下列選項可用：

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

步驟 3. 設定工作啟動排程

設定工作排程，例如手動。

步驟 4. 定義工作名稱

輸入工作名稱，例如 *修改監控範圍後重置狀態*。

步驟 5. 完成工作建立

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

**如何在網頁主控台中重設系統完整性狀態**

1. 在網頁主控台的主視窗中，選擇**資產（裝置）→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 Windows 12.12.0"**。
   b. 在**"工作類型"**下拉式清單中，選取**"系統完整性狀態重設"**。
   c. 在 **工作名稱** 欄位中，輸入簡短描述，例如，*修改監控範圍後重置狀態*。
   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。前往下一步。
5. 選取要執行工作的帳戶。預設情況下，Kaspersky Endpoint Security 將使用本機使用者帳戶的權限啟動工作。
6. 結束精靈。
   在工作清單中將顯示一個新工作。
7. 選中該工作旁邊的核取方塊。
8. 點擊**"開始"**。

結果，如果電腦的狀態因為系統完整性監控事件變更為 *警告* 或者 *緊急*，電腦的狀態重設為 *確定*。如果電腦的狀態也因其他事件而變更，則電腦的狀態保持不變。

# Cloud Discovery

Cloud Discovery 管理使用者對雲端服務的存取。雲端服務包括（舉例）Microsoft Teams、Salesforce、Microsoft Office 365。雲端服務按類別分組，例如*檔案共用*、*Messengers*、*電子郵件*。卡巴斯基專家定期更新 Cloud Discovery 類別和在類別中分類的雲端服務。Kaspersky Endpoint Security 會更新類別集合和包含應用程式資料庫的雲端服務。這意味著 Cloud Discovery 不使用卡巴斯基安全網路來分類雲端服務。

Cloud Discovery 提供以下功能：

- 監控雲端服務使用
- 封鎖使用者對雲端服務的存取

## 系統要求

如果以下條件得到滿足則 Cloud Discovery 可用：

- 應用程式安裝在執行工作站版本 Windows 的電腦上。

  該元件對於伺服器不可用。

- 卡巴斯基安全管理中心版本 15.1 或更高版本。

  此元件在管理主控台 (MMC) 中不可用。您可以在卡巴斯基安全管理中心網頁主控台或卡巴斯基安全管理中心雲端主控台中配置 Cloud Discovery。

- Kaspersky Next 產品授權。

啟用 Cloud Discovery 元件所需的應用程式功能：

1. **掃描加密連線**這對於 HTTPS 流量監控是必要的。您可以在 **網路設定** 部分中管理此功能。
2. **注入指令碼到網頁流量從而與網頁互動**指令碼將啟用 Cloud Discovery 事件的註冊。指令碼也提供對雲端服務存取的全面封鎖。如果沒有指令碼，應用程式將僅封鎖雲端服務網域的存取。您可以在 **網路設定** 部分中管理此功能。

您也可以啟用 **記錄允許頁面的開啟** 功能。該功能包括分組使用者造訪屬於同一個網域的網頁時的事件。這樣，當使用者使用雲端服務時，Cloud Discovery 將為每個網頁僅記錄一個而不是多個事件。您可以在 **Web 控制** 部分中管理此功能。

## 監控雲端服務

當使用者開始使用雲端服務時，Kaspersky Endpoint Security 將註冊該事件並在報告中建立一個項目。Cloud Discovery 可控制在瀏覽器以及相應應用程式中雲端服務的使用。Cloud Discovery 可控制透過 HTTP 和 HTTPS 的雲端服務使用。

**如何在 Cloud Console 中啟用雲端服務監控**

1. 在網頁主控台的主視窗中，選擇**資產（裝置）→政策和設定檔**。
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**"→"**Cloud Discovery**"。
5. 開啟"**Cloud Discovery 已啟用**"開關。
6. 儲存變更。

結果，應用程式會將有關正在使用的雲端服務的資訊轉寄到卡巴斯基安全管理中心。您可以在報告中檢視雲端服務使用情況。必要的話，您可以封鎖對雲端服務的存取。

## 封鎖對雲端服務的存取

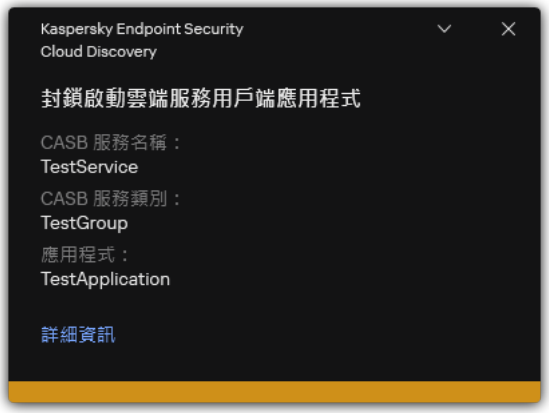
封鎖存取雲端服務僅適用於 Kaspersky Next EDR Optimum 和 XDR Expert 產品授權。此功能不適用於 Kaspersky Next EDR Foundations 產品授權。根據 Kaspersky Next 產品授權類型進行應用程式功能比較，請參見 Kaspersky Next 說明。

管理員可以限制使用者對 Cloud Discovery 類別或單個雲端服務的存取。通過這種方式，管理員可以僅允許安全的雲端服務並避免資料洩露。*風險等級資訊*會為 Cloud Discovery 中的每個雲端服務顯示。風險等級有助於偵測不滿足組織的安全要求的服務。

風險等級是估測，不暗示對雲端服務的品質或其供應商做出任何聲明。風險等級不過是卡巴斯基專家的建議。

雲端服務的風險等級顯示在所有受控制雲端服務的清單中政策的**Cloud Discovery**區域。

其他 Kaspersky Endpoint Security 元件可提供威脅防護和追蹤使用雲端服務時的可疑使用者活動。




Cloud Discovery 通知

Cloud Discovery 不會封鎖在 Kaspersky Endpoint Security 之前啟動的雲端應用程式。

### 如何在 Cloud Console 中封鎖存取雲端服務

1. 在網頁主控台的主視窗中，選擇**資產（裝置）→政策和設定檔**。
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**"→"**Cloud Discovery**"。
5. 開啟"**Cloud Discovery 已啟用**"開關。
   一個所有雲端服務的清單將得到顯示。雲端服務按類別分組，例如：*檔案共用*，*Messengers*，*電子郵件*。卡巴斯基專家定期更新 Cloud Discovery 類別和在類別中分類的雲端服務。Kaspersky Endpoint Security 會更新類別集合和包含應用程式資料庫的雲端服務。
6. 使用**存取**列中的開關來設定對雲端服務的存取。
7. 儲存變更。

結果，應用程式可控制在瀏覽器以及相應應用程式中雲端服務的使用。

# 應用程式掃描排除項目

*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。管理員還可以允許使用者為特定電腦建立自己的本機受信任區域。這樣，除了政策中的一般受信任區域之外，使用者還可以建立自己的"排除項目"和"受信任應用程式"的本機清單。

從 Kaspersky Endpoint Security 12.5 for Windows 開始，您可以 將 EDR 遙測資料新增至受信任區域。這可讓您最佳化應用程式傳送到 Kaspersky Anti Targeted Attack Platform (EDR) 解決方案的遙測資料收集伺服器的資料。

從 Kaspersky Endpoint Security 12.6 for Windows 開始，掃描排除項目和受信任應用程式被新增到受信任區域。預先定義的掃描排除項目和受信任應用程式有助於在 SQL 伺服器、Microsoft Exchange 伺服器和 System Center Configuration Manager 上快速設定 Kaspersky Endpoint Security。這意味著您無需在伺服器上為應用程式手動設定受信任區域。

從 Kaspersky Endpoint Security 12.8 for Windows 開始，您可以在 Light Agent 模式下安裝應用程式以防護虛擬環境。預定義掃描排除項目和受信任的應用程式可以幫助您在Citrix 和 VMware虛擬環境中快速設定 Kaspersky Endpoint Security。

# 建立掃描排除項目

"*掃描排除項目*"是一組條件，必須滿足這些條件，Kaspersky Endpoint Security 才不會掃描特定物件是否存在病毒和其他威脅。掃描排除項目可確保安全使用可能被入侵者用於損害電腦或使用者資料的合法軟體。儘管這類應用程式並不具備任何惡意功能，它們可能被入侵者利用。有關可被入侵者用來破壞電腦或個人資料的合法軟體的詳細資訊，請造訪 Kaspersky IT 百科全書網站。

這類應用程式可以被 Kaspersky Endpoint Security 封鎖。若要防止它們被封鎖，您可以為正在使用的應用程式排除掃描排除項目。為此，請將 Kaspersky IT 百科全書中列出的名稱或名稱遮罩新增到受信任區域。例如，您經常使用 Radmin 應用程式來遠端管理電腦。Kaspersky Endpoint Security 會將這些活動看做潛在危險並進行封鎖。若要防止應用程式被封鎖，請使用 Kaspersky IT 百科全書中列出的名稱或名稱遮罩建立掃描排除項目。

如果您電腦上安裝的某個應用程式收集資訊並將其傳送以供處理，則 Kaspersky Endpoint Security 可能會將其歸類為惡意軟體。若要避免此資訊，您可以按照文件所述透過配置 Kaspersky Endpoint Security 從掃描中排除此應用程式。

掃描排除項目可用於下列特定應用程式元件和系統管理員配置的工作：

- 行為偵測
- 弱點利用防禦
- 主機入侵防禦
- 檔案威脅防護
- Web 威脅防護

- 郵件威脅防護
- *惡意軟體掃描*工作

如果包含某個物件的磁碟或資料夾在掃描工作啟動時包括在掃描範圍中，則 Kaspersky Endpoint Security 將不對此物件進行掃描。但是，當啟動了針對該特殊物件的自訂掃描工作時，掃描排除項目將不應用。

管理主控台 (MMC) 和網頁主控台中受信任區域的分組方式不同。同樣，防止受信任區域參數變更的方式也不同（不同的"掛鎖"）。我們建議僅使用網頁主控台來管理應用程式。如果在不同主控台中配置受信任區域，管理外掛程式可能會將"掛鎖"重設為其預設狀態。

**如何在管理主控台 (MMC) 中建立掃描排除項目**

1. 在卡巴斯基安全管理中心管理主控台樹狀目錄中，選取**政策**。
2. 選擇必要的政策並點擊以開啟政策內容。
3. 在政策視窗中，選擇"**一般設定 → 排除項目和物件類型**"。
4. 在"**掃描排除項目和受信任應用程式 → 掃描排除項目**"塊中，點擊"**設定**"按鈕。

   這將開啟包含排除項目清單的視窗。
5. 如果要為公司內的所有電腦建立排除項目的綜合清單，請選取"**繼承時合併值**"核取方塊。將合併父政策和子政策中的排除項目清單。如果啟用繼承時合併值，則將合併清單。父政策中的排除項目以唯讀視圖的形式顯示在子政策中。無法變更或刪除父政策的排除項目。
6. 如果想要使用者能夠建立本機排除項目清單，請選中"**允許使用本機排除項目**"核取方塊。這樣，除了在政策中產生的排除項目的一般清單外，使用者还可以建立自己的排除項目本機清單。管理員可以使用卡巴斯基安全管理中心檢視、新增、編輯或刪除電腦屬性中的清單項目。

   如果核取方塊被清理，使用者只能存取政策中產生的排除項目的一般清單。此外，如果清除此核取方塊，Kaspersky Endpoint Security 會在應用程式的使用者介面中隱藏掃描排除項目的合併清單。
7. 點擊**新增** 並選擇一個操作：
   - **類別**您可以將掃描排除項目分組到不同的類別。若要建立新類別，請輸入類別名稱並在該類別中新增至少一個掃描排除項目。
   - **新排除項目**Kaspersky Endpoint Security 會將新的掃描排除項目新增至清單的根目錄。
   - **從清單中選取排除項目**為了在 SQL 伺服器、Microsoft Exchange 伺服器和 System Center Configuration Manager 上快速設定 Kaspersky Endpoint Security，應用程式包括*預定義的掃描排除項目*。另外還新增了預先定義的掃描排除項目，以支援 Citrix 和 VMware 虛擬環境中的應用程式安裝。您必須根據受防護伺服器的用途選擇預先定義的掃描排除項目。
   - **所選類別中新排除項目**若要將新的掃描排除項目新增至特定類別，請選擇一個類別。

8. 要從掃描中排除某個檔案或資料夾，請執行以下操作：




排除項目設定

a. 在“**內容**“塊中，選中“**檔案或資料夾**”核取方塊。

b. 點擊下面區塊中的連結以開啟 **檔案或資料夾名稱** 視窗。




選擇檔案或資料夾

a. 輸入檔案或資料夾名稱，或者檔案或資料夾名稱遮罩，或者點擊“**瀏覽**”選取資料夾樹狀目錄中的檔案或資料夾。

使用遮罩：

- `*`（星號）字元代表任意一組字元，但 `\` 和 `/` 字元除外（這兩個字元是檔案和資料夾路徑中的檔案和資料夾名稱的分隔符號）。例如，遮罩“`C:\*\*.txt`”將包括位於 C: 磁碟機但是不在子資料夾中所有帶 TXT 副檔名的檔案的路徑。

- 兩個連續 `*` 字元在檔案或資料夾名稱中代表任意一組字元（包括空集），包括 `\` 和 `/` 字元（這兩個字元是檔案和資料夾路徑中的檔案和資料夾名稱的分隔符號）。例如，遮罩 `C:\Folder\**\*.txt` 將包括位於巢嵌在 `Folder` 內的資料夾（`Folder`自身除外）中所有帶 TXT 副檔名的檔案的路徑。遮罩必須包含至少一個嵌套等級。遮罩 `C:\**\*.txt` 不是有效遮罩。

- `?`（問號）字元代表任意單個字元，但 `\` 和 `/` 字元除外（這兩個字元是檔案和資料夾路徑中的檔案和資料夾名稱的分隔符號）。例如，遮罩 `C:\Folder\???.txt` 將包括位於 `Folder` 資料夾中所有帶 TXT 副檔名且名稱由三個字元構成的檔案的路徑。

您可以在路徑的開始、中間或者結尾使用遮罩。例如，如果您想要將一個針對所有使用者的資料夾新增到排除項目，請輸入 `?:\Users\*\Folder\` 遮罩。

Kaspersky Endpoint Security 支援環境變數

您可以排除網路資料夾。為此，請手動輸入網路資料夾的路徑（例如，`\\Network Share\*`）。

當使用卡巴斯基安全管理中心主控台產生排除項目清單時，Kaspersky Endpoint Security 不支援“%userprofile%”環境變量。若要將項目套用到所有使用者帳戶，您可以使用 * 字元（例如，C:\Users*\Documents\File.exe）。無論何時新增新的環境變數，您都需要重啟應用程式。

b. 儲存變更。

9. 要從掃描中排除帶有指定名稱的物件，請執行以下操作：

a. 在“**內容**“塊中，選中“**偵測到的物件類型**”核取方塊。

b. 點擊下面區塊中的連結以開啟 **偵測到的物件類型** 視窗。




選擇項目

a. 根據 Kaspersky 百科全書的分類輸入物件的名稱（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 Kaspersky Endpoint Security 將從掃描中排除`Client-IRC`、`Client-P2P`和`Client-SMTP`物件。

b. 儲存變更。

10. 如果要從掃描中排除單個檔案，請：

a. 在“**內容**“塊中，選中“**物件雜湊**”核取方塊。

b. 點擊下面區塊中的連結以開啟 **物件雜湊** 視窗。




選擇檔案

a. 輸入檔案雜湊或點擊“**瀏覽**”按鈕選擇檔案。

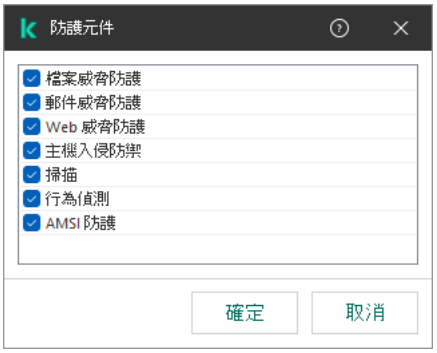
如果檔案被修改，檔案雜湊也將被修改。如果發生這種情況，修改後的檔案將不會新增到排除項目中。

b. 儲存變更。

11. 如有必要，在“**註解**”欄位，輸入您建立的掃描排除項目的簡要說明。

12. 指定應該使用掃描排除項目的 Kaspersky Endpoint Security 元件：

    a. 點擊下面區塊中的連結以開啟 **防護元件** 視窗。




選擇防護元件

    a. 選取必須應用掃描排除項目的元件旁的核取方塊。

    如果在掃描排除項目設定中指定了元件，則只有在 Kaspersky Endpoint Security 的這些元件掃描期間才會應用該排除項目。

    如果在掃描排除項目的設定中沒有指定元件，則在 Kaspersky Endpoint Security 的所有元件掃描期間都會套用該排除規則。

13. 點擊**"確定"**。

    新的排除項目將被新增到清單中。您可以使用物件旁邊的核取方塊隨時停用排除項目。

14. 儲存變更。

### 如何在網頁主控台和 Cloud Console 中掃描排除項目

1. 在網頁主控台的主視窗中，選擇**資產（裝置）→政策和設定檔**。
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**"惡意軟體掃描排除項目"**連接。
6. 如果要為公司內的所有電腦建立排除項目的綜合清單，請選取**"繼承時合併值"**核取方塊。將合併父政策和子政策中的排除項目清單。如果啟用繼承時合併值，則將合併清單。父政策中的排除項目以唯讀視圖的形式顯示在子政策中。無法變更或刪除父政策的排除項目。
7. 如果想要使用者能夠建立本機排除項目清單，請選中**"允許使用本機排除項目"**核取方塊。這樣，除了在政策中產生的排除項目的一般清單外，使用者还可以建立自己的排除項目本機清單。管理員可以使用卡巴斯基安全管理中心檢視、新增、編輯或刪除電腦屬性中的清單項目。

   如果核取方塊被清理，使用者只能存取政策中產生的排除項目的一般清單。此外，如果清除此核取方塊，Kaspersky Endpoint Security 會在應用程式的使用者介面中隱藏掃描排除項目的合併清單。

8. 點擊**新增** 並選擇一個操作：

   - **類別**您可以將掃描排除項目分組到不同的類別。若要建立新類別，請輸入類別名稱並在該類別中新增至少一個掃描排除項目。

   - **新排除項目**Kaspersky Endpoint Security 會將新的掃描排除項目新增至清單的根目錄。

   - **從清單中選取排除項目**為了在 SQL 伺服器、Microsoft Exchange 伺服器和 System Center Configuration Manager 上快速設定 Kaspersky Endpoint Security，應用程式包括*預定義的掃描排除項目*。另外還新增了預先定義的掃描排除項目，以支援 Citrix 和 VMware 虛擬環境中的應用程式安裝。您必須根據受防護伺服器的用途選擇預先定義的掃描排除項目。

   若要將新的掃描排除項目新增至特定類別，請選取該類別旁的核取方塊並選取**新排除項目**選項。

9. 選擇要如何新增排除項目：**檔案或資料夾路徑**、**物件類型**或**物件雜湊**。

10. 要從掃描中排除某個檔案或資料夾，請手動輸入路徑。Kaspersky Endpoint Security 輸入遮罩時支援環境變量以及`*`和`?`字元：

    - `*`（星號）字元代表任意一組字元，但`\`和`/`字元除外（這兩個字元是檔案和資料夾路徑中的檔案和資料夾名稱的分隔符號）。例如，遮罩"`C:\*\*.txt`"將包括位於 C: 磁碟機但是不在子資料夾中所有帶 TXT 副檔名的檔案的路徑。

    - 兩個連續`*`字元在檔案或資料夾名稱中代表任意一組字元（包括空集），包括`\`和`/`字元（這兩個字元是檔案和資料夾路徑中的檔案和資料夾名稱的分隔符號）。例如，遮罩`C:\Folder\**\*.txt`將包括位於巢嵌在`Folder`內的資料夾（`Folder`自身除外）中所有帶 TXT 副檔名的檔案的路徑。遮罩必須包含至少一個嵌套等級。遮罩`C:\**\*.txt`不是有效遮罩。

    - `?`（問號）字元代表任意單個字元，但`\`和`/`字元除外（這兩個字元是檔案和資料夾路徑中的檔案和資料夾名稱的分隔符號）。例如，遮罩`C:\Folder\???.txt`將包括位於`Folder`資料夾中所有帶 TXT 副檔名且名稱由三個字元構成的檔案的路徑。

      您可以在路徑的開始、中間或者結尾使用遮罩。例如，如果您想要將一個針對所有使用者的資料夾新增到排除項目，請輸入`?:\Users\*\Folder\`遮罩。

      您可以排除網路資料夾。為此，請手動輸入網路資料夾的路徑（例如，`\\Network Share\*`）。

11. 如果要從掃描中排除特定類型的物件，請在"**物件類型**"欄位中根據 Kaspersky 百科全書的分類輸入物件的名稱（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 Kaspersky Endpoint Security 將從掃描中排除`Client-IRC`、`Client-P2P`和`Client-SMTP`物件。

12. 如果要從掃描中排除單個檔案，請在"**物件雜湊**"欄位中輸入檔案雜湊。

    如果檔案被修改，檔案雜湊也將被修改。如果發生這種情況，修改後的檔案將不會新增到排除項目中。

13. 在"**套用排除項目到**"塊中，選擇要掃描排除項目套用的元件。

14. 如有必要，在"**註釋**"欄位，輸入您建立的掃描排除項目的簡要說明。

15. 點擊**OK**。

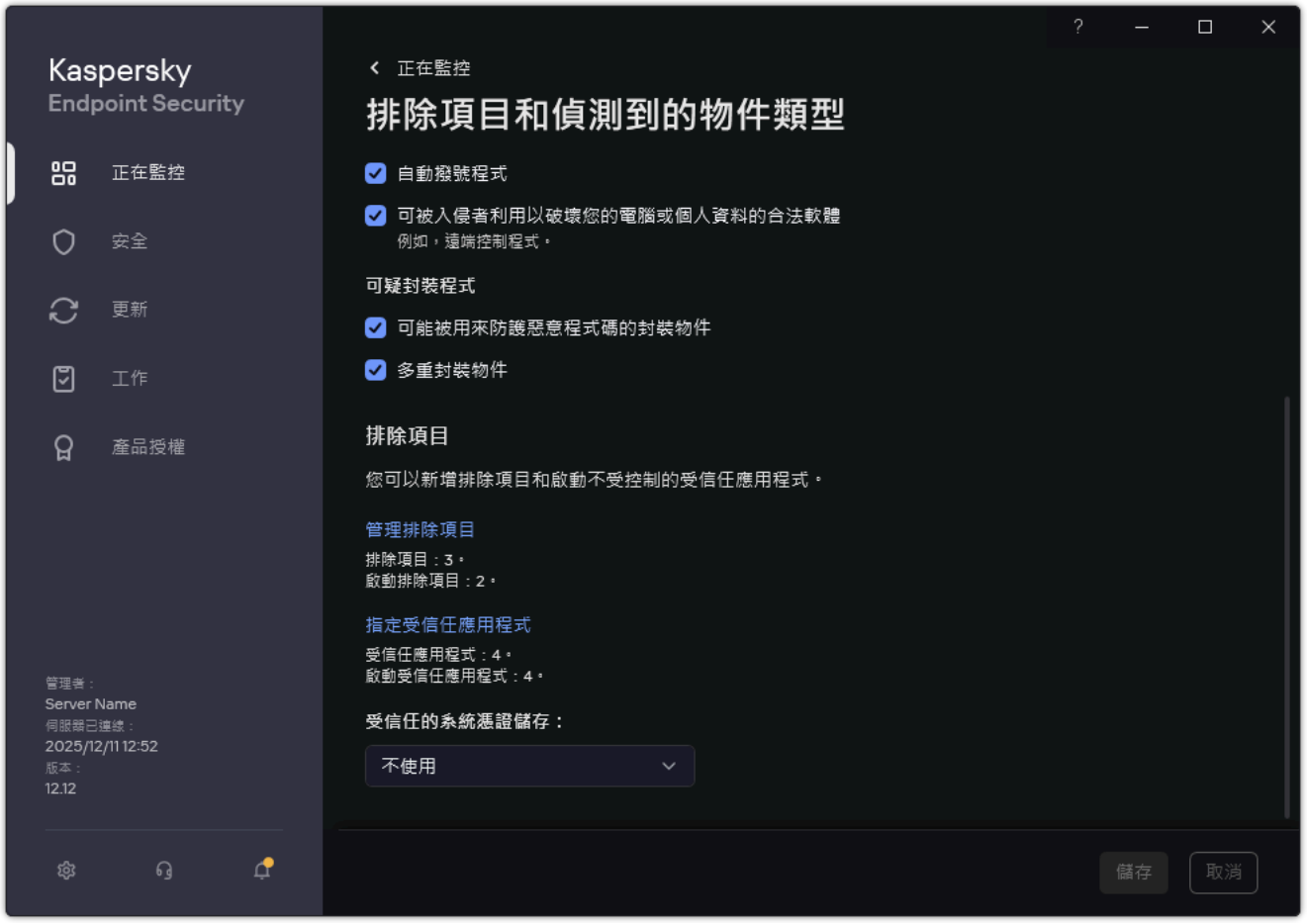
    新的排除項目將被新增到清單中。您可以隨時使用開關停止排除。

16. 儲存變更。

**如何在應用程式介面中建立掃描排除項目**

1. 在"應用程式主視窗"中，點擊⚙按鈕。
2. 在應用程式設定視窗中，選取"**一般設定**"→"**排除項目和偵測到的物件類型**"。
3. 在"**排除項目**"塊中，點擊"**管理排除項目**"連接。

如果管理員在主控台中封鎖可信任應用程式的配置（"關閉的鎖"符號）並且禁止本機可信任應用程式（**允許使用本機排除項目**核取方塊被清除），Kaspersky Endpoint Security 將在應用程式的使用者介面中隱藏掃描排除項目清單。




排除項目設定

4. 點擊**新增**並選擇一個操作：

   - **類別**您可以將掃描排除項目分組到不同的類別。若要建立新類別，請輸入類別名稱並在該類別中新增至少一個掃描排除項目。
   - **新排除項目**Kaspersky Endpoint Security 會將新的掃描排除項目新增至清單的根目錄。
   - **從清單中選取排除項目**為了在 SQL 伺服器、Microsoft Exchange 伺服器和 System Center Configuration Manager 上快速設定 Kaspersky Endpoint Security，應用程式包括*預定義的掃描排除項目*。另外還新增了預先定義的掃描排除項目，以支援 Citrix 和 VMware 虛擬環境中的應用程式安裝。您必須根據受防護伺服器的用途選擇預先定義的掃描排除項目。

   若要將新的掃描排除項目新增至特定類別，請選取該類別旁的核取方塊並選取**新排除項目**選項。

5. 如果要從掃描中排除某個檔案或資料夾，請點擊"**瀏覽**"按鈕選擇檔案或資料夾。

您也可以手動輸入路徑。Kaspersky Endpoint Security 輸入遮罩時支援環境變量以及`*`和`?`字元：

- `*`（星號）字元代表任意一組字元，但`\`和`/`字元除外（這兩個字元是檔案和資料夾路徑中的檔案和資料夾名稱的分隔符號）。例如，遮罩"`C:\*\*.txt`"將包括位於 C: 磁碟機但是不在子資料夾中所有帶 TXT 副檔名的檔案的路徑。

- 兩個連續`*`字元在檔案或資料夾名稱中代表任意一組字元（包括空集），包括`\`和`/`字元（這兩個字元是檔案和資料夾路徑中的檔案和資料夾名稱的分隔符號）。例如，遮罩`C:\Folder\**\*.txt`將包括位於巢嵌在`Folder`內的資料夾（`Folder`自身除外）中所有帶 TXT 副檔名的檔案的路徑。遮罩必須包含至少一個嵌套等級。遮罩`C:\**\*.txt`不是有效遮罩。

- `?`（問號）字元代表任意單個字元，但`\`和`/`字元除外（這兩個字元是檔案和資料夾路徑中的檔案和資料夾名稱的分隔符號）。例如，遮罩`C:\Folder\???.txt`將包括位於`Folder`資料夾中所有帶 TXT 副檔名且名稱由三個字元構成的檔案的路徑。

  您可以在路徑的開始、中間或者結尾使用遮罩。例如，如果您想要將一個針對所有使用者的資料夾新增到排除項目，請輸入`?:\Users\*\Folder\`遮罩。

  您可以排除網路資料夾。為此，請手動輸入網路資料夾的路徑（例如，`\\Network Share\*`）。

6. 如果要從掃描中排除特定類型的物件，請在"**偵測到的物件類型**"欄位中根據 Kaspersky 百科全書的分類輸入物件的名稱（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 Kaspersky Endpoint Security 將從掃描中排除`Client-IRC`、`Client-P2P`和`Client-SMTP`物件。

7. 如果要從掃描中排除單個檔案，請在"**物件雜湊**"欄位中輸入檔案雜湊。

   如果檔案被修改，檔案雜湊也將被修改。如果發生這種情況，修改後的檔案將不會新增到排除項目中。

8. 在"**防護元件**"塊中，選擇要掃描排除項目套用的元件。

9. 如有必要，在"**註釋**"欄位，輸入您建立的掃描排除項目的簡要說明。

10. 選擇排除項目的"**啟動**"狀態。

11. 點擊"**新增**"。

    新的排除項目將被新增到清單中。您可以隨時使用**狀態**列中的核取方塊停用排除項目。

12. 儲存變更。




排除項目清單

路徑遮罩示例：

我們建議指定相對路徑，而非絕對路徑。這不僅允許排除檔案系統物件，還允許排除無檔案物件。例如，`*\Program Files (x86)\Folder\Subfolder`。

位於任意資料夾的檔案的路徑：

- 遮罩 `*.exe` 將包括具有 exe 副檔名的檔案的所有路徑。
- 遮罩 `example*` 將包括名為 EXAMPLE 的檔案的所有路徑。

位於指定資料夾的檔案的路徑：

- 遮罩 `C:\dir\*.*` 將包括位於 `C:\dir\` 資料夾中的所有檔案的路徑，但不包括 `C:\dir\` 的子資料夾中的檔案的路徑。
- 遮罩 `C:\dir\*` 將包括位於 `C:\dir\` 資料夾（包括子資料夾）中的檔案的所有路徑。
- 遮罩 `C:\dir\` 將包括位於 `C:\dir\` 資料夾（包括子資料夾）中的檔案的所有路徑。
- 遮罩 `C:\dir\*.exe` 將包括位於 `C:\dir\` 資料夾中具有 EXE 副檔名的所有檔案的路徑，但不包括 `C:\dir\` 的子資料夾中的此類檔案的路徑。
- 遮罩 `C:\dir\test` 將包括位於 `C:\dir\` 資料夾中名為"test"的所有檔案的路徑，但不包括 `C:\dir\` 的子資料夾中的此類檔案的路徑。
- 遮罩 `C:\dir\*\test` 將包括位於 `C:\dir\` 資料夾及 `C:\dir\` 的子資料夾中名為"test"的所有檔案的路徑。
- 遮罩 `C:\dir1\*\dir3\` 將把 dir3 子資料夾一個級別中的所有檔案路徑包括在 `C:\dir1\` 資料夾中。
- 遮罩 `C:\dir1\**\dirN\` 將包括 `C:\dir1\` 資料夾中任何級別的 dirN 子資料夾中的所有檔案路徑。

位於所有資料夾中具有指定名稱的檔案的路徑：

- 遮罩 `dir\*.*` 將包括名為"dir"的資料夾中的所有檔案的路徑，但不包括這些資料夾的子資料夾中的檔案的路徑。
- 遮罩 `dir\*` 將包括名為"dir"的資料夾中的所有檔案的路徑，但不包括這些資料夾的子資料夾中的檔案的路徑。
- 遮罩 `dir\` 將包括名為"dir"的資料夾中的所有檔案的路徑，但不包括這些資料夾的子資料夾中的檔案的路徑。
- 遮罩 `dir\*.exe` 將包括名為"dir"的資料夾中具有 EXE 副檔名的所有檔案的路徑，但不包括這些資料夾的子資料夾中的此類檔案的路徑。
- 遮罩 `dir\test` 將包括名為"dir"的資料夾中名為"test"的所有檔案的路徑，但不包括這些資料夾的子資料夾中的此類檔案的路徑。

# 依偵測到的物件類型建立排除項目

Kaspersky Endpoint Security 將偵測到的物件按以下方式分類：

- **病毒和蠕蟲**

  **子分類**：病毒和蠕蟲 (Viruses_and_Worms)

  **危險等級**：高

  典型的病毒和蠕蟲會執行未經使用者授權的操作。它們會建立可自我複製的副本。

  **經典病毒**

  典型病毒侵入電腦後，會感染檔案，啟動並執行惡意操作，以及將自身的副本新增到其他檔案中。

典型病毒僅在電腦本機資源上複製副本，不會自行侵入其他電腦。僅當此病毒將其副本新增至儲存在共用資料夾或放入電腦中的 CD 中的檔案時，或者在使用者傳送附有受感染檔案的電子郵件訊息時，此病毒才會傳染給其他電腦。

典型病毒代碼可以入侵電腦、作業系統和應用程式的各種區域。根據具體的環境，病毒可分為*檔案病毒*、*引導磁區病毒*、*指令碼病毒*和*巨集病毒*。

病毒可以使用多種不同的技術來感染檔案。*Overwriting*病毒會使用其代碼覆蓋受感染檔案的代碼，從而抹除檔案的內容。感染的檔案會停止發揮作用，且無法還原。*Parasitic*病毒會修改檔案，從而使自身發揮全部或部分功能。*Companion*不會修改檔案，而是建立副本。當您開啟受感染的檔案時會啟動此檔案的副本（實際上是病毒）。您也會遇到以下類型的病毒：*Link病毒*、*OBJ 病毒*、*LIB 病毒*、*原始程式碼病毒*和許多其他病毒。

**蠕蟲**

與典型病毒一樣，蠕蟲在侵入電腦後，其代碼將啟動並執行惡意操作。之所以稱為蠕蟲，是因為它們能夠從一台電腦"爬"到另一台電腦，並不需使用者權限即可透過許多資料通道來傳播副本。

可用於區分各種類型蠕蟲的主要特徵是蠕蟲的傳播方式。下表提供了各種類型蠕蟲的概覽，這些蠕蟲按其傳播方式進行了分類。

蠕蟲傳播方式

| 類型 | 名稱 | 描述 |
|---|---|---|
| **電子郵件蠕蟲** | 電子郵件蠕蟲 | 這些蠕蟲透過電子郵件傳播。<br>受感染的電子郵件訊息包含帶有蠕蟲副本的附件，或指向上傳到可能已被攻擊或者專門建立用於傳播蠕蟲的網站上某檔案的連結。開啟此附件時，蠕蟲將被啟動。在您點擊此連結，進行下載，然後開啟檔案時，蠕蟲還會開始執行其惡意操作。之後，蠕蟲會繼續傳播其副本，搜尋其他電子郵件信箱，並向它們傳送受感染的郵件。 |
| **IM 蠕蟲** | 即時通訊用戶端蠕蟲 | 它們透過 IM 傳播。<br>通常，此類蠕蟲會利用使用者的連絡人清單傳送訊息，其中包含指向某網站上帶有蠕蟲副本的檔案的連結。使用者下載並開啟檔案時，蠕蟲將被啟動。 |
| **IRC 蠕蟲** | 網際網路聊天蠕蟲 | 這些蠕蟲會透過Internet Relay Chats（允許透過網際網路與其他人即時通信的服務系統）傳播。<br>這些蠕蟲會在網際網路聊天中發佈包含自身副本的檔案或指向此檔案的連結。使用者下載並開啟檔案時，蠕蟲將被啟動。 |
| **網路蠕蟲** | 網路蠕蟲 | 這些蠕蟲透過電腦網路傳播。<br>與其他類型的蠕蟲不同，典型的網路蠕蟲不需使用者參與即可傳播。它會掃描區域網路來尋找安裝了有弱點的程式的電腦。為此，它會傳送特殊格式的網路封包（弱點），其中包含蠕蟲代碼或部分蠕蟲代碼。如果網路上存在"有弱點"的電腦，此電腦會接收到此種網路封包。蠕蟲完全入侵電腦後，將被啟動。 |
| **P2P 蠕蟲** | 檔案共用網路蠕蟲 | 它們透過點對點檔案共用網路傳播。<br>為了滲透到 P2P 網路，蠕蟲會將自身複製到通常位於使用者電腦上的檔案共用資料夾中。P2P 網路會顯示有關此檔案的資訊，以便使用者可以在網路中像任何其他檔案一樣"找到"受感染的檔案，然後下載並開啟此檔案。<br>更加狡猾的蠕蟲會模仿特定 P2P 網路的網路協定：它們會返回對搜尋程式的積極回應，並提供自身的副本供下載。 |
| **蠕蟲** | 其他類型的蠕蟲 | 其他類型的蠕蟲包括：<br>• 透過網路資源傳播自身副本的蠕蟲。透過使用作業系統的功能，它們掃描可用的網路資料夾，連線到網際網路上的電腦，並嘗試獲取對磁碟機的完全存取。與之前描述的蠕蟲類型不同，其他類型的蠕蟲不會自行啟動，而是在使用者開啟包含蠕蟲副本的檔案時啟動。<br>• 不使用上表中所述的任何方式進行傳播的蠕蟲（例如，透過手機傳播的蠕蟲）。 |

- **木馬（包含勒索軟體）**

  **子類別**：木馬程式

  **危險等級**：高

  與蠕蟲和病毒不同，木馬不能進行自我複製。例如，使用者存取受感染的網頁時，它們會透過電子郵件或瀏覽器侵入電腦。木馬透過使用者參與而啟動。木馬啟動後即會開始執行惡意操作。

在受感染的電腦上，不同的木馬會表現出不同的行為。木馬的主要功能包括封鎖、修改或破壞資訊，以及停用電腦或網路。木馬還可以接收或傳送檔案，在螢幕上顯示訊息，請求網頁，下載和安裝程式，以及重新啟動電腦。

駭客通常使用各種不同木馬的"集合"。

下表中介紹了木馬行為的類型。

受感染電腦上木馬行為的類型

| 類型 | 名稱 | 描述 |
|---|---|---|
| **木馬炸彈** | 木馬 –"壓縮檔案炸彈" | 解壓縮時，這些壓縮檔案的大小會急劇增加，從而影響電腦的操作。<br>使用者嘗試解壓縮這種壓縮檔案時，電腦可能會執行緩慢或停止執行；硬碟可能會充滿"空白"資料。"壓縮檔案炸彈"對於檔案和郵件伺服器尤為危險。如果伺服器使用自動系統處理接收資訊，則"壓縮檔案炸彈"可能會中斷伺服器執行。 |
| **後門** | 用於遠端管理的木馬 | 此種木馬被視為最危險的木馬類型。在功能方面，這些木馬與安裝在電腦上的遠端管理應用程式相似。<br>這些程式會在不被使用者發覺的情況下將自身安裝到電腦上，以便入侵者遠端管理電腦。 |
| **木馬** | 木馬 | 木馬包括以下惡意應用程式：<br>• **典型木馬**。這些程式僅執行木馬的主要功能：封鎖、修改或破壞資訊，以及停用電腦或網路。它們沒有任何進階功能，與表中描述的其他類型的木馬不同。<br>• **萬能木馬**。這些程式具有多種典型木馬類型的進階功能。 |
| **勒索木馬** | 勒索木馬 | 這些木馬將使用者資訊作為"人質"，修改或封鎖資訊，或者影響電腦的操作，以使使用者無法使用資訊。入侵者向使用者進行勒索，許諾傳送應用程式來還原電腦的效能以及電腦上儲存的資料。 |
| **木馬點擊器** | 木馬點擊器 | 這些木馬透過自行向瀏覽器傳送指令或變更在作業系統檔案中指定的網址的方式，從使用者的電腦存取網頁。<br>透過使用這些程式，入侵者進行網路攻擊並提高網站存取量，從而增加條幅廣告的顯示次數。 |
| **木馬下載器** | 木馬下載器 | 這些木馬會存取入侵者的網頁，從中下載其他惡意應用程式，並將它們安裝到使用者的電腦。這些木馬包含要下載的惡意應用程式的檔案名稱，或從存取的網頁中接收此檔案名稱。 |
| **木馬釋放器** | 木馬釋放器 | 這些木馬包含安裝在硬碟磁碟機上並隨後進行安裝的其他木馬。<br>入侵者可能會使用木馬釋放器類型的程式來達到以下目的：<br>• 未通知使用者就安裝惡意應用程式：木馬釋放器類型的程式不會顯示訊息，或者會顯示虛假訊息，例如通知壓縮檔案中存在錯誤或作業系統的版本不相容。<br>• 防護另一個已知惡意應用程式不被偵測：並非所有病毒防護軟體都可偵測到木馬釋放器類型應用程式中的惡意應用程式。 |
| **通知型木馬** | 通知型木馬 | 這些木馬會通知入侵者受感染的電腦可供存取，並向入侵者傳送有關電腦的資訊：IP 位址、已開放埠號或電子郵件信箱。它們透過電子郵件、FTP、存取入侵者的網頁或以其他方式與入侵者聯絡。<br>通知型木馬類型的程式通常用於包含多種木馬的集合中。這些木馬會通知入侵者其他木馬已成功安裝到使用者的電腦。 |
| **代理型木馬** | 代理型木馬 | 這些木馬允許入侵者使用使用者的電腦匿名存取網頁，它們通常用於傳送垃圾郵件。 |
| **木馬 PSW** | 密碼竊盜軟體 | 密碼竊盜軟體是竊盜使用者帳戶（如軟體註冊資料）的一種木馬。這些密碼會尋找系統檔案和登錄檔中包含的機密資料，並透過電子郵件、FTP、存取入侵者的網頁或以其他方式將機密資料傳送給"攻擊者"。<br>部分這些木馬分類為此表中敘述的單獨類型。這些木馬會盜竊銀行帳戶（網銀竊賊木馬），竊取 IM 用戶端使用者的資料（IM 木馬），以及盜竊線上遊戲使用者的資訊（遊戲竊賊木馬）。 |
| **間諜木馬** | 間諜木馬 | 這些木馬暗中監視使用者，收集有關使用者使用電腦時所做的操作的資訊。它們可能會攔截使用者透過鍵盤輸入的資料，截取螢幕，或收集活動應用程式的清單。收到資訊後，這些木馬會透過電子郵件、FTP、存取入侵者的網頁或以其他方式將資訊傳輸給入侵者。 |
| **分散式拒絕服務攻擊木馬** | 木馬網路攻擊者 | 這些木馬會從使用者電腦將大量請求傳送至遠端伺服器。伺服器缺少資源來處理所有請求，因此會停止執行（拒絕服務，或簡稱為 DoS）。駭客通常會使用這些程式感染許多電腦，以使用這些電腦來同時攻擊一個伺服器。<br>DoS 程式在使用者知悉的情況下從一台電腦發起攻擊。DDoS（分散式 DoS）程式在不被受感染電腦使用者發覺的情況下從多台電腦發起分散式攻擊。 |
| **木馬 IM** | 從 IM 用戶端使用者那裡竊取資訊的木馬 | 它們會竊取 IM 用戶端使用者的帳戶和密碼。這些木馬會透過電子郵件、FTP、存取入侵者的網頁或以其他方式將資料傳輸給入侵者。 |
| **Rootkit** | Rootkits | 這些木馬會掩蓋其他惡意應用程式及其活動，從而延長這些應用程式在作業系統中持續存在的時間。它們還會隱藏檔案、受感染電腦記憶體中的處理程序或執行惡意應用程式的登錄機碼。Rootkit 會掩蓋使用者電腦上的應用程式與網路上其他電腦之間進行的資料交換。 |

| 類型 | 名稱 | 描述 |
| --- | --- | --- |
| **木馬 SMS** | SMS 格式的木馬 | 這些木馬會感染手機，向額外收費的手機號碼傳送 SMS。 |
| **遊戲竊賊木馬** | 從線上遊戲使用者那裡竊取資訊的木馬 | 這些木馬會竊取線上遊戲使用者的帳戶憑證，然後將這些憑證透過電子郵件、FTP、存取駭客的網頁或以其他方式傳送給駭客。 |
| **網銀竊賊木馬** | 竊取銀行帳戶的木馬 | 這些木馬會竊取銀行帳戶資料或電子貨幣系統資料，然後將這些資料透過電子郵件、FTP、存取駭客的網頁或以其他方式傳送給駭客。 |
| **郵件偵測木馬** | 收集電子郵件信箱的木馬 | 這些木馬會收集儲存在電腦上的電子郵件信箱，然後透過電子郵件、FTP、存取入侵者的網頁或以其他方式將它們傳送給入侵者。入侵者可能會向收集到的位址傳送垃圾郵件。 |

- **惡意工具**

  **子類別**：惡意工具

  **危險等級**：中

  與其他類型的惡意軟體不同，惡意工具在啟動過後不會執行其操作。惡意工具可以在使用者的電腦上安全地儲存和啟動。入侵者通常使用這些程式的功能來建立病毒、蠕蟲和木馬，對遠端伺服器進行網路入侵，攻擊電腦或執行其他惡意操作。

  惡意工具的各種功能按下表中所述的類型進行分組。

  惡意工具的功能

| 類型 | 名稱 | 描述 |
| --- | --- | --- |
| **構建器** | 構建器 | 透過它們可以建立新的病毒、蠕蟲和木馬。一些構建器揚言構建了基於視窗的標準介面，使用者可在此介面中選擇要建立的惡意應用程式的類型，對付偵錯工具的方式，以及其他功能。 |
| **拒絕服務攻擊** | 網路攻擊 | 這些木馬會從使用者電腦將大量請求傳送至遠端伺服器。伺服器缺少資源來處理所有請求，因此會停止執行（拒絕服務，或簡稱為 DoS）。 |
| **弱點利用** | 弱點 | *弱點*是一組資料或程式碼，利用處理它們的應用程式的缺陷對電腦執行惡意操作。例如，弱點可以寫入或讀取檔案，或請求"受感染"的網頁。<br>不同的弱點會利用不同應用程式或網路服務的缺陷。弱點會偽裝成網路封包透過網路傳輸到許多電腦，然後搜尋網路服務存在缺陷的電腦。DOC 檔案中的弱點會利用文字編輯器的缺陷。在使用者開啟受感染的檔案時，它可能會開始執行駭客程式設計的操作。嵌入在電子郵件訊息中的弱點會搜尋電子郵件用戶端的缺陷。使用者在電子郵件用戶端中開啟受感染的郵件時，弱點會立即開始執行惡意操作。<br>網路蠕蟲會使用弱點透過網路進行傳播。Nuker 弱點是可停用電腦的網路封包。 |
| **檔案加密器** | 加密器 | 加密器會加密其他惡意應用程式，以隱藏它們不被防毒應用程式發現。 |
| **洪水攻擊器** | 用於"污染"網路的程式 | 這些程式會透過網路通道傳送大量郵件。例如，此類型的工具包括污染網際網路中繼聊天的程式。<br>洪水攻擊器工具不包括"污染"電子郵件、IM 用戶端以及行動通信系統所使用通道的程式。這些程式可分為表中介紹的各種類型（電子郵件洪水攻擊器、IM 洪水攻擊器和 SMS 洪水攻擊器）。 |
| **駭客工具** | 駭客工具 | 這些工具可以破壞其所在的電腦，或攻擊其他電腦（例如，未經使用者許可新增新系統帳戶，或清除系統日誌以隱藏在作業系統中的存在路徑）。這種類型的工具包括一些具有惡意功能的嗅探器，例如密碼截取。嗅探器是允許檢視網路流量的程式。 |
| **惡作劇程式** | 惡作劇程式 | 這些程式會警告使用者類似病毒的訊息：它們可能會在未受感染的檔案中"偵測到病毒"，或通知使用者磁碟已被格式化，儘管這些情況實際並未發生。 |
| **位址欺騙程式** | 位址欺騙工具 | 這些工具使用偽造的寄件者位址傳送郵件和網路請求。例如，入侵者會使用位址欺騙程式類型的工具來掩蓋他們作為郵件實際寄件者的事實。 |
| **病毒修改工具** | 修改惡意應用程式的工具 | 透過這些工具可以修改其他惡意軟體，隱藏它們不被防毒程式發現。 |
| **電子郵件洪水攻擊器** | "污染"電子郵件信箱的程式 | 這些程式會向各種電子郵件信箱傳送大量郵件，從而"污染"這些位址。大量的接收郵件會妨礙使用者檢視收件箱中的有用郵件。 |

| 類型 | 名稱 | 描述 |
| --- | --- | --- |
| **IM 洪水攻擊器** | "污染"IM 流量的程式 | 它們向 IM 的使用者傳送大量訊息。大量的資訊會妨礙使用者檢視有用的接收資訊。 |
| **SMS 洪水攻擊器** | 使用 SMS"污染"流量的程式 | 這些程式向手機傳送大量 SMS。 |

- **廣告軟體**

  **子類別**：廣告軟體

  **危險等級**：中

  廣告軟體向使用者顯示廣告資訊。廣告軟體程式會在其他程式的介面中顯示條幅廣告，並將搜尋查詢重新導向至廣告網頁。某些廣告軟體程式會收集有關使用者的行銷資訊，並將其傳送給開發者：此資訊可能包括使用者存取的網站的名稱，或使用者搜尋查詢的內容。與間諜木馬類型的程式不同，廣告軟體程式會在使用者許可的情況下將此資訊傳送給開發者。

- **自動撥號程式**

  **子類別**：自動撥號器（Dialer）。

  **危險等級**：中

  自動撥號器可以使用資料機秘密地建立電話連線。

- **可被入侵者利用以破壞您的電腦或個人資料的合法軟體**

  **子類別**：可被入侵者利用以破壞您的電腦或個人資料的合法軟體。

  **危險等級**：中

  大多數這些應用程式都很有用，因此有許多使用者使用它們。這些應用程式包括 IRC 用戶端、自動撥號器、檔案下載程式、電腦系統活動監控器、密碼實用程式以及用於 FTP、HTTP 和 Telnet 的網際網路伺服器。

  但是，如果入侵者獲得了這些程式的存取權限，或如果他們在使用者的電腦上安置這些程式，應用程式的某些功能可能會被用來危害安全。

  這些應用程式具有不同的功能，下表介紹了它們的類型。

| 類型 | 名稱 | 描述 |
| --- | --- | --- |
| **Client-IRC** | 網際網路聊天用戶端 | 使用者安裝這些程式與他人進行網際網路中繼聊天。入侵者使用這些程式來傳播惡意軟體。 |
| **Downloader** | 用於下載的程式 | 這些程式可以在隱藏模式下從網頁下載檔案。 |
| **Monitor** | 用於監控的程式 | 這些程式可監控其安裝到的電腦上的活動（檢視哪些應用程式正在活動，以及它們如何與安裝在其他電腦上的應用程式交換資料）。 |
| **PSWTool** | 密碼還原器 | 透過它們可以檢視和還原已忘記的密碼。入侵者出於相同的目的，秘密地將它們安置在使用者的電腦上。 |
| **RemoteAdmin** | 遠端管理程式 | 系統管理員廣泛使用的一些程式。透過這些程式可以獲取對遠端電腦介面的存取權限，以監控和管理此電腦。入侵者出於同樣的目的，秘密地將它們安置在使用者的電腦上：用於監控和管理遠端電腦。<br>合法的遠端管理程式與實現遠端管理的後門類型的木馬不同。木馬能夠獨自入侵作業系統並自行安裝；合法的程式則無法做到這些。 |
| **Server-FTP** | FTP 伺服器 | 這些程式可起到 FTP 伺服器的作用。入侵者將它們安置在使用者電腦上，以開啟透過 FTP 對此電腦的遠端存取。 |
| **Server-Proxy** | 代理伺服器 | 這些程式可起到代理伺服器的作用。入侵者將它們安置在使用者電腦上，以使用者名義傳送垃圾郵件。 |

| 類型 | 名稱 | 描述 |
| --- | --- | --- |
| **Server-Telnet** | Telnet 伺服器 | 這些程式可起到 Telnet 伺服器的作用。入侵者將它們安置在使用者電腦上，以開啟透過 Telnet 對此電腦的遠端存取。 |
| **Server-Web** | Web 伺服器 | 這些程式可起到 Web 伺服器的作用。入侵者將它們安置在使用者電腦上，以開啟透過 HTTP 對此電腦的遠端存取。 |
| **RiskTool** | 在本機電腦上工作的工具 | 在使用者自己的電腦上工作時，這些工具會為使用者提供其他選項。透過這些工具，使用者可以隱藏檔案或活動應用程式的視窗，並終止活動的處理程序。 |
| **NetTool** | 網路工具 | 與網路上的其他電腦配合工作時，這些工具會為使用者提供其他選項。透過這些工具可以進行重新啟動，偵測開放的連接埠，以及啟動安裝在電腦上的應用程式。 |
| **Client-P2P** | P2P 網路用戶端 | 透過它們可以在對等網路中工作。入侵者可能會利用它們傳播惡意軟體。 |
| **Client-SMTP** | SMTP 用戶端 | 它們未經使用者的同意便傳送電子郵件。入侵者將它們安置在使用者電腦上，以使用者名義傳送垃圾郵件。 |
| **WebToolbar** | Web 工具列 | 它們會向其他應用程式的介面中新增工具列，以使用搜尋引擎。 |
| **FraudTool** | 欺騙程式 | 這些程式將自己偽裝為其他程式。例如，一些欺騙防毒程式會顯示有關惡意軟體偵測的資訊。但實際上，它們並未找到任何內容或進行解毒。 |

- **可能被用來防護惡意程式碼的封裝物件**

  **子類別**：可能造成損害的封裝檔案。

  **危險等級**：中。

  檔案使用特殊的封裝程式進行封裝，該封裝程式用於封裝惡意軟體：病毒、蠕蟲、木馬。Kaspersky Endpoint Security 會掃描 SFX（自解壓）存檔中的解壓縮工具模組。

  為了隱藏惡意軟體不被防毒軟體偵測到，駭客會使用特殊的封裝程式對其進行封裝。卡巴斯基專家已識別出駭客最常使用的解壓縮工具。

- **多重封裝物件**

  **子類別**：多重封裝檔案。

  **危險等級**：中。

  該檔案被一個或多個封裝程式封裝了 3 次或更多次。

  為了隱藏惡意軟體不被防毒軟體偵測到，駭客可能會多次封裝檔案。Kaspersky Endpoint Security 將掃描封裝的檔案。

預設情況下，Kaspersky Endpoint Security 會偵測所有物件類型。為了提高電腦的安全性，我們建議啟用偵測所有類型的物件。如果您使用的內部實用程式被應用程式偵測為惡意程式，將這些實用程式新增至排除清單，但不要停用對所有類型物件的偵測。

### 如何在管理主控台 (MMC) 中選擇可偵測物件的類型

1. 開啟卡巴斯基安全管理中心管理主控台。
2. 在主控台樹狀目錄中，選擇“**政策**”。
3. 選擇必要的政策並點擊以開啟政策內容。
4. 在政策視窗中，選擇“**一般設定 → 排除項目和物件類型**”。

5. 在"**偵測到的物件類型**"塊中，點擊"**設定**"按鈕。

6. 在開啟的視窗中，選取您想要 Kaspersky Endpoint Security 偵測的物件類型旁邊的核取方塊。

7. 儲存變更。若要在電腦上套用該政策，請關閉掛鎖。

**如何在網頁主控台和雲端主控台中選擇可偵測物件的類型**

1. 在網頁主控台的主視窗中，選擇**資產（裝置）→政策和設定檔**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**"→"**偵測設定**"。

5. 在"**偵測其他類型的物件**"塊中，請選取您想要 Kaspersky Endpoint Security 偵測威脅類型旁邊的核取方塊。

6. 儲存變更。若要在電腦上套用該政策，請關閉掛鎖。

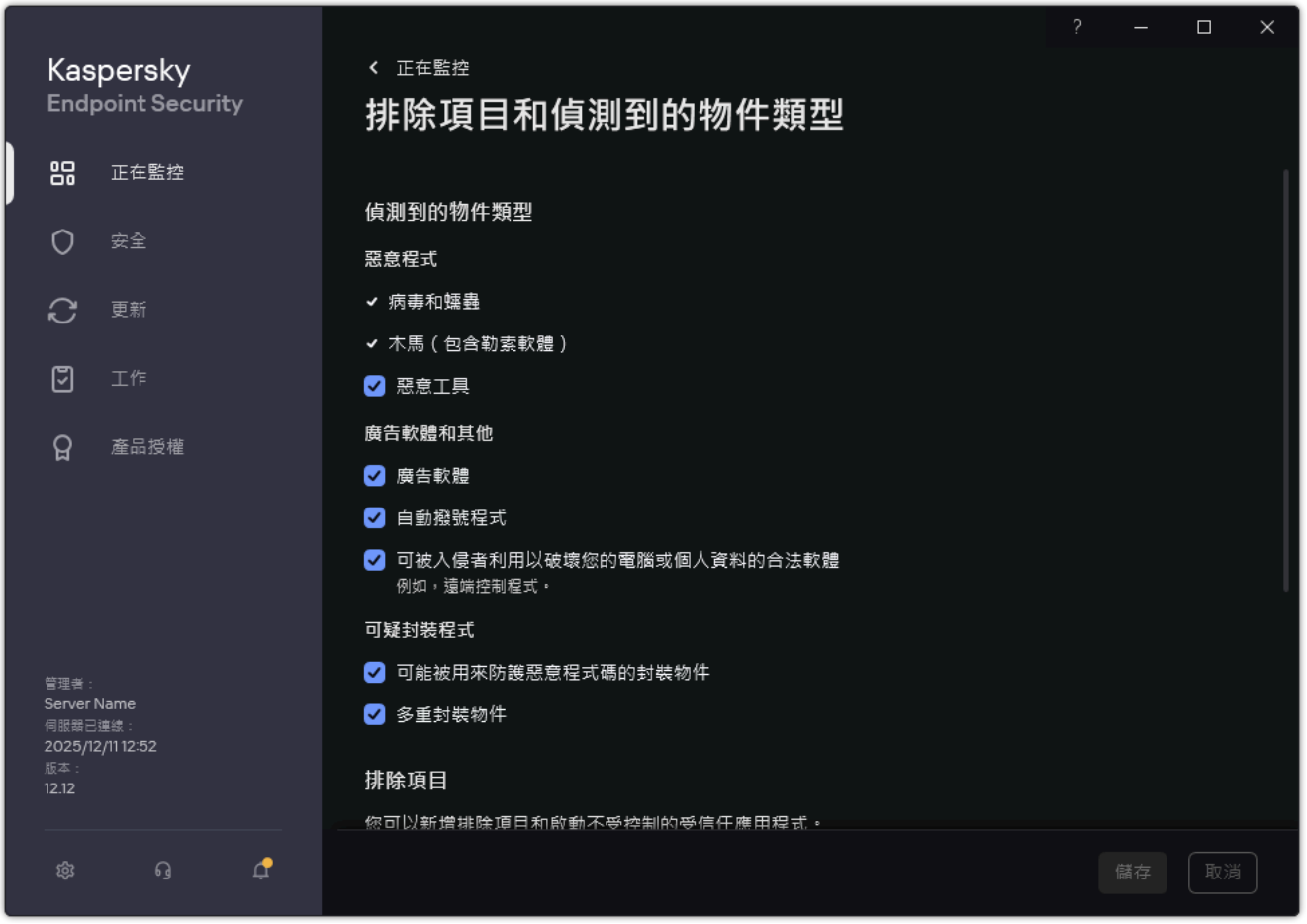
**如何在應用程式介面中選擇可偵測物件的類型**

1. 在"應用程式主視窗"中，點擊 按鈕。

2. 在應用程式設定視窗中，選取"**一般設定**"→"**排除項目和偵測到的物件類型**"。

3. 在“**偵測到的物件類型**“塊中，請選取您想要 Kaspersky Endpoint Security 偵測威脅類型旁邊的核取方塊。

4. 儲存變更。




可偵測物件的類型

# 編輯信任應用程式清單

*受信任應用程式清單*包含應用程式的檔案和網路活動（包括可疑活動）以及對系統登錄檔的存取不受 Kaspersky Endpoint Security 的監控。預設情況下，Kaspersky Endpoint Security 將監控任何應用程式處理程序開啟、執行或儲存的物件，並控制所有應用程式的活動及其產生的網路流量。應用程式被新增到受信任應用程式清單後，Kaspersky Endpoint Security 將停止監控該應用程式的活動。

掃描排除項目和受信任的應用程式之間的區別在於，對於排除項目，Kaspersky Endpoint Security 不掃描檔案，而對於受信任的應用程式，它不控制啟動的處理程序。如果受信任的應用程式在未包含在掃描排除項目中的資料夾中建立惡意檔案，Kaspersky Endpoint Security 將偵測該檔案並消除威脅。如果資料夾被新增到排除項目，Kaspersky Endpoint Security 將略過該檔案。

例如，如果您認為由標準 Microsoft Windows 記事本應用程式使用的物件是安全的，也即您信任此應用程式，則您可將 Microsoft Windows 記事本新增到受信任應用程式清單中，這樣該應用程式使用的物件就不會被監控。這會提高電腦效能，在使用伺服器應用程式時尤為重要。

此外，Kaspersky Endpoint Security 分類為危險的特定操作，在很多應用程式的功能環境中可能是安全的。例如，攔截鍵盤輸入的內容，是自動鍵盤設定切換器中的一種例行程式（例如 Punto Switcher）。考慮到此類程式的特點並將其行為從監控中排除，我們建議您可將此類程式新增到信任應用程式清單中。

受信任的應用程式有助於避免 Kaspersky Endpoint Security 與其他應用程式之間的相容性問題（例如，Kaspersky Endpoint Security 和另一個病毒防護應用程式對第三方電腦的網路流量進行雙重掃描的問題）。

同時，信任應用程式的可執行檔和處理程序仍然會掃描病毒和其他惡意軟體。您可以透過掃描排除項目將應用程式從 Kaspersky Endpoint Security 掃描中完全排除。

管理主控台 (MMC) 和網頁主控台中受信任區域的分組方式不同。同樣，防止受信任區域參數變更的方式也不同（不同的"掛鎖"）。我們建議僅使用網頁主控台來管理應用程式。如果在不同主控台中配置受信任區域，管理外掛程式可能會將"掛鎖"重設為其預設狀態。

**如何在管理主控台（MMC）中將應用程式新增到受信任清單中**

1. 在卡巴斯基安全管理中心管理主控台樹狀目錄中，選取**政策**。
2. 選擇必要的政策並點擊以開啟政策內容。
3. 在政策視窗中，選擇"**一般設定 → 排除項目和物件類型**"。
4. 在"**掃描排除項目和受信任應用程式 → 受信任應用程式**"塊中，點擊"**設定**"按鈕。

   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。如果啟用繼承時合併值，則將合併清單。父政策中的受信任應用程式以唯讀視圖的形式顯示在子政策中。無法變更或刪除父政策的受信任應用程式。
6. 如果想要使用者能夠建立本機受信任應用程式清單，請選中"**允許使用受信任應用程式**"核取方塊。這樣，除了在政策中產生的受信任應用程式的一般清單外，使用者还可以建立自己的受信任應用程式的本機清單。管理員可以使用卡巴斯基安全管理中心檢視、新增、編輯或刪除電腦屬性中的清單項目。

   如果核取方塊被清理，使用者只能存取政策中產生的受信任應用程式的一般清單。此外，如果清除此核取方塊，Kaspersky Endpoint Security 會在應用程式的使用者介面中隱藏受信任應用程式的合併清單。
7. 點擊**新增** 並選擇一個操作：

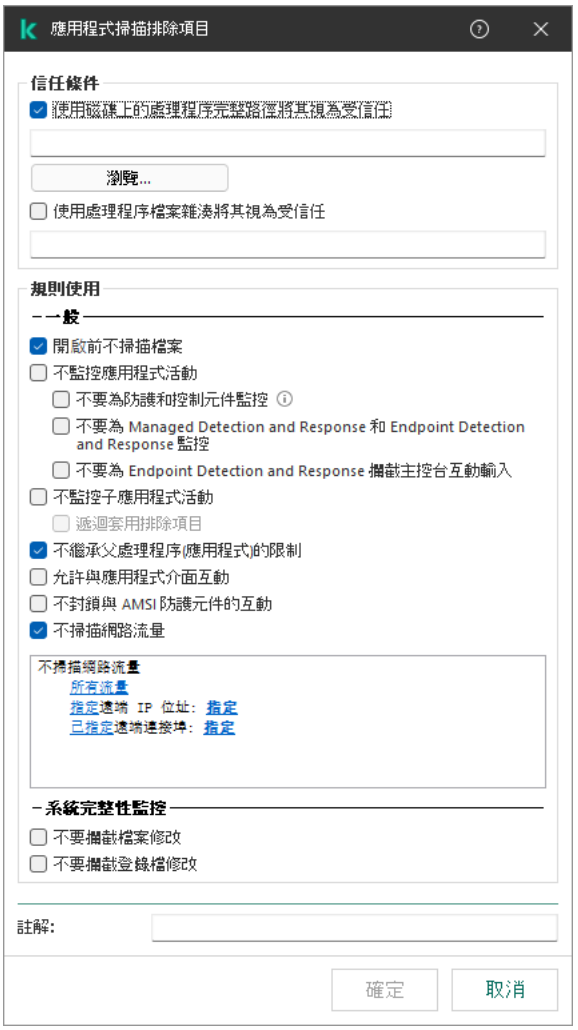
   - **類別**您可以將受信任的應用程式分為不同的類別。若要建立新類別，請輸入類別名稱並在該類別中新增至少一個受信任的應用程式。
   - **新排除項目**Kaspersky Endpoint Security 會將新的受信任應用程式新增至清單的根目錄。
   - **從清單中選取排除項目**為了在 SQL 伺服器、Microsoft Exchange 伺服器和 System Center Configuration Manager 上快速設定 Kaspersky Endpoint Security，應用程式包括*預定義的可信任應用程式*。另外還新增了預先定義的受信任應用程式，以支援 Citrix 和 VMware 虛擬環境中的應用程式安裝。您必須根據受防護伺服器的用途選擇預先定義的受信任應用程式。
   - **所選類別中新排除項目**若要將新的受信任應用程式新增至特定類別，請選擇一個類別。
8. 選擇信任標準：

   - **使用磁碟上的處理程序完整路徑將其視為受信任**輸入受信任應用程式的可執行檔的完整路徑。

     Kaspersky Endpoint Security 輸入遮罩時支援環境變量以及`*`和`?`字元。

     Kaspersky Endpoint Security 將受信任應用程式的檔案名稱視為區分大小寫。如果您輸入的檔案名稱大小寫錯誤，Kaspersky Endpoint Security 將無法辨識受信任的應用程式。
   - **使用處理程序檔案雜湊將其視為受信任**

當在卡巴斯基安全管理中心主控台上產生受信任應用程式清單時，Kaspersky Endpoint Security 不支援“%userprofile%”環境變量。若要將項目套用到所有使用者帳戶，您可以使用 * 字元（例如，C:\Users*\Documents\File.exe）。無論何時新增新的環境變數，您都需要重啟應用程式。




受信任應用程式設定

9. 為受信任應用程式配置進階設定（請參閱下表）。

10. 點擊**“確定”**。

    新的受信任應用程式將被新增到清單中。您可以隨時使用物件旁邊的核取方塊將應用程式從受信任區域中排除。

11. 儲存變更。




受信任應用程式清單

### 如何在管理主控台（MMC）和雲端主控台中將應用程式新增到受信任清單中

1. 在網頁主控台的主視窗中，選擇**資產（裝置）→政策和設定檔**。

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**"應用程式"**連接。

   這將開啟包含受信任應用程式清單的視窗。

6. 如果要為公司內的所有電腦建立受信任应用程式的綜合清單，請選取**"繼承時合併值"**核取方塊。將合併父政策和子政策中的受信任應用程式清單。如果啟用繼承時合併值，則將合併清單。父政策中的受信任應用程式以唯讀視圖的形式顯示在子政策中。無法變更或刪除父政策的受信任應用程式。

7. 如果想要使用者能夠建立本機受信任應用程式清單，請選中**"允許使用本機排除項目"**核取方塊。這樣，除了在政策中產生的受信任應用程式的一般清單外，使用者还可以建立自己的受信任應用程式的本機清單。管理員可以使用卡巴斯基安全管理中心檢視、新增、編輯或刪除電腦屬性中的清單項目。

   如果核取方塊被清理，使用者只能存取政策中產生的受信任應用程式的一般清單。此外，如果清除此核取方塊，Kaspersky Endpoint Security 會在應用程式的使用者介面中隱藏受信任應用程式的合併清單。

8. 點擊**新增** 並選擇一個操作：

   - **類別**您可以將受信任的應用程式分為不同的類別。若要建立新類別，請輸入類別名稱並在該類別中新增至少一個受信任的應用程式。
   - **新排除項目**Kaspersky Endpoint Security 會將新的受信任應用程式新增至清單的根目錄。
   - **從清單中選取排除項目**為了在 SQL 伺服器、Microsoft Exchange 伺服器和 System Center Configuration Manager 上快速設定 Kaspersky Endpoint Security，應用程式包括*預定義的可信任應用程式*。另外還新增了預先定義的受信任應用程式，以支援 Citrix 和 VMware 虛擬環境中的應用程式安裝。您必須根據受防護伺服器的用途選擇預先定義的受信任應用程式。

   若要將新的受信任應用程式新增至特定類別，請選取該類別旁的核取方塊並選取**新排除項目**選項。

9. 選擇信任標準：

   - **檔案或資料夾路徑**輸入受信任應用程式的可執行檔的完整路徑。

     Kaspersky Endpoint Security 輸入遮罩時支援環境變量以及`*`和`?`字元。

     Kaspersky Endpoint Security 將受信任應用程式的檔案名稱視為區分大小寫。如果您輸入的檔案名稱大小寫錯誤，Kaspersky Endpoint Security 將無法辨識受信任的應用程式。

   - **應用程式雜湊**

   當在卡巴斯基安全管理中心主控台中產生受信任應用程式清單時，Kaspersky Endpoint Security 不支援 "%userprofile%" 環境變量。若要將項目套用到所有使用者帳戶，您可以使用`*`字元（例如，`C:\Users\*\Documents\File.exe`）。無論何時新增新的環境變數，您都需要重啟應用程式。

10. 為受信任應用程式配置進階設定（請參閱下表）。

11. 點擊**"確定"**。

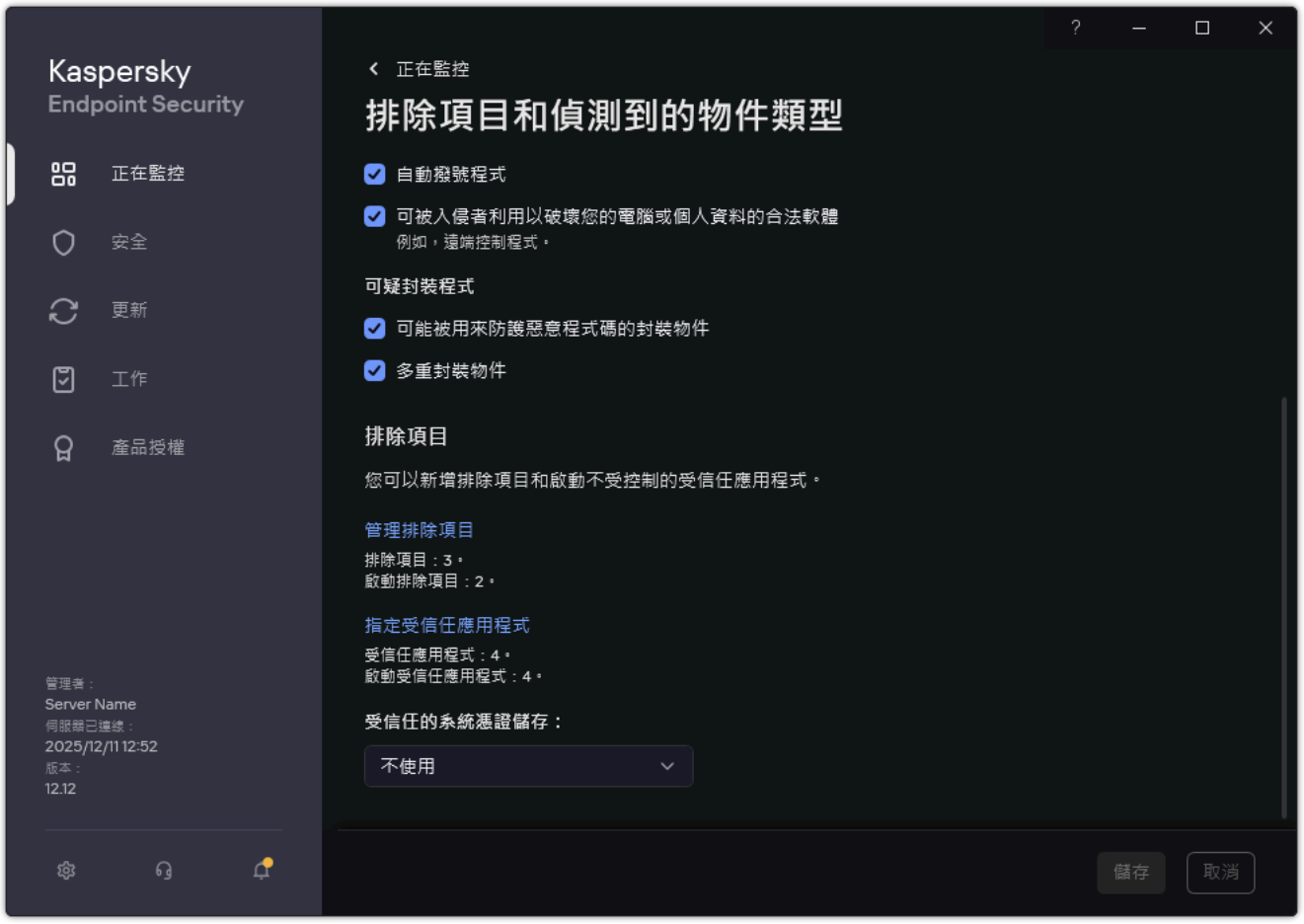
    新的受信任應用程式將被新增到清單中。您可以隨時使用**狀態**列中的核取方塊將應用程式排除在受信任區域之外。

12. 儲存變更。

**如何在應用程式介面中將應用程式新增到受信任清單中**

1. 在"應用程式主視窗"中，點擊⚙按鈕。
2. 在應用程式設定視窗中，選取**"一般設定"→"排除項目和偵測到的物件類型"**。
3. 在**"排除項目"**塊中，點擊**"指定受信任應用程式"**連接。

如果管理員在主控台中封鎖可信任應用程式的配置（“關閉的鎖”符號）並且禁止本機可信任應用程式（**允許使用受信任應用程式**核取方塊被清除）。




排除項目設定

4. 點擊**新增**並選擇一個操作：

- **類別**您可以將受信任的應用程式分為不同的類別。若要建立新類別，請輸入類別名稱並在該類別中新增至少一個受信任的應用程式。
- **新排除項目**Kaspersky Endpoint Security 會將新的受信任應用程式新增至清單的根目錄。
- **從清單中選取排除項目**為了在 SQL 伺服器、Microsoft Exchange 伺服器和 System Center Configuration Manager 上快速設定 Kaspersky Endpoint Security，應用程式包括*預定義的可信任應用程式*。另外還新增了預先定義的受信任應用程式，以支援 Citrix 和 VMware 虛擬環境中的應用程式安裝。您必須根據受防護伺服器的用途選擇預先定義的受信任應用程式。

若要將新的受信任應用程式新增至特定類別，請選取該類別旁的核取方塊並選取**新排除項目**選項。

5. 選擇信任標準：

- **使用磁碟上的完整處理程序路徑來將它視為受信任**輸入受信任應用程式的可執行檔的完整路徑。

  Kaspersky Endpoint Security 輸入遮罩時支援環境變量以及`*`和`?`字元。

  Kaspersky Endpoint Security 將受信任應用程式的檔案名稱視為區分大小寫。如果您輸入的檔案名稱大小寫錯誤，Kaspersky Endpoint Security 將無法辨識受信任的應用程式。

- **使用處理程序檔案雜湊將其視為受信任**

Kaspersky Endpoint Security 可支援環境變數並轉換應用程式本機介面中的路徑。換言之，如果您輸入檔案路徑 `%userprofile%\Documents\File.exe`，將為使用者 Fred123 在應用程式的本機介面中新增 `C:\Users\Fred123\Documents\File.exe` 記錄。因此，Kaspersky Endpoint Security 會忽略針對其他使用者的 `File.exe` 受信任程式。若要將項目套用到所有使用者帳戶，您可以使用 `*` 字元（例如，`C:\Users\*\Documents\File.exe`）。無論何時新增新的環境變數，您都需要重啟應用程式。

6. 在"受信任應用程式屬性"視窗中，配置進階設定。

7. 點擊**"確定"**。

   新的受信任應用程式將被新增到清單中。您可以隨時使用**狀態**列中的核取方塊將應用程式排除在受信任區域之外。

8. 儲存變更。




受信任應用程式清單

受信任應用程式設定

| 參數 | 描述 |
| --- | --- |
| **開啟前不掃描檔案** | Kaspersky Endpoint Security 的掃描將排除應用程式開啟的所有檔案。例如，如果您正在使用應用程式備份檔案，則此功能有助於減少 Kaspersky Endpoint Security 的資源消耗。 |
| **不監控應用程式活動** | Kaspersky Endpoint Security 將不會監控作業系統中應用程式的檔案和網路活動。您可以為 Kaspersky Endpoint Security 的不同元件設定應用程式活動監控：<br>• **不要為防護和控制元件監控**應用程式活動由以下元件監控：行為偵測，弱點利用防禦，主機入侵防禦，修復引擎和防火牆。<br>• **不要為 Managed Detection and Response 和 Endpoint Detection and Response 監控**應用程式活動由內建 MDR 代理 和 內建 EDR (KATA) 代理監控。<br>• **不要為 Endpoint Detection and Response 攔截主控台互動輸入**Kaspersky Endpoint Security 不會傳送有關在主控台上管理應用程式的遙測資料。遙測資料由 Kaspersky Anti Targeted Attack Platform (EDR) 使用。 |
| **不監控子應用程式活動** | Kaspersky Endpoint Security 將不會監控該應用程式啟動的應用程式的檔案活動或網路活動。您可以遞歸套用排除項目。這樣應用程式就不會監視整個子應用程式鏈的活動。 |

| 參數 | 描述 |
| --- | --- |
| **不繼承父處理程序(應用程式)的限制** | Kaspersky Endpoint Security 不會將為父程序配置的限制套用於子程序。父程序由配置了應用程式權限（主機入侵防禦）和應用程式網路規則（防火牆）的應用程式啟動。 |
| **不監控子應用程式活動** | Kaspersky Endpoint Security 將不會監控該應用程式啟動的應用程式的檔案活動或網路活動。您可以遞歸套用排除項目。這樣應用程式就不會監視整個子應用程式鏈的活動。 |
| **允許與應用程式介面互動** | Kaspersky Endpoint Security 自我防護可封鎖從遠端電腦管理應用程式服務的所有嘗試。如果選擇該核取方塊，則允許遠端存取應用程式透過 Kaspersky Endpoint Security 介面管理 Kaspersky Endpoint Security 設定。 |
| **不封鎖與 AMSI 防護元件的互動** | Kaspersky Endpoint Security 將不會監控受信任應用程式對AMSI 防護元件要掃描的物件的請求。 |
| **不掃描網路流量** | Kaspersky Endpoint Security 將從掃描中排除由應用程式啟動的網路流量。您可以從掃描中排除所有流量或僅排除加密流量。您也可以從掃描中排除單個 IP 位址和連接埠號。 |
| **不要攔截檔案修改**<br>*（僅在卡巴斯基安全管理中心主控台中可用）* | Kaspersky Endpoint Security 不會監控來自 系統完整性監控 監測範圍的檔案中的變更。該應用程式會將排除項目套用於所有系統完整性監控模式： 即時系統完整性監控 和 按需系統完整性檢查。 |
| **不要攔截登錄檔修改**<br>*（僅在卡巴斯基安全管理中心主控台中可用）* | Kaspersky Endpoint Security 不會監控來自 系統完整性監控 監測範圍的登錄機碼中的變更。該應用程式會將排除項目套用於所有系統完整性監控模式： 即時系統完整性監控 和 按需系統完整性檢查。 |
| **註釋** | 如有必要，您可以為受信任應用程式提供簡短註解。註解有助於簡化對受信任應用程式的搜尋和排序。 |
| **狀態** | 受信任應用程式的狀態：<br>• **啟動** 狀態表示應用程式在受信任區域中。<br>• **未啟動** 狀態表示應用程式被從受信任區域中排除。 |

# 建立本機信任區域

使用者現在可以為特定電腦建立自己的本機信任區域。這樣，除了政策中的一般受信任區域之外，使用者還可以建立自己的"掃描排除項目"和"受信任應用程式"的本機清單。管理員可以在政策設定中允許或封鎖使用本機排除項目或本機受信任的應用程式。為此，請使用政策的 **允許使用本機排除項目** 和 **允許使用受信任應用程式** 中的核取方塊 **排除項目** 區域。

如果管理員允許建立本機信任區域，則使用者可以在應用程式的使用者介面中新增自己的掃描排除項目和可信應用程式。同時，使用者無權修改或刪除政策中配置的信任區域中的物件。如果需要為單台電腦新增排除項目，管理員還可以在卡巴斯基安全管理中心主控台中查看、新增、修改或刪除清單項目。

如果管理員在主控台中封鎖可信任區域的配置（"關閉的鎖"符號）並且禁止本機掃描排除項目和受信任應用程式，Kaspersky Endpoint Security 將在應用程式的使用者介面中隱藏掃描排除項目和受信任應用程式清單。

### 如何在管理主控台（MMC）中將物件新增到本機信任區域中

1. 開啟卡巴斯基安全管理中心管理主控台。
2. 在管理主控台樹狀目錄的"**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"**裝置**"標籤。
4. 點擊以開啟電腦內容視窗。
5. 在電腦內容視窗中，選取"**應用程式**"區域。
6. 在電腦上安裝的 Kaspersky 應用程式清單中，選取 **Kaspersky Endpoint Security for Windows (12.12)** 並點擊以開啟應用程式內容。

7. 在應用程式設定視窗中，選取"**一般設定**"→"**排除項目和物件類型**"。

8. 在"**掃描排除項目和受信任應用程式 → 本機掃描排除項目**"塊中，點擊"**設定**"按鈕。

   這將開啟包含本機排除項目清單的視窗。




受信任區域設定

9. 製作本機掃描排除項目清單。

   建立本機掃描排除項目的規則與一般排除項目的規則相同。Kaspersky Endpoint Security 輸入遮罩時支援環境變量以及 * 和 ? 字元。

10. 在"**掃描排除項目和受信任應用程式 → 本機受信任應用程式**"塊中，點擊"**設定**"按鈕。

    這將開啟包含本機受信任應用程式清單的視窗。

11. 製作本機受信任應用程式清單。

    新增應用程式到本機可信應用程式清單的規則與將它們新增到一般清單的規則相同。Kaspersky Endpoint Security 輸入遮罩時支援環境變量以及 * 和 ? 字元。

12. 儲存變更。

**如何在管理主控台（MMC）和雲端主控台中將物件新增到本機信任區域中**

1. 在網頁主控台的主視窗中，選擇**資產（裝置）→ 受管理裝置**。

2. 點擊您想要允許使用者在上面執行被封鎖操作的電腦的名稱。

3. 選擇"**應用程式**"標籤。

4. 點擊"**Kaspersky Endpoint Security for Windows**"。

   這將開啟本機應用程式設定。

5. 選擇“**應用程式設定**”標籤。

6. 在應用程式設定視窗中，選取”**一般設定**“→“**排除項目和偵測到的物件類型**”。

7. 在”**掃描排除項目和受信任應用程式**”塊中，點擊”**本機掃描排除項目**”連接。

8. 製作本機掃描排除項目清單。

   建立本機排除項目的規則與建立一般排除項目的規則相同。Kaspersky Endpoint Security 輸入遮罩時支援環境變量以及 * 和 ? 字元。

9. 在”**掃描排除項目和受信任應用程式**”塊中，點擊”**本機受信任應用程式**”連接。

10. 製作本機受信任應用程式清單。

    新增應用程式到本機可信應用程式清單的規則與將它們新增到一般清單的規則相同。Kaspersky Endpoint Security 輸入遮罩時支援環境變量以及 * 和 ? 字元。

11. 儲存變更。

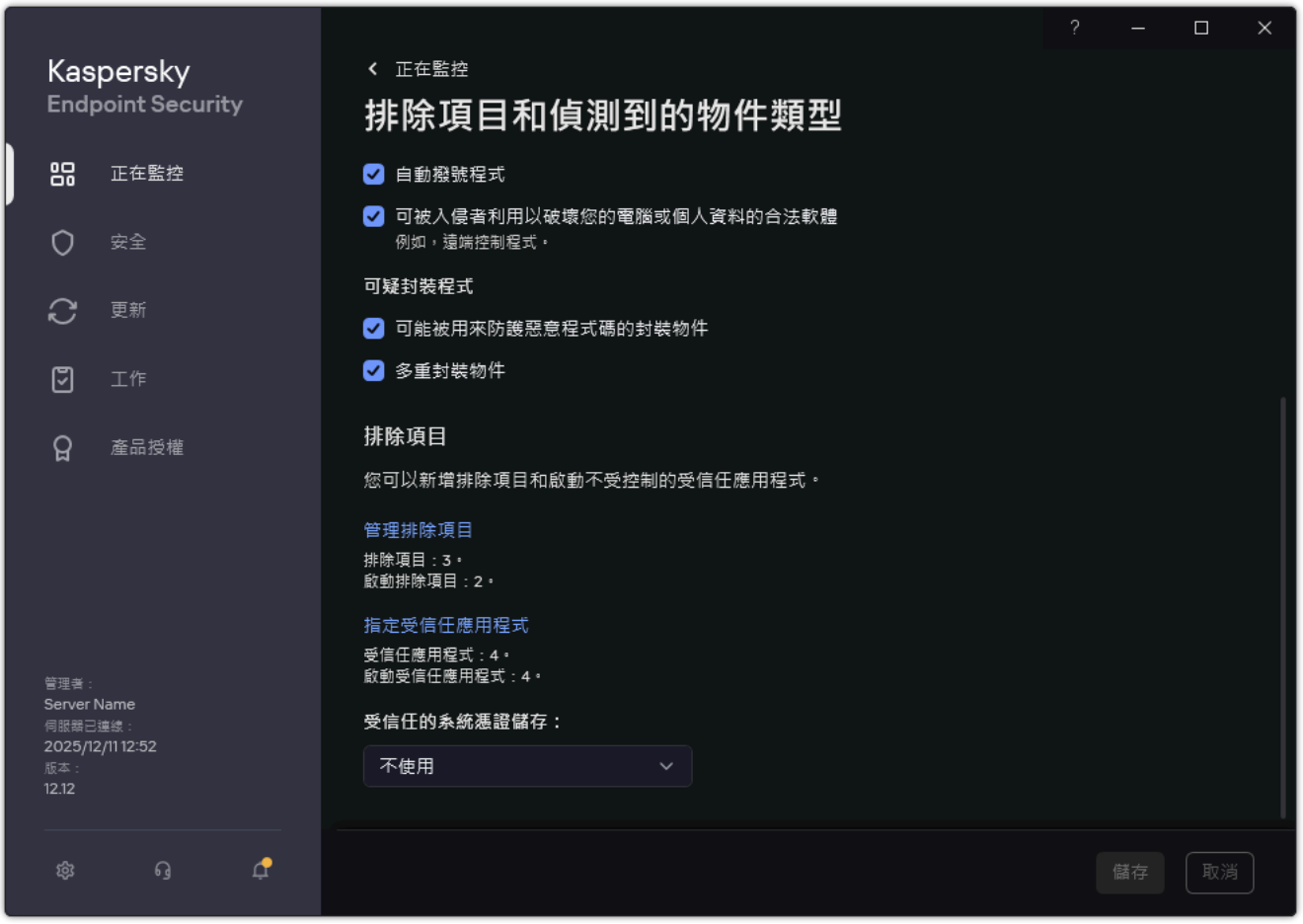
**如何在應用程式介面中建立本機掃描排除項目**

1. 在“應用程式主視窗”中，點擊⚙ 按鈕。

2. 在應用程式設定視窗中，選取”**一般設定**“→“**排除項目和偵測到的物件類型**”。

3. 在”**排除項目**”塊中，點擊”**管理排除項目**”連接。

如果管理員在主控台中封鎖可信任應用程式的配置（“關閉的鎖”符號）並且禁止本機可信任應用程式（**允許使用本機排除項目**核取方塊被清除），Kaspersky Endpoint Security 將在應用程式的使用者介面中隱藏掃描排除項目清單。




排除項目設定

4. 點擊**新增**並選擇一個操作：

   - **類別**您可以將掃描排除項目分組到不同的類別。若要建立新類別，請輸入類別名稱並在該類別中新增至少一個掃描排除項目。
   - **新排除項目**Kaspersky Endpoint Security 會將新的掃描排除項目新增至清單的根目錄。
   - **從清單中選取排除項目**為了在 SQL 伺服器、Microsoft Exchange 伺服器和 System Center Configuration Manager 上快速設定 Kaspersky Endpoint Security，應用程式包括*預定義的掃描排除項目*。另外還新增了預先定義的掃描排除項目，以支援 Citrix 和 VMware 虛擬環境中的應用程式安裝。您必須根據受防護伺服器的用途選擇預先定義的掃描排除項目。

   若要將新的掃描排除項目新增至特定類別，請選取該類別旁的核取方塊並選取**新排除項目**選項。

5. 如果要從掃描中排除某個檔案或資料夾，請點擊**“瀏覽”**按鈕選擇檔案或資料夾。

您也可以手動輸入路徑。Kaspersky Endpoint Security 輸入遮罩時支援環境變量以及`*`和`?`字元：

- `*`（星號）字元代表任意一組字元，但`\`和`/`字元除外（這兩個字元是檔案和資料夾路徑中的檔案和資料夾名稱的分隔符號）。例如，遮罩"`C:\*\*.txt`"將包括位於 C: 磁碟機但是不在子資料夾中所有帶 TXT 副檔名的檔案的路徑。

- 兩個連續`*`字元在檔案或資料夾名稱中代表任意一組字元（包括空集），包括`\`和`/`字元（這兩個字元是檔案和資料夾路徑中的檔案和資料夾名稱的分隔符號）。例如，遮罩`C:\Folder\**\*.txt`將包括位於巢嵌在`Folder`內的資料夾（`Folder`自身除外）中所有帶 TXT 副檔名的檔案的路徑。遮罩必須包含至少一個嵌套等級。遮罩`C:\**\*.txt`不是有效遮罩。

- `?`（問號）字元代表任意單個字元，但`\`和`/`字元除外（這兩個字元是檔案和資料夾路徑中的檔案和資料夾名稱的分隔符號）。例如，遮罩`C:\Folder\???.txt`將包括位於`Folder`資料夾中所有帶 TXT 副檔名且名稱由三個字元構成的檔案的路徑。

  您可以在路徑的開始、中間或者結尾使用遮罩。例如，如果您想要將一個針對所有使用者的資料夾新增到排除項目，請輸入`?:\Users\*\Folder\`遮罩。

  您可以排除網路資料夾。為此，請手動輸入網路資料夾的路徑（例如，`\\Network Share\*`）。

6. 如果要從掃描中排除特定類型的物件，請在"**偵測到的物件類型**"欄位中根據 Kaspersky 百科全書的分類輸入物件的名稱（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 Kaspersky Endpoint Security 將從掃描中排除`Client-IRC`、`Client-P2P`和`Client-SMTP`物件。

7. 如果要從掃描中排除單個檔案，請在"**物件雜湊**"欄位中輸入檔案雜湊。

   如果檔案被修改，檔案雜湊也將被修改。如果發生這種情況，修改後的檔案將不會新增到排除項目中。

8. 在"**防護元件**"塊中，選擇要掃描排除項目套用的元件。

9. 如有必要，在"**註釋**"欄位，輸入您建立的掃描排除項目的簡要說明。

10. 選擇排除項目的"**啟動**"狀態。

11. 點擊"**新增**"。

    新的排除項目將被新增到清單中。您可以隨時使用**狀態**列中的核取方塊停用排除項目。

12. 儲存變更。

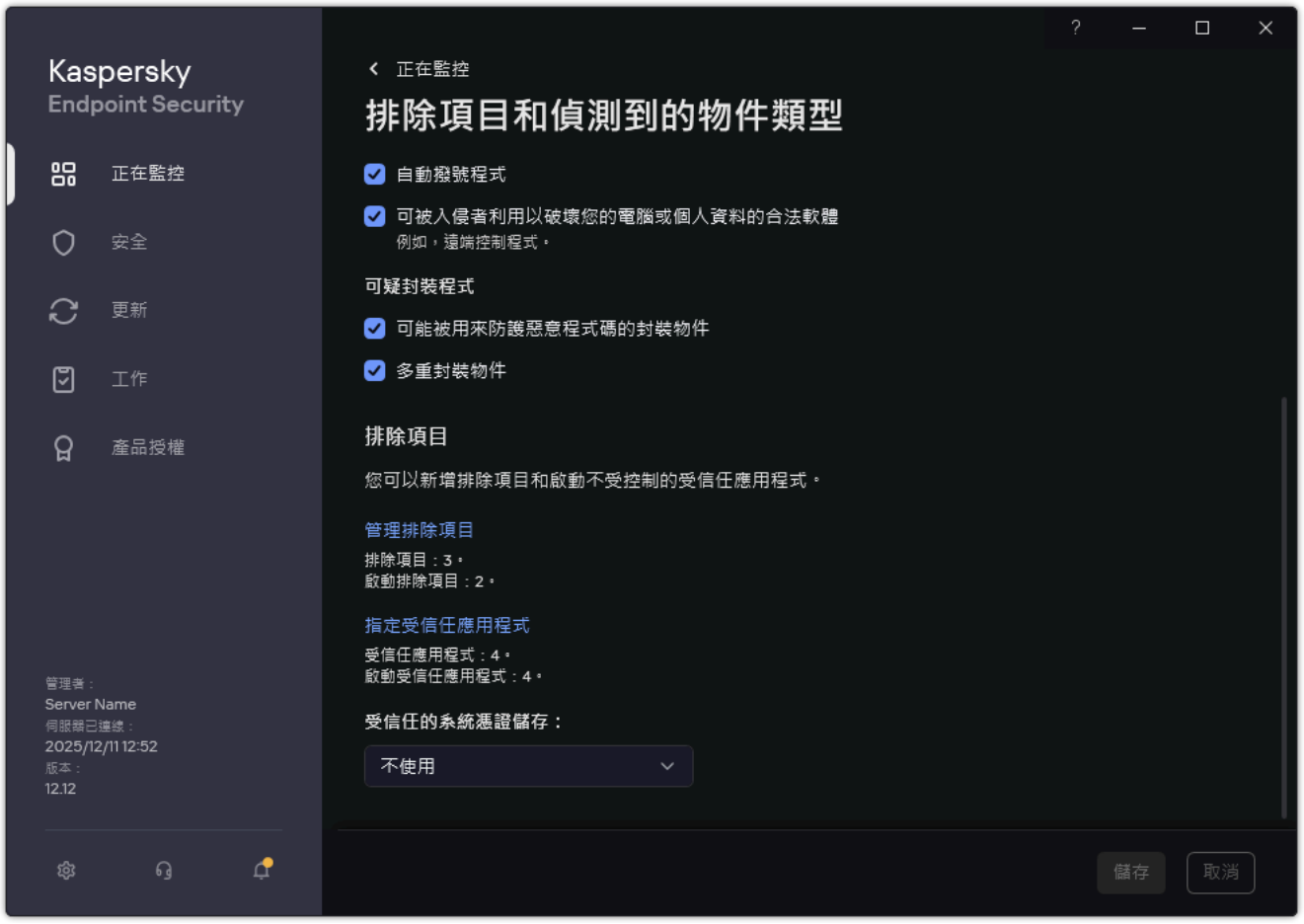



排除項目清單

### 如何在應用程式介面中將應用程式新增到本機受信任應用程式清單中

1. 在“應用程式主視窗”中，點擊⚙按鈕。
2. 在應用程式設定視窗中，選取”**一般設定**“→“**排除項目和偵測到的物件類型**”。
3. 在”**排除項目**”塊中，點擊”**指定受信任應用程式**”連接。

如果管理員在主控台中封鎖可信任應用程式的配置（“關閉的鎖”符號）並且禁止本機可信任應用程式（**允許使用受信任應用程式**核取方塊被清除）。




排除項目設定

4. 點擊**新增**並選擇一個操作：

- **類別**您可以將受信任的應用程式分為不同的類別。若要建立新類別，請輸入類別名稱並在該類別中新增至少一個受信任的應用程式。
- **新排除項目**Kaspersky Endpoint Security 會將新的受信任應用程式新增至清單的根目錄。
- **從清單中選取排除項目**為了在 SQL 伺服器、Microsoft Exchange 伺服器和 System Center Configuration Manager 上快速設定 Kaspersky Endpoint Security，應用程式包括*預定義的可信任應用程式*。另外還新增了預先定義的受信任應用程式，以支援 Citrix 和 VMware 虛擬環境中的應用程式安裝。您必須根據受防護伺服器的用途選擇預先定義的受信任應用程式。

若要將新的受信任應用程式新增至特定類別，請選取該類別旁的核取方塊並選取**新排除項目**選項。

5. 選擇信任標準：

- **使用磁碟上的完整處理程序路徑來將它視為受信任**輸入受信任應用程式的可執行檔的完整路徑。

  Kaspersky Endpoint Security 輸入遮罩時支援環境變量以及`*`和`?`字元。

  Kaspersky Endpoint Security 將受信任應用程式的檔案名稱視為區分大小寫。如果您輸入的檔案名稱大小寫錯誤，Kaspersky Endpoint Security 將無法辨識受信任的應用程式。

- **使用處理程序檔案雜湊將其視為受信任**

Kaspersky Endpoint Security 可支援環境變數並轉換應用程式本機介面中的路徑。換言之，如果您輸入檔案路徑 `%userprofile%\Documents\File.exe`，將為使用者 Fred123 在應用程式的本機介面中新增 `C:\Users\Fred123\Documents\File.exe` 記錄。因此，Kaspersky Endpoint Security 會忽略針對其他使用者的 `File.exe` 受信任程式。若要將項目套用到所有使用者帳戶，您可以使用 `*` 字元（例如，`C:\Users\*\Documents\File.exe`）。無論何時新增新的環境變數，您都需要重啟應用程式。

6. 在"受信任應用程式屬性"視窗中，配置進階設定。

7. 點擊**"確定"**。

   新的受信任應用程式將被新增到清單中。您可以隨時使用**狀態**列中的核取方塊將應用程式排除在受信任區域之外。

8. 儲存變更。




受信任應用程式清單

# 匯出和匯入受信任區域

*信任區域*是在其有效時，管理員建立的 Kaspersky Endpoint Security 不進行監控的物件和應用程式的清單。信任區域由以下清單組成：*掃描排除項目*和*受信任應用程式*。您可以將這些清單匯出到 XML 檔案和其它格式。然後，您可以修改檔案，例如，新增大量相同類型的排除項目。您還可以使用匯出/匯入功能來備份排除項目清單和受信任應用程式清單，或將清單遷移到其他伺服器。

應用程式使用以下格式匯出和匯入*排除項目清單*：

- XML 在管理主控台 (MMC)、網頁主控台和雲端主控台中可用。
- DAT 僅在在管理主控台 (MMC) 中可用。此格式的目的是維護與舊版應用程式的相容性。您可以在管理主控台 (MMC) 中將 DAT 檔案轉換為 XML 以將排除項目清單遷移到網頁主控台。
- CSV 僅可在應用程式的本機介面中使用。

Kaspersky Endpoint Security 使用 XML 格式匯出和匯入*受信任應用程式清單*。

**如何在管理主控台 (MMC) 中匯出和匯入信任區域**

1. 在卡巴斯基安全管理中心管理主控台樹狀目錄中，選取**政策**。
2. 選擇必要的政策並點擊以開啟政策內容。
3. 在政策視窗中，選擇"**一般設定 → 排除項目和物件類型**"。
4. 在**掃描排除項目和受信任應用程式**下方，選擇要匯出或匯入的受信任區域的元件：**掃描排除項目** 或者 **受信任應用程式**。
5. 點擊"**設定**"。
6. 要匯出規則清單：
   a. 選取您想要匯出的排除項目。要選擇多個連接埠，請使用**CTRL**或**SHIFT**鍵。
      如果您未選擇任何排除項目，則 Kaspersky Endpoint Security 將匯出所有排除項目。
   b. 點擊 → **匯出** 按鈕。
   c. 在開啟的視窗中，指定您要將排除項目清單匯出到的 XML 檔案的名稱，然後選取要儲存此檔案的資料夾。

d. 儲存檔案。

Kaspersky Endpoint Security 會將整個排除項目清單匯出到 XML 檔案。Kaspersky Endpoint Security 也支援將排除項目清單匯出到 DAT 檔案。




受信任應用程式清單

7. 若要匯入排除項目清單：

a. 點擊 → **匯入** 按鈕。

b. 在開啟的視窗中，選取要從中匯入排除項目清單的 XML 檔案。

c. 開啟檔案。

如果電腦已經具有排除項目清單，則 Kaspersky Endpoint Security 將提示您刪除現有清單或從 XML 檔案向其中新增新項目。Kaspersky Endpoint Security 也支援從 DAT 檔案匯入排除項目清單。

8. 儲存變更。

**如何在網頁主控台和雲端中控台中匯出和匯入信任區域清單**

1. 在網頁主控台的主視窗中，選擇**資產（裝置）** → **政策和設定檔**。

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. 要匯出規則清單：

   a. 點擊**"惡意軟體掃描排除項目"**連接。

   b. 選取您想要匯出的排除項目。

   c. 點擊 → **匯出** 按鈕。

      Kaspersky Endpoint Security 會將排除項目清單匯出到預設下載資料夾中的 JSON 檔案。

6. 要匯出受信任應用程式的清單：

   a. 選擇您要匯出的受信任應用程式。

   b. 點擊 → **匯出** 按鈕。

      Kaspersky Endpoint Security 會將受信任應用程式清單匯出到預設下載資料夾中的 JSON 檔案。

7. 若要匯入排除項目清單：

   a. 點擊**"惡意軟體掃描排除項目"**連接。

   b. 點擊 → **匯入** 按鈕。

      在開啟的視窗中，選取要從中匯入排除項目清單的 JSON 檔案。

   c. 開啟檔案。

      如果電腦已經具有排除項目清單，則 Kaspersky Endpoint Security 將提示您刪除現有清單或從 JSON 檔案向其中新增新項目。

8. 要匯入受信任應用程式的清單：

   a. 點擊**"應用程式"**連接。

   b. 點擊 → **匯入** 按鈕。

      這將開啟一個視窗；在此視窗中，選取要從中匯入受信任應用程式清單的 JSON 檔案。

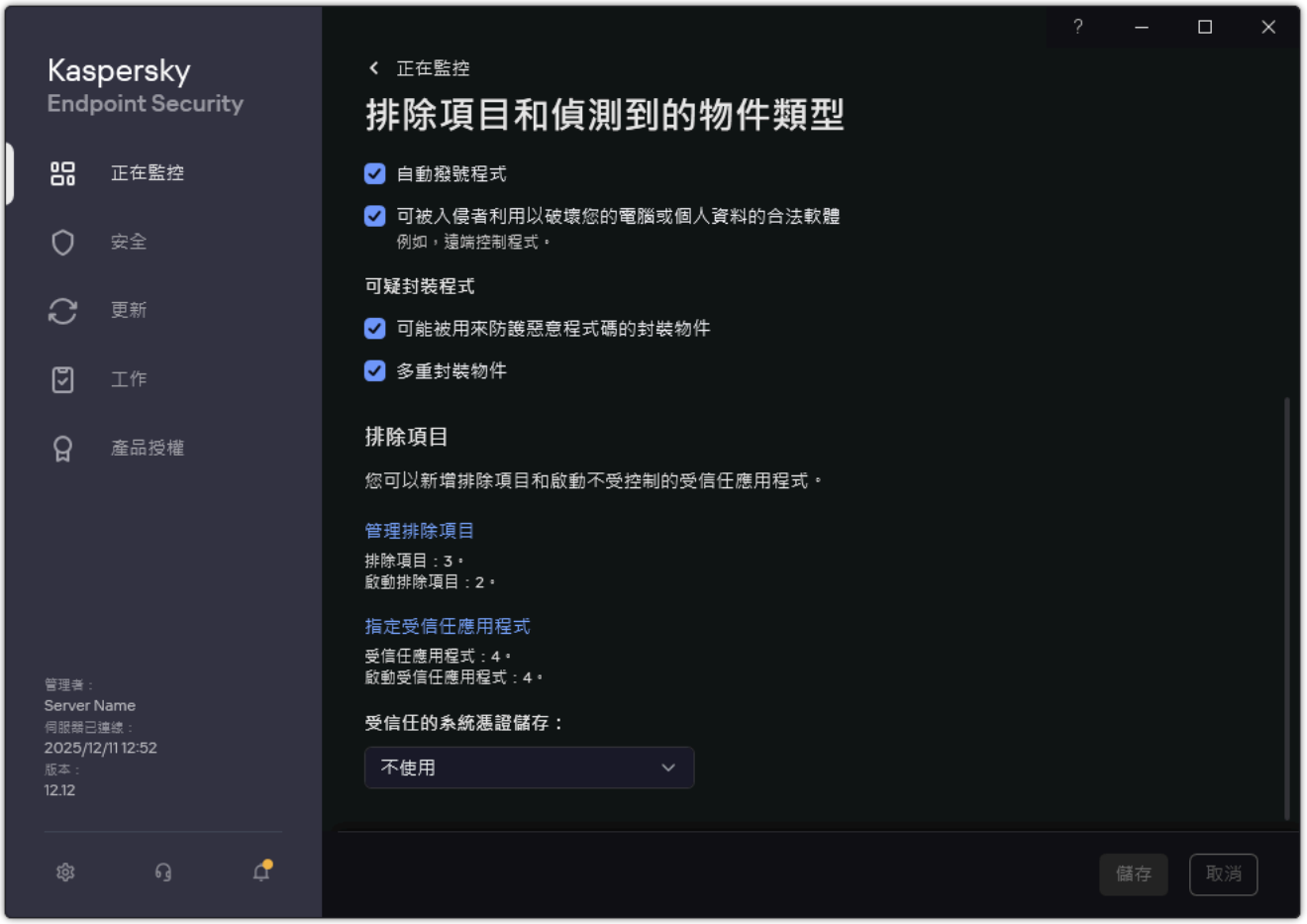
   c. 開啟檔案。

      如果電腦已經具有受信任應用程式清單，則 Kaspersky Endpoint Security 將提示您刪除現有清單或從 JSON 檔案向其中新增新項目。

9. 儲存變更。

### 如何在應用程式介面中匯出或匯入信任區域

1. 在“應用程式主視窗”中，點擊⚙按鈕。
2. 在應用程式設定視窗中，選取”**一般設定**“→“**排除項目和偵測到的物件類型**”。




排除項目設定

3. 要匯出規則清單：
   a. 在”**排除項目**”塊中，點擊”**管理排除項目**”連接。
   b. 選取您想要匯出的排除項目。
   c. 點擊“**匯出**”。
   d. 確認您只想匯出選定的排除項目，或匯出整個排除項目清單。
   e. 在開啟的視窗中，指定您要將排除項目清單匯出到的 CSV 檔案的名稱，然後選取要儲存此檔案的資料夾。

f. 儲存檔案。

Kaspersky Endpoint Security 會將整個排除項目清單匯出到 CSV 檔案。




排除項目清單

4. 要匯出受信任應用程式的清單：

a. 在"**排除項目**"塊中，點擊"**指定受信任應用程式**"連接。

b. 選擇您要匯出的受信任應用程式。

c. 點擊"**匯出**"。

d. 確認您只想匯出選定的受信任應用程式，還是匯出整個清單。

e. 這將開啟一個視窗；在此視窗中，輸入您要將受信任應用程式清單匯出到的 XML 檔案的名稱，然後選取要儲存此檔案的資料夾。

f. 儲存檔案。

Kaspersky Endpoint Security 會將整個受信任應用程式清單匯出到 XML 檔案。




受信任應用程式清單

5. 若要匯入排除項目清單：

a. 在"**排除項目**"塊中，點擊"**管理排除項目**"連接。

b. 點擊"**匯入**"。

c. 在開啟的視窗中，選取要從中匯入排除項目清單的 CSV 檔案。

d. 開啟檔案。

如果電腦已經具有排除項目清單，則 Kaspersky Endpoint Security 將提示您刪除現有清單或從 CSV 檔案向其中新增新項目。

6. 要匯入受信任應用程式的清單：

a. 在"**排除項目**"塊中，點擊"**指定受信任應用程式**"連接。

b. 點擊"**匯入**"。

c. 這將開啟一個視窗；在此視窗中，選取要從中匯入受信任應用程式清單的 XML 檔案。

d. 開啟檔案。

如果電腦已經具有受信任應用程式清單，則 Kaspersky Endpoint Security 將提示您刪除現有清單或從 XML 檔案向其中新增新項目。

7. 儲存變更。

# 使用受信任數位簽章處理應用程式

使用系統憑證儲存允許您從病毒掃描中排除由受信任數位簽章簽發的應用程式。Kaspersky Endpoint Security 會自動將此類應用程式分配給*受信任*群組。

**如何在管理主控台 (MMC) 中啟動受信任系統憑證儲存的使用**

1. 在卡巴斯基安全管理中心管理主控台樹狀目錄中，選取**政策**。
2. 選擇必要的政策並點擊以開啟政策內容。
3. 在政策視窗中，選擇"**一般設定 → 排除項目和物件類型**"。
4. 在"**受信任的系統憑證儲存**"塊中，選中"**使用受信任的系統憑證儲存**"核取方塊。
5. 在下拉清單中，選取必須被 Kaspersky Endpoint Security 視為受信任的系統儲存。
6. 儲存變更。

**如何在網頁主控台和雲端主控台中啟動受信任系統憑證儲存的使用**

1. 在網頁主控台的主視窗中，選擇**資產（裝置）→ 政策和設定檔**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"**受信任憑證**"連接。
6. 在開啟的視窗中，選中"**使用受信任的系統憑證儲存**"核取方塊。
7. 選取必須被 Kaspersky Endpoint Security 視為受信任的系統儲存。
8. 儲存變更。若要在電腦上套用該政策，請關閉掛鎖 。

**如何在應用程式界面中啟動受信任系統憑證儲存的使用**

1. 在"應用程式主視窗"中，點擊 按鈕。
2. 在應用程式設定視窗中，選取"**一般設定**"→"**排除項目和偵測到的物件類型**"。
3. 在"**受信任的系統憑證儲存**"下拉清單中，選取必須被 Kaspersky Endpoint Security 視為受信任的系統儲存。
4. 儲存變更。

# 附錄。預先定義的掃描排除項目和受信任的應用程式

從 Kaspersky Endpoint Security 12.6 for Windows 開始，掃描排除項目和受信任應用程式被新增到受信任區域。預先定義的掃描排除項目和受信任應用程式有助於在 SQL 伺服器、Microsoft Exchange 伺服器和 System Center Configuration Manager 上快速設定 Kaspersky Endpoint Security。這意味著您無需在伺服器上為應用程式手動設定受信任區域。從 Kaspersky Endpoint Security 12.8 for Windows 開始，您可以在 Light Agent 模式下安裝應用程式以防護虛擬環境。預定義掃描排除項目和受信任的應用程式可以幫助您在Citrix 和 VMware虛擬環境中快速設定 Kaspersky Endpoint Security。

您可以透過以下方式選擇預先定義的排除項目和受信任的應用程式：

- 安裝應用程式。
  - 使用精靈在本機安裝應用程式
  - 安裝套件內容
- 制定政策。
  - 新政策精靈
  - 政策內容：掃描排除項目和受信任的應用程式

## SQL 伺服器

在 SQL 伺服器上安裝 Kaspersky Endpoint Security 時，您必須從預先定義的排除項目和受信任應用程式建立受信任區域以確保伺服器的運作不被幹擾。

預定義掃描排除項目

| 路徑 | SQL 版本 |
|---|---|
| %ProgramFiles%\Microsoft SQL Server\MSSQL??. MSSQLSERVER\MSSQL\DATA*.mdf | 2012<br>2014<br>2016<br>2017<br>2019<br>2022 |
| %ProgramFiles(x86)%\Microsoft SQL Server\MSSQL.?*\Data*.mdf | 2012 |
| %ProgramFiles%\Microsoft SQL Server\MSSQL.?*\Data*.mdf | 2012 |
| %ProgramFiles%\Microsoft SQL Server\MSSQL??. MSSQLSERVER\MSSQL\DATA*.ldf | 2012<br>2014<br>2016<br>2017<br>2019<br>2022 |
| %ProgramFiles(x86)%\Microsoft SQL Server\MSSQL.?*\Data*.ldf | 2012 |
| %ProgramFiles%\Microsoft SQL Server\MSSQL.?*\Data*.ldf | 2012 |

| 路徑 | SQL 版本 |
| --- | --- |
| %ProgramFiles%\Microsoft SQL Server\MSSQL??.*\MSSQL\DATA*.mdf | 2012<br>2014<br>2016<br>2017<br>2019<br>2022 |
| %ProgramFiles%\Microsoft SQL Server\MSSQL??.**\MSSQL\DATA*.ldf | 2012<br>2014<br>2016<br>2017<br>2019<br>2022 |

# Microsoft Exchange 伺服器

在 Microsoft Exchange 伺服器上安裝 Kaspersky Endpoint Security 時，您必須從預先定義的排除項目和受信任應用程式建立受信任區域以確保伺服器的運作不被幹擾。

預定義掃描排除項目

| 路徑 | Microsoft Exchange 版本 |
| --- | --- |
| C:\Program Files\Microsoft\Exchange Server\V15\Mailbox*.Chk | 2013<br>2016<br>2019 |
| C:\Program Files\Microsoft\Exchange Server\V15\Mailbox*.Edb | 2013<br>2016<br>2019 |
| C:\Program Files\Microsoft\Exchange Server\V15\Mailbox*.Jrs | 2013<br>2016<br>2019 |
| C:\Program Files\Microsoft\Exchange Server\V15\Mailbox*.log | 2013<br>2016<br>2019 |
| C:\Program Files\Microsoft\Exchange Server\V15\Mailbox*.Que | 2013<br>2016<br>2019 |
| C:\Program Files\Microsoft\Exchange Server\V15\Mailbox*.jsl | 2013<br>2016<br>2019 |
| C:\Program Files\Microsoft\Exchange Server\V15\TransportRoles\Data\Queue*.Chk | 2013<br>2016<br>2019 |
| C:\Program Files\Microsoft\Exchange Server\V15\TransportRoles\Data\Queue*.Edb | 2013<br>2016<br>2019 |
| C:\Program Files\Microsoft\Exchange Server\V15\TransportRoles\Data\Queue*.Jrs | 2013<br>2016<br>2019 |
| C:\Program Files\Microsoft\Exchange Server\V15\TransportRoles\Data\Queue*.log | 2013<br>2016<br>2019 |
| C:\Program Files\Microsoft\Exchange Server\V15\TransportRoles\Data\Queue*.Que | 2013<br>2016<br>2019 |
| C:\Program Files\Microsoft\Exchange Server\V15\TransportRoles\Data\Queue*.jsl | 2013<br>2016<br>2019 |

預定義的受信任應用程式

| 路徑 | Microsoft Exchange 版本 |
| --- | --- |
| %ProgramFiles%\Microsoft\Exchange Server\V15\Bin\EdgeTransport.exe | 2013<br>2016<br>2019 |
| %ProgramFiles%\Microsoft\Exchange Server\V15\Bin\MSExchangeFrontendTransport.exe | 2013<br>2016<br>2019 |

# 系統中心配置管理器

預定義掃描排除項目

| 路徑 | 系統中心配置管理器版本 |
| --- | --- |
| %ProgramFiles%\Microsoft Configuration Manager\Inboxes | 2012<br>2012 R2 |

# Citrix

在 Citrix 虛擬環境中安裝 Kaspersky Endpoint Security 時，您必須從預先定義的排除項目和受信任應用程式建立受信任區域以確保伺服器的運作不被幹擾。

預定義掃描排除項目

| 路徑 |
| --- |
| %SystemRoot%\ServiceProfiles\NetworkService\HaDatabaseName.mdf |
| %SystemRoot%\ServiceProfiles\NetworkService\HaImportDatabaseName.mdf |
| %SystemRoot%\ServiceProfiles\NetworkService\HaDatabaseName_log.ldf |
| %SystemRoot%\ServiceProfiles\NetworkService\HaImportDatabaseName_log.ldf |
| %ProgramData%\Citrix\Broker\Cache |
| %SystemRoot%\System32\drivers\CtxUvi.sys |
| %ProgramFiles%\Citrix\HDX\bin\CitrixLogonCsp.dll |
| mcsdif.vhdx |
| %Temp%\Citrix\RTMediaEngineSRV\MediaEngineSRVDebugLogs**.txt |
| %Temp%\Citrix\HDXRTConnector**.txt |
| %UserProfile%\AppData\Local\Temp\Citrix\RTMediaEngineSRV\MediaEngineSRVDebugLogs**.txt |
| %ProgramFiles(x86)%\Citrix\ICA Client\epclient32.dll |
| %ProgramFiles(x86)%\Citrix\ICA Client\epclient64.dll |

| 路徑 |
| --- |
| %ProgramFiles(x86)%\Citrix\ICA Client\epinject.sys |
| %ProgramFiles(x86)%\Citrix\ICA Client\EntryProtect.dll |
| *.vhd |
| *.avhd |
| *.vhdx |
| *.avhdx |
| *.pvp |
| *.lok |
| %SystemRoot%\System32\drivers\CVhdMp.sys (Windows Server 2012 R2) |
| %SystemRoot%\System32\drivers\CfsDep2.sys |
| %ProgramData%\Citrix\Provisioning Services\Tftpboot\ARDBP32.BIN |
| .vdiskcache |
| vdiskdif.vhdx |
| %SystemRoot%\ServiceProfiles\NetworkService\AppData\Roaming\Citrix\SubscriptionsStore**\PersistentDictionary.edb |

預定義的受信任應用程式

| 路徑 | Cirix 解決方案 |
| --- | --- |
| %ProgramFiles%\Citrix\Broker\Service\BrokerService.exe | 虛擬應用程式和桌面 |
| %ProgramFiles%\Microsoft SQL Server\150\LocalDB\Binn\sqlservr.exe | 虛擬應用程式和桌面 |
| %ProgramFiles%\Citrix\Broker\Service\HighAvailabilityService.exe | 虛擬應用程式和桌面 |
| %ProgramFiles%\Citrix\ConfigSync\ConfigSyncService.exe | 虛擬應用程式和桌面 |
| %ProgramFiles%\Citrix\User Profile Manager\UserProfileManager.exe | 虛擬應用程式和桌面 |
| %ProgramFiles%\Citrix\Virtual Desktop Agent\BrokerAgent.exe | 虛擬應用程式和桌面 |
| %SystemRoot%\System32\drivers\CVhdFilter.sys | 虛擬應用程式和桌面 |
| %ProgramFiles(x86)%\Citrix\ICAService\CtxSvcHost.exe | 虛擬應用程式和桌面 |
| %ProgramFiles%\Citrix\System32\ctxgfx.exe | 虛擬應用程式和桌面 |
| %ProgramFiles%\Citrix\ICAService\picaSvc2.exe | 虛擬應用程式和桌面 |
| %ProgramFiles%\Citrix\ICAService\CpSvc.exe | 虛擬應用程式和桌面 |
| %ProgramFiles%\Citrix\HDX\bin\ctxgfx.exe | 虛擬應用程式和桌面 |
| %ProgramFiles%\Citrix\HDX\bin\CtxSvcHost.exe | 虛擬應用程式和桌面 |
| %ProgramFiles%\Citrix\HDX\bin\ctxgfx.exe | 虛擬應用程式和桌面 |

| 路徑 | Cirix 解決方案 |
| --- | --- |
| %ProgramFiles%\Citrix\HDX\bin\picaSvc2.exe | 虛擬應用程式和桌面 |
| %ProgramFiles%\Citrix\HDX\bin\CpSvc.exe | 虛擬應用程式和桌面 |
| %ProgramFiles(x86)%\Citrix\System32\WebSocketService.exe | 虛擬應用程式和桌面 |
| %ProgramFiles%\Citrix\ICAService\WebSocketService.exe | 虛擬應用程式和桌面 |
| %ProgramFiles(x86)%\Citrix\HDX\bin\WebSocketService.exe | 虛擬應用程式和桌面 |
| %ProgramFiles(x86)%\Citrix\HDX RealTime Connector\AudioTranscoder.exe | 虛擬應用程式和桌面 |
| %ProgramFiles(x86)%\Citrix\HDX RealTime Connector\MediaEngine.Net.Service.exe | 虛擬應用程式和桌面 |
| %ProgramFiles(x86)%\Citrix\HDX RealTime Connector\MediaEngineService.exe | 虛擬應用程式和桌面 |
| %ProgramFiles(x86)%\Citrix\ICA Client\MediaEngineService.exe | 工作區應用程式 |
| %ProgramFiles(x86)%\Citrix\ICA Client\CDViewer.exe | 工作區應用程式 |
| %ProgramFiles(x86)%\Citrix\ICA Client\concentr.exe | 工作區應用程式 |
| %ProgramFiles(x86)%\Citrix\ICA Client\wfica32.exe | 工作區應用程式 |
| %ProgramFiles(x86)%\Citrix\ICA Client\bgblursvc.exe | 工作區應用程式 |
| %ProgramFiles(x86)%\Citrix\ICA Client\AuthManager\AuthManSvr.exe | 工作區應用程式 |
| %ProgramFiles(x86)%\Citrix\ICA Client\SelfServicePlugin\SelfService.exe | 工作區應用程式 |
| %ProgramFiles(x86)%\Citrix\ICA Client\SelfServicePlugin\SelfServicePlugin.exe | 工作區應用程式 |
| %ProgramFiles(x86)%\Citrix\ICA Client\HdxRtcEngine.exe | 工作區應用程式 |
| %ProgramFiles(x86)%\Citrix\ICA Client\HdxTeams.exe | 工作區應用程式 |
| %ProgramFiles%\Citrix\Provisioning Services\BNTFTP.EXE | Provisioning |
| %ProgramFiles%\Citrix\Provisioning Services\PVSTSB.EXE | Provisioning |
| %ProgramFiles%\Citrix\Provisioning Services\StreamService.exe | Provisioning |
| %ProgramFiles%\Citrix\Provisioning Services\StreamProcess.exe | Provisioning |
| %ProgramFiles%\Citrix\Provisioning Services\soapserver.exe | Provisioning |
| %ProgramFiles%\Citrix\Provisioning Services\Inventory.exe | Provisioning |
| %ProgramFiles%\Citrix\Provisioning Services\Notifier.exe | Provisioning |
| %ProgramFiles%\Citrix\Provisioning Services\MgmtDaemon.exe | Provisioning |
| %ProgramFiles%\Citrix\Provisioning Services\BNPXE.exe | Provisioning |
| %ProgramFiles%\Citrix\Provisioning Services\CdfSvc.exe | Provisioning |
| %ProgramFiles%\Citrix\Provisioning Services\BNAbsService.exe | Provisioning |
| %SystemRoot%\System32\drivers\bnistack6.sys | Provisioning |

| 路徑 | Cirix 解決方案 |
| --- | --- |
| %SystemRoot%\System32\drivers\CfsDep2.sys | Provisioning |
| %SystemRoot%\System32\drivers\cnicteam.sys | Provisioning |
| %ProgramFiles%\Citrix\Provisioning Services\BNDevice.exe | Provisioning |
| %ProgramFiles%\Citrix\Provisioning Services\drivers\BNIstack6.sys | Provisioning |
| %ProgramFiles%\Citrix\Provisioning Services\drivers\CNicTeam.sys | Provisioning |
| %ProgramFiles%\Citrix\Provisioning Services\drivers\CFsDep2.sys | Provisioning |
| %ProgramFiles%\Citrix\Provisioning Services\drivers\CVhdMp.sys | Provisioning |
| %ProgramFiles%\Citrix\Receiver StoreFront\Services\SubscriptionsStoreService\Citrix.DeliveryServices.SubscriptionsStore.ServiceHost.exe | StoreFront |
| %ProgramFiles%\Citrix\Receiver StoreFront\Services\CredentialWallet\Citrix.DeliveryServices.CredentialWallet.ServiceHost.exe | StoreFront |

# VMware

在 VMware 虛擬環境中安裝 Kaspersky Endpoint Security 時，您必須從預先定義的受信任應用程式建立一個受信任區域以確保伺服器作業不被幹擾。

預定義的受信任應用程式

| 路徑 | VMware 解決方案 |
| --- | --- |
| C:\Program Files\VMware\VMware View\Agent\bin\wsnm.exe | Horizon |
| C:\Program Files\VMware\VMware View\Agent\bin\wsnm_jms.exe | Horizon |
| C:\Program Files\VMware\VMware View\Agent\bin\ws_scripthost.exe | Horizon |
| C:\Program Files\VMware\VMware View\Agent\VMware Blast\VMBlastS.exe | Horizon |
| C:\Program Files\VMware\VMware View\Agent\VMware Blast\VMBlastW.exe | Horizon |
| C:\Program Files\VMware\VMware View\Agent\bin\SecurityGateway.exe | Horizon |
| C:\Program Files\Common Files\VMware\Teradici PCoIP Server\x64\pcoip_server_win32.exe | Horizon |
| C:\Program Files\Common Files\VMware\Teradici PCoIP Server\pcoip_server_win32.exe | Horizon |
| C:\Program Files (x86)\Common Files\VMware\USB\vmware-usbarbitrator64.exe | Horizon |
| C:\Program Files\Common Files\VMware\ScannerRedirection\Scanner.exe | Horizon |
| C:\Program Files\VMware\VMware View\Agent\bin\tsdrvdisvc.dll | Horizon |
| C:\Program Files\VMware\VMware View\Server\appblastgateway\nssm.exe | Horizon |
| C:\Program Files\VMware\VMware View\Server\bin\wsnm.exe | Horizon |
| C:\Program Files\VMware\VMware View\Server\bin\SecurityGateway.exe | Horizon |
| C:\Program Files\VMware\VMware View\Server\bin\ws_TunnelService.exe | Horizon |
| C:\Program Files\VMware\VMware View\Server\bin\ws_SecurityServer.exe | Horizon |
| C:\Program Files\VMware\VMware Horizon View Client\vmUpdateLauncher.exe | Horizon |
| C:\Program Files\VMware\VMware Horizon View Client\vmware-appstub.exe | Horizon |
| C:\Program Files\VMware\VMware Horizon View Client\vmware-view.exe | Horizon |
| C:\Program Files\VMware\VMware Horizon View Client\vmware-print-helper.exe | Horizon |
| C:\Program Files\VMware\VMware Horizon View Client\vmware-print-previewer.exe | Horizon |
| C:\Program Files\VMware\VMware Horizon View Client\vmware-print-redir-client.exe | Horizon |

| 路徑 | VMware 解決方案 |
| --- | --- |
| C:\Program Files\VMware\VMware Horizon View Client\vmware-remotemks.exe | Horizon |
| C:\Program Files\VMware\VMware Horizon View Client\vmware-view-usbloader.exe | Horizon |
| C:\Program Files\VMware\VMware Horizon View Client\ClientService\horizon_client_service.exe | Horizon |
| C:\Program Files\VMware\VMware Horizon View Client\DCT\ws_diag.exe | Horizon |
| C:\Program Files\VMware\VMware Horizon View Client\cef\HTML5VideoPlayer.exe | Horizon |
| C:\Program Files (x86)\Common Files\VMware\USB\vmware-usbarbitrator.exe | Horizon |
| C:\Program Files (x86)\Common Files\VMware\USB\vmware-usbarbitrator64.exe | Horizon |
| C:\Program Files (x86)\Common Files\VMware\USB\vnetlib.exe | Horizon |
| C:\Program Files (x86)\Common Files\VMware\USB\vnetlib64.exe | Horizon |
| C:\Program Files (x86)\Common Files\VMware\USB\DriverCache\vnetlib.exe | Horizon |
| C:\Program Files (x86)\Common Files\VMware\USB\DriverCache\vnetlib64.exe | Horizon |
| C:\Program Files\Common Files\VMware\DeviceRedirectionCommon\ftnlping.exe | Horizon |
| C:\Program Files\Common Files\VMware\DeviceRedirectionCommon\ftnlsv.exe | Horizon |
| C:\Program Files\Common Files\VMware\ScannerRedirection\diagutil.exe | Horizon |
| C:\Program Files\Common Files\VMware\ScannerRedirection\ftscanmgrhv.exe | Horizon |
| C:\Program Files\Common Files\VMware\ScannerRedirection\scan.exe | Horizon |
| C:\Program Files\Common Files\VMware\ScannerRedirection\scan64.exe | Horizon |
| C:\Program Files\Common Files\VMware\SerialPortRedirection\Client\vmwsprrdpwks.exe | Horizon |

# 管理備份

*備份區*儲存保留在解毒過程中刪除或修改的檔案的備份副本。*備份副本*是指對檔案進行病毒清除或移除前建立的檔案副本。檔案的備份副本以特定格式儲存並且不會帶來威脅。

檔案的備份副本儲存在 `C:\ProgramData\Kaspersky Lab\KES.12.12\QB` 資料夾中。

管理員群組中的使用者被授予存取該資料夾的完整權限。其帳戶用於安裝 Kaspersky Endpoint Security 的使用者被授予該資料夾的有限存取權限。

Kaspersky Endpoint Security 不提供用於設定檔備份副本的使用者存取權限的功能。

有時，在清除過程中無法維護檔案的完整性。如果您在解毒後失去對受感染檔案重要資訊的部分或全部存取權限，可以嘗試將檔案從其備份副本還原到其原始資料夾中。

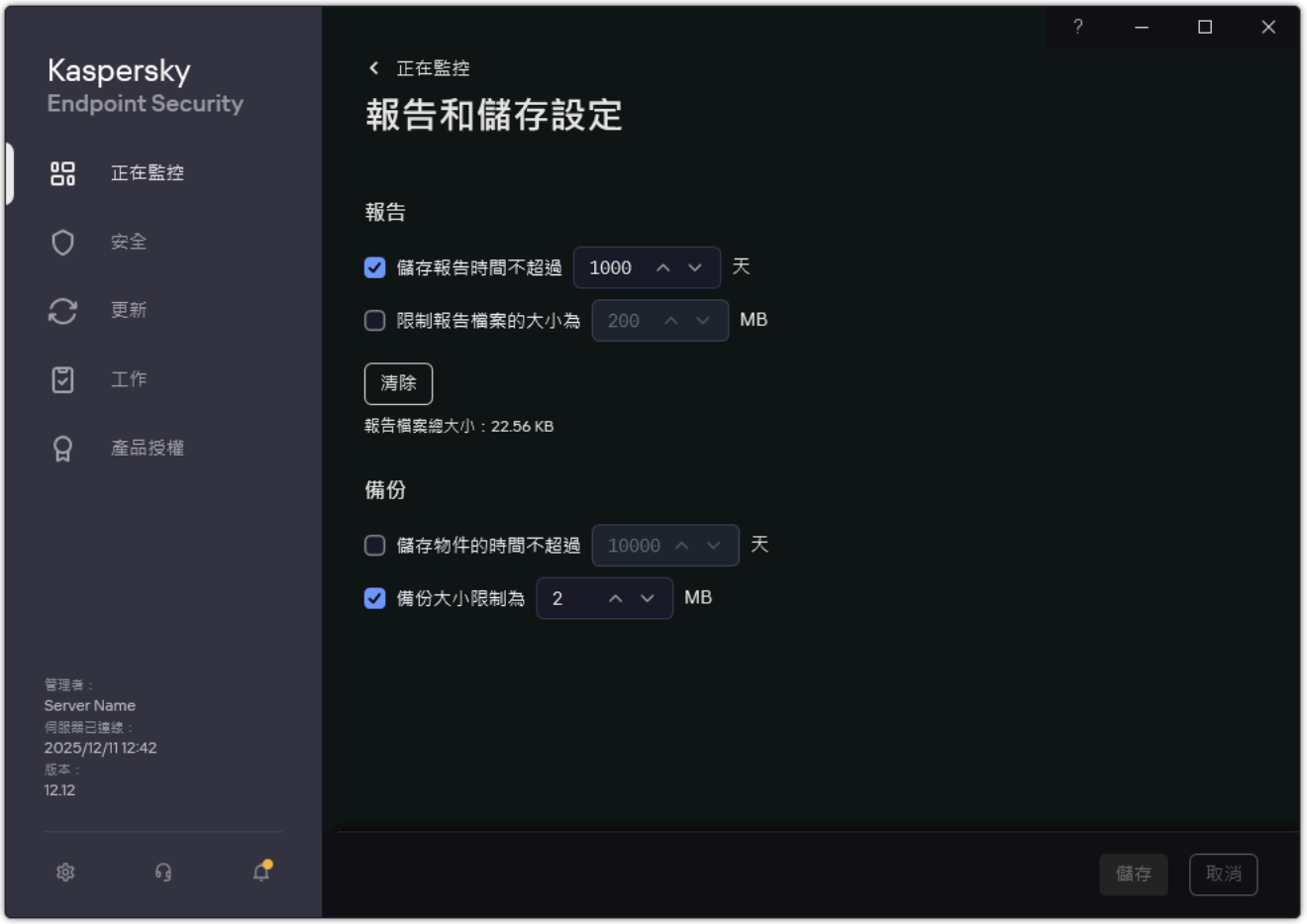
如果 Kaspersky Endpoint Security 在卡巴斯基安全管理中心管理下執行，則檔案的備份副本可能會傳送至卡巴斯基安全管理中心管理伺服器。有關在卡巴斯基安全管理中心管理檔案的備份副本的更多詳細資訊，請參閱《卡巴斯基安全管理中心說明》系統。

# 配置備份區中的檔案的最長儲存期

備份區中的檔案副本的預設最長儲存期限是 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。

*要配置備份區中的檔案的最長儲存期：*

1. 在“應用程式主視窗”中，點擊 按鈕。
2. 在應用程式設定視窗中，在 **一般設定** 下面，點擊 **報告和儲存。** 瓷片。




備份設定

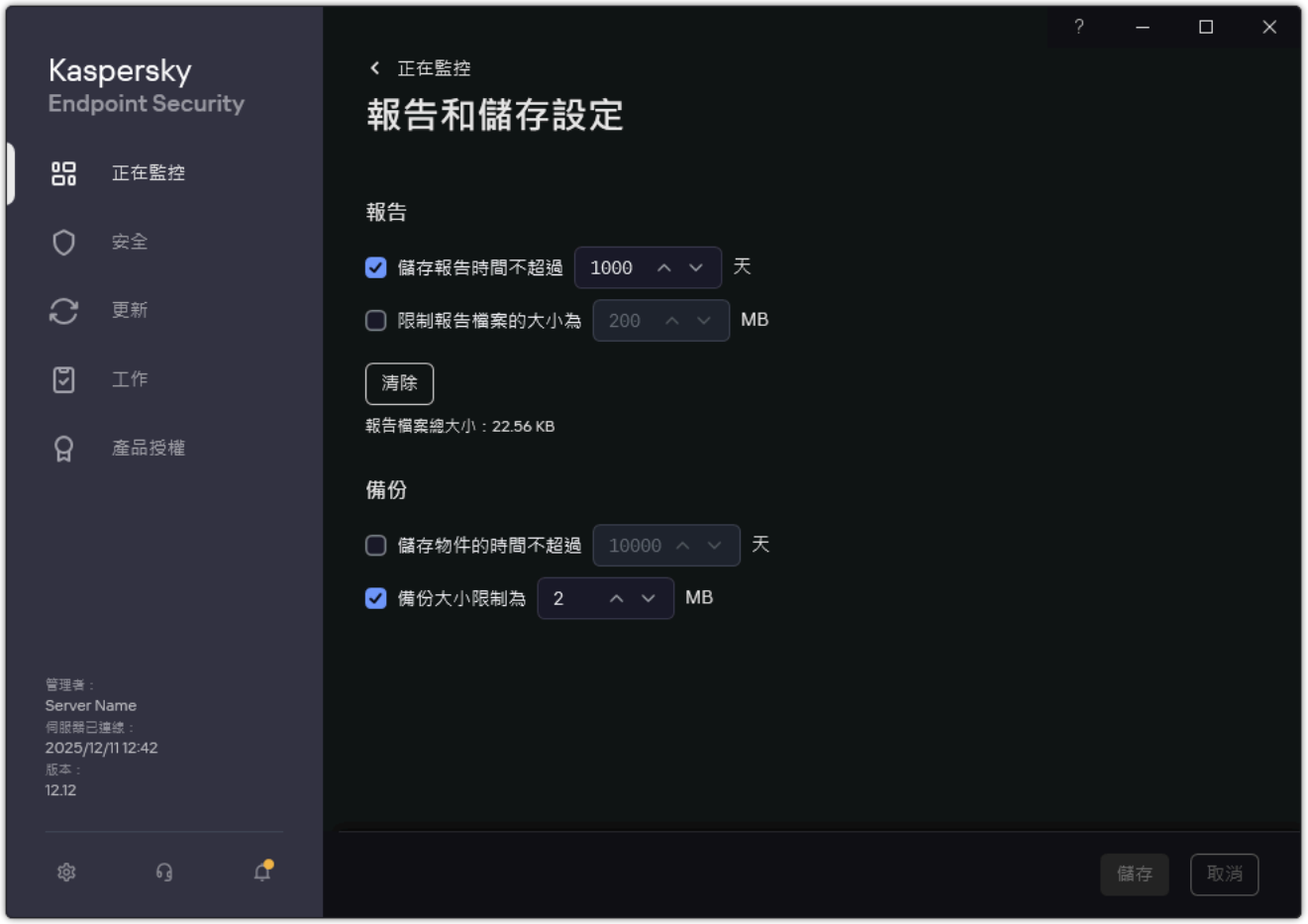
3. 如果要限制“備份”中檔案副本的儲存期限，請選中“**備份**“塊中的“ **儲存物件的時間不超過 N 天**”核取方塊。輸入備份區中的檔案副本的最長儲存期。
4. 儲存變更。

# 設定備份區的最大容量

您可以指定備份的最大大小。預設情況下，備份區容量無限制。當達到最大容量後，Kaspersky Endpoint Security 將自動刪除備份區中最舊的檔案。

*要設定備份區的最大容量：*

1. 在"應用程式主視窗"中，點擊⚙按鈕。
2. 在應用程式設定視窗中，在 **一般設定** 下面，點擊 **報告和儲存。** 瓷片。




備份設定

3. 在「**備份**」區塊中，選擇「**備份大小限制為 N MB**」核取方塊。如果選中該核取方塊，則最大儲存大小限制為定義值。預設情況下，最大大小為 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。
4. 儲存變更。

# 從備份區中還原檔案

如果在檔案中偵測到惡意程式碼，Kaspersky Endpoint Security 將封鎖此檔案、為其指派"*未解毒*"狀態，並將其副本放到"備份區"中並嘗試對其解毒。檔案成功解毒後，備份副本的狀態將變為*已解毒*。檔案在原始資料夾中將不可用。如果檔案無法被解毒，Kaspersky Endpoint Security 將把它從原始資料夾中刪除。您可以將此檔案從它的備份副本還原到它的原資料夾。

具有*將在電腦重新啟動時被刪除*狀態的檔案無法被還原。重新啟動電腦，檔案狀態將變更為"*已解毒*"或"*已刪除*"。您還可以將此檔案從它的備份副本還原到它的原資料夾。

在屬於 Windows Store 應用程式的檔案中偵測到惡意程式碼以後，Kaspersky Endpoint Security 將立即刪除檔案，而不會將其備份副本移至備份區。您可以使用作業系統的適當工具還原 Windows Store 應用程式的完整性（有關還原 Windows Store 應用程式的詳細資訊，請參閱 Microsoft Windows 說明檔案）。

檔案備份副本集合以表格顯示。對於檔案的備份副本，顯示檔案的原始資料夾位置。檔案原始資料夾位置中可能包含個人資料。

如果將位於同一資料夾中具有相同名稱但內容不同的多個檔案移至備份區，則只能復原最後放入備份區的檔案。

*要從備份區中還原檔案，請執行以下操作：*

1. 在應用程式主視窗的**"正在監控"**區域中，點擊**"備份"**圖標。
2. 這將開啟備份中的檔案清單；在此清單中，選擇您想要還原的檔案然後點擊**"還原"**。

   Kaspersky Endpoint Security 會將把所選檔案的備份副本還原至它們原來所在的資料夾。




備份

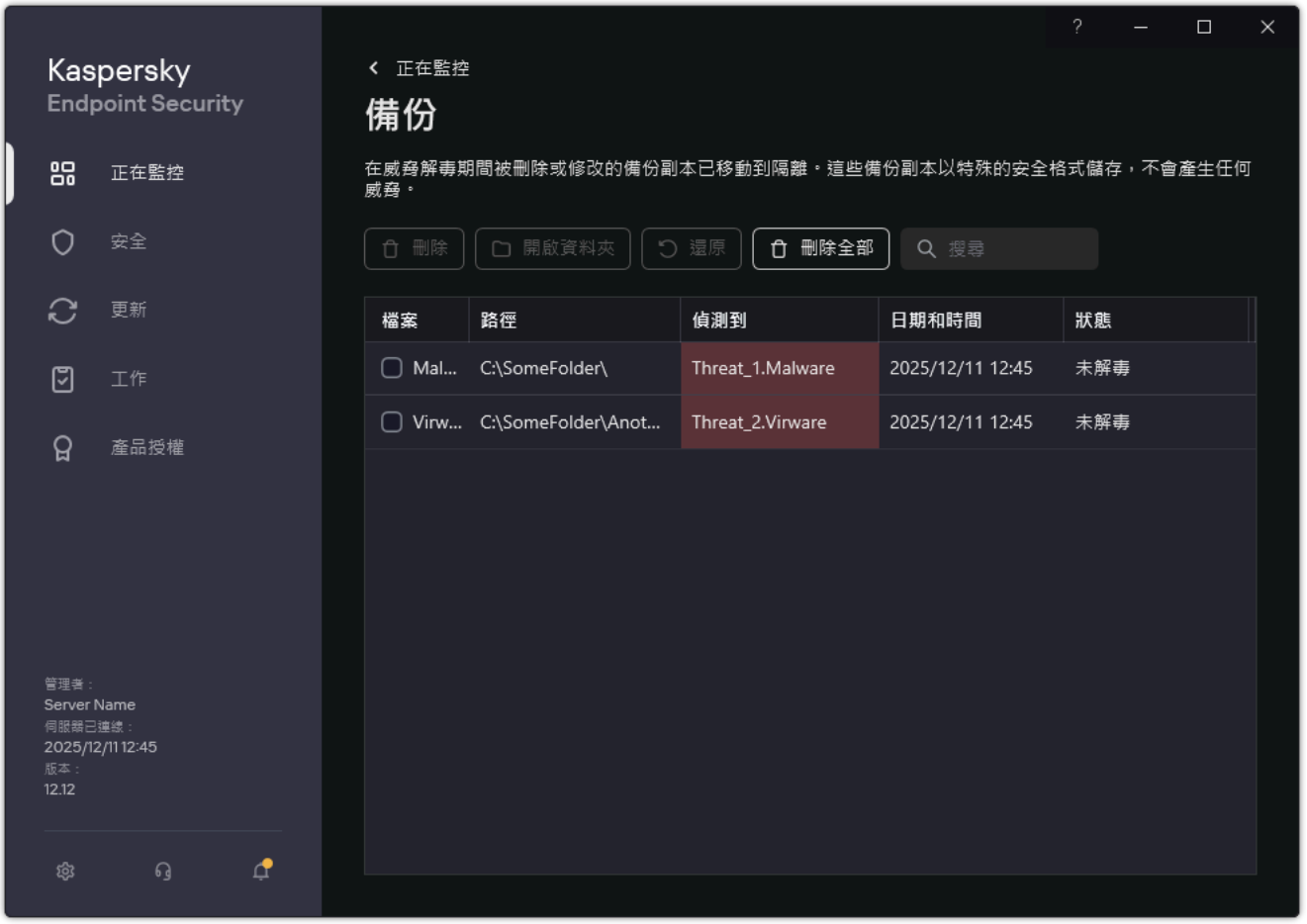
# 從備份區中刪除檔案備份副本

當應用程式設定中設定的儲存條件後，Kaspersky Endpoint Security 將自動刪除備份區中的所有檔案備份副本，不管它們的狀態是什麼。您也可以手動從備份區中刪除檔案的副本。

*要從備份區中刪除檔案備份副本：*

1. 在應用程式主視窗的**"正在監控"**區域中，點擊**"備份"**圖標。
2. 這將開啟備份中的檔案清單；在此清單中，選擇您想要從備份中刪除的檔案然後點擊**"刪除"**。

Kaspersky Endpoint Security 從本分區中刪除所選檔案備份副本。




備份

# 通知服務

Kaspersky Endpoint Security 執行操作時發生的所有類型的事件。這些事件通知可以是純粹的資訊或包含重要資訊。例如，通知可以告知成功更新了資料庫和應用程式模組或記錄需要糾正的元件錯誤。

Kaspersky Endpoint Security 支援記錄 Microsoft Windows 應用程式日誌和 / 或 Kaspersky Endpoint Security 事件日誌操作中的事件資訊。

Kaspersky Endpoint Security 透過下列方式傳送通知：

- 使用 Microsoft Windows 工作列通知區域中的彈窗通知；
- 透過電子郵件。

您可以設定事件通知的傳送方式。您可以為每一類事件設定通知傳送方式。

使用事件表設定通知服務時，您可以執行以下操作：

- 按列值或者自訂篩選條件篩選通知服務事件。
- 使用搜尋功能搜尋通知服務事件。
- 對通知服務事件進行排序。
- 變更通知服務事件清單中的顯示順序和列設定。

# 設定事件日誌設定

*要配置事件日誌設定，請執行以下操作：*

1. 在"應用程式主視窗"中，點擊⚙ 按鈕。
2. 在應用程式設定視窗中，選取"**一般設定**"→"**介面**"。
3. 在"**通知**"塊中，點擊"**設定通知**"按鈕。

   Kaspersky Endpoint Security 元件和工作顯示在該視窗的左側。該視窗的右側列出了為選取元件或工作產生的事件。

   事件可能包含以下使用者資料：

   - Kaspersky Endpoint Security 掃描的檔案的路徑。
   - 在 Kaspersky Endpoint Security 執行期間修改的登錄機碼路徑。
   - Microsoft Windows 使用者名稱。
   - 使用者開啟的網頁的位址。
4. 在視窗左側，選取您要為其設定事件日誌設定的元件或工作。

5. 選中“**儲存在本機報告中**”和“**儲存於 Windows 事件記錄中**”欄中相關事件旁的核取方塊。

   在“**儲存在本機報告中**”列中選中了其核取方塊的事件將顯示在“應用程式日誌“中。在“**儲存於 Windows 事件記錄中**”列中選中了其核取方塊的事件將顯示在“`Application`”渠道的“Windows 日誌“中。

6. 儲存變更。

# 設定通知的顯示和傳送

*若要設定通知的顯示和傳送：*

1. 在“應用程式主視窗”中，點擊⚙ 按鈕。
2. 在應用程式設定視窗中，選取”**一般設定**“→“**介面**”。
3. 在”**通知**”塊中，點擊”**設定通知**”按鈕。

   Kaspersky Endpoint Security 元件和工作顯示在該視窗的左側。該視窗的右側列出了為選取元件或工作產生的事件。

   事件可能包含以下使用者資料：

   - Kaspersky Endpoint Security 掃描的檔案的路徑。
   - 在 Kaspersky Endpoint Security 執行期間修改的登錄機碼路徑。
   - Microsoft Windows 使用者名稱。
   - 使用者開啟的網頁的位址。

4. 在視窗的左側，選取要為其設定螢幕通知傳送的元件或工作。
5. 在“**在螢幕上通知**”列中，選取相關事件旁的核取方塊。

   關於選取事件的資訊會以 Microsoft Windows 工作列通知區域中彈出訊息的形式顯示在螢幕上。

6. 在“**透過電子郵件通知**”列中，選取相關事件旁的核取方塊。

   如果配置了郵件通知傳遞設定，則透過電子郵件傳送選定事件的資訊。

7. 點擊“**確定**”。
8. 如果啟用了電子郵件通知，請設定電子郵件傳送設定：

   a. 點擊“**設定電子郵件通知**”。

   b. 選取“**通知事件**”核取方塊以啟用傳送有關在“**透過電子郵件通知**”列中選定的 Kaspersky Endpoint Security 事件資訊的功能。

   c. 指定電子郵件事件通知傳送設定。

   d. 點擊“**確定**”。

9. 儲存變更。

# 設定應用程式狀態警告在通知區域的顯示

*若要設定通知區域中應用程式狀態警告的顯示：*

1. 在"應用程式主視窗"中，點擊 按鈕。
2. 在應用程式設定視窗中，選取"**一般設定**"→"**介面**"。
3. 在"**在通知區域顯示應用程式的狀態**"塊中，選取您要在 Microsoft Windows 通知區域中看到通知的事件類型旁的核取方塊。
4. 儲存變更。

發生與選定類別關聯的事件時，通知區域的應用程式圖示將根據警告的嚴重性變更為 或 。

# 使用者和管理員之間的訊息傳遞

"應用程式控制"、"裝置控制"、"Web 控制"和"適應性異常控制"元件允許其電腦已安裝 Kaspersky Endpoint Security 的 LAN 使用者向管理員傳送訊息。

在以下情況下，使用者可能需要向本機公司網路系統管理員傳送郵件：

- 裝置控制封鎖對此裝置的存取。

  請求被封鎖裝置存取權限的郵件範本在"裝置控制"區域中 Kaspersky Endpoint Security 介面內。

- "應用程式控制"封鎖了某個應用程式的啟動。

  請求允許啟動被封鎖的應用程式的郵件範本在 Kaspersky Endpoint Security 介面的"應用程式控制"區域中提供。

- Web 控制封鎖對網頁資源的存取。

  請求被封鎖網頁資源存取權限的郵件範本在"Web 控制"區域中 Kaspersky Endpoint Security 介面內。

用於傳送訊息的方式和所使用的範本取決於安裝 Kaspersky Endpoint Security 的電腦上執行卡巴斯基安全管理中心政策，是否連線了卡巴斯基安全管理中心管理伺服器。有以下情景：

- 如果安裝了 Kaspersky Endpoint Security 的電腦上沒有執行卡巴斯基安全管理中心政策，使用者的訊息將透過電子郵件傳送給本機區域網路管理員。

  訊息欄位的內容將來自 Kaspersky Endpoint Security 本機介面中定義的範本。

- 如果安裝了 Kaspersky Endpoint Security 的電腦上執行著卡巴斯基安全管理中心政策，標準訊息將傳送至卡巴斯基安全管理中心管理伺服器。

  在這種情況下，可以在卡巴斯基安全管理中心事件儲存中檢視使用者訊息（參見下方說明）。訊息欄位的內容將來自卡巴斯基安全管理中心政策中定義的範本。

- 卡巴斯基安全管理中心漫遊政策執行在安裝了 Kaspersky Endpoint Security 的電腦上，用於傳送郵件的方法將取決於是否連線了卡巴斯基安全管理中心。

  - 如果建立了與卡巴斯基安全管理中心的連線，Kaspersky Endpoint Security 會將標準郵件傳送至卡巴斯基安全管理中心管理伺服器。

  - 如果沒有卡巴斯基安全管理中心連線，則使用者的訊息透過電子郵件傳送給本機區域網路管理員。

  在這兩種情況中，訊息欄位的內容將來自卡巴斯基安全管理中心政策中定義的範本。

*若要在卡巴斯基安全管理中心事件儲存中檢視使用者訊息，請執行以下操作：*

1. 開啟卡巴斯基安全管理中心管理主控台。

2. 在管理主控台樹狀目錄的**管理伺服器**節點中選取**事件**標籤。

   卡巴斯基安全管理中心工作區將顯示 Kaspersky Endpoint Security 執行期間發生的所有事件，包括接收自區域網路使用者傳送給管理員的郵件。

3. 若要設定事件篩選，則在"**事件分類**"下拉清單中選取"**使用者請求**"。

4. 在事件清單中選取傳送給管理員的訊息。

5. 點擊管理主控台工作區右側的"**開啟事件內容視窗**"按鈕。

# 管理報告

有關每個 Kaspersky Endpoint Security 元件的操作、資料加密事件、每個掃描工作的效能、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記錄在報告中。

報告儲存在 `C:\ProgramData\Kaspersky Lab\KES.12.12\Report` 資料夾中。

報告可能包含以下使用者資料：

- Kaspersky Endpoint Security 掃描的檔案的路徑。
- 在 Kaspersky Endpoint Security 執行期間修改的登錄機碼路徑。
- Microsoft Windows 使用者名稱。
- 使用者開啟的網頁的位址。

報告中的資料以表格形式顯示。每個表格行都含有一個單獨事件的相關資訊。事件內容位元於表格列中。部分列為複合列，包含有帶附加內容的嵌套列。要檢視附加內容，您點擊列名稱旁邊的 ⊞ 按鈕。在各種不同元件或各種工作執行過程中記錄下來的事件擁有不同的內容整合。

以下報告可用：

- **系統稽核**報告。包含在應用程式操作和與使用者互動時記錄的事件的相關資訊。
- 有關 Kaspersky Endpoint Security 元件操作的報告。
- Kaspersky Endpoint Security 工作執行報告。
- **資料加密**報告。包含資料加密和解密期間所發生事件的資訊。

報告使用以下事件重要性等級：

ⓘ **資訊訊息**。通常不包含重要資訊的參考事件。

⚠ **警告**。顯示了 Kaspersky Endpoint Security 操作上的重要情況而需要注意的事件。

⓪ **緊急事件**。十分重要的事件以及 Kaspersky Endpoint Security 執行問題或在防護使用者電腦時的弱點。

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：

- 透過各種不同的規則篩選事件清單。
- 使用搜尋功能尋找特定的事件。
- 在單獨的區域中檢視所選事件。
- 按照每個表格列的值排列事件清單。
- 使用 ⊞ 按鈕顯示和隱藏按照事件篩選分組的事件。
- 變更報告中表格列的順序和排列。

如有需要，您可以將產生的報告儲存為文字檔案。您還可以刪除合併成組的 Kaspersky Endpoint Security 元件和工作的報告資訊。

如果 Kaspersky Endpoint Security 在卡巴斯基安全管理中心的管理下執行，則有關事件的資訊可能會傳送至卡巴斯基安全管理中心管理伺服器（有關更多詳細資訊，請參閱卡巴斯基安全管理中心說明）。

# 檢視報告

如果使用者能檢視報告，該使用者也能檢視報告中反映的所有事件。

*若要檢視報告：*

1. 在應用程式主視窗的**"正在監控"**區域中，點擊**"報告"**圖標。




報告

2. 在元件和工作清單中，選擇元件或工作。

   視窗右側部分顯示的報告中包含 Kaspersky Endpoint Security 的選定元件或選定工作執行所生成的事件清單。您可以根據其中一列的單元格中的值對報告中的事件進行排序。

3. 要檢視事件的相關詳細資訊，請在報告中選擇事件。

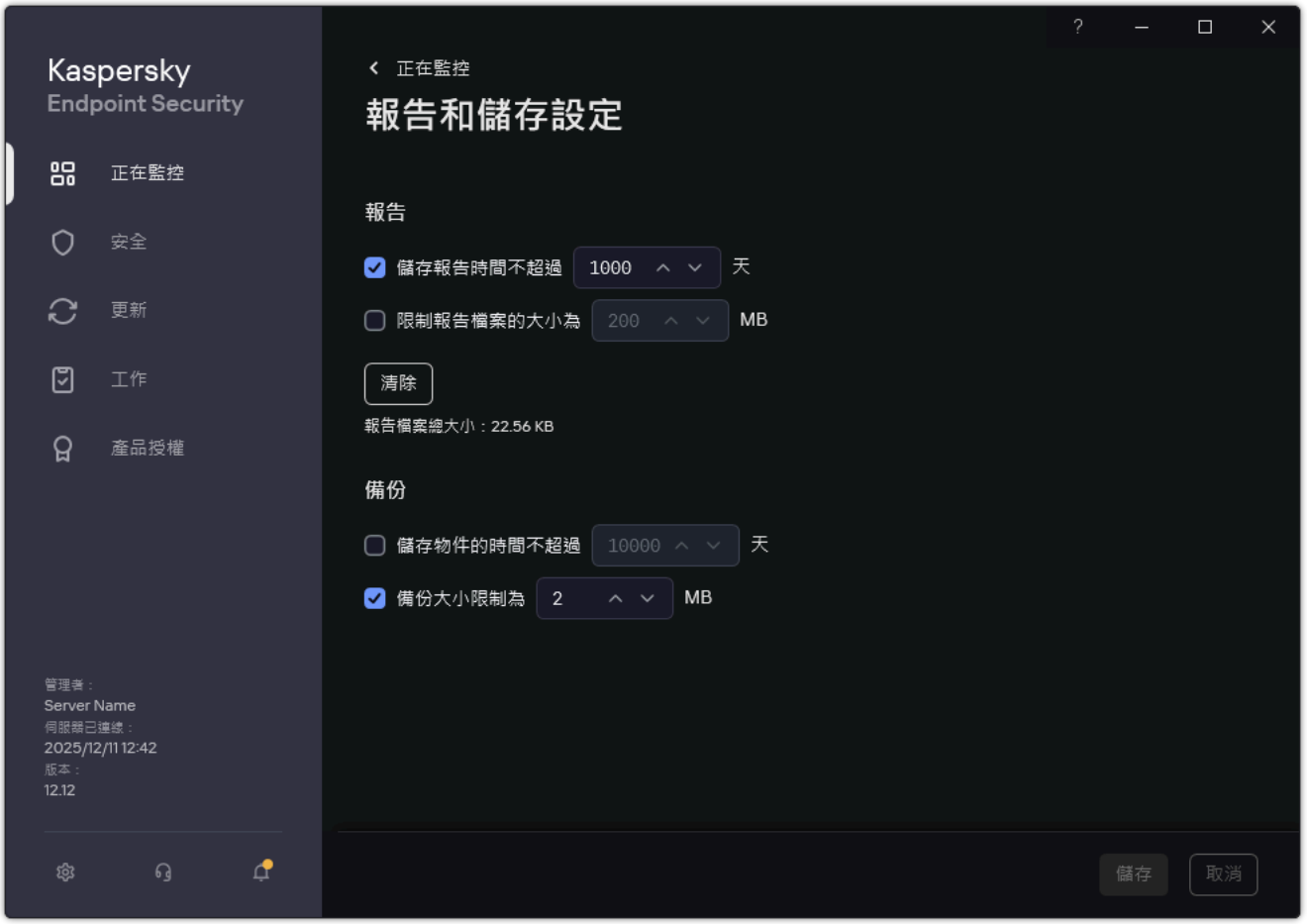
   帶有事件概覽的塊將顯示在視窗的底部。

# 設定最大報告儲存時間

Kaspersky Endpoint Security 記錄的事件報告的最長儲存時間預設為 30 天。在此時間之後，Kaspersky Endpoint Security 將自動移除報告檔案中的最早項目。

*要修改報告的最大儲存期限，請執行下列操作：*

1. 在“應用程式主視窗”中，點擊⚙按鈕。
2. 在應用程式設定視窗中，在 **一般設定** 下面，點擊 **報告和儲存。** 瓷片。




報告設定

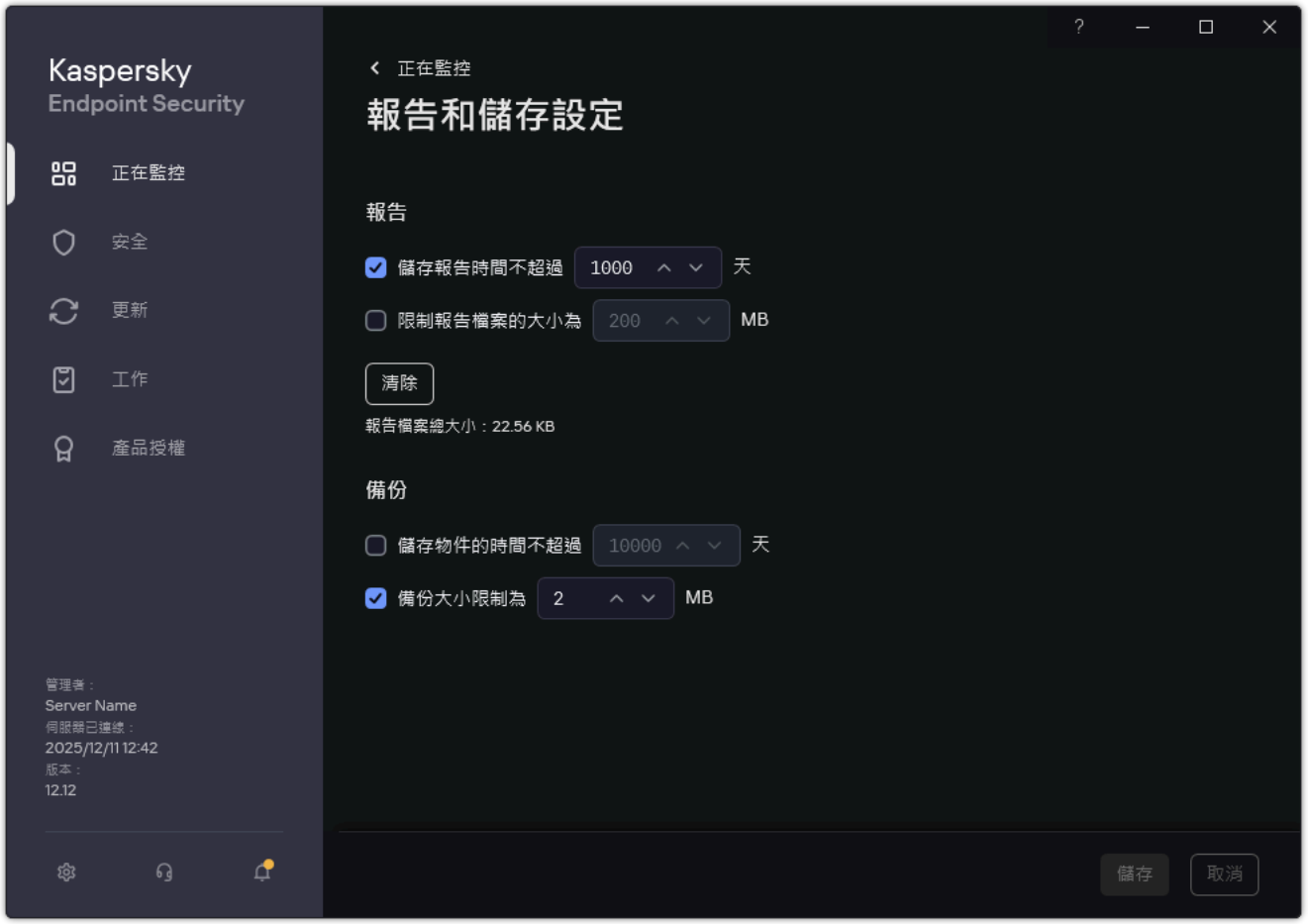
3. 如果要限制報告儲存期限，請選中“**報告**“塊中的“**儲存報告時間不超過 N 天**”核取方塊。定義最大報告儲存期限。
4. 儲存變更。

# 設定報告檔案的最大容量

您可以指定包含報告的檔案的最大容量。預設情況下，最大報告檔案容量為 1024 MB。要避免超過最大報告檔案容量，當達到最大報告檔案容量時，Kaspersky Endpoint Security 將自動刪除報告檔案中的最早項目。

*要設定報告檔案的最大容量，請執行以下操作：*

1. 在“應用程式主視窗”中，點擊⚙按鈕。
2. 在應用程式設定視窗中，在 **一般設定** 下面，點擊 **報告和儲存。** 瓷片。




報告設定

3. 如果要限制報告檔案的大小，請在“**報告**“塊中選中“**限制報告檔案的大小為 N MB**”核取方塊。定義報告檔案的最大容量。
4. 儲存變更。

# 將報告儲存到檔案

使用者個人負責確保儲存為檔案的報告的資訊安全，尤其是控制和限制存取該資訊。

您可以將所產生的報告儲存到內容格式 (TXT) 檔案或 CSV 檔案中。

Kaspersky Endpoint Security 在報告中記錄事件的方式與其在螢幕上的顯示方式相同，換言之，兩者使用相同的事件內容和序列。

*要將報告儲存到檔案中，請執行下列操作：*

1. 在應用程式主視窗的“**正在監控**”區域中，點擊“**報告**”圖標。




報告

2. 這將開啟一個視窗；在此視窗中，選擇元件或者工作。
   報告顯示在視窗的右側，其中包含所選 Kaspersky Endpoint Security 元件或工作操作中事件的清單。

3. 如有必要，您可以透過下列方法修改報告中的資料呈現方式：

   - 篩選事件
   - 執行事件搜尋
   - 欄位重新排列
   - 事件排序

4. 點選視窗右上部的“**儲存報告**”按鈕。

5. 在開啟的視窗中，指定報告檔案的目的資料夾。

6. 輸入報告檔案名稱。

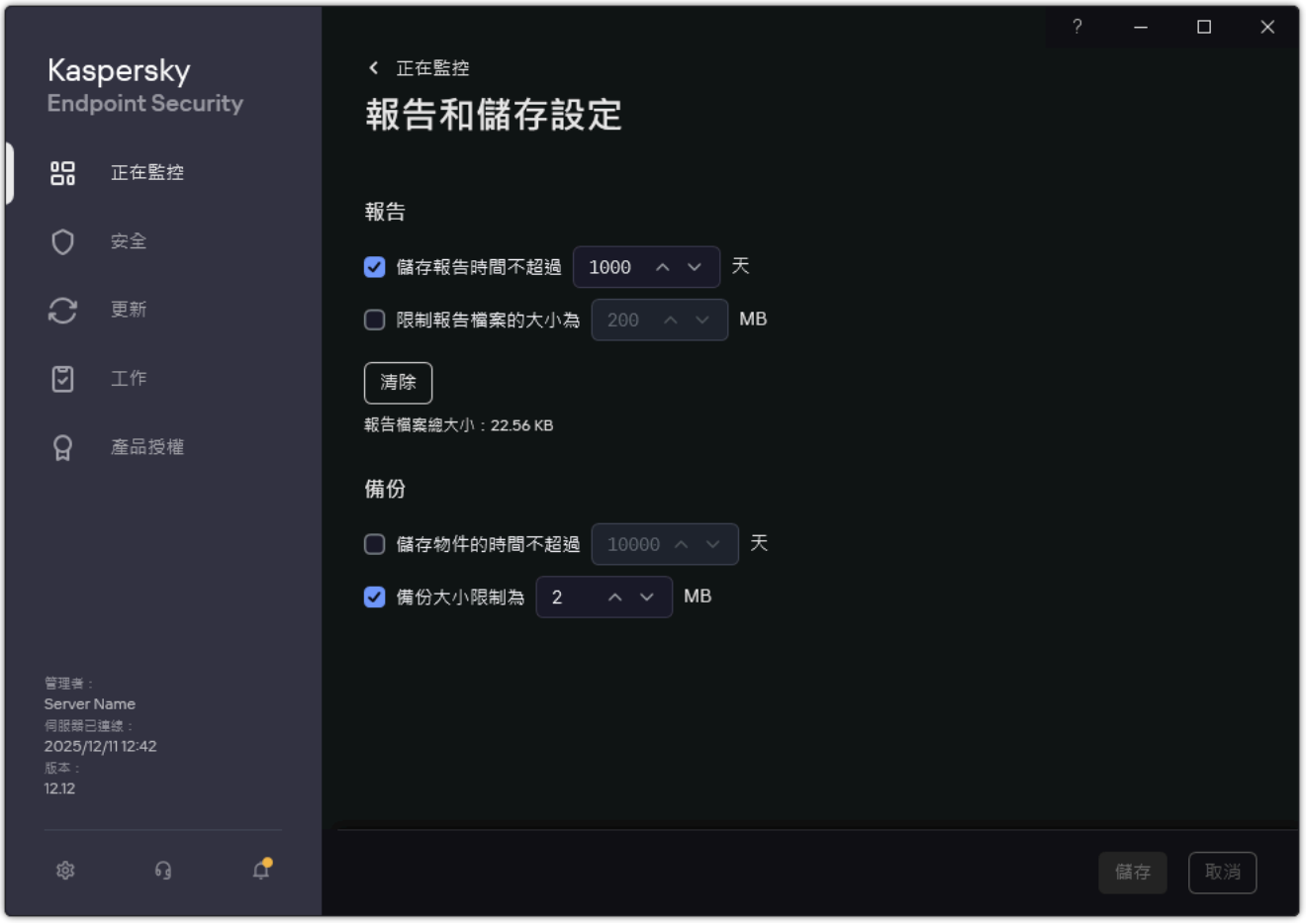
7. 選擇所需報告檔案格式：TXT 或 CSV。

8. 儲存變更。

# 清理報告

*要刪除報告中的資訊，請執行下列操作:*

1. 在"應用程式主視窗"中，點擊⚙按鈕。
2. 在應用程式設定視窗中，在 **一般設定** 下面，點擊 **報告和儲存。** 瓷片。




報告設定

3. 在"**報告**"塊中，點擊"**清除**"按鈕。
4. 如果啟用了密碼防護 ，Kaspersky Endpoint Security 可能會提示您輸入使用者帳戶憑據。如果使用者沒有所需的權限，則應用程式將提示使用者提供帳戶憑據。

Kaspersky Endpoint Security 將刪除所有應用程式元件和工作的所有報告。

# Kaspersky Endpoint Security 自我防護

自我防護可防止其他應用程式執行可能干預 Kaspersky Endpoint Security 的操作和，例如，從電腦移除 Kaspersky Endpoint Security 的操作。對 Kaspersky Endpoint Security 可以使用的自我防護技術集合取決於作業系統是 32 位元還是 64 位元（請參見下表）。自我防禦還包括密碼防護和管理伺服器連線防護。

*密碼防護*允許您根據使用者被授予的權限（例如，結束應用程式的權限）來限制使用者對 Kaspersky Endpoint Security 的存取。

*管理伺服器連線防護* 防止電腦未經授權重新連線到不受信任的伺服器。

Kaspersky Endpoint Security 自我防護技術

| 技術 | 描述 | x86 電腦 | x64 電腦 |
|---|---|---|---|
| **自我防護機制** | 該技術可封鎖對以下應用程式元件的存取：<br>• Kaspersky Endpoint Security 安裝資料夾中的檔案和應用程式的其他檔案；<br>• 記錄屬於應用程式的登錄機碼；<br>• 應用程式執行的處理程序。 | ✓ | ✓ |
| **AM-PPL（惡意軟體防護受防護輕型處理程序）** | 該技術可防護 Kaspersky Endpoint Security 處理程序抵禦惡意操作。有關 AM-PPL 技術的詳細資訊，請存取 Microsoft 網站。<br>AM-PPL 技術適用於 Windows 10 版本 1703 (RS2) 或更高版本以及 Windows Server 2019 作業系統。 | ✓ | ✓ |
| **外部管理防護機制** | 該技術可防止其他應用程式（例如，TeamViewer 或者 RemotelyAnywhere）獲取對 Kaspersky Endpoint Security 的存取權限。 | ✓ | –<br>（Windows 7 除外） |

# 啟用和停用自我防護

Kaspersky Endpoint Security 可避免修改或刪除磁碟機中的應用程式檔案、記憶體程序和系統登錄中的項目。該技術可封鎖對以下應用程式元件的存取：

- Kaspersky Endpoint Security 安裝資料夾中的檔案和應用程式的其他檔案；
- 記錄屬於應用程式的登錄機碼；
- 應用程式執行的處理程序。

預設情況下已啟用 Kaspersky Endpoint Security 的自我防護機制。

**如何在管理主控台（MMC）中啟用或停用自我防護**

1. 在卡巴斯基安全管理中心管理主控台樹狀目錄中，選取**政策**。
2. 選擇必要的政策並點擊以開啟政策內容。
3. 在政策視窗中，選擇“**一般設定 → 應用程式設定**”。

4. 使用“**啟用自我防護**”核取方塊可以啟用或停用自我防護機制。

5. 儲存變更。

**如何在網頁主控台和雲端主控台中啟用或停用自我防護**

1. 在網頁主控台的主視窗中，選擇**資產（裝置）→政策和設定檔**。

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. 使用“**自我防護已啟用**”切換開關可以啟用或停用自我防護機制。

6. 儲存變更。

**如何在應用程式介面中啟用或停用自我防護**

1. 在“應用程式主視窗”中，點擊⚙按鈕。

2. 在應用程式設定視窗中，選取”**一般設定**“→“**應用程式設定**”。




Kaspersky Endpoint Security for Windows 設定

3. 使用“**啟用自我防護**”核取方塊可以啟用或停用自我防護機制。

4. 儲存變更。

# 啟用和停用 AM-PPL 支援

Kaspersky Endpoint Security 支援 Microsoft 的Antimalware Protected Process Light技術（以下簡稱"AM-PPL"）。AM-PPL 防護 Kaspersky Endpoint Security 處理程序免受惡意操作（例如，終止應用程式）。AM-PPL 僅允許執行受信任的處理程序。Kaspersky Endpoint Security 處理程序根據 Windows 安全需求進行簽章，因此它們是受信任的。有關 AM-PPL 技術的詳細資訊，請存取 Microsoft 網站。預設情況下啟用 AM-PPL 技術。

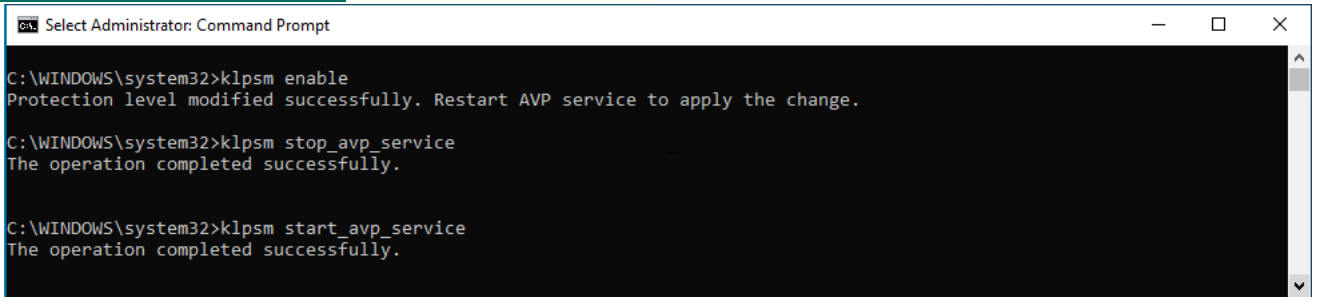
Kaspersky Endpoint Security 還具有用於防護應用程式處理程序的內建機制。AM-PPL 支援允許您將處理程序安全功能委派給作業系統。從而可以提高應用程式的速度並減少電腦資源的消耗。

請持續使用 AM-PPL 技術。AM-PPL 是作業系統防護的重要組成部分。停用 AM-PPL 支援可能會導致某些 Kaspersky Endpoint Security 功能失效（例如，應用程式與 Windows Security Center 的整合）。僅允許在單獨的測試環境中出於故障排除目的停用 AM-PPL 支援。

AM-PPL 技術適用於 Windows 10 版本 1703 (RS2) 或更高版本以及 Windows Server 2019 作業系統。

*要啟用或停用 AM-PPL 技術：*

1. 關閉應用程式的自我防護機制。
   自我防護機制會封鎖修改和刪除電腦記憶體中的應用程式處理程序，包括變更 AM-PPL 狀態。
2. 以管理員身分執行命令列解譯器 (cmd.exe)。
3. 轉到 Kaspersky Endpoint Security 可執行檔所在資料夾。
   您可以在應用程式安裝期間將可執行檔的路徑新增到 %PATH% 系統變數。
4. 在命令列中輸入以下指令：
   - `klpsm.exe enable` – 啟用對 AM-PPL 技術的支援（請參見下圖）。
   - `klpsm.exe disable` – 停用對 AM-PPL 技術的支援。
5. 重新啟動 Kaspersky Endpoint Security。
6. 還原應用程式的自我防護機制。




啟用對 AM-PPL 技術的支援

# 防護應用程式服務抵禦外部管理

防護應用程式服務抵禦外部管理可封鎖使用者和其它應用程式嘗試停止 Kaspersky Endpoint Security 服務。防護可確保以下服務的作業：

- Kaspersky Endpoint Security 服務 (AVP.KES.12.12)
- Kaspersky Seamless Update Service 服務（ AVPSUS.KES.12.12 ）

要從命令列退出結束應用程式，請停用針對外部管理的 Kaspersky Endpoint Security 服務防護。

您只能在不支援 AM-PPL 技術或停用了該技術的電腦上允許對應用程式服務進行外部管理。

**如何在管理主控台 (MMC) 中啟用或停用防護應用程式服務抵禦外部管理**

1. 在卡巴斯基安全管理中心管理主控台樹狀目錄中，選取**政策**。
2. 選擇必要的政策並點擊以開啟政策內容。
3. 在政策視窗中，選擇"**一般設定 → 應用程式設定**"。
4. 使用"**封鎖應用程式服務的外部管理**"核取方塊來啟用或停用針對外部管理的 Kaspersky Endpoint Security 服務防護。
5. 儲存變更。

**如何在網頁主控台和雲端主控台中啟用或停用防護應用程式服務抵禦外部管理**

1. 在網頁主控台的主視窗中，選擇**資產（裝置） → 政策和設定檔**。
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. 使用"**封鎖應用程式服務的外部管理**"核取方塊來啟用或停用針對外部管理的 Kaspersky Endpoint Security 服務防護。
6. 儲存變更。

**如何在應用程式介面中啟用或停用防護應用程式服務抵禦外部管理**

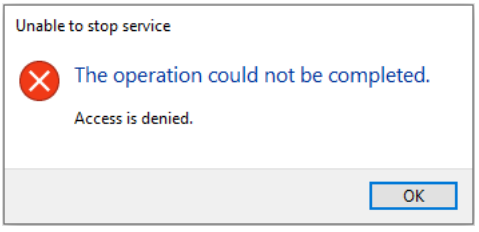
1. 在"應用程式主視窗"中，點擊⚙按鈕。
2. 在應用程式設定視窗中，選取"**一般設定**"→"**應用程式設定**"。




Kaspersky Endpoint Security for Windows 設定

3. 使用"**封鎖應用程式服務的外部管理**"核取方塊來啟用或停用針對外部管理的 Kaspersky Endpoint Security 服務防護。
4. 儲存變更。

結果，當使用者嘗試停止應用程式服務時，會出現一個帶有錯誤訊息的系統視窗。使用者只能從 Kaspersky Endpoint Security 介面管理應用程式服務。




應用程式服務存取錯誤

# 支援遠端管理應用程式

在啟用外部管理防護後，您可能偶爾會需要使用遠端管理應用程式。

*若要啟用遠端系統管理應用程式的操作，請執行以下操作：*

1. 在"應用程式主視窗"中，點擊 按鈕。
2. 在應用程式設定視窗中，選取"**一般設定**"→"**排除項目和偵測到的物件類型**"。
3. 在"**排除項目**"塊中，點擊"**指定受信任應用程式**"連接。
4. 在開啟的視窗中，點擊"**新增**"按鈕。
5. 選擇遠端管理應用程式的可執行檔。

   您也可以手動輸入路徑。Kaspersky Endpoint Security 輸入遮罩時支援環境變量以及`*`和`?`字元。
6. 選擇"**允許與 Kaspersky Endpoint Security 的應用程式介面進行互動**"核取方塊。
7. 儲存變更。

# 密碼防護

多個不同電腦知識水準的使用者可以共用一台電腦。如果使用者可以無限制存取 Kaspersky Endpoint Security 及其設定，則電腦防護的層級可能會下降。密碼防護允許您根據使用者被授予的權限（例如，結束應用程式的權限）來限制使用者對 Kaspersky Endpoint Security 的存取。

如果啟動 Windows 連線的使用者（*連線使用者*）擁有執行操作的權限，則 Kaspersky Endpoint Security 不會請求使用者名稱和密碼或臨時密碼。使用者將按照授予的權限獲得 Kaspersky Endpoint Security 的存取權限。

如果連線使用者沒有執行操作的權限，該使用者可以透過以下方式獲得應用程式的存取權限：

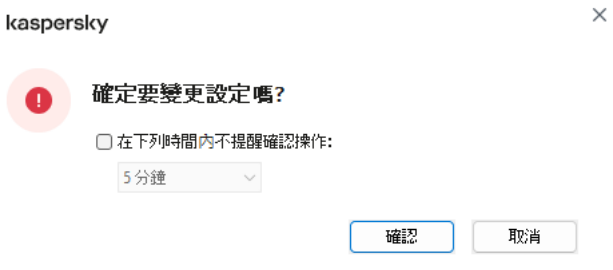
- 輸入使用者名稱和密碼。

  此方法適合日常操作。要執行受密碼防護的操作，必須輸入具有所需權限的使用者的網域帳戶憑證。在這種情況下，電腦必須位於該網域中。如果電腦不在網域中，您可以使用 KLAdmin 帳戶或手動新增帳戶。
- 輸入暫時密碼。

  此方法適合為公司網路外部的使用者授予執行被封鎖操作（例如，結束應用程式）的暫時權限。當暫時密碼到期或連線結束後，Kaspersky Endpoint Security 會將其設定還原為先前狀態。

當使用者嘗試執行受密碼防護的操作時，Kaspersky Endpoint Security 會提示使用者輸入使用者名稱和密碼或者暫時密碼（請參見下圖）。

在密碼輸入視窗中，您只可以透過按 **ALT+SHIFT**來切換語言。使用其他捷徑（即使他們在作業系統中進行了配置）對切換語言無效。




Kaspersky Endpoint Security 存取密碼提示

## 使用者名稱和密碼

要存取 Kaspersky Endpoint Security，您應該輸入帳戶憑證。密碼防護支援以下帳戶：

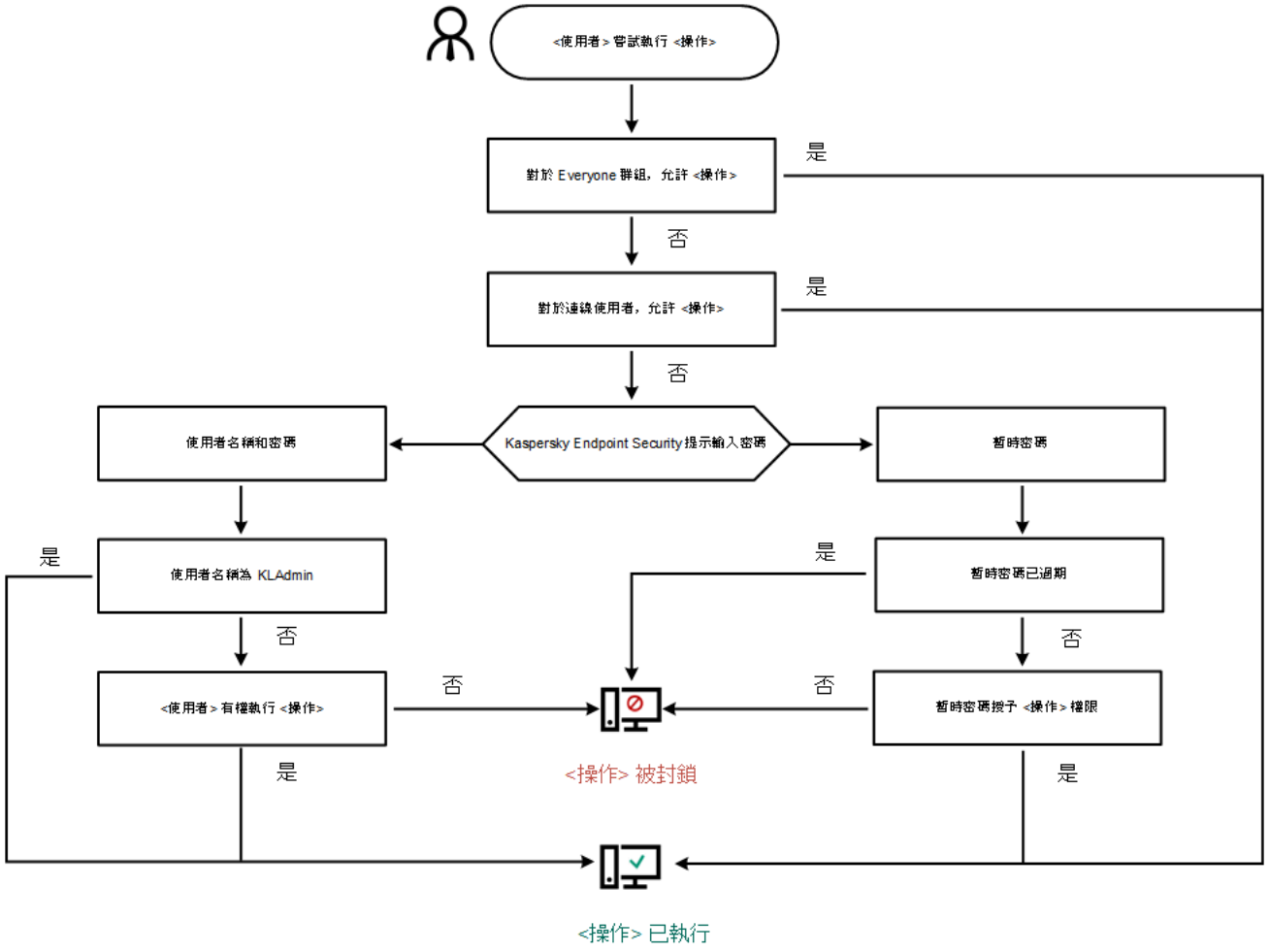
- **KLAdmin**。具有 Kaspersky Endpoint Security 無限制存取權限的管理員帳戶。KLAdmin 帳戶有權執行任何受密碼防護的操作。KLAdmin 帳戶的權限無法撤銷。當啟用密碼防護時，Kaspersky Endpoint Security 會提示您設定 KLAdmin 帳戶的密碼。
- **手動新增的帳戶**。一個 Active Directory 網域之外的帳戶。如果不想共用管理員密碼，您可以使用該服務帳戶而不是 KLAdmin。您可以使用任何使用者名稱和密碼並設定單個權限。
- **Everyone 群組**。Windows 內建的群組，包括公司網路內的所有使用者。Everyone 群組中的使用者可以根據其被分配的權限存取應用程式。
- **單個使用者或群組**。可以為其配置單個權限的使用者帳戶。例如，如果針對 Everyone 群組封鎖某個操作，您可以允許單個使用者或群組執行該操作。
- **連線使用者**。啟動了 Windows 連線的使用者帳戶。當系統提示輸入密碼時，您可以轉換到其他連線使用者（"**儲存目前連線的密碼**"核取方塊）。此時，Kaspersky Endpoint Security 會將輸入了帳戶憑證的使用者（而不是啟動了 Windows 連線的使用者）視為連線使用者。

## 暫時密碼

暫時密碼可用於授權公司網路外部的單台電腦暫時存取 Kaspersky Endpoint Security。管理員在卡巴斯基安全管理中心的電腦內容中為單台電腦生成暫時密碼。管理員選取將以暫時密碼防護的操作，並指定暫時密碼的有效期。

密碼防護操作演算法

Kaspersky Endpoint Security 根據以下演算法決定是允許還是封鎖受密碼防護的操作（請參見下圖）。




密碼防護操作演算法

# 啟用密碼防護

密碼防護允許您根據使用者被授予的權限（例如，結束應用程式的權限）來限制使用者對 Kaspersky Endpoint Security 的存取。

**如何在管理主控台 (MMC) 中啟用密碼防護**

1. 在卡巴斯基安全管理中心管理主控台樹狀目錄中，選取**政策**。
2. 選擇必要的政策並點擊以開啟政策內容。
3. 在政策視窗中，選擇"**一般設定 → 介面**"。
4. 在"**密碼防護**"塊中，點擊"**設定**"按鈕。
   這將開啟一個帶有密碼防護設定的視窗。
5. 使用"**啟用密碼防護**"核取方塊來啟用或停用元件。

6. 在 **權限**下面，選擇 KLAdmin 帳戶。
7. 這會開啟一個視窗；在該視窗中，點擊 **密碼** 並為 KLAdmin 帳戶設定密碼。
   KLAdmin 帳戶有權執行任何受密碼防護的操作。

   如果忘記了 KLAdmin 帳戶密碼，您可以在政策內容中重設密碼。
8. 返回帳戶清單。
9. 設定公司網路內所有使用者的權限：
   a. 在**權限**下面，選擇"所有人"群組。
      *Everyone 群組*是 Windows 內建的群組，包括公司網路內的所有使用者。
   b. 在開啟的視窗中，選中使用者不必輸入密碼即可執行的操作旁邊的核取方塊。
      如果清除某個核取方塊，使用者將被封鎖執行相應操作。例如，如果清除"**結束應用程式** "權限旁邊的核取方塊，則只有您以 KLAdmin 身分登入或者以擁有所需權限的單個使用者身分登入或者輸入暫時密碼才能結束應用程式。

      密碼防護權限有幾個需要考慮的重要方面。確保已滿足存取 Kaspersky Endpoint Security 的所有條件。
10. 儲存變更。

**如何在網頁主控台和雲端主控台中啟用密碼防護**

1. 在網頁主控台的主視窗中，選擇**資產（裝置）→政策和設定檔**。
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. 在**密碼防護**下面，使用"**密碼防護已啟用**"切換開關可啟用或停用元件。
6. 指定 KLAdmin 帳戶的密碼並確認。
   KLAdmin 帳戶有權執行任何受密碼防護的操作。

   如果忘記了 KLAdmin 帳戶密碼，您可以在政策內容中重設密碼。
7. 返回帳戶清單。
8. 設定公司網路內所有使用者的權限：
   a. 在帳戶表中，選擇"所有人"群組。
      *Everyone 群組*是 Windows 內建的群組，包括公司網路內的所有使用者。

b. 在開啟的視窗中，選中使用者不必輸入密碼即可執行的操作旁邊的核取方塊。

如果清除某個核取方塊，使用者將被封鎖執行相應操作。例如，如果清除**"結束應用程式"**權限旁邊的核取方塊，則只有您以 KLAdmin 身分登入或者以擁有所需權限的單個使用者身分登入或者輸入暫時密碼才能結束應用程式。

密碼防護權限有幾個需要考慮的重要方面。確保已滿足存取 Kaspersky Endpoint Security 的所有條件。

9. 儲存變更。

**如何在應用程式介面中啟用密碼防護**

1. 在"應用程式主視窗"中，點擊⚙ 按鈕。
2. 在應用程式設定視窗中，選取"**一般設定**"→"**介面**"。
3. 使用"**密碼防護**"切換開關可啟用或停用元件。
4. 指定 KLAdmin 帳戶的密碼並確認。

KLAdmin 帳戶有權執行任何受密碼防護的操作。

如果電腦在某個政策下執行，管理員可以在政策內容中重設 KLAdmin 帳戶的密碼。如果電腦未連線到卡巴斯基安全管理中心並且您忘記了 KLAdmin 帳戶的密碼，則無法還原密碼。

5. 設定公司網路內所有使用者的權限：

a. 在帳戶表中，點擊**"編輯"**以開啟 Everyone 群組的權限清單。

*Everyone 群組*是 Windows 內建的群組，包括公司網路內的所有使用者。

b. 選中使用者不必輸入密碼即可執行的操作旁邊的核取方塊。

如果清除某個核取方塊，使用者將被封鎖執行相應操作。例如，如果清除**"結束應用程式"**權限旁邊的核取方塊，則只有您以 KLAdmin 身分登入或者以擁有所需權限的單個使用者身分登入或者輸入暫時密碼才能結束應用程式。

密碼防護權限有幾個需要考慮的重要方面。確保已滿足存取 Kaspersky Endpoint Security 的所有條件。

6. 儲存變更。

啟用密碼防護後，應用程式將根據 Everyone 群組被授予的權限來限制使用者對 Kaspersky Endpoint Security 的存取。只有您使用 KLAdmin 帳戶，使用被授予所需權限的其他帳戶或者輸入暫時密碼時，才能執行 Everyone 群組被封鎖的操作。

僅當您以 KLAdmin 身分登入時，才能停用密碼防護。如果您使用任何其他使用者帳戶或臨時密碼，則無法停用密碼防護。

在密碼檢查期間，可以選中**"儲存目前連線的密碼"**核取方塊。在這種情況下，當使用者嘗試在連線期間執行其他受密碼防護的操作時，Kaspersky Endpoint Security 不會提示輸入密碼。

# 為單個使用者或群組授予權限

密碼防護允許授予 Kaspersky Endpoint Security 對單個 Active Directory 使用者帳戶和手動新增的使用者帳戶進行存取的權限。

## Active Directory 使用者帳戶

您可以授予 Kaspersky Endpoint Security 對 Active Directory 網域內的當個使用者或群組進行存取的權限。例如，如果 Everyone 群組被封鎖結束應用程式，您可以將**"結束應用程式"**權限授予給單個使用者。這樣，只有以該使用者或以 KLAdmin 身分登入時才能結束應用程式。

僅當電腦位於網域中時，才能使用帳戶憑證存取應用程式。如果電腦不在網域中，您可以使用 KLAdmin 帳戶或臨時密碼。

## 手動新增的使用者帳戶

您可以建立一個不在 Active Directory 中的使用者帳戶並向該使用者帳戶指派單個權限。即您可以建立一個*服務使用者帳戶*並使用它而不是 KLAdmin。這樣，您就無需與其他使用者共用您的 KLAdmin 密碼或建立新的 Active Directory 使用者帳戶。您可以指定任何使用者名稱和密碼。例如，您可以向服務使用者帳戶授予**檢視報告**權限。因此，如果對"All"群組禁止了檢視報告，您可以使用服務使用者帳戶或 KLAdmin 使用者帳戶開啟報告。

## 為單個使用者或群組授予權限

**如何在管理主控台 (MMC) 中為單個使用者或群組授予權限**

1. 在卡巴斯基安全管理中心管理主控台樹狀目錄中，選取**政策**。
2. 選擇必要的政策並點擊以開啟政策內容。
3. 在政策視窗中，選擇**"一般設定 → 介面"**。
4. 在**"密碼防護"**塊中，點擊**"設定"**按鈕。
   這將開啟一個帶有密碼防護設定的視窗。
5. 在帳戶表中，點擊**新增**。
6. 選擇您想要新增的使用者帳戶類型：
   - **從 Active Directory 中選擇一個使用者/群組** – Active Directory 使用者帳戶。
     選取使用者帳戶請點擊**選擇**。選取 Active Directory 中的使用者或群組，然後確認選取。
   - **手動新增使用者/群組** 用於手動新增的服務使用者帳戶。

若要新增服務使用者帳戶，請輸入使用者名稱和密碼（例如，SecureAdmin）。

您可以在政策設定中重設服務使用者帳戶密碼。重設使用者服務帳戶密碼的方式必須與重設 KLAdmin 密碼的方式一樣。如果允許編輯密碼防護設定（"鎖"開啟）或電腦上沒有套用任何政策，您可以在應用程式介面中重設服務使用者帳戶的密碼。為此，確認使用 KLAdmin 密碼的服務使用者帳戶資訊的變更。

7. 在"**權限**"清單中，選中選定使用者或群組在不被提示輸入密碼的情況下即可執行的操作旁邊的核取方塊。

   如果清除某個核取方塊，使用者將被封鎖執行相應操作。例如，如果清除"**結束應用程式**"權限旁邊的核取方塊，則只有您以 KLAdmin 身分登入或者以擁有所需權限的單個使用者身分登入或者輸入暫時密碼才能結束應用程式。

   密碼防護權限有幾個需要考慮的重要方面。確保已滿足存取 Kaspersky Endpoint Security 的所有條件。

8. 儲存變更。

**如何在網頁主控台和雲端主控台中向單個使用者或群組授予權限**

1. 在網頁主控台的主視窗中，選擇**資產（裝置）→ 政策和設定檔**。
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. 在"**密碼防護**"塊中，點擊"**使用者權限**"連接。

   這將開啟"啟用密碼"權限授予表單。
6. 點擊"**新增**"。
7. 選擇您想要新增的使用者帳戶類型：

   - **從 Active Directory 選擇** – Active Directory 使用者帳戶。

     選取使用者帳戶請點擊**編輯**。選取 Active Directory 中的使用者或群組，然後確認選取。
   - **手動新增** 用於手動新增的服務使用者帳戶。

     若要新增服務使用者帳戶，請輸入使用者名稱和密碼（例如，SecureAdmin）。

     您可以在政策設定中重設服務使用者帳戶密碼。重設使用者服務帳戶密碼的方式必須與重設 KLAdmin 密碼的方式一樣。如果允許編輯密碼防護設定（"鎖"開啟）或電腦上沒有套用任何政策，您可以在應用程式介面中重設服務使用者帳戶的密碼。為此，確認使用 KLAdmin 密碼的服務使用者帳戶資訊的變更。
8. 在"**權限**"清單中，選中選定使用者或群組在不被提示輸入密碼的情況下即可執行的操作旁邊的核取方塊。

   如果清除某個核取方塊，使用者將被封鎖執行相應操作。例如，如果清除"**結束應用程式**"權限旁邊的核取方塊，則只有您以 KLAdmin 身分登入或者以擁有所需權限的單個使用者身分登入或者輸入暫時密碼才能結束應用程式。

密碼防護權限有幾個需要考慮的重要方面。確保已滿足存取 Kaspersky Endpoint Security 的所有條件。

9. 點擊**"新增"**。
10. 儲存變更。

**如何在應用程式的使用者介面中為單個使用者或群組授予權限**

1. 在"應用程式主視窗"中，點擊⚙ 按鈕。
2. 在應用程式設定視窗中，選取"**一般設定**"→"**介面**"。
3. 在帳戶表中，點擊**新增**。
4. 選擇您想要新增的使用者帳戶類型：
   - **從 Active Directory 中選擇一個使用者/群組** – Active Directory 使用者帳戶。
     選取使用者帳戶請點擊**選擇使用者或群組**。選取 Active Directory 中的使用者或群組，然後確認選取。
   - **手動新增使用者** 用於手動新增的服務使用者帳戶。
     若要新增服務使用者帳戶，請輸入使用者名稱和密碼（例如，SecureAdmin）。

     您可以在政策設定中重設服務使用者帳戶密碼。重設使用者服務帳戶密碼的方式必須與重設 KLAdmin 密碼的方式一樣。如果允許編輯密碼防護設定（"鎖"開啟）或電腦上沒有套用任何政策，您可以在應用程式介面中重設服務使用者帳戶的密碼。為此，確認使用 KLAdmin 密碼的服務使用者帳戶資訊的變更。
5. 在"**權限**"清單中，選中選定使用者或群組在不被提示輸入密碼的情況下即可執行的操作旁邊的核取方塊。
   如果清除某個核取方塊，使用者將被封鎖執行相應操作。例如，如果清除"**結束應用程式**"權限旁邊的核取方塊，則只有您以 KLAdmin 身分登入或者以擁有所需權限的單個使用者身分登入或者輸入暫時密碼才能結束應用程式。

   密碼防護權限有幾個需要考慮的重要方面。確保已滿足存取 Kaspersky Endpoint Security 的所有條件。
6. 儲存變更。

結果，如果限制了 Everyone 群組存取應用程式，將根據使用者的單個權限授予使用者存取 Kaspersky Endpoint Security 的權限。

# 使用暫時密碼授予權限

暫時密碼可用於授權公司網路外部的單台電腦暫時存取 Kaspersky Endpoint Security。要允許使用者在不獲取 KLAdmin 帳戶憑證的情況下執行被封鎖的操作，這是必需的。要使用暫時密碼，必需將電腦新增到卡巴斯基安全管理中心中。

**如何允許使用者透過管理主控台 (MMC) 用暫時密碼執行被封鎖的操作**

1. 開啟卡巴斯基安全管理中心管理主控台。
2. 在管理主控台樹狀目錄的**"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**"裝置"**標籤。
4. 點擊以開啟電腦內容視窗。
5. 在電腦內容視窗中，選取**"應用程式"**區域。
6. 在電腦上安裝的 Kaspersky 應用程式清單中，選取 **Kaspersky Endpoint Security for Windows (12.12)** 並點擊以開啟應用程式內容。
7. 在應用程式設定視窗中，選取**"一般設定"→"介面"**。
8. 在**"密碼防護"**塊中，點擊**"設定"**按鈕。
9. 在開啟的視窗中的 **暫時密碼**塊中，點擊 **暫時密碼清單** 按鈕。
   暫時密碼管理視窗開啟。
10. 點擊**"新增"**。
11. 在**"到期日期"**欄位中，指定暫時密碼的到期日期。
12. 在**"暫時密碼範圍"**表中，選中使用者在輸入暫時密碼後可以執行的操作旁邊的核取方塊。
13. 點擊**"建立"**。
    將開啟一個包含暫時密碼的視窗（請參見下圖）。
14. 複製密碼並將其提供給使用者。

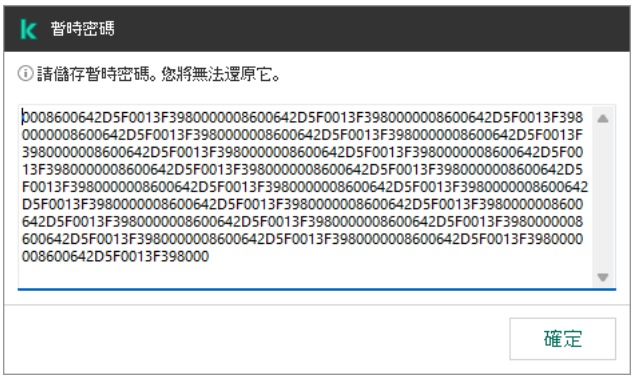
**如何允許使用者透過網頁主控台和雲端主控台用暫時密碼執行被封鎖的操作**

1. 在網頁主控台的主視窗中，選擇**資產（裝置）→ 受管理裝置**。
2. 點擊您想要允許使用者在上面執行被封鎖操作的電腦的名稱。
3. 選擇**"應用程式"**標籤。
4. 點擊**"Kaspersky Endpoint Security for Windows"**。
   這將開啟本機應用程式設定。
5. 選擇**"應用程式設定"**標籤。
6. 在應用程式設定視窗中，選取**"一般設定"→"介面"**。
7. 在**"暫時密碼"**塊中，點擊**"新增"**按鈕。
8. 在**"到期日期"**欄位中，指定暫時密碼的到期日期。
9. 在**"暫時密碼範圍"**表中，選中使用者在輸入暫時密碼後可以執行的操作旁邊的核取方塊。

10. 點擊“**建立**”。

包含暫時密碼的視窗將開啟。

11. 複製密碼並將其提供給使用者。

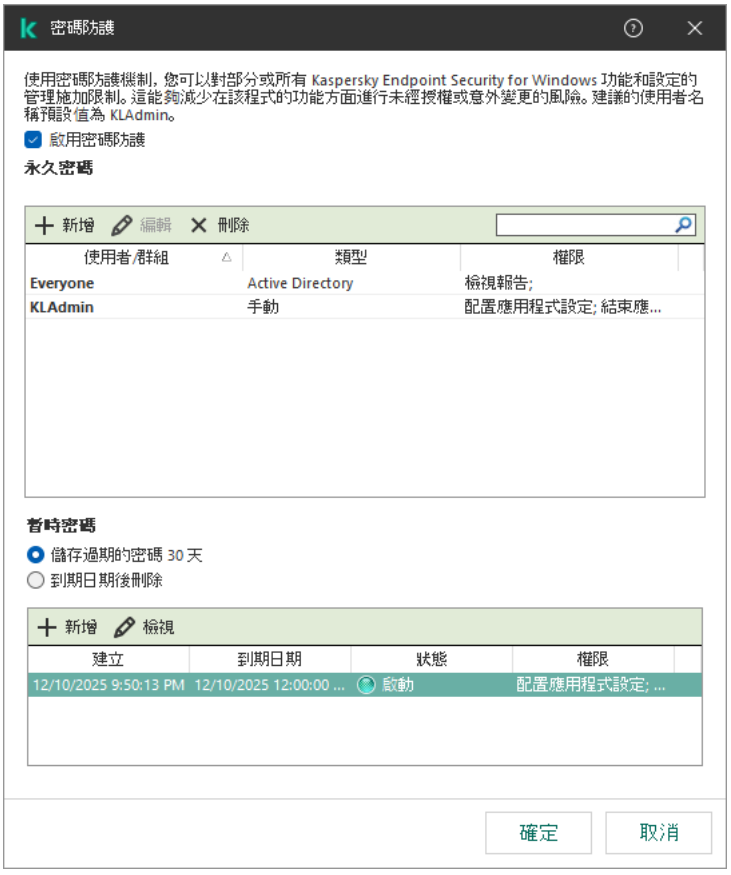



暫時密碼

# 撤銷暫時密碼

從版本 12.9 開始，Kaspersky Endpoint Security for Windows 包括 *管理暫時密碼*功能。管理暫時密碼可讓您執行以下操作：

- 儲存密碼歷史記錄（最多 30 天）。
- 監控暫時密碼狀態：*啟動*，*已到期*，*已吊銷*。
- 撤銷暫時密碼。




暫時密碼管理

暫時密碼管理僅在將電腦與卡巴斯基安全管理中心同步後才更新密碼的狀態並撤銷密碼。

**如何使用管理主控台 (MMC) 撤銷暫時密碼**

1. 開啟卡巴斯基安全管理中心管理主控台。
2. 在管理主控台樹狀目錄的**"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**"裝置"**標籤。
4. 點擊以開啟電腦內容視窗。
5. 在電腦內容視窗中，選取**"應用程式"**區域。
6. 在電腦上安裝的 Kaspersky 應用程式清單中，選取 **Kaspersky Endpoint Security for Windows (12.12)** 並點擊以開啟應用程式內容。
7. 在應用程式設定視窗中，選取**"一般設定"→"介面"**。
8. 在**"密碼防護"**塊中，點擊**"設定"**按鈕。
9. 這將開啟一個視窗；在此視窗的 **暫時密碼** 下面，配置過期密碼的儲存設定。
10. 點擊**"暫時密碼清單"**。

    暫時密碼管理視窗開啟。暫時密碼管理會顯示密碼的有效期限、密碼的狀態和權限清單。
11. 選擇要撤銷的活動暫時密碼，然後雙擊該密碼以開啟其屬性。
12. 在開啟的視窗中，點擊**"吊銷"**按鈕。
13. 儲存變更。若要在電腦上套用該政策，請關閉掛鎖。

**如何使用網頁主控台和雲端主控台撤銷暫時密碼**

1. 在網頁主控台的主視窗中，選擇**資產（裝置）→ 受管理裝置**。
2. 點擊您想要允許使用者在上面執行被封鎖操作的電腦的名稱。
3. 選擇**"應用程式"**標籤。
4. 點擊**"Kaspersky Endpoint Security for Windows"**。

   這將開啟本機應用程式設定。
5. 選擇**"應用程式設定"**標籤。
6. 在應用程式設定視窗中，選取**"一般設定"→"介面"**。
7. 在**暫時密碼**下面，配置過期密碼的儲存。
8. 點擊**"暫時密碼"**連接。

   暫時密碼管理視窗開啟。暫時密碼管理會顯示密碼的有效期限、密碼的狀態和權限清單。
9. 選擇要撤銷的活動暫時密碼。

10. 在開啟的視窗中，點擊**"撤銷密碼"**按鈕。

11. 儲存變更。若要在電腦上套用該政策，請關閉掛鎖。

結果，暫時密碼管理將密碼的狀態設定為 *正在撤銷（正在與主機同步）*。將電腦與卡巴斯基安全管理中心同步後，應用程式會立即撤銷暫時密碼並封鎖授予的權限。

# 密碼防護權限的特殊方面

密碼防護權限有幾個需要考慮的重要方面和限制。

## 配置應用程式設定

如果使用者的電腦在某個政策下執行，請確保政策中的所有必需設定均可編輯（內容是開啟的）。

## 結束應用程式

沒有特殊注意事項或限制。

## 停用防護元件

- 無法為 Everyone 群組授予停用防護元件的權限。要允許除 KLAdmin 之外的使用者停用控制元件，請在"密碼防護"設定中新增具有**"停用防護元件"**權限的使用者或群組。
- 如果使用者的電腦在某個政策下執行，請確保政策中的所有必需設定均可編輯（內容是開啟的）。
- 要在應用程式設定中停用防護元件，使用者必須具有**"配置應用程式設定"**權限。
- 若要從內容功能表中停用防護元件（透過使用**"暫停防護"**功能表項目），除了**"停用防護元件"**權限外，使用者還必須具有**"停用控制元件"**權限。

## 停用控制元件

- 無法為 Everyone 群組授予停用控制元件的權限。要允許除 KLAdmin 之外的使用者停用控制元件，請在"密碼防護"設定中新增具有**"停用控制元件"**權限的使用者或群組。
- 如果使用者的電腦在某個政策下執行，請確保政策中的所有必需設定均可編輯（內容是開啟的）。
- 要在應用程式設定中停用控制元件，使用者必須具有**"配置應用程式設定"**權限。
- 若要從內容功能表中停用控制元件（透過使用**"暫停防護"**功能表項目），除了**"停用防護元件"**權限外，使用者還必須具有**"停用控制元件"**權限。

停用卡巴斯基安全管理中心政策

您不能為"Everyone"群組授予停用卡巴斯基安全管理中心政策的權限。要允許除 KLAdmin 之外的使用者停用政策，請在"密碼防護"設定中新增具有"**停用卡巴斯基安全管理中心政策**"權限的使用者或群組。

移除金鑰

沒有特殊注意事項或限制。

移除/修改/還原應用程式

如果您允許移除、修改和還原"全部"群組的應用程式， 則當使用者嘗試執行這些操作時 Kaspersky Endpoint Security 不要求密碼。因此，任何使用者（包括來自網域之外的使用者）可以安裝、修改或者還原應用程式。

還原加密磁碟資料的存取權限

只有以 KLAdmin 身分登入時，才能還原對加密磁碟機資料的存取。執行此操作的權限不能授予給任何其他使用者。

檢視報告

沒有特殊注意事項或限制。

從備份區還原

沒有特殊注意事項或限制。

設定匯出

預設情況下，對"全部"群組拒絕匯出應用程式設定。您可以使用 KLAdmin 使用者帳戶匯出應用程式設定。匯出應用程式設定僅包括 在應用程式介面中建立包含 Kaspersky Endpoint Security 設定的設定檔案。此權限不限制匯出掃描排除清單、受信任的網址、受信任裝置或應用程式元件維護的其他清單。

# 重設 KLAdmin 密碼

如果忘記了 KLAdmin 帳戶密碼，您可以在政策內容中重設密碼。您不能在應用程式介面中重設密碼。

您可以使用暫時密碼執行密碼防護的動作。在此情況下，您無需輸入 KLAdmin 憑據。

如果電腦未連線到卡巴斯基安全管理中心並且您忘記了 KLAdmin 帳戶的密碼，則無法還原密碼。

**如何使用管理主控台 (MMC) 重設 KLAdmin 帳戶密碼**

1. 在卡巴斯基安全管理中心管理主控台樹狀目錄中，選取**政策**。
2. 選擇必要的政策並點擊以開啟政策內容。
3. 在政策視窗中，選擇"**一般設定 → 介面**"。
4. 在"**密碼防護**"塊中，點擊"**設定**"按鈕。
5. 在開啟的視窗中，清除"**啟用密碼防護**"核取方塊。
6. 儲存變更。
7. 再次選擇"**啟用密碼防護**"核取方塊。
8. 點擊"**確定**"。
   這將開啟"管理員密碼"視窗。
9. 指定 KLAdmin 帳戶的新密碼並確認。
10. 儲存變更。

**如何在網頁主控台和雲端主控台中重設 KLAdmin 帳戶密碼**

1. 在網頁主控台的主視窗中，選擇**資產（裝置）→ 受管理裝置**。
2. 選取要為其配置本機應用程式設定的電腦。
   這將開啟電腦內容。
3. 選擇"**應用程式**"標籤。
4. 點擊"**Kaspersky Endpoint Security for Windows**"。
   這將開啟本機應用程式設定。
5. 選擇"**應用程式設定**"標籤。
6. 轉到"**一般設定**"→"**自我防護**"。
7. 在"**密碼防護**"下方，關閉"**密碼防護**"開關。
8. 儲存變更。

9. 再次開啟“**密碼防護**”開關。

10. 指定 KLAdmin 帳戶的新密碼並確認。

11. 儲存變更。

因此，您的 KLAdmin 帳戶的密碼會在套用政策後得到更新。

# 管理員伺服器連線防護

將電腦連線到管理伺服器透過使用卡巴斯基安全管理中心的*網路代理*元件實現。如果入侵者有足夠的權限修改伺服器連線設定，則存在將電腦連線到不受信任的伺服器的風險。這將允許入侵者套用他們自己的群組政策和（例如）停用應用程式自我防禦。Kaspersky Endpoint Security 可以防止未經授權將電腦重新連線到不同伺服器。為了防護伺服器連線，應用程式會建議設定一個密碼並使用Password-Based key Derivation Function (PBKDF2)。結果，不可能沒有密碼而存取應用程式。

為了確保全面防護 Kaspersky Endpoint Security 和網路代理免於未經授權的存取，我們建議啟用額外防護。對於 Kaspersky Endpoint Security，我們建議啟用密碼防護。為了防護網路代理，我們建議設定解除安裝密碼。有關防護網路代理被移除的詳細資訊，請參閱卡巴斯基安全管理中心說明。

管理將電腦連線到管理伺服器透過使用*管理伺服器連線防護*工作實現。該工作允許您執行以下操作：

- 設定密碼以防護伺服器連線。
- 變更密碼。
- 將電腦重新連線到不同伺服器。
- 停用伺服器連線防護。

## 連線到管理伺服器時對電腦進行身分驗證

設定密碼後，應用程式將使用密碼的 PBKDF2 轉換方法建立一個資料陣列。應用程式然後會使用網路代理金鑰加密該資料陣列。應用程式會使用加密的資料陣列來檢查管理伺服器的權限用於隨後連線。

隨後，只要有嘗試將電腦重新連線到管理伺服器，應用程式就會用網路代理金鑰解密資料陣列並將其與本機副本比對。如果他們不比對，應用程式存取將受到限制。

## 管理員伺服器連線防護

### 如何在管理主控台 (MMC) 中設定伺服器連線防護密碼

1. 在卡巴斯基安全管理中心管理主控台樹狀目錄中，選取**工作**。

   工作清單開啟。

2. 點擊“**新工作**”。

啟動“工作精靈”。按照精靈的說明進行操作。

### 步驟 1. 選取工作類型

選取“**Kaspersky Endpoint Security for Windows (12.12)**”→“**管理伺服器連線防護**”。

### 步驟 2. 防護管理伺服器連線

設定密碼以防護管理伺服器連線：

1. 在**管理伺服器連線防護**下面，選擇**用密碼防護**。
2. 在“**管理伺服器**”下拉式清單中，選取“**新伺服器**”。
3. 在**連線至管理伺服器的密碼**欄位中，設定管理伺服器連線密碼並進行確認。

   如果忘記了密碼，您可以使用工作變更密碼。
4. 如果您部署了 Kaspersky Endpoint Security 12.7 或更早版本的應用程式，請選擇 **為先前的應用程式版本（12.7 或更低版本）啟用密碼加密相容** 核取方塊。

   從 Kaspersky Endpoint Security 12.8 for Windows 開始，該應用程式使用更強的密碼加密。如果您部署了 Kaspersky Endpoint Security 12.8 或更高版本，我們建議清除此核取方塊並使用更強的密碼加密。該應用程式的早期版本不支援強密碼加密。若要執行該工作，您必須選取該核取方塊。

### 步驟 3. 選取要執行工作的帳戶

選擇“**預設帳戶**”。預設情況下，Kaspersky Endpoint Security 作為系統使用者帳戶 (SYSTEM) 啟動工作。

### 步驟 4. 設定工作啟動排程

在**排程開始**下面，選擇**手動**。

### 步驟 5. 定義工作名稱

輸入工作的名稱，例如“*主伺服器連線密碼*”。

步驟 6. 完成工作建立

結束精靈。選擇**精靈完成時執行工作**核取方塊或手動執行工作。您可以在工作內容中監控工作進度。

**如何在網頁主控台和 Cloud Console 中設定伺服器連線防護密碼**

1. 在網頁主控台的主視窗中，選擇**資產（裝置）→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 Windows 12.12.0"**。
   b. 在**"工作類型"**下拉式清單中，選取**"管理伺服器連線防護"**。
   c. 在**"工作名稱"**欄位中，輸入簡要說明，例如，*"主伺服器連線密碼"*。
   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。前往下一步。
5. 選取預設使用者帳戶。預設情況下，Kaspersky Endpoint Security 作為系統使用者帳戶 (SYSTEM) 啟動工作。
6. 結束精靈。
   在工作清單中將顯示一個新工作。
7. 點擊 Kaspersky Endpoint Security 的**"管理伺服器連線防護"**工作。
   工作內容視窗將開啟。
8. 選擇**"應用程式設定"**標籤。
9. 在**管理伺服器連線防護**下面，選擇**用密碼防護**。
10. 在**"連線至管理伺服器"**下拉式清單中，選取**"新密碼"**。
11. 在**密碼**欄位中，設定管理伺服器連線密碼並進行確認。
    如果忘記了密碼，您可以使用工作變更密碼。
12. 如果您部署了 Kaspersky Endpoint Security 12.7 或更早版本的應用程式，請選擇 **為先前的應用程式版本（12.7 或更低版本）啟用密碼加密相容** 核取方塊。
    從 Kaspersky Endpoint Security 12.8 for Windows 開始，該應用程式使用更強的密碼加密。如果您部署了 Kaspersky Endpoint Security 12.8 或更高版本，我們建議清除此核取方塊並使用更強的密碼加密。該應用程式的早期版本不支援強密碼加密。若要執行該工作，您必須選取該核取方塊。
13. 儲存變更。

14. 選中該工作旁邊的核取方塊。

15. 點擊**"開始"**。

您可以監控工作的狀態，以及成功完成工作或完成工作時發生錯誤的裝置數量。

## 將電腦重新連線到不同伺服器

將電腦重新連線到不同管理伺服器涉及以下步驟：

1. 在目前 [KSC1] 伺服器的主控台中，為網路代理執行*變更管理伺服器*工作。

   執行工作後，電腦將重新連線到新的 [KSC2] 伺服器。

   電腦將顯示在 [KSC1] 伺服器主控台中，狀態為 *緊急* 。不可能使用政策設定應用程式或在電腦上遠端執行工作。

2. 在新的 [KSC2] 伺服器的主控台中，為 Kaspersky Endpoint Security 建立一個新的*管理伺服器連線防護*工作。在工作內容中，輸入先前伺服器的密碼並為新的伺服器設定密碼。

   **如何在管理主控台 (MMC) 中設定用於重新連線到新伺服器的密碼**

   1. 在卡巴斯基安全管理中心管理主控台樹狀目錄中，選取**工作**。

      工作清單開啟。

   2. 點擊**"新工作"**。

   啟動"工作精靈"。按照精靈的說明進行操作。

### 步驟 1. 選取工作類型

選取**"Kaspersky Endpoint Security for Windows (12.12)"→"管理伺服器連線防護"**。

### 步驟 2. 防護管理伺服器連線

設定密碼防護到新管理伺服器的連線：

1. 在**管理伺服器連線防護**下面，選擇**用密碼防護**。

2. 在**"管理伺服器"**下拉式清單中，選取**"從其他伺服器重新連線"**。

3. 在**目前密碼**欄位中，輸入為先前使用的受信任伺服器連線設定的密碼。

4. 在**新密碼**欄位中，設定新的管理伺服器連線密碼並進行確認。

   如果忘記了密碼，您可以使用工作變更密碼。

5. 如果您部署了 Kaspersky Endpoint Security 12.7 或更早版本的應用程式，請選擇 **為先前的應用程式版本（12.7 或更低版本）啟用密碼加密相容** 核取方塊。

   從 Kaspersky Endpoint Security 12.8 for Windows 開始，該應用程式使用更強的密碼加密。如果您部署了 Kaspersky Endpoint Security 12.8 或更高版本，我們建議清除此核取方塊並使用更強的密碼加密。該應用程式的早期版本不支援強密碼加密。若要執行該工作，您必須選取該核取方塊。

步驟 3. 選取要執行工作的帳戶

選擇“**預設帳戶**”。預設情況下，Kaspersky Endpoint Security 作為系統使用者帳戶 (SYSTEM) 啟動工作。

步驟 4. 設定工作啟動排程

在**排程開始**下面，選擇**手動**。

步驟 5. 定義工作名稱

輸入工作的名稱，例如“*主伺服器連線密碼*”。

步驟 6. 完成工作建立

結束精靈。選擇**精靈完成時執行工作**核取方塊或手動執行工作。您可以在工作內容中監控工作進度。

**如何在網頁主控台和 Cloud Console 中設定用於重新連線到新伺服器的密碼**

1. 在網頁主控台的主視窗中，選擇**資產（裝置）→ 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 Windows 12.12.0**”。

   b. 在“**工作類型**”下拉式清單中，選取“**管理伺服器連線防護**”。

   c. 在“**工作名稱**”欄位中，輸入簡要說明，例如，“*主伺服器連線密碼*”。

   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。前往下一步。

5. 選取預設使用者帳戶。預設情況下，Kaspersky Endpoint Security 作為系統使用者帳戶 (SYSTEM) 啟動工作。

6. 結束精靈。

   在工作清單中將顯示一個新工作。

7. 點擊 Kaspersky Endpoint Security 的**"管理伺服器連線防護"**工作。

   工作內容視窗將開啟。

8. 選擇**"應用程式設定"**標籤。

9. 在**管理伺服器連線防護**下面，選擇**用密碼防護**。

10. 在**"連線至管理伺服器"**下拉式清單中，選取**"從其他伺服器重新連線"**。

11. 在**目前密碼**欄位中，輸入為先前使用的受信任伺服器連線設定的密碼。

12. 在**新密碼**欄位中，設定新的管理伺服器連線密碼並進行確認。

    如果忘記了密碼，您可以使用工作變更密碼。

13. 如果您部署了 Kaspersky Endpoint Security 12.7 或更早版本的應用程式，請選擇 **為先前的應用程式版本（12.7 或更低版本）啟用密碼加密相容** 核取方塊。

    從 Kaspersky Endpoint Security 12.8 for Windows 開始，該應用程式使用更強的密碼加密。如果您部署了 Kaspersky Endpoint Security 12.8 或更高版本，我們建議清除此核取方塊並使用更強的密碼加密。該應用程式的早期版本不支援強密碼加密。若要執行該工作，您必須選取該核取方塊。

14. 儲存變更。

15. 選中該工作旁邊的核取方塊。

16. 點擊**"開始"**。

    您可以監控工作的狀態，以及成功完成工作或完成工作時發生錯誤的裝置數量。

完成工作後，請確保在新的 [KSC2] 伺服器的主控台中，電腦狀態為 *確定*。測試是否可以遠端執行工作和使用政策設定應用程式。

## 重新設定管理伺服器連線密碼

如果忘記了管理伺服器連線密碼或密碼被洩露，您可以在工作內容中重新設定密碼。您也可以重新設定密碼和為具有不同管理伺服器連線防護狀態的一組電腦設定一個新密碼。意思是，如果某些電腦啟用了防護而某些停用了防護，工作將為所有電腦設定一個密碼。

您只能在電腦連線到的受信任伺服器的主控台中重新設定管理伺服器連線密碼。

### 如何使用管理主控台 (MMC) 重設管理伺服器連線密碼

1. 開啟卡巴斯基安全管理中心管理主控台。

2. 在主控台樹狀目錄中，選擇**"工作"**。

3. 選擇**管理伺服器連線防護**工作並雙擊以開啟工作內容。
4. 在工作內容視窗中，選取**"設定"**區域。
5. 在**管理伺服器連線防護**下面，選擇**防護和變更密碼**。
6. 在**連線至管理伺服器的密碼**欄位中，設定新的連線到目前受信任的伺服器的密碼並進行確認。
7. 儲存變更。
8. 執行工作。

**如何在網頁主控台和雲端主控台中重設管理伺服器連線密碼**

1. 在網頁主控台的主視窗中，選擇**資產（裝置）→ 工作**。
   工作清單開啟。
2. 點擊 Kaspersky Endpoint Security 的**"管理伺服器連線防護"**工作。
   工作內容視窗將開啟。
3. 選擇**"應用程式設定"**標籤。
4. 在**管理伺服器連線防護**下面，選擇**防護和變更密碼**。
5. 在**密碼**欄位中，設定新的連線到目前受信任的伺服器的密碼並進行確認。
6. 儲存變更。
7. 選中該工作旁邊的核取方塊。
8. 點擊**"開始"**。

結果，管理伺服器連線密碼將在工作結束後重設。

## 停用管理員伺服器連線防護

您只能在電腦連線到的受信任伺服器的主控台中遠端停用管理伺服器連線防護。您也可以使用命令列本機停用防護。

**如何在管理主控台 (MMC) 中停用伺服器連線防護**

1. 開啟卡巴斯基安全管理中心管理主控台。
2. 在主控台樹狀目錄中，選擇**"工作"**。
3. 選擇**管理伺服器連線防護**工作並雙擊以開啟工作內容。
4. 在工作內容視窗中，選取**"設定"**區域。
5. 在**管理伺服器連線防護**下面，選擇**不防護**。

6. 儲存變更。

7. 執行工作。

   您可以監控工作的狀態，以及成功完成工作或完成工作時發生錯誤的裝置數量。

**如何在網頁主控台和 Cloud Console 中停用伺服器連線防護**

1. 在網頁主控台的主視窗中，選擇**資產（裝置）→工作**。

   工作清單開啟。

2. 點擊 Kaspersky Endpoint Security 的**"管理伺服器連線防護"**工作。

   工作內容視窗將開啟。

3. 選擇**"應用程式設定"**標籤。

4. 在**管理伺服器連線防護**下面，選擇**不防護**。

5. 儲存變更。

6. 選中該工作旁邊的核取方塊。

7. 點擊**"開始"**。

   您可以監控工作的狀態，以及成功完成工作或完成工作時發生錯誤的裝置數量。

**如何使用命令行停用伺服器連線防護**

1. 以管理員身分執行命令列解譯器 (cmd.exe)。

2. 轉到 Kaspersky Endpoint Security 可執行檔所在資料夾。

3. 執行以下指令：

   ```
   avp.com SERVERBINDINGDISABLE [/password=<password>]
   ```

   其中 <password> 是 KLAdmin 使用者帳戶的密碼或 *管理伺服器連線防護* 工作的密碼。如果未指定參數，Kaspersky Endpoint Security 將提示您在下一行輸入密碼。

   > 要執行此指令，必須啟用密碼防護。

   範例：

   ```
   avp.com SERVERBINDINGDISABLE /password=samplePassword
   ```

# 資料加密

Kaspersky Endpoint Security 允許您加密儲存在本機和卸除式磁碟機上的檔案和資料夾，或者整個卸除式磁碟機和硬碟。筆記型電腦、卸除式磁碟機或硬碟遺失或被竊取時，又或者在未經許可的使用者或應用程式存取資料時，資料加密功能能夠將資訊洩露的危險降至最低。Kaspersky Endpoint Security 使用進階加密標準 (AES) 加密演算法。

如果產品授權已到期，本程式不會加密新資料，舊的已加密資料仍保持加密狀態並且可用。在此情況下，加密新資料將要求用允許使用加密的新產品授權來啟動應用程式。

如果產品授權已到期，或違反了最終使用者產品授權協議，亦或已刪除產品授權金鑰、Kaspersky Endpoint Security 或加密元件，則先前加密檔案的加密狀態將得不到保證。這是因為某些應用程式，例如 Microsoft Office Word，會在編輯期間建立暫存檔案副本。儲存原始檔案時，臨時副本將替換原始檔案。因此，在沒有加密功能或無法存取加密功能的電腦上，檔案保持未加密狀態。

Kaspersky Endpoint Security 提供了以下幾個方面的資料防護：

- **本機電腦磁碟機上檔案級加密**。您可以根據副檔名或副檔名群組編制檔案清單，和儲存在本機電腦磁碟上的資料夾清單，並且為特定應用程式建立的檔案建立加密規則。套用政策後，卡巴斯基安全管理中心將加密和解密以下檔案：
  - 單獨新增到加密和解密清單中的檔案。
  - 儲存在新增到加密和解密清單中的資料夾內的檔案。
  - 單獨應用程式建立的檔案。
- **卸除式磁碟機加密**。您可以指定預設加密規則，應用程式將根據此規則對所有卸除式磁碟機套用相同操作，您也可以為個別卸除式磁碟機指定加密規則。

  預設加密規則的優先順序低於為個別卸除式磁碟機建立的加密規則。為擁有特定裝置型號的卸除式磁碟機建立的加密規則，其優先順序低於為擁有特定裝置 ID 的卸除式磁碟機建立的檔案加密規則。

  若要為卸除式磁碟機中的檔案選取加密規則，Kaspersky Endpoint Security 將會檢查裝置的型號和 ID 是否已知。然後此程式將執行以下操作之一：
  - 如果只有裝置型號已知，程式將使用為特定裝置型號的卸除式磁碟機建立的加密規則（如果已建立）。
  - 如果只有裝置 ID 已知，程式將使用為特定裝置 ID 的卸除式磁碟機建立的加密規則（如果已建立）。
  - 如果裝置型號和 ID 已知，程式將使用為特定裝置 ID 的卸除式磁碟機建立的加密規則（如果已建立）。如果不存在此類規則，但是存在為特定裝置型號的卸除式磁碟機建立的加密規則，則應用程式將套用此規則。如果沒有為特定的裝置 ID 或特定的裝置型號指定加密規則，應用程式將應用預設的加密規則。
  - 如果裝置型號和裝置 ID 都未知，程式將使用預設的加密規則。

  程式可以讓您準備卸除式磁碟機以攜帶模式使用磁碟機上儲存的加密資料。啟用攜帶模式後，您可以存取連線到沒有加密功能之電腦上的卸除式磁碟機中的加密檔案。
- **管理應用程式存取加密檔案的規則**。對於任何應用程式，您可以建立加密檔案存取規則，封鎖對加密檔案的存取或者允許僅使用加密文字（應用加密時獲得的字串）存取加密檔案。
- **建立加密資料**。您可以建立加密存檔，並使用密碼防護對此類存檔的存取。只有輸入您防護此檔案的密碼才能存取加密檔案中的內容。此類檔案可以安全的透過網路或透過卸除式磁碟機傳輸。

- **完整磁碟加密**。您可以選取加密技術：卡巴斯基磁碟加密或 BitLocker 磁碟機加密（以下簡稱"BitLocker"）。

  *BitLocker* 技術是 Windows 作業系統的一部分。如果電腦配備了受信任平台模組 (TPM)，BitLocker 將用其儲存提供加密硬碟存取的還原金鑰。電腦啟動時，BitLocker 將從受信任平台模組請求硬碟還原金鑰並解鎖磁碟機。您可以設定存取還原金鑰使用密碼和/或 PIN 碼。

  您可以指定預設的完整磁碟加密規則，並建立要從加密中排除的硬碟的清單。套用卡巴斯基安全管理中心政策後，Kaspersky Endpoint Security 將按照磁區執行完整磁碟加密。應用程式加密將同時套用至硬碟的所有邏輯分區上。

  加密系統硬碟後，在下次電腦啟動時，使用者要能夠存取硬碟並且作業系統載入前，使用者必須透過身分驗證代理的驗證。這需要輸入權杖或連線到電腦的智能卡的密碼，或者輸入由局域網管理員使用"*管理身分驗證代理帳戶*"工作建立的身分驗證代理帳戶的使用者名稱和密碼。這些帳戶以使用者登入作業系統的 Microsoft Windows 帳戶為基礎。您還可以使用Single Sign-On (SSO) 技術，此技術允許您使用身分驗證代理帳戶的使用者名稱和密碼自動登入至作業系統。

  > 如果您備份電腦，然後對電腦資料進行加密，之後還原電腦備份副本並再次加密電腦資料，Kaspersky Endpoint Security 將會建立相同的身分驗證代理帳戶。要刪除重複帳戶，請使用帶有 `dupfix` 金鑰的 klmover 實用程式。Klmover 實用程式含在卡巴斯基安全管理中心分發套件中。您可以在《卡巴斯基安全管理中心說明》中瞭解有關其操作的更多資訊。

  只能在安裝了帶有完整磁碟加密功能的 Kaspersky Endpoint Security 的電腦上存取已加密的硬碟。當出現公司區域網路之外的連接嘗試存取加密檔案時，此功能會大大降低加密硬碟中的檔案洩露的風險。

若要加密硬碟和卸除式磁碟機，您可以使用"僅加密使用的磁碟空間"功能。建議您僅為先前未使用的新裝置使用此功能。如果您在已使用的裝置上套用加密，建議您加密整個裝置。這將確保所有資料受到防護 – 即使刪除了可能仍包含擷取資訊的資料。

開始加密之前，Kaspersky Endpoint Security 將獲得檔案系統磁區圖。第一波加密包括開始加密時檔案佔用的磁區。第二波加密包括加密開始後寫入的磁區。加密完成後，所有包含資料的磁區都將被加密。

加密完成並且使用者刪除檔案後，儲存刪除檔案的磁區可以在檔案系統等級儲存新的資訊但是仍保持為加密狀態。因此，在啟用**"僅加密使用的磁碟空間"**功能的情況下，隨著檔案寫入新裝置和定期加密該裝置，在一段時間後所有磁區都將加密。

解密檔案所需的檔案由加密時控制電腦的卡巴斯基安全管理中心管理伺服器提供。如果含有加密物件的電腦因某種原因由其他管理伺服器管理，則可以透過下列方式之一獲得對加密資料的存取權限：

- 同一層次結構中的管理伺服器：
  - 您無需執行其他任何操作。使用者將保留對加密物件的存取權限。加密金鑰將分發到所有管理伺服器。
- 單獨的管理伺服器：
  - 向區域網路管理員請求加密物件的存取權限。
  - 使用"還原實用工具"還原加密裝置上的資料。
  - 從備份副本還原在加密時控制電腦的卡巴斯基安全管理中心管理伺服器的配置，並且在現在控制包含加密物件的電腦的管理伺服器上使用此配置。

如果沒有加密資料的存取權限，請遵循有關處理加密資料的特殊說明（還原對加密檔案的存取權限、無法存取加密裝置時的裝置使用）。

# 加密功能限制

資料加密具有以下限制：

- 程式將在加密期間建立服務檔案。需要硬碟上大約 0.5% 的非碎片的磁碟空間來儲存這些檔案。如果硬碟磁碟機上的可用磁碟空間不足，加密操作不會運行，直至您清理出足夠的空間。
- 您可以在卡巴斯基安全管理中心管理主控台和卡巴斯基安全管理中心網頁主控台中管理所有資料加密元件。在卡巴斯基安全管理中心雲端主控台中，您只能管理 Bitlocker。
- 僅當將 Kaspersky Endpoint Security 與卡巴斯基安全管理中心管理系統或卡巴斯基安全管理中心雲端主控台（僅限 BitLocker）一起使用時，資料加密才可用。在離線模式下使用 Kaspersky Endpoint Security 時，無法使用資料加密，因為 Kaspersky Endpoint Security 將加密金鑰儲存在卡巴斯基安全管理中心中。
- 如果將 Kaspersky Endpoint Security 安裝在執行 Microsoft Windows for Servers 的電腦上，則只有使用 BitLocker 磁碟機加密技術的完整磁碟加密可用。如果 Kaspersky Endpoint Security 安裝在執行 Windows for Workstations 的電腦上，則資料加密功能完全可用。

對於不滿足軟硬體需求的硬碟磁碟機，無法使用卡巴斯基磁碟加密技術進行完整磁碟加密。

Kaspersky Endpoint Security 的完整磁碟加密功能與 Kaspersky Anti-Virus for UEFI 之間不相容。Kaspersky Anti-Virus for UEFI 在作業系統載入前啟動。使用完整磁碟加密時，應用程式將偵測電腦上是否缺少已安裝的作業系統。因此，Kaspersky Anti-Virus for UEFI 的執行將以錯誤結束。檔案級加密 (FLE) 不會影響 Kaspersky Anti-Virus for UEFI 的操作。

Kaspersky Endpoint Security 支援以下設定：

- HDD，SSD 和 USB 磁碟機。

  卡巴斯基磁碟加密（FDE）技術支援使用 SSD，同時保留 SSD 磁碟機的效能和使用壽命。

- 透過匯流排連線的磁碟機：SCSI，ATA，IEEE1934，USB，RAID，SAS，SATA，NVME。
- 透過 SD 或 MMC 匯流排連線的非卸除式磁碟機。
- 具有 512 位元組磁區的磁碟機。
- 具有 4096 位元組磁區（模擬 512 位元組）的磁碟機。
- 具有以下類型磁碟分割的磁碟機：GPT，MBR 和 VBR（卸除式磁碟機）。
- UEFI 64 和 Legacy BIOS 標準的內嵌軟體。
- UEFI 標準的內嵌軟體，具有安全開機支援。

  *安全開機*是一項旨在驗證 UEFI 加載程式應用程式和驅動程式的數位簽章的技術。安全開機會封鎖未簽名或由未知發行者簽名的 UEFI 應用程式和驅動程式啟動。卡巴斯基磁碟加密（FDE）完全支援安全開機。身分驗證代理由 Microsoft Windows UEFI Driver Publisher 憑證簽署。

  在某些裝置（例如，Microsoft Surface Pro 和 Microsoft Surface Pro 2）上，預設情況下可能會安裝數位簽章驗證憑證的過期清單。在加密磁碟機之前，您需要更新憑證清單。

- UEFI 標準的內嵌軟體，具有快速開機支援。

  *快速開機*是一項有助於電腦更快啟動的技術。啟用快速開機技術後，通常電腦僅加載啟動作業系統所需的最少 UEFI 驅動程式集合。啟用快速開機技術後，當身分驗證代理執行時，USB 鍵盤、鍵鼠、USB 權杖、觸控板和觸控熒幕可能無法工作。

  要使用卡巴斯基磁碟加密（FDE）的話，建議停用快速開機技術。您可以使用FDE 測試實用程式來測試卡巴斯基磁碟加密（FDE）的運行。

Kaspersky Endpoint Security 不支援以下配置：

- 引導載入程式位於某個磁碟上而作業系統位於其他磁碟上。
- 系統包含 UEFI 32 標準的嵌入式軟體。
- 系統有 Intel® 快速開機技術和即使 Intel® 快速開機技術被停用時也擁有休眠磁碟分割的磁碟機。
- MBR 格式的磁碟擁有超過 10 個延伸磁碟分割。
- 系統有一個交換檔案位於非系統磁碟機上。
- 同時安裝有多個作業系統的多啟動系統。
- 動態磁碟分割（僅支援主要磁碟分割）。
- 未經過磁碟整理可用空間少於 0.5% 的磁碟。
- 磁區大小不是 512 位元組或類比 512 位元組的 4096 位元組的磁碟。
- 混合磁碟。
- 系統有協力廠商載入程式。
- 具有壓縮的 NTFS 目錄的磁碟機。
- 卡巴斯基磁碟加密（FDE）技術與其他完整磁碟加密（例如 BitLocker、McAfee Drive Encryption 和 WinMagic SecureDoc）不相容。
- 卡巴斯基磁碟加密（FDE）技術與 ExpressCache 技術不相容。
- 不支援在加密磁碟機上建立、刪除和修改磁碟分割。您可能會丟失資料。
- 不支援檔案系統格式化。您可能會丟失資料。

  如果需要格式化使用卡巴斯基磁碟加密（FDE）技術加密的磁碟機，請在不具有 Kaspersky Endpoint Security for Windows 的電腦上格式化該磁碟機，並僅使用完整磁碟加密。

  下次將用快速磁碟機選項格式化的加密磁碟機連線到安裝了 Kaspersky Endpoint Security for Windows 的電腦時，可能會錯誤地將其標識為已加密。使用者資料將不可用。
- 身分驗證代理最多支援 100 個帳戶。
- 單一登入技術與協力廠商開發人員的其他技術不相容。

- 以下型號的裝置不支援卡巴斯基磁碟加密（FDE）技術：
  - Dell Latitude E6410（UEFI 模式）
  - HP Compaq nc8430（Legacy BIOS 模式）
  - Lenovo ThinkCentre 8811（Legacy BIOS 模式）。
- 啟用 Legacy USB Support 時，身分驗證代理不支援使用 USB 權杖。在電腦上只能進行基於密碼的身分驗證。
- 在 Legacy BIOS 模式下加密磁碟機時，建議在以下型號的裝置上啟用 Legacy USB Support：
  - Acer Aspire 5560G
  - Acer Aspire 6930
  - Acer TravelMate 8572T
  - Dell Inspiron 1420
  - Dell Inspiron 1545
  - Dell Inspiron 1750
  - Dell Inspiron N4110
  - Dell Latitude E4300
  - Dell Studio 1537
  - Dell Studio 1569
  - Dell Vostro 1310
  - Dell Vostro 1320
  - Dell Vostro 1510
  - Dell Vostro 1720
  - Dell Vostro V13
  - Dell XPS L502x
  - Fujitsu Celsius W370
  - Fujitsu LifeBook A555
  - HP Compaq dx2450 Microtower PC
  - Lenovo G550
  - Lenovo ThinkPad L530
  - Lenovo ThinkPad T510

- Lenovo ThinkPad W540
- Lenovo ThinkPad X121e
- Lenovo ThinkPad X200s (74665YG)
- Samsung R530
- Toshiba Satellite A350
- Toshiba Satellite U400 10O
- MSI 760GM-E51（主機板）

# 變更加密金鑰的長度 (AES56 / AES256)

Kaspersky Endpoint Security 使用進階加密標準 (AES) 加密演算法。Kaspersky Endpoint Security 支援有效金鑰長度為 256 或 56 位元的 AES 加密演算法。資料加密演算法取決於分發套件中包含的 AES 加密庫：*強加密 (AES256)* 或 *簡單加密 (AES56)*。AES 加密庫與應用程式一起安裝。

只有 Kaspersky Endpoint Security 11.2.0 或更高版本可以變更加密金鑰的長度。

變更加密金鑰長度包括以下步驟：

1. 開始變更加密金鑰長度之前，解密 Kaspersky Endpoint Security 加密的物件：
   a. 解密硬碟磁碟機。
   b. 解密本機磁碟機上的檔案。
   c. 解密卸除式磁碟機。

   改變加密金鑰長度後，先前加密的物件變為不可使用。
2. 移除 Kaspersky Endpoint Security。
3. 從包含其他加密庫的 Kaspersky Endpoint Security 分發套件安裝 Kaspersky Endpoint Security。

您也可以透過升級應用程式來變更加密金鑰長度。只有滿足以下條件，才可以透過應用程式升級來變更金鑰長度：

- 電腦上已安裝 Kaspersky Endpoint Security 版本 10 Service Pack 2 或更高版本。
- 電腦上未安裝資料加密元件（檔案級加密、完整磁碟加密）。

  預設情況下，Kaspersky Endpoint Security 不包含資料加密元件。BitLocker 管理元件不會影響加密金鑰長度的變更。

要變更加密金鑰長度，請執行包含必要加密庫的分發套件中的 kes_win.msi 或 setup_kes.exe 檔案。您還可以使用安裝套件遠端升級應用程式。

無法使用與電腦上安裝的應用程式版本相同的分發套件變更加密金鑰的長度，除非先移除應用程式。

# 卡巴斯基磁碟加密

卡巴斯基磁碟加密僅適用於執行面向工作站的 Windows 作業系統的電腦。對於執行面向伺服器的 Windows 作業系統的電腦，請使用 BitLocker 磁碟機加密技術。

Kaspersky Endpoint Security 支援 FAT32、NTFS 和 exFat 檔案系統的完整磁碟加密。

啟動完整磁碟加密之前， 應用程式會執行一些檢查，以確定裝置是否可以被加密，其中包括檢查系統硬碟磁碟機與驗證代理或 BitLocker 加密元件的相容性。若要檢查相容性，電腦必須重新啟動。重新啟動電腦後，應用程式會自動執行所有必需的檢查。如果相容性檢查成功，則在載入作業系統和啟動應用程式後開始完整磁碟加密。如果系統硬碟磁碟機不相容驗證代理或 BitLocker 加密元件不相容，必須按下硬體重置按鈕，重新啟動電腦。Kaspersky Endpoint Security 將會記錄有關不相容的資訊記錄。根據此資訊，應用程式在作業系統啟動時不會啟動完整磁碟加密。有關此資訊的事件將會記錄在卡巴斯基安全管理中心的報告中。

如果電腦硬體設定已經變更，先前不相容的檢查記錄資訊將會予以刪除，以重新檢查系統硬碟磁碟機與身分驗證代理和 BitLocker 加密元件的相容性。要執行此操作，請在完整磁碟加密前，在命令列執行加密類型的 `avp pbatestreset` 指令。如果作業系統未能在檢查系統硬碟磁碟機是否與身分驗證代理相容之後載入，您必須在身分驗證代理測試執行之後使用還原實用工具刪除剩餘物件和資料，然後啟動 Kaspersky Endpoint Security 並再次執行 `avp pbatestreset` 指令。

啟動完整磁碟加密後，Kaspersky Endpoint Security 將加密硬碟上的所有資料。

如果使用者在完整磁碟加密期間關閉或重新啟動電腦，下次啟動作業系統之前系統將載入身分驗證代理。成功透過身分驗證並在作業系統啟動後，Kaspersky Endpoint Security 將還原完整磁碟加密。

如果作業系統在完整磁碟加密期間切換至休眠模式，作業系統結束休眠模式時將載入身分驗證代理。成功透過身分驗證並在作業系統啟動後，Kaspersky Endpoint Security 將還原完整磁碟加密。

如果作業系統在完整磁碟加密期間進入休眠模式，則當作業系統結束休眠模式時，Kaspersky Endpoint Security 將還原完整磁碟加密，且不會載入身分驗證代理。

可以透過兩種方式在身分驗證代理中執行使用者身分驗證：

- 輸入區域網路管理員使用卡巴斯基安全管理中心工具建立的身分驗證代理帳戶的使用者名稱和密碼。
- 輸入連線至電腦的令牌的密碼或智慧卡的密碼。

  如果電腦硬碟磁碟機使用 AES256 加密演算法進行加密，則可以使用令牌或智慧卡。如果使用 AES256 演算法加密了電腦硬碟磁碟機，新增電子憑證檔案到指令將被拒絕。

身分驗證代理支援以下語言的鍵盤配置：

- 英語（英國）
- 英語（美國）
- 阿拉伯語（阿爾及利亞、摩洛哥、突尼斯、AZERTY 佈局）
- 西班牙語（拉丁美洲）
- 意大利語
- 德語（德國和奧地利）
- 德語（瑞士）
- 葡萄牙語（巴西、ABNT2 佈局）
- 俄語（針對帶有 QWERTY 佈局的 105 鍵 IBM / Windows 鍵盤）
- 土耳其語（QWERTY 佈局）
- 法語（法國）
- 法語（瑞士）
- 法語（比利時 AZERTY 佈局）
- 日語（針對帶有 QWERTY 佈局的 106 鍵鍵盤）

如果作業系統的語言和區域標準設定中新增了此佈局，則在身分驗證代理中可以使用此鍵盤佈局。

如果身分驗證代理帳戶名稱包含身分驗證代理中無法使用鍵盤配置輸入的符號，則只能使用還原實用工具還原後或還原身分驗證代理帳戶名稱和密碼還原後存取加密的硬碟磁碟機。

# SSD 磁碟機加密的特殊功能

該應用程式支援對 SSD 磁碟機，混合式 SSHD 磁碟機以及具有 Intel Smart Response 功能的磁碟機進行加密。該應用程式不支援對對具有 Intel Rapid Start 功能的磁碟機進行加密。在加密此類磁碟機之前，請停用 Intel Rapid Start 功能。

SSD 磁碟機加密具有以下特殊功能：

- 如果 SSD 磁碟機是新的並且不包含機密資料，請僅對占用的空間進行加密。這樣就可以覆蓋相關的磁碟機磁區。
- 如果 SSD 磁碟機正在使用中並且具有機密資料，請選擇以下選項之一：
  - 完整擦除 SSD 磁碟機（安全擦除），安裝作業系統並執行 SSD 磁碟機加密，可以選擇僅加密啟用的佔用空間。
  - 執行 SSD 磁碟機加密，可選擇僅加密停用的佔用空間。

SSD 磁碟機的加密需要 5-10 GB 的可用空間。下表提供了用於儲存加密管理資料的可用空間要求。

儲存加密管理資料的可用空間要求

| SSD 磁碟機大小（GB） | SSD 磁碟機主要磁碟分割上的可用空間（MB） | SSD 磁碟機次要磁碟分割上的可用空間（MB） |
|---|---|---|
| 128 | 250 | 64 |
| 256 | 250 | 640 |
| 512 | 300 | 128 |

# 啟動卡巴斯基磁碟加密

在開始完整磁碟加密之前，建議您確保電腦未受到感染。若要執行操作，應啟動完整掃描或關鍵區域掃描工作。在已被 rootkit 感染的電腦上執行完整磁碟加密可能導致電腦無法執行。

在啟動磁碟加密之前，您必須檢查身分驗證代理帳戶的設定。使用採用卡巴斯基磁碟加密 (FDE) 技術保護的磁碟機時，需要身分驗證代理。載入作業系統之前，使用者需要使用代理完成身分驗證。Kaspersky Endpoint Security 允許您在加密磁碟機之前自動建立身分驗證代理帳戶。您可以在"完整磁碟加密"政策設定中啟用自動建立身分驗證代理帳戶（請見下方的操作指示）。您還可以使用單點登入 (SSO) 技術。

Kaspersky Endpoint Security 允許您為以下使用者群組自動建立身分驗證代理：

- **電腦上的所有帳戶**任何時間啟動過的電腦上的所有帳戶。
- **電腦上所有網域帳戶**屬於某些網域且在任何時間啟動過的電腦上的所有帳戶。
- **電腦上所有本機帳戶**任何時間啟動過的電腦上的所有本機帳戶。
- **具有一次性密碼的服務賬戶**獲取電腦的存取權限時（例如，當使用者忘記密碼時）需要該服務帳戶。您也可以將服務帳戶作為備用帳戶。您可以輸入帳戶名稱（預設為 `ServiceAccount`）。Kaspersky Endpoint Security 會自動建立密碼。您只能在卡巴斯基安全管理中心主控台中查找密碼。
- **本機管理員**Kaspersky Endpoint Security 會為電腦的本機管理員建立一個身分驗證代理使用者帳戶。
- **電腦管理者**Kaspersky Endpoint Security 會為電腦管理者的帳戶建立一個身分驗證代理使用者帳戶。您可以在 Active Directory 的電腦內容中查看哪個帳戶有電腦管理者角色。預設未定義電腦管理者角色，即它不相應任何帳戶。
- **目前帳戶**Kaspersky Endpoint Security 會為磁碟加密時啟動的帳戶自動建立一個身分驗證代理帳戶。

"*管理身分驗證代理帳戶*"工作設計用於設定使用者身分驗證設定。您可以使用該工作新增帳戶、修改目前帳戶的設定、或者必要時刪除帳戶。對於單一電腦可以使用本機工作，對於單獨管理群組中的電腦或一組選定電腦，可以使用群組工作。

**如何透過管理主控台 (MMC) 執行卡巴斯基磁碟加密**

1. 在卡巴斯基安全管理中心管理主控台樹狀目錄中，選取**政策**。
2. 選擇必要的政策並點擊以開啟政策內容。
3. 在政策視窗中，選擇"**資料加密 → 完整磁碟加密**"。

4. 在“**加密技術**”下拉式清單中，選取“**卡巴斯基磁碟加密**”。

如果電腦的硬碟磁碟機先前使用 BitLocker 加密，則無法使用卡巴斯基磁碟加密。

5. 在“**加密模式**”下拉式清單中，選取“**加密所有硬碟磁碟機**”。

如果電腦安裝了多個作業系統，則在加密所有硬碟後，您將只能載入安裝了此應用程式的作業系統。

如果您需要從加密中排除某些硬碟磁碟機，則建立此類硬碟磁碟機的清單。

6. 設定進階卡巴斯基磁碟加密選項（參見下表）。

7. 儲存變更。

**如何透過網頁主控台和雲端主控台執行卡巴斯基磁碟加密**

1. 在網頁主控台的主視窗中，選擇**資產（裝置）→政策和設定檔**。

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”**資料加密**”→”**完整磁碟加密**”。

5. 選擇 **卡巴斯基磁碟加密** 技術。

如果電腦的硬碟磁碟機先前使用 BitLocker 加密，則無法使用卡巴斯基磁碟加密。

6. 在“**裝置操作**”塊中，選取“**加密所有硬碟磁碟機**”。

如果電腦安裝了多個作業系統，在加密後，您將能夠只載入執行了加密的作業系統。

如果您需要從加密中排除某些硬碟磁碟機，則建立此類硬碟磁碟機的清單。

7. 設定進階卡巴斯基磁碟加密選項（參見下表）。

8. 儲存變更。

您可以使用加密監控工具來控制使用者電腦上的磁盤加密或解密過程。您可以從"主應用程式視窗"執行加密監控工具。




加密監控器

如果系統硬碟磁碟機被加密，則身分驗證代理在作業系統啟動之前載入。使用身分驗證代理完成身分驗證以便存取加密的系統硬碟磁碟機並載入作業系統。在成功完成身分驗證過程後，作業系統將載入。身分驗證過程將在每次作業系統重新啟動時重新開始。

卡巴斯基磁碟加密元件設定

| 參數 | 描述 |
| --- | --- |
| **對以下使用者自動建立身分驗證代理帳戶 使用者 加密期間** | 如果選中此核取方塊，則應用程式將基於電腦上的 Windows 使用者帳戶清單建立身分驗證代理帳戶。預設情況下，Kaspersky Endpoint Security 使用在過去30 天內登入到作業系統的使用者所使用的所有本機帳戶和網域帳戶。 |
| **首次登入時為此電腦的所有使用者自動建立身分驗證代理帳戶** | 如果選中此核取方塊，則應用程式將在啟動身分驗證代理之前檢查電腦上 Windows 使用者帳戶的資訊。如果 Kaspersky Endpoint Security 偵測到沒有身分驗證代理帳戶的 Windows 使用者帳戶，則應用程式將建立一個新帳戶來存取加密的磁碟機。新的身分驗證代理帳戶將具有以下預設設定：僅受密碼防護的登錄，以及首次身分驗證時變更密碼。因此，對於具有已加密磁碟機的電腦，不需要使用"*管理身分驗證代理帳戶*"工作手動新增身分驗證代理帳戶。 |
| **儲存在身分驗證代理中輸入的使用者名稱** | 如果選中該核取方塊，應用程式將儲存身分驗證代理帳戶的名稱。下次使用同一帳戶在身分驗證代理中嘗試完成憑證時不會被提示輸入帳戶名稱。 |

| 參數 | 描述 |
| --- | --- |
| **僅加密使用的磁碟空間(減少加密時間)** | 該核取方塊可啟用/停用將加密區域僅限為已用硬碟磁區的選項。該限制可減少加密時間。<br><br>在啟動加密後啟用或者停用**"僅加密使用的磁碟空間(減少加密時間)"**功能不會修改此設定，直到硬碟磁碟機被解密為止。開始加密之前您必須選擇或清除該核取方塊。<br><br>如果選定該核取方塊，則僅加密使用的硬碟部分。Kaspersky Endpoint Security 將自動加密新增的新資料。<br>如果清空該核取方塊，整個硬碟將被加密，包括先前刪除和修改檔案殘留的碎片。<br><br>建議對尚未修改或刪除資料的新硬碟使用該選項。如果對已在使用中的硬碟應用加密，則建議加密整個硬碟。這樣可確保防護所有資料，甚至已刪除的資料也能夠部分還原。<br><br>預設情況下，會取消勾選核取方塊。 |
| **啟用 Legacy USB Support(不建議)** | 此核取方塊啟用或停用 Legacy USB Support 功能。*Legacy USB Support* **是**一種 BIOS/UEFI 功能，允許您在啟動作業系統（BIOS 模式）之前，在電腦的引導階段使用 USB 裝置（例如安全性權杖）。Legacy USB Support不會影響作業系統啟動後對 USB 裝置的支援。<br><br>如果選中該核取方塊，在電腦初始啟動期間對 USB 裝置的支援將啟用。<br><br>啟用Legacy USB Support功能時，BIOS 模式下的身分驗證代理不支援透過 USB 使用權杖。建議僅當存在硬體相容性問題時並僅對發生問題的電腦使用此選項。 |

# 建立硬碟磁碟機加密排除清單

您可以僅為卡巴斯基磁碟加密技術建立加密排除項目清單。

*若要建立從加密範圍中排除的硬碟磁碟機清單，請執行以下操作：*

1. 在卡巴斯基安全管理中心管理主控台樹狀目錄中，選取**政策**。
2. 選擇必要的政策並點擊以開啟政策內容。
3. 在政策視窗中，選擇**"資料加密 → 完整磁碟加密"**。
4. 在**"加密技術"**下拉式清單中，選取**"卡巴斯基磁碟加密"**。

   從加密項目中排除的硬碟磁碟機所對應的項目將顯示在**"請勿加密以下硬碟磁碟機"**清單中。如果您先前並未建立硬碟磁碟機加密排除清單，此清單將是空白。
5. 若要向從加密範圍中排除的硬碟磁碟機清單中新增硬碟磁碟機，請執行以下操作：
   a. 點擊**"新增"**。
   b. 在開啟的視窗中，指定 **裝置名稱**, **電腦**, **磁碟類型**, **卡巴斯基磁碟加密** 的值。
   c. 點擊**"重新整理"**。
   d. 在**"名稱"**列中，在表行中選擇與您要新增到硬碟磁碟機加密排除清單中的硬碟磁碟機對應的核取方塊。
   e. 點擊**"確定"**。

對應於選定硬碟磁碟機的項目將顯示在**"請勿加密以下硬碟磁碟機"**清單中。

6. 儲存變更。

# 匯出和匯入從加密範圍中排除的硬碟磁碟機清單

您可以將硬碟磁碟機加密排除項目清單匯出到 XML 檔案。然後，您可以修改檔案，例如，新增大量相同類型的排除項目。您還可以使用匯出/匯入功能來備份排除項目清單，或將排除項目遷移到其他伺服器。

**如何在管理主控台 (MMC) 中匯出和匯入硬碟磁碟機加密排除項目清單**

1. 在卡巴斯基安全管理中心管理主控台樹狀目錄中，選取**政策**。
2. 選擇必要的政策並點擊以開啟政策內容。
3. 在政策視窗中，選擇**"資料加密 → 完整磁碟加密"**。
4. 在**"加密技術"**下拉式清單中，選取**"卡巴斯基磁碟加密"**。
   從加密項目中排除的硬碟磁碟機所對應的項目將顯示在**"請勿加密以下硬碟磁碟機"**清單中。
5. 若要匯出排除項目清單：
   a. 選取您想要匯出的排除項目。要選擇多個連接埠，請使用**CTRL**或**SHIFT**鍵。
      如果您未選擇任何排除項目，則 Kaspersky Endpoint Security 將匯出所有排除項目。
   b. 點擊 → **匯出** 按鈕。
   c. 在開啟的視窗中，指定您要將排除項目清單匯出到的 XML 檔案的名稱，然後選取要儲存此檔案的資料夾。
   d. 儲存檔案。
      Kaspersky Endpoint Security 會將整個排除項目清單匯出到 XML 檔案。
6. 要匯入規則清單：
   a. 點擊 → **匯入** 按鈕。
   b. 在開啟的視窗中，選取要從中匯入排除項目清單的 XML 檔案。
   c. 開啟檔案。
      如果電腦已經具有排除項目清單，則 Kaspersky Endpoint Security 將提示您刪除現有清單或從 XML 檔案向其中新增新項目。
7. 儲存變更。

**如何在網頁主控台中匯出和匯入硬碟磁碟機加密排除項目清單**

1. 在網頁主控台的主視窗中，選擇**資產（裝置）→ 政策和設定檔**。
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"**資料加密**"→"**完整磁碟加密**"。

   選擇 **卡巴斯基磁碟加密** 技術。

5. 點擊"**排除項目**"連接。

   排除項目清單開啟。

6. 要匯出規則清單：

   a. 選取您想要匯出的排除項目。

   b. 點擊 → **匯出** 按鈕。

      Kaspersky Endpoint Security 會將排除項目清單匯出到預設下載資料夾中的 JSON 檔案。

7. 若要匯入排除項目清單：

   a. 點擊 → **匯入** 按鈕。

      在開啟的視窗中，選取要從中匯入排除項目清單的 JSON 檔案。

   b. 開啟檔案。

      如果電腦已經具有排除項目清單，則 Kaspersky Endpoint Security 將提示您刪除現有清單或從 JSON 檔案向其中新增新項目。

8. 儲存變更。

# 啟用單點登入 (SSO) 技術

Single Sign-On (SSO) 技術允許您使用身分驗證代理的憑證自動登入作業系統。這意味著使用者在登入 Windows（身分驗證代理帳戶密碼）時只需要輸入密碼一次。單點登入技術還可以讓您在 Windows 帳戶密碼變更時自動更新身分驗證代理帳戶密碼。

使用單點登入技術時，身分驗證代理將忽略卡巴斯基安全管理中心中指定的密碼強度要求。您可以在作業系統設定中設定密碼強度要求。

啟用單點登入技術

**如何在管理主控台 (MMC) 中啟用單點登入技術**

1. 在卡巴斯基安全管理中心管理主控台樹狀目錄中，選取**政策**。

2. 選擇必要的政策並點擊以開啟政策內容。

3. 在政策視窗中，選擇"**資料加密 → 一般加密設定**"。

4. 在"**密碼設定**"塊中，點擊"**設定**"按鈕。

5. 在開啟之視窗的"**身分驗證代理**"標籤上，選中"**使用單點登入 (SSO) 技術**"核取方塊。

6. 如果您正在使用協力廠商憑據提供者，請選擇**包裝第三方憑據提供商**核取方塊。

7. 儲存變更。

結果，使用者只需與代理完成一次身分驗證過程。載入作業系統不需要身分驗證過程。作業系統會自動載入。

**如何在網頁主控台中啟用單點登入**

1. 在網頁主控台的主視窗中，選擇**資產（裝置）→政策和設定檔**。

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**"資料加密"→"完整磁碟加密"**。

5. 選擇 **卡巴斯基磁碟加密** 技術。

6. 在**"密碼設定"**塊中，選中**"使用單點登入 (SSO) 技術"**核取方塊。

7. 如果您正在使用協力廠商憑據提供者，請選擇**包裝第三方憑據提供商**核取方塊。

8. 儲存變更。

結果，使用者只需與代理完成一次身分驗證過程。載入作業系統不需要身分驗證過程。作業系統會自動載入。

為使單點登入發揮作用，Windows 帳戶密碼和身分驗證代理帳戶的密碼必須相符。如果密碼不相符，使用者需要執行兩次身分驗證過程：在身分驗證代理的介面中以及在載入作業系統之前。這些操作只需要執行一次以同步密碼。之後，Kaspersky Endpoint Security 會用 Windows 帳戶的密碼替換身分驗證代理帳戶的密碼。當 Windows 帳戶密碼變更時，應用程式將自動更新身分驗證代理帳戶的密碼。

協力廠商憑據提供者

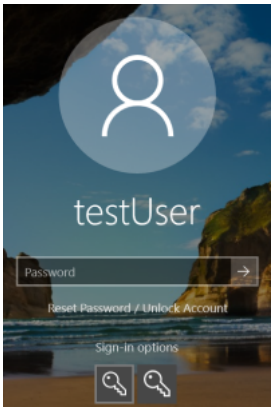
Kaspersky Endpoint Security 支援協力廠商憑據提供者 ADSelfService Plus。

當使用協力廠商憑據提供者時，身分驗證代理會在作業系統載入前攔截密碼。這意味著使用者在登入 Windows 時只需要輸入密碼一次。登入 Windows 後，使用者可以在公司服務（例如）中利用協力廠商憑據提供者的功能進行身分驗證。協力廠商憑據提供者還可讓使用者獨立重設自己的密碼。在此情況下，Kaspersky Endpoint Security 將自動更新身分驗證代理的密碼。

如果您正在使用不受應用程式支援的協力廠商憑據提供者，您可能會在單點登入技術操作中遇到某些限制。當登入到 Windows 時，有兩個設定檔對使用者可用：系統內憑據提供者和協力廠商憑據提供者。這些設定檔的圖示一樣（請參見下圖）。使用者有以下選項可繼續：

- 如果使用者選擇*協力廠商憑據提供者*，身分驗證代理將無法用 Windows 帳戶同步密碼。因此，如果使用者變更了 Windows 帳戶密碼，Kaspersky Endpoint Security 將無法更新身分驗證代理帳戶的密碼。結果，使用者需要執行兩次身分驗證過程：在身分驗證代理的介面中以及在載入作業系統之前。在此情況下，使用者可以在公司服務（例如）中利用協力廠商憑據提供者的功能進行身分驗證。

- 如果使用者選擇*系統內憑據提供者*，身分驗證代理將用 Windows 帳戶同步密碼。在此情況下，使用者將無法在公司服務（例如）中利用協力廠商憑據提供者的功能進行身分驗證。




用於 Windows 登入的系統身分驗證設定檔和協力廠商身分驗證設定檔

# 管理身分驗證代理帳戶

使用採用卡巴斯基磁碟加密 (FDE) 技術保護的磁碟機時，需要身分驗證代理。載入作業系統之前，使用者需要使用代理完成身分驗證。“*管理身分驗證代理帳戶*”工作設計用於設定使用者身分驗證設定。對於單一電腦可以使用本機工作，對於單獨管理群組中的電腦或一組選定電腦，可以使用群組工作。

您無法設定用於啟動“*管理身分驗證代理帳戶*”工作的規劃。也不能強制停止工作。

**如何在管理主控台 (MMC) 中建立“管理身分驗證代理帳戶”工作**

1. 在卡巴斯基安全管理中心管理主控台樹狀目錄中，選取**工作**。

   工作清單開啟。

2. 點擊**“新工作”**。

   啟動“工作精靈”。按照精靈的說明進行操作。

步驟 1. 選取工作類型

選取**“Kaspersky Endpoint Security for Windows (12.12)”→“管理身分驗證代理帳戶”**。

步驟 2. 選取身分驗證代理帳戶管理指令

產生身分驗證代理帳戶管理指令清單。管理指令允許您新增、修改和刪除身分驗證代理帳戶（請參閱以下說明）。只有擁有身分驗證代理帳戶的使用者可以完成身分驗證過程、載入作業系統和獲得對加密磁碟機的存取權限。

步驟 3. 選取將要對其分配工作的裝置

選取將要執行工作的電腦。下列選項可用：

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

步驟 4. 定義工作名稱

輸入工作的名稱，例如"*管理員帳戶*"。

步驟 5. 完成工作建立

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

結果，在下次電腦啟動時，當工作完成後，新使用者可以完成身分驗證過程、載入作業系統和獲得對加密磁碟機的存取權限。

**如何在網頁主控台中建立"管理身分驗證代理帳戶"工作**

1. 在網頁主控台的主視窗中，選擇**資產（裝置）→ 工作**。

   工作清單開啟。

2. 點擊"**新增**"。

啟動"工作精靈"。按照精靈的說明進行操作。

步驟 1. 配置一般工作設定

配置一般工作設定：

1. 在“**應用程式**”下拉清單中，選取“**Kaspersky Endpoint Security for Windows (12.12)**”。
2. 在“**工作類型**”下拉式清單中，選取“**管理身分驗證代理帳戶**”。
3. 在“**工作名稱**”欄位中，輸入簡要說明，例如“*管理員帳戶*”。
4. 在“**要將工作指派給的裝置**”塊中，選取工作範圍。

步驟 2. 管理身分驗證代理帳戶

產生身分驗證代理帳戶管理指令清單。管理指令允許您新增、修改和刪除身分驗證代理帳戶（請參閱以下說明）。只有擁有身分驗證代理帳戶的使用者可以完成身分驗證過程、載入作業系統和獲得對加密磁碟機的存取權限。

步驟 3. 完成工作建立

結束精靈。在工作清單中將顯示一個新工作。

要執行工作，請選中與工作對應的核取方塊，然後點擊“**開始**”按鈕。

結果，在下次電腦啟動時，當工作完成後，新使用者可以完成身分驗證過程、載入作業系統和獲得對加密磁碟機的存取權限。

要新增身分驗證代理帳戶，您需要向“*管理身分驗證代理帳戶*”工作新增特殊指令。使用群組工作很方便，例如，將管理員帳戶新增至所有電腦。

Kaspersky Endpoint Security 允許您在加密磁碟機之前自動建立身分驗證代理帳戶。您可以在“完整磁碟加密”政策設定中啟用自動建立身分驗證代理帳戶。您還可以使用單點登入 (SSO) 技術。

**如何透過管理主控台 (MMC) 新增身分驗證代理帳戶**

1. 開啟“*管理身分驗證代理帳戶*”工作的內容。
2. 在工作內容中，選取“**設定**”區域。
3. 點擊“**新增**”→“**新增帳戶指令**”。
4. 在開啟之視窗的“**Windows 帳戶**”欄位中，指定將用於建立身分驗證代理帳戶的 Microsoft Windows 帳戶名稱。
5. 如果您手動輸入了 Windows 帳戶名稱，請點擊“**允許**”按鈕以定義帳戶安全識別碼 (SID)。
   如果您點擊“**允許**”按鈕時選取不決定安全標識符 SID，SID 將在工作在電腦上執行時確定。

若要驗證 Windows 帳戶名稱是否正確輸入，必須定義 Windows 帳戶安全識別碼。如果電腦或受信任網域中不存在 Windows 帳戶，則"*管理身分驗證代理帳戶*"工作將以發生錯誤結束。

6. 如果您希望將先前為身分驗證代理建立的現有帳戶取代為正在建立的帳戶，請選擇"**更換現有帳戶**"核取方塊。

當您在管理身分驗證代理帳戶的群組工作中新增身分驗證代理建立命令時，此步驟將可用。當您在*管理身分驗證代理帳戶*本機工作的內容中新增身分驗證代理建立命令時，此步驟將不可用。

7. 在"**使用者名稱**"欄位中，輸入在身分驗證過程中必須輸入的身分驗證代理帳戶名，以便存取加密的硬碟磁碟機。

8. 如果您希望在身分驗證期間應用程式提示使用者輸入身分驗證代理帳戶以便存取加密硬碟，請選取"**允許基於密碼的身分驗證**"。設定身分驗證代理帳戶的密碼。如有必要，您可以在首次身分驗證後向使用者請求新密碼。

9. 如果您希望在存取加密硬碟磁碟機身分驗證期間應用程式提示使用者輸入連線至電腦的令牌或智慧卡，請選取"**允許基於憑證的身分驗證**"。選取一個憑證檔案以使用智慧卡或權杖進行身分驗證。

10. 如有必要，在"**指令敘述**"欄位中輸入您需要管理指令的身分驗證代理帳戶的詳細資料。

11. 在"**在身分驗證代理進行驗證的權限**"塊中，為使用指令中指定的帳戶的使用者設定在身分驗證代理中存取身分驗證。

12. 儲存變更。

**如何透過網頁主控台新增身分驗證代理帳戶**

1. 在網頁主控台的主視窗中，選擇**資產（裝置）→工作**。

   工作清單開啟。

2. 點擊 Kaspersky Endpoint Security 的"**管理身分驗證代理帳戶**"工作。

   工作內容視窗將開啟。

3. 選擇"**應用程式設定**"標籤。

4. 在身分驗證代理帳戶清單中，點擊"**新增**"按鈕。

   這將啟動"身分驗證代理帳戶管理精靈"。

5. 選取"**新增**"指令類型。

6. 選取使用者帳戶。您可以從網域帳戶清單中選取帳戶，也可以手動輸入帳戶名稱。前往下一步。

   Kaspersky Endpoint Security 會確定帳戶安全識別碼 (SID)。這是驗證帳戶所必需的。如果輸入的使用者名稱不正確，Kaspersky Endpoint Security 將以發生錯誤結束工作。

7. 設定身分驗證代理帳戶設定。

   - **建立新的身分驗證代理帳戶來取代現有帳戶**Kaspersky Endpoint Security 將掃描電腦上的現有帳戶。如果電腦上和工作中的使用者安全 ID 相符，則 Kaspersky Endpoint Security 將根據工作變更使用者帳戶設定。

   - **使用者名稱**身分驗證代理帳戶的預設使用者名稱與使用者的網域名稱相對應。

- **允許基於密碼的身分驗證**設定身分驗證代理帳戶的密碼。如有必要，您可以在首次身分驗證後向使用者請求新密碼。如此一來，每個使用者將擁有自己的唯一密碼。您還可以在政策中為身分驗證代理帳戶設定密碼強度要求。

- **允許基於憑證的身分驗證**選取一個憑證檔案以使用智慧卡或權杖進行身分驗證。如此一來，使用者將需要輸入智慧卡或權杖的密碼。

- **帳戶對加密資料的存取權限**設定使用者對加密磁碟機的存取權限。例如，您可以暫時停用使用者身分驗證，而不是刪除身分驗證代理帳戶。

- **註釋**如有必要，輸入帳戶說明。

8. 儲存變更。

9. 選中工作旁邊的核取方塊，然後點擊**"開始"**按鈕。

結果，在下次電腦啟動時，當工作完成後，新使用者可以完成身分驗證過程、載入作業系統和獲得對加密磁碟機的存取權限。

要變更身分驗證代理帳戶的密碼和其他設定，您需要向*"管理身分驗證代理帳戶"*工作新增特殊指令。使用群組工作很方便，例如，替換所有電腦上的管理員權杖憑證。

**如何透過管理主控台 (MMC) 變更身分驗證代理帳戶**

1. 開啟*"管理身分驗證代理帳戶"*工作的內容。

2. 在工作內容中，選取**"設定"**區域。

3. 點擊**"新增"→"編輯帳戶指令"**。

4. 在開啟之視窗的**"Windows 帳戶"**欄位中，指定要變更的 Microsoft Windows 使用者帳戶的名稱。

5. 如果您手動輸入了 Windows 帳戶名稱，請點擊**"允許"**按鈕以定義帳戶安全識別碼 (SID)。

   如果您點擊**"允許"**按鈕時選取不決定安全標識符 SID，SID 將在工作在電腦上執行時確定。

   若要驗證 Windows 帳戶名稱是否正確輸入，必須定義 Windows 帳戶安全識別碼。如果電腦或受信任網域中不存在 Windows 帳戶，則*"管理身分驗證代理帳戶"*工作將以發生錯誤結束。

6. 如果您想讓 Kaspersky Endpoint Security 將使用 Microsoft Windows 帳戶用**"Windows 帳戶"**栏位中指明的名稱建立的所有身分驗證代理帳戶的使用者名稱變更為在下面栏位中輸入的名稱，請選中**"變更使用者名稱"**核取方块並輸入身分驗證代理帳戶的新名稱。

7. 選取**"修改基於密碼的身分驗證設定"**核取方塊使基於密碼的身分驗證設定變為可用。

8. 如果您希望在身分驗證期間應用程式提示使用者輸入身分驗證代理帳戶以便存取加密硬碟，請選取**"允許基於密碼的身分驗證"**。設定身分驗證代理帳戶的密碼。

9. 如果您想讓 Kaspersky Endpoint Security 变更使用 Microsoft Windows 帳戶用**"Windows 帳戶"**栏位中指定的名称建立的所有身分驗證代理帳戶的密碼的值变更到下面指定的设定值，請選中**"編輯在身分驗證代理進行驗證時密碼變更的規則"**核取方块。

10. 在身分驗證中驗證身分時指定密碼變更設定的值。

11. 選取**"修改基於憑證的身分驗證設定"**核取方塊以便編輯基於 eToken 或智慧卡電子憑證的驗證設定。

12. 如果您希望在身分驗證期間應用程式提示使用者輸入連線至電腦的 eToken 或智能卡以便存取加密硬碟，請選取“**允許基於憑證的身分驗證**”。選取一個憑證檔案以使用智慧卡或權杖進行身分驗證。

13. 如果您想讓 Kaspersky Endpoint Security 變更使用 Microsoft Windows 帳戶用”**Windows 帳戶**“栏位中指定的名稱建立的所有身分驗證代理帳戶的指令敘述，請選中“**編輯指令敘述**“核取方块並編輯指令敘述。

14. 如果您想讓 Kaspersky Endpoint Security 變更身分驗證代理中使用者存取身分驗證對話的規則到以下使用 Microsoft Windows 帳戶用“**Windows 帳戶**”栏位中指明的名称指定的设定值，請選中“**編輯身分驗證代理中的身分驗證存取規則**“核取方块。

15. 在身分驗證代理中指定存取身分驗證對話方塊的規則。

16. 儲存變更。

**如何透過網頁主控台變更身分驗證代理帳戶**

1. 在網頁主控台的主視窗中，選擇**資產（裝置）→ 工作**。

   工作清單開啟。

2. 點擊 Kaspersky Endpoint Security 的“**管理身分驗證代理帳戶**”工作。

   工作內容視窗將開啟。

3. 選擇“**應用程式設定**”標籤。

4. 在身分驗證代理帳戶清單中，點擊“**新增**”按鈕。

   這將啟動“身分驗證代理帳戶管理精靈”。

5. 選取“**變更**”指令類型。

6. 選取使用者帳戶。您可以從網域帳戶清單中選取帳戶，也可以手動輸入帳戶名稱。前往下一步。

   Kaspersky Endpoint Security 會確定帳戶安全識別碼 (SID)。這是驗證帳戶所必需的。如果輸入的使用者名稱不正確，Kaspersky Endpoint Security 將以發生錯誤結束工作。

7. 選中要編輯的設定旁邊的核取方塊。

8. 設定身分驗證代理帳戶設定。

   - **建立新的身分驗證代理帳戶來取代現有帳戶**Kaspersky Endpoint Security 將掃描電腦上的現有帳戶。如果電腦上和工作中的使用者安全 ID 相符，則 Kaspersky Endpoint Security 將根據工作變更使用者帳戶設定。

   - **使用者名稱**身分驗證代理帳戶的預設使用者名稱與使用者的網域名稱相對應。

   - **允許基於密碼的身分驗證**設定身分驗證代理帳戶的密碼。如有必要，您可以在首次身分驗證後向使用者請求新密碼。如此一來，每個使用者將擁有自己的唯一密碼。您還可以在政策中為身分驗證代理帳戶設定密碼強度要求。

   - **允許基於憑證的身分驗證**選取一個憑證檔案以使用智慧卡或權杖進行身分驗證。如此一來，使用者將需要輸入智慧卡或權杖的密碼。

   - **帳戶對加密資料的存取權限**設定使用者對加密磁碟機的存取權限。例如，您可以暫時停用使用者身分驗證，而不是刪除身分驗證代理帳戶。

   - **註釋**如有必要，輸入帳戶說明。

9. 儲存變更。

10. 選中工作旁邊的核取方塊，然後點擊**"開始"**按鈕。

要刪除身分驗證代理帳戶，您需要向*"管理身分驗證代理帳戶"*工作新增特殊指令。使用群組工作很方便，例如，刪除已解雇員工的帳戶。

**如何透過管理主控台 (MMC) 刪除身分驗證代理帳戶**

1. 開啟*"管理身分驗證代理帳戶"*工作的內容。

2. 在工作內容中，選取**"設定"**區域。

3. 點擊**"新增"**→**"刪除帳戶指令"**。

4. 在開啟之視窗的**"Windows 帳戶"**欄位中，指定用於建立您要刪除的身分驗證代理帳戶的 Windows 使用者帳戶名稱。

5. 如果您手動輸入了 Windows 帳戶名稱，請點擊**"允許"**按鈕以定義帳戶安全識別碼 (SID)。

   如果您點擊**"允許"**按鈕時選取不決定安全標識符 SID，SID 將在工作在電腦上執行時確定。

   若要驗證 Windows 帳戶名稱是否正確輸入，必須定義 Windows 帳戶安全識別碼。如果電腦或受信任網域中不存在 Windows 帳戶，則*"管理身分驗證代理帳戶"*工作將以發生錯誤結束。

6. 儲存變更。

**如何透過網頁主控台刪除身分驗證代理帳戶**

1. 在網頁主控台的主視窗中，選擇**資產（裝置）→工作**。

   工作清單開啟。

2. 點擊 Kaspersky Endpoint Security 的**"管理身分驗證代理帳戶"**工作。

   工作內容視窗將開啟。

3. 選擇**"應用程式設定"**標籤。

4. 在身分驗證代理帳戶清單中，點擊**"新增"**按鈕。

   這將啟動"身分驗證代理帳戶管理精靈"。

5. 選取**"刪除"**指令類型。

6. 選取使用者帳戶。您可以從網域帳戶清單中選取帳戶，也可以手動輸入帳戶名稱。

7. 儲存變更。

8. 選中工作旁邊的核取方塊，然後點擊**"開始"**按鈕。

結果，在下次電腦啟動時，當工作完成後，使用者將無法完成身分驗證過程和載入作業系統。Kaspersky Endpoint Security 將拒絕對加密資料的存取。

要查看可以透過代理完成身分驗證並載入作業系統的使用者清單，您需要前往受管理電腦的內容。

**如何透過管理主控台 (MMC) 查看身分驗證代理帳戶清單**

1. 開啟卡巴斯基安全管理中心管理主控台。
2. 在主控台樹狀目錄中，選擇**"裝置"**。
3. 點擊以開啟電腦內容視窗。
4. 在電腦內容視窗中，選取**"工作"**區域。
5. 在工作清單中，選擇**"管理身分驗證代理帳戶"**，然後點擊兩下開啟工作內容。
6. 在工作內容中，選取**"設定"**區域。

結果，您將能夠存取此電腦上的身分驗證代理帳戶清單。只有清單中的使用者可以透過代理完成身分驗證並載入作業系統。

**如何透過網頁主控台查看身分驗證代理帳戶清單**

1. 在網頁主控台的主視窗中，選擇**資產（裝置）→ 受管理裝置**。
2. 點擊要查看其中身分驗證代理帳戶清單的電腦名稱。
3. 在電腦內容中選取**工作**標籤。
4. 在工作清單中，選取**"管理身分驗證代理帳戶"**。
5. 在工作內容中，選取**"應用程式設定"**區域。

結果，您將能夠存取此電腦上的身分驗證代理帳戶清單。只有清單中的使用者可以透過代理完成身分驗證並載入作業系統。

# 配合身分驗證代理使用令牌和智慧卡

存取加密硬碟時可將令牌或智慧卡用於身分驗證。為此，必須將權杖或智慧卡的電子憑證檔案新增到*"管理身分驗證代理帳戶"*工作中。

如果電腦硬碟磁碟機使用 AES256 加密演算法進行加密，則可以使用令牌或智慧卡。如果使用 AES256 演算法加密了電腦硬碟磁碟機，新增電子憑證檔案到指令將被拒絕。

Kaspersky Endpoint Security 支援以下權杖、智慧卡讀卡器和智慧卡：

- SafeNet eToken PRO 64K (4.2b)；
- SafeNet eToken PRO 72K Java；
- SafeNet eToken 4100-72K Java；
- SafeNet eToken 5100；
- SafeNet eToken 5105；

- SafeNet eToken 7300；
- EMC RSA SID 800；
- Gemalto IDPrime.NET 510；
- Gemalto IDPrime.NET 511；
- Rutoken ECP；
- Rutoken ECP Flash；
- Athena IDProtect Laser；
- SafeNet eToken PRO 72K Java；
- Aladdin-RD JaCarta PKI。

要把令牌檔案或智慧卡電子憑證檔案新增到用於建立身分驗證代理帳戶的指令中，請首先使用用於管理憑證的協力廠商軟體儲存檔案。

權杖或智慧卡憑證必須具有下列內容：

- 憑證必須相容 X.509 標準，並且憑證必須具有 DER 編碼。
- 此憑證包含至少 1024 位長度的 RSA 金鑰。

如果權杖或智慧卡的電子憑證不符合此要求，則無法將憑證檔案載入至用於建立身分驗證代理帳戶的指令中。

憑證"`KeyUsage`"參數的值必須為 `keyEncipherment` 或 `dataEncipherment`。`KeyUsage` 參數可確認憑證的用途。如果參數的值不同，卡巴斯基安全管理中心將下載憑證檔案，但會顯示警告。

如果使用者遺失了令牌或智慧卡，則管理員必須將令牌或智慧卡電子憑證檔案新增到指令，以建立身分驗證代理帳戶。然後使用者必須完成在加密裝置上接受加密裝置存取或還原資料的過程。

# 硬碟磁碟機解密

即使沒有允許資料加密的目前產品授權，您也可以解密硬碟磁碟機。

*若要解密硬碟磁碟機，請執行以下操作：*

1. 在卡巴斯基安全管理中心管理主控台樹狀目錄中，選取**政策**。
2. 選擇必要的政策並點擊以開啟政策內容。
3. 在政策視窗中，選擇"**資料加密 → 完整磁碟加密**"。
4. 在"**加密技術**"下拉清單中選取加密硬碟磁碟機的技術。

5. 請執行以下操作之一：

- 在“**加密模式**”下拉清單中，選取“**解密所有硬碟磁碟機**”選取方塊，如果您希望解密所有加密的硬碟磁碟機。
- 將您希望解密的加密硬碟磁碟機新增至“**請勿加密以下硬碟磁碟機**”表。

該選項僅對卡巴斯基磁碟加密技術有效。

6. 儲存變更。

您可以使用加密監控工具來控制使用者電腦上的磁盤加密或解密過程。您可以從“主應用程式視窗”執行加密監控工具。




加密監控器

如果使用者在解密使用卡巴斯基磁碟加密技術進行了加密的硬碟磁碟機期間關閉了或重新啟動了電腦，下次啟動作業系統之前系統將載入身分驗證代理。成功透過身分驗證並在作業系統啟動後，Kaspersky Endpoint Security 將還原硬碟磁碟機解密。

如果作業系統在在解密使用卡巴斯基磁碟加密技術進行了加密的硬碟磁碟機期間切換至休眠模式，作業系統退出休眠模式時將載入身分驗證代理。成功透過身分驗證並在作業系統啟動後，Kaspersky Endpoint Security 將還原硬碟磁碟機解密。進行硬碟磁碟機解密後，在第一次重新開機作業系統之前，休眠模式將不可用。

如果作業系統在硬碟磁碟機解密期間進入休眠模式，則當作業系統結束休眠模式時，Kaspersky Endpoint Security 將還原硬碟磁碟機加密，且無需載入身分驗證。

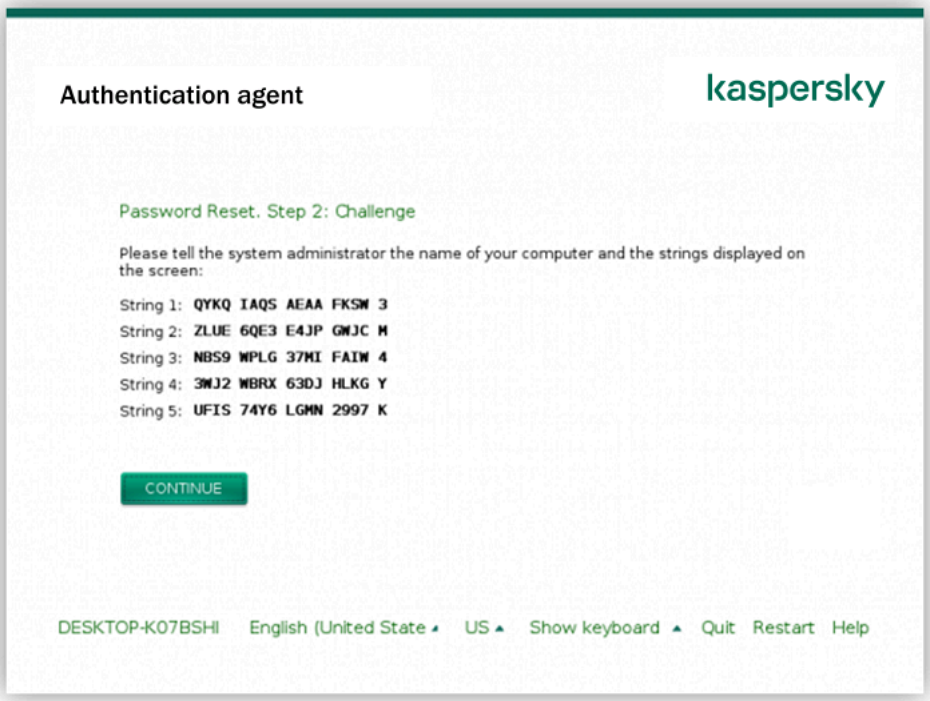
# 還原對受卡巴斯基磁碟加密技術防護的磁碟機的存取權限

如果使用者忘記受卡巴斯基磁碟加密技術防護之硬碟的存取密碼，則需要啟動還原程序（請求-回應）。如果在磁碟加密設定中啟用了該功能，則您也可以使用“服務帳戶”獲取對硬碟的存取權限。

## 還原對系統硬碟的存取權限

還原對受卡巴斯基磁碟加密技術防護的系統硬碟的存取權限包括以下步驟：

1. 使用者將請求模組報告給管理員（請參見下圖）。
2. 管理員將請求模組輸入卡巴斯基安全管理中心，接收回應模組並將回應模組報告給使用者。
3. 使用者在“身分驗證代理”介面中輸入回應模組，並獲得對硬碟的存取權限。




還原對受卡巴斯基磁碟加密技術防護的系統硬碟的存取權限

要啟動還原程序，使用者需要在“身分驗證代理”介面中點擊“**Forgot your password**”按鈕。

**如何在管理主控台 (MMC) 中獲取受卡巴斯基磁碟加密技術防護的系統硬碟的回應模組**

1. 開啟卡巴斯基安全管理中心管理主控台。
2. 在主控台樹狀目錄中，選擇“**裝置**”。
3. 在“**裝置**”標籤上，選取使用者正在請求加密資料存取權限的電腦，然後點擊滑鼠右鍵開啟內容功能表。
4. 在內容功能表中，選取“**授予離線模式下的存取權限**”。

5. 在開啟的視窗中選擇**"身分驗證代理"**標籤。

6. 在**"正在使用的加密演算法"**塊中，選取加密演算法：**AES56** 或 **AES256**。

   資料加密演算法取決於分發套件中包含的 AES 加密庫：*強加密* 或 *簡單加密*。AES 加密庫與應用程式一起安裝。

7. 在**"帳戶"**下拉清單中，選取請求還原磁碟機存取權限的使用者身分驗證代理帳戶名稱。

8. 在**硬碟磁碟機**下拉清單中，選取您要還原存取的加密硬碟磁碟機。

9. 在**"使用者請求"**塊中輸入使用者填寫的請求塊。

結果，對使用者的還原身分驗證代理帳戶的使用者名稱和密碼的請求回應模組內容將顯示在**"存取金鑰"**欄位中。將回應模組的內容傳達給使用者。




授予在離線模式下存取

### 如何在網頁主控台中獲取受卡巴斯基磁碟加密技術防護的系統硬碟的回應模組

1. 在網頁主控台的主視窗中，選擇**資產（裝置）→ 受管理裝置**。

2. 選中要還原其磁碟機存取權限的電腦名稱旁邊的核取方塊。

3. 點擊**"同意存取離線模式下的裝置"**。

4. 在開啟的視窗中，選擇**"身分驗證代理"**區域。

5. 在**"帳戶"**下拉清單中，選取為請求還原身分驗證代理帳戶名稱和密碼的使用者建立的身分驗證代理帳戶的名稱。

6. 輸入使用者傳達的請求模組。

對使用者的還原身分驗證代理帳戶的使用者名稱和密碼的請求回應模組內容將顯示在視窗底部。將回應模組的內容傳達給使用者。

完成還原程序後，身分驗證代理將提示使用者變更密碼。

還原對非系統硬碟的存取權限

還原對受卡巴斯基磁碟加密技術防護的非系統硬碟的存取權限包括以下步驟：

1. 使用者將請求存取檔案傳送給管理員。
2. 管理員將根據請求存取檔案新增到卡巴斯基安全管理中心中，建立存取金鑰檔案並將該檔案傳送給使用者。
3. 使用者將存取金鑰檔案新增到 Kaspersky Endpoint Security 並獲得對硬碟的存取權限。

要啟動還原程序，使用者需要嘗試存取硬碟。結果，Kaspersky Endpoint Security 將建立一個請求存取檔案（副檔名為 KESDC 的檔案），使用者需要將該檔案傳送給管理員，例如透過電子郵件傳送。

**如何在管理主控台 (MMC) 中獲取加密的非系統硬碟的存取金鑰檔案**

1. 開啟卡巴斯基安全管理中心管理主控台。
2. 在主控台樹狀目錄中，選擇**"裝置"**。
3. 在**"裝置"**標籤上，選取使用者正在請求加密資料存取權限的電腦，然後點擊滑鼠右鍵開啟內容功能表。
4. 在內容功能表中，選取**"授予離線模式下的存取權限"**。
5. 在開啟的視窗中選擇**"資料加密"**標籤。
6. 在**"資料加密"**標籤上點擊**"瀏覽"**按鈕 。
7. 在用來選取請求存取檔案的視窗中，指定從使用者那裡接收的檔案路徑。

您將看到有關使用者請求的資訊。卡巴斯基安全管理中心會產生一個金鑰檔案。透過電子郵件將產生的加密資料存取金鑰檔案傳送給使用者。或儲存該存取檔案並使用任何可用方法來傳輸該檔案。




授予在離線模式下存取

**如何在中網頁主控台獲取非系統硬碟存取金鑰檔案**

1. 在網頁主控台的主視窗中，選擇**資產（裝置）→受管理裝置**。
2. 選中要還原其資料存取權限的電腦名稱旁邊的核取方塊。
3. 點擊**"同意存取離線模式下的裝置"**。
4. 選擇**"資料加密"**。
5. 點擊**"選擇檔案"**按鈕，然後選取從使用者處收到的請求存取檔案（副檔名為 KESDC 的檔案）。
   網頁主控台將顯示有關請求的資訊。這將包括使用者請求存取的檔案所在的電腦名稱。
6. 點擊**"儲存金鑰"**按鈕，然後選取一個資料夾來儲存加密資料存取金鑰檔案（副檔名為 KESDR 的檔案）。

結果，您將能夠獲取加密資料存取金鑰，您需要將該金鑰傳輸給使用者。

# 使用身分驗證代理服務帳戶登入

Kaspersky Endpoint Security 允許您在加密磁碟機之前新增身分驗證代理服務帳戶。獲取電腦的存取權限時（例如，當使用者忘記密碼時）需要該服務帳戶。您也可以將服務帳戶作為備用帳戶。若要新增帳戶，在**"**磁碟加密設定**"**中選擇一個服務帳戶，然後輸入使用者帳戶名稱（預設為 `ServiceAccount`）。若要使用代理進行身分驗證，您需要一個一次性密碼。

**如何在管理主控台 (MMC) 中查找一次性密碼**

1. 開啟卡巴斯基安全管理中心管理主控台。
2. 在主控台樹狀目錄中，選擇**"裝置"**。
3. 點擊以開啟電腦內容視窗。
4. 在電腦內容視窗中，選取**"工作"**區域。
5. 在工作清單中，選擇**"管理身分驗證代理帳戶"**，然後點擊兩下開啟工作內容。
6. 在工作內容視窗中，選取**"設定"**區域。
7. 在帳戶清單中，選擇身分驗證代理服務帳戶（比如，`WIN10-USER\ServiceAccount`）。
8. 在**"動作"**下拉式清單中，選取**"檢視帳戶"**。
9. 在帳戶內容中，選擇**"顯示原始密碼"**核取方塊。
10. 複製用來用服務帳戶登入的一次性密碼。

**如何在網頁主控台中查找一次性密碼**

1. 在網頁主控台的主視窗中，選擇**資產（裝置）→受管理裝置**。
2. 點擊要查看其中身分驗證代理帳戶清單的電腦名稱。
   這將開啟電腦內容。

3. 在電腦內容中選取**工作**標籤。

4. 在工作清單中，選取**"管理身分驗證代理帳戶"**。

5. 在工作內容中，選取**"應用程式設定"**區域。

6. 在帳戶清單中，選擇身分驗證代理服務帳戶（比如，`WIN10-USER\ServiceAccount`）。

7. 在帳戶內容中，選擇**"顯示密碼"**核取方塊。

8. 複製用來用服務帳戶登入的一次性密碼。

每次使用者用服務帳戶進行身分驗證時，Kaspersky Endpoint Security 都會自動更新密碼。使用代理進行身分驗證後，您必須輸入 Windows 帳戶密碼。當使用服務帳戶登入時，您無法使用 SSO 技術。

# 更新作業系統

更新受完整磁碟加密 (FDE) 防護的電腦的作業系統有許多特殊注意事項。按如下方式更新作業系統：先更新一台電腦上的作業系統，然後更新一小部分電腦上的作業系統，再更新網路中所有電腦上的作業系統。

如果正在使用 Kaspersky 磁碟加密技術，則在啟動作業系統之前會載入身分驗證代理。使用身分驗證代理，使用者可以登入系統並獲得對加密磁碟機的存取權限。然後，作業系統開始載入。如果在使用 Kaspersky 磁碟加密技術防護的電腦上啟動作業系統更新，則作業系統更新精靈將刪除身分驗證代理。結果，電腦可被鎖定，因為作業系統載入程式將無法存取加密磁碟機。

作業系統更新的特點：

- **透過 WSUS 更新作業系統**。您可以按照常規方式更新作業系統。
- **從 ISO 更新作業系統**。若要更新作業系統，您必須指定包含卡巴斯基磁碟加密驅動程式的資料夾。應用程式會自動將驅動程式複製到單獨的資料夾。請執行以下操作：

  1. 掛載 ISO 映像。
  2. 使用以下金鑰開始安裝系統更新：

     ```
     setup.exe /ReflectDrivers %ProgramFiles(x86)%\Kaspersky
     Lab\KES.12.12\reflect_drivers
     ```

只有當電腦執行 Windows 10 1607 (RS1) 或更高版本時才可以自動進行作業系統更新。若要升級早期版本的作業系統，建議您先解密磁碟，執行作業系統升級，然後加密磁碟。

如果正在使用 BitLocker 磁碟機加密技術，則無需解密硬碟磁碟機即可更新 Windows 10。有關 BitLocker 的詳細資訊，請存取 Microsoft 網站。

# 消除加密功能更新的錯誤

在以前版本的應用程式升級到 Kaspersky Endpoint Security for Windows 12.12 時，將更新"完整磁碟加密"。

開始更新“完整磁碟加密”功能時，可能出現以下錯誤：

- 無法初始化更新。
- 裝置與身分驗證代理不相容。

*要消除在開始新應用程式版本中的“完整磁碟加密”功能的更新流程時出現的錯誤：*

1. 解密硬碟磁碟機。
2. 再次加密硬碟磁碟機。

在更新“完整磁碟加密”功能的過程中，可能出現以下錯誤：

- 無法完成更新。
- “完整磁碟加密”升級回溯完成但出錯。

*要消除在“完整磁碟加密”功能更新流程中出現的錯誤，*

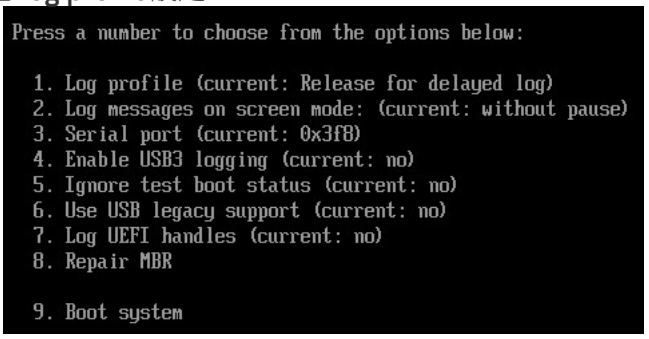
請使用還原實用程式還原對加密裝置的存取權限。

# 身分驗證代理偵錯

偵錯檔案中關於身分驗證代理的應用程式記錄服務資訊和關於身分驗證代理使用者操作的資訊。

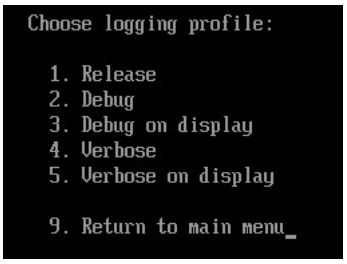
*若要啟用身分驗證代理偵錯：*

1. 啟用 Kaspersky Endpoint Security 偵錯。
2. 重新啟動電腦。
3. 當帶有加密硬碟磁碟機的電腦啟動後，請按 **F3** 按鈕，調出用於設定身分驗證代理設定的視窗。
4. 在 FDE 引導程式啟動後，選取 **KES (FDE <version>)** 啟動管理員。
5. 在啟動管理員功能表中，前往**Log profile**設定。




啟動管理員功能表

6. 在記錄設定檔設定視窗中，選取偵錯等級：




身分驗證代理偵錯等級

- **Release**如果選定此選項，應用程式不會在偵錯檔案中記錄有關身分驗證代理事件的資訊。
- **Debug**如果選取此選項，應用程式在偵錯檔案中記錄身分驗證代理的操作和身分驗證代理的使用者執行操作。
- **Debug on display**如果選取此選項，應用程式將在偵錯檔案中記錄身分驗證代理的操作輸入和身分驗證代理的使用者執行操作，並透過 COM 連接埠傳輸此檔案。

  如果帶有已加密硬碟磁碟機的電腦透過 COM 連接埠連線至另一台電腦時，可以從另一台電腦檢查身分驗證代理事件。
- **Verbose**如果選取此選項，應用程式將把身分驗證代理的操作輸入和身分驗證代理的使用者執行操作納入偵錯等級。

  > 與"**Debug**"選項的等級相比，在此選項下，輸入項的詳細資訊程度要更高。輸入項的詳細資訊程度更高將會減慢身分驗證代理和作業系統的啟動。
- **Verbose on display**如果選取此選項，應用程式將在偵錯檔案中詳細記錄身分驗證代理的操作輸入和身分驗證代理的使用者操作，並透過 COM 連接埠傳輸此檔案。

  > 與"**Debug on display**"選項的等級相比，在此選項下，輸入項的詳細資訊程度要更高。輸入項的詳細資訊程度更高將會減慢身分驗證代理和作業系統的啟動。

選取偵錯等級後，啟動管理員會再次顯示功能表。

7. 在啟動管理員功能表中，選取**Boot system**。

FDE 引導程式會啟動身分驗證代理。

重現該問題。

如果電腦上有已加密的硬碟磁碟機或者在完整磁碟加密期間，資料將記錄在身分驗證代理偵錯檔案中。

8. 若要停止偵錯過程，請返回「支援工具」視窗並停用偵錯。

結果，將在 `%ProgramData%\Kaspersky Lab\KES.12.12\Traces` 資料夾中建立身分驗證代理 KES.SRV 操作偵錯檔案。與其他程式偵錯檔案不一樣，身分驗證代理偵錯檔案不會傳送至 Kaspersky。如有必要，您可以手動將身分驗證代理偵錯檔案傳送至 Kaspersky 以供分析。

# 編輯身分驗證代理說明文字

> 在編輯身分驗證代理的說明訊息之前，請檢視預啟動環境中支援的字元清單（請參見下文）。

*若要編輯身分驗證說明郵件，請執行以下操作：*

1. 在卡巴斯基安全管理中心管理主控台樹狀目錄中，選取**政策**。
2. 選擇必要的政策並點擊以開啟政策內容。
3. 在政策視窗中，選擇**"資料加密 → 一般加密設定"**。
4. 在**"範本"**塊中，點擊**"說明"**按鈕。
5. 在開啟的視窗中，執行以下操作：
   - 輸入帳戶憑證時選取**"身分驗證"**標籤編輯身分驗證代理視窗中顯示的說明。
   - 選取**"變更密碼"**標籤可編輯在變更身分驗證代理帳戶密碼時顯示在身分驗證視窗中的說明。
   - 選取**"還原密碼"**標籤可編輯在還原身分驗證代理帳戶密碼時顯示在身分驗證視窗中的說明。
6. 編輯說明訊息。
   如果您希望還原原始文字，則點擊**"根據預設"**按鈕。

   > 您可以輸入包含 16 或更少行的說明文字。每行的最大長度為 64 個字元。

7. 儲存變更。

身分驗證代理說明郵件中字串的有限支援

在預啟動環境下，支援以下 Unicode 字元：

- 基本拉丁字母 (0000 - 007F)
- 附加 Latin-1 字元 (0080 - 00FF)
- 延伸 Latin-A (0100 - 017F)
- 延伸 Latin-B (0180 - 024F)
- 未組合的延伸 ID 字元 (02B0 - 02FF)
- 組合變音標記 (0300 - 036F)
- 希臘和科普特字母 (0370 - 03FF)
- 西瑞爾字母 (0400 - 04FF)
- 希伯來語 (0590 - 05FF)
- 阿拉伯語 (0600 - 06FF)
- 附加延伸拉丁語 (1E00 - 1EFF)

- 標點符號 (2000 - 206F)
- 貨幣符號 (20A0 - 20CF)
- 類似字母的符號 (2100 - 214F)
- 幾何符號 (25A0 - 25FF)
- 阿拉伯語 Script-B (FE70 - FEFF)

該清單中未指定的字元在預啟動環境中不受支援。不建議在身分驗證代理說明訊息中使用此類字元。

## 測試執行身分驗證代理後，刪除剩餘物件與資料

應用程式移除期間，如果 Kaspersky Endpoint Security 在身分驗證代理測試執行後偵測到系統硬碟上遺留物件和資料，則應用程式移除將被中斷且在刪除此類物件和資料之前無法繼續。

僅在例外情況下，當身分驗證代理測試執行後，遺留的物件和資料才能留在系統硬碟上。舉例來說，這可能發生在已套用卡巴斯基安全管理中心加密政策時，如果沒有重新啟動電腦，或者如果身分驗證代理測試執行後應用程式啟動失敗。

您可以使用以下方式刪除身分驗證代理在測試執行之後遺留在系統硬碟磁碟機中的物件和資料：

- 使用卡巴斯基安全管理中心政策。
- 使用還原實用程式。

*若要使用卡巴斯基安全管理中心政策，刪除測試身分驗證代理後剩餘資料與物件：*

1. 將帶有配置為解密所有電腦硬碟設定的卡巴斯基安全管理中心政策套用至電腦。
2. 啟動 Kaspersky Endpoint Security。

*若要刪除與驗證代理不相容的應用程式資訊，請執行以下操作：*

請在命令列中輸入 `avp pbatestreset`。

# BitLocker 管理

*BitLocker* 是 Windows 作業系統內建的加密技術。Kaspersky Endpoint Security 可讓您利用 Kaspersky Next 基礎架構控制和管理 Bitlocker。BitLocker 可對邏輯磁區進行加密。BitLocker 不能用於卸除式磁碟機的加密。有關 BitLocker 的詳細資訊，請參閱 Microsoft 文件。

加密磁碟時，BitLocker將引導程式和其他輔助檔案放入 system partition。此分割區未加密。作業系統在安裝 Windows 時會自動建立系統分割區。如果在安裝 Windows 之前磁碟已完全分割，則作業系統無法建立系統分割區。在這種情況下，當啟動 BitLocker 磁碟加密時，作業系統會提示使用者對磁碟重新分割，並建立系統分割區。建立系統分割區後，作業系統啟動 BitLocker 加密。

BitLocker 使用受信任平台模組提供對存取金鑰的安全儲存。A *Trusted Platform Module* (TPM) 是一個與安全相關並提供基本功能的微晶片（例如用於儲存加密金鑰）。受信任平台模組通常安裝在電腦主機板上並且透過硬體匯流排與其他所有系統元件進行互動。使用 TPM 是儲存 BitLocker 存取金鑰最安全的方式，因為 TPM 提供了啟動前系統完整性驗證。您仍然可以在沒有 TPM 的電腦上對磁碟機進行加密。在這種情況下，將使用密碼對存取金鑰進行加密。BitLocker 使用以下身分驗證方式：

- TPM。
- TPM 和 PIN。
- 密碼。

對系統硬碟磁碟機進行加密後，使用者需要透過 BitLocker 身分驗證才能啟動作業系統。身分驗證完成後，BitLocker 將允許使用者登入。BitLocker 不支援單點登錄技術 (SSO)。

在對磁碟機進行加密後，BitLocker 會建立一個主密碼。Kaspersky Endpoint Security 會將主密碼傳送到卡巴斯基安全管理中心，以便您可以還原對磁碟的存取，例如，如果使用者忘記了密碼。

如果使用者使用 BitLocker 對磁碟進行加密，Kaspersky Endpoint Security 會將有關磁碟加密的資訊傳送到卡巴斯基安全管理中心。但是，Kaspersky Endpoint Security 不會將主密碼傳送到卡巴斯基安全管理中心，因此將無法使用卡巴斯基安全管理中心還原對磁碟的存取。為使 BitLocker 與卡巴斯基安全管理中心正常協同工作，請解密磁碟機，然後使用政策重新對該磁碟機進行加密。您可以在本機解密磁碟機，也可以使用政策來解密磁碟機。

如果正在使用 Windows 群組政策，請在政策設定中關閉 BitLocker 管理。Windows 政策設定可能與 Kaspersky Endpoint Security 政策設定衝突。在對磁碟機進行加密時，可能會發生錯誤。

# 啟動 BitLocker 磁碟機加密

在開始完整磁碟加密之前，建議您確保電腦未受到感染。若要執行操作，應啟動完整掃描或關鍵區域掃描工作。在已被 rootkit 感染的電腦上執行完整磁碟加密可能導致電腦無法執行。

若要在執行適用於伺服器的 Windows 作業系統的電腦上使用 BitLocker 磁碟機加密，可能需要安裝“BitLocker 磁碟機加密”元件。可使用作業系統工具（新增角色和元件精靈）安裝該元件。有關安裝“BitLocker 磁碟機加密”的更多資訊，請參閱 Microsoft 文件。

**如何透過管理主控台 (MMC) 執行 BitLocker 磁碟機加密**

1. 在卡巴斯基安全管理中心管理主控台樹狀目錄中，選取**政策**。
2. 選擇必要的政策並點擊以開啟政策內容。
3. 在政策視窗中，選擇“**資料加密 → 完整磁碟加密**”。
4. 在“**加密技術**”下拉式清單中，選取“**BitLocker 磁碟機加密**”。
5. 在“**加密模式**”下拉式清單中，選取“**加密所有硬碟磁碟機**”。

如果電腦安裝了多個作業系統，在加密後，您將能夠只載入執行了加密的作業系統。

6. 設定進階 BitLocker 磁碟機加密選項（參見下表）。

7. 儲存變更。

**如何透過網頁主控台和雲端主控台執行 BitLocker 磁碟機加密**

1. 在網頁主控台的主視窗中，選擇**資產（裝置）→政策和設定檔**。

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”**資料加密**”→”**完整磁碟加密**”。

5. 選擇 **BitLocker 磁碟加密** 技術。

6. 在“**裝置操作**”塊中，選取“**加密所有硬碟磁碟機**”。

   如果電腦安裝了多個作業系統，在加密後，您將能夠只載入執行了加密的作業系統。

7. 設定進階 BitLocker 磁碟機加密選項（參見下表）。

8. 儲存變更。

您可以使用加密監控工具來控制使用者電腦上的磁盤加密或解密過程。您可以從“主應用程式視窗”執行加密監控工具。




加密監控器

套用政策後，應用程式將顯示以下查詢（取決於身分驗證設定）：

- 僅 TPM。無需使用者輸入。磁碟將在電腦重新啟動時被加密。
- TPM + PIN / 密碼。如果 TPM 模組可用，將顯示 PIN 碼提示視窗。如果 TPM 模組不可用，您將看到一個用於預啟動身分驗證的密碼提示視窗。
- 僅密碼。您將看到一個用於預啟動身分驗證的密碼提示視窗。

如果為電腦作業系統啟用聯邦資訊處理標準相容模式，則在 Windows 8 及更早版本的作業系統中，將顯示儲存裝置連線請求以儲存還原金鑰檔案。您可以將多個還原金鑰檔案儲存在單一儲存裝置上。

設定密碼或 PIN 後，BitLocker 將要求您重新啟動電腦以完成加密。接下來，使用者需要完成 BitLocker 身分驗證過程。完成身分驗證過程後，使用者必須登入到系統。載入作業系統後，BitLocker 將完成加密。

如果無法存取加密金鑰，使用者可以請求區域網路管理員提供還原金鑰（如果還原金鑰在較早前未儲存在儲存裝置上或已遺失）。

BitLocker 磁碟機加密元件設定

| 參數 | 描述 |
| --- | --- |
| **啟用需要在平板電腦上預啟動鍵盤輸入的 BitLocker 身分驗證** | 在預啟動環境中使用需要資料輸入的身分驗證，即使此平台沒有能力進行預啟動輸入（例如使用平板電腦上的觸控式螢幕鍵盤）。<br>平板電腦的觸控式螢幕在預啟動環境中不可用。例如，要在平板電腦上完成 BitLocker 身分驗證，使用者必須連線 USB 鍵盤。<br>如果選定此核取方塊，則允許使用需要預啟動輸入的身分驗證。我們建議在預啟動環境中僅對擁有備用資料輸入的裝置（例如除了觸控式螢幕鍵盤之外的 USB 鍵盤）使用此設定。<br>如果清除此核取方塊，則無法在平板電腦上使用 BitLocker 磁碟機加密。 |
| **使用硬體加密(Windows 8 和後續版本)** | 如果選定此核取方塊，則應用程式將應用硬體加密。這可以提高加密速度並使用較少的電腦資源。 |
| **僅加密使用的磁碟空間(Windows 8 和後續版本)** | 該核取方塊可啟用/停用將加密區域僅限為已用硬碟磁區的選項。該限制可減少加密時間。<br>在啟動加密後啟用或者停用"**僅加密使用的磁碟空間(減少加密時間)**"功能不會修改此設定，直到硬碟磁碟機被解密為止。開始加密之前您必須選擇或清除該核取方塊。<br>如果選定該核取方塊，則僅加密使用的硬碟部分。Kaspersky Endpoint Security 將自動加密新增的新資料。<br>如果清空該核取方塊，整個硬碟將被加密，包括先前刪除和修改檔案殘留的碎片。<br>建議對尚未修改或刪除資料的新硬碟使用該選項。如果對已在使用中的硬碟應用加密，則建議加密整個硬碟。這樣可確保防護所有資料，甚至已刪除的資料也能夠部分還原。<br>預設情況下，會取消勾選核取方塊。 |

| 參數 | 描述 |
| --- | --- |
| **身分驗證方法** | **僅限密碼（Windows 8 和後續版本）**<br>如果選定此選項，Kaspersky Endpoint Security 將在使用者嘗試存取加密磁碟時提示使用者輸入密碼。<br>沒有使用受信任平台模組 (TPM) 時可以選擇此選項。<br>**受信任平台模組 (TPM)**<br>如果選定此核取方塊，則 BitLocker 使用受信任平台模組 (TPM)。<br>A *Trusted Platform Module* (TPM) 是一個與安全相關並提供基本功能的微晶片（例如用於儲存加密金鑰）。受信任平台模組通常安裝在電腦主機板上並且透過硬體匯流排與其他所有系統元件進行互動。<br>對於執行 Windows 7 或 Windows Server 2008 R2 的電腦，只能使用 TPM 模組進行加密。如果未安裝 TPM 模組，則無法進行 BitLocker 加密。不支援在這些電腦上使用密碼。<br>配有受信任平台模組的裝置可以建立只能使用此裝置解密的加密金鑰。受信任平台模組將使用其自有的根儲存金鑰加密加密金鑰。根儲存金鑰儲存在受信任平台模組中。這提供了防禦駭客攻擊加密金鑰的附加防護。<br>預設情況下已選擇此操作。<br>您可以為存取加密金鑰設定一層額外防護，用密碼或者 PIN 加密金鑰：<br>• **為 TPM 使用 PIN**如果選中此核取方塊，使用者可以使用 PIN 碼存取儲存在受信任平台模組 (TPM) 中的加密金鑰。如果清除此核取方塊，則會禁止使用者使用 PIN 碼。要存取加密金鑰，使用者必須輸入密碼。<br>• **受信任平台模組 (TPM)，或密碼（如果 TMP 不可使用）**如果選定此選項，當受信任平台模組 (TPM) 不可用時，使用者可使用密碼存取加密金鑰。如果清除該核取方塊且 TPM 不可用，則將不會啟動完整磁碟加密。<br>選取的身分驗證方法必須透過指定密碼或 PIN 要求來進行設定：<br>• **最小 PIN 長度(字元數)**<br>• **最小密碼長度(字元數)**<br>• **限制 TPM 的密碼/PIN 代碼有效期（天）**<br>• **使用增強型 PIN (字母和數字)**。*增強 PIN* 允許使用除了數字字元的其它字元：大寫和小寫拉丁字母，特殊字元，和空格。 |
| **自動重新建立還原金鑰（天）** | 自動更新密碼以還原對 BitLocker 防護的磁碟機的存取權限。如果該核取方塊被選中，請指定還原金鑰密碼的有效期。這將有助於防止還原金鑰密碼重新使用。 |

# 解密受 BitLocker 防護的硬碟磁碟機

使用者可以使用作業系統解密磁碟（"*關閉 BitLocker*"功能）。之後，Kaspersky Endpoint Security 將提示使用者重新對磁碟進行加密。除非在政策中啟用磁碟解密，否則 Kaspersky Endpoint Security 將提示您加密磁碟。

### 如何透過管理主控台 (MMC) 解密受 BitLocker 防護的硬碟磁碟機

1. 在卡巴斯基安全管理中心管理主控台樹狀目錄中，選取**政策**。
2. 選擇必要的政策並點擊以開啟政策內容。
3. 在政策視窗中，選擇"**資料加密 → 完整磁碟加密**"。
4. 在"**加密技術**"下拉式清單中，選取"**BitLocker 磁碟機加密**"。
5. 在"**加密模式**"下拉式清單中，選取"**解密所有硬碟磁碟機**"。
6. 儲存變更。

### 如何透過網頁主控台和雲端主控台解密 BitLocker 加密的硬碟磁碟機

1. 在網頁主控台的主視窗中，選擇**資產（裝置）→ 政策和設定檔**。
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”**資料加密**”→”**完整磁碟加密**”。

5. 選擇 **BitLocker 磁碟加密** 技術。

6. 在“**裝置操作**”塊中，選取“**解密所有硬碟磁碟機**”。

7. 儲存變更。

您可以使用加密監控工具來控制使用者電腦上的磁盤加密或解密過程。您可以從“主應用程式視窗”執行加密監控工具。




加密監控器

# 還原對 BitLocker 防護的磁碟機的存取權限

如果使用者忘記了由 BitLocker 加密的硬碟存取密碼，則需要啟動還原程序（請求-回應）。

如果電腦的作業系統啟用了聯邦資訊處理標準 (FIPS) 相容模式，則在 Windows 8 和更早版本中，還原金鑰檔案將在加密之前儲存到卸除式磁碟機中。要恢復對磁碟機的存取權限，請插入卸除式磁碟機，然後按照螢幕上的說明進行操作。

還原對 BitLocker 加密的硬碟存取權限包括以下步驟：

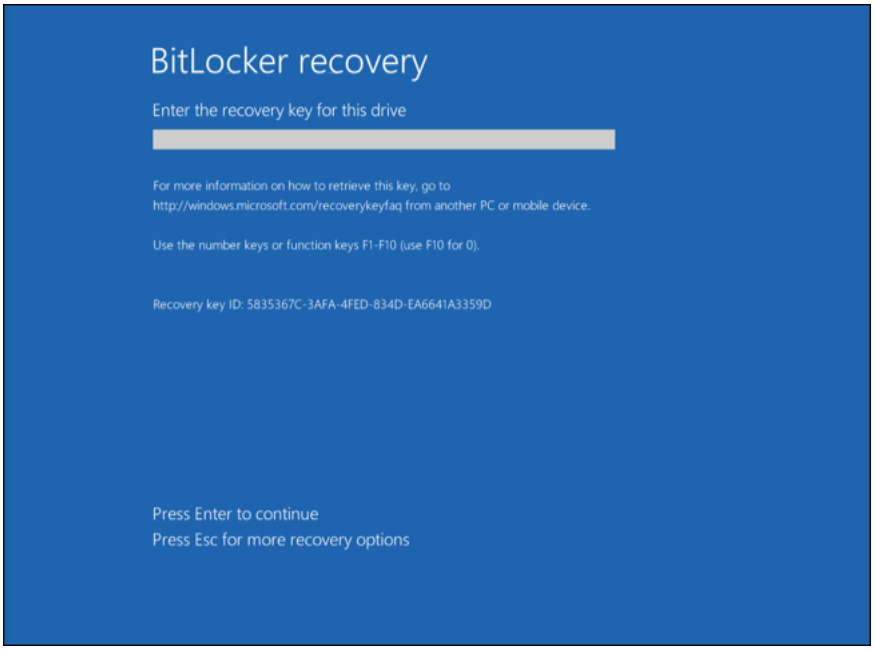
1. 使用者告知管理員還原金鑰 ID（請參見下圖）。
2. 管理員在卡巴斯基安全管理中心中驗證電腦內容中的還原金鑰 ID。使用者提供的 ID 必須與電腦內容中顯示的 ID 相符。
3. 如果還原金鑰 ID 相符，管理員將為使用者提供還原金鑰或傳送還原金鑰檔案。

   還原金鑰檔案用於執行以下作業系統的電腦：

   - Windows 7
   - Windows 8
   - Windows Server 2008
   - Windows Server 2011
   - Windows Server 2012

   對於所有其他作業系統，請使用還原金鑰。

   若要防止重新使用還原金鑰密碼，您可以在政策設定中設定密碼自動更新。
4. 使用者輸入還原金鑰，然後獲得對硬碟的存取權限。




還原對 BitLocker 加密磁碟機的存取權限

還原對系統磁碟機的存取權限

要啟動還原程序，使用者需要在預先引導身分驗證階段按 **Esc** 鍵。

### 如何在管理主控台 (MMC) 中檢視由 BitLocker 加密的系統磁碟機的還原金鑰

1. 開啟卡巴斯基安全管理中心管理主控台。
2. 在主控台樹狀目錄中，選擇**"受管理裝置"**。
3. 在**"裝置"**標籤上，選取使用者正在請求加密資料存取權限的電腦，然後點擊滑鼠右鍵開啟內容功能表。
4. 在內容功能表中，選取**"授予離線模式下的存取權限"**。
5. 在開啟的視窗中選擇**"存取受 BitLocker 防護的系統磁碟機"**標籤。
6. 提示使用者在 BitLocker 密碼輸入視窗中輸入還原金鑰 ID，然後在**"還原金鑰 ID"**欄位中對比該 ID。

> 如果 ID 不比對，該金鑰無法用於還原指定系統磁碟的存取。請確保選定電腦的名稱與使用者電腦的名稱相符合。

結果，您將有權存取還原金鑰或還原金鑰檔案，該金鑰或金鑰檔案將需要傳輸給使用者。




還原對用 BitLocker 加密的磁碟機的存取權限

### 如何在網頁主控台和雲端主控台中檢視由 BitLocker 加密的系統磁碟機的還原金鑰

1. 在網頁主控台的主視窗中，選擇**資產（裝置）→ 受管理裝置**。
2. 選中要還原其磁碟機存取權限的電腦名稱旁邊的核取方塊。
3. 點擊**"同意存取離線模式下的裝置"**。
4. 在開啟的視窗中，選擇**"BitLocker"**區域。

5. 驗證還原金鑰 ID使用者提供的 ID 必須與電腦設定中顯示的 ID 相符。

如果 ID 不比對，該金鑰無法用於還原指定系統磁碟的存取。請確保選定電腦的名稱與使用者電腦的名稱相符合。

6. 點擊“**接收金鑰**”。

結果，您將有權存取還原金鑰或還原金鑰檔案，該金鑰或金鑰檔案將需要傳輸給使用者。

載入作業系統後，Kaspersky Endpoint Security 會提示使用者變更密碼或 PIN 代碼。設定新密碼或 PIN 代碼後，BitLocker 將建立一個新的主密碼，並將該金鑰傳送給卡巴斯基安全管理中心。結果，還原金鑰和還原金鑰檔案將被更新。如果使用者未變更密碼，您可以在下次作業系統載入時使用舊的還原金鑰。

Windows 7 电脑不允許變更密碼或 PIN 代碼。輸入還原金鑰並載入作業系統後，Kaspersky Endpoint Security 將不再提示使用者變更密碼或 PIN 代碼。因此，不可能設定新的密碼或 PIN 代碼。此問題源於作業系統的特殊性。要繼續，您需要重新加密硬碟磁碟機。

還原對非系統磁碟機的存取權限

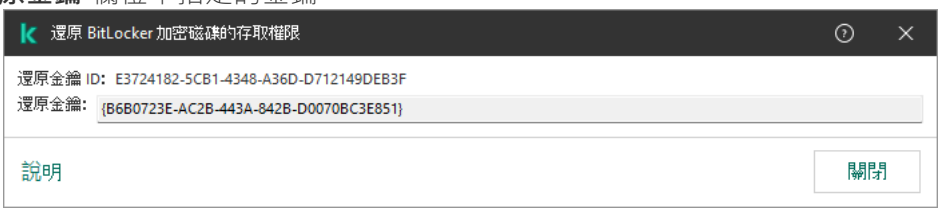
要啟動還原程序，使用者需要在提供磁碟機存取的視窗中點擊“**Forgot your password**”連結。獲得對加密磁碟機的存取權限後，使用者可以在 BitLocker 設定中啟用在 Windows 身分驗證期間自動解鎖磁碟機。

**如何在管理主控台 (MMC) 中檢視由 BitLocker 加密的非系統磁碟機的還原金鑰**

1. 開啟卡巴斯基安全管理中心管理主控台。
2. 在管理主控台樹狀目錄中，選擇**進階 → 資料加密與防護 → 加密磁碟機**資料夾。
3. 在工作區中選取您想要為其建立存取金鑰檔案的加密裝置，然後在裝置的內容功能表中，點擊“**在 Kaspersky Endpoint Security 中獲取裝置的存取權限**”。
4. 提示使用者在 BitLocker 密碼輸入視窗中輸入還原金鑰 ID，然後在“**還原金鑰 ID**”欄位中對比該 ID。

如果 ID 不比對，該金鑰無法用於還原指定磁碟的存取。請確保選定電腦的名稱與使用者電腦的名稱相符合。

5. 向使用者傳送“**還原金鑰**”欄位中指定的金鑰。




還原對用 BitLocker 加密的磁碟機的存取權限

**如何在網頁主控台和雲端 中檢視由 BitLocker 加密的非系統磁碟機的還原金鑰**

1. 在網頁主控台的主視窗中，選擇**操作 → 資料加密與防護 → 加密磁碟機**。
2. 選中要還原其磁碟機存取權限的電腦名稱旁邊的核取方塊。
3. 點擊**"同意存取離線模式下的裝置"**。
   這將啟動用於授予裝置存取權限的精靈。
4. 按照精靈的說明授予對裝置的存取權限：
   a. 選擇 **Kaspersky Endpoint Security for Windows** 外掛程式
   b. 驗證還原金鑰 ID使用者提供的 ID 必須與電腦設定中顯示的 ID 相符。

      如果 ID 不比對，該金鑰無法用於還原指定系統磁碟的存取。請確保選定電腦的名稱與使用者電腦的名稱相符合。

   c. 點擊**"接收金鑰"**。

結果，您將有權存取還原金鑰或還原金鑰檔案，該金鑰或金鑰檔案將需要傳輸給使用者。

# 暫停 BitLocker 防護以更新軟體

更新作業系統、安裝作業系統的更新套件、或者更新開啟了 BitLocker 防護的其它軟體有眾多特殊考量。安裝更新可能需要多次重啟電腦。每次重啟後，使用者必須完成 BitLocker 身分驗證。為了確保更新正確安裝，您可以暫時關閉 BitLocker 身分驗證。在此情況下，磁碟機保持加密，使用者可以在登入系統後存取資料。若要管理 BitLocker 身分驗證，您可以使用"*BitLocker 防護管理*"工作。您可以使用此工作指定不需要 BitLocker 身分驗證的電腦重啟次數。按這種方式，在更新安裝和 *BitLocker 防護管理*工作完成後，BitLocker 身分驗證將自動啟用。您可以隨時啟用 BitLocker 身分驗證。

**如何使用管理主控台 (MMC) 暫停 BitLocker 防護**

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

啟動"工作精靈"。按照精靈的說明進行操作。

步驟 1. 選取工作類型

選取"**Kaspersky Endpoint Security for Windows (12.12)**"→"**BitLocker 防護管理**"。

步驟 2. BitLocker 防護管理

配置 BitLocker 身份驗證.若要暫停 BitLocker 防護，請選擇**暫時允許略過 BitLocker 身分驗證**並輸入無需 BitLocker 身分驗證進行重啟的次數（1 到 15 次）。如有必要，輸入工作的到期日期和時間。工作會在指定時間關閉，當電腦重啟時使用者必須完成 BitLocker 身分驗證。

步驟 3. 選取將要對其分配工作的裝置

選取將要執行工作的電腦。下列選項可用：

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

步驟 4. 定義工作名稱

輸入工作名稱，例如 *更新到 Windows 10*。

步驟 5. 完成工作建立

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

**如何使用網頁主控台暫停 BitLocker 防護**

1. 在網頁主控台的主視窗中，選擇**資產（裝置）→ 工作**。
   工作清單開啟。
2. 點擊"**新增**"。

啟動"工作精靈"。按照精靈的說明進行操作。

步驟 1. 配置一般工作設定

配置一般工作設定：

1. 在**應用程式**下拉式清單中，選取 **Kaspersky Endpoint Security**。
2. 在"**工作類型**"下拉式清單中，選取"**BitLocker 防護管理**"。

3. 在**"工作名稱"**欄位中，輸入簡要說明，例如，*"更新到 Windows 10"*。

4. 在**"要將工作指派給的裝置"**塊中，選取工作範圍。

步驟 2. BitLocker 防護管理

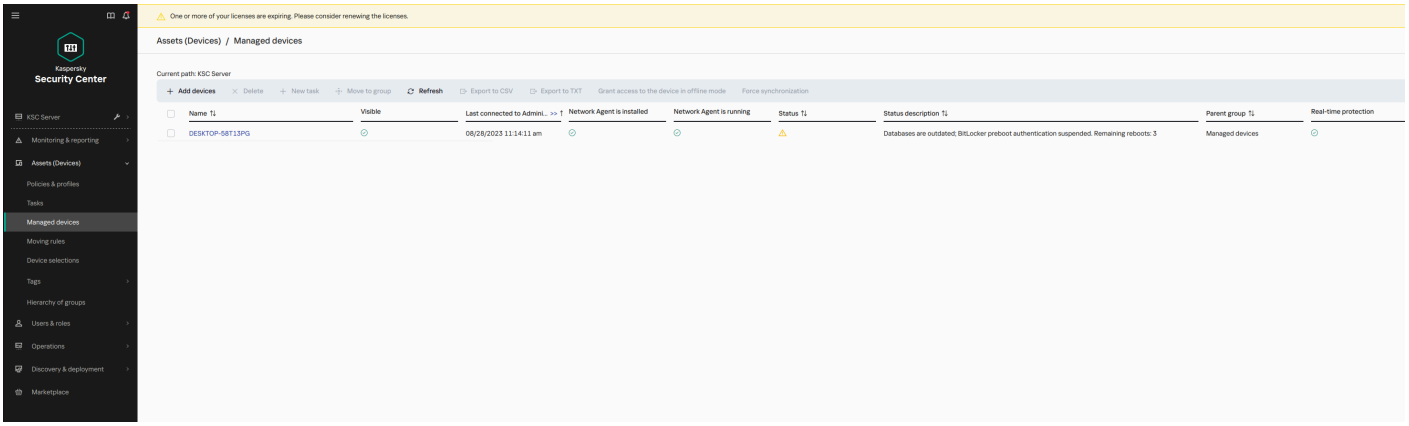
配置 BitLocker 身份驗證.若要暫停 BitLocker 防護，請選擇**暫時允許略過 BitLocker 身分驗證**並輸入無需 BitLocker 身分驗證進行重啟的次數（1 到 15 次）。如有必要，輸入工作的到期日期和時間。工作會在指定時間關閉，當電腦重啟時使用者必須完成 BitLocker 身分驗證。

步驟 3. 完成工作建立

結束精靈。在工作清單中將顯示一個新工作。

要執行工作，請選中與工作對應的核取方塊，然後點擊**"開始"**按鈕。

因此，當工作執行時，下次電腦重啟後，BitLocker 不會提示使用者進行身分驗證。每次電腦未經 BitLocker 身分驗證重啟後，Kaspersky Endpoint Security 都會產生相應事件並記錄剩餘的重啟次數。Kaspersky Endpoint Security 然後會傳送事件到卡巴斯基安全管理中心供管理員監控。您還可以在裝置狀態描述中卡巴斯基安全管理中心主控台的**受管理裝置**資料夾中檢視剩餘的重新啟動次數。




受管理裝置清單

當達到指定的重啟次數或者工作的到期時間時，BitLocker 身分驗證會自動開啟。要獲得對資料的存取權限，使用者必須完成 BitLocker 身分驗證。

在執行 Windows 7 的電腦上，BitLocker 不能計數電腦重啟。計數 Windows 7 電腦上的重啟由 Kaspersky Endpoint Security 處理。因此，若要在每次重啟後自動開啟 BitLocker 身分驗證，必須啟動 Kaspersky Endpoint Security。

若要提前開啟 BitLocker 身分驗證，請開啟 *BitLocker 防護管理*工作內容並選擇**"每次重啟請求身分驗證"**。

# 本機電腦磁碟機上檔案級加密

如果 Kaspersky Endpoint Security 安裝在執行 Windows for Workstations 的電腦上，則該元件可用。如果 Kaspersky Endpoint Security 安裝在執行 Windows for Servers 的電腦上，則該元件不可用。

檔案加密具有以下特殊功能：

- Kaspersky Endpoint Security 僅為作業系統本機使用者設定資料加密/解密標準資料夾內的檔案。Kaspersky Endpoint Security 不會加密/解密標準資料夾內的行動使用者設定檔、強制使用者設定檔、臨時使用者設定檔或重新定位的資料夾。
- Kaspersky Endpoint Security 不會加密其修改可能損害作業系統和安裝的應用程式的檔案。例如，加密排除項清單中包含以下檔案和包含所有內嵌物件內的檔案：
  - %WINDIR%；
  - %PROGRAMFILES% 和 %PROGRAMFILES(X86)%；
  - Windows 登錄檔。

  您無法檢視或編輯這個加密排除清單。儘管加密排除項目清單中的檔案和資料夾可以新增至加密清單，但在檔案加密期間，它們不會被加密。

# 加密本機電腦磁碟中的檔案

Kaspersky Endpoint Security 不加密位於 OneDrive 雲端儲存或者其他資料夾中以 OneDrive 作為名稱的檔案。Kaspersky Endpoint Security 還會封鎖將加密檔案複製到 OneDrive 資料夾（如果這些檔案未被新增至解密規則）。

*若要在本機磁碟機上加密檔案，請執行以下操作：*

1. 在卡巴斯基安全管理中心管理主控台樹狀目錄中，選取**政策**。
2. 選擇必要的政策並點擊以開啟政策內容。
3. 在政策視窗中，選擇**"資料加密 → 檔案級加密"**。
4. 在**"加密模式"**下拉式清單中，選取**"根據規則"**。
5. 在**"加密"**標籤下，點擊**"新增"**按鈕，在下拉清單中選取以下項目之一：
   a. 選取**"預定義資料夾"**項目將 Kaspersky 專家建議的本機使用者設定檔資料夾的檔案新增至加密規則。
      - **文件**作業系統的*"檔案"*資料夾及其子資料夾中的檔案。
      - **我的最愛**作業系統標準的*"我的最愛"*資料夾及其子資料夾中的檔案。

- **桌面**作業系統的"*桌面*"資料夾及其子資料夾中的檔案。
- **暫存檔**與電腦上安裝的應用程式的操作有關的暫存檔案。例如，Microsoft Office 應用程式會建立包含文件備份副本的暫存檔案。

  不建議加密暫存檔案，因為這可能造成資料損失。例如，Microsoft Word 會在處理文件時建立暫存檔案。如果加密了暫存檔卻沒有加密原始檔案，使用者在嘗試儲存文件時可能會收到"*存取被拒絕*"錯誤。此外，Microsoft Word 可以儲存檔案，但是下次卻無法開啟文件，即資料將丟失。

- **Outlook 檔案**與 Outlook 郵件用戶端操作有關的檔案：資料檔案 (PST)、離線資料檔案 (OST)、離線通訊錄檔案 (OAB) 和個人通訊錄檔案 (PAB)。

b. 選取"**自訂資料夾**"項目手動將資料夾路徑輸入至加密規則。

新增資料夾路徑時，請遵循以下規則：

- 使用環境變數（例如，`%FOLDER%\UserFolder\`）。您只能在路徑的開頭使用一次環境變數。
- 不要使用相對路徑。
- 不要使用 `*` 和 `?` 字元。
- 不要使用 UNC 路徑。
- 使用 `;` 或 `,` 作為分隔符號。

c. 選取"**根據副檔名選取檔案**"項目將單個檔案副檔名新增至加密規則。Kaspersky Endpoint Security 將加密電腦本機磁碟機中所有指定副檔名的檔案。

d. 選取"**根據副檔名群組選擇檔案**"項將成組的檔案副檔名新增至加密規則（例如，*Microsoft Office 文件*）。Kaspersky Endpoint Security 會加密電腦上所有本機磁碟機上副檔名群組中列出副檔名的檔案。

6. 儲存變更。

一旦套用該政策，Kaspersky Endpoint Security 將加密所有加密規則中包括的和解密規則中不包括的檔案。

檔案加密具有以下特殊功能：

- 如果將同一檔案新增到加密規則和解密規則中，則 Kaspersky Endpoint Security 將執行以下操作：
  - 如果檔案未加密，則 Kaspersky Endpoint Security 不會對此檔案進行加密。
  - 如果檔案已加密，則 Kaspersky Endpoint Security 會解密此檔案。
- 如果新檔案符合加密規則的條件，則 Kaspersky Endpoint Security 會繼續對這些檔案進行加密。例如，當您變更未加密檔案的內容（路徑或副檔名）時，該檔案將符合加密規則的條件。Kaspersky Endpoint Security 將對該檔案進行加密。
- 當使用者建立其內容複合加密規則條件的新檔案時，Kaspersky Endpoint Security 將在檔案開啟時加密檔案。
- Kaspersky Endpoint Security 將會延遲加密已開啟的檔案，直至其關閉。

- 如果您在本機磁碟機上將加密檔案移動至另一個資料夾，該檔案仍保持為加密狀態，而與該資料夾是否包含在加密規則中無關。
- 如果您解密檔案並將其複製到解密規則中未包含的另一個本機資料夾中，則可能會對該檔案的副本進行加密。要防止對複製的檔案進行加密，請為目標資料夾建立解密規則。

# 為應用程式建立加密檔案存取規則

預設情況下，所有應用程式都以解密狀態處理加密檔案。如果您經常使用某些應用程式（例如，瀏覽器或文字編輯器），您可以建立加密檔案存取規則來保護資訊。

我們建議為 Microsoft Internet Explorer 和 Microsoft Edge 瀏覽器建立加密檔案存取規則。由於這些瀏覽器的工作方式，如果您將加密檔案上傳到網站（例如，雲端儲存），該檔案會自動解密。這可能會導致資料外洩。無法使用這些瀏覽器上傳加密檔案。我們建議設定 **僅授予存取採用密文格式加密的檔案** 規則。您不需要為其他瀏覽器（例如 Google Chrome）建立規則。

*要為應用程式建立加密檔案存取規則：*

1. 在卡巴斯基安全管理中心管理主控台樹狀目錄中，選取**政策**。
2. 選擇必要的政策並點擊以開啟政策內容。
3. 在政策視窗中，選擇**"資料加密 → 檔案級加密"**。
4. 在**"加密模式"**下拉式清單中，選取**"根據規則"**。

   存取規則僅在**"根據規則"**模式下可以套用。在**"根據規則"**模式下套用存取規則後，如果您切換到**"保留不變"**模式，則 Kaspersky Endpoint Security 將忽略所有存取規則。所有應用程式將能夠存取所有加密檔案。

5. 在視窗右側，選取**"應用程式規則"**標籤。
6. 如果您只希望從卡巴斯基安全管理中心清單中選取應用程式，則點擊**"新增"**按鈕並在下拉清單中選取**"卡巴斯基安全管理中心應用程式清單"**項目。
   a. 指定篩選條件以縮小表中的應用程式清單。若要執行操作，指定**"應用程式"**、**"供應商"**和**"新增的時間段"**參數的值和**"群組"**塊中所有核取方塊。
   b. 點擊**"重新整理"**。
   c. 清單將列出比對所套用篩選條件的應用程式。
   d. 在**"應用程式"**列中，選取您要為其建立加密檔案存取規則的應用程式旁邊的核取方塊。
   e. 在**"應用程式規則"**下拉清單中，選取確定應用程式對加密檔案存取權限的規則。
   f. 在**"之前為應用程式選擇的動作"**下拉清單中，選取根據先前為應用程式所建立加密檔案存取規則 Kaspersky Endpoint Security 所執行的操作。

應用程式加密檔案存取規則的詳情將顯示在**"應用程式規則"**標籤中。

7. 如果您希望手動選取應用程式，則點擊**"新增"**按鈕並在下拉清單中選取**"自訂應用程式"**項目。

   a. 在輸入欄位中，輸入應用程式可執行檔的名稱或名稱清單，包括其副檔名。

      您也可以從卡巴斯基安全管理中心清單中新增應用程式可執行檔的名稱，請點擊**"從卡巴斯基安全管理中心清單中新增"**按鈕。

   b. 如有必要，在**"敘述"**欄位中輸入應用程式清單的說明。

   c. 在**"應用程式規則"**下拉清單中，選取確定應用程式對加密檔案存取權限的規則。

   應用程式加密檔案存取規則的詳情將顯示在**"應用程式規則"**標籤中。

8. 儲存變更。

# 加密特定應用程式建立或修改的檔案

您可以建立規則，Kaspersky Endpoint Security 將加密此規則內指定的應用程式建立或修改的檔案。

加密規則應用前指定應用程式建立或修改的檔案將不會被加密。

*若要加密特定應用程式建立或修改的檔案：*

1. 在卡巴斯基安全管理中心管理主控台樹狀目錄中，選取**政策**。
2. 選擇必要的政策並點擊以開啟政策內容。
3. 在政策視窗中，選擇**"資料加密 → 檔案級加密"**。
4. 在**"加密模式"**下拉式清單中，選取**"根據規則"**。

   加密規則僅在**"根據規則"**模式下可以套用。在**"根據規則"**模式下套用加密規則後，如果您切換到**"保留不變"**模式，則 Kaspersky Endpoint Security 將忽略所有加密規則。先前加密的檔案將保持為加密。

5. 在視窗右側，選取**"應用程式規則"**標籤。
6. 如果您只希望從卡巴斯基安全管理中心清單中選取應用程式，則點擊**"新增"**按鈕並在下拉清單中選取**"卡巴斯基安全管理中心應用程式清單"**項目。

   a. 指定篩選條件以縮小表中的應用程式清單。若要執行操作，指定**"應用程式"**、**"供應商"**和**"新增的時間段"**參數的值和**"群組"**塊中所有核取方塊。

   b. 點擊**"重新整理"**。

      清單將列出比對所套用篩選條件的應用程式。

   c. 在**"應用程式"**欄中選中您要加密其建立之檔案的應用程式旁的核取方塊。

   d. 在**"應用程式規則"**下拉式清單中，選取**"加密所有已建立的檔案"**。

   e. 在**"之前為應用程式選擇的動作"**下拉清單中，選取根據先前為應用程式所建立加密檔案存取規則 Kaspersky Endpoint Security 所執行的操作。

選定應用程式建立或修改檔案的加密規則的資訊將顯示在**"應用程式規則"**標籤上的表中。

7. 如果您希望手動選取應用程式，則點擊**"新增"**按鈕並在下拉清單中選取**"自訂應用程式"**項目。

   a. 在輸入欄位中，輸入應用程式可執行檔的名稱或名稱清單，包括其副檔名。

      您也可以從卡巴斯基安全管理中心清單中新增應用程式可執行檔的名稱，請點擊**"從卡巴斯基安全管理中心清單中新增"**按鈕。

   b. 如有必要，在**"敘述"**欄位中輸入應用程式清單的說明。

   c. 在**"應用程式規則"**下拉式清單中，選取**"加密所有已建立的檔案"**。

   選定應用程式建立或修改檔案的加密規則的資訊將顯示在**"應用程式規則"**標籤上的表中。

8. 儲存變更。

# 生成解密規則

*若要生成解密規則：*

1. 在卡巴斯基安全管理中心管理主控台樹狀目錄中，選取**政策**。
2. 選擇必要的政策並點擊以開啟政策內容。
3. 在政策視窗中，選擇**"資料加密 → 檔案級加密"**。
4. 在**"加密模式"**下拉式清單中，選取**"根據規則"**。
5. 在**"解密"**標籤下，點擊**"新增"**按鈕，在下拉清單中選取以下項目之一：

   a. 選取**"預定義資料夾"**項目將 Kaspersky 專家建議的本機使用者設定檔資料夾的檔案新增至解密規則。

   b. 選取**"自訂資料夾"**項目手動將資料夾路徑輸入至解密規則。

   c. 選取**"根據副檔名選取檔案"**項目將單個檔案副檔名新增至解密規則。Kaspersky Endpoint Security 不會加密電腦本機磁碟機中所有指定副檔名的檔案。

   d. 選取**"根據副檔名群組選擇檔案"**項將成組的檔案副檔名新增至解密規則（例如，*Microsoft Office 文件*）。Kaspersky Endpoint Security 不會加密電腦所有本機磁碟機上副檔名群組中列出副檔名的檔案。

6. 儲存變更。

如果同一個的檔案被新增至加密規則和解密規則中，Kaspersky Endpoint Security 不會加密已加密的檔案，但是會解密已經加密的檔案。

# 在本機電腦磁碟機上解密檔案

*若要在本機磁碟機上解密檔案，請執行以下操作：*

1. 在卡巴斯基安全管理中心管理主控台樹狀目錄中，選取**政策**。
2. 選擇必要的政策並點擊以開啟政策內容。
3. 在政策視窗中，選擇**"資料加密 → 檔案級加密"**。
4. 在視窗右側，選取**"加密"**標籤。
5. 從加密清單中移除您要解密的檔案和資料夾。為此，請選擇檔案，然後在**"刪除"**按鈕的內容功能表中選擇**" 刪除規則並解密檔案"**項目。

   從加密清單中刪除的檔案和資料夾將自動新增至解密清單中。
6. 建立檔案解密清單。
7. 儲存變更。

套用政策後，Kaspersky Endpoint Security 將會解密被新增至解密清單的已加密檔案。

如果未加密檔案的參數（檔案路徑/檔案名稱/檔案副檔名）已變更為比對已新增至解密清單的物件的參數時，Kaspersky Endpoint Security 將會解密這些加密檔案。

Kaspersky Endpoint Security 將會延遲解密已開啟的檔案，直至其關閉。

# 建立加密資料

在將檔案傳送給公司網路外部的使用者時，為了防護您的資料，可以使用加密封包。由於電子郵件使用者端具有檔案大小限制，因此使用加密檔案可以方便地透過卸除式磁碟機傳輸大檔案。

在建立加密封包之前，Kaspersky Endpoint Security 將提示使用者輸入密碼。為了可靠地防護資料，您可以啟用密碼強度檢查並指定密碼強度要求。這將防止使用者使用短密碼和簡單密碼，例如 1234。

**在管理主控台 (MMC) 中建立新的加密存檔時如何啟用密碼強度檢查**

1. 在卡巴斯基安全管理中心管理主控台樹狀目錄中，選取**政策**。
2. 選擇必要的政策並點擊以開啟政策內容。
3. 在政策視窗中，選擇**"資料加密 → 一般加密設定"**。
4. 在**"密碼設定"**塊中，點擊**"設定"**按鈕。
5. 在開啟的視窗中選擇**"加密檔案"**標籤。
6. 在建立加密封包時進行密碼複雜度設定。

**在網頁主控台中建立新的加密存檔時如何啟用密碼強度檢查**

1. 在網頁主控台的主視窗中，選擇**資產（裝置）→政策和設定檔**。
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**"資料加密"→"檔案級加密"**。
5. 在**加密套件密碼設定**塊中，配置建立加密資料時所需的密碼強度條件。

您可以在安裝了Kaspersky Endpoint Security 且具有檔案級加密功能的電腦上建立加密封包。

向其內容位於 OneDrive 雲端儲存中的加密檔案中新增檔案時，Kaspersky Endpoint Security 會下載檔案內容並執行加密。

*若要建立加密檔案，請執行以下操作：*

1. 在任意檔案管理員中，選取要新增到加密封包的檔案或資料夾。右鍵點擊以開啟其內容功能表。
2. 在內容功能表中，選取**"新增加密檔案"**。




建立加密封包

3. 在開啟的視窗中，指定密碼並確認。
   密碼必須符合政策中指定的複雜度標準。
4. 點擊**"建立"**。

加密檔案建立過程將啟動。Kaspersky Endpoint Security 建立加密檔案時不會執行檔案壓縮。該程序完成後，將在選定的目標資料夾中建立一個受密碼防護的自行解壓縮加密封包（副檔名為 .exe 的可執行檔– ）。

要存取加密封包中的檔案，請按兩下以啟動解壓縮精靈，然後輸入密碼。如果忘記或遺失密碼，將無法還原密碼和存取加密封包中的檔案。您可以重新建立加密封包。

# 還原對加密檔案的存取權限

加密檔案時，Kaspersky Endpoint Security 會收到用於直接存取加密檔案的加密金鑰。如果使用者在資料加密過程中處於活動狀態的任何 Windows 帳戶下工作，則可以使用此加密金鑰直接存取加密檔案。如果使用者在資料加密過程中處於非活動狀態的 Windows 帳戶下工作，則必須連線至卡巴斯基安全管理中心才能存取加密檔案。

在以下情況下可能無法存取加密檔案：

- 使用者電腦上儲存了加密金鑰，但是未連線卡巴斯基安全管理中心以管理這些加密金鑰。在這種情況下，要存取加密檔案，使用者必須從區域網路管理員處請求加密檔案存取權限。

  如果不存在對卡巴斯基安全管理中心的存取權限，您必須：

  - 請求存取金鑰以存取電腦硬碟磁碟機上的加密檔案；
  - 若要存取卸除式磁碟機上所儲存的加密檔案，請為每個卸除式磁碟機上加密的檔案請求單獨的存取金鑰。

- 加密元件被從使用者電腦上移除。在此情況下，使用者可以開啟本機和移動磁碟上的加密檔案，但是檔案內容將顯示為加密。

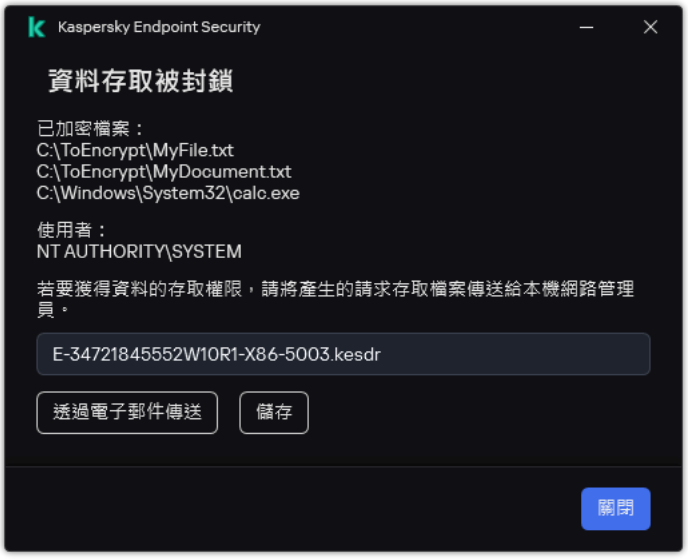
  在以下情況下，使用者可以使用加密檔案：

  - 檔案放置在建立於安裝了 Kaspersky Endpoint Security 的電腦上的加密檔案里。
  - 檔案儲存在允許攜帶式模式的卸除式磁碟機上。

要獲得對加密檔案的存取權限，使用者需要啟動還原程序（請求-回應）。

還原對加密檔案的存取權限包括以下步驟：

1. 使用者請求存取檔案並將其傳送給管理員（請參見下圖）。
2. 管理員將根據請求存取檔案新增到卡巴斯基安全管理中心中，建立存取金鑰檔案並將該檔案傳送給使用者。
3. 使用者將存取金鑰檔案新增到 Kaspersky Endpoint Security 並獲得對檔案的存取權限。




還原對加密檔案的存取權限

要啟動還原程序，使用者需要嘗試存取檔案。結果，Kaspersky Endpoint Security 將建立一個請求存取檔案（副檔名為 KESDC 的檔案），使用者需要將該檔案傳送給管理員，例如透過電子郵件傳送。

Kaspersky Endpoint Security 會產生請求存取檔案，該檔案可用來存取儲存在電腦磁碟機（本機磁碟機或卸除式磁碟機）上的所有加密檔案。

### 如何在管理主控台 (MMC) 中獲取加密資料存取金鑰檔案

1. 開啟卡巴斯基安全管理中心管理主控台。
2. 在主控台樹狀目錄中，選擇**"裝置"**。
3. 在**"裝置"**標籤上，選取使用者正在請求加密資料存取權限的電腦，然後點擊滑鼠右鍵開啟內容功能表。
4. 在內容功能表中，選取**"授予離線模式下的存取權限"**。
5. 在開啟的視窗中選擇**"資料加密"**標籤。
6. 在**"資料加密"**標籤上點擊**"瀏覽"**按鈕 。
7. 在用來選取請求存取檔案的視窗中，指定從使用者那裡接收的檔案路徑。

您將看到有關使用者請求的資訊。卡巴斯基安全管理中心會產生一個金鑰檔案。透過電子郵件將產生的加密資料存取金鑰檔案傳送給使用者。或儲存該存取檔案並使用任何可用方法來傳輸該檔案。




授予在離線模式下存取

### 如何在網頁主控台中獲取加密資料存取金鑰檔案

1. 在網頁主控台的主視窗中，選擇**資產（裝置）→ 受管理裝置**。
2. 選中要還原其資料存取權限的電腦名稱旁邊的核取方塊。
3. 點擊**"同意存取離線模式下的裝置"**。
4. 選擇**"資料加密"**。
5. 點擊**"選擇檔案"**按鈕，然後選取從使用者處收到的請求存取檔案（副檔名為 KESDC 的檔案）。
   網頁主控台將顯示有關請求的資訊。這將包括使用者請求存取的檔案所在的電腦名稱。
6. 點擊**"儲存金鑰"**按鈕，然後選取一個資料夾來儲存加密資料存取金鑰檔案（副檔名為 KESDR 的檔案）。

結果，您將能夠獲取加密資料存取金鑰，您需要將該金鑰傳輸給使用者。

收到加密資料存取金鑰檔案後，使用者需要點擊來執行該檔案。結果，Kaspersky Endpoint Security 將授予對磁碟機上儲存的所有加密檔案的存取權限。要存取其他卸除式磁碟機上儲存的加密檔案，您必須為每個卸除式磁碟機獲取單獨的存取金鑰檔案。

# 作業系統故障後還原對加密檔案的存取

只有使用了檔案級加密 (FLE) 時，才能在作業系統故障後還原對資料的存取。如果使用了完整磁碟加密 (FDE)，則無法還原對資料的存取。

*要在作業系統故障後還原對加密資料的存取：*

1. 不格式化硬碟的情況下重新安裝作業系統。
2. 安裝 Kaspersky Endpoint Security。
3. 在電腦與資料被加密時控制電腦的卡巴斯基安全管理中心管理伺服器之間建立連線。

授予加密資料存取權限的條件與作業系統發生故障之前適用的條件相同。

# 編輯加密檔案存取訊息範本

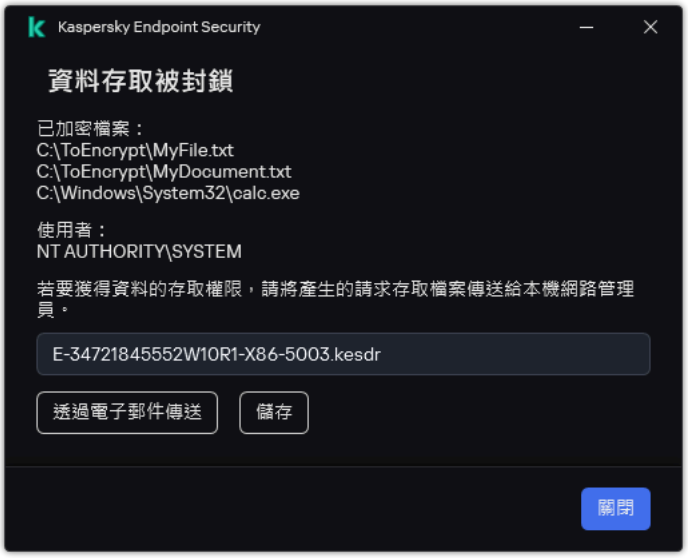
*若要編輯加密檔案存取訊息範本，請執行以下操作：*

1. 在卡巴斯基安全管理中心管理主控台樹狀目錄中，選取**政策**。
2. 選擇必要的政策並點擊以開啟政策內容。
3. 在政策視窗中，選擇**"資料加密 → 一般加密設定"**。
4. 在**"範本"**塊中，點擊**"範本"**按鈕。
5. 在開啟的視窗中，執行以下操作：
   - 如果您希望編輯使用者郵件範本，則選取**"使用者訊息"**標籤。使用者電腦上沒有可用金鑰用於存取加密檔案而存取加密檔案時，以下視窗將開啟（請見下圖）。點擊**透過電子郵件傳送**按鈕將自動建立一條使用者訊息。該郵件會將請求存取加密檔案存取權限的檔案一起傳送給公司區域網路管理員。
   - 如果您希望編輯管理員郵件範本，則選取**"管理員訊息"**標籤。授予對加密檔案的存取權限後，使用者會收到此訊息。
6. 編輯資訊範本。

   若要將變數新增至範本文字，請將游標置於所需位置，點擊**變數**，然後從可用選項清單中選取所需變數。

   此外，您也可使用**根據預設**按鈕，還原預設範本文字。

7. 儲存變更。




還原對加密檔案的存取權限

# 卸除式磁碟機加密

如果 Kaspersky Endpoint Security 安裝在執行 Windows for Workstations 的電腦上，則該元件可用。如果 Kaspersky Endpoint Security 安裝在執行 Windows for Servers 的電腦上，則該元件不可用。

Kaspersky Endpoint Security 支援加密 FAT32 和 NTFS 檔案系統中的檔案。如果將具有不支援的檔案系統的卸除式磁碟機連線到電腦，對該卸除式磁碟機的加密工作將以出錯結束，Kaspersky Endpoint Security 會為該卸除式磁碟機分配唯讀狀態。

要防護卸除式磁碟機上的資料，可以使用以下類型的加密：

- Full Disk Encryption (FDE)。

  加密整個卸除式磁碟機，包括檔案系統。

  無法在公司網路外部存取加密資料。如果電腦未連線到卡巴斯基安全管理中心（例如"訪客"電腦），也無法存取公司網路內部的加密資料。

- File Level Encryption (FLE)。

  僅加密卸除式磁碟機上的檔案。檔案系統保持不變。

  是卸除式磁碟機上的檔案加密使用一種稱為*攜帶模式*的特殊模式，提供存取公司網路外部資料的功能。

在加密期間，Kaspersky Endpoint Security 會建立一個主要金鑰。Kaspersky Endpoint Security 將主要金鑰儲存在以下儲存區中：

- 卡巴斯基安全管理中心。
- 使用者的電腦。

  主要金鑰使用使用者的金鑰加密。
- 卸除式磁碟機。

  主要金鑰使用卡巴斯基安全管理中心的公開金鑰加密。

加密完成後，可在公司網路內存取卸除式磁碟機上的資料，就像資料在未加密的一般卸除式磁碟機一樣。

## 存取加密資料

連線帶有加密資料的卸除式磁碟機後，Kaspersky Endpoint Security 會執行以下操作：

1. 檢查使用者電腦本機儲存的主要金鑰。

   如果找到主要金鑰，使用者將獲得卸除式磁碟機上的資料存取權限。

   如果找不到之要金鑰，Kaspersky Endpoint Security 會執行以下操作：

   a. 向卡巴斯基安全管理中心傳送請求。

      收到請求後，卡巴斯基安全管理中心將傳送一個包含主要金鑰的回應。

   b. Kaspersky Endpoint Security 將主要金鑰儲存在使用者電腦的本機中，以供以後對加密的卸除式磁碟機進行操作。
2. 解密資料。

## 卸除式磁碟機加密的特殊功能

卸除式磁碟機加密具有以下特殊功能：

- 已經為指定的受管理電腦群組形成針對卸除式磁碟機加密且帶有預設設定的政策。因此，套用為加密/解密卸除式磁碟機配置的卡巴斯基安全管理中心政策的結果取決於抽取式磁碟機連線到的電腦。
- Kaspersky Endpoint Security 不會加密/解密卸除式磁碟機上儲存的唯讀檔案。
- 支援以下裝置類型的卸除式磁碟機：
  - 透過 USB 介面連接的資料媒體
  - 透過 USB 和 FireWire 介面連接的固定磁碟機
  - 透過 USB 和 FireWire 介面連接的 SSD 磁碟機

# 啟動卸除式磁碟機加密

您可以使用政策來解密卸除式磁碟機。將為特定管理群組產生具有已定義的卸除式磁碟機加密設定的政策。因此，卸除式磁碟機上的資料解密結果取決於其連接的電腦。

Kaspersky Endpoint Security 支援加密 FAT32 和 NTFS 檔案系統中的檔案。如果將具有不支援的檔案系統的卸除式磁碟機連線到電腦，對該卸除式磁碟機的加密工作將以出錯結束，Kaspersky Endpoint Security 會為該卸除式磁碟機分配唯讀狀態。

在加密卸除式磁碟機上的檔案之前，請確保它已格式化並且沒有隱藏的瓷碟分割（例如 EFI 系統分割）。如果磁碟機包含未格式化或隱藏的分割，檔案加密可能會失敗並出現錯誤。

*若要加密卸除式磁碟機，請執行以下操作：*

1. 在卡巴斯基安全管理中心管理主控台樹狀目錄中，選取**政策**。
2. 選擇必要的政策並點擊以開啟政策內容。
3. 在政策視窗中，選擇"**資料加密 → 卸除式磁碟機加密**"。
4. 在"**加密模式**"下拉清單中，選取您希望 Kaspersky Endpoint Security 對卸除式磁碟機執行的預設操作：
   - **加密整個卸除式磁碟機** (FDE)。Kaspersky Endpoint Security 逐個磁區加密卸除式磁碟機的內容。因此，應用程式不僅會加密卸除式磁碟機中儲存的檔案，還會加密其檔案系統，包括卸除式磁碟機上的檔案名稱和資料夾結構。
   - **加密所有檔案** (FLE)。Kaspersky Endpoint Security 會加密卸除式磁碟機中儲存的所有檔案。應用程式不會加密卸除式磁碟機的檔案系統，包括檔案名稱和資料夾結構。
   - **僅加密新檔案** (FLE)。Kaspersky Endpoint Security 只加密已新增到卸除式磁碟機的檔案或者儲存在卸除式磁碟機中並且在上次套用卡巴斯基安全管理中心政策後已修改的檔案。

   Kaspersky Endpoint Security 不會對已經加密的卸除式磁碟機進行加密。
5. 如果要使用攜帶模式對卸除式磁碟機進行加密，請選中"**攜帶模式**"核取方塊。

   *攜帶模式*是卸除式磁碟機上的檔案加密 (FLE) 模式，它提供了存取公司網路外部資料的功能。攜帶模式還允許您在未安裝 Kaspersky Endpoint Security 的電腦上使用加密資料。
6. 如果要加密新的卸除式磁碟機，建議選中"**僅加密使用的磁碟空間**"核取方塊。如果清除該核取方塊，Kaspersky Endpoint Security 將加密所有檔案，包括已刪除或已修改檔案的殘留片段。
7. 如果要配置對單個卸除式磁碟機的加密，請定義加密規則。
8. 如果要在離線模式下使用卸除式磁碟機的完整磁碟加密，請選擇"**允許在離線模式下加密卸除式磁碟機**"核取方塊。

   *離線加密模式*是指未連線卡巴斯基安全管理中心時加密卸除式磁碟機 (FDE)。在加密過程中，Kaspersky Endpoint Security 只將主金鑰儲存在使用者的電腦上。Kaspersky Endpoint Security 將在下次同步期間將主金鑰傳送到卡巴斯基安全管理中心。

如果儲存主金鑰的電腦損壞，並且資料未傳送到卡巴斯基安全管理中心，則無法存取卸除式磁碟機。

如果清除**"允許在離線模式下加密卸除式磁碟機"**核取方塊，並且未連線到卡巴斯基安全管理中心，則無法進行卸除式磁碟機加密。

9. 儲存變更。

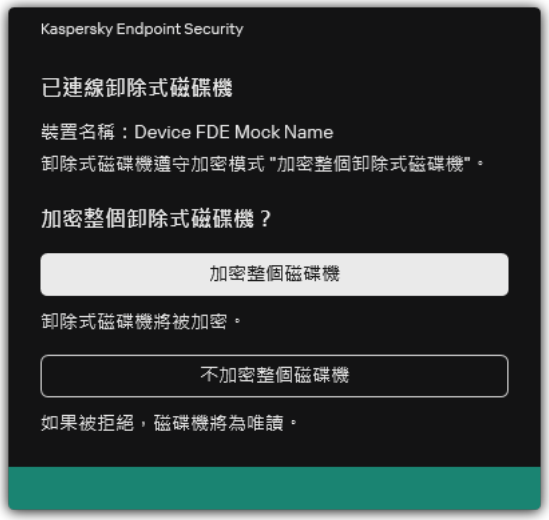
套用政策後，當使用者連線卸除式磁碟機或卸除式磁碟機已連線時，Kaspersky Endpoint Security 會提示使用者確認執行加密操作（請參見下圖）。

應用程式允許您執行以下操作：

- 如果使用者確認加密請求，Kaspersky Endpoint Security 將加密資料。
- 如果使用者拒絕加密請求，Kaspersky Endpoint Security 將保留資料不變，並為該卸除式磁碟機分配唯讀存取權限。
- 如果使用者未回應加密請求，Kaspersky Endpoint Security 將保留資料不變，並為該卸除式磁碟機分配唯讀存取權限。隨後套用政策或下次連線該卸除式磁碟機時，應用程式將再次提示確認。

如果在資料加密期間，使用者安全刪除卸除式磁碟機，Kaspersky Endpoint Security 將會在加密過程完成前中斷資料加密過程，允許刪除卸除式磁碟機。下次將卸除式磁碟機連線到此電腦時，將繼續資料加密。

如果對卸除式磁碟機的加密失敗，請在 Kaspersky Endpoint Security 介面中檢視**"資料加密"**報告。對檔案的存取可能被其他應用程式拒絕。在這種情況下，請嘗試從電腦上拔下卸除式磁碟機，然後重新連接。




卸除式磁碟機加密請求

# 新增卸除式磁碟機加密規則

*若要為卸除式磁碟機新增加密規則，請執行以下操作：*

1. 在卡巴斯基安全管理中心管理主控台樹狀目錄中，選取**政策**。
2. 選擇必要的政策並點擊以開啟政策內容。

3. 在政策視窗中，選擇**"資料加密 → 卸除式磁碟機加密"**。

4. 點擊**"新增"**按鈕並在下拉清單中選取以下項目之一：

   - 如果您希望為裝置控制元件的受信任裝置清單中的卸除式磁碟新增加密規則，則選取**"從此政策的受信任裝置清單"**。
   - 如果您希望為卡巴斯基安全管理中心清單中卸除式磁碟新增加密規則，則選取**"從卡巴斯基安全管理中心的裝置清單"**。

5. 在**"選定裝置的加密模式"**下拉清單中，選取 Kaspersky Endpoint Security 對選定卸除式磁碟機上檔案執行的操作。

6. 如果您希望 Kaspersky Endpoint Security 在加密前準備卸除式磁碟機，請選取**"攜帶模式"**核取方塊，這將能夠在攜帶模式中使用上面儲存的加密檔案。

   攜帶模式可以在存有加密檔案的卸除式磁碟機連線至沒有加密功能的電腦時能夠存取卸除式磁碟機中的加密檔案。

7. 如果您希望 Kaspersky Endpoint Security 只加密包含有檔案的磁碟磁區，則選取**"僅加密使用的磁碟空間"**核取方塊。

   如果您在已使用的磁碟上應用加密，建議加密整個磁碟。這將確保所有資料受到防護 – 即使刪除了可能仍包含擷取資訊的資料。建議為先前未使用的新磁碟使用**"僅加密使用的磁碟空間"**功能。

   如果先前使用**"僅加密使用的磁碟空間"**功能加密了裝置，則在**"加密整個卸除式磁碟機"**模式中套用政策，未包含檔案的磁區將不會被加密。

8. 在**"之前為裝置選擇的動作"**下拉清單中，選取根據先前為卸除式磁碟機所建立加密檔案存取規則 Kaspersky Endpoint Security 所執行的操作：

   - 如果您希望先前為卸除式磁碟建立的加密規則不變，則選取**"略過"**。
   - 如果您希望先前為卸除式磁碟機建立的加密規則由新規則代替，則選取**"重新整理"**。

9. 儲存變更。

新增的卸除式磁碟機加密規則將套用於連線到組織中任何電腦的卸除式磁碟機。

# 匯出和匯入卸除式磁碟機的加密規則清單

您可以將卸除式磁碟機加密規則清單匯出到 XML 檔案。然後，您可以修改檔案，例如，為相同類型的卸除式磁碟機新增大量規則。您還可以使用匯出/匯入功能來備份規則清單，或將規則則遷移到其他伺服器。

**如何在管理主控台 (MMC) 中匯出和匯入卸除式磁碟機加密規則清單**

1. 在網頁主控台的主視窗中，選擇**資產（裝置）→ 政策和設定檔**。

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**"資料加密"→"卸除式磁碟機加密"**。

5. 在"**選定裝置的加密規則**"塊中，點擊"**<N> 條規則**"連接。

   這將開啟卸除式磁碟機的加密規則清單。

6. 要匯出卸除式磁碟機的加密規則清單：

   a. 選取您想要匯出的規則。

   b. 點擊"**匯出**"。

   c. 確認您只想匯出選定的規則，還是匯出整個清單。

   d. 儲存檔案。

      Kaspersky Endpoint Security 會將規則清單匯出到預設下載資料夾中的 XML 檔案。

7. 要匯入規則清單：

   a. 點擊"**匯入**"連接。

      在開啟的視窗中，選取要從中匯入規則清單的 XML 檔案。

   b. 開啟檔案。

      如果電腦已經具有規則清單，則 Kaspersky Endpoint Security 將提示您刪除現有清單或從 XML 檔案向其中新增新項目。

8. 儲存變更。

1. 在卡巴斯基安全管理中心管理主控台樹狀目錄中，選取**政策**。

2. 選擇必要的政策並點擊以開啟政策內容。

3. 在政策視窗中，選擇"**資料加密 → 卸除式磁碟機加密**"。

4. 要匯出卸除式磁碟機的加密規則清單：

   a. 選取您想要匯出的規則。要選擇多個連接埠，請使用**CTRL**或**SHIFT**鍵。

      如果您未選擇任何規則，則 Kaspersky Endpoint Security 將匯出所有規則。

   b. 點擊"**匯出**"連接。

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

   d. 儲存檔案。

      Kaspersky Endpoint Security 會將規則清單匯出到 XML 檔案。

5. 要匯入卸除式磁碟機的加密規則清單：

   a. 點擊"**匯入**"連接。

      在開啟的視窗中，選取要從中匯入規則清單的 XML 檔案。

   b. 開啟檔案。

      如果電腦已經具有規則清單，則 Kaspersky Endpoint Security 將提示您刪除現有清單或從 XML 檔案向其中新增新項目。

6. 儲存變更。

# 用於存取卸除式磁碟機上加密檔案的攜帶模式

*攜帶模式*是卸除式磁碟機上的檔案加密 (FLE) 模式，它提供了存取公司網路外部資料的功能。攜帶模式還允許您在未安裝 Kaspersky Endpoint Security 的電腦上使用加密資料。

攜帶模式在以下情況下便於使用：

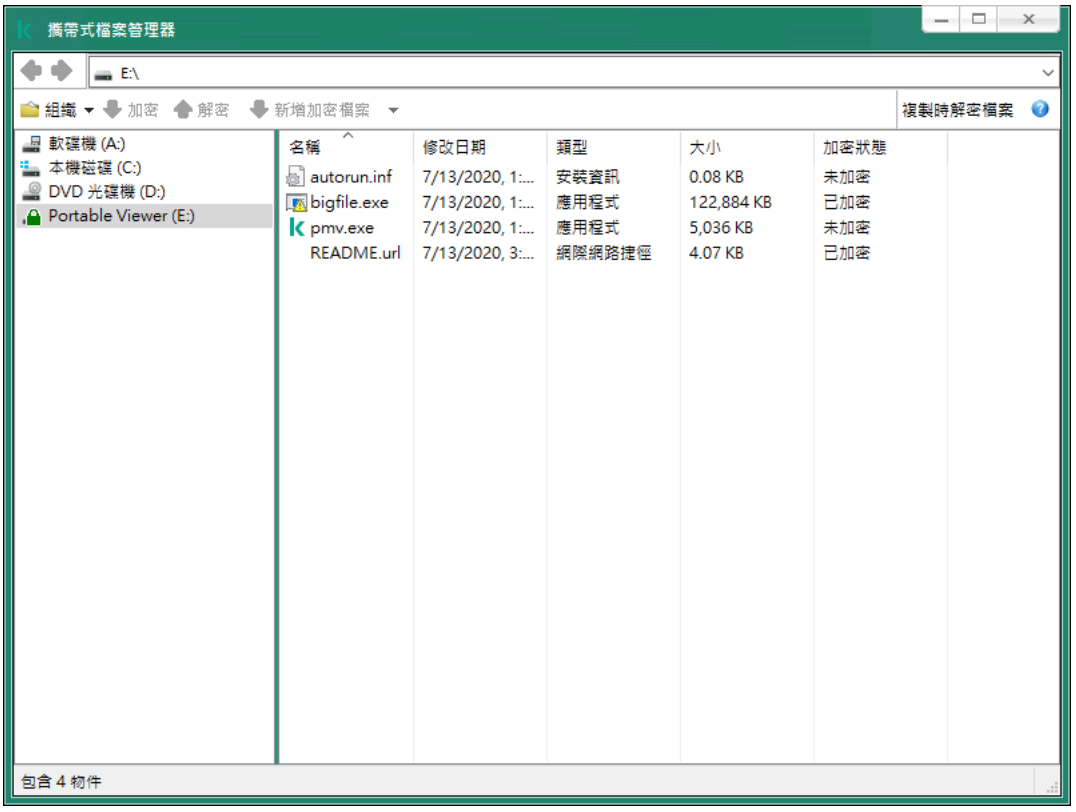
- 電腦和卡巴斯基安全管理中心管理伺服器之間沒有連線。
- 基礎結構已隨著卡巴斯基安全管理中心管理伺服器的變更而發生變化。
- 電腦上未安裝 Kaspersky Endpoint Security。

## 攜帶式檔案管理器

為了在攜帶模式下工作，Kaspersky Endpoint Security 會在卸除式磁碟機上安裝一個名為"*攜帶式檔案管理員*"的特殊加密模組。如果電腦上未安裝 Kaspersky Endpoint Security，攜帶式檔案管理員提供了一個處理加密資料的介面（請參見下圖）。如果電腦上安裝了 Kaspersky Endpoint Security，則可以使用一般的檔案管理員（例如資源管理器）使用加密的卸除式磁碟機。

攜帶式檔案管理員會儲存用於加密卸除式磁碟機上的檔案金鑰。該金鑰使用使用者密碼加密。使用者可在加密卸除式磁碟機的檔案之前先設定密碼。

當卸除式磁碟機連線到未安裝 Kaspersky Endpoint Security 的電腦時，會自動啟動攜帶式檔案管理員。如果電腦上已停用自動啟動應用程式，請手動啟動攜帶式檔案管理員。要執行此操作，請執行卸除式磁碟機上儲存名為 pmv.exe 的檔案。




攜帶式檔案管理器

支援攜帶模式以處理加密檔案

**如何在管理主控台 (MMC) 中啟用攜帶模式支援，以處理卸除式磁碟機上的加密檔案**

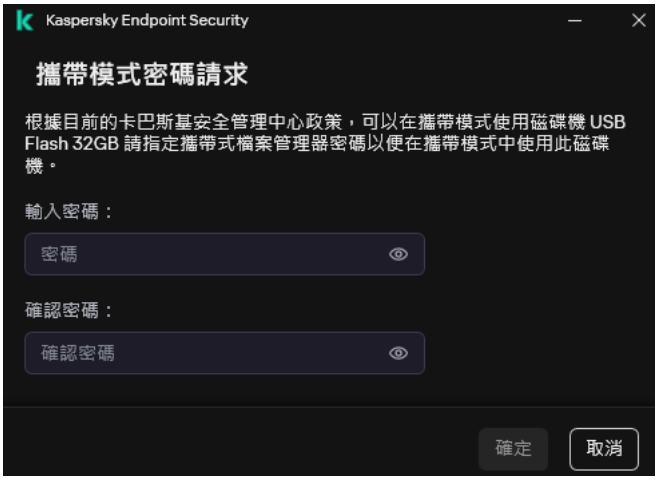
1. 在卡巴斯基安全管理中心管理主控台樹狀目錄中，選取**政策**。
2. 選擇必要的政策並點擊以開啟政策內容。
3. 在政策視窗中，選擇**"資料加密 → 卸除式磁碟機加密"**。
4. 在**"選定裝置的加密模式"**下拉式清單中，選擇**"加密所有檔案"**或者**"僅加密新檔案"**。

   攜帶模式僅適用於檔案級加密 (FLE)。無法為完整磁碟加密 (FDE) 啟用攜帶模式支援。

5. 選擇**"攜帶模式"**核取方塊。
6. 如有必要，可為單一卸除式磁碟機新增加密規則。
7. 儲存變更。

8. 應用政策後，將卸除式磁碟機連接到電腦。

9. 確認卸除式磁碟機加密操作。
   這會開啟一個視窗，您可以在其中為攜帶式檔案管理員建立密碼。




攜帶模式密碼請求

10. 指定滿足強度要求的密碼並確認。

11. 儲存變更。

**如何在網頁主控台中啟用攜帶模式支援，以處理卸除式磁碟機上的加密檔案**

1. 在網頁主控台的主視窗中，選擇**資產（裝置）→政策和設定檔**。

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"**資料加密**"→"**卸除式磁碟機加密**"。

5. 在**預設操作**塊中，選擇**加密所有檔案** or **僅加密新檔案**。

   > 攜帶模式僅適用於檔案級加密 (FLE)。無法為完整磁碟加密 (FDE) 啟用攜帶模式支援。

6. 選擇"**攜帶模式**"核取方塊。

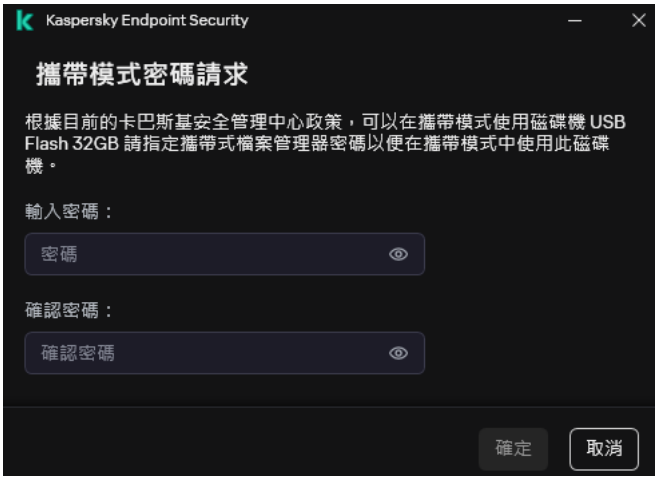
7. 如有必要，可為單一卸除式磁碟機新增加密規則。

8. 儲存變更。

9. 應用政策後，將卸除式磁碟機連接到電腦。

10. 確認卸除式磁碟機加密操作。

這會開啟一個視窗，您可以在其中為攜帶式檔案管理員建立密碼。




攜帶模式密碼請求

11. 指定滿足強度要求的密碼並確認。

12. 儲存變更。

Kaspersky Endpoint Security 會加密卸除式磁碟機上的檔案。用來操作加密檔案的攜帶式檔案管理員也將被新增至卸除式磁碟機。如果卸除式磁碟機上已經有加密檔案，Kaspersky Endpoint Security 將使用自己的金鑰再次對其進行加密。這允許使用者在攜帶模式下存取卸除式磁碟機上的所有檔案。

## 存取卸除式磁碟機上的加密檔案

在攜帶模式支援下，加密卸除式磁碟機上的檔案後，可以使用以下檔案存取方法：

- 如果電腦上未安裝 Kaspersky Endpoint Security，則攜帶式檔案管理員將提示您輸入密碼。每次重新啟動電腦或重新連線卸除式磁碟機時，都需要輸入密碼。
- 如果電腦位於公司網路外部，並且電腦上已安裝 Kaspersky Endpoint Security，則應用程式將提示您輸入密碼或向管理員傳送存取檔案的請求。獲得對卸除式磁碟機上檔案的存取權限後，Kaspersky Endpoint Security 會將金鑰儲存在電腦的金鑰儲存區中。如此一來，將來便無需輸入密碼或詢問管理員即可存取檔案（請見下圖）。
- 如果電腦位於公司網路內部，並且電腦上已安裝 Kaspersky Endpoint Security，則無需輸入密碼即可存取裝置。Kaspersky Endpoint Security 將從與電腦連線的卡巴斯基安全管理中心管理伺服器接收金鑰。




存取卸除式磁碟機上的加密檔案

還原在攜帶模式下工作的密碼

如果您忘記了在攜帶模式下工作的密碼，則需要將卸除式磁碟機與公司網路內安裝了 Kaspersky Endpoint Security 的電腦連線。您將獲得檔案存取權限，因為金鑰儲存在電腦的金鑰儲存區或管理伺服器中。使用新密碼解密和重新加密檔案。

將卸除式磁碟機連線到其他網路中的電腦時，攜帶模式的功能

如果電腦位於公司網路外部，並且電腦上已安裝 Kaspersky Endpoint Security，您可以透過以下方式存取檔案：

- **依據密碼進行存取**

  輸入密碼後，您將能夠檢視、修改並將檔案儲存在卸除式磁碟機上（*透明存取*）。如果在卸除式磁碟機的加密政策設定中配置了以下參數，Kaspersky Endpoint Security 可以為卸除式磁碟機設定為唯讀存取權限：

  - 攜帶模式支援已停用。
  - 選取了 "**加密所有檔案**" 或 "**僅加密新檔案**" 模式。

  在所有其他情況下，您將獲得對卸除式磁碟機的完全存取權限（讀/寫權限）。您將能夠新增和刪除檔案。

  即使卸除式磁碟機連線到電腦時，您也可以變更卸除式磁碟機的存取權限。如果變更卸除式磁碟機存取權限，Kaspersky Endpoint Security 將封鎖對檔案的存取，並再次提示您輸入密碼。

  輸入密碼後，您無法對卸除式磁碟機套用加密政策設定。在這種情況下，無法對卸除式磁碟機上的檔案進行解密或重新加密。

- **請管理員提供檔案存取權限**

  如果您忘了在攜帶模式下工作的密碼，則請管理員提供檔案存取權限。要存取檔案，使用者需要向管理員傳送請求存取檔案（副檔名為 KESDC 的檔案）。例如，使用者可以透過電子郵件傳送請求存取檔案。管理員將傳送加密資料存取檔案（副檔名為 KESDR 的檔案）。

  完成請求-回應密碼還原程序之後，您將獲得對卸除式磁碟機上檔案的透明存取權限，以及對卸除式磁碟機的完全存取權限（讀/寫權限）。

  例如，您可以套用卸除式磁碟機加密政策並解密檔案。在還原密碼後或在更新政策後，Kaspersky Endpoint Security 將提示您確認變更。

  **如何在管理主控台 (MMC) 中取得加密資料存取檔案**

  1. 開啟卡巴斯基安全管理中心管理主控台。
  2. 在主控台樹狀目錄中，選擇"**裝置**"。
  3. 在"**裝置**"標籤上，選取使用者正在請求加密資料存取權限的電腦，然後點擊滑鼠右鍵開啟內容功能表。
  4. 在內容功能表中，選取"**授予離線模式下的存取權限**"。
  5. 在開啟的視窗中選擇"**資料加密**"標籤。
  6. 在"**資料加密**"標籤上點擊"**瀏覽**"按鈕 。
  7. 在用來選取請求存取檔案的視窗中，指定從使用者那裡接收的檔案路徑。

您將看到有關使用者請求的資訊。卡巴斯基安全管理中心會產生一個金鑰檔案。透過電子郵件將產生的加密資料存取金鑰檔案傳送給使用者。或儲存該存取檔案並使用任何可用方法來傳輸該檔案。




授予在離線模式下存取

**如何在網頁主控台中獲取加密資料存取檔案**

1. 在網頁主控台的主視窗中，選擇**資產（裝置）→ 受管理裝置**。
2. 選中要還原其資料存取權限的電腦名稱旁邊的核取方塊。
3. 點擊**"同意存取離線模式下的裝置"**。
4. 選擇**"資料加密"**。
5. 點擊**"選擇檔案"**按鈕，然後選取從使用者處收到的請求存取檔案（副檔名為 KESDC 的檔案）。
   網頁主控台將顯示有關請求的資訊。這將包括使用者請求存取的檔案所在的電腦名稱。
6. 點擊**"儲存金鑰"**按鈕，然後選取一個資料夾來儲存加密資料存取金鑰檔案（副檔名為 KESDR 的檔案）。

結果，您將能夠獲取加密資料存取金鑰，您需要將該金鑰傳輸給使用者。

# 卸除式磁碟機解密

您可以使用政策來解密卸除式磁碟機。將為特定管理群組產生具有已定義的卸除式磁碟機加密設定的政策。因此，卸除式磁碟機上的資料解密結果取決於其連接的電腦。

*若要解密卸除式磁碟機，請執行以下操作：*

1. 在卡巴斯基安全管理中心管理主控台樹狀目錄中，選取**政策**。
2. 選擇必要的政策並點擊以開啟政策內容。
3. 在政策視窗中，選擇**"資料加密 → 卸除式磁碟機加密"**。

4. 如果您希望解密所有儲存在卸除式磁碟機上的加密檔案，請在**"加密模式"**下拉清單中選取**"解密整個卸除式磁碟機"**。

5. 若要解密儲存在個人卸除式磁碟機上的資料，請為您要解密其資料的卸除式磁碟機編輯加密規則。為此，請執行以下操作：

   a. 已配置加密規則的卸除式磁碟機清單中，選擇對應您所需卸除式磁碟機的項目。

   b. 點擊**"設定規則"**按鈕為卸除式磁碟機編輯加密規則。

   c. 在**設定規則**按鈕的內容功能表中，選取在**"解密整個卸除式磁碟機"**項目。

6. 儲存變更。

結果是，如果使用者連線卸除式磁碟機或該磁碟機已經連線，Kaspersky Endpoint Security 將解密該卸除式磁碟機。程式將警告使用者解密過程可能會花費些時間。如果在資料解密期間，使用者安全刪除卸除式磁碟機，Kaspersky Endpoint Security 將會在解密過程完成前中斷資料解密過程，並且允許刪除卸除式磁碟機。下次將卸除式磁碟機連線到此電腦時，將繼續資料解密。

如果對卸除式磁碟機的解密失敗，請在 Kaspersky Endpoint Security 介面中檢視**"資料加密"**報告。對檔案的存取可能被其他應用程式拒絕。在這種情況下，請嘗試從電腦上拔下卸除式磁碟機，然後重新連接。

# 檢視資料加密詳細資訊

當正在執行加密或解密工作時，卡巴斯基安全管理中心會將應用於使用者端電腦的加密參數狀態的相關資訊轉發給卡巴斯基安全管理中心。

## 檢視加密狀態

您可以查看狀態以監控資料加密。Kaspersky Endpoint Security 可分配以下加密狀態：

- **不符合政策；被使用者取消**。使用者已取消資料加密。
- **由於錯誤而無法套用政策**資料加密錯誤，例如缺少產品授權。
- **正在套用政策；需要重新啟動**正在這台電腦上進行資料加密。重新啟動應用程式以完成資料加密。
- **未指定加密政策**資料加密已在政策設定中關閉。
- **不支援**。電腦上未安裝資料加密元件。
- **正在套用政策**正在這台電腦上進行資料加密和/或解密。

*若要檢視電腦資料的加密狀態，請執行以下操作：*

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

3. 在工作區的**"裝置"**標籤中，將捲軸滑向右側。如果**"加密狀態"**列未顯示，請在卡巴斯基安全管理中心主控台設定中新增此列。

   **"加密狀態"**列將顯示選定管理群組中電腦上資料的加密狀態。該狀態是基於電腦本機磁碟機上的檔案加密資訊和完整磁碟加密的資訊形成的。

4. 如果電腦的資料加密狀態為**"正在套用政策"**，您可以監控加密進度面板：

   a. 點擊兩下，開啟包含**"正在套用政策"**狀態的電腦內容。

   b. 在電腦內容視窗中，選取**"應用程式"**區域。

   c. 在電腦上安裝的卡巴斯基應用程式清單中，選擇**"Kaspersky Endpoint Security for Windows"**。

   d. 點擊**"統計"**。

   e. 在**"裝置加密"**下方，您可以以百分比形式查看資料加密的目前進度。

# 在卡巴斯基安全管理中心的資訊顯示器上檢視加密統計資訊

*要在卡巴斯基安全管理中心的資訊顯示器上檢視加密狀態：*

1. 開啟卡巴斯基安全管理中心管理主控台。
2. 在主控台樹狀目錄中，選擇**管理伺服器**節點。
3. 在管理主控台樹狀目錄的右側工作區中選取**"統計"**標籤。
4. 使用包含資料加密統計資訊的詳細視窗建立新頁面。為此，請執行以下操作：

   a. 在**"統計"**標籤上點擊**"自訂檢視"**按鈕 。

   b. 在開啟的視窗中，點擊**"新增"**按鈕。

   c. 這將開啟一個視窗；在該視窗的**"一般"**區域中輸入頁面名稱。

   d. 在**"資訊視窗"**區域中點擊**"新增"**按鈕。

   e. 在開啟視窗的**"防護狀態"**群組中，選擇**"裝置加密"**項目。

   f. 點擊**"確定"**。

   g. 必要時編輯詳細資訊窗格的設定。為此，請使用**"檢視"**和**"裝置"**區域。

   h. 點擊**"確定"**。

   i. 重複說明中的步驟 d – h，在**"防護狀態"**區域中選擇**"卸除式磁碟機加密"**項目。

   新增的詳細資訊窗格將出現在**"資訊視窗"**清單中。

j. 點擊**"確定"**。

在前面的步驟中建立的帶有詳細資訊窗格的頁面名稱將顯示在**"頁面"**清單中。

k. 點擊**"關閉"**按鈕。

5. 在**"統計"**標籤上，開啟在該說明的先前步驟中建立的頁面。

詳情頁面將出現，其中顯示了電腦和卸除式磁碟機的加密狀態。

# 檢視本機電腦磁碟機上檔案加密錯誤

*若要檢視本機電腦磁碟上檔案加密錯誤：*

1. 開啟卡巴斯基安全管理中心管理主控台。
2. 在主控台樹狀目錄中，選擇**"受管理裝置"**。
3. 在**"裝置"**頁簽上，選取清單中電腦的名稱，點擊右鍵開啟內容功能表。
4. 在電腦的內容功能表中選取**"內容"**項。在開啟的視窗中，選擇**"防護"**區域。
5. 點擊"**檢視資料加密錯誤**"連接開啟**"資料加密錯誤"**視窗。

該視窗將顯示本機電腦磁碟機上資料加密錯誤的詳情。錯誤被修正後，卡巴斯基安全管理中心會將該錯誤詳情從**"資料加密錯誤"**視窗中刪除。

# 檢視資料加密報告

卡巴斯基安全管理中心可讓您建立資料加密報告：

- **受管理裝置加密狀態報告**該報告包括有關電腦的加密狀態是否符合加密政策的資訊。
- **大容量儲存裝置加密狀態報告**該報告包括有關外部裝置和儲存裝置加密狀態的資訊。
- **加密磁碟機存取權限報告**該報告包括有關有權存取加密磁碟機的帳戶狀態的資訊。
- **檔案加密錯誤報告**該報告包含有關在電腦上執行資料加密或解密工作期間發生的錯誤的資訊。
- **封鎖存取加密檔案的報告**該報告包括有關被封鎖存取加密檔案的應用程式的資訊。

*若要檢視資料加密報告，請執行以下操作：*

1. 開啟卡巴斯基安全管理中心管理主控台。
2. 在管理主控台樹狀目錄的**管理伺服器**節點中選取**"報告"**標籤。
3. 點擊**"新增報告範本"**按鈕。

"新報告範本精靈"將啟動。

4. 按照"報告範本精靈"的說明進行操作。在**選取報告範本類型** 視窗中的 **其他** 部分，選擇一份資料加密報告。

完成新報告範本精靈之後，新報告範本將出現在**"報告"**標籤上。

5. 選取在說明的上個步驟中建立的報告範本。

6. 在範本的內容功能表中選取**"顯示報告"**。

報告建立過程將開始。此報告將顯示在新視窗中。

# 無法存取加密裝置時的裝置使用

## 獲取存取加密裝置的權限

在以下情況下使用者可能被要求請求存取加密裝置：

- 硬碟磁碟機在其他電腦上進行的加密。
- 裝置的加密金鑰不在電腦上（例如，首次嘗試存取電腦上的加密卸除式磁碟機時），電腦未連線到卡巴斯基安全管理中心。

  使用者套用存取金鑰到加密裝置後，Kaspersky Endpoint Security 將把加密金鑰儲存在使用者的電腦上，允許在隨後的存取嘗試時存取此裝置（即使未連線到卡巴斯基安全管理中心）。

可用以下方式獲得加密裝置的存取權限：

1. 使用者使用 Kaspersky Endpoint Security 應用程式介面建立帶有 kesdc 副檔名的請求存取檔案並將其傳送給公司區域網路管理員。
2. 管理員使用卡巴斯基安全管理中心管理主控台建立帶有 kesdc 副檔名的存取金鑰檔案並將其傳送給使用者。
3. 使用者套用存取金鑰。

## 還原加密裝置上的資料

使用者可用使用加密裝置還原實用程式（以下簡稱"還原實用程式"）使用加密裝置。在下列情況中可能要求這樣做：

- 使用存取金鑰獲取存取權限的過程不成功。
- 帶有加密裝置的電腦上尚未安裝加密元件。

需要使用"還原實用工具"還原對加密裝置存取的資料有一段時間以未加密形式在使用者電腦的記憶體裡。要降低有人未經授權存取此類別資料的風險，建議您在受信任的電腦上還原存取加密裝置。

可用以下方式還原加密裝置上的資料：

1. 使用者使用"還原實用工具"建立帶有 fdertc 副檔名的請求存取檔案並將其傳送給公司區域網路管理員。
2. 管理員使用卡巴斯基安全管理中心管理主控台建立帶有 fdertr 副檔名的存取金鑰檔案並將其傳送給使用者。
3. 使用者套用存取金鑰。

若要還原加密系統硬碟磁碟機上的資料，使用者也可以在"還原實用工具"中指定身分驗證代理帳戶憑證。如果身分驗證代理帳戶的元資料已損壞，使用者必須使用請求存取檔案完成還原程序。

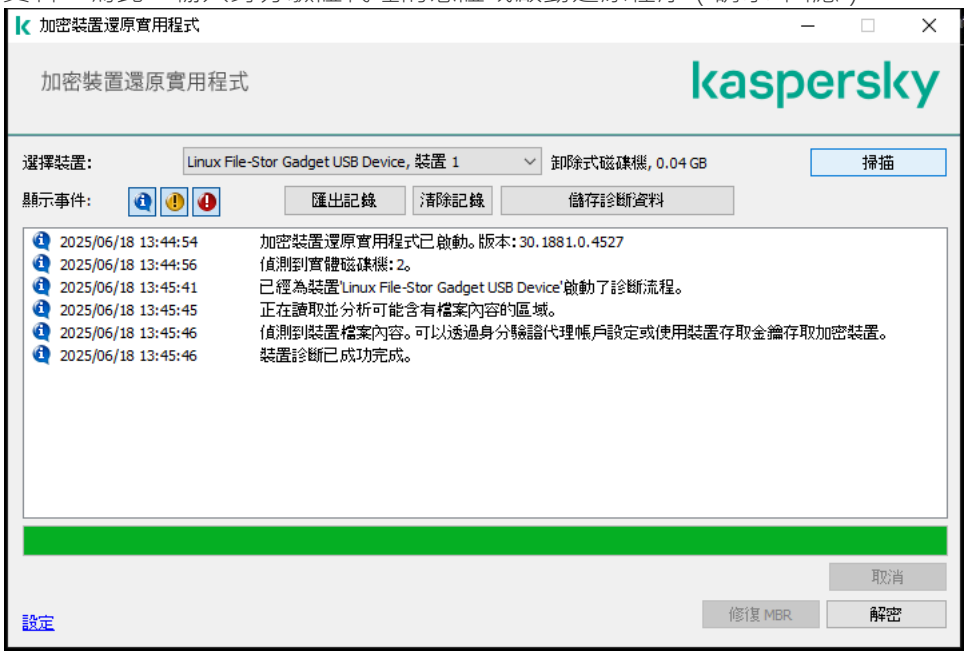
在還原加密裝置上的資料前，建議在將執行過程的電腦上取消卡巴斯基安全管理中心政策或停用卡巴斯基安全管理中心政策設定中的加密。這可以防止重新加密裝置。

# 使用 FDERT 還原實用程式還原資料

如果硬碟發生故障，檔案系統可能已損壞。如果是這種情況，由卡巴斯基磁碟加密技術防護的資料將不可使用。您可以解密資料並將資料複製到新的磁碟機。

對由卡巴斯基磁碟加密技術防護的磁碟機的資料還原包括以下步驟：

1. 建立一個獨立還原實用程式（請參見下圖）。
2. 將磁碟機連線到未安裝 Kaspersky Endpoint Security 加密元件的電腦。
3. 執行還原實用程式並診斷硬碟。
4. 存取磁碟機上的資料。為此，輸入身分驗證代理的憑證或啟動還原程序（請求-回應）。




FDERT 還原實用程式

## 建立獨立還原實用程式

*若要建立還原工具的可執行檔，請執行以下操作：*

1. 開啟應用程式主視窗並點擊 按鈕。
2. 在開啟的視窗中，點擊**"還原已加密裝置"**按鈕。

   加密裝置還原實用程式啟動。
3. 在還原實用程式視窗中，點擊**"建立獨立還原實用程式"**按鈕。
4. 將獨立還原實用程式儲存到電腦記憶體中。

結果，該還原實用程式的可執行檔 (fdert.exe) 將儲存在指定的資料夾中。將該還原實用程式複製到未安裝 Kaspersky Endpoint Security 加密元件的電腦。這可以防止重新加密磁碟。

需要使用"還原實用工具"還原對加密裝置存取的資料有一段時間以未加密形式在使用者電腦的記憶體裡。要降低有人未經授權存取此類別資料的風險，建議您在受信任的電腦上還原存取加密裝置。

## 還原硬碟上的資料

*若要使用還原工具還原對加密裝置的存取權限。*

1. 執行名為 fdert.exe 的檔案，該檔案是還原實用程式的可執行檔。此檔案由 Kaspersky Endpoint Security 建立。
2. 在"還原公用程式"視窗中，選擇您想要還原其存取權限的已加密裝置。
3. 點擊**"掃描"**按鈕允許此實用工具定義應在裝置上執行何種操作：是否應解鎖或者解密。

   如果電腦可以存取 Kaspersky Endpoint Security 加密功能，"還原實用工具"將提示您解鎖裝置。解鎖裝置並不進行解密，解鎖的裝置將可以直接存取。如果電腦不可以存取 Kaspersky Endpoint Security 加密功能，"還原實用工具"將提示您解密裝置。
4. 如果要匯入診斷資訊，請點擊**"儲存診斷資料"**按鈕。

   該實用程式將儲存一個壓縮檔案，其中的檔案包含診斷資訊。
5. 如果加密系統硬碟磁碟機的診斷提示裝置主引導記錄 (MBR) 出現問題，請點擊**"修復 MBR"**按鈕。

   修復裝置的主引導記錄可以使獲取解鎖或解密裝置時所需資訊的過程加快。
6. 根據診斷結果點擊**解鎖**或**解密**按鈕。
7. 如果您想要使用身分驗證代理戶還原資料，請選取**"使用身分驗證代理帳戶設定"**選項，然後輸入身分驗證代理的憑證。

   這種方法僅當還原系統硬碟磁碟機上的資料時可用。如果系統硬碟磁碟機損壞且身分驗證代理帳戶資料已遺失，您必須從公司區域網路管理員獲得存取金鑰才能還原加密裝置上的資料。

8. 如果要啟動還原程序，請執行以下操作：

   a. 請選擇**手動指定裝置存取金鑰**選項。

   b. 點擊**"接收存取金鑰"**按鈕，然後將請求存取檔案（副檔名為 FDERTC 的檔案）儲存到電腦記憶體中。

   c. 將此請求存取檔案傳送給公司區域網路管理員。

   > 在接收到存取金鑰前不要關閉**接收裝置存取金鑰**視窗。當此視窗再次開啟時，您將無法套用之前由管理員建立的存取金鑰。

   d. 接收並儲存由公司區域網路管理員建立並傳送給您的存取檔案（副檔名為 FDERTR 的檔案）（請參見以下說明）。

   e. 在**"接收裝置存取金鑰"**視窗中下載存取檔案。

9. 如果要解密裝置，則必須設定其他解密設定：

   - 指定解密區域：
     - 如果您想要解密整個裝置，請選擇**解密整個裝置**選項。
     - 如果您想要解密裝置上的部分資料，請選取**解密裝置中單一區域**選項，然後指定解密區域邊界。
   - 選擇寫入解密資料的位置：
     - 如果您想要用解密資料複寫原始裝置上的資料，請清除**"解密至磁碟映像檔案"**核取方塊。
     - 如果您想要將解密資料與原始加密資料分開儲存，請選中**"解密至磁碟映像檔案"**核取方塊，然後使用**"瀏覽"**按鈕指定儲存 VHD 檔案的路徑。

10. 點擊**"確定"**。

裝置解鎖/解密過程將啟動。

### 如何在管理主控台 (MMC) 中建立加密資料存取檔案

1. 開啟卡巴斯基安全管理中心管理主控台。
2. 在管理主控台樹狀目錄中，選擇**進階 → 資料加密與防護 → 加密磁碟機**資料夾。
3. 在工作區中選取您想要為其建立存取金鑰檔案的加密裝置，然後在裝置的內容功能表中，點擊**"在 Kaspersky Endpoint Security 中獲取裝置的存取權限"**。

   > 如果您不確定存取請求檔案是為哪台電腦產生的，請在管理主控台樹狀目錄中選擇**進階 → 資料加密與防護**資料夾，並在工作區中點擊**在 Kaspersky Endpoint Security 中獲取裝置加密金鑰**。

4. 在開啟的視窗中，選取要使用的加密 演算法：AES256 或 AES56。

   資料加密演算法取決於分發套件中包含的 AES 加密庫：*強加密* 或 *簡單加密*。AES 加密庫與應用程式一起安裝。

5. 點擊**"瀏覽"**開啟視窗；在此視窗中，指定具有從使用者收到的 fdertc 副檔名的請求檔案路徑。

6. 點擊**"解鎖"**。

您將看到有關使用者請求的資訊。卡巴斯基安全管理中心會產生一個金鑰檔案。透過電子郵件將產生的加密資料存取金鑰檔案傳送給使用者。或儲存該存取檔案並使用任何可用方法來傳輸該檔案。

**如何在網頁主控台中建立加密資料存取檔案**

1. 在網頁主控台的主視窗中，選擇**操作 → 資料加密與防護 → 加密磁碟機**。

2. 選中要還原其資料的電腦名稱旁邊的核取方塊。

3. 點擊**"同意存取離線模式下的裝置"**。

   這將啟動用於授予裝置存取權限的精靈。

4. 按照精靈的說明授予對裝置的存取權限：

   a. 選擇 Kaspersky Endpoint Security for Windows 外掛程式。

   b. 選取使用中的加密演算法：AES256 或 AES56。

      資料加密演算法取決於分發套件中包含的 AES 加密庫：*強加密* 或 *簡單加密*。AES 加密庫與應用程式一起安裝。

   c. 選取從使用者處收到的請求存取檔案（副檔名為 FDERTC 的檔案）。

   d. 選取一個資料夾來儲存加密資料存取金鑰檔案（副檔名為 FDERTR 的檔案）。

結果，您將能夠獲取加密資料存取金鑰，您需要將該金鑰傳輸給使用者。

# 建立作業系統緊急修復光碟

當加密硬碟由於某種原因而無法存取，因而作業系統無法載入時，作業系統救援光碟可能就會很有用。

您可以使用救援光碟載入 Windows 作業系統的映像，並且使用作業系統映像中包括的還原工具還原對加密硬碟的存取。

*若要建立作業系統救援光碟：*

1. 建立加密裝置還原實用程式的可執行檔。

2. 建立 Windows 預啟動環境的自訂映像。在建立 Windows 預啟動環境的自訂映像的同時，將還原實用工具的可執行檔新增至映像。

3. 將 Windows 預安裝環境的自訂映像儲存至開機磁碟機，如 CD 或卸除式磁碟機。

   有關建立 Windows 預啟動環境的自訂映像的說明，請參閱 Microsoft 說明檔案（例如，Microsoft TechNet 資源）。

# Detection and Response 解決方案

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，允許管理 Threat Response 操作。

因此，Detection and Response 解決方案執行以下操作：

- 接收有關電腦、伺服器或其他裝置（遙測）操作的資訊。
- 自動分析資訊以偵測威脅。
- 產生警示詳細資訊作為威脅發展鏈的列，以供分析和選擇 Threat Response 動作。
- 執行 Threat Response 動作（例如，電腦的網路隔離）。

Kaspersky Endpoint Security 使用內建代理支援 Detection and Response 解決方案。內建代理將遙測資料傳送到解決方案的伺服器並執行 Threat Response 動作。內建代理支援：

- Kaspersky Managed Detection and Response (MDR)
- Kaspersky Endpoint Detection and Response Optimum 2.0 (EDR Optimum)
- Kaspersky Endpoint Detection and Response Expert (EDR Expert)
- Kaspersky Anti Targeted Attack Platform：
  - Endpoint Detection and Response (EDR) 7.1 或更早版本
  - Network Detection and Response (NDR)
  - KATA Sandbox
- Endpoint Detection and Response Expert (on-premise)
- Kaspersky Sandbox 2.0。

您可以在各種設定中使用 Kaspersky Endpoint Security 與 Detection and Response 解決方案，例如：[EDR Optimum+MDR]。

# MDR 和 EDR Optimum 許可

Kaspersky Endpoint Security 支援 Kaspersky Managed Detection and Response (MDR) 和 Kaspersky Endpoint Detection and Response Optimum (EDR Optimum) 解決方案。您可以在各種配置中將 Kaspersky Endpoint Security 與這些解決方案結合使用，並建立符合您特定要求的自訂防護系統。為此，您必須為每個解決方案購買產品授權。該產品授權可能涵蓋使用單一解決方案（例如，僅 MDR Add-on）或多個解決方案 [EDR Optimum+MDR] Add-on 的權利。

MDR 和 EDR Optimum 支援以下授權方法：

- MDR 或 EDR Optimum 功能包括在 Kaspersky Endpoint Security for Windows 產品授權中。

  這些功能將在啟動 Kaspersky Endpoint Security for Windows 後立即可用。您只需要新增一個金鑰。

- MDR 或 EDR Optimum 的單獨產品授權（MDR Add-on、EDR Optimum Add-on、[EDR Optimum+MDR] Add-on）。

  為 MDR Add-on、EDR Optimum Add-on 或 [EDR Optimum+MDR] Add-on 新增單獨的金鑰後，功能可用。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 MDR 或 EDR Optimum。Kaspersky Endpoint Security 金鑰必須第一個新增。

Kaspersky Endpoint Security 只允許新增一個*活動金鑰*用於 MDR 和 EDR 許可。因此，如果您需要啟動這兩種解決方案，則必須新增一個 [EDR Optimum+MDR] Add-on 金鑰，而不是為每個解決方案新增單獨的金鑰。您還可以新增一個*備用金鑰*。

如果您在部署 MDR 時使用了 BLOB 檔案，則不需要單獨的金鑰來啟動 MDR。BLOB 檔案已包含產品授權資訊。

## 解決方案的初始許可

首次部署 MDR 和 EDR Optimum 時，解決方案的啟動方式與 Kaspersky Endpoint Security 應用程式相同。您可以使用 *新增金鑰* 工作或使用自動金鑰分發功能新增金鑰。如果選取相關的核取方塊，產品授權金鑰將被作為第二個活動金鑰或備用金鑰新增至應用程式。

## 從一個產品授權切換到另一個產品授權

如果您的組織已部署這些解決方案之一，並且相應的金鑰已被新增至應用程式中，則新配置的授權涉及一些特殊注意事項。當切換到不同的產品授權時，應用程式不會將新金鑰新增至應用程式中，而是用新金鑰取代目前金鑰。原因是有限制應用程式只能新增一個金鑰來啟動 MDR 和 EDR Optimum。

例如，假設您的組織部署了 [EDR Optimum+MDR] 解決方案，並且您決定切換到 MDR Add-on 配置。若要切換至新配置，您必須將 [EDR Optimum+MDR] Add-on 金鑰替換為 MDR Add-on 金鑰。

EDR Optimum 和 MDR（[EDR Optimum+MDR] Add-on）的單獨產品授權不再可用。如果要使用這兩種解決方案，則必須使用 BLOB 檔案啟動 MDR，使用產品授權金鑰來啟動 EDR Optimum。

透過金鑰自動分發功能，應用程式會拒絕涵蓋相同數量解決方案的產品授權金鑰。也就是說，如果您新增了 EDR Optimum Add-on 金鑰，則無法用 MDR Add-on 金鑰替換該金鑰。但是，您可以將 EDR Optimum Add-on 金鑰替換為 [EDR Optimum+MDR] Add-on 金鑰。如果您嘗試用 EDR Add-on 金鑰替換 MDR Add-on 金鑰，應用程式也會拒絕金鑰。若要替換金鑰，您可以執行 *新增金鑰* 工作。*新增金鑰* 工作允許替換任意數量的解決方案的產品授權金鑰。

如果您新增了 [EDR Optimum+MDR] Add-on 備用金鑰，若要正確新增 EDR Optimum Add-on 或 MDR Add-on 的活動金鑰，您必須先將備用金鑰替換為 EDR Optimum Add-on 或 MDR Add -on 金鑰，或刪除備用金鑰，然後替換活動金鑰。

# Kaspersky Endpoint Agent

*Kaspersky Endpoint Agent* 支援在應用程式與其他卡巴斯基解決方案（例如，Kaspersky Sandbox）之間進行互動以偵測進階威脅。卡巴斯基解決方案與特定版本的 Kaspersky Endpoint Agent 相容。

若要將 Kaspersky Endpoint Agent 作為 Kaspersky 解決方案的一部分使用，您必須用相應的產品授權金鑰啟動那些解決方案。

有關您所使用的軟體解決方案中包含的 Kaspersky Endpoint Agent 的完整資訊，以及有關獨立解決方案的完整資訊，請參閱相關產品的說明指南：

- Kaspersky Anti Targeted Attack Platform 說明
- Kaspersky Sandbox 說明
- Kaspersky Endpoint Detection and Response Optimum 說明
- Kaspersky Managed Detection and Response 說明

Kaspersky Endpoint Security 版本 11.2.0 – 11.8.0 的分發套件包括 Kaspersky Endpoint Agent。您可以在安裝 Kaspersky Endpoint Security for Windows 時選擇分發套件 Kaspersky Endpoint Agent。因此，您的電腦上將安裝兩個應用程式：KEA 和 KES。在 Kaspersky Endpoint Security 11.9.0 中，Kaspersky Endpoint Agent 分發套件不再是 Kaspersky Endpoint Security 分發套件的一部分。

KEA 版本（作為 KES 的一部分）與 KES 版本的對應關係

| Kaspersky Endpoint Security for Windows | Kaspersky Endpoint Agent |
|---|---|
| 11.8.0 | 3.11.0.216.mr1 |
| 11.7.0 | 3.11 |
| 11.6.0 | 3.10 |
| 11.5.0 | 3.9 |
| 11.4.0 | 3.9 |
| 11.3.0 | 3.9 |
| 11.2.0 | 3.9 |

卡巴斯基正在將所有 Detection and Response 切換為使用 Kaspersky Endpoint Security 內建代理，而不是 Kaspersky Endpoint Agent。卡巴斯基正在逐步增加對這些解決方案的支援並逐步淘汰 Kaspersky Endpoint Agent（見下表）。從版本 12.1 開始，該應用程式支援所有 Detection and Response 解決方案。此外，從 12.1 版本開始，該應用程式不再與 Kaspersky Endpoint Agent 相容，並且不再可能在同一台電腦上同時安裝這兩個應用程式。

| Kaspersky Endpoint Security 的版本 | Kaspersky Managed Detection and Response | Kaspersky Sandbox | Kaspersky Endpoint Detection and Response Optimum | Kaspersky Endpoint Detection and Response Expert | Kaspersky Anti Targeted Attack Platform（Endpoint Detection and Response 元件） | Kaspersky Anti Targeted Attack Platform（Network Detection and Response 元件） |
|---|---|---|---|---|---|---|
| 11.5.0 | Kaspersky Endpoint Agent | Kaspersky Endpoint Agent | Kaspersky Endpoint Agent | Kaspersky Endpoint Agent | Kaspersky Endpoint Agent | Kaspersky Endpoint Agent |
| 11.6.0 | **內建代理** | Kaspersky Endpoint Agent | Kaspersky Endpoint Agent | Kaspersky Endpoint Agent | Kaspersky Endpoint Agent | Kaspersky Endpoint Agent |
| 11.7.0 | **內建代理** | **內建代理** | **內建代理** | Kaspersky Endpoint Agent | Kaspersky Endpoint Agent | Kaspersky Endpoint Agent |
| 11.8.0 | **內建代理** | **內建代理** | **內建代理** | **內建代理** | Kaspersky Endpoint Agent | Kaspersky Endpoint Agent |
| 11.9.0 | **內建代理** | **內建代理** | **內建代理** | **內建代理** | Kaspersky Endpoint Agent | Kaspersky Endpoint Agent |
| 11.10.0 | **內建代理** | **內建代理** | **內建代理** | **內建代理** | Kaspersky Endpoint Agent | Kaspersky Endpoint Agent |
| 11.11.0 | **內建代理** | **內建代理** | **內建代理** | **內建代理** | Kaspersky Endpoint Agent | Kaspersky Endpoint Agent |
| 12 | **內建代理** | **內建代理** | **內建代理** | **內建代理** | Kaspersky Endpoint Agent | Kaspersky Endpoint Agent |
| 12.1 | **內建代理** | **內建代理** | **內建代理** | **內建代理** | **內建代理** | Kaspersky Endpoint Agent |
| 12.6 | **內建代理** | **內建代理** | **內建代理** | **內建代理** | **內建代理** | **內建代理** |

# 將 [KES+KEA] 配置遷移到 [KES+內建代理] 配置

Kaspersky Endpoint Security 包括可處理 Detection and Response 解決方案的內建代理。您再也無需分開 Kaspersky Endpoint Agent 應用程式來使用這些解決方案。當您在安裝了 Kaspersky Endpoint Agent 的電腦上部署 Kaspersky Endpoint Security 時，Detection and Response 解決方案將繼續與 Kaspersky Endpoint Security 一起工作。此外，Kaspersky Endpoint Agent 將被從電腦移除。

Kaspersky Endpoint Security 版本 11.2.0 – 11.8.0 的分發套件包括 Kaspersky Endpoint Agent。您可以在安裝 Kaspersky Endpoint Security for Windows 時選擇分發套件 Kaspersky Endpoint Agent。因此，您的電腦上將安裝兩個應用程式：KEA 和 KES。在 Kaspersky Endpoint Security 11.9.0 中，Kaspersky Endpoint Agent 分發套件不再是 Kaspersky Endpoint Security 分發套件的一部分。

將 [KES+KEA] 配置遷移到 [KES+內建代理] 包含以下步驟：

1. **升級卡巴斯基安全管理中心**

   將所有卡巴斯基安全管理中心元件升級到版本 13.2 或更高版本，包括使用者電腦和網頁主控台上的網路代理。

2. **升級 Kaspersky Endpoint Security 網頁外掛程式**

   在卡巴斯基安全管理中心網頁主控台中，升級 Kaspersky Endpoint Security 網頁外掛程式到版本 11.7.0 或更高版本。若要管理 EDR Optimum 和 Kaspersky Sandbox 元件，您必須使用網頁主控台。

   要使用 Kaspersky Anti Targeted Attack Platform (EDR)，您需要一個適用於 Kaspersky Endpoint Security 12.1 或更高版本的 Web 外掛程式。

   要使用 Kaspersky Anti Targeted Attack Platform (NDR)，您需要一個適用於 Kaspersky Endpoint Security 12.7 或更高版本的 Web 外掛程式。

### 3 遷移政策和工作

使用 Kaspersky Endpoint Agent 政策和工作遷移精靈將 Kaspersky Endpoint Agent 設定遷移到 Kaspersky Endpoint Security for Windows。

這將建立一個新的 Kaspersky Endpoint Security 政策。新政策的狀態為*非作用中*。若要套用政策，請開啟政策內容，接受卡巴斯基安全網路聲明，然後將狀態設定為*作用中*。

### 4 產品授權功能

如果您使用 Kaspersky Endpoint Detection and Response Optimum 或 Kaspersky Optimum Security 產品授權來啟動 Kaspersky Endpoint Security for Windows 和 Kaspersky Endpoint Agent，EDR Optimum 功能將在升級應用程式到版本 11.7.0 後自動啟動。您不需要做任何其它事情。

如果使用獨立 Kaspersky Endpoint Detection and Response Optimum 附加元件產品授權啟動 EDR Optimum 功能，您必須確保 EDR Optimum 附加元件金鑰已新增到卡巴斯基安全管理中心存放庫且產品授權金鑰自動分發功能已啟用。升級應用程式到版本 11.7.0 後，EDR Optimum 功能將被自動啟動。

如果使用 Kaspersky Endpoint Detection and Response Optimum 或 Kaspersky Optimum Security 產品授權啟動 Kaspersky Endpoint Agent，使用其他產品授權啟動 Kaspersky Endpoint Security for Windows，您必須將 Kaspersky Endpoint Security for Windows 金鑰替換為普通的 Kaspersky Endpoint Detection and Response Optimum 金鑰或 Kaspersky Optimum Security 金鑰。您可以使用"*新增金鑰*"工作取代金鑰。

您不需要啟動 Kaspersky Sandbox 功能。升級和啟動 Kaspersky Endpoint Security for Windows 後，Kaspersky Sandbox 功能將立即可用。

只有 Kaspersky Anti Targeted Attack Platform 產品授權可用於啟動作為 Kaspersky Anti Targeted Attack Platform 解決方案一部分的 Kaspersky Endpoint Security 。升級應用程式到版本 12.1 後，EDR (KATA) 功能將被自動啟動。您不需要做任何其它事情。

### 5 升級 Kaspersky Endpoint Security 應用程式

升級和遷移 EDR Optimum 和 Kaspersky Sandbox 功能建議使用遠端安裝工作。

若要使用遠端安裝工作升級應用程式，您必須編輯以下設定：

- 在安裝套件的設定中選擇適用於 Detection and Response 解決方案的元件。
- 在安裝套件的設定中排除 Kaspersky Endpoint Agent 元件（適用於 Kaspersky Endpoint Security for Windows 版本 11.2.0 – 11.8.0）。
- 如果啟用密碼防護來限制對 Kaspersky Endpoint Agent 的存取，請在*遠端安裝應用程式*工作的設定中輸入應用程式解除安裝密碼。從卡巴斯基安全管理中心 Linux 15.1 開始，您可以輸入解除安裝密碼。

您還可以使用以下方法升級應用程式：

- 使用 Kaspersky 更新服務（無縫更新 - SMU）。
- 本機使用安裝精靈。

當在安裝了 Kaspersky Endpoint Agent 的電腦上升級應用程式時，Kaspersky Endpoint Security 支援自動選擇元件。自動選擇元件取決於升級應用程式的使用者帳戶的權限。

如果在系統帳戶 (SYSTEM) 下使用 EXE 或 MSI 檔案升級 Kaspersky Endpoint Security，Kaspersky Endpoint Security 將獲得對 Kaspersky 解決方案的目前產品授權的存取權限。因此，如果電腦安裝了 Kaspersky Endpoint Agent 且啟動了 EDR Optimum 解決方案，Kaspersky Endpoint Security 安裝程式將自動配置元件集合並選擇 EDR Optimum 元件。這將使得 Kaspersky Endpoint Security 切換到使用內建代理並刪除 Kaspersky Endpoint Agent。在系統帳戶 (SYSTEM) 下執行 MSI 安裝程式通常在透過 Kaspersky 更新服務 (SMU) 升級或透過卡巴斯基安全管理中心部署安裝套件時進行。

如果在沒有權限的帳戶下使用 MSI 檔案升級 Kaspersky Endpoint Security，Kaspersky Endpoint Security 將缺少對 Kaspersky 解決方案的目前產品授權的存取權限。在此情況下，Kaspersky Endpoint Security 將基於 Kaspersky Endpoint Agent 配置自動選擇元件。此後，Kaspersky Endpoint Security 將切換到使用內建代理並刪除 Kaspersky Endpoint Agent。

6. **電腦重新啟動**

   重新啟動電腦以完成用內建代理升級應用程式。升級應用程式時，安裝程式會在重新啟動電腦前移除 Kaspersky Endpoint Agent。重新啟動電腦後，安裝程式會新增內建代理。這意味著只有在重新啟動電腦後 Kaspersky Endpoint Security 才會執行 EDR 和 Kaspersky Sandbox 的功能。

7. **檢查 Kaspersky Endpoint Detection and Response Optimum 和 Kaspersky Sandbox 的健康**

   如果升級後電腦在卡巴斯基安全管理中心中具有"*緊急*"狀態：

   - 請確保電腦安裝了網路代理 13.2或更高版本。
   - 透過檢視"*應用程式元件狀態報告*"來檢查內建代理的運行狀態。如果元件的狀態為"*未安裝*"，請使用*變更應用程式元件*工作來安裝元件。
   - 請確保在 Kaspersky Endpoint Security for Windows 的新政策中接受卡巴斯基安全網路聲明。
   - 確保使用*應用程式元件狀態報告*啟動 EDR Optimum 功能 。如果元件的狀態為"*產品授權不支援*"，請確保 EDR Optimum 的產品授權金鑰自動分發功能已開啟。

# Kaspersky Endpoint Agent 的政策和工作遷移

Kaspersky Endpoint Security for Windows 包含從 Kaspersky Endpoint Agent 遷移到 Kaspersky Endpoint Security 的精靈。您可以遷移以下解決方案的政策和工作設定：

- Kaspersky Sandbox
- Kaspersky Endpoint Detection and Response Optimum (EDR Optimum)
- Kaspersky Anti Targeted Attack Platform

從 Kaspersky Endpoint Agent 遷移到 Kaspersky Endpoint Security 的精靈僅適用於網頁主控台和 Cloud Console。在管理主控台 (MMC) 中，您只能使用標準卡巴斯基安全管理中心政策和工作移轉精靈遷移 Kaspersky Anti Targeted Attack Platform (EDR) 解決方案的設定。

建議先在單個電腦上將 Kaspersky Endpoint Agent 遷移到 Kaspersky Endpoint Security，然後在一組電腦上執行，然後在組織的所有電腦上完成遷移。

*要將政策和工作設定從 Kaspersky Endpoint Agent 遷移到 Kaspersky Endpoint Security，*

在網頁主控台的主視窗中，選擇**操作 → 從 Kaspersky Endpoint Agent 遷移**。

這會執行政策和工作遷移精靈。按照精靈的說明進行操作。

步驟 1. 政策遷移

遷移精靈會建立一個新政策，將 Kaspersky Endpoint Security 和 Kaspersky Endpoint Agent 政策的設定合併。在政策清單中，選擇您想將其設定與 Kaspersky Endpoint Security 政策合併的 Kaspersky Endpoint Agent 政策。點擊 Kaspersky Endpoint Agent 政策以選擇您想與其合併設定的 Kaspersky Endpoint Security 政策。確保選擇了正確的政策然後前往下一步。

步驟 2. 工作遷移

遷移精靈將為 Kaspersky Endpoint Security 建立新工作。在工作清單中，選擇您想為其設定 Kaspersky Endpoint Security 政策的 Kaspersky Endpoint Agent 工作。精靈支援 Kaspersky Endpoint Detection and Response 和 Kaspersky Sandbox 的工作。前往下一步。

步驟 3. 精靈完成

結束精靈。結果，精靈將執行以下操作：

- 建立一個新的 Kaspersky Endpoint Security 政策。

  政策將合併 Kaspersky Endpoint Security 和 Kaspersky Endpoint Agent 的設定。政策稱為 *<Kaspersky Endpoint Security 政策名稱> & <Kaspersky Endpoint Agent 政策名稱>*。新政策的狀態為*非作用中*。若要繼續，將 Kaspersky Endpoint Agent 和 Kaspersky Endpoint Security 政策的狀態變更為*非作用中*，然後啟動新合併的政策。

  從 Kaspersky Endpoint Agent 遷移到 Kaspersky Endpoint Security for Windows 後，請確保新政策已設定將資料傳輸到管理伺服器的功能（隔離檔案資料和威脅發展鏈資料）。資料傳輸參數值不會從 Kaspersky Endpoint Agent 政策遷移。

  從 Kaspersky Endpoint Agent 遷移到 Kaspersky Endpoint Security 以用於 Kaspersky Anti Targeted Attack Platform (EDR) 解決方案時，您在將電腦連線到中央節點伺服器時可能會遇到錯誤。原因是網頁主控台中的遷移精靈略過了以下政策設定並且不遷移它們：

  - 設定修改禁止 **連線到 KATA 伺服器**（“鎖”）。

    預設情況下，設定可以被修改（“鎖”是開啟的）。因此，設定不會套用到電腦上。您必須禁止修改設定並關閉“鎖”。

  - 加密容器。

    如果您使用雙向身分驗證連線到中央節點伺服器，則必須重新新增加密容器。遷移精靈正確遷移了伺服器的 TLS 憑證。

  管理主控台 (MMC) 中的政策和工作遷移精靈可遷移 Kaspersky Anti Targeted Attack Platform (EDR) 解決方案的所有設定。

- 建立新的 Kaspersky Endpoint Security 工作。

  新工作是 Kaspersky Endpoint Detection and Response 和 Kaspersky Sandbox 的 Kaspersky Endpoint Agent 工作的副本。同時，精靈不會變更 Kaspersky Endpoint Agent 工作。

**如何在管理主控台 (MMC)（僅適用於 KATA (EDR)）中將政策和工作設定從 Kaspersky Endpoint Agent 遷移到 Kaspersky Endpoint Security**

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

政策和工作批量轉換精靈將啟動。按照精靈的說明進行操作。

步驟 1. 選擇需要為其轉換政策和工作的應用程式

在此步驟，您需要選擇 Kaspersky Endpoint Security for Windows。前往下一步。

步驟 2. 轉換政策

移轉精靈會建立新的 Kaspersky Endpoint Security 政策，Kaspersky Endpoint Agent 政策設定將遷移到該政策中。在政策清單中，選擇您想將其設定轉移至 Kaspersky Endpoint Security 政策的 Kaspersky Endpoint Agent 政策。前往下一步。

遷移精靈將開始轉換政策。在政策轉換期間，移轉精靈會提示您接受卡巴斯基安全網路聲明。新政策將被命名為 *<政策名稱>（已轉換）*。

步驟 3. 轉換工作

略過此步驟。精靈僅支援 Kaspersky Endpoint Detection and Response Optimum 和 Kaspersky Sandbox 的工作。這些元件的管理僅在網頁主控台中可用。前往下一步。

步驟 4. 精靈完成

結束精靈。作為精靈的結果，將建立新的 Kaspersky Endpoint Security 政策。

# Endpoint Detection and Response Agent (EDR Agent)

從 Kaspersky Endpoint Security 12.3 for Windows 開始，應用程式包含 Endpoint Detection and Response Agent (EDR Agent) 配置。*Endpoint Detection and Response Agent* 是一個應用程式，安裝在組織 IT 基礎結構中的各個工作站和伺服器上，用於支援卡巴斯基的 Detection and Response 解決方案：

- Kaspersky Managed Detection and Response
- Kaspersky Anti Targeted Attack Platform (EDR)
- Kaspersky Unified Monitoring and Analysis Platform (KUMA)（從版本 12.6 開始）

- Kaspersky Anti Targeted Attack Platform (NDR)（從版本 12.7 開始）
- Kaspersky Endpoint Detection and Response Expert (on-premise)（自版本 12.11 起）

EDR Agent 持續監視在這些電腦上執行的處理程序、開啟的網路連線以及正在修改的檔案。應用程式的防護和控制元件不可用於 EDR Agent。

EDR Agent 與協力廠商 EPP應用程式相容。這使您可以將協力廠商基礎結構安全工具與卡巴斯基的 Detection and Response 一起使用。

要部署 EDR Agent，電腦必須安裝網路代理，並且必須將電腦新增到卡巴斯基安全管理中心主控台中。要啟用 EDR Agent 與卡巴斯基安全管理中心的交互，您必須安裝 Kaspersky Endpoint Security for Windows 管理外掛程式。您可以使用群組政策指定 EDR Agent 設定。要整合 EDR Agent，您必須在適當的政策區域中配置整合。

以下卡巴斯基應用程式必須安裝在基礎結構上以支援 Kaspersky Detection and Response 解決方案：

| | |
|---|---|
|  | • 網路代理<br>• EDR Agent |
| **Endpoint** | |
|  | Kaspersky Endpoint Security for Windows 管理外掛程式 |
| **卡巴斯基安全管理中心** | |
|  | |
| **Detection and Response 解決方案：MDR、KATA（EDR）、KATA（NDR）、KUMA、EDR Expert (on-premise)** | |

# 安裝 EDR Agent

對於 Kaspersky Managed Detection and Response 解決方案，Kaspersky Endpoint Security 在 Endpoint Detection and Response Agent (EDR Agent) 中配置的安裝方式相同。

EDR Agent 可以通過以下方式之一安裝在電腦上：

- 遠端使用卡巴斯基安全管理中心。
- 本機使用安裝精靈。
- 本機透過命令列（僅適用於 KATA (EDR) 和 EDR Expert (內部部署)）。

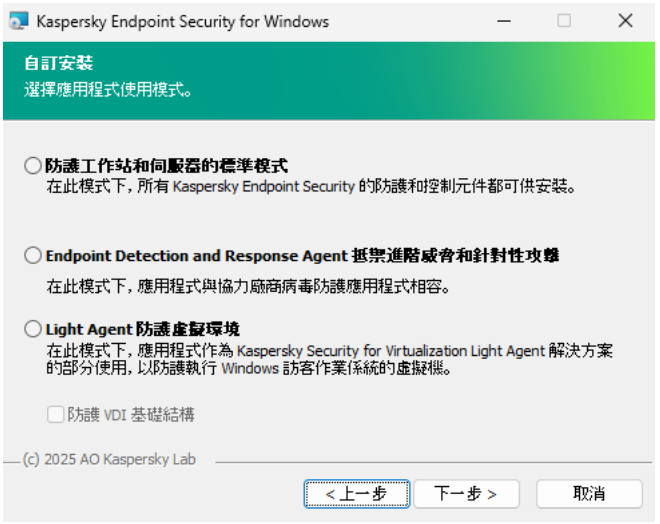
要安裝 EDR Agent，您必須在安裝套件設定或在安裝精靈中選擇適當的配置。

**如何使用安裝精靈安裝 EDR Agent**

1. 複製"分發套件"資料夾到使用者的電腦。
2. 執行 setup_kes.exe。

   啟動"安裝精靈"。

## Kaspersky Endpoint Security 的配置



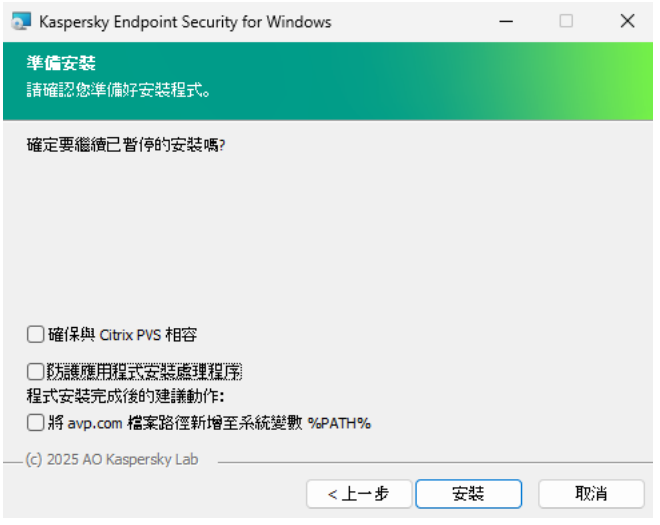

選擇應用程式的配置

選擇 **Endpoint Detection and Response Agent** 配置。在此配置中，您只能安裝為 Detection and Response 解決方案提供支援的元件： MDR，EDR (KATA)， NDR (KATA)， EDR Expert (on-premise) 以及 KUMA。如果您的組織中與 Kaspersky Detection and Response 解決方案一起部署了協力廠商Endpoint Protection Platform (EPP)，則需要此配置。這使得 Endpoint Detection and Response Agent 配置中的 Kaspersky Endpoint Security 與協力廠商 EPP 應用程式相容。

## Kaspersky Endpoint Security 元件

選擇您要安裝的元件。安裝應用程式後，您可以變更可用的應用程式元件。為此，您需要再次執行安裝精靈，然後選擇變更可用元件。

## 進階設定




*進階應用程式安裝設定*

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

**確保與 Citrix PVS 相容**您可以啟用Citrix Provisioning Services支援以將 Kaspersky Endpoint Security 安裝到虛擬機。

**將 avp.com 檔案路徑新增至系統變數 %PATH%**您可以將安裝路徑新增到%PATH%變數中，以方便使用命令列介面。

**如何在命令行上安裝 EDR Agent（僅適用於 KATA (EDR) 和 EDR Expert (on-premise)）**

1. 以管理員身分執行命令列解譯器 (cmd.exe)。
2. 轉到 Kaspersky Endpoint Security 分發套件所在資料夾。
3. 執行以下指令：

   ```
   setup_kes.exe /pEULA=1 /pPRIVACYPOLICY=1 /pKSN=1 /pSTANDALONEMODE=1 [/s]
   ```

   或

   ```
   msiexec /i <distribution kit name> EULA=1 PRIVACYPOLICY=1 KSN=1 STANDALONEMODE=1 [/qn]
   ```

   因此，用於與 Kaspersky Anti Targeted Attack Platform (EDR) 或者 Kaspersky Endpoint Detection and Response Expert（內部數）整合的 EDR Agent 應用程式將安裝在電腦上。您可以透過"`status`"命令確認應用程式是否已安裝並檢查應用程式設定。

**如何使用管理主控台 (MMC) 安裝 EDR Agent**

1. 開啟卡巴斯基安全管理中心管理主控台。
2. 在主控台樹狀目錄中，選擇**進階 → 遠端安裝 → 安裝套件**資料夾。

   這將開啟已下載到卡巴斯基安全管理中心的安裝套件清單。
3. 開啟安裝套件的內容。

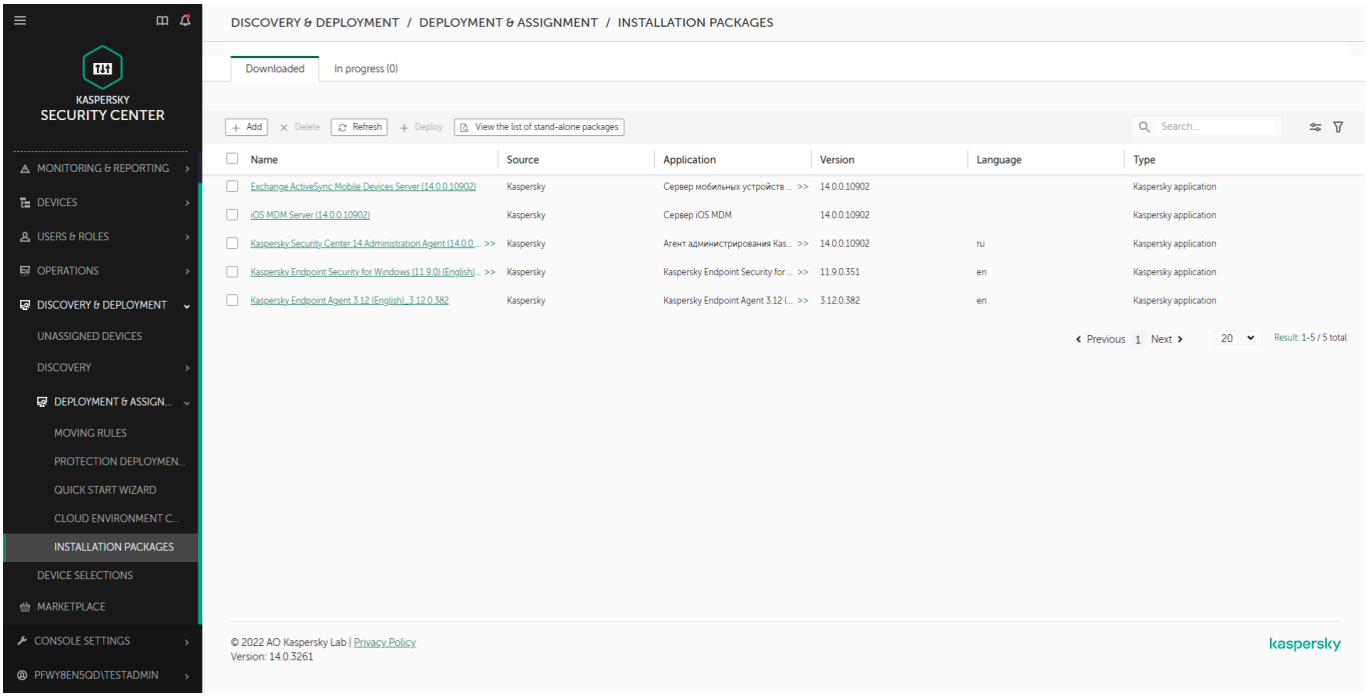
   如果有需要的話，建立新的安裝套件。
4. 轉到"**防護元件**"區域。
5. 選擇 **Endpoint Detection and Response Agent 抵禦進階威脅和針對性攻擊** 配置。在此配置中，您只能安裝為 Detection and Response 解決方案提供支援的元件：MDR，EDR (KATA)，NDR (KATA)，EDR Expert (on-premise) 以及 KUMA。如果您的組織中與 Kaspersky Detection and Response 解決方案一起部署了協力廠商 Endpoint Protection Platform (EPP)，則需要此配置。這使得 Endpoint Detection and Response Agent 配置中的 Kaspersky Endpoint Security 與協力廠商 EPP 應用程式相容。
6. 選擇您要安裝的元件。

   安裝應用程式後，您可以變更可用的應用程式元件。
7. 儲存變更。
8. 建立遠端安裝工作。在工作屬性中，選擇您創建的安裝包。

**如何使用網頁主控台安裝 EDR Agent**

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

這將開啟已下載到卡巴斯基安全管理中心的安裝套件清單。



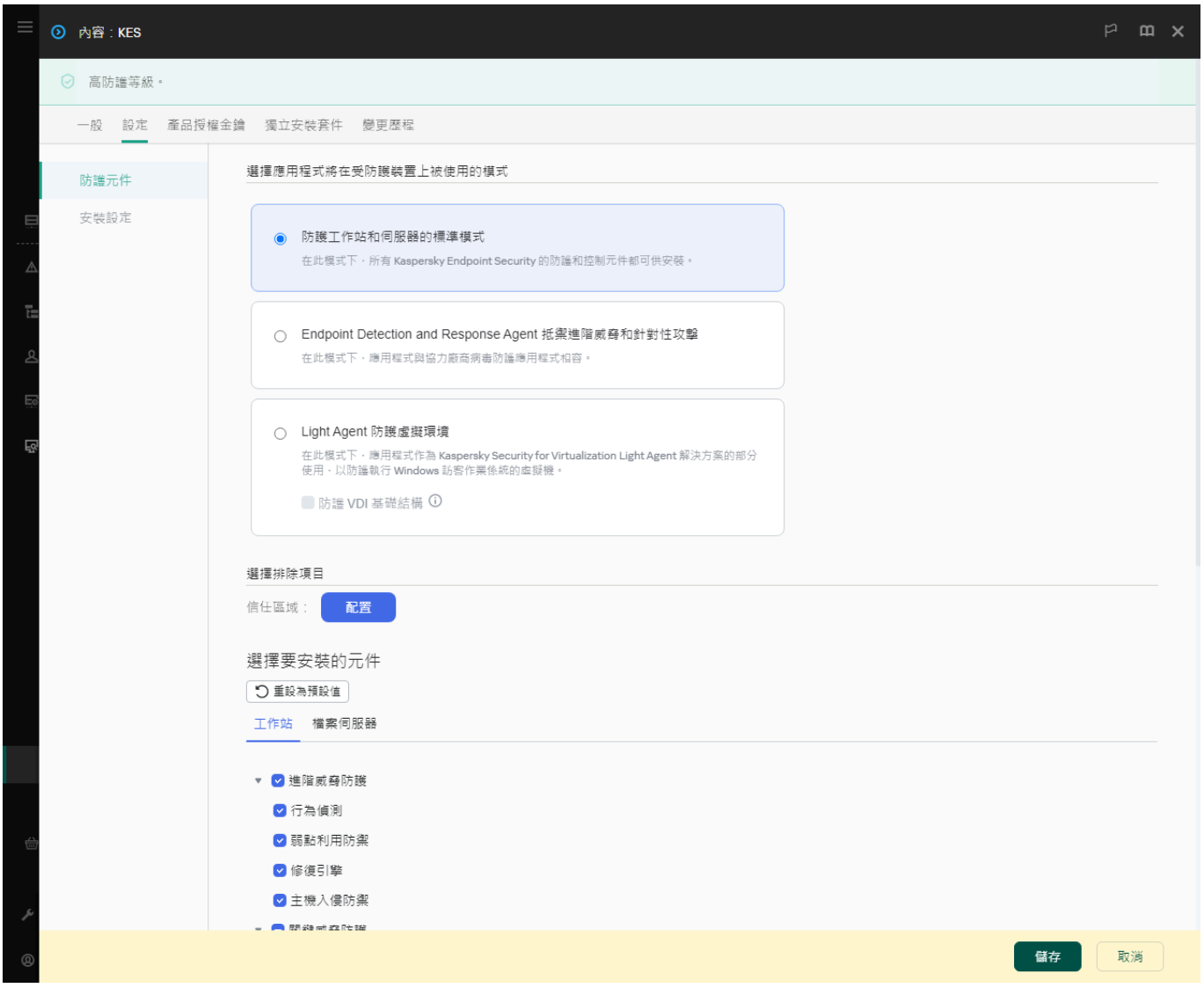

安裝套件清單

2. 開啟安裝套件的內容。

   如果有需要的話，建立新的安裝套件。

3. 選擇**"設定"**標籤。

4. 轉到“**防護元件**”區域。




安裝套件中包含的元件

5. 選擇 **Endpoint Detection and Response Agent 抵禦進階威脅和針對性攻擊** 配置。在此配置中，您只能安裝為 Detection and Response 解決方案提供支援的元件： MDR，EDR (KATA)，NDR (KATA)，EDR Expert (on-premise) 以及 KUMA。如果您的組織中與 Kaspersky Detection and Response 解決方案一起部署了協力廠商 Endpoint Protection Platform (EPP)，則需要此配置。這使得 Endpoint Detection and Response Agent 配置中的 Kaspersky Endpoint Security 與協力廠商 EPP 應用程式相容。

6. 選擇您要安裝的元件。

   安裝應用程式後，您可以變更可用的應用程式元件。

7. 儲存變更。

8. 建立遠端安裝工作。在工作屬性中，選擇您創建的安裝包。

結果，EDR Agent 被安裝在使用者的電腦上。您可以使用應用程式的介面，通知區域中會顯示應用程式的圖示 。

在卡巴斯基安全管理中心中，在 EDR Agent 配置中安裝了應用程式的電腦具有緊急狀態 - 。電腦出現此狀態是因為缺少檔案威脅防護元件。您無需執行其他任何操作。

如果由於安裝程式在電腦上發現不相容的軟體而無法在具有協力廠商 EPP 應用程式的電腦上安裝 EDR Agent，您可以跳過不相容軟體檢查。




EDR Agent 的主視窗

現在，您必須配置與 Kaspersky Managed Detection and Response、Kaspersky Anti Targeted Attack (EDR) 或者 Kaspersky Anti Targeted Attack (NDR)解決方案的整合。您還可以指定應用程式的進階設定，例如，建立信任區域或者隱藏應用程式的介面。以下區域中的設定可用：

- 卡巴斯基安全網路
- 應用程式設定
- 網路設定
- 排除項目
- 報告

- 介面
- 管理設定

# 將 EDR Agent 與 MDR 整合

EDR Agent 安裝在組織 IT 基礎結構中的工作站和伺服器上。EDR Agent 可處理資料並通過卡巴斯基安全網路串流將其傳送到 Kaspersky Managed Detection and Response。

若要透過卡巴斯基安全管理中心網頁主控台讓 Kaspersky Managed Detection and Response 和管理伺服器一起工作，您必須建立一個新的安全連線，一個*背景連線*。Kaspersky Managed Detection and Response 提示您在部署解決方案時建立一個背景連線。確保背景連線已建立。

**在網頁主控台中建立一個背景連線**

1. 在網頁主控台的主視窗中，選擇**設定 → 整合**。
2. 轉到"**整合**"區域。
3. 開啟"**整合的背景連線 已啟用**"開關。
4. 儲存變更。

與 Kaspersky Managed Detection and Response 整合包括以下步驟：

1. **安裝 Managed Detection and Response 元件**

   您可以在安裝或者升級期間以及使用*變更應用程式元件*工作時選擇 MDR 元件。

   > 您必須重新啟動電腦以完成升級含新元件的應用程式。

2. **配置卡巴斯基私有安全網路**

   > 如果您使用的是卡巴斯基安全管理中心雲端主控台，略過這一步。卡巴斯基安全管理中心雲端主控台會在安裝 MDR 外挂程式時自動配置卡巴斯基私有安全網路。

   *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。

   在管理伺服器屬性中上傳卡巴斯基安全網路設定檔。卡巴斯基安全網路設定檔位於 MDR 設定檔的 ZIP 存檔中。您可以在 Kaspersky Managed Detection and Response 主控台中獲取 ZIP 存檔。有關配置卡巴斯基私有安全網路的詳細資訊，請參閱 卡巴斯基安全管理中心說明。您也可以從命令行將卡巴斯基安全網路設定檔上傳到電腦（請參閱以下說明）。

   **如何從命令行配置卡巴斯基私有安全網路**

   1. 以管理員身分執行命令列解譯器 (cmd.exe)。
   2. 轉到 Kaspersky Endpoint Security 可執行檔所在資料夾。
   3. 執行以下指令：

      ```
      avp.com KSN /private <file name>
      ```

其中<file name>是包含私有卡巴斯基私有安全網路設定（PKCS7 或 PEM 檔案格式）的設定檔的名稱。

範例:
```
avp.com KSN /private C:\kpsn_config.pkcs7
```

結果，Kaspersky Endpoint Security 將使用私有卡巴斯基私有安全網路來確定檔案、應用程式和網站的信譽。政策設定的**卡巴斯基安全網路**部分將顯示以下運行狀態：*基礎結構: 卡巴斯基私有安全網路*。

您必須啟用延伸 KSN 模式才能使 Managed Detection and Response 正常工作。

3. **啟動 Kaspersky Managed Detection and Response**

從 Kaspersky Endpoint Security for Windows 12.10 開始，若要啟動 Managed Detection and Response 功能，作為 啟動碼的替代方式，您也可以使用 金鑰檔案。

您需要單獨購買 MDR（Kaspersky Network Detection and Response 附加元件）的產品授權。

為 Kaspersky Managed Detection and Response 附加元件新增單獨的金鑰後，該功能將可用。獨立 Managed Detection and Response 功能的授權和 Kaspersky Endpoint Security 的授權一樣。

確保 MDR 功能包括在產品授權中且在應用程式的本機介面中工作。

4. **啟用 Managed Detection and Response 元件**

在 Kaspersky Endpoint Security 政策中加載 BLOB 設定檔（請參閱以下說明）。BLOB 檔案包含用戶端 ID 以及有關卡巴斯基 Managed Detection and Response 產品許可的資訊。BLOB 檔案位於 MDR 設定檔的 ZIP 存檔中。您可以在 Kaspersky Managed Detection and Response 主控台中獲取 ZIP 存檔。有關 BLOB 檔案的詳細資訊，請參閱 Kaspersky Managed Detection and Response 說明。

從 Kaspersky Endpoint Security 12.6 for Windows 開始，如果您擁有目前產品授權，則對於沒有租戶的 Kaspersky Managed Detection and Response 來說，新增 BLOB 檔案可選。

**如何在管理主控台 (MMC) 中啟用 Managed Detection and Response 元件**

1. 在卡巴斯基安全管理中心管理主控台樹狀目錄中，選取**政策**。
2. 選擇必要的政策並點擊以開啟政策內容。
3. 在政策視窗中，選擇“**Detection and Response → Managed Detection and Response (Industrial CyberSecurity)**”。
4. 選擇“**Managed Detection and Response (Industrial CyberSecurity)**”核取方塊。
5. 在“**設定**“塊中，點擊“**上傳**”，然後選擇在 Kaspersky Managed Detection and Response Console 中接收到的 BLOB 檔案。該檔案具有 P7 副檔名。

   預設情況下，允許使用者管理應用程式設定（“掛鎖”開啟）。若要在電腦上套用該政策，請關閉掛鎖。

6. 儲存變更。

**如何在網頁主控台和雲端主控台中啟用 Managed Detection and Response 元件**

1. 在網頁主控台的主視窗中，選擇**資產（裝置）→政策和設定檔**。
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**"→"**Managed Detection and Response**"。
5. 開啟"**已啟用 Managed Detection and Response**"開關。
6. 點擊"**上傳**"，然後選擇在 Kaspersky Managed Detection and Response 主控台中獲取的 BLOB 檔案。該檔案具有 P7 副檔名。

   預設情況下，允許使用者管理政策設定（"掛鎖"開啟）。若要在電腦上套用該政策，請關閉掛鎖。
7. 儲存變更。

**如何從命令行啟用 Managed Detection and Response 元件**

1. 以管理員身分執行命令列解譯器 (cmd.exe)。
2. 轉到 Kaspersky Endpoint Security 可執行檔所在資料夾。
3. 執行以下指令：

   ```
   avp.com MDRLICENSE /ADD <file name> /login=<user name> /password=<password>
   ```

   要執行此指令，必須啟用密碼防護。使用者必須具有"**配置應用程式設定**"權限。

結果，Kaspersky Endpoint Security 將驗證 BLOB 檔案。BLOB 檔案驗證包括檢查數位簽章和產品授權期限。如果 BLOB 檔案驗證成功，在與卡巴斯基安全管理中心進行下一次同步時，Kaspersky Endpoint Security 將下載該檔案並將其傳送到電腦。透過檢視"*應用程式元件狀態報告*"來檢查元件的運行狀態。您還可以在 Kaspersky Endpoint Security 的本地介面中的報告中檢視元件的運行狀態。"**Managed Detection and Response**"元件將新增到 Kaspersky Endpoint Security 元件清單中。

**5 配置應用程式的其他元件以接收遙測資料**

您必須啟用延伸以下元件才能使 Managed Detection and Response 正常工作：

- 卡巴斯基安全網路（延伸模式）。

  當透過 Kerberos 身分驗證使用代理伺服器時，建議使用 KSN Proxy 和 HTTPS 傳輸協定。請參閱 卡巴斯基安全管理中心說明 瞭解更多詳情。

- 行為偵測。

必須啟用這些元件。否則，因為沒有收到所需的遙測資料，Kaspersky Managed Detection and Response 將無法工作。

此外，Kaspersky Managed Detection and Response 使用從其他應用程式元件收到的資料。可選擇啟用這些元件。提供其他資料的元件包括：

- Web 威脅防護。
- 郵件威脅防護。
- 防火牆。

1. 在網頁主控台的主視窗中，選擇**資產（裝置）→政策和設定檔**。
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**"→"**Managed Detection and Response**"。
5. 開啟"**已啟用 Managed Detection and Response**"開關。
6. 儲存變更。

1. 在卡巴斯基安全管理中心管理主控台樹狀目錄中，選取**政策**。
2. 選擇必要的政策並點擊以開啟政策內容。
3. 在政策視窗中，選擇"**Detection and Response → Managed Detection and Response (Industrial CyberSecurity)**"。
4. 選擇"**Managed Detection and Response (Industrial CyberSecurity)**"核取方塊。
5. 儲存變更。

# 將 EDR Agent 與 EDR (KATA) 整合

EDR Agent 安裝在組織 IT 基礎結構中的工作站和伺服器上。在這些電腦上，EDR Agent 持續監視處理程序、開啟的網路連線和正在修改的檔案，並將監視資料傳送到具有中央節點元件的伺服器。

要與 EDR (KATA) 整合，您必須啟用 Endpoint Detection and Response (KATA) 元件並配置 EDR Agent。

Endpoint Detection and Response (KATA) 要工作必須滿足以下條件：

- Kaspersky Anti Targeted Attack Platform 版本 5.0–7.1。
- 卡巴斯基安全管理中心版本 14.2 或更高版本。在早期版本的卡巴斯基安全管理中心中，無法啟動 Endpoint Detection and Response (KATA) 功能。

與 Endpoint Detection and Response (KATA) 整合涉及以下步驟：

1. **啟用 Endpoint Detection and Response (KATA)**

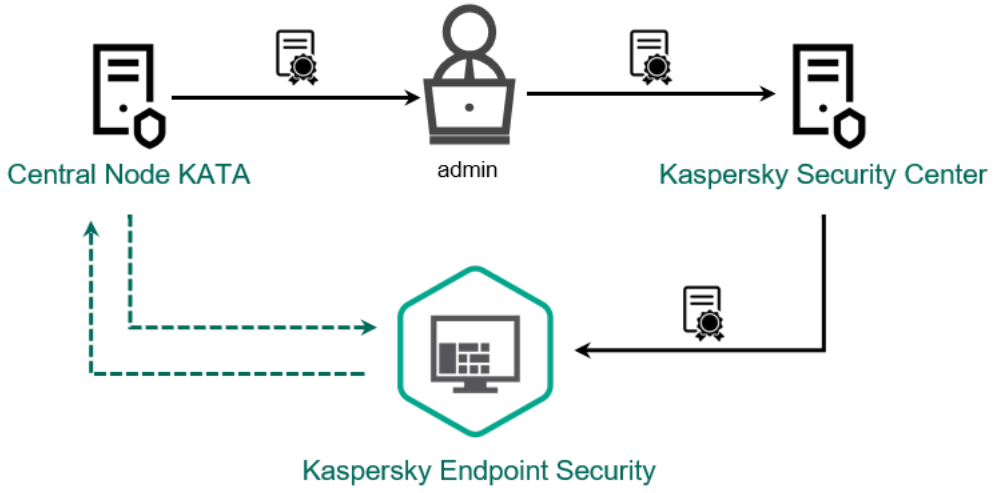
   您需要單獨購買 EDR (KATA)（Kaspersky Endpoint Detection and Response (KATA) 附加元件）的產品授權。

   為 Kaspersky Endpoint Detection and Response (KATA) 新增單獨的金鑰後，該功能將可用。獨立 Endpoint Detection and Response (KATA) 功能的授權和 Kaspersky Endpoint Security 的授權一樣。

確保 EDR (KATA) 功能包括在產品授權中且在應用程式的本機介面中執行。

### 2 連線到中央節點

Kaspersky Anti Targeted Attack Platform 要求在 Kaspersky Endpoint Security 和中央節點元件之間建立可信連線。要配置可信連線，您必須使用 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 ）。然後您必須將 TLS 憑證新增到 Kaspersky Endpoint Security（參見下面的說明）。




將 TLS 憑證新增到 Kaspersky Endpoint Security

預設情況下，Kaspersky Endpoint Security 僅檢查中央節點的 TLS 憑證。為了使連線更安全，您可以額外啟用在中央節點上進行電腦驗證（雙向身分驗證）。要啟用此驗證，您必須在中央節點和 Kaspersky Endpoint Security 設定中開啟雙向身分驗證。要使用雙向身分驗證，您還需要一個加密容器。*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 ）。

**如何使用管理主控台 (MMC) 將 Kaspersky Endpoint Security 電腦連線到中央節點**

1. 開啟卡巴斯基安全管理中心管理主控台。
2. 在主控台樹狀目錄中，選擇**"政策"**。
3. 選擇必要的政策並點擊以開啟政策內容。
4. 在政策視窗中，選擇**"Detection and Response → Endpoint Detection and Response Expert (on-premise)"**。
5. 選擇**"Endpoint Detection and Response Expert (on-premise)"**核取方塊。
6. 點擊**"伺服器連線設定"**。
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 TLS 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**"正常"**。
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。

   您可以新增多個中央節點伺服器位址。Kaspersky Endpoint Security 嘗試連線到第一個 IP 位址的伺服器。如果無法建立連線，Kaspersky Endpoint Security 將嘗試連線到清單中的第二個 IP 位址，依此類推。
10. 如果有需要的話，配置遙測。
11. 儲存變更。若要在電腦上套用該政策，請關閉掛鎖。

**如何使用網頁主控台將 Kaspersky Endpoint Security 電腦連線到中央節點**

1. 在網頁主控台的主視窗中，選擇**資產（裝置）→政策和設定檔**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 (on-premise)"**。
5. 開啟**"Endpoint Detection and Response Expert (on-premise) 已啟用"**開關。
6. 若要設定 EDR (KATA)，請從解決方案清單中選取 **Endpoint Detection and Response Expert（版本 7.1 或者更早版本）**。
7. 點擊**"連線設定"**。
8. 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。

9. 點擊**"確定"**。
10. 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。

    您可以新增多個中央節點伺服器位址。Kaspersky Endpoint Security 嘗試連線到第一個 IP 位址的伺服器。如果無法建立連線，Kaspersky Endpoint Security 將嘗試連線到清單中的第二個 IP 位址，依此類推。
11. 如果有需要的話，配置遙測。
12. 儲存變更。若要在電腦上套用該政策，請關閉掛鎖。

結果，電腦會被新增到 Kaspersky Anti Targeted Attack Platform 主控台上。透過檢視*"應用程式元件狀態報告"*來檢查元件的運行狀態。您還可以在 Kaspersky Endpoint Security 的本地介面中的報告中檢視元件的運行狀態。**"Endpoint Detection and Response Expert (on-premise)"**元件將新增到 Kaspersky Endpoint Security 元件清單中。

# 將 EDR Agent 與 NDR (KATA) 整合

EDR Agent 安裝在組織 IT 基礎結構中的工作站和伺服器上。在這些電腦上，EDR Agent 持續監視處理程序、開啟的網路連線和正在修改的檔案，並將監視資料傳送到具有中央節點元件的伺服器。

要與 NDR (KATA) 整合，您必須啟用 Network Detection and Response (KATA) 元件並配置 EDR Agent。

Network Detection and Response (KATA) 要工作必須滿足以下條件：

- Kaspersky Anti Targeted Attack Platform 版本 7.0 或更高版本。
- 卡巴斯基安全管理中心版本 14.2 或更高版本。在早期版本的卡巴斯基安全管理中心中，無法啟動 Network Detection and Response (KATA) 功能。

https://www.youtube.com/watch?v=gd-rySv0ThQ

與 Network Detection and Response (KATA) 整合涉及以下步驟：

1. **啟用 Network Detection and Response (KATA)**

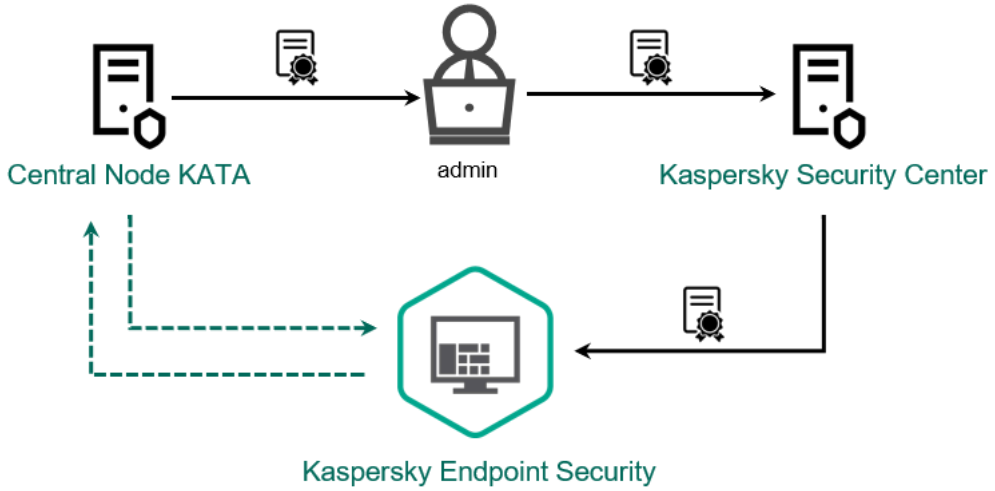
   您需要單獨購買 NDR (KATA)（Kaspersky Network Detection and Response (KATA) 附加元件）的產品授權。

   為 Kaspersky Network Detection and Response (KATA) 新增單獨的金鑰後，該功能將可用。獨立 Network Detection and Response (KATA) 功能的授權和 Kaspersky Endpoint Security 的授權一樣。

   確保 NDR (KATA) 功能包括在產品授權中且在應用程式的本機介面中執行。

2. **連線到中央節點**

   Kaspersky Anti Targeted Attack Platform 要求在 Kaspersky Endpoint Security 和中央節點元件之間建立可信連線。要配置可信連線，您必須使用 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）。然後您必須將 TLS 憑證新增到 Kaspersky Endpoint Security（參見下面的說明）。




將 TLS 憑證新增到 Kaspersky Endpoint Security

預設情況下，Kaspersky Endpoint Security 僅檢查中央節點的 TLS 憑證。為了使連線更安全，您可以額外啟用在中央節點上進行電腦驗證（雙向身分驗證）。要啟用此驗證，您必須在中央節點和 Kaspersky Endpoint Security 設定中開啟雙向身分驗證。要使用雙向身分驗證，您還需要一個加密容器。*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）。

**如何使用管理主控台 (MMC) 將 Kaspersky Endpoint Security 電腦連線到中央節點**

1. 在卡巴斯基安全管理中心管理主控台樹狀目錄中，選取**政策**。
2. 選擇必要的政策並點擊以開啟政策內容。
3. 在政策視窗中，選擇"**Detection and Response → Network Detection and Response (KATA)**"。
4. 選擇"**Network Detection and Response (KATA)**"核取方塊。
5. 點擊"**連線設定**"。
6. 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。
7. 點擊"**確定**"。
8. 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。
9. 您可以新增多個中央節點伺服器位址。Kaspersky Endpoint Security 嘗試連線到第一個 IP 位址的伺服器。如果無法建立連線，Kaspersky Endpoint Security 將嘗試連線到清單中的第二個 IP 位址，依此類推。
10. 如果有需要的話，配置遙測。
11. 儲存變更。

**如何使用網頁主控台將 Kaspersky Endpoint Security 電腦連線到中央節點**

1. 在網頁主控台的主視窗中，選擇**資產（裝置）→ 政策和設定檔**。
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**”→”**Network Detection and Response (KATA)**”。

5. 開啟“**Network Detection and Response (KATA) 已啟用**“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 嘗試連線到第一個 IP 位址的伺服器。如果無法建立連線，Kaspersky Endpoint Security 將嘗試連線到清單中的第二個 IP 位址，依此類推。

11. 如果有需要的話，配置遙測。

12. 儲存變更。

結果，電腦會被新增到 Kaspersky Anti Targeted Attack Platform 主控台上。透過檢視”*應用程式元件狀態報告*”來檢查元件的運行狀態。您還可以在 Kaspersky Endpoint Security 的本地介面中的報告中檢視元件的運行狀態。“**Network Detection and Response (KATA)**”元件將新增到 Kaspersky Endpoint Security 元件清單中。

# EDR Agent 與 EDR Expert (on-premise) 整合

EDR Agent 安裝在組織 IT 基礎結構中的工作站和伺服器上。在這些電腦上，EDR Agent 持續監視處理程序、開啟的網路連線和正在修改的檔案，並將監視資料傳送到 EDR Expert (on-premise) 伺服器。

要與 EDR Expert (on-premise) 整合，您必須啟用 Endpoint Detection and Response Expert (on-premise) 元件並配置 EDR Agent。

與 Endpoint Detection and Response Expert (on-premise) 整合涉及以下步驟：

1. **啟動 Kaspersky Endpoint Detection and Response Expert (on-premise)**

您需要單獨購買 EDR Expert (on-premise)（Kaspersky Endpoint Detection and Response Expert (on-premise) 附加元件）的產品授權。

為 Kaspersky Endpoint Detection and Response Expert (on-premise) 新增單獨的金鑰後，該功能將可用。獨立 Endpoint Detection and Response Expert (on-premise) 功能的授權和 Kaspersky Endpoint Security 的授權一樣。

確保 EDR Expert (on-premise) 功能包括在產品授權中且在應用程式的本機介面中執行。

2 **連線到遙測資料收集伺服器和回應伺服器**

Kaspersky Endpoint Detection and Response Expert (on-premise) 需要 Kaspersky Endpoint Security 與兩台伺服器之間建立可信任連線：

- *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。

要配置可信連線，您必須使用 TLS 憑證。您可以在開放式單一管理平台上取得 TLS 憑證（請參閱 Kaspersky Endpoint Detection and Response Expert （內部部署版）說明）。然後您必須將 TLS 憑證新增到 Kaspersky Endpoint Security（參見下面的說明）。

預設情況下，Kaspersky Endpoint Security 僅檢查伺服器 TLS 憑證。為了使連線更安全，您可以額外啟用在伺服器上進行電腦驗證（雙向身分驗證）。要啟用此驗證，您必須在伺服器和 Kaspersky Endpoint Security 設定中開啟雙向身分驗證。要使用雙向身分驗證，您還需要一個加密容器。*加密容器*是一個帶有憑證和私鑰的 PFX 存檔。您可以在開放式單一管理平台上取得加密容器（請參閱 Kaspersky Endpoint Detection and Response Expert （內部部署版）說明）。

**如何使用網頁主控台將 Kaspersky Endpoint Security 電腦連線到 EDR Expert (on-premise)**

1. 在網頁主控台的主視窗中，選擇**資產（裝置）** → **政策和設定檔**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 (on-premise)** ”。
5. 開啟“**Endpoint Detection and Response Expert (on-premise) 已啟用**“開關。
6. 若要設定 EDR Expert (on-premise)，請從解決方案清單中選取 **Endpoint Detection and Response Expert（版本 8.0 或者更高版本）**。
7. 配置 *遙測資料收集伺服器* 連線：
   a. 在”**遙測資料收集伺服器連線**”塊中，點擊”**連線設定**”連接。
   b. 配置遙測資料收集伺服器連線：
      - **逾時（秒）**伺服器回應最長逾時。當逾時用完時，Kaspersky Endpoint Security 會嘗試連線到不同的伺服器。
      - **伺服器憑證**用於與伺服器建立可信連線的 TLS 憑證。您可以在開放式單一管理平台上取得 TLS 憑證（請參閱 Kaspersky Endpoint Detection and Response Expert （內部部署版）說明）。

- **使用雙向身分驗證**在 Kaspersky Endpoint Security 和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。您可以在開放式單一管理平台上取得加密容器（請參閱 Kaspersky Endpoint Detection and Response Expert （內部部署版）說明）。配置伺服器設定後，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。

c. 點擊**"確定"**。

d. 新增遙測資料收集伺服器。為此，請指定伺服器位址（IPv4、IPv6）和連線到伺服器的連接埠。

您可以新增多個遙測資料收集伺服器位址。Kaspersky Endpoint Security 嘗試連線到第一個 IP 位址的伺服器。如果無法建立連線，Kaspersky Endpoint Security 將嘗試連線到清單中的第二個 IP 位址，依此類推。

e. 如果有需要的話，配置遙測。

8. 配置*回應伺服器*連線：

a. 在**"連線至回應伺服器"**區塊中，配置**傳送同步請求到伺服器的時間間隔 (分)**設定。傳送到伺服器的同步請求的頻率。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。

b. 點擊**"連線設定"**連接。

c. 配置回應伺服器連線：

- **逾時（秒）**伺服器回應最長逾時。當逾時用完時，Kaspersky Endpoint Security 會嘗試連線到不同的伺服器。
- **伺服器憑證**用於與伺服器建立可信連線的 TLS 憑證。您可以在開放式單一管理平台上取得 TLS 憑證（請參閱 Kaspersky Endpoint Detection and Response Expert （內部部署版）說明）。
- **使用雙向身分驗證**在 Kaspersky Endpoint Security 和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。您可以在開放式單一管理平台上取得加密容器（請參閱 Kaspersky Endpoint Detection and Response Expert （內部部署版）說明）。配置伺服器設定後，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。

d. 點擊**"確定"**。

e. 新增回應伺服器。為此，請指定伺服器位址（IPv4、IPv6）和連線到伺服器的連接埠。

您可以新增多個回應伺服器位址。Kaspersky Endpoint Security 嘗試連線到第一個 IP 位址的伺服器。如果無法建立連線，Kaspersky Endpoint Security 將嘗試連線到清單中的第二個 IP 位址，依此類推。

9. 儲存變更。若要在電腦上套用該政策，請關閉掛鎖。

因此，電腦被加入到開放單一管理平台（OSMP）中。透過檢視"*應用程式元件狀態報告*"來檢查元件的運行狀態。您還可以在 Kaspersky Endpoint Security 的本地介面中的報告中檢視元件的運行狀態。"**Endpoint Detection and Response Expert (on-premise)** "元件將新增到 Kaspersky Endpoint Security 元件清單中。

# 與協力廠商 EPP 應用程式的相容性

EDR Agent 支援 Kaspersky Detection and Response 解決方案的功能。防護和控制元件不可用於 EDR Agent。此配置允許安裝協力廠商 EPP 應用程式並在組織的基礎結構中部署 Kaspersky Detection and Response 解決方案。EDR Agent 支援使用 Kaspersky Managed Detection and Response、Kaspersky Anti Targeted Attack Platform (EDR) 和 Kaspersky Anti Targeted Attack Platform (NDR)。

EDR Agent 與以下供應商的 EPP 應用程式相容：

- **Dr.Web**

  EDR Agent 與 Dr.Web for Windows 13.0.1 或更高版本及 Dr.Web 伺服器 (x64) 13.0.0.10200 相容。

- **Dallas Lock**

  EDR Agent 與 Dallas Lock 8.0-C 版本 11.4.2.843 或更高版本相容。

  要使 EDR Agent 在安裝了 Dallas Lock 軟體的電腦上執行，您必須在防火牆模組的設定中允許連線到卡巴斯基外部服務。

- **Secret Net Studio**

  EDR Agent 與 Secret Net Studio 版本 8.11 或更高版本相容。

  應用程式無法安裝在使用病毒防護元件部署了 Secret Net Studio 的電腦上。若要允許交互操作，您必須從 Secret Net Studio 中刪除病毒防護元件。

- **Trend Micro**

  EDR Agent 與 Trend Micro Apex One 版本 14.0.12994 或更高版本（包括 Security Agent）相容。

  EDR Agent 與 Trend Micro Deep Security 版本 20.0.2-4960 或更高版本（包括 Security Agent）相容。

- **Windows Defender**

- **Sophos**

  EDR Agent 與 Sophos Intercept X 版本 2024.1.2 或更高版本（包括 Endpoint Agent）和 Sophos Core Agent 版本 2024.3.2.3 相容。

- **Bitdefender**

  EDR Agent 與 Bitdefender Endpoint Security Tools 版本 7.9.21.523 或更高版本相容。

- **ESET**

  EDR Agent 與 ESET Endpoint Security 版本 12.0.2049.0 或更高版本以及 ESET Management Agent 版本 12.0 或更高版本相容。

必須按以下順序安裝應用程式：首先安裝 EPP 應用程式，然後安裝卡巴斯基安全管理中心網路代理，最後安裝 EDR Agent。必需這樣，因為 EPP 應用程式的安裝程式可能會將 EDR Agent 和網絡代理偵測為不相容的軟體並將其刪除。更新協力廠商 EPP 應用程式後，還應檢查 EDR Agent 和網路代理的運行情況，因為其安裝程式可能會重新掃描電腦中是否有不相容的軟體並刪除這些應用程式。

如果由於安裝程式在電腦上發現不相容的軟體而無法在具有協力廠商 EPP 應用程式的電腦上安裝 EDR Agent，您可以跳過不相容軟體檢查。

# Managed Detection and Response



Kaspersky Endpoint Security for Windows 支援與 Managed Detection and Response 解決方案整合。*Kaspersky Managed Detection and Response (MDR)* 解決方案可自動偵測和分析您的基礎架構中的安全事件。為此，MDR 會使用從端點和機學習收到的遙測資料。MDR 會將事件資料傳送給卡巴斯基專家。專家然後可以處理事件，並且，例如，新增新項目至病毒資料庫。或者，專家可以簽發事件處理建議，並且，例如，建議從網路中隔離電腦。如欲瞭解該解決方案如何工作的詳細資訊，請參閱 Kaspersky Managed Detection and Response 說明。

## 配置 Kaspersky Endpoint Security 以與 MDR 整合

以下配置可用於使用 MDR：

- **[KES+內建代理]**。在此配置中，Kaspersky Endpoint Security 既充當確保電腦安全的應用程式，又充當使用 MDR 的應用程式。Kaspersky Endpoint Security 11.6.0 for Windows 或更高版本提供內建代理。

- **【協力廠商 EPP EDR Agent】**。在此配置中，IT 基礎結構的安全性由協力廠商 Endpoint Protection Platform (EPP) 提供。與 MDR 的交互由 Kaspersky Endpoint Security 在 Endpoint Detection and Response Agent (EDR Agent) 配置中提供。在此配置中，EDR Agent 與協力廠商 EPP應用程式相容。EDR Agent 在 Kaspersky Endpoint Security 12.3 for Windows 或更高版本中可用。

## 對以前版本的 Kaspersky Endpoint Security 的支援

Kaspersky Endpoint Security 版本11和更高版本支援 MDR 解決方案。Kaspersky Endpoint Security 版本 11 – 11.5.0 僅傳送遙測資料到 Kaspersky Managed Detection and Response 以啟用威脅偵測。Kaspersky Endpoint Security 版本 11.6.0 有內建代理 (Kaspersky Endpoint Agent) 的所有功能。

如果您使用的是 Kaspersky Endpoint Security 11 – 11.5.0，則必須將資料庫更新到最新版本才能使用 MDR 解決方案。您還必須安裝 Kaspersky Endpoint Agent。

如果您正在使用 Kaspersky Endpoint Security 11.6.0 或者更高版本，則不需要安裝 Kaspersky Endpoint Agent 以使用 MDR 解決方案。

如果 Kaspersky Endpoint Security 政策也套用到沒有安裝 Kaspersky Endpoint Security 11 – 11.5.0 的電腦，則您必須為這些電腦單獨建立 Kaspersky Endpoint Agent 政策。在新政策中，設定與 Kaspersky Managed Detection and Response 的整合。

# 內建代理與 MDR 整合

要設定與 Kaspersky Managed Detection and Response 的整合，您必須啟用 Managed Detection and Response 元件並配置 Kaspersky Endpoint Security。

若要透過卡巴斯基安全管理中心網頁主控台讓 Kaspersky Managed Detection and Response 和管理伺服器一起工作，您必須建立一個新的安全連線，一個*背景連線*。Kaspersky Managed Detection and Response 提示您在部署解決方案時建立一個背景連線。確保背景連線已建立。

**在網頁主控台中建立一個背景連線**

1. 在網頁主控台的主視窗中，選擇**設定 → 整合**。
2. 轉到"**整合**"區域。
3. 開啟"**整合的背景連線 已啟用**"開關。
4. 儲存變更。

與 Kaspersky Managed Detection and Response 整合包括以下步驟：

1. **安裝 Managed Detection and Response 元件**

   您可以在安裝或者升級期間以及使用*變更應用程式元件*工作時選擇 MDR 元件。

   您必須重新啟動電腦以完成升級含新元件的應用程式。

2. **配置卡巴斯基私有安全網路**

   如果您使用的是卡巴斯基安全管理中心雲端主控台，略過這一步。卡巴斯基安全管理中心雲端主控台會在安裝 MDR 外挂程式時自動配置卡巴斯基私有安全網路。

   *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。

   在管理伺服器屬性中上傳卡巴斯基安全網路設定檔。卡巴斯基安全網路設定檔位於 MDR 設定檔的 ZIP 存檔中。您可以在 Kaspersky Managed Detection and Response 主控台中獲取 ZIP 存檔。有關配置卡巴斯基私有安全網路的詳細資訊，請參閱 卡巴斯基安全管理中心說明。您也可以從命令行將卡巴斯基安全網路設定檔上傳到電腦（請參閱以下說明）。

**如何從命令行配置卡巴斯基私有安全網路**

1. 以管理員身分執行命令列解譯器 (cmd.exe)。
2. 轉到 Kaspersky Endpoint Security 可執行檔所在資料夾。
3. 執行以下指令：

   ```
   avp.com KSN /private <file name>
   ```

   其中`<file name>`是包含私有卡巴斯基私有安全網路設定（PKCS7 或 PEM 檔案格式）的設定檔的名稱。

   範例:
   ```
   avp.com KSN /private C:\kpsn_config.pkcs7
   ```

結果，Kaspersky Endpoint Security 將使用私有卡巴斯基私有安全網路來確定檔案、應用程式和網站的信譽。政策設定的**卡巴斯基安全網路**部分將顯示以下運行狀態：*基礎結構: 卡巴斯基私有安全網路*。

您必須啟用延伸 KSN 模式才能使 Managed Detection and Response 正常工作。

### 3 啟動 Kaspersky Managed Detection and Response

從 Kaspersky Endpoint Security for Windows 12.10 開始，若要啟動 Managed Detection and Response 功能，作為 啟動碼的替代方式，您也可以使用 金鑰檔案。

Kaspersky Managed Detection and Response 支援以下授權方法：

- Managed Detection and Response 功能包括在 Kaspersky Endpoint Security for Windows 產品授權中。

  這些功能將在啟動 Kaspersky Endpoint Security for Windows 後立即可用。

- 對 MDR (Kaspersky Managed Detection and Response Add-on) 將使用一個單獨的產品授權。

  為 Kaspersky Managed Detection and Response 附加元件新增單獨的金鑰後，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 Managed Detection and Response。

  獨立 Managed Detection and Response 功能的授權和 Kaspersky Endpoint Security 的授權一樣。

確保 MDR 功能包括在產品授權中且在應用程式的本機介面中工作。

### 4 啟用 Managed Detection and Response 元件

在 Kaspersky Endpoint Security 政策中加載 BLOB 設定檔（請參閱以下說明）。BLOB 檔案包含用戶端 ID 以及有關卡巴斯基 Managed Detection and Response 產品許可的資訊。BLOB 檔案位於 MDR 設定檔的 ZIP 存檔中。您可以在 Kaspersky Managed Detection and Response 主控台中獲取 ZIP 存檔。有關 BLOB 檔案的詳細資訊，請參閱 Kaspersky Managed Detection and Response 說明。

從 Kaspersky Endpoint Security 12.6 for Windows 開始，如果您擁有目前產品授權，則對於沒有租戶的 Kaspersky Managed Detection and Response 來說，新增 BLOB 檔案可選。

**如何在管理主控台 (MMC) 中啟用 Managed Detection and Response 元件**

1. 在卡巴斯基安全管理中心管理主控台樹狀目錄中，選取**政策**。
2. 選擇必要的政策並點擊以開啟政策內容。

3. 在政策視窗中，選擇“**Detection and Response → Managed Detection and Response (Industrial CyberSecurity)**”。

4. 選擇“**Managed Detection and Response (Industrial CyberSecurity)**”核取方塊。

5. 在“**設定**“塊中，點擊“**上傳**”，然後選擇在 Kaspersky Managed Detection and Response Console 中接收到的 BLOB 檔案。該檔案具有 P7 副檔名。

   預設情況下，允許使用者管理應用程式設定（“掛鎖”開啟）。若要在電腦上套用該政策，請關閉掛鎖。

6. 儲存變更。

**如何在網頁主控台和雲端主控台中啟用 Managed Detection and Response 元件**

1. 在網頁主控台的主視窗中，選擇**資產（裝置）→ 政策和設定檔**。

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**”→”**Managed Detection and Response**”。

5. 開啟“**已啟用 Managed Detection and Response**“開關。

6. 點擊“**上傳**”，然後選擇在 Kaspersky Managed Detection and Response 主控台中獲取的 BLOB 檔案。該檔案具有 P7 副檔名。

   預設情況下，允許使用者管理政策設定（“掛鎖”開啟）。若要在電腦上套用該政策，請關閉掛鎖。

7. 儲存變更。

**如何從命令行啟用 Managed Detection and Response 元件**

1. 以管理員身分執行命令列解譯器 (cmd.exe)。

2. 轉到 Kaspersky Endpoint Security 可執行檔所在資料夾。

3. 執行以下指令：

   ```
   avp.com MDRLICENSE /ADD <file name> /login=<user name> /password=<password>
   ```

   要執行此指令，必須啟用密碼防護。使用者必須具有“**配置應用程式設定**”權限。

結果，Kaspersky Endpoint Security 將驗證 BLOB 檔案。BLOB 檔案驗證包括檢查數位簽章和產品授權期限。如果 BLOB 檔案驗證成功，在與卡巴斯基安全管理中心進行下一次同步時，Kaspersky Endpoint Security 將下載該檔案並將其傳送到電腦。透過檢視”*應用程式元件狀態報告*”來檢查元件的運行狀態。您還可以在 Kaspersky Endpoint Security 的本地介面中的報告中檢視元件的運行狀態。“**Managed Detection and Response**”元件將新增到 Kaspersky Endpoint Security 元件清單中。

**5 配置應用程式的其他元件以接收遙測資料**

您必須啟用延伸以下元件才能使 Managed Detection and Response 正常工作：

- 卡巴斯基安全網路（延伸模式）。

  當透過 Kerberos 身分驗證使用代理伺服器時，建議使用 KSN Proxy 和 HTTPS 傳輸協定。請參閱 卡巴斯基安全管理中心說明 瞭解更多詳情。

- 行為偵測。

必須啟用這些元件。否則，因為沒有收到所需的遙測資料，Kaspersky Managed Detection and Response 將無法工作。

此外，Kaspersky Managed Detection and Response 使用從其他應用程式元件收到的資料。可選擇啟用這些元件。提供其他資料的元件包括：

- Web 威脅防護。
- 郵件威脅防護。
- 防火牆。

1. 在網頁主控台的主視窗中，選擇**資產（裝置）→ 政策和設定檔**。
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**"→"**Managed Detection and Response**"。
5. 開啟"**已啟用 Managed Detection and Response**"開關。
6. 儲存變更。

1. 在卡巴斯基安全管理中心管理主控台樹狀目錄中，選取**政策**。
2. 選擇必要的政策並點擊以開啟政策內容。
3. 在政策視窗中，選擇"**Detection and Response → Managed Detection and Response (Industrial CyberSecurity)**"。
4. 選擇"**Managed Detection and Response (Industrial CyberSecurity)**"核取方塊。
5. 儲存變更。

# MDR 的 KEA 到 KES 遷移指南

Kaspersky Endpoint Security for Windows 包括用於 Kaspersky Managed Detection and Response 應解決方案的內置代理。您再也無需分開 Kaspersky Endpoint Agent 應用程式來使用 MDR。Kaspersky Endpoint Agent 的所有功能將由 Kaspersky Endpoint Security 執行。

當您在安裝了 Kaspersky Endpoint Agent 的電腦上部署 Kaspersky Endpoint Security 時，Kaspersky Managed Detection and Response 解決方案將繼續與 Kaspersky Endpoint Security 一起工作。此外，Kaspersky Endpoint Agent 將被從電腦移除。當您將 Kaspersky Endpoint Security 更新到版本 11.6.0 或更高版本時，系統中會發生相同的行為。

Kaspersky Endpoint Security 與 Kaspersky Endpoint Agent 不相容。您不能在同一台電腦上同時安裝這些應用程式。

Kaspersky Endpoint Security 必須滿足以下條件才能作為 Kaspersky Managed Detection and Response 的一部分工作：

- 卡巴斯基安全管理中心版本 13.2 或更高版本（包括網路代理）。在早期版本的卡巴斯基安全管理中心中，無法啟動 Managed Detection and Response 功能。
- 已建立在卡巴斯基安全管理中心網頁主控台和管理伺服器之間的背景連線。若要透過卡巴斯基安全管理中心網頁主控台讓 MDR 和管理伺服器一起工作，您必須建立一個新的安全連線，一個*背景連線*。

將 [KES+KEA] 配置遷移到 [KES+built-in agent] for MDR 的步驟

1. **升級 Kaspersky Endpoint Security 管理外掛程式**

   MDR 元件可以使用 Kaspersky Endpoint Security 管理外掛程式版本 11.6 或更高版本進行管理。根據您使用的卡巴斯基安全管理中心主控台類型，更新管理主控台 (MMC) 中的管理外掛程式或網頁主控台中的 Web 外掛程式。

2. **遷移政策和工作**

   將 Kaspersky Endpoint Agent 設定傳輸到 Kaspersky Endpoint Security for Windows。下列選項可用：

   - 用於從 Kaspersky Endpoint Agent 遷移到 Kaspersky Endpoint Security 的精靈。從 Kaspersky Endpoint Agent 遷移到 Kaspersky Endpoint Security 的精靈僅適用於網頁主控台

     **如何將政策和工作設定從 Kaspersky Endpoint Agent 遷移到網頁主控台中的 Kaspersky Endpoint Security**

     在網頁主控台的主視窗中，選擇**操作 → 從 Kaspersky Endpoint Agent 遷移**。

     這會執行政策和工作遷移精靈。按照精靈的說明進行操作。

     步驟 1. 政策遷移

     遷移精靈會建立一個新政策，將 Kaspersky Endpoint Security 和 Kaspersky Endpoint Agent 政策的設定合併。在政策清單中，選擇您想將其設定與 Kaspersky Endpoint Security 政策合併的 Kaspersky Endpoint Agent 政策。點擊 Kaspersky Endpoint Agent 政策以選擇您想與其合併設定的 Kaspersky Endpoint Security 政策。確保選擇了正確的政策然後前往下一步。

     步驟 2. 工作遷移

     遷移精靈不支援 MDR 工作。略過此步驟。

步驟 3. 精靈完成

結束精靈。作為精靈的結果，將建立新的 Kaspersky Endpoint Security 政策。政策將合併 Kaspersky Endpoint Security 和 Kaspersky Endpoint Agent 的設定。政策稱為 *<Kaspersky Endpoint Security 政策名稱> & <Kaspersky Endpoint Agent 政策名稱>*。新政策的狀態為*非作用中*。若要繼續，將 Kaspersky Endpoint Agent 和 Kaspersky Endpoint Security 政策的狀態變更為*非作用中*，然後啟動新合併的政策。

- 標準政策和工作批量轉換精靈。政策和工作批量轉換精靈僅在管理主控台 (MMC) 中可用。有關政策和工作批量轉換精靈的詳細資訊，請參閱卡巴斯基安全管理中心說明。

**3 授權 MDR 功能**

要將 Kaspersky Endpoint Security 作為 Kaspersky Managed Detection and Response 解決方案的一部分啟動，您需要單獨的 Kaspersky Managed Detection and Response 附加產品授權。您可以使用"*新增金鑰*"工作新增金鑰。結果，兩個金鑰將被新增到應用程式：*Kaspersky Endpoint Security* 和 *Kaspersky Managed Detection and Response*。

**4 安裝/升級 Kaspersky Endpoint Security 應用程式**

要在應用程式安裝或升級期間遷移 MDR 功能，建議使用遠端安裝工作。建立遠端安裝工作時，您需要在安裝套件設定中選擇 MDR 元件。

您還可以使用以下方法升級應用程式：

- 使用 Kaspersky 更新服務。
- 本機使用安裝精靈。

當在安裝了 Kaspersky Endpoint Agent 的電腦上升級應用程式時，Kaspersky Endpoint Security 支援自動選擇元件。自動選擇元件取決於升級應用程式的使用者帳戶的權限。

如果在系統帳戶 (SYSTEM) 下使用 EXE 或 MSI 檔案升級 Kaspersky Endpoint Security，Kaspersky Endpoint Security 將獲得對 Kaspersky 解決方案的目前產品授權的存取權限。因此，如果電腦安裝了 Kaspersky Endpoint Agent 且啟動了 MDR 解決方案，Kaspersky Endpoint Security 安裝程式將自動配置元件集合並選擇 MDR 元件。這將使得 Kaspersky Endpoint Security 切換到使用內建代理並刪除 Kaspersky Endpoint Agent。在系統帳戶 (SYSTEM) 下執行 MSI 安裝程式通常在透過 Kaspersky 更新服務升級或透過卡巴斯基安全管理中心部署安裝套件時進行。

如果在沒有權限的帳戶下使用 MSI 檔案升級 Kaspersky Endpoint Security，Kaspersky Endpoint Security 將缺少對 Kaspersky 解決方案的目前產品授權的存取權限。在這種情況下，Kaspersky Endpoint Security 會根據 Kaspersky Endpoint Agent 的一組元件自動選擇元件。此後，Kaspersky Endpoint Security 將切換到使用內建代理並刪除 Kaspersky Endpoint Agent。

Kaspersky Endpoint Security 支援在不重啟電腦的情況下升級。您可以選擇政策屬性中的應用程式升級模式。

**5 檢查應用程式運行情況**

如果安裝或升級後應用程式後電腦在卡巴斯基安全管理中心主控台中具有"*緊急*"狀態：

- 請確保電腦安裝了網路代理 13.2或更高版本。
- 透過檢視"*應用程式元件狀態報告*"來檢查內建代理的運行狀態。如果元件的狀態為"*未安裝*"，請使用*變更應用程式元件*工作來安裝元件。如果一個元件的狀態為 *產品授權不支援*，確保您已啟動內建代理功能。
- 請確保在 Kaspersky Endpoint Security for Windows 的新政策中接受卡巴斯基安全網路聲明。

# Endpoint Detection and Response

Kaspersky Endpoint Security for Windows 包括 Kaspersky Endpoint Detection and Response Optimum 解決方案（以下也稱為 "EDR Optimum"）的內建代理。從版本 11.8.0 開始，Kaspersky Endpoint Security for Windows 包括 Kaspersky Endpoint Detection and Response 解決方案（以下也稱為 "EDR Expert"）的內建代理。*Kaspersky Endpoint Detection and Response* 是用於防護組織的 IT 基礎架構抵禦進階網路威脅的一系列解決方案。解決方案的功能結合了自動偵測威脅和回應這些威脅的能力，以抵消包括新漏洞、勒索軟體、無檔案攻擊以及使用合法系統工具的方法。EDR Expert 比 EDR Optimum 提供更多的威脅監控和回應功能。有關解決方案的詳細資訊，請參閱 Kaspersky Endpoint Detection and Response Optimum 說明 與 Kaspersky Endpoint Detection and Response Expert 說明。

## 威脅情報工具

Kaspersky Endpoint Detection and Response 使用以下威脅情報工具：

- 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。
- Cloud Sandbox 技術，可讓您在隔離環境中執行偵測的檔案並檢查其聲譽。

## 解決方案的工作原理

Kaspersky Endpoint Detection and Response 會審查和分析威脅發展並向*安全人員*或者*管理員*提供有關需要作出及時回應的潛在攻擊的資訊。Kaspersky Endpoint Detection and Response 會在單獨視窗中顯示偵測詳情。*警示*是企業 IT 基礎架構中的事件，應用程式已將其識別為異常或可疑，可能對企業 IT 基礎架構構成安全威脅。*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。

## 對以前版本的 Kaspersky Endpoint Security 的支援

如果您使用 Kaspersky Endpoint Security 11.2.0–11.6.0 與 Kaspersky Endpoint Detection and Response Optimum 進行交互操作，應用程式將包括 Kaspersky Endpoint Agent。您可以在安裝 Kaspersky Endpoint Security 的過程中安裝 Kaspersky Endpoint Agent。在 Kaspersky Endpoint Security 11.9.0 中，Kaspersky Endpoint Agent 分發套件不再是 Kaspersky Endpoint Security 分發套件的一部分。

Kaspersky Endpoint Detection and Response Expert 解決方案不支援與 Kaspersky Endpoint Agent 的交互操作性。Kaspersky Endpoint Detection and Response Expert 解決方案用內建代理（版本 11.8.0 和以後的版本）使用 Kaspersky Endpoint Security。

# 內建代理與 EDR Optimum / EDR Expert 整合

若要與 Kaspersky Endpoint Detection and Response 進行整合，您必須新增 Endpoint Detection and Response Optimum (EDR Optimum) 元件或者 Endpoint Detection and Response Expert (EDR Expert) 元件，並設定 Kaspersky Endpoint Security。

EDR Optimum、EDR Expert 和 EDR (KATA) 元件彼此不相容。

Endpoint Detection and Response 要工作必須滿足以下條件：

- 卡巴斯基安全管理中心版本 13.2 或更高版本。在早期版本的卡巴斯基安全管理中心中，無法啟動 Endpoint Detection and Response 功能。
- Kaspersky Endpoint Detection and Response 管理外掛程式。

  從 Kaspersky Endpoint Security 版本 12.6 開始，警示詳細資訊顯示已從 Kaspersky Endpoint Security 管理外掛程式移至 EDR 管理外掛程式。EDR 管理外掛程式是一個單一外掛程式，可與 Windows、Mac 和 Linux 作業系統上的代理程式一起使用。現在，當使用 EDR Optimum 時，您將需要 Kaspersky Endpoint Security 管理外掛程式來建立威脅回應工作，並需要 EDR 管理外掛程式來檢視警示詳細資訊。
- EDR Optimum 元件作為 Kaspersky Endpoint Security 的一部分支援與 Kaspersky Endpoint Detection and Response Optimum 2.0 解決方案的交互。不支援與 Kaspersky Endpoint Detection and Response Optimum version 1.0 的交互。
- EDR Optimum 可在卡巴斯基安全管理中心網頁主控台或卡巴斯基安全管理中心雲端主控台中進行管理。

  EDR Expert 功能只可以使用卡巴斯基安全管理中心雲端主控台進行管理。您不能使用管理主控台 (MMC) 管理此功能。
- 應用程式被啟動，功能受產品授權覆蓋。
- Endpoint Detection and Response 元件已開啟。
- Endpoint Detection and Response 依靠的應用程式元件已啟用且可操作。Endpoint Detection and Response 依靠以下元件：
  - 檔案威脅防護。
  - Web 威脅防護。
  - 郵件威脅防護。
  - 弱點利用防禦。
  - 行為偵測。
  - 主機入侵防禦。
  - 修復引擎。
  - 適應性異常控制。

與 Kaspersky Endpoint Detection and Response 涉及以下步驟：

1. **安裝 Endpoint Detection and Response 元件**

   您可以在安裝或者更新期間以及使用*變更應用程式元件*工作時選擇 EDR Optimum 或 EDR Expert 元件。

   > 您必須重新啟動電腦以完成升級含新元件的應用程式。

2. **啟動 Kaspersky Endpoint Detection and Response**

   您可以用以下方式之一獲取使用 Kaspersky Endpoint Detection and Response 的產品授權：

   - Endpoint Detection and Response 功能包括在 Kaspersky Endpoint Security for Windows 產品授權中。

     這些功能將在啟動 Kaspersky Endpoint Security for Windows 後立即可用。

   - 單獨購買 EDR Optimum 或 EDR Expert（Kaspersky Endpoint Detection and Response 附加元件）的產品授權。

     為 Kaspersky Endpoint Detection and Response 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。

     獨立 Endpoint Detection and Response 功能的授權和 Kaspersky Endpoint Security 的授權一樣。

   確保 EDR Optimum 或 EDR Expert 功能包括在產品授權中且在應用程式的本機介面中執行。

   有關 EDR Optimum 最終使用者產品授權協議的更多資訊，請參見Kaspersky Endpoint Detection and Response Optimum 說明。

3. **啟用 Endpoint Detection and Response 元件**

   您可以在 Kaspersky Endpoint Security for Windows 政策設定中啟用或者停用該元件。

   **如何在網頁主控台和雲端主控台中啟用或停用 Endpoint Detection and Response 元件**

   1. 在網頁主控台的主視窗中，選擇**資產（裝置）→政策和設定檔**。
   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. 開啟**"Endpoint Detection and Response 已啟用"**開關。
   6. 儲存變更。

   Kaspersky Endpoint Detection and Response 元件已啟用。透過檢視*"應用程式元件狀態報告"*來檢查元件的運行狀態。您還可以在 Kaspersky Endpoint Security 的本地介面中的報告中檢視元件的運行狀態。**"Endpoint Detection and Response Optimum"**或**"Endpoint Detection and Response Expert"**元件已新增到 Kaspersky Endpoint Security 元件清單中。

4. **啟用到管理伺服器的資料傳輸**

若要啟用所有 Endpoint Detection and Response 功能，必須為以下類型的資料啟用傳輸：

- 隔離檔案資料。

  透過網頁主控台和雲端主控台獲取電腦上的隔離檔案資訊需要該資料。例如，您可以從隔離區下載檔案用於在網頁主控台和雲端主控台中分析。

- 威脅發展鏈資料。

  在網頁主控台和雲端主控台中獲取電腦上偵測到的威脅資訊需要該資料。您可以在網頁主控台和雲端主控台中檢視偵測詳細資訊並採取回應動作。

**如何在網頁主控台和雲端主控台中啟用資料傳輸到管理伺服器**

1. 在網頁主控台的主視窗中，選擇**資產（裝置）→政策和設定檔**。
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**到管理伺服器的資料傳輸**下面，選擇以下核取方塊：
   - **關於隔離檔案**
   - **關於威脅發展鏈條**
6. 儲存變更。

# 掃描洩露指示器（標準工作）

*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，許多登入系統的不成功嘗試可以構成一個洩露指示器。"*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。

Kaspersky Endpoint Security 可使用 IOC 檔案搜尋洩露指示器。*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。

## IOC 掃描 工作執行模式

Kaspersky Endpoint Detection and Response 可讓您建立標準 IOC 掃描工作以偵測洩露的資料。"*標準 IOC 掃描工作*"是一個在網頁主控台中手動建立和配置的群組或本機工作。工作使用使用者準備的 IOC 檔案執行。如果您想要手動新增洩露指示器，請閱讀 IOC 檔案要求。

您可以點擊下面的連接下載該檔案，它包含一個表格，其中有 OpenIOC 標準的 IOC 字詞完整清單。

**下載 IOC_TERMS.XLSX 檔案**

當應用程式被用作 Kaspersky Sandbox 解決方案的一部分時，Kaspersky Endpoint Security 也支援獨立的 IOC 掃描工作。

建立 IOC 檔案

從 Kaspersky Endpoint Security 12.10 for Windows 開始，您可以直接在工作設定中建立 IOC 檔案。要建立 IOC 檔案，您必須準備一個包含入侵指標清單的 TXT 檔案。您可以新增以下物件的清單作為入侵指標：

- 檔案雜湊（MD5/SHA256）。
  應用程式會準備一個掃描範圍為 FileItem/Md5sum 或者 FileItem/Sha256sum 的 IOC 檔案。
- IP 位址（IPv4、IPv6）。
  應用程式會準備一個掃描範圍為 PortItem/RemoteIP 的 IOC 檔案。
- DNS 名稱。
  應用程式會準備一個掃描範圍為 DnsEntryItem/RecordName 的 IOC 檔案。

**如何在網頁主控台中建立 IOC 檔案**

1. 在網頁主控台的主視窗中，選擇**資產（裝置）→工作**。
   工作清單開啟。
2. 選擇 **IOC 掃描** 工作。
   工作內容視窗將開啟。需要的話建立 **IOC 掃描** 工作。
3. 選擇**"應用程式設定"**標籤。
4. 轉到**"IOC 掃描設定"**區域。
5. 點擊**"重新定義 IOC 檔案"**。
6. 這將開啟用於建立 IOC 檔案的表單：
   a. 在**IOC 檔案來源**下面，選擇**產生自檔案**。
   b. 輸入 IOC 檔案名稱。
   c. 選擇一個包含入侵指標清單的 TXT 檔案。
   d. 選擇 IOC 檔案的類型：**DNS 名稱**，**檔案雜湊**，**IP 位址**。
   e. 點擊**"建立"**。

   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。
7. 儲存變更。

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。

您可以在網頁主控台和雲端主控台中配置 EDR Optimum 的工作。適用於 EDR Expert 的工作設定僅在雲端主控台中可以使用。

*建立一個 IOC 掃描工作：*

1. 在網頁主控台的主視窗中，選擇**資產（裝置）→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 Windows 12.12.0"**。

   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。前往下一步。

5. 輸入您希望用其權限執行工作的使用者的帳戶認證。前往下一步。

   預設情況下，Kaspersky Endpoint Security 作為系統使用者帳戶 (SYSTEM) 啟動工作。

   系統帳戶 (SYSTEM) 沒有權限在網路磁碟機上執行"*IOC 掃描*"工作。如果您想要為網路磁碟機執行工作，請選擇有此磁碟機存取權限的使用者的帳戶。

   對於網路磁碟機上的獨立 IOC 掃描工作，您需要在工作內容中手動選擇則可以存取該磁碟機的使用者帳戶。

6. 結束精靈。

   在工作清單中將顯示一個新工作。

7. 點擊新工作。

   工作內容視窗將開啟。

8. 選擇"**應用程式設定**"標籤。

9. 轉到"**IOC 掃描設定**"區域。

10. 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。

    不建議在執行工作後新增或刪除 IOC 檔案。這可能會導致 IOC 掃描結果對於先前執行的工作顯示不正確。要根據新的 IOC 檔案搜尋洩露指示器，建議新增工作。

11. 如有必要，選中"**追溯 IOC 掃描**"核取方塊。*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。此模式旨在偵測電腦網路活動資料中的入侵指標。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）。

12. 配置偵測到 IOC 後的動作：

    - **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 Optimum 元件設定"中配置隔離時長。

      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 IOC，您可以直接從 IOC（*IOC 掃描* → **應用程式設定** → **IOC 掃描結果** 工作的屬性）將電腦與網路隔離。Kaspersky Endpoint Security 還允許立即管理其他設定：網路隔離停用期和網路隔離排除項目。

    - **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 會建立備份副本以防物件以後需要還原。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。

    - **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 會掃描內核記憶體、執行處理序和磁碟的開啟磁區。

13. 轉到"**進階**"區域。

14. 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。

您還可以為以下資料類型配置掃描範圍：

- **檔案 - FileItem**在使用預設範圍的電腦上設定 IOC 掃描範圍。

  預設情況下，Kaspersky Endpoint Security 僅掃描電腦中重要區域的 IOC，例如"下載"資料夾、桌面、具有臨時作業系統檔案的資料夾等等。您也可以手動新增掃描範圍。

- **Windows 事件記錄 - EventLogItem**輸入記錄事件的時間段。您也可以選擇必須使用哪些 Windows 事件記錄進行 IOC 掃描。預設選擇以下事件記錄：應用程式事件記錄，系統事件記錄，和安全事件記錄。

- **Windows 登錄檔 - RegistryItem**在登錄檔中設定 IOC 掃描範圍。

  預設 Kaspersky Endpoint Security 會掃描一個登錄機碼集合。

15. 在工作內容視窗中，選取"**排程**"標籤。

16. 設定工作排程。

    網路喚醒對於該工作不可用。確保電腦已開啟以執行工作。

17. 儲存變更。

18. 選中該工作旁邊的核取方塊。

19. 點擊"**開始**"。

因此，Kaspersky Endpoint Security 將執行搜尋電腦上的洩露指示器。您可以在工作內容的"**結果**"區域中檢視工作結果。您可以在工作內容中檢視偵測到的洩露指示器的有關資訊：**應用程式設定 → IOC 掃描結果**。在 IOC 掃描結果中，您也可以手動 隔離偵測到的檔案 或者 將電腦與網路隔離。

Kaspersky Endpoint Security 會在為同一個 IOC 檔案建立的記錄中尋找重複項，並在工作結果中僅保留唯一記錄。重複項指類型相同且所有比較欄位值都相同的記錄。如果一個或多個欄位缺少值，應用程式也可能不會建立記錄（請參閱下表）。

| 類型 | 比較欄位 | 不建立記錄的條件 |
| --- | --- | --- |
| FileItem | • FullPath<br>• Md5sum<br>• Sha256sum<br>• PID<br>• UPID<br>• ImagePath | • FullPath、Md5sum、Sha256sum欄位缺失的值。<br>• FullPath 欄位缺失的值和Md5sum、Sha256sum 欄位相同的值 。 |
| RegistryItem | • Hive<br>• KeyPath<br>• ValueName<br>• Text<br>• Type | 至少缺少以下欄位的值：Hive，KeyPath，ValueName。 |
| ProcessItem | • startTime<br>• PID | startTime 或者 PID 欄位缺失的值。 |

**提醒詳情** 視窗可能會顯示具有相同欄位值的 RegistryItem 記錄。這些記錄不是重複項，因為它們的文字欄位值不同，而這些值不會顯示在介面中。

IOC 掃描結果保留 30 天。在此期間之後，Kaspersky Endpoint Security 將自動移除最舊條目。

# IOC 掃描的延伸遙測

我們建議在電腦上啟用延伸遙測功能以進行回顧 IOC 掃描。延伸遙測技術可提高 IOC 偵測的準確性，但會佔用更多電腦資源。

延伸遙測包括支援以下附加術語：

- FileItem/Md5sum
- FileItem/Sha256sum
- FileItem/SizeInBytes
- FileItem/Created
- FileItem/Modified
- FileItem/Changed
- FileItem/Accessed
- FileItem/FileAttributes

如果停用延伸遙測功能，Kaspersky Endpoint Security 可能會輪換有關偵測到的入侵指標的資訊。

*啟用延伸遙測功能：*

1. 在網頁主控台的主視窗中，選擇**資產（裝置）→政策和設定檔**。
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"**啟用進階系統活動記錄**"核取方塊。
6. 儲存變更。

# 移動檔案到隔離

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。隔離檔案以加密狀態儲存，不會威脅裝置安全。Kaspersky Endpoint Security 僅在使用以下 Detection and Response 解決方案時使用隔離：EDR Optimum、EDR Expert、KATA (EDR)、Kaspersky Sandbox。在其他情況下，Kaspersky Endpoint Security 將相關檔案放置在備份中。若要瞭解將隔離作為解決方案的一部分進行管理的詳情，請參見Kaspersky Sandbox 說明、Kaspersky Endpoint Detection and Response Optimum 說明、Kaspersky Endpoint Detection and Response Expert 說明、Kaspersky Anti Targeted Attack Platform 說明。

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。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。

  您必須輸入檔案路徑或者雜湊（SHA256 或者 MD5），或者檔案路徑和檔案雜湊二者。

- 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。

“*移動檔案到隔離區*”工作有以下限制：

1. 檔案大小不得超過 100 MB。
2. 系統關鍵物件 (SCO) 無法被隔離。SCO 是作業系統和 Kaspersky Endpoint Security for Windows 應用程式要求能夠執行的檔案。
3. 您可以在網頁主控台和雲端主控台中配置 EDR Optimum 的工作。適用於 EDR Expert 的工作設定僅在雲端主控台中可以使用。
4. 您不能掃描因為*移動檔案到隔離區*工作被隔離的物件。

*建立一個 移動檔案到隔離區工作：*

1. 在網頁主控台的主視窗中，選擇**資產（裝置）→ 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 Windows 12.12.0**”。

   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. 輸入您希望用其權限執行工作的使用者的帳戶認證。點擊“**下一步**”。

預設情況下，Kaspersky Endpoint Security 作為系統使用者帳戶 (SYSTEM) 啟動工作。

6. 點擊**"完成"**按鈕結束精靈。

   在工作清單中將顯示一個新工作。

7. 點擊新工作。

   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，您必須輸入檔案的的完整路徑、或雜湊和路徑二者。

    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。

11. 在工作內容視窗中，選取**"排程"**標籤。

12. 設定工作排程。

    網路喚醒對於該工作不可用。確保電腦已開啟以執行工作。

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。為檔案建立終止處理程序然後重試。

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。清空隔離區或者擴大隔離區。然後再試。

您可以從隔離區還原檔案或者使用網頁主控台清空隔離區。您可以使用命令列在電腦上本機還原物件。.

# 獲取檔案

您可以從使用者的電腦獲取檔案。例如，您可以配置獲取由協力廠商應用程式建立的事件記錄檔案。因為執行工作，檔案被儲存在隔離區中。*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從隔離區下載此檔案到電腦（**操作 → 儲存 → 隔離區**）。在使用者的電腦上，檔案將保留在原始資料夾中。

檔案大小不得超過 100 MB。

您可以在網頁主控台和雲端主控台中配置 EDR Optimum 的工作。適用於 EDR Expert 的工作設定僅在雲端主控台中可以使用。

*建立一個 獲取檔案工作：*

1. 在網頁主控台的主視窗中，選擇**資產（裝置）→ 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 Windows 12.12.0"**。
   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. 輸入您希望用其權限執行工作的使用者的帳戶認證。點擊**"下一步"**。

   預設情況下，Kaspersky Endpoint Security 作為系統使用者帳戶 (SYSTEM) 啟動工作。

6. 點擊**"完成"**按鈕結束精靈。
   在工作清單中將顯示一個新工作。
7. 點擊新工作。
   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，您必須輸入檔案的的完整路徑、或雜湊和路徑二者。

    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。

11. 在工作內容視窗中，選取"**排程**"標籤。

12. 設定工作排程。

    網路喚醒對於該工作不可用。確保電腦已開啟以執行工作。

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。

# 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。

"*刪除檔案*"工作有以下限制：

- 系統關鍵物件 (SCO) 無法被刪除。SCO 是作業系統和 Kaspersky Endpoint Security 應用程式要求能夠執行的檔案。
- 您可以在網頁主控台和雲端主控台中配置 EDR Optimum 的工作。適用於 EDR Expert 的工作設定僅在雲端主控台中可以使用。

*建立一個 刪除檔案工作：*

1. 在網頁主控台的主視窗中，選擇**資產（裝置）→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 Windows 12.12.0**"。

   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. 輸入您希望用其權限執行工作的使用者的帳戶認證。點擊“**下一步**”。

   預設情況下，Kaspersky Endpoint Security 作為系統使用者帳戶 (SYSTEM) 啟動工作。

6. 點擊“**完成**”按鈕結束精靈。
   在工作清單中將顯示一個新工作。

7. 點擊新工作。
   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，您必須輸入檔案的的完整路徑、或雜湊和路徑二者。

    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。

11. 在工作內容視窗中，選取“**排程**”標籤。

12. 設定工作排程。

    網路喚醒對於該工作不可用。確保電腦已開啟以執行工作。

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。

如果您試圖刪除一個目前在執行的可執行檔，“*刪除檔案*”工作可能完成但有“*存取被拒絕*”錯誤。為檔案建立終止處理程序然後重試。

# 處理程序啟動

您可以使用“*啟動處理程序*”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*”工作接收在卡巴斯基安全管理中心網頁主控台中建立的檔案。

您可以在網頁主控台和雲端主控台中配置 EDR Optimum 的工作。適用於 EDR Expert 的工作設定僅在雲端主控台中可以使用。

*建立一個 啟動處理程序工作：*

1. 在網頁主控台的主視窗中，選擇**資產（裝置）→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 Windows 12.12.0**”。

   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. 輸入您希望用其權限執行工作的使用者的帳戶認證。點擊“**下一步**”。

   預設情況下，Kaspersky Endpoint Security 作為系統使用者帳戶 (SYSTEM) 啟動工作。

6. 點擊“**完成**”按鈕結束精靈。

   在工作清單中將顯示一個新工作。

7. 點擊新工作。

8. 工作內容視窗將開啟。

9. 選擇“**應用程式設定**”標籤。

10. 輸入處理程序啟動指令。

假設您想要執行一個公用程式(`utility.exe`)，將電腦配置資訊儲存到目前資料夾中一個名為 `conf.txt` 的檔案（預設）。該公用程式位於 `C:\Users\admin\Diagnostic\` 資料夾中。您必須將設定檔儲存在 `C:\Users\admin\Documents\Configuration` 資料夾中。輸入以下值：

- **可執行指令** – `C:\Users\admin\Diagnostic\utility.exe`
- **指令行參數(可選)** – `/R conf.txt`
- **工作資料夾路徑(可選)** – `C:\Users\admin\Documents\Configuration`

11. 在工作內容視窗中，選取"**排程**"標籤。
12. 設定工作排程。

    網路喚醒對於該工作不可用。確保電腦已開啟以執行工作。

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"*停止處理程序*"工作遠端終止處理程序。例如，您可以遠端終止一個使用"*執行處理程序*"工作啟動的網際網路速度測試公用程式。

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。

"*停止處理程序*"工作有以下限制：

- 系統關鍵物件 (SCO) 的處理程序無法被終止。SCO 是作業系統和 Kaspersky Endpoint Security 應用程式要求能夠執行的檔案。
- 您可以在網頁主控台和雲端主控台中配置 EDR Optimum 的工作。適用於 EDR Expert 的工作設定僅在雲端主控台中可以使用。

*建立一個 停止處理程序工作：*

1. 在網頁主控台的主視窗中，選擇**資產（裝置）→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 Windows 12.12.0**”。

   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. 輸入您希望用其權限執行工作的使用者的帳戶認證。點擊“**下一步**”。

   預設情況下，Kaspersky Endpoint Security 作為系統使用者帳戶 (SYSTEM) 啟動工作。

6. 點擊“**完成**”按鈕結束精靈。
   在工作清單中將顯示一個新工作。

7. 點擊新工作。
   工作內容視窗將開啟。

8. 選擇“**應用程式設定**”標籤。

9. 若要完成處理程序，您必須選擇想要終止的檔案。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。

    網路喚醒對於該工作不可用。確保電腦已開啟以執行工作。

12. 點擊“**儲存**”。

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。例如，如果 GAME 應用程式正在執行，而您終止了 game.exe 處理程序，應用程式將不儲存資料即關閉。您可以在工作內容的“**結果**”區域中檢視工作結果。

# 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。這樣的話，您可以（例如）防止執行您認為不安全的應用程式。因此，威脅擴散可以被停止。執行防護支援Office 檔案延伸程式集合和指令碼解譯器集合。

## 執行防護規則

執行防護使用執行防護規則管理使用者對檔案的存取。*執行防護規則*是應用程式對物件執行進行回應（例如，封鎖物件執行時）時考慮的一組條件。應用程式根據檔案路徑或者使用 MD5 和 SHA256 雜湊演算法計算的總和檢查碼來識別檔案。

您可以建立執行防護規則：

- 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。

- 使用群組政策或者本機應用程式設定。

  您必須輸入檔案路徑或者雜湊（SHA256 或者 MD5），或者檔案路徑和檔案雜湊二者。

您也可以使用命令列本機管理執行防護。

執行防止有以下限制：

1. 防護規則不覆蓋 CD 上或者 ISO 映像中的檔案。應用程式不會封鎖執行或者開啟這些規則。
2. 無法封鎖系統關鍵物件 (SCO) 的啟動。SCO 是作業系統和 Kaspersky Endpoint Security 應用程式要求能夠執行的檔案。
3. 不建議建立超過 5000 個執行防護規則，因為這可能造成系統不穩定。

## 執行防護規則模式

執行防護元件可以在兩種模式下工作：

- **僅統計**

  在此模式中，Kaspersky Endpoint Security 會將嘗試執行可執行物件或者開啟匹配防護規則條件的文件的事件發佈到 Windows 事件記錄和卡巴斯基安全管理中心，但是不會封鎖執行或者開啟物件或者文件的嘗試。預設情況下已選擇此模式。

- **啟動**

  在此模式中，應用程式會封鎖執行物件或者開啟匹配防護規則條件的文件。應用程式也會將嘗試執行物件或者開啟文件的事件發佈到 Windows 事件記錄和卡巴斯基安全管理中心事件記錄。

管理執行防護

您只可以在網頁主控台中配置元件設定。

*要防護執行：*

1. 在網頁主控台的主視窗中，選擇**資產（裝置）→政策和設定檔**。
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**"執行防止"**標籤。
6. 開啟**"執行防止已啟用"**開關。
7. 在**"執行或開啟被禁止的物件時的動作"**塊中，選擇元件操作模式：
   - **封鎖並新增至事件記錄**在此模式中，應用程式會封鎖執行物件或者開啟匹配防護規則條件的文件。應用程式也會將嘗試執行物件或者開啟文件的事件發佈到 Windows 事件記錄和卡巴斯基安全管理中心事件記錄。
   - **新增至事件記錄**在此模式中，Kaspersky Endpoint Security 會將嘗試執行可執行物件或者開啟匹配防護規則條件的文件的事件發佈到 Windows 事件記錄和卡巴斯基安全管理中心，但是不會封鎖執行或者開啟物件或者文件的嘗試。預設情況下已選擇此模式。
8. 建立執行防護規則清單：
   a. 點擊**"手動新增"**。
   b. 這會開啟一個視窗；在此視窗中，輸入執行防護規則名稱（例如*Application A*）。
   c. 在**"類型"**下拉清單中，選擇您想要封鎖的物件：**可執行檔**，**指令碼**，**Microsoft Office 文件**。
   如果您選擇了錯誤的物件類型，則 Kaspersky Endpoint Security 不封鎖檔案或者指令碼。
   d. 若要新增檔案，您必須輸入檔案的雜湊（SHA256 或者 MD5）、檔案的完整路徑、或雜湊和路徑二者。

   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，則 Kaspersky Endpoint Security 不封鎖檔案或者指令碼。

   執行防護支援Office 檔案延伸程式集合和指令碼解譯器集合。
9. 儲存變更。

結果，Kaspersky Endpoint Security 會封鎖執行物件：執行可執行檔和指令碼，開啟 Office 格式檔案。不過，您可以（例如）在文本編輯器中開啟指令碼檔案（即使執行指令碼被禁止）。當封鎖執行物件時，如果在應用程式設定中啟用了通知，則 Kaspersky Endpoint Security 會顯示一個標準通知（請見下圖）。




執行防護通知

# 電腦網路隔離

電腦網路隔離可自動從網路中隔離電腦以回應偵測到洩露指示器 (IOC)，這就是*自動模式*。您可以在研究偵測到的威脅時手動開啟網路隔離，這就是*手動模式*。

當開啟網路隔離時，應用程式會斷開電腦上的所有活動連線並封鎖所有新的 TCP/IP 連線，以下連線除外：

- 網路隔離排除項目中列出的連線。
- Kaspersky Endpoint Security 服務安裝的連線。
- 卡巴斯基安全管理中心網路代理啟動的連線。
- 與 SVM 和 Integration Server 的連線（如果應用程式正在 Light Agent 模式下使用）。

您只可以在網頁主控台中配置元件設定。

## 自動網路隔離模式

您可以配置網路隔離自動開啟以回應 IOC 偵測。您可以使用群組政策配置自動網路隔離模式。

**如何配置網路隔離自動開啟以回應 IOC 偵測**

1. 在網頁主控台的主視窗中，選擇**資產（裝置）→工作**。
   工作清單開啟。
2. 點擊 Kaspersky Endpoint Security 的"**IOC 掃描**"工作。
   工作內容視窗將開啟。
   需要的話建立 *IOC 掃描* 工作。
3. 選擇"**應用程式設定**"標籤。

4. 在“**偵測到 IOC 後的動作**”塊中，選擇“**發現 IOC 後採取回應動作**”和“**從網路中隔離電腦**”核取方塊。

5. 儲存變更。

結果，當偵測到 IOC 時，應用程式會從網路中隔離電腦以防止威脅散佈。

您可以設定網路隔離功能，使其在一段時間後自動停用。預設情況下，應用程式在開啟網路隔離 8 小時後將其關閉。您也可以手動關閉網路隔離（請參閱下面的指示）。關閉網路隔離後，電腦可以不受限制地使用網路。

**如何配置在自動模式中延遲關閉電腦的網路隔離**

1. 在網頁主控台的主視窗中，選擇**資產（裝置）→ 政策和設定檔**。

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“**網路隔離**”標籤。

6. 選擇關閉網路隔離的延遲時間。

7. 儲存變更。

手動網路隔離模式

您也可以手動開啟和關閉網路隔離。您可以使用卡巴斯基安全管理中心主控台中的電腦屬性配置手動網路隔離模式。

您可以開啟網路隔離：

- 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。

- 使用本機應用程式設定。

- 在 *IOC 掃描* 工作設定中。

  如果 *IOC 掃描* 工作偵測到 IOC，您可以直接從 IOC（*IOC 掃描* → **應用程式設定** → **IOC 掃描結果** 工作的屬性）將電腦與網路隔離。Kaspersky Endpoint Security 還允許立即管理其他設定：網路隔離停用期和網路隔離排除項目。

**如何手動開啟電腦的網路隔離**

1. 在網頁主控台的主視窗中，選擇**資產（裝置）→ 受管理裝置**。

2. 選取要為其配置本機應用程式設定的電腦。

   這將開啟電腦內容。

3. 選擇**"應用程式"**標籤。
4. 點擊**"Kaspersky Endpoint Security for Windows"**。
   這將開啟本機應用程式設定。
5. 選擇**"應用程式設定"**標籤。
6. 轉到**"Detection and Response"→"Endpoint Detection and Response"**。
7. 在**"網路隔離"**塊中，點擊**"從網路中隔離電腦"**。

您可以配置在指定時間經過後自動關閉網路隔離。預設情況下，應用程式在開啟網路隔離 8 小時後將其關閉。關閉網路隔離後，電腦可以不受限制地使用網路。

**如何配置延遲手動關閉電腦的網路隔離**

1. 在網頁主控台的主視窗中，選擇**資產（裝置）→受管理裝置**。
2. 選取要為其配置本機應用程式設定的電腦。
   這將開啟電腦內容。
3. 選擇**"工作"**標籤。
   這將顯示電腦上可用的工作清單。
4. 選擇 **網路隔離** 工作。
5. 選擇**"應用程式設定"**標籤。
6. 這會開啟一個視窗；在此視窗中，選擇延遲關閉網路隔離。
7. 儲存變更。

**如何手動關閉電腦的網路隔離**

1. 在網頁主控台的主視窗中，選擇**資產（裝置）→受管理裝置**。
2. 選取要為其配置本機應用程式設定的電腦。
   這將開啟電腦內容。
3. 選擇**"應用程式"**標籤。
4. 點擊**"Kaspersky Endpoint Security for Windows"**。
   這將開啟本機應用程式設定。
5. 選擇**"應用程式設定"**標籤。
6. 轉到**"Detection and Response"→"Endpoint Detection and Response"**。
7. 在**"網路隔離"**塊中，點擊**"解除封鎖從網路中隔離的電腦"**。

您也可以使用命令列本機停用網路隔離。

從 Kaspersky Endpoint Security 12.10 for Windows 開始，您可以在警示詳細資料中管理網路隔離。此外，您可以在警示詳細資料中指定電腦網路隔離時間段。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。

網路隔離排除項目

您可以配置網路隔離排除項目。當開啟網路隔離時，電腦上匹配規則的網路連線不會被封鎖。

要配置網路隔離排除項目，您可以使用"*標準網路設定檔*"清單。預設情況下，排除項目包括包含確保裝置（具有 DNS/DHCP 伺服器和 DNS/DHCP 用戶端角色）不中斷操作的規則的網路設定檔。您也可以修改標準網路設定檔的設定或者手動定義排除項目（請見以下指示）。

只有當網路隔離回應偵測到的威脅自動開啟時，政策內容中指定的排除項目才會套用。只有當網路隔離在卡巴斯基安全管理中心主控台的電腦內容或者警示詳情中手動開啟時，電腦內容中指定的排除項目才會套用。

活動政策不會阻止套用在電腦內容中配置的網路隔離的排除項目，因為這些參數有不同的使用案例。

**如何自動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（裝置）→ 政策和設定檔**。
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"**網路隔離**"標籤。
6. 在"**網路隔離排除項目**"塊中， 點擊"**排除項目**"。
7. 這會開啟一個視窗；在此視窗中，點擊**新增 → 從設定檔新增**然後選擇用於配置排除項目的標準網路設定檔。

   來自設定檔的網路隔離排除項目被新增至網路隔離排除項目清單。您可以檢視網路連線的內容。如有必要，您可以修改網路連線設定。
8. 如有必要，手動新增網路隔離排除項目。為此，在排除項目清單視窗中點擊**新增 → 手動新增**並手動編輯網路連線設定。
9. 儲存變更。

**如何手動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（裝置）→ 受管理裝置**。
2. 選取要為其配置本機應用程式設定的電腦。

   這將開啟電腦內容。
3. 選擇"**工作**"標籤。

   這將顯示電腦上可用的工作清單。
4. 選擇 **網路隔離** 工作。

5. 選擇"**應用程式設定**"標籤。
6. 這將開啟一個視窗；在此視窗中，點擊**排除項目**。
7. 這會開啟一個視窗；在此視窗中，點擊"**從設定檔新增**"然後選擇用於配置排除項目的標準網路設定檔。

   來自設定檔的網路隔離排除項目被新增至網路隔離排除項目清單。您可以檢視網路連線的內容。如有必要，您可以修改網路連線設定。
8. 如有必要，手動新增網路隔離排除項目。為此，在排除項目清單視窗中點擊"**新增**"並手動編輯網路連線設定。
9. 儲存變更。

您也可以使用命令列本機檢視網路隔離排除項目清單。在這種情況下，電腦必須被隔離。

從 Kaspersky Endpoint Security 12.10 for Windows 開始，您可以在警示詳細資料中新增網路隔離排除項目。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。

# 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識別惡意活動和決定其信譽。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。

如果您正在使用卡巴斯基私有安全網路，則 Cloud Sandbox 技術不可使用。

Cloud Sandbox 技術永久啟用，對所有卡巴斯基安全網路使用者可用，與他們使用的產品授權類型無關。如果您已經部署 Endpoint Detection and Response 解決方案 (EDR Optimum 或者 EDR Expert)，則可以為 Cloud Sandbox 偵測到的威脅啟用單獨的計數器。您可以使用此計數器在分析偵測到的威脅時產生統計資料。

*若要啟用 Cloud Sandbox 計數器：*

1. 在網頁主控台的主視窗中，選擇**資產（裝置）→政策和設定檔**。
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. 開啟"**Cloud Sandbox 已啟用**"開關。

7. 儲存變更。

每當有威脅，Kaspersky Endpoint Security 就會在**威脅偵測技術**下的應用程式主視窗中為使用 Cloud Sandbox 偵測到的威脅啟動計數器。Kaspersky Endpoint Security 也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 威偵測技術。

# EDR Optimum 的 KEA 到 KES 遷移指南

Kaspersky Endpoint Security for Windows 包括用於 Kaspersky Managed Detection and Response Optimum 應解決方案的內置代理。您再也無需分開 Kaspersky Endpoint Agent 應用程式來使用 EDR Optimum。Kaspersky Endpoint Agent 的所有功能將由 Kaspersky Endpoint Security 執行。

當您在安裝了 Kaspersky Endpoint Agent 的電腦上部署 Kaspersky Endpoint Security 時，Kaspersky Endpoint Detection and Response Optimum 解決方案將繼續與 Kaspersky Endpoint Security 一起工作。此外，Kaspersky Endpoint Agent 將被從電腦移除。當您將 Kaspersky Endpoint Security 更新到版本 11.7.0 或更高版本時，系統中會發生相同的行為。

Kaspersky Endpoint Security 與 Kaspersky Endpoint Agent 不相容。您不能在同一台電腦上同時安裝這些應用程式。

Kaspersky Endpoint Security 必須滿足以下條件才能作為 Kaspersky Managed Detection and Response Optimum 的一部分工作：

- Kaspersky Endpoint Detection and Response Optimum 2.0 或更高版本。
- 卡巴斯基安全管理中心版本 13.2 或更高版本（包括網路代理）。在早期版本的卡巴斯基安全管理中心中，無法啟動 EDR Optimum 功能。
- EDR Optimum 功能只可以使用卡巴斯基安全管理中心網頁主控台進行管理。
- 已啟用到管理伺服器的資料傳輸。透過網頁主控台獲取電腦上的隔離檔案需要該資料。
- 已建立在卡巴斯基安全管理中心網頁主控台和管理伺服器之間的背景連線。若要透過卡巴斯基安全管理中心網頁主控台讓 EDR Optimum 和管理伺服器一起工作，您必須建立一個新的安全連線，一個*背景連線*。

將 [KES+KEA] 配置遷移到 [KES+built-in agent] for EDR Optimum 的步驟

1. **升級 Kaspersky Endpoint Security 網頁外掛程式**

   EDR Optimum 元件可以使用 Kaspersky Endpoint Security 網頁外掛程式版本 11.7.0 或更高版本進行管理。

2. **遷移政策和工作**

   將 Kaspersky Endpoint Agent 設定傳輸到 Kaspersky Endpoint Security for Windows。為此，請使用 Web 主控台中的 Kaspersky Endpoint Agent 遷移精靈。

   **如何將政策和工作設定從 Kaspersky Endpoint Agent 遷移到網頁主控台中的 Kaspersky Endpoint Security**

   在網頁主控台的主視窗中，選擇**操作 → 從 Kaspersky Endpoint Agent 遷移**。

這會執行政策和工作遷移精靈。按照精靈的說明進行操作。

步驟 1. 政策遷移

遷移精靈會建立一個新政策，將 Kaspersky Endpoint Security 和 Kaspersky Endpoint Agent 政策的設定合併。在政策清單中，選擇您想將其設定與 Kaspersky Endpoint Security 政策合併的 Kaspersky Endpoint Agent 政策。點擊 Kaspersky Endpoint Agent 政策以選擇您想與其合併設定的 Kaspersky Endpoint Security 政策。確保選擇了正確的政策然後前往下一步。

步驟 2. 工作遷移

遷移精靈將為 Kaspersky Endpoint Security 建立新工作。在工作清單中，選擇您想為其設定 Kaspersky Endpoint Security 政策的 Kaspersky Endpoint Agent 工作。前往下一步。

步驟 3. 精靈完成

結束精靈。結果，精靈將執行以下操作：

- 建立一個新的 Kaspersky Endpoint Security 政策。

  政策將合併 Kaspersky Endpoint Security 和 Kaspersky Endpoint Agent 的設定。政策稱為 *<Kaspersky Endpoint Security 政策名稱> & <Kaspersky Endpoint Agent 政策名稱>*。新政策的狀態為*非作用中*。若要繼續，將 Kaspersky Endpoint Agent 和 Kaspersky Endpoint Security 政策的狀態變更為*非作用中*，然後啟動新合併的政策。

  從 Kaspersky Endpoint Agent 遷移到 Kaspersky Endpoint Security for Windows 後，請確保新政策已設定將資料傳輸到管理伺服器的功能（隔離檔案資料和威脅發展鏈資料）。資料傳輸參數值不會從 Kaspersky Endpoint Agent 政策遷移。

- 建立新的 Kaspersky Endpoint Security 工作。

  新工作是 Kaspersky Endpoint Agent 工作的副本。同時，精靈不會變更 Kaspersky Endpoint Agent 工作。

**3 授權 EDR Optimum 功能**

如果您使用 Kaspersky Endpoint Detection and Response Optimum 或 Kaspersky Optimum Security 產品授權來啟動 Kaspersky Endpoint Security for Windows 和 Kaspersky Endpoint Agent，EDR Optimum 功能將在升級應用程式到版本 11.7.0 或更高版本後自動啟動。您不需要做任何其它事情。

如果使用獨立 Kaspersky Endpoint Detection and Response Optimum 附加元件產品授權啟動 EDR Optimum 功能，您必須確保 EDR Optimum 金鑰已新增到卡巴斯基安全管理中心存放庫且產品授權金鑰自動分發功能已啟用。升級應用程式到版本 11.7.0 或更高版本後，EDR Optimum 功能將被自動啟動。

如果使用 Kaspersky Endpoint Detection and Response Optimum 或 Kaspersky Optimum Security 產品授權啟動 Kaspersky Endpoint Agent，使用其他產品授權啟動 Kaspersky Endpoint Security for Windows，您必須將 Kaspersky Endpoint Security for Windows 金鑰替換為普通的 Kaspersky Endpoint Detection and Response Optimum 金鑰或 Kaspersky Optimum Security 金鑰。您可以使用"*新增金鑰*"工作取代金鑰。

**4 安裝/升級 Kaspersky Endpoint Security 應用程式**

要在應用程式安裝或升級期間遷移 EDR Optimum 功能，建議使用遠端安裝工作。建立遠端安裝工作時，您需要在安裝套件設定中選擇 EDR Optimum 元件。

您還可以使用以下方法升級應用程式：

- 使用 Kaspersky 更新服務。
- 本機使用安裝精靈。

當在安裝了 Kaspersky Endpoint Agent 的電腦上升級應用程式時，Kaspersky Endpoint Security 支援自動選擇元件。自動選擇元件取決於升級應用程式的使用者帳戶的權限。

如果在系統帳戶 (SYSTEM) 下使用 EXE 或 MSI 檔案升級 Kaspersky Endpoint Security，Kaspersky Endpoint Security 將獲得對 Kaspersky 解決方案的目前產品授權的存取權限。因此，如果電腦安裝了 Kaspersky Endpoint Agent 且啟動了 EDR Optimum 解決方案，Kaspersky Endpoint Security 安裝程式將自動配置元件集合並選擇 EDR Optimum 元件。這將使得 Kaspersky Endpoint Security 切換到使用內建代理並刪除 Kaspersky Endpoint Agent。在系統帳戶 (SYSTEM) 下執行 MSI 安裝程式通常在透過 Kaspersky 更新服務升級或透過卡巴斯基安全管理中心部署安裝套件時進行。

如果在沒有權限的帳戶下使用 MSI 檔案升級 Kaspersky Endpoint Security，Kaspersky Endpoint Security 將缺少對 Kaspersky 解決方案的目前產品授權的存取權限。在此情況下，Kaspersky Endpoint Security 將基於 Kaspersky Endpoint Agent 配置自動選擇元件。此後，Kaspersky Endpoint Security 將切換到使用內建代理並刪除 Kaspersky Endpoint Agent。

Kaspersky Endpoint Security 支援在不重啟電腦的情況下升級。您可以選擇政策屬性中的應用程式升級模式。

5. **檢查應用程式運行情況**

如果安裝或升級後應用程式後電腦在卡巴斯基安全管理中心主控台中具有"*緊急*"狀態：

- 請確保電腦安裝了網路代理 13.2或更高版本。
- 透過檢視"*應用程式元件狀態報告*"來檢查內建代理的運行狀態。如果元件的狀態為"*未安裝*"，請使用*變更應用程式元件*工作來安裝元件。如果一個元件的狀態為 *產品授權不支援*，確保您已啟動內建代理功能。
- 請確保在 Kaspersky Endpoint Security for Windows 的新政策中接受卡巴斯基安全網路聲明。

# Kaspersky Sandbox



Kaspersky Endpoint Security for Windows 包含一個用於與 Kaspersky Sandbox 解決方案整合的內建代理。*Sandbox*元件可偵測和自動封鎖電腦上的進階威脅。Sandbox 會分析物件行為以偵測惡意行動和組織的 IT 基礎架構上的針對性攻擊所特有的活動。Sandbox 會分析和掃描部署了 Microsoft Windows 作業系統的虛擬影像的特殊伺服器（Sandbox 伺服器）上的物件。有關解決方案的詳細資訊，請參閱 Kaspersky Sandbox 說明 和 Kaspersky Anti Targeted Attack Platform 說明。

# 內建代理與 Kaspersky Sandbox 整合

與 Kaspersky Sandbox 元件整合需要新增 Sandbox 元件。您可以在安裝或者升級期間以及使用*變更應用程式元件*工作時選擇 Sandbox 元件。

要使用該元件必須滿足以下條件：

- 卡巴斯基安全管理中心 13.2卡巴斯基安全管理中心的較早版本不允許為威脅回應建立獨立 IOC 掃描工作。
- 該元件只可以使用網頁主控台進行管理。您不能使用管理主控台 (MMC) 管理此元件。
- 應用程式被啟動，功能受產品授權覆蓋。
- 已啟用到管理伺服器的資料傳輸。

  若要使用 Kaspersky Sandbox 的所有功能，請確保已啟用隔離檔案資料傳輸。透過網頁主控台獲取電腦上的隔離檔案需要該資料。例如，您可以從隔離區下載檔案用於在網頁主控台中分析。

  **如何在網頁主控台中啟用資料傳輸到管理伺服器**

  1. 在網頁主控台的主視窗中，選擇**資產（裝置）→ 政策和設定檔**。
  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. 在“**到管理伺服器的資料傳輸**“塊中，選中“**關於隔離檔案**”核取方塊。
  6. 儲存變更。
- 已建立在卡巴斯基安全管理中心網頁主控台和管理伺服器之間的背景連線

  若要透過卡巴斯基安全管理中心網頁主控台讓 Kaspersky Sandbox 和管理伺服器一起工作，您必須建立一個新的安全連線，一個*背景連線*。有關卡巴斯基安全管理中心與其他卡巴斯基解決方案整合的詳細資訊，請參閱卡巴斯基安全管理中心說明。

  **在網頁主控台中建立一個背景連線**

  1. 在網頁主控台的主視窗中，選擇**設定 → 整合**。
  2. 轉到**“整合”**區域。
  3. 開啟**“整合的背景連線 已啟用”**開關。
  4. 儲存變更。

  如果未在卡巴斯基安全管理中心網頁主控台和管理伺服器之間建立背景連線，則無法作為威脅回應的一部分建立獨立的 IOC 掃描工作。
- 若要配置與 Sandbox 伺服器的受信任連線，您必須 TLS 憑證。然後，您必須使用政策將憑證新增至電腦。您還需要將憑證新增至 Sandbox 伺服器。

  > 使用加密容器的雙向身分驗證不適用於 Kaspersky Sandbox。

  您也可以在網頁主控台中或者本機使用命令列新增 TLS 憑證。.
- Kaspersky Sandbox 元件被啟用。

- 確保 Sandbox 操作的應用程式元件已啟用且正常操作。以下元件可確保 Sandbox 的操作：
  - 檔案威脅防護。
  - 主機入侵防禦。
  - 防火牆。
  - AMSI 防護。
  - 背景掃描。

*要啟用或停用與 Kaspersky Sandbox 的整合：*

1. 在網頁主控台的主視窗中，選擇**資產（裝置）→政策和設定檔**。
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. 使用"**Sandbox 整合已啟用**"切換開關可啟用或停用元件。
6. 在"**整合模式**"塊中，選擇元件操作模式：**Kaspersky Sandbox**。
7. 點擊"**連線設定**"連接。
   這會開啟 Sandbox 伺服器連線設定視窗。
8. 在"**伺服器 TLS 憑證**"塊中，點擊"**上傳**"然後選擇 TLS 憑證檔案。
   對於一個 Sandbox 伺服器 Kaspersky Endpoint Security 只能有一個 TLS 憑證。如果您之前新增過 TLS 憑證，那個憑證將被撤銷。只有最近新增的憑證會得到使用。
9. 為 Sandbox 伺服器配置進階連線設定：
   - **逾時 (毫秒)**Sandbox 伺服器連線逾時。配置的逾時經過後，Kaspersky Endpoint Security 會傳送請求給下一個伺服器。如果您的連線速度慢或者連線不穩定，您可以增加伺服器的連線逾時。建議的請求逾時為 0.5 秒鐘或更短。
   - **請求佇列**請求佇列資料夾大小在 Sandbox 中傳送多個物件進行掃描時，Kaspersky Endpoint Security 會建立一個請求佇列。預設情況下，請求佇列資料夾大小限制為 100 MB。在達到最大的大小後，Sandbox 會停止向佇列新增請求並將相應事件傳送到卡巴斯基安全管理中心。您可以根據伺服器配置來設定請求佇列資料夾大小。
10. 在"**連線到 Sandbox 伺服器**"塊中，點擊"**新增**"按鈕。

11. 這會開啟一個視窗，在視窗中，輸入 Sandbox 伺服器位址 (IPv4, IPv6, DNS) 和連接埠。

    有關部署虛擬映像和配置 Sandbox 伺服器的詳情，請參見 Kaspersky Sandbox 說明。

12. 儲存變更。

結果，Kaspersky Endpoint Security 會驗證 TLS 憑證。如果憑證驗證成功，在與卡巴斯基安全管理中心進行下一次同步時，Kaspersky Endpoint Security 將上傳該憑證檔案到電腦。如果您新增了兩個 TLS 憑證，Kaspersky Sandbox 將使用最新的憑證來建立受信任連線。透過檢視"*應用程式元件狀態報告*"來檢查元件的運行狀態。您還可以在 Kaspersky Endpoint Security 的本地介面中的報告中檢視元件的運行狀態。"**Sandbox**"元件將新增到 Kaspersky Endpoint Security 元件清單中。

您可以在 Web 主控台中或本機使用命令行啟用或停用與 Kaspersky Sandbox 的整合。

Kaspersky Endpoint Security 會將 Kaspersky Sandbox 元件工作的相關資訊儲存到一個報告中。報告也包含錯誤資訊。如果您得到一個錯誤，描述符合 `Error code: XXX` 格式（例如 `0xa67b01f4`），請聯絡技術支援。

# 掃描洩露指示器（獨立工作）

*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，許多登入系統的不成功嘗試可以構成一個洩露指示器。"*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。

Kaspersky Endpoint Security 可使用 IOC 檔案搜尋洩露指示器。*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。Kaspersky Endpoint Security 自動為 Kaspersky Sandbox 產生 IOC 檔案。

## IOC 掃描 工作執行模式

應用程式為 Kaspersky Sandbox 建立獨立的 IOC 掃描工作。"*獨立 IOC 掃描工作*"是一個當回應 Kaspersky Sandbox偵測到的威脅時自動建立的群組工作。Kaspersky Endpoint Security 會自動產生 IOC 檔案。自訂 IOC 檔案不受支援。工作會在建立時間 30 天后被自動刪除。有關獨立 IOC 掃描工作的更多詳情，請參見 Kaspersky Sandbox 說明。

## IOC 掃描工作設定

Kaspersky Sandbox 可以在回應威脅時自動建立並執行"*IOC 掃描*"工作。

您只可以在網頁主控台中配置設定。

您需要卡巴斯基安全管理中心 13.2 以便 Kaspersky Sandbox 的獨立 IOC 掃描工作有效。

*要變更IOC 掃描工作的設定：*

1. 在網頁主控台的主視窗中，選擇**資產（裝置）→工作**。

   工作清單開啟。

2. 點擊 Kaspersky Endpoint Security 的"**IOC 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. 轉到"**IOC 掃描設定**"區域。

5. 配置偵測到 IOC 後的動作：

   - **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 會建立備份副本以防物件以後需要還原。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 會掃描內核記憶體、執行處理序和磁碟的開啟磁區。

   - **僅在電腦空閒時執行**電腦資源繁忙時，推遲工作的啟動。如果電腦已鎖定或熒幕保護程式已開啟，Kaspersky Endpoint Security 會啟動掃描工作。如果您中斷了執行工作（例如，透過解鎖電腦），Kaspersky Endpoint Security 會自動執行工作，從被中斷的地方繼續。此排程選項可讓您在使用電腦時節省電腦資源。

6. 儲存變更。

您可以在工作內容的"**結果**"區域中檢視工作結果。您可以在工作內容中檢視偵測到的洩露指示器的有關資訊：**應用程式設定 → IOC 掃描結果**。

IOC 掃描結果保留 30 天。在此期間之後，Kaspersky Endpoint Security 將自動移除最舊條目。

# Kaspersky Sandbox 的 KEA 到 KES 遷移指南

Kaspersky Endpoint Security for Windows 包含一個用於 Kaspersky Sandbox 解決方案的內建代理。您再也無需分開 Kaspersky Endpoint Agent 應用程式來使用 Kaspersky Sandbox。Kaspersky Endpoint Agent 的所有功能將由 Kaspersky Endpoint Security 執行。

當您在安裝了 Kaspersky Endpoint Agent 的電腦上部署 Kaspersky Endpoint Security 時，Kaspersky Sandbox 解決方案將繼續與 Kaspersky Endpoint Security 一起工作。此外，Kaspersky Endpoint Agent 將被從電腦移除。當您將 Kaspersky Endpoint Security 更新到版本 11.7.0 或更高版本時，系統中會發生相同的行為。

Kaspersky Endpoint Security 與 Kaspersky Endpoint Agent 不相容。您不能在同一台電腦上同時安裝這些應用程式。

Kaspersky Endpoint Security 必須滿足以下條件才能作為 Kaspersky Sandbox 的一部分工作：

- Kaspersky Sandbox 版本 2.0 或更高版本。
- 卡巴斯基安全管理中心版本 13.2 或更高版本（包括網路代理）。在早期版本的卡巴斯基安全管理中心中，無法啟動 Kaspersky Sandbox 功能。
- Kaspersky Sandbox 只可以使用卡巴斯基安全管理中心網頁主控台進行管理。
- 已啟用到管理伺服器的資料傳輸。透過網頁主控台獲取電腦上的隔離檔案需要該資料。
- 已建立在卡巴斯基安全管理中心網頁主控台和管理伺服器之間的背景連線。若要透過卡巴斯基安全管理中心網頁主控台讓 Kaspersky Sandbox 和管理伺服器一起工作，您必須建立一個新的安全連線，一個*背景連線*。

將 [KES+KEA] 配置遷移到 [KES+built-in agent] for Kaspersky Sandbox 的步驟

1. **升級 Kaspersky Endpoint Security 網頁外掛程式**

   Kaspersky Sandbox 元件可以使用 Kaspersky Endpoint Security 網頁外掛程式版本 11.7.0 或更高版本進行管理。

2. **遷移政策和工作**

   將 Kaspersky Endpoint Agent 設定傳輸到 Kaspersky Endpoint Security for Windows。為此，請使用 Web 主控台中的 Kaspersky Endpoint Agent 遷移精靈。

   **如何將政策和工作設定從 Kaspersky Endpoint Agent 遷移到網頁主控台中的 Kaspersky Endpoint Security**

   在網頁主控台的主視窗中，選擇**操作 → 從 Kaspersky Endpoint Agent 遷移**。

   這會執行政策和工作遷移精靈。按照精靈的說明進行操作。

   步驟 1. 政策遷移

   遷移精靈會建立一個新政策，將 Kaspersky Endpoint Security 和 Kaspersky Endpoint Agent 政策的設定合併。在政策清單中，選擇您想將其設定與 Kaspersky Endpoint Security 政策合併的 Kaspersky Endpoint Agent 政策。點擊 Kaspersky Endpoint Agent 政策以選擇您想與其合併設定的 Kaspersky Endpoint Security 政策。確保選擇了正確的政策然後前往下一步。

   步驟 2. 工作遷移

   遷移精靈將為 Kaspersky Endpoint Security 建立新工作。在工作清單中，選擇您想為其設定 Kaspersky Endpoint Security 政策的 Kaspersky Endpoint Agent 工作。前往下一步。

步驟 3. 精靈完成

結束精靈。結果，精靈將執行以下操作：

- 建立一個新的 Kaspersky Endpoint Security 政策。

  政策將合併 Kaspersky Endpoint Security 和 Kaspersky Endpoint Agent 的設定。政策稱為 *<Kaspersky Endpoint Security 政策名稱> & <Kaspersky Endpoint Agent 政策名稱>*。新政策的狀態為*非作用中*。若要繼續，將 Kaspersky Endpoint Agent 和 Kaspersky Endpoint Security 政策的狀態變更為*非作用中*，然後啟動新合併的政策。

  從 Kaspersky Endpoint Agent 遷移到 Kaspersky Endpoint Security for Windows 後，請確保新政策已設定將資料傳輸到管理伺服器的功能（隔離檔案資料和威脅發展鏈資料）。資料傳輸參數值不會從 Kaspersky Endpoint Agent 政策遷移。

- 建立新的 Kaspersky Endpoint Security 工作。

  新工作是 Kaspersky Endpoint Agent 工作的副本。同時，精靈不會變更 Kaspersky Endpoint Agent 工作。

**3 許可 Kaspersky Sandbox 功能**

要將 Kaspersky Endpoint Security 作為 Kaspersky Sandbox 解決方案的一部分啟動，您需要單獨的 Kaspersky Sandbox 附加產品授權。您可以使用"*新增金鑰*"工作新增金鑰。結果，兩個金鑰將被新增到應用程式：*Kaspersky Endpoint Security* 和 *Kaspersky Sandbox*。

**4 安裝/升級 Kaspersky Endpoint Security 應用程式**

要在應用程式安裝或升級期間遷移 Kaspersky Sandbox 功能，建議使用遠端安裝工作。建立遠端安裝工作時，您需要在安裝套件設定中選擇 Kaspersky Sandbox 元件。

您還可以使用以下方法升級應用程式：

- 使用 Kaspersky 更新服務。
- 本機使用安裝精靈。

當在安裝了 Kaspersky Endpoint Agent 的電腦上升級應用程式時，Kaspersky Endpoint Security 支援自動選擇元件。自動選擇元件取決於升級應用程式的使用者帳戶的權限。

如果在系統帳戶 (SYSTEM) 下使用 EXE 或 MSI 檔案升級 Kaspersky Endpoint Security，Kaspersky Endpoint Security 將獲得對 Kaspersky 解決方案的目前產品授權的存取權限。因此，如果電腦安裝了 Kaspersky Endpoint Agent 且啟動了 Kaspersky Sandbox 解決方案，Kaspersky Endpoint Security 安裝程式將自動配置元件集合並選擇 Kaspersky Sandbox 元件。這將使得 Kaspersky Endpoint Security 切換到使用內建代理並刪除 Kaspersky Endpoint Agent。在系統帳戶 (SYSTEM) 下執行 MSI 安裝程式通常在透過 Kaspersky 更新服務升級或透過卡巴斯基安全管理中心部署安裝套件時進行。

如果在沒有權限的帳戶下使用 MSI 檔案升級 Kaspersky Endpoint Security，Kaspersky Endpoint Security 將缺少對 Kaspersky 解決方案的目前產品授權的存取權限。在此情況下，Kaspersky Endpoint Security 將基於 Kaspersky Endpoint Agent 配置自動選擇元件。此後，Kaspersky Endpoint Security 將切換到使用內建代理並刪除 Kaspersky Endpoint Agent。

Kaspersky Endpoint Security 支援在不重啟電腦的情況下升級。您可以選擇政策屬性中的應用程式升級模式。

**5 檢查應用程式運行情況**

如果安裝或升級後應用程式後電腦在卡巴斯基安全管理中心主控台中具有"*緊急*"狀態：

- 請確保電腦安裝了網路代理 13.2或更高版本。
- 透過檢視"*應用程式元件狀態報告*"來檢查內建代理的運行狀態。如果元件的狀態為"*未安裝*"，請使用*變更應用程式元件*工作來安裝元件。如果一個元件的狀態為 *產品授權不支援*，確保您已啟動內建代理功能。
- 請確保在 Kaspersky Endpoint Security for Windows 的新政策中接受卡巴斯基安全網路聲明。

# Kaspersky Anti Targeted Attack Platform



Kaspersky Endpoint Security for Windows 支援與 Kaspersky Anti Targeted Attack Platform (EDR (KATA)) 解決方案一起使用。*Kaspersky Anti Targeted Attack Platform* 是旨在及時偵測複雜威脅（如針對性攻擊、進階持久性威脅 (APT)、零日攻擊等）的解決方案。Kaspersky Anti Targeted Attack Platform 包括三個功能單元：

- Kaspersky Anti Targeted Attack Platform (*KATA*)
- Kaspersky Endpoint Detection and Response (*EDR (KATA)*)
- Network Detection and Response (*NDR (KATA)*)

您可以單獨購買所有功能單元或單獨的功能單元。有關解決方案的詳細資訊，請參閱 Kaspersky Anti Targeted Attack Platform 說明。該應用程式包括 EDR、NDR 元件的內建代理程式。該應用程式還支援與 Sandbox 元件一起使用，它是 KATA 的一部分。

## 威脅情報工具

Kaspersky Endpoint Detection and Response 使用以下威脅情報工具：

- 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 Kaspersky Anti Targeted Attack Platform 伺服器。在此情況下，Kaspersky Endpoint Security 應用程式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 Kaspersky Anti Targeted Attack Platform 伺服器。

EDR (KATA) 和 NDR (KATA) 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 Kaspersky Anti Targeted Attack Platform 主控台進行管理，包括執行工作、管理隔離物件、檢視報告和其他操作。

### 用於使用 EDR / NDR (KATA) 的 Kaspersky Endpoint Security 配置

以下配置可用於使用 EDR / NDR (KATA)：

- **[KES+內建代理]**。在此配置中，Kaspersky Endpoint Security 既充當確保電腦安全的應用程式，又充當使用 EDR / NDR (KATA) 的應用程式。Kaspersky Endpoint Security 12.1 for Windows 或更高版本提供 EDR (KATA) 的內建代理。Kaspersky Endpoint Security 12.7 for Windows 或更高版本提供 NDR (KATA) 的內建代理。

- **【協力廠商 EPP EDR Agent】**。在此配置中，IT 基礎結構的安全性由協力廠商 Endpoint Protection Platform (EPP) 提供。與 EDR / NDR (KATA) 的交互由 Kaspersky Endpoint Security 在 Endpoint Detection and Response Agent (EDR Agent) 配置中提供。在此配置中，EDR Agent 與協力廠商 EPP應用程式相容。EDR Agent for EDR (KATA) 在 Kaspersky Endpoint Security 12.3 for Windows 或更高版本中可用。EDR Agent for NDR (KATA) 在 Kaspersky Endpoint Security 12.7 for Windows 或更高版本中可用。

### 對以前版本的 Kaspersky Endpoint Security 的支援

如果您使用 Kaspersky Endpoint Security 11.2.0–11.8.0 與 Kaspersky Anti Targeted Attack Platform (EDR) 進行交互操作，應用程式將包括 Kaspersky Endpoint Agent。您可以在安裝 Kaspersky Endpoint Security 的過程中安裝 Kaspersky Endpoint Agent。

如果您使用的是 Kaspersky Endpoint Security 11.9.0 – 12.0，您需要單獨安裝 Kaspersky Endpoint Agent，因為從 Kaspersky Endpoint Security 11.9.0 開始，Kaspersky Endpoint Agent 分發套件不再是 Kaspersky Endpoint Security 分發套件的一部分。

## 內建代理與 EDR / NDR (KATA) 整合

若要與 EDR / NDR (KATA) 整合，您必須新增相關元件：Endpoint Detection and Response (KATA) 或 Network Detection and Response (KATA)。您可以在安裝或者更新應用程式時以及使用*變更應用程式元件*工作選擇與 EDR / NDR (KATA) 進行整合的元件。

從 Kaspersky Endpoint Security for Windows 12.11 版本開始，EDR (KATA) 元件已重新命名為 **Endpoint Detection and Response Expert（版本 8.0 或者更高版本）**。在此版本的應用程式中，元件與 Kaspersky Anti Targeted Attack Platform 7.1 及更早版本以及 Kaspersky Endpoint Detection and Response Expert (on-premise) 相容。

EDR Optimum、EDR Expert 和 EDR (KATA) 元件彼此不相容。

要使用 EDR / NDR (KATA) 必須滿足以下條件：

- EDR (KATA): Kaspersky Anti Targeted Attack Platform 版本 5.0–7.1。

- NDR (KATA): Kaspersky Anti Targeted Attack Platform 版本 7.0 或更高版本。

- EDR (KATA)：Kaspersky Endpoint Security for Windows 12.1 或更高版本。有關 KATA 與不同版本 Kaspersky Endpoint Security 的相容性的更多詳細資訊，請參閱 Kaspersky Anti Targeted Attack Platform 說明。

- NDR (KATA)：Kaspersky Endpoint Security for Windows 12.7 或更高版本。
- 卡巴斯基安全管理中心版本 14.2 或更高版本。在早期版本的卡巴斯基安全管理中心中，無法啟動 EDR / NDR (KATA) 功能。
- 應用程式被啟動，功能受產品授權覆蓋。
- Endpoint Detection and Response (KATA) 和 Network Detection and Response (KATA) 元件已啟用。
- 確保 EDR / NDR (KATA) 運作的應用程式元件已啟用並運作。以下元件可確保 EDR / NDR (KATA) 的操作：
  - 檔案威脅防護。
  - Web 威脅防護。
  - 郵件威脅防護。
  - 弱點利用防禦。
  - 行為偵測。
  - 主機入侵防禦。
  - AMSI 防護。
  - 背景掃描。
  - 卡巴斯基安全網路。

與 Endpoint Detection and Response (KATA) 整合涉及以下步驟：

1. **安裝 Endpoint Detection and Response (KATA) 和 Network Detection and Response (KATA) 元件**

   您可以在安裝或者更新期間以及使用*變更應用程式元件*工作時選擇 EDR (KATA) 和 NDR (KATA) 元件。

   > 您必須重新啟動電腦以完成升級含新元件的應用程式。

2. **啟動 Endpoint Detection and Response (KATA) 和 Network Detection and Response (KATA)**

   您需要單獨購買 EDR (KATA) 和 NDR (KATA)（例如，Kaspersky Endpoint Detection and Response (KATA) 附加元件）的產品授權。

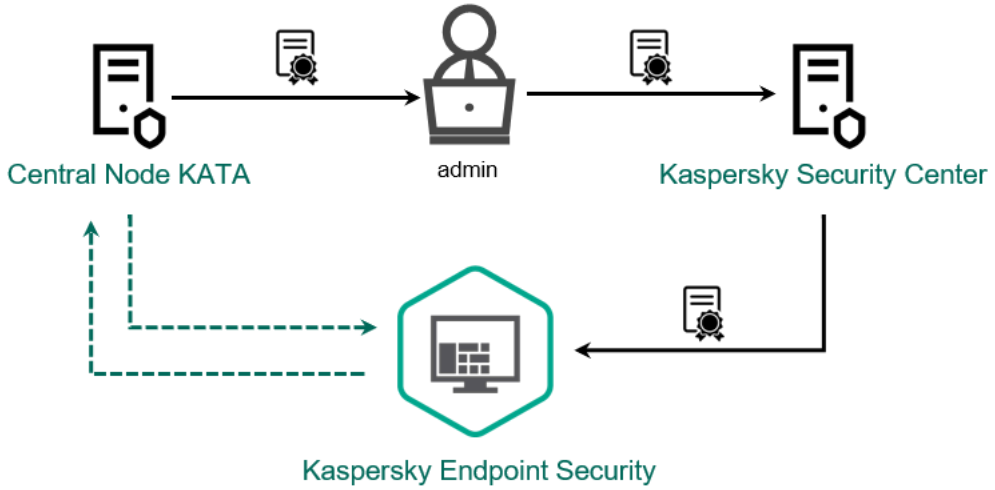
   在新增涵蓋 EDR (KATA) 和 NDR (KATA) 功能的單獨金鑰後，此功能可用。因此，電腦上將新增多個金鑰：一個金鑰用於 Kaspersky Endpoint Security，其他金鑰用於 Kaspersky Endpoint Detection and Response (KATA) 和 Network Detection and Response (KATA)。

   獨立 EDR (KATA) 和 NDR (KATA) 功能的授權和 Kaspersky Endpoint Security 的授權一樣。

   確保 EDR (KATA) 和 NDR (KATA) 功能包括在產品授權中且在應用程式的本機介面中執行。

3. **連線到中央節點**

Kaspersky Anti Targeted Attack Platform 要求在 Kaspersky Endpoint Security 和中央節點元件之間建立可信連線。要配置可信連線，您必須使用 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 ）。然後您必須將 TLS 憑證新增到 Kaspersky Endpoint Security（參見下面的說明）。




將 TLS 憑證新增到 Kaspersky Endpoint Security

預設情況下，Kaspersky Endpoint Security 僅檢查中央節點的 TLS 憑證。為了使連線更安全，您可以額外啟用在中央節點上進行電腦驗證（雙向身分驗證）。要啟用此驗證，您必須在中央節點和 Kaspersky Endpoint Security 設定中開啟雙向身分驗證。要使用雙向身分驗證，您還需要一個加密容器。*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 ）。

**如何使用管理主控台 (MMC) 將 Kaspersky Endpoint Security 電腦連線到中央節點**

1. 開啟卡巴斯基安全管理中心管理主控台。
2. 在主控台樹狀目錄中，選擇**"政策"**。
3. 選擇必要的政策並點擊以開啟政策內容。
4. 在政策視窗中，選擇 **Detection and Response** 並選擇您要設定的元件： **Endpoint Detection and Response Expert (on-premise)** 或者 **Network Detection and Response (KATA)**。
5. 選擇相應的核取方塊：**Endpoint Detection and Response Expert（版本 7.1 或者更早版本）** 或者 **Network Detection and Response (KATA)**。
6. 點擊**"伺服器連線設定"**。
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 TLS 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**"正常"**。
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。

   您可以新增多個中央節點伺服器位址。Kaspersky Endpoint Security 嘗試連線到第一個 IP 位址的伺服器。如果無法建立連線，Kaspersky Endpoint Security 將嘗試連線到清單中的第二個 IP 位址，依此類推。
10. 如果有需要的話，配置遙測。
11. 儲存變更。若要在電腦上套用該政策，請關閉掛鎖。

**如何使用網頁主控台將 Kaspersky Endpoint Security 電腦連線到中央節點**

1. 在網頁主控台的主視窗中，選擇**資產（裝置）** → **政策和設定檔**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. 前往 **內置代理設定** 部分並選擇您要配置的元件：**Endpoint Detection and Response Expert (on-premise)** 或者 **Network Detection and Response (KATA)**。
5. 打開相應的撥動開關：**Endpoint Detection and Response Expert (on-premise) 已啟用** 或者 **Network Detection and Response (KATA) 已啟用**。
6. 若要設定 EDR (KATA)，請從解決方案清單中選取 **Endpoint Detection and Response Expert（版本 7.1 或者更早版本）**。
7. 點擊**"連線設定"**。
8. 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。

9. 點擊**"確定"**。
10. 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。

    您可以新增多個中央節點伺服器位址。Kaspersky Endpoint Security 嘗試連線到第一個 IP 位址的伺服器。如果無法建立連線，Kaspersky Endpoint Security 將嘗試連線到清單中的第二個 IP 位址，依此類推。
11. 如果有需要的話，配置遙測。
12. 儲存變更。若要在電腦上套用該政策，請關閉掛鎖。

您也可以使用命令列新增 TLS 憑證。

結果，電腦會被新增到 Kaspersky Anti Targeted Attack Platform 主控台上。透過檢視*"應用程式元件狀態報告"*來檢查元件的運行狀態。您還可以在 Kaspersky Endpoint Security 的本機介面中的報告中檢視元件的運行狀態。**Endpoint Detection and Response Expert（版本 8.0 或者更高版本）**和 **Network Detection and Response (KATA)** 元件將被新增到 Kaspersky Endpoint Security 元件清單中。

您可以卡巴斯基安全管理中心主控台中在電腦屬性的 **元件** 部分中檢查元件的狀態。在主控台中檢查元件的狀態時，請考慮以下事項。如果未安裝該元件且產品授權不涵蓋該功能，則主控台會顯示 **不受產品授權支援** 狀態而不是 **未安裝**。

從 Kaspersky Endpoint Security 12.6 for Windows 開始，您可以在卡巴斯基安全管理中心管理主控台 (MMC) 中監控 EDR (KATA) 元件的狀態。元件的目前狀態顯示在**端點感應器狀態**列的電腦屬性中（*執行中*, *正在啟動*, *已停止*, *已暫停*, *失敗*, *未知*）。網頁主控台不會顯示 Endpoint Sensor 的狀態。

# 配置 EDR (KATA) 遙測

*遙測*是受防護電腦上發生的事件的清單。Kaspersky Endpoint Security 會分析遙測資料並在同步期間將其傳送到 Kaspersky Anti Targeted Attack Platform。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）。

如果您將 Kaspersky Anti Targeted Attack Platform 與另一個也使用遙測的解決方案一起使用，您可以關閉 KATA (EDR) 的遙測（請參閱以下說明）。這可讓您最佳化這些解決方案的伺服器負載。例如，如果您部署了 Managed Detection and Response 解決方案和 KATA (EDR)，則可以使用 MDR 遙測並在 KATA (EDR) 中建立威脅回應工作。

**如何在管理主控台 (MMC) 上設定遙測**

1. 開啟卡巴斯基安全管理中心管理主控台。
2. 在主控台樹狀目錄中，選擇"**政策**"。
3. 選擇必要的政策並點擊以開啟政策內容。
4. 在政策視窗中，選擇 **Detection and Response** 並選擇您要設定的元件： **Endpoint Detection and Response Expert (on-premise)** 或者 **Network Detection and Response (KATA)**。
5. 配置 **傳送同步請求到 KATA 伺服器的間隔（分）** 設定。傳送到伺服器的同步請求的頻率。在同步期間，Kaspersky Endpoint Security 傳送有關被修改應用程式設定和工作的資訊。
6. 請確保選中**傳送遙測資料到 KATA**核取方塊。
7. 如有必要，請在**資料傳輸設定**塊中配置與伺服器設定同步：
   - **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。
8. 如有必要，在**請求節流**塊中選擇**啟用請求節流**核取方塊。

   該功能有助於最佳化伺服器負載。如果選中該核取方塊，應用程式將限制傳輸的事件。如果事件數量超過配置的限制，Kaspersky Endpoint Security 將停止傳送事件。
9. 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%。
10. 儲存變更。若要在電腦上套用該政策，請關閉掛鎖。

**如何在網頁主控台上配置遙測**

1. 在網頁主控台的主視窗中，選擇**資產（裝置）→ 政策和設定檔**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 (on-premise)** "。

5. 若要設定 EDR (KATA)，請從解決方案清單中選取 **Endpoint Detection and Response Expert（版本 7.1 或者更早版本）**。

6. 確保 **將遙測資料傳送至 KATA 伺服器** 核取方塊已在 **資料傳輸設定** 區塊中被選中。

7. 配置 **傳送同步請求到伺服器的時間間隔 (分)** 設定。傳送到伺服器的同步請求的頻率。在同步期間，Kaspersky Endpoint Security 傳送有關被修改應用程式設定和工作的資訊。

8. 請確保選中**將遙測資料傳送至 KATA 伺服器**核取方塊。

9. 如有必要，請在**資料傳輸設定**塊中配置與伺服器設定同步：

   - **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。

10. 如有必要，在**請求節流**塊中選擇**啟用請求節流**核取方塊。

    該功能有助於最佳化伺服器負載。如果選中該核取方塊，應用程式將限制傳輸的事件。如果事件數量超過配置的限制，Kaspersky Endpoint Security 將停止傳送事件。

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. 儲存變更。若要在電腦上套用該政策，請關閉掛鎖。

1. 在網頁主控台的主視窗中，選擇**資產（裝置）→ 政策和設定檔**。

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 **KATA 整合 → 遙測排除項目** 部分。

5. 在**資料傳輸設定**下，選擇**使用排除項目**核取方塊。

6. 點擊**新增**並配置排除項目：

標準與邏輯 *AND* 相結合。

- **Path**.文件的完整路徑，包括其名稱和副檔名。Kaspersky Endpoint Security 輸入遮罩時支援環境變量以及 `*`和`?`字元。要使排除項目生效，必須指定檔案路徑。
- **命令行**。用於執行物件的命令。
- **描述**。來自 RT_VERSION (VersionInfo) 資源的 FileDescription 參數的值。
  有關 VersionInfo 資源的詳細資訊，請造訪 Microsoft 網站。
- **原始檔案名稱**。來自 RT_VERSION (VersionInfo) 資源的 OriginalFilename 參數的值。
- **版本**。來自 RT_VERSION (VersionInfo) 資源的 FileVersion 參數的值。
- **MD5**。檔案的 MD5 雜湊。
- **SHA256**。檔案的 SHA256 雜湊。
- **事件類型**。要使排除項目生效，您必須至少選擇一種事件類型。

7. 儲存變更。

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

啟動"工作精靈"。按照精靈的說明進行操作。

步驟 1. 選取工作類型

1. 選取"**Kaspersky Endpoint Security for Windows (12.12)**"→"**更新回溯**"。

步驟 2. 選取將要對其分配工作的裝置

選取將要執行工作的電腦。下列選項可用：

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

步驟 3. 設定工作啟動排程

設定工作排程，例如手動。

步驟 4. 定義工作名稱

輸入工作的名稱。

步驟 7. 完成工作建立

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

# EDR (KATA) 遙測排除項目

為了提高效能並最佳化到遙測伺服器的資料傳輸，您可以配置遙測排除項目。例如，您可以選擇不傳送單個應用程式的網路通訊資料。

**如何在管理主控台 (MMC) 中建立遙測資料排除項目**

1. 在卡巴斯基安全管理中心管理主控台樹狀目錄中，選取**政策**。
2. 選擇必要的政策並點擊以開啟政策內容。
3. 在政策視窗中，選擇**"一般設定 → 排除項目和物件類型"**。
4. 在**"遙測設定 → EDR (KATA) / NDR (KATA) 遙測"**塊中，點擊**"設定"**按鈕。
5. 在開啟的視窗中，設定遙測排除項目（請參閱下表）。

   應用程式將排除條件與邏輯"AND"結合。要建立規則，您必須在 **完全路徑** 欄位中指定一個值並 **用於以下事件類型** 清單中選擇至少一個事件類型。
6. 儲存變更。

**如何在網頁主控台和 Cloud Console 中建立遙測排除項目**

1. 在網頁主控台的主視窗中，選擇**資產（裝置）→ 政策和設定檔**。
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 (KATA) / NDR (KATA) 遙測"**標籤。

6. 在開啟的視窗中，設定遙測排除項目（請參閱下表）。

   應用程式將排除條件與邏輯"AND"結合。要建立規則，您必須在 **完全路徑** 欄位中指定一個值並選擇至少一個事件類型。

7. 儲存變更。

遙測排除項目參數

| 參數 | 描述 |
| --- | --- |
| **被排除的處理程序** | **最佳化要傳送的遙測資料大小**Kaspersky Endpoint Security 允許最佳化被傳輸的資料量並從遙測中排除具有某些代碼的事件：Microsoft SMB 協定、WinRM 服務和網路代理的 klnagent.exe 處理程序的代碼 102（基本通訊）和 8（處理程序的網路活動），以及有關所有類型網路協定的網路套件類型的延伸資訊。<br><br>Kaspersky Endpoint Security 可將規則觸發條件與邏輯 AND 相結合。<br><br>**處理** 和 **父處理程序**：<br>• **完全路徑**文件的完整路徑，包括其名稱和副檔名。Kaspersky Endpoint Security 輸入遮罩時支援環境變量以及 * 和 ? 字元。<br>• **命令行文字**用於執行檔案的命令。<br>• **描述**來自 RT_VERSION (VersionInfo) 資源的 FileDescription 參數的值。<br>• **原始檔案名稱**來自 RT_VERSION (VersionInfo) 資源的 OriginalFilename 參數的值。<br>• **版本**來自 RT_VERSION (VersionInfo) 資源的 FileVersion 參數的值。<br>• **檔案總和檢查碼**MD5 和 SHA256。<br>您也可以手動選擇檔案，應用程式將自動填寫所選檔案中的欄位。<br><br>在 64 位元作業係統中，您必須從 `C:\windows\system32` 資料夾手動輸入處理程序的 64 位元版本可執行檔案的參數，因為應用程式使用 `C:\windows\syswow64` 資料夾中同一可執行檔的 32 位元 版本的屬性中的資料填充可執行檔參數欄位。例如，如果選擇 `C:\windows\system32\cmd.exe`，則外掛程式將顯示 `C:\windows\syswow64\cmd.exe` 的參數。這種行為是由作業係統的特性決定的。<br><br>**用於以下事件類型**：<br>• **檔案修改**<br>• **網路事件**<br>• **處理程序：主控台互動輸入**<br>• **模組已載入**<br>• **登錄檔已修改**<br>• **DNS 記錄**<br>• **處理程序存取**<br>• **程式碼注入**<br>• **WMI 查詢**<br>• **管道**<br>• **LDAP**<br>• **AMSI** |
| **被排除的網路通信** | **規則名稱**<br>**方向**<br>**協定**<br>**原始套接字**<br>**協定編號**<br>**TLS 憑證**<br>**本機連接埠或範圍**<br>**遠端連接埠或範圍**<br>**本機位址**Kaspersky Endpoint Security 為其從網路流量中排除遙測的電腦的網路位址。<br>**遠端位址**Kaspersky Endpoint Security 為其從網路流量中排除遙測的電腦的網路位址。<br>IP 位址僅支援 IPv4 格式。<br>**應用程式**Kaspersky Endpoint Security 為其從網路流量中排除 EDR 遙測的應用程式的可執行檔清單。 |

| 參數 | 描述 |
| --- | --- |
| **被排除的檔案作業** | **規則名稱**<br>**檔案名稱或遮罩**檔案或資料夾的名稱或遮罩；當此檔案或資料夾被存取時，Kaspersky Endpoint Security 將套用排除規則。Kaspersky Endpoint Security 輸入遮罩時支援`*`和`?`字元。<br>**作業類型**<br>**先前的路徑**<br>Kaspersky Endpoint Security 可將規則觸發條件與邏輯 AND 相結合。<br>**處理**和**父處理程序**：<br>• **完全路徑**文件的完整路徑，包括其名稱和副檔名。Kaspersky Endpoint Security 輸入遮罩時支援環境變量以及 * 和 ? 字元。<br>• **命令行文字**用於執行檔案的命令。<br>• **描述**來自 RT_VERSION (VersionInfo) 資源的 FileDescription 參數的值。<br>• **原始檔案名稱**來自 RT_VERSION (VersionInfo) 資源的 OriginalFilename 參數的值。<br>• **版本**來自 RT_VERSION (VersionInfo) 資源的 FileVersion 參數的值。<br>• **檔案總和檢查碼**MD5 和 SHA256。<br>您也可以手動選擇檔案，應用程式將自動填寫所選檔案中的欄位。<br>在 64 位元作業係統中，您必須從 `C:\windows\system32` 資料夾手動輸入處理程序的 64 位元版本可執行檔案的參數，因為應用程式使用 `C:\windows\syswow64` 資料夾中同一可執行檔的 32 位元 版本的屬性中的資料填充可執行檔參數欄位。例如，如果選擇 `C:\windows\system32\cmd.exe`，則外掛程式將顯示 `C:\windows\syswow64\cmd.exe` 的參數。這種行為是由作業係統的特性決定的。 |
| **被排除的 DNS 作業** | **規則名稱**<br>Kaspersky Endpoint Security 可將規則觸發條件與邏輯 AND 相結合。<br>**處理**和**父處理程序**：<br>• **完全路徑**文件的完整路徑，包括其名稱和副檔名。Kaspersky Endpoint Security 輸入遮罩時支援環境變量以及 * 和 ? 字元。<br>• **命令行文字**用於執行檔案的命令。<br>• **描述**來自 RT_VERSION (VersionInfo) 資源的 FileDescription 參數的值。<br>• **原始檔案名稱**來自 RT_VERSION (VersionInfo) 資源的 OriginalFilename 參數的值。<br>• **版本**來自 RT_VERSION (VersionInfo) 資源的 FileVersion 參數的值。<br>• **檔案總和檢查碼**MD5 和 SHA256。<br>您也可以手動選擇檔案，應用程式將自動填寫所選檔案中的欄位。<br>在 64 位元作業係統中，您必須從 `C:\windows\system32` 資料夾手動輸入處理程序的 64 位元版本可執行檔案的參數，因為應用程式使用 `C:\windows\syswow64` 資料夾中同一可執行檔的 32 位元 版本的屬性中的資料填充可執行檔參數欄位。例如，如果選擇 `C:\windows\system32\cmd.exe`，則外掛程式將顯示 `C:\windows\syswow64\cmd.exe` 的參數。這種行為是由作業係統的特性決定的。<br>**DNS**：<br>• **DNS 伺服器 IP 位址**<br>• **查詢選項**<br>• **狀態**<br>• **網域名稱**<br>• **設定類型 ID**<br>• **回應資料** |

| 參數 | 描述 |
| --- | --- |
| **被排除的 LDAP 作業** | **規則名稱**<br>**LDAP 搜尋範圍**<br>**篩選器**<br>**LDAP 物件搜尋的可分辨名稱**<br>**物件屬性**<br><br>Kaspersky Endpoint Security 可將規則觸發條件與邏輯 AND 相結合。<br><br>**處理** 和 **父處理程序**：<br>• **完全路徑**文件的完整路徑，包括其名稱和副檔名。Kaspersky Endpoint Security 輸入遮罩時支援環境變量以及 * 和 ? 字元。<br>• **命令行文字**用於執行檔案的命令。<br>• **描述**來自 RT_VERSION (VersionInfo) 資源的 FileDescription 參數的值。<br>• **原始檔案名稱**來自 RT_VERSION (VersionInfo) 資源的 OriginalFilename 參數的值。<br>• **版本**來自 RT_VERSION (VersionInfo) 資源的 FileVersion 參數的值。<br>• **檔案總和檢查碼**MD5 和 SHA256。<br>您也可以手動選擇檔案，應用程式將自動填寫所選檔案中的欄位。<br><br>在 64 位元作業係統中，您必須從 `C:\windows\system32` 資料夾手動輸入處理程序的 64 位元版本可執行檔案的參數，因為應用程式使用 `C:\windows\syswow64` 資料夾中同一可執行檔的 32 位元 版本的屬性中的資料填充可執行檔參數欄位。例如，如果選擇 `C:\windows\system32\cmd.exe`，則外掛程式將顯示 `C:\windows\syswow64\cmd.exe` 的參數。這種行為是由作業係統的特性決定的。 |
| **被排除的處理程序存取查詢** | **規則名稱**<br>**作業類型**<br>**對處理程序的請求存取**<br>**呼叫堆疊偵錯**<br><br>Kaspersky Endpoint Security 可將規則觸發條件與邏輯 AND 相結合。<br><br>**處理**, **父處理程序**, **目標處理程序**, **來源處理程序檔案** 和 **目標處理程序檔案**。<br>• **完全路徑**文件的完整路徑，包括其名稱和副檔名。Kaspersky Endpoint Security 輸入遮罩時支援環境變量以及 * 和 ? 字元。<br>• **命令行文字**用於執行檔案的命令。<br>• **指定規則觸發條件和使用此規則的事件類型。**來自 RT_VERSION (VersionInfo) 資源的 FileDescription 參數的值。<br>• **原始檔案名稱**來自 RT_VERSION (VersionInfo) 資源的 OriginalFilename 參數的值。<br>• **版本**來自 RT_VERSION (VersionInfo) 資源的 FileVersion 參數的值。<br>• **檔案總和檢查碼**MD5 和 SHA256。<br>您也可以手動選擇檔案，應用程式將自動填寫所選檔案中的欄位。<br><br>在 64 位元作業係統中，您必須從 `C:\windows\system32` 資料夾手動輸入處理程序的 64 位元版本可執行檔案的參數，因為應用程式使用 `C:\windows\syswow64` 資料夾中同一可執行檔的 32 位元 版本的屬性中的資料填充可執行檔參數欄位。例如，如果選擇 `C:\windows\system32\cmd.exe`，則外掛程式將顯示 `C:\windows\syswow64\cmd.exe` 的參數。這種行為是由作業係統的特性決定的。 |

| 參數 | 描述 |
| --- | --- |
| **被排除的代碼注入** | **規則名稱**<br>**存取方法**<br>**呼叫堆疊**<br>**已修改的指令行**<br>**注入位址**<br>**注入的 DLL 名稱**<br><br>Kaspersky Endpoint Security 可將規則觸發條件與邏輯 AND 相結合。<br><br>**處理** 和 **父處理程序**：<br>• **完全路徑**文件的完整路徑，包括其名稱和副檔名。Kaspersky Endpoint Security 輸入遮罩時支援環境變量以及 * 和 ? 字元。<br>• **命令行文字**用於執行檔案的命令。<br>• **描述**來自 RT_VERSION (VersionInfo) 資源的 FileDescription 參數的值。<br>• **原始檔案名稱**來自 RT_VERSION (VersionInfo) 資源的 OriginalFilename 參數的值。<br>• **版本**來自 RT_VERSION (VersionInfo) 資源的 FileVersion 參數的值。<br>• **檔案總和檢查碼**MD5 和 SHA256。<br>您也可以手動選擇檔案，應用程式將自動填寫所選檔案中的欄位。<br><br>在 64 位元作業係統中，您必須從 `C:\windows\system32` 資料夾手動輸入處理程序的 64 位元版本可執行檔案的參數，因為應用程式使用 `C:\windows\syswow64` 資料夾中同一可執行檔的 32 位元 版本的屬性中的資料填充可執行檔參數欄位。例如，如果選擇 `C:\windows\system32\cmd.exe`，則外掛程式將顯示 `C:\windows\syswow64\cmd.exe` 的參數。這種行為是由作業係統的特性決定的。 |
| **被排除的 WMI 查詢** | **規則名稱**<br>**WMI 作業類型**<br>**遠端查詢**<br>**執行 WMI 指令的電腦的名稱**<br>**WMI 使用者帳戶**<br>**執行的 WMI 指令**<br>**WMI 命名空間**<br>**WMI 事件消費者篩選器**<br>**已建立的 WMI 事件消費者的名稱**<br>**WMI 事件消費者的源代碼**<br><br>Kaspersky Endpoint Security 可將規則觸發條件與邏輯 AND 相結合。<br><br>**處理** 和 **父處理程序**：<br>• **完全路徑**文件的完整路徑，包括其名稱和副檔名。Kaspersky Endpoint Security 輸入遮罩時支援環境變量以及 * 和 ? 字元。<br>• **命令行文字**用於執行檔案的命令。<br>• **描述**來自 RT_VERSION (VersionInfo) 資源的 FileDescription 參數的值。<br>• **原始檔案名稱**來自 RT_VERSION (VersionInfo) 資源的 OriginalFilename 參數的值。<br>• **版本**來自 RT_VERSION (VersionInfo) 資源的 FileVersion 參數的值。<br>• **檔案總和檢查碼**MD5 和 SHA256。<br>您也可以手動選擇檔案，應用程式將自動填寫所選檔案中的欄位。<br><br>在 64 位元作業係統中，您必須從 `C:\windows\system32` 資料夾手動輸入處理程序的 64 位元版本可執行檔案的參數，因為應用程式使用 `C:\windows\syswow64` 資料夾中同一可執行檔的 32 位元 版本的屬性中的資料填充可執行檔參數欄位。例如，如果選擇 `C:\windows\system32\cmd.exe`，則外掛程式將顯示 `C:\windows\syswow64\cmd.exe` 的參數。這種行為是由作業係統的特性決定的。 |

| 參數 | 描述 |
| --- | --- |
| **被排除的管道作業** | **規則名稱**<br>**管道名稱**<br>**作業類型**<br><br>Kaspersky Endpoint Security 可將規則觸發條件與邏輯 AND 相結合。<br><br>**處理** 和 **父處理程序**：<br>• **完全路徑**文件的完整路徑，包括其名稱和副檔名。Kaspersky Endpoint Security 輸入遮罩時支援環境變量以及 * 和 ? 字元。<br>• **命令行文字**用於執行檔案的命令。<br>• **描述**來自 RT_VERSION (VersionInfo) 資源的 FileDescription 參數的值。<br>• **原始檔案名稱**來自 RT_VERSION (VersionInfo) 資源的 OriginalFilename 參數的值。<br>• **版本**來自 RT_VERSION (VersionInfo) 資源的 FileVersion 參數的值。<br>• **檔案總和檢查碼**MD5 和 SHA256。<br>您也可以手動選擇檔案，應用程式將自動填寫所選檔案中的欄位。<br><br>在 64 位元作業係統中，您必須從 `C:\windows\system32` 資料夾手動輸入處理程序的 64 位元版本可執行檔案的參數，因為應用程式使用 `C:\windows\syswow64` 資料夾中同一可執行檔的 32 位元 版本的屬性中的資料填充可執行檔參數欄位。例如，如果選擇 `C:\windows\system32\cmd.exe`，則外掛程式將顯示 `C:\windows\syswow64\cmd.exe` 的參數。這種行為是由作業係統的特性決定的。 |
| **被排除的登錄檔變更** | **規則名稱**<br>**作業類型**<br>**路徑**<br>**值名稱**<br>**機碼值**<br>**登錄檔檔案全稱**<br><br>Kaspersky Endpoint Security 可將規則觸發條件與邏輯 AND 相結合。<br><br>**處理** 和 **父處理程序**：<br>• **完全路徑**文件的完整路徑，包括其名稱和副檔名。Kaspersky Endpoint Security 輸入遮罩時支援環境變量以及 * 和 ? 字元。<br>• **命令行文字**用於執行檔案的命令。<br>• **描述**來自 RT_VERSION (VersionInfo) 資源的 FileDescription 參數的值。<br>• **原始檔案名稱**來自 RT_VERSION (VersionInfo) 資源的 OriginalFilename 參數的值。<br>• **版本**來自 RT_VERSION (VersionInfo) 資源的 FileVersion 參數的值。<br>• **檔案總和檢查碼**MD5 和 SHA256。<br>您也可以手動選擇檔案，應用程式將自動填寫所選檔案中的欄位。<br><br>在 64 位元作業係統中，您必須從 `C:\windows\system32` 資料夾手動輸入處理程序的 64 位元版本可執行檔案的參數，因為應用程式使用 `C:\windows\syswow64` 資料夾中同一可執行檔的 32 位元 版本的屬性中的資料填充可執行檔參數欄位。例如，如果選擇 `C:\windows\system32\cmd.exe`，則外掛程式將顯示 `C:\windows\syswow64\cmd.exe` 的參數。這種行為是由作業係統的特性決定的。 |
| **被排除的裝置操作** | **規則名稱**<br>**裝置類型**<br><br>**裝置 ID**<br><br>**裝置名稱** |

# 例 1。被排除的處理程序

若要從遙測中排除協力廠商應用程式（處理程序）事件，請在**被排除的處理程序**頁簽上開啟 EDR 遙測排除視窗並添加應用程式的可執行檔。

Kaspersky Endpoint Security 可將規則觸發條件與邏輯 AND 相結合。

Kaspersky Endpoint Security 輸入遮罩時支援環境變量以及`*`和`?`字元。範例：

- `C:\Program Files\*\notepad++.exe`
- `%ProgramFiles(x86)%\Notepad++\notepad++.exe`。




排除處理程序

例 1。檔案修改

如果您經常在 Notepad++ 應用程式中編輯指令碼，並且想要排除相應指令碼的修改事件，請新增 Notepad++ 可執行檔到遙測排除項目。

如下指定設定：

- **完全路徑**： `C:\Program Files\Notepad++\notepad++.exe`。
- **SHA256**: 64F7A36C01E79CD4B041E8A8607DFF06D5B606D36E3DFF9CFB5FFFA22D14D34。
- **用於以下事件類型**： 檔案修改。

例 2。網路事件

如果您使用 WinSCP 應用程式管理遠端伺服器上的檔案，並且想要排除網路事件，請新增 WinSCP 可執行檔到遙測排除項目。

如下指定設定：

- **完全路徑**： `C:\Program Files (x86)\WinSCP\WinSCP.exe`。
- **SHA256**：47204338f0e092057024c9186f228c02417e917777f3e841d52b58251a956a74（可選）。
- **用於以下事件類型**： 網路事件。

## 例 2。被排除的網路通訊

若要從遙測中排除遠端服務連線事件，請在**被排除的網路通信**頁簽上開啟 EDR 遙測排除視窗並新增連線設定：協定、連接埠、方向、IP 位址、TLS 憑證等。

Kaspersky Endpoint Security 可將規則觸發條件與邏輯 AND 相結合。

> 您不能指定子網路位址（例如，10.28.0.0/24）。該應用程式僅允許指定一個 IP 位址（例如，10.28.0.105）。




網路通訊排除項目

如果您使用公司 Web 伺服器，想要在連線到該 Web 伺服器時排除瀏覽器事件，請將伺服器的 IP 位址和瀏覽器的執行檔新增至遙測排除項目。

如下指定設定：

- **協定**：TCP。
- **遠端連接埠或範圍**：443。

- **遠端位址**：10.28.0.105。
- **應用程式**： `C:\Program Files (x86)\Google\Chrome\Application\chrome.exe`； `C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe`。

## 例 3。被排除的檔案操作

為了從遙測中排除涉及受信任檔案操作的事件，請在在**被排除的檔案作業**頁簽上開啟 EDR 遙測排除項目視窗並新增受信任的檔案。

Kaspersky Endpoint Security 可將規則觸發條件與邏輯 AND 相結合。




排除檔案操作

如果應用程式寫入日誌並且您想要排除日誌檔案修改事件，請從遙測中新增日誌檔案和應用程式的可執行檔。

如下指定設定：

- **檔案名稱或遮罩**： `C:\Apache24\logs\error.log`。
- **作業類型**： 檔案修改。
- **完全路徑**： `C:\Apache24\bin\httpd.exe`。
- **SHA256**: 64F7A36C01E79CD4B041E8A8607DFF06D5B606D36E3DFF9CFB5FFFA22D14D34。

## 例 4。被排除的登錄檔修改

若要從遙測中排除登錄檔修改事件，請在**被排除的登錄檔變更**頁簽上開啟 EDR 遙測排除項目視窗並新增登錄機碼。

Kaspersky Endpoint Security 可將規則觸發條件與邏輯 AND 相結合。

如果應用程式經常修改其登錄檔值，並且您想要從遙測中排除這些登錄檔修改事件，請將登錄機碼和應用程式的可執行檔新增至遙測排除項目。

如下指定設定：

- **作業類型**： 修改。
- **路徑**： HKEY_LOCAL_MACHINE\SOFTWARE\SimonTatham\PuTTY64。
- **完全路徑**： `C:\Program Files\PuTTY\putty.exe`。
- **SHA256**: 64F7A36C01E79CD4B041E8A8607DFF06D5B606D36E3DFF9CFB5FFFA22D14D34。

# KATA Sandbox

Kaspersky Anti Targeted Attack Platform 包括 Sandbox （KATA Sandbox）元件。*Sandbox* 技術可讓您偵測電腦上的進階威脅。Sandbox 會分析物件行為以偵測惡意行動和組織的 IT 基礎架構上的針對性攻擊所特有的活動。Sandbox 會分析和掃描部署了 Microsoft Windows 作業系統的虛擬影像的特殊伺服器（Sandbox 伺服器）上的物件。有關解決方案的詳細資訊，請參閱 Kaspersky Anti Targeted Attack Platform 說明。

若要啟動 KATA Sandbox，需要包含 KATA 或 KEDR 功能的產品授權金鑰。有關可用功能的詳細資訊，請參閱 Kaspersky Anti Targeted Attack Platform 說明。

KATA Sandbox 允許以下列模式掃描檔案：

- *手動*。使用者從內容功能表（**傳送到 Sandbox**）中手動提交檔案進行掃描。將檔案傳送到 Sandbox 時，應用程式也會使用防毒資料庫掃描檔案。
- *自動*。應用程式自動偵測物件並將其提交到 Sandbox 進行掃描。

將檔案傳送到 Sandbox 後，使用者仍然可以存取該檔案。Kaspersky Endpoint Security 記錄相應的事件並將該事件傳送至卡巴斯基安全管理中心和 Kaspersky Anti Targeted Attack Platform 主控台。如果 Sandbox 偵測到惡意活動，Kaspersky Endpoint Security 會自動執行 威脅回應操作（例如，它會刪除物件並啟動關鍵區域掃描）。

若要讓 KATA Sandbox 在手動模式下執行，必須部署 Kaspersky Anti Targeted Attack Platform 7.0 或更高版本。若要讓 KATA Sandbox 在自動模式下運行，必須部署 Kaspersky Anti Targeted Attack Platform 8.0 或更高版本。




從內容功能表掃描 KATA Sandbox

# 內建代理與 KATA Sandbox 整合

與 KATA Sandbox 元件整合需要新增 Sandbox 元件。您可以在安裝或者升級期間以及使用*變更應用程式元件*工作時選擇 Sandbox 元件。

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。該元件只可以使用卡巴斯基安全管理中心網頁主控台進行管理。您不能使用管理主控台 (MMC) 管理此元件。

*要啟用或停用與 KATA Sandbox 的整合：*

1. 在網頁主控台的主視窗中，選擇**資產（裝置）→政策和設定檔**。
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. 使用“**Sandbox 整合已啟用**“切換開關可啟用或停用元件。

6. 選取 KATA Sandbox 執行模式：

   - **手動**使用者從內容功能表（**傳送到 Sandbox**）中手動提交檔案進行掃描。
   - **自動**應用程式自動偵測物件並將其提交到 Sandbox 進行掃描。
   - **組合**

7. 點擊"**連線設定**"連接。

8. 配置中心節點伺服器連線設定：

   - **逾時 (毫秒)**中央節點伺服器連線逾時。配置的逾時經過後，Kaspersky Endpoint Security 會傳送請求給下一個伺服器。如果您的連線速度慢或者連線不穩定，您可以增加伺服器的連線逾時。建議的請求逾時為 0.5 秒鐘或更短。
   - **請求佇列**請求佇列資料夾大小在 Sandbox 中傳送多個物件進行掃描時，Kaspersky Endpoint Security 會建立一個請求佇列。預設情況下，請求佇列資料夾大小限制為 100 MB。在達到最大的大小後，Sandbox 會停止向佇列新增請求並將相應事件傳送到卡巴斯基安全管理中心。您可以根據伺服器配置來設定請求佇列資料夾大小。
   - **伺服器 TLS 憑證**若要配置與中央節點伺服器的受信任連線，您必須準備 TLS 憑證。然後，您必須使用政策將憑證新增至電腦。您還需要將憑證新增到中央節點伺服器。
   - **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。

9. 在"**連線到 Sandbox 伺服器**"塊中，點擊"**新增**"按鈕。

10. 這會開啟一個視窗，在視窗中，輸入 Central Node 伺服器位址 (IPv4, IPv6, DNS) 和連接埠。

    有關部署虛擬影像和配置 Central Node 伺服器的詳情，請參見 Kaspersky Anti Targeted Attack Platform 說明。

11. 儲存變更。若要在電腦上套用該政策，請關閉掛鎖。

    因此，Sandbox 元件被啟用。透過檢視"*應用程式元件狀態報告*"來檢查元件的運行狀態。您還可以在 Kaspersky Endpoint Security 的本地介面中的報告中檢視元件的運行狀態。"**Sandbox**"元件將新增到 Kaspersky Endpoint Security 元件清單中。

## 配置威脅回應操作

如果 Sandbox 偵測到惡意活動，Kaspersky Endpoint Security 會自動執行 威脅回應操作（例如，它會刪除物件並啟動關鍵區域掃描）。

*配置威脅回應操作：*

1. 在網頁主控台的主視窗中，選擇**資產（裝置）→ 政策和設定檔**。

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"**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 會建立備份副本以防物件以後需要還原。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 會掃描內核記憶體、執行處理序和磁碟的開啟磁區。

   - **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、掃描範圍和偵測到 IOC 後的動作：刪除物件，執行*關鍵區域掃描*工作。若要修改 "*IOC 掃描*"工作的其它設定，請前往工作設定。

6. 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**如果選擇該選項，則 Kaspersky Endpoint Security 僅在電腦的關鍵檔案區域執行 IOC 掃描：內核記憶體和開機磁區。

   - **電腦的系統磁碟機上的檔案區域**如果選擇該選項，則 Kaspersky Endpoint Security 會在電腦的系統磁碟機上執行 IOC 掃描。

7. 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**執行模式，只要偵測到威脅 Kaspersky Endpoint Security 就執行 *IOC 掃描*工作。

   - **僅在電腦空閒時執行**執行模式，如果熒幕防護程式啟動或者熒幕被鎖定則 Kaspersky Endpoint Security 執行 *IOC 掃描*工作。如果使用者解鎖了電腦，Kaspersky Endpoint Security 會暫停工作。這意味著工作可能會費時數天完成。

8. 配置進階工作設定：*IOC 掃描*。

9. 儲存變更。若要在電腦上套用該政策，請關閉掛鎖。

# EDR (KATA) 的 KEA 到 KES 遷移指南

從版本 12.1 開始，Kaspersky Endpoint Security for Windows 包含一個內建代理，用於管理 Kaspersky Endpoint Detection and Response 元件，作為 Kaspersky Anti Targeted Attack Platform 解決方案的一部分。您再也無需分開 Kaspersky Endpoint Agent 應用程式來使用 EDR (KATA)。Kaspersky Endpoint Agent 的所有功能將由 Kaspersky Endpoint Security 執行。Kaspersky Anti Targeted Attack Platform 伺服器上的負載將保持不變。

當您在安裝了 Kaspersky Endpoint Agent 的電腦上部署 Kaspersky Endpoint Security 時，Kaspersky Anti Targeted Attack Platform (EDR) 解決方案將繼續與 Kaspersky Endpoint Security 一起工作。此外，Kaspersky Endpoint Agent 將被從電腦移除。當您將 Kaspersky Endpoint Security 更新到版本 12.1 或者更高版本時，系統中會發生相同的行為。

Kaspersky Endpoint Security 與 Kaspersky Endpoint Agent 不相容。您不能在同一台電腦上同時安裝這些應用程式。

Kaspersky Endpoint Security 必須滿足以下條件才能作為 Endpoint Detection and Response (KATA) 的一部分工作：

- Kaspersky Anti Targeted Attack Platform 版本 5.0 或更高版本。
- 卡巴斯基安全管理中心版本 14.2 或更高版本（包括網路代理）。在早期版本的卡巴斯基安全管理中心中，無法啟動 Endpoint Detection and Response (KATA) 功能。

將 [KES+KEA] 配置遷移到 [KES+built-in agent] for EDR (KATA) 的步驟

1. **升級 Kaspersky Endpoint Security 管理外掛程式**

   EDR (KATA) 元件可以使用 Kaspersky Endpoint Security 管理外掛程式版本 12.1 或更高版本進行管理。根據您使用的卡巴斯基安全管理中心主控台類型，更新管理主控台 (MMC) 中的管理外掛程式或網頁主控台中的 Web 外掛程式。

2. **遷移政策和工作**

   將 Kaspersky Endpoint Agent 設定傳輸到 Kaspersky Endpoint Security for Windows。下列選項可用：

   - 用於從 Kaspersky Endpoint Agent 遷移到 Kaspersky Endpoint Security 的精靈。從 Kaspersky Endpoint Agent 遷移到 Kaspersky Endpoint Security 的精靈僅適用於網頁主控台

     **如何將政策和工作設定從 Kaspersky Endpoint Agent 遷移到網頁主控台中的 Kaspersky Endpoint Security**

     在網頁主控台的主視窗中，選擇**操作 → 從 Kaspersky Endpoint Agent 遷移**。

     這會執行政策和工作遷移精靈。按照精靈的說明進行操作。

     步驟 1. 政策遷移

     遷移精靈會建立一個新政策，將 Kaspersky Endpoint Security 和 Kaspersky Endpoint Agent 政策的設定合併。在政策清單中，選擇您想將其設定與 Kaspersky Endpoint Security 政策合併的 Kaspersky Endpoint Agent 政策。點擊 Kaspersky Endpoint Agent 政策以選擇您想與其合併設定的 Kaspersky Endpoint Security 政策。確保選擇了正確的政策然後前往下一步。

     步驟 2. 工作遷移

     遷移精靈不支援 EDR (KATA) 工作。略過此步驟。

     步驟 3. 精靈完成

     結束精靈。作為精靈的結果，將建立新的 Kaspersky Endpoint Security 政策。政策將合併 Kaspersky Endpoint Security 和 Kaspersky Endpoint Agent 的設定。政策稱為 *<Kaspersky Endpoint Security 政策名稱> & <Kaspersky Endpoint Agent 政策名稱>*。新政策的狀態為*非作用中*。若要繼續，將 Kaspersky Endpoint Agent 和 Kaspersky Endpoint Security 政策的狀態變更為*非作用中*，然後啟動新合併的政策。

網頁主控台中的遷移精靈略過了以下政策設定並且不遷移它們：

- 設定修改禁止 **連線設定**（“鎖”）。

  預設情況下，設定可以被修改（“鎖”是開啟的）。因此，設定不會套用到電腦上。您必須禁止修改設定並關閉“鎖”。

- 加密容器。

  如果您使用雙向身分驗證連線到中央節點伺服器，則必須重新新增加密容器。

由於遷移精靈不遷移這些設定，您在將電腦連線到 Central Node 伺服器時可能會遇到錯誤。若要修復錯誤，您需要轉到政策內容並配置連線設定。

- 標準政策和工作批量轉換精靈。政策和工作批量轉換精靈僅在管理主控台 (MMC) 中可用。有關政策和工作批量轉換精靈的詳細資訊，請參閱卡巴斯基安全管理中心說明。

為確保 Kaspersky Endpoint Security 在伺服器上正常工作，建議將對伺服器功能重要的檔案新增到受信任區域。對於 SQL 伺服器，您必須新增 MDF 和 LDF 資料庫檔案。對於 Microsoft Exchange 伺服器，您必須新增 CHK、EDB、JRS、LOG 和 JSL 檔案。您可以使用遮罩，例如，`C:\Program Files (x86)\Microsoft SQL Server\*.mdf`。

從 Kaspersky Endpoint Security 12.6 for Windows 開始，掃描排除項目和受信任應用程式被新增到受信任區域。預先定義的掃描排除項目和受信任應用程式有助於在 SQL 伺服器、Microsoft Exchange 伺服器和 System Center Configuration Manager 上快速設定 Kaspersky Endpoint Security。這意味著您無需在伺服器上為應用程式手動設定受信任區域。

EDR 遙測排除項目不會從 Kaspersky Endpoint Agent 政策遷移到 Kaspersky Endpoint Security 政策。Kaspersky Endpoint Security 有自己的排除工具：受信任應用程式。Kaspersky Endpoint Security 的操作經過最佳化，與 Kaspersky Endpoint Agent 相比，缺少單個 EDR 遙測排除項目不會對您的電腦造成任何額外負載。Kaspersky Endpoint Security 不僅將遙測用於 EDR (KATA)，還用於應用程式防護元件的運行。因此，無需傳輸單個 EDR 遙測排除項目。如果您經歷電腦效能下降，請檢查應用程式的運行情況（請參閱步驟 7 檢查效能）。

### 3 授權 EDR (KATA) 功能

要將 Kaspersky Endpoint Security 作為 Kaspersky Anti Targeted Attack Platform 解決方案的一部分啟動，您需要單獨的 Kaspersky Endpoint Detection and Response (KATA) 附加產品授權。您可以使用“*新增金鑰*”工作新增金鑰。結果，兩個金鑰將被新增到應用程式：*Kaspersky Endpoint Security* 和 *Kaspersky Endpoint Detection and Response (KATA)*。

在具有先前啟動的 EDR Optimum 或 EDR Expert 功能的電腦上許可 Kaspersky Endpoint Detection and Response (KATA) 附加涉及以下特殊注意事項：

- 如果使用的是 *金鑰檔案*授權具有 EDR Optimum 或 EDR Expert 功能的 Kaspersky Endpoint Security，您無法為 Kaspersky Endpoint Detection and Response (KATA) 附加新增單獨金鑰。您可以切換到使用啟動碼進行許可，或者聯絡您的服務提供商以獲取新的金鑰檔案來啟動 Kaspersky Endpoint Security 和 EDR 功能。服務提供商將提供一個或多個用於許可的金鑰檔案。

- 如果您使用 *金鑰檔案*授權沒有 EDR Optimum 或 EDR Expert 功能的 Kaspersky Endpoint Security，您可以為 Kaspersky Endpoint Detection and Response (KATA) 附加新增單獨金鑰，而無需重新發布金鑰檔案。

- 如果您使用*啟動碼*授權，則卡巴斯基啟動伺服器將自動重新發布金鑰，EDR (KATA) 功能將自動可用。在這種情況下，EDR Optimum 和 EDR Expert 將被停用。

- Kaspersky Endpoint Security 允許您新增最多兩個啟動金鑰：Kaspersky Endpoint Security 金鑰和附加類型金鑰。您還可以新增最多兩個備用金鑰。一個 Kaspersky Endpoint Security 備用金鑰和一個附加類型備用金鑰。

**4 安裝/升級 Kaspersky Endpoint Security 應用程式**

要在應用程式安裝或升級期間遷移 EDR (KATA) 功能，建議使用遠端安裝工作。建立遠端安裝工作時，您需要在安裝套件設定中選擇 EDR（KATA）元件。

您還可以使用以下方法升級應用程式：

- 使用 Kaspersky 更新服務。

- 本機使用安裝精靈。

當在安裝了 Kaspersky Endpoint Agent 的電腦上升級應用程式時，Kaspersky Endpoint Security 支援自動選擇元件。自動選擇元件取決於升級應用程式的使用者帳戶的權限。

如果在系統帳戶 (SYSTEM) 下使用 EXE 或 MSI 檔案升級 Kaspersky Endpoint Security，Kaspersky Endpoint Security 將獲得對 Kaspersky 解決方案的目前產品授權的存取權限。因此，如果電腦安裝了 Kaspersky Endpoint Agent 且啟動了 EDR (KATA) 解決方案，Kaspersky Endpoint Security 安裝程式將自動配置元件集合並選擇 EDR (KATA) 元件。這將使得 Kaspersky Endpoint Security 切換到使用內建代理並刪除 Kaspersky Endpoint Agent。在系統帳戶 (SYSTEM) 下執行 MSI 安裝程式通常在透過 Kaspersky 更新服務升級或透過卡巴斯基安全管理中心部署安裝套件時進行。

如果在沒有權限的帳戶下使用 MSI 檔案升級 Kaspersky Endpoint Security，Kaspersky Endpoint Security 將缺少對 Kaspersky 解決方案的目前產品授權的存取權限。在這種情況下，Kaspersky Endpoint Security 會根據 Kaspersky Endpoint Agent 的一組元件自動選擇元件。此後，Kaspersky Endpoint Security 將切換到使用內建代理並刪除 Kaspersky Endpoint Agent。

Kaspersky Endpoint Security 支援在不重啟電腦的情況下升級。您可以選擇政策屬性中的應用程式升級模式。

**5 檢查應用程式運行情況**

如果安裝或升級後應用程式後電腦在卡巴斯基安全管理中心主控台中具有"*緊急*"狀態：

- 請確保電腦安裝了網路代理 13.2或更高版本。

- 透過檢視"*應用程式元件狀態報告*"來檢查內建代理的運行狀態。如果元件的狀態為"*未安裝*"，請使用*變更應用程式元件*工作來安裝元件。如果一個元件的狀態為 *產品授權不支援*，確保您已啟動內建代理功能。

- 請確保在 Kaspersky Endpoint Security for Windows 的新政策中接受卡巴斯基安全網路聲明。

**6 檢查與 Kaspersky Anti Targeted Attack Platform 伺服器的連線**

檢查與 Kaspersky Anti Targeted Attack Platform 伺服器的連線。為此，請執行以下操作：

1. 檢查您是否擁有有效的憑證。

2. 檢查伺服器連線設定。

3. 檢查事件記錄。

   如果建立了與伺服器的連線，應用程式將傳送事件 *成功連線到 EDR Expert 伺服器*。如果沒有成功連線事件並且沒有連線錯誤事件，檢查事件記錄設定並為 Endpoint Detection and Response (KATA) 啟用事件傳送。

伺服器連線狀態不會影響卡巴斯基安全管理中心主控台中的電腦狀態。因此，如果沒有連線到伺服器，電腦仍然可以擁有"*確定*"狀態。檢查事件日誌以驗證與伺服器的連線。

**7 檢查效能**

如果您的電腦在安裝或更新應用程式後效能下降，您可以最佳化資料傳輸。為此，請執行以下操作：

1. 停用 EDR (KATA) 元件 並檢查效能下降是由於 EDR (KATA)。
2. 針對受信任的應用程式，關閉主控台輸入操作的遙測收集（預設啟用）。
3. 將降低電腦效能的應用程式新增到受信任的應用程式清單。
4. 聯絡卡巴斯基技術支援。支援專家將幫助您在 Kaspersky Anti Targeted Attack Platform 中配置遙測過濾。這將減少流量。如果您的電腦效能受到某個應用程式的影響，請在請求中附上該應用程式的分發套件。

# Endpoint Detection and Response Expert（本地部署）

Kaspersky Endpoint Security for Windows 支援與 Kaspersky Endpoint Detection and Response Expert (on-premise) 解決方案整合。*Kaspersky Endpoint Detection and Response Expert（本地部署）*是一款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（本地部署）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 (on-premise) 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 (on-premise) 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 (on-premise) 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 使用以下威脅情報工具：

- 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 (on-premise) 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 (on-premise) 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。

### 用於使用 EDR Expert (on-premise) 的 Kaspersky Endpoint Security 配置

以下配置可用於使用 EDR Expert (on-premise)：

- **[KES+內建代理]**。在此配置中，Kaspersky Endpoint Security 既充當確保電腦安全的應用程式，又充當使用 EDR Expert (on-premise) 的應用程式。Kaspersky Endpoint Security 12.11 for Windows 或更高版本提供 EDR Expert (on-premise) 的內建代理。
- **【協力廠商 EPP EDR Agent】**。在此配置中，IT 基礎結構的安全性由協力廠商 Endpoint Protection Platform (EPP) 提供。與 EDR Expert (on-premise) 的交互由 Kaspersky Endpoint Security 在 Endpoint Detection and Response Agent (EDR Agent) 配置中提供。在此配置中，EDR Agent 與協力廠商 EPP應用程式相容。EDR Expert (on-premise) 的 EDR Agent 在 Kaspersky Endpoint Security 12.11 for Windows 或更高版本中可用。

## 內建代理與 EDR Expert (on-premise) 整合

要與 Kaspersky Endpoint Detection and Response Expert (on-premise) 解決方案整合，您必須新增 Endpoint Detection and Response Expert (on-premise) 元件，並配置 Kaspersky Endpoint Security。

EDR Optimum、EDR Expert 和 EDR Expert (on-premise) 元件彼此不相容。

Endpoint Detection and Response Expert (on-premise) 要工作必須滿足以下條件：

- OSMP（Open Single Management Platform已安裝。
- 應用程式被啟動，功能受產品授權覆蓋。
- Endpoint Detection and Response Expert (on-premise) 元件已開啟。
- 確保 EDR Expert (on-premise) 運作的應用程式元件已啟用並運作。以下元件可確保 EDR Expert (on-premise) 的操作：
  - 檔案威脅防護。
  - Web 威脅防護。
  - 郵件威脅防護。
  - 弱點利用防禦。
  - 行為偵測。
  - 主機入侵防禦。
  - 修復引擎。
  - 適應性異常控制。

設定 EDR Expert (on-premise) 整合涉及以下步驟：

1. **安裝 EDR Expert (on-premise) 元件**

   您可以在安裝或者升級期間以及使用*變更應用程式元件*工作時選擇 EDR Expert (on-premise) 元件。

   > 您必須重新啟動電腦以完成升級含新元件的應用程式。

2. **啟動 Kaspersky Endpoint Detection and Response Expert (on-premise)**

   您需要單獨購買 EDR Expert (on-premise)（Kaspersky Endpoint Detection and Response Expert (on-premise) 附加元件）的產品授權。

   為 Kaspersky Endpoint Detection and Response Expert (on-premise) 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 (on-premise)。

   獨立 Endpoint Detection and Response Expert (on-premise) 功能的授權和 Kaspersky Endpoint Security 的授權一樣。

   確保 EDR Expert (on-premise) 功能包括在產品授權中且在應用程式的本機介面中執行。

3. **連線到遙測資料收集伺服器和回應伺服器**

   Kaspersky Endpoint Detection and Response Expert (on-premise) 需要 Kaspersky Endpoint Security 與兩台伺服器之間建立可信任連線：

   - *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。

   要配置可信連線，您必須使用 TLS 憑證。您可以在開放式單一管理平台上取得 TLS 憑證（請參閱 Kaspersky Endpoint Detection and Response Expert （內部部署版）說明）。然後您必須將 TLS 憑證新增到 Kaspersky Endpoint Security（參見下面的說明）。

   預設情況下，Kaspersky Endpoint Security 僅檢查伺服器 TLS 憑證。為了使連線更安全，您可以額外啟用在伺服器上進行電腦驗證（雙向身分驗證）。要啟用此驗證，您必須在伺服器和 Kaspersky Endpoint Security 設定中開啟雙向身分驗證。要使用雙向身分驗證，您還需要一個加密容器。*加密容器*是一個帶有憑證和私鑰的 PFX 存檔。您可以在開放式單一管理平台上取得加密容器（請參閱 Kaspersky Endpoint Detection and Response Expert （內部部署版）說明）。

   **如何使用網頁主控台將 Kaspersky Endpoint Security 電腦連線到 EDR Expert (on-premise)**

   1. 在網頁主控台的主視窗中，選擇**資產（裝置）** → **政策和設定檔**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 (on-premise)"**。
   5. 開啟**"Endpoint Detection and Response Expert (on-premise) 已啟用"**開關。
   6. 若要設定 EDR Expert (on-premise)，請從解決方案清單中選取 **Endpoint Detection and Response Expert（版本 8.0 或者更高版本）**。

7. 配置 *遙測資料收集伺服器* 連線：

   a. 在"**遙測資料收集伺服器連線**"塊中，點擊"**連線設定**"連接。

   b. 配置遙測資料收集伺服器連線：

   - **逾時（秒）**伺服器回應最長逾時。當逾時用完時，Kaspersky Endpoint Security 會嘗試連線到不同的伺服器。
   - **伺服器憑證**用於與伺服器建立可信連線的 TLS 憑證。您可以在開放式單一管理平台上取得 TLS 憑證（請參閱 Kaspersky Endpoint Detection and Response Expert （內部部署版）說明）。
   - **使用雙向身分驗證**在 Kaspersky Endpoint Security 和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。您可以在開放式單一管理平台上取得加密容器（請參閱 Kaspersky Endpoint Detection and Response Expert （內部部署版）說明）。配置伺服器設定後，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。

   c. 點擊"**確定**"。

   d. 新增遙測資料收集伺服器。為此，請指定伺服器位址（IPv4、IPv6）和連線到伺服器的連接埠。

   您可以新增多個遙測資料收集伺服器位址。Kaspersky Endpoint Security 嘗試連線到第一個 IP 位址的伺服器。如果無法建立連線，Kaspersky Endpoint Security 將嘗試連線到清單中的第二個 IP 位址，依此類推。

   e. 如果有需要的話，配置遙測。

8. 配置*回應伺服器*連線：

   a. 在"**連線至回應伺服器**"區塊中，配置**傳送同步請求到伺服器的時間間隔 (分)**設定。傳送到伺服器的同步請求的頻率。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。

   b. 點擊"**連線設定**"連接。

   c. 配置回應伺服器連線：

   - **逾時（秒）**伺服器回應最長逾時。當逾時用完時，Kaspersky Endpoint Security 會嘗試連線到不同的伺服器。
   - **伺服器憑證**用於與伺服器建立可信連線的 TLS 憑證。您可以在開放式單一管理平台上取得 TLS 憑證（請參閱 Kaspersky Endpoint Detection and Response Expert （內部部署版）說明）。
   - **使用雙向身分驗證**在 Kaspersky Endpoint Security 和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。您可以在開放式單一管理平台上取得加密容器（請參閱 Kaspersky Endpoint Detection and Response Expert （內部部署版）說明）。配置伺服器設定後，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。

d. 點擊**"確定"**。

e. 新增回應伺服器。為此，請指定伺服器位址（IPv4、IPv6）和連線到伺服器的連接埠。

您可以新增多個回應伺服器位址。Kaspersky Endpoint Security 嘗試連線到第一個 IP 位址的伺服器。如果無法建立連線，Kaspersky Endpoint Security 將嘗試連線到清單中的第二個 IP 位址，依此類推。

9. 儲存變更。若要在電腦上套用該政策，請關閉掛鎖。

因此，電腦被加入到開放單一管理平台（OSMP）中。透過檢視"*應用程式元件狀態報告*"來檢查元件的運行狀態。您還可以在 Kaspersky Endpoint Security 的本地介面中的報告中檢視元件的運行狀態。**"Endpoint Detection and Response Expert (on-premise)** "元件將新增到 Kaspersky Endpoint Security 元件清單中。

# 配置 EDR Expert (on-premise) 遙測設定

*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）。

*要配置遙測設定，請執行下列步驟：*

1. 在網頁主控台的主視窗中，選擇**資產（裝置）→政策和設定檔**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 (on-premise)** "。
5. 若要設定 EDR Expert (on-premise)，請從解決方案清單中選取 **Endpoint Detection and Response Expert（版本 8.0 或者更高版本）**。
6. 確保 **將遙測資料傳送至遙測資料收集伺服器** 核取方塊已在 **資料傳輸設定** 區塊中被選中。
7. 如有必要，選中**"僅傳送具有 IOA 的遙測"**核取方塊。*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。

8. 如有必要，請在**資料傳輸設定**塊中配置與伺服器設定同步：

   - **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. 如有必要，在**請求節流**塊中選擇**啟用請求節流**核取方塊。

   該功能有助於最佳化伺服器負載。如果選中該核取方塊，應用程式將限制傳輸的事件。如果事件數量超過配置的限制，Kaspersky Endpoint Security 將停止傳送事件。

10. 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%。

11. 在 **連線至回應伺服器** 區塊中，輸入**傳送同步請求到伺服器的時間間隔 (分)**參數的值。

12. 傳送到伺服器的同步請求的頻率。在同步期間，Kaspersky Endpoint Security 傳送有關被修改應用程式設定和工作的資訊。

13. 儲存變更。若要在電腦上套用該政策，請關閉掛鎖。

# EDR Expert (on-premise) 遙測排除項目

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。

使用過多的規則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。

*在網頁主控台和雲端主控台中建立遙測排除項目：*

1. 在網頁主控台的主視窗中，選擇**資產（裝置）→ 政策和設定檔**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 (on-premise) 遙測**”標籤。
6. 在”**一般排除項目**”塊中，點擊”**新增**”按鈕。

   開啟“**新增排除規則**”視窗。

7. 如有必要，可變更規則的狀態。預設情況下規則已啟用。

8. 輸入規則的名稱。

9. 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。

10. 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 (on-premise) 說明 。

11. 指定篩選條件：

    a. 選擇用於篩選的欄位名稱。

    b. 選擇一個運算子（請參閱下表），並指定要與事件中的欄位值進行比較的值。

條件運算子清單

| 運算子 | 描述 |
| --- | --- |
| **<** | 如果欄位值小於條件中指定的值，則該事件將被過濾掉。 |
| **≤** | 如果欄位值小於或等於條件中指定的值，則該事件將被過濾掉。 |
| **=** | 如果欄位值等於條件中指定的值，則該事件將被過濾掉。 |
| **≥** | 如果欄位值大於或等於條件中指定的值，則該事件將被過濾掉。 |
| **>** | 如果欄位值大於條件中指定的值，則該事件將被過濾掉。 |
| **≠** | 如果欄位值與條件中指定的值不相等，則該事件將被過濾掉。 |
| **類似** | 如果欄位值與條件中指定的遮罩匹配，則該事件將被過濾掉。應用程式輸入遮罩時支援 `*` 和 `?` 字元： |
| **不類似** | 如果欄位值與條件中指定的遮罩不匹配，則該事件將被過濾掉。應用程式輸入遮罩時支援 `*` 和 `?` 字元： |
| **其中一個** | 如果欄位值與條件中指定的清單中的某個值匹配，則該事件被視為已篩選。 |
| **無一** | 如果欄位值與條件中指定的清單中的任何值都不匹配，則該事件被視為已篩選。 |
| **類似其中一個** | 如果欄位值與條件中指定的某個遮罩匹配，則該事件將被過濾掉。應用程式在輸入遮罩時支援 * 和 ? 字元。 |
| **不類似其中一個** | 如果欄位值與條件中指定的任何遮罩都不匹配，則該事件將被過濾掉。應用程式在輸入遮罩時支援 * 和 ? 字元。 |
| **存在** | 如果事件中存在條件中指定的欄位，則該事件將被過濾掉。 |
| **不存在** | 如果事件中不存在條件中指定的欄位，則該事件將被過濾掉。 |
| **包含** | 如果條件中指定的值存在於欄位值中，則該事件將被過濾掉。 |
| **等於** | 如果欄位值等於條件中指定的值，則該事件將被過濾掉。掃描不區分大小寫。 |
| **按位與** | 如果欄位值與條件中指定的值進行 Bitwise AND (&) 運算的結果為 1，則該事件將被過濾掉。 |

12. 如有必要，您可以透過新增多個篩選條件和條件群組來建立複雜的篩選條件。您也可以向條件群組中新增嵌套條件和條件群組。您可以使用以下運算子：

    - **AND** 表示該篩選器會選擇符合所有指定條件的事件。
    - **OR** 表示該篩選器會選擇符合指定條件之一的事件。
    - **NOT**（若要使用此運算子，請選擇）**新增 NOT 然後** 選項）表示該篩選器選擇不符合任何指定條件的事件。

    條件和一級條件組與 **AND** 運算子結合。

13. 如果您的電腦執行的是 Open Single Management Platform (OSMP)，則您可以掃描您建立的篩選規則。若要執行掃描，請點擊 **檢查規則** 按鈕。

    在開啟的視窗中，將顯示根據建立的規則篩選的事件表。更多詳細資訊請參閱... EDR Expert (on-premise) 說明。

14. 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. 如有必要，請使用 **傳送事件** 撥動開關配置所選事件類型的遙測傳輸。預設情況下，為所有事件類型啟用遙測傳輸。

    d. 在**"排除規則"**塊中，點擊**"新增"**按鈕。

    開啟**"新增排除規則"**視窗。

    e. 對新增的每條規則執行步驟 7-13 中所述的操作。

15. 對於某些事件類型，您還可以新增包含規則來擴展收集的遙測資料：

    a. 在**"包括規則"**塊中，點擊**"新增"**按鈕。

    開啟**"新增包容規則"**視窗。

    b. 輸入規則的名稱。

    c. 在**條件**下面，輸入所顯示欄位的值。可用欄位類型取決於所選事件。

    排除規則的優先權高於包含規則。

16. 要將此政策套用到電腦，請關閉... 掛鎖圖示並儲存變更。

# 匯出和匯入 EDR Expert (on-premise) 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。

使用過多的規則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。

**如何在管理主控台 (MMC) 中匯出和匯入事件篩選器**

1. 開啟卡巴斯基安全管理中心管理主控台。
2. 在主控台樹狀目錄中，選擇**"政策"**。
3. 選擇必要的政策並點擊以開啟政策內容。
4. 在政策視窗中，選擇**"一般設定 → 排除項目和物件類型"**。
5. 在**"遙測設定 → EDR Expert (on-premise) 遙測"**塊中，點擊**"設定"**按鈕。
6. 若要匯出事件篩選器：
   a. 點擊**"匯出"**。
   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。
   b. 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. 開啟檔案。
   如果電腦上已存在事件篩選規則，Kaspersky Endpoint Security 會在匯入時將其替換。
8. 儲存變更。若要在電腦上套用該政策，請關閉掛鎖。

**如何在網頁主控台中匯出和匯入事件篩選器**

1. 在網頁主控台的主視窗中，選擇**資產（裝置）→ 政策和設定檔**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 (on-premise) 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. 儲存變更。若要在電腦上套用該政策，請關閉掛鎖。

您也可以在命令列上匯出或匯入事件篩選器。

# 管理隔離

*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。隔離檔案以加密狀態儲存，不會威脅裝置安全。Kaspersky Endpoint Security 僅在使用以下 Detection and Response 解決方案時使用隔離：EDR Optimum、EDR Expert、KATA (EDR)、Kaspersky Sandbox。在其他情況下，Kaspersky Endpoint Security 將相關檔案放置在備份中。若要瞭解將隔離作為解決方案的一部分進行管理的詳情，請參見Kaspersky Sandbox 說明、Kaspersky Endpoint Detection and Response Optimum 說明、Kaspersky Endpoint Detection and Response Expert 說明、Kaspersky Anti Targeted Attack Platform 說明。

Kaspersky Endpoint Security 使用系統帳戶 (SYSTEM) 隔離檔案。

您只可以在卡巴斯基安全管理中心主控台中配置隔離設定。您也可以使用卡巴斯基安全管理中心主控台來管理隔離的物件（還原，刪除，新增，等等）。在本機電腦上，您只能使用命令列還原物件。

# 配置最大隔離大小

預設情況下，隔離大小限制為 1024 MB。當隔離區達到最大大小時，Kaspersky Endpoint Security 會停止傳送檔案並產生*隔離區儲存空間不足*事件。為防止隔離區用盡磁碟空間，您可以設定一個閾值，當達到此值時 Kaspersky Endpoint Security 會產生*隔離區儲存幾乎用盡空間*事件。您無法為隔離檔案設定保留期以使其自動移除。

如果您的組織中部署了 Kaspersky Anti Targeted Attack Platform (EDR) 解決方案，我們建議增加隔離大小。當進行 YARA 掃描時，應用程式可能遇到大型記憶體傾印。如果記憶體傾印的大小超過隔離大小，則 YARA 掃描將以錯誤結束，記憶體傾印不會被隔離。我們建議將隔離區大小設定為等於電腦上的 RAM 的總大小（例如 8 GB），或停用隔離區的大小限制。

**如何在管理主控台 (MMC) 中配置最大隔離大小**

1. 在卡巴斯基安全管理中心管理主控台樹狀目錄中，選取**政策**。

2. 選擇必要的政策並點擊以開啟政策內容。

3. 在政策視窗中，選擇**"一般設定 → 報告和儲存"**。

4. 在"**隔離區**"塊中配置隔離大小：

   - **隔離區大小限制為 N MB**。如果選中該核取方塊，則最大隔離區大小限制為定義值。預設情況下，最大大小為 1024 MB。當隔離區達到最大大小時，Kaspersky Endpoint Security 會將*隔離區儲存空間不足*事件發送到卡巴斯基安全管理中心並在 Windows 事件記錄中發佈事件。同時，應用程式會停止隔離新物件。您必須手動清空隔離區。

     如果清除該核取方塊，隔離區大小會受到可用磁碟空間的限制。

   - **通知隔離區儲存達到 N 百分比**。隔離的閾值。例如，您可以設定隔離閾值為 50%。當隔離達到閾值時，Kaspersky Endpoint Security 會發送相應事件到卡巴斯基安全管理中心並在Windows 事件記錄中發佈事件。同時，應用程式會繼續隔離新物件。

     如果清除該核取方塊，當隔離區達到閾值時，應用程式不會產生事件。

5. 儲存變更。

**如何在網頁主控台和雲端主控台中配置隔離區最大容量**

1. 在網頁主控台的主視窗中，選擇**資產（裝置）→政策和設定檔**。
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**"塊中配置隔離大小：

   - **限制隔離區大小**如果選中該核取方塊，則最大隔離區大小限制為指定值。如果清除該核取方塊，隔離區大小會受到可用磁碟空間的限制。這對於 YARA 掃描來說可能很有必要，因為該應用程式可能會保存大型記憶體傾印檔案。

   - **隔離區的最大大小 (MB)**如果選中該核取方塊，則最大隔離區大小限制為定義值。預設情況下，最大大小為 1024 MB。當隔離區達到最大大小時，Kaspersky Endpoint Security 會將*隔離區儲存空間不足*事件發送到卡巴斯基安全管理中心並在 Windows 事件記錄中發佈事件。同時，應用程式會停止隔離新物件。您必須手動清空隔離區。

     如果清除該核取方塊，隔離區大小會受到可用磁碟空間的限制。

   - **通知隔離區儲存達到 (%)**隔離的閾值。例如，您可以設定隔離閾值為 50%。當隔離達到閾值時，Kaspersky Endpoint Security 會發送相應事件到卡巴斯基安全管理中心並在Windows 事件記錄中發佈事件。同時，應用程式會繼續隔離新物件。

6. 儲存變更。

# 將有關隔離檔案的資料傳送到卡巴斯基安全管理中心

要在 Web 主控台中對隔離物件執行操作，您必須啟用將隔離檔案資料傳送到管理伺服器。例如，您可以從隔離區下載檔案用於在網頁主控台中分析。必須啟用傳送隔離檔案資料，Kaspersky Sandbox 和 Kaspersky Endpoint Detection and Response的所有功能才能工作。

**如何啟用在管理主控台 (MMC) 中傳輸隔離檔案資料**

1. 在卡巴斯基安全管理中心管理主控台樹狀目錄中，選取**政策**。
2. 選擇必要的政策並點擊以開啟政策內容。
3. 在政策視窗中，選擇**"一般設定 → 報告和儲存"**。
4. 在**"到管理伺服器的資料傳輸"**塊中，點擊**"設定"**按鈕。
5. 在開啟的視窗中，選中**"隔離檔案"**核取方塊。
6. 儲存變更。

**如何啟用在網頁主控台中傳輸隔離檔案資料**

1. 在網頁主控台的主視窗中，選擇**資產（裝置）→ 政策和設定檔**。
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. 在**"到管理伺服器的資料傳輸"**塊中，選中**"關於隔離檔案"**核取方塊。
6. 儲存變更。

結果，您可以在卡巴斯基安全管理中心主控台中檢視已在您的電腦上隔離的檔案清單。您也可以使用網頁主控台來管理隔離的物件（還原，刪除，新增，等等）。有關使用隔離的詳細資訊，請參閱卡巴斯基安全管理中心說明。

# 從隔離區中還原檔案

預設情況下，Kaspersky Endpoint Security 將檔案還原到其原始資料夾。如果目的地資料夾已被刪除或者使用者沒有此資料夾的存取權限，應用程式將把檔案放置於**"%DataRoot%\QB\Restored"**資料夾中。然後您必須手動將檔案移動到目的地資料夾。

*要從隔離區中還原檔案：*

1. 在網頁主控台的主視窗中，選擇**操作 → 儲存區 → 隔離**。
2. 這將開啟隔離區中的檔案清單；在該清單中，選取您想要還原的檔案然後點擊**還原**。

Kaspersky Endpoint Security 將還原該檔案。如果目的地資料夾已經有同名檔案，則應用程式會取消檔案還原。對於 EDR Optimum 和 EDR Expert 解決方案，應用程式會在還原後刪除檔案。對於其它解決方案，應用程式將在隔離區中保留檔案備份。

# 監控 EDR 操作

Kaspersky Endpoint Security for Windows 12.9 引進了 EDR 操作監控中心。*EDR 操作監控中心* 是一個主控台，您可以在其中檢視所有 Kaspersky Detection and Response 解決方案的威脅回應歷史記錄。如果您的組織部署了多個 Detection and Response（例如，EDR Optimum 和 MDR），Kaspersky Endpoint Security 將顯示所有解決方案的威脅回應歷史記錄。這使您可以在單獨的電腦上分析 Detection and Response 解決方案的效能並最佳化這些解決方案的設定。

監控中心提供以下資訊：

- 有關威脅回應工作的資訊（例如 *停止處理程序* 工作）
- 網路隔離和執行預防規則的變化

如果威脅回應遇到與存取網路共用相關的錯誤，則會從顯示的威脅回應歷史記錄中省略此類錯誤。

*若要導覽至 EDR 操作監控中心：*

1. 在網頁主控台的主視窗中，選擇**資產（裝置）→ 受管理裝置**。
2. 選取要為其配置本機應用程式設定的電腦。

   這將開啟電腦內容。
3. 選擇“**應用程式**”標籤。
4. 點擊“**Kaspersky Endpoint Security for Windows**”。

   這將開啟本機應用程式設定。
5. 選擇“**應用程式設定**”標籤。
6. 轉到”**Detection and Response**”→”**回應歷史**”。

   這將開啟 EDR 操作監控中心主控台。您可以使用主控台檢視威脅回應工作狀態、工作持續時間、規則變更和發起者詳細資訊。

# Kaspersky Unified Monitoring and Analysis Platform (KUMA)



Kaspersky Endpoint Security for Windows 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。

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。在其主控台中，KUMA 將事件顯示為沒有標記的清單，類似於 Windows 事件日誌。

Kaspersky Endpoint Security 不提供 KUMA 代理的所有功能。應用程式僅將事件傳送到 KUMA，不帶標記。要存取所有 KUMA 功能，您必須購買產品許可並按照KUMA 管理員指南部署解決方案。

# Kaspersky Endpoint Security 與 KUMA 整合

要使用 KUMA 必須滿足以下條件：

- 卡巴斯基安全管理中心版本 14.2 或更高版本。在早期版本的卡巴斯基安全管理中心中，無法啟動 KUMA 整合功能。
- 應用程式被啟動，功能受產品授權覆蓋。
- KUMA 整合元件被啟用。

設定 KUMA 整合涉及以下步驟：

1. **安裝 KUMA 整合元件**

   您可以在安裝或者更新應用程式，以及使用*變更應用程式元件*工作期間選擇 KUMA 整合元件。

   您必須重新啟動電腦以完成升級含新元件的應用程式。

2. **KUMA 啟動**

   除了 Kaspersky Endpoint Security 應用程式產品授權（例如 Kaspersky Endpoint Security for Business Standard）之外，您還需要單獨的產品授權才能將 Kaspersky Endpoint Security 與 KUMA（Kaspersky Endpoint Security for Windows KUMA 整合插件）進行整合。

   如果您要在 EDR Agent 模式下安裝應用程式，則需要用於將 Kaspersky Endpoint Security 與 KUMA 進行整合的產品授權以及 Kaspersky Anti Targeted Attack Platform (KATA) 產品授權或 Kaspersky Managed Detection and Response (MDR) 產品授權。您無法僅為 KUMA 部署 EDR Agent。

新增單獨的 KUMA 金鑰後，該功能即可使用。因此，電腦上將有另一個用於 Kaspersky Endpoint Security 與 KUMA 整合的活動金鑰。

獨立 KUMA 功能的授權和 Kaspersky Endpoint Security 的授權一樣。

確保 KUMA 功能包括在產品授權中且在應用程式的本機介面中工作。

### 3 連線至 KUMA

若要將裝有 Kaspersky Endpoint Security 應用程式的電腦連線到 KUMA 解決方案：

1. 在 Kaspersky Endpoint Security 政策中，新增 KUMA 伺服器位址並指定已連線的網路設定。
2. 在 KUMA 主控台中，新增具有 tcp 或 udp 類型連線器的收集器，並指定連線的基本網路設定。有關管理收集器的詳細資訊，請參閱 Kaspersky Unified Monitoring and Analysis Platform 說明。

您可以在 Kaspersky Endpoint Security 和 KUMA 伺服器之間建立可信任連線。要配置可信連線，您必須使用 TLS 憑證。您可以在 KUMA Core 伺服器上取得 TLS 憑證（請參閱 Kaspersky Unified Monitoring and Analysis Platform 說明中 tcp 類型連線器的設定）。然後您必須將 TLS 憑證新增到 Kaspersky Endpoint Security（參見下面的說明）。

為了使連線更安全，您可以額外啟用在 KUMA 中進行電腦驗證（雙向身分驗證）。要啟用此驗證，您必須在 KUMA 和 Kaspersky Endpoint Security 設定中開啟雙向身分驗證。要使用雙向身分驗證，您還需要一個加密容器。*加密容器*是一個帶有憑證和私鑰的 PFX 存檔。您必須在外部憑證授權單位中使用 PKCS#12 容器格式的私密金鑰產生憑證。然後，您必須在 KUMA 主控台和 Kaspersky Endpoint Security 中新增 PFX 存檔（請參閱 Kaspersky Unified Monitoring and Analysis Platform 說明）。

**如何使用管理主控台 (MMC) 將 Kaspersky Endpoint Security 電腦連線到 KUMA**

1. 在卡巴斯基安全管理中心管理主控台樹狀目錄中，選取**政策**。
2. 選擇必要的政策並點擊以開啟政策內容。
3. 在政策視窗中，選取“**KUMA 整合**”。
4. 選擇“**KUMA 整合**”核取方塊。
5. 在“**整合設定**“塊中，選中“**$IsKUMATelemetry ? "啟用將 Windows 事件傳輸到 SIEM 伺服器": "啟用將 Windows 事件傳輸到 SIEM 伺服器**”核取方塊。
6. 如有必要，在**KUMA 伺服器連線設定**塊中選擇**使用 TLS 加密**核取方塊。
7. 設定受信任連線：
   a. 點擊**“KUMA 伺服器連線設定”**。
   b. 配置伺服器連線：
      - **逾時（秒）**KUMA 伺服器響應最大逾時。當超時用完時，Kaspersky Endpoint Security 會嘗試連線到不同的 KUMA 伺服器。
      - **伺服器 TLS 憑證**用於與 KUMA 伺服器建立可信連線的 TLS 憑證。您可以在 Kaspersky Unifield Monitoring and Analysis Platform 主控台中取得 TLS 憑證（請參閱 Kaspersky Unifield Monitoring and Analysis Platform 中的說明）。

        若要建立可信任連線，在 KUMA 主控台的 tcp 連線器設定中，您必須選擇 **With verification** TLS 模式（請參閱 Kaspersky Unified Monitoring and Analysis Platform 說明中 tcp 類型連線器的設定）。

- **使用雙向身分驗證**在 Kaspersky Endpoint Security 和 KUMA 之間建立安全連線時進行雙向身分驗證。若要使用雙向身分驗證，在 KUMA 主控台的 tcp 連線器設定中，您必須選擇 **Custom PFX** TLS 模式（請參閱 Kaspersky Unified Monitoring and Analysis Platform 說明 中 tcp 類型連線器的設定）。然後您必須取得加密容器並設定密碼來保護該加密容器。*加密容器*是一個帶有憑證和私鑰的 PFX 存檔。配置 KUMA 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。

c. 點擊**"確定"**。

8. 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. 選擇連線至 KUMA 伺服器的協定：**HTTP / HTTPS**, **TCP**, **UDP**。

   如果您預設選擇 **HTTP/HTTPS** 協定，則應用程式使用 HTTPS 連線到 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）和連線到伺服器的連接埠。

   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。

9. 如有必要，在**資料傳輸設定**塊中配置**最大事件傳輸延遲時間（秒）**設定。當指定的時間用完時，Kaspersky Endpoint Security 會嘗試連線到相同伺服器，或連線到清單中的下一個伺服器（如果有多個伺服器）。預設設定是 30 秒。

10. 儲存變更。

**如何使用網頁主控台將 Kaspersky Endpoint Security 電腦連線到 KUMA**

1. 在網頁主控台的主視窗中，選擇**資產（裝置）→ 政策和設定檔**。

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. 開啟**"KUMA 整合已啟用"**開關。

6. 如有必要，在**伺服器連線設定**塊中開啟**使用 TLS 加密**切換開關。

7. 設定受信任連線：

   a. 點擊**"連線設定"**。

   b. 配置伺服器連線：

   - **逾時（秒）** KUMA 伺服器響應最大逾時。當超時用完時，Kaspersky Endpoint Security 會嘗試連線到不同的 KUMA 伺服器。
   - **伺服器 TLS 憑證**用於與 KUMA 伺服器建立可信連線的 TLS 憑證。您可以在 Kaspersky Unifield Monitoring and Analysis Platform 主控台中取得 TLS 憑證（請參閱 Kaspersky Unifield Monitoring and Analysis Platform 中的說明）。

     若要建立可信任連線，在 KUMA 主控台的 tcp 連線器設定中，您必須選擇 **With verification** TLS 模式（請參閱 Kaspersky Unified Monitoring and Analysis Platform 說明 中 tcp 類型連線器的設定）。
   - **使用雙向身分驗證**在 Kaspersky Endpoint Security 和 KUMA 之間建立安全連線時進行雙向身分驗證。若要使用雙向身分驗證，在 KUMA 主控台的 tcp 連線器設定中，您必須選擇 **Custom PFX** TLS 模式（請參閱 Kaspersky Unified Monitoring and Analysis Platform 說明 中 tcp 類型連線器的設定）。然後您必須取得加密容器並設定密碼來保護該加密容器。*加密容器*是一個帶有憑證和私鑰的 PFX 存檔。配置 KUMA 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。

   c. 點擊**OK**。

8. 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. 選擇連線至 KUMA 伺服器的協定：**HTTP / HTTPS**, **TCP**, **UDP**。

   如果您預設選擇 **HTTP/HTTPS** 協定，則應用程式使用 HTTPS 連線到 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）和連線到伺服器的連接埠。

   d. 點擊**OK**。

   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。

9. 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。當指定的時間用完時，Kaspersky Endpoint Security 會嘗試連線到相同伺服器，或連線到清單中的下一個伺服器（如果有多個伺服器）。預設設定是 30 秒。

10. 儲存變更。

您可以驗證 KUMA 主控台中是否正確配置了 KUMA 整合（有關詳細資訊，請參閱 Kaspersky Unified Monitoring and Analysis Platform 說明）。透過在卡巴斯基安全管理中心主控台中檢視*"應用程式元件狀態報告"*來檢查元件的運行狀態。您還可以在 Kaspersky Endpoint Security 的本地介面中的報告中檢視元件的運行狀態。**"KUMA 整合"**元件將新增到 Kaspersky Endpoint Security 元件清單中。

### 4 啟用向 KUMA 伺服器傳送遙測資料

預設情況下，向 KUMA 伺服器傳送事件被停用。為確保 KUMA 正常運作，您必須啟用遙測資料傳送功能。您可以從標準記錄中選擇一個事件來源：*Application*、*Security*或*System*。

**如何在管理主控台 (MMC) 中啟用向 KUMA 伺服器傳送遙測資料**

1. 開啟卡巴斯基安全管理中心管理主控台。
2. 在主控台樹狀目錄中，選擇**"政策"**。
3. 選擇必要的政策並點擊以開啟政策內容。
4. 在政策視窗中，選擇**"一般設定 → 排除項目和物件類型"**。
5. 在**"遙測設定 → KUMA 遙測"**塊中，點擊**"設定"**按鈕。
6. 選擇要用作事件來源的事件日誌：*Application*、*Security* 或者 *System*。
   除了標準日誌外，您還可以指定 協力廠商應用程式的日誌。
7. 要將此政策套用到電腦，請關閉... 掛鎖圖示並儲存變更。

**如何在網頁主控台中啟用將遙測資料傳送到 KUMA 伺服器**

1. 在網頁主控台的主視窗中，選擇**資產（裝置）→ 政策和設定檔**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**"KUMA 遙測"**標籤。
6. 選擇要用作事件來源的事件日誌：*Application*、*Security* 或者 *System*。
   除了標準日誌外，您還可以指定 協力廠商應用程式的日誌。
7. 要將此政策套用到電腦，請關閉... 掛鎖圖示並儲存變更。

# 篩選要傳送到 KUMA 的事件

預設情況下，向 KUMA 伺服器傳送事件被停用。為確保 KUMA 正常運作，您必須啟用遙測資料傳送功能。您可以從標準記錄中選擇一個事件來源：*Application*、*Security*或*System*。為了提高效能並最佳化到 KUMA 伺服器的資料傳輸，您可以從遙測中手動新增或排除個別事件。例如，您可以排除 Sysmon 事件。

**如何在管理主控台 (MMC) 中建立要傳送到 KUMA 的事件清單**

1. 開啟卡巴斯基安全管理中心管理主控台。
2. 在主控台樹狀目錄中，選擇**"政策"**。
3. 選擇必要的政策並點擊以開啟政策內容。

4. 在政策視窗中，選擇"**一般設定 → 排除項目和物件類型**"。

5. 在"**遙測設定 → KUMA 遙測**"塊中，點擊"**設定**"按鈕。

6. 在顯示的視窗中，設定要傳送到 KUMA 的事件篩選器。

   您可以為標準的 *Application*、*Security*、*System* 記錄設定事件篩選，或手動新增其他記錄。

   a. 點擊 **新增** 或開啟記錄內容。

   b. 選取事件傳送模式：

   - **傳送所有事件**在此模式下，應用程式會傳送 Windows 日誌中的所有事件（新增到排除規則的事件除外）。
   - **僅傳送選取的事件**在此模式下，應用程式僅會傳送包含規則中新增的事件。

   c. 為相關事件傳送模式建立排除規則或包含規則的清單。

   若要新增規則，需要指定 Windows 事件記錄中的事件 ID。您可以在一個規則中列出多個事件 ID。若要指定多個事件 ID，請使用逗號 (",")。

7. 要將此政策套用到電腦，請關閉... 掛鎖圖示並儲存變更。

**如何在網頁主控台中建立要傳送到 KUMA 的事件清單**

1. 在網頁主控台的主視窗中，選擇**資產（裝置）→ 政策和設定檔**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"**KUMA 遙測**"標籤。

6. 在顯示的視窗中，設定要傳送到 KUMA 的事件篩選器。

   您可以為標準的 *Application*、*Security*、*System* 記錄設定事件篩選，或手動新增其他記錄。

   a. 點擊 **新增** 或開啟記錄內容。

   b. 選取事件傳送模式：

   - **傳送所有事件**在此模式下，應用程式會傳送 Windows 日誌中的所有事件（新增到排除規則的事件除外）。
   - **僅傳送選取的事件**在此模式下，應用程式僅會傳送包含規則中新增的事件。

   c. 為相關事件傳送模式建立排除規則或包含規則的清單。

   若要新增規則，需要指定 Windows 事件記錄中的事件 ID。您可以在一個規則中列出多個事件 ID。若要指定多個事件 ID，請使用逗號 (",")。

7. 要將此政策套用到電腦，請關閉... 掛鎖圖示並儲存變更。

# 匯出和匯入 KUMA 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。

使用過多的規則會增加 KUMA 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。

**如何在管理主控台 (MMC) 中匯出和匯入事件篩選器**

1. 開啟卡巴斯基安全管理中心管理主控台。
2. 在主控台樹狀目錄中，選擇**"政策"**。
3. 選擇必要的政策並點擊以開啟政策內容。
4. 在政策視窗中，選擇**"一般設定 → 排除項目和物件類型"**。
5. 在**"遙測設定 → KUMA 遙測"**塊中，點擊**"設定"**按鈕。
6. 若要匯出事件篩選器：
   a. 選取您要匯出的包含篩選器的事件記錄。
   b. 點擊 → **匯出** 按鈕。
   c. 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。
   d. 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** 按鈕。
   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. 開啟檔案。
      如果電腦上已存在事件篩選規則，Kaspersky Endpoint Security 會在匯入時將其替換。
8. 儲存變更。若要在電腦上套用該政策，請關閉掛鎖。

**如何在網頁主控台中匯出和匯入事件篩選器**

1. 在網頁主控台的主視窗中，選擇**資產（裝置）→ 政策和設定檔**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"**KUMA 遙測**"標籤。

6. 若要匯出事件篩選器：

   a. 選取您要匯出的包含篩選器的事件記錄。

   b. 點擊 → **匯出** 按鈕。

   c. 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。

   d. 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** 按鈕。

   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. 開啟檔案。

   如果電腦上已存在事件篩選規則，Kaspersky Endpoint Security 會在匯入時將其替換。

8. 儲存變更。若要在電腦上套用該政策，請關閉掛鎖。

您也可以在命令列上匯出或匯入事件篩選器。

# KSWS 到 KES 遷移指南

從版本 11.8.0 開始，Kaspersky Endpoint Security for Windows 支援 Kaspersky Security for Windows Server (KSWS) 解決方案的基本功能。*Kaspersky Security for Windows Server* 防護執行 Microsoft Windows 作業系統和網路附加儲存的伺服器免受病毒和其他電腦安全威脅，伺服器和網路附加儲存在交換檔案時會受到這些威脅。如欲瞭解該解決方案如何工作的詳細資訊，請參閱 Kaspersky Security for Windows Server 說明。從 Kaspersky Endpoint Security 11.8.0 開始，您可以從 Kaspersky Security for Windows Server 遷移到 Kaspersky Endpoint Security for Windows，並使用同一個解決方案來防護工作站和伺服器。

## 軟體要求

在開始從 KSWS 遷移到 KES 之前，請確保您的伺服器滿足 Kaspersky Endpoint Security for Windows 的硬件和軟體要求。KES 和 KSWS 支援的作業系統版本清單不同。例如，KES 不支援執行 Windows Server 2003 的伺服器。

從 KSWS 遷移到 KES 的最低軟體要求：

- Kaspersky Endpoint Security for Windows 12.0。
- Kaspersky Security 11.0.1 for Windows Server。

  如果您安裝了早期版本的 Kaspersky Security for Windows Server，我們建議將應用程式升級到最新版本。政策和工作轉換精靈不支援早期版本的 Kaspersky Security for Windows Server。
- 卡巴斯基安全管理中心 14.2

  如果您安裝了早期版本的卡巴斯基安全管理中心，請將其更新到 14.2 或更高版本。在此版本的卡巴斯基安全管理中心中，政策和工作批量轉換精靈允許您將政策遷移到設定檔而不是政策。在此版本的卡巴斯基安全管理中心中，政策和工作批量轉換精靈還允許您遷移範圍更廣的政策設定。
- Kaspersky Endpoint Agent 3.10。

  如果您安裝了早期版本的 Kaspersky Endpoint Agent，我們建議將應用程式升級到最新版本。從 Kaspersky Endpoint Agent 3.10 開始，Kaspersky Endpoint Security 支援將 [KSWS+KEA] 配置遷移到 [KES+內建代理]。

## 遷移建議

從 KSWS 遷移到 KES 時，請遵循以下建議：

- 提前規劃好 KSWS 到 KES 的遷移時間。選擇伺服器在最輕負載下執行的時間，例如周末。
- 遷移後，逐步開啟應用程式元件。即，例如，首先單獨啟用檔案威脅防護元件，然後啟用其他防護元件，再啟用控制元件，依此類推。在每一步，您都必須確保應用程式正常工作，並監控伺服器的效能。KES 的架構與 KSWS 不同，因此作業系統的行為也可能不同。
- 逐步進行遷移。首先遷移單台伺服器，然後遷移多台伺服器，然後在組織的所有伺服器上進行遷移。

- 分別遷移不同類型的伺服器。也就是說，例如，首先遷移資料庫伺服器，然後遷移郵件伺服器，等等。
- 在高負載伺服器上遷移涉及一些特殊注意事項。

### 遷移步驟

從 KSWS 到 KES 的遷移是半自動執行的。這是必要的，因為應用程式的架構不同。要遷移政策設定，您必須執行政策和工作批量轉換精靈（遷移精靈）。遷移政策設定後，您必須手動配置遷移精靈無法自動遷移的設定（例如，密碼防護設定）。遷移後，還建議檢查遷移精靈是否正確遷移了所有設定。

按以下順序從 KSWS 遷移到 KES：

1. **遷移 KSWS 工作和政策**

   遷移政策和工作後，您必須執行額外的配置步驟。我們還建議確保 Kaspersky Endpoint Security 在從 KSWS 遷移後提供必要的安全級別。

   > Kaspersky Security for Windows Server 的政策和工作批量轉換精靈僅在管理主控台 (MMC) 中可用。政策和工作設定無法在網頁主控台和卡巴斯基安全管理中心雲端主控台中進行遷移。

2. **安裝 Kaspersky Endpoint Security**

   您可以通過以下方式安裝 Kaspersky Endpoint Security：

   - 刪除 KSWS 後安裝 KES（建議）。

     > kavremover 實用程式 不支援管理 KSWS。

   - 在 KSWS 之上安裝 KES。

3. **使用 KSWS 金鑰啟動 KES**

4. **確認應用程式在遷移後處於工作狀態**

   從 KSWS 遷移到 KES 後，確保應用程式運行正常。在主控台查看伺服器狀態（應該是*確定*）。確保應用程式沒有報告任何錯誤，還要檢查最後一次連線到管理伺服器的時間、最後一次更新資料庫的時間和伺服器防護狀態。

   > 特別注意排除項目清單、受信任應用程式、受信任網址、應用程式控制規則的遷移。

# KSWS 和 KES 元件的對應關係

從 KSWS 遷移到 KES 時，僅當應用程式在本機安裝時才遷移元件集。

| Kaspersky Security for Windows Server 元件 | Kaspersky Endpoint Security for Windows 元件 |
|---|---|
| 基本功能 | 應用程式內核 |
| 記錄檢查 | 記錄審查 |
| 裝置控制 | 裝置控制 |
| 防火牆管理 | *（不受支援）*<br>KSWS 防火墻功能由系統級別的防火墻執行。在 KES 中，一個單獨的元件負責防火牆功能。您可以在遷移後配置 Kaspersky Endpoint Security 防火墻。 |
| 檔案完整性監控 | 系統完整性監控 |
| 弱點利用防禦 | 弱點利用防禦 |
| 系統托盤圖示 | *（不受支援）*<br>您可以在 應用程式介面設定中配置使用者互動。 |
| 與卡巴斯基安全管理中心的整合 | 網路代理連線器 |
| Endpoint Agent | *（不受支援）*<br>在 Kaspersky Endpoint Security 11.9.0 中，Kaspersky Endpoint Agent 分發套件不再是 Kaspersky Endpoint Security 分發套件的一部分。您必須單獨下載 Kaspersky Endpoint Agent 分發套件。 |
| 網路威脅防護 | 網路威脅防護 |
| Anti-Cryptor | 行為偵測 |
| Anti-Cryptor for NetApp | *（不受支援）* |
| 流量安全 | Web 威脅防護<br>郵件威脅防護<br>Web 控制 |
| 按需掃描 | 應用程式內核 |
| ICAP 網路儲存防護 | *（不受支援）*<br>Kaspersky Endpoint Security 不支援網路附加儲存防護元件。如果您需要這些元件，您可以繼續使用 Kaspersky Security for Windows Server。 |
| RPC 網路儲存防護 | *（不受支援）*<br>Kaspersky Endpoint Security 不支援網路附加儲存防護元件。如果您需要這些元件，您可以繼續使用 Kaspersky Security for Windows Server。 |
| 即時檔案防護 | 檔案威脅防護 |
| 指令碼監控 | *（不受支援）*<br>指令碼監控由其他元件處理，例如，AMSI 防護。 |
| KSN 使用 | 卡巴斯基安全網路 |
| 應用程式啟動控制 | 應用程式控制 |
| 效能計數器 | *（不受支援）* |

# KSWS 和 KES 設定的對應關係

遷移政策和工作時，會根據 KSWS 設定配置 KES。KSWS 沒有的應用程式元件被設定為預設值。

## 應用程式設定

### 可擴展性、介面和掃描設定

Kaspersky Endpoint Security for Windows 不支援應用程式設定。

應用程式設定

| Kaspersky Security for Windows Server 設定 | Kaspersky Endpoint Security for Windows 設定 |
|---|---|
| **延伸性設定** | *（不遷移）*<br>Kaspersky Endpoint Security 管理所有工作流程。 |
| **顯示系統托盤圖示** | *（不遷移）*<br>在用戶端電腦上，Kaspersky Endpoint Security 的主視窗和 Windows 通知區域中的圖示均預設可用。在該圖示的內容功能表中，使用者可以使用 Kaspersky Endpoint Security 執行操作。Kaspersky Endpoint Security 還會在應用程式圖示上方顯示通知。您可以在 應用程式介面設定中配置使用者互動。 |
| **掃描後還原檔案內容** | *（不遷移）*<br>Kaspersky Endpoint Security 會在掃描檔案後自動還原檔案屬性。 |
| **限制執行緒掃描的 CPU 使用率** | *（不遷移）*<br>Kaspersky Endpoint Security 在掃描時不限制 CPU 使用。您可以 配置當電腦在最小負載下運行時要執行的工作。 |
| **用於儲存在掃描期間建立的暫存檔案的資料夾** | *（不遷移）*<br>Kaspersky Endpoint Security 將暫存檔放在 `C:\Windows\Temp` 資料夾中。 |
| **HSM 系統設定** | *（不遷移）*<br>Kaspersky Endpoint Security 不支援 HSM 系統。 |

## 安全性和可靠性

KSWS 安全設定被遷移到**一般設定**區段的**應用程式設定**和**介面**子區段。

應用程式安全設定

| Kaspersky Security for Windows Server 設定 | Kaspersky Endpoint Security for Windows 設定 |
|---|---|
| **防護應用程式處理程序免受外部威脅** | **啟用自我防護**（**應用程式設定**子區段） |
| **套用密碼防護** | *（不遷移）*<br>Kaspersky Endpoint Security 具有內建密碼防護功能（請參見"**介面**"子區段）。 |
| **重新啟動工作** | *（不遷移）*<br>Kaspersky Endpoint Security 僅自動還原*惡意軟體掃描*工作。Kaspersky Endpoint Security 按排程執行其他工作。 |
| **不啟動已排程掃描工作** | **使用電池供電時延遲排程工作**（**應用程式設定**子區段） |
| **停止目前掃描工作** | *（不遷移）*<br>當電腦由 UPS 供電時，Kaspersky Endpoint Security 不會停止已在執行的掃描工作。 |

## 連線設定

管理伺服器互動設定被遷移到**一般設定**區段的**網路設定**和**應用程式設定**子區段。

管理伺服器互動設定

| Kaspersky Security for Windows Server 設定 | Kaspersky Endpoint Security for Windows 設定 |
|---|---|
| **代理伺服器設定** | **代理伺服器設定**（**網路設定**子區段） |
| **對於本機位址不使用代理伺服器** | **本機位址略過代理伺服器**（**網路設定**子區段） |
| **代理伺服器身分驗證設定** | **使用代理伺服器身分驗證**（**網路設定**子區段）<br>代理伺服器身分驗證密碼未遷移。政策遷移後，必須手動輸入密碼。 |
| **啟動應用程式時使用卡巴斯基安全管理中心作為代理伺服器** | **使用卡巴斯基安全管理中心作為啟動代理伺服器**（**應用程式設定**子區段） |

## 執行本機系統工作

Kaspersky Endpoint Security 會忽略用於執行 Kaspersky Security for Windows Server 的本機系統工作的設定。您可以在 **本機工作**, **工作管理** 下面配置如何使用本機 KES 工作。您也可以在這些工作的內容中配置用於執行*惡意軟體掃描* and *資料庫和應用程式模組更新*工作的排程。

補充

### 應用程式掃描排除項目

KSWS 受信任區段設定被遷移到 **一般設定** 區段的**排除項目**子區段。

受信任區域設定

| Kaspersky Security for Windows Server 設定 | Kaspersky Endpoint Security for Windows 設定 |
|---|---|
| **要掃描的物件**（排除項目） | **掃描排除項目** (掃描排除項目)<br>KSWS 和 KES 用於選擇物件的方法不同。遷移時，KES 支援定義為單個檔案或檔案/資料夾路徑的排除項目。如果 KSWS 將排除項目配置為預定義區域或指令碼 URL，則不會遷移此類排除項目。遷移後，您必須手動新增此類排除項目。作為預定義區域的排除項目必須在*惡意軟體掃描*工作設定中進行配置。作為指令碼網址的排除項目必須新增到 Web 威脅防護的受信任網址。 |
| **同時套用於子資料夾**（排除項目） | **包含子資料夾** (掃描排除項目) |
| **偵測物件**（排除項目） | **偵測到的物件類型** (掃描排除項目) |
| **排除使用範圍**（排除項目） | **防護元件** (掃描排除項目)<br>如果在 KSWS 中選擇了至少一個元件，則 KES 會將排除項目套用到所有應用程式元件。 |
| **註解**（排除項目） | **註解** (掃描排除項目) |
| **受信任處理程序**（受信任處理程序） | **受信任應用程式**<br>KSWS 和 KES 中的受信任處理程序/應用程式選擇方法不同。遷移時，KES 支援配置為可執行檔或遮罩路徑的受信任應用程式。如果 KSWS 具有配置為檔案雜湊的受信任處理程序，則不會遷移此類受信任處理程序。遷移後，您必須手動新增此類受信任處理程序。 |
| **不檢查檔案備份操作**（受信任處理程序） | **不監控應用程式活動** (受信任應用程式) |

### 卸除式磁碟機掃描

卸除式磁碟機掃描設定被遷移到 **本機工作** 區段的**卸除式磁碟機掃描**子區段。

"卸除式磁碟機掃描"設定

| Kaspersky Security for Windows Server 設定 | Kaspersky Endpoint Security for Windows 設定 |
|---|---|
| **掃描透過 USB 連接的卸除式磁碟機** | **連接到卸除式磁碟機的操作** |
| **掃描卸除式磁碟機，如果其儲存的資料量未超過 (MB)** | **卸除式磁碟機最大容量** |

| Kaspersky Security for Windows Server 設定 | Kaspersky Endpoint Security for Windows 設定 |
| --- | --- |
| **掃描時使用的安全等級**：<br>• **最佳防護**<br>• **建議**<br>• **最佳效能** | **連接到卸除式磁碟機的操作**：<br>• **最大防護**<br>• **建議防護**<br>KSWS 安全等級對應於 KES 掃描模式如下：<br>• 最佳防護 – 最大防護。<br>• 建議 – 建議防護。<br>• 最佳效能 – 建議防護。 |

### 應用程式管理使用者權限

Kaspersky Endpoint Security 不支援為應用程式管理和應用程式服務管理分配使用者存取權限。您可以為使用者和使用者群組配置用來管理卡巴斯基安全管理中心中的應用程式的存取設定。

### 卡巴斯基安全服務管理的使用者存取權限

Kaspersky Endpoint Security 不支援為應用程式管理和應用程式服務管理分配使用者存取權限。您可以為使用者和使用者群組配置用來管理卡巴斯基安全管理中心中的應用程式的存取設定。

### 儲存

KSWS 儲存設定被遷移到**一般設定**區段的 **報告和儲存**子區段，和**關鍵威脅防護**區段的**網路威脅防護**子區段。

儲存設定

| Kaspersky Security for Windows Server 設定 | Kaspersky Endpoint Security for Windows 設定 |
| --- | --- |
| **備份資料夾** | *（不遷移）*<br>Kaspersky Endpoint Security 將檔案的備份副本儲存在 `C:\ProgramData\Kaspersky Lab\KES.12.12\QB` 資料夾中。 |
| **最大備份空間 (MB)** | **備份大小限制為 N MB**（**一般設定** → **報告和儲存**區段） |
| **可用空間上限值(MB)** | *（不遷移）*<br>當達到 50% 的閾值時，Kaspersky Endpoint Security 會記錄*隔離區儲存幾乎用盡空間*事件。 |
| **還原物件的指定資料夾** | *（不遷移）*<br>Kaspersky Endpoint Security 將檔案還原到其原始資料夾。 |
| **隔離資料夾** | *（不遷移）*<br>Kaspersky Endpoint Security 將檔案的備份副本儲存在 `C:\ProgramData\Kaspersky Lab\KES.12.12\QB` 資料夾中。 |
| **最大隔離區空間 (MB)** | *（不遷移）*<br>Kaspersky Endpoint Security 使用備份來儲存可能受感染的物件。在遷移過程中，Kaspersky Endpoint Security 會忽略隔離設定。 |
| **可用空間上限值(MB)** | *（不遷移）*<br>Kaspersky Endpoint Security 使用備份來儲存可能受感染的物件。在遷移過程中，Kaspersky Endpoint Security 會忽略隔離設定。 |
| **還原物件的指定資料夾** | *（不遷移）*<br>Kaspersky Endpoint Security 將檔案還原到其原始資料夾。 |
| **在該時間後自動解除封鎖： N** | **封鎖攻擊裝置 N 分 (關鍵威脅防護** → **網路威脅防護**區段） |

## 即時伺服器防護

### 即時檔案防護

KSWS 即時檔案防護設定被遷移到**關鍵威脅防護**區段的**檔案威脅防護**子區段。

即時檔案防護設定

| Kaspersky Security for Windows Server 設定 | Kaspersky Endpoint Security for Windows 設定 |
|---|---|
| **物件防護模式**：<br>• **智慧模式**<br>• **執行時**<br>• **存取時**<br>• **存取及修改時** | **掃描模式**：<br>• **智慧模式**<br>• **執行時**<br>• **存取時**<br>• **在存取及修改時** |
| **對啟動處理程序的更深度分析** | *（不遷移）*<br>Kaspersky Endpoint Security 僅支援一種分析模式，即最佳模式。 |
| **啟發式分析器**：<br>• **輕度**<br>• **中度**<br>• **深度** | **啟發式分析**：<br>• **輕度掃描**<br>• **中度掃描**<br>• **深度掃描** |
| **套用信任區域** | *（不遷移）*<br>Kaspersky Endpoint Security 將受信任區域套用到所有元件。您可以在 受信任區域設定中配置排除項目。 |
| **使用 KSN 防護** | *（不遷移）*<br>Kaspersky Endpoint Security 將 KSN 用於所有應用程式元件。 |
| **封鎖對顯示惡意活動的主機的網路共用資源的存取** | *（不遷移）*<br>預設情況下，Kaspersky Endpoint Security 會對於顯示惡意活動的主機封鎖存取網路共用資源。 |
| **偵測到感染活動時啟動關鍵區域掃描** | *（不遷移）*<br>偵測到活動感染時，Kaspersky Endpoint Security 不會啟動關鍵區域掃描工作。 |
| **使用 Kaspersky Sandbox 防護** | *（不遷移）*<br>預設情況下，Kaspersky Endpoint Security 將要掃描的物件傳送到 Kaspersky Sandbox。 |
| **防護範圍** | **防護範圍** |
| **排程設定** | *（不遷移）*<br>Kaspersky Endpoint Security 使用自己的排程來暫停檔案威脅防護。 |

## KSN 使用

卡巴斯基安全網路的 KSWS 設定被遷移到**進階威脅防護**區段的**卡巴斯基安全網路**子區段。

卡巴斯基安全網路設定

| Kaspersky Security for Windows Server 設定 | Kaspersky Endpoint Security for Windows 設定 |
|---|---|
| **我確認已完全閱讀、瞭解並接受參加卡巴斯基安全網路聲明的條款** | **卡巴斯基安全網路聲明**<br>在安裝應用程式、建立新政策或啟用卡巴斯基安全網路使用時，Kaspersky Endpoint Security 會請求同意卡巴斯基安全網路聲明。 |
| **傳送關於已掃描檔案的資料** | *（不遷移）*<br>如果啟用 KSN，Kaspersky Endpoint Security 會自動傳送有關掃描檔案的資料。 |
| **傳送關於請求的 URL 的資料** | *（不遷移）*<br>如果啟用 KSN，Kaspersky Endpoint Security 會自動傳送有關請求的 URL 的資料。 |
| **傳送卡巴斯基安全網路統計資訊** | **啟用延伸 KSN 模式** |
| **接受卡巴斯基管理防護聲明的條款** | *（不遷移）*<br>Kaspersky Endpoint Security 不包括 KMP 服務。 |
| **對 KSN 不信任的物件執行的操作** | *（不遷移）*<br>您可以在防護元件設定和掃描工作設定中配置偵測到威脅後的動作。 |
| **如果檔案大小超過以下大小，則在傳送到 KSN 之前不計算核對總和： N MB** | *（不遷移）*<br>您可以在防護元件設定和掃描工作設定中配置大檔案掃描限制。 |

| Kaspersky Security for Windows Server 設定 | Kaspersky Endpoint Security for Windows 設定 |
| --- | --- |
| **使用卡巴斯基安全管理中心作為 KSN 代理** | **使用管理伺服器為 KSN 代理伺服器** |
| **排程設定** | *（不遷移）*<br>無法為元件配置單獨排程。該元件在 Kaspersky Endpoint Security 運行時始終處於開啟狀態。 |

## 流量安全

KSWS 流量安全設定被遷移到**關鍵威脅防護**區段的**Web 威脅防護**和**郵件威脅防護**子區段，**安全控制**區段的**Web 控制**子區段，**一般設定**區段的**網路設定**子區段。

流量安全設定

| Kaspersky Security for Windows Server 設定 | Kaspersky Endpoint Security for Windows 設定 |
| --- | --- |
| **套用基於 URL 的規則** | **Web 控制**（**Web 控制**子區段）<br>基於 URL 的規則被遷移到 Kaspersky Endpoint Security 中的單獨規則。 |
| **套用基於憑證的規則** | *（不遷移）*<br>Kaspersky Endpoint Security 不支援基於憑證的規則。 |
| **套用 Web 流量類別控制規則** | **Web 控制**（**Web 控制**子區段）<br>用於 Web 流量類別控制的封鎖規則被遷移到 Kaspersky Endpoint Security 中的單個封鎖規則。Kaspersky Endpoint Security 會忽略類別控制的允許規則。<br>下面列出了 KSWS 和 KES 類別的對應關係。 |
| **如果無法分類網頁，則允許存取** | *（不遷移）*<br>如果網頁無法分類，則 Kaspersky Endpoint Security 允許存取。 |
| **允許存取可用於損壞受防護裝置的合法 Web 資源** | *（不遷移）*<br>Kaspersky Endpoint Security 允許存取可用於損壞受防護裝置的合法 Web 資源。 |
| **允許存取合法廣告** | *（不遷移）*<br>您可以使用 Web 控制設定中的*廣告* Web 資源類別管理對合法廣告的存取。 |
| **執行模式**：<br>• **驅動程式攔截器**<br>• **重定向器**<br>• **外部代理** | *（不遷移）*<br>Kaspersky Endpoint Security 僅支援"驅動程式攔截器"模式。 |
| **ICAP 服務連線設定** | *（不遷移）*<br>Kaspersky Endpoint Security 不支援 ICAP 網路儲存防護。 |
| **檢查透過 HTTPS 協定建立的安全連線** | **掃描加密連線 / 始終掃描加密連線** 模式（**網路設定** 子區域） |
| **使用 TLS 合約版本** | *（不遷移）*<br>Kaspersky Endpoint Security 掃描透過以下協定傳輸的加密網路流量：<br>• SSL 3.0。<br>• TLS 1.0、TLS 1.1、TLS 1.2、TLS 1.3。<br>您還可以在加密連線掃描設定中封鎖 SSL 2.0 連線 |
| **不信任具有無效憑證的 Web 伺服器** | **位址**（**網路設定**子區段） |
| **攔截連接埠**（攔截區域） | **監控的連接埠**（**網路設定**子區段）<br>遷移期間，KES 會清除核取方塊**監控卡巴斯基建議的清單中的應用程式的所有連接埠**和**監控指定應用程式的所有連接埠**。 |
| **排除連接埠**（攔截區域） | *（不遷移）* |
| **排除 IP 位址**（攔截區域） | **設定受信任位址**（**網路設定**子區段） |
| **排除處理程序**（攔截區域） | **設定受信任應用程式**（**網路設定**子區段）<br>遷移過程中，KES 會配置受信任應用程式的以下設定：<br>• "**不掃描網路流量**"核取方塊會被選中。KES 不掃描網路流量查找任何 IP 位址和任何連接埠。<br>• 受信任應用程式設定中的其它核取方塊會被清除。 |
| **安全連接埠** | *（不遷移）* |

| Kaspersky Security for Windows Server 設定 | Kaspersky Endpoint Security for Windows 設定 |
| --- | --- |
| **使用惡意 URL 資料庫掃描 Web 連結** | **檢查網址是否在惡意網址資料庫中**（**Web 威脅防護**子區段） |
| **使用釣魚防護資料庫掃描網頁** | **檢查網址是否在釣魚網址資料庫中**（**Web 威脅防護**子區段） |
| **使用 KSN 防護** | *（不遷移）*<br>Kaspersky Endpoint Security 將 KSN 用於所有應用程式元件。 |
| **使用信任區域** | *（不遷移）*<br>Kaspersky Endpoint Security 將受信任區域套用到所有元件。您可以在 受信任區域設定中配置排除項目。 |
| **使用啟發式分析器** | **使用啟發式分析 (Web 威脅防護** and **郵件威脅防護**子區段） |
| **安全等級** | *（不遷移）*<br>Kaspersky Endpoint Security 對於 Web 威脅防護和郵件威脅防護元件有自己的安全等級。預設情況下，Kaspersky Endpoint Security 會設定建議的安全等級。 |
| **啟用郵件威脅防護** | **郵件威脅防護**（**郵件威脅防護**子區段）<br>**連線 Microsoft Outlook 延伸程式**<br><br>**僅接收的郵件** (防護範圍)<br>**接收時掃描** (電子郵件防護) |
| **排程設定** | *（不遷移）*<br>無法為元件配置單獨排程。該元件在 Kaspersky Endpoint Security 運行時始終處於開啟狀態。 |

## 弱點利用防禦

KSWS 弱點利用防禦設定被遷移到**進階威脅防護**區段的**弱點利用防禦**子區段。

弱點利用防禦設定

| Kaspersky Security for Windows Server 設定 | Kaspersky Endpoint Security for Windows 設定 |
| --- | --- |
| **防止易受感染的處理程序被弱點利用**：<br>• **發現弱點利用時終止**<br>• **僅通知** | **偵測到弱點時**：<br>• **封鎖**<br>• **通知** |
| **透過"終端服務"通知被利用的處理程序** | *（不遷移）*<br>Kaspersky Endpoint Security 不支援終端機服務。 |
| **即使 Kaspersky Security 服務已停用，也會防止易受感染的處理程序被弱點利用** | *（不遷移）*<br>Kaspersky Endpoint Security 不斷防止易受攻擊的處理程序利用。 |
| **受防護處理程序** | **啟用系統處理程序記憶體防護**<br>Kaspersky Endpoint Security 不支援選擇受防護的處理程序。您只能啟用系統處理程序記憶體防護。 |
| **弱點利用防禦技術**：<br>• **套用所有可用的弱點利用防禦技術**<br>• **套用所選的弱點利用防禦技術** | *（不遷移）*<br>Kaspersky Endpoint Security 套用所有可用的弱點利用防禦技術。 |

## 網路威脅防護

KSWS 網路威脅防護設定被遷移到**關鍵威脅防護**區段的**網路威脅防護**子區段。

網路威脅防護設定

| Kaspersky Security for Windows Server 設定 | Kaspersky Endpoint Security for Windows 設定 |
| --- | --- |
| **執行模式**：<br>• **直通**<br>• **僅通知網路攻擊**<br>• **偵測到攻擊時封鎖連線** | **網路威脅防護**<br>如果選擇"**直通**"模式，網路威脅防護將被停用。<br>如果選擇"**僅通知網路攻擊**"模式或"**偵測到攻擊時封鎖連線**"模式，網路威脅防護將被啟用。Kaspersky Endpoint Security 始終適用於**偵測到攻擊時封鎖連線**模式。 |
| **工作未執行時不停止流量分析** | *（不遷移）*<br>如果啟用該元件，Kaspersky Endpoint Security 會持續分析流量。 |

| Kaspersky Security for Windows Server 設定 | Kaspersky Endpoint Security for Windows 設定 |
| --- | --- |
| **不控制排除的 IP 位址** | **排除項目** |
| **排程設定** | *（不遷移）*<br>無法為元件配置單獨排程。該元件在 Kaspersky Endpoint Security 運行時始終處於開啟狀態。 |

### 指令碼監控

Kaspersky Endpoint Security 不支援指令碼監控元件。指令碼監控由其他元件處理，例如，AMSI 防護。

### 網站類別

Kaspersky Endpoint Security 不支援所有類別的 Kaspersky Security for Windows Server。不會遷移 Kaspersky Endpoint Security 中不存在的類別。因此，具有不受支援的類別 Web 資源分類規則不會被遷移。

網站類別

| Kaspersky Security for Windows Server 類別 | Kaspersky Endpoint Security for Windows 類別 |
| --- | --- |
| 戰爭遊戲 | 電腦遊戲 |
| 墮胎 | *（不遷移）* |
| 彩票（延伸） | 賭博、彩票、抽獎 |
| 酒精 | 酒精、煙草、毒品 |
| 匿名代理伺服器 | 匿名網站 |
| 厭食症 | *（不遷移）* |
| 房地產租金 | *（不遷移）* |
| 音訊、視訊和軟體 | 軟體、音訊、影片 |
| 銀行 | 銀行 |
| 部落格 | 網誌 |
| 軍隊 | 武器、爆裂物、軍事 |
| 針對孩子 | *（不遷移）* |
| 歧視 | 暴力，不寬容 |
| 家庭和家人 | *（不遷移）* |
| 託管和網域服務 | 網際網路通訊 |
| 寵物和動物 | *（不遷移）* |
| 法律與政治 | 被地區法律禁止 |
| 受 Roskomnadzor (RF) 限制 | 被俄羅斯聯邦法律禁止 |
| 受聯邦法律 436 限制 (RF) | 被俄羅斯聯邦法律禁止 |
| 受 RF 立法限制 | 被俄羅斯聯邦法律禁止 |
| 受全球立法限制 | 被地區法律禁止 |
| 成人約會 | 成人內容 |
| 網際網路服務 | *（不遷移）* |
| 性用品商店 | 成人內容 |
| 資訊技術 | *（不遷移）* |
| 賭場、紙牌遊戲 | 賭博、彩票、抽獎 |
| 書籍和寫作 | *（不遷移）* |
| 電腦遊戲 | 電腦遊戲 |
| 健康和美容 | *（不遷移）* |

| Kaspersky Security for Windows Server 類別 | Kaspersky Endpoint Security for Windows 類別 |
| --- | --- |
| 文化與社會 | *（不遷移）* |
| LGBT | 成人內容 |
| 彩票 | 賭博、彩票、抽獎 |
| 藥物 | *（不遷移）* |
| 時尚 | *（不遷移）* |
| 音樂 | *（不遷移）* |
| 毒品 | 酒精、煙草、毒品 |
| 暴力 | 暴力，不寬容 |
| 不滿 | *（不遷移）* |
| 非法毒品 | 酒精、煙草、毒品 |
| 仇恨和歧視 | 暴力，不寬容 |
| 淫穢詞彙 | 不雅文字 |
| 女用貼身內衣褲 | 成人內容 |
| 新聞 | 新聞媒體 |
| 裸體主意 | 成人內容 |
| 教育 | *（不遷移）* |
| 線上購物 | 線上商店 |
| 所有通訊媒體 | 網際網路通訊 |
| 信用卡支付 | 支付系統 |
| 線上購物（擁有支付系統） | 線上商店 |
| 線上百科全書 | *（不遷移）* |
| 線上銀行 | 銀行 |
| 武器 | 武器、爆裂物、軍事 |
| 釣魚和打獵 | *（不遷移）* |
| 支付系統 | 支付系統 |
| 求職 | 求職網站 |
| 搜尋引擎 | *（不遷移）* |
| 政策決定 (JP) | 被日本警方禁止 |
| 受 KPSN 信任 | *（不遷移）* |
| 不受 KPSN 信任 | *（不遷移）* |
| 煽情 | 成人內容 |
| 媒體託管和流 | 新聞媒體 |
| Web 郵件 | 網頁式電子郵件 |
| 旅行 | *（不遷移）* |
| 電視和廣播 | 新聞媒體 |
| 預告片和廣告服務 | 廣告 |
| 宗教 | 宗教活動 |
| 餐館、咖啡館和食物 | *（不遷移）* |
| 交友網站 | 約會網站 |
| 性教育 | 成人內容 |
| 社群網路 | 社群網路 |

| Kaspersky Security for Windows Server 類別 | Kaspersky Endpoint Security for Windows 類別 |
| --- | --- |
| 運動 | *（不遷移）* |
| 賭博 | 賭博、彩票、抽獎 |
| 自殺 | 暴力，不寬容 |
| 煙草 | 酒精、煙草、毒品 |
| 下載種子 | 檔案下載種子 |
| 聯邦極端分子名單中提及(RF) | 被俄羅斯聯邦法律禁止 |
| 檔案共用 | 檔案共用 |
| 藥房 | *（不遷移）* |
| 愛好和娛樂 | *（不遷移）* |
| 聊天和論壇 | 聊天、論壇、即時通訊 |
| 學校和大學頁面 | *（不遷移）* |
| 占星術和神秘學 | *（不遷移）* |
| 極端主義和種族主義 | 暴力，不寬容 |
| 電子商務 | 線上商店 |
| 情色 | 成人內容 |
| 幽默 | *（不遷移）* |

## 本機活動控制

### 應用程式啟動控制

KSWS 應用程式控制設定被遷移到**安全控制**區段的**應用程式控制**子區段。

應用程式啟動控制設定

| Kaspersky Security for Windows Server 設定 | Kaspersky Endpoint Security for Windows 設定 |
| --- | --- |
| **執行模式**：<br>• **僅統計**<br>• **啟動** | **動作**（應用程式控制）：<br>• **測試規則**<br>• **套用規則** |
| **在此檔案的所有後續啟動中重複針對首次檔案啟動執行的操作** | *（不遷移）*<br>Kaspersky Endpoint Security 在應用程式每次嘗試執行時對其掃描。 |
| **在沒有可執行的指令時拒絕指令解譯器啟動** | *（不遷移）*<br>如果命令解釋器未被應用程式控制禁止，則 Kaspersky Endpoint Security 允許執行它們。 |
| **規則** | **應用程式控制規則** *（支援但有限制）*<br>Kaspersky Endpoint Security 11.11.0 引入了對遷移應用程式啟動控制規則的支援。<br>應用程式啟動控制規則遷移功能有一些限制。預設情況下，KSWS 應用程式啟動控制包括兩條規則：<br>• **作業系統可信任憑證允許執行指令碼和 MSI**<br>• **作業系統可信任憑證允許執行可執行檔**<br>如果至少一個來源 KSWS 規則擁有**允許**類型，則在遷移過程中 KES 將建立一個新的允許規則，**擁有信任根憑證的應用程式**。換而言之，KES 應用程式控制規則將使用一個單個規則來允許執行的受信任指令碼、MSI 套件和可執行檔。如果兩個來源 KSWS 規則都擁有**拒絕**類型，則 KES 不新增用於管理擁有信任根憑證的應用程式的規則。 |
| **將規則套用於可執行檔** | *（不遷移）*<br>規則套用範圍不可在 KES 應用程式控制設定中進行配置。KES 應用程式控制可將規則套用到所有類型的檔案：可執行檔，指令碼和 MSI 套件。如果所有檔案類型包括在 KSWS 中的規則套用範圍中，在遷移過程中 KES 將移轉 KSWS 規則。如果某些檔案類型被從 KSWS 中的規則套用範圍中排除，則在遷移過程中 KES 也會移轉 KSWS 規則，但是**測試規則**會被選為應用程式控制動作。 |

| Kaspersky Security for Windows Server 設定 | Kaspersky Endpoint Security for Windows 設定 |
| --- | --- |
| **監控 DLL 模組的載入** | **監控 DLL 模組的載入（顯著增加系統負載）** |
| **將規則套用於指令碼和 MSI 資料套件** | *（不遷移）*<br>規則套用範圍不可在 KES 應用程式控制設定中進行配置。KES 應用程式控制可將規則套用到所有類型的檔案：可執行檔，指令碼和 MSI 套件。如果所有檔案類型包括在 KSWS 中的規則套用範圍中，在遷移過程中 KES 將移轉 KSWS 規則。如果某些檔案類型被從 KSWS 中的規則套用範圍中排除，則在遷移過程中 KES 會移轉 KSWS 規則，但是**測試規則**會被選為應用程式控制動作。 |
| **拒絕 KSN 不信任的應用程式** | *（不遷移）*<br>Kaspersky Endpoint Security 不考慮應用程式的聲譽，並根據規則允許或拒絕執行應用程式。 |
| **允許 KSN 信任的應用程式** | 遷移過程中，KES 會新增一個允許規則。**其他軟體\根據 KSN 信譽受信任的其他軟體** KL 類別被指定為規則觸發條件。 |
| **允許執行 KSN 信任的應用程式的使用者和/或使用者群組** | **使用者及其權限** 在包含 KL 類別的應用程式控制允許規則中 **其他軟體\根據 KSN 信譽受信任的其他軟體**。 |
| **自動允許透過列出的應用程式和套件分發軟體** | KSWS 和 KES 中的軟體分發控制工作方式不同。在遷移過程中，KES 會為允許自動軟體分發的應用程式新增允許規則。檔案雜湊被指定為規則觸發條件。 |
| **始終允許透過 Windows Installer 進行軟體分發** | KSWS 和 KES 中的軟體分發控制工作方式不同。在遷移過程中，KES 會為允許自動軟體分發的應用程式新增允許規則 (**允許的軟體分發應用程式和套件**)。檔案雜湊被指定為規則觸發條件。在帳戶屬性中**信任的更新程式**核取方塊被選取。 |
| **始終允許使用背景智慧傳輸服務透過 SCCM 進行軟體分發** | *（不遷移）* |
| **允許的軟體分發應用程式和資料套件** | KSWS 和 KES 中的軟體分發控制工作方式不同。在遷移過程中，KES 會為允許自動軟體分發的應用程式新增允許規則。檔案雜湊被指定為規則觸發條件。在帳戶屬性中**信任的更新程式**核取方塊被選取。 |
| **排程設定** | *（不遷移）*<br>如果在 KSWS 設定中為元件配置了排程，則在遷移時將啟用應用程式控制元件。如果在 KSWS 設定中沒有為元件配置排程，則在遷移時將停用應用程式控制。<br>無法為元件配置單獨排程。該元件在 Kaspersky Endpoint Security 運行時始終處於開啟狀態。 |

### 裝置控制

KSWS 裝置控制設定被遷移到**安全控制**區段的**裝置控制**子區段。

裝置控制設定

| Kaspersky Security for Windows Server 設定 | Kaspersky Endpoint Security for Windows 設定 |
| --- | --- |
| **執行模式**：<br>• **啟動**<br>• **僅統計** | *（不遷移）*<br>應用程式控制在"*啟動*"模式下運行。Audit 持續提供裝置連線統計。 |
| **未執行裝置控制工作時，允許使用所有外部裝置** | *（不遷移）*<br>在 Kaspersky Endpoint Security 執行時，裝置控制始終處於開啟狀態。 |
| **裝置控制規則** | **受信任裝置**<br>在遷移過程中，Kaspersky Endpoint Security 會忽略已停用的 KSWS 規則。 |
| **排程設定** | *（不遷移）*<br>Kaspersky Endpoint Security 使用自己的排程來獲取對某些裝置類型的存取權限。 |

## 網路附加儲存防護

### RPC 網路儲存防護

Kaspersky Endpoint Security 不支援網路附加儲存防護元件。如果您需要這些元件，您可以繼續使用 Kaspersky Security for Windows Server。

### ICAP 網路儲存防護

Kaspersky Endpoint Security 不支援網路附加儲存防護元件。如果您需要這些元件，您可以繼續使用 Kaspersky Security for Windows Server。

### Anti-Cryptor for NetApp

Kaspersky Endpoint Security 不支援 Anti-Cryptor for NetApp。Anti-Cryptor 功能由其他應用程式元件提供，例如行為偵測。

## 網路活動控制

### 防火牆管理

Kaspersky Endpoint Security 不支援 KSWS 防火牆管理。KSWS 防火牆功能由系統級別的防火牆執行。您可以在遷移後配置 Kaspersky Endpoint Security 防火牆。

### Anti-Cryptor

網路 Anti-Cryptor 設定被遷移到**進階威脅防護**區段的**行為偵測**子區段。

Anti-Cryptor 設定

| KSWS 設定 | KES 設定 |
| --- | --- |
| **執行模式**：<br>• **僅統計**<br>• **啟動** | **偵測到共用資料夾的外部加密時**：<br>• **通知**<br>• **封鎖** |
| **啟發式分析器** | *（不遷移）*<br>Kaspersky Endpoint Security 不使用啟發式分析進行行為偵測。 |
| **防護範圍的配置**：<br>• **受防護裝置上的所有共用網路資料夾**<br>• **僅指定的共用資料夾** | *（不遷移）*<br>Kaspersky Endpoint Security 禁止加密受防護電腦的所有共用網路資料夾。 |
| **排除** | *（不遷移）*<br>Kaspersky Endpoint Security 對於行為偵測元件有自己的排除項目。您可以在遷移後手動新增排除項目。 |
| **排程設定** | *（不遷移）*<br>無法為元件配置單獨排程。該元件在 Kaspersky Endpoint Security 運行時始終處於開啟狀態。 |

## 系統檢查

### 檔案完整性監控

來自 KSWS 的檔案完整性監控設定被遷移到**安全控制**區域的**系統完整性監控**子區域。

檔案完整性監控設定

| KSWS 設定 | KES 設定 |
| --- | --- |
| **記錄監控中斷期間發生的檔案操作資訊** | *（不遷移）*<br>Kaspersky Endpoint Security 不記錄監控中斷期間執行的檔案操作事件。 |
| **封鎖對 USN 記錄的入侵嘗試** | *（不遷移）*<br>Kaspersky Endpoint Security 不封鎖 USN 記錄入侵嘗試。 |
| **監控範圍** | **監控範圍 → *檔案*** *（支援但有限制）*<br>被停用的監控範圍紀錄不會被遷移到 KES。Kaspersky Endpoint Security 僅將啟用的紀錄遷移到監控範圍。 |
| **受信任使用者** | **受信任的使用者和/或使用者群組** |
| **檔案操作標記** | **檔案作業標誌** |
| **如果可能，計算檔案的總和檢查碼** | **散列** |
| **排除** | **排除項目 → 檔案** |

### 記錄檢查

KSWS 記錄檢查設定被遷移到**安全控制**區段的**記錄審查**子區段。

記錄檢查設定

| Kaspersky Security for Windows Server 設定 | Kaspersky Endpoint Security for Windows 設定 |
| --- | --- |
| **套用記錄審查的自訂規則** | *（不遷移）*<br>Kaspersky Endpoint Security 套用所有啟用的自訂規則。 |
| **自訂規則** | **自訂規則**<br>**系統中已安裝服務（用於 Server 2003 OS）**預定義規則不會被遷移到 KES。 |
| **針對記錄審查套用預定義規則** | *（不遷移）*<br>Kaspersky Endpoint Security 套用所有啟用的預定義規則。 |
| **預定義規則** | **預定義規則** |
| **密碼暴力破解偵測** | **暴力破解攻擊偵測** |
| **網路登入偵測** | **網路登入偵測** |
| **排除**（IP 位址） | **排除項目** (IP 位址) |
| **排除**（使用者） | **排除項目** (使用者) |
| **排程設定** | *（不遷移）*<br>無法為元件配置單獨排程。該元件在 Kaspersky Endpoint Security 運行時始終處於開啟狀態。 |

## 記錄和通知

### 工作記錄

KSWS 記錄設定被遷移到**一般設定**區段的**介面**和**報告和儲存。**子區段。

記錄設定

| Kaspersky Security for Windows Server 設定 | Kaspersky Endpoint Security for Windows 設定 |
| --- | --- |
| **事件記錄** | **通知**（**介面**子區段） |
| **記錄資料夾** | *（不遷移）*<br>Kaspersky Endpoint Security 將報告儲存在 `C:\ProgramData\Kaspersky Lab\KES.12.12\Report` 資料夾中。 |

| Kaspersky Security for Windows Server 設定 | Kaspersky Endpoint Security for Windows 設定 |
| --- | --- |
| **刪除 N 天前的工作記錄** | *（不遷移）*<br>您可以在**一般設定**、**報告和儲存。**下面配置 KES 報告的儲存期。 |
| **從稽核記錄事件中刪除 N 天** | *（不遷移）*<br>Kaspersky Endpoint Security 將報告儲存限制套用於所有報告，包括系統稽核報告。 |
| **與 SIEM 整合** | *（不遷移）*<br>您可以在卡巴斯基安全管理中心中配置與 SIEM 整合。 |

### 事件通知

KSWS 通知設定被遷移到**一般設定**區段的 **介面**子區段。

通知設定

| Kaspersky Security for Windows Server 設定 | Kaspersky Endpoint Security for Windows 設定 |
| --- | --- |
| **通知** | **通知** |
| **通知使用者**：<br>• **使用終端服務**<br>• **使用 Windows Messenger 服務指令** | *（不遷移）*<br>Kaspersky Endpoint Security 不支援修改通知文字。Kaspersky Endpoint Security 顯示標準通知。 |
| **通知管理員**：<br>• **使用 Windows Messenger 服務指令**<br>• **透過執行可執行檔**<br>• **透過傳送電子郵件** | 僅電子郵件通知設定被遷移到 Kaspersky Endpoint Security – **電子郵件通知設定 (通知** 塊）。不支援其他通知管理員的方法。 |
| **應用程式資料庫已過期** | **如果資料庫未更新時間如下，則傳送"資料庫過期"通知** |
| **應用程式資料庫已嚴重過期** | **如果資料庫未更新時間如下，則傳送"資料庫嚴重過期"通知** |
| **長時間未執行關鍵區域掃描** | *（不遷移）*<br>Kaspersky Endpoint Security 在三天后產生一個錯過的關鍵區域掃描事件。 |

### 與管理伺服器互動

KSWS 管理伺服器互動設定被遷移到**一般設定**區段的**報告和儲存。**子區段。

管理伺服器互動設定

| Kaspersky Security for Windows Server 設定 | Kaspersky Endpoint Security for Windows 設定 |
| --- | --- |
| **已隔離的檔案** | **隔離檔案** |
| **已備份的檔案** | **備份檔案** |
| **已封鎖的主機** | *（不遷移）*<br>Kaspersky Endpoint Security 會自動傳送有關被封鎖主機的資料。 |

## 工作

### 啟動應用程式

Kaspersky Endpoint Security 不支援*應用程式啟動*工作（KSWS）。您可以建立*新增金鑰*工作（KES），將產品授權金鑰新增到安裝套件, 或啟用產品授權金鑰自動分發。

### 複製更新

*複製更新*工作設定 (KSWS) 被遷移到*資料庫和應用程式模組更新*工作 (KES)。

複製更新工作設定

| Kaspersky Security for Windows Server 設定 | Kaspersky Endpoint Security for Windows 設定 |
|---|---|
| **更新來源**：<br>• **卡巴斯基安全管理中心管理伺服器**<br>• **卡巴斯基更新伺服器**<br>• **自訂 HTTP 或 FTP 伺服器，或網路資料夾** | **更新來源**：<br>• **卡巴斯基安全管理中心**<br>• **卡巴斯基更新伺服器**<br>• **由使用者指定** |
| **如果指定的伺服器無法使用，則使用卡巴斯基更新伺服器** | *（不遷移）*<br>Kaspersky Endpoint Security 允許選擇多個更新來源，包括卡巴斯基更新伺服器。如果第一個更新來源不可用，Kaspersky Endpoint Security 允許您從清單中的另一個來源獲取更新。 |
| **使用代理伺服器設定連線到卡巴斯基更新伺服器** | *（不遷移）*<br>Kaspersky Endpoint Security 為所有元件使用代理伺服器。你可以在應用程式的網路選項中配置代理伺服器連線。 |
| **使用代理伺服器設定連線至其他伺服器** | *（不遷移）*<br>Kaspersky Endpoint Security 為所有元件使用代理伺服器。你可以在應用程式的網路選項中配置代理伺服器連線。 |
| **複製更新設定**：<br>• **複製資料庫更新**<br>• **複製重要軟體模組更新**<br>• **複製資料庫更新和重要應用程式模組的更新** | *（不遷移）*<br>Kaspersky Endpoint Security 複製資料庫更新和應用程式模組的關鍵更新為當個套件。 |
| **用於本機儲存已複製更新的資料夾** | **將更新複製到資料夾** |

## 基線檔案完整性監控

*基線檔案完整性監控*工作設定 (KSWS) 被遷移到 *系統完整性檢查* 工作和政策部分 **安全控制**,子部分 **系統完整性監控**。

基線檔案完整性監控工作設定

| Kaspersky Security for Windows Server 設定 | Kaspersky Endpoint Security for Windows 設定 |
|---|---|
| **雜湊計算演算法**：<br>• **MD5**。<br>• **SHA256**。 | *（不遷移）*<br>Kaspersky Endpoint Security 使用 SHA256 演算法進行總和檢查碼計算。 |
| **掃描範圍** | **監控範圍**（**系統完整性監控**子區段） |

## 資料庫更新

*資料庫更新*工作設定 (KSWS) 被遷移到*資料庫和應用程式模組更新*工作 (KES)。

"資料庫更新"工作設定

| Kaspersky Security for Windows Server 設定 | Kaspersky Endpoint Security for Windows 設定 |
|---|---|
| **更新來源**：<br>• **卡巴斯基安全管理中心管理伺服器**<br>• **卡巴斯基更新伺服器**<br>• **自訂 HTTP 或 FTP 伺服器，或網路資料夾** | **更新來源**：<br>• **卡巴斯基安全管理中心**<br>• **卡巴斯基更新伺服器**<br>• **由使用者指定** |
| **如果指定的伺服器無法使用，則使用卡巴斯基更新伺服器** | *（不遷移）*<br>Kaspersky Endpoint Security 允許選擇多個更新來源，包括卡巴斯基更新伺服器。如果第一個更新來源不可用，Kaspersky Endpoint Security 允許您從清單中的另一個來源獲取更新。 |
| **使用代理伺服器設定連線到卡巴斯基更新伺服器** | *（不遷移）*<br>Kaspersky Endpoint Security 為所有元件使用代理伺服器。你可以在應用程式的網路選項中配置代理伺服器連線。 |

| Kaspersky Security for Windows Server 設定 | Kaspersky Endpoint Security for Windows 設定 |
| --- | --- |
| **使用代理伺服器設定連線至其他伺服器** | *（不遷移）*<br>Kaspersky Endpoint Security 為所有元件使用代理伺服器。你可以在應用程式的網路選項中配置代理伺服器連線。 |
| **降低磁碟 I/O 上的負載** | *（不遷移）* |

## 軟體模組更新

*軟體模組更新*工作設定 (KSWS) 被遷移到*資料庫和應用程式模組更新*工作 (KES)。

"軟體模組更新"工作設定

| Kaspersky Security for Windows Server 設定 | Kaspersky Endpoint Security for Windows 設定 |
| --- | --- |
| **更新來源**：<br>• **卡巴斯基安全管理中心管理伺服器**<br>• **卡巴斯基更新伺服器**<br>• **自訂 HTTP 或 FTP 伺服器，或網路資料夾** | **更新來源**：<br>• **卡巴斯基安全管理中心**<br>• **卡巴斯基更新伺服器**<br>• **由使用者指定** |
| **如果指定的伺服器無法使用，則使用卡巴斯基更新伺服器** | *（不遷移）*<br>Kaspersky Endpoint Security 允許選擇多個更新來源，包括卡巴斯基更新伺服器。如果第一個更新來源不可用，Kaspersky Endpoint Security 允許您從清單中的另一個來源獲取更新。 |
| **使用代理伺服器設定連線到卡巴斯基更新伺服器** | *（不遷移）*<br>Kaspersky Endpoint Security 為所有元件使用代理伺服器。你可以在應用程式的網路選項中配置代理伺服器連線。 |
| **使用代理伺服器設定連線至其他伺服器** | *（不遷移）*<br>Kaspersky Endpoint Security 為所有元件使用代理伺服器。你可以在應用程式的網路選項中配置代理伺服器連線。 |
| **複製並安裝重要軟體模組更新** | **安裝重大和批准的更新** |
| **僅檢查關鍵軟體更新是否可用** | *（不遷移）*<br>Kaspersky Endpoint Security 不斷檢查應用程式模組重大更新的可用性。 |
| **允許作業系統重新啟動** | *（不遷移）*<br>Kaspersky Endpoint Security 會提示使用者出示權限以重新啟動電腦。 |
| **接收有關可用的排程軟體模組更新的資訊** | *（不遷移）*<br>Kaspersky Endpoint Security 顯示有關軟體模組更新的通知。 |

## 應用程式資料庫更新回溯

*應用程式資料庫更新回溯*工作設定 (KSWS) 被遷移到*更新回溯*工作 (KES)。新的 *更新回溯* 工作（KES）有一個工作啟動排程 – *手動*。

## 按需掃描

*按需掃描*工作設定 (KSWS) 被遷移到*惡意軟體掃描*工作 (KES)。

"病毒掃描"工作設定

| Kaspersky Security for Windows Server 設定 | Kaspersky Endpoint Security for Windows 設定 |
| --- | --- |
| **掃描範圍** | **掃描範圍** |
| **防護等級**：<br>• **最佳防護**<br>• **建議**<br>• **最佳效能** | **安全等級**：<br>• **高**<br>• **建議防護**<br>• **低**<br>KSWS 和 KES 中的安全等級設定不同。 |

| Kaspersky Security for Windows Server 設定 | Kaspersky Endpoint Security for Windows 設定 |
| --- | --- |
| **掃描物件**：<br>• **所有物件**<br>• **按格式掃描物件**<br>• **按病毒資料庫中指定的副檔名清單掃描物件**<br>• **按指定的副檔名清單掃描物件** | **檔案類型**：<br>• **所有檔案**<br>• **按格式掃描檔案**<br>• **按副檔名掃描檔案**<br>Kaspersky Endpoint Security 不允許建立自訂副檔名清單。Kaspersky Endpoint Security 用**按副檔名掃描檔案**值替換了**按指定的副檔名清單掃描物件**值。 |
| **子資料夾** | **包含子資料夾** |
| **子檔案** | *（不遷移）* |
| **掃描開機磁區和 MBR** | *（不遷移）* |
| **掃描 NTFS 交換資料串流** | *（不遷移）* |
| **僅掃描新增與變更過的檔案** | **只掃描新增及修改的檔案** |
| **掃描複合檔案**：<br>• **全部 壓縮檔案**<br>• **所有 SFX 壓縮檔案**<br>• **全部 電子郵件資料庫**<br>• **全部 封包物件**<br>• **全部 普通電子郵件**<br>• **全部 內嵌 OLE 物件** | **掃描複合檔案**：<br>• **掃描壓縮檔案**<br>• **掃描受密碼防護的壓縮檔案**<br>• **掃描分發套件**<br>• **掃描電子郵件格式檔案**<br>• **掃描 Microsoft Office 格式的檔案** |
| **對受感染物件和其他物件執行的操作**：<br>• **解毒**<br>• **解毒。無法解毒時刪除**<br>• **刪除**<br>• **執行建議的操作**<br>• **僅通知** | **偵測到威脅後的動作**：<br>• **解毒；若解毒失敗則刪除**<br>• **解毒；若解毒失敗則通知**<br>• **通知** |
| **對可疑物件執行的操作**：<br>• **隔離**<br>• **刪除**<br>• **執行建議的操作**<br>• **僅通知** | *（不遷移）*<br>如果偵測到任何威脅，則 Kaspersky Endpoint Security 套用該動作。 |
| **根據偵測到的物件的類型執行操作** | *（不遷移）* |
| **如果偵測到嵌入物件，完全刪除應用程式無法修改的複合檔案** | *（不遷移）* |
| **排除檔案** | *（不遷移）*<br>Kaspersky Endpoint Security 將受信任區域套用到所有元件。您可以在 受信任區域設定中配置排除項目。 |
| **不偵測** | *（不遷移）* |
| **如果時間超過 N 秒，則停止掃描** | **略過掃描時間超過以下值的檔案 N 秒** |
| **不掃描大小大於 N MB 的復合物件** | **複合檔案大於指定值時不解壓縮** |
| **使用 iSwift 技術** | **iSwift 技術** |
| **使用 iChecker 技術** | **iChecker 技術** |
| **掃描離線檔案**：<br>• **不掃描**<br>• **僅掃描檔案常駐部分**<br>• **掃描完整檔案**<br>• **僅當指定週期內存取了檔案（天）**<br>• **如果可以，不複製檔案到本機硬碟磁碟機** | *（不遷移）*<br>Kaspersky Endpoint Security 完整掃描線下檔案。 |

### 應用程式完整性檢查

*應用程式完整性控制*工作設定 (KSWS) 被遷移到*應用程式完整性檢查*工作 (KES)。

### 應用程式啟動控制規則產生器

Kaspersky Endpoint Security 不支援*應用程式啟動控制產生器*工作。您可以在應用程式控制設定中產生規則。

**裝置控制規則產生器**

Kaspersky Endpoint Security 不支援*裝置控制規則產生器*工作。您可以在裝置控制設定中產生存取規則。

# 遷移 KSWS 元件

在本機安裝前，Kaspersky Endpoint Security 會檢查電腦中是否存在卡巴斯基應用程式。如果電腦上安裝了 Kaspersky Security for Windows Server，KES 會偵測已安裝的 KSWS 元件集合並選擇相同的元件進行安裝。

KSWS 沒有的 KES 元件安裝如下：

- AMSI 防護、主機入侵防禦、修復引擎均使用預設設定安裝。
- BadUSB 攻擊防護、適應性異常控制、資料加密、Detection and Response 元件被忽略。

遠端安裝時，KES 應用程式會忽略已安裝的 KSWS 元件集合。安裝程式會安裝您在安裝套件的屬性中選擇的元件。安裝 Kaspersky Endpoint Security 和遷移政策和工作後，KES 設定會根據 KSWS 設定進行配置。

# 遷移 KSWS 工作和政策

您可以用下方式遷移 KSWS 政策和工作設定：

- 使用政策和工作批量轉換精靈（以下也稱為"遷移精靈"）。

  > KSWS 的遷移精靈僅在管理主控台 (MMC) 中可用。政策和工作設定無法在網頁主控台和雲端主控台中進行遷移。

  對於不同版本的卡巴斯基安全管理中心，批量轉換精靈有不同的運作方式。我們建議將解決方案升級到版本 14.2 或更高版本。在此版本的卡巴斯基安全管理中心中，政策和工作批量轉換精靈允許您將政策遷移到設定檔而不是政策。在此版本的卡巴斯基安全管理中心中，政策和工作批量轉換精靈還允許您遷移範圍更廣的政策設定。

- 使用 Kaspersky Endpoint Security for Windows 的新政策精靈。

  新政策精靈允許您基於 KSWS 政策建立 KES 政策。

使用遷移精靈和新政策精靈時，KSWS 政策遷移過程不同。

## 政策和工作批量轉換精靈

遷移精靈將 KSWS 政策設定而不是 KES 政策設定轉移到政策設定檔中。*政策設定檔*是一組政策設定，如果電腦滿足配置的啟動規則，它們就會在電腦上啟動。`UpgradedFromKSWS` 裝置標籤被選擇作為政策設定檔的觸發標準。卡巴斯基安全管理中心自動新增 `UpgradedFromKSWS` 標籤到您使用遠端安裝工作在 KSWS 之上安裝 KES 的所有電腦。如果您選擇了不同的安裝方法，您可以手動將標籤分配給裝置。

向裝置新增標籤：

1. 為伺服器建立一個新標籤 — `UpgradedFromKSWS`。

   有關為裝置建立標籤的詳細資訊，請參閱卡巴斯基安全管理中心說明。

2. 在卡巴斯基安全管理中心主控台中建立一個新的管理群組，新增您要為其分配標籤的伺服器。

   您可以使用選擇工具對伺服器進行分組。有關使用選擇的詳細資訊，請參閱卡巴斯基安全管理中心說明。

3. 在卡巴斯基安全管理中心主控台中選擇管理組的所有伺服器，開啟所選伺服器的屬性並分配標籤。

如果您要遷移多個 KSWS 政策，則每個政策都將被轉換為一個總體政策中的設定檔。如果 KSWS 政策已包含設定檔，這些設定檔也將作為設定檔遷移。因此，您將獲得一個單一的政策，其中包括與所有 KSWS 政策相對應的設定檔。

**如何使用政策和工作批量轉換精靈遷移 KSWS 政策設定**

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

   政策和工作批量轉換精靈將啟動。按照精靈的說明進行操作。

### 步驟 1. 選擇需要為其轉換政策和工作的應用程式

在此步驟，您需要選擇 Kaspersky Endpoint Security for Windows。前往下一步。

### 步驟 2. 轉換政策

遷移精靈在 KES 政策內建立 KSWS 政策設定檔。選擇要轉換為政策設定檔的 Kaspersky Security for Windows Server 政策。前往下一步。

遷移精靈將開始轉換政策。新政策設定檔的名稱將與原始 KSWS 政策相對應。

### 步驟 3. 政策遷移報告

遷移精靈將建立一個政策遷移報告。政策遷移報告包含政策轉換的日期和時間、原始 KSWS 政策的名稱、目標 KES 政策的名稱以及新政策設定檔的名稱。

### 步驟 4. 轉換工作

遷移精靈將為 Kaspersky Endpoint Security for Windows 建立新工作。在工作清單中，選擇您想為 Kaspersky Endpoint Security 建立的 KSWS 工作。新工作將被命名為 *<KSWS 工作名稱>（已轉換）*。前往下一步。

### 步驟 5. 精靈完成

結束精靈。結果，精靈將執行以下操作：

- 新政策設定檔被新增到 Kaspersky Endpoint Security 政策中。

  該政策包括具有 Kaspersky Security for Windows Server 的設定的設定檔。新政策的狀態為“*作用中*”。精靈保持 KSWS 政策不變。

- 建立新的 Kaspersky Endpoint Security 工作。

  新工作是 KSWS 工作的副本。精靈保持 KSWS 工作不變。

具有 KSWS 設定的新政策設定檔將被命名為 *UpgradedFromKSWS <Kaspersky Security for Windows Server 政策名稱>*。在設定檔屬性中，遷移精靈會自動選擇 `UpgradedFromKSWS` 裝置標籤作為觸發標準。因此，政策設定檔的設定會被自動套用到伺服器。

## 基於 KSWS 政策建立政策的精靈

當基於 KSWS 政策建立 KES 政策時，精靈會相應地將設定傳輸到新政策。即一個 KES 政策對應一個 KSWS 政策。該精靈不會將政策轉換為設定檔。

**如何使用新政策精靈遷移 KSWS 政策設定**

1. 開啟卡巴斯基安全管理中心管理主控台。
2. 在管理主控台樹狀目錄的“**受管理裝置**”資料夾中，選取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. 點擊“**新政策**”。

   啟動“政策精靈”。
5. 按照“政策精靈”的說明進行操作。

### 步驟 1. 選取要建立群組政策的應用程式

選取 **Kaspersky Endpoint Security for Windows (12.12)**應用程式。

### 步驟 2. 命名群組政策

輸入群組政策的名稱，例如，*辦公室政策*。

選擇“**使用早期版本應用程式的政策設定**”核取方塊。點擊“**瀏覽**”並選擇 KSWS 政策。

### 步驟 3. 參與卡巴斯基安全網絡

請閱讀並接受卡巴斯基安全網路 (KSN) 聲明的條款。

### 步驟 4.選擇電腦上的應用程式使用模式

選擇"**標準模式**"。Kaspersky Endpoint Security 為所有應用程式模式和作業係統類型提供通用政策。

我們建議針對不同模式和作業系統類型使用不同的政策。

### 步驟 5. 配置受信任區域

配置受信任區域。您可以新增預定義的 掃描排除項目 和 受信任應用程式。預先定義的掃描排除項目和受信任應用程式有助於在 SQL 伺服器、Microsoft Exchange 伺服器和 System Center Configuration Manager 上快速設定 Kaspersky Endpoint Security。這意味著您無需在伺服器上為應用程式手動設定受信任區域。預定義掃描排除項目和受信任應用程式還可以幫助您在Citrix 和 Vmware虛擬環境中以虛擬環境中以 Light Agent 模式快速設定 Kaspersky Endpoint Security。

### 步驟 6. 選擇政策狀態

- **作用中**下次同步後，該政策將用作電腦上的活動政策。

  活動政策的設定在同步期間儲存到用戶端電腦上。您無法同時將多個政策套用到一台電腦，因此每個群組只能有一個政策處於活動狀態。

- **非作用中**備份政策。如有必要，不活動政策可切換為活動狀態。

  您可以建立無限數量的不活動政策。不活動政策不影響網路中電腦的應用程式設定。不活動政策用作緊急情況（如病毒攻擊）的後備。如果存在透過快閃記憶體磁碟機進行的攻擊，您可以啟動用於封鎖存取快閃記憶體磁碟機的政策。在這種情況下，活動政策會自動變為不活動。

- **漫遊**當電腦離開組織網路周界時，將啟動該政策。

結束精靈。

## 遷移後政策和工作的額外配置

KSWS 和 KES 具有不同的元件集合和政策設定，因此遷移後您必須驗證政策設定是否滿足您的公司安全要求。

檢查以下基本政策設定：

- 密碼防護。KSWS 密碼防護設定未遷移。Kaspersky Endpoint Security 具有內建密碼防護功能。如有需要，開啟密碼防護並設定密碼。

- 受信任區域。KSWS 和 KES 用於選擇物件的方法不同。遷移時，KES 支援定義為單個檔案或檔案/資料夾路徑的排除項目。如果 KSWS 將排除項目配置為預定義區域或指令碼 URL，則不會遷移此類排除項目。遷移後，您必須手動新增此類排除項目。

  為確保 Kaspersky Endpoint Security 在伺服器上正常工作，建議將對伺服器功能重要的檔案新增到受信任區域。對於 SQL 伺服器，您必須新增 MDF 和 LDF 資料庫檔案。對於 Microsoft Exchange 伺服器，您必須新增 CHK、EDB、JRS、LOG 和 JSL 檔案。您可以使用遮罩，例如，`C:\Program Files (x86)\Microsoft SQL Server\*.mdf`。

  從 Kaspersky Endpoint Security 12.6 for Windows 開始，掃描排除項目和受信任應用程式被新增到受信任區域。預先定義的掃描排除項目和受信任應用程式有助於在 SQL 伺服器、Microsoft Exchange 伺服器和 System Center Configuration Manager 上快速設定 Kaspersky Endpoint Security。這意味著您無需在伺服器上為應用程式手動設定受信任區域。

- 防火牆。KSWS 防火牆功能由系統級別的防火牆執行。在 KES 中，一個單獨的元件負責防火牆功能。您可以在遷移後配置 Kaspersky Endpoint Security 防火牆。

- 卡巴斯基安全網路。Kaspersky Endpoint Security 不支援為單個元件配置 KSN。Kaspersky Endpoint Security 將 KSN 用於所有應用程式元件。要使用 KSN，您必須接受卡巴斯基安全網路聲明的新條款和條件。

- Web 控制。用於 Web 流量類別控制的封鎖規則被遷移到 Kaspersky Endpoint Security 中的單個封鎖規則。Kaspersky Endpoint Security 會忽略類別控制的允許規則。Kaspersky Endpoint Security 不支援所有類別的 Kaspersky Security for Windows Server。不會遷移 Kaspersky Endpoint Security 中不存在的類別。因此，具有不受支援的類別 Web 資源分類規則不會被遷移。如有需要，新增 Web 控制規則。

- 代理伺服器。代理伺服器連線密碼未遷移。手動輸入用於連線代理伺服器的密碼。

- 單個元件的排程。Kaspersky Endpoint Security 不支援為單個元件配置排程。元件在 Kaspersky Endpoint Security 運行時始終處於開啟狀態。

- 元件集合。可用的 Kaspersky Endpoint Security 功能集取決於作業系統的類型：工作站或伺服器。例如，在加密工具之外，伺服器上只有 BitLocker 磁碟機加密可用。

- 屬性。屬性的狀態未遷移。屬性將具有預設值。預設情況下，新政策中的幾乎所有設定都禁止修改子政策和本機應用程式介面中的設定。對於**Managed Detection and Response (Industrial CyberSecurity)**區段中的政策設定和**使用者支援**設定群組（**介面**區段），該屬性具有 值 。必要的話，配置從父政策繼承設定。

- *處理活動威脅*。進階解毒的工作方式對工作站和伺服器不同。您可以在*惡意軟體掃描*工作設定和應用程式設定中配置進階解毒。

- 升級應用程式。要在不重新啟動的情況下安裝主要更新和修補程式，您必須變更應用程式升級模式。預設情況下，安裝應用程式更新而不重新啟動功能被停用。

- Kaspersky Endpoint Agent。Kaspersky Endpoint Security 具有可處理 Detection and Response 解決方案的內建代理。如有需要，將 Kaspersky Endpoint Agent 政策設定傳輸到 Kaspersky Endpoint Security 政策。

- *資料庫和應用程式模組更新*工作。確保*資料庫和應用程式模組更新*工作的設定已正確遷移。KES 使用單個 KES 工作而不是 KSWS 的三個工作。您可以最佳化*資料庫和應用程式模組更新*工作並刪除多餘的工作。

- 其他工作。應用程式控制、裝置控制和檔案完整性監視元件在 KSWS 和 KES 中的工作方式不同。KES 不使用*基線檔案完整性監控*、*應用程式啟動控制產生器*、*裝置控制規則產生器*工作。因此，這些工作不會被遷移。遷移後，您可以配置檔案完整性監控、應用程式控制、裝置控制元件。

# 遷移 KSWS 受信任區域

*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。您可以使用 *政策和工作批量轉換精靈*或*根據 KSWS 政策建立新的 KES 政策精靈* 將信任區域物件從 KSWS 遷移到 KES。KSWS 和 KES 具有不同的元件集合和功能，因此遷移後您必須驗證排除項目是否滿足您的公司安全要求。將排除項目新增到受信任區域的方法對於 KES 和 KSWS 也不同。遷移精靈沒有可遷移所有 KSWS 排除項目的工具。這意味著遷移後您必須手動新增某些 KSWS 排除項目。

為確保 Kaspersky Endpoint Security 在伺服器上正常工作，建議將對伺服器功能重要的檔案新增到受信任區域。對於 SQL 伺服器，您必須新增 MDF 和 LDF 資料庫檔案。對於 Microsoft Exchange 伺服器，您必須新增 CHK、EDB、JRS、LOG 和 JSL 檔案。您可以使用遮罩，例如，`C:\Program Files (x86)\Microsoft SQL Server\*.mdf`。

從 Kaspersky Endpoint Security 12.6 for Windows 開始，掃描排除項目和受信任應用程式被新增到受信任區域。預先定義的掃描排除項目和受信任應用程式有助於在 SQL 伺服器、Microsoft Exchange 伺服器和 System Center Configuration Manager 上快速設定 Kaspersky Endpoint Security。這意味著您無需在伺服器上為應用程式手動設定受信任區域。

KES 和 KSWS 受信任區域建立方法。

| KSWS | | KES |
|---|---|---|
| **要掃描的物件** | | |
| • 預定義範圍 | *（不遷移）* | |
| • 瓷碟，資料夾或網路位置 | → | **檔案或資料夾** |
| • 檔案 | → | **檔案或資料夾** |
| • 指令碼檔案或網址 | *（不遷移）* | |
| **偵測到的物件** | → | **偵測到的物件類型** |
| **受信任處理程序** | → | **受信任應用程式** |

## 掃描物件遷移

在內容中選擇了**要掃描的物件**方法的 KSWS 排除項目將被遷移到在內容中選擇了**檔案或資料夾**方法的 KES 排除項目，但是有某些限制。排除項目遷移取決於物件選擇方法：

- 預定義範圍 – *不遷移*。

  遷移後，您必須手動新增此類排除項目。作為預定義區域的排除項目必須在*惡意軟體掃描*工作設定中進行配置。

- 瓷碟，資料夾或網路位置 – 遷移到在內容中選擇了“檔案或資料夾”方法的 KES 排除項目。

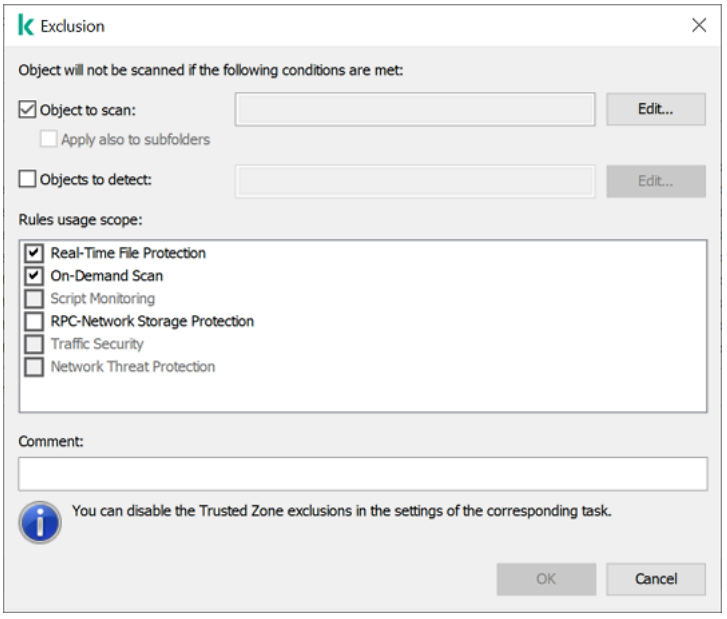
- 檔案 – 遷移到在內容中選擇了"檔案或資料夾"方法的 KES 排除項目。
- 指令碼檔案或網址 – *不遷移*。

  遷移後，您必須手動新增此類排除項目。作為指令碼網址的排除項目必須新增到 Web 威脅防護的受信任網址。

如果為被掃描物件選擇了**也套用到子資料夾**核取方塊，則該設定將被遷移到 KES 排除項目（**包含子資料夾**核取方塊）。




KES 排除項目設定




KSWS 排除項目設定

## 遷移偵測到的物件

在內容中選擇了**偵測到的物件**方法的 KSWS 排除項目將被遷移到在內容中選擇了**偵測到的物件類型**方法的 KES 排除項目。對應Kaspersky 百科全書分類的偵測到的物件的名稱（例如，`Email-Worm`、`Rootkit` 或 `RemoteAdmin`）。Kaspersky Endpoint Security 支援包含問號 `?`（比對任何單個字元）和星號 `*`（比對任何字元序列）的遮罩。

## 遷移排除項目使用範圍

排除項目的使用範圍是排除項目對其套用的元件集合。KES 和 KSWS 的元件集合不同，因此遷移精靈無法遷移排除項目使用範圍。因此，如果在 KSWS 使用範圍中選擇了至少一個元件，則 KES 會將排除項目套用到所有應用程式元件。

您可以在受信任區域設定中和 KSWS 防護元件的設定中設定 KSWS 使用範圍。為此，您可以在政策的相應區域中選擇或清除**套用信任區域**核取方塊。KES 防護元件的設定不包括此類核取方塊。這意味著單個元件設定中的受信任區域狀態會在遷移時丟失。完成遷移後，請在 KES 政策的受信任區域設定中選擇排除項目對其套用的元件。

## 遷移註解

KSWS 受信任區域的註解會不做修改遷移到 KES 排除項目註解。

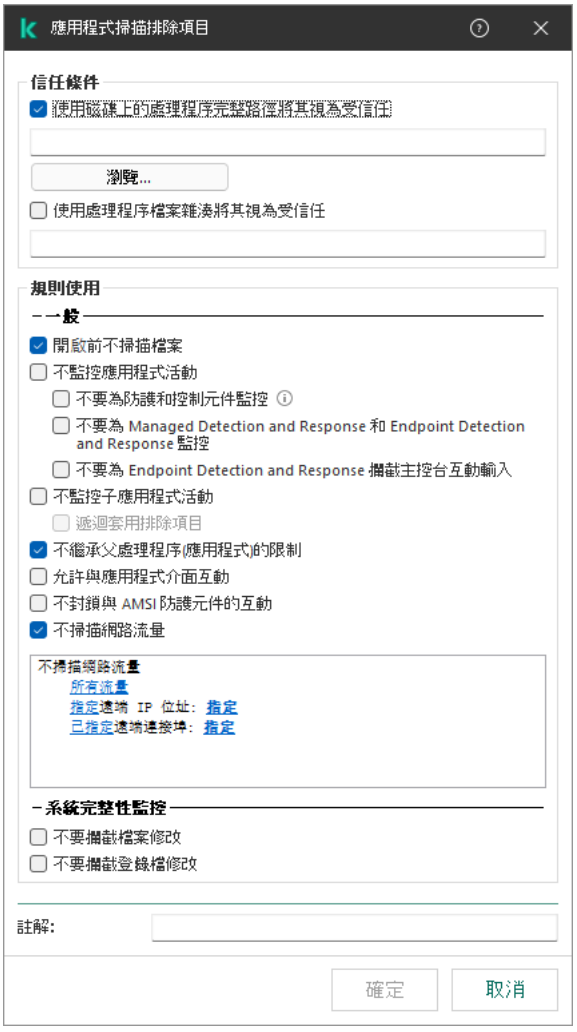
## 遷移受信任處理程序

KSWS 受信任處理程序可遷移到 KES 受信任處理程序，但有某些限制。遷移受信任處理程序取決於物件選擇方法：

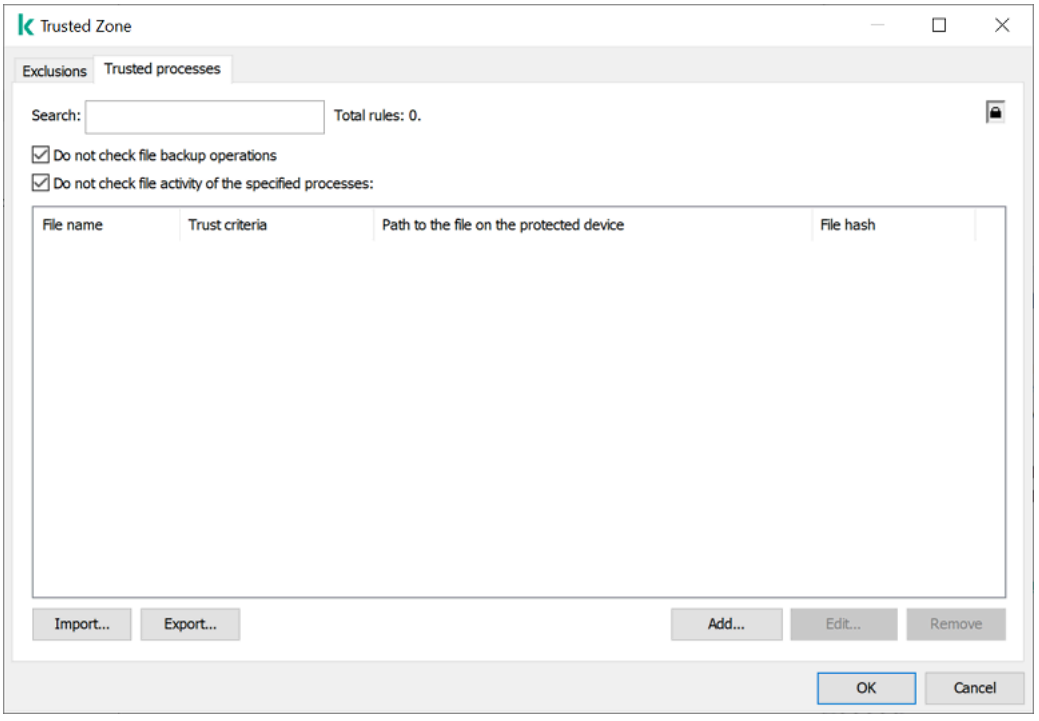
- 受防護裝置上的檔案路徑 – 遷移到 KES 受信任應用程式。
- 檔案雜湊 – *不遷移*。

如果 KSWS 具有配置為檔案雜湊的受信任處理程序，則不會遷移此類受信任處理程序。遷移後，您必須手動新增此類受信任處理程序。

如果在受信任處理程序設定中選擇了**不檢查檔案備份操作**核取方塊，則該設定將被遷移到 KES 受信任應用程式（**不監控應用程式活動**核取方塊）。




KES 受信任應用程式設定




KSWS 受信任處理程序設定

# 遷移 KSWS 應用程式啟動控制規則

KSWS 應用程式啟動控制被預設封鎖。也就是說，應用程式啟動控制會自動封鎖規則中未指定為允許的應用程式的所有應用程式。因此，KES 應用程式控制的遷移精靈會自動設定**允許清單**控制模式，對應預設封鎖原則。

您可以使用 *政策和工作批量轉換精靈*或*根據 KSWS 政策建立新的 KES 政策精靈* 將規則從 KSWS 遷移到 KES。

## 遷移應用程式啟動控制的模式

KSWS 應用程式啟動控制的模式遷移到 KES 應用程式控制，如下所示：

- **僅統計 → 測試規則**;
- **作用中 → 套用規則**。

## 遷移 KSWS 應用程式啟動控制預定義規則

預設情況下，KSWS 應用程式啟動控制包括兩條規則：

- **作業系統可信任憑證允許執行指令碼和 MSI**
- **作業系統可信任憑證允許執行可執行檔**

預定義規則允許執行由受信任的根憑證簽章的*指令碼*、*MSI 套件*和 *執行檔* 。如果至少一個預定義 KSWS 規則擁有**允許**類型，則遷移精靈將建立一個新的允許規則，**擁有信任根憑證的應用程式**。換而言之，KES 應用程式控制規則將使用一個單個規則來允許執行的受信任指令碼、MSI 套件和可執行檔。

如果兩個 KSWS 預先定義規則都有**拒絕**類型，KES 將略過預定義的規則。

## 遷移 KSWS 應用程式啟動控制自訂規則

KSWS 應用程式啟動控制規則根據以下標準調節檔案的執行：

- 包含數位憑證的簽章；
- SHA256 雜湊；
- 檔案路徑。

KSWS 和 KES 中的規則建立方式不同，因此遷移精靈會建立 *應用程式類別*，其中包括 KSWS 規則的條件和排除項目，並將這些應用程式類別新增至 KES 規則。精靈使用 應用類別中的**憑證**, **資料夾路徑**和**檔案雜湊**條件。卡巴斯基安全管理中心管理主控台在**應用程式管理 → 應用程式類別**部分中提供新的應用程式類別。

遷移精靈依照類型和使用者對 KSWS 規則進行分組。接下來，精靈將建立包含 KSWS 規則中的條件和排除項目的應用程式類別，並將應用程式類別新增至新的 KES 規則中。精靈會在 KES 規則的**敘述**欄位中指定 KSWS 規則的名稱。

## 遷移 KSWS 應用程式啟動控制進階設定

KSWS 應用程式啟動控制和 KES 應用程式控制的操作原理不同，因此遷移精靈可能會遷移設定的子集。

應用程式啟動控制設定

| Kaspersky Security for Windows Server 設定 | Kaspersky Endpoint Security for Windows 設定 |
| --- | --- |
| **在此檔案的所有後續啟動中重複針對首次檔案啟動執行的操作** | *（不遷移）*<br>Kaspersky Endpoint Security 在應用程式每次嘗試執行時對其掃描。 |
| **在沒有可執行的指令時拒絕指令解譯器啟動** | *（不遷移）*<br>如果命令解釋器未被應用程式控制禁止，則 Kaspersky Endpoint Security 允許執行它們。 |
| **將規則套用於可執行檔** | *（不遷移）*<br>規則套用範圍不可在 KES 應用程式控制設定中進行配置。KES 應用程式控制可將規則套用到所有類型的檔案：可執行檔，指令碼和 MSI 套件。如果所有檔案類型包括在 KSWS 中的規則套用範圍中，在遷移過程中 KES 將移轉 KSWS 規則。如果某些檔案類型被從 KSWS 中的規則套用範圍中排除，則在遷移過程中 KES 也會移轉 KSWS 規則，但是**測試規則**會被選為應用程式控制動作。 |
| **監控 DLL 模組的載入** | **監控 DLL 模組的載入（顯著增加系統負載）** |
| **將規則套用於指令碼和 MSI 資料套件** | *（不遷移）*<br>規則套用範圍不可在 KES 應用程式控制設定中進行配置。KES 應用程式控制可將規則套用到所有類型的檔案：可執行檔，指令碼和 MSI 套件。如果所有檔案類型包括在 KSWS 中的規則套用範圍中，在遷移過程中 KES 將移轉 KSWS 規則。如果某些檔案類型被從 KSWS 中的規則套用範圍中排除，則在遷移過程中 KES 會移轉 KSWS 規則，但是**測試規則**會被選為應用程式控制動作。 |
| **拒絕 KSN 不信任的應用程式** | *（不遷移）*<br>Kaspersky Endpoint Security 不考慮應用程式的聲譽，並根據規則允許或拒絕執行應用程式。 |
| **允許 KSN 信任的應用程式** | 遷移過程中，KES 會新增一個允許規則。**其他軟體\根據 KSN 信譽受信任的其他軟體** KL 類別被指定為規則觸發條件。 |
| **允許執行 KSN 信任的應用程式的使用者和/或使用者群組** | **使用者及其權限** 在包含 KL 類別的應用程式控制允許規則中 **其他軟體\根據 KSN 信譽受信任的其他軟體**。 |
| **自動允許透過列出的應用程式和套件分發軟體** | KSWS 和 KES 中的軟體分發控制工作方式不同。在遷移過程中，KES 會為允許自動軟體分發的應用程式新增允許規則。檔案雜湊被指定為規則觸發條件。 |
| **始終允許透過 Windows Installer 進行軟體分發** | KSWS 和 KES 中的軟體分發控制工作方式不同。在遷移過程中，KES 會為允許自動軟體分發的應用程式新增允許規則 (**允許的軟體分發應用程式和套件**)。檔案雜湊被指定為規則觸發條件。在帳戶屬性中**信任的更新程式**核取方塊被選取。 |
| **始終允許使用背景智慧傳輸服務透過 SCCM 進行軟體分發** | *（不遷移）* |
| **允許的軟體分發應用程式和資料套件** | KSWS 和 KES 中的軟體分發控制工作方式不同。在遷移過程中，KES 會為允許自動軟體分發的應用程式新增允許規則。檔案雜湊被指定為規則觸發條件。在帳戶屬性中**信任的更新程式**核取方塊被選取。 |
| **排程設定** | *（不遷移）*<br>如果在 KSWS 設定中為元件配置了排程，則在遷移時將啟用應用程式控制元件。如果在 KSWS 設定中沒有為元件配置排程，則在遷移時將停用應用程式控制。<br>無法為元件配置單獨排程。該元件在 Kaspersky Endpoint Security 運行時始終處於開啟狀態。 |

# 安裝 KES 而不是 KSWS

您可以通過以下方式安裝 Kaspersky Endpoint Security：

- 刪除 KSWS 後安裝 KES（建議）。
- 在 KSWS 之上安裝 KES。

## 刪除 Kaspersky Security for Windows Server

您可以使用*遠端解除安裝應用程式*工作遠端刪除應用程式或在伺服器上本機刪除應用程式 。刪除 KSWS 後，您可能需要重新啟動伺服器。如果您想在不重啟的情況下安裝 Kaspersky Endpoint Security，請確保 Kaspersky Security for Windows Server 已被完全刪除。如果應用程式未被完全刪除，安裝 Kaspersky Endpoint Security 可能會導致伺服器運行錯誤。如果您使用了 kavremover 實用程式，還建議確保應用程式已被完全刪除。kavremover 實用程式 不支援管理 KSWS。

如果啟用密碼防護來限制對 KSWS 的存取，請在 KES 安裝套件的設定中輸入解除安裝密碼。

刪除 KSWS 後，使用任何可用的方法安裝 Kaspersky Endpoint Security for Windows。

## 安裝 Kaspersky Endpoint Security

當您遠端安裝 KES 時，您在安裝套件屬性中選擇的元件會被安裝在伺服器上。我們建議在安裝套件屬性中選擇預設元件。在 KSWS 上安裝 KES 時不需要重新啟動。

在本機安裝前，Kaspersky Endpoint Security 會檢查電腦中是否存在卡巴斯基應用程式。如果電腦上安裝了 Kaspersky Security for Windows Server，KES 會偵測已安裝的 KSWS 元件集合並選擇相同的元件進行安裝。在 KSWS 上安裝 KES 時不需要重新啟動。

如果在 KSWS 之上安裝 KES 失敗，您可以還原安裝。還原安裝後，建議重啟伺服器再試。

安裝 Kaspersky Endpoint Security for Windows 時，KSWS 設定和工作不會被遷移。若要遷移設定和工作，請執行政策和工作批次轉換精靈。

您可以使用`status`指令或者在電腦內容的卡巴斯基安全管理中心主控台中，在應用程式介面的“**安全**”區域中檢查已安裝元件清單。您可以在安裝後使用*變更應用程式元件*變更元件集合。

# 將 [KSWS+KEA] 配置遷移到 [KES+內建代理] 配置

為了支援使用 Kaspersky Endpoint Security for Windows 作為 EDR (KATA)、EDR Optimum、EDR Expert、Kaspersky Sandbox、KUMA 和 MDR的一部分，內建代理已被新增到應用程式中。您再也無需分開 Kaspersky Endpoint Agent 應用程式來使用這些解決方案。

從 KSWS 遷移到 KES 時，EDR (KATA)、EDR Optimum、EDR Expert、Kaspersky Sandbox、KUMA 和 MDR 解決方案繼續與 Kaspersky Endpoint Security 內建代理協同工作。此外，Kaspersky Endpoint Agent 將被從電腦移除。

將 [KSWS+KEA] 配置遷移到 [KES+內建代理] 包含以下步驟：

### 1 從 KSWS 遷移到 KES

從 KSWS 遷移到 KES 涉及安裝 Kaspersky Endpoint Security 而不是 Kaspersky Security for Windows Server。

管理員通常啟用密碼防護以限制對 KSWS 和 KEA 的存取。從卡巴斯基安全管理中心 Linux 15.1 開始，您可以在*遠端安裝應用程式*工作設定中輸入應用程式解除安裝密碼。此工作只允許輸入一個解除安裝密碼。也就是說，如果為 KSWS 和 KEA 設定相同的密碼，則 KSWS 和 KEA 應用程式將被成功刪除。如果密碼不同，則刪除其中一個應用程式將失敗並出現存取錯誤。要完成遷移，您必須對無法在*遠端安裝應用程式*工作設定中輸入其密碼的應用程式停用密碼防護。

要執行遷移，您必須選擇支援 Detection and Response 解決方案所需的元件作為 Kaspersky Endpoint Security 的一部分。安裝應用程式後，Kaspersky Endpoint Security 將切換到使用內建代理並刪除 Kaspersky Endpoint Agent。

### 2 遷移政策和工作

將 [KSWS+KEA] 政策和工作遷移到 [KES+內建代理] 包含以下步驟：

1. 使用政策和工作批量轉換精靈將政策和工作從 KSWS 遷移到 KES（僅在管理主控台 (MMC) 上可用）。

   結果，名為*UpgradedFromKSWS<Kaspersky Security for Windows Server 政策名稱>*的政策設定檔被新增到 KES 政策中。名為*<KSWS 工作名稱>（已轉換）*的新 KES 工作也得到建立。

2. 使用用於從 Kaspersky Endpoint Agent 遷移的精靈將政策和工作從 KEA 遷移到 KES（僅在 Web 主控台和雲端主控台中可用）。

   結果會建立一個名為*<Kaspersky Endpoint Security 政策名稱>&<Kaspersky Endpoint Agent 政策名稱>*的新政策。新工作和 KES 工作也會建立。

### 3 產品授權功能

如果您使用 Kaspersky Endpoint Detection and Response Optimum 或 Kaspersky Optimum Security 產品授權來啟動 Kaspersky Endpoint Security for Windows 和 Kaspersky Endpoint Agent，EDR Optimum 功能將在升級應用程式到版本 11.7.0 後自動啟動。您不需要做任何其它事情。

如果使用獨立 Kaspersky Endpoint Detection and Response Optimum 附加元件產品授權啟動 EDR Optimum 功能，您必須確保 EDR Optimum 附加元件金鑰已新增到卡巴斯基安全管理中心存放庫且產品授權金鑰自動分發功能已啟用。升級應用程式到版本 11.7.0 後，EDR Optimum 功能將被自動啟動。

如果使用 Kaspersky Endpoint Detection and Response Optimum 或 Kaspersky Optimum Security 產品授權啟動 Kaspersky Endpoint Agent，使用其他產品授權啟動 Kaspersky Endpoint Security for Windows，您必須將 Kaspersky Endpoint Security for Windows 金鑰替換為普通的 Kaspersky Endpoint Detection and Response Optimum 金鑰或 Kaspersky Optimum Security 金鑰。您可以使用"*新增金鑰*"工作取代金鑰。

您不需要啟動 Kaspersky Sandbox 功能。升級和啟動 Kaspersky Endpoint Security for Windows 後，Kaspersky Sandbox 功能將立即可用。

只有 Kaspersky Anti Targeted Attack Platform 產品授權可用於啟動作為 Kaspersky Anti Targeted Attack Platform 解決方案一部分的 Kaspersky Endpoint Security 。升級應用程式到版本 12.1 後，EDR (KATA) 功能將被自動啟動。您不需要做任何其它事情。

4. **檢查 Kaspersky Endpoint Detection and Response Optimum 和 Kaspersky Sandbox 的健康**

   如果升級後電腦在卡巴斯基安全管理中心中具有"*緊急*"狀態：

   - 請確保電腦安裝了網路代理 13.2或更高版本。
   - 透過檢視"*應用程式元件狀態報告*"來檢查內建代理的運行狀態。如果元件的狀態為"*未安裝*"，請使用*變更應用程式元件*工作來安裝元件。
   - 請確保在 Kaspersky Endpoint Security for Windows 的新政策中接受卡巴斯基安全網路聲明。

   確保使用*應用程式元件狀態報告*啟動 EDR Optimum 功能 。如果元件的狀態為"*產品授權不支援*"，請確保EDR Optimum 的產品授權金鑰自動分發功能已開啟。

# 確保已成功刪除 Kaspersky Security for Windows Server

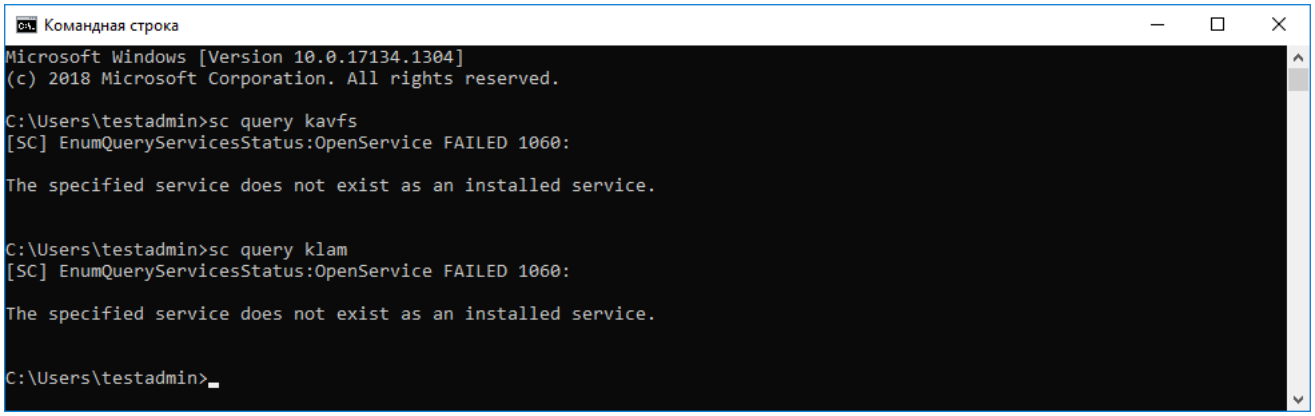
確保 Kaspersky Security for Windows Server 被完全刪除：

- `%ProgramFiles%\Kaspersky Lab\Kaspersky Security for Windows Server\` 資料夾不存在。
- 以下服務不存在：
  - Kaspersky Security Service （ KAVFS ）
  - Kaspersky Security Management 服務（ KAVFSGT ）
  - Kaspersky Security Exploit Prevention 服務（ KAVFSSLP ）
  - Kaspersky Security Script Checker 服務（ KAVFSSCS ）

  您可以在工作管理器中或透過發出 `sc query` 命令檢查正在執行的服務（見下圖）。
- 以下驅動程式不存在：
  - klam.sys
  - klflt.sys
  - klramdisk.sys
  - klelaml.sys
  - klfltdev.sys

- klips.sys
- klids.sys
- klwtpee

您可以在 `C:\Windows\System32\drivers` 資料夾中或透過發出 `sc query` 命令檢查已安裝的驅動程式。如果缺少服務或驅動程式，您將收到以下響應：




確保已成功刪除 Kaspersky Security for Windows Server 服務和驅動程式

如果應用程式或驅動程式檔案仍然在伺服器上，請手動刪除相關檔案。如果 Kaspersky Security for Windows Server 服務仍在伺服器上執行，請手動停止（`sc stop`）和刪除（`sc delete`）服務。要停止 klam.sys 驅動程式，請使用 `fltmc unload klam` 命令。

# 使用 KSWS 金鑰啟動 KES

安裝應用程式後，您可以使用 Kaspersky Security for Windows Server (KSWS) 產品授權金鑰啟動 Kaspersky Endpoint Security for Windows (KES)。遷移後的啟動過程取決於 KSWS 啟動方法（見下表）。

Kaspersky Endpoint Security 不支援 *Kaspersky Security for Storage 產品授權*。要使用此產品授權，您需要使用 Kaspersky Security for Windows Server。

要使用 KSWS 金鑰啟動 KES，您只能使用啟動碼。如果使用金鑰檔案啟動應用程式，您需要聯絡技術支援服務獲取 Kaspersky Endpoint Security 金鑰檔案。

使用 Kaspersky Security for Windows Server 金鑰啟動 Kaspersky Endpoint Security for Windows

| Kaspersky Security for Windows Server 啟動方法 | 將金鑰遷移到 Kaspersky Endpoint Security for Windows。 |
|---|---|
| 將 KSWS 產品授權金鑰自動分發到電腦。 | 如果在 KSWS 產品授權金鑰內容中啟用了自動金鑰分發，則會使用 KSWS 金鑰自動啟動 KES。 |
| KSWS 金鑰由工作新增。 | 如果您的 KSWS 是使用工作啟動的，則 KSWS 產品授權金鑰會在從 KSWS 遷移期間被刪除。您必須再次啟動應用程式。例如，您可以向 Kaspersky Endpoint Security for Windows 安裝套件新增產品授權金鑰。 |
| KSWS 金鑰在應用程式介面本機新增。 | 如果您的 KSWS 是使用應用程式啟動精靈在本機啟動的，則 KSWS 產品授權金鑰會在從 KSWS 遷移期間被刪除。您必須再次啟動應用程式。例如，您可以向 Kaspersky Endpoint Security for Windows 安裝套件新增產品授權金鑰。 |
| KSWS 金鑰被新增至安裝套件。 | 如果您的 KSWS 是使用安裝套件的金鑰啟動的，則 KSWS 產品授權金鑰會在從 KSWS 遷移期間被刪除 。您必須再次啟動應用程式。例如，您可以向 Kaspersky Endpoint Security for Windows 安裝套件新增產品授權金鑰。 |

| Kaspersky Security for Windows Server 啟動方法 | 將金鑰遷移到 Kaspersky Endpoint Security for Windows。 |
| --- | --- |
| Amazon Web Services (AWS) 中的付費虛擬機映像 (Amazon Machine Image – AMI)。 | 如果您購買了卡巴斯基安全管理中心作為 Amazon Web Services (AWS) 中的付費虛擬機映像（Amazon Machine Image – AMI），則不需要啟動 KES。在這種情況下，卡巴斯基安全管理中心使用已新增到應用程式的 AWS 訂購。 |
| 帶有您自己的產品授權的現成免費卡巴斯基安全管理中心映像（自帶產品授權 - BYOL 模型）。 | 如果您在雲環境中使用帶有您自己的產品授權的開箱即用的免費卡巴斯基安全管理中心映像（自帶產品授權 – BYOL 模型），您必須使用任何可用方法啟動該應用程式。您將需要 Kaspersky Hybrid Cloud Security 產品授權。 |

# 遷移高負載伺服器的特殊注意事項

在高負載伺服器上，監控效能和避免錯誤很重要。遷移到 Kaspersky Endpoint Security for Windows 後，我們建議暫時停用相對於其他元件使用大量伺服器資源的應用程式元件。確保伺服器正常執行後，您可以重新開啟應用程式元件。

我們建議按如下方式遷移高負載伺服器：

1. 使用預設設定建立 Kaspersky Endpoint Security 政策。

   預設設定被認為最佳。此設定由 Kaspersky 專家建議。預設設定提供建議的防護等級和最佳資源使用。

2. 在政策設定中，關閉以下元件：網路威脅防護，行為偵測，弱點利用防禦，修復引擎，應用程式控制。

   如果您的組織部署了 Kaspersky Managed Detection and Response (MDR) 解決方案，將 BLOB 組態檔上傳到 Kaspersky Endpoint Security 政策。

3. 從伺服器中刪除 Kaspersky Security for Windows Server。

4. 使用預設元件集合安裝 Kaspersky Endpoint Security for Windows。

   如果您的組織部署了 Detection and Response 解決方案，請在安裝套件的屬性中選擇相關元件。

5. 檢查應用程式的設定：

   - 該應用程式使用 KSWS 產品授權金鑰啟動。
   - 新政策已套用。先前選擇的元件被停用。

6. 確保伺服器正常工作。確保 Kaspersky Endpoint Security for Windows 使用的伺服器資源不超過 1%。

7. 如有需要，建立掃描排除項目，新增受信任應用程式，建立受信任網址清單。

8. 開啟行為偵測、弱點利用防禦、修復引擎元件。確保 Kaspersky Endpoint Security for Windows 使用的伺服器資源不超過 1%。

9. 開啟網路威脅防護元件。確保 Kaspersky Endpoint Security for Windows 使用的伺服器資源不超過 2%。

10. 在規則測試模式中開啟應用程式控制元件。

11. 確保應用程式控制正常工作。如有需要，新增新的應用程式控制規則，在確認應用程式控制正常工作後關閉規則測試模式。

從 KSWS 遷移到 KES 後，確保應用程式運行正常。在主控台查看伺服器狀態（應該是*確定*）。確保應用程式沒有報告任何錯誤，還要檢查最後一次連線到管理伺服器的時間、最後一次更新資料庫的時間和伺服器防護狀態。

# 在 Server Core 模式下管理伺服器上的應用程式

"Server Core 模式"中的伺服器沒有 GUI。因此，您只能遠端使用卡巴斯基安全管理中心主控台或者本機使用命令列來管理應用程式。

## 使用卡巴斯基安全管理中心主控台管理應用程式

使用卡巴斯基安全管理中心主控台安裝應用程式與用正常方式安裝它沒有區別。建立安裝套件時，您可以新增產品授權金鑰以啟動應用程式。您可以使用 Kaspersky Endpoint Security for Windows 金鑰或者 Kaspersky Security for Windows Server 金鑰

> 在 Server Core 模式中的伺服器上，以下應用程式元件不可使用：Web 威脅防護、郵件威脅防護、Web 控制、BadUSB 攻擊防護、檔案級加密 (FLE)、卡巴斯基磁碟加密 (FDE)。

安裝 Kaspersky Endpoint Security 時，不需要重新啟動。僅當在安裝前必須移除不相容的應用程式時，才需要重新啟動。更新應用程式版本時也可能需要重新啟動。應用程式無法顯示視窗提示使用者重新啟動伺服器。您可以從卡巴斯基安全管理中心主控台中的報告瞭解是否需要重新啟動伺服器。

管理 Server Core 模式中伺服器上的應用程式與管理電腦沒有差別。您可以使用政策和工作來設定應用程式。

在 Server Core 模式下管理伺服器上的應用程式涉及以下特別考慮：

- Server Core 模式中的伺服器沒有 GUI，因此 Kaspersky Endpoint Security 不顯示警告告訴使用者需要進階解毒。若要解毒威脅，您需要在應用程式設定中啟用進階解毒技術，在"*惡意軟體掃描*"工作設定中啟用立即執行進階解毒。然後您需要啟動"*惡意軟體掃描*"工作。
- BitLocker 磁碟機加密僅適用於受信任平台模組 (TPM)。PIN/密碼不能用於加密，因為應用程式無法顯示預開機身分驗證的密碼提示視窗。如果作業系統啟用了聯邦資訊處理標準 (FIPS) 相容模式，請在開始加密磁碟機之前連線用來儲存加密金鑰的卸除式磁碟機。

## 從命令列管理應用程式

如果不能使用 GUI，您可以從命令列管理 Kaspersky Endpoint Security。

若要在 Server Core 模式下將應用程式安裝到伺服器，請執行以下指令：

```
setup_kes.exe /pEULA=1 /pPRIVACYPOLICY=1 /s
```

若要啟動應用程式，執行以下指令：

```
avp.com license /add <activation code or key file>
```

若要檢查應用程式設定檔狀態，執行以下指令：

```
avp.com status
```

若要檢視應用程式管理指令清單，執行以下指令：

```
avp.com help
```

# 將 [KSWS+KEA] 遷移到 [KES+內建代理]

從 Kaspersky Security for Windows Server (KSWS) 遷移到 Kaspersky Endpoint Security (KES) 時，您可以使用以下建議來配置伺服器防護和最佳化效能。在這裡，我們將查看一個單個組織的遷移範例。

## 組織的基礎結構

公司安裝了以下設備：

- 卡巴斯基安全管理中心 14.2

  管理員使用管理主控台 (MMC) 管理卡巴斯基解決方案。Kaspersky Endpoint Detection and Response Optimum (EDR Optimum) 也得到部署

  在卡巴斯基安全管理中心中，建立了三個管理群組，包含組織的伺服器：兩個用於 SQL 伺服器的管理群組和一個用於 Microsoft Exchange 伺服器的管理群組。每個管理群組都由自己的政策管理。*資料庫更新*和*隨需掃描*工作為組織中的所有伺服器建立。

  KSWS 啟動金鑰已新增到卡巴斯基安全管理中心。自動金鑰分發被啟用。

- 安裝了 Kaspersky Security for Windows Server 11.0.1 和 Kaspersky Endpoint Agent 3.11 的 SQL 伺服器。SQL 伺服器被合併成兩個叢集。

  KSWS 由 *SQL_Policy(1)* 和 *SQL_Policy(2)* 政策管理。*資料庫更新*和*按需掃描*工作也被建立。

- 安裝了 Kaspersky Security for Windows Server 11.0.1 和 Kaspersky Endpoint Agent 3.11 的 Microsoft Exchange 伺服器。

  KSWS 由 *Exchange_Policy* 政策管理。*資料庫更新*和*按需掃描*工作也被建立。

## 規劃遷移

遷移涉及以下步驟：

1. 使用政策和工作批量轉換精靈遷移 KSWS 工作和政策。
2. 使用政策和工作批量轉換精靈遷移 Kaspersky Endpoint Agent 政策。
3. 使用標籤啟動新政策屬性中的政策設定檔。
4. 安裝 KES 而不是 KSWS。
5. 啟動 EDR Optimum。
6. 確認 KES 正在執行。

遷移方案最初在 SQL 伺服器叢集之一上執行。然後遷移方案在 SQL 伺服器的另一個叢集上執行。然後遷移方案在 Microsoft Exchange 上執行。

## 使用政策和工作批量轉換精靈遷移 KSWS 工作和政策

要遷移 KSWS 工作，您可以使用政策和工作批量轉換精靈（遷移精靈）。結果，您將獲得一個政策，其中包含分別用於 SQL 和 Microsoft Exchange 伺服器的三個設定檔，而不是 *SQL_Policy(1)*、*SQL_Policy(2)* 和 *Exchange_Policy* 政策。具有 KSWS 設定的新政策設定檔將被命名為 *UpgradedFromKSWS <Kaspersky Security for Windows Server 政策名稱>*。在設定檔屬性中，遷移精靈會自動選擇 `UpgradedFromKSWS` 裝置標籤作為觸發標準。因此，政策設定檔的設定會被自動套用到伺服器。

## 使用政策和工作批量轉換精靈遷移 Kaspersky Endpoint Agent 政策

要遷移 Kaspersky Endpoint Agent 政策，您可以使用政策和工作批量轉換精靈。Kaspersky Endpoint Agent 的政策和工作遷移精靈僅在 Web 主控台中可用。

## 使用標籤啟動新政策屬性中的政策設定檔

選擇您之前分配的裝置標籤作為設定檔啟動條件。開啟政策屬性並選擇*政策設定檔啟動一般規則*作為設定檔啟動條件。

## 安裝 KES 而不是 KSWS

在安裝 KES 之前，您必須在 KSWS 政策屬性中停用密碼防護。

安裝 KES 涉及以下步驟：

1. 準備安裝套件。在安裝套件屬性中，選擇 Kaspersky Endpoint Security for Windows 12.0 分發套件並選擇預設元件集合。
2. 為其中一個 SQL 伺服器管理群組建立一個*遠端安裝應用程式*工作。
3. 在工作屬性中，選擇安裝套件和產品授權金鑰檔案。
4. 等待工作成功完成。
5. 為剩餘的管理群組重複 KES 安裝。

KES 安裝完成後，卡巴斯基安全管理中心自動新增 `UpgradedFromKSWS` 標記到主控台上的電腦名稱。

要檢查 KES 安裝，您可以使用*防護佈署報告*。您還可以檢查裝置狀態。要確認應用程式啟動，您可以使用*產品授權金鑰使用報告*。

## 啟動 EDR Optimum

您可以使用獨立的 Kaspersky Endpoint Detection and Response Optimum 附加產品授權啟動 EDR Optimum 功能。您必須確認 EDR Optimum 金鑰已新增到卡巴斯基安全管理中心儲存庫並且啟用了產品授權金鑰自動分發功能。

要檢查 EDR Optimum 啟動，您可以使用 *應用程式元件狀態報告*。

## 確認 KES 正在工作

要確認 KES 是否在工作，您可以查看沒有報錯。裝置狀態必須是*確定*。更新和惡意軟體掃描工作成功完成。

# 用來防護虛擬機的 Light Agent 模式

從版本 12.8 開始，您可以將 Kaspersky Endpoint Security for Windows 作為 Kaspersky Security for Virtualization Light Agent 的一部分使用。*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，您必須在 Light Agent 模式下安裝應用程式。

從版本 6.2 開始，您可以在 Light Agent 模式下使用 Kaspersky Endpoint Security 作為 Kaspersky Security for Virtualization Light Agent 的一部分。

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 可將需要掃描的檔案片段傳送到 SVM。掃描結果適用於所有安裝了 Light Agent 的虛擬機（SharedCash技術）。因此，SharedCash技術提高了解決效率並能更快地應對威脅。

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 元件用於解決方案元件和虛擬基礎架構之間的互動。*Integration Server* - Kaspersky Security for Virtualization Light Agent 解決方案的一個元件，可產生可用 SVM 清單並將該資料傳輸到 Light Agent、參與 Light Agent 對 SVM 的偵測、保護 Light Agent 和 SVM 之間的連線和執行其他功能。

# Light Agent 模式的特殊注意事項

您可以使用 Kaspersky Endpoint Security 政策和工作在標準模式和 Light Agent 模式下管理 Kaspersky Endpoint Security。在 Light Agent 模式下，應用程式的某些元件和功能不可用。

## 更新資料庫和程式模組

作為 Kaspersky Security for Virtualization Light Agent 解決方案的一部分工作時，Light Agent 模式下的 Kaspersky Endpoint Security 使用應用程式所需的特殊惡意軟體資料庫。Kaspersky Endpoint Security 從 Protection Server 獲取資料庫和應用程式模組更新。

受防護虛擬機上的資料庫和模組使用特殊的 *資料庫和應用程式模組更新* 工作進行更新，其中 SVM 上的一個資料夾被指定為更新來源。Light Agent 可自動執行 *資料庫和應用程式模組更新* 工作。您無法選擇不同的更新來源、設定工作排程或刪除工作。

最新惡意軟體資料庫更新的回溯也在 Protection Server 端處理。在 SVM 上回溯資料庫和應用程式模組更新後，一個特殊的本機 *資料庫和應用程式模組更新* 工作在受防護的虛擬機上啟動。此工作將使 Light Agent 返回使用之前的惡意軟體資料庫集合。

Light Agent 模式下的 Kaspersky Endpoint Security 不支援 *更新回溯* 工作。

### 啟動 Light Agent

若要啟動應用程式，您必須將產品授權金鑰新增至 Light Agent 連線的 SVM。您需要單獨 啟動應用程式。

### Light Agent 模式的其他特殊注意事項

- 當 為應用程式建立政策時，我們建議選擇 Light Agent 模式。在此模式下，新政策精靈會提示您設定 SVM 連線。應用程式需要這些設定才能在 Light Agent 模式下運作。
- 您無法在 Light Agent 模式下安裝資料加密元件和適應性異常控制。元件集合也取決於來賓作業系統的類型：工作站或伺服器。
- Light Agent 不支援與 Kaspersky Endpoint Detection and Response Expert (cloud) 整合。
- 您可以在管理主控台 (MMC) 和卡巴斯基安全管理中心網頁主控台中管理 Light Agent。無法在卡巴斯基安全管理中心雲端主控台中管理 Light Agent。
- 不支援變更 VDI 虛擬機上的應用程式元件集合。
- Kaspersky Endpoint Security 透過 KSN 代理伺服器與 KSN 伺服器進行通訊。不支援與 KSN 直接通訊。
- 不支援卡巴斯基安全網路的雲端模式。
- 不支援在連線到 Integration Server (VIIS)、Protection Server (SVM) 和 KSN 伺服器時使用應用程式代理伺服器。

# 虛擬機的初步配置

您可以在使用虛擬平台技術的虛擬機上安裝 Kaspersky Endpoint Security。Kaspersky Endpoint Security 支援 VMware、Microsoft Hyper-V、Citrix 虛擬平台。在安裝之前，您必須對虛擬機進行初步配置。

# 與 Citrix App Layering 技術的相容性

如果您打算使用 Full User Layer 以儲存臨時虛擬機的狀態，在安裝虛擬機範本之前您必須執行以下操作：

1. 建立 C:\Program Files\Unidesk\Uniservice\UserExclusions\KESLA.txt 檔案並向其新增以下排除項目：
   - `C:\ProgramData\KasperskyLab\`
   - `C:\ProgramData\Kaspersky Lab\`
   - `C:\Program Files (x86)\Kaspersky Lab\`
2. 在作業系統的登錄檔中，在 HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Unifltr 登錄機碼中，建立一個名為 MiniFilterBypass 的新 DWORD 值並將其設為 1。

3. 在作業系統的登錄檔中，在 HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Unirsd 登錄機碼中，建立一個名為 ExcludeKey 的新 MULTI_SZ 值並將其設為 \Registry\Machine\SOFTWARE\WOW6432Node\KasperskyLab。

4. 重新啟動虛擬機。

若要在使用 Citrix App Layering 的基礎結構中的虛擬機上安裝，您必須執行下列操作：

1. 在應用程式層的虛擬機範本上安裝卡巴斯基安全管理中心管理代理程式和 Kaspersky Endpoint Security for Windows。

2. 建立由多層組成的虛擬機映像。

3. 在支援 Citrix App Layering 解決方案的 Hypervisor 上部署建立的映像。

4. 從建立的映像配置臨時虛擬機的建立。

有關與 Citrix App Layering 一起安裝防毒軟體的詳細資訊，請參閱 Citrix App Layering 文件。

# 與 Citrix Provisioning (Citrix Provisioning Services) 技術的相容性

若要確保應用程式與 Citrix Provisioning 技術 (Citrix Provisioning Services) 相容，請執行下列操作：

- 如果虛擬機上安裝了 Citrix Provisioning Target Device 軟體，您必須在安裝 Kaspersky Endpoint Security 應用程式之前將其移除。安裝應用程式後，必須安裝 Citrix Provisioning Target Device。

- 使用設定精靈或者遠端使用卡巴斯基安全管理中心安裝應用程式時，您必須選擇 **確保與 Citrix PVS 相容** 核取方塊。

# 與 Omnissa App Volumes 技術的相容性

在虛擬機範本上安裝之前，您必須建立 %SVAgent%\Config\Custom\snapvol.cfg 檔案並向其新增以下排除項目：

- `exclude_path=\ProgramData\Kaspersky Lab`
- `exclude_path=\ProgramData\KasperskyLab`
- `exclude_path=\Program Files\Kaspersky Lab`
- `exclude_path=\Program Files\Common Files\Kaspersky Lab`
- `exclude_path=\Program Files\Kaspersky Lab`
- `exclude_path=\Program Files (x86)\Kaspersky Lab`
- `exclude_path=\Program Files (x86)\Common Files\Kaspersky Lab`
- `exclude_process_path=\Program Files (x86)\Kaspersky Lab`

- exclude_process_path=\Program Files (x86)\Common Files\Kaspersky Lab
- exclude_process_path=\Program Files\Common Files\Kaspersky Lab
- exclude_process_path=\Program Files\Kaspersky Lab
- exclude_process_name=avp.exe
- exclude_process_name=klnagent.exe
- exclude_registry=\REGISTRY\MACHINE\SOFTWARE\Wow6432Node\KasperskyLab
- exclude_registry=\REGISTRY\MACHINE\SOFTWARE\KasperskyLab
- exclude_registry=\REGISTRY\MACHINE\SYSTEM\CurrentControlSet\Services\klupd_klif_arkmon
- exclude_registry=\REGISTRY\MACHINE\SYSTEM\CurrentControlSet\Services\klupd_klif_klark
- exclude_registry=\REGISTRY\MACHINE\SYSTEM\CurrentControlSet\Services\klupd_klif_klbg
- exclude_registry=\REGISTRY\MACHINE\SYSTEM\CurrentControlSet\Services\klupd_klif_mark
- exclude_registry=\REGISTRY\MACHINE\SYSTEM\CurrentControlSet\Services\klupd_klif_swmon

如欲瞭解詳細資訊，請參閱 Omnissa 文件。

# 安裝 Light Agent

在 Light Agent 模式下安裝應用程式與在標準模式下安裝相同。在虛擬機上安裝 Light Agent 之前，您必須確保已安裝卡巴斯基安全管理中心網路代理。*網路代理*可促進管理伺服器與虛擬機之間的互動。

Light Agent 可以通過以下方式之一安裝在虛擬機上：

- 遠端使用卡巴斯基安全管理中心。
- 本機使用安裝精靈。
- 本機使用命令列。

要安裝 Light Agent，您必須在安裝套件設定或在安裝精靈中選擇適當的配置。

在伺服器上安裝 Light Agent 時，進階防護元件（行為偵測、弱點利用防禦、修復引擎）會從應用程式的預設設定中排除。應用程式的預設設定可提供建議的防護等級並最佳化伺服器資源的使用。在工作站上安裝 Light Agent 時，進階防護元件會包含在應用程式的預設設定中。

安裝 Light Agent 時，我們建議為相關虛擬環境選擇預先定義的排除項目和受信任的應用程式。預定義掃描排除項目和受信任的應用程式可協助您快速設定應用程式並避免虛擬環境相容性問題。您還可以安裝後在政策中 配置預定義的掃描排除項目和受信任的應用程式。

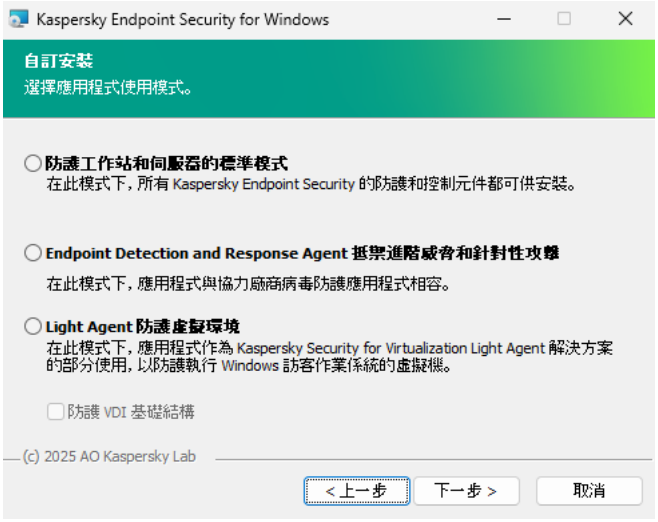
在持久虛擬機上安裝 Light Agent 時，您可能需要更改 Sensor ID產生演算法。Sensor ID 在 Kaspersky Anti Targeted Attack Platform 解決方案中用於識別向伺服器傳送遙測資料的電腦。若要建立唯一的Sensor ID，請在命令列上安裝應用程式時設定 `EnableUniqueSensorID=1`。

**如何使用安裝精靈安裝 Light Agent**

1. 複製"分發套件"資料夾到虛擬機。
2. 執行 setup_kes.exe。

   啟動"安裝精靈"。

## Kaspersky Endpoint Security 的配置



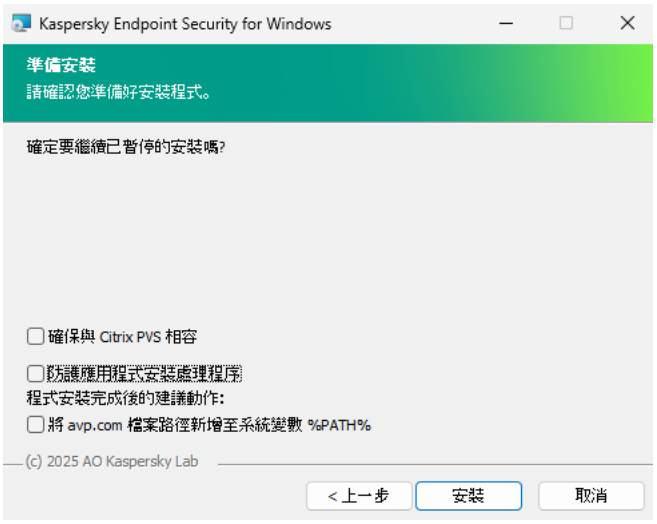

選擇應用程式的配置

選擇 **Light Agent 防護虛擬環境** 配置。此配置適用於用作 Kaspersky Security for Virtualization Light Agent 解決方案一部分的應用程式。Light Agent 必須安裝在需要使用此解決方案防護的每台虛擬機上。在此配置中，您無法使用資料加密元件或自適應異常控制。如果您要在將用於建立的虛擬機範本上安裝 Light Agent *非持久虛擬機*，選擇 **防護 VDI 基礎結構** 核取方塊（VDI 代表 Virtual Desktop Infrastructure）。VDI 防護模式有助於最佳化 Kaspersky Endpoint Security 在非持久虛擬機上的效能。在此模式下，Light Agent 會拒絕需要重新啟動虛擬機的應用程式更新。當收到需要重新啟動的應用程式更新時，Light Agent 會產生一個有關需要更新受防護虛擬機範本的事件。

Kaspersky Endpoint Security 元件

選擇您要安裝的元件（見下圖）。安裝應用程式後，您可以變更可用的應用程式元件。為此，您需要再次執行安裝精靈，然後選擇變更可用元件。

進階設定




*進階應用程式安裝設定*

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

**確保與 Citrix PVS 相容**您可以啟用Citrix Provisioning Services支援以將 Kaspersky Endpoint Security 安裝到虛擬機。

**將 avp.com 檔案路徑新增至系統變數 %PATH%**您可以將安裝路徑新增到%PATH%變數中，以方便使用命令列介面。

**如何使用命令列安裝 Light Agent**

1. 以管理員身分執行命令列解譯器 (cmd.exe)。
2. 轉到 Kaspersky Endpoint Security 分發套件所在資料夾。
3. 執行以下指令：

   ```
   setup_kes.exe /pEULA=1 /pPRIVACYPOLICY=1 /pKSN=1 /pLIGHTAGENTMODE=1 [/pVDI=1] [/s]
   ```

   或

   ```
   msiexec /i <distribution kit name> EULA=1 PRIVACYPOLICY=1 KSN=1 LIGHTAGENTMODE=1
   [VDI=1] [/qn]
   ```

   VDI 選項啟用 VDI (Virtual Desktop Infrastructure）防護模式。VDI 防護模式有助於最佳化 Kaspersky Endpoint Security 在非持久虛擬機上的效能。在此模式下，Light Agent 會拒絕需要重新啟動虛擬機的應用程式更新。當收到需要重新啟動的應用程式更新時，Light Agent 會產生一個有關需要更新受防護虛擬機範本的事件。預設停用 VDI 防護模式。

結果，Light Agent 將使用預設元件集合安裝在虛擬機上。您可以編輯元件集合並使用 setup.ini 檔案指定進階設定。您還可以在 命令列上指定安裝設定。

**如何使用管理主控台 (MMC) 安裝 Light Agent**

1. 開啟卡巴斯基安全管理中心管理主控台。
2. 在主控台樹狀目錄中，選擇**進階 → 遠端安裝 → 安裝套件**資料夾。

   這將開啟已下載到卡巴斯基安全管理中心的安裝套件清單。
3. 開啟 Kaspersky Endpoint Security for Windows 安裝套件的屬性。

   如果有需要的話，建立新的安裝套件。
4. 轉到**"設定"**區域。
5. 選擇 **Light Agent 防護虛擬環境** 配置。此配置適用於用作 Kaspersky Security for Virtualization Light Agent 解決方案一部分的應用程式。Light Agent 必須安裝在需要使用此解決方案防護的每台虛擬機上。在此配置中，您無法使用資料加密元件或自適應異常控制。如果您要在將用於建立的虛擬機範本上安裝 Light Agent *非持久虛擬機*，選擇 **防護 VDI 基礎結構** 核取方塊（VDI 代表 Virtual Desktop Infrastructure）。VDI 防護模式有助於最佳化 Kaspersky Endpoint Security 在非持久虛擬機上的效能。在此模式下，Light Agent 會拒絕需要重新啟動虛擬機的應用程式更新。當收到需要重新啟動的應用程式更新時，Light Agent 會產生一個有關需要更新受防護虛擬機範本的事件。
6. 選擇您要安裝的元件。

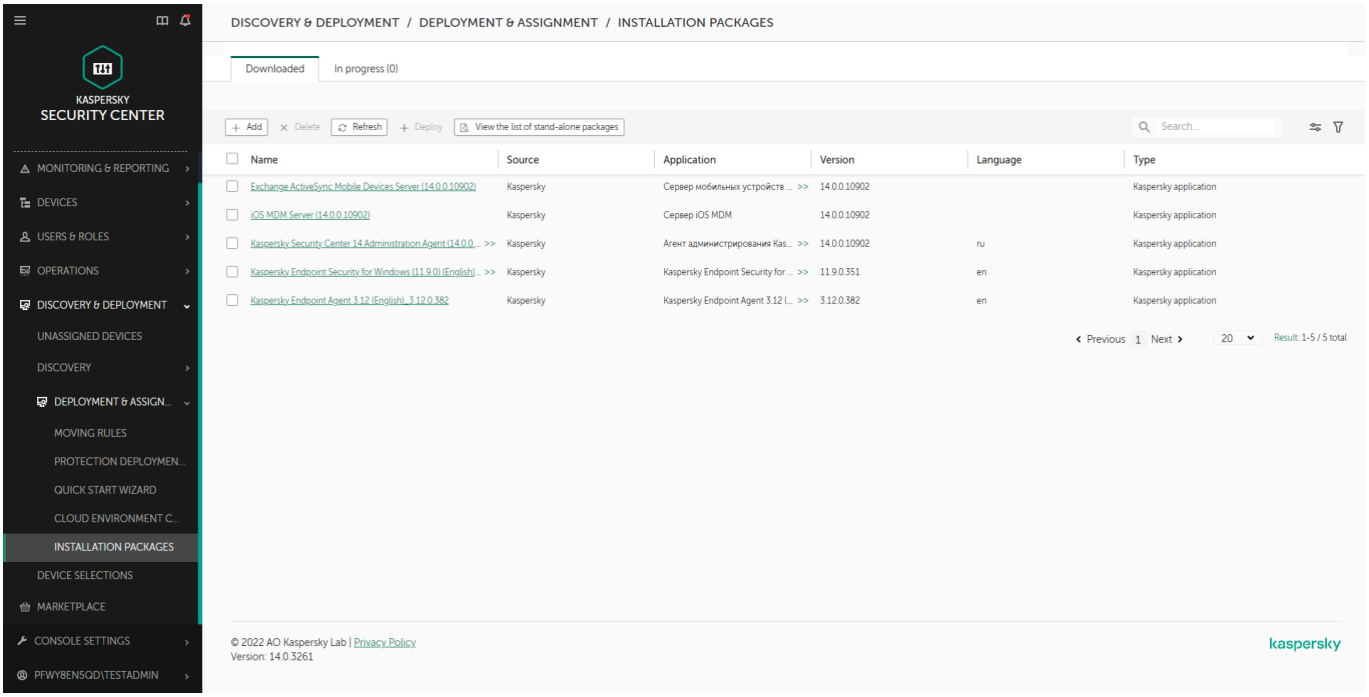
   安裝應用程式後，您可以變更可用的應用程式元件。
7. 配置受信任區域。為要在其中安裝應用程式的虛擬環境選擇預定義掃描排除項目和受信任的應用程式。

   預定義掃描排除項目和受信任的應用程式可協助您快速設定應用程式並避免虛擬環境相容性問題。
8. 儲存變更。
9. 建立遠端安裝工作。在工作屬性中，選擇您創建的安裝包。

**如何使用網頁主控台安裝 Light Agent**

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

這將開啟已下載到卡巴斯基安全管理中心的安裝套件清單。



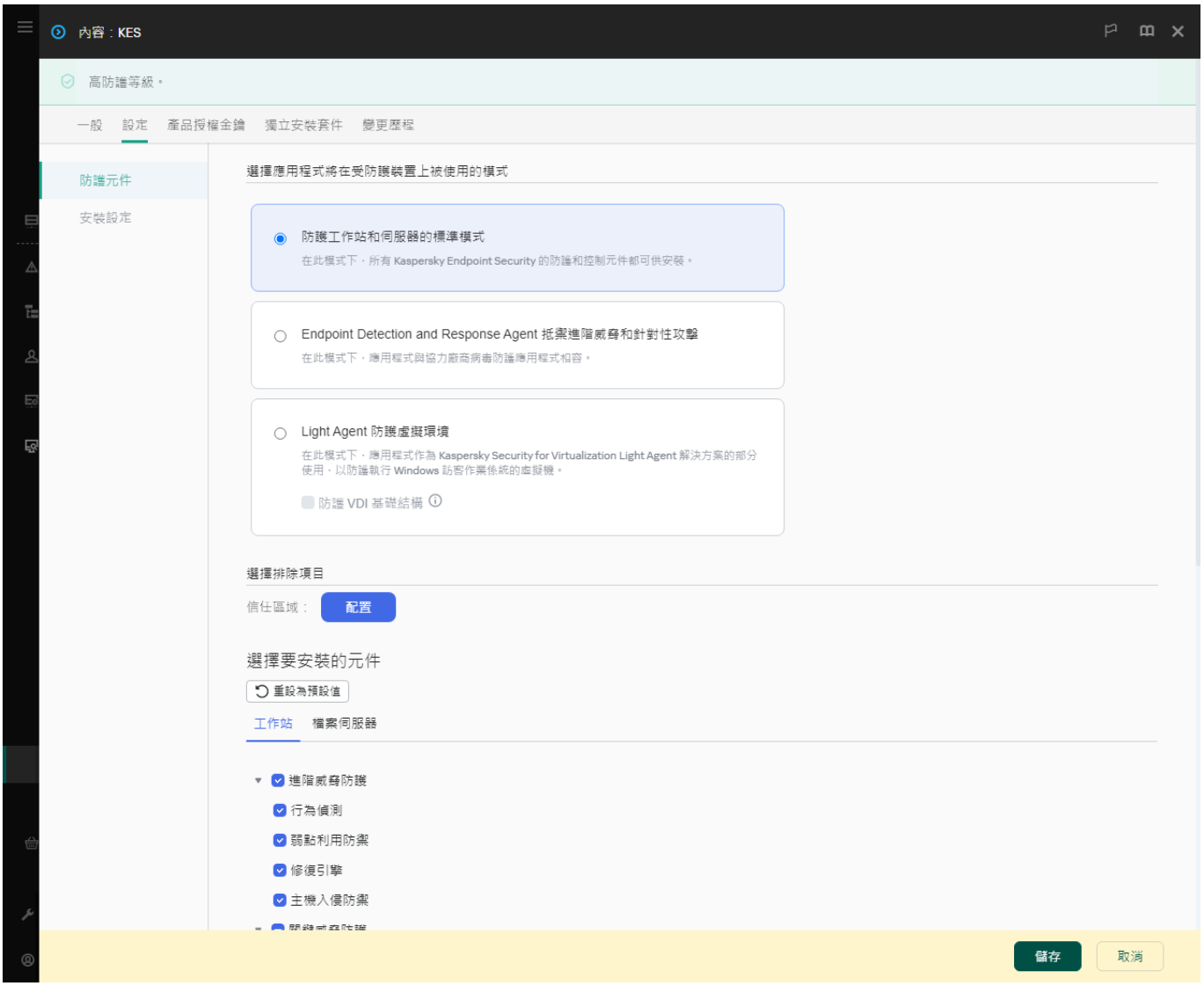

安裝套件清單

2. 開啟 Kaspersky Endpoint Security for Windows 安裝套件的屬性。

   如果有需要的話，建立新的安裝套件。

3. 選取“**設定**”標籤。

4. 轉到“**防護元件**”區域。




安裝套件中包含的元件

5. 選擇 **Light Agent 防護虛擬環境** 配置。此配置適用於用作 Kaspersky Security for Virtualization Light Agent 解決方案一部分的應用程式。Light Agent 必須安裝在需要使用此解決方案防護的每台虛擬機上。在此配置中，您無法使用資料加密元件或自適應異常控制。如果您要在將用於建立的虛擬機範本上安裝 Light Agent *非持久虛擬機*，選擇 **防護 VDI 基礎結構** 核取方塊（VDI 代表 Virtual Desktop Infrastructure）。VDI 防護模式有助於最佳化 Kaspersky Endpoint Security 在非持久虛擬機上的效能。在此模式下，Light Agent 會拒絕需要重新啟動虛擬機的應用程式更新。當收到需要重新啟動的應用程式更新時，Light Agent 會產生一個有關需要更新受防護虛擬機範本的事件。

6. 選擇您要安裝的元件。

   安裝應用程式後，您可以變更可用的應用程式元件。

7. 配置受信任區域。為要在其中安裝應用程式的虛擬環境選擇預定義掃描排除項目和受信任的應用程式。

   預定義掃描排除項目和受信任的應用程式可協助您快速設定應用程式並避免虛擬環境相容性問題。

8. 儲存變更。

9. 建立遠端安裝工作。在工作屬性中，選擇您創建的安裝包。

結果，Light Agent 安裝在虛擬機上。您可以使用應用程式的介面，通知區域中會顯示應用程式的圖示 。現在，您需要配置 Light Agent 與 SVM 的連線。




Light Agent 的主視窗

# 將 Light Agent 連線到 SVM

Kaspersky Security for Virtualization Light Agent 解決方案需要 Light Agent 和 SVM 持續通訊。這對於掃描 Light Agent 傳送的檔案中是否存在病毒和其他惡意軟體必不可少。如果沒有 SVM 連線，Light Agent 將無法傳送檔案進行掃描，如果超過五分鐘無法建立連線，掃描將結束並出現錯誤。

將 Light Agent 連線到 SVM 涉及以下步驟：

1. Light Agent 取得可用 SVM 的清單。
2. Light Agent 根據 VM 選取演算法 確定最適合連線的可用 Protection Server (SVM)。
3. Light Agent 可檢查其他 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。

您可以在 Kaspersky Endpoint Security 中或使用應用程式指令取得 Light Agent 與 SVM 連線狀態的資訊： 。每當 Light Agent 的 SVM 連線遺失或建立，應用程式都會產生事件，並將這些事件傳送到卡巴斯基安全管理中心。如果您使用 Integration Server 進行 SVM 發現，則可以在 Integration Server 主控台中取得有關 SVM 狀態和已連線 Light Agent 數量的資訊。有關 VM 態監控的詳細資訊，請參見 Kaspersky Security for Virtualization Light Agent 說明。

# SVM 發現

您可以為 Light Agent 選擇一種 SVM 發現方法：

- 使用 Integration Server (VIIS)。

  *Integration Server* 是可啟用 Kaspersky Security for Virtualization Light Agent 與虛擬基礎結構互動的解決方案元件。Integration Server 可維護可連線的 SVM 清單。Light Agent 與 Integration Server 建立連線並取得 SVM 位址清單。

  Integration Server 在大規模虛擬基礎結構中非常有用，因為 Integration Server 會自動平衡 SVM 之間的負載。Integration Server 獲取有關可用 SVM 的資訊，對其進行分析並向 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 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。

**如何在管理主控台 (MMC) 中透過 Light Agent 配置 SVM 發現**

1. 在卡巴斯基安全管理中心管理主控台樹狀目錄中，選取**政策**。
2. 選擇必要的政策並點擊以開啟政策內容。
3. 在政策視窗中，選擇"**Light Agent 模式 → SVM 發現設定**"。
4. 選擇 SVM 發現方法。

   - **使用 Integration Server**輸入 Integration Server 連線設定。輸入安裝了 Integration Server 的裝置的 IPv4 格式的 IP 位址或完全限定網域名稱 (FQDN)。
   - **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)。您可以透過換行輸入 SVM 的多個 IP 位址或完整網域名稱。

     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。

5. 儲存變更。

**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（裝置）→ 政策和設定檔**。
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**輸入 Integration Server 連線設定。輸入安裝了 Integration Server 的裝置的 IPv4 格式的 IP 位址或完全限定網域名稱 (FQDN)。
   - **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)。您可以透過換行輸入 SVM 的多個 IP 位址或完整網域名稱。

     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. 儲存變更。

**如何在應用程式介面中透過 Light Agent 配置 SVM 發現**

1. 在"應用程式主視窗"中，點擊⚙按鈕。
2. 在應用程式設定視窗中，在 **Light Agent 模式** 下面，點擊 **SVM 發現設定** 瓷片。
3. 選擇 SVM 發現方法。

   - **使用 Integration Server**輸入 Integration Server 連線設定。輸入安裝了 Integration Server 的裝置的 IPv4 格式的 IP 位址或完全限定網域名稱 (FQDN)。
   - **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)。您可以透過換行輸入 SVM 的多個 IP 位址或完整網域名稱。

     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。

4. 儲存變更。

# 配置 Light Agent 的 SVM 選取演算法

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。

Light Agent 可以套用下列 SVM 選取演算法之一進行連線：

- **標準演算法** （預設）

  標準演算法涉及以下步驟：

  1. Light Agent 可識別*本機 SVM*。

     為了將 SVM 標識為本機，Light Agent 主要使用 SVM 在虛擬基礎結構中的位置。如果 SVM 與 Light Agent 位於相同 Hypervisor 中，Light Agent 會將此類 SVM 視為本機。在某些虛擬基礎結構中，您必須使用設定檔手動指定本機 SVM。

  2. 如果 Light Agent 偵測到多個本機 SVM，Light Agent 會選擇連線的 Light Agent 數量最少的 SVM。如果您無法辨識本機 SVM，Light Agent 會選擇整個虛擬基礎結構中連線的 Light Agent 數量最少的 SVM。

有關本機 SVM 的詳細資訊，請參閱 Kaspersky Security for Virtualization Light Agent 說明。

- **延伸演算法**

  延伸演算法可讓您手動指定本機 SVM 選擇標準或停用本機 SVM 發現。為此，您需要選擇 SVM 在虛擬基礎結構中的路徑：Hypervisor、叢集或資料中心。也就是說，您必須選擇要在其中發現本機 SVM 的範圍。如果 Light Agent 無法連線到設定的發現範圍內的本機 SVM，它將停止嘗試連線。延伸演算法還允許停用 Light Agent 的本機 SVM 發現。在這種情況下，Light Agent 會選擇整個虛擬基礎結構中連線的 Light Agent 數量最少的 SVM。

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。

**如何在管理主控台 (MMC) 中配置 Light Agent 的 SVM 選取演算法**

1. 在卡巴斯基安全管理中心管理主控台樹狀目錄中，選取**政策**。
2. 選擇必要的政策並點擊以開啟政策內容。
3. 在政策視窗中，選擇"**Light Agent 模式 → SVM 選取演算法**"。
4. 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。
5. 如果需要，請為延伸 SVM 選取演算法選擇 SVM 路徑：
   - **Hypervisor**Light Agent 選擇符合特定標準的 SVM 進行連線（取決於虛擬基礎結構的類型）：
     - SVM 部署在與安裝了 Light Agent 的虛擬機相同的 Hypervisor 中（在 Microsoft Hyper-V、XenServer、VMware vSphere、KVM、Proxmox VE、Basis (Skala-R)、HUAWEI FusionSphere、Nutanix Acropolis 上的虛擬基礎結構中）、ALT Virtualization Server、Astra Linux 或 Numa vServer）。
     - SVM 與安裝了 Light Agent 的虛擬機位於同一伺服器群組中（在 OpenStack 平台、VK 雲端平台或 TIONIX 雲端平台上執行的虛擬基礎結構中）。

     如果帶有 Light Agent 的虛擬機所在的相同管理程式或相同伺服器群組中沒有可用的 SVM，則 Light Agent 不會連線到 SVM。
   - **叢集**Light Agent 選擇符合特定標準的 SVM 進行連線（取決於虛擬基礎結構的類型）：
     - SVM 部署在與安裝了 Light Agent 的虛擬機相同的 Hypervisor 叢集中（在 Microsoft Hyper-V、XenServer、VMware vSphere、KVM、Proxmox VE、Basis (Skala-R)、HUAWEI FusionSphere、Nutanix Acropolis 上的虛擬基礎結構中）、ALT Virtualization Server、Astra Linux 或 Numa vServer）。
     - SVM 與安裝了 Light Agent 的虛擬機位於同一 OpenStack 項目中（在 OpenStack 平台、VK 雲端平台或 TIONIX 雲端平台上執行的虛擬基礎結構中）。

     如果帶有 Light Agent 的虛擬機所在的相同 Hypervisor 叢集或相同 OpenStack 項目中沒有可用的 SVM，則 Light Agent 不會連線到 SVM。

- **資料中心**Light Agent 選擇符合特定標準的 SVM 進行連線（取決於虛擬基礎結構的類型）：

  - SVM 部署在與安裝了 Light Agent 的虛擬機相同的資料中心中（在 Microsoft Hyper-V、XenServer、VMware vSphere、KVM、Proxmox VE、Basis (Skala-R)、HUAWEI FusionSphere、Nutanix Acropolis 上的虛擬基礎結構中）、ALT Virtualization Server、Astra Linux 或 Numa vServer）。

  - SVM 與安裝了 Light Agent 的虛擬機位於同一可用性區域中（在 OpenStack 平台、VK 雲端平台或 TIONIX 雲端平台上執行的虛擬基礎結構中）。

  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。

6. 儲存變更。

**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（裝置）→ 政策和設定檔**。

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 選取演算法**"。

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 選擇符合特定標準的 SVM 進行連線（取決於虛擬基礎結構的類型）：

     - SVM 部署在與安裝了 Light Agent 的虛擬機相同的 Hypervisor 中（在 Microsoft Hyper-V、XenServer、VMware vSphere、KVM、Proxmox VE、Basis (Skala-R)、HUAWEI FusionSphere、Nutanix Acropolis 上的虛擬基礎結構中）、ALT Virtualization Server、Astra Linux 或 Numa vServer）。

     - SVM 與安裝了 Light Agent 的虛擬機位於同一伺服器群組中（在 OpenStack 平台、VK 雲端平台或 TIONIX 雲端平台上執行的虛擬基礎結構中）。

     如果帶有 Light Agent 的虛擬機所在的相同管理程式或相同伺服器群組中沒有可用的 SVM，則 Light Agent 不會連線到 SVM。

- **叢集**Light Agent 選擇符合特定標準的 SVM 進行連線（取決於虛擬基礎結構的類型）：

  - SVM 部署在與安裝了 Light Agent 的虛擬機相同的 Hypervisor 叢集中（在 Microsoft Hyper-V、XenServer、VMware vSphere、KVM、Proxmox VE、Basis (Skala-R)、HUAWEI FusionSphere、Nutanix Acropolis 上的虛擬基礎結構中）、ALT Virtualization Server、Astra Linux 或 Numa vServer）。

  - SVM 與安裝了 Light Agent 的虛擬機位於同一 OpenStack 項目中（在 OpenStack 平台、VK 雲端平台或 TIONIX 雲端平台上執行的虛擬基礎結構中）。

  如果帶有 Light Agent 的虛擬機所在的相同 Hypervisor 叢集或相同 OpenStack 項目中沒有可用的 SVM，則 Light Agent 不會連線到 SVM。

- **資料中心**Light Agent 選擇符合特定標準的 SVM 進行連線（取決於虛擬基礎結構的類型）：

  - SVM 部署在與安裝了 Light Agent 的虛擬機相同的資料中心中（在 Microsoft Hyper-V、XenServer、VMware vSphere、KVM、Proxmox VE、Basis (Skala-R)、HUAWEI FusionSphere、Nutanix Acropolis 上的虛擬基礎結構中）、ALT Virtualization Server、Astra Linux 或 Numa vServer）。

  - SVM 與安裝了 Light Agent 的虛擬機位於同一可用性區域中（在 OpenStack 平台、VK 雲端平台或 TIONIX 雲端平台上執行的虛擬基礎結構中）。

  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. 儲存變更。

**如何在應用程式介面中配置 Light Agent 的 SVM 選取演算法**

1. 在“應用程式主視窗”中，點擊⚙ 按鈕。

2. 在應用程式設定視窗中，在 **Light Agent 模式** 下面，點擊 **SVM 發現設定** 瓷片。

3. 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。

4. 如果需要，請為延伸 SVM 選取演算法選擇 SVM 路徑：

   - **Hypervisor**Light Agent 選擇符合特定標準的 SVM 進行連線（取決於虛擬基礎結構的類型）：

     - SVM 部署在與安裝了 Light Agent 的虛擬機相同的 Hypervisor 中（在 Microsoft Hyper-V、XenServer、VMware vSphere、KVM、Proxmox VE、Basis (Skala-R)、HUAWEI FusionSphere、Nutanix Acropolis 上的虛擬基礎結構中）、ALT Virtualization Server、Astra Linux 或 Numa vServer）。

     - SVM 與安裝了 Light Agent 的虛擬機位於同一伺服器群組中（在 OpenStack 平台、VK 雲端平台或 TIONIX 雲端平台上執行的虛擬基礎結構中）。

     如果帶有 Light Agent 的虛擬機所在的相同管理程式或相同伺服器群組中沒有可用的 SVM，則 Light Agent 不會連線到 SVM。

- **叢集**Light Agent 選擇符合特定標準的 SVM 進行連線（取決於虛擬基礎結構的類型）：

  - SVM 部署在與安裝了 Light Agent 的虛擬機相同的 Hypervisor 叢集中（在 Microsoft Hyper-V、XenServer、VMware vSphere、KVM、Proxmox VE、Basis (Skala-R)、HUAWEI FusionSphere、Nutanix Acropolis 上的虛擬基礎結構中）、ALT Virtualization Server、Astra Linux 或 Numa vServer）。

  - SVM 與安裝了 Light Agent 的虛擬機位於同一 OpenStack 項目中（在 OpenStack 平台、VK 雲端平台或 TIONIX 雲端平台上執行的虛擬基礎結構中）。

  如果帶有 Light Agent 的虛擬機所在的相同 Hypervisor 叢集或相同 OpenStack 項目中沒有可用的 SVM，則 Light Agent 不會連線到 SVM。

- **資料中心**Light Agent 選擇符合特定標準的 SVM 進行連線（取決於虛擬基礎結構的類型）：

  - SVM 部署在與安裝了 Light Agent 的虛擬機相同的資料中心中（在 Microsoft Hyper-V、XenServer、VMware vSphere、KVM、Proxmox VE、Basis (Skala-R)、HUAWEI FusionSphere、Nutanix Acropolis 上的虛擬基礎結構中）、ALT Virtualization Server、Astra Linux 或 Numa vServer）。

  - SVM 與安裝了 Light Agent 的虛擬機位於同一可用性區域中（在 OpenStack 平台、VK 雲端平台或 TIONIX 雲端平台上執行的虛擬基礎結構中）。

  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。

5. 儲存變更。

# 將 Light Agent 的連線分發到 SVM（標籤）

多個 Light Agent 可以連線到一個 SVM。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。

**如何在管理主控台 (MMC) 中將 SVM 連線標籤指派給 Light Agent**

1. 在卡巴斯基安全管理中心管理主控台樹狀目錄中，選取**政策**。

2. 選擇必要的政策並點擊以開啟政策內容。

3. 在政策視窗中，選擇“**Light Agent 模式 → SVM 連線標記**”。

4. 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。您可以使用除 ; 之外i的任何字元。

5. 儲存變更。

**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（裝置）→政策和設定檔**。

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。您可以使用除 ; 之外i的任何字元。

6. 儲存變更。

**如何在應用程式介面中將 SVM 連線標籤指派給 Light Agent**

1. 在"應用程式主視窗"中，點擊⚙按鈕。

2. 在應用程式設定視窗中，在 **Light Agent 模式** 下面，點擊 **SVM 連線標記** 瓷片。

3. 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。您可以使用除 ; 之外i的任何字元。

4. 儲存變更。

# 防護 Light Agent 和 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。

使用加密防護連線可能會影響 Kaspersky Security for Virtualization Light Agent 的效能。

**如何在管理主控台 (MMC) 的 Light Agent 中配置連線防護**

1. 在卡巴斯基安全管理中心管理主控台樹狀目錄中，選取**政策**。

2. 選擇必要的政策並點擊以開啟政策內容。

3. 在政策視窗中，選擇“**Light Agent 模式 → 連線防護**”。
4. 選擇“**加密 Light Agent 和 Protection Server 之間的資料渠道**”核取方塊。
5. 儲存變更。

**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（裝置）→ 政策和設定檔**。
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. 儲存變更。

**如何在應用程式介面的 Light Agent 中配置連線防護**

1. 在“應用程式主視窗”中，點擊⚙按鈕。
2. 在應用程式設定視窗中，在 **Light Agent 模式** 下面，點擊 **連線防護** 瓷片。
3. 選擇“**加密 Light Agent 和 Protection Server 之間的資料渠道**”核取方塊。
4. 儲存變更。

# 啟動 Light Agent

如果在 Light Agent 模式下使用 Kaspersky Endpoint Security 來防護虛擬環境，則無需單獨啟動該應用程式。要啟動應用程式，您必須向 SVM 新增一個產品授權金鑰。您可以使用卡巴斯基安全管理中心主控台中的特殊工作新增產品授權金鑰。您無法在 Light Agent 介面中管理產品授權金鑰，但可以檢視產品授權資訊（請參閱下圖）。您也可以在命令列上檢視 Light Agent 許可資訊（請參閱下面的說明）。Light Agent 從 SVM 取得此資訊。有關啟動解決方案和管理產品授權金鑰的詳細資訊，請參閱 Kaspersky Security for Virtualization Light Agent 說明。

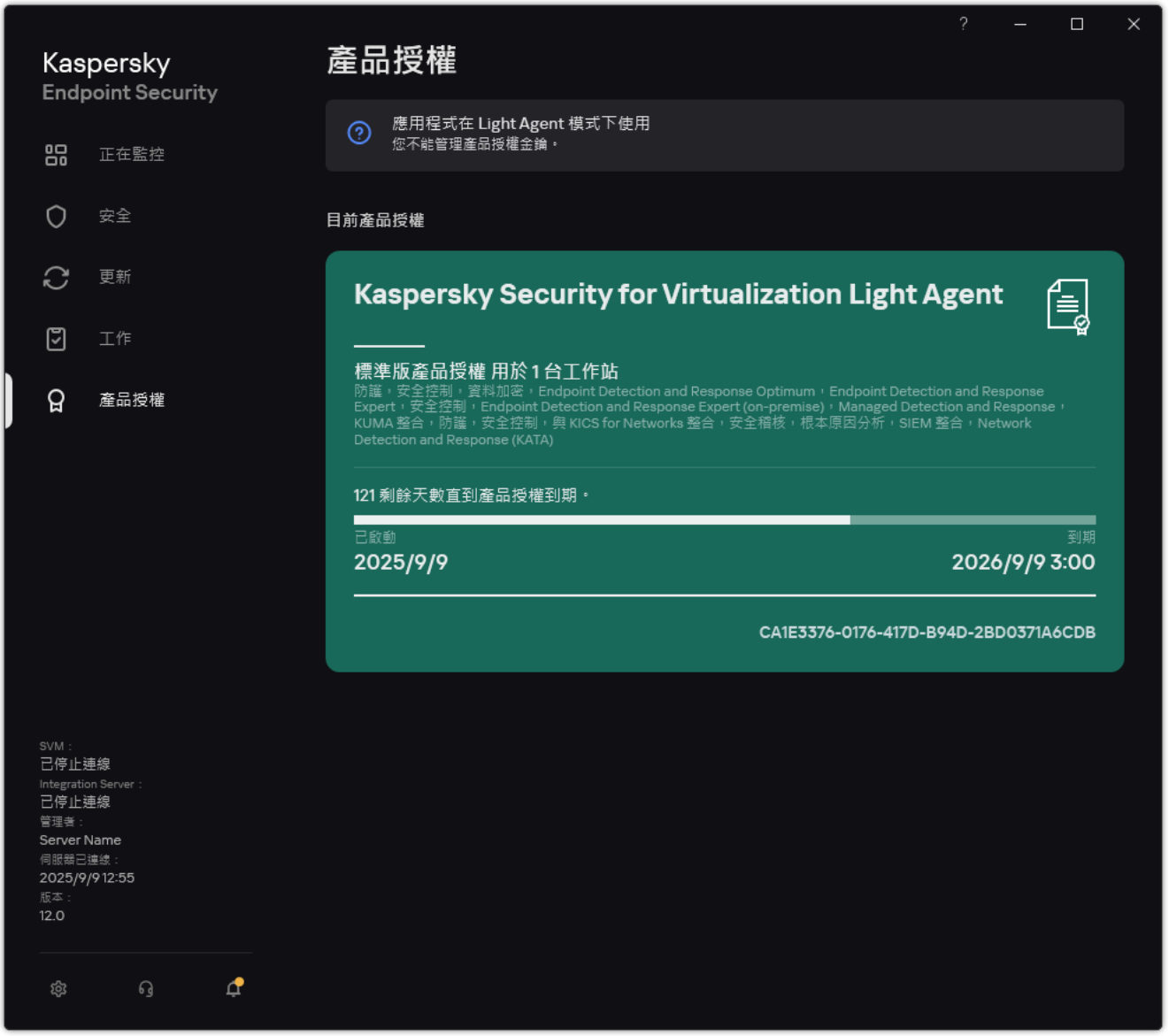
*若要檢視 Light Agent 許可資訊：*

1. 以管理員身分執行命令列解譯器 (cmd)。
2. 轉到 Kaspersky Endpoint Security 可執行檔所在資料夾。

3. 執行以下指令：

```
avp.com LICENSE /CHECK
```

結果，Kaspersky Endpoint Security 將顯示產品授權資訊：Light Agent 連線的 SVM 位址、產品授權到期前的天數以及其他資訊。如果您在啟動 Light Agent 時遇到任何問題，請參閱 技術支援知識庫。




"產品授權管理"視窗

# KSVLA Light Agent 到 KES Light Agent 遷移指南

Kaspersky Security for Virtualization 5.2 Light Agent 包括 Light Agent for Windows 5.2 元件（以下也稱為"KSVLA Light Agent"）。在 Kaspersky Security for Virtualization Light Agent 6.2 中，Light Agent 模式下的 Kaspersky Endpoint Security 被用作 Light Agent 元件。若要將解決方案更新至版本 6.2，您必須從 KSVLA Light Agent 5.2 移轉到 Light Agent 模式下的 Kaspersky Endpoint Security（以下也稱為"KES Light Agent"）。有關更新 Kaspersky Security for Virtualization Light Agent 解決方案版本的詳細資訊，請參閱 Kaspersky Security for Virtualization Light Agent 說明。

## 軟體要求

在開始從 KSVLA Light Agent 遷移到 KES Light Agent 之前，請確保您的虛擬機滿足 Kaspersky Endpoint Security for Windows 的硬件和軟體要求。KES 和 KSWS 支援的作業系統版本清單不同。例如，KES 不支援執行 Windows Server 2003 的伺服器。

從 KSVLA Light Agent 遷移到 KES Light Agent 的最低軟體需求：

- Kaspersky Endpoint Security for Windows 12.8。
- Kaspersky Security for Virtualization Light Agent 6.2（包括 Protection Server 和 Integration Server 元件）。
- 卡巴斯基安全管理中心 14.2

  如果您安裝了早期版本的卡巴斯基安全管理中心，請將其更新到 14.2 或更高版本。在此版本的卡巴斯基安全管理中心中，政策和工作批量轉換精靈允許您將政策遷移到設定檔而不是政策。在此版本的卡巴斯基安全管理中心中，政策和工作批量轉換精靈還允許您遷移範圍更廣的政策設定。

## 遷移步驟

從 KSVLA Light Agent 到 KES Light Agent 的遷移半自動執行。這是必要的，因為應用程式的架構不同。

依下列順序從 KSVLA Light Agent 遷移到 KES Light Agent：

1. **遷移 KSVLA Light Agent 工作和政策**

   要遷移政策設定，您必須執行政策和工作批量轉換精靈（遷移精靈）。遷移政策設定後，您必須手動配置遷移精靈無法自動遷移的設定（例如，資料庫更新設定）。遷移後，還建議檢查遷移精靈是否正確遷移了所有設定。

   如果啟用密碼防護來限制對 KSVLA Light Agent 的存取，則在安裝 KES Light Agent 之前，您需要在 KSVLA Light Agent 原則中停用密碼防護。您無法在 KES Light Agent 安裝套件設定中輸入解除安裝密碼。在 KSVLA Light Agent 之上完成 KES Light Agent 的安裝後，您必須在 KES 政策中啟用密碼防護。

2. **在 Light Agent 模式下安裝 Kaspersky Endpoint Security**

   您可以通過以下方式安裝 KES Light Agent：

   - 刪除 KSVLA Light Agent 後安裝 KES Light Agent（建議）
   - 在 KSVLA Light Agent 之上安裝 KES Light Agent

3. **確認應用程式在遷移後處於工作狀態**

   從 KSVLA Light Agent 遷移到 KES Light Agent 後，確保應用程式運行正常。啟動轉換的政策。在卡巴斯基安全管理中心主控台中查看虛擬機狀態（應該是*OK*）。確保應用程式沒有報告錯誤，同時檢查上次連線到 SVM 的時間以及虛擬機防護狀態。你不需要 啟動 Light Agent，因為產品授權金鑰已新增到 SVM。

# 安裝 KES Light Agent 而不是 KSVLA Light Agent

您可以通過以下方式安裝 KES Light Agent：

- 刪除 KSVLA Light Agent 後安裝 KES Light Agent（建議）
- 在 KSVLA Light Agent 之上安裝 KES Light Agent

### 刪除 KSVLA Light Agent

您可以使用 *遠端安裝應用程式*工作遠端刪除該應用程式、在虛擬機上本機或在虛擬機範本中刪除該應用程式。刪除 KSVLA Light Agent 後，您可能需要重新啟動虛擬機。

刪除 KSVLA Light Agent 後，使用任何合適的方法 安裝 KES Light Agent。

### 安裝 Kaspersky Endpoint Security

如果啟用密碼防護來限制對 KSVLA Light Agent 的存取，則在安裝 KES Light Agent 之前，您需要在 KSVLA Light Agent 原則中停用密碼防護。您無法在 KES Light Agent 安裝套件設定中輸入解除安裝密碼。在 KSVLA Light Agent 之上完成 KES Light Agent 的安裝後，您必須 在 KES 政策中啟用密碼防護。

當 安裝 Kaspersky Endpoint Security時，您必須選擇 **Light Agent 防護虛擬環境** 模式。在虛擬機上安裝 KES Light Agent 之前，安裝程式會將 KSVLA Light Agent 偵測為不相容軟體並將其移除。不支援遷移 KSVLA Light Agent 配置。也就是說，當您安裝 KES Light Agent 時，要安裝的元件集合由您在安裝套件屬性或安裝精靈中的選擇決定。刪除 KSVLA Light Agent 後，您必須重新啟動虛擬機。

安裝 KES Light Agent 時，不會遷移 KSVLA Light Agent 的設定和工作。若要遷移設定和工作，請執行政策和工作批次轉換精靈。

您可以使用`status`指令或者在電腦內容的卡巴斯基安全管理中心主控台中，在應用程式介面的"**安全**"區域中檢查已安裝元件清單。您可以在安裝後使用*變更應用程式元件*變更元件集合。

# KSVLA Light Agent 和 KES Light Agent 元件的對應關係

KSVLA Light Agent 和 KES Light Agent 的元件集合幾乎相同。KES Light Agent 比 KSVLA Light Agent 有更多設定。遷移後，新設定具有預設值。

KSVLA Light Agent 和 KES Light Agent 元件的對應關係

| Light Agent 5.2 | KES Light Agent |
|---|---|
| Scan kernel | 應用程式內核 |
| File Anti-Virus | 檔案威脅防護 |
| Mail Anti-Virus | 郵件威脅防護 |

| Light Agent 5.2 | KES Light Agent |
| --- | --- |
| Web Anti-Virus | Web 威脅防護 |
| Firewall | 防火牆 |
| Network Attack Blocker | 網路威脅防護 |
| Application Privilege Control | 主機入侵防禦 |
| Applications Launch Control | 應用程式控制 |
| Web Control | Web 控制 |
| Device Control | 裝置控制 |
| System Watcher | 在 Kaspersky Endpoint Security 中，此元件分為以下元件：<br>• 弱點利用防禦<br>• 行為偵測<br>• 修復引擎 |
| System Integrity Monitoring | 系統完整性監控 |
| Integration with Kaspersky Endpoint Agent | *（不受支援）*<br>從 Kaspersky Endpoint Security for Windows 11.9.0 開始，Kaspersky Endpoint Agent 分發套件不再是分發包的一部分。 |
| AMSI Protection | AMSI 防護 |

# 遷移 KSVLA Light Agent 工作和政策

您可以使用政策和工作批量轉換精靈（以下也稱為"遷移精靈"）遷移 KSVLA Light Agent 政策和工作的設定。

KSVLA Light Agent 的遷移精靈僅在管理主控台 (MMC) 中可用。政策和工作設定無法在網頁主控台和雲端主控台中進行遷移。

遷移政策和工作涉及以下特殊注意事項：

- 一項新政策的名稱是 *<Policy>（已轉換）*。
- 新政策的狀態為*停用政策*。
- 禁止修改設定（"掛鎖"）不會被遷移。遷移精靈會設定預設值。
- 政策設定檔不會遷移。您必須手動新增政策設定檔。
- 改進了信任區域管理。在 KSVLA Light Agent 中，您只能在建立政策時新增預先定義的排除項目。隨後，在政策屬性中，您可以設定先前新增的預定義排除項目或手動新增排除項目。您無法在政策屬性中新增預先定義的排除項目。在 KES Light Agent 中，預先定義的排除項目在政策建立期間和已建立政策的屬性中均可用。您也可以選擇安裝套件中預先定義的排除項目。
- Kaspersky Endpoint Security 中應用程式使用者介面的配置已被從安裝程式移至政策。例如，如果您需要隱藏應用程式的使用者介面，管理政策設定。
- Kaspersky Endpoint Security 和 KSVLA Light Agent 中用於設定基於權限的存取控制 (RBAC) 的功能集合不同。您必須從頭開始設定使用者對功能區域的存取權限。

**如何使用政策和工作批量轉換精靈遷移 KSVLA Light Agent 政策設定**

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

政策和工作批量轉換精靈將啟動。按照精靈的說明進行操作。

步驟 1. 選擇需要為其轉換政策和工作的應用程式

在此步驟，您需要選擇 Kaspersky Endpoint Security for Windows。前往下一步。

步驟 2. 轉換政策

選擇要轉換的 Kaspersky Security for Virtualization 5.2 Light Agent for Windows 政策。前往下一步。

遷移精靈將開始轉換政策。在轉換期間，遷移精靈會提示您接受 KSN 聲明的條件。一項新政策的名稱是 *<Policy>（已轉換）*。

步驟 3. 轉換工作

遷移精靈將為 Kaspersky Endpoint Security for Windows 建立新工作。在工作清單中，選擇您想為 Kaspersky Endpoint Security 建立的 KSVLA Light Agent 工作。新工作將被命名為 *<工作名稱>（已轉換）*。前往下一步。

步驟 4. 精靈完成

結束精靈。

遷移政策後，必須開啟該政策的屬性，檢查其設定並儲存該政策。如果您不完成這些步驟，KES Light Agent 可能會忽略轉換後的政策。

特別注意Light Agent 的 SVM 連線設定、排除項目清單、受信任應用程式、受信任網址、應用程式控制規則的遷移。

# 將 [KSVLA Light Agent+KEA] 配置遷移到 [KES Light Agent+內建代理] 配置

為了支援使用 Kaspersky Endpoint Security for Windows 作為 EDR (KATA)、EDR Optimum、Kaspersky Sandbox 的一部分，內建代理已被新增到應用程式中。您再也無需分開 Kaspersky Endpoint Agent 應用程式來使用這些解決方案。

從 KSVLA Light Agent 遷移到 KES Light Agent 時，EDR (KATA)、EDR Optimum、Kaspersky Sandbox 解決方案繼續與 Kaspersky Endpoint Security 內建代理協同工作。此外，Kaspersky Endpoint Agent 將被從電腦移除。

從 KSVLA Light Agent 遷移到 KES Light Agent 之前，您必須將 Kaspersky Security for Virtualization 的所有元件更新至版本 6.2，包括 Protection Server 和 Integration Server。有關更新 Kaspersky Security for Virtualization Light Agent 解決方案版本的詳細資訊，請參閱 Kaspersky Security for Virtualization Light Agent 說明。

將 [KSVLA Light Agent+KEA] 配置遷移到 [KES Light Agent+內建代理] 配置涉及以下步驟：

1. **遷移政策和工作**

   將 [KSVLA Light Agent+KEA] 政策和工作遷移到 [KES Light Agent+內建代理] 包含以下步驟：

   1. 使用政策和工作批量轉換精靈將政策和工作從 KSVLA Light Agent 遷移到 KES Light Agent（僅在管理主控台 (MMC) 上可用）。

      結果，建立了一個名為*<Policy>（已轉換）*的新政策。名為*<工作名稱>（已轉換）*的新 KES 工作也得到建立。

   2. 使用用於從 Kaspersky Endpoint Agent 遷移的精靈將政策和工作從 KEA 遷移到 KES（僅在 Web 主控台和雲端主控台中可用）。

      結果會建立一個名為*<Kaspersky Endpoint Security 政策名稱>&<Kaspersky Endpoint Agent 政策名稱>*的新政策。新工作和 KES 工作也會建立。

2. **從 KSVLA Light Agent 遷移到 KES Light Agent**

   從 KSVLA Light Agent 遷移到 KES Light Agent 涉及 安裝 KES Light Agent 而不是 KSVLA Light Agent。

   管理員通常啟用密碼防護以限制對 KSVLA Light Agent 和 KEA 的存取。您只能在*遠端安裝應用程式*工作的屬性中輸入 KEA 解除安裝密碼。若要遷移，您必須停用 KSVLA Light Agent 的密碼防護。

   要執行遷移，您必須選擇支援 Detection and Response 解決方案所需的元件作為 Kaspersky Endpoint Security 的一部分。安裝應用程式後，Kaspersky Endpoint Security 將切換到使用內建代理並刪除 Kaspersky Endpoint Agent。

3. **產品授權功能**

   如果在 Light Agent 模式下使用應用程式，則無需啟動該應用程式。要啟動應用程式，您必須向 SVM 新增一個產品授權金鑰。您還必須將用於啟動附加功能（例如 EDR Optimum）的產品授權金鑰新增至 SVM。也就是說，作為遷移的一部分，功能許可會自動發生。

4. **檢查 Kaspersky Endpoint Detection and Response Optimum 和 Kaspersky Sandbox 的健康**

   如果升級後電腦在卡巴斯基安全管理中心中具有"*緊急*"狀態：

   - 請確保電腦安裝了網路代理 13.2或更高版本。
   - 透過檢視"*應用程式元件狀態報告*"來檢查內建代理的運行狀態。如果元件的狀態為"*未安裝*"，請使用*變更應用程式元件*工作來安裝元件。
   - 請確保在 Kaspersky Endpoint Security for Windows 的新政策中接受卡巴斯基安全網路聲明。
   - 確保使用*應用程式元件狀態報告*啟動 EDR Optimum 功能 。如果元件的狀態為"*產品授權不支援*"，請確保 EDR Optimum 的產品授權金鑰自動分發功能已開啟。
   - 檢查虛擬機與 SVM 的連線狀態。您可以在 Kaspersky Endpoint Security 中或使用應用程式指令取得 Light Agent 與 SVM 連線狀態的資訊： 。

# 從命令列管理應用程式

您可以從命令列管理 Kaspersky Endpoint Security。可以執行 `avp.com HELP` 指令來檢視用於管理應用程式的指令清單。要閱讀特定指令的語法，請輸入 `avp.com HELP <command>`。

指令中的特殊字元必須逸出。要逸出字元 `&`, `|`、`(`, `)`、`<`、`>`、`^`，請使用 `^` 字元（例如，若要使用 `&` 字元，請輸入 `^&`）。若要逸出 `%` 字元，輸入 `%%`。

`1` 值的替代值為 `yes`、`on`、`enable`、`enabled` 和 `true`。`0` 值的替代值為 `no`、`off`、`disable`、`disabled` 和 `false`。

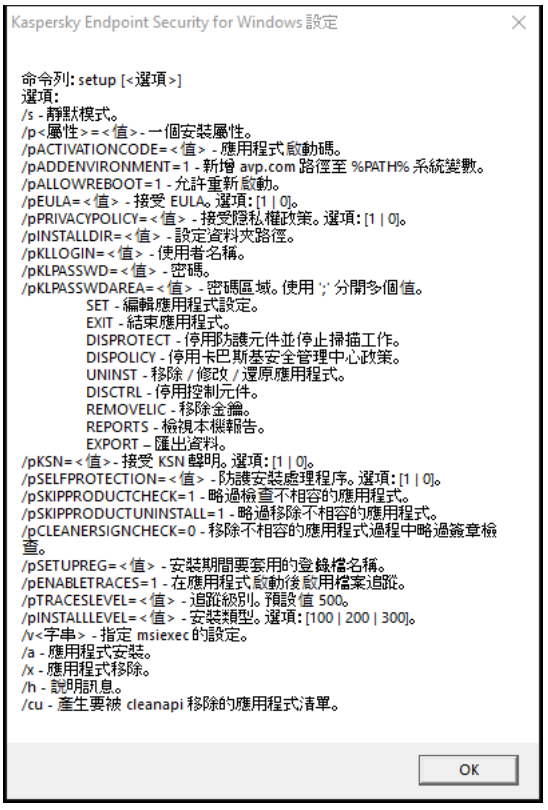
# Setup。安裝應用程式

可以在以下模式之一下從命令列安裝 Kaspersky Endpoint Security：

- 使用應用程式安裝精靈互動模式。
- 在靜默模式下。以靜默模式啟動安裝後，安裝過程不再需要您的參與（靜默安裝）。要在靜默模式下安裝應用程式，請使用 `/s` 和 `/qn` 鍵。

  在靜默模式下安裝應用程式之前，請開啟並閱讀最終使用者產品授權協議和隱私政策文字。最終使用者產品授權協議和隱私政策文字包含在 Kaspersky Endpoint Security 分發套件中。只有在您已經完全閱讀、理解和接受最終使用者產品授權協議的規定和條款，理解並同意您的資料將按照隱私政策進行處理和傳輸（包括傳輸到協力廠商國家/地區），並且您已經完全閱讀和理解隱私政策的情況下，您才可以繼續安裝應用程式。如果您不接受最終使用者產品授權協議的規定和條款以及隱私政策，請不要安裝或使用 Kaspersky Endpoint Security。

您可以執行 /h 指令來檢視用於安裝應用程式的指令清單。要獲取安裝指令語法說明，請輸入 setup_kes.exe /h。結果，安裝程式會顯示一個具有指令選項說明的視窗（請見下圖）。




安裝指令選項說明

*要安裝應用程式或升級以前版本的應用程式：*

1. 以管理員身分執行命令列解譯器 (cmd.exe)。
2. 轉到 Kaspersky Endpoint Security 分發套件所在資料夾。
3. 執行以下指令：

```
setup_kes.exe /pEULA=1 /pPRIVACYPOLICY=1 [/pKSN=1|0] [/pCONFIGPATH=<path to the configuration file>] [/pALLOWREBOOT=1] [/pSKIPPRODUCTCHECK=1] [/pSKIPPRODUCTUNINSTALL=1] [/pKLLOGIN=<user name> /pKLPASSWD=<password> /pKLPASSWDAREA=<password scope>] [/pENABLETRACES=1|0 /pTRACESLEVEL=<tracing level>] [/pSKIPKB5007186CHECK=1] [/s]
```

或

```
msiexec /i <distribution kit name> EULA=1 PRIVACYPOLICY=1 [KSN=1|0] [CONFIGPATH=<path to the configuration file>] [ALLOWREBOOT=1] [SKIPPRODUCTCHECK=1] [KLLOGIN=<user name> KLPASSWD=<password> KLPASSWDAREA=<password scope>] [ENABLETRACES=1|0 TRACESLEVEL=<tracing level>] [SKIPKB5007186CHECK=1] [/qn]
```

結果，應用程式被安裝在電腦上。您可以透過“status”命令確認應用程式是否已安裝並檢查應用程式設定。

| | |
|---|---|
| EULA=1 | 接受最終使用者產品授權協議的條款。授權協議的內容包括在 Kaspersky Endpoint Security 分發套件中。<br>必須接受最終使用者產品授權協議才能安裝應用程式或升級應用程式版本。 |
| PRIVACYPOLICY=1 | 接受隱私政策。隱私政策的文字包含在 Kaspersky Endpoint Security 分發套件中。<br>要安裝應用程式或升級應用程式版本，您必須接受隱私政策。 |
| KSN | 接受或拒絕參與卡巴斯基安全網路 (KSN)。如果沒有為此參數設定任何值，在首次啟動 Kaspersky Endpoint Security 時，Kaspersky Endpoint Security 將提示您確認同意或拒絕加入 KSN。可用值：<br>• 1 – 同意加入 KSN。<br>• 0 – 拒絕加入 KSN（預設值）。<br>Kaspersky Endpoint Security 分發套件已針對與卡巴斯基安全網路配合使用進行最佳化。如果您選擇不加入卡巴斯基安全網路，則應該在安裝完成後立即更新 Kaspersky Endpoint Security。 |
| CONFIGPATH=<path to the configuration file> | 使用預定義設定安裝應用程式。為此，您需要上傳定義 Kaspersky Endpoint Security 設定的檔案。您可以在應用程式的本機介面中建立設定檔。 |
| ALLOWREBOOT=1 | 自動重新啟動電腦（如果安裝或升級應用程式後需要重新啟動）。如果未為此參數設定任何值，則阻止電腦自動重新啟動。<br>安裝 Kaspersky Endpoint Security 時，不需要重新啟動。僅當在安裝前必須移除不相容的應用程式時，才需要重新啟動。更新應用程式版本時也可能需要重新啟動。 |
| SKIPPRODUCTCHECK=1 | 停用已安裝軟體檢查。分發套件中包含的 incompatible.txt 檔案提供了可能引起相容性問題的軟體清單。如果沒有為此參數設定任何值，並且偵測到清單中的軟體，則將終止 Kaspersky Endpoint Security 的安裝。 |
| SKIPPRODUCTUNINSTALL=1 | 停用從incompatible.txt清單中自動移除偵測到的軟體。如果沒有為此參數設定任何值，則 Kaspersky Endpoint Security 將嘗試移除可能引起相容性問題的軟體。<br>當使用 msiexec 安裝程式安裝 Kaspersky Endpoint Security 時，不可啟用自動移除軟體。若要自動刪除可能導致相容性問題的軟體，請使用 setup_kes.exe 檔案。 |
| CLEANERSIGNCHECK=0\|1 | 驗證 incompatible.txt 清單中偵測到的軟體檔案的數位簽章。若要刪除軟體，Kaspersky Endpoint Security 會執行軟體安裝程式檔案。如果安裝程式檔案沒有數位簽章，Kaspersky Endpoint Security 會將檔案視為不受信任並停止移除軟體以免執行潛在惡意代碼。如果應用程式無法驗證被偵測到的軟體檔案的數位簽章，Kaspersky Endpoint Security 安裝將以錯誤停止。<br>預設值依據軟體安裝方法而異：<br>• 0 意味著數位簽章驗證被停用（如果透過卡巴斯基安全管理中心佈署，則是預設值）。<br>• 1 意味著數位簽章驗證被啟用（如果應用程式本機安裝，則是預設值）。 |
| STANDALONEMODE=1 | 在 Endpoint Detection and Response Agent (EDR Agent) 配置中安裝應用程式以與 Kaspersky Endpoint Detection and Response (KATA) 或者 Kaspersky Endpoint Detection and Response Expert (on-premise) 解決方案進行整合。如果您的組織中與 Kaspersky Endpoint Detection and Response 類解決方案一起部署了協力廠商端點防護平台 (EPP)，則需要此配置。這使得 Endpoint Detection and Response Agent 配置中的 Kaspersky Endpoint Security 與協力廠商 EPP 應用程式相容。 |
| KLLOGIN | 設定用於存取 Kaspersky Endpoint Security 功能和設定的使用者名稱（"密碼防護"元件）。該使用者名稱與"KLPASSWD"和"KLPASSWDAREA"設定一起進行設定。預設使用使用者名稱 KLAdmin。 |
| KLPASSWD | 指定用於存取 Kaspersky Endpoint Security 功能和設定的密碼（該密碼與"KLLOGIN"和"KLPASSWDAREA"參數一起指定）。<br>如果您指定了密碼，但沒有指定帶有 KLLOGIN 參數的使用者名稱，將預設使用KLAdmin 使用者名稱。 |

| | |
|---|---|
| KLPASSWDAREA | 指定用於存取 Kaspersky Endpoint Security 的密碼範圍。當使用者嘗試執行包含在此範圍中的操作時，Kaspersky Endpoint Security 將提示使用者輸入帳戶憑證（"KLLOGIN"和"KLPASSWD"參數）。使用";"字元以指定多個值。<br>可用值：<br>• SET – 修改應用程式設定。<br>• EXIT – 結束應用程式。<br>• DISPROTECT – 停用防護元件並停止掃描工作。<br>• DISPOLICY – 停用卡巴斯基安全管理中心政策。<br>• UNINST – 從電腦中移除應用程式。<br>• DISCTRL – 停用控制元件。<br>• REMOVELIC – 刪除金鑰。<br>• REPORTS – 檢視報告。<br>• EXPORT – 匯出應用程式設定。<br>例如，KLPASSWDAREA=SET;KLPASSWDAREA=UNINST;KLPASSWDAREA=EXIT。<br>KLAdmin 帳戶有權執行任何受密碼防護的操作。因此，配置 KLAdmin 帳戶的密碼範圍是不可能的。如果您嘗試配置 KLAdmin 帳戶的密碼範圍，應用程式將禁止"Everyone"群組執行指定的操作。 |
| PROTECTOSSERVICES | 作業係統防護服務功能。作業係統服務防護可防止協力廠商應用程式干擾作業係統服務的運作。此類服務（例如）包括應用程式自動啟動服務。<br>• 1 表示作業係統服務防護已啟用（預設值）。<br>• 0 表示作業係統服務防護已停用。 |
| ENABLETRACES | 啟用或停用應用程式跟蹤。Kaspersky Endpoint Security 在啟動後將偵錯檔案儲存在資料夾 %ProgramData%\Kaspersky Lab\KES.12.12\Traces 中。可用值：<br>• 1 – 跟蹤已啟用。<br>• 0 – 跟蹤已停用（預設值）。 |
| TRACESLEVEL | 偵錯詳細等級。可用值：<br>• 100（關鍵）。僅包含有關致命錯誤的訊息。<br>• 200（高）。有關所有錯誤的訊息，包括致命錯誤。<br>• 300（診斷）。有關所有錯誤的訊息以及警告。<br>• 400（重要）。所有錯誤訊息、警告和其他資訊。<br>• 500（一般）。有關所有錯誤的訊息和警告，以及有關正常模式下應用程式操作的詳細資訊（預設）。<br>• 600（低）。所有訊息。 |
| ENABLEAZURESUPPORT | 啟用或停用 Azure WVD 相容模式。可用值：<br>• 1 – Azure WVD 相容模式被啟用。<br>• 0 – Azure WVD 相容模式被停用（預設值）。<br>此功能可確保在 Kaspersky Anti Targeted Attack Platform 主控台中正確顯示 Azure 虛擬機狀態。為了監控電腦的效能，Kaspersky Endpoint Security 將遙測資料傳送到 KATA 伺服器。遙測包括電腦的 ID（Sensor ID）。Azure WVD 相容模式允許為這些虛擬機分配永久唯一的 Sensor ID。如果關閉相容模式，由於 Azure 虛擬機的工作方式，Sensor ID 可能會在電腦重新啟動後發生變化。這可能會導致主控台上出現重複的虛擬機。 |
| AMPPL | 啟用或停用 Kaspersky Endpoint Security 處理程序使用 AM-PPL 技術（Antimalware Protected Process Light）提供的防護。有關 AM-PPL 技術的詳細資訊，請存取 Microsoft 網站。<br>AM-PPL 技術適用於 Windows 10 版本 1703 (RS2) 或更高版本以及 Windows Server 2019 作業系統。<br>可用值：<br>• 1 – 啟用 Kaspersky Endpoint Security 處理程序使用 AM-PPL 技術提供的防護。<br>• 0 – 停用 Kaspersky Endpoint Security 處理程序使用 AM-PPL 技術提供的防護。 |
| UPGRADEMODE | 應用程式升級模式：<br>• Seamless 意味著用電腦重新啟動升級應用程式（預設值）。<br>• Force 意味著升級應用程式而無需重新啟動。<br>從版本 11.10.0 開始您可以升級應用程式而無需重新啟動。若要升級更早版本的應用程式，您必須重新啟動電腦。從版本 11.11.0 開始您可以安裝修補程式而無需重新啟動。<br>安裝 Kaspersky Endpoint Security 時，不需要重新啟動。因此，應用程式的升級模式將在應用程式設定中指定。您可以在應用程式設定中或政策中變更該參數。<br>當升級已安裝的應用程式時，命令行參數的優先順序比在應用程式設定或 setup.ini 檔案中指定的參數的優先順序低。例如，如果在命令行中指定"Force"升級模式，在應用程式設定中指定"Seamless"模式，升級將透過電腦重新啟動安裝（Seamless）。 |

| | |
|---|---|
| RESTAPI | 透過 REST API 管理應用程式。要透過 REST API 管理應用程式，必須指定使用者名稱（ RESTAPI_User 參數）。<br>可用值：<br>• 1 –允許透過 REST API 進行管理。<br>• 0 –封鎖透過 REST API 進行管理（預設值）。<br>要透過 REST API 管理應用程式，必須允許使用管理系統進行管理。要執行此操作，請設定 AdminKitConnector=1 參數。如果透過 REST API 管理應用程式，則無法使用 Kaspersky 的管理系統來管理應用程式。 |
| RESTAPI_User | 用於透過 REST API 管理應用程式的 Windows 網域帳戶的使用者名稱。只有此使用者可以透過 REST API 管理應用程式。輸入格式為 <DOMAIN>\<UserName> 的使用者名稱（例如， RESTAPI_User=COMPANY\Administrator ）。您只能選擇一個使用者來使用 REST API。<br>新增使用者名稱是透過 REST API 管理應用程式的先決條件。 |
| RESTAPI_Port | 用於透過 REST API 管理應用程式的連接埠。預設情況下使用 6782 連接埠。確保連接埠空閒。 |
| RESTAPI_Certificate | 用於識別請求的憑證（例如， RESTAPI_Certificate=C:\cert.pem ）。Kaspersky Endpoint Security 與 REST 用戶端進行安全交互需要設定請求識別。為此，您必須安裝憑證並隨後簽署每個請求的承載。 |
| ADMINKITCONNECTOR | 使用管理系統管理應用程式。例如，管理系統包括卡巴斯基安全管理中心。除了 Kaspersky 管理系統，您還可以使用協力廠商解決方案。Kaspersky Endpoint Security 為此提供了一個 API。<br>可用值：<br>• 1 - 允許在管理系統的幫助下管理應用程式（預設值）。<br>• 0 - 僅允許透過本機介面管理應用程式。 |
| EnableUniqueSensorID | 在安裝或更新應用程式期間建立唯一的電腦識別符 (Sensor ID)。Sensor ID 在 Kaspersky Anti Targeted Attack Platform 解決方案中用於識別向伺服器傳送遙測資料的電腦。建立 Sensor ID 時，應用程式使用的演算法會考慮電腦的配置，例如主機板序號。在某些情況下，例如，在虛擬環境中使用應用程式時，Sensor ID 可能會重複。因此， Kaspersky Anti Targeted Attack Platform 無法辨識傳送遙測資料的電腦。要建立唯一的 Sensor ID，需要設定參數 EnableUniqueSensorID=1 。結果，應用程式將使用不同的演算法來建立 Sensor ID，該演算法會考慮有關電腦的其他資料。這可確保唯一的 Sensor ID。<br>預設情況下，未設定此參數。應用程式在以下情況下繼承 Sensor ID：<br>• 更新應用程式版本；<br>• 將 [KES+KEA] 配置遷移到 [KES+內建代理] 配置。<br>作為應用程式修復的一部分，安裝程式会嘗試繼承Sensor ID。如果 Sensor ID 無法還原，應用程式會建立一個新的 Sensor ID。 |
| SKIPKB5007186CHECK=1 | 停用檢查已安裝的作業系統更新 KB5007186。<br>在安裝應用程式之前，安裝程式會檢查已安裝的作業系統更新。KB5007186 更新位於可能導致應用程式出現問題的作業系統更新清單中。有關詳細資訊，請參閱卡巴斯基知識庫。因此，如果發現此更新，安裝程式將中止安裝。若要繼續安裝，請設定 SKIPKB5007186CHECK=1 。 |
| | |

範例:

```
setup_kes.exe /pEULA=1 /pPRIVACYPOLICY=1 /pKSN=1 /pALLOWREBOOT=1

msiexec /i kes_win.msi EULA=1 PRIVACYPOLICY=1 KSN=1 KLLOGIN=Admin KLPASSWD=Password
KLPASSWDAREA=EXIT;DISPOLICY;UNINST /qn

setup_kes.exe /pEULA=1 /pPRIVACYPOLICY=1 /pKSN=1 /pENABLETRACES=1 /pTRACESLEVEL=600 /s
```

安裝 Kaspersky Endpoint Security 後，將啟動試用版產品授權，除非您在 setup.ini 檔案中提供了啟動碼。試用版產品授權通常擁有較短的有效期。當試用版授權到期，所有 Kaspersky Endpoint Security 功能將轉為停用。要繼續使用應用程式，您需要使用應用程式啟動精靈或特殊指令以正式產品授權啟動應用程式。

以靜默模式安裝應用程式或升級應用程式版本時，支援以下檔案的使用：

- setup.ini – 應用程式安裝的一般設定。

  要應用 setup.ini 檔案中的設定，請將該檔案放入包含 Kaspersky Endpoint Security 分發套件的資料夾。

- install.cfg – – Kaspersky Endpoint Security 的執行設定

  如果要套用 install.cfg 設定檔的設定，您需要在以下應用程式安裝指令中指定檔案的路徑：`CONFIGPATH=<path to the configuration file>`。

- setup.reg – 登錄機碼。

  僅當在setup.ini 檔案中為`SetupReg`參數設定了`setup.reg`值時，setup.reg 檔案中的登錄機碼才會被寫入登錄。setup.reg 檔案由 Kaspersky 專家生成。不建議修改該檔案的內容。要應用 setup.reg 檔案中的設定，請將該檔案放入包含 Kaspersky Endpoint Security 分發套件的資料夾。您也可以將 setup.reg 檔案放在其他資料夾中。如果這樣做，則需要在以下應用程式安裝指令中指定檔案的路徑：`SETUPREG=<path to the setup.reg file>`。

# Setup /x。移除應用程式

可以透過以下方式之一從命令列移除 Kaspersky Endpoint Security：

- 使用應用程式安裝精靈互動模式。
- 在靜默模式下。以靜默模式啟動移除後，移除過程不再需要您的參與（靜默解除安裝）。要在靜默模式下移除應用程式，請使用 `/s` 和 `/qn` 開關。

*要在靜默模式下移除應用程式：*

1. 以管理員身分執行命令列解譯器 (cmd.exe)。
2. 轉到 Kaspersky Endpoint Security 分發套件所在資料夾。
3. 執行以下指令：

   - 如果移除過程沒有密碼防護：

     ```
     setup_kes.exe /s /x
     ```

     或

     ```
     msiexec.exe /x <GUID> /qn
     ```

     `<GUID>` 是應用程式的唯一 ID。您可以在技術支援知識庫中或者使用以下命令找到應用程式的 GUID：

     ```
     wmic product where "Name like '%Kaspersky Endpoint Security%'" get Name, IdentifyingNumber
     ```

   - 如果移除過程有密碼防護：

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

     或

     ```
     msiexec.exe /x <GUID> KLLOGIN=<user name> KLPASSWD=<password> /qn
     ```

   您也可以使用 `SAVEQB` 參數來儲存應用程式掃描並放置在備份中的檔案。檔案的備份副本儲存在 `C:\ProgramData\Kaspersky Lab\KES.12.12\QB` 資料夾中。預設情況下，停用在備份中儲存檔案（`SAVEQB=0`）。

   範例：

   ```
   msiexec.exe /x {9A017278-F7F4-4DF9-A482-0B97B70DD7ED} KLLOGIN=KLAdmin KLPASSWD=samplePassword /qn
   ```

# msiexec /i.還原應用程式

復原時，應用程式會檢查並還原所有損壞的應用程式模組和在應用程式安裝過程中建立的系統登錄機碼的完整性。

可以在以下模式之一下從命令列恢復 Kaspersky Endpoint Security：

- 使用應用程式安裝精靈互動模式。
- 在靜默模式下。以靜默模式啟動還原後，還原過程不再需要您的參與。

如果 Kaspersky Endpoint Security 安裝程式在還原模式下執行，且應用程式不需要還原，則安裝程式不會進行任何變更。

如果 Kaspersky Endpoint Security 安裝程式在復原模式下執行，且應用程式未安裝，則安裝程式將啟動安裝處理程序。

*要在靜默模式下還原應用程式：*

1. 以管理員身分執行命令列解譯器 (cmd.exe)。
2. 轉到 Kaspersky Endpoint Security 分發套件所在資料夾。
3. 執行以下指令：
   - 如果還原過程沒有密碼防護：

     ```
     msiexec.exe /i <GUID> REINSTALL=ALL /qn
     ```

     <GUID> 是應用程式的唯一 ID。您可以在技術支援知識庫中或者使用以下命令找到應用程式的 GUID：

     ```
     wmic product where "Name like '%Kaspersky Endpoint Security%'" get Name,
     IdentifyingNumber
     ```

   - 如果還原過程有密碼防護：

     ```
     msiexec.exe /i <GUID> REINSTALL=ALL KLLOGIN=<user name> KLPASSWD=<password> /qn
     ```

     範例：

     ```
     msiexec.exe /i {9A017278-F7F4-4DF9-A482-0B97B70DD7ED} REINSTALL=ALL KLLOGIN=KLAdmin
     KLPASSWD=samplePassword /qn
     ```

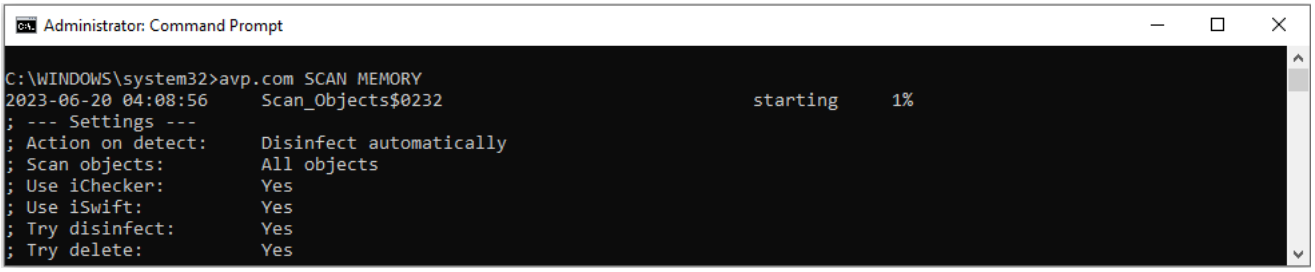
# AVP 命令

*要從命令列管理 Kaspersky Endpoint Security：*

1. 以管理員身分執行命令列解譯器 (cmd.exe)。
2. 轉到 Kaspersky Endpoint Security 可執行檔所在資料夾。
   您可以在應用程式安裝期間將可執行檔的路徑新增到 %PATH% 系統變數。
3. 使用以下模板來執行命令：

```
avp.com <command> [options]
```

結果，Kaspersky Endpoint Security 將執行該指令（參見下圖）。




從命令列管理應用程式

# SCAN。惡意軟體掃描

執行"*惡意軟體掃描*"工作

若要執行命令，請轉到 Kaspersky Endpoint Security 可執行檔所在的資料夾。您也可以將可執行檔路徑新增至 %PATH% 系統變數並執行命令，而無需導覽至應用程式資料夾。

指令語法

```
avp.com SCAN [<scan scope>] [<action on threat detection>] [<file types>] [<scan exclusions>] [/R[A]:<report file>] [<scan technologies>] [/C:<file with scan settings>]
```

| **掃描範圍** | |
|---|---|
| `<files to scan>` | 以空格分隔的檔案和資料夾清單。長路徑必須用引號括起來。短路徑（MS-DOS 格式）不需要用引號括起來。範例：<br>• `"C:\Program Files (x86)\Example Folder"` – 長路徑。<br>• `C:\PROGRA~2\EXAMPL~1` – 短路徑。 |

| | |
|---|---|
| /ALL | 執行"*惡意軟體掃描*"工作。Kaspersky Endpoint Security 掃描以下物件：<br>• 內核記憶體<br>• 作業系統啟動時載入的物件<br>• 開機磁區<br>• 作業系統備份儲存區<br>• 所有硬碟磁碟機和卸除式磁碟機<br>在 Kaspersky Endpoint Security for Windows 12.12 中，電子郵件被排除在應用程式掃描範圍之外。傳入和傳出電子郵件的掃描由 郵件威脅防護元件執行。如果您使用的是較早版本的管理外掛程式，即使政策中包含電子郵件，該應用程式也會將電子郵件排除在掃描範圍之外。 |
| /MEMORY | 掃描內核記憶體 |
| /STARTUP | 掃描在作業系統啟動時載入的物件 |
| /REMDRIVES | 掃描卸除式磁碟機。 |
| /FIXDRIVES | 掃描硬碟磁碟機。 |
| /NETDRIVES | 掃描網路磁碟機。 |
| /QUARANTINE | 掃描 Kaspersky Endpoint Security 備份區中的檔案。 |
| /@:<file list.lst> | 掃描清單中的檔案和資料夾。清單中的每個檔案都必須另起一行。長路徑必須用引號括起來。短路徑（MS-DOS 格式）不需要用引號括起來。範例：<br>• `"C:\Program Files (x86)\Example Folder"` – 長路徑。<br>• `C:\PROGRA~2\EXAMPL~1` – 短路徑。 |

| **偵測到威脅後的動作** | |
|---|---|
| /i0 | **通知**如果選擇此選項，Kaspersky Endpoint Security 會在偵測到受感染檔案時將這些檔案的相關資訊新增到活動威脅清單。 |
| /i1 | **解毒；若解毒失敗則通知**如果選擇該選項，Kaspersky Endpoint Security 將自動對已經偵測到的所有受感染的檔案執行解毒操作。如果解毒失敗，Kaspersky Endpoint Security 會將偵測到的受感染檔案的相關資訊新增到活動威脅清單。 |
| /i2 | **解毒；若解毒失敗則刪除**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。<br>預設情況下已選擇此操作。 |
| /i3 | **解毒失敗則刪除**如果無法解毒或刪除已感染檔案，還會刪除複合檔案（例如，存檔）。 |
| /i4 | **刪除**如果無法刪除已感染檔案，還會刪除複合檔案（例如，存檔）。 |

| **檔案類型** | |
|---|---|
| /fe | **按副檔名掃描檔案**如果啟用該設定，則應用程式僅掃描被感染的檔案。此時，系統將根據檔案的副檔名確定檔案格式。 |
| /fi | **按格式掃描檔案**如果啟用該設定，則應用程式僅掃描被感染的檔案。在掃描檔案以尋找惡意程式碼之前，系統將分析檔案的內部頭以確定檔案的格式（例如，.txt、.doc 或 .exe）。掃描還會查找具有特定副檔名的檔案。 |
| /fa | **所有檔案**如果啟用該設定，應用程式將毫無例外地掃描所有檔案（所有格式和副檔名）。<br>這是預設設定。 |

| **掃描排除項目** | |
|---|---|
| -e:a | RAR、ARJ、ZIP、CAB、LHA、JAR 和 ICE 壓縮檔案將從掃描範圍中排除。 |
| -e:<file mask> | 與檔案遮罩比對的檔案將從掃描範圍中排除。範例：<br>• 遮罩 `*.exe` 將包括具有 exe 副檔名的檔案的所有路徑。<br>• 遮罩 `example*` 將包括名為 EXAMPLE 的檔案的所有路徑。 |

| | |
|---|---|
| `-e:<seconds>` | 掃描時間長於指定時間限制（以秒為單位）的檔案將從掃描範圍中排除。 |
| `-es:<megabytes>` | 大於指定大小限制（以百萬位元組為單位）的檔案將從掃描範圍中排除。 |

| **將事件儲存至報告檔案模式（僅適用於掃描、更新程式和回溯設定檔）** | |
|---|---|
| `/R:<report file>` | 僅將關鍵事件儲存到報告檔案中。 |
| `/RA:<report file>` | 將所有事件儲存到報告檔案中。 |

| **掃描技術** | |
|---|---|
| `/iChecker=on\|off` | 該技術允許透過排除特定檔案不掃描的方式提高掃描速度。該技術將使用特殊演算法將檔案排除在掃描範圍之外，該演算法會考慮 Kaspersky Endpoint Security 資料庫的發佈日期、檔案的上次掃描日期以及對掃描設定的任何修改。iChecker 技術受到幾個限制：它無法操作大檔案，並且僅能套用至擁有程式可辨識結構的檔案 (例如：.exe、.dll、.lnk、.ttf、.inf、.sys、.com、.chm、.zip 和 .rar)。 |
| `/iSwift=on\|off` | 該技術允許透過排除特定檔案不掃描的方式提高掃描速度。該技術將使用特殊演算法將檔案排除在掃描範圍之外，該演算法會考慮 Kaspersky Endpoint Security 資料庫的發佈日期、檔案的上次掃描日期以及對掃描設定的任何修改。iSwift 技術是對用於 NTFS 檔案系統的 iChecker 技術的增強版。 |

| **進階設定** | |
|---|---|
| `/C:<file with scan settings>` | 包含“*惡意軟體掃描*”工作設定的檔案。必須手動建立該檔案並以 TXT 格式儲存。該檔案可以具有以下內容：`[<scan scope>] [<action on threat detection>] [<file types>] [<scan exclusions>] [/R[A]:<report file>] [<scan technologies>]`。 |

範例：
```
avp.com SCAN /R:log.txt /MEMORY /STARTUP "C:\Documents and Settings\All Users\My Documents" "C:\Program Files"
```

# UPDATE。更新資料庫和程式模組

執行“*資料庫和應用程式模組更新*”工作

若要執行命令，請轉到 Kaspersky Endpoint Security 可執行檔所在的資料夾。您也可以將可執行檔路徑新增至 %PATH% 系統變數並執行命令，而無需導覽至應用程式資料夾。

如果應用程式在 Light Agent 模式下安裝則不可執行此命令。

指令語法

```
avp.com UPDATE [local] ["<update source>"] [/R[A]:<report file>] [/C:<包含更新設定的檔案>]
```

| **更新工作設定** | |
|---|---|
| `local` | 開始安裝應用程式後自動建立的“*資料庫和應用程式模組更新*”工作。您可以在本機應用程式介面或卡巴斯基安全管理中心的主控台中變更“*資料庫和應用程式模組更新*”工作的設定。如果未配置此設定，則 Kaspersky Endpoint Security 會使用預設設定或命令中指定的設定來開始“*資料庫和應用程式模組更新*”工作。您可以按以下方式配置“*資料庫和應用程式模組更新*”工作設定：<br>• `UPDATE` 使用預設設定啟動“*資料庫和應用程式模組更新*”工作：更新來源是卡巴斯基更新伺服器，帳戶是 System，以及其他預設設定。<br>• `UPDATE local` 啟動安裝後自動建立的“*資料庫和應用程式模組更新*”工作（預定義工作）。<br>• `UPDATE <update settings>` 使用手動定義的設定啟動“*資料庫和應用程式模組更新*”工作（請參見下文）。 |

| **更新來源** | |
|---|---|
| `"<update source>"` | HTTP 或 FTP 伺服器的位址，或具有更新套件的共用資料夾的位址。只能指定一個更新來源。如果未指定更新來源，則 Kaspersky Endpoint Security 將使用預設來源：卡巴斯基更新伺服器。 |

| 將事件儲存至報告檔案模式（僅適用於掃描、更新程式和回溯設定檔） | |
|---|---|
| /R:<report file> | 僅將關鍵事件儲存到報告檔案中。 |
| /RA:<report file> | 將所有事件儲存到報告檔案中。 |

| 進階設定 | |
|---|---|
| /C:<file with update settings> | 包含"*資料庫和應用程式模組更新*"工作設定的檔案。必須手動建立該檔案並以 TXT 格式儲存。該檔案可以具有以下內容：["<update source>"] [/R[A]:<report file>]。 |

範例:
```
avp.com UPDATE local
avp.com UPDATE "ftp://my_server/kav updates" /RA:avbases_upd.txt
```

# ROLLBACK。最近更新還原

回溯上次病毒資料庫更新。這允許您在必要時將資料庫和應用程式模組回溯到以前的版本，例如，當新資料庫版本包含無效簽章而導致 Kaspersky Endpoint Security 封鎖了安全的應用程式時。

若要執行命令，請轉到 Kaspersky Endpoint Security 可執行檔所在的資料夾。您也可以將可執行檔路徑新增至 %PATH% 系統變數並執行命令，而無需導覽至應用程式資料夾。

如果應用程式在 Light Agent 模式下安裝則不可執行此命令。

指令語法

```
avp.com ROLLBACK [/R[A]:<report file>]
```

| 將事件儲存至報告檔案模式（僅適用於掃描、更新程式和回溯設定檔） | |
|---|---|
| /R:<report file> | 僅將關鍵事件儲存到報告檔案中。 |
| /RA:<report file> | 將所有事件儲存到報告檔案中。 |

範例:
```
avp.com ROLLBACK /RA:rollback.txt
```

# TRACES。偵錯

只要應用程式在使用中，就會在電腦中儲存偵錯檔案，當應用程式被移除後，偵錯檔案將被永久移除。偵錯檔案（身分驗證代理的偵錯檔案除外）儲存在%ProgramData%\Kaspersky Lab\KES.12.12\Traces資料夾中。預設情況下，停用偵錯。

若要執行命令，請轉到 Kaspersky Endpoint Security 可執行檔所在的資料夾。您也可以將可執行檔路徑新增至 %PATH% 系統變數並執行命令，而無需導覽至應用程式資料夾。

指令語法

```
avp.com TRACES on|off [<tracing level>] [<advanced settings>]
```

| 偵錯等級 | |
|---|---|
| `<tracing level>` | 偵錯詳細等級。可用值：<br>• `100`（關鍵）。僅包含有關致命錯誤的訊息。<br>• `200`（高）。有關所有錯誤的訊息，包括致命錯誤。<br>• `300`（診斷）。有關所有錯誤的訊息以及警告。<br>• `400`（重要）。所有錯誤訊息、警告和其他資訊。<br>• `500`（一般）。有關所有錯誤的訊息和警告，以及有關正常模式下應用程式操作的詳細資訊（預設）。<br>• `600`（低）。所有訊息。 |

| 進階設定 | |
|---|---|
| `all` | 使用`file`和`mem`參數執行指令。 |
| `file` | 儲存一個偵錯檔案（無大小限制）。 |
| `rot` | 將偵錯儲存到有限數量的大小有限的檔案集合中，並在達到最大大小時覆蓋舊檔案。 |
| `mem` | 將偵錯儲存到 dump 檔案。 |

例如：
```
avp.com TRACES on 500
avp.com TRACES off
avp.com TRACES on 500 mem
avp.com TRACES off file
```

# START。啟動設定檔

啟動設定檔（例如，啟動資料庫更新或啟用防護元件）。

若要執行命令，請轉到 Kaspersky Endpoint Security 可執行檔所在的資料夾。您也可以將可執行檔路徑新增至 %PATH% 系統變數並執行命令，而無需導覽至應用程式資料夾。

指令語法

```
avp.com START <profile> [/R[A]:<report file>]
```

| 設定檔 | |
|---|---|
| `<profile>` | 設定檔名稱。*設定檔*是 Kaspersky Endpoint Security 元件、工作或功能。您可以執行`HELP START`指令來檢視可用設定檔清單。 |

| 將事件儲存至報告檔案模式（僅適用於掃描、更新程式和回溯設定檔） | |
|---|---|
| `/R:<report file>` | 僅將關鍵事件儲存到報告檔案中。 |
| `/RA:<report file>` | 將所有事件儲存到報告檔案中。 |

範例:
```
avp.com START Scan_Objects
```

# STOP。停止設定檔

停止設定檔執行（例如，停止卸除式磁碟機掃描或停用防護元件）。

要執行此指令，必須啟用密碼防護。使用者必須具有**"停用防護元件"**和**"停用控制元件"**權限。

若要執行命令，請轉到 Kaspersky Endpoint Security 可執行檔所在的資料夾。您也可以將可執行檔路徑新增至 %PATH% 系統變數並執行命令，而無需導覽至應用程式資料夾。

指令語法

```
avp.com STOP <profile> /login=<user name> /password=<password>
```

| 設定檔 | |
|---|---|
| `<profile>` | 設定檔名稱。*設定檔*是 Kaspersky Endpoint Security 元件、工作或功能。您可以執行 `HELP STOP` 指令來檢視可用設定檔清單。 |

| 身分驗證 | |
|---|---|
| `/login=<user name> /password=<password>` | 具有所需"密碼防護"權限的使用者帳戶憑據。 |

# STATUS。設定檔狀態

顯示應用程式設定檔的狀態資訊（例如，`running` 或 `completed`）。您可以執行 `HELP STATUS` 指令來檢視可用設定檔清單。

Kaspersky Endpoint Security 還會顯示有關服務設定檔狀態的資訊。聯絡卡巴斯基技術支援時，可能需要有關服務設定檔狀態的資訊。

若要執行命令，請轉到 Kaspersky Endpoint Security 可執行檔所在的資料夾。您也可以將可執行檔路徑新增至 %PATH% 系統變數並執行命令，而無需導覽至應用程式資料夾。

指令語法

```
avp.com STATUS [<profile>]
```

如果您輸入沒有設定檔的指令，Kaspersky Endpoint Security 將顯示應用程式所有設定檔的狀態。

# STATISTICS。設定檔操作統計

顯示應用程式設定檔的統計資訊（例如，掃描持續時間或偵測到的威脅數）。您可以執行 `HELP STATISTICS` 指令來檢視可用設定檔清單。

若要執行命令，請轉到 Kaspersky Endpoint Security 可執行檔所在的資料夾。您也可以將可執行檔路徑新增至 %PATH% 系統變數並執行命令，而無需導覽至應用程式資料夾。

指令語法

```
avp.com STATISTICS <profile>
```

# RESTORE。從備份區中還原檔案

將檔案從備份區還原到原始資料夾。如果指定路徑中已存在具有相同名稱的檔案，則應用程式將要求確認以替換檔案。要還原的檔案將保留其原始名稱進行複製。

要執行此指令，必須啟用密碼防護。使用者必須具有"**從備份區還原**"權限。

*備份區*儲存保留在解毒過程中刪除或修改的檔案的備份副本。*備份副本*是指對檔案進行病毒清除或移除前建立的檔案副本。檔案的備份副本以特定格式儲存並且不會帶來威脅。

檔案的備份副本儲存在 `C:\ProgramData\Kaspersky Lab\KES.12.12\QB` 資料夾中。

管理員群組中的使用者被授予存取該資料夾的完整權限。其帳戶用於安裝 Kaspersky Endpoint Security 的使用者被授予該資料夾的有限存取權限。

Kaspersky Endpoint Security 不提供用於設定檔備份副本的使用者存取權限的功能。

若要執行命令，請轉到 Kaspersky Endpoint Security 可執行檔所在的資料夾。您也可以將可執行檔路徑新增至 %PATH% 系統變數並執行命令，而無需導覽至應用程式資料夾。

指令語法

```
avp.com RESTORE [/REPLACE] <file name> /login=<user name> /password=<password>
```

| **進階設定** | |
|---|---|
| `/REPLACE` | 覆蓋現有檔案。 |
| `<file name>` | 要還原的檔案的名稱。 |

| **身分驗證** | |
|---|---|
| `/login=<user name> /password=<password>` | 具有所需"密碼防護"權限的使用者帳戶憑據。 |

範例:

```
avp.com RESTORE /REPLACE true_file.txt /login=KLAdmin /password=samplePassword
```

# EXPORT。匯出應用程式設定

將 Kaspersky Endpoint Security 設定匯出到檔案。如果該命令僅包含要將設定匯出到的檔案的名稱，則應用程式將如下放置該檔案：

- 如果 avp.com 的路徑被新增至 %PATH% 系統變數中，應用程式會將檔案放置在 `C:\Windows\SysWOW64` 資料夾中。
- 如果從應用程式安裝資料夾執行命令，匯出將失敗，因為應用程式的自我防護功能會封鎖在應用程式資料夾中建立新檔案。若要將應用程式設定匯出到檔案，請輸入檔案路徑。

要執行此指令，必須啟用密碼防護。使用者必須具有**"設定匯出"**權限。

若要執行命令，請轉到 Kaspersky Endpoint Security 可執行檔所在的資料夾。您也可以將可執行檔路徑新增至 %PATH% 系統變數並執行命令，而無需導覽至應用程式資料夾。

指令語法

```
avp.com EXPORT <profile> <file name> /login=<user name> /password=<password>
```

| **設定檔** | |
|---|---|
| `<profile>` | 設定檔名稱。*設定檔*是 Kaspersky Endpoint Security 元件、工作或功能。您可以執行 `HELP EXPORT` 指令來檢視可用設定檔清單。 |

| **要匯出的檔案** | |
|---|---|
| `<file name>` | 應用程式設定將匯出到的檔案的名稱。您也可以輸入檔案路徑。您可以將 Kaspersky Endpoint Security 設定匯出為 DAT 或 CFG 設定檔、TXT 文字檔案或 XML 檔。 |

| **身分驗證** | |
|---|---|
| `/login=<user name> /password=<password>` | 具有所需"密碼防護"權限的使用者帳戶憑據。 |

例如：

```
avp.com EXPORT ids ids_C:\Users\Fred123\Documents\config.dat
avp.com EXPORT fm fm_config.txt
```

# IMPORT。匯入應用程式設定

從使用`EXPORT`命令建立的檔案匯入 Kaspersky Endpoint Security 設定。

要執行此指令，必須啟用密碼防護。使用者必須具有**"配置應用程式設定"**權限。

若要執行命令，請轉到 Kaspersky Endpoint Security 可執行檔所在的資料夾。您也可以將可執行檔路徑新增至 %PATH% 系統變數並執行命令，而無需導覽至應用程式資料夾。

指令語法

```
avp.com IMPORT <file name> /login=<user name> /password=<password>
```

| 要匯入的檔案 | |
|---|---|
| <file name> | 將從中匯入應用程式設定的檔案的名稱。您可以從 DAT 或 CFG 設定檔、TXT 文字檔案或 XML 檔匯入 Kaspersky Endpoint Security 設定。 |

| 身分驗證 | |
|---|---|
| /login=<user name> /password=<password> | 具有所需"密碼防護"權限的使用者帳戶憑據。 |

範例:
```
avp.com IMPORT config.dat /login=KLAdmin /password=samplePassword
```

# ADDKEY。套用金鑰檔案

使用金鑰檔案啟動 Kaspersky Endpoint Security。如果應用程式已啟動，則該金鑰將作為備用金鑰新增。

若要執行命令，請轉到 Kaspersky Endpoint Security 可執行檔所在的資料夾。您也可以將可執行檔路徑新增至 %PATH% 系統變數並執行命令，而無需導覽至應用程式資料夾。

如果應用程式在 Light Agent 模式下安裝則不可執行此命令。

指令語法

```
avp.com ADDKEY <file name> [/login=<user name> /password=<password>]
```

| 金鑰檔案 | |
|---|---|
| <file name> | 金鑰檔案名稱。 |

| 身分驗證 | |
|---|---|
| /login=<user name> /password=<password> | 使用者帳戶憑證。只有啟用了密碼防護時，才需要輸入這些憑證。 |

範例:
```
avp.com ADDKEY file.key
```

# LICENSE。產品授權

管理 Kaspersky Endpoint Security、EDR Optimum 或 EDR Expert (Kaspersky Endpoint Detection and Response Add-on) 的產品授權金鑰。

要執行此指令並刪除產品授權金鑰，必須啟用密碼防護。使用者必須具有**"移除金鑰"**權限。

若要執行命令，請轉到 Kaspersky Endpoint Security 可執行檔所在的資料夾。您也可以將可執行檔路徑新增至 %PATH% 系統變數並執行命令，而無需導覽至應用程式資料夾。

如果應用程式在 Light Agent 模式下安裝則不可執行此命令。

指令語法

```
avp.com LICENSE <operation> [/login=<user name> /password=<password>]
```

| **操作** | |
|---|---|
| `/ADD <file name>` | 使用金鑰檔案啟動 Kaspersky Endpoint Security。如果應用程式已啟動，則該金鑰將作為備用金鑰新增。 |
| `/ADD <activation code>` | 使用啟動碼啟動 Kaspersky Endpoint Security。如果應用程式已啟動，則該金鑰將作為備用金鑰新增。 |
| `/REFRESH` | 更新 Kaspersky Endpoint Security 產品授權的狀態。結果，應用程式將從卡巴斯基啟動伺服器收到最新的產品授權狀態資訊。 |
| `/REFRESH <license ID>` | 使用產品授權 ID 更新產品授權狀態。透過使用此命令，您可以更新 EDR Add-on、MDR Add-on、KUMA Add-on 或其他產品授權的狀態。您可以從產品授權憑證中取得產品授權 ID。結果，應用程式將從卡巴斯基啟動伺服器收到最新的產品授權狀態資訊。 |
| `/CHECK` | 獲取產品授權資訊。Kaspersky Endpoint Security 顯示有關所有新增的產品授權金鑰的資訊，包括備用金鑰、EDR Add-on、MDR Add-on、KUMA Add-on 金鑰和其他金鑰。<br><br>Kaspersky Endpoint Security 顯示以下產品授權資訊：<br><br>• 產品授權名稱；<br>• 產品授權識別符；<br>• 以 Light Agent 模式安裝應用程式的虛擬機所連線的 Protection Server (SVM) 的位址；<br>• 產品授權類型：試用版、商業版、Beta 版、訂購；<br>• 應用程式啟動的日期和時間；<br>• 產品授權到期的日期和時間；<br>• 產品授權到期前的天數。 |
| `/CHECK <license ID>` | 透過 ID 獲取產品授權資訊。您可以使用此命令取得產品授權資訊。您可以從產品授權憑證中取得產品授權 ID。 |
| `/DEL /login=<user name> /password=<password>` | 刪除應用程式的產品授權金鑰。備用金鑰也將被刪除。 |
| `/DEL <license ID> /login=<user name> /password=<password>` | 使用產品授權 ID 刪除金鑰。使用此命令，您可以從 EDR Add-on、MDR Add-on、KUMA Add-on 或其他產品授權中刪除金鑰。您可以從產品授權憑證中取得產品授權 ID。 |

| **身分驗證** | |
|---|---|
| `/login=<user name> /password=<password>` | 具有所需"密碼防護"權限的使用者帳戶憑據。 |

範例:

```
avp.com LICENSE /ADD file.key
avp.com LICENSE /ADD AAAAA-BBBBB-CCCCC-DDDDD
avp.com LICENSE /DEL 3084-000789-456AB78C /login=KLAdmin /password=samplePassword
```

# RENEW。購買產品授權

開啟卡巴斯基網站以購買或續約產品授權。

若要執行命令，請轉到 Kaspersky Endpoint Security 可執行檔所在的資料夾。您也可以將可執行檔路徑新增至 %PATH% 系統變數並執行命令，而無需導覽至應用程式資料夾。

如果應用程式在 Light Agent 模式下安裝則不可執行此命令。

# PBATESTRESET。在加密磁碟之前重設磁碟檢查結果

重設完整磁碟加密 (FDE) 的相容性檢查結果，包括卡巴斯基磁碟加密和 BitLocker 磁碟機加密技術。

在執行完整磁碟加密之前，應用程式會執行大量檢查以驗證是否可以對電腦進行加密。如果電腦不支援完整磁碟加密，Kaspersky Endpoint Security 會記錄有關不相容性的資訊。下次嘗試加密時，應用程式不會執行此檢查，並警告您無法進行加密。如果電腦的硬體設定已變更，則必須重設應用程式先前記錄的相容性檢查結果，以重新檢查系統硬碟磁碟機與卡巴斯基磁碟加密或 BitLocker 磁碟機加密技術的相容性。

若要執行命令，請轉到 Kaspersky Endpoint Security 可執行檔所在的資料夾。您也可以將可執行檔路徑新增至 %PATH% 系統變數並執行命令，而無需導覽至應用程式資料夾。

# EXIT。結束應用程式

結束 Kaspersky Endpoint Security。應用程式將從電腦的 RAM 中移除。

要執行此指令，必須啟用密碼防護。使用者必須具有**"結束應用程式"**權限。

若要執行命令，請轉到 Kaspersky Endpoint Security 可執行檔所在的資料夾。您也可以將可執行檔路徑新增至 %PATH% 系統變數並執行命令，而無需導覽至應用程式資料夾。

指令語法

```
avp.com EXIT /login=<user name> /password=<password>
```

# EXITPOLICY。停用政策

在電腦上停用卡巴斯基安全管理中心政策。所有 Kaspersky Endpoint Security 設定均可進行配置，包括政策中已上鎖的設定 (🔒)。

要執行此指令，必須啟用密碼防護。使用者必須具有**"停用卡巴斯基安全管理中心政策"**權限。

若要執行命令，請轉到 Kaspersky Endpoint Security 可執行檔所在的資料夾。您也可以將可執行檔路徑新增至 %PATH% 系統變數並執行命令，而無需導覽至應用程式資料夾。

指令語法

```
avp.com EXITPOLICY /login=<user name> /password=<password>
```

# STARTPOLICY。啟用政策

在電腦上啟用卡巴斯基安全管理中心政策。將根據政策配置應用程式設定。

若要執行命令，請轉到 Kaspersky Endpoint Security 可執行檔所在的資料夾。您也可以將可執行檔路徑新增至 %PATH% 系統變數並執行命令，而無需導覽至應用程式資料夾。

# DISABLE。停用防護

停用具有過期 Kaspersky Endpoint Security 產品授權的電腦上的檔案威脅防護。無法在未啟動應用程式或具有有效產品授權的電腦上執行此指令。

若要執行命令，請轉到 Kaspersky Endpoint Security 可執行檔所在的資料夾。您也可以將可執行檔路徑新增至 %PATH% 系統變數並執行命令，而無需導覽至應用程式資料夾。

# SPYWARE。間諜軟體偵測

管理間諜軟體偵測。預設情況下已啟用間諜軟體偵測。

若要執行命令，請轉到 Kaspersky Endpoint Security 可執行檔所在的資料夾。您也可以將可執行檔路徑新增至 %PATH% 系統變數並執行命令，而無需導覽至應用程式資料夾。

指令語法

```
avp.com SPYWARE on|off
```

# KSN。在 KSN / KPSN 之間切換

選擇卡巴斯基解決方案以確定檔案或網站的信譽。Kaspersky Endpoint Security 支援以下用於使用 Kaspersky 信譽資料庫的基礎結構解決方案：

- *卡巴斯基安全網路 (KSN)* 是大多數 Kaspersky 應用程式使用的解決方案。KSN 參與者從卡巴斯基接收資訊，並向 Kaspersky 傳送使用者電腦上偵測到的物件的資訊，以便 Kaspersky 分析人員進行額外分析，並包括在信譽和統計資料庫中。

- *卡巴斯基安全網路 (KSN)* 是讓承載 Kaspersky 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。

  - 法律禁止或公司安全政策限制將任何資料傳輸到國家/地區外部或公司 LAN 外部。

若要執行命令，請轉到 Kaspersky Endpoint Security 可執行檔所在的資料夾。您也可以將可執行檔路徑新增至 %PATH% 系統變數並執行命令，而無需導覽至應用程式資料夾。

如果應用程式在 Light Agent 模式下安裝則不可執行此命令。

指令語法

```
avp.com KSN /global | /private <file name>
```

| **卡巴斯基安全網路設定檔** | |
|---|---|
| `<file name>` | 包含卡巴斯基私有安全網路設定的設定檔的名稱。此檔案具有 PKCS7 或 PEM 副檔名。 |

範例:

```
avp.com KSN /global
avp.com KSN /private C:\ksn_config.pkcs7
```

# SERVERBINDINGDISABLE。停用伺服器連線防護

執行*管理伺服器連線防護*工作，移除電腦連線管理伺服器的密碼。透過這種方式，工作停用管理伺服器連線的防護。

要執行此指令，必須啟用密碼防護。

若要執行命令，請轉到 Kaspersky Endpoint Security 可執行檔所在的資料夾。您也可以將可執行檔路徑新增至 %PATH% 系統變數並執行命令，而無需導覽至應用程式資料夾。

指令語法

```
avp.com SERVERBINDINGDISABLE [/password=<password>]
```

| 密碼 | |
|---|---|
| /password=<password> | KLAdmin 使用者帳戶的密碼或*管理伺服器連線防護*工作的密碼。<br>如果未指定參數，Kaspersky Endpoint Security 將提示您在下一行輸入密碼。 |

# KESCLI 命令

KESCLI 命令可讓您接收用 OPSWAT 元件進行電腦防護的狀態的相關資訊，讓您執行 "*惡意軟體掃描*"和"*資料庫和應用程式模組更新*"等標準工作。

您可以透過使用 `kescli --help` 命令或者縮寫命令 `kescli -h` 來檢視 KESCLI 命令清單。

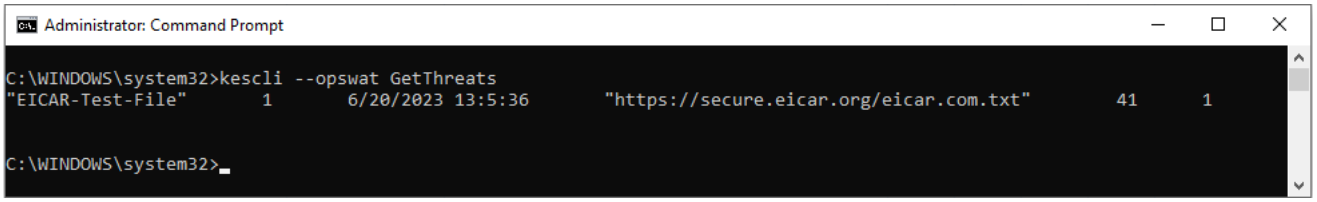
*要從命令列管理 Kaspersky Endpoint Security：*

1. 以管理員身分執行命令列解譯器 (cmd.exe)。
2. 轉到 Kaspersky Endpoint Security 可執行檔所在資料夾。

   您可以在應用程式安裝期間將可執行檔的路徑新增到 %PATH% 系統變數。
3. 使用以下模板來執行命令：

   ```
   kescli <指令> [選項]
   ```

結果，Kaspersky Endpoint Security 將執行該指令（參見下圖）。




從命令列管理應用程式

# Scan。惡意軟體掃描

執行"*惡意軟體掃描* (完整掃描) "工作。

若要執行工作，管理員必須在政策中允許使用本機工作。

若要執行命令，請轉到 Kaspersky Endpoint Security 可執行檔所在的資料夾。

指令語法

```
kescli --opswat Scan "<scan scope>" <action on threat detection>
```

您可以使用 `GetScanState` 指令檢查"*惡意軟體掃描*"工作完成的狀態，使用 `GetLastScanTime` 指令檢視掃描上次完成的日期和時間。

| 掃描範圍 | |
|---|---|
| `<scan scope>` | `;`-以空格分隔的檔案和資料夾清單。例如，`"C:\Program Files (x86)\Example Folder"`。 |

| 偵測到威脅後的動作 | |
|---|---|
| `0` | **通知**如果選擇此選項，Kaspersky Endpoint Security 會在偵測到受感染檔案時將這些檔案的相關資訊新增到活動威脅清單。 |
| `1` | **解毒；若解毒失敗則刪除**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。<br>預設情況下已選擇此操作。 |

範例:
```
kescli --opswat Scan "C:\Documents and Settings\All Users\My Documents;C:\Program Files" 1
```

# GetScanState。掃描完成狀態

顯示有關"*惡意軟體掃描* (完整掃描) "工作完成狀態的資訊：

- `1` – 掃描進行中。
- `0` – 掃描未執行。

若要執行命令，請轉到 Kaspersky Endpoint Security 可執行檔所在的資料夾。

指令語法

```
kescli --opswat GetScanState
```

# GetLastScanTime。確定掃描完成時間

顯示上次"*惡意軟體掃描* (完整掃描)"工作完成的日期和時間的相關資訊。

若要執行命令，請轉到 Kaspersky Endpoint Security 可執行檔所在的資料夾。

指令語法

```
kescli --opswat GetLastScanTime
```

# GetThreats。獲取偵測到的威脅的資料

顯示偵測到的威脅清單（*威脅報告*）。該報告包含建立報告前最後 30 天內的威脅和病毒活動的相關資訊。

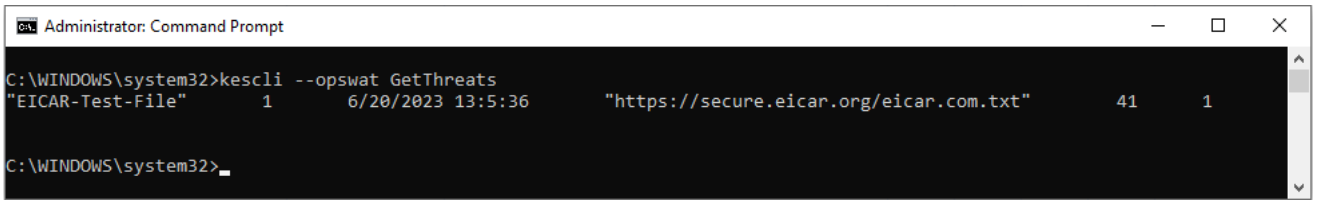
若要執行命令，請轉到 Kaspersky Endpoint Security 可執行檔所在的資料夾。

指令語法

```
kescli --opswat GetThreats
```

當執行該指令時，Kaspersky Endpoint Security 將傳送以下格式的回應：

```
<name of detected object> <type of object> <detection date and time> <path to file>
<action on threat detection> <threat danger level>
```




從命令列管理應用程式

| 物件類型 | |
|---|---|
| 0 | 不知道(Unknown)。 |
| 1 | 病毒(Virware)。 |
| 2 | 木馬程式(Trojware)。 |
| 3 | 惡意程式(Malware)。 |
| 4 | 廣告程式(Adware)。 |
| 5 | 自動撥號程式(Pornware)。 |
| 6 | 可能被網路犯罪分子用來傷害使用者的電腦或資料的應用程式(Riskware)。 |
| 7 | 可能被用來防護惡意程式碼的封裝物件(Packed)。 |
| 20 | 未知物件(Xfiles)。 |
| 21 | 已知應用程式(Software)。 |
| 22 | 隱藏的檔案(Hidden)。 |
| 23 | 需要注意的應用程式(Pupware)。 |
| 24 | 異常成為(Anomaly)。 |
| 30 | 未確定(Undetect)。 |
| 40 | 廣告橫幅(Banner)。 |
| 50 | 網路攻擊(Attack)。 |
| 51 | 登錄檔存取(Registry)。 |
| 52 | 可疑活動(Suspicion)。 |
| 60 | 弱點(Vulnerability)。 |
| 70 | Phishing(Phishing)。 |
| 80 | 垃圾電子郵件附件(Attachment)。 |
| 90 | 卡巴斯基安全網路偵測到的惡意軟體(Urgent)。 |
| 100 | 未知連接(Suspic URL)。 |
| 110 | 其它惡意軟體(Behavioral)。 |

| 偵測到威脅後的動作 | |
|---|---|
| 0 | 不知道(unknown)。 |
| 1 | 威脅得到補救(ok)。 |
| 2 | 物件被感染，尚未得到清除(infected)。 |
| 5 | 物件在壓縮文檔中，尚未得到清除(archive)。 |
| 9 | 物件已被清除(disinfected)。 |
| 10 | 物件尚未得到清除(not disinfected)。 |
| 11 | 物件被刪除(deleted)。 |
| 13 | 已建立物件的備份副本(backupped)。 |
| 15 | 物件已被移動到備份(quarantined)。 |
| 23 | 物件在電腦重啟時被刪除(delete on reboot)。 |
| 25 | 物件在電腦重啟時被清除(disinfect on reboot)。 |
| 29 | 物件被使用者移動到了備份(added by user)。 |
| 30 | 物件被新增至排除項目(added to exclude)。 |
| 31 | 物件在電腦重啟時被移動到了備份(quarantine on reboot)。 |
| 36 | 誤報(false alarm)。 |
| 38 | 處理程序被終止(terminated)。 |
| 40 | 未偵測到物件(not found)。 |
| 41 | 無法解析威脅(untreatable)。 |
| 42 | 物件被還原(rolled back)。 |
| 43 | 物件因為威脅活動而建立(produced by threat)。 |
| 44 | 物件在電腦重啟時被還原(roll back on reboot)。 |
| 0xffffffff | 物件未處理(discarded)。 |

| 威脅危險級別 | |
|---|---|
| 0 | 未知 |
| 1 | 高 |
| 2 | 中度掃描 |
| 4 | 低 |
| 8 | 資訊（小於*低*） |

# UpdateDefinitions。更新資料庫和程式模組

執行"*資料庫和應用程式模組更新*"工作Kaspersky Endpoint Security 使用預設來源：卡巴斯基更新伺服器。

若要執行工作，管理員必須在政策中允許使用本機工作。

若要執行命令，請轉到 Kaspersky Endpoint Security 可執行檔所在的資料夾。

如果應用程式在 Light Agent 模式下安裝則不可執行此命令。

指令語法

```
kescli --opswat UpdateDefinitions
```

您可以使用 `GetDefinitionsetState` 指令檢視目前病毒防護資料庫的發佈日期和時間。

## GetDefinitionState。確定資料庫的上次更新日期和時間

顯示有關被使用的病毒防護資料庫的上次更新日期和時間的資訊。

若要執行命令，請轉到 Kaspersky Endpoint Security 可執行檔所在的資料夾。

指令語法

```
kescli --opswat GetDefinitionState
```

## EnableRTP。啟用防護

在電腦上啟用 Kaspersky Endpoint Security 防護元件：檔案威脅防護，網頁威脅防護，郵件威脅防護，網路威脅防護，主機侵入防護。

若要啟用防護元件，管理員必須確保相關政策設定可以修改（ 屬性開啟）。

若要執行命令，請轉到 Kaspersky Endpoint Security 可執行檔所在的資料夾。

指令語法

```
kescli --opswat EnableRTP
```

因此，即使您使用密碼防護禁止修改應用程式設定，防護元件也會被啟用。

您可以使用 `GetRealTimeProtectionState` 指令檢查檔案威脅防護的操作狀態。

## GetRealTimeProtectionState。“檔案威脅防護”狀態

顯示有關“檔案威脅防護”元件的狀態的資訊：

- `1` – 元件已啟用。
- `0` – 元件已停用。

若要執行命令，請轉到 Kaspersky Endpoint Security 可執行檔所在的資料夾。

指令語法

```
kescli --opswat GetRealTimeProtectionState
```

## GetEncryptionState。瓷碟加密狀態

顯示有關瓷碟加密狀態的資訊：

- `1` 意味著瓷碟受卡巴斯基或 BitLocker 瓷碟加密技術防護。
- `0` 意味著瓷碟未加密。

若要執行命令，請轉到 Kaspersky Endpoint Security 可執行檔所在的資料夾。

指令語法

```
kescli --opswat GetEncryptionState
```

## Version。識別應用程式版本

顯示 Kaspersky Endpoint Security for Windows 的版本。

若要執行命令，請轉到 Kaspersky Endpoint Security 可執行檔所在的資料夾。

指令語法

```
kescli --Version
```

您也可以使用縮寫指令 `-v`。

# Detection and Response 管理指令

您可以使用命令列管理 Detection and Response 解決方案的內建功能（例如，Kaspersky Sandbox 或者 Kaspersky Endpoint Detection and Response Optimum）。如果無法使用卡巴斯基安全管理中心主控台進行管理，您可以管理 Detection and Response 解決方案。可以執行 `HELP` 指令來檢視用於管理應用程式的指令清單。要閱讀特定指令的語法，請輸入 `HELP <command>`。

*使用命令列管理 Detection and Response 解決方案的內建功能：*

1. 以管理員身分執行命令列解譯器 (cmd.exe)。
2. 轉到 Kaspersky Endpoint Security 可執行檔所在資料夾。

3. 使用以下模板來執行命令：

```
avp.com <command> [options]
```

結果，Kaspersky Endpoint Security 將執行該指令。

# SANDBOX。管理 Sandbox

用來管理 Sandbox 元件的指令：

- 啟用或者停用 Sandbox 元件。

  Sandbox 元件提供與 Kaspersky Sandbox 解決方案和 KATA Sandbox 元件的交互，是 Kaspersky Anti Targeted Attack Platform 的一部分。

- 配置 Kaspersky Sandbox 元件：

  - 將電腦連線到 Sandbox 伺服器。

    伺服器使用部署的 Microsoft Windows 作業系統的虛擬影像來執行需要掃描的物件。您可以輸入一個 IP 位址（IPv4 或者 IPv6）或者完全限定網域名稱。有關部署虛擬鏡像和配置 Sandbox 伺服器的詳細資訊，請參閱 Kaspersky Sandbox 說明 和 Kaspersky Anti Targeted Attack Platform 說明。

  - 配置伺服器的連線逾時。

    沙盒伺服器（用於 Kaspersky Sandbox）或中央節點伺服器（用於 KATA）的連線逾時。配置的逾時經過後，Kaspersky Endpoint Security 會傳送請求給下一個伺服器。如果您的連線速度慢或者連線不穩定，您可以增加伺服器的連線逾時。建議的請求逾時為 0.5 秒鐘或更短。

  - 在電腦和伺服器之間配置受信任連線。

    要設定與沙盒伺服器（對於 Kaspersky Sandbox）或中央節點伺服器（對於 KATA）的可信任連線，您必須準備 TLS 憑證。然後，您必須使用政策將憑證新增至電腦。您還需要將憑證新增至 Sandbox 伺服器（對於 Kaspersky Sandbox）或 Central Node 伺服器（用於 KATA）。

- 顯示元件的目前設定。

若要執行命令，請轉到 Kaspersky Endpoint Security 可執行檔所在的資料夾。您也可以將可執行檔路徑新增至 %PATH% 系統變數並執行命令，而無需導覽至應用程式資料夾。

指令語法

```
avp.com stop sandbox [/login=<user name> /password=<password>]
avp.com start sandbox
avp.com sandbox /set [--tls=yes|no] [--servers=<server address>:<port>] [--timeout=<Sandbox server connection
timeout (ms)>] [--pinned-certificate=<path to the TLS certificate>][/login=<user name> /password=<password>][--
client-certificate=<path to the PFX archive>]
avp.com sandbox /show
```

| 操作 | |
|---|---|
| stop | 停用 Sandbox 元件。 |
| start | 啟用 Sandbox 元件。 |

| | |
|---|---|
| set | 配置 Sandbox 元件。您可以配置以下設定：<br>• 使用受信任連線（--tls ）<br>• 新增 TLS 憑證（ --pinned-certificate ）<br>• 設定伺服器連線逾時（--timeout ）<br>• 新增 Sandbox 伺服器（ --servers ）<br>• 新增加密容器（ --client-certificate ） |
| show | 顯示元件的目前設定。您會獲得以下回應：<br>sandbox.timeout=<Sandbox server connection timeout (ms)><br>sandbox.tls=<trusted connection status><br>sandbox.servers=<list of Sandbox servers> |

| **身分驗證** | |
|---|---|
| /login=<user name> /password=<password> | 具有所需"密碼防護"權限的使用者帳戶憑據。 |

```
範例:
avp.com start sandbox
avp.com sandbox /set --tls=yes --pinned-certificate="C:\Users\Admin\certificate.pem"
avp.com sandbox /set --servers=10.10.111.0:147
```

# PREVENTION。管理執行防護

停用執行防護元件或顯示該元件的目前設定，包括執行防護規則清單。

若要執行命令，請轉到 Kaspersky Endpoint Security 可執行檔所在的資料夾。您也可以將可執行檔路徑新增至 %PATH% 系統變數並執行命令，而無需導覽至應用程式資料夾。

指令語法

```
avp.com prevention disable
avp.com prevention /show
```

執行"`prevention /show`"指令時，您將得到以下回應：

```
prevention.enable=true|false

prevention.mode=audit|prevent

prevention.rules

id: <rule ID>
target: script|process|document
md5: <MD5 hash of the file>
sha256: <SHA256 hash of the file>
pattern: <path to the object>
case-sensitive: true|false
```

指令返回值：

- `-1` 意味著指令不受安裝在電腦上的應用程式版本支援。
- `0` 意味著指令已成功執行。
- `1` 意味著強制引數沒有傳遞給指令。

- 2 意味著發生了一般錯誤。
- 4 意味著有語法錯誤。
- 9 – 錯誤操作（例如，嘗試停用元件而元件已停用）。

# ISOLATION。管理網路隔離

停用電腦的網路隔離或者顯示元件的目前設定。元件設定也包含一個新增到排除項目的網路連線清單。

若要執行命令，請轉到 Kaspersky Endpoint Security 可執行檔所在的資料夾。您也可以將可執行檔路徑新增至 %PATH% 系統變數並執行命令，而無需導覽至應用程式資料夾。

指令語法：

```
avp.com isolation /OFF /login=<user name> /password=<password>
avp.com isolation /STAT
```

由於執行`stat`指令，您將受到以下回應：`Network isolation on|off`。

# RESTORE。從隔離區中還原檔案

將檔案從隔離區還原到原始資料夾。*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。隔離檔案以加密狀態儲存，不會威脅裝置安全。Kaspersky Endpoint Security 僅在使用以下 Detection and Response 解決方案時使用隔離：EDR Optimum、EDR Expert、KATA (EDR)、Kaspersky Sandbox。在其他情況下，Kaspersky Endpoint Security 將相關檔案放置在備份中。若要瞭解將隔離作為解決方案的一部分進行管理的詳情，請參見Kaspersky Sandbox 說明、Kaspersky Endpoint Detection and Response Optimum 說明、Kaspersky Endpoint Detection and Response Expert 說明、Kaspersky Anti Targeted Attack Platform 說明。

要執行此指令，必須啟用密碼防護。使用者必須具有**"從備份區還原"**權限。

物件在系統帳戶 (SYSTEM) 下隔離。

從隔離區中還原檔案包含以下特別考量：

- 如果目的地資料夾已被刪除或者使用者沒有此資料夾的存取權限，應用程式將把檔案放置於 "`%DataRoot%\QB\Restored`"資料夾中。然後您必須手動將檔案移動到目的地資料夾。
- 應用程式對被還原檔案名稱的大小寫敏感。如果您在輸入檔案名稱時沒有執行大小寫規則，則應用程式不會還原檔案。
- 如果目的地資料夾已經有同名檔案，則應用程式會取消檔案還原。
- 如果您使用的是 KATA (EDR) 解決方案，應用程式會在還原檔案後將檔案副本儲存在隔離區中。您可以手動清空隔離區。對於 EDR Optimum 和 EDR Expert 解決方案，應用程式會在還原後刪除檔案。

若要執行命令，請轉到 Kaspersky Endpoint Security 可執行檔所在的資料夾。您也可以將可執行檔路徑新增至 %PATH% 系統變數並執行命令，而無需導覽至應用程式資料夾。

指令語法

```
avp.com RESTORE [/REPLACE] <file name> /login=<user name> /password=<password>
```

| 進階設定 | |
|---|---|
| /REPLACE | 覆蓋現有檔案。 |
| <file name> | 要還原的檔案的名稱。 |

| 身分驗證 | |
|---|---|
| /login=<user name> /password=<password> | 具有所需"密碼防護"權限的使用者帳戶憑據。 |

範例:
```
avp.com RESTORE /REPLACE true_file.txt /login=KLAdmin /password=samplePassword
```

指令返回值：

- -1 意味著指令不受安裝在電腦上的應用程式版本支援。
- 0 意味著指令已成功執行。
- 1 意味著強制引數沒有傳遞給指令。
- 2 意味著發生了一般錯誤。
- 4 意味著有語法錯誤。

# IOCSCAN。掃描查找洩露指示器 (IOC)

執行"*IOC 掃描*"工作*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，許多登入系統的不成功嘗試可以構成一個洩露指示器。"*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。

若要執行命令，請轉到 Kaspersky Endpoint Security 可執行檔所在的資料夾。您也可以將可執行檔路徑新增至 %PATH% 系統變數並執行命令，而無需導覽至應用程式資料夾。

在與 IOC 規則中所述的入侵指標進行 128 次配對後，IOC 掃描將中止。有必要限制 IOC 掃描工作報告中的項目數量，以便於分析並防止由於不精確制定的入侵指標而產生大量匹配導致報告溢出。

指令語法

```
avp.com IOCSCAN <full path to the IOC file>|/path=<path to the IOC files folder> [/process=on|off] [/hint=<full
path to executable file of a process|full file path>] [/registry=on|off] [/dnsentry=on|off] [/arpentry=on|off]
[/ports=on|off] [/services=on|off] [/system=on|off] [/users=on|off] [/volumes=on|off] [/eventlog=on|off]
[/datetime=<event publication date>] [/channels=<list of channels>] [/files=on|off] [/drives=
<all|system|critical|custom>] [/excludes=<list of exclusions>][/scope=<list of folders to scan>]
```

| IOC 檔案 | |
|---|---|
| `<full path to the IOC file>` | 您想要用於掃描的 IOC 檔案的完整路徑。您可以指定多個 IOC 檔案，之間由空格分開。輸入 IOC 檔案的完整路徑時不得有 `/path` 引數。<br>例如，`C:\Users\Admin\Desktop\IOC\file1.ioc` |
| `/path=<path to the folder with IOC files>` | 您想要用於掃描的包含 IOC 檔案的資料夾路徑。*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。<br>例如，`C:\Users\Admin\Desktop\IOC` |

| 用於 IOC 掃描的資料類型 | |
|---|---|
| `/process=on\|off` | 執行 IOC 掃描時分析處理程序資料（ProcessItem 字詞）。<br>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）。<br>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=<full path to the executable file of the process\|full path to the file>` | 執行 IOC 掃描時分析檔案資料（(ProcessItem 和 FileItem 字詞）。<br>您可以採用以下方式之一選擇檔案：<br>• `<full path to the executable file of the process>` – ProcessItem 字詞；<br>• `<full path to the file>` – FileItem 字詞。 |
| `/registry=on\|off` | 執行 IOC 掃描時分析 Windows 登錄檔資料（RegistryItem 字詞）。<br>如果引數值為 `off`，則 Kaspersky Endpoint Security 不掃描 Windows 登錄檔。如果 IOC 檔案包含 RegistryItem IOC 文件字詞，則他們會被忽略（偵測為不匹配）。<br>如果未指定引數，則僅當 RegistryItem IOC 文件在供掃描的 IOC 檔案中得到說明時，Kaspersky Endpoint Security 才分析 Windows 登錄檔資料。<br>對於 RegistryItem 資料類型，Kaspersky Endpoint Security 會掃描一個登錄機碼集合。 |
| `/dnsentry=on\|off` | 執行 IOC 掃描時分析本機 DNS 快取中的記錄相關資料（DnsEntryItem 字詞）。<br>如果引數值為 `off`，則 Kaspersky Endpoint Security 不掃描本機 DNS 快取。如果 IOC 檔案包含 DnsEntryItem IOC 文件字詞，則他們會被忽略（偵測為不匹配）。<br>如果未指定引數，則僅當 DnsEntryItem IOC 文件在供掃描的 IOC 檔案中得到說明時，Kaspersky Endpoint Security 才分析本機 DNS 快取。 |
| `/arpentry=on\|off` | 執行 IOC 掃描時分析本機 ARP 表格中的記錄相關資料（ArpEntryItem 字詞）。<br>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）。<br>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。 |
| `/ports=on\|off` | 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）。<br>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）。<br>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。 |
| `/services=on\|off` | 執行 IOC 掃描時分析安裝在裝置上的服務相關資料（ServiceItem 字詞）。<br>如果引數值為 `off`，則 Kaspersky Endpoint Security 不掃描安裝在裝置上的服務相關資料。如果 IOC 檔案包含 ServiceItem IOC 文件字詞，則他們會被忽略（偵測為不匹配）。<br>如果未指定引數，則僅當 ServiceItem IOC 文件在供掃描的 IOC 檔案中得到說明時，Kaspersky Endpoint Security 才分析服務資料。 |
| `/system=on\|off` | 執行 IOC 掃描時分析環境資料（SystemInfoItem 字詞）。<br>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）。<br>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。 |

| | |
|---|---|
| `/users=on\|off` | 執行 IOC 掃描時分析使用者相關資料（UserItem 字詞）。<br><br>如果引數值為 `off`，則 Kaspersky Endpoint Security 不分析在系統中建立的使用者相關資料。如果 IOC 檔案包含 UserItem IOC 文件字詞，則他們會被忽略（偵測為不匹配）。<br><br>如果未指定引數，則僅當 UserItem IOC 文件在供掃描的 IOC 檔案中得到說明時，Kaspersky Endpoint Security 才分析在系統中建立的使用者相關資料。 |
| `/volumes=on\|off` | 執行 IOC 掃描時分析磁碟區相關資料（VolumeItem 字詞）。<br>如果引數值為 `off`，則 Kaspersky Endpoint Security 不掃描裝置上的磁碟區相關資料。如果 IOC 檔案包含 VolumeItem IOC 文件字詞，則他們會被忽略（偵測為不匹配）。<br>如果未指定引數，則僅當 VolumeItem IOC 文件在供掃描的 IOC 檔案中得到說明時，Kaspersky Endpoint Security 才分析磁碟區資料。 |
| `/eventlog=on\|off` | 執行 IOC 掃描時分析 Windows 事件日誌中的記錄相關資料（EventLogItem 字詞）。<br>如果引數值為 `off`，則 Kaspersky Endpoint Security 不掃描 Windows 事件日誌中的記錄。如果 IOC 檔案包含 EventLogItem IOC 文件字詞，則他們會被忽略（偵測為不匹配）。<br>如果未指定引數，則僅當 EventLogItem IOC 文件在供掃描的 IOC 檔案中得到說明時，Kaspersky Endpoint Security 才分析 Windows 事件日誌。 |
| `/datetime=<event publication date>` | 當確定相應 IOC 文件的 IOC 掃描範圍時，請考慮事件在 Windows 事件日誌中發佈的日期。<br>當執行 IOC 掃描時，Kaspersky Endpoint Security 會掃描從指定時間和日期到執行工作時這段期間內發佈的 Windows 事件日誌。<br>Kaspersky Endpoint Security 允許將事件發佈日期指定為引數值。僅對指定日期後和執行掃描前在 Windows 事件日誌中發佈的事件進行掃描。<br>如果未指定引數，Kaspersky Endpoint Security 會掃描具有任何發佈日期的事件。`TaskSettings::BaseSettings::EventLogItem::datetime` 設定不可編輯。<br>設定只有當 EventLogItem IOC 文件在供掃描的 IOC 檔案中得到說明時才使用。 |
| `/channel=<list of channels>` | 您想要為其進行 IOC 掃描的通道清單 (log) 名稱。<br>如果指定了引數，Kaspersky Endpoint Security 會掃描發佈在指定日誌中的記錄。IOC 文件必須說明 EventLogItem 字詞。<br>日誌名稱被根據日誌內容（Full Name參數）或者事件內容（事件的 xml 架構中的 `<Channel></Channel>` 參數）中指定的日誌名稱（通道）指定為字串。您可以指定多個通道，之間由空格分開。<br>如果未指定引數，則 Kaspersky Endpoint Security 會掃描通道 `Application`、`System`、`Security` 的記錄。 |
| `/files=on\|off` | 執行 IOC 掃描時分析檔案資料（FileItem 字詞）。<br>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）。<br>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=<all\|system\|critical\|custom>` | 設定分析 FileItem IOC 文件的資料時的 IOC 掃描範圍。<br>您可以為掃描範圍設定以下值：<br>• `<all>`，對於所有可用的檔案範圍。<br>• `<system>`，對於安裝了作業系統的資料夾中的檔案。<br>• `<critical>`，對於使用者和系統資料夾中的臨時檔案。<br>• `<custom>`，對於使用者定義的範圍中的檔案（`/scope=<list of folders to scan>`）。<br>如果未指定引數，則為關鍵領域進行掃描。 |
| `/excludes=<list of exclusions>` | 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=<list of folders to scan>` | 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。 |
| `/retro /<number of days>` | *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。此模式旨在偵測電腦網路活動資料中的入侵指標。<br><br>您可以設定 1 到 14 天的時間段。預設情況下，該應用程式會掃描入侵指標一天。 |
| `/network=on\|off` | 網路資料分析（NetworkItem）。 |
| `/url=on\|off` | 瀏覽器日誌資料分析（UrlHistoryItem）。<br>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）。 |
| `/email` | 郵件物件分析（EmailItem）。 |
| `/route` | 路由和轉發表分析（RouteEntryItem）。 |

指令返回值：

- `-1` 意味著指令不受安裝在電腦上的應用程式版本支援。
- `0` 意味著指令已成功執行。
- `1` 意味著強制引數沒有傳遞給指令。
- `2` 意味著發生了一般錯誤。
- `4` 意味著有語法錯誤。

如果指令得到成功執行（返回值`0`）且順便偵測到了洩露指示器，Kaspersky Endpoint Security 會將以下工作結果資訊輸出到指令行：

| | |
|---|---|
| `Uuid` | 來自 IOC 檔案結構標頭的 IOC 檔案 ID（`<ioc id="">` 標籤） |
| `Name` | 來自 IOC 檔案結構標頭的 IOC 檔案說明（`<description></description>` 標籤） |
| `Matched Indicator Items` | 所有匹配指示器的 ID 清單。 |
| `Matched objects` | 對其具有匹配的每個 IOC 文件的資料。 |

# MDRLICENSE.MDR 啟動

新增 BLOB 設定檔以啟動 Managed Detection and Response。BLOB 檔案包含用戶端 ID 以及有關卡巴斯基 Managed Detection and Response 產品許可的資訊。BLOB 檔案位於 MDR 設定檔的 ZIP 存檔中。您可以在 Kaspersky Managed Detection and Response 主控台中獲取 ZIP 存檔。有關 BLOB 檔案的詳細資訊，請參閱 Kaspersky Managed Detection and Response 說明。

使用 BLOB 檔案執行操作需要管理員權限。政策中的 Managed Detection and Response 設定也必須可用於編輯（ ）。

若要執行命令，請轉到 Kaspersky Endpoint Security 可執行檔所在的資料夾。您也可以將可執行檔路徑新增至 %PATH% 系統變數並執行命令，而無需導覽至應用程式資料夾。

指令語法

```
avp.com MDRLICENSE <operation> [/login=<user name> /password=<password>]
```

| **操作** | |
|---|---|
| `/ADD <file name>` | 套用 BLOB 設定檔與 Kaspersky Managed Detection and Response（P7 檔案格式）整合。您只能套用一個 BLOB 檔案。如果已將 BLOB 檔案新增到電腦，則該檔案將被替換。 |
| `/DEL` | 刪除 BLOB 設定檔。 |

| **身分驗證** | |
|---|---|
| `/login=<user name> /password=<password>` | 具有所需"密碼防護"權限的使用者帳戶憑據。 |

範例：

```
avp.com MDRLICENSE /ADD file.key
avp.com MDRLICENSE /DEL /login=KLAdmin /password=samplePassword
```

# EDRKATA。與 EDR (KATA) 進行整合

用於管理 Detection and Response 元件 (KATA) 的命令：

- 啟用或停用 EDR (KATA) 元件。

  EDR 元件 (KATA) 提供與 Kaspersky Anti Targeted Attack Platform 解決方案的互操作性。

- 配置與 Kaspersky Anti Targeted Attack Platform 伺服器的連線。

- 顯示元件的目前設定。

若要執行命令，請轉到 Kaspersky Endpoint Security 可執行檔所在的資料夾。您也可以將可執行檔路徑新增至 %PATH% 系統變數並執行命令，而無需導覽至應用程式資料夾。

指令語法

```
avp.com START EDRKATA
avp.com STOP EDRKATA
avp.com edrkata /set /servers=<server address>:<port> /server-certificate=<path to the TLS certificate> [/timeout=
<Central Node server connection timeout (s)>] [/sync-period=<Central Node server synchronization period (min)>]
avp.com edrkata /show
```

| 操作 | |
|---|---|
| stop | 停用 EDR (KATA) 元件。 |
| start | 啟用 EDR (KATA) 元件。 |
| set | 配置 EDR (KATA) 元件。您可以配置以下設定：<br>• 新增中央節點伺服器（ servers=<server address>:<port> ）<br>• 新增 TLS 憑證（ server-certificate=<path to the TLS certificate> ）<br>• 設定中央節點伺服器連線逾時 (/timeout=<Central Node server connection timeout (s)> )<br>• 設定與中央節點伺服器同步的周期（ /sync-period=<Central Node server synchronization period (min)> ） |
| show | 顯示元件的目前設定。 |

# KUMA。與 KUMA 整合

用於管理內建 KUMA 代理的指令：

- 啟用或停用 KUMA 整合。

  內建的 KUMA 代理可提供與 Kaspersky Unified Monitoring and Analysis Platform 解決方案的互通性。

- 配置與 Kaspersky Unified Monitoring and Analysis Platform 伺服器的連線。

- 顯示元件的目前設定。

若要執行命令，請轉到 Kaspersky Endpoint Security 可執行檔所在的資料夾。您也可以將可執行檔路徑新增至 %PATH% 系統變數並執行命令，而無需導覽至應用程式資料夾。

指令語法

```
avp.com START KUMA
avp.com STOP KUMA [/login=<使用者名稱> /password=<密碼>]
avp.com KUMA /SET /servers=<server address>:<port> /server-certificate=<path to the TLS certificate> [/timeout=
```

```
<KUMA server connection timeout (s)>] [/client-certificate=<加密容器路徑> ] [ /client-certificate-password=<密碼> ]
[/maximum-data-transfer-time= <事件傳輸延遲最長時間（秒）>]
avp.com KUMA /SHOW
```

| 操作 | |
|---|---|
| stop | 禁用 KUMA 整合。 |
| start | 啟用 KUMA 整合。 |
| set | 配置內建的 KUMA 代理。您可以配置以下設定：<br>• 新增 KUMA 伺服器（/servers=<protocol>://<server address>:<port>）<br>應用程式支援以下伺服器連接協定：tcp、udp、http、https。<br>• 新增 TLS 憑證（/server-certificate=<path to the TLS certificate>）<br>• 設定伺服器連線逾時（/timeout=<KUMA server connection timeout (s)>）<br>• 新增加密容器（/client-certificate=<path to the crypto-container> /client-certificate-password=<password>）<br>• 配置事件傳輸延遲（/maximum-data-transfer-time=<maximum events transmission delay (sec)）|
| show | 顯示元件的目前設定。 |

| 身分驗證 | |
|---|---|
| /login=<user name> /password=<password> | 具有所需"密碼防護"權限的使用者帳戶憑據。 |

範例：

```
avp.com start kuma
avp.com KUMA /SET /servers=https://127.0.0.1:8080 /server-certificate=c:\\folder\\certificate.cer /timeout=15
/login=login /password=password
avp.com KUMA /SET /servers=https://kuma.server.com:8000 /server-certificate=c:\\folder\\certificate.cer
/login=login /password=password
```

# YARA。執行 YARA 掃描

執行 *執行 YARA 掃描* 工作。應用程式使用 YARA 規則資料庫來掃描檔案和物件，以查找針對企業 IT 基礎設施的針對性攻擊的指標。*YARA 規則* 是針對企業 IT 基礎設施的定向攻擊和入侵的特徵描述，Kaspersky Endpoint Security 使用這些特徵來掃描物件。

要執行 YARA 掃描，您必須準備描述規則的 YARA 檔案。在建立 YARA 檔案時，請考慮以下要求：

- Kaspersky Endpoint Security 支援副檔名為 YARA 和 YAR 的檔案，其遵循用於描述入侵指標的 YARA 4.2.3 開放標準。
- 只能為工作指定具有 YARA 規則的檔案。*執行 YARA 掃描* 工作不支援其他規則類型。
- 如果您新增了 Kaspersky Endpoint Security 不支援的 YARA 檔案，或者規則包含語法錯誤，則工作將被中止並顯示相應的錯誤訊息。
- 在單個工作中使用的所有 IOC 檔案的識別符必須為唯一。如果有識別符一樣的 YARA 檔案，它可能會影響工作執行結果。
- 在與 YARA 規則中所述的指標進行 128 次配對後，YARA 掃描將中止。有必要限制 YARA 掃描報告中的項目數量，以便於分析並防止由於不精確制定的 YARA 規則而產生大量匹配並導致報告溢出。

卡巴斯基建議為每個 YARA 檔案建立一條規則。這將使掃描結果更具可讀性。

YARA 掃描可能會花很長時間。根據磁碟機大小、工作設定和磁碟上的物件數量，YARA 掃描可持續幾分鐘到幾小時。應用程式不顯示進度指示器。無法停止或取消 YARA 掃描。建議您等到 YARA 掃描結果可用。

指令語法

```
avp.com YARA <full path to the YARA file>|/path=<path to the folder with YARA files> [<advanced settings>]
```

| **YARA 檔案** | |
|---|---|
| `<full path to the YARA file>` | 您想要用於掃描的 YARA 檔案的完整路徑。您可以指定多個 YARA 檔案路徑，之間由空格分開。<br>如果未指定 `/path=<path to the folder with YARA files>` 值，則其是必需參數。<br>範例:<br>`C:\Users\Admin\Desktop\YARA\file1.yar`<br>`C:\Users\Admin\Desktop\YARA\file2.yar` |
| `/path=<path to the folder with YARA files>` | 您想要用於掃描的包含 YARA 檔案的資料夾完整路徑。<br>如果未指定 `<full path to the YARA file>` 值，則其是必需參數。<br>範例:<br>`/path=C:\Users\Admin\Desktop\YARA` |

| **進階設定** | |
|---|---|
| `/fastScan=<on\|off>` | 快速 YARA 掃描。對於每個物件，應用程式都會記錄一次偵測到的指標。應用程式還隱藏日誌中檢測到的指標的重複項。快速 YARA 掃描可以更快地掃描大檔案。<br>如果未指定此設定，應用程式將執行標準 YARA 掃描。在這種模式下，應用程式會記錄偵測到的指標的重複項。 |
| `/maxRules=<maximum number of scan rules>` | 獨特觸發規則的次數限制，當達到時會使應用程式停止 YARA 掃描。<br>如果未指定此設定的值，或者 `0` 被指定，應用程式將無限制執行 YARA 掃描。 |
| `/timeOut=<stop scan after the specified time in seconds>` | YARA 掃描持續時間限制（秒鐘）。當此時間用完時，應用程式將停止 YARA 掃描。<br>如果未指定此設定的值，或者 `0` 被指定，應用程式將無限制執行 YARA 掃描。 |
| `/recursive=<on\|off>` | 此參數會啟動對 `/scanFolders` 自訂掃描內子資料夾的遞歸掃描。 |
| `/scanFolders=<list of folders to be scanned>` | 此參數會啟動指定資料夾清單中的檔案進行 YARA 掃描。您可以指定多個值，之間由空格分開。Kaspersky Endpoint Security 在輸入資料夾路徑遮罩時支援 `*` 和 `?` 字元。<br>如果未指定此設定，應用程式將對除網路共用、雲端磁碟機和可移動媒體之外的所有本機磁碟執行 YARA 掃描。 |
| `/scanMemory=<on\|off>` | 掃描所有正在執行的處理程序的記憶體。 |
| `/scanProcess=<process name>` | 僅為所列處理程序掃描記憶體。指定處理程序可執行檔的完整路徑，路徑之間以空格分隔。您也可以使用 `*` 和 `?` 字元輸入遮罩。 |
| `/maxSize=<file size in bytes>` | YARA 掃描的檔案大小限制。應用程式會跳過較大的檔案。 |
| `/includes=<list of objects to be scanned>>` | 編輯掃描範圍。您可以指定多個值，之間由空格分開。以下值可用：<br>• 檔案名稱<br>• 檔案副檔名<br>掃描範圍必須用 `/scanFolders` 參數指定。<br>範例:<br>`/scanFolders C:\*.* /includes=*.exe *.dll` – 應用程式掃描 C 碟上所有副檔名為 EXE 和 DLL 的檔案。 |

| | |
|---|---|
| `/excludes=<list of objects to be scanned>` | 從 YARA 掃描中排除檔案。您可以指定多個值，之間由空格分開。以下值可用：<br>• 檔案路徑<br>• 檔案路徑遮罩<br>排除項目必須用 `/scanFolders` 參數指定。<br>範例:<br>`/scanFolders C:\*.* /excludes readme.txt C:\trusted\*.* *.xml` – 應用程式略過 readme.txt 檔案，來自 C:\trusted 資料夾的所有檔案以及磁碟 C 根資料夾中所有以 xml 為副檔名的檔案。 |
| `/scanAutoruns=<on\|off>` | 自動執行點物件的 YARA 掃描。 |
| `/excludeAutoruns=<list of autorun point areas to skip>` | 從掃描範圍內排除自動執行點物件。指定處理程序可執行檔的完整路徑，路徑之間以空格分隔。您也可以使用 `*` 和 `?` 字元輸入遮罩。 |
| `/logFolder=<path to the folder for saving the scan results in a TXT file>` | 如果指定資料夾路徑，應用程式會將掃描結果儲存到指定路徑下的名為 yara_<computer name>_<scan completion time>.txt 的檔案中。<br>如果指定特定 TXT 檔案的路徑，應用程式會將掃描結果儲存到該檔案中。<br>例如，`/logFolder=C:\test` 或 `/logFolder=C:\test\abc.txt`。<br>無論是否指定 `/logFolder` 選項，掃描結果都會被輸出到命令列。 |

指令返回值：

- `-1` 意味著指令不受安裝在電腦上的應用程式版本支援。
- `0` – 指令成功完成。
- `1` 意味著強制引數沒有傳遞給指令。
- `2` 意味著發生了一般錯誤。
- `4` 意味著有語法錯誤。
- `5`: 無法找到參數中指定的一個或者多個 YARA 規則檔案。

如果指令得到成功執行（返回值`0`）且順便偵測到了洩露指示器，Kaspersky Endpoint Security 會將以下工作結果資訊輸出到指令行：

| | |
|---|---|
| `Started at <time>`<br>`Finished at <time>` | 掃描的開始時間和完成時間。 |
| `Host name: <computer name>` | 在上面偵測到該物件的電腦名稱。 |
| `Result: <error>` | 執行工作時發生的錯誤的錯誤代碼。如果沒有錯誤，應用程式將輸出 `0x00000000`。 |
| `Comment: <comment text>` | 執行工作時發生的錯誤的錯誤描述。例如，`Operation timeout`。 |
| `Object Name:` 或者 `Process:`（掃描處理程序記憶體時） | 在上面觸發了 YARA 規則的物件或處理程序的名稱。 |
| `Md5: <md5 hash>`<br>`Sha256: <sha256 hash>` | 在上面觸發了 YARA 規則的物件的雜湊。 |
| `Rule Name` | 觸發的 YARA 規則的名稱。 |
| `Meta:`<br>`Author: <author>`<br>`Date: <date>`<br>`Description: <description>` | YARA 規則中指定的中繼資料。 |
| `Detects:`<br>`Offset : String name : String data`<br>`<offset> : <string name> : <string data>` | 在物件中找到的符合 YARA 規則條件的項目：<br>• 處理程序記憶體或檔案中偵測到匹配項的偏移量（`Offset`）。<br>• YARA 規則中匹配字串的名稱（`String name`）。<br>• 處理程序記憶體或檔案中的匹配字串（`String data`）。 |

# 遙測篩選器。篩選要傳送到 KUMA 的事件

為了提高效能並最佳化到 KUMA 伺服器的資料傳輸，您可以從遙測中手動新增或排除個別事件。例如，您可以排除 Sysmon 事件。

您可以從命令列將排除項目清單匯出到 JSON 檔案。

如果該命令僅包含要將設定匯出到的檔案的名稱，則應用程式將如下放置該檔案：

- 如果 avp.com 的路徑新增至 %PATH% 系統變數中，應用程式會將檔案放置在 `C:\Windows\SysWOW64` 資料夾中。
- 如果從應用程式安裝資料夾執行命令，匯出將失敗，因為應用程式的自我防護功能會封鎖在應用程式資料夾中建立新檔案。若要將應用程式設定匯出到檔案，請輸入檔案路徑。

若要執行命令，請轉到 Kaspersky Endpoint Security 可執行檔所在的資料夾。您也可以將可執行檔路徑新增至 %PATH% 系統變數並執行命令，而無需導覽至應用程式資料夾。

指令語法

```
avp.com TELEMETRYFILTERS /export <file name>
avp.com TELEMETRYFILTERS /import <file name>
```

| 操作 | |
|---|---|
| `export` | 匯出要傳送到 KUMA 的事件篩選器。 |
| `import` | 匯入要傳送到 KUMA 的事件篩選器。如果電腦上已存在事件篩選規則，Kaspersky Endpoint Security 會在匯入時將其替換。 |

| 用於匯出或匯入的檔案 | |
|---|---|
| `<file name>` | 包含要傳送到 KUMA 的事件篩選器之檔案名稱。您也可以輸入檔案路徑。您可以將要傳送到 KUMA 的篩選器匯出到 JSON 檔案。 |

# Light Agent 管理指令

您可以在 Light Agent 中管理應用程式，以在命令列上防護虛擬環境。如果無法使用卡巴斯基安全管理中心主控台進行管理，您可以在 Light Agent 模式下管理應用程式。可以執行 `HELP` 指令來檢視用於管理應用程式的指令清單。要閱讀特定指令的語法，請輸入 `HELP <command>`。

*若要從命令列以 Light Agent 模式管理應用程式：*

1. 以管理員身分執行命令列解譯器 (cmd.exe)。
2. 轉到 Kaspersky Endpoint Security 可執行檔所在資料夾。

3. 使用以下模板來執行命令：

```
avp.com <command> [options]
```

結果，Kaspersky Endpoint Security 將執行該指令。

以 Light Agent 模式安裝的應用程式支援以標準模式安裝的應用程式的幾乎所有 AVP指令。在 Light Agent 模式下，病毒資料庫更新工作和產品授權金鑰管理工作受到限制。

# KSVLAINFO。確定 Light Agent 模式

確定 Light Agent 模式。

若要執行命令，請轉到 Kaspersky Endpoint Security 可執行檔所在的資料夾。您也可以將可執行檔路徑新增至 %PATH% 系統變數並執行命令，而無需導覽至應用程式資料夾。

指令語法

```
avp.com KSVLAINFO
```

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：已啟用或停用。

  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：啟用或停用。

  VDI 防護模式有助於最佳化 Kaspersky Endpoint Security 在非持久虛擬機上的效能。如果啟用 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非持久性虛擬機上。當收到需要重新啟動的更新時，安裝在非持久虛擬機上的 Light Agent 會向卡巴斯基安全管理中心傳送一則訊息，通知其受防護的虛擬機範本需要更新。

- 受防護虛擬機的類型：持久性或非持久性。

- 受防護虛擬機在虛擬基礎結構中的角色：伺服器或工作站。

- 受防護虛擬機的識別符 (UUID)。

# VIISINFO。Light Agent 與 Integration Server 的連線狀態

檢視關於 Light Agent 與 Integration Server 的連線的資訊。

若要執行命令，請轉到 Kaspersky Endpoint Security 可執行檔所在的資料夾。您也可以將可執行檔路徑新增至 %PATH% 系統變數並執行命令，而無需導覽至應用程式資料夾。

指令語法

```
avp.com VIISINFO
```

此命令向主控台輸出以下資訊：

- Light Agent 連線的 Integration Server 的位址和連接埠。
- Integration Server 連線狀態。
- Light Agent 上次連線到 Integration Server 的日期和時間。

# SVMINFO。Light Agent 與 Protection Server 的連線狀態

檢視關於 Light Agent 與 Protection Server 的連線的資訊。

若要執行命令，請轉到 Kaspersky Endpoint Security 可執行檔所在的資料夾。您也可以將可執行檔路徑新增至 %PATH% 系統變數並執行命令，而無需導覽至應用程式資料夾。

指令語法

```
avp.com SVMINFO
```

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 SVM 在虛擬基礎結構中相對於 Light Agent 的位置：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（如果選擇 SVM 位址清單作為 SVM 發現方法）。
- 用於將 Light Agent 連線到 SVM 的標籤。
- SVM 選取演算法：標準或延伸。如果使用延伸 SVM 選取演算法，也會顯示 SVM 在虛擬基礎結構中的路徑類型。
- Light Agent 和 Protection Server 之間的連線的防護狀態。

# 錯誤代碼

透過指令行使用應用程式時，可能會發生錯誤。發生錯誤時，Kaspersky Endpoint Security 會顯示錯誤訊息，例如，“`Error: Cannot start task 'EntAppControl'`”。Kaspersky Endpoint Security 還可以顯示代碼形式的其他資訊，例如，`error=8947906D`（請參見下表）。

錯誤代碼

| 錯誤代碼 | 描述 |
| --- | --- |
| 09479001 | 此金鑰已經在使用中。 |
| 0947901D | 產品授權已到期，資料庫更新無法使用。 |
| 89479002 | 找不到金鑰。 |
| 89479003 | 數位簽章遺失或已損壞。 |
| 89479004 | 資料已損壞。 |

| 錯誤代碼 | 描述 |
| --- | --- |
| 89479005 | 金鑰檔案已損壞。 |
| 89479006 | 產品授權已到期。 |
| 89479007 | 未指定金鑰檔案。 |
| 89479008 | 金鑰檔案無效。 |
| 89479009 | 儲存資料失敗。 |
| 8947900A | 讀取資料失敗。 |
| 8947900B | I/O 錯誤。 |
| 8947900C | 找不到資料庫。 |
| 8947900E | 產品授權庫尚未被載入。 |
| 8947900F | 資料庫已損壞或已經手動更新。 |
| 89479010 | 資料庫損壞。 |
| 89479011 | 無法將無效的金鑰檔案當作備用金鑰。 |
| 89479012 | 系統錯誤。 |
| 89479013 | 金鑰拒絕清單已損壞。 |
| 89479014 | 檔案數位簽章與卡巴斯基的數位簽章不相同。 |
| 89479015 | 無法使用試用版產品授權金鑰做為商業產品授權金鑰。 |
| 89479016 | 使用 Beta 版應用程式需要用於 Beta 測試的產品授權。 |
| 89479017 | 金鑰檔案與此應用程式不相容，無法使用其他應用程式的金鑰檔案啟動 Kaspersky Endpoint Security for Windows，請檢查已安裝的應用程式。 |
| 89479018 | 產品授權金鑰被卡巴斯基封鎖。 |
| 89479019 | 該應用程式已經使用了試用版產品授權。無法再次使用試用版產品授權新增金鑰。 |
| 8947901A | 金鑰檔案已損壞。 |
| 8947901B | 數位簽章已遺失、已損壞或者與卡巴斯基數位簽章不相符。 |
| 8947901C | 如果相應的非正式產品授權已到期，則無法新增金鑰。 |
| 8947901E | 金鑰檔案的建立或使用日期無效。請檢查系統日期。 |
| 8947901F | 無法新增試用版產品授權金鑰:已在在使用其他試用版產品授權金鑰。 |
| 89479020 | 金鑰拒絕清單已損壞或遺失。 |
| 89479021 | 更新敘述遺失或損壞。 |
| 89479022 | 金鑰不適合該應用程式。 |
| 89479023 | 無法將無效的金鑰檔案當作備用金鑰。 |
| 89479025 | 傳送啟動伺服器請求時出現錯誤。可能原因：網際網路連線問題或啟動伺服器臨時故障。請稍候(1-2 小時後)再次嘗試使用啟動碼啟動。如果問題仍然存在，請聯絡您的網路供應商。 |
| 89479026 | 請求含有錯誤的啟動碼。 |
| 89479027 | 無法取得回應狀態。 |
| 89479028 | 儲存暫存檔案時出錯。 |
| 89479029 | 輸入的啟動碼不正確，或電腦上設定的系統日期不正確，請檢查電腦上的系統日期。 |
| 8947902A | 金鑰與此程式不相容，或產品授權已到期 |
| 8947902B | 無法接收金鑰檔案，輸入的啟動碼無效。 |
| 8947902C | 啟動伺服器傳回錯誤 400。 |
| 8947902D | 啟動伺服器傳回錯誤 401。 |
| 8947902E | 啟動伺服器傳回錯誤 403。 |

| 錯誤代碼 | 描述 |
| --- | --- |
| 8947902F | 啟動伺服器上的必需資源不可用。 啟動伺服器回應錯誤代碼 404。 請檢查網際網路連線設定。 |
| 89479030 | 啟動伺服器傳回錯誤 405。 |
| 89479031 | 啟動伺服器傳回錯誤 406。 |
| 89479032 | 需要代理身分驗證。請檢查您的網路設定。 |
| 89479033 | 請求逾時。 |
| 89479034 | 啟動伺服器傳回錯誤 409。 |
| 89479035 | 啟動伺服器上的必需資源不可用。 啟動伺服器回應錯誤代碼 410。 請檢查網際網路連線設定。 |
| 89479036 | 啟動伺服器傳回錯誤 411。 |
| 89479037 | 啟動伺服器傳回錯誤 412。 |
| 89479038 | 啟動伺服器傳回錯誤 413。 |
| 89479039 | 啟動伺服器傳回錯誤 414。 |
| 8947903A | 啟動伺服器傳回錯誤 415。 |
| 8947903C | 伺服器內部錯誤。 |
| 8947903D | 不支援此功能。 |
| 8947903E | 閘道無回應，請檢查您的網路設定 |
| 8947903F | 資源暫時無法使用。 |
| 89479040 | 閘道回應逾時，請檢查您的網路設定。 |
| 89479041 | 伺服器不支援該協定。 |
| 89479043 | 未知的 HTTP 錯誤。 |
| 89479044 | 無法的資源 ID。 |
| 89479046 | 無效的網址。 |
| 89479047 | 目標資料夾無效。 |
| 89479048 | 記憶體分配錯誤。 |
| 89479049 | 將參數轉換為 ANSI 字元(網址、資料夾、代理)時出錯。 |
| 8947904A | 建立工作執行緒時出錯。 |
| 8947904B | 工作執行緒已經執行。 |
| 8947904C | 工作執行緒尚未執行。 |
| 8947904D | 啟動伺服器上未找到金鑰檔案。 |
| 8947904E | 金鑰已被封鎖。 |
| 8947904F | 啟動伺服器內部錯誤。 |
| 89479050 | 在啟動請求中沒有足夠的資料。 |
| 89479053 | 屬於新增的金鑰已經到期。 |
| 89479054 | 電腦上的系統日期設定不正確，請檢查系統日期。 |
| 89479055 | 試用版產品授權已到期。 |
| 89479056 | 程式啟動時間已到期。 |
| 89479057 | 指定啟動碼已超過程式啟動的最大數量。 |
| 89479058 | 啟動過程返回系統錯誤 |
| 89479059 | 無法使用試用版產品授權金鑰做為商業產品授權金鑰。 |
| 8947905C | 需要啟動碼。 |
| 89479062 | 無法連線到啟動伺服器。 |

| 錯誤代碼 | 描述 |
| --- | --- |
| 89479064 | 啟動伺服器不可用。請檢查您的網際網路連線設定並再次嘗試啟動。 |
| 89479065 | 產品授權已到期 |
| 89479066 | 不能使用到期金鑰取代啟動金鑰。 |
| 89479067 | 如果對應的產品授權在啟動的產品授權之前到期，則無法新增備用金鑰。 |
| 89479068 | 更新的訂購金鑰遺失。 |
| 8947906A | 啟動碼無效。 |
| 8947906B | 金鑰已經啟動。 |
| 8947906C | 與啟動金鑰和備用金鑰對應的產品授權類型不比對。 |
| 8947906D | 產品產品授權不支援元件 |
| 8947906E | 無法新增訂購金鑰作為備用金鑰。 |
| 89479213 | 傳輸層一般錯誤 |
| 89479214 | 無法連線啟動伺服器 |
| 89479215 | 無效的網址格式 |
| 89479216 | 無法轉換代理伺服器位址 |
| 89479217 | 未能轉換伺服器位址，請檢查網際網路連線設定 |
| 89479218 | 伺服器嘗試連線失敗 |
| 89479219 | 遠端存取被拒絕 |
| 8947921A | 操作逾時 |
| 8947921B | 傳送 HTTP 請求時出現錯誤 |
| 8947921C | SSL 連線錯誤 |
| 8947921D | 操作被回呼中斷 |
| 8947921E | 重新導向過多 |
| 8947921F | 收件者檢查失敗 |
| 89479220 | 來自伺服器的空回應 |
| 89479221 | 傳送資料時出現錯誤 |
| 89479222 | 接收資料時出現錯誤 |
| 89479223 | SSL 憑證相關問題 |
| 89479224 | SSL 加密相關問題 |
| 89479225 | SSL 憑證中心相關問題 |
| 89479226 | 無效的網路封包內容 |
| 89479227 | 帳戶存取被拒絕 |
| 89479228 | 無效的 SSL 憑證檔案 |
| 89479229 | 無法結束 SSL 連線 |
| 8947922A | 循環錯誤 |
| 8947922B | 含有註銷且無效憑證的檔案 |
| 8947922C | SSL 憑證請求錯誤 |
| 89479401 | 未知的伺服器錯誤 |
| 89479402 | 伺服器內部錯誤 |
| 89479403 | 所輸入的啟動碼沒有可用的金鑰 |
| 89479404 | 啟動金鑰已被封鎖 |

| 錯誤代碼 | 描述 |
| --- | --- |
| 89479405 | 請求啟動所需的參數遺失 |
| 89479406 | 無效的用戶端號碼或密碼 |
| 89479407 | 啟動碼無效。 |
| 89479408 | 啟動碼與此應用程式不相容，無法使用其他應用程式的啟動碼啟動 Kaspersky Endpoint Security for Windows，請檢查已安裝的應用程式。 |
| 89479409 | 需要啟動碼 |
| 8947940B | 啟動日期已到期 |
| 8947940C | 該啟動碼的啟動次數已超過限制 |
| 8947940D | 請求 ID 的格式無效 |
| 8947940E | 啟動碼已在使用中 |
| 8947940F | 無法續約啟動碼 |
| 89479410 | 啟動碼對該國家無效。 |
| 89479411 | 該啟動碼不適用於該此程式版本。 |
| 89479412 | 此啟動碼設計用於目前程式的新版本，請取得其他啟動碼以啟動目前安裝版本程式。 |
| 89479413 | 啟動伺服器回傳錯誤代碼 643 |
| 89479414 | 啟動伺服器回傳錯誤代碼 644 |
| 89479415 | 啟動伺服器回傳錯誤代碼 645 |
| 89479416 | 啟動伺服器回傳錯誤代碼 646 |
| 89479417 | 需要啟動伺服器版本 1.0 |
| 89479418 | 錯誤的啟動碼格式 |
| 89479419 | 電腦時間沒有與啟動伺服器時間同步 |
| 8947941A | 錯誤的程式版本 |
| 8947941B | 訂購服務已到期 |
| 8947941C | 超出啟動數量 |
| 8947941D | 無效的 ticket 簽章 |
| 8947941E | 需要額外的資料 |
| 8947941F | 資料驗證失敗 |
| 89479420 | 訂購未啟動 |
| 89479421 | 啟動伺服器正在維護中 |
| 89479501 | 意外錯誤 |
| 89479502 | 傳輸的參數無效，範例啟動伺服器位址清單是空的 |
| 89479503 | 無效的啟動碼(雜湊值無效) |
| 89479504 | 使用者 ID 無效 |
| 89479505 | 使用者密碼無效 |
| 89479506 | 來自啟動伺服器的無效回應 |
| 89479507 | 啟動請求已中斷 |
| 89479509 | 啟動伺服器傳回了空的轉發清單 |

# 附錄。應用程式設定檔

*設定檔*是 Kaspersky Endpoint Security 元件、工作或功能。設定檔用於從命令列管理應用程式。您可以使用設定檔執行 `START`、`STOP`、`STATUS`、`STATISTICS`和`EXPORT`指令。使用設定檔，您可以配置應用程式設定（例如，`STOP DeviceControl`）或執行工作（例如，`START Scan_My_Computer`）。

以下設定檔可用：

- `AdaptiveAnomaliesControl` – 適應性異常控制。
- `AMSI` – AMSI 防護。
- `AntiCryptor`
- `BehaviorDetection` – 行為偵測。
- `DeviceControl` – 裝置控制。
- `EntAppControl` - 應用程式控制。
- `File_Monitoring` 或 `FM` – 檔案威脅防護。
- `Firewall` 或 `FW` – 防火牆。
- `HIPS` – 主機入侵防禦。
- `IDS` – 關於網路威脅防護。
- `IntegrityCheck` – 完整性檢查。
- `LogInspector` – 記錄檢查。
- `Mail_Monitoring` 或 `EM` – 郵件威脅防護。
- `Rollback` – 更新回溯（如果應用程式在 Light Agent 模式下安裝則不可套用設定檔）。
- `Scan_ContextScan` – 從內容功能表掃描。
- `Scan_IdleScan` – 背景掃描。
- `Scan_Memory` - 內核記憶體掃描。
- `Scan_My_Computer` – 完整掃描。
- `Scan_Objects` – 自訂掃描。
- `Scan_Qscan` - 掃描在作業系統啟動時載入的物件。
- `Scan_Removable_Drive` – 卸除式磁碟機掃描。
- `Scan_Startup` 或 `STARTUP` – 關鍵區域掃描。

- `Updater` – 更新（如果應用程式在 Light Agent 模式下安裝則不可套用設定檔）。
- `Web_Monitoring` 或 `WM` – Web 威脅防護。
- `WebControl` – Web 控制。

Kaspersky Endpoint Security 還支援服務設定檔。聯絡卡巴斯基技術支援時，可能需要服務設定檔。

# 透過 REST API 管理應用程式

Kaspersky Endpoint Security 允許您使用協力廠商解決方案配置應用程式設定，執行掃描，更新病毒資料庫以及執行其他工作。Kaspersky Endpoint Security 為此提供了一個 API。Kaspersky Endpoint Security REST API 透過 HTTP 執行，並且由一組請求/回應方法組成。換句話說，您可以透過協力廠商解決方案而不是本機應用程式介面或卡巴斯基安全管理中心管理主控台來管理 Kaspersky Endpoint Security。

要開始使用 REST API，您需要安裝帶 REST API 支援的 Kaspersky Endpoint Security。REST 用戶端和 Kaspersky Endpoint Security 必須安裝在同一台電腦上。

為確保 Kaspersky Endpoint Security 與 REST 用戶端之間的安全交互，請執行以下操作：

- 根據 REST 用戶端開發人員的建議配置 REST 用戶端的防護以防止未經授權的存取。配置 REST 用戶端資料夾防護，以防止在判別存取控制清單（DACL）的幫助下進行寫入。
- 要執行 REST 用戶端，請使用具有管理員權限的單獨帳戶。拒絕此帳戶交互式登入到系統。

透過位於 http://127.0.0.1 或 http://localhost 的 REST API 管理應用程式。無法透過 REST API 遠端系統管理 Kaspersky Endpoint Security。

**開啟 REST API 文件**

# 使用 REST API 安裝應用程式

要透過 REST API 管理應用程式，您需要安裝帶 REST API 支援的 Kaspersky Endpoint Security。如果透過 REST API 管理 Kaspersky Endpoint Security，則無法使用卡巴斯基安全管理中心管理該應用程式。

## 準備安裝帶 REST API 支援的應用程式

Kaspersky Endpoint Security 與 REST 用戶端進行安全交互需要設定請求識別。為此，您必須安裝憑證並隨後簽署每個請求的承載。

若要建立憑證，您可以使用，例如，OpenSSL。

範例:

```
$ openssl req -x509 -newkey rsa:4096 -keyout key.pem -out cert.pem -days 1825 -nodes
```

使用金鑰長度為 2048 位元或者更多的 RSA 加密演算法。

因此，您將獲得一個 `cert.pem` 憑證和一個 `key.pem` 私密金鑰。

安裝帶 REST API 支援的應用程式

*要安裝帶 REST API 支援的 Kaspersky Endpoint Security：*

1. 以管理員身分執行命令列解譯器 (cmd.exe)。
2. 轉到包含 Kaspersky Endpoint Security 版本 11.2.0 或更高版本分發套件的資料夾。
3. 使用以下設定安裝 Kaspersky Endpoint Security：

   - `RESTAPI=1`
   - `RESTAPI_User=<user name>`

     用於透過 REST API 管理應用程式的使用者名稱。輸入格式為 `<DOMAIN>\<UserName>` 的使用者名稱（例如，`RESTAPI_User=COMPANY\Administrator`）。您只能在此帳戶下透過 REST API 管理應用程式。您只能選擇一個使用者來使用 REST API。
   - `RESTAPI_Port=<port>`

     用於透過 REST API 管理應用程式的連接埠。預設情況下使用 6782 連接埠。確保連接埠空閒。可選參數。
   - `RESTAPI_Certificate=<path to certificate>`

     用於識別請求的憑證（例如，`RESTAPI_Certificate=C:\cert.pem`）。

     您可以在安裝應用程式後安裝憑證或者在憑證到期後更新憑證。

     **如何安裝憑證用於 REST API 請求識別**

     1. 停用 Kaspersky Endpoint Security 自我防護

        自我防護機制可防止變更或刪除硬碟上的應用程式檔案、記憶體中的處理程序和系統登錄檔中的項目。
     2. 前往包含 REST API 設定的登錄機碼：
        `HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\KasperskyLab\protected\KES\settings\RestAp`
     3. 輸入憑證路徑，例如，`Certificate = C:\Folder\cert.pem`。
     4. 啟用 Kaspersky Endpoint Security 自我防護。
     5. 重啟應用程式。
   - `AdminKitConnector=1`

     使用管理系統管理應用程式。預設情況下允許管理。

   您還可以使用 setup.ini 檔案來定義 REST API 的使用設定。

   ```
   範例:
   setup_kes.exe /pEULA=1 /pPRIVACYPOLICY=1 /pKSN=1 /pALLOWREBOOT=1 /pAdminKitConnector=1 /pRESTAPI=1
   /pRESTAPI_User=COMPANY\Administrator /pRESTAPI_Certificate=C:\cert.pem /s
   ```

結果，您將能夠透過 REST API 管理應用程式。要驗證其操作，請使用 GET 請求開啟 REST API 文件。

範例:

```
GET http://localhost:6782/kes/v1/api-docs
```

如果您已安裝帶 REST API 支援的應用程式，Kaspersky Endpoint Security 將自動在用於存取 Web 資源的 Web 控制設定中建立一個允許規則（*REST API 的服務規則*）。所有時候都需要該規則來允許 REST 用戶端存取 Kaspersky Endpoint Security。例如，如果您有受限制的 Web 資源使用者存取權限，這不會影響透過 REST API 管理應用程式。我們建議您不要刪除規則或者變更"*REST API 的服務規則*"設定。如果您刪除規則，Kaspersky Endpoint Security 將在重啟應用程式後還原它。

# 使用 API

無法使用密碼防護透過 REST API 限制對應用程式的存取。例如，無法封鎖使用者透過 REST API 停用防護。您可以透過 REST API 配置密碼防護，並透過本機介面限制使用者對應用程式的存取。

要透過 REST API 管理應用程式，需要在安裝帶 REST API 支援的應用程式時指定的帳戶下執行 REST 用戶端。您只能選擇一個使用者來使用 REST API。

**開啟 REST API 文件**

透過 REST API 管理應用程式包括以下步驟：

1. 獲取應用程式設定的當前值。為此，請傳送一個 GET 請求。

   範例:

   ```
   GET http://localhost:6782/kes/v1/settings/ExploitPrevention
   ```

2. 應用程式將傳送包含設定的結構和值的回應。Kaspersky Endpoint Security 支援 XML 和 JSON 格式。

   範例:

   ```
   {
   "action": 0,
   "enableSystemProcessesMemoryProtection": true,
   "enabled": true
   }
   ```

3. 編輯應用程式設定。使用在對 GET 請求的回應中收到的設定結構。

   範例:

   ```
   {
   "action": 0,
   "enableSystemProcessesMemoryProtection": false,
   "enabled": true
   }
   ```

4. 在 JSON 中儲存應用程式核定（承載）(payload.json)。

5. 用 PKCS7 格式簽署 JSON。

   範例:

   ```
   $ openssl smime -sign -in payload.json -signer cert.pem -inkey key.pem -nodetach -binary -outform pem -out
   signed_payload.pem
   ```

   因此，您會得到一個具有請求的承載的署名檔案(`signed_payload.pem`)。

6. 編輯應用程式設定。為此，請傳送一個 POST 請求並附上有請求承載的署名檔案(`signed_payload.pem`)。

應用程式會套用新設定並傳送包含應用程式配置結果的回應（回應可以為空）。您可以使用 GET 請求驗證設定已更新。

# 關於應用程式的資訊源

## 卡巴斯基網站上的 Kaspersky Endpoint Security 頁面

在Kaspersky Endpoint Security 頁面，您可以檢視有關應用程式及其功能和特性的一般資訊。

Kaspersky Endpoint Security 頁面包含線上商店的連接。您可以在那裡購買或更新應用程式。

## 知識庫中的 Kaspersky Endpoint Security 頁面

*知識庫* 是技術支援網站上的一個部分。

在 知識庫中的 Kaspersky Endpoint Security 頁面，您可以閱讀提供有關如何購買、安裝和使用應用程式的有用資訊、建議和常見問題解答的文章。

知識庫文章不僅可以回答與 Kaspersky Endpoint Security 相關的問題，還可以回答與其他卡巴斯基應用程式相關的問題。知識庫中的文章還可能包含來自技術支援的新聞。

## 論壇中關於卡巴斯基應用程式的討論

如果您的問題不需要緊急回答，您可以在我們的論壇上與卡巴斯基專家和其他使用者討論。

在論壇中，您可以檢視現有主題、發表自己的評論以及建立新的討論主題。

# 聯絡技術支援服務

如果您無法在檔案中或Kaspersky Endpoint Security 相關資訊源中找到您問題的解決方案，建議您聯絡技術支援。技術支援會為您解答關於安裝和使用 Kaspersky Endpoint Security 的問題。

Kaspersky 在應用程式的生命週期內為 Kaspersky Endpoint Security 提供支援（請參閱應用程式生命週期頁面）。與技術支援部門聯絡之前，請閱讀支援規則。

您可以透過以下方式取得技術支援：

- 透過造訪技術支援網站
- 透過 Kaspersky CompanyAccount 網站向 Kaspersky 技術支援傳送請求

將您的問題通知 Kaspersky 技術支援專家後，他們可能會請您建立一個*偵錯檔案*。偵錯檔案可以跟逐步蹤執行應用程式指令的過程，可確定應用程式操作中發生錯誤的階段。

技術支援專家可能還需要更多相關資訊，關於作業系統、電腦中執行的處理程序、應用程式元件操作的詳細報告。

執行診斷時，技術支援專家將要求您透過以下方式變更應用程式設定：

- 啟動用於接收延伸診斷資訊的功能。
- 透過變更從標準使用者介面無法存取的特別設定來設定應用程式單獨模組。
- 變更診斷資訊儲存的設定。
- 設定網路流量擷取和記錄。

技術支援專家會提供執行這些操作所需的所有資訊（步驟順序說明、要修改的設定、設定檔、指令碼、附加的命令列功能、調試模組、特定用途的實用程式等），並會告知您調試時所使用的資料的範圍。延伸診斷資訊儲存在使用者的電腦中。資料不會自動傳輸到 Kaspersky。

以上列出的操作請在技術支援專家的引導下，按照指示操作。擅自以未在“線上說明”或“技術支援”建議中予以描述的方式變更應用程式設定可能引起作業系統速度減緩和崩潰，降低您的電腦的防護等級，以及損害正在被處理的資訊的可用性和完整性。

# 偵錯檔案的內容和儲存

您親自負責電腦上儲存的資料的安全性，尤其是在資料提交到 Kaspersky 前監控和限制對資料的存取。

只要應用程式在使用中，就會在電腦中儲存偵錯檔案，當應用程式被移除後，偵錯檔案將被永久移除。

偵錯檔案（身分驗證代理的偵錯檔案除外）儲存在`%ProgramData%\Kaspersky Lab\KES.12.12\Traces`資料夾中。

偵錯檔案按如下方式命名：`KES<12.12_dateXX.XX_timeXX.XX_pidXXX.><trace file type>.log`。

您可以檢視偵錯檔案中儲存的資料。

所有偵錯檔案都包含下列一般資料：

- 事件時間
- 執行線程編號

  > 身分驗證代理偵錯檔案不包含該資訊。

- 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。

Kaspersky Endpoint Security 僅以加密形式將使用者密碼儲存到偵錯檔案中。

## SRV.log、GUI.log 和 ALL.log 偵錯檔案的內容

`SRV.log`、`GUI.log` 和 `ALL.log` 偵錯檔案可儲存一般資料之外的下列資訊：

- 個人資料，包括姓氏、名字和中間名，如果此資料封包含在本機電腦檔案的路徑中。
- 電腦上安裝的硬體資料（如 BIOS/UEFI 韌體資料）。當執行卡巴斯基磁碟加密時，此資料將寫入偵錯檔案。
- 使用者名稱和密碼，如果它們公開傳送。在網際網路流量掃描期間，此資料可被記錄偵錯檔案中。
- 使用者名稱和密碼，如果它們包含在 HTTP 標題中。
- Microsoft Windows 帳戶名稱，如果該帳戶名稱包含在檔案名中。
- 包含您的帳戶名和密碼的電子郵件位址或網頁位址，如果它們包含在被偵測的物件名中。
- 您存取的網站和從這些網站被重定向的網站。當應用程式掃描網路時，將會把此資料寫入偵錯檔案。
- 登入代理伺服器的代理伺服器位址、電腦名稱、連接埠、IP 位址和使用者名稱。當應用程式使用代理伺服器時，將會把此資料寫入偵錯檔案。
- 您的電腦要與其建立連線的遠端 IP 位址。
- 郵件主旨、ID、社群網路寄件者網頁的寄件者名稱和位址。當啟用 Web 控制元件時，將會把此資料寫入偵錯檔案。
- 網路流量資料。如果啟用流量監控元件（如 Web 控制），則此資料將寫入偵錯檔案。
- 從 Kaspersky 伺服器接收的資料（如病毒資料庫的版本）。

- Kaspersky Endpoint Security 元件的狀態及其操作資料。
- 應用程式中的使用者活動資料。
- 作業系統事件。

## HST.log、BL.log、Dumpwriter.log、WD.log 和 AVPCon.dll.log 偵錯檔案的內容

除了一般資料之外，HST.log 偵錯檔案包含關於資料庫執行和程式模組更新工作的資訊。

除了一般資料之外，BL.log 偵錯檔案包含應用程式執行期間發生的事件資訊，以及對應用程式錯誤進行故障排除所需的資料。如果使用 avp.exe –bl 參數啟動應用程式，將建立此檔案。

除了一般資料之外，當進行應用程式記憶體傾印時，Dumpwriter.log 偵錯檔案包含對錯誤進行故障排除時必要服務資訊。

除了一般資料之外，WD.log 偵錯檔案包含 avpsus 服務執行期間所發生的事件資訊，包括應用程式模組更新事件。

除了一般資料之外，AVPCon.dll.log 偵錯檔案包含卡巴斯基安全管理中心連線模組執行期間所發生的事件資訊。

## 效能跟蹤檔案的內容

效能跟蹤檔案按如下方式命名：KES<12.12_dateXX.XX_timeXX.XX_pidXXX.>PERF.HAND.etl。

除了一般資料，效能跟蹤檔案還包含有關處理器負載的資訊、有關作業系統和應用程式的載入時間的資訊以及有關正在執行的處理程序資訊。

## AMSI 防護元件偵錯檔案的內容

除了一般資料，AMSI.log偵錯檔案還包含有關對協力廠商應用程式的請求執行掃描的結果的資訊。

## “郵件威脅防護”元件的偵錯檔案的內容

除一般資料外，偵錯檔案 mcou.OUTLOOK.EXE.log 可能還包含電子郵件的一部分，包括電子郵件信箱。

### “從內容功能表掃描”元件的偵錯檔案的內容

除一般資訊外，`shellex.dll.log` 偵錯檔案還包含有關掃描工作完成情況的資訊以及調試應用程式所需的資料。

### 應用程式 Web 外掛程式偵錯檔案的內容

應用程式 Web 外掛程式的偵錯檔案儲存在部署了卡巴斯基安全管理中心網頁主控台的電腦上，位於資料夾 `Program Files\Kaspersky Lab\Kaspersky Security Center Web Console\logs` 中。

應用程式 Web 外掛程式的偵錯檔案按如下方式命名： `logs-kes_windows-<type of trace file>.DESKTOP-<date of file update>.log`。網頁主控台在安裝後開始寫入資料，在刪除網頁主控台後會刪除偵錯檔案。

除了一般資料之外，應用程式 Web 外掛程式偵錯檔案包含以下資訊：

- 用於解鎖 Kaspersky Endpoint Security 介面的 KLAdmin 使用者密碼（密碼防護）。
- 用於解鎖 Kaspersky Endpoint Security 介面的暫時密碼（密碼防護）。
- SMTP 郵件伺服器的使用者名稱和密碼（電子郵件通知）。
- 網際網路代理伺服器的使用者名稱和密碼（代理伺服器）。
- *變更應用程式元件* 工作的使用者名稱和密碼。
- 在 Kaspersky Endpoint Security 工作和政策內容中指定的帳戶憑證和路徑。

### 身分驗證代理偵錯檔案的內容

身分驗證代理偵錯檔案儲存在System Volume Information資料夾中，並按如下方式命名：`KLFDE.{EB2A5993-DFC8-41a1-B050-F0824113A33A}.PBELOG.bin`。

除了一般資料之外，身分驗證代理偵錯檔案包含身分驗證代理執行資訊和使用者使用身分驗證代理所執行操作的資訊。

# 應用程式操作追蹤

*應用程式追蹤*是應用程式執行的操作以及有關應用程式執行期間發生的事件的訊息的詳細記錄。在追蹤過程中，應用程式會建立包含有關不同應用程式元件操作的資料的一組檔案（例如，SRV.log、WD.log 等）。

應用程式追蹤應在 Kaspersky 技術支援的監督下執行。

*要建立應用程式偵錯檔案：*

1. 開啟應用程式主視窗並點擊 按鈕。
2. 在開啟的視窗中，點擊**"支援工具"**按鈕。
3. 使用**"啟用應用程式追蹤"**開關可以啟用或停用對應用程式操作的追蹤。
4. 在**"追蹤"**下拉式清單中，選擇一個應用程式偵錯模式：
   - **有大小限制**將偵錯儲存到有限數量的大小有限的檔案集合中，並在達到最大大小時覆蓋舊檔案。如果選擇此模式，則可以定義要用於循環的檔案集合的最大數量和每個檔案集合的最大大小。

     預設情況下，應用程式儲存五組偵錯檔案。每組檔案的大小為 3072 MB。這樣，您需要 15 GB 的可用磁碟空間來儲存偵錯檔案。
   - **沒有限制**儲存一個偵錯檔案（無大小限制）。
5. 在**"等級"**下拉清單中，選取偵錯等級。

   我們建議您透過技術支援專家瞭解所需偵錯等級。如果技術支援專家未提供指導，請將偵錯等級設定為**"正常"**。
6. 重新啟動 Kaspersky Endpoint Security。
7. 要停止偵錯過程，請返回"支援工具"視窗並停用偵錯。

> 您也可以在從命令列安裝應用程式時（包括使用 setup.ini 檔案）建立偵錯檔案。

結果，將在 `%ProgramData%\Kaspersky Lab\KES.12.12\Traces` 資料夾中建立應用程式操作偵錯檔案。建立偵錯檔案後，將檔案傳送給卡巴斯基技術支援。

Kaspersky Endpoint Security 可在應用程式被移除時自動刪除偵錯檔案。您也可以手動刪除檔案。為此，您必須停用偵錯並停止應用程式。

# 應用程式效能追蹤

Kaspersky Endpoint Security 允許您在使用應用程式時接收有關電腦操作問題的資訊。例如，您可以在安裝應用程式後收到有關作業系統載入延遲的資訊。為此，Kaspersky Endpoint Security 會建立效能偵錯檔案。*效能追蹤*是指為了診斷 Kaspersky Endpoint Security 的效能問題而對應用程式執行的操作進行記錄。為接收資訊，Kaspersky Endpoint Security 使用 Windows 事件跟蹤服務 (ETW)。Kaspersky 技術支援負責診斷 Kaspersky Endpoint Security 的問題並確定這些問題的原因。

> 應用程式追蹤應在 Kaspersky 技術支援的監督下執行。

*要建立效能偵錯檔案：*

1. 開啟應用程式主視窗並點擊 按鈕。
2. 在開啟的視窗中，點擊**"支援工具"**按鈕。
3. 使用**"啟用效能追蹤"**開關可以啟用或停用對應用程式效能的追蹤。

4. 在"**追蹤**"下拉式清單中，選擇一個應用程式偵錯模式：

   - **有大小限制**將偵錯儲存到有限數量的大小有限的檔案中，並在達到最大大小時覆蓋舊檔案。如果選擇此模式，您可以定義每個檔案的最大大小。
   - **沒有限制**儲存一個偵錯檔案（無大小限制）。

5. 在"**等級**"下拉清單中，選取偵錯等級：

   - **輕**Kaspersky Endpoint Security 會分析與效能相關的最重要作業系統處理程序。
   - **詳情**Kaspersky Endpoint Security 會分析與效能相關的所有作業系統處理程序。

6. 在"**追蹤類型**"下拉清單中，選取偵錯類型：

   - **基本資訊**Kaspersky Endpoint Security 在作業系統執行時分析處理程序。如果在載入作業系統後問題仍然存在（例如在瀏覽器中存取網際網路時出現問題），請使用此偵錯類型。
   - **重新啟動中**Kaspersky Endpoint Security 僅在作業系統載入時分析處理程序。作業系統載入後，Kaspersky Endpoint Security 將停止偵錯。如果問題與作業系統的延遲載入有關，請使用此偵錯類型。

7. 重新啟動電腦並嘗試重現該問題。

8. 要停止偵錯過程，請返回"支援工具"視窗並停用偵錯。

結果，將在 `%ProgramData%\Kaspersky Lab\KES.12.12\Traces` 資料夾中建立效能追蹤檔案。建立偵錯檔案後，將檔案傳送給 Kaspersky 技術支援。

# 傾印寫入

傾印檔案包含此檔案建立時 Kaspersky Endpoint Security 處理程序的工作記憶體的所有相關資訊。

> 已儲存的轉儲檔案可能包含機密資料。要控制資料的存取，必須單獨確保傾印檔案的安全性。

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。傾印檔案儲存在 `%ProgramData%\Kaspersky Lab\KES.12.12\Traces` 資料夾中。

**如何在管理主控台 (MMC) 中啟用傾印寫入**

1. 在卡巴斯基安全管理中心管理主控台樹狀目錄中，選取**政策**。
2. 選擇必要的政策並點擊以開啟政策內容。
3. 在政策視窗中，選擇"**一般設定 → 應用程式設定**"。
4. 在"**偵錯資訊**"塊中，點擊"**設定**"按鈕。
5. 在開啟的視窗中，使用"**啟用傾印寫入**"核取方塊來啟用或停用應用程式傾印寫入。
6. 儲存變更。

**如何在網頁主控台和雲端主控台中啟用傾印寫入**

1. 在網頁主控台的主視窗中，選擇**資產（裝置）→政策和設定檔**。
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**"→"**技術支援**"。
5. 在"**偵錯資訊**"塊中，使用"**傾印寫入已啟用**"核取方塊來啟用或停用應用程式傾印寫入。
6. 儲存變更。

**如何在應用程式介面中啟用傾印寫入**

1. 在"應用程式主視窗"中，點擊⚙按鈕。
2. 在應用程式設定視窗中，選取"**一般設定**"→"**應用程式設定**"。




Kaspersky Endpoint Security for Windows 設定

3. 在"**偵錯資訊**"塊中，使用"**啟用傾印寫入**"核取方塊來啟用或停用應用程式傾印寫入。
4. 儲存變更。

# 防護傾印檔案和偵錯檔案

傾印檔案和偵錯檔案包含作業系統的資訊，可能還包含使用者資料。為了防止未經授權地存取此類資料，您可以啟用防護傾印檔案和偵錯檔案。

如果啟用了傾印檔案和偵錯檔案防護，則以下使用者可以存取這些檔案：

- 系統管理員和本機管理員以及啟用寫入傾印檔案和偵錯檔案的使用者可以存取傾印檔案。
- 只有系統管理員和本機管理員可以存取偵錯檔案。

**如何在管理主控台 (MMC) 中啟用傾印檔案和偵錯檔案的防護**

1. 在卡巴斯基安全管理中心管理主控台樹狀目錄中，選取**政策**。
2. 選擇必要的政策並點擊以開啟政策內容。
3. 在政策視窗中，選擇"**一般設定 → 應用程式設定**"。
4. 在"**偵錯資訊**"塊中，點擊"**設定**"按鈕。
5. 在開啟的視窗中，使用"**啟用傾印和偵錯檔案防護**"核取方塊來啟用或停用檔案防護。
6. 儲存變更。

**如何在網頁主控台和雲端主控台中啟用對傾印檔案和偵錯檔案的防護**

1. 在網頁主控台的主視窗中，選擇**資產（裝置）→ 政策和設定檔**。
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**"→"**技術支援**"。
5. 在"**偵錯資訊**"塊中，使用"**傾印和偵錯檔案防護已啟用**"核取方塊來啟用或停用檔案防護。
6. 儲存變更。

**如何在應用程式介面中啟用對傾印檔案和偵錯檔案的防護**

1. 在“應用程式主視窗”中，點擊⚙按鈕。
2. 在應用程式設定視窗中，選取”**一般設定**“→“**應用程式設定**”。




Kaspersky Endpoint Security for Windows 設定

3. 在“**偵錯資訊**“塊中，使用“**啟用傾印和偵錯檔案防護**”核取方塊來啟用或停用檔案防護。
4. 儲存變更。

防護有效期間寫入的傾印檔案和偵錯檔案即使該功能被停用也會保持為防護狀態。

# 取得作業系統資料 (Kaspersky Get System Info)

安裝 Kaspersky Endpoint Security 應用程式後，作業系統或應用程式可能無法正常運作。應用程式與電腦元件的軟體或驅動程式之間存在衝突。

為了確定問題的原因，卡巴斯基技術支援需要 Kaspersky Get System Info 實用程式（以下簡稱 GSI）的報告。有關使用該實用程式的詳細資訊，請參閱 卡巴斯基知識庫。

# 限制和警告

Kaspersky Endpoint Security 設計了眾多不會影響應用程式執行的限制。

**安裝應用程式**

- 有關對 Microsoft Windows 10、Microsoft Windows Server 2016 和 Microsoft Windows Server 2019 作業系統的支援的詳細資訊，請參閱技術支援知識庫。
- 有關對 Microsoft Windows Server 11 和 Microsoft Windows Server 2022 作業系統的支援的詳細資訊，請參閱技術支援知識庫。
- 在安裝到受感染的電腦之後，該應用程式不會通知使用者需要執行電腦掃描的資訊。您可能在啟動應用程式時遇到問題。要解決這些問題，請開始"關鍵區域掃描"。
- 如果在 setup.ini和setup.reg 檔案中使用了非 ASCII 字元（例如，俄語字母），建議您使用 notepad.exe 編輯檔案並以 UTF-16LE 編碼儲存檔案。不支援其他編碼。
- 在安裝套件設定中指定應用程式安裝路徑時，該應用程式不支援使用非ASCII字元。
- 從 CFG 檔案匯入應用程式設定時，將不會套用定義參與卡巴斯基安全網路的設定的值。匯入設定後，請閱讀卡巴斯基安全網路聲明的文本，並確認您同意加入卡巴斯基安全網路。您可以在應用程式介面或包含應用程式分發套件的資料夾中的ksn_*.txt檔案中閱讀聲明的文本。
- 如果要刪除然後重新安裝加密（FLE或FDE）或裝置控制元件，您必須在重新安裝之前重新啟動系統。
- 使用Microsoft Windows 10作業系統時，必須在刪除檔案級別加密（FLE）元件後重新啟動系統。
- 當移除單個應用程式元件（例如，使用*變更應用程式元件*工作）時，可能需要電腦重新啟動。
- 在 *變更應用程式元件*工作的屬性中，當切換安裝模式時（**單獨模式 / 組合模式**），在不同模式之間同步元件集合不受支援。重新開啟工作屬性後，應用程式會在模式之間同步元件集合。
- 應用程式的安裝可能會以錯誤結尾，指出*您的電腦上安裝了名稱丟失或無法讀取的應用程式*。這意味著不相容的應用程式或其片段保留在您的電腦上。要刪除不相容應用程式的工件，請透過 Kaspersky CompanyAccount 向 Kaspersky 技術支援傳送請求，其中包含情況的詳細說明。
- 如果您取消了移除 Kaspersky Endpoint Security，請在重新啟動電腦後啟動應用程式還原。
- 應用程式需要 Microsoft .NET Framework 4.0 或後續版本。Microsoft .NET Framework 4.6.1 有弱點。如果您正在使用 Microsoft .NET Framework 4.6.1，必須安裝安全更新。有關 Microsoft .NET Framework 安全更新的詳情，請參閱Microsoft Technical Support 網站。
- 如果在伺服器作業系統中選擇的 Kaspersky Endpoint Agent 元件未成功安裝該應用程式，並且出現*Windows Installer Coordinator Error*視窗，請參閱 Microsoft 支援網站上的說明。
- 如果應用程式以非交互方式在本機安裝，請使用提供的setup.ini 檔案替換已安裝的元件。
- 在 Windows 7 的某些配置中安裝 Kaspersky Endpoint Security for Windows 之後，Windows Defender 會繼續運行。建議您手動停用 Windows Defender，以防止系統效能下降。

- 當在安裝了 Kaspersky Security for Windows Server (KSWS) 和 Windows Defender 應用程式的伺服器上安裝 Kaspersky Endpoint Security for Windows 時，您必須重新啟動系統。即使您啟用了應用程式安裝無需系統重新啟動，也必需重新啟動系統。Windows Defender for Windows Server 包括在與 Kaspersky Endpoint Security for Windows 不相容的軟體清單中。在安裝應用程式前，安裝程式將移除 Windows Defender for Windows Server。移除不相容的軟體必需重新啟動系統。

- 在安裝了 Kaspersky Security for Windows Server (KSWS) 的伺服器上安裝 Kaspersky Endpoint Security for Windows (KES) 之前，您必須關閉 KSWS 密碼防護。從 KSWS 遷移到 KES 後，請在應用程式設定中啟用密碼防護。

- 若要在執行部署了 Veeam Backup & Replication 軟體的 Windows 7 或 Windows Server 2008 R2 的電腦上安裝應用程式，您可能需要重新啟動電腦並再次執行安裝。

- 自 KSOS 版本 21.16 *.*開始，可以在啟用密碼防護的情況下從 Kaspersky Small Office Security (KSOS) 遷移到 Kaspersky Endpoint Security (KES)。若要遷移更早版本的 KSOS，您必須停用密碼防護或手動移除 KSOS。在停用密碼防護的情況下從 KSOS 遷移到 KES 執行成功。

- 您無法在可啟動的卸除式磁碟機上安裝 Kaspersky Endpoint Security。安裝時，Kaspersky Endpoint Security 會顯示錯誤訊息：*您選擇的資料夾或磁碟無效，程式必須安裝在本機磁碟上*。。如果您設法使用第三方工具將應用程式安裝在卸除式磁碟機上，這可能會導致作業系統在啟動過程中崩潰（BSOD）。這意味著 Kaspersky Endpoint Security 不支援 Windows To Go 和類似的解決方案。要從卸除式磁碟機掃描電腦，您可以使用免費的 卡巴斯基救援光碟 應用程式。

- 在具有多使用者 RDP 工作階段的終端伺服器上安裝含網路元件的 Kaspersky Endpoint Security 時，需考慮一些特殊注意事項。作業系統會強制所有使用者工作階段在管理員工作階段結束後終止。若要連線到終端伺服器，您必須重新啟動伺服器或在本機登入系統。此行為是由 Windows 作業系統的運作特性決定的。

- 如果 Web 外掛程式 Kaspersky Endpoint Security for Windows（內建版本 12.11.0.2004）和 Kaspersky Endpoint Security for Linux（內建版本 12.4.0.1354）安裝在卡巴斯基安全管理中心 16.0 或者卡巴斯基安全管理中心 16.1 中，則將 Kaspersky Endpoint Security for Windows Web 外掛程式更新到版本 12.11.0.6004 可能導致 Kaspersky Endpoint Security for Linux 政策中發生故障。

  可能的解決方案：前往 **設定 → Web 外掛程式** 視窗，並從清單中移除 Kaspersky Endpoint Security for Windows Web 外掛程式、Kaspersky Endpoint Security for Linux Web 外掛程式和 Unified Protection and Management Plug-in。然後先安裝 Kaspersky Endpoint Security for Linux Web 外掛程式，接著安裝 Kaspersky Endpoint Security for Windows Web 外掛程式。

- 在 Web 主控台中，Kaspersky Endpoint Security 12.11 for Windows 的安裝套件屬性中的元件清單顯示不正確。此版本的應用程式中不提供單獨的元件 Anti-Cryptor。行為偵測元件中包含防護共用資料夾免受外部加密的功能。在 Kaspersky Endpoint Security 12.12 for Windows 中，此功能是一個單獨的元件。同時，在管理主控台（MMC）中，元件清單顯示正確。

**升級應用程式**

- 從 11.0.0 應用程式版本開始，您可以在之前的外掛程式版本上安裝 Kaspersky Endpoint Security for Windows MMC 外掛程式。若要返回之前的外掛程式版本，請刪除目前的外掛程式然後安裝之前版本的外掛程式。

- 升級 Windows 版的 Kaspersky Endpoint Security 11.0.0 或 11.0.1 時，不會儲存 *資料庫和應用程式模組更新*、*關鍵區域掃描*、*自訂掃描* 和 *應用程式完整性檢查* 工作的本機工作排程設定。

- 在執行 Windows 10 版本 1903 和 1909 的電腦上，從安裝了檔案級加密（FLE）元件的 Kaspersky Endpoint Security 10 for Windows Service Pack 2 Maintenance Release 3 (build 10.3.3.275)、Service Pack 2 Maintenance Release 4 (build 10.3.3.304)、11.0.0 和 11.0.1 升級可能會以錯誤結尾。這是因為在 Windows 10 版本 1903 和 1909 中這些版本的 Kaspersky Endpoint Security for Windows 不支援檔案加密。在安裝此升級之前，建議您刪除檔案加密元件。

- 應用程式需要 Microsoft .NET Framework 4.0 或後續版本。Microsoft .NET Framework 4.6.1 有弱點。如果您正在使用 Microsoft .NET Framework 4.6.1，必須安裝安全更新。有關 Microsoft .NET Framework 安全更新的詳情，請參閱Microsoft Technical Support 網站。

- 升級 Kaspersky Endpoint Security 時，應用程式會停用 KSN 的使用直到卡巴斯基安全網路聲明被接受。此外，卡巴斯基安全管理中心中的電腦狀態可以被變更為"*緊急*"；會收到事件"*KSN 伺服器不可用*"。如果使用 Kaspersky Managed Detection and Response，您將收到有關解決方案操作中違規的事件。Kaspersky Managed Detection and Response 的操作需要使用 KSN。Kaspersky Endpoint Security 將在套用管理員在其中接受 KSN 使用條款的政策後啟用使用 KSN。一旦卡巴斯基安全網路聲明得到接受，Kaspersky Endpoint Security 就還原操作。

- 在將 Kaspersky Endpoint Security 升級到版本 11.10.0 或更高版本而沒有重新啟動後，電腦上將安裝兩個 Kaspersky Endpoint Security 應用程式。不要手動移除先前版本的應用程式。電腦重新啟動時，先前版本將被自動移除。

- 在執行 Microsoft Windows 11 的電腦上升級 Kaspersky Endpoint Security 後，檔案上下文功能表可能會顯示先前和新應用程式版本的項目。重新啟動電腦兩次以確保檔案上下文功能表的正確操作。

- 如果關閉應用程式的自我防禦並停止所有網路適配器，則在應用程式升級結束和電腦重新啟動之間，應用程式的網路元件將無法運作。應用程式的網路元件包括 Web 威脅防護、郵件威脅防護、網路威脅防護、防火牆、主機入侵防護和 Web 控制。重新啟動電腦以使應用程式正常工作。

- BadUSB 攻擊防護元件在應用程式升級結束和電腦重新啟動之間無法運作。重新啟動電腦以使應用程式正常工作。

- 如果您在上次升級後跳過重新啟動電腦的步驟，則無法升級應用程式。重新啟動電腦以使應用程式正常工作。

- 從 Kaspersky Endpoint Security 11 for Windows 之前的版本升級應用程式後，必須重新啟動電腦。

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

**伺服器平台支援**

- 在啟用了*重複資料刪除*的伺服器上，您需要新增 fsdmhost.exe 檔案到 受信任應用程式清單。這有助於最佳化應用程式的效能並防止 CPU 負載過重。

- ReFS 檔案系統被有限制支援：

  - Kaspersky Endpoint Security 可能不正確處理威脅解毒事件。例如，如果應用程式刪除了一個惡意檔案，報告可能會有一個物件未處理項目。同時，Kaspersky Endpoint Security 會根據應用程式設定解毒威脅。Kaspersky Endpoint Security 也可以為同一個物件建立一個"*物件將在重新啟動後解毒*"事件的副本。

  - 檔案威脅防護可以略過一些威脅。同時，惡意軟體掃描可正常工作。

  - *惡意軟體掃描*工作啟動後，用 iChecker 新增的排除項目將在伺服器重啟時重設。

  - 不支援 iSwift 技術。Kaspersky Endpoint Security 不考慮使用 iSwift 技術新增的掃描排除項目。

  - 如果在安裝 Kaspersky Endpoint Security 之前電腦上存在 meicar.exe 檔案，則 Kaspersky Endpoint Security 不會偵測 eicar.com 和 susp-eicar.com 檔案。

  - Kaspersky Endpoint Security 可能不正確顯示威脅解毒通知。例如，應用程式可能顯示之間解毒的威脅的威脅通知。

- 伺服器平台不支援檔案級加密 (FLE) 和卡巴斯基磁碟加密技術 (FDE)。同時，Kaspersky Endpoint Security 可能不正確地處理資料加密事件。
- 在伺服器作業系統中，不會顯示需要進行進階解毒的警告。
- Microsoft Windows Server 2008 已從支援範圍中排除。不支援在執行 Microsoft Windows Server 2008 作業系統的電腦上安裝該應用程式。
- 如果 Kaspersky Endpoint Security 安裝在部署了 Microsoft Data Protection Manager (DPM) 的伺服器上，可能造成 DPM 工作不正常。這與 DPM 操作中的限制有關。若要消除故障，您應該將本機伺服器磁碟機新增到檔案威脅防護元件和*惡意軟體掃描*工作的排除項目。
- Server Core 模式支援有以下限制：
  - 本機圖形使用者介面不可用，包括通知、彈出通知和其他介面控件。應用程式無法顯示提示視窗，包括以下視窗：
    - 應用程式版本和模組升級確認提示；
    - 電腦重新啟動提示；
    - 提示輸入代理伺服器身分驗證憑據；
    - 提示獲取裝置存取（裝置控制）。
  - 以下元件不可以使用：Web 威脅防護，郵件威脅防護，BadUSB 攻擊防護。
  - 橋接防護不可使用。
  - 您只能在卡巴斯基安全管理中心主控台的應用程式政策中接受卡巴斯基安全網路聲明。
  - BitLocker 磁碟機加密僅適用於受信任平台模組 (TPM)。PIN/密碼不能用於加密，因為應用程式無法顯示預開機身分驗證的密碼提示視窗。如果作業系統啟用了聯邦資訊處理標準 (FIPS) 相容模式，請在開始加密磁碟機之前連線用來儲存加密金鑰的卸除式磁碟機。

**虛擬平台支援：**

- 不支援Hyper-V虛擬機上的完整磁碟加密（FDE）。
- 不支Citrix虛擬平台上的完整磁碟加密（FDE）。
- Windows 10 Enterprise 多工作階段受支援，但有限制：
  - Kaspersky Endpoint Security 可在不通知使用者的情況下解毒啟動威脅，就像解毒伺服器上的啟動威脅時一樣。因為作業系統繼續以多工作階段模式執行，則如果威脅沒有得到立即解決，其它活動使用者可能會失去資料。
  - 完整磁碟加密(FDE)不受支援。
  - 管理 BitLocker 不受支援。
  - 用卸除式磁碟機使用 Kaspersky Endpoint Security 不受支援。Microsoft Azure 基礎結構將卸除式磁碟機定義為網路磁碟機。
- 不支援在Citrix虛擬平台上安裝和使用檔案級加密（FLE）。

- 要支援 Windows Kaspersky Endpoint Security for Windows 與 Citrix PVS 的相容性，請在啟用**確保與 Citrix PVS 相容**選項的情況下執行安裝，確保相容性。可以在安裝精靈中啟用此選項，也可以使用命令列參數 `/pCITRIXCOMPATIBILITY=1` 啟用此選項。如果是遠端安裝，則必須透過向其新增以下參數來編輯KUD 檔案：`/pCITRIXCOMPATIBILITY=1`。

- Citrix XenDesktop。在開始複製之前，必須停用自我防護以複製使用 vDisk 的虛擬機。

- 在為帶有 預裝 Kaspersky Endpoint Security for Windows 和 Windows 和卡巴斯基安全管理中心網路代理的的 Citrix XenDesktop 主映像準備範本電腦時，請將以下類型的排除項目新增到設定檔中：

  ```
  [Rule-Begin]
  Type=File-Catalog-Construction
  Action=Catalog-Location-Guest-Modifiable
  name="%ALLUSERSPROFILE%\Kaspersky Lab\**\*"
  name="%ALLUSERSPROFILE%\KasperskyLab\**\*"
  [Rule-End]
  ```

  有關 Citrix XenDesktop 的詳細資訊，請造訪Citrix 支援網站。

- 在某些情況下，嘗試安全斷開卸除式磁碟機的連線可能會在部署在 VMware ESXi hypervisor 上的虛擬機上失敗。嘗試再次安全斷開裝置連線。

- Kaspersky Endpoint Security 與 VMware ESXi Hypervisor 相容，但有以下限制：

  - Kaspersky Endpoint Security 可能與 Guest Introspection 驅動程式（vnetWFP.sys、vnetFLT.sys 等）不相容。若要解決不相容問題，請將驅動程式更新至最新版本或解除安裝驅動程式。

  - 在某些情況下，嘗試安全移除虛擬機上的卸除式磁碟可能會失敗。嘗試再次安全斷開裝置連線。

- 在裝有 Citrix VDA 代理的虛擬機上安裝 Kaspersky Endpoint Security 可能會出現相容性錯誤。這是因為 Citrix Provisioning Services 與防毒解決方案的相容性有限。有關將防毒解決方案與 Citrix Provisioning Services 結合使用的最佳實踐，請造訪 Citrix 支援網站。

- 如果卸除式磁碟機已連線到 Citrix Hypervisor 上的虛擬機，則 Kaspersky Endpoint Security 將跳過對該磁碟機的掃描（*卸除式磁碟機掃描*任務）。在此類裝置上，作業系統會將連線的卸除式磁碟機識別為網路磁碟機。在此情況下，您可以使用*自訂掃描*工作。應用程式在標準模式和 Light Agent 模式下的行為相同。

- 如果 Kaspersky Endpoint Security 安裝在採用 Citrix App Layering 技術的基礎架構中的虛擬機上，則應用程式偵測到的感染狀態為 *物件將在重新啟動後刪除* 的檔案在虛擬機重新啟動時不會被自動刪除。

  若要刪除此類檔案，您必須將包含使用者層的 VHDX 檔案掛載到 Citrix App Layering 管理員的電腦上，並對掛載的磁碟執行惡意軟體掃描。

**與卡巴斯基安全管理中心的相容性**

- 在卡巴斯基安全管理中心網頁主控台 14.1 和更早的版本上，記錄檢查和檔案完整性監控元件的功能區域名稱在管理伺服器內容的使用者存取權限設定區域中顯示不正確。

- 卡巴斯基安全管理中心 Linux 提供對 Kaspersky Endpoint Security 的有限支援。有關支援限制的詳細資訊，請參閱 卡巴斯基安全管理中心 Linux 14.2 說明。

- 修復應用程式後，電腦到管理伺服器連線的防護將被停用。修復應用程式後，請再次執行*管理伺服器連線防護*工作。

- 在卡巴斯基安全管理中心 15.1 中，您可以每隔幾週執行一次工作（**按每週中的指定日**排程）。Kaspersky Endpoint Security 不支援以數週為間隔執行工作。如果您為 Kaspersky Endpoint Security 安排了每隔幾週執行一次的工作，則應用程式會在每週的指定日期和時間執行工作。

- 在卡巴斯基安全管理中心管理主控台中，**請選擇一個使用者或一組使用者** 從卡巴斯基安全管理中心使用者清單中選擇使用者時，視窗僅顯示前 50,000 位使用者。請參閱 卡巴斯基安全管理中心說明 瞭解更多詳情。

**產品授權**

- 如果顯示"*接收資料錯誤*"系統訊息，請驗證您要執行啟動的電腦是否具有網路存取權限，或透過卡巴斯基安全管理中心啟動代理配置啟動設定。

- 在應用程式介面中，產品授權的到期日期顯示為電腦的本機時間。

- 在具有不穩定網際網路存取的電腦上安裝具有內嵌金鑰檔案的應用程式可能會導致臨時顯示事件，表明該應用程式未啟動或產品授權不允許元件操作。這是因為在安裝過程中應用程式首先啟動嵌入式試用產品授權。它需要存取網際網路。

- 在試用期內，如果在網際網路存取不穩定的電腦上安裝任何應用程式升級或修補程式，可能會導致臨時顯示事件，表明該應用程式未啟動。這是因為在更新安裝過程中應用程式首先啟動嵌入式試用產品授權。它需要存取網際網路。

- 如果在安裝應用程式期間自動啟動了試用版產品授權，然後在不儲存產品授權資訊的情況下刪除了該應用程式，則重新安裝後該應用程式不會使用試用版產品授權自動啟動。在這種情況下，請手動啟動應用程式。

- 如果您使用的是卡巴斯基安全管理中心 11 和 Kaspersky Endpoint Security 12.12，則元件效能報告可能無法正常工作。如果安裝了產品授權中未包含的 Kaspersky Endpoint Security 元件，則網路代理可能會將元件狀態錯誤傳送到 Windows 事件日誌。為避免錯誤，請刪除產品授權中未包含的元件。

**郵件威脅防護**

- 當使用Microsoft Outlook的郵件威脅防護延伸程式掃描郵件時，建議您使用快取Exchange模式（"使用快取Exchange模式"選項）。

- Kaspersky Endpoint Security 不支援 64 位元版本的 MS Outlook 電子郵件用戶端。這意味著如果電腦上安裝了 64 位元版本的 MS Outlook，則即使郵件包含在掃描範圍內，Kaspersky Endpoint Security 也不掃描 MS Outlook 檔案（PST 和 OST 檔案）。

**修復引擎**

- 應用程式只能還原檔案系統為 NTFS 或 FAT32 的裝置上的檔案。

- 應用程式可還原具有以下副檔名的檔案：odt, ods, odp, odm, odc, odb, doc, docx, docm, wps, xls, xlsx, xlsm, xlsb, xlk, ppt, pptx, pptm, mdb, accdb, pst, dwg, dxf, dxg, wpd, rtf, wb2, pdf, mdf, dbf, psd, pdd, eps, ai, indd, cdr, jpg, jpe, dng, 3fr, arw, srf, sr2, bay, crw, cr2, dcr, kdc, erf, mef, mrw, nef, nrw, orf, raf, raw, rwl, rw2, r3d, ptx, pef, srw, x3f, der, cer, crt, pem, pfx, p12, p7b, p7c, 1cd。

- 無法還原位於網路磁碟機或可重寫 CD/DVD 上的檔案。

- 無法還原使用加密檔案系統 (EFS) 加密的檔案。有關 EFS 操作的詳細資訊，請造訪 Microsoft 網站。

- 應用程式不會監控由作業系統內核等級的處理程序對檔案執行的修改。

- 應用程式不會監控透過網路介面對檔案執行的修改（例如，如果某個檔案儲存在共用資料夾中，並且處理程序從其他電腦上遠端啟動）。

- 如果網路封包規則或應用程式網路規則指定了 DNS 名稱，Kaspersky Endpoint Security 可能會向 DNS 伺服器傳送請求以確定這些資源的 IP 位址。防火牆使用 IP 位址來監視網路活動。因此，應用程式將 DNS 名稱解析為 IP 位址。建議將規則中的 DNS 名稱僅用於 LAN 電腦後者內部服務。

- 若要為所有 IPv6 位址指定規則，請新增::-ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff 位址範圍。防火牆不支援 ::/0 遮罩。

- 在以下情況下，支援按本機位址、物理接口和封包生存時間（TTL）篩選封包或連線：

  - 按 TCP 和 UDP 的應用程式規則和封包規則中的輸出封包或連線的本機位址。

  - 按封鎖應用程式規則和封包規則中輸入封包或連線的本機位址（UDP 除外）。

  - 按輸入或輸出封包的封鎖封包規則中的封包生存時間（TTL）。

  - 按封包規則中輸入和輸出封包或連線的網路介面。

- 如果為允許的封包規則配置了網路介面卡或封包的生存時間（TTL），則此規則的優先級低於封鎖的應用程式規則。換句話說，如果某個應用程式的網路活動被封鎖（例如，該應用程式位於“*高限制*”信任群組中），則無法透過使用具有這些設定的封包規則來允許該應用程式的網路活動。在所有其他情況下，封包規則的優先級高於應用程式網路規則。

- 當匯入防火墻封包規則時，Kaspersky Endpoint Security 可以修改規則名稱。該應用程式可確定有同樣一般參數集合的規則：通訊協定，方向，遠端和本機連接埠，封包生存時間 (TTL)。如果該一般參數集合對於多個規則都一樣，則應用程式將把同樣的名稱分配給這些規則或者將參數標籤附加至名稱。按這種方式，Kaspersky Endpoint Security 將匯入所有封包規則，但是具有相同一般設定的規則的名稱可以被變更。

- 如果您已在網路規則中啟用了應用程式事件報告，當把應用程式移動到不同的信任群組後，則不會套用對該信任群組的限制。因此，如果應用程式在受信任應用程式群組中，它將沒有網路限制。然後您為此應用程式啟用事件報告，將其移動到*不信任*信任群組。防火牆不會為此應用程式強制實施網路限制。我們建議您先將應用程式移動到適當的信任群組，然後再啟用事件報告。如果該方法不合適，您可以在網路規則設定中手動配置該應用程式的限制。限制僅套用到應用程式的本機介面。在政策中的信任群組之間移動應用程式工作正確。

- 防火牆和侵入防護元件有通用設定：應用程式權限和受防護的資源。如果變更防火牆的這些設定，Kaspersky Endpoint Security 將自動把新設定套用到侵入防護。例如，如果您允許對防火牆政策的一般設定進行變更（掛鎖開啟），侵入防護設定也將變得可以編輯。

- 當網路封包規則在 Kaspersky Endpoint Security 11.6.0 或更早版本中被觸發時，防火牆報告中的“**應用程式名稱**”欄將總是顯示“*Kaspersky Endpoint Security*”值。此外，防火牆將對所有應用程式封鎖封包級別的連線。該行為已為 Kaspersky Endpoint Security 11.7.0 或更新版本做了修改。“**規則類型**”欄已新增到防火牆報告。當網路封包規則被觸發時，“**應用程式名稱**”欄中的值仍然為空。

- 如果您使用防火牆禁止所有網路活動，網路威脅防護元件可能會偵測到連接埠掃描類型的攻擊。發生這種情況的原因是應用程式在防火牆之前啟動網路威脅防護以偵測網路中的可疑活動。

### BadUSB 攻擊防護

- 當電腦鎖定時 Kaspersky Endpoint Security 會重設 USB 裝置的逾時（例如，屏幕鎖定逾時已經過）。這意味著如果您多次輸入錯誤的 USB 裝置授權代碼，應用程式鎖定了 USB 裝置，Kaspersky Endpoint Security 將允許您在解鎖電腦後重複授權嘗試。在此情況下，Kaspersky Endpoint Security 將在 "BadUSB 攻擊防護元件設定"中指定的時間內不鎖定 USB 裝置。

- Kaspersky Endpoint Security 會在電腦防護被暫停時重設 USB 裝置鎖定逾時。這意味著如果您多次輸入錯誤的 USB 裝置授權代碼，應用程式鎖定了 USB 裝置，Kaspersky Endpoint Security 將允許您在恢復電腦防護後重複授權嘗試。在此情況下，Kaspersky Endpoint Security 將在 "BadUSB 攻擊防護元件設定"中指定的時間內不鎖定 USB 裝置。

### 卡巴斯基安全網路

- 如果伺服器位址包含非拉丁字母（非 ASCII 符號），則連線到 KSN 代理時 Kaspersky Endpoint Security 不支援 HTTPS（**使用 HTTPS** 核取方塊在 KSN 代理連線設定中被選擇）。

- 在卡巴斯基安全管理中心中，當從使用全局卡巴斯基安全網路切換到使用私有卡巴斯基安全網路 (KPSN) 或相反時，在指定產品的政策中將停用參與卡巴斯基安全網路的選項。切換後，請仔細閱讀卡巴斯基安全網路聲明的文本，並確認您同意參加 KSN。您可以在應用程式介面中或在編輯產品政策時閱讀聲明的文本。

- Kaspersky Endpoint Security 不會將文字檔案（例如不包含巨集的 TXT、CSV、LOG 和 DOCX 檔案）傳送至卡巴斯基安全網路進行掃描。該應用程式會傳送可能對 KSN 構成威脅的檔案進行掃描。這些檔案包括可執行檔或可能包含可執行程式碼（例如 DOCX 檔案中的巨集）的檔案。應用程式的其他元件負責掃描文字檔案。您也可以 從文件上下文功能表手動檢查文字檔案的信譽。如果文字檔案包含 *不受信任* 信譽，應用程式將忽略為偵測到的威脅定義的操作。

- 從 Kaspersky Endpoint Security 12.9 for Windows 開始，從 KPSN 切換到全球 KSN 時，您需要重新確認同意卡巴斯基安全網路聲明。為此，您需要在政策屬性或應用程式介面中啟用卡巴斯基安全網路的使用，並確認您同意卡巴斯基安全網路聲明。如果您已經使用全球 KSN，則必須先停用 KSN 使用，然後重新啟用它並確認您同意卡巴斯基安全網路聲明。如果您不同意卡巴斯基安全網路聲明，應用程式將無法存取卡巴斯基安全網路的資料。

### 應用程式控制

- 使用「應用程式控制」規則時，建議不要為不同類別的應用程式添加超過 100000 個包含和排除條件，前提是 Kaspersky Endpoint Security 在滿足最低硬體要求且作業系統為 Microsoft Windows 10 的電腦上執行。

- 在卡巴斯基安全管理中心網頁主控台中使用應用程式控制規則時，僅支援 ZIP 格式的存檔。其他格式的存檔（例如 RAR 或 7z）不受支援。如果您在管理主控台 (MMC) 中使用應用程式控制規則，則沒有此限制。

- 在卡巴斯基安全管理中心網頁主控台中使用應用程式控制規則時，受支援的上傳檔案的最大大小為 104 MB。如果您在管理主控台 (MMC) 中使用應用程式控制規則，則沒有此限制。

- 在應用程式拒絕清單模式下的 Microsoft Windows 10 中工作時，封鎖規則可能被不正確套用，這可能導致封鎖未在規則中指定的應用程式。

- 如果您在升級 Kaspersky Endpoint Security 時新增了新的 *預定義應用程式控制規則*，則您無法將這些規則套用到先前版本的應用程式。

- 當漸進式網頁應用程式（PWA）被應用程式控制元件封鎖時，appManifest.xml 在報告中指示為被封鎖的應用程式。

- 當把標準 Notepad 應用程式新增至 Windows 11 的應用程式控制規則時，不建議指定應用程式路徑。在執行 Windows 11 的電腦上，作業系統使用位於資料夾 `C:\Program Files\WindowsApps\Microsoft.WindowsNotepad*\Notepad\Notepad.exe` 中的 Metro Notepad。在之前版本的作業系統中，Notepad 位於以下資料夾中：

  - `C:\Windows\notepad.exe`
  - `C:\Windows\System32\notepad.exe`
  - `C:\Windows\SysWOW64\notepad.exe`

  當把 Notepad 新增至應用程式控制規則時，您可以從執行應用程式的內容（例如）指定應用程式名稱和檔案雜湊。

- 當將 KSWS 政策遷移到 KES 政策設定檔時，如果類別名稱包含以下被禁止的字元，則政策和工作批次轉換精靈（遷移精靈）將重新命名應用程式類別：`'` `*` `<` `>` `?` `\` `:` `|`。遷移精靈會將這些字元替換為 `_` 字元。例如，`KSWS::\Everyone:[C61F-3B7C-4D89-96A1]` 應用程式類別被重新命名為 `KSWS_Everyone_[C61F-3B7C-4D89-96A1]`。

**裝置控制**

- Kaspersky Endpoint Security 可以記錄外部裝置連線和斷開連線事件。Windows 服務使用系統使用者帳戶以連線或斷開連線裝置。這使得無法知道哪個使用者正在連線或斷開連線裝置。Kaspersky Endpoint Security 指定事件中的 SYSTEM 使用者帳戶。

- 存取新增到受信任清單的印表機裝置被裝置和匯流排封鎖規則封鎖。

- 對於 MTP 裝置，如果您使用作業系統的內建 Microsoft 驅動，則支援對讀，寫和連線操作的控制。如果使用者安裝了用於與裝置一起使用的自訂驅動（例如，作為iTunes或Android Debug Bridge的一部分），則對讀和寫操作的控制可能不起作用。

- 使用 MTP 裝置時，重新連線裝置後會變更存取規則。

- 裝置控制元件登錄與受監視裝置有關的事件，例如裝置的連線和斷開連線，從裝置讀取檔案，將檔案寫入裝置以及其他事件。Kaspersky Endpoint Security 僅註冊以下裝置類型的斷開連線事件： 可攜式裝置(MTP), 卸除式磁碟機, 軟碟, CD/DVD 磁碟機。對於其他裝置類型，應用程式不會註冊斷開連線事件。該應用程式為所有裝置類型註冊將裝置連線到電腦的操作。

- 如果要基於型號遮罩將裝置新增到受信任清單，並使用 ID 中包含但型號名稱中沒有包含的字元，則不會新增這些裝置。在工作站上，這些裝置將基於 ID 遮罩被新增到受信任清單。

- 當應用程式升級而不重新啟動電腦時，裝置控制不會將存取規則套用至重新連線的裝置。但是，如果裝置在升級之前已連線，則裝置控制會正確套用規則。重新啟動電腦，應用程式才能正常使用重新連線的裝置。

- 在安裝了 Kaspersky Endpoint Security 12.0 版的電腦上，如果在電腦上套用了 Kaspersky Endpoint Security 12.1 版政策，則**網路印表機**裝置類型的**允許且不記錄**印表機存取模式被稱為**取決於連線匯流排**。在這些模式下，應用程式執行相同的操作。在 Kaspersky Endpoint Security 12.1 版中，網路印表機的存取模式被正確命名為**允許且不記錄**。

- 從 Kaspersky Endpoint Security 12.0 for Windows 開始，應用程式允許配置印表機的列印規則（列印控制）。安裝帶列印控制的應用程式或將應用程式升級到帶列印控制的版本後，必須重新啟動電腦。在電腦重新啟動之前，Kaspersky Endpoint Security 不會套用列印規則並且只能控制對印表機的存取。如果重新啟動電腦對您組織中的工作流程產生不利影響，您可以只重新啟動 spoolsv 服務（Print Spooler）。

- 從 Kaspersky Endpoint Security 12.0 for Windows 開始，應用程式支援 WPA3 協定用於 **Wi-Fi** 類型的裝置。如果在電腦上套用 Kaspersky Endpoint Security 12.2 政策，則在電腦上對於 Kaspersky Endpoint Security 11.11.0 及更早版本選擇 WPA2 協定；對於 12.0 到 12.1 版本選擇 WPA2 / WPA3；對於 12.2 及更高版本選擇 WPA3。

- Apple 裝置被歸類為攜帶式裝置 (MTP) 和 iTunes 裝置。作業係統可能會錯誤辨識 Apple 裝置的連線，無法確定 Apple 裝置為攜帶式裝置 (MTP)。因此，Apple 裝置將在檔案管理程式中不可使用，但是可以在 iTunes 應用程式中存取。結果，Kaspersky Endpoint Security 將僅在 iTunes 應用程式中控制 Apple 裝置的存取。若要將 Apple 裝置作為攜帶式裝置 (MTP) 存取，您需要前往 Device Manager 將 Apple Mobile Device USB Driver 從 USB Controllers 清單中刪除。電腦重新啟動後，作業係統將辨識 Apple 裝置為攜帶式裝置 (MTP) 和 iTunes 裝置。Kaspersky Endpoint Security 將在 iTunes 應用程式和檔案管理程式中都控制對裝置的存取。

- 在 Kaspersky Endpoint Security 12.3 for Windows 中，**藍芽** 裝置類型的存取設定不同。如果您在之前版本的應用程式中指定了 **取決於連線匯流排** 值，則將應用程式升級到版本12.3後，配置的值變更為 **允許且不記錄**。這不會改變裝置的行為。

- 裝置控制僅通過 Microsoft Windows 藍牙堆疊支援藍牙裝置。裝置控制可能無法與協力廠商藍牙堆疊一起正常運行。

- 如果藍牙裝置隱藏或欺騙其裝置類別 (COD)，則裝置控制可能無法正常工作。

- 在具有某些 Realtek 藍牙適配器驅動程式的 Windows 7 或 Windows 8 電腦上，可能無法僅允許將藍牙裝置作為輸入裝置（HID 類別）連線。也就是說，如果您在應用程式設定中禁止存取藍牙裝置並將輸入裝置新增至排除項目，則裝置控制可能會阻止存取所有藍牙裝置。

**Web 控制**

- 不支援 OGV 和 WEBM 格式。

- 不支援 RTMP 協定。

- Web 控制僅支援 WSL1。應用程式不控制 WSL2 流量。

**適應性異常控制**

- 建議根據事件自動建立排除。手動新增排除項目時，在指定目標物件時，請在路徑的開頭新增`*`字元。

- 如果樣本包含即使一個名稱超過 260 個字元的事件，則無法產生適應性異常控制規則報告。

- 如果物件或處理程序的內容的值包含超過256個字元（例如，目標物件的路徑），則不支援從適應性異常控制規則觸發存儲庫中新增排除項目。您可以在"政策"設定中手動新增排除項目。您還可以在已觸發的適應性異常控制規則的報告中新增排除項目。

- 卡巴斯基安全管理中心 15.1 無法針對特定規則產生詳細的「**自適應異常控制規則狀態報告**」報告。

**磁碟機加密（FDE）**

- 安裝應用程式後，必須重新啟動作業系統，硬碟磁碟機加密才能正常工作。

- 身分驗證代理不支援象形文字或特殊字元`|`和`\`。

- 為了使加密後電腦達到最優效能，要求處理器支援 AES-NI 指令集（英特爾進階加密標準新指令）。如果處理器不支援 AES-NI，則電腦效能可能會降低。

- 當某些程序嘗試在應用程式授予對此類裝置存取權限之前嘗試存取加密的裝置時，該應用程式將顯示警告，指出必須終止此類程序。如果無法終止程序，請重新連線已加密裝置。

- 硬碟磁碟機的唯一 ID 以反向格式顯示在裝置加密統計資訊中。

- 不建議在加密裝置時格式化裝置。

- 當多個卸除式磁碟機同時連線到一台電腦時，加密政策只能套用於一個卸除式磁碟機。重新連線卸除式裝置後，將正確套用加密政策。
- 加密可能無法在分散嚴重的硬碟磁碟機上啟動。對硬碟磁碟機進行磁碟重組。
- 加密硬碟磁碟機後，從加密工作開始直到第一次重新啟動執行 Microsoft Windows 7/8/8.1/10 的電腦，以及安裝硬碟磁碟機加密之後直到首次重新啟動 Microsoft Windows 8/8.1/10 作業系統為止，休眠將被封鎖。解密硬碟磁碟機後，從完全解密開機磁碟機直到首次重新啟動作業系統之時，休眠將被封鎖。在 Microsoft Windows 8/8.1/10 中啟用"快速啟動"選項時，封鎖休眠將防止您關閉作業系統。
- 使用 BitLocker 技術加密磁碟後，Windows 7 电脑不允許在還原過程中變更密碼。輸入還原金鑰並載入作業系統後，Kaspersky Endpoint Security 將不再提示使用者變更密碼或 PIN 代碼。因此，不可能設定新的密碼或 PIN 代碼。此問題源於作業系統的特殊性。要繼續，您需要重新加密硬碟磁碟機。
- 不建議在啟用了其他提供者的情況下使用 xbootmgr.exe 工具。例如，發送器、網路或驅動。
- 安裝了 Kaspersky Endpoint Security for Windows 的電腦不支援格式化加密的卸除式磁碟機。
- 不支援使用 FAT32 檔案系統格式化加密的卸除式磁碟機（該磁碟機顯示為已加密）。要格式化磁碟機，請將其重新格式化為 NTFS 檔案系統。
- 一台加密電腦上不能同時存在多個下載代理。
- 嘗試在未加密狀態下還原可啟動 GPT 磁碟的映像，作業系統可能會使系統無法運作。為避免這種情況，請遵循以下建議：
  - 從備份還原映像之前，請先完整解密磁碟。
  - 建立映像時使用逐個磁區複製的方式。
  - 在還原映像並重新初始化磁碟之前，請從加密磁碟的第一個磁區中刪除資料。
- 同時滿足以下所有條件時，將無法存取以前在其他電腦上加密的卸除式磁碟機：
  - 沒有與卡巴斯基安全管理中心伺服器連線。
  - 使用者正在嘗試使用新的權杖或密碼進行授權。

  如果發生類似情況，請重新啟動電腦。重新啟動電腦後，將授予對加密的卸除式磁碟機的存取權限。
- 在 BIOS 設定中啟用 USB 的 xHCI 模式時，可能不支援透過身分驗證代理髮現 USB 裝置。
- SSHD 裝置不支援用於快取最常用資料的裝置的 SSD 部分的卡巴斯基磁碟加密（FDE）。
- 不支援以 UEFI 模式執行的 32 位元 Microsoft Windows 8/8.1/10 作業系統中對硬碟磁碟機進行加密。
- 加密解密的硬碟磁碟機之前，請重新啟動電腦。
- 硬碟磁碟機加密與 Kaspersky Anti-Virus for UEFI 不相容。不建議在已安裝 Kaspersky Anti-Virus for UEFI 的電腦上使用硬碟磁碟機加密。
- 支援基於 Microsoft 帳戶建立身分驗證代理帳戶，但存在以下限制：
  - 不支援單點登入技術。
  - 如果選擇了為最近 N 天內登入系統的使用者建立帳戶的選項，則不支援自動建立身分驗證代理帳戶。

- 如果身分驗證代理帳戶的名稱具有以下格式：`<domain>/<Windows account name>`，在變更電腦名稱後，您還需要變更為此電腦的本機使用者建立的帳戶名稱。例如，假設在`Ivanov`電腦上有一個本機使用者`Ivanov`，並且為此使用者建立了一個名為`Ivanov/Ivanov`的身分驗證代理帳戶。如果電腦名稱`Ivanov`已變更為`Ivanov-PC`，則需要將使用者`Ivanov`的身分驗證代理帳戶的名稱從`Ivanov/Ivanov`變更為`Ivanov-PC/Ivanov`。您可以使用身分驗證代理的本機帳戶管理工作來變更帳戶名稱。在變更帳戶名稱之前，可以使用舊名稱（例如`Ivanov/Ivanov`）在預開啟環境中進行身分驗證。

- 如果只允許使用者使用權杖存取使用卡巴斯基磁碟加密技術加密的電腦，並且該使用者需要完成存取還原程序，請確保加密電腦的存取權限還原後，該使用者被授予對該電腦基於密碼的存取權限。使用者還原存取時設定的密碼可能不會被儲存。在這種情況下，使用者將必須在下次重新啟動電腦時再次完成還原對加密電腦的存取的程序。

- 使用FDE 還原工具解密硬碟磁碟機時，如果源裝置上的資料被解密後的資料覆蓋，則解密程序可能會以錯誤結束。硬碟磁碟機上的部分資料將保持加密狀態。建議使用FDE還原工具時在裝置解密設定中選擇將解密的資料儲存到檔案的選項。

- 如果身分驗證代理密碼已變更，則有包含文本"*您的密碼已成功變更*"的訊息。"*點擊確定*"出現，使用者重新啟動電腦，新密碼未儲存。在開機前環境中，必須使用舊密碼進行後續身分驗證。

- 磁碟加密與Intel Rapid Start技術不相容。

- 磁碟加密與ExpressCache技術不相容。

- 在某些情況下，當嘗試使用FDE 還原工具解密加密磁碟機時，該工具在完成"請求-回應"程序後會錯誤地將裝置狀態偵測為"未加密"。工具的日誌會顯示一個事件，指出裝置已成功解密。在這種情況下，必須重新啟動資料還原程序以解密裝置。

- 在網頁主控台中更新 Kaspersky Endpoint Security for Windows 外掛程式之後，在重新啟動網頁主控台服務之前，用戶端電腦屬性不會顯示 BitLocker 還原金鑰。

- 要查看完整磁碟加密支援的其他限制以及受限制支援硬碟磁碟機加密的裝置清單，請參閱技術支援知識庫。

**檔案級加密 (FLE)**

- Microsoft Windows Embedded 系列的作業系統不支援檔案和資料夾加密。

- 一旦安裝該應用程式後，必須重新啟動作業系統，檔案和資料夾加密才能正常工作。

- 應用程式僅在具有 NTFS 和 FAT32 檔案系統的裝置上支援檔案加密。如果加密的檔案被傳輸到具有不受支援的檔案系統（例如，exFAT）的裝置，此裝置上的檔案將不會被加密，可進行修改。

- 如果加密檔案儲存在具有可用加密功能的電腦上，而您從沒有加密功能的電腦上存取該檔案，則將提供對該檔案的直接存取。儲存在具有可用加密功能的電腦上的網路資料夾中的加密檔案將以解密形式複製到不具有可用加密功能的電腦上。

- 建議您在使用 Kaspersky Endpoint Security for Windows 加密檔案之前，先解密使用Encrypting File System加密的檔案。

- 檔案加密後大小會增加 4 kB。

- 加密檔案後，在檔案屬性中設定"*封存*"屬性。

- 例如，將解密的檔案複製到可移動媒體時，該檔案可能會保持加密狀態。發生這種情況的原因是，當檔案管理器（例如，explorer.exe）嘗試存取加密檔案時，它會將檔案的雜湊值儲存到處理程序的特殊清單中。解密檔案後，當檔案管理器嘗試存取該檔案時，處理程序會在清單中搜尋該檔案的雜湊值。如果發現雜湊值，Kaspersky Endpoint Security 將對檔案進行加密。為了避免這種情況，您需要清除處理程序清單。隨著處理程序清單填滿，作業系統會自動清除清單。您也可以手動清空清單。為此，您可以重新啟動電腦，重新啟動用於存取檔案的處理程序（例如，explorer.exe），或使用未使用過的其他檔案管理器來存取加密檔案。

- 如果加密存檔的解壓縮檔案與電腦上現有的檔案名稱相同，則後者將被從加密存檔中解壓縮的新檔案所覆寫。使用者不會被通知有關被覆蓋操作的資訊。

- 在解壓縮加密存檔之前，確保您有足夠的可用磁碟空間來容納解壓縮的檔案。如果您沒有足夠的磁碟空間，存檔解壓縮可能完成了，但檔案可能已損壞。在這種情況下，Kaspersky Endpoint Security 可能不會顯示任何錯誤訊息。

- "攜帶式檔案管理器"介面不顯示有關其操作程序中發生的錯誤的訊息。

- Kaspersky Endpoint Security for Windows 不會在安裝了檔案級加密元件的電腦上啟動攜帶式檔案管理器。

- 如果以下條件同時為真，則您不能使用攜帶式檔案管理器來存取卸除式磁碟機：

  - 沒有與卡巴斯基安全管理中心連線；
  - 電腦上已安裝 Kaspersky Endpoint Security for Windows；
  - 沒有在電腦上執行資料加密 (FDE 或 FLE)。

  即使您知道攜帶式檔案管理器的密碼，也無法存取。

- 使用檔案加密時，應用程式與 Sylpheed 郵件用戶端不相容。

- Kaspersky Endpoint Security for Windows 不支援一些應用程式的存取加密檔案限制規則。這是由於某些檔案操作由協力廠商應用程式執行。例如，檔案複製由檔案管理程式執行，而不是應用程式本身執行。因此，如果 Outlook 郵件用戶端被拒絕存取加密檔案，Kaspersky Endpoint Security 將允許郵件用戶端存取加密檔案（如果使用者透過剪貼簿或者使用拖放功能將檔案複製到了電子郵件訊息）。複製操作由檔案管理程式執行，對於該程式未指定加密檔案存取限制規則，即存取被允許。

- 如果使用攜帶模式支援對卸除式磁碟機進行加密，則無法停用密碼期限控制。

- 不支援變更頁面檔案設定。作業系統使用預設值而不是指定的參數值。

- 使用加密卸除式磁碟機時，請使用安全移除。如果未安全移除卸除式磁碟機，我們將不能保證資料完整性。

- 檔案加密後，將安全刪除其未加密的原始檔案。

- 不支援使用Client-Side Caching（CSC）同步離線檔案。加密離線檔案或對伺服器透過 SMB 使用 Branch Caching 技術也不受支援。建議禁止在群組政策級別對共用資源進行離線管理。處於離線模式的檔案可以進行編輯。同步後，對離線檔案所做的變更可能會丟失。

- 不支援在系統硬碟磁碟機的根目錄中建立加密封存 。

- 透過網路存取加密檔案時，您可能會遇到問題。建議您將檔案移至其他來源，或確保用作檔案伺服器的電腦由同一台卡巴斯基安全管理中心管理伺服器進行管理。

- 變更鍵盤佈局可能會導致加密的自動解壓縮封存的密碼輸入視窗掛起。要解決此問題，請關閉密碼輸入視窗，切換到作業系統中的鍵盤佈局，然後重新輸入加密封存的密碼。

- 當在一個磁碟上具有多個磁碟分割的系統上使用檔案加密時，建議您使用可自動確定 pagefile.sys 檔案大小的選項。電腦重新啟動後，pagefile.sys 檔案可能會在磁碟分割之間移動。

- 在套用檔案加密規則（包括"*我的文件*"資料夾中的檔案）之後，請確保已對其套用加密的使用者可以成功存取加密的檔案。為此，請在與卡巴斯基安全管理中心建立連線時讓每個使用者登入系統。如果使用者嘗試存取加密檔案而未連線到卡巴斯基安全管理中心，係統可能會掛起。

- 如果系統檔案某種程度上包含在檔案級加密的範圍內，則與加密這些檔案有關的錯誤事件可能會出現在報告中。這些事件中指定的檔案實際上並未加密。

- 不支援 Pico 程序。

- 不支援區分大小寫的路徑。套用加密規則或解密規則時，產品事件中的路徑以小寫形式顯示。

- 不建議對啟動時系統使用的檔案進行加密。如果加密這些檔案，則在未連線卡巴斯基安全管理中心的情況下嘗試存取加密檔案可能會導致系統掛起或提示存取未加密檔案。

- 如果使用者透過使用檔案到記憶體對應方法的應用程式（例如 WordPad 或 FAR）和旨在處理大檔案的應用程式（例如 Notepad ++）共同透過網路根據 FLE 規則處理檔案，則未加密形式的檔案可能會被無限期封鎖，而無法從其所在的電腦存取它。

- Kaspersky Endpoint Security 不加密位於 OneDrive 雲端儲存或者其他資料夾中以 OneDrive 作為名稱的檔案。Kaspersky Endpoint Security 還會封鎖將加密檔案複製到 OneDrive 資料夾（如果這些檔案未被新增至解密規則）。

- 安裝檔案級加密元件後，使用者和組的管理在WSL模式（Windows Subsystem for Linux）下不起作用。

- 安裝檔案級加密元件時，用於重命名和刪除檔案的 POSIX（Portable Operating System Interface）不受支援。

- 不建議加密暫存檔案，因為這可能造成資料損失。例如，Microsoft Word 會在處理文件時建立暫存檔案。如果加密了暫存檔卻沒有加密原始檔案，使用者在嘗試儲存文件時可能會收到"*存取被拒絕*"錯誤。此外，Microsoft Word 可以儲存檔案，但是下次卻無法開啟文件，即資料將丟失。為了防止資料丟失，您需要將暫存檔資料夾從加密規則中排除。

**Detection and Response (EDR, NDR, MDR, XDR, Sandbox)**

- 您無法掃描因*移動檔案到隔離區*工作被隔離的物件。

- 無法隔離大於 4 MB 的 Alternate Data Stream (ADS)。Kaspersky Endpoint Security 會略過任何這麼大的 ADS 而不通知使用者。

- 如果工作內容中的資料夾路徑用磁碟機字母開始，則 Kaspersky Endpoint Security 不執行網路磁碟機上的"*IOC 掃描*"工作。Kaspersky Endpoint Security 僅支援網路磁碟機上"*IOC 掃描*"工作的 UNC 路徑格式。例如，`\\server\shared_folder`。

- 為了正確運行 *IOC 掃描*（包含使用 Web 主控台建立的 Email/* 條款工作），必須將 Kaspersky Endpoint Security Web 外掛程式更新至最新版本。

- 如果在設定檔中啟用了"與 Kaspersky Sandbox 整合"設定，則"匯入應用程式設定檔"會以錯誤結束。在匯出應用程式設定前，請啟用 Kaspersky Sandbox。然後執行匯出/匯入程序。匯入設定檔後，請啟用 Kaspersky Sandbox。

- 從 KLP 檔案匯入政策時，用於確定是否接受 Kaspersky Detection and Response Expert 協議條款及條件的參數值不會套用。因此，匯入政策後，Kaspersky Endpoint Security 不會執行 EDR Agent 的功能。若要讓 EDR Agent 運作，請開啟政策，變更任一參數，然後儲存政策設定。

- 如果在執行 *IOC 掃描*工作時偵測到侵入指示，應用程式將僅隔離 FileItem 字詞的檔案。不支援隔離其它字詞的檔案。

- 管理警示詳情需要 Kaspersky Endpoint Security for Windows Web 外掛程式 11.7.0 或更新版本。使用 Endpoint Detection and Response 解決方案（EDR Optimum 和 EDR Expert）時需要警示詳情。偵測詳情僅在卡巴斯基安全管理中心網頁主控台或卡巴斯基安全管理中心雲端主控台中可用。

- 將 [KES+KEA] 設定遷移到 [KES+built-in agent] 設定可能會以 Kaspersky Endpoint Agent 應用程式移除錯誤完成。該應用程式移除錯誤在最新版本的 Kaspersky Endpoint Agent 中得到了修正。若要移除 Kaspersky Endpoint Agent，請重新啟動電腦並建立一個應用程式移除工作。

- 不支援 [KES+KEA+內建代理] 配置。此類配置會破壞應用程式與組織中部署的 Detection and Response 解決方案之間的交互。此外，在同一台電腦上使用 Kaspersky Endpoint Agent 和內建代理會導致重複遙測並增加電腦和網路的負載。遷移到 [KES + 內建代理] 配置後，請確保 Kaspersky Endpoint Agent 已從電腦中刪除。如果 Kaspersky Endpoint Agent 在遷移後繼續工作，請手動解除安裝應用程式（例如，使用*遠端解除安裝應用程式*工作）。

  安裝程式允許您在安裝了 Kaspersky Endpoint Security 和內建代理的電腦上部署 Kaspersky Endpoint Agent。Kaspersky Endpoint Agent 和內建代理也可以因為 *變更應用程式元件* 工作安裝在一台電腦上。該行為取決於 Kaspersky Endpoint Security 和 Kaspersky Endpoint Agent 的版本。

- 產生警示詳細資訊時，應用程式會提供有關偵測到的威脅的資訊，包括已修改檔案的雜湊。Kaspersky Endpoint Security 在產生提醒詳細資訊時計算檔案的雜湊值。請考慮產生檔案修改事件時檔案的原始雜湊可能與產生提醒詳細資料時計算的雜湊不同。

- 管理 EDR Optimum 和 Kaspersky Sandbox 元件需要 Kaspersky Endpoint Security for Windows Web 外掛程式 11.7.0 或更新版本。管理 EDR Expert 元件需要 Kaspersky Endpoint Security for Windows Web 外掛程式 11.8.0 或更新版本。如果您使用 Web 外掛程式建立了*變更應用程式元件*工作，而外掛程式不支援與這些元件合作，安裝程式將在安裝了 EDR Optimum、EDR Expert 或 Kaspersky Sandbox 的電腦上刪除這些元件。

- 內建代理 EDR (KATA) 會在電腦重新啟動後還原電腦的網路隔離，即使隔離期已過。為防止電腦重複隔離，您需要在 Kaspersky Anti Targeted Attack Platform 主控台中關閉網路隔離。

- 我們建議在網路隔離完成後升級應用程式。升級 Kaspersky Endpoint Security 後，可以停止網路隔離。

- EDR (KATA)、EDR Optimum 和 EDR 專家的內建代理彼此不相容。因此，如果您啟用了具有不同 EDR 功能的 Kaspersky Endpoint Security，則可以略過使用獨立 Kaspersky Endpoint Detection and Response 附加元件產品授權啟用 EDR 內建代理。例如，如果您已使用 [KES EDR Optimum] 產品授權啟用 Kaspersky Endpoint Security，則將略過使用獨立產品授權啟用 EDR (KATA) 內建代理。

- 在 Kaspersky Endpoint Security 版本 12.1 中，內建 EDR (KATA) 代理不支援 *獲取 NTFS 中繼檔*工作的以下中繼檔：$Secure:$SDH:$INDEX_ROOT；$Secure:$SDH:$INDEX_ALLOCATION；$Secure:$SDH:$BITMAP；$Secure:$SII:$INDEX_ROOT；$Secure:$SII:$INDEX_ALLOCATION；$Secure:$SII:$BITMAP；$Extend\$UsnJrnl:$J:$DATA；$Extend\$UsnJrnl:$Max:$DATA。對這些中繼檔的支援已新增到 Kaspersky Endpoint Security 12.2。

- 從 Kaspersky Endpoint Agent 遷移到 Kaspersky Endpoint Security 以用於 Kaspersky Anti Targeted Attack Platform (EDR) 解決方案時，您在將電腦連線到中央節點伺服器時可能會遇到錯誤。原因是網頁主控台中的遷移精靈略過了以下政策設定並且不遷移它們：

  - 設定修改禁止 **連線設定**（“鎖”）。

    預設情況下，設定可以被修改（“鎖”是開啟的）。因此，設定不會套用到電腦上。您必須禁止修改設定並關閉“鎖”。

  - 加密容器。

    如果您使用雙向身分驗證連線到中央節點伺服器，則必須重新新增加密容器。遷移精靈正確遷移了伺服器的 TLS 憑證。

管理主控台 (MMC) 中的政策和工作遷移精靈可遷移 Kaspersky Anti Targeted Attack Platform (EDR) 解決方案的所有設定。

- 當為了支援未連線到卡巴斯基安全管理中心的 Kaspersky Managed Detection and Response 解決方案、在 Endpoint Detection and Response Agent 模式中安裝應用程式時，應用程式啟動狀態會顯示不正確。BLOB 檔案下載後，Windows 工作列通知區域會顯示不正確的狀態：*應用程式未啟動*。不過，應用程式介面會顯示正確的啟動狀態。重新啟動電腦以使應用程式正常工作。

- Kaspersky Endpoint Security 允許使用 EDR (KATA) 元件或 Endpoint Sensor（不支援）與 Kaspersky Anti Targeted Attack Platform 解決方案整合。請注意，您只能使用其中一個元件與 Kaspersky Anti Targeted Attack Platform 互動。若要檢視元件狀態，請在管理主控台 (MMC) 中開啟電腦屬性，在**應用程式** 部分，開啟 Kaspersky Endpoint Security for Windows 的屬性，然後前往**元件**部分。以下特殊注意事項適用於與 Kaspersky Anti Targeted Attack Platform 互動的元件狀態顯示：

  - 對於管理外掛程式 12.0 及更早版本，應用程式顯示**端點感應器**的目前狀態。在 Kaspersky Endpoint Security 12.0 及更早版本中，EDR (KATA) 元件無法使用。EDR (KATA) 元件是在版本 12.1 中引入的。

  - 對於管理外掛程式 12.1 和以上版本，應用程式顯示**Endpoint Detection and Response (KATA)**的整體狀態，這可能表示 Endpoint Sensor 狀態或 EDR (KATA) 元件狀態。這取決於用戶電腦上安裝的應用程式版本以及可用於與 Kaspersky Anti Targeted Attack Platform 互動的可用元件。

- 從 Kaspersky Endpoint Security 版本 12.6 及更高版本開始，卡巴斯基安全管理中心網頁主控台版本 14.2 及更低版本將無法在電腦屬性中正確顯示 **Endpoint Detection and Response (KATA)** 元件的名稱。應用程式將不顯示 **Endpoint Detection and Response (KATA)**元件的名稱，而是顯示**Endpoint Detection and Response Expert (KATA EDR)**元件的名稱。若要檢視元件清單，請在網頁主控台中開啟電腦屬性，在**應用程式**部分，開啟 Kaspersky Endpoint Security for Windows 的屬性，然後前往**元件**部分。從卡巴斯基安全管理中心網頁主控台版本 15.1 及更高版本開始，應用程式可以正確顯示元件名稱。

- 將網頁主控台版本 14.0–14.2 中安裝的 Kaspersky Endpoint Detection and Response 管理外掛程式更新至版本 15.3 時，警示詳細資訊會顯示不正確。為了使警示詳細資訊正常運作，請重新啟動卡巴斯基安全管理中心管理伺服器。

- Kaspersky Endpoint Detection and Response 管理外掛程式版本 15.4 及更高版本不支援卡巴斯基安全管理中心版本 14.0。更新管理外掛程式後，警示詳細資訊會顯示不正確。

- Kaspersky Extended Detection and Response (XDR) 1.4 版解決方案不支援 Kaspersky Endpoint Security for Windows Web 外掛程式 12.12 版或更高版本。您可以保留目前的 Web 外掛程式版本，或將 XDR 解決方案更新至 2.0 版本或更高版本。

**其他限制**

- Windows 作業系統從版本 11 24H2 開始支援 UDP Receive Segment Coalescing Offload（URO）技術。如果電腦上安裝了相容的網路卡和驅動程式，則預設啟用該技術。在使用者的電腦上停用 URO 會顯著降低應用程式的效能。

- Kaspersky Endpoint Security 支援 WSL 子系統 (Windows Subsystem for Linux)，但有限制：

  - WSL 1。該應用程式會監控網路流量並透過 HTTP/HTTPS 偵測威脅。由於 Kaspersky Endpoint Security 使用自己的憑證掃描安全的 HTTPS 連線，某些協力廠商應用程式的運作可能會中斷。

  - WSL 2。該應用程式不支援 WSL 2。

- 如果該應用程式返回錯誤，或者在執行期間掛起，它可能會自動重新啟動。如果程式遇到反覆導致程式異常關閉的錯誤，它將執行以下操作：

  1. 停用控制和防護功能（加密功能仍啟用）。

  2. 通知使用者某些功能已被停用。

  3. 更新病毒資料庫或應用程式模組更新之後嘗試還原程式的功能。

- 新增到受信任清單的網址可能未正確處理。

- 在卡巴斯基安全管理中心主控台中，您無法將檔案從以下位置儲存到瓷碟：**進階 → 儲存區 → 活動威脅**資料夾。要儲存檔案，您必須解毒受感染的檔案。解毒時，應用程式會在備份中儲存檔案的副本。現在您可以將檔案從**進階 → 儲存區 → 備份**資料夾儲存到磁碟。

- 繼承資料傳輸到管理伺服器的設定（**一般設定 → 報告和儲存 → 到管理伺服器的資料傳輸**）與其他設定的繼承不同。如果您允許變更政策中的資料傳輸設定（"鎖"開啟），則這些設定將在主控台的本機電腦屬性中重置為預設值（如果之前未定義）。如果之前定義了這些設定，則它们的值將被還原。刪除政策時，將以相同的方式繼承設定。在這些情況下，本機電腦屬性中的其他設定將從政策繼承。

- Kaspersky Endpoint Security 監視符合 RFC 2616、RFC 7540、RFC 7541、RFC 7301 標準的 HTTP 通信。如果 Kaspersky Endpoint Security 在 HTTP 流量中偵測到另一種資料交換格式，則該應用程式將封鎖此連線，以防止從網際網路下載惡意檔案。

- Kaspersky Endpoint Security 阻止透過 QUIC 通訊協定進行通訊。無論在瀏覽器中是否啟用了 QUIC 支援，瀏覽器都使用標準傳輸通訊協定 (TLS or SSL)。

- 當協力廠商軟體使用 Libcurl 庫時，可能會出現 TLS 連線錯誤。這可能與 Kaspersky Endpoint Security 用於掃描加密連線使用的卡巴斯基憑證有關。要繼續工作，您可以停用協力廠商軟體的憑證驗證（不建議）或將卡巴斯基憑證本文新增到 cURL 憑證儲存。有關詳細資訊，請參閱卡巴斯基知識庫。

- 首次啟動 Kaspersky Endpoint Security for Windows 時，經過數位簽章的應用程式可能會暫時放置在錯誤的組中。經過數位簽章的應用程式將在以後放入正確的組中。

- 在重新掃描被協力廠商軟體封鎖的惡意物件的過程中，再次偵測到威脅時不會通知使用者。威脅重新偵錯事件將顯示在應用程式報告和卡巴斯基安全管理中心報告中。

- 關於裝置加密的卡巴斯基安全管理中心報告將不包含有關使用 Microsoft BitLocker 在未安裝裝置控制元件的伺服器平台或工作站上加密的裝置的資訊。

- 無法在卡巴斯基安全管理中心雲端主控台中啟用顯示所有報告條目。在網頁主控台中，您只可以變更顯示在報告中的條目的數目。預設情況下，卡巴斯基安全管理中心網頁主控台顯示 1000 條報告條目。您可以在管理主控台 (MMC) 中啟用顯示所有報告條目。

- 無法在卡巴斯基安全管理中心雲端主控台中設定顯示超過 1000 條報告條目。如果設定高於 1000 的值，卡巴斯基安全管理中心將只顯示 1000 條報告條目。

- 使用政策階層時，如果父政策禁止修改這些設定，則子政策中"卸除式磁碟機加密"部分的設定可以進行編輯。

- 您必須在作業系統設定中啟用"審核登入"，以確保防止共用資料夾被外部加密的排除項目正常運行。

- 如果啟用了共用資料夾防護，則 Kaspersky Endpoint Security for Windows 將監控在啟動 Kaspersky Endpoint Security for Windows 之前啟動的每個遠端存取工作階段加密共用資料夾（包括從其啟動了遠端存取工作階段的電腦是否已被新增到了排除項目中）的嘗試。如果您不希望 Kaspersky Endpoint Security for Windows 監控加密從被新增到排除項目的電腦上啟動、並且是從啟動 Windows Kaspersky Endpoint Security 之前啟動的遠端存取工作階段的共用資料夾的嘗試，請終止並重新啟動遠端存取工作階段或重新啟動安裝了 Windows Kaspersky Endpoint Security 的電腦。

- 如果更新工作是使用特定使用者帳戶的權限執行的，從需要授權的來源進行更新時，將不會下載產品修補程式。

- 由於系統效能不足，應用程式可能無法啟動。要解決此問題，請使用Ready Boot選項或增加啟動服務的作業系統超時。

- 應用程式無法在 Safe Mode 下工作。

- 在安裝應用程式後第一次重新啟動前，我們無法保證音訊控制能正常工作。

- 在管理主控台 (MMC) 中，在用來配置應用程式權限的侵入防護設定中，“**刪除**”按鈕不可使用。您可以透過應用程式的內容功能表從信任群組中刪除應用程式。

- 在應用程式的本機介面中，在侵入防護設定中，如果電腦由政策管理，則應用程式權限和受防護的資源不可使用。滾動、搜尋、篩選和其它視窗控制不可使用。您可以在卡巴斯基安全管理中心主控台的政策內容中檢視應用程式權限。

- 啟用旋轉的偵錯檔案時，不會為 AMSI 元件和 Outlook 外掛程式建立任何追蹤。

- 無法在 Windows Server 2008 中手動收集效能追蹤。

- 不支援“重新啟動”追蹤類型的效能追蹤。

- 對於 pico 處理程序，轉儲記錄不受支援。

- 關閉“**停用系統服務的外部管理(D)**”選項將不允許您停止使用`AMPPL=1`參數安裝的應用程式的服務（預設情況下，該參數值從 Windows 10RS2 作業系統版本開始設定為`1`）。值為`1`的`AMPPL`參數可將防護程序技術用於產品服務。

- 要執行資料夾的自訂掃描，啟動自訂掃描的使用者必須具有讀取此資料夾的屬性的權限。否則，自訂資料夾掃描將無法進行，並以錯誤結束。

- 如果政策中定義的掃描規則在末尾包含不帶`\`字元的路徑，例如`C:\folder1\folder2`，則將對路徑`C:\folder1\`執行掃描。

- 如果使用软体限制政策（Software Restriction Policies, SRP），則电脑可能無法加載（黑屏）。為了防止故障，您需要在 SRP 內容中允許使用應用程式庫。在 SRP 內容中，新增 khkum.dll 檔案的安全等級為“**不受限制**”的規則（**新雜湊規則**“功能表項）。該檔案位於 `C:\Program Files (x86)\Common Files\Kaspersky Lab\KES.12.12\klhk\klhk_x64\` 資料夾中。如果選擇了此方法，您還需要在 Kaspersky Endpoint Security 的*更新*工作設定中清除**下載應用程式模組更新**核取方塊。有關使用 SRP 的詳細資訊，請參閱 Microsoft 文件。

  您也可以停用 SRP，使用 Kaspersky Endpoint Security 的應用程式控制元件來控制應用程式使用。

- 如果電腦屬於 Windows 群組政策物件 (Group Policy Object, GPO) 下的網域，且DriverLoadPolicy參數被設定為 8（Good only），則重新啟動安裝了 Kaspersky Endpoint Security 的電腦會導致 BSOD。為了防止失敗，群組政策中的Early Launch Antimalware (ELAM) 參數必須設定為 1 (Good and unknown）。ELAM 設定位於政策中，在**Computer Configuration → Administrative Templates → System → Early Launch Antimalware**下面。

- 不支援透過 Rest API 管理 Outlook 外掛程式設定。
- 特定使用者的工作執行設定無法透過設定檔在裝置之間傳輸。從設定檔套用設定後，手動指定使用者名稱和密碼。
- 安裝更新後，完整性檢查工作將在重新啟動系統以套用更新之前不起作用。
- 透過遠端診斷實用程式變更旋轉的這種等級時，Kaspersky Endpoint Security for Windows 將錯誤顯示偵錯等級的空白值。但是，偵錯檔案是根據正確的偵錯等級編寫的。透過應用程式的本機介面變更旋轉的追蹤等級時，將正確修改追蹤等級，但是遠端診斷實用程式將錯誤顯示實用程式最後定義的追蹤等級。這可能會導致管理員沒有當前追蹤等級的最新資訊，並且如果使用者在應用程式的本機介面中手動變更追蹤等級，則追蹤中可能會缺少相關資訊。
- 在本機介面中，密碼防護設定不允許變更管理員帳戶的名稱（預設為 KLAdmin）。要變更管理員帳戶的名稱，需要停用密碼防護，然後啟用密碼防護並指定管理員帳戶的新名稱。
- 如果 Kaspersky Endpoint Security 應用程式安裝在 Windows Server 2019 伺服器上，其與 Docker 不相容。在安裝了 Kaspersky Endpoint Security 的電腦上部署 Docker 會引起崩潰 (BSOD)。
- 如果 Kaspersky Endpoint Security 安裝在 SQL Server DBMS 的伺服器上，應用程式會向伺服器實例傳送請求。這對於掃描 SQL Server 代理並阻止惡意作業執行必不可少。Kaspersky Endpoint Security 使用 SQL Server 使用者帳戶來掃描作業。應用程式在掃描系統記憶體時和更新病毒資料庫後向伺服器傳送請求。
- 與 Kaspersky Endpoint Security 和 Secret Net Studio 軟體的相容受限制：
  - Kaspersky Endpoint Security 應用程式與 Secret Net Studio 軟體的病毒防護元件不相容。

    應用程式無法安裝在使用病毒防護元件部署了 Secret Net Studio 的電腦上。若要允許交互操作，您必須從 Secret Net Studio 中刪除病毒防護元件。
  - Kaspersky Endpoint Security 應用程式與 Secret Net Studio 軟體的磁碟保護和資料加密元件不相容。

    應用程式無法安裝在使用磁碟保護和資料加密元件部署了 Secret Net Studio 的電腦上。若要允許交互操作，您必須從 Secret Net Studio 中刪除磁碟保護和資料加密元件。
  - Secret Net Studio 與 Kaspersky Endpoint Security 的檔案級加密 (FLE) 元件不相容。

    當您使用檔案級加密 (FLE) 元件安裝 Kaspersky Endpoint Security 時，Secret Net Studio 可能在操作時出錯。為了保證交互操作，您必須從 Kaspersky Endpoint Security 中刪除檔案級加密 (FLE) 元件。
- 匯入系統完整性監控規則時，應用程式會檢查規則的 ID 和名稱。如果規則 ID 相同，Kaspersky Endpoint Security 會將現有規則替換為新規則。匯出規則時，應用程式會自動指派 ID。例如，如果您手動編輯了已匯出的規則 XML 檔案，則可以存在具有相同 ID 的規則。如果規則 ID 為唯一，但規則名稱相同，Kaspersky Endpoint Security 會新增 `(1)` 等等到規則的名稱。
- 從 Kaspersky Endpoint Security for Windows的 12.11 版本開始，無法在網頁主控台中檢視在子群組中開啟的父政策的設定。網頁主控台還會顯示警告：*該政策是繼承的。您僅可以在建立政策的管理群組編輯政策設定。*
- 超過 256 個字元的彈出通知不會顯示在管理主控台 (MMC) 中。

# 詞彙表

## Cloud Discovery

Cloud Discovery 管理使用者對雲端服務的存取。雲端服務包括（舉例）Microsoft Teams、Salesforce、Microsoft Office 365。雲端服務按類別分組，例如*檔案共用*、*Messengers*、 *電子郵件*。

## Integration Server

Kaspersky Endpoint Security for Virtualization Light Agent 元件。Kaspersky Endpoint Security 元件與虛擬基礎結構之間進行互動。

## IOC

元件指示器。一個有關惡意物件或者活動的資料集合。

## IOC 檔案

一個包含應用程式試圖匹配以計數偵測的洩露指示器 (IOC) 集合的檔案。如果經過掃描為物件找到了與多個 IOC 檔案的精確匹配，則偵測可能性更高。

## Kerberos 身分驗證

用戶端和伺服器在建立連線之前進行相互認證的機制，使得透過不安全的網路進行通訊成為可能。該機制基於票據，使用者可從可信任身分驗證中心獲得該票據。

## Light Agent

Kaspersky Endpoint Security for Virtualization Light Agent 元件。它安裝在每個需要防護的虛擬機上。

## OLE 物件

附加的檔案或嵌入到其他檔案中的檔案。Kaspersky 應用程式允許掃描 OLE 物件以尋找病毒。例如，如果您在 Microsoft Office Word 手冊中插入一個 Microsoft Office Excel® 表格，此表格將作為 OLE 物件被掃描。

## OpenIOC

基於 XML 的洩露指示器 (IOC) 開放標準說明，包括超過 500 個不同的洩露指示器。

## SVM

安全虛擬機 – 上面安裝了 scanserver 服務（Protection Server，一個 Kaspersky Endpoint Security for Virtualization Light Agent 的元件）的特殊虛擬機。

## 受信任平台模組

一個與安全相關的提供基本功能的微晶片（例如用於儲存加密金鑰）。受信任平台模組通常安裝在電腦主機板上並且透過硬體匯流排與其他所有系統元件進行互動。

## 受感染的檔案

包含惡意程式碼（在掃描檔案時偵測到已知惡意軟體的代碼）的檔案。Kaspersky 建議您不要使用此類別檔案，原因是它們可能會感染您的電腦。

## 可疑網頁位址資料庫

其內容被視為存在危險的網址清單。這是一個由 Kaspersky 專家建立的清單。它會定期更新，並且會包含在 Kaspersky 應用程式分發套件中。

## 存檔

封裝到單一壓縮檔案的一個或幾個檔案。需要一個名叫 archiver 的應用程式以開啟和解包資料。

## 工作

卡巴斯基應用程式作為工作要執行的功能，例如：即時檔案防護、完整裝置掃描、資料庫更新。

## 已感染檔案

根據檔案的結構或格式，某些檔案可能會作為儲存和傳播惡意程式碼的"容器"而成為入侵者的工具。一般來說，此類別檔案是可執行檔，例如副檔名為 .com、.exe 和 .dll 的檔案。有相當高的風險此類檔案中有惡意代碼侵入。

## 憑證發佈者

發佈憑證的認證中心。

## 掃描範圍

Kaspersky Endpoint Security 在執行掃描工作時掃描的物件。

## 授權憑證

與金鑰檔案或啟動碼一起由 Kaspersky 傳輸給使用者的檔案。此檔案包含授予使用者的產品授權資訊。

## 攜帶式檔案管理器

這是一個應用程式，用於在電腦上沒有加密功能時透過提供的介面處理卸除式磁碟機上的加密檔案。

## 啟動金鑰

程式目前正在使用的金鑰。

## 病毒資料庫

資料庫包含截至病毒資料庫發佈之日 Kaspersky 已知的電腦安全威脅的資訊。病毒資料庫簽章有助於偵測掃描物件中的惡意代碼。病毒資料庫由 Kaspersky 建立並且每小時都會更新。

## 管理群組

一組共用一般功能的裝置和一組在這些裝置上安裝的 Kaspersky 應用程式。將裝置歸類在群組是為了讓您輕易的把電腦群當作一台電腦進行管理。一個群組可能包含其他的群組。您可以為群組中每個安裝的應用程式建立群組政策和群組工作。

## 網路代理

一個卡巴斯基安全管理中心模組，它實現了管理伺服器和特定網路節點（工作站或伺服器）上安裝的 Kaspersky 應用程式之間的互動。此元件對在 Windows 下執行的所有 Kaspersky 應用程式通用。網路代理的獨立版本是為在其他作業系統下執行的應用程式而設計。

## 網頁資源位址的正規表示式

網頁資源的正規表示式位址是透過正規化獲得的網頁資源位址的文字表達。*正規化*是一個網頁資源位址文字表達根據特定規則而改變的過程，例如從網頁資源位址的文字表示中排除使用者登入、密碼和連線連接埠；此外網頁資源位址的字元將從大寫變更為小寫。

在防護元件的執行中，正規化網頁資源位址的目的是為了防止再次掃描實際上等效但是語法不同的網站位址。

範例:
非正規表示式的位址: www.Example.com\。
正規表示式的位址: www.example.com。

## 解毒

能夠完全或部分還原物件資料的一種處理已感染物件的處理方式。並非所有受感染的物件都能被解毒。

## 誤報

當 Kaspersky 應用程式由於未受感染檔案的簽章與病毒的簽章類似而將其報告為受感染的檔案時，稱為誤報。

## 身分驗證代理

可啟動硬碟磁碟機加密後，讓您完成身分驗證以存取加密的硬碟磁碟機並載入作業系統啟動的介面。

## 遮罩

使用萬用字元表示檔案名稱和副檔名。

檔案遮罩可包含檔案名稱中允許使用的任何字元，包括萬用字元：

- `*`（星號）字元代表任意一組字元，但 `\` 和 `/` 字元除外（這兩個字元是檔案和資料夾路徑中的檔案和資料夾名稱的分隔符號）。例如，遮罩"`C:\*\*.txt`"將包括位於 C: 磁碟機但是不在子資料夾中所有帶 TXT 副檔名的檔案的路徑。

- 兩個連續 `*` 字元在檔案或資料夾名稱中代表任意一組字元（包括空集），包括 `\` 和 `/` 字元（這兩個字元是檔案和資料夾路徑中的檔案和資料夾名稱的分隔符號）。例如，遮罩 `C:\Folder\**\*.txt` 將包括位於巢嵌在 `Folder` 內的資料夾（`Folder` 自身除外）中所有帶 TXT 副檔名的檔案的路徑。遮罩必須包含至少一個嵌套等級。遮罩 `C:\**\*.txt` 不是有效遮罩。**遮罩僅可用於建立掃描排除項目。

- `?`（問號）字元代表任意單個字元，但 `\` 和 `/` 字元除外（這兩個字元是檔案和資料夾路徑中的檔案和資料夾名稱的分隔符號）。例如，遮罩 `C:\Folder\???.txt` 將包括位於 `Folder` 資料夾中所有帶 TXT 副檔名且名稱由三個字元構成的檔案的路徑。

## 釣魚網頁位址資料庫

Kaspersky 專家確定與網路釣魚相關的網址清單。此資料庫會定期更新，並且會包含在 Kaspersky 應用程式分發套件中。

## 防護範圍

在執行時被關鍵威脅防護元件持續掃描的物件。不同元件的防護範圍有不同的參數。

# 附錄

本節包含的資訊是對文件本文的補充。

# 附錄 1。應用程式設定

您可以使用政策、工作或應用程式介面來配置 Kaspersky Endpoint Security。有關應用程式元件的詳細資訊，請參見相應章節。

## 檔案威脅防護

“檔案威脅防護”元件允許您防止電腦的檔案系統受到感染。預設情況下，檔案威脅防護元件會永久駐留在電腦的 RAM 中，並即時掃描所有開啟、儲存或執行的檔案。該元件會掃描所有電腦磁碟機（包括已連線的磁碟機）上的檔案。該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來提供電腦防護。

該元件將掃描使用者或應用程式存取的檔案。如果偵測到惡意檔案，Kaspersky Endpoint Security 將封鎖檔案操作。應用程式隨後將根據“檔案威脅防護”元件的設定來清除或刪除惡意檔案。

當嘗試存取其內容位於 OneDrive 雲端儲存中的檔案時，Kaspersky Endpoint Security 會下載並掃描檔案內容。

檔案威脅防護元件設定

| 參數 | 描述 |
| --- | --- |
| **安全等級**<br>*（僅在管理主控台（MMC）和 Kaspersky Endpoint Security 介面中可用）* | 對於檔案威脅防護，Kaspersky Endpoint Security 可以套用不同的設定群組。這些儲存在應用程式中的設定群組稱為“*安全防護等級*”：<br>• **高**選擇此檔案安全等級後，“檔案威脅防護”元件將對開啟、儲存和執行的所有檔案實施最嚴格的控制。“檔案威脅防護”元件會掃描電腦的所有硬碟磁碟機、卸除式磁碟機和網路磁碟機上的所有檔案類型。它還掃描存檔、安裝套件和嵌入式 OLE 物件。<br>• **建議**Kaspersky Lab 專家建議此檔案安全等級。“檔案威脅防護”元件僅掃描電腦的所有硬碟磁碟機、卸除式磁碟機和網路磁碟機上的指定檔案格式，以及嵌入式 OLE 物件。“檔案威脅防護”元件不掃描壓縮套件或安裝套件。<br>• **低**此檔案安全等級的設定可確保最大掃描速度。“檔案威脅防護”元件僅掃描電腦的所有硬碟磁碟機、卸除式磁碟機以及網路磁碟機上擁有指定副檔名的檔案。“檔案威脅防護”元件不掃描複合檔案。 |
| **檔案類型**<br>*（僅在管理主控台（MMC）和 Kaspersky Endpoint Security 介面中可用）* | **所有檔案**如果啟用該設定，Kaspersky Endpoint Security 將毫無例外地掃描所有檔案（所有格式和副檔名）。<br>**按格式掃描檔案**如果啟用該設定，則應用程式僅掃描被感染的檔案。在掃描檔案以尋找惡意程式碼之前，系統將分析檔案的內部頭以確定檔案的格式（例如，.txt、.doc 或 .exe）。掃描還會查找具有特定副檔名的檔案。<br>**按副檔名掃描檔案**如果啟用該設定，則應用程式僅掃描被感染的檔案。此時，系統將根據檔案的副檔名確定檔案格式。 |
| **掃描範圍** | 包含“檔案威脅防護”元件掃描的物件。掃描物件可能是硬碟、卸除式磁碟機、網路磁碟機、資料夾、檔案或由遮罩定義的多個檔案。<br>預設情況下，“檔案威脅防護”元件將掃描任何硬碟、網路磁碟機或卸除式磁碟機中啟動的檔案。無法變更或刪除這些物件的防護範圍。您只可以從掃描中排除項（例如卸除式磁碟機）。 |
| **機器學習和簽章分析**<br>*（僅在管理主控台（MMC）和 Kaspersky Endpoint Security 介面中可用）* | 機器學習和簽章分析使用 Kaspersky Endpoint Security 資料庫，其中包含已知威脅的敘述以及消除它們的方法。使用此方法的防護提供了可接受的最低安全等級。<br>根據 Kaspersky 專家的建議，機器學習和簽章分析始終啟用。 |

| 參數 | 描述 |
| --- | --- |
| **啟發式分析**<br>*（僅在管理主控台（MMC）和 Kaspersky Endpoint Security 介面中可用）* | 開發該技術的目的是偵測使用 Kaspersky 應用程式資料庫無法偵測到的威脅。它可以偵測受未知病毒或已知病毒新變種感染的可疑檔案。<br>掃描檔案中的惡意代碼時，啟發式分析器將執行可執行檔案中的指令。啟發式分析器執行的指令數取決於為啟發式分析器指定的級別。啟發式分析等級可在全面搜尋新威脅、載入作業系統資源和啟發式分析持續時間之間進行平衡。 |
| **偵測到威脅後的動作** | **解毒；若解毒失敗則刪除**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。<br>**解毒；若解毒失敗則封鎖**如果選擇該選項，Kaspersky Endpoint Security 將自動對已經偵測到的所有受感染的檔案執行解毒操作。如果解毒失敗，Kaspersky Endpoint Security 將阻止檔案（讀取/寫入）。<br>**封鎖**如果選擇該選項，"檔案威脅防護"元件將自動封鎖所有受感染的檔案，而不對其進行解毒處理。<br>在嘗試解毒或刪除受感染的檔案之前，應用程式會建立該檔案的備份副本，以防您需要還原該檔案或將來可以對其進行解毒。 |
| **只掃描新增及修改的檔案** | 僅掃描新檔案和自上次掃描以來已被修改的檔案。這有助於縮短掃描的持續時間。此模式適用於簡單檔案和複合檔案。 |
| **掃描壓縮檔案** | 掃描 ZIP、GZIP、BZIP、RAR、TAR、ARJ、CAB、LHA、JAR、ICE 和其它存檔。應用程式不僅依照副檔名而且依照格式掃描存檔。當檢查封存時，應用程式會執行巡迴解壓縮。這可讓人偵測多層封存（封存內的封存）內的威脅。 |
| **掃描分發套件** | 掃描協力廠商應用程式的分發套件。 |
| **掃描 Microsoft Office 格式的檔案** | 掃描 Microsoft Office 檔案（DOC、DOCX、XLS、PPT 和其他 Microsoft 副檔名）。Office 格式檔案也包含 OLE 物件。應用程式掃描小於 1MB 的 office 格式檔案，無論該核取方塊是否被選中。 |
| **掃描電子郵件格式檔案** | 掃描電子郵件格式的檔案。應用程式掃描 MSG 和 EML 檔案。電子郵件格式檔案也包含 OLE 物件和 MHT 檔案。Kaspersky Endpoint Security 掃描小於 1MB 的電子郵件格式檔案，無論該核取方塊是否被選中。 |
| **不解壓縮大型複合檔案** | 如果選中該核取方塊，應用程式不會掃描其大小超過指定值的複合檔案。<br>如果清除該核取方塊，應用程式將掃描所有大小的複合檔案。<br>應用程式會掃描從存檔中提取的大檔案，而不管是否選中該核取方塊。 |
| **在背景解壓縮複合檔案** | 如果選中該核取方塊，應用程式會提供對大於指定值的複合檔案的存取權限，然後再掃描這些檔案。在這種情況下，Kaspersky Endpoint Security 在背景解壓並掃描複合檔案。<br>對於小於該值的複合檔案，只有在解壓和掃描這些檔案後，應用程式才會提供對這些檔案的存取權限。<br>如果未選中該核取方塊，則只有在解壓和掃描任何大小的複合檔案後，應用程式才會提供對這些檔案的存取權限。 |
| **掃描模式**<br>*（僅在管理主控台（MMC）和 Kaspersky Endpoint Security 介面中可用）* | Kaspersky Endpoint Security 掃描由使用者、作業系統或以使用者帳戶執行的應用程式存取的檔案。<br>**智慧模式**在此模式中，檔案威脅防護將基於對物件所做操作進行分析以掃描物件。例如，當操作某個 Microsoft Office 手冊時，Kaspersky Endpoint Security 將在其首次開啟和最後一次關閉時掃描該檔案。覆蓋檔案的操作過程不會掃描檔案。<br>**在存取及修改時**在該模式中，檔案威脅防護將在出現開啟/修改檔案的嘗試時掃描物件。<br>**存取時**在此模式中，檔案威脅防護將在出現開啟/修改檔案的嘗試時掃描物件。<br>**執行時**在該模式中，檔案威脅防護僅在出現執行檔案的嘗試時掃描物件。 |
| **使用 iSwift 技術**<br>*（僅在管理主控台（MMC）和 Kaspersky Endpoint Security 介面中可用）* | 該技術允許透過排除特定檔案不掃描的方式提高掃描速度。該技術將使用特殊演算法將檔案排除在掃描範圍之外，該演算法會考慮 Kaspersky Endpoint Security 資料庫的發佈日期、檔案的上次掃描日期以及對掃描設定的任何修改。iSwift 技術是對用於 NTFS 檔案系統的 iChecker 技術的增強版。 |
| **使用 iChecker 技術**<br>*（僅在管理主控台（MMC）和 Kaspersky Endpoint Security 介面中可用）* | 該技術允許透過排除特定檔案不掃描的方式提高掃描速度。該技術將使用特殊演算法將檔案排除在掃描範圍之外，該演算法會考慮 Kaspersky Endpoint Security 資料庫的發佈日期、檔案的上次掃描日期以及對掃描設定的任何修改。iChecker 技術受到幾個限制：它無法操作大檔案，並且僅能套用至擁有程式可辨識結構的檔案 (例如：.exe、.dll、.lnk、.ttf、.inf、.sys、.com、.chm、.zip 和 .rar)。 |

| 參數 | 描述 |
| --- | --- |
| **暫停檔案威脅防護**<br>*（僅在管理主控台（MMC）和 Kaspersky Endpoint Security 介面中可用）* | 在指定的時間或使用指定的應用程式時，這會臨時自動暫停檔案威脅防護的操作。 |
| **掃描在 Windows 容器中排除的檔案操作** | 如果在容器內偵測到威脅，應用程式將套用 為檔案威脅防護元件所選擇的操作。<br>**如果清除失敗則停止容器**應用程式對於偵測到的物件可能沒有足夠的讀寫權限。在這種情況下，不可能對檢測到的物件進行解毒或刪除。如果選取此核取方塊，應用程式將封鎖偵測到的物件並停止容器。如果清除此核取方塊，應用程式將僅封鎖偵測到的物件。<br>**不掃描在 Windows 容器中排除的檔案操作**如果選取該核取方塊，則應用程式僅在容器啟動時掃描容器。如果清除該核取方塊，應用程式將即時連續掃描容器。 |

# 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，同時封鎖惡意網站和釣魚網站。該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來提供電腦防護。

Kaspersky Endpoint Security 掃描 HTTP、HTTPS 和 FTP 流量。Kaspersky Endpoint Security 掃描 URL 和 IP 位址。

若要使用 Web 威脅防護，您必須完成應用程式的初始設定：

- 對於 HTTPS 流量監控， 啟用加密連線掃描 （預設為啟用）。
- 選擇 Kaspersky Endpoint Security 必須監控的連接埠（預設情況下，應用程式監控所有連接埠）。
- 選擇您希望 Kaspersky Endpoint Security 監控其流量的應用程式。大多數瀏覽器已出現在卡巴斯基推薦的應用程式清單中。如果清單中缺少您的瀏覽器，請手動新增。
- 我們建議 將網頁交互指令碼注入到 Web 流量中 （預設情況下，指令碼注入被停用）。此指令碼可啟用為應用程式事件日誌、OS 事件日誌和報告註冊 Web 威脅防護事件。

當使用者嘗試開啟惡意網站或釣魚網站時，Kaspersky Endpoint Security 將封鎖其存取並顯示警告（請參見下圖）。




網站存取被拒絕的訊息

Web 威脅防護元件設定

| 參數 | 描述 |
| --- | --- |
| **安全等級**<br>*（僅在管理主控台（MMC）和 Kaspersky Endpoint Security 介面中可用）* | 對於 Web 威脅防護，應用程式可以套用不同的設定群組。這些儲存在應用程式中的設定群組稱為*"安全防護等級"*：<br>• **高**在此安全等級下，"Web 威脅防護"元件對電腦透過 HTTP 和 FTP 收到的 Web 流量執行最大限度的掃描。"Web 威脅防護"使用整個程式應用資料庫詳細掃描所有 Web 流量物件，並盡可能執行最深度的啟發式分析。<br>• **建議**該安全等級在應用程式的效能和 Web 流量的安全之間提供最佳平衡。"Web 威脅防護"元件執行中度掃描等級的啟發式分析。Kaspersky 專家建議使用此 Web 流量安全等級。<br>• **低**此 Web 流量安全等級的設定可確保最快的 Web 流量掃描速度。"Web 威脅防護"元件執行輕度掃描等級的啟發式分析。 |
| **偵測到威脅後的動作** | **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。<br>**通知**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"元件將允許此物件下載到電腦，但會將受感染物件的相關資訊新增到活動威脅清單中。 |
| **檢查網址是否在惡意網址資料庫中**<br>*（僅在管理主控台（MMC）和 Kaspersky Endpoint Security 介面中可用）* | 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。 |
| **使用啟發式分析**<br>*（僅在管理主控台（MMC）和 Kaspersky Endpoint Security 介面中可用）* | 開發該技術的目的是偵測使用 Kaspersky 應用程式資料庫無法偵測到的威脅。它可以偵測受未知病毒或已知病毒新變種感染的可疑檔案。<br>當掃描網路流量中的病毒和其他構成威脅的應用程式時，啟發式分析將在可執行檔案中執行指令。啟發式分析器執行的指令數取決於為啟發式分析器指定的級別。啟發式分析等級可在全面搜尋新威脅、載入作業系統資源和啟發式分析持續時間之間進行平衡。 |
| **檢查網址是否在釣魚網址資料庫中**<br>*（僅在管理主控台（MMC）和 Kaspersky Endpoint Security 介面中可用）* | 釣魚網址資料庫包含目前用於啟動釣魚攻擊的已知網站的位址。卡巴斯基使用從名為"釣魚防護工作組"的國際組織獲得的位址來補充網路釣魚連線資料庫。釣魚位址資料庫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。 |
| **不掃描受信任網址的 Web 流量** | 如果選擇此選項，"Web 威脅防護"元件將不再掃描其網址包含在受信任網址清單中的網頁或網站的內容。您可以將網頁/網站的特定位址和位址遮罩新增至受信任網址清單。<br>您也可以建立一個通用加密連線排除項目清單。在此情況下，當 Web 威脅防護、郵件威脅防護、Web 控制元件執行工作時，Kaspersky Endpoint Security 不掃描受信任網址的 HTTPS 流量。 |

# 郵件威脅防護

"郵件威脅防護"元件掃描傳送和接收電子郵件的附件是否有病毒和其他威脅。該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來提供電腦防護。

郵件威脅防護可以掃描傳入和傳出的郵件。該應用程式在以下郵件用戶端中支援 POP3、SMTP、IMAP 和 NNTP：

- Microsoft Office Outlook
- Mozilla Thunderbird
- Windows Mail
- MyOffice Mail
- R7-Office Organizer

若要掃描 Mozilla Thunderbird、MyOffice Mail 及 R7-Office Organizer 郵件用戶端的流量，您需要將卡巴斯基憑證新增至專屬憑證儲存區，並選擇該專屬憑證儲存區。

郵件威脅防護不支援其他協定和郵件用戶端。

郵件威脅防護並不總是能夠獲得*協定級別*的郵件存取權限（例如，當使用 Microsoft Exchange 解決方案時）。為此，郵件威脅防護包括 Microsoft Office Outlook 延伸程式。該延伸程式允許在*郵件用戶端級別*掃描郵件。郵件威脅防護延伸支援 Outlook 2010、2013、2016、2019 和 2021 的操作。

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。

如果在附件中偵測到惡意檔案，Kaspersky Endpoint Security 會將有關已執行操作的資訊新增到郵件主旨，例如，*[郵件已處理] <郵件主旨>*。

郵件威脅防護元件設定

| 參數 | 描述 |
| --- | --- |
| **安全等級**<br>*（僅在管理主控台（MMC）和 Kaspersky Endpoint Security 介面中可用）* | 對於郵件威脅防護，應用程式可以套用不同的設定群組。這些儲存在應用程式中的設定群組稱為"*安全防護等級*"：<br>• **高**選擇此電子郵件安全等級時，"郵件威脅防護"元件會最徹底地掃描電子郵件。"郵件威脅防護"元件將掃描傳送和接收的電子郵件訊息，並執行深度啟發式分析。對於高風險環境，建議使用"高"郵件安全防護等級。這種情況的一個例子就是，未獲得集中式電子郵件防護的家用網路連線免費的電子郵件服務。<br>• **建議**此電子郵件安全等級在應用程式的效能和電子郵件安全性之間提供最佳平衡。"郵件威脅防護"元件將掃描傳送和接收的電子郵件，並執行中度啟發式分析。Kaspersky 專家建議採用這一郵件流量安全等級。<br>• **低**選擇此電子郵件安全等級時，"郵件威脅防護"元件只掃描接收的電子郵件訊息，執行輕度啟發式分析，不掃描電子郵件的壓縮套件附件。在這一郵件安全等級中，"郵件威脅防護"元件將使用最少的作業系統資源，以最大速度掃描電子郵件。在防護良好的環境中工作時，建議使用"低"郵件安全等級。這類環境的一個例子是具有集中式電子郵件防護的企業區域網路。 |
| **偵測到威脅後的動作** | **解毒；若解毒失敗則刪除**在入站或出站郵件中偵測到受感染的物件時，應用程式會嘗試對偵測到的物件進行解毒。使用者將能夠存取帶安全附件的郵件。如果無法解毒物件，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到郵件主旨，例如，*[郵件已處理] <郵件主旨>*。<br>**解毒；若解毒失敗則封鎖**在入站郵件中偵測到受感染的物件時，應用程式會嘗試對偵測到的物件進行解毒。使用者將能夠存取帶安全附件的郵件。如果無法解毒物件，應用程式會將警告新增到郵件主旨。使用者將能夠存取帶原始附件的郵件。在出站郵件中偵測到受感染的物件時，應用程式會嘗試對偵測到的物件進行解毒。如果無法解毒物件，應用程式會封鎖郵件的傳輸，郵件使用者端會顯示錯誤。<br>**封鎖**如果在入站郵件中偵測到受感染的物件，應用程式會將警告新增到郵件主旨。使用者將能夠存取帶原始附件的郵件。如果在出站郵件中偵測到受感染的物件，應用程式會封鎖郵件的傳輸，郵件使用者端會顯示錯誤。 |

| 參數 | 描述 |
| --- | --- |
| **防護範圍**<br>*（僅在管理主控台（MMC）和 Kaspersky Endpoint Security 介面中可用）* | *防護範圍*包括元件執行時檢查的物件： 接收和傳送的郵件或僅接收的訊息 。<br>為了防護您的電腦，您只需要掃描傳入的郵件。您可以開啟對傳出郵件的掃描功能，以防止受感染的檔案在存檔中傳送。如果要防止傳送特定格式的檔案（例如音訊和視訊檔案），您也可以開啟傳出郵件的掃描功能。 |
| **掃描 POP3、SMTP、NNTP 和 IMAP 流量** | "郵件威脅防護"元件掃描透過 POP3、SMTP、NNTP 和 IMAP 協定傳送的流量。 |
| **連線 Microsoft Outlook 延伸程式** | 如果選中該核取方塊，則在 Microsoft Outlook 中集成的延伸程式一側啟用對透過 POP3、SMTP、NNTP、IMAP 協定傳輸的電子郵件的掃描。<br>如果使用 Microsoft Outlook 的延伸程式掃描郵件，建議使用Cached Exchange Mode。有關 Cached Exchange 模式的詳細資訊和對其用途的建議，請參閱 Microsoft 知識庫。 |
| **啟發式分析**<br>*（僅在管理主控台（MMC）和 Kaspersky Endpoint Security 介面中可用）* | 開發該技術的目的是偵測使用 Kaspersky 應用程式資料庫無法偵測到的威脅。它可以偵測受未知病毒或已知病毒新變種感染的可疑檔案。<br>掃描檔案中的惡意代碼時，啟發式分析器將執行可執行檔案中的指令。啟發式分析器執行的指令數取決於為啟發式分析器指定的級別。啟發式分析等級可在全面搜尋新威脅、載入作業系統資源和啟發式分析持續時間之間進行平衡。 |
| **掃描附件中的壓縮檔案** | 掃描 ZIP、GZIP、BZIP、RAR、TAR、ARJ、CAB、LHA、JAR、ICE 和其它存檔。應用程式不僅依照副檔名而且依照格式掃描存檔。當檢查封存時，應用程式會執行巡迴解壓縮。這可讓人偵測多層封存（封存內的封存）內的威脅。<br>如果在掃描期間應用程式在郵件的文字中偵測到存檔的密碼，該密碼將被用來掃描惡意應用程式的存檔的內容。在此情況下不儲存密碼。存檔在掃描期間被解壓縮。如果在解壓縮過程中發生應用程式錯誤，您可以手動刪除儲存到以下路徑的解壓縮檔案： %systemroot%\temp。這些檔案有 PR 前綴。 |
| **掃描 Microsoft Office 格式的附加檔案** | 掃描 Microsoft Office 檔案（DOC，DOCX，XLS，PPT 和其他 Microsoft 副檔名）。Office 格式檔案也包含 OLE 物件。應用程式掃描小於 1 MB 的 office 格式檔案，無論該核取方塊是否被選中。 |
| **不掃描大於該值的存檔 N MB 的存檔** | 如果選擇此方塊，"郵件威脅防護"元件將在掃描中排除大小超過指定值的電子郵件附件。如果清空此方塊，則"郵件威脅防護"元件可以掃描任意尺寸的電子郵件附件。 |
| **限制壓縮檔案的檢查時間為 N 秒** | 如果選擇此方塊，則分配的用於掃描電子郵件壓縮檔案附件的時間將被限制為指定的長度。 |
| **附件篩選** | 附件篩選器不適用於發出的電子郵件。<br>**停用篩選功能**如果選擇此選項，"郵件威脅防護"元件將不篩選屬於電子郵件附件的檔案。<br>**重新命名選取類型的附件**如果選擇此選項，郵件威脅防護元件將用下劃線字符（例如，attachment.doc__）替換在指定類型的附件檔案中找到的最後一個延伸字符。因此，為了開啟檔案，使用者必須重命名檔案。<br>**刪除選取類型的附件**如果選擇此選項，"郵件威脅防護"元件將從電子郵件中刪除指定的附件類型。<br>在檔案遮罩清單中，可以指定要重命名或從電子郵件中刪除的附加檔案的類型。 |

# 網路威脅防護

*網路威脅防護*元件（也稱為入侵偵測系統，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。

| 參數 | 描述 |
| --- | --- |
| **將連接埠掃描和網路洪水當做攻擊處理** | *網路泛洪*是對組織的網路資源（例如 Web 伺服器）的攻擊。這種攻擊包括傳送大量請求以超載網路資源的帶寬。發生這種情況時，使用者將無法存取組織的網路資源。<br>*連接埠掃描*攻擊包括掃描電腦上的 UDP 連接埠、TCP 連接埠和網路服務。此攻擊使攻擊者可以在進行更危險類型的網路攻擊之前確定電腦的漏洞程度。連接埠掃描還使攻擊者能夠識別電腦上的作業系統，並為該作業系統選擇適當的網路攻擊。<br>若選中此核取方塊，則 Kaspersky Endpoint Security 將監控網路流量以偵測這些攻擊。如果偵測到攻擊，應用程式會通知使用者並將相應事件傳送到卡巴斯基安全管理中心。該應用程式提供有關攻擊電腦的資訊，這對於及時採取威脅響應操作很有必要。<br>如果某些允許的應用程式執行這些類型攻擊的典型操作，您可以停用對這些類型攻擊的偵測。這將有助於避免誤報。 |
| **封鎖攻擊裝置 N 分鐘** | 如果啟用此選項，"網路威脅防護"元件將把發動攻擊的電腦新增至封鎖清單。這意味著，"網路威脅防護"元件將會在該攻擊電腦的首次網路攻擊嘗試後的指定時間段內，封鎖與該電腦的網路連線。此封鎖操作將會自動防護電腦避免以後來自同一位址的攻擊。攻擊電腦必須待在封鎖清單中的最短時間為一分鐘。最長時間為 999 分鐘。<br>您可以在"網路監控工具"視窗中檢視封鎖清單。<br>重新啟動應用程式以及變更網路威脅防護設定時，Kaspersky Endpoint Security 會清除封鎖清單。 |
| **排除項目** | 此清單包含某些 IP 位址，"網路威脅防護"不會封鎖這些 IP 位址發起的網路攻擊。<br>您可以新增具有指定連接埠和協定的 IP 位址。<br>應用程式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。 |
| **MAC 欺騙防護** | *MAC 欺騙攻擊*包括變更網路裝置（網卡）的 MAC 位址。結果，攻擊者可以將傳送到某台裝置的資料重新導向到另一台裝置，並獲得對該資料的存取權限。Kaspersky Endpoint Security 允許您封鎖 MAC 欺騙攻擊並接收關於攻擊的通知。 |

# 防火牆

在網際網路或區域網路上工作時，防火牆會封鎖未經授權的電腦連線。防火牆還控制腦上應用程式的網路活動。這允許您防護公司區域網路免受身分竊盜和其他攻擊。該元件借助防毒資料庫、卡巴斯基安全網路雲端服務和預先定義的*網路規則*來提供電腦防護。

網路代理用於與卡巴斯基安全管理中心進行交互。防火牆會自動建立應用程式和網路代理正常工作所需的網路規則。結果，防火牆在电脑上開啟了多個連接埠。哪個連接埠開啟取決於电脑的角色（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。

## 網路規則

您可以在以下等級配置網路規則：

- *網路封包規則*。網路封包規則將對網路封包進行限制，與應用程式無關。此類規則將限制透過特定連接埠的選定資料協定傳送和接收的網路流量。Kaspersky Endpoint Security 具有預先定義的網路封包規則，其中的權限由 Kaspersky 專家推薦。
- *應用程式網路規則*。應用程式網路規則將對特定應用程式的網路活動進行限制。它們不僅將網路封包的特徵列入重要參考因素，還把接收或傳送此網路封包的應用程式列入重要參考因素中。

應用程式對作業系統資源、處理程序和個人資料的控制存取由"主機入侵防禦"元件透過*應用程式權限*提供。

在應用程式首次啟動期間，“防火牆”會執行以下操作：

1. 使用下載的防毒資料庫檢查應用程式的安全性。
2. 在卡巴斯基安全網路中檢查應用程式安全性。

   建議您加入卡巴斯基安全網路以幫助“防火牆”元件更有效地工作。
3. 將應用程式放置在其中一個信任群組中：*受信任*，*低限制*，*高限制*，*不信任*。

   信任群組定義了在控制應用程式活動時 Kaspersky Endpoint Security 所引用的權限。Kaspersky Endpoint Security 會將應用程式放置在某個信任群組中，實際取決於該應用程式可能對電腦造成的危險等級而定。

   Kaspersky Endpoint Security 將應用程式放置在“防火牆”和“主機入侵防禦”元件的信任群組中。您不能僅變更“防火牆”或“主機入侵防禦”的信任群組。

   如果您拒絕加入 KSN 或沒有網路，Kaspersky Endpoint Security 會根據“主機入侵防禦”元件的設定將應用程式放置在某個信任群組中。從 KSN 收到應用程式的信譽後，可以自動變更信任群組。
4. 它是根據信任群組封鎖應用程式的網路活動。例如，不允許“*高限制*”信任群組中的應用程式使用任何網路連線。

下次啟動應用程式時，Kaspersky Endpoint Security 會檢查該應用程式的完整性。如果應用程式未變更，則該元件將對其套用目前的網路權限。如果應用程式已經過修改，Kaspersky Endpoint Security 會分析應用程式，就像它初次開機時一樣。

## 網路規則優先順序

每條規則都有優先順序。規則在清單中的位置越高，優先順序越高。如果將網路活動新增到多條規則中，“防火牆”會根據優先等級最高的規則來管理網路活動。

網路封包規則的優先順序比應用程式網路規則高。如果網路封包規則和應用程式網路規則指定了同一類別的網路活動，則該網路活動將根據網路封包規則進行處理。

應用程式的網路規則以特定方式工作。應用程式的網路規則包括基於網路狀態的存取規則：*公用網路*，*本機網路*，*受信任網路*。例如，預設情況下，“*高限制*”信任群組中的應用程式在所有狀態的網路中均不允許進行任何網路活動。如果為單個應用程式（父應用程式）指定了網路規則，則其他應用程式的子處理程序將依據父應用程式的網路規則執行。如果應用程式沒有網路規則，則子程序將根據應用程式信任組的網路存取規則執行。

例如，對於瀏覽器 X 以外的所有應用程式，您已禁止所有狀態的網路中的任何網路活動。如果從瀏覽器 X（父應用程式）開始安裝瀏覽器 Y（子處理程序），則瀏覽器 Y 安裝程式將存取網路並下載必要的檔案。安裝後，根據防火牆設定，瀏覽器 Y 將被拒絕執行任何網路連線。要禁止作為子處理程序的瀏覽器 Y 安裝程式的網路活動，必須為瀏覽器 Y 的安裝程式新增網路規則。

網路連線類型

“防火牆”允許您根據網路連線類型來控制網路活動。Kaspersky Endpoint Security 從電腦的作業系統接收網路連線類型。作業系統中的網路連線類型由使用者在設定連線時設定。您可以在 Kaspersky Endpoint Security 設定中變更網路連線的類型。“防火牆”將根據 Kaspersky Endpoint Security 設定中指定的而不是作業系統中的網路類型來監控網路活動。

下列網路連線類型可以使用：

- **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）。當使用者操作連接到此類網路的電腦時，防火牆可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。防火牆根據為每一個應用程式設定的網路規則，篩選應用程式的網路活動。

  防火牆預設為網際網路分配*公用網路*類型。您無法變更網際網路的類型。

- **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。

防火牆元件設定

| 參數 | 描述 |
| --- | --- |
| **封包規則** | 包含網路封包規則清單的表。網路封包規則將對網路封包進行限制，與應用程式無關。此類規則將限制透過特定連接埠的選定資料協定傳送和接收的網路流量。<br>此表格列出了由 Kaspersky 建議的預配置網路封包規則，它們能最好地為 Microsoft Windows 作業系統的電腦提供網路流量防護。<br>防火牆將為每條網路封包規則設定執行優先順序。防火牆將按照封包規則清單上的順序從上到下處理網路封包規則。防火牆將找到最適合網路連線的網路封包規則，並套用該規則來允許或封鎖網路活動。然後，防火牆會對特定網路連線略過所有後續網路封包規則。<br>網路封包規則的優先順序比應用程式網路規則高。 |
| **可用網路** | 此表格包含防火牆在電腦上偵測到的網路連線的資訊。<br>預設情況下已將“*公用網路*”狀態分配給網際網路。您無法變更網際網路的狀態。 |
| **應用程式規則** | **應用程式**“防火牆”元件控制的應用程式清單。應用程式分配到信任群組中。信任群組會定義 Kaspersky Endpoint Security 控制應用程式的網路活動時使用的權限。<br>您可以從受政策影響的電腦上安裝的所有應用程式的單一清單中選取應用程式，並將該應用程式新增到信任群組。<br>**網路規則**屬於信任群組的應用程式網路規則清單。防火牆按照這些規則管理應用程式的網路活動。<br>該表顯示 Kaspersky 專家推薦的自訂網路規則。這些網路規則已新增，以最佳方式防護執行 Windows 作業系統的電腦網路流量。無法刪除自訂網路規則。 |

# BadUSB 攻擊防護

某些病毒會修改 USB 裝置的固件以欺騙作業系統，將 USB 偽裝為鍵盤。結果，該病毒可能在您的使用者帳戶下執行命令以下載惡意軟體（例如）。

BadUSB 攻擊防護元件可以防止受感染的模擬鍵盤的 USB 裝置連線至電腦。

當 USB 裝置連線到電腦並被作業系統識別為鍵盤時，應用程式會提示使用者用該鍵盤或螢幕鍵盤（如適用）輸入由應用程式產生的數字代碼（請參閱下圖）。這個步驟稱為鍵盤授權。

如果輸入的代碼正確，應用程式會將識別參數（鍵盤的 VID/PID 及其所連接的連接埠號碼）儲存在授權鍵盤清單之中。重新啟動作業系統後重新連線鍵盤時無需重複鍵盤授權。

經授權的鍵盤連接至該電腦不同 USB 連接埠時，程式將再次提示為該鍵盤授權。

如果錯誤輸入數位代碼，則程式將生成新的代碼。您可以設定輸入數位代碼的嘗試次數。如果數位代碼多次輸入不正確，或者鍵盤授權視窗被關閉（請見下圖），則應用程式封鎖來自此鍵盤的輸入。當 USB 裝置封鎖時間經過或者作業系統重新啟動後，程式將再次提示使用者重新執行鍵盤授權。

程式將允許使用經過授權的鍵盤並封鎖未經授權的鍵盤。

預設情況下，未安裝“BadUSB 攻擊防護”元件。如果需要“BadUSB 攻擊防護”元件，可以在安裝應用程式前在安裝套件的內容中新增該元件，或者在安裝應用程式後變更可用的應用程式元件。




*鍵盤授權*

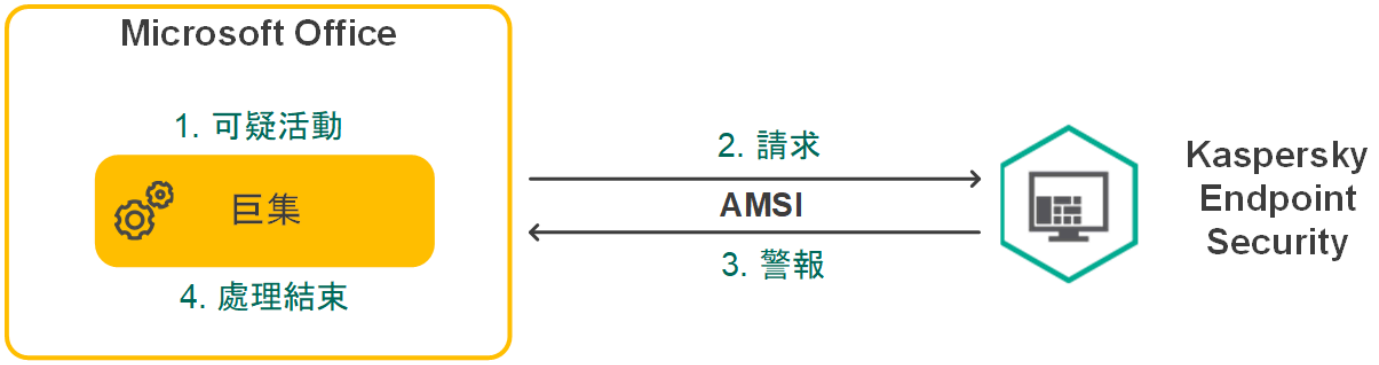
BadUSB 攻擊防護元件設定

| 參數 | 描述 |
| --- | --- |
| **禁止使用螢幕鍵盤授權 USB 裝置** | 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。 |
| **禁止使用條形碼授權 USB 裝置** | 如果啟用此切換開關，應用程式將不會在條碼掃描器驗證通知中顯示條碼。 |
| **USB 裝置授權嘗試最大次數** | 在授權碼不正確輸入達到指定次數時自動封鎖 USB 裝置。有效值為 1 到 10。例如，如果您允許嘗試輸入授權碼五次，則應用程式會在第五次嘗試失敗後封鎖 USB 裝置。Kaspersky Endpoint Security 會顯示 USB 裝置的封鎖時長。該時間經過後，您可以有 5 次嘗試輸入授權碼。 |
| **達到嘗試的最大數量時逾時** | 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。有效值為 1 到 180（分鐘）。 |

# AMSI 防護

AMSI 防護元件設計用於支援 Microsoft 的反惡意軟件掃描接口。*惡意軟體防護掃描介面 (AMSI)* 允許具有 AMSI 支援的協力廠商應用程式將物件（例如，PowerShell 指令碼）傳送到 Kaspersky Endpoint Security 進行附加掃描，然後接收這些物件的掃描結果。例如，協力廠商應用程式可能包括 Microsoft Office 應用程式（請參見下圖）。有關 AMSI 的詳細資訊，請參閱 Microsoft 文件。

AMSI 防護元件只能偵測威脅並將偵測到的威脅通知給協力廠商應用程式。在收到威脅通知後，協力廠商應用程式將不允許惡意操作（例如，終止操作）。




AMSI 操作示範

AMSI 防護元件可能會拒絕協力廠商應用程式的請求，例如，如果該應用程式超出了指定間隔內的最大請求數。Kaspersky Endpoint Security 將有關來自協力廠商應用程式的被拒絕請求的資訊傳送至管理伺服器。AMSI 防護元件不會拒絕來自對其啟用了與 AMSI 防護元件的持續整合的協力廠商應用程式的請求。

AMSI 防護元件可用於以下適用於工作站和伺服器的作業系統：

- Windows 10 Home / Pro / Pro for Workstations / Education / Enterprise / Enterprise 多工作階段
- Windows 11 Home / Pro / Pro for Workstations / Education / Enterprise
- Windows Server 2016 Essentials / Standard / Datacenter（包括 Server Core 模式）
- Windows Server 2019 Essentials / Standard / Datacenter（包括 Server Core 模式）
- Windows Server 2022 Standard / Datacenter / Datacenter: Azure Edition（包括 Server Core 模式）
- Windows Server 2025 Standard / Datacenter

"AMSI 防護"設定

| 參數 | 描述 |
| --- | --- |
| **掃描壓縮檔案** | 掃描 ZIP、GZIP、BZIP、RAR、TAR、ARJ、CAB、LHA、JAR、ICE 和其它存檔。應用程式不僅依照副檔名而且依照格式掃描存檔。當檢查封存時，應用程式會執行巡迴解壓縮。這可讓人偵測多層封存（封存內的封存）內的威脅。 |
| **掃描分發套件** | 掃描協力廠商應用程式的分發套件。 |
| **掃描 Microsoft Office 格式的檔案** | 掃描 Microsoft Office 檔案（DOC、DOCX、XLS、PPT 和其他 Microsoft 副檔名）。Office 格式檔案也包含 OLE 物件。應用程式掃描小於 1 MB 的 office 格式檔案，無論該核取方塊是否被選中。 |
| **不解壓縮大型複合檔案** | 如果選中該核取方塊，應用程式不會掃描其大小超過指定值的複合檔案。<br>如果清除該核取方塊，應用程式將掃描所有大小的複合檔案。<br>應用程式會掃描從存檔中提取的大檔案，而不管是否選中該核取方塊。 |

# 弱點利用防禦

"弱點利用防禦"元件可偵測利用電腦弱點來利用管理員權限或執行惡意活動的程式程式碼。例如，弱點利用程式可以利用緩衝區溢位攻擊。為此，弱點利用程式會向易受攻擊的應用程式傳送大量資料。處理此資料時，易受攻擊的應用程式會執行惡意程式碼。此攻擊的結果是，弱點利用程式可啟動未經授權的惡意軟體安裝。當存在從易於感染的應用程式執行可執行檔的嘗試，並且該嘗試並非由使用者執行時，Kaspersky Endpoint Security 將封鎖該檔案執行或通知使用者。

漏洞利用防護元件也會監控網路連接埠，以查找可能威脅電腦安全的應用程式處理程序。應用程式透過病毒資料庫獲取有關此類處理程序的資訊。

弱點利用防禦元件設定

| 參數 | 描述 |
| --- | --- |
| **偵測到弱點時** | **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。<br>**通知**如果選擇此項目，Kaspersky Endpoint Security 將在偵測到弱點時記錄包含弱點相關資訊的項目，並將此弱點的相關資訊新增至活動威脅清單。 |
| **啟用系統處理程序記憶體防護** | 如果開啟此切換按鈕，Kaspersky Endpoint Security 將封鎖嘗試存取系統處理程序記憶體的外部處理程序。 |

# 行為偵測

“行為偵測”元件接收您電腦上的應用程式操作的資料，並將此資訊提供給其他防護元件以提高效能。“行為偵測”元件將行為流簽章 (BSS) 用於應用程式。如果應用程式操作比對危險活動行為流簽章，Kaspersky Endpoint Security 將執行選定的回應操作。Kaspersky Endpoint Security 基於行為特徵碼，可為電腦提供主動防禦。

行為偵測元件也會監控網路連接埠，以查找可能威脅電腦安全的應用程式處理程序。應用程式透過病毒資料庫獲取有關此類處理程序的資訊。

行為偵測元件設定

| 參數 | 描述 |
| --- | --- |
| **偵測到惡意軟體活動時的動作** | **刪除**如果選取此選項，在偵測到惡意活動時，Kaspersky Endpoint Security 會刪除惡意應用程式的可執行檔，同時在備份區建立該檔案的備份副本。<br>**封鎖**如果選取此選項，在偵測到惡意活動時，Kaspersky Endpoint Security 會終止該應用程式。<br>**通知**如果選取此選項並且偵測到應用程式的惡意活動，Kaspersky Endpoint Security 不會終止該應用程式，但會將應用程式的惡意活動的相關資訊新增至活動威脅清單。 |

# 主機入侵防禦

“主機入侵防禦”元件可避免應用程式執行可能給作業系統帶來危險的操作，並確保控制對作業系統資源和個人資料的存取。該元件借助防毒資料庫和卡巴斯基安全網路雲端服務來提供電腦防護。

該元件透過*應用程式權限*來控制應用程式的操作。應用程式權限包括以下存取參數：

- 對作業系統資源（例如，自動啟動選項、登錄機碼）的存取權限
- 對個人資料（例如，檔案和應用程式）的存取權限

防火牆元件使用*網絡規則*控制應用程式的網絡活動。

在應用程式首次啟動期間，“主機入侵防禦”元件會執行以下操作：

1. 使用下載的防毒資料庫檢查應用程式的安全性。
2. 在卡巴斯基安全網路中檢查應用程式安全性。

   建議您加入卡巴斯基安全網路以幫助“主機入侵防禦”元件更有效地工作。

3. 將應用程式放置在其中一個受信任群組中：*受信任*，*低限制*，*高限制*，*不信任*。

   信任群組定義了在控制應用程式活動時 Kaspersky Endpoint Security 所引用的權限。Kaspersky Endpoint Security 會將應用程式放置在某個信任群組中，實際取決於該應用程式可能對電腦造成的危險等級而定。

   Kaspersky Endpoint Security 將應用程式放置在“防火牆”和“主機入侵防禦”元件的信任群組中。您不能僅變更“防火牆”或“主機入侵防禦”的信任群組。

   如果您拒絕加入 KSN 或沒有網路，Kaspersky Endpoint Security 會根據“主機入侵防禦”元件的設定將應用程式放置在某個信任群組中。從 KSN 收到應用程式的信譽後，可以自動變更信任群組。

4. 根據信任群組封鎖應用程式操作。例如，“*高限制*”信任群組中的應用程式會被拒絕存取作業系統模組。

下次啟動應用程式時，Kaspersky Endpoint Security 會檢查該應用程式的完整性。如果應用程式未變更，則該元件對其應用目前應用程式權限。如果應用程式已經過修改，Kaspersky Endpoint Security 會分析應用程式，就像它初次開機時一樣。

主機入侵防禦元件設定

| 參數 | 描述 |
| --- | --- |
| **應用程式權限** | “主機入侵防禦”元件監控的應用程式清單。應用程式分配到信任群組中。信任群組定義了在控制應用程式活動時 Kaspersky Endpoint Security 所引用的權限。<br>您可以從受政策影響的電腦上安裝的所有應用程式的單一清單中選取應用程式，並將該應用程式新增到信任群組。<br>下表顯示應用程式的存取權限：<br>• **檔案和系統登錄檔**屬於信任群組的應用程式的作業系統資源和個人資料存取權限表。<br>• **權限**屬於信任群組的應用程式的作業系統錯處理程序和資源存取權限表。<br>• **網路規則**屬於信任群組的應用程式網路規則清單。防火牆按照這些規則管理應用程式的網路活動。該表顯示 Kaspersky 專家推薦的自訂網路規則。這些網路規則已新增，以最佳方式防護執行 Windows 作業系統的電腦網路流量。無法刪除自訂網路規則。 |
| **受防護資源** | 該表包含分類的電腦資源。“主機入侵防禦”元件監控其他應用程式存取該表資源的嘗試。<br>資源可以是登錄類別、檔案或資料夾或登錄機碼。 |
| **在 Kaspersky Endpoint Security 之前啟動的應用程式信任群組** | Kaspersky Endpoint Security 將在其中放置應用程式的信任群組，這些應用程式在 Kaspersky Endpoint Security 啟動之前啟動。 |
| **從 KSN 為之前未知應用程式更新規則** | 如果選中該核取方塊，“主機入侵防禦”元件將透過使用卡巴斯基安全網路資料庫來更新以前未知的應用程式的權限。 |
| **信任具有數位簽章的應用程式** | 如果選中此核取方塊，“主機入侵防禦”元件會將帶有受信任供應商的數位簽章的應用程式放置在“*受信任*”群組中。<br>*受信任供應商*是卡巴斯基信任的软体供應商。您還可以手動將供應商憑證新增到受信任憑證儲存中。<br>如果清空此核取方塊，“主機入侵防禦”元件將不信任此類應用程式，並使用其他參數以確定它們的信任群組。 |

| 參數 | 描述 |
| --- | --- |
| **刪除超過以下時間未啟動的應用程式的規則 N 天 (從 1 到 90)** | 如果選中該核取方塊，則在滿足以下條件的情況下，Kaspersky Endpoint Security 會自動刪除有關該應用程式的訊息（信任群組和存取權限）：<br>• 您手動將應用程式放入信任群組或配置其存取權限。<br>• 該應用程式在定義的時間段內未啟動。<br>如果應用程式的信任組和權限已自動確認，Kaspersky Endpoint Security 將在 30 天後刪除有關此應用程式的訊息。不能變更應用程式訊息的儲存期限或關閉自動刪除。<br>下次啟動該應用程式時，Kaspersky Endpoint Security 會像首次啟動該應用程式一樣對其進行分析。 |
| **不包含在其他群組中的應用程式信任群組** | 此下拉清單中的項目決定了 Kaspersky Endpoint Security 將未知應用程式分配到哪個信任群組。<br>您可以選擇以下項目之一：<br>• **低限制**<br>• **高限制**<br>• **不信任** |

# 修復引擎

修復引擎允許 Kaspersky Endpoint Security 復原惡意軟體在作業系統中執行的操作。

回溯作業系統中的惡意軟體活動時，Kaspersky Endpoint Security 將處理以下類型的惡意軟體活動：

- **檔案活動**

  Kaspersky Endpoint Security 執行以下操作：

  - 移除惡意軟體（在除網路磁碟外的所有介質上）建立的可執行檔。
  - 移除已被惡意軟體入侵的程式所建立的可執行檔。
  - 還原被惡意軟體修改或刪除的檔案。

  檔案還原功能有一些限制。

- **登錄檔活動**

  Kaspersky Endpoint Security 執行以下操作：

  - 刪除由惡意軟體建立的登錄機碼。
  - 不會還原被惡意軟體修改或刪除的登錄機碼。

- **系統活動**

  Kaspersky Endpoint Security 執行以下操作：

  - 終止由惡意軟體啟動的處理程序。
  - 終止被惡意應用程式滲透的處理程序。
  - 不會還原被惡意程式掛起的處理程序。

- **網絡活動**

Kaspersky Endpoint Security 執行以下操作：

- 封鎖惡意軟體的網路活動。
- 封鎖被惡意軟體入侵的處理程序的網路活動。

"檔案威脅防護"或"行為偵測"元件或在惡意軟體掃描過程中可以啟動惡意軟體操作回溯。

回溯惡意程式操作的過程將會影響一組嚴格限定的資料。回溯對於作業系統或您的電腦中資料的完整性不會產生負面影響。

# 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。

KSN 功能可能無法在美國的應用程式中使用。

*卡巴斯基安全網路（KSN）*是雲端服務的基礎結構，可提供對線上卡巴斯基知識庫的存取，該知識庫包含有關檔案、網頁資源和軟體信譽的資訊。使用卡巴斯基安全網路的資料可確保 Kaspersky 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 提供有關所掃描檔案的類別和信譽的資訊，以及有關所掃描網址的信譽的資訊。

卡巴斯基安全網路的使用是自願的。應用程式將在初始化設定期間提示您使用 KSN。使用者可以隨時開始或停止加入 KSN。

有關在參與 KSN 期間生成的 Kaspersky 統計資訊的傳送詳情，以及有關此類資訊的儲存和銷毀，請參閱卡巴斯基安全網路聲明和 Kaspersky 網站。含有卡巴斯基安全網路聲明文字的 ksn_<語言 ID>.txt 檔案包括在應用程式分發套件中。

## 卡巴斯基信譽資料庫的基礎結構

Kaspersky Endpoint Security 支援以下用於使用 Kaspersky 信譽資料庫的基礎結構解決方案：

- *卡巴斯基安全網路 (KSN)* 是大多數 Kaspersky 應用程式使用的解決方案。KSN 參與者從卡巴斯基接收資訊，並向 Kaspersky 傳送使用者電腦上偵測到的物件的資訊，以便 Kaspersky 分析人員進行額外分析，並包括在信譽和統計資料庫中。
- *卡巴斯基安全網路 (KSN)* 是讓承載 Kaspersky 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。

法律禁止或公司安全政策限制將任何資料傳輸到國家/地區外部或公司 LAN 外部。

| 參數 | 描述 |
| --- | --- |
| **啟用延伸 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。無論切換位置如何，Kaspersky Endpoint Security 皆使用 KSN 偵測威脅。 |
| **啟用雲端模式** | *雲端模式* 是指 Kaspersky Endpoint Security 使用輕量級版本的病毒資料庫的應用程式執行模式。當使用輕量級病毒資料庫時，卡巴斯基安全網路支援應用程式執行。與通常的資料庫相比，輕量級版本的病毒資料庫僅需要大約一半的電腦 RAM。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。<br>如果開啟該切換按鈕，Kaspersky Endpoint Security 將使用病毒資料庫的輕量級版本，這可以減少作業系統資源上的負載。<br>選中該核取方塊後，Kaspersky Endpoint Security 在下次更新期間下載病毒資料庫的輕量級版本。<br>如果關閉該切換按鈕，Kaspersky Endpoint Security 將使用病毒資料庫的完全版本。<br>清除該核取方塊後，Kaspersky Endpoint Security 在下次更新期間下載病毒資料庫的完全版本。 |
| **KSN 伺服器不可用時電腦狀態**<br>*（僅在卡巴斯基安全管理中心主控台中可用）* | 此下拉清單中的項可確定當 KSN 伺服器不可用時，電腦在卡巴斯基安全管理中心中的狀態。 |
| **使用管理伺服器為 KSN 代理伺服器**<br>*（僅在卡巴斯基安全管理中心主控台中可用）* | 如果選中該核取方塊，Kaspersky Endpoint Security 將使用 KSN 代理服務。您可以在管理伺服器內容中配置 KSN 代理服務設定。 |
| **當 KSN 代理伺服器不可用時使用卡巴斯基安全網路伺服器**<br>*（僅在卡巴斯基安全管理中心主控台中可用）* | 如果選中該核取方塊，當 KSN 代理服務不可用時，Kaspersky Endpoint Security 將使用 KSN 伺服器。KSN 伺服器可以位於 Kaspersky 側，也可以位於協力廠商一側的伺服器（使用卡巴斯基私有安全網路時）。 |

# 記錄檢查

如果 Kaspersky Endpoint Security 安裝在執行 Windows for Servers 的電腦上，則該元件可用。如果 Kaspersky Endpoint Security 安裝在執行 Windows for Workstations 的電腦上，則該元件不可用。

從 11.11.0 版本開始，Kaspersky Endpoint Security for Windows 包括記錄檢查元件。記錄檢查會基於 Windows 事件記錄分析監控受防護環境的完整性。如果應用程式在系統中偵測到有非典型行為的跡象，它會通知管理員，因為該行為可能表明有人嘗試網路攻擊。

Kaspersky Endpoint Security 根據規則分析 Windows 事件記錄和偵測違規。元件包括預定義規則。預定義規則由啟發式分析提供支援。您也可以新增您自己的規則（自訂規則）。當規則觸發時，應用程式會建立一個狀態為"緊急"的事件（請見下圖）。

如果您想要使用記錄檢查，請確保稽核政策安全設定已配置且系統正在記錄相關事件（詳情請見 Microsoft 技術支援網站）。




記錄檢查通知

記錄檢查設定

| 參數 | 描述 |
| --- | --- |
| **預定義規則** | 記錄檢查規則清單。預定義規則包括受防護電腦上異常活動的範本。異常活動可能表明有人嘗試攻擊。 |
| **自訂規則** | 使用者新增的記錄檢查規則清單。您可以設定自己的記錄檢查規則觸發條件。為此，您必須輸入一個事件 ID 並選擇一個事件來源。<br>您可以從標準記錄中選擇一個事件來源：*Application*、*Security*或*System*。您也可以指定協力廠商應用程式的記錄。 |

# Anti-Cryptor

Anti-Cryptor 元件可分析共用資料夾中的活動。如果該活動與外部加密的典型行為流簽章比對，Kaspersky Endpoint Security 將執行選定操作。

Kaspersky Endpoint Security 可防止只在具有 NTFS 檔案系統的媒體上且未被 EFS 系統加密的檔案被外部加密。

| 參數 | 描述 |
| --- | --- |
| **按照名稱或 IP 位址的排除項目** | **按照名稱或 IP 位址的排除項目**嘗試加密共用資料夾的電腦的清單不會受到監控。<br><br>要套用防止共用資料夾被外部加密的電腦排除清單，必須在 Windows 安全審核政策中啟用審核登入。預設情況下，審核登入處於停用狀態。有關 Windows 安全審核政策的詳細資訊，請造訪 Microsoft 網站。<br><br>**按遮罩排除**防護範圍排除項目。如果您的組織在使用共用資料夾交換檔案時使用資料加密，從防護範圍中排除資料夾可減少誤報的數量。例如，當使用者在共用資料夾中處理具有 ENC 副檔名的檔案時，行為偵測可能提高誤判數量。此類活動比對外部加密通常有的行為模式。如果您加密了共用資料夾中的檔案以防護資料，請將該資料夾新增到排除項目。<br><br>使用遮罩：<br>• `*`（星號）字元代表任意一組字元，但 `\` 和 `/` 字元除外（這兩個字元是檔案和資料夾路徑中的檔案和資料夾名稱的分隔符號）。例如，遮罩"`C:\*\*.txt`"將包括位於 C: 磁碟機但是不在子資料夾中所有帶 TXT 副檔名的檔案的路徑。<br>• 兩個連續 `*` 字元在檔案或資料夾名稱中代表任意一組字元（包括空集），包括 `\` 和 `/` 字元（這兩個字元是檔案和資料夾路徑中的檔案和資料夾名稱的分隔符號）。例如，遮罩 `C:\Folder\**\*.txt` 將包括位於巢嵌在 `Folder` 內的資料夾（`Folder`自身除外）中所有帶 TXT 副檔名的檔案的路徑。遮罩必須包含至少一個嵌套等級。遮罩 `C:\**\*.txt` 不是有效遮罩。<br>• `?`（問號）字元代表任意單個字元，但 `\` 和 `/` 字元除外（這兩個字元是檔案和資料夾路徑中的檔案和資料夾名稱的分隔符號）。例如，遮罩 `C:\Folder\???.txt` 將包括位於 `Folder` 資料夾中所有帶 TXT 副檔名且名稱由三個字元構成的檔案的路徑。 |
| **偵測到威脅後的動作** | • **通知**如果選擇此選項，則在偵測到修改共用資料夾中的檔案的嘗試時，Kaspersky Endpoint Security 會將有關此嘗試的資訊新增至活動威脅清單中，並將項目新增至本機應用程式介面報告並將有關偵測到的惡意活動的資訊傳送至卡巴斯基安全管理中心。<br>• **封鎖連線（分鐘）N 分鐘**。如果選擇了該選項，則當 Kaspersky Endpoint Security 偵測到嘗試修改共用資料夾中的檔案時，它會封鎖啟動了惡意活動的工作階段的檔案修改存取權限，並建立修改檔案的備份副本。<br><br>如果啟用了"修復引擎"元件，並且選擇"**封鎖連線（分鐘）N 分鐘**"選項，被修改的檔案會被從備份副本還原。 |
| **防護範圍** | *防護範圍*是 Kaspersky Endpoint Security 監控檔案活動的共用資料夾的路徑清單。Kaspersky Endpoint Security 輸入遮罩時支援環境變量以及 `*` 和 `?` 字元。預設情況下，應用程式會自動識別共用資料夾並監視所有資料夾中的檔案活動。 |

# Web 控制

"Web 控制"管理使用者對 Web 資源的存取。這有助於減少流量和工作時間的不當使用。當使用者嘗試開啟受"Web 控制"限制的網站時，Kaspersky Endpoint Security 將封鎖存取或顯示警告（請參見下圖）。

若要使用 Web Control，您必須完成應用程式的初始設定：

- 對於 HTTPS 流量監控，啟用加密連線掃描（預設為啟用）。
- 選擇 Kaspersky Endpoint Security 必須監控的連接埠（預設情況下，應用程式監控所有連接埠）。
- 選擇您希望 Kaspersky Endpoint Security 監控其流量的應用程式。大多數瀏覽器已出現在卡巴斯基推薦的應用程式清單中。如果清單中缺少您的瀏覽器，請手動新增。
- 我們建議 將網頁交互指令碼注入到 Web 流量中（預設情況下，指令碼注入被停用）。此指令碼可啟用為應用程式事件日誌、OS 事件日誌和報告註冊 Web 控制事件。

## 管理對網站的存取的方法

"Web 控制"允許您使用以下方法配置對網站的存取：

- **網站類別**。網站按照卡巴斯基安全網路雲端服務、啟發式分析和已知網站資料庫（包含在應用程式資料庫中）進行分類。例如，您可以限制使用者存取"*社群網路*"類別或"其它類別"。
- **資料類型**。例如，您可以限制使用者存取網站上的資料，並隱藏影像。Kaspersky Endpoint Security 根據檔案格式確定資料類型，而不是基於其副檔名。

  > Kaspersky Endpoint Security 不掃描壓縮檔案內的檔案。例如，如果影像檔案放在壓縮檔案中，Kaspersky Endpoint Security 會辨識"*壓縮檔案*"資料類型而不是"*圖形*"。

- **單個位址**。您可以輸入網址或使用遮罩。

可以同時使用多種方法來管理對網站的存取。例如，您可以僅針對"*網頁式電子郵件*"網站類別限制對"*Office 應用程式檔案*"資料類型的存取。

## 網站存取規則

"Web 控制"透過使用*存取規則*管理使用者對網站的存取。您可以為網站存取規則配置以下進階設定：

- 規則適用的使用者。

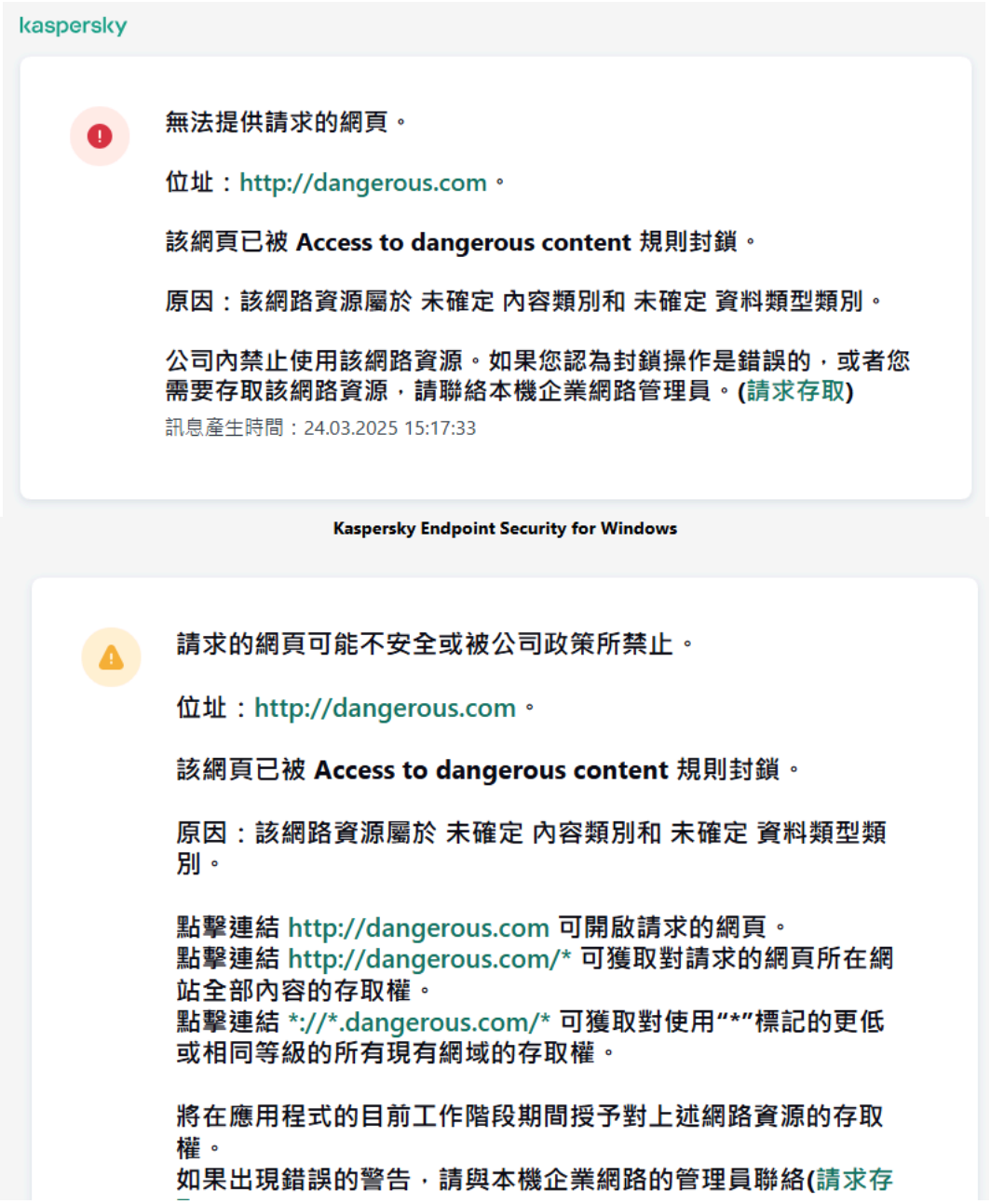
  例如，您可以限制公司內除 IT 部門以外的所有使用者透過瀏覽器存取網際網路。

- 規則排程。

  例如，您可以限制只能在工作時間透過瀏覽器存取網際網路。

## 存取規則優先順序

每條規則都有優先順序。規則在清單中的位置越高，優先順序越高。如果某個網站已新增到多條規則，"Web 控制"會基於優先順序最高的規則來管理對該網站的存取。例如，Kaspersky Endpoint Security 可能將公司入口辨識為社群網路。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。公司 Web 入口存取規則的優先順序必須高於社群網路存取規則的優先順序。




"Web 控制"訊息

Web 控制元件設定

| 參數 | 描述 |
| --- | --- |
| **網路資源存取規則** | 包含 Web 資源存取規則的清單。每條規則都有優先順序。規則在清單中的位置越高，優先順序越高。如果某個網站已新增到多條規則，"Web 控制"會基於優先順序最高的規則來管理對該網站的存取。 |
| **預設規則** | *預設規則*是對不被任何其他規則覆蓋的 Web 資源的存取規則。下列選項可用：<br>• **允許除規則清單外的所有內容**，也稱為禁止網站的拒絕清單模式。<br>• **拒絕除規則清單外的所有內容**，也稱為允許網站的允許清單模式。 |
| **套用規則後終止活動的使用者瀏覽器工作階段** | 如果該核取方塊被選中，Web 控制將在套用政策之後立即終止與被封鎖的 Web 資源的連線。瀏覽器立即停止從網頁下載資料。當您重新整理網頁或前往另一個被禁止的網頁時，應用程式會顯示警告。<br>Web 控制僅允許在 Web 瀏覽器中立即中斷 Web 資源。對於其他應用程式，Web 控制僅限制新連線。<br>如果清除該核取方塊，Web 控制將僅限制與禁止的 Web 資源的新連線。Web 控制不會終止活動連線。 |

| 參數 | 描述 |
| --- | --- |
| **範本** | **警告**該項目欄位包含一個訊息範本，嘗試存取不需要的網頁資源觸發警告訊息規則時就會顯示警告訊息。<br>**有關封鎖的訊息**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。<br>**傳送郵件給管理員**如果使用者認為封鎖是錯誤時要傳送給區域網路管理員的訊息範本。在使用者請求提供存取權限後，Kaspersky Endpoint Security 會向卡巴斯基安全管理中心傳送一個事件：**傳送給管理員的網頁存取封鎖訊息**。事件描述包含一條給管理員的訊息，其中包含被替換的變數。您可以使用預定義事件選擇**使用者請求**在卡巴斯基安全管理中心主控台中檢視這些事件。如果您的組織沒有部署卡巴斯基安全管理中心或者沒有連線到管理伺服器，應用程式將向管理員傳送一條訊息到指定的電子郵件信箱。<br>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。 |
| **記錄允許頁面的開啟** | Kaspersky Endpoint Security 會記錄對所有網站（包括允許的網站）的存取資料。Kaspersky Endpoint Security 將事件傳送到卡巴斯基安全管理中心、Kaspersky Endpoint Security 本機記錄和 Windows 事件記錄。要監控使用者網際網路活動，您需要配置用於儲存事件的設定。<br>支援監控功能的瀏覽器：Microsoft Edge、Microsoft Internet Explorer、Google Chrome、Yandex Browser、Mozilla Firefox。使用者活動監控在其他瀏覽器中不工作。<br>在解密 HTTPS 流量時，監控使用者網際網路活動可能需要更多電腦資源。 |

# 裝置控制

"裝置控制"管理使用者對安裝在電腦上或連線到電腦的裝置（例如，硬碟磁碟機、相機或 Wi-Fi 模組）的存取。這樣可以在連線此類裝置時防護電腦免受感染，並防止資料遺失或洩漏。

如果啟用了裝置控制，則應用程式會將有關已連線裝置的資訊轉送到卡巴斯基安全管理中心。您可以在卡巴斯基安全管理中心的"**進階 → 儲存區 → 硬體**"資料夾中檢視已連線裝置的清單。

## 裝置存取等級

"裝置控制"控制以下等級的存取權限：

- **裝置類型**。例如，印表機、卸除式磁碟機和 CD/DVD 磁碟機。
  您可以按如下方式配置裝置存取權限：
  - 允許 – ✓。
  - 封鎖 – ⊘。
  - 按規則（僅限印表機和攜帶式裝置）– 。
  - 取決於連線匯流排（Wi-Fi 除外）– 。
  - 封鎖但帶有例外（僅限 Wi-Fi）– 。
- **連線匯流排**。*連線匯流排*是用於將裝置連線至電腦的介面（範例 USB 或 FireWire）。如果為裝置類型選擇 **取決於連線匯流排** 模式後，應用程式會根據連線介面（例如 USB）允許或拒絕對裝置的存取。

您可以按如下方式配置裝置存取權限：

- 允許 – ✓。
- 封鎖 – ⊘。

- **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。

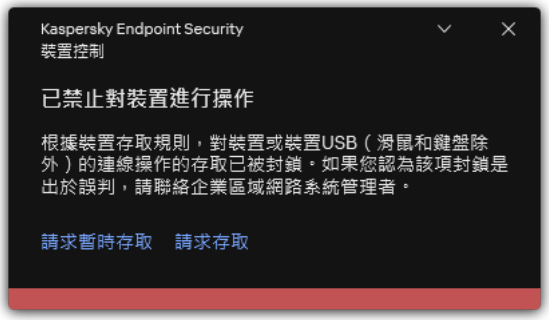
  您可以根據以下資料新增受信任裝置：

  - **透過裝置 ID**每個裝置都有一個唯一識別碼（硬體 ID 或 HWID）。您可以使用作業系統工具在裝置內容中檢視 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。
  - **透過裝置型號**每個裝置都有一個供應商 ID (VID) 和一個產品 ID (PID)。您可以使用作業系統工具在裝置內容中檢視 ID。用於輸入 VID 和 PID 的範本：`VID_1234&PID_5678`。如果在組織中使用特定型號的裝置，則按型號新增裝置很方便。這樣，您可以新增該型號的所有裝置。
  - **透過裝置 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到受信任清單。`*` 字元可替換任意一組字元。輸入遮罩時，Kaspersky Endpoint Security 不支援 `?` 字元。例如，`WDC_C*`。
  - **依型號遮罩列出的裝置**如果您使用具有相似 VID 或 PID 的多個裝置（例如，同一製造商的裝置），則可以使用遮罩將裝置新增到受信任清單。`*` 字元可替換任意一組字元。輸入遮罩時，Kaspersky Endpoint Security 不支援 `?` 字元。例如，`VID_05AC&PID_*`。

“裝置控制”透過使用*存取規則*來管理使用者對裝置的存取。“裝置控制”還允許您儲存裝置連線/斷開連線事件。要儲存事件，您需要在政策中配置事件註冊。

如果對裝置的存取權限取決於連線介面（狀態），Kaspersky Endpoint Security 不會儲存裝置連線/斷開連線事件。要使 Kaspersky Endpoint Security 儲存裝置連線/斷開連線事件，請允許存取相應的裝置類型（✓ 狀態）或將裝置新增到信任清單。

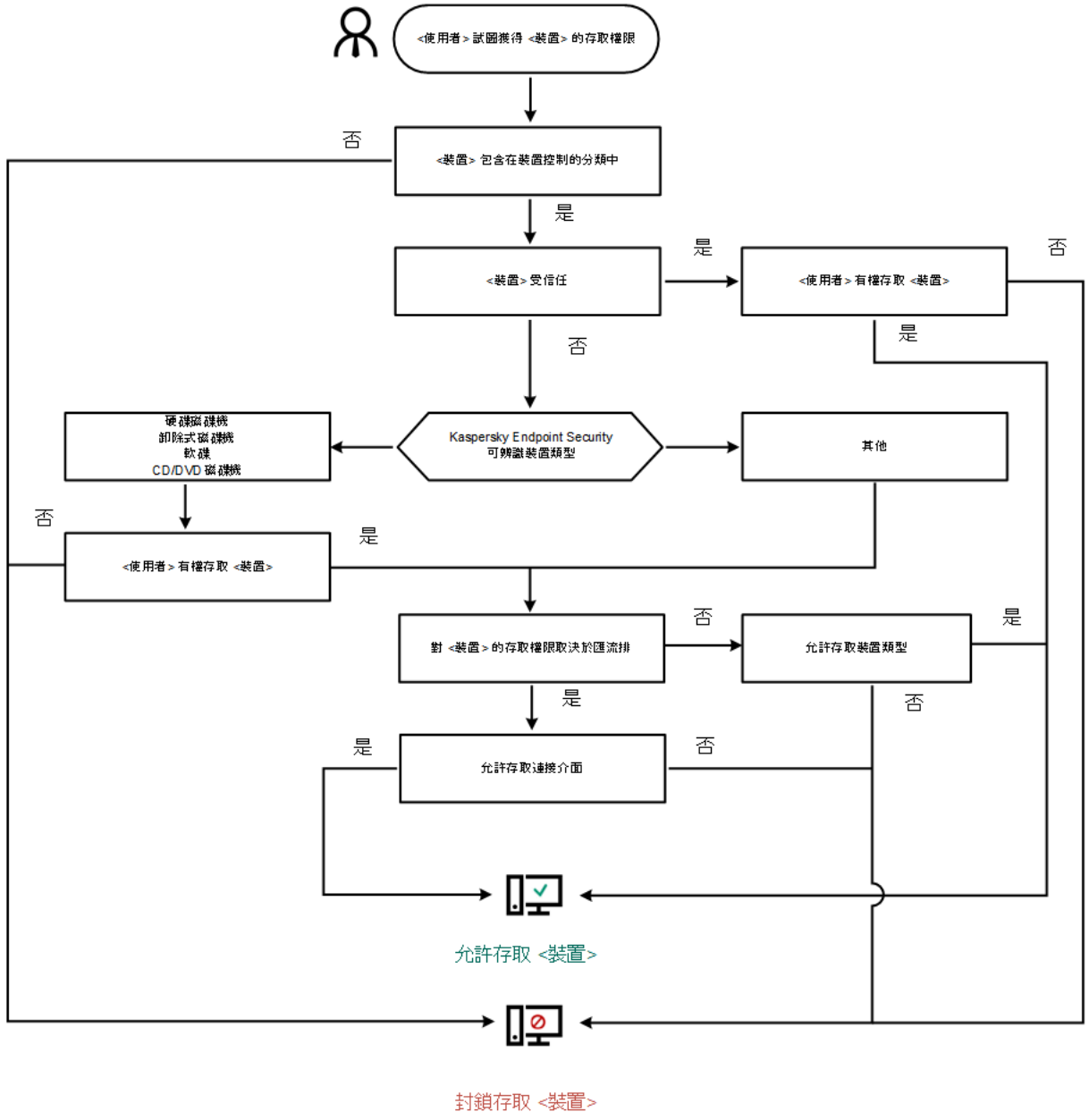
當被“裝置控制”封鎖的裝置連線到電腦時，Kaspersky Endpoint Security 將封鎖存取並顯示通知（請參見下圖）。




“裝置控制”通知

## 裝置控制執行演算法

Kaspersky Endpoint Security 在使用者將裝置連線到電腦之後做出是否允許存取該裝置的決定（請參見下圖）。




裝置控制執行演算法

如果已連線裝置並允許存取，您可以編輯存取規則並封鎖存取。在這種情況下，下次有人嘗試存取該裝置（例如檢視資料夾樹或執行讀取或寫入操作）時，Kaspersky Endpoint Security 會封鎖存取。沒有檔案系統的裝置僅在該裝置下一次連接時被封鎖。

如果已安裝有 Kaspersky Endpoint Security 的電腦上的使用者需要請求被錯誤封鎖的裝置的存取權限，則向該使用者傳送請求存取說明。

| 參數 | 描述 |
| --- | --- |
| **允許暫時存取請求**<br>*（僅在卡巴斯基安全管理中心主控台中可用）* | 如果選中此方塊，“**請求存取**”按鈕將在 Kaspersky Endpoint Security 的本機介面中可用。使用者可以使用該按鈕來請求臨時存取被封鎖的裝置。 |
| **裝置和 Wi-Fi 網路** | 該表包含根據裝置控制元件的分類所有可能的裝置類型，包括這些裝置類型各自的存取狀態。 |
| **連線匯流排** | 符合“裝置控制”元件分類的所有可用連線匯流排的清單，包括這些連線匯流排各自的存取狀態。如果選擇了**取決於連線匯流排**模式，Kaspersky Endpoint Security 會根據連線匯流排的類型允許或拒絕對裝置的存取。 |
| **受信任裝置** | 被授權存取這些裝置的受信任裝置和使用者的清單。 |
| **繼承時合併值**<br>*（僅在卡巴斯基安全管理中心主控台中可用）* | 這會合併卡巴斯基安全管理中心的父級和子級政策中的受信任裝置的清單。要合併清單，必須將子政策設定為繼承卡巴斯基安全管理中心父政策的設定。<br>如果選中此核取方塊，則子政策中將顯示卡巴斯基安全管理中心父政策的清單項目。這樣，您可以（例如）建立整個組織的受信任裝置的合併清單。<br>子政策中繼承的清單項無法被刪除或編輯。在繼承過程中合併的受信任裝置清單中的項目只能在父政策中進行刪除和編輯。您可以新增、編輯或刪除較低等級之政策中的清單項目。<br>如果子政策和父政策清單上的項目相符，則這些項目將顯示為父政策的同一項目。<br>如果未選中該核取方塊，則在繼承卡巴斯基安全管理中心政策設定時不會合併清單項。<br>此功能還允許合併政策設定檔中的清單。若要合併清單，請在最高優先順序的設定檔中啟用從較低優先順序的設定檔繼承設定。有關政策設定檔優先順序的詳細資訊，請參閱卡巴斯基安全管理中心說明。 |
| **橋接防護** | 橋接防護透過封鎖為一台電腦同時建立多個網路連線來禁止建立橋接器。這樣可以防護公司網路避免未受防護和未經授權的網路上的攻擊。<br>橋接防護根據裝置的優先順序封鎖建立多個連線。裝置在清單中的位置越高，優先順序越高。<br>如果活動連線和新連線屬於同一類型（例如 Wi-Fi），則 Kaspersky Endpoint Security 會封鎖活動連線並允許建立新連線。<br>如果活動連線和新連線屬於不同類型（例如，網路介面卡和 Wi-Fi），則 Kaspersky Endpoint Security 會封鎖具有較低優先順序的連線，允許具有較高優先順序的連線。<br>橋接防護支援以下類型的裝置的操作：網路介面卡、Wi-Fi 和數據機。 |
| **訊息範本** | **有關封鎖的訊息**當使用者嘗試存取封鎖的裝置時所顯示的訊息的範本。當使用者嘗試對被封鎖使用的裝置內容執行操作時，也會顯示此訊息。<br>**傳送郵件給管理員**當使用者確信裝置的存取權限或裝置內容操作被錯誤地禁止時，傳送給 LAN 管理員的訊息的範本。在使用者請求提供存取權限後，Kaspersky Endpoint Security 會向卡巴斯基安全管理中心傳送一個事件：**傳送給管理員的裝置存取封鎖訊息**。事件描述包含一條給管理員的訊息，其中包含被替換的變數。您可以使用預定義事件選擇**使用者請求**在卡巴斯基安全管理中心主控台中檢視這些事件。如果您的組織沒有部署卡巴斯基安全管理中心或者沒有連線到管理伺服器，應用程式將向管理員傳送一條訊息到指定的電子郵件信箱。 |

# 應用程式控制

“應用程式控制”管理使用者電腦上的應用程式啟動。這允許您在使用應用程式時實行公司安全政策。“應用程式控制”還透過限制對應用程式的存取來降低電腦感染的風險。

設定“應用程式控制”包括以下步驟：

1. 建立應用程式類別。

   管理員建立管理員想要管理的應用程式類別。應用程式類別適用於公司網路中的所有電腦，與管理群組無關。要建立類別，您可以使用以下條件：KL 類別（例如，*瀏覽器*）、檔案雜湊、應用程式供應商和其他條件。

2. 建立應用程式控制規則。

   管理員在管理群組的政策中建立應用程式控制規則。該規則包括應用程式類別和這些類別中的應用程式啟動狀態：已封鎖或已允許。管理員可以建立許多規則。一個應用程式可能符合多個規則的條件。封鎖規則的優先等級高於允許規則的優先等級。Kaspersky Endpoint Security 每次啟動時都會檢查應用程式是否符合規則。Kaspersky Endpoint Security 會依序將應用程式與所有應用程式控制規則進行比對。

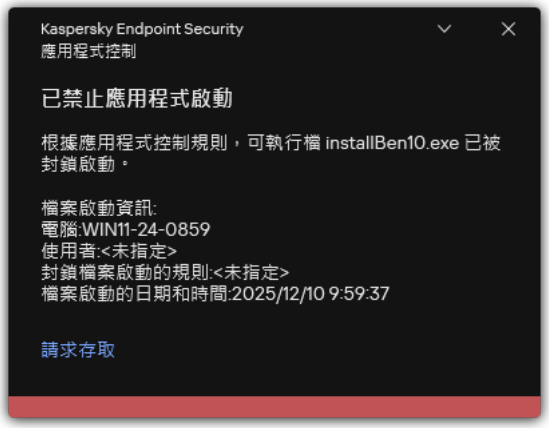
3. 選取應用程式控制模式。

   管理員選取對未包含在以下任何規則中之應用程式的處理模式（應用程式拒絕清單和允許清單）。

當使用者嘗試啟動已禁止的應用程式時，Kaspersky Endpoint Security 將封鎖該應用程式啟動並顯示通知（請參見下圖）。

系統提供了一種*測試模式*來檢查"應用程式控制"的設定。在此模式下，Kaspersky Endpoint Security 會執行以下操作：

- 允許啟動應用程式，包括已禁止的應用程式。
- 顯示有關已禁止之應用程式啟動的通知，並將資訊新增到使用者電腦上的報告中。
- 將有關已禁止之應用程式啟動的資料傳送到卡巴斯基安全管理中心。




"應用程式控制"通知

"應用程式控制"執行模式

"應用程式控制"元件可在兩種模式下執行：

- **拒絕清單**在此模式下，"應用程式控制"允許使用者啟動除了應用程式控制規則中禁止的應用程式以外的所有應用程式。

  預設情況下，會啟用"應用程式控制"此一模式。

- **允許清單**在此模式下，"應用程式控制"會封鎖使用者啟動除了應用程式控制規則中允許和未禁止的應用程式以外的所有應用程式。

  如果完整設定了"應用程式控制"的允許規則，則該元件將封鎖啟動所有未經區域網路管理員驗證的新應用程式，同時允許執行使用者在工作中依賴的作業系統和受信任應用程式。

  您可以閱讀有關在允許清單模式下設定應用程式控制規則的建議。

可以使用 Kaspersky Endpoint Security 本機介面和卡巴斯基安全管理中心將"應用程式控制"設定為在這些模式下執行。

但是，卡巴斯基安全管理中心提供了在 Kaspersky Endpoint Security 本機介面中不可使用的工具，例如以下工作所需的工具：

- 建立應用程式類別。

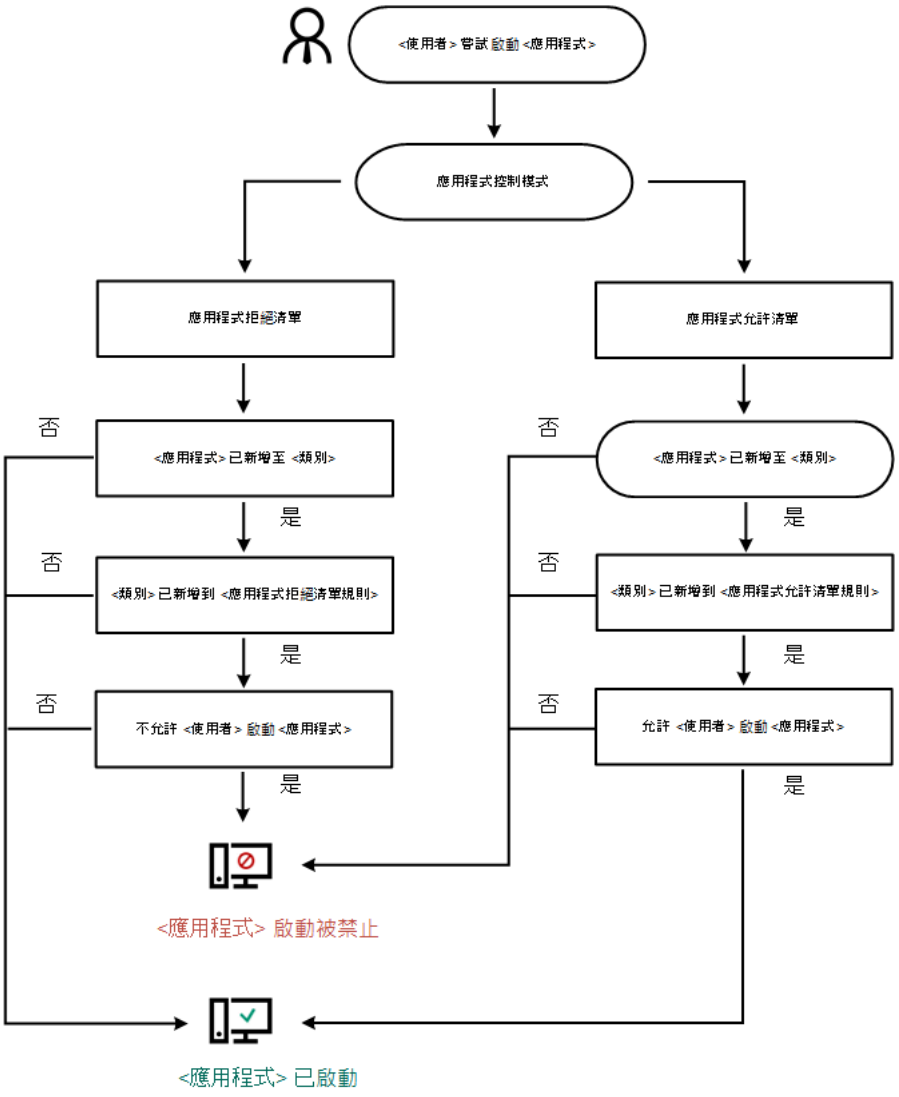
  在卡巴斯基安全管理中心管理主控台中建的應用程式控制規則，以您的自訂的應用程式類別為主，而不是以像 Kaspersky Endpoint Security 本機介面中的包含和排除條件為主。

- 接收有關安裝在公司區域網路電腦上的應用程式資訊。

因此，建議使用卡巴斯基安全管理中心設定“應用程式控制”元件的執行。

“應用程式控制”執行演算法

Kaspersky Endpoint Security 使用算法來決定是否啟動應用程式（請參見下圖）。




“應用程式控制”執行演算法

| 參數 | 描述 |
| --- | --- |
| **啟動被規則封鎖的應用程式時的動作** | **套用規則**Kaspersky Endpoint Security 會根據選定模式管理應用程式的啟動。<br>**測試規則**Kaspersky Endpoint Security 允許啟動在目前應用程式控制模式中封鎖的應用程式，但是在報告中記錄其啟動資訊。 |
| **應用程式啟動控制模式** | 您可以選取以下選項之一：<br>• **拒絕清單**如果選擇此選項，應用程式控制將允許所有使用者啟動所有應用程式，符合應用程式控制封鎖規則的應用程式除外。<br>• **允許清單**如果選擇此選項，應用程式控制將封鎖所有使用者啟動任何應用程式，符合應用程式控制允許規則的應用程式除外。<br>選取**允許清單**模式後，會自動建立兩個應用程式控制規則：<br>• **黃金映像**<br>• **信任的更新程式**<br>您不能編輯自動建立的規則的設定，也不能刪除這些規則。您可以啟用或停用這些規則。 |
| **監控 DLL 模組載入** | 如果選定此核取方塊，Kaspersky Endpoint Security 將在使用者啟動應用程式時控制 DLL 模組的載入。有關 DLL 模組和載入此 DLL 模組的應用程式的資訊將記錄在此報告中。<br>當啟用對載入 DLL 模組和驅動程式的控制時，請確保在"應用程式控制"設定中已啟用以下規則之一：預設**黃金映像**規則或其他包含"**黃金映像\受信任憑證**" KL 類別的規則，並確保在啟動 Kaspersky Endpoint Security 之前載入受信任的 DLL 模組和驅動程式。如果在停用"**黃金映像**"規則時啟用對載入 DLL 模組和驅動程式的控制，可能導致作業系統不穩定。<br>Kaspersky Endpoint Security 僅監控自選中核取方塊後載入的 DLL 模組和驅動程式。選中核取方塊後，建議重新啟動電腦以確保應用程式監控所有 DLL 模組和驅動，包括在啟動 Kaspersky Endpoint Security 之前加載的模組和驅動。 |
| **使用嚴格的數位簽章驗證** | 您可以選擇憑證作為應用程式控制規則的觸發條件。<br>如果選取此核取方塊，Kaspersky Endpoint Security 會將規則套用於僅使用來自受信任的系統憑證存儲的憑證簽署的應用程式。使用此類憑證簽署的應用程式也被視為受防護元件信任，例如 *惡意軟體掃描* 工作。但是，如果您在應用程式控制規則中指定來自不同儲存空間的憑證，Kaspersky Endpoint Security 不會套用此類規則。<br>如果清除該核取方塊，Kaspersky Endpoint Security 會將規則套用於由 Windows 受信任根憑證儲存中的憑證簽署的應用程式。此類應用程式不屬於受信任區域。防護元件監視此類應用程式的活動。 |
| **有關應用程式封鎖的訊息範本** | **有關封鎖的訊息**當觸發了某個封鎖應用程式啟動的應用程式控制規則時所顯示的訊息範本。<br>**傳送郵件給管理員**當使用者相信某個應用程式被錯誤地封鎖時，可以傳送給公司區域網路管理員的訊息模組。在使用者請求提供存取權限後，Kaspersky Endpoint Security 會向卡巴斯基安全管理中心傳送一個事件：**傳送給管理員的應用程式啟動封鎖訊息**。事件描述包含一條給管理員的訊息，其中包含被替換的變數。您可以使用預定義事件選擇**使用者請求**在卡巴斯基安全管理中心主控台中檢視這些事件。如果您的組織沒有部署卡巴斯基安全管理中心或者沒有連線到管理伺服器，應用程式將向管理員傳送一條訊息到指定的電子郵件信箱。 |

# 適應性異常控制

如果 Kaspersky Endpoint Security 安裝在執行 Windows for Workstations 的電腦上，則該元件可用。如果 Kaspersky Endpoint Security 安裝在執行 Windows for Servers 的電腦上，則該元件不可用。

自適應異常控制元件會監視並封鎖不是公司網路內電腦典型操作的相關操作。自適應異常控制使用一組規則來偵錯非典型行為（例如，*從 Office 應用程式啟動 Microsoft PowerShell* 規則）。規則由 Kaspersky 專家根據惡意活動的典型情景建立。您可以配置"自適應異常控制"處理每條規則的方式，例如，允許執行使某些工作流工作自動化的 PowerShell 指令碼。Kaspersky Endpoint Security 會同時更新規則集和應用程式資料庫。規則集的更新必須手動確認。

“自適應異常控制”設定

配置“自適應異常控制”包括以下步驟：

1. 訓練“自適應異常控制”。

   啟用“自適應異常控制”後，其規則在*訓練模式*下工作。在訓練期間，“自適應異常控制”監控規則觸發並將觸發事件傳送到卡巴斯基安全管理中心。每條規則都有自己的訓練模式持續時間。訓練模式持續時間由 Kaspersky 專家設定。通常，訓練模式保持活動兩周。

   如果在訓練期間某條規則完全未觸發，“自適應異常控制”會將與此規則關聯的操作視為非典型操作。Kaspersky Endpoint Security 將封鎖與該規則相關的所有操作。

   如果在訓練期間觸發了某條規則，Kaspersky Endpoint Security 會將事件記錄在規則觸發報告和**智慧培訓狀態中的規則觸發器**儲存區中。

2. 分析規則觸發報告。

   管理員分析 規則觸發報告 或內容 **智慧培訓狀態中的規則觸發器** 儲存區。然後管理員可以選取在觸發規則時“自適應異常控制”的行為：封鎖或允許。管理員還可以繼續監控規則的工作方式並延長訓練模式的持續時間。如果管理員未採取任何操作，應用程式也將繼續在訓練模式下工作。訓練模式期限重新開始。

“自適應異常控制”透過以下通道即時配置：

- “自適應異常控制”自動開始封鎖與從未在訓練模式中觸發的規則相關聯的操作。
- Kaspersky Endpoint Security 新增新規則或刪除過時規則。
- 管理員在檢視規則觸發報告和“**智慧培訓狀態中的規則觸發器**”儲存區的內容後配置“適應性異常控制”的操作。我們建議檢查有關規則觸發的報告以及 **智慧培訓狀態中的規則觸發器** 儲存區的內容。

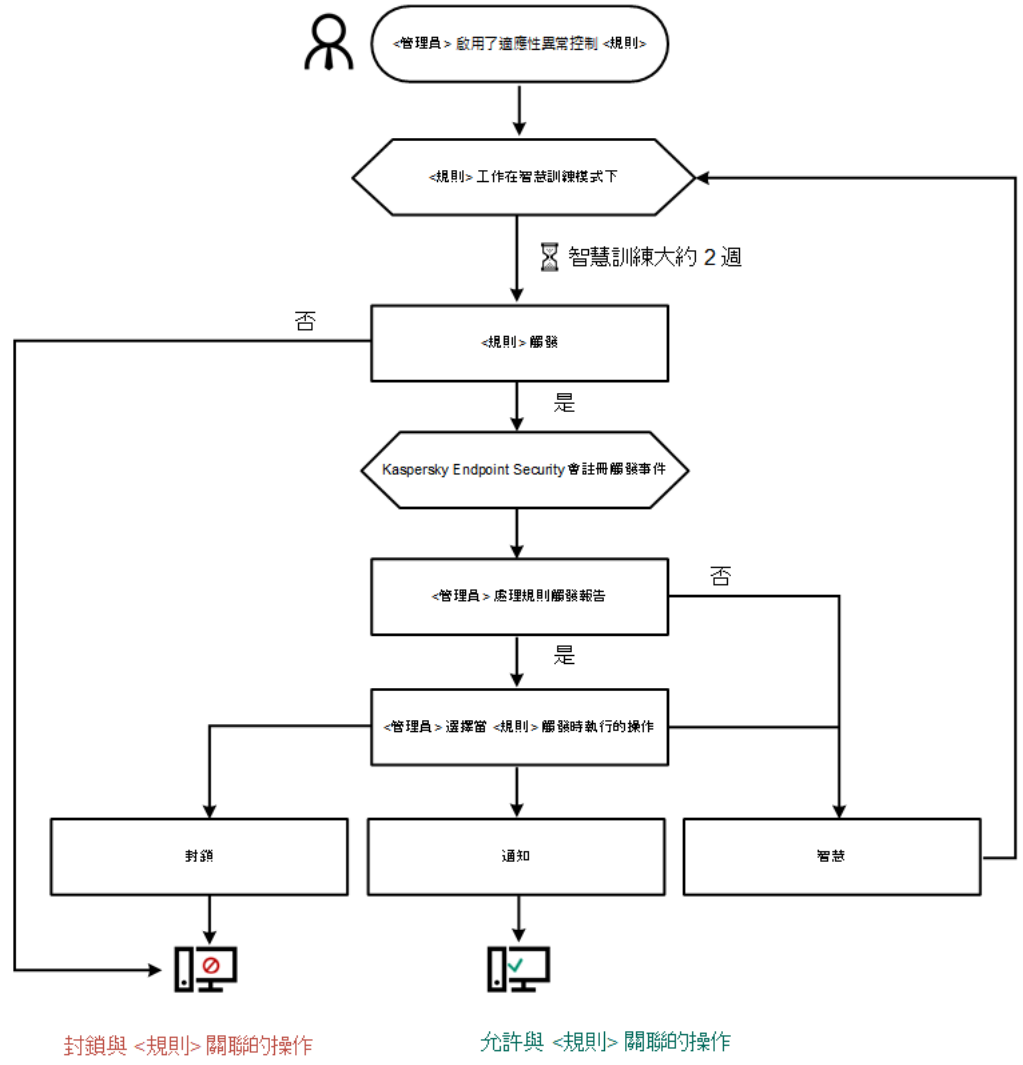
當惡意應用程式嘗試執行操作時，Kaspersky Endpoint Security 將封鎖該操作並顯示通知（請參見下圖）。




“自適應異常控制”通知

## “自適應異常控制”操作演算法

Kaspersky Endpoint Security 根據以下演算法決定是允許還是封鎖與某條規則關聯的操作（請參見下圖）。




“自適應異常控制”操作演算法

適應性異常控制元件設定

| 參數 | 描述 |
| --- | --- |
| **自適應異常控制規則狀態報告**<br>*（僅在卡巴斯基安全管理中心主控台中可用）* | 該報告包含有關適應性異常控制偵測規則狀態的資訊（例如，*已停用*或*封鎖*）。該報告針對所有管理群組生成。 |
| **自適應異常控制規則觸發報告**<br>*（僅在卡巴斯基安全管理中心主控台中可用）* | 該報告包含使用“適應性異常控制”偵測到的非典型操作的相關資訊。該報告針對所有管理群組生成。 |

| 參數 | 描述 |
| --- | --- |
| **規則** | 適應性異常控制規則表。規則由 Kaspersky 專家根據惡意活動的典型情景建立。 |
| **範本** | **有關封鎖的訊息**當封鎖非典型操作的自適應異常控制規則觸發時，顯示給使用者的訊息的範本。<br>**傳送郵件給管理員**當使用者認為封鎖是錯誤的時可以傳送給本機公司網路系統管理員的訊息的範本。在使用者請求提供存取權限後，Kaspersky Endpoint Security 會向卡巴斯基安全管理中心傳送一個事件：**傳送給管理員的應用程式活動封鎖訊息**。事件描述包含一條給管理員的訊息，其中包含被替換的變數。您可以使用預定義事件選擇**使用者請求**在卡巴斯基安全管理中心主控台中檢視這些事件。如果您的組織沒有部署卡巴斯基安全管理中心或者沒有連線到管理伺服器，應用程式將向管理員傳送一條訊息到指定的電子郵件信箱。 |

# 系統完整性監控

如果 Kaspersky Endpoint Security 安裝在執行 Windows for Servers 的電腦上，則該元件可用。如果 Kaspersky Endpoint Security 安裝在執行 Windows for Workstations 的電腦上，則該元件不可用。

從版本 12.6 開始，Kaspersky Endpoint Security for Windows 包含系統完整性監控元件，而不是檔案完整性監控元件。系統完整性監控元件包括檔案完整性監控的所有功能，此外還允許監控登錄機碼變更和外部裝置的連線。

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示。系統完整性監控可以即時模式運行，也可以按需執行系統完整性檢查。

## 即時系統完整性監控

在即時模式下，系統完整性監控追蹤您包含在元件範圍（*監控範圍*）中的物件的變更。系統完整性監控還可以即時封鎖對此類物件的未經授權的存取。

## 按需系統完整性檢查

按需系統完整性檢查是一項可以手動或按排程執行的工作。若要執行*系統完整性檢查*工作，您必須配置元件的範圍（*監控範圍*）並建立基線。*基線*是系統中物件的記錄狀態，應用程式在與目前狀態進行比較時將其用作參考。

系統完整性監控設定

| 參數 | 描述 |
| --- | --- |
| **用於封鎖規則的操作模式** | • **封鎖**在此模式下，系統完整性監控會封鎖監控範圍內的檔案和登錄機碼的操作，並產生對應的事件。<br>• **通知**在此模式下，系統完整性監控允許對監控範圍內的檔案和登錄機碼進行操作，並產生相應的事件。 |
| **即時系統完整性監控** | 在即時模式下，系統完整性監控追蹤您包含在元件範圍（*監控範圍*）中的物件的變更。系統完整性監控還可以即時封鎖對此類物件的未經授權的存取。 |
| **監控裝置** | 系統完整性監控監控外部裝置的連線和斷開連線。 |
| **監控檔案和登錄檔** | 系統完整性監控監控檔案、資料夾和登錄機碼的變更。 |
| **系統完整性檢查** | 按需系統完整性檢查是一項可以手動或按排程執行的工作。若要執行*系統完整性檢查*工作，您必須配置元件的範圍（*監控範圍*）並建立基線。*基線*是系統中物件的記錄狀態，應用程式在與目前狀態進行比較時將其用作參考。 |

# Endpoint Sensor

Kaspersky Endpoint Security 11.4.0 不包含 Endpoint Sensor。

您可以在卡巴斯基安全管理中心網頁主控台和卡巴斯基安全管理中心管理主控台中管理 Endpoint Sensor。
無法在卡巴斯基安全管理中心雲端主控台中管理 Endpoint Sensor。

*Endpoint Sensor* 設計用於與 Kaspersky Anti Targeted Attack Platform 進行互動。*Kaspersky Anti Targeted Attack Platform* 是旨在及時偵測複雜威脅（如針對性攻擊、進階持久性威脅 (APT)、零日攻擊等）的解決方案。
Kaspersky Anti Targeted Attack Platform 包括三個功能單元：

- Kaspersky Anti Targeted Attack Platform (*KATA*)
- Kaspersky Endpoint Detection and Response (*EDR (KATA)*)
- Network Detection and Response (*NDR (KATA)*)

您可以單獨購買所有功能單元或單獨的功能單元。有關解決方案的詳細資訊，請參閱 Kaspersky Anti Targeted Attack Platform 說明。

管理 Endpoint Sensor 具有以下限制：

- 如果電腦上已安裝 Kaspersky Endpoint Security 版本11.0.0 至11.3.0，則可以使用政策設定 Endpoint Sensor 設定。有關使用政策設定 Endpoint Sensor 設定的更多資訊，請參閱適用於 Kaspersky Endpoint Security 早期版本的說明文章。
- 如果電腦上已安裝 Kaspersky Endpoint Security 版本11.4.0 及更高版本，則無法在政策中設定 Endpoint Sensor 設定。

“Endpoint Sensor”安裝在用戶端電腦上。在這些電腦上，該元件將持續監控處理程序、活動網路連線和被修改的檔案。Endpoint Sensor 將資訊中繼給 KATA 伺服器。

此元件的功能在以下作業系統下可用：

- Windows 7 Service Pack 1 Home / Professional / Enterprise；
- Windows 8.1.1 Professional / Enterprise；
- Windows 10 RS3 Home / Professional / Education / Enterprise;
- Windows 10 RS4 Home / Professional / Education / Enterprise;
- Windows 10 RS5 Home / Professional / Education / Enterprise;
- Windows 10 RS6 Home / Professional / Education / Enterprise;
- Windows Server 2008 R2 Foundation / Standard / Enterprise（64 位元）；
- Windows Server 2012 Foundation / Standard / Enterprise（64 位元）；

- Windows Server 2012 R2 Foundation / Standard / Enterprise（64 位元）；
- Windows Server 2016 Essentials / Standard（64 位元）。

有關 KATA 操作的詳細資訊，請參閱 Kaspersky Anti Targeted Attack Platform 說明。

# Sandbox

Kaspersky Endpoint Security for Windows 包含一個用於與 Kaspersky Sandbox 解決方案整合的內建代理。*Sandbox*元件可偵測和自動封鎖電腦上的進階威脅。Sandbox 會分析物件行為以偵測惡意行動和組織的 IT 基礎架構上的針對性攻擊所特有的活動。Sandbox 會分析和掃描部署了 Microsoft Windows 作業系統的虛擬影像的特殊伺服器（Sandbox 伺服器）上的物件。有關解決方案的詳細資訊，請參閱 Kaspersky Sandbox 說明 和 Kaspersky Anti Targeted Attack Platform 說明。

從版本 12.7 開始，Kaspersky Endpoint Security for Windows 支援 Sandbox 元件，該元件是 Kaspersky Anti Targeted Attack Platform 解決方案的一部分。與 Kaspersky Sandbox 解決方案相比，KATA Sandbox 元件不僅允許自動掃描檔案，還允許從檔案內容功能表中手動掃描檔案。

KATA Sandbox 需要部署 Kaspersky Anti Targeted Attack Platform 7.0 或更高版本。

該元件只可以使用卡巴斯基安全管理中心網頁主控台進行管理。您不能使用管理主控台 (MMC) 管理此元件。

Sandbox 元件設定

| 參數 | 描述 |
| --- | --- |
| **整合模式** | **Kaspersky Sandbox**與 Kaspersky Sandbox 解決方案整合。應用程式僅會在自動模式下將檔案傳送到 Kaspersky Sandbox 進行掃描。<br>**KATA Sandbox**與 Kaspersky Anti Targeted Attack Platform 解決方案的 Sandbox 元件整合。您可以選取用於掃描的檔案提交模式：<br>• **手動**使用者從內容功能表（**傳送到 Sandbox**）中手動提交檔案進行掃描。<br>• **自動**應用程式自動偵測物件並將其提交到 Sandbox 進行掃描。<br>• **組合** |
| **伺服器連線設定** | **逾時 (毫秒)**沙盒伺服器（用於 Kaspersky Sandbox）或中央節點伺服器（用於 KATA）的連線逾時。配置的逾時經過後，Kaspersky Endpoint Security 會傳送請求給下一個伺服器。如果您的連線速度慢或者連線不穩定，您可以增加伺服器的連線逾時。建議的請求逾時為 0.5 秒鐘或更短。<br>**請求佇列**請求佇列資料夾大小在 Sandbox 中傳送多個物件進行掃描時，Kaspersky Endpoint Security 會建立一個請求佇列。預設情況下，請求佇列資料夾大小限制為 100 MB。在達到最大的大小後，Sandbox 會停止向佇列新增請求並將相應事件傳送到卡巴斯基安全管理中心。您可以根據伺服器配置來設定請求佇列資料夾大小。<br>**伺服器 TLS 憑證**要設定與沙盒伺服器（對於 Kaspersky Sandbox）或中央節點伺服器（對於 KATA）的可信任連線，您必須準備 TLS 憑證。然後，您必須使用政策將憑證新增至電腦。您還需要將憑證新增至 Sandbox 伺服器（對於 Kaspersky Sandbox）或 Central Node 伺服器（用於 KATA）。<br>**使用雙向身分驗證**（僅適用於 KATA Sandbox）。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。 |
| **連線到 Sandbox 伺服器** | **Kaspersky Sandbox**。Sandbox 伺服器連線設定。伺服器使用部署的 Microsoft Windows 作業系統的虛擬影像來執行需要掃描的物件。您可以輸入一個 IP 位址（IPv4 或者 IPv6）或者完全限定網域名稱。<br>**KATA Sandbox**。中心節點伺服器連線設定。中央節點可選擇最佳掃描設定並平衡沙盒伺服器之間的負載。 |

| 參數 | 描述 |
| --- | --- |
| **偵測到威脅後的動作** | **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 會建立備份副本以防物件以後需要還原。Kaspersky Endpoint Security 會將備份副本移動到隔離。<br>**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 會掃描內核記憶體、執行處理序和磁碟的開啟磁區。<br>**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、掃描範圍和偵測到 IOC 後的動作：刪除物件，執行*關鍵區域掃描*工作。若要修改 "*IOC 掃描*"工作的其它設定，請前往工作設定。 |
| **IOC 掃描範圍** | **關鍵檔案區域**如果選擇該選項，則 Kaspersky Endpoint Security 僅在電腦的關鍵檔案區域執行 IOC 掃描：內核記憶體和開機磁區。<br>**電腦的系統磁碟機上的檔案區域**如果選擇該選項，則 Kaspersky Endpoint Security 會在電腦的系統磁碟機上執行 IOC 掃描。 |
| **執行 IOC 掃描工作** | **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。<br>**自動**執行模式，只要偵測到威脅 Kaspersky Endpoint Security 就執行 *IOC 掃描*工作。<br>**僅在電腦空閒時執行**執行模式，如果熒幕防護程式啟動或者熒幕被鎖定則 Kaspersky Endpoint Security 執行 *IOC 掃描*工作。如果使用者解鎖了電腦，Kaspersky Endpoint Security 會暫停工作。這意味著工作可能會費時數天完成。 |

# Managed Detection and Response

Kaspersky Endpoint Security for Windows 支援與 Managed Detection and Response 解決方案整合。*Kaspersky Managed Detection and Response (MDR)* 解決方案可自動偵測和分析您的基礎架構中的安全事件。為此，MDR 會使用從端點和機學習收到的遙測資料。MDR 會將事件資料傳送給卡巴斯基專家。專家然後可以處理事件，並且，例如，新增新項目至病毒資料庫。或者，專家可以簽發事件處理建議，並且，例如，建議從網路中隔離電腦。如欲瞭解該解決方案如何工作的詳細資訊，請參閱 Kaspersky Managed Detection and Response 說明。

Managed Detection and Response 設定

| 參數 | 描述 |
| --- | --- |
| MDR 設定檔 | BLOB 檔案包含用戶端 ID 以及有關卡巴斯基 Managed Detection and Response 產品許可的資訊。BLOB 檔案位於 MDR 設定檔的 ZIP 存檔中。您可以在 Kaspersky Managed Detection and Response 主控台中獲取 ZIP 存檔。有關 BLOB 檔案的詳細資訊，請參閱 Kaspersky Managed Detection and Response 說明。 |

# Endpoint Detection and Response

Kaspersky Endpoint Security for Windows 包括 Kaspersky Endpoint Detection and Response Optimum 解決方案（以下也稱為 "EDR Optimum"）的內建代理。從版本 11.8.0 開始，Kaspersky Endpoint Security for Windows 包括 Kaspersky Endpoint Detection and Response 解決方案（以下也稱為 "EDR Expert"）的內建代理。*Kaspersky Endpoint Detection and Response* 是用於防護組織的 IT 基礎架構抵禦進階網路威脅的一系列解決方案。解決方案的功能結合了自動偵測威脅和回應這些威脅的能力，以抵消包括新漏洞、勒索軟體、無檔案攻擊以及使用合法系統工具的方法。EDR Expert 比 EDR Optimum 提供更多的威脅監控和回應功能。有關解決方案的詳細資訊，請參閱 Kaspersky Endpoint Detection and Response Optimum 說明 與 Kaspersky Endpoint Detection and Response Expert 說明。

Kaspersky Endpoint Detection and Response 會審查和分析威脅發展並向*安全人員*或者*管理員*提供有關需要作出及時回應的潛在攻擊的資訊。Kaspersky Endpoint Detection and Response 會在單獨視窗中顯示偵測詳情。*警示*是企業 IT 基礎架構中的事件，應用程式已將其識別為異常或可疑，可能對企業 IT 基礎架構構成安全威脅。*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。

您可以在網頁主控台和雲端主控台中配置 EDR Optimum 元件。適用於 EDR Expert 的元件設定僅在雲端主控台中可以使用。

| 參數 | 描述 |
| --- | --- |
| **啟用進階系統活動記錄** | 延伸遙測技術可提高 IOC 偵測的準確性，但會佔用更多電腦資源。我們建議在電腦上啟用延伸遙測功能以進行回顧 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。此模式旨在偵測電腦網路活動資料中的入侵指標。<br>如果停用延伸遙測功能，Kaspersky Endpoint Security 可能會輪換有關偵測到的入侵指標的資訊。 |
| **網路隔離** | 回應偵測到的威脅自動將電腦從網路中隔離。<br>當開啟網路隔離時，應用程式會斷開電腦上的所有活動連線並封鎖所有新的 TCP/IP 連線。應用程式只會讓以下連線處於活動狀態：<br>• 網路隔離排除項目中列出的連線。<br>• Kaspersky Endpoint Security 服務安裝的連線。<br>• 卡巴斯基安全管理中心網路代理啟動的連線。 |
| **自動解鎖隔離裝置的時間 (小時)** | 指定時間後可以自動或者手動關閉網路隔離。預設情況下，Kaspersky Endpoint Security 會在隔離啟動 5 小時後關閉網路隔離。 |
| **網路隔離排除項目** | 從網路隔離中排除的規則清單當開啟網路隔離時，電腦上匹配規則的網路連線不會被封鎖。<br>要配置網路隔離排除項目，您可以使用"*標準網路設定檔*"清單。預設情況下，排除項目包括包含確保裝置（具有 DNS/DHCP 伺服器和 DNS/DHCP 用戶端角色）不中斷操作的規則的網路設定檔。您也可以修改標準網路設定檔的設定或者手動定義排除項目。<br>只有當網路隔離回應偵測到的威脅自動開啟時，政策內容中指定的排除項目才會套用。只有當網路隔離在卡巴斯基安全管理中心主控台的電腦內容或者警示詳情中手動開啟時，電腦內容中指定的排除項目才會套用。 |
| **執行防止** | 控制可執行檔和指令碼的執行以及 Office 格式檔案的開啟。例如，您可以防止執行在選取電腦上被認為不安全的應用程式。執行防護支援Office 檔案延伸程式集合和指令碼解譯器集合。<br>所要使用執行防護元件，您需要新增執行防護規則。*執行防護規則*是應用程式對物件執行進行回應（例如，封鎖物件執行時）時考慮的一組條件。應用程式根據檔案路徑或者使用 MD5 和 SHA256 雜湊演算法計算的總和檢查碼來識別檔案。 |
| **執行或開啟被禁止的物件時的動作** | **封鎖並新增至事件記錄**在此模式中，應用程式會封鎖執行物件或者開啟匹配防護規則條件的文件。應用程式也會將嘗試執行物件或者開啟文件的事件發佈到 Windows 事件記錄和卡巴斯基安全管理中心事件記錄。<br>**新增至事件記錄**在此模式中，Kaspersky Endpoint Security 會將嘗試執行可執行物件或者開啟匹配防護規則條件的文件的事件發佈到 Windows 事件記錄和卡巴斯基安全管理中心，但是不會封鎖執行或者開啟物件或者文件的嘗試。預設情況下已選擇此模式。 |
| **執行防止規則** | *執行防護規則*是應用程式對物件執行進行回應（例如，封鎖物件執行時）時考慮的一組條件。應用程式根據檔案路徑或者使用 MD5 和 SHA256 雜湊演算法計算的總和檢查碼來識別檔案。 |
| **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識別惡意活動和決定其信譽。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。<br>Cloud Sandbox 技術永久啟用，對所有卡巴斯基安全網路使用者可用，與他們使用的產品授權類型無關。<br>如果選擇該核取方塊，Kaspersky Endpoint Security 將在 **威脅偵測技術** 下的應用程式主視窗中啟用使用 Cloud Sandbox 偵測到的威脅的計數器。Kaspersky Endpoint Security 也會在應用程式事件中和在卡巴斯基安全管理中心主控台的*威脅報告*中指明 Cloud Sandbox 威偵測技術。 |

# Endpoint Detection and Response Expert（本地部署）

## Endpoint Detection and Response Expert（本地部署）

Kaspersky Endpoint Security for Windows 支援與 Kaspersky Endpoint Detection and Response Expert (on-premise) 解決方案整合。*Kaspersky Endpoint Detection and Response Expert（本地部署）*是一款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（本地部署）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 (on-premise) 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 (on-premise) 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 (on-premise) 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。

## Endpoint Detection and Response (KATA)

Kaspersky Endpoint Security for Windows 支援 Kaspersky Endpoint Detection and Response 元件作為 Kaspersky Anti Targeted Attack Platform (EDR (KATA)) 解決方案的一部分工作。*Kaspersky Anti Targeted Attack Platform* 是旨在及時偵測複雜威脅（如針對性攻擊、進階持久性威脅 (APT)、零日攻擊等）的解決方案。Kaspersky Anti Targeted Attack Platform 包括三個功能單元：

- Kaspersky Anti Targeted Attack Platform (*KATA*)
- Kaspersky Endpoint Detection and Response (*EDR (KATA)*)
- Network Detection and Response (*NDR (KATA)*)

您可以單獨購買所有功能單元或單獨的功能單元。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 Anti Targeted Attack Platform 伺服器。在此情況下，Kaspersky Endpoint Security 應用程式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 Kaspersky Anti Targeted Attack Platform 伺服器。

EDR (KATA) 和 NDR (KATA) 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 Kaspersky Anti Targeted Attack Platform 主控台進行管理，包括執行工作、管理隔離物件、檢視報告和其他操作。

| 參數 | 描述 |
| --- | --- |
| **遙測資料收集伺服器連線** | *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。<br>配置以下內容以連線到遙測資料收集伺服器（KUMA）：<br>• **逾時（秒）**伺服器回應最長逾時。當逾時用完時，Kaspersky Endpoint Security 會嘗試連線到不同的伺服器。<br>• **伺服器憑證**用於與伺服器建立可信連線的 TLS 憑證。您可以在開放式單一管理平台上取得 TLS 憑證（請參閱 Kaspersky Endpoint Detection and Response Expert （內部部署版）說明）。<br>• **使用雙向身分驗證**在 Kaspersky Endpoint Security 和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。您可以在開放式單一管理平台上取得加密容器（請參閱 Kaspersky Endpoint Detection and Response Expert （內部部署版）說明）。配置伺服器設定後，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。<br>加密容器必須受密碼防護。無法新增密碼為空的加密容器。 |
| **位址** 和 **連接埠**（遙測資料收集伺服器） | 遙測資料收集伺服器的連線設定。您可以輸入 IP 位址（IPv4 或 IPv6）。<br>您可以新增多個遙測資料收集伺服器位址。Kaspersky Endpoint Security 嘗試連線到第一個 IP 位址的伺服器。如果無法建立連線，Kaspersky Endpoint Security 將嘗試連線到清單中的第二個 IP 位址，依此類推。 |
| **將遙測資料傳送至遙測資料收集伺服器** | 此功能可讓您完全關閉向 KATA 伺服器傳送遙測。例如，如果您將 Kaspersky Anti Targeted Attack Platform 與另一個也使用遙測的解決方案一起使用，您可以關閉 KATA (EDR) 的遙測資料傳送。這可讓您最佳化這些解決方案的伺服器負載。如果您部署了 Managed Detection and Response 解決方案和 KATA (EDR)，則可以使用 MDR 遙測並在 KATA (EDR) 中建立「威脅回應」工作。<br>• **僅傳送具有 IOA 的遙測**這可以最佳化遙測資料，並僅傳送含 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。<br>• **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。<br>• **限制每次傳輸的事件封包數量**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。此功能允許在與伺服器同步之前停用事件緩衝。 |
| **啟用請求節流** | 該功能有助於最佳化伺服器負載。如果選中該核取方塊，應用程式將限制傳輸的事件。如果事件數量超過配置的限制，Kaspersky Endpoint Security 將停止傳送事件。<br>配置遙測設定：<br>• **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。<br>• **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%。 |
| **傳送同步請求到伺服器的時間間隔 (分)** | 傳送到伺服器的同步請求的頻率。在同步期間，Kaspersky Endpoint Security 傳送有關被修改應用程式設定和工作的資訊。 |
| **連線至回應伺服器** | *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。<br>為回應伺服器連線設定以下內容：<br>• **逾時（秒）**伺服器回應最長逾時。當逾時用完時，Kaspersky Endpoint Security 會嘗試連線到不同的伺服器。<br>• **伺服器憑證**用於與伺服器建立可信連線的 TLS 憑證。您可以在開放式單一管理平台上取得 TLS 憑證（請參閱 Kaspersky Endpoint Detection and Response Expert （內部部署版）說明）。<br>• **使用雙向身分驗證**在 Kaspersky Endpoint Security 和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。您可以在開放式單一管理平台上取得加密容器（請參閱 Kaspersky Endpoint Detection and Response Expert （內部部署版）說明）。配置伺服器設定後，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。 |
| **位址** 和 **連接埠**（回應伺服器） | 回應伺服器的連線設定。您可以輸入 IP 位址（IPv4 或 IPv6）。<br>您可以新增多個遙測資料收集伺服器位址。Kaspersky Endpoint Security 嘗試連線到第一個 IP 位址的伺服器。如果無法建立連線，Kaspersky Endpoint Security 將嘗試連線到清單中的第二個 IP 位址，依此類推。 |

| 參數 | 描述 |
| --- | --- |
| **傳送同步請求到伺服器的時間間隔 (分)** | 傳送到伺服器的同步請求的頻率。在同步期間，Kaspersky Endpoint Security 傳送有關被修改應用程式設定和工作的資訊。 |
| **連線到 KATA 伺服器** | 為 Central Node 伺服器連線設定以下內容：<br>• **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。<br>• **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）。<br>• **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。<br>加密容器必須受密碼防護。無法新增密碼為空的加密容器。 |
| **位址** 和 **連接埠**（KATA 伺服器） | Kaspersky Anti Targeted Attack Platform 伺服器的連線設定。請輸入 Central Node 伺服器 IP 位址（IPv4 或 IPv6）和連線到伺服器的連接埠。<br>您可以新增多個中央節點伺服器位址。Kaspersky Endpoint Security 嘗試連線到第一個 IP 位址的伺服器。如果無法建立連線，Kaspersky Endpoint Security 將嘗試連線到清單中的第二個 IP 位址，依此類推。 |
| **傳送遙測資料到 KATA** | 此功能可讓您完全關閉向 KATA 伺服器傳送遙測。例如，如果您將 Kaspersky Anti Targeted Attack Platform 與另一個也使用遙測的解決方案一起使用，您可以關閉 KATA (EDR) 的遙測資料傳送。這可讓您最佳化這些解決方案的伺服器負載。如果您部署了 Managed Detection and Response 解決方案和 KATA (EDR)，則可以使用 MDR 遙測並在 KATA (EDR) 中建立「威脅回應」工作。<br>配置遙測設定：<br>• **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。<br>• 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。 |
| **啟用請求節流** | 該功能有助於最佳化伺服器負載。如果選中該核取方塊，應用程式將限制傳輸的事件。如果事件數量超過配置的限制，Kaspersky Endpoint Security 將停止傳送事件。<br>配置遙測設定：<br>• **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。<br>• **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%。 |

# Network Detection and Response (KATA)

Kaspersky Endpoint Security for Windows 支援 Kaspersky Network Detection and Response 元件作為 Kaspersky Anti Targeted Attack Platform (EDR (KATA)) 解決方案的一部分工作。*Kaspersky Anti Targeted Attack Platform* 是旨在及時偵測複雜威脅（如針對性攻擊、進階持久性威脅 (APT)、零日攻擊等）的解決方案。Kaspersky Anti Targeted Attack Platform 包括三個功能單元：

- Kaspersky Anti Targeted Attack Platform (*KATA*)
- Kaspersky Endpoint Detection and Response (*EDR (KATA)*)
- Network Detection and Response (*NDR (KATA)*)

您可以單獨購買所有功能單元或單獨的功能單元。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 Anti Targeted Attack Platform 伺服器。在此情況下，Kaspersky Endpoint Security 應用程式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 Kaspersky Anti Targeted Attack Platform 伺服器。

EDR (KATA) 和 NDR (KATA) 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 Kaspersky Anti Targeted Attack Platform 主控台進行管理，包括執行工作、管理隔離物件、檢視報告和其他操作。

僅 Network Detection and Response (KATA) 參數

| 參數 | 描述 |
| --- | --- |
| **伺服器連線設定** | **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。<br>**伺服器 TLS 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）。<br>**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。<br>加密容器必須受密碼防護。無法新增密碼為空的加密容器。 |
| **位址**和**連接埠** | Kaspersky Anti Targeted Attack Platform 伺服器的連線設定。請輸入 Central Node 伺服器 IP 位址（IPv4 或 IPv6）和連線到伺服器的連接埠。<br>您可以新增多個中央節點伺服器位址。Kaspersky Endpoint Security 嘗試連線到第一個 IP 位址的伺服器。如果無法建立連線，Kaspersky Endpoint Security 將嘗試連線到清單中的第二個 IP 位址，依此類推。 |
| **傳送同步請求到 NDR 伺服器的間隔（分）** | 傳送到伺服器的同步請求的頻率。在同步期間，Kaspersky Endpoint Security 傳送有關被修改應用程式設定和工作的資訊。 |
| **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。 |
| **啟用請求節流** | 該功能有助於最佳化伺服器負載。如果選中該核取方塊，應用程式將限制傳輸的事件。如果事件數量超過配置的限制，Kaspersky Endpoint Security 將停止傳送事件。 |
| **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%。 |

# 與 KUMA 整合

Kaspersky Endpoint Security for Windows 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。

| 參數 | 描述 |
| --- | --- |
| **傳送事件時的最大延遲（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。 |
| **連線到 KUMA 伺服器** | **逾時（秒）** KUMA 伺服器響應最大逾時。當超時用完時，Kaspersky Endpoint Security 會嘗試連線到不同的 KUMA 伺服器。<br>**伺服器憑證**用於與 KUMA 伺服器建立可信連線的 TLS 憑證。您可以在 Kaspersky Unified Monitoring and Analysis Platform 主控台中取得 TLS 憑證（請參閱 Kaspersky Unified Monitoring and Analysis Platform 中的說明）。<br>若要建立可信任連線，在 KUMA 主控台的 tcp 連線器設定中，您必須選擇 **With verification** TLS 模式（請參閱 Kaspersky Unified Monitoring and Analysis Platform 說明 中 tcp 類型連線器的設定）。<br>**使用雙向身分驗證**在 Kaspersky Endpoint Security 和 KUMA 之間建立安全連線時進行雙向身分驗證。若要使用雙向身分驗證，在 KUMA 主控台的 tcp 連線器設定中，您必須選擇 **Custom PFX** TLS 模式（請參閱 Kaspersky Unified Monitoring and Analysis Platform 說明 中 tcp 類型連線器的設定）。然後您必須取得加密容器並設定密碼來保護該加密容器。*加密容器*是一個帶有憑證和私鑰的 PFX 存檔。配置 KUMA 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。<br>加密容器必須受密碼防護。無法新增密碼為空的加密容器。 |
| KUMA 伺服器 | 與 Kaspersky Unified Monitoring and Analysis Platform 伺服器的連線設定。您可以輸入 IP 位址（IPv4 或 IPv6）。<br>您可以新增多個 KUMA 伺服器位址。Kaspersky Endpoint Security 嘗試連線到第一個 IP 位址的伺服器。如果無法建立連線，Kaspersky Endpoint Security 將嘗試連線到清單中的第二個 IP 位址，依此類推。 |

# 完整磁碟加密

您可以選取加密技術：卡巴斯基磁碟加密或 BitLocker 磁碟機加密（以下簡稱"BitLocker"）。

## 卡巴斯基磁碟加密

加密系統硬碟後，在下次電腦啟動時，使用者要能夠存取硬碟並且作業系統載入前，使用者必須透過身分驗證代理的驗證。這需要輸入權杖或連線到電腦的智能卡的密碼，或者輸入由局域網管理員使用"*管理身分驗證代理帳戶*"工作建立的身分驗證代理帳戶的使用者名稱和密碼。這些帳戶以使用者登入作業系統的 Microsoft Windows 帳戶為基礎。您還可以使用Single Sign-On (SSO) 技術，此技術允許您使用身分驗證代理帳戶的使用者名稱和密碼自動登入至作業系統。

可以透過兩種方式在身分驗證代理中執行使用者身分驗證：

- 輸入區域網路管理員使用卡巴斯基安全管理中心工具建立的身分驗證代理帳戶的使用者名稱和密碼。
- 輸入連線至電腦的令牌的密碼或智慧卡的密碼。

如果電腦硬碟磁碟機使用 AES256 加密演算法進行加密，則可以使用令牌或智慧卡。如果使用 AES256 演算法加密了電腦硬碟磁碟機，新增電子憑證檔案到指令將被拒絕。

## BitLocker 磁碟機加密

*BitLocker* 是 Windows 作業系統內建的加密技術。Kaspersky Endpoint Security 可讓您利用 Kaspersky Next 基礎架構控制和管理 Bitlocker。BitLocker 可對邏輯磁區進行加密。BitLocker 不能用於卸除式磁碟機的加密。有關 BitLocker 的詳細資訊，請參閱 Microsoft 文件。

加密磁碟時，BitLocker將引導程式和其他輔助檔案放入 system partition。此分割區未加密。作業系統在安裝 Windows 時會自動建立系統分割區。如果在安裝 Windows 之前磁碟已完全分割，則作業系統無法建立系統分割區。在這種情況下，當啟動 BitLocker 磁碟加密時，作業系統會提示使用者對磁碟重新分割，並建立系統分割區。建立系統分割區後，作業系統啟動 BitLocker 加密。

BitLocker 使用受信任平台模組提供對存取金鑰的安全儲存。A *Trusted Platform Module* (TPM) 是一個與安全相關並提供基本功能的微晶片（例如用於儲存加密金鑰）。受信任平台模組通常安裝在電腦主機板上並且透過硬體匯流排與其他所有系統元件進行互動。使用 TPM 是儲存 BitLocker 存取金鑰最安全的方式，因為 TPM 提供了啟動前系統完整性驗證。您仍然可以在沒有 TPM 的電腦上對磁碟機進行加密。在這種情況下，將使用密碼對存取金鑰進行加密。BitLocker 使用以下身分驗證方式：

- TPM。
- TPM 和 PIN。
- 密碼。

對系統硬碟磁碟機進行加密後，使用者需要透過 BitLocker 身分驗證才能啟動作業系統。身分驗證完成後，BitLocker 將允許使用者登入。BitLocker 不支援單點登錄技術 (SSO)。

在對磁碟機進行加密後，BitLocker 會建立一個主密碼。Kaspersky Endpoint Security 會將主密碼傳送到卡巴斯基安全管理中心，以便您可以還原對磁碟的存取，例如，如果使用者忘記了密碼。

如果使用者使用 BitLocker 對磁碟進行加密，Kaspersky Endpoint Security 會將有關磁碟加密的資訊傳送到卡巴斯基安全管理中心。但是，Kaspersky Endpoint Security 不會將主密碼傳送到卡巴斯基安全管理中心，因此將無法使用卡巴斯基安全管理中心還原對磁碟的存取。為使 BitLocker 與卡巴斯基安全管理中心正常協同工作，請解密磁碟機，然後使用政策重新對該磁碟機進行加密。您可以在本機解密磁碟機，也可以使用政策來解密磁碟機。

如果正在使用 Windows 群組政策，請在政策設定中關閉 BitLocker 管理。Windows 政策設定可能與 Kaspersky Endpoint Security 政策設定衝突。在對磁碟機進行加密時，可能會發生錯誤。

卡巴斯基磁碟加密元件設定

| 參數 | 描述 |
| --- | --- |
| **加密模式** | **加密所有硬碟磁碟機**如果選擇此選項，套用政策後，應用程式將加密所有硬碟。<br>如果電腦安裝了多個作業系統，在加密後，您將能夠只載入安裝了應用程式的作業系統。<br>**解密所有硬碟磁碟機**如果選擇此選項，套用政策後，應用程式將解密先前已加密的所有硬碟。<br>**保留不變**如果選定了該選項，套用政策後，應用程式將保留硬碟不動。如果磁碟機已加密，則其仍加密。如果磁碟機已解密，則其仍解密。預設情況下已勾選此項目。 |
| **加密時對 Windows 使用者自動建立身分驗證代理帳戶** | 如果選中此核取方塊，則應用程式將基於電腦上的 Windows 使用者帳戶清單建立身分驗證代理帳戶。預設情況下，Kaspersky Endpoint Security 使用在過去30 天內登入到作業系統的使用者所使用的所有本機帳戶和網域帳戶。 |

| 參數 | 描述 |
| --- | --- |
| **身分驗證代理帳戶建立設定** | **電腦上的所有帳戶**任何時間啟動過的電腦上的所有帳戶。<br>**電腦上所有網域帳戶**屬於某些網域且在任何時間啟動過的電腦上的所有帳戶。<br>**電腦上所有本機帳戶**任何時間啟動過的電腦上的所有本機帳戶。<br>**具有一次性密碼的服務賬戶**獲取電腦的存取權限時（例如，當使用者忘記密碼時）需要該服務帳戶。您也可以將服務帳戶作為備用帳戶。您可以輸入帳戶名稱（預設為 `ServiceAccount`）。Kaspersky Endpoint Security 會自動建立密碼。您只能在卡巴斯基安全管理中心主控台中查找密碼。<br>**本機管理員**Kaspersky Endpoint Security 會為電腦的本機管理員建立一個身分驗證代理使用者帳戶。<br>**電腦管理者**Kaspersky Endpoint Security 會為電腦管理者的帳戶建立一個身分驗證代理使用者帳戶。您可以在 Active Directory 的電腦內容中查看哪個帳戶有電腦管理者角色。預設未定義電腦管理者角色，即它不相應任何帳戶。<br>**目前帳戶**Kaspersky Endpoint Security 會為磁碟加密時啟動的帳戶自動建立一個身分驗證代理帳戶。 |
| **首次登入時為此電腦的所有使用者自動建立身分驗證代理帳戶** | 如果選中此核取方塊，則應用程式將在啟動身分驗證代理之前檢查電腦上 Windows 使用者帳戶的資訊。如果 Kaspersky Endpoint Security 偵測到沒有身分驗證代理帳戶的 Windows 使用者帳戶，則應用程式將建立一個新帳戶來存取加密的磁碟機。新的身分驗證代理帳戶將具有以下預設設定：僅受密碼防護的登錄，以及首次身分驗證時變更密碼。因此，對於具有已加密磁碟機的電腦，不需要使用*"管理身分驗證代理帳戶"*工作手動新增身分驗證代理帳戶。 |
| **儲存在身分驗證代理中輸入的使用者名稱** | 如果選中該核取方塊，應用程式將儲存身分驗證代理帳戶的名稱。下次使用同一帳戶在身分驗證代理中嘗試完成憑證時不會被提示輸入帳戶名稱。 |
| **僅加密使用的磁碟空間(減少加密時間)** | 該核取方塊可啟用/停用將加密區域僅限為已用硬碟磁區的選項。該限制可減少加密時間。<br>在啟動加密後啟用或者停用**"僅加密使用的磁碟空間(減少加密時間)"**功能不會修改此設定，直到硬碟磁碟機被解密為止。開始加密之前您必須選擇或清除該核取方塊。<br>如果選定該核取方塊，則僅加密使用的硬碟部分。Kaspersky Endpoint Security 將自動加密新增的新資料。<br>如果清空該核取方塊，整個硬碟將被加密，包括先前刪除和修改檔案殘留的碎片。<br>建議對尚未修改或刪除資料的新硬碟使用該選項。如果對已在使用中的硬碟應用加密，則建議加密整個硬碟。這樣可確保防護所有資料，甚至已刪除的資料也能夠部分還原。<br>預設情況下，會取消勾選核取方塊。 |
| **啟用 Legacy USB Support(不建議)** | 此核取方塊啟用或停用 Legacy USB Support 功能。*Legacy USB Support* **是**一種 BIOS/UEFI 功能，允許您在啟動作業系統（BIOS 模式）之前，在電腦的引導階段使用 USB 裝置（例如安全性權杖）。Legacy USB Support不會影響作業系統啟動後對 USB 裝置的支援。<br>如果選中該核取方塊，在電腦初始啟動期間對 USB 裝置的支援將啟用。<br>啟用Legacy USB Support功能時，BIOS 模式下的身分驗證代理不支援透過 USB 使用權杖。建議僅當存在硬體相容性問題時並僅對發生問題的電腦使用此選項。 |
| **密碼設定** | 身分驗證代理帳戶密碼強度設定。使用單點登入技術時，身分驗證代理將忽略卡巴斯基安全管理中心中指定的密碼強度要求。您可以在作業系統設定中設定密碼強度要求。 |
| **使用單點登入 (SSO) 技術** | SSO 技術允許使用同一個帳戶憑證存取加密磁碟機並登入作業系統。<br>如果選中此核取方塊，您必須輸入用於存取加密硬碟磁碟機以及隨後自動登入作業系統的帳戶憑證。<br>如果清除該核取方塊，要存取加密硬碟磁碟機並隨後登入作業系統，您必須分別輸入用於存取加密硬碟磁碟機的憑證和作業系統使用者帳戶憑證。 |
| **包裝第三方憑據提供商** | Kaspersky Endpoint Security 支援協力廠商憑據提供者 ADSelfService Plus。<br>當使用協力廠商憑據提供者時，身分驗證代理會在作業系統載入前攔截密碼。這意味著使用者在登入 Windows 時只需要輸入密碼一次。登入 Windows 後，使用者可以在公司服務（例如）中利用協力廠商憑據提供者的功能進行身分驗證。協力廠商憑據提供者還可讓使用者獨立重設自己的密碼。在此情況下，Kaspersky Endpoint Security 將自動更新身分驗證代理的密碼。<br>如果您正在使用不受應用程式支援的協力廠商憑據提供者，您可能會在單點登入技術操作中遇到某些限制。 |
| **說明** | **身分驗證**輸入帳戶憑證時，"身分驗證代理"視窗中顯示的說明文字。<br>**變更密碼**變更身分驗證代理帳戶的密碼時，"身分驗證代理"視窗中顯示的說明文字。<br>**還原密碼**還原身分驗證代理帳戶的密碼時，"身分驗證代理"視窗中顯示的說明文字。 |

| 參數 | 描述 |
| --- | --- |
| **加密模式** | **加密所有硬碟磁碟機**如果選擇此選項，套用政策後，應用程式將加密所有硬碟。<br>如果電腦安裝了多個作業系統，在加密後，您將能夠只載入安裝了應用程式的作業系統。<br>**解密所有硬碟磁碟機**如果選擇此選項，套用政策後，應用程式將解密先前已加密的所有硬碟。<br>**保留不變**如果選定了該選項，套用政策後，應用程式將保留硬碟不動。如果磁碟機已加密，則其仍加密。如果磁碟機已解密，則其仍解密。預設情況下已勾選此項目。 |
| **啟用需要在平板電腦上預啟動鍵盤輸入的 BitLocker 身分驗證** | 在預啟動環境中使用需要資料輸入的身分驗證，即使此平台沒有能力進行預啟動輸入（例如使用平板電腦上的觸控式螢幕鍵盤）。<br>平板電腦的觸控式螢幕在預啟動環境中不可用。例如，要在平板電腦上完成 BitLocker 身分驗證，使用者必須連線 USB 鍵盤。<br>如果選定此核取方塊，則允許使用需要預啟動輸入的身分驗證。我們建議在預啟動環境中僅對擁有備用資料輸入的裝置（例如除了觸控式螢幕鍵盤之外的 USB 鍵盤）使用此設定。<br>如果清除此核取方塊，則無法在平板電腦上使用 BitLocker 磁碟機加密。 |
| **使用硬體加密(Windows 8 和後續版本)** | 如果選定此核取方塊，則應用程式將應用硬體加密。這可以提高加密速度並使用較少的電腦資源。 |
| **僅加密使用的磁碟空間(Windows 8 和後續版本)** | 該核取方塊可啟用/停用將加密區域僅限為已用硬碟磁區的選項。該限制可減少加密時間。<br>在啟動加密後啟用或者停用**"僅加密使用的磁碟空間(減少加密時間)"**功能不會修改此設定，直到硬碟磁碟機被解密為止。開始加密之前您必須選擇或清除該核取方塊。<br>如果選定該核取方塊，則僅加密使用的硬碟部分。Kaspersky Endpoint Security 將自動加密新增的新資料。<br>如果清空該核取方塊，整個硬碟將被加密，包括先前刪除和修改檔案殘留的碎片。<br>建議對尚未修改或刪除資料的新硬碟使用該選項。如果對已在使用中的硬碟應用加密，則建議加密整個硬碟。這樣可確保防護所有資料，甚至已刪除的資料也能夠部分還原。<br>預設情況下，會取消勾選核取方塊。 |

| 參數 | 描述 |
| --- | --- |
| **身分驗證方法** | **僅限密碼（Windows 8 和後續版本）**<br>如果選定此選項，Kaspersky Endpoint Security 將在使用者嘗試存取加密磁碟時提示使用者輸入密碼。<br>沒有使用受信任平台模組 (TPM) 時可以選擇此選項。<br>**受信任平台模組 (TPM)**<br>如果選定此核取方塊，則 BitLocker 使用受信任平台模組 (TPM)。<br>A *Trusted Platform Module* (TPM) 是一個與安全相關並提供基本功能的微晶片（例如用於儲存加密金鑰）。受信任平台模組通常安裝在電腦主機板上並且透過硬體匯流排與其他所有系統元件進行互動。<br>對於執行 Windows 7 或 Windows Server 2008 R2 的電腦，只能使用 TPM 模組進行加密。如果未安裝 TPM 模組，則無法進行 BitLocker 加密。不支援在這些電腦上使用密碼。<br>配有受信任平台模組的裝置可以建立只能使用此裝置解密的加密金鑰。受信任平台模組將使用其自有的根儲存金鑰加密加密金鑰。根儲存金鑰儲存在受信任平台模組中。這提供了防禦駭客攻擊加密金鑰的附加防護。<br>預設情況下已選擇此操作。<br>您可以為存取加密金鑰設定一層額外防護，用密碼或者 PIN 加密金鑰：<br>• **為 TPM 使用 PIN**如果選中此核取方塊，使用者可以使用 PIN 碼存取儲存在受信任平台模組 (TPM) 中的加密金鑰。如果清除此核取方塊，則會禁止使用者使用 PIN 碼。要存取加密金鑰，使用者必須輸入密碼。<br>• **受信任平台模組 (TPM)，或密碼（如果 TMP 不可使用）**如果選定此選項，當受信任平台模組 (TPM) 不可用時，使用者可使用密碼存取加密金鑰。如果清除該核取方塊且 TPM 不可用，則將不會啟動完整磁碟加密。<br>選取的身分驗證方法必須透過指定密碼或 PIN 要求來進行設定：<br>• **最小 PIN 長度(字元數)**<br>• **最小密碼長度(字元數)**<br>• **限制 TPM 的密碼/PIN 代碼有效期（天）**<br>• **使用增強型 PIN (字母和數字)**。*增強 PIN* 允許使用除了數字字元的其它字元：大寫和小寫拉丁字母，特殊字元，和空格。 |
| **自動重新建立還原金鑰（天）** | 自動更新密碼以還原對 BitLocker 防護的磁碟機的存取權限。如果該核取方塊被選中，請指定還原金鑰密碼的有效期。這將有助於防止還原金鑰密碼重新使用。 |

# 檔案級加密

您可以根據副檔名或副檔名群組編制檔案清單，和儲存在本機電腦磁碟上的資料夾清單，並且為特定應用程式建立的檔案建立加密規則。套用政策後，卡巴斯基安全管理中心將加密和解密以下檔案：

- 單獨新增到加密和解密清單中的檔案。
- 儲存在新增到加密和解密清單中的資料夾內的檔案。
- 單獨應用程式建立的檔案。

如果 Kaspersky Endpoint Security 安裝在執行 Windows for Workstations 的電腦上，則該元件可用。如果 Kaspersky Endpoint Security 安裝在執行 Windows for Servers 的電腦上，則該元件不可用。

檔案加密具有以下特殊功能：

- Kaspersky Endpoint Security 僅為作業系統本機使用者設定資料加密/解密標準資料夾內的檔案。Kaspersky Endpoint Security 不會加密/解密標準資料夾內的行動使用者設定檔、強制使用者設定檔、臨時使用者設定檔或重新定位的資料夾。

- Kaspersky Endpoint Security 不會加密其修改可能損害作業系統和安裝的應用程式的檔案。例如，加密排除項清單中包含以下檔案和包含所有內嵌物件內的檔案：

  - %WINDIR%；
  - %PROGRAMFILES% 和 %PROGRAMFILES(X86)%；
  - Windows 登錄檔。

  您無法檢視或編輯這個加密排除清單。儘管加密排除項目清單中的檔案和資料夾可以新增至加密清單，但在檔案加密期間，它們不會被加密。

檔案級加密元件設定

| 參數 | 描述 |
| --- | --- |
| **加密模式** | **保留不變**如果選定該項，Kaspersky Endpoint Security 將不變更檔案和資料夾，不進行加密或解密。<br>**根據規則**如果選擇此項目，則 Kaspersky Endpoint Security 會根據加密規則對檔案和資料夾進行加密，根據解密規則對檔案和資料夾進行解密，並根據應用程式規則來控制應用程式對加密檔案的存取。<br>**全部解密**如果選定該選項，Kaspersky Endpoint Security 將解密所有加密的檔案和資料夾。 |
| **加密** | 該標籤將顯示本機磁碟機上儲存的檔案的加密規則。您可以新增檔案，如下所示：<br>• **預定義資料夾**Kaspersky Endpoint Security 允許您新增以下區域：<br>**文件**作業系統的"*檔案*"資料夾及其子資料夾中的檔案。<br>**我的最愛**作業系統標準的"*我的最愛*"資料夾及其子資料夾中的檔案。<br>**桌面**作業系統的"*桌面*"資料夾及其子資料夾中的檔案。<br>**暫存檔**與電腦上安裝的應用程式的操作有關的暫存檔案。例如，Microsoft Office 應用程式會建立包含文件備份副本的暫存檔案。<br>**Outlook 檔案**與 Outlook 郵件用戶端操作有關的檔案：資料檔案 (PST)、離線資料檔案 (OST)、離線通訊錄檔案 (OAB) 和個人通訊錄檔案 (PAB)。<br>• **自訂資料夾**您還可以輸入資料夾的路徑。新增資料夾路徑時，請遵循以下規則：<br>使用環境變數（例如，`%FOLDER%\UserFolder\`）。您只能在路徑的開頭使用一次環境變數。<br>不要使用相對路徑。<br>不要使用 `*` 和 `?` 字元。<br>不要使用 UNC 路徑。<br>使用 `;` 或 `,` 作為分隔符號。<br>• **根據副檔名選取檔案**您可以從清單中選擇副檔名群組，例如"*壓縮檔案*"副檔名群組。您也可以手動新增檔案副檔名。 |
| **解密** | 該標籤將顯示本機磁碟機上儲存的檔案的解密規則。 |
| **應用程式規則** | 該標籤將顯示包含應用程式加密檔案存取規則的表以及由單個應用程式建立或修改的檔案的加密規則。 |
| **加密檔案** | 建立加密封包時要滿足的密碼強度要求。 |

# 卸除式磁碟機加密

如果 Kaspersky Endpoint Security 安裝在執行 Windows for Workstations 的電腦上，則該元件可用。如果 Kaspersky Endpoint Security 安裝在執行 Windows for Servers 的電腦上，則該元件不可用。

Kaspersky Endpoint Security 支援加密 FAT32 和 NTFS 檔案系統中的檔案。如果將具有不支援的檔案系統的卸除式磁碟機連線到電腦，對該卸除式磁碟機的加密工作將以出錯結束，Kaspersky Endpoint Security 會為該卸除式磁碟機分配唯讀狀態。

要防護卸除式磁碟機上的資料，可以使用以下類型的加密：

- Full Disk Encryption (FDE)。
  加密整個卸除式磁碟機，包括檔案系統。

  無法在公司網路外部存取加密資料。如果電腦未連線到卡巴斯基安全管理中心（例如"訪客"電腦），也無法存取公司網路內部的加密資料。

- File Level Encryption (FLE)。
  僅加密卸除式磁碟機上的檔案。檔案系統保持不變。

  是卸除式磁碟機上的檔案加密使用一種稱為*攜帶模式*的特殊模式，提供存取公司網路外部資料的功能。

在加密期間，Kaspersky Endpoint Security 會建立一個主要金鑰。Kaspersky Endpoint Security 將主要金鑰儲存在以下儲存區中：

- 卡巴斯基安全管理中心。
- 使用者的電腦。
  主要金鑰使用使用者的金鑰加密。
- 卸除式磁碟機。
  主要金鑰使用卡巴斯基安全管理中心的公開金鑰加密。

加密完成後，可在公司網路內存取卸除式磁碟機上的資料，就像資料在未加密的一般卸除式磁碟機一樣。

存取加密資料

連線帶有加密資料的卸除式磁碟機後，Kaspersky Endpoint Security 會執行以下操作：

1. 檢查使用者電腦本機儲存的主要金鑰。
   如果找到主要金鑰，使用者將獲得卸除式磁碟機上的資料存取權限。
   如果找不到之要金鑰，Kaspersky Endpoint Security 會執行以下操作：
   a. 向卡巴斯基安全管理中心傳送請求。
      收到請求後，卡巴斯基安全管理中心將傳送一個包含主要金鑰的回應。
   b. Kaspersky Endpoint Security 將主要金鑰儲存在使用者電腦的本機中，以供以後對加密的卸除式磁碟機進行操作。
2. 解密資料。

卸除式磁碟機加密的特殊功能

卸除式磁碟機加密具有以下特殊功能：

- 已經為指定的受管理電腦群組形成針對卸除式磁碟機加密且帶有預設設定的政策。因此，套用為加密/解密卸除式磁碟機配置的卡巴斯基安全管理中心政策的結果取決於抽取式磁碟機連線到的電腦。
- Kaspersky Endpoint Security 不會加密/解密卸除式磁碟機上儲存的唯讀檔案。
- 支援以下裝置類型的卸除式磁碟機：
  - 透過 USB 介面連接的資料媒體
  - 透過 USB 和 FireWire 介面連接的固定磁碟機
  - 透過 USB 和 FireWire 介面連接的 SSD 磁碟機

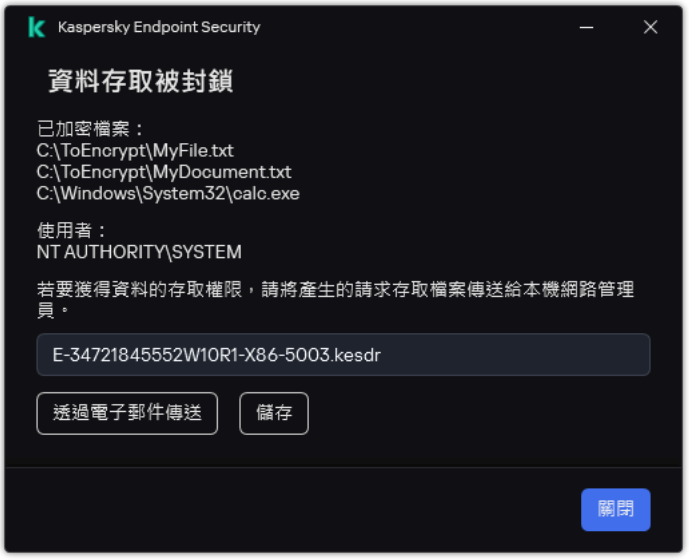
卸除式磁碟機元件設定加密

| 參數 | 描述 |
| --- | --- |
| **加密模式** | **加密整個卸除式磁碟機**如果選定了該項，為卸除式磁碟機套用帶有指定加密設定的政策時，Kaspersky Endpoint Security 將會逐個磁區加密卸除式磁碟機，包括其檔案系統。<br>**加密所有檔案**如果選定了該選項，為卸除式磁碟機套用帶有指定加密設定的政策時，Kaspersky Endpoint Security 將會加密卸除式磁碟機上儲存的所有檔案。Kaspersky Endpoint Security 不會再次加密已經加密的檔案。卸除式磁碟機的檔案系統內容，包括加密檔案的資料夾結構和名稱在內都不會被加密，仍可以被存取。<br>**僅加密新檔案**如果選定了該選項，為卸除式磁碟機套用帶有指定加密設定的政策時，Kaspersky Endpoint Security 將只會加密在上次應用卡巴斯基安全管理中心政策之後在卸除式磁碟機上新增或修改的檔案。當某個卸除式磁碟機由兩個人使用或在工作中使用時，該加密模式很有用。該加密模式可以使您保留所有舊的未變更過的檔案，加密那些使用者在已安裝 Kaspersky Endpoint Security 並啟用加密功能的工作電腦建立的檔案。結果是個人檔案是否可以被存取，與啟用了加密功能的電腦上是否安裝了 Kaspersky Endpoint Security 無關。<br>**解密整個卸除式磁碟機**如果選定了該選項，為卸除式磁碟機套用帶有指定加密設定的政策時，Kaspersky Endpoint Security 將會解密卸除式磁碟機上儲存的先前加密的所有檔案和檔案系統。<br>**保留不變**如果選定了該選項，套用政策後，應用程式將保留硬碟不動。如果磁碟機已加密，則其仍加密。如果磁碟機已解密，則其仍解密。預設情況下已勾選此項目。 |
| **攜帶模式** | 該核取方塊可啟用/停用準備卸除式磁碟機，以便能夠在公司網路外部的電腦上存取卸除式磁碟機中儲存的檔案。<br>如果選定該核取方塊，Kaspersky Endpoint Security 將提示使用者在根據政策加密卸除式磁碟機之前指定一個密碼。在公司網路外部的電腦上存取卸除式磁碟機中的加密檔案時需要該密碼。您可以設定密碼強度。<br>攜帶模式可用於"**加密所有檔案**"或"**僅加密新檔案**"模式。 |
| **僅加密使用的磁碟空間** | 該核取方塊將啟用/停用加密模式，其中僅加密已使用磁碟磁區。建議為尚未修改或刪除資料的新裝置使用該模式。<br>如果選定該核取方塊，則僅加密使用的磁碟部分。Kaspersky Endpoint Security 將自動加密新增的新資料。<br>如果清空該核取方塊，整個磁碟機將被加密，包括先前刪除和修改檔案殘留的碎片。<br>僅加密已占用空間的功能僅在"**加密整個卸除式磁碟機**"模式下可用。<br>開始加密後，啟用/停用"**僅加密使用的磁碟空間**"功能不會變更該設定。開始加密之前您必須選擇或清除該核取方塊。 |
| **自訂規則** | 該表包含了已其定義自訂加密規則的裝置。您可以透過以下方式為單一卸除式磁碟機建立加密規則：<br>• 從"裝置控制"的受信任裝置清單中新增卸除式磁碟機。<br>• 手動新增卸除式磁碟機：<br>  • 按裝置 ID（Hardware ID 或 HWID）<br>  • 按裝置型號：Vendor ID （ VID ）和 Product ID （ PID ） |

| 參數 | 描述 |
| --- | --- |
| **允許在離線模式下加密卸除式磁碟機** | 如果選中該核取方塊，則即使沒有連線至卡巴斯基安全管理中心，Kaspersky Endpoint Security 也會加密卸除式磁碟機。在這種情況下，解密卸除式磁碟機所需的資料儲存在與卸除式磁碟機連線的電腦的硬碟上，不會傳輸到卡巴斯基安全管理中心。<br>如果清除該核取方塊，則 Kaspersky Endpoint Security 無法在未連線至卡巴斯基安全管理中心的情況下加密卸除式磁碟機。 |
| **加密密碼設定/攜帶式檔案管理器** | 攜帶式檔案管理器的密碼強度設定。 |

# 模組（資料加密）

進行資料加密後，Kaspersky Endpoint Security 可能會限制對資料的存取，例如，由於組織基礎結構發生變化和卡巴斯基安全管理中心管理伺服器發生變化。如果使用者無權存取加密資料，使用者可以請管理員提供資料存取權限。換句話說，使用者需要將請求存取檔案傳送給管理員。然後，使用者需要將從管理員處收到的回應檔案上傳到 Kaspersky Endpoint Security。Kaspersky Endpoint Security 允許您透過電子郵件向管理員請求資料存取權限（請參見下圖）。




請求加密資料的存取權限

系統提供了一個模組，用於報告缺少對加密資料的存取權限。為方便使用者，您可以填寫以下欄位：

- **收件者**輸入擁有資料加密功能權限的管理員群組的電子郵件地址。
- **主旨**輸入包含加密檔案存取請求的電子郵件主旨。例如，您可以新增標籤以篩選郵件。
- **使用者訊息**如有必要，可變更郵件的內容。您可以使用變數來獲取必要資料（例如，`%USER_NAME%` 變數）。

# 排除

*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。管理員還可以允許使用者為特定電腦建立自己的本機受信任區域。這樣，除了政策中的一般受信任區域之外，使用者還可以建立自己的"排除項目"和"受信任應用程式"的本機清單。

從 Kaspersky Endpoint Security 12.5 for Windows 開始，您可以 將 EDR 遙測資料新增至受信任區域。這可讓您最佳化應用程式傳送到 Kaspersky Anti Targeted Attack Platform (EDR) 解決方案的遙測資料收集伺服器的資料。

從 Kaspersky Endpoint Security 12.6 for Windows 開始，掃描排除項目和受信任應用程式被新增到受信任區域。預先定義的掃描排除項目和受信任應用程式有助於在 SQL 伺服器、Microsoft Exchange 伺服器和 System Center Configuration Manager 上快速設定 Kaspersky Endpoint Security。這意味著您無需在伺服器上為應用程式手動設定受信任區域。

從 Kaspersky Endpoint Security 12.8 for Windows 開始，您可以在 Light Agent 模式下安裝應用程式以防護虛擬環境。預定義掃描排除項目和受信任的應用程式可以幫助您在Citrix 和 VMware虛擬環境中快速設定 Kaspersky Endpoint Security。

## 掃描排除項目

"*掃描排除項目*"是一組條件，必須滿足這些條件，Kaspersky Endpoint Security 才不會掃描特定物件是否存在病毒和其他威脅。掃描排除項目可確保安全使用可能被入侵者用於損害電腦或使用者資料的合法軟體。儘管這類應用程式並不具備任何惡意功能，它們可能被入侵者利用。有關可被入侵者用來破壞電腦或個人資料的合法軟體的詳細資訊，請造訪 Kaspersky IT 百科全書網站。

這類應用程式可以被 Kaspersky Endpoint Security 封鎖。若要防止它們被封鎖，您可以為正在使用的應用程式排除掃描排除項目。為此，請將 Kaspersky IT 百科全書中列出的名稱或名稱遮罩新增到受信任區域。例如，您經常使用 Radmin 應用程式來遠端管理電腦。Kaspersky Endpoint Security 會將這些活動看做潛在危險並進行封鎖。若要防止應用程式被封鎖，請使用 Kaspersky IT 百科全書中列出的名稱或名稱遮罩建立掃描排除項目。

如果您電腦上安裝的某個應用程式收集資訊並將其傳送以供處理，則 Kaspersky Endpoint Security 可能會將其歸類為惡意軟體。若要避免此資訊，您可以按照文件所述透過配置 Kaspersky Endpoint Security 從掃描中排除此應用程式。

掃描排除項目可用於下列特定應用程式元件和系統管理員配置的工作：

- 行為偵測
- 弱點利用防禦
- 主機入侵防禦
- 檔案威脅防護
- Web 威脅防護
- 郵件威脅防護
- *惡意軟體掃描*工作

## 受信任應用程式清單

*受信任應用程式清單*包含應用程式的檔案和網路活動（包括可疑活動）以及對系統登錄檔的存取不受 Kaspersky Endpoint Security 的監控。預設情況下，Kaspersky Endpoint Security 將監控任何應用程式處理程序開啟、執行或儲存的物件，並控制所有應用程式的活動及其產生的網路流量。應用程式被新增到受信任應用程式清單後，Kaspersky Endpoint Security 將停止監控該應用程式的活動。

掃描排除項目和受信任的應用程式之間的區別在於，對於排除項目，Kaspersky Endpoint Security 不掃描檔案，而對於受信任的應用程式，它不控制啟動的處理程序。如果受信任的應用程式在未包含在掃描排除項目中的資料夾中建立惡意檔案，Kaspersky Endpoint Security 將偵測該檔案並消除威脅。如果資料夾被新增到排除項目，Kaspersky Endpoint Security 將略過該檔案。

例如，如果您認為由標準 Microsoft Windows 記事本應用程式使用的物件是安全的，也即您信任此應用程式，則您可將 Microsoft Windows 記事本新增到受信任應用程式清單中，這樣該應用程式使用的物件就不會被監控。這會提高電腦效能，在使用伺服器應用程式時尤為重要。

此外，Kaspersky Endpoint Security 分類為危險的特定操作，在很多應用程式的功能環境中可能是安全的。例如，攔截鍵盤輸入的內容，是自動鍵盤設定切換器中的一種例行程式（例如 Punto Switcher）。考慮到此類程式的特點並將其行為從監控中排除，我們建議您可將此類程式新增到信任應用程式清單中。

受信任的應用程式有助於避免 Kaspersky Endpoint Security 與其他應用程式之間的相容性問題（例如，Kaspersky Endpoint Security 和另一個病毒防護應用程式對第三方電腦的網路流量進行雙重掃描的問題）。

同時，信任應用程式的可執行檔和處理程序仍然會掃描病毒和其他惡意軟體。您可以透過掃描排除項目將應用程式從 Kaspersky Endpoint Security 掃描中完全排除。

排除項目設定

| 參數 | 描述 |
| --- | --- |

**偵測到的物件類型**

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。

- **病毒和蠕蟲**

  **子分類**：病毒和蠕蟲 (Viruses_and_Worms)

  **危險等級**：高

  典型的病毒和蠕蟲會執行未經使用者授權的操作。它們會建立可自我複製的副本。

  **經典病毒**

  典型病毒侵入電腦後，會感染檔案，啟動並執行惡意操作，以及將自身的副本新增到其他檔案中。

  典型病毒僅在電腦本機資源上複製副本，不會自行侵入其他電腦。僅當此病毒將其副本新增至儲存在共用資料夾或放入電腦中的 CD 中的檔案時，或者在使用者傳送附有受感染檔案的電子郵件訊息時，此病毒才會傳染給其他電腦。

  典型病毒代碼可以入侵電腦、作業系統和應用程式的各種區域。根據其體的環境，病毒可分為*檔案病毒*、*引導磁區病毒*、*指令碼病毒*和*巨集病毒*。

  病毒可以使用多種不同的技術來感染檔案。*Overwriting*病毒會使用其代碼覆蓋受感染檔案的代碼，從而抹除檔案的內容。感染的檔案會停止發揮作用，且無法還原。*Parasitic*病毒會修改檔案，從而使自身發揮全部或部分功能。*Companion*不會修改檔案，而是建立副本。當您開啟受感染的檔案時會啟動此檔案的副本（實際上是病毒）。您也會遇到以下類型的病毒：*Link病毒*、*OBJ 病毒*、*LIB 病毒*、*原始程式碼病毒*和許多其他病毒。

  **蠕蟲**

  與典型病毒一樣，蠕蟲在侵入電腦後，其代碼將啟動並執行惡意操作。之所以稱為蠕蟲，是因為它們能夠從一台電腦"爬"到另一台電腦，並不需使用者權限即可透過許多資料通道來傳播副本。

  可用於區分各種類型蠕蟲的主要特徵是蠕蟲的傳播方式。下表提供了各種類型蠕蟲的概覽，這些蠕蟲按其傳播方式進行了分類。

  蠕蟲傳播方式

  | 類型 | 名稱 | 描述 |
  |---|---|---|
  | **電子郵件蠕蟲** | 電子郵件蠕蟲 | 這些蠕蟲透過電子郵件傳播。<br>受感染的電子郵件訊息包含帶有蠕蟲副本的附件，或指向上傳到可能已被攻擊或者專門建立用於傳播蠕蟲的網站上某檔案的連結。開啟此附件時，蠕蟲將被啟動。在您點擊此連結，進行下載，然後開啟檔案時，蠕蟲還會開始執行其惡意操作。之後，蠕蟲會繼續傳播其副本，搜尋其他電子郵件信箱，並向它們傳送受感染的郵件。 |
  | **IM 蠕蟲** | 即時通訊用戶端蠕蟲 | 它們透過 IM 傳播。<br>通常，此類蠕蟲會利用使用者的連絡人清單傳送訊息，其中包含指向某網站上帶有蠕蟲副本的檔案的連結。使用者下載並開啟檔案時，蠕蟲將被啟動。 |
  | **IRC 蠕蟲** | 網際網路聊天蠕蟲 | 這些蠕蟲會透過Internet Relay Chats（允許透過網際網路與其他人即時通信的服務系統）傳播。<br>這些蠕蟲會在網際網路聊天中發佈包含自身副本的檔案或指向此檔案的連結。使用者下載並開啟檔案時，蠕蟲將被啟動。 |
  | **網路蠕蟲** | 網路蠕蟲 | 這些蠕蟲透過電腦網路傳播。<br>與其他類型的蠕蟲不同，典型的網路蠕蟲不需使用者參與即可傳播。它會掃描區域網路來尋找安裝了有弱點的程式的電腦。為此，它會傳送特殊格式的網路封包（弱點），其中包含蠕蟲代碼或部分蠕蟲代碼。如果網路上存在"有弱點"的電腦，此電腦會接收到此種網路封包。蠕蟲完全入侵電腦後，將被啟動。 |
  | **P2P 蠕蟲** | 檔案共用網路蠕蟲 | 它們透過點對點檔案共用網路傳播。<br>為了滲透到 P2P 網路，蠕蟲會將自身複製到通常位於使用者電腦上的檔案共用資料夾中。P2P 網路會顯示有關此檔案的資訊，以便使用者可以在網路中像任何其他檔案一樣"找到"受感染的檔案，然後下載並開啟此檔案。<br>更加狡猾的蠕蟲會模仿特定 P2P 網路的網路協定：它們會返回對搜尋程式的積極回應，並提供自身的副本供下載。 |
  | **蠕蟲** | 其他類型的蠕蟲 | 其他類型的蠕蟲包括：<br>• 透過網路資源傳播自身副本的蠕蟲。透過使用作業系統的功能，它們掃描可用的網路資料夾，連線到網際網路上的電腦，並嘗試獲取對磁碟機的完全存取。與之前描述的蠕蟲類型不同，其他類型的蠕蟲不會自行啟動，而是在使用者開啟包含蠕蟲副本的檔案時啟動。<br>• 不使用上表中所述的任何方式進行傳播的蠕蟲（例如，透過手機傳播的蠕蟲）。 |

- **木馬（包含勒索軟體）**

  **子類別**：木馬程式

  **危險等級**：高

  與蠕蟲和病毒不同，木馬不能進行自我複製。例如，使用者存取受感染的網頁時，它們會透過電子郵件或瀏覽器侵入電腦。木馬透過使用者參與而啟動。木馬啟動後即會開始執行惡意操作。

  在受感染的電腦上，不同的木馬會表現出不同的行為。木馬的主要功能包括封鎖、修改或破壞資訊，以及停用電腦或網路。木馬還可以接收或傳送檔案，在螢幕上顯示訊息，請求網頁，下載和安裝程式，以及重新啟動電腦。

  駭客通常使用各種不同木馬的"集合"。

  下表中介紹了木馬行為的類型。

  受感染電腦上木馬行為的類型

| 類型 | 名稱 | 描述 |
| --- | --- | --- |
| **木馬炸彈** | 木馬 –"壓縮檔案炸彈" | 解壓縮時，這些壓縮檔案的大小會急劇增加，從而影響電腦的操作。<br>使用者嘗試解壓縮這種壓縮檔案時，電腦可能會執行緩慢或停止執行；硬碟可能會充滿"空白"資料。"壓縮檔案炸彈"對於檔案和郵件伺服器尤為危險。如果伺服器使用自動系統處理接收資訊，則"壓縮檔案炸彈"可能會中斷伺服器執行。 |
| **後門** | 用於遠端管理的木馬 | 此種木馬被視為最危險的木馬類型。在功能方面，這些木馬與安裝在電腦上的遠端管理應用程式相似。<br>這些程式會在不被使用者發覺的情況下將自身安裝到電腦上，以便入侵者遠端管理電腦。 |
| **木馬** | 木馬 | 木馬包括以下惡意應用程式：<br>• **典型木馬**。這些程式僅執行木馬的主要功能：封鎖、修改或破壞資訊，以及停用電腦或網路。它們沒有任何進階功能，與表中描述的其他類型的木馬不同。<br>• **萬能木馬**。這些程式具有多種典型木馬類型的進階功能。 |
| **勒索木馬** | 勒索木馬 | 這些木馬將使用者資訊作為"人質"，修改或封鎖資訊，或者影響電腦的操作，以使使用者無法使用資訊。入侵者向使用者進行勒索，許諾傳送應用程式來還原電腦的效能以及電腦上儲存的資料。 |
| **木馬點擊器** | 木馬點擊器 | 這些木馬透過自行向瀏覽器傳送指令或變更在作業系統檔案中指定的網址的方式，從使用者的電腦存取網頁。<br>透過使用這些程式，入侵者進行網路攻擊並提高網站存取量，從而增加條幅廣告的顯示次數。 |
| **木馬下載器** | 木馬下載器 | 這些木馬會存取入侵者的網頁，從中下載其他惡意應用程式，並將它們安裝到使用者的電腦。這些木馬包含要下載的惡意應用程式的檔案名稱，或從存取的網頁中接收此檔案名稱。 |
| **木馬釋放器** | 木馬釋放器 | 這些木馬包含安裝在硬碟磁碟機上並隨後進行安裝的其他木馬。<br>入侵者可能會使用木馬釋放器類型的程式來達到以下目的：<br>• 未通知使用者就安裝惡意應用程式：木馬釋放器類型的程式不會顯示訊息，或者會顯示虛假訊息，例如通知壓縮檔案中存在錯誤或作業系統的版本不相容。<br>• 防護另一個已知惡意應用程式不被偵測：並非所有病毒防護軟體都可偵測到木馬釋放器類型應用程式中的惡意應用程式。 |
| **通知型木馬** | 通知型木馬 | 這些木馬會通知入侵者受感染的電腦可供存取，並向入侵者傳送有關電腦的資訊：IP 位址、已開放埠號或電子郵件信箱。它們透過電子郵件、FTP、存取入侵者的網頁或以其他方式與入侵者聯絡。<br>通知型木馬類型的程式通常用於包含多種木馬的集合中。這些木馬會通知入侵者其他木馬已成功安裝到使用者的電腦。 |
| **代理型木馬** | 代理型木馬 | 這些木馬允許入侵者使用使用者的電腦匿名存取網頁，它們通常用於傳送垃圾郵件。 |
| **木馬 PSW** | 密碼竊盜軟體 | 密碼竊盜軟體是竊盜使用者帳戶（如軟體註冊資料）的一種木馬。這些密碼會尋找系統檔案和登錄檔中包含的機密資料，並透過電子郵件、FTP、存取入侵者的網頁或以其他方式將機密資料傳送給"攻擊者"。<br>部分這些木馬分類為此表中敘述的單獨類型。這些木馬會盜竊銀行帳戶（網銀竊賊木馬），竊取 IM 用戶端使用者的資料（IM 木馬），以及盜竊線上遊戲使用者的資訊（遊戲竊賊木馬）。 |
| **間諜木馬** | 間諜木馬 | 這些木馬暗中監視使用者，收集有關使用者使用電腦時所做的操作的資訊。它們可能會攔截使用者透過鍵盤輸入的資料，截取螢幕，或收集活動應用程式的清單。收到資訊後，這些木馬會透過電子郵件、FTP、存取入侵者的網頁或以其他方式將資訊傳輸給入侵者。 |
| **分散式拒絕服務攻擊木馬** | 木馬網路攻擊者 | 這些木馬會從使用者電腦將大量請求傳送至遠端伺服器。伺服器缺少資源來處理所有請求，因此會停止執行（拒絕服務，或簡稱為 DoS）。駭客通常會使用這些程式感染許多電腦，以使用這些電腦來同時攻擊一個伺服器。<br>DoS 程式在使用者知悉的情況下從一台電腦發起攻擊。DDoS（分散式 DoS）程式在不被受感染電腦使用者發覺的情況下從多台電腦發起分散式攻擊。 |
| **木馬 IM** | 從 IM 用戶端使用者那裡竊取資訊的木馬 | 它們會竊取 IM 用戶端使用者的帳戶和密碼。這些木馬會透過電子郵件、FTP、存取入侵者的網頁或以其他方式將資料傳輸給入侵者。 |
| **Rootkit** | Rootkits | 這些木馬會掩蓋其他惡意應用程式及其活動，從而延長這些應用程式在作業系統中持續存在的時間。它們還會隱藏檔案、受感染電腦記憶體中的處理程序或執行惡意應用程式的登錄機碼。Rootkit 會掩蓋使用者電腦上的應用程式與網路上其他電腦之間進行的資料交換。 |
| **木馬 SMS** | SMS 格式的木馬 | 這些木馬會感染手機，向額外收費的手機號碼傳送 SMS。 |
| **遊戲竊賊木馬** | 從線上遊戲使用者那裡竊取資訊的木馬 | 這些木馬會竊取線上遊戲使用者的帳戶憑證，然後將這些憑證透過電子郵件、FTP、存取駭客的網頁或以其他方式傳送給駭客。 |
| **網銀竊賊木馬** | 竊取銀行帳戶的木馬 | 這些木馬會竊取銀行帳戶資料或電子貨幣系統資料，然後將這些資料透過電子郵件、FTP、存取駭客的網頁或以其他方式傳送給駭客。 |
| **郵件偵測木馬** | 收集電子郵件信箱的木馬 | 這些木馬會收集儲存在電腦上的電子郵件信箱，然後透過電子郵件、FTP、存取入侵者的網頁或以其他方式將它們傳送給入侵者。入侵者可能會向收集到的位址傳送垃圾郵件。 |

- **惡意工具**

  **子類別**：惡意工具

  **危險等級**：中

  與其他類型的惡意軟體不同，惡意工具在啟動過後不會執行其操作。惡意工具可以在使用者的電腦上安全地儲存和啟動。入侵者通常使用這些程式的功能來建立病毒、蠕蟲和木馬，對遠端伺服器進行網路入侵，攻擊電腦或執行其他惡意操作。

  惡意工具的各種功能按下表中所述的類型進行分組。

  惡意工具的功能

| 類型 | 名稱 | 描述 |
| --- | --- | --- |
| **構建器** | 構建器 | 透過它們可以建立新的病毒、蠕蟲和木馬。一些構建器揚言構建了基於視窗的標準介面，使用者可在此介面中選擇要建立的惡意應用程式的類型，對付偵錯工具的方式，以及其他功能。 |
| **拒絕服務攻擊** | 網路攻擊 | 這些木馬會從使用者電腦將大量請求傳送至遠端伺服器。伺服器缺少資源來處理所有請求，因此會停止執行（拒絕服務，或簡稱為 DoS）。 |
| **弱點利用** | 弱點 | *弱點*是一組資料或程式碼，利用處理它們的應用程式的缺陷對電腦執行惡意操作。例如，弱點可以寫入或讀取檔案，或請求"受感染"的網頁。<br>不同的弱點會利用不同應用程式或網路服務的缺陷。弱點會偽裝成網路封包透過網路傳輸到許多電腦，然後搜尋網路服務存在缺陷的電腦。DOC 檔案中的弱點會利用文字編輯器的缺陷。在使用者開啟受感染的檔案時，它可能會開始執行駭客程式設計的操作。嵌入在電子郵件訊息中的弱點會搜尋電子郵件用戶端的缺陷。使用者在電子郵件用戶端中開啟受感染的郵件時，弱點會立即開始執行惡意操作。<br>網路蠕蟲會使用弱點透過網路進行傳播。Nuker 弱點是可停用電腦的網路封包。 |

| | | |
|---|---|---|
| **檔案加密器** | 加密器 | 加密器會加密其他惡意應用程式，以隱藏它們不被防毒應用程式發現。 |
| **洪水攻擊器** | 用於"污染"網路的程式 | 這些程式會透過網路通道傳送大量郵件。例如，此類型的工具包括污染網際網路中繼聊天的程式。<br>洪水攻擊器工具不包括"污染"電子郵件、IM 用戶端以及行動通信系統所使用通道的程式。這些程式可分為表中介紹的各種類型（電子郵件洪水攻擊器、IM 洪水攻擊器和 SMS 洪水攻擊器）。 |
| **駭客工具** | 駭客工具 | 這些工具可以破壞其所在的電腦，或攻擊其他電腦（例如，未經使用者許可新增新系統帳戶，或清除系統日誌以隱藏在作業系統中的存在路徑）。這種類型的工具包括一些具有惡意功能的嗅探器，例如密碼截取。嗅探器是允許檢視網路流量的程式。 |
| **惡作劇程式** | 惡作劇程式 | 這些程式會警告使用者類似病毒的訊息：它們可能會在未受感染的檔案中"偵測到病毒"，或通知使用者磁碟已被格式化，儘管這些情況實際並未發生。 |
| **位址欺騙程式** | 位址欺騙工具 | 這些工具使用偽造的寄件者位址傳送郵件和網路請求。例如，入侵者會使用位址欺騙程式類型的工具來掩蓋他們作為郵件實際寄件者的事實。 |
| **病毒修改工具** | 修改惡意應用程式的工具 | 透過這些工具可以修改其他惡意軟體，隱藏它們不被防毒程式發現。 |
| **電子郵件洪水攻擊器** | "污染"電子郵件信箱的程式 | 這些程式會向各種電子郵件信箱傳送大量郵件，從而"污染"這些位址。大量的接收郵件會妨礙使用者檢視收件箱中的有用郵件。 |
| **IM 洪水攻擊器** | "污染"IM 流量的程式 | 它們向 IM 的使用者傳送大量訊息。大量的資訊會妨礙使用者檢視有用的接收資訊。 |
| **SMS 洪水攻擊器** | 使用 SMS"污染"流量的程式 | 這些程式向手機傳送大量 SMS。 |

- **廣告軟體**

  **子類別**：廣告軟體

  **危險等級**：中

  廣告軟體向使用者顯示廣告資訊。廣告軟體程式會在其他程式的介面中顯示條幅廣告，並將搜尋查詢重新導向至廣告網頁。某些廣告軟體程式會收集有關使用者的行銷資訊，並將其傳送給開發者：此資訊可能包括使用者存取的網站的名稱，或使用者搜尋查詢的內容。與間諜木馬類型的程式不同，廣告軟體程式會在使用者許可的情況下將此資訊傳送給開發者。

- **自動撥號程式**

  **子類別**：可被入侵者利用以破壞您的電腦或個人資料的合法軟體。

  **危險等級**：中

  大多數這些應用程式都很有用，因此有許多使用者使用它們。這些應用程式包括 IRC 用戶端、自動撥號器、檔案下載程式、電腦系統活動監控器、密碼實用程式以及用於 FTP、HTTP 和 Telnet 的網際網路伺服器。

  但是，如果入侵者獲得了這些程式的存取權限，或如果他們在使用者的電腦上安置這些程式，應用程式的某些功能可能會被用來危害安全。

  這些應用程式具有不同的功能，下表介紹了它們的類型。

| 類型 | 名稱 | 描述 |
|---|---|---|
| **Client-IRC** | 網際網路聊天用戶端 | 使用者安裝這些程式與他人進行網際網路中繼聊天。入侵者使用這些程式來傳播惡意軟體。 |
| **Downloader** | 用於下載的程式 | 這些程式可以在隱藏模式下從網頁下載檔案。 |
| **Monitor** | 用於監控的程式 | 這些程式可監控其安裝到的電腦上的活動（檢視哪些應用程式正在活動，以及它們如何與安裝在其他電腦上的應用程式交換資料）。 |
| **PSWTool** | 密碼還原器 | 透過它們可以檢視和還原已忘記的密碼。入侵者出於相同的目的，秘密地將它們安置在使用者的電腦上。 |
| **RemoteAdmin** | 遠端管理程式 | 系統管理員廣泛使用的一些程式。透過這些程式可以獲取對遠端電腦介面的存取權限，以監控和管理此電腦。入侵者出於同樣的目的，秘密地將它們安置在使用者的電腦上：用於監控和管理遠端電腦。<br>合法的遠端管理程式與實現遠端管理的後門類型的木馬不同。木馬能夠獨自入侵作業系統並自行安裝；合法的程式則無法做到這些。 |
| **Server-FTP** | FTP 伺服器 | 這些程式可起到 FTP 伺服器的作用。入侵者將它們安置在使用者電腦上，以開啟透過 FTP 對此電腦的遠端存取。 |
| **Server-Proxy** | 代理伺服器 | 這些程式可起到代理伺服器的作用。入侵者將它們安置在使用者電腦上，以使用者名義傳送垃圾郵件。 |
| **Server-Telnet** | Telnet 伺服器 | 這些程式可起到 Telnet 伺服器的作用。入侵者將它們安置在使用者電腦上，以開啟透過 Telnet 對此電腦的遠端存取。 |
| **Server-Web** | Web 伺服器 | 這些程式可起到 Web 伺服器的作用。入侵者將它們安置在使用者電腦上，以開啟透過 HTTP 對此電腦的遠端存取。 |
| **RiskTool** | 在本機電腦上工作的工具 | 在使用者自己的電腦上工作時，這些工具會為使用者提供其他選項。透過這些工具，使用者可以隱藏檔案或活動應用程式的視窗，並終止活動的處理程序。 |
| **NetTool** | 網路工具 | 與網路上的其他電腦配合工作時，這些工具會為使用者提供其他選項。透過這些工具可以進行重新啟動，偵測開放的連接埠，以及啟動安裝在電腦上的應用程式。 |
| **Client-P2P** | P2P 網路用戶端 | 透過它們可以在對等網路中工作。入侵者可能會利用它們傳播惡意軟體。 |
| **Client-SMTP** | SMTP 用戶端 | 它們未經使用者的同意便傳送電子郵件。入侵者將它們安置在使用者電腦上，以使用者名義傳送垃圾郵件。 |
| **WebToolbar** | Web 工具列 | 它們會向其他應用程式的介面中新增工具列，以使用搜尋引擎。 |
| **FraudTool** | 欺騙程式 | 這些程式將自己偽裝為其他程式。例如，一些欺騙防毒程式會顯示有關惡意軟體偵測的資訊。但實際上，它們並未找到任何內容或進行解毒。 |

- **可被入侵者利用以破壞您的電腦或個人資料的合法軟體**

**子類別**：可被入侵者利用以破壞您的電腦或個人資料的合法軟體。

**危險等級**：中

大多數這些應用程式都很有用，因此有許多使用者使用它們。這些應用程式包括 IRC 用戶端、自動撥號器、檔案下載程式、電腦系統活動監控器、密碼實用程式以及用於 FTP、HTTP 和 Telnet 的網際網路伺服器。

但是，如果入侵者獲得了這些程式的存取權限，或如果他們在使用者的電腦上安置這些程式，應用程式的某些功能可能會被用來危害安全。

這些應用程式具有不同的功能，下表介紹了它們的類型。

| 類型 | 名稱 | 描述 |
| --- | --- | --- |
| Client-IRC | 網際網路聊天用戶端 | 使用者安裝這些程式與他人進行網際網路中繼聊天。入侵者使用這些程式來傳播惡意軟體。 |
| Downloader | 用於下載的程式 | 這些程式可以在隱藏模式下從網頁下載檔案。 |
| Monitor | 用於監控的程式 | 這些程式可監控其安裝到的電腦上的活動（檢視哪些應用程式正在活動，以及它們如何與安裝在其他電腦上的應用程式交換資料）。 |
| PSWTool | 密碼還原器 | 透過它們可以檢視和還原已忘記的密碼。入侵者出於相同的目的，秘密地將它們安置在使用者的電腦上。 |
| RemoteAdmin | 遠端管理程式 | 系統管理員廣泛使用的一些程式。透過這些程式可以獲取對遠端電腦介面的存取權限，以監控和管理此電腦。入侵者出於同樣的目的，秘密地將它們安置在使用者的電腦上：用於監控和管理遠端電腦。<br>合法的遠端管理程式與實現遠端管理的後門類型的木馬不同。木馬能夠獨自入侵作業系統並自行安裝；合法的程式則無法做到這些。 |
| Server-FTP | FTP 伺服器 | 這些程式可起到 FTP 伺服器的作用。入侵者將它們安置在使用者電腦上，以開啟透過 FTP 對此電腦的遠端存取。 |
| Server-Proxy | 代理伺服器 | 這些程式可起到代理伺服器的作用。入侵者將它們安置在使用者電腦上，以使用者名義傳送垃圾郵件。 |
| Server-Telnet | Telnet 伺服器 | 這些程式可起到 Telnet 伺服器的作用。入侵者將它們安置在使用者電腦上，以開啟透過 Telnet 對此電腦的遠端存取。 |
| Server-Web | Web 伺服器 | 這些程式可起到 Web 伺服器的作用。入侵者將它們安置在使用者電腦上，以開啟透過 HTTP 對此電腦的遠端存取。 |
| RiskTool | 在本機電腦上工作的工具 | 在使用者自己的電腦上工作時，這些工具會為使用者提供其他選項。透過這些工具，使用者可以隱藏檔案或活動應用程式的視窗，並終止活動的處理程序。 |
| NetTool | 網路工具 | 與網路上的其他電腦配合工作時，這些工具會為使用者提供其他選項。透過這些工具可以進行重新啟動，偵測開放的連接埠，以及啟動安裝在電腦上的應用程式。 |
| Client-P2P | P2P 網路用戶端 | 透過它們可以在對等網路中工作。入侵者可能會利用它們傳播惡意軟體。 |
| Client-SMTP | SMTP 用戶端 | 它們未經使用者的同意便傳送電子郵件。入侵者將它們安置在使用者電腦上，以使用者名義傳送垃圾郵件。 |
| WebToolbar | Web 工具列 | 它們會向其他應用程式的介面中新增工具列，以使用搜尋引擎。 |
| FraudTool | 欺騙程式 | 這些程式將自己偽裝為其他程式。例如，一些欺騙防毒程式會顯示有關惡意軟體偵測的資訊。但實際上，它們並未找到任何內容或進行解毒。 |

- **可能被用來防護惡意程式碼的封裝物件**

  **子類別**：可能造成損害的封裝檔案。

  **危險等級**：中。

  檔案使用特殊的封裝程式進行封裝，該封裝程式用於封裝惡意軟體：病毒、蠕蟲、木馬。Kaspersky Endpoint Security 會掃描 SFX（自解壓）存檔中的解壓縮工具模組。

  為了隱藏惡意軟體不被防毒軟體偵測到，駭客會使用特殊的封裝程式對其進行封裝。卡巴斯基專家已識別出駭客最常使用的解壓縮工具。

- **多重封裝物件**

  **子類別**：可能造成損害的封裝檔案。

  **危險等級**：中。

  檔案使用特殊的封裝程式進行封裝，該封裝程式用於封裝惡意軟體：病毒、蠕蟲、木馬。Kaspersky Endpoint Security 會掃描 SFX（自解壓）存檔中的解壓縮工具模組。

  為了隱藏惡意軟體不被防毒軟體偵測到，駭客會使用特殊的封裝程式對其進行封裝。卡巴斯基專家已識別出駭客最常使用的解壓縮工具。

**排除項目**

此表包含掃描排除項目的相關資訊。

我們建議指定相對路徑，而非絕對路徑。這不僅允許排除檔案系統物件，還允許排除無檔案物件。例如，`*\Program Files (x86)\Folder\Subfolder`。

| | |
|---|---|
| | 可以使用以下方法從掃描中排除物件：<br>• 指定檔案或資料夾的路徑。<br>• 輸入物件雜湊。<br>• 使用遮罩：<br>  • `*`（星號）字元代表任意一組字元，但 `\` 和 `/` 字元除外（這兩個字元是檔案和資料夾路徑中的檔案和資料夾名稱的分隔符號）。例如，遮罩"`C:\*\*.txt`"將包括位於 C: 磁碟機但是不在子資料夾中所有帶 TXT 副檔名的檔案的路徑。<br>  • 兩個連續 `*` 字元在檔案或資料夾名稱中代表任意一組字元（包括空集），包括 `\` 和 `/` 字元（這兩個字元是檔案和資料夾路徑中的檔案和資料夾名稱的分隔符號）。例如，遮罩 `C:\Folder\**\*.txt` 將包括位於巢嵌在 `Folder` 內的資料夾（`Folder` 自身除外）中所有帶 TXT 副檔名的檔案的路徑。遮罩必須包含至少一個嵌套等級。遮罩 `C:\**\*.txt` 不是有效遮罩。<br>  • `?`（問號）字元代表任意單個字元，但 `\` 和 `/` 字元除外（這兩個字元是檔案和資料夾路徑中的檔案和資料夾名稱的分隔符號）。例如，遮罩 `C:\Folder\???.txt` 將包括位於 `Folder` 資料夾中所有帶 TXT 副檔名且名稱由三個字元構成的檔案的路徑。<br>  您可以在檔案或者資料夾路徑的任何地方使用遮罩。例如，如果您想要掃描範圍包括電腦上的所有使用者帳戶的"下載"資料夾，請輸入 `C:\Users\*\Downloads\` 遮罩。<br>  Kaspersky Endpoint Security 支援環境變數<br>  > 當使用卡巴斯基安全管理中心主控台產生排除項目清單時，Kaspersky Endpoint Security 不支援"`%userprofile%`"環境變量。若要將項目套用到所有使用者帳戶，您可以使用 * 字元（例如，`C:\Users\*\Documents\File.exe`）。無論何時新增新的環境變數，您都需要重啟應用程式。<br>• 根據 Kaspersky 百科全書 的分類輸入物件的名稱（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。<br>> 如果管理員在主控台中封鎖可信任應用程式的配置（"關閉的鎖"符號）並且禁止本機可信任應用程式（ **允許使用本機排除項目** 核取方塊被清除），Kaspersky Endpoint Security 將在應用程式的使用者介面中隱藏掃描排除項目清單。 |
| **受信任應用程式** | 此表列出了受信任應用程式，其活動在操作過程中不受 Kaspersky Endpoint Security 監控。<br>Kaspersky Endpoint Security 輸入遮罩時支援環境變量以及 `*` 和 `?` 字元。<br>> 當在卡巴斯基安全管理中心主控台上產生受信任應用程式清單時，Kaspersky Endpoint Security 不支援"`%userprofile%`"環境變量。若要將項目套用到所有使用者帳戶，您可以使用 * 字元（例如，`C:\Users\*\Documents\File.exe`）。無論何時新增新的環境變數，您都需要重啟應用程式。<br>"應用程式控制"元件控制每個應用程式的啟動，不管該應用程式是否包括在受信任應用程式表中。<br>> 如果管理員在主控台中封鎖可信任應用程式的配置（"關閉的鎖"符號）並且禁止本機可信任應用程式（ **允許使用受信任應用程式** 核取方塊被清除）。 |
| **繼承時合併值**<br>*（僅在卡巴斯基安全管理中心主控台中可用）* | 這會合併卡巴斯基安全管理中心的父級和子級政策中的掃描排除項目和受信任應用程式的清單。要合併清單，必須將子政策設定為繼承卡巴斯基安全管理中心父政策的設定。<br>如果選中此核取方塊，則子政策中將顯示卡巴斯基安全管理中心父政策的清單項目。這樣，您可以（例如）建立整個組織的受信任應用程式的合併清單。<br>子政策中繼承的清單項無法被刪除或編輯。在繼承過程中合併的掃描排除項目清單和受信任應用程式清單中的項目只能在父政策中進行刪除和編輯。您可以新增、編輯或刪除較低等級之政策中的清單項目。<br>如果子政策和父政策清單上的項目相符，則這些項目將顯示為父政策的同一項目。<br>如果未選中該核取方塊，則在繼承卡巴斯基安全管理中心政策設定時不會合併清單項。<br>此功能還允許合併政策設定檔中的清單。若要合併清單，請在最高優先順序的設定檔中啟用從較低優先順序的設定檔繼承設定。有關政策設定檔優先順序的詳細資訊，請參閱卡巴斯基安全管理中心說明。 |

| | |
|---|---|
| **允許使用本機排除項目/允許使用受信任應用程式**<br>*（僅在卡巴斯基安全管理中心主控台中可用）* | *本機排除項目和本機受信任的應用程式* – Kaspersky Endpoint Security 中特定電腦的使用者定義的物件和應用程式清單。Kaspersky Endpoint Security不 會監控本機受信任區域中的物件和應用程式。這樣，除了政策中的一般受信任區域之外，使用者還可以建立自己的排除項目和受信任應用程式"的本機清單。<br>如果選中此核取方塊，則使用者可以建立掃描排除項目本機清單和受信任應用程式本機清單。管理員可以使用卡巴斯基安全管理中心檢視、新增、編輯或刪除電腦屬性中的清單項目。<br>如果核取方塊被清理，使用者只能存取政策中產生的掃描排除項目和受信任應用程式的一般清單。 |
| **EDR (KATA) / NDR (KATA) 遙測**<br>*（僅在卡巴斯基安全管理中心主控台中可用）* | 此表包含 EDR 遙測排除項目的相關資訊。 |
| **KUMA 遙測**<br>*（僅在卡巴斯基安全管理中心主控台中可用）* | 要傳送到 Kaspersky Unified Monitoring and Analysis Platform (KUMA) 的事件清單。Kaspersky Endpoint Security 以下列模式運作：<br>• **傳送所有事件**在此模式下，應用程式會傳送 Windows 日誌中的所有事件（新增到排除規則的事件除外）。<br>• **僅傳送選取的事件**在此模式下，應用程式僅會傳送包含規則中新增的事件。 |
| **受信任的系統憑證儲存** | 如果選擇了一個受信任的系統憑證儲存，則 Kaspersky Endpoint Security 將從掃描中排除使用受信任數位簽章簽名的應用程式。Kaspersky Endpoint Security 會自動將此類應用程式分配給**受信任**群組。<br>如果選擇了**不使用**，Kaspersky Endpoint Security 將掃描應用程式，無論它們是否具有數位簽章。Kaspersky Endpoint Security 會將應用程式放置在某個信任群組中，實際取決於該應用程式可能對電腦造成的危險等級而定。 |

# 應用程式設定

您可以配置應用程式的以下一般設定：

- 操作模式
- 自我防護
- 效能
- 偵錯資訊
- 套用設定時的電腦狀態

應用程式設定

| 參數 | 描述 |
|---|---|
| **在電腦啟動時啟動應用程式（建議）** | 選取此選項後，Kaspersky Endpoint Security 將隨作業系統啟動，且在整個工作階段保護電腦。<br>若未選取此選項，Kaspersky Endpoint Security 將不會隨作業系統啟動，需使用者手動啟動。電腦防護已停用，使用者資料可能受到威脅。 |
| **使用進階解毒技術 (需要大量電腦資源)** | 通常情況下，Kaspersky Endpoint Security 會在電腦被感染之前終止偵測到的惡意軟體。進階解毒技術可防護電腦免受活動的惡意軟體（活動感染）的侵害，從而最大限度地降低資料遺失和威脅擴散的風險。<br>如果啟用此技術，當偵測到惡意活動時，Kaspersky Endpoint Security 會顯示彈出通知。Kaspersky Endpoint Security 會在通知中建議使用者對電腦執行進階解毒。使用者批准此過程後，Kaspersky Endpoint Security 會解毒此威脅，然後重慶電腦。進階解毒技術會佔用相當多的電腦資源，這可能會降低其他應用程式的執行速度。<br>當應用程式偵測活動感染時，作業系統的一些功能可能無法使用。作業系統的可用性將在進階解毒完成和電腦重新啟動後還原。<br>如果 Kaspersky Endpoint Security 安裝在執行 Windows for Servers 的電腦上，則 Kaspersky Endpoint Security 不顯示通知。因此，您無法選擇解毒活動威脅的動作。若要解毒威脅，您需要在應用程式設定中啟用進階解毒技術，在"*惡意軟體掃描*"工作設定中啟用立即執行進階解毒。然後您需要啟動"*惡意軟體掃描*"工作。 |

| 參數 | 描述 |
| --- | --- |
| **使用卡巴斯基安全管理中心作為啟動代理伺服器**<br>*（僅在卡巴斯基安全管理中心主控台中可用）* | 如果選中此核取方塊，應用程式將使用卡巴斯基安全管理中心管理伺服器作為連線到啟動伺服器的代理伺服器。當您使用啟動碼在無法存取網際網路的隔離網段中啟動應用程式時，這是必要的。如果您使用金鑰檔案啟動應用程式，則无需存取網際網路。 |
| **啟用自我防護** | 如果啟用該功能，Kaspersky Endpoint Security 可避免修改或刪除磁碟機中的應用程式檔案、記憶體程序和系統登錄中的項目。 |
| **封鎖應用程式服務的外部管理** | 如果啟用該功能，Kaspersky Endpoint Security 不會允許使用第三方應用程式（如 CMD）管理應用程式服務。當出現使用協力廠商應用程式管理應用程式服務的企圖時，一條通知將顯示在 Microsoft Windows 工作列的應用程式圖示上方（除非使用者停用了通知服務）。<br>您只能在不支援 AM-PPL 技術或停用了該技術的電腦上允許對應用程式服務進行外部管理。 |
| **使用電池供電時延遲排程工作** | 如果勾選此核取方塊，則當電腦使用電池供電時，將啟用省電模式。Kaspersky Endpoint Security 延遲排程工作。如果需要，您可以手動啟動掃描和更新工作。<br>啟用節能模式且電腦使用電池執行時，即使排程了以下工作，以下工作也不會執行：<br>• *資料庫和應用程式模組更新*<br>• *完整掃描*<br>• *關鍵區域掃描*<br>• *自訂掃描*<br>• *應用程式完整性檢查*<br>• *IOC 掃描* |
| **將資源讓給其他應用程式** | Kaspersky Endpoint Security 在掃描電腦時對電腦資源的使用，可能會增加 CPU 和硬碟子系統的負載。這可能減緩其他應用程式的速度。為了最佳化效能，Kaspersky Endpoint Security 提供了一種*將資源傳輸到其他應用程式的模式*。在此模式中，當 CPU 負載過高時，作業係統可降低 Kaspersky Endpoint Security 掃描工作執行緒的優先順序。這可允許重新分配作業係統資源到其他應用程式。因此，掃描工作將收到更少的 CPU 時間。結果，Kaspersky Endpoint Security 將花更多時間來掃描電腦。預設情況下，應用程式已設定為允許其他應用程式使用資源。 |
| **限制掃描工作的 CPU 使用** | 若要最佳化 Kaspersky Endpoint Security 效能，您可以透過 *惡意軟體掃描* 工作限制 CPU 使用率。<br>如果選取該核取方塊，則 *惡意軟體掃描* 工作的所有 CPU 核心上的平均負載會接近指定的值。<br>預設情況下，會取消勾選核取方塊。 |
| **啟用傾印寫入** | 如果選擇此核取方塊，Kaspersky Endpoint Security 將在當機時寫入傾印檔案。<br>如果清除此核取方塊，Kaspersky Endpoint Security 將不再寫入傾印。應用程式也會從電腦硬碟中刪除現有的傾印檔案。 |
| **啟用傾印和偵錯檔案防護** | 如果選中此核取方塊，本機管理員和系統管理員以及啟用了傾印寫入的使用者可以存取傾印檔案。只有系統和本機管理員可以存取偵錯檔案。<br>如果清空此核取方塊，任何使用者可以存取傾印檔案和偵錯檔案。 |
| **套用設定時的電腦狀態**<br>*（僅在卡巴斯基安全管理中心主控台中可用）* | 套用政策或執行工作出錯時，安裝了 Kaspersky Endpoint Security 的用戶端電腦的狀態在網頁主控台中的顯示設定。以下狀態可以使用：*確定*，*警告*和*緊急*。 |
| **安裝更新而不重新啟動電腦** | 升級應用程式而無需重新啟動電腦可讓您確保不中斷的伺服器作業。<br>從版本 11.10.0 開始您可以升級應用程式而無需重新啟動。若要升級更早版本的應用程式，您必須重新啟動電腦。<br>從版本 11.11.0 開始，您可以執行以下操作而無需重啟電腦：<br>• 安裝修補程式<br>• 變更應用程式元件集合<br>• 在 Kaspersky Security for Windows Server 上安裝 Kaspersky Endpoint Security<br>預設參數值因作業系統類型而異。如果應用程式安裝在工作站上，升級應用程式而無需重新啟動選項將被停用。如果應用程式安裝在伺服器上，升級應用程式而無需重新啟動選項將被啟用。 |

| 參數 | 描述 |
| --- | --- |
| **與遠端管理軟體相容**<br>*（僅在卡巴斯基安全管理中心主控台中可用）* | 如果將 Kaspersky Endpoint Security 與遠端管理工具 (RAT) 一起使用會導致問題，您可以啟用相容模式。這些問題可能與 RAT 與應用程式的Secure Desktop功能不相容有關。此功能的目的是確認可能降低電腦安全等級的操作。此功能允許應用程式顯示與其他處理程序隔離的確認對話方塊。此功能使用提升的權限來防護請求。這樣，只有使用者才能確認操作，而惡意軟體無法確認。<br>如果選擇此選項，則啟用 RAT 相容模式。應用程式會顯示一個沒有此功能的確認對話方塊。這會降低電腦的安全等級。如果 Kaspersky Endpoint Security 沒有導致您的 RAT 出現問題，我們不建議啟用相容模式。<br>如果清除此選項，則停用 RAT 相容模式。預設情況下，會取消勾選核取方塊。<br>示例：在 RemoteApp 模式中使用瀏覽器時，Kaspersky Endpoint Security 在訪問具有不受信任憑證的網站時可能不會顯示確認視窗，因為 RemoteApp 不支援應用程式的安全桌面功能。這可能會導致瀏覽器無響應。為了使瀏覽器在 RemoteApp 模式中正常工作，必須啟用相容模式。如果您在使用其他協力廠商軟體時遇到安全桌面功能問題，也可以嘗試啟用相容模式。 |

# 報告和儲存

## 報告

有關每個 Kaspersky Endpoint Security 元件的操作、資料加密事件、每個掃描工作的效能、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記錄在報告中。

報告儲存在 `C:\ProgramData\Kaspersky Lab\KES.12.12\Report` 資料夾中。

## 備份

*備份區*儲存保留在解毒過程中刪除或修改的檔案的備份副本。*備份副本*是指對檔案進行病毒清除或移除前建立的檔案副本。檔案的備份副本以特定格式儲存並且不會帶來威脅。

檔案的備份副本儲存在 `C:\ProgramData\Kaspersky Lab\KES.12.12\QB` 資料夾中。

管理員群組中的使用者被授予存取該資料夾的完整權限。其帳戶用於安裝 Kaspersky Endpoint Security 的使用者被授予該資料夾的有限存取權限。

Kaspersky Endpoint Security 不提供用於設定檔備份副本的使用者存取權限的功能。

## 隔離

*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。隔離檔案以加密狀態儲存，不會威脅裝置安全。Kaspersky Endpoint Security 僅在使用以下 Detection and Response 解決方案時使用隔離：EDR Optimum、EDR Expert、KATA (EDR)、Kaspersky Sandbox。在其他情況下，Kaspersky Endpoint Security 將相關檔案放置在備份中。若要瞭解將隔離作為解決方案的一部分進行管理的詳情，請參見Kaspersky Sandbox 說明、Kaspersky Endpoint Detection and Response Optimum 說明、Kaspersky Endpoint Detection and Response Expert 說明、Kaspersky Anti Targeted Attack Platform 說明。

隔離只能使用網頁主控台進行配置。您也可以使用網頁主控台來管理隔離的物件（還原，刪除，新增，等等）。您可以使用命令列在電腦上本機還原物件。.

Kaspersky Endpoint Security 使用系統帳戶 (SYSTEM) 隔離檔案。

報告和儲存的設定

| 參數 | 描述 |
| --- | --- |
| **以下時間後刪除報告 (天)** | 如果選中該核取方塊，則最大報告儲存期限制為定義的時間隔。預設的報告最長儲存期限是 30 天。在此時間之後，Kaspersky Endpoint Security 將自動移除報告檔案中的最早項目。 |
| **報告檔案大小限制為 (MB)** | 如果選中該核取方塊，則最大報告檔案大小限制為定義值。預設情況下，最大檔案大小資料為 1024 MB。要避免超過最大報告檔案容量，當達到最大報告檔案容量時，Kaspersky Endpoint Security 將自動刪除報告檔案中的最早項目。 |
| **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。預設的檔案最長儲存期限是 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。 |
| **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，最大大小為 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。 |
| **限制隔離區大小** | 如果選中該核取方塊，則最大隔離區大小限制為定義值。預設情況下，最大大小為 1024 MB。當隔離區達到最大大小時，Kaspersky Endpoint Security 會將*隔離區儲存空間不足*事件發送到卡巴斯基安全管理中心並在 Windows 事件記錄中發佈事件。同時，應用程式會停止隔離新物件。您必須手動清空隔離區。 |
| **通知隔離區儲存達到 (%)** | 隔離的閾值。例如，您可以設定隔離閾值為 50%。當隔離達到閾值時，Kaspersky Endpoint Security 會發送相應事件到卡巴斯基安全管理中心並在Windows 事件記錄中發佈事件。同時，應用程式會繼續隔離新物件。 |
| **到管理伺服器的資料傳輸**<br>*（僅在卡巴斯基安全管理中心中可用）* | 其資訊必須傳送到管理伺服器的用戶端電腦上的事件類別。您可以停用某些資料的傳輸以最佳化管理伺服器上的磁碟空間。<br>應用程式發送以下類別的事件：<br>• **關於隔離檔案**您可以在卡巴斯基安全管理中心主控台的"**進階 → 儲存區 → 隔離區**"資料夾中檢視正在執行的可執行檔的清單。Kaspersky Endpoint Security 僅在與 Detection and Response 解決方案整合時使用隔離區。<br>• **關於備份區中的檔案**您可以在卡巴斯基安全管理中心主控台的"**進階 → 儲存區 → 備份**"資料夾中檢視備份區中的檔案清單。<br>• **關於未處理的檔案**您可以在卡巴斯基安全管理中心主控台的**進階 → 儲存區 → 活動威脅**資料夾中檢視未處理檔案的清單。<br>• **關於已安裝的裝置**您可以在卡巴斯基安全管理中心主控台的"**進階 → 儲存區 → 硬體**"資料夾中檢視已連線裝置的清單。裝置清單也可在電腦屬性和 Kaspersky Endpoint Security for Windows 政策中找到（**裝置控制** 部分）。<br>• **關於已啟動的應用程式**您可以在卡巴斯基安全管理中心主控台的"**進階 → 應用程式管理 → 可執行檔**"資料夾中檢視可執行檔的清單。可執行檔清單也可在電腦屬性中找到。<br>• **關於檔案加密錯誤**您可以在卡巴斯基安全管理中心主控台的"**進階 → 資料加密與防護 → 加密事件**"資料夾中檢視檔案加密錯誤清單。錯誤清單也可在電腦屬性中找到。<br>• **自適應異常控制規則觸發報告**您可以在 在卡巴斯基安全管理中心 主控台中 **管理伺服器** 節點上的 **報告** 頁簽上檢視報告。此報告也可在 Kaspersky Endpoint Security for Windows 政策屬性 (**自適應異常控制** 部分）中找到。<br>• **關於觸發的自適應異常控制規則的報告**您可以在 在卡巴斯基安全管理中心 主控台中 **管理伺服器** 節點上的 **報告** 頁簽上檢視報告。此報告也可在 Kaspersky Endpoint Security for Windows 政策屬性 (**自適應異常控制** 部分）中找到。<br>• **關於威脅發展鏈條**您可以在卡巴斯基安全管理中心網頁主控台的 **監控和報告 → 警示** 部分中檢視偵測詳情。有關威脅發展鏈的資訊由 Kaspersky Endpoint Detection and Response 解決方案使用。 |

# 網路設定

您可以設定用於連線到網際網路和更新病毒資料庫的代理伺服器，選擇網路連接埠監控模式，以及設定加密連線掃描。

| 參數 | 描述 |
| --- | --- |
| **連線按流量收費時限制流量** | 如果選擇該核取方塊，應用程式將在網際網路連線受限時限制其網路流量。Kaspersky Endpoint Security 會將高速移動網際網路連線辨識為受限制連線，將 Wi-Fi 連線辨識為無限制連線。<br>網路數據流量控制可在執行 Windows 8 或更高版本的電腦上使用。 |
| **注入指令碼到網頁流量從而與網頁互動** | 如果選定該核取方塊，Kaspersky Endpoint Security 會將網頁監聽指令碼注入網頁流量。此指令碼可確保 Web 控制元件正常工作。指令碼將啟用 Web 控制事件的註冊。沒有此指令碼，您將無法啟用使用者網際網路活動監控 。<br>卡巴斯基專家建議將此網頁交互指令碼注入流量中，以確保 Web 控制的正確運行。 |
| **代理伺服器設定** | 用於用戶端電腦使用者存取網際網路的代理伺服器的設定。Kaspersky Endpoint Security 使用這些設定來配置某些防護元件，包括進行與更新資料庫和程式模組有關的配置。<br>為了自動配置代理伺服器，Kaspersky Endpoint Security 使用了 WPAD 協定（Web 代理自動發現協定）。如果使用該協定無法確定代理伺服器的 IP 位址，則應用程式使用在 Microsoft Internet Explorer 瀏覽器設定中指定的代理伺服器位址。 |
| **本機位址略過代理伺服器** | 如果選擇此方塊，則 Kaspersky Endpoint Security 從共用資料夾執行更新時不使用代理伺服器。 |
| **代理伺服器身分驗證設定** | 若要驗證代理伺服器上的應用程式的網際網路存取權限，您必須輸入使用者的憑據。Kaspersky Endpoint Security 支援在代理伺服器上進行自動身分驗證。如果自動身分驗證失敗，應用程式會提示您輸入憑據。<br>**不使用身分驗證**<br>**NTLM 身分驗證**使用目前使用者帳戶進行 NTLM 身分驗證（預設）。<br>**使用使用者名稱和密碼進行 NTLM 身分驗證**使用手動指定的憑據進行 NTLM 身分驗證。<br>**使用者名稱和密碼**使用手動指定的憑據進行身分驗證。<br>**自動進行身分驗證**<br>**Kerberos 身分驗證**使用目前使用者帳戶進行 Kerberos 身分驗證。<br>**使用使用者名稱和密碼進行 Kerberos 身分驗證**使用手動指定的憑據進行 Kerberos 身分驗證。<br>如果選擇 Kerberos 驗證，Kaspersky Endpoint Security 可以根據代理伺服器設定使用 Kerberos 或 NTLM 協定執行身分驗證。 |
| **監控的連接埠** | **監控所有網路連接埠**在此網路連接埠監控模式下，防護元件（檔案威脅防護、Web 威脅防護和郵件威脅防護）會監控透過任何開放的電腦網路連接埠傳輸的資料流。<br>**僅監控選定網路連接埠**在此網路連接埠監視模式下，防護元件將監控電腦的選定連接埠和選定應用程式的網路活動。通常用於傳輸電子郵件和網路流量的網路連接埠的清單按照 Kaspersky 專家的建議進行配置。<br>**監控卡巴斯基建議的清單中的應用程式的所有連接埠**這將使用其網路連接埠受 Kaspersky Endpoint Security 監控的應用程式的預定義清單。例如，此清單包括 Google Chrome、Adobe Reader、Java 和其他應用程式。<br>**監控指定應用程式的所有連接埠**這將使用其網路連接埠受 Kaspersky Endpoint Security 監控的應用程式清單。 |
| **加密連線掃描** | Kaspersky Endpoint Security 掃描透過以下協定傳輸的加密網路流量：<br>• SSL 3.0。<br>• TLS 1.0、TLS 1.1、TLS 1.2、TLS 1.3。<br>Kaspersky Endpoint Security 支援以下加密連線掃描模式：<br>• **不掃描加密連線**Kaspersky Endpoint Security 將無法存取其位址以 `https://` 開頭的網站的內容。<br>• **根據防護元件的請求掃描加密連線**僅在 Web 威脅防護、郵件威脅防護和 Web 控制元件要求時，Kaspersky Endpoint Security 才會掃描加密流量。<br>• **始終掃描加密連線**即使防護元件被停用，Kaspersky Endpoint Security 也會掃描加密的網路流量。<br>Kaspersky Endpoint Security 不會掃描由停用了流量掃描的受信任應用程式建立的加密連線。Kaspersky Endpoint Security 不會掃描預定義的受信任網站清單中的加密連線。預定義的受信任網站清單由卡巴斯基專家建立。此清單已使用應用程式的病毒資料庫更新。您只能在 Kaspersky Endpoint Security 介面中檢視預定義的受信任網站清單。您只能在卡巴斯基安全管理中心主控台中檢視清單。 |

| 參數 | 描述 |
| --- | --- |
| **信任根憑證** | 信任根憑證清單。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，你會因為憑證問題得到一個連線錯誤。若要新增至系統憑證商店，您可以使用 Active Directory 群組政策。 |
| **正在造訪具有不受信任憑證的網域** | • **允許**當存取具有不受信任憑證的網域時，Kaspersky Endpoint Security 將允許網路連線。<br>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，其中顯示警告和不建議存取該網域的原因。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。<br>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，Kaspersky Endpoint Security 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。<br>• **封鎖**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。 |
| **造訪包含加密連線掃描錯誤的網域** | • **封鎖**如果選取此項，在發生加密連線掃描錯誤時，Kaspersky Endpoint Security 會封鎖網路連線。<br>• **允許並新增網域至排除項目**如果選取此項，在發生加密連線掃描錯誤時，Kaspersky Endpoint Security 將導致錯誤的網域新增到具有掃描錯誤的網域清單中，並且在存取此網域時不監控加密網路流量。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。要清除清單內容，您需要選擇"**封鎖**"。Kaspersky Endpoint Security 還會為加密連線掃描錯誤產生一個事件。 |
| **封鎖 SSL 2.0 連線** | 如果選中該核取方塊，應用程式將監控和封鎖透過 SSL 2.0 協定建立的網路連線。<br>如果清除該核取方塊，應用程式將不封鎖透過 SSL 2.0 協定建立的網路連線。不過，該應用程式不會監控通過該協定的網路流量。 |
| **封鎖 SSL 3.0 連線** | 如果選中該核取方塊，應用程式將封鎖透過 SSL 3.0 協定建立的網路連線。<br>如果清除該核取方塊，應用程式將不封鎖透過 SSL 3.0 協定建立的網路連線。應用程式將監控透過該協定的網路流量。應用程式的所有組件均不受限制地運作。 |
| **封鎖 TLS 1.0 連線** | 如果選中該核取方塊，應用程式將封鎖透過 TLS 1.0 協定建立的網路連線。<br>如果清除該核取方塊，應用程式將不封鎖透過 TLS 1.0 協定建立的網路連線。應用程式將監控透過該協定的網路流量。應用程式的所有組件均不受限制地運作。 |
| **解密與使用 EV 憑證的網站之間的加密連線** | EV 憑證（Extended Validation Certificate）確認網站的真實性並增強連線的安全性。瀏覽器在網址列中使用鎖定圖示來指示網站具有 EV 憑證。瀏覽器也可能用綠色部分或完全渲染網址列。<br>如果選中該核取方塊，應用程式將解密並監控具有 EV 憑證的網站的加密連線。<br>如果清除該核取方塊，應用程式無權存取 HTTPS 流量的內容。為此，應用程式僅基於網址（例如 `https://bing.com`）監控 HTTPS 流量。<br>如果您第一次開啟具有 EV 憑證的網站，則無論是否選中該核取方塊，加密連線都將被解密。 |
| **設定受信任位址** | 這將使用 Kaspersky Endpoint Security 不對其掃描加密網路連線的網址清單。在此情況下，當 Web 威脅防護、郵件威脅防護、Web 控制元件執行工作時，Kaspersky Endpoint Security 不掃描受信任網址的 HTTPS 流量。<br>您可以輸入網域名稱或 IP 位址。Kaspersky Endpoint Security 支援 `*` 字元用於在網域名稱中輸入遮罩。<br>Kaspersky Endpoint Security 不支援 IP 位址的 `*` 符號。您可以使用子網路遮罩（例如，198.51.100.0/24）選擇一個 IP 位址範圍。<br>例如：<br>• `domain.com` – 該記錄包括以下位址：`https://domain.com`，`https://www.domain.com`，`https://domain.com/page123`。該記錄排除子網域（例如，`subdomain.domain.com`）。<br>• `subdomain.domain.com` – 該記錄包括以下位址：`https://subdomain.domain.com`，`https://subdomain.domain.com/page123`。該記錄排除 `domain.com` 子網域。<br>• `*.domain.com` – 該記錄包括以下位址：`https://movies.domain.com`，`https://images.domain.com/page123`。該記錄排除 `domain.com` 子網域。 |
| **設定受信任應用程式** | 其活動在操作過程中不受 Kaspersky Endpoint Security 監控的應用程式清單。您可以選擇 Kaspersky Endpoint Security 不會監控的應用程式活動的類型（例如，不掃描網路流量）。Kaspersky Endpoint Security 輸入遮罩時支援環境變量以及 `*` 和 `?` 字元。 |

| 參數 | 描述 |
| --- | --- |
| **若要使用其自己的憑證儲存來掃描應用程式中的加密連線，請使用**<br>*（僅在 Kaspersky Endpoint Security 介面中可用）* | 如果選中此核取方塊，則應用程式會掃描 Mozilla Firefox 瀏覽器和 Thunderbird 郵件用戶端中的加密流量。透過 HTTPS 協定存取一些網站可能被封鎖。<br>若要掃描 Mozilla Firefox 瀏覽器和 Thunderbird 郵件用戶端中的流量，您必須啟用加密連線掃描。如果停用加密連線掃描，則應用程式不會掃描 Mozilla Firefox 瀏覽器和 Thunderbird 郵件用戶端中的流量。<br>應用程式使用 Kaspersky 根憑證來解密和分析加密的流量。您可以選擇將包含卡巴斯基根憑證的憑證儲存。<br>• **Windows 憑證儲存(建議)**在安裝 Kaspersky Endpoint Security 期間，會將 Kaspersky 根憑證新增到此儲存中。<br>• **自有憑證儲存**Mozilla Firefox 和 Thunderbird 使用它們自己的憑證儲存。如果選擇了 Mozilla 憑證儲存，則需要通過瀏覽器屬性手動將 Kaspersky 根憑證新增到該儲存中。 |

# 介面

您可以配置應用程式介面的設定。

介面設定

| 參數 | 描述 |
| --- | --- |
| **使用者互動**<br>*（僅在卡巴斯基安全管理中心主控台中可用）* | **顯示簡化介面**在用戶端電腦上，主應用程式視窗不可存取，只有 Windows 通知區域中的圖示可用。在該圖示的內容功能表中，使用者可以使用 Kaspersky Endpoint Security 執行有限數量的操作。Kaspersky Endpoint Security 還會在應用程式圖示上方顯示通知。<br>**顯示使用者介面**在用戶端電腦上，Kaspersky Endpoint Security 的主視窗和 Windows 通知區域中的圖示均可用。在該圖示的內容功能表中，使用者可以使用 Kaspersky Endpoint Security 執行操作。Kaspersky Endpoint Security 還會在應用程式圖示上方顯示通知。<br>**隱藏應用程式活動監控區域**在用戶端電腦的 Kaspersky Endpoint Security 的主視窗中，**應用程式活動監控**按鈕不可用。*應用程式活動監控*是一個用於即時檢視使用者電腦上的應用程式活動資訊的工具。<br>**不顯示使用者介面**在用戶端電腦上，不顯示 Kaspersky Endpoint Security 操作的跡象。Windows 通知區域中的圖示和通知不可用。 |
| **設定通知** | 此表包含在元件、工作或整個應用程式操作過程中可能發生的具有不同重要等級的事件的相關通知的設定。Kaspersky Endpoint Security 將在螢幕上顯示這些事件的通知，透過電子郵件傳送它們或者在記錄中記錄它們。 |
| **設定電子郵件通知** | SMTP 伺服器設定，用於傳送有關應用程式執行期間註冊的事件的通知。<br>預設情況下，Kaspersky Endpoint Security 使用來自卡巴斯基安全管理中心的電子郵件通知設定。有關電子郵件通知設定的詳細資訊，請參閱卡巴斯基安全管理中心說明。<br>如果您需要配置單獨的電子郵件通知，您可以編輯以下設定：<br>• **寄件者郵件信箱**寄件者的電子郵件信箱。不建議使用不存在的位址。<br>• **SMTP 伺服器**您所在組織的電子郵件伺服器的一個或多個位址（例如， `mail.company.com`）。您可以輸入 IP 位址（IPv4 或 IPv6）。<br>要在 SMTP 伺服器上驗證使用者，請在相應欄位中輸入寄件者憑據。要測試電子郵件通知，您可以傳送測試訊息。<br>• **收件者郵件信箱**應用程式將向其傳送通知的收件人的電子郵件信箱。<br>• **傳送方式**電子郵件通知的傳送模式。Kaspersky Endpoint Security 可以在事件發生時立即傳送訊息；或者，它可以遵循預先配置的時間表。 |
| **在通知區域顯示應用程式的狀態** | 使 Kaspersky Endpoint Security 圖示在 Microsoft Windows 工作列通知區域中發生變化（ 或 ）並生成彈出通知的應用程式事件的類別。 |
| **本機惡意軟體資料庫狀態通知** | 應用程式使用的病毒資料庫過期的通知設定。 |
| **密碼防護** | 如果開啟切換按鈕，當使用者嘗試執行密碼防護範圍內的操作時，Kaspersky Endpoint Security 將提示使用者輸入密碼。密碼防護範圍包括禁止的操作（如停用防護元件）和密碼防護範圍適用的使用者帳戶。<br>啟用密碼防護後，Kaspersky Endpoint Security 會提示您設定 KLAdmin 帳戶的密碼。 |

| 參數 | 描述 |
| --- | --- |
| **使用者支援/網路資源連結**<br><br>*（僅在卡巴斯基安全管理中心主控台中可用）* | Web 資源連結清單，包含有關 Kaspersky Endpoint Security 技術支援的資訊。所新增的連結顯示在 Kaspersky Endpoint Security 本機介面的"**支援**"視窗中，而不是標準連結。 |
| **使用者支援/敘述**<br><br>*（僅在卡巴斯基安全管理中心主控台中可用）* | Kaspersky Endpoint Security 本機介面的"**支援**"視窗中顯示的訊息。 |

# 監控設定

您可以將當前的 Kaspersky Endpoint Security 設定儲存到檔案中，並使用它們在另一台電腦上快速配置應用程式。透過卡巴斯基安全管理中心使用安裝套件部署應用程式時，也可以使用設定檔。您可以隨時還原預設設定 。

應用程式配置管理設定僅在 Kaspersky Endpoint Security 介面中可用。

應用程式配置管理設定

| 設定 | 描述 |
| --- | --- |
| **匯入** | 以 CFG 格式獲取應用程式設定並應用它們。 |
| **匯出** | 以 CFG 格式將目前應用程式設定儲存至檔案。 |
| **還原** | 您可以隨時還原卡巴斯基建議的應用程式設定 。還原設定之後，應用程式將為所有防護元件設定"**建議**"安全等級。 |

# 更新資料庫和程式模組

更新 Kaspersky Endpoint Security 的資料庫和程式模組可為您的電腦提供最新防護。新病毒和其他類型的惡意程式每天都在全世界出現。Kaspersky Endpoint Security 資料庫包含關於威脅的資訊和解毒的方法。要快速偵測到威脅，建議您定期更新資料庫和應用程式模組。

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

定期更新需要一份程式要使用的活動授權檔案。如果目前沒有產品授權，您將只能執行一次更新。

您的電腦必須連線到網際網路才能成功下載來自卡巴斯基更新伺服器的更新資料。預設情況下，系統將自動確定網際網路連線設定。如果您使用代理伺服器，則需要設定代理伺服器設定。

透過 HTTPS 協定下載更新。當無法透過 HTTPS 協定下載更新時，也可以透過 HTTP 協定下載。

當執行更新時，以下物件將下載並安裝到您的電腦中：

- Kaspersky Endpoint Security 資料庫。由於資料庫包含了威脅簽章和關於如何刪除威脅的資訊，電腦因此而獲得防護。當搜尋並為受感染檔案解毒時，防護元件將使用此資訊。資料庫將不斷更新應對它們的方法和新威脅記錄。因此，我們建議您定期更新資料庫。

  除了 Kaspersky Endpoint Security 資料庫之外，系統也會更新已啟用程式元件以攔截網路流量的網路驅動程式。

- 程式模組。除了 Kaspersky Endpoint Security 資料庫，您也可以更新程式模組。更新程式模組可以修復 Kaspersky Endpoint Security 中的弱點、新增新功能或強化現有功能。

更新時，您的電腦上的程式模組和資料庫將與最新版本更新來源進行對比。如果您目前資料庫和程式模組與對應的最新版本不同，缺少的更新部分將安裝在您的電腦上。

如果資料庫過期，更新量可能會很大，這可能會花費更多的網際網路流量（最多達幾十 MB）。

Kaspersky Endpoint Security 資料庫的目前狀態相關資訊顯示在應用程式主視窗中，或者通知區域中當您將游標懸浮在應用程式圖示上看到的工具提示中。

有關更新工作執行期間更新結果和所有發生事件的資訊將記錄在 Kaspersky Endpoint Security 報告中。

如果應用程式正在 Light Agent 模式下運作，更新應用程式資料庫和模組時將涉及特別考慮 。

應用程式模組和資料庫更新設定

| 參數 | 描述 |
| --- | --- |
| **資料庫更新排程** | **自動**在該模式下，應用程式將按特定頻率檢查更新來源，以確定新更新軟體套件的可用性。檢查更新軟體套件的頻率在病毒爆發期間會增加，在其他時候會減小。在偵測到全新的更新軟體套件之後，Kaspersky Endpoint Security 會下載並將其安裝到您的電腦上。<br>**手動**使用該更新工作執行模式可以手動啟動更新工作。<br>**依排程**在該更新工作執行模式下，Kaspersky Endpoint Security 將按照您已經指定的排程執行更新工作。如果選擇該更新工作執行模式，您也可以手動啟動 Kaspersky Endpoint Security 更新工作。 |
| **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。<br>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。 |
| **更新來源** | *更新來源*是包含 Kaspersky Endpoint Security 的資料庫和程式模組更新的資源。<br>更新來源包括卡巴斯基安全管理中心、卡巴斯基更新伺服器、以及網路或本機資料夾。<br>更新來源的預設清單包括了卡巴斯基安全管理中心和卡巴斯基更新伺服器。您可以在清單中新增其他更新來源。您可以指定 HTTP/FTP 伺服器和共用資料夾作為更新來源。<br>除非它們是卡巴斯基的更新伺服器，否則 Kaspersky Endpoint Security 不支援來自 HTTPS 伺服器的更新。<br>如果選取了多個來源作為更新來源，Kaspersky Endpoint Security 將嘗試從清單頂端開始依次連接，使用從第一個可用源檢索到的更新資料執行更新工作。<br>預設情況下，Kaspersky Endpoint Security 使用卡巴斯基安全管理中心伺服器作為第一個更新來源。這有助於在更新時節省流量。如果政策未被套用到電腦，卡巴斯基伺服器將被選為*資料庫和應用程式模組更新*本機工作設定中的第一個更新來源，因為應用程式可能無法存取卡巴斯基安全管理中心伺服器。<br>如果應用程式在 Light Agent 模式下執行，SVM 上的一個資料夾將被選為更新來源。 |
| **執行資料庫更新身分** | 預設情況下，Kaspersky Endpoint Security 使用您用來登入作業系統的帳戶執行更新工作。但是，Kaspersky Endpoint Security 可以從使用者沒有存取權限的更新來源（例如，含有更新資料的共用資料夾）進行更新，或者從沒有設定過代理伺服器身分驗證的更新來源進行更新。在應用程式設定中，您可以指定一個擁有以上權限的使用者，然後使用此使用者帳戶開始 Kaspersky Endpoint Security 更新工作。 |

| 參數 | 描述 |
| --- | --- |
| **下載應用程式模組更新** | 使用應用程式資料庫更新下載應用程式模組更新。<br>如果選中此方塊，Kaspersky Endpoint Security 將會向使用者傳送關於可用應用程式模組更新的通知，並在執行更新工作時將應用程式模組更新包含到更新軟體套件中。應用程式模組更新的方式取決於以下設定：<br>• **安裝重大和指定的更新**如果選擇此選項，當有應用程式模組更新可用時，僅在這些更新透過應用程式介面或在卡巴斯基安全管理中心一側被本機批准後，Kaspersky Endpoint Security 才會自動安裝關鍵更新和所有其他應用程式模組更新。<br>• **僅安裝指定的更新**如果選擇此選項，當有應用程式模組更新可用時，僅在這些更新透過應用程式介面或在卡巴斯基安全管理中心一側被本機批准後，Kaspersky Endpoint Security 才會安裝它們。預設情況下已勾選此選項。<br>如果不選中此方塊，Kaspersky Endpoint Security 將不會向使用者傳送關於可用應用程式模組更新的通知，並且在執行更新工作時不將應用程式模組更新包含的更新軟體套件中。<br>如果應用程式模組更新需要檢視和接受最終使用者產品授權協議，應用程式將在最終使用者產品授權協議被接受後，安裝更新。<br>預設情況下選擇此核取方塊。 |
| **將更新複製到資料夾** | 如果選取該核取方塊，Kaspersky Endpoint Security 會將更新軟體套件複製到該核取方塊下指定的共用資料夾。然後，區域網路其他電腦可從此共用資料夾中接收更新資料。這可以減少網際網路流量，因為更新軟體套件僅下載一次。預設情況下指定了以下資料夾：`C:\ProgramData\Kaspersky Lab\KES.12.12\Update distribution\`。 |
| **要更新的代理伺服器**<br>*（僅在 Kaspersky Endpoint Security 介面中可用）* | 用戶端電腦使用者存取網際網路以更新應用程式模組和資料庫的代理伺服器設定。<br>為了自動配置代理伺服器，Kaspersky Endpoint Security 使用 WPAD 協定（Web Proxy Auto-Discovery Protocol）。如果使用該協定無法確定代理伺服器的 IP 位址，則 Kaspersky Endpoint Security 使用在Microsoft Internet Explorer瀏覽器設定中指定的代理伺服器位址。 |
| **本機位址略過代理伺服器**<br>*（僅在 Kaspersky Endpoint Security 介面中可用）* | 如果選擇此方塊，則 Kaspersky Endpoint Security 從共用資料夾執行更新時不使用代理伺服器。 |

# 附錄 2。應用程式信任群組

Kaspersky Endpoint Security 會將電腦上啟動的所有應用程式歸類到信任群組中。系統將根據應用程式給作業系統造成威脅的級別將其歸類到信任群組中。

信任群組的組別類型如下：

- **受信任**此群組中的應用程式，將會符合下列其中一個或多個條件：
  - 擁有信任開發者數位簽章的應用程式。
  - 在應用程式資料庫中記錄為卡巴斯基安全網路受信任應用程式。
  - 使用者將此應用程式置於*受信任*群組。

  不封鎖這些應用程式執行任何操作。
- **低限制**此群組中的應用程式，將會符合下列條件：
  - 未獲得信任供應商的數位簽章。
  - 在應用程式資料庫中未記錄為卡巴斯基安全網路受信任應用程式。
  - 使用者將此應用程式置於*低限制*群組。

應用程式將受最小限制進行作業系統資源的存取。

- **高限制**此群組中的應用程式，將會符合下列條件：
  - 未獲得信任供應商的數位簽章。
  - 在應用程式資料庫中未記錄為卡巴斯基安全網路受信任應用程式。
  - 使用者將此應用程式置於*高限制*群組。

  將會封鎖這些應用程式大部分的操作。
- **不信任**此群組中的應用程式，將會符合下列條件：
  - 未獲得信任供應商的數位簽章。
  - 在應用程式資料庫中未記錄為卡巴斯基安全網路受信任應用程式。
  - 使用者將此應用程式置於*不信任*群組。

  對於此類應用程式，所有操作都將被禁止。

# 附錄 3。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 4。郵件威脅防護附件篩選器的檔案類型

請注意檔案的實際格式可能不比對其檔案名副檔名。

如果您啟用了電子郵件附件篩選，則“郵件威脅防護”元件可能重新命名或刪除帶有以下副檔名的檔案：

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。與外部服務交互的網路設定

Kaspersky Endpoint Security 和卡巴斯基安全管理中心使用帶有 TLS（傳輸層安全性）的加密通訊通道來與 Kaspersky 的外部服務一起使用。

Kaspersky Endpoint Security 用以下網路設定與外部服務進行交互。

網路設定

| 位址 | 描述 |
| --- | --- |
| activation-v2.kaspersky.com/activationservice/activationservice.svc<br>通訊協定：HTTPS<br>連接埠：443 | 啟動應用程式。 |

| 位址 | 描述 |
| --- | --- |
| `s00.upd.kaspersky.com`<br>`s01.upd.kaspersky.com`<br>`s02.upd.kaspersky.com`<br>`s03.upd.kaspersky.com`<br>`s04.upd.kaspersky.com`<br>`s05.upd.kaspersky.com`<br>`s06.upd.kaspersky.com`<br>`s07.upd.kaspersky.com`<br>`s08.upd.kaspersky.com`<br>`s09.upd.kaspersky.com`<br>`s10.upd.kaspersky.com`<br>`s11.upd.kaspersky.com`<br>`s12.upd.kaspersky.com`<br>`s13.upd.kaspersky.com`<br>`s14.upd.kaspersky.com`<br>`s15.upd.kaspersky.com`<br>`s16.upd.kaspersky.com`<br>`s17.upd.kaspersky.com`<br>`s18.upd.kaspersky.com`<br>`s19.upd.kaspersky.com`<br>`cm.k.kaspersky-labs.com`<br>通訊協定：`HTTPS`<br>連接埠：`443` | 更新資料庫和應用程式軟體模組。 |
| `downloads.upd.kaspersky.com`<br>通訊協定：`HTTPS`<br>連接埠：`443` | • 更新資料庫和應用程式軟體模組。<br>• 驗證對卡巴斯基伺服器的存取。如果無法使用系統 DNS 存取伺服器，則應用程式將使用公用 DNS。為了確保更新病毒資料庫和維持電腦的安全水平，這很有必要。Kaspersky Endpoint Security 按以下順序使用下列公用 DNS 伺服器清單：<br>1. Google Public DNS (8.8.8.8)。<br>2. Cloudflare DNS (1.1.1.1)。<br>3. Alibaba Cloud DNS (223.6.6.6)。<br>4. Quad9 DNS (9.9.9.9)。<br>5. CleanBrowsing (185.228.168.168)。<br>應用程式發出的請求可能包含使用者的網域位址和公用 IP 位址，因為應用程式使用 DNS 伺服器建立 TCP/UDP 連線。該資訊需要用來（例如）在使用 HTTPS 時驗證網頁資源的憑證。如果 Kaspersky Endpoint Security 使用的是公用 DNS 伺服器，則資料處理將受相關服務的隱私權政策管理。如果您想要防止 Kaspersky Endpoint Security 使用公用 DNS 伺服器，請聯絡技術支援服務請求私人修補程式。 |
| `touch.kaspersky.com`<br>通訊協定：`HTTP` | • 接收檢查憑證有效期的受信任時間（TLS 連線）。<br>• 當 Web 威脅防護執行時在瀏覽器中警告被拒絕的 Web 資源存取。 |

| 位址 | 描述 |
| --- | --- |
| p00.upd.kaspersky.com<br>p01.upd.kaspersky.com<br>p02.upd.kaspersky.com<br>p03.upd.kaspersky.com<br>p04.upd.kaspersky.com<br>p05.upd.kaspersky.com<br>p06.upd.kaspersky.com<br>p07.upd.kaspersky.com<br>p08.upd.kaspersky.com<br>p09.upd.kaspersky.com<br>p10.upd.kaspersky.com<br>p11.upd.kaspersky.com<br>p12.upd.kaspersky.com<br>p13.upd.kaspersky.com<br>p14.upd.kaspersky.com<br>p15.upd.kaspersky.com<br>p16.upd.kaspersky.com<br>p17.upd.kaspersky.com<br>p18.upd.kaspersky.com<br>p19.upd.kaspersky.com<br>downloads.kaspersky-labs.com<br>cm.k.kaspersky-labs.com<br>通訊協定：`HTTP`<br>連接埠：`80` | 更新資料庫和應用程式軟體模組。 |
| ds.kaspersky.com<br>dc1.ksn.kaspersky-labs.com<br>dc1-file.ksn.kaspersky-labs.com<br>dc1-pp.ksn.kaspersky-labs.com<br>dc1-st.ksn.kaspersky-labs.com<br>通訊協定：`HTTPS`<br>連接埠：`443` | 使用卡巴斯基安全網路。 |
| ksn-a-stat-geo.kaspersky-labs.com<br>ksn-file-geo.kaspersky-labs.com<br>ksn-verdict-geo.kaspersky-labs.com<br>ksn-url-geo.kaspersky-labs.com<br>ksn-a-p2p-geo.kaspersky-labs.com<br>ksn-info-geo.kaspersky-labs.com<br>ksn-cinfo-geo.kaspersky-labs.com<br>通訊協定：`KSN`<br>連接埠：`443`, `1443` | 使用卡巴斯基安全網路。 |
| click.kaspersky.com<br><br>redirect.kaspersky.com<br>通訊協定：`HTTPS`<br>連接埠：`443` | 跟隨介面中的連接。 |

設定，用於加密

| 位址 | 描述 |
| --- | --- |
| crl.kaspersky.com<br>ocsp.kaspersky.com<br>通訊協定：`HTTP`<br>連接埠：`80` | 公鑰基礎結構（PKI）。 |

# 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記錄在卡巴斯基安全管理中心事件日誌和 Windows 事件日誌中。

Kaspersky Endpoint Security 可產生以下類型的事件：一般事件和具體事件。具體事件只能由 Kaspersky Endpoint Security for Windows 建立。具體事件具有簡單 ID，諸如`000000cb`。具體事件包含以下所需參數：

- `GNRL_EA_DESCRIPTION` 是事件內容。
- `GNRL_EA_ID` 是事件的服務 ID。
- `GNRL_EA_SEVERITY` 是事件狀態。`1` – *資訊*, `2` – *警告*, `3` – *功能失效*, `4` – *緊急*。
- `EVENT_TYPE_DISPLAY_NAME` 是事件標題。
- `TASK_DISPLAY_NAME` 是發起事件的應用程式元件的名稱。

一般事件可以由 Kaspersky Endpoint Security for Windows 以及其它 Kaspersky 應用程式（例如，Kaspersky Security for Windows Server）建立。一般事件具有更複雜的 ID，諸如`GNRL_EV_VIRUS_FOUND`。除了所需設定，一般事件包含進階設定。

事件儲存在伺服器上的時間

## 緊急

### 產品授權已到期

| | |
|---|---|
| 狀態 | ! |
| 元件 | 系統稽核 |
| Windows 事件 ID | 201 |
| 卡巴斯基安全管理中心事件 ID | GNRL_EV_LICENSE_EXPIRATION |
| Windows 事件日誌（預設） | ✓ |
| 卡巴斯基安全管理中心事件日誌（預設） | ✓ |

### 產品授權快到期了

| | |
|---|---|
| 狀態 | ! |
| 元件 | 系統稽核 |
| Windows 事件 ID | 203 |
| 卡巴斯基安全管理中心事件 ID | 000000cb |
| Windows 事件日誌（預設） | – |
| 卡巴斯基安全管理中心事件日誌（預設） | ✓ |

## 資料庫遺失或損壞

| | |
|---|---|
| 狀態 | ⓘ |
| 元件 | 系統稽核 |
| Windows 事件 ID | 206 |
| 卡巴斯基安全管理中心事件 ID | 000000ce |
| Windows 事件日誌（預設） | – |
| 卡巴斯基安全管理中心事件日誌（預設） | – |

## 資料庫嚴重過期

| | |
|---|---|
| 狀態 | ⓘ |
| 元件 | 系統稽核 |
| Windows 事件 ID | 207 |
| 卡巴斯基安全管理中心事件 ID | 000000cf |
| Windows 事件日誌（預設） | – |
| 卡巴斯基安全管理中心事件日誌（預設） | ✓ |

## 應用程式自動執行已停用

| | |
|---|---|
| 狀態 | ⓘ |
| 元件 | 系統稽核 |
| Windows 事件 ID | 209 |
| 卡巴斯基安全管理中心事件 ID | 000000d1 |
| Windows 事件日誌（預設） | – |
| 卡巴斯基安全管理中心事件日誌（預設） | ✓ |

## 啟動錯誤

| | |
|---|---|
| 狀態 | ⓘ |
| 元件 | 系統稽核 |
| Windows 事件 ID | 229 |
| 卡巴斯基安全管理中心事件 ID | – |
| Windows 事件日誌（預設） | ✓ |
| 卡巴斯基安全管理中心事件日誌（預設） | ✓ |

## 偵測到活動威脅。應該啟動進階解毒技術

| | |
|---|---|
| 狀態 | ⓘ |
| 元件 | 系統稽核 |
| Windows 事件 ID | 231 |
| 卡巴斯基安全管理中心事件 ID | 000000e7 |
| Windows 事件日誌（預設） | ✓ |
| 卡巴斯基安全管理中心事件日誌（預設） | ✓ |

## KSN 伺服器不可用

| | |
|---|---|
| 狀態 | ⓘ |
| 元件 | 系統稽核 |
| Windows 事件 ID | 2023 |
| 卡巴斯基安全管理中心事件 ID | 000007e7 |
| Windows 事件日誌（預設） | – |
| 卡巴斯基安全管理中心事件日誌（預設） | ✓ |

## 隔離區儲存空間不足

| | |
|---|---|
| 狀態 | ⓘ |
| 元件 | 系統稽核 |
| Windows 事件 ID | 343 |
| 卡巴斯基安全管理中心事件 ID | 00000157 |
| Windows 事件日誌（預設） | ✓ |
| 卡巴斯基安全管理中心事件日誌（預設） | ✓ |

## 物件未被從隔離區還原

| | |
|---|---|
| 狀態 | ⓘ |
| 元件 | 系統稽核 |
| Windows 事件 ID | 346 |
| 卡巴斯基安全管理中心事件 ID | 0000015a |
| Windows 事件日誌（預設） | ✓ |
| 卡巴斯基安全管理中心事件日誌（預設） | ✓ |

## 物件未被從隔離區刪除

| | |
|---|---|
| 狀態 | ⓘ |
| 元件 | 系統稽核 |
| Windows 事件 ID | 348 |
| 卡巴斯基安全管理中心事件 ID | 0000015c |
| Windows 事件日誌（預設） | ✓ |
| 卡巴斯基安全管理中心事件日誌（預設） | ✓ |

## 應用程式建立了與具有不受信任憑證的網站的連線

| | |
|---|---|
| 狀態 | ⓘ |
| 元件 | 系統稽核 |
| Windows 事件 ID | 57 |
| 卡巴斯基安全管理中心事件 ID | 00000039 |
| Windows 事件日誌（預設） | – |
| 卡巴斯基安全管理中心事件日誌（預設） | ✓ |

## 驗證加密連線失敗。網域被新增到排除項目清單

| | |
|---|---|
| 狀態 | ! |
| 元件 | 系統稽核 |
| Windows 事件 ID | 60 |
| 卡巴斯基安全管理中心事件 ID | 0000003c |
| Windows 事件日誌（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<br>Web 威脅防護<br>郵件威脅防護<br>AMSI 防護<br>主機入侵防禦<br>行為偵測<br>加密軟體防護<br>弱點利用防禦<br>惡意軟體掃描 |
| Windows 事件 ID | 302 |
| 卡巴斯基安全管理中心事件 ID | GNRL_EV_VIRUS_FOUND |
| 事件參數 | • GNRL_EA_PARAM_1 是物件的雜湊 (SHA256)。<br>• GNRL_EA_PARAM_2 是物件名稱。<br>當偵測到外部加密共用資料夾時，應用程式將顯示目標檔案的路徑。<br>• GNRL_EA_PARAM_5 是根據 Kaspersky 分類的威脅名稱，例如，EICAR-Test-File。<br>• GNRL_EA_PARAM_7 是工作階段使用者的名稱。<br>• GNRL_EA_PARAM_8 是威脅類型 (type)。<br>• GNRL_EA_PARAM_9 是被偵測到物件的其它資訊：<br>應用程式元件 (engine)。<br>威脅偵測技術 (method)。<br>卡巴斯基私人安全網路偵測到的威脅 (blacklist)：true 或者 false。<br>EDR 版本。<br>EDR 中的威脅識別符。<br>物件的 MD5 雜湊。 |
| Windows 事件日誌（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 (KSN)

| | |
|---|---|
| 狀態 | ! |
| 元件 | 檔案威脅防護<br>Web 威脅防護<br>郵件威脅防護<br>AMSI 防護<br>主機入侵防禦<br>行為偵測<br>加密軟體防護<br>弱點利用防禦<br>惡意軟體掃描 |
| Windows 事件 ID | 302 |

| | |
|---|---|
| 卡巴斯基安全管理中心事件 ID | GNRL_EV_VIRUS_FOUND_BY_KSN |
| 事件參數 | • GNRL_EA_PARAM_1 是物件的雜湊 (SHA256)。<br>• GNRL_EA_PARAM_2 是物件名稱。<br>• GNRL_EA_PARAM_5 是根據 Kaspersky 分類的威脅名稱，例如，EICAR-Test-File。<br>• GNRL_EA_PARAM_7 是工作階段使用者的名稱。<br>• GNRL_EA_PARAM_8 是威脅類型 (type)。<br>• GNRL_EA_PARAM_9 是被偵測到物件的其它資訊：<br>應用程式元件 (engine)。<br>威脅偵測技術 (method)。<br>卡巴斯基私人安全網路偵測到的威脅 (blacklist)：true 或者 false。<br>EDR 版本。<br>EDR 中的威脅識別符。<br>物件的 MD5 雜湊。 |
| Windows 事件日誌（預設） | ✓ |
| 卡巴斯基安全管理中心事件日誌（預設） | ✓ |

## 無法解毒

| | |
|---|---|
| 狀態 | ! |
| 元件 | 檔案威脅防護<br>郵件威脅防護<br>主機入侵防禦<br>行為偵測<br>加密軟體防護<br>惡意軟體掃描 |
| Windows 事件 ID | 312 |
| 卡巴斯基安全管理中心事件 ID | GNRL_EV_OBJECT_NOTCURED |
| 事件參數 | • GNRL_EA_PARAM_1 是物件的雜湊 (SHA256)。<br>• GNRL_EA_PARAM_2 是物件名稱。<br>• GNRL_EA_PARAM_5 是根據 Kaspersky 分類的威脅名稱，例如，EICAR-Test-File。<br>• GNRL_EA_PARAM_7 是工作階段使用者的名稱。<br>• GNRL_EA_PARAM_8 是威脅類型 (type)。<br>• GNRL_EA_PARAM_9 是被偵測到物件的其它資訊：<br>應用程式元件 (engine)。<br>威脅偵測技術 (method)。<br>卡巴斯基私人安全網路偵測到的威脅 (blacklist)：true 或者 false。<br>EDR 版本。<br>EDR 中的威脅識別符。<br>物件的 MD5 雜湊。 |
| Windows 事件日誌（預設） | ✓ |
| 卡巴斯基安全管理中心事件日誌（預設） | ✓ |

## 無法刪除

| | |
|---|---|
| 狀態 | ! |
| 元件 | 檔案威脅防護<br>主機入侵防禦<br>行為偵測<br>加密軟體防護<br>惡意軟體掃描 |
| Windows 事件 ID | 313 |
| 卡巴斯基安全管理中心事件 ID | 00000139 |
| Windows 事件日誌（預設） | – |
| 卡巴斯基安全管理中心事件日誌（預設） | ✓ |

## 處理錯誤

| | |
|---|---|
| 狀態 | ! |
| 元件 | 檔案威脅防護<br>Web 威脅防護<br>郵件威脅防護<br>主機入侵防禦<br>AMSI 防護<br>惡意軟體掃描 |
| Windows 事件 ID | 317 |
| 卡巴斯基安全管理中心事件 ID | 0000013d |
| Windows 事件日誌（預設） | ✓ |
| 卡巴斯基安全管理中心事件日誌（預設） | ✓ |

## 處理程序已終止

| | |
|---|---|
| 狀態 | ! |
| 元件 | 檔案威脅防護<br>主機入侵防禦<br>行為偵測<br>惡意軟體掃描 |
| Windows 事件 ID | 452 |
| 卡巴斯基安全管理中心事件 ID | 000001c4 |
| Windows 事件日誌（預設） | – |
| 卡巴斯基安全管理中心事件日誌（預設） | ✓ |

## 無法終止處理程序

| | |
|---|---|
| 狀態 | ! |
| 元件 | 檔案威脅防護<br>主機入侵防禦<br>行為偵測<br>惡意軟體掃描 |
| Windows 事件 ID | 453 |
| 卡巴斯基安全管理中心事件 ID | 000001c5 |
| Windows 事件日誌（預設） | – |
| 卡巴斯基安全管理中心事件日誌（預設） | – |

## 已封鎖危險連結

| | |
|---|---|
| 狀態 | ! |
| 元件 | Web 威脅防護 |
| Windows 事件 ID | 362 |
| 卡巴斯基安全管理中心事件 ID | GNRL_EV_VIRUS_FOUND_AND_BLOCKED |
| 事件參數 | • GNRL_EA_PARAM_2 是物件路徑。<br>• GNRL_EA_PARAM_5 是根據卡巴斯基分類的物件名稱。<br>• GNRL_EA_PARAM_7 是工作階段使用者的名稱。<br>• GNRL_EA_PARAM_8 是威脅類型（type）。<br>• GNRL_EA_PARAM_9 是被偵測到物件的其它資訊：<br>應用程式元件（engine）。<br>威脅偵測技術（method）。<br>私有 KSN 偵測到的威脅（blacklist）：true 或者 false。 |

| | |
|---|---|
| Windows 事件日誌（預設） | ✓ |
| 卡巴斯基安全管理中心事件日誌（預設） | ✓ |

## 已開啟危險連結

| | |
|---|---|
| 狀態 | ! |
| 元件 | Web 威脅防護 |
| Windows 事件 ID | 363 |
| 卡巴斯基安全管理中心事件 ID | GNRL_EV_VIRUS_FOUND_AND_REPORTED |
| 事件參數 | • GNRL_EA_PARAM_2 是物件路徑。<br>• GNRL_EA_PARAM_5 是根據卡巴斯基分類的物件名稱。<br>• GNRL_EA_PARAM_7 是工作階段使用者的名稱。<br>• GNRL_EA_PARAM_8 是威脅類型 (type)。<br>• GNRL_EA_PARAM_9 是被偵測到物件的其它資訊：<br>應用程式元件 (engine)。<br>威脅偵測技術 (method)。<br>私有 KSN 偵測到的威脅（blacklist）：true 或者 false。 |
| Windows 事件日誌（預設） | ✓ |
| 卡巴斯基安全管理中心事件日誌（預設） | ✓ |

## 偵測到之前開啟的危險連結

| | |
|---|---|
| 狀態 | ! |
| 元件 | Web 威脅防護 |
| Windows 事件 ID | 1201 |
| 卡巴斯基安全管理中心事件 ID | GNRL_EV_VIRUS_FOUND_AND_PASSED |
| 事件參數 | • GNRL_EA_PARAM_2 是物件路徑。<br>• GNRL_EA_PARAM_5 是根據卡巴斯基分類的物件名稱。<br>• GNRL_EA_PARAM_7 是工作階段使用者的名稱。<br>• GNRL_EA_PARAM_8 是威脅類型 (type)。<br>• GNRL_EA_PARAM_9 是被偵測到物件的其它資訊：<br>應用程式元件 (engine)。<br>威脅偵測技術 (method)。<br>私有 KSN 偵測到的威脅（blacklist）：true 或者 false。 |
| Windows 事件日誌（預設） | ✓ |
| 卡巴斯基安全管理中心事件日誌（預設） | ✓ |

## 處理程序操作已封鎖

| | |
|---|---|
| 狀態 | ! |
| 元件 | 自適應異常控制 |
| Windows 事件 ID | 2200 |
| 卡巴斯基安全管理中心事件 ID | GNRL_EV_ADSEC_DETECT |
| 事件參數 | • GNRL_EA_PARAM_1 是適應性異常控制規則的名稱。<br>• GNRL_EA_PARAM_2 是啟發式規則的 ID。<br>• GNRL_EA_PARAM_3 是工作階段使用者的名稱。<br>• GNRL_EA_PARAM_4 是來源處理程序。<br>• GNRL_EA_PARAM_5 是來源物件。<br>• GNRL_EA_PARAM_6 是目標處理程序。<br>• GNRL_EA_PARAM_7 是目標物件。<br>• GNRL_EA_PARAM_8 是被偵測到物件的其它資訊：<br>來源處理程序 / 物件和目標處理程序 / 物件的總和檢查碼。<br>處理程序被封鎖 (verdict_type): true 或 false。<br>使用者安全 ID (SID)。 |

| | |
|---|---|
| Windows 事件日誌（預設） | ✓ |
| 卡巴斯基安全管理中心事件日誌（預設） | ✓ |

### 鍵盤未授權

| | |
|---|---|
| 狀態 | ⓘ |
| 元件 | BadUSB 攻擊防護 |
| Windows 事件 ID | 2051 |
| 卡巴斯基安全管理中心事件 ID | 00000803 |
| Windows 事件日誌（預設） | ✓ |
| 卡巴斯基安全管理中心事件日誌（預設） | ✓ |

### AMSI 請求被封鎖

| | |
|---|---|
| 狀態 | ⓘ |
| 元件 | AMSI 防護 |
| Windows 事件 ID | 2200 |
| 卡巴斯基安全管理中心事件 ID | 00000898 |
| Windows 事件日誌（預設） | ✓ |
| 卡巴斯基安全管理中心事件日誌（預設） | ✓ |

### 網路活動已封鎖

| | |
|---|---|
| 狀態 | ⓘ |
| 元件 | 防火牆 |
| Windows 事件 ID | 602 |
| 卡巴斯基安全管理中心事件 ID | 00000329 |
| Windows 事件日誌（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 |
| Windows 事件 ID | 651 |
| 卡巴斯基安全管理中心事件 ID | GNRL_EV_ATTACK_DETECTED |
| 事件參數 | • GNRL_EA_PARAM_1 是攻擊名稱。<br>• GNRL_EA_PARAM_2 是通訊協定。<br>• GNRL_EA_PARAM_3 是作為網路攻擊來源的電腦的 IP 位址。IP 位址按照主機的位元順序指明。例如，2886729929 對 172.16.0.201。<br>• GNRL_EA_PARAM_4 是連接埠號。<br>• GNRL_EA_PARAM_5 是 IPv6 位址，例如，12B012B012B012B012B012B012B012B0。<br>• GNRL_EA_PARAM_6 是被網路攻擊針對的電腦的 IP 位址。IP 位址按照主機的位元順序指明。例如，2886729929 對 172.16.0.201。 |
| Windows 事件日誌（預設） | ✓ |
| 卡巴斯基安全管理中心事件日誌（預設） | ✓ |

## 已禁止應用程式啟動

| | |
|---|---|
| 狀態 | ⊗ |
| 元件 | 應用程式控制 |
| Windows 事件 ID | 702 |
| 卡巴斯基安全管理中心事件 ID | GNRL_EV_APPLICATION_LAUNCH_DENIED |
| 事件參數 | • GNRL_EA_PARAM_2 是工作階段使用者的名稱。<br>• GNRL_EA_PARAM_3 是手動建立的類別識別符。<br>• GNRL_EA_PARAM_4 是應用程式類別 ID。<br>• GNRL_EA_PARAM_5 是有關應用程式的數位簽章的資訊。<br>• GNRL_EA_PARAM_6 是應用程式的可執行檔（例如，chrome.exe）。<br>• GNRL_EA_PARAM_7 是可執行檔路徑。<br>• GNRL_EA_PARAM_8 是物件的雜湊 (SHA256)。<br>• GNRL_EA_PARAM_9 是使用者努力執行的應用程式的版本。 |
| Windows 事件日誌（預設） | – |
| 卡巴斯基安全管理中心事件日誌（預設） | ✓ |

## 禁止的處理程序在 Kaspersky Endpoint Security 啟動前啟動

| | |
|---|---|
| 狀態 | ⊗ |
| 元件 | 應用程式控制 |
| Windows 事件 ID | 710 |
| 卡巴斯基安全管理中心事件 ID | 000002c6 |
| Windows 事件日誌（預設） | – |
| 卡巴斯基安全管理中心事件日誌（預設） | ✓ |

## 存取被拒絕 (本機資料庫)

| | |
|---|---|
| 狀態 | ⊗ |
| 元件 | Web 控制 |
| Windows 事件 ID | 752 |
| 卡巴斯基安全管理中心事件 ID | GNRL_EV_WEB_URL_BLOCKED |
| 事件參數 | • GNRL_EA_PARAM_1 是網址。<br>• GNRL_EA_PARAM_2 是工作階段使用者的名稱。<br>• GNRL_EA_PARAM_3 是網頁控制規則的名稱。 |
| Windows 事件日誌（預設） | – |
| 卡巴斯基安全管理中心事件日誌（預設） | ✓ |

## 存取被拒絕 (KSN)

| | |
|---|---|
| 狀態 | ⊗ |
| 元件 | Web 控制 |
| Windows 事件 ID | 752 |
| 卡巴斯基安全管理中心事件 ID | GNRL_EV_WEB_URL_BLOCKED_BY_KSN |
| 事件參數 | • GNRL_EA_PARAM_1 是網址。<br>• GNRL_EA_PARAM_2 是工作階段使用者的名稱。<br>• GNRL_EA_PARAM_3 是網頁控制規則的名稱。 |

| | |
|---|---|
| Windows 事件日誌（預設） | – |
| 卡巴斯基安全管理中心事件日誌（預設） | ✓ |

## 已禁止對該裝置進行操作

| | |
|---|---|
| 狀態 | ! |
| 元件 | 裝置控制 |
| Windows 事件 ID | 802 |
| 卡巴斯基安全管理中心事件 ID | GNRL_EV_DEVCTRL_DEV_PLUG_DENIED |
| 事件參數 | • GNRL_EA_PARAM_1 是硬體 ID (HWID)。<br>• GNRL_EA_PARAM_2 是工作階段使用者的名稱。 |
| Windows 事件日誌（預設） | – |
| 卡巴斯基安全管理中心事件日誌（預設） | ✓ |

## 已封鎖網路連線

| | |
|---|---|
| 狀態 | ! |
| 元件 | 裝置控制 |
| Windows 事件 ID | 809 |
| 卡巴斯基安全管理中心事件 ID | 00000329 |
| Windows 事件日誌（預設） | – |
| 卡巴斯基安全管理中心事件日誌（預設） | ✓ |

## 更新元件錯誤

| | |
|---|---|
| 狀態 | ! |
| 元件 | 更新 |
| Windows 事件 ID | 1011 |
| 卡巴斯基安全管理中心事件 ID | 000003f3 |
| Windows 事件日誌（預設） | – |
| 卡巴斯基安全管理中心事件日誌（預設） | ✓ |

## 分發元件更新時出錯

| | |
|---|---|
| 狀態 | ! |
| 元件 | 更新 |
| Windows 事件 ID | 1012 |
| 卡巴斯基安全管理中心事件 ID | 000003f4 |
| Windows 事件日誌（預設） | – |
| 卡巴斯基安全管理中心事件日誌（預設） | – |

## 本機更新錯誤

| | |
|---|---|
| 狀態 | ! |
| 元件 | 更新 |
| Windows 事件 ID | 1014 |

| | |
|---|---|
| 卡巴斯基安全管理中心事件 ID | 000003f6 |
| Windows 事件日誌（預設） | – |
| 卡巴斯基安全管理中心事件日誌（預設） | – |

### 網路更新錯誤

| | |
|---|---|
| 狀態 | ⊗ |
| 元件 | 更新 |
| Windows 事件 ID | 1015 |
| 卡巴斯基安全管理中心事件 ID | 000003f7 |
| Windows 事件日誌（預設） | – |
| 卡巴斯基安全管理中心事件日誌（預設） | – |

### 不能同時執行兩項工作

| | |
|---|---|
| 狀態 | ⊗ |
| 元件 | 更新 |
| Windows 事件 ID | 1017 |
| 卡巴斯基安全管理中心事件 ID | 000003f9 |
| Windows 事件日誌（預設） | – |
| 卡巴斯基安全管理中心事件日誌（預設） | ✓ |

### 驗證應用程式資料庫和模組時出錯

| | |
|---|---|
| 狀態 | ⊗ |
| 元件 | 更新 |
| Windows 事件 ID | 1018 |
| 卡巴斯基安全管理中心事件 ID | 000003fa |
| Windows 事件日誌（預設） | – |
| 卡巴斯基安全管理中心事件日誌（預設） | ✓ |

### 與卡巴斯基安全管理中心互動時發生錯誤

| | |
|---|---|
| 狀態 | ⊗ |
| 元件 | 更新 |
| Windows 事件 ID | 1019 |
| 卡巴斯基安全管理中心事件 ID | 000003fb |
| Windows 事件日誌（預設） | – |
| 卡巴斯基安全管理中心事件日誌（預設） | ✓ |

### 未更新所有元件

| | |
|---|---|
| 狀態 | ⊗ |
| 元件 | 更新 |
| Windows 事件 ID | 1021 |

| | |
|---|---|
| 卡巴斯基安全管理中心事件 ID | 000003fd |
| Windows 事件日誌（預設） | – |
| 卡巴斯基安全管理中心事件日誌（預設） | ✓ |

### 成功完成更新，更新發佈失敗

| | |
|---|---|
| 狀態 | ⓘ |
| 元件 | 更新 |
| Windows 事件 ID | 1023 |
| 卡巴斯基安全管理中心事件 ID | 000003ff |
| Windows 事件日誌（預設） | – |
| 卡巴斯基安全管理中心事件日誌（預設） | – |

### 內部工作錯誤

| | |
|---|---|
| 狀態 | ⓘ |
| 元件 | 系統稽核 |
| Windows 事件 ID | 101 |
| 卡巴斯基安全管理中心事件 ID | 00000065 |
| Windows 事件日誌（預設） | – |
| 卡巴斯基安全管理中心事件日誌（預設） | – |

### 修補程式安裝失敗

| | |
|---|---|
| 狀態 | ⓘ |
| 元件 | 更新 |
| Windows 事件 ID | 2153 |
| 卡巴斯基安全管理中心事件 ID | 00000869 |
| Windows 事件日誌（預設） | – |
| 卡巴斯基安全管理中心事件日誌（預設） | ✓ |

### 修補程式回溯失敗

| | |
|---|---|
| 狀態 | ⓘ |
| 元件 | 更新 |
| Windows 事件 ID | 2156 |
| 卡巴斯基安全管理中心事件 ID | 0000086c |
| Windows 事件日誌（預設） | – |
| 卡巴斯基安全管理中心事件日誌（預設） | ✓ |

### 套用檔案加密/解密規則時出錯

| | |
|---|---|
| 狀態 | ⓘ |
| 元件 | 資料加密 |
| Windows 事件 ID | 904 |

| | |
|---|---|
| 卡巴斯基安全管理中心事件 ID | 00000388 |
| Windows 事件日誌（預設） | ✓ |
| 卡巴斯基安全管理中心事件日誌（預設） | ✓ |

### 檔案加密/解密錯誤

| | |
|---|---|
| 狀態 | ! |
| 元件 | 資料加密 |
| Windows 事件 ID | 912 |
| 卡巴斯基安全管理中心事件 ID | GNRL_EV_ENCRYPTION_ERROR |
| 事件參數 | • GNRL_EA_PARAM_1 是檔案路徑。<br>• GNRL_EA_PARAM_2 是錯誤原因。<br>• GNRL_EA_PARAM_3 是裝置類型。 |
| Windows 事件日誌（預設） | ✓ |
| 卡巴斯基安全管理中心事件日誌（預設） | ✓ |

### 存取檔案被封鎖

| | |
|---|---|
| 狀態 | ! |
| 元件 | 資料加密 |
| Windows 事件 ID | 940 |
| 卡巴斯基安全管理中心事件 ID | GNRL_EV_ENCRYPTION_DATAACCESS_VIOLATION |
| 事件參數 | • GNRL_EA_PARAM_1 是目標物件。<br>• GNRL_EA_PARAM_2 是工作階段使用者的名稱。<br>• GNRL_EA_PARAM_3 是正在試圖存取檔案的應用程式的可執行檔名稱（例如，chrome.exe）。 |
| Windows 事件日誌（預設） | ✓ |
| 卡巴斯基安全管理中心事件日誌（預設） | – |

### 啟用攜帶模式時出錯

| | |
|---|---|
| 狀態 | ! |
| 元件 | 資料加密 |
| Windows 事件 ID | 951 |
| 卡巴斯基安全管理中心事件 ID | 000003b7 |
| Windows 事件日誌（預設） | ✓ |
| 卡巴斯基安全管理中心事件日誌（預設） | ✓ |

### 停用攜帶模式時出錯

| | |
|---|---|
| 狀態 | ! |
| 元件 | 資料加密 |
| Windows 事件 ID | 953 |
| 卡巴斯基安全管理中心事件 ID | 000003b9 |
| Windows 事件日誌（預設） | ✓ |
| 卡巴斯基安全管理中心事件日誌（預設） | ✓ |

### 建立加密檔案時出錯

| | |
|---|---|
| 狀態 | ⓘ |
| 元件 | 資料加密 |
| Windows 事件 ID | 931 |
| 卡巴斯基安全管理中心事件 ID | 000003a3 |
| Windows 事件日誌（預設） | ✓ |
| 卡巴斯基安全管理中心事件日誌（預設） | ✓ |

### 裝置加密/解密時出錯

| | |
|---|---|
| 狀態 | ⓘ |
| 元件 | 資料加密 |
| Windows 事件 ID | 1305 |
| 卡巴斯基安全管理中心事件 ID | 00000519 |
| Windows 事件日誌（預設） | ✓ |
| 卡巴斯基安全管理中心事件日誌（預設） | ✓ |

### 無法載入加密模組

| | |
|---|---|
| 狀態 | ⓘ |
| 元件 | 資料加密 |
| Windows 事件 ID | 1311 |
| 卡巴斯基安全管理中心事件 ID | 0000051f |
| Windows 事件日誌（預設） | ✓ |
| 卡巴斯基安全管理中心事件日誌（預設） | ✓ |

### 用於管理身分驗證代理帳戶的工作最後發生錯誤

| | |
|---|---|
| 狀態 | ⓘ |
| 元件 | 資料加密 |
| Windows 事件 ID | 1340 |
| 卡巴斯基安全管理中心事件 ID | 0000053c |
| Windows 事件日誌（預設） | ✓ |
| 卡巴斯基安全管理中心事件日誌（預設） | ✓ |

### 無法套用政策

| | |
|---|---|
| 狀態 | ⓘ |
| 元件 | 系統稽核 |
| Windows 事件 ID | 1312 |
| 卡巴斯基安全管理中心事件 ID | 00000520 |
| Windows 事件日誌（預設） | – |
| 卡巴斯基安全管理中心事件日誌（預設） | ✓ |

## FDE 升級失敗

| | |
|---|---|
| 狀態 | ⓘ |
| 元件 | 資料加密 |
| Windows 事件 ID | 1342 |
| 卡巴斯基安全管理中心事件 ID | 0000053e |
| Windows 事件日誌（預設） | ✓ |
| 卡巴斯基安全管理中心事件日誌（預設） | ✓ |

## FDE 升級回溯失敗(要瞭解更多資訊，請參閱 Kaspersky Endpoint Security for Windows 線上說明)

| | |
|---|---|
| 狀態 | ⓘ |
| 元件 | 資料加密 |
| Windows 事件 ID | 1344 |
| 卡巴斯基安全管理中心事件 ID | 00000540 |
| Windows 事件日誌（預設） | ✓ |
| 卡巴斯基安全管理中心事件日誌（預設） | ✓ |

## Kaspersky Anti Targeted Attack Platform 伺服器不可用

| | |
|---|---|
| 狀態 | ⓘ |
| 元件 | Endpoint Sensor |
| Windows 事件 ID | 2100 |
| 卡巴斯基安全管理中心事件 ID | 00000834 |
| Windows 事件日誌（預設） | – |
| 卡巴斯基安全管理中心事件日誌（預設） | ✓ |

## 刪除物件失敗

| | |
|---|---|
| 狀態 | ⓘ |
| 元件 | Sandbox |
| Windows 事件 ID | 2252 |
| 卡巴斯基安全管理中心事件 ID | 000008cc |
| Windows 事件日誌（預設） | – |
| 卡巴斯基安全管理中心事件日誌（預設） | ✓ |

## 物件未隔離 (Sandbox)

| | |
|---|---|
| 狀態 | ⓘ |
| 元件 | Sandbox |
| Windows 事件 ID | 2603 |
| 卡巴斯基安全管理中心事件 ID | 00000a2b |
| Windows 事件日誌（預設） | ✓ |
| 卡巴斯基安全管理中心事件日誌（預設） | ✓ |

### 發生內部錯誤

| | |
|---|---|
| 狀態 | ! |
| 元件 | Sandbox |
| Windows 事件 ID | 2607 |
| 卡巴斯基安全管理中心事件 ID | 00000a2f |
| Windows 事件日誌（預設） | ✓ |
| 卡巴斯基安全管理中心事件日誌（預設） | ✓ |

### 無效的 Sandbox 伺服器憑證

| | |
|---|---|
| 狀態 | ! |
| 元件 | Sandbox |
| Windows 事件 ID | 2613 |
| 卡巴斯基安全管理中心事件 ID | 00000a35 |
| Windows 事件日誌（預設） | ✓ |
| 卡巴斯基安全管理中心事件日誌（預設） | ✓ |

### Sandbox 節點無法使用

| | |
|---|---|
| 狀態 | ! |
| 元件 | Sandbox |
| Windows 事件 ID | 2614 |
| 卡巴斯基安全管理中心事件 ID | 00000a36 |
| Windows 事件日誌（預設） | ✓ |
| 卡巴斯基安全管理中心事件日誌（預設） | ✓ |

### 未能處理 Sandbox 中的物件

| | |
|---|---|
| 狀態 | ! |
| 元件 | Sandbox |
| Windows 事件 ID | 2617 |
| 卡巴斯基安全管理中心事件 ID | 00000a39 |
| Windows 事件日誌（預設） | ✓ |
| 卡巴斯基安全管理中心事件日誌（預設） | ✓ |

### 已超過 Sandbox 的最大負載

| | |
|---|---|
| 狀態 | ! |
| 元件 | Sandbox |
| Windows 事件 ID | 2618 |
| 卡巴斯基安全管理中心事件 ID | 00000a3a |
| Windows 事件日誌（預設） | ✓ |
| 卡巴斯基安全管理中心事件日誌（預設） | – |

## 發現 IOC

| | |
|---|---|
| 狀態 | ! |
| 元件 | Endpoint Detection and Response |
| Windows 事件 ID | 2651 |
| 卡巴斯基安全管理中心事件 ID | 00000a5b |
| Windows 事件日誌（預設） | ✓ |
| 卡巴斯基安全管理中心事件日誌（預設） | ✓ |

## Sandbox 產品授權驗證失敗

| | |
|---|---|
| 狀態 | ! |
| 元件 | Sandbox |
| Windows 事件 ID | 2620 |
| 卡巴斯基安全管理中心事件 ID | 00000a3c |
| Windows 事件日誌（預設） | ✓ |
| 卡巴斯基安全管理中心事件日誌（預設） | ✓ |

## 使用者未能將掃描工作提交到 Sandbox

| | |
|---|---|
| 狀態 | ! |
| 元件 | Sandbox |
| Windows 事件 ID | 2623 |
| 卡巴斯基安全管理中心事件 ID | 00000a3e |
| Windows 事件日誌（預設） | ✓ |
| 卡巴斯基安全管理中心事件日誌（預設） | ✓ |

## 建立 Sandbox 工作時出錯

| | |
|---|---|
| 狀態 | ! |
| 元件 | Sandbox |
| Windows 事件 ID | 2621 |
| 卡巴斯基安全管理中心事件 ID | 00000a3d |
| Windows 事件日誌（預設） | ✓ |
| 卡巴斯基安全管理中心事件日誌（預設） | ✓ |

## 物件啟動被封鎖

| | |
|---|---|
| 狀態 | ! |
| 元件 | Endpoint Detection and Response |
| Windows 事件 ID | 2553 |
| 卡巴斯基安全管理中心事件 ID | 000009f9 |
| Windows 事件日誌（預設） | ✓ |
| 卡巴斯基安全管理中心事件日誌（預設） | ✓ |

### 處理程序啟動被封鎖

| | |
|---|---|
| 狀態 | ! |
| 元件 | Endpoint Detection and Response |
| Windows 事件 ID | 2551 |
| 卡巴斯基安全管理中心事件 ID | 000009f7 |
| Windows 事件日誌（預設） | ✓ |
| 卡巴斯基安全管理中心事件日誌（預設） | ✓ |

### 指令碼執行已被封鎖

| | |
|---|---|
| 狀態 | ! |
| 元件 | Endpoint Detection and Response |
| Windows 事件 ID | 2559 |
| 卡巴斯基安全管理中心事件 ID | – |
| Windows 事件日誌（預設） | ✓ |
| 卡巴斯基安全管理中心事件日誌（預設） | ✓ |

### 物件未隔離 (Endpoint Detection and Response)

| | |
|---|---|
| 狀態 | ! |
| 元件 | Endpoint Detection and Response |
| Windows 事件 ID | 2556 |
| 卡巴斯基安全管理中心事件 ID | 000009fc |
| Windows 事件日誌（預設） | ✓ |
| 卡巴斯基安全管理中心事件日誌（預設） | ✓ |

### 處理程序啟動未被封鎖

| | |
|---|---|
| 狀態 | ! |
| 元件 | Endpoint Detection and Response |
| Windows 事件 ID | 2561 |
| 卡巴斯基安全管理中心事件 ID | 00000a01 |
| Windows 事件日誌（預設） | ✓ |
| 卡巴斯基安全管理中心事件日誌（預設） | ✓ |

### 物件未被封鎖

| | |
|---|---|
| 狀態 | ! |
| 元件 | Endpoint Detection and Response |
| Windows 事件 ID | 2562 |
| 卡巴斯基安全管理中心事件 ID | 00000a02 |
| Windows 事件日誌（預設） | ✓ |
| 卡巴斯基安全管理中心事件日誌（預設） | ✓ |

### 指令碼執行未被封鎖

| | |
|---|---|
| 狀態 | ! |
| 元件 | Endpoint Detection and Response |
| Windows 事件 ID | 2563 |
| 卡巴斯基安全管理中心事件 ID | 00000a03 |
| Windows 事件日誌（預設） | ✓ |
| 卡巴斯基安全管理中心事件日誌（預設） | ✓ |

### 變更應用程式元件時出錯

| | |
|---|---|
| 狀態 | ! |
| 元件 | 系統稽核 |
| Windows 事件 ID | 1401 |
| 卡巴斯基安全管理中心事件 ID | 00000579 |
| Windows 事件日誌（預設） | – |
| 卡巴斯基安全管理中心事件日誌（預設） | ✓ |

### 系統中存在疑似暴力破解攻擊模式

| | |
|---|---|
| 狀態 | ! |
| 元件 | 記錄審查 |
| Windows 事件 ID | 2800 |
| 卡巴斯基安全管理中心事件 ID | 00000af0 |
| Windows 事件日誌（預設） | ✓ |
| 卡巴斯基安全管理中心事件日誌（預設） | ✓ |

### 存在可能的 Windows 事件記錄濫用模式

| | |
|---|---|
| 狀態 | ! |
| 元件 | 記錄檢查 |
| Windows 事件 ID | 2801 |
| 卡巴斯基安全管理中心事件 ID | 00000af1 |
| Windows 事件日誌（預設） | ✓ |
| 卡巴斯基安全管理中心事件日誌（預設） | ✓ |

### 代替安裝的新服務偵測到了非典型操作

| | |
|---|---|
| 狀態 | ! |
| 元件 | 記錄檢查 |
| Windows 事件 ID | 2802 |
| 卡巴斯基安全管理中心事件 ID | 00000af2 |
| Windows 事件日誌（預設） | ✓ |
| 卡巴斯基安全管理中心事件日誌（預設） | ✓ |

### 偵測到使用明顯憑據的非典型登入名稱

| | |
|---|---|
| 狀態 | ⓘ |
| 元件 | 記錄審查 |
| Windows 事件 ID | 2803 |
| 卡巴斯基安全管理中心事件 ID | 00000af3 |
| Windows 事件日誌（預設） | ✓ |
| 卡巴斯基安全管理中心事件日誌（預設） | ✓ |

### 系統中存在疑似 Kerberos 偽造 PAC (MS14-068) 攻擊模式

| | |
|---|---|
| 狀態 | ⓘ |
| 元件 | 記錄審查 |
| Windows 事件 ID | 2804 |
| 卡巴斯基安全管理中心事件 ID | 00000af4 |
| Windows 事件日誌（預設） | ✓ |
| 卡巴斯基安全管理中心事件日誌（預設） | ✓ |

### 在有權限的內建管理員群組中偵測到可疑變更

| | |
|---|---|
| 狀態 | ⓘ |
| 元件 | 記錄檢查 |
| Windows 事件 ID | 2805 |
| 卡巴斯基安全管理中心事件 ID | 00000af5 |
| Windows 事件日誌（預設） | ✓ |
| 卡巴斯基安全管理中心事件日誌（預設） | ✓ |

### 網路登入工作階段中偵測到一個非典型活動

| | |
|---|---|
| 狀態 | ⓘ |
| 元件 | 記錄審查 |
| Windows 事件 ID | 2806 |
| 卡巴斯基安全管理中心事件 ID | 00000af6 |
| Windows 事件日誌（預設） | ✓ |
| 卡巴斯基安全管理中心事件日誌（預設） | ✓ |

### 記錄審查規則被觸發

| | |
|---|---|
| 狀態 | ⓘ |
| 元件 | 記錄審查 |
| Windows 事件 ID | 2807 |
| 卡巴斯基安全管理中心事件 ID | 00000af7 |
| Windows 事件日誌（預設） | ✓ |
| 卡巴斯基安全管理中心事件日誌（預設） | ✓ |

### 非典型事件發生太頻繁。事件彙總啟動

| | |
|---|---|
| 狀態 | ⓘ |
| 元件 | 記錄檢查 |
| Windows 事件 ID | 2808 |
| 卡巴斯基安全管理中心事件 ID | 00000af8 |
| Windows 事件日誌（預設） | ✓ |
| 卡巴斯基安全管理中心事件日誌（預設） | ✓ |

### 彙總期間的非典型事件報告

| | |
|---|---|
| 狀態 | ⓘ |
| 元件 | 記錄檢查 |
| Windows 事件 ID | 2809 |
| 卡巴斯基安全管理中心事件 ID | 00000af9 |
| Windows 事件日誌（預設） | ✓ |
| 卡巴斯基安全管理中心事件日誌（預設） | ✓ |

### 連線到 EDR Expert 伺服器時發生錯誤

| | |
|---|---|
| 狀態 | ⓘ |
| 元件 | Endpoint Detection and Response Expert (on-premise) |
| Windows 事件 ID | 2850 |
| 卡巴斯基安全管理中心事件 ID | 00000b22 |
| Windows 事件日誌（預設） | ✓ |
| 卡巴斯基安全管理中心事件日誌（預設） | ✓ |

### 無效的 EDR Expert 伺服器憑證

| | |
|---|---|
| 狀態 | ⓘ |
| 元件 | Endpoint Detection and Response Expert (on-premise) |
| Windows 事件 ID | 2851 |
| 卡巴斯基安全管理中心事件 ID | 00000b23 |
| Windows 事件日誌（預設） | ✓ |
| 卡巴斯基安全管理中心事件日誌（預設） | ✓ |

### 無效的 EDR Expert 伺服器上的代理的憑證

| | |
|---|---|
| 狀態 | ⓘ |
| 元件 | Endpoint Detection and Response Expert (on-premise) |
| Windows 事件 ID | 2852 |
| 卡巴斯基安全管理中心事件 ID | 00000b24 |
| Windows 事件日誌（預設） | ✓ |
| 卡巴斯基安全管理中心事件日誌（預設） | ✓ |

## 連線到 EDR Expert 回應伺服器時發生錯誤

| | |
|---|---|
| 狀態 | ! |
| 元件 | Endpoint Detection and Response Expert (on-premise) |
| Windows 事件 ID | 2858 |
| 卡巴斯基安全管理中心事件 ID | 00000b22 |
| Windows 事件日誌（預設） | ✓ |
| 卡巴斯基安全管理中心事件日誌（預設） | ✓ |

## EDR Expert 回應伺服器的憑證無效

| | |
|---|---|
| 狀態 | ! |
| 元件 | Endpoint Detection and Response Expert (on-premise) |
| Windows 事件 ID | 2859 |
| 卡巴斯基安全管理中心事件 ID | 00000b23 |
| Windows 事件日誌（預設） | ✓ |
| 卡巴斯基安全管理中心事件日誌（預設） | ✓ |

## EDR Expert 回應伺服器上的代理憑證無效

| | |
|---|---|
| 狀態 | ! |
| 元件 | Endpoint Detection and Response Expert (on-premise) |
| Windows 事件 ID | 2860 |
| 卡巴斯基安全管理中心事件 ID | 00000b24 |
| Windows 事件日誌（預設） | ✓ |
| 卡巴斯基安全管理中心事件日誌（預設） | ✓ |

## EDR Expert 遙測資料收集伺服器連線錯誤

| | |
|---|---|
| 狀態 | ! |
| 元件 | Endpoint Detection and Response Expert (on-premise) |
| Windows 事件 ID | 2854 |
| 卡巴斯基安全管理中心事件 ID | 00000b22 |
| Windows 事件日誌（預設） | ✓ |
| 卡巴斯基安全管理中心事件日誌（預設） | ✓ |

## EDR Expert 遙測資料收集伺服器的憑證無效

| | |
|---|---|
| 狀態 | ! |
| 元件 | Endpoint Detection and Response Expert (on-premise) |
| Windows 事件 ID | 2855 |
| 卡巴斯基安全管理中心事件 ID | 00000b23 |
| Windows 事件日誌（預設） | ✓ |
| 卡巴斯基安全管理中心事件日誌（預設） | ✓ |

### EDR Expert 遙測資料收集伺服器上的代理的憑證無效

| | |
|---|---|
| 狀態 | ! |
| 元件 | Endpoint Detection and Response Expert (on-premise) |
| Windows 事件 ID | 2856 |
| 卡巴斯基安全管理中心事件 ID | 00000b24 |
| Windows 事件日誌（預設） | ✓ |
| 卡巴斯基安全管理中心事件日誌（預設） | ✓ |

### 連線到 NDR 伺服器錯誤

| | |
|---|---|
| 狀態 | ! |
| 元件 | Network Detection and Response (KATA) |
| Windows 事件 ID | 3080 |
| 卡巴斯基安全管理中心事件 ID | 00000c08 |
| Windows 事件日誌（預設） | ✓ |
| 卡巴斯基安全管理中心事件日誌（預設） | ✓ |

### NDR 伺服器上的憑證無效

| | |
|---|---|
| 狀態 | ! |
| 元件 | Network Detection and Response (KATA) |
| Windows 事件 ID | 3081 |
| 卡巴斯基安全管理中心事件 ID | 00000c09 |
| Windows 事件日誌（預設） | ✓ |
| 卡巴斯基安全管理中心事件日誌（預設） | ✓ |

### NDR 伺服器上的代理憑證無效

| | |
|---|---|
| 狀態 | ! |
| 元件 | Network Detection and Response (KATA) |
| Windows 事件 ID | 3082 |
| 卡巴斯基安全管理中心事件 ID | 00000c0a |
| Windows 事件日誌（預設） | ✓ |
| 卡巴斯基安全管理中心事件日誌（預設） | ✓ |

### 您的裝置已連線至不受信任的管理伺服器。請聯絡管理員。

| | |
|---|---|
| 狀態 | ! |
| 元件 | 管理伺服器連線防護 |
| Windows 事件 ID | 3301 |
| 卡巴斯基安全管理中心事件 ID | 00000ce5 |
| Windows 事件日誌（預設） | – |
| 卡巴斯基安全管理中心事件日誌（預設） | ✓ |

### 偵測到對檔案或資料夾的變更

| | |
|---|---|
| 狀態 | ⓘ / ⚠ / ⓔ |
| 元件 | 系統完整性監控 |
| Windows 事件 ID | 2950 |
| 卡巴斯基安全管理中心事件 ID | 00000b86 |
| Windows 事件日誌（預設） | – |
| 卡巴斯基安全管理中心事件日誌（預設） | ✓ |

若要配置此事件的保留期，請前往政策的 **事件組態** 部分並設定一般系統完整性監控事件的保留期 – *偵測到對檔案或資料夾的變更*。

### 物件變更頻繁。事件彙總已啟動

| | |
|---|---|
| 狀態 | ⓘ / ⚠ / ⓔ |
| 元件 | 系統完整性監控 |
| Windows 事件 ID | 2955 |
| 卡巴斯基安全管理中心事件 ID | 00000b8b |
| Windows 事件日誌（預設） | – |
| 卡巴斯基安全管理中心事件日誌（預設） | ✓ |

### 彙總期間的物件修改報告

| | |
|---|---|
| 狀態 | ⓘ / ⚠ / ⓔ |
| 元件 | 系統完整性監控 |
| Windows 事件 ID | 2956 |
| 卡巴斯基安全管理中心事件 ID | 00000b8c |
| Windows 事件日誌（預設） | – |
| 卡巴斯基安全管理中心事件日誌（預設） | ✓ |

若要配置此事件的保留期，請前往政策的 **事件組態** 部分並設定一般系統完整性監控事件的保留期 – *偵測到對檔案或資料夾的變更*。

### 監控範圍包括不正確的物件

| | |
|---|---|
| 狀態 | ⓔ |
| 元件 | 系統完整性監控 |
| Windows 事件 ID | 2953 |
| 卡巴斯基安全管理中心事件 ID | 00000b89 |
| Windows 事件日誌（預設） | – |
| 卡巴斯基安全管理中心事件日誌（預設） | ✓ |

### 偵測到登錄檔變更

| | |
|---|---|
| 狀態 | ⓘ / ⚠ / ⓔ |
| 元件 | 系統完整性監控 |
| Windows 事件 ID | 2951 |

| | |
|---|---|
| 卡巴斯基安全管理中心事件 ID | 00000b87 |
| Windows 事件日誌（預設） | – |
| 卡巴斯基安全管理中心事件日誌（預設） | ✓ |

若要配置此事件的保留期，請前往政策的 **事件組態** 部分並設定一般系統完整性監控事件的保留期 – *偵測到對檔案或資料夾的變更*。

### 偵測到裝置連線 / 連線中斷

| | |
|---|---|
| 狀態 | ⓘ / ⚠ / ! |
| 元件 | 系統完整性監控 |
| Windows 事件 ID | 2952 |
| 卡巴斯基安全管理中心事件 ID | 00000b88 |
| Windows 事件日誌（預設） | – |
| 卡巴斯基安全管理中心事件日誌（預設） | ✓ |

若要配置此事件的保留期，請前往政策的 **事件組態** 部分並設定一般系統完整性監控事件的保留期 – *偵測到對檔案或資料夾的變更*。

### 監控範圍包括不正確的物件

| | |
|---|---|
| 狀態 | ⓘ / ⚠ / ! |
| 元件 | 系統完整性監控 |
| Windows 事件 ID | 2903 |
| 卡巴斯基安全管理中心事件 ID | 00000b89 |
| Windows 事件日誌（預設） | – |
| 卡巴斯基安全管理中心事件日誌（預設） | ✓ |

若要配置此事件的保留期，請前往政策的 **事件組態** 部分並設定一般系統完整性監控事件的保留期 – *偵測到對檔案或資料夾的變更*。

### 嘗試對物件進行受限制操作的次數太多。事件匯總已啟動

| | |
|---|---|
| 狀態 | ! |
| 元件 | 系統完整性監控 |
| Windows 事件 ID | 2963 |
| 卡巴斯基安全管理中心事件 ID | 00000b93 |
| Windows 事件日誌（預設） | – |
| 卡巴斯基安全管理中心事件日誌（預設） | ✓ |

### 對監控範圍中檔案的操作被封鎖

| | |
|---|---|
| 狀態 | ! |
| 元件 | 系統完整性監控 |
| Windows 事件 ID | 2959 |
| 卡巴斯基安全管理中心事件 ID | 00000b8f |

| | |
|---|---|
| Windows 事件日誌（預設） | – |
| 卡巴斯基安全管理中心事件日誌（預設） | ✓ |

若要配置此事件的保留期，請前往政策的 **事件組態** 部分並設定一般系統完整性監控事件的保留期 – *偵測到對檔案或資料夾的變更*。

### 已封鎖登錄修改

| | |
|---|---|
| 狀態 | ⚠ |
| 元件 | 系統完整性監控 |
| Windows 事件 ID | 2960 |
| 卡巴斯基安全管理中心事件 ID | 00000b90 |
| Windows 事件日誌（預設） | – |
| 卡巴斯基安全管理中心事件日誌（預設） | ✓ |

若要配置此事件的保留期，請前往政策的 **事件組態** 部分並設定一般系統完整性監控事件的保留期 – *偵測到對檔案或資料夾的變更*。

### 處理錯誤

| | |
|---|---|
| 狀態 | ⚠ |
| 元件 | 系統完整性監控 |
| Windows 事件 ID | 2954 |
| 卡巴斯基安全管理中心事件 ID | 00000b8a |
| Windows 事件日誌（預設） | – |
| 卡巴斯基安全管理中心事件日誌（預設） | ✓ |

### 系統完整性監控：已為沒有匹配安全識別碼 (SID) 的使用者帳戶停用規則觸發

| | |
|---|---|
| 狀態 | ⚠ |
| 元件 | 系統完整性監控 |
| Windows 事件 ID | 2964 |
| 卡巴斯基安全管理中心事件 ID | 00000b94 |
| Windows 事件日誌（預設） | – |
| 卡巴斯基安全管理中心事件日誌（預設） | ✓ |

### 應用程式控制：已為沒有匹配安全識別碼 (SID) 的使用者帳戶停用規則觸發

| | |
|---|---|
| 狀態 | ⚠ |
| 元件 | 應用程式控制 |
| Windows 事件 ID | 711 |
| 卡巴斯基安全管理中心事件 ID | 000002c7 |
| Windows 事件日誌（預設） | – |
| 卡巴斯基安全管理中心事件日誌（預設） | ✓ |

### 裝置控制：已為沒有匹配安全識別碼 (SID) 的使用者帳戶停用規則觸發

| | |
|---|---|
| 狀態 | ⚠ |
| 元件 | 裝置控制 |
| Windows 事件 ID | 810 |
| 卡巴斯基安全管理中心事件 ID | 0000032a |
| Windows 事件日誌（預設） | – |
| 卡巴斯基安全管理中心事件日誌（預設） | ✓ |

### Web 控制：已為沒有匹配安全識別碼 (SID) 的使用者帳戶停用規則觸發

| | |
|---|---|
| 狀態 | ⚠ |
| 元件 | Web 控制 |
| Windows 事件 ID | 757 |
| 卡巴斯基安全管理中心事件 ID | 000002f5 |
| Windows 事件日誌（預設） | – |
| 卡巴斯基安全管理中心事件日誌（預設） | ✓ |

### 自適應異常控制：已為沒有匹配安全識別碼 (SID) 的使用者帳戶停用規則觸發

| | |
|---|---|
| 狀態 | ⚠ |
| 元件 | 自適應異常控制 |
| Windows 事件 ID | 504 |
| 卡巴斯基安全管理中心事件 ID | 000001f8 |
| Windows 事件日誌（預設） | – |
| 卡巴斯基安全管理中心事件日誌（預設） | ✓ |

### 記錄審查：已為沒有匹配安全識別碼 (SID) 的使用者帳戶停用規則觸發

| | |
|---|---|
| 狀態 | ⚠ |
| 元件 | 記錄審查 |
| Windows 事件 ID | 2810 |
| 卡巴斯基安全管理中心事件 ID | 00000afa |
| Windows 事件日誌（預設） | – |
| 卡巴斯基安全管理中心事件日誌（預設） | ✓ |

### 無法連線到 Integration Server 超過 6 小時。請檢查 Integration Server 狀態和網路設定。

| | |
|---|---|
| 狀態 | ⚠ |
| 元件 | Light Agent |
| Windows 事件 ID | 3103 |
| 卡巴斯基安全管理中心事件 ID | 00000c1f |
| Windows 事件日誌（預設） | – |
| 卡巴斯基安全管理中心事件日誌（預設） | ✓ |

### SVM 不可用

| | |
|---|---|
| 狀態 | ! |
| 元件 | Light Agent |
| Windows 事件 ID | 3151 |
| 卡巴斯基安全管理中心事件 ID | 00000c4f |
| Windows 事件日誌（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。進階解毒應該在虛擬機範本上啟動

| | |
|---|---|
| 狀態 | ! |
| 元件 | Light Agent |
| Windows 事件 ID | 3182 |
| 卡巴斯基安全管理中心事件 ID | 00000c6e |
| Windows 事件日誌（預設） | – |
| 卡巴斯基安全管理中心事件日誌（預設） | ✓ |

### 透過棄用協定建立的網路連線被封鎖

| | |
|---|---|
| 狀態 | ! |
| 元件 | 防護 |
| Windows 事件 ID | 75 |
| 卡巴斯基安全管理中心事件 ID | 0000004b |
| Windows 事件日誌（預設） | – |
| 卡巴斯基安全管理中心事件日誌（預設） | ✓ |

### KUMA 伺服器連線錯誤

| | |
|---|---|
| 狀態 | ! |
| 元件 | KUMA 整合 |
| Windows 事件 ID | 2854 |
| 卡巴斯基安全管理中心事件 ID | 00000b26 |
| Windows 事件日誌（預設） | – |
| 卡巴斯基安全管理中心事件日誌（預設） | ✓ |

### KUMA 伺服器上的憑證無效

| | |
|---|---|
| 狀態 | ! |
| 元件 | KUMA 整合 |
| Windows 事件 ID | 2855 |
| 卡巴斯基安全管理中心事件 ID | 00000b27 |
| Windows 事件日誌（預設） | – |
| 卡巴斯基安全管理中心事件日誌（預設） | ✓ |

### KUMA 伺服器上的代理憑證無效

| | |
|---|---|
| 狀態 | ⓘ |
| 元件 | KUMA 整合 |
| Windows 事件 ID | 2856 |
| 卡巴斯基安全管理中心事件 ID | 00000b28 |
| Windows 事件日誌（預設） | – |
| 卡巴斯基安全管理中心事件日誌（預設） | ✓ |

# 功能失敗

### 無法執行工作

| | |
|---|---|
| 狀態 | ⓘ |
| 元件 | 系統稽核 |
| Windows 事件 ID | 212 |
| 卡巴斯基安全管理中心事件 ID | 000000d4 |
| Windows 事件日誌（預設） | – |
| 卡巴斯基安全管理中心事件日誌（預設） | ✓ |

### 工作設定無效，未套用設定

| | |
|---|---|
| 狀態 | ⓘ |
| 元件 | 系統稽核 |
| Windows 事件 ID | 707 |
| 卡巴斯基安全管理中心事件 ID | 000002c3 |
| Windows 事件日誌（預設） | – |
| 卡巴斯基安全管理中心事件日誌（預設） | ✓ |

# 警告

### 應用程式在先前工作階段中崩潰

| | |
|---|---|
| 狀態 | ⚠ |
| 元件 | 系統稽核 |
| Windows 事件 ID | 237 |
| 卡巴斯基安全管理中心事件 ID | – |
| Windows 事件日誌（預設） | ✓ |
| 卡巴斯基安全管理中心事件日誌（預設） | – |

### 產品授權即將到期

| | |
|---|---|
| 狀態 | ⚠ |
| 元件 | 系統稽核 |

| | |
|---|---|
| Windows 事件 ID | 204 |
| 卡巴斯基安全管理中心事件 ID | 000000cc |
| Windows 事件日誌（預設） | – |
| 卡巴斯基安全管理中心事件日誌（預設） | ✓ |

### 資料庫已過期

| | |
|---|---|
| 狀態 | ⚠ |
| 元件 | 系統稽核 |
| Windows 事件 ID | 208 |
| 卡巴斯基安全管理中心事件 ID | 000000d0 |
| Windows 事件日誌（預設） | ✓ |
| 卡巴斯基安全管理中心事件日誌（預設） | ✓ |

### 自動更新已停用

| | |
|---|---|
| 狀態 | ⚠ |
| 元件 | 系統稽核 |
| Windows 事件 ID | 210 |
| 卡巴斯基安全管理中心事件 ID | 000000d2 |
| Windows 事件日誌（預設） | – |
| 卡巴斯基安全管理中心事件日誌（預設） | ✓ |

### 自我防護被停用

| | |
|---|---|
| 狀態 | ⚠ |
| 元件 | 系統稽核 |
| Windows 事件 ID | 211 |
| 卡巴斯基安全管理中心事件 ID | 000000d3 |
| Windows 事件日誌（預設） | – |
| 卡巴斯基安全管理中心事件日誌（預設） | ✓ |

### 防護元件被停用

| | |
|---|---|
| 狀態 | ⚠ |
| 元件 | 系統稽核 |
| Windows 事件 ID | 214 |
| 卡巴斯基安全管理中心事件 ID | 000000d6 |
| Windows 事件日誌（預設） | – |
| 卡巴斯基安全管理中心事件日誌（預設） | ✓ |

### 電腦正在安全模式下執行

| | |
|---|---|
| 狀態 | ⚠ |
| 元件 | 系統稽核 |

| | |
|---|---|
| Windows 事件 ID | 215 |
| 卡巴斯基安全管理中心事件 ID | 000000d7 |
| Windows 事件日誌（預設） | – |
| 卡巴斯基安全管理中心事件日誌（預設） | – |

### 存在未處理的檔案

| | |
|---|---|
| 狀態 | ⚠ |
| 元件 | 系統稽核 |
| Windows 事件 ID | 216 |
| 卡巴斯基安全管理中心事件 ID | 000000d8 |
| Windows 事件日誌（預設） | – |
| 卡巴斯基安全管理中心事件日誌（預設） | ✓ |

### 群組政策已套用

| | |
|---|---|
| 狀態 | ⚠ |
| 元件 | 系統稽核 |
| Windows 事件 ID | 219 |
| 卡巴斯基安全管理中心事件 ID | 000000db |
| Windows 事件日誌（預設） | ✓ |
| 卡巴斯基安全管理中心事件日誌（預設） | ✓ |

### 工作已停止

| | |
|---|---|
| 狀態 | ⚠ |
| 元件 | 系統稽核 |
| Windows 事件 ID | 222 |
| 卡巴斯基安全管理中心事件 ID | 000000de |
| Windows 事件日誌（預設） | – |
| 卡巴斯基安全管理中心事件日誌（預設） | ✓ |

### 結束並重新開啟應用程式以完成更新

| | |
|---|---|
| 狀態 | ⚠ |
| 元件 | 系統稽核 |
| Windows 事件 ID | 224 |
| 卡巴斯基安全管理中心事件 ID | 0000057b |
| Windows 事件日誌（預設） | – |
| 卡巴斯基安全管理中心事件日誌（預設） | ✓ |

### 需要重新啟動電腦

| | |
|---|---|
| 狀態 | ⚠ |
| 元件 | 系統稽核 |

| | |
|---|---|
| Windows 事件 ID | 225 |
| 卡巴斯基安全管理中心事件 ID | 000000e1 |
| Windows 事件日誌（預設） | ✓ |
| 卡巴斯基安全管理中心事件日誌（預設） | ✓ |

### 產品授權允許使用尚未安裝的元件

| | |
|---|---|
| 狀態 | ⚠ |
| 元件 | 系統稽核 |
| Windows 事件 ID | 226 |
| 卡巴斯基安全管理中心事件 ID | 000000e2 |
| Windows 事件日誌（預設） | ✓ |
| 卡巴斯基安全管理中心事件日誌（預設） | ✓ |

### 進階解毒技術已啟動

| | |
|---|---|
| 狀態 | ⚠ |
| 元件 | 系統稽核 |
| Windows 事件 ID | 232 |
| 卡巴斯基安全管理中心事件 ID | 000000e8 |
| Windows 事件日誌（預設） | – |
| 卡巴斯基安全管理中心事件日誌（預設） | ✓ |

### 進階解毒技術已執行完成

| | |
|---|---|
| 狀態 | ⚠ |
| 元件 | 系統稽核 |
| Windows 事件 ID | 233 |
| 卡巴斯基安全管理中心事件 ID | 000000e9 |
| Windows 事件日誌（預設） | – |
| 卡巴斯基安全管理中心事件日誌（預設） | ✓ |

### 備用金鑰不正確

| | |
|---|---|
| 狀態 | ⚠ |
| 元件 | 系統稽核 |
| Windows 事件 ID | 230 |
| 卡巴斯基安全管理中心事件 ID | 000000e6 |
| Windows 事件日誌（預設） | – |
| 卡巴斯基安全管理中心事件日誌（預設） | ✓ |

### 訂購即將到期

| | |
|---|---|
| 狀態 | ⚠ |
| 元件 | 系統稽核 |

| | |
|---|---|
| Windows 事件 ID | 240 |
| 卡巴斯基安全管理中心事件 ID | 000000f0 |
| Windows 事件日誌（預設） | ✓ |
| 卡巴斯基安全管理中心事件日誌（預設） | ✓ |

### 已封鎖

| | |
|---|---|
| 狀態 | ⚠ |
| 元件 | 行為偵測<br>加密軟體防護<br>弱點利用防禦<br>Web 威脅防護 |
| Windows 事件 ID | 331 |
| 卡巴斯基安全管理中心事件 ID | GNRL_EV_OBJECT_BLOCKED |
| 事件參數 | • GNRL_EA_PARAM_1 是物件的雜湊 (SHA256)。<br>• GNRL_EA_PARAM_2 是物件名稱。<br>當偵測到外部加密共用資料夾時，應用程式將顯示目標檔案的路徑。<br>• GNRL_EA_PARAM_5 是根據 Kaspersky 分類的威脅名稱，例如，EICAR-Test-File。<br>• GNRL_EA_PARAM_7 是工作階段使用者的名稱。<br>• GNRL_EA_PARAM_8 是威脅類型 (type)。<br>• GNRL_EA_PARAM_9 是被偵測到物件的其它資訊：<br>應用程式元件 (engine)。<br>威脅偵測技術 (method)。<br>卡巴斯基私人安全網路偵測到的威脅 (blacklist)：true 或者 false。<br>EDR 版本。<br>EDR 中的威脅識別符。<br>物件的 MD5 雜湊。 |
| Windows 事件日誌（預設） | ✓ |
| 卡巴斯基安全管理中心事件日誌（預設） | – |

### 作業係統設定不允許控制對 Wi-Fi 網路的存取。

| | |
|---|---|
| 狀態 | ⚠ |
| 元件 | 裝置控制 |
| Windows 事件 ID | 249 |
| 卡巴斯基安全管理中心事件 ID | 000000f9 |
| Windows 事件日誌（預設） | ✓ |
| 卡巴斯基安全管理中心事件日誌（預設） | – |

### 物件未從備份中還原

| | |
|---|---|
| 狀態 | ⚠ |
| 元件 | 系統稽核 |
| Windows 事件 ID | 336 |
| 卡巴斯基安全管理中心事件 ID | 00000150 |
| Windows 事件日誌（預設） | ✓ |
| 卡巴斯基安全管理中心事件日誌（預設） | – |

### 偵測到可疑的網路活動

| | |
|---|---|
| 狀態 | ⚠ |
| 元件 | 系統稽核 |
| Windows 事件 ID | 2001 |
| 卡巴斯基安全管理中心事件 ID | 000007d1 |
| Windows 事件日誌（預設） | – |
| 卡巴斯基安全管理中心事件日誌（預設） | ✓ |

### 加密連線已終止

| | |
|---|---|
| 狀態 | ⚠ |
| 元件 | 系統稽核 |
| Windows 事件 ID | 250 |
| 卡巴斯基安全管理中心事件 ID | 000007d3 |
| Windows 事件日誌（預設） | ✓ |
| 卡巴斯基安全管理中心事件日誌（預設） | ✓ |

### 已停用參與 KSN

| | |
|---|---|
| 狀態 | ⚠ |
| 元件 | 系統稽核 |
| Windows 事件 ID | 2021 |
| 卡巴斯基安全管理中心事件 ID | 000007e5 |
| Windows 事件日誌（預設） | – |
| 卡巴斯基安全管理中心事件日誌（預設） | ✓ |

### 已停用處理某些 OS 功能。

| | |
|---|---|
| 狀態 | ⚠ |
| 元件 | 系統稽核 |
| Windows 事件 ID | 245 |
| 卡巴斯基安全管理中心事件 ID | 000000f5 |
| Windows 事件日誌（預設） | ✓ |
| 卡巴斯基安全管理中心事件日誌（預設） | ✓ |

### 隔離區儲存幾乎用盡空間

| | |
|---|---|
| 狀態 | ⚠ |
| 元件 | 系統稽核 |
| Windows 事件 ID | 344 |
| 卡巴斯基安全管理中心事件 ID | 00000158 |
| Windows 事件日誌（預設） | ✓ |
| 卡巴斯基安全管理中心事件日誌（預設） | ✓ |

### 已封鎖網路連線

| | |
|---|---|
| 狀態 | ⚠ |
| 元件 | 系統稽核 |
| Windows 事件 ID | 809 |
| 卡巴斯基安全管理中心事件 ID | 00000abe |
| Windows 事件日誌（預設） | – |
| 卡巴斯基安全管理中心事件日誌（預設） | ✓ |

## 無法建立備份副本

| | |
|---|---|
| 狀態 | ⚠ |
| 元件 | 檔案威脅防護<br>郵件威脅防護<br>主機入侵防禦<br>AMSI 防護<br>惡意軟體掃描 |
| Windows 事件 ID | 314 |
| 卡巴斯基安全管理中心事件 ID | GNRL_EV_OBJECT_REPORTED |
| 事件參數 | • GNRL_EA_PARAM_1 是物件的雜湊 (SHA256)。<br>• GNRL_EA_PARAM_2 是物件名稱。<br>• GNRL_EA_PARAM_5 是根據 Kaspersky 分類的威脅名稱，例如，EICAR-Test-File。<br>• GNRL_EA_PARAM_7 是工作階段使用者的名稱。<br>• GNRL_EA_PARAM_8 是威脅類型 (type)。<br>• GNRL_EA_PARAM_9 是被偵測到物件的其它資訊：<br>應用程式元件 (engine)。<br>威脅偵測技術 (method)。<br>卡巴斯基私人安全網路偵測到的威脅 (blacklist)：true 或者 false。<br>EDR 版本。<br>EDR 中的威脅識別符。<br>物件的 MD5 雜湊。 |
| Windows 事件日誌（預設） | – |
| 卡巴斯基安全管理中心事件日誌（預設） | ✓ |

| | |
|---|---|
| 狀態 | ⚠ |
| 元件 | 檔案威脅防護<br>行為偵測<br>加密軟體防護<br>主機入侵防禦<br>惡意軟體掃描 |
| Windows 事件 ID | 310 |
| 卡巴斯基安全管理中心事件 ID | 00000136 |
| Windows 事件日誌（預設） | – |
| 卡巴斯基安全管理中心事件日誌（預設） | ✓ |

## 物件已加密

| | |
|---|---|
| 狀態 | ⚠ |
| 元件 | 主機入侵防禦 |
| Windows 事件 ID | 320 |
| 卡巴斯基安全管理中心事件 ID | 00000140 |
| Windows 事件日誌（預設） | – |
| 卡巴斯基安全管理中心事件日誌（預設） | – |

## 物件已損壞

| | |
|---|---|
| 狀態 | ⚠ |
| 元件 | 檔案威脅防護<br>Web 威脅防護<br>郵件威脅防護<br>AMSI 防護<br>主機入侵防禦<br>惡意軟體掃描 |
| Windows 事件 ID | 321 |
| 卡巴斯基安全管理中心事件 ID | 00000141 |
| Windows 事件日誌（預設） | – |
| 卡巴斯基安全管理中心事件日誌（預設） | – |

## 偵測到可被入侵者利用以破壞您的電腦或個人資料的合法軟體（本機基底）

| | |
|---|---|
| 狀態 | ⚠ |
| 元件 | 檔案威脅防護<br>Web 威脅防護<br>郵件威脅防護<br>主機入侵防禦<br>AMSI 防護<br>行為偵測<br>加密軟體防護<br>加密軟體防護<br>惡意軟體掃描 |
| Windows 事件 ID | 303 |
| 卡巴斯基安全管理中心事件 ID | GNRL_EV_SUSPICIOUS_OBJECT_FOUND |
| 事件參數 | • GNRL_EA_PARAM_1 是物件的雜湊 (SHA256)。<br>• GNRL_EA_PARAM_2 是物件名稱。<br>• GNRL_EA_PARAM_5 是根據 Kaspersky 分類的威脅名稱，例如，EICAR-Test-File。<br>• GNRL_EA_PARAM_7 是工作階段使用者的名稱。<br>• GNRL_EA_PARAM_8 是威脅類型 (type)。 |
| Windows 事件日誌（預設） | – |
| 卡巴斯基安全管理中心事件日誌（預設） | ✓ |

## 偵測到可被入侵者利用以破壞您的電腦或個人資料的合法軟體 (KSN)

| | |
|---|---|
| 狀態 | ⚠ |
| 元件 | 檔案威脅防護<br>Web 威脅防護<br>郵件威脅防護<br>主機入侵防禦<br>AMSI 防護<br>行為偵測<br>加密軟體防護<br>加密軟體防護<br>惡意軟體掃描 |
| Windows 事件 ID | 303 |
| 卡巴斯基安全管理中心事件 ID | GNRL_EV_SUSPICIOUS_OBJECT_FOUND |
| 事件參數 | • GNRL_EA_PARAM_1 是物件的雜湊 (SHA256)。<br>• GNRL_EA_PARAM_2 是物件名稱。<br>• GNRL_EA_PARAM_5 是根據 Kaspersky 分類的威脅名稱，例如，EICAR-Test-File。<br>• GNRL_EA_PARAM_7 是工作階段使用者的名稱。<br>• GNRL_EA_PARAM_8 是威脅類型 (type)。 |
| Windows 事件日誌（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<br>郵件威脅防護<br>主機入侵防禦<br>弱點利用防禦<br>行為偵測<br>加密軟體防護<br>惡意軟體掃描 |
| Windows 事件 ID | 307 |
| 卡巴斯基安全管理中心事件 ID | GNRL_EV_OBJECT_DELETED |
| 事件參數 | • GNRL_EA_PARAM_1 是物件的雜湊 (SHA256)。<br>• GNRL_EA_PARAM_2 是物件名稱。<br>• GNRL_EA_PARAM_5 是根據 Kaspersky 分類的威脅名稱，例如，EICAR-Test-File。<br>• GNRL_EA_PARAM_7 是工作階段使用者的名稱。<br>• GNRL_EA_PARAM_8 是威脅類型 (type)。<br>• GNRL_EA_PARAM_9 是被偵測到物件的其它資訊：<br>應用程式元件 (engine)。<br>威脅偵測技術 (method)。<br>卡巴斯基私人安全網路偵測到的威脅 (blacklist)：true 或者 false。<br>EDR 版本。<br>EDR 中的威脅識別符。<br>物件的 MD5 雜湊。 |
| Windows 事件日誌（預設） | – |
| 卡巴斯基安全管理中心事件日誌（預設） | ✓ |

## 物件已解毒

| | |
|---|---|
| 狀態 | ⚠ |
| 元件 | 檔案威脅防護<br>郵件威脅防護<br>主機入侵防禦<br>惡意軟體掃描 |
| Windows 事件 ID | 306 |
| 卡巴斯基安全管理中心事件 ID | GNRL_EV_OBJECT_CURED |
| 事件參數 | • GNRL_EA_PARAM_1 是物件的雜湊 (SHA256)。<br>• GNRL_EA_PARAM_2 是物件名稱。<br>• GNRL_EA_PARAM_5 是根據 Kaspersky 分類的威脅名稱，例如，EICAR-Test-File。<br>• GNRL_EA_PARAM_7 是工作階段使用者的名稱。<br>• GNRL_EA_PARAM_8 是威脅類型 (type)。<br>• GNRL_EA_PARAM_9 是被偵測到物件的其它資訊：<br>應用程式元件 (engine)。<br>威脅偵測技術 (method)。<br>卡巴斯基私人安全網路偵測到的威脅 (blacklist)：true 或者 false。<br>EDR 版本。<br>EDR 中的威脅識別符。<br>物件的 MD5 雜湊。 |
| Windows 事件日誌（預設） | – |
| 卡巴斯基安全管理中心事件日誌（預設） | ✓ |

## 物件將在重新啟動後解毒

| | |
|---|---|
| 狀態 | ⚠ |
| 元件 | 主機入侵防禦<br>檔案威脅防護<br>惡意軟體掃描 |
| Windows 事件 ID | 324 |

| | |
|---|---|
| 卡巴斯基安全管理中心事件 ID | – |
| Windows 事件日誌（預設） | ✓ |
| 卡巴斯基安全管理中心事件日誌（預設） | – |

### 物件將在重新啟動後刪除

| | |
|---|---|
| 狀態 | ⚠ |
| 元件 | 行為偵測<br>加密軟體防護<br>弱點利用防禦<br>主機入侵防禦<br>檔案威脅防護<br>惡意軟體掃描 |
| Windows 事件 ID | 323 |
| 卡巴斯基安全管理中心事件 ID | – |
| Windows 事件日誌（預設） | ✓ |
| 卡巴斯基安全管理中心事件日誌（預設） | – |

### 根據設定刪除物件

| | |
|---|---|
| 狀態 | ⚠ |
| 元件 | 郵件威脅防護 |
| Windows 事件 ID | 342 |
| 卡巴斯基安全管理中心事件 ID | – |
| Windows 事件日誌（預設） | ✓ |
| 卡巴斯基安全管理中心事件日誌（預設） | – |

### 回溯已完成

| | |
|---|---|
| 狀態 | ⚠ |
| 元件 | 檔案威脅防護<br>行為偵測<br>加密軟體防護<br>弱點利用防禦<br>惡意軟體掃描 |
| Windows 事件 ID | 455 |
| 卡巴斯基安全管理中心事件 ID | 000001c7 |
| Windows 事件日誌（預設） | – |
| 卡巴斯基安全管理中心事件日誌（預設） | ✓ |

### 物件下載被封鎖

| | |
|---|---|
| 狀態 | ⚠ |
| 元件 | Web 威脅防護 |
| Windows 事件 ID | 341 |

| | |
|---|---|
| 卡巴斯基安全管理中心事件 ID | GNRL_EV_OBJECT_BLOCKED |
| 事件參數 | • GNRL_EA_PARAM_1 是物件的雜湊 (SHA256)。<br>• GNRL_EA_PARAM_2 是物件名稱。<br>• GNRL_EA_PARAM_5 是根據 Kaspersky 分類的威脅名稱，例如，EICAR-Test-File。<br>• GNRL_EA_PARAM_7 是工作階段使用者的名稱。<br>• GNRL_EA_PARAM_8 是威脅類型 (type)。<br>• GNRL_EA_PARAM_9 是被偵測到物件的其它資訊：<br>應用程式元件 (engine)。<br>威脅偵測技術 (method)。<br>卡巴斯基私人安全網路偵測到的威脅 (blacklist)：true 或者 false。<br>EDR 版本。<br>EDR 中的威脅識別符。<br>物件的 MD5 雜湊。 |
| Windows 事件日誌（預設） | – |
| 卡巴斯基安全管理中心事件日誌（預設） | ✓ |

### 鍵盤授權錯誤

| | |
|---|---|
| 狀態 | ⚠ |
| 元件 | BadUSB 攻擊防護 |
| Windows 事件 ID | 2052 |
| 卡巴斯基安全管理中心事件 ID | 00000804 |
| Windows 事件日誌（預設） | ✓ |
| 卡巴斯基安全管理中心事件日誌（預設） | ✓ |

### 物件掃描結果已傳送至協力廠商應用程式

| | |
|---|---|
| 狀態 | ⚠ |
| 元件 | AMSI 防護 |
| Windows 事件 ID | 1512 |
| 卡巴斯基安全管理中心事件 ID | GNRL_EV_OBJECT_REPORTED |
| 事件參數 | • GNRL_EA_PARAM_1 是物件的雜湊 (SHA256)。<br>• GNRL_EA_PARAM_2 是物件名稱。<br>• GNRL_EA_PARAM_5 是根據 Kaspersky 分類的威脅名稱，例如，EICAR-Test-File。<br>• GNRL_EA_PARAM_7 是工作階段使用者的名稱。<br>• GNRL_EA_PARAM_8 是威脅類型 (type)。<br>• GNRL_EA_PARAM_9 是被偵測到物件的其它資訊：<br>應用程式元件 (engine)。<br>威脅偵測技術 (method)。<br>卡巴斯基私人安全網路偵測到的威脅 (blacklist)：true 或者 false。<br>EDR 版本。<br>EDR 中的威脅識別符。<br>物件的 MD5 雜湊。 |
| Windows 事件日誌（預設） | – |
| 卡巴斯基安全管理中心事件日誌（預設） | ✓ |

### 工作設定已成功套用

| | |
|---|---|
| 狀態 | ⚠ |
| 元件 | 應用程式控制 |
| Windows 事件 ID | 708 |
| 卡巴斯基安全管理中心事件 ID | 000002c4 |
| Windows 事件日誌（預設） | – |
| 卡巴斯基安全管理中心事件日誌（預設） | ✓ |

## 有關不良內容的警告 (本機資料庫)

| | |
|---|---|
| 狀態 | ⚠ |
| 元件 | Web 控制 |
| Windows 事件 ID | 708 |
| 卡巴斯基安全管理中心事件 ID | GNRL_EV_WEB_URL_WARNING |
| 事件參數 | • GNRL_EA_PARAM_1 是網址。<br>• GNRL_EA_PARAM_2 是工作階段使用者的名稱。<br>• GNRL_EA_PARAM_3 是網頁控制規則的名稱。 |
| Windows 事件日誌（預設） | – |
| 卡巴斯基安全管理中心事件日誌（預設） | ✓ |

## 有關不良內容的警告 (KSN)

| | |
|---|---|
| 狀態 | ⚠ |
| 元件 | Web 控制 |
| Windows 事件 ID | 708 |
| 卡巴斯基安全管理中心事件 ID | GNRL_EV_WEB_URL_WARNING |
| 事件參數 | • GNRL_EA_PARAM_1 是網址。<br>• GNRL_EA_PARAM_2 是工作階段使用者的名稱。<br>• GNRL_EA_PARAM_3 是網頁控制規則的名稱。 |
| Windows 事件日誌（預設） | – |
| 卡巴斯基安全管理中心事件日誌（預設） | ✓ |

## 在警告後存取了不良內容

| | |
|---|---|
| 狀態 | ⚠ |
| 元件 | Web 控制 |
| Windows 事件 ID | 754 |
| 卡巴斯基安全管理中心事件 ID | 000002f2 |
| Windows 事件日誌（預設） | – |
| 卡巴斯基安全管理中心事件日誌（預設） | – |

## 已啟動對裝置的暫時存取

| | |
|---|---|
| 狀態 | ⚠ |
| 元件 | 裝置控制 |
| Windows 事件 ID | 803 |
| 卡巴斯基安全管理中心事件 ID | 000002f2 |
| Windows 事件日誌（預設） | ✓ |
| 卡巴斯基安全管理中心事件日誌（預設） | – |

## 操作被使用者取消

| | |
|---|---|
| 狀態 | ⚠ |
| 元件 | 更新 |

| | |
|---|---|
| Windows 事件 ID | 1016 |
| 卡巴斯基安全管理中心事件 ID | 000003f8 |
| Windows 事件日誌（預設） | – |
| 卡巴斯基安全管理中心事件日誌（預設） | ✓ |

### 使用者選擇了結束加密政策

| | |
|---|---|
| 狀態 | ⚠ |
| 元件 | 資料加密 |
| Windows 事件 ID | 1306 |
| 卡巴斯基安全管理中心事件 ID | 0000051a |
| Windows 事件日誌（預設） | – |
| 卡巴斯基安全管理中心事件日誌（預設） | ✓ |

### 已中斷套用檔案加密/解密規則

| | |
|---|---|
| 狀態 | ⚠ |
| 元件 | 資料加密 |
| Windows 事件 ID | 903 |
| 卡巴斯基安全管理中心事件 ID | – |
| Windows 事件日誌（預設） | ✓ |
| 卡巴斯基安全管理中心事件日誌（預設） | – |

### 檔案加密/解密已中斷

| | |
|---|---|
| 狀態 | ⚠ |
| 元件 | 資料加密 |
| Windows 事件 ID | 914 |
| 卡巴斯基安全管理中心事件 ID | – |
| Windows 事件日誌（預設） | ✓ |
| 卡巴斯基安全管理中心事件日誌（預設） | – |

### 已中斷裝置加密/解密

| | |
|---|---|
| 狀態 | ⚠ |
| 元件 | 資料加密 |
| Windows 事件 ID | 1303 |
| 卡巴斯基安全管理中心事件 ID | – |
| Windows 事件日誌（預設） | ✓ |
| 卡巴斯基安全管理中心事件日誌（預設） | – |

### 無法在 WinRE 映像中安裝或升級卡巴斯基磁碟加密驅動程式

| | |
|---|---|
| 狀態 | ⚠ |
| 元件 | 資料加密 |
| Windows 事件 ID | 1345 |

| | |
|---|---|
| 卡巴斯基安全管理中心事件 ID | 00000541 |
| Windows 事件日誌（預設） | ✓ |
| 卡巴斯基安全管理中心事件日誌（預設） | ✓ |

### 模組簽章檢查失敗

| | |
|---|---|
| 狀態 | ⚠ |
| 元件 | 系統完整性檢查 |
| Windows 事件 ID | 2002 |
| 卡巴斯基安全管理中心事件 ID | 000007d2 |
| Windows 事件日誌（預設） | – |
| 卡巴斯基安全管理中心事件日誌（預設） | ✓ |

### 已封鎖應用程式啟動

| | |
|---|---|
| 狀態 | ⚠ |
| 元件 | Endpoint Sensor |
| Windows 事件 ID | 2105 |
| 卡巴斯基安全管理中心事件 ID | 00000839 |
| Windows 事件日誌（預設） | ✓ |
| 卡巴斯基安全管理中心事件日誌（預設） | ✓ |

### 已封鎖開啟文件

| | |
|---|---|
| 狀態 | ⚠ |
| 元件 | Endpoint Sensor |
| Windows 事件 ID | 2106 |
| 卡巴斯基安全管理中心事件 ID | 0000083a |
| Windows 事件日誌（預設） | ✓ |
| 卡巴斯基安全管理中心事件日誌（預設） | ✓ |

### 處理程序已被 Kaspersky Anti Targeted Attack Platform 伺服器管理員終止

| | |
|---|---|
| 狀態 | ⚠ |
| 元件 | Endpoint Sensor |
| Windows 事件 ID | 2112 |
| 卡巴斯基安全管理中心事件 ID | 00000840 |
| Windows 事件日誌（預設） | ✓ |
| 卡巴斯基安全管理中心事件日誌（預設） | ✓ |

### 應用程式已被 Kaspersky Anti Targeted Attack Platform 伺服器管理員終止

| | |
|---|---|
| 狀態 | ⚠ |
| 元件 | Endpoint Sensor |
| Windows 事件 ID | 2113 |

| | |
|---|---|
| 卡巴斯基安全管理中心事件 ID | 00000841 |
| Windows 事件日誌（預設） | ✓ |
| 卡巴斯基安全管理中心事件日誌（預設） | ✓ |

### 檔案或串流已被 Kaspersky Anti Targeted Attack Platform 伺服器管理員刪除

| | |
|---|---|
| 狀態 | ⚠ |
| 元件 | Endpoint Sensor |
| Windows 事件 ID | 2111 |
| 卡巴斯基安全管理中心事件 ID | 0000083f |
| Windows 事件日誌（預設） | ✓ |
| 卡巴斯基安全管理中心事件日誌（預設） | ✓ |

### 檔案已被管理員從 Kaspersky Anti Targeted Attack Platform 伺服器上的隔離區還原

| | |
|---|---|
| 狀態 | ⚠ |
| 元件 | Endpoint Sensor |
| Windows 事件 ID | 2110 |
| 卡巴斯基安全管理中心事件 ID | 0000083e |
| Windows 事件日誌（預設） | ✓ |
| 卡巴斯基安全管理中心事件日誌（預設） | ✓ |

### 檔案已被管理員在 Kaspersky Anti Targeted Attack Platform 伺服器上隔離

| | |
|---|---|
| 狀態 | ⚠ |
| 元件 | Endpoint Sensor |
| Windows 事件 ID | 2109 |
| 卡巴斯基安全管理中心事件 ID | 0000083d |
| Windows 事件日誌（預設） | ✓ |
| 卡巴斯基安全管理中心事件日誌（預設） | ✓ |

### 所有協力廠商應用程式的網路活動均已封鎖

| | |
|---|---|
| 狀態 | ⚠ |
| 元件 | Endpoint Sensor |
| Windows 事件 ID | 2107 |
| 卡巴斯基安全管理中心事件 ID | 0000083b |
| Windows 事件日誌（預設） | ✓ |
| 卡巴斯基安全管理中心事件日誌（預設） | ✓ |

### 所有協力廠商應用程式的網路活動均已解除封鎖

| | |
|---|---|
| 狀態 | ⚠ |
| 元件 | Endpoint Sensor |
| Windows 事件 ID | 2108 |

| | |
|---|---|
| 卡巴斯基安全管理中心事件 ID | 0000083c |
| Windows 事件日誌（預設） | ✓ |
| 卡巴斯基安全管理中心事件日誌（預設） | ✓ |

### 物件將在重新啟動後刪除 (Sandbox)

| | |
|---|---|
| 狀態 | ⚠ |
| 元件 | Sandbox |
| Windows 事件 ID | 2605 |
| 卡巴斯基安全管理中心事件 ID | 00000a2d |
| Windows 事件日誌（預設） | ✓ |
| 卡巴斯基安全管理中心事件日誌（預設） | ✓ |

### 掃描工作總大小超過限制

| | |
|---|---|
| 狀態 | ⚠ |
| 元件 | Sandbox |
| Windows 事件 ID | 2612 |
| 卡巴斯基安全管理中心事件 ID | 00000a34 |
| Windows 事件日誌（預設） | ✓ |
| 卡巴斯基安全管理中心事件日誌（預設） | ✓ |

### 允許物件啟動。事件已記錄

| | |
|---|---|
| 狀態 | ⚠ |
| 元件 | Endpoint Detection and Response |
| Windows 事件 ID | 2553 |
| 卡巴斯基安全管理中心事件 ID | 000009fa |
| Windows 事件日誌（預設） | ✓ |
| 卡巴斯基安全管理中心事件日誌（預設） | ✓ |

### 允許處理程序啟動，事件已記錄

| | |
|---|---|
| 狀態 | ⚠ |
| 元件 | Endpoint Detection and Response |
| Windows 事件 ID | 2554 |
| 卡巴斯基安全管理中心事件 ID | 000009f8 |
| Windows 事件日誌（預設） | ✓ |
| 卡巴斯基安全管理中心事件日誌（預設） | ✓ |

### 物件將在重新啟動後刪除 (Endpoint Detection and Response)

| | |
|---|---|
| 狀態 | ⚠ |
| 元件 | Endpoint Detection and Response |
| Windows 事件 ID | 2558 |

| | |
|---|---|
| 卡巴斯基安全管理中心事件 ID | 000009fe |
| Windows 事件日誌（預設） | ✓ |
| 卡巴斯基安全管理中心事件日誌（預設） | ✓ |

### 網路隔離

| | |
|---|---|
| 狀態 | ⚠ |
| 元件 | Endpoint Detection and Response |
| Windows 事件 ID | 2700 |
| 卡巴斯基安全管理中心事件 ID | 00000a8c |
| Windows 事件日誌（預設） | ✓ |
| 卡巴斯基安全管理中心事件日誌（預設） | ✓ |

### 終止網路隔離

| | |
|---|---|
| 狀態 | ⚠ |
| 元件 | Endpoint Detection and Response |
| Windows 事件 ID | 2701 |
| 卡巴斯基安全管理中心事件 ID | 00000a8d |
| Windows 事件日誌（預設） | ✓ |
| 卡巴斯基安全管理中心事件日誌（預設） | ✓ |

### 完成工作需要重新啟動

| | |
|---|---|
| 狀態 | ⚠ |
| 元件 | 系統稽核 |
| Windows 事件 ID | 225 |
| 卡巴斯基安全管理中心事件 ID | 0000057b |
| Windows 事件日誌（預設） | ✓ |
| 卡巴斯基安全管理中心事件日誌（預設） | ✓ |

### 傳送給管理員的應用程式啟動封鎖訊息

| | |
|---|---|
| 狀態 | ⚠ |
| 元件 | 應用程式控制 |
| Windows 事件 ID | 503 |
| 卡巴斯基安全管理中心事件 ID | GNRL_EV_AC_USER_REQUEST |
| 事件參數 | • GNRL_EA_DESCRIPTION 是傳送給使用者的訊息。<br>• GNRL_EA_PARAM_2 是工作階段使用者的名稱。<br>• GNRL_EA_PARAM_6 是應用程式的可執行檔（例如，chrome.exe）。<br>• GNRL_EA_PARAM_7 是可執行檔路徑。<br>• GNRL_EA_PARAM_8 是物件的雜湊 (SHA256)。<br>• GNRL_EA_PARAM_9 是使用者努力執行的應用程式的版本。 |
| Windows 事件日誌（預設） | – |
| 卡巴斯基安全管理中心事件日誌（預設） | ✓ |

### 傳送給管理員的裝置存取封鎖訊息

| | |
|---|---|
| 狀態 | ⚠ |
| 元件 | 裝置控制 |
| Windows 事件 ID | 804 |
| 卡巴斯基安全管理中心事件 ID | GNRL_EV_DC_USER_REQUEST |
| 事件參數 | • c_er_descr 是傳送給使用者的訊息。<br>• GNRL_EA_PARAM_1 是硬體 ID (HWID)。<br>• GNRL_EA_PARAM_2 是工作階段使用者的名稱。 |
| Windows 事件日誌（預設） | – |
| 卡巴斯基安全管理中心事件日誌（預設） | ✓ |

### 傳送給管理員的網頁存取封鎖訊息

| | |
|---|---|
| 狀態 | ⚠ |
| 元件 | Web 控制 |
| Windows 事件 ID | 755 |
| 卡巴斯基安全管理中心事件 ID | GNRL_EV_WC_USER_REQUEST |
| 事件參數 | • GNRL_EA_DESCRIPTION 是傳送給使用者的訊息。<br>• GNRL_EA_PARAM_1 是網址。<br>• GNRL_EA_PARAM_2 是工作階段使用者的名稱。 |
| Windows 事件日誌（預設） | – |
| 卡巴斯基安全管理中心事件日誌（預設） | ✓ |

### 已封鎖裝置連接

| | |
|---|---|
| 狀態 | ⚠ |
| 元件 | 裝置控制 |
| Windows 事件 ID | 807 |
| 卡巴斯基安全管理中心事件 ID | GNRL_EV_DEVCTRL_DEV_PLUG_DENIED |
| 事件參數 | • GNRL_EA_PARAM_1 是硬體 ID (HWID)。<br>• GNRL_EA_PARAM_2 是工作階段使用者的名稱。 |
| Windows 事件日誌（預設） | – |
| 卡巴斯基安全管理中心事件日誌（預設） | ✓ |

### 傳送給管理員的應用程式活動封鎖訊息

| | |
|---|---|
| 狀態 | ⚠ |
| 元件 | 檔案完整性監控 |
| Windows 事件 ID | 2901 |
| 卡巴斯基安全管理中心事件 ID | 00000b55 |
| Windows 事件日誌（預設） | ✓ |
| 卡巴斯基安全管理中心事件日誌（預設） | ✓ |

| | |
|---|---|
| 狀態 | ⚠ |
| 元件 | 檔案完整性監控 |
| Windows 事件 ID | 2900 |

| | |
|---|---|
| 卡巴斯基安全管理中心事件 ID | 00000b54 |
| Windows 事件日誌（預設） | ✓ |
| 卡巴斯基安全管理中心事件日誌（預設） | ✓ |

| | |
|---|---|
| 狀態 | ⚠ |
| 元件 | 自適應異常控制 |
| Windows 事件 ID | 503 |
| 卡巴斯基安全管理中心事件 ID | GNRL_EV_ADSEC_USER_REQUEST |
| 事件參數 | • GNRL_EA_DESCRIPTION 是傳送給使用者的訊息。<br>• GNRL_EA_PARAM_1 是適應性異常控制規則的名稱。<br>• GNRL_EA_PARAM_2 是啟發式規則的 ID。<br>• GNRL_EA_PARAM_3 是工作階段使用者的名稱。<br>• GNRL_EA_PARAM_4 是來源處理程序。<br>• GNRL_EA_PARAM_5 是來源物件。<br>• GNRL_EA_PARAM_6 是目標處理程序。<br>• GNRL_EA_PARAM_7 是目標物件。<br>• GNRL_EA_PARAM_8 是被偵測到物件的其它資訊：來源處理程序 / 物件和目標處理程序 / 物件的雜湊。處理程序被封鎖 (verdict_type): true 或 false。使用者安全 ID (SID)。 |
| Windows 事件日誌（預設） | – |
| 卡巴斯基安全管理中心事件日誌（預設） | ✓ |

## 封鎖啟動雲端服務用戶端應用程式

| | |
|---|---|
| 狀態 | ⚠ |
| 元件 | Cloud Discovery |
| Windows 事件 ID | 2212 |
| 卡巴斯基安全管理中心事件 ID | 000008a4 |
| Windows 事件日誌（預設） | – |
| 卡巴斯基安全管理中心事件日誌（預設） | ✓ |

## 封鎖存取雲端服務

| | |
|---|---|
| 狀態 | ⚠ |
| 元件 | Cloud Discovery |
| Windows 事件 ID | 2213 |
| 卡巴斯基安全管理中心事件 ID | 000008a5 |
| Windows 事件日誌（預設） | – |
| 卡巴斯基安全管理中心事件日誌（預設） | ✓ |

## 偵測到對檔案或資料夾的變更

| | |
|---|---|
| 狀態 | ⓘ / ⚠ / ⓘ |
| 元件 | 系統完整性監控 |
| Windows 事件 ID | 2950 |
| 卡巴斯基安全管理中心事件 ID | 00000b86 |
| Windows 事件日誌（預設） | – |

| | |
|---|---|
| 卡巴斯基安全管理中心事件日誌（預設） | ✓ |

若要配置此事件的保留期，請前往政策的 **事件組態** 部分並設定一般系統完整性監控事件的保留期 – *偵測到對檔案或資料夾的變更*。

### 物件變更頻繁。事件彙總已啟動

| | |
|---|---|
| 狀態 | ⓘ / ⚠ / ❗ |
| 元件 | 系統完整性監控 |
| Windows 事件 ID | 2955 |
| 卡巴斯基安全管理中心事件 ID | 00000b8b |
| Windows 事件日誌（預設） | – |
| 卡巴斯基安全管理中心事件日誌（預設） | ✓ |

### 彙總期間的物件修改報告

| | |
|---|---|
| 狀態 | ⓘ / ⚠ / ❗ |
| 元件 | 系統完整性監控 |
| Windows 事件 ID | 2956 |
| 卡巴斯基安全管理中心事件 ID | 00000b8c |
| Windows 事件日誌（預設） | – |
| 卡巴斯基安全管理中心事件日誌（預設） | ✓ |

若要配置此事件的保留期，請前往政策的 **事件組態** 部分並設定一般系統完整性監控事件的保留期 – *偵測到對檔案或資料夾的變更*。

### 偵測到登錄檔變更

| | |
|---|---|
| 狀態 | ⓘ / ⚠ / ❗ |
| 元件 | 系統完整性監控 |
| Windows 事件 ID | 2951 |
| 卡巴斯基安全管理中心事件 ID | 00000b87 |
| Windows 事件日誌（預設） | – |
| 卡巴斯基安全管理中心事件日誌（預設） | ✓ |

若要配置此事件的保留期，請前往政策的 **事件組態** 部分並設定一般系統完整性監控事件的保留期 – *偵測到對檔案或資料夾的變更*。

### 偵測到裝置連線 / 連線中斷

| | |
|---|---|
| 狀態 | ⓘ / ⚠ / ❗ |
| 元件 | 系統完整性監控 |
| Windows 事件 ID | 2952 |
| 卡巴斯基安全管理中心事件 ID | 00000b88 |
| Windows 事件日誌（預設） | – |

| | |
|---|---|
| 卡巴斯基安全管理中心事件日誌（預設） | ✓ |

若要配置此事件的保留期，請前往政策的 **事件組態** 部分並設定一般系統完整性監控事件的保留期 – *偵測到對檔案或資料夾的變更*。

### 監控範圍包括不正確的物件

| | |
|---|---|
| 狀態 | ⓘ / ⚠ / ⓘ |
| 元件 | 系統完整性監控 |
| Windows 事件 ID | 2903 |
| 卡巴斯基安全管理中心事件 ID | 00000b89 |
| Windows 事件日誌（預設） | – |
| 卡巴斯基安全管理中心事件日誌（預設） | ✓ |

若要配置此事件的保留期，請前往政策的 **事件組態** 部分並設定一般系統完整性監控事件的保留期 – *偵測到對檔案或資料夾的變更*。

### 測試模式中允許被禁止的操作

| | |
|---|---|
| 狀態 | ⚠ |
| 元件 | 系統完整性監控 |
| Windows 事件 ID | 2961 |
| 卡巴斯基安全管理中心事件 ID | 00000b91 |
| Windows 事件日誌（預設） | – |
| 卡巴斯基安全管理中心事件日誌（預設） | ✓ |

### 無法連線到 Integration Server 超過 30 分鐘。請檢查 Integration Server 狀態和網路設定。

| | |
|---|---|
| 狀態 | ⚠ |
| 元件 | Light Agent |
| Windows 事件 ID | 3102 |
| 卡巴斯基安全管理中心事件 ID | 00000c1e |
| Windows 事件日誌（預設） | – |
| 卡巴斯基安全管理中心事件日誌（預設） | ✓ |

### 無法連線到 Integration Server。請檢查 Integration Server 狀態和網路設定。

| | |
|---|---|
| 狀態 | ⚠ |
| 元件 | Light Agent |
| Windows 事件 ID | 3101 |
| 卡巴斯基安全管理中心事件 ID | 00000c1d |
| Windows 事件日誌（預設） | – |
| 卡巴斯基安全管理中心事件日誌（預設） | ✓ |

### 虛擬機範本需要更新

| | |
|---|---|
| 狀態 | ⚠ |
| 元件 | Light Agent |
| Windows 事件 ID | 3181 |
| 卡巴斯基安全管理中心事件 ID | 00000c6d |
| Windows 事件日誌（預設） | – |
| 卡巴斯基安全管理中心事件日誌（預設） | ✓ |

### Standard 產品授權已終止。應用程式正在 Enterprise 產品授權下執行

| | |
|---|---|
| 狀態 | ⚠ |
| 元件 | Light Agent |
| Windows 事件 ID | 3171 |
| 卡巴斯基安全管理中心事件 ID | 00000c64 |
| Windows 事件日誌（預設） | – |
| 卡巴斯基安全管理中心事件日誌（預設） | ✓ |

## 資訊訊息

### 應用程式已啟動

| | |
|---|---|
| 狀態 | ⓘ |
| 元件 | 系統稽核 |
| Windows 事件 ID | 235 |
| 卡巴斯基安全管理中心事件 ID | – |
| Windows 事件日誌（預設） | ✓ |
| 卡巴斯基安全管理中心事件日誌（預設） | – |

### 應用程式已停止

| | |
|---|---|
| 狀態 | ⓘ |
| 元件 | 系統稽核 |
| Windows 事件 ID | 236 |
| 卡巴斯基安全管理中心事件 ID | – |
| Windows 事件日誌（預設） | ✓ |
| 卡巴斯基安全管理中心事件日誌（預設） | – |

### 自我防護限制存取受防護資源

| | |
|---|---|
| 狀態 | ⓘ |
| 元件 | 系統稽核 |
| Windows 事件 ID | 213 |
| 卡巴斯基安全管理中心事件 ID | 000000d5 |

| | |
|---|---|
| Windows 事件日誌（預設） | – |
| 卡巴斯基安全管理中心事件日誌（預設） | ✓ |

## 報告已清除

| | |
|---|---|
| 狀態 | ⓘ |
| 元件 | 系統稽核 |
| Windows 事件 ID | 217 |
| 卡巴斯基安全管理中心事件 ID | 000000d9 |
| Windows 事件日誌（預設） | ✓ |
| 卡巴斯基安全管理中心事件日誌（預設） | ✓ |

## 群組政策已停用

| | |
|---|---|
| 狀態 | ⓘ |
| 元件 | 系統稽核 |
| Windows 事件 ID | 220 |
| 卡巴斯基安全管理中心事件 ID | 000000dc |
| Windows 事件日誌（預設） | – |
| 卡巴斯基安全管理中心事件日誌（預設） | – |

## 應用程式設定已變更

| | |
|---|---|
| 狀態 | ⓘ |
| 元件 | 系統稽核 |
| Windows 事件 ID | 218 |
| 卡巴斯基安全管理中心事件 ID | 000000da |
| Windows 事件日誌（預設） | ✓ |
| 卡巴斯基安全管理中心事件日誌（預設） | – |

## 工作已啟動

| | |
|---|---|
| 狀態 | ⓘ |
| 元件 | 系統稽核 |
| Windows 事件 ID | 221 |
| 卡巴斯基安全管理中心事件 ID | 000000dd |
| Windows 事件日誌（預設） | – |
| 卡巴斯基安全管理中心事件日誌（預設） | ✓ |

## 工作已完成

| | |
|---|---|
| 狀態 | ⓘ |
| 元件 | 系統稽核 |
| Windows 事件 ID | 223 |
| 卡巴斯基安全管理中心事件 ID | 000000df |

| | |
|---|---|
| Windows 事件日誌（預設） | – |
| 卡巴斯基安全管理中心事件日誌（預設） | ✓ |

### 產品授權定義的所有應用程式元件均已安裝並且以正常模式執行

| | |
|---|---|
| 狀態 | ⓘ |
| 元件 | 系統稽核 |
| Windows 事件 ID | 227 |
| 卡巴斯基安全管理中心事件 ID | 000000e3 |
| Windows 事件日誌（預設） | – |
| 卡巴斯基安全管理中心事件日誌（預設） | – |

### 訂購設定已變更

| | |
|---|---|
| 狀態 | ⓘ |
| 元件 | 系統稽核 |
| Windows 事件 ID | 238 |
| 卡巴斯基安全管理中心事件 ID | 000000ee |
| Windows 事件日誌（預設） | – |
| 卡巴斯基安全管理中心事件日誌（預設） | ✓ |

### 訂購已續約

| | |
|---|---|
| 狀態 | ⓘ |
| 元件 | 系統稽核 |
| Windows 事件 ID | 239 |
| 卡巴斯基安全管理中心事件 ID | 000000ef |
| Windows 事件日誌（預設） | ✓ |
| 卡巴斯基安全管理中心事件日誌（預設） | ✓ |

### 物件已從備份還原

| | |
|---|---|
| 狀態 | ⓘ |
| 元件 | 系統稽核 |
| Windows 事件 ID | 335 |
| 卡巴斯基安全管理中心事件 ID | 0000014f |
| Windows 事件日誌（預設） | – |
| 卡巴斯基安全管理中心事件日誌（預設） | ✓ |

### 使用者名稱和密碼輸入

| | |
|---|---|
| 狀態 | ⓘ |
| 元件 | 系統稽核 |
| Windows 事件 ID | 2000 |
| 卡巴斯基安全管理中心事件 ID | 000007d0 |

| | |
|---|---|
| Windows 事件日誌（預設） | – |
| 卡巴斯基安全管理中心事件日誌（預設） | – |

### 已啟用參與 KSN

| | |
|---|---|
| 狀態 | ⓘ |
| 元件 | 系統稽核 |
| Windows 事件 ID | 2020 |
| 卡巴斯基安全管理中心事件 ID | 000007e4 |
| Windows 事件日誌（預設） | – |
| 卡巴斯基安全管理中心事件日誌（預設） | ✓ |

### KSN 伺服器可用

| | |
|---|---|
| 狀態 | ⓘ |
| 元件 | 系統稽核 |
| Windows 事件 ID | 2022 |
| 卡巴斯基安全管理中心事件 ID | 000007e6 |
| Windows 事件日誌（預設） | – |
| 卡巴斯基安全管理中心事件日誌（預設） | ✓ |

### 應用程式依照相關法律運作和處理資料，並使用適當的基礎結構

| | |
|---|---|
| 狀態 | ⓘ |
| 元件 | 系統稽核 |
| Windows 事件 ID | 2024 |
| 卡巴斯基安全管理中心事件 ID | 000007e8 |
| Windows 事件日誌（預設） | ✓ |
| 卡巴斯基安全管理中心事件日誌（預設） | ✓ |

### 物件被從隔離區還原

| | |
|---|---|
| 狀態 | ⓘ |
| 元件 | 系統稽核 |
| Windows 事件 ID | 345 |
| 卡巴斯基安全管理中心事件 ID | 00000159 |
| Windows 事件日誌（預設） | ✓ |
| 卡巴斯基安全管理中心事件日誌（預設） | ✓ |

### 物件被從隔離區刪除

| | |
|---|---|
| 狀態 | ⓘ |
| 元件 | 系統稽核 |
| Windows 事件 ID | 347 |
| 卡巴斯基安全管理中心事件 ID | 0000015b |

| | |
|---|---|
| Windows 事件日誌（預設） | ✓ |
| 卡巴斯基安全管理中心事件日誌（預設） | ✓ |

## 物件的備份副本已建立

| | |
|---|---|
| 狀態 | ⓘ |
| 元件 | 檔案威脅防護<br>郵件威脅防護<br>行為偵測<br>加密軟體防護<br>主機入侵防禦<br>Sandbox<br>惡意軟體掃描 |
| Windows 事件 ID | 308 |
| 卡巴斯基安全管理中心事件 ID | 00000134 |
| Windows 事件日誌（預設） | ✓ |
| 卡巴斯基安全管理中心事件日誌（預設） | ✓ |

## 已被先前解毒的副本覆寫

| | |
|---|---|
| 狀態 | ⓘ |
| 元件 | 檔案威脅防護<br>主機入侵防禦<br>惡意軟體掃描 |
| Windows 事件 ID | 327 |
| 卡巴斯基安全管理中心事件 ID | 00000147 |
| Windows 事件日誌（預設） | – |
| 卡巴斯基安全管理中心事件日誌（預設） | – |

## 偵測到受密碼防護的壓縮檔案

| | |
|---|---|
| 狀態 | ⓘ |
| 元件 | 檔案威脅防護<br>Web 威脅防護<br>郵件威脅防護<br>AMSI 防護<br>主機入侵防禦<br>惡意軟體掃描 |
| Windows 事件 ID | 322 |
| 卡巴斯基安全管理中心事件 ID | GNRL_EV_PASSWD_ARCHIVE_FOUND |
| 事件參數 | • GNRL_EA_PARAM_2 是物件名稱。<br>• GNRL_EA_PARAM_3 是物件的建立日期（可選）。<br>• GNRL_EA_PARAM_7 是工作階段使用者的名稱。<br>• GNRL_EA_PARAM_9 是被偵測到物件的其它資訊：<br>應用程式元件 (engine)。<br>威脅偵測技術 (method)。<br>私有 KSN 偵測到的威脅（denylist）：true 或者 false。 |
| Windows 事件日誌（預設） | – |
| 卡巴斯基安全管理中心事件日誌（預設） | ✓ |

## 有關偵測物件的資訊

| 狀態 | ⓘ |
| --- | --- |
| 元件 | 檔案威脅防護<br>Web 威脅防護<br>郵件威脅防護<br>AMSI 防護<br>主機入侵防禦<br>惡意軟體掃描 |
| Windows 事件 ID | 332 |
| 卡巴斯基安全管理中心事件 ID | 0000014c |
| Windows 事件日誌（預設） | – |
| 卡巴斯基安全管理中心事件日誌（預設） | ✓ |

### 該物件在卡巴斯基私有安全網路允許清單中

| 狀態 | ⓘ |
| --- | --- |
| 元件 | 檔案威脅防護<br>Web 威脅防護<br>郵件威脅防護<br>AMSI 防護<br>主機入侵防禦<br>惡意軟體掃描 |
| Windows 事件 ID | 340 |
| 卡巴斯基安全管理中心事件 ID | 00000154 |
| Windows 事件日誌（預設） | ✓ |
| 卡巴斯基安全管理中心事件日誌（預設） | ✓ |

### 物件已重新命名

| 狀態 | ⓘ |
| --- | --- |
| 元件 | 郵件威脅防護<br>弱點利用防禦<br>行為偵測<br>加密軟體防護<br>惡意軟體掃描 |
| Windows 事件 ID | 329 |
| 卡巴斯基安全管理中心事件 ID | 00000149 |
| Windows 事件日誌（預設） | – |
| 卡巴斯基安全管理中心事件日誌（預設） | ✓ |

### 物件已處理

| 狀態 | ⓘ |
| --- | --- |
| 元件 | 主機入侵防禦<br>檔案威脅防護<br>Web 威脅防護<br>郵件威脅防護<br>惡意軟體掃描 |
| Windows 事件 ID | 301 |
| 卡巴斯基安全管理中心事件 ID | – |
| Windows 事件日誌（預設） | ✓ |
| 卡巴斯基安全管理中心事件日誌（預設） | – |

### 已略過物件

| 狀態 | |
|---|---|
| 元件 | 主機入侵防禦<br>檔案威脅防護<br>AMSI 防護<br>惡意軟體掃描 |
| Windows 事件 ID | 315 |
| 卡巴斯基安全管理中心事件 ID | – |
| Windows 事件日誌（預設） | ✓ |
| 卡巴斯基安全管理中心事件日誌（預設） | – |

## 偵測到壓縮檔案

| 狀態 | |
|---|---|
| 元件 | 主機入侵防禦<br>檔案威脅防護<br>Web 威脅防護<br>郵件威脅防護<br>AMSI 防護<br>惡意軟體掃描 |
| Windows 事件 ID | 318 |
| 卡巴斯基安全管理中心事件 ID | – |
| Windows 事件日誌（預設） | ✓ |
| 卡巴斯基安全管理中心事件日誌（預設） | – |

## 偵測到封裝物件

| 狀態 | |
|---|---|
| 元件 | 主機入侵防禦<br>檔案威脅防護<br>Web 威脅防護<br>郵件威脅防護<br>AMSI 防護<br>惡意軟體掃描 |
| Windows 事件 ID | 319 |
| 卡巴斯基安全管理中心事件 ID | – |
| Windows 事件日誌（預設） | ✓ |
| 卡巴斯基安全管理中心事件日誌（預設） | – |

## 已處理連結

| 狀態 | |
|---|---|
| 元件 | Web 威脅防護 |
| Windows 事件 ID | 361 |
| 卡巴斯基安全管理中心事件 ID | – |
| Windows 事件日誌（預設） | ✓ |
| 卡巴斯基安全管理中心事件日誌（預設） | – |

## 已允許應用程式啟動

| 狀態 | |
|---|---|
| 元件 | 應用程式控制 |

| | |
|---|---|
| Windows 事件 ID | 701 |
| 卡巴斯基安全管理中心事件 ID | – |
| Windows 事件日誌（預設） | ✓ |
| 卡巴斯基安全管理中心事件日誌（預設） | – |

### 已選擇更新來源

| | |
|---|---|
| 狀態 | ⓘ |
| 元件 | 更新 |
| Windows 事件 ID | 1001 |
| 卡巴斯基安全管理中心事件 ID | – |
| Windows 事件日誌（預設） | ✓ |
| 卡巴斯基安全管理中心事件日誌（預設） | – |

### 已選擇代理伺服器

| | |
|---|---|
| 狀態 | ⓘ |
| 元件 | 更新 |
| Windows 事件 ID | 1002 |
| 卡巴斯基安全管理中心事件 ID | – |
| Windows 事件日誌（預設） | ✓ |
| 卡巴斯基安全管理中心事件日誌（預設） | – |

### 該連結在卡巴斯基私有安全網路允許清單中

| | |
|---|---|
| 狀態 | ⓘ |
| 元件 | Web 威脅防護 |
| Windows 事件 ID | 370 |
| 卡巴斯基安全管理中心事件 ID | 00000172 |
| Windows 事件日誌（預設） | ✓ |
| 卡巴斯基安全管理中心事件日誌（預設） | ✓ |

### 應用程式被放置在受信任群組

| | |
|---|---|
| 狀態 | ⓘ |
| 元件 | 主機入侵防禦 |
| Windows 事件 ID | 401 |
| 卡巴斯基安全管理中心事件 ID | 00000191 |
| Windows 事件日誌（預設） | – |
| 卡巴斯基安全管理中心事件日誌（預設） | ✓ |

### 應用程式被放置在受限制群組

| | |
|---|---|
| 狀態 | ⓘ |
| 元件 | 主機入侵防禦 |

| | |
|---|---|
| Windows 事件 ID | 402 |
| 卡巴斯基安全管理中心事件 ID | 00000192 |
| Windows 事件日誌（預設） | – |
| 卡巴斯基安全管理中心事件日誌（預設） | ✓ |

## 主機入侵防禦已觸發

| | |
|---|---|
| 狀態 | ⓘ |
| 元件 | 主機入侵防禦 |
| Windows 事件 ID | 403 |
| 卡巴斯基安全管理中心事件 ID | 00000193 |
| Windows 事件日誌（預設） | – |
| 卡巴斯基安全管理中心事件日誌（預設） | ✓ |

## 檔案已還原

| | |
|---|---|
| 狀態 | ⓘ |
| 元件 | 行為偵測<br>加密軟體防護<br>弱點利用防禦<br>主機入侵防禦 |
| Windows 事件 ID | 457 |
| 卡巴斯基安全管理中心事件 ID | 000001c9 |
| Windows 事件日誌（預設） | – |
| 卡巴斯基安全管理中心事件日誌（預設） | ✓ |

## 登錄檔值已還原

| | |
|---|---|
| 狀態 | ⓘ |
| 元件 | 行為偵測<br>弱點利用防禦 |
| Windows 事件 ID | 458 |
| 卡巴斯基安全管理中心事件 ID | 000001ca |
| Windows 事件日誌（預設） | – |
| 卡巴斯基安全管理中心事件日誌（預設） | – |

## 登錄檔值已刪除

| | |
|---|---|
| 狀態 | ⓘ |
| 元件 | 行為偵測<br>弱點利用防禦 |
| Windows 事件 ID | 459 |
| 卡巴斯基安全管理中心事件 ID | 000001cb |
| Windows 事件日誌（預設） | – |
| 卡巴斯基安全管理中心事件日誌（預設） | – |

## 已略過處理程序操作

| | |
|---|---|
| 狀態 | ⓘ |
| 元件 | 自適應異常控制 |
| Windows 事件 ID | 2201 |
| 卡巴斯基安全管理中心事件 ID | GNRL_EV_ADSEC_DETECT |
| 事件參數 | • GNRL_EA_PARAM_1 是適應性異常控制規則的名稱。<br>• GNRL_EA_PARAM_2 是啟發式規則的 ID。<br>• GNRL_EA_PARAM_3 是工作階段使用者的名稱。<br>• GNRL_EA_PARAM_4 是來源處理程序。<br>• GNRL_EA_PARAM_5 是來源物件。<br>• GNRL_EA_PARAM_6 是目標處理程序。<br>• GNRL_EA_PARAM_7 是目標物件。<br>• GNRL_EA_PARAM_8 是被偵測到物件的其它資訊：來源處理程序 / 物件和目標處理程序 / 物件的雜湊。處理程序被封鎖 (verdict_type): true 或 false。使用者安全 ID (SID)。 |
| Windows 事件日誌（預設） | – |
| 卡巴斯基安全管理中心事件日誌（預設） | ✓ |

## 鍵盤已授權

| | |
|---|---|
| 狀態 | ⓘ |
| 元件 | BadUSB 攻擊防護 |
| Windows 事件 ID | 2050 |
| 卡巴斯基安全管理中心事件 ID | 00000802 |
| Windows 事件日誌（預設） | – |
| 卡巴斯基安全管理中心事件日誌（預設） | ✓ |

## 網路活動已允許

| | |
|---|---|
| 狀態 | ⓘ |
| 元件 | 防火牆 |
| Windows 事件 ID | 601 |
| 卡巴斯基安全管理中心事件 ID | 00000259 |
| Windows 事件日誌（預設） | – |
| 卡巴斯基安全管理中心事件日誌（預設） | – |

## 禁止應用程式在測試模式下啟動

| | |
|---|---|
| 狀態 | ⓘ |
| 元件 | 應用程式控制 |
| Windows 事件 ID | 703 |
| 卡巴斯基安全管理中心事件 ID | GNRL_EV_APP_LAUNCH_TESTED_DENIED |
| 事件參數 | • GNRL_EA_PARAM_2 是工作階段使用者的名稱。<br>• GNRL_EA_PARAM_3 是手動建立的類別識別符。<br>• GNRL_EA_PARAM_4 是帳戶安全識別符 (SID)。<br>• GNRL_EA_PARAM_5 是有關應用程式的數位簽章的資訊。<br>• GNRL_EA_PARAM_6 是應用程式的可執行檔（例如，chrome.exe）。<br>• GNRL_EA_PARAM_7 是可執行檔路徑。<br>• GNRL_EA_PARAM_8 是物件的雜湊 (SHA256)。<br>• GNRL_EA_PARAM_9 是使用者努力執行的應用程式的版本。 |

| | |
|---|---|
| Windows 事件日誌（預設） | – |
| 卡巴斯基安全管理中心事件日誌（預設） | ✓ |

## 允許應用程式在測試模式下啟動

| | |
|---|---|
| 狀態 | ⓘ |
| 元件 | 應用程式控制 |
| Windows 事件 ID | 704 |
| 卡巴斯基安全管理中心事件 ID | GNRL_EV_APP_LAUNCH_TESTED_ALLOW |
| 事件參數 | • GNRL_EA_PARAM_2 是工作階段使用者的名稱。<br>• GNRL_EA_PARAM_3 是手動建立的類別識別符。<br>• GNRL_EA_PARAM_4 是帳戶安全識別符 (SID)。<br>• GNRL_EA_PARAM_5 是有關應用程式的數位簽章的資訊。 |
| Windows 事件日誌（預設） | – |
| 卡巴斯基安全管理中心事件日誌（預設） | – |

## 允許頁面已開啟

| | |
|---|---|
| 狀態 | ⓘ |
| 元件 | Web 控制 |
| Windows 事件 ID | 751 |
| 卡巴斯基安全管理中心事件 ID | 000002f4 |
| Windows 事件日誌（預設） | – |
| 卡巴斯基安全管理中心事件日誌（預設） | – |

## 已允許對裝置進行操作

| | |
|---|---|
| 狀態 | ⓘ |
| 元件 | 裝置控制 |
| Windows 事件 ID | 801 |
| 卡巴斯基安全管理中心事件 ID | 00000321 |
| Windows 事件日誌（預設） | – |
| 卡巴斯基安全管理中心事件日誌（預設） | – |

## 檔案操作已執行

| | |
|---|---|
| 狀態 | ⓘ |
| 元件 | 裝置控制 |
| Windows 事件 ID | 808 |
| 卡巴斯基安全管理中心事件 ID | GNRL_EV_USB_FILE_OPERATION |
| 事件參數 | • GNRL_EA_PARAM_1 是檔案操作（寫入或刪除）。<br>• GNRL_EA_PARAM_2 是檔案路徑。<br>• GNRL_EA_PARAM_3 是裝置名稱。<br>• GNRL_EA_PARAM_4 是工作階段使用者的名稱。<br>• GNRL_EA_PARAM_5 是硬體 ID (HWID)。 |
| Windows 事件日誌（預設） | – |
| 卡巴斯基安全管理中心事件日誌（預設） | – |

## 沒有可用更新

| 狀態 | ⓘ |
| --- | --- |
| 元件 | 更新 |
| Windows 事件 ID | 1020 |
| 卡巴斯基安全管理中心事件 ID | 000003fc |
| Windows 事件日誌（預設） | – |
| 卡巴斯基安全管理中心事件日誌（預設） | – |

## 已成功完成更新發佈

| 狀態 | ⓘ |
| --- | --- |
| 元件 | 更新 |
| Windows 事件 ID | 1022 |
| 卡巴斯基安全管理中心事件 ID | 000003fe |
| Windows 事件日誌（預設） | – |
| 卡巴斯基安全管理中心事件日誌（預設） | – |

## 正在下載檔案

| 狀態 | ⓘ |
| --- | --- |
| 元件 | 更新 |
| Windows 事件 ID | 1003 |
| 卡巴斯基安全管理中心事件 ID | – |
| Windows 事件日誌（預設） | ✓ |
| 卡巴斯基安全管理中心事件日誌（預設） | – |

## 已下載檔案

| 狀態 | ⓘ |
| --- | --- |
| 元件 | 更新 |
| Windows 事件 ID | 1004 |
| 卡巴斯基安全管理中心事件 ID | – |
| Windows 事件日誌（預設） | ✓ |
| 卡巴斯基安全管理中心事件日誌（預設） | – |

## 已安裝檔案

| 狀態 | ⓘ |
| --- | --- |
| 元件 | 更新 |
| Windows 事件 ID | 1005 |
| 卡巴斯基安全管理中心事件 ID | – |
| Windows 事件日誌（預設） | ✓ |
| 卡巴斯基安全管理中心事件日誌（預設） | – |

## 已更新檔案

| 狀態 | ⓘ |
| --- | --- |
| 元件 | 更新 |
| Windows 事件 ID | 1006 |
| 卡巴斯基安全管理中心事件 ID | – |
| Windows 事件日誌（預設） | ✓ |
| 卡巴斯基安全管理中心事件日誌（預設） | – |

### 由於更新錯誤，檔案已回溯

| 狀態 | ⓘ |
| --- | --- |
| 元件 | 更新 |
| Windows 事件 ID | 1007 |
| 卡巴斯基安全管理中心事件 ID | – |
| Windows 事件日誌（預設） | ✓ |
| 卡巴斯基安全管理中心事件日誌（預設） | – |

### 正在更新檔案

| 狀態 | ⓘ |
| --- | --- |
| 元件 | 更新 |
| Windows 事件 ID | 1008 |
| 卡巴斯基安全管理中心事件 ID | – |
| Windows 事件日誌（預設） | ✓ |
| 卡巴斯基安全管理中心事件日誌（預設） | – |

### 正在發佈更新

| 狀態 | ⓘ |
| --- | --- |
| 元件 | 更新 |
| Windows 事件 ID | 1009 |
| 卡巴斯基安全管理中心事件 ID | – |
| Windows 事件日誌（預設） | ✓ |
| 卡巴斯基安全管理中心事件日誌（預設） | – |

### 正在回溯檔案

| 狀態 | ⓘ |
| --- | --- |
| 元件 | 更新 |
| Windows 事件 ID | 1010 |
| 卡巴斯基安全管理中心事件 ID | – |
| Windows 事件日誌（預設） | ✓ |
| 卡巴斯基安全管理中心事件日誌（預設） | – |

### 正在建立下載檔案清單

| 狀態 | ⓘ |
| --- | --- |
| 元件 | 更新 |
| Windows 事件 ID | 1013 |
| 卡巴斯基安全管理中心事件 ID | – |
| Windows 事件日誌（預設） | ✓ |
| 卡巴斯基安全管理中心事件日誌（預設） | – |

### 正在下載修補程式

| 狀態 | ⓘ |
| --- | --- |
| 元件 | 更新 |
| Windows 事件 ID | 2150 |
| 卡巴斯基安全管理中心事件 ID | – |
| Windows 事件日誌（預設） | ✓ |
| 卡巴斯基安全管理中心事件日誌（預設） | – |

### 正在安裝修補程式

| 狀態 | ⓘ |
| --- | --- |
| 元件 | 更新 |
| Windows 事件 ID | 2151 |
| 卡巴斯基安全管理中心事件 ID | – |
| Windows 事件日誌（預設） | ✓ |
| 卡巴斯基安全管理中心事件日誌（預設） | – |

### 已安裝修補程式

| 狀態 | ⓘ |
| --- | --- |
| 元件 | 更新 |
| Windows 事件 ID | 2152 |
| 卡巴斯基安全管理中心事件 ID | – |
| Windows 事件日誌（預設） | ✓ |
| 卡巴斯基安全管理中心事件日誌（預設） | – |

### 正在回溯修補程式

| 狀態 | ⓘ |
| --- | --- |
| 元件 | 更新 |
| Windows 事件 ID | 2154 |
| 卡巴斯基安全管理中心事件 ID | – |
| Windows 事件日誌（預設） | ✓ |
| 卡巴斯基安全管理中心事件日誌（預設） | – |

### 已回溯修補程式

| 狀態 | ⓘ |
| --- | --- |
| 元件 | 更新 |
| Windows 事件 ID | 2155 |
| 卡巴斯基安全管理中心事件 ID | – |
| Windows 事件日誌（預設） | ✓ |
| 卡巴斯基安全管理中心事件日誌（預設） | – |

### 已開始套用檔案加密/解密規則

| 狀態 | ⓘ |
| --- | --- |
| 元件 | 資料加密 |
| Windows 事件 ID | 901 |
| 卡巴斯基安全管理中心事件 ID | 00000385 |
| Windows 事件日誌（預設） | – |
| 卡巴斯基安全管理中心事件日誌（預設） | ✓ |

### 已完成套用檔案加密/解密規則

| 狀態 | ⓘ |
| --- | --- |
| 元件 | 資料加密 |
| Windows 事件 ID | 902 |
| 卡巴斯基安全管理中心事件 ID | 00000386 |
| Windows 事件日誌（預設） | – |
| 卡巴斯基安全管理中心事件日誌（預設） | ✓ |

### 已還原套用檔案加密/解密規則

| 狀態 | ⓘ |
| --- | --- |
| 元件 | 資料加密 |
| Windows 事件 ID | 905 |
| 卡巴斯基安全管理中心事件 ID | – |
| Windows 事件日誌（預設） | ✓ |
| 卡巴斯基安全管理中心事件日誌（預設） | – |

### 檔案加密/解密已啟動

| 狀態 | ⓘ |
| --- | --- |
| 元件 | 資料加密 |
| Windows 事件 ID | 910 |
| 卡巴斯基安全管理中心事件 ID | – |
| Windows 事件日誌（預設） | ✓ |
| 卡巴斯基安全管理中心事件日誌（預設） | – |

### 已完成檔案加密/解密

| 狀態 | ⓘ |
| --- | --- |
| 元件 | 資料加密 |
| Windows 事件 ID | 911 |
| 卡巴斯基安全管理中心事件 ID | – |
| Windows 事件日誌（預設） | ✓ |
| 卡巴斯基安全管理中心事件日誌（預設） | – |

### 檔案未被加密，因其屬於排除項目的檔案

| 狀態 | ⓘ |
| --- | --- |
| 元件 | 資料加密 |
| Windows 事件 ID | 913 |
| 卡巴斯基安全管理中心事件 ID | – |
| Windows 事件日誌（預設） | ✓ |
| 卡巴斯基安全管理中心事件日誌（預設） | – |

### 已啟用攜帶模式

| 狀態 | ⓘ |
| --- | --- |
| 元件 | 資料加密 |
| Windows 事件 ID | 950 |
| 卡巴斯基安全管理中心事件 ID | – |
| Windows 事件日誌（預設） | ✓ |
| 卡巴斯基安全管理中心事件日誌（預設） | – |

### 已停用攜帶模式

| 狀態 | ⓘ |
| --- | --- |
| 元件 | 資料加密 |
| Windows 事件 ID | 952 |
| 卡巴斯基安全管理中心事件 ID | – |
| Windows 事件日誌（預設） | ✓ |
| 卡巴斯基安全管理中心事件日誌（預設） | – |

### 已開始裝置加密/解密

| 狀態 | ⓘ |
| --- | --- |
| 元件 | 資料加密 |
| Windows 事件 ID | 1301 |
| 卡巴斯基安全管理中心事件 ID | – |
| Windows 事件日誌（預設） | ✓ |
| 卡巴斯基安全管理中心事件日誌（預設） | – |

### 已完成裝置加密/解密

| 狀態 | ⓘ |
| --- | --- |
| 元件 | 資料加密 |
| Windows 事件 ID | 1302 |
| 卡巴斯基安全管理中心事件 ID | – |
| Windows 事件日誌（預設） | ✓ |
| 卡巴斯基安全管理中心事件日誌（預設） | – |

### 已還原裝置加密/解密

| 狀態 | ⓘ |
| --- | --- |
| 元件 | 資料加密 |
| Windows 事件 ID | 1304 |
| 卡巴斯基安全管理中心事件 ID | – |
| Windows 事件日誌（預設） | ✓ |
| 卡巴斯基安全管理中心事件日誌（預設） | – |

### 裝置未加密

| 狀態 | ⓘ |
| --- | --- |
| 元件 | 資料加密 |
| Windows 事件 ID | 1307 |
| 卡巴斯基安全管理中心事件 ID | – |
| Windows 事件日誌（預設） | ✓ |
| 卡巴斯基安全管理中心事件日誌（預設） | – |

### 已將裝置加密/解密過程切換至主動模式

| 狀態 | ⓘ |
| --- | --- |
| 元件 | 資料加密 |
| Windows 事件 ID | 1308 |
| 卡巴斯基安全管理中心事件 ID | – |
| Windows 事件日誌（預設） | ✓ |
| 卡巴斯基安全管理中心事件日誌（預設） | – |

### 已將裝置加密/解密過程切換至被動模式

| 狀態 | ⓘ |
| --- | --- |
| 元件 | 資料加密 |
| Windows 事件 ID | 1309 |
| 卡巴斯基安全管理中心事件 ID | – |
| Windows 事件日誌（預設） | ✓ |
| 卡巴斯基安全管理中心事件日誌（預設） | – |

### 加密模組已載入

| 狀態 | |
|---|---|
| 元件 | 資料加密 |
| Windows 事件 ID | 1310 |
| 卡巴斯基安全管理中心事件 ID | 0000051e |
| Windows 事件日誌（預設） | – |
| 卡巴斯基安全管理中心事件日誌（預設） | – |

### 已建立新的身分驗證代理帳戶

| 狀態 | |
|---|---|
| 元件 | 資料加密 |
| Windows 事件 ID | 1330 |
| 卡巴斯基安全管理中心事件 ID | 00000532 |
| Windows 事件日誌（預設） | – |
| 卡巴斯基安全管理中心事件日誌（預設） | – |

### 已刪除身分驗證代理帳戶

| 狀態 | |
|---|---|
| 元件 | 資料加密 |
| Windows 事件 ID | 1331 |
| 卡巴斯基安全管理中心事件 ID | 00000533 |
| Windows 事件日誌（預設） | – |
| 卡巴斯基安全管理中心事件日誌（預設） | – |

### 身分驗證代理帳戶密碼已變更

| 狀態 | |
|---|---|
| 元件 | 資料加密 |
| Windows 事件 ID | 1332 |
| 卡巴斯基安全管理中心事件 ID | 00000534 |
| Windows 事件日誌（預設） | – |
| 卡巴斯基安全管理中心事件日誌（預設） | – |

### 成功使用身分驗證代理進行登入

| 狀態 | |
|---|---|
| 元件 | 資料加密 |
| Windows 事件 ID | 1333 |
| 卡巴斯基安全管理中心事件 ID | 00000535 |
| Windows 事件日誌（預設） | – |
| 卡巴斯基安全管理中心事件日誌（預設） | – |

### 身分驗證代理登入嘗試失敗

| 狀態 | |
|---|---|
| 元件 | 資料加密 |
| Windows 事件 ID | 1334 |
| 卡巴斯基安全管理中心事件 ID | 00000536 |
| Windows 事件日誌（預設） | – |
| 卡巴斯基安全管理中心事件日誌（預設） | – |

### 使用用於請求加密裝置存取權限的方式存取硬碟磁碟機

| 狀態 | |
|---|---|
| 元件 | 資料加密 |
| Windows 事件 ID | 1335 |
| 卡巴斯基安全管理中心事件 ID | 00000537 |
| Windows 事件日誌（預設） | – |
| 卡巴斯基安全管理中心事件日誌（預設） | – |

### 無法使用用於請求加密裝置存取權限的方式存取硬碟磁碟機

| 狀態 | |
|---|---|
| 元件 | 資料加密 |
| Windows 事件 ID | 1336 |
| 卡巴斯基安全管理中心事件 ID | 00000538 |
| Windows 事件日誌（預設） | – |
| 卡巴斯基安全管理中心事件日誌（預設） | – |

### 未新增帳戶，此帳戶已存在

| 狀態 | |
|---|---|
| 元件 | 資料加密 |
| Windows 事件 ID | 1337 |
| 卡巴斯基安全管理中心事件 ID | 00000539 |
| Windows 事件日誌（預設） | – |
| 卡巴斯基安全管理中心事件日誌（預設） | – |

### 未修改帳戶，此帳戶不存在

| 狀態 | |
|---|---|
| 元件 | 資料加密 |
| Windows 事件 ID | 1338 |
| 卡巴斯基安全管理中心事件 ID | 0000053a |
| Windows 事件日誌（預設） | – |
| 卡巴斯基安全管理中心事件日誌（預設） | – |

### 未刪除帳戶，此帳戶不存在

| 狀態 | ⓘ |
| --- | --- |
| 元件 | 資料加密 |
| Windows 事件 ID | 1339 |
| 卡巴斯基安全管理中心事件 ID | 0000053b |
| Windows 事件日誌（預設） | – |
| 卡巴斯基安全管理中心事件日誌（預設） | – |

### FDE 升級成功

| 狀態 | ⓘ |
| --- | --- |
| 元件 | 資料加密 |
| Windows 事件 ID | 1341 |
| 卡巴斯基安全管理中心事件 ID | 0000053d |
| Windows 事件日誌（預設） | ✓ |
| 卡巴斯基安全管理中心事件日誌（預設） | ✓ |

### FDE 升級回溯成功

| 狀態 | ⓘ |
| --- | --- |
| 元件 | 資料加密 |
| Windows 事件 ID | 1343 |
| 卡巴斯基安全管理中心事件 ID | 0000053f |
| Windows 事件日誌（預設） | ✓ |
| 卡巴斯基安全管理中心事件日誌（預設） | ✓ |

### 無法從 WinRE 映像中移除卡巴斯基磁碟加密驅動程式

| 狀態 | ⓘ |
| --- | --- |
| 元件 | 資料加密 |
| Windows 事件 ID | 1346 |
| 卡巴斯基安全管理中心事件 ID | 00000542 |
| Windows 事件日誌（預設） | ✓ |
| 卡巴斯基安全管理中心事件日誌（預設） | ✓ |

### BitLocker 還原金鑰已變更

| 狀態 | ⓘ |
| --- | --- |
| 元件 | 資料加密 |
| Windows 事件 ID | 1370 |
| 卡巴斯基安全管理中心事件 ID | 0000055a |
| Windows 事件日誌（預設） | ✓ |
| 卡巴斯基安全管理中心事件日誌（預設） | ✓ |

### BitLocker 密碼/PIN 已變更

| 狀態 | ⓘ |
| --- | --- |
| 元件 | 資料加密 |
| Windows 事件 ID | 1371 |
| 卡巴斯基安全管理中心事件 ID | 0000055b |
| Windows 事件日誌（預設） | ✓ |
| 卡巴斯基安全管理中心事件日誌（預設） | ✓ |

### BitLocker 還原金鑰已儲存到卸除式磁碟機

| 狀態 | ⓘ |
| --- | --- |
| 元件 | 資料加密 |
| Windows 事件 ID | 1372 |
| 卡巴斯基安全管理中心事件 ID | 0000055c |
| Windows 事件日誌（預設） | ✓ |
| 卡巴斯基安全管理中心事件日誌（預設） | ✓ |

### 對來自 Kaspersky Anti Targeted Attack Platform 伺服器的工作的處理處於非作用中狀態

| 狀態 | ⓘ |
| --- | --- |
| 元件 | Endpoint Sensor |
| Windows 事件 ID | 2103 |
| 卡巴斯基安全管理中心事件 ID | 00000837 |
| Windows 事件日誌（預設） | – |
| 卡巴斯基安全管理中心事件日誌（預設） | ✓ |

### Endpoint Sensor 已連線到伺服器

| 狀態 | ⓘ |
| --- | --- |
| 元件 | Endpoint Sensor |
| Windows 事件 ID | 2101 |
| 卡巴斯基安全管理中心事件 ID | 00000835 |
| Windows 事件日誌（預設） | – |
| 卡巴斯基安全管理中心事件日誌（預設） | ✓ |

### 已還原與 Kaspersky Anti Targeted Attack Platform 伺服器的連線

| 狀態 | ⓘ |
| --- | --- |
| 元件 | Endpoint Sensor |
| Windows 事件 ID | 2102 |
| 卡巴斯基安全管理中心事件 ID | 00000836 |
| Windows 事件日誌（預設） | – |
| 卡巴斯基安全管理中心事件日誌（預設） | ✓ |

### 正在處理來自 Kaspersky Anti Targeted Attack Platform 伺服器的工作

| 狀態 | ⓘ |
| --- | --- |
| 元件 | Endpoint Sensor |
| Windows 事件 ID | 2104 |
| 卡巴斯基安全管理中心事件 ID | 00000838 |
| Windows 事件日誌（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 | 抹除資料 |
| Windows 事件 ID | 2251 |
| 卡巴斯基安全管理中心事件 ID | 000008cb |
| Windows 事件日誌（預設） | – |
| 卡巴斯基安全管理中心事件日誌（預設） | – |

### 抹除工作統計資訊

| 狀態 | ⓘ |
| --- | --- |
| 元件 | Endpoint Detection and Response Expert (on-premise) |
| Windows 事件 ID | 2853 |
| 卡巴斯基安全管理中心事件 ID | 00000b25 |
| Windows 事件日誌（預設） | ✓ |
| 卡巴斯基安全管理中心事件日誌（預設） | ✓ |

| 狀態 | ⓘ |
| --- | --- |
| 元件 | 抹除資料 |
| Windows 事件 ID | 2253 |
| 卡巴斯基安全管理中心事件 ID | 000008cd |
| Windows 事件日誌（預設） | – |
| 卡巴斯基安全管理中心事件日誌（預設） | ✓ |

### 物件已隔離 (Sandbox)

| 狀態 | ⓘ |
| --- | --- |
| 元件 | Sandbox |
| Windows 事件 ID | 2602 |
| 卡巴斯基安全管理中心事件 ID | 00000a2a |
| Windows 事件日誌（預設） | ✓ |
| 卡巴斯基安全管理中心事件日誌（預設） | ✓ |

### 物件已刪除 (Sandbox)

| 狀態 | ⓘ |
| --- | --- |
| 元件 | Sandbox |

| | |
|---|---|
| Windows 事件 ID | 2604 |
| 卡巴斯基安全管理中心事件 ID | 00000a2c |
| Windows 事件日誌（預設） | ✓ |
| 卡巴斯基安全管理中心事件日誌（預設） | – |

## IOC 掃描已啟動

| | |
|---|---|
| 狀態 | ⓘ |
| 元件 | Endpoint Detection and Response |
| Windows 事件 ID | 2652 |
| 卡巴斯基安全管理中心事件 ID | 00000a5c |
| Windows 事件日誌（預設） | ✓ |
| 卡巴斯基安全管理中心事件日誌（預設） | ✓ |

## IOC 掃描已完成

| | |
|---|---|
| 狀態 | ⓘ |
| 元件 | Endpoint Detection and Response |
| Windows 事件 ID | 2653 |
| 卡巴斯基安全管理中心事件 ID | 00000a5d |
| Windows 事件日誌（預設） | ✓ |
| 卡巴斯基安全管理中心事件日誌（預設） | ✓ |

## 物件已隔離 (Endpoint Detection and Response)

| | |
|---|---|
| 狀態 | ⓘ |
| 元件 | Endpoint Detection and Response |
| Windows 事件 ID | 2555 |
| 卡巴斯基安全管理中心事件 ID | 000009fb |
| Windows 事件日誌（預設） | ✓ |
| 卡巴斯基安全管理中心事件日誌（預設） | ✓ |

## 物件已刪除 (Endpoint Detection and Response)

| | |
|---|---|
| 狀態 | ⓘ |
| 元件 | Endpoint Detection and Response |
| Windows 事件 ID | 2557 |
| 卡巴斯基安全管理中心事件 ID | 000009fd |
| Windows 事件日誌（預設） | ✓ |
| 卡巴斯基安全管理中心事件日誌（預設） | ✓ |

## 應用程式元件已成功變更

| | |
|---|---|
| 狀態 | ⓘ |
| 元件 | 系統稽核 |

| | |
|---|---|
| Windows 事件 ID | 1402 |
| 卡巴斯基安全管理中心事件 ID | 0000057a |
| Windows 事件日誌（預設） | – |
| 卡巴斯基安全管理中心事件日誌（預設） | ✓ |

| | |
|---|---|
| 狀態 | ⓘ |
| 元件 | Sandbox |
| Windows 事件 ID | 2606 |
| 卡巴斯基安全管理中心事件 ID | – |
| Windows 事件日誌（預設） | ✓ |
| 卡巴斯基安全管理中心事件日誌（預設） | – |

| | |
|---|---|
| 狀態 | ⓘ |
| 元件 | Sandbox |
| Windows 事件 ID | 2609 |
| 卡巴斯基安全管理中心事件 ID | – |
| Windows 事件日誌（預設） | ✓ |
| 卡巴斯基安全管理中心事件日誌（預設） | – |

| | |
|---|---|
| 狀態 | ⓘ |
| 元件 | Sandbox |
| Windows 事件 ID | 2610 |
| 卡巴斯基安全管理中心事件 ID | – |
| Windows 事件日誌（預設） | ✓ |
| 卡巴斯基安全管理中心事件日誌（預設） | – |

| | |
|---|---|
| 狀態 | ⓘ |
| 元件 | Sandbox |
| Windows 事件 ID | 2616 |
| 卡巴斯基安全管理中心事件 ID | – |
| Windows 事件日誌（預設） | ✓ |
| 卡巴斯基安全管理中心事件日誌（預設） | – |

**您的裝置連線到的管理伺服器被設定為受信任。**

| | |
|---|---|
| 狀態 | ⓘ |
| 元件 | 管理伺服器連線防護 |
| Windows 事件 ID | 3300 |
| 卡巴斯基安全管理中心事件 ID | 00000ce4 |
| Windows 事件日誌（預設） | – |
| 卡巴斯基安全管理中心事件日誌（預設） | ✓ |

**您的裝置已被連線到新的受信任管理伺服器。**

| | |
|---|---|
| 狀態 | ⓘ |
| 元件 | 管理伺服器連線防護 |
| Windows 事件 ID | 3302 |
| 卡巴斯基安全管理中心事件 ID | 00000ce6 |
| Windows 事件日誌（預設） | – |
| 卡巴斯基安全管理中心事件日誌（預設） | ✓ |

### 您的裝置連線到的管理伺服器不再被設定為受信任。

| | |
|---|---|
| 狀態 | ⓘ |
| 元件 | 管理伺服器連線防護 |
| Windows 事件 ID | 3303 |
| 卡巴斯基安全管理中心事件 ID | 00000ce7 |
| Windows 事件日誌（預設） | – |
| 卡巴斯基安全管理中心事件日誌（預設） | ✓ |

## 異步 Sandbox 偵測

| | |
|---|---|
| 狀態 | ⓘ |
| 元件 | Sandbox |
| Windows 事件 ID | 2619 |
| 卡巴斯基安全管理中心事件 ID | GNRL_EV_APP_INCIDENT_OCCURED |
| 事件參數 | • GNRL_EA_PARAM_1 是Sandbox元件的參數。<br>• GNRL_EA_PARAM_2 是物件路徑。<br>• GNRL_EA_PARAM_3 是事件 ID。<br>• GNRL_EA_PARAM_4 是物件的雜湊 (SHA256)。 |
| Windows 事件日誌（預設） | – |
| 卡巴斯基安全管理中心事件日誌（預設） | ✓ |

### 掃描工作已被使用者成功傳送至 Sandbox

| | |
|---|---|
| 狀態 | ⓘ |
| 元件 | Sandbox |
| Windows 事件 ID | 2622 |
| 卡巴斯基安全管理中心事件 ID | 00000a3e |
| Windows 事件日誌（預設） | – |
| 卡巴斯基安全管理中心事件日誌（預設） | ✓ |

## 裝置已連接

| | |
|---|---|
| 狀態 | ⓘ |
| 元件 | 裝置控制 |
| Windows 事件 ID | 805 |
| 卡巴斯基安全管理中心事件 ID | GNRL_EV_DEVCTRL_DEV_PLUGGED |
| 事件參數 | • GNRL_EA_PARAM_1 是硬體 ID (HWID)。<br>• GNRL_EA_PARAM_2 是工作階段使用者的名稱。 |

| | |
|---|---|
| Windows 事件日誌（預設） | – |
| 卡巴斯基安全管理中心事件日誌（預設） | ✓ |

### 裝置已斷開

| | |
|---|---|
| 狀態 | ⓘ |
| 元件 | 裝置控制 |
| Windows 事件 ID | 806 |
| 卡巴斯基安全管理中心事件 ID | GNRL_EV_DEVCTRL_DEV_UNPLUGGED |
| 事件參數 | • GNRL_EA_PARAM_1 是硬體 ID (HWID)。<br>• GNRL_EA_PARAM_2 是工作階段使用者的名稱。 |
| Windows 事件日誌（預設） | – |
| 卡巴斯基安全管理中心事件日誌（預設） | ✓ |

### 移除先前版本的應用程式時發生錯誤

| | |
|---|---|
| 狀態 | ⓘ |
| 元件 | 系統稽核 |
| Windows 事件 ID | 246 |
| 卡巴斯基安全管理中心事件 ID | 000000f6 |
| Windows 事件日誌（預設） | ✓ |
| 卡巴斯基安全管理中心事件日誌（預設） | ✓ |

### 成功連線到 EDR Expert 伺服器

| | |
|---|---|
| 狀態 | ⓘ |
| 元件 | Endpoint Detection and Response Expert (on-premise) |
| Windows 事件 ID | 2853 |
| 卡巴斯基安全管理中心事件 ID | 00000b25 |
| Windows 事件日誌（預設） | ✓ |
| 卡巴斯基安全管理中心事件日誌（預設） | ✓ |

### 成功連線至 EDR Expert 回應伺服器

| | |
|---|---|
| 狀態 | ⓘ |
| 元件 | Endpoint Detection and Response Expert (on-premise) |
| Windows 事件 ID | 2853 |
| 卡巴斯基安全管理中心事件 ID | 00000b25 |
| Windows 事件日誌（預設） | ✓ |
| 卡巴斯基安全管理中心事件日誌（預設） | ✓ |

### 成功連線至 EDR Expert 遙測資料收集伺服器

| | |
|---|---|
| 狀態 | ⓘ |
| 元件 | Endpoint Detection and Response Expert (on-premise) |
| Windows 事件 ID | 2857 |

| | |
|---|---|
| 卡巴斯基安全管理中心事件 ID | 00000b26 |
| Windows 事件日誌（預設） | ✓ |
| 卡巴斯基安全管理中心事件日誌（預設） | ✓ |

### 成功連線至 NDR 伺服器

| | |
|---|---|
| 狀態 | ⓘ |
| 元件 | Network Detection and Response (KATA) |
| Windows 事件 ID | 3083 |
| 卡巴斯基安全管理中心事件 ID | 00000c0b |
| Windows 事件日誌（預設） | ✓ |
| 卡巴斯基安全管理中心事件日誌（預設） | ✓ |

### 允許啟動雲端服務用戶端應用程式

| | |
|---|---|
| 狀態 | ⓘ |
| 元件 | Cloud Discovery |
| Windows 事件 ID | 2210 |
| 卡巴斯基安全管理中心事件 ID | 000008a2 |
| Windows 事件日誌（預設） | – |
| 卡巴斯基安全管理中心事件日誌（預設） | ✓ |

### 允許存取雲端服務

| | |
|---|---|
| 狀態 | ⓘ |
| 元件 | Cloud Discovery |
| Windows 事件 ID | 2211 |
| 卡巴斯基安全管理中心事件 ID | 000008a3 |
| Windows 事件日誌（預設） | – |
| 卡巴斯基安全管理中心事件日誌（預設） | ✓ |

### 存取受防護區域

| | |
|---|---|
| 狀態 | ⓘ |
| 元件 | 系統稽核 |
| Windows 事件 ID | 2004 |
| 卡巴斯基安全管理中心事件 ID | 000007d4 |
| Windows 事件日誌（預設） | ✓ |
| 卡巴斯基安全管理中心事件日誌（預設） | ✓ |

### 偵測到對檔案或資料夾的變更

| | |
|---|---|
| 狀態 | ⓘ / ⚠ / ⓘ |
| 元件 | 系統完整性監控 |
| Windows 事件 ID | 2950 |

| | |
|---|---|
| 卡巴斯基安全管理中心事件 ID | 00000b86 |
| Windows 事件日誌（預設） | – |
| 卡巴斯基安全管理中心事件日誌（預設） | ✓ |

若要配置此事件的保留期，請前往政策的 **事件組態** 部分並設定一般系統完整性監控事件的保留期 – *偵測到對檔案或資料夾的變更*。

### 物件變更頻繁。事件彙總已啟動

| | |
|---|---|
| 狀態 | ⓘ / ⚠ / ⓘ |
| 元件 | 系統完整性監控 |
| Windows 事件 ID | 2955 |
| 卡巴斯基安全管理中心事件 ID | 00000b8b |
| Windows 事件日誌（預設） | – |
| 卡巴斯基安全管理中心事件日誌（預設） | ✓ |

### 彙總期間的物件修改報告

| | |
|---|---|
| 狀態 | ⓘ / ⚠ / ⓘ |
| 元件 | 系統完整性監控 |
| Windows 事件 ID | 2956 |
| 卡巴斯基安全管理中心事件 ID | 00000b8c |
| Windows 事件日誌（預設） | – |
| 卡巴斯基安全管理中心事件日誌（預設） | ✓ |

若要配置此事件的保留期，請前往政策的 **事件組態** 部分並設定一般系統完整性監控事件的保留期 – *偵測到對檔案或資料夾的變更*。

### 偵測到登錄檔變更

| | |
|---|---|
| 狀態 | ⓘ / ⚠ / ⓘ |
| 元件 | 系統完整性監控 |
| Windows 事件 ID | 2951 |
| 卡巴斯基安全管理中心事件 ID | 00000b87 |
| Windows 事件日誌（預設） | – |
| 卡巴斯基安全管理中心事件日誌（預設） | ✓ |

若要配置此事件的保留期，請前往政策的 **事件組態** 部分並設定一般系統完整性監控事件的保留期 – *偵測到對檔案或資料夾的變更*。

### 偵測到裝置連線 / 連線中斷

| | |
|---|---|
| 狀態 | ⓘ / ⚠ / ⓘ |
| 元件 | 系統完整性監控 |
| Windows 事件 ID | 2952 |
| 卡巴斯基安全管理中心事件 ID | 00000b88 |

| | |
|---|---|
| Windows 事件日誌（預設） | – |
| 卡巴斯基安全管理中心事件日誌（預設） | ✓ |

若要配置此事件的保留期，請前往政策的 **事件組態** 部分並設定一般系統完整性監控事件的保留期 – *偵測到對檔案或資料夾的變更*。

## 監控範圍包括不正確的物件

| | |
|---|---|
| 狀態 | ⓘ / ⚠ / ⓘ |
| 元件 | 系統完整性監控 |
| Windows 事件 ID | 2903 |
| 卡巴斯基安全管理中心事件 ID | 00000b89 |
| Windows 事件日誌（預設） | – |
| 卡巴斯基安全管理中心事件日誌（預設） | ✓ |

若要配置此事件的保留期，請前往政策的 **事件組態** 部分並設定一般系統完整性監控事件的保留期 – *偵測到對檔案或資料夾的變更*。

## 建立的基線

| | |
|---|---|
| 狀態 | ⓘ |
| 元件 | 系統完整性監控 |
| Windows 事件 ID | 2957 |
| 卡巴斯基安全管理中心事件 ID | 00000b8d |
| Windows 事件日誌（預設） | – |
| 卡巴斯基安全管理中心事件日誌（預設） | ✓ |

## 更新的基線

| | |
|---|---|
| 狀態 | ⓘ |
| 元件 | 系統完整性監控 |
| Windows 事件 ID | 2958 |
| 卡巴斯基安全管理中心事件 ID | 00000b8e |
| Windows 事件日誌（預設） | – |
| 卡巴斯基安全管理中心事件日誌（預設） | ✓ |

## 操作由受信任使用者執行

| | |
|---|---|
| 狀態 | ⓘ |
| 元件 | 系統完整性監控 |
| Windows 事件 ID | 2962 |
| 卡巴斯基安全管理中心事件 ID | 00000b92 |
| Windows 事件日誌（預設） | – |

| | |
|---|---|
| 卡巴斯基安全管理中心事件日誌（預設） | ✓ |

若要配置此事件的保留期，請前往政策的 **事件組態** 部分並設定一般系統完整性監控事件的保留期 – *偵測到對檔案或資料夾的變更*。

## 已連線到 SVM

| | |
|---|---|
| 狀態 | ⓘ |
| 元件 | Light Agent |
| Windows 事件 ID | 3152 |
| 卡巴斯基安全管理中心事件 ID | 00000c50 |
| Windows 事件日誌（預設） | – |
| 卡巴斯基安全管理中心事件日誌（預設） | ✓ |

## 一個新的臨時密碼已建立

| | |
|---|---|
| 狀態 | ⓘ |
| 元件 | 系統稽核 |
| Windows 事件 ID | 265 |
| 卡巴斯基安全管理中心事件 ID | 00000109 |
| Windows 事件日誌（預設） | – |
| 卡巴斯基安全管理中心事件日誌（預設） | ✓ |

## 已連線至 Integration Server

| | |
|---|---|
| 狀態 | ⓘ |
| 元件 | Light Agent |
| Windows 事件 ID | 3105 |
| 卡巴斯基安全管理中心事件 ID | 00000c21 |
| Windows 事件日誌（預設） | – |
| 卡巴斯基安全管理中心事件日誌（預設） | ✓ |

## 正在還原連線到 Intergration Server

| | |
|---|---|
| 狀態 | ⓘ |
| 元件 | Light Agent |
| Windows 事件 ID | 3104 |
| 卡巴斯基安全管理中心事件 ID | 00000c20 |
| Windows 事件日誌（預設） | – |
| 卡巴斯基安全管理中心事件日誌（預設） | ✓ |

## 成功連線至 KUMA 伺服器

| | |
|---|---|
| 狀態 | ⓘ |
| 元件 | KUMA 整合 |
| Windows 事件 ID | 2857 |

| | |
|---|---|
| 卡巴斯基安全管理中心事件 ID | 00000b29 |
| Windows 事件日誌（預設） | – |
| 卡巴斯基安全管理中心事件日誌（預設） | ✓ |

# 附錄 7。受支援的執行防護的檔案副檔名

Kaspersky Endpoint Security 支援禁止在某些應用程式中開啟 Office 格式檔案。有關受支援的檔案副檔名和應用程式的資訊請見下表。

受支援的執行防護的檔案副檔名

| 應用程式名稱 | 可執行檔 | 檔案副檔名 |
|---|---|---|
| Microsoft Word | winword.exe | rtf<br>doc<br>dot<br>docm<br>docx<br>dotx<br>dotm<br>docb |
| WordPad | wordpad.exe | docx<br>rtf |
| Microsoft Excel | excel.exe | xls<br>xlt<br>xlm<br>xlsx<br>xlsm<br>xltx<br>xltm<br>xlsb<br>xla<br>xlam<br>xll<br>xlw |
| Microsoft PowerPoint | powerpnt.exe | ppt<br>pot<br>pps<br>pptx<br>pptm<br>potx<br>potm<br>ppam<br>ppsx<br>ppsm<br>sldx<br>sldm |

| 應用程式名稱 | 可執行檔 | 檔案副檔名 |
| --- | --- | --- |
| Adobe Acrobat | acrord32.exe | pdf |
| Foxit PDF Reader | FoxitReader.exe | |
| STDU Viewer | STDUViewerApp.exe | |
| Microsoft Edge | MicrosoftEdge.exe | |
| Google Chrome | chrome.exe | |
| Mozilla Firefox | firefox.exe | |
| Yandex Browser | browser.exe | |
| Tor Browser | tor.exe | |

# 附錄 8。支援執行防止的指令碼解譯器

執行防護支援以下指令碼解譯器：

- AutoHotkey.exe
- AutoHotkeyA32.exe
- AutoHotkeyA64.exe
- AutoHotkeyU32.exe
- AutoHotkeyU64.exe
- InstallUtil.exe
- RegAsm.exe
- RegSvcs.exe
- autoit.exe
- cmd.exe
- control.exe
- cscript.exe
- hh.exe
- mmc.exe
- msbuild.exe
- mshta.exe
- msiexec.exe
- perl.exe
- powershell.exe

- python.exe
- reg.exe
- regedit.exe
- regedt32.exe
- regsvr32.exe
- ruby.exe
- rubyw.exe
- rundll32.exe
- runlegacycplelevated.exe
- wscript.exe
- wwahost.exe

執行防護支援與 Java 應用程式在 Java 執行階段環境中一起工作（java.exe 和 javaw.exe 處理程序）。

# 附錄 9。登錄檔中的IOC 掃描範圍 (RegistryItem)

當您將 **Windows 登錄檔 - RegistryItem** 資料類型新增至 IOC 掃描範圍時，預設 Kaspersky Endpoint Security 將掃描以下登錄機碼：

```
HKEY_CLASSES_ROOT\htafile

HKEY_CLASSES_ROOT\batfile

HKEY_CLASSES_ROOT\exefile

HKEY_CLASSES_ROOT\comfile

HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Lsa

HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Print\Monitors

HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\NetworkProvider

HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Class

HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\SecurityProviders

HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Terminal Server

HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Session Manager
```

```
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services

HKEY_LOCAL_MACHINE\Software\Classes\piffile

HKEY_LOCAL_MACHINE\Software\Classes\htafile

HKEY_LOCAL_MACHINE\Software\Classes\exefile

HKEY_LOCAL_MACHINE\Software\Classes\comfile

HKEY_LOCAL_MACHINE\Software\Classes\CLSID

HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run

HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\ShellServiceObjectDelayLoad

HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer

HKEY_LOCAL_MACHINE\Software\Wow6432Node\Microsoft\Windows\CurrentVersion\Run

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Active Setup\Installed Components

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Windows

HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Image File Execution
Options

HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Aedebug

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon
```

# 附錄 10。IOC 檔案要求

當建立 IOC 掃描工作時，請考量以下 IOC 檔案要求和限制：

- 應用程式在用於描述洩露指示器的開放標準 OpenIOC 版本 1.0 和 1.1 中支援具有 IOC 和 XML 延伸程式的 IOC 檔案。
- 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。
- 如果用命令行建立 *IOC 掃描* 工作時上傳 IOC 檔案而其中一些不受支援，當執行工作時，應用程式將僅使用受支援的 IOC 檔案。如果用命令行建立 *IOC 掃描*工作時您上傳的所有 IOC 檔案不受支援，工作仍然可以被執行，但是將不會偵測任何洩露指示器。無法使用網頁主控台或雲端主控台上傳不受支援的 IOC 檔案。
- 語義錯誤和不受支援的 IOC 字詞以及 IOC 檔案中的標籤不會引起工作執行失敗。在 IOC 檔案的此類區域中，應用程式會偵測到不符合。
- 在單個 IOC 掃描工作中使用的所有 IOC 檔案的識別符必須為唯一。如果有識別符一樣的 IOC 檔案，它可能會影響工作執行結果。

- 單個 IOC 檔案的大小不得超過 2 MB。使用更大的檔案將引起 IOC 掃描工作以錯誤終止。新增至 IOC 集合的所有檔案的總大小不應該超過 10 MB。如果所有檔案的總大小超過 10 Mb，則需要拆分 IOC 集合並建立多個 *IOC 掃描* 工作。

- 建議為每個威脅建立一個 IOC 檔案。這會讓分析*IOC 掃描*工作的結果更容易。

您可以點擊下面的連接下載該檔案，它包含一個表格，其中有 OpenIOC 標準的 IOC 字詞完整清單。



下載 IOC_TERMS.XLSX 檔案

應用程式對 OpenIOC 標準支援的功能和限制顯示在下表中。

對 OpenIOC 版本 1.0 和 1.1 支援的功能和限制。

| | |
|---|---|
| 受支援條件 | OpenIOC 1.0:<br><br>`is`<br>`isnot`（作為集合中的例外）<br>`contains`<br>`containsnot`（作為集合中的例外）<br>OpenIOC 1.1:<br><br>`is`<br>`contains`<br>`starts-with`<br>`ends-with`<br>`matches`<br>`greater-than`<br>`less-than`<br><br>對於電子郵件/* 條款，僅支援 `contains` 和 `is` 條件。為了使回溯 IOC 掃描正常運作，在使用 `is` 條件時，IOC 檔案中的電子郵件地址必須採用以下格式指定：`"name@example.org" <SMTP:name@example.org>`。當正常執行 *IOC 掃描* 工作時，只需按以下格式指定電子郵件地址即可：`name@example.org`。 |
| 受支援條件屬性 | OpenIOC 1.1:<br><br>`preserve-case`<br>`negate` |
| 受支援運算子 | `AND`<br>`OR` |
| 受支援資料類型 | `"date"`:日期（適用條件：`is`, `greater-than`, `less-than`）<br><br>`"int"`:整數（適用條件：`is`, `greater-than`, `less-than`）<br><br>`"string"`: 字串（適用條件：`is`, `contains`, `matches`, `starts-with`, `ends-with`）<br><br>`"duration"`:以秒為單位的持續時間（適用條件：`is`, `greater-than`, `less-than`） |
| 資料類型解譯的功能 | `"boolean string"`、`"restricted string"`、`"md5"`、`"IP"`、`"sha256"` 和 `"base64Binary"` 資料類型被解譯為字串。<br><br>當 `int` 和 `date` 資料類型的“`Content`”設定以間隔的形式設定時，應用程式支援其解譯：<br><br>OpenIOC 1.0:<br>使用“`TO`”欄位中的“`Content`”運算子：<br>`<Content type="int">49600 TO 50700</Content>`<br>`<Content type="date">2009-04-28T10:00:00Z TO 2009-04-28T16:00:00Z</Content>`<br>`<Content type="int">[154192 TO 154192]</Content>`<br>OpenIOC 1.1:<br>使用“`greater-than`”和“`less-than`”條件<br>使用“`TO`”欄位中的“`Content`”運算子<br>應用程式支援對 `date` 和 `duration` 資料類型的解釋（如果指標設定為 `ISO 8601, Zulu time zone, UTC` 格式）。 |

# 附錄 11。應用程式元件規則中的使用者帳戶

若要配置某些應用程式元件，您必須新增特殊規則。例如，對於 Web 控制，您必須新增包含您希望應用程式封鎖的網址清單的規則。在應用程式元件規則中，您還可以配置元件的排程或選擇應用程式必須對其套用規則的使用者。

必須新增規則來配置以下應用程式元件：

- 應用程式控制。
- Web 控制。
- 裝置控制。
- 記錄檢查。
- 適應性異常控制。
- 系統完整性監控。

從 Kaspersky Endpoint Security for Windows 12.5 開始，您不僅可以從 Active Directory 選擇使用者，還可以從卡巴斯基安全管理中心的使用者清單中選擇使用者。您還可以手動輸入本機使用者帳戶資料。這意味著您可以透過以下方式新增使用者：

- Active Directory（推荐）
- 卡巴斯基安全管理中心中的使用者清單
- 本機使用者帳戶

為了正確利用所有使用者分類方法，您需要將 Kaspersky Endpoint Security 應用程式和管理外掛程式升級到 12.5 或更高版本。

卡巴斯基建議僅在無法使用網域使用者帳戶的特殊情況下使用本機使用者帳戶。使用本機帳戶的安全風險請參見微软知識庫。如果使用本機使用者帳戶，您將對電腦的安全承擔全部責任；特別是，這包括控制和限制對 Kaspersky Endpoint Security 設定進行存取的責任。

應用程式使用使用者的 SID（安全識別符）來識別使用者。當使用 Active Directory 或卡巴斯基安全管理中心使用者清單中的使用者帳戶時，應用程式會確定管理伺服器上的 SID。這意味著應用程式不會為了識別使用者而給電腦帶來額外負載。如果您向應用程式規則新增了超過 1000 個本機使用者帳戶，應用程式將聯絡網域控制器來識別使用者。這意味著電腦的負載增加了。為了最佳化對電腦效能的影響，我們建議使用 Active Directory 或卡巴斯基安全管理中心使用者清單中的使用者帳戶。

應用程式使用 NetBIOS 名稱來識別手動新增的 `<username>` 和 `<hostname>\<username>` 格式的使用者帳戶。NetBIOS 名稱的長度最多可達 16 個位元組（15 個字元）。如果電腦名稱長度超過 15 個字符，應用程式將無法識別使用者。然後應用程式將停用規則並產生錯誤，例如，*Web 控制：已為沒有匹配安全識別碼 (SID) 的使用者帳戶停用規則觸發*。為了使規則起作用，您必須手動縮短電腦名稱。您可以從 Active Directory 或卡巴斯基安全管理中心新增使用者帳戶。在這種情況下，應用程式會自動縮短電腦名稱。

Kaspersky Endpoint Security 也支援規則中的內建使用者和群組（例如"All"群組）。由於使用者 SID 的確定方式，應用程式僅允許使用從 Active Directory 或卡巴斯基安全管理中心中的使用者清單新增的內建使用者帳戶。本機新增內建使用者帳戶的規則不起作用。

# 附錄 12。EDR 威脅回應的 API

Kaspersky Endpoint Security 12.9 for Windows 引入了使用 卡巴斯基安全管理中心 API 對 EDR 威脅回應操作的支援 (EDR responses)。也就是說，您可以呼叫 OpenAPI 方法使用 Python 自動化 EDR 威脅回應。當與 SIEM 解決方案整合時，您可以呼叫這些方法。*卡巴斯基統一監控與分析平台*（卡巴斯基 SIEM 解決方案）從 3.4.1 版本開始支援 EDR 威脅回應 OpenAPI。有關範例指令碼，請參閱 KUMA 文件。

若要執行 EDR 威脅回應操作，您需要建立一個請求並使用 KSC Open API (`AddIncident`) 傳送它。處理請求後，將在卡巴斯基安全管理中心主控台中建立特殊工作。

若要在回應 EDR 威脅時建立工作，您必須在管理伺服器和卡巴斯基安全管理中心網頁主控台之間建立背景連線。背景連線服務在卡巴斯基安全管理中心 Windows 14.2 或更高版本以及卡巴斯基安全管理中心 Linux 15.2 或更高版本中可用。其他主控台（包括 Kaspersky Detection and Response 解決方案的主控台）不受支援。

對於 EDR 威脅回應，您需要以 JSON 格式指定基本請求參數，例如：

- `task` 是工作的類型（見下文）。
- `targetHost` 是必須執行指令碼的電腦的 ID。必需參數。指令碼從事件中取得此參數。
- `responseEventIncidentArea` 是執行指令碼的應用程式的名稱（例如，`KUMA`）。此參數會被新增到所建立工作的名稱中。

要配置 EDR 威脅回應，您需要以 JSON 格式在 `"KLINCDT_BODY": json.dumps(data)` 參數中指定工作設定。結果，應用程式在卡巴斯基安全管理中心主控台中建立 `[Response][KUMA] <task type> - <Date> <Time> - <ID>`。

## 連線到卡巴斯基安全管理中心 OpenAPI

作為 EDR 威脅回應的一部分，該應用程式可在卡巴斯基安全管理中心主控台中建立特殊工作。建立這些工作需要在電腦和卡巴斯基安全管理中心之間建立連線。為此，必須在請求中指定卡巴斯基安全管理中心連線參數。

卡巴斯基安全管理中心連線參數

| 參數 | 類型 | 描述 |
|---|---|---|
| `kscHost` | `string` | 卡巴斯基安全管理中心管理伺服器位址。必須參數。 |
| `kscPort` | `int` | 管理員伺服器連線連接埠。必須參數。 |
| `kscCert` | `string` | 用於連線到卡巴斯基安全管理中心管理伺服器的憑證檔案的路徑。預設情況下，參數被設為 `False`。 |
| `kscUser` | `string` | 使用者帳戶名稱。必須參數。 |
| `kscPassword` | `string` | 使用者帳戶密碼。必須參數。 |

範例

```
# KSC connection info
# reads Environment variables by default, change with corresponding values
# KSC host, string, required
kscHost = "kscHost"
# KSC port, required, default is "13299"
kscPort = "13299"
# KSC certificate file path, default is False
kscCert = False
# KSC user, string, required
kscUser = "kscUser"
# KSC password, string, required
kscPassword = "kscPassword"

server_url = 'https://' + kscHost + ':' + str(kscPort)
    server = KlAkAdmServer.Create(
        server_url, kscUser, kscPassword, verify=kscCert)

    params = validate(args)

    data = {"targetHost": <MyHost>,
            "task": task,
            "params": params,
            "responseEventIncident": True,
            "responseEventIncidentArea":"Kuma"}

    oHostGroup = KlAkHostGroup(server)

    incdnt = oHostGroup.AddIncident({"KLINCDT_SEVERITY": 2,
                                     "KLINCDT_ADDED": paramDateTime(datetime.datetime.now()),
                                     "KLINCDT_BODY": json.dumps(data),
                                     "KLHST_WKS_HOSTNAME":  args.targetHost}).RetVal()

    oHostGroup.UpdateIncident(incdnt, {"KLINCDT_IS_HANDLED": False,
                                       "KLHST_WKS_HOSTNAME":  args.targetHost})
```

使用者帳戶資料不受保護，因此您需要指定一個單獨的使用者來執行這些操作。

## 獲取檔案 – getFile

獲取檔案工作設定

| 參數 | 類型 | 描述 |
| --- | --- | --- |
| md5hash | `string` | 您想要取得的檔案的 MD5 雜湊值。 |
| sha256hash | `string` | 您想要取得的檔案的 SHA256 雜湊值。 |
| path | `string` | 您想要取得的檔案的路徑。 |

範例

```
type getFile = {
  task: 'getFile';
  targetHost: string;
  params: {
    // an empty string or a valid md5 hash of the file
    md5hash: string;
    // an empty string or a valid sha256 hash of the file
    sha256hash: string;
    // the path to the file
    path: string;
  };
  responseEventIncidentArea: string;
};
```

## 刪除檔案 – deleteFile

刪除檔案工作設定

| 參數 | 類型 | 描述 |
| --- | --- | --- |
| md5hash | string | 您要刪除的檔案的 MD5 雜湊值。 |
| sha256hash | string | 您要刪除的檔案的 SHA256 雜湊值。 |
| path | string | 您要刪除的檔案的路徑。 |
| searchInSubfolders? | boolean | 在子資料夾中搜尋要刪除的檔案。 |

範例

```
type deleteFile = {
  task: 'deleteFile';
  targetHost: string;
  params: {
    // an empty string or a valid md5 hash of the file
    md5hash: string;
    // an empty string or a valid sha256 hash of the file
    sha256hash: string;
    // the path to the file
    path: string;
    // recursive search for a file (subfolder), optional
    searchInSubfolders?: boolean;
  };
  responseEventIncidentArea: string;
};
```

## 移動檔案到隔離區 – quarantineFile

移動檔案到隔離區工作設定

| 參數 | 類型 | 描述 |
| --- | --- | --- |
| md5hash | string | 您要隔離的檔案的 MD5 雜湊值。 |
| sha256hash | string | 您要隔離的檔案的 SHA256 雜湊值。 |
| path | string | 您想要隔離的檔案的路徑。 |

範例

```
type quarantineFile = {
  task: 'quarantineFile';
  targetHost: string;
  params: {
    // an empty string or a valid md5 hash of the file
    md5hash: string;
    // an empty string or a valid sha256 hash of the file
    sha256hash: string;
    // the path to the file
    path: string;
  };
  responseEventIncidentArea: string;
};
```

## IOC 掃描 – iocScan

IOC 掃描工作設定

| 參數 | 類型 | 描述 |
| --- | --- | --- |
| ioc | `string` | 您想要用於掃描的包含 IOC 檔案的 ZIP 壓縮檔案路徑。 |
| isolateHost | `boolean` | 當偵測到入侵指標時將電腦與網路隔離，以防止威脅蔓延。 |
| scanCriticalAreas | `boolean` | 當偵測到入侵指標時執行 *關鍵區域掃描*工作。 |
| quarantineObject | `boolean` | 當偵測到入侵指標時刪除惡意物件。在刪除物件之前，Kaspersky Endpoint Security 會建立備份副本以防物件以後需要還原。Kaspersky Endpoint Security 會將備份副本移動到隔離。 |

範例

```
type iocScan = {
  task: 'iocScan';
  targetHost: string;
  params: {
    // the path to the zip archive with ioc files in base64 encoding
    ioc: string;
    // isolation of the computer from the network
    isolateHost: boolean;
    // critical areas scan
    scanCriticalAreas: boolean;
    // quarantine the file
    quarantineObject: boolean;
  };
  responseEventIncidentArea: string;
};
```

## 啟動處理程序 – startProcess

啟動處理程序工作設定

| 參數 | 類型 | 描述 |
| --- | --- | --- |
| executablePath | `string` | 用於啟動處理程序的可執行檔的路徑。 |
| arguments? | `string` | 用於啟動處理程序的附加命令列參數。 |
| workingFolder? | `string` | 處理程序工作資料夾的路徑。 |

範例

```
type startProcess = {
  task: 'startProcess';
  targetHost: string;
  params: {
    // the path to the file
    executablePath: string;
    // command line arguments, optional
    arguments?: string;
    // a working folder, optional
    workingFolder?: string;
  };
  responseEventIncidentArea: string;
};
```

## 停止處理程序 – terminateProcess

停止處理程序工作設定

| 參數 | 類型 | 描述 |
| --- | --- | --- |
| md5hash | string | 您想要終止其處理程序的檔案的 MD5 雜湊值。 |
| sha256hash | string | 您想要終止其處理程序的檔案的 SHA256 雜湊值。 |
| path | string | 您要刪除的檔案的路徑。 |
| caseSensitive | boolean | 搜尋文件時區分大小寫。 |

範例

```
type terminateProcess = {
  task: 'terminateProcess';
  targetHost: string;
  params: {
    // an empty string or a valid md5 hash of the file
    md5hash: string;
    // an empty string or a valid sha256 hash of the file
    sha256hash: string;
    // the path to the file
    path: string;
    // case sensitive of the file name
    caseSensitive: boolean;
  };
  responseEventIncidentArea: string;
};
```

## 電腦網路隔離 – isolateHost

電腦網路隔離設定

| 參數 | 類型 | 描述 |
| --- | --- | --- |
| action | string | 網路隔離的操作模式。 |

範例

```
type isolateHost = {
  task: 'isolateHost';
  targetHost: string;
  params: {
    // 0 - turning off network isolation, 1 - turning on network isolation
    action: number;
  };
  responseEventIncidentArea: string;
};
```

## 執行防護 – – preventExecution

執行防護設定

| 參數 | 類型 | 描述 |
| --- | --- | --- |
| hash | `string` | 您想要阻止執行的檔案的 MD5 雜湊值。 |
| path | `string` | 您想要阻止執行的檔案的路徑。 |
| caseSensitive | `boolean` | 搜尋文件時區分大小寫。 |

範例

```
type preventExecution = {
  task: 'preventExecution';
  targetHost: string;
  params: {
    // a valid md5 hash of the file
    hash: string;
    // the path to the file
    path: string;
    // case sensitive of the file name
    caseSensitive: boolean;
  };
  responseEventIncidentArea: string;
};
```

## 惡意軟體掃描 – onDemandScan

惡意軟體掃描工作設定

| 參數 | 類型 | 描述 |
| --- | --- | --- |
| path | `string` | 自訂掃描的檔案和資料夾的空格分隔清單。 |
| recursive | `boolean` | 遞歸掃描模式。 |
| type | `number` | 掃描範圍。 |

```
ScanObjectType = Enum("ScanObjectType",
                      [
                          ("SystemMemory", 14),
                          ("StartupObjectsAndRunningProcesses", 15),
                          ("DiskBootSectors", 16),
                          ("SystemBackupStorage", 17),
                          ("Email", 18),
                          ("Folder", 22),
                          ("AllRemovableDrives", 23),
                          ("AllNetworkDrives", 24),
                          ("AllFixedDrives", 25)])
```

範例

```
type onDemandScan = {
  task: 'onDemandScan';
  targetHost: string;
  // please note, this is an array
  // array of scan object
  params: [{
    // enabling the scan object
    enabled: boolean;
    // an empty string or the path to the folder to scan
    path: string;
    // recursive scan mode
    recursive: boolean;
    // ID scan object
    type: number;
  }];
```

```
  responseEventIncidentArea: string;
};
```

# 有關協力廠商代碼的資訊

有關協力廠商代碼的資訊包含在本應用程式安裝資料夾中的 legal_notices.txt 內。

# 商標聲明

註冊商標及服務標誌均為其各自所有人的財產。

Adobe、Acrobat、Flash、Reader 和 Shockwave 是 Adobe 在美國和/或其他國家/地區的註冊商標或商標。

Amazon、Amazon Web Services、AWS 是 Amazon.com, Inc. 或其附屬公司的商標。

Apple、FireWire、iTunes、Mac 和 Safari 是 Apple Inc 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。

Bluetooth 文字、標誌和商標歸 Bluetooth SIG, Inc. 所有。

Borland 是 Borland Software Corporation 的商標或註冊商標。

Cisco、Cisco AnyConnect、IOS 是 Cisco Systems, Inc. 和/或其分支機構在美國和某些其他國家/地區的註冊商標或商標。

Citrix、Citrix Provisioning、Citrix Provisioning Services、Citrix Virtual Apps and Desktop、XenDesktop 和 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 Workers 和 Cloudflare 標誌是 Cloudflare, Inc. 在美國和其它司法區域的商標和/或註冊商標。

Core 是 Intel Corporation 或其子公司的商標。

dBase 是 dataBased Intelligence, Inc. 的商標

Dell Technologies、Dell、EMC 和其它商標是 Dell Inc. 或其子公司的商標。

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。

ESET 是 ESET spol. s r.o.或相應的 ESET 實體的商標或註冊商標。

Foxit 是 Foxit 公司的註冊商標。

Radmin 是 Famatech 的注冊商標。

Google、Android、Google Public DNS，Google Chrome 和 Chrome 是 Google LLC 的商標。

HUAWEI、FusionCompute 和 FusionSphere 是華為技術有限公司的商標。

ICQ 是 ICQ LLC 的商標和/或服務標章。

Intel 是 Intel Corporation 或其子公司的商標。

IBM 是 International Business Machines Corporation 在全球多個地區註冊的商標。

Lenovo 和 Lenovo ThinkPad 是聯想在美國和/或其他地區的商標。

Linux 是 Linus Torvalds 在美國和其他國家/地區的註冊商標。

Logitech 是 Logitech 在美國和/或其他國家/地區的注冊商標或商標。

LogMeIn Pro 和 Remotely Anywhere 是 LogMeIn，Inc. 的商標。

Mail.ru 是 Mail.Ru LLC 的註冊商標。

McAfee 是 McAfee LLC 或其子公司在美國和/或其它國家/地區的商標或者註冊商標。

Microsoft、Access、Active Directory、ActiveSync、Bing、BitLocker、Excel、Hyper-V、Internet Explorer、JScript、LifeCam Cinema、Microsoft Edge、MSDN、MS-DOS、MultiPoint、Office 365、Outlook、PowerPoint、PowerShell、Skype、SQL Server、Surface、Visual Basic、Visual FoxPro、Windows、Windows Live、Windows PowerShell、Windows Server 和 Windows Store 是 Microsoft 集團公司的商標。

Mozilla、Firefox 和 Thunderbird 是 Mozilla Foundation 在美國和其它國家/地區的商標。

NetApp 是 NetApp，Inc.在美國和/或其他國家/地區的商標或註冊商標。

OpenSSL 是 OpenSSL Software Foundation 擁有的商標。

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。

Realtek 是 Realtek Semiconductor Corporation 商標。

SAMSUNG 是 SAMSUNG 在美國或其他國家（地區）的商標。

Thawte 是 Symantec Corporation 或其分支機構在美國和其他國家（地區）的的商標或註冊商標。

Trend Micro 是 Trend Micro Incorporated 的商標或註冊商標。

VERISIGN 是 VeriSign，Inc.及其附屬公司在美國和其他地方的註冊商標或未註冊商標。

Vmware、VMware ESXi、VMware Horizon、VMware Workstation、VMware Tools、 VMware vSphere是 VMware, Inc. 在美國和其他國家的註冊商標或商標。